# UCC 5G SMF 構成および管理ガイド、リリース 2025.01

**最終更新**：2025 年 9 月 5 日


**シスコシステムズ合同会社**
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2025 Cisco Systems, Inc. All rights reserved.

# 目 次


はじめに：

このガイドについて lxxi

使用する表記法 lxxi

第 1 章

5G アーキテクチャ 1

機能の概要と変更履歴 1

要約データ 1

更新履歴 1

アーキテクチャの概要 2

コントロール プレーン ネットワーク機能 2

ユーザー プレーン ネットワーク機能 3

サブスクライバ マイクロサービスのインフラストラクチャのアーキテクチャ 4

コントロール プレーン ネットワーク機能アーキテクチャ 5

第 2 章

5G SMF の概要 9

機能の概要と変更履歴 9

要約データ 9

更新履歴 10

製品の説明 10

コンバージド コアの概要 11

サービス間ポッド通信 12

機能説明 12

機能の仕組み 13

機能設定 13

OAM サポート 14

ユースケースと機能 14
基本 SMF 構成 14
4G セッションのサポート 15
5G セッションのサポート 16
アクセスとモビリティのサポート 17
課金統合 17
クラウド ネイティブ インフラストラクチャ 18
コンバージド コア ネットワーク 18
IMS サポート 19
IPAM のサポート 19
合法的傍受 19
MVNO サポート 20
NF 管理 20
OAM サポート 20
ポリシー統合 21
RADIUS サポート 21
冗長性サポート 22
ローミングのサポート 22
SMF インライン サービス 22
SMF 仕様への準拠 23
サブスクリプション管理 23
UPF 統合 23
Wi-Fi サポート 23
展開アーキテクチャおよびインターフェイス 24
SMF アーキテクチャ 24
SMF の展開 24
コンバージド コア アーキテクチャ 25
コンバージド コア展開 26
サポートされるインターフェイス 27
データ パケットのライフサイクル 27
セッション アフィニティ 34

ライセンス情報 35
標準準拠 35

第 3 章 Ops センターを介した SMP の展開と構成 37
機能の概要と変更履歴 37
要約データ 37
更新履歴 37
機能説明 38
SMP Ops センター 38
前提条件 39
SMF の展開とアクセス 39
SMF の展開 40
SMF Ops センターへのアクセス 40
SMF サービスの構成 41
ノードラベルを持つマッピング ポッド 41
Day 1 構成のロード 42

第 4 章 スマートライセンス 43
機能の概要と変更履歴 43
要約データ 43
更新履歴 43
機能説明 44
Cisco Software Central 44
スマート アカウントとバーチャル アカウント 44
Cisco スマート アカウントの要求 45
SMF スマート ライセンス 46
ソフトウェアタグと権限付与タグ 46
スマート ライセンスの設定 47
CSC へのアクセス権を持つユーザー 47
CSC にアクセスできないユーザー 52
スマート ソフトウェア ライセンシングのモニタリングとトラブル シューティング 58

第 5 章 SMF ローリング ソフトウェアの更新 59
機能の概要と変更履歴 59
要約データ 59
更新履歴 59
機能説明 60
SMFを更新しています 61
SMI Cluster Manager を使用したローリング ソフトウェアの更新 61
前提条件 62
ローリング ソフトウェア アップグレードのトリガ 66
アップグレードのモニタリング 68
ポッド詳細の表示 69
ローリング アップグレード最適化 71
ローリング アップグレード最適化の仕組み 74
ポッドのアップグレード 74
ローリング アップグレード最適化サポートを利用したバージョンへのソフトウェアのアップグレード 78
制限事項 79
ローリング アップグレードのサポートされる機能の構成 79
ローリング アップグレード最適化の確認 80
OAM サポート 80
バルク統計 80
第 6 章 AN によって開始されたセッションの変更とリリース 83
機能の概要と変更履歴 83
要約データ 83
更新履歴 83
機能説明 84
機能の仕組み 84
第 7 章 Cisco Common Data Layer 91

機能の概要と変更履歴 91
要約データ 91
更新履歴 91
SMF の Cisco Common Data Layer の Geo 冗長性 92
アーキテクチャ 92
SMF での CDL の仕組み 93
コール フロー 94
CDL エンドポイント障害のコール フロー 94
制限事項 95
SMF Ops センターによる CDL の構成 96
CDL セッション データベースを構成して基本構成を定義する 96
CDLでの Zookeeper の構成 99
CDL セッション データベースの構成例 100
イベント トレース データの構成 100

第 8 章 コンテンツ フィルタリングと X-Header の強化 103
機能の概要と変更履歴 103
要約データ 103
更新履歴 103
機能説明 104
コンテンツ フィルタリング 104
機能説明 104
コンテンツフィルタリングの構成 104
アクティブ課金サービスでのコンテンツ フィルタリングの構成 104
ルールベースでのコンテンツ フィルタリングの構成 105
APN でのコンテンツ フィルタリングの構成 105
N7 インターフェイス上のコンテンツ フィルタリング ポリシー ID 105
X-Header の挿入 106
サポートされている X ヘッダー 情報 106

第 9 章 Diameter エンドポイント 109

機能の概要と変更履歴 109
要約データ 109
更新履歴 110
機能説明 110
サポートされるインターフェイス 111
Diameter エンドポイント インスタンス 111
Diameter クライアント プロファイル 111
Diameter エンドポイント プロファイル 112
ピア要求管理の切断 112
機能説明 113
DWR と DWA の処理 114
機能説明 114
機能の仕組み 114
アーキテクチャ 115
機能の仕組み 116
標準準拠 116
制限事項 116
Diameter エンドポイントの構成 116
Diameter エンドポイント インスタンスの構成 117
設定例 117
設定の確認 118
Diameter クライアント プロファイルの構成 118
設定例 119
設定の確認 119
Gx および Gy インターフェイスでの Diameter プロファイル エンドポイントの構成 120
設定例 124
設定の確認 125
DPR のビジー時間の構成 126
DPR の通話禁止時の構成 127
DPR のドレイン時間の構成 127
DPR の再起動時間の構成 128

ダイナミックな構成変更 128
機能説明 128
機能の仕組み 128
CCR の宛先ホスト AVP および宛先レルム AVP 130
機能説明 130
宛先ホスト AVP の構成 131
設定例 131
ピア管理 132
機能説明 132
ルート フラグ 132
ルート ステータス 133
ピア管理に関する考慮事項 133
ルートの選択 134
ルートソート順序 135
ホスト選択 135
機能説明 135
機能の仕組み 135
Diameter エンドポイントによるホスト選択の構成 136
ルート障害 137
機能説明 137
ルート障害の構成 137
バインドされたピア 139
機能説明 139
機能の仕組み 139
失敗のハンドリング（Failure Handling） 139
機能説明 139
機能の仕組み 140
障害処理の構成 141
障害処理プロファイルの構成 141
設定例 143
設定の確認 144

OAM サポート 145
バルク統計サポート 145
トラブルシューティング情報 155
プロトコルをモニタし、サブスクライバをモニタする 155
機能説明 155
機能の仕組み 156
モニタ サブスクライバおよびモニタ プロトコル サポートの構成 156
データ収集のデバッグ 157

第 10 章 DSCP マーキング 159
機能の概要と変更履歴 159
要約データ 159
更新履歴 159
機能説明 160
データパケットの DSCP マーキング 160
機能説明 160
データ パケットの DSCP マーキングの動作方法 160
5QI-QoS マッピングの構成 161
UP パケットの DSCP 構成の確認 162
コントロール プレーン シグナリングの DSCP マーキング 163
機能説明 163
制御シグナリングに対する DSCP マーキングの仕組み 163
制限事項 164
コントロール プレーン シグナリングの DSCP マーキングの構成 164
エンドポイントごとの DSCP マーキングの構成 165
インターフェイスごとの DSCP マーキングの構成 165
CP シグナリング メッセージの DSCP 構成 166
DSCP マーキングの OAM サポート 166
Monitoring Support 166

第 11 章 BGP を使用したダイナミック ルーティング 167

機能の概要と変更履歴 167
要約データ 167
更新履歴 167
機能説明 168
機能の仕組み 168
外部ネットワーク障害 170
Geo スイッチオーバー 171
内部ネットワーク障害 171
ローカル スイッチオーバー 172
リカバリとフェールバック 172
コール フロー 172
アクティブ/スタンバイ モードでの着信トラフィックのルートの公開 172
シングル プロトコル ポッド障害コール フロー 174
発信トラフィック コール フローのルートの学習 175
BGP を使用したダイナミック ルーティングの構成 177
モニタリングおよびトラブルシューティング 180

第 12 章 緊急 SoS サポート 185
機能の概要と変更履歴 185
要約データ 185
更新履歴 185
SoS 緊急サービスの LTE へのフォールバック 186
機能説明 186
機能の仕組み 186
コール フロー 186
緊急 SoS サポートの構成 189
ローカル認証の構成 189
セカンダリ認証の構成 190
課金障害処理の構成 190
緊急サービス サポート 191
機能説明 191

機能の仕組み 191
緊急サービス サポートの構成 194
DNN プロファイルでのデフォルトのフロー専用タイマーの構成 194
緊急 DNN の構成 194
緊急DNNの確認 195
緊急サービスの OAM サポート 196
バルク統計サポート 196

第 13 章 EPS インターワーキング 197
機能の概要と変更履歴 198
要約データ 198
更新履歴 198
機能説明 200
アーキテクチャ 201
機能の仕組み 203
標準準拠 205
UE 初期接続のサポート 205
機能説明 205
機能の仕組み 206
コール フロー 206
UE 初期接続の構成 212
SMF プロファイル構成で FQDN を定義する 212
S5 バインディング アドレスの構成 212
GTP エンドポイント パラメータの構成 213
CSR での APN-AMBR の構成 214
PCRF、PCF、および OCS インターフェイスの構成 214
UE 初期接続構成の確認 215
OAM サポート 216
show コマンドのサポート 216
SMF での EPS の切り離し手順 217
機能説明 217

機能の仕組み 217
専用ベアラーのアクティブ化と非アクティブ化 227
機能説明 227
機能の仕組み 227
EPS フォールバック 235
機能説明 235
機能の仕組み 235
EPS フォールバック トリガ原因の構成 238
間接データ転送トンネル（IDFT）タイマーのサポート 238
機能説明 238
機能の仕組み 239
コール フロー 239
IDFT タイマーの構成 243
EPS フォールバック ガード タイマーのサポート 244
機能説明 244
機能の仕組み 244
標準準拠 246
EPS フォールバック ガード タイマーの構成 246
EPS フォールバック レポートの生成 247
機能説明 247
機能の仕組み 248
コール フロー 248
SMF での EPS セッションのベアラー変更 250
機能説明 250
機能の仕組み 251
標準準拠 267
EPS および 5GC インターワーキングのセッション管理手順 267
機能説明 267
機能の仕組み 270
コール フロー 270
標準準拠 296

5G PDU セッション パラメータからの EPS PDN 接続パラメータの生成 296
N26 インターフェイスを使用する 5G から EPS へのハンドオーバー 298
機能説明 298
機能の仕組み 298
標準準拠 300
専用ベアラの作成に対する遅延および再試行のサポート 301
機能説明 301
機能の仕組み 301
コール フロー 301
専用ベアラー作成の遅延および再試行のサポートの構成 303
タイマーの期限切れによる専用ベアラー手順エラーの処理 304
機能説明 304
機能の仕組み 305
コール フロー 305
専用ベアラー手順障害処理機能の構成 311
手順 SLA タイマーの構成 311
専用ベアラー手順障害処理機能の認証 312
専用ベアラ手順失敗処理機能の OAM サポート 312
バルク統計サポート 312
トラブルシューティング情報 312
4G セッションの GTP-U エラー通知の処理 313
機能説明 313
標準準拠 314
機能の仕組み 314
GTP-U エラー処理手順 314
Diameter インターフェイスでの GTP-U エラーの表示 316
GTP パス障害の処理、復元、およびリカバリ 317
機能説明 317
コール フロー 317
GTP-C パス管理 318
GTP-C エコー要求の処理 319

PGW-C/SMF での GTP-C 復元 319
メモリおよびパフォーマンスの影響 320
GTP エンド ポイントでのエコーの構成 320
設定例 320
コマンドの表示 321
バルク統計 321
制限事項 322
GTP-C サービスのモニターとトラブルシューティング 323
機能説明 323
GTP-C テスト エコー コマンドの使用 323
4G 専用デバイスを拒否するための構成サポート 324
変更通知要求の処理 325
機能説明 325
ULI の変更による変更通知 325
ULI の変更がない変更通知 327
コール フロー 327
ULI の変更による変更通知 327
ULI の変更がない変更通知 329
ダイナミックな構成変更のサポート 330
機能説明 330
機能の仕組み 330
アクセスプロファイル 330
4G および 5G のセマンティックおよび構文エラー処理 332
機能説明 332
原因の処理 334
セマティックおよび構文エラー処理の構成 335
設定例 337
バルク統計サポート 338

第 14 章 イベント詳細レコード 339
機能の概要と変更履歴 339

要約データ 339
更新履歴 340
機能説明 340
EDR トランザクション ファイル 343
手順レベルの EDR 生成 345
EDR トランザクションコリジョン 391
EDR 属性 393
制限事項 401
EDR の構成 402
EDR レポートの構成 402
EDR ファイルの生成の構成 403
EDR パラメータの構成 404
EDR トランザクションを確認する 407
EDR ロギングの OAM サポート 408
バルク統計サポート 408

第 15 章 障害処理サポート 411
機能の概要と変更履歴 411
要約データ 411
更新履歴 412
機能説明 412
アクセスおよびモビリティ管理機能の障害処理 413
機能説明 413
機能の仕組み 413
要求メッセージの再送信の構成 413
設定例 414
充電機能の失敗の処理 415
機能説明 415
機能の仕組み 416
CHF サーバ障害の処理 416
オフライン CHF サーバへのリレー 417

HTTP 原因コードと失敗アクションのマッピング 417
アプリケーション エラー コードベースの障害処理 418
料金設定グループレベルの失敗の処理 418
コール フロー 419
障害アクションに対する SMF の動作 423
標準準拠 424
制限事項 424
CHF 障害処理の構成 424
障害処理プロファイルの構成 425
オフライン サーバ クライアントとオフライン障害処理プロファイルの構成 426
グループレベルおよびアプリケーションレベルのエラーの評価に対するアクションの構成 426
ネットワーク リポジトリ機能障害処理 427
機能説明 427
機能の仕組み 427
通話フロー 429
NRF 障害処理の構成 431
障害処理テンプレートの構成 431
障害処理の構成アクション 434
NRF 登録フェールオーバー オプションの構成 437
ネットワーク要素プロファイルの障害処理の構成 438
設定例 438
NRF 障害処理の確認 440
NF 管理の障害処理 440
NF 検出の障害処理 441
ポリシー制御機能の失敗の処理 442
機能説明 442
機能の仕組み 443
PCF 障害処理機能の構成 444
PCF 障害処理プロファイルの構成 445
障害処理プロファイルの 関連付けの構成 446

セカンダリおよびターシャリ IP アドレスの構成 446
PCF 障害処理に対する OAM サポート 447
バルク統計サポート 447
統合データ管理の失敗の処理 448
機能説明 448
機能の仕組み 448
UDM 障害処理機能の構成 451
UDM 障害処理プロファイルの構成 451
FH プロファイルの関連付けの構成 452
セカンダリおよびターシャリ IP アドレスの構成 453
応答タイムアウトパラメータの構成 454
統計 454
UDM 障害処理機能の OAM サポート 454
バルク統計サポート 454
ユーザー プレーン機能障害の処理 456
UPF 障害処理方法 456
UPF 障害処理を有効にする 457
UPF 障害処理プロファイルの構成 457
障害プロファイルの関連付けの構成 461
UPF 障害処理の統計 462

第 16 章
アクセスおよびモビリティの手順のフロー失敗の処理 463
機能の概要と変更履歴 463
要約データ 463
更新履歴 463
機能説明 464
機能の仕組み 464
コール フロー 464
XN ハンドオーバー中の QoS フロー障害処理 465
N2 ハンドオーバー中の QoS フロー障害処理 467
N26 4G から 5G へのハンドオーバー中の QoS フロー障害の処理 470

サービス要求手順の QoS フロー障害 473
PDU UE 同期手順 475
PDU セットアップ手順中の失敗した QoS フロー識別子の処理 478
PDU セッション変更中に失敗した QoS フロー識別子の処理 480
フロー障害管理コール フロー 483
標準準拠 488

第 17 章 GTPP エンドポイント 489
機能の概要と変更履歴 489
要約データ 489
更新履歴 489
機能説明 490
課金関連の転送 490
GTPP を介した CDR トランスポート 490
パス プロトコル 491
GTPP メッセージ タイプ 491
エンドポイント GTP Prime 492
GTPP レジリエンシ 492
CDR アーカイブ 492
CDR ファイル ストレージ 493
情報要素サポート 493
標準準拠 494
制限事項 494
GTPP プロファイルの構成 495
GTPP プロファイルの確認 497
GTPP エンドポイントの構成 498
GTPP エンドポイントの確認 499
GTP Prime プライム 構成の確認 499
GTPP サービスのモニターとトラブルシューティング 500
機能説明 500
GTPP テスト エコー コマンドの使用 500

第 18 章 ハンドオーバー手順 503

機能の概要と変更履歴 503

要約データ 503

更新履歴 503

機能説明 504

4G から 5G へのデータ セッションのハンドオーバー 504

機能説明 504

機能の仕組み 505

アーキテクチャ 506

コール フロー 507

標準準拠 520

制限事項 520

アクセスとモビリティの手順のための CHF と PCF の統合 521

機能説明 521

機能の仕組み 522

コール フロー 523

標準準拠 532

gNodeB 間ハンドオーバー 533

機能説明 533

機能の仕組み 533

コール フロー 533

制限事項 548

OAM サポート 548

統計情報サポート 548

Wi-Fi ハンドオーバー 549

機能説明 549

アーキテクチャ 550

標準準拠 554

機能の仕組み 554

EPC から非 3GPP への信頼できない Wi-Fi ハンドオーバー コール フロー 554

非 3GPP 信頼できない Wi-Fi から EPC へのハンドオーバー コール フロー 558
EPS フォールバック コール フローによる非 3GPP 信頼できない Wi-Fi から 5GS へのハンドオーバー 562
非 3GPP 信頼できない Wi-Fi から 5GS へのハンドオーバー コール フロー 571
5GS から非 3GPP への信頼できない Wi-Fi ハンドオーバー コール フロー 575
非信頼 3GPP LTE から WiFi へのハンドオーバー 580
GTPC の IE サポート 582
代替 RAT トンネル作成コール フローによる Wi-Fi から 5G へのハンドオーバー 583
代替 RAT トンネル作成コール フローによる 5G から Wi-Fi へのハンドオーバー 584
Wi-Fi ハンドオーバーの構成 586
コンプライアンス プロファイルの構成 586
ハンドオーバー通知を伴うコールの構成 587

第 19 章

**音声用の IMS PDU セッション 589**
機能の概要と変更履歴 589
要約データ 589
更新履歴 589
機能説明 590
LTE の音声サポート 590
機能説明 590
機能の仕組み 590
VoLTE および緊急コールの優先順位付けの構成 602
標準準拠 602
制限事項 602
VoLTE および VoNR の NPLI サポート 603
機能説明 603
アーキテクチャ 604
コール フロー 604
標準準拠 604
VoWi-Fi サポート 604
機能説明 604

アーキテクチャ 604
機能の仕組み 605
コール フロー 605
標準準拠 611
制限事項 611
音声の新しいラジオ 611
機能説明 611
標準準拠 612
DNS プロキシを使用したアドレス解決 612
機能説明 612
アドレス解決のための DNS プロキシの構成 612
DNS からの P-CSCF アドレスのランダム化 615
DNS テスト クエリ 616
ローカル構成を使用したアドレス解決 618
P-CSCF アドレスの選択メカニズム 618
アドレス解決のための P-CSCF サーバの構成 619
P-CSCF アドレスの再選択と復元 622
機能説明 622
機能の仕組み 622
P-CSCF の復元と再選択の構成 624
Gm および Mw インターフェイスのマッピング構成 625
失敗した P-CSCF をオンラインにマークする構成 626
OAM サポート 626
VoNR MO と MT コール サポート 627
機能説明 627
VoNR ページング ポリシー差別化 637
機能説明 637
VoNR ページング プロファイル差別化の構成 640

第 20 章 インターフェイス サポート 643
機能の概要と変更履歴 643

要約データ 643
更新履歴 644
機能説明 647
SMF インターフェイスの 3GPP 仕様コンプライアンス 649
機能説明 649
URI バージョン選択ロジック 649
標準準拠 650
インターフェイスの 3GPP 仕様コンプライアンスの構成 652
設定の確認 655
サポートされている SMF インターフェイス 655
GTP インターフェイス 656
GTP 原因コードの処理 656
GTPv2 IE および原因コード 664
Gx インターフェイス 667
機能説明 667
機能の仕組み 667
Gx 初期接続とデタッチ サポート 669
Gx の発信元ホストと発信元レルム 672
ダイナミックおよび事前定義済みのルール サポート 672
Gy インターフェイス 674
Gy 使用状況レポート 674
Gy 障害処理 683
Gy MSCC レベルの失敗結果コード 693
Gy Quota Validity Time（QVT）と Quota Holding Time（QHT） 697
Gy Tarif 時間のサポート 700
Gy の発信元ホストと発信元レルム 701
Diameter インターフェイスを介した保留中のトラフィック処理 702
ルーティング データのサポート 702
Gz インターフェイス 703
Gz インターフェイスを使用した PDN 接続および接続解除 704
Gz 使用状況レポート 714

ベアラー要求トリガの変更の処理 731
Gz デフォルト ベアラーの変更 747
セカンダリ RAT の使用状況に関する定期レポートの処理 762
EGCDR 最終レコード終了原因のサポート 769
ゼロ ボリュームで CDR を抑制 770
N1/NAS インターフェイス 771
無効なプロトコル データの処理に対する NAS メッセージのコンプライアンス 771
5GSM 原因コードの処理 773
N2/NGAP インターフェイス 779
N2 原因および診断 IE サポート 780
N4 インターフェイス 792
N4 Over IPSec 792
ユーザー プレーン整合性保護 797
ユーザー プレーンの機密性保護 807
SMF での UPCP および UPIP 機能の非アクティブ化 816
N7 インターフェイス 817
HTTP エラー コードによるエラー処理 817
構成ベースの PCF メッセージの制御 823
N10 インターフェイス 826
構成ベースの UDM メッセージの制御 826
3GPP リリース 16 準拠の N10 属性 829
UDM サブスクリプション S-NSSAI に対する S-NSSAI の検証 829
N11 インターフェイス 832
ProblemDetails JSON オブジェクト 832
原因情報要素 843
N16 インターフェイス 854
ProblemDetails JSON オブジェクト 854
N40 インターフェイス 861
Nnrf インターフェイス 861
NRF メッセージの構成ベースの制御 862
RADIUS インターフェイス 864

S2b インターフェイス 865
S5 インターフェイス 865
SBA インターフェイス 865
TLS を使用した HTTP/2 865
SCP インターフェイス 869
SCP モデル D による NF の間接通信 872
FQDN の概要 881
FQDN：制限事項 882
FQDN の構成 882
ピア通信用 FQDN の構成 883
障害処理の構成 884
SMF FQDN の構成 885
OAM サポート 885
バルク統計サポート 885
インターフェイスの設定 887
設定例 888
設定の確認 890
OAM サポート 891
バルク統計サポート 891

第 21 章 IP アドレス管理 893
機能の概要と変更履歴 894
要約データ 894
更新履歴 895
機能説明 896
機能の仕組み 897
SMF 内の IPAM 統合 897
機能説明 897
アーキテクチャ 898
IPAMの統合 898
IP 割り当ての送信元 898

コンポーネント 898
機能の仕組み 899
コール フロー 899
IPAM の構成 901
IPv4 アドレス範囲の構成 902
IPv6 アドレス範囲の構成 903
IPv6 プレフィックス範囲の構成 904
ネクスト ホップ転送アドレスを使用した IPv4 アドレスとプレフィックス範囲の設定 905
ネクスト ホップ転送アドレスでの IPv6 アドレス範囲の構成 906
SMF タグの構成 908
IPv4 アドレス範囲のしきい値の構成 909
IPv6 アドレス範囲のしきい値の構成 910
IPv6 プレフィックス範囲のしきい値の構成 910
IPv4 アドレス範囲分割の構成 911
IPv6 アドレス範囲分割の構成 912
グローバルなしきい値の構成 913
IPAM 送信元の構成 914
IPAM 統合構成の確認 914
データ プレーンの詳細の確認 914
データ プレーンのしきい値の確認 915
データ プレーンに割り当てられた IPv4 アドレス範囲の確認 915
データ プレーンに割り当てられた IPv6 アドレス範囲の確認 915
IP プール選択方法の構成 916
UPF グループ プロファイルの IP プール 選択の構成 916
IP プール選択用のスライス グループ リストの構成 917
静的 IP サポート 918
機能説明 918
機能の仕組み 920
コール フロー 923
DNN の追加 924

静的 IP アドレス範囲の追加 925
静的 IP プールの追加 925
UPF の追加 926
UPF の削除 926
静的 IP アドレス範囲の削除 927
静的 IP プールの削除 927
オフライン UPF との Sx の関連付けの削除 927
UPF の Sx パス障害 928
制限事項 928
静的 IP の構成 929
スタティック IP プールの構成 929
重複静的 IP 検出の構成 929
統計情報サポート 932
IPAM によるデュアルスタック静的 IP サポート 933
機能説明 933
機能の仕組み 933
制限事項 934
デュアル スタック 静的 IP の構成 934
IPAM 分割なしの構成 934
IPAM オフライン モードのサポート 935
機能説明 935
機能の仕組み 935
IPAM オフライン モードに構成 936
オフライン モードにプールを構成 936
IPv4 アドレス範囲をオフライン モードに設定 936
オフライン モードへの IPv6 プレフィックス範囲の設定 937
UPF ごとの IPAM 冗長性サポート 938
機能説明 938
機能の仕組み 938
IPAM 隔離タイマー（IPAM Quarantine Timer） 939
機能説明 939

IPAM 隔離タイマーの構成 939
IPAM 隔離タイマーの構成 939
IPAM 隔離タイマーの構成 940
システム診断の IP 検証 940
統計 940
IPAM データの照合 941
機能説明 941
IPAM 調整のトリガー 941
インスタンス レベルでの IPAM 調整のトリガ 942
プール レベルでの IPAM 調整のトリガ 942
チャンク レベルでの IPAM 調整のトリガー 942
IPAMの定期的調整 942
制限事項 943
機能設定 943
設定例 944
IPv6 プレフィックス委任 945
IPv6 プレフィックス委任の仕組み 947
IPv6 プレフィックス委任の割り当て 947
プロファイル DNN を構成 949
IPAM の構成 950
ローカル プールからのプレフィックス委任を確認 951
ipam pool を表示 951
メトリック 952
IPAM の隔離 Qsize の構成 952
IPAM 隔離キュー サイズの構成 952
IP アドレス プールをオーバーラップ 953
機能説明 953
重複する IP アドレス プールの構成 953
使用率の低い IP チャンクの自動再利用 954
機能説明 954
制限事項 954

十分に活用されていない IP チャンクのインスタント再利用プロセスの構成 955
設定例 955
十分に活用されていない IP チャンクの定期再利用プロセスの構成 955
設定例 956
設定の確認 956
OAM サポート 957
バルク統計 957
UPF の一意の IP プール 957
機能説明 957
一意の IP プールの SMF の構成 957
ロケーション DNN に基づくタグの構成 958
UPF フォールバックの有効化 958
設定例 958
SMF と UPF の間での IP チャンクの調整 961
機能説明 961
機能の仕組み 961
IP チャンクの調整を有効または無効にするための構成 962
設定例 963
OAM サポート 963
バルク統計 963
IP チャンク スロットリング 963
機能説明 963
機能の仕組み 964
制限事項 965
SMF での UPF の最大サポート セッションの構成 965
設定例 965
UPF ごとの vDNN ごとにサポートされる最大セッション数の構成 965
設定例 966
IP チャンク スロットリングの無効化 967
OAM サポート 967
メトリック 968

IPAM キャッシュ データ シャーディング 969
データ シャーディングの制限事項 970
IPAMデータ シャーディングの有効化 970
IP の割り当てと再利用 971
UE IP アドレスの保持および再利用の利点 972
ローリング アップグレードおよびダウングレード中の IP 再利用に関する注意事項 972
UE IP アドレスの保持と再利用に関する制限事項 972
保留状態時の接続または PDU セットアップの失敗の処理 973
IP 再利用の基準 974
SMF が UE IP アドレスの再利用を許可する仕組み 975
UE IP アドレスの保持と再利用の前提条件 975
IP再利用機能の有効化 976
コンバージド コアでのセッション ホールド タイマーの構成 976
DNN でのセッション ホールド タイマーの構成 977
IP 再利用機能のトラブルシューティング情報 978
コマンドの表示 978
clear コマンド 979
バルク統計情報出力 979
スイッチ制限を処理するためのルート集約 980
機能説明 980
機能の仕組み 980
チャンク グループのない古いプールからチャンク グループのあるプールへの移行 981
制限事項 982
チャンク グループ サイズを定義する IPv4 アドレス範囲の構成 982
設定例 983
設定の確認 984
チャンクグループを定義するための IPv6 プレフィックス範囲の構成 984
設定例 984
チャンク グループを定義するための IPv6 アドレス範囲の設定 985
設定例 985
IPv6 プレフィックス範囲とアドレス範囲の構成の確認 986

最大セッション サイズに基づく IP チャンクの事前割り当て 987
設定例 987
OAM サポート 988
メトリック 988
NAT のサポート 988
機能説明 989
機能の仕組み 989
コール フロー 989
NAT バインディング手順の PFCP IE 995
SMF でのネットワーク アドレス変換バインディング レコードの処理 997
NAT バインド手順の Radius AVP 997
制限事項 998
NAT バインディング更新の設定 998
OAM サポート 998
バルク統計 998
トラブルシューティング情報 999
UPF に割り当てられる IPv6 の範囲 999
UPF に割り当てられる IPv4 の範囲 1000
IP プール マッピング エラー ログ 1000
N4 リソースまたは関連付けをリリース 1001
機能説明 1001
機能の仕組み 1001
N4 リソースまたは関連付けのリリースの構成 1002
OAM サポート 1003
破損した IP チャンクの識別 1003
機能説明 1003
機能の仕組み 1003
OAM サポート 1004

第 22 章 **IPv6 PDU セッション 1005**
機能の概要と変更履歴 1005

要約データ 1005
更新履歴 1005
機能説明 1006
未承諾のルータ アドバタイズメント 1006
要請ルータ アドバタイズメント 1007
ルータ要請とルータ アドバタイズメントの構成 1007
ルータ アドバタイズメントのパラメータの構成 1008
仮想 MAC アドレスの構成 1009
ICMPv6 プロファイルと SMF サービス プロファイルの関連付け 1010

第 23 章 **MBR 短回線の最適化 1011**
機能の概要と変更履歴 1011
要約データ 1011
更新履歴 1011
機能説明 1012
機能の仕組み 1012
制限事項 1013
MBR 短回線最適化のサポート 1013
統計 1013

第 24 章 **すべての UPF へのメッシュ接続 1015**
機能の概要と変更履歴 1015
要約データ 1015
更新履歴 1015
機能説明 1015

第 25 章 **PCO での MTU サポート 1017**
機能の概要と変更履歴 1017
要約データ 1017
更新履歴 1017
機能説明 1018

IPv4 リンク MTU の構成 1018
設定の確認 1019

第 26 章 DNN のサポート 1021
機能の概要と変更履歴 1021
要約データ 1021
更新履歴 1022
機能説明 1022
機能の仕組み 1023
制限事項 1024
仮想 DNN の構成 1024
サブスクライバ ポリシーの構成 1025
設定の確認 1026
オペレータ ポリシーの構成と DNN ポリシーの関連付け 1027
DNN ポリシーの構成 1027
DNN プロファイルでの 仮想 DNNの構成 1028
SMF サービスでのサブスクライバ ポリシーの関連付け 1030
SMF インスタンスに基づくネットワーク機能の選択 1031
機能説明 1031
SMF インスタンスの構成 1032
動的構成更新中に DNN プロファイルをオフライン モードに切り替える 1033
機能説明 1033
機能の仕組み 1033
DNN ポリシー 1034
DNN プロファイル 1034
サブスクライバ ポリシー 1035
制限事項 1035
オフライン DNN プロファイルを構成 1036
DNNプロファイルをオフライン モードに切り替える 1036
DNN プロファイルのオフライン モード構成の確認 1036
DNN プロファイルのオフライン モード設定の OAM サポート 1037

バルク統計サポート 1037
DNN 継承 1037
機能説明 1037
機能の仕組み 1037
DNN継承の構成 1041
DNN ごとの IP プールの割り当て 1042
機能説明 1042
機能の仕組み 1043
IP プールの割り当ての構成 1044
DNN ごとの IP プールの割り当て 1044
IP プール割り当ての構成の確認 1045
スライス および DNN ごとの IP プール割り当て 1045
機能説明 1045
機能の仕組み 1046
制限事項 1046
機能設定 1046
許可 NSSAI 値の構成 1046
スライスベースの IP プール割り当ての構成 1047

第 27 章
**複数 PLMN のサポート 1049**
機能の概要と変更履歴 1049
要約データ 1049
更新履歴 1049
機能説明 1050
機能の仕組み 1050
複数の PLMN の構成 1051
構成ベースのピア NF の選択 1051
PLMN ID の構成 1051
非標準 PLMN リストの構成 1052
非標準 PLMN リストの確認 1052
プライマリ PLMN の構成 1052

NRF 検出での PLMN の構成 1053
サービング PLMN MNC リストの構成 1053
オペレータ ポリシーのローマを構成 1054
複数の PLMN の OAM サポート 1054
バルク統計サポート 1054

第 28 章 非 3GPP アクセスのための N3IWF 1055
機能説明 1056
アーキテクチャ 1058
N3IWF の UE アイドル モード エントリ 1058
機能の仕組み 1059
コール フロー 1059
N3GA ロケーション パラメータ 1080
アクティブなベアラー機能を使用した N3IWF および HO サポートを使用した Wi-Fi 経由の音声またはビデオ通話 1082
N3IWF セッションの RAT タイプの処理 1082
標準準拠 1082
OAM サポート 1083

第 29 章 ネットワーク開始型セッション変更手順 1085
機能の概要と変更履歴 1085
要約データ 1085
更新履歴 1085
機能説明 1086
機能の仕組み 1086
コール フロー 1086
CM 接続状態のアクティブなユーザー プレーンと UE のネットワーク開始の変更コール フロー 1087
CM 接続状態の非アクティブなユーザー プレーンと UE に対してネットワークが開始した変更コール フロー 1088
非アクティブなユーザー プレーンと CM-Idle 状態の UE に対してネットワークが開始した変更コール フロー 1089

標準準拠 1091
OAM サポート 1091
バルク統計サポート 1091

第 30 章 新しい無線デュアル接続 1093
機能の概要と変更履歴 1093
要約データ 1093
更新履歴 1093
機能説明 1093
機能の仕組み 1094
コール フロー 1094

第 31 章 NF の検出と管理 1099
機能の概要と変更履歴 1099
要約データ 1099
更新履歴 1100
機能説明 1100
NF 管理 1101
機能説明 1101
登録 1101
NF 管理用の NRF エンドポイント プロファイル パラメータの構成 1102
最適化された NRF 登録要求メッセージを使用したスライス使用率の向上 1104
NRF による SMF の登録解除 1106
機能説明 1106
機能の仕組み 1106
NF ハートビート 1110
機能説明 1110
機能の仕組み 1110
NRF ハートビート 間隔を構成 1112
SMF サブスクリプションおよび通知の NRF サポート 1113
機能説明 1113

機能の仕組み 1114
サブスクリプションおよび通知の NRF の構成 1119
標準準拠 1120
NF プロファイルの更新 1120
機能説明 1120
機能の仕組み 1121
NF ディスカバリ 1123
機能説明 1123
機能の仕組み 1124
コール フロー 1124
標準準拠 1126
制限事項 1126
検出のために NRF を構成 1127
NRF を登録 1127
NRF の検出 1127
NF クライアント プロファイルを構成 1128
検出グループと NF タイプの関連付け 1129
NF ディスカバリ用の NRF エンドポイント プロファイル パラメータの構成 1130
NF タイプの局所性の構成 1132
SMF の地域の構成 1133
DNN の NF プロファイルの構成 1134
NF プロファイル内での局在性の定義 1134
NF クライアント プロファイルの NF エンドポイント プロファイル パラメータの構成 1135
ピア NF タイプごとの NRF の選択 1137
機能説明 1137
ピア NF タイプごとの NRF の選択の構成 1138
検出された NF プロファイルのキャッシング 1141
機能説明 1141
機能の仕組み 1142
NF 検出キャッシュの無効化（NF Discovery Cache Invalidation） 1143

代替 AMF の選択 1145
機能説明 1146
AMF クエリ パラメータの検出応答フィルタの構成 1146
ピア NF 管理の静的構成 1147
静的 IP アドレス サポートへのフォールバック 1147
機能説明 1147
機能の仕組み 1147
フォールバックから静的 IP アドレスへの構成 1150
NRF 障害の処理 1153
機能説明 1153

第 32 章 負荷および過負荷管理 1155
機能の概要と変更履歴 1155
要約データ 1155
更新履歴 1156
機能説明 1157
SBA インターフェイス過負荷制御 1158
機能説明 1158
機能の仕組み 1158
メッセージの優先順位 1158
エンドポイントでオーバーロード保護 1159
オーバーロードの防止の設定 1159
エンドポイント レベルで過負荷の防止の構成 1159
クライアント レベルでオーバーロードの防止の構成 1160
過負荷保護の構成の確認 1161
メッセージの優先順位の構成 1162
SBA インターフェイス メッセージの自己過負荷処理 1163
NRF への自己負荷情報の伝達 1163
SBI メッセージの自己過負荷スロットリングと除外 1163
制限事項 1164
GTP-C ロードおよびオーバーロード制御 1165

機能説明 1165
GTP-C 負荷制御 1166
GTP-C 過負荷制御 1166
メッセージ スロットリング 1167
過負荷ピア検出 1168
機能の仕組み 1169
標準準拠 1171
制限事項 1171
GTP-C ロードおよびオーバーロード制御の OAM サポート 1171
バルク統計サポート 1171
N4 インターフェイス負荷および過負荷制御 1173
N4 インターフェイスの負荷と過負荷のレポート 1173
N4 メッセージの自己過負荷スロットリングと除外 1174
N4 インターフェイスのピア負荷とオーバーロードの処理 1176
輻輳中のピアの N4 障害処理 1177
SMF での負荷および過負荷制御の構成 1177
負荷プロファイルの作成 1178
負荷プロファイルの構成の確認 1179
除外プロファイルの作成 1179
除外プロファイルの構成の確認 1180
過負荷プロファイルの作成 1180
過負荷プロファイルの構成の確認 1182
負荷プロファイルと過負荷プロファイルの関連付け 1184
負荷と過負荷プロファイルの関連付けの確認 1184
負荷係数の構成 1185
設定の確認 1186
ノード過負荷 1186
モニタリングおよびトラブルシューティング 1188
統計 1188

第 33 章 実行最適化サポート 1191

機能の概要と変更履歴 1191
要約データ 1191
更新履歴 1193
機能説明 1194
バッチ ID の割り当て、リリース、および調整のサポート 1194
機能説明 1194
機能の仕組み 1194
機能設定 1195
OAM サポート 1196
キャッシュ ポッドの最適化 1197
機能説明 1197
CDL フラッシュ間隔およびセッション有効期限のチューニング構成 1197
機能説明 1197
機能設定 1197
Ops センターを使用したドメインベースのユーザー認可 1198
機能説明 1198
機能の仕組み 1199
機能設定 1199
設定例 1200
設定の確認 1201
エッジ エコーの実装 1201
機能説明 1201
機能の仕組み 1201
OAM サポート 1202
バルク統計サポート 1202
GTPC エンドポイント ポッドのエンコーダとデコーダの最適化 1203
機能説明 1203
機能設定 1203
ETCD ピア最適化サポート 1204
機能説明 1204
機能の仕組み 1204

ローミング ピア最適化 1204
機能説明 1204
機能の仕組み 1205
インターフェイスに基づくローミング ピア検出 1205
アプリケーションによるローミング ピア検出 1205
ピア最適化 1205
制限事項 1206
機能設定 1206
設定例 1207
設定の確認 1207
ETCD トラフィックの最適化 1207
機能説明 1207
機能の仕組み 1208
ETCD クライアントのフォールバック 1209
機能説明 1209
ETCD クライアント ロード バランサ 1209
ETCD のクライアントの再試行メカニズム 1210
フラグ DB データベースの更新 1210
機能説明 1210
RRC 非アクティブ原因コードに基づく PDU セッション変更の処理 1211
機能説明 1211
機能の仕組み 1211
コール フロー 1212
機能設定 1218
設定例 1219
設定の確認 1219
K8 活性プローブを使用したポッド障害検出 1220
復元力の処理 1221
機能説明 1221
機能の仕組み 1221
機能設定 1222

設定例 1224
設定の確認 1224
OAM サポート 1224
バルク統計サポート 1224
Monitoring Support 1225
IoT 展開でのサブスクライバ セッションのスケーリング 1226
SMF インフラストラクチャの最適化の利点 1227
RADIUS および GTPC エンドポイントのパフォーマンス最適化の構成 1227
RADIUS エンドポイントの非同期通信の有効化 1228
セッション要求の作成に対するレート制限の有効化 1228

第 34 章 ポッドとサービスの参考資料 1231
機能の概要と変更履歴 1231
要約データ 1231
更新履歴 1232
機能説明 1232
ポッド 1233
レプリカ 1236
UDP プロキシ ポッド 1236
機能説明 1236
ノード モニタリング ポッド 1238
ノード モニタリング ポッドの構成 1238
サービス 1239
オープン ポートおよびサービス 1242
ノードへのポッドの割り当て 1244
ポッドの詳細とステータスの表示 1244
状態 1245
UDP プロキシ バイパスを使用した PFCP プロトコル エンドポイント マージ 1246
機能説明 1246
プロトコル マイクロサービスに統合された UDP プロキシ機能 1247
機能説明 1247

機能の仕組み 1247

第 35 章 ポリシーおよびユーザー プレーンの管理 1251

機能の概要と変更履歴 1252

要約データ 1252

更新履歴 1252

機能説明 1254

SMF での QoS 管理 1255

機能説明 1255

使用例 1255

登録済み QoS 1258

QoS 交渉力 1258

QoS フロー管理 1260

3GPP インターフェイスでの QoS 通信 1261

QoS 変更内容 1262

PCF および SMF 相互作用の QoS 機能のサポート 1263

ビットレートマッピングのサポート 1265

機能説明 1265

機能の仕組み 1266

標準準拠 1266

ビット レート マッピングの構成 1266

機能の設定の確認 1267

Diameter インターフェイス間のビットレート マッピング 1267

Diameter インターフェイスとのビット レート マッピングの構成 1267

デフォルト ベアラの許可された QoS の処理 1268

機能説明 1268

機能の仕組み 1269

4G および Wi-Fi セッションのデフォルトのベアラー QoS 処理 1269

5G セッションのデフォルト ベアラー QoS 処理 1270

WiFi ハンドオーバー中のデフォルト ベアラー QoS 処理 1270

障害処理中のデフォルト ベアラー QoS の変更 1271

制限事項 1271
承認された QoS 処理の OAM サポート 1272
統計情報サポート 1272
ローカル ポリシーに基づく GBR ベアラーの作成 1272
機能説明 1272
機能の仕組み 1272
PCF を使用しないデフォルトの非 GBR ベアラと専用 GBR ベアラーの作成 1272
専用GBRベアラーの作成による5G接続 1273
専用 GBR ベアラーの作成による 4G 接続 1276
制限事項 1277
PCF を使用せずにデフォルトの非 GBR ベアラと専用 GBR ベアラを作成するための設定 1277
QoS プロファイルとイベント管理ポリシーを DNN プロファイルに関連付ける構成 1278
イベント管理ポリシーを追加するための構成 1278
ルール定義ポリシーを追加するための構成 1279
アクション定義ポリシーを追加するための構成 1279
設定例 1280
OAM サポート 1281
メトリック 1281
UPF での EDR 生成の SMF トリガーされたメタデータ 1282
構成の動的な更新 1282
機能説明 1282
機能の仕組み 1283
動的な構成変更のサポートの構成 1284
動的な構成変更のサポート構成の確認 1285
ダイナミック PCC ルールの適用 1285
機能説明 1285
サポートされる機能の交渉 1285
セッション AMBR とデフォルト QoS のプロビジョニングと管理 1286
ポリシー再検証時間のプロビジョニング 1287
追加 QoS フローのプロビジョニングと管理 1288

QoS 適用 1290
ポリシー制御要求のトリガー 1290
ゲート制御 1292
機能の仕組み 1293
標準準拠 1294
制限事項 1295
動的 PCC ルール適用機能の構成 1295
QoS プロファイルの作成 1295
QoS パラメータの構成 1295
DNN プロファイル構成での QoS プロファイルの定義 1296
ダイナミック PCC ルール適用機能の構成の確認 1297
PCF および SMF インタラクションの制御 1297
専用 UE サービスのトラフィック フローの処理 1299
機能説明 1299
機能の仕組み 1300
N7 最適化 1301
機能説明 1302
機能の仕組み 1302
N7 最適化の構成 1306
OAM サポート 1307
ダイナミック QOS フローベースのアプリケーション検出および制御 1308
機能説明 1308
機能の仕組み 1309
インターフェイスの詳細 1309
制限事項 1310
Gx を介したダイナミック ADC ルールの適用 1311
機能説明 1311
機能の仕組み 1312
ダイナミック ADC ルールのインストール 1312
ダイナミック ADC ルールの変更 1314
ダイナミック ADC ルールの削除 1318

制限事項 1319
OAM サポート 1320
バルク統計サポート 1320
show コマンドの出力 1320
Monitoring Support 1321
静的 PCC ルールのサポート 1322
機能説明 1322
関係 1322
機能の仕組み 1322
構成時の前処理 1323
PDU セッションの作成時 1324
PDU セッションの変更時 1324
スタティック PCC ルールの構成 1325
課金アクションでの構成 1326
パケット フィルタの構成 1328
ACS ルールデフの構成 1329
ルール定義の ACS グループの構成 1331
ルールベースおよび事前定義済みルールプレフィックスの構成 1331
ACS ルールベースの構成（APN 構成モード） 1332
URR ID の構成 1332
GTPP グループの構成 1333
APN の構成 1333
GTPP グループと APN の関連付け 1333
ACS ルールベースの構成（ACS 構成モード） 1334
DNN プロファイル構成での UPF APN プロファイルの定義 1336
QoS パラメータの構成 1336
静的 PCC ルールのサポート機能構成の確認 1337
定義済み PCC ルール 1339
機能説明 1339
定義済みルール vs 静的ルール 1339
静的ルール、事前定義済みルール、動的なルールの組み合わせアプリケーション 1340

ベアラー QCI サポート 1340
機能説明 1340
ダイナミック PCC およびセッション ルールの非標準 QCI サポート 1343
機能説明 1343
機能の仕組み 1344
制限事項 1344
OAM サポート 1344
統計情報サポート 1345
トラブルシューティング情報 1345
帯域幅 ID の構成のサポート 1345
機能説明 1345
制限事項 1345
帯域幅 ID の構成 1345
BGP リンク帯域幅構成の確認 1346
PCF の UE キャンペーン レポートの生成 1347
機能説明 1347
UPF ノード選択 1348
クエリ パラメータに基づく UPF の選択 1349
機能説明 1349
機能の仕組み 1349
UPF 選択機能の構成 1353
UPF 選択 OA&M サポート 1364
IP しきい値ベースの UPF の選択 1365
機能説明 1365
機能の仕組み 1365
IP しきい値ベースの UPF 選択の OAM サポート 1366
初期 EPS 接続中の共存 UPF の選択 1368
機能説明 1368
機能の仕組み 1368
ノード ID の構成 1369
統計情報サポート 1369

ハンドオーバー中の共存 UPF の選択 1370
機能説明 1370
共存 UPF 選択のパラメータの構成 1370
UPF ノード レポートと独自のセッション レポートのサポート 1372
機能説明 1372
機能の仕組み 1372
PFCP ノード レポートの処理 1372
PFCP セッション レポートの処理 1373
コリジョン処理 1373
復元力の処理 1373
標準準拠 1373
制限事項 1374
OAM サポート 1374
Monitoring Support 1374
show コマンドのサポート 1375
統計情報サポート 1376
外部ヘッダー形式 1378
外部ヘッダー IE の機能構成 1380
グレースフル セッション終了の拡張された PFCP 関連付けのリリース手順 1381
UPF が開始した PFCP セッションのリリース 1382
UPF によって開始された拡張 PFCP 関連付けの解除 1384
EPFAR 機能の有効化 1384
バルク統計 1385
PCF を介した使用状況監視 1386
機能説明 1386
機能の仕組み 1386
使用状況レポート 1387
通信内容管理データの変更 1388
エラー処理 1389
コール フロー 1389
標準準拠 1391

制限事項 1392
事前定義されたルールの使用状況モニタリング キーの構成 1392
設定の確認 1393
OAM サポート 1393
使用率モニタリング統計情報 1393
N7 上の Ruledefs の QoS グループのサポート 1394
機能説明 1394
機能の仕組み 1395
QGR の処理フロー 1395
QGR パラメータ 1395
データパスの適用 1402
コール フロー 1402
制限事項 1405

第 36 章 **RADIUS 認証およびアカウンティング 1407**
機能の概要と変更履歴 1407
要約データ 1407
更新履歴 1407
機能説明 1409
RADIUS 認証 1410
スループットの制限 1411
RADIUS アカウンティング 1412
RADIUS 切断要求メッセージの処理 1412
アーキテクチャ 1414
SMF での RADIUS クライアント統合 1414
機能の仕組み 1415
認証のための RADIUS インタラクション 1415
RADIUS 認証属性 1419
コール フロー 1422
アカウンティングのための RADIUS 相互作用 1423
RADIUS アカウンティング属性 1424

コール フロー 1427
ご利用明細レポートルールの処理 1429
構成の動的な更新 1430
RADIUS 属性定義 1431
標準準拠 1441
制限事項と制約事項 1441
RADIUS クライアントの構成 1441
RADIUS サーバーの構成 1442
RADIUS 設定の確認 1443
RADIUS サーバー選択ロジックの構成 1444
RADIUS 属性の構成 1444
RADIUS 認証許可パラメータの有効化 1445
連続的障害の構成 1446
プロトコル エンド ポイントの内部仮想 IP の構成 1446
RADIUS 検出デッド サーバの構成 1447
RADIUS デッド タイムの構成 1448
RADIUS ディクショナリの構成 1448
RADIUS DTLS 接続再試行回数の設定 1449
最大送信数の構成 1449
RADIUS タイムアウトの構成 1450
RADIUS POD の構成 1451
RADIUS NAS-IP の構成 1452
セカンダリ認証メソッドの構成 1454
RADIUS 認証構成の確認 1454
PAP、CHAP、または MSCHAP ベースの認証の構成 1455
認証アルゴリズムの優先順位の定義 1455
ホスト パスワードの構成 1455
RADIUS アカウンティングの有効化 1456
DNN プロファイルでの RADIUS サーバー グループの定義 1457
RADIUS アカウンティング オプションの構成 1457
RADIUS アカウンティング サーバー グループの構成 1459

RADIUS アカウンティング 構成の確認 1459
セッション切断機能の構成 1459
動的認可サービスの構成 1459
CoA-NAS インターフェイスの構成 1461
RADIUS クライアント OA&M サポート 1461
統計情報サポート 1461
トラブルシューティング情報 1469
RADIUS バルク統計情報 1469
RADIUS 固有の情報のサブスクライバの詳細 1517
RADIUS エンドポイントの認証とアカウンティングの統計情報 1518
RADIUS エンドポイント切断メッセージおよび CoA 統計情報 1519
外部インバウンドおよびアウトバウンド接続 1519
内部および外部の接続 1520
ポッドのステータス 1520
設定エラー 1520
アラートの表示 1520
RADIUS アラート 1522
RADIUS EP ダウン アラート 1522
RADIUS アカウンティング確立の失敗しきい値アラート 1523
RADIUS アカウンティングのリリースの失敗しきい値アラート 1523
RADIUS 認証失敗しきい値アラート 1523
RADIUS 接続解除メッセージの失敗しきい値アラート 1524
RADIUS サーバ RTT アラート 1524
RADIUS アカウンティング開始初期メッセージの失敗しきい値アラート 1524
RADIUS アカウンティング暫定/更新メッセージ失敗しきい値アラート 1525
RADIUS アカウンティングの停止/終了メッセージの失敗しきい値アラート 1525
RADIUS 認証タイプ メッセージ失敗しきい値アラート 1525
Grafana チャート 1526
エラー ログ 1526
RADIUS 認証 1526
RADIUS アカウンティング 1528

アイドル タイムアウトに基づくリリース 1528
切断メッセージ 1529
RADIUS テスト CLI サポート 1530
RADIUS アカウンティング サーバのテスト 1530
RADIUS 認証サーバのテスト 1531

第 37 章 冗長性サポート 1533
機能の概要と変更履歴 1533
要約データ 1533
更新履歴 1534
機能説明 1534
サポートされる冗長性のタイプ 1534
高可用性のサポート 1535
機能説明 1535
UDP プロキシの高可用性 1536
ノード マネージャの高可用性 1536
内部ラックの高可用性 1536
アーキテクチャ 1537
SMF ポッドおよび VM の展開レイアウト 1537
機能の仕組み 1538
ポッドレベルのラベル付けとレプリカの構成 1539
設定例 1540
設定の確認 1540
アクティブ インスタンスの L2 VIP でのトラフィック モニタリング 1541
機能説明 1541
機能の仕組み 1541
HA および GR シナリオの構成 1542
OAM サポート 1542
ラック間冗長性サポート 1544
機能説明 1544
機能の仕組み 1544

概要 1544
ラック間冗長性トリガ 1546
ラック NF ロール 1546
一般的なガイドライン 1547
インスタンス認識 1548
ラック間冗長性インスタンスの構成 1548
エンドポイント インスタンス認識の構成 1549
プロファイル SMF インスタンス認識の構成 1551
ダイナミック ルーティング 1551
外部ネットワーク障害 1554
Geo スイッチオーバー 1555
内部ネットワーク障害 1555
ローカル スイッチオーバー 1556
リカバリとフェールバック 1556
コール フロー 1556
BGP を使用したダイナミック ルーティングの構成 1560
BGP スピーカーの構成 1564
モニタリングおよびトラブルシューティング 1564
IPAM 1568
IPAM の構成 1569
Geo レプリケーション 1570
ETCD/CachePod レプリケーションの構成 1571
Geo モニタリング 1572
ポッド モニタリング 1572
リモート クラスタ モニタリング 1573
トラフィック モニタリング 1574
Geo 冗長性の強化 1574
機能の仕組み 1575
OAM サポート 1575
BFD モニタリング 1576
CDL GR の展開 1579

CDL GR の前提条件 1579
CDL インスタンス認識とレプリケーション 1580
合法的傍受 1584
RADIUS 設定 1585
GR ペアのソフトウェア アップデート 1586
GR CLI 1591
Geo レプリケーション プル データ 1591
Geo ロールのリセット 1591
Geo スイッチ ロール 1592
障害対応 1592
show/clear コマンド 1592
モニタ サブスクライバ 1603
モニタープロトコル 1605
地理的冗長 OAM サポート 1606
ヘルス チェック 1606
回復手順 1610
主要業績評価指標（KPI） 1612
バルク統計 1617
アラート 1620
サイト間の地理的冗長性 1627
機能説明 1627
アーキテクチャ 1628
前提条件 1628
一般的なガイドライン 1629
機能の仕組み 1629
BGP ルート アドバタイズメント 1629
サイト間展開の構成 1632
ポッドの L3 ルーティング 1633
サイト間の冗長性シナリオ 1633
スプリットブレイン 1635
KPI 1637

第 38 章 ローミングのサポート 1643

機能の概要と変更履歴 1643

要約データ 1643

更新履歴 1644

機能説明 1644

ローカル ブレークアウト ローミングのサポート 1645

機能説明 1645

アーキテクチャ 1645

自宅ルート ローミングのサポート 1654

機能説明 1654

アーキテクチャ 1655

機能の仕組み 1659

vSMF セッション作成手順 1659

hSMF セッション作成手順 1662

vSMF セッション変更手順 1664

hSMF セッション変更手順 1666

vSMF リリース セッションの手順 1667

hSMF リリース セッションの手順 1669

vSMF クリア サブスクライバのリリースセッションの手順 1670

N26 インターフェイスを使用した EPS から 5G へのハンドオーバー 1672

N26インターフェイスを使用したシングル登録モードでの5GSからEPSへのハンドオーバー 1675

N26 インターフェイスを使用しない EPS から 5G へのハンドオーバー 1678

N26 インターフェイスを使用しない 5G から EPS へのハンドオーバー 1679

標準準拠 1681

制限事項 1682

HR ローミングの課金サポート 1682

HR ローミングの課金の構成 1686

人事ローミングでのデフォルトの DNN サポート 1688

HR ローミングでの IPv6 RS/RA サポート 1688

SEPP サポート 1688
機能説明 1688
機能の仕組み 1689
SEPP の構成 1692
OAM サポート 1696
N3 および N9 ユーザー プレーンの分離 1697
N3 と N9 の分離での ホーマー コール 1700
専用ベアラー コール フロー 1700
N3 と N9 の分離でのローマ コール 1701
許可された PLMN リストのサポート 1701
PLMN ローミング モビリティのサポート 1702
制限事項と制約事項 1703
標準準拠 1704
機能の仕組み 1704
コール フロー 1704
PLMN 間ハンドオーバーの構成 1711
DTSSA および ACSCR の送信 1712
OAM サポート 1713
バルク統計サポート 1713
N4 インターフェイスのローミング ステータス 1714
トラブルシューティング情報 1714
ローミング固有の情報の回線詳細 1714
hSMF に関するローミング固有の情報のサブスクライバの詳細 1715
hSMF に関するローミング固有の情報のサブスクライバ セッションの詳細 1722
vSMFのローミング固有情報のサブスクライバの詳細 1724
vSMFに関するローミング固有の情報のサブスクライバ セッションの詳細 1728
ローマ UE アラート 1729
ローマ内 UE 障害しきい値アラート 1730
アウトローマ UE 障害しきい値アラート 1730
ローマー UE バルク統計情報 1730
ローミング エラー ログ 1731

第 39 章 セッションおよびサービス継続性モード 1733
機能の概要と変更履歴 1733
要約データ 1733
更新履歴 1733
機能説明 1734
SSC モードの選択 1734
SSC モードを選択するための優先順位 1734
SSC モードの選択方法 1735
SSC モードの構成 1735

第 40 章 セッション タイマー 1737
機能の概要と変更履歴 1737
要約データ 1737
更新履歴 1737
機能説明 1738
3GPP 準拠タイマー 1739
GTP および N11 タイマー 1739
機能説明 1739
機能の仕組み 1739
標準準拠 1740
N11 タイマーおよび GTP タイマーの構成 1740
バックオフ タイマー サポート 1741
機能説明 1741
機能の仕組み 1742
標準準拠 1748
バックオフ タイマーの構成 1749
非 3GPP 準拠タイマー 1752
機能説明 1752
非 3GPP セッション タイマーの構成 1752
設定例 1754

設定の確認 1754

第 41 章 統合された SMF による複数世代のデバイス サポートの管理 1755

機能の概要と変更履歴 1755

要約データ 1755

更新履歴 1756

機能説明 1756

機能の仕組み 1758

標準準拠 1759

制限事項 1759

4G および 5G デバイスをサポートするためのパラメータの構成 1760

NSSAI の構成 1760

DNN プロファイルでの DCNR の有効化 1761

UPF 選択の構成 1761

セカンダリ RAT 使用状況レポートの構成 1762

プレゼンス レポートの構成 1763

設定の確認 1763

OAM サポート 1764

統計情報サポート 1764

バルク統計 1766

トラブルシューティング情報 1768

DCNR およびプレゼンス レポートが有効になっているサブスクライバの詳細 1768

オプション 3x：DCNR 対応 UE アラート 1769

DCNR UE 接続失敗しきい値アラート 1769

プレゼンス レポートを使用した DCNR UE 接続失敗しきい値アラート 1770

DCNR UE バルク統計情報 1770

オプション - 3x デバイス固有のエラーログ 1770

SMF における 2G および 3G ネットワーク統合 1772

2G および 3G ネットワーク統合概要 1772

S4-SGSN の接続と切断の手順コール フロー 1775

S4-SGSN を介した PDN 切断 1776

S4-SGSN を介した PDN 切断 1777
2G と 3G RAT タイプの S4-SGSN を有効化 1785
2G および 3G サポートのための S4-SGSN MBR およびハンドオーバー手順 1790
ユーザーのロケーション変更のための MBR 手順 1790
S4-SGSN RAT 間ハンドオーバーの手順 1792
S4-SGSN での専用ベアラーによるハンドオーバー手順 1800
S4-SGSN の RAT 内ハンドオーバー 1802
コンバージド コアにおける S4-SGSN 向けのダイナミック QoS の変更 1804
HSS によって開始される QoS の変更 1804
HSS によって開始される QoS の変更 1806
S4-SGSN PCF によって開始された変更 1807
GTPv1 SGSN の接続と切断の手順コール フロー 1809
PDN が SGSN 経由で切断 1809
PDN が SGSN 経由で切断 1811
GTPv1 2G および 3G セッションの Show コマンド出力 1814
monitor subscriber CLI コマンドのサンプル出力 1816
2G および 3G セッションの統計 1818

第 42 章
**SMF の有用性 1821**
ピア モニタリング 1822
Grafana を介したピア ステータスの表示 1822
ログ モニタリング 1823
機能の概要と変更履歴 1823
要約データ 1823
更新履歴 1824
機能説明 1824
関係 1824
機能の仕組み 1825
コールの失敗ログ 1829
コール失敗ログの構成 1830
手順失敗ログ 1831

手順失敗ログの構成 1832
一般的なプロシージャ失敗ログ 1834
一般的な手順失敗ログを構成 1834
追加のコールフロー失敗ログ 1835
追加のコールフロー失敗ログの構成 1836
イベント トレース ログ 1838
イベント トレース ログの構成 1841
コール フロー統計ログ 1842
コール フロー統計ログの構成 1843
コア ダンプ ユーティリティ ログ 1843
コア ダンプ ユーティリティ ログの構成 1844
サブスクライバ(MonSub)ログを監視 1845
モニタ サブスクライバ ログの構成 1847
N40 追加のログと 1849
N40 追加ログと統計情報の構成 1850
N7 の追加のログと統計情報 1851
N7 の追加ログと統計情報の構成 1851

第 43 章 サブスクライバの課金 1853
機能の概要と変更履歴 1853
要約データ 1853
更新履歴 1854
機能説明 1854
コンバージド課金 1856
課金対象イベント 1856
課金 ID 1857
請求情報 1857
機能の仕組み 1858
充電セッション 1858
オフライン充電とオンライン充電 1858
CHF の選択 1862

SMF での課金アクティビティ 1863
課金に関する静的ルールおよび事前定義済みルール 1871
課金の変更シナリオ 1872
URR のリンク 1874
ローカル設定 1875
ゼロ使用レポート抑制 1875
コール フロー 1876
制限事項 1878
標準準拠 1878
充電インターフェイスに関する 3GPP の 2019 年 6 月の適合規格 1878
SMF 課金の構成 1879
DNN プロファイルの構成 1879
課金特性プロファイルの構成 1879
課金特性 ID の構成 1880
課金プロファイルの構成 1880
さまざまなインターフェイスでの課金シナリオのマッピング 1885
機能説明 1885
機能の仕組み 1885
制限事項 1892
標準準拠 1892
障害処理シナリオ 1893
アプリケーション エラーおよび結果コードの処理 1893
N40 アプリケーション エラー コード 1894
Gy アプリケーション エラー コード 1894
RG レベル結果コード 1898
課金無効化機能の処理 1899
課金サーバーの調整 1899
課金構成のダイナミックな更新 1900
機能説明 1900
機能の仕組み 1901
ACS プロファイル 1901

課金プロファイル 1907
静的ルールおよび事前定義済みルールを使用したプリエンプティブ クォータの取得 1912
機能説明 1912
機能の仕組み 1913
コール フロー 1914
プリエンプティブ クォータ要求の構成 1919
OAM サポート 1920
バルク統計サポート 1920

第 44 章 AMF からの TAI 選択 1921
機能の概要と変更履歴 1921
要約データ 1921
更新履歴 1921
機能説明 1922
機能の仕組み 1922
TAI 選択機能の構成 1925
TAI グループ リストの構成 1925
TAI グループ リストの確認 1925
TAI グループの構成 1926
TAC リストの構成 1926
TAC 範囲リストの構成 1926
TAI グループ構成の確認 1927
プライオリティの設定 1927
優先順位構成の確認 1927

第 45 章 UDM の統合 1929
機能の概要と変更履歴 1929
要約データ 1929
更新履歴 1930
機能説明 1930
機能の仕組み 1930

UDM を構成 1931
SDM メッセージを制御するためのオプションの構成 1931
RAT タイプの設定 1931
セッション タイプの構成 1932
オプションの IE を無効にする構成 1933
即時レポートによるサブスクリプション通知の構成ベースの制御 1934
機能説明 1935
機能の仕組み 1935
即時レポートによるサブスクリプション通知の構成 1936
即時レポートによるサブスクリプション通知の確認 1936
OAM サポート 1936
メトリック 1936
コンバージド コアで N10 フェール オープン 1938
機能説明 1938
サブスクリプション メッセージの構成ベースの制御 1939
機能説明 1939
機能の仕組み 1939
標準準拠 1940
コール フロー 1940
サブスクライブ解除メッセージの OAM サポート 1941
統計情報サポート 1941
UDM 登録メッセージの構成ベースの制御 1942
機能説明 1942
機能の仕組み 1942
UDM 登録メッセージの制御の構成 1943
UDM データ変更通知に基づくセッション管理 1944
UDM データ変更通知に基づくセッション管理 1944
SMF が UDM データ変更通知を使用してセッションを管理する方法 1944
ユーザー定義の設定でセッションを管理 1945
システム定義の構成によるセッションの管理 1946
イベント管理ポリシーでサブスクリプション変更イベントを有効にします 1948

サブスクリプション変更イベントを構成します 1948
サブスクリプション変更イベントのルールと条件の定義 1949
サブスクリプション変更イベントの構成アクション 1950
サブスクリプション変更イベントの構成例 1951
バルク統計情報を利用してセッションを管理する 1951

第 46 章 UP セッションのアクティブ化と非アクティブ化のサービス要求手順 1953
機能の概要と変更履歴 1953
要約データ 1953
更新履歴 1954
機能説明 1954
UE 開始サービス要求の手順 1954
機能説明 1955
機能の仕組み 1955
PDU セッションのユーザープレーン接続の非アクティブ化 1955
PDU セッションのユーザー プレーン接続のアクティブ化 1957
ネットワーク開始型サービスのリクエスト手順 1959
機能説明 1960
機能の仕組み 1960
コール フロー 1960
標準準拠 1973
制限事項 1973
N3 トンネル プロファイルの構成 1973
常時接続の PDU セッションのサポート 1974
機能説明 1974
機能の仕組み 1974
コール フロー 1974
常時接続の PDU セッション サポートの構成 1978
常時接続の PDU セッションサポートの確認 1979
常時接続の PDU セッション OAM のサポート 1981
バルク統計サポート 1981

N3 接続再アクティブ化のための DLDR 処理 1982
機能説明 1982
機能の仕組み 1982
N3 接続再アクティブ化の構成 1982

第 47 章 UPF パスの管理と復元 1983
機能の概要と変更履歴 1983
要約データ 1983
更新履歴 1983
機能説明 1984
標準準拠 1984
機能の仕組み 1984
UPF パス管理および復元の構成サポート 1985
インターフェイス レベルでハートビートの構成 1985
SMF のハートビート構成の確認 1986
UPF グループ レベルでのハートビートの構成 1987
UPF グループ レベルのハートビート構成の確認 1987
個々の UPF ネットワーク構成への UPF グループの関連付け 1988
UPF グループと個々の UPF の関連付けの確認 1988
Sx/N4 パス障害検出ポリシーの構成 1988
Sx/N4 パス障害検出ポリシーの確認 1989
OAM サポート 1990
バルク統計 1990

第 48 章 仮想ルーティングおよび転送 1993
機能の概要と変更履歴 1993
要約データ 1993
更新履歴 1993
機能説明 1994
機能の仕組み 1995
VRF の作成 1995

VRF 変更内容 1995
VRFの削除 1996
制限事項 1996
仮想ルーティングと転送の構成 1996
VRF 設定 1996
設定例 1997
エンドポイントの設定 1997
設定例 1998
RADIUS プロファイルにおける VRF 構成 1998
BGP ピアリングの VRF 関連付け 1999
設定例 1999
設定の確認 2000
OAM サポート 2001
バルク統計サポート 2001

第 49 章 ワイヤレス優先順位サービス 2003
機能の概要と変更履歴 2004
要約データ 2004
更新履歴 2004
機能説明 2005
使用例 2005
マルチメディア優先サービス 2005
PFCP を介した N3、S5-U、または S2-B の DSCP マーキング 2011
WPS プロファイルのサポート 2012
SBI メッセージ優先メカニズム 2012
機能の仕組み 2014
標準準拠 2014
5QI マッピングのサポート 2015
機能説明 2015
ダイナミック ルールの QCI 変更 2015
元の QCI と再マッピングされた QCI の衝突 2016

ワイヤレス優先順位サービスの構成 2016
DNN プロファイルの構成 2016
DNN プロファイルでの WPS プロファイルの関連付け 2017
設定の確認 2018
非標準 QCI から標準 QCI への再マッピング 2019
メッセージの優先順位プロファイルの構成 2020
メッセージの優先順位プロファイルの関連付け 2021
オーバーロード スロットリングから WPS セッションを除外するための SMF の構成 2024
エンドポイント レベルでの過負荷除外の構成 2025
優先度の高いメッセージに対するメッセージ プライオリティのネゴシエーション 2027
WPS OAM サポート 2028

第 50 章 トラブルシューティング情報 2031
機能の概要と変更履歴 2031
要約データ 2031
更新履歴 2032
説明 2033
CLI データの使用 2033
Show and Clear コマンド 2033
show コマンド 2033
clear コマンド 2059
サブスクライバのモニタリングとプロトコルのモニタリング 2063
機能説明 2063
モニター サブスクライバおよびモニター プロトコル機能の構成 2063
SMF から UPF モニター サブスクライバ 2066
機能説明 2066
SMF からの UPF モニターサブスクライバの構成 2067
GTP-C サービスのモニターとトラブルシューティング 2069
機能説明 2069
GTP-C テスト エコー コマンドの使用 2069
GTPP テスト エコー コマンドの使用 2070

アラート 2071
機能説明 2071
機能の仕組み 2071
アラート ルールの構成 2072
アラート ロガーの表示 2073
コール フロー手順に関するアラート 2074
インターフェイス固有のアラート 2080
IPプール 2086
メッセージ レベル アラート 2086
ポリシー ルール アラート 2093
SMF 過負荷/輻輳 2094
SMF セッション 2094
メトリック 2096
機能説明 2096
機能の仕組み 2097
メトリック収集の設定 2097
設定例 2098
設定の確認 2099
バルク統計情報と重要業績評価指標 2100
機能説明 2100
ログ 2100
機能説明 2100
OAM および EDR モニタ ポッド ファイルのダウンロード 2101
機能の仕組み 2102
ログの構成 2102
トランザクション メッセージの有効化または無効化 2102
ロギング レベルを構成 2105
永続的なトランザクション ログの構成 2105
JSON ロギングのイネーブル化またはディセーブル化 2106
イベント障害のログ 2107
イベント障害ロギングの仕組み 2109

イベント ロギングの有効化 2111
ディスパッチャ 2112
機能説明 2112
S11 インターフェイス用のディスパッチャの構成 2113
設定例 2114
OAM サポート 2114
メトリック 2114

第 51 章 SMF 構成例 2115
設定例 2115

# このガイドについて

（注） この製品のマニュアルセットは、偏向のない言語を使用するように配慮されています。このドキュメントセットでの偏向のない言語とは、年齢、障害、性別、人種的アイデンティティ、民族的アイデンティティ、性的指向、社会経済的地位、およびインターセクショナリティに基づく差別を意味しない言語として定義されています。既存の偏った用語が置換される間は、製品ソフトウェアのユーザー インターフェイスにハードコードされている言語、RFP のドキュメントに基づいて使用されている言語、または参照されているサードパーティ製品で使用されている言語によりドキュメントに例外が存在する場合があります。

この序文では、『*5G* セッション管理機能ガイド』、その構成、および表記法について説明します。

このガイドでは Cisco セッション管理機能（CDL）について説明しており、これにはインフラストラクチャとインターフェイス、機能の説明、仕様の準拠、セッションフロー、設定手順、およびシステムのモニタリングと障害対応のための CLI コマンドが含まれています。

• 使用する表記法 （lxxi ページ）

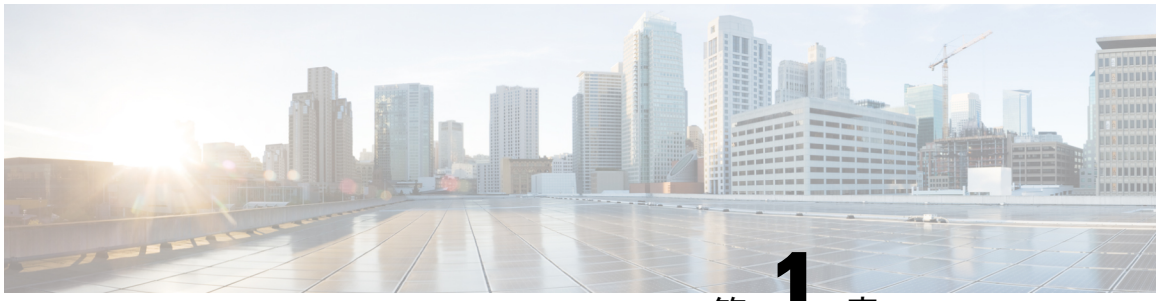
## 使用する表記法

次の表に、このマニュアル全体で使用される表記法を示します。

| 通知タイプ | 説明 |
|---|---|
| 情報メモ | 重要な機能または手順に関する情報を提供します。 |
| 注意 | プログラム、デバイス、またはシステムに損傷を与えるおそれがあることを注意喚起します。 |

| 通知タイプ | 説明 |
| --- | --- |
| 警告 | 人身傷害または死亡事故のおそれがあることを警告します。また、電気的障害のおそれがあることを警告する場合もあります。 |

| 書体の表記法 | 説明 |
| --- | --- |
| スクリーンディスプレイとして表されるテキスト | この書体は、端末画面に表示されるディスプレイを表します。次に例を示します。<br>ログイン： |
| **commands** として表現されるテキスト | この書体は、入力したコマンドを表します。次に例を示します。<br>**show ip access-list**<br>このマニュアルでは、コマンドの完全表記に常に小文字を使用しています。コマンドには、大文字と小文字の区別はありません。 |
| **command** *variable*として表されるテキスト | この書体は、コマンドの一部である変数を表します。次に例を示します。<br>**show card** *slot_number*<br>*slot_number* は、目的のシャーシのスロット番号を表す変数です。 |
| メニュー名またはサブメニュー名として表されるテキスト | この書体は、ソフトウェアアプリケーション内でアクセスするメニューとサブメニューを表します。次に例を示します。<br>[File] メニュー、[New] の順にクリックてください。 |



第 1 章

# 5G アーキテクチャ


- 機能の概要と変更履歴, on page 1
- アーキテクチャの概要, on page 2
- サブスクライバ マイクロサービスのインフラストラクチャのアーキテクチャ, on page 4
- コントロール プレーン ネットワーク機能アーキテクチャ, on page 5


# 機能の概要と変更履歴

## 要約データ

***Table 1:*** 要約データ

| | |
|---|---|
| 該当製品または機能エリア | • PC-F<br>• SMF<br>• UPF |
| 該当プラットフォーム | SMI |
| 機能のデフォルト設定 | N/A |
| 関連資料 | 該当なし |

## 更新履歴

***Table 2:*** マニュアルの変更履歴

| 改訂の詳細 | リリース |
|---|---|
| 最初の導入。 | 2020.02.0 より前 |

# アーキテクチャの概要

Ultra Cloud Core は、5G 新しい無線（NR）スタンドアロン（SA）モードの 3GPP 標準規格をサポートする Cisco のソリューションです。これらの標準規格では、CUPS など、コントロール プレーン（CP）とユーザー プレーン（UP）の分離に基づいてさまざまなネットワーク機能（NF）を定義します。この分離により、ネットワークのパフォーマンスと機能が向上します。

## コントロール プレーン ネットワーク機能

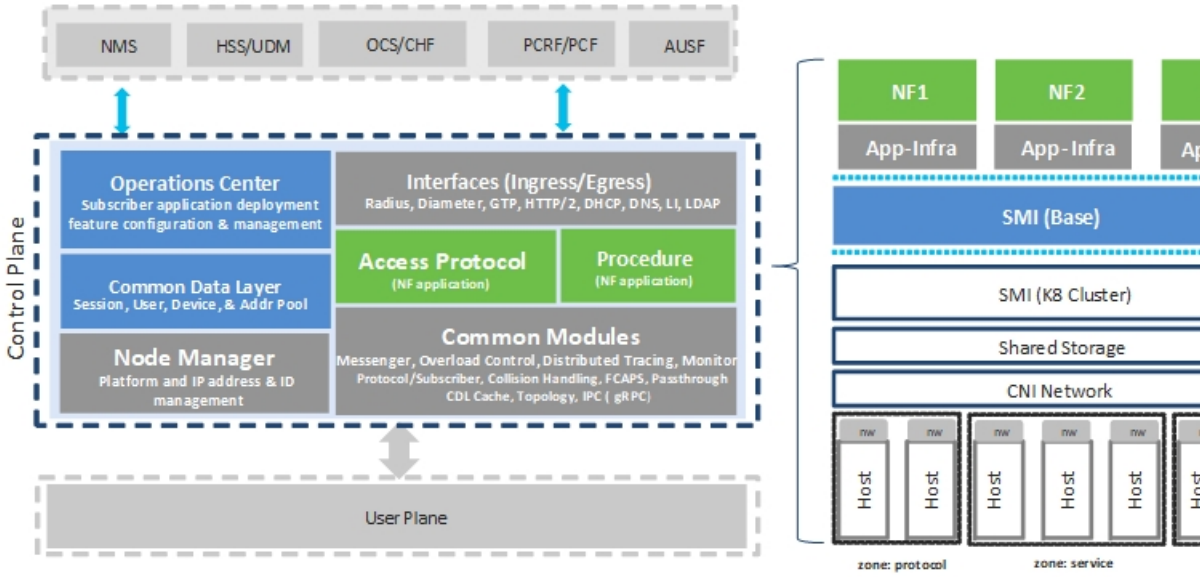
Ultra Cloud Core の CP 関連 NF は、次のテナントを持つ共通アーキテクチャを使用します。

- クラウドスケール：完全に仮想化され、シンプルさ、スピード、柔軟性を実現します。
- 自動化とオーケストレーション：最適化された運用、サービスの構築、およびインフラストラクチャ。
- セキュリティ：インフラストラクチャから NF アプリケーションまで、展開スタック全体における複数のセキュリティ層。
- API 公開：オープンかつ広範で、可視性、制御、およびサービス イネーブルメントが向上します。
- アクセスに依存しない：複数のネットワーク タイプをサポート（5G、4G、3G、Wi-Fi など）。

コントロールプレーン NF は、マイクロサービスなどのコンテナ化されたアプリケーションとして設計されています。Subscriber Microservices Infrastructure (SMI) を介して展開されます。

SMI は、ライフサイクル管理（LCM）、運用と管理（OAM）、パッケージングなど、NF の機能面の共通アプリケーション レイヤを定義します。

*Figure 1: Ultra Cloud Core CP* アーキテクチャ コンポーネント




# ユーザー プレーン ネットワーク機能

Ultra Cloud Core 内の 5G UP NF は、ユーザー プレーン機能（UPF）です。CP 関連の NF とは異なり、5G UPF は、Cisco 4G CUPS アーキテクチャと同じベクトル パケット処理（VPP）テクノロジーを使用します。この共通性により、4G と 5G の間で次のような一貫した機能のセットが提供されます。

- 超高速パケット転送。
- 広範に統合された IP サービス（サブスクライバ ファイアウォール、テザリング、ディープ パケット インスペクション（DPI）、Internet Content Adaption Protocol（ICAP）、アプリケーションの検出および制御（ADC）、ヘッダーエンリッチメント（HE）など）。
- トラフィックおよびTCPを最適化するための統合されたサードパーティ製アプリケーション。

# サブスクライバ マイクロサービスのインフラストラクチャのアーキテクチャ

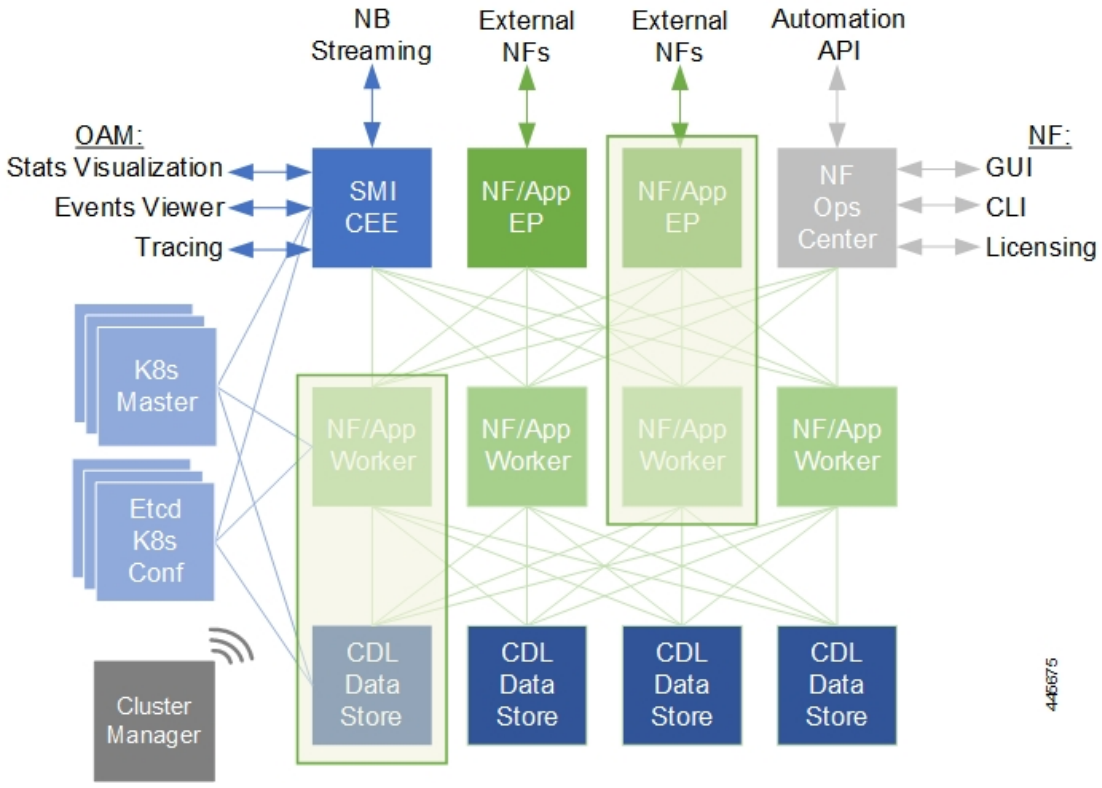
Ultra Cloud Core（UCC）サブスクライバマイクロサービス インフラストラクチャ（SMI）は、クラウド テクノロジーの階層化されたスタックです。マイクロサービスベースのアプリケーションの迅速な展開とシームレスなライフサイクル運用を可能にします。

SMI スタックは、次のコンポーネントで構成されています。

- SMI クラスタ マネージャ：Kubernetes（K8s）クラスタを作成し、ソフトウェア リポジトリを作成して、展開、アップグレード、拡張を含むクラスタの継続的な LCM を提供します。
- Kubernetes 管理：クラスタに展開される NF アプリケーションに LCM を提供する K8s プライマリおよび etcd 機能が含まれます。このコンポーネントは、クラスタ ヘルス モニタリングとリソース スケジューリングも提供します。
- 共通実行環境（CEE）：Cisco Cloud ネイティブ NF およびアプリケーションにユーティリティおよび OAM 機能を提供します。これには、ライセンスおよび権限付与機能、構成管理、テレメトリが含まれます。また、アラームの可視化、ログ管理、およびトラブルシューティング ユーティリティも提供します。また、これらのツールと展開されたアプリケーションに関連するすべてのお客様との接触ポイントと統合ポイントで、一貫した対話とエクスペリエンスを提供します。
- Common Data Layer（CDL）：5G およびサブスクライバ アプリケーション向けに特別に設計された、高性能で低遅延のステートフルなデータストアを提供します。この次世代データストアは、ローカルまたは地理的冗長性の展開で高可用性を提供します。
- サービス メッシュ：アプリケーション コンテナ間の高度なメッセージ ルーティングを提供し、管理された相互接続性、追加のセキュリティ、および低リスクの方法で新しいコードと新しい構成を展開する機能を実現します。
- NB ストリーミング：課金および課金システムに「ノースバウンド データ ストリーミング」サービスを提供します。
- NF またはアプリケーション ワーカー ノード：NF アプリケーションポッドを構成するコンテナ。
- NF またはアプリケーション エンドポイント（EP）：NF またはアプリケーションと、それらのネットワーク上の他のエンティティへのインターフェイス
- アプリケーションプログラミングインターフェイス（API）：展開、構成、および管理の自動化のためのさまざまな API を提供します。

次の図は、これらのコンポーネントがどのように相互接続し、マイクロサービスベースの NF またはアプリケーションを構成するかを示しています。

*Figure 2: SMI* コンポーネント




SMI コンポーネントの詳細については、『Ultra Cloud Core サブスクライバ マイクロサービス インフラストラクチャ』および『展開ガイド』の 「概要」の 章にある関連ドキュメントを参照してください。

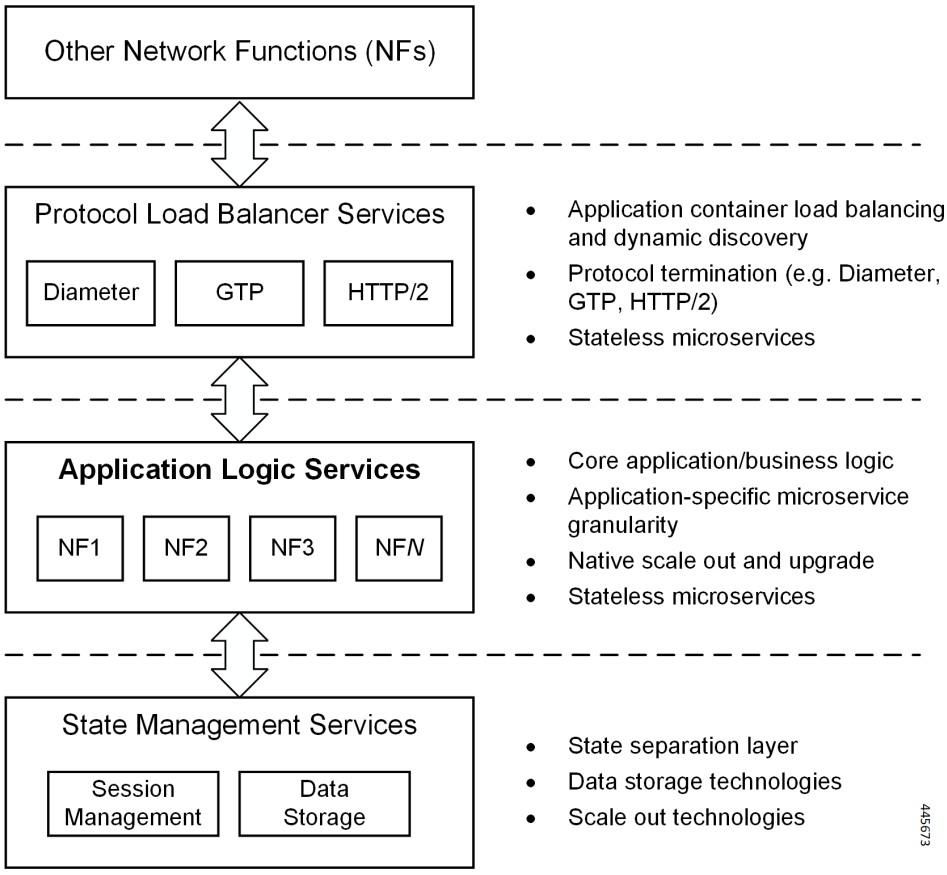
# コントロールプレーンネットワーク機能アーキテクチャ

コントロールプレーン（CP）NFは、3階層アーキテクチャを使用します。このアーキテクチャは、クラウドネイティブ環境でステートフルまたはステートレス機能を活用します。アーキテクチャ層は次のとおりです。

- プロトコル ロード バランサ サービス：このサービスは、アプリケーション コンテナの動的な検出と、プロトコルのプロキシと終了を主な役割とするステートレスマイクロサービスです。これには、従来の 3GPP プロトコルと、5G で導入された新しいプロトコルが含まれます。
- アプリケーション サービス：コア アプリケーションまたはビジネス ロジックの実装を行い、受信した情報に基づいて実際のアプリケーションをレンダリングするステートレス サービスです。このレイヤには、さまざまなレベルのマイクロサービスの粒度が含まれる場合があります。アプリケーション サービスはステートレスです。

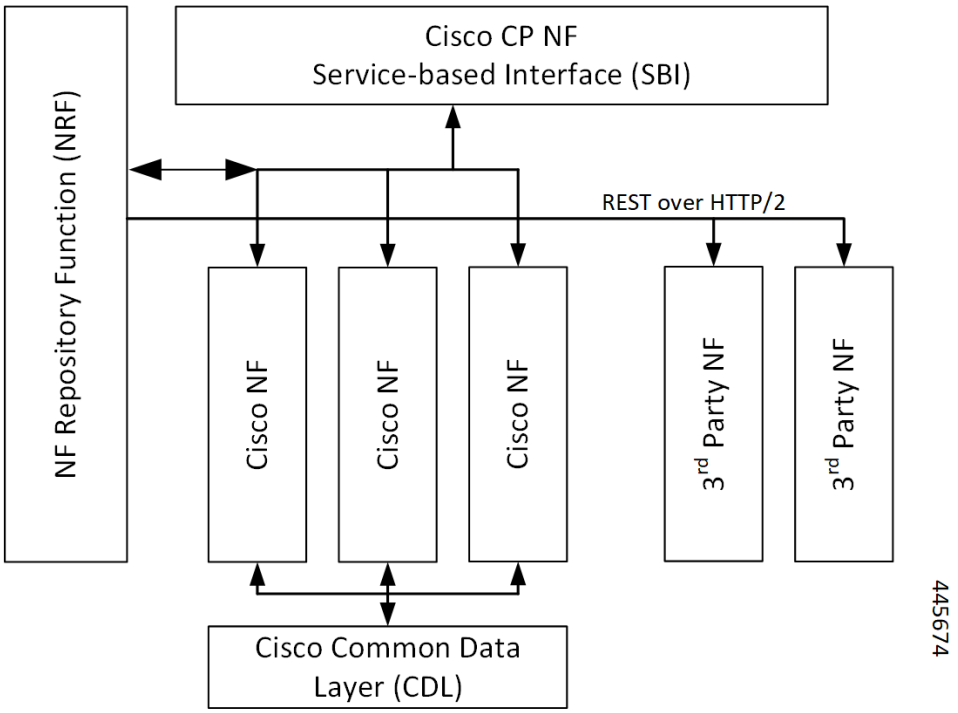
- ステート管理サービス：ステートレス アプリケーション サービスは、セッション データやサブスクライバデータなどのステート情報を保存またはキャッシュするための共通データ層（CDL）を提供します。この層は、インメモリ キャッシュから本格的なデータベースまで、さまざまなデータ ストレージ テクノロジーをサポートします。

***Figure 3:*** 制御プラン、ネットワーク機能階層型アーキテクチャ

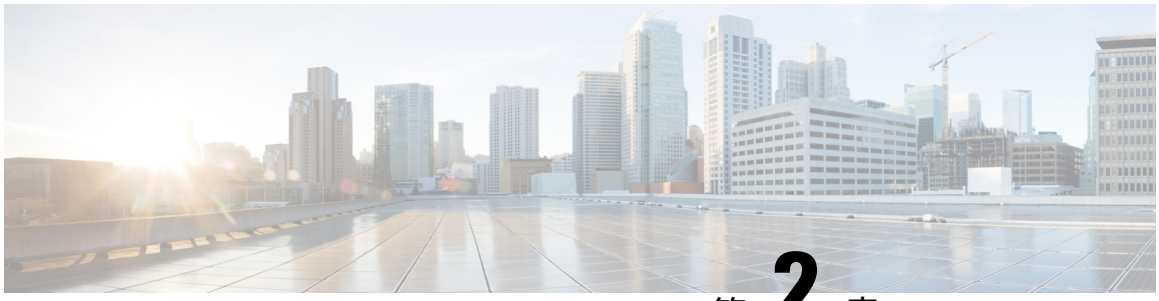



Cisco CP NF が設計されている 3 階層アーキテクチャは、3GPP で定義されている 5G コア（5GC）のサービスベース アーキテクチャ（SBA）を完全にサポートしています。これらの NF は、サービスベースのインターフェイス（SBI）を使用して通信します。3GPP で定義されているように、TCP 経由の HTTP/2 を使用します。

*Figure 4: Cisco CP NF* サービスベース アーキテクチャのサポート




Cisco のネットワーク機能の詳細については、対応するネットワーク機能のマニュアルを参照してください。



第 2 章

# 5G SMF の概要


- 機能の概要と変更履歴 （9 ページ）
- 製品の説明 （10 ページ）
- コンバージド コアの概要 （11 ページ）
- ユースケースと機能 （14 ページ）
- 展開アーキテクチャおよびインターフェイス （24 ページ）
- データ パケットのライフサイクル （27 ページ）
- セッション アフィニティ, on page 34
- ライセンス情報 （35 ページ）
- 標準準拠 （35 ページ）


## 機能の概要と変更履歴

### 要約データ

**表 *3* : 要約データ**

| | |
|---|---|
| 該当製品または機能エリア | SMF |
| 該当プラットフォーム | SMI |
| 機能のデフォルト設定 | N/A |
| このリリースでの関連する変更点 | N/A |
| 関連資料 | 該当なし |

# 更新履歴

**表 *4:* マニュアルの変更履歴**

| 改訂の詳細 | リリース |
|---|---|
| このリリースでは、SMF + cnSGWc の組み合わせに対する統合型コアのサポートが追加されています。 | 2021.01.0 |
| 最初の導入。 | 2020.02.0 より前 |

# 製品の説明

シスコ セッション管理機能（SMF）は、5G コア ネットワーク（5GC）のコントロール プレーン ネットワーク機能（NF）の 1 つです。SMF は、セッションごとにサポートされる個々の機能とのセッション管理を担当します。

SMF の 1 つのインスタンスが SMF の一部またはすべての機能をサポートできます。 *3GPP TS 23.501*で規定されているように、SMF は次の機能をサポートしています。

- セッション管理を処理します。たとえば、ユーザープレーン機能（UPF）とアクセス ネットワーク（AN）間のトンネルを含む、セッションの確立、変更、およびリリースです。
- オプションの承認を含む、ユーザー要素（UE）IP アドレスの割り当てと管理を処理します。
- Dynamic Host Configuration Protocol for IPv4（DHCPv4）および DHCPv6 機能を、サーバーとクライアントの両方として実行します。
- イーサネット PDU に対して Address Resolution Protocol（ARP）プロキシおよび IPv6 ネイバー要請プロキシ機能を実行します。SMF は、MAC アドレスを提供することで、ARP および IPv6 ネイバー要請要求に応答します。このアドレスは、要求に存在する IP アドレスに対応します。
- イーサネット PDU セッションの UPF を選択および制御します。UP 機能には、プロキシ ARP または IPv6 ネイバー探索への UPF の制御、および SMF へのすべての ARP または IPv6 ネイバー要請トラフィックの転送が含まれます。
- 対応するデータネットワーク（DN）にトラフィックをルーティングするように、UPF でトラフィック ステアリングを構成します。
- ポリシー制御機能（PCF）へのインターフェイスを終端します。
- セッション マネージャ（SM）のイベントと LI システムへのインターフェイスの合法的傍受（LI）を処理します。
- UPF での課金データ収集を制御および同期します。

- Non-Access-Stratum（NAS）メッセージの SM 部分を終了します。
- パケットをルーティングし、ダウンリンク データ通知（DDN）を介した情報配信を確保します。
- アクセスモビリティ管理機能（AMF）を通じて N2 インターフェイスを介して AN に送信される AN 固有の SM 情報を開始します。
- セッションのセッションとサービス継続性（SSC）モードを決定します。
- 次のローミング機能を提供します：
  - Quality of Service（QoS）SLA（VPLMN）を適用するようにローカルの適用を管理します。
  - 課金データを収集し、課金インターフェイスをサポートします。
  - 外部 DN との通信をサポートします。通信は、外部 DN による PDU セッション承認または認証のためのシグナリングのトランスポートのためのものです。

SMF は、モバイル仮想ネットワークオペレータ（MVNO）モデルをサポートします。これにより、モバイルネットワークオペレータ（MNO）は、リースされた MVNO サブスクライバのセカンダリ認証を実行できます。さらに、SMF は他の MVNO 機能をサポートしていますが、RADIUS クライアント、vDNN などに限定されません。

# コンバージド コアの概要

コンバージド コア ソリューションは、4G および 5G デバイス、およびユースケースをサポートする機能を備えた、クラウドネイティブの高度な統合コントロールプレーンを提供します。

**重要** このリリースでは、S5C および cnSGW-C 機能を備えたクラウドネイティブ統合 S-GW および SMF インスタンスのみがサポートされています。

コンバージド コア ソリューションは、あらゆるタイプのサブスクライバとユースケースを処理するコンバージド コア ネットワークを提供することで、運用の複雑さを軽減します。

オペレータには、次の利点があります。

- 4G サブスクライバまたは 5G から 4G カバレッジエリアへのハンドオフを処理しながら、cnSGW-C と SMF 間のシグナリングを減らすことで、全体的なネットワーク効率を向上させます。
- 4G カバレッジエリア内のサブスクライバの追加ホップ SGW-U が原因で発生する遅延を削減し、統合 UPF のデータパスを折りたたむことで、全体的なユーザー体験を向上します。
- 4G および 5G デバイスの SBA インターフェイスを使用して、統一されたサブスクライバポリシーと課金インフラストラクチャを使用する機能を提供します。

このソリューションは、次の統合コントロールプレーンおよびユーザープレーン機能をサポートしています。

- 統合コントロールプレーン機能
  - S-GW および SMF ネットワーク機能を単一の Kubernetes 名前空間の下で単一の展開として統合し、E-UTRAN/NR（コンバージド コア ゲートウェイ）から 4G および 5G デバイスをサポートします。
  - 論理ネットワーク機能（データ）をサポート
- 統合ユーザー プレーン機能
  - UPF 機能と SGW-U 機能を単一のネットワーク機能として統合
  - N4 インターフェイスと Sxa インターフェイスの同時サポートを提供
  - 単一の展開で複数のコントロールプレーンを終端

# サービス間ポッド通信

## 機能説明

サブスクライバ用に選択された cnSGW サービスと SMF サービスが同じクラスタおよび同じラック上にある場合、2 つのサービス間で交換されるメッセージは gtpc-ep ポッドを介して流れます。

併存セッションが特定され、 **enable-gtpc-bypass** CLI コマンドが GTP エンドポイントで設定されている場合、SMF と cnSGW-C は、gtpc-ep ポッドを介してメッセージを交換せずに相互に直接通信します。このアプローチにより、遅延と gtpc-ep の処理負荷が軽減されます。コマンドの詳細については、機能設定 （13 ページ） セクションを参照してください。

SMF サービスは cnSGW サービスと直接通信して、次の要求を処理します。

- ベアラー要求の作成
- ベアラー要求（UBR）の更新（ベアラーコマンド(MBCの変更)によってトリガーされるUBRを想定）
- Delete Bearer Request (DBR)（Delete Bearer コマンド (DBC) がトリガーする DBR を想定してください）

cnSGW サービスは SMF サービスと直接通信して、次の要求を処理します。

- セッション要求の作成
- ベアラー変更要求
- セッション要求の削除

サブスクライバセッションが配置されていない場合、SMF または cnSGW-C からの着信メッセージと発信メッセージは、gtpc-ep ポッドを介して引き続き交換されます。

cnSGW のこの機能のサポートについては、『*UCC 5G cnSGWc* 構成および管理ガイド』を参照してください。

## 機能の仕組み

ここでは、この機能の仕組みを説明します。

この機能を実装するには、次の手順を実行します。

1. SMF と cnSGW-C の展開タイプを特定します。

   展開タイプを特定するために、SMF または cnSGW-C は、メッセージのターゲット GTPC ピア IP アドレスを、関連する GR インスタンスの S5e または S5 インターフェイスのローカルに構成された IP アドレスと比較します。SMF または cnSGW-C は、比較の結果に基づいて、サブスクライバ セッションをコロケーション サービスとしてマークします。

2. ターゲットのサービス ポッドを特定する

   SMF は、メッセージを cnSGW サービス ポッド インスタンスに適切にルーティングするために、Common ID から派生した TEID に基づいて cnSGW 名前空間でセッション アフィニティを使用します。

3. 識別された展開タイプとターゲットサービス ポッドに基づいて、メッセージを適切なピアにルーティングします。

   サービス間ポッド通信は、プロトコル バッファとともに既存のフレームワークを使用して、シグナリング メッセージのコンテンツを伝送します。

   SMF と cnSGW-C 間のサービス間通信は、次の例外で発生します。

   - パケット スニファ ツールおよび **monitor subscriber** コマンドを使用して GTPC メッセージをキャプチャすることはできません。
   - パス管理は、同じ場所にある GTPC ピアに対しては実行されません。
   - GTPC エンドポイントはこのようなメッセージではバイパスされるため、（GTPC エンドポイントで）GTPC メッセージ レベルのメトリックはサービス間 GTPC メッセージについてはペグされません。
   - 既存のサービス間メトリックは、サービス間メッセージに対してペグされます。
   - コマンド メッセージで開始された UBR と DBR は、既存のメッセージ フロー パスに従います。つまり、SMF は gtpc-ep ポッドを介して cnSGW サービスにコマンド メッセージを送信します。

## 機能設定

cnSGW と SMF サービス間の GTPC バイパスを有効にするには、次の構成例を使用します。

```
config
  instance instance-id gr_instance_id
    endpoint gtp
      enable-gtpc-bypass { false | true }
      end
```

注：

- **endpoint gtp**：GTP エンドポイント構成を入力します。
- **enable-gtpc-bypass { false | true }**：cnSGW と SMF サービス間の GTPC バイパスを有効または無効にするオプションを指定します。

  true に設定すると、SMF と cnSGW の間で GTPC バイパスが有効になります。つまり、SMF と cnSGW は、gtpc-ep ポッドを介さずに直接通信します。デフォルトは False です。

## OAM サポート

ここでは、この機能の操作、管理、およびメンテナンス サポートについて説明します。

### バルク統計サポート

この機能をサポートするために、次の統計情報が更新されています。

- smf_service_stats：この統計には、GTPC バイパス メッセージを追跡するための gtpc_bypass ラベルが含まれます。

バルク統計情報のサポートの詳細については、「*UCC 5G SMF* メトリック リファレンス」を参照してください。

# ユースケースと機能

ここでは、SMF がサポートする使用例について説明します。

# 基本 SMF 構成

SMF 基本構成は、SMF を動作させるために必要な構成の詳細なビューを提供します。これには、SMF を展開するためのインフラストラクチャの構成、SMI を介した SMF の展開、および長期的に SMF の機能を利用するための Ops センターの構成が含まれます。

SMI の詳細については、『*Ultra Cloud Core SMI* クラスタ デプロイヤ操作ガイド』を参照してください。

次の機能は、このユース ケースに関連しています。

- Ops センターを介した SMP の展開と構成 （37 ページ）

# 4G セッションのサポート

表 *5:* 機能の履歴

| 機能名 | リリース情報 | 説明 |
|---|---|---|
| FWA サポート | 2025.01.0 | SMF は、個別のサブスクライバグループ（4Gインターフェイス（RADIUS および Gz）を使用しているグループと 5G SBA インターフェイス（N7 および N40）を使用しているグループ）の 4G 固定ワイヤレスアクセス（FWA）を検証およびサポートします。 |

UE の場合、SMF は 5G と 4G NAS の両方をサポートして、4G と 5G の両方のコア ネットワークに接続します。SMF には EPS インターワーキング サポートが含まれており、PGW-C + SMF として機能します。4G セッションの作成に使用される Gx、Gy、Gz などのインターフェイスは、Npcf や Nchf などの対応する 5G コア SBI インターフェイスに置き換えられます。

SMF は N26 インターフェイス（MME と 5GS AMF 間の CN 間インターフェイス）を使用して EPS とのインターワーキングをサポートし、Evolved Packet Core（EPC）と NG コアネットワーク間のインターワーキングを可能にします。ネットワークでの N26 インターフェイスのサポートは、インターワーキングではオプションです。N26 インターフェイスは、S10 インターフェイスの機能のサブセットをサポートし、インターワーキングを可能にします。UE では、コアネットワークに基づく EPC NAS または 5GC NAS の手順を使用します。SMF は、アクセスおよびモビリティ手順の QoS フロー障害をサポートしています。

次に、FWA サブスクライバを処理するための SMF からのサポートを確認するために検証された 2 つのシナリオを示します。

1. RADIUS アカウンティングと Gz アカウンティングを使用するサブスクライバ。
2. ポリシーに N7 を使用し、オンライン課金設定に N40 を使用するサブスクライバ。

次の表に、前述のシナリオで FWA サブスクライバに対してサポートされているインターフェイスとサポートされていないインターフェイスの詳細を示します。

| | RADIUS 認証 | RADIUS Acct | N7 | N40 | N10 | Gz（CDR） | Gy | Gx |
|---|---|---|---|---|---|---|---|---|
| シナリオ 1 | 非対応 | はい | 非対応 | いいえ | 非対応 | はい | 非対応 | 非対応 |
| シナリオ 2 | いいえ | 非対応 | はい | はい（オンラインのみ） | いいえ | いいえ | いいえ | 非対応 |

（注） SMF は、異なる DNN にまたがるコンバージド コア上の 4G と 5G SBI インターフェイスを使用して、両方のタイプのサブスクライバをサポートします。

SMF では、すべてのサブスクライバで次を実行できます：

- デフォルトの QoS フロー識別子（QFI）の QoS クラス識別子（QCI）のアップグレードとダウングレード
- APN-AMBR のアップグレードとダウングレード：APN 集約最大ビットレートを調整する機能。

次の機能は、このユース ケースに関連しています。

- 4G から 5G へのデータ セッションのハンドオーバー （504 ページ）
- EPS インターワーキング （197 ページ）
- アクセスおよびモビリティの手順のフロー失敗の処理 （463 ページ）
- 統合された SMF による複数世代のデバイス サポートの管理 （1755 ページ）
- セッション タイマー （1737 ページ）

# 5G セッションのサポート

5G システム アーキテクチャのセッションおよびサービス継続性（SSC）サポートは、ユーザー機器（UE）のさまざまなアプリケーションとサービスの継続的な要件に対応します。5G システムは、ネットワークが UE への接続サービスを維持するように、SSC モードをサポートします。SMF は、セッションを確立するための UE IP アドレスと ID の割り当てを管理します。SMF は、課金を容易にするために、N40、N4、N7、N10 などのインターフェイスでセッション接続を維持します。

SMF は、AMF が変更されておらず、UPF を再配置することなく、Xn インターフェイスを使用してソース NG-RAN からターゲット NG-RAN に UE をハンドオーバーします。SMF には、コントロール プレーン（CP）での通知を有効にし、UPF でバッファリングを有効にするための N3 トンネル プロファイル構成が含まれています。SMF は、PDU セッションのユーザープレーン（UP）接続のアクティブ化および非アクティブ化をサポートしています。SMF には、ホスト名とその IP アドレスを解決するためのプロキシ サーバーを構成する DNS プロキシ機能も含まれています。

次の機能は、このユース ケースに関連しています。

- gNodeB 間ハンドオーバー （533 ページ）
- DNN ごとの IP プールの割り当て （1042 ページ）
- UP セッションのアクティブ化と非アクティブ化のサービス要求手順 （1953 ページ）
- セッションおよびサービス継続性モード （1733 ページ）

- 静的 IP サポート （918 ページ）
- AMF からの TAI 選択 （1921 ページ）

# アクセスとモビリティのサポート

SMF では、PDU セッションの確立、変更、およびリリースのセッション管理手順を通じたアクセスとモビリティがサポートされます。SMF は、データ転送トンネル（DFT）および間接データ転送トンネル（IDFT）の場合に、UE が 1 つの NG-RAN から別の NG-RAN に移動するときに、SMF 内または AMF 間での N2 ベースのハンドオーバーをサポートします。マルチ DNN のサポートにより、SMF は複数の PDN 接続を提供し、インターネットや Voice over New Radio（VoNR）サービスなどのさまざまなサービスを提供します。SMF では、UE が CM アイドル状態または CM 接続状態の場合に、ネットワーク開始メッセージがサポートされます。

アクセスとモビリティのサポートには、次のハンドオーバーをサポートする 5G 内ハンドオーバーのユースケースが含まれます：

- Xn ハンドオーバー
- AMF 内 N2 ハンドオーバー
- AMF 間 N2 ハンドオーバー

次の機能は、このユース ケースに関連しています。

- 5GSM 原因コードの処理 （773 ページ）
- AN によって開始されたセッションの変更とリリース （83 ページ）
- アクセスとモビリティの手順のための CHF と PCF の統合 （521 ページ）
- gNodeB 間ハンドオーバー （533 ページ）
- PCO での MTU サポート （1017 ページ）
- DNN のサポート （1021 ページ）
- ネットワーク開始型セッション変更手順 （1085 ページ）
- ポリシーおよびユーザー プレーンの管理 （1251 ページ）
- UDM の統合 （1929 ページ）
- 音声の新しいラジオ （611 ページ）

# 課金統合

SMF はコンバージド チャージングをサポートし、Nchf または N40 インターフェイスを使用して課金イベントを生成します。SMF は、課金（CHF）サーバで障害が発生した場合の課金のオフライン フェールオーバーをサポートしています。SMF は、受信する課金データ情報に基づいて、オンライン課金とオフライン課金をレポート レベルでサポートします。

次の機能は、このユース ケースに関連しています。

- サブスクライバの課金 （1853 ページ）

# クラウド ネイティブ インフラストラクチャ

SMF サービスには、PDU セッション管理 API 呼び出しを処理するための構成が含まれています。IP アドレス管理（IPAM）技術は、ネットワークの IP アドレス空間を追跡および管理するために、アプリケーション サービス レイヤの SMF と統合されています。SMF は、システムレベルのインフラストラクチャであるオペレーション センター インターフェイスを使用して、マイクロサービスの展開を開始し、アプリケーション固有の構成を 1 つ以上のマイクロサービスにプッシュし、アプリケーション固有のコマンドを実行してアプリケーション固有のポッドで API を呼び出します。

次の機能は、このユース ケースに関連しています。

- 負荷および過負荷管理 （1155 ページ）

# コンバージド コア ネットワーク

SMF は、スタンドアロン展開、または 4G および 5G サブスクライバにサービスを提供するための cnSGWc との統合展開をサポートします。コンバージド コントロール プレーン機能は、4G および 5G のコントロール プレーン インスタンス、つまり SMF と cnSGWc の組み合わせで構成されます。

コンバージドコア展開では、同じ PDN セッションに対して、S-GW と SMF は同じ UPF インスタンスを選択するため、データパスが最適化されます。コンバージドコア アーキテクチャは、運用コストと複数の異なるネットワークを維持する複雑さを軽減し、新しいインターフェイスとビジネス手段を活用します。

統合コアの展開では、SMF のいくつかの基本的な構成、ポッド レイアウトの変更、およびコール処理によるパフォーマンスの最適化が必要になります。

次の機能は、このユース ケースに関連しています。

- アラート （2071 ページ）
- コンテンツ フィルタリングと X-Header の強化
- Ops センターを介した SMP の展開と構成 （37 ページ）
- ダイナミック ルーティング （1551 ページ）
- EPS インターワーキング （197 ページ）
  - GTP パス障害の処理、復元、およびリカバリ （317 ページ）
  - UE 初期接続のサポート （205 ページ）
- サブスクライバのモニタリングとプロトコルのモニタリング （2063 ページ）

- ポッドとサービスの参考資料 （1231 ページ）
- ポリシーおよびユーザー プレーンの管理 （1251 ページ）
  - UPF ノード レポートと独自のセッション レポートのサポート （1372 ページ）
  - 静的 PCC ルールのサポート （1322 ページ）
- メトリック （2096 ページ）
- UPF パスの管理と復元 （1983 ページ）
- ワイヤレス優先順位サービス （2003 ページ）

# IMS サポート

IP マルチ メディア サブシステム（IMS）は LTE ネットワークおよび 5G コアに（UPF ノードを介して）接続し、Voice over LTE（VoLTE）や Voice over New Radio（VoNR）などの音声サービスを提供します。

次の機能は、このユース ケースに関連しています。

- LTE の音声サポート （590 ページ）
- 音声の新しいラジオ （611 ページ）
- VoLTE および VoNR の NPLI サポート （603 ページ）

# IPAM のサポート

IPアドレス管理（IPAM）は、ネットワークの IP アドレスを追跡および管理するための技術です。IPAM は、サブスクライバ管理システムのコア コンポーネントの 1 つです。IPAM は、クラウドネイティブのサブスクライバ管理システムと連携するために必要なすべての機能を提供します。また、IPAM は、セッション管理機能（SMF）、ポリシー制御機能（PCF）など、さまざまなネットワーク機能の汎用 IP アドレス管理システムとして機能します。

次の機能は、このユース ケースに関連しています。

- IP アドレス管理 （893 ページ）

# 合法的傍受

合法的傍受（LI）機能を使用すると、法執行機関（LEA）がサブスクライバの通信を傍受できます。LI 機能を使用すると、ネットワーク オペレータは、対象のモバイル ユーザーのデータ メッセージを傍受と制御できるようになります。PDU セッションのコントロール プレーンのアクションを処理する SMF には、関連する xIRI を生成する LI 機能を持つ IRI-POI が含まれます。

詳細については、Cisco アカウント担当者にご連絡ください。

# MVNO サポート

SMF は、エンタープライズ MVNO モデルをサポートします。モバイル ネットワーク オペレータは、リースされた MVNO サブスクライバのセカンダリ認証を実行でき、AAA サーバーに関連する追加の機能もサポートできます。SMF は、このようなセカンダリ認証の目的で RADIUS プロトコルを使用します。

次の機能は、このユース ケースに関連しています。

- 複数および仮想 DNN のサポート
  - DNN の大文字と小文字を区別しないサポート
- ポリシーおよびユーザー プレーンの管理
  - 帯域幅ポリシーあたりの最大グループ数の増加
- RADIUS Client
  - RADIUS 切断および CoA 要求の処理
  - RADIUS アクセス管理
  - RADIUS アカウンティング
  - RADIUS PAP/CHAP/MSCHAP サポート
  - RADIUS NAS-IP サポート

# NF 管理

データ接続用の 5G システム用に 3GPP で定義されたアーキテクチャ モデルに基づいて、SMF は一連の NF インスタンスとそれらに関連する NF サービス インスタンスを検出します。NF プロファイルに基づくこれらのインスタンスは、ネットワーク リポジトリ機能（NRF）に登録され、さまざまな入力クエリ パラメータを満たします。

次の機能は、このユース ケースに関連しています。

- NF の検出と管理 （1099 ページ）
- 障害処理サポート （411 ページ）

# OAM サポート

このユース ケースは、SMF のすべての運用、管理、およびメンテナンス（OAM）機能を対象としています。

次の機能は、このユース ケースに関連しています。

- アラート （2071 ページ）

- バルク統計情報と重要業績評価指標 （2100 ページ）
- Ops センターを介した SMP の展開と構成 （37 ページ）
- ログ （2100 ページ）
- メトリック （2096 ページ）
- サブスクライバのモニタリングとプロトコルのモニタリング （2063 ページ）
- ポッドとサービスの参考資料 （1231 ページ）
- スマートライセンス （43 ページ）
- SMF ローリング ソフトウェアの更新 （59 ページ）

# ポリシー統合

SMF は、統合データ管理（UDM）およびポリシー制御機能（PCF）と通信して、次のことを実行します。

- 保証ビットレート（GBR）および非 GBR フローの登録済みおよび承認済み QoS パラメータを取得する
- 関連情報を UE（NAS）、gNB（NGAP）、UPF（PFCP）に渡す

これにより、ネットワーク上のすべてのノードが PDU セッションに必要な QoS を提供するようになります。

SMF は PCF とサービス ベースの N7 インターフェイスを使用して、UE の PDU セッションに対応するセッション管理ポリシー情報を取得します。SMF は、PDU セッション確立手順中に PCF を選択します。また、PCF が提供するセッション管理ポリシーサービスのコンシューマとしても機能します。

次の機能は、このユース ケースに関連しています。

- DSCP マーキング
- ポリシーおよびユーザー プレーンの管理 （1251 ページ）
- ワイヤレス優先順位サービス （2003 ページ）

# RADIUS サポート

5G アーキテクチャでは、サービスを提供するネットワークは、認証時にサブスクリプション永久識別子（SUPI）を認証し、UE とネットワーク間のキー契約を認証します。さらに、サービスを提供するネットワークは、携帯電話事業者のドメイン外のデータ ネットワークに対してセカンダリ認証を実行できます。

次の機能は、このユース ケースに関連しています。

- RADIUS 認証およびアカウンティング （1407 ページ）

# 冗長性サポート

K8 クラスタでの SMF の導入は、高可用性（HA）と地理的冗長性（GR）をサポートする上で重要な役割を果たします。冗長性サポートは、ラックまたはクラスタの障害時にクラスタ間のステートフル セッションの継続性を保証します。

SMF は、シングルポイント障害を回避するための各クラスタ コンポーネントの冗長なセットアップにより HA を実現します。

GR は、ラック間で 2 つの個別の K8 クラスタ間でデータを複製するラック レベルの冗長性を提供します。これにより、ラックまたはクラスタで障害が発生した場合、トラフィックをリモート ラックに切り替えてトラフィックを処理できます。ラックまたはクラスタの障害は、電源障害、マルチコンピューティング障害、ネットワーク障害、マルチポッド障害、BFD リンク障害などが原因である可能性があります。

次の機能は、このユース ケースに関連しています。

- 高可用性のサポート （1535 ページ）
- ラック間冗長性サポート （1544 ページ）
- すべての UPF へのメッシュ接続 （1015 ページ）

# ローミングのサポート

モバイル ネットワーク事業者は、ローミング パートナーシップを結び、ネットワークが到達しない地域でも、サブスクライバにシームレスにサービスを提供します。PLMNは、通信事業者ネットワークの境界を定義します。HPLMN はサブスクライバのホーム ネットワークで、VPLMN はサービスのレンダリング元の訪問先ネットワークです。

次の機能は、このユース ケースに関連しています。

- ローミングのサポート （1643 ページ）
- 複数 PLMN のサポート （1049 ページ）

# SMF インライン サービス

SMF は、オペレータが課金関連のコストを削減し、サブスクライバに階層化された、詳細な、項目化された請求を提供できるようにする、Enhanced Charging Service（ECS）などのインライン サービス機能を使用します。シャローおよびディープ パケット インスペクション（DPI）を使用して、ECS（アクティブ課金サービス（ACS）とも呼ばれる）では、オペレータは実際の使用状況、バイト数、プレミアム サービス、ロケーションなどに基づいて加入者に請求できます。ECS は、後払いおよびプリペイドの請求システムの料金レコードも生成します。

次の機能は、このユース ケースに関連しています。

- コンテンツ フィルタリングと X-Header の強化
- イベント詳細レコード （339 ページ）
- ポリシーおよびユーザー プレーンの管理 （1251 ページ）

# SMF 仕様への準拠

SMF では、SMF インターフェイス用にさまざまな 3GPP 仕様バージョンがサポートされます。インターフェイスからのメッセージは、対応するサービス用に構成されたコンプライアンス プロファイルに従って処理されます。

次の機能は、このユース ケースに関連しています。

- インターフェイス サポート （643 ページ）

# サブスクリプション管理

SMF は、N10 インターフェイスを介したユーザー サブスクリプション管理を処理します。

次の機能は、このユース ケースに関連しています。

- UDM の統合 （1929 ページ）

# UPF 統合

SMF は、この UPF とインターワーキングするための UPF ノードの非標準要件を満たすために、使用可能な StarOS ベースの UPF ノードを使用します。IPv6 ステートレス自動構成に準拠するために、SMF は ICMPv6 ルータ要請およびアドバタイズメントをサポートしています。

次の機能は、このユース ケースに関連しています。

- ポリシーおよびユーザー プレーンの管理 （1251 ページ）
- IPv6 PDU セッション （1005 ページ）
- UPF パスの管理と復元 （1983 ページ）

# Wi-Fi サポート

SMF は Voice over Wi-Fi（VoWiFi）をサポートしています。VoWiFi テクノロジーは、Wi-Fi ネットワーク経由で接続されているモバイル デバイスから Voice over IP（VoIP）を使用してテレフォニー サービスを提供します。

次の機能は、このユース ケースに関連しています。

- VoWi-Fi サポート （604 ページ）
- Wi-Fi ハンドオーバー （549 ページ）

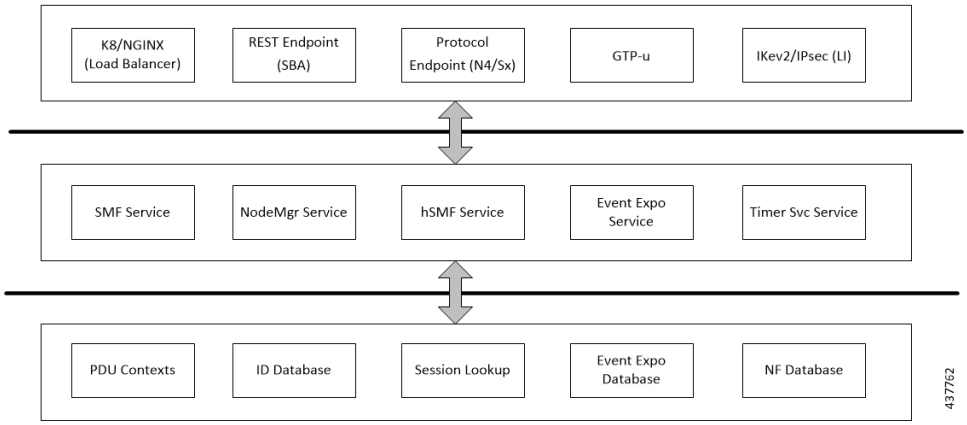
# 展開アーキテクチャおよびインターフェイス

Cisco SMF は、共通のモバイル コア プラットフォーム アーキテクチャを使用する 5G コア ネットワーク機能ポートフォリオの一部です。コア ネットワーク機能には、アクセスおよびモビリティ管理機能（AMF）、ネットワーク リポジトリ（NRF）、ポリシー制御機能（PCF）、ネットワーク スライス選択機能（NSSF）、およびユーザー プレーン機能（UPF）が含まれます。

## SMF アーキテクチャ

SMF ネットワーク機能は、粗い結合のマイクロサービスで構成されます。マイクロサービスの分解は、次の図に示す 3 層のアーキテクチャに基づいています。

**図 *5 : SMF 3* 層のマイクロ サービス アーキテクチャ**




次に、cnSGW-C アーキテクチャの 3 つのレイヤを示します。

- レイヤ 1：プロトコルおよびロード バランサ サービス（ステートレス）
- レイヤ 2：アプリケーション サービス（ステートレス）
- レイヤ 3：データベース サービス（ステートフル）

## SMF の展開

5G モビリティ NF の展開では、次のモードがサポートされます。

- スタンドアロン モード：このモードでは、各 NF は必要なマイクロサービスとともに、Kubernetes の個別の名前空間に展開されます。
- コンバージド モード：このモードでは、複数の NF が単一の名前空間にまとめて展開され、NF に共通のマイクロ サービスが、展開されたすべての NF にサービスを提供します。

# コンバージド コア アーキテクチャ

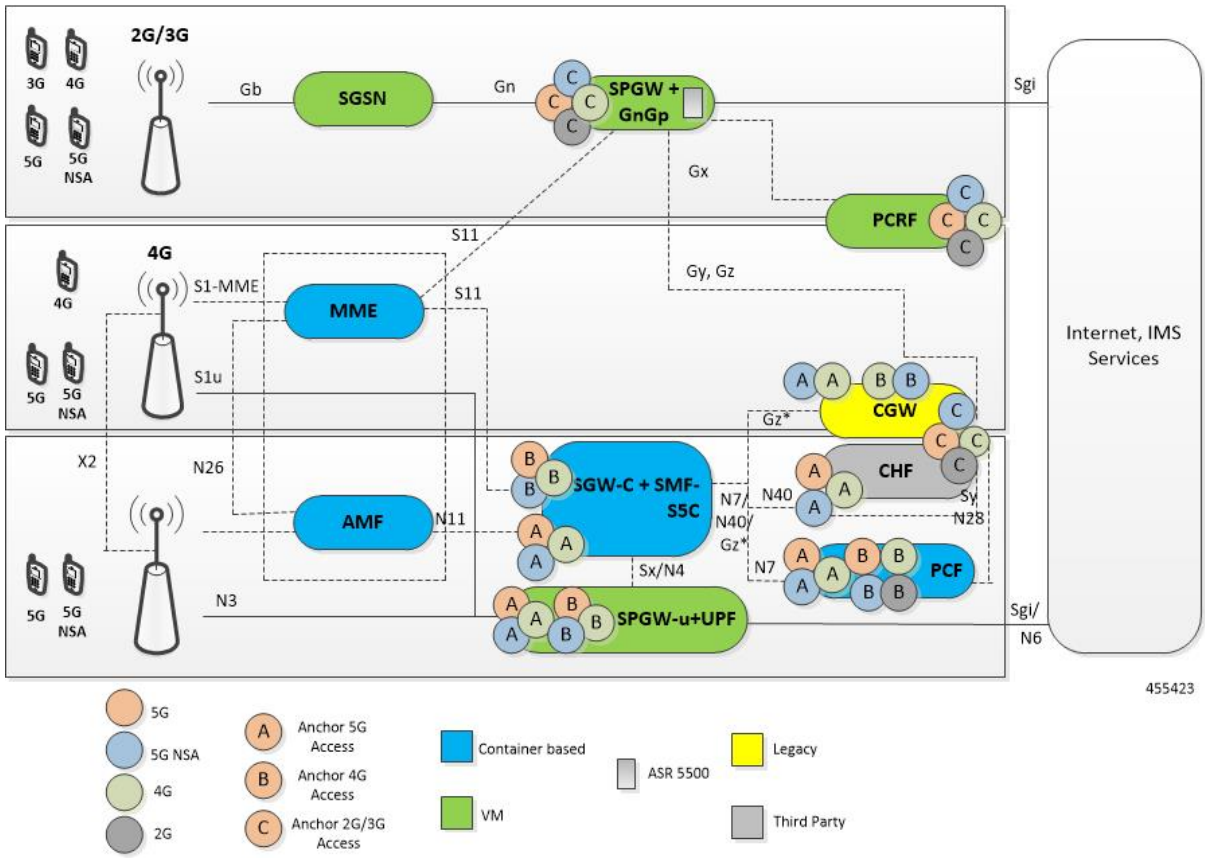
コンバージドコア ソリューションは、SMI アーキテクチャに基づく単一の統合プラットフォームを提供します。サポート アーキテクチャにより、クラウド ネイティブの S-GW および SMF の展開が 5GC および cnSGW-C 機能と統合されます。このソリューションでは、ポリシーおよび課金機能に 3GPP 定義の SBA インターフェイスが使用されます。

コンバージド コア アーキテクチャでは、4G および 5G 対応 UE は、同じコントロール プレーン インスタンスにアンカーされます。コントロール プレーン インスタンスは、SMF、5GC、および cnSGW-C 機能を提供します。

4G と 5G アクセス タイプ間のハンドオフは、5G 対応デバイスではシームレスです。LTE から UTRAN（4G/5G と 3G/2G 間の双方向通信）へのハンドオフは、4G 対応デバイスでシームレスではありません。

次の図に、サポートされるネットワーク アーキテクチャを示します。

**図 *6 :* コンバージド コア アーキテクチャ**




このソリューションの一部として展開される UPF は VPC-SI VM です。UPF の展開は VM ベースであり、以下をサポートしています。

- 同じインスタンス内の SGW-U、PGW-U、および UPF 機能、およびコントロール プレーンへの Sxa、Sxb、Sxab、または N4 インターフェイスの公開。

- 同時に複数の CP インスタンス（最大 4）。

# コンバージド コア展開

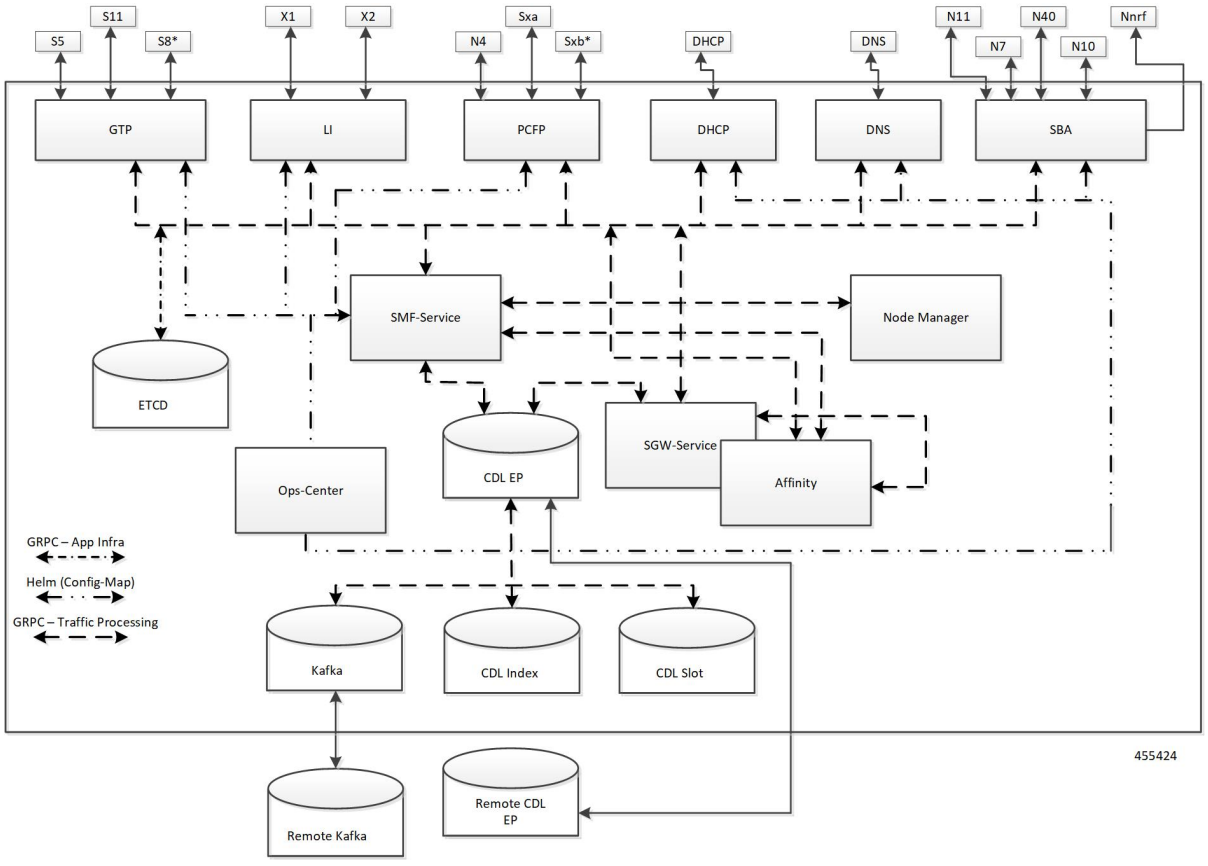
コンバージド コアの展開は、すべてのユースケースに対応するコンバージド コントロール プレーンと統一ユーザー プレーン インフラストラクチャに基づいています。

コンバージド コアの展開では、すべての 4G および 5G 対応 UE は 5G コア（SMF）にアンカーされ、PCF に対しては SBA インターフェイスが使用されます。

コンバージドコア展開には、cnSGW-C や SMF サービスをはじめとする各種マイクロサービスの構成を可能にするコンバージド Ops センターが含まれています。コンポーネントのインストールには、単一の製品 Helm チャートが使用されます。

次の図は、コンバージド S-GW および SMF ネットワーク機能の Kubernetes 展開を示しています。

**図 *7 : Kubernetes* 展開**




プロトコル層サービスは SMF と S-GW 全体で共有されます。GTP エンドポイントは、S11 インターフェイスと S5/S8 インターフェイスを終了します。同様に、PFCP（プロトコル）エンドポイントは、N4 インターフェイスと Sxa インターフェイスを終了します。

SMF および S-GW サービスは個別のポッドとして展開され、セッションの処理は分離されます。両方のサービス ポッドは、サブスクライバ セッションの保存に CDL を使用します。

# サポートされるインターフェイス

このセクションでは、SMF と 5GC の他のネットワーク機能との間でサポートされるインターフェイスについて説明します。

- Diameter：IP ベースのネットワーク全体で、アクセス、許可、およびアカウンティング（AAA）またはポリシーのサポートを必要とするサービスのフレームワークを提供するインターフェイス。
- GTP：2 つのコア UPF 間の基準ポイントとして N9 インターフェイスを使用します。
- Gx：SMF と PCRF 間のインターフェイス。
- Gy：SMF CTF と OCS Charging Data Function（CDF）間のインターフェイス。
- N1/NAS：UE と AMF 間の基準点。
- N2/NGAP -- RANとAMF間の参照ポイント。
- N4：SMF と UPF の間の基準点。
- N7：SMF と PCF の間の基準点。
- N10：UDM と SMF 間の基準点。
- N11：AMF と SMF 間の基準点。
- N40：SMF と CHF の間の基準点。
- Nnrf：インターフェイスは、3GPP 5G システム アーキテクチャ上の NRF によって表示されます。
- RADIUS：ネットワーク アクセスを管理するインターフェイス。
- S2b：PGW-C と ePDG 間のインターフェイス。
- S5：PGW-C と S-GW 間のインターフェイス。
- SBA：NF が相互に通信するためのインターフェイス。

サポートされるインターフェイスの詳細については、インターフェイス サポート （643 ページ） の章を参照してください。

# データ パケットのライフサイクル

次のコール フローは、PDU セッションが正常に確立されるために、SMF のさまざまなポッドを通過するデータ パケットのライフサイクルを示しています。

SMF アプリケーションには、次のポッドが含まれています：

- REST-EP
- キャッシュ
- サービス
- Nodemgr
- プロトコル
- UDP-Proxy
- CDL

図 ***8 : 4G*** セッションの手順 **-** 完全なバイパス（***PFCP*** および ***GTP***）

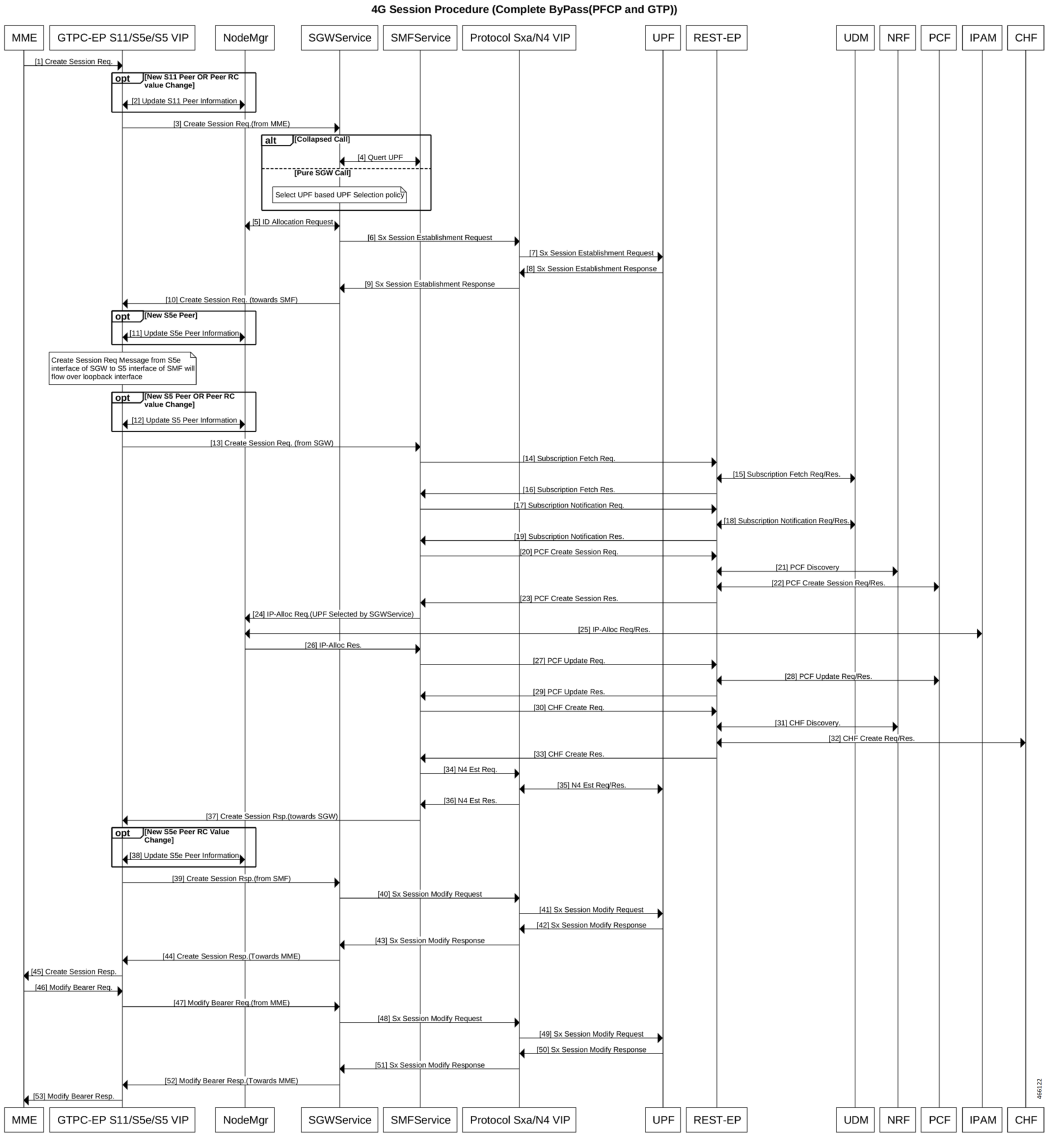


図 *9 : PFCP* および *GTP* 用の *UDP* プロキシを使用した *4G* セッションの手順

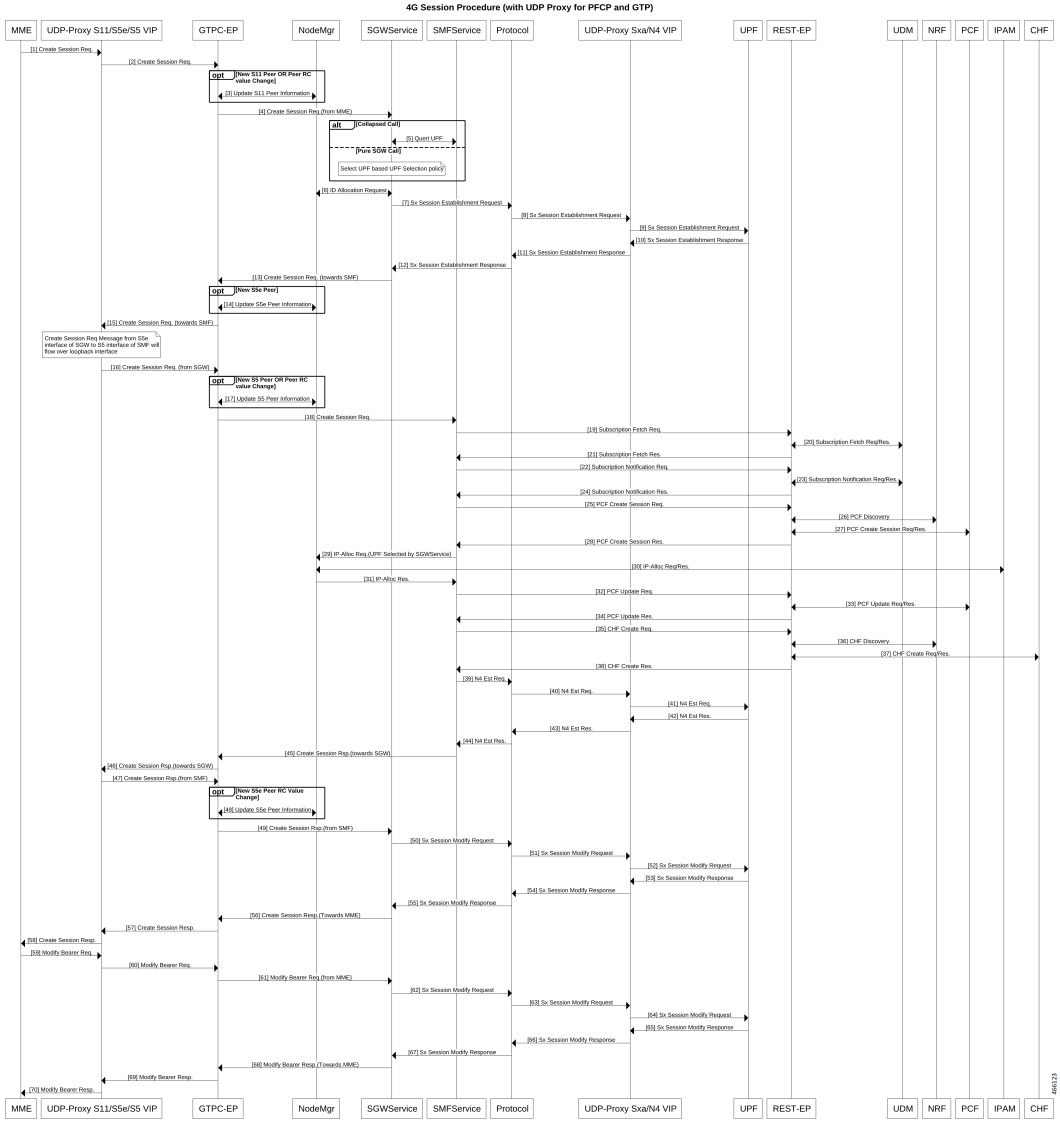


図 *10 :* データ パケットのエンドツーエンド *PDU* セッション確立コール フロー

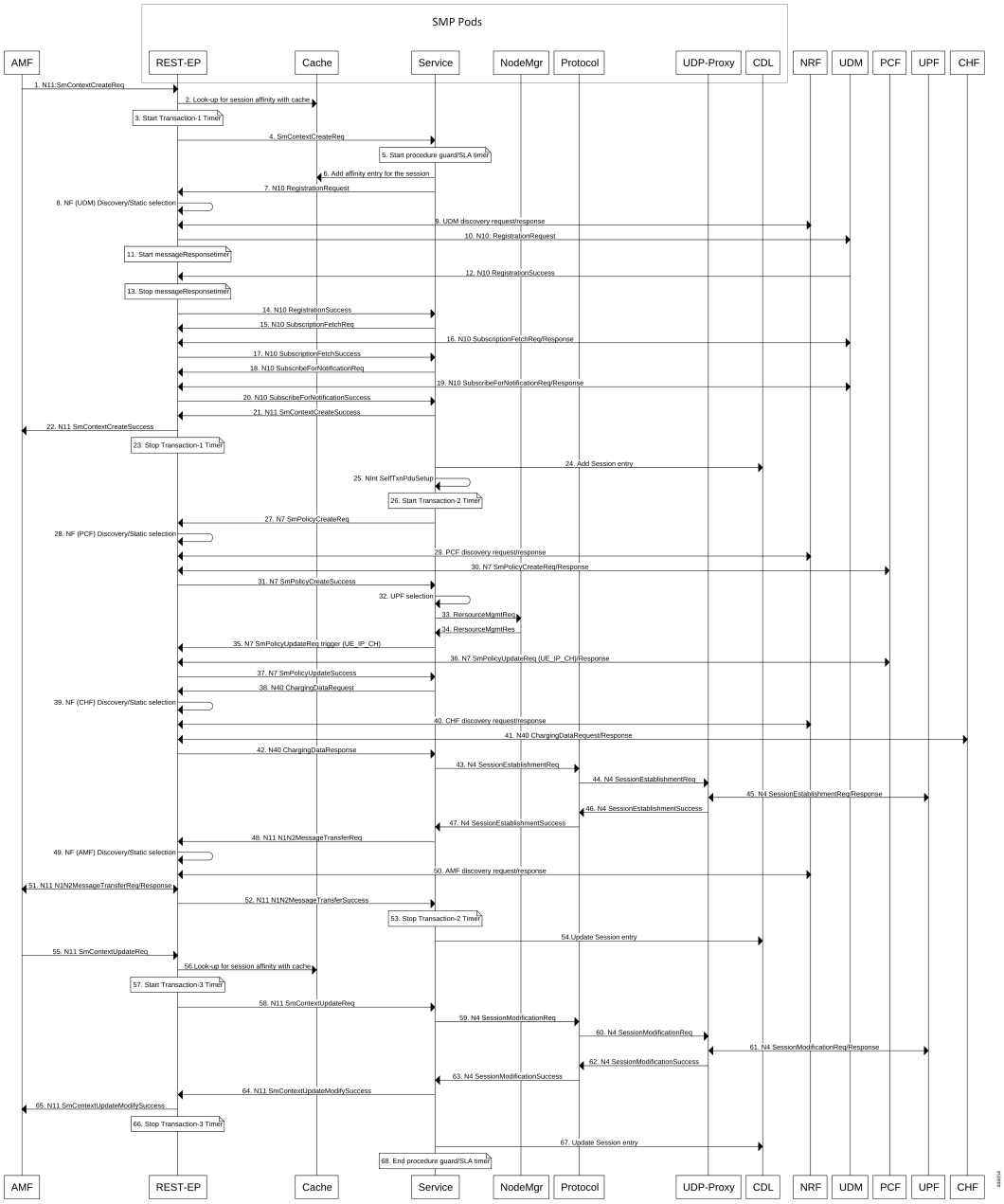



表 *6 :* エンドツーエンド *PDU* セッション確立コール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | AMF は N11:SMContextCreateRequest を SMF に送信し、REST-EP ポッドの VIP IP/外部 IP で終端します。 |

| ステップ | 説明 |
|---|---|
| 2 | REST-EP ポッドは、キャッシュ ポッドとセッション アフィニティのルックアップを実行します。SMF にユーザー セッションのエントリがありません。キャッシュ出力は、ユーザー セッションの SMF サービス アフィニティにはなりません。<br>Kubernetes サービス/ISTIO ロード バランサは、構成されている複数の SMF サービス ポッドから 1 つの SMF サービス ポッドを選択します。 |
| 3 | REST-EP が、トランザクション 1 に関連付けられたタイマーを開始します。PDU セッションの確立手順では、コール フローの異なる段階で開始される 3 つのトランザクションを使用します。<br>SMF のデフォルトのトランザクション タイマーは 10 秒です。トランザクション タイマーは、サービス レベル契約（SLA）の機能を使用して構成できます。 |
| 4 | REST-EP は N11:SMContextCreateRequest を選択した SMF サービスに転送します。 |
| 5 | SMF サービスが手順タイマー（ガード タイマー/SLA タイマー）を開始します。SLA タイマーは構成可能です。 |
| 6 | SMF サービスは、セッションのキャッシュ ポッドを含むアフィニティ エントリを追加します。SMF は、キャッシュが期限切れになるまで、コール フローの後続の段階で、選択された同じ SMF サービスを引き続き使用します。 |
| 7 | SMF サービスは、N10 登録要求をトリガーするよう REST-EP ポッドに指示します。 |
| 8 | REST-EP は、構成に基づいて UDM の NF 検出または静的 NF 選択を実行するかどうかを決定します。 |
| 9 | REST-EP は、UDM 検出要求をコード化して NRF に送信し、UDM のリストを含む正常な応答を受信します。 |
| 10 | REST-EP が N10:RegistrationRequest をエンコードして選択した UDM に送信します。 |
| 11 | REST-EP が messageResponseTimer を開始します。構成可能な messageResponseTimeout のデフォルト値は 2 秒です。messageResponseTimer は、SMF によって開始されるすべてのアウトバウンド HTTP2 メッセージに適用できます。これらは、コール フローの後続の段階では明示的に呼び出されません。 |
| 12 | REST-EP は、UDM から成功した N10:RegistrationResponse を受信します。 |
| 13 | REST-EP が messageResponseTimer を停止します。 |
| 14 | REST EP は N10:RegistrationResponse を SMF サービスに転送します。 |
| 15 | SMF サービスは、N10:SubscriptionFetchRequest をトリガするように REST-EP ポッドに指示します。 |
| 16 | REST-EP は N10: SubscriptionFetchRequest をエンコードして UDM に送信します。<br>REST-EP が UDM から応答を受信します。 |

| ステップ | 説明 |
|---|---|
| 17 | REST-EP は N10:SubscriptionFetchResponse を SMF サービスに転送します。 |
| 18 | SMF サービスは、N10:SubscribeNotificationRequest をトリガするように REST-EP ポッドに指示します。 |
| 19 | REST-EP は N10:SubscribeNotificationRequest をエンコードして UDM に送信します。REST-EP が UDM から応答を受信します。 |
| 20 | REST-EP は N10:SubscribeNotificationRequest を SMF サービスに転送します。 |
| 21 | SMF サービスは N11:SMContextCreateResponse を REST-EP に送信します。 |
| 22 | REST-EP は、N11:SMContextCreateResponse を AMF に転送します。 |
| 23 | REST-EP は、ステップ 3 で開始した transaction-1 タイマーを停止します。 |
| 24 | SMF サービスによって、CDL にセッション エントリ情報が追加されます。 |
| 25 | SMF サービスは、NItSelfTxnPduSetup メッセージを送信することにより、内部トランザクションを開始します。 |
| 26 | SMFサービスが、トランザクション2に関連付けられているタイマーを開始します。 |
| 27 | SMF サービスは、N7:SMPolicyCreateReq をトリガするように REST-EP ポッドに指示します。 |
| 28 | REST-EP は、構成に基づいて PCF の NF 検出またはスタティック NF 選択を実行するかどうかを決定します。 |
| 29 | REST-EP は、PCF ディスカバリ要求をエンコードして NRF に送信し、PCF のリストとともに正常な応答を受信します。 |
| 30 | REST-EP が N7:SMPolicyCreateReq をエンコードし、選択した PCF に送信します。REST-EP が PCF から応答を受信します。 |
| 31 | REST-EP は N7:SmPolicyCreateSuccess を SMF サービスに転送します。 |
| 32 | SMF サービスが UPF 選択を実行します。 |
| 33 | SMF サービスは ResourceMgmtReq を Nodemgr の IPAM モジュールに送信して、UE の IP アドレスを要求します。 |
| 34 | SMF サービスは、IP アドレスを持つ Nodemgr の IPAM モジュールから UE への ResourceMgmtResp を受信します。 |
| 35 | SMF サービスは、トリガ「UE_IP_CH」を使用して N7:SMPolicyUpdateReq をトリガするように REST-EP ポッドに指示します。 |
| 36 | REST-EP エンコードし、選択された PCF に UE_IP_CH トリガを使用して N7:SMPolicyUpdateReq を送信します。REST-EP が PCF から応答を受信します。 |
| 37 | REST-EP が N7:SMPolicyUpdateSuccess を SMF サービスに送信します。 |

| ステップ | 説明 |
|---|---|
| 38 | SMF サービスは、N40:ChargingDataRequest をトリガするように REST-EP ポッドに指示します。 |
| 39 | REST-EP は、構成に基づいて CHF の NF 検出またはスタティック NF 選択を実行するかどうかを決定します。 |
| 40 | REST-EP は、CHF ディスカバリ要求をエンコードして NRF に送信します。REST-EP は、CHF のリストとともに成功応答を受信します。 |
| 41 | REST-EP は N40:ChargingDataRequest をエンコードして、選択された CHF に送信します。REST-EP は CHF から応答を受信します。 |
| 54 | REST-EP は N40:ChargingDataResponse を SMF サービスに転送します。 |
| 43 | SMF サービスは、N4:SessionEstablishmentRequest をトリガするように SMF プロトコル ポッドに指示します。 |
| 44 | SMF プロトコルは N4:SessionEstablishmentRequest をエンコードして UDP プロキシ ポッドに送信します。 |
| 45 | UDP プロキシ ポッドは、N4:SessionEstablishmentRequest を UPF に送信します。UDP プロキシが UPF から応答を受信します。 |
| 46 | UDP プロキシは、N4:SessionEstablishmentResponse を SMF プロトコル ポッドに転送します。 |
| 47 | SMF プロトコルは、N4:SessionEstablishmentResponse を SMF サービスに転送します。 |
| 48 | SMF サービスは、REST-EP に N11:N1N2MessageTransferReq をトリガするように指示します。 |
| 49 | REST-EP は、構成に基づいて AMF の NF 検出またはスタティック NF 選択を実行するかどうかを決定します。 |
| 50 | REST-EP は、AMF ディスカバリ要求をエンコードして NRF に送信します。REST-EP は、AMF のリストとともに成功応答を受信します。 |
| 51 | REST-EP が N11:N1N2MessageTransferReq をエンコードして、選択した AMF に送信します。REST-EP が AMF から成功の応答を受信します。 |
| 52 | REST-EP は N11:N1N2MessageTransferSuccess を SMF サービスに転送します。 |
| 53 | REST-EP は、手順 26 で開始した transaction-2 タイマーを停止します。 |
| 54 | SMF サービスは、CDL のセッション エントリを更新します。 |
| 55 | REST-EP が AMF から N11:SMContextUpdate を受信します。 |
| 72 | REST-EP はキャッシュ ポッドでセッション アフィニティを検索し、セッションを処理する SMF サービスを識別します。 |

| ステップ | 説明 |
|---|---|
| 57 | REST-EP が、トランザクション 3 に関連付けられたタイマーを開始します。 |
| 58 | REST-EP は、N11:SMContextUpdate をステップ 56 で学習した SMF サービス ポッドに転送します。 |
| 59 | SMF サービスは、N4:SessionModificationRequest をトリガするように SMF プロトコル ポッドに指示します。 |
| 60 | SMF プロトコルは、N4:SessionModificationRequest をエンコードして UDP プロキシ ポッドに送信します。 |
| 61 | UDP プロキシ ポッドは、N4:SessionModificationRequest を UPF に送信します。UDP プロキシが UPF から応答を受信します。 |
| 62 | UDP プロキシは、N4:SessionModificationResponse を SMF プロトコル ポッドに転送します。 |
| 63 | SMF プロトコルは、N4:SessionModificationResponse を SMF サービスに転送します。 |
| 64 | SMF サービスは N11:SMContextUpdateSuccess を REST-EP に転送します。 |
| 65 | REST-EP は N11:SMContextUpdateSuccess を AMF に転送します。 |
| 66 | REST-EP は、ステップ 57 で開始された transaction-3 タイマーを停止します。 |
| 67 | SMF サービスは、CDL のセッション エントリを更新します。 |
| 68 | SMF サービスにより手順タイマー（ガード タイマー/SLA タイマー）が停止します。 |

# セッション アフィニティ

SMF はセッション アフィニティをサポートし、ステートレス アーキテクチャを促進します。

一部の SMF サービスインスタンスでサブスクライバセッションのセッション管理手順が進行中の場合、その間に同じサブスクライバに対してネットワークからの別のイベントが送信されます。次に、「smf-rest-ep」や「smf-protocol」などの SMF プロトコルレイヤマイクロサービスによって、これらのイベントが関連する SMF サービスインスタンスに転送されます。これにより、手順が完了するまで、サブスクライバセッションの進行中の手順に関連するすべてのネットワークイベントが同じ SMF サービスインスタンスによって処理されるようになります。

手順が完了すると、サブスクライバセッション情報がデータベースで更新され、SMF サービスインスタンスに対するセッションアフィニティが削除されます。後続のネットワークイベントは、関連するサブスクライバセッション情報をデータベースから取得することにより、使用可能な SMF サービスインスタンスのいずれかで処理できます。

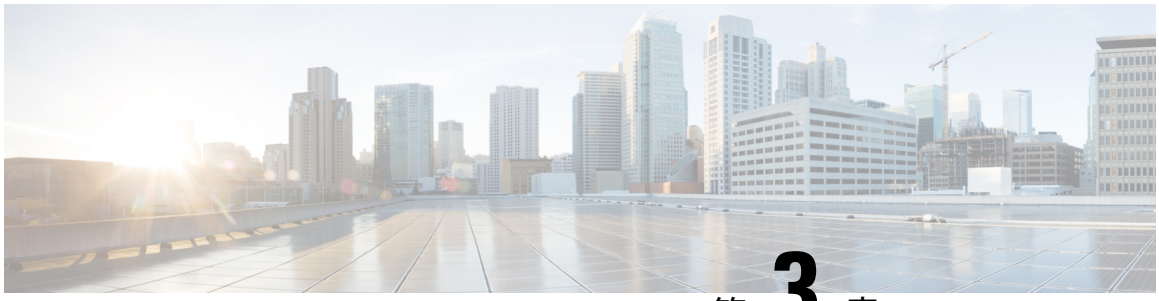
# ライセンス情報

は、シスコ スマート ライセンスをサポートしています。詳細については、「ポリシーを使用してスマート ライセンシングを使用」の章を参照してください。

# 標準準拠

Cisco SMF は、2019 年 6 月 15 日のリリースに記載されている次の 3GPP 標準に準拠しています：

- *3GPP TS 23.510*、バージョン *15.4.0*
- *3GPP TS 29.274*、バージョン *15.8.0*
- *3GPP TS 23.007*、バージョン *15.4.0*
- *3GPP TS 23.501*、バージョン *15.6.0*
- *3GPP TS 29.244*、バージョン *15.6.0*
- *3GPP TS 33.515*、バージョン *0.4.0*
- *3GPP TS 29.510*、バージョン *15.3.0*
- *3GPP TS 32.255*、バージョン *15.3.0*
- *3GPP TS 32.291*、バージョン *15.3.0*
- *3GPP TS 32.290*、バージョン *15.4.0*
- *3GPP TS 29.501*、バージョン *15.4.0*
- *3GPP TS 23.503*、バージョン *15.6.0*
- *3GPP TS 24.501*、バージョン *15.4.0*
- *3GPP TS 24.502*、バージョン *15.4.0*
- *3GPP TS 24.503*、バージョン *15.4.0*
- *3GPP TS 29.518*、バージョン *15.4.0*
- *3GPP TS 23.402*、バージョン *15.3.0*
- *3GPP TS 38.413*、バージョン *15.4.0*
- *3GPP TS 23.401*、バージョン *15.8.0*
- *3GPP TS 29.500*、バージョン *15.8.0*



第 3 章

# Ops センターを介した SMP の展開と構成


- 機能の概要と変更履歴 （37 ページ）
- 機能説明 （38 ページ）
- SMF の展開とアクセス （39 ページ）
- SMF サービスの構成 （41 ページ）
- Day 1 構成のロード （42 ページ）


## 機能の概要と変更履歴

### 要約データ

表 *7:* 要約データ

| | |
|---|---|
| 該当製品または機能エリア | SMF |
| 該当プラットフォーム | SMI |
| 機能のデフォルト設定 | 無効：設定が必要 |
| このリリースでの関連する変更点 | N/A |
| 関連資料 | 該当なし |

### 更新履歴

表 *8:* マニュアルの変更履歴

| 改訂の詳細 | リリース |
|---|---|
| ベア メタル サーバでの SMF の展開がサポートされ、このリリースで完全に認定されています。 | 2021.01.0 |
| 最初の導入。 | 2020.02.0 より前 |

# 機能説明

SMF の展開手順と構成手順では、サブスクライバ マイクロサービス インフラストラクチャ（SMI）の Cluster Deployer を通じて SMF を展開し、SMF オペレーション (Ops) センター を通じて設定やカスタマイズを行います。Ops-Center は ConfD CLI に基づいています。SMF の構成には、NRF プロファイルのデータ構成と、外部から見える IP アドレスとポートが含まれます。

## SMP Ops センター

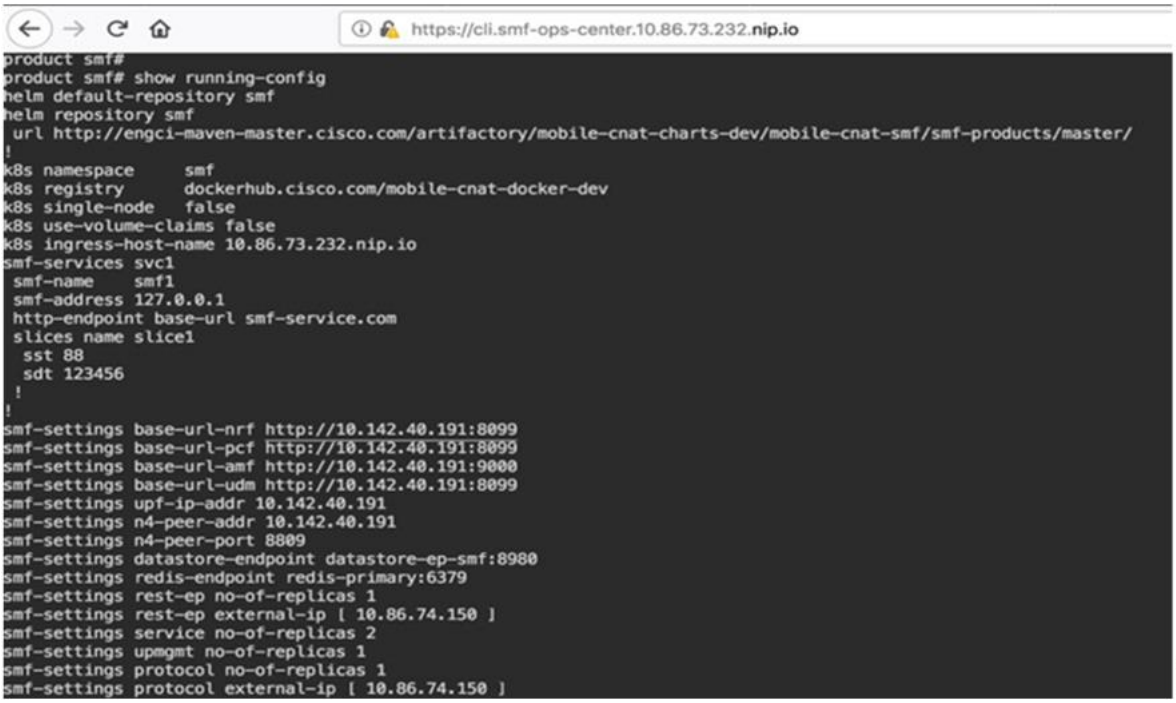
Ops センターは、次の機能を提供するシステムレベルのインフラストラクチャです：

- 展開に関連付けられた Kubernetes オブジェクト（展開、ポッド、サービスなど）のスケールとプロパティを制御する変数 helm チャート パラメータを提供できる柔軟性を備えた、マイクロ サービスの展開をトリガーするユーザー インターフェイス。
- Kubernetes の構成マップを介して、アプリケーション固有の構成を 1 つ以上のマイクロサービスにプッシュするユーザー インターフェイスです。
- アプリケーション固有の実行コマンド（show コマンドや clear コマンドなど）を発行するユーザー インターフェイスです。これらのコマンド：
  - アプリケーション固有のポッドでいくつかの API を呼び出
  - ユーザー インターフェイス アプリケーションから返された情報を表示する

SMF Ops センターを使用すると、ライセンス、SMF エンジン、REST エンドポイント、CDL などの機能を構成できます。

次のスクリーンショットは、Web ベースのコマンドライン インターフェイスの例を示しています：

図 *11 : Ops* センター の *Web* ベース *CLI*




## 前提条件

SMI レイヤに SMF を展開する前に、次の手順を実行します：

- すべての仮想ネットワーク機能（VNF）が展開されていることを確認します。
- SMF Ops センターとクラウドネイティブ共通実行環境（CN-CEE）の SMI 同期操作を実行します。
- 推奨されたポッド展開レイアウトに従って、ノードラベルが構成されていることを確認します。
- NF の要件に従って外部 VIP を設定します。
- ポッド間トラフィックのロードバランスのために Istio を有効にします

# SMF の展開とアクセス

ここでは、SMF を展開する方法と、SMF Ops センターにアクセスする方法について説明します。

# SMF の展開

サブスクライバ マイクロサービス インフラストラクチャ（SMI）プラットフォームは、Cloud Native 5G SMF アプリケーションとその他のネットワーク機能の展開および管理を担当します。

vCenter 環境で SMF Ops Center を展開する方法については、『 *Ultra Cloud Core* サブスクライバ マイクロサービス インフラストラクチャ操作ガイド』の 「製品の展開とアップグレード」の項を参照してください。

ベア メタル サーバ（現在は Cisco UCS-C サーバ）環境に SMF Ops Center を展開する方法については、『ウルトラ クラウド コア サブスクライバ マイクロサービス インフラストラクチャ：オペレーション ガイド』の「ベアメタル上の *SMI Cluster Manager* の運用」のセクションを参照してください。

# SMF Ops センターへのアクセス

次のいずれかのオプションを使用して SMF Ops センターに接続できます。

- SSH
- Web ベースのコンソール

SSH を介して SMF Ops センターに接続するには、次のコマンドを使用します。

**ssh admin**@*ops_center_pod_ip* **-p 2024**

SMI Ops センターで設定したものと同じユーザー名とパスワードを使用します。アクセス制御のユーザー管理の詳細については、*CEE* 構成および管理ガイドを参照してください。

Web ベースのコンソールから Ops センターに接続するには、次の手順を実行します。

1. Kubernetes マスター ノードにログインします。
2. 次のコマンドを実行します。

   **kubectl get ingress** <*namespace*>

   使用可能な入力接続が一覧表示されます。
3. 適切な入力を選択し、SMF Ops センターにアクセスします。
4. Web ブラウザから以下の URL にアクセスします。

   **cli**.<*namespace*>**-ops-center**<*ip_address*>**nip.io**

デフォルトでは、Day 0 の構成が SMF にロードされます。

FQDN およびパスベースの URL ルーティングを使用して Ops センターに接続するには、『 *Ultra Cloud Core Subscriber Microservices Infrastructure - Deployment Guide* 』の「 Configuring Hostname and URL-based Routing for Ingress」セクションを参照してください。

# SMF サービスの構成

SMF サービスには、PDU セッション管理 API コールを処理するための基本構成が含まれています。

## ノードラベルを持つマッピング ポッド

### 前提条件

- ノード ラベルがポッドの展開レイアウトに従っていることを確認します。
- 外部 VIP が NF の要件に従っていることを確認します。
- ポッド間トラフィックのロードバランスのために Istio を有効にします。

ノード ラベルは、クラスタ同期でノードにアタッチされるキーと値のペアです。各ノードには、キーと値のラベルのセットを定義することができます。各キーはノードに対して一意である必要があります。ラベルを使用すると、ユーザーは NF ポッドを疎結合でノードにマッピングできます。

**重要**

- ポッドレベルのラベル付け構成は、SMF がベア メタル サーバに展開されている場合にのみ適用されます。
- ポッドをマッピングする前に、必ず SMI クラスタ デプロイヤでノード ラベルを構成してください。以下は、master-1 ラベル付けのコマンド例です。

```
[cndp-clpnc-cm-cm-primary] SMI Cluster Deployer (config-nodes-master-1)# k8s
node-labels smi.cisco.com/svc-type smf-node
```

ポッドをノード ラベルにマッピングするには、以下の構成例を使用してください。

```
config
   k8 label protocol-layer key label_key value label_value
   k8 label service-layer key label_key value label_value
   k8 label cdl-layer key label_key value label_value
   k8 label oam-layer key label_key value label_value
   end
```

以下は、ポッドからノード ラベルへのマッピングの例です。

```
k8 label protocol-layer key smi.cisco.com/node-type value smf-proto
exit
k8 label service-layer key vm-type value smf-svc
exit
k8 label cdl-layer key smi.cisco.com/node-type value smf-cdl
exit
k8 label oam-layer key smi.cisco.com/node-type value oam
exit
```

# Day 1 構成のロード

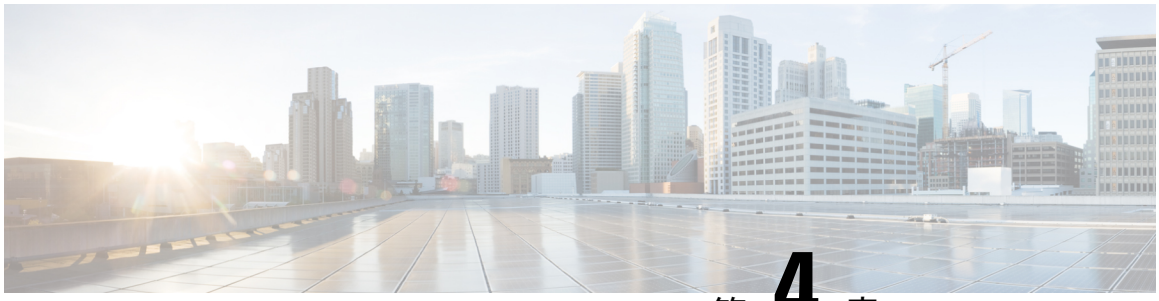
SMF の Day 1 構成をロードするには、以下のコマンドを実行します。

```
ssh admin@ops_center_pod_ip -p 2024  < Day1config.cli
```

または、Day 1 構成をコピーして SMF Ops Center CLI に貼り付け、Day 1 の構成をロードすることもできます。

```
config
  <Paste the Day 1 configuration here>
  commit
  exit
```

SMF の Day 1 構成については、「SMF 構成例 （2115 ページ）」の章を参照してください。



第 4 章

# スマートライセンス


- 機能の概要と変更履歴 （43 ページ）
- 機能説明 （44 ページ）
- スマート ライセンスの設定 （47 ページ）
- スマート ソフトウェア ライセンシングのモニタリングとトラブル シューティング （58 ページ）


## 機能の概要と変更履歴

### 要約データ

**表 *9* : 要約データ**

| | |
|---|---|
| 該当製品または機能エリア | SMF |
| 該当プラットフォーム | SMI |
| 機能のデフォルト設定 | 有効、常時オン |
| このリリースでの関連する変更点 | N/A |
| 関連資料 | 該当なし |

### 更新履歴

**表 *10* : マニュアルの変更履歴**

| 改訂の詳細 | リリース |
|---|---|
| 最初の導入。 | 2020.02.0 より前 |

# 機能説明

シスコでは、従来のライセンシングとスマート ソフトウェア ライセンシングの 2 種類のライセンスモデルを採用しています。従来のライセンシングは、製品アクティベーションキー（PAK） をシスコ製品にインストールすることによって、ソフトウェア アクティベーションで構成されます。製品アクティベーションキーは、他のシスコ機器と同様の方法で発注し、シスコ製品の機能セットのライセンスファイルを取得するために使用する購入可能品目です。この従来のライセンスの場合、Cisco ライセンス サーバとのオンライン通信は不要です。

スマート ソフトウェア ライセンシングは、ライセンスレポートを承認および提供するいくつかのツールを使用する、エンドツーエンドプラットフォームのクラウドベースのライセンシングです。NF に組み込まれたスマート ソフトウェア ライセンシング機能により、製品の登録と承認が完了します。 SMF スマート ソフトウェア ライセンシング モデルをサポートしています。

スマートライセンシングは、シスコのソフトウェア資産の購入、展開、管理を簡素化します。権限付与は Cisco Commerce Workspace（CCW）を介し、Cisco アカウントを通じて購入され、使用するためにバーチャルアカウントにすぐに取り込まれます。このアプローチにより、すべてのデバイスにライセンス ファイルをインストールする必要がなくなります。スマート対応製品では、レポートの使用状況が Cisco に直接通知されます。Cisco Software Central では、お客様は Cisco ソフトウェア ライセンスを1 つの場所で管理できます。ライセンスの所有権と使用状況に関する情報をすぐに利用でき、使用状況やビジネス ニーズに基づいてより良い購入判断ができます。

Cisco スマート ライセンシングの詳細については、
https://www.cisco.com/c/en/us/buy/smart-accounts/software-licensing.html を参照してください。

## Cisco Software Central

Cisco Software Central（CSC）を使用すると、ソフトウェア ライセンスの管理と、単一ポータルからのスマート アカウントの管理が可能になります。CSC インターフェイスを使用して、製品の有効化、ライセンスの管理、更新、ソフトウェアのアップグレードを行うことができます。登録プロセスを完了するには、機能しているスマートアカウントが必要です。

Cisco Software Central にアクセスするには、https://software.cisco.com を参照してください。

## スマート アカウントとバーチャル アカウント

スマートアカウントでは、スマート対応のすべての製品と権限付与を 1 つの場所で管理します。これにより、Cisco ソフトウェアの調達、展開、およびメンテナンスを行うことができます。スマートアカウントを作成するには、要求元の組織を代表する権限が必要です。送信後、要求は承認プロセスを経由します。

バーチャル アカウントは、スマート アカウント内のサブアカウントとして存在します。バーチャルアカウントは、組織の配置、ビジネス機能、地域、または定義された階層に基づくお客

様定義です。スマート アカウント管理者は、バーチャル アカウントを作成および維持できます。

スマート アカウントのセットアップまたは管理の詳細については、https://software.cisco.comを参照してください。

# Cisco スマート アカウントの要求

Cisco スマート アカウントは、スマート ライセンシング対応製品が利用可能なアカウントです。Cisco スマート アカウントを使用すると、デバイスのライセンスの管理とアクティブ化し、ライセンス使用状況のモニタ、Cisco ライセンスの購入の追跡を行えます。透過的なアクセスにより、スマート ライセンス製品をリアルタイムで表示できます。IT 管理者は、Cisco Software Central を使用して、組織のスマート アカウント内のライセンスとアカウント ユーザーを管理できます。Cisco スマート アカウントを作成するには、次の手順を実行します。

**手順**

**ステップ 1** 次の URL にアクセスしてください。

```
https://software.cisco.com
```

**ステップ 2** クレデンシャルを使用してログインし、**[管理（Administration）]** エリアで **[スマート アカウントの要求（Request a Smart Account）]** をクリックします。

**[スマート アカウント要求（Smart Account Request）]** ウィンドウが表示されます。

**ステップ 3** [Create Account] で、次のいずれかのオプションを選択します。

- **はい。私は、自分の会社を代表してスマート アカウントを作成する権限を持っています。**このオプションを選択した場合は、組織を代表して製品とサービスの資格、ユーザー、およびロールを作成し、管理する権限に同意したことになります。
- **いいえ。以下に指定された人がアカウントを作成します。**このオプションを選択した場合は、スマート アカウントを作成する担当者の電子メールアドレスを入力する必要があります。

**ステップ 4** **[アカウント情報（Account Information）]** で

a) [Account Domain Identifier] の横にある [Edit] をクリックします。
b) [Edit Account Identifier] ダイアログボックスで、ドメインを入力し、[OK] をクリックします。デフォルトでは、ドメインはアカウントを作成する担当者の電子メールアドレスに基づいており、このアカウントを所有する企業に帰属している必要があります。
c) [Account Name] に入力します（通常は会社名）。

**ステップ 5** [Continue] をクリックします。
スマート アカウント要求は、アカウント ドメイン識別子によって承認されるまで保留中の状態になります。承認後、設定プロセスを実行するための手順を含む電子メールの確認が送信されます。

# SMF スマート ライセンス

スマート ライセンス機能は、すべての 5G アプリケーション（PCF、SMF、、および NRF）のオンライン ライセンスとオフライン ライセンスのアプリケーション権限をサポートしています。アプリケーションの使用は、コンプライアンス違反（OOC）と期限切れの段階を含む、ライセンスのすべての段階で制限されません。

（注） 使用中のすべてのライセンスに対して 90 日間の評価期間が付与されます。現在、評価期間の終了後も、5G アプリケーションの機能と操作は制限されません。

# ソフトウェアタグと権限付与タグ

このセクションでは、レポートの識別とライセンスの強制に使用できるソフトウェアおよび権限付与タグについて説明します。

### ソフトウェアタグ

製品タグとも呼ばれるソフトウェア タグは、デバイス上の各ライセンス可能なソフトウェア製品または製品スイートを識別するための Smart Licensing システムの一意の識別子です。スマート クライアントは、Cisco ソフトウェア Central 内のスマート製品インスタンスの追加中に識別のためにこのタグを使用します。

SMFには、次のソフトウェア タグがあります。

| 製品タイプと説明 | ソフトウェアタグ |
|---|---|
| Ultra Cloud Core：セッション管理機能（SMF）、基本最小 | regid.2020-04.com.cisco.SMF、1.0_37ffdc21-3e95-4192-bcda-d3225b6590ce |

### 利用資格タグ

権限付与タグはソフトウェアの一部であり、イメージで使用されている機能を識別します。これらのタグは、デバイス上にインストールされているソフトウェア製品の使用状況と権限付与に関する通信の基盤となります。権限付与タグは、プロダクト ID（PID）ライセンスとソフトウェア イメージの両方にマッピングされます。すべてのスマート対応 PID には、1 つ以上の権限タグが含まれています。

以下の権限付与タグで使用するライセンスを識別します。

| 製品タイプと説明 | 権限付与タグ |
|---|---|
| Ultra Cloud Core：セッション管理機能（SMF）、基本最小 | regid.2020-04.com.cisco.SMF_BASE、1.0_b49f5997-21aa-4d15-9606-0cff88729f69 |

（注） ライセンス情報は、ソフトウェアのアップグレードとロールバック中に保持されます。

# スマート ライセンスの設定

SMF の展開後にスマート ライセンスを構成できます。

## CSC へのアクセス権を持つユーザー

このセクションでは、お使いの環境からポータルにアクセスできる場合のスマートライセンスの構成方法について説明します。

### CSC での製品と権限の設定

開始する前に、CSC で製品と権限を設定する必要があります。製品と権限を設定するには、次の手順を実行します：

1. CSC アカウントにログインします。
2. **[製品の追加（Add Product）]** をクリックして、次の詳細を入力します：
   - **[製品名（Product name）]**：展開された製品の名前を指定します。たとえば、 SMF となります。
   - **[プライマリ PM CEC ID（Primary PM CEC ID）]**：展開された製品のプライマリ プロジェクト マネージャの CEC ID を指定します。
   - **[開発マネージャの CEC ID（Dev Manager CEC ID）]**：展開された製品の開発マネージャの CEC ID を指定します。
   - **[説明（Description）]**（任意）：展開する製品の簡単な説明を指定します。
   - **[製品タイプ（Product Type）]**：製品タイプを指定します。
   - **[ソフトウェア ID タグ（Software ID Tag）]**：Cisco アカウント チームから提供されたソフトウェア ID タグを指定します。
3. [作成（Create）] をクリックします。
4. **[製品/権限のセットアップ（Product/Entitlement Setup）]** グリッドから製品を選択してください。
5. **[権限付与（Entitlement）]** ドロップダウン リストから **[新しい権限の作成（Create New Entitlement）]**を選択します。
6. **[権限の追加（Add Entitlement）]** で **[新しい権限（New Entitlement）]** を選択し、次の詳細を入力します。

- **[権限付与の名前（Entitlement Name）]**：ライセンス資格名を指定します。たとえば、 SMF_BASEようになります。
- **説明**：（任意）ライセンスの権限付与に関する簡単な説明を入力します。
- **[権限付与タグ（Entitlement Tag）]**：Ciscoアカウント チームから提供された権限付与タグを指定します。
- **[権限付与タイプ（Entitlement Type）]**：ライセンス権限付与のタイプを指定します。
- **[ベンダー文字列（Vendor String）]**：ベンダー名を指定します。

7. **[権限付与の割り当て（Entitlement Allocation）]**をクリックします。
8. **[権限付与の割り当ての追加（Add Entitlement Allocation）]** をクリックします。
9. **[新しいライセンスの割り当て（New License Allocation）]** に、次の詳細を入力します。
   - **[製品（Product）]**：ドロップダウン リストから製品を選択します。
   - **[権限付与（Entitlement）]**：ドロップダウン リストから権限付与を選択します。
10. [続行（Continue）] をクリックします。
11. **[新しいライセンスの割り当て（New License Allocation）]** ウィンドウに、次の詳細を入力します：
    - **[数量（Quantity）]**：ライセンスの数を指定します。
    - **[ライセンス タイプ（License Type）]**：ライセンスのタイプを指定します。
    - **[有効期限（Expiring Date）]**：購入したライセンスの有効期限を指定します。
12. [作成（Create）] をクリックします。
13. 次のコマンドを使用して、スマート ライセンスのステータスを確認します。

    **show license all**

    **例**：

```
SMF# show license all

Smart Licensing Status
======================
Smart Licensing is ENABLED

Registration:
  Status: UNREGISTERED
  Export-Controlled Functionality: Not Allowed

License Authorization:
  Status: EVAL MODE
  Evaluation Period Remaining: 83 days, 0 hr, 15 min, 8 sec
  Last Communication Attempt: NONE

License Conversion:
```

```
 Automatic Conversion Enabled: true
 Status: NOT STARTED

Utility:
  Status: DISABLED
Transport:
   Type: Smart Transport
   Registration URL: null
   Utility URL: null

Evaluation Period:
  Evaluation Mode: In Use
  Evaluation Period Remaining: 83 days, 0 hr, 15 min, 8 sec

License Usage
=============
License Authorization Status: EVALUATION MODE
  Evaluation Period Remaining: 83 days, 0 hr, 15 min, 8 sec

UCC 5G SMF BASE (SMF_BASE)
  Description: Ultra Cloud Core - Session Management Function (SMF), Base Minimum
  Count: 1
  Version: 1.0
  Status: EVAL MODE
  Export status: RESTRICTED_NOTALLOWED
  Feature Name: <empty>
  Feature Description: <empty>

Product Information
===================
UDI: PID:SMF,SN:6GKJ2OA-NMUWA7Y

Agent Version
=============
Smart Agent for Licensing: 3.0.13
```

### スマートライセンスの登録

ライセンスの対象となる製品を CSC に登録する必要があります。登録するには、CSC から ID トークンを生成する必要があります。

1. CSC アカウントにログインします。
2. **[一般（General）] > [新しいトークン（New Token）]** の順にクリックし、次の詳細を入力します。
   - **[説明（Description）]**：ID トークンについて簡単な説明を提供します。
   - **[期限切れまでの日数（Expires After）]**：トークンが期限切れになるまでの日数を指定します。
   - **[ユーザーの使用の最大数（Max. Number Users）]**：ユーザーのの最大数を指定します。
3. [トークンの作成（Create Token）] をクリックします。
4. **[製品インスタンス登録トークン（Product Instance Registration Token）]** で **[新しい ID トークン（New ID token）]** を選択します。

5. **[アクション（Actions）] > [コピー（Copy）]** の順にクリックします。
6. SMF Ops Center CLI にログオンし、次のコマンドを使用して **ID トークン** を貼り付けます。

   **license smart register** *idtoken*

   例：

```
SMF# license smart register
Value for 'idtoken' (<string>):
MTI2Y2FlNTAtOThkMi00YTAxLWE4M2QtOTNhNzNjNjY4ZmFiLTE2MTc4N
Tky%0AMTA5MDh8ck1jUHNwc3k1ZC9nWFFCSnVEcUp4QU1jTFoxOGxDTU5kQ3lpa25E%0Ab04wST0%3D%0A
SMF#
```

7. 次のコマンドを使用して、スマート ライセンスのステータスを確認します。

   **show license all**

   例：

```
SMF# show license all

Smart Licensing Status
======================
Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: Cisco Systems, Inc.
  Virtual Account: SMF-SMF
  Export-Controlled Functionality: Allowed
  Initial Registration: SUCCEEDED on Apr 15 05:45:07 2020 GMT
  Last Renewal Attempt: SUCCEEDED on Apr 15 05:45:07 2020 GMT
  Next Renewal Attempt: Oct 12 05:45:07 2020 GMT
  Registration Expires: Apr 15 05:40:31 2021 GMT

License Authorization:
  Status: AUTHORIZED on Apr 15 05:45:12 2020 GMT
  Last Communication Attempt: SUCCEEDED on Apr 15 05:45:12 2020 GMT
  Next Communication Attempt: May 15 05:45:12 2020 GMT
  Communication Deadline: Jul 14 05:40:40 2020 GMT

License Conversion:
 Automatic Conversion Enabled: true
 Status: NOT STARTED

Utility:
  Status: DISABLED

Transport:
   Type: Smart Transport
   Registration URL: null
   Utility URL: null

Evaluation Period:
  Evaluation Mode: Not In Use
  Evaluation Period Remaining: 83 days, 0 hr, 10 min, 43 sec

License Usage
=============
License Authorization Status: AUTHORIZED as of Apr 15 05:45:12 2020 GMT

UCC 5G SMF BASE (SMF_BASE)
  Description: Ultra Cloud Core - Session Management Function (SMF), Base Minimum
```

```
  Count: 1
  Version: 1.0
  Status: AUTHORIZED
  Export status: RESTRICTED_ALLOWED
  Feature Name: <empty>
  Feature Description: <empty>

Product Information
===================
UDI: PID:SMF,SN:6GKJ2OA-NMUWA7Y

Agent Version
=============
Smart Agent for Licensing: 3.0.13
```

**注**：

- **license smart register** ：CSC にスマート ライセンスを登録します。
- *idtoken* ：CSC から生成された ID トークンを指定します。

### スマートライセンスの登録解除

スマート ライセンスを登録解除するには、次の手順を実行します。

1. SMF Ops Center CLI にログインして、次のコマンドを使用します。

   **license smart deregister**

2. 次のコマンドを使用して、スマート ライセンスのステータスを確認します：

   **show license all**

   **例**：

```
SMF# show license all

Smart Licensing Status
======================
Smart Licensing is ENABLED

Registration:
  Status: UNREGISTERED
  Export-Controlled Functionality: Not Allowed

License Authorization:
  Status: EVAL MODE
  Evaluation Period Remaining: 83 days, 0 hr, 10 min, 43 sec
  Last Communication Attempt: NONE

License Conversion:
 Automatic Conversion Enabled: true
 Status: NOT STARTED

Utility:
  Status: DISABLED
Transport:
   Type: Smart Transport
   Registration URL: null
   Utility URL: null

Evaluation Period:
```

```
  Evaluation Mode: In Use
  Evaluation Period Remaining: 83 days, 0 hr, 10 min, 43 sec

License Usage
=============
License Authorization Status: EVALUATION MODE
  Evaluation Period Remaining: 83 days, 0 hr, 10 min, 43 sec

UCC 5G SMF BASE (SMF_BASE)
  Description: Ultra Cloud Core - Session Management Function (SMF), Base Minimum
  Count: 1
  Version: 1.0
  Status: EVAL MODE
  Export status: RESTRICTED_NOTALLOWED
  Feature Name: <empty>
  Feature Description: <empty>

Product Information
===================
UDI: PID:SMF,SN:6GKJ2OA-NMUWA7Y

Agent Version
=============
Smart Agent for Licensing: 3.0.13

SMF#
```

**注**：

- **license smart deregister** ：CSC からスマート ライセンスを登録解除します。

# CSC にアクセスできないユーザー

スマート ライセンスの予約機能（永続予約）は、内部環境から CSC にアクセスできないお客様向けに予約されています。この機能で Cisco では、お客様が仮想カウントからライセンスを予約し、それをデバイスの固有デバイス識別子（UDI）に関連付けることができます。スマートライセンス予約は、お客様は、予約済みライセンスを使用してデバイスを切断モードで使用できます。

次のセクションでは、内部環境から CSC にアクセスできないユーザーに向けてスマート ライセンスを予約する手順について説明します。

### スマート ライセンス予約の有効化

SMF Ops Center CLI を使用してスマート ライセンスの予約を有効にするには、次の手順を実行します。

cnSGW-C Ops Center にログインし、次の構成を使用します。

```
config
   license smart reservation
   commit
   exit
```

**注**：

**license smart reservation**：ライセンスの予約をイネーブルにします。

### スマート ライセンス予約要求コードの生成

（注） スマート ライセンス予約要求コードを生成する前に、「スマートライセンス予約の有効化」の手順を実行します。

スマート ライセンス予約要求コードを生成するには、次のコマンドを使用します：

**license smart reservation request**

例：

```
SMF# license smart reservation request
reservation-request-code CJ-ZSMF:6GKJ2OA-NMUWA7Y-Ai75GxtBs-3B
SMF#
Message from confd-api-manager at 2020-04-15 05:51:37...
Global license change NotifyReservationInProgress reason code Success - Successful.
SMF#
```

注：

- **license smart reservation** ：ライセンス予約要求コードを有効にします。
- **license smart reservation request** ：ライセンス予約要求コードを生成します。

重要 SMF Ops Center CLI から生成されたライセンス要求コードをコピーする必要があります。

### CSC からの承認コードの生成

ライセンス予約要求コードを使用してCSCから承認コードを生成するには、以下の手順を実行します。

1. CSC アカウントにログインします。
2. **[ライセンスの予約（License Reservation）]** をクリックします。
3. SMF Ops センター CLI とリクエスト コードをコピーし、**[予約要求コード（Reservation Request Code）]**テキストボックスからリクエスト コードをペーストします。
4. **[特定ライセンスの予約（Reserve a Specific License）** ] オプションをクリックし、*[UCC 5G SMF BASE]*を選択します。

（注） **[予約（Reserve）]** テキストボックスに、値 *1*を入力します。

5. 選択内容を確認します。

6. [承認コードを生成（Generate Authorization Code）] をクリックします。
7. 承認コードが生成され、画面に表示されます。**[クリップボードにコピー（Copy to Clipboard）]** または、**[ファイルとしてダウンロード（Download as File）]** をクリックして、承認コードをダウンロードします。
8. [**閉じる（Close**）] をクリックします。

### スマート ライセンスの予約

スマート ライセンスを予約するには、次の 2 つの方法を使用できます：

- キーベース：CSC から直接、承認コードのコピー済みクリップボードの内容を使用します。
- URL ベース：ローカルサーバーに保存されている、CSC からの承認コードを含むダウンロードしたファイルを使用します。

展開された製品のスマート ライセンスを予約するには：

1. SMF Ops Center CLI にログインして、次のコマンドを入力します。

   **キーベース**：

   **license smart reservation install** *authorization_code*

   **例**：

   ```
   SMF# license smart reservation install
   Value for 'key' (<string>):
   <specificPLR><authorizationCode><flag>A</flag><version>C</version>
   <piid>35757dc6-2bdf-4fa1-ba7e-4190f5b6ea22</piid><timestamp>1586929992297</timestamp>
   <entitlements><entitlement><tag>regid.2020-04.com.cisco.SMF_BASE,1.0_60b1da6f-3832-4687-90c9-8879dc815a27</tag>
   <count>1</count><startDate>2020-Apr-08 UTC</startDate><endDate>2020-Oct-05
   UTC</endDate>
   <licenseType>TERM</licenseType><displayName>UCC 5G SMF BASE</displayName>
   <tagDescription>Ultra Cloud Core - Session Management Function (SMF), Base
   Minimum</tagDescription>
   <subscriptionID></subscriptionID></entitlement></entitlements></authorizationCode>
   <signature>MEYCIQC/9v5LpgFoEk2l4omIgjjk83g5WXjzs09kQnsO8D0jRgIhAMh+
   D6DRuYmqh1TlfJoZxNte0fPKw6fHEY5CEF3+kPQj</signature>
   <udi>P:SMF,S:6GKJ2OA-NMUWA7Y</udi></specificPLR>
   SMF#
   ```

   **URL ベース**：

   **license smart reservation install url { path** *httpPath*
   **[ username** *username* **| password** *password* **] }**

   **例**：

   ```
   SMF# license smart reservation install url { username smf password **** path http://
   209.165.202.155:8000/AuthorizationCode_SN_6OUP5ZY-LMXHB2A.txt }
   ```

2. 次のコマンドを使用して、スマート ライセンスのステータスを確認します。

   **show license all**

   **例**：

```
show license all
Smart Licensing Status
======================
Smart Licensing is ENABLED
License Reservation is ENABLED

Registration:
  Status: REGISTERED - SPECIFIC LICENSE RESERVATION
  Export-Controlled Functionality: Allowed
  Initial Registration: SUCCEEDED on Wed Apr 15 05:53:31 GMT 2020
  Last Renewal Attempt: None

License Authorization:
  Status: AUTHORIZED - RESERVED on Wed Apr 15 05:53:31 GMT 2020

Utility:
  Status: DISABLED
Transport:
   Type: Smart Transport
   Registration URL: null
   Utility URL: null

Evaluation Period:
  Evaluation Mode: Not In Use
  Evaluation Period Remaining: 83 days, 0 hr, 5 min, 15 sec

License Usage
=============
License Authorization Status:
  Status: AUTHORIZED - RESERVED on Wed Apr 15 05:53:31 GMT 2020
  Last Communication Attempt: SUCCEEDED on Apr 15 05:53:31 2020 GMT
  Next Communication Attempt: NONE
  Communication Deadline: NONE

UCC 5G SMF BASE (SMF_BASE)
  Description: Ultra Cloud Core - Session Management Function (SMF),
 Base Minimum
  Count: 1
  Version: 1.0
  Status: AUTHORIZED
  Export status: NOT RESTRICTED
  Feature Name: <empty>
  Feature Description: <empty>
  Reservation:
    Reservation Status: SPECIFIC INSTALLED
    Total Reserved Count: 1
    Term expiration: 2020-Oct-05 GMT

Product Information
===================
UDI: PID:SMF,SN:6GKJ2OA-NMUWA7Y

Agent Version
=============
Smart Agent for Licensing: 3.0.13
```

注：

- **license smart reservation install key** *authorization_code* ：スマート ライセンス承認コードをインストールします。

- **license smart reservation install url** *path* ：ローカル サーバーに保存されている、CSC からの承認コードを含むファイルをダウンロードします。

### 予約済みライセンスの返却

必要に応じて、予約したライセンスを CSC に戻すことができます。次の手順を使用して予約済みのライセンスを返却するします：

1. SGW Ops センターにライセンス予約承認をインストールする場合：
   1. SMF Ops Center CLI にログインして、次のコマンドを使用します。

      **license smart reservation return**

      **例**：

      ```
      SMF# license smart reservation return
      reservation-return-code CJ6m3k-RAvu6b-hMNmwf-mrdcko-NoSwKL-tF7orz-9aNtEu-yVjGAm-D6j
      SMF#
      ```

      （注） 戻りコードの生成に関する問題がある場合は、Cisco Technical Assistance Center に連絡してください。

   2. SMF Ops Center CLI で生成されたライセンス予約の返却コードをコピーします。
   3. CSC アカウントにログインします。
   4. 製品インスタンス タブ内のリストから製品インスタンスを選択します。
   5. **[アクション（Actions）] > [削除（Remove）]** をクリックします。
   6. **[予約リターン コード（Reservation Return Code）]** テキストボックスにリターン コードを貼り付けます。
   7. **[製品インスタンスの削除（Remove Product Instance）]** を選択します。

   **注**：

   - **license smart reservation return**：予約済みのスマート ライセンスを返します。

2. ライセンス予約承認コードがSMF Opsセンターにインストールされていない場合は、次のメッセージが通知されます。
   1. SMF Ops Center CLI にログインし、次のコマンドを使用してリターン コードを生成します。

      **license smart reservation return**
      *authorization_code*

      CSC で生成されたライセンス予約承認コードを貼り付けて、リターン コードを生成します。

2. CSC アカウントにログインします
3. 製品インスタンス タブ内のリストから製品インスタンスを選択します。
4. **[アクション（Actions）] > [削除（Remove）]** をクリックします。
5. **[予約リターン コード（Reservation Return Code）]** テキストボックスにリターン コードを貼り付けます。
6. **[製品インスタンスの削除（Remove Product Instance）]** を選択します。

3. 次のコマンドを使用して、スマート ライセンスのステータスを確認します。

**show license all**

例：

**SMF# show license all**

```
Smart Licensing Status
======================
Smart Licensing is ENABLED
License Reservation is ENABLED

Registration:
  Status: UNREGISTERED
  Export-Controlled Functionality: Not Allowed

License Authorization:
  Status: EVAL MODE
  Evaluation Period Remaining: 83 days, 0 hr, 5 min, 15 sec
  Last Communication Attempt: SUCCEEDED on Apr 15 05:53:31 2020 GMT
  Next Communication Attempt: NONE
  Communication Deadline: NONE

License Conversion:
 Automatic Conversion Enabled: true
 Status: NOT STARTED

Utility:
  Status: DISABLED

Transport:
   Type: Smart Transport
   Registration URL: null
   Utility URL: null

Evaluation Period:
  Evaluation Mode: In Use
  Evaluation Period Remaining: 83 days, 0 hr, 5 min, 15 sec

License Usage
=============
License Authorization Status: EVALUATION MODE
  Evaluation Period Remaining: 83 days, 0 hr, 5 min, 15 sec

UCC 5G SMF BASE (SMF_BASE)
  Description: Ultra Cloud Core - Session Management Function (SMF), Base Minimum
  Count: 1
  Version: 1.0
  Status: EVAL MODE
  Export status: RESTRICTED_NOTALLOWED
```

```
  Feature Name: <empty>
  Feature Description: <empty>

Product Information
===================
UDI: PID:SMF,SN:6GKJ2OA-NMUWA7Y

Agent Version
=============
Smart Agent for Licensing: 3.0.13

SMF#
```

### ライセンス予約要求のキャンセル

SMF Ops Center CLI でライセンス予約要求をキャンセルするには、次の手順を実行します：

SMF Ops Center CLI にログインして、次のコマンドを使用します。

**license smart reservation cancel**

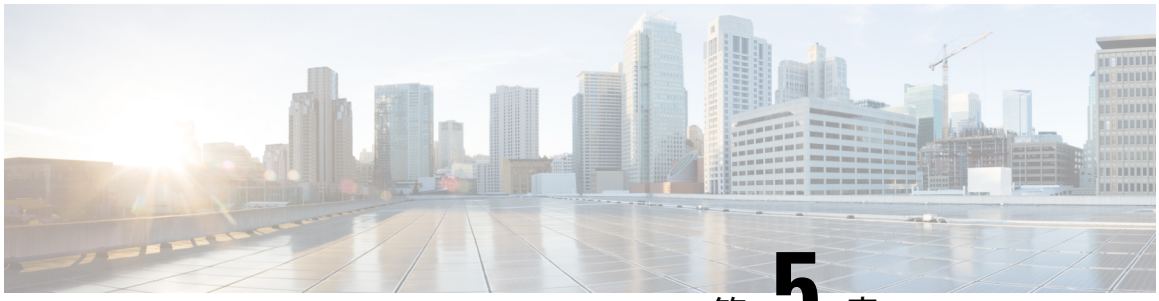
# スマートソフトウェアライセンシングのモニタリングとトラブル シューティング

SMF Ops センターでスマートライセンス情報を表示するには、次の show コマンドを使用します。

**show license [ all | UDI | displaylevel | reservation | smart | status | summary | tech-support | usage ]**

注：

- **all**：ライセンス ステータス、使用状況、製品情報、スマート エージェント バージョンなどのスマートライセンス情報の概要を表示します。
- **UDI**：固有のデバイス識別子（UDI）の詳細を表示します。
- **displaylevel**：情報を表示する深さ。
- **reservation**：スマート ライセンスの予約情報を表示します。
- **smart**：スマート ライセンス情報を表示します。
- **status**：スマート ライセンスのステータス全体を表示します。
- **summary**：スマート ライセンスの概要を表示します。
- **tech-support**：スマート ライセンスのデバッグ情報を表示します。
- **usage**：現在使用されているすべての権限付与のライセンス使用状況情報を表示します。



第 5 章

# SMF ローリング ソフトウェアの更新


- 機能の概要と変更履歴 （59 ページ）
- 機能説明 （60 ページ）
- SMFを更新しています （61 ページ）
- ローリング アップグレード最適化 （71 ページ）


## 機能の概要と変更履歴

### 要約データ

表 *11* : 要約データ

| | |
|---|---|
| 該当製品または機能エリア | SMF |
| 該当プラットフォーム | SMI |
| 機能のデフォルト設定 | N/A |
| このリリースでの関連する変更点 | N/A |
| 関連資料 | 該当なし |

### 更新履歴

表 *12* : マニュアルの変更履歴

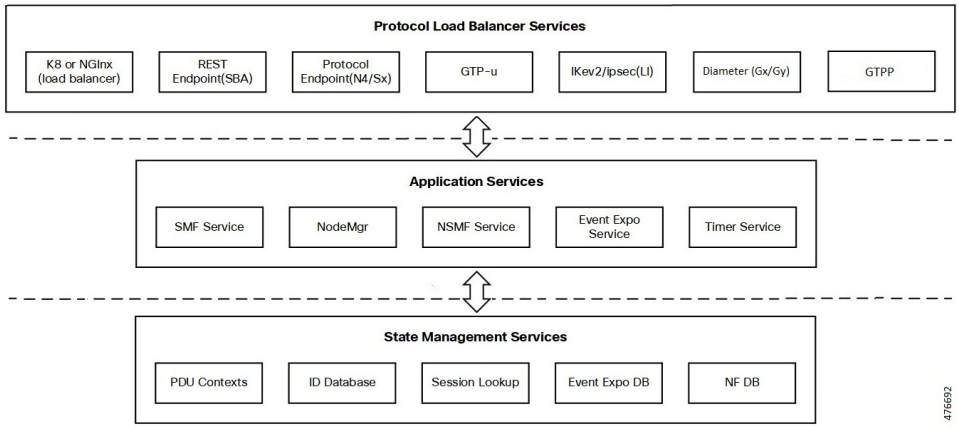
| 改訂の詳細 | リリース |
|---|---|
| Diameter Gx、Gy、およびGZ(GTP-Prime) のサポートを追加 | 2023.02.0 |
| 最初の導入。 | 2020.02.0 より前 |

# 機能説明

Cisco SMF は、プロトコル、サービス、セッション階層で構成される 3 層アーキテクチャで構成されています。各階層には、特定の機能に対する一連のマイクロサービス（ポッド）が含まれます。これらの階層内には、Kubernetes（K8s）マスター ノードとワーカー ノード（運用および管理ノードを含む）で構成される Kubernetes クラスタが存在します。

高可用性と耐障害性を確保するために、各階層に最低2つの K8s ワーカーノードが必要とされています。ワーカー ノードごとに複数のレプリカを設定できます。Kubernetes は、StatefulSets コントローラを使用してポッドをオーケストレーションします。ポッドには、耐障害性のために少なくとも 2 つのレプリカが必要です。

**図 *12 : SMF* アーキテクチャ**




SMF K8s クラスタには 12 のノードが含まれます :

- 3 つのマスター ノード。
- 3 つの運用および管理（OAM）ワーカー ノード。

  OAM ワーカー ノードは、構成管理用の Ops Center ポッドと、統計および重要業績評価指標（KPI）用のメトリック ポッドをホストします。

- 2 つのプロトコル ワーカー ノード。

  プロトコル ワーカー ノードは、サービスベースのインターフェイス（N11、N7、N10、N40、NRF）、UDP ベースのプロトコル インターフェイス（N4, S5/S8, RADIUS）および TCP ベース インターフェイス Diameter（Gx/Gy）と GTPP（Gz）に対応する SMF プロトコル関連ポッドをホストします。

- 2 つのサービス ワーカー ノード。

  サービス ワーカー ノードは、セッション管理処理を実行する SMF アプリケーション関連ポッドをホストします。

- 2 つのセッション（データ ストア）ワーカー ノード。

セッション ワーカー ノードは、サブスクライバのセッション データを保存するデータベース関連ポッドをホストします。

# SMFを更新しています

ここでは、SMF ソフトウェアの更新に関連する手順について説明します。

## SMI Cluster Manager を使用したローリング ソフトウェアの更新

ローリング ソフトウェア アップグレードとは、アプリケーション ポッドの所定の展開セットに対して、ビルドを古いバージョンから新しいバージョンにアップグレードまたは移行したり、パッチをアップグレードしたりするプロセスです。

（注） 2021.02 リリースは、非 HA 展開でのローリングアップグレードまたはインサービス アップグレードをサポートしていません。非 HA 展開でリリース 2021.02 にアップグレードするには、Ops センターから新しい SMF 展開を実行する必要があります。

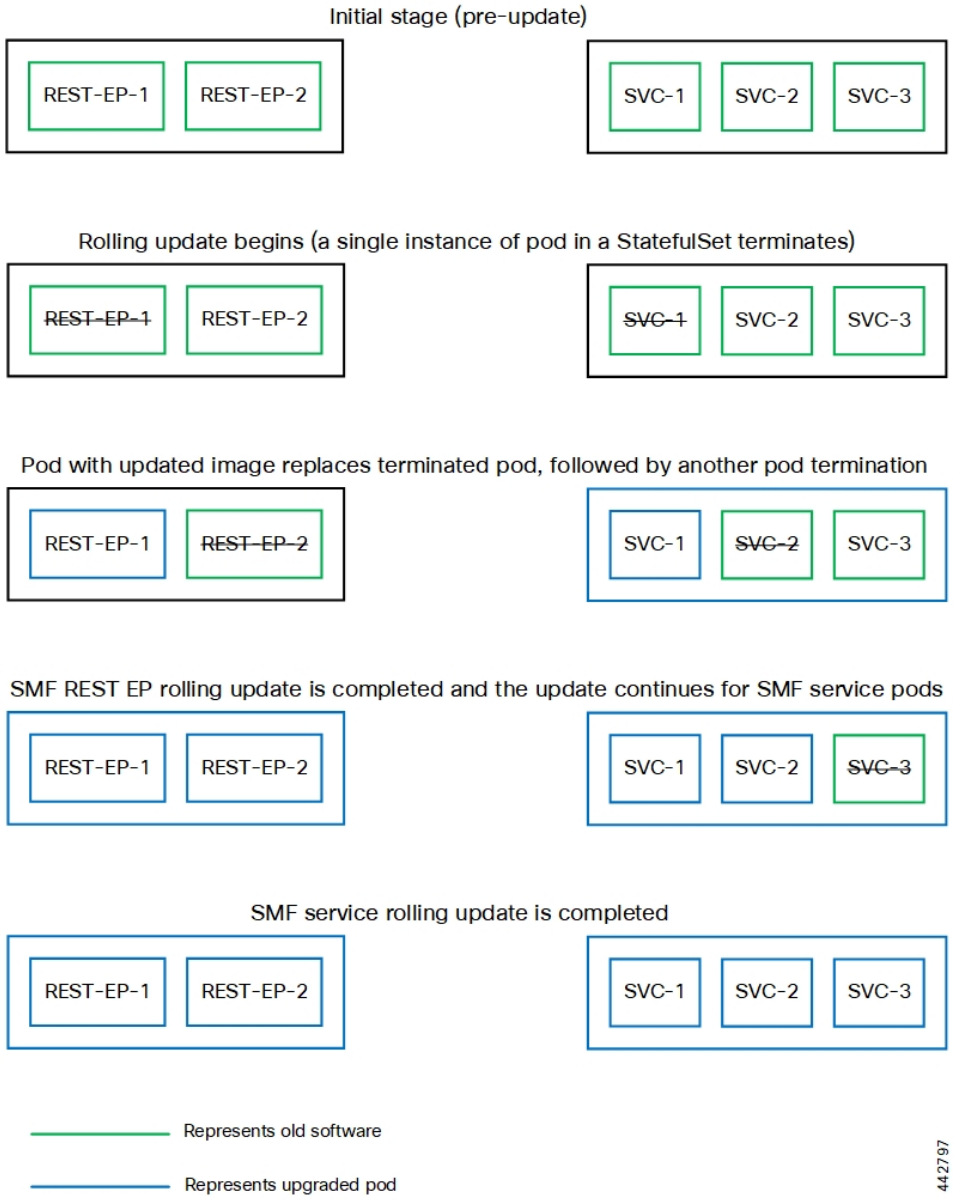
新規展開が完了したら、すべての Geo 冗長（GR）インスタンス対応構成の変更が使用可能であることを確認します。また、 ***k8s volume-claims true*** コマンドを介して ***etcd persistence*** が有効になっている場合は、etcdエントリを必ずクリーンアップしてください。クリーンアップ操作には、 ***kubectl exec -it etcd- <namespace> -etcd-cluster-0 -n cn-cn1 -- etcdctl del --prefix ""***コマンドを実行します。

SMF ソフトウェアのlぴ祖㎜またはインサービスの更新手順では、K8s ローリング戦略を利用してポッドイメージを更新します。K8s ローリング更新戦略では、進行中のプロセスが影響を受けないように、StatefulSet のポッドが順次更新されます。最初に、StatefulSet のローリング更新により、単一のポッドインスタンスが終了します。終了したポッドは、更新されたイメージを持つポッドに置き換えられます。このプロセスは、StatefulSet のすべての複製が更新されるまで続行されます。終了ポッドは、進行中のすべてのプロセスを終了した後、正常に終了します。他のインサービス ポッドは、シームレスなソフトウェアの更新を提供するために、トラフィックを受信して処理し続けます。ソフトウェア更新 プロセスは、Ops Center CLI を使用して制御できます。

（注） 高可用性を実現するには、各ポッドに少なくとも 2 つのポッドが必要です。最悪の場合、ソフトウェアの更新が進行中のときにポッドの処理キャパシティが 50% まで低下することがあります。

次の図は、プロトコル ワーカー ノード上の SMF REST エンドポイント ポッド（2 つのレプリカ）と、サービス ワーカー ノード上の SMF サービス ポッド（3 つのレプリカ）に対する SMF ローリング更新を示しています。

図 *13 : SMF* ローリング更新




重要 ETCD v3.5.x は、3.4.x へのインサービス ダウングレードをサポートしていません。2023.04.0 ビルドから以前のリリースにダウングレードしている場合。ダウングレードの前にシステム モード シャットダウンを実行します。

## 前提条件

SMF のアップグレードのための前提条件は以下の通りです：

- ポッドを含むすべてのノードがアクティブです。
- SMF ソフトウェアのパッチ バージョン。

（注） メジャー バージョンではローリング アップグレードはサポートされていません。

重要 ノードの CPU 使用率が 50% 未満の場合にのみ、ローリング更新をトリガします。

## SMF 正常性チェック

ヘルス チェックを実行する前に、すべてのサービスが実行され、ノードが準備完了状態になっていることを確認します。ヘルス チェックを実行するには、マスター ノードにログ オンし、次の構成を使用します：

```
kubectl get pods -n smi
kubectl get nodes
kubectl get pod --all-namespaces -o wide
kubectl get pods -n smf-wsp -o wide
kubectl get pods -n cee-wsp -o wide
kubectl get pods -n smi-vips -o wide
helm list
kubectl get pods -A | wc -l
```

## アップグレードの準備

ここでは、バックアップ構成、ログ、および展開ファイルを作成する手順について説明します。ファイルをバックアップするには、次の手順を実行します。

1. **ubuntu** ユーザーとして SMI クラスタ マネージャ ノードにログインします。
2. 展開する新しいディレクトリを作成します。

   例：

   ```
   test@smismf-cm01:~$ mkdir -p "temp_$(date +'%m%d%Y_T%H%M')" && cd "$_"
   ```

3. 新しく作成した展開ディレクトリに作業ファイルを移動します。
4. *cnsgw* 展開ファイルを解凍します。

   例：

   ```
   test@smi1smf01-cm01:~/temp_08072019_T1651$ tar -xzvf smf.2020.01.0-1.SPA.tgz
   ./
   ./smf_REL_KEY-CCO_RELEASE.cer
   ./cisco_x509_verify_release.py
   ./smf.2020.01.0-1.tar
   ./smf.2020.01.0-1.tar.signature.SPA
   ./smf.2020.01.0-1.tar.SPA.README
   ```

5. ダウンロードしたイメージを確認します。

   例：

   ```
   test@smi1smf01-cm01:~/temp_08072019_T1651$ cat smf.2020.01.0-1.tar.SPA.README
   ```

重要 「Ops Center 構成のバックアップ」セクションに進む前に、*SPA.README* ファイルに記載されている手順に従ってビルドを確認します。

## Ops センター構成のバックアップ

このセクションでは、Ops Center の構成のバックアップを作成する手順について説明します。

Ops Center の構成のバックアップを実行するには、次の手順を実行します：

1. **ubuntu** ユーザーとして SMI クラスタ マネージャ ノードにログインします。
2. 次のコマンドを実行して、SMI Ops センター構成を `/home/ubuntu/smiops.backup` ファイルにバックアップします。

   **ssh -p** *port_number* **admin@$(kubectl get svc -n smi | grep '.*netconf.*<port_number>' | awk '{ print $4 }') "show run | nomore" > smiops.backup_$(date +'%m%d%Y_T%H%M')**

3. 次のコマンドを実行して、CEE Ops センターの構成を `/home/ubuntu/ceeops.backup` ファイルにバックアップします。

   **ssh admin@<cee-vip> "show run | nomore" > ceeops.backup_$(date +'%m%d%Y_T%H%M')**

4. 次のコマンドを実行して、SMF Ops センターの構成を `/home/ubuntu/smfops.backup` ファイルにバックアップします。

   **ssh admin@<smf-vip> "show run | nomore" > smfops.backup_$(date +'%m%d%Y_T%H%M')**

## CEE および SMF Opsセンター構成のバックアップ

このセクションでは、マスター ノードから CEE および Ops センター構成のバックアップを作成する手順について説明します。

CEE および Ops センターの構成のバックアップを実行するには、次の手順を実行します：

1. マスター ノードに **ubuntu** ユーザーとしてログインします。
2. 構成ファイルをバックアップするためのディレクトリを作成します。

   **mkdir backups_$(date +'%m%d%Y_T%H%M') && cd "$_"**

3. SMF Ops Center の構成をバックアップし、バック アップ ファイルの行数を確認します。

   **ssh -p** *port_number* **admin@$(kubectl get svc -n $(kubectl get namespaces | grep -oP 'smf-(\d+|\w+)') | grep***port_number* **| awk '{ print $3 }') "show run | nomore" >**

**smfops.backup_$(date +'%m%d%Y_T%H%M') && wc -l smfops.backup_$(date +'%m%d%Y_T%H%M')**

例：

```
ubuntu@posmf-mas01:~/backups_09182019_T2141$ ssh -p 2024 admin@$(kubectl get svc -n
 $(kubectl get namespaces | grep -oP 'smf-(\d+|\w+)') | grep <port_number> | awk '{
 print $3 }') "show run | nomore" > smfops.backup_$(date +'%m%d%Y_T%H%M') && wc -l
smfops.backup_$(date +'%m%d%Y_T%H%M')
admin@<ipv4address>'s password: smf-OPS-PASSWORD
334 smfops.backup
```

4. CEE Ops Center の構成をバックアップし、バック アップ ファイルの行数を確認します。

   **ssh -p** *port_number* **admin@$(kubectl get svc -n $(kubectl get namespaces | grep -oP 'cee-(\d+|\w+)') | grep** *port_number* **| awk '{ print $3 }') "show run | nomore" > ceeops.backup_$(date +'%m%d%Y_T%H%M') && wc -l ceeops.backup_$(date +'%m%d%Y_T%H%M')**

   例：

```
ubuntu@posmf-mas01:~/backups_09182019_T2141$ ssh -p <port_number> admin@$(kubectl
get svc -n $(kubectl get namespaces | grep -oP 'cee-(\d+|\w+)') | grep <port_number>
 | awk '{ print $3 }') "show run | nomore" > ceeops.backup_$(date +'%m%d%Y_T%H%M')
&& wc -l ceeops.backup_$(date +'%m%d%Y_T%H%M')
admin@<ipv4address>'s password: CEE-OPS-PASSWORD
233 ceeops.backup
```

5. SMI Cluster Manager からの SMI Ops Center のバックアップ ファイルをバックアップ ディレクトリに移動します。

   **scp $(grep cm01 /etc/hosts | awk '{ print $1 }'):/home/ubuntu/smiops.backup_$(date +'%m%d%Y_T%H%M') .**

   例：

```
ubuntu@posmf-mas01:~/backups_09182019_T2141$ scp $(grep cm01 /etc/hosts | awk '{
print $1 }'):/home/ubuntu/smiops.backup_$(date +'%m%d%Y_T%H%M') .
ubuntu@<ipv4address>'s password: SMI-CM-PASSWORD
smiops.backup                                                 100% 9346
22.3MB/s   00:00
```

6. バックアップ ファイルの行数を確認します。

   例：

```
ubuntu@posmf-mas01:~/backups_09182019_T2141$ wc -l *
  233 ceeops.backup
  334 smfops.backup
  361 smiops.backup
  928 total
```

## 新しい SMF イメージのステージング

このセクションでは、アップグレードを開始する前に新しい SMF イメージをステージングする手順について説明します。

新しい SMF イメージをステージングするには、次の手順を実行します：

1. 新しい SMF イメージをダウンロードして確認します。

2. **ubuntu** ユーザーとして SMI クラスタ マネージャ ノードにログインします。
3. イメージを **Uploads** ディレクトリにコピーします。

   **sudo mv** *smf_new_image.tar* **/data/software/uploads**

（注） SMI は、**Uploads** ディレクトリに存在する新しいイメージを使用して更新します。

4. **Uploads** ディレクトリから処理するために、イメージが SMI によって取得されているかどうかを確認します。

   **sleep 30; ls /data/software/uploads**

   **例**：

   ```
   ubuntu@posmf-cm01:~/temp_08072019_T1651$ sleep 30; ls /data/software/uploads
   ubuntu@posmf-cm01:~/temp_08072019_T1651$
   ```

5. イメージが正常に取得され、処理されたかどうかを確認します。

   **例**：

   ```
   auser@unknown:$ sudo du -sh /data/software/packages/*
   1.6G /data/software/packages/cee.2019.07
   5.3G /data/software/packages/smf.2019.08-04
   16K /data/software/packages/sample
   ```

   SMIは、ステージングを完了するためにイメージを**packages**ディレクトリに抽出する必要があります。

## ローリング ソフトウェア アップグレードのトリガ

SMF は SMI クラスタ マネージャを使用して、ローリング ソフトウェア更新を実行します。SMI Cluster Manager を使用して SMF を更新するには、次の構成を使用します。

**重要** 開始する前に、SMFが稼働しており、最新のバージョンのソフトウェアを実行していることを確認します。

1. SMI Cluster Manager Ops Center にログインします。
2. **software-packages download** *url* コマンドを使用して、URL から最新の TAR ボールをダウンロードします。

   **注**：

   **software-packages download** *url*：HTTP または HTTPS を介してダウンロードするソフトウェア パッケージを指定します。

3. TAR ボールがロードされているかどうかを確認します。

   **例**：

```
SMI Cluster Manager# software-packages list
[ smf-2019-08-21 ]
[ sample ]
```

注：

**software-packages list** ：使用可能なソフトウェア パッケージのリストを指定します。

4. 製品チャートの最新バージョンで製品リポジトリ URL を更新します。

（注） リポジトリのURLに複数のバージョンが含まれている場合、Opsセンターは自動的に最新バージョンを選択します。

```
configure
 cluster cluster_name
  ops-centers app_name smf_instance_name
      repository url
       exit
     exit
```

例：

```
SMI Cluster Manager# config
SMI Cluster Manager(config)# clusters test2
SMI Cluster Manager(config-clusters-test2)# ops-centers smf data
SMI Cluster Manager(config-ops-centers-smf/data)# repository <url>
SMI Cluster Manager(config-ops-centers-smf/data)# exit
SMI Cluster Manager(config-clusters-test2)# exit
```

注：

**clusters** *cluster_name*：展開するノードに関する情報を指定します。 *cluster_name* は、クラスタの名前です。

5. 製品チャートの最新バージョンに更新するには、次のコマンドを実行します。

```
clusters cluster_name actions sync run
```

例：

```
SMI Cluster Manager# clusters test2 actions sync run
```

注：

- **ops-centers** *app_name instance_name* ：製品 Ops センターとインスタンスを指定します。 *app_name* は、アプリケーション名です。 *instance_name* は 、インスタンスの名前です。
- **repository** *url*：チャートをダウンロードするためのローカル レジストリの URL を指定します。
- **actions** ：クラスタで実行されるアクションを指定します。
- **sync run** ：クラスタの同期をトリガーします。

重要
- クラスタ同期により、SMF Ops センターが更新され、アプリケーション ポッドが 1 つずつ自動的に更新されます（**helm sync** コマンドを介して）。
- 特定のポッドでローリング アップグレードをトリガすると、SMF はそのポッドへの新しいコールのルーティングを回避します。
- SMF は、ローリング アップグレードが開始されたポッドを再起動する前に、30 秒間待機して進行中のコールを受け入れます。また、SMF は、アップグレード期間中（最大コール設定時間は 10 秒）に、進行中のすべてのコールを 30 秒以内に完全に確立します。

## アップグレードのモニタリング

以下の構成例を使用して、SMI Cluster Manager Ops Center を介してアップグレードのステータスをモニタします。

```
config
  clusters cluster_name actions sync run debug true
  clusters cluster_name actions sync logs
  monitor sync-logs cluster_name
  clusters cluster_name actions sync status
  exit
```

注：
- **clusters** *cluster_name*：展開するノードに関する情報を指定します。 *cluster_name* は、クラスタの名前です。
- **actions**：クラスタで実行されるアクションを指定します。
- **sync run**：クラスタの同期をトリガーします。
- **sync logs**：現在のクラスタ同期ログを表示します。
- **sync status** ：クラスタ同期の現在のステータスを示します。**debug true**：デバッグ モードを開始します。
- **monitor sync logs**：クラスタの同期プロセスをモニタします。

例：

```
SMI Cluster Manager# clusters test1 actions sync run
SMI Cluster Manager# clusters test1 actions sync run debug true
SMI Cluster Manager# clusters test1 actions sync logs
SMI Cluster Manager# monitor sync-logs test1
SMI Cluster Manager# clusters test1 actions sync status
```

重要 アップグレード後は、CEE Ops センターでポッドの詳細を確認できます。ポッドの詳細については、「ポッド詳細の表示」セクションを参照してください。

# ポッド詳細の表示

CEE Ops センター CLI 内の CEE Ops センターを通して現在のポッドの詳細を表示するために次のサンプル構成を使用します：

**cluster pods** *instance_name pod_name* **detail**

**注**：

- **cluster pods**：クラスタ内の現在のポッドを指定します。
- *instance_name*：インスタンスの名前を指定します。
- *pod_name*：ポッドの名前を指定します。
- **detail**：指定されたポッドの詳細を表示します。

次に、 *smf-data* インスタンスの *alertmanager-0* という名前のポッドの詳細を表示する例を示します。

**例**：

```
cee# cluster pods smf-data alertmanager-0 detail
details apiVersion: "v1"
kind: "Pod"
metadata:
  annotations:
    alermanager.io/scrape: "true"
    cni.projectcalico.org/podIP: "<ipv4address/subnet>"
    config-hash: "5532425ef5fd02add051cb759730047390b1bce51da862d13597dbb38dfbde86"
  creationTimestamp: "2020-02-26T06:09:13Z"
  generateName: "alertmanager-"
  labels:
    component: "alertmanager"
    controller-revision-hash: "alertmanager-67cdb95f8b"
    statefulset.kubernetes.io/pod-name: "alertmanager-0"
  name: "alertmanager-0"
  namespace: "smf"
  ownerReferences:
  - apiVersion: "apps/v1"
    kind: "StatefulSet"
    blockOwnerDeletion: true
    controller: true
    name: "alertmanager"
    uid: "82a11da4-585e-11ea-bc06-0050569ca70e"
  resourceVersion: "1654031"
  selfLink: "/api/v1/namespaces/smf/pods/alertmanager-0"
  uid: "82aee5d0-585e-11ea-bc06-0050569ca70e"
spec:
  containers:
  - args:
    - "/alertmanager/alertmanager"
    - "--config.file=/etc/alertmanager/alertmanager.yml"
    - "--storage.path=/alertmanager/data"
    - "--cluster.advertise-address=$(POD_IP):6783"
    env:
    - name: "POD_IP"
      valueFrom:
        fieldRef:
          apiVersion: "v1"
          fieldPath: "status.podIP"
    image: "<path_to_docker_image>"
```

```
    imagePullPolicy: "IfNotPresent"
    name: "alertmanager"
    ports:
    - containerPort: 9093
      name: "web"
      protocol: "TCP"
    resources: {}
    terminationMessagePath: "/dev/termination-log"
    terminationMessagePolicy: "File"
    volumeMounts:
    - mountPath: "/etc/alertmanager/"
      name: "alertmanager-config"
    - mountPath: "/alertmanager/data/"
      name: "alertmanager-store"
    - mountPath: "/var/run/secrets/kubernetes.io/serviceaccount"
      name: "default-token-kbjnx"
      readOnly: true
  dnsPolicy: "ClusterFirst"
  enableServiceLinks: true
  hostname: "alertmanager-0"
  nodeName: "for-smi-cdl-1b-worker94d84de255"
  priority: 0
  restartPolicy: "Always"
  schedulerName: "default-scheduler"
  securityContext:
    fsGroup: 0
    runAsUser: 0
  serviceAccount: "default"
  serviceAccountName: "default"
  subdomain: "alertmanager-service"
  terminationGracePeriodSeconds: 30
  tolerations:
  - effect: "NoExecute"
    key: "node-role.kubernetes.io/oam"
    operator: "Equal"
    value: "true"
  - effect: "NoExecute"
    key: "node.kubernetes.io/not-ready"
    operator: "Exists"
    tolerationSeconds: 300
  - effect: "NoExecute"
    key: "node.kubernetes.io/unreachable"
    operator: "Exists"
    tolerationSeconds: 300
  volumes:
  - configMap:
      defaultMode: 420
      name: "alertmanager"
    name: "alertmanager-config"
  - emptyDir: {}
    name: "alertmanager-store"
  - name: "default-token-kbjnx"
    secret:
      defaultMode: 420
      secretName: "default-token-kbjnx"
status:
  conditions:
  - lastTransitionTime: "2020-02-26T06:09:02Z"
    status: "True"
    type: "Initialized"
  - lastTransitionTime: "2020-02-26T06:09:06Z"
    status: "True"
    type: "Ready"
  - lastTransitionTime: "2020-02-26T06:09:06Z"
```

```
    status: "True"
    type: "ContainersReady"
  - lastTransitionTime: "2020-02-26T06:09:13Z"
    status: "True"
    type: "PodScheduled"
  containerStatuses:
  - containerID:
"docker://821ed1a272d37e3b4c4c9c1ec69b671a3c3fe6eb4b42108edf44709b9c698ccd"
    image: "<path_to_docker_image>"
    imageID: "docker-pullable://<path_to_docker_image>"
    lastState: {}
    name: "alertmanager"
    ready: true
    restartCount: 0
    state:
      running:
        startedAt: "2020-02-26T06:09:05Z"
  hostIP: "<host_ipv4address>"
  phase: "Running"
  podIP: "<pod_ipv4address>"
  qosClass: "BestEffort"
  startTime: "2020-02-26T06:09:02Z"
cee#
```

# ローリング アップグレード最適化

**表 *13 :* 機能の履歴**

| 機能名 | リリース情報 | 説明 |
|---|---|---|
| プロトコルPFCPポッドのローリング アップグレード最適化 | 2024.04.0 | プロトコル（PFCP）ポッドの場合、コンバージドコア ゲートウェイは、再送信された要求を処理するために、サービス ポッドにセッション レベルの応答メッセージ キャッシュを導入します。この最適化は、アップグレード手順中のセッションと 1 秒あたりのコール イベント（CEPS）の損失の削減に役立ちます。 |

| 機能名 | リリース情報 | 説明 |
| --- | --- | --- |
| エンドポイント ポッドのローリングアップグレード最適化 | 2024.03.0 | コンバージド コア ゲートウェイは、次のポッドのローリング アップグレード最適化サポートを提供します。<br>• Radius エンドポイント ポッド<br>• Diameter エンドポイント ポッド<br>• UDP プロキシ ポッド<br>• GTPPエンドポイントポッド<br>この最適化は、既存の最適化の強化です。<br>この機能は、統合コア プロファイルで既存の CLI コマンド **supported-features [ app-rx-retx-cache \| app-tx-retx \| rolling-upgrade-all \| rolling-upgrade-enhancement-infra ]** を使用します。 |

| 機能名 | リリース情報 | 説明 |
|---|---|---|
| ローリング アップグレード最適化 | 2024.02.0 | コンバージド コア ゲートウェイは、次のサポートを提供します。<br>• アップグレード中のサービスおよびプロトコル ポッドでの再試行メカニズム<br>• 構成ベースのローリング アップグレードの機能拡張<br>この最適化は、アップグレード手順中のセッションと 1 秒あたりのコール イベント（CEPS）の損失の削減に役立ちます。構成可能なローリングアップグレードの機能拡張により、変更のスムーズなロールアウトが可能になります。<br>この機能により、統合コア プロファイルに新しい CLI コマンド **supported-features [ app-rx-retx-cache \| app-tx-retx \| rolling-upgrade-all \| rolling-upgrade-enhancement-infra ]** が導入されます。<br>**デフォルト設定**：無効：構成が必要 |

コンバージド コア ゲートウェイ（CCG）ソフトウェア バージョン 2024.02.0 以降は、最適化の強化を備えたローリング アップグレードをサポートしています。ローリング アップグレードを使用すると、セッションと CEPS への影響を最小限に抑えて、すべてのポッドのグレースフル アップグレードを実行できます。最適化の強化により、必要に応じて、アップグレード プロセスの CLI コマンドを使用してローリング アップグレード機能を有効または無効にするオプションが提供され、運用上の柔軟性がもたらされます。

この機能は、次のアプリケーション レベルの機能拡張をサポートしています。

- サービス ポッドのアップグレード中のプロトコルポッドにおける再試行メカニズム。
- アップグレード中のサービス ポッドおよびプロトコル ポッドでの一時的なセッションまたはトランザクションの処理。

- 再起動中または非アクティブなポッドを検出するためのトポロジとIPCメカニズムの変更処理。非アクティブなポッドの場合、再試行オプションはポッドの他のインスタンスに対して試行されます。
- プロトコル（PFCP）ポッドの着信および発信の再送信要求を処理するためのキャッシュの維持。

**supported-features [ app-rx-retx-cache | app-tx-retx | rolling-upgrade-all | rolling-upgrade-enhancement-infra ]** CLI コマンドを使用して、ローリング アップグレードの拡張機能を設定できます。

**重要**

- 既存のセッションへの影響を防ぐために、実行時にローリングアップグレード機能を有効または無効にしないことを推奨します。
- 他のコマンドオプションはすべてデバッグ目的でのみ使用できるため、**rolling-upgrade-all** オプションのみを使用することを強く推奨します。

# ローリング アップグレード最適化の仕組み

このセクションでは、さまざまなポッドのアップグレードとローリングアップグレードの手順について説明します。

## ポッドのアップグレード

### サービス ポッド

ピア ポッドは特定のポッドのアップグレードや再起動を認識するため、そのポッドとの間のトランザクションが正常に処理されるようになります。

ここでは、サービス ポッドでの着信および発信メッセージの処理について説明します。

**着信メッセージ（Incoming Messages）**

- アップグレード中、サービスポッドの状態は、トポロジの更新を介して他のポッドに伝達されます。セッションにアフィニティが存在しない場合、そのポッドは新しいメッセージの転送用に選択されません。
- セッションでは、サービス ポッドにコンテキストがない場合、これがキャッシュ タイムアウト後のユーザーに対する最初のメッセージであり、アプリケーション停止メッセージがプロトコルポッドに伝達されます。このポッドは、他のサービス ポッド インスタンスにメッセージをリダイレクトします。
- サービスポッドにセッションのコンテキストがあり、セッションまたはユーザーに対する保留中の手順やトランザクションがない場合、アプリケーション停止メッセージがプロトコル ポッドに送信します。このポッドは、他のサービス ポッド インスタンスにメッセージをリダイレクトします。ただし、プロトコルポッドと通信する前に、セッション状態の

強制同期が CDL に対して実行されます。さらに、セッションまたはユーザーのアフィニティ エントリが削除されます。

#### 発信メッセージ（Outgoing Messages）

- セッションまたはユーザーのコール フローまたは手順の完了後、サービス ポッドがアップグレードまたは再起動の通知を受信すると、セッションまたは PDU の状態と CDL との同期が実行されます。さらに、サービスまたは ユーザーのアフィニティ エントリが削除され、サービス ポッド インスタンスに対する後続メッセージのトリガーが許可されません。
- 進行中の既存のコール フローについては、コールを完了させるためのベスト エフォートでトランザクションが処理されます。

## プロトコル ポッド

ここでは、REST エンドポイント、GTPC エンドポイント、およびプロトコル（PFCP）エンドポイント ポッドでのメッセージの処理について説明します。

### REST エンドポイント ポッド

ここでは、REST エンドポイント ポッドでの着信および発信メッセージの処理について説明します。

#### 着信メッセージ（Incoming Messages）

- 新しいTCP接続の場合、入力K8サービスはアップグレードまたは再起動中に特定のREST エンドポイント ポッドを選択しません。そのような要求は他のインスタンスに転送されます。
- アップグレード通知または再起動通知を受信後、既存の接続で GOAWAY フレームが送信されます。このフレームを送信すると、新しいメッセージがピア ノードの新しい接続で送信されます。

#### 発信メッセージ（Outgoing Messages）

- サービス ポッドから発信要求メッセージを受信後、アプリケーション停止通知がサービス ポッドに送り返されます。その結果、サービス ポッドが、メッセージをトリガする別の REST エンドポイント インスタンスを選択できます。
- 既存の一時的なメッセージの発信応答では、ベストエフォート方式でトランザクションが完了します。

### GTPC エンドポイント ポッド

#### 着信メッセージ（Incoming Messages）

GTPCエンドポイント ポッドの再起動中時に、着信要求メッセージの処理をサポートするために、セッション レベルの応答メッセージ キャッシュがサービス ポッドに追加されました。サー

ビス ポッドは、シーケンス番号、送信元 IP アドレス、送信元ポート、および要求メッセージ タイプに基づいて、応答メッセージ バッファを保存します。

- GTPC エンドポイントポッドの再起動が原因で回線上の応答メッセージが失われた場合、ピアで要求メッセージが再試行されます。このメッセージは、セッション レベルの応答メッセージ キャッシュを使用して応答されます。
- 応答メッセージがサービス ポッドで生成されない場合でも、メッセージは再送信としてサービスで検出されて適宜処理されます。

### 発信メッセージ（Outgoing Messages）

GTPC エンドポイント ポッドの再起動中、発信要求メッセージは次の方法で処理されます。

- サービス ポッドが、BGIPC を実行する際の要求のタイムアウト間隔と再送信回数を設定します。タイムアウト間隔と送信回数は、S5、S11、および S5E インターフェイスに対して定義されている N3 T3 に基づいています。
- GTPCエンドポイントポッドの代わりに、サービスポッドが送信元ポートとシーケンス番号を設定します。
- このメカニズムは、ポッドの再起動中に応答メッセージが失われた場合の発信メッセージの再送信に役立ちます。サービス ポッドは、シーケンス番号とポートを生成します。この場合、ピアでもメッセージが再送信として検出されるため、回線上のメッセージに不明瞭さはありません。

## プロトコル（PFCP）エンドポイント ポッド

### 着信メッセージ（Incoming Messages）

セッション レベルの応答メッセージ キャッシュがサービス ポッドに追加され、PFCP エンドポイント ポッドの再起動時に、着信要求メッセージの処理をサポートします。サービス ポッドは、シーケンス番号、送信元 IP アドレス、送信元ポート、および要求メッセージ タイプに基づいて、応答メッセージ バッファを保存します。

- プロトコル エンドポイント ポッドの再起動が原因で回線上の応答メッセージが失われた場合、ピアで要求メッセージが再試行されます。このメッセージは、セッション レベルの応答メッセージ キャッシュを使用して応答されます。
- 応答メッセージがサービス ポッドで生成されない場合でも、メッセージは再送信としてサービスで検出されて適宜処理されます。

### 発信メッセージ（Outgoing Messages）

プロトコル エンドポイント ポッドの再起動中、発信要求メッセージは次の方法で処理されます。

- サービス ポッドが、BGIPC を実行する際の要求のタイムアウト間隔と再送信回数を設定します。タイムアウト間隔と送信回数は、PFCPインターフェイスに対して定義されたN3 T3 タイマーに基づいています。

- プロトコル エンドポイント ポッドの代わりに、サービス ポッドが送信元ポートとシーケンス番号を設定します。
- このメカニズムは、ポッドの再起動中に応答メッセージが失われた場合の発信メッセージの再送信に役立ちます。サービス ポッドは、シーケンス番号とポートを生成します。この場合、ピアでメッセージが再送信として検出されるため、回線上のメッセージに不明瞭さはありません。

### ノード マネージャ ポッド

ノード マネージャ ポッドの 1 つのインスタンスは、アップグレード中にコールを処理するために使用できます。準備プローブとタイマーも、アップグレード シナリオ用に構成されます。ポッドが非アクティブの場合、サービス ポッドは他のノード マネージャのポッド インスタンスを再試行します。

### CDL ポッド

CDL ポッドには、アップグレード プロセス中にサービスを継続するための複数のレプリカがあります。アップグレードおよび再起動プロセス中の障害を最小限に抑えるために、CDL エンドポイントに対して複数の接続ストリームを使用できます。これらのプロセスでエラーが発生した場合、再試行メカニズムは別の CDL エンドポイント接続に対しても実装されます。

### RADIUS エンドポイント ポッド

次に、ローリング アップグレード中の RADIUS エンドポイント ポッドの動作を示します。

- アップグレード中、ポッドの状態は、トポロジの更新を介して他のポッドに伝達されます。非アクティブになるポッドは、新しいメッセージを転送するために選択されていません。
- アップグレードの RADIUS エンドポイント ポッドでメッセージを受信すると、**アプリケーション停止**指示が他のポッドに伝達されます。
- **アプリケーション停止**指示を受信すると、メッセージは他のアクティブな RADIUS エンドポイント ポッドにリダイレクトされます。

### Diameter エンドポイント ポッド

次に、ローリング アップグレード中の Diameter エンド ポイント ポッドの動作を示します：

- VIP スイッチ オーバーの前に、着信メッセージはサービス ポッドまたは Diameter ピアに転送されます。
- VIP スイッチオーバー後、新しいメッセージは停止中のポッドで受信されません。

### UDP プロキシ ポッド

アップグレード中、UDP プロキシ ポッドは着信メッセージを許可します。

### GTPP エンドポイント ポッド

アップグレード中、GTPP エンドポイント ポッドは着信メッセージを許可します。

## ローリング アップグレード最適化サポートを利用したバージョンへのソフトウェアのアップグレード

ここでは、ローリング アップグレードを実行する方法と、ローリング アップグレードの拡張機能を有効にする方法について説明します。

**重要** ローリング アップグレードの手順に関連する、次の重要な注意事項を確認します。

- ローリング アップグレード最適化機能は、リリース 2024.02.0 以降からアップグレードする場合にのみ使用する必要があります。

  リリース 2024.02.0 以前のバージョンからリリース 2024.02.0 以降にアップグレードする場合は、最初にシャットスタート アップグレードを実行します。

- アップグレード後、CLI コマンドを使用して、ローリング アップグレードの拡張機能を有効にしてください。その後、将来のリリースへの後続のローリング アップグレードには、利用可能な最適化が含まれます。

### ローリング アップグレードの考慮事項

SMF の両方のラック（Rack 1 と Rack 2）は日のシナリオであり、リリース 2024.02.0 より前のバージョンです。

ローリング方法を実行するには、次の手順に従います。

1. Rack 1 を雷日のシナリオに移動し、Rack 2 を両方の GR インスタンスでアクティブのままにします。
2. Rack 1 の GR インスタンスを Standby_ERROR に移動します。
3. Rack 1 をシャットダウンします。
4. Rack 1 をリリース 2024.02 に移行するには、sync- Phase ops-center を介してクラスタ同期を実行します。
5. ローリング アップグレードの拡張機能を有効にするには、推奨構成を適用します。

   ローリング アップグレードの推奨構成は次のとおりです。

   ```
   config
     profile converged-core converged_core_profile_name
     supported-features [ rolling-upgrade-all ]
     end
   ```

6. Rack 1 を開始します。
7. CDL の調整が完了するまで 30 分間待機します。

8. GR インスタンスをプライマリに切り替えて、Rack 1 をアクティブにします。
9. Rack 2 をシャットダウンします。
10. Rack 2 のステップ 4 ～ 6 を続けます。
11. 日のシナリオには Rack 1 と Rack 2 の構成を行います。

# 制限事項

この機能には、次の制限事項があります。

- ローリング アップグレードの間、サービス ポッドは一度に 1 つずつ再起動します。このアップグレードにより、セッションが均等に再配布されます。最初に再起動するサービス ポッドのセッション数が多くなります。同様に、最後に再起動したサービス ポッドのセッション数が最小になります。このようなセッションの再配布により、一部のサービス ポッドのメモリ要件が一時的に急増する可能性があります。セッションがサービス ポッドのローカル キャッシュから削除された後、システムは期待どおりに動作します。
- サービス ポッドでの一連の手順は、ローリング アップグレード中も継続されます。ただし、これらを正常に完了させるためのベストエフォート メカニズムが実装されています。

# ローリング アップグレードのサポートされる機能の構成

ローリングアップグレードでサポートされている機能を有効にするには、次の構成例を使用します。

```
config
  profile converged-core cc_profile_name
     supported-features [ app-rx-retx-cache | app-tx-retx |
rolling-upgrade-all | rolling-upgrade-enhancement-infra ]
     end
```

**注**：

- **profile converged-core** *cc_profile_name*：コンバージド コア プロファイルの名前を指定します。このキーワードを使用すると、コンバージド コア プロファイル構成モードを開始できます。
- **supported-features [ app-rx-retx-cache | app-tx-retx | rolling-upgrade-all | rolling-upgrade-enhancement-infra ]**：ローリング アップグレードでサポートされている機能を有効にするには、次のいずれかのオプションを指定します。
  - **app-rx-retx-cache**：アプリケーションでの着信メッセージの再送信キャッシュを有効にします。
  - **app-tx-retx**：アプリケーションでのアウトバウンド メッセージの再送信を有効にします。

- **rolling-upgrade-all**： **rolling-upgrade-enhancement-infra**、 **app-rx-retx-cache**、および **app-tx-retxrolling** キーワード オプションで使用可能なすべてのローリング アップグレード機能を有効にします。デフォルトでは、ローリング アップグレード機能は無効になっています。

  **rolling-upgrade-all** は推奨オプションです。

- **rolling-upgrade-enhancement-infra**：インフラレベルの機能を有効にします。

重要

- 既存のセッションへの影響を防ぐために、実行時にローリングアップグレード機能を有効または無効にしないことを推奨します。
- 他のコマンドオプションはすべてデバッグ目的でのみ使用できるため、**rolling-upgrade-all** オプションのみを使用することを強く推奨します。

## ローリング アップグレード最適化の確認

**show running-config profile amf-services** コマンドを使用して、ローリング アップグレードでサポートされる機能を確認します。

**show running-config amf-services** コマンドの出力例を次に示します。

```
show running-config profile amf-services
amf-services am1
   supported-features [ rolling-upgrade-all ]
exit
```

# OAM サポート

## バルク統計

ローリング アップグレード最適化機能では、次の統計情報がサポートされています。

**IPC 再試行統計情報**：

「ipc_request_total」統計は、再試行の原因に関する追加のラベル「retry_cause」で更新されます。

**CDL 統計情報**：

CDL 操作に次の統計が追加されます。

- cdl_request_total
- cdl_response_total
- cdl_request_seconds_total

- cdl_request_duration_histgram_total

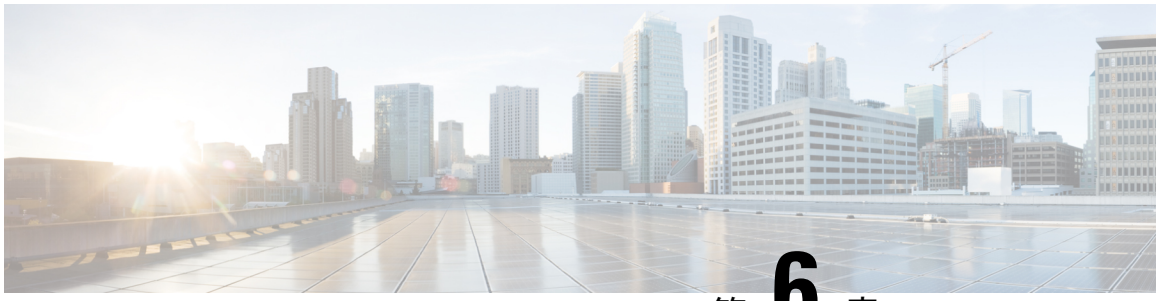
これらの CDL 統計は、次のフィルタで更新されます。

- **retry**：再試行メッセージを表示するために使用されます
- **method_name**：CDL 強制同期更新を表示するために使用されます

（注） 以前のリリースでは、CDL 統計は、フィルタ **rpc_name** を STREAM_SESSION_DB として、RPC 統計を介して表示されていました。リリース 2024.02 以降、CDL 統計は、前述の CDL 統計を使用する場合にのみ使用できます。

**アプリケーション停止カウンタ**：

App-infra でアクションを表示するために、「application_stop_action」統計が追加されました。これらのアクションの例には、セッション キャッシュの削除やアフィニティの削除があります。



第 6 章

# AN によって開始されたセッションの変更とリリース


- 機能の概要と変更履歴 （83 ページ）
- 機能説明 （84 ページ）
- 機能の仕組み （84 ページ）


## 機能の概要と変更履歴

### 要約データ

*Table 14:* 要約データ

| | |
|---|---|
| 該当製品または機能エリア | SMF |
| 該当プラットフォーム | SMI |
| 機能のデフォルト設定 | 有効：常時オン |
| このリリースでの関連する変更点 | N/A |
| 関連資料 | 該当なし |

### 更新履歴

*Table 15:* マニュアルの変更履歴

| 改訂の詳細 | リリース |
|---|---|
| 最初の導入。 | 2020.02.0 |

# 機能説明

RAN または AMF の障害により、NG-AP シグナリング接続が失われる可能性があります。このシナリオでは、RAN または AMF は、RAN および AMF 間のシグナリングに依存することなく、AN リリース手順を開始します。

AN が開始した PDU セッションの解放手順には、RAN と AMF および関連する N3 ユーザー プレーン接続間の UE の論理 NG-AP シグナリング接続の解放、および、UE と RAN および関連する RAN リソース間の RAN シグナリング接続の解放が含まれます。

AN リリースの開始は、次の理由で発生する可能性があります：

- RANが原因で開始されました。たとえば、O&Mの介入、未指定の障害、RAN(たとえば、無線)リンク障害、ユーザーの非アクティブ、システム間リダイレクト、IMS音声のQoSフローの確立要求、UE生成シグナリングによるリリースなどです。接続の解放、モビリティの制限、UE からのリリース アシスタンス 情報（RAI）など。または
- 未指定の障害などの原因により AMF が開始

（注） AN によって開始された変更の場合、SMF は、セクション 4.3.3.2-1「3GPP TS 23.502 の UE またはネットワークで PDU セッションの変更が要求された」のステップ 2 で説明されているように、PCF にポリシー更新メッセージを送信しません。

# 機能の仕組み

このセクションでは、PDU セッションに関連付けられている NG-AP シグナリング接続、UP 接続、および AN リソースがどのように解放されるかについて説明します。

### RAN が開始した PDU セッションのリリース コール フロー

次のコール フロー図は、PDU セッションの解放が RAN または AMF によって開始されたときに、UE と SMF の間で交換されるメッセージを表しています。RANセッションの解放は、3GPP 23.502 で定義されています。

この手順では、影響を受ける SMF と UPF はすべて、UE にサービスを提供する PLMN の制御下にあります。たとえば、ホームルーティングローミングの場合、HPLMN の SMF と UPF は関与しません。

図 *14 : RAN* が開始した *PDU* セッションのリリース コール フロー

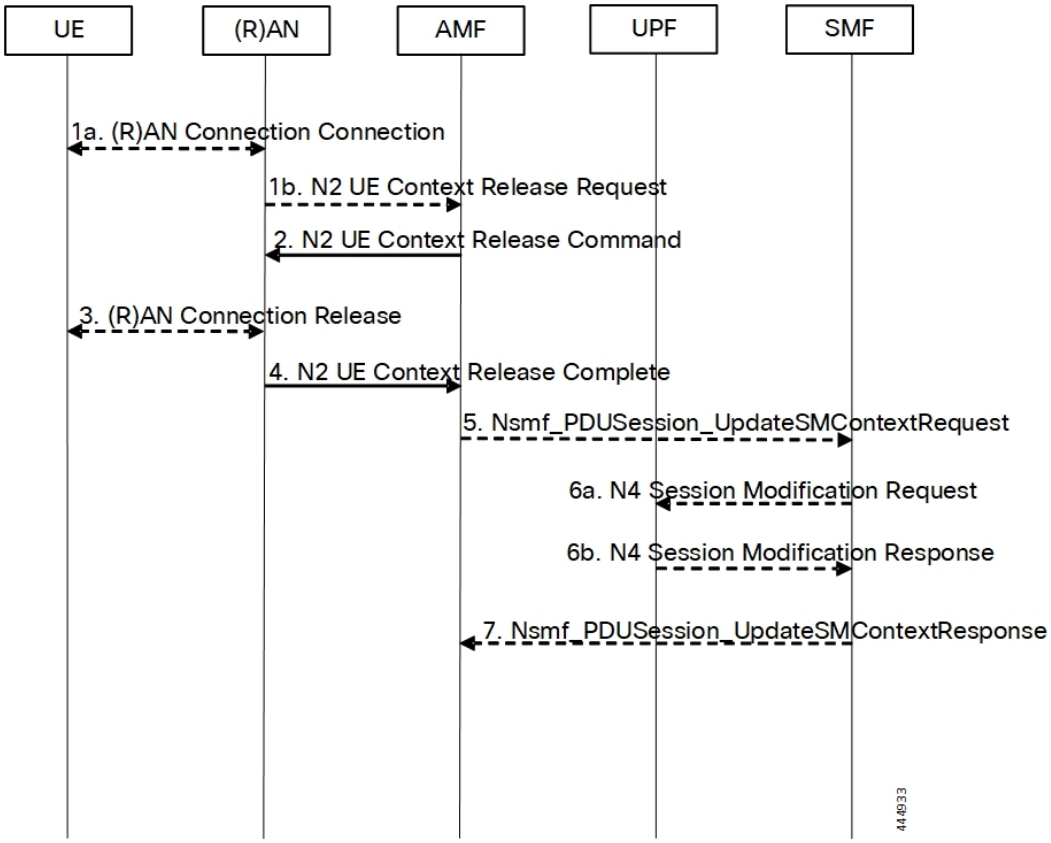



表 *16 : RAN* が開始した *PDU* セッションのリリース コール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | 無線リンクの障害やRANの内部障害などの場合、RANはUEコンテキストの解放を開始することを決定し、N2 UE コンテキストの解放要求メッセージを AMF に送信します。<br><br>解放の理由が NG-RAN が AS リリース支援インジケータ（RAI）を受信したことである場合、NG-RAN は RRC 接続を解放しませんが、N2 UE コンテキスト解放要求メッセージを AMF に送信します。AS RAI が単一のダウンリンク送信のみが予想されることを示している場合、NG-RAN は 1 つのダウンリンク NAS PDU または N3 データ PDU が転送された後、N2 UE コンテキストリリース要求のみを送信します。<br><br>N2 コンテキストのリリース要求の原因がリリースを示している場合は、ユーザーの非アクティブまたは AS RAI が原因でリリースが要求されます。次に、AMF は、保留中の MT トラフィックまたはシグナリングを認識しない限り、AN リリース手順を続行します。 |

| ステップ | 説明 |
|---|---|
| 2 | RAN からリリース要求メッセージを受信すると、AMF は N2 UE コンテキスト リリース コマンドを RAN に送信します。<br>AMF が RAN 経由で別の NAS シグナリング接続を確立するためにサービス要求または登録要求を受信した場合、UE を正常に認証した後、AMF は既存の NAS シグナリング接続を解放します。次に、AMF はサービス要求または登録要求の手順を続行します。<br>原因は、(R)AN からの原因または AMF イベントによる原因のいずれかを示しています。 |
| 3 | UE 接続がステップ 1 で解放されなかった場合、RAN は次のいずれかの操作を実行します。<br>• RAN 接続のリリースの確認時に、RAN が UE のコンテキストを削除します。<br>• Context Release コマンドの [原因（Cause）] に、UE が RRC 接続をローカルで解放したことが示されている場合、RANは、RRC 接続をローカルで解放します。 |
| 4 | （注）<br>UE が RRC 接続の解放を確認しない場合は、ステップ 2 の後にこのステップを実行します。<br><br>RAN は、UE の AMF との N2 シグナリング接続を解放し、N2 UE コンテキスト リリース完了メッセージを AMF に送信します。このメッセージには、次の情報が含まれます。<br>• RAN がアクティブな N3 ユーザー プレーンでサービスを提供するPDU セッション ID のリスト<br>• ユーザー ロケーション情報<br>• ロケーション情報の経過時間<br><br>AMF は、NG-RAN ノードから UE 無線機能情報または NB-IoT 固有の UE 無線アクセス機能情報を受信します。NG-RAN は、CE 対応 UE のページング支援データ（使用可能な場合）を N2 UE コンテキスト リリース完了メッセージを介して AMF に送信します。AMF は、後続のページング手順のために、CE 対応 UE の受信したページング支援データを UE コンテキストに保存します。<br>（注）<br>PLMN がセカンダリ RAT 使用状況レポートを設定している場合、NG-RAN ノードは RAN 使用状況データ レポートを提供します。 |

| ステップ | 説明 |
| --- | --- |
| 5 | N2 UE コンテキスト リリース 完了の各 PDU セッションに対して、AMF は Nsmf PDU セッション更新 SM コンテキスト要求を SMF に送信します。この要求メッセージには次の情報が含まれています。<br>• PDU セッション ID<br>• PDU セッションの非アクティブ化<br>• 原因（ステップ 2 と同じ）<br>• 操作タイプ<br>• ユーザー ロケーション情報<br>• ロケーション情報の経過時間<br>• N2 SM 情報（セカンダリ RAT 使用状況のデータ）<br>ステップ 1 のようなアクティブな N3 ユーザープレーンを含む PDU セッション ID のリストがリリース要求メッセージに含まれている場合、SMF および AMF はステップ 2 の前にステップ 5 ～ 7 を実行します。<br>動作タイプは「UP deactivate」に設定され、PDU セッションのユーザー プレーン リソースを非アクティブにすることを示します。<br>PDU セッションがコントロール プレーン CIoT 5GS 最適化を使用し、UE が拡張アイドル モード DRX の使用をネゴシエートした場合、AMF は、UE のダウンリンク データが SMF に到達不能であると通信します。<br>PDU セッションがコントロール プレーン CIoT 5GS 最適化を使用し、UE がアクティブ タイムで MICO モードの使用をネゴシエートした場合、AMF は、アクティブ タイムの期限切れ後に、UE のダウンリンク データが SMF に到達不能であると通信します。 |

| ステップ | 説明 |
|---|---|
| 6 | コントロール プレーン CIoT 5GS 最適化を使用しない PDU セッションの場合、SMF は N4 セッション変更要求を UPF に送信します。この要求メッセージには、次のことを示す詳細が含まれています。<br>• AN または UPF 終端 N3 のトンネル情報を削除するかどうか。<br>• 着信 DL PDU をバッファするかどうか。<br>UE のダウンリンクデータが到達不能であることを AMF が示している場合、SMF は N4 セッション変更手順を開始して UPF のバッファリングをアクティブにします。<br>PDU セッションで複数の UPF が使用されている場合、SMF は、N3 を終端する特定の UPF に変更要求を送信してから、その UPF に関連付けられている N4 セッションを解放します。<br>ユーザーの非アクティブまたは UE リダイレクションによる AN リリースの場合、SMF は GBR QoS フローを保持します。それ以外の場合、SMF は、AN リリース手順の完了後に、UE の GBR QoS フローの PDU セッション変更手順をトリガーします。<br>信頼性の高い低遅延通信（URLLC）が冗長 I-UPF を使用する場合、SMF は各 I-UPF に N4 セッション変更要求を送信します。SMF はバッファリング命令を使用して、DL パケットをバッファリング、ドロップ、または転送するための冗長 I-UPF を選択します。<br>URLLC で冗長 N3 トンネルが使用されている場合、SMF は、対応する PDU セッションの N3 トンネルのデュアル AN トンネル情報を削除するための変更要求を N3 ターミネーション ポイントの UPF に送信します。 |
| 6b | UPF が SMF に N4 セッション変更応答を送信します。 |
| 7 | SMF は、Nsmf PDU セッション更新 SM コンテキスト応答を AMF に送信します。次に、AMF は N2 および N3 接続を解放した後、CM-IDLE 状態になり、SMF に確認応答を送信します。 |

### デュアル接続で RAN が開始する QoS フローモビリティ

RAN によって開始された QoS フロー モビリティの手順では、SMF および UPF を再割り当てすることなく、セカンダリ RAN ノードとの間で QoS フローを転送します。UPF とプライマリ RAN ノード間、および UPF とセカンダリ RAN ノード間に IP 接続が存在することを前提としています。

次のコールフロー図は、プライマリ RAN ノードとセカンダリ RAN ノード間の QoS フロー交換を表しています。

図 *15 : NG-RAN* が開始した *QoS* フロー モビリティ手順

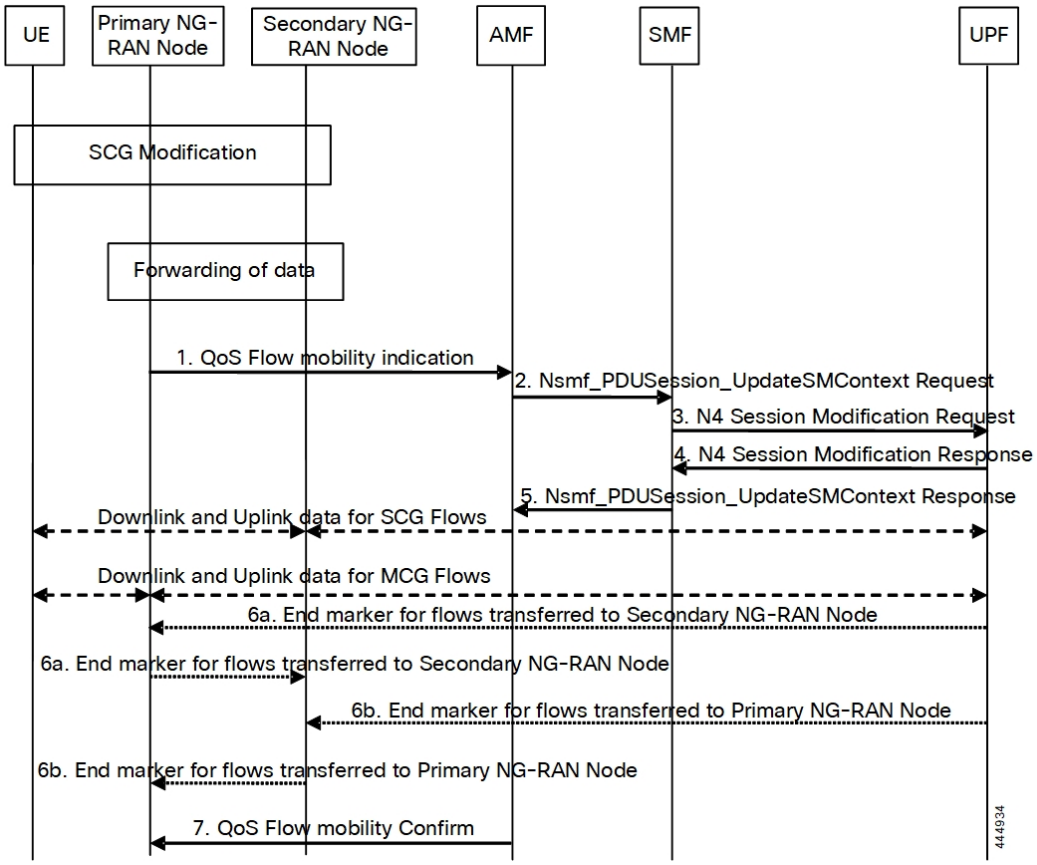
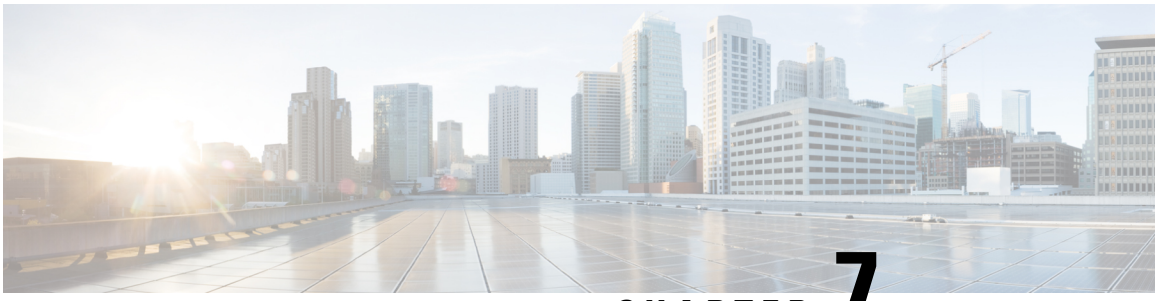



表 *17 : NG-RAN* が開始した *QoS* フロー モビリティ コール フローの説明

| ステップ | 説明 |
|---|---|
| 1. | プライマリ RAN ノードは、N2 QoS フロー モビリティ通知メッセージを AMF に送信します。QoS フローは、マスター セル グループ（MCG）およびセカンダリ セル グループ（SCG）に関連しています。指示メッセージには、PDU セッション ID、QFI、および AN トンネル情報が含まれます。トンネル情報には、QFI の新しい RAN トンネルエンドポイントが含まれます。 |
| 2. | AMF は、Nsmf PDU セッション更新 SM コンテキスト要求を SMF に送信します。この要求メッセージには、N2 QoS フロー モビリティ通知メッセージと PDU セッション ID が含まれます。 |
| 3. | SMF は、N4 セッション変更要求メッセージを UPF に送信します。この変更要求には、ダウンリンク ユーザー プレーンの PDU セッション ID、QFI、および AN トンネル情報が含まれています。 |

| ステップ | 説明 |
|---|---|
| 4. | UPF（PSA）は、N4 セッション変更応答メッセージを SMF に送信します。応答メッセージには、アップリンク トラフィックの CN トンネル情報が含まれています。<br>**重要**<br>ステップ 7 は、SMF で N4 セッション変更応答を受信した後はいつでも実行できます。 |
| 5. | SMF は、正常に切り替えられた PDU セッションの QFI に対して、Nsmf PDU Session Update SM Context Response を AMF に送信します。要求された QFI が正常に切り替えられなかった場合、SMF は N2 QoS フロー モビリティ障害メッセージを送信します。 |
| 6. | 影響を受ける各 N3 トンネルについて、プライマリ RAN ノードおよび/またはセカンダリ RAN ノードの再順序付け機能を支援するために、UPF は QFI のトンネルを切り替えた直後に、古いトンネルに 1 つ以上の「エンド マーカー」パケットを送信します。UPF はターゲット NG-RAN にダウンロード パケットの送信を開始します。 |
| 7. | AMF は、プライマリ RAN ノードに確認応答メッセージを送信します。このメッセージは、QoS フロー モビリティ手順の完了を示します。 |



CHAPTER 7

# Cisco Common Data Layer


- 機能の概要と変更履歴, on page 91
- SMF の Cisco Common Data Layer の Geo 冗長性, on page 92
- SMF での CDL の仕組み, on page 93
- コール フロー, on page 94
- SMF Ops センターによる CDL の構成 （96 ページ）
- イベント トレース データの構成 （100 ページ）


## 機能の概要と変更履歴

### 要約データ

表 *18* : 要約データ

| | |
|---|---|
| 該当製品または機能エリア | SMF |
| 該当プラットフォーム | SMI |
| 機能のデフォルト設定 | 無効：設定が必要 |
| このリリースでの関連する変更点 | N/A |
| 関連資料 | 該当なし |

### 更新履歴

表 *19* : マニュアルの変更履歴

| 改訂の詳細 | リリース |
|---|---|
| 失敗処理のサポートが追加されました。 | 2023.03.0 |

| 改訂の詳細 | リリース |
|---|---|
| CDL データベース レコードのイベント トレース データの構成と検証に関する手順を追加しました。 | 2021.02.0 |
| 最初の導入。 | 2020.02.0 より前 |

# SMF の Cisco Common Data Layer の Geo 冗長性

Common Data Layer（CDL）は、クラウドネイティブなすべてのアプリケーションに対応する、高性能の次世代キー値（KV）データ ストア レイヤです。これらのアプリケーションは、高可用性（HA）と Geo HA 機能を備えた状態管理として CDL を使用します。

この機能により、SMF で CDL の Geo 冗長（GR）バージョンをサポートできます。CDL エンドポイントポッドは、SMF アプリケーションから CDL に対する要求を受信するためのフロントエンドです。プライマリ CDL エンドポイントに障害が発生すると、SMF は次に評価の高いセカンダリ エンドポイントにデータベース サービス要求を送信します。次の評価対象エンドポイントが使用できない場合、SMF は、評価が最も高い後続のエンドポイントで操作を再試行します。

CDL から SMF への特定のエラーまたは障害が発生した場合、再試行メカニズムは、作成、検索、更新、および削除のリクエストに使用されます。再試行回数は SLA に従います。

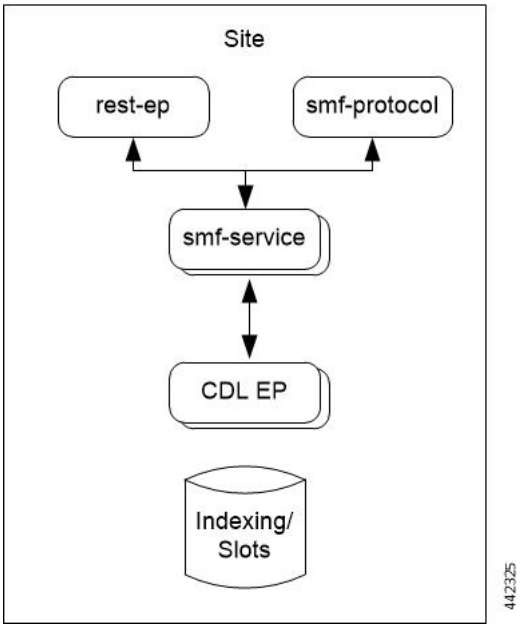
再試行中に SMF が成功応答を受信すると、再試行は中止され、応答がアプリケーションに送信されます。

この機能により、SMF は中断のない N7 または Diameter メッセージ処理を提供します。

## アーキテクチャ

次の図は、SMF サービスが CDL データストア エンドポイントにアクセスできない場合に発生するフェールオーバを示しています。

*Figure 16: CDL データストア アーキテクチャ*




このアーキテクチャとの関連性により、SMF Ops Center を介して CDL を構成できます。SMF は CDL に接続するときに、ローカル エンドポイントを使用します。

# SMF での CDL の仕組み

SMF Ops Center を介して SMF で CDL が設定されると、SMF は複数の CDL データストア エンドポイントをサポートできるようになります。エンドポイントを設定するには、IPアドレス、ポートを指定し、各エンドポイントに評価を割り当てます。デフォルトでは、SMFはローカル エンドポイントを、最大の評価を持つプライマリ エンドポイントと見なします。SMF は、プライマリエンドポイントで CDL API オペレーションを実行します。このエンドポイントが使用できない場合、SMFは、次に最大評価のエンドポイントに操作をルーティングします。SMF は、設定されたすべてのセカンダリエンドポイントが使い果たされるまで、アクセス可能なセカンダリエンドポイントにフェールオーバーし続けます。エンドポイントが到達可能でも、エラーまたはタイムアウトで応答する場合、次に評価されたエンドポイントでクエリを再試行しません。

SMF がクラスタ内のどのエンドポイントにもアクセスできない場合、CDL 操作は「Datastore Unavailable」というエラーで失敗します。

次の表は、シナリオ、予想される動作、および CDL からの関連エラー応答を示しています。

*Table 20:* シナリオ、予想される動作、および *CDL* からのエラー応答

| シナリオ | 予期される動作 | CDL からのエラー応答 |
|---|---|---|
| すべてのポッドはアクティブかつ正常であり、CDL 操作をトリガーします。 | CDL の作成、読み取り、更新、削除（CRUD）操作は、リトライされません。 | N/A |
| CDL エンドポイント ポッドは、CDL 操作を再開し、トリガーします。 | CDL CRUD 操作はリトライされます。 | CDL はエラー コードとともに次のエラー応答を送信します。<br>• ERROR_FROM_INDEXING [501]<br>• ERROR_FROM_SLOT [502]<br>• DATASTORE_EP_QUEUE_FULL [503]<br>• MAX_CAPACITY_REACHED [507 |

# コール フロー

ここでは、この機能に関連したコール フローについて説明します。

• CDL エンドポイント障害のコール フロー, on page 94

# CDL エンドポイント障害のコール フロー

このセクションでは、SMF ローカル データ ストア エンドポイントの失敗のコール フローについて説明します。

*Figure 17: CDL* エンドポイント障害のコール フロー

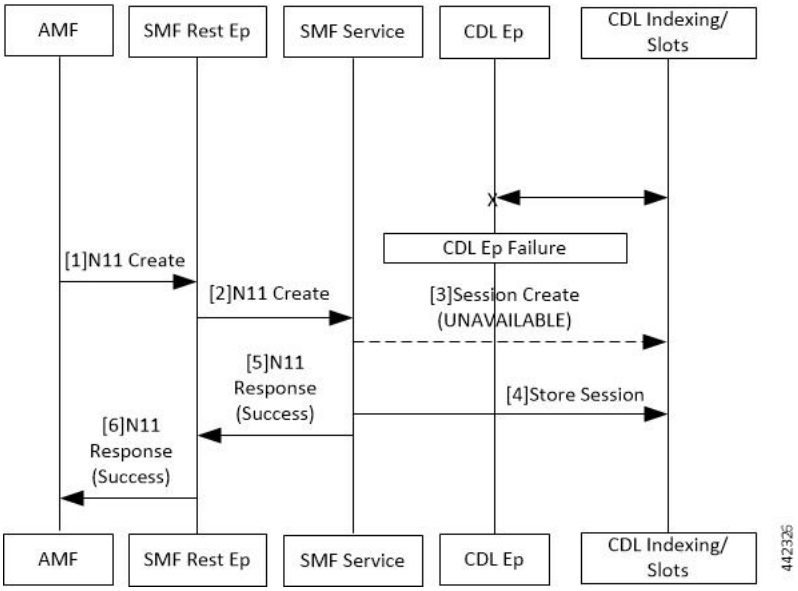



*Table 21: CDL* エンドポイント障害コール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | AMF は、N11 インターフェイスを介して SMF REST エンドポイントに作成要求を送信します。 |
| 2 | 要求を受信した後、SMF REST エンドポイントは、SMF サービスに作成要求を転送します。 |
| 3 | SMF サービスは、CDL エンドポイントに到達してセッション作成要求を送信しようとします。ただし、CDL エンドポイントは到達不能です。 |
| 4 | 要求の作成は保存されているセッションで評価され、SMF サービスがその要求を CDL エンドポイントに転送します。 |
| 5 | コール要求が成功すると、SMF サービスは SMF REST エンドポイントに成功メッセージを通知します。 |
| 6 | SMF REST エンドポイントが AMF に成功メッセージを転送します。 |

# 制限事項

SMF の CDL 構成には、次の制限があります：

- SMF サービスでは、UNAVAILABLE などの gRPC エラーが発生した場合にのみコールの再ルーティングが試行されます。データストアエンドポイントが DEADLINE_EXCEEDED gRPC ステータス コードなどの実際の gRPC タイムアウトを返すエラーは確認しません。
- SMF サービスは、インデックス作成やスロット障害など、データストアで発生した障害を解決しません。CDL レイヤはこれらの障害を解決する必要があり、必要に応じてリモートに API コールを送信します。
- デフォルトでは、要求の最大再試行制限は 3 です。この制限に達すると、再試行は停止し、応答がアプリケーションに送信されます。
- 再試行中に成功の応答メッセージを受信すると、再試行は中止され、応答がアプリケーションに送信されます。

# SMF Ops センターによる CDL の構成

SMF Ops センターを使用した CDL の構成には、次の手順が含まれます。

1. CDL セッション データベースを構成して基本構成を定義する （96 ページ）
2. CDLでの Zookeeper の構成 （99 ページ）

# CDL セッション データベースを構成して基本構成を定義する

CDL データベースコレクタを構成するには、次の手順を実行します：

## 手順

**ステップ 1** CDL セッション データベースを設定するには、グローバル構成モードでシステム ID、ノード タイプ、Zookeeper レプリカ サーバー ID を定義します。

| CLI コマンド | 説明 | 範囲 | デフォルト値 |
|---|---|---|---|
| **cdl system-id** *system_id* | システムまたは Kubernetes クラスタの ID を指定します。 | 該当なし | 1 |
| **cdl node-type** *node_type* | ノード アフィニティを構成するための Kubernetes ノード ラベルを指定します。値は、文字列である必要があります。 | 0～64 | session |

| CLI コマンド | 説明 | 範囲 | デフォルト値 |
|---|---|---|---|
| **cdl zookeeper replica** *zookeeper_replica_id* | zookeeper レプリカ サーバーの ID を指定します。 | 該当なし | 該当なし |

**ステップ 2** ログレベル、クラスタ、レプリカ、スロット、インデックス、およびスライス パラメータを構成して、CDL データストア セッションの基本構成を定義し、構成を保存します。

| CLI コマンド | 説明 | 範囲 | デフォルト値 |
|---|---|---|---|
| **cdl logging default-log-level** *debug_level* | **cdl logging default-log-level** *debug_level*：デフォルトのログ レベルを指定します。 | 該当なし | 該当なし |
| **cluster-id** *cluster-id* | **cluster-id** *cluster-id*：Kubernetes クラスタの ID を指定します。 | 該当なし | 1 |
| **endpoint replica** *num_replica* | **endpoint replica** *num_replica*：作成するレプリカの数を指定します。値は必ず整数にしてください。 | *num_replica*：値は 1 ～ 16 の範囲の整数である必要があります。 | *num_replica*：デフォルト値は 1 です。 |
| **slot { replica** *num_replica* \| **map** *num_map/shards*\| **write-factor** *write_factor* **}** | • **replica** *num_replica*：作成するレプリカの数を指定します。<br>• **map** *num_map/shards*：スロット内のパーティション数を指定します。<br>• **write-factor** *write_factor*：正常な応答の前に書き込まれるコピーの数を指定します。<br>（注）<br>値がレプリカ数以下であることを確認してください。 | • *num_replica*：値は 1 ～ 16 の範囲の整数である必要があります。<br>• *num_map/shards*：値は、1 ～ 1024 の範囲の整数である必要があります。<br>• *write_factor*：値は 0 ～ 16 の範囲の整数である必要があります。 | • *num_replica*：デフォルト値は 1 です。<br>• *num_map/shards*：デフォルト値は 1 です。<br>• *write_factor*：デフォルト値は 1 です。 |

| CLI コマンド | 説明 | 範囲 | デフォルト値 |
|---|---|---|---|
| **slot notification { host** *host* \| **port** *port* \| **limit** *tps* **}** | • **notification host** *host*：通知サーバーのホスト名または IP アドレスを指定します。<br>• **slot notification port** *port*：通知サーバーのポート番号を指定します。<br>• **slot notification limit** *tps* ：1 秒あたりの通知上限を指定します。 | NA | • *host*：デフォルト値は datastore-notification-ep です。<br>.<br>• *port*：デフォルト値は 8890 です。<br>• *tps* ：デフォルト値は 2000 です。 |
| **index { replica** *num_replica* \| **map** *num_map/shards* \| **write-factor** *write_factor* **}** | • **replica** *num_replica*：作成するレプリカの数を指定します。<br>• **map** *num_map/shards*：スロット内のパーティション数を指定します。CDL の展開後は、この値を変更しないでください。<br>• **write-factor** *write_factor*：正常な応答の前に書き込まれるコピーの数を指定します。 | • *num_replica*：値は 1 ～ 16 の範囲の整数である必要があります。<br>• **map** *num_map/shards*：値は、1 ～ 1024 の範囲の整数である必要があります。<br>• **write-factor** *write_factor* ：値は 0 ～ 16 の範囲の整数である必要があります。 | • *num_replica*：デフォルト値は 2 です。<br>• *num_map/shards*：デフォルト値は 1 です。<br>• *write_factor* ：デフォルト値は 1 です。 |
| **slice-names** *cdl_slice_name* | **slice-names** *cdl_slice_name*：CDL スライス名を指定します。値は、英数文字列である必要があります。 | *cdl_slice_name*：値は 0 ～ 16 の範囲の整数である必要があります。 | NA |

## 次のタスク

CDLでの Zookeeper の構成

# CDLでの Zookeeper の構成

CDLでの Zookeeper の構成にはこれらのステップを使用します。

**手順**

**ステップ 1** グローバル コンフィギュレーション モードで、Zookeeper データ ストレージのサイズをギガバイト単位で指定します。

**cdl zookeeper data-storage-size** *data_storage_size_in_gb*

**例**：

```
[smf] smf(config)# cdl zookeeper data-storage-size 20 GB
```

（注）
デフォルト値は 20 GB です。この値には 1 ～ 65535 の範囲の整数を指定する必要があります。

**ステップ 2** Zookeeper データ ログのストレージ サイズをギガバイト単位で指定します。

**log-storage-size** *log_storage_size_in_gb*

**例**：

```
[smf] smf(config-cdl-zookeeper)# log-storage-size 20 GB
```

（注）
デフォルト値は 20 GB です。この値には 1 ～ 65535 の範囲の整数を指定する必要があります。

**ステップ 3** zookeeper で作成するレプリカの数を指定します。

**replica** *num_replicas*

**例**：

```
[smf] smf(config-cdl-zookeeper)# replica 3
```

（注）
デフォルト値は 3 です。1 ～ 16 の範囲の整数で指定する必要があります。

**ステップ 4** JMX メトリックのステータスを指定します。

**enable-JMX-metrics** *boolean_value*

**例**：

```
[smf] smf(config-cdl-zookeeper-replica)# enable-JMX-metrics true
```

（注）
デフォルト値は true です。値はブール値である必要があります。

**ステップ 5** Zookeeper データの永続ストレージのステータスを指定し、構成を保存します。

**enable-persistence** *boolean_value*

例：

```
[smf] smf(config-cdl-zookeeper-replica)# enable-persistence false
```

（注）
デフォルト値は false です。値はブール値である必要があります。

# CDL セッション データベースの構成例

このセクションでは、HA 環境での CDL の構成例を示します。

```
config
cdl system-id system_id
cdl zookeeper replica num_zk_replica
cdl datastore session
 endpoint replica ep_replica
 index map index_shard_count
 slot replica slot_replica
 slot map slot_shard_count
 slice-names cdl_slice_name
exit
```

# イベント トレース データの構成

このセクションでは、イベント トレース データを CDL データベース レコードに保存するように SMF を構成する方法について説明します。システム診断用の CDL データベース レコード内のイベント トレース データ ストレージを有効または無効にします。イベント トレース データは、サブスクライバのコール フローイベントを示します。

手順

**ステップ 1** システム診断用に、グローバル コンフィギュレーション モードでのイベント トレース データの保存を有効にします。

**system-diagnostics event-trace** *[ enable | disable ]*

例：

```
[smf] smf(config)# system-diagnostics event-trace  enable
```

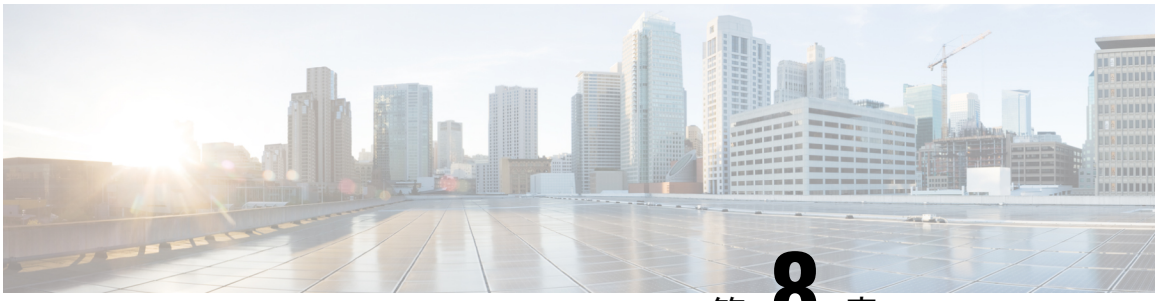
（注）
*event_trace_state* を無効にすると、各 SMF データベース レコードに対して約 1 KB のデータベース ストレージを節約できます。

構成を保存してコミットします。

**ステップ 2** [オプション（*Optional*）] **show running-config system-diagnostics event-trace** コマンドを使用して、サブスクリプションの変更が有効かどうかを確認します。

例：

```
[smf] smf# show running-config system-diagnostics event-trace
system-diagnostics event-trace enabled
```



第 8 章

# コンテンツ フィルタリングと X-Header の強化


- 機能の概要と変更履歴, on page 103
- 機能説明, on page 104
- コンテンツ フィルタリング, on page 104
- X-Header の挿入, on page 106


# 機能の概要と変更履歴

## 要約データ

***Table 22:*** 要約データ

| | |
|---|---|
| 該当製品または機能エリア | SMF |
| 該当プラットフォーム | SMI |
| 機能のデフォルト設定 | 無効：設定が必要 |
| このリリースでの関連する変更点 | N/A |
| 関連資料 | 該当なし |

## 更新履歴

***Table 23:*** マニュアルの変更履歴

| 改訂の詳細 | リリース |
|---|---|
| 最初の導入。 | 2020.02.0 より前 |

# 機能説明

SMF は、以下の機能と機能性をサポートします。

- コンテンツ フィルタリング
- X ヘッダーの強化

# コンテンツ フィルタリング

## 機能説明

コンテンツ フィルタリング（CF）サービスは、一般的に許容されないコンテンツ、またはサブスクライバの設定として不適切なコンテンツをサブスクライバが誤って公開するのを防ぎます。CF サービスは、サブスクライバ要求内の URL に基づいて、モバイル サブスクライバからの HTTP 要求と WAP 要求をフィルタ処理します。オペレータは、個々のサブスクライバがアクセスするコンテンツをフィルタリングおよび制御できます。

## コンテンツフィルタリングの構成

このセクションでは、CF サポートの構成方法を説明します。

**Note** 次の設定を除き、他のすべての設定は UPF でのみ使用され、SMF はそれを UPF に送信します。SMF は、これらの設定を使用しません。UPF の機能を有効にする方法の詳細については、『*UCC 5G UPF* 構成および管理ガイド』を参照してください。

### アクティブ課金サービスでのコンテンツ フィルタリングの構成

アクティブな課金サービスで CF を構成するには、次の構成例を使用します：

```
config
   active-charging service service_name
      content-filtering category policy-id cf_policy_id
      end
```

注：

- **content-filtering category policy-id** *cf_policy_id*: CF ポリシー番号を指定します。 *cf_policy_id* は 、1 ～ 4294967295 の範囲の整数である必要があります。

## ルールベースでのコンテンツ フィルタリングの構成

ルールベース下で CF を構成するには、次の構成例を使用します：

```
config
   active-charging service service_name
      rulebase rulebase_name
         content-filtering category policy-id cf_policy_id
         end
```

注：

- **content-filtering category policy-id** *cf_policy_id*: CF ポリシー番号を指定します。 *cf_policy_id* は 、1 ～ 4294967295 の範囲の整数である必要があります。

## APN でのコンテンツ フィルタリングの構成

APN 下で CF を構成するには、次の構成例を使用します：

```
config
   apn apn_name
      content-filtering category policy-id cf_policy_id
      end
```

注：

- **content-filtering category policy-id** *cf_policy_id*: CF ポリシー番号を指定します。 *cf_policy_id* は 、1 ～ 4294967295 の範囲の整数である必要があります。

## N7 インターフェイス上のコンテンツ フィルタリング ポリシー ID

CF カテゴリは、特定のポリシー ID の下のアクティブな課金サービスで構成されます。ルールベースと APN には、関連付けられたポリシー ID もあります。どのセッションでも、1 つのポリシー ID をいつでもセッションに関連付けることができます。その CF ポリシー ID で構成されたカテゴリは、UPF のセッションに適用できます。

PCF は、N7 インターフェイスでこの値を送信することで、CF ポリシー ID をオーバーライドできます。この目的で、N7 インターフェイスの YAML 定義で独自の IE を使用できます。CF ポリシー ID の階層は次のとおりです：

```
smPolicyDecision
   ciscoAvpSet:
      cfPolicyId: uint32 value
```

PCF が CF ポリシー ID を送信しない場合、ルールベース構成の既存の CF ポリシー ID、または APN 構成で構成されたポリシー ID が優先順に選択されます。この CF ポリシー ID 値は、「Subscriber Parameters」属性の PFCP セッション確立要求メッセージで UPF に送信されます。PDU セッションの変更中に、PCF が CF ポリシー ID を変更すると、その ID は PFCP セッション変更要求メッセージで UPF に送信されます。

# X-Header の挿入

X-Header 挿入機能と X-Header Encryption 機能（総称してヘッダー強化と呼ばれます）により、HTTP または WSP の GET および POST 要求パケット、および HTTP 応答パケットにヘッダーを追加して、エンドアプリケーションで使用できます。たとえば、モバイル広告の挿入（電話番号、IMSI、IP アドレス、ユーザーのカスタマイズ可能など）。

## サポートされている X ヘッダー 情報

構成可能なすべての X ヘッダー情報のうち、一部の情報では、SMF が対応する値を UPF に送信する必要があります。次のテーブルに、X ヘッダーの挿入のために SMF から UPF に送信される情報を示します。

***Table 24: XHeader* 情報**

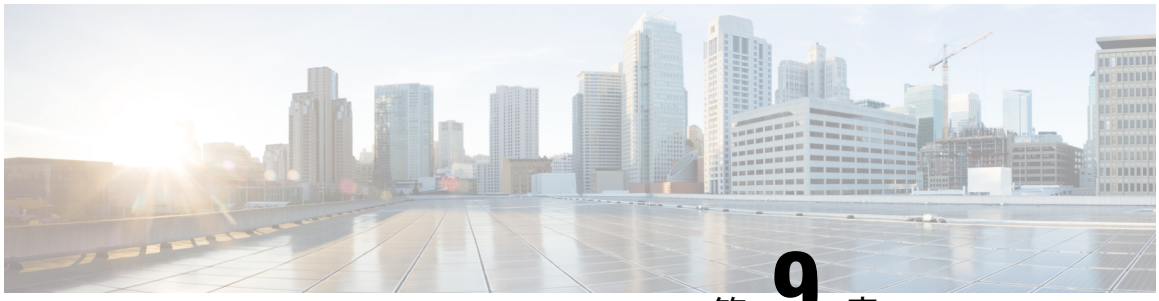
| Xheader フィールド | 説明 | セッションの確立で存在 | セッションの変更で変更 |
|---|---|---|---|
| 文字列定数 | 構成された文字列を xheader に挿入する | — | — |
| 課金 ID | フローまたはベアラー課金 ID ごと | ○ | — |
| IMEI | コールの IMEI | ○ | — |
| IMSI | コールの IMSI | ○ | — |
| Rat-Type | UE セッションの RAT タイプ | はい | はい |
| s-mcc-mnc | SGW または AMF の MCC または MNC | ○ | — |
| Sgsn-address | AMF または SGW アドレス | はい | はい |
| ULI | ユーザー ロケーション情報 | はい | はい |
| GGSN-Address | SMF の N4 または S5 エンドポイント | はい | はい |
| Radius-station-ID | UE の MSISDN | — | — |
| Sn-rulebase | コールのルールベース | はい | はい |
| Subscriber-ip-address | UE に割り当てられた IP アドレス | — | — |
| Msisdn-no-cc | MSISDN から取得 | はい | 非対応 |

subscriber-specific fields（IMSI、MSIDN、および IMEI）は、「ユーザー ID」標準 IE でエンコードされます。詳細については、3GPP 29.244、Section 8.2.101 を参照してください。

残りのフィールドは、「サブスクライバパラメータ」独自の AVP で送信されます。「Rulebase」や「UE IP address」などの一部のフィールドは、作成された PDR の一部として送信されます。

**Note**

- Xヘッダー構成が使用可能かどうかに関係なく、すべてのパラメータが常にSMFからUPFに送信されます。これらのパラメータを使用すると、セッション作成後の構成変更がただちに UPF に適用されます。
- SMF は、X ヘッダー挿入関連の構成をサポートしています。SMF では、その機能に対してこれらの構成は必要ありません。これらの構成は、UPF に送信されます。



第 9 章

# Diameter エンドポイント


- 機能の概要と変更履歴 （109 ページ）
- 機能説明 （110 ページ）
- 機能の仕組み （116 ページ）
- Diameter エンドポイントの構成 （116 ページ）
- ダイナミックな構成変更 （128 ページ）
- CCR の宛先ホスト AVP および宛先レルム AVP （130 ページ）
- ピア管理 （132 ページ）
- 失敗のハンドリング（Failure Handling） （139 ページ）
- OAM サポート （145 ページ）
- トラブルシューティング情報 （155 ページ）


## 機能の概要と変更履歴

### 要約データ

**表 *25 :* 要約データ**

| | |
|---|---|
| 該当製品または機能エリア | SMF |
| 該当プラットフォーム | SMI |
| 機能のデフォルト設定 | 有効：常時オン |
| 関連資料 | 該当なし |

# 更新履歴

表 *26 :* マニュアルの変更履歴

| 改訂の詳細 | リリース |
|---|---|
| 次のサポートが追加されました：<br>• RAR メッセージの Gx および Gy カスタム ディクショナリのサポート<br>• DWR および DWA の処理<br>• バインドされたピア | 2023.04.0 |
| 最初の導入。 | 2023.03.0 |

# 機能説明

Diameter エンドポイントは、SMF サービスの Diameter 機能を有効にするアプリ インフラ ベースのサービスです。SMF では、Diameter エンドポイントが Gx クライアントと Gy クライアントを実装します。Diameterエンドポイントは、構成、運用、およびアクションの CLI コマンドと、ポッド間通信、RPC、モニタ サブスクライバ、モニタ プロトコル、ロギング、統計などの App-infra 機能に Ops Center を活用します。

Diameter エンドポイントは次のサポートを提供します：

- Gx インターフェイスと Gy インターフェイスの両方の Diameter ピアおよび接続の管理。
- Diameter メッセージの障害処理および再試行動作を構成するための障害処理テンプレート。
- 複数の Diameter ルーティング エージェント（DRA）とピアリングし、DRA を介してリモート Diameter エンドポイントに Diameter メッセージをルーティングする機能。

（注） Diameterスタックは、DRA として機能する機能を実装していません。

- Diameter メッセージのプロトコルとサブスクライバのモニタ（SUPI および IMSI サブスクライバ キー）。
- ロギングと統計。

Diameterエンドポイントを使用するには、インターフェイスごとにアクティブまたはスタンバイ構成（Gx および Gy）で Diameter ポッドのペアを展開します。内部および外部 VIP のペアを使用して、ホスト ネットワーク構成でこれらのポッドを展開します。

オンライン課金の場合、Diameterクレジット制御アプリケーションが使用されます。オンライン クライアントである課金転送機能（CTF）は、リソース割り当てを要求し、クレジット制御情報をオンライン課金システム（OCS）に報告します。Diameterを介したクレジット制御をサポートするには、CCR（クレジット制御要求）およびCCA（クレジット制御応答）メッセージが使用されます。

サービス ポッドは、クレジット制御メッセージのDiameterエンドポイントにgRPCメッセージを送信します。Diameterエンドポイントは、Diameter CCRメッセージを変換し、それらをPCRFまたはOCSであるGxサーバおよびGyサーバに送信します。CCAを受信した後、CCAメッセージはgRPCメッセージに変換され、応答としてSMFに送信されます。

# サポートされるインターフェイス

SMFは次インターフェイスをサポートします。

- Gxインターフェイス
- Gyインターフェイス

Gxおよび Gyインターフェイスに関連する機能については、「インターフェイス サポート」の章を参照してください。

**重要** SMFに搭載されている Diameterインターフェース機能は、StarOSまたはCUPS製品と完全な機能互換性や機能性を有しているとは仮定すべきではありません。さらに、このドキュメントで言及されている構成（コマンド、統計、属性、MIBオブジェクト、アラーム、ログ、サービスを含むがこれらに限定されない）が、StarOSレガシー製品またはCUPS以外の製品との機能的な同等性を示すと想定しないでください。

この製品と StarOS レガシー製品または CUPS 以外の製品間のパリティについてのご質問は、Cisco のアカウント担当者またはサポート担当者にお問い合わせください。

# Diameter エンドポイント インスタンス

Diameter エンドポイント インスタンスは、Gx や Gy などのさまざまなインターフェイスのDiameterエンドポイントを構成するために使用されます。この構成により、展開されるDiameter エンドポイント ポッドの数が決まります。Diameter エンドポイント インスタンスの構成は必須です。

# Diameter クライアント プロファイル

Diameterクライアントは、Diameterクライアントアプリケーションと基本プロトコルをサポートするDiameterノードです。Diameterクライアントは、ネットワークのエッジに配置されているデバイスに実装され、そのネットワークにアクセス制御サービスを提供します。

Diameterプロファイルは、Diameterアプリケーションのネットワーク アクセス情報を提供します。各 Diameter クライアント プロファイルは、既存のエンドポイント プロファイルと、その名前で障害処理テンプレートに関連付けられます。SMF は、クライアント プロファイル名を使用して、Diameterエンドポイントが関連付けられたエンドポイントプロファイルを取得できるようにします。SMFはこのプロファイルを使用して、メッセージを送信するために一致するエンドポイントを評価します。

クレジット制御要求（CCR）のエンコーディングと、対応する応答、クレジット制御応答（CCA）メッセージのデコードについては、Diameterクライアントプロファイルでディクショナリを構成する必要があります。ディクショナリには、標準 AVP またはベンダー固有 AVP とともに、CCR および CCA メッセージで使用される説明を含む AVP のリストが含まれています。

# Diameter エンドポイント プロファイル

Diameter エンドポイント プロファイルは次の情報を提供します。

- 元の構成（発信元レルム、発信元ホスト名、発信元状態 ID、および発信元アドレスなど）。

  発生元状態 ID の場合、SMF はクレジット制御要求（CCR）またはデバイス ウォッチドッグ要求（DWR）メッセージに対して Diameter エンドポイントから発信される OSI サポートを提供します。 **dynamic-origin-state-id** CLI コマンドを使用して、Ops Center でダイナミック OSI 値を有効または無効にすることができます。Nodemgrは、キャッシュポッドの OSI 値を更新します。次に、Diameter エンドポイントはこの値を使用して、Capability Exchange Request（CER）メッセージ、CCR メッセージ、DWR メッセージを送信します。

- ピア レルム、宛先ホスト名、ピア IP、ピア ポートなどのピア構成。
- グローバル パラメータ（宛先ホスト AVP、VSA サポート、最大未処理メッセージ数など）。
- タイムアウト時間。

インターフェイスごとに Diameter エンドポイント プロファイルを構成できます。これらのプロファイルは、インターフェイスに対応する Diameter エンドポイント ポッドにプロビジョニングされます。次に、これらのプロファイルは、特定の Diameter クライアント プロファイルに関連付けられます。

（注） Diameter ポッド展開用の Diameter エンドポイント プロファイルを構成します。

# ピア要求管理の切断

このセクションでは、ピア要求の切断（DPR）、ピア応答の切断（DPA）、およびDiameterエンドポイントで DPR と DPA を構成するための関連 CLI コマンドについて説明します。

# 機能説明

SMF は DPR をサポートし、サーバーから受信した DPR を処理します。転送接続をシャットダウンする意図を通知するために、DPR がピアに送信されます。ピア ノードが別のノードに DPR を送信する場合、ノードはすべての必要な AVP について DPR を検証します。検証が失敗した場合、ノードはエラーを含む DPA をピア ノードに送信します。

検証に成功した場合：

- SMF ノードは、ピア ノードに DPA を送信する前に、ドレイン タイムまで待機します。DrainTime は、Diameter エンド ポイントによる DPR の受信から DPA 応答を送信するまでの時間間隔です。この間隔中に、Diameter-ep によってピアへの新しい要求は開始されません。ただし、ピアから受信したメッセージはこの間隔で処理されます。ドレイン時間は構成可能なパラメータです。ドレイン時間の値は、インバウンドメッセージのタイムアウト値よりも小さく構成することをお勧めします。この間、そのピアに新しい要求を送信しないようにアドバイスされますが、ピアから要求が着信した場合は応答する必要があります。
- 以前にメッセージがクライアントに転送され、応答を待っているかどうかに関係なく、DPA を正常に送信します。ピア ノードは成功の DPA を送信します。

サーバーがピア SMF ノードから自分自身を切断する場合、そのサーバーは切断原因 AVP とともに DPR を送信します。

- 切断の原因が再起動（REBOOTING）の場合は、Tc タイマーに基づいて接続を遅らせます。Tc は、構成可能なパラメータです。
  - 再起動時間は、接続解除の原因が「REBOOTING」で DPR を受信したピアに対して接続を再試行するまでの時間です。この間隔は、DPA 応答と接続ティアダウンの送信後に開始されます。
- 切断の原因が BUSY または DO_NOT_WANT_TO_TALK_TO_Y の場合は、より長い時間、再接続を延期します。接続時間は構成可能なパラメータです。BUSY または DO_NOT_WANT_TO_TALK_TO_YOU の場合は接続しないことをお勧めします。そのため、値を負またはゼロに構成して、決して再接続しないようにできます。
  - DoNotTalkTimeは、切断原因「DO_NOT_WANT_TO_TALK_TO_YOU」で DPR を受信したピアに対して接続が再試行されるまでの時間です。この間隔は、DPA 応答と接続ティアダウンの送信後に開始されます。
  - BusyTime は、切断の原因が「BUSY」の DPR を受信したピアに対して接続が再試行されるまでの時間です。この間隔は、DPA 応答と接続ティアダウンの送信後に開始されます。
- 再接続の時間は、すべてのポッドの再起動またはポッドのフェールオーバーに適用されますが、サイトのフェールオーバーには適用されません。

# DWR と DWA の処理

## 機能説明

Diameterエンドポイントは、ピアからの着信デバイス ウォッチドッグ要求（DWR）を処理し、成功結果コードを含むデバイス ウォッチドッグ応答（DWA）で応答します。Diameter エンドポイントは、DWR メッセージを送信することにより、アイドル接続に問題があるか、または転送が失敗しているピアの検出もサポートしています。

## 機能の仕組み

DWR をピアに送信するために、Diameter エンドポイントは、app-infra で提供されるホスト モニタリングを使用して、DWR を生成する必要があるかどうかを確認します。

各ホスト モニタリング チェックで、Diameter エンドポイントは、最後のチェックから現在のチェックの間に発生したメッセージ交換をチェックします。メッセージの要求と応答の両方がある場合、Diameter エンドポイントはそれをメッセージ交換と見なします。メッセージ交換は、次のシナリオでは考慮されません。

- Diameter エンドポイントが要求を送信し、ピアからの応答を受信しない場合。
- Diameterエンドポイントが要求を受信したものの、ピアに応答を送信できなかった場合。

Diameterエンドポイントとピアの間でメッセージ交換が発生しない場合、Diameterエンドポイントはピアに向けて DWR を生成します。Diameter エンドポイントは、次のシナリオを DWR の障害と見なします。

- DWR の送信に失敗した場合。
- **basemsg retransmission-timeout** パラメータで構成された時間内に DWA を受信しなかった場合。
- 応答があるが、失敗結果コードが含まれる場合。

DWR に障害が発生した場合は、 **basemsg retransmissions** パラメータ値がゼロ以外の値に構成されていると、再試行が行われます。再試行は、次のホスト モニタリング チェックで実行されます。再試行中に、Diameter エンドポイントが以前に送信された DWR のいずれかに対する DWA を受信した場合、Diameter エンドポイントはそれを無視し、成功した DWR に対して考慮しません。

設定された再試行の後でも、DWR が成功しない場合は、ステータスが失敗として報告され、接続がリセットされます。次のホストモニタリングチェック中にのみ接続をリセットした後、接続を再確立します。次に、機能交換要求（CER）と DWR が送信されます。ただし、DWR または DWA が成功しない場合、Diameter エンドポイントはピアにメッセージを送信しません。DWR または DWA 障害が発生した場合、接続がリセットされます。

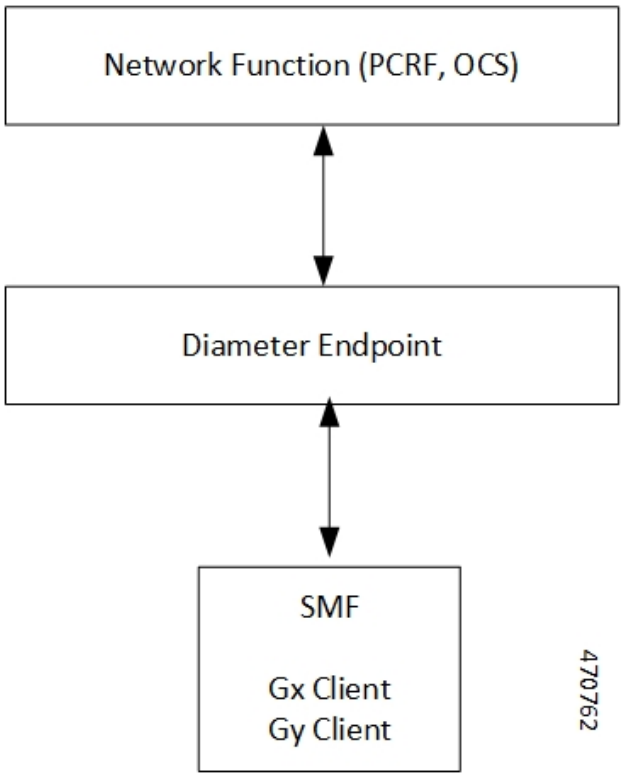
（注） すべてのホストのホストモニタリングが並行して実行されますが、モニタリングはすべてのホストの完了後に完了します。1 つのホストのモニタリングが遅延すると、すべてのホストの次のモニタリングも遅延します。

# アーキテクチャ

Diameter エンドポイントである Diameter 共通スタックは、NF と、サポートされているアプリケーションのクライアントモードとサーバーモードの両方間のインターフェイスです。

次の図は、共通 Diameter スタックのアーキテクチャを示しています。

**図 *18 :* 共通 *Diameter* スタック**




共通の Diameter スタックには、次のコンポーネントが含まれています。

- ネットワーク機能：ポリシーおよび課金ルール機能（PCRF）とオンライン課金システム（OCS）
- Diameter エンドポイント
- SMF-Gx および Gy クライアントの Diameter インターフェイス

サポートされている Diameter インターフェイスとその関連機能の詳細については、「インターフェイスのサポート」の 章を参照してください。

# 機能の仕組み

Diameter エンドポイントは、Diameter メッセージを Diameter ピアに、および内部 IPC メッセージを他のポッドに送受信するために、アプリ インフラ フレームワークを使用します。たとえば、P-GW サービス、cnBNG サービスなどです。SMF では、Diameter エンドポイントが Gx クライアントと Gy クライアントを実装します。

Diameter を介してクレジット制御をサポートするため、Diameter メッセージの 2 つである「クレジット制御要求（CCR）」と「クレジット制御応答（CCA）」が使用されます。サービスポッドは、gRPC メッセージを Diameter エンドポイントに送信し、gRPC メッセージをクレジット制御メッセージに変換します。その後、Diameter エンドポイントが CCR メッセージを Gx または Gy サーバ（PCRF または OCS）に送信します。Gx または Gy サーバが CCA メッセージを送信した後、Diameter エンドポイントは CCA メッセージを gRPC メッセージに変換し、応答として P-GW サービスに送信します。

Diameter は、Gx および Gy インターフェイスの *3GPP 29.212* バージョン *15.3.0* および *3GPP 32.299* バージョン *12.9.0* 仕様に従って、標準 AVP をサポートします。

## 標準準拠

この直径エンドポイントは、以下の基準に準拠しています：

- *3GPP 29.212* バージョン *15.3.0*
- *3GPP 32.299* バージョン *12.9.0*

## 制限事項

Diameter エンドポイントには次の制限があります：

- Diameter エンドポイントは、インターフェイスごとに 1 ペアのポッドのみをサポートします。

# Diameter エンドポイントの構成

Diameter エンドポイントの構成には、次の手順が含まれます：

1. Diameter エンドポイント インスタンスの構成 （117 ページ）
2. Diameter クライアント プロファイルの構成 （118 ページ）

3. Gx および Gy インターフェイスでの Diameter プロファイル エンドポイントの構成 （120 ページ）

# Diameter エンドポイント インスタンスの構成

Diameter エンドポイント インスタンスを構成するには、次の構成例を使用します：

```
config
   instance instance-id instance-id
      endpoint diameter
      interface interface_name
         internal-vip ip_address
         vip-ip ip_address
         mode mode_value
      exit
```

注：

- **instance instance-id** *instance-id* **endpoint diameter** ：展開する Diameter エンドポイント ポッドの数を指定します。
- **interface** *interface_name*：Diameter エンドポイントのインターフェイス（Gx や Gy など）を指定します。
- **internal-vip** *ip_address*：Diameter エンドポイントがサービスからの要求をリッスンするための内部 VIP IP アドレスを指定します。 **internal-vip** は必須パラメータです。
- **vip-ip** *ip_address*：Diameter クライアントに対応する の VIP IPv4 アドレスを指定します。 **vip-ip** は必須パラメータです。
- **mode** *mode_value*：特定のモードで Diameter エンドポイントを指定します。 **mode** は必須パラメータです。

（注） SMF では *mode_value* として クライアントのみがサポートされます。

## 設定例

以下は、Diameter エンドポイント インスタンスの構成例です。

```
instance instance-id 1
endpoint diameter
  interface gy
   internal-vip 209.165.200.234
   vip-ip 209.165.200.234
   mode client
   exit
  exit
  interface gx
   internal-vip 209.165.200.234
```

```
   vip-ip 209.165.200.234
   mode client
  exit
```

## 設定の確認

Diameter エンドポイント インスタンスが構成されているかどうかを確認するには、次の **show running-config instance instance-id** *instance_id* **endpoint diameter** コマンドを使用します。

```
smf# show running-config instance instance-id 1 endpoint diameter
instance instance-id 1
endpoint diameter
  interface gy
   internal-vip 209.165.200.234
   vip-ip 209.165.200.234
   mode client
   exit
  exit
  interface gx
   internal-vip 209.165.200.234
   vip-ip 209.165.200.234
   mode client
  exit
```

# Diameter クライアント プロファイルの構成

**表 *27*: 機能の履歴**

| 機能名 | リリース情報 | 説明 |
|---|---|---|
| 同じディクショナリのサポートがRARメッセージにも拡張されています。 | 2023.04 | 以前のリリースでは、CCR-I、CCA-U、および CCA-T メッセージの場合、クライアントで指定されたディクショナリ（カスタム ディクショナリ）が適用されていました。RAR メッセージでは、共通のディクショナリが使用されていました。このリリースでは、RAR メッセージも CCR-I、CCA-U、および CCA-T メッセージが使用するのと同じディクショナリを使用します。 |

Diameter クライアント プロファイルを構成するには、次の構成例を使用します：

```
config
  profile diameter-client diameter_client_name
    endpoint endpoint_profile_name
    failure-handling-profile profile_name
```

```
dictionary-name { dcca-custom8 | default | r8-gx-standard }
end
```

注：

- **profile diameter-client** *diameter_client_name*：Diameter クライアント プロファイル名を指定します。
- **endpoint** *endpoint_profile_name*：Diameter クライアント プロファイルに関連付ける既存のエンドポイント プロファイル名を指定します。最大 100 個のクライアント プロファイルを定義できます。
- **failure-handling-profile** *profile_name*：Diameter クライアント プロファイルに関連付ける既存の障害処理プロファイルを指定します。
- **dictionary-name { dcca-custom8 | default | r8-gx-standard }**：次のディクショナリのいずれかを指定します。
  - **dcca-custom8**：このディクショナリは標準の Gy ディクショナリです。
  - **default**：このディクショナリはデフォルトのディクショナリです。
  - **r8-gx-standard**：このディクショナリは標準の Gx ディクショナリです。

（注） 指定されたディクショナリは、クレジット制御 - 初期（CCR-I）、クレジット制御 - 更新（CCR-U）、クレジット制御 - 終了（CCR-T）、および再認証要求（RAR）メッセージに使用されます。

## 設定例

以下は、Diameter クライアント プロファイルの構成例です。

```
profile diameter-client gydc01
    endpoint gxProf1
    failure-handling-profile fh1
    exit
```

## 設定の確認

Diameter クライアント プロファイルが構成されているかどうかを確認するには、**show running-config profile diameter-client** コマンドを使用します：

```
[smf] smf# show running-config profile diameter-client
profile diameter-client gydc01 endpoint gxProf1 failure-handling-profile fh1
dictionary-name kt-gy
exit
profile diameter-client gydc11 endpoint gyProf1 failure-handling-profile fh2
exit
profile diameter-client gydc12 endpoint gyProf2 failure-handling-profile fh3
exit
```

```
profile diameter-client gxdc02 endpoint gxProf1 failure-handling-profile fh4
exit
```

# Gx および Gy インターフェイスでの Diameter プロファイル エンドポイントの構成

表 *28 :* 機能の履歴

| 機能名 | リリース情報 | 説明 |
|---|---|---|
| Diameter Gx および Gy インターフェイスの VRF サポート | 2023.04 | SMF は、Diameter Gx および Gy インターフェイスのクライアント側 VRF をサポートします。プロファイルの Diameter エンドポイントは、Diameter エンドポイントから構成する VRF 名とインターフェイス名を参照します。Diameter エンドポイントは、VRF 名を使用して、Diameter クライアントから TCP 接続を作成します。 |

Diameter Gx および Gy インターフェイスの Diameter プロファイル エンドポイント インスタンスを構成するには、次の構成例を使用します :

```
config
  profile diameter-endpoint interface_name
     name profile_name
     internal-vip ip_address
        destination-host-avp message_type
        vsa-support vendorId-source
        max-outstanding number_of_messages
        response-timeout response_timeout_value
        connection-timeout connection-timeout_value
        basemsg retransmission-timeout retransmission_timeout_value
        basemsg retransmissions max_retry_value
        basemsg watchdog-interval interval_value
       dscp [ dscp_value | af11 | af12 | af13 | af21 | af22 | af23 | af31
 | af32 | af33 | af41 | af42 | af43 | be | cs1 | cs2 | cs3 | cs4 | cs5
 | cs6 | cs7 | ef ]
        origin realm realm_name
        origin host host_name address ipv4 ip_address
        origin peer origin_peer_name
        realm  realm_name
        address ipv4 ip_address
        address vrf vrf_name
        port peer_port
        destination-host-name  destination_host_name
```

```
        load-balancing-algorithm highest-weight
       route-entry host [ host-name | * ] realm [ realm-name | * ] peer
 peer_name weight weight_value
        route-failure deadtime deadtime_value result-code result_code_value
threshold  number
        route-failure result-code result_codes_value
        route-failure threshold  threshold_number
       route-failure recovery-threshold percent  recovery_threshold_percentage

        dynamic-route expiry-timeout  expiry_timeout_value
        dynamic-origin-state-id  boolean_value
        exit
```

注：

- **profile diameter-endpoint** *interface_name*：Gx または Gy インターフェイスの Diameter プロファイルを指定します。
- **name** *profile_name*：Diameter プロファイル インターフェイスのプロファイル名を指定します。各プロファイルは、これらのピアに送信される Diameter メッセージの Diameter 送信元情報とピア情報を設定します。

（注） インターフェイスごとに最大 100 個のプロファイルを定義できます。

- **internal-vip** *ip_address*：サービス ポッドと通信するための内部 VIP IP アドレスを指定します。 **internal-vip** は必須パラメータです。
- **destination-host-avp** *message_type*：宛先ホスト AVP をエンコードするメッセージのタイプを指定します。

（注） SMF は *message_type* の *always*値のみをサポートします。

- **vsa-support** *vendorId-source*：Diameter ピア機能の交渉に使用されるベンダー ID DIABASE の送信元を指定します。

（注） SMF では、*vendorId-source* の *all-from-dictionary*値だけがサポートされます。

- **max-outstanding** *number_of_messages*：応答を待機している間に、プロファイル内のピアに送信される Diameter メッセージの最大数を指定します。デフォルト値は 256 です。number_of_messages は 1 ～ 4096 の範囲である必要があります。

- **response-timeout** *response_timeout_value*：Diameter アプリケーションが Diameter サーバーに送信する要求メッセージの最大許容応答時間を指定します。デフォルト値は 60 です。response_timeout_value は　1 ～ 300 の範囲である必要があります。
- **connection-timeout** *connection-timeout_value*：Diameter サーバーへの TCP 接続など、トランスポート層の接続を確立するために許容される最大時間を指定します。デフォルト値は 30 です。connection -*timeout_value* は 1 ～ 300 の範囲である必要があります。
- **basemsg retransmission-timeout** *retransmission_timeout_value*：デバイス ウォッチドッグ要求（DWR）や機能交換要求（CER）などの基本メッセージの再送信間のタイムアウト値を、Diameter サーバーに指定します。デフォルト値は 30 です。retransmission_timeout_value は 1 ～ 120 の範囲である必要があります。
- **basemsg retransmissions** *max-retries*：基本メッセージを再送信する必要がある最大回数を指定します。デフォルト値は 1 です。*max-retries* は 1 ～ 10 の範囲で指定する必要があります。
- **basemsg watchdog-interval** *interval_value*：Diameter サーバーに送信される 2 つの DWR メッセージ間の最小時間間隔を指定します。デフォルト値は 5 です。*interval_value* は 5 ～ 30 の範囲である必要があります。
- **dscp [** *dscp_value* **| af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef ]** ：Diameter サーバーに送信される Diameter メッセージの IP ヘッダーにある DiffServ コードポイント（DSCP）値を指定します。デフォルト値は、**be** です。*dscp_value* は、0 ～ 63 の範囲のである必要があります。必要に応じて、次の他の DSCP 値を選択します。
  - **af**xx：ホップ動作（PHB）単位の相対的優先転送 xx を使用する場合は、この値を指定します。
  - **be**：ベストエフォートの転送 PHB を使用するには、この値を指定します。 **be** がデフォルト値です。
  - **cs**[x]：PHB ごとにクラスセレクタ x を使用するには、この値を指定します。
  - **ef**：完全優先転送 PHB を使用するには、この値を指定します。
- **origin realm** *realm_name*：Diameter エンドポイントのレルムの名前を指定します。このパラメータは必須です。
- **origin host** *host_name* **address ipv4** *ip_address* ：Diameter エンドポイントの FQDN であるホスト名を指定します。IPv4 アドレスを指定します。これは、Diameter クライアント接続の Diameter エンドポイントのバインド IP アドレスです。
- **origin peer** *origin_peer_name* ：Diameter ピアの識別子を指定します。このパラメータは必須です。

（注）　最大 5000 のピアを構成できます。

- **realm** *realm_name*：ピアの名前でピアのレルムの名前を指定します。このパラメータは必須です。
- **address ipv4** *ip_address*：Diameter ピアの IP アドレスを指定します。
- **address vrf** *vrf_name*：Diameter エンドポイントから参照される VRF 名を指定します。
- **port** *peer_port*：Diameter ピアのポートを指定します。このパラメータは必須です。
- **destination-host-name** *destination_host_name*：宛先ホスト AVP で使用されるカスタム宛先ホスト名を指定します。このパラメータはオプションです。
- **load-balancing-algorithm highest-weight** ：障害シナリオで最も高い重み付けを持つアイドル サーバを選択します。複数のサーバーの負荷が同じ高い場合、ロード バランシングはそれらのサーバー間で行われます。
- **route-entry host [ host-name | * ] realm [ realm-name | * ] peer** *peer_name* **weight** *weight_value* ：このコマンドを使用して、ルートテーブルのピアなど、2 つの静的エントリを構成します。既存の同じフラグ、ホスト、レルムを使用してエントリを構成すると、重みのみがそれら 2 つのうち上位のもので更新されます。 **host** および **realm** パラメータでは、ワイルドカード文字の値を使用できます。 **weight** はオプション パラメータで、デフォルト値は 10 です。**peer** は必須パラメータです。

（注） 同じホストとレルムで異なるピアを使用する複数のルートエントリを、上書きせずに構成できます。

- **route-failure deadtime** *deadtime_value***result-code** *result_code_value* **threshold** *number*：システムがルートを **FAILED** ステータスに保持する期間を秒単位で指定します。構成された期間が経過すると、システムはステータスを **AVAILABLE**に変更します。 *deadtime_value* は、1 ～ 86400 の範囲の整数である必要があります。デフォルト値は 60 です。
- **route-failure recovery-threshold percent** *recovery_threshold_percentage*：ステータスを **FAILED** から **AVAILABLE**に一時的に変更するときに、エラー カウンタがリセットされる割合の値を指定します。たとえば、エラー カウンタが 16 の場合、 **AVAILABLE** ステータスは **FAILED** ステータスに変わりました。構成されたデッドタイムが経過すると、ステータスが **AVAILABLE**に変わります。 *recovery_threshold_percentage* が 75% で構成した場合、に失敗カウンタは 12 にリセットされ、これは 16 の 75% です。デフォルトは 90 です。
- **dynamic-route expiry-timeout** *expiry_timeout_value*：Diameter 宛先ホストに到達した後に作成したダイナミック ルートの有効期限を指定します。デフォルト値は 1 日 に相当する 86,400 秒です。
- **dynamic-origin-state-id** *boolean_value* ：ダイナミックな送信元状態 ID を有効にするか無効にするかを指定します。デフォルト値は true です。

（注） 設定がダイナミックから静的に変更された後、ピアがダイナミック送信元状態 ID または静的な送信元状態 ID のいずれかで起動すると、ピアはデフォルトの静的な値を送信します。同様に、ダイナミックから静的への構成変更の場合、ピアは、Diameter エンドポイントがキャッシュ ポッドからフェッチする動的な値を送信します。この場合、再接続があります。

## 設定例

以下は、Gy インターフェイスの Diameter エンドポイントの構成例です。

```
profile diameter-endpoint gy
 internal-vip 209.165.200.234
 name gyProf1
  destination-host-avp always
  vsa-support all-from-dictionary
  max-outstanding  128
  response-timeout 80
  connection-timeout 20
  dscp af11
  basemsg retransmission-timeout 20
  basemsg retransmissions 2
  basemsg watchdog-interval 25
  origin realm gy-cisco
  origin host gy.cisco.com
   address ipv4 209.165.200.229
  exit
  peer gyPeer1
   realm  GyServer1.com
   destination-host-name dest.host2.com
   address ipv4 209.165.200.230
   port 3900
  exit
  peer gyPeer2
   realm GyServer2.com
   address ipv4 209.165.200.231
   port 3901
  exit
exit
```

以下は、VRF と関連付けられた Diameter エンドポイントの構成例です。

```
profile diameter-endpoint gx
instance instance-id 1
  name gxProf1
   destination-host-avp always
   vsa-support all-from-dictionary
   max-outstanding 128
   response-timeout 20
   connection-timeout 5
   dscp be
   basemsg retransmission-timeout 2
   basemsg retransmissions 10
   basemsg watchdog-interval 6
   origin realm gx-cisco
   origin host gx.cisco.com
    address ipv4 209.165.200.230
```

```
    address vrf vrf_signaling
   exit
   peer gxPeer1
    realm dummyDestRealm.com
    address ipv4 209.165.200.231
    port  3868
   exit
   peer gxTest
    realm xyznetworks.com
    address ipv4 209.165.200.232
    port  4868
   exit
  exit
 exit
exit
```

## 設定の確認

Gx または Gy インターフェイスの Diameter エンドポイントが構成されているかどうかを確認するには、次の **show running-config profile diameter-endpoint** コマンドを使用します。

```
[smf] smf# show running-config profile diameter-endpoint
 profile diameter-endpoint gx
 internal-vip 209.165.200.234
 name gxProf1
  destination-host-avp always
  vsa-support all-from-dictionary
  origin realm gx-cisco
  origin host gx.cisco.com
   address ipv4 209.165.200.235
  exit
  peer gxPeer1
   realm  GxServer1.com
   destination-host-name dest.host1.com
   address ipv4 ipv4 209.165.200.230
   port 3870
  exit
  peer gxPeer2
   realm GxServer2.com
   address ipv4 10.84.27.161
  exit
 exit

profile diameter-endpoint gy
 internal-vip 209.165.200.234
 name gyProf1
  destination-host-avp always
  vsa-support all-from-dictionary
  max-outstanding  128
  response-timeout 80
  connection-timeout 20
  dscp af11
  basemsg retransmission-timeout 20
  basemsg retransmissions 2
  basemsg watchdog-interval 25
  origin realm gy-cisco
  origin host gy.cisco.com
   address ipv4 209.165.200.229
  exit
  peer gyPeer1
   realm  GyServer1.com
   destination-host-name dest.host2.com
   address ipv4 209.165.200.230
```

```
   port 3900
  exit
  peer gyPeer2
   realm GyServer2.com
   address ipv4 209.165.200.231
   port 3901
  exit
exit
```

Diameter エンドポイントが VRF に関連付けられているかどうかを確認するには、次の **show running-config profile diameter-endpoint gx** コマンドを使用します。

```
profile diameter-endpoint gx
instance instance-id 1
  name gxProf1
   destination-host-avp always
   vsa-support all-from-dictionary
   max-outstanding 128
   response-timeout 20
   connection-timeout 5
   dscp be
   basemsg retransmission-timeout 2
   basemsg retransmissions 10
   basemsg watchdog-interval 6
   origin realm gx-cisco
   origin host gx.cisco.com
    address ipv4 209.165.200.230
   address vrf vrf_signaling
   exit
   peer gxPeer1
    realm dummyDestRealm.com
    address ipv4 209.165.200.231
    port  3868
   exit
   peer gxTest
    realm xyznetworks.com
    address ipv4 209.165.200.232
    port  4868
   exit
  exit
 exit
exit
```

# DPR のビジー時間の構成

Diameter ep で DPR のビジータイムを構成するには、次の構成を使用します：

```
config
  profile diameter-client diameter_client_name
    endpoint endpoint-profile-name
      peer peer_name
      disconnect peer request
        busy time time_duration
        end
```

注：

- **profile diameter-client** *diameter_client_name*：Diameter クライアント プロファイル名を指定します。

- **endpoint** *endpoint-profile-name*：Diameter クライアント プロファイルに関連付ける既存のエンドポイント プロファイル名を指定します。
- **peer** *peer_name*：ピア ノードの名前を指定します。
- **busy time** *time_duration*：ピアへの接続を再試行するまでの時間を指定します。継続時間の値は、1 ー 300 秒の範囲の整数である必要があります。デフォルト値は 3 秒です。

# DPR の通話禁止時の構成

Diameter ep で DPR の通話禁止時間を構成するには、次の構成を使用します：

```
config
  profile diameter-client diameter_client_name
    endpoint endpoint-profile-name
      peer peer_name
      disconnect peer request
        do not talk time time_interval
        end
```

注：

- **profile diameter-client** *diameter_client_name*：Diameter クライアント プロファイル名を指定します。
- **endpoint** *endpoint-profile-name*：Diameter クライアント プロファイルに関連付ける既存のエンドポイント プロファイル名を指定します。
- **peer** *peer_name*：ピア ノードの名前を指定します。
- **do not talk time** *time_interval*：Diameter エンドポイントによる DPR の受信から DPA 応答の送信までの時間間隔を指定します。時間間隔値の値は、1 ー 300 秒の範囲の整数である必要があります。デフォルト値は 3 秒です。

# DPR のドレイン時間の構成

Diameter ep で DPR のドレイン時間を構成するには、次の構成を使用します：

```
config
  profile diameter-client diameter_client_name
    endpoint endpoint-profile-name
      peer peer_name
      disconnect peer request
        drain time time_interval
        end
```

注：

- **profile diameter-client** *diameter_client_name*：Diameter クライアント プロファイル名を指定します。

- **endpoint** *endpoint-profile-name*：Diameter クライアント プロファイルに関連付ける既存のエンドポイント プロファイル名を指定します。
- **peer** *peer_name*：ピア ノードの名前を指定します。
- **drain time** *time_interval*：Diameter エンドポイントによる DPR の受信から DPA 応答の送信までの時間間隔を指定します。時間間隔値は、1 ～ 10 秒の範囲の整数である必要があります。デフォルト値は 3 秒です。

## DPR の再起動時間の構成

Diameter ep で DPR のリブート タイムを構成するには、次の構成を使用します：

```
config
  profile diameter-client diameter_client_name
    endpoint endpoint-profile-name
      peer peer_name
      disconnect peer request
        reboot time time_duration
        end
```

注：

- **profile diameter-client** *diameter_client_name*：Diameter クライアント プロファイル名を指定します。
- **endpoint** *endpoint-profile-name*：Diameter クライアント プロファイルに関連付ける既存のエンドポイント プロファイル名を指定します。
- **peer** *peer_name*：ピア ノードの名前を指定します。
- **reboot time** *time_duration*：ピアへの接続を再試行するまでの時間を指定します。継続時間の値は、1 ー 300 秒の範囲の整数である必要があります。デフォルト値は 3 秒です。

# ダイナミックな構成変更

## 機能説明

SMF を使用すると、既存のコールに影響を与えずに、Diameter エンドポイント構成をダイナミックに変更できます。

## 機能の仕組み

次の表に、さまざまな Diameter エンドポイント構成に対する動的更新の影響を示します：

表 *29 : Diameter* エンドポイント構成の動的更新

| 設定（Configuration） | ダイナミックな変更 | 既存のセッションへの影響 |
|---|---|---|
| 接続属性：<br>• BaseMsg 属性（retransmissionTimeout、再送信など）<br>• connectionTimeout<br>• responseTimeout<br>• originStateId<br>• ホスト アドレス、ホスト名、レルムなどの発信元属性<br>• アドレス、ポート、レルムなどのピア属性 | 許可 | 接続属性の変更は、次の影響があります：<br>• RPC は登録解除され、エンドポイント プロファイル内のすべてのピアの新しい値で登録されます。<br>• ピアで開始されたすべてのメッセージは、接続がダウンすると失敗します。<br>• ピアで送信中のすべての要求がドロップされます。サーバーは、既存のコールに対するこれらの接続で要求メッセージ（RAR）と応答メッセージ（CCA）を送信できません。 |
| DisconnectPeerRequest のプロパティ：<br>• drainTime<br>• rebootTime<br>• doNotTalkTime<br>• busyTime | 不可 | ピアの DisconnectPeerRequest プロパティが更新されると、新しい値はポッドの再起動後または接続のリセット後にのみ有効になります。 |
| ルートエントリの更新または追加 | 許可 | ルート エントリの更新または追加は、次の影響があります：<br>• ルート エントリは、変更後に再作成されます。<br>• ピアの登録を解除すると、そのピアのすべてのルート エントリが削除されます。 |

| 設定（Configuration） | ダイナミックな変更 | 既存のセッションへの影響 |
|---|---|---|
| Diameter エンドポイント プロファイルの削除 | 許可 | エンドポイント プロファイルを削除すると、次のような影響があります：<br>• エンドポイント プロファイルのすべてのピアが登録解除されます。<br>• これらのピアまたはルートを使用する既存のコールは失敗します。<br>• これらのピアで新しいコールは開始されません。 |

# CCR の宛先ホスト AVP および宛先レルム AVP

## 機能説明

宛先ホスト AVP は、Diameter 要求メッセージの転送またはルーティングに使用されます。GxやGyなどのアプリケーションが使用する宛先ホスト名は、着信アプリケーション レベル メッセージから識別されます。宛先ホストAVPが存在しない場合、メッセージは、宛先レルム AVPで指定されたレルム内のアプリケーションをサポートする任意のDiameterサーバーに送信されます。

エンドユーザーの構成に基づいて、CCR の宛先ホスト AVP と再試行メッセージを含めることができます。

宛先ホスト AVP は、指定された基準に基づいて CCR メッセージに含めるか除外します。

- destination-host-avp が **always**に設定されている場合、CCR-I/U/T の宛先ホスト AVP が（再試行されたメッセージでも）含まれます。
- destination-host-avp が **session-binding**に設定されている場合、再試行されていない、またはセカンダリ ピアに送信されていない宛先ホスト専用 CCR-U/T メッセージが含まれます。

宛先レルム AVP は次のように設定されます。

- CCR-I メッセージおよび非 DRA 場合の CCR-U/T のピアのレルム。
- DRA のケースで、以前の CCA-I/U で受信した Origin-Realm。

# 宛先ホスト AVP の構成

宛先ホスト AVP の構成するには、次のサンプル構成を使用します：

```
config
  profile diameter-endpoint interface_name
    instance instance-id instance-id
      name profile_name
        destination-host-avp [ always | session-binding ]
  exit
```

注：

- **profile diameter-endpoint** *interface_name*：Diameter エンドポイント プロファイル（Gx または Gy インターフェイス）を指定します。
- **instance instance-id** *instance-id* ：GR インスタンスを指定します。
- **name** *profile_name*：Diameter エンドポイント プロファイル名を指定します。

（注） インターフェイスごとに最大 100 個のプロファイルを定義できます。

- **destination-host-avp [ always | session-binding ]**：宛先ホスト AVP をエンコードする次のいずれかのメッセージ タイプを指定します：
  - **always**：destination-host-avp がこのメッセージタイプに構成されている場合は、CCR-I、CCR-U、または CCR-T メッセージと再試行メッセージの両方に destination-host-avp を含めます。 **always** がデフォルトのメッセージ タイプです。
  - **session-binding**：destination-host-avp がこのメッセージ タイプに構成されている場合は、destination-host-avp を CCR-U および CCR-T メッセージでエンコードします。CCR-I メッセージと再試行メッセージはエンコードされません。

## 設定例

宛先ホスト AVP の構成例を次に示します。

```
profile diameter-endpoint gx
   instance instance-id 1
      name gxProf1
         destination-host-avp session-binding
exit
```

# ピア管理

## 機能説明

SMFは、ルーティング内のピア管理をサポートしています。これにより、トランザクションを発生させる適切なピアを選択できます。

ピア選択ロジックは、Diameterのエンドポイントとホストの選択の構成によって異なります。

Diameter サーバは、DRA を介して直接的および間接的な方法でゲートウェイに接続します。ピア管理に関与するエンティティは次のとおりです。

1. Destination-Host：要求にサービスを提供する Diameter エンティティまたは Diameter メッセージの最終宛先
2. ピア：トランスポート（TCP）接続を直接確立する Diameter エンティティと接続します。DS または DRA のいずれかです。
3. ルート エントリ：ゲートウェイから Diameter エンティティに到達するためのパスを定義します。基本的に、特定のDiameterエンティティに到達するために接続する次の直近のピアです。
4. ルーティング テーブル：diabase ライブラリは、ルートエントリのテーブルを維持します。ルーティング テーブルの構築は、Diameter エンドポイント（ピアおよびルートエントリ CLI）での構成を通じて構築され、応答メッセージからダイナミックに学習されます。
5. マルチパス ルート：マルチパス ルートは、特定の Diameter エンティティに到達するための複数のルート エントリがある場合です。

## ルート フラグ

次に、Diameter エンドポイントのルート フラグを示します：

**表 *30 :* ルート フラグ**

| フラグ名 | 説明 |
|---|---|
| 静的（S） | スタティック ルートは、Diameter エンドポイントの構成に基づくルート エントリです。 |
| パスキャッシュ（P） | すべての Diameter セッションには、ルーティング テーブル内のルート エントリへの参照があります。セッションのスタティック ルートを選択すると、そのスタティック ルートのコピーまたはパスキャッシュ ルートが作成されます。フラグ値以外はスタティック ルートと同じです。 |

| フラグ名 | 説明 |
| --- | --- |
| ダイナミック（D） | ダイナミック ルートは、ピアからの応答メッセージから学習したルート エントリです。 |

## ルート ステータス

Diameter エンドポイントのピアのルート ステータスは次のとおりです。

**表 *31* : ルート ステータス**

| ルート ステータス | 説明 |
| --- | --- |
| Pending | すべてのスタティック ルートはこのステータスから始まり、RPC ホストの登録を確認します。 |
| アクティブ | ping メソッドが成功すると、[保留（Pending）] ステータスは [アクティブ（Active）] ステータスに移行します。 |
| 非アクティブ | ping 方式が失敗すると、そのピアを含むすべてのルートが非アクティブとしてマークされます。このステータスは、ピアが到達可能になるまで維持されます。 |
| 失敗しました（Failed） | アクティブなルートは、ルート失敗基準を満たすと、失敗ステータスに移行します。 |
| Deleted | どのルートもハード削除されていませんが、ソフト削除されたままで、ステータスは[削除済み（Deleted）] になります。 |
| Expired | 期限切れ後のダイナミック ルートは、[期限切れ（Expired）] ステータスに設定されます。 |
| クローン | スタティック ルートから Path-Cache ルートが作成されると、元のスタティック ルートのステータスが [複製（Cloned）] に変わります。[複製（Cloned）] は内部ステートであり、レガシーの実装から借用されていません。 |

## ピア管理に関する考慮事項

Diameter エンドポイントでのピア管理に関する考慮事項は次のとおりです。

- DRA は、各エンドポイント プロファイルのルートテーブルを作成します。エンドポイント内で構成されたピアは、ルート テーブルのルート エントリのプライマリ ソースです。

- ピアには、ピア名とは異なる Destination-Host-Name を設定するオプションの CLI があります。宛先ホスト名が設定されていない場合は、ピア名を Destination-Host-Name にコピーします。
- 各ピアは、ダイレクトおよびレルムベースのルート エントリを作成します。Destination-Host-Name がピア名と異なる場合、ルート エントリを 1 つ追加します。
- スタティック ルートのデフォルトの重みは 10 です。ピア エントリから形成されたルートの重みは構成できません。ただし、同じホストとレルムの組み合わせを持つルートエントリを使用して、より高い値で上書きできます。
- ルート テーブルには、エンドポイント プロファイルの更新通知が表示され、各エントリのステータスは [保留中（Pending）] になります。
- セッションがレルム ベースのルート エントリを参照している場合にのみ、応答パスのダイナミック ルートを追加できます。直接ルート エントリの場合、応答パスにダイナミック ルートを追加することはできません。
- 新しいダイナミック ルートの重みは、要求パスで選択されたルートと同じです。
- ダイナミック ルートには有効期限が構成されています。その動的ルートを使用したメッセージ交換がある場合、または応答の発信元ホストと発信元レルムが宛先とは異なるその動的ルートを応答が指している場合、動的ルートの有効期限は、新しい有効期限で更新されます。要求のホストおよび宛先レルム。

# ルートの選択

ルート選択プロセスとその再試行での使用方法は次のとおりです。

1. CCR-I メッセージまたは CCR-U メッセージへの応答を提供する際に、Diameter エンドポイントは、プライマリ ホスト、セカンダリ ホスト、レルム、およびバインドされたピアの詳細をルートデータの一部として送信します。同じ詳細が、後続の要求の一部としてサービスによって提供されます。
2. サービスからの要求にルートデータフィールドがない場合、Diameter エンドポイントは、プライマリ ホスト、セカンダリ ホスト、および要求で指定されたクライアント プロファイルに関連付けられているホスト選択プロファイルからのレルムを決定します。
3. ホスト選択プロファイルには、必須のプライマリとオプションのセカンダリ ホストレルムのペアがあります。レルムはオプションの CLI ですが、デフォルト値に設定されます。
4. ホストとレルムは、考えられる一致する複数のルートを見つけるためのルート検索アルゴリズムへの入力として機能します。順序は 、ステータス、 フラグ、および重みによって異なります。
5. ホスト選択プロファイルの構成がない場合、ピア管理モジュールはルート テーブル内のすべてのアクティブ ルートを選択してソートします。

（注） ルートの選択は、プライマリ ホストまたはセカンダリ ホストの順序付きルート リストからのラウンド ロビン方式で行われます。この方法により、プライマリ ホストのすべてのルートを試行してから、セカンダリ ホストのすべてのルートを試行する必要がなくなります。

## ルートソート順序

Diameter ピアのエントリのルート ソート 順序は次のとおりです。

- アクティブ ステータスを持つルートが最も優先されます。
- 同じステータスを持つルートの中で、バインドされたピアと一致するルートがある場合、そのルートが最も優先されます。次に、ダイナミック ルート、続いてパスキャッシュ ルートが優先されます。
- ピアは、重みに基づいて同じフラグの複数のルートを自分自身の間に配置します。この場合、より高い値が優先されます。
- 重みは、ホストとレルムエントリが完全に一致するルートよりも常に優先されます。
- 完全一致エントリは、同じ重みを持つ 2 つのルートがある場合にのみ優先されます。

# ホスト選択

このセクションでは、ホストの選択、その実装、およびDiameterエンドポイントでのホスト選択の構成例について説明します。

## 機能説明

Diameterエンドポイントは、個々のプロファイル名のデータを、アルゴリズム、およびプライマリとセカンダリのホストの詳細のリストとともに保持します。ローカルデータ構造では、インデックス付き形式で最大 64 のホストの詳細を保持できます。ホストの詳細には、プライマリ ホスト レルムとセカンダリ ホスト レルムが含まれます。

## 機能の仕組み

ピア管理モジュールは、プロファイル名、電話番号、および IPv4 アドレスとともに要求をホスト選択モジュールに送信します。ホスト選択モジュールは、構成マップから取り込まれたローカルデータ構造のプロファイル名を確認します。プロファイル名が一致すると、次のアルゴリズムを使用してホストの詳細が取得されます。

- 電話番号モジュール：電話番号は数値に変換されます。次に、MSIDN mod ホスト エントリの利用可能な数によってインデックスが計算されます。
- IP アドレス モジュール：IP アドレスは数値に変換されます。インデックスは、数字 IP アドレス値 mod host エントリの利用可能な数によって計算されます。

- ラウンドロビン：デフォルトのアルゴリズムは、プロファイル名ごとの使用可能なエントリのラウンドロビンです。

（注） ホスト選択プロファイルは、Diameter クライアントとバインドされます。複数の Diameter クライアントに対して 1 つのホスト選択プロファイルをバインドできます。

## Diameter エンドポイントによるホスト選択の構成

Diameter ホスト選択の構成は、Diameter プロファイルで使用できます。複数の Diameter ホストを構成し、これらのホストを別の Diameter クライアントにバインドできます。

ホスト選択で Diameter エンドポイントを構成するには、次の構成例を使用します：

```
config
  profile diameter-host-selection host_selection_name
     algorithm algorithm-name
     hosts hosts_number
        primary host host_ip_address
        primary realm realm_name
        secondary host host_ip_address
        secondary realm realm_name
     end
```

注：

- **profile diameter-host-selection** *host_selection_name*：Diameter ホスト選択プロファイル名を指定します。
- **algorithm***algorithm-name*：ホストを選択するアルゴリズムを選択します。 *algorithm-name* には **ipaddr-modulus**、 **msisdn-modulus**、 **round-robin** の値があります。
- **hosts** *hosts_number*：ホストの優先順位を 1 ～ 64 のインデックス形式で指定します。
- **primary host** *host_ip_address*：プライマリ ホスト名を指定します。
- **primary realm** *realm_name*：プライマリ ホスト レルムを指定します。
- **secondary host** *host_ip_address*：セカンダリ ホスト名を指定します。
- **secondary realm** *realm_name*：セカンダリ ホスト レルムを指定します。

### 設定例

次に、ホスト選択の構成例を示します。

```
profile diameter-host-selection hs1
 algorithm ipaddr-modulus
 hosts 1
  primary host 209.165.200.239
  primary realm cisco.com
  secondary host g192.168.2.1
  secondary realm google.com
```

```
 exit
 hosts 2
  primary host 209.165.200.240
  primary realm facebook.com
  secondary host 209.165.200.241
  secondary realm conflunt.com
 exit
exit

profile diameter-client dc1
 endpoint       gxProf1
 host-selection hs1
exit
profile diameter-client dc2
 endpoint       gyProf1
 host-selection hs1
exit
```

# ルート障害

## 機能説明

ルート機能不全カウンタはゼロから始まります。このカウンタは、次のシナリオで増加します：

- そのルートを使用してトランザクションが試行されたとき。
- 設定された機能不全の結果コードと一致する結果コードを含む応答を受信した場合。

カウントは、成功応答を受信するたびに減少します。機能不全の数がしきい値を超えると、そのルートは機能不全とマークされます。機能不全が発生したルートを使用できるようにするために、定期的に、ルートの機能不全の数が回復しきい値分だけ減らされます。

## ルート障害の構成

ルート障害を構成するには、次の構成例を使用します：

```
config
  profile diameter-endpoint interface_name
     name profile_name
     internal-vip ip_address
        route-failure deadtime deadtime_valueresult-code result_code_value
threshold  number
        route-failure result-code result_codes_value
        route-failure threshold  threshold_number
       route-failure recovery-threshold percent  recovery_threshold_percentage
exit
```

注：

- **route-failure deadtime** *deadtime_value***result-code** *result_code_value* **threshold** *number*：システムがルートを **FAILED** ステータスに保持する期間を秒単位で指定します。構成された期間が経過すると、システムはステータスを **AVAILABLE**に変更します。 *deadtime_value* は、1 ～ 86400 の範囲の整数である必要があります。デフォルト値は 60 です。

- **route-failure result-code** *result_codes_value*：タイムアウトする要求に加えて、失敗と見なされる応答メッセージを指定します。

（注） 最大 16 の結果コードを指定できます。

- **route-failure threshold** *threshold_number*： **FAILED** ステータスになる原因となるエラーの数を指定します。デフォルト値は 16 です。

（注） エラー カウンタはゼロから始まります。応答が良好な場合、エラーカウンタは減少または増加します。このカウンタは、構成されたしきい値よりもゼロ未満に減少することも、増加することもありません。

- **route-failure recovery-threshold percent** *recovery_threshold_percentage*：ステータスを **FAILED** から **AVAILABLE**に一時的に変更するときに、エラー カウンタがリセットされる割合の値を指定します。たとえば、エラー カウンタが 16 の場合、 **AVAILABLE** ステータスは **FAILED** ステータスに変わりました。構成されたデッドタイムが経過すると、ステータスが **AVAILABLE**に変わります。 *recovery_threshold_percentage* が 75% に構成されている場合、失敗カウンタは 12 にリセットされ、これは 16 の 75% です。デフォルトは 90 です。

## 設定例

ルート障害の構成例を次に示します。

```
profile diameter-endpoint gydc01
   name gyProf1
   internal-vip ip_address
      route-failure deadtime  600
      recovery-threshold 16
      percent 90
      result-code rc1
exit
```

## 設定の確認

Gx または Gy インターフェイスの Diameter エンドポイントが構成されているかどうかを確認するには、次の **show running-config profile diameter-endpoint** コマンドを使用します。

```
[smf] smf# show running-config profile diameter-endpoint
 profile diameter-endpoint gx
 internal-vip 209.165.200.234
 name gxProf1
   internal-vip ip_address
      route-failure deadtime 600
      recovery-threshold 16
      percent 90
      result-code rc1
exit
```

# バインドされたピア

## 機能説明

最後のクレジット制御要求 - 初期（CCR-I）またはクレジット制御要求 - 更新（CCR-U）のインターバルが発生したピアは、バインドされたピアと見なされます。現在の要求処理に基づいて、Diameter エンドポイントは、プライマリ ホストまたはセカンダリ ホストのサービスとバインドされたピアと通信します。その後、サービスは、プライマリホストまたはセカンダリホストのDiameterエンドポイントと、要求処理に使用されるバインドされたピアと通信します。

バインドされたピアのルートの一致は、後続の CCR-U またはクレジット制御要求 - 終了（CCR-T）メッセージを送信するために最も優先されます。ホストのルートリストにアクティブなエントリが存在し、そのピアがバウンドされたピアと一致する場合、そのルートエントリは要求処理において最も高い優先順位を付与されます。

## 機能の仕組み

ここでは、バインドされたピアの仕組みを説明します。

- プライマリ ホストとセカンダリホスト、およびバインドされたピアに関する詳細は、サービスからの要求に含まれています。同様に、これらの詳細は、サービスへの応答に含まれています。
- ホストのルート リストにダイナミック ルート エントリのみがある場合は、ルートに関連付けられているピアのスタティックまたはパッチキャッシュ ルート エントリがリストに追加されます。
- ホストのルートリストに1つ以上のアクティブエントリがあり、ピアがバインドされたピアと一致する場合、要求の処理ではルートエントリが優先されます。
- RAR の場合、diameter-ep はホスト、レルム、およびプライマリのバインドされたピアを埋めます。サービスは、セカンダリ ホスト/レルム/バインドされたピアの情報が失われないように、詳細を既存のルーティング データとマージします。

# 失敗のハンドリング（Failure Handling）

## 機能説明

障害処理は、Diameter メッセージと障害の障害処理プロファイルを構成することで管理されます。この構成により、障害シナリオでのDiameterポッドの動作が決まります。任意の数の障害処理プロファイルを構成できます。

障害処理プロファイルを構成したら、特定の Diameter クライアント プロファイルに関連付けます。構成済みの障害処理プロファイルを Diameter クライアント プロファイルに関連付けない場合、デフォルトの障害プロファイルが考慮されます。

# 機能の仕組み

障害処理は次のように機能します：

- 障害が発生した場合、Diameterエンドポイントは該当する障害処理プロファイルを取得します。
- 障害処理プロファイルが定義されていない場合、または失敗した要求と一致する必要があるメッセージおよび障害タイプが定義されていない場合、デフォルトの障害処理が適用されます。デフォルトの障害処理では、 **action terminate** を使用した再試行は行われず、サブアクションは *with-term-req*となります。これは終了要求がないことを意味します。
- Diameterエンドポイントは、要求が成功するか、該当する障害処理プロファイルで指定されている構成された再試行回数に達するまで、代替ピアまたはルートを使用して要求を再試行します。
- ルートは、各ホストの順序付きルート リストからラウンド ロビン方式で選択されます。たとえば、host1 のルートの障害では、host2 のルートのリスト内の次のルートが再試行に使用されます。再試行中に、いずれかのホストのルートリストが使い果たされると、他のホストの残りのルートが再試行に使用されます。
- CCR-U/T の DRA と対話するときに、プライマリのルート リストにダイナミック ルートがない場合、セカンダリがメッセージを送信するために最初に考慮されます。
- 再試行中に、すでに試行されたルートが見つかった場合、そのルートはスキップされます。
- 適用可能なピアまたはルートの数が再試行回数よりも少ない場合、残りの再試行は、適用可能なすべてのピアまたはルートが試行された後に破棄されます。
- 要求が送信された後の最初の失敗時に決定される再試行回数が使用されます。再試行中に障害が発生し、その障害が別の再試行回数を持つ別の障害処理プロファイルに対応する場合、Diameter エンドポイントも、最初の障害時に決定された再試行回数を続行します。
- 再試行カウントは、少なくとも 1 つの要求が送信された後にのみ開始されます。再試行回数の前に障害が発生しました。
- すべての再試行またはすべてのピアまたはルーティングの再試行の後でも、要求が成功しなかった場合、Diameterエンドポイントは、サービスへの応答の一部としてアクションとサブアクションを送信します。
- 最新の失敗に適用可能なアクションとサブアクションが応答で使用されます。
- これらのアクションまたはサブアクションのアクションは次のようにサービス側で実行されるため、Diameter エンドポイントでは追加の処理は行われません。

  **アクション（Action）**

  - **continue**：セッションの続行
  - **terminate**：セッションを終了します。このアクションはデフォルトのアクションになります。

サブアクション

- **discard-traffic**：データ トラフィックをブロックまたは破棄します。このサブアクションは **continue** 、のアクションに関連付けられています。 Gy インターフェイスにのみ適用可能です。
- **local-fallback**：ローカル ポリシーを適用します。このサブアクションは **continue** 、アクションに関連付けられます。
- **none**：アクションは必要ありません。このサブアクションは **continue** のアクションに関連付けられており、Gy インターフェイスにのみ適用されます。 **none** は、 **continue** アクションの Gy コールのデフォルト オプションです。
- **retry-server-on-event**：クレジット制御更新要求時にサーバに再接続します。このサブアクションは、 **continue** アクションに関連付けられており、Gx インターフェイスにのみ適用されます。
- **send-ccrt-on-call-termination**：クレジット制御更新要求の失敗に関して、CCR-T 要求を PCRF に送信します。このサブアクションは、 **continue** アクションに関連付けられており、Gx インターフェイスにのみ適用されます。 **send-ccrt-on-call-termination** は、 **continue** アクションの Gx コールのデフォルトオプションです。
- **with-term-req**：終了要求（CCR-T）を送信してセッションを終了します。このサブアクションは、 **terminate** アクションに関連付けられており、Gx インターフェイスにのみ適用されます。 **with-term-req** は、**terminate** アクションの Gx コールのデフォルト オプションです。

# 障害処理の構成

障害処理の構成には、次の手順が含まれます。

1. 障害処理プロファイルの構成 （141 ページ）
2. 障害処理プロファイルを構成したら、特定の Diameter クライアント プロファイルに関連付けます。Diameter クライアント プロファイルを構成するには、 Diameter クライアント プロファイルの構成 （118 ページ） の手順を参照してください。

## 障害処理プロファイルの構成

SCP 障害処理プロファイルを構成するには、次の構成例を使用します：

```
config
  profile failure-handling failure_handling_profile_name
     interface diameter
      message [ any | credit-control-initial | credit-control-terminate
 | credit-control-update ]
          failure-type [ any | local-error | result-code {result-code-value
 | result-code-range-start-value | result-code-range-end-value |
comma-separated-result-code-value-or-range  } | experimental-result-code
```

```
experimental-result-code-value | experimental-result-code-start-value
| experimental-result-code-end-value |
comma-separated-experimental-result-code-value-or-range
}experimental-result-code-value | experimental-result-code-start-value |
experimental-result-code-end-value |
comma-separated-experimental-result-code-value-or-range ]
            retry count
            action [ continue discard-traffic | local-fallback |
retry-server-on-event | send-ccrt-on-call-termination | terminate with-term-request
| without-term-request ]
  exit
```

注：

- **profile failure-handling** *failure-handling_profile_name* ：障害処理プロファイル名を指定します。
- **interface diameter**：Diameter インターフェイスの障害処理プロファイルを指定します。
- **message [ any | credit-control-initial | credit-control-terminate | credit-control-update ]**：使用可能なオプションからメッセージ値を選択します。これは必須パラメータです。
- **failure-type [ any | local-error | result-code {***result-code-value* | *result-code-range-start-value* | *result-code-range-end-value* | *comma-separated-result-code-value-or-range* | **experimental-result-code experimental-result-code-value | experimental-result-code-start-value | experimental-result-code-end-value | comma-separated-experimental-result-code-value-or-range }***experimental-result-code-value* | *experimental-result-code-start-value* | *experimental-result-code-end-value* | *comma-separated-experimental-result-code-value-or-range* **]**: ：アクションを実行する必要がある Diameter の障害タイプを指定します。使用可能なオプションから障害タイプの値を選択します。これは必須パラメータです。

（注） 複数の障害タイプを構成できます。

- **retry** *count*：障害応答の受信時に再試行する代替ピア またはルート の数を指定します。デフォルト値は 0 です。
- **action [ continue** *discard-traffic* | *local-fallback* | *retry-server-on-event* | *send-ccrt-on-call-termination* **| terminate** *with-term-request* | *without-term-request* **]**：**continue** または **terminate** としてアクション値を選択します。必要に応じて、使用可能なオプションから選択したアクションのサブアクションを選択します。

（注） **continue** アクションまたは **terminate** アクションのサブアクションをクリアしたり、デフォルトにリセットしたりするには、構成を保存する前に次のステップを実行します。

1. **no profile failure-handling** *failure-handling-profile-name*
   **interface diameter message***diameter-message*
   **failure-type***failure_name* **result-code** *result_code*
   **action***action_name sub_action*
   **exit**
2. **profile failure-handling** *failure-handling-profile-name*
   **interface diameter message***diameter_message*
   **failure-type***failure_name* **result-code** *result_code*
   **action***action_name*
   **exit**

## 設定例

次に、SCP 障害処理プロファイルの構成例を示します：

```
profile failure-handling fh1
  interface diameter
    message credit-control-initial
      failure-type any
        retry 2
        action terminate with-term-req
      exit
      failure-type local-error
        retry 3
        action continue local-fallback
      exit
      failure-type result-code 3000
        retry 2
        action continue discard-traffic
       exit
      exit
      failure-type result-code 4000
        action continue retry-server-on-event
       exit
      exit
      failure-type result-code 4001-4010
        action continue send-ccrt-on-call-termination
       exit
      exit
      failure-type result-code 4011-4020,4025,4030-4040
        action terminate without-term-req
       exit
      exit
      failure-type exp-result-code 5000
        action terminate with-term-req
       exit
```

```
      exit
      failure-type exp-result-code 5010-5015
        action terminate
       exit
      exit
    exit

    message credit-control-terminate
      failure-type any
        retry 2
        action terminate
      failure-type local-error
        action continue retry-server-on-event
      exit
    exit

    message credit-control-update
      failure-type any
        action continue send-ccrt-on-call-termination
      exit
      failure-type local-error
        action continue discard-traffic
      exit
    exit

    message any
      failure-type any
        action continue discard-traffic
      exit
      failure-type local-error
        action continue
      exit
    exit
  exit
exit

profile failure-handling fh2
  interface diameter
    message credit-control-update
      failure-type any
        retry 2
        action continue
      exit
      failure-type local-error
        action terminate without-term-req
      exit
    exit
  exit
exit
```

## 設定の確認

UDM メッセージ処理プロファイルが構成されているかどうかを確認するには、次の **show running-config profile diameter-client** コマンドを使用します：

```
show running-config profile diameter-client
   profile diameter-client dc2
    endpoint gyProf1
       failure-handling-profile FH1
exit
```

# OAM サポート

## バルク統計サポート

SMF は、Diameter エンドポイントの一部として次のメトリックを維持します。

**diameter_request_message_total**

説明：Diameter エンドポイントによって処理された Diameter 要求の数を示します。

（注）
- インバウンド要求の peer_address カウンタは空であり、障害ポイントによっては、アウトバウンド要求のこのカウンタが空の場合があります。
- 再試行カウンタは、IPC タイムアウトの再試行カウンタとして常にゼロとして記録されます。
- transaction_type カウンタは「origin」にハードコードされています。
- endpoint_nameカウンタはインバウンド要求に対して空であり、障害ポイントによっては、アウトバウンド要求に対して空になる場合があります。

メトリック タイプ：カウンタ

デフォルトのレベル：MetricsVerboseLevelProduction

ラベルの詳細：

- **インターフェイス**：gx、gy
- **message_name**：ccri、ccru、ccrt、rar、asr peer_address
- **status**：attempted、peer_down、err_cfg、err_maxout、timeout_ipc、err_ipc、err_unmarshal
- **retry**：retry count gr_instance transcation_type
- **endpoint_name**： 処理中に使用されるエンドポイント プロファイルの名前
- **message_direction**：inbound、outbound

ラベル製品：

- インターフェイス
- message_name
- peer_address status

ラベル デバッグ：

- retry
- gr_instance
- transaction_type

ラベル トレース：

- endpoint_name
- message_direction

**diameter_response_message_total**

説明：Diameter エンドポイントが処理する Diameter 応答の数を示します。

（注）
- インバウンド要求の peer_address カウンタは空であり、障害ポイントによっては、アウトバウンド要求のこのカウンタが空の場合があります。
- result_code カウンタでは、アウトバウンド応答、ローカル障害、応答タイムアウト、および IPC タイムアウトが「」として記録されます。
- アクションまたはサブアクションカウンタは、アウトバウンド応答と「success」応答の場合は空です。
- endpoint_name カウンタはインバウンド要求に対して空であり、障害ポイントによっては、アウトバウンド要求に対して空になる場合があります。

メトリック タイプ：カウンタ

デフォルトのレベル：MetricsVerboseLevelProduction

ラベルの詳細：

- **インターフェイス**：gx、gy
- **message_name**：ccai, ccau, ccat, raa, asa
- **peer_address**
- **status**：success, err_cfg、err_maxout、err_send、timeout_res、timeout_ipc、 err_ipc、err_unmarshal、err_rc、err_exp_rc
- **result_code**：Diameter ノードが応答処理中に検出した result-code または experimental-result-code
- **action**：continue、terminate
- **サブアクション**：discard-traffic、local-fallback、retry-server-on-event、send-ccrt-on-call-termination、with-term-req、without-term-req
- **endpoint_name**：処理中に使用されるエンドポイント プロファイルの名前

- **gr_instance**
- **message_direction**：inbound、outbound

ラベル製品：

- インターフェイス
- message_name
- peer_address status
- status
- result_code

ラベル デバッグ：

- action
- subaction
- gr_instance

ラベル トレース：

- endpoint_name
- message_direction

#### diameter_response_message_seconds_tot

説明：Diameterエンドポイントが処理するDiameter要求の累積応答時間を秒単位で示します。

（注）
- インバウンド要求の peer_address カウンタは空であり、障害ポイントによっては、アウトバウンド要求のこのカウンタが空の場合があります。
- result_code カウンタでは、アウトバウンド応答、ローカル障害、応答タイムアウト、および IPC タイムアウトが「」として記録されます。
- アクションまたはサブアクションカウンタは、アウトバウンド応答と「success」応答の場合は空です。
- endpoint_nameカウンタはインバウンド要求に対して空であり、障害ポイントによっては、アウトバウンド要求に対して空になる場合があります。
- このカウンタは、ローカル障害または IPC タイムアウトでは増分されません。

デフォルトのレベル：MetricsVerboseLevelProduction

ラベルの詳細：

- **インターフェイス**：gx、gy

- **message_name**：ccai, ccau, ccat, raa, asa
- **peer_address**
- **status**：success, err_cfg、err_maxout、err_send、timeout_res、timeout_ipc、 err_ipc、err_unmarshal、err_rc、err_exp_rc
- **result_code**：Diameter ノードが応答処理中に検出した result-code または experimental-result-code
- **action**：continue、terminate
- **サブアクション**：discard-traffic、local-fallback、retry-server-on-event、send-ccrt-on-call-termination、with-term-req、without-term-req
- **gr_instance**
- **endpoint_name**：処理中に使用されるエンドポイント プロファイルの名前
- **message_direction**：inbound、outbound

ラベル製品：

- message_name
- origin_host
- origin_realm
- disconnect_cause
- result_code

ラベル デバッグ：

- action
- subaction
- gr_instance

ラベル トレース：

- endpoint_name
- message_direction

#### diam_base_msg_total

説明：Diameterエンドポイントが処理するDiameterベースのメッセージ要求の数を示します。

（注）
- DPR カウンタは、ピアから受信した DPR でのみサポートされます。
- 受信した DPR に必須の AVP がない場合、または DPR の origin-host と origin-realm が接続の詳細の destination-host および destination-realm と一致しない場合、result_code カウンタは 5012 としてログに記録されます。

メトリック タイプ：カウンタ

デフォルトのレベル：MetricsVerboseLevelProduction

ラベルの詳細：

- **message_name**：DPR
- **origin_host**
- **origin_realm**
- **disconnect_cause**：REBOOTING、BUSY、DO_NOT_WANT_TO_TALK_TO_YOU
- **result_code**：2001、5012
- **gr_instance**

ラベル製品：

- message_name
- origin_host
- origin_realm
- disconnect_cause
- result_code

ラベル デバッグ：

- gr_instance

ラベル トレース：

- endpoint_name
- message_direction

#### diam_base_msg_seconds_tottal

説明：Diameterエンドポイントが処理するDiameterベースのメッセージ要求の累積応答時間を秒単位で示します。

（注）
- DPR カウンタは、ピアから受信した DPR でのみサポートされます。
- 受信した DPR に必須の AVP がない場合、または DPR の origin-host と origin-realm が接続の詳細の destination-host および destination-realm と一致しない場合、result_code カウンタは 5012 としてログに記録されます。

デフォルトのレベル：MetricsVerboseLevelProduction

ラベルの詳細：

- **message_name**：DPR
- **origin_host**
- **origin_realm**
- **disconnect_cause**：REBOOTING、BUSY、DO_NOT_WANT_TO_TALK_TO_YOU
- **result_code**：2001、5012
- **gr_instance**

ラベル製品：

- インターフェイス
- message_name
- diameter_dictionary_type
- status
- unknown_avp

ラベル デバッグ：

- gr_instance

**diameter_encode_message_tottal**

説明：Diameterエンドポイントが処理するDiameterベースのメッセージ要求の数を示します。

（注）
- DPR カウンタは、ピアから受信した DPR でのみサポートされます。
- 受信した DPR に必須の AVP がない場合、または DPR の origin-host と origin-realm が接続の詳細の destination-host および destination-realm と一致しない場合、result_code カウンタは 5012 としてログに記録されます。

メトリック タイプ：カウンタ

デフォルトのレベル：MetricsVerboseLevelProduction

ラベルの詳細：

- **インターフェイス**：gx、gy、「」
- **message_name**：ccri、ccru、ccrt、raa、asa
- **endpoint_name**：処理中に使用されるエンドポイント プロファイルの名前
- **dict_name**
- **status**：success、failure、partial
- **unknown_avp**：0、1
- **gr_instance**

ラベル製品：

- インターフェイス
- message_name
- diameter_dictionary_type
- status
- unknown_avp

ラベル デバッグ：

- status_code
- gr_instance

#### diameter_decode_message_total

説明：Diameter エンドポイントが実行したデコードの数を示します。

（注）
- サポートされていないインターフェイスまたはコマンドコードに対して、インターフェイスが空になっています。
- サポートされていないインターフェイスまたはコマンド コードの message_name カウンタが空です
- デフォルトのディクショナリが使用されている場合、dict_name カウンタは空です。それ以外の場合、このカウンタは、操作に使用されるディクショナリの名前を示します。
- ステータス カウンタは、サポートされていないインターフェイスまたはコマンド コードについてのみ失敗として記録されます。エンコーディング中に発生した問題が無視された場合、このカウンタは Partial としてログに記録されます。たとえば、不明な AVP などです。
- unknown_avp カウンタは、エンコード中に不明な AVP が検出されたかどうかを示します。ゼロは検出されないことを示し、1 は検出されたことを示します。

メトリック タイプ：カウンタ

デフォルトのレベル：MetricsVerboseLevelProduction

ラベルの詳細：

- **インターフェイス**：gx、gy、「」
- **message_name**：ccai、ccau、ccat、rar、asr
- **endpoint_name**：処理中に使用されるエンドポイント プロファイルの名前
- **dict_name**
- **status**：success、failure、partial
- **unknown_avp**：0、1
- **gr_instance**

ラベル製品：

- インターフェイス
- message_name
- diameter_dictionary_type
- status
- unknown_avp

ラベル デバッグ：

- status_code

- result_code
- gr_instance

ラベル トレース：

- endpoint_name

#### diameter_pod_status

[説明（Description）]：ポッドのステータスをアクティブまたはスタンバイとして示します。

（注）
- 値 1 はアクティブのステータスを示し、ゼロはスタンバイのステータスを示します。
- Diameter ポッドがサーバ モードで実行されている場合、ポッド ステータスの判断に VIP カウンタは使用されません。この場合、VIP はサーバ モードでは空です。

メトリック タイプ：ゲージ（Gauge）

デフォルトのレベル：MetricsVerboseLevelProduction

ラベルの詳細：

- **vip**: ポッド ステータスの決定に使用される VIP

ラベル製品：

- vip

ラベル デバッグ：

- gr_instance

ラベル トレース：

- endpoint_name

#### dispatch_error_tottal

説明：サービスへのディスパッチ中にエラーまたはタイムアウトが発生したインバウンド要求の数を示します。

メトリック タイプ：カウンタ

デフォルトのレベル：MetricsVerboseLevelProduction

ラベルの詳細：

- **application**
- **command_code**
- **error_code**

- **gr_instance**

ラベル製品：

- アプリケーション
- command_code
- error_code

ラベル デバッグ：

- gr_instance

#### dispatch_error_seconds_tottal

説明：エラーまたはタイムアウトが発生した、サービスへの着信要求のディスパッチ中に費やされた累積時間を秒単位で示します。

デフォルトのレベル：MetricsVerboseLevelProduction

ラベルの詳細：

- **application**
- **command_code**
- **error_code**
- **gr_instance**

ラベル製品：

- アプリケーション
- command_code
- error_code

ラベル デバッグ：

- gr_instance

#### policy_engine_message_total

説明：応答を受信したサービスに送信されたメッセージの数を示します。

メトリック タイプ：カウンタ

デフォルトのレベル：MetricsVerboseLevelProduction

ラベルの詳細：

- **application**
- **command_code**
- **gr_instance**

ラベル製品：

- アプリケーション
- command_code

ラベル デバッグ：

- gr_instance

**policy_engine_message_seconds_total**

説明：サービスに送信されたメッセージの処理中に費やされた累積時間を秒単位で示します。

デフォルトのレベル：MetricsVerboseLevelProduction

ラベルの詳細：

- **application**
- **command_code**
- **gr_instance**

ラベル製品：

- アプリケーション
- command_code

ラベル デバッグ：

- gr_instance

# トラブルシューティング情報

## プロトコルをモニタし、サブスクライバをモニタする

### 機能説明

SMF は、Diameter メッセージの [モニタ プロトコル（Monitor Protocol）] および [モニタ サブスクライバ（Monitor Subscriber）] 機能の SUPI および IMSI サブスクライバ キーをサポートします。[モニタ プロトコル（Monitor Protocol）] を使用して、インターフェイス タイプを Diameter として追加します。

#### モニタ サブスクライバ

CLI コマンドを使用して、特定のサブスクライバまたはサブスクライバのセットのメッセージを表示できます。インターワーキングでは、NF サービスを SMF として使用します。

### モニタープロトコル

Diameter インターフェイスの場合、SMF はパケットにモニタ プロトコルを使用します。

（注） Diameter クライアントの場合、少なくとも 1 つのピアをリーダー ポッドに接続するまで、モニタ プロトコルは機能しません。

## 機能の仕組み

Ops センターの CLI コマンドを使用して、[モニタ サブスクライバ（Monitor Subscriber）] および [モニタ プロトコル（Monitor Protocol）] 機能を構成できます。

## モニタ サブスクライバおよびモニタ プロトコル サポートの構成

このセクションでは、[モニタ サブスクライバ（Monitor Subscriber）] および [モニタ プロトコル（Monitor Protocol）] サポートを構成する方法について説明します。

### サブスクライバ セッションのモニタリング

SMF でサブスクライバをモニターするには、次の CLI コマンドを使用します：

**monitor subscriber [ capture-duration** *duration* **| dump filename** *file_name* **| gr-instance** *gr_instance_id* **| imei** *imei_id* **| imsi** *imsi_value* **| internal-messages [ yes ] | list** *file_list* **| nf-service [ sgw | smf ] | supi** *supi_id* **| transaction-logs [ yes | no ] ]**

注：

- **capture-duration** *duration*：モニタ サブスクライバを有効にする期間を秒単位で指定します。デフォルトは 300 秒（5 分）です。これは省略可能なパラメータです。
- **dump filename** *file_name*：SMF Ops Center で並べ替えられたファイルを表示するファイル名を指定します。
- **gr-instance** *gr_instance_id*：GR インスタンス ID を指定します。インスタンス ID 1 はローカル インスタンス ID を示しています。
- **imei** *imi_id*：サブスクライバ IMEI を指定します。例：123456789012345、*
- **imsi** *imsi_value*：サブスクライバ IMSI を指定します。たとえば、123456789、* などです。
- **internal-messages [ yes | no ]**：内部メッセージの表示を有効または無効にします。デフォルトでは、**yes** オプションは無効になっています。これは省略可能なパラメータです。
- **nf-service [ sgw | smf ]**：指定した NF サービスを有効にします。デフォルトでは、**nf-service** は none に設定されています。

重要 **nf-service** キーワードは、リリース 2021.02 以降では **namespace** キーワードに置き換わります。

- **supi** *supi_id*：サブスクライバ ID を指定します。例：imsi-123456789、imsi-123*
- **transaction-logs [ yes | no ]**：**yes** に設定されている場合はトランザクション ログを有効にします。デフォルトでは、このパラメータは無効になっています。これは省略可能なパラメータです。

  トランザクション履歴ログを表示するには、**dump transactionhistory** コマンドを使用します。

（注） 最新のトランザクション ログは、トランザクション ログ サイズが 1024 の循環キューに保存されます。

### Diameter インターフェイス プロトコルのモニタリング

SMF で Diameter インターフェイス プロトコルをモニタするには、次の CLI コマンドを使用します：

**monitor protocol interface diameter [ capture-duration** *duration* **| gr-instance** *gr_instance_id* **| pcap yes gr-instance** *gr_instance_id* **]**

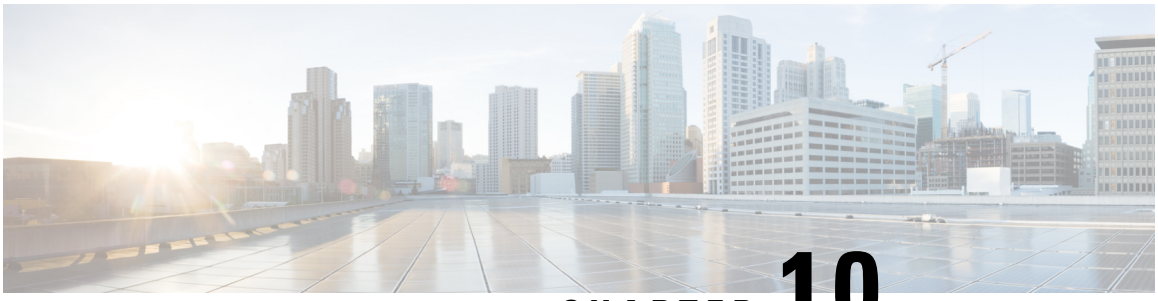
注：

- **interface diameter** ：インターフェイス名を Diameter に指定します。
- **capture-duration** *duration*：pcap がキャプチャされる期間を秒単位で指定します。デフォルトは 300 秒（5 分）です。
- **gr-instance** *gr_instance_id*：GR インスタンス ID を指定します。インスタンス ID 1 はローカル インスタンス ID を示しています。
- **pcap yes gr-instance** *gr_instance_id*：このオプションを構成すると、PCAP ファイルの生成が有効になります。デフォルトでは、このオプションは無効になっています。

# データ収集のデバッグ

Diameter の問題をデバッグする際に、Ops センターを介して次のコマンドの出力を使用します。

- **kubectl get pods -n** 名前空間
- **kubectl get statefulsets -n** 名前空間
- **kubectl get cm -n** 名前空間
- **kubectl get service -n** 名前空間
- **helm list**
- **show full-configuration** または **show running-configuration**



CHAPTER 10

# DSCP マーキング


- 機能の概要と変更履歴, on page 159
- 機能説明, on page 160
- データパケットの DSCP マーキング （160 ページ）
- コントロール プレーン シグナリングの DSCP マーキング （163 ページ）


## 機能の概要と変更履歴

### 要約データ

| | |
|---|---|
| 該当製品または機能エリア | SMF |
| 該当プラットフォーム | SMI |
| 機能のデフォルト設定 | 無効：設定が必要 |
| このリリースでの関連する変更点 | N/A |
| 関連資料 | 該当なし |

### 更新履歴

| 改訂の詳細 | リリース |
|---|---|
| コントロールプレーンシグナリングメッセージの DSCP マーキングのサポートを提供 | 2021.01.0 |
| 最初の導入。 | 2020.02.0 より前 |

# 機能説明

SMF では、ユーザープレーンデータ パケットおよびコントロールプレーン シグナリング メッセージの DiffServ コードポイント（DSCP）マーキングのメカニズムがサポートされています。

DSCP マーキング機能により、SMF はトラフィックの分類と優先順位付けを実行して、適切な Quality of Service（QoS）処理を提供できます。DSCP は DiffServ フィールドの有効ビットです。

この機能は、CLI コマンドを使用して、シグナリング メッセージとデータ パケットの両方の DSCP パラメータを構成します。構成の詳細に関しては、本章の 5QI-QoS マッピングの構成, on page 161 および コントロール プレーン シグナリングの DSCP マーキングの構成, on page 164 を参照してください。

**Note** この機能は、レガシー インターフェイスを使用する 4G コールに適用されます。

# データパケットの DSCP マーキング

## 機能説明

DSCP マーキングでは、詳細な構成がサポートされます。インタラクティブ トラフィック クラス（ITC）の場合、SMF では、5QI および ARP 優先順位レベルに基づくアップリンクおよびダウンリンク方向の APN ごとの構成可能な DSCP マーキングがサポートされます。このサポートにより、ユーザーは同じ 5QI で ARP 優先度の値が異なるフローに異なる DSCP の値を割り当てることができます。たとえば、5QI + ARP に基づく DSCP 値を割り当てる機能を使用して、VoLTE を介した優先コールと緊急コールのコンプライアンスを満たすことができます。

DSCP マーキングは CLI 制御の機能であり、5QI および ARP 値を作成および適用可能な QoS パラメータにマッピングできます。

SMF は構成された DSCP 値を UPF に送信します。次に、UPF は、5QI と ARP に基づいて、アップリンクとダウンリンクのパケットに DSCP マーキングを適用します。

## データ パケットの DSCP マーキングの動作方法

このセクションでは、データ パケットに対して DSCP マーキングを実行する方法について説明します。

同じ 5QI で ARP 値が異なるフローに対する異なる DSCP 値の割り当ては、次のように機能します。

- 5QI と ARP の組み合わせに基づいてパケットの DSCP マーキングを使用できます。

- 5QI と ARP の構成は、5QI と ARP の組み合わせに基づいていたパケットの DSCP マーキングのプレエントリを上書きします。
- 5QI のみの DSCP エントリは、既存のすべての 5QI および ARP 構成を上書きします。
- アップリンクとダウンリンク トラフィックに対する 5QI および ARP に関連する DSCP マーキングの実装を可能にします。

# 5QI-QoS マッピングの構成

5QI 値を作成し、適用可能な QoS パラメータにマッピングするには、次のサンプル構成を使用します。

```
config
   profile qos qos_profile_name
      dscp-map qi5 qos_id
      arp-priority-level arp_value uplink user-datagram dscp-marking
dscp_marking_value
      arp-priority-level arp_value downlink { encsp-header { copy-inner
| dscp-marking dscp_marking_value } | user-datagram dscp-marking
dscp_marking_value } }
      commit
```

注：

- **dscp-map qi5** *qos_id*：承認された QoS パラメータの ID を指定します。 *qos_id* は、1 ～ 255 の範囲の整数である必要があります。

**Note** DSCP 設定が QoS フロー レベルで使用できず、QoS プロファイル レベルで使用できる場合、DSCP 構成は QoS プロファイルレベルから使用されます。

- **arp-priority-level** *arp_value* **uplink user-datagram dscp-marking** *dscp_marking_value*：ARP 優先度レベルを構成し、次にアップリンク方向の内部 IP ヘッダーに DSCP 値を設定します。この DSCP 値は、5QI 値が構成されているパケットに適用されます。

  *arp_value* は 1ー255 の範囲の整数である必要がありま。

  *dscp_marking_value* は、0x00 から 0x3F までの 16 進数である必要があります。

- **arp-priority-level** *arp_value* **downlink { encsp-header { copy-inner | dscp-marking** *dscp_marking_value* **} | user-datagram dscp-marking** *dscp_marking_value* **} }**：ARP 優先度レベルを設定し、カプセル化ヘッダーまたはユーザーデータグラムに適用する DSCP 値を構成します。

  **encsp-header** が構成されている場合は、ダウンリンク方向の外部 IP ヘッダーの DSCP を設定するか、内部 IP ヘッダーから外部 IP ヘッダーに DSCP 値をコピーします。

**user-datagram** が構成されている場合は、ダウンリンク方向の内部 IP ヘッダーに DSCP を設定します。

*arp_value* は 1ー255 の範囲の整数である必要がありま。

*dscp_marking_value* は、0x00 から 0x3F までの 16 進数である必要があります。

次に、設定例を示します。

```
profile qos test
 dscp-map qi5 1 downlink encaps-header copy-inner
 dscp-map qi5 1 downlink encaps-header dscp-marking 0x3b
 dscp-map qi5 2 downlink user-datagram dscp-marking 0x3b
 dscp-map qi5 3 downlink user-datagram dscp-marking 0x3b encaps-header copy-inner
 dscp-map qi5 4 downlink user-datagram dscp-marking 0x3b encaps-header dscp-marking 0x3f

 dscp-map qi5 2 uplink user-datagram dscp-marking 0x3b

 dscp-map qi5 1 arp-priority-level 1 downlink encaps-header copy-inner
 dscp-map qi5 2 arp-priority-level 2 downlink encaps-header dscp-marking 0x3b
 dscp-map qi5 4 arp-priority-level 3 downlink user-datagram dscp-marking 0x3b
 dscp-map qi5 2 arp-priority-level 4 downlink user-datagram dscp-marking 0x3b encaps-header
 copy-inner
 dscp-map qi5 4 arp-priority-level 5 downlink user-datagram dscp-marking 0x3b encaps-header
 dscp-marking 0x3f
 dscp-map qi5 4 arp-priority-level 5 uplink user-datagram dscp-marking 0x3b
```

## UP パケットの DSCP 構成の確認

このセクションでは、UP パケットの DSCP マーキング機能の構成を確認する方法について説明します。

**show running-config profile qos** コマンドを使用して、UP パケットの DSCP 構成を確認します。

**show running-config profile qos** コマンドの出力例を次に示します。

```
smf# show running-config profile qos
profile qos abc
 ambr ul "250 Kbps"
 ambr dl "500 Kbps"
 qi5      7
 arp priority-level 14
 arp preempt-cap NOT_PREEMPT
 arp preempt-vuln PREEMPTABLE
 priority 120
 max data-burst 2000
exit
profile qos qos_1
 dscp-map qi5 1 arp-priority-level 5 uplink user-datagram dscp-marking 0x1e
 dscp-map qi5 1 arp-priority-level 5 downlink user-datagram dscp-marking 0x22 encsp-header
 copy-inner
 dscp-map qi5 2 arp-priority-level 6 uplink user-datagram dscp-marking 0x3e
 dscp-map qi5 2 arp-priority-level 6 downlink user-datagram dscp-marking 0x23 encsp-header
 copy-inner
 dscp-map qi5 3 arp-priority-level 12 uplink user-datagram dscp-marking 0x2f
 dscp-map qi5 3 arp-priority-level 12 downlink user-datagram dscp-marking 0x14 encsp-header
 copy-inner
 dscp-map qi5 6 downlink encsp-header copy-inner
 dscp-map qi5 7 downlink encsp-header dscp-marking 0x01
exit
```

# コントロール プレーン シグナリングの DSCP マーキング

## 機能説明

SMFは、インターフェイスでの構成に従ってパケットを制御するためのDSCP値のマーキングをサポートしています。

（注） DSCPマーキングの現在の実装は、インターフェイスおよびプロトコルエンドポイントごとのみをサポートします。また、お客様はDSCPコードの値の範囲と、その指定された優先順位を認識しておく必要があります。

## 制御シグナリングに対する DSCP マーキングの仕組み

SMF は QoS 分類の後に、入力パケットと出力パケットをマークします。プロトコル エンドポイントは、エンドポイントとインターフェイスの登録時に DSCP 値を提供します。

SMF は、エンドポイントおよびインターフェイスの構成で **dscp** コマンドを使用して DSCP 値を定義します。

次の表に、RFC 2475 に記述されている、一般的に使用される DSCP の値を示します。

表 *32 :* 一般的に使用される *DSCP* 値

| DSCP 値 | 10 進値 | 意味 | 廃棄確率 | 同等 IP precedence 値の値 |
|---|---|---|---|---|
| 101 110 | 46 | 高い優先順位の緊急転送（EF） | — | 101：重大 |
| 000 000 | 0 | ベスト エフォート | — | 000：ルーチン |
| 001 010 | 10 | AF11 | 低 | 001：優先度 |
| 001 100 | 12 | AF12 | 中 | 001：優先度 |
| 001 110 | 14 | AF13 | 高 | 001：優先度 |
| 010 010 | 18 | AF21 | 低 | 010：即時 |
| 010 100 | 20 | AF22 | 中 | 010：即時 |
| 010 110 | 22 | AF23 | 高 | 010：即時 |
| 011 010 | 26 | AF31 | 低 | 011：フラッシュ |

| DSCP 値 | 10 進値 | 意味 | 廃棄確率 | 同等 IP precedence 値の値 |
|---|---|---|---|---|
| 011 100 | 28 | AF32 | 中 | 011：フラッシュ |
| 011 110 | 30 | AF33 | 高 | 011：フラッシュ |
| 100 010 | 34 | AF41 | 低 | 100：フラッシュオーバーライド（Flash Override） |
| 100 100 | 36 | AF42 | 中 | 100：フラッシュオーバーライド（Flash Override） |
| 100 110 | 38 | AF43 | 高 | 100：フラッシュオーバーライド（Flash Override） |
| 001 000 | 8 | CS1 | | 1 |
| 010 000 | 16 | CS2 | | 2 |
| 011 000 | 24 | CS3 | | 3 |
| 100 000 | 32 | CS4 | | 4 |
| 101 000 | 40 | CS5 | | 5 |
| 110 000 | 48 | CS6 | | 6 |
| 111 000 | 72 | CS7 | | 7 |
| 000 000 | 0 | デフォルト | | |
| 101 110 | 46 | EF | | |

## 制限事項

DSCP マーキング機能には次の制限があります。

- DSCP マーキングはインターフェイス単位で適用され、ピアまたはセッション単位ではありません。

# コントロール プレーン シグナリングの DSCP マーキングの構成

このセクションでは、CP シグナリングメッセージの DSCP マーキング機能を構成する方法について説明します。

DSCP マーキング機能の構成には、次の手順が含まれます：

• エンドポイントごとの DSCP マーキングの構成 （165 ページ）
• インターフェイスごとの DSCP マーキングの構成 （165 ページ）

## エンドポイントごとの DSCP マーキングの構成

エンドポイント レベルで DSCP 値を構成するには、次の構成例を使用します。

```
config
   instance instance-id gr_instance_id
      endpoint { gtp | li | protocol | radius | sbi }
         dscp dscp_value
         commit
```

注：

- DSCP マーキング構成は、次のエンドポイントにのみ適用されます：
  - protocol
  - sbi
  - gtp
  - radius
  - li
- **dscp** *dscp_value*：コントロール プレーン シグナリング メッセージの DSCP 値を指定します。*dscp_value* は 、0x00 ～ 0x3F の 16 進数、または 0 ～ 63 の範囲の 10 進数値である必要があります。
- DSCP マーキング機能では、構成のダイナミックな変更がサポートされます。

## インターフェイスごとの DSCP マーキングの構成

インターフェイス レベルで DSCP 値を構成するには、次の構成例を使用します。

```
config
   instance instance-id gr_instance_id
      endpoint { gtp | li | protocol | radius | sbi }
         interface { coa-nas | gtpu | n4 | n7 | n10 | n11 | n16 | n40
| nrf | radius-client | s2b | s5 | s8 | upf-rcm-conn | upf-rcm-reg }
            dscp dscp_value
            commit
```

注：

- DSCPマーキング構成は、構成されたエンドポイント内で定義されたすべてのインターフェイスに適用できます。

- **dscp** *dscp_value*：コントロール プレーン シグナリング メッセージの DSCP 値を構成します。 *dscp_value* は 、0x00 ～ 0x3F の 16 進数、または 0 ～ 63 の範囲の 10 進数値である必要があります。
- DSCP マーキング機能では、構成のダイナミックな変更がサポートされます。
- サービスベースのインターフェイス（SBI）構成は、すべてのインターフェイスに適用されます。特定のインターフェイス構成が存在する場合、DSCP 値は上書きされます。
- インターフェイスを正しく動作させるには、各インターフェイス レベルで vip-ip、vip-port、および loopbackPort を構成する必要があります。

## CP シグナリング メッセージの DSCP 構成

このセクションでは、CP シグナリング メッセージの DSCP マーキング機能の構成を確認する方法について説明します。

**show running-config instance instance-id** *gr_instance_id* **endpoint** コマンドを使用して、制御パケットの DSCP 構成を確認します：

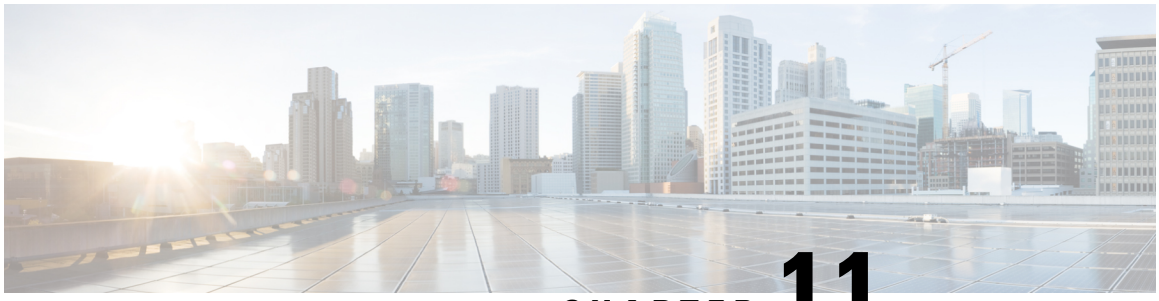
**show running-config instance instance-id 1 endpoint** コマンドの出力例を次に示します。

```
smf# show running-config instance instance-id 1 endpoint
instance instance-id 1
 endpoint sbi
  replicas 2
  nodes 1
  dscp 24
  vip-ip 209.165.200.230
  interface nrf
   loopbackPort 9050
   vip-ip 209.165.200.236 vip-port 8090
   dscp 24
  exit
 exit
exit
```

# DSCP マーキングの OAM サポート

## Monitoring Support

SMF では **monitor protocol** および **monitor subscriber** コマンドを使用して、構成された DSCP 値が表示されます。



CHAPTER 11

# BGP を使用したダイナミック ルーティング


- 機能の概要と変更履歴 （167 ページ）
- 機能説明, on page 168
- 機能の仕組み, on page 168
- BGP を使用したダイナミック ルーティングの構成, on page 177
- モニタリングおよびトラブルシューティング, on page 180


## 機能の概要と変更履歴

### 要約データ

***Table 33:*** 要約データ

| | |
|---|---|
| 該当製品または機能エリア | SMF |
| 該当プラットフォーム | SMI |
| デフォルト設定 | 無効：有効化するには構成が必要 |
| このリリースでの関連する変更点 | N/A |
| 関連資料 | 該当なし |

### 更新履歴

**表 *34 :*** マニュアルの変更履歴

| 改訂の詳細 | リリース |
|---|---|
| 最初の導入。 | 2021.02.0 |

# 機能説明

ボーダー ゲートウェイ プロトコル（BGP）では、自律システム（AS）間にループフリーのドメイン間ルーティングを作成可能です。AS は、単一の技術管理に基づくルータのまとまりです。ルータは、外部ゲートウェイ プロトコルを使用して AS の外部にパケットをルーティングできます。BGP を使用したダイナミック ルーティング機能を使用すると、優先順位とルートとともに IP アドレスにサービスを提供する代替ローカル アドレスを持つ BGP ルータのネクストホップ属性を構成できます。SMF BGP スピーカー ポッドは、BGP を使用してポッド ルートをサービス VIP にアドバタイズすることにより、トラフィックのダイナミック ルーティングを可能にします。

この機能は、次の機能をサポートしています。

- BGP を使用したダイナミック ルーティングによる着信トラフィックのサービス IP アドレスのアドバタイズ。
- 発信トラフィックのルートの学習。
- BGP ポッド フェールオーバーの処理。
- プロトコル ポッド フェールオーバーの処理。
- BGP スピーカーの統計と KPI。
- BGP スピーカーをデバッグするためのログ メッセージ。
- BGP スピーカー ポッドを有効または無効にします。
- BGP を構成するための新しい CLI コマンド。

# 機能の仕組み

ここでは、ダイナミック ルーティング機能の動作について説明します。

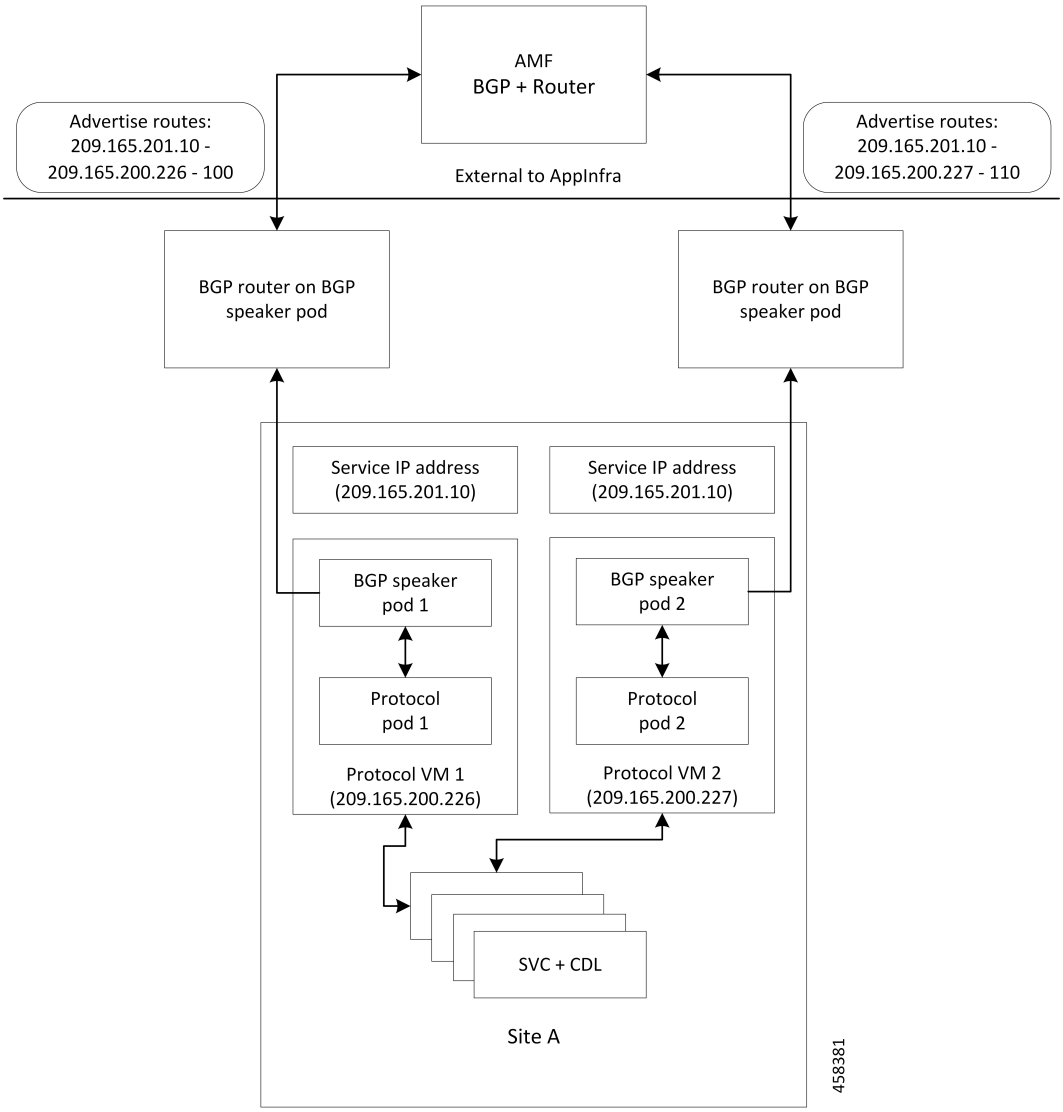
### 着信トラフィック

BGP は、ポート 179 でトランスポートプロトコルとして TCP を使用します。2 台の BGP ルータは相互に TCP 接続を形成し、各ルータはピアルータです。ピアルータはメッセージを交換し、接続パラメータを開いて確認します。

BGP スピーカーは、アクティブ/スタンバイモードで着信トラフィックのプロトコルポッドのルーティング情報を公開します。次の図を例として使用して、ダイナミック ルーティングの機能を理解してください。pod1 と pod2 の 2 つのプロトコル ポッドがあります。pod1 はアクティブで、pod2 はスタンバイ モードになっています。サービス IP アドレス 209.165.201.10 は、209.165.200.226 と 209.165.200.227 の両方のノードで構成されています。pod1 はホスト 209.165.200.226 で、pod2 はホスト 209.165.200.227 で実行されています。ホスト IP アドレスはポッド サービスを公開します。BGP スピーカーは、ルート 209.165.201.10 を 209.165.200.226

と 209.165.200.227 に公開します。また、ポッドの優先順位を決定するために、プリファレンス値 110 と 100 を公開します。

***Figure 19:*** アクティブ/スタンバイ トポロジでの着信トラフィックのダイナミック ルーティング




高可用性を実現するため、各クラスタにはアクティブ/スタンバイ トポロジを備えた 2 つの BGP スピーカーポッドがあります。カーネル ルートの変更は、プロトコルポッドが実行されているホスト/ネットワーク レベルで実行されます。

## MED 値

ローカル プリファレンスは IGP ネイバーでのみ使用され、MED 属性は EGP ネイバーでのみ使用されます。BGP では、より低い MED 値が推奨されます。

*Table 35: MED* 値

| ボンディングインターフェイスがアクティブ | VIP の存在 | MED 値 | Local Preference |
|---|---|---|---|
| はい | はい | 1210 | 2220 |
| はい | 非対応 | 1220 | 2210 |
| 非対応 | はい | 1215 | 2215 |
| いいえ | 非対応 | 1225 | 2205 |

### BGP スピーカー ポッドのブートストラップ

次の一連の手順で、BGP スピーカー ポッドをセットアップします。

1. BGP スピーカー ポッドは、ポート 179 でトランスポート プロトコルとして TCP を使用し、これらのポッドは、Ops Center CLI で構成されている AS 番号を使用します。
2. Topology Manager を登録します。
3. リーダー ポッドを選択します。アクティブなスピーカー ポッドがデフォルトの選択肢です。
4. Ops Center CLI によって提供されるすべての BGP ピアへの接続を確立します。
5. ETCD から既存のすべてのルートを公開します。
6. CLI 構成を使用して、ルーティングのインポート ポリシーを構成します。
7. 両方のスピーカー ポッドで gRPC ストリーム サーバを開始します。
8. キャッシュ ポッドと同様に、各名前空間で 2 つの BGP スピーカー ポッドを実行する必要があります。

# 外部ネットワーク障害

NF インスタンスの起動により、BGP スピーカー K8s ポッドは、優先順位とルートとともに IP アドレスにサービスを提供するための代替ローカル アドレスを使用して、BGP ルータのネクストホップ属性を構成します。

地理的 HA がトリガされると、宛先サービスの IP アドレス、パスの接続性、および優先度の値に基づいてパスが選択されます。

**Note** ポッド間の透過的な移行により、サブスクライバ セッションは影響を受けません。

# Geo スイッチオーバー

SMF は、サービス IP アドレスを、対応するピア K8s クラスタ、コロケーションされたラック、または地理的に配置されたラックに透過的に移行することで、Geo スイッチオーバーを実現します。NF の起動時に、すべての K8s クラスタ名前空間はネクストホップの BGP ルータに登録し、サービス IP アドレスとローカル IP アドレス、優先順位とルート修飾値をアドバタイズします。

各論理 NF は、NRF または DNS に対する個別の NF インスタンス、個別の構成、および名前空間の個別 LCM を公開する。

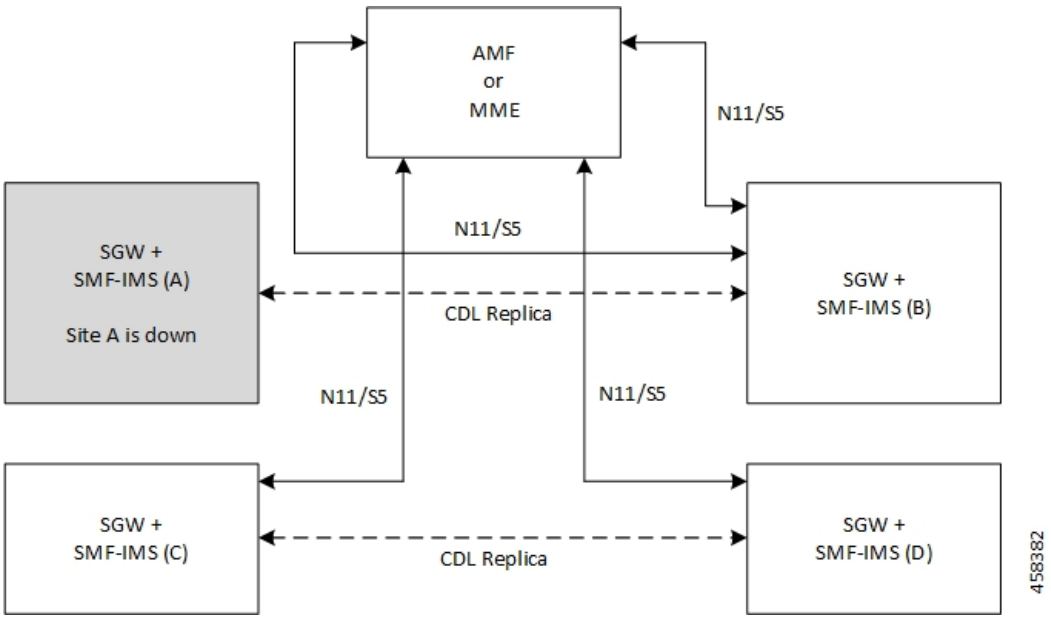
# 内部ネットワーク障害

マスター ノードとのサーバ通信の中断、BFD の障害、または K8s ポッドのネットワークの問題が原因で、機能している K8s クラスタに内部ネットワーク障害が発生した場合、K8s の稼働状態の障害に基づく K8s の依存関係チェックにより、Geo HA がトリガされます。

次の図に示した例では、AMF または MME が透過的に代替ラック サーバの使用を開始しています。N11/S11/S5 および N4/Sxa サービスアドレスはサイト B のラック B に移行されます。システムはラック A のラック B からのシグナリングを継続します。ラック B では、既存のサブスクライバ セッションに影響を与えることなくセッションが続行されます。

**Note** UE が再接続する前にコールが終了される状態によっては、接続中のコールがほとんど失敗する場合があります。

***Figure 20:*** 内部ネットワーク障害に対する ***Geo HA***



# ローカル スイッチオーバー

SMF は、同じデータセンター内に配置されたピア K8s クラスタまたはラックにサービス IP アドレスを透過的に移行することで、Geo スイッチオーバーを実現します。NF の起動時に、すべての K8s クラスタ名前空間はネクストホップの BGP ルータに登録し、サービス IP アドレスとローカル IP アドレス、優先順位とルート修飾値をアドバタイズします。各論理 NF は、NRF または DNS に対する個別の NF インスタンス、個別の構成、および名前空間の個別 LCM を公開する。

# リカバリとフェールバック

シームレスなフェールオーバーとフェールバックのために、UE セッションと対応するサービス IP アドレスがグループ化されます。

次のシナリオでは、UE セッションのシームレスなフェールオーバーとフェールバックのメカニズムについて説明します。

- **通常**：UE セッション セットは、最初のラックから作成、更新、または削除され、2 番目のラックに複製されます。
- **失敗**：UE セッション セットは、2 番目のラックから作成、更新、または削除されますが、可用性が低いため、最初のラックには複製されません。
- **リカバリ**：すべての UE セッション データをリカバリするために、最初のラックの CDL が 2 番目のラックの CDL と自動同期を実行します。リカバリ中は、2 番目のラックはセッション セットからのトラフィックを処理し続けます。

# コール フロー

ここでは、BGP を使用したダイナミック ルーティングの主要なコール フローについて説明します。

## アクティブ/スタンバイ モードでの着信トラフィックのルートの公開

ここでは、アクティブ/スタンバイ モードでのコントロール プレーンとデータ プレーンのコール フローについて説明します。

### コントロール プレーンのコール フロー

ここでは、コントロール プレーンのコール フローについて説明します。

***Figure 21:*** コントロール プレーンのコール フロー

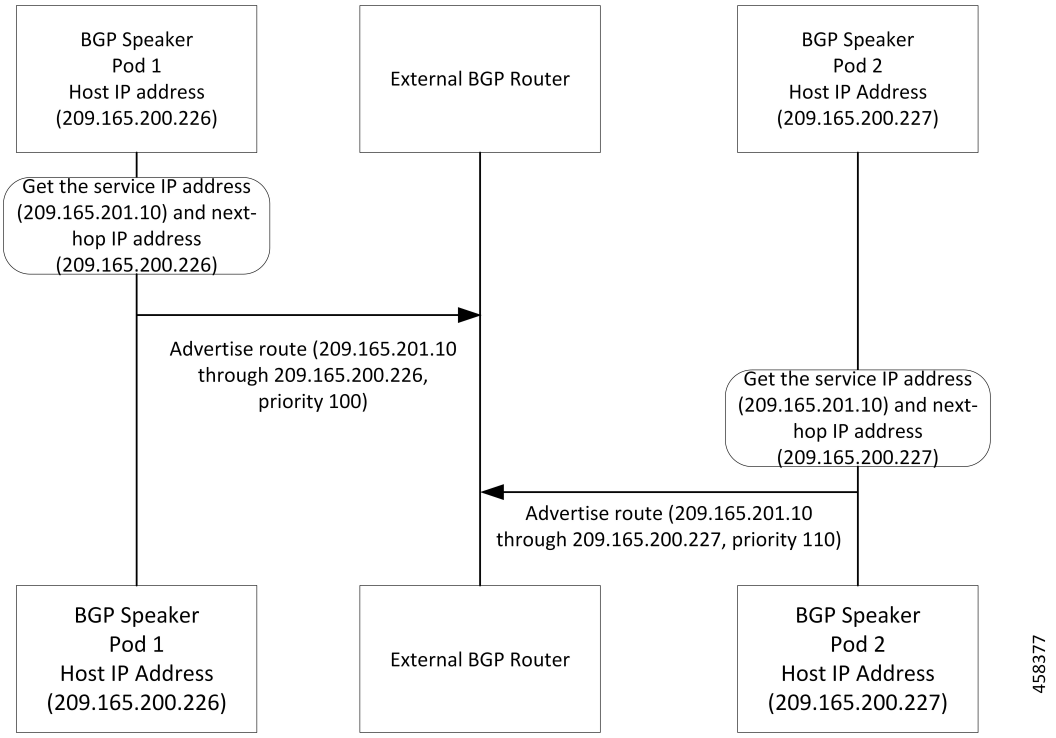



***Table 36:*** コントロール プレーンのコール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | BGP スピーカーポッドが起動し、サービス IP アドレス、ネクストホップ IP アドレス（ホスト IP または loopbackEth）、および BGP スピーカー ポッドのインスタンス ID を取得します。<br>ポッド サービスは、ホスト IP または構成された loopbackEth を介して公開されます。<br>NF インスタンス ID は、ルートの優先順位やプリファレンスを検索するために使用されます。 |
| 2 | BGP スピーカー ポッドは、Ops Center から vip-ip（サービス IP アドレス）を取得してルートをアドバタイズします。 |

## データ プレーンのコール フロー

ここでは、データ プレーンのコール フローについて説明します。

***Figure 22:*** データ プレーンのコール フロー

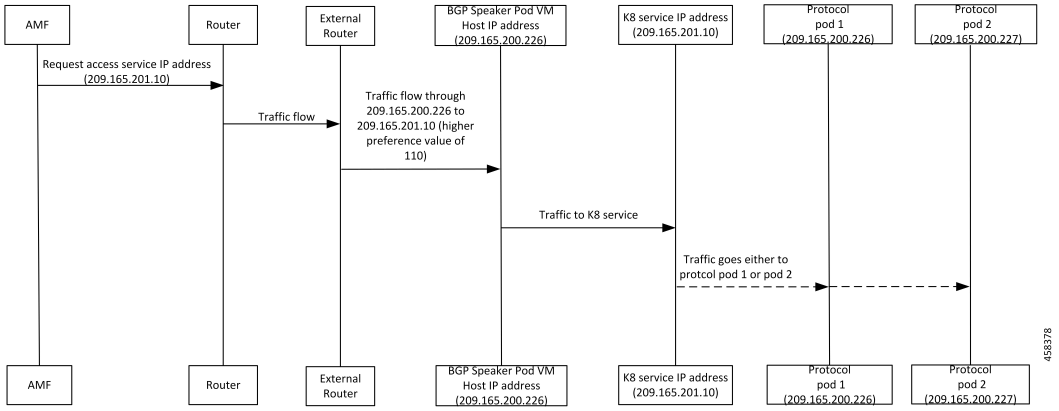



***Table 37:*** データ プレーンのコール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | サービス IP アドレスの AMF 要求。要求は、複数の外部ルータを介して、接続された最も近いルータに送信されます。次に、ルータは優先順位が最も高いBGP スピーカーポッドに要求を送信します。 |
| 2 | BGP ルータは、プリファレンス値に基づいてデータ プレーン フローを設定します。前述のコール フローの例では、ルータは、プリファレンス値がより高いため、サービス要求をホスト 209.165.200.226 を介してポッド 1 にルーティングします。<br>ホスト（209.165.200.226）からのトラフィックは K8 サービス IP アドレス（209.165.201.10）に転送され、プロトコルポッド 1（209.165.200.226）またはポッド 2（209.165.200.227）に送信されます。 |

## シングル プロトコル ポッド障害コール フロー

ここでは、シングル プロトコル ポッド障害コール フローについて説明します。

***Figure 23:*** シングル プロトコル ポッド障害コール フロー

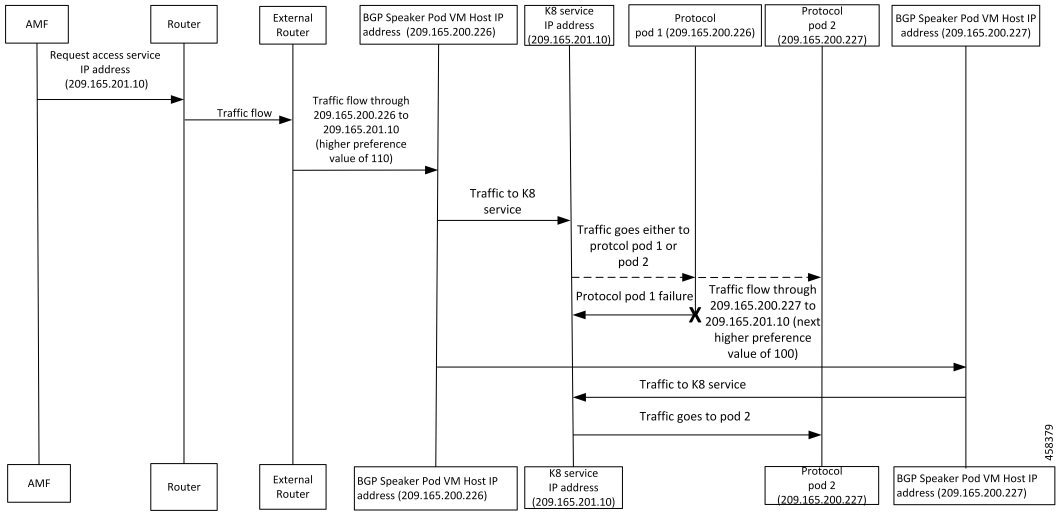


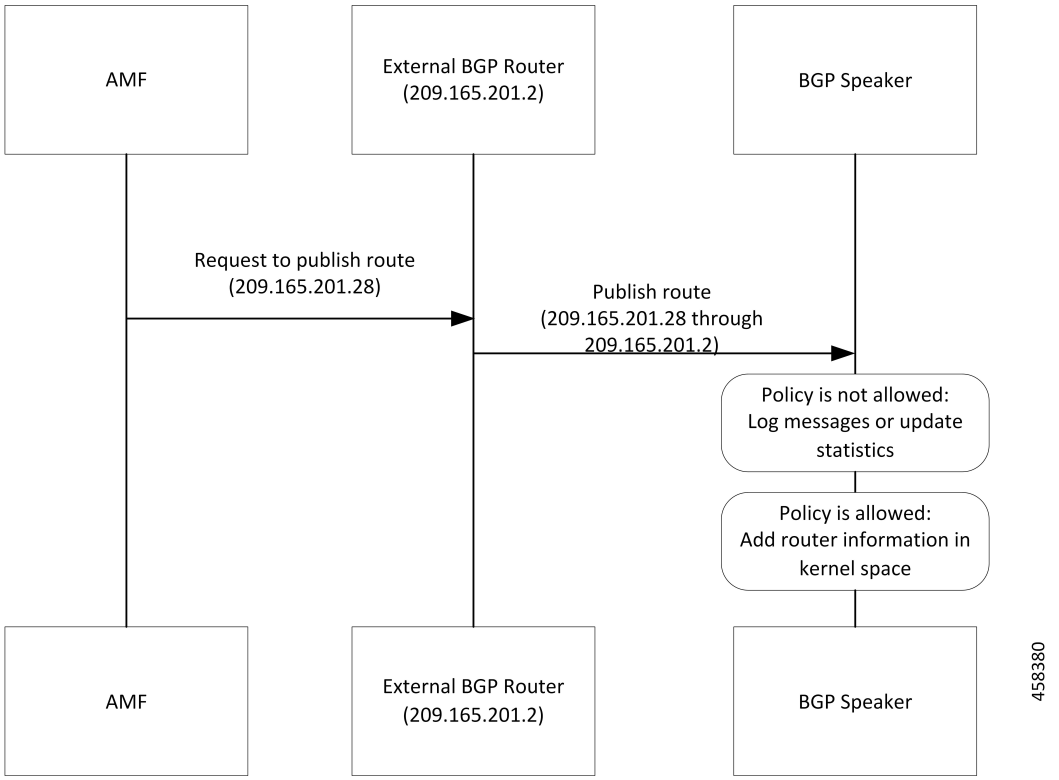

***Table 38:*** シングル プロトコル ポッド障害コール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | サービス IP アドレスの AMF 要求。要求は、次に高いプリファレンス値に基づいて、複数の外部ルータを介して、最も近く接続された BGP ルータに送信されます。 |
| 2 | BGP ルータは、プリファレンス値に基づいてデータ プレーン フローを設定します。最も高いプリファレンス値を持つポッドが使用できない場合、要求は K8 サービス ポッドを介して次に高いプリファレンス値を持つポッドにルーティングされます。<br>前述のコール フローの図に示した例では、IP アドレスの 209.165.200.227 を持つポッド 2 が、より高いプリファレンス値のために要求を処理します。 |

# 発信トラフィック コール フローのルートの学習

ここでは、発信トラフィックのルートの学習コール フローについて説明します。

***Figure 24:*** 発信トラフィックのルートの学習コール フロー




AMF などのシステムが外部BGPルートにルートをアドバタイズします。次に、外部BGPルータがBGP を介してそのサービスのルートをアドバタイズします。

***Table 39:*** 発信トラフィックのルートの学習コール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | BGP スピーカーがルーティング情報を受信します。 |
| 2 | BGP プロトコルを使用してルートを学習します。 |
| 3 | 構成ポリシーに基づいて、システムはルーティング情報を確認するか、無視します。 |
| 4 | ポリシーが許可されていない場合、システムはメッセージをログに記録し、統計情報を更新します。 |
| 5 | プロトコル ポッドは、netlink go API を介してホスト上のカーネル スペースでルートを構成します。 |

# BGP を使用したダイナミック ルーティングの構成

ここでは、BGP を使用してダイナミック ルーティングを構成する方法について説明します。

### AS と BGP ルータの IP アドレスの構成

BGP ルータの AS と IP アドレスを構成するには、次のコマンドを使用します。

```
config
   router bgp local_as_number
   exit
exit
```

注：

- **router bgp** *local_as_number*：BGP ルータの AS の ID 番号を指定します。

### BGP サービス リスニング IP アドレスの構成

BGP サービス リスニング IP アドレスを構成するには、次のコマンドを使用します。

```
config
   router bgp local_as_number
      interface interface_name
   exit
exit
```

注：

- **router bgp** *local_as_number*：BGP ルータの AS の ID 番号を指定します。
- **interface** *interface_name*：インターフェイスの名前を指定します。

### BGP ネイバーの構成

BGP ネイバーを構成するには、次のコマンドを使用します。

```
config
   router bgp local_as_number
      interface interface_name
      neighbor neighbor_ip_address remote-as as_number
   exit
exit
```

注：

- **router bgp** *local_as_number*：BGP ルータの AS の ID 番号を指定します。
- **interface** *interface_name*：インターフェイスの名前を指定します。
- **neighbor** *neighbor_ip_address*：ネイバー BGP ルータの IP アドレスを指定します。
- **remote-as** *as_number*：AS の ID 番号を指定します。

### ボンディング インターフェイスの構成

インターフェイスに関連するボンディングインターフェイスを構成するには、次のコマンドを使用します。

```
config
   router bgp local_as_number
      interface interface_name
      bondingInterface interface_name
   exit
exit
```

注：

- **router bgp** *local_as_number*：BGP ルータの AS の ID 番号を指定します。
- **interface** *interface_name*：インターフェイスの名前を指定します。
- **bondingInterface** *interface_name*：インターフェイスに関連するボンディングインターフェイスを指定します。ボンディング インターフェイスがアクティブである場合、BGP は、より低い MED 値を提供することで、インターフェイス サービスに高いプリファレンスを与えます。

### 学習デフォルト ルートの構成

システム上に特定のルートを構成し、すべてのルートをサポートする必要があるユーザーは、**learnDefaultRoute** を **true** に設定する必要があります。

**Note** この設定は任意です。

デフォルト ルートの学習を構成するには、次のコマンドを使用します。

```
config
   router bgp local_as_number
      learnDefaultRoute true/false
   exit
exit
```

注：

- **router bgp** *local_as_number*：BGP ルータの AS の ID 番号を指定します。
- **learnDefaultRoute** *true/false*： **learnDefaultRoute** パラメータを有効または無効にするオプションを指定します。true に設定すると、BGP はデフォルト ルートを学習し、カーネルスペースに追加します。デフォルトは False です。

### BGP ポートの構成

BGP サービスのポート番号を構成するには、次のコマンドを使用します。

```
config
   router bgp local_as_number
      loopbackPort port_number
   exit
exit
```

注：

- **router bgp** *local_as_number*：BGP ルータの AS の ID 番号を指定します。
- **loopbackPort** *port_number*：BGP サービスのポート番号を指定します。デフォルト値は 179 です。

### ポリシーの追加

BGP スピーカー ポッドは、ネイバーから多くのルート情報を学習します。ただし、発信トラフィックのサポートに使用されるのはそのうちのごく一部です。これは、 SMF が 外部の AMF/PCF に情報を送信している場合、出力トラフィックの処理にのみ必要です。ルートは、BGP スピーカーでインポート ポリシーを構成することでフィルタリングされ、学習したルートをプロトコルポッドに送信するために使用されます。

ポリシー追加用のサンプル CLI コードと、各パラメータに対応する説明を以下に示します。

```
$bgp policy <policy_Name> ip-prefix 209.165.200.225 subnet 16 masklength-range 21..24
as-path-set "^65100"
```

***Table 40:*** インポート ポリシーのパラメータ

| 要素 | 説明 | 例 | オプション |
|---|---|---|---|
| **as-path-set** | AS パス値 | “^65100” | 対応 |
| **ip-prefix** | プレフィックス値 | “209.165.200.225/16” | 対応 |
| **masklength-range** | 長さの範囲 | “21..24” | はい |
| **interface** | 送信元 IP として設定するインターフェイス（デフォルトは VM IP） | eth0 | 対応 |
| **gateWay** | 着信ルートのゲートウェイを変更します | 209.165.201.30 | 対応 |
| **modifySourceIp** | 着信ルートの送信元IPの変更<br>デフォルト値は False です。 | true | はい |

| 要素 | 説明 | 例 | オプション |
|---|---|---|---|
| **isStaticRoute** | カーネルルートにスタティック IP アドレスを追加するフラグ<br>デフォルト値は False です。 | true | はい |

# モニタリングおよびトラブルシューティング

この項では、BGP を使用したダイナミック ルーティング機能でサポートされている show コマンドについて説明します。

### show bgp-kernel-route

BGP ルータのカーネル レベルのすべてのルートを表示するには、 **show bgp-kernel-route** コマンドを使用します。

以下の構成は、**show bgp-kernel-route** コマンドの出力例です。

```
kernel-route

-----bgpspeaker-pod-1 ----

 DestinationIP       SourceIP        Gateway

 209.165.200.235     209.165.200.239   209.165.200.239

-----bgpspeaker-pod-2 ----

 DestinationIP       SourceIP        Gateway

 209.165.200.235     209.165.200.229   209.165.200.244
```

### show bgp-global

すべての BGP グローバル コンフィギュレーションを表示するには、 **show bgp-global** コマンドを使用します。

以下の構成は、**show bgp-global** コマンドの出力例です。

```
global-details

-----bgpspeaker-pod-1 ----
AS:        65000
Router-ID: 209.165.200.239
Listening Port: 179, Addresses: 209.165.200.239
AS:        65000
Router-ID: 209.165.200.232
Listening Port: 179, Addresses: 209.165.200.232

-----bgpspeaker-pod-2 ----
AS:        65000
Router-ID: 209.165.200.235
Listening Port: 179, Addresses: 209.165.200.235
```

```
AS:        65000
Router-ID: 209.165.200.246
Listening Port: 179, Addresses: 209.165.200.246
```

### show bgp-neighbors

BGP ルータのすべての BGP ネイバーを表示するには、**show bgp-neighbors** コマンドを使用します。

以下の構成は、**show bgp-neighbors** コマンドの出力例です。

```
neighbor-details

-----bgpspeaker-pod-2 ----
Peer              AS  Up/Down State       |#Received  Accepted
209.165.200.244 60000 00:34:20 Establ      |       10        10
Peer           AS  Up/Down State       |#Received  Accepted
209.165.200.250 60000 00:34:16 Establ      |        3         3

-----bgpspeaker-pod-1 ----
Peer              AS  Up/Down State       |#Received  Accepted
209.165.200.244 60000 00:33:53 Establ      |       10        10
Peer           AS  Up/Down State       |#Received  Accepted
209.165.200.250 60000 00:33:53 Establ      |        3         3
```

### show bgp-neighbors *ip*

BGP ルータのネイバーの詳細を表示するには、**show bgp-neighbors** *ip* コマンドを使用します。

以下の構成は、**show bgp-neighbors** *ip* コマンドの出力例です。

```
neighbor-details

-----bgpspeaker-pod-1 ----
BGP neighbor is 209.165.200.244, remote AS 60000
  BGP version 4, remote router ID 209.165.200.244
  BGP state = ESTABLISHED, up for 00:34:50
  BGP OutQ = 0, Flops = 0
  Hold time is 90, keepalive interval is 30 seconds
  Configured hold time is 90, keepalive interval is 30 seconds

  Neighbor capabilities:
    multiprotocol:
        ipv4-unicast:   advertised and received
    route-refresh:      advertised and received
    extended-nexthop:   advertised
        Local:  nlri: ipv4-unicast, nexthop: ipv6
    4-octet-as: advertised and received
  Message statistics:
                         Sent       Rcvd
    Opens:                  1          1
    Notifications:          0          0
    Updates:                1          2
    Keepalives:            70         70
    Route Refresh:          0          0
    Discarded:              0          0
    Total:                 72         73
  Route statistics:
    Advertised:             0
    Received:              10
    Accepted:              10

-----bgpspeaker-pod-2 ----
```

```
BGP neighbor is 209.165.200.244, remote AS 60000
  BGP version 4, remote router ID 209.165.200.244
  BGP state = ESTABLISHED, up for 00:35:17
  BGP OutQ = 0, Flops = 0
  Hold time is 90, keepalive interval is 30 seconds
  Configured hold time is 90, keepalive interval is 30 seconds

  Neighbor capabilities:
    multiprotocol:
        ipv4-unicast:   advertised and received
    route-refresh:      advertised and received
    extended-nexthop:   advertised
        Local:  nlri: ipv4-unicast, nexthop: ipv6
    4-octet-as: advertised and received
  Message statistics:
                         Sent       Rcvd
    Opens:                  1          1
    Notifications:          0          0
    Updates:                1          2
    Keepalives:            71         71
    Route Refresh:          0          0
    Discarded:              0          0
    Total:                 73         74
  Route statistics:
    Advertised:             0
    Received:              10
    Accepted:              10
```

### show bgp-route-summary

BGP ルータのすべてのルートの詳細を表示するには、**show bgp-route-summary** コマンドを使用します。

以下の構成は、**show bgp-route-summary** コマンドの出力例です。

```
route-details

-----bgpspeaker-pod-1 ----
Table afi:AFI_IP safi:SAFI_UNICAST
Destination: 5, Path: 5

-----bgpspeaker-pod-2 ----
Table afi:AFI_IP safi:SAFI_UNICAST
Destination: 5, Path: 5
```

### show bgp-routes

BGP ルータのすべてのルートを表示するには、**show bgp-routes** コマンドを使用します。

以下の構成は、**show bgp-routes** コマンドの出力例です。

```
bgp-route

-----bgpspeaker-pod-1 ----
   Network              Next Hop             AS_PATH       Age        Attrs
*> 209.165.200.235/24   209.165.200.250      60000         00:36:39   [{Origin: i} {Med:
 0}]
*> 209.165.200.227/32   209.165.200.232                    00:36:44   [{Origin: e}
{LocalPref: 220} {Med: 3220}]
*> 209.165.200.247/24   209.165.200.250      60000         00:36:39   [{Origin: i} {Med:
 0}]
*> 209.165.200.251/24   209.165.200.250      60000         00:36:39   [{Origin: i} {Med:
 0}]
```

```
*> 209.165.200.252/32   209.165.200.232                    00:36:44   [{Origin: e}
{LocalPref: 220} {Med: 3220}]

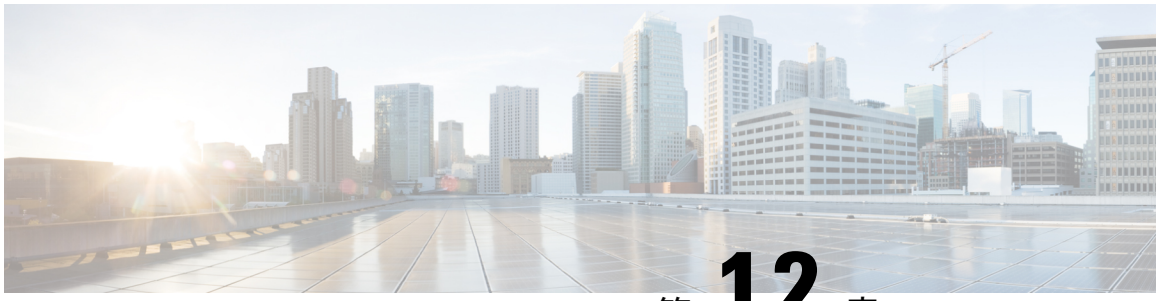
-----bgpspeaker-pod-2 ----
   Network              Next Hop             AS_PATH         Age        Attrs
*> 209.165.200.235/24   209.165.200.250      60000          00:37:02   [{Origin: i} {Med:
 0}]
*> 209.165.200.227/32   209.165.200.246                      00:37:11   [{Origin: e}
{LocalPref: 220} {Med: 3220}]
*> 209.165.200.228/24   209.165.200.234      60000          00:37:02   [{Origin: i} {Med:
 0}]
*> 209.165.200.229/24   209.165.200.234      60000          00:37:02   [{Origin: i} {Med:
 0}]
*> 209.165.200.230/32   209.165.200.246                      00:37:11   [{Origin: e}
{LocalPref: 220} {Med: 3220}]
```

## KPI

以下の KPI は、この機能でサポートされます。

***Table 41: BGP* を使用したダイナミック ルーティングの統計情報**

| KPI 名 | タイプ | 説明/式 | ラベル |
|---|---|---|---|
| bgp_outgoing_route request_total | カウンタ | 受信ルートの総数。 | local_pref、med、next_hope、service_IP |
| bgp_outgoing_failed route request_total | カウンタ | 障害の発生した受信ルートの総数。 | local_pref、med、next_hope、service_IP |
| bgp_incoming_route request_total | カウンタ | 着信ルートの総数。 | interface、next_hope、service_IP |
| bgp_incoming_failedroute request_total | カウンタ | 障害の発生した着信ルートの総数。 | interface、next_hope、service_IP |
| bgp_peers_total | カウンタ | 追加されたピアの総数。 | peer_ip、as_path |
| bgp_failed_peertotal | カウンタ | 障害が発生したピアの総数。 | peer_ip、as_path、error |



第 12 章

# 緊急 SoS サポート


- 機能の概要と変更履歴 （185 ページ）
- SoS 緊急サービスの LTE へのフォールバック （186 ページ）
- 緊急サービス サポート （191 ページ）


## 機能の概要と変更履歴

### 要約データ

| | |
|---|---|
| 該当製品または機能エリア | SMF |
| 該当プラットフォーム | SMI |
| 機能のデフォルト設定 | 有効：常時オン |
| このリリースでの関連する変更点 | N/A |
| 関連資料 | 該当なし |

### 更新履歴

**表 *42 :* マニュアルの変更履歴**

| 改訂の詳細 | リリース |
|---|---|
| 最初の導入。 | 2020.02.5.t1 |

# SoS 緊急サービスの LTE へのフォールバック

## 機能説明

緊急 SoS サポート機能により、同じ場所に配置されたクラウドネイティブ SMF と PGW-C で、4G ネットワークに配置されているサブスクライバの LTE を介した SoS 緊急サービスと、5G ネットワークに配置されているサブスクライバの LTE への SoS 緊急サービスフォールバックをサポートできます。

この緊急 SoS サポート機能は、次の機能をサポートしています。

- UDM の対話をスキップする新しい構成を提供します。
- PGW-C の 4G（LTE）での緊急 PDN 接続の作成を有効にします。
- NR の SMF サービング サブスクライバの LTE 要件への緊急サービスフォールバックをサポートします。
- 障害発生時に緊急通報の作成を「続行」するための既存の課金インターフェイスの障害処理とのインターワーキングをサポートします。
- radius を使用した既存のセカンダリ認証とのインターワーキングをサポートし、構成されていない場合は緊急コールの radius 認証をスキップします。
- EPS インターワーキング対応サブスクライバに RAT 間ハンドオーバー サポート（4G から 5G、5G から 4G）を提供します。

## 機能の仕組み

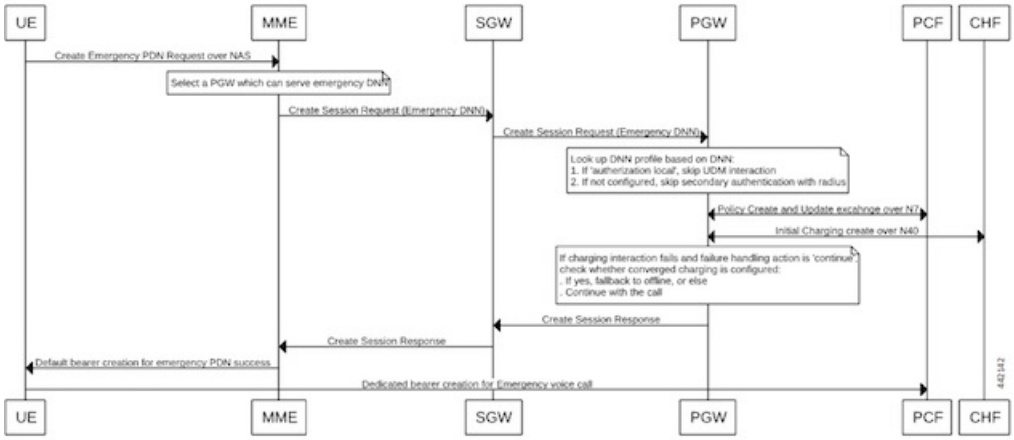
この項では、緊急 SoS のサポート機能の仕組みについて簡単に説明します。

### コール フロー

この項では、次のコールフローについて説明します。

## LTE コール フローの緊急セッション作成

***Figure 25: LTE* での緊急セッションの作成**

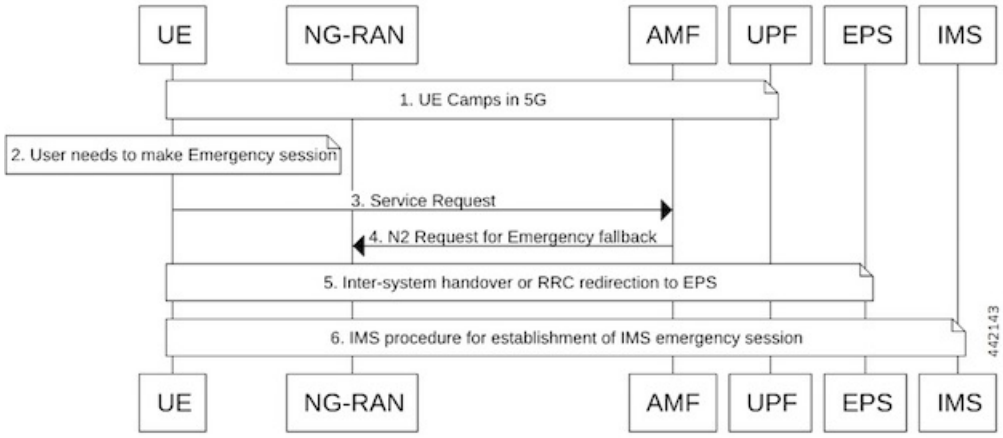



| ステップ | 説明 |
|---|---|
| 1 | 緊急サービスが必要で、緊急 PDU セッションがまだ確立されていない場合、UE は、LTE で「緊急要求」という要求タイプを示す、UE 要求の PDU セッションの確立手順を開始します。 |
| 2 | MME は、緊急 PDN を作成するための APN または DNN を選択し、S-GW を介して「セッション要求を作成」を PGW-C に送信します。 |
| 3 | PGW-C での DNN プロファイルのルックアップは、サブスクライバ ポリシーまたは DNN ポリシーに基づいています。これらのポリシーは、SMF プロファイルに関連付けられています。両方の構成が存在する場合、サブスクライバ ポリシーは DNN ポリシーよりも高い優先順位を持ちます。 |
| 4 | DNN ポリシーには、MME または S-GW からの「セッション要求の作成」で受信した、UE 要求の各 APN または DNN の DNN プロファイルを設定できます。 |
| 5 | 選択した DNN プロファイルの下に新しい構成「承認ローカル」が存在する場合：<br>• PGW-C は、サブスクリプションを取得するために UDM の連携動作をスキップし、MMEから「セッション要求の作成」メッセージで受信した値を使用します。<br>• PGW-C は、UDM から「Subscribe-for-Notification」への UDM 対話をスキップします。 |
| 6 | 選択した DNN プロファイルの下にある「Secondary Authentication Radius」が存在しない場合、PGW-C は RADIUS ベースのセカンダリ認証を拒否します。 |

| ステップ | 説明 |
|---|---|
| 7 | 課金インタラクションの「失敗の処理」が「アクション続行」に設定されている場合：<br>• コンバージド課金が構成されていない場合、PGW-C はコールを続行します。<br>• PGW-C はオフラインの充電にフォールバックし、通話を続行します。 |
| 8 | N26 を使用した 4G から 5G へのハンドオーバー中に、緊急 PDN が引き渡されると、SMF は DNN プロファイルをチェックし、「ローカル認証」が存在する場合、登録と登録解除のための UDM の連携動作をスキップします。 |

## LTE コール フローへの緊急サービス フォールバック

***Figure 26: LTE* への緊急サービスのフォールバック**




| ステップ | 説明 |
|---|---|
| 1 | UE は 5GS（CM_IDLE または CM_CONNECTED 状態）の E-UTRA または NR セルで判断を下します。 |
| 2 | UE に上位レイヤからの保留中の IMS 緊急セッション要求（音声など）があります。 |
| 3 | AMF が現在の RAT の「Registration Accept」メッセージを介してフォールバックを使用した緊急サービスのサポートを示している場合、UEは緊急サービスのフォールバックが必要であることを示す「Service Request」メッセージを送信します。 |

| ステップ | 説明 |
|---|---|
| 4 | 5GC は NG-AP 手順を実行し、これが緊急サービスのフォールバックであることを NG-RAN に示します。この手順では、「Emergency Services Fallback」要求がトリガーされます。現在、Cisco SMF と PGW-C は、EPC コア ネットワーク（LTE）での緊急サービスをサポートしています。AMF には、RAT 間フォールバックをトリガーするターゲット CN として EPC が含まれます。AMF が正常に認証された UE のリダイレクションを開始すると、AMF は NG-RAN へのフォールバックをトリガーする要求にセキュリティ コンテキストを含めます。 |
| 5 | NG-RAN は、EPS に接続された E-UTRAN へのハンドオーバーまたはリダイレクションを開始します（N26 インターフェイス ベースのハンドオーバーまたはリダイレクション手順）。NG-RAN は、AMF がリダイレクト手順を確保するためにセキュリティ コンテキストを使用します。<br>リダイレクション手順を使用する場合、ターゲット CN も UE に伝達され、S1 モード NAS 手順を実行できるようになります。UE は、RRC メッセージ内の緊急通知を使用し、E-UTRAN は「トラッキング エリア更新」中に MME に緊急通知を提供します。 |
| 6 | ターゲット セルへのハンドオーバー後、UE は IMS 緊急サービスの PDU セッションまたは PDN 接続を確立し、IMS 緊急セッション（音声など）の確立に関する IMS 手順を実行します。 |

# 緊急 SoS サポートの構成

ここでは、緊急 SoS サポート機能の構成方法について説明します。

この緊急 SoS サポートには、次の手順が含まれます。

- DNN プロファイルでのローカル認証の構成
- DNN プロファイルでのセカンダリ認証の構成
- 課金プロファイルでの課金失敗処理の構成

## ローカル認証の構成

次の構成例を使用して、DNN プロファイルでローカル認証を構成し、以下のコマンドを使用します：

```
config
  profile dnn pool_name
    [ no ] authorization local
    end
```

注：

- **profile dnn**：DNN プロファイル名を指定します。*profile_name* は英数字の文字列である必要があります。
- **no**：DNN プロファイルに基づいてセカンダリ認証を無効にします。

## セカンダリ認証の構成

次の構成例を使用して、DNN プロファイルでセカンダリ認証を設定します：

```
config
  profile dnn pool_name
    [ no ] secondary authentication radius
    end
```

注：

- **no**：DNN プロファイルに基づいてセカンダリ認証を無効にします。
- **secondary authentication**：DNN プロファイルでセカンダリ認証を有効にし、方式を RADIUS に設定します。
- **radius**：セカンダリ認証の RADIUS を指定します。

## 課金障害処理の構成

課金プロファイルでコンバージド課金とオフライン課金の両方の障害例に対する障害処理アクションを設定するには、次の構成例を使用します。

```
config
  profile network-element chf charging_profile_name
    nf-client-profile offline_charging_profile_name
    failure-handling-profile failure_handling_profile_name
    end
```

注：

- **profile network-element chf** *scp_profile_name*：SCP をネットワーク要素プロファイルとして指定します。 *scp_profile_name* には、対応するネットワーク要素のプロファイル名を表す英数字の文字列を指定する必要があります。
- **nf-client-profile** *profile_name*：クライアント プロファイルを指定します。 *profile_name* は、対応する NF クライアント プロファイル名を表す英数字の文字列を指定する必要があります。
- **failure-handling-profile** *failure_handling_scp_profile_name*：構成された SCP の SCP 障害処理ネットワーク プロファイルを指定します。 *failure_handling_scp_profile_name* には、対応する SCP 障害処理ネットワーク プロファイル名を表す英数字の文字列を含める必要があります。

### 設定例

次に、コンバージド課金の失敗処理アクションの構成例を示します。

```
profile nf-client-failure nf-type chf
profile failure-handling fh1
service name type nchf-convergedcharging
message type ChfConvergedchargingCreate
status-code httpv2 0
action continue
exit
```

# 緊急サービス サポート

## 機能説明

緊急サービスとは、緊急サービスをサポートするようにネットワークが構成されている場合に、サービスを提供しているネットワークによって提供される機能を指します。IMS 緊急セッションをサポートするために緊急サービスが提供されます。

4G および 5G に IMS 緊急サービスを実装するために、SMF は次の機能を実行します。

- SmContextCreate メッセージの要求タイプまたは DNN の緊急構成に基づいて、5G の緊急セッションを識別します。
- DNN の緊急構成に基づいて 4G の緊急セッションを識別します。
- SUPI/IMSI が認証され、**authorization local** コマンドが DNN プロファイルで構成されていない場合、UDM と対話します。それ以外の場合は、UDM との対話をスキップします。
- PEI または IMEI を使用した緊急サービスの PDU セッション確立を有効にします。
- 新しい構成を採用して、DNN を緊急 DNN として分類します。
- 緊急サービスの P-CSCF プロファイルの構成
- 緊急サービスの UPF の構成
- PCF からの専用ベアラーのティアダウン時に使用される緊急サービスとフローのみのタイマーのデフォルトの QoS プロファイルを構成します。

## 機能の仕組み

### 緊急サービス セッションの識別

**5G**

SMF は、AMF から SmContextCreate Message で受信した要求タイプ（「Initial Emergency Request」または「Existing Emergency PDU Session」）に基づいて、または DNN が緊急 DNN として構成されている場合に、緊急セッションを識別します。

**4G**

SMF は、IMSI の認証ステータスに基づいて緊急セッションを識別します。IMSI が認証されていない場合（UIMSI が 1 に設定されている）、セッションは緊急セッションと見なされます。

IMSI が認証され（UIMSI が 0 に設定）、SMF で DNN が緊急 DNN として（新しい CLI を使用して）構成されている場合、セッションは緊急セッションとして識別されます。

- 非緊急セッションの場合、SUPI または IMSI は必須です。
- 緊急セッションの場合：
  - 認証された SUPI または IMSI の場合、SUPI または IMSI は、現在の実装に基づいてセッション キーとして使用されます。
  - 認証されていない SUPI または IMSI の場合、PEI または IMEI は常にセッション キーとして使用されます。PEI または IMEI が存在しない場合、コールは拒否されます。

### 緊急セッションでの UDM インタラクション

1. SUPI または IMSI が認証されていない場合、SMF は UDM の相互作用をスキップします。
2. SUPI/IMSI が認証され、DNN 構成の「authorization」が「local」に設定されている場合、SMF は UDM の対話をスキップします。
3. SMF は、SUPI または IMSI が認証され、DNN 構成で「承認」がローカルに設定されていない場合、UDM と対話します。
   - UDM が拒否した場合、通話は却下されます。
   - UDM 交換が失敗した場合は、テンプレートのプロビジョニングを処理している UDM の失敗に基づいて、追加の処理が行われます。

**重要** SMF では、DNN プロファイルで「ローカル認証」が構成されているかどうかを考慮しません。

### 緊急セッションの構成

1. 既存の DNN、P-CSCF、UPF、および QoS プロファイルの構成は、緊急セッションで機能します。
2. CLI を使用して、DNN を緊急 DNN として分類します。
3. 「**authorization**」が（CLI を使用して）DNN で local に設定されている場合、UDM の連携動作は必要ありません。
4. デフォルトのフロー専用タイマー構成を使用してデフォルトのベアラーを保持し、PSAP コールバック セッションを有効にします。

### 要求タイプが「既存の緊急 PDU セッション」の場合の緊急サービスのサポート

1. 要求タイプが「Existing Emergency PDU Session」を示している場合、SMF はその要求が EPS（4G および WiFi）からの HO であると判断します。現在の実装では、要求タイプに「既存の緊急 PDU セッション」を使用した Wi-Fi から 5G HO への緊急セッション モビリティ、および N26 インターフェイスを使用した 4G から 5G HO への緊急セッション モビリティがサポートされている。
2. SMF は、PDU セッション ID に基づいて既存の PDU セッションを識別します。
3. SMF は、新しい SM を作成する代わりに、既存の SM コンテキストを更新して、更新された SM コンテキストの表現を応答内で AMF に提供します。これは、「既存の PDU セッション」の処理と同等です。

### 緊急サービス（専用ベアラー）のデフォルトのフローのみのタイマー

緊急サービスに制限された PDU セッションから 1 つまたは複数の PCC ルールを削除する HTTP POST メッセージを受信した場合：

- QoS フローにバインドされているすべての PCC ルールが削除されると、SMF は QoS フロー終了手順を開始します。
- QoS フローにバインドされているすべての PCC ルールが削除されていない場合、SMF は QoS フロー変更手順を開始します。

さらに、SMF はデフォルトの QoS フローの 5QI 以外の 5QI を持つすべての PCC ルール、または IMS シグナリングに使用される 5QI が緊急サービスに制限された PDU セッションから削除された場合にのみ、デフォルト フローを開始します（例： Public Safety Answering Point（PSAP）コールバック セッション）。デフォルトのフロー専用タイマーの期限が切れると、SMF は PDU セッション終了手順を開始します。

1. SMF は、PCF によって開始された変更手順によって専用ベアラ（音声/ビデオ）が削除されると、デフォルトのフローのみのタイマーを開始します。このタイマーの主な目的は、緊急セッションをしばらく保持して PSAP コールバックを容易にすることです。
2. デフォルトのフローのみのタイマーが期限切れになると、PCEF は IMS 緊急セッションの終了を開始します。
3. SMF は、新しいベアラーを作成するために PCF によって開始された変更要求を受信すると、デフォルトのフローのみのタイマーを停止します。

### EPS FB

gNB が QFI を拒否した場合、EPS フォールバックはアーム状態になります。SMfは、通常の緊急以外のセッションに対して実行されるように、EPS フォールバックを実行します。

### セッション キーとしての PEI の使用

SMF では、SUPI が存在しないか、認証されていない場合、PEI をセッション キーとして使用します。SMF での PduContext は、次の条件を満たす必要があります。

1. REST-EP は、メッセージを受信すると、SUPI と PEI に基づいてアフィニティをチェックします。最初のルックアップはSUPIで行われます。失敗した場合は、PEI でチェックします。

   または

   SUPI キーと PEI キーの両方を検索できます。

2. Smf-Service は、キーとして PEI を選択すると、PEI を使用してキャッシュ ポッドにアフィニティを設定します。
3. Smf-Service がキーとして PEI を使用して CDL レコードを挿入すると、PEI はプライマリ キー タイプとして追加されます。プライマリ キーは、SUPI + PduSessionid または PEI + PduSessionID のいずれかです。
4. 最初のトランザクション後、CDL ルックアップは、SUPI または PEI の両方で使用可能なもので行われます。
5. SEID は、PEI ハッシュを使用して生成されます。

# 緊急サービス サポートの構成

このセクションでは、緊急サービス サポートを構成する方法を説明します。

## DNN プロファイルでのデフォルトのフロー専用タイマーの構成

[デフォルトフロー専用タイマー（Default Flow Only Timer）] を構成するには、次の構成例を使用します：

```
config
   profile dnn profile_name
      timeout default-flow-only flow_only_timer
     end
```

注：

- **timeout default-flow-only** *flow_only_timer* ：PDU/PDN セッションの最大許容アイドル時間。この時間が経過すると、システムはそのセッションを自動的に終了します。*flow_only_timer* は、0 ～ 2147483647 ミリ秒の整数である必要があります。デフォルトは 0 で、機能が無効であることを示します。

## 緊急 DNN の構成

次の構成例を使用して、緊急 DNN を構成します：

```
config
   profile dnn profile_name
     emergency { false | true }
     end
```

注：

- **emergency {** いいえ | *true* **}**：dnn が緊急 DNN かどうかを示します。*false* | *true* は false または true である必要があります。デフォルトは false です。

## 緊急DNNの確認

次の show コマンドを使用して、Emergency DNN 構成を確認します。

**show subscriber all**

**show subscriber all** コマンドの出力例を次に示します。

```
subscriber-details
{
  "subResponses": [
    [
      "supi:imsi-123456789012345",
      "gpsi:msisdn-9999988888",
      "pei:imei-123456786666660",
      "psid:5",
      "dnn:intershat",
      "emergency:false",
      "rat:nr",
      "access:3gpp access",
      "connectivity:5g",
      "udm-uecm:209.165.202.131",
      "udm-sdm:209.165.202.151",
      "pcfGroupId:PCF-dnn=;",
      "pcf:209.165.202.151",
      "policy:2",
      "upf:209.165.202.151",
      "upfEpKey:209.165.202.151:209.165.202.150",
      "ipv4-addr:poolv4/209.165.200.225",
      "ipv4-pool:poolv4",
      "ipv4-range:poolv4/209.165.200.225",
      "ipv4-startrange:poolv4/209.165.200.225",
      "amf:209.165.202.151",
      "peerGtpuEpKey:209.165.202.151:209.165.202.158"
    ],
    [
      "gpsi:msisdn-9999988888",
      "pei:imei-352099001761480",
      "psid:6",
      "dnn:intershat",
      "emergency:true",
      "rat:nr",
      "access:3gpp access",
      "connectivity:5g",
      "pcfGroupId:PCF-dnn=;",
      "pcf:209.165.202.151",
      "policy:2",
      "upf:209.165.202.151",
      "upfEpKey:209.165.202.151:209.165.202.150",
      "ipv4-addr:poolv4/209.165.200.234",
      "ipv4-pool:poolv4",
      "ipv4-range:poolv4/209.165.200.225",
      "ipv4-startrange:poolv4/209.165.200.234",
      "amf:209.165.202.151",
      "peerGtpuEpKey:209.165.202.151:209.165.202.158"
    ]
  ]
}
```

「emergency」の値を使用して、サブスクライバに対して緊急サービス機能を有効または無効にします。

# 緊急サービスの OAM サポート

ここでは、この機能の操作、管理、およびメンテナンスに関して説明します。

## バルク統計サポート

緊急 SoS サポート機能では、次の統計情報がサポートされています。

- smf_session_counters：現在アクティブなセッション数を表示するようにゲージが更新されていることを示します。

  この統計には「emergency_call」ラベルが含まれます。このラベルのフラグが true に設定されている場合は、緊急通報を示します。

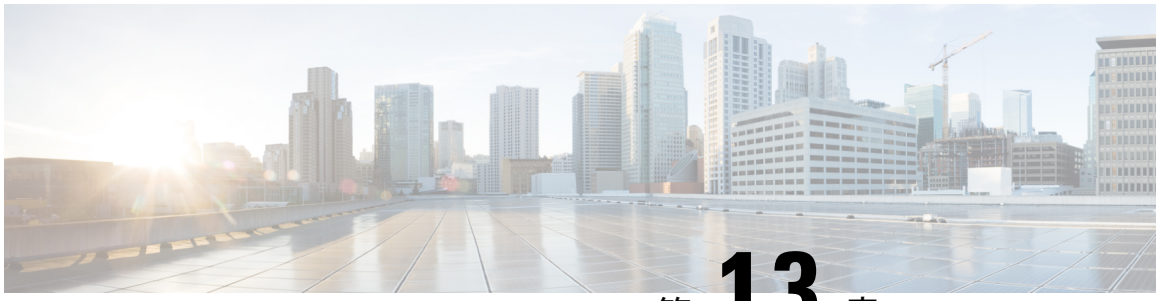
- smf_service_stats：SMF コール フロー手順カウンタを示します。

  この統計には「emergency_call」ラベルが含まれます。このラベルのフラグが true に設定されている場合は、緊急通報を示します。

- smf_service_resource_mgmt_stats：SMF サービス リソース管理の統計情報を示します。

  この統計には「emergency_call」ラベルが含まれます。このラベルのフラグが true に設定されている場合は、緊急通報を示します。

SMF のバルク統計情報のサポートの詳細については、「*UCC 5G SMF* メトリック リファレンス」を参照してください。



第 13 章

# EPS インターワーキング


- 機能の概要と変更履歴, on page 198
- 機能説明, on page 200
- アーキテクチャ, on page 201
- 機能の仕組み , on page 203
- 標準準拠, on page 205
- UE 初期接続のサポート, on page 205
- SMF での EPS の切り離し手順, on page 217
- 専用ベアラーのアクティブ化と非アクティブ化, on page 227
- EPS フォールバック, on page 235
- 間接データ転送トンネル（IDFT）タイマーのサポート （238 ページ）
- EPS フォールバック ガード タイマーのサポート （244 ページ）
- EPS フォールバック レポートの生成 （247 ページ）
- SMF での EPS セッションのベアラー変更 （250 ページ）
- EPS および 5GC インターワーキングのセッション管理手順, on page 267
- N26 インターフェイスを使用する 5G から EPS へのハンドオーバー, on page 298
- 専用ベアラの作成に対する遅延および再試行のサポート （301 ページ）
- タイマーの期限切れによる専用ベアラー手順エラーの処理 （304 ページ）
- 4G セッションの GTP-U エラー通知の処理 （313 ページ）
- GTP パス障害の処理、復元、およびリカバリ （317 ページ）
- 4G 専用デバイスを拒否するための構成サポート （324 ページ）
- 変更通知要求の処理 （325 ページ）
- ダイナミックな構成変更のサポート （330 ページ）
- 4G および 5G のセマンティックおよび構文エラー処理 （332 ページ）

# 機能の概要と変更履歴

## 要約データ

***Table 43:*** 要約データ

| | |
|---|---|
| 該当製品または機能エリア | SMF |
| 該当プラットフォーム | SMI |
| 機能のデフォルト設定 | 有効：常時オン |
| このリリースでの関連する変更点 | N/A |
| 関連資料 | 該当なし |

## 更新履歴

***Table 44:*** マニュアルの変更履歴

| 改訂の詳細 | リリース |
|---|---|
| 次のサポートが追加されました：<br>• PDU セッション確立での 2 オクテットの ePCO 長のオプションを使用した QoS ルールおよび QoS 記述の受信。<br>• 5G-4G インターネット ワーキングをサポートする PDU セッションでの 5G での PDU セッション確立中の S1 ノードの TFT のローカル IP アドレスの表示。<br>• QoS ルールと QoS の説明、または UE からのマッピングされた EPS ベアラー コンテキスト エラーのセマンティックおよび構文エラー処理。<br>• 5GSM の原因を含む ePCO で CB または UB 応答を処理します。<br>• PCF から GBR フロー作成または QoS 変更を受信する際に、MFBR 検証を必須にします。<br>• 4G UE の HSS によって開始された QoS の変更。 | 2023.04.0 |

| 改訂の詳細 | リリース |
| --- | --- |
| 次のサポートが追加されました。<br>• レガシー インターフェイスを使用する 4G コールの ULI で受信した変更通知要求用。<br>• 4G 用の代替 RAT トンネルの作成。<br>• RAT タイプの出力の変更に対して、4G コールの Show コマンドを追加しました。 | 2023.03.0 |
| 次に対するサポートが追加されました：<br>• Diameter インターフェイスを使用した E-UTRAN 初期接続手順。<br>• Diameterインターフェイスを使用したネットワーク開始型のデタッチ手順<br>• PCRF によって開始された CCAU または RAR<br>• S-GW の変更あり/なしによるベアラー変更要求<br>• UE 開始型デタッチ手順<br>• コンテキスト置換のサポート | 2023.02.0 |
| FB コール継続原因コードの拡張 | 2021.02.2 |
| 次に対するサポートが追加されました：<br>• セッション作成応答での APN-AMBR アクションの構成<br>• [コンテナ（Container）] フィールド：セッション作成応答の PCO、ePCO、または aPCO IE で 0005H（選択されたベアラー制御モード）<br>• GTP-C パス障害検出およびデバッグの改善<br>• GTP-C ピア再起動検出の改善<br>• 手順 SLA タイマーの期限切れ時に発生した専用ベアラー手順エラーの処理 | 2021.02.0 |
| アクセス プロファイル構成の動的構成をサポートする手順が導入されました。 | 2020.03.0 |
| 4G 専用 UE デバイスからのコールを拒否する DNN プロファイル構成の新しい CLI コマンド。 | 2020.02.1 |
| 最初の導入。 | 2020.02.0 より前 |

# 機能説明

### 5G コア ネットワークを介した EPS インターワーキング

コア ネットワークを介した EPS インターワーキングは、Evolved Packet System（EPS）、5G コア ネットワーク（5GC）、および Diameter インターフェイスとのインターワーキングに関する 3GPP 推奨事項に準拠する機能です。

**Important** この章で使用されている PGW-C という用語は、SMF によってサポートされている EPS インターワーキング機能を意味しており、LTE ネットワークで使用されるスタンドアロン P-GW として想定してはなりません。

この機能により、接続を維持しながら、4G（EPS）ネットワークと 5G ネットワーク間を移動できます。5G コア ネットワークを活用して、4G 環境で発信された可能性のあるセッションを管理します。

SMF は、説明されているように、4G と 5G の両方をサポートする UE からの接続を処理します

- UEはE-UTRAN と 5GC ネットワークに接続します。
- EPS インターワーキング機能を備えた SMF は SMF として機能し、S-GW の S5 または S8 インターフェイスを使用して 4G セッション要求の作成を受信します。
- SMF は、4G インターフェイス（Gx、Gy、Gz）を対応する 5GC サービス ベースのインターフェイス（Npcf および Nchf）に置き換えます。
- E-UTRAN、MME、および S-GW を使用して SMF で PDU セッションが作成された後、UE は E-UTRAN および 5G New Radio（NR）間でハンドオーバーできます。
- SMF は N26 インターフェイスを使用して EPS とインターワーキングします。N26 インターフェースは、MME と AMF 間の CN 間インターフェイスであり、S10インターフェイスの機能の一部をサポートし、相互接続を可能にします。

E-UTRAN、モビリティ管理エンティティ（MME）、およびサービング ゲートウェイ（S-GW）を使用して SMF で PDU セッションが作成された後、UE は E-UTRAN を 5G New Radio（NR）に渡すことができ、逆にします。

SMF は N26 インターフェイスを使用して EPS とインターワーキングします。このインターフェイスは、MME と AMF 間の CN 間インターフェイスであり、S10インターフェイスの機能の一部をサポートし、相互接続を可能にします。

UE は、サービスを提供しているコア ネットワークに応じて、EPC NAS または 5GC NAS の手順を使用します。

次に、E-UTRAN アクセス タイプの SMF Diameter インターフェイスのコール フロー手順を示します。

- Diameter インターフェイスを使用した E-UTRAN での初期接続, on page 208
- S-GW 変更によるベアラー要求の変更
- S-GW の変更がないベアラー変更要求
- PCRF によって開始された RAR
- SMF、UPF、PCRF、および RADIUS からのネットワークによって開始されたデタッチ
- UE によって開始されたデタッチ

**Note** SMF に搭載されている Diameter インターフェース機能は、StarOS または CUPS 製品と完全な機能互換性や機能性を有しているとは仮定すべきではありません。

さらに、このドキュメントで言及されている構成（コマンド、統計、属性、MIB オブジェクト、アラーム、ログ、サービスを含むがこれらに限定されない）が、StarOS レガシー製品または CUPS 以外の製品との機能的な同等性を示すと想定しないでください。

この製品と StarOS レガシー製品または CUPS 以外の製品間のパリティについてのご質問は、Cisco のアカウント担当者またはサポート担当者にお問い合わせください。

### 4G 向けの代替 RAT トンネルの作成

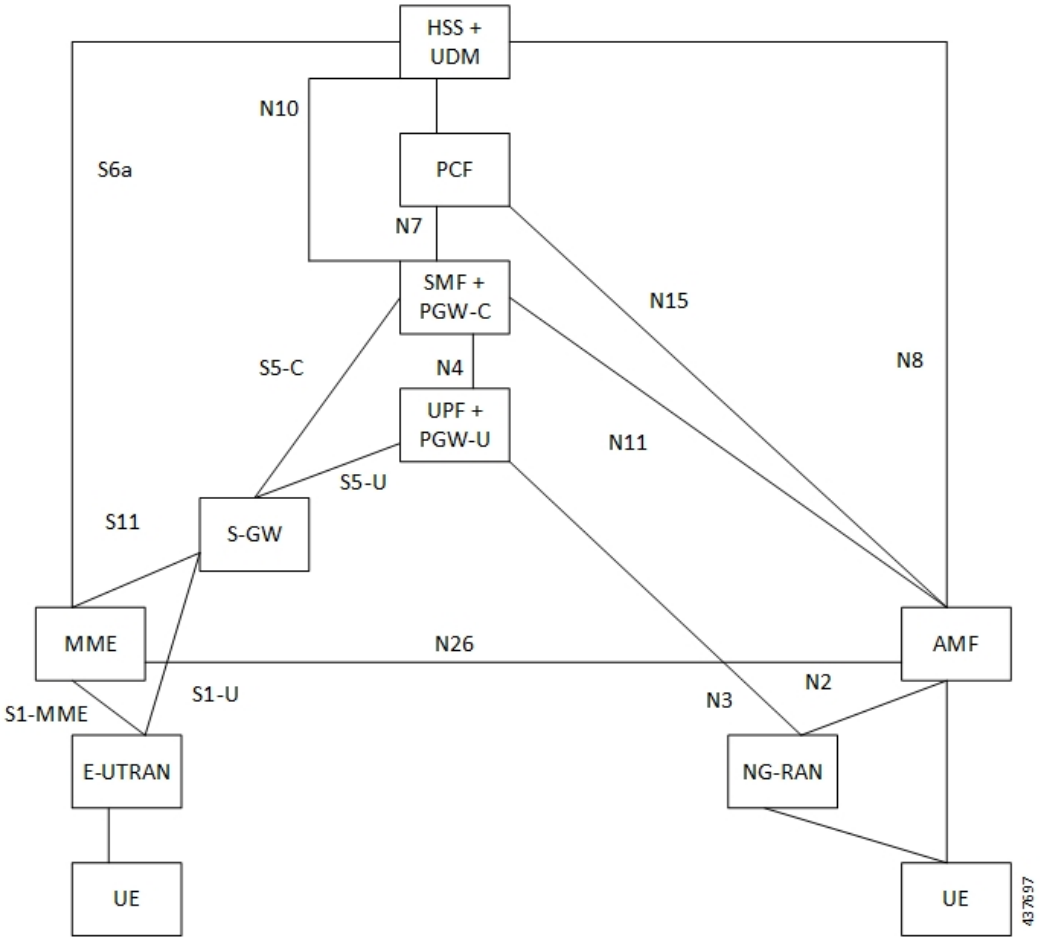
SMF は、4G 接続および専用ベアラーの手順のために、4G セッション中に代替 RAT トンネルを作成します。このトンネルは、サブスクライバが移行中に別の RAT に移動するときに再利用されます。

**Note**
- 代替 RAT トンネルの作成は、PLMN 間ハンドオーバー サポートの前提条件です。
- SMF は、EPS インターワーキングが有効な場合にのみ、代替 RAT トンネルを割り当てます。
- SMF は、4G 接続中に 4G 専用 UE に代替 RAT トンネルを割り当てません。

# アーキテクチャ

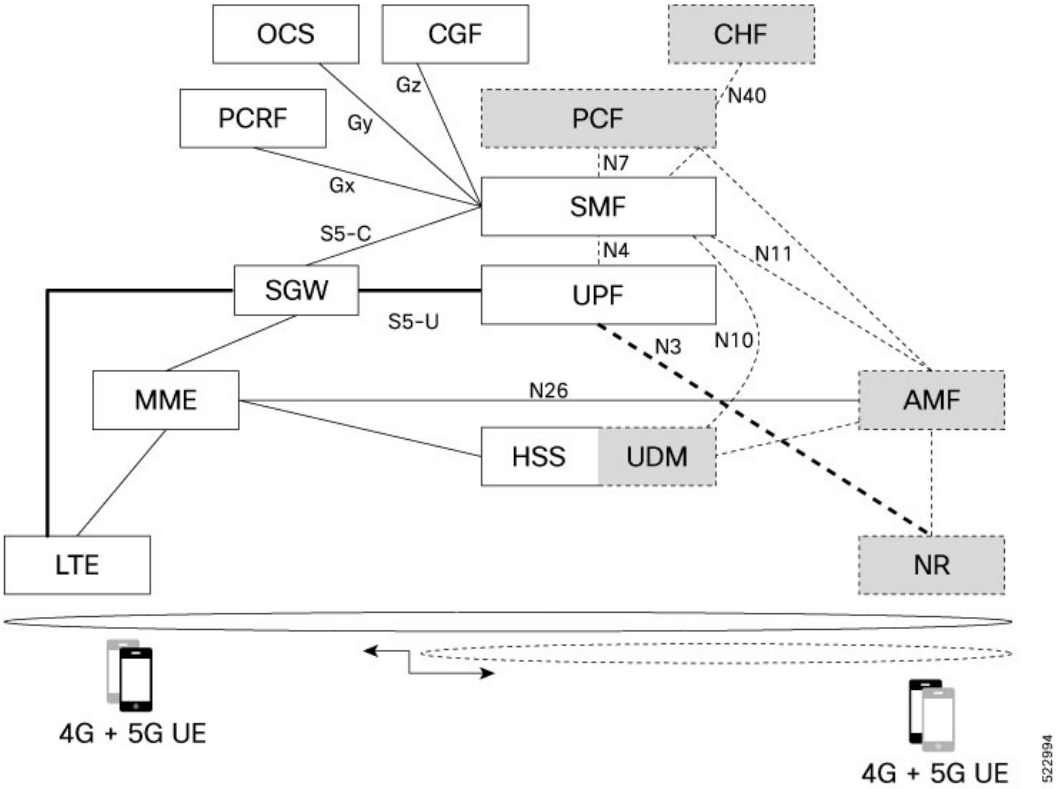
次の図は、EPS-5G コア と 4G インターワーキングのネットワークアーキテクチャを示しています。

*Figure 27: EPS-5GC インターワーキングのための 3GPP 非ローミングアーキテクチャ*




次のアーキテクチャ図は、ポリシーおよびオンラインチャージングにDiameterインターフェイスとオフラインチャージングに Gz を使用する SMF を示しています。UPF に対して N4 インターフェイスを使用します。このアーキテクチャ図では、グレー表示の要素は、4G 専用 UE には使用されない 5G ノードです。

*Figure 28: Diameter* および *GTPP* インターフェイスとの *SMF* インターワーキング




# 機能の仕組み

*Table 45:* 機能の履歴

| 機能名 | リリース情報 | 説明 |
|---|---|---|
| TFT での ePCO 長とローカル IP のサポート | 2023.04 | SMF では、QoS ルールと QoS の説明に 2 オクテットの ePCO 長を使用でき、TFT でローカル IP アドレスを示します。<br>**デフォルト設定**：有効 - 常にオン |

セカンダリ RAT NR を使用した EPS ベースのデュアル接続のみをサポートする UE。

- 最初のアクセスは常に E-UTRA（LTE-Uu）経由で実行されますが、NR 経由では実行されません。
- 3GPP TS 24.301 で定義されている E-UTRA を介した EPS NAS 手順（つまり、モビリティ管理、セッション管理など）を実行します。

5GC NAS を備えた 5G システムでのキャンペーンをサポートする UE：

- 5GC に接続する E-UTRAN または 5GC への NR を介して最初のアクセスを実行します。
- サポートされており必要な場合は、E-UTRAN を介して EPS への初期アクセスを実行します。
- UE が 5GC アクセスを要求するか、EPS アクセスを要求するかに応じて、E-UTRAN または NR を介して、EPS NAS または 5GC NAS の手順（つまり、モビリティ管理、セッション管理など）を実行します（UE も EPS NAS もサポートしている場合）。

EPS とのインターワーキングの場合、5GC と EPS NAS の両方をサポートする UE は次のいずれかのモードで動作できます。

- 単一登録モード：UE のアクティブ MM 状態（5GC の RM 状態または EPS の EMM 状態のいずれか）のみがあり、5GC NAS モードまたは EPS NAS モード（それぞれ 5GC または EPS に接続されている場合）のいずれかになります。
- デュアル登録モード：UE は、個別の RRC 接続を使用して 5GC と EPS の独立した登録を処理します。このモードでは、UE は 5GC のみ、EPS のみ、または 5GC と EPS の両方に登録できます。

EPS とのインターワーキングをサポートするネットワークは、N26 インターフェイスを使用するインターワーキング手順、または N26 インターフェイスを使用しないインターワーキング手順をサポートする場合があります。

- N26 をサポートするインターワーキング手順により、5GC NAS および EPS NAS をサポートし、シングル登録モードで動作する UE に対して、システム間モビリティに関する IP アドレスの連続性が提供されます。N26 インターフェイスを使用するインターワーキング手順により、ソース ネットワークとターゲット ネットワーク間で MM および SM の状態を交換できます。
- N26 のないインターワーキング手順をサポートするネットワークは、シングル登録モードとデュアル登録モードの両方で動作する UE にシステム間モビリティで IP アドレスの継続性を提供する手順をサポートします。N26 インターフェイスを使用しないインターワーキングの場合、IP アドレスの保持は、HSS + UDM を介して PGW-C + SMF および対応する APN または DNN 情報を保存およびフェッチすることにより、システム間モビリティの UE に提供されます。
- N26 インターフェイスをサポートするネットワークの S1 モードで動作する UE は、EPS とのインターワーキングをサポートするために、5G での PDU セッション確立手順中に TFT のローカル IP アドレスをサポートすることも示します。

**Important** SMF と EPS のインターワーキングは現在、N26 インターフェイスでのみ機能します。

# 標準準拠

5GC と EPS インターワーキング機能は、以下の基準に準拠しています：

- *3GPP TS 23.401*、バージョン *15.6.0*
- *3GPP TS 23.501*、バージョン *15.4.0*
- *3GPP TS 23.502*、バージョン *15.4.0*
- *3GPP TS 29.502*、バージョン *15.2.1*
- *3GPP TS 29.512*、バージョン *15.2.0*
- *3GPP TS 23.401*、バージョン *5.3.2.1*

# UE 初期接続のサポート

## 機能説明

SMF は、デフォルトのベアラーを作成するために MME および S-GW を介して E-UTRAN 上で初期接続を実行する UE をサポートします。

E-UTRAN または EPS での初期接続は、3GPP 仕様 23.401、セクション 5.3.2.1 で定義されている手順に従います。5G コアまたはレガシー GW を介した接続を有効にするために定義された手順からはいくつかの逸脱があります。価格偏差は次のとおりです。

- 手順のパケット データ ネットワーク ゲートウェイ（PGW-C）は、SMF に置き換えられます。
- IP-CAN セッションの確立と変更は、SM ポリシーの関連付けの確立手順に置き換えられます。
- Gy および Gz インターフェースを使用したオンラインおよびオフライン課金機能は、課金機能（CHF）を備えた Nchf インターフェイス経由の統合課金機能に置き換えられます。
- ユーザー プレーン ノードとのインターフェイスは、Sxb インターフェイスではなく N4 インターフェイスを経由します。

### Diameter インターフェイスとの SMF インターワーキング

UE は、5.3.2.1、23.401 で説明されているように、Diameter インターフェイスの E-UTRAN 初期接続手順をサポートしており、次の機能を提供します。

- デフォルト EPS ベアラーの確立
- Gx 参照ポイントは PCRF と SMF の間に配置されているため、SMF で事前定義された PCEF ルールをアクティブにします。これは、PCC ルールのプロビジョニングと削除に使用され

ます。Gx インターフェイスは、Diameter 接続として機能します。Gx メッセージには、ダイナミック ルールのインストール/削除、事前定義されたルール、APN-AMBR とデフォルトのベアラー QoS のアクティブ化と非アクティブ化を含みます。

# 機能の仕組み

## コール フロー

### E-UTRAN または EPS での初期接続の手順

次の図は、E-UTRAN または EPS での初期アタッチのための 3GPP リファレンスから派生したコール フローを示しています。

***Figure 29: 5G** コアを介した **E-UTRAN** での初期アタッチのコール フロー*

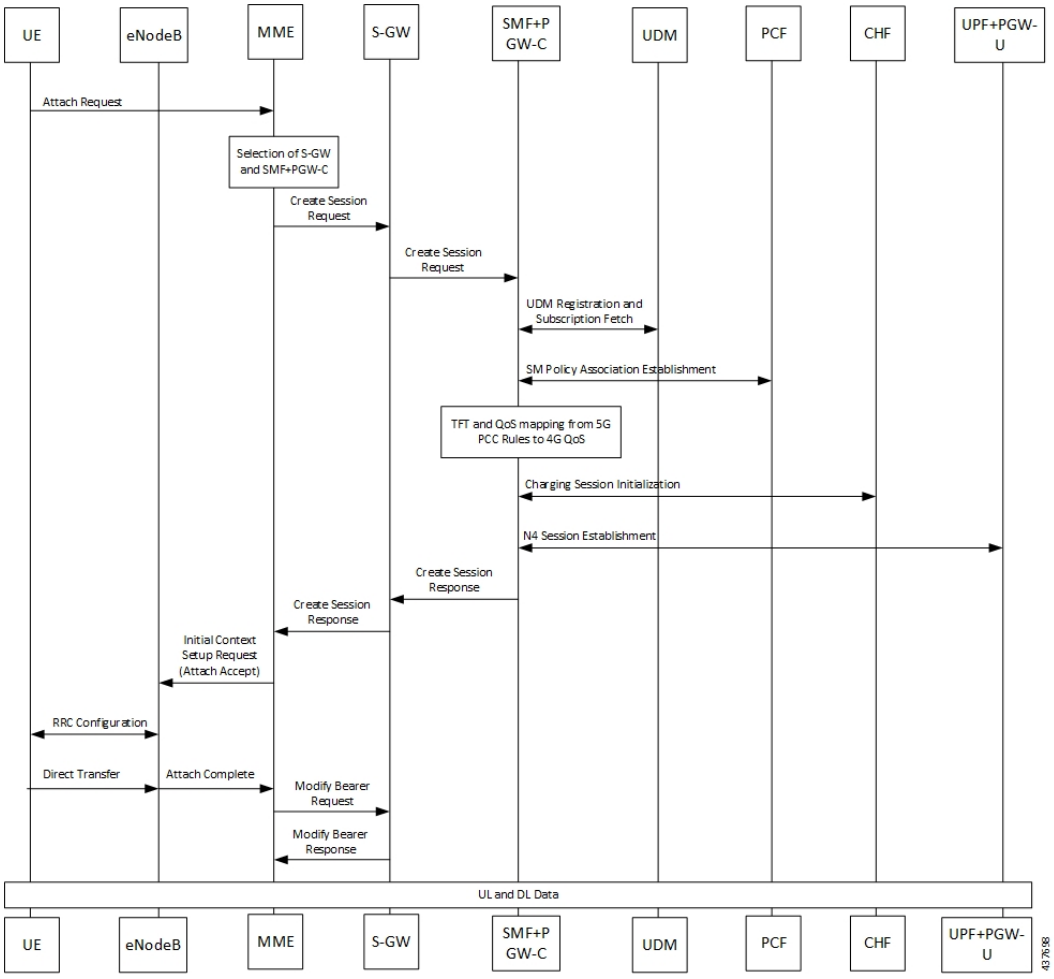


*Table 46: 5G コアを介した E-UTRAN での初期接続のコール フローの説明*

| ステップ | 説明 |
|---|---|
| 1 | UE は eNodeB を介して MME に接続要求を送信します。 |
| 2 | MME は、UE が NR へのハンドオフが可能であり、登録済みであることを判断します。この PDU セッションの PGW-C として SMF ノードを選択します。 |
| 3 | MME は、選択した S-GW にセッション作成要求を送信し、選択した SMF アドレスをそれに含めます。 |
| 4 | S-GW は、SMF に対するセッション要求の作成を開始します。 |
| 5 | SMF は、UE によって送信された PDU セッション ID をプロトコル構成オプション（PCO）001AH（PDU セッション ID）で抽出して保存します。次に、Unified Data Management（UDM）登録を実行し、PGW-C 完全修飾ドメイン名（FQDN）を UDM に送信します。登録後、SMF は UDM からのサブスクリプションの取得を開始します。 |
| 6 | SMF は Npcf_SMPolicyControl_Create を PCF に送信して、SM ポリシーの関連付けの確立を開始します。<br>SMF では、Create Session Request メッセージで受信した情報要素を次のように Npcf_SMPolicyControl_Create Service に含めます：<br>• SUPI には IMSI が含まれています。<br>• DNN には APN が含まれています。<br>• PEI には IMEI-SV が含まれています。<br>• セッション AMBR には APN-AMBR が含まれます。<br>• デフォルト QoS 情報には、デフォルトの EPS ベアラー QoS が含まれます。QCI 値は 5QI 値にマッピングされます。 |
| 7 | SMF は、ポリシー課金および制御（PCC）ルールと PDU セッションポリシー情報、PCC ルールおよび EPS QoS 情報にマッピングされた PDU セッション ポリシー情報で 5G QoS 情報を受信します。SMF は、PCC ルールで受信したサービス データ フィルタ（SDF）からトラフィック フローテンプレート（TFT）を作成し、対応するデフォルトおよび専用のベアラーに関連付けます。 |
| 8 | PCF から受信した課金ポリシーに基づいて、SMF は CHF に対して Nchf_ConvergedCharging_Create 操作を開始します。この手順は、5G セッションに似ており、PCF から受信した課金ルールに基づきます。 |

| ステップ | 説明 |
|---|---|
| 9 | SMF は UPF + PGW-U の選択と N4 セッション確立を実行します。これは SMF を接続する 4G セッションであるため、個別の CN トンネルが各ベアラーに作成され、QoS フロー ID（QFI）は QoS 適用ルール（QER）およびパケット検出ルール（PDR）で送信されません。 |
| 10 | SMF は S-GW に Create Session Response を送信し、デフォルトのベアラーに関するベアラー情報とトンネルエンドポイント ID（TEID）を含めます。SMF には、PCO および UE への ePCO オプション 001CH/0023H（QoS ルール）、001DH（セッション AMBR）、001EH（PDU セッションアドレスの有効期間）、および 001FH/0024H（QoS フローの説明）の 5G QoS パラメータも含まれます。<br>SMF はコンテナ識別子 0005H（選択されたベアラー制御モード）を PCO、ePCO、および aPCO IE の Create Session Response に入力します。コンテナ識別子コンテンツフィールド値 2 は、MS/NW モードが選択されていることを示しています。 |
| 11 | S-GW が、セッション作成応答を MME に送信します。 |
| 12 | MME は、初期コンテキスト設定要求を N1 接続承認メッセージとともに eNodeB に送信します。 |
| 13 | eNodeB と UE は、無線リソース制御（RRC）構成を実行します。 |
| 14 | UE が、Direct transfer メッセージを eNodeB に送信します。 |
| 15 | eNodeB は、初期コンテキストセットアップ応答で接続完了メッセージを、eNodeB の TEID とともに MME に送信します。 |
| 16 | MME が、eNodeB TEID とともに S-GW にベアラー変更要求を送信します。 |
| 17 | SMF が、ベアラー変更応答を S-GW に送信します。 |
| 18 | S-GW が、ベアラー変更応答を MME に送信します。 |

## Diameter インターフェイスを使用した E-UTRAN での初期接続

登録が必要なサービスを利用するには、UE をネットワークに登録する必要があります。

次の図は、 Diameter インターフェイス Gx および Gy を使用した E-UTRAN での初期接続の 3GPP リファレンスから派生したコール フローを示しています。

図 *30 : E-UTRAN* 初期接続のコール フロー

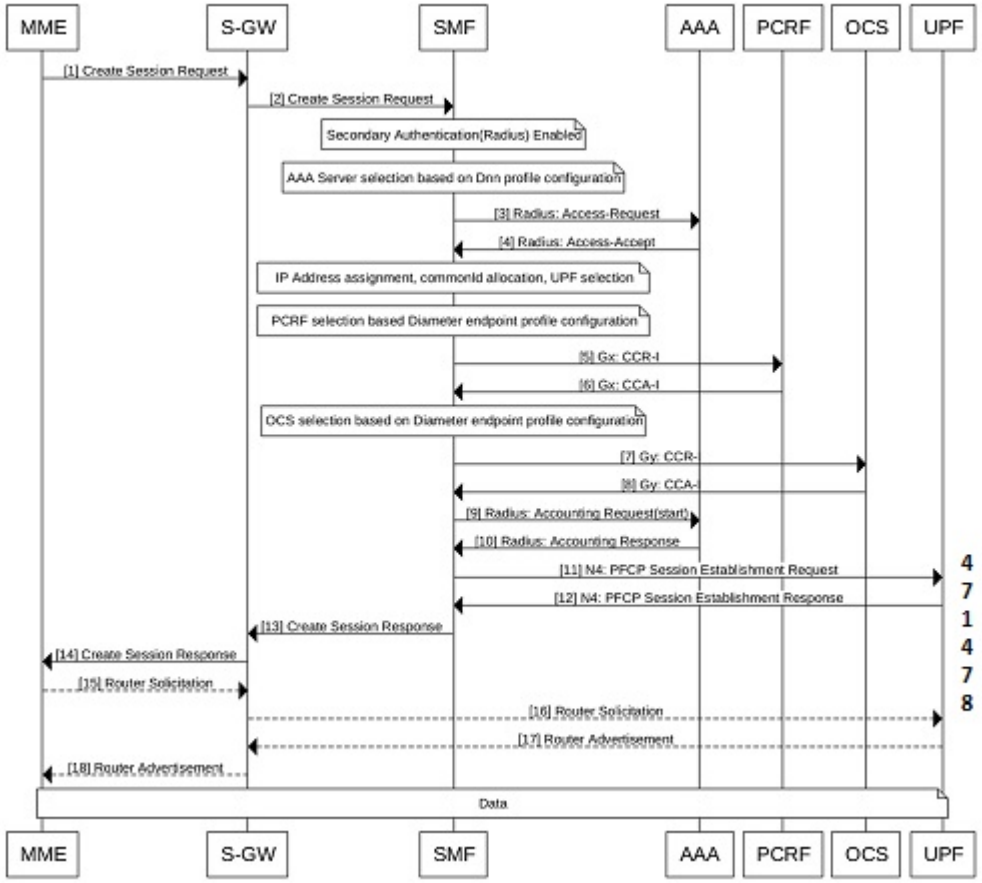



表 *47 : E-UTRAN* 初期接続のコール フロー説明

| 手順 | 説明 |
|---|---|
| 1 | MME がセッション作成要求を S-GW に送信します。 |
| 2 | S-GW は、セッション作成要求を SMF に送信します。 |
| （注）<br>このコール フローの一部として、RADIUS を使用したセカンダリ認証が DNN プロファイルで有効になり、AAA サーバが RADIUS プロファイル構成に基づいて選択されます。 | |
| 3 | SMF は、認証のために RADIUS Access-Request を AAA サーバに送信します。 |
| 4 | AAA サーバが SMF に Access-Accept を送信します。 |

| 手順 | 説明 |
|---|---|
| （注）<br>SMF により IP アドレス、 commonId の割り当て、および UPF の選択が割り当てられます。SMF は、Diameter エンドポイント プロファイルの構成に基づいて PCRF サーバを選択します。 | |
| 5 | SMF は、Gx クレジット制御要求の初期を PCRF サーバに送信してポリシーを要求します。 |
| 6 | PCRF サーバは、Gx クレジット制御応答の初期を SMF に送信します。 |
| （注）<br>SMF は、Diameter エンドポイント プロファイル構成に基づいて、Online Charging System（OCS）サーバを選択します。 | |
| 7 | SMF は、Gy Credit Control Request Initial を OCS サーバに送信し、クォータを要求します。<br>（注）<br>*diameter send-ccri traffic-start* が構成されていない場合、CCR-I は、デフォルトのベアラーの Gx 応答後にクォータ要求なしで OCS に送信されます。OCS から正常な応答があった場合、「初期接続」手順を続行します。 |
| 8 | OCS サーバが SMF に Gy Credit Control Answer Initial を送信します。 |
| 9 | SMF は Radius アカウンティングの開始要求を AAA サーバーに送信します。 |
| 10 | AAAサーバーは、Radiusアカウンティング応答をSMFに送信します。 |
| 11 | SMF は N4 PFCP セッション確立要求を UPF に送信して、PDR/FAR/QER/URR を作成します。 |
| 12 | UPF は、N4 PFCP セッション確立応答を SMF に送信します。 |
| 13 | SMF は、セッション作成応答を S-GW に送信します。 |
| 14 | S-GW がセッション応答の作成を MME に送信します。 |
| 15 | MME は、IPv6 コールでルータ要請を S-GW に送信します。 |
| 16 | S-GW は、IPv6 コールの UPF にルータ要請を送信します。 |
| 17 | UPF は、IPv6 コール用に S-GW にルータ アドバタイズメントを送信します。 |
| 18 | S-GW は、IPv6 コールの MME にルータ アドバタイズメントを送信します。 |

## コンテキスト置換コール フロー

SMF は、既存のサブスクライバが存在する既存の IMSI と EBI の組み合わせを持つセッション要求の作成（CSReq）を受信すると、コンテキスト置換手順をサポートします。

SMF は、既存のセッションの CSReq を 受信できます。新しい CSReq を 受信すると、新しい要求に基づいて、既存のセッションが新しいセッションに置き換えられます。コンテキスト置換手順は、create-over-create 手順とも呼ばれます。

このプロセスの最初のステップとして、既存のセッションの切断手順を開始します。その後、新しい要求に基づいてセッションを確立します。

次の図は、コンテキスト置換手順のコール フローを説明しています。

**図 *31 :* コンテキスト置換手順のコール フロー**

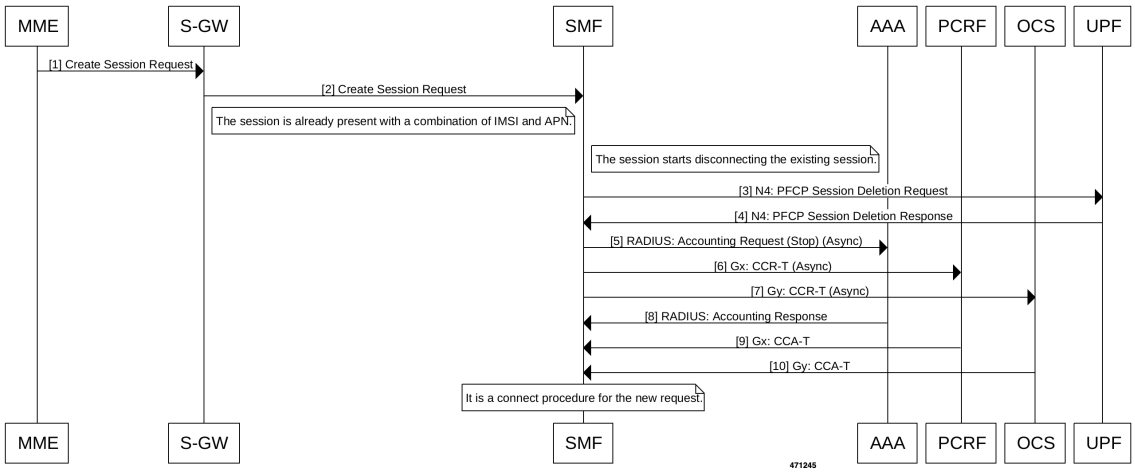



**表 *48 :* コンテキスト置換手順のコール フローの説明**

| ステップ | 説明 |
|---|---|
| 1 | MME がセッション要求の作成を S-GW に送信します。 |
| 2 | S-GW は SMF にセッション要求の作成を送信します。<br>（注）<br>この IMSI と EBI の組み合わせには、古いセッションがすでに存在していました。既存のセッションの切断手順が開始されます。 |
| 3 | SMF は PCRF セッション削除要求を UPF に送信します。 |
| 4 | UPF は N4 PFCP セッション削除応答を SMF に送信します。 |
| 5 | SMF は Async RADIUS Accounting-Request Stop を AAA サーバに送信します。 |
| 6 | SMF は PCRF に非同期 Gx CCR-T を送信します。 |
| 7 | SMF は OCS に非同期 Gy CCR-T を送信します。 |

| ステップ | 説明 |
|---|---|
| 8 | AAA サーバは、SMF に Radius アカウンティング応答を送信します。 |
| 9 | 次に、PCRF は Gx CCA-T を SMF に送信します。 |
| 10 | OCS は SMF に Gy CCA-T を送信します。<br>（注）<br>このアクションの後、接続手順は新しい要求に対して続行されます。 |

（注） ステップ 8 ～ 10 で概説した応答メッセージの順序は、可用性に応じて変更される可能性があります。

# UE 初期接続の構成

ここでは、UE 初期接続を構成する方法について説明します。

UE 初期接続構成には、次の手順が含まれます：

1. SMF プロファイル構成で FQDN を定義する
2. SMF サービス構成での S5 バインディング アドレスの構成
3. SMF GTP エンドポイント ポッドの Kubernetes 構成の有効化

## SMF プロファイル構成で FQDN を定義する

SMFの FQDN を指定するには、次の構成を使用します。構成された FQDN は、登録時に UDM に送信されます。

```
config
   profile smf smf_profile_name
   instances instance_id fqdn fqdn_name
      end
```

注：

- **instances** *instance_id* **fqdn** *fqdn_name*： ローカルまたはリモート インスタンスに対応する PGW-C FQDN を構成します。*fqdn_name* は 英数字の文字列である必要があります。

## S5 バインディング アドレスの構成

SMF が S-GW（S5 インターフェイス）からの GTP メッセージをリッスンする S5 バインディング アドレスを定義するには、次の構成例を使用します。

```
config
  instance instance-id instance_id
    endpoint gtp
      replicas replica_count
      nodes node_id
      enable-cpu-optimization true
      interface s5
      vip-ip vip_ip_address
      exit
    interface s5e
      echo
      vip-ip vip_ip_address
      exit
    interface s2b
      vip-ip vip_ip_address
      end
```

注：

- **interface s5**：メッセージが S-GW から SMF に送信されるときに経由する S5 インターフェイスを構成します。
- **vip-ip** *vip_ip_address*：SMF が S5 インターフェイスを介して S-GW からの GTP メッセージをリッスンする IP アドレスを入力します。標準の IPv4 のドット付き 10 進形式または標準の IPv6 コロン表記形式のいずれかでアドレスを入力します。

## GTP エンドポイント パラメータの構成

次の構成例を使用して、GTP エンドポイントのパラメータを定義します。

```
config
   instance instance-id gr_instance_id
      endpoint gtp
         replicas replica_count
         vip-ip ipv4_address
         vip-ipv6 ipv6_address
         end
```

注：

- **endpoint gtp**：GTP エンドポイント構成を入力します。
- **replicas** *replica_count*：ノードごとに作成するレプリカの数を入力します。デフォルト値は 1 です。
- **vip-ip**：GTP エンドポイントの IPv4 アドレスを指定します。
- **vip-ipv6**：GTP エンドポイントの IPv6 アドレスを指定します。

# CSR での APN-AMBR の構成

SMF は、セッション要求の作成で APN-AMBR を受信しない場合、または PCF ネゴシエーションの一環として値が変更された場合に、セッション応答の作成で APN-AMBR を送信します。アクセス プロファイルでの構成は、この動作を上書きします。

以下の構成例を使用して、セッション応答の作成で APN-AMBR アクションを構成します。す。

```
config
  profile access access_profile_name
    gtpc message-handling create-session-response action apn-ambr
    exit
```

注：

- **action apn-ambr**：GTPC メッセージの APN-AMBR アクションを指定します。

# PCRF、PCF、および OCS インターフェイスの構成

dnnprofile の下にポリシープロファイルを追加して、5G サブスクライバ（N7 または N40 インターフェイス）と 4G サブスクライバ（Gx、Gy/Gz）を構成できます。

重要　Gx（PCRF）、Gy（OCS）、Gz（CGF）、または N40（CHF）が有効になっていない場合、SMF はこれらのインターフェイスと対話しません。

## PCRF インターフェイスの構成

次のコマンドを使用して、PCRF インターフェイスを構成します。

```
config
  profile dnn dnnprofile-ims
  network-element-profiles pcrf pcrf pcrf1
    exit
```

注

- **network-element-profiles pcrf** *pcf1*：PCRF メッセージ処理プロファイルの構成を指定します。

## PCF インターフェイスの構成

次のコマンドを使用して、PCF インターフェイスを構成します。

```
config
  profile dnn dnnprofile-ims
  network-element-profiles pcf pcf nfprf-pcf1
    exit
```

注

- **network-element-profiles pcf** *pcf nfprf-pcf1* ：PCF メッセージ処理プロファイル構成を指定します。

### OCS インターフェイスの構成

次のコマンドを使用して、OCS インターフェイスを構成します。

```
config
  profile dnn dnnprofile-ims
  network-element-profiles ocs  ocs1
    exit
```

注

- **network-element-profiles ocs***ocs1* ：OCS メッセージ処理プロファイルの構成を指定します。

# UE 初期接続構成の確認

このセクションでは、UE 初期接続構成を確認する方法を説明します。

以下の構成は、 **show running-config** コマンドの出力例です：

```
show running-config
.
.
.
profile smf smf1
 node-id          ABC123
 bind-address ipv4 209.165.200.230
 bind-port        8008
instances 1  allowed-nssai  [ slice1 ]
 plmn-id mcc 123
 plmn-id mnc 456
 fqdn ciscosmf1
 service name nsmf-pdu
  type               pdu-session
  .
  .
  .
  n4 bind-address ipv4 209.165.200.240
  s5 bind-address ipv4 209.165.200.240
  http-endpoint base-url http://smf-service
.
.
.
k8 smf local redis-endpoint redis-primary:6379
k8 smf local service no-of-replicas 1
k8 smf local nodemgr no-of-replicas 1

.
.
.
```

# OAM サポート

ここでは、この機能の操作、管理、およびメンテナンスに関して説明します。

## show コマンドのサポート

**show subscriber supi imsi** *imsi_value* **nf-service smf full** コマンドを使用して、4G コールのサブスクライバの詳細に関連する構成を表示します。

次に出力例があります。

```
smf# show subscriber supi imsi-123456789012345 nf-service smf full
subscriber-details
{
  "subResponses": [
    {
      "status": true,
      "genericInfo": {
        "supi": "imsi-123456789012345",
        "pei": "imeisv-1122334455667788",
        "pduSessionId": 69,
        "pduSesstype": "Ipv4V6PduSession",
        "accessType": "3GPP_ACCESS",
        "dnn": "intershat",
        "plmnId": {
          "mcc": "123",
          "mnc": "765"
        },
        "sScMode": 1,
        "allocatedIp": "12.0.0.4",
        "allocatedIpv6": "2001:db0:0:2003::",
        "allocatedIntfid": "tG1H//5HR0c=",
        "eUtranLocation": {
          "ecgi": {
            "mcc": "214",
            "mnc": "365",
            "eutraCellId": "1234567"
          },
          "tai": {
            "mcc": "214",
            "mnc": "365",
            "tac": "6789"
          },
          "ueLocationTimestamp": "2022-08-08T13:16:09Z"
        },
        "alwaysOn": "None",
        "dcnr": "None",
        "wps": "Non-Wps Session",
        "ratType": "EUTRA",
        "ueType": "4G Capable UE",
        "sessTimeStamp": "2022-08-08 13:16:09.107469768 +0000 UTC",
        "callDuration": "3.531530696s",
        "ipPool": "poolv4",
        "ipv6Pool": "poolv6",
        "commonId": 2097156,
        "linkedEbi": 5,
        "snssai": {
          "sd": "Abf123",
          "sst": 2
        },
        "authStatus": "Unauthenticated",
        "roamingStatus": "Roamer",
```

```
        "uePlmnId": {
          "mcc": "123",
          "mnc": "456"
        },
      }
    }
  ]
}
```

（注） 上記の出力例では、4G コールの場合、RAT タイプは「EUTRA」と表示されます。

# SMF での EPS の切り離し手順

## 機能説明

**5G コア ネットワークを介した EPS インターワーキング**

SMF は、E-UTRAN、MME、および S-GW を介して接続された UE のデフォルトのベアラー削除手順をサポートしています。

**Diameter インターフェイスとの SMF インターワーキング**

UE が E-UTRAN に接続されている場合、SMF は Diameter インターフェイスを使用した次のネットワーク開始型切断手順をサポートします。

- SMF によって開始されたデタッチ手順
- UPF によって開始されたデタッチ手順
- PCRF によって開始されたデタッチ手順
- UE によって開始されたデタッチ手順
- RADIUS によって開始されたデタッチ手順

## 機能の仕組み

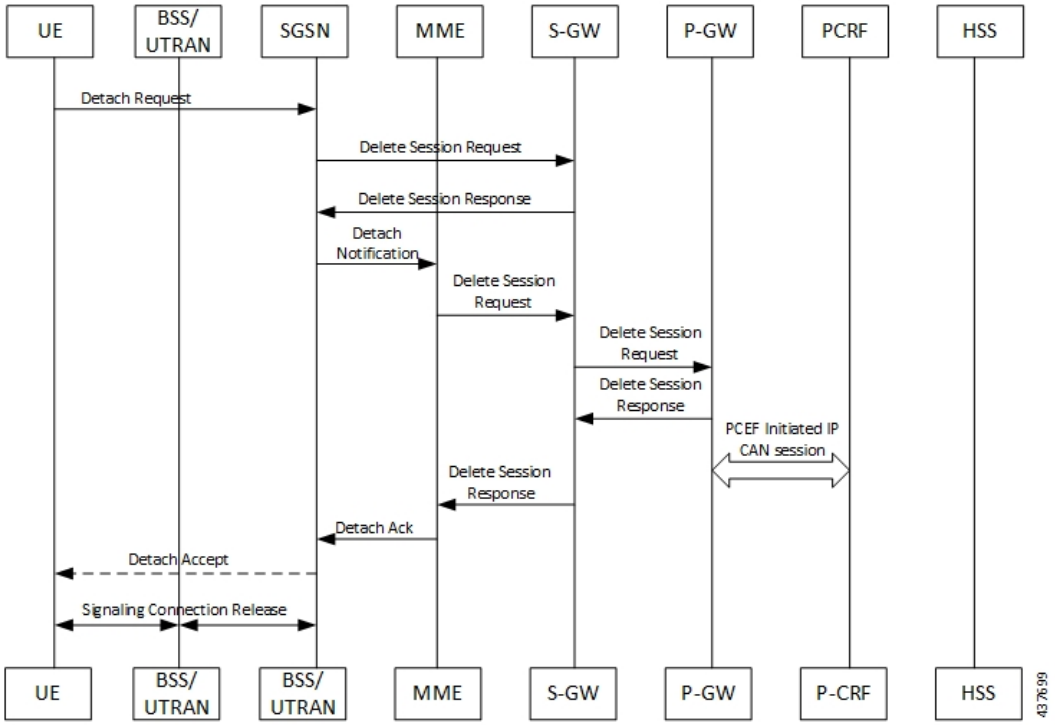
### コール フロー

ここでは、この機能に関連したコール フローについて説明します。

#### *UE* により開始された *EPS* コールのリリース手順

次の図は、EPS コールの UE によって開始されるリリースのコール フローを示しています。

*Figure 32: UE* により開始された *EPS* コール リリース フロー



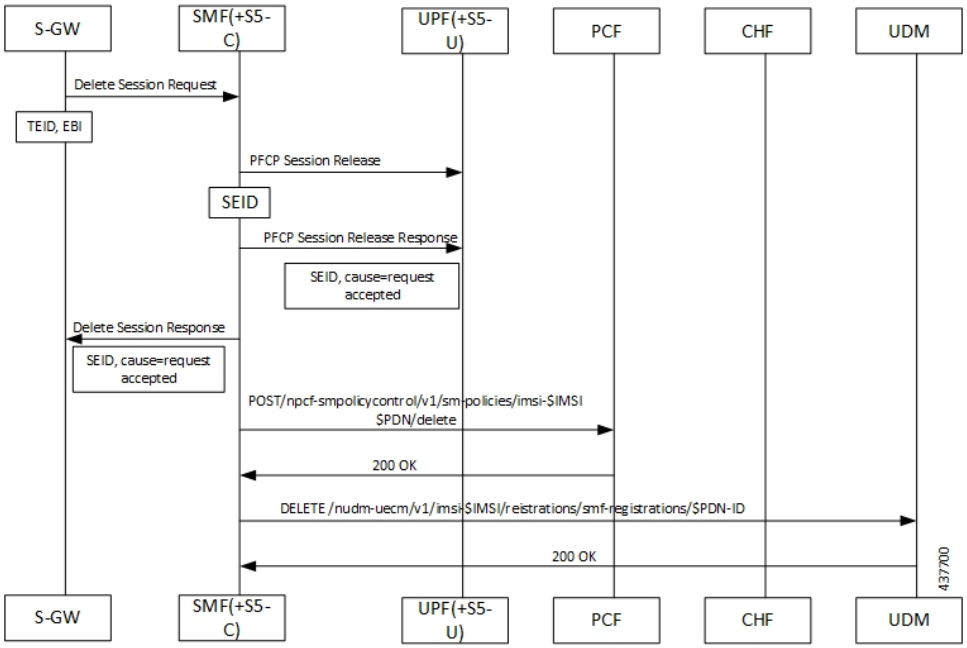

EPS の切り離し手順は、3GPP 23.401、セクション 5.3.8 で定義されています。UE が E-UTRAN に接続されている場合、デタッチ手順は、次の変更を除き、指定された 3GPP セクションに記載されているものと同じです。

- PGW-C と PCRF 間の PCEF によって開始される IP-CAN セッションである PCRF（CCR-T）に対する対話は、SMF から PCF への Npcf_SMPolicyControl_Update 要求に置き換えられます。このメッセージで送信されるパラメータは、最初の接続用のセッション要求の作成メッセージと同様の方法で、セッション要求コンテンツの削除からのマッピングに従います。
- すべての Gy および Gz インターフェイス メッセージは、Nchf_ConvergedCharging_Release サービス操作に置き換えられます。
- ユーザー プレーン リソースは、UPF に対する N4 セッション リリース手順を使用して削除されます。

## *UE* によって開始されたコール リリースの詳細な手順

次の図は、UE によって開始される EPS コールのリリースの詳細な手順を示しています。

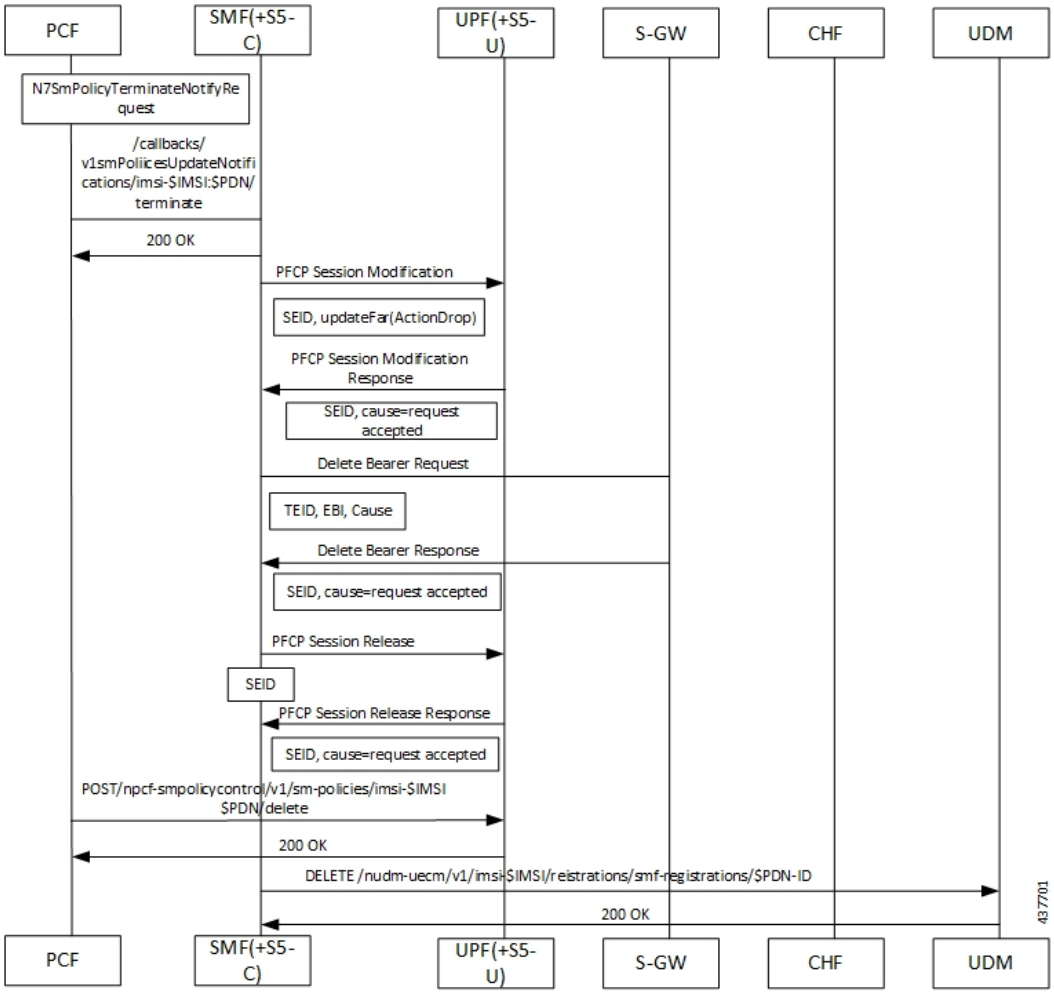
*Figure 33: UE* が開始する *EPS* コール リリースの詳細なコール フロー




## *PCF* によって開始されたコール リリースの詳細な手順

次の図は、UE によって開始される EPS コールのリリースの詳細な手順を示しています。

*Figure 34: PCF* が開始する *EPS* コール リリースの詳細なコール フロー




*Diameter* インターフェイスを使用したネットワーク開始型のデタッチ手順

ここでは、ネットワークによって開始されたデタッチの通話フローと手順について説明します。

SMF によって開始された切断手順

SMF は、次のいずれかの方法でセッションの解放要求を受信します：

- サブスクライバをクリア
- GTP パス障害
- ピアの再起動
- 絶対セッション タイムアウト
- Cp アイドル タイムアウト

次のコール フローは、E-UTRAN ネットワーク（SMF）が開始した切断の手順を示しています。

**図 *35 : SMF* によって開始されたデタッチのコール フロー**

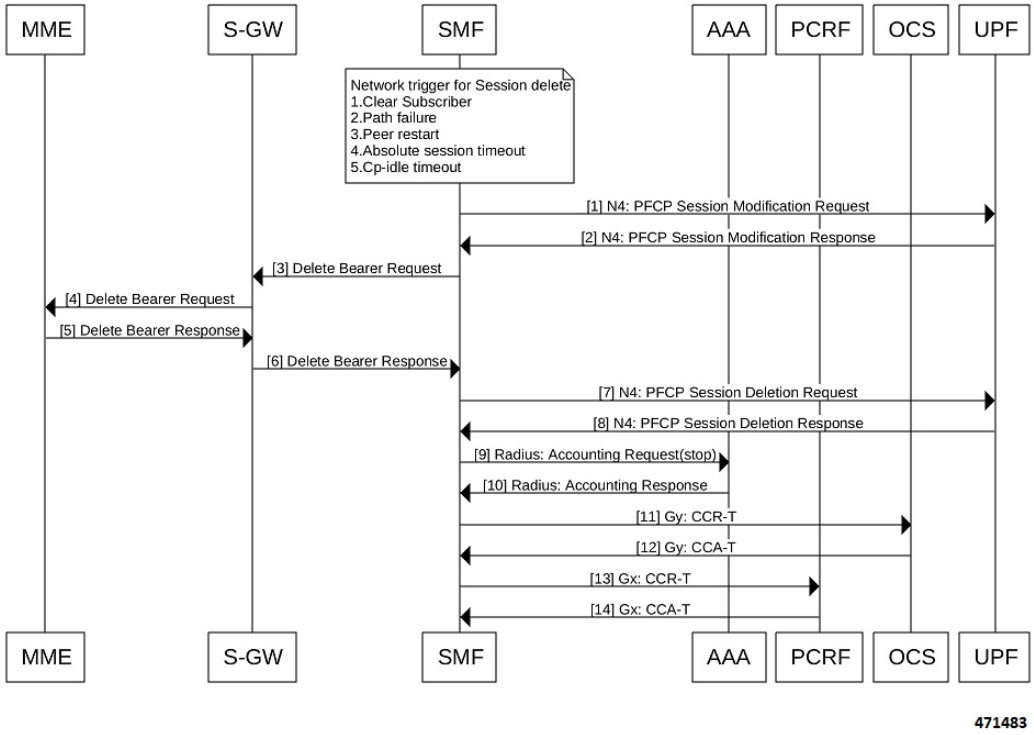



**表 *49 : SMF* によって開始されたデタッチのコール フローの説明**

| 手順 | 説明 |
|---|---|
| 1 | SMF は、適用アクションがドロップに設定された FAR を使用して、N4 PFCP セッション変更要求を UPF に送信します |
| 2 | UPF が SMF に N4 PFCP セッション変更応答を送信します。 |
| 3 | SMF が S-GW にベアラーの削除要求を送信します。 |
| 4 | S-GW が MME にベアラー要求の作成を送信します。 |
| 5 | MME が S-GW にベアラー応答の削除を送信します。 |
| 6 | S-GW が SMF にベアラー応答の削除を送信します。 |
| 7 | SMF は、N4 PFCP セッション削除要求を UPF に送信して N4 セッションを解放します。 |
| 8 | UPF は N4 PFCP セッション削除応答を SMF に送信します。 |

| 手順 | 説明 |
|---|---|
| 9 | SMF は、Radius アカウンティング要求の停止を AAA サーバーに送信して、アカウンティング セッションを解放します。 |
| 10 | AAA サーバが Radius アカウンティング応答を SMF に送信します。 |
| 11 | SMF は、Gy セッションを解放するために Gx クレジット制御要求の終了を OCS に送信します。 |
| 12 | OCS が SMF に Gx クレジット制御応答終了を送信します。 |
| 13 | SMF は、Gx セッションを解放するために、Gx クレジット制御要求の終了を PCRF に送信します。 |
| 14 | PCRF は SMF に Gx クレジット制御応答終了を送信します。 |

## UPF によって開始されたデタッチ手順

次のコール フローは、E-UTRAN ネットワーク（UPF）が開始した切断を示しています。

**図 *36 : UPF* によって開始されたデタッチのコール フロー**

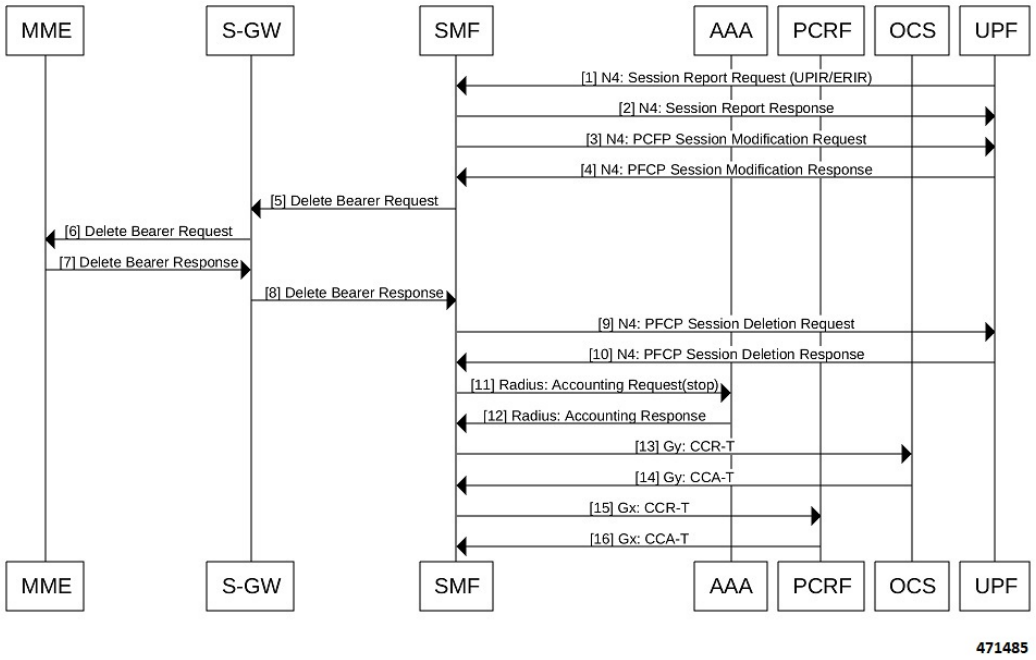



**表 *50 : UPF* によって開始されたデタッチのコール フローの説明**

| 手順 | 説明 |
|---|---|
| 1 | UPF は N4 セッション レポート要求（ERIR[default bearer]/UPIR）を SMF に送信します。 |

| 手順 | 説明 |
|---|---|
| （注）<br>UPF で GTP-U エラー通知が受信されたときに、タイプ ERIR のセッションレポート要求を受信したことを示します。UPF で UPF 非アクティブ タイマーが期限切れになると、UPIR タイプのセッション レポート要求を受信します。（ERIR がデフォルトのベアラーで受信された場合）どちらの場合でもセッションが終了します。 | |
| 2 | SMF が N4 セッション レポート応答を UPF に送信します。 |
| 3 | SMF は、適用アクションがドロップに設定された FAR を使用して、N4 PFCP セッション変更要求を UPF に送信します |
| 4 | UPF が SMF に N4 PFCP セッション変更応答を送信します。 |
| 5 | SMF が S-GW にベアラーの削除要求を送信します。 |
| 6 | S-GW が MME にベアラー要求の作成を送信します。 |
| 7 | MME が S-GW にベアラー応答の削除を送信します。 |
| 8 | S-GW が SMF にベアラー応答の削除を送信します。 |
| 9 | SMF は、N4 PFCP セッション削除要求を UPF に送信して N4 セッションを解放します。 |
| 10 | UPF は N4 PFCP セッション削除応答を SMF に送信します。 |
| 11 | SMF は、Radius アカウンティング要求の停止を AAA サーバーに送信して、アカウンティング セッションを解放します。 |
| 12 | AAA サーバーが Radius アカウンティング応答を SMF に送信します。 |
| 13 | SMF は、Gy セッションを解放するために Gy クレジット制御要求の終了を OCS に送信します。 |
| 14 | OCS が SMF に Gy クレジット制御応答終了を送信します。 |
| 15 | SMF は、Gx セッションを解放するために、Gx クレジット制御要求の終了を PCRF に送信します。 |
| 16 | PCRF は SMF に Gx クレジット制御応答終了を送信します。 |

## PCRF によって開始されたデタッチ手順

次のコール フローは、E-UTRAN ネットワーク（PCRF）が開始した切断の手順を示しています。

図 *37 : PCRF* によって開始されたデタッチのコール フロー

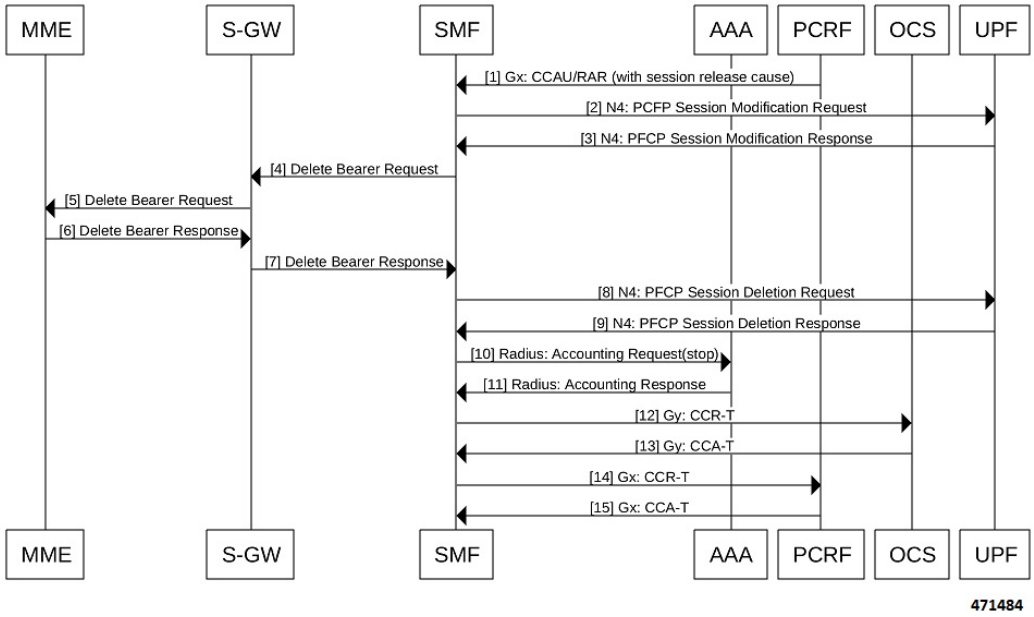



表 *51 : PCRF* によって開始されたデタッチのコール フローの説明

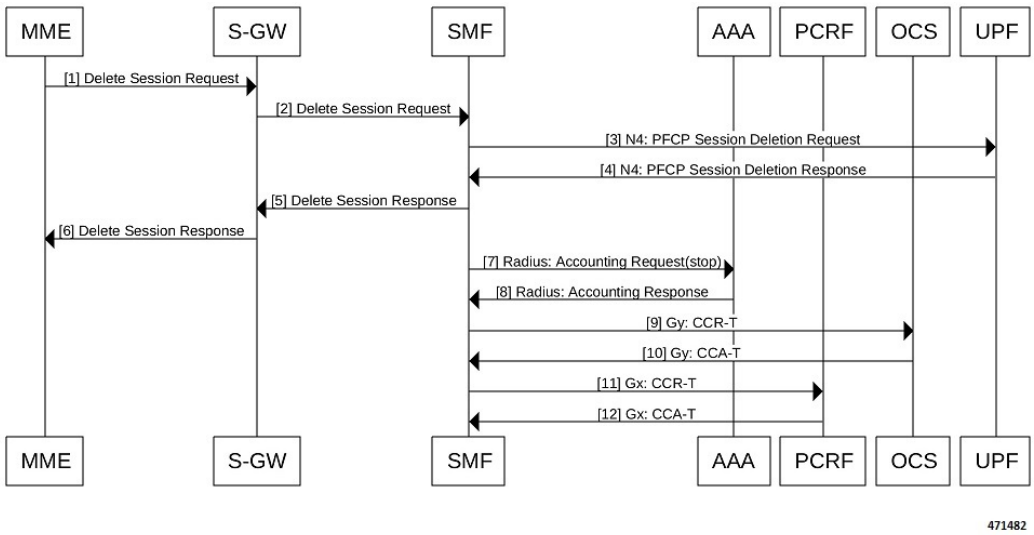
| 手順 | 説明 |
|---|---|
| 1 | PCRF は、セッション リリース原因を含む Gx クレジット制御応答または RAR を SMF に送信します。 |
| 2 | SMF は、適用アクションがドロップに設定された FAR を使用して、N4 PFCP セッション変更要求を UPF に送信します。 |
| 3 | UPF が SMF に N4 PFCP セッション変更応答を送信します。 |
| 4 | SMF が S-GW にベアラーの削除要求を送信します。 |
| 5 | S-GW が MME にベアラー要求の作成を送信します。 |
| 6 | MME が S-GW にベアラー応答の削除を送信します。 |
| 7 | S-GW が SMF にベアラー応答の削除を送信します。 |
| 8 | SMF は、N4 PFCP セッション削除要求を UPF に送信して N4 セッションを解放します。 |
| 9 | UPF は N4 PFCP セッション削除応答を SMF に送信します。 |
| 10 | SMF は、RADIUS アカウンティング要求の停止を AAA サーバに送信して、RADIUS セッションを解放します。 |
| 11 | AAA サーバが RADIUS アカウンティング応答を SMF に送信します。 |

| 手順 | 説明 |
|---|---|
| 12 | SMF は、Gy セッションを解放するために Gx クレジット制御要求の終了を OCS に送信します。 |
| 13 | OCS が SMF に Gx クレジット制御応答終了を送信します。 |
| 14 | SMF は、Gx セッションを解放するために、Gx クレジット制御要求の終了を PCRF に送信します。 |
| 15 | PCRF は SMF に Gx クレジット制御応答終了を送信します。 |

UE によって開始された切断手順

次の図は、Diameter インターフェイスの UE によって開始されるリリースのコール フローを示しています。

**図 *38 : Diameter* インターフェイスを使用した *UE* 開始リリースのコール フロー**




次の表に、E-UTRAN UE 開始のデタッチの詳細な手順を示します。

**表 *52 : Diameter* インターフェイスを使用した *UE* 開始型リリースのコール フローの説明**

| 手順 | 説明 |
|---|---|
| 1 | MME が S-GW に「セッション削除要求」を送信します。 |
| 2 | S-GW は、セッション要求の削除を SMF に送信します。 |
| 3 | SMF は、N4 PFCP セッション削除要求を UPF に送信して N4 セッションを解放します。 |
| 4 | UPF は N4 PFCP セッション削除応答を SMF に送信します。 |

| 手順 | 説明 |
|---|---|
| 5 | SMF は、セッション応答の削除を S-GW に送信します。 |
| 6 | S-GW はセッション応答の削除を MME に送信します。 |
| 7 | SMF は、Radius アカウンティング要求の停止を AAA サーバに送信して、アカウンティング セッションを解放します。 |
| 8 | AAA サーバが RADIUS アカウンティング応答を SMF に送信します。 |
| 9 | SMF は、Gy セッションを解放するために Gy クレジット制御要求の終了を OCS に送信します。 |
| 10 | OCS が SMF に Gy クレジット制御応答終了を送信します。 |
| 11 | SMF は、Gx クレジット制御要求の終了を PCRF に送信します。 |
| 12 | PCRF は、Gx セッションを解放するために、Gx クレジット制御回答の終了を SMF に送信します。 |

RADIUS によって開始されたデタッチ手順

次の図に、E-UTRAN RADIUS 切断メッセージのコール フローを示します。

**図 *39 : RADIUS* によって開始されたデタッチのコール フロー**

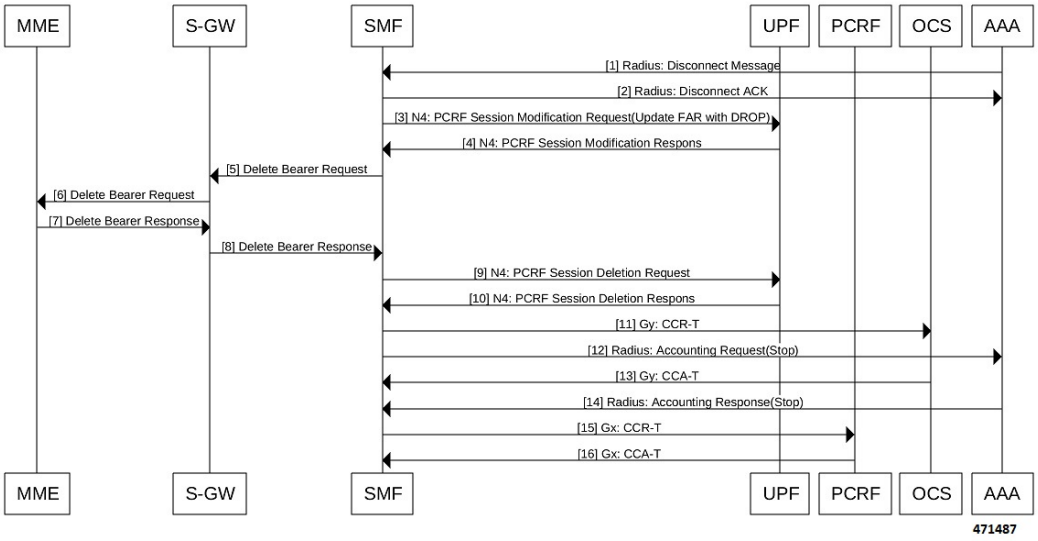



**表 *53 : RADIUS* 開始によるデタッチのコール フローの説明**

| 手順 | 説明 |
|---|---|
| 1 | SMF への AAA RADIUS 切断メッセージ。 |

| 手順 | 説明 |
|---|---|
| 2 | SMF が RADIUS 切断の確認応答を返します。 |
| 3 | SMF は PCRF セッション変更要求を UPF に送信します。 |
| 4 | UPF は PCRF セッション変更応答で SMF に応答します。 |
| 5 | SMF が S-GW にベアラーの削除要求を送信します |
| 6 | S-GW は、ベアラー応答の削除を MME に転送します。 |
| 7 | MME はベアラー応答の削除で S-GW に応答します。 |
| 8 | S-GW は、ベアラー応答の削除を SMF に転送します。 |
| 9 | SMF は PCRF セッション削除要求を UPF に送信します。 |
| 10 | UPF は、PCRF セッション削除応答で SMF に応答します。 |
| 11 | SMF は OCS に CCR-T を送信します。 |
| 12 | SMF がアカウンティング要求（停止）を AAA に送信します。 |
| 13 | OCS は CCA-T で SMF に応答します。 |
| 14 | SMF はアカウンティング応答（停止）で AAA に応答します。 |
| 14 | SMF は CCR-T を PCRF に送信します。 |
| 15 | PCRF は CCA-T で SMF に応答します。 |

# 専用ベアラーのアクティブ化と非アクティブ化

## 機能説明

SMF は、E-UTRAN、MME、および S-GW を介して接続された UE に対して、PCF によって開始された専用ベアラーの作成および専用ベアラーの削除手順をサポートします。

### 機能の仕組み

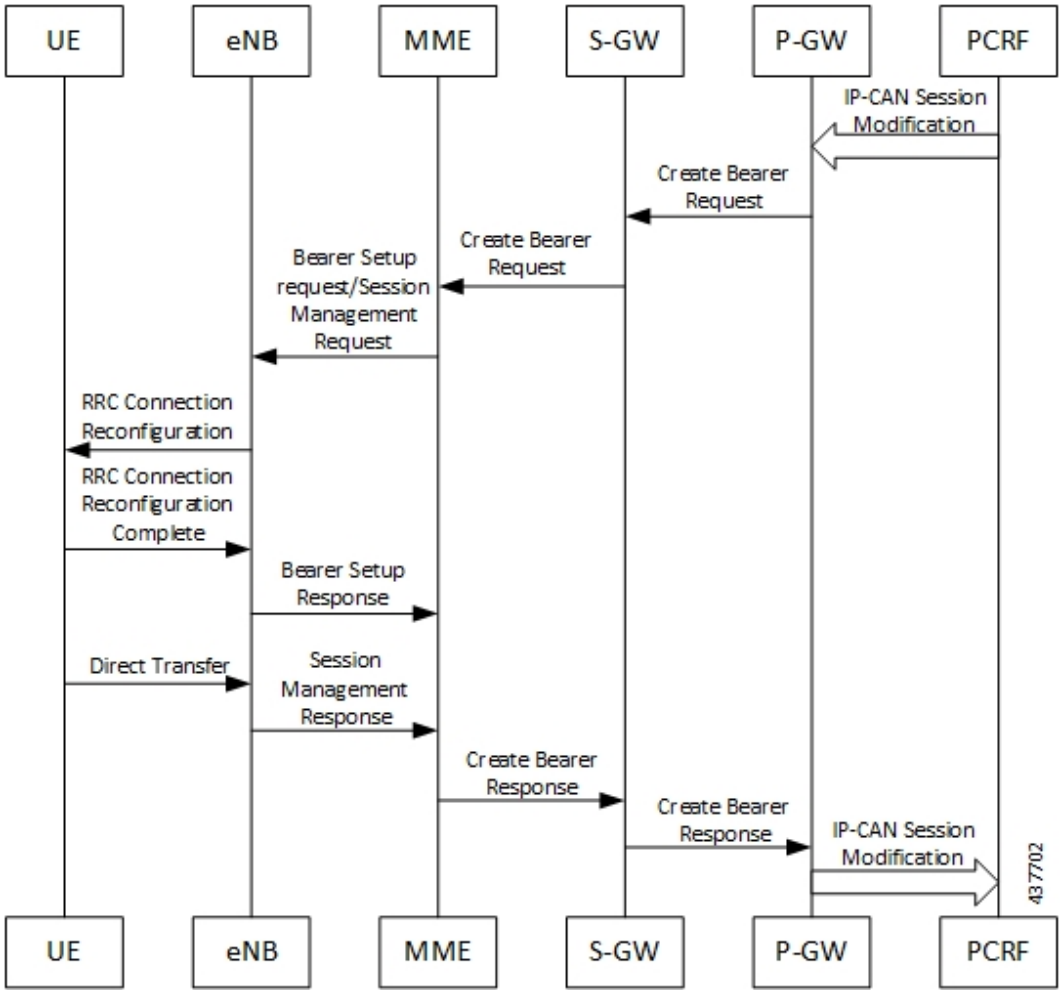
#### コール フロー

ここでは、この機能に関連したコール フローについて説明します。

専用ベアラー作成コール フロー

次の図は、専用ベアラーの作成手順を説明しています。

*Figure 40:* 専用ベアラー作成コール フロー



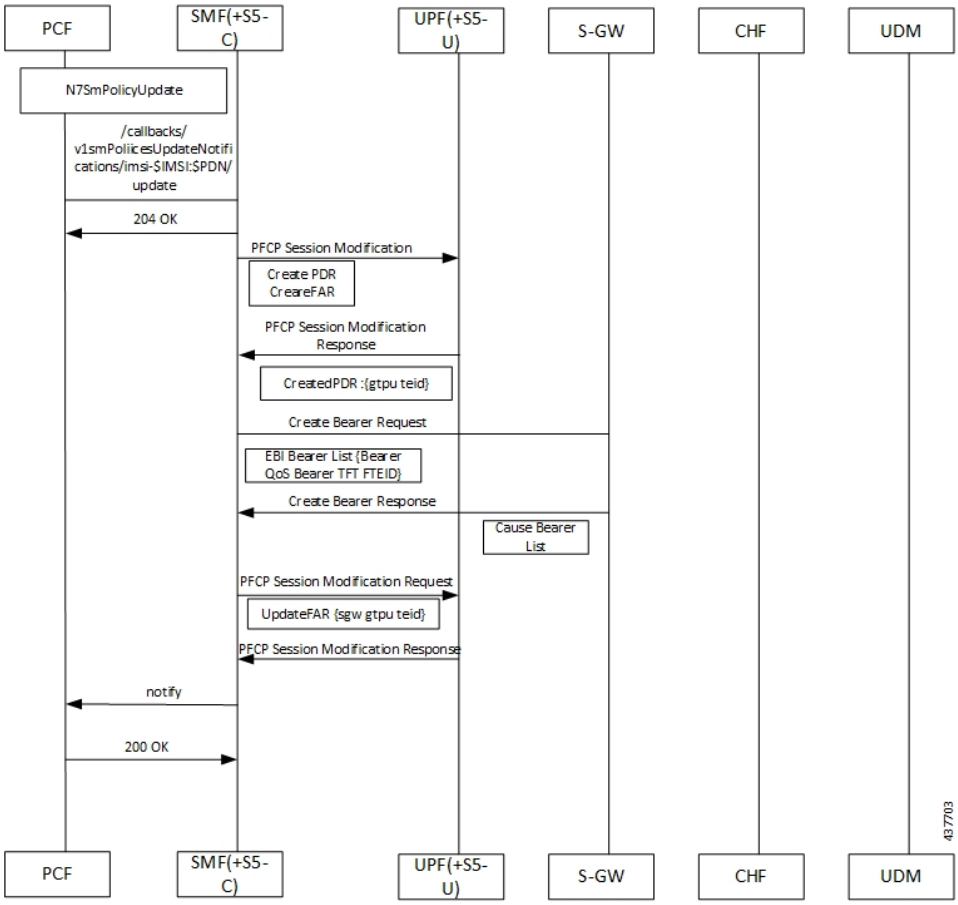

EPS セッションの専用ベアラーの作成またはアクティベーションの手順は、3GPP 23.401、Section 5.4.1 で定義されています。UE が E-UTRAN に接続されている場合、専用ベアラーの手順は、次の変更を除き、指定された 3GPP セクションに記載されている手順と同じままです。

- PCRF（PCRF または CCR-U から PCRF への RAR）に対するインタラクションは、PCF から SMF への Npcf_SMPolicyControl_UpdateNotify 要求と、SMF から PCF への Npcf_SMPolicyControl_Update 要求にそれぞれ置き換えられます。
- PCF によって提供される PCC ルールは、新しい専用ベアラーの TFT にマッピングされ、関連付けられた QoS は 5G PDU セッション パラメータからの EPS PDN 接続パラメータの生成, on page 296で定義されている 4G QoS にマッピングされます。
- すべての Gy および Gz インターフェイス メッセージは、Nchf_ConvergedCharging_Update サービス操作に置き換えられます。
- 専用ベアラーのユーザー プレーン リソースは、新しい専用ベアラーの SDF フィルタに PDR、QER、および FAR が追加される UPF に対する N4 セッション変更手順を使用して追加されます。

• SMFベアラー応答の作成で受信した専用ベアラーの EBI を保存します。

次の図は、PCF によって開始される専用ベアラーのアクティブ化手順を示しています。

***Figure 41: PCF*によって開始された専用ベアラーの有効化**




## *N4*最適化コール フローを使用した非ローミング *4G PDN*接続

このセクションでは、N4 最適化を使用した非ローミング 4G PDN 接続のコール フローについて説明します。

図 *42 : N4* 最適化コール フローを使用した非ローミング *4G PDN* 接続

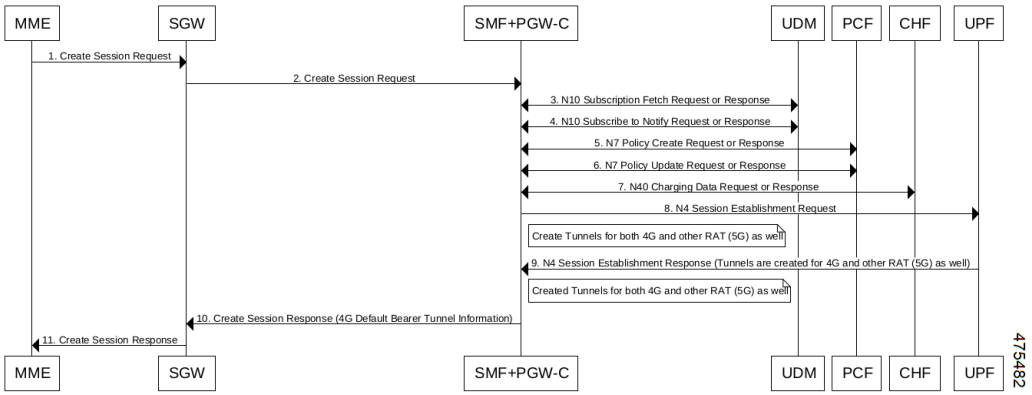


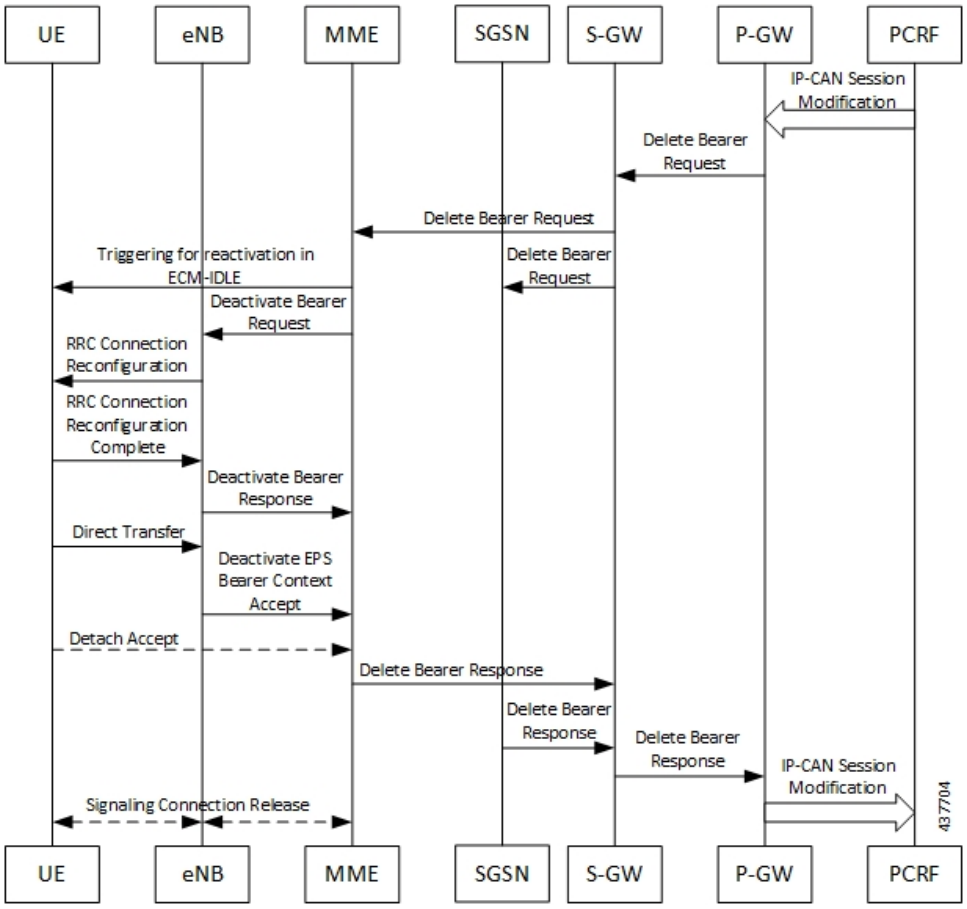

表 *54 : N4* 最適化コール フローの説明を使用した非ローミング *4G PDN* 接続

| ステップ | 説明 |
|---|---|
| 1 | MME がセッション作成要求を S-GW に送信します。 |
| 2 | S-GW は、セッション作成要求を SMF+PGW-C に送信します。 |
| 3 | SMF + PGW-C は、N10 サブスクリプション取得要求を UDM に送信します。次に、UDMは、N10サブスクリプション取得応答をSMF + PGW-Cに送信します。 |
| 4 | SMF + PGW-C は、UDM に N10 サブスクライブ要求を送信します。次に、UDMは、N10 Subscribe to Notify 応答をSMF + PGW-Cに送信します。 |
| 5 | SMF + PGW-C は、N7 ポリシー作成要求を PCF に送信します。PCF は、SMF + PGW-C に N7 ポリシー作成応答を送信します。 |
| 6 | SMF + PGW-C は PCF に N7 ポリシー更新要求を送信します。PCF は、SMF + PGW-C に N7 ポリシー更新応答を送信します。 |
| 7 | SMF + PGW-C は CHF に N40 課金データ要求を送信します。CHF は、N40 課金データ応答を SMF+PGW-C に送信します。 |
| 8 | SMF+PGW-C は UPF に N4 セッション確立要求を送信します。SMF は、5G とその他の RAT（4G）の両方のトンネルを作成します。 |
| 9 | トンネルの作成後、UPF は N4 セッション確立応答を SMF + PGW-C に送信します。 |
| 10 | SMF+PGW-C は、セッション作成応答を S-GW に送信します。この応答には、4G のデフォルトのベアラー トンネル情報が含まれています。 |
| 11 | S-GW はセッション応答の作成を MME に送信します。 |

専用ベアラー非活性化コール フロー

次の図は、専用ベアラーの非アクティブ化手順を説明しています。

***Figure 43:*** **専用ベアラー非活性化コール フロー**




EPS セッションの専用ベアラー非アクティブ化手順は、3GPP 23.401、Section 5.4.4 で定義されています。UE が E-UTRAN に接続されている場合、専用ベアラーの手順は、次の変更を除き、指定された 3GPP セクションに記載されている手順と同じままです。

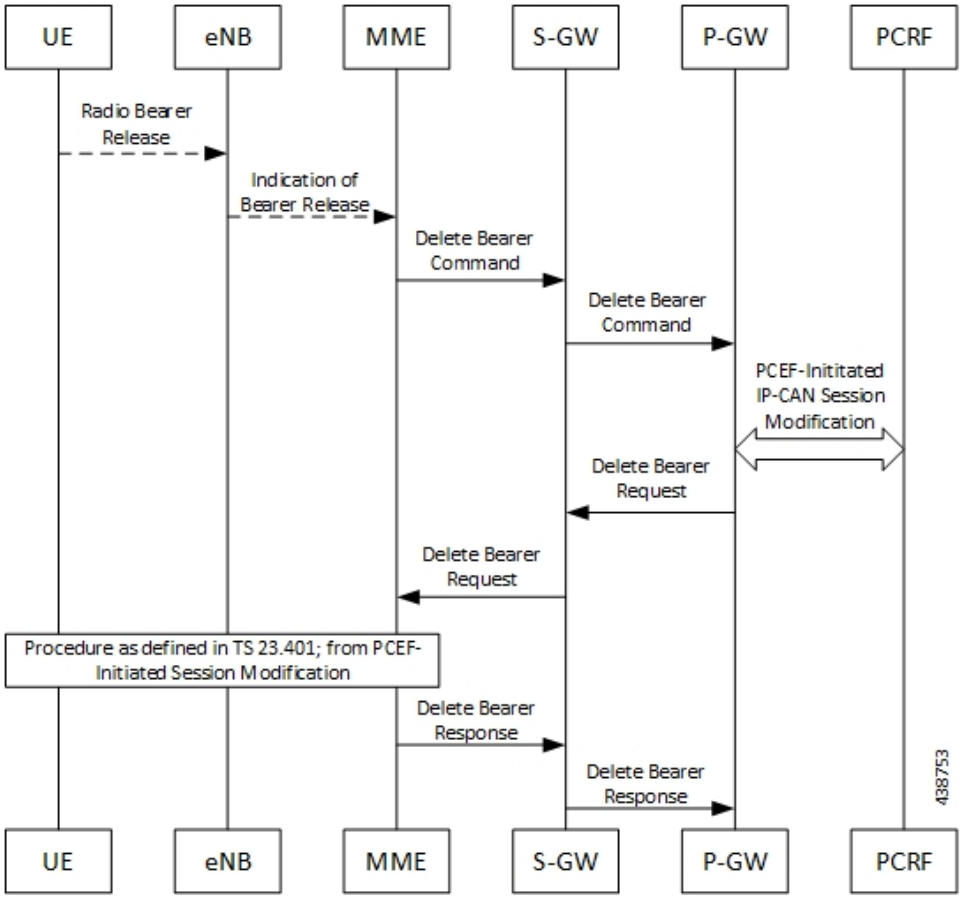
- PCRF（PCRF/CCR-U から PCRF への RAR）に対するインタラクションは、PCF から SMF への Npcf_SMPolicyControl_UpdateNotify 要求と、SMF から PCF への Npcf_SMPolicyControl_Update 要求にそれぞれ置き換えられます。
- PCF によって削除された PCC ルールは、対応する専用ベアラーにマッピングされ、ベアラーの非アクティブ化がこれらのベアラーに対してトリガされます。
- すべての Gy および Gz インターフェイス メッセージは、Nchf_ConvergedCharging_Update サービス操作に置き換えられます。
- 専用ベアラーのユーザー プレーン リソースは、削除された専用ベアラーの SDF フィルタの PDR、QER、および転送アクション ルール（FAR）が削除される UPF に対する N4 セッション変更手順を使用して削除されます。

### MME によって開始された専用ベアラーの非アクティブ化

MME は、UE または MME が要求した PDN の切断手順を使用して、PDN 接続の解放を開始します。次のコール フローは、専用ベアラを非アクティブ化する手順を示しています。

**Note** デフォルトのベアラーは、切断プロセス中に影響を受けません。

***Figure 44: MME*** によって開始された専用ベアラーの非アクティブ化




| ステップ | 説明 |
|---|---|
| 1 | ECM-CONNECTED 状態にある UE の無線ベアラーのリリースは、異常なリソース制限などのローカルの理由により発生します。UE は、リリースされた無線ベアラーに関連するベアラー コンテキストを削除します。 |

| ステップ | 説明 |
|---|---|
| 2 | eNodeB が無線ベアラーを解放すると、MME にベアラー解放の指示を送信します。この表示は、MME へのベアラー リリース要求（EPS ベアラー識別）メッセージ、または初期コンテキスト セットアップ完了、ハンドオーバー要求応答、UE コンテキスト応答のいずれかです。パス スイッチ要求は、ベアラーのリリースを示すこともできます。eNodeB が MME に送信される指示に ECGI と TAI を含めます。 |
| 3 | MME は S-GW への PDN 接続ごとに、ベアラー コマンドの削除（EPS ベアラー ID、ユーザー ロケーション情報、UE タイムゾーン、RAN または NAS リリース原因（使用可能な場合））メッセージを送信し、選択された専用ベアラーを非アクティブ化します。RAN または NAS のリリース原因は、RAN のリリース原因または NAS のリリースの原因を示します。RAN または NAS のリリース原因は、MME オペレータ ポリシーに従って許可されている場合にのみ、MME によって PGW-C に送信されます。 |
| 4 | S-GW は、PGW-C への PDN 接続ごとに、ベアラー コマンドの削除（EPS ベアラー識別、ユーザー ロケーション情報、UE タイム ゾーン、RAN/NAS リリースの原因）メッセージを送信します。 |
| 5 | PCC インフラストラクチャが配備されている場合、PGW-C は、3GPP TS 23.203 に定義されているように、PCEF 主導の IPnon-breaking hyphen - U+2011CAN セッション変更手順により、リソースの損失について PCRF に通知し、3GPP TS 23.203 に定義されているように、PCRF から要求された場合、S-GW からのベアラー コマンドの削除で受信したユーザー ロケーション情報、UE タイム ゾーン、および RAN または NAS リリースの原因（利用可能な場合）を提供します。PCRF は、更新された PCC 決定を PGW-C に送信します。<br>**Note**<br>MME または S-GW が以前のリリースであり、この情報を提供しなかった場合、ユーザーの場所情報と UE タイムゾーンは利用できない場合があります。 |
| 6 | PGW-C は、ベアラー要求の削除（EPS ベアラー識別）メッセージを S-GW に送信します。 |
| 7 | S-GW は、ベアラー要求の削除（EPS ベアラー識別）メッセージを MME に送信します。 |
| 8 | この手順では、手順 5 から手順 8 を呼び出します。ステップ 1 とステップ 2 で eNodeB によってベアラーの非アクティブ化がトリガされた場合、これらのステップは省略されることに注意してください。<br>また、引き継ぎ中にベアラーのセットアップに失敗したために MME がベアラーの解放を開始した場合、UE と MME は失敗したコンテキストをピアツーピア ESM シグナリングなしでローカルに非アクティブにします。 |

| ステップ | 説明 |
|---|---|
| 9 | MME は、非アクティブ化された EPS ベアラーに関連するベアラー コンテキストを削除し、ベアラー応答の削除（EPS ベアラー ID、ユーザー場所情報（ECGI））メッセージを送信することによって、S-GW に対してベアラーの非アクティブ化を確認します。 |
| 10 | S-GW は、非アクティブ化された EPS ベアラーに関連するベアラー コンテキストを削除し、ベアラー応答の削除（EPS ベアラー識別）メッセージを送信することによって、PGW-C にベアラーの非アクティブ化を確認します。 |

### SMF によって開始された専用ベアラーの非アクティブ化

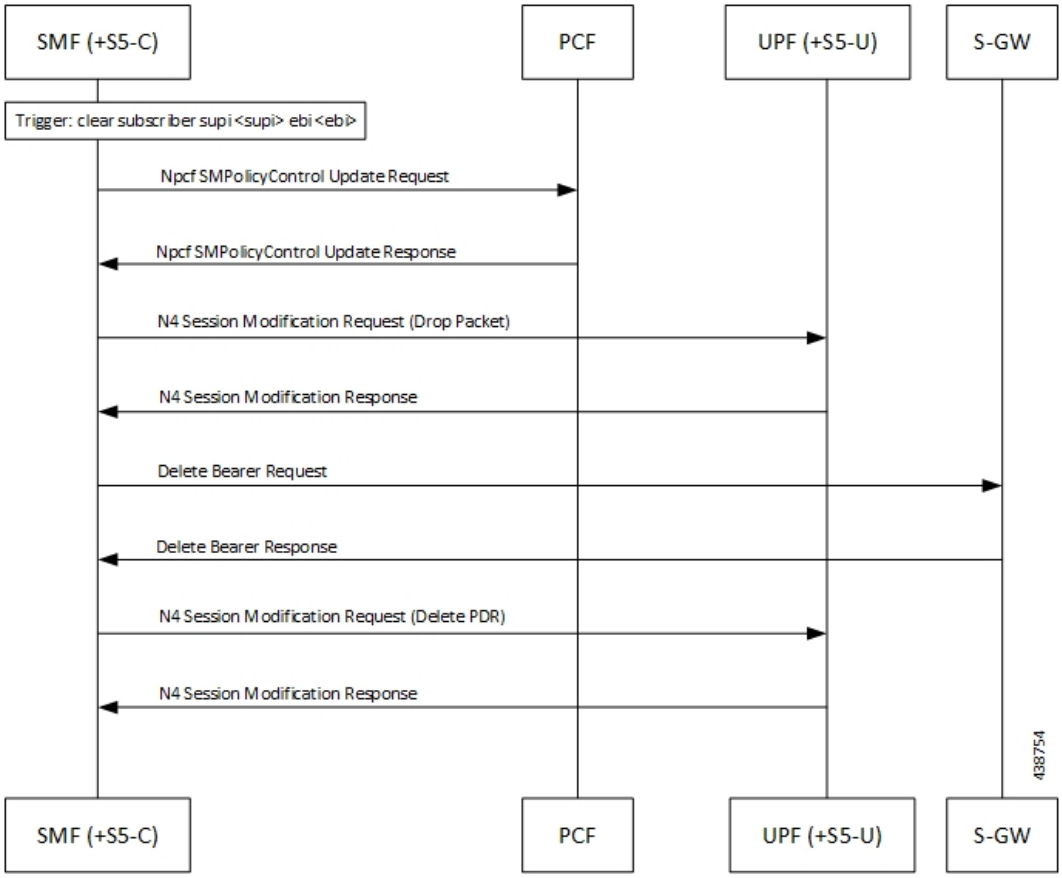
次の手順では、3GPP TS 23.203 で定義されている SMF によって開始される専用ベアラーの非アクティブ化プロセスについて説明します。

**Note** デフォルト ベアラーは、専用ベアラーの非アクティブ化プロセスの間は影響を受けません。

- SMF によって開始された削除ベアラーは、 **clear subscriber** コマンドを使用してトリガされます。
- PCC インフラストラクチャが配備されている場合、PGW-C は、PCEF 主導の IPnon-breaking hyphen - U+2011CAN セッション変更手順により、リソースの損失について PCRF に通知し、PCRF から要求された場合、S**clear subscriber** コマンドで受信したユーザー ロケーション情報、UE タイム ゾーン、および RAN または NAS リリースの原因（利用可能な場合）を提供します。PCRF は、更新された PCC 決定を PGW-C に送信します。
- PGW-C は、ベアラー要求の削除（EPS ベアラー識別）メッセージを S-GW に送信します。
- S-GW は、非アクティブ化された EPS ベアラーに関連するベアラーコンテキストを削除し、ベアラー応答の削除（EPS ベアラー識別）メッセージを送信することによって、PGW-C にベアラーの非アクティブ化を確認します。

次のコール フローは、SMF によって開始される専用ベアラーの非アクティブ化を示しています。

*Figure 45: SMF* によって開始された専用ベアラの非アクティブ化




# EPS フォールバック

## 機能説明

SMF は、ims-voice-eps-fallback または rate-fallback がトリガーされた専用ベアラの作成を gNB が拒否した場合、IMS セッションの 5GC からの EPS へのフォールバックをサポートします。

VoNR をサポートしていない UE デバイスの場合、SMF は音声コールに対して EPS へのフォールバックを実行します。これには、5G から EPS へのハンドオーバーと、音声通話用の 4G での専用ベアラーの作成が含まれます。

## 機能の仕組み

### コール フロー

次のコール フローは、EPS フォールバックの手順を示しています。

*Figure 46: EPS* フォールバック コール フロー

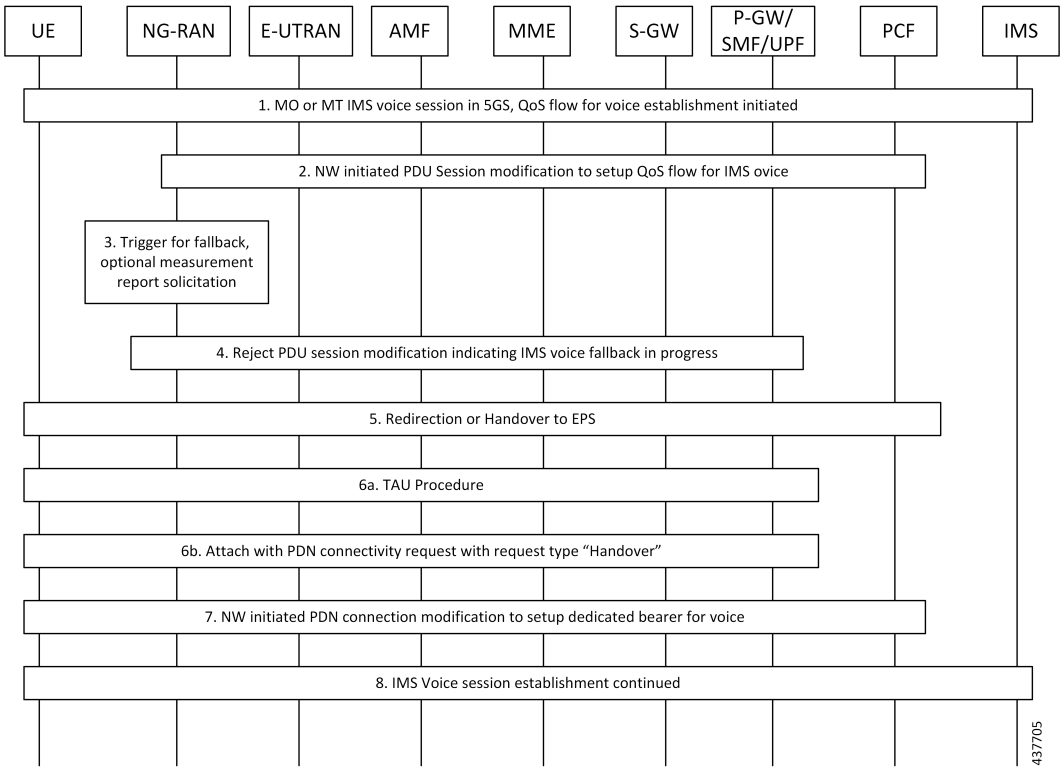



*Table 55: EPS* フォールバック コール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | UEは、5GSのNG-RANを使用して、モバイル発信（MO）またはモバイル着信（MT）IMS 通話の確立手順を開始します。 |
| 2 | 音声の QoS フローを設定するためにネットワークが開始した PDU セッション変更要求が NG-RAN に到達します。 |
| 3 | NG-RAN は、IMS 音声の EPS フォールバックをサポートするように構成されています。UEの機能に基づき、AMFからの指示により、音声、ネットワーク構成、および無線条件における EPS のフォールバックを再ルーティングするため、NG-RANはEPSへのフォールバックをトリガします。NG-RANがEPSへのフォールバックをトリガしないと判断した場合、手順は停止し、次のステップは実行されません。<br>NG-RAN は、E-UTRAN をターゲットとして含む UE から測定レポートの要求を開始します。 |

| ステップ | 説明 |
|---|---|
| 4 | NG-RAN は、ステップ 2 で受信した PDU セッション変更要求を拒否し、IMS 音声のフォールバックによるモビリティが進行中であることを示します。<br><br>NG-RAN は、AMF を介した SMF への PDU セッション応答メッセージとしてステップ 2 で受信した IMS 音声の QoS フローを構成するための PDU セッション変更の拒否を示します。このメッセージには、IMS 音声のフォールバックに伴う現在の移動に関する詳細が含まれています。SMF は、QoS フローに関連する PCC ルールを維持しています。<br><br>ローミング シナリオの場合、PDU セッション応答メッセージは V-SMF を介して H-SMF に送信されます。<br><br>または<br><br>NG-RAN は、EPS へのフォールバックをトリガする可能性がある構成済みの原因で応答します。gNB によって送信された原因が SMF で構成された EPS フォールバックの原因と一致する場合、次の手順で説明したように動作し続けます。5 以降。<br><br>**Note**<br>SMF での構成により、gNB が「IMS 音声 EPS フォールバックまたは RAT フォールバックがトリガされた」という理由で N2 メッセージを拒否した場合でも、構成された原因を常にチェックします。 |
| 5 | UE の機能に基づいて、NG-RAN は EPS へのハンドオーバーを開始します。PCF がサブスクライブされている場合、SMF は RAT タイプの変更を報告します。<br><br>EPS フォールバックの障害を追跡するためのタイマーが開始します。タイマーの期限が切れると、SMF は、専用ベアラーの作成が失敗し、「smf_eps_fb」および「timeout」ラベル付きの新しい統計情報が増加したことを PCF に通知します。 |
| 6a | 5GS から EPS へのハンドオーバーの場合、UE は TAU 手順を開始します。 |
| 6b | UE は、PDN 接続要求を「ハンドオーバー」要求タイプで送信します。 |
| 7 | 5GS から EPS へのハンドオーバー手続きが完了した後、SMF または PGW-C は IMS 音声用の専用ベアラーの構成を再初期化し、5G の QoS を EPC の QoS パラメータにマッピングします。SMF は、PCF がサブスクライブされている場合、成功したリソース割り当て、およびアクセス ネットワーク情報について通知します。 |
| 8 | IMS 音声セッション確立が続行します。 |

# EPS フォールバック トリガ原因の構成

EPS フォールバック トリガーの原因を構成するには、次の構成例を使用します。

```
config
  profile access access_profile_name
    eps-fallback trigger-cause group radioNetwork value radioNetwork_value

     exit
```

注：

- **trigger-cause** ：EPSFallback をトリガーする原因を示します。
- **group** ：原因グループを示します。

```
[smf] smf(config-access-access1)# eps-fallback trigger-cause group
Possible completions:
misc nas protocol radioNetwork transport
[smf] smf(config-access-access1)# eps-fallback trigger-cause group radioNetwork value
Possible completions:
unsignedInt, 0 .. 46
```

### EPS フォールバック トリガー原因の構成の確認

このセクションでは、SMF で EPS フォールバック トリガー原因の構成を検証する方法について説明します。

次の構成例を使用して、EPS フォールバック トリガーの原因である無線ネットワークの値の構成を確認します。

```
smf# show running-config profile access access1
 eps-fallback trigger-cause group radioNetwork
 value [ 22 36 ]
 exit
 eps-fallback trigger-cause group transport
 value [ 0 ]
 exit
 eps-fallback trigger-cause group nas
 value [ 0 ]
 exit
 eps-fallback trigger-cause group misc
 value [ 1 ]
 exit
exit
```

# 間接データ転送トンネル（IDFT）タイマーのサポート

## 機能説明

SMF は、5G から 4G へのハンドオーバーの IDFT 手順中に、間接データ転送トンネル（IDFT）タイマーをサポートします。ハンドオーバー中に、5G の IDFT トンネルは解放されます。SMF は、NSMF PDU セッション更新 SM コンテキスト要求を受信して、AMF からの転送トンネル

を解放します。SMF がこの要求を受信しない場合、IDFT タイマーが未使用のトンネルを解放します。

# 機能の仕組み

## コール フロー

ここでは、次のコール フローについて説明します。

### IDFT タイマー コール フローによる 5G から EPS へのハンドオーバー

このセクションは、IDFT タイマー コール フローでの 5G から EPS へのハンドオーバーを説明します。

**図 *47 : IDFT* タイマーコール フローによる *5G* から *EPS* へのハンドオーバー**

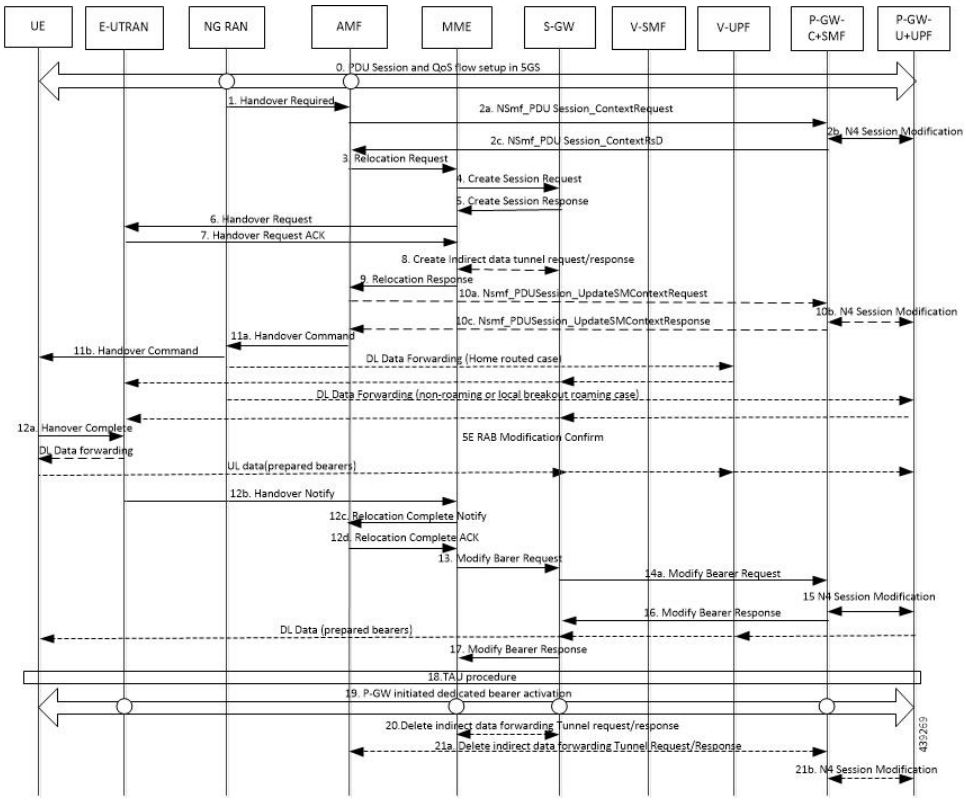


表 *56 : IDFT* タイマーを使用した *5G* から *EPS* へのハンドオーバーのコール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | NG-RAN は、UE を E-UTRAN に引き渡すかどうかを決定します。QoS フローのセットアップによってトリガーされた IMS 音声のフォールバックが原因で NG-RAN が RAT 間モビリティを実行するように設定されていて、IMS 音声の QoS フローをセットアップするリクエストを受信した場合、NG-RAN は QoS フロー確立の拒否を示します。 この指示は、N2 SM 情報を介した IMS 音声のフォールバックによるモビリティのため、E-UTRAN へのハンドオーバーをトリガーします。NG-RAN が AMF にハンドオーバーが必要であることを示すメッセージを送信します。このメッセージには、ターゲット eNB ID、直接転送パスの可用性、送信元からターゲットへの透過的コンテナ、およびシステム間ハンドオーバーの表示に関する詳細が含まれています。<br>NG-RAN は、送信元からターゲットの透過コンテナを使用して、データ転送のために、対応する5G QoSフローのベアラーを示します。 |
| 2a | AMF は、NSMF PDU セッション コンテキスト リクエストを SMF + PGW-C に送信して、SM コンテキストを提供します。 |
| 2b | SMF + PGW-C は N4 セッション変更を PGW-U + UPF に送信して、各 EPS ベアラーの CN トンネルを確立します。PCC が送信する 5G QoS および PCC ルールへのベアラー マッピングは、SMF で使用できます。SMF には、ベアラー ID の割り当て手順から受信したベアラー ID も含まれます。SMF + PGW-C は、N4 セッションの新しい PDR を作成し、4G システムのリクエストに応じて各ベアラに割り当てられる TEID を取得します。<br><br>SMF + PGW-C のタイマーは、この手順で開始されます。このタイマーは、解放される UPF の間接データ転送のリソースをモニターします。<br><br>IDFT タイマーの期限切れのケースは次のとおりです。<br>• ステップ 21a が実行されず、タイマーが期限切れになる：間接トンネルに必要ない PDR と FAR は、ステップ 21a の前に削除されます。<br>• タイマーは、ステップ 14a および 16 の前または中に期限切れになります。間接トンネルに必要ない PDR および FAR は削除され、コール フローは独立して続行されます。<br>• 手順 21a はタイマーの期限切れ後に発生します。リソースがタイマーの期限切れで解放されるため、SMF は N4 変更リクエストを UPF + PGW-U に送信しません。 |
| 2c | SMF + PGW-C は、EPS ベアラー コンテキストを AMF に送信します。ベアラー コンテキストは、UE EPS PDN 接続 IE をエンコードする base64 エンコード文字であるバイト形式の文字列です。<br><br>SMF + PGW-C は、E-UTRAN からのアップリンク トラフィックのすべてのベアラーの AMF に CN トンネル情報も提供します。 |

| ステップ | 説明 |
|---|---|
| 3 | AMF は転送再配置リクエストを MME に送信します。AMF には、現用系 UP 接続の有無にかかわらず、PDU セッションにマッピングされた SM EPS UE コンテキストが含まれます。 |
| 4 | MME がセッション作成リクエストを SGW に送信します。詳細については 、*3GPP TS 23.401*、*5.5.1.2.2* 節の「*S1-based handover in the normal Case*」の項を 参照してください。 |
| 5 | SGW はセッション応答の作成を MME に送信します。詳細については 、*3GPP TS 23.401*、*5.5.1.2.2* 節の「*S1-based handover in the normal Case*」の項を 参照してください。 |
| 6 | MME は、E-UTRAN へハンドオーバー リクエストを送信します。 |
| 7 | E-UTRAN は MME に引き継ぎリクエストの確認応答を送信します。 |
| 8 | MME と SGW は、間接データ転送リクエストと応答を相互に送受信します。 |
| 9 | MME が再配置応答を AMF に送信します。 |
| 10a | 間接的なデータ転送の場合、AMF は NSMF PDU セッション更新 SM コンテキスト リクエストを PGW-C + SMF に送信します。このリクエストは、データ転送および間接データ転送トンネルの作成のための SGW アドレスおよび SGW DL TEID に対するものです。 |
| 10b | PGW-C+SMF は、N4 変更リクエストを UPF+PGW-U に送信して、より多くの PDR と FAR を作成します。PDR と FAR は、NG RAN から間接トンネルを介してリダイレクトされた DL データを受信し、それらを eNodeB に転送するために作成されます。UL PDR には、NG RAN から転送された DL データと一致する QFI があります。関連付けられた QER には、データを eNodeB に転送する QFI があります。また、FAR は、受信したデータを QFI に基づいて適切なトンネルを介して eNodeB にリダイレクトします。 |
| 10c | PGW-C+SMF は、NSMF PDU セッション更新 SM コンテキスト応答を AMF に送信します。この応答には、原因、データ転送の CN トンネル情報、およびデータ転送の QoS フローに関する詳細が含まれています。PGW-C+SMF はこの応答を送信して、間接的なデータ転送を作成します。QFI と SGW アドレスとデータ転送用の TEID の相関関係に基づいて、PGW-U+UPF は QoS フローを EPC のデータ転送トンネルにマッピングします。 |
| 11a | AMF は、送信元の NG-RAN にハンドオーバー コマンドを送信します。 |

| ステップ | 説明 |
|---|---|
| 11b | 送信もとの NG-RAN は、UE にハンドオーバー コマンドを送信して、ターゲットのアクセス ネットワークに引き継ぎます。<br><br>UE は、進行中の QoS フローを、ハンドオーバーコマンドで設定される指定された EPS ベアラー ID（EBI）に関連付けます。PDU セッションのデフォルト QoS ルールに関連付けられている QoS フローに未割り当ての EBI がある場合、UE は PDU セッションをローカルで削除します。デフォルトの QoS ルールに関連付けられている QoS フローに EBI が割り当てられている場合、UE は PDU セッションを保持します。未割り当ての EBI を伴う QoS フローの場合、UE は QoS ルールと QoS フロー レベルの QoS パラメータをローカルで削除します（それらの QoS フローに関連付けられているものがある場合）。その後、UE は、影響を受けるアプリケーションに、専用の QoS 技術情報が解放されたことを通知します。UE は、UE から派生した QoS ルールを削除します。PDU セッションのデフォルトの QoS ルールの QoS フローに割り当てられた EBI は、対応する PDN 接続のデフォルトのベアラーの EBI になります。 |
| 12a | UE は、ハンドオーバー完了の通知を E-UTRAN に送信します。 |
| 12 b | E-UTRAN が MME にハンドオーバー通知リクエストを送信します。 |
| 12c | MME が再配置完了通知を AMF に送信します。 |
| 12 d | AMF が再配置完了通知の確認応答を MME に送信します。 |
| 13 | MME が、ベアラー リクエストの変更を SGW に送信します。 |
| 14a | SGW は、SMF＋PGW-C にベアラー リクエストの変更を送信します。このリクエストには、ベアラーの SMF の DL TEID に関する情報が含まれています。 |
| 15 | PGW-C＋SMF は、UPF＋PGW-U に対して N4 セッション変更手順を開始し、ユーザー プレーンパスを更新します。これは、指定された PDU セッションの DL ユーザー プレーンが E-UTRAN に切り替えられることを意味します。PGW-C + SMF は、UPF + PGW-U の PDU セッションの CN トンネルのリソースを解放します。 |
| 16 | PGW-C+SMF は、ベアラー変更応答を SGW に送信します。この段階で、UE、ターゲット eNodeB、SGW、および PGW-U+UPF 間のデフォルト ベアラーおよび専用 EPS ベアラーに対してユーザー プレーンパスが確立されます。PGW-C+SMF は、QoS フローの確立中に専用 EPS ベアラーに割り当てられた EPS QoS パラメータを使用します。PGW-C+SMF は、他のすべての IP フローをデフォルトの EPS ベアラーにマッピングします。<br><br>間接転送トンネルが確立されると、PGW-C+SMF はタイマーを開始し、間接データ転送に使用されるリソースを解放します。 |
| 17 | SGW が、ベアラー変更応答を MME に送信します。 |

| ステップ | 説明 |
|---|---|
| 18 | UE がトラッキング エリアの更新手順を開始します。詳細については 、*3GPP TS 23.401*、*5.5.1.2.2* 節の「*S1-based handover in the normal Case*」の項を 参照してください。<br>この手順では、HSS+UDM から 3GPP アクセス用に古い AMF を登録解除します。古いAMF での非3GPP アクセスに関連付けられている登録は削除されません。これは、3GPP アクセスと非3GPP アクセスの両方を介して UE にサービスを提供している AMF は、非3GPP アクセスを介して登録解除された UE とは見なさず、登録されたまま、UDM のサブスクリプションデータ更新にサブスクライブすることを意味します。 |
| 19 | PCC が展開されている場合、PCF は、以前に削除された PCC ルールを PGW-C+SMF に再度提供するように決定します。これらの PCC ルールにより、PGW-C+SMF は専用ベアラのアクティベーション手順を開始します。 |
| 20 | SGW は MME に間接データ転送トンネルの削除リクエストを送信します。MME が SGW に、間接データ転送トンネルの削除リクエストを送信します。 |
| 21a | AMF は、転送トンネルを解放するように指示して、NSMF PDU セッション更新 SM コンテキスト リクエスト サービス操作を開始します。 |
| 21b | SMF は N4 変更リクエストを UPF + PGW-U に送信して、間接トンネルの PDR と FAR を削除します。不要な 5G セッションの PDR と FAR も削除されます。ステップ 2b で開始した IDFT タイマーが停止します。 |

### 標準準拠

IDFT タイマー サポート機能は、以下の基準に準拠しています。

- *3GPP TS 23.502 V16.1.1*（*2019-06*）
- *3GPP TS 23.401* バージョン *12.6.0* リリース *12*

# IDFT タイマーの構成

このセクションでは、IDFT タイマーの構成方法について説明します。

```
config
  profile access test [ eps-fallback | n2 | n26 ]
  eps-fallback guard enable timeout timeout_value
  n26 idft enable timeout n26_timeout_value
  n2 idft enable timeout n2_timeout_value
    end
exit
```

注：

- **profile access**：プロファイル構成にアクセスします。
- **test**：プロファイル インスタンスにアクセスします。
- **eps-fallback**：EPS フォールバック 構成を入力します。
- **n26**：E-UTRAN および NG-RAN の構成である N26 インターフェイスを開始します。
- **n2**：NG-RAN 構成の N2 インターフェイスを開始します。
- **idft enable timeout**：IDFT タイマーが期限切れになるまでの値（15 ～ 60）を入力します。

# EPS フォールバック ガード タイマーのサポート

## 機能説明

SMF は、EPS フォールバックの障害を追跡するためのガードタイマーをサポートしています。タイマーが開始すると、EPS のフォールバックが発生するのを待ってから、ベアラー作成の失敗情報が PCF に伝達されます。

### 機能の仕組み

EPS フォールバック タイマーは、AMF を介して gNB から EPS フォールバック原因による専用ベアラー作成の失敗に関する通知を受信した後、開始されます。この場合、SMF は PCF に障害通知を送信せず、5G から 4G へのハンドオーバーが完了するのを待ちます。その後、SMF は 4G でベアラーの作成をトリガーします。EPS フォールバック タイマーは、5G から 4G へのハンドオーバーの完了時に停止します。

5G から 4G へのハンドオーバーの完了前にタイマーが期限切れになった場合、SMF は専用ベアラー作成失敗の通知を PCF に送信します。次に、「smf_eps_fb」および「timeout」ラベルが付いた新しい統計カウンタが増分されます。ただし、5G から 4G へのハンドオーバー手順は続行されます。

#### コール フロー

ここでは、次のコール フローについて説明します。

##### *EPS* フォールバック ガード タイマー コール フロー

このセクションでは、5G から EPS へのフォールバック ガード タイマー コール フローについて説明します。

図 *48 : EPS* フォールバック ガード タイマー コール フロー

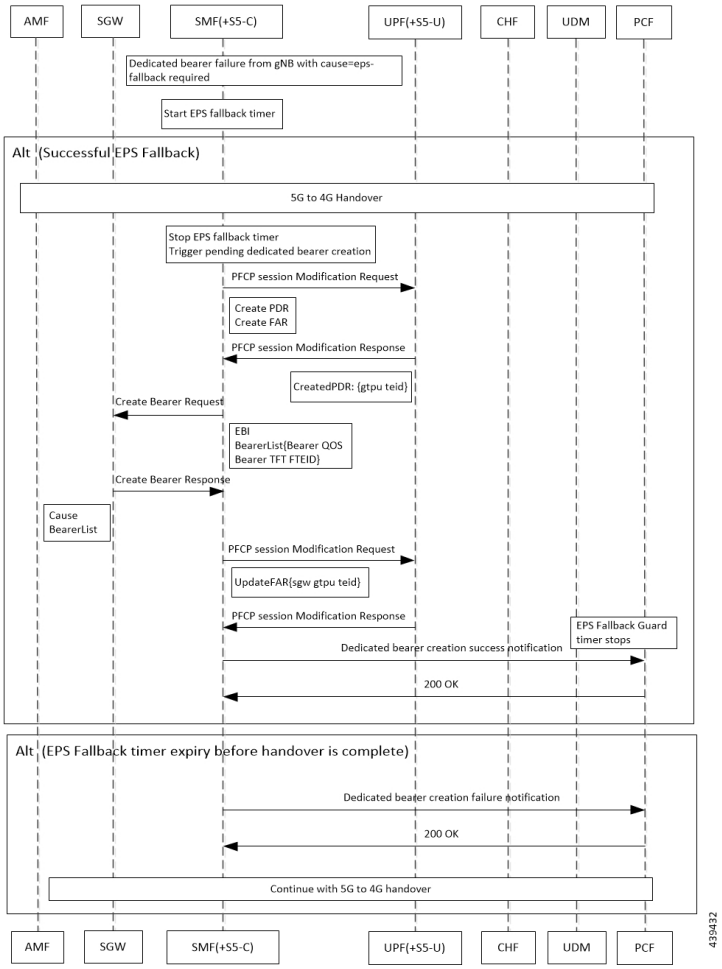



表 *57 : EPS* フォールバック ガード タイマー コール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | gNB は、AMF を介してフォールバック原因とともに専用ベアラ作成の失敗情報を送信します。 |
| 2 | EPS フォールバック タイマーが開始されます。 |
| 5G から 4G へのハンドオーバー シナリオで正常に完了した EPS フォールバックでは、ステップ 3 ー 12 が発生します。 | |
| 3 | EPS フォールバック タイマーが停止し、保留中の専用ベアラーの作成をトリガーします。 |
| 4 | SMF（+S5-C）は、PFCP セッション変更要求を UPF（+S5-U）に送信します。 |

| ステップ | 説明 |
|---|---|
| 5 | PDR と FAR が作成されています。 |
| 6 | UPF（+S5-U）は、PFCP セッション変更応答を SMF（+S5-C）に送信します。 |
| 7 | GTP-U TEID を持つ作成された PDR の情報が利用可能です。 |
| 8 | SMF（+S5-C）が SGW にベアラー要求の作成を送信します。 |
| 9 | SGW は、SMF（+S5-C）にベアラー応答の作成を送信します。 |
| 10 | SMF（+S5-C）は、PFCP セッション変更要求を UPF（+S5-U）に送信します。 |
| 11 | UPF（+S5-U）は、専用ベアラーの作成に成功したという通知を PCF に送信します。 |
| 12 | EPS フォールバック ガード タイマーが停止します。 |
| 13 | PCF が SMF に「200 OK」の確認応答を送信（+S5-C） |
| 引き継ぎが完了する前に EPS フォールバック タイマーが期限切れになるシナリオでは、ステップ 14 ー 16 が発生します。 | |
| 14 | SMF（+S5-C）は、専用ベアラー作成の失敗通知を PCF に送信します。 |
| 15 | PCF は「200 OK」の確認応答を SMF（+S5-C）に送信します。 |
| 16 | 5G から 4G へのハンドオーバー手順が続行されます。 |

## 標準準拠

EPS フォールバック ガード タイマー サポート機能は、次の規格に準拠しています：

- *3GPP TS 23.502 V16.1.1（2019-06）*

# EPS フォールバック ガード タイマーの構成

この項では、EPS フォールバック ガード タイマー機能の構成方法について説明します。

```
config
  profile access test [ eps-fallback | n2 | n26 ]
  eps-fallback guard timeout timeout_value
  n26 idft enable timeout n26_timeout_value
  n2 idft enable timeout n2_timeout_value
  end
```

注：

- **profile access**：プロファイル構成にアクセスします。
- **test**：プロファイル インスタンスにアクセスします。
- **eps-fallback**：EPS フォールバック 構成を入力します。

- **eps-fallback guard timeout**：EPS フォールバック タイマーの値を 500 ～ 15000 ミリ秒の範囲で入力します。
- **n26**：E-UTRAN および NG-RAN の構成である N26 インターフェイスを開始します。
- **n2**：NG-RAN 構成の N2 インターフェイスを開始します。
- **idft enable timeout**：IDFT タイマーが期限切れになるまでの値（15 ～ 60）を入力します。

# EPS フォールバック レポートの生成

**表 *58* : 機能の履歴**

| 機能名 | リリース情報 | 説明 |
|---|---|---|
| EPS フォールバック レポート | 2024.01 | SMF が、PCF によって EPS_FALLBACK トリガが送信された PCC ルールの EPS フォールバック レポート機能をサポートしています。<br>**デフォルト設定**：コンプライアンス バージョン 16.10.0 が npcf-smpolicycontrol に設定されている場合に有効になります。 |

## 機能説明

SMF により、PCC ルールの EPS フォールバック レポートの PCF からの EPS_FALLBACK ポリシー制御要求トリガーが許可されます。次の機能が発生します：

- **supported-features** リストで **EPSFallbackReport** が有効になっていて、PCF が値「EPS_FALLBACK」を使用してトリガー「policyCtrlReqTriggers」を使用している場合、SMF は「reqData」を使用して「lastReqRuleData」属性で参照される PCC ルールの EPS フォールバックを PCF に通知します。属性値を EPS_FALLBACK として設定します。
- SMF では、PCF への EPS フォールバックを示すために、SmPolicyUpdateContextData に次のものが含まれます。
  - 「repPolicyCtrlReqTriggers」属性内の「EPS_FALLBACK」値。
  - 「ruleStatus」属性が ACTIVE に設定されている「ruleReports」属性に含まれる「pccRuleIds」属性内の影響を受ける PCC ルール。

重要 EPS フォールバック レポートを有効にするには、npcf-smpolicycontrol のコンプライアンス バージョンを 16.10 に構成してください。0

# 機能の仕組み

EPS フォールバック レポートは、EPS フォールバック後に実行されます。レポート手順は、PCF によって EPS_FALLBACK トリガーが送信され、EPS フォールバック後にリソース セットアップも成功した pccRules に対してのみ実行されます。

## コール フロー

次のコール フローは、EPS フォールバック レポートの処理手順を示しています。

図 *49 : EPS* フォールバック レポートのコール フロー

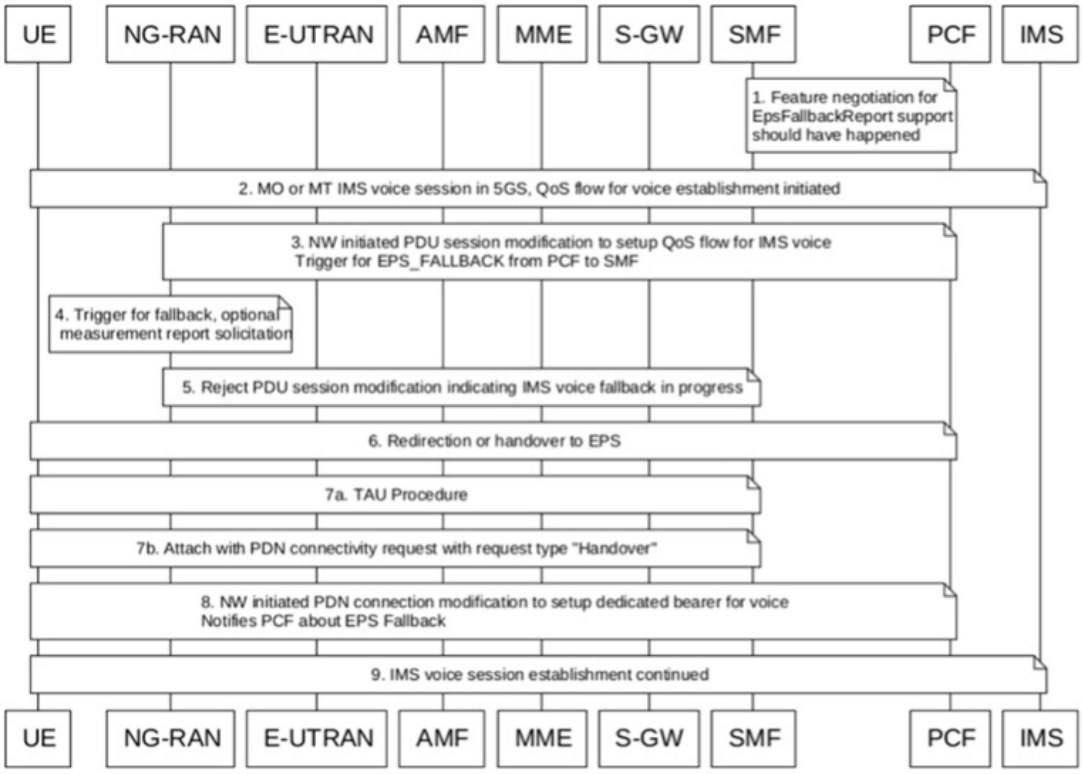


表 *59 : EPS* フォールバック ガード タイマー コール フローの説明

| 手順 | 説明 |
|---|---|
| 1 | EPSFallbackReport サポートの機能ネゴシエーションは、セッションの確立中に SMF と PCF の間で行われている必要があります。 |
| 2 | UEは、5GSのNG-RAN を使用して、モバイル発信（MO）またはモバイル着信（MT）IMS通話の確立手順を開始します。 |
| 3 | 音声の QoS フローを設定するためにネットワークが開始した PDU セッション変更要求が NG-RAN に到達します。PCF は、EpsFallbackReport の EPS_FALLBACK トリガを使用して SMF にも対応します。 |
| 4 | NG-RAN は、IMS 音声の EPS フォールバックをサポートするように構成されています。UE の機能に基づき、AMF からの指示により、音声、ネットワーク構成、および無線条件における EPS のフォールバックを再ルーティングするため、NG-RAN は EPS へのフォールバックをトリガします。<br>NG-RAN は、E-UTRAN をターゲットとして、UEから測定報告の収集を開始します。 |
| 5 | NG-RANは、ステップ 3 で受信した PDU セッション変更要求を拒否し、IMS 音声のフォールバックによるモビリティが進行中であることを示します。<br>NG-RAN は、AMF を介した SMF への PDU セッション応答メッセージとしてステップ 3 で受信した IMS 音声の QoS フローを構成するための PDU セッション変更の拒否を示します。このメッセージには、IMS 音声のフォールバックに伴う現在の移動に関する詳細が含まれています。SMF は、QoS フローに関連する PCC ルールを維持しています。<br>ローミング シナリオの場合、PDU セッション応答メッセージは V-SMF を介して H-SMF に送信されます。<br>または<br>NG-RAN は、EPS へのフォールバックをトリガする可能性がある構成済みの原因で応答します。gNB によって送信された原因が SMF で構成された EPS フォールバックの原因と一致する場合、次の手順で説明したように動作し続けます。6 以降。<br>（注）<br>SMF での構成により、gNB が「IMS 音声 EPS フォールバックまたは RAT フォールバックがトリガされた」という理由で N2 メッセージを拒否した場合でも、構成された原因を常にチェックします。 |
| 6 | UE の機能に基づいて、NG-RAN は EPS へのハンドオーバーを開始します。PCF がサブスクライブされている場合、SMF は RAT タイプの変更を報告します。<br>EPS フォールバックの障害を追跡するためのタイマーが開始します。タイマーが期限切れになると、SMF は専用ベアラー作成の失敗を PCF に通知します。 |
| 7a | 5GS から EPS へのハンドオーバーの場合、UE は TAU 手順を開始します。 |
| 7b | UE は、PDN 接続要求を「ハンドオーバー」要求タイプで送信します。 |

| 手順 | 説明 |
|---|---|
| 8 | 5GS から EPS へのハンドオーバー手続きが完了した後、SMF または PGW-C は IMS 音声用の専用ベアラーの構成を再初期化し、5G の QoS を EPC の QoS パラメータにマッピングします。SMF は、PCF がサブスクライブされている場合、EPS フォールバック、成功したリソース割り当て、およびアクセス ネットワーク情報について通知します。 |
| 9 | IMS 音声セッション確立が続行します。 |

（注） この機能が SMF で有効になっているが、最初のネゴシエーション中に PCF によって記載されておらず、PCF が引き続き PolicyControlRequestTrigger を EPS_FALLBACK として送信する場合、SMF はこのトリガで機能し、EPS フォールバック レポートがEPS フォールバックの場合の PCF に送信されます。

# SMF での EPS セッションのベアラー変更

表 *60 :* 機能の履歴

| 機能名 | リリース情報 | 説明 |
|---|---|---|
| HSS によって開始されるベアラー QoS の変更 | 2023.04 | APN-AMBR と、任意で 1 つ以上の EPS ベアラー QoS パラメータを変更するには、SMF は HSS によって開始されるベアラー QoS 変更手順を使用します。<br>**[デフォルト設定（Default Setting）]**：有効 – 常時オン |

## 機能説明

### 5G コア ネットワークを介した EPS インターワーキング

SMF は、PCF または MME が開始する EPS ベアラーの変更をサポートします。SMF + PGW は、この機能の次のトリガーを処理します：

- QoS 変更。
- RAT、URI、および SGW の変更。
- UE タイムゾーンの変更。

### Diameter インターフェイスとの SMF インターワーキング

SMF は、次の機能によるトラッキング エリア更新情報の EPS ベアラーの変更をサポートします。

- PCRF によって開始された RAR
- S-GW の変更による E-UTRAN PDN の変更
- S-GW の変更なしの E-UTRAN PDN の変更
- HSS によって開始される QoS の変更

## 機能の仕組み

SMF 上の EPS セッションのベアラー変更は、次の変更と機能します：

- SMF での EPS セッションに対する PCF および MME 開始ベアラーの変更：これらの手順は、1 つまたは複数の EPS ベアラー QoS パラメータ QCI、GBR、MBR、または ARP が変更されるか、APN-AMBR を変更するために使用されます。PCF によって開始されたまたは MME によって開始されたベアラーの変更手順は、非 GBR リソース タイプの QCI から GBR リソース タイプ QCI への変更、およびその逆の変更をサポートしていません。
- [SMF に接続された EPS セッションでの X2 および S1 ベースのハンドオーバー（X2 and S1 Based Handover for EPS Session Connected to SMF）]：X2 ベースのハンドオーバー手順は、X2 を使用して送信元 eNodeB からターゲット eNodeB に UE をハンドオーバーするために使用されます。この手順では、MME は変更されず、MME は SGW の再配置を決定します。

  S1 ベースの引き継ぎ手順は、X2 ベースの引き継ぎが使用できない場合に使用されます。ソース eNodeB は、S1-MME 参照ポイントを介して Handover Required メッセージを送信して、ハンドオーバーを開始します。この手順により、MMEまたはSGWが再配置される可能性があります。

### コール フロー

ここでは、次のコール フローについて説明します：

- SMF コール フローでの EPS セッションの PCF によって開始されたベアラーの変更
- SMF コール フローでの EPS セッションの MME 開始ベアラーの変更
- SMF コール フローに接続された EPS セッションの X2 および S1 ベースのハンドオーバー

#### *SMF* での *EPS* セッションの *PCF* によって開始されたベアラーの変更

このセクションでは、SMF コール フローでの EPS セッションの PCF によって開始されたベアラーの変更について説明します。

***Figure 50: PCF*** によって開始されるベアラーの変更のコール フロー

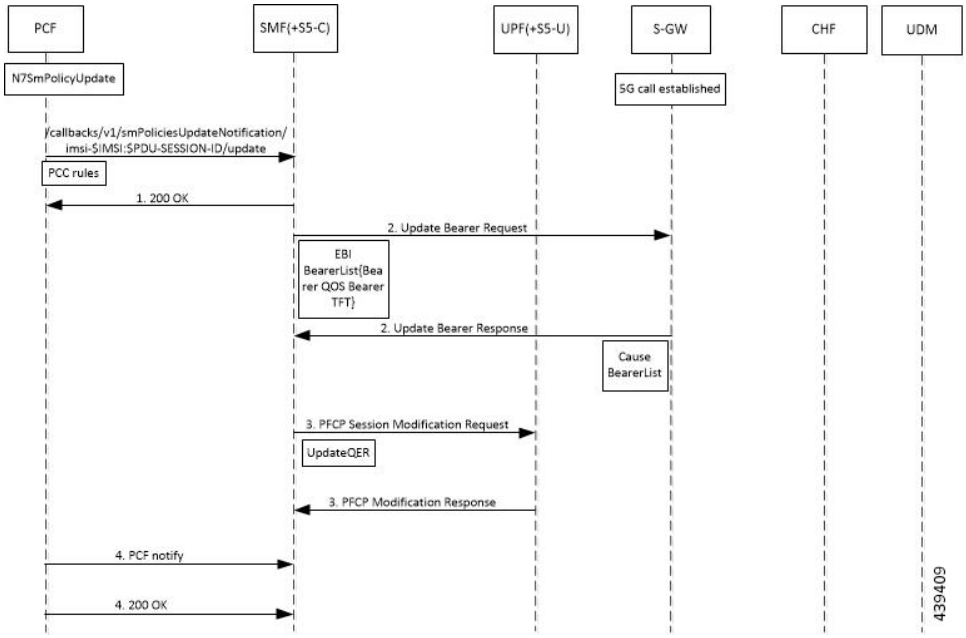



***Table 61: PCF*** によって開始されたベアラーの変更のコール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | PCF は、SMF に対する QoS または TFT の更新されたパラメータを使用して N7 ポリシー更新通知を開始します。 |
| 2 | SMF は「200 OK」の確認応答を PCF に送信します。PCF が提供する PCC ルールは、変更された専用ベアラの TFT にマッピングされます。関連付けられた QoS は 4G QoS にマッピングされます。 |
| 3 | SMF は、SGW にベアラー要求の更新を送信します。 |
| 4 | SGW は、EPS ベアラー ID および関連付けられたベアラー用に変更された QoS または TFT を使用して、SMF にベアラー応答の更新を送信します。 |
| 5 | SMF は UPF への PFCP 変更要求を開始します。 |
| 6 | UPF は、更新された QER を使用して SMF に PFCP 変更応答を送信します。 |
| 7 | SMF が PCF に PCF 通知メッセージを送信します。 |
| 8 | PCF は「200 OK」の確認応答を SMF に送信します。 |

## *EPS* セッションの *MME* 開始ベアラーの変更

このセクションでは、SMF コール フローでの EPS セッションの MME によって開始される専用ベアラーの変更について説明します。

*Figure 51: MME*によって開始されるベアラーの変更のコール フロー

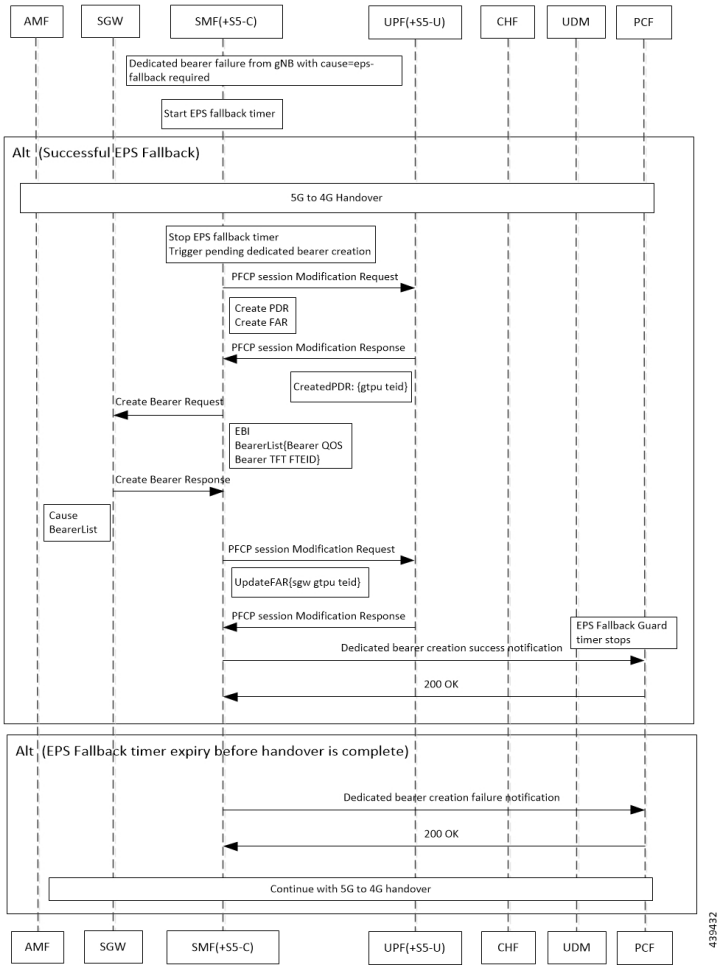



*Table 62: PCF*によって開始されるベアラーの変更のコール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | HSS は MME に Insert Subscriber Data メッセージを送信します。サブスクリプション データには、IMSI、EPS のサブスクライブされた QoS（QCI と ARP）、およびサブスクライブされた UE-AMBR と APN-AMBR に関する詳細が含まれます。 |
| 2 | サブスクライブされた UE-AMBR が変更された場合、MME は新しい UE-AMBR 値を計算し、Modify Bearer コマンドを SGW に送信します。 |
| 3 | SGW は、Modify Bearer Command メッセージを SMF または PDN GW に送信します。このメッセージには、EPS ベアラー ID、EPS ベアラー QoS、および APN-AMBR に関する詳細が含まれています。 |
| 4 | SMF または PDN GW は、更新された APN-AMBR を PCF に送信します。 |

| ステップ | 説明 |
|---|---|
| 5 | PCF は、更新された PCC 決定を SMF または PDN ゲートウェイに送信します。PCF は、SMF または PDN GW への応答として、デフォルトのベアラーに関連付けられている APN-AMBR を変更します。 |
| 6 | SMF は、SGW にベアラー要求の更新を送信します。 |
| 7 | SGW が MME にベアラー要求の更新を送信します。この要求メッセージには、EBI、EPS ベアラー QoS、TFT、および APN-AMBR の詳細が含まれています。 |
| 8 | MME が SGW にベアラー応答の更新を送信します。 |
| 9 | SGW は、ベアラーの変更の確認としてベアラーの更新応答を SMF または PDN ゲートウェイに送信します。応答メッセージには、EBI の詳細とユーザーの場所情報が含まれます。 |
| 10 | UPF が SMF に PFCP セッション変更応答を送信します。PCF から受信した PCC デシジョン プロビジョニング メッセージ（QoS ポリシー）に基づいて、SMF または PDN GW は、専用ベアラの変更手順を開始します。SMF または PDN GW は QoS ポリシーを使用して、サービスデータフローをアクティブなベアラーに追加するのか、またはアクティブなベアラーから削除するのか、またはサービスデータフローの承認された QoS を変更するのかを決定します。 |
| 11 | UPF は PFCP パラメータを更新し、PFCP セッション変更応答を SMF または PDN GW に送信します。UPF は、PFCP セッションの変更が正常に行われたことを確認します。 |
| 12 | SMF または PDN GW は、要求された PCC が適用されたかどうかの決定について PCF に通知します。 |
| 13 | PCF は「200 OK」の確認応答を SMF または PDN GW に送信します。 |

## *SMF* に接続された *EPS* セッションの *X2* および *S1* ベースのハンドオーバー

このセクションでは、SMF に接続された EPS セッションの X2 および S1 ベースのハンドオーバーについて説明します。

*Figure 52: SMF* に接続された *EPS* セッションでの *X2* および *S1* ベースのハンドオーバーのコール フロー

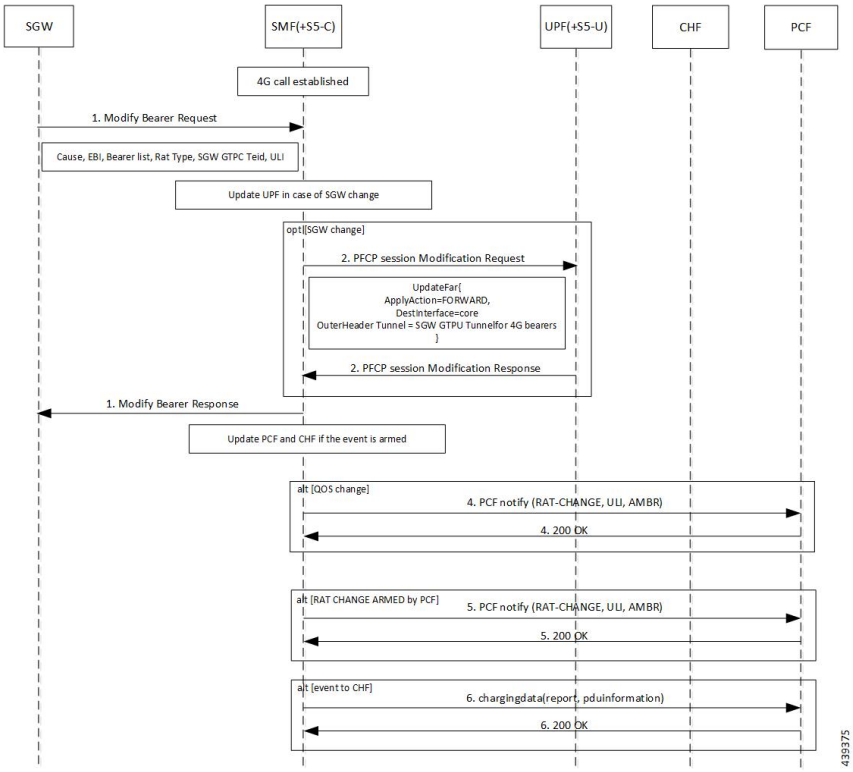


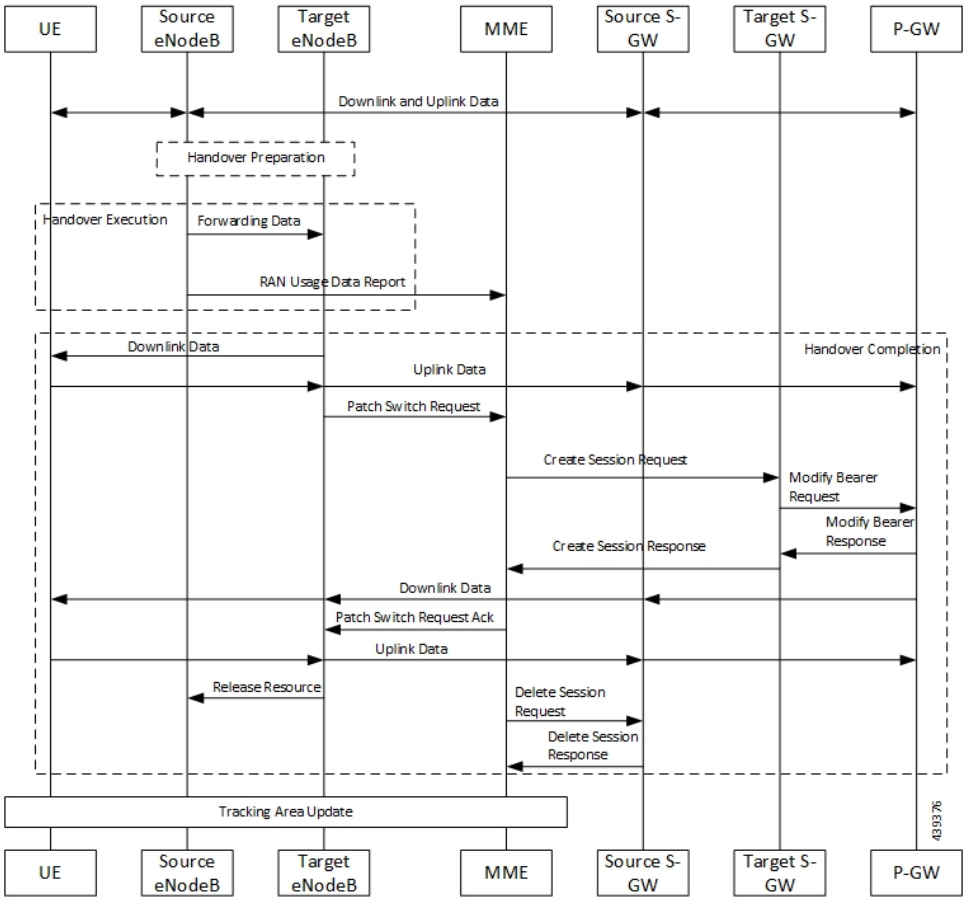

*Table 63: X2* および *S1* ベースのハンドオーバーのコール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | SGW は、SMF にベアラー要求の変更を送信します。この要求には、ユーザー ロケーション情報 IE、UE タイムゾーン IE、および MME から受信した関連する PDN GW 情報への PDN 接続ごとのサービング ネットワーク IE が含まれます。 |
| 2 | S-GW が変更された場合、SMF または PGW-C は PFCP セッション変更要求を UPF に送信します。 |
| 3 | ステップ 2 が発生した場合、UPF は SMF または PDN GW に PFCP セッション変更応答を送信します。 |
| 4 | UPF からの応答を受信した後、SMF または PGW-C は、Modify Bearer Response を S-GW に送信します。 |
| 5 | PCF が QoS 変更の通知を待機している場合、SMF または PGW-C は PCF に通知を送信します。 |
| 6 | ステップ 5 が発生した場合、PCF は「200 OK」の確認応答を SMF または PGW-C に送信します。 |

| ステップ | 説明 |
|---|---|
| 7 | PCF が ULI または RAT の変更に関する通知を待機している場合、SMF または PDN GW は PCF に通知を送信します。 |
| 8 | ステップ 7 が発生した場合、PCF は「200 OK」の確認応答を SMF または PDN GW に送信します。 |
| 9 | CHF が QoS、URI、または RAT の変更に関する通知を待機している場合、SMF または PDN GW は PCF に通知を送信します。 |
| 10 | ステップ 9 が発生した場合、PCF は「200 OK」の確認応答を SMF または PDN GW に送信します。 |

次のコール フローは、S-GW の再配置を伴う X2 ベースのハンドオーバーを示しています。

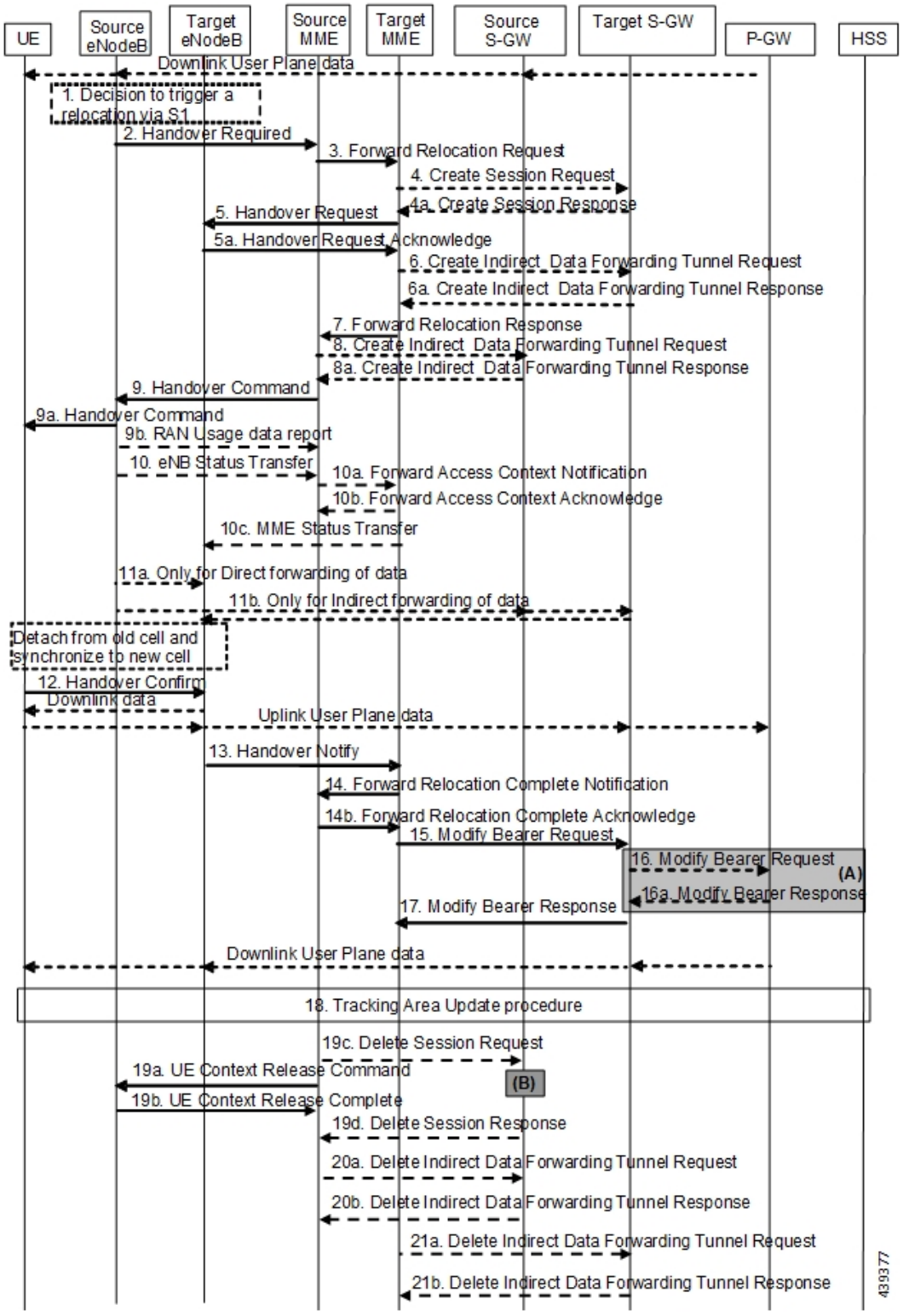
***Figure 53: SGW* 再配置コール フローと一緒の *X2* ベースのハンドオーバー**




コール フローの説明については、 *3GPP TS 23.401*の 5.5.1.1.3「X2-based handover with Serving GW relocation」のセクションを参照してください。

次のコール フローは、S1 ベースのハンドオーバーを示しています：

***Figure 54: S1*** ベースのハンドオーバー コール フロー



コール フローの説明については、 *3GPP TS 23.401*、バージョン *15.8.0*の 5.5.1.2.2「S1-based handover, normal」を参照してください。

## *PCRF* によって開始された *RAR/CCAU*

次の図は、E-UTRAN ネットワーク クレジット制御応答の更新（CCAU）または再許可要求（RAR）によって開始された 更新ベアラ要求（UBR）のコール フローを示しています。

**図 *55 : E-UTRAN* ネットワーク（*PCRF*）の *CCAU/RAR* 開始 *UBR* のコール フロー**

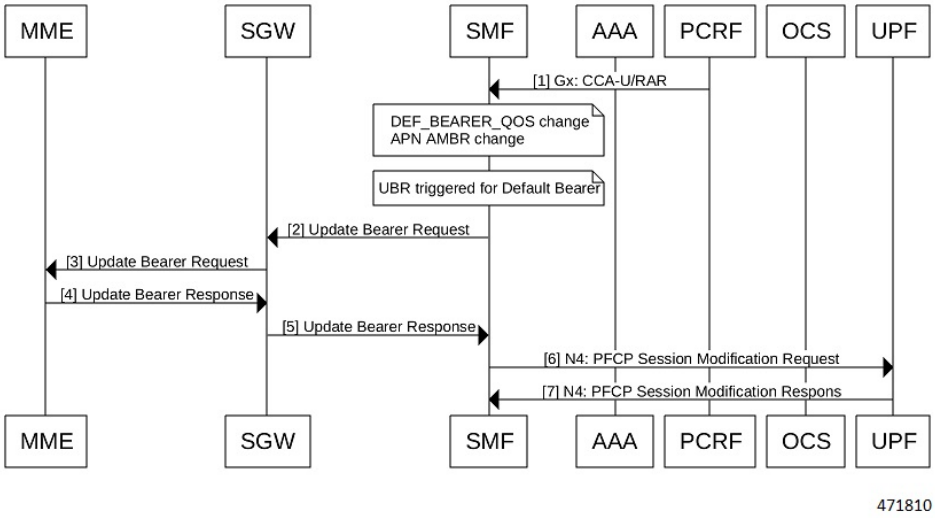



**表 *64 : PCRF* によって開始された *CCAU* または *RAR* のコール フローの説明**

| 手順 | 説明 |
|---|---|
| 1 | PCRF は、変更されたデフォルトのベアラー QoS や APN AMBR の変更とともに、RAR を SMF に、または CCAU を SMF に送信します。 |
| （注）<br>デフォルトのベアラー QoS および/または APN AMBR のいずれかが変更されたため、UBR がデフォルト ベアラーに対してトリガされます。 | |
| 2 | SMF は、更新されたデフォルトのベアラー QoS や APN AMBR とともに、更新されたベアラー要求を S-GW に送信します。 |
| 3 | SGW が MME にベアラー要求の更新を送信します。 |
| 4 | MME が S-GW にベアラー応答の更新を送信します。 |
| 5 | SGW は、SMF にベアラー応答の更新を送信します。 |
| 6 | SMF は、N4 PFCP セッション変更要求を UPF に送信して、ベアラー レベル情報（デフォルトのベアラー QoS が変更された場合）および/または APN AMBR QER（APN AMBR が変更された場合）を更新します。 |

| 手順 | 説明 |
|---|---|
| 7 | UPF が SMF に N4 PFCP セッション変更応答を送信します。 |

## *S-GW* の変更による *E-UTRAN PDN* の変更

次の図は、S-GW の変更による PDN の変更のコール フローを示しています。

**図 *56 : S-GW* の変更のない *E-UTRAN PDN* の変更**

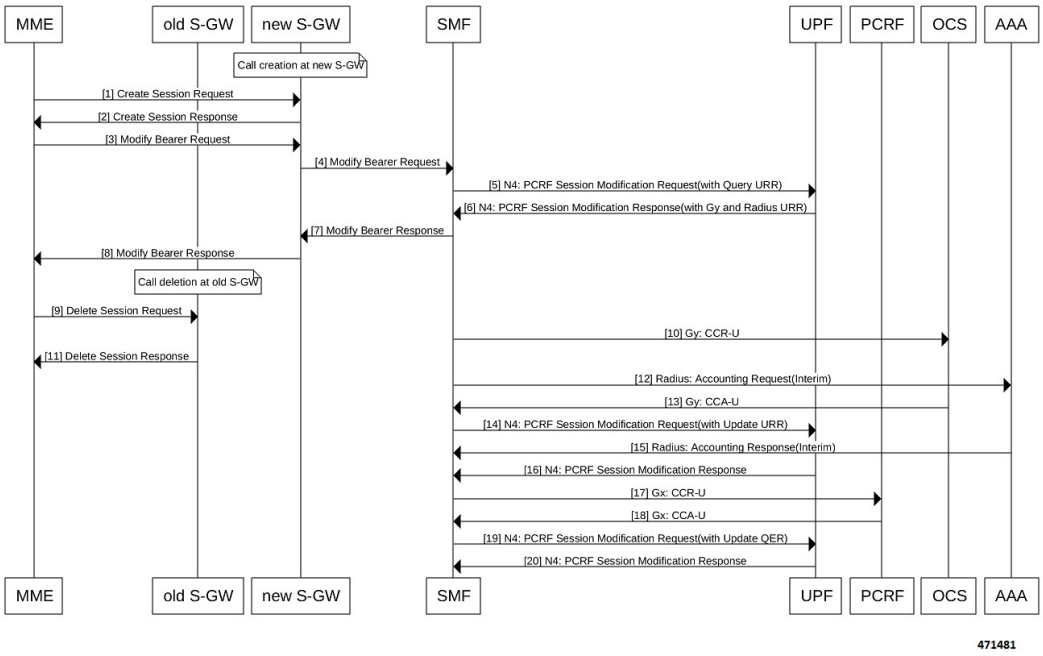



**表 *65 : S-GW* の変更による *PDN* の変更のコール フローの説明**

| 手順 | 説明 |
|---|---|
| 1 | 新しい S-GW でのコール作成の一環として、MME は新しい S-GW にセッション要求の作成を送信します。 |
| 2 | 新しい S-GW が MME に「セッション応答の作成」で応答します。 |
| 3 | MME が、ベアラー要求の変更を新しい S-GW に送信します。 |
| 4 | 新しい S-GW は、ベアラー要求の変更を SMF に転送します。 |
| 5 | SMF は、イベント トリガに基づいて、クエリ URR を持つセッション変更要求を UPF に送信します。<br>（注）<br>S-GW 変更の serv-node-change イベント トリガ。 |

| 手順 | 説明 |
|---|---|
| 6 | UPF は、Gy および RADIUS の構成に基づいて、SMF に対して N4：PCRF セッション変更応答（Gy および RADIUS URR を含む）を返します。この構成は有効または無効に設定可能です。 |
| 7 | 新しい S-GW が新しい S-GW に「ベアラー変更応答」で送信します。 |
| 8 | 新しいSGW-C が、ベアラー応答の変更を MME に転送します。 |
| 9 | 古い S-GW でのコール削除の一環として、MME は新しい S-GW にセッション要求の削除を送信します。 |
| 10 | SMF は CCR-U を OCS に、アカウンティング要求（Interim）を AAA に送信します。 |
| 11 | 古い S-GW はセッション応答の削除を MME に送信します。 |
| 12 | OCS と AAA は、それぞれ CCA-U と中間アカウンティング応答で SMF に応答します。 |
| 13 | SMF は更新 URR を持つ PCRF セッション変更要求を UPF に送信します。 |
| 14 | UPF は PCRF セッション変更応答で SMF に応答します。 |
| 15 | イベント トリガが用意されている場合、SMF は PCRF に対して CCR-U を送信します。<br>（注）<br>AN_GW_CHANGE イベントは、S-GW の変更に対してトリガします。 |
| 16 | PCRF は CCA-U で SMF に応答します。 |
| 17 | SMF は更新 QER を持つ PCRF セッション変更要求を UPF に送信します。 |
| 18 | SMF が UPF に PFCP セッション変更応答を送信します。 |

### *S-GW* の変更なしの *E-UTRAN PDN* の変更

次の図は、S-GW の変更がない PDN の変更のために 3GPP リファレンスから派生したコールフローを示しています。

図 *57 : S-GW* の変更なしの *PDN* 変更のコール フロー

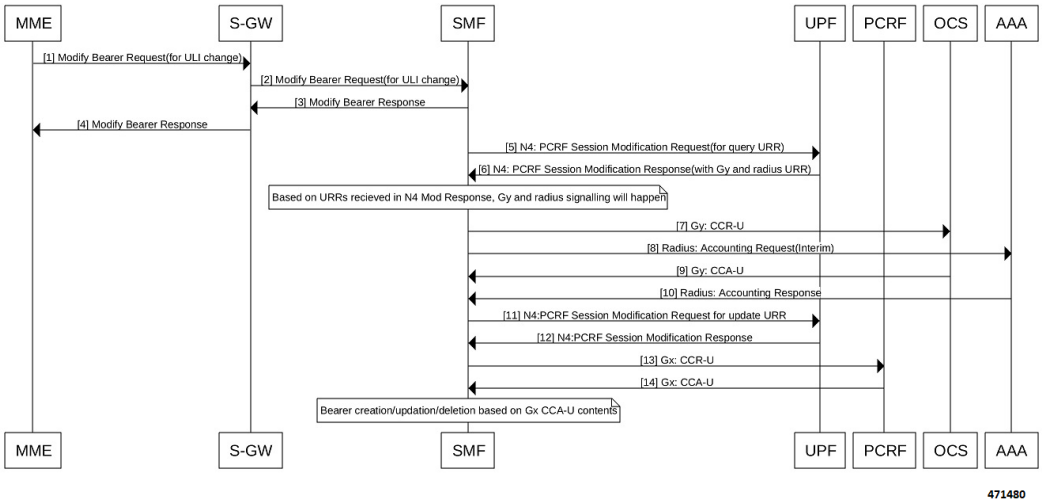



表 *66 : S-GW* 変更なしの *PDN* 変更のコールフローの説明

| 手順 | 説明 |
|---|---|
| 1 | MME が、ベアラー要求の変更（ULI 変更用）を S-GW に送信します。 |
| 2 | S-GW は、ベアラー応答の変更を SMF に転送します。<br>（注）<br>セッションが存在し、切断状態でない場合、SMF は成功を送信し、以降の処理を行います。 |
| 3 | SMF は、ベアラー応答の変更を S-GW に送信します。 |
| 4 | S-GW が、ベアラー応答の変更を MME に転送します。 |
| 5 | SMF は、イベント トリガーに基づいて、クエリ使用状況レポート ルール（URR）の N4 セッション変更要求を UPF に送信します。<br>（注）<br>user-loc-change イベントは、URI の変更をトリガーします。 |
| 6 | UPF は、Gy と RADIUS の構成に基づいて、Gy および有効または無効にすることができる RADIUS URR SMF を使用した N4 セッション変更応答で応答します。 |
| 7 | N4 セッション変更応答、Gy、および RADIUS シグナリングは、N4 変更応答で受信した URR に基づいて発生します。 |
| 8 | SMF は CCR-U を OCS に、RADIUS アカウンティング要求を AAA に送信します。 |
| 9 | OCS は、CCA-U および RADIUS アカウンティング応答付き AAA で応答します。 |
| 10 | SMF は、URR の更新の N4 セッション変更要求を UPF に送信します。 |

| 手順 | 説明 |
|---|---|
| 11 | UPF が SMF に N4 セッション変更応答を送信します。 |
| 12 | イベント トリガーが機能している場合、SMF は CCR-U を PCRF に送信します。<br>（注）<br>USER_LOCATION_CHANGE イベントは、URI の変更をトリガーします。 |
| 13 | 次に、PCRF は CCA-U を SMF に送信します。 |
| 14 | Gx CCA-U のコンテンツに基づいてベアラーの作成、更新、または、削除が行われます。 |

## *Diameter* インターフェイスを使用した *SMF* の *HSS* 開始ベアラー *QoS* の変更

APN-AMBR と、任意で 1 つ以上の EPS ベアラー QoS パラメータを変更するには、HSS 開始ベアラー QoS 変更手順を使用します。たとえば、EPS ベアラーの QoS パラメータは、デフォルトの EPS ベアラーの QCI または ARP にすることができます。HSS がデフォルトのベアラー QCI、または ARP と APN-AMBR を変更すると、HSS はそのようなメッセージを MME に対して開始し、MME は S-GW を介して P-GW に対してベアラーの変更コマンド（MBC）を生成します。

次のコールフローは、HSS によって開始されたベアラー QoS の変更の手順を示しています。

**図 *58 : HSS* によって開始されたベアラー *QoS* の変更でのコール フロー**

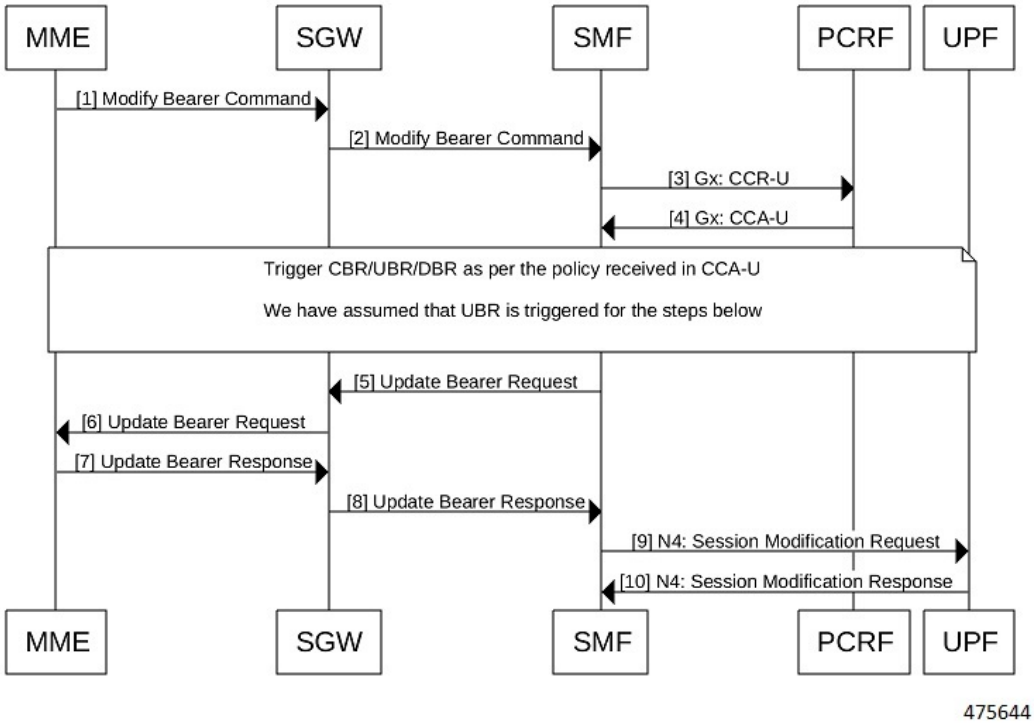


表 *67 : HSS* によって開始されたベアラー *QoS* の変更に関するコール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | MME は、HSS が開始したサブスクライブ QoS の変更手順の一環として、S-GW にベアラー コマンドの変更を送信します。 |
| 2 | S-GW はベアラー変更コマンドを SMF に送信します。 |
| 3 | SMF は、APN AMBR の変更、およびオプションでデフォルトのベアラー QoS の変更（PCRF によるサブスクライバである場合）の関連イベント トリガーとともに、Gx CCR-U を PCRF に送信します。要求されたデフォルトのベアラー QoS、APN-AMBR は PCRF に送信され、PCRF からの承認された値が他のポリシーとともにサブスクライバに適用されます。<br>たとえば、Dynamic Rules が適用されます。と、デフォルトのベアラー QoS の変更（PCRF によってサブスクライバされている場合）。 |
| 4 | PCRF は Gx CCA-U を SMF に送信します。<br>（注）<br>CCA-U および N4 通信の一部として適用されるすべての課金サポートは、Gy/RADIUS トリガーを介して継続されます。 |
| （注）<br>PCRF から受信したポリシーに基づいて、CBR、UBR、または DBR のいずれかの手順がトリガーされます。 | |
| 5 | SMF は、新しい APN AMBR とデフォルトのベアラー QoS 値を使用して、S-GW にベアラーの更新要求を送信します。 |
| 6 | SGW は、新しい APN AMBR とデフォルトのベアラー QoS 値を使用して、MME にベアラー更新要求を送信します。 |
| 7 | MME が S-GW にベアラー応答の更新を送信します。 |
| 8 | S-GW は、SMF にベアラー応答の更新を送信します。 |
| 9 | SMF は、APN AMBR とデフォルトのベアラー QoS がそれぞれ PCRF によって更新された場合、APN AMBR QER とベアラー レベル情報を更新するために、PFCP セッション変更要求を UPF に送信します。 |
| （注）<br>QER の更新とともに、CCA-U を介した、または PCRF が無効になっているときにベアラーの変更コマンドを使用してデフォルトのベアラー QoS の変更がある場合、UPF への PFCP セッション変更要求には更新 PDR があり、これは他の手順に一般的です。 | |
| 10 | UPF が SMF に PFCP セッション変更応答を送信します。 |

# ルールベースの変更によるベアラー コマンドの変更

次のコール フローは、Gx CCA-U のポリシー サーバーから受信したルールベースの変更によりベアラー コマンドを変更する手順を示しています。

**図 *59 :* ルールベースの変更を伴うベアラー コマンドのコール フロー**

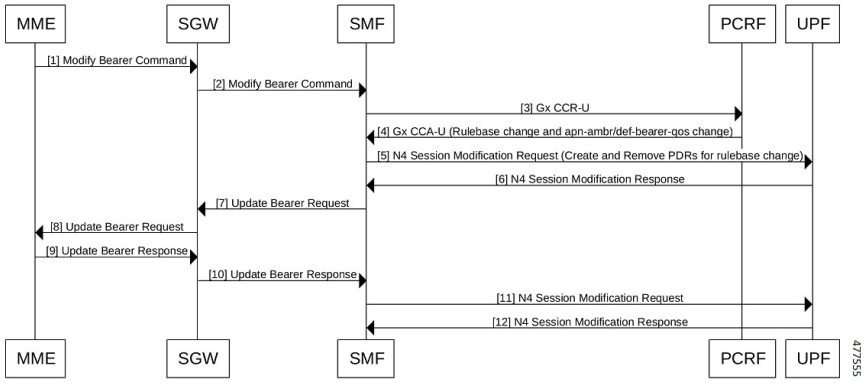



**表 *68 :* ルールベースの変更を伴うベアラー コマンドのコール フローの説明**

| ステップ | 説明 |
|---|---|
| 1 | MME は、HSS が開始した登録済み QoS 変更手順の一部として S-GW にベアラー変更コマンドを送信します。 |
| 2 | S-GW は、SMF にベアラー変更コマンドを送信します。 |
| 3 | SMF は、APN AMBR の変更、およびオプションでデフォルトのベアラー QoS の変更（PCRF によるサブスクライバである場合）の関連イベント トリガーとともに、Gx CCR-U を PCRF に送信します。 |
| 4 | PCRF は、ルールベースの変更、および APN-AMBR とデフォルトのベアラー QoS の変更を伴う Gx CCA-U を SMF に送信します。 |
| 5 | SMF は、ルールベースの変更のために PDR を作成および削除することとともに、N4 セッション変更要求を UPF に送信します。 |
| 6 | UPF が N4 セッション変更応答を送信します |
| 7 | SMF は、新しい APN AMBR とデフォルトのベアラー QoS 値を使用して、SGW にベアラーの更新要求を送信します。 |
| 8 | S-GW は、新しい APN-AMBR とデフォルトのベアラー QoS 値を使用して、MME にベアラー要求の更新を送信します。 |
| 9 | MME が S-GW にベアラー応答のアップデートを送信します。 |

| ステップ | 説明 |
|---|---|
| 10 | S-GW が SMF にベアラー応答のアップデートを送信します。 |
| 11 | SMF は、APN AMBR とデフォルトのベアラー QoS がそれぞれ PCRF によって更新された場合、APN AMBR QER とベアラー レベル情報を更新するために、PFCP セッション変更要求を UPF に送信します。 |
| （注）<br>QER の更新とともに、PCRF が無効になっているときに CCA-U を介してまたは MBC を使用してデフォルトのベアラー QOS の変更がある場合、UPF への PFCP セッション変更要求には他の手順に一般的な PDR の更新も含まれます。 | |
| 12 | UPF が SMF に PFCP セッション変更応答を送信します。 |

## ベアラーコマンドの変更の障害

次のコール フローは、ベアラーコマンドの変更が失敗した場合の手順を示しています。

**図 *60* : ベアラー コマンドの変更失敗時のコール フロー**

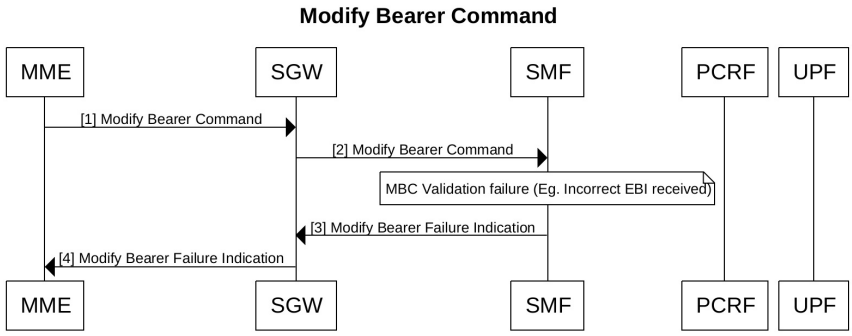



**表 *69* : ベアラー コマンドの変更の失敗におけるコール フローの説明**

| ステップ | 説明 |
|---|---|
| 1 | MME は、HSS が開始した登録済み QoS 変更手順の一部として S-GW にベアラー変更コマンドを送信します。 |
| 2 | S-GW は、SMF にベアラー変更コマンドを送信します。 |
| （注）<br>MBC 検証エラーが発生します。たとえば、Modify Bearer コマンドで誤った EBI を受信したとします。 | |

| ステップ | 説明 |
|---|---|
| 3 | SMF は、S-GW へベアラー障害表示の変更を送信します。 |
| 4 | SMF は、MME へベアラー障害表示の変更を送信します。 |

## ベアラー コマンド再送信処理の変更

これらのシナリオでは、MBC 再送信は次のように処理されます：

- MBC がまだ進行中であるか、MBC が正常に処理されているときに再送信を受信した場合、その再送信は適切なログと統計情報とともにドロップされます。
- MBC が MB 障害通知を行ったときに再送信を受信すると、SMF はキャッシュされている MB 障害通知で応答します。
- smf-service でアフィニティが失われた後に再送信を受信すると、新しい MBC として扱われます。

## ベアラー コマンド シナリオおよび関連する UBReq 値の変更

ポリシー サーバを使用した標準の MBC シナリオでは、PCRF から承認された **APN-AMBR** および **Def-bearer-QOS** の値が、UBReq で S-GW に送信される最終値です。ただし、いくつかの例外的な MBC シナリオでは、動作は異なります。次のテーブルでは、これらのシナリオについて説明します。

| シナリオ | 説明 |
|---|---|
| 空の Gx CCA-U を含む MBC | UBR は、以前の PCRF 承認値でトリガされます。 |
| APN-AMBR および def-bearer-qos の変更に関するイベント トリガがないため、MBC 用の Gx CCR-U はありません。 | UBR は、MBC で受信した値でトリガされます。 |
| 既存のセッション値と同じ APN-AMBR および def-bearer-qos 値を持つ MBC。したがって、MBC の Gx CCR-U はありません。 | UBR は、既存のセッション値でトリガされます。<br>（注）<br>UPF に通信される変更がないため、UBR 後の N4 の変更は必要ありません。 |
| APN-AMBR および def-bearer-qos 値が異なる MBC ただし、Gx CCA-U で PCRF から受信した値は既存のセッション値と同じです | UBR は PCRF から受信した値でトリガされます。<br>（注）<br>UPF に通信される変更がないため、UBR 後の N4 の変更は必要ありません。 |

| | |
|---|---|
| Gx 構成なし：MBC で受信した値で UBR がトリガされます。 | UBR は、MBC で受信した値でトリガされます。 |
| アクションが続行しその後 MBC が続く：MBC で受信した値で UBR がトリガされた Gx CCA-I 障害 | UBR は、MBC で受信した値でトリガされます。 |
| アクションの継続での MBC の Gx CCA-U 障害：MBC で受信した値で UBR がトリガされました。 | UBR は、MBC で受信した値でトリガされます。 |

## 標準準拠

SMF での EPS セッションのベアラ変更機能は、次の標準に準拠しています：

- *3GPP TS 23.401*
- *3GPP TS 23.502 V16.1.1*（*2019-06*）
- *3GPP TS 29.274*、バージョン *15.8.0*

# EPS および 5GC インターワーキングのセッション管理手順

## 機能説明

*3GPP TS 23.502* で定義されている 5G セッション管理の手順により、5G NR 無線への最初の接続を実行した後に UE が LTE 4G 無線に移行した場合、EPS インターワーキングが正常に行われることが保証されます。

### NAS メッセージでのパケット フィルタ数のサポート

UE は、PDU 確立および変更要求メッセージでパケット フィルタ IE の数を SMF に送信します。デフォルトでは、UE は最大 16 個のパケット フィルタを送信します。

UE は、次のシナリオで 16 を超えるパケット フィルタをサポートします：

- UE が N1 モードで SMF に接続している場合。
- S1 モードでの SMF への初期接続が完了し、4G から 5G へのハンドオーバーが進行中の場合。

SMF は、「NumOfPackFilter」フィールドで PolicyCreateControl の PCF に最大フィルタ数を送信します。パケット フィルタ数 IE が N1 モードの UE から受信された場合、SMF は PDU 確立要求の「サポートされるフィルタの最大数」フィールドを使用します。この IE を N1 モードの UE から受信しなかった場合、または受信した値が 16 未満の場合、SMF は最大フィルタ数を 16 として送信します。UE が S1 モードで SMF に接続し、4G から 5G または 5G から 4G へのハンドオーバーが進行中の場合、SMF はデフォルト値（16 個のパケット フィルタ）を送信します。

パケットフィルタの値に変更がある場合、SMF は、NUM_OF_PACKET_FILTER トリガーとともに PolicyUpdate メッセージを介して新しい値を PCF に送信します。

SMF は numOfPackFilter IE に基づいて、PDU セッションごとに許可される最大フィルタ数を制御します。パケット フィルタの数が UE で許可されている最大数を超えると、SMF はパケット フィルタに上限を設定します。これは、制限を超えたときに SMF が PCC ルールをドロップし、INCOR_FLOW_INFO 障害コードを含むルール レポートを送信することを意味します。

**Note** 現在、3GPP 仕様には、INCOR_FLOW_INFO の適切な障害コードが含まれていません。3GPP 仕様で利用可能になると、障害コードはそれに応じて更新されます。

サポートされている最大フィルタ数は、ダイナミック ルールに対してのみ有効であり、スタティック ルールや事前定義済みのルールでは有効ではありません。

「pcc_rule_report_max_supported_filter」統計情報が policy_pcc_rule_report カテゴリに導入されました。この統計情報は、サポートされているフィルタの最大数に達したときに PCC ルール レポートが生成された場合に増分されます。

### SmContextCreate での PCF ID のサポート

AMF は、Nsmf_PDUSession_CreateSMContext 要求に PCF ID を含めます。PCF ID は、非ローミングのケースではホームポリシー制御機能（H-PCF）、ローカル ブレークアウト ローミングの場合は訪問先ポリシー制御機能（V-PCF）を識別します。AMF が PCF ID を SMF に転送するタイミングの詳細については、3GPP 仕様 23.501、セクション 6.3.7.1 を参照してください。

SMF が PCF ID を受け取ったら、PCF ネットワーク プロファイルで次の CLI 構成を使用し、PCF ID を使用して SMF の動作を制御します。

**UseAmfProvidedPCF [True/False]**

デフォルトの動作では、SmContextCreate で AMF によって提供される PCF ID が使用されます。

AMF によって提供された PCF ID に到達できない場合、SMF は構成された障害処理テンプレートに従って動作します。この場合、静的構成を使用します。

### SmContextCreate での DNN 選択モードのサポート

SMF は DNN 選択モードを使用して、UE 要求を受け入れるか拒否するかを決定します。

SMF は、DNN 選択モードを使用して、セッション管理サブスクリプション データを取得するかどうかを判断します。HPLMN の DNN、S-NSSAI が明示的に登録されていない場合、SMF はセッション管理サブスクリプション データではなくローカル構成を使用します。

**Note** 前述のユース ケースはサポートされていません。

SMF は SmContextCreate データ内の IE を検証します。DnnSelectionMode と構成されている CLI との間の不一致が原因で DnnSelectionMode が失敗した場合、SMF は登録を続行しません。DnnSelectionMode 障害が発生すると、「disc_pdusetup_sm_cxt_unsupported_ie」が切断理由の一部として増加します。

| **DnnSelectionMode タイプ** | **説明** |
|---|---|
| 存在しない | SMF は、サブスクリプション要求を送信してサブスクリプション データを取得します。 |
| 確認済み | SMF は、サブスクリプション要求を送信してサブスクリプション データを取得します。 |
| UE_DNN_NOT_VERIFIED | **dnn-selection-mode verified ue-provided** CLI コマンドが次の構成に示すように構成されている場合、SMF はサブスクリプション要求を送信してサブスクリプション データを取得します。それ以外の場合、SMF は、「Invalid DNN selection Mode」の原因でコンテキスト要求を拒否します。 |
| NW_DNN_NOT_VERIFIED | **dnn-selection-mode verified network-provided**CLI が構成されている場合、SMF は、サブスクリプション要求を送信してサブスクリプション データを取得します。それ以外の場合、SMF は、「Invalid DNN selection Mode」の原因でコンテキスト要求を拒否します。 |

SMF は次の構成例を使用して DnnSelectionMode を構成します。

```
config
  profile smf profile_name
    dnn-selection-mode [ verified ue-provided | network-provided ]
    end
```

1 つ以上の DnnSelectionMode タイプを構成できます。デフォルトでは、DnnSelectionMode が確認されます。

サブスクリプション要求後、サブスクリプション データが UDM から取得されない場合、SMF はサブスクリプション データのローカル DNN プロファイルにフォールバックします。サブスクリプション データが UDM から取得されず、ローカル構成が存在しない場合、SMF は SmContextCreateError をサブスクリプションの失敗とともに送信します。

# 機能の仕組み

## コール フロー

このセクションでは、EPS と 5GC のインターワーキングをサポートするための 5G セッション管理の手順について説明します。

### PDU セッション作成のコール フロー

このセクションでは、*3GPP TS 23.502*（セクション *4.3.2.2.1*）で指定されている PDU セッションの変更手順について説明します。

***Figure 61: PDU* セッション作成のコール フロー**

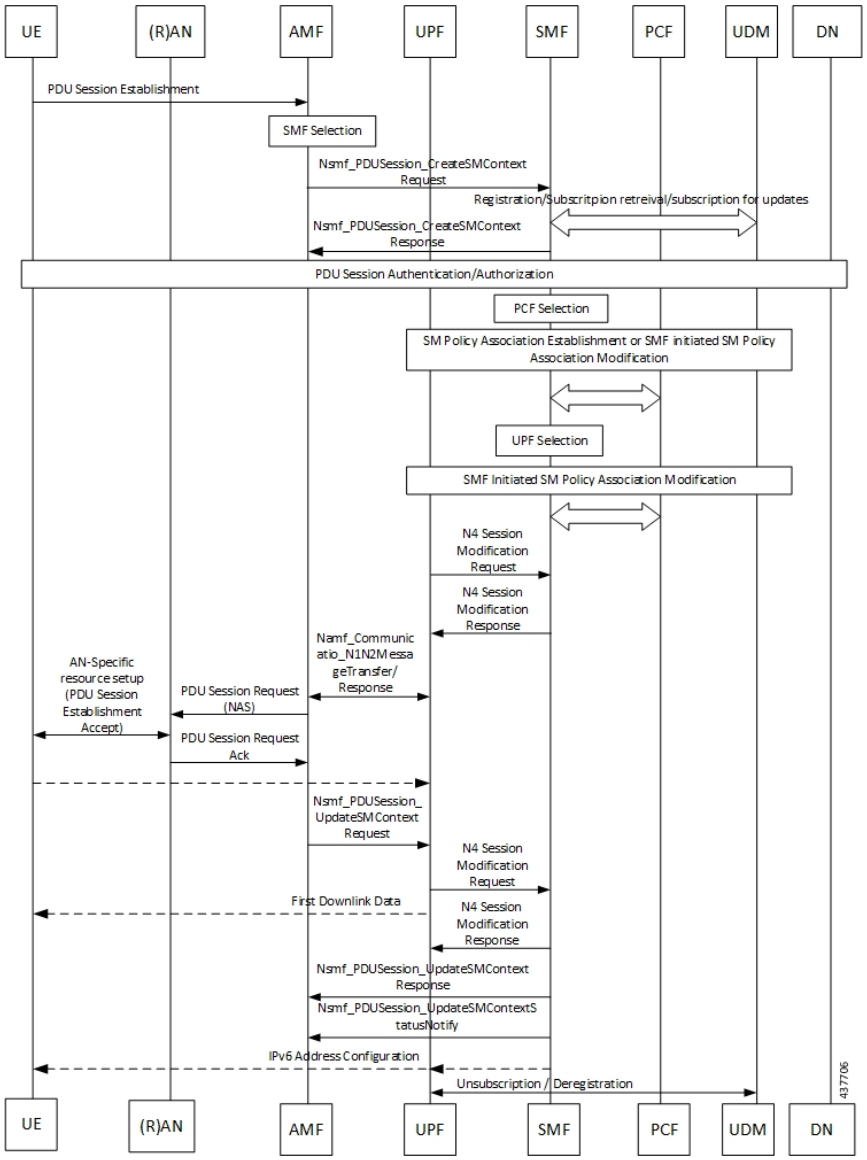


*Table 70: PDU* セッション作成コール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | UE は、N1 SM コンテナ内で PDU セッション確立要求を含む NAS メッセージを送信することにより、UE 要求 PDU セッション確立手順を開始する。PDU セッション確立要求には、PDU セッション ID、要求された PDU セッション タイプ、要求された SSC モード、5GSM 機能 PCO、SM PDU DN 要求コンテナ、パケット フィルタ数、および任意で要求された常時接続 PDU セッションが含まれます。 |
| 2 | AMF は、3GPP 仕様で説明されているように SMF の選択を実行します。 |
| 3 | AMF では、SMF に送信された Nsmf_PDUSession_CreateSMContext Request メッセージに EPS インターワーキングの表示が含まれています。このパラメータは、UE が 4G から 5G へのハンドオーバー（およびその逆）を実行できるかどうか、および AMF と MME 間の N26 インターフェイスの有無にかかわらず、これが許可されるかどうかを示します。 |
| 4 | AMF から受信した EPS インターワーキング指示が、UE が EPS インターワーキングをサポートしていることを示し、SMF が（たとえば、UE サブスクリプション データに基づいてこの DNN および S-NSSAI に対して EPS インターワーキングが許可されているかどうか）を PDU セッションが EPS インターワーキングをサポートしていると判断した場合、 S5/S8 インターフェイスの PGW-C+SMF FQDN が Nudm_UECM_Registration Request メッセージに含まれています。 |
| 5 | SMF は、ステップ 3 で受信した要求に応じて、Nsmf_PDUSession_CreateSMContext 応答（原因、SM コンテキスト ID or N1 SM コンテナ（PDU セッション拒否（原因））） または Nsmf_PDUSession_UpdateSMContext 応答のいずれかを送信します。<br><br>SMF がステップ 3 の Nsmf_PDUSession_CreateSMContext 要求を受信し、SMF が PDU セッション確立要求を処理できる場合、SMF は SM コンテキストを作成し、SM コンテキスト識別子を提供して AMF に応答します。 |
| 6 | （オプション）ステップ 3 の要求タイプが「既存の PDU セッション」を示している場合、SMF はセカンダリの認可と認証を実行しません。<br><br>ステップ 3 で受信した要求タイプが「緊急要求」または「既存の緊急 PDU セッション」の場合、SMF はセカンダリ許可および認証を実行しません。<br><br>*3GPP TS 23.501*、セクション *5.6.6*に記載されているように、DN-AAA サーバによる PDU セッションの確立中に SMF がセカンダリ許可および認証を実行する必要がある場合、SMF は *3GPP TS 23.501*、セクション *4.3.2.3*に記載されているように PDU セッション確立認証および許可をトリガします。 |

| ステップ | 説明 |
|---|---|
| 7a | ダイナミック PCC が PDU セッションに使用される場合、SMF は *3GPP TS 23.501*、セクション *6.3.7.1*に記載されているように PCF の選択を実行します。要求タイプが「既存の PDU セッション」または「既存の緊急 PDU セッション」を示している場合、SMF は PDU セッションに対してすでに選択されている PCF を使用します。そうしない場合、SMF はローカル ポリシーを適用する場合があります。 |
| 7b | SMF は、本書の「5G PDU セッション パラメータからの EPS PDN 接続パラメータの生成」の項で説明されているように、PCC ルールおよび 5G QoS パラメータから 4G TFT および 4G QoS へのマッピングを実行します。SMF + PGW-C は、QoS フローに基づいて、EPS にハンドオフするときにセッションに必要な専用ベアラーの数と、デフォルトのベアラーで必要なフロー（すべての GBR 以外のフロー）も決定します。SMF + PGW-C は、5G フローから 4G ベアラーへのマッピングを保存します。 |
| 8 | ステップ 3 の要求タイプが「初期要求」を示している場合、SMF は、*3GPP TS 23.501*、セクション *5.6.9.3*に記載されているように、PDU セッションの SSC モードを選択します。また、SMF は *3GPP TS 23.501*、セクション *6.3.3*で説明されているように、必要に応じて 1 つ以上の UPF も選択します。 |
| 9 | SMF は、*3GPP TS 23.502*、セクション *4.16.5.1* で定義されている SMF によって開始される SM ポリシー関連付けの変更手順を実行し、満たされたポリシー制御要求のトリガ条件に関する情報を提供します。要求タイプが「初期要求」であり、ダイナミック PCC が導入され、PDU セッション タイプが IPv4 または IPv6 または IPv4v6 の場合、SMF は割り当てられた UE IP アドレス/プレフィックスを PCF に通知します（ポリシー制御要求トリガ条件が満たされている場合）。<br><br>SMF + PGW-C は、*3GPP TS 23.502*、セクション *4.11.1.4*で定義されている EBI 割り当て手順を開始します。 |
| 10 | 要求タイプが「初期要求」を示している場合、SMF は、選択された UPF を使用して N4 セッション確立手順を開始します。それ以外の場合は、選択した UPF で N4 セッション変更手順を開始します。<br><br>PDU セッションに対して複数の UPF が選択されている場合、SMF はこの手順の PDU セッションの各 UPF で N4 セッション確立/変更手順を開始します。 |
| 11 | 非ローミングまたは LBO シナリオでは、PGW-C+SMF には、マッピングされた EPS ベアラー コンテキストと、N1 SM コンテナ内の UE に送信される対応する QoS フローが含まれます。PGW-C+SMF は、QoS フローと N1 SM コンテナ内のマッピングされた EPS ベアラー コンテキスト間のマッピングも示します。PGW-C+SMF には、NG-RAN に送信する N2 SM 情報に、受信した EBI と QFI の間のマッピングも含まれています。<br><br>PGW-C+SMF は、Namef_Communication_N1N2MessageTransfer メッセージを介して、N1 SM コンテナと N2 SM の情報を AMF に送信します。 |

| ステップ | 説明 |
|---|---|
| 12 | AMF は、N2 PDU セッション要求（N2 SM 情報、NAS メッセージ（PDU セッション ID、N1 SM コンテナ（PDU セッション確立承認））を (R)AN に送信します。<br>AMF は、UE を対象とした PDU セッション ID と PDU セッション確立承認を含む NAS メッセージと、N2 PDU セッション要求内で SMF から受信した N2 SM 情報を含む NAS メッセージを (R)AN に送信します。 |
| 13 | (R)AN は、SMF から受信した情報に関連する UE との AN 固有のシグナリング交換を発行する場合があります。たとえば NG-RAN の場合、ステップ 12 で受信した PDU セッション要求の QoS ルールに関連する必要な NG-RAN リソースを確立する UE で、RRC 接続再構成が行われる可能性があります。 |
| 14 | (R)AN は N2 PDU セッション応答（PDU セッション ID、原因、N2 SM 情報（PDU セッション ID、AN トンネル情報、承認/拒否された QFI のリスト、ユーザー プレーン適用ポリシー通知））を AMF に発行します。 |
| 15 | AMF は、Nsmf_PDUSession_UpdateSMContext 要求（N2 SM 情報、要求タイプ）を SMF に送信します。<br>AMF は、(R)AN から受信した N2 SM 情報を SMF に転送します。 |
| 16a | SMF は UPF に対して N4 セッション変更手続きを開始します。SMF は、(R)AN トンネル情報と対応する転送ルールを UPF に提供します。 |
| 16b | UPF は、SMF に N4 セッション変更応答を提供します。<br>PDU セッションで複数の UPF が使用されている場合、ステップ 16a の UPF は N3 を終端する UPF を参照します。<br>このステップの後、UPF はこの PDU セッション用にバッファされている可能性のあるダウンリンク パケットを UE に配信します。 |
| 17 | SMF は Nsmf_PDUSession_UpdateSMContext Response（原因）を AMF に送信します。 |
| 18 | （条件付き）SMF は Nsmf_PDUSession_SMContextStatusNotify（Release）を AMF に送信します。<br>手順中に、ステップ 5 以降の任意の時点で PDU セッションの確立が成功しなかった場合、SMF は Nsmf_PDUSession_SMContextStatusNotify（リリース）を呼び出して AMF に通知します。SMF は、作成されたすべての N4 セッション、割り当てられている場合は PDU セッション アドレス（IP アドレスなど）を解放し、PCF との関連付けを解放します（存在する場合）。 |
| 19 | PDU セッション タイプが IPv6 または IPv4v6 の場合、SMF は IPv6 ルータ アドバタイズメントを生成し、N4 および UPF 経由で UE に送信します。 |

| ステップ | 説明 |
|---|---|
| 20 | ステップ 4 の後に PDU セッション確立が失敗した場合、SMF は次を実行します。<br>• SMF が UE のセッション（DNN、S-NSSAI）の PDU をこれ以上処理していない場合、SMF は Nudm_SDM_Unsubscribe（SUPI、セッション管理サブスクリプションデータ、DNN、S-NSSAI）を使用して、対応する（SUPI、DNN、S-NSSAI）のセッション管理サブスクリプションデータの変更をサブスクライブ解除します。。UDM は、Nudr_DM_Unsubscribe（SUPI、サブスクリプションデータ、セッション管理サブスクリプション データ、S-NSSAI、DNN）により、UDR からの変更通知をサブスクライブ解除できます。<br>• SMF は、Nudm_UECM_Deregistration（SUPI、DNN、PDU セッション ID）を使用して、指定された PDU セッションの登録を解除します。UDM は、Nudr_DM_Update（SUPI、サブスクリプション データ、SMF データの UE コンテキスト）によって、対応する UE コンテキストを更新できます。 |

## PDU セッション変更コール フロー

このセクションでは 、*3GPP TS 23.502*（セクション *4.3.3.2*）で規定されている PDU セッションの変更手順について説明します。

図 *62 : PDU* セッション変更コール フロー

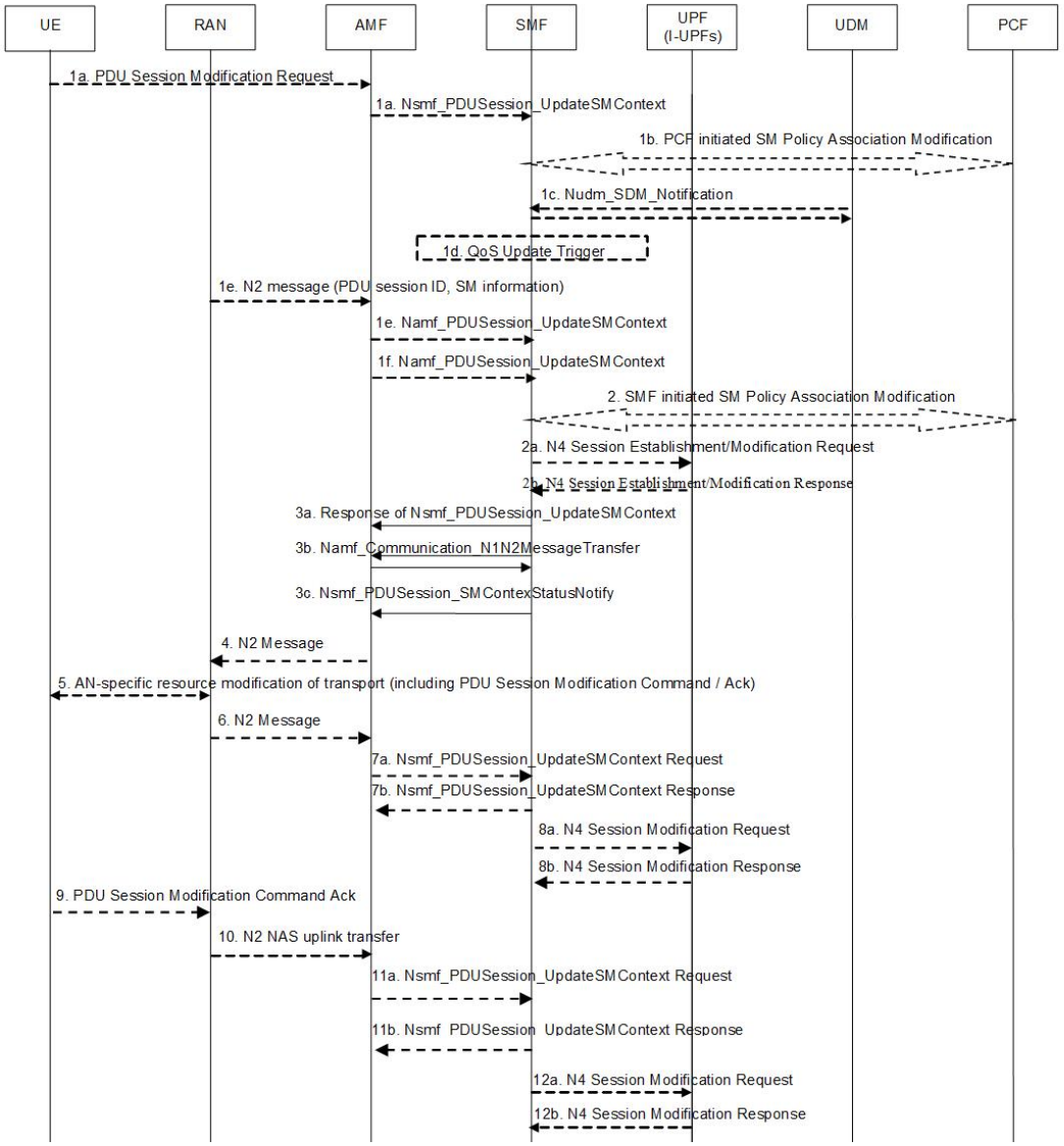



表 *71 : PDU* セッション変更のコール フローの説明

| ステップ | 説明 |
|---|---|
| 1a | UE は、N1 SM コンテナ内の PDU セッション変更要求を含む NAS メッセージを送信することで、UE 要求済み PDU セッション変更手順を開始します。PDU セッション変更要求には、PDU セッション ID、パケットフィルタ、動作、要求された QoS、分離、および 5GSM コアネットワーク機能が含まれます。 |

| ステップ | 説明 |
|---|---|
| 1b | （SMF 要求による変更）PCF は、PCF によって開始された SM ポリシー関連付け変更手順を実行して、ポリシーの変更について SMF に通知します。ポリシーの決定または AF 要求（アプリケーション機能がトラフィック ルーティングに影響を与える場合など）は、この手順をトリガーします。 |
| 1c | （SMF 要求された変更）UDM は、Nudm_SDM_Notification（SUPI、セッション管理サブスクリプション データ）によって SMF のサブスクリプションデータを更新します。SMF は、セッション管理サブスクリプション データを更新し、（SUPI）で Ack を返すことによって UDM を確認します。 |
| 1d | （SMF 要求された変更）SMF は PDU セッションの変更を決定します。この手順は、ローカルに構成されたポリシーに基づいてトリガーされることも、（R）AN からトリガーされることもあります。<br><br>SMF は、ステップ 1b ～ 1d のいずれかのトリガーを受信すると、SMF 要求された PDU セッション変更手順を開始します。 |
| 1e | （AN 開始の変更）（R）AN は、通知制御が設定されているかどうかに関係なく、QoS フローがマッピングされる AN リソースが解放されたときに SMF に示します。<br><br>（R）AN は、N2 メッセージ（PDUセッション ID、N2 SM 情報）を AMF に送信します。smf_PDU_Session_UpdateContext の N2 SM 情報には、次の情報が含まれます。<br><br>• QoS フロー識別子（QFI）<br><br>• ユーザー ロケーション情報<br><br>• QoS フロー リリースリスト IE - NG-RAN ノードによってリリースされる QoS フローのリスト<br><br>• QoS フロー通知リスト IE および通知原因 IE：特定の基準を満たした GBR QoS フローと、基準を満たさなかったフローのリスト<br><br>SMF は、RAN から QFI を解放するために AN によって開始された変更をサポートしています。このサポートの詳細については、次のセクションを参照してください。 |
| 2 | SMF は、SMF によって開始された SM ポリシー関連付けの変更手順を実行することにより、サブスクライブされたイベントを PCF に報告します。ステップ 1b または 1d によって PDU セッション変更手順がトリガーされた場合、SMF はこのステップをスキップします。ダイナミック PCC が展開されていない場合、SMF はローカル ポリシーを適用して、QoS プロファイルを変更するかどうかを判断できます。PDU セッション変更で UPF でのアクションのみ（ゲートウェイなど）が必要な場合、SMF はステップ 3 ～ 7 を呼び出しません。 |

| ステップ | 説明 |
|---|---|
| 3a | UE または AN が開始した変更の場合、SMF は、N2 SM 情報と N1 SM コンテナを含む Nsmf_PDUSession_UpdateSMContext を介して AMF に応答します。<br><br>N2 SM 情報は、AMF が (R) AN に提供する情報を伝送します。1 つまたは複数の QoS フローが追加または変更されたことを（R）AN に通知する QoS プロファイルおよび対応する QFI が含まれます。1 つ以上の QoS フローが削除されたことを（R）AN に通知するための QFI のみが含まれています。<br><br>N1 SM コンテナは、AMF が UE に提供する PDU セッション変更コマンドを伝送します。これには QoS ルール、QoS ルールの動作、QoS フローレベルの QoS パラメータ（QoS ルールに関連付けられた QoS フローに必要な場合）、およびセッション AMBR が含まれます。 |
| 3b | SMF 要求による変更の場合、SMF は、N2 SM 情報と N1 SM コンテナを含む Namef_Communication_N1N2MessageTransfer を呼び出します。<br><br>UE が CM-IDLE 状態で、非同期タイプの通信（ATC）がアクティブになっている場合、AMF は Namef_Communication_N1N2MessageTransfer に基づいて UE コンテキストを更新して保存し、ステップ 4、5、6、7 をスキップします。UE が到達可能な場合、つまり UE が CM-CONNECTED 状態になると、AMF は N1 メッセージを転送して UE コンテキストを UE と同期します。 |
| 4 | AMF は、N2 PDU セッション要求（SMF から受信した N2 SM 情報、NAS メッセージ（PDU セッション ID、N1 SM コンテナ（PDU セッション変更コマンド））） メッセージを（R）AN に送信します。 |
| 5 | （R）AN は、SMF から受信した情報に関連する UE との AN 固有のシグナリング交換を発行します。たとえば、 NG-RAN 内で RRC 接続再構成は、UE が PDU セッションに関連した必要な（R）AN 技術情報の変更をして行われます。 |
| 6 | （R）AN は、AMF に N2 PDU セッション確認メッセージを送信して、N2 PDU セッション要求を確認します。 |
| 7 | AMF は、Nsmf_PDUSession_UpdateSMContext サービス操作を介して AN から SMF に N2 SM 情報とユーザーロケーション情報を転送します。SMF は Nsmf_PDUSession_UpdateSMContext 応答を送信します。<br><br>（R）AN が QFI を拒否した場合、SMF は QoS ルールおよび QoS フローレベルの QoS パラメータを、必要に応じて UE の QoS ルールに関連付けられた QoS フローに応じて更新します。 |
| 8 | SMF は、N4 セッション変更要求メッセージを UPF に送信することにより、PDU セッション変更に関わっている UPF の N4 セッションを更新します。 |
| 9 | UE は NAS メッセージ（PDU セッション ID、N1 SM コンテナ（PDU セッション変更コマンド Ack））を送信して PDU セッション変更コマンドを確認します。 |

| ステップ | 説明 |
|---|---|
| 10 | （R）AN は、NAS メッセージを AMF に転送します。 |
| 11 | AMF は、Nsmf_PDUSession_UpdateSMContext サービス操作を通じて、N1 SM コンテナ（PDUセッション変更コマンドAck）とユーザーロケーション情報をANからSMFに転送します。SMF は Nsmf_PDUSession_UpdateSMContext 応答を送信します。 |
| 12 | SMF は、N4 セッション変更要求（N4 セッション ID）メッセージを UPF に送信することにより、PDU セッション変更に関わっている UPF の N4 セッションを更新します。<br>イーサネット PDU セッション タイプの PDU セッションの場合、SMF は UPF にイーサネット パケット フィルタ セットと転送ルールの追加または削除を通知します。 |
| 13 | ステップ 1b または、2 内で SMF が PCF と相互作用した場合、SMF は、SMF によって開始される SM ポリシー関連付けの変更手順を実行することによって、PCC の決定を適用されるかどうかを PCF に通知します。<br>SMF は、PDU セッションの変更に関連するユーザーの場所情報を登録しているすべてのエンティティに通知します。<br>ステップ 1b がトリガーされてトラフィック ルーティングのアプリケーション機能が実行されると、SMF は PDU セッションのユーザー プレーンを再構成します。 |

### AN によって開始された変更手順中の QFI のリリース

SMF が QFI を解放するために AN が開始した変更をサポートするには、次の手順を実行します：

1. 特定の PDU セッションで EPS インターワーキング インジケータが有効になっている場合、SMF は AMF に対して EBI リリースを開始します。
2. SMF は UPF に N4 変更を送信し、解放されるフローに関連するパケット検出ルール（PDR）、QoS 適用ルール（QER）、および使用状況レポート ルール（URR）を削除します。
3. SMF は、N1 PDU Session Modification コマンドを含む N1N2TransferMessage を開始します。このメッセージには、削除されたフロー、マップされた EPS ベアラーコンテキストに関する情報が含まれています。
4. 次に、SMF は PCF と対話して、「RES_RELEASE」トリガーが設定されている場合、ルールに対してリリースされたフローを報告します。

（注） 「policy_pdu_flows_total」統計を使用して、リリースされたフローを確認できます。

### PDU セッション変更時の EPS インターワーキングの表示

[EpsInternetworkingIndication] フィールドには、EPS と 5GC の間のハンドオーバーの可能性が表示されます。このフィールドは、次の値を保持します：

- [なし（NONE）]：PDU セッションを EPS に移動できません。
- WITH_N26：PDU セッションが EPS に移動され、EPS インターワーキング手順中に N26 インターフェイスがサポートされます。
- WITHOUT_N26：EPS インターワーキング手順中にサポートされる N26 インターフェイスなしで、PDU セッションが EPS に移動されます。

SMF では、EpsInternetworkingIndication 値が WITH_N26 に設定されている場合にのみ、4G から 5G へのハンドオーバーが許可され、その逆も許可されます。EpsInternetworkingIndication の他の値の場合、SMF はハンドオーバーを拒否します。

4Gおよび5G PDUセッションの確立中に、AMFからEPSインターネットワーキング指示を受信すると、SMFはS5/S8インターフェイス用のPGW-C＋SMF FQDNをUDM登録要求に含めます。

**EPS インターワーキング通知のサポートが有効になっている場合**：

作成された PDU セッションの EpsInternetworkingIndication 値が NONE または WITHOUT_N26 から WITH_N26 に変更された場合は、次の手順に従って、PDU の変更手順で EPS インターワーキング表示の変更をサポートします。

1. AMF は、変更された EpsInterworkingIndication 値を使用して Nsmf_PDUSession_UpdateSMContext 要求を呼び出します。
2. SMF は AMF から Nsmf_PDUSession_UpdateSMContext 要求を受信し、Namf_Communication_EbiAssignmentRequest を開始します。この要求には、PDU セッション ID と割り当て/保持優先順位（ARP）リストが含まれています。
3. AMF は、Namef_Communication_EbiAssignmentResponse を SMF に送信します。AMFは、応答を通じて以下を送信します。
   - 正常に割り当てられた EBI を含む assignedEbiList。
   - EBI 割り当てが失敗した失敗した ARP を含む failedArpList。
   - 4XX/5XX エラーと、EBI 割り当ての失敗を表す AssignEbiError。
4. SMF は、EBI が正常に作成されると、N1N2MessageTransfer 要求メッセージを送信します。この要求には次の内容が含まれます：
   - N1:PDU SESSION MODIFICATION COMMAND ([Mapped EPS Bearer Contexts,Create])
   - N2:N2_PDU_SESSION_RESOURCE_MODIFY_REQUEST_TRANSFER（QoS フローでは EPS 無線アクセス ベアラー（E-RAB）ID と QoS フロー ID を持つ要求項目の追加または変更）

（注） UE がアイドルモードの場合、SMF は N2 メッセージの送信をスキップします。

5. SMF は N1 メッセージを使用して、UE のマップされた EPS ベアラー コンテキストを通知します。SMF は N1：PDU セッション変更完了メッセージを待機します。
6. SMF は N2 メッセージを使用して、EBI to QoS フロー識別子（QFI）の gNodeB へのマッピングを通知します。SMF は N2: PDU SESSION RESOURCE MODIFY RESPONSE TRANSFER メッセージを待機します。
7. SMF で PDU セッション変更手順を実行します。

**EPS インターワーキング表示のサポートが無効の場合**：

作成された PDU セッションの EpsInternetworkingIndication 値が WITH_N26 から NONE または WITHOUT_N26 に変更された場合は、次の手順に従って、PDU の変更手順で EPS インターワーキング表示の変更をサポートします。

1. SMF は、AMF から、変更された EpsInterworkingIndication 値を持つ Nsmf_PDUSession_UpdateSMContext 要求を受信します。
2. SMF が N1N2MessageTransfer 要求メッセージを送信します。この要求には次の内容が含まれます。
   - N1:PDU SESSION MODIFICATION COMMAND ([Mapped EPS Bearer Contexts,Delete])
   - N2:N2_PDU_SESSION_RESOURCE_MODIFY_REQUEST_TRANSFER

（注） UE がアイドルモードの場合、SMF は N2 メッセージの送信をスキップします。

3. SMF は N1 メッセージを使用して、UE でマッピングされた EPS ベアラー コンテキストを削除します。SMF は N1：PDU セッション変更完了メッセージを待機します。
4. SMF は N2 メッセージを使用して、gNodeB への EBI から QFI へのマッピングを削除します。SMF は N2: PDU SESSION RESOURCE MODIFY RESPONSE TRANSFER メッセージを待機します。
5. SMF で PDU セッション変更手順を実行します。

**show subscriber** コマンドを使用して、PDU セッションの EPS インターワーキング ステータスと QoS フローの EBI マッピングを確認します。

## PDU セッションの解放コール フロー

PDU セッションのリリース手順は、次を含む、PDU セッションに関連付けられているすべてのリソースを解放するために使用されます。

- IP ベースの PDU セッションに割り当てられた IP アドレス/プレフィックス

- PDU セッションで使用された任意の UPF リソース。
- PDU セッションで使用されたアクセス リソース。

SMF は、PDU セッションに関連付けられているエンティティ（PCF、データ ネットワーク（DN）（たとえば、PDU セッションの確立時に DN の承認が行われた場合）など）に通知します。

PDU セッションの解放を開始する方法は複数あります。UE、ネットワーク、AMF、または RAN から取得できます。

## *UE* が開始した *PDU* セッションのリリース コール フロー

UE が開始した PDU セッションの解放手順により、UE は PDU セッションの解放を要求できます。ローカル ブレークアウト（LBO）の場合、手順は非ローミングの場合と同じですが、AMF、SMF、UPF、および PCF がアクセスしたネットワークにあるという違いがあります。

次の図は、*3GPP TS 23.502*、セクション *4.3.4.2*に指定されている SMF での EPS インターワーキングをサポートするための、UE によって開始される PDU セッションの解放手順を示しています。

**図 *63 : UE* が開始した *PDU* セッションのリリース コール フロー**

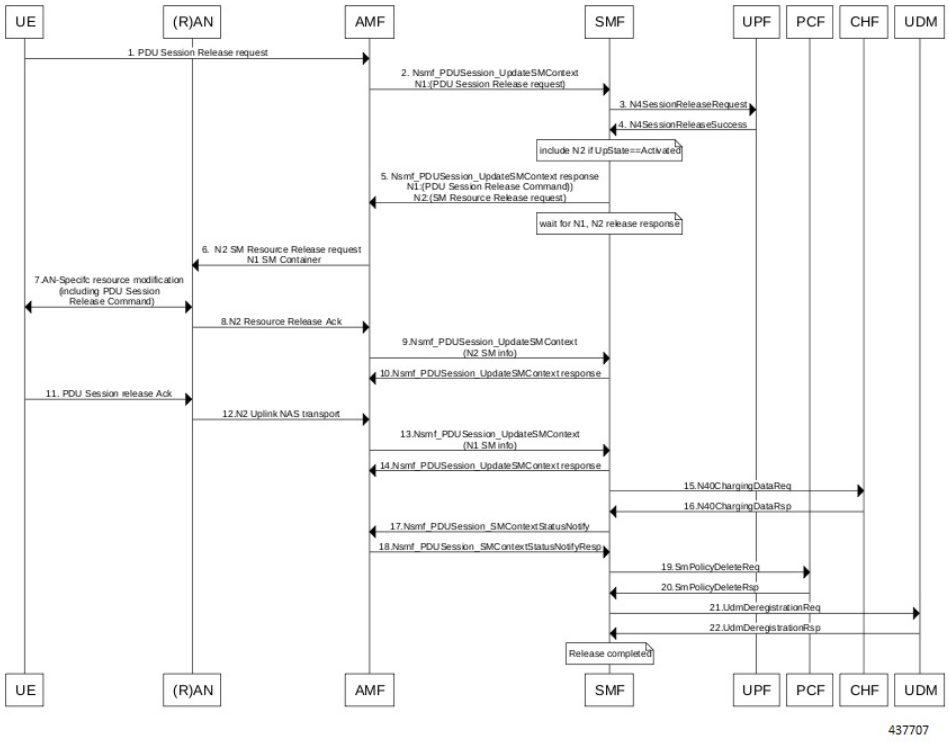


表 *72 : UE* が開始した *PDU* セッションの作成コール フローの説明

| ステップ | 説明 |
|---|---|
| 1、2 | UEは、NAS メッセージの PDU_SESSION_RELEASE_REQUEST を RAN 経由で AMF に送信します。AMF は、SmContextUpdateRequest で SMF にメッセージを送信します。 |
| 3、4 | SMF は N4SessionReleaseRequest を UPF に送信します。UPF は同じ応答を送信します。 |
| 5 | SMF は、N1 および N2 コンテンツを含む SmContextUpdateResponse メッセージを送信します。<br>• N1：PDU_SESSION_RELEASE_COMMAND<br>• N2：N2_PDU_SESSION_RESOURCE_RELEASE_COMMAND。 SMF が IDLE モードの場合は、 を除外します。また、ステップ 8、9、10 は省略します。 |
| 6、7 | AMF は RAN とメッセージを交換します。RAN はそれを UE に転送します。 |
| 8、9、10 | RAN は、N2 リリース応答を AMF に送信します。AMF は、N11 SmContextUpdateRequest メッセージで N2 リリース応答（N2_PDU_SESSION_RESOURCE_RELEASE_RESPONSE_TRANSFER）を送信します。SMF は SmContextUpdateResponse として AMF に応答します。 |
| 11, 12, 13, 14 | UEは、N1リリース応答をNASメッセージでRANを介してAMFに送信します。AMF は、N11 SmContextUpdateRequest メッセージで N1 リリース応答（PDU_SESSION_RELEASE_COMPLETE）を送信します。SMF は SmContextUpdateResponse として AMF に応答します。 |
| 15、16 | SMF は削除課金要求を CHF に送信します。CHF は SMF に削除応答を返します。 |
| 17、18 | SMF は SmContextStatusNotify を AMF に送信します。AMF は SmContextStatusNotifyResponse メッセージで応答を返します。 |
| 19、20 | SMF から PCF に削除要求が送信されます。PCF は SMF に削除応答を返します。 |
| 21、22 | SMF が UDM の登録解除要求を送信します。UDM は、登録解除応答で SMF に応答を返します。 |

## ネットワークが開始した *PDU* セッションのリリース コール フロー

ネットワーク開始型PDUセッションの解放手順により、AMF、SMF、またはPCFがPDUセッションの解放を開始できます。

次の図に、ネットワークによって開始された PDU セッションのリリース コールのフローを示します。

図 *64 :* ネットワークが開始した *PDU* セッションのリリース コール フロー

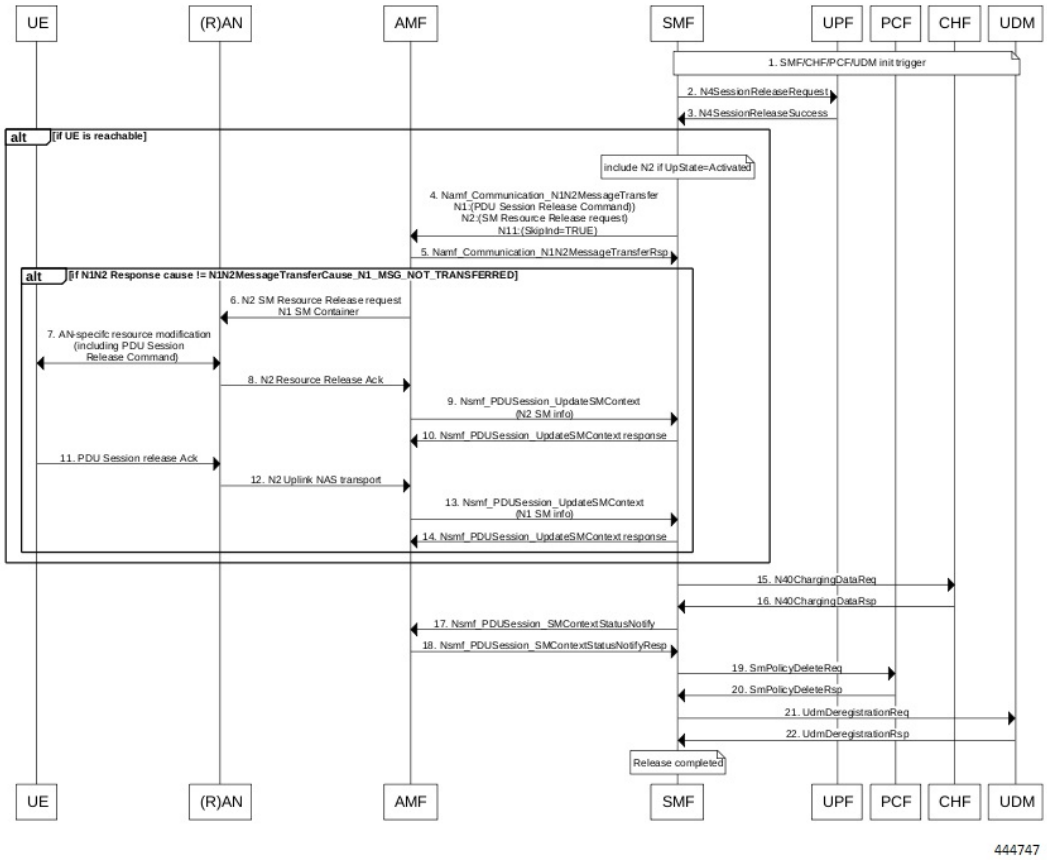



表 *73 :* ネットワークによって開始された *PDU* セッションの作成コール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | この手順は、PCF、CHF、UDM、UPF、またはCLI（サブスクライバのクリア）によってトリガされ、PDU セッションのリリースを開始できます。 |
| 2、3 | SMF は N4SessionReleaseRequest を UPF に送信します。UPF は同じ応答を送信します。<br>（注）<br>AMF が UE に到達不能であることを通知している場合は、ステップ 4 ～ 14 をスキップします。 |

| ステップ | 説明 |
|---|---|
| 4 | SMF は、N11、N1、および N2 コンテンツを含む N1N2MessageTransfer メッセージを送信します。<br>• N11：SkipInd=True<br>• N1：PDU_SESSION_RELEASE_COMMAND<br>• N2：N2_PDU_SESSION_RESOURCE_RELEASE_COMMAND。 SMF が IDLE モードの場合は、 を除外します。また、ステップ 8、9、10 は省略します。 |
| 5 | AMF は、N1N2MessageTransferRsp メッセージに原因を含めて SMF に応答します。<br>（注）<br>AMF がステップ 5 で原因をN1_MSG_NOT_TRANSFERREDとして送信した場合は、ステップ 6 ー 14 をスキップします。 |
| 6、7 | AMF は RAN とメッセージを交換します。RAN はそれを UE に転送します。 |
| 8、9、10 | RAN は、N2 リリース応答を AMF に送信します。AMF は、N11 SmContextUpdateRequest メッセージで N2 リリース応答（N2_PDU_SESSION_RESOURCE_RELEASE_RESPONSE_TRANSFER）を転送します。SMF は SmContextUpdateResponse として AMF に応答します。 |
| 11, 12, 13, 14 | UE は、NAS メッセージに含まれる N1 リリース応答を RAN を介して AMF に送信します。AMF は、N11 SmContextUpdateRequest メッセージで N1 リリース応答（PDU_SESSION_RELEASE_COMPLETE）を送信します。SMF は SmContextUpdateResponse として AMF に応答します。 |
| 15、16 | SMF は削除課金要求を CHF に送信します。CHF は SMF に削除応答を返します。 |
| 17、18 | SMF は SmContextStatusNotify を AMF に送信します。AMF は SmContextStatusNotifyResponse メッセージで応答を返します。 |
| 19、20 | SMF から PCF に削除要求が送信されます。PCF は SMF に削除応答を返します。 |
| 21、22 | SMF が UDM の登録解除要求を送信します。UDM は、登録解除応答で SMF に応答を返します。 |

### *AMF* によって開始された *PDU* セッションの解放

AMF が開始した PDU セッションの解放手順により、AMF は PDU セッションの解放を開始できます。

次の図は、AMF によって開始された PDU セッションのリリース コール フローを示しています。

図 *65 : UE* が開始した *PDU* セッションのリリース コール フロー

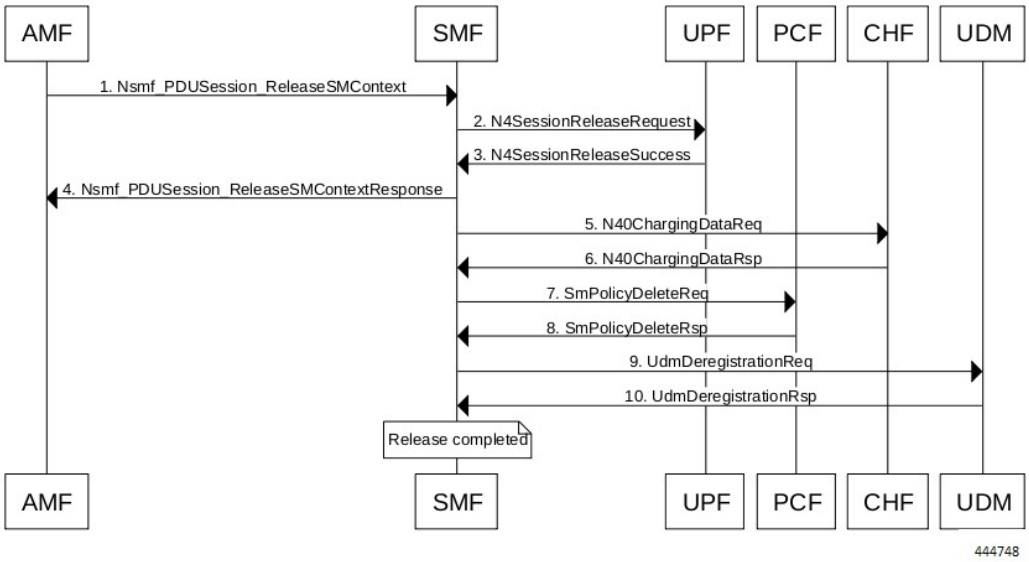



表 *74 : AMF* によって開始された *PDU* セッションの作成コール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | AMF は SmContextReleaseRequest を送信します。 |
| 2、3 | SMF は N4SessionReleaseRequest を UPF に送信します。UPF は同じ応答を送信します。 |
| 4 | SMF は、SmContextReleaseResponse を AMF に送信します。 |
| 5、6 | SMF は削除課金要求を CHF に送信します。CHF は SMF に削除応答を返します。 |
| 7、8 | SMF から PCF に削除要求が送信されます。PCF は SMF に削除応答を返します。 |
| 9、10 | SMF が UDM の登録解除要求を送信します。UDM は、登録解除応答で SMF に応答を返します。 |

## *N11 Release = True* での *AMF* によって開始された *PDU* セッションのリリース

**表 *75 :* 機能の履歴**

| 機能名 | リリース情報 | 説明 |
|---|---|---|
| 3GPP リリース 16 に準拠するための AMF によって開始される PDU セッションリリースの機能強化 | 2025.01.0 | AMF は、UE サブスクリプションの変更の通知を受信すると、PDU セッションを解放します。ただし、PDU セッション解放の原因は指定されていませんでした。この機能では、UE サブスクリプションの変更による PDU セッションの解放を示すために、新しい PDU セッションの解放原因 **REL_DUE_TO_SUBSCRIPTION_CHANGE** を導入することで、PDU セッションの解放プロセスが強化されています。 |

AMF が開始した PDU セッションのリリース手順により、AMF は、SmContextModifyRequest の N11 リリースが True に設定された PDU セッションのリリースを開始できます。

次の図は、N11 release=True での AMF によって開始された PDU セッションのリリース コールフローを示しています。

図 *66 : N11 Release = True* での *AMF* によって開始された *PDU* セッションのリリース

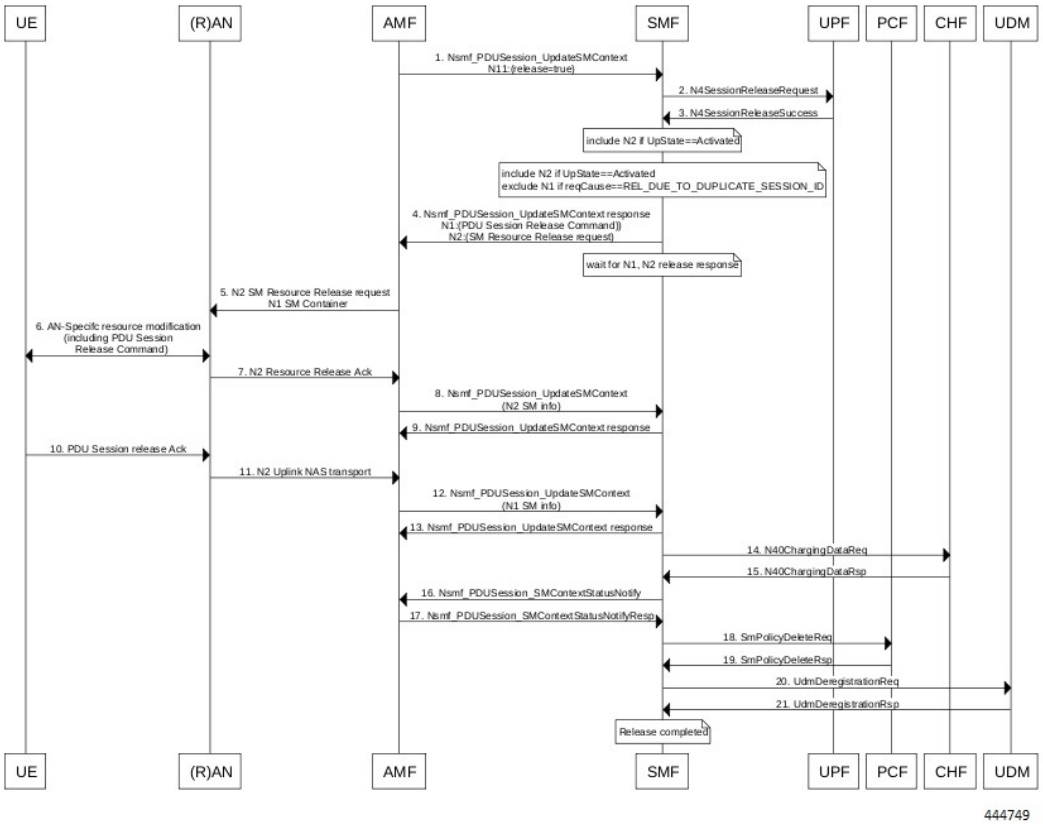



表 *76 : AMF* によって開始された *PDU* セッション作成コール フロー（*N11 release=true*）の説明

| ステップ | 説明 |
|---|---|
| 1 | AMF は、次の理由で SmContextModifyRequest を release=True で送信します。<br>• REL_DUE_TO_DUPLICATE_SESSION_ID：同一の PDU セッション ID を使用して新しい PDU セッションを確立する UE 要求によるリリース。<br>• REL_DUE_TO_SLICE_NOT_AVAILABLE：関連付けられた S-NSSAI が使用できなくなったことによるリリース。<br>• REL_DUE_TO_SUBSCRIPTION_CHANGE：UE サブスクリプションの変更（サブスクライブ対象の DNN の削除、または PDU セッションのリリースを引き起こす ODB の変更など）によるリリース。 |
| 2、3 | SMF は N4SessionReleaseRequest を UPF に送信します。UPF は同じ応答を送信します。 |

| ステップ | 説明 |
|---|---|
| 4 | SMF は、N1 および N2 コンテンツを含む SmContextUpdateResponse メッセージを送信します。<br>• N1：PDU_SESSION_RELEASE_COMMAND、原因が REL_DUE_TO_DUPLICATE_SESSION_ID の場合は除外し、ステップ 10、11、12、13 をスキップします。<br>• N2：N2_PDU_SESSION_RESOURCE_RELEASE_COMMAND。 SMF が IDLE モードの場合は、 を除外します。また、手順 7、8、9 は省略します。 |
| 5、6 | AMF は RAN とメッセージを交換します。RAN はそれを UE に転送します。 |
| 7、8、9 | RAN は、N2 リリース応答を AMF に送信します。AMF は、N11 SmContextUpdateRequest メッセージで N2 リリース応答（N2_PDU_SESSION_RESOURCE_RELEASE_RESPONSE_TRANSFER）を送信します。SMF は SmContextUpdateResponse として AMF に応答します。 |
| 10、11、12、13 | UEは、N1リリース応答をNASメッセージでRANを介してAMFに送信します。AMF は、N11 SmContextUpdateRequest メッセージで N1 リリース応答（PDU_SESSION_RELEASE_COMPLETE）を送信します。SMF は SmContextUpdateResponse として AMF に応答します。 |
| 14、15 | SMF は削除課金要求を CHF に送信します。CHF は SMF に削除応答を返します。 |
| 16、17 | SMF は SmContextStatusNotify を AMF に送信します。AMF は SmContextStatusNotifyResponse メッセージで応答を返します。 |
| 18、19 | SMF から PCF に削除要求が送信されます。PCF は SMF に削除応答を返します。 |
| 20、21 | SMF が UDM の登録解除要求を送信します。UDM は、登録解除応答で SMF に応答を返します。 |

## *RAN* が開始した *PDU* セッションのリリース コール フロー

RAN が開始した PDU セッションの解放手順により、RAN は PDU セッションの解放を開始できます。

次の図は、RAN によって開始された PDU セッションのリリース コール フローを示しています。

図 *67 : RAN* が開始した *PDU* セッションのリリース コール フロー

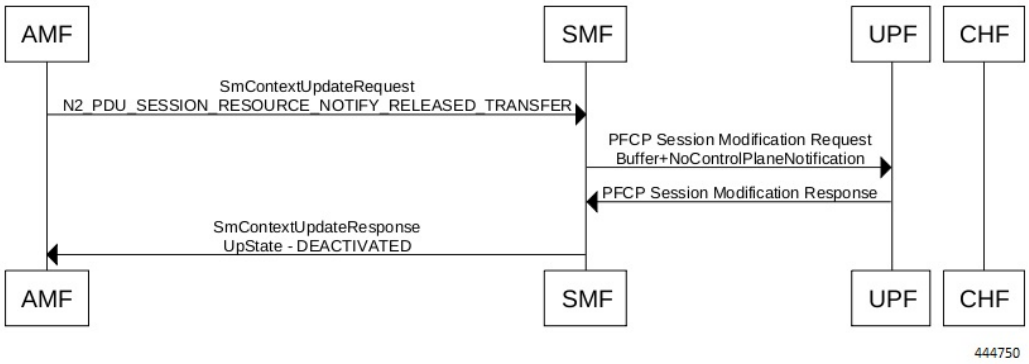


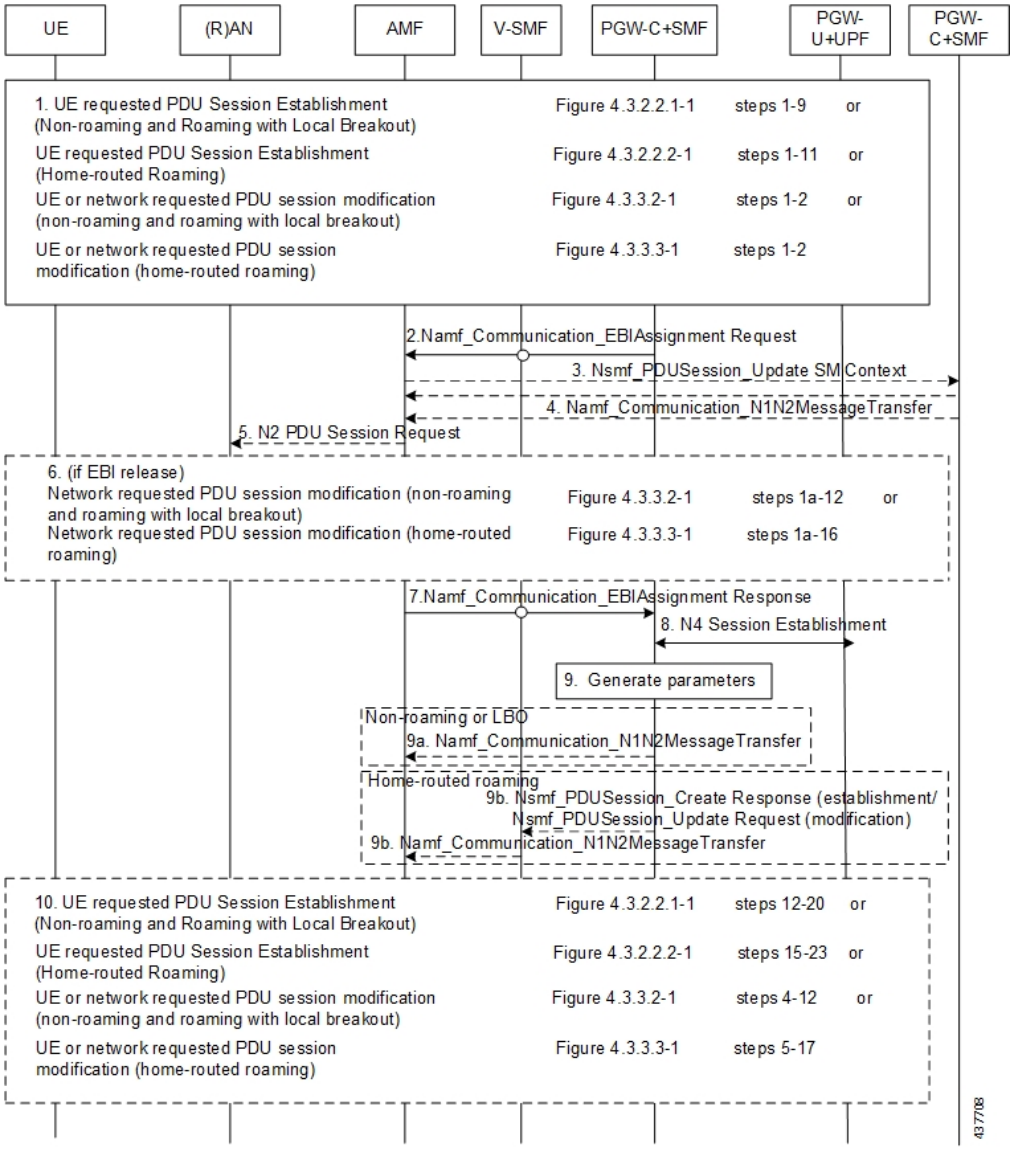

表 *77 : AMF* によって開始された *PDU* セッションの作成コール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | AMF は、N2 タイプ（N2_PDU_SESSION_RESOURCE_NOTIFY_RELEASED_TRANSFER）を使用して SmContextModifyRequest を送信します。 |
| 2、3 | SMF は、パケット ルールを [転送からバッファ（Buffer from Forward）] に変更して、N4SessionModificationRequest を UPF に送信します。UPF は同じ、つまり SMF が IDLE 状態に移行していることに対する応答を送信します。 |
| 4 | SMF は、UpState が Deactivated になっている SmContextUpdateResponse メッセージを送信します。 |

## EPS ベアラー ID の割り当て

ここでは、EPS ベアラー ID の割り当て手順について説明します。

*Figure 68: EPS* ベアラー *ID* の割り当てコール フロー




**Note** 前述のコールフローのすべてのステップがサポートされているわけではありません。詳細については、次の表の説明を参照してください。

*Table 78: EPS* ベアラ *ID* の割り当てコールフローの説明

| ステップ | 説明 |
|---|---|
| 1 | PGW-C + SMF（またはホームルーティングの場合は H-SMF）が、（オペレータポリシー、S-NSSAI、ユーザー プレーン セキュリティ適用情報に基づいて）PDU の QoS フローに EPS ベアラー ID を割り当てる必要があると判断した場合PGW-C+SMF は Namef_Communication_EBIAssignment Request（PDU セッション ID、ARP リスト）を呼び出します。 |
| ステップ 2 からステップ 5 は、同じ UE に対する EBI の新しい SMF 要求を処理するために、以前に UE に割り当てられていた EBI を AMF が取り消す必要がある場合にのみ適用されます。 | |
| 2 | （条件付き）AMF に使用可能な EBI がない場合、AMF は、PDU セッションの確立中に保存された ARP および S-NSSAI、UE コンテキストの EBI 情報、およびローカル ポリシーに基づいて、QoS フローに割り当てられた EBI を取り消す場合があります。割り当てられた EBI が取り消される場合、AMF は 関連する SMF（「解放されたリソースを提供する SMF」と呼ばれる）を要求し、取り消す EBI に対応するマップされた EPS QoS パラメータをリリースするために Nsmf_PDUSession_UpdateSMContext（取り消される EBI）を呼び出します。AMF は、割り当てられた EBI、ARP ペアと対応する PDU セッション ID および SMF アドレスとの関連付けを保存します。 |
| 3 | ステップ3 で要求を受信した「解放されたリソースを提供するSMF」は、Namf_Communication_N1N2Message Transfer（N2 SM 情報（PDU セッション ID、失効する EBI）、N1 SMコンテナ（PDUセッション変更コマンド（PDU セッション ID、失効するEBI））を呼び出して、（R）AN と UE に、失効する EBI に対応するマッピングされた EPS QoS パラメータを削除するように通知します。ホームルーティング ローミングのシナリオでは、H-SMF に V-SMF に対して無効にされる EBI が含まれており、無効にされる EBI に対応するマップされた EPS ベアラー コンテキストを削除するよう V-SMF に通知します。<br><br>対応する EPS QoS パラメータを割り当てることができず、サービスの続行が受け入れられない場合、SMF は QoS フローの削除を決定することもできます。<br><br>ホーム ルーティングのローミング シナリオの場合、「解放されたリソースを提供する SMF」は、N4 セッション変更要求を送信し、失効した EBI に対応する N4 セッションを解放するように PGW-U+UPF に要求します。<br><br>ホーム ルーティング ローミングの場合、V-SMF は PDU セッションに対して VPLMN が開始する QoS 変更を開始します。V-SMF は、H-SMF から受信した対応する QoS 変更メッセージに基づいて、Namef_Communication_N1N2Message Transfer を呼び出します。 |

| ステップ | 説明 |
|---|---|
| 4 | UE が CM-CONNECTED 状態の場合、AMF は N2 PDU セッション要求（SMF から受信した N2 SM 情報、NAS メッセージ（PDU セッション ID、N1 SM コンテナ（PDU セッション変更コマンド））メッセージを（R）AN に送信します。<br><br>UE が CM-IDLE 状態で、ATC がアクティブになっている場合、AMF は Namef_Communication_N1N2MessageTransfer に基づいて UE コンテキストを更新および保存し、ステップ 5 とステップ 6 はスキップされます。たとえば、UE が CM-CONNECTED 状態になると、AMF は N1 メッセージを転送して UE コンテキストを UE と同期します。 |
| 5 | この手順の関連ステップは、前の図で指定されているように実行されます。 |
| 6 | AMF は EBI の割り当てに成功すると、割り当てられた EBI で応答します。それ以外の場合は、EBI 割り当ての失敗を示す原因で応答します。<br><br>同じ DNN に対して、別の SMF からの PDU セッションがすでに存在する場合、AMF は、EBI 割り当て要求を拒否するか、既存の PDU セッションから同じ DNN で異なる SMF への EBI を取り消します。AMF は、オペレータ ポリシーに基づいて決定を行います。<br><br>**Note**<br>上記のステートメントは、PDU セッションの S-NSSAI が異なる場合にのみ適用されます。それ以外の場合は、同じ DNN への PDU セッションに対して同じ SMF が選択されます。 |

| ステップ | 説明 |
|---|---|
| 7 | PGW-C+SMF は、PGW-U+UPF への N4 セッション確立/変更要求を送信します。<br>家庭用ローミングのシナリオでは、EBIが正常に割り当てられている場合、PGW-C+SMF は各 EPS ベアラーの CN トンネル情報を準備します。CN トンネル情報が PGW-C+SMF によって割り当てられている場合、EPS ベアラーの PGW-U トンネル情報は PGW-U + UPF に提供される場合があります。CN トンネル情報が PGW-U + UPF によって割り当てられている場合、PGW-U+UPF は、EPS ベアラーの PGW-U トンネル情報を PGW-C + SMF に送信します。PGW-U + UPF は、NG-RAN からアップリンク パケットを受信します。<br>**Note**<br>• ホームルーティング ローミングのシナリオでは、PGW-C+SMF は各 EPS ベアラーの CN トンネル情報を作成し、V-SMF に提供します。したがって、UE が EPS ネットワークに移動する場合、V-SMF は EPS ベアラー コンテキストを取得するために PGW-C+SMF と対話する必要はありません。<br>• CN トンネル情報が PGW-C + SMF によって割り当てられ、PDU セッションの確立時に PGW-U + UPF に提供されない場合、UE がターゲット RAT に移動すると、PGW-U + UPF はPGW-C+SMF は、N4 セッション変更で PGW-U+UPF にトンネル情報を提供しています。これにより、システム間引き継ぎの実行中に UL データの短時間の中断が発生します。<br>• SMF は、5G PDU 確立中および 5G PDU 変更（新しいフロー作成時）において、EPS ベアラー用の他の RAT トンネルの作成をサポートします。SMF は、N4 確立で EPS ベアラーに追加の PDR を送信し、EPS ベアラー向けにこれらの追加のトンネルを作成すると、UPF と通信するための N4 変更要求を送信します。 |
| 8 | PGW-C+SMF は、AMF から任意の EBI を受信すると、受信した EBI をマッピングされた EPS ベアラー コンテキストに追加します。<br>ホームルーティング ローミングのシナリオでは、PGW-C+SMF は EPS ベアラー コンテキストを生成します。これには、EPS ベアラーごとの PGW-U トンネル情報が含まれます。さらに、デフォルトの EPS ベアラーが PDU セッションの対応する PDN 接続に対して生成された場合（つまり、PDU セッションの確立手順中に）、PGW-C + SMF は PDN 接続の PGW-C トンネル情報を生成し、それをUE EPS PDN 接続に含めます。 |
| 8a | （条件付き）非ローミングまたは LBO シナリオでは、PGW-C+SMF には、マップされた EPS ベアラー コンテキストと、N1 SM コンテナで UE に送信される対応する QoS フローが含まれます。PGW-C+SMF は、QoS フローと N1 SM コンテナ内のマッピングされた EPS ベアラー コンテキスト間のマッピングも示します。PGW-C+SMF には、NG-RAN に送信する N2 SM 情報で受信した EBI と QFI 間のマッピングも含まれます。PGW-C+SMFは、Namef_Communication_N1N2MessageTransferを介してN1 SMコンテナとN2 SMの情報をAMFに送信します。 |

| ステップ | 説明 |
|---|---|
| 8b | （条件付き）ホームルーティング ローミングのシナリオでは、PGW-C+SMF は、マッピングされた EPS ベアラー コンテキスト、受信した EBI と QFI の間のマッピング、および PDU セッション確立中に Nsmf_PDUSession_Create 応答を介して、または PDU セッション変更中に Nsmf_PDUSession_Update 要求を介して EPS ベアラーコンテキストを V-SMF に送信します。V-SMF は EPS ベアラーコンテキストを保存し、N1 SM コンテナと N2 SM の情報を生成して、Namef_Communication_N1N2MessageTransfer を介して AMF に転送します。 |
| 9 | N1 SM コンテナと N2 SM の情報は、それぞれ UE と NG-RAN に送信されます。この手順の関連ステップは、前の図で指定されているように実行されます。 |

## N4 最適化コール フローによる非ローミング 5G PDU の確立

このセクションでは、N4 最適化を使用した非ローミング 5G PDU の確立のコール フローについて説明します。

**図 *69 : N4* 最適化コール フローによる非ローミング *5G PDU* の確立**

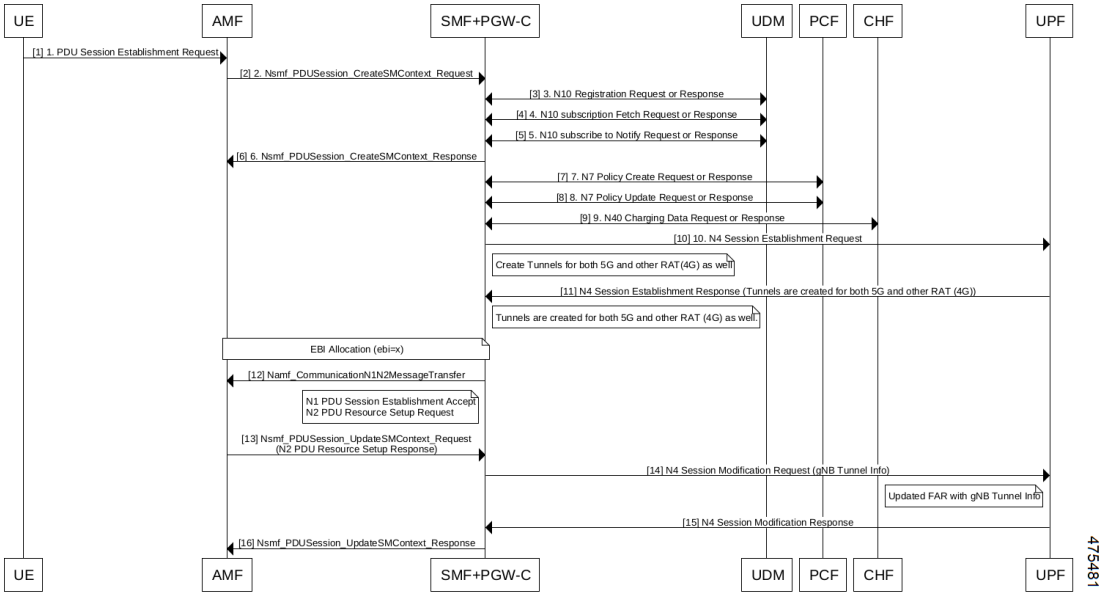



**表 *79 : N4* 最適化コール フローの説明による非ローミング *5G PDU* 確立**

| ステップ | 説明 |
|---|---|
| 1 | UE は PDU セッション確立要求を AMF に送信します。 |

| ステップ | 説明 |
|---|---|
| 2 | AMF は、Nsmf PDU セッションの CreateSMContext 要求を SMF+PGW-C に送信します。 |
| 3 | SMF + PGW-C は、UDMにN10登録要求を送信します。次に、UDMは、N10登録応答をSMF + PGW-Cに送信します。 |
| 4 | SMF + PGW-C は、N10 サブスクリプション取得要求を UDM に送信します。次に、UDMは、N10サブスクリプション取得応答をSMF + PGW-Cに送信します。 |
| 5 | SMF + PGW-C は、UDM に N10 サブスクライブ要求を送信します。次に、UDMは、N10 Subscribe to Notify 応答をSMF + PGW-Cに送信します。 |
| 6 | SMF + PGW-C は、Nsmf PDU セッション CreateSMContext 応答を AMF に送信します。 |
| 7 | SMF + PGW-C は、N7 ポリシー作成要求を PCF に送信します。PCF は、SMF + PGW-C に N7 ポリシー作成応答を送信します。 |
| 8 | SMF + PGW-C は PCF に N7 ポリシー更新要求を送信します。PCF は、SMF + PGW-C に N7 ポリシー更新応答を送信します。 |
| 9 | SMF + PGW-C は CHF に N40 課金データ要求を送信します。CHF は、N40 課金データ応答を SMF+PGW-C に送信します。 |
| 10 | SMF + PGW-C は、N4 セッション確立要求を UPF に送信します。SMF は、5G とその他の RAT（4G）の両方のトンネルを作成します。 |
| 11 | トンネルの作成後、UPF は N4 セッション確立応答を SMF + PGW-C に送信します。 |
| 12 | SMF + PGW-C は、EBI 割り当て手順を開始します。次に、SMF + PGW-C は、Namef 通信 N1N2Message 転送要求を AMF に送信します。 |
| 13 | N1 PDU セッションの確立が承認され、N2 PDU リソース設定要求が送信された後、SMF + PGW-C は、Nsmf PDU セッション UpdateSMContext 要求（N2 PDU リソース設定応答）を SMF + PGW-C に送信します。 |
| 14 | SMF + PGW-C は、N4 セッション変更要求を UPF に送信します。この要求には、gNB トンネルの詳細が含まれています。 |
| 15 | UPF は、N4 セッション変更応答を SMF + PGW-C に送信します。応答には、更新された FAR と gNB トンネルの詳細が含まれます。 |
| 16 | SMF+PGW-C は、Nsmf PDU Session UpdateSMContext Response を AMF に送信します。 |

### PDU セッション管理での N1N2 メッセージ転送

表 *80*：機能の履歴

| 機能名 | リリース情報 | 説明 |
|---|---|---|
| 3GPP リリース 16 の準拠に対する PDU セッション管理プロセスの強化 | 2025.01.0 | PDUセッション管理プロセス中に、後続のN1N2メッセージ転送要求を受信すると、AMF は、この要求が新しく選択された SMF によって発行されたか、または元々選択されていた SMF によって発行されたかを判断できません。この機能により、SMF は既存の nfId 属性で、N1N2 メッセージ転送要求で **NFInstanceID** を送信できます。 |

PDU セッション中、SMF は AMF に対して N1N2 メッセージ転送要求を送信します。N1N2 メッセージ転送は、PDUセッションの確立、PDUセッションの変更、PDUセッションのリリース、NG-RAN 間ノード N2 ベースのハンドオーバーなどの手順で送信されます。

N1N2 メッセージ転送要求に、N1 メッセージと N2 メッセージのいずれかまたは両方が含まれている。N1 PDU メッセージは、既存の nfId 属性で、N1N2 メッセージ転送要求の **NFInstanceID** を示します。これにより、AMF は N1 メッセージの送信を要求している SMF インスタンスを識別できます。

## 標準準拠

この機能は、以下の基準に準拠しています。

- *3GPP TS 23.401*、バージョン *15.6.0*
- *3GPP TS 23.502*、バージョン *15.4.0*
- *3GPP TS 29.502*、バージョン *16.2.0*
- *3GPP TS 29.518*、バージョン *16.4.0*

# 5G PDU セッション パラメータからの EPS PDN 接続パラメータの生成

このセクションでは、PGW-C+SMF の 5G PDU セッション パラメータから EPS PDN 接続パラメータを生成する方法について説明します。

PGW-C+SMF が EPS と 5GC 間のインターワーキングをサポートする PDN 接続または PDU セッションの設定または変更を要求されると、PGW-C+SMF は PDU セッション パラメータから PDN 接続パラメータを生成します。

PGW-C+SMF が PDU セッション パラメータに基づいて PDN 接続パラメータを生成する場合、次のルールが適用されます。

- PDN タイプ：PDU セッション タイプがそれぞれ IPv4 または IPv6 の場合、PDN タイプは IPv4 または IPv6 に設定されます。PDN タイプは、イーサネットおよび非構造化 PDU セッション タイプの非 IP に設定されます。
- EPS ベアラー ID：EPS と 5GC 間のインターワーキングをサポートする PDU セッションにおいて、 *3GPP TS 23.502*、セクション *4.11.1.4.1*で説明されているように、QoS フローの確立中に AMF から EBI が要求されます。EBI は、PGW-C+SMF によってホストされる PDN 接続用の *3GPP TS 23.401* で定義されているように、（QoS フローの確立によってトリガされる）EPS ベアラーの確立中に MME から取得されます。EBI と QoS フローとの関連付けは、SMF によって保存されます。
- APN-AMBR：APN-AMBR は、オペレータ ポリシーに従って設定されます。たとえば、セッション AMBR を考慮します。
- EPS QoS パラメータ（ARP、QCI、GBR、MBR など）：
  - QoS フローが 1 つの EPS ベアラーにマッピングされている場合：EPS ベアラーの ARP、GBR、および MBR は、対応する QoS フローのそれぞれの ARP、GFBR、および MFBR に設定されます。
  - 標準化された 5QI の場合、QCI は 5QI に 1:1 でマッピングされます。標準化されていない 5QI の場合、PGW-C+SMF は、5QI およびオペレータ ポリシーに基づいて QCI を導出します。

**Note** EBI が割り当てられている場合、GBR QoS フローは GBR 専用 EPS ベアラーに 1:1 でマッピングされます。他の GBR QoS フローは、インターワーキング中に終了されます。複数の QoS フローが 1 つの EPS ベアラーにマッピングされている場合、EPS ベアラーパラメータはオペレータポリシーに基づいて設定されます。たとえば、EPS ベアラーの QoS パラメータは、すべてのマッピングされた QoS フローの最高 QoS に従って設定されます。

**Note** EBI が割り当てられていない非 GBR QoS フローは、デフォルトの EPS ベアラーにマッピングされます。

# N26 インターフェイスを使用する 5G から EPS へのハンドオーバー

## 機能説明

SMF は、MME と AMF の間に N26 インターフェイスが存在する場合、5GC 上の EPS への PDU セッションのハンドオーバーをサポートします。ハンドオーバーは、適用可能なデフォルトベアラーと専用ベアラーの作成をサポートします。

### 機能の仕組み

このセクションでは、5GからEPSへのハンドオーバー手順と5GからEPSへのハンドオーバーをキャンセルする手順について説明します。

#### コール フロー

このセクションでは、次のコールフローについて説明します。

- 5G から EPS へのハンドオーバー コール フロー
- 5G から EPS へのハンドオーバー キャンセルのフロー

##### *5G* から *EPS* へのハンドオーバーのコール フロー

このセクションでは、N26 インターフェイスを使用した 5G から EPS へのハンドオーバー コール フローを説明します。

EPS セッションでの 5G から EPS へのハンドオーバー手順は、3GPP 23.502、セクション 4.11.1.2.1 に準拠しています。

1. AMF は、Nsmf_PDUSession_ContextRequest を使用して SM コンテキストを提供するように SMF に要求します。
2. SMF は N4 セッション変更を UPF に送信して、各 EPS ベアラーの CN トンネルを確立します。PCC から受信した 5G QoS および PCC ルールへのベアラー マッピングは、SMF にすでに存在している必要があります。SMF には、ベアラー ID の割り当て手順から取得したベアラー ID も必要です。

   SMF は N4 セッションの新しい PDR を作成し、4G システムの要求に応じて各ベアラーに割り当てられる TEID を取得します。
3. SMF は AMF に EPS ベアラー コンテキストを提供します。SMF は、E-UTRAN からのアップリンク トラフィックのすべてのベアラーの CN トンネル情報を AMF に提供します。

4. 間接データ転送が適用される場合、AMFは、間接データ転送トンネルを作成するために、Nsmf_PDUSession_UpdateSMContext要求（データ転送用のS-GWアドレスおよびS-GW DL TEID）をSMFに送信します。
5. SMF は、N4 変更要求を UPF に送信して追加の PDR と FAR を作成し、NG RAN から間接トンネルを介してリダイレクトされた DL データを受信し、それらを eNodeB に転送します。アップリンク PDR は、NG-RAN から転送された DL データと一致するために QFI を持っている必要があり、データをeNodeB に転送する必要があるため、関連付けられた QER は QFI を持ちません。FAR は、QFI に基づく適切なトンネルを介して受信したデータを eNodeB にリダイレクトします。
6. S-GW は、ベアラーの SMF の DL TEID を使用して、ベアラー要求の変更を SMF に送信します。
7. SMF は N4 変更要求を UPF に送信し、E-UTRAN への DL データ パスをアクティブにします。この時点で、間接トンネルと直接 DL パスの両方が eNodeB に対してアクティブになります。
8. SMF は、ベアラー応答の変更を S-GW に送信します。
9. AMF は、転送トンネルを解放するように指示して、Nsmf_PDUSession_UpdateSMContext Request サービス操作を開始します。
10. SMF は、間接トンネルの PDR と FAR を削除するために、N4 変更要求を UPF に送信します。不要な 5G セッションの PDR と FAR も削除されます。

## *5G* から *EPS* へのハンドオーバー キャンセルのコール フロー

準備フェーズの後に送信元無線アクセスネットワーク(RAN)がハンドオーバー キャンセルをトリガーすると、AMF は SMF に対して「Nsmf_PDUSession_UpdateSMContext 要求（SUPI、Relocation Cancel Indication）」を呼び出します。再配置キャンセル通知に基づいて、SMF はハンドオーバーの準備フェーズ中に確立されたセッション リソースを削除します。つまり、SMF は、間接トンネルと 5G セッションのハンドオフの準備で割り当てられたすべてのパケット検出ルール（PDR）、転送アクション ルール（FAR）、およびその他のルールを削除します。

次のコール フローは、5GS から EPS へのハンドオーバーのキャンセル手順を示しています。

図 *70 : 5GS* から *EPS* へのハンドオーバー キャンセルのコール フロー

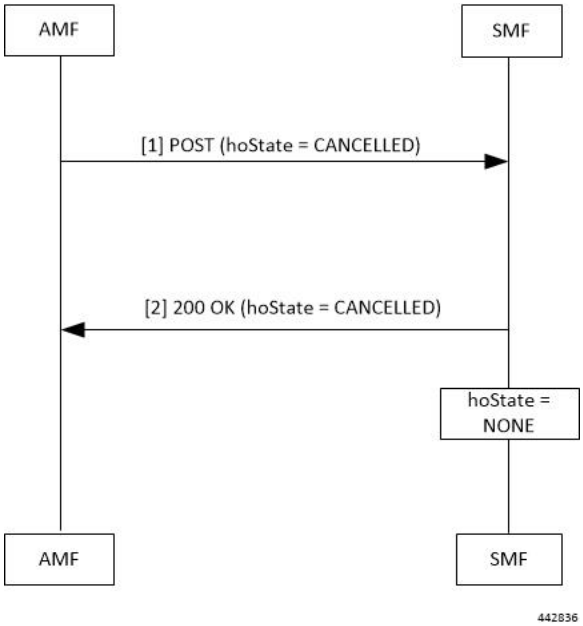



表 *81 : 5GS* から *EPS* へのハンドオーバーのキャンセルコール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | AMF は、Sm コンテキスト更新サービスの POST 要求を送信して、既存の PDU セッションのハンドオーバーをキャンセルするよう SMF に要求します。その際、次の情報が提供されます。<br>• SMF の個々の SM コンテキスト リソースの hoState 属性を [キャンセル済み（CANCELED）] に更新する<br>• 原因情報 |
| 2 | SMF は、次の情報を含む 200 OK 応答メッセージを返します。<br>• hostState 属性を CANCELED に設定<br>SMF は、ターゲット RAN へのハンドオーバー用に予約されているリソースを解放するなど、ハンドオーバーの実行をキャンセルします。その後、SMF は hoState を NONE に設定し、保存されている targetServingNfId を削除します。 |

## 標準準拠

5GからEPSへのハンドオーバー機能は、*3GPP TS 23.502*、バージョン*15.3.0*に準拠しています。

# 専用ベアラの作成に対する遅延および再試行のサポート

## 機能説明

専用ベアラーの作成に対する遅延および再試行のサポート機能によって、次の処理が容易になります。

- 引き継ぎが完了した後、構成された時間に基づいて専用ベアラーの作成を遅らせます。
- 次のいずれかのシナリオで、IMS ベアラー専用ベアラーの作成を再試行します。
  - 移行中の移行中に MME に障害が発生した場合。
  - IMS ベアラーが一時的に到達不能な場合。
- ハンドオーバーが完了すると、SMF サービスが構成されたタイマーで開始されます。次に、専用ベアラーの作成が開始されます。
- IMS 専用ベアラーの作成が失敗した場合、最大再試行回数の構成によって、作成プロセスで試行される再試行回数が決まります。構成されたタイムアウトにより、各再試行の遅延が決まります。

## 機能の仕組み

このセクションでは、専用ベアラー作成の遅延およびサポート機能の再試行の動作の概要について説明します。

### コール フロー

ここでは、次のコール フローについて説明します。

図 *71 : EPS* フォールバック ガード タイマー コール フロー

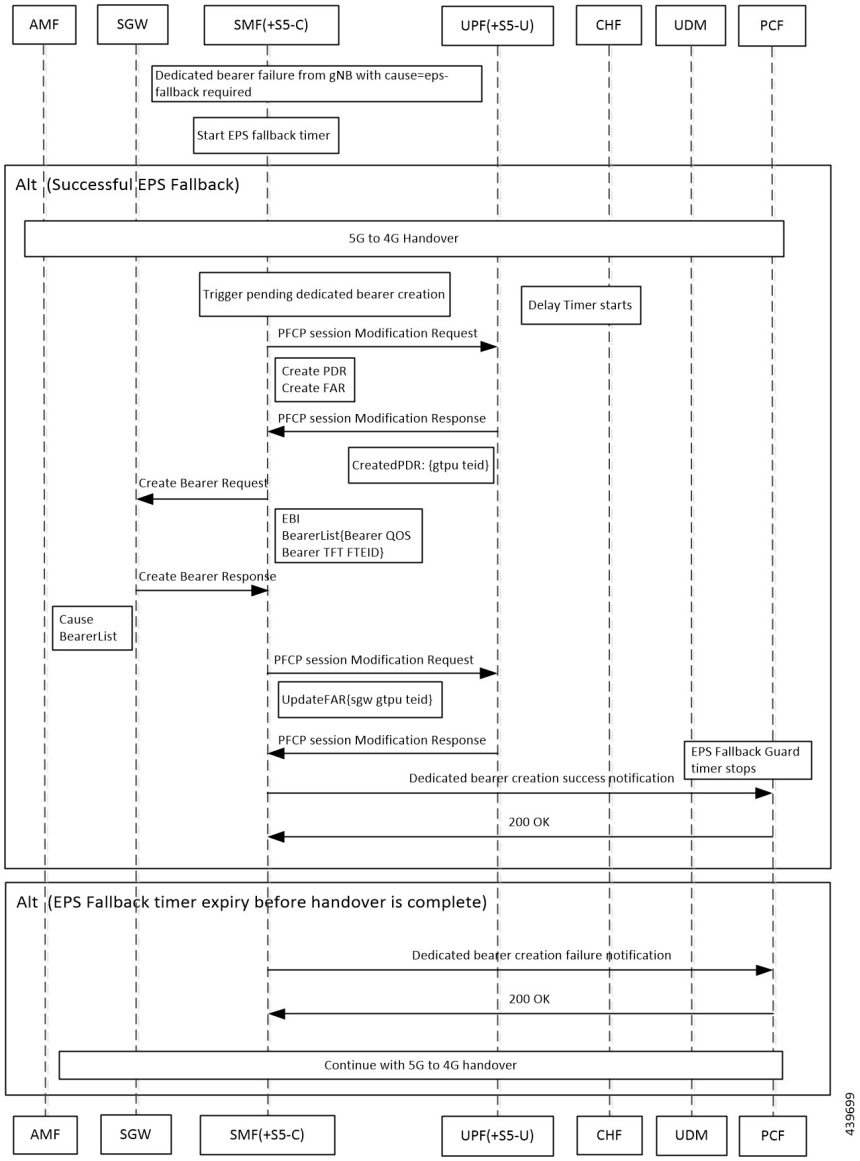



表 *82 : EPS* フォールバック ガード タイマー コール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | gNB は、AMF を介してフォールバック原因とともに専用ベアラ作成の失敗情報を送信します。 |
| 2 | EPS フォールバック タイマーが開始されます。 |
| 5G から 4G へのハンドオーバー後に EPS フォールバックが成功すると、手順 3 ー 12 が発生します。 | |

| ステップ | 説明 |
|---|---|
| 3 | EPS は、保留中の専用ベアラーの作成をトリガーします。 |
| 4 | 遅延タイマーが開始されます。 |
| 5 | SMF（+S5-C）は、PFCP セッション変更要求を UPF（+S5-U）に送信します。 |
| 6 | PDR および FAR が作成されます。 |
| 7 | UPF（+S5-U）は、PFCP セッション変更応答を SMF（+S5-C）に送信します。 |
| 8 | GTP-U TEID で作成された PDR の情報が利用できます。 |
| 9 | SMF（+S5-C）は、S-GW にベアラー要求の作成を送信します。 |
| 10 | S-GW は、SMF（+S5-C）にベアラー応答の作成を送信します。 |
| 11 | SMF（+S5-C）は、PFCP セッション変更要求を UPF（+S5-U）に送信します。 |
| 12 | UPF（+S5-U）は、専用ベアラーの作成に成功したという通知を PCF に送信します。 |
| 13 | EPS フォールバック ガード タイマーが停止します。 |
| 14 | PCF は「200 OK」の確認応答を SMF（+S5-C）に送信します。 |
| 引き継ぎが完了する前に EPS フォールバック タイマーが期限切れになるシナリオでは、ステップ 13 ～ 15 が発生します。 | |
| 15 | SMF（+S5-C）は、専用ベアラー作成の失敗通知を PCF に送信します。 |
| 16 | PCF は「200 OK」の確認応答を SMF（+S5-C）に送信します。 |
| 17 | 5G から 4G へのハンドオーバー手順が続行されます。 |

# 専用ベアラー作成の遅延および再試行のサポートの構成

このセクションでは、専用ベアラー作成の遅延および再試行サポート機能の構成について説明します。

```
config
   profile access accesstemp
     eps-fallback cbr delay delay_time max-retry retry_count
     timeout timeout_value
     end
```

注：

- **delay** *delay_time*：専用ベアラーの作成の遅延時間をミリ秒単位で指定します。有効値の範囲は 0 ～ 10000 ミリ秒です。デフォルトは 0 です。
- **max-retry** *retry_count*：専用ベアラーの作成を再試行する回数を指定します。有効な値の範囲は 0 ～ 10 です。デフォルトは 0 です。

- **timeout** *timeout_value*：専用ベアラーの作成を再試行するまでのタイムギャップを秒単位で指定します。有効な値の範囲は、1 ～ 3 秒です。デフォルトは 1 です。

### 専用ベアラー作成の遅延および再試行サポート構成の確認

ここでは、専用ベアラー作成の遅延と再試行サポートの構成を確認する方法について説明します。

**show running-config** コマンドを使用して、設定を表示します。

次に、**show running-config** コマンドの出力例を示します。

```
profile smf smf1
service name smf-service
  access-profile access1
!
!
profile access access1
eps-fallback cbr delay 100 max-retry 5 timeout 2
```

# タイマーの期限切れによる専用ベアラー手順エラーの処理

## 機能説明

このセクションでは、専用ベアラー手順が定義された手順タイムアウト値内に終了しない場合のSMFの動作について説明します。このタイムアウトをサービス レベル契約（SLA）タイマーと呼びます。手順レベルで定義される SLA タイムアウトは、手順 SLA タイマーと呼ばれます。

専用ベアラー手順の処理中に、SMF はピア NF と連携します。ピア NF は、次のいずれかになります：

- S-GW
- PC-F
- CHF
- UPF

専用ベアラー手順の完了前に SLA タイマーが期限切れになると、SMF およびピア ノードでグレースフルクリーンアップが実行されます。このクリーンアップアクションは、専用ベアラーの手順が実行されている段階に基づきます。

# 機能の仕組み

SMF は、専用ベアラー手順の開始時に手順 SLA タイマーを開始し、手順の終了時に停止します。エンドポイント構成により、インターフェイス（N11、N7、N40）レベルでSLAタイマーを定義できます。構成の詳細は、このガイドの 専用ベアラー手順障害処理機能の構成 （311 ページ） セクションを参照してください。

手順 SLA は、専用ベアラー手順を開始する次のトランザクションでサポートされます。

- N7 ポリシー通知要求（PCF によって開始される変更）
- ベアラー削除コマンド（SGW によって開始された削除）
- 専用ベアラー手順を開始する内部トランザクション。たとえば、NintSelfTxnExpPcfUpdNotifyReq には、N7 ポリシー通知要求（PCF によって開始される変更）と同様の SLA タイムアウト処理があります。

手順タイマーが期限切れになると、SMF とピア ノードで必要なクリーンアップが実行されます。このクリーンアップ アクションは、専用ベアラーのコール フローが存在する段階に基づきます。この操作は、ピアからの応答を長時間待機しているプロシージャ インスタンスを特定し、それに応じてそれらを処理するのに役立ちます。

## コール フロー

ここでは、この機能に関連した次のコール フローについて説明します。

### PCF によって開始された変更コール フロー

このセクションでは、プロシージャ SLA タイマーが期限切れになった場合の、PCF によって開始された専用ベアラー変更コール フローの処理について説明します。

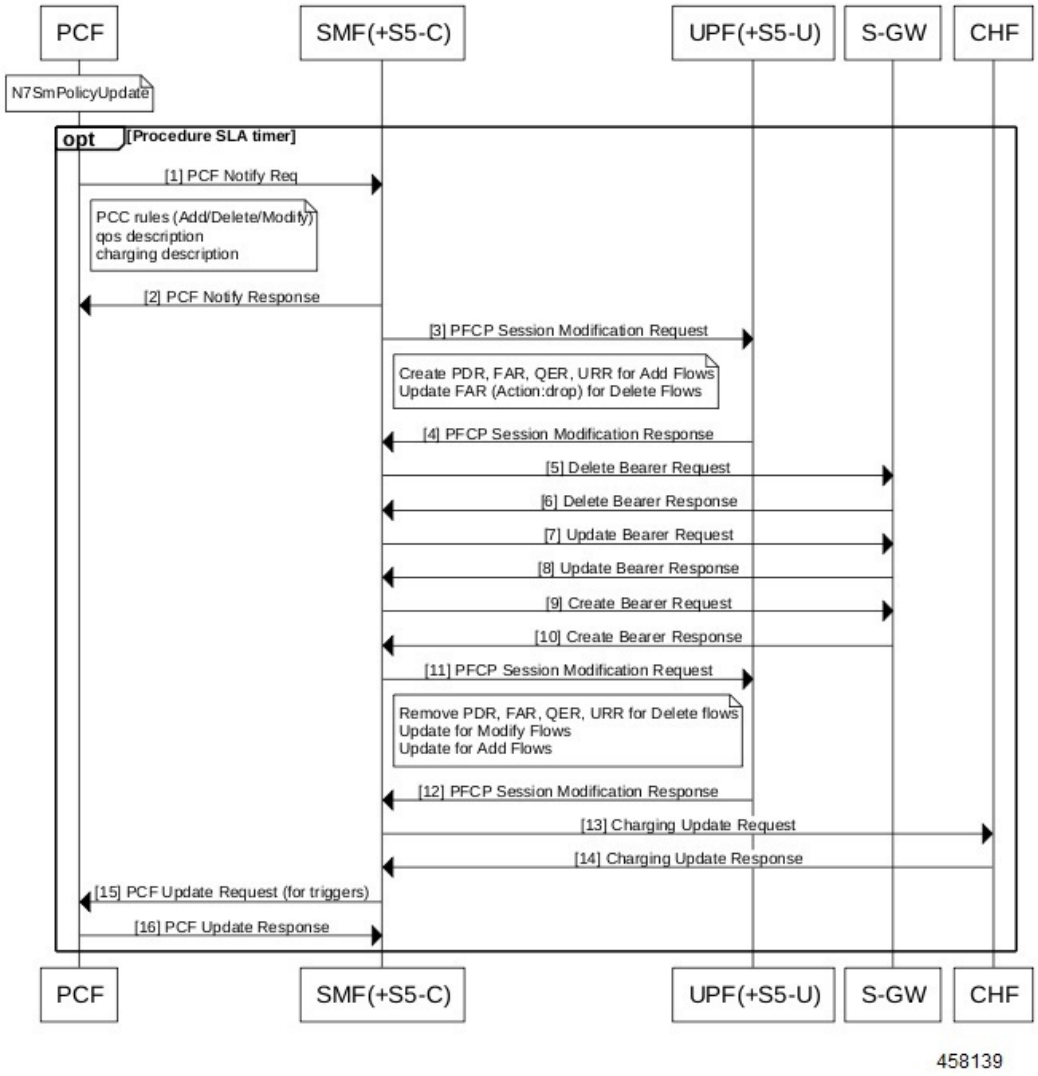
この項で説明する手順 SLA 処理には、次のトリガーにより内部トランザクションによって開始される、他の種類の専用ベアラー手順が含まれます：

- PCF によって開始されたトリガー：ピギーバック専用ベアラ手順、PCF 更新/通知応答がトリガーした専用ベアラ手順、NIntSelfTxnExpPcfUpdNotifyReq など。
- その他のトリガー：Call Sub、Revalidation Timeout、N4 セッションレポート、内部 Txn により、コリジョンの中断時に専用ベアラー手順を再起動します。

（注） SMF は、専用ベアラー手順のエラーを処理するために、N7 インターフェイスの手順 SLA 構成を使用します。

次の図は、PCF からの N7 ポリシー通知要求によって開始される専用ベアラー変更のコール フローを示しています。

図 *72 : PCF* によって開始された変更コール フロー




次の表に、プロシージャ SLA タイマーが期限切れになったときに各段階で実行される処理を示します。

表 *83 : SLA* タイマー期限切れ中の *PCF* によって開始された変更の処理

| タイムラインまたはスライスの可用性 | 要求または、イベント | ステージ：失敗 | SLA によるタイムアウト |
|---|---|---|---|
| 構成された手順の SLA | N7 PCF 通知要求 | PCF 通知 | HTTP ステータス コード「504 Gateway Timeout」と「TIMED_OUT_REQUEST」のプロトコルエラーで N7 PCF 通知に応答します。 |
| 構成された手順の SLA | | 最初の N4 変更要求 | **新しく追加されたフローの場合**：<br>非同期N4変更により、新しいフローのN4トンネルを削除します。<br>トリガーに基づいてルール レポートを使用して非同期 PCF 更新を送信します。<br>**削除されたフローの場合**：<br>ベアラー削除要求（DBR）<br>N4 を同期して、削除されたルールのトンネルを削除します。削除されたフローの N4 変更応答で UPF が送信する使用状況レポートの損失を回避するために、同期手順を実行します。<br>トリガーに基づくルールレポートを使用した非同期 PCF 更新。 |

| タイムラインまたはスライスの可用性 | 要求または、イベント | ステージ：失敗 | SLA によるタイムアウト |
|---|---|---|---|
| 構成された手順の SLA | | ベアラー要求の削除 | N4 を同期して、削除されたルールのトンネルを削除します。削除されたフローの N4 変更応答で UPF が送信する使用状況レポートの損失を回避するために、同期手順を実行します。<br>トリガーに基づくルールレポートを使用した非同期 PCF 更新。 |
| 構成された手順の SLA | | ベアラー更新の要求 | 現在サポート対象外 |
| 構成された手順の SLA | | ベアラー要求の作成 | 削除されたフローと新しいフローの N4 トンネルを削除する非同期 N4 変更。<br>トリガーに基づいてルール レポートとともに PCF 更新を送信します。 |
| 構成された手順の SLA | | 第 2 の N4 変更要求 | **追加されたフローの場合**：<br>非同期 DBR および非同期 N4 変更を実行します。非同期障害ルールレポートを PCF に送信します。<br>**削除されたフローの場合**：<br>非同期成功ルール レポートを PCF に送信します。次に、PDU コンテキストを更新します。 |

| タイムラインまたはスライスの可用性 | 要求または、イベント | ステージ：失敗 | SLA によるタイムアウト |
|---|---|---|---|
| 構成された手順の SLA | | 課金更新要求 | 最後のレッグ、手順の成功として扱います。<br>トリガーに基づいて成功ルール レポートとともに PCF 更新を送信します。次に、PDU コンテキストを更新します。 |
| 最終段階：寛容なアプローチ、SLA なし | | PCF 更新要求 | 変更完了のマークを付けます。 |

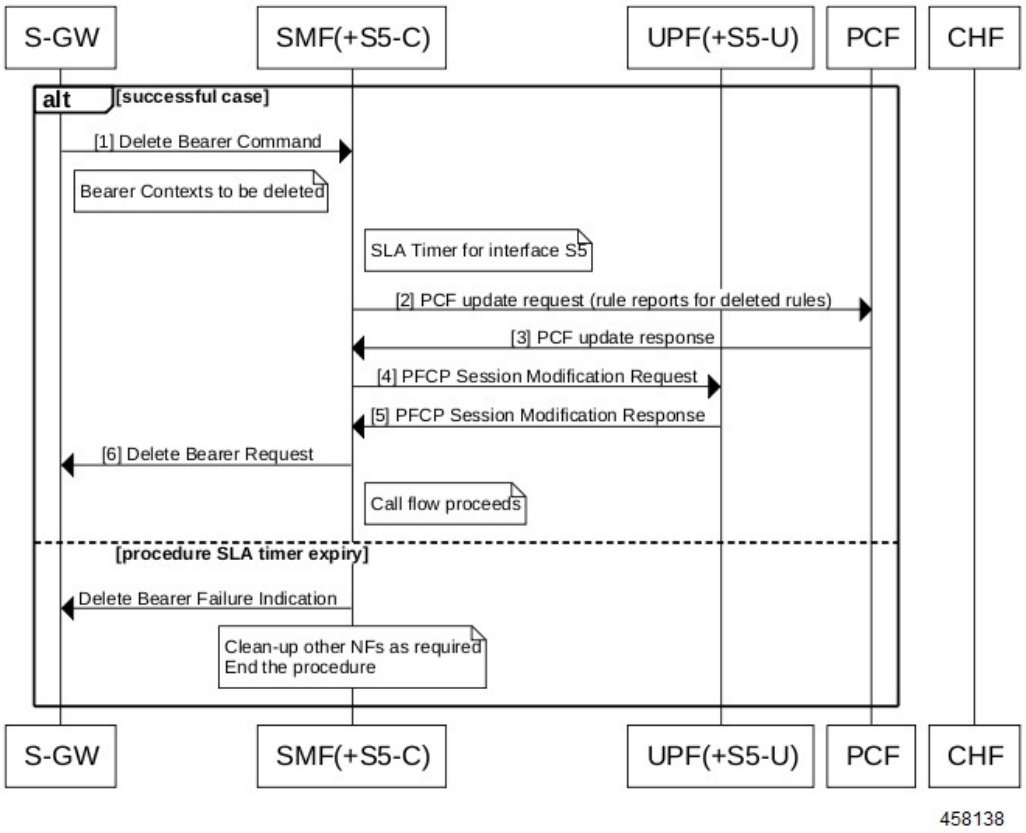
## PCRF 開始セッション削除のコール フロー

このセクションでは、手順 SLA タイマーが期限切れになった場合の MME によって開始された専用ベアラー削除コールフローの処理について説明します。ベアラーコマンドの削除（DBC）の手順 SLA タイマーが期限切れになると、SMF はベアラー障害の削除表示を送信します。

（注） SMF は、RAT タイプに基づいて、S5 または S2b インターフェイスに対して SLA 設定手順を使用します。

次の図は、ベアラー コマンドの削除の受信時に MME によって開始される専用ベアラー削除コール フローを示しています。

図 *73 : PCRF* 開始セッション削除のコール フロー




次の表に、SLA タイマーが期限切れになったときに各段階で実行される処理を示します。

表 *84 : SLA* タイマーの期限切れ中に *MME* によって開始された削除の処理

| タイムラインまたはスライスの可用性 | 要求または、イベント | ステージ：失敗 | トランザクション SLA によるタイムアウト |
|---|---|---|---|
| 構成された手順の SLA | ベアラー削除コマンド | アイドル（Idle） | ベアラー障害表示の削除の送信 |
| 構成された手順の SLA | | PCF 更新要求 | ベアラー障害表示の削除の送信 |

| タイムラインまたはスライスの可用性 | 要求または、イベント | ステージ：失敗 | トランザクション SLA によるタイムアウト |
|---|---|---|---|
| 構成された手順の SLA | | 最初の N4 変更要求 | 非同期 DBR<br>N4 を同期して、削除されたルールのトンネルを削除します。削除されたフローの N4 変更応答を UPF が送信する使用状況レポートが失われるのを避けるために、同期手順を実行します。 |
| 構成された手順の SLA | | ベアラー要求の削除 | N4 を同期して、削除されたルールのトンネルを削除します。削除されたフローの N4 変更応答を UPF が送信する使用状況レポートが失われるのを避けるために、同期手順を実行します。 |
| 構成された手順の SLA | | 第 2 の N4 変更要求 | 手順の成功として処理します。次に、PDU コンテキストを更新します。 |
| 構成された手順の SLA | | 課金更新要求 | 手順の成功として処理します。次に、PDU コンテキストを更新します。 |

# 専用ベアラー手順障害処理機能の構成

このセクションでは、専用ベアラー手順障害処理機能を構成する方法を説明します。

## 手順 SLA タイマーの構成

次の構成例を使用して、手順 SLA タイマーを構成します。SMF はこのタイマーを使用して、専用ベアラ手順失敗処理を実行します。

```
config
   instance instance-id gr_instance_id
      endpoint { dns-proxy | gtp | gtpprime | li | nodemgr | pfcp |
```

```
protocol | radius | radius-dns | sbi | service | sgw-service }
         interface { n7 | s2b | s5 }
            sla procedure procedure_time
            end
```

注：

- **endpoint { dns-proxy | gtp | gtpprime | li | nodemgr | pfcp | protocol | radius | radius-dns | sbi | service | sgw-service }**：選択したインターフェイスのエンドポイント構成を開始します。たとえば、 **endpoint sbi** コマンドを使用すると、SBI エンドポイント構成を入力できます。
- **interface { n7 | s2b | s5 }**：手順タイマーが実行されているエンド ポイント インターフェイスを指定します。
- **sla procedure** *process_time* ：選択したインターフェイス固有の手順の手順 SLA タイマーを指定します。

  *procedure_time* は、1000 ～ 120000 の範囲である必要があります。

## 専用ベアラー手順障害処理機能の認証

ここでは、専用ベアラー手順障害処理機能の構成を確認する方法について説明します。

手順 SLA タイマー構成を確認するには、**show running-config instance instance-id** *gr_instance_id* **endpoint** コマンドを使用します。

**show running-config instance instance-id 1 endpoint sbi** コマンドの出力例を次に示します。

```
smf# show running-config instance instance-id 1 endpoint sbi
instance instance-id 1
 endpoint sbi
  replicas 2
  vip-ip 209.165.200.225
  interface n7
   loopbackPort 9118
   vip-ip 209.165.201.1 vip-port 8090
   sla procedure 4000
  exit
 exit
exit
```

# 専用ベアラ手順失敗処理機能の OAM サポート

ここでは、この機能の操作、管理、およびメンテナンスに関して説明します。

## バルク統計サポート

この機能の一部として、smf_service_stats 統計の「reason」ラベルに新しい値「timeout」が追加されます。この新しい値は、手順の SLA タイマーの期限切れを示します。

## トラブルシューティング情報

ここでは、トラブルシューティング情報について説明します。

- 警告とエラーのログを収集します。
- **monitor protocol** コマンドと pcap 機能を使用して、メッセージトレースを収集します。
- smf_service_stats の統計情報を調べます。

  プロシージャ SLA タイマーの期限切れ中に、理由が「タイムアウト」として表示されます。次に、smf_service_stats の例を示します。

専用ベアラ作成の場合：

```
smf_service_stats{Cause="SMF_Internal_Failure",Detailed_Cause="timeout",always_on="disable",app_name="SMF",
cluster="Local",data_center="DC",dcnr="disable",dnn="intershat",emergency_call="false",fourg_only_ue="false",
instance_id="0",pdu_type="ipv4",pra="none",procedure_type="pcf_req_ded_brr_create",qos_5qi="2",
rat_type="EUTRA",reason="timeout",roaming_status="homer",service_name="smf-service",
smf_current_procedure="",status="failures",up_state="UpState_Activated"} 1
```

専用ベアラ削除の場合：

```
smf_service_stats{Cause="SMF_Internal_Failure",Detailed_Cause="timeout",always_on="disable"
,app_name="SMF",cluster="Local",data_center="DC",dcnr="disable",dnn="intershat",emergency_call="false",
fourg_only_ue="false",instance_id="0",pdu_type="ipv4",pra="none",procedure_type="pcf_req_ded_brr_delete",
qos_5qi="3",rat_type="EUTRA",reason="timeout",roaming_status="homer",service_name="smf-service",
smf_current_procedure="",status="failures",up_state="UpState_Activated"} 1
```

# 4G セッションの GTP-U エラー通知の処理

## 機能説明

このセクションでは、SMF が GPRS トンネリング プロトコル、4G セッションのユーザー プレーン（GTP-U）エラー表示を処理する方法について説明します。

サービング ゲートウェイ（S-GW）は、不明なトンネル エンドポイント識別子（TEID）を持つ GTP-U メッセージを受信すると、トンネル ID を含む GTP-U エラー通知メッセージを UPF に送信します。GTP-U エラー通知を受信した UPF は、エラー通知（ERIR）を含む SMF に N4SessionReportRequest を送信します。SMF は N4SessionReportRequest に含まれる Fteid に基づいて EBI を取得し、セッションまたはベアラーの削除を開始します。SMF が S-GW にベアラー要求の削除を送信します。S-GW からの応答を受信すると、SMF は、ベアラーのタイプ（専用ベアラーまたはデフォルト ベアラー）に基づいて、N4 セッション変更要求または N4 セッション リリース要求のいずれかを UPF に送信します。CHF と PCF も、ベアラー タイプに基づいて通知されます。

（注） SMF が PFCPSessionReportRequest を受信すると、デバッグ メッセージの一部として IntSelfTxnN4SessRptReq メッセージが表示されます。

このセクションでは、SMF が Diameter インターフェイスで GTP-U エラー通知を処理する方法についても説明します。

## 標準準拠

GTP-U エラー通知処理機能は、次の標準に準拠しています。

- *3GPP TS 29.244*、バージョン *15.6.0*
- *3GPP TS 23.527*、バージョン *15.3.0*

# 機能の仕組み

## GTP-U エラー処理手順

このセクションでは、4Gセッションの GTP-Uエラー処理手順に関連付けられたコール フローについて説明します。

図 *74 : GTP-U* エラー通知処理コール フロー

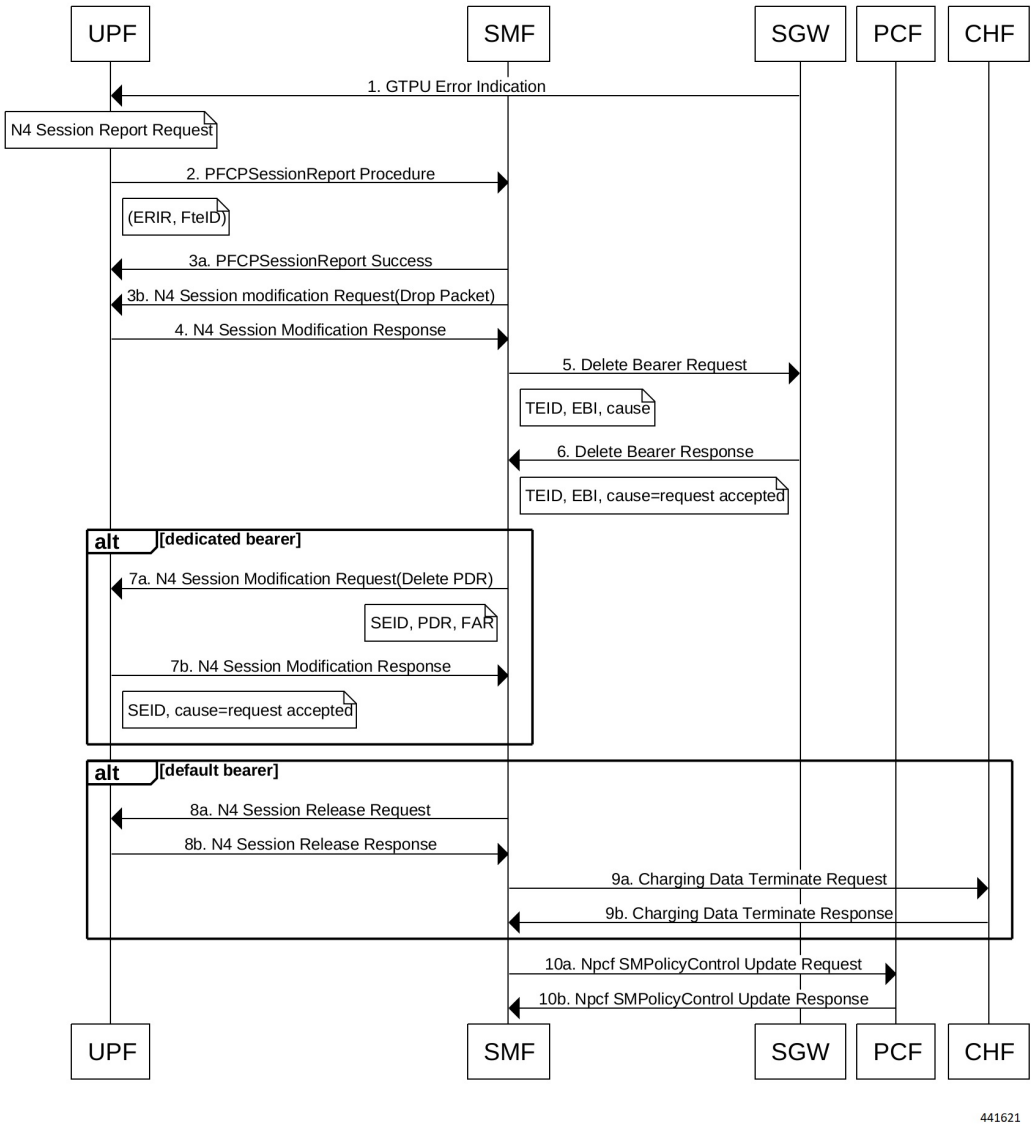



表 *85 : GTP-U* エラー処理コール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | S-GW は UPF に対して GTP-U エラー通知を送信し、失敗したベアラー ID をベアラーに示します。 |
| 2 | GTP-U エラー通知を受信した後、UPF は、失敗したベアラー ID とともに、PFCPSessionReport を SMF に送信します。 |

| ステップ | 説明 |
|---|---|
| 3a および 3b | SMF は、ドロップされたパケットの PFCPSessionReport Success メッセージおよび N4 セッション変更要求を UPF に向けて送信します。 |
| 4 | UPF が SMF に N4 セッション変更応答を送信します。 |
| 5 | SMF が、TEID、EBI、および原因とともに S-GW にベアラー要求の削除を送信します。 |
| 6 | S-GW は、TEID、EBI、および要求として受け入れられた原因とともに、SMF にベアラー応答の削除を送信します。 |
| 7a | TEID が専用ベアラーの場合、SMF は PDR の削除を含む N4 セッション変更要求を送信します。 |
| 7b | UPF が N4 セッション変更応答を送信します。 |
| 8a | デフォルト ベアラーの場合、SMF は N4 セッション リリース要求を送信します。 |
| 8b | UPF は N4 セッション リリース応答を送信します。 |
| 9a | SMF は、CHF に課金データ終了要求を送信します。 |
| 9b | CHF は課金データ終了応答で応答します。 |
| 10a | SMF は、NPCF SMPolicyControl 更新要求を PCF に送信します。 |
| 10b | PCF は、SMF に SMPolicyControl 更新応答を送信します。 |

# Diameter インターフェイスでの GTP-U エラーの表示

SMF はエラー通知（ERIR）を含むセッション レポートをサポートしています。SMF はセッション レポート ステートレスに応答し、要求を処理します。SMF は ERIR を受信時に 4G セッションの切断手順を開始し、ERIR がデフォルトのベアラー用の場合は、S-GW または MME に対するベアラー応答の削除（DBR）をトリガーします。コール フローと説明の詳細については、「UPF によって開始されたデタッチ手順」の セクションを参照してください。

## セッションの遅延削除の構成

ERIR を含むセッション レポートの受信後にセッション切断を遅らせるように、SMF で次の構成を使用します。この設定は、デフォルトのベアラーにのみ適用されます。

```
config
   profile access access
      erir delay  delay_interval
   exit
```

注：

**erir delay** *delay_interval*：遅延時間をミリ秒単位で 0 ～ 3000 の範囲で指定します。デフォルト値は、0 です（無効）。

# GTP パス障害の処理、復元、およびリカバリ

## 機能説明

SMF は以下をサポートします。

- *3GPP TS 29.274*に従った次の GTP-C パス管理メッセージの処理
  - エコー要求
  - エコー応答
- 設定に従って、新しく検出された GTP-C ピアにエコー要求メッセージを送信します。
- GTP-C ピアからエコー要求メッセージを受信した場合に、エコー応答メッセージを応答として送信する。
- 応答を受信しない場合に、エコー要求メッセージを構成された回数だけ GTP-C ピアに再送信します。
- その GTP-C ピアに構成された回数だけ、エコー要求メッセージに対する応答を受信しなかった場合に、GTP-C ピアに関連付けられているすべてのサブスクライバをクリアします。
- その GTP-C ピアから受信したリカバリ値が異なる場合に、その GTP-C ピアに関連付けられているすべてのサブスクライバをクリアします。

この機能は、以下の基準に準拠しています：

- *3GPP TS 29.274*、バージョン *15.8.0*
- *3GPP TS 23.007*

（注） この機能は、レガシー インターフェイスを使用する 4G コールに適用されます。

## コール フロー

次のコール フローは、GTP-C パス管理と GTP-C 復元メッセージの処理方法に固有の情報をキャプチャします。

# GTP-C パス管理

図 *75 : GTP-C* パス管理

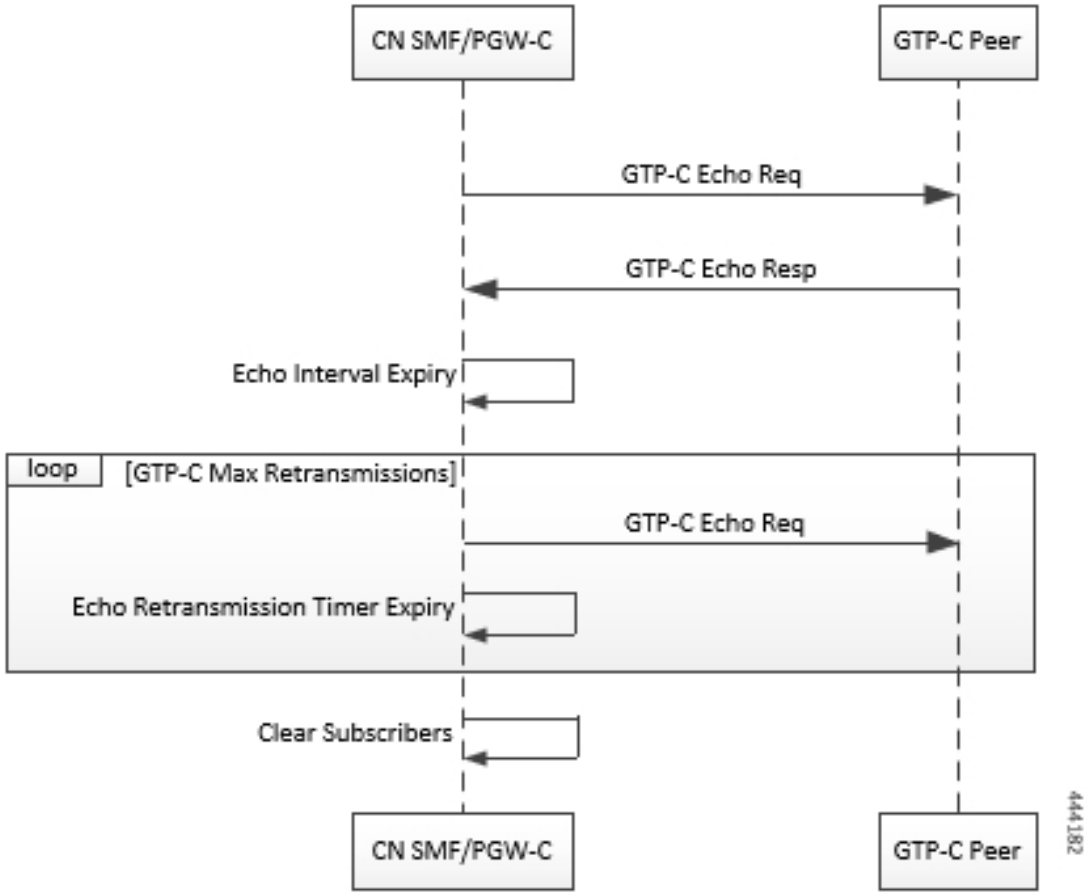



表 *86 : GTP-C* パス管理

| ステップ | 説明 |
|---|---|
| 1 | GTP-C ピアが検出されると（初期 GTP-C 作成セッション要求または GTP-C 変更ベアラー要求メッセージを受信）、CN SMF/PGW-C は、構成に従って、新しい GTP-C ピアへの定期的な GTP-C エコー要求メッセージの送信を開始します。 |
| 2 | GTP-C エコー応答を受信しない場合、CN SMF/PGW-C は、構成された T3 タイマーの期限切れごとに、GTP-C エコー要求（構成済み）を N3 回再試行します。 |
| 3 | すべての再試行が試行されると、CN SMF/PGW-C はその GTP-C ピアに関連付けられているすべてのセッションをクリアします。 |

## GTP-C エコー要求の処理

図 *76 : GTP-C* エコー要求の処理

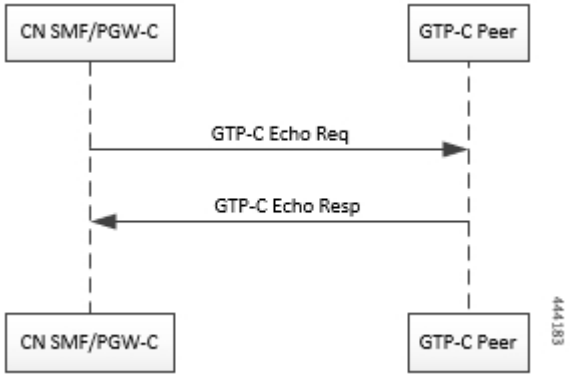



表 *87 : GTP-C* エコー要求の処理

| ステップ | 説明 |
|---|---|
| 1 | GTP-C エコー要求メッセージを GTP-C ピアから受信するたびに、CN SMF/PGW-C は、GTP-C エコー応答メッセージを応答として送信します。 |

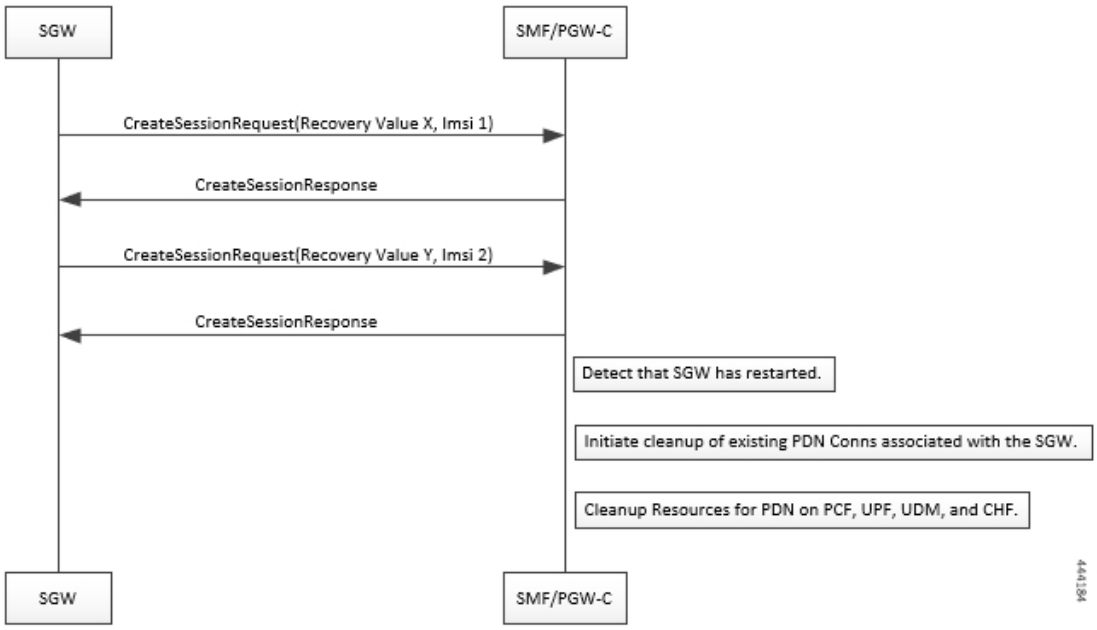
## PGW-C/SMF での GTP-C 復元

PGW-C/SMF は、SGW の回復値に変化があることを検出できます。PGW-C/SMF は、次のメッセージからこの値を検出できます：

- セッション要求の作成
- ベアラー変更要求
- ベアラー作成応答
- エコー応答

PGW-C/SMF が回復値に変更があることを検出した場合、SGW に関連付けられているすべての PDN 接続のクリーンアップを開始します。

図 *77 : SGW* の再起動による *GTP* の復元




# メモリおよびパフォーマンスの影響

Node Manager ポッドから GTP-C ピアへのパス マッピングは、etcd に保持され、NodeMgr および GTP-C ポッドのローカル キャッシュにも保持されます。

# GTP エンド ポイントでのエコーの構成

GTP エンドポイントのエコー パラメータを構成するには、次のサンプル構成を使用します。

```
config
   instance instance-id gr_instance_id
   endpoint gtp
      interface { s2b | s5 | s5e | s8 | s11 }
      echo interval echo_interval
      echo retransmission-timeout retransmission_timeout_value
      echo max-retransmissions max_retry_count
      end
```

## 設定例

```
[unknown] smf# config
Entering configuration mode terminal
[unknown] smf(config)# instance instance-id 1
[unknown] smf(config-instance-id-1)# endpoint gtp
[unknown] smf(config-endpoint-gtp)#
[unknown] smf(config-endpoint-gtp)# interface
s2b s5 s5e s8 s11
[unknown] smf(config-endpoint-gtp)# interface s5
```

```
[unknown] smf(config-interface-s5)# echo interval 60
echo – Enable gtpc path management
interval - Configure echo interval in seconds, ranging from <60-360>
[unknown] smf(config-interface-s5)# echo retransmission-timeout 3
retransmission-timeout - Configure the echo retransmission timeout in seconds, ranging
from <1-20>
[unknown] smf(config-interface-s5)# echo max-retransmissions 10
max-retransmissions  - Configure maximum retries for GTP echo request, ranging from
<0-10>
[unknown] smf(config-interface-s5)#
```

## コマンドの表示

`show peers all` コマンドは、接続されたすべての GTP ピアとそのノード情報を表示します。

**例**：

```
[unknown] smf# show peers all
CONNECTED
ENDPOINT LOCAL ADDRESS PEER ADDRESS DIRECTION POD INSTANCE TYPE TIME RPC ADDITIONAL
DETAILS GR INSTANCE
------------------------------------------------------------------------------------------
S5/S8 209.165.201.15:2123209.165.201.16:2123Inbound smf-nodemgr-1 Udp 4 minutes SGW
Recovery: 100, MaxRemoteRcChange:1 1
```

`show peers all` コマンドは最後の再起動情報を表示するように拡張されています。

**例**：

```
[unknown] smf# show peers all
CONNECTED
ENDPOINT LOCAL ADDRESS PEER ADDRESS DIRECTION POD INSTANCE TYPE TIME RPC ADDITIONAL
DETAILS GR INSTANCE
------------------------------------------------------------------------------------------
S5/S8 209.165.201.15:2123209.165.201.16:2123Inbound smf-nodemgr-1 Udp 4 minutes SGW
Recovery: 100 last-restart-time 1
```

# バルク統計

ピア GTP-C の再起動またはパスの障害が原因でクリアされた PDN 接続には、次の専用の切断理由が使用されます。

- disk_pdnrel_gtpc_peer_restart
- disk_pdnrel_gtpc_peer_pathfail

次のバルク統計が ECS スキーマに追加されました。

```
# HELP nodemgr_gtpc_msg_stats Gtpc Msg Stats
# TYPE nodemgr_gtpc_msg_stats counter
nodemgr_gtpc_msg_stats{app_name="SMF",cluster="Local",data_center="DC",
gtpc_msg_type="gtpc_echo_req_rx",gtpc_peer_ip="209.165.200.239",instance_id="0",service_name="nodemgr"}
 1
nodemgr_gtpc_msg_stats{app_name="SMF",cluster="Local",data_center="DC",
gtpc_msg_type="gtpc_echo_req_tx",gtpc_peer_ip="209.165.200.239",instance_id="0",service_name="nodemgr"}
 4
nodemgr_gtpc_msg_stats{app_name="SMF",cluster="Local",data_center="DC",
gtpc_msg_type="gtpc_echo_res_rx",gtpc_peer_ip="209.165.200.239",instance_id="0",service_name="nodemgr"}
 1
nodemgr_gtpc_msg_stats{app_name="SMF",cluster="Local",data_center="DC",
```

```
gtpc_msg_type="gtpc_echo_res_tx",gtpc_peer_ip="209.165.200.239",instance_id="0",service_name="nodemgr"}
 1
# HELP nodemgr_gtpc_peer_status Gtpc Peer Status
# TYPE nodemgr_gtpc_peer_status counter
nodemgr_gtpc_peer_status{app_name="SMF",cluster="Local",data_center="DC",
gtpc_peer_ip="209.165.200.239",gtpc_peer_status="gtpc_peer_path_down",instance_id="0",service_name="nodemgr"}
 1
nodemgr_gtpc_peer_status{app_name="SMF",cluster="Local",data_center="DC",
gtpc_peer_ip="209.165.200.239",gtpc_peer_status="gtpc_peer_path_up",instance_id="0",service_name="nodemgr"}
 1
nodemgr_gtpc_peer_status{app_name="SMF",cluster="Local",data_center="DC",
gtpc_peer_ip="209.165.200.239",gtpc_peer_status="gtpc_peer_restarted",instance_id="0",service_name="nodemgr"}
 1
```

次のバルク統計情報が GTP-C パス障害拡張機能の一部として追加されています。

```
nodemgr_gtpc_msg_stats{app_name="SMF",cluster="Local",data_center="DC",gtpc_msg_type="
 gtpc_false_peer_restart_ignore_rc_cfg
",gtpc_peer_ip="209.165.200.239",instance_id="0",service_name="smf-nodemgr"} 1
nodemgr_gtpc_msg_stats{app_name="SMF",cluster="Local",data_center="DC",gtpc_msg_type="
gtpc_ignore_echo_timeout "
,gtpc_peer_ip="209.165.200.239",instance_id="0",service_name="smf-nodemgr"} 1
```

次のバルク統計情報が GTP ピア再起動検出機能拡張の一部として追加されています。

```
nodemgr_gtpc_msg_stats{app_name="SMF",cluster="Local",data_center="DC",gtpc_msg_type=
"
gtpc_false_peer_restart_cfg_rc_change",gtpc_peer_ip="209.165.200.239",instance_id="0",service_name="smf-nodemgr"}
 1
# HELP nodemgr_gtpc_peer_status Gtpc Peer Status
# TYPE nodemgr_gtpc_peer_status counter
nodemgr_gtpc_peer_status{app_name="SMF",cluster="Local",data_center="DC",gtpc_peer_ip="209.165.200.239"
,gtpc_peer_status="gtpc_peer_path_down",instance_id="0",service_name="smf-nodemgr"} 1
nodemgr_gtpc_peer_status{app_name="SMF",cluster="Local",data_center="DC",gtpc_peer_ip="209.165.200.239"
,gtpc_peer_status="gtpc_peer_path_up",instance_id="0",service_name="smf-nodemgr"} 1
nodemgr_gtpc_peer_status{app_name="SMF",cluster="Local",data_center="DC",gtpc_peer_ip="209.165.200.239"
,gtpc_peer_status="gtpc_peer_restarted",instance_id="0",service_name="smf-nodemgr"} 1
```

# 制限事項

***3GPP TS 23.007*のセクション 20**： GTPv2 エコー要求は、GTP-C エンティティが、GTP-C パスで以前に送信した要求メッセージに対するGTP応答メッセージを受信していない場合にのみ、実装に依存する時間に送信することが推奨されます。

現時点では、これはサポートされていません。

SMF がピアから GTPC エコー要求を受信した場合でも、パスがアップしていると見なされます。エコー間隔の満了後に、SMF からの後続のエコー要求を受信します。

# GTP-C サービスのモニターとトラブルシューティング

表 *88 :* 機能の履歴

| 機能名 | リリース情報 | 説明 |
|---|---|---|
| GTP-C サービスのトラブルシューティング | 2024.02.0 | この機能により、cnSGW＋SMF＋PGW-C は GTPC テスト エコー コマンドをピア ノードに送信して、次のことを実行できます：<br>• ピア ノードの接続性のトラブルシューティングとモニタリングを行います。<br>• ピアのラウンド トリップ時間（RTT）をテストします。<br>• S11、S5E、S5、S2B、S8 GTPC インターフェイス、IPv4、IPv6 トランスポート タイプをサポートします。<br>**[デフォルト設定（Default Setting）]**：有効 – 常時オン |

## 機能説明

GTP-C テスト エコー CLI コマンド サービスを使用すると、ピア ノードの接続のトラブルシューティングとモニタリングができ、システム動作中のピアのラウンド トリップ時間（RTT）が提供されます。

## GTP-C テスト エコー コマンドの使用

システムは次のテストコマンドを使用して、GTP-C ピア ノードとの接続性を確認します。

**test gtpc echo instance-id** *id* **interface** *interface_type* **peer-address** *ip_address*

**注**：

- **instance-id** *id*：システム上に構成されている GR インスタンスのインスタンス ID を指定します。
- **interface** *interface_type*：s11、s5e、s5、s2b、s8 などの GTP-C インターフェイス タイプを指定します。
- **peer address** *ip_address*：GTP-C エコー要求が送信される特定のピアの IPv4 アドレスまたは IPv6 アドレスを指定します。

次の例では、出力例を示します。

```
Success Case
[sgw] smf# test gtpc echo instance-id 1 interface s11 peer-address 1.1.1.1
 result
{
  "testGtpcEchoResponse": {
    "rx": 1,
    "tx": 1,
    "rtt(ms)": 3,
    "recovery": "10 (0x0A)",
    "status": {
      "success": true
    }
  }
}

Timeout Case:
[sgw] smf# test gtpc echo instance-id 1 interface s5 peer-address 2.2.2.2

Wed Jan  10 13:38:51.415 UTC+00:00
result
{
  "testGtpcEchoResponse": {
    "tx": 4,
    "recovery": "NA",
    "status": {
      "errorMsg": "No Response Received, Timeout"
    }
  }
}
```

# 4G 専用デバイスを拒否するための構成サポート

SMF は、4G 専用 UE デバイスからのコールを拒否するための構成サポートを提供します。

4G 専用 UE デバイスからのコールを拒否するには、次の構成を使用します。

```
config
   profile dnn dnnprofile_name
      only-nr-capable-ue true
      end
```

注：

- **only-nr-capable-ue true**：このコマンドを有効にすると、4G 専用 UE デバイスからの PDN セッション作成の新しいコール試行を拒否できます。

# 変更通知要求の処理

## 機能説明

SMF は、レガシー インターフェイスを使用する 4G コールの ULI を使用した変更通知要求をサポートします。

SMF は、Gx または Gy インターフェイスが有効な場合にのみ、次の要求メッセージを処理できます：

- ULI の変更による変更通知
- ULI の変更がない変更通知

## ULI の変更による変更通知

このセクションでは、変更通知の要求と応答のコール フローについて説明します。

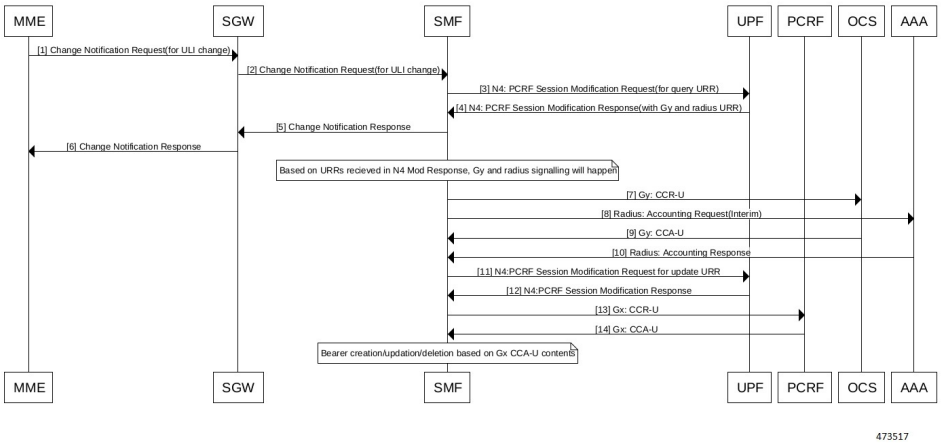



**表 *89* : 変更通知 *ULI* のコール フローの説明**

| ステップ | 説明 |
|---|---|
| 1 | MMEが変更通知要求（ULI変更向け）をSGWに送信します。 |
| 2 | SGW は変更通知要求を SMF に転送します。 |

| ステップ | 説明 |
|---|---|
| 3 | SMF は、用意されたイベントトリガーに基づいて、クエリ URR の N4 セッション変更要求を UPF に送信します。<br>（注）<br>USER_LOCATION_CHANGE イベントは、URI の変更をトリガーします。 |
| 4 | UPF は、Gy と RADIUS の構成（有効/無効）に基づいて、Gy および RADIUS URR SMF を使用した N4 セッション変更応答で応答します。 |
| 5 | SMF は変更通知応答を SGW に送信します。 |
| 6 | SGW は変更通知応答を SGW に送信します。 |
| 7 | N4 変更応答、Gy、および RADIUS シグナリングは、N4 変更応答で受信した URR に基づいて発生します。 |
| 8 | SMF は CCR-U を OCS に、Radius アカウンティング要求を AAA に送信します。 |
| 9 | CCA-U および RADIUS アカウンティング応答付き AAA で応答します。 |
| 10 | SMF は、URR の更新の N4 セッション変更要求を UPF に送信します。 |
| 11 | UPF は SMF に N4 セッション変更応答を送信します。 |
| 12 | イベントトリガーが作動すれば、SMF は PCRF に CCR-U を送信します。<br>（注）<br>USER_LOCATION_CHANGE イベントは、URI の変更をトリガーします。 |
| 13 | 次に、PCRF は CCA-U を SMF に送信します。 |
| 14 | 現在では、Gx CCA-U のコンテンツに基づいてベアラーの作成/更新/削除が行われます。 |

# ULI の変更がない変更通知

このセクションでは、変更通知の要求と、ULI で変更がない応答のコール フローについて説明します。

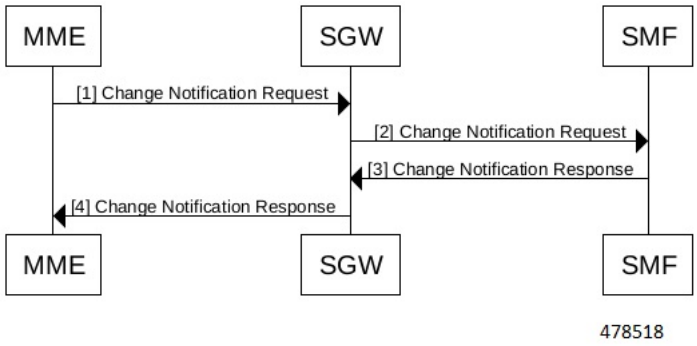



表 *90 : ULI* の変更がない変更通知

| ステップ | 説明 |
|---|---|
| 1 | MME が変更通知要求を SGW に送信します。 |
| 2 | SGW は変更通知要求を SMF に転送します。 |
| 3 | SMF は変更通知応答を SGW に送信します。 |
| 4 | SGW は変更通知応答を SGW に送信します。 |

# コール フロー

ここでは、この機能の主要なコール フローについて説明します。

• ULI の変更による変更通知 （325 ページ）
• ULI の変更がない変更通知 （327 ページ）

## ULI の変更による変更通知

このセクションでは、変更通知の要求と応答のコール フローについて説明します。

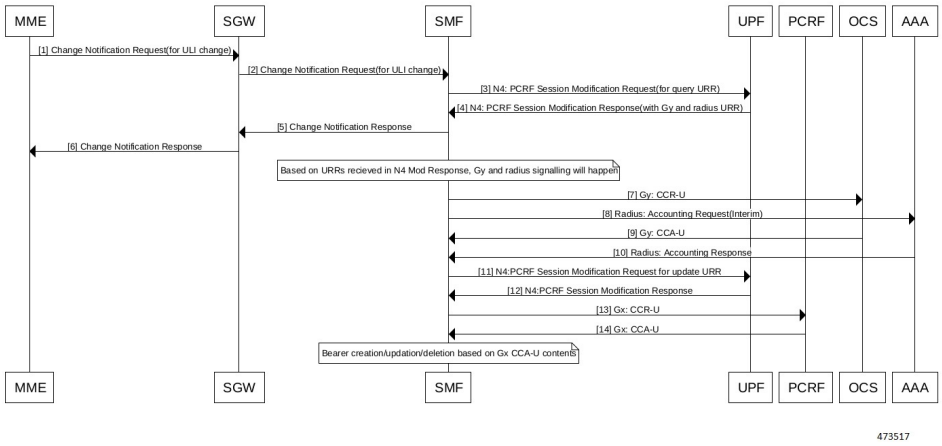



表 *91 :* 変更通知 *ULI* のコール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | MME が変更通知要求（ULI 変更向け）を SGW に送信します。 |
| 2 | SGW は変更通知要求を SMF に転送します。 |
| 3 | SMF は、用意されたイベント トリガーに基づいて、クエリ URR の N4 セッション変更要求を UPF に送信します。<br>（注）<br>USER_LOCATION_CHANGE イベントは、URI の変更をトリガーします。 |
| 4 | UPF は、Gy と RADIUS の構成（有効/無効）に基づいて、Gy および RADIUS URR SMF を使用した N4 セッション変更応答で応答します。 |
| 5 | SMF は変更通知応答を SGW に送信します。 |
| 6 | SGW は変更通知応答を SGW に送信します。 |
| 7 | N4 変更応答、Gy、および RADIUS シグナリングは、N4 変更応答で受信した URR に基づいて発生します。 |
| 8 | SMF は CCR-U を OCS に、Radius アカウンティング要求を AAA に送信します。 |
| 9 | CCA-U および RADIUS アカウンティング応答付き AAA で応答します。 |

| ステップ | 説明 |
|---|---|
| 10 | SMF は、URR の更新の N4 セッション変更要求を UPF に送信します。 |
| 11 | UPF は SMF に N4 セッション変更応答を送信します。 |
| 12 | イベントトリガーが作動すれば、SMF は PCRF に CCR-U を送信します。<br>（注）<br>USER_LOCATION_CHANGE イベントは、URI の変更をトリガーします。 |
| 13 | 次に、PCRF は CCA-U を SMF に送信します。 |
| 14 | 現在では、Gx CCA-U のコンテンツに基づいてベアラーの作成/更新/削除が行われます。 |

## ULI の変更がない変更通知

このセクションでは、変更通知の要求と、ULI で変更がない応答のコールフローについて説明します。

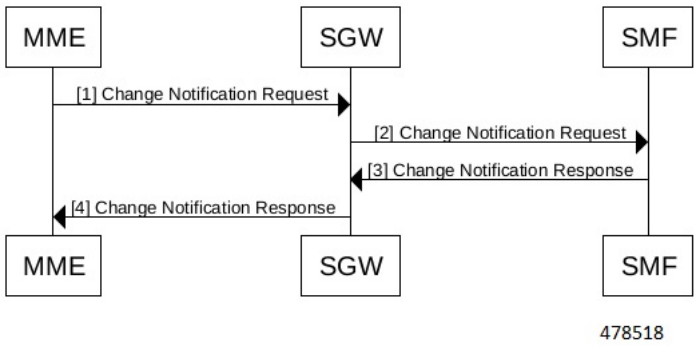



表 *92 : ULI* の変更がない変更通知

| ステップ | 説明 |
|---|---|
| 1 | MME が変更通知要求を SGW に送信します。 |
| 2 | SGW は変更通知要求を SMF に転送します。 |
| 3 | SMF は変更通知応答を SGW に送信します。 |
| 4 | SGW は変更通知応答を SGW に送信します。 |

# ダイナミックな構成変更のサポート

## 機能説明

SMF を使用すると、既存のセッションに影響を与えずに、アクセス プロファイル構成をダイナミックに変更できます。たとえば、構成が動的に更新される場合、現在のセッションは進行中のコール フローまたは手順で古い値を使用し続けます。

## 機能の仕組み

このセクションでは、サポートされているアクセスプロファイル構成で構成の動的な変更がどのように機能するかについて説明します。

### アクセスプロファイル

アクセスプロファイルは、アクセスプロファイル構成のさまざまなパラメータを定義します。

次の表に、ダイナミックな更新が許可される構成を示します。

**表 *93 :* プロファイル パラメータへのアクセス**

| 設定パラメータ | 設定（Configuration） | ダイナミックな変更 | 既存のセッションへの影響 |
|---|---|---|---|
| eps-fallback cbr | **eps-fallback cbr delay** *delay* **max-retry** *retry_count* **timeout** *timeout* | 許可 | コール フローおよび手順で古い値を使用しているセッションでは、引き続き古い値が使用されます。 |
| n1 t3591-pdu-mod-cmd | **n1 t3591-pdu-mod-cmd timeout** *timeout* **max-retry** *retry_count* | 許可 | コール フローおよび手順で古い値を使用しているセッションでは、引き続き古い値が使用されます。 |

| 設定パラメータ | 設定（Configuration） | ダイナミックな変更 | 既存のセッションへの影響 |
|---|---|---|---|
| n1 t3592-pdu-rel-cmd | **n1 t3592-pdu-rel-cmd timeout** *timeout* **max-retry** *retry_count* | 許可 | コール フローおよび手順で古い値を使用しているセッションでは、引き続き古い値が使用されます。<br>（注）<br>SMF は、この構成に関連付けられているタイマー機能をサポートしていません。 |
| n2 idft enable | **n2 idft enable timeout** *timeout* | 許可 | コール フローおよび手順で古い値を使用しているセッションでは、引き続き古い値が使用されます。 |
| n26 idft enable | **n26 idft enable timeout** *timeout* | 許可 | コール フローおよび手順で古い値を使用しているセッションでは、引き続き古い値が使用されます。 |
| n11 n11-failure-profile | **n11 n11-failure-profile** *failure_profile* | 許可 | コール フローおよび手順で古い値を使用しているセッションでは、引き続き古い値が使用されます。<br>関連付けられた Failure-Handling Profile が削除されるか、またはいずれかのパラメータが変更されても、既存のコール フローは影響を受けません。つまり、既存のコール フローでは古い値が引き続き使用されます。 |

| 設定パラメータ | 設定（Configuration） | ダイナミックな変更 | 既存のセッションへの影響 |
|---|---|---|---|
| gtpc<br>gtpc-failure-profile | **gtpc gtpc-failure-profile** *failure_profile* | 許可 | コール フローおよび手順で古い値を使用しているセッションでは、引き続き古い値が使用されます。<br>関連付けられた Failure-Handling Profile が削除されるか、またはいずれかのパラメータが変更されても、既存のコール フローは影響を受けません。つまり、既存のコール フローでは古い値が引き続き使用されます。 |

# 4G および 5G のセマンティックおよび構文エラー処理

表 *94 :* 機能の履歴

| 機能名 | リリース情報 | 説明 |
|---|---|---|
| 4G および 5G の MBFR、セマンティックおよび構文エラー処理 | 2023.04 | SMF は QFI、QoS の MBFR、セマンティックおよび構文エラーを処理し、5GSM の原因を示します。イベント名、ルール、アクションを使用する構成には、4G および 5G エラーのものが含まれています。<br>**デフォルト設定** 無効：有効にするには構成が必要です。 |

## 機能説明

SMF は QoS ルールと QoS の説明、またはマッピングされた EPS ベアラー コンテキストの構文および構文エラーを UE から受信します。

### UE が 5G RAT にあるときにエラーを受信しました

- SMF は次の 5G エラーを受信します：
  - QoS 動作で構文エラーが発生しました
  - QoS 動作の構文エラー
  - マッピングされた EPS ベアラー ID が無効です

  構成に適用可能なアクションは次のとおりです：
  - release-session
  - release-flow
- SMF は次の 4G エラーを受信します：
  - パケット フィルタの構文エラー
  - パケット フィルタの構文エラー
  - TFT 操作の構文エラー
  - TFT 操作での構文エラー

  構成に適用可能なアクションは次のとおりです：
  - release-session
  - release-flow：リリース ベアラーとも見なされます
  - release-session-ho：SMF は 5G のフローを保持し、5G から 4G の HO 中にリリースします。5G から WIFI HO への影響はありません。

### UEが4G RATにあるときにエラーを受信しました

- SMF は次の 4G エラーを受信します：
  - パケット フィルタの構文エラー
  - パケット フィルタの構文エラー
  - TFT 操作の構文エラー
  - TFT 操作での構文エラー

  構成に適用可能なアクションは次のとおりです：
  - release-session
  - release-flow：リリース ベアラーとも見なされます
- SMF は次の 5G エラーを受信します：

- QoS 動作で構文エラーが発生しました
- QoS 動作の構文エラー
- マッピングされた EPS ベアラー ID が無効です
- パケット フィルタの構文エラー
- パケット フィルタの構文エラー

構成に適用可能なアクションは次のとおりです：

- release-session
- release-flow
- release-session-ho：SMF は 4G のフローを保持し、4G から 5G の HO 中にリリースします。4G から WIFI HO への影響はありません。

# 原因の処理

SMF では、UE によって開始された手順とネットワークによって開始された手順の 4G および 5G セッション管理（5GSM）の原因処理をサポートしています。

### 5G の N1 原因処理

サポートされている手順は次のとおりです：

- PDU セッション変更拒否
- PDU セッション変更要求

### PDU セッション変更拒否

N1 PDU セッション変更拒否では、SMF はフローの作成または変更を失敗と見なし、手順を中止します。障害通知は PCF に送信されます。

この原因に対して、`pdu-modify` 統計が追加されます。

### PDU セッション変更要求

SMF は、適切な EBI と **Delete existing EPS bearer** を示す操作コードを使用して、マップされた EPS ベアラー コンテキストを使用して N1 PDU セッション変更要求を処理します。実行されるアクションの構成は、このシナリオに対応します。

### 4G の構文および構文エラー処理

### CB 応答と UB 応答

SMF は、5GSM の原因を含む ePCO とともに CB または UB 応答を処理します。

異なるアクションは、 actiondef の構成値に基づいて発生します。

SMF は、MME からの CB 応答と UB 応答をサポートしています。以下は、MME/UE 原因評価の順序です。

1. セッション レベル
2. ベアラー レベル
3. ePCO レベル

デフォルトのベアラー アクションでは、ベアラーのリリースはサポートされていません。

（注） SMF は緊急セッションのこれらすべての原因をサポートします。

### GBR QoS フローの MFBR パラメータ

MFBR（最大フロー ビット レート）検証は、PCF から GBR フロー作成または QoS 変更を受信した場合に追加されます。

フローが GBR QoS フローの場合は、必須パラメータとして MFBR アップリンクまたは MFBR ダウンリンクを追加します。以下は検証の条件です。

- MFBR UL（アップリンク）または MFBR DL（ダウンリンク）のいずれかがゼロ以外である必要があります
- GFBR UL は MFBR UL 以下である必要があります
- GFBR DL は MFBR DL 以下にする必要があります

コール フローからの検証メソッドは次のとおりです。

- PCF からルールを受信している間に、SMF が SMF（ホーム）および SMF（ローミング）として機能する場合の条件を検証します。
- フローを SMF（ビジター）の hSMF（ローミング）から受信したときの状態に関して、N16 QoS フローを検証します。

# セマティックおよび構文エラー処理の構成

### イベント管理ポリシーを追加するための構成

イベント管理ポリシーの追加は、次の構成によって行われます。

```
config
  policy eventmgmt policy_eventmgmt_name
    priority  event_priority [ event event_name ] ruledef ruledef_name actiondef
 actiondef_name
     exit
```

注：

- **eventmgmt** *policy_eventmgmt_name*：この CLI では、イベント管理ポリシーを構成し、属性を定義できます。
- **priority** *event_priority*：特定のイベント管理ポリシーの優先順位を定義できます。
- **event** *event_name*：特定のアクションが実行されるイベントを定義するオプションの CLI です。次のイベント名がサポートされています。

  **表 *95*：構文および構文エラー処理のイベント**

| イベント | 説明 |
|---|---|
| n1-modify | N1 変更要求/応答 |
| cb-resp | ベアラー応答の作成 |
| ub-resp | ベアラー応答の更新 |

  **event** が構成されていない場合、ルールが一致すると、すべての定義済みイベントに対して **actiondef** が実行されます。
- **ruledef** *ruledef_name*：一致した場合にアクションを実行するローカル ポリシーのルールを定義します。
- **actiondef** *actiondef_name*：実行されるアクション名を構成します。

### ルール定義ポリシーを追加するための構成

次の構成では、ルール定義ポリシーを追加できます：

```
config
  policy rulemgmt policy_rulemgmt_name
    ruledef rule_def condition cause cause_string source source_value
    exit
```

- **rulemgmt** *policy_rulemgmt_name*：ポリシーに追加するルールを定義します。
- **ruledef** *rule_def*：ルール属性を構成します。ruledef は、条件が一致したときに宣言されます。
- conditioncondition_string：ルールの使用例を定義します。

  **Cause** *cause_string* ：必須のソース値とともに **cause-value matches** 条件をサポートします。
- **source** *source_value* ：ルールの送信元を定義します。

  **ue**、**ran**、 **mme**、および **amf** は、使用可能な送信元の値です。

### アクション定義ポリシーを追加するための構成

次の構成では、アクション定義ポリシーを追加します：

```
config
  policy actionmgmt policy_actionmgmt_name
    actiondef actiondef_name
      priority priority_number action action_name [ attributes { rulebase
rulebase_name [ rules rules_name ] } ]
      exit
```

注：

- **actionmgmt** *policy_actionmgmt_name*：実行されるアクションを構成します。
- **actiondef** *actiondef_name*：実行されるアクション属性を定義します。

  UE が 4G または 5G RAT にある場合、アクションは異なります。
- **priority** *priority_number*：アクションが実行される優先順位を定義します。
- **action** *action_name*：actiondefに関連付けられたアクションを優先順に定義します。ここでは、次のアクション名が使用されます。
  - release-session
  - release-flow
  - release-flow-ho
- **attributes** ：特定のアクションの属性を定義します。これは任意のコマンドです。
- **rulebase** *rulebase_name*：フローと一致させるプロトコルルールのコレクションと、フローと一致するために実行する関連アクションを定義します。
- **rules** *rules_name*：実行されるルールのリストを定義します。

# 設定例

例 1：次に、イベント管理構成に **n1-modify** イベント名を使用した構成例を示します：

```
policy eventmgmt evt1
priority 1 event n1-modify ruledef rd1 actiondef ad1
```

例 2： **cause-source matches** ルール定義ポリシーを追加するための構成例を次に示します：

```
policy rulemgmt rm1
ruledef rd1
condition cause matches [ 83 ] source ue
```

例 3：次に、エラー処理アクション定義ポリシーを追加するための構成例を示します

```
policy actionmgmt am1
actiondef ad1
priority 1 action release-session
priority 2 action release-flow
exit
actiondef ad2
priority 1 action release-flow
exit
actiondef ad3
priority 100 action release-flow-ho
```

# バルク統計サポート

1. 以下は、4G の原因エラーを伴う CB 応答または UB 応答処理の統計です。

   - `disk_admin_event_mgmt` ：セッション リリース アクションの切断理由。

     次に例を示します。

     ```
     smf_disconnect_stats
     {app_name="SMF",cluster="SMF",data_center="DC",gr_instance_id="1",instance_id="1",rat_type="EUTRA",
     reason="disc_admin_event_mgmt",roaming_status="homer",service_name="smf-service",severity="normal",snssai=""}
      11
     ```

   - `create_bearer_resp` ：リリース ベアラーまたはリリース ベアラー HO アクションのそれぞれの原因とアクションを含むメッセージ タイプ。

     次に例を示します。

     ```
     smf_gtpc_msg_stats
     {app_name="SMF",cluster="SMF",data_center="DC",dnn="",gr_instance_id="1",
     instance_id="0",message_type="create_bearer_resp",qos_5qi="",rat_type="EUTRA",reason="76_mme_release_flow",
     service_name="smf-service",smf_current_procedure="pcf_req_ded_brr_create",snssai="",status="failures"}
      1
     ```

2. 次に、4G および 5G でエラーを引き起こす N1 PDU セッション変更拒否または N1 PDU セッション変更要求を処理するための統計を示します。

```
smf_service_stats :

Cause = updated with the cause received in “N1 PDU Session Modification Command Reject”
 or “N1 PDU Session Modification Request”

Detailed_Cause = updated with the Source of cause
procedure_type = updated with "ue_req_pdu_sess_mod” or “pcf_req_pdu_sess_mod”
reason  =  Updated with "Cause"_"Detailed_Cause"_"Action"
```

その他の例を次に示します。

```
smf_service_stats{Cause="84",Detailed_Cause="ue",always_on="",app_name="SMF",
cluster="SMF",data_center="DC",dcnr="",dnn="",emergency_call="false",fourg_only_ue="",
gr_instance_id="1",gtpc_bypass="",idle_mode="",instance_id="1",local_policy="",pdu_type="ipv4",
policy_type="",pra="",procedure_type="ue_req_pdu_sess_mod",qos_5qi="",rat_type="NR",
reason="84_ue_release_flow",roaming_status="homer",
service_name="smf-service",smf_current_procedure="",snssai="",status="success",
up_state="UpState_Activated",upip_active=""}

smf_service_stats{Cause="85",Detailed_Cause="ue",always_on="",app_name="SMF",
cluster="SMF",data_center="DC",dcnr="",dnn="",
emergency_call="false",fourg_only_ue="",
gr_instance_id="1",gtpc_bypass="",idle_mode="",instance_id="1",local_policy="",pdu_type="ipv4",
policy_type="",pra="",procedure_type="pdu_session_modification_command_reject",qos_5qi="",
rat_type="NR",reason="85_ue_release_flow_Ho",
roaming_status="homer",service_name="smf-service",
smf_current_procedure="pcf_req_pdu_sess_mod",snssai="",status="failures",
up_state="UpState_Activated",upip_active=""}
```

第 14 章

# イベント詳細レコード


- 機能の概要と変更履歴 （339 ページ）
- 機能説明 （340 ページ）
- EDR の構成 （402 ページ）
- EDR ロギングの OAM サポート （408 ページ）


## 機能の概要と変更履歴

### 要約データ

表 *96 :* 要約データ

| | |
|---|---|
| 該当製品または機能エリア | SMF |
| 該当するプラットフォーム | SMI |
| 機能のデフォルト設定 | 無効：設定が必要 |
| このリリースでの関連する変更点 | N/A |
| 関連資料 | 該当なし |

# 更新履歴

表 *97:* マニュアルの変更履歴

| 改訂の詳細 | リリース |
|---|---|
| 次の拡張機能のサポートが導入されています：<br>• 専用ベアラーとハンドオーバー（pathswitchreq（Xn handover）、pdun2ho、pdn5g4gHo、nrtountrustwifiho、pdun26ho、utn3gppto5g）の EDR 生成<br>• EDR モニターポッドでの EDR ファイルのアーカイブ<br>• 新しいコマンドへ<br>  • すべてのサブスクライバの EDR の有効化<br>  • トランザクション EDR レート、CPU しきい値、セッションしきい値、およびファイル アーカイブ ポリシーを構成する | 2022.04.0 |
| ローミングおよび非ローミング シナリオの PDU セッション変更手順に対する EDR サポートの導入 | 2021.02.2 |
| イベント レベルの EDR 生成のサポート | 2021.02.0 |
| カスタム EDR 生成 | 2021.01.0 |

# 機能説明

イベント データ レコード（EDR）は、次の機能を実行するために使用できる情報を収集します。

- アプリケーションの動作をデバッグまたは把握する
- 特定のサブスクライバのコール フローの診断

SMF は 、非ローミングおよびローミングセッションを含む4G と 5G の両方のサブスクライバセッションの EDR のロギングをサポートしています。EDR サポート機能が有効になっている場合、ローミング シナリオでは、hSMF および vSMF は PDU セッションの確立およびリリースの手順のために EDR を生成します。SMF は、コンマ区切り値（CSV）形式の EDR ファイルを生成します。SMF は 1 行に 1 つの CSV レコードを保存します。CSV ファイルは、外部サーバに送信する前に任意で圧縮できます。

SMF では、要求メッセージと応答メッセージが 1 つの EDR イベント レコードとして扱われます。たとえば、N11SmContextCreateReq 属性と N11SmContextCreateResp 属性は EDR イベントとしてログに記録されます。

SMF では、サブスクライバ セッションのトランザクションおよびトランザクション コリジョン レベルの詳細に関する EDR ファイルの生成がサポートされています。デフォルトでは、EDR の生成は無効になっています。

リリース 2021.02.0 では、SMF は手順レベルの詳細、イベントレベルの詳細、およびフィールド レベルの詳細を含む EDR を生成します。これらの詳細は、エラーや問題のデバッグに役立ちます。

### EDR 形式

アプリケーションは、既存の トランザクション EDR フィールドに加えて、procedure-id と event-id をそれぞれのフィールド値とともに追加します。アプリケーションは、procedure-id、event-id、および field-id を対応する名前とともに登録します。このマッピングは、EDR の CSV イベント エントリのフォーマットに使用されます。各イベント エントリは、コンマ区切りのプロシージャ ID、イベント ID、およびフィールド値で構成されます。これらの登録済みマッピングを CLI コマンドで使用して、手順、イベント、またはフィールド レベルで EDR を無効にすることもできます。EDR は、実行時に動的に有効または無効にできます。既存の EDR レコードは同じままで、ランタイムの変更は新しく生成された EDR レコードにのみ反映されます。

#### トランザクション EDR 形式

Transaction-EDR-Fields、list of event-entries [ ]

#### イベント エントリ

Procedure-id1、Event-id1、list of field-id1-values [ ]

次に、CSV 形式のイベント リストとともにトランザクション エントリの例を示します。

```
Version, Field-Count, Transaction-id-value, Start-Time, Elapsed-Time, ……,
Procedure-id1, event-id1, field-id1-value, field-id2-value……,
Procedure-id1, event-id2, field-id1-value, field-id2-value……,
Procedure-id1, event-id3, field-id1-value, field-id2-value……
```

（注） 手順 ID とイベント ID の組み合わせに対して、異なるフィールド セットが存在する場合があります。 CLI コマンドを使用して、実行時に EDR を動的に有効または無効にできます。構成の詳細は、このガイドの EDR ファイルの生成の構成 （403 ページ） セクションを参照してください。

### EDR ファイル ストレージ

このセクションでは、SMF サービス ポッドおよび EDR モニタ ポッド内の EDR ファイルのアーカイブの場所について詳しく説明します。

#### SMF サービス ポッドの EDR ファイル

EDR ファイルは、サブスクライバセッションとイベントが処理される各 SMF サービス ポッドで生成されます。EDR ファイルのサイズに基づいて、ファイルは非永続ボリューム、つまり SMF サービス ポッドに定期的にアーカイブされます。既存のファイルをアーカイブする前に、新しいファイルが作成されます。

トランザクション EDR ファイル名およびトランザクション コリジョン EDR ファイル名の形式は次のとおりです。

*<pod-name>_<pod_instance>_<PodStartTime>.transaction.csv*

*<pod-name>_<pod_instance>_<PodStartTime>.transaction_collision.csv*

サービス ポッドのディレクトリ パスは、`/tmp/edr/`です。

**例**：

*smf-service-n0-0_0_ 20220730233455.transaction.csv*

ポッド名は smf-service-n0-0、ポッド インスタンスは 0、ポッド開始時刻「20220730181014」は、2022 年 7 月 30 日（UTC）の 18 時 10 分 14 秒（UTC）を意味します。

圧縮ファイル名の形式は次のとおりです。

*<pod-name>_<pod_instance>_<PodStartTime>.transaction.csv.<fileArchivedTime>.<FileRotationCounter>.gz*

**例**：

*example-service-n0-0_1_20220730181014.transaction.csv.20220730181844.1.gz*

**EDR モニタ ポッドの EDR ファイル**

SMF サービス ポッドは、30 秒ごとにすべての EDR ファイルを edr-monitor ポッドに送信します。EDR ファイルは、edr-monitor ポッドの永続的なディレクトリに .csv ファイルとして残ります。すべてのファイルの合計サイズが構成されている最大ファイル サイズを超えると、最も古いファイルが削除されます。

edr-monitor ポッドのファイル名の形式は *<pod-name>_<pod_instance>_<PodStartTime>.transaction.csv* です。

**例**：

*edr-monitor pod-n0-0_0_ 20220730233455.transaction.csv*

edr-monitor ポッドのディレクトリ パスは `/logs/edr/`です。

EDR ファイルのサイズ、アーカイブされる EDR ファイルの最大数、および永続的なボリュームの最大サイズは、CLI コマンドを使用して構成します。構成コマンドに関する詳細は、「EDR パラメータの構成 （404 ページ）」セクションを参照してください。

EDR モニタ ポッドの永続ボリューム内のファイルにアクセスするには、必要なログイン情報で Ops センターにログオンし、edr-monitor ポッドの入力 URL を使用します。

入力 URL を決定するには、次のコマンドを使用します：

**kubectl get ingress -n** *namespace* **| grep edr**

**例**：

*cloud-user@svi-cndp-tb41-gr-setup-smf-cluster-2-cndp-server-1:~$* **kubectl get ingress -n smf-smf | grep edr**

edr-archives-smf-smf nginx **edr-archives.smf-smf.172.18.128.82.nip.io** 10.109.13.65 80, 443 4d5h

# EDR トランザクション ファイル

EDR トランザクション ファイルは、トランザクションの最後にトランザクション情報をダンプします。デフォルトでは、ファイルの生成は無効になっています。

次の表に、ファイルに保存される情報を示します。

**表 *98 : EDR* トランザクション ファイル フィールド**

| フィールド番号 | フィールド名 | フィールドの説明 |
|---|---|---|
| 1 | Version | EDR バージョン番号。デフォルト値は v1 です。<br>（注）<br>バージョンが変更されるのは、トランザクション ヘッダー フィールドのエンコード順序または各フィールドのエンコード手順が変更された場合のみです。 |
| 2 | フィールド数 | トランザクション EDR ヘッダーのフィールドの合計数。デフォルト値は 15 です。 |
| 3 | Transaction ID | Transaction ID |
| 4 | 開始時刻 | yyyyy/MM/dd HH:mm:ss.SSS 形式のトランザクション開始時刻。 |
| 5 | 経過時間（ミリ秒） | トランザクションの終了にかかった時間（ミリ秒単位）。 |
| 6 | サブスクライバ ID | サブスクライバ ID 例えば、imsi-123456789012345 |
| 7 | トランザクションタイプ | アプリケーションに内部的に定義されているトランザクション タイプ（整数）。 |
| 8 | トランザクションの説明 | 文字列形式のトランザクションの説明。 |
| 9 | セッション プライマリ キー（Session Primary Key） | セッションのプライマリ キー。 |

| フィールド番号 | フィールド名 | フィールドの説明 |
|---|---|---|
| 10 | セッション固有のキー | \| で区切られたセッションの一意のキー。 |
| 11 | セッションの固有でないキー | \| で区切られたセッションの固有でないキー。 |
| 12 | ステータス | トランザクションのステータス（成功またはエラー）。 |
| 13 | 状態コード | 失敗の理由を示すトランザクション ステータス コード。 |
| 14 | 手順名 | トランザクションが送信される手順名。 |
| 15 | サブ プロシージャ名 | トランザクションが送信されるサブ手順の名前。 |
| 16 | 状態 | トランザクション状態次のいずれかになります。<br>• 開始済み<br>• 新規作成（New）<br>• 待受中<br>• アクティブ<br>• 保留中<br>• 一時停止<br>• 応答の保留を中断する（SuspendWaitingFor Response）<br>• ロックの保留中保留（SuspendWaitingForLock）<br>• Abort<br>• 完了<br>• タイムアウト（Timeout）<br>• 不明 |
| 17 | 実行段階 | \| で区切られた、トランザクションのライフサイクルにおけるステージのリスト |

注：

- 各フィールドはカンマ（,）で区切られます。
- フィールド session_uks、session_nuks、execution_stages はリストです。フィールドはパイプ（|）で区切ります。たとえば、session_uks は uk1|uk2|uk3 と表記されます。

**CSV フォーマット例**：

```
V1,15,1,2022/08/03
2:12:19.48,29,insi-234567890123451,S5S8CreateSessReq,insi-234567890123451,insi-234567890123451:12.0.0.1|intershat:12.0.0.1|insi-234567890123451:201:db0::|intershat:201:db0::|1|insi-234567890123451:db0:5|insi-234567890123451:intershat,carrierstatushome|type1-apn|spi:insi-234567890123451|gpsi:msisdn-233101010101|pei:imei-234567866666601|psi:5|ssmi:02:bf:23|dnn:intershat|emergency:false|atwan|accesstrusted non-3gpp access|
creativity:4|duration:1296|dash:1296|ratstatus:unauthenticated|ofcqi:PCF-policy2|pcf:10.12.96.6|pcf:198.18.1.3|pfcp:198.18.1.3|198.18.1.4|ipv4addrpool4:2.0.0.1|ipv6prefixpool4:ipv4range:pool4:2.0.0.1|ipv4startrangepool4:2.0.0.1|ipv6prefixpool6:2001:db0::|ipv6prefixpool6:ipv6rangepool6:2001:db0::|ipv6startrangepool6:2001:db0::|chrisk:10.12.96|value01|cfgqciPCFdnn:intershat;pcf:10.12.96|peer:198.18.1.10|
peerGtpuEpKey:198.18.1.3:198.17.1.6,success,success,PDN Connect
[LTE],S5S8CreateSessReq,Active,init_done|4G SETUP: Idle|4G SETUP: Await UDM Registration|4G SETUP: Await UDM Subscription Fetch|4G SETUP: Await UDM Subscribe for Notification|
4G SETUP: Await PCF Create|4G SETUP: Await Address Allocation|4G SETUP: Await PCF Update|4G SETUP: Await Charging
Create|finished,3,1313,V2,4,Success,201,3,,3,1316,V2,4,Success,200,3,,3,1319,V2,4,Success,201,3,,3,3329,V2,9,imsi-123456789012345,
imei-123456786666660,msisdn-223310101010101,Success,201,3,||3|1;2;2|3000 mbps|4000
mbps|1000 mbps|2000 mbps,200000 kbps|400000
kbps,,3,3332,V2,4,Success,204,3,,3,1003,V2,4,Success,201,3,,3,524,V2,4,Success,,3,Request_Accepted,3,2051,V2,18,
insi-123456789012345,imei-123456866666,123456789012345,233101010101,msisdn-233101010101,Success,,ARC||||||2;Abf123;;|||1;1|1;0|0|,3,1,intershat,,||5|0;0;15||||,200
 mbps|400 mbps,16,12.0.0.1|2001:db0::b46d:47ff:fe47:4747,2|Abf123||,
WAN,3,1000,V2,4,insi-123456789012345,imei-123456866666,123456789012345,233101010101,msisdn-233101010101,123|456,Extra|Rgci:123;456;123456|Tai:123;456;180,2022-08-03
 22:12:19.485844223 +0000 UTC,2022-08-03 22:12:19.772243364
+0000
UTC,Ue,,198.18.1.100,Succes,3,,intershat,WAN,+00:15+1,3,123|456,10000000,12500000,5,1|1|15,12.0.0.1|2001:db0::b46d:47ff:fe47:4747,46111543,67559941059321,1,5,,2,2|Abf123||,16,1,NR
 Capable UE,1580,198.17.1.6,6168582,198.17.1.3,intershat
```

# 手順レベルの EDR 生成

イベントロギング機能は、サブスクライバごとに手順レベルの情報をキャプチャします。手順が正常に完了したとき、または失敗したときに、SMF は手順とイベントの詳細を含むイベントデータ レコードを生成します。

手順ごとの EDR 生成は構成可能です。構成の詳細は、このガイドの EDR ファイルの生成の構成 （403 ページ） セクションを参照してください。

次の表に、サポートされている手順と対応する ID を示します。

**表 *99 :* 手順リスト**

| 手順 | Procedure-ID |
|---|---|
| PDN-SESSION-CREATE または PDU-SESSION-CREATE | 3 |
| PDN-SESSION-DELETEまたはPDU-SESSION-DELETE | 4 |
| PDU-SESSION-MODIFY | 5 |
| DEDICATEDBEARER | 6 |
| ハンドオーバー | 7 |

（注） 手順 ID は、ローミングと非ローミングの両方の手順で同じままです。

さらに、SMF は手順ごとにイベントレベルの情報をキャプチャします。次の表に、サブスクライバ イベントとそれぞれのイベント ID の詳細を示します。

手順ごとにキャプチャされるイベントは設定可能です。構成の詳細は、このガイドのEDR ファイルの生成の構成 （403 ページ） セクションを参照してください。

**表 *100 :* イベント *ID***

| EVENT | EVENT-ID | 手順に対するイベントの適用性 | | | |
|---|---|---|---|---|---|
| | | 作成 | リリース | 修正 | 専用ベラー |
| N11SmContext CreateReq | 1287 | ○ | — | — | — |
| N11SmContext UpdateReq | 1290 | はい | はい | はい | — |
| N11N1N2Message TransferReq | 1299 | はい | はい | はい | — |
| N11SmContext UpdateModifyReq | 1293 | — | — | — | — |
| N11Ebi AssignmentReq | 1302 | ○ | — | ○ | — |
| N11SmContext ReleaseReq | 1304 | — | ○ | — | — |
| N11SmContext StatusNotifyReq | 1310 | はい | はい | — | — |
| N11N1N2Message TransferFail NotificationReq | 1339 | — | はい | はい | — |
| N4Session ModificationReq | 527 | はい | はい | はい | はい |
| N4Session ReleaseReq | 530 | はい | はい | — | — |
| N4Session EstablishmentReq | 524 | ○ | — | — | — |
| N7SmPolicy CreateReq | 3329 | ○ | — | — | — |
| N7SmPolicy DeleteReq | 3335 | はい | はい | — | — |
| N7SmPolicy UpdateReq | 3332 | ○ | — | はい | はい |
| N7SmPolicy TerminateNotify Req | 3341 | — | ○ | — | — |
| N7SmPolicy UpdateNotifyReq | 3338 | — | — | はい | はい |
| N10UnsubscribeFor NotificationReq | 1432 | — | ○ | — | — |
| N10SubscribeFor NotificationReq | 1319 | ○ | — | — | — |
| N10Registration Request | 1313 | ○ | — | — | — |

| | | | | | |
|---|---|---|---|---|---|
| N10Subscription FetchReq | 1316 | ○ | — | — | — |
| N10Deregistration Request | 1325 | はい | はい | — | — |
| S5S8Delete BearerCmd | 2066 | — | — | — | はい |
| N10Update NotifyReq | 1322 | — | はい | はい | — |
| N40ChargingDataCreateReq | 1003 | ○ | — | — | — |
| N40Charging DataUpdateReq | 1004 | — | — | ○ | — |
| N40Charging DataReleaseReq | 1005 | — | ○ | — | |
| N40Charging NotificationReq | 3588 | ○ | — | ○ | — |
| Secondary AuthenReq | 2307 | ○ | — | — | — |
| S5S8Create SessReq | 2051 | ○ | — | — | — |
| S5S8Delete BearerReq | 2057 | — | ○ | — | はい |
| S5S8Delete SessReq | 2055 | — | ○ | — | |
| RadiusCoa DisconnectReq | 2313 | — | ○ | — | — |
| RadiusAcctReq | 2309 | はい | はい | はい | — |
| metaData | 1000 | はい | はい | はい | はい |
| N16PduSession CreateReq | 1444 | ○ | — | — | — |
| N16VsmfPdu SessionRelease Req | 1471 | はい | はい | — | — |
| N16PduSession HsmfUpdateReq | 1447 | はい | はい | はい | はい |
| N16PduSession HsmfUpdateReq Client | 1477 | はい | はい | はい | はい |
| N16VsmfPdu SessionCreateReq | 1468 | ○ | — | — | — |
| N16PduSession VsmfUpdateReq | 1451 | はい | はい | はい | はい |
| N16PduSession NotifyReq | 1458 | — | ○ | — | — |
| N11SmContext RetrieveReq | 1307 | — | ○ | — | — |
| N16PduSession VsmfUpdateReq Client | 1478 | はい | はい | はい | はい |
| N16PduSession NotifyReqClient | 1488 | — | ○ | — | — |
| S5S8Update BearerReq | 2062 | — | — | — | はい |
| S5S8Create BearerReq | 2059 | — | — | — | はい |
| S5S8Bearer ResourceCmd | 2061 | — | — | — | ○ |
| S5S8Modify BearerCmd | 2064 | — | — | — | ○ |

| | | | | | |
|---|---|---|---|---|---|
| N4GtpuRouter AdvertisementReq | 542 | — | — | — | — |
| S5S8Modify BearerReq | 2053 | — | — | — | — |
| NInternalTxnMsg[1] | 1001(xxxx) | はい | はい | はい | はい |
| Ntimer NotificationMsg[1] | 1002(xxxx) | はい | はい | はい | はい |

1: SMF は、3GPP コール フローを処理するために複数の内部メッセージを使用します。これらの内部イベントはSMFによって送
3GPPに準拠していません。NInternalTxnMsg および NTimerNotificationMsg は、SMF で使用されるこのような内部メッセージを表
る 2 つの汎用イベント ID です。イベント ID の **xxxx** は、デバッグを容易にするために SMF 内部で使用される元のメッセージ タ

SMF は、PDU/PDN の作成とリリースに、N40ChargingDataReq の代わりに N40ChargingDataCreateReq、N40ChargingDataUpdateRe
N40ChargingDataReleaseReq を使用します。

次の表に、PDUセッションの作成、変更、削除、引き継ぎ、および専用ベアラーの手順の詳細なイベント レコードを示します。

**表 *101 : PDU* セッション作成イベント**

| 注 | 番号 | | 名前 | プレゼンス | タイプ | 説明 |
|---|---|---|---|---|---|---|
| N EDR フィールド | | | | M | | |
| **OCEDURE** | **E ID** | **EVENT-ID** | VERSION | M | | **Event = N11SmContext CreateReq** |
| | | | **FIELD-COUNT** | M | | |
| | | | SUPI | M | | |
| | | | IMEI/PEI | M | | |
| | | | IMSI | M | | |
| | | | [MSISDN] | M | | |
| | | | GPSI | M | | |
| | | | STATUS | M | | |
| | | | STATUS-CODE | O | | |
| | | | N1-REQ-PDU（PDN）-SESSION-TYPE | O | PduSessionType | |
| | | | N1-REQ-SSC-MODE | O | | |
| | | | CAUSE | O | | |
| | | | N1-PCO | O | PCO | |
| | | | N1-REQ-MSG-TYPE | O | N1N2MSGREQ CONTENT | PDU-SESSION-ESTB-REQUEST |

| 属性 | 番号 | | 名前 | プレゼンス | タイプ | 説明 |
|---|---|---|---|---|---|---|
| | | | N2-REQ-MSG-TYPE | O | N1N2MSGREQ CONTENT | |
| | | | N1-RSP-MSG-TYPE | O | N1N2MSGRSP CONTENT | |
| | | | N2-RSP-MSG-TYPE | O | N1N2MSGRSP CONTENT | |
| | | | N1-REQ-MAX-SUPP-FILTERS | O | | |
| | | | N1-ALWAYS-ON | O | | |
| | | | RAT-TYPE | M | | |
| | | | S-NSSAI-REQUESTED | O | NSSAI | |
| | | | GUAMI | O | | |
| | | | REQUEST-TYPE | O | | |
| | | | AN-TYPE | O | | |
| | | | OLD-PDU-SESS-ID | O | | |
| | | | N1-DNN/APN | O | | |
| | | | SERVING-NFID | O | | |
| | | | SERVING-PLMN | O | | |
| | | | UNAUTH-SUPI | O | | |
| | | | S-NSSAI-ASSIGNED | O | NSSAI | |
| | | | UP-CONTEXT-STATE | O | | |
| | | | N1-PDU-SESS ID | O | | |
| | | | INDIRECTFWD FLAG | O | | |
| | | | DIRECTFWD FLAG | O | | |
| | | | HO-STATE | O | | |
| **PROCEDURE ID** | | **EVENT-ID** | VERSION | M | クライアント | **Event = N11Sm ContextUpdateReq** |
| | | | **FIELD-COUNT** | M | | |
| | | | STATUS | M | | |
| | | | STATUS-CODE | O | | |
| | | | SUPI | M | | |
| | | | IMEI | M | | |

| 注 | 番号 | | 名前 | プレゼンス | タイプ | 説明 |
|---|---|---|---|---|---|---|
| | | | IMSI | M | | |
| | | | [MSISDN] | M | | |
| | | | PDU(PDN)-SESSION-TYPE | O | | |
| | | | N1-REQ-MSG-TYPE | O | N1N2MSG REQCONTENT | pdu_session_modification_request<br>pdu_sess_modification_command<br>pdu_session_release_req<br>pdu_session_release_command<br>pdu_session_release_complete<br>pdu_session_modification_reject<br>pdu_session_modification_complete<br>pdu_session_release_reject |
| | | | N2-REQ-MSG-TYPE | O | N1N2MSG REQCONTENT | |
| | | | N1-RSP-MSG-TYPE | O | N1N2MSG RSPCONTENT | pdu_session_modification_request<br>pdu_sess_modification_command<br>pdu_session_release_req<br>pdu_session_release_command<br>pdu_session_release_complete<br>pdu_session_modification_reject<br>pdu_session_modification_complete<br>pdu_session_release_reject |
| | | | N2-RSP-MSG-TYPE | O | N1N2MSG RSPCONTENT | |
| | | | N1-PCO | NA | PCO | |
| | | | N1-QOS-RULE | O | QOS-RULE | |
| | | | N1-QOS-DESC | O | QoS-DESC | |
| | | | CAUSE | O | | |
| | | | N1-ALWAYS-ON | O | | |
| | | | 5G-SM-CAP | O | | |
| | | | N1-RSP-MAX-SUPP-FILTERS | O | | |
| | | | RAT-TYPE | O | | |

| 属性 | 番号 | | 名前 | プレゼンス | タイプ | 説明 |
|---|---|---|---|---|---|---|
| | | | UP-CONTEXT -STATE | O | | |
| | | | HO-STATE | O | | |
| | | | N1-BACKOFF-TIME | NA | | |
| | | | N1-PDU-SESS ID | O | | |
| | | | N1-VCSMREATTEMPTIND | NA | | |
| | | | N1-RE-ATTEMPT -IND | NA | | |
| | | | N1-SESS-AMBR | O | | |
| | | | N1-CONGREATTEMPTIND | O | | |
| | | | N1-RSP-ALWAYS-ON | — | | |
| **PROCEDURE ID** | | **EVENT-ID** | VERSION | M | | **Event=N11N1N2 MessageTransfer Req** |
| | | | **FIELD-COUNT** | M | | |
| | | | STATUS | M | | |
| | | | STATUS-CODE | O | | |
| | | | PDU-SESSION-TYPE | M | | |
| | | | N1-REQ-MSG-TYPE | O | N1N2MSG REQCONTENT | PDU-SESSION-ESTB-ACCEPT<br>PDU-SESSION-ESTB-REJECT<br>PDU_SESSION_RELEASE_COMMAND<br>PDU_SESSION_ MODIFICATION_ COMMAND |
| | | | N2-REQ-MSG-TYPE | | N1N2MSG REQCONTENT | |
| | | | N1-RSP-MSG-TYPE | O | N1N2MSG REQCONTENT | |
| | | | N2-RSP-MSG-TYPE | | N1N2MSG RSPCONTENT | |
| | | | N1-PCO | O | PCO | |
| | | | N1-QOS-RULE | O | QOS-RULE | |
| | | | N1-QOS-DESC | O | QoS-DESC | |
| | | | CAUSE | O | | |
| | | | N1-ALWAYS-ON | O | | |

| 注 | 番号 | | 名前 | プレゼンス | タイプ | 説明 |
|---|---|---|---|---|---|---|
| | | | N1-SESSION-AMBR | O | SESS-AMBR | |
| | | | N1-PAA | O | PAA | |
| | | | N1-S-NSSAI | O | NSSAI | |
| | | | N1-PDU-SESS ID | O | | |
| | | | N1-DNN/APN | O | | |
| | | | N1-BACKOFF-TIME | NA | | |
| | | | N1-REQ-SSC-MODE-SELECTED | O | | |
| | | | N1-REQ-PDU(PDN)-SESSION-TYPE-SELECTED | O | | |
| | | | N1-SSC-MODE -ALLOWED | O | | |
| | | | N1-CONGRE-ATTEMPT-IND | O | | |
| | | | N1-RE-ATTEMPT -IND | NA | | |
| | | | N1-RSP-AN-TYPE | 該当なし | | |
| **OCEDURE** | **E ID** | **EVENT-ID** | VERSION | M | | **Event=N7SmPolicy CreateReq** |
| | | | **FIELD-COUNT** | M | | |
| | | | SUPI | M | | |
| | | | IMEI/PEI | M | | |
| | | | GPSI | M | | |
| | | | STATUS | M | | |
| | | | STATUS-CODE | O | | |
| | | | PDU(PDN)-SESSION-TYPE | O | | |
| | | | QoS-DESC | O | QoS-DESC | |
| | | | SESSION-AMBR | O | SESS-AMBR | |
| | | | CAUSE | O | | |

| 属性 | 番号 | | 名前 | プレゼンス | タイプ | 説明 |
|---|---|---|---|---|---|---|
| **PROCEDURE ID** | | **EVENT-ID** | VERSION | M | | **EVENT= N4Session ModificationReq**<br>**N10Deregistration Request**<br>**N7SmPolicy UpdateReq**<br>**N10Subscription FetchReq**<br>**N10Unsubscribe ForNotificationReq**<br>**SecondaryAuthenReq**<br>**N10SubscribeFor NotificationReq**<br>**N40ChargingDataCreateReq**<br>**N40Charging DataUpdateReq**<br>**N40Charging DataReleaseReq**<br>**N7SmPolicy DeleteReq**<br>**N11Ebi AssignmentReq**<br>**N4Session EstablishmentReq**<br>**N4Session ReleaseReq**<br>**N10Registration Request**<br>**RadiusAcctReq**<br>**N11SmContext RetrieveReq**<br>**N11SmContext StatusNotifyReq** |
| | | | **FIELD-COUNT** | M | | |
| | | | STATUS | M | | |
| | | | STATUS-CODE | O | | |
| | | | PDU-SESSION-TYPE | M | | |
| | | | CAUSE | O | | |
| **PROCEDURE ID** | | **EVENT-ID** | VERSION | M | | **Event=S5S8Create SessReq** |
| | | | **FIELD-COUNT** | M | | |
| | | | SUPI | M | | |
| | | | IMEI/PEI | M | | |

| | 番号 | | 名前 | プレゼンス | タイプ | 説明 |
|---|---|---|---|---|---|---|
| | | | IMSI | M | | |
| | | | [MSISDN] | M | | |
| | | | GPSI | M | | |
| | | | STATUS | M | | |
| | | | STATUS-CODE | O | | |
| | | | PCO | O | PCO | |
| | | | PDU-SESSION-TYPE | O | | |
| | | | SSC-MODE | O | | |
| | | | DNN/APN | O | | |
| | | | QOS-RULE | O | QOS-RULE | |
| | | | QoS-DESC | O | QoS-DESC | |
| | | | SESSION-AMBR | O | SESS-AMBR | |
| | | | CAUSE | O | | |
| | | | PAA | O | PAA | |
| | | | S_NSSAI | O | NSSAI | |
| | | | RAT-TYPE | M | | |
| | | | HO-INDICATION | | | |
| **OCEDURE ID** | | **EVENT-ID** | VERSION | M | | **Event=N16Pdu SessionCreateReq**<br>**N16VsmfPdu SessionCreateReq** |
| | | | **FIELD-COUNT** | M | | |
| | | | SUPI | O | | |
| | | | IMEI/PEI | O | | |
| | | | GPSI | O | | |
| | | | GUAMI | O | GUAMI | |
| | | | REQUEST-TYPE | M | RequestType | |
| | | | STATUS | M | | |
| | | | STATUS-CODE | O | | |
| | | | PDU/PDN-SESSION-TYPE | O | PduSessionType | |
| | | | DNN/APN | M | | |

| 属性 | 番号 | | 名前 | プレゼンス | タイプ | 説明 |
|---|---|---|---|---|---|---|
| | | | RAT-TYPE | O | | |
| | | | S_NSSAI | O | NSSAI | |
| | | | SERVING-PLMN | M | PLMN-ID | |
| | | | VSMF ID | M | | |
| | | | VCNTUNNEL-INFO | M | TUNNEL-INFO | |
| | | | HO-PREP-INDICATION | O | | |
| | | | PGW-S8-CFTEID | O | | |
| | | | ALWAYS-ON -REQUESTED | O | | |
| | | | UE-LOCATION | O | UE-LOCATION | |
| | | | ROAMING-CHRG-PROF-REQUESTED | O | CHARGING-PROF | |
| | | | ALWAYS-ON-GRANTED | O | | |
| | | | SSC-MODE | O | | |
| | | | HCNTUNNEL-INFO | M | TUNNEL-INFO | |
| | | | SESSION-AMBR | O | SESS-AMBR | |
| | | | UE-IPV4-ADDRESS | O | | |
| | | | UE-IPV6-PREFIX | O | | |
| | | | QOS-FLOWS-SETUP-LIST | O | QFS | |
| | | | ROAMING-CHRG -PROF- SELECTED | O | CHARGING-PROF | |
| | | | CAUSE | O | | |
| | | | N1SM-CAUSE | O | | |
| | | | UE-IPV6-INTERFACE -ID | O | | |
| | | | N1-REQ-MSG-TYPE | O | | PDU_SESSION_ ESTABLISHMENT _REQ |
| | | | N2-REQ-MSG-TYPE | O | | |
| | | | N1-RSP-MSG-TYPE | O | | PDU_SESSION_ ESTABLISHMENT _ACCEPT |
| | | | N2-RSP-MSG-TYPE | O | | |

| 注 | 番号 | | 名前 | プレゼンス | タイプ | 説明 |
|---|---|---|---|---|---|---|
| | | | N1-PDU-SESS ID | O | | |
| | | | N1-REQ-PDU（PDN）-SESSION-TYPE | O | | |
| | | | N1-REQ-SSC -MODE | O | | |
| | | | N1-PCO | O | | |
| | | | N1-REQ-MAX-SUPP -FILTERS | O | | |
| | | | N1-ALWAYS-ON | O | | |
| | | | N1-REQ-PDU(PDN)-SESSION-TYPE-SELECTED | O | | |
| | | | N1-REQ-SSC-MODE -SELECTED | O | | |
| | | | N1-QOS-RULES | O | | |
| | | | N1-QOS-DESC | O | | |
| | | | N1-SESS-AMBR | O | | |
| | | | N1-REQ-ALWAYS-ON | O | | |
| | | | N1-REQ-SSC-MODE -ALLOWED | O | | |
| | | | N1-CONGRE-ATTEMPT-IND | O | | |
| | | | N1-RSP-RE-ATTEMPT-IND | O | | |
| | | | N1-DNN/APN | O | | |
| **OCEDURE ID** | | **EVENT-ID** | VERSION | M | | **Event= N16VsmfPdu SessionReleaseReq** |
| | | | **FIELD-COUNT** | M | | |
| | | | STATUS | M | | |
| | | | STATUS-CODE | O | | |
| | | | CAUSE | O | | |
| | | | VGMM-CAUSE | O | | |
| | | | NCAP-CAUSE | O | NCAP-CAUSE | |

| 属性 | 番号 | | 名前 | プレゼンス | タイプ | 説明 |
|---|---|---|---|---|---|---|
| **PROCEDURE ID** | | **EVENT-ID** | VERSION | M | | **Event= N16PduSession VsmfUpdateReq**<br>**N16PduSession VsmfUpdate ReqClient** |
| | | | **FIELD-COUNT** | M | | |
| | | | STATUS | M | | |
| | | | STATUS-CODE | O | | |
| | | | REQUEST-INDICATION | O | N1N2MSG REQCONTENT | |
| | | | SESSION-AMBR | O | N1N2MSG REQCONTENT | |
| | | | ALWAYS-ON-GRANTED | O | RequestIndication | |
| | | | CAUSE | O | SESS-AMBR | |
| | | | N1SM-CAUSE | O | | |
| | | | BACKOFF-TIMER | | | |
| | | | N1-REQ-MSG-TYPE | O | | PDU_SESSION_ MODIFICATION _COMMAND<br>PDU_SESSION_ MODIFICATION _COMMAND_REJECT |
| | | | N1-RSP-MSG-TYPE | | | PDU_SESSION_ MODIFICATION _COMMAND<br>PDU_SESSION_ MODIFICATION _COMMAND_REJECT<br>PDU_SESSION_ MODIFICATION _REJECT |
| | | | N1-PCO | O | | |
| | | | N1-QOS-RULE | O | | |
| | | | N1-QOS-DESC | O | | |
| | | | N1-PDU-SESS ID | O | | |
| | | | N1-ALWAYS-ON | O | | |
| | | | N1-SESSION-AMBR | O | | |

| 注 | 番号 | | 名前 | プレゼンス | タイプ | 説明 |
|---|---|---|---|---|---|---|
| **OCEDURE** | **E ID** | **EVENT-ID** | VERSION | M | | **Event=N16Pdu SessionHsmf UpdateReq**<br>**N16PduSessionHsmf UpdateReqClient** |
| | | | **FIELD-COUNT** | M | | |
| | | | STATUS | M | | |
| | | | STATUS-CODE | O | | |
| | | | IMEI/PEI | O | | |
| | | | REQUEST-INDICATION | M | RequestIndication | |
| | | | VCNTUNNEL-INFO | O | TUNNEL-INFO | |
| | | | SERVING-PLMN | O | | |
| | | | AN-TYPE | O | AccessType | |
| | | | RAT-TYPE | O | | |
| | | | HO-PREP-INDICATION | O | | |
| | | | CAUSE | O | | |
| | | | VGMM-CAUSE | O | | |
| | | | NCAP-CAUSE | O | NCAP-CAUSE | |
| | | | ALWAYS-ON | O | | |
| | | | EPS-IWK | O | | |
| | | | AN-TYPE-CAN-BE-CHANGED | O | | |
| | | | UE-LOCATION | O | UE-LOCATION | |
| | | | N1-REQ-MSG-TYPE | O | | PDU_SESSION_MODIFICATION_REQUEST<br>PDU_SESSION_RELEASE_REQUEST |
| | | | N1-RSP-MSG-TYPE | O | | |
| | | | N1-PDU-SESS ID | O | | |
| | | | N1-PCO | O | | |
| | | | N1-RSP-MAX-SUPP-FILTERS | O | | |
| | | | N1-REQ-ALWAYS-ON | O | | |

| 属性 | 番号 | | 名前 | プレゼンス | タイプ | 説明 |
|---|---|---|---|---|---|---|
| | | | N1-QOS-RULES | O | | |
| | | | N1-QOS-DESC | O | | |
| **PROCEDURE ID** | | **EVENT ID=1000** | VERSION | M | | **Event=META DATA** |
| | | | **FIELD-COUNT** | M | | |
| | | | SUPI | M | | |
| | | | IMEI/PEI | M | | |
| | | | IMSI | M | | |
| | | | [MSISDN] | M | | |
| | | | GPSI | | | |
| | | | SERVING-PLMN | M | | |
| | | | UE-LOCATION | M | UE-LOCATION | |
| | | | START-TIME | M | | |
| | | | END-TIME | M | | |
| | | | TRIGGER-NF | M | | |
| | | | TRIGGER-EVENT | M | | |
| | | | SGW-ID | O | | |
| | | | STATUS | M | | |
| | | | USERPLANE-STATUS | O | Userplane-status | |
| | | | DISCONNECT-REASON | O | | |
| | | | DNN/APN | M | | |
| | | | RAT-TYPE | M | | |
| | | | UE-TIMEZONE | M | | |
| | | | PDU/PDN-SESSION-TYPE | M | | |
| | | | UE-PLMN | M | | |
| | | | SUBSCRIBED-SESS-AMBR-UPLINK | M | | |
| | | | SUBSCRIBED-SESS-AMBR-DOWNLINK | M | | |
| | | | SUBSCRIBED-5QI | M | | |
| | | | SUBSCRIBED-ARP | M | | |

| 注 | 番号 | | 名前 | プレゼンス | タイプ | 説明 |
|---|---|---|---|---|---|---|
| | | | PAA | M | | |
| | | | LOCAL-SEID | M | | |
| | | | REMOTE-SEID | M | | |
| | | | ROAMING-STATUS | M | | |
| | | | PDU/PDN-SESSION-ID | O | | |
| | | | ALWAYS-ON | O | | |
| | | | EPS-IWK | O | | |
| | | | S_NSSAI | O | | |
| | | | MAX-SUPP-FILTERS | O | | |
| | | | SSC-MODE | O | | |
| | | | UE-TYPE | O | | |
| | | | LOCAL-CFTEID-TEID | O | | |
| | | | LOCAL-CFTEID -IP | O | | |
| | | | REMOTE-CFTEID-TEID | O | | |
| | | | REMOTE-CFTEID -IP | O | | |
| | | | VIRTUAL-DNN/APN | O | | |

表 *102 : PDU Session Modify Events*

| 属性 | | 名前 | プレゼンス | 説明 |
|---|---|---|---|---|
| TIME-STAMP | EVENT-ID1=1290 | PROCEDURE-ID | M | N11SmContextUpdateReq |
| EVENT-LIST | | VERSION | M | PduSessionModification Request (MESSAGE-<br>5G-SM-CAP<br>MAX-SUPP-FILTERS<br>PCO<br>ALWAYS-ON<br>QOS-RULE<br>QoS-DESC<br>CAUSE |

| 属性 | | 名前 | プレゼンス | 説明 |
|---|---|---|---|---|
| | | **FIELD-COUNT** | M | |
| | | STATUS | M | |
| | | STATUS-CODE | O | |
| | | SUPI | M | |
| | | IMEI | M | |
| | | IMSI | M | |
| | | [MSISDN] | M | |
| | | PDU(PDN)-SESSION -TYPE | O | |
| | | N1-REQ-MSG-TYPE | O | N1N2MSGREQ CONTENT |
| | | N2-REQ-MSG-TYPE | O | N1N2MSGREQ CONTENT |
| | | N1-RSP-MSG-TYPE | O | N1N2MSGRSP CONTENT |
| | | N2-RSP-MSG-TYPE | O | N1N2MSGRSP CONTENT |
| | | N1-PCO | NA | PCO |
| | | N1-QOS-RULE | O | QOS-RULE |
| | | N1-QOS-DESC | O | QoS-DESC |
| | | CAUSE | O | |
| | | N1-ALWAYS-ON | O | |
| | | 5G-SM-CAP | O | |
| | | N1-RSP-MAX-SUPP -FILTERS | O | |
| | | RAT-TYPE | O | |
| | | UP-CONTEXT-STATE | O | |
| | | HO-STATE | O | |
| | | N1-BACKOFF-TIME | NA | |
| | | N1-PDU-SESS ID | M | |
| | | N1-VGSM-RE -ATTEMPT-IND | NA | |
| | | N1-RE-ATTEMPT-IND | NA | |
| | | N1-SESS-AMBR | O | |
| | | N1-CONG-RE-ATTEMPT-IND | O | |
| | | N1-RSP-ALWAYS-ON | NA | |
| | | DATAFORWARDING | O | |
| | EVENT-ID | PROCEDURE-ID | M | N10UpdateNotifyReq |

| 属性 | | 名前 | プレゼンス | 説明 |
|---|---|---|---|---|
| | | VERSION | M | |
| | | **FIELD-COUNT** | M | |
| | | STATUS | M | |
| | | STATUS-CODE | O | |
| | | PDU(PDN)-SESSION -TYPE | M | |
| | | CAUSE | O | |
| | EVENT-ID4=1299 | PROCEDURE-ID | M | N11N1N2Message TransferReq |
| | | **FIELD-COUNT** | M | |
| | | STATUS | M | |
| | | STATUS-CODE | O | |
| | | PDU-SESSION-TYPE | M | |
| | | N1MSGREQTYPE | O | N1N2MSGREQ CONTENT |
| | | N2MSGREQTYPE | O | N1N2MSGREQ CONTENT |
| | | N1-PCO | O | PCO |
| | | N1-QOS-RULE | O | QOS-RULE |
| | | N1-QOS-DESC | O | QoS-DESC |
| | | CAUSE | O | |
| | | N1-ALWAYS-ON | O | |
| | | N1-SESSION-AMBR | O | SESS-AMBR |
| | | N1-PAA | O | PAA |
| | | N1-S-NSSAI | O | NSSAI |
| | | N1-PDU-SESS ID | | |
| | | N1-DNN/APN | O | |
| | | N1-BACKOFF-TIME | NA | |
| | | N1-REQ-SSC- MODE-SELECTED | O | |
| | | N1-REQ-PDU(PDN) -SESSION-TYPE -SELECTED | O | |
| | | N1-SSC-MODE-ALLOWED | O | |
| | | N1-CONG-RE-ATTEMPT-IND | O | |
| | | N1-RSP-RE-ATTEMPT-IND | NA | |
| | | N1-RSP-AN-TYPE | NA | |

| 属性 | | 名前 | プレゼンス | 説明 |
|---|---|---|---|---|
| **PROCEDURE-ID** | **EVENT-ID** | VERSION | M | **Event=N16PduSession HsmfUpdateReq**<br>**N16PduSessionHsmf UpdateReqClient** |
| | | **FIELD-COUNT** | M | |
| | | STATUS | M | |
| | | STATUS-CODE | O | |
| | | IMEI/PEI | O | |
| | | REQUEST-INDICATION | M | RequestIndication |
| | | VCNTUNNEL-INFO | O | TUNNEL-INFO |
| | | SERVING-PLMN | O | |
| | | AN-TYPE | O | AccessType |
| | | RAT-TYPE | O | |
| | | HO-PREP-INDICATION | O | |
| | | CAUSE | O | |
| | | VGMM-CAUSE | O | |
| | | NCAP-CAUSE | O | NCAP-CAUSE |
| | | ALWAYS-ON | O | |
| | | EPS-IWK | O | |
| | | AN-TYPE-CAN-BE -CHANGED | O | |
| | | N1-PDU-SESS ID | O | |
| | | N1-PCO | O | |
| | | N1-RSP-MAX- SUPP-FILTERS-REQUESTED | O | |
| | | N1-ALWAYS-ON | O | |
| | | N1-QOS-RULES | O | |
| | | N1-QOS-DESC | O | |
| **PROCEDURE-ID** | **EVENT-ID** | VERSION | M | **Event= N16PduSession VsmfUpdateReq**<br>**N16PduSessionVsmf UpdateReqClient** |
| | | **FIELD-COUNT** | M | |
| | | STATUS | M | |
| | | STATUS-CODE | O | |
| | | REQUEST-INDICATION | O | N1N2MSGREQ CONTENT |
| | | SESSION-AMBR | O | N1N2MSGREQ CONTENT |

| 属性 | | 名前 | プレゼンス | 説明 |
|---|---|---|---|---|
| | | ALWAYS-ON-GRANTED | O | RequestIndication |
| | | CAUSE | O | SESS-AMBR |
| | | N1SM-CAUSE | O | |
| | | BACKOFF-TIMER | O | |
| | | N1-REQ-MSG-TYPE | O | PDU_SESSION_ MODIFICATION_ COMMA<br>PDU_SESSION_ MODIFICATION_ COMMA |
| | | N1-RSP-MSG-TYPE | | PDU_SESSION_ MODIFICATION_ COMMA<br>PDU_SESSION_MODIFICATION_COMMA<br>PDU_SESSION_MODIFICATION_REJECT |
| | | N1-PCO | O | |
| | | N1-QOS-RULE | O | |
| | | N1-QOS-DESC | O | |
| | | N1-PDU-SESS ID | O | |
| | | N1-ALWAYS-ON | O | |
| | | N1-SESSION-AMBR | O | |
| | EVENT-ID | PROCEDURE-ID | M | N4Session ModificationReq<br>N40Charging NotificationReq<br>N11N1N2MessageTransfer FailNotificationRe<br>RadiusAcctReq<br>N40ChargingData CreateReq<br>N40ChargingDataUpdateReq<br>N40ChargingData<br>N11EbiAssignmentReq<br>N7SmPolicyUpdate NotifyReq<br>N7SmPolicyUpdateReq |
| | | VERSION | M | |
| | | **FIELD-COUNT** | M | |
| | | STATUS | M | |
| | | STATUS-CODE | O | |
| | | PDU-SESSION-TYPE | O | |
| | | CAUSE | O | |

| 属性 | | 名前 | プレゼンス | 説明 |
|---|---|---|---|---|
| | EVENT-ID1 = 1000 | PROCEDURE-ID | M | META-DATA |
| | | VERSION | M | |
| | | **FIELD-COUNT** | M | |
| | | SUPI | M | |
| | | IMEI/PEI | M | |
| | | IMSI | M | |
| | | [MSISDN] | M | |
| | | GPSI | M | |
| | | SERVING-PLMN | M | |
| | | UE-LOCATION | M | |
| | | START-TIME | M | |
| | | END-TIME | M | |
| | | TRIGGER-NF | M | |
| | | TRIGGER-EVENT | M | |
| | | USERPLANE-STATUS | M | |
| | | SGW-ID | O | |
| | | DISCONNECT-REASON | NA | |
| | | STATUS | M | |
| | | SUBSCRIBED-SESS -AMBR-UPLINK | M | |
| | | SUBSCRIBED-SESS -AMBR-DOWNLINK | M | |
| | | ALWAYS-ON | O | |
| | | MAX-SUPP-FILTERS | O | |
| | | LOCAL-CFTEID-TEID | O | |
| | | LOCAL-CFTEID-IP | O | |
| | | REMOTE-CFTEID-TEID | O | |
| | | REMOTE-CFTEID-IP | O | |

表 *103 : PDU* セッション削除イベント

| | | 番号 | 名前 | プレゼンス | タイプ | 説明 |
|---|---|---|---|---|---|---|
| ィー | | | | M | | |
| **E ID** | **EVE** | **ENT-ID** | **VERSION** | **M** | | **EVENT=N11Sm ContextReleaseReq**<br>**N40ChargingData**<br>**N7SmPolicy DeleteReq**<br>**N10Unsubscribe ForNotificationReq**<br>**N10Deregistration Request**<br>**N7SmPolicy TerminateNotifyReq**<br>**RadiusCoa DisconnectReq**<br>**RadiusAcctReq**<br>**N7SmPolicy TerminateNotifyReq**<br>**N40Charging NotificationReq**<br>**N10Update NotifyReq**<br>**N11SmContext StatusNotifyReq**<br>**N11N1N2Message TransferFail NotificationReq**<br>**S5S8DeleteSessReq**<br>**N11SmContext RetrieveReq** |
| | | | **FIELD-COUNT** | M | | |
| | | | STATUS | M | | |
| | | | STATUS-CODE | O | | |
| | | | PDU(PDN)-SESSION -TYPE | M | | |
| | | | CAUSE | O | | |
| **E ID** | **EVE** | **ENT-ID** | VERSION | M | | **Event = N11SmContext UpdateReq** |
| | | | **FIELD-COUNT** | M | | |
| | | | STATUS | M | | |
| | | | STATUS-CODE | O | | |
| | | | SUPI | M | | |
| | | | IMEI | M | | |
| | | | IMSI | M | | |
| | | | [MSISDN] | M | | |

| | | 番号 | 名前 | プレゼンス | タイプ | 説明 |
|---|---|---|---|---|---|---|
| | | | PDU(PDN)- SESSION-TYPE | O | | |
| | | | N1-REQ-MSG-TYPE | O | N1N2MSGREQ CONTENT | pdu_session_modification_request<br>pdu_sess_modification_command<br>pdu_session_release_req<br>pdu_session_release_command<br>pdu_session_release_complete<br>pdu_session_modification_reject<br>pdu_session_modification_complete<br>pdu_session_release_reject |
| | | | N2-REQ-MSG-TYPE | O | N1N2MSGREQ CONTENT | |
| | | | N1-RSP-MSG-TYPE | O | N1N2MSGRSP CONTENT | pdu_session_modification_request<br>pdu_sess_modification_command<br>pdu_session_release_req<br>pdu_session_release_command<br>pdu_session_release_complete<br>pdu_session_modification_reject<br>pdu_session_modification_complete<br>pdu_session_release_reject |
| | | | N2-RSP-MSG-TYPE | O | N1N2MSGRSP CONTENT | |
| | | | N1-PCO | NA | PCO | |
| | | | N1-QOS-RULE | O | QOS-RULE | |
| | | | N1-QOS-DESC | O | QoS-DESC | |
| | | | CAUSE | O | | |
| | | | N1-ALWAYS-ON | O | | |
| | | | 5G-SM-CAP | O | | |
| | | | N1-RSP-MAX-SUPP-FILTERS | O | | |
| | | | RAT-TYPE | O | | |
| | | | UP-CONTEXT-STATE | O | | |
| | | | HO-STATE | O | | |
| | | | N1-BACKOFF-TIME | NA | | |

| | | 番号 | 名前 | プレゼンス | タイプ | 説明 |
|---|---|---|---|---|---|---|
| | | | N1-PDU-SESS ID | O | | |
| | | | N1-VGSM-RE -ATTEMPT-IND | NA | | |
| | | | N1-RE-ATTEMPT -IND | NA | | |
| | | | N1-SESS-AMBR | O | | |
| | | | N1-CONG-RE-ATTEMPT-IND | O | | |
| | | | N1-RSP-ALWAYS -ON | NA | | |
| | | | DATAFORWARDING | O | | |
| **E ID** | **EVENT-ID** | | VERSION | **M** | | **Event=N11N1N2 MessageTransfer Req** |
| | | | **FIELD-COUNT** | M | | |
| | | | STATUS | M | | |
| | | | STATUS-CODE | O | | |
| | | | PDU-SESSION-TYPE | M | | |
| | | | N1-REQ-MSG-TYPE | O | N1N2MSGREQ CONTENT | PDU-SESSION-ESTB-ACCEPT<br>PDU-SESSION-ESTB-REJECT<br>PDU_SESSION_RELEASE_COMMAND<br>PDU_SESSION_ MODIFICATION_ COMMAND |
| | | | N2-REQ-MSG-TYPE | O | N1N2MSGREQ CONTENT | |
| | | | N1-RSP-MSG-TYPE | | N1N2MSGREQ CONTENT | |
| | | | N2-RSP-MSG-TYPE | | N1N2MSGREQ CONTENT | |
| | | | N1-PCO | O | PCO | |
| | | | N1-QOS-RULE | O | QOS-RULE | |
| | | | N1-QOS-DESC | O | QoS-DESC | |
| | | | CAUSE | O | | |
| | | | N1-ALWAYS-ON | O | | |
| | | | N1-SESSION-AMBR | O | SESS-AMBR | |
| | | | N1-PAA | O | PAA | |
| | | | N1-S-NSSAI | O | NSSAI | |
| | | | N1-PDU-SESS ID | | | |

| | | 番号 | 名前 | プレゼンス | タイプ | 説明 |
|---|---|---|---|---|---|---|
| | | | N1-DNN/APN | O | | |
| | | | N1-BACKOFF-TIME | NA | | |
| | | | N1-REQ-SSC-MODE-SELECTED | O | | |
| | | | N1-REQ-PDU(PDN)-SESSION-TYPE -SELECTED | O | | |
| | | | N1-SSC-MODE- ALLOWED | O | | |
| | | | N1-CONG-RE-ATTEMPT-IND | O | | |
| | | | N1-RE-ATTEMPT -IND | NA | | |
| | | | N1-RSP-AN-TYPE | 該当なし | | |
| **URE ID** | **EVE** | **ENT-ID** | VERSION | M | | **Event=N16Pdu SessionHsmf UpdateReq**<br>**N16PduSessionHsmf UpdateReqClient** |
| | | | **FIELD-COUNT** | M | | |
| | | | STATUS | M | | |
| | | | STATUS-CODE | O | | |
| | | | IMEI/PEI | O | | |
| | | | REQUEST- INDICATION | M | RequestIndication | |
| | | | VCNTUNNEL-INFO | O | TUNNEL-INFO | |
| | | | SERVING-PLMN | O | | |
| | | | AN-TYPE | O | AccessType | |
| | | | RAT-TYPE | O | | |
| | | | HO-PREP- INDICATION | O | | |
| | | | CAUSE | O | | |
| | | | VGMM-CAUSE | O | | |
| | | | NCAP-CAUSE | O | NCAP-CAUSE | |
| | | | ALWAYS-ON | O | | |
| | | | EPS-IWK | O | | |
| | | | AN-TYPE-CAN-BE -CHANGED | O | | |
| | | | N1-PDU-SESS ID | O | | |
| | | | N1-PCO | O | | |

| | | 番号 | 名前 | プレゼンス | タイプ | 説明 |
|---|---|---|---|---|---|---|
| | | | N1-RSP-MAX-SUPP-FILTERS | O | | |
| | | | N1-ALWAYS-ON | O | | |
| | | | N1-QOS-RULES | O | | |
| | | | N1-QOS-DESC | O | | |
| **E ID** | **EVENT-ID** | | VERSION | M | | **Event= N16PduSession VsmfUpdateReq**<br>**N16PduSessionVsmf UpdateReqClient** |
| | | | **FIELD-COUNT** | M | | |
| | | | STATUS | M | | |
| | | | STATUS-CODE | O | | |
| | | | REQUEST- INDICATION | O | N1N2MSGREQ CONTENT | |
| | | | SESSION-AMBR | O | N1N2MSGREQ CONTENT | |
| | | | ALWAYS-ON- GRANTED | O | RequestIndication | |
| | | | CAUSE | O | SESS-AMBR | |
| | | | N1SM-CAUSE | O | | |
| | | | BACKOFF-TIMER | O | | |
| | | | N1-REQ-MSG-TYPE | O | | PDU_SESSION_ MODIFICATION _COMMAND<br>PDU_SESSION_ MODIFICATION_ COMMAND_REJECT |
| | | | N1-RSP-MSG-TYPE | O | | PDU_SESSION_ MODIFICATION _COMMAND<br>PDU_SESSION_ MODIFICATION_ COMMAND_REJECT<br>PDU_SESSION_ MODIFICATION _REJECT |
| | | | N1-PCO | O | | |
| | | | N1-QOS-RULE | O | | |
| | | | N1-QOS-DESC | O | | |
| | | | N1-PDU-SESS ID | O | | |
| | | | N1-ALWAYS-ON | O | | |
| | | | N1-SESSION-AMBR | O | | |
| **E ID** | **EVENT-ID** | | VERSION | M | | **Event= N16Vsmf PduSession ReleaseReq** |
| | | | **FIELD-COUNT** | M | | |

| | | 番号 | 名前 | プレゼンス | タイプ | 説明 |
|---|---|---|---|---|---|---|
| | | | STATUS | O | | |
| | | | STATUS-CODE | O | | |
| | | | CAUSE | O | | |
| | | | VGMM-CAUSE | O | | |
| | | | NCAP-CAUSE | O | | |
| **URE ID** | **EVE** | **NT-ID** | VERSION | M | | **Event=N16Pdu SessionNotify ReqClient N16PduSession NotifyReq** |
| | | | **FIELD-COUNT** | M | | |
| | | | STATUS | M | | |
| | | | STATUS-CODE | O | | |
| | | | RESOURCE-STATUS | O | Resourcestatus | |
| | | | CAUSE | O | | |
| **URE ID** | **EVE** | **NT-ID** | VERSION | M | | **Event=S5S8Delete BearerReq** |
| | | | FIELD-COUNT | M | | |
| | | | STATUS | M | | |
| | | | STATUS-CODE | O | | |
| | | | LBI-REQUESTED | O | | |
| | | | EBIS | O | | |
| | | | FAILED-BEARER -CTX | O | BEARER-CTX | |
| | | | CAUSE-REQUESTED | O | | |
| | | | PCO | O | | |
| | | | CAUSE-RESPONDED | O | | |
| | | | LBI-RESPONDED | O | | |
| | | | UE-LOCAL-IP | O | | |
| | | | UE-UDP-PORT | O | | |
| | | | BEARER-CTX | O | | |
| **URE ID** | **EVE** | **NT-ID=1000** | VERSION | M | | **Event= META-DATA** |
| | | | **FIELD-COUNT** | M | | |
| | | | SUPI | M | | |
| | | | IMEI/PEI | M | | |
| | | | IMSI | M | | |

| | | 番号 | 名前 | プレゼンス | タイプ | 説明 |
|---|---|---|---|---|---|---|
| | | | [MSISDN] | M | | |
| | | | GPSI | | | |
| | | | SERVING-PLMN | M | | |
| | | | UE-LOCATION | M | | |
| | | | START-TIME | M | | |
| | | | END-TIME | M | | |
| | | | TRIGGER-NF | M | | |
| | | | TRIGGER-EVENT | M | | |
| | | | SGW-ID | O | | |
| | | | STATUS | M | | |
| | | | USERPLANE -STATUS | M | | |
| | | | DISCONNECT -REASON | O | | |
| | | | STATUS | M | | |
| | | | UPDATE-TIME | — | | |

表 *104* : 専用ベアラー イベント

| 属性 | | 名前 | プレゼンス | タイプ | 説明 |
|---|---|---|---|---|---|
| TXN EDR フィールド | | | M | | |
| **PROCEDURE ID** | **EVENT-ID** | **VERSION** | **M** | | **Event=N7SmPolicy UpdateNotif**<br>**N7SmPolicy UpdateReq**<br>**N4Session ModificationReq**<br>**N10UpdateNotify Req** |
| | | **FIELD-COUNT** | M | | |
| | | STATUS | M | | |
| | | STATUS-CODE | O | | |
| | | PDU-SESSION-TYPE | O | | |
| | | CAUSE | O | | |
| **PROCEDURE ID** | **EVENT-ID** | VERSION | **M** | | **Event=S5S8Delete BearerCmd** |
| | | FIELD-COUNT | M | | |
| | | STATUS | M | | |

| 属性 | | 名前 | プレゼンス | タイプ | 説明 |
|---|---|---|---|---|---|
| | | STATUS-CODE | O | | |
| | | BEARER-CTX-REQUESTED | O | BEARER-CTX | |
| | | CAUSE | O | | |
| | | BEARER-CTX-RESPONDED | O | BEARER-CTX | |
| | | 復旧 | O | | |
| **PROCEDURE ID** | **EVENT-ID** | VERSION | **M** | | **Event= S5S8Bearer Resource** |
| | | FIELD-COUNT | M | | |
| | | STATUS | M | | |
| | | STATUS-CODE | O | | |
| | | LBI-REQUESTED | O | | |
| | | RAT-TYPE | O | | |
| | | SERVING-PLMN | O | | |
| | | EBI | O | | |
| **PROCEDURE ID** | **EVENT-ID** | VERSION | M | | **Event=S5S8Modify BearerCr** |
| | | FIELD-COUNT | M | | |
| | | STATUS | M | | |
| | | STATUS-CODE | O | | |
| | | APN-AMBR | O | | |
| | | BEARER-CTX | O | BEARER-CTX | |
| | | CAUSE | O | | |
| | | 復旧 | O | | |
| **PROCEDURE ID** | **EVENT-ID** | VERSION | M | | **Event=S5S8Update BearerRe** |
| | | FIELD-COUNT | M | | |
| | | STATUS | M | | |
| | | STATUS-CODE | O | | |
| | | AMBR | O | | |
| | | BEARER-CTX | O | BEARER-CTX | |
| | | CAUSE | O | | |
| | | 復旧 | O | | |
| **PROCEDURE ID** | **EVENT-ID** | VERSION | M | | **Event=S5S8Create BearerRe** |

| 属性 | | 名前 | プレゼンス | タイプ | 説明 |
|---|---|---|---|---|---|
| | | FIELD-COUNT | M | | |
| | | STATUS | M | | |
| | | STATUS-CODE | O | | |
| | | LINKED-BEARER -ID | O | | |
| | | PCO | O | | |
| | | BEARER-CTX | O | BEARER-CTX | |
| | | CAUSE | O | | |
| **PROCEDURE ID** | **EVENT-ID** | VERSION | M | | **Event=S5S8Delete BearerReq** |
| | | FIELD-COUNT | M | | |
| | | STATUS | M | | |
| | | STATUS-CODE | O | | |
| | | LBI-REQUESTED | O | | |
| | | EBIS | O | | |
| | | FAILED-BEARER -CTX | O | BEARER-CTX | |
| | | CAUSE- REQUESTED | O | | |
| | | PCO | O | | |
| | | CAUSE- RESPONDED | O | | |
| | | LBI-RESPONDED | O | | |
| | | UE-LOCAL-IP | O | | |
| | | UE-UDP-PORT | O | | |
| | | BEARER-CTX | O | | |
| **PROCEDURE ID** | **EVENT-ID** | VERSION | M | | **Event=Metadata** |
| | | FIELD-COUNT | M | | |
| | | STATUS | M | | |
| | | STATUS-CODE | O | | |
| | | SUPI | M | | |
| | | IMEI/PEI | O | | |
| | | IMSI | M | | |
| | | [MSISDN] | O | | |
| | | GPSI | O | | |
| | | SERVING-PLMN | O | | |
| | | UE-LOCATION | O | | |

| 属性 | | 名前 | プレゼンス | タイプ | 説明 |
|---|---|---|---|---|---|
| | | START-TIME | O | | |
| | | END-TIME | O | | |
| | | TRIGGER-NF | O | | |
| | | TRIGGER-EVENT | O | | |
| | | SGW-ID | O | | |
| | | STATUS | O | | |
| | | SUBSCRIBED-SESS -AMBR-UPLINK | O | | |
| | | SUBSCRIBED-SESS -AMBR-DOWNLINK | O | | |
| | | LOCAL-CFTEID -TEID | O | | |
| | | LOCAL-CFTEID -IP | O | | |
| | | REMOTE-CFTEID -TEID | O | | |
| | | REMOTE-CFTEID -IP | O | | |

表 ***105*** *:* ハンドオーバー イベント

| 属性 | | 名前 | プレゼンス | タイプ | 説明 |
|---|---|---|---|---|---|
| TXN EDR フィールド | | | M | | |
| **PROCEDURE-ID** | **EVENT-ID** | **VERSION** | **M** | | **N4Session ModificationReq**<br>**N40ChargingData**<br>**N40ChargingDataUpdateReq**<br>**N40ChargingData CreateReq**<br>**RadiusAcctReq**<br>**N4GtpuRouter Advertisemen**<br>**N7SmPolicy UpdateReq**<br>**N7SmPolicyUpdate NotifyRe**<br>**N11SmContext RetrieveReq**<br>**S5S8DeleteSessReq**<br>**N11EbiAssignment Req**<br>**N11SmContextStatus NotifyR** |
| | | **FIELD-COUNT** | M | | |

| 属性 | | 名前 | プレゼンス | タイプ | 説明 |
|---|---|---|---|---|---|
| | | STATUS | M | | |
| | | STATUS-CODE | O | | |
| | | PDU(PDN)-SESSION -TYPE | M | | |
| | | CAUSE | O | | |
| **PROCEDURE ID** | **EVENT-ID** | VERSION | M | | **Event = N11SmContext UpdateR** |
| | | **FIELD-COUNT** | M | | |
| | | STATUS | M | | |
| | | STATUS-CODE | O | | |
| | | SUPI | M | | |
| | | IMEI/PEI | M | | |
| | | IMSI | M | | |
| | | [MSISDN] | M | | |
| | | PDU(PDN)-SESSION -TYPE | O | | |
| | | N1-REQ-MSG-TYPE | O | N1N2MSGREQ CONTENT | pdu_session_modification_request<br>pdu_sess_modification_command<br>pdu_session_release_req<br>pdu_session_release_command<br>pdu_session_release_complete<br>pdu_session_modification_reject<br>pdu_session_modification_comple<br>pdu_session_release_reject |
| | | N2-REQ-MSG-TYPE | O | N1N2MSGREQ CONTENT | |
| | | N1-RSP-MSG-TYPE | O | N1N2MSGRSP CONTENT | pdu_session_modification_request<br>pdu_sess_modification_command<br>pdu_session_release_req<br>pdu_session_release_command<br>pdu_session_release_complete<br>pdu_session_modification_reject<br>pdu_session_modification_comple<br>pdu_session_release_reject |

| 属性 | | 名前 | プレゼンス | タイプ | 説明 |
|---|---|---|---|---|---|
| | | N2-RSP-MSG-TYPE | O | N1N2MSGRSP CONTENT | |
| | | N1-PCO | NA | PCO | |
| | | N1-QOS-RULE | O | QOS-RULE | |
| | | N1-QOS-DESC | O | QoS-DESC | |
| | | CAUSE | O | | |
| | | N1-ALWAYS-ON | O | | |
| | | 5G-SM-CAP | O | | |
| | | N1-RSP-MAX-SUPP-FILTERS | O | | |
| | | RAT-TYPE | O | | |
| | | UP-CONTEXT -STATE | O | | |
| | | HO-STATE | O | Hostate | |
| | | N1-BACKOFF-TIME | NA | | |
| | | N1-PDU-SESS ID | O | | |
| | | N1-VGSM-RE -ATTEMPT-IND | NA | | |
| | | N1-RE-ATTEMPT -IND | NA | | |
| | | N1-SESS-AMBR | O | | |
| | | N1-CONG-RE-ATTEMPT -IND | O | | |
| | | N1-RSP-ALWAYS-ON | NA | | |
| | | DATAFORWARDING | O | | |
| **PROCEDURE ID** | **EVENT-ID** | **VERSION** | **M** | | **Event=N11N1N2 MessageTra** |
| | | **FIELD-COUNT** | M | | |
| | | STATUS | M | | |
| | | STATUS-CODE | O | | |
| | | PDU-SESSION-TYPE | M | | |
| | | N1-REQ-MSG-TYPE | O | N1N2MSGREQ CONTENT | PDU-SESSION-ESTB-ACCEP<br>PDU-SESSION-ESTB-REJEC<br>PDU_SESSION_RELEASE_C<br>PDU_SESSION_MODIFICATIO |
| | | N2-REQ-MSG-TYPE | O | N1N2MSGREQ CONTENT | |

| 属性 | | 名前 | プレゼンス | タイプ | 説明 |
|---|---|---|---|---|---|
| | | N1-RSP-MSG-TYPE | O | N1N2MSGREQ CONTENT | |
| | | N2-RSP-MSG-TYPE | O | N1N2MSGREQ CONTENT | |
| | | N1-PCO | O | PCO | |
| | | N1-QOS-RULE | O | QOS-RULE | |
| | | N1-QOS-DESC | O | QoS-DESC | |
| | | CAUSE | O | | |
| | | N1-ALWAYS-ON | O | | |
| | | N1-SESSION-AMBR | O | SESS-AMBR | |
| | | N1-PAA | O | PAA | |
| | | N1-S-NSSAI | O | NSSAI | |
| | | N1-PDU-SESS ID | O | | |
| | | N1-DNN/APN | O | | |
| | | N1-BACKOFF-TIME | NA | | |
| | | N1-REQ-SSC-MODE -SELECTED | O | | |
| | | N1-REQ-PDU(PDN) -SESSION-TYPE -SELECTED | O | | |
| | | N1-SSC-MODE -ALLOWED | O | | |
| | | N1-CONG-RE-ATTEMPT-IND | O | | |
| | | N1-RE-ATTEMPT -IND | NA | | |
| | | N1-RSP-AN-TYPE | NA | | |
| **PROCEDURE ID** | **EVENT-ID** | VERSION | M | | **Event=S5S8Create SessReq** |
| | | **FIELD-COUNT** | M | | |
| | | SUPI | M | | |
| | | IMEI/PEI | M | | |
| | | IMSI | M | | |
| | | [MSISDN] | M | | |
| | | GPSI | M | | |
| | | STATUS | M | | |
| | | STATUS-CODE | O | | |

| 属性 | | 名前 | プレゼンス | タイプ | 説明 |
|---|---|---|---|---|---|
| | | PCO | O | PCO | |
| | | PDU-SESSION-TYPE | O | | |
| | | SSC-MODE | O | | |
| | | DNN/APN | O | | |
| | | QOS-RULE | O | QOS-RULE | |
| | | QoS-DESC | O | QoS-DESC | |
| | | SESSION-AMBR | O | SESS-AMBR | |
| | | CAUSE | O | | |
| | | PAA | O | PAA | |
| | | S_NSSAI | O | NSSAI | |
| | | RAT-TYPE | M | | |
| | | HO-INDICATION | O | | |
| **PROCEDURE ID** | **EVENT-ID** | VERSION | M | | **Event=S5S8Update BearerRe** |
| | | FIELD-COUNT | M | | |
| | | STATUS | M | | |
| | | STATUS-CODE | O | | |
| | | AMBR | O | | |
| | | BEARER-CTX | O | BEARER-CTX | |
| | | CAUSE | O | | |
| | | 復旧 | O | | |
| **PROCEDURE ID** | **EVENT-ID** | VERSION | M | | **Event=S5S8Create BearerRe** |
| | | FIELD-COUNT | M | | |
| | | STATUS | M | | |
| | | STATUS-CODE | O | | |
| | | LINKED-BEARER -ID | O | | |
| | | PCO | O | | |
| | | BEARER-CTX | O | BEARER-CTX | |
| | | CAUSE | O | | |
| **PROCEDURE ID** | **EVENT-ID** | VERSION | M | | **Event=S5S8Delete BearerRe** |
| | | FIELD-COUNT | M | | |
| | | STATUS | M | | |

| 属性 | | 名前 | プレゼンス | タイプ | 説明 |
|---|---|---|---|---|---|
| | | STATUS-CODE | O | | |
| | | LBI-REQUESTED | O | | |
| | | EBIS | O | | |
| | | FAILED-BEARER -CTX | O | BEARER-CTX | |
| | | CAUSE-REQUESTED | O | | |
| | | PCO | O | | |
| | | CAUSE-RESPONDED | O | | |
| | | LBI-RESPONDED | O | | |
| | | UE-LOCAL-IP | O | | |
| | | UE-UDP-PORT | O | | |
| | | BEARER-CTX | O | | |
| **PROCEDURE ID** | **EVENT-ID** | VERSION | M | | **Event=S5S8Delete BearerCmd** |
| | | FIELD-COUNT | M | | |
| | | STATUS | M | | |
| | | STATUS-CODE | O | | |
| | | BEARER-CTX-REQUESTED | O | BEARER-CTX | |
| | | CAUSE | O | | |
| | | BEARER-CTX-RESPONDED | O | BEARER-CTX | |
| | | 復旧 | O | | |
| **PROCEDURE ID** | **EVENT-ID** | VERSION | M | | **Event=S5S8Modify BearerReq** |
| | | FIELD-COUNT | M | | |
| | | STATUS | M | | |
| | | STATUS-CODE | O | | |
| | | MEI | O | | |
| | | SERVING-PLMN | O | | |
| | | RAT-TYPE | O | | |
| | | FQ_TEID | O | | |
| | | AMBR- REQUESTED | O | | |
| | | MME-S4SGSN-ID | O | | |
| | | M_MBR | O | | |

| 属性 | | 名前 | プレゼンス | タイプ | 説明 |
|---|---|---|---|---|---|
| | | UE-LOCAL-ADDR | O | | |
| | | HENB-LOCAL -ADDR | O | | |
| | | UE-UDP-PORT | O | | |
| | | CAUSE | O | | |
| | | 復旧 | O | | |
| | | LINKED-EBI | O | | |
| | | [MSISDN] | O | | |
| | | AMBR-RESP | O | | |
| | | APN-RESTRICT | O | | |
| | | BEARER-CTX-RESPONDED | O | | |
| **PROCEDURE ID** | **EVENT-ID** | VERSION | M | | **Event=N16Pdu SessionHsmf N16PduSession HsmfUpdate** |
| | | **FIELD-COUNT** | M | | |
| | | STATUS | M | | |
| | | STATUS-CODE | O | | |
| | | IMEI/PEI | O | | |
| | | REQUEST-INDICATION | M | RequestIndication | |
| | | VCNTUNNEL-INFO | O | TUNNEL-INFO | |
| | | SERVING-PLMN | O | | |
| | | AN-TYPE | O | AccessType | |
| | | RAT-TYPE | O | | |
| | | HO-PREP-INDICATION | O | | |
| | | CAUSE | O | | |
| | | VGMM-CAUSE | O | | |
| | | NCAP-CAUSE | O | NCAP-CAUSE | |
| | | ALWAYS-ON | O | | |
| | | EPS-IWK | O | | |
| | | AN-TYPE-CAN-BE-CHANGED | O | | |
| | | UE-LOCATION | O | UE-LOCATION | |

| 属性 | | 名前 | プレゼンス | タイプ | 説明 |
|---|---|---|---|---|---|
| | | N1-REQ-MSG-TYPE | O | | PDU_SESSION_MODIFICATION<br>PDU_SESSION_RELEASE_REQ |
| | | N1-RSP-MSG-TYPE | O | | |
| | | N1-PDU-SESS ID | O | | |
| | | N1-PCO | O | | |
| | | N1-RSP-MAX-SUPP-FILTERS | O | | |
| | | N1-REQ-ALWAYS-ON | O | | |
| | | N1-QOS-RULES | O | | |
| | | N1-QOS-DESC | O | | |
| **PROCEDURE ID** | **EVENT-ID** | VERSION | M | | **Event=N16Pdu SessionCreateRe**<br>**N16VsmfPdu SessionCreateReq** |
| | | **FIELD-COUNT** | M | | |
| | | SUPI | O | | |
| | | IMEI/PEI | O | | |
| | | GPSI | O | | |
| | | GUAMI | O | GUAMI | |
| | | REQUEST-TYPE | M | RequestType | |
| | | STATUS | M | | |
| | | STATUS-CODE | O | | |
| | | PDU/PDN-SESSION -TYPE | O | PduSessionType | |
| | | DNN/APN | M | | |
| | | RAT-TYPE | O | | |
| | | S_NSSAI | O | NSSAI | |
| | | SERVING-PLMN | M | PLMN-ID | |
| | | VSMF ID | M | | |
| | | VCNTUNNEL-INFO | M | TUNNEL-INFO | |
| | | HO-PREP-INDICATION | O | | |
| | | PGW-S8-CFTEID | O | | |
| | | ALWAYS-ON-REQUESTED | O | | |
| | | UE-LOCATION | O | UE-LOCATION | |

| 属性 | | 名前 | プレゼンス | タイプ | 説明 |
|---|---|---|---|---|---|
| | | ROAMING-CHRG-PROF-REQUESTED | O | CHARGING-PROF | |
| | | ALWAYS-ON-GRANTED | O | | |
| | | SSC-MODE | O | | |
| | | HCNTUNNEL-INFO | M | TUNNEL-INFO | |
| | | SESSION-AMBR | O | SESS-AMBR | |
| | | UE-IPV4-ADDRESS | O | | |
| | | UE-IPV6-PREFIX | O | | |
| | | QOS-FLOWS-SETUP-LIST | O | QFS | |
| | | ROAMING-CHRG-PROF-SELECTED | O | CHARGING- PROF | |
| | | CAUSE | O | | |
| | | N1SM-CAUSE | O | | |
| | | UE-IPV6-INTERFACE-ID | O | | |
| | | N1-REQ-MSG-TYPE | O | | PDU_SESSION_ ESTABLISH |
| | | N2-REQ-MSG-TYPE | O | | |
| | | N1-RSP-MSG-TYPE | O | | PDU_SESSION_ ESTABLISHM |
| | | N2-RSP-MSG-TYPE | O | | |
| | | N1-PDU-SESS ID | O | | |
| | | N1-REQ-PDU(PDN) -SESSION-TYPE | O | | |
| | | N1-REQ-SSC-MODE | O | | |
| | | N1-PCO | O | | |
| | | N1-REQ-MAX-SUPP-FILTERS | O | | |
| | | N1-ALWAYS-ON | O | | |
| | | N1-REQ-PDU(PDN)-SESSION-TYPE -SELECTED | O | | |
| | | N1-REQ-SSC-MODE -SELECTED | O | | |
| | | N1-QOS-RULES | O | | |
| | | N1-QOS-DESC | O | | |

| 属性 | | 名前 | プレゼンス | タイプ | 説明 |
|---|---|---|---|---|---|
| | | N1-SESS-AMBR | O | | |
| | | N1-REQ-ALWAYS -ON | O | | |
| | | N1-REQ-SSC-MODE -ALLOWED | O | | |
| | | N1-CONG-RE-ATTEMPT-IND | O | | |
| | | N1-RSP-RE-ATTEMPT-IND | O | | |
| | | N1-DNN/APN | O | | |
| **PROCEDURE ID** | **EVENT-ID** | VERSION | M | | **Event = N11SmContext CreateR** |
| | | **FIELD-COUNT** | M | | |
| | | SUPI | M | | |
| | | IMEI/PEI | M | | |
| | | IMSI | M | | |
| | | [MSISDN] | M | | |
| | | GPSI | M | | |
| | | STATUS | M | | |
| | | STATUS-CODE | O | | |
| | | N1-REQ-PDU(PDN) -SESSION-TYPE | O | PduSessionType | |
| | | N1-REQ-SSC-MODE | O | | |
| | | CAUSE | O | | |
| | | N1-PCO | O | PCO | |
| | | N1-REQ-MSG-TYPE | O | N1N2MSGREQ CONTENT | PDU-SESSION -ESTB-REQUEST |
| | | N2-REQ-MSG-TYPE | O | N1N2MSGREQ CONTENT | |
| | | N1-RSP-MSG-TYPE | O | N1N2MSGRSP CONTENT | |
| | | N2-RSP-MSG-TYPE | O | N1N2MSGRSP CONTENT | |
| | | N1-REQ-MAX-SUPP-FILTERS | O | | |
| | | N1-ALWAYS-ON | O | | |
| | | RAT-TYPE | M | | |
| | | S-NSSAI- REQUESTED | O | NSSAI | |

| 属性 | | 名前 | プレゼンス | タイプ | 説明 |
|---|---|---|---|---|---|
| | | GUAMI | O | | |
| | | REQUEST-TYPE | O | | |
| | | AN-TYPE | O | | |
| | | OLD-PDU-SESS-ID | O | | |
| | | N1-DNN/APN | O | | |
| | | SERVING-NFID | O | | |
| | | SERVING-PLMN | O | | |
| | | UNAUTH-SUPI | O | | |
| | | S-NSSAI- ASSIGNED | O | NSSAI | |
| | | UP-CONTEXT -STATE | O | | |
| | | N1-PDU-SESS ID | O | | |
| | | INDIRECTFWDFLAG | O | | |
| | | DIRECTFWDFLAG | O | | |
| | | HO-STATE | O | | |
| **PROCEDURE ID** | **EVENT-ID** | VERSION | M | | **Event=Metadata** |
| | | FIELD-COUNT | M | | |
| | | SUPI | M | | |
| | | IMEI/PEI | O | | |
| | | IMSI | M | | |
| | | [MSISDN] | O | | |
| | | GPSI | O | | |
| | | SERVING-PLMN | O | | |
| | | UE-LOCATION | O | | |
| | | START-TIME | O | | |
| | | END-TIME | O | | |
| | | TRIGGER-NF | O | | |
| | | TRIGGER-EVENT | O | | |
| | | SGW-ID | O | | |
| | | STATUS | O | | |
| | | RAT-TYPE | O | | |
| | | UE-TIMEZONE | O | | |
| | | SESS-AMBR- UPLINK | O | | |

| 属性 | | 名前 | プレゼンス | タイプ | 説明 |
|---|---|---|---|---|---|
| | | SESS-AMBR-DOWNLINK | O | | |
| | | LINKED-EBI | O | | |
| | | USERPLANE- STATUS | O | | |
| | | LOCAL-CFTEID -TEID | O | | |
| | | LOCAL-CFTEID -IP | O | | |
| | | REMOTE-CFTEID -TEID | O | | |
| | | REMOTE-CFTEID -IP | O | | |
| | | DISCONNECT -REASON | O | | |

注：

- subscribed-sess-ambr-uplink および subscribed-sess-ambr-downlink：これらのフィールドは、一部の手順のメタデータ イベントでキャプチャされます。これらのフィールドの値は、Pdu コンテキストに保存されているものとして出力されます。メタデータイベントのビットレートは、bps、kbps、mbps などの単位がありません。デフォルトのビットレートは、毎秒のビット（bps）として読み込まれます。
- Status：イベント METADATA（ID = 1000）では、このフィールドは手順のステータスを示します。他のイベントの場合は、受信した応答メッセージのタイプまたは意図した送信応答タイプが示されます。ステータスは、次のいずれかになります。
  - 成功
  - 失敗
  - PartialFailure
  - NoRspValidation：このステータスは、要求が **ASYNC（ファイア アンド フォーステップ）** モードで送信され、応答が予期されず、SMF で処理されない場合に使用されます。
- ステータス コード：このフィールドは、応答メッセージの HTTP ステータス コードを示します。smf-service は rest-ep によって入力された実際のステータス コードを認識していないため、このフィールドは発信応答メッセージの場合は空にする必要があります。このような場合、ステータス フィールドは、成功または失敗応答など、SMF が送信する予定の応答タイプを示します。
- userplane-status のタイプは number です。番号は次のいずれかです。
  - UpStateNone = 0
  - UpStateEstablishing = 1 // UPF セッションが確立中またはセットアップ中

- UpStateActivating = 2 // アクセス トンネルをアクティブ化するように UPF セッションが変更されています
- UpStateActivated = 3 // アクセスおよびコア トンネルの UPF セッションアクティブ
- UpStateDeactivating = 4 // アクセス トンネルを非アクティブ化するために UPF セッションが変更されています
- UpStateDeactivated = 5 // アクセス用に非アクティブ化された UPF セッション、有効なコア トンネルのみ
- UpStateModifying = 6 // QoS またはフロー パラメータの UPF セッションが変更されています
- UpStateDeleting = 7 // UPF セッションがリリースされています
- UpStateDeleted = 8 // UPF セッションがリリースされました

• PduSessionType はタイプ番号です。番号は次のいずれかです。

- UnknownSessionType または Invalid = 0
- Ipv4PduSession = 1
- Ipv6PduSession = 2
- Ipv4V6PduSession = 3
- Unstrutured = 4
- Ethernet = 5
- FutureUsePduSessionType = 7

• SSC モードはタイプ番号です。番号は次のいずれかです。

- UnknownSscMode = 0
- SscMode1 = 1
- SscMode2 = 2
- SscMode3 = 3
- DupSscMode1 = 4
- DupSscMode2 = 5
- DupSscMode3 = 6
- FutureUseSscMode = 7

• Eps Iwk（タイプ：番号）

- EpsInterworkingIndication_DummyEnum = 0
- EpsInterworkingIndication_NONE = 1

- EpsInterworkingIndication_WITH_N26 = 2
- EpsInterworkingIndication_WITHOUT_N26 = 3

- ローミング ステータス（タイプ：番号）
  - ROAMING_STATUS_NONE = 0
  - ROAMING_STATUS_HOMER = 1 *//HOMER*
  - ROAMING_STATUS_VISITOR_LBO = 2 *//LBO*
  - ROAMING_STATUS_VISITOR_HR = 3 *//IN-HR*
  - ROAMING_STATUS_ROMER = 4 *//OUT-HR*

- PreemptionCapability（タイプ：数字）

  **5G:**

  - 0："PreemptionCapability_DummmyEnum"
  - 1："NOT_PREMPT"
  - 2："MAY_PREMPT"

  **4G および Wi-Fi**：

  - 0 = 無効
  - 1 = 有効

- PreemptionVulnerability（タイプ：番号）

  **5G:**

  - 0："PreemptionVulnerability_DummmyEnum"
  - 1："NOT_PREMPTABLE"
  - 2："PREEMPTABLE"

  **4G および Wi-Fi**：

  - 0 = 無効
  - 1 = 有効

- 切断理由（型：文字列）

  Disconnect-Reason には自明の文字列が含まれています。数値を保持する場合、文字列は次のように解釈されます。

  - PduRelReason_Error = 1
  - PduRelReason_SessIdleTimeout = 2
  - PduRelReason_SessCpIdleTimeout = 3

- PduRelReason_SessAbsoluteTimeout = 4

- RequestType（型：数値）
  - RequestType_DummyEnum = 0
  - INITIAL_REQUEST = 1
  - EXISTING_PDU_SESSION = 2
  - INITIAL_EMERGENCY_REQUEST = 3
  - EXISTING_EMERGENCY_PDU_SESSION = 4

- RequestIndication（タイプ：数値）
  - RequestIndication_DummyEnum = 0
  - UE_REQ_PDU_SES_MOD = 1
  - UE_REQ_PDU_SES_REL = 2
  - PDU_SES_MOB = 3
  - NW_REQ_PDU_SES_AUTH = 4
  - NW_REQ_PDU_SES_MOD = 5
  - NW_REQ_PDU_SES_REL = 6
  - EBI_ASSIGNMENT_REQ = 7

- AccessType （タイプ： 番号）
  - AccessType_DummyEnum = 0
  - AccessType_3GPP_ACCESS = 1
  - AccessType_NON_3GPP_ACCESS AccessType = 2

- PartialRecordMethod（タイプ：数値）
  - PartialRecordMethod_DummyEnum = 0
  - DEFAULT = 1
  - INDIVIDUAL = 2

- TriggerCategory（タイプ：数値）
  - TriggerCategory_DummmyEnum = 0
  - IMMEDIATE_REPORT = 1
  - DEFERRED_REPORT = 2

- TriggerType（タイプ：数値）
  - TriggerType_DummyEnum = 0

- QUOTA_THRESHOLD = 1
- QHT = 2
- FINAL = 3
- QUOTA_EXHAUSTED = 4
- VALIDITY_TIME = 5
- OTHER_QUOTA_TYPE = 6
- FORCED_REAUTHORISATION = 7
- UNUSED_QUOTA_TIMER = 8
- UNIT_COUNT_INACTIVITY_TIMER = 9
- ABNORMAL_RELEASE = 10
- QOS_CHANGE = 11
- VOLUME_LIMIT = 12
- TIME_LIMIT = 13
- PLMN_CHANGE = 14
- USER_LOCATION_CHANGE = 15
- RAT_CHANGE = 16
- UE_TIMEZONE_CHANGE = 17
- TARIFF_TIME_CHANGE = 18
- MAX_NUMBER_OF_CHANGES_IN_POWER_CONDITIONS = 19
- MANAGEMENT_INTERVENTION = 20
- CHANGE_OF_UE_PRESENCE_IN_PRESENCE_REPORTING_AREA = 21
- CHANGE_OF_3GPP_PS_DATA_OFF_STATUS = 22
- SERVING_NODE_CHANGE = 23
- REMOVAL_OF_UPF = 24
- ADDITION_OF_UPF = 25
- START_OF_SERVICE_DATA_FLOW = 26
- AMBR_CHANGE = 27

- Resourcestatus（タイプ：数値）
  - DummyEnum = 0
  - RELEASED = 1

- HostState（タイプ：数値）

- DummyEnum = 0
- NONE = 1
- PREPARING = 2
- PREPARED = 3
- COMPLETED = 4
- CANCELLED = 5

リストされる属性の詳細については、「EDR 属性 （393 ページ）」セクションの表を参照してください。

**手順 EDR の例**：

```
V1,15,2814,10:36.1,97,imsi-310310120106401,1287,N11SmContextCreateReq,imsi-310310120106401:5,,roaming-status:home|ue-type:nr-capable|supi:imsi-310310120106401
|gpsi:msisdn-12000006001|pei:imeisv-1031014232100100|psid:5|snssai:001|dnn:fast.t-mobile.com|emergency:false|rat:nr|access:3gpp
 access|connectivity:5g|udm-uecm:10.178.118.192
|udm-sdm:10.178.118.192|auth-status:unauthenticated,success,success,PDU Session
Establishment,N11SmContextCreateReq,Active,init_done|SETUP: Idle|SETUP: Await UDM
Registration|
SETUP: Await UDM Subscription
Fetch|finished,3,1287,V2,33,imsi-310310120106401,imeisv-1031014232100100,3.1031E+14,12000006001,msisdn-12000006001,Success,,2,1,,,193|,,,,,,,NR,
1|||,0100EC|310|310,1,1,,fast.t-mobile.com,3a4528c-851d-4728-856c-1b186ac992e5,310|310,0,,,5,0,0,3,1313,V2,4,Success,201,2,,3,1316,V2,4,Success,200,2,,3,1319,V2,4,Success,201,
2,,,,,,,
```

表 *106 : EDR* トランザクション コリジョン ファイル フィールド

| フィールド番号 | フィールド名 | フィールドの説明 |
|---|---|---|
| 1 | サブスクライバ ID | サブスクライバ ID 例えば、imsi-123456789012345 |
| 2 | コリジョン時間 | yyyyy/MM/dd HH:mm:ss.SSS 形式のコリジョンタイム。 |
| 3 | 解決の強制 | 解決が強制的に行われるかどうかを示します（true/false）。 |
| 4 | コリジョンの原因 | 衝突の原因。 |
| 5 | コリジョン前の新しいトランザクション | \| で区切られたコリジョン処理前の新しい状態のトランザクション。 |
| 6 | コリジョン前の保留中のトランザクション | \| で区切られたコリジョン処理前の保留状態のトランザクション。 |
| 7 | コリジョン前のアクティブ トランザクション | \| で区切られたコリジョン処理前のアクティブ状態のトランザクション。 |
| 8 | コリジョン前の中断されたトランザクション | \| で区切られたコリジョン処理前の一時停止状態のトランザクション。 |
| 9 | コリジョン後の新しいトランザクション | \| で区切られたコリジョン処理後の新しい状態のトランザクション。 |
| 10 | コリジョン後の保留中のトランザクション | \| で区切られたコリジョン処理後の保留状態のトランザクション。 |
| 11 | コリジョン後の現用系トランザクション | \| で区切られたコリジョン処理後のアクティブ状態のトランザクション。 |
| 12 | コリジョン後の一時停止トランザクション | \| で区切られたコリジョン処理後の一時停止状態のトランザクション。 |
| 13 | コリジョン後に中止されたトランザクション | \| で区切られたコリジョン処理後、中止状態のトランザクション。 |

**CSV フォーマット例**：

```
supi:imsi-123456789012345,2020/10/06
16:15:11.801,true,SessionLockSamePriority,17,,,,,,|17,,

supi:imsi-123456789012345,2020/10/06
16:15:11.824,true,SessionLockSamePriority,18,,,,,,|18,,

supi:imsi-123456789012345,2020/10/06
16:15:11.857,true,SessionLockSamePriority,19,,,,,,|19,,
```

```
supi:imsi-123456789012345,2020/10/06
16:15:11.883,true,SessionLockSamePriority,20,,,,,,|20,,

supi:imsi-123456789012345,2020/10/06 16:15:11.888,true,SessionLockRelease,,,,,,,,,x
```

# EDR 属性

このセクションでは、EDR 属性とそのサブ属性の詳細について説明します。

**表 *107 : QOS-RULE***

| QOS-RULE-LIST | qr-id\|qr-opcode\|qr-dqr\|qr-qfi\|qr-prededence\|num-filters\| **filters:**flter-id;flter-dir;cmp-type-m<br>cmp-type-proto;proto-id;cmp-type-local-addr;local-ip;<br>local-port;cmp-type-remote-addr;;remote-ip;cmp-type-remote-port;<br>remote-port;cmp-type-tos;tos-trffic-class | | | |
|---|---|---|---|---|
| | フィールド | サブ フィールド | サブサブ フィールド | プレゼンス |
| | QOS-RULE | | | |
| | | QOS-RULE-ID | | M |
| | | QOS-RULE-OPCODE | | M |
| | | QOS-RULE-DQR | | M |
| | | QOS-RULE-QFI | | M |
| | | QOS-RULE-PRECEDENCE | | M |
| | | NO-PKT-FILTERS | | |
| | | PKT-FILTER-LIST | | O |
| | | | PKT-FILTER-ID | M |
| | | | PKT-FILTER-DIRECTION | M |
| | | | CMP-TYPE-MATCH-ALL | O |
| | | | CMP-TYPE-PROTO | O |
| | | | PROTO-ID | O |
| | | | CMP-TYPE-LOCAL-ADDRESS | O |
| | | | LOCAL-IP-ADDRESS | O |
| | | | LOCAL-CMP-TYPE-PORT | O |
| | | | LOCAL-PORT | O |

| | | | | |
|---|---|---|---|---|
| | | | CMP-TYPE-REMOTE-ADDRESS | O |
| | | | REMOTE-IP-ADDRESS | O |
| | | | CMP-TYPE-REMOTE-PORT | O |
| | | | REMOTE-PORT | O |
| | | | CMP-TYPE-TOS | O |
| | | | TOS-TRAFFIC-CLASS | O |

（注） デリミタは、属性内の QOS-RULE の位置に基づいて変更される可能性があります。

表 *108 : QOS-DESC*

| **QOS-DESC** | [qfi\|opcode\|5qi\|arp\|mbr-ul\|mbr-dl\|gbr-ul\|gbr-dl] | |
|---|---|---|
| サブ フィールド | [タイプ（Type）] | プレゼンス |
| QFI | | M |
| Opcode | | M |
| 5QI | | O |
| ARP | ARP | O |
| MBR-UPLINK | | O |
| MBR-DOWNLINK | | O |
| GBR-UPLINK | | O |
| GBR-DOWNLINK | | O |

（注） デリミタは、属性内の QOS-DESC の位置に基づいて変更される可能性があります。

表 *109 : PCO*

| **PCO** | [タイプ \| PCSCF-ADDR-LIST \| DNS-ADDR-LIST\| pdu セッション ID \| QOS-RULE-LIST \| SESSION-AMBR\| QOS-DESC\|S-NSSAI\|ms-support-nw_addr-tft\|nw-support-nw_addr-tft\| PCSCF-ADDR-REQ\|DNS-ADDR-REQ\|mtu-req\|mtu-size] | | |
|---|---|---|---|
| サブ フィールド | [タイプ（Type）] | プレゼンス | |

| | | | |
|---|---|---|---|
| TYPE | 文字列 | M | EPCO または PCO または APCO |
| PCSCF-ADDR-LIST | PCSCF-ADDR | O | SMF から送信されている CSR 応答から |
| DNS-ADDR-LIST | DNS-ADDR | O | SMF から送信されている CSR 応答から |
| PDU-SESSION-ID | | O | SMF から送信されている CSR 応答から |
| QOS-RULE-LIST | QOS-RULE | O | SMF から送信されている CSR 応答から |
| SESSION-AMBR | SESS-AMBR | O | SMF から送信されている CSR 応答から |
| QOS-DESC | QOS-DESC | O | SMF から送信されている CSR 応答から |
| S_NSSAI | NSSAI | O | SMF から送信されている CSR 応答から |
| MS-SUPPORT-NW_ADDR-TFT | ブール | O | 受信元の CSR リクエスト |
| NW-SUPPORT-NW_ADDR-TFT | ブール | O | SMF から送信されている CSR 応答から |
| PCSCF-ADDR-REQ | PCSCF-ADDR-REQ | O | 受信元の CSR リクエスト |
| DNS-ADDR-REQ | DNS-ADDR-REQ | O | 受信元の CSR リクエスト |
| IPV4-MTU-REQUEST | ブール | O | 受信元の CSR リクエスト |
| IPV4-MTU-SIZE | 文字列 | O | SMF から送信されている CSR 応答から |

（注） 上記の表で、CSR 要求および CSR 応答メッセージは、4G および Wi-Fi のコールフローを参照しています。N11 SM コンテキスト作成要求および応答メッセージは 5G コールフローを参照します。

**表 *110 : PCSCF-ADDR-REQ***

| | |
|---|---|
| **PCSCF-ADDR-REQ** | [pco-pcsf-addr-ipv4-req;pco-pcsf-addr-ipv6-req] |

| サブ フィールド | プレゼンス | [タイプ（Type）] |
|---|---|---|
| PCO-PCSF-ADDR-IPV4-REQ | M | ブール |
| PCO-PCSF-ADDR-IPV6-REQ | M | ブール |

表 *111 : PCSCF-ADDR*

| **PCSCF-ADDR** | [ipv4-primary;ipv4-secondary;ipv4-tertiary;ipv6-primary;ipv6-secondary;ipv6-tertiary] | |
|---|---|---|
| サブ フィールド | プレゼンス | [タイプ（Type）] |
| PCSF-ADDR-IPV4-LIST | O | リスト |
| PCSF-ADDR-IPV6-LIST | O | リスト |

表 *112 : DNS* アドレス

| **DNS アドレス** | [ipv4-primary;ipv4-secondary;ipv4-tertiary;ipv6-primary;ipv6-secondary;ipv6-tertiary] | |
|---|---|---|
| サブ フィールド | プレゼンス | [タイプ（Type）] |
| DNS-ADDR-IPV4-LIST | O | リスト |
| DNS-ADDR-IPV6-LIST | O | リスト |

表 *113 : DNS-ADDR-REQ*

| **DNS-ADDR-REQ** | [pco-pcsf-addr-ipv4-req;pco-pcsf-addr-ipv6-req] | |
|---|---|---|
| サブ フィールド | プレゼンス | [タイプ（Type）] |
| PCO-PCSF-ADDR-IPV4-REQ | M | ブール |
| PCO-PCSF-ADDR-IPV6-REQ | M | ブール |

表 *114 : NSSAI*

| **NSSAI** | [sst\|sd\|hplmnsst\|hplmnsd] | |
|---|---|---|
| サブ フィールド | プレゼンス | [タイプ（Type）] |
| SST | M | 番号 |
| SD | O | 文字列 |
| HPLMN-SST | O | 番号 |
| HPLMN SD | O | 文字列 |

（注） デリミタは、属性内の S-NSSAI の位置に基づいて変更される可能性があります。

表 *115 : PAA*

| **PAA** | [ipv4-addr\|ipv6-addr] | |
|---|---|---|
| サブ フィールド | プレゼンス | [タイプ（Type）] |
| IPV4-ADDR | O | 文字列 |
| IPV6-ADDR | O | 文字列 |

表 *116 : N1N2MSGREQCONTENT* または *N1N2MSGRSPCONTENT*

| N1N2MSGREQCONTENT\|N1N2MSGRSPCONTENT | [msg-type\|cause] | |
|---|---|---|
| サブ フィールド | プレゼンス | [タイプ（Type）] |
| MSG-TYPE | M | SMF N1N2MsgType |
| 原因 | O | 文字列 |

**例:** 195|REQUEST_REJECTED_UNSPECIFIED

表 *117 : PLMN-ID*

| **PLMN-ID** | [mcc\|mnc] |
|---|---|
| サブ フィールド | プレゼンス |
| MCC | M |
| MNC | M |

（注） 区切り文字は、親属性の PLMN-ID の位置に基づいて変更される可能性があります。

表 *118 : GUAMI*

| **GUAMI** | [amf-id\|plmn-id] | |
|---|---|---|
| サブ フィールド | プレゼンス | [タイプ（Type）] |
| AMF-ID | M | 文字列 |
| PLMN-ID | M | PLMN-ID |

表 *119 : SESS-AMBR*

| **SESS-AMBR** | [ambr-dl\|ambr-ul] | |
|---|---|---|
| サブ フィールド | プレゼンス | [タイプ（Type） |
| AMBR-DL | O | 文字列 |
| AMBR-UL | O | 文字列 |

表 *120 : UE-LOCATION*

| **UE-LOCATION** | [locationType\|**Ecgi:** ECGI\|**Tai:**TAI] または<br>[locationType\|**Ncgi:** NCGI\|**Tai:**TAI] | | |
|---|---|---|---|
| サブ フィールド | プレゼンス | [タイプ（Type）] | — |
| locationType | M | 文字列 | 「 |
| ECGI または NCGI | O | ECGI/NCGI | — |
| Tai | O | TAI | — |

表 *121 : ECGI* または *NCGI*

| **ECGI/NCGI** | [plmn-id;cellId] | |
|---|---|---|
| サブ フィールド | プレゼンス | [タイプ（Type）] |
| Plmn-id | M | PLMN-ID |
| Cell-id | M | 文字列 |

表 *122 : TAI*

| **TAI** | [plmn-id; tac] | |
|---|---|---|
| サブ フィールド | プレゼンス | [タイプ（Type）] |
| Plmn-id | M | PLMN-ID |
| Tac | M | 文字列 |

表 *123 : ARP*

| 『**ARP**』 | [preEmpCap;preEmpVul;priority] | |
|---|---|---|
| PRE-EMP-CAP | M | PreemptionCapability |
| PRE-EMP-VUL | M | PreemptionVulnerabi |

| | | |
|---|---|---|
| 優先度 | M | 番号 |

（注） 属性内の ARP の位置に基づいて変更される可能性があるデリミタ。

表 *124 : NCAP-CAUSE*

| **NCAP-CAUSE** | [group\|value] | |
|---|---|---|
| GROUP | O | 番号 |
| VALUE | O | 番号 |

表 *125 : TUNNEL-INFO*

| **TUNNEL-INFO** | [gtp-teid\|ipv4-addr\|ipv6-addr] | |
|---|---|---|
| GTP-TEID | O | 文字列 |
| IPV4-ADDR | O | 文字列 |
| IPV6-ADDR | | 文字列 |

表 *126 : QFS*

| **QFS** | [qos-rule\|qos-desc] | |
|---|---|---|
| Qos-rules | O | QOS-RULE |
| QOS-DESC | O | QoS-DESC |

表 *127 : CHARGING-PROF*

| **CHARGING-PROF** | partial-rec-method\|category:max-cc:time-limit;type:vol-limit | | | |
|---|---|---|---|---|
| | PARTIAL-REC-METHOD | | | PartialRecordMethod |
| | TRIGGERS-LIST | TRIGGERS | CATEGORY | TriggerCategory |
| | | | MAX-CCC | |
| | | | TIME-LIMIT | |
| | | | TYPE | TriggerType |
| | | | VOL-LIMIT | |

表 *128 : BEARER-CTX*

| **BEARER-CTX** | [ebi\|pkt-flow-id\|cause\|pco\|tft\|fqteid\|qos-desc\|charging-id] |
|---|---|

| サブ フィールド | プレゼンス | [タイプ（Type）] |
|---|---|---|
| EBI/LBI | M | |
| PKT-FLOW-ID | O | |
| CAUSE | O | |
| PCO | O | PCO |
| TFT | O | |
| FQTEID | O | |
| QoS-DESC | O | QoS-DESC |
| CHARGING-ID | O | |

SMF は、イベントごとにフィールド レベルの詳細を含む詳細レコードを生成します。次の表に、さまざまな N1N2 メッセージおよび関連 ID を示します。

表 *129 : SMF N1N2* メッセージ タイプ

| **MESSAGE** | **MESSAGE-ID** |
|---|---|
| PDU-SESSION-ESTB-REQUEST | 193 |
| PDU-SESSION-ESTB-ACCEPT | 194 |
| PDU-SESSION-ESTB-REJECT | 195 |
| PDU-SESSION-MOD-REQ | 201 |
| PDU-SESSION-MOD-CMD | 203 |
| PDU-SESSION-MOD-CMD-REJ | 202 |
| PDU-SESSION-MOD-CMD-COMP | 204 |
| PDU-SESSION-REL-REQ | 209 |
| PDU-SESSION-REL-CMD | 211 |
| PDU-SESSION-REL-REJ | 210 |
| PDU-SESSION-REL-COMP | 212 |
| N2_PDU_SESSION_RESOURCE_RELEASE_COMMAND | 76 |
| N2_PDU_SESSION_RESOURCE_RELEASE_RESPONSE | 130 |
| N2_PDU_SESSION_RESOURCE_SETUP_REQUEST | 77 |
| N2_PDU_SESSION_RESOURCE_SETUP_RESPONSE_TRANSFER | 78 |
| N2_PDU_SESSION_RESOURCE_MODIFY_CONFIRM_TRANSFER | 62 |
| N2_PDU_SESSION_RESOURCE_MODIFY_INDICATION_TRANSFER | 63 |
| N2_PDU_SESSION_RESOURCE_MODIFY_REQUEST_TRANSFER | 64 |

| | |
|---|---|
| N2_PDU_SESSION_RESOURCE_MODIFY_RESPONSE_TRANSFER | 65 |
| N2_PDU_SESSION_RESOURCE_MODIFY_UNSUCCESS_TRANSFER | 79 |
| N2_PDU_SESSION_HANDOVER_PREP_UNSUCCESS_TRANSFER | 93 |
| N2_PDU_SESSION_HANDOVER_COMMAND_TRANSFER | 91 |
| N2_PDU_SESSION_PATH_SWITCH_REQUEST_ACK_TRANSFER | 84 |
| N2_PDU_SESSION_PATH_SWITCH_REQUEST_UNSUCCESS_TRANSFER | 97 |
| N2_PDU_SESSION_PATH_SWITCH_REQUEST_TRANSFER | 82 |
| N2_PDU_SESSION_HANDOVER_REQUIRED_TRANSFER | 85 |
| N2_PDU_SESSION_HANDOVER_REQUEST_ACK_TRANSFER | 87 |
| N2_PDU_SESSION_HANDOVER_RESOURCE_ ALLOC_UNSUCCESS_TRANSFER | 89 |
| N2_PDU_SESSION_PATH_SWITCH_REQUEST_SETUP_FAILED_TRANSFER | 95 |
| N2_PDU_SESSION_RESOURCE_SETUP_UNSUCCESS_TRANSFER | 99 |
| N2_PDU_SESSION_RESOURCE_NOTIFY_TRANSFER | 101 |
| N2_PDU_SESSION_SECONDARY_RAT_USAGE_TRANSFER | 103 |
| N2_PDU_SESSION_RESOURCE_NOTIFY_RELEASED_TRANSFER | 105 |
| N2_PDU_SESSION_RESOURCE_SETUP_FAIL_TRANSFER | 107 |
| N2_PDU_SESSION_PATH_SWITCH_SETUP_FAIL_TRANSFER | 109 |
| N2_PDU_SESSION_HANDOVER_RESPONSE_ ALLOC_FAIL_TRANSFER | 111 |

# 制限事項

EDR ロギング機能には次の制限があります。

- 次のシナリオでは、イベント レコード生成は機能しません。
  - Xn HO、N2 HO、5G から 4G HO、4G から 5G HO、5G から Wi-Fi HO、および Wi-Fi から 5 G HO を除くすべてのハンドオーバー（HO）手順
  - アイドルからアクティブへの遷移
  - アクティブ/アイドルの遷移
  - 4G PDN の変更
- SMF は、IMSI（SUPI）ベースの EDR レポートのみをサポートします。
- SMF は現在、CSV 形式での EDR 生成をサポートしています。EDR ファイルのストレージ形式は設定できません。
- この機能は、着信要求に明示的に応答を送信しない手順には適用されません。

# EDR の構成

ここでは、EDR ロギング機能の構成方法について説明します。

## EDR レポートの構成

（注） EDR の生成は、サブスクライバ ID の構成後に発生します。次に、特定のサブスクライバまたはすべてのサブスクライバに対して EDR レポートを有効にできます。すべてのサブスクライバの EDR レポートを有効にしている場合、SMF は個々のサブスクライバ ID 構成を無視します。

（注） パフォーマンスを最適化するために、特定の手順 ID を持つサブスクライバのサブセットに対してのみ EDR レポートを有効にすることをお勧めします。

サブスクライバの EDR 生成を有効または無効にするには、次の構成例を使用します。

```
config
    edr reporting { enable [ all subscribers | file [ transaction |
transaction-collision ] ] | disable file [ transaction |
transaction-collision ] }
    edr all subscribers
    end
```

注：

- **edr reporting { enable [ all subscribers | file [ transaction | transaction-collision ] ] | disable file [ transaction | transaction-collision ] }**：SMF での EDR レポートを構成するには、このキーワードを指定します。EDR レポート機能を有効にするには、**edr reporting enable** コマンドを使用します。特定のファイルの EDR レポート機能を無効にするには、 **edr reporting disable***file* コマンドを使用します。デフォルトでは、EDR の生成は無効になっています。
- **edr reporting enable all subscribers** コマンドまたは **edr all subscribers** を使用して、すべてのサブスクライバの EDR を有効にします。

（注）

- サブスクライバの EDR レポートを有効にするには、 **edr subscribers** *subscriber_id* コマンドを使用します。 *subscriber_id* は英数字の文字列である必要があります。デフォルト値は空です。このコマンドでは、正確なサブスクライバキーを指定してください。SMF は、IMSI（SUPI）ベースの EDR レポートのみをサポートします。
- EDR レポートを有効にするときに、少なくとも 1 つのサブスクライバを構成します。
- トランザクション衝突 EDR を生成するために、最大 10 のサブスクライバを構成できます。

# EDR ファイルの生成の構成

トランザクション レベルで EDR イベントを生成するには、次の構成例を使用します。

```
config
   edr file { transaction | transaction-collision }
      procedure-id procedure_value
         event-id event_value
            field-id field_value
            end
```

- **edr file { transaction | transaction-collision }**：サブスクライバ セッションのトランザクションまたはトランザクションコリジョン レベルの詳細を含む EDR ファイルを生成するように指定します。
- **procedure-id** *procedure_value*：イベント レポートを有効にする必要がある手順 ID または手順名を指定します。
- **event-id** *event_value*：イベント レポートを有効にする必要があるイベント ID またはイベント名を指定します。
- **field-id** *field_value*：イベント レポートを有効にする必要があるフィールド ID またはフィールド名を指定します。
- アプリケーションによって登録されたすべての手順 ID、イベント ID、およびフィールド ID はデフォルトで有効になっています。
- 1 つ以上の手順が有効になっている場合、他のすべての手順は無効になり、トランザクション EDR に入力されません。同様に、手順で 1 つ以上のイベントを有効にすると、その手順で他のすべてのイベントは無効になり、トランザクション EDR に入力されません。
- 手順 ID が無効になっている場合、手順 ID に対してイベント開始、追加フィールド、またはイベント終了は行われません。

- 手順 ID 内で event-id が無効になっている場合、event-start、event-end、または add フィールドは、手順 ID と event-id の組み合わせに対して適用されません。
- field-id が event-id に対して無効になっている場合、add-field は適用されず、CSV エントリの値の代わりに空白のエントリが表示されます。

**設定例**：

```
edr file transaction
  procedure-id 24 32
  procedure-id 25
    event-id 5 7 8
    event-id 5
      field-id 10 12 14
```

上記の例では、 **event-id 5 7 8** は、手順 ID 25 のイベント ID 5、7、および 8 を有効にすることを意味します。 **field-id 10 12 14** は、手順 ID 25 とイベント ID 5 のフィールド ID 10、12、および 14 を有効にすることを意味します。

# EDR パラメータの構成

EDR パラメータを定義するには、次の構成例を使用します：

```
config
   [ no ] edr file transaction
      field priorityClass
      flush interval file_flush_interval
      limit [ size file_size | count file_count| storage edr_storage_size ]
      procedure procedure_value event event_value field field_value
      rate rate_value
      reporting [ disable | enable ]
      threshold [ cpu cpu_threshold | session session_thresold  ]
      end
```

**注**：

- **field priorityClass**：メッセージの優先順位クラスを指定します。メッセージはデフォルト優先順位メッセージまたは高優先順位メッセージになります。この CLI を有効にすると、EDR トランザクション ファイルに、次の 2 つの値のいずれかを含む追加のフィールドが表示されます：
  - DefaultPriority
  - HighPriority
- **flush interval** *file_flush_interval*：EDR ファイルをフラッシュする間隔をミリ秒単位で指定します。デフォルト値は 1000 ミリ秒です。
- **limit [ size** *file_size* **| count** *file_count*| **storage** *edr_storage_size*]：ファイル関連の制限を指定します。

- **limit size** *file_size* コマンドを使用して、EDR ファイルの最大サイズを指定します。最大サイズを指定すると、EDR ファイルが圧縮され、新しい CSV ファイルが作成されます。デフォルトのファイル サイズは 100 MB です。

  *file_size* は、1 ～ 20 の範囲の整数で指定する必要があります。

（注） システムは、EDR ファイルのサイズを 1 秒に 1 回、また構成されたフラッシュ間隔の後のいずれか大きい方の値を定期的にモニターします。EDR ファイルが最大サイズに達すると、圧縮され、新しい CSV ファイルが作成されます。ただし、一部のシナリオでは、前述のしきい値制限に基づいて定期的なチェックをシステムが実行する直前に、データが EDR ファイルに継続的に書き込まれます。これにより、構成されている最大ファイル サイズをわずかに超える EDR ファイルが生成されます。

- **limit count** *file_count* コマンドを使用して、保持する EDR ファイルの最大数を指定します。デフォルトのファイル数は 10 です。

  *file_count* は、2 ～ 128 の範囲の整数である必要があります。

  構成されたファイル数に達すると、ファイルは永続ボリュームに移動されてから削除されます。

- **limit storage** *edr_storage_size* コマンドを使用して、永続ボリュームの EDR ストレージ サイズを GiB 単位で指定します。

  *edr_storage_size* は 、0 ～ 64 の範囲の整数である必要があります。Edr-monitor ポッドで永続ボリュームを無効にするには、値を 0 に設定します。デフォルトのストレージ サイズは 24 GiB です。

重要 ストレージ制限は「system mode shutdown」モードでのみ変更できます。したがって、永続ボリュームの無効化は、システムがシャットダウン状態のときにのみ実行できます。

- **procedure** *process_value* **event** *event_value* **field** *field_value*：トランザクション レベルの手順 ID 構成情報を指定します。*process_value* は、手順 ID または手順名である必要があります。*event_value* は 、フィールド値とともにイベント ID またはイベント名である必要があります。

（注）

- デフォルトでは、application-start 時に登録されたすべての手順 ID、イベント ID、およびフィールド ID が有効になります。
- 1 つ以上の手順が有効になっている場合、他のすべての手順は無効になり、トランザクション EDR に入力されません。
- 手順で 1 つ以上のイベントが有効になっている場合、その手順の他のすべてのイベントは無効になり、トランザクション EDR に入力されません。
- イベントで 1 つ以上のフィールドが有効になっている場合、そのイベント内の他のすべてのフィールドは無効になり、トランザクション EDR に入力されません。
- 無効な手順 ID の場合、event-start、add field、または event-end は受け入れられません。
- 手順 ID 内の無効なイベント ID の場合、その手順 ID とイベント ID の組み合わせに対しては、event-start、event-end、または add フィールドは適用されません。
- イベント ID 内の無効なフィールド ID の場合、追加フィールドは尊重されず、CSV エントリの値の代わりに空白のエントリが使用できます。

- **rate** *rate_value* ：EDR レコード生成の許容レートを 1 秒あたりに指定します。デフォルトレートは 4096 です。

  *rate_value* は、32 ～ 65535 の範囲の整数を指定できます。

  EDR 生成レート制限に達すると、トランザクション EDR がドロップされ、生成された EDR、ドロップされた、ドロップ理由などを追跡するためのメトリックが追加されます。レート制限は、サービス（smf-service）ポッドインスタンスごとに実行されることに注意してください。

- **reporting [ disable | enable ]**：レポートを有効または無効にする必要があるファイルを指定します。

重要　edr-monitor ポッドは、トランザクション EDR が有効な場合にのみ生成されます。

- **threshold [ cpu** *cpu_threshold* **| session** *session_thresled* **]**：EDR の生成を制限するしきい値を指定します。

- CPU しきい値をパーセンテージで構成するには、 **threshold cpu** *cpu_threshold* コマンドを使用します。SMF サービス ポッド インスタンスのしきい値に違反すると、アプリケーションは EDR の生成を停止します。*cpu_threshold* は 、1 ～ 100 の範囲の整数である必要があります。デフォルト値は 80% です。
- **threshold session** *session_threshold* コマンドを使用して、GR インスタンスごとのセッションしきい値を構成します。GRインスタンスのしきい値に違反すると、アプリケーションは EDR の生成を停止します。 *session_threshold* は 、0 ～ 1,000,000 の範囲の整数である必要があります。デフォルト値は 100,000 です。

（注） ラックがアクティブ-アクティブモードで動作している場合、セッションしきい値は両方のGRインスタンスに個別に適用されます。

# EDR トランザクションを確認する

現在登録されているアプリケーションの手順、イベント、およびフィールドと、それぞれの ID を表示するには次の show コマンドを使用します。

**show edr transaction-procedure** *procedure_id* **event** *event_id*

**show edr event** *event_id*

すべての手順とイベントを提供できます。それ以外の場合は、特定の手順名とイベント名、または手順 ID とイベント ID を指定できます。

（注） show コマンド出力は、アプリケーションによって登録されたマッピングに基づきます。

次に、show コマンドの出力例を示します。

```
Procedure-id 20, Procedure-Name: xyz
    Event-id 1, Event-Name: abc
         1 - Field1-Name
         2 - Field2-Name
         …
         …
         …
     Event-id 2, Event-Name: efgh
          1 - Field1-Name
          2 - Field2-Name
          …
          …
          …
    …
    …
    …
Procedure-id 21, Procedure-Name: bbbb
     Event-id 1, Event-Name: cccc
          1 - Field1-Name
          2 - Field2-Name
          …
```

```
        …
        …
Event-id 2, Event-Name: dddd
        1 - Field1-Name
        2 - Field2-Name
        …
        …
        …
```

この出力は、オペレータが特定のプロシージャ ID とイベント ID のペアの現在の CSV 形式を知るのに役立ちます。

# EDR ロギングの OAM サポート

ここでは、この機能の操作、管理、およびメンテナンスに関して説明します。

## バルク統計サポート

### EDR トランザクションと EDR レポートのバルク統計情報

SMF は、この機能の一部として次のバルク統計情報を維持します。

- edr_error_total

  **ラベル**：

  - error_code：EDR 書き込みエラー コード

このメトリックは、EDRの書き込み中にエラーが発生するたびにペグされます。このメトリックでは、書き込みキューがいっぱいになり、EDR がドロップされた場合、error_code として「EdrQueueFull」が表示されます。

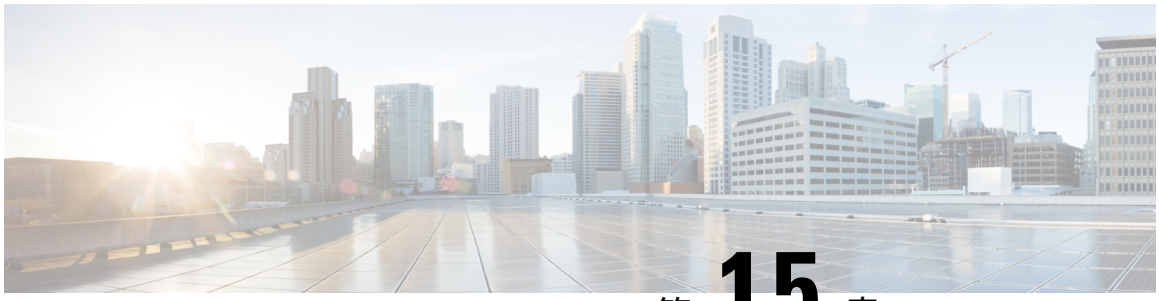
次のメトリックは、EDR数とステータスをモニタするために使用されます。

- edr_total

  **ラベル**：

  - name：トランザクション EDR の名前。
  - ステータス：EDRトランザクションのステータス（成功したかエラーが発生したか）。
  - status_code：次のステータス コードがサポートされています：
    - EdrReportingDisabled
    - EdrTxnReportingDisabled
    - EdrSessThreshold
    - EdrCpuThreshold
    - EdrRateLimitExceeded
    - EdrFileWriteFailed

- EdrInvalidEdrId
- EdrQueueFull
- EdrIgnored_NoEventRecorded



第 15 章

# 障害処理サポート


- 機能の概要と変更履歴 （411 ページ）
- 機能説明 （412 ページ）
- アクセスおよびモビリティ管理機能の障害処理 （413 ページ）
- 充電機能の失敗の処理 （415 ページ）
- ネットワーク リポジトリ機能障害処理 （427 ページ）
- ポリシー制御機能の失敗の処理 （442 ページ）
- 統合データ管理の失敗の処理 （448 ページ）
- ユーザー プレーン機能障害の処理 （456 ページ）


## 機能の概要と変更履歴

### 要約データ

**表 *130* : 要約データ**

| | |
|---|---|
| 該当製品または機能エリア | SMF |
| 該当プラットフォーム | SMI |
| 機能のデフォルト設定 | 無効：設定が必要 |
| このリリースでの関連する変更点 | N/A |
| 関連資料 | 該当なし |

# 更新履歴

表 *131 :* マニュアルの変更履歴

| 改訂の詳細 | リリース |
|---|---|
| 原因コード 0 ～ 255 をサポートするように N4SessionModificationReq メッセージの既存の失敗処理の構成を拡張しました。 | 2021.02.3 |
| N4SessionModificationReq メッセージの既存の失敗処理の構成を拡張し、事前定義された手順に基づいてセッション終了を制御する条件を含めました。 | 2021.02.3 |
| 次の要求メッセージの再送信のサポートが追加されました。<br>• Namef_Communication EBI 割り当て要求<br>• Namef_CommunicationN1N2 メッセージ転送要求 | 2021.02.2 |
| PCF および UDM 構成の **response-timeout** コマンドに許容される範囲の値を追加しました | 2021.02.0 |
| RAT タイプ FHT のサポートとグレースフル タイムアウトの処理、および関連する統計情報が導入されました。 | 2021.01.0 |
| 最初の導入。 | 2020.02.0 より前 |

# 機能説明

システムは、エラー コードを回復可能なエラー コードと回復不可能なエラー コードに分離することにより、エラー処理を実行します。SMF が NF 登録、NF 更新、NF ハートビートなどのメッセージで NRF サーバから回復可能なエラーを受信すると、継続的な再試行でエンドポイントの回復を試みます。この機能は、課金機能（CHF）、ネットワーク リポジトリ機能（NRF）、ポリシー制御機能（PCF）、統合データ管理（UDM）とユーザー プレーン機能（UPF）などの NRF 連携動作と SMF およびその他のネットワーク機能との相互作用中に発生するエラーを柔軟に処理する方法を提供します。

この機能は、次の機能をサポートしています。

- NRF と他の NF との相互作用中に発生する特定のエラー コードに対する構成可能な再試行アクション。
- NRF 内のすべてのエンドポイントを再試行した後、エラー コードの再試行アクションを柔軟に決定できます。
- **profile nf-client-failure** テンプレートの下にある CLI 構成を使用して、NRF メッセージのエラー コードと対応する再試行アクションを構成します。NRF のすべてのエンドポイン

トを再試行した後、エラー コードのフェールオーバー オプションを設定することもできます。

- 他の NF の障害処理テンプレートで、HTTPv2 ステータス コード範囲のサポートを提供します。

# アクセスおよびモビリティ管理機能の障害処理

## 機能説明

SMF はアクセスおよびモビリティ管理機能（AMF）の障害処理をサポートします。要求メッセージに基づいて、SMF は同じエンドポイントへの再送信をサポートします。

## 機能の仕組み

SMF は、次の要求メッセージの再送信サポートを提供します：

- Namef_Communication EBI 割り当て要求
- Namef_CommunicationN1N2 メッセージ転送要求

SMF が上記のメッセージに対する応答を受信しない場合、SMF は同じエンドポイントにメッセージを再送信します。SMF はこれらのメッセージをAMFに送信した後、内部に構成されたタイマーを開始します。SMF が AMF からの応答を受信した後、タイマーは停止します。応答の待機中にタイマーが期限切れになった場合、SMFは、再試行回数が設定された再試行メカニズムを使用します。

## 要求メッセージの再送信の構成

Namef_Communication EBI Assignment および Namef_Communication EBI Assignment メッセージの再送信を設定するには、次の構成例を使用します：

```
config
  profile nf-client-failure nf-type amf
     profile failure-handling failure_handling_name
     service name type namf-comm
      message type { AmfCommEBIAssignment | AmfCommN1N2MessageTransfer
 | AmfCommSMStatusChangeNotify }
        status-code httpv2 status_code
        retransmit retransmit_value
        retransmit interval retransmit_interval_value
        retry retry_value
        action retry-and-continue
     exit
  exit
```

注：

- **service name type namf-comm**：AMF サービス名のタイプを「namf-comm」として指定します。
- **message type { AmfCommEBIAssignment | AmfCommN1N2MessageTransfer | AmfCommSMStatusChangeNotify }**：namf-comm AMF サービス名タイプのメッセージ タイプを **AmfCommEBIAssignment**、 **AmfCommN1N2MessageTransfer**、または **AmfCommSMStatusChangeNotify** として指定します。
- **status-code httpv2** *status_code* ：サービスのステータス コードを指定します。 *status_code* は 0 ～ 599 の範囲の整数である必要があります。
- **retransmit** *retransmit_value*：同じエンドポイントの最大再送信値を指定します。 *retransmit_value* は、1 ー 10 の範囲の整数である必要があります。

  SMF がメッセージを送信して HTTP ステータス コードのエラーを受信した場合に、有効な再送信回数が設定されていれば、その回数の再送信が同じエンドポイントに対して行われます。最大再送信回数は、HTTP ステータス コードの初回設定から使用されます。

  SMF が再送信後も失敗エラーの HTTP コードを受信する場合、SMF は次の条件で同じエンドポイントに再送信します。

  - SMF が受信した最初の HTTP ステータス コードに有効な再送信回数が設定されている場合。
  - 受信したHTTPエラー コードの有効な再送信回数（ゼロであってはなりません）が存在する場合。

- **retransmit interval** *retransmit_interval_value*：再送信間隔の値をミリ秒単位で指定します。デフォルト値は 1000 です。

  再送信間隔が構成されている場合、SMF は再送信間のタイムアウトを待ちます。
- **retry** *retry_value*：使用可能な別のエンドポイントへの再試行回数を指定します。 *retry_value* は、1 ー 10 の範囲の整数である必要があります。
- **action retry-and-continue**：構成された再試行回数に従って再試行回数を指定し、セッションを続行します。

## 設定例

次に、Namef_Communication EBI Assignment メッセージの再送信の構成例を示します：

```
config
  profile nf-client-failure nf-type amf
    profile failure-handling FHAMF
    service name type namf-comm
      message type AmfCommEBIAssignment
      status-code httpv2 504
      retransmit 1
      retransmit interval 1000
```

```
        retry 1
        action retry-and-continue
      exit
    exit
```

# 充電機能の失敗の処理

## 機能説明

***Table 132:*** 機能の履歴

| 機能名 | リリース情報 | 説明 |
|---|---|---|
| 料金設定グループおよびアプリケーション レベルでの CHF の失敗の処理 | 2024.01 | SMF では、構成可能なアクションを定義して、アプリケーション エラーおよび料金設定グループ ID に関連付けられた障害を処理できます。<br>この機能により、新しい **failure-handling error-type [ rg \| app ]** コマンドが課金プロファイル構成に導入されました。詳細については、 profilecharge failure-handling error-type コマンドを参照してください。<br>**デフォルト設定**：無効：構成が必要 |

SMF は、課金機能（CHF）サーバの障害処理をサポートしています。オンライン CHF サーバで障害が発生した場合、SMF はオフラインの CHF サーバに課金情報をリレーします。

課金情報のシームレスな転送のために、SMF は CHF 障害処理プロファイルに関連付けられた構成を呼び出します。障害処理を構成済みの場合、SMF は、別のプロファイルに構成されている、選択された CHF のセッションを続行します。

SMF は、次のレベルで課金機能（CHF）サーバの障害処理をサポートします。

- HTTP レベルのステータス コード
- アプリケーションレベルのエラー コード
- 料金設定グループレベルの結果コード

アプリケーション エラーに対して以下のアクションを構成できます。

- ドロップ データ：課金 ID に対応するドロップ データ。

- 終了：PDU セッションを解放します。
- 続行：課金を無効にします。

料金設定グループのエラーに対して以下のアクションを構成できます。

- オフラインへの変換：オフライン課金に変換します。
- フローの削除：料金設定グループに関連付けられているフローまたはルールを削除します。
- ドロップ データ：料金設定グループに対応するトラフィックをドロップします。
- 終了：PDU セッションを解放します。

構成がなければ、SMF はデフォルトの動作を続けます。デフォルトの動作については、表 5 および表 6 を 参照してください。

課金サーバーの選択方法については、このガイドの 「サブスクライバの課金, on page 1853」の章の 「CHF の選択, on page 1862」セクションを参照してください。

# 機能の仕組み

このセクションは、課金機能のオフライン フェールオーバー サポートの機能の仕組みを説明します。

## CHF サーバ障害の処理

CHF サーバー障害は、選択した CHF が障害応答を送信するか、応答を送信しない場合に発生します。CHF サーバーの障害の場合、NF ライブラリは障害テンプレートに基づくステータス コードを送信します。このテンプレートは、CHF ネットワーク プロファイルに関連付けられています。smf-service は、IPC メッセージの送信中にプロファイル情報を smf-rest-ep に送信します。

失敗テンプレートには、必要に応じて、HTTP エラーコードのリストと、関連する失敗アクションと再試行回数が設定されます。この機能は、機能不全発生時のアクションをサポートしています。

- [再試行して続行（Retry and Continue）]：この失敗アクションの場合、NF ライブラリはフォールバック前に構成された回数だけ試行します。設定された回数が完了すると、NF ライブラリは優先順位の低い CHF サーバーの IP アドレスにフォールバックします。失敗した場合、または CHF サーバーから応答を受信しない場合は、「続行」アクションが smf サービスに返されます。
- Terminate：この失敗アクションの場合、NF ライブラリは他の CHF サーバーにメッセージの送信を試みません。ライブラリは、アクションが「terminate」として、smf-service に応答を送信します。「terminate」の失敗アクションの場合、smf-service はセッションを削除します。

- [続行（Continue）]：この失敗アクションでは、smf-service はセッションを続行し、オフライン CHF サーバーに課金メッセージを送信します。このサーバーは、オフライン用のローカル静的 CHF プロファイルの一部として構成されています。また、オフライン CHF の障害処理プロファイルを構成します。

**Note** 「続行」失敗アクションの場合は、別のプロファイルの SMF でオフライン CHF サーバーを構成できます。SMF は、CHF サーバーの障害発生後、このプロファイルを使用します。オフライン CHF サーバーが構成されていない場合、セッションは課金を課さずに続行されます。

## オフライン CHF サーバへのリレー

CHF サーバで障害が発生した後、SMF が続行すると、進行中の課金サービスが次のように変換されます。

- オンラインとオフラインの両方の課金方式を持つサービスをオフラインの課金方式に変換します。
- オンライン課金方式のサービスをオフライン課金方式に変換します。
- オフライン課金方式のサービスに変更はありません。

## HTTP 原因コードと失敗アクションのマッピング

次の表に、関連する HTTP 原因コードと失敗アクションのマッピングを示します。ネットワーク要件に基づいて、マッピングを変更できます。

***Table 133: HTTP* 原因コードと失敗アクションのマッピング**

| **HTTP-2 原因コードと説明** | | **コンバージド CHF 障害時のアクション** | | | **オフライン CHF 障害時のアクション** | | |
|---|---|---|---|---|---|---|---|
| コード | 説明 | CDR-I | CDR-U | CDR T | CDR-I | CDR-U | CDR T |
| 400 | Bad Request | Terminate | 構成なし | 構成なし | Terminate | 構成なし | 構成なし |
| 403 | Forbidden | Terminate | 構成なし | 構成なし | Terminate | 構成なし | 構成なし |
| 404 | 見つかりません | Terminate | 構成なし | 構成なし | Terminate | 構成なし | 構成なし |
| 405 | メソッドは許可されていません | 再試行して続行 | 再試行して続行 | 再試行して続行 | Terminate | 構成なし | 構成なし |
| 408 | Request Timeout | 再試行して続行 | 再試行して続行 | 再試行して続行 | Terminate | 再試行して続行 | 再試行して続行 |
| 500 | Internal Server Error | 再試行して続行 | 再試行して続行 | 再試行して続行 | Terminate | 再試行して続行 | 再試行して続行 |

| HTTP-2 原因コードと説明 | | コンバージド CHF 障害時のアクション | | | オフライン CHF 障害時のアクション | | |
|---|---|---|---|---|---|---|---|
| 503 | Service Unavailable | 再試行して続行 | 再試行して続行 | 再試行して続行 | Terminate | 再試行して続行 | 再試行して続行 |
| 508 | ゲートウェイのタイムアウト（Gateway Timeout） | 再試行して続行 | 再試行して続行 | 再試行して続行 | Terminate | 再試行して続行 | 再試行して続行 |
| 0 | サーバからの応答がありません | 再試行して続行 | 再試行して続行 | 再試行して続行 | Terminate | 再試行して続行 | 再試行して続行 |

## アプリケーション エラー コードベースの障害処理

次の表に、アプリケーション エラー結果コードと関連する SMF 障害処理を示します。

**表 *134* : アプリケーション エラー結果コードと *SMF* 障害処理アクションとのマッピング**

| アプリケーション エラー結果コード | SMF 障害処理アクション |
|---|---|
| CHARGING_NOT_APPLICABLE | セッションの終了 |
| END_USER REQUEST_DENIED | セッションの終了 |
| QUOTA_LIMIT_REACHED | セッションのトラフィックをドロップする |
| END_USER_REQUEST_REJECTED | セッションの終了 |

## 料金設定グループレベルの失敗の処理

下表に、料金設定グループレベルのエラー結果コードと、関連する SMF 失敗の処理アクションを示します。

**表 *135* : *SMF* 失敗処理アクションとの評価グループ レベルのエラー結果コードのマッピング**

| 料金設定グループ レベルのエラー結果コード | SMF 障害処理アクション |
|---|---|
| RATING_FAILED | 料金グループに該当するトラフィックをドロップする |
| QUOTA_MANAGEMENT_NOT_APPLICABLE | オフラインに変換 |

| 料金設定グループ レベルのエラー結果コード | SMF 障害処理アクション |
|---|---|
| USER_UNKNOWN | 無視<br>（注）<br>SMF は、このアクションをセッション レベルでのみサポートします。 |
| END_USER_SERVICE_DENIED | 料金グループに該当するトラフィックをドロップする |
| QUOTA_LIMIT_REACHED | 料金グループに該当するトラフィックをドロップする |
| END_USER_SERVICE_REJECTED | 料金グループに該当するトラフィックをドロップする |

## コール フロー

ここでは、CHF 障害処理に関連するコール フローについて説明します。

### 5G フロー削除アクションのコール フロー

このセクションでは、セッションの5G削除フローアクションのコールフローについて説明します。

図 *78 : 5G* フロー削除アクションのコール フロー

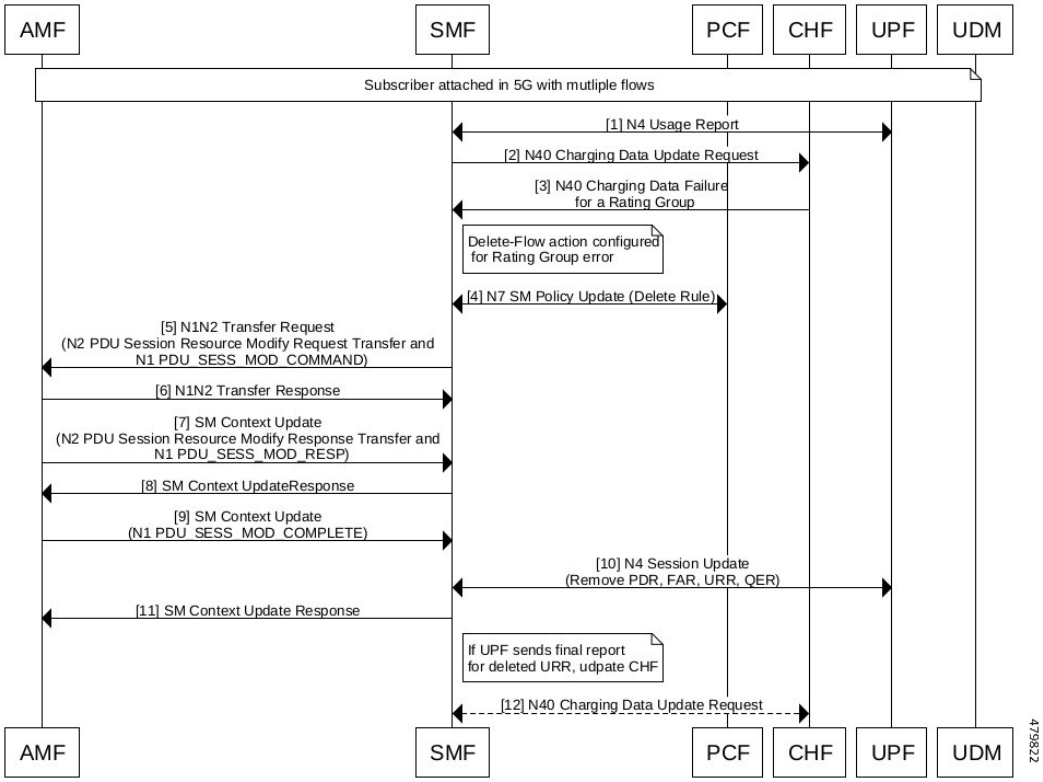



表 *136 : 5G* フロー削除アクションのコール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | サブスクライバは、5G で複数のフローで接続されます。<br>UPF は、N4 使用状況レポートを SMF に送信します。 |
| 2 | SMF は N40 課金データ更新要求を CHF に送信します。 |
| 3 | CHF が料金設定グループの N40 課金データ エラーを SMF に送信します。<br>（注）<br>料金設定グループエラーの削除フローアクションを構成します。このアクションは、フローまたは、料金設定グループに関連したルールの削除に使用されています。 |
| 4 | SMF は、ルールを削除するための N7 SM ポリシー更新を PCF に送信します。 |
| 5 | SMF は、N1N2 転送要求を AMF に送信します。このリクエストは、N2 PDU セッション リソース変更リクエスト転送と N1 PDU セッション変更メッセージを含みます。 |
| 6 | AMF は、N1N2 転送応答を SMF に送信します。 |

| ステップ | 説明 |
|---|---|
| 7 | AMF が SMF に SM コンテキスト更新を送信します。この更新メッセージには、N2 PDU セッション リソース変更応答転送と N1 PDU セッション変更応答が含まれます。 |
| 8 | SMF は、SM コンテキスト更新応答を AMF に送信します。 |
| 9 | AMF が SMF に SM コンテキスト更新を送信します。この更新には、N1 PDU セッションの変更の完了に関する詳細が含まれます。 |
| 10 | SMF は N4 セッション更新を UPF に送信します。このアップデートは、削除される PDR、FAR、URR、と QER についての詳細を含みます。 |
| 11 | SMF は、SM コンテキスト更新応答を AMF に送信します。<br>（注）<br>UPF は、削除済み URR の最終レポートを送信した場合、SMF は、CHF にこのアップデートを送信します。 |
| 12 | SMF は N40 課金データ更新要求を CHF に送信します。 |

## 4G フロー削除アクションのコール フロー

このセクションでは、セッションの4G削除フローアクションのコールフローについて説明します。

図 *79 : 4G* フロー削除アクションのコール フロー

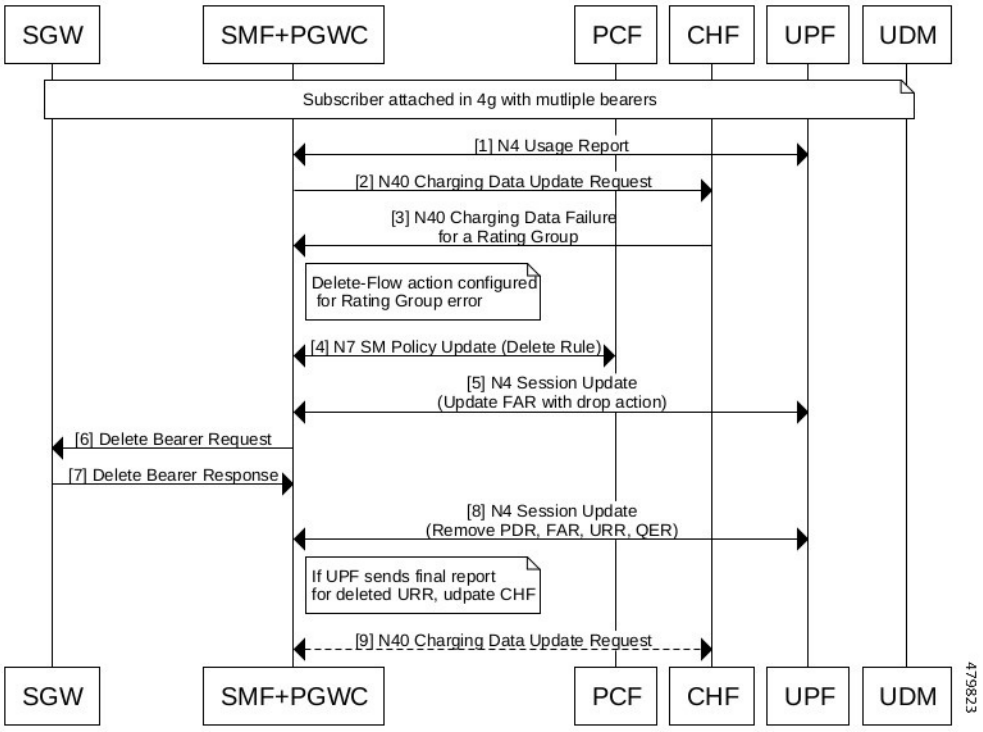



表 *137 : 4G* フロー削除アクションのコール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | サブスクライバは複数のベアラーを使用して 4G で接続されます。<br>UPF は N4 使用状況レポートを SMF + PGW-C に送信します。 |
| 2 | SMF + PGW-C は CHF に N40 課金データ更新要求を送信します。 |
| 3 | CHF が料金設定グループの N40 課金データ エラーを SMF+PGW-C に送信します。<br>（注）<br>料金設定グループエラーの削除フローアクションを構成します。このアクションは、フローまたは、料金設定グループに関連したルールの削除に使用されています。 |
| 4 | SMF+PGW-C は、ルールを削除するための N7 SM ポリシー更新を PCF に送信します。 |
| 5 | SMF+PGW-C は N4 セッション更新を UPF に送信します。このメッセージには、ドロップ アクションによる FAR の更新に関する詳細が含まれています。 |
| 6 | SMF+PGW-C が S-GW にベアラー要求の削除を送信します。 |

| ステップ | 説明 |
|---|---|
| 7 | S-GW がベアラー応答 SMF+PGW-C の削除を送信します。 |
| 8 | SMF + PGW-C は PCF に N4 セッション更新を送信します。このアップデートは、削除される PDR、FAR、URR、と QER についての詳細を含みます。<br>（注）<br>UPF は、削除済み URR の最終レポートを送信した場合、SMF は、CHF にこのアップデートを送信します。 |
| 9 | SMF + PGW-C は CHF に N40 課金データ更新要求を送信します。 |

## 障害アクションに対する SMF の動作

次の表に、CDR-（I/U/T）でさまざまな失敗（続行、無視、終了）を受信した場合の SMF の動作を示します。

| CHF 障害アクション | 統合された CHF | | | オフライン CHF | | |
|---|---|---|---|---|---|---|
| | CDR-I | CDR-U | CDR T | CDR-I | CDR-U | CDR T |
| 続行（Continue） | CDR をオフライン CHF に送信します。オフライン CHF が設定されていない場合は、課金せずにセッションを続行します。 | CDR をオフライン CHF に送信します。オフライン CHF が設定されていない場合は、課金せずにセッションを続行します。 | オフライン CHF が設定されている場合は、CDR をオフラインCHF に送信します | 課金せずにセッションを続行する | 課金せずにセッションを続行する | セッションの続行 |
| Terminate | セッションの削除 | セッションの削除 | セッションの削除の続行 | セッションの削除 | セッションの削除 | セッションの削除の続行 |
| [無視（Ignore）] | セッションの削除 | アクションは実行されません。レコードは次の CDR 要求で再試行されます。 | セッションの削除の続行 | セッションの削除 | アクションは実行されません。レコードは次の CDR 要求で再試行されます。 | セッションの削除の続行 |

## 標準準拠

課金機能のオフライン フェールオーバー サポートは、次の標準に準拠しています。

- *3GPP TS 32.255*、バージョン *15.3.0*
- *3GPP TS 32.290*、バージョン *15.4.0*
- *3GPP TS 32.291*、バージョン *15.3.0*

## 制限事項

課金機能のオフライン フェールオーバー サポートには、次の制限があります。

- セッション レベルの制限はCHFから必須であるか、ローカルで構成する必要があります。3GPP 仕様によると、オンライン URR をオフライン URR からリンク解除する必要がある場合、最後にリンクされた URR は削除できません。

料金設定グループおよびアプリケーション レベルでの CHF 失敗の処理機能には、次の制限があります。

- vSMF では、アプリケーション エラーの **terminate** アクションのみが適用されます。
- **drop-data** アクションは、オンライン課金でのみサポートされます。
- 複数の料金設定グループがエラーを返し、そのうちの 1 つに **terminate** アクションが構成されている場合、その PDU セッションは終了します。
- 複数の料金設定グループがエラーを返し、デフォルトフローへの料金設定グループマッピングに**delete-flow**アクションが構成されている場合、そのPDUセッションは終了します。
- 複数の PCC ルールと料金設定グループが 1 つのフローにマッピングされている場合、**delete-flow**アクションに構成されている料金設定グループ エラーにより、フロー全体が削除されます。
- 1つのフローにマッピングされた複数の料金設定グループの場合、以下のシナリオでは、複数の料金設定グループが失敗します。
  - **terminate** アクションが構成されている場合、このアクションが最も優先されます。
  - **delete-flow**アクションと**drop-data**アクションの両方が構成されている場合、**delete-flow** アクションが優先されます。
  - **convert-to-offline** アクションと **drop-data** アクションの両方が構成されている場合、**drop-data** アクションが優先されます。

# CHF 障害処理の構成

ここでは、CHF 障害処理の構成方法について説明します。

この機能には、次の手順が含まれます：

1. 障害処理プロファイルの構成, on page 425
2. オフライン サーバ クライアントとオフライン障害処理プロファイルの構成, on page 426

## 障害処理プロファイルの構成

CHF 作成、更新、またはリリース メッセージの対応するアクションで HTTP ステータス コードを構成できます。障害処理プロファイルの構成に基づいて、CHF サーバーの障害が発生した場合、SMF はアクションを実行します。

失敗処理プロファイルを構成するには、次の構成例を使用します：

```
config
  profile nf-client-failure nf-type chf
    profile failure-handling fh_profile_name
      service name type servicename_type
        message type messagetype_value
          status-code httpv2 statuscode_value
           action { continue | retry-and-continue | retry-and-ignore
 | retry-and-terminate } retry retry_value
            exit
```

注：

- **profile nf-client-failure nf-type chf**：NF クライアント障害後に必要なネットワーク機能の名前を指定します。
- **profile failure-handling** *fh_profile_name*：障害処理のプロファイルの名を指定します。
- **service name type** *servicename_type*：サービス タイプの名前を指定します。 CHF の *servicename_type* は 、次のいずれかの値です。
  - nchf-convergedcharging
  - nchf-spendinglimitcontrol
- **message type** *messagetype_value*：メッセージのタイプの値を指定します。 *messagetype_value* は、CHF の次のいずれかになります：
  - ChfConvergedchargingCreate
  - ChfConvergedchargingUpdate
  - ChfConvergedchargingDelete
- **status-code httpv2** *statuscode_value* ：構成された障害テンプレートに従って、ステータス コードを指定します。 *statuscode_value* は 、0 ～ 599 の範囲の整数である必要があります。ステータス コードの範囲には、区切り文字として - または ' を使用します。
- **action { continue | retry-and-continue | retry-and-ignore | retry-and-terminate } retry** *retry_value*：障害アクションと再試行回数を指定します。 *retry_value* は 1 ～ 10 の範囲の整数である必要があります。

## オフライン サーバ クライアントとオフライン障害処理プロファイルの構成

選択した CHF サーバに対してオフライン クライアント プロファイルとオフライン障害処理プロファイルを設定するには、次の設定例を使用します。

```
config
  profile network-element chf chf_name
     nf-client-profile nf_client_profile_name
     failure-handling-profile fh_profile_name
     nf-client-profile-offline offline_server_profile_name
     failure-handling-profile-offline fh_profile_offline_name
     exit
```

注：

- **profile network-element chf** *chf_name*：CHF サーバーの名前を指定します。
- **nf-client-profile** *nf_client_profile_name*：NF クライアント プロファイル名を指定します。
- **failure-handling-profile** *fh_profile_name*：障害処理プロファイル名を指定します。
- **nf-client-profile-offline** *offline_server_profile_name*：オフライン サーバーの NF クライアントプロファイル名を指定します。
- **failure-handling-profile-offline** *fh_profile_offline_name*：オフライン サーバーの障害処理プロファイル名を指定します。

# グループレベルおよびアプリケーションレベルのエラーの評価に対するアクションの構成

料金設定グループレベルおよびアプリケーションレベルのエラーに対するアクションを構成するには、次の構成例を使用します。

```
config
  profile charging profile_name
     failure-handling error-type [ rg | app ] error-value error_value
action action_value
     exit
```

注：

- **profile charging** *profile_name*：課金プロファイル コンフィギュレーション モードを開始します。
- **failure-handling error-type [ rg | app ] error-value** *error_value* **action** *action_value*：障害処理エラータイプを料金設定グループまたはアプリケーションとしてエラー値で構成します。アプリケーションレベルのエラーの場合は、*action_value* に次のいずれかの値を入力します。
  - **drop-data**：この値を指定すると、課金 ID に対応するデータをドロップできます。
  - **terminate**：PDU セッションを解放するには、この値を指定します。

- **continue**：課金を無効にするには、この値を指定します。

料金設定グループレベルのエラーの場合は、 *action_value*に次のいずれかの値を入力します。

- **convert-offline**：オフライン課金に変換するには、この値を指定します。
- **delete-flow**：料金設定グループに関連付けられているフローまたはルールを削除するには、この値を指定します。
- **drop-data**：料金設定グループに対応するデータをドロップするには、この値を指定します。
- **terminate**：PDU セッションを解放するには、この値を指定します。

（注）
- 料金設定グループレベルとアプリケーションレベルのエラーに対するアクションをまだ構成していない場合、SMF はデフォルトの動作を続行します。
- SMF では、ダイナミック ルールの同じ料金設定グループに複数の QoS フローをマッピングできません。
- **drop-data** アクションは、料金設定グループに関連付けられているすべてのフローに適用されます。

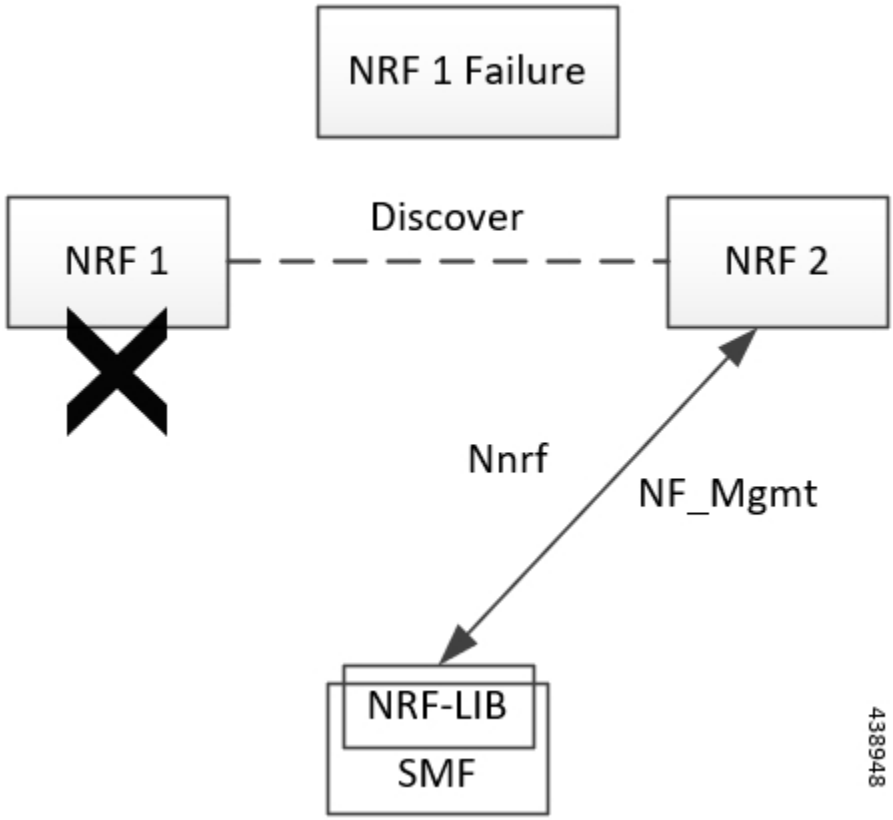
# ネットワーク リポジトリ機能障害処理

## 機能説明

ネットワーク リポジトリ機能（NRF）通信障害処理ロジックは、SMF内に実装されています。SMF は、管理 NRF グループの動作ステータスを追跡するために NF 登録メッセージを使用します。

## 機能の仕組み

次の図は、SMF が NRF 障害を処理する方法を示しています。




上記の図では、NRF 1 がプライマリで、NRF 2 が SMF のセカンダリです。起動時に、SMF は NRF 1 に登録（NF 登録）し、NF ハートビートを NRF 1 と開始します。SMF はハートビート応答を使用して動作ステータスを追跡します。

SMF が NF ハートビート応答を欠落していることで NRF 1 の障害を検出した場合、SMF は NRF 2（セカンダリ NRF）に登録して NF ハートビートの送信を開始します。SMF は自身のステータスを追跡するために、NF 登録メッセージを NRF 1 に送信し続けます。

SMF は NRF 1 から登録応答を受信すると、NRF 1 が再び起動したことを検出します。SMF は、回復すると NRF 1 をアクティブとしてマークし、NF ハートビートの NRF 2 への送信を停止します。

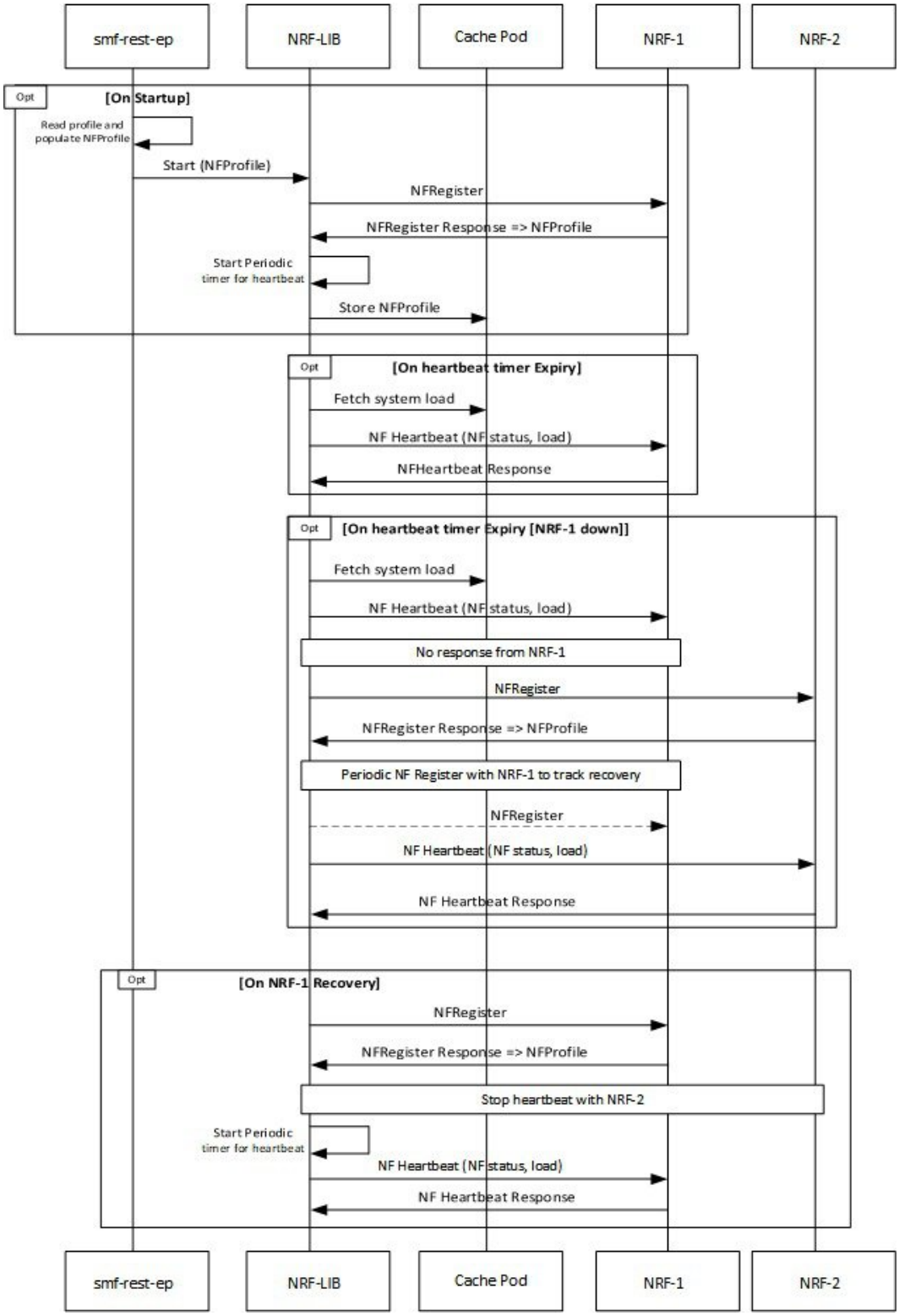
（注） フェールオーバーおよびフォールバック時の NF 再登録（デフォルト動作）は、構成駆動型です。NRF 2 は、SMF がハートビートの送信を停止したことを検出すると、SMF インスタンス ID を使用したディスカバリを使用して SMF 登録を受信したかどうかを NRF 1 から確認します。

管理エンドポイント グループとディスカバリ エンドポイント グループは別であるため、登録ベースの動作ステータス チェックは NF ディスカバリ中の NRF 障害処理に使用されません。NF の検出中、グループ内の構成済みの NRF エンドポイントが優先順位で試行されます。

# 通話フロー

次の図は、NF 登録、NF 管理、および NRF 障害処理をカバーする基本的な NF 管理コール フローを示しています。

図 *80 : NF* 管理コール フロー



# NRF 障害処理の構成

このセクションでは、その他 NFの失敗の処理に必要な NRF の構成について説明します。

## 障害処理テンプレートの構成

失敗処理テンプレートを構成するには、次の構成例を使用します：

```
config
  profile nf-client-failure { nf-type { amf | chf | nrf | pcf | udm }
    profile failure-handling failure_handling_name
    end
```

注：

- **profile nf-client-failure { nf-type { amf | chf | nrf | pcf | udm }**：必要な NF クライアント障害プロファイルを指定し、次の構成された NF のローカル構成のサポートを提供します。
  - **amf**：AMF ローカル構成を有効にします。
  - **chf**：CHF ローカル構成を有効にします。
  - **nrf**：NRF ローカル 構成を有効にします。
  - **pcf**：PCF ローカル 構成を有効にします。
  - **udm**：UDM ローカル 構成を有効にします。

    たとえば、選択した NF タイプが **udm**の場合、このコマンドは UDM のローカル構成を有効にします。他の構成済み NF に同じアプローチが適用されます。

- **profile failure-handling** *failure_handling_name*：失敗処理プロファイル名を指定します。例えば、「udmFail」と入力します。

### 設定例

次に、NRF 障害処理プロファイルの構成例を示します：

```
group nf-mgmt NFMGMT1
   nrf-mgmt-group nrf-nfmgmt-grp
      failure-handling-profile FHNRF
         locality       LOC1
            heartbeat interval 50
         exit

profile nf-client-failure nf-type nrf
   profile failure-handling FHNRF
      service name type nrf-nfm
         responsetimeout 2300
            message type NRFRegistration
               failover-enabled true
               status-code httpv2 400,500
            action retry
         exit
         status-code httpv2 401,504
         action retry-next
      exit
```

```
   exit
message type NFUpdate
   failover-enabled true
      status-code httpv2 400,503
   action retry
exit
status-code httpv2 411,500
   action retry-next
   exit
exit
message type Heartbeat
      re-registration-enabled true
      status-code httpv2 400,429
   action retry
exit
         status-code httpv2 411,500
            action retry-next
          exit
        exit
     exit
  exit
exit
```

AMF 障害が発生した場合は、障害処理テンプレートで同じ retry-action と retry-count を使用して、エラー コードの範囲に次の構成例を使用します。

**Note** 他の NF の障害時にも同様の構成を使用できます。

```
profile nf-client-failure nf-type amf
 profile failure-handling FH1
  service name type namf-comm
   message type AmfCommEBIAssignment
    status-code httpv2 100,200,300,400-410
     retry  4
     action continue
    exit
   exit
  exit
 exit
 profile failure-handling FH2
  service name type namf-comm
   message type AmfCommEBIAssignment
    status-code httpv2 401
     retry  4
     action continue
    exit
   exit
  exit
 exit

profile failure-handling FH3
  service name type namf-comm
   message type AmfCommEBIAssignment
    status-code httpv2 250-260
     retry  4
     action continue
    exit
   exit
  exit
 exit
 profile failure-handling FH4
```

```
  service name type namf-comm
   message type AmfCommEBIAssignment
    status-code httpv2 100,200,300,400-410
     action continue
    exit
   exit
  exit
 exit
 profile failure-handling FH5
  service name type namf-loc
   message type AmfCommEBIAssignment
    status-code httpv2 150,160,170-175
     action continue
    exit
   exit
  exit
 exit
exit
```

次の構成は、DNN への失敗テンプレート マッピングの例です。

```
profile dnn intershat
 network-element-profiles chf chf1
 network-element-profiles amf amf1
 network-element-profiles pcf pcf1
 network-element-profiles udm udm1
 ssc-mode 2 allowed [ 3 ]
 session type IPV4 allowed [ IPV4V6 ]
 upf apn intershat
exit
```

次の構成は、SMF への失敗テンプレート マッピングの例です。

```
profile smf smf1
 node-id          12b888e1-8e7d-49fd-9eb5-e2622a57722
 locality         LOC1
 bind-address ipv4 209.165.202.129
 bind-port        8008
 fqdn             example.com.apn.epc.mnc456.mcc123
 plmn-id mcc 123
 plmn-id mnc 456
exit

profile network-element amf amf1
 nf-client-profile        AMF-L1
 failure-handling-profile FH1
 query-params [ target-nf-instance-id ]
exit
profile network-element pcf pcf1
 nf-client-profile        PCF-L1
 failure-handling-profile FH1
exit
profile network-element udm udm1
 nf-client-profile        UDM-L1
 failure-handling-profile FH1
exit
profile network-element chf chf1
 nf-client-profile        CHF-L1
 failure-handling-profile FH2
exit
end
```

# 障害処理の構成アクション

各 NF サービスとさまざまなメッセージタイプの失敗した再試行とアクションを構成するには、次の構成例を使用します。

```
config
  profile nf-client-failure { nf-type { amf | chf | pcf | udm }
  profile failure-handling failure_handling_name
     service name type service_type
        message type message_type
           status-code httpv2 status_code
           retry retry_count
           action { continue | retry-and-continue | retry-and-terminate
 | terminate }
           end
```

注：

- **service name type** *service_type*：構成された NF サービスの種類を指定し、以下の構成されたNFに対してローカル構成のサポートを提供します。サービスタイプは、構成されたサービスによって異なります。

  AMF サービスは、次のサービス タイプをサポートしています。

  - **namf-comm**
  - **namf-evts**
  - **namf-loc**
  - **namf-mt**

  CHF サービスは、次のサービス タイプをサポートしています。

  - **nchf-convergedcharging**
  - **nchf-spendinglimitcontrol**

  NRF サービスは、次のサービス タイプをサポートしています。

  - **nrf-nfm**

  PCF サービスは、次のサービス タイプをサポートしています。

  - **npcf-am-policy-control**
  - **npcf-bdtpolicycontrol**
  - **npcf-eventexposure**
  - **npcf-policyauthorization**
  - **npcf-smpolicycontrol**
  - **npcf-ue-policy-control**

  UDM サービスは、次のサービス タイプをサポートしています。

- **nudm-ee**
- **nudm-pp**
- **nudm-sdm**
- **nudm-ueau**
- **nudm-uecm**

たとえば、選択した *service_type* が **nudm-sdm** の場合、このコマンドは UDM のローカル構成を有効にします。他の構成済み NF に同じアプローチが適用されます。

- **message type** *message_type*：構成された NF メッセージ タイプを指定し、構成された NF のローカル構成のサポートを提供します。

  メッセージ タイプは、構成されたプロファイルとサービス タイプによって異なります。

- **status code httpv2** *status_code* ：NF サービスのステータス コードと再試行アクションを指定します。現在、「http」ステータス コードのみが提供されます。 *status_code* は 0 ～ 599 の範囲の整数である必要があります。

- **retry** *retry_count*：アクションを進める前に NF サービスが再試行する必要がある回数を指定します。 *retry_count* は 1 ～ 10 の範囲の整数である必要があります。

- **action**：アクションを指定します。次のアクションがサポートされます。

  - **continue**：再試行せずにセッションを続行する場合に指定します。このアクションでは、再試行回数の構成は無効です。
  - **retry-and-continue**：構成された再試行回数に従って再試行回数を指定し、セッションを続行します。
  - **retry-and-terminate**：構成された再試行回数に従って再試行し、すべての再試行が失敗した場合はセッションを終了するように指定します。
  - **terminate**：再試行なしでセッションを終了する場合に指定します。このアクションでは、再試行回数の構成は無効です。

    メッセージ送信の再試行とアクションは、最初に送信したステータス コードの失敗に基づいて選択されます。再試行のステータス コードが異なる場合、新しい再試行回数やアクションが選択されることはありません。

次の表に、構成されたプロファイル、サービス、およびメッセージタイプのオプションの例を示します。

| プロファイル | サービス タイプ | メッセージ タイプ オプション |
|---|---|---|
| amf | namf-comm | • AmfCommEBIAssignment<br>• AmfCommN1N2MessageTransfer<br>• AmfCommSMStatusChangeNotify<br>• range |
| chf | nchf-convergedcharging | • ChfConvergedchargingCreate<br>• ChfConvergedchargingDelete<br>• ChfConvergedchargingUpdate<br>• range |
| nrf | nrf-nfm | • ハートビート<br>• NFUpdate<br>• NRFRegistration |
| pcf | npcf-am-policy-control | • PcfSmpolicycontrolCreate<br>• PcfSmpolicycontrolDelete<br>• PcfSmpolicycontrolUpdate<br>• range |
| udm | nudm-sdm | • UdmRegistrationReq<br>• UdmSdmGetUESMSubscriptionData<br>• UdmSdmSubscribeToNotification<br>• UdmSubscriptionReq<br>• UdmUecmRegisterSMF<br>• UdmUecmUnregisterSMF<br>• UdmSdmUnsubscribeToNotification<br>• range |

**Note** この例は、各プロファイルおよびサービス タイプに提供されるすべてのメッセージ オプションを網羅しているわけではありません。

# NRF 登録フェールオーバー オプションの構成

NRF 登録フェールオーバー機能を使用すると、ユーザーはすべてのエラー コードに対して再試行アクションを構成できます。アクションは、SMF やその他の NF との NRF の相互作用中に発生します。

すべてのホストまたはエンドポイントを試行した後、エラー コードの構成されているフェールオーバー オプションに基づいて次のアクションが決定されます。

NRF フェールオーバー機能を構成するには、次の構成例を使用します：

```
config
  profile nf-client-failure nrf
    profile failure-handling failure_handling_name
      service name type nrf-nfm
        message type { Heartbeat [ re-registration-enabled { false |
 true } ] | NFUpdate [ failover-enabled { false | true } ] |
NRFRegistration [ failover-enabled { false | true } ] }
          status-code httpv2 status_code  action { retry | retry-next
}
          end
```

注：

- **message type { Heartbeat [ re-registration-enabled { false | true } ] | NFUpdate [ failover-enabled { false | true } ] | NRFRegistration [ failover-enabled { false | true } ] }** ：NRF メッセージ タイプを指定して、フェールオーバー機能を有効にします。

  NRF メッセージのフェールオーバー オプションは次のとおりです：

  - **NRFRegistration** または **NFUpdate**
    - **true**：NRF 内のすべてのホストまたはエンドポイントを試行した後、システムは次に使用可能な NRF を選択します。
    - **false**：NRF 内のすべてのホストまたはエンドポイントを試した後、次に使用可能な NRF は選択されません。

    バックアップ ルーチンの生成は、エンドポイントが試行された NRF でのみ使用できます。
  - ハートビート
    - **true**：再登録開始オプションが有効な場合、NRF 内のすべてのホストまたはエンドポイントで試行した後に、NF クライアントの再登録プロセスが開始されます。
    - **false**：NRF ですべてのホストまたはエンドポイントを試行した後、システムは同じ登録済み NRF でハートビート ルーチンを続行します。

- **status-code httpv2** *status_code* **action { retry | retry-next }**：NRF サービスのステータス コードと再試行アクションを指定します。現在、「http」ステータス コードのみが提供されます。 *status_code* は 0 ～ 599 の範囲の整数である必要があります。

- **再試行**：システムは同じエンドポイントまたはホストに対してもう一度再試行を試みます。
- **retry-next**：システムは同じエンドポイントまたはホストを再試行しませんが、次に使用可能なエンドポイントまたはホストに対して再試行アクションを試みます。

- NF 登録、NF ハートビート、および NF 更新のエラー処理は、ステータス コードに基づいています。この機能は、サブスクリプションおよび NF 登録解除メッセージでは使用できません。ユーザーは **group nrf management** 、 CLI で使用可能なエンドポイント構成を使用して、サブスクリプションおよび NF 登録解除メッセージの最大再試行回数を設定できます。システムはその構成に基づいて再試行アクションを試みます。
- failover-enabled オプションは、NF 登録メッセージと NF 更新メッセージに適用できます。
- reregistration-enabled オプションは、NF ハートビート メッセージに適用できます。
- failover-enabled または reregistration-enabled オプションは、NF 登録解除メッセージには適用されません。
- フェールオーバーと再登録のオプションは、デフォルトで有効になっています。

## ネットワーク要素プロファイルの障害処理の構成

ネットワーク要素プロファイルの失敗処理を構成するには、次の構成例を使用します：

```
config
  profile network-element { { amf | chf | pcf | udm } nf_profile_name }
    failure-handling-profile profile_name
    end
```

注：

- **failure-handling-profile** *profile_name*：構成された NRF の SCP 障害処理ネットワーク プロファイルを指定します。*profile_name* には、対応する NRF 障害処理ネットワーク プロファイル名を表す英数字の文字列を含める必要があります。

## 設定例

次に、設定例を示します。

```
group nf-mgmt NFMGMT1
   nrf-mgmt-group nrf-nfmgmt-grp
      failure-handling-profile FHNRF
         locality       LOC1
            heartbeat interval 50
         exit

profile nf-client-failure nf-type nrf
   profile failure-handling FHNRF
      service name type nrf-nfm
         responsetimeout 2300
            message type NRFRegistration
               failover-enabled true
               status-code httpv2 400,500
```

```
            action retry
          exit
          status-code httpv2 401,504
          action retry-next
       exit
   exit
message type NFUpdate
   failover-enabled true
      status-code httpv2 400,503
   action retry
exit
status-code httpv2 411,500
   action retry-next
   exit
exit
message type Heartbeat
      re-registration-enabled true
      status-code httpv2 400,429
   action retry
exit
         status-code httpv2 411,500
            action retry-next
          exit
        exit
     exit
  exit
exit
```

AMF 障害が発生した場合は、障害処理テンプレートで同じ retry-action と retry-count を使用して、エラー コードの範囲に次の構成例を使用します。

```
profile nf-client-failure nf-type amf
 profile failure-handling FH1
  service name type namf-comm
   message type AmfCommEBIAssignment
    status-code httpv2 100,200,300,400-410
     retry  4
     action continue
    exit
   exit
  exit
 exit
 profile failure-handling FH2
  service name type namf-comm
   message type AmfCommEBIAssignment
    status-code httpv2 401
     retry  4
     action continue
    exit
   exit
  exit
 exit

profile failure-handling FH3
  service name type namf-comm
   message type AmfCommEBIAssignment
    status-code httpv2 250-260
     retry  4
     action continue
    exit
   exit
  exit
 exit
 profile failure-handling FH4
```

```
  service name type namf-comm
   message type AmfCommEBIAssignment
    status-code httpv2 100,200,300,400-410
     action continue
    exit
   exit
  exit
 exit
 profile failure-handling FH5
  service name type namf-loc
   message type AmfCommEBIAssignment
    status-code httpv2 150,160,170-175
     action continue
    exit
   exit
  exit
 exit
exit
```

# NRF 障害処理の確認

## NF 管理の障害処理

次に、管理 NRF エンドポイントの構成例を示します。

```
product smf# show running-config group nf-mgmt
group nf-mgmt MGM
 nrf-mgmt-group mgmt_group
 locality       LOC1
exit
product smf# show running-config group nrf mgmt
group nrf mgmt mgmt_group
 service type nrf nnrf-nfm
  endpoint-profile epprof
   uri-scheme http
   endpoint-name EP1
    priority 2
    primary ip-address ipv4 209.165.200.237
    primary ip-address port 8082
    secondary ip-address ipv4 209.165.200.238
    secondary ip-address port 8082
   exit
   endpoint-name EP2
    priority 10
    primary ip-address ipv4 209.165.200.237
    primary ip-address port 8082
    secondary ip-address ipv4 209.165.200.238
    secondary ip-address port 8082
   exit
  exit
 exit
exit
product smf#
```

構成例では、EP1 は優先順位が EP2 よりも低いため（2 対 10）、より優先順位の高いエンドポイント名です。起動時に、SMF は EP1 [209.165.200.235:8082] のプライマリ IP:ポートに NF 登録を送信します。プライマリがダウンしている場合、SMF は EP1 のセカンダリ ip:port を使用します。SMF は、EP1 のすべての ip: ポートがダウンしている場合にのみ、EP2 へのエンドポイントのフェールオーバーを実行します。

EP1 プライマリに正常に登録されると、SMF は EP1 プライマリとのハートビートを開始します。EP1 プライマリがダウンした場合、SMF はハートビート応答の欠落でダウンを検出します。EP1 プライマリがダウンしていることが検出されると、SMF は再登録せずに EP1 セカンダリにハートビートを送信します。また、プライマリ EP1 が回復したかどうかを検出するために、NF ハートビートを定期的にプライマリに送信します。

SMF が EP1 のプライマリおよびセカンダリがダウンしていることを検出すると、SMF は EP2 へのエンドポイントのフェールオーバーを実行します。EP2 プライマリへのフェールオーバーが成功すると、再登録を送信します（デフォルトの動作）。エンドポイント名を持つすべてのエンドポイントは同じデータベースを共有することが想定されているため、再登録はエンドポイント名にまたがるフェールオーバーの場合にのみサポートされます。この場合、EP1 プライマリとセカンダリは同じデータベースを共有します。同様に、EP2 のプライマリとセカンダリは別のデータベースを共有します。EP2 プライマリへのフェールオーバーでは、定期的な NF 登録が EP1 のプライマリにのみ送信されます（リカバリを検出するため）。

より優先順位の高いエンドポイント名が回復対象であることが検出されるたびに、SMF は回復された IP：ポートにフォールバックします。たとえば、現在アクティブな NRF エンドポイントが EP2 プライマリであり、SMF が EP1 プライマリが回復したことを検出すると、SMF は EP1 プライマリへの再登録を実行し（デフォルトの動作）、EP2 プライマリのハートビートを停止します。

エンドポイント内では、NF ハートビートを使用して動作ステータスを追跡する。エンドポイント全体で、登録を使用して動作ステータスを追跡する。要求メッセージのタイムアウト、RPC エラー、および HTTP 応答コード 408、429、500、501、502、503 は、次の NRF への移動の失敗と見なされます。

## NF 検出の障害処理

以下は検出 NRF エンドポイント構成の例です。

```
product smf# show running-config profile nf-pair nf-type UDM
profile nf-pair nf-type UDM
 nrf-discovery-group others_group
 locality client LOC1
exit
product smf# show running-config group nrf discovery others_group
group nrf discovery others_group
 service type nrf nnrf-disc
  endpoint-profile ep1
   capacity 30
   priority 50
   uri-scheme http
   endpoint-name ED1
    priority 56
    primary ip-address ipv4 209.165.201.19
    primary ip-address port 8082
    secondary ip-address ipv4 209.165.201.20
    secondary ip-address port 8082
    exit
   endpoint-name ED2
    priority 10
    primary ip-address ipv4 209.165.201.21
    primary ip-address port 8082
    secondary ip-address ipv4 209.165.201.22
    secondary ip-address port 8082
```

```
   exit
  exit
 exit
exit
product smf#
```

サンプル構成では、ED1 の優先順位が ED2 よりも低いため（2 対 10）、ED1 の方が優先順位の高いエンドポイント名です。NRFディスカバリが必要な場合は常に、ED1 [209.165.201.19:8082] のプライマリ IP:ポートが試行されます。SMF は、ED1 のセカンダリ ip:port を使用します（プライマリがダウンしている場合）。SMF は、ED1 のすべての ip: ポートがダウンしている場合にのみ、ED2 へのエンドポイントのフェールオーバーを実行します。NRF エンドポイントでの NRF 検出の失敗に関する状態は維持されていません。SMF は常に ED1 プライマリから開始し、障害が発生した場合は ED1 セカンダリにフォールバックし、次に ED2 プライマリにフォールバックします。

# ポリシー制御機能の失敗の処理

## 機能説明

SMF は NF フェールオーバー サポートを利用して PCF フェールオーバー機能を実現します。

NF フェールオーバー機能は、次の機能をサポートしています：

- プライマリ エンドポイントとセカンダリ エンドポイントとしてのサービスの複数のエンドポイント。エンドポイントは、NRF クライアント プロファイル構成および NRF 障害プロファイル構成を使用して構成できます。
- 以下に基づく障害の動作：
  - メッセージの種類
  - 応答メッセージの HTTP ステータス コード

PCSCF プロファイルが構成されると、SMF は PDU のアクティベーションが IMS 向けで、IMS が PCF を必要とするものと想定します。その後、SMF は失敗処理の構成に関係なく PDU を拒否します。

- SMF は、profile dnn の下に「pccf-profile」がある場合、失敗処理設定を無視して PDU の作成を拒否します。
- オペレータは、同じ「profile dnn」で次のパラメータを構成できません：
  - pcf-interaction false
  - pcscf-profile

# 機能の仕組み

このセクションでは、SMF がメッセージ レベルの障害と、対応する HTTP ステータス コード ベースの障害を処理する方法について説明します。

SMF は、次のメッセージを開始します。

- PcfSmpolicycontrolCreate
- PcfSmpolicycontrolUpdate
- PcfSmpolicycontrolDelete

PDU セッションのライフサイクル中の、SMF は、さまざまな段階でメッセージを PDF と交換します。NRF 障害プロファイルに構成された HTTP ステータス コードに応じて、SMF は次のいずれかのアクションを実行します：

- [無視（Ignore）]
- 続行（Continue）
- Terminate

**表 *138 : PCF* フェールオーバー メッセージとアクションとの関係**

| | **PcfSmpolicy controlCreate** | **PcfSmpolicy controlUpdate** | **PcfSmpolicy controlDelete** |
|---|---|---|---|
| [無視（Ignore）] | ローカルに構成された、または UDM が提供するポリシー パラメータを続行します。<br>**（注）**<br>後続のメッセージについては PCF に問い合わせないでください。<br>**PCF-Interaction Status: OFF** | 現在利用可能なポリシー パラメータのスナップショットを続行します。<br>後続のメッセージについては、PCF にお問い合わせください。<br>**PCF-Interaction Status: ON** | 現在の障害を無視して、セッションを削除します。<br>**PCF-Interaction ステータス：セッション削除** |
| 続行（Continue） | ローカルに構成された、または UDM が提供するポリシー パラメータを続行します。<br>**（注）**<br>後続のメッセージについては PCF に問い合わせないでください。<br>**PCF-Interaction Status: OFF** | 現在利用可能なポリシー パラメータのスナップショットを続行します。<br>**（注）**<br>後続のメッセージについては PCF に問い合わせないでください。<br>**PCF-Interaction Status: OFF** | 現在の障害を無視して、セッションを削除します。<br>**PCF-Interaction ステータス：セッション削除** |
| Terminate | セッションを終了します。 | セッションを終了します。 | セッションを終了します。 |

### PCF インタラクション ステータス

この機能は、SMF 開始メッセージと PCF 開始メッセージに対して次のステータス メッセージをサポートします。

- **PCF-Interaction Status: ON**

  SMF 開始のメッセージ：SMF は、基準が満たされるたびに、PCF へのメッセージを開始し続けます。

  PCF によって開始されたメッセージ：SMF は、PCF から SMF へのすべてのメッセージを受け入れ続けます。

- **PCF-Interaction Status: OFF**

  SMF 開始のメッセージ：SMF は、基準が満たされるたびに、PCF 向けのメッセージを開始したり、送信したりしません。SMF は PCF を利用できないものとして扱い、さらにアクションを続行します。

  PCF 開始メッセージ：PCF によって開始されるメッセージは 2 つあります。

  - SmPolicyUpdateNotifyReq：このメッセージを受信すると、SMF は応答で 404 エラーコードを送信し、セッションをクリーンアップして、削除要求を PCF に送信しません。

（注） また、SMF は、FIVEG_PDU_SESSION_RELEASE_COMMAND 内に **REACTIVATION REQUESTED** として FIVEGSM_CAUSE 値を 5G の UE に送信します。4G の場合、SMF は DELETE BEARER REQUEST メッセージで **REACTIVATION REQUESTED** を S-GW に送信します。

  - SmPolicyAssociationTerminationReq：このメッセージを受信すると、SMF は成功応答を送信し、セッションをクリーンアップします。この連携の一環として、SMF は PCF に削除要求を送信します。

（注） これは、[PCF-Interaction ステータス（PCF-Interaction Status）] が [オフ（OFF）] に設定されている場合の例外です。

# PCF 障害処理機能の構成

ここでは、PCF 障害処理機能の構成方法について説明します。

PCF 障害処理機能の構成には、次の手順が含まれます：

- PCF 障害処理プロファイルの構成 （445 ページ）
- 障害処理プロファイルの 関連付けの構成 （446 ページ）

• セカンダリおよびターシャリ IP アドレスの構成 （446 ページ）

## PCF 障害処理プロファイルの構成

アクションを使用してPCF障害処理プロファイルを構成するには、次の構成例を使用します：

```
config
  profile nf-client-failure nf-type pcf
     profile failure-handling fhprofile_name
        service name type servicename_type
           message type messagetype_value
              status-code httpv2 status_code
              action { continue | retry-and-continue | retry-and-ignore
| retry-and-terminate } retry retry_value
              exit
```

注：

- **profile failure-handling** *fhprofile_name*：障害処理プロファイル名を指定します。
- **service name type** *servicename_type*：PCF サービス名のタイプを指定します。 *servicename_type* は 、次のいずれかの値です。
  - npcf-am-policy-control
  - npcf-bdtpolicycontrol
  - npcf-evenxposure
  - npcf-policy authorization
  - npcf-smpolicycontrol
  - npcf-ue-policy-control
- **message type** *messagetype_value*：メッセージ タイプを指定します。 *messagetype_value* には、次のいずれかの値を指定できます。
  - PcfAmfPolicyControlCreate
  - PcfSmpolicycontrolCreate
  - PcfSmpolicycontrolDelete
  - PcfSmpolicycontrolUpdate
- **status-code httpv2** *status_code*：HTTPv2 ステータス コードを指定します。 *status_code*は 、「-」または「,」で区切られた0ー599の範囲の整数である必要があります。
- **action { continue | retry-and-continue | retry-and-ignore | retry-and-terminate } retry** *retry_value*：アクションと再試行回数を指定します。 *retry_value* は 1 ～ 10 の範囲の整数である必要があります。

# 障害処理プロファイルの 関連付けの構成

PCF で FH プロファイルの関連付けを構成するには、次の構成例を使用します：

```
config
  profile network-element pcf pcf_profile_name
     nf-client-profile nf_profile_name
     failure-handling-profile fh_profile_name
     exit
```

注：

- **nf-client-profile** *nf_profile_name*：NF クライアントプロファイル名を指定します。
- **failure-handling-profile** *fh_profile_name*：障害処理プロファイル名を指定します。

# セカンダリおよびターシャリ IP アドレスの構成

セカンダリ IP アドレスとターシャリ IP アドレスを構成するには、次の構成例を使用します：

```
config
  profile nf-client nf-type pcf
     pcf-profile pcfprofile_name
        locality locality_name
           service name type npcf-smpolicycontrol
              endpoint-profile endpointprofile_name
                 endpoint-name endpoint_name
                    primary ip-address { ipv4 primary_ipv4_address | ipv6
primary_ipv6_address | port primary_port_number }
                    secondary ip-address { ipv4 secondary_ipv4_address | ipv6
 secondary_ipv6_address | port secondary_port_number }
                    tertiary ip-address { ipv4 tertiary_ipv4_address | ipv6
tertiary_ipv6_address | port tertiary_port_number }
                    end
```

注：

- **primary ip-address ipv4** *primary_ipv4_address*：プライマリ エンドポイントの IPv4 アドレスを指定します。
- **primary ip-address ipv6** *primary_ipv6_address*：プライマリ エンドポイントの IPv6 アドレスを指定します。
- **primary ip-address port** *primary_port_number*：プライマリ エンドポイントのポート番号を指定します。
- **secondary ip-address ipv4** *secondary_ipv4_address*：セカンダリ エンドポイントの IPv4 アドレスを指定します。
- **secondary ip-address ipv6** *secondary_ipv6_address*：セカンダリ エンドポイントの IPv6 アドレスを指定します。
- **secondary ip-address port** *secondary_port*：セカンダリ エンドポイントのポート番号を指定します。

- **tertiary ip-address ipv4** *tertiary_ipv4_address*：ターシャリ エンドポイントの IPv4 アドレスを指定します。
- **tertiary ip-address ipv6** *tertiary_ipv6_address*：ターシャリ エンドポイントの IPv6 アドレスを指定します。
- **tertiary ip-address port** *tertiary_port_number*：ターシャリ エンドポイントのポート番号を指定します。

# PCF 障害処理に対する OAM サポート

ここでは、この機能の操作、管理、およびメンテナンスに関して説明します。

## バルク統計サポート

この機能では、次の統計がサポートされます。

- PcfSmpolicyControlCreate
  - 無視した応答の数
  - 続行した応答の数
  - 終了した応答の数
- PcfSmPolicyControlUpdate
  - 無視した応答の数
  - 続行した応答の数
  - 終了した応答の数
- PcfSmpolicyControlDelete
  - 無視した応答の数
  - 続行した応答の数
  - 終了した応答の数
- PolicyUpdateNotifyReq
  - 承認された要求の数
  - 承認された要求の数
  - スキップされた要求の数
- PolicyDeleteReq
  - 承認された要求の数
  - 承認された要求の数

- スキップされた要求の数

- PolicyUpdateRequest
  - 承認された要求の数
  - 承認された要求の数
  - スキップされた要求の数

- ポリシー タイプが local/pcf であるサブスクライバの数のゲージ カウンタ。

# 統合データ管理の失敗の処理

## 機能説明

統合データ管理（UDM）は主にサブスクライバ データを保存する役割を果たし、SMF はネットワーク上のユーザー セッションを管理するためにこのデータにアクセスします。

SMF での UDM 障害処理のサポートでは、新しい障害処理テンプレート（FHT）プロファイルが導入されています。このプロファイルは、SMF の UDM プロファイルに関連付けられています。

FHT テンプレートにより、SMF はセッションの N10 を介して UDM との相互作用を柔軟に微調整できます。これは、新しいセッションと既存の両方のセッションについて、UDM からの応答で HTTP ステータス コードを処理する SMF をサポートしています。

NF フェールオーバーのサポートは、NF クライアントプロファイル設定と NF 障害プロファイル構成を使用して SMF で利用できます。この機能は、次の機能をサポートしています。

- サービスの複数のエンドポイントをプライマリ エンドポイントとセカンダリ エンドポイントとして構成します。
- 次に基づいて失敗の処理動作を指定します：
  - メッセージの種類
  - 応答メッセージの HTTP ステータス コード

## 機能の仕組み

SMF は NF フェールオーバーを使用して、UDM フェールオーバー サポート機能を実現します。このセクションでは、SMF がメッセージ レベルの障害と、対応する HTTP ステータス コード ベースの障害を処理する方法について説明します。

SMF は、次のメッセージを開始します。

- UE-Connection-Management（UE-CM）

- Nudm_UECM_Registration
- Nudm_UECM_DeRegistration

- UE-Subscription-Management (UE-SDM)
  - Nudm_SDM_Get
  - Nudm_SDM_Subscribe
  - Nudm_SDM_Unsubscribe

PDUセッションのライフサイクル中の、SMFは、さまざまな段階で上記のメッセージをUDMと交換します。NF障害プロファイルに構成されたHTTPステータス コードに応じて、SMFは次のいずれかのアクションを実行します。

- [無視（Ignore）]
- 続行（Continue）
- Terminate

SMFでは、他の使用可能なUDMサーバに対して同じ要求を試行するための次のアクションが提供されます。

- retry-and-terminate
- retry-and-ignore
- retry-and-continue

すべての再試行が失敗すると、SMFは適切な失敗処理アクションを実行します。たとえば、FHアクションがretry-and-terminateの場合、SMFはすべての試行が失敗した後に通話を終了します。

（注） SMFでは、障害処理テンプレートの構成をダイナミックに変更できます。構成への変更が新規コールにのみ適用されます。

表 *139 : N10* メッセージとフェールオーバー アクションとの関係

| シナリオ | サービス | メッセージ | 条件 | 操作 | 成功の応答 | 障害敗応答の処理 | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | **Terminate** | 続行（**Continue**） | [無視（**Ignore**）] |
| 5G、4G、および Wi-Fi での PDU セッションの作成手順<br>RAT 間ハンドオーバーの手順 | UECM | Nudm_UECM_Registration | Nudm UECM 登録が完了しておらず、アクセス タイプが 4G でない場合 | メッセージを送信する | 登録が成功したことをマークする | コールの終了 | 通話を続行する | 通話を続行する |
| | | Nudm_UECM_登録解除 | Nudm UECM 登録が完了した場合 | メッセージを送信する | アクションなし | コールの終了 | コールの終了 | コールの終了 |
| 5G、4G、および Wi-Fi での PDU セッションの作成手順 | SDM | Nudm_SDM_Get | サブスクリプション取得構成をスキップした場合は有効になっていません | メッセージを送信する | サブスクリプションの取得が成功したことをマークします | コールの終了 | 通話を続行する | 通話を続行する |
| | | Nudm_SDM_Subscribe | サブスクリプションの取得が成功した場合 | メッセージを送信する | アクションなし | コールの終了 | サブスクリプションが完了していない場合に通話を続行 | サブスクリプションが完了していない場合に通話を続行 |

| シナリオ | サービス | メッセージ | 条件 | 操作 | 成功の応答 | 障害敗応答の処理 | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | Terminate | 続行（Continue） | [無視（Ignore）] |
| 5G、4G、および Wi-Fi での PDU セッションのリリース手順 | SDM | Nudm_SDM_Unsubscribe | サブスクリプションの取得が成功し、登録が完了していない場合 | メッセージを送信する | アクションなし | コールの終了 | 通話を続行する | 通話を続行する |

- **終了**：SMF は任意のメッセージ タイプの通話を終了します。
- **続行**：SMF は現在の障害を無視し、同じサービス グループ内の他のメッセージに対する後続の操作をスキップします。
- **無視**：SMF は現在のインタラクションの失敗のみを無視してコールを続行します。SMF は、後続のメッセージのインタラクションを処理します。
- UDM サブスクリプション取得は、EPS および NR ネットワークでのセッション確立中にのみ実行してください。

  UDM サブスクリプションの取得が失敗し、FH アクションが「無視」であるか、または通知への登録をスキップする構成が有効になっている場合、SMF は通知への登録の相互作用をスキップします。
- UDM 障害処理テンプレートが構成されていない場合、デフォルトの障害処理アクションは「終了」です。

# UDM 障害処理機能の構成

このセクションでは、UDM 障害処理機能の構成方法について説明します。

UDM 障害処理機能の構成には、次の手順が含まれます：

- UDM 障害処理プロファイルの構成 （451 ページ）
- FH プロファイルの関連付けの構成 （452 ページ）
- セカンダリおよびターシャリ IP アドレスの構成 （453 ページ）

## UDM 障害処理プロファイルの構成

次の構成例を使用して、アクションを使用して UDM 障害処理プロファイルを構成します。

```
config
   profile nf-client-failure nf-type udm
```

```
      profile failure-handling fh_profile_name
         service name type { nudm-ee | nudm-pp | nudm-sdm | nudm-ueau
         | nudm-uecm }
         message type { UdmRegistrationReq |
UdmSdmGetUESMSubscriptionData
         | UdmSdmSubscribeToNotification | UdmSubscriptionReq
         | UdmUecmRegisterSMF | UdmUecmUnregisterSMF |
         UdmSdmUnsubscribeToNotification }
            status-code httpv2 0
             action { continue | retry-and-continue | retry-and-ignore

              | retry-and-terminate | terminate }
              end
```

## FH プロファイルの関連付けの構成

UDM で FH プロファイルの関連付けを構成するには、次の構成例を使用します：

```
config
   profile network-element udm udm_profile_name
      nf-client-profile nf_profile_name
      failure-handling-profile fh_profile_name
      failure-handling-profile-rat nr
         failure-handling-profile fh_profile_name
         exit
```

注：

- **failure-handling-profile-rat nr**：RAT タイプに固有の失敗処理プロファイルを指定します。
- **failure-handling-profile** *fh_profile_name*：障害処理ネットワークプロファイル名を指定します。 *fh_profile_name* は 文字列である必要があります。

### RAT ベースの FH プロファイルの確認

このセクションでは、UDM で RAT ベースの FH プロファイルを確認する方法について説明します。

**show running-config profile network-element udm** *udm_profile_name* コマンドを使用して、機能構成の詳細を確認します。

次に出力例があります。

```
nf-client-profile UP1
   failure-handling-profile FH1
   failure-handling-profile-rat nr
      failure-handling-profile FH4
      exit
exit
```

この例では、FH1 がデフォルトの障害処理プロファイルです。ただし、RAT タイプが **nr**に構成されている場合は、障害処理プロファイル FH4 が使用されます。

# セカンダリおよびターシャリ IP アドレスの構成

セカンダリ IP アドレスとターシャリ IP アドレスを構成するには、次の構成例を使用します：

```
config
   profile nf-client nf-type udm
      udm-profile udmprofile_name
         locality LOC
           service name type { nudm-ee | nudm-pp | nudm-sdm | nudm-ueau
 | nudm-uecm }
               endpoint-profile epprofile_name
                  endpoint-name endpoint_name
                     primary ip-address { ipv4 primary_ipv4_address | ipv6
 primary_ipv6_address | port primary_port_number }
                     secondary ip-address { ipv4 secondary_ipv4_address |
ipv6 secondary_ipv6_address | port secondary_port_number }
                     tertiary ip-address { ipv4 tertiary_ipv4_address |
ipv6 tertiary_ipv6_address | port tertiary_port_number }
                     end
```

注：

- **primary ip-address ipv4** *primary_ipv4_address*：プライマリ エンドポイントの IPv4 アドレスを指定します。
- **primary ip-address ipv6** *primary_ipv6_address*：プライマリ エンドポイントの IPv6 アドレスを指定します。
- **primary ip-address port** *primary_port_number*：プライマリ エンドポイントのポート番号を指定します。
- **secondary ip-address ipv4** *secondary_ipv4_address*：セカンダリ エンドポイントの IPv4 アドレスを指定します。
- **secondary ip-address ipv6** *secondary_ipv6_address*：セカンダリ エンドポイントの IPv6 アドレスを指定します。
- **secondary ip-address port** *secondary_port*：セカンダリ エンドポイントのポート番号を指定します。
- **tertiary ip-address ipv4** *tertiary_ipv4_address*：ターシャリ エンドポイントの IPv4 アドレスを指定します。
- **tertiary ip-address ipv6** *tertiary_ipv6_address*：ターシャリ エンドポイントの IPv6 アドレスを指定します。
- **tertiary ip-address port** *tertiary_port_number*：ターシャリ エンドポイントのポート番号を指定します。

## 応答タイムアウトパラメータの構成

UDM インターフェイス（N10）を介したフェールオープンサポートの応答タイムアウトを構成するには、次の構成例を使用します：

```
config
  profile network-element udm udm_profile_name
    response-timeout timeout_value
    exit
```

注：

- **response-timeout** *timeout_value*：応答のタイムアウトをミリ秒単位で指定します。*timeout_value* は 1000 ～ 30000 の範囲の整数である必要があります。

  デフォルト：4000

### 応答タイムアウトの構成の確認

次に、設定例を示します。

```
[unknown] smf# show running-config profile network-element udm
profile network-element udm udm1
nf-client-profile UP1
failure-handling-profile FH4
query-params [ dnn ]
response-timeout 2000
exit
[unknown] smf#
```

## 統計

次の統計情報は、すべての UDM サービスとメッセージの組み合わせについて、ステータスが試行/成功/スキップ/失敗のすべての UDM メッセージステータスに対してサポートされています。

```
udm_msg_processing_status{app_name="SMF",cluster="Local",data_center="DC"
,instance_id="1",msg_status="attempted",rat_type="nr",service_name="smfservice",
udm_end_point="",udm_msg="UdmSmSubscription”} 1
```

```
udm_msg_processing_status{app_name="SMF",cluster="Local",data_center="DC",
instance_id="1",msg_status="skipped",rat_type="nr",service_name="smfservice",udm_end_point="",
udm_msg="UdSmSubscription"} 1
```

# UDM 障害処理機能の OAM サポート

ここでは、この機能の操作、管理、およびメンテナンスに関して説明します。

## バルク統計サポート

SMF は、UDM 障害処理機能のサポートで、以下の統計情報を保持します。

- Nudm_UECM_Registration
  - 無視した応答の数

- 続行した応答の数
- 終了した応答の数

- Nudm_UECM_DeRegistration
  - 無視した応答の数
  - 続行した応答の数
  - 終了した応答の数

- Nudm_SDM_Get
  - 無視した応答の数
  - 続行した応答の数
  - 終了した応答の数

- Nudm_SDM_Subscribe
  - 無視した応答の数
  - 続行した応答の数
  - 終了した応答の数

- Nudm_SDM_Unsubscribe
  - 無視した応答の数
  - 続行した応答の数
  - 終了した応答の数

smf-serviceの「udm_msg_processing_status」統計は、ステータスが [試行（Attempted）]、[成功（Success）]、[スキップ（Skipped）]、および [失敗（Failed）] の UDM メッセージの数を追跡します。

例：

```
udm_msg_processing_status
{app_name="SMF",cluster="Local",data_center="DC",instance_id="1",msg_status="attempted",
rat_type="nr",
service_name="smf-service",udm_end_point="",udm_msg="UdmSmSubscription"} 1
udm_msg_processing_status
{app_name="SMF",cluster="Local",data_center="DC",instance_id="1",msg_status="skipped",
rat_type="nr",
service_name="smf-service",udm_end_point="",udm_msg="UdSmSubscription"} 1
```

# ユーザー プレーン機能障害の処理

ユーザー プレーン機能（UPF）の障害処理により、SMF は、新しいセッションと既存のセッションの両方中に、UPF の応答で受信したエラー原因コードを管理できます。SMF は、パケット転送制御プロトコル（PFCP）PFCP の障害処理テンプレート（FHT）プロファイルを提供します。このプロファイルは、SMF の UPF プロファイルに関連付けられています。FHT テンプレートにより、SMF はセッション中に UPF との相互作用を柔軟に微調整できます。

### FHT でサポートされている構成可能なアクション

この機能は、UPF からの応答で受信したエラー原因コードに基づいて、構成可能なアクションを提供します。

- ignore
- terminate
- continue
- 再試行終了
- retry-ignore
- retry-continue

## UPF 障害処理方法

### process_workflow

UPF 障害処理プロセスの段階は次のとおりです。

1. セッションの確立中に UPF が輻輳している場合、UPF は SMF からの PFCP 確立メッセージを拒否します。
2. UPF は、応答メッセージで原因コードを SMF に送信します。
3. SMF はユーザー定義の障害処理テンプレートをチェックします。テンプレートで再試行が構成されている場合、SMF はコール損失を減らすために PFCP 確立メッセージの別の UPF への送信を再試行します。
4. SMF は構成された優先順位の値とキャパシティ（UPF からの負荷情報）に基づいて UPF を選択します。
5. SMF は FHT でのユーザー定義のアクションに基づいて、セッションを無視、終了、または続行します。

# UPF 障害処理を有効にする

UPF 障害処理機能を有効にするには、次の手順を実行します。

手順

**ステップ 1** UPF 障害処理プロファイルを構成します。
**ステップ 2** 障害プロファイルの関連付けを構成します。

## UPF 障害処理プロファイルの構成

グローバル コンフィギュレーション モードで UPF 障害処理プロファイルを構成します。

手順

**ステップ 1** 障害処理プロファイルを作成するプロファイル名を指定します。

**profile failure-handling** *fh_profile_name*

**例**：

```
[smf] smf# config
[smf] smf(config)# profile failure-handling  fh1
```

**ステップ 2** 障害処理を構成する PFCP メッセージ タイプを指定します。

**例**：

```
[smf] smf# config
[smf] smf(config-failure-handling-fh1)#  interface pfcp message N4SessionModificationReq
```

- N4SessionEstablishmentReq：N4SessionEstablishmentReq（新しいセッションの場合）、N4SessionModificationReq メッセージ（既存のセッションの場合）、および N4 セッション レポート要求の失敗処理を指定します。
- N4SessionModificationReq：既存のセッションの障害処理メッセージを指定します。
- N4SessionReportReq：セッション レポートの失敗処理メッセージを指定します。

  N4SessionReportReq キーワードが構成されている場合、SMF はセッション削除要求をトリガし、その後セッション レポートの拒否をトリガします。UPF は削除要求に応答し、セッションをクリアします。

（注）
セッションが UPF ですでにアクティブであるため、UPF の再選択はメッセージ タイプ N4SessionModificationReq には適用されません。

**ステップ 3** SMF が UPF からの障害応答メッセージで受信する原因コードを指定します。

**cause-code** *cause_ID*

例：

```
[smf] smf(config-failure-handling-fh1)#  cause-code  pfcp-entity-in-congestion
```

**表 *140*：原因コード**

| 原因（**Cause**）コード | 説明 |
|---|---|
| • *pfcp* エンティティの輻輳<br>• *peer-overload-reduction* | • *pfcp-entity-in-congestion*：UPF が輻輳している場合は、この原因コードを指定します。<br>• *peer-overload-reduction*：このオプションを指定すると、OCI で受信したピアの過負荷削減のために N4 メッセージをドロップしながら、SMF 上のセッションをクリアできます。 |
| • システム障害<br>• サービスがサポートされていない<br>*session-ctx-not-found* | • *system-failure*：メッセージ処理中の内部またはシステム障害の原因コードを指定します。<br>• *service-not-supported*：サービスがサポートされない場合は、この原因コードを指定します。<br>• *session-ctx-not-found*：メッセージで参照されているセッション コンテキストが存在しない場合に、この原因コードを指定します。 |
| • リソースなし（*no-resource-available*）<br>• 応答を受信しませんでした | • *no-resource-available*：使用可能なリソースがない場合に、この原因コードを指定します。<br>• *no-response-received*：このオプションを指定して、SMF が UPF からの応答を受信しないシナリオを決定します。 |
| 拒否 | この原因コードを指定すると、UPF からの障害応答メッセージ内の原因コードを処理します。原因コードは、この機能で使用可能な CLI コマンドを使用して構成されません。 |
| *mandatory-ie -incorrect* | 受信したメッセージに無効なデータが含まれている場合は、この原因コードを指定します。 |
| • *74*<br>• *2–255* | • *74*：SMF が UPF から原因コード 74 を受信し、かつ N4 障害処理プロファイルで原因コード 74 のアクション終了と構成されている場合、SMF はセッションを削除します。<br>• *2–255*：複数の原因コードを指定する場合は、原因コード値を「-」または「,」のいずれか、または両方を使用して区切ります。たとえば、原因コード 72-74、76、78-100 です。 |

原因コード 0 ～ 255 がサポートされています。原因コードの優先順位は次のとおりです：

1. 定義済みの文字列
2. 番号
3. 範囲
4. 却下

（注）
拒否がデフォルトの原因コードです。

**表 *141* : 原因コードの構成**

| 原因（Cause）コード | 設定 |
|---|---|
| 0–63 | 対応するテンプレート構成 |
| 64-255 | 却下 |

FHT は、デフォルトの動作で構成されている以下の原因コードをサポートしていません：

- request-reject-unspecified
- cond-ie-missing
- invalid-length
- invalid-fw-policy
- invalid-fteid-alloc-opt
- no-established-pfcp-assoc
- rule-creation-mod-failure

**ステップ 4** 障害処理の条件とアクションを構成します。

**action {***ignore* | *retry-terminate* **{ max-retry** *retry_value* **} [condition {** *handover-execution* | *handover-preparation modify* | *idft* | *handover-cancel* **}]**

**例**：

```
[smf] smf(config-failure-handling-fh1)# cause-code pfcp-entity-in-congestion action terminate
  condition handover-execution
```

**condition** コマンドの構成は任意です。

表 *142 :* 構成マトリックス

| メッセージ タイプ | 適用可能なアクション | 該当する原因コード | デフォルトの動作 |
|---|---|---|---|
| N4Session EstablishmentReq | retry-terminate max-retry *retry_value* | • pfcp エンティティの輻輳<br>• peer-overload-reduction<br>• システム障害<br>• サービスがサポートされていない<br>• リソースなし（no-resource-available）<br>• 応答を受信しませんでした<br>• 拒否<br>• 74 | terminate |
| N4Session ModificationReq | terminate | • peer-overload-reduction<br>• mandatory-ie -incorrect<br>• session-ctx-not-found<br>• no-response -received<br>• 拒否<br>• no-resource -available<br>• 74 | continue |
| N4SessionReportReq | • ignore<br>• terminate | 2-255 | terminate |

表 *143 :* 構成可能なアクション

| アクション | 説明 |
|---|---|
| retry-terminate max-retry *retry_value* | 代替 UPF への再試行回数を指定します。再試行が失敗した場合、セッションは終了します。再試行値の範囲は 1 ～ 5 です。デフォルト値は 2 です。<br>（注）<br>すべての UPF が輻輳状態の場合、アクションが続行に設定されていても、コールは失敗します。 |

| アクション | 説明 |
|---|---|
| terminate | セッションを終了するようにアクションを指定します。 |
| ignore | セッションを無視するようにアクションを指定します。 |

- SMF は、N4SessionModificationReq メッセージタイプの障害処理に対してのみ、1 つ以上の条件を構成することを許可します。。

**ステップ 5** （オプション） **show running-config profile failure-handling interface pfcp** コマンドを使用して、UPF 障害処理構成を確認します。

```
[smf] smf# show running-config profile failure-handling interface pfcp
 profile failure-handling fh1
 interface pfcp message N4SessionEstablishmentReq
  cause-code pfcp-entity-in-congestion action retry-terminate max-retry 2
  cause-code system-failure action terminate
  cause-code service-not-supported action terminate
  cause-code no-resource-available action retry-terminate max-retry 3
  cause-code no-response-received action retry-terminate max-retry 1
  cause-code reject action terminate
 exit
 interface pfcp message N4SessionModificationReq
  cause-code mandatory-ie-incorrect action terminate
  cause-code session-ctx-not-found action terminate
  cause-code reject action terminate
 exit
 interface pfcp message N4SessionReportReq
  cause-code 69 action terminate
  cause-code 72-74,76,78-100 action terminate
 exit
exit
```

## 障害プロファイルの関連付けの構成

この構成により、UPF 障害プロファイルが UPF グループ プロファイルに関連付けられます。

### 手順

**ステップ 1** グローバル コンフィギュレーション モードで UPF グループ名を定義します。

**profile upf-group** *upf_group_name*

例：

```
[smf] smf# config
[smf] smf(config)# profile upf-group upfg
```

**ステップ 2** UPF 障害プロファイル名を指定して設定を保存します。

**failure-profile** *failure_profile_name*

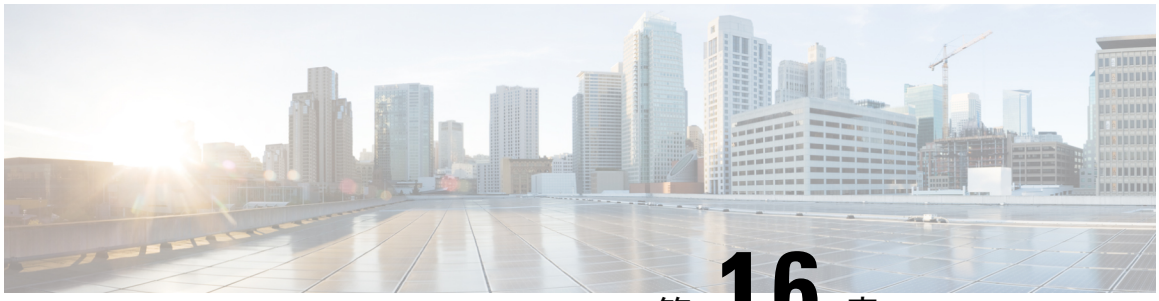
例：

```
[smf] smf(config-upf-group-upfg)# failure-profile failure_profile_name
```

# UPF 障害処理の統計

SMF は、UPF 障害処理に関して、次の統計情報をサポートしています。

- smf_sess_pdn_rel_peer_request_reject：smf_disconnect_stats が拡張され、4G コールと Wi-Fi コールの両方に適用されるこの切断理由が含まれるようになりました。
- smf_sess_pdu_rel_peer_request_reject—smf_disconnect_stats が拡張され、この切断理由が追加されました。これは 5G コールに適用されます。



第 16 章

# アクセスおよびモビリティの手順のフロー失敗の処理


- 機能の概要と変更履歴, on page 463
- 機能説明, on page 464
- 機能の仕組み, on page 464


## 機能の概要と変更履歴

### 要約データ

***Table 144:*** 要約データ

| | |
|---|---|
| 該当製品または機能エリア | SMF |
| 該当プラットフォーム | SMI |
| 機能のデフォルト設定 | 無効：設定が必要 |
| このリリースでの関連する変更点 | N/A |
| 関連資料 | 該当なし |

### 更新履歴

***Table 145:*** マニュアルの変更履歴

| 改訂の詳細 | リリース |
|---|---|
| 最初の導入。 | 2020.02.0 より前 |

# 機能説明

SMF は、アクセスおよびモビリティ手順の QoS フロー障害をサポートしています。SMF は、NG-RAN から N2 への次のコール フローの一部として、QoS フロー障害の詳細を受信します。

- Xn ハンドオーバー
- サービス リクエスト手順（UE とネットワーク開始型）
- AMF 変更あり/変更なしの N2 ハンドオーバー
- N26 4G から 5G へのハンドオーバー
- N26 5G から 4G へのハンドオーバー

# 機能の仕組み

SMF は N2 メッセージの詳細を含む N11 メッセージを処理して、承認された、および失敗した QoS フロー ID を判断します。失敗した QoS フロー ID については、SMF はリソースをローカルで除外し、次の情報を外部インターフェイスに伝達します。

- N4 セッション変更要求を UPF に送信し、QoS フロー ID に適用可能な QER、URR、UL または DL PDR、UL または DL FAR を削除します。
- 削除された URR のマルチユニットの使用状況の詳細を含めて、課金データ更新要求を CHF に送信します。SMF が UPF から使用状況レポートを受信すると、SMF はこのレポートを CHF に送信します。
- N1 メッセージの詳細を含む N1 N2 転送メッセージを PDU セッション変更コマンドとして UE に送信します。
- SMF は、受信したポリシー制御要求トリガおよび SM ポリシー決定の最後の要求ルール データに基づいて、ルール レポートの SM ポリシー制御更新を PCF に送信します。

## コール フロー

このセクションでは、次のコールフローについて説明します。

- XN ハンドオーバー コール フローの QoS フロー障害処理
- N2 ハンドオーバー コール フローの QoS フロー障害処理
- N26 4G から 5G へのハンドオーバー コール フローの QoS フロー障害処理
- サービス要求手順の QoS フロー障害
- PDU UE 同期手順

- フロー障害管理コール フロー

# XN ハンドオーバー中の QoS フロー障害処理

このセクションでは、XN 引き継ぎ中の QoS フロー障害の処理について説明します。

***Figure 81: XN ハンドオーバー中の QoS フロー障害処理***

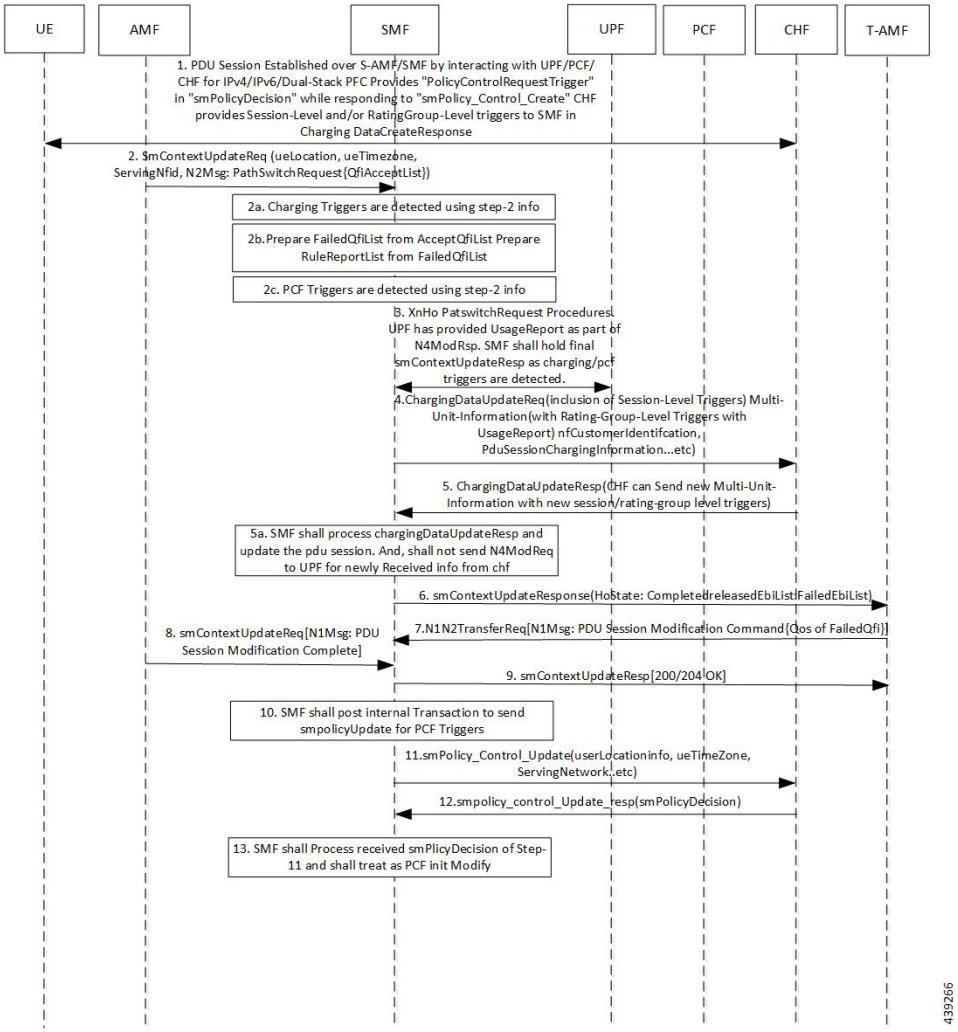


*Table 146: QoS* フロー障害処理コール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | PDU セッションは、IPv4、IPv6、またはデュアルスタックの UPF、PCF、または CHF との通信により、S-AMF および SMF 経由で確立されます。<br>PCF は、SM ポリシー制御の作成要求への応答として、SM ポリシー決定のポリシー制御要求トリガーを提供します。<br>CHF は、課金データ作成応答として、セッションレベルおよび料金設定グループレベルのトリガーを SMF に提供します。 |
| 2 | AMF が SMF に SM コンテキスト更新要求を送信します。この要求には、承認された QoS フロー識別子 (QFI) のリストとともに、UE ロケーション、UE タイムゾーン、および N2 メッセージ パス切り替え要求に関する情報が含まれます。 |
| 2a | SMF は、SM コンテキスト更新要求で受信されたアクセス側の変更を識別します。課金トリガは、ステップ 2 で受信した情報に基づいて識別されます。 |
| 2b | SMF は、受け入れた QFI のリストから失敗した QFI、失敗したルール レポート、および失敗した EPS ベアラー ID（EBI）のリストを抽出します。 |
| 2c | PCF トリガは、ステップ 2 で受信した情報に基づいて識別されます。 |
| 3 | Xn ハンドオーバーの準備手順では、SMF は N4 セッション変更要求を UPF に送信し、受信した T-gNB の DL トンネル情報を更新します。トンネル情報が更新されると、UPF は N4 変更応答として使用レポートを SMF に送信します。SMF は、課金または PCF トリガーが識別されたときに、最終的な SM コンテキスト更新応答を保持します。 |
| 4 | SMF は、CHF に課金データ更新要求を送信します。この要求には、セッションレベルのトリガー、料金設定グループレベルのトリガーと使用レポートを含むマルチユニット情報、顧客識別情報、PDU セッション課金情報などの詳細が含まれます。 |
| 5 | CHF は、課金データ更新応答を SMF に送信します。この応答には、新しいセッションまたは料金設定グループレベルのトリガーを含む複数のユニットの情報が含まれる場合があります。 |
| 5a | SMF は課金データ更新応答を処理し、PDU セッションを更新します。SMF は、CHF から受信した情報の N4 モード要求を UPF に送信しません。 |
| 6 | SMF は、N2 メッセージ パス スイッチ要求の確認応答と失敗した EBI リストのリストを含めて、SM コンテキスト更新応答を送信します。 |
| 7 | SMF および T-AMF は、失敗した QFI に関する QoS の PDU セッション変更の N1 N2 転送要求を処理します。SMF には、QoS フロー障害リストの情報を UE に伝達するための PDU セッション変更コマンドが含まれています。 |

| ステップ | 説明 |
|---|---|
| 8 | AMF は、SM コンテキスト更新要求 N1 メッセージを SMF に送信して、ハンドオーバーの完了について通信します。 |
| 9 | SMF は T-AMF に「200/204 OK」として SM コンテキスト更新応答を送信します。SMF は UE から受信した N1 メッセージを処理しません。 |
| 10 | SMF は内部トランザクションをポストして、PCF トリガーの SM ポリシー更新を PCF に送信します。SMF は、この情報を投稿して、失敗した QFI または特定された防御されたアクセス側トリガーに関するルール レポートを通信します。 |
| 11 | SMF は PCF に SM ポリシー制御の更新を送信します。この更新には、ユーザーの場所情報や UE タイムゾーンなどの詳細が含まれます。 |
| 12 | PCF は、SM ポリシー決定である SM ポリシー制御更新応答を SMF に送信します。 |
| 13 | SMF は受信した SM ポリシー決定を処理し、PCF 変更手順を開始します。 |

## N2 ハンドオーバー中の QoS フロー障害処理

このセクションでは、N2 ハンドオーバー中のフロー障害の処理手順について説明します。

*Figure 82: N2* ハンドオーバー中のフロー障害処理

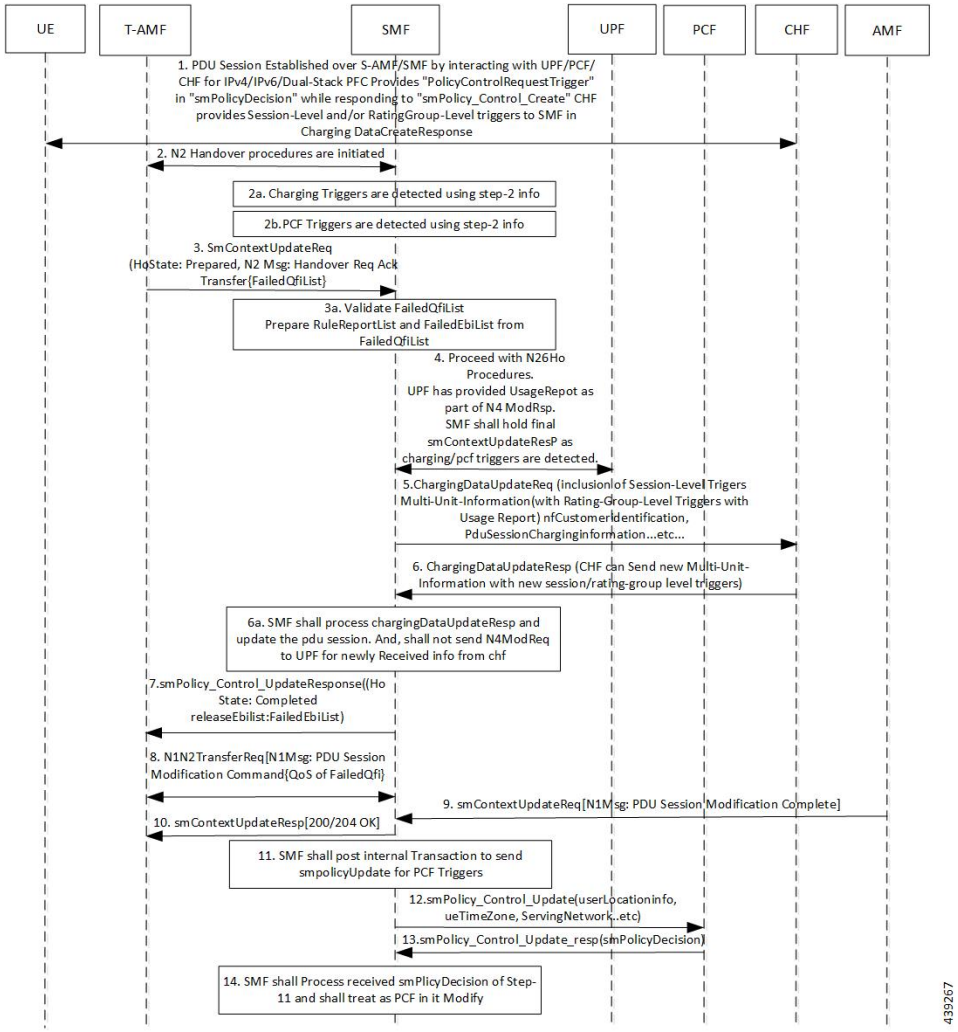



*Table 147: N2* ハンドオーバー中のフロー障害処理の説明

| ステップ | 説明 |
|---|---|
| 1 | PDU セッションは、IPv4、IPv6、またはデュアルスタックの UPF、PCF、または CHF との通信により、S-AMF および SMF 経由で確立されます。<br><br>PCF は、SM ポリシー制御の作成要求への応答として、SM ポリシー決定のポリシー制御要求トリガーを提供します。<br><br>CHF は、課金データ作成応答として、セッションレベルおよび料金設定グループレベルのトリガーを SMF に提供します。 |

| ステップ | 説明 |
|---|---|
| 2 | T-AMF は、SM コンテキスト更新要求を SMF に送信します。この要求には、準備されたハンドオーバー状態、UEの場所、UEのタイムゾーン、ターゲット サービスNF ID、サービス ネットワークに関する情報が含まれます。AMF 間ハンドオフの場合、AMF には NF ID を提供するターゲットが含まれます。 |
| 2a | SMF は、SM コンテキスト更新要求で受信されたアクセス側の変更を識別します。課金トリガは、ステップ 2 で受信した情報に基づいて識別されます。 |
| 2b | PCF トリガは、ステップ 2 で受信した情報に基づいて識別されます。 |
| 3 | T-AMF は、SM コンテキスト更新要求を SMF に送信します。この要求には、Handover Required Transfer Request の N2 メッセージとともに準備されたハンドオーバー状態に関する情報が含まれます。転送要求には、失敗した QFI のリストが含まれます。 |
| 3a | SMF は失敗した QFI のリストを検証して、失敗したルールレポートと失敗した EBI のリストを抽出します。 |
| 4 | N2 ハンドオーバーの準備手順では、SMF は N4 セッション変更要求を UPF に送信し、受信した T-gNB の DL トンネル情報を更新します。トンネル情報が更新されると、UPF は N4 変更応答として使用レポートを SMF に送信します。SMF は、課金または PCF トリガーが識別されたときに、最終的な SM コンテキスト更新応答を保持します。 |
| 5 | SMF は、CHF に課金データ更新要求を送信します。この要求には、セッションレベルのトリガー、料金設定グループレベルのトリガーと使用レポートを含むマルチユニット情報、顧客識別情報、PDU セッション課金情報などの詳細が含まれます。 |
| 6 | CHF は、課金データ更新応答を SMF に送信します。この応答には、新しいセッション レベルまたは料金設定グループレベルのトリガーとともに、マルチユニット情報が含まれています。 |
| 6a | SMF は課金データ更新応答を処理し、PDU セッションを更新します。SMF は、CHF から受信した情報の N4 モード要求を UPF に送信しません。 |
| 7 | SMF は、SM コンテキスト更新応答を完了したハンドオーバー状態で T-AMF に送信します。この応答には、リリースされた EBI と失敗した EBI のリストも含まれています。 |
| 8 | SMF および T-AMF は N1 N2 転送要求を処理します。この要求には、QoS フロー障害リストの情報を UE に伝えるための PDU セッション変更コマンドとしての N1 メッセージが含まれています。 |
| 9 | CHF は、PDU セッション変更の完了に関する N1 メッセージを含む SM コンテキスト更新要求を送信します。 |
| 10 | SMF は、SM コンテキスト更新応答を「200/204 OK」として T-AMF に送信します。SMF は UE から受信した N1 メッセージを処理しません。 |

| ステップ | 説明 |
|---|---|
| 11 | SMF は、内部トランザクションをポストして PCF トリガーの SM ポリシーの更新を送信します。SMF は、この更新を送信して、失敗した QFI または装備されたアクセス側トリガーに関するルール レポートを伝達します。 |
| 12 | SMF は PCF に SM ポリシー制御の更新を送信します。この更新には、ユーザーの場所と UE のタイムゾーンに関する詳細が含まれます。 |
| 13 | PCF は、SM ポリシー決定である SM ポリシー制御更新応答を SMF に送信します。 |
| 14 | SMF は SM ポリシー決定を処理し、PCF によって開始された PDU セッション変更手順として扱います。 |

## N26 4G から 5G へのハンドオーバー中の QoS フロー障害の処理

このセクションでは、N26 4G から 5G へのハンドオーバー中のフロー障害の処理手順について説明します。

*Figure 83: N26 4G から 5G へのハンドオーバー中の QoS フロー障害の処理*

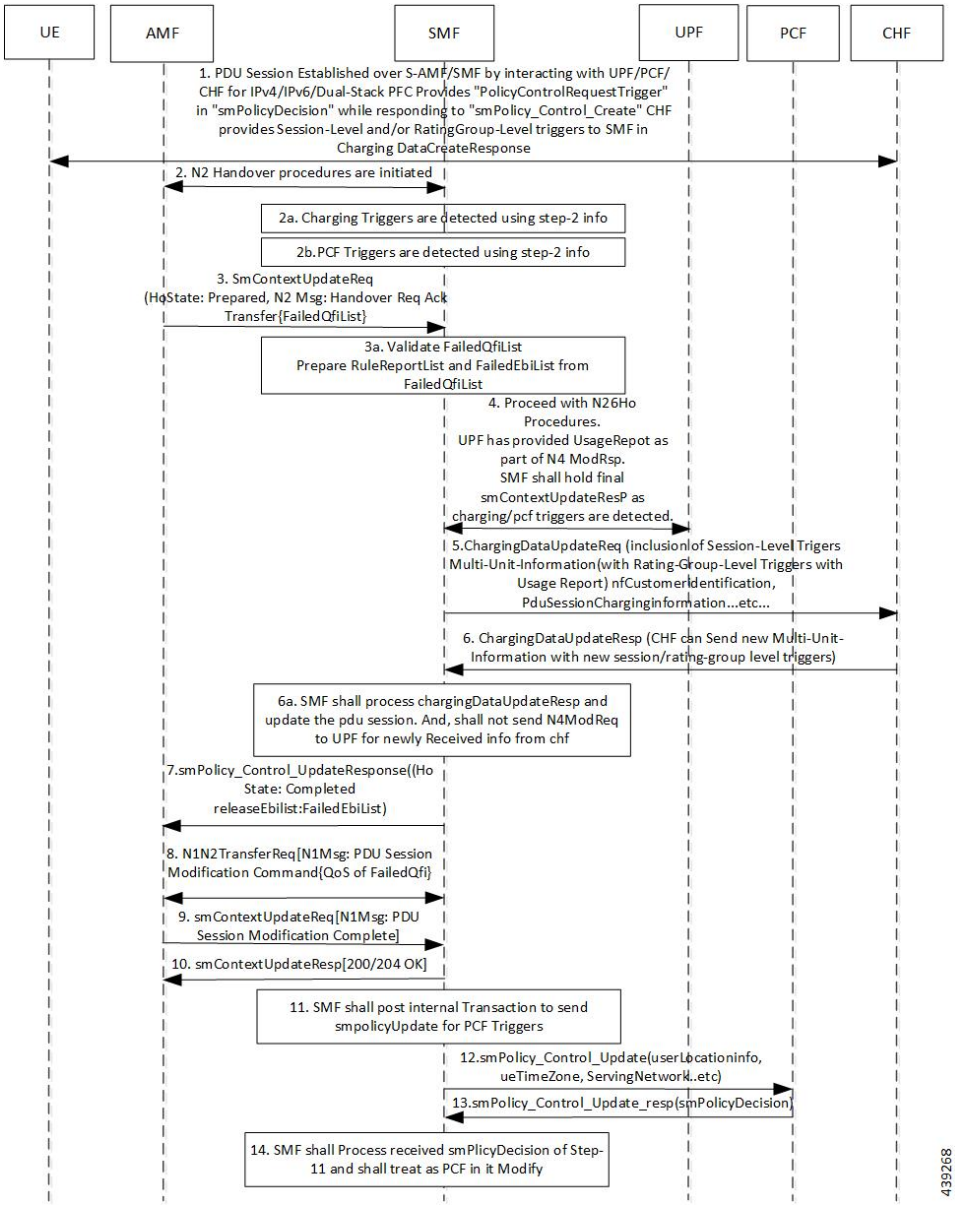


*Table 148: N26 4G から 5G へのハンドオーバー中の QoS フロー障害処理の説明*

| ステップ | 説明 |
|---|---|
| 1 | PDU セッションは、IPv4、IPv6、またはデュアルスタックの UPF、PCF、または CHF との通信により、S-AMF および SMF 経由で確立されます。<br>PCF は、SM ポリシー制御の作成要求への応答として、SM ポリシー決定のポリシー制御要求トリガーを提供します。<br>CHF は、課金データ作成応答として、セッションレベルおよび料金設定グループレベルのトリガーを SMF に提供します。 |
| 2 | T-AMF は、SM コンテキスト更新要求を SMF に送信します。この要求には、準備されたハンドオーバー状態、UEの場所、UEのタイムゾーン、ターゲット サービスNF ID、サービス ネットワークに関する情報が含まれます。AMF 間ハンドオフの場合、AMF には、NF ID を提供するターゲットと、SMF に対して受け入れられた QFI のリストを含む N2 メッセージパス切り替え要求が含まれます。 |
| 2a | SMF は、SM コンテキスト更新要求で受信されたアクセス側の変更を識別します。課金トリガは、ステップ 2 で受信した情報に基づいて識別されます。 |
| 2b | PCF トリガは、ステップ 2 で受信した情報に基づいて識別されます。 |
| 3 | T-AMF は、SM コンテキスト更新要求を SMF に送信します。この要求には、Handover Required Transfer Request の N2 メッセージとともに準備されたハンドオーバー状態に関する情報が含まれます。転送要求には、失敗した QFI のリストが含まれます。 |
| 3a | SMF は失敗した QFI のリストを検証して、失敗したルールレポートと失敗した EBI のリストを抽出します。 |
| 4 | N26 ハンドオーバーの準備手順では、SMF は N4 セッション変更要求を UPF に送信し、受信した T-gNB の DL トンネル情報を更新します。トンネル情報が更新されると、UPF は使用レポートを N4 変更応答として SMF に送信します。SMF は、課金または PCF トリガーが識別されたときに、最終的な SM コンテキスト更新応答を保持します。 |
| 5 | SMF は、CHF に課金データ更新要求を送信します。この要求には、セッションレベルのトリガー、料金設定グループレベルのトリガーと使用レポートを含むマルチユニット情報、顧客識別情報、PDU セッション課金情報などの詳細が含まれます。 |
| 6 | CHF は、課金データ更新応答を SMF に送信します。この応答には、新しいセッション レベルまたは料金設定グループレベルのトリガーとともに、マルチユニット情報が含まれています。 |
| 6a | SMF は課金データ更新応答を処理し、PDU セッションを更新します。SMF は、CHF から受信した情報の N4 モード要求を UPF に送信しません。 |

| ステップ | 説明 |
|---|---|
| 7 | SMF は、SM Context Update Response を完了したハンドオーバー状態で T-AMF に送信します。この応答には、リリースされた EBI と失敗した EBI のリストも含まれています。 |
| 8 | SMF および T-AMF は N1 N2 転送要求を処理します。この要求には、QoS フロー障害リストの情報を UE に伝えるための PDU セッション変更コマンドとしての N1 メッセージが含まれています。 |
| 9 | CHF は、PDU セッション変更の完了に関する N1 メッセージを含む SM コンテキスト更新要求を送信します。 |
| 10 | SMF は、SM コンテキスト更新応答を「200/204 OK」として T-AMF に送信します。SMF は UE から受信した N1 メッセージを処理しません。 |
| 11 | SMF は、内部トランザクションをポストして PCF トリガーの SM ポリシーの更新を送信します。SMF は、この更新を送信して、失敗した QFI または装備されたアクセス側トリガーに関するルール レポートを伝達します。 |
| 12 | SMF は PCF に SM ポリシー制御の更新を送信します。この更新には、ユーザーの場所と UE のタイムゾーンに関する詳細が含まれます。 |
| 13 | PCF は、SM ポリシー決定である SM ポリシー制御更新応答を SMF に送信します。 |
| 14 | SMF は SM ポリシー決定を処理し、PCF によって開始された PDU セッション変更手順として扱います。 |

## サービス要求手順の QoS フロー障害

SMF では、UE とネットワーク サービス要求の両方の手順がサポートされています。これらの手順では、SMF は受信した SM コンテキスト更新要求を処理して、N3 トンネル パスをアイドル状態からアクティブ状態に更新します。

サービス要求手順の QoS フロー障害は、3GPP 23.502、セクション 4.2.3.2 で説明されている方法と同じ方法で処理されます。ただし、QoS フロー失敗リストは、サブスクライバがアイドル状態からアクティブ状態に移行するときに SM コンテキスト更新応答として受信される PDU セッション セットアップ応答転送 N2 メッセージで処理されます。

*Figure 84: PDUIM* アイドルからアクティブ モードへ

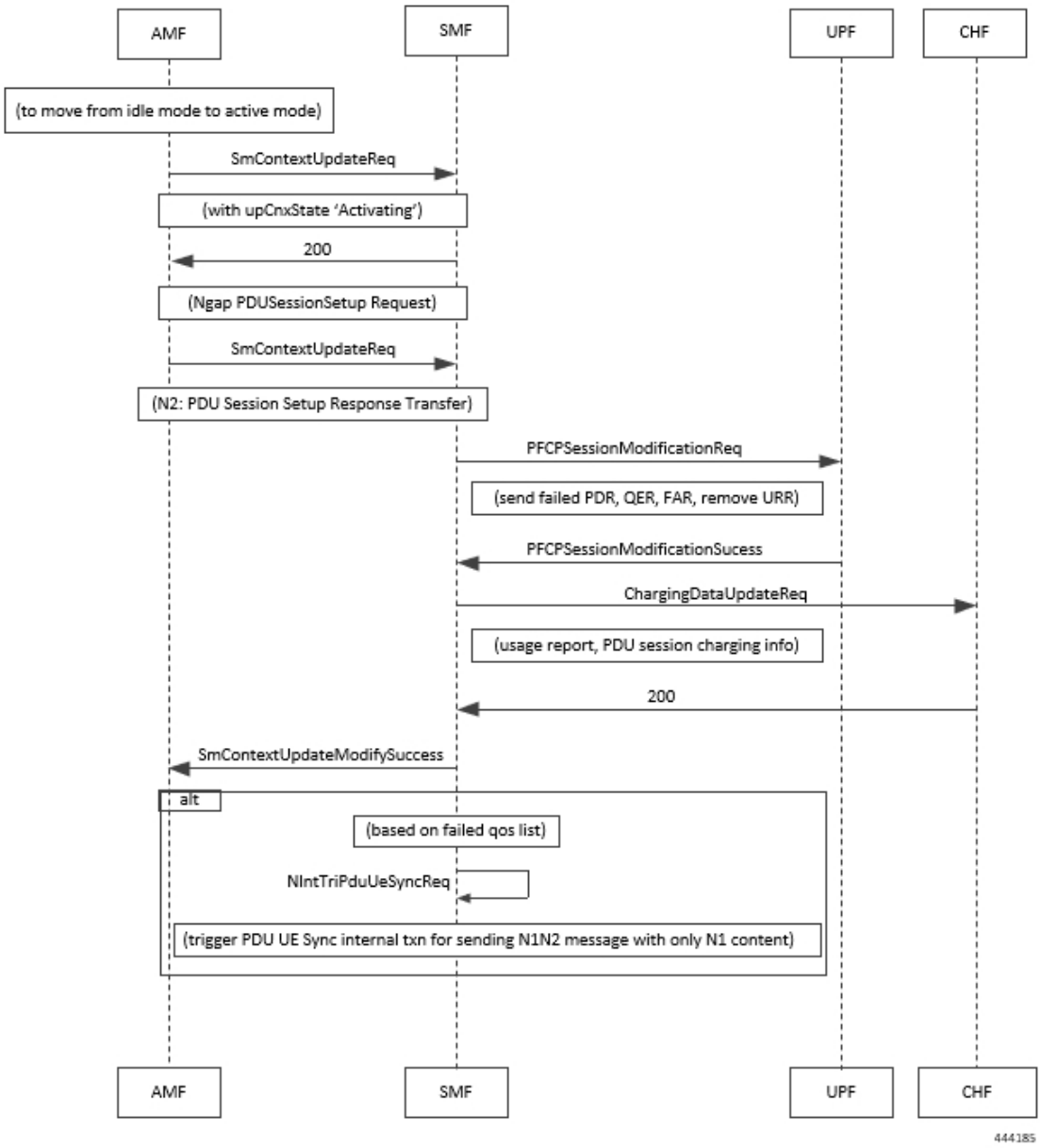



*Table 149:* サービス要求手順の *QoS* フロー障害

| ステップ | 説明 |
|---|---|
| 1 | SMF は、ユーザー プレーンの接続状態が Activated の SM コンテキスト更新要求メッセージを送信します。 |

| ステップ | 説明 |
|---|---|
| 2 | SMF は、AMF への PDU セッション設定要求とともに 200 応答を送信します。AMF は、QoS フロー障害リストを含む N2 メッセージ「**PDU セッション セットアップ応答転送**」 を送信します。 |
| 3 | SMF は、失敗した QFI を検証して、失敗した PCC ルールと失敗したフローを抽出します。 |
| 4 | SMF は受信した DL トンネル情報（gNB、削除 PDR、削除 QER）を更新します。トンネル情報が更新されると、SMF は失敗したフローに基づいて URR を削除し、N4 セッション変更要求を UPF に送信します。 |
| 5 | UPF は、N4 セッション変更応答の一部として使用状況レポートを提供します。SMF は、ユーザープレーンの接続状態に対する SM コンテキスト更新応答をアクティブとして、リリースされた EBI が失敗した EBI として送信され、内部トランザクションをトリガして課金と PCF トリガを処理します。 |
| 6 | SMF は課金データ更新要求を CHF に送信します。この要求には、セッション レベルのトリガー、料金設定グループレベルのトリガーと使用レポートを含むマルチユニット情報、顧客識別情報、PDU セッション課金情報などの詳細が含まれます。 |
| 7 | SMF は、失敗した QFI に基づいて内部トランザクションを送信し、N1/NAS シグナリングを送信するための PDU UE 同期手順を開始します。N1N2 メッセージ転送の PDU UE 同期手順のコール フロー図を参照してください。 |

## PDU UE 同期手順

ここでは UE 同期手順について説明します。

1. アイドル モードでの PDU UE 同期手順では、失敗した QFI、QoS ルール、および EBI を受信します。
2. UE 同期手順では、受信した QFI、QoS ルール ID、および EBI からそれぞれ QoS の説明、QoS ルール、および EPS ベアラー コンテキストを使用して、N1 メッセージ PDU セッション変更コマンドが満たされます。
3. SMF には、作成された N1 コンテナ to N11 メッセージが、N2 コンテンツなしで含まれます。
4. SMF は N1N2 転送要求メッセージを AMF に送信し、N1N2 再送信タイマーを開始します。SMF は N1N2 転送応答を待機しています。
5. N1N2 Transfer Success を受信すると、SMF は N1 の更新を含む SM コンテキスト更新要求を待ちます。N1 更新には、リソース変更成功/リソース変更拒否情報が含まれます。

### 統計

この手順では、次のイベントの統計情報を作成します：

- N1N2TransferRequest の試行
- N1の変更に成功しました
- N1 変更失敗
- UE 同期手順の一時停止
- 他の手順によって一時停止された場合の UE 同期手順の再開時

### N1N2 再送信

N1N2 再送信タイマーが期限切れになると、次のアクションが実行されます：

1. SMF は N1N2 再試行カウンタをインクリメントする
2. SMF は、N11N1N2 転送要求メッセージを AMF に送信し、N1N2 再送信タイマーを再開します。SMF は N1N2 転送応答を待機します。
3. N1N2 Transfer Success を受信すると、SMF は N1 の更新を含む SM コンテキスト更新要求を待ちます。N1 更新には、リソース変更成功/リソース変更拒否情報が含まれます。
4. N1N2 再試行カウンタが構成された最大数に達すると、手順は中止されます。

### 衝突ケース

AMF は、一時的な拒否の原因で N1N2 転送要求を拒否することによって、HO 手順について SMF に通知します。また、他の手順では、UE からの N1 更新を待っている間に UE 同期手順をプリエンプション処理することができます。

図 *85* : 衝突ケース

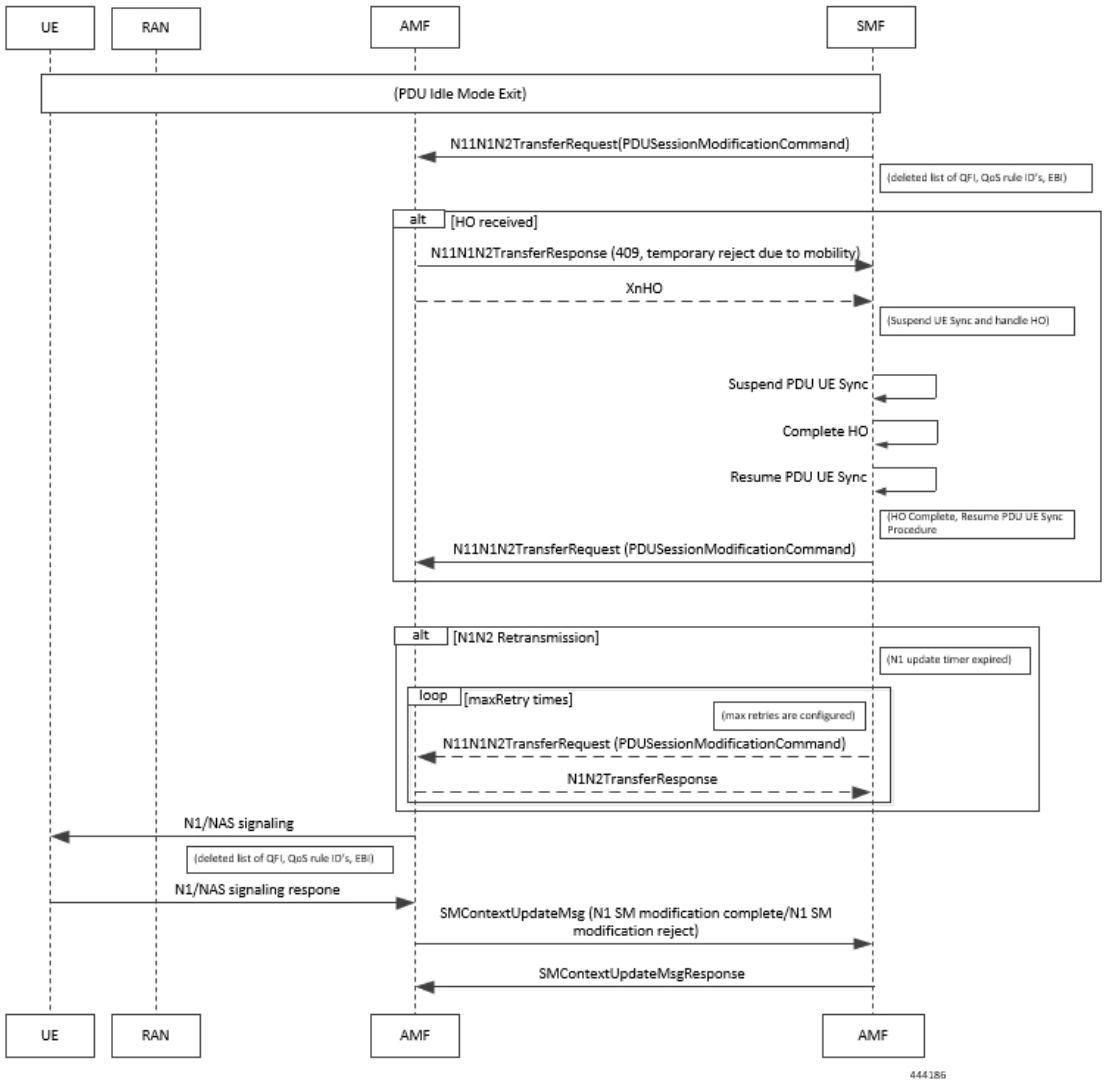



表 *150* : 衝突ケース

| ステップ | 説明 |
|---|---|
| 1 | **一時的な拒否 ハンドオーバー 進行中**の原因による N1N2 転送失敗を受信した場合、SMF は、PDU UE 同期手順をプリエンプトするための HO 手順を待ちます。 |

| ステップ | 説明 |
|---|---|
| 2 | UE からの N1 更新またはハンドオーバーを待っている間に、何らかの手順（ハンドオーバーを含む）がトリガされると、次のようになります。<br>• ハンドオーバー手順によって一時停止されると、N1N2 再試行タイマーが開始されます。<br>• PDU リリースまたは PDU セットアップ手順によって中止された場合、すべてのタイマーがクリーンアップされ、N1N2 再試行が中止されます。 |
| 3 | UE 同期手順がハンドオーバーによって中断された場合、N1N2 再試行タイマーの期限切れ時に、ハンドオーバーが処理された後に UE 同期が再開されます。 |
| 4 | UE 同期手順で RAT が変更されたことが検出された場合、再開時に手順を中止し、タイマーを停止します。 |
| 5 | 同じ RAT で手順を再開すると、UE 同期手順により N11N1N2Transfer 要求メッセージが再開されます。 |

## PDU セットアップ手順中の失敗した QoS フロー識別子の処理

SMF は、PDU セットアップ手順中に失敗した QoS フロー識別子（QFI）の処理をサポートしています。

NG-RANは、さまざまな理由によりQoS フローを拒否します。NG-RAN ノードが QoS フローの確立に失敗したと報告すると、SMF は原因値を使用して確立が失敗した理由を特定します。

図 *86 : PDU* セットアップ手順中の失敗した *QFI* の処理

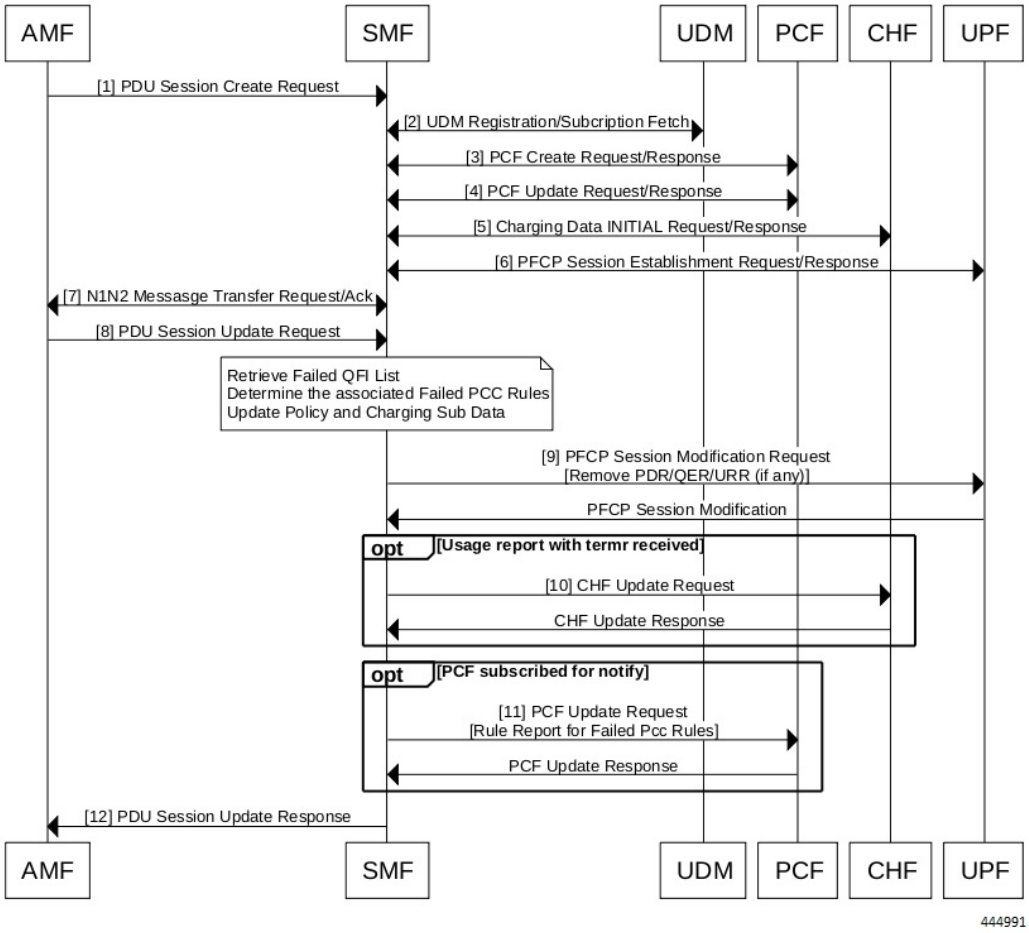



表 *151 : PDU* セットアップ中に失敗した *QFI* 処理の説明

| ステップ | 説明 |
|---|---|
| 1-7 | SMF、AMF、UDM、PCF、CHF、およびUPFは相互に通信して、3GPP仕様で定義されている PDU セットアップ手順を実行します。 |
| 8 | AMF は、SM コンテキスト更新要求を SMF に送信します。この要求は、N2 ペイロード「PDU セッション リソース セットアップ応答転送」を伝送します。このメッセージには、QoS フローの確立に失敗した QoS フローのリスト（存在する場合）がリスト IE に含まれます。<br>SMF は失敗した PCC ルールとそれらに関連付けられた課金記述子を削除対象としてマークします。 |

| ステップ | 説明 |
|---|---|
| 9 | SMF は UPF に PFCP セッション変更メッセージを送信します。このメッセージは、ダウンリンク（DL）トンネルのエンドポイント識別子（TEID）の既存の更新 FAR に加えて、失敗した PCC ルールのパケット検出ルール（PDR）の削除、QoS 適用ルールの削除（QER）、および使用状況レポートルールの削除（URR）を送信します。の成功した PCC ルール。 |
| 10 | SMF は終了要求を受け取ると、CHF 更新要求メッセージを CHF に送信します。CHF は、CHF 更新応答を確認応答として送信します。 |
| 11 | PCF が失敗した PCC ルールに関する通知をサブスクライブしている場合、SMF は、NG-RAN によってドロップされた失敗した PCC ルールを含むルール レポートとともに PCF 更新要求を送信します。 |
| 12 | SMF は PDU セッション更新応答を AMF に送信します。<br>SMF は、失敗した QFI リストに基づいて内部トランザクションをトリガーします。次に、SMF は PDU UE 同期手順を開始して、N1/NAS シグナリングを送信します。<br>SMF は N1 メッセージングを使用して、失敗した QoS フローについて UE に通知し、関連する失敗した PCC ルールについては UPF ノードと PCF ノードに通知します。 |

# PDU セッション変更中に失敗した QoS フロー識別子の処理

SMF は、PDU セッション変更中に N2 インターフェイスを介して失敗した QoS フローの処理をサポートしています。

PDU セッションまたは QoS フローの変更が失敗した場合、NG-RAN ノードは古い構成にフォールバックします。つまり、PDU SESSION RESOURCE MODIFY REQUEST メッセージを受信する前に使用できたセッションまたはフローの構成にフォールバックします。

SMF は、PDU SESSION RESOURCE MODIFY REQUEST 中にフローの追加/変更が失敗した QoS フロー識別子を受信します。

新しいフローの追加が失敗した場合、SMF は次の操作を実行します。

- N1（UE）に向かう失敗したフローを削除します。
- 失敗したフロー関連情報の N4（UPF）への送信を停止します。
- N40（CHF）への失敗したフロー関連情報の送信を停止します。
- トリガーが有効になっているかどうかを確認し、失敗したフローのルール レポートを N7（PCF）に送信します。

フローの変更が失敗した場合、SMF は次の処理を実行します。

- N1（UE）に失敗したフローの古い情報を置き換えます。

- 変更されたフロー関連情報の N4（UPF）への送信を停止します。
- 変更されたフロー関連情報の N40（CHF）への送信を停止します。
- トリガが有効になっているかどうかを確認し、失敗したフローのルール レポートを N7（PCF）に送信します。

以下の表は、PDU セッション リソース変更失敗転送 IE に含まれる原因値に対する SMF の動作をまとめたものです。これらの原因値は、PDU セッション変更手順に適用されます。

| 原因グループ | 原因値 | SMF の動作 | コメント |
|---|---|---|---|
| 無線ネットワーク層の原因 | | | |
| | 未指定 | | 全般 |
| | 不明な PDU セッション ID | セッションの削除 | N1 FiberGSM 原因の再アクティブ化が要求されました |
| | 不明な QoS フロー ID | 削除の詳細を N1 に送信します<br>ルールに関するPCFレポートを送信します | |
| | 複数の PDU セッション ID インスタンス | セッションの削除 | |
| | 複数のインスタンス | セッションの削除 | N1 FiberGSM 原因の再アクティブ化を要求 |
| | XN ハンドオーバーがトリガーされました | コリジョン処理に基づいて対処する | |
| | サポートされていない 5QI 値 | 削除の詳細を N1 に送信<br>ルールに関するPCFレポートの送信 | |
| | IMS 音声 EPS フォールバックまたは RAT フォールバックがトリガされました | すでにサポート済み | |
| トランスポート層 | | | |

| 原因グループ | 原因値 | SMF の動作 | コメント |
|---|---|---|---|
| | リソースが使用できません | 削除の詳細を N1 に送信<br>ルールに関するPCFレポートの送信 | |
| | 未指定 | | |
| NAS の原因 | | | |
| | 通常リリース | セッションの削除 | |
| | 認証の失敗 | セッションの削除 | |
| | 登録解除 | セッションの削除 | |
| | 未指定 | セッションの削除 | |
| プロトコル原因 | | | |
| | 転送構文エラー | N1 ロールバック<br>エラーログの失敗手順 | |
| | 抽象構文エラー（拒否） | N1 ロールバック<br>エラーログの失敗手順 | |
| | 抽象構文エラー（無視および通知） | N1 ロールバック<br>エラーログの失敗手順 | |
| | メッセージに受信状態との互換性がありません。 | N1 ロールバック<br>エラーログの失敗手順 | |
| | 構文エラー | N1 ロールバック<br>エラーログの失敗手順 | |
| | 抽象構文エラー（誤って作成されたメッセージ） | N1 ロールバック<br>エラーログの失敗手順 | |
| | 未指定 | N1 ロールバック<br>エラーログの失敗手順 | |
| その他の原因 | | | |

| 原因グループ | 原因値 | SMF の動作 | コメント |
|---|---|---|---|
| | 処理の過負荷を制御する | N1 ロールバック<br>エラーログの失敗手順 | |
| | ユーザープレーンの処理リソースが不足しています | N1 ロールバック<br>エラーログの失敗手順 | |
| | ハードウェア障害 | セッションの削除 | |
| | O&M 介入 | N1 ロールバック<br>エラーログの失敗手順 | |
| | 不明な PLMN | セッションの削除 | |

### バルク統計

次の統計情報は、N2 インターフェイスを介した失敗した QoS フローに関する詳細を提供します。

- policy_pdu_flows_total
  - 試行回数の合計
  - 成功の合計
  - 失敗回数の合計
- policy_pdu_flows_current
  - 現在の試行回数
  - 現在は成功しました
  - 現在は失敗しました

## フロー障害管理コール フロー

次のコール フローは、EPS から 5GS へのハンドオーバー中のさまざまなフロー障害シナリオの詳細を示しています。このコール フローでは、SMF がこれらの障害を管理し、5GS ネットワーク要素とサブスクライバ間でフローが失われないように維持する方法についても説明します。

- EPSの送信元から5GSのハンドオーバーへのフロー障害
- EPSのターゲットから5GSのハンドオーバーへのフロー障害

図 *87 :* フロー障害管理コール フロー

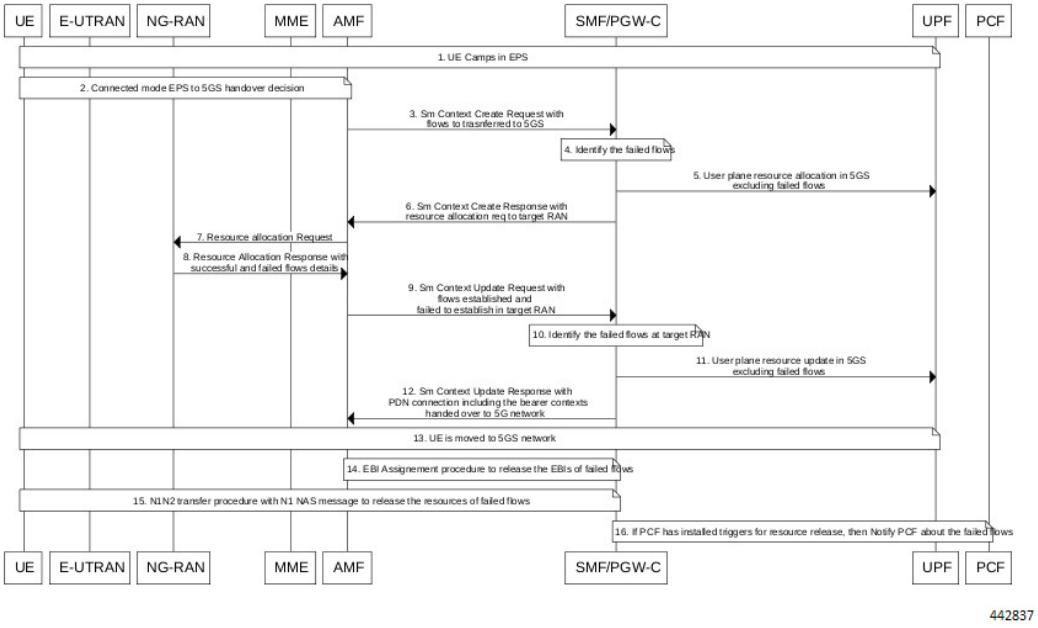



表 *152 :* フロー障害管理コール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | EPS インターワーキング対応 UE は、最初に EPS ネットワークに配置します。 |
| 2 | この手順では、接続モードの EPS から 5GS へのハンドオーバーの決定を行います。 |
| 3 | EPS から 5GS へのハンドオーバー手順中に、AMF からの Sm コンテキスト作成要求の PDN 接続は、5GS ネットワークに渡されるEPS ベアラー コンテキストを伝送します。 |
| 4 | SMF は、EPS で確立され、PDN 接続で欠落しているベアラー コンテキストを失敗したフローとして識別します。 |
| 5 | SMF は5GS ネットワークでリソース割り当てを実行し、失敗したフローを除いてUPF に送信します。 |
| 6 | SMF は、リソース割り当て要求を含む Sm コンテキスト作成応答をターゲット RAN に送信します。 |
| 7 | AMF は、リソース割り当て要求をNG-RANに転送します。 |

| ステップ | 説明 |
|---|---|
| 8 | NG-RANは、成功したフローと失敗したフローの詳細を含むリソース割り当て応答をAMFに送信します。<br>ターゲット RAN ノードは、EPS から 5GS への引き継ぎ手続き中に、要求されたすべてのフローにリソースを割り当てることができない場合があります。ターゲットRANは、リソース割り当て応答でこれらの失敗したフローに関する情報を共有します。 |
| 9 | AMF は、ターゲット RAN で確立および確立に失敗したフローを含む Sm コンテキスト更新要求を送信します。 |
| 10 | SMF は、ターゲット RAN で失敗したフローを識別します。 |
| 11 | SMF は、失敗したフローを除く 5G ネットワークでユーザー プレーン リソースの更新を実行します。 |
| 12 | SMF は、5GS ネットワークに渡されたベアラー コンテキストを含む PDN 接続を使用して Sm コンテキスト更新応答を送信します。 |
| 13 | UE が 5GS ネットワークに移動します。 |
| 14 | SMF は EBI 割り当て手順を使用して、失敗したフローの EBI を解放します。 |
| 15 | SMF は、失敗したフローのリソースを削除するために、N1 NAS メッセージを含む N1N2 転送要求を UE に送信します。 |
| 16 | PCFがリソースを解放するためのトリガーをインストールしている場合、SMFは失敗したフローを PCF に通知します。 |

## EPS から 5GS ハンドオーバーへの送信元からのフロー失敗の処理

次のコール フローは、EPS の送信元 RAN から 5GS ハンドオーバーへのフロー障害の処理を示しています。

図 *88 :* フロー失敗処理コール フロー（*EPS* の送信元から *5GS* ハンドオーバーへ）

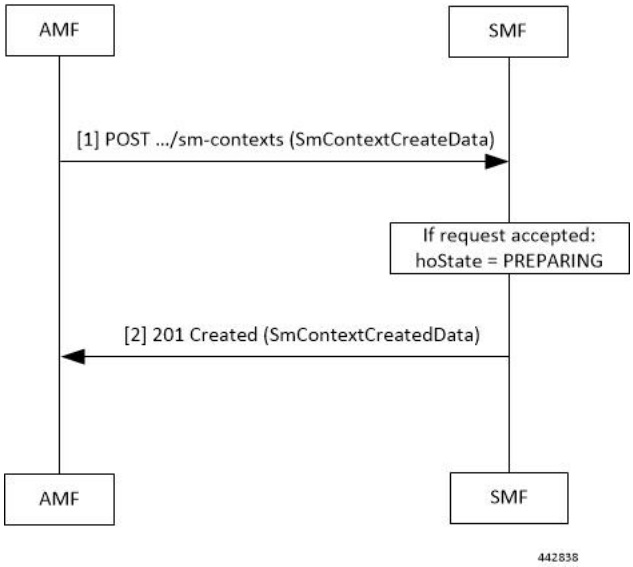



表 *153 :* フロー失敗処理コール フローの説明（*EPS* の送信元から *5GS* ハンドオーバーへ）

| ステップ | 説明 |
|---|---|
| 1 | AMF は、次の追加情報を含む Sm Context Create Service の POST 要求を送信します。<br>• 作成される個々の SM コンテキスト リソースを表す、EPS ベアラー コンテキストを含む UE EPS PDN 接続。UE EPS PDN 接続は、送信元が 5GS ネットワークで確立を望まないフローを伝送できない場合があります。<br>• hoState attribute set to PREPARING<br>• ソースMMEから転送要求メッセージで受信したターゲットID IEに基づいて、ターゲットRANノードIDとTAIを識別するtargetId。 |

| ステップ | 説明 |
|---|---|
| 2 | 対応する PDU セッションが EPS ベアラー コンテキストに基づいて検出され、5GS ネットワークへの PDN 接続のハンドオーバーが可能な場合、SMF は次の情報を含む 201 Created 応答を返します。<br>• PREPARING および N2 SM 情報に構成された hoState 属性。これにより、UE EPS PDN接続で受信されなかったフローを除き、PDUセッションにリソースを割り当てるようターゲット RAN に要求します。<br>• EPS PDN 接続のデフォルトの EPS ベアラー ID に対応する PDU セッション ID。<br>• PDU セッションに割り当てられた EBI を含む allocatedEbiList。<br>POST 応答には、Location ヘッダーと、作成された SM コンテキスト リソースの URI が含まれます。<br>AMF は、PDU セッション ID と SMF ID の関連付け、および PDU セッション ID に関連付けられた割り当て済みの EBI を保存します。 |

## EPS から 5GS へのハンドオーバーでのターゲットからのフロー失敗の処理

次のコールフローは、EPSのターゲットRANから5GSのハンドオーバーへのフロー障害の処理を示しています。

**図 *89 :* フロー失敗処理コール フロー（*EPS* のターゲットから *5GS* ハンドオーバーへ）**

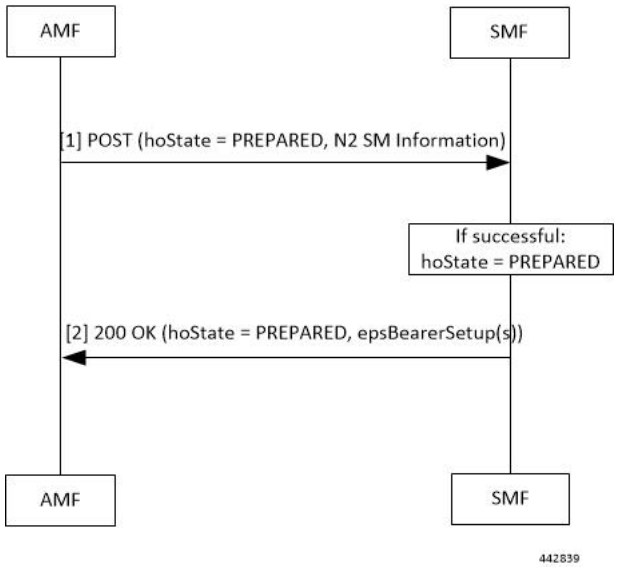


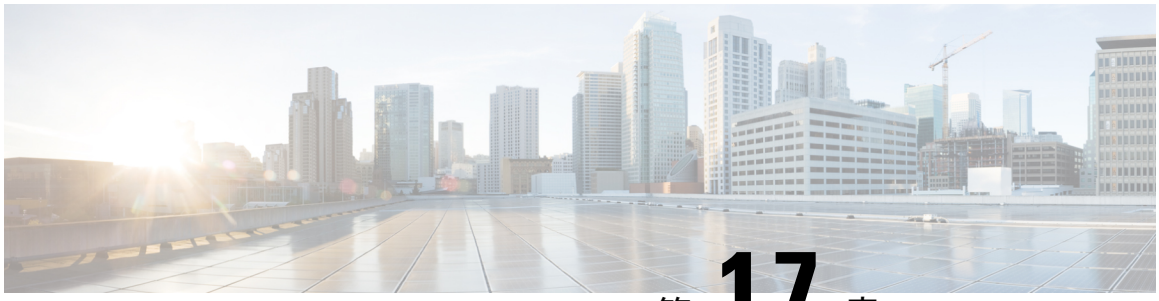
表 *154 :* フロー失敗処理コール フローの説明（*EPS* のターゲットから *5GS* ハンドオーバーへ）

| ステップ | 説明 |
|---|---|
| 1 | AMFは、次の情報を含む POST 要求を送信することにより、SMF内のSMコンテキストを更新します：<br>• hoState attribute set to PREPARED<br>• ターゲット RAN から受信した N2 SM 情報。これには、この PDU セッションのユーザー データのダウンリンク ターミネーション ポイントのトランスポート層アドレスとトンネル エンドポイントが含まれます（つまり、ダウンリンク トラフィックのターゲット RAN の GTP-U F-TEID）。ターゲットの RAN が PDU セッションのリソースの確立に成功した。ターゲットRANがすべてのフローのリソースを確立できない可能性があります。ターゲット RAN には、これらの失敗したフロー情報が含まれます。 |
| 2 | ターゲットRANがPDUセッションのリソースの確立に成功した場合、SMFはhoState属性を PREPARED に設定し、次の情報を含む 200 OK 応答を返します。<br>• hoState attribute set to PREPARED<br>• 5GS に正常に渡された EPS ベアラー コンテキストのリストと、RAN から受信した受け入れられた QFI のリストに基づいて生成されたデータ転送用の CN トンネル情報を含む epsBearerSetup IE。これは、5GS ネットワークに渡されるフローの最終リストです。 |

# 標準準拠

アクセスおよびモビリティ手順の QoS フロー障害処理機能は、次の規格に準拠します。

- *3GPP TS 23.502 V16.1.1（2019-06）*



第 17 章

# GTPP エンドポイント


- 機能の概要と変更履歴 （489 ページ）
- 機能説明 （490 ページ）
- 情報要素サポート （493 ページ）
- 標準準拠 （494 ページ）
- 制限事項 （494 ページ）
- GTPP プロファイルの構成 （495 ページ）
- GTPP エンドポイントの構成 （498 ページ）
- GTPP サービスのモニターとトラブルシューティング （500 ページ）


## 機能の概要と変更履歴

### 要約データ

表 *155* : 要約データ

| | |
|---|---|
| 該当製品または機能エリア | SMF |
| 該当プラットフォーム | SMI |
| 機能のデフォルト設定 | 有効：常時オン |
| 関連資料 | 該当なし |

### 更新履歴

表 *156* : マニュアルの変更履歴

| 改訂の詳細 | リリース |
|---|---|
| 最初の導入。 | 2023.03.0 |

# 機能説明

GTPP エンドポイントは、SMF サービスの GPRS Tunneling Protocol Prime（GTPP）プロトコル機能を有効にするアプリ インフラベースのサービスです。レガシー インターフェイスを使用する SMF は、GTPP エンドポイントの GTPP 課金（Gz）インターフェイスをサポートします。

オフライン課金の場合、Gz は、課金データ機能 (CDF) から CDR の転送に関する CGF への参照ポイントです。

GTPP エンドポイントは、SMF サービスに次のサポートを提供します。

- ベアラー レベルで使用状況とイベント アカウンティングを処理し、アカウンティング情報はサブスクライバ セッションの一部として保存されます。
- このアカウンティング情報から CDR コンテンツを生成し、GTPP エンドポイントに転送します。GTPP エンドポイントは、（構成されたディクショナリに基づいて）受信した CDR を ASN.1 にエンコードします。
- GTPP プロトコルを使用して、受信した CDR を CGF サーバーに送信します。

この機能の詳細については、『UCC 5G SMF 構成および管理ガイド > GTPP エンドポイント』章を参照してください。

## 課金関連の転送

各課金データ機能（CDF）には、CDR を送信できる課金ゲートウェイ機能（CGF）の O&M 構成可能なアドレス リストがあります。リストは CGF アドレス 優先順位に構成されています。プライマリ CGF が使用できない場合、CDF はセカンダリ CGF などに CDR を送信します。

各 CDR 生成関数は、同じ PLMN の CGF にのみレコードを送信し、他の PLMN にある CGF には送信しません。

PLMN の各 CGF は、冗長性を確保する場合に別の CGF アドレスを推奨するために、他の CGF のネットワーク アドレスを認識している必要があります。これは、各 CGF がピアの CGF アドレスの構成可能なリストを持つことができるようにする O&M 構成機能によって実現されます。

## GTPP を介した CDR トランスポート

GTPP は、課金データ機能（CDF）から課金データ レコード（CDR）を配信し、課金ゲートウェイ機能 CGF に CDR を生成します。CGF が CDF の外側に存在する場合は、GTPP プロトコルが必要です。これは、バックボーン ネットワークでパケット データのトンネリングに使用される GTP のいくつかの側面を利用します。

GTPP は Gz インターフェイス上で動作し、次の機能を実行します。

- CDF と CGF 間で CDR を転送します。

- CDR を別の CGF にリダイレクトします。
- エコー メッセージングを使用して、通信しているピア間の通信障害を検出します。
- CDR 転送機能についてピアにアドバタイズします。たとえば、一定期間のサービス ダウンタイム後などです。
- 冗長動作中に発生する可能性のある重複 CDR を防止します。構成されている場合、CDR 重複防止機能は、重複する可能性のある CDR パケットをマークし、最終的な重複削除タスクを CGF または課金ドメインに委任することによって実行されます。

# パス プロトコル

GTPP は、課金を促進するため、パス プロトコルを使用して CDF から CGF に Gz インターフェイス経由で CDR を転送します。GTPP では UDP パス プロトコルがサポートされています。

（注） パス プロトコル TCP はサポートされていません

- 要求メッセージのシグナリング用ポート：
  - サーバ ポート番号 3386 の UDP 宛先ポートは、GTPP 用に予約されています。または、O&M によって構成された別のポートを使用できます。
  - UDP送信元ポートは、ネットワーク要素を送信するためにローカルに割り当てられたポート番号です。
- 応答メッセージのシグナリング用ポート：
  - UDP 宛先ポートは、対応する要求メッセージの送信元ポートの値です。
  - UDP 送信元ポートは、対応する要求の宛先ポートからの値です。

# GTPP メッセージ タイプ

GTPP は、関連付けられた 2 つのノード間のメッセージのセットを定義します。次の表に、syslog メッセージとそのフォーマットを示します。

**表 *157: GTPP* メッセージ**

| メッセージ タイプ値（10 進数） | GTPP メッセージ |
|---|---|
| 1 | エコー要求 |
| 2 | エコー応答 |
| 3 | サポートされていないバージョン。 |

| メッセージ タイプ値（10 進数） | GTPP メッセージ |
|---|---|
| 4 | ノード存続要求 |
| 5 | ノード存続応答 |
| 6 | リダイレクト要求 |
| 7 | リダイレクト応答 |
| 240 | データ レコード転送要求 |
| 241 | データ レコード転送応答 |

# エンドポイント GTP Prime

**k8s use-volume-claim Pod** が true に設定されている場合、エンドポイント GTP Prime を主に使用して、該当するストレージ サイズ制限（デフォルト 1 GB）を設定します。gtpp-profiles の構成だけで gtpp-ep ポッドが起動しますが、**storage**や**replica**などの基本構成を使用して、gtpprime エンドポイントも構成することをお勧めします。この構成は、gtpp-ep ポッドによって使用されます。

Gz インターフェイスの下のエンドポイントで、GTPP プロファイルの課金エージェントの IP アドレスとポートを構成します。

（注） **gtpp-ep** は常に **nodes** 構成を無視します。**k8s single-node** が false に設定されている場合、レプリカとノードの構成に関係なく、アクティブ モードまたはスタンバイ モードで gtpp-epP ポッドの 2 つのレプリカが生成されます。

# GTPP レジリエンシ

GTPP エンドポイントは、CDR アーカイブとファイル ストレージをサポートすることでレジリエンスを提供します。

## CDR アーカイブ

CDR 過負荷のシナリオでは、CGF サーバーの応答が遅くなります。このシナリオでは、sendReqList バッファがいっぱいであるために CDR が確認されず、CDR がドロップします。このような場合、CDR のドロップを回避するために、GTPP エンドポイントは新しい CDR をアーカイブ リストにエンキューします。

GTPP は次の方法で CDR アーカイブを実行します。

- アーカイブ リストのフラッシュは、ネットワークの負荷の状態に応じて、ペースを加えて行われます。

- すべての CGF が非アクティブになった後、またはバックツーバック スイッチオーバーにより、アーカイブ済みの CDR が失われないように、アーカイブ レコードはペースを加えて HDD に書き込まれます。
- アーカイブ リストは、スタンバイ GTPP エンドポイント ポッドに複製されます。

（注）
- アーカイブ リストは、GTPP プロファイル レベルごとに維持されます。アーカイブ リストの最大サイズは 5M です。
- 構成された最大サイズに達すると、最も古いレコードが消去され、新しいレコードが追加されます。
- アーカイブ リストがスタンバイ ポッドに複製されます。アクティブ ポッドが非アクティブになると、スタンバイ ポッドがアクティブ ポッドになり、すべてのアーカイブ レコードを保持するために CDR の処理を開始します。

## CDR ファイル ストレージ

GTPP は次の方法で CDR ファイル ストレージを実行します：

1. すべての CGF が非アクティブの場合、すべての CDR はアクティブな GTTP エンドポイント上の HDD 内のファイルに書き込まれます。
2. CDR はスタンバイ GTPP エンドポイントに保存されます。
3. 非アクティブの CGF がアクティブになると、アクティブな GTPP エンドポイント上のファイルから CDR が読み取られ、CGF に送信されます。
4. 1 つのファイルからすべての CDR が読み取られた後、ファイルはアクティブな GTPP エンドポイントから削除されます。次に、ファイルの複製の削除情報がスタンバイ GTPP エンドポイントに送信されます。
5. スタンバイ GTPP エンドポイントが HDD からファイルを削除します。

（注） HDD からの CDR の読み取りプロセス中に、一部の CDR が CGF に送信され、一部の CDR がまだファイル内にあり、アクティブな GTPP エンドポイントが非アクティブになると、最後の読み取りファイルが新しいアクティブな GTPP エンドポイントポッドから送信されます。このような場合、CGF はさまざまな重複 CDR を受信します。

# 情報要素サポート

GTPP 機能による Gz サポートでサポートされる情報要素（IE）を次に示します。

表 *158 : TLV* および *TV IE*

| 情報要素 | 説明 |
|---|---|
| **TLV 情報要素** | |
| 254 | 推奨ノードのアドレス |
| 253 | 要求の応答数 |
| 252 | データ レコード パケット |
| 251 | 課金ゲートウェイ アドレス（この IE は TS 29.060 [200] でも使用されます） |
| 250 | キャンセルされたパケットのシーケンス番号 |
| 249 | リリースされたパケットのシーケンス番号 |
| **TV 情報要素** | |
| 127 | 課金 ID |
| 126 | パケット転送コマンド |

# 標準準拠

GTPP エンドポイントは、次の課金固有の 3GPP 標準規格に準拠しています。

- *3GPP TS 32.251*「*Telecommunication management;Charging management;Packet Switched (PS) domainCharging*」
- *3GPP TS 32.295*「*Telecommunication management; Charging management; Charging Data Record (CDR) transfer*」
- *3GPP TS 32.297*「*Telecommunication management; Charging management; Charging Data Record (CDR) file format and transfer*」
- *3GPP TS 32.298*「*Telecommunication management; Charging management; Charging Data Record (CDR) parameter description*」

# 制限事項

次に、Diameter インターフェイス課金機能を使用した SMF の制限を示します。

- Diameter インターフェイスを備えた SMF は、ローカル ストレージ モード、TCP、およびリダイレクト要求または応答をサポートしていません。

- Diameter インターフェイスを使用した SMF は、custom24 CDR ディクショナリのみをサポートします。
- スイッチオーバーの場合、新しいスタンバイ GTPP ポッドでは、新しい CDR 送信要求バッファのみがチェックされます。
- スイッチオーバーの場合、新しいアーカイブのみが新しいスタンバイ GTPP ポッドでチェックされます。
- 二重障害では、古いアーカイブ CDR と古い送信要求バッファが失われます。

# GTPP プロファイルの構成

GTPP プロファイルを構成するには、次の構成を使用します。

```
config
  profile gtpp-profile profile_name gtpp
    dictionary
    ignore  ignore_value
    instance-id
      charging-agent address IPv4_adress port UDP_port
     server{ cgf address IPv4_adress max-cdrs max_cdrs { node-alive Enable
| Disable}
           port UDP_port priority priority deadtime time_interval
           echo-interval  echo_interval timeout timeout_val max-retry
           max_retry max-pdu-size max_pdu_size wait-time time_interval }
    local-storage
    mode
      local
      streaming-parallel
    cgf-server-redundancy-support
   exit
 exit
exit
```

注：

- **dictionary**：CDR の ASN.1 ベースのエンコーディング用のディクショナリを指定します。
- **ignore** *ignore_value*：エコー RC 変更を無視する構成を指定します。この CLI 制御オプションでは、エコー応答 RC の変更による CGF パス障害を柔軟に検出できます。
- instance-id **gr_instanceID**：GR インスタンス ID を指定します。
  - **charging-agent**：課金エージェントを構成します。
    - **address***IPv4_address*：CGF に CDR レコードを送信するために使用されるエンドポイント内に構成されているインターフェイスの IP アドレスを指定します。
    - **port**：UDP ポートを指定します。

（注） GTPP プロファイルで構成された課金エージェントの IP アドレスとポートは、Gz インターフェイス下のエンドポイント gtpprime でも構成する必要があります。課金エージェントの IP アドレスとポートのランタイム構成の更新は推奨されません。新しい課金エージェントの IP アドレスとポートを含む新しいプロファイルを追加してください。

- **server**：電子メール サーバの詳細の構成
  - **cgf**：DHCP サーバで次のパラメータを構成します。
    - **address** *IPv4_address*：CGF サーバの IPv4 アドレスをドット付き 10 進表記の範囲を使用して入力します。
    - **max**：CGF の未確認 CDR の最大数を構成します。1 ～ 20 の整数です。

（注） **max** の実行時の構成変更は推奨されません。以下の手順を実行します。

1. 古い **cgf** がある **max** ] を削除してから、変更を確定します。
2. 新しい **max** 値で **cgf** を再度追加します。

- **node-alive Enable | Disable** ：GTPP サーバ（CGF など）へのノード アライブ要求の送信を有効または無効にします。
- **port**：CGF が使用しているポートを指定します。
- **priority**：システムが使用する CGF サーバを選択しているときに、このサーバの相対的な優先順位を指定します。

- **deadtime**：デッドタイムを秒単位で構成します。入力値は 1 ～ 65535 までの整数である必要があります。デフォルトは 120 です。
- **max-cdrs**：GTPP メッセージ内の CDR の最大数を指定します。値は 1 から 255 までの整数値です。
- **max-pdu-size**：PDU の最大サイズ（バイト単位）を指定します。1024 ー 1460 の範囲の である必要があります。
- **timeout**：システムが応答しない CGF との通信を試行する回数を指定します。
- **wait-time**：GTPP 要求を送信するまでの待機時間を指定します。

- **local-storage**：ローカル ストレージの詳細を指定します。

- **mode**：使用するストレージ モードを指定します。
  - **local**：HDD を使用して CDR を保存するように指定します。
  - **streaming-parallel**：CGF が失敗した場合は、HDD を使用して CDR を保存するように指定します。CGF が起動したら、CDR を CGF にストリーミングします。ストリーミングは並行して行われ、新しく生成された CDR は HDD からストリーミングされた CDR とともに CGF に送信されます。
- **cgf-server-redundancy-support**：GTPP プロファイルごとに CGF サーバの冗長性サポートを有効または無効にします。デフォルトでは、この構成は無効になっています。

### 設定例

次に、GTPP プロファイルの構成例を示します。

```
profile gtpp-profile pf2 gtpp
 dictionary custom24
 mode       streaming
 cgf-server-redundancy-support disable
 instance-id 1
  charging-agent
   address 10.10.10.205
   port    3386
  exit
  server
   max-pdu-size  1460
   timeout       30
   max-retry     3
   max-cdrs      5
   wait-time     30
   echo-interval 60
   deadtime      120
   cgf address 10.10.10.80 port 3386 max 100 priority 1 node-alive disable
   cgf address 10.10.10.90 port 3386 max 100 priority 2 node-alive disable
  exit
 exit
exit
```

# GTPP プロファイルの確認

**show running-config profile gtpp-profile pf2 gtpp** コマンドを使用して、GTPP プロファイルの構成を確認します。

次に、show running-config profile gtpp-profile pf2 gtpp コマンドの出力例を示します。

```
profile gtpp-profile pf2 gtpp
 dictionary custom24
 mode       streaming
 cgf-server-redundancy-support disable
 instance-id 1
  charging-agent
   address 10.10.10.205
   port    3386
  exit
  server
   max-pdu-size  1460
   timeout       30
```

```
    max-retry     3
    max-cdrs      5
    wait-time     30
    echo-interval 60
    deadtime      120
    cgf address 10.10.10.80 port 3386 max 100 priority 1 node-alive disable
    cgf address 10.10.10.90 port 3386 max 100 priority 2 node-alive disable
   exit
  exit
 exit
```

# GTPP エンドポイントの構成

（注）
- GTPP-EP ポッドはこの構成を使用します。
- GTPP-EP ポッドは常にノード構成を無視します。
- **k8s single-node** が **false** に設定されている場合、レプリカとノードの構成に関係なく、アクティブ モードまたはスタンバイ モードで GTPP-EP ポッドの 2 つのレプリカが生成されます。
- **k8s single-node** が **true** に設定されている場合、構成済みのレプリカが影響を受けます。
- **k8s use-volume-claim** が **true** に設定されている場合、エンドポイント GTP Prime を使用してストレージ サイズの制限が設定されます。ストレージ サイズ制限のデフォルト値は 1 GB です。
- システムが稼働している場合、ストレージ サイズは変更できません。

GTPP エンドポイントを構成するには、次のコマンドを使用します。

```
config
 instance instance-id instance_id
   endpoint gtpprime
      storage storage_capacity
      replicas replicas_count
      nodes nodes_count
      interface Gz
        vip-ip   vip_ip vip-port vip-port vip-interface vip-interface vrf vrf
      end
```

注：

- **endpoint gtpprime** ：次のパラメータを指定して、エンドポイントを構成します。
  - **storage** *storage_capacity*：永続ボリュームのストレージ サイズを GB 単位で指定します。1 ～ 100 の範囲の整数である必要があります。

（注） CLI では、システムの実行中にストレージサイズを変更できません。ストレージサイズを変更するには、最初にシステムを停止します。

- **replicas** *replicas_count*：ノードごとのレプリカ数を指定します。整数で指定する必要があります。
- **nodes** *nodes_count*：このプロパティは無視されます。その構成は省略できます。
- **interface Gz** ：VIP IPv4 アドレス、VIP ポート、VIP インターフェイス、仮想ルーティングと転送の詳細などの Gz インターフェイスの詳細を構成します。

（注） システムがアクティブで Gz インターフェイス下にあるときに、新しい値を使用するための **vip** 構成の追加または更新がある場合は、必ず **udp-proxy**を再起動してください。

### 設定例

次に、エンドポイント gtpprime の構成例を示します。

```
instance instance-id 1
 endpoint gtpprime
  replicas 1
  nodes    1
  storage  1
  interface gz
   vip-ip 10.10.10.205 vip-port 7202 vip-interface v303 vrf GTPP-VRF
  exit
 exit
exit
```

# GTPP エンドポイントの確認

**show gtpp-ep endpoints** コマンドを使用して、GTPP エンドポイントを確認します。

次に、show gtpp-ep endpoints コマンドの出力例を示します。

```
result List of gtpp pods with their names and IPs
gtpp-ep-0  192.168.42.116
gtpp-ep-1  192.168.42.126
```

# GTP Prime プライム 構成の確認

**show running-config instance instance-id 1 endpoint gtpprime** コマンドを使用して、GTP Prime の構成を確認します。

次に、show running-config instance instance-id 1 endpoint gtpprime コマンドの出力例を示します。

```
instance instance-id 1
 endpoint gtpprime
  replicas 1
  nodes    1
  storage  1
  interface gz
   vip-ip 10.10.10.205 vip-port 7202 vip-interface v303 vrf GTPP-VRF
  exit
 exit
exit
```

# GTPP サービスのモニターとトラブルシューティング

表 *159* : 機能の履歴

| 機能名 | リリース情報 | 説明 |
|---|---|---|
| GTPPサービスのトラブルシューティング | 2024.02.0 | この機能により、SMF＋PGW-CはGTPCテストエコーコマンドをCGFサーバーに送信しできます。<br>• CGFサーバーの接続性のトラブルシューティングとモニタリングを行います。<br>• ピアのラウンドトリップ時間（RTT）をテストします。<br>**デフォルト設定**：有効：常時オン |

## 機能説明

GTPPテストエコーCLIコマンドを使用すると、CGFサーバの接続のトラブルシューティングとモニタリングができ、システム動作中のピアのラウンドトリップ時間（RTT）が提供されます。

## GTPP テスト エコー コマンドの使用

システムは、次のテストコマンドを使用して、GTPPプロファイルに構成されていない新しいCGFサーバ接続を確認します。

**test gtpp echo instance-id** *id* **ca-address** *ip_address* **[ ca-port** *port* **] [ cgf-address** *ip_address* **] [ cgf-port** *port* **]**

**注**：

- **instance-id** id：システム上に構成されている *GR* インスタンスのインスタンス *ID* を指定します。
- **ca-address** *ip_address*：gtpp プロファイル内で構成された課金エージェントの IPv4 アドレスを指定します。
- **ca-port** *port*：gtpp プロファイル内で構成された課金エージェント ポートを指定します。範囲は 1 ～ 65535 です。デフォルトのポートは 49999 です。
- **cgf-address** *ip_address*：GTPP エコー要求の送信先である特定の CGF サーバの IPv4 アドレスを指定します。
- **cgf-port** *port*: 1 ～ 65535 の範囲で特定の CGF サーバ ポートを指定します。デフォルトのポートは 3386 です。

以下の例では、GTPP Echo コマンド出力の例を表示します。

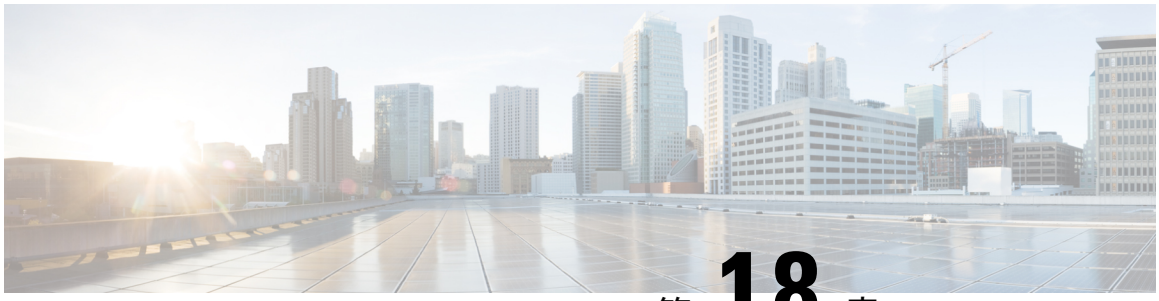
```
Success Case:
[sgw] smf# test gtpp echo instance-id 1 ca-address 10.0.0.1 ca-port 2222 cgf-address
11.0.0.1

Tue Jan  23 12:26:40.164 UTC+00:00
result
{
  "testGtppEchoResponse": {
    "rx": 1,
    "tx": 1,
    "rtt(ms)": 3,
    "recovery": "10 (0x0A)",
    "status": {
      "success": true
    }
  }
}

Timeout Case:

[sgw] smf# test gtpp echo instance-id 1 ca-address 10.0.0.1 ca-port 2222 cgf-address
11.0.0.2

Tue Jan  24 07:43:22.164 UTC+00:00
result
{
  "testGtppEchoResponse": {
    "tx": 4,
    "recovery": "NA",
    "status": {
      "errorMsg": "No Response Received, Timeout"
    }
  }
}
```



第 18 章

# ハンドオーバー手順


- 機能の概要と変更履歴 （503 ページ）
- 機能説明 （504 ページ）
- 4G から 5G へのデータ セッションのハンドオーバー （504 ページ）
- アクセスとモビリティの手順のための CHF と PCF の統合 （521 ページ）
- gNodeB 間ハンドオーバー （533 ページ）
- Wi-Fi ハンドオーバー （549 ページ）


## 機能の概要と変更履歴

### 要約データ

表 *160* : 要約データ

| | |
|---|---|
| 該当製品または機能エリア | SMF |
| 該当プラットフォーム | SMI |
| 機能のデフォルト設定 | N/A |
| このリリースでの関連する変更点 | N/A |
| 関連資料 | 該当なし |

### 更新履歴

表 *161* : マニュアルの変更履歴

| 改訂の詳細 | リリース |
|---|---|
| 5G および Wi-Fi 用の代替 RAT トンネルの作成のサポートが追加されました。 | 2023.03.0 |

| 改訂の詳細 | リリース |
|---|---|
| FB コール継続原因コードの拡張 | 2021.02.2 |
| 次に対するサポートが追加されました：<br>• 引き継ぎ通知を伴う通話の構成。<br>• GTPC メッセージ内の UE ローカル IP アドレスおよび UE UDP ポート IE。<br>• ユーザーロケーション情報（ULI）レポート | 2021.02.0 |
| Wi-Fi ハンドオーバーの TFT 処理がサポートされています。 | 2021.01.0 |
| EPS フォールバック機能を使用した Wi-Fi から 5GS へのハンドオーバーは、このリリースで完全に認定されています。 | 2020.02.2 |
| EPS フォールバック機能を使用した Wi-Fi から 5GS へのハンドオーバーは、このリリースでは完全には認定されていません。詳細については、シスコのアカウント担当者にお問い合わせください。 | 2020.02.1 |
| 最初の導入。 | 2020.02.0 より前 |

# 機能説明

この章では、3GPP 仕様に準拠する SMF によって実行されるさまざまなハンドオーバー手順について説明します。

# 4G から 5G へのデータ セッションのハンドオーバー

## 機能説明

**Important** この章で使用されている PGW-C という用語は、SMF でサポートされている EPS インターワーキング機能を意味しており、LTE ネットワークで使用されるスタンドアロン P-GW として想定してはなりません。

UE の場合、SMF は 5G と 4G NAS の両方をサポートしており、E-UTRAN と 5G コア ネットワークに接続できます。SMF には EPS インターワーキング サポートが含まれており、PGW-C + SMF として機能します。SMF は、S5/S8 インターフェイスを使用して 4G セッション作成要

求を受信します。4G セッションの作成に使用される Gx、Gy、または Gz インターフェイスは、NPCF や NCHF など、対応する 5G コア SBI インターフェイスに置き換えられます。

E-UTRAN、MME、および S-GW を介した PGW-C + SMF での PDU セッションの作成後、SMF は 4G から 5G へのデータ セッションのハンドオーバーを実行します。

### 5G 向けの代替 RAT トンネルの作成

SMF は、5G PDU 確立シナリオの 5G セッション中に代替 RAT トンネルを作成します。このトンネルは、サブスクライバが移行中に別の RAT に移動するときに再利用されます。

**Note** 代替 RAT トンネルの作成は、PLMN 間ハンドオーバー サポートの前提条件です。

# 機能の仕組み

EPS と相互運用するため、5GC と EPS NAS の両方をサポートする UE は、以下のいずれかのモードで動作します：

- シングル登録モード：このモードでは、UE のアクティブな MM 状態は 1 つだけです。5GC の RM 状態または EPS の EMM 状態のいずれかになります。さらに、5GC または EPS に接続すると、この状態は 5GC NAS モードまたは EPS NAS モードのいずれかになります。
- デュアル登録モード：UE は、このモードでは、個別の RRC 接続を使用して 5GC と EPS の独立した登録を処理します。UE は 5GC のみ、EPS のみ、または 5GC と EPS の両方に登録できます。

### 4G、5G、および Wi-Fi 向けの代替 RAT トンネルの作成

DNN プロファイルで PLMN 間ハンドオーバー CLI が有効になっている場合、SMF は代替 RAT トンネルを作成します。さらに、SMF は、特定の条件を満たすことに基づいてこのトンネルを作成します。次の表に、このトンネルの作成および非作成の条件を示します。

***Table 162:*** 代替 ***RAT*** トンネルの作成と作成以外の条件

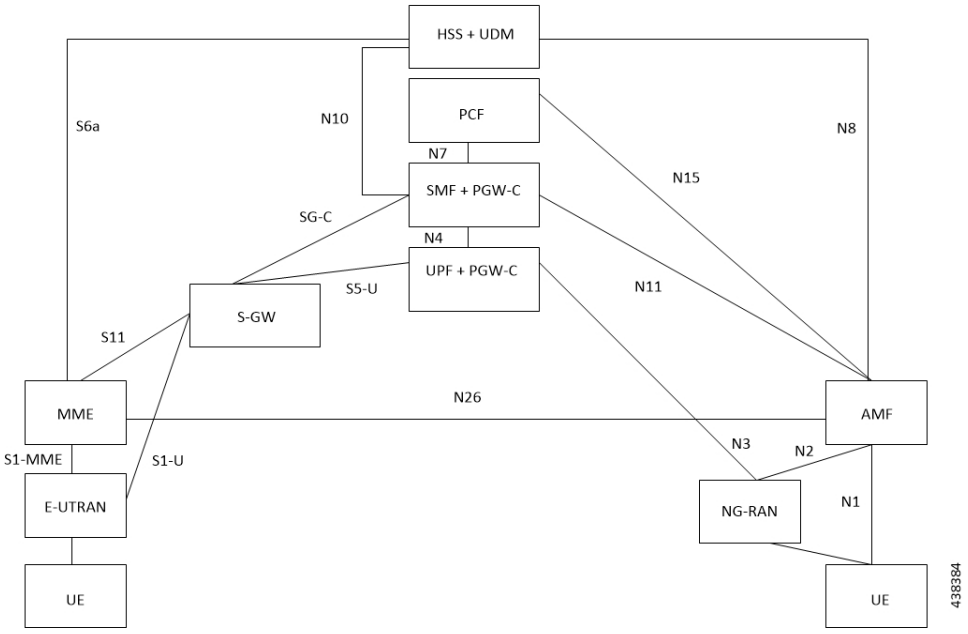
| セッション要求の作成 | **N11 SMContext** の作成 | サブスクリプション データ | 代替 **RAT** トンネルの作成 |
|---|---|---|---|
| | epsInterworkingInd': 'WITH_N26' | dnnInfo->IwkEpsInd=true | ○ |
| | epsInterworkingInd': 'WITH_N26' | dnnInfo->IwkEpsInd=false | 非対応 |
| | epsInterworkingInd': 'WITHOUT_N26' | dnnInfo->IwkEpsInd=false | 非対応 |

| セッション要求の作成 | N11 SMContext の作成 | サブスクリプションデータ | 代替 RAT トンネルの作成 |
|---|---|---|---|
| | epsInterworkingInd': 'WITHOUT_N26' | dnnInfo->IwkEpsInd=true | 非対応 |
| IWK_5GS indication flag=true, pduSessionId received from UE | ○ | dnnInfo->IwkEpsInd=true | ○ |
| IWK_5GS indication flag=true, pduSessionId received from UE | 非対応 | dnnInfo->IwkEpsInd=false | 非対応 |
| IWK_5GS indication flag=false, pduSessionId not received from UE | ○ | dnnInfo->IwkEpsInd=false | 非対応 |
| IWK_5GS indication flag=false, pduSessionId not received from UE | 非対応 | dnnInfo->IwkEpsInd=true | 非対応 |

# アーキテクチャ

このセクションでは、EPS-5G コア インターワーキングのネットワーク アーキテクチャについて説明します。

***Figure 90: EPS-5G* コア インターワーキングのネットワーク アーキテクチャ**



# コール フロー

このセクションでは、次のコール フローについて説明します。

- N26 インターフェイスを使用した EPS から 5G へのハンドオーバー：準備コール フロー
- N26 インターフェイスを使用した EPS から 5G へのハンドオーバー：実行コール フロー
- N26 インターフェイスを使用した EPS から 5GS への UE アイドル モード モビリティ

## N26 インターフェイスを使用した EPS から 5G へのハンドオーバー：準備コール フロー

このセクションでは、N26 インターフェイスを使用した EPS から 5G へのハンドオーバーの準備のコール フローについて説明します。

***Figure 91: N26** インターフェイスを使用した **EPS** から **5G** へのハンドオーバーの準備コールフロー*

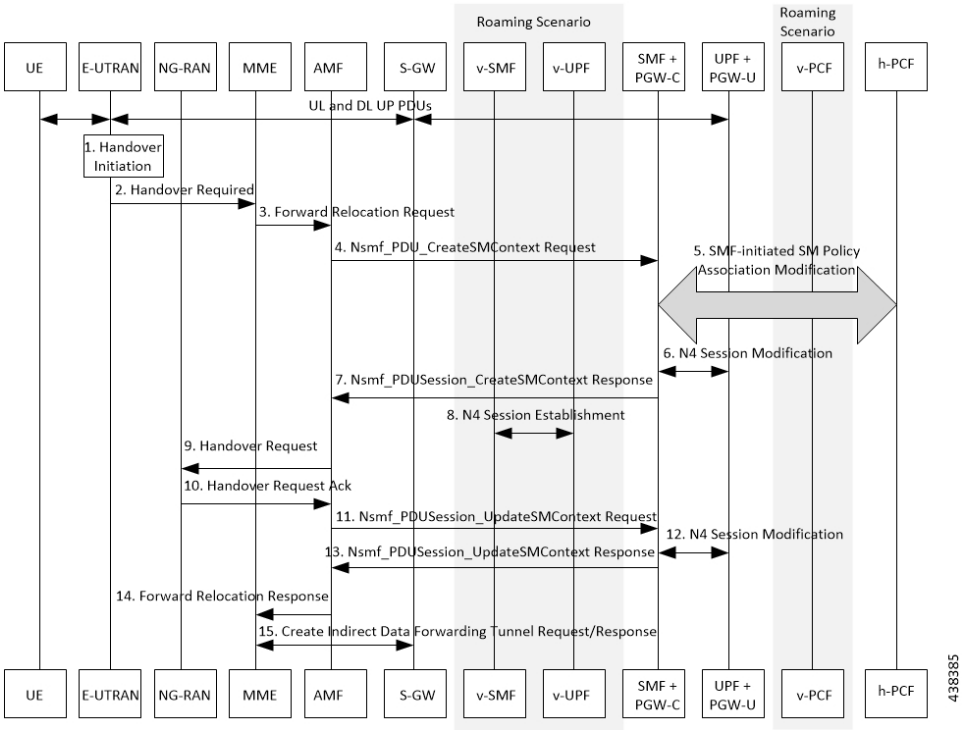



***Table 163: N26** インターフェイスを使用した **EPS** から **5G** へのハンドオーバーの準備コールフロ ーの説明*

| ステップ | 説明 |
|---|---|
| 1 | コール ハンドオーバーの開始は、UE と E-UTRAN から相互に向けて開始され、E-UTRAN から S-GW へと進みます。次に、ローミング コールでは、コール ハンドオーバーの開始は S-GW から UPF + PGW-CU に行われます。 |
| 2 | E-UTRAN が MME にハンドオーバー コール要求を送信します。 |

| ステップ | 説明 |
|---|---|
| 3 | MME は再配置要求を AMF に転送します。 |
| 4 | AMF は、SMF で NsmfPDUSessionCreateSMContext サービス操作を呼び出します。PGW-C+SMFアドレスは、このサービス操作を識別します。サービス操作は、[UE EPS PDN接続（UE EPS PDN Connection）]、[AMF ID]、または [ダイレクト転送フラグ（Direct Forwarding Flag）] です。AMFは、稼働パスの切り替えを回避するための引き継ぎの準備を示します。SMF は EPS ベアラー コンテキストに基づいて、対応する PDU セッションを検索します。AMF には、間接データ転送の適用可能性を SMF に通知するための Direct Forwarding Flag が含まれています。 |
| 5 | ダイナミック PCC を導入した場合、SMF + PGW-C は SMF によって開始される SM ポリシーの変更を PCF に対して開始します。<br>**Important**<br>Cisco SMF は この手順をサポートしていません |
| 6 | PGW-C+SMF は PGW-U+UPF に N4 セッション変更を送信して、PDU セッションの CN トンネルを確立します。PGW-U + UPF は、NG-RAN からアップリンク パケットを受信します。この手順では、既存の 4G ベアラーからマッピングされた QFI とともに、5G セッションのアップリンク PDR および FAR を作成する必要があります。 |
| 7 | PGW-C+SMFは、NsmfPDUSessionCreateSMContext 応答を AMF に送信します。この応答には、PDU セッション ID、S-NSSAI、および N2 SM の情報が含まれます。<br>N2 SM 情報には、PDU セッション ID、S-NSSAI、QFI、QoS プロファイル、EPS ベアラー セットアップ リスト、EBI と QFI の間のマッピング、CN トンネル情報、および原因コードの詳細が含まれます。<br>SMF には、EBI と QFI 間のマッピングが N2 SM 情報コンテナとして含まれています。EPS から 5GS へのセッション継続性が PDU セッションでサポートされていないと PGW-C-C+SMF が判断した場合、PGW-C-C+SMF は対応する PDU セッションのセッションマネージャ情報を提供しません。ただし、PGW-C-C+SMF には、N2 SM 情報に PDU セッション転送を拒否する原因コードの詳細が含まれています。 |
| 8 | V-SMF と V-UPF は、相互に N4 セッションを確立します。 |
| 9 | AMF は、NG-RAN にハンドオーバー要求を送信します。 |
| 10 | NG-RANは、受信したハンドオーバー要求の確認応答をAMFに送信します。 |
| 11 | AMF は、N3 トンネル情報を更新するために、NsmfPDUSessionUpdateSMContext 要求、T-RAN SM N3 転送情報リスト メッセージを SMF に送信します。<br>NsmfPDUSessionUpdateSMContext 要求には、PDU セッション ID、S-NSSAI、N2 SM の情報が含まれています。トンネル情報は、NG-RAN から受信したハンドオフ要求承認の NGAP IE DL 転送 UP TNL 情報に存在します。 |

| ステップ | 説明 |
|---|---|
| 12 | SMF + PGW-U に対する N4 セッション変更を実行し、eNodeB から NG-RAN に DL データを転送するための間接トンネルを作成します。この手順では、リダイレクトされた DL データの UL PDR を作成し、それらに FAR を関連付けて FAR を NG-RAN に転送することも含まれます。これらの PDR と FAR のマッピングは、QFI と対応するベアラー ID に基づいています。 |
| 13 | PGW-C+SMF は、NsmfPDUSessionUpdateSMContext 応答を AMF に送信します。この応答には、PDU セッション ID、EPS ベアラー セットアップ リスト、およびデータ転送用の CN トンネル情報が含まれます。この時点で、DL データ転送用の間接トンネルが確立されます。 |
| 14 | AMF が再配置応答を MME に送信します。 |
| 15 | MME は、間接データ転送トンネルの作成要求を S-GW に送信します。S-GW は、間接データ転送トンネルの応答を MME に送信します。 |

## N26 インターフェイスを使用した EPS から 5G へのハンドオーバー：実行コールフロー

このセクションでは、N26 インターフェイスを使用した EPS から 5G へのハンドオーバーの実行のコール フローについて説明します。

***Figure 92: N26** インターフェイスを使用した **EPS** から **5G** へのハンドオーバーの実行コール フロー*

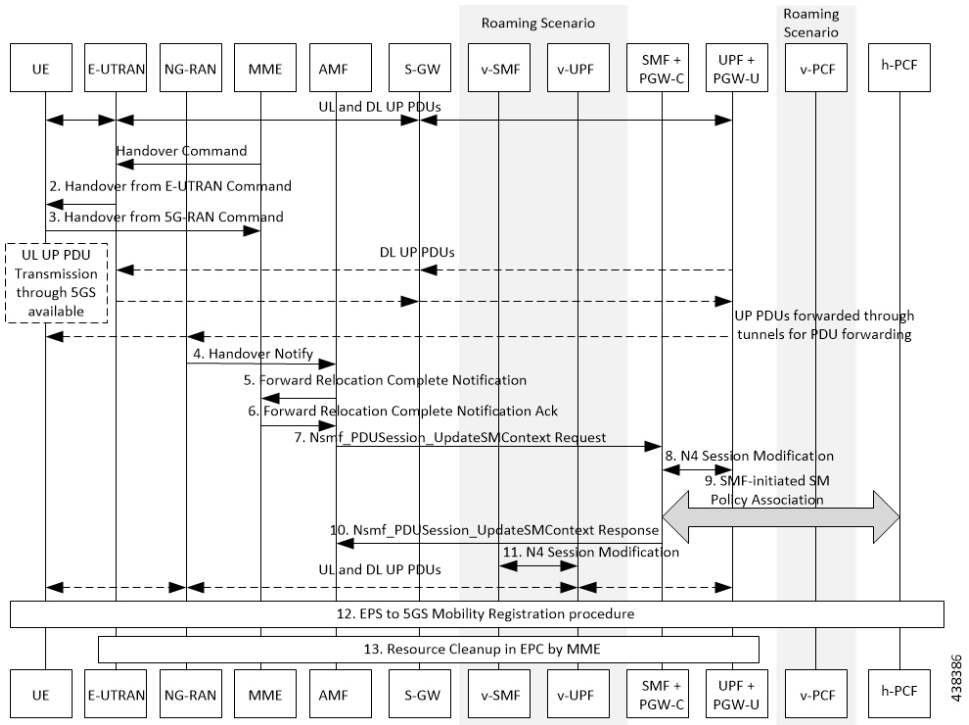


*Table 164: N26* インターフェイスを使用した *EPS* から *5G* へのハンドオーバーの実行コール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | コール ハンドオーバーの開始は、UE と E-UTRAN から相互に向けて開始され、E-UTRAN から S-GW へと進みます。次に、ローミング コールでは、コール ハンドオーバーの開始は S-GW から UPF + PGW-CU に行われます。<br>MME が E-UTRAN に引き継ぎコマンドを送信します。 |
| 2 | E-UTRAN は UE に引き継ぎコマンドを送信します。 |
| 3 | UE は、5G-RAN への受信についての確認メッセージを NG-RAN に送信します。 |
| 4 | NG-RAN が AMF にハンドオーバー通告メッセージを送信します。 |
| 5 | AMF が再配置完了通告を MME に送信します。 |
| 6 | MME は、受信した転送再配置完了通知の確認応答を送信します。 |
| 7 | AMF は、NsmfPDUSessionUpdateSMContext 要求を SMF +PGW-C に送信します。この要求には、PDU セッション ID の詳細に関するハンドオーバー完了の表示が含まれています。間接転送の場合、SMF + PGW-C のタイマーが、UPF 内のリソースを解放するタイミングの確認を開始します。 |
| 8 | SMF は UPF + PGW-U で N4 変更要求を実行し、5G セッションの DL PDR に関連付けられている FAR の DL トンネル情報を更新します。DL データ パスがアクティブ化されます。この時点で、間接トンネルも存在します。 |
| 9 | SMF は、PDU セッション ID 付きのNsmfPDUSessionUpdateSMContext 応答を AMF に送信します。SMF は Handover Complete の受信を確認します。 |
| 10 | ステップ 7 で開始したタイマーの期限が切れると、SMF は N4 変更要求を UPF に送信します。この要求は、間接データ トンネルに関連付けられている PDR と FAR を削除することです。 |
| 11 | UE が EPS から 5GS モビリティへの登録手順を開始し、それを H-PCF に送信します。 |
| 12 | E-UTRAN は、MME によって EPC でリソースのクリーンアップを実行します。 |

## N26 インターフェイスを使用した EPS から 5GS への UE アイドル モード モビリティ

SMF と PGW-C は、EPS から 5GS へのアイドル モード モビリティの手順をサポートします。EPS から 5GS へのアイドルモードモビリティの場合、UE は AMF を使用してモビリティ登録の更新手順を実行します。AMF と SMF は EPS から MM および SM コンテキストを取得し、他のコア NF と対話することによって UE コンテキストを EPS から 5GS に移動します。

この機能により、EPS および 5GS のコア ネットワーク要素は、EPS から 5GS へのアイドル モード モビリティの手順中に、次のユース ケースをサポートできます。

- N26 インターフェイスを使用した EPS から 5GS への UE アイドル モード モビリティ：非アクティブ状態の PDU セッション

- N26 インターフェイスを使用した EPS から 5GS への UE アイドル モード モビリティ：ユーザープレーン接続再アクティブ化要求

## *PDU* が非アクティブ状態になっています

次のコール フローは、PDU セッションが非アクティブ状態にある際に、N26 インターフェースを使用して EPS から 5GS へ UE アイドル モード移動に関する情報を取得するプロセスを説明しています。

**図 *93 : PDU* セッションが非アクティブ状態になっています**

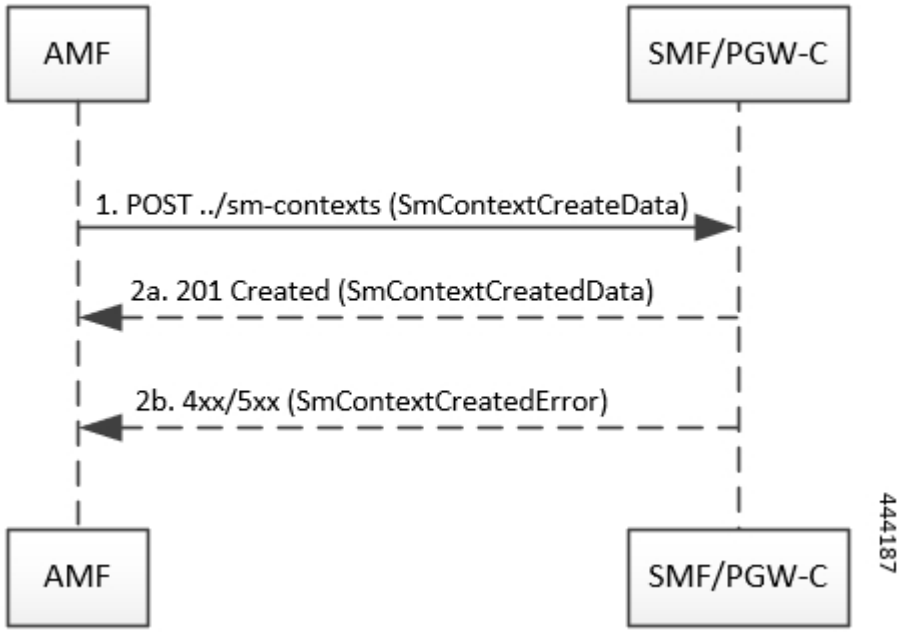



**表 *165 : PDU* セッションが非アクティブ状態になっています**

| ステップ | 説明 |
|---|---|
| 1 | AMF は、各 UE EPS PDN 接続の SMF/PGW-C に対して、次の情報と POST 要求を送信します。<br>• MME から受信した、作成される個々の SM コンテキストを表す、EPS ベアラー コンテキストを含む UE EPS PDN 接続。<br>• EPS ベアラー コンテキスト ステータス属性。対応する情報が UE からの登録要求で受信された場合、UE 内のすべての EPS ベアラー コンテキストのステータスを示します。 |

| ステップ | 説明 |
|---|---|
| 2 | このような要求を受け取った場合、次のいずれかに該当する場合とします。<br>• 対応する PDU セッションが EPS ベアラー コンテキストに基づいて検出されます。<br>• 対応する PDU セッションのデフォルトの EPS ベアラー コンテキストを受信した場合、EPS ベアラー 接続ステータス属性で UE によって非アクティブとして報告されません。受信した場合、<br>• 5GS への PDN 接続移行を続行できます。 |
| 2a | SMF は次の情報を含む 201 作成済み応答を返します。<br>• EPS PDN 接続のデフォルトの EPS ベアラー ID に対応する PDU セッション ID。<br>• PDU セッションに割り当てられた EBI を含む割り当て済み EBI リスト。<br>POST 応答に存在するロケーション ヘッダーには、作成された SM コンテキスト リソースの URI が含まれます。<br>AMF は、PDU セッション ID と SMF ID の関連付け、および PDU セッション ID に関連付けられた割り当て済みの EBI を保存します。<br>要求で EPS ベアラー コンテキスト ステータス属性を受信すると、SMF は、対応する PDU セッションの一部の EPS ベアラーが UE によって削除されたものの、EPS に通知されていないかどうかを確認します。サポートされている場合、SMF はこれらの EPS ベアラー、対応する QoS ルール、および QoS フロー レベルのパラメータをローカルに解放します。 |
| 2b | 次の場合、SMF は 4xx/5xx 障害応答を返します。<br>• SMF は、PDU セッションで EPS から 5GS へのシームレスなセッション継続がサポートされていないことを判断します。SMF は、問題の詳細構造内の原因属性を `NO_EPS_5GS_CONTINUITY`に設定します。<br>• PDU セッションのデフォルトの EPS ベアラー コンテキストは、EPS ベアラー コンテキストのステータス属性の UE によって非アクティブとして報告されます。SMF は、問題の詳細構造内の原因属性を `DEFAULT_EPS_BEARER_INACTIVE`に設定します。 |

ユーザー プレーン接続の再アクティブ化要求

次のコール フローは、N26 インターフェイスを使用した UP（ユーザー プレーン）接続の再アクティブ化を使用した EPS から 5GS への UE アイドル モード モビリティに関する情報をキャプチャしたものです。

図 *94 :* ユーザー プレーン接続の再アクティブ化要求

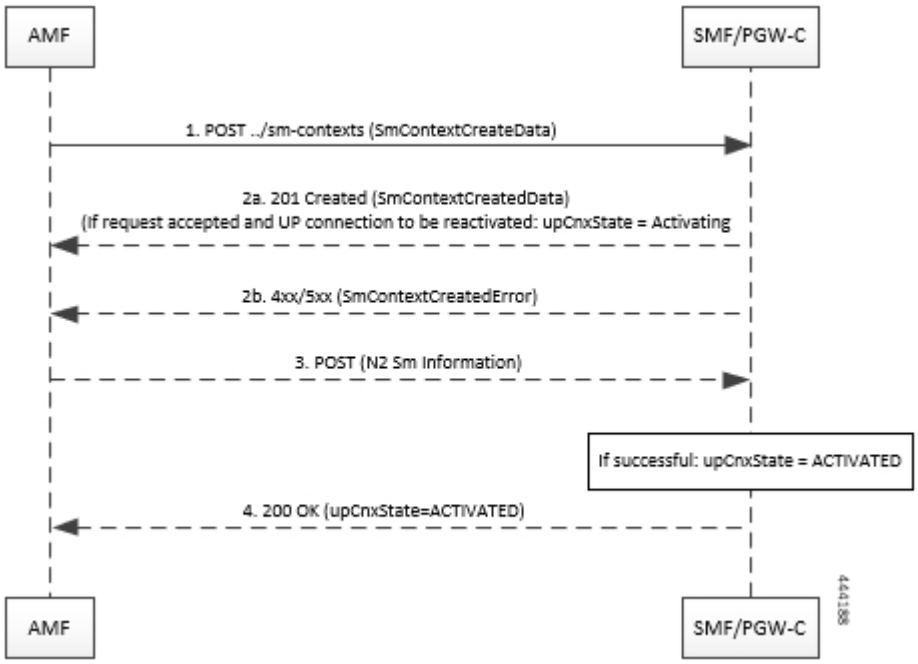



表 *166 :* ユーザー プレーン接続の再アクティブ化要求

| ステップ | 説明 |
|---|---|
| 1 | AMF は、各 UE EPS PDN 接続の SMF/PGW-C に対して、次の情報と POST 要求を送信します。<br>• MME から受信した、作成される個々の SM コンテキストを表す、EPS ベアラー コンテキストを含む UE EPS PDN 接続。<br>• PDUセッションのアクティブ化リスト属性。これには、再度アクティブ化するすべての PDU セッションの PDU セッション ID が含まれます。<br>• EPS ベアラー コンテキスト ステータス属性。対応する情報が UE からの登録要求で受信された場合、UE 内のすべての EPS ベアラー コンテキストのステータスを示します。 |

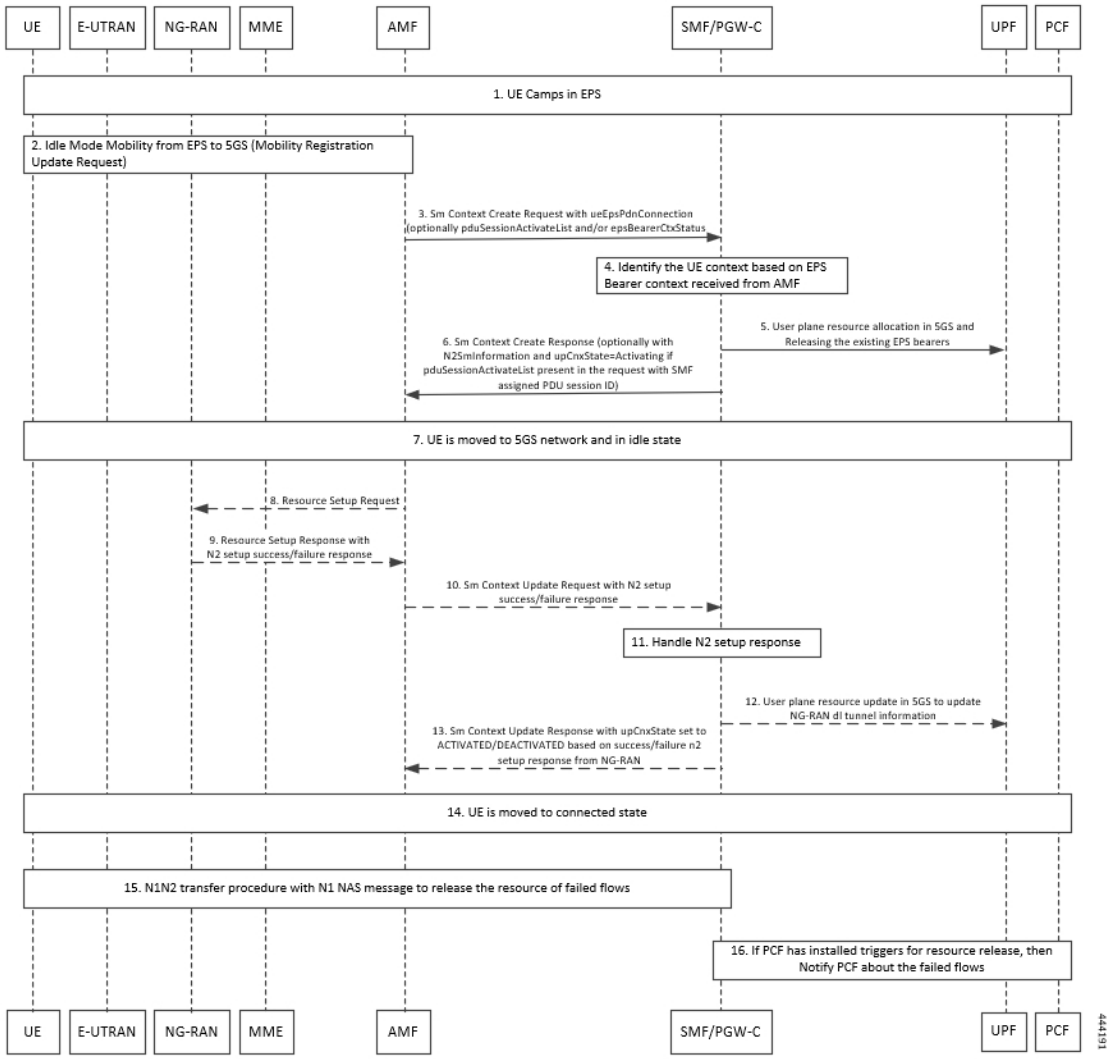
| ステップ | 説明 |
|---|---|
| 2 | このような要求を受け取った場合、次のいずれかに該当する場合とします。<br>• 対応する PDU セッションが EPS ベアラー コンテキストに基づいて検出されます。<br>• 対応する PDU セッションのデフォルトの EPS ベアラー コンテキストを受信した場合、EPS ベアラー コンテキスト属性で UE によって非アクティブとして報告されません。受信した場合、<br>• 5GS への PDN 接続移行を続行できます。 |
| 2a | SMF は次の情報を含む 201 作成済み応答を返します。<br>• EPS PDN 接続のデフォルトの EPS ベアラー ID に対応する PDU セッション ID。<br>• PDU セッションに割り当てられた EBI を含む割り当て済み EBI リスト。<br><br>EPS ベアラー コンテキストに基づいて SMF によって取得された PDU セッションの再アクティブ化が要求された場合、つまり PDU セッション ID が PDU セッションアクティブ化リストに存在していた場合、<br>• ユーザー プレーン接続状態属性が ACTIVATING に設定されます。<br>• この PDU セッションのユーザー プレーン データのアップリンク終端点のトランスポート層アドレスおよびトンネル終端点（すなわち、アップリンク トラフィックの UPF の GTP-U F-TEID）を含む、PDU セッションにリソースを割り当てるよう5G-ANに要求するための N2 SM情報（PDU セッション リソース設定要求転送）。<br><br>POST 応答に存在するロケーション ヘッダーには、作成された SM コンテキスト リソースの URI が含まれます。<br><br>AMF は、PDU セッション ID と SMF ID の関連付け、および PDU セッション ID に関連付けられた割り当て済みの EBI を保存します。<br><br>要求で EPS ベアラー コンテキスト ステータス属性を受信すると、SMF は、対応する PDU セッションの一部の EPS ベアラーが UE によって削除されたものの、EPS に通知されていないかどうかを確認します。サポートされている場合、SMF はこれらの EPS ベアラー、対応する QoS ルール、および QoS フロー レベルのパラメータをローカルに解放します。 |

| ステップ | 説明 |
|---|---|
| 2b | 次の場合、SMF は 4xx/5xx 障害応答を返します。<br>• SMF は、PDU セッションで EPS から 5GS へのシームレスなセッション継続がサポートされていないことを判断します。SMF は、問題の詳細構造内の原因属性を NO_EPS_5GS_CONTINUITY に設定します。<br>• PDU セッションのデフォルトの EPS ベアラー コンテキストは、EPS ベアラー コンテキストのステータス属性の UE によって非アクティブとして報告されます。SMF は、問題の詳細構造内の原因属性を DEFAULT_EPS_BEARER_INACTIVE に設定します。 |
| 3 | SMF が 200 OK 応答を返した場合、AMF は、次の情報を含む POST 要求を送信することによって、SMF 内の SM コンテキストを更新します。<br>• 5G-AN（PDU セッション リソース セットアップ応答転送 IE）から受信した N2 SM 情報。これには、トランスポート層アドレス、1 つまたは 2 つのダウンリンク ターミネーション ポイントのトンネル エンドポイントが含まれます。また、5G-AN が PDU セッションのリソースの確立に成功した場合、この PDU セッションの QoS フローの関連リスト（つまり、ダウンリンク トラフィック用の 5G-AN の GTP-U F-TEID）も含まれます。または<br>• PDUセッションのリソース確立に失敗した場合、失敗の原因を含む、5G-AN（PDU セッション リソース セットアップ失敗転送 IE）から受信した N2 SM 情報。<br>この要求を受信すると、SMF は以下を行います。<br>• 5G-AN が PDU セッション用のリソースの確立に成功した場合、5G-AN の F-TEID で UPF を更新し、ユーザープレーン接続状態属性を ACTIVATED に設定します。または<br>• ユーザープレーン接続のアクティブ化が失敗したことを考慮し、ユーザープレーン接続状態属性を DEACTIVATED に設定します。 |
| 4 | SMF は、ユーザー プレーン接続の最終状態を表すユーザー プレーン接続状態属性を含む 200 OK 応答を返します。 |

メッセージ フロー

次のメッセージ フローでは、5GS ネットワーク要素とサブスクライバにおけるアイドル モード モビリティ手順のさまざまなシナリオについて説明します。

図 *95 : 5GS NE* とサブスクライバ間のメッセージ フロー




## 代替 RAT トンネル作成コール フローによる非ローミング 5GS から EPS へのハンドオーバー

このセクションでは、代替 RAT トンネルの作成による非ローミング 5GS から EPS へのハンドオーバーのコール フローについて説明します。

図 *96 :* 代替 *RAT* トンネル作成コール フローによる非ローミング *5GS* から *EPS* へのハンドオーバー

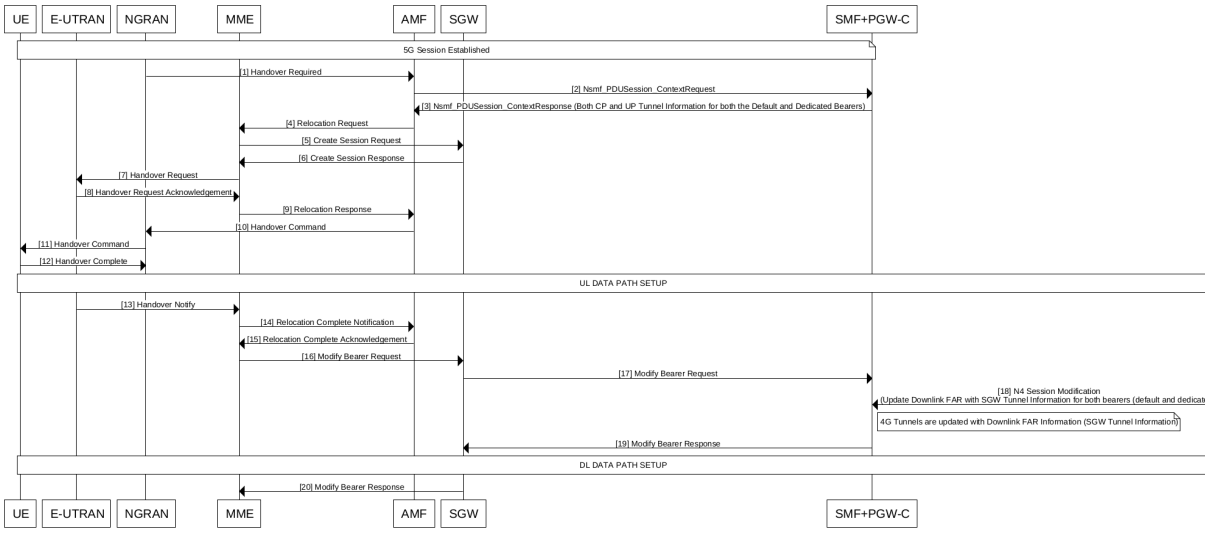



表 *167 :* 代替 *RAT* トンネル作成による非ローミング *5GS* から *EPS* へのハンドオーバー コール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | 5G セッションが UE、E-UTRAN、NGRAN、MME、AMF、S-GW、および SMF + PGW-C 間で確立されます。<br>NG-RANがAMF へのハンドオーバーを開始します。 |
| 2 | AMF は、Nsmf PDU セッション コンテキスト要求を SMF + PGW-C に送信します。 |
| 3 | SMF + PGW-C は、Nsmf PDU セッション CreateSMContext 応答を AMF に送信します。この応答には、デフォルトと専用ベアラーの両方の CP トンネルと UP トンネルに関する詳細が含まれています。 |
| 4 | AMF が再配置要求を MME に送信します。 |
| 5 | MME がセッション作成要求を S-GW に送信します。 |
| 6 | S-GW はセッション応答の作成を MME に送信します。 |
| 7 | MME が E-UTRAN にハンドオーバー要求を送信します。 |
| 8 | E-UTRAN は、ハンドオーバー要求の確認応答を MME に送信します。 |
| 9 | MME が再配置応答を AMF に送信します。 |
| 10 | AMFはNG-RAN にハンドオーバー コマンドを送信します。 |
| 11 | NG-RANはUE にハンドオーバー コマンドを送信します。 |

| ステップ | 説明 |
|---|---|
| 12 | UE はハンドオーバー完了メッセージを NG-RAN に送信します。 |
| 13 | UL データパスは、UE、E-UTRAN、NG-RAN、MME、AMF、S-GW、SMF＋PGW-C、および UPF 間に設定されます。<br>E-UTRAN が MME にハンドオーバー通知メッセージを送信します。 |
| 14 | MME が再配置の完了に関する通知を AMF に送信します。 |
| 15 | AMF は、再配置完了の確認応答メッセージを MME に送信します。 |
| 16 | MME が、ベアラー リクエストの変更を S-GW に送信します。 |
| 17 | S-GW は、SMF+PGW-C にベアラー要求の変更を送信します。 |
| 18 | SMF + PGW-C は、N4 セッション変更要求を UPF に送信します。この要求には、デフォルトと専用ベアラーの両方の S-GW トンネルを使用して DL FAR を更新するための詳細が含まれています。 |
| 19 | 4G トンネルは DL FAR 情報（S-GW トンネル情報）で更新されます。<br>SMF + PGW-C は、ベアラー応答の変更を S-GW に送信します。 |
| 20 | DL データパスは、UE、E-UTRAN、NG-RAN、MME、AMF、S-GW、SMF＋PGW-C、および UPF 間に設定されます。<br>S-GW が、ベアラー応答の変更を MME に送信します。 |

## 代替 RAT トンネル作成コール フローによる非ローミング EPS から 5GS へのハンドオーバー

このセクションでは、代替 RAT トンネルの作成による非ローミング EPS から 5GS へのハンドオーバーのコール フローについて説明します。

図 *97* : 代替 *RAT* トンネル作成コール フローによる非ローミング *EPS* から *5GS* へのハンドオーバー

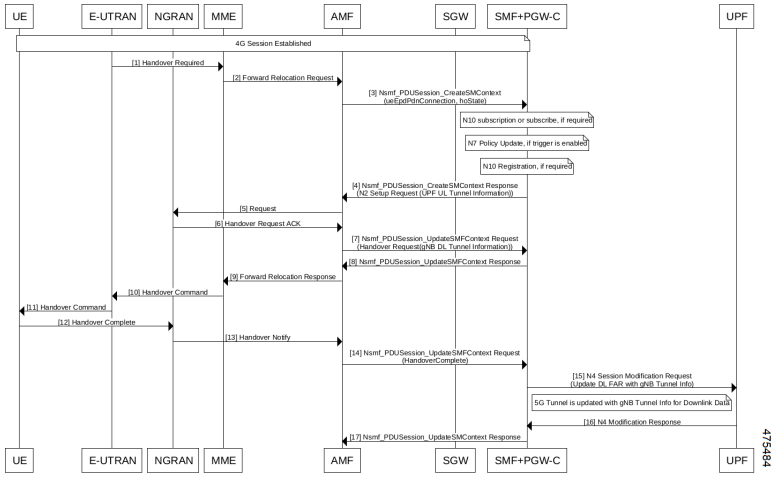



表 *168* : 代替 *RAT* トンネル作成コール フローの説明による非ローミング *EPS* から *5GS* へのハンドオーバー

| ステップ | 説明 |
|---|---|
| 1 | 5G セッションが UE、E-UTRAN、NG-RAN、MME、AMF、S-GW、および SMF + PGW-C 間で確立されます。<br>E-UTRAN が MME へのハンドオーバーを開始します。 |
| 2 | MME は転送再配置要求を AMF に送信します。 |
| 3 | AMF は、Nsmf PDU Session CreateSMContext 要求を SMF+PGW-C に送信します。この要求には、UE PDN 接続と引き継ぎ状態に関する詳細が含まれています。 |
| 4 | SMF + PGW-C は、次の手順をチェックします：<br>• N10 サブスクリプションまたは必要に応じてサブスクライブすることができます。<br>• トリガーが有効な場合、N7 ポリシー更新。<br>• N10 登録が必要です。<br>SMF + PGW-C は、Nsmf PDUsession CreateSMContext Response を AMF に送信します。この応答には、UPF UL トンネル情報を含む N2 設定要求が含まれています。 |
| 5 | AMF は、NG-RAN へハンドオーバー リクエストを送信します。 |
| 6 | NG-RAN はハンドオーバー要求の確認応答を AMF に送信します。 |
| 7 | AMF は、Nsmf PDU セッション更新 SMF コンテキスト要求を SMF+PGW-C に送信します。この要求には、gNB DL トンネル情報を伴うハンドオーバー要求が含まれます。 |

| ステップ | 説明 |
|---|---|
| 8 | SMF + PGW-C は、Nsmf PDU セッション更新 SMF コンテキスト応答を AMF に送信します。 |
| 9 | AMF は、転送再配置応答を MME に送信します。 |
| 10 | MME が E-UTRAN に引き継ぎコマンドを送信します。 |
| 11 | E-UTRAN は UE に引き継ぎコマンドを送信します。 |
| 12 | UE は、ハンドオーバー完了のメッセージを NG-RAN に送信します。 |
| 13 | NG-RAN は、AMF にハンドオーバー通知メッセージを送信します。 |
| 14 | AMF は、ハンドオーバーの完了後、Nsmf PDU セッション更新 SMF コンテキスト要求を SMF + PGW-C に送信します。 |
| 15 | SMF + PGW-C は、N4 セッション変更要求を UPF に送信します。この要求は、gNB トンネル情報を使用して DL FAR を更新するためのものです。 |
| 16 | 5G トンネルは、DL データの gNB トンネル情報で更新されます。<br>UPF が SMF+PGW-C に N4 変更応答を送信します。 |
| 17 | SMF + PGW-C は、Nsmf PDU セッション更新 SM コンテキスト応答を AMF に送信します。 |

## 標準準拠

4G から 5G へのデータ セッション ハンドオーバー機能向けの SMF サポートは、3GPP TS 23.502 V15.2.0（2018-09）標準に準拠しています。

## 制限事項

4G から 5G へのデータ セッション引き継ぎ機能には、次の制限があります：

- SMF は、単一の UPF での N26 4G から 5G へのハンドオフをサポートしています。これは、UPF の選択と UPF の変更がサポートされていないことを意味します。

# アクセスとモビリティの手順のための CHF と PCF の統合

## 機能説明

**Important** この章で使用されている PGW-C という用語は、SMF でサポートされている EPS インターワーキング機能を意味しており、LTE ネットワークで使用されるスタンドアロン P-GW として想定してはなりません。

アクセスとモビリティの手順の場合、SMF は次の手順のために課金機能（CHF）とポリシー制御機能（PCF）を統合します。

- AMF 内および AMF 間の N2 ベースのハンドオーバー SMF は、データ転送トンネル（DFT）および間接データ転送トンネル（IDFT）の場合に、UE が 1 つの NG-RAN から別の NG-RAN に移動するときにこの機能をサポートします。
- N26 4G から 5G へのハンドオーバー：SMF は、N26 インターフェイスを使用した EPS から 5GS への手順をサポートします。SMF は、5GS の認定 EPS ベアラー識別（EBI）リストを使用してアップリンク（UL）のパケット検出ルール（PDR）またはダウンリンク（DL）PDR を確立し、EBI をそれぞれのフローに複製します。SMF は IDFT を作成して、UPF を介した SGW-U から NR へのダウンリンク転送トラフィックをサポートします。
- N26 5G から 4G へのハンドオーバー：SMF は、N26 インターフェイスでの 5GS から EPS への手順をサポートします。PGW-C は、5GS の認定フローを使用して SGW-U に対して UL PDR または DL PDR を確立し、それぞれのフローに EBI を複製します。PGW-C は IDFT トンネルも作成して、UPF を介した NR から SGW-U へのダウンリンク転送トラフィックをサポートします。セッションレベルまたは課金設定グループレベルの課金トリガは、PDU セッションの確立中、または EPS 手順での SMF によって開始された課金更新要求または CHF によって開始された課金更新通知応答への応答として受信されます。
- Xn ハンドオーバー：SMF は、UPF 再割り当ての有無にかかわらず、Xn ベースの NG-RAN 間ハンドオーバーをサポートします。SMF は、AMF 内モビリティのみの Xn ハンドオーバーをサポートします。SMF は、パス スイッチ要求 N2 ベースのメッセージとアクセス側パラメータが含まれている、受信した SM コンテキスト更新要求を処理します。これらのパラメータは、PDU セッション確立中に受信される CHF トリガと PCF トリガを識別します。
- サービス要求手順：SMF は、UE とネットワーク開始手順の両方からのサービス要求をサポートします。CM アイドル状態の UE または 5GC は、サービス要求手順を使用して、AMF へのセキュアな接続の確立を要求します。CM アイドル状態と CM 接続状態の両方の UE は、サービス要求手順を使用して、確立された PDU セッションに対するユーザープレーン接続をアクティブにします。進行中のサービス要求手順が存在する場合、UE はサービス要求手順を開始しません。

SMF は、セッションの作成、または PCF または UE によって開始された変更の一部として受信する CHF および PCF トリガーを保存します。UE が上記の機能のアクセス手順とモビリティ手順をトリガすると、SMF は受信したアクセス パラメータに対して CHF および PCF からのトリガを識別します。次に、SMF は CHF と PCF への更新を送信します。

# 機能の仕組み

SMF は、次の情報に基づいて CHF 機能と PCF 機能を統合します：

- ポリシー制御要求トリガー。PDU セッションの確立、または PCF または UE により開始された変更中の、SM ポリシーの決定で受信されます。
- PDU セッションの確立中、または SMF によって開始された課金更新要求または CHF によって開始された課金更新通知要求への応答として受信される、セッション レベルまたは料金設定グループ レベルの課金トリガー。

SMF は、PCF および CHF トリガーを検出するために、次のアクセス側情報をサポートしています。SMF は N2 ベースのハンドオーバー時に、CHF および PCF にトリガ情報を送信します。

***Table 169: PCF* および *CHF* トリガーに関するアクセス側の情報**

| アクセス側の情報 | **CHF** トリガー | **PCF** トリガー |
|---|---|---|
| UserLocation | USER_LOCATION_CHANGE | SAREA_CH |
| UeTimeZone | UE_TIMEZONE_CHANGE | SAREA_CH |
| ServingNetwork | PLMN_CHANGE | PLMN_CH |
| TargetServingNfId | SERVING_NODE_CHANGE | |

サブスクライバのロケーションの変更の場合、SMF は CHF に USER_LOCATION_CHANGE トリガーを、PCF に SARE_CH トリガーを送信します。

SMF は、次のメッセージでサブスクライバの場所の変更が検出されるたびに使用状況レポートを生成します。

- ベアラー削除コマンド
- ベアラー削除応答
- ベアラー変更要求

たとえば、ベアラー応答の作成ベアラー コマンドの削除が新しい ULI で受信すると、CDR イベントが新しい ULI でトリガーされます。PCF または CHF が ULI の変更に関する通知を待機している場合、SMF は PCF と CHF にそれぞれ通知を送信します。

この機能は、3GPP TS 32.291、バージョン 15.4.0 に準拠しています。

# コール フロー

このセクションでは、次のコールフローについて説明します。

- AMF 内および AMF 間 N2 ベースのハンドオーバー コール フローにおける CHF と PCF の統合
- N26 4G から 5G へのハンドオーバー コール フローの CHF と PCF の統合
- N26 の 5G から 4G へのハンドオーバー コール フローの CHF と PCF の統合
- Xn ハンドオーバー コール フローの CHF と PCF の統合
- サービス要求手順のための CHF と PCF の統合

## AMF 内および AMF 間の N2 ベースのハンドオーバー コール フロー

このセクションでは、CHF と PCF の統合をサポートするための AMF 内および AMF 間 N2 ベースのハンドオーバー コール フローについて説明します。

***Figure 98: AMF** 内および **AMF** 間の **N2** ベースのハンドオーバー コール フロー*

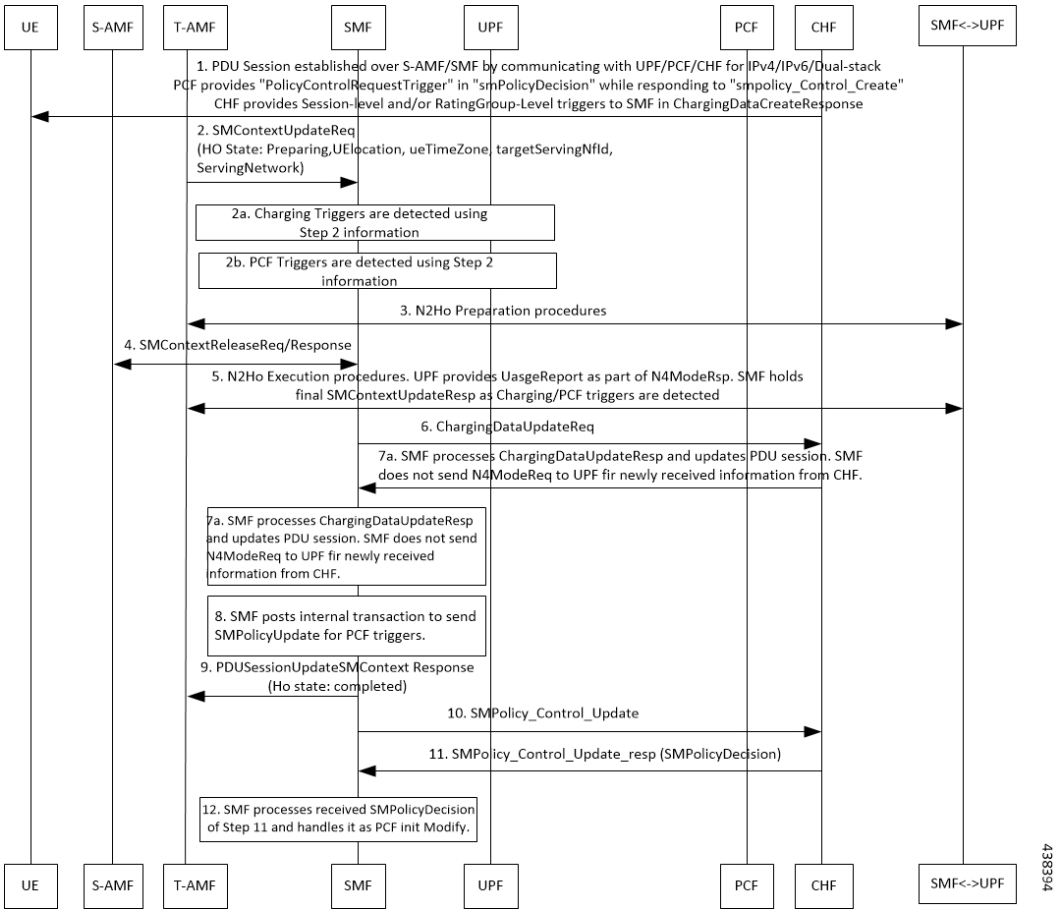


*Table 170: AMF* 内および *AMF* 間 *N2* ベースのハンドオーバーの *CHF* と *PCF* の統合コール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | PDU セッションは、IPv4、IPv6、またはデュアルスタックの UPF、PCF、または CHF との通信により、S-AMF および SMF 経由で確立されます。<br>PCF は、SM ポリシー制御の作成要求への応答として、SM ポリシー決定のポリシー制御要求トリガーを提供します。<br>CHF は、セッション レベルと料金設定グループレベルのトリガーを、課金データ作成応答として SMF に送信します。 |
| 2 | T-AMF は、SMF へのハンドオーバー状態を含めることで SM コンテキスト更新要求を送信します。ハンドオーバー状態には、準備、UE の場所、UE のタイムゾーン、ターゲットのサービス NFID、およびサービスのネットワークに関する情報が含まれます。AMF には、AMF 間ハンドオフのためのターゲット サービス NFID 情報が含まれています。 |
| 2a | SMF は、SM コンテキスト更新要求で受信したアクセス側の変更を検出し、ステップ 2 で利用可能な情報を使用して課金がトリガーされます。 |
| 2b | SMF は、ステップ 2 で使用可能な情報を使用して PCF トリガーを検出します。 |
| 3 | N2 ベースのハンドオーバーの準備手順は、T-AMF から SMF および CHF へ、および反対方向に向けて開始します。 |
| 4 | N2 ベースのハンドオーバー実行手順では、AMF 間ハンドオフの場合、SMF は S-AMF から SM コンテキスト リリース要求を受信し、SM コンテキスト リリース応答で S-AMF に応答します。 |
| 5 | N2 ベースのハンドオーバー実行手順では、UPF は N4 変更応答の一部として使用状況レポートを提供します。SMF は、CHF トリガーまたは PCF トリガを検出すると、最終的な SM コンテキスト リリース応答を保持します。 |
| 6 | SMF は、CHF に課金データ更新要求を送信します。この要求には、セッションレベルのトリガーに関する情報、複数のユニット情報（使用状況レポートを含む料金設定グループレベルのトリガーを使用）、顧客 ID、および PDU セッション課金情報が含まれます。 |
| 7 | CHF は、オプションのマルチユニット情報とともに課金データ更新応答を送信します。CHF は、新しいセッションまたは料金設定グループレベルのトリガーを SMF に送信します。 |
| 7a | SMF は課金データ更新応答を処理し、PDU セッションを更新します。SMF は、CHF から新しく受信した情報の N4 変更要求を UPF に送信しません。 |
| 8 | SMF は内部トランザクションをポストして、PCF トリガーの SM ポリシーの更新情報を送信します。 |

| ステップ | 説明 |
|---|---|
| 9 | SMF は、ハンドオーバー状態が完了した SM コンテキスト更新応答を T-AMF に送信します。 |
| 10 | SMF は PCF に SM ポリシー制御の更新情報を送信します。SM ポリシー制御の更新情報には、ユーザーの場所情報、UE タイム ゾーン、サービス提供ネットワークなどの詳細が含まれます。 |
| 11 | PCF は、SM ポリシー決定である SM ポリシー制御更新応答を SMF に送信します。 |
| 12 | SMF は、応答として受け取った SM ポリシー決定を処理し、PCF によって開始される変更手順をトリガします。 |

## N26 4G から 5G へのハンドオーバー コール フローの CHF と PCF の統合

このセクションでは、N26 4G から 5G へのハンドオーバーの CHF と PCF 統合のコール フローを説明します。

**図 *99 : N26 4G* から *5G* へのハンドオーバー コール フローの *CHF* と *PCF* の統合**

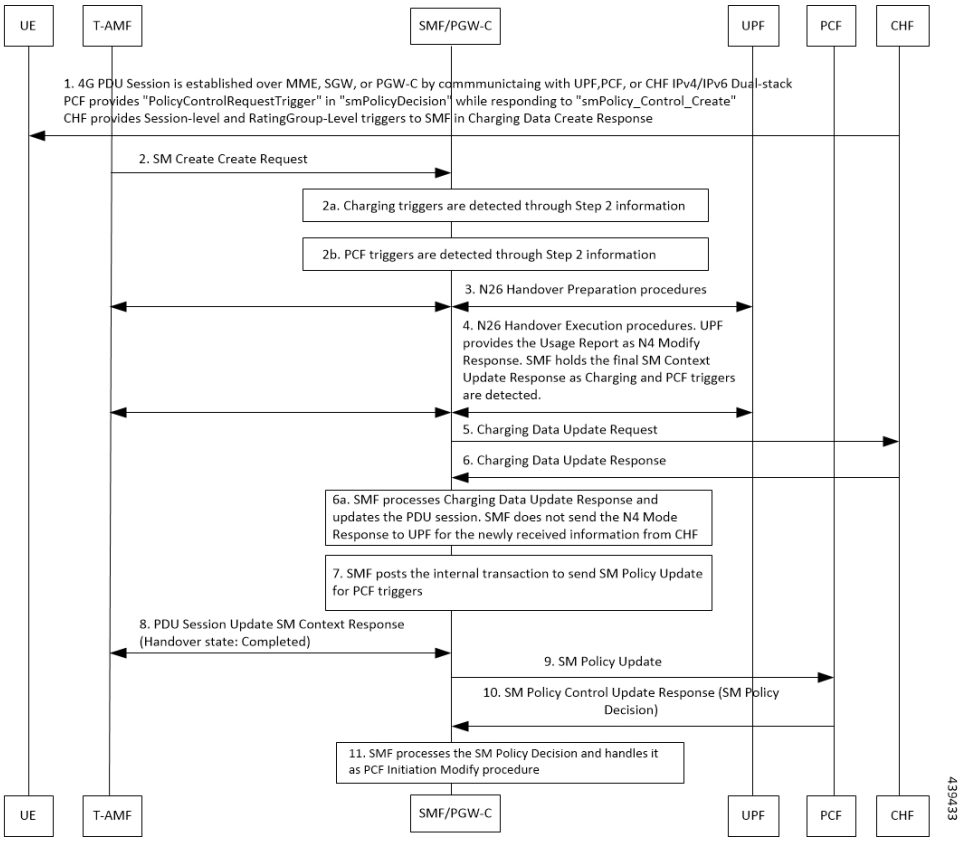


表 *171 : N26* の *4G* から *5G* へのハンドオーバー コール フローの *CHF* と *PCF* の統合

| ステップ | 説明 |
|---|---|
| 1 | PDU セッションは、IPv4、IPv6、またはデュアルスタックの UPF、PCF、または CHF との通信により、MME、SGW、および SMF を介して確立されます。<br>PCF は、SM ポリシー制御の作成要求への応答として、SM ポリシー決定のポリシー制御要求トリガを提供します。<br>CHF は、課金データ作成応答として、セッションレベルおよび料金設定グループレベルのトリガーを SMF に提供します。 |
| 2 | T-AMF は、SM コンテキスト作成要求を SMF に送信します。この要求には、準備されたハンドオーバー状態、UE のロケーション、UE のタイムゾーン、サービス NFID、サービス ネットワーク、RAT タイプに関する情報が含まれます。 |
| 2a | SMF は、SM コンテキスト作成要求で受信したアクセス側の変更を検出し、ステップ 2 で利用可能な情報を使用して課金がトリガされます。 |
| 2b | SMF は、ステップ 2 で使用可能な情報を使用して PCF トリガーを検出します。 |
| 3 | N26 ベース ハンドオーバーの準備手順は、*3GPP TS 23.502, section 4.1.9.3* で定義されているように、SMF または PGW-C および UPF へ、そしてその逆へ、T-AMF から始まります。 |
| 4 | N26 ハンドオーバー実行手順では、UPF は SMF への N4 変更応答の一部として使用状況レポートを提供します。SMF は、CHF トリガーまたは PCF トリガを検出すると、最終的な SM コンテキスト更新応答を保持します。 |
| 5 | SMF は、CHF に課金データ更新要求を送信します。この要求には、セッションレベルのトリガーに関する情報、マルチユニット情報（料金設定グループレベルのトリガーと使用状況レポートを含む）、顧客 ID、および PDU セッション課金情報が含まれます。 |
| 6 | CHF は、オプションのマルチユニット情報とともに課金データ更新応答を送信します。CHF は、新しいセッションまたは料金設定グループレベルのトリガーを SMF に送信します。 |
| 6a | SMF は課金データ更新応答を処理し、PDU セッションを更新します。SMF は、CHF から新しく受信した情報の N4 変更要求を UPF に送信しません。 |
| 7 | SMF は内部トランザクションをポストして、PCF トリガの SM ポリシーの更新情報を送信します。 |
| 8 | SMF は、ハンドオーバー状態が完了した SM コンテキスト更新応答を T-AMF に送信します。 |

| ステップ | 説明 |
|---|---|
| 9 | SMF は PCF に SM ポリシー制御の更新情報を送信します。SM ポリシー制御の更新情報には、ユーザーの場所情報、UE タイム ゾーン、サービス提供ネットワークなどの詳細が含まれます。 |
| 10 | PCF は、SM ポリシー決定である SM ポリシー制御更新応答を SMF に送信します。 |
| 11 | SMF は、応答として受け取った SM ポリシー決定を処理し、 *3GPP TS 23.502*、セクション *4.3.3.2* で定義されているように、その応答を PCF 初期変更手順として処理します。 |

## N26 の 5G から 4G へのハンドオーバー コール フローの CHF と PCF の統合

**表 *172*: 機能の履歴**

| 機能名 | リリース情報 | 説明 |
|---|---|---|
| 3GPPリリース16に準拠した5Gから4Gへのハンドオーバー プロセスの強化 | 2025.01.0 | SM コンテキストの取得中に、SMF は各 EPS ベアラの CN トンネルを確立するために UPF に N4 セッションの変更を送信する場合があります。UPF が到達不能である場合、AMF に適切な原因が返されませんでした。<br>この機能では、新しい応答値 **UPF_NOT_RESPONDING** を導入することで、5G から 4G へのハンドオーバープロセスを強化します。これは、UPF が応答しない場合に SMF によって送信されます。 |

このセクションでは、N26 5G から 4G へのハンドオーバーの CHF と PCF 統合のコール フローを説明します。

図 *100 : N26* の *5G* から *4G* へのハンドオーバー コール フローの *CHF* と *PCF* の統合

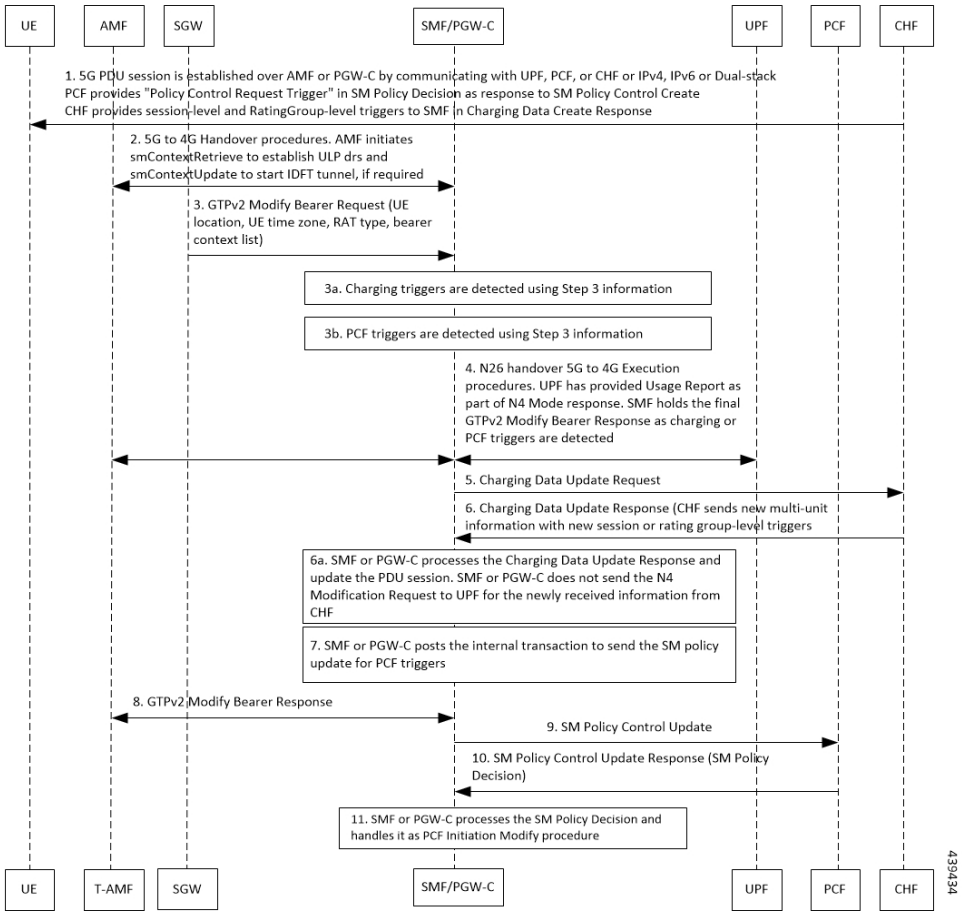



表 *173 : N26* の *5G* から *4G* へのハンドオーバー コール フローの *CHF* と *PCF* の統合

| ステップ | 説明 |
|---|---|
| 1 | PDU セッションは、IPv4、IPv6、またはデュアルスタックの UPF、PCF、または CHF との通信により、S-AMF または SMF 経由で確立されます。<br>PCF は、SM ポリシー制御の作成要求への応答として、SM ポリシー決定のポリシー制御要求トリガーを提供します。<br>CHF は、課金データ作成応答として、セッションレベルおよび料金設定グループレベルのトリガーを SMF に提供します。 |

| ステップ | 説明 |
|---|---|
| 2 | 5Gから4Gへのハンドオーバー手順は、AMFからSMFまたはPGW-Cへ、およびその逆から始まります。AMF は、SM コンテキスト取得要求を開始して UL PDR を確立し、必要に応じて SM コンテキスト更新応答を送信して IDFT トンネルを開始します。<br>リモートピア UPF から応答を受信しない場合、SMF は **UPF_NOT_RESPONDING** を原因とするエラーコード **504 Gateway Timeout** を AMF に送信し、UPF からの応答を受信しないために N4 セッション変更要求が拒否されたことを通知します。 |
| 3 | N26 5G から 4G へのハンドオーバー実行手順では、SGW は GTPv2 ベアラー変更要求を PGW-C に送信します。この要求には、UE の場所、UE のタイムゾーン、RAT タイプ、ベアラー コンテキスト リストの情報が含まれます。 |
| 3a | SMF は、SM コンテキスト更新要求で受信したアクセス側の変更を検出し、ステップ 3 で利用可能な情報を使用して課金がトリガーされます。 |
| 3b | SMF は、ステップ 3 で使用可能な情報を使用して PCF トリガーを検出します。 |
| 4 | N26 ハンドオーバー 5G から 4G への実行手順では、PGW-C は UPF に各フローの GTP-U トンネルを作成するように要求します。このトンネルは、GTPv2 ベアラー変更要求のベアラー コンテキスト リストで受信した EBI 用です。DL PDR が確立されると、UPF は N4 変更応答の一部として使用状況レポートを SMF に送信します。SMF は、CHF または PCF トリガーを検出すると、最終的な GTPv2 ベアラ変更応答を保持します。 |
| 5 | SMF は、CHF に課金データ更新要求を送信します。この要求には、セッションレベルのトリガーに関する情報、マルチユニット情報（料金設定グループレベルのトリガーと使用状況レポートを含む）、顧客 ID、および PDU セッション課金情報が含まれます。 |
| 6 | CHF は、オプションのマルチユニット情報とともに課金データ更新応答を送信します。CHF は、新しいセッションまたは料金設定グループレベルのトリガーを SMF に送信します。 |
| 6a | SMF または PGW-C は課金データ更新応答を処理し、PDU セッションを更新します。SMF は、CHF から新しく受信した情報の N4 変更要求を UPF に送信しません。 |
| 7 | SMF または PGW-C は内部トランザクションをポストして、PCF トリガの SM ポリシーの更新情報を送信します。 |
| 8 | SMF または PGW-C は、ハンドオーバー状態が完了した SM コンテキスト更新応答を AMF に送信します。 |
| 9 | SMF または PGW-C は PCF に SM ポリシー制御の更新情報を送信します。SM ポリシー制御の更新情報には、ユーザーの場所情報、UE タイム ゾーン、サービス提供ネットワークなどの詳細が含まれます。 |
| 10 | PCF は、SM ポリシー決定である SM ポリシー制御更新応答を SMF に送信します。 |

| ステップ | 説明 |
|---|---|
| 11 | SMF は、応答として受け取った SM ポリシー決定を処理し、 *3GPP TS 23.502*、セクション *4.3.3.2* で定義されているように、その応答を PCF 初期変更手順として処理します。 |

## Xn ハンドオーバー コール フローの CHF と PCF の統合

ここでは、Xn ハンドオーバーのための CHF と PCF の統合のコール フローについて説明します。

**図 *101 : Xn* ハンドオーバー コール フローの *CHF* と *PCF* の統合**

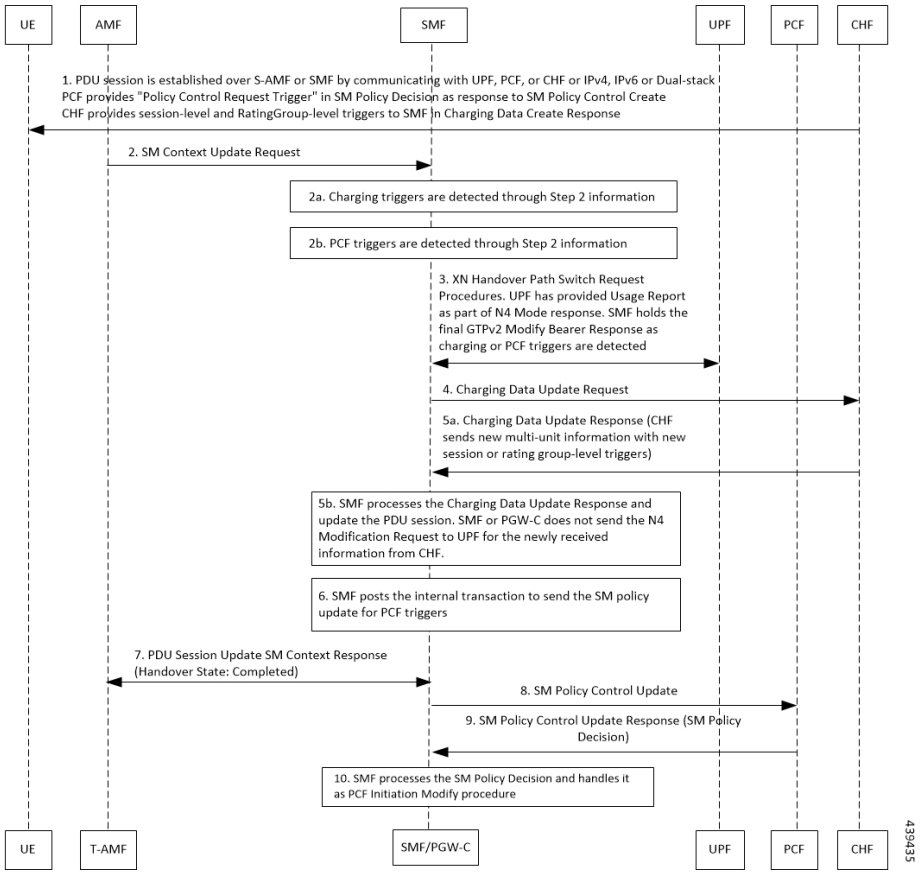


表 *174 : Xn* ハンドオーバー コール フローの説明のための *CHF* と *PCF* の統合

| ステップ | 説明 |
|---|---|
| 1 | PDU セッションは、IPv4、IPv6、またはデュアルスタックの UPF、PCF、または CHF との通信により、MME、SGW、および SMF を介して確立されます。<br>PCF は、SM ポリシー制御の作成要求への応答として、SM ポリシー決定のポリシー制御要求トリガを提供します。<br>CHF は、課金データ作成応答として、セッションレベルおよび料金設定グループレベルのトリガーを SMF に提供します。 |
| 2 | AMF は、SM コンテキスト更新要求を SMF に送信します。SM コンテキスト更新要求には、UE の場所、UE のタイムゾーン、およびパス スイッチ要求 N2 メッセージに関する情報が含まれます。 |
| 2a | SMF は、SM コンテキスト更新要求で受信したアクセス側の変更を検出し、ステップ 2 で利用可能な情報を使用して課金がトリガーされます。 |
| 2b | SMF は、ステップ 2 で使用可能な情報を使用して PCF トリガーを検出します。 |
| 3 | Xn ハンドオーバーの準備手順は、*3GPP TS 23.502*、セクション *4.9.1.2* で定義されているように、SMF から UPF へ、およびその逆の方向に始まります。<br>SMF は N4 変更要求を UPF に送信し、受信した T-gNB の DL トンネル情報を更新します。トンネル情報が更新されると、UPF は N4 変更応答の一部として使用状況レポートを提供します。SMF は、CHF トリガーまたは PCF トリガを検出すると、最終的な SM コンテキスト更新応答を保持します。 |
| 4 | SMF は、CHF に課金データ更新要求を送信します。この要求には、セッションレベルのトリガーに関する情報、マルチユニット情報（料金設定グループレベルのトリガーと使用状況レポートを含む）、顧客 ID、および PDU セッション課金情報が含まれます。 |
| 5 | CHF は、オプションのマルチユニット情報とともに課金データ更新応答を送信します。CHF は、新しいセッションまたは料金設定グループレベルのトリガーを SMF に送信します。 |
| 5a | SMF は課金データ更新応答を処理し、PDU セッションを更新します。SMF は、CHF から新しく受信した情報の N4 変更要求を UPF に送信しません。 |
| 6 | SMF は内部トランザクションをポストして、PCF トリガの SM ポリシーの更新情報を送信します。 |
| 7 | SMF は、SM コンテキスト更新応答を AMF に送信します。この応答には、パス スイッチ要求の確認応答 N2 メッセージが含まれています。 |
| 8 | SMF は PCF に SM ポリシー制御の更新情報を送信します。SM ポリシー制御の更新には、ユーザーの場所情報や UE タイムゾーンなどの詳細が含まれます。 |

| ステップ | 説明 |
|---|---|
| 9 | PCF は、SM ポリシー決定である SM ポリシー制御更新応答を SMF に送信します。 |
| 10 | SMF は、応答として受け取った SM ポリシー決定を処理し、*3GPP TS 23.502*、セクション*4.3.3.2*で定義されているように、その応答を PCF 初期変更手順として処理します。 |

### サービス要求手順のための CHF と PCF の統合

このセクションでは、サービス要求手順に関する CHF と PCF の統合について説明します。

SMF は受信した SM コンテキスト更新要求を処理して、N3 トンネルパスの状態をアイドルからアクティブ、またはアクティブからアイドルに更新します。SMF は次のステップを実行します：

1. UE が AMF で CM アイドル状態（アクティブからアイドル モード）の場合、SMF は構成に基づき、N4 セッション モード要求を送信して N3 トンネル状態の UPF をドロップまたはバッファに更新します。課金構成に基づいて、SMF は使用状況レポートを受信します。セッション作成中に認定された課金トリガーに基づいて、SMF は N40 課金更新要求を送信します。
2. UE が AMF で CM 接続状態になっている場合（これは、SMF が UE 要求の手順を受信してサブスクライバ N3 トンネル パスをアイドル状態からアクティブ状態に変更するための手順を受信することを意味します）：SMF は、SM コンテキスト更新要求で更新されたユーザーの場所と UE タイムゾーンを受信します。SMF は、N4 セッション変更要求を UPF に送信して、gNB の DL トンネルの詳細を更新します。課金構成に基づいて、SMF は使用状況レポートを受信します。セッション作成中に認定された課金トリガーに基づいて、SMF は N40 課金更新要求を送信します。
3. N3 トンネルがネットワーク サービス要求トリガーに対して使用できない場合（これは、UE が AMF で CM-アイドル状態であることを意味します）、SMF は、エンド ユーザーに対してページングを開始するために AMF のネットワーク サービス要求手順を開始します。次に、AMF は、UE サービス要求手順を開始して、ステップ 2 で指定したように N3 トンネルを構成します。

## 標準準拠

アクセスとモビリティ手順の CHF と PCF の統合は、次の標準に準拠しています。

- *3GPP TS 23.502* バージョン *15.4.0* リリース *15*（セクション *4.9.1.3*、*4.11.1.2*、*4.9.1.2*、および *4.2.3*）：*5G 5G* システムの手順
- *3GPP TS 29.502*、バージョン *16.2.0*

# gNodeB 間ハンドオーバー

## 機能説明

SMF は、Xn または N2 参照ポイントを使用してソース NG-RAN ノードからターゲット NG-RAN ノードに UE を渡すための Xn ベースおよび N2 ベースのハンドオーバー手順をサポートしています。この手順の開始は、新しい無線条件、ロードバランシング、または特定のサービスによる場合があります。

SMF は、それぞれのインターフェイス N4（UPF）と N1（UE）での Xn および N2 ハンドオーバー中にターゲット NG-RAN で設定できなかった QoS フローを解放します。SMF は、防御状態の場合、トリガに基づいて N7（PCF）に適切な通知を送信します。SMF は、解放された QoS フローの使用状況レポートを N40（CHF）に送信します。

## 機能の仕組み

### コール フロー

次のセクションでは、Xn ベースおよび N2 ベースのハンドオーバー手順の実行について説明します。

#### Xn ベースの NG-RAN間ハンドオーバー

このセクションでは、UPF 再割り当てを使用しない Xn ベースの NG-RAN 間ハンドオーバーに関する詳細について説明します。

引き継ぎの準備と実行段階は、*3GPP TS 38.300* で規定されているとおりに実装されます。共有ネットワークでハンドオーバーを実行する場合、送信元の NG-RAN は、*3GPP TS 23.501* で指定されているように、ターゲット ネットワークで使用する PLMN を決定します。Xn ハンドオーバー中にサービス提供している PLMN が変更された場合、ソースの NG-RAN ノードは、選択した PLMN ID をターゲットの NG-RAN ノードに示します。

AMF が N2 ダウンリンク シグナリングを生成し、実行中の N2 ハンドオーバーが原因で N2 インターフェイス手順の拒否を受信した場合、AMF は ハンドオーバー手順が完了するか、失敗したと見なされたときに、同じ N2 インターフェイス手順を再試行します。障害は、N2 インターフェイス手順を保護するタイマーの期限切れによってわかります。

SMF によって開始された N1 および/または N2 要求を受信し、進行中の Xn ハンドオーバー手順のために要求が一時的に拒否されたことを示して、SMF はローカルに構成されたガード タイマーを開始します。SMF は、ハンドオーバーが完了した、またはハンドオーバーが失敗したかキャンセルされたかを検出しない限り、ハンドオーバーの準備フェーズ中に AMF に向けられたシグナリング メッセージを保持します。SMF は、ハンドオーバーが完了したこと、または失敗したことを検出した場合に、メッセージ受信またはガード タイマーの期限切れを検出すると、事前に構成された回数まで再試行します。

Xn ベースの NG-RAN 間ハンドオーバーは、AMF が変更されず、SMF が既存の UPF を維持することを決定した場合に、Xn を使用してソース NG-RAN からターゲット NG-RAN に UE を渡すために使用されます。

以下の図は、UPF の再割り当てを行わない Xn ベースの相互 NG-RAN ハンドオーバーのコールフローを示している。

**図 *102 : Xn* ベースの *NG-RAN* 間ハンドオーバー（*UPF* 再割り当てなし）**

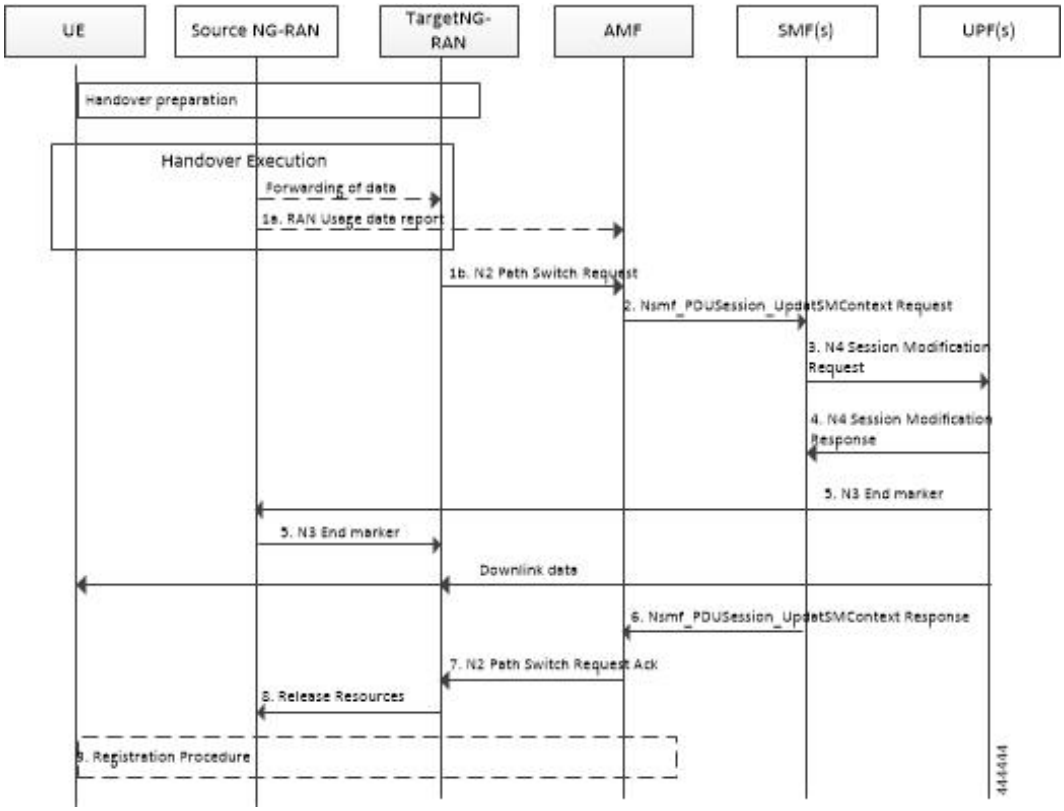



**表 *175 : Xn* ベースの *NG-RAN* 間ハンドオーバー コール フローの説明（*UPF* 再割り当てなし）**

| ステップ | 説明 |
|---|---|
| 1a | ハンドオーバーの実行中、送信元の NG-RAN ノードは、RAN 使用状況データ レポートを AMF に提供します。送信元 NG-RAN ノードは、ターゲット NG-RAN が Xn インターフェイスを介した引き継ぎを確認した場合にのみ、このレポートを提供します。<br><br>このレポートには、N2 SM 情報（セカンダリ RAT 使用状況データ）、ハンドオーバーフラグ、および送信元から対象への透過コンテナが含まれます。ハンドオーバーフラグは、レポートが SMF によってバッファされる必要があることを示します。 |

| ステップ | 説明 |
|---|---|
| 1b | 対象 NG-RAN は、N2 パス切り替え要求メッセージを AMF に送信して、UE が新しい対象セルに移動したことを通知します。NG-RAN は、[切り替えられるPDUセッションのリスト（List Of PDU Sessions To Be Switched）] を提供します。N2 SM 情報には、スイッチされる各 PDU セッションの AN トンネル情報が含まれます。 |
| 2 | AMF は、N2 パススイッチ要求で受信した PDU セッションのリスト内の各 PDU セッションに対する Nsmf_PDUSession_UpdateSMContext 要求サービス操作を呼び出すことにより、N2 SM 情報を送信します。 |
| 3 | SMF は、N4 セッション変更要求メッセージを UPF に送信します。SMF は、データ通知を発信した UPF に、PDU セッションのダウンリンク データを破棄したり、それ以降のデータ通知メッセージを提供しないように通知したりする場合があります。 |
| 4 | UPF は、要求された PDU セッションが切り替えられた後、SMF に N4 セッション変更応答メッセージを返します。 |
| 5 | UPF は、パスを切り替える直後に、古いパス上の各 N3 トンネルに 1 つ以上の「エンド マーカー」パケットを送信します。UPF はターゲットの NG-RAN へのダウンリンク パケットの送信を開始します。 |
| 6 | SMF は、正常に切り替えられた PDU セッションの AMF に、Nsmf_PDUSession_UpdateSMContext 応答（CN トンネル情報）を送信します。<br>**重要**<br>ステップ 6 は、SMF で N4 セッション変更応答を受信した後はいつでも実行できます。 |
| 7 | すべての SMF から Nsmf_PDUSession_UpdateSMContext 応答を受信すると、AMF は受信した CN トンネル情報を集約し、この集約情報を N2 SM 情報の一部として、N2 パス スイッチ要求 Ack の失敗した PDU セッションと共にターゲット NG-RAN に送信します。要求された PDU セッションのいずれも正常に切り替えられなかった場合、AMF はターゲットの NG-RAN に N2 パス切り替え要求の失敗メッセージを送信します。 |
| 8 | ターゲットの NG-RAN は、リソースの解放メッセージをソースの NG-RAN に送信することで、ハンドオーバーが成功したことを確認します。 |
| 9 | 登録手順のトリガのいずれかが適用される場合、UE はモビリティ登録の更新手順を開始します。 |

次の図は、UPF 再割り当てを使用しない Xn ハンドオーバーの詳細なコール フローを示しています。

図 *103 : UPF* 再配置がない *Xn* ハンドオーバー コール フロー

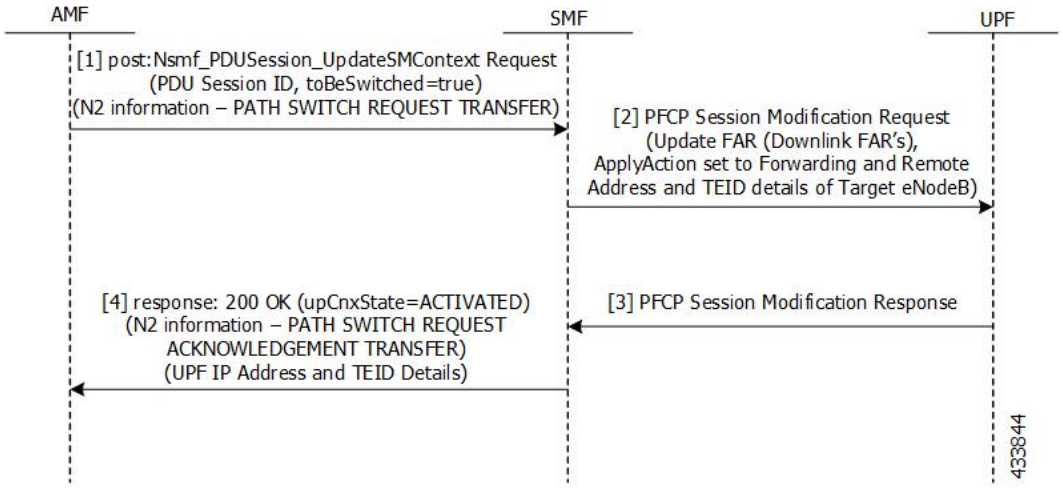



表 *176 : UPF* 再配置なしの *XN* ハンドオーバーに関するコール フローの詳細な説明

| ステップ | 説明 |
|---|---|
| 1 | NF サービス コンシューマ（AMF）は、SMF に PDU セッションのユーザー プレーン接続を切り替えるように要求します。AMF は次の情報を含む POST 要求を送信します。<br>• toBeSwitched 指示。<br>• 5G-AN（PDU セッション パス スイッチ要求転送 IE）から受信した N2 SM 情報。これには、この PDU セッションのユーザー データに対する新しいトランスポート層アドレス、ダウンリンク ターミネーション ポイントのトンネル エンドポイントが含まれます。<br>• ユーザーの場所とユーザーの場所のタイムスタンプ。<br>• その他の情報（必要な場合）。 |
| 2 | SMF では、要求を受信した後に PDU セッションの N3 トンネルを切り替えます。SMF は、次のオプションで更新されたダウンリンク FAR を使用して、UPF に対する PFCP セッション変更手順を開始します。<br>• 転送アクションは、IP アドレスや GTP-U F-TEID などのリモート ノードの「転送パラメータ」の詳細とともに有効になります。 |
| 3 | SMF は、UPF ノードから正常な応答を受信した後、PDU の引き継ぎを正常とマークします。 |

| ステップ | 説明 |
|---|---|
| 4 | SMF は 200 OK 応答を開始します。この応答には、この PDU セッションのユーザープレーンデータのアップリンク終端ポイントのトランスポート層アドレスとトンネルエンドポイント（アップリンク トラフィックの UPF GTP-U F-TEID）を含む N2 SM 情報が含まれています。 |

## N2 ベースの NG-RAN 間ハンドオーバー

**表 *177:* 機能の履歴**

| 機能名 | リリース情報 | 説明 |
|---|---|---|
| N2 ベースのハンドオーバーのための IDFT での DRB レベルのデータ転送 | 2023.04 | SMF は、データ転送要求の確認応答メッセージにデータ転送応答 DRB リストがあり、セッション レベルの転送の基準を満たしていない場合に、DRB レベルのデータ転送をサポートします。 |

送信元の NG-RAN は、ターゲットの NG-RAN に N2 ベースのハンドオーバー（HO）を開始することを決定します。この手順を開始する理由として、次のいずれかが考えられます：

- 新しい無線条件
- ロード バランシング
- ターゲット NG-RAN への XN 接続がない場合
- Xn ベースのハンドオーバーが失敗した後（つまり、ターゲット RAN（T-RAN）と送信元 UPF（S-UPF）の間に IP 接続がない場合）、ターゲット NG-RAN からエラーが表示されます。
- 送信元 RAN（S-RAN）から学習したダイナミックな情報に基づいています

送信元 NG-RAN は、直接転送パスの可用性を判断し、SMF にそれを示します。送信元とターゲットの NG-RAN 間で IP 接続が使用可能で、それらの間にセキュリティ関連付けが設定されている場合、直接転送パスが使用できます。直接転送パスが使用できない場合は、間接転送を使用します。SMF は、送信元 NG-RAN からの指示を使用して、データ転送パスを選択します。

共有ネットワークでハンドオーバーを実行する場合、送信元の NG-RAN は、*3GPP TS 23.501* で指定されているように、ターゲット ネットワークで使用する PLMN を決定します。送信元の NG-RAN は、HO 要求メッセージで送信されるトラッキング エリアの一部として、選択された PLMN ID を AMF に示します。

AMF が N2 ダウンリンク シグナリングを生成し、実行中の N2 ハンドオーバーが原因で N2 インターフェイス手順の拒否を受信した場合、AMF は ハンドオーバーが完了するか、失敗したと見なされたときに、同じ N2 インターフェイス手順を再試行します。NG-RAN ノード間のハンドオーバーによってサービング AMF が変更された場合、送信元の AMF は、ハンドオーバー手順を除く他の進行中の N2 インターフェイス手順を終了します。

AMF がまだ AMF を提供している場合、AMF は非ハンドオーバー関連の N2 インターフェイス手順を一時停止し、N2 ハンドオーバーが完了した後にそれらの手順を再開します。

変更する必要があることを AMF が検出すると、AMF は SMF によって開始された N2 要求を拒否し、進行中の N2 ハンドオーバー手順のために要求が一時的に拒否されたという指示を含めます。

次の図は、N2 ベースの NG-RAN 間ハンドオーバー手順の準備段階のコールフローを示しています。

**図 *104 : NG-RAN* ノード *N2* ベースのハンドオーバー：準備フェーズ**

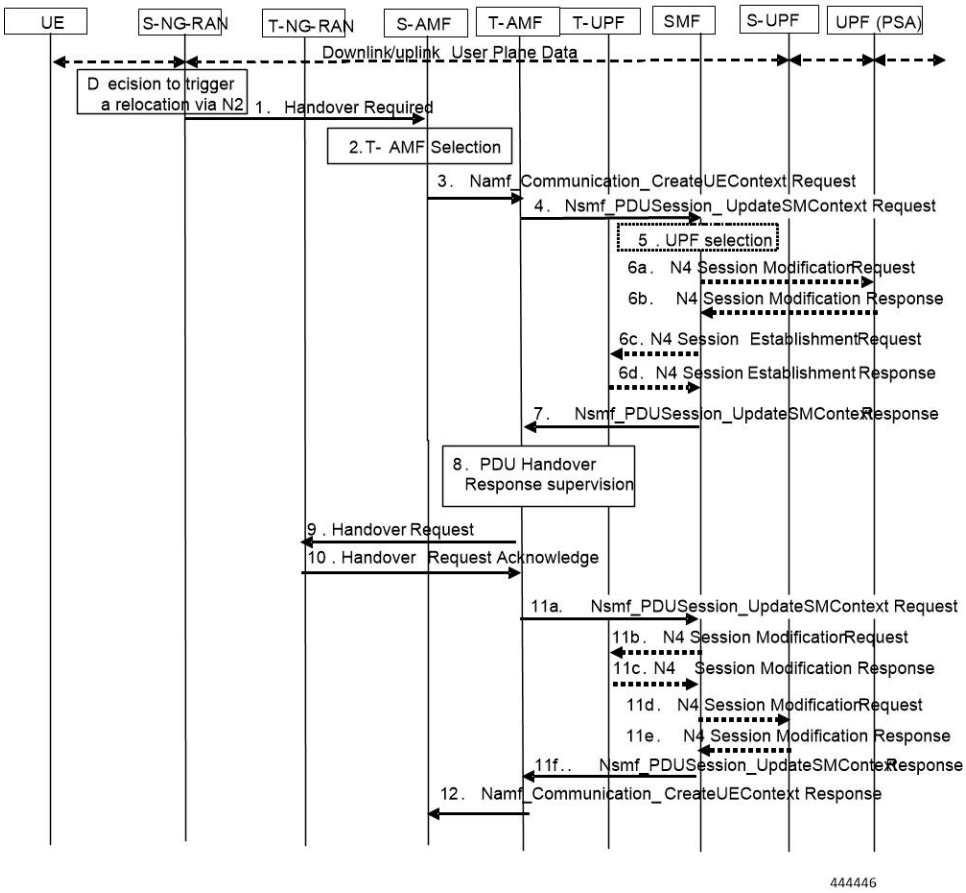


表 *178 : NG-RAN* ノードの *N2* ベースのハンドオーバー コールフローの説明：準備フェーズ

| ステップ | 説明 |
|---|---|
| 1 | 送信元 NG-RAN（S-RAN）が送信元 AMF（S-AMF）にハンドオーバーが必要であることを示すメッセージを送信します。このメッセージには、次の内容が含まれます：<br>• ターゲットID<br>• 送信元からターゲットへの透過コンテナ<br>• SM N2 情報リスト<br>• PDU セッション ID<br>• システム内引き継ぎの表示<br>送信元からターゲットへの透過コンテナには、ターゲットRAN（T-RAN）で使用する NG-RAN 情報が含まれ、5GC に対して透過的です。また、対応するユーザー プレーン セキュリティ施行情報、データ転送の対象となる QoS フロー/DRB 情報も含まれます。<br>直接データ転送が使用可能な場合、SM N2 情報には、直接転送パスの可用性が含まれます。<br>直接転送パスの可用性は、S-RAN から T-RAN への直接転送が使用可能かどうかを示します。S-RAN からのこの通知は、S-RAN と T-RAN 間の IP 接続とセキュリティ関連付けの存在に基づいています。 |
| 2 | S-AMF が UE に対応できなくなる場合、S-AMF は、 *TS 23.501*の「AMF 選択機能」のセクション 6.3.5 で説明されているように T-AMF を選択します。 |

| ステップ | 説明 |
|---|---|
| 3 | S-AMF は、T-AMF に対して Namef_Communication_CreateUEContext サービス操作を呼び出すことにより、ハンドオーバー リソース割り当て手順を開始します。<br>Namef_Communication_CreateUEContext 要求には、次のものが含まれます：<br>• N2 情報<br>• ターゲットID<br>• 送信元からターゲットへの透過コンテナ<br>• SM N2 情報リスト<br>• PDU セッション ID<br>• UE コンテキスト情報<br>• SUPI<br>• サービス エリアの制限<br>• アクセス タイプごとに NSSAI を許可（利用可能な場合）<br>• トレース要件<br>• PDU セッション ID と、対応する SMF 情報と、対応する S-NSSAI、PCF ID、および DNN のリスト<br>S-AMF が依然として UE にサービスを提供できる場合、このステップとステップ 12 は不要です。 |
| 4 | S-RAN によって指定された PDU セッションごとに、AMF は、関連付けられている SMF に対して Nsmf_PDUSession_UpdateSMContext 要求を呼び出します。ただし、PDU セッションに関連付けられている S-NSSAI が T-AMF で使用できない場合、T-AMF はこの PDU セッションの Nsmf_PDUSession_UpdateSMContext を呼び出しません。<br>T-AMF が、UE がサービス エリア制限に基づいて制限されたエリアに移動することを検出した場合、T-AMF は、UE 到達可能性イベントにサブスクライブしている各 NF コンシューマに対して、規制上優先されるサービスのみが UE に到達可能であることを通知します。 |
| 5 | ターゲット ID に基づいて、SMF は指定された PDU セッションに対する N2 ハンドオーバーの受け入れを確認します。SMF は UPF 選択基準もチェックします。UE が NG-RAN に接続している UPF のサービス エリアから移動した場合、SMF は新しい中間 UPF を選択します。 |

| ステップ | 説明 |
|---|---|
| 6a | SMF が PDU セッションの中間 UPF として機能する新しい UPF を選択し、別の CN トンネル情報を使用する必要がある場合、SMF は N4 セッション変更要求メッセージを UPF（PDU セッションアンカー（PSA））に送信します。SMF が CN トンネル情報を割り当てると、N9 上で CN トンネル情報が提供され、UPF（PSA）は CN トンネル情報を UL パケット検出ルールに関連付けます。 |
| 6b | UPF（PSA）は、N4 セッション確立応答メッセージを SMF に送信します。UPF（PSA）が UPF（PSA）の CN トンネル情報（N9 上）を割り当てる場合、CN トンネル情報（N9 上）を SMF に提供します。UPF（PSA）は、CN トンネル情報（N9 上）を SMF によって提供される UL パケット検出ルールと関連付けます。 |
| 6c | SMF が新しい中間 UPF（T-UPF）を選択し、T-UPF が CN トンネル情報を割り当てる場合、SMF は N4 セッション確立要求メッセージを T-UPF に送信します。この要求により、パケット検出、適用、およびレポート ルールを T-UPF にインストールできるようになります。T-UPF は、この PDU セッションの UPF（PSA）の CN トンネル情報（N9 上）を受信します。これは、N9 トンネルのセットアップに使用されます。 |
| 6d | T-UPF は、DL CN トンネル情報および UL CN トンネル情報（つまり、N3 トンネル情報）とともに N4 セッション確立応答メッセージを SMF に送信します。SMF は、実行フェーズのステップ 13a で使用される S-UPF のリソースを解放するためのタイマーを開始します。 |
| 7 | PDU セッションの N2 ハンドオーバーが受け入れられた場合、SMF は Nsmf_PDUSession_UpdateSMContext 応答に N2 SM 情報を含めます。N2 SM 情報には、N3 UP アドレス、UPF の UL CN トンネル ID、および N2 SM 情報がターゲットの NG-RAN 用であることを示す QoS パラメータが含まれます。<br><br>ステップ 4 で受信した N2 SM 情報にダイレクト転送パスの可用性が含まれず、SMF が送信元とターゲットの間に間接的なデータ転送接続がないことを認識している場合、N2 SM 情報にはデータ転送が不可能であるという指示が含まれます。<br><br>ステップ 5 の説明に従って PDU セッションの N2 ハンドオーバーが受け入れられない場合、ターゲットの NG-RAN での無線リソースの確立を回避するため、SMF には N2 SM 情報が含まれません。SMF は、受け入れられなかった理由を提示します。SMF は、規制の優先サービスでのみ UE に到達可能であるという通知を T-AMF から受信した場合、PDU セッションを非アクティブ化します。 |
| 8 | AMF は、関係する SMF からの Nsmf_PDUSession_UpdateSMContext 応答メッセージを監視します。最大待機時間の期限切れ時、またはすべての Nsmf_PDUSession_UpdateSMContext 応答メッセージを受信した時点で、AMF は N2 ハンドオーバー手順（ステップ9のハンドオーバー要求メッセージ）を続行します。 |

| ステップ | 説明 |
|---|---|
| 9 | サブスクリプション情報にトレース要件が含まれている場合、ターゲット AMF は、ハンドオーバー要求でトレース要件をターゲット RAN に提供します。<br><br>ハンドオーバー要求には、送信元からターゲットへの透過コンテナ、N2 MM 情報、N2 SM 情報リスト、およびトレース要件が含まれます。<br><br>T-AMF は、ターゲット ID に基づいて T-RAN を決定します。T-AMF は、AMF とターゲット TAI の UE に有効な 5G-GUTI を割り当てます。<br><br>N2 MM 情報には、たとえば、セキュリティ情報やモビリティ制限リスト（T-AMF で入手可能な場合）が含まれます。N2 SM 情報リストには、ステップ 8 で T-AMF によって監視された許可最大遅延内で受信した Nsmf_PDUSession_UpdateSMContext 応答メッセージ内の T-RAN の N2 SM 情報が含まれます。 |
| 10 | T-RAN は、T-AMF にハンドオーバー要求の確認応答を送信します。確認応答メッセージには、ターゲットから送信元への透過コンテナ、N2 SM 情報を使用したハンドオーバーする PDU セッションのリスト、N2 SM 情報要素で指定された障害原因で確立に失敗した PDU セッションのリストが含まれます。 |

| ステップ | 説明 |
|---|---|
| 11a | AMF は、Nsmf_PDUSession_UpdateSMContext 要求（PDU セッション ID、N2 SM 応答）を SMF に送信します。<br>T-RAN から受信した N2 SM 応答ごとに、AMF は N2 SM 応答をそれぞれの PDU セッション ID で指定された SMF に送信します。<br>新しい T-UPF が選択されていない場合、SMF は N2 ハンドオーバーが T-RAN によって受け入れられると、N2 SM 応答からの T-RAN の N3 トンネル情報を保存します。<br>SMF/UPF は、T-RAN によって確立されたデータ転送トンネル エンドポイントに対応する間接データ転送用の N3 UP アドレスとトンネル ID を割り当てます。<br>ターゲットの NG-RAN によって PDU セッションが拒否された PDU セッションとして示されている場合、SMF はこの PDU セッションの解放をトリガーします。PDU セッション拒否のその他のすべての場合、SMF は PDU セッションを解放するか、この PDU セッションの UP 接続を非アクティブにするかを決定します。<br>PDU セッションの一部の QoS フローがターゲットの NG-RAN によって受け入れられない場合、SMF は、ハンドオーバーの完了後に、受け入れられていない QoS フローを PDU セッションから削除するための PDU セッション変更手順を開始します。<br>（注）<br>N2 ハンドオーバーで、S-RAN と T-RAN の間で直接パスが使用できない場合、SMF はデータ転送用に IDFT を有効にすることを決定できます。<br>したがって、SMF は、間接データ転送用に T-RAN から DL 転送 UP トンネル情報を受信すると、セッション レベルのデータ転送を行います。SMF は、データ転送応答 DRB リストを受信すると、DRB レベルのデータ転送を開始します。<br>T-RAN が DL 転送 UP トンネル情報を提供しない場合、SMF は IDFT なしで HO を続行します。 |
| 11b | SMF は、N4 セッション変更要求を T-UPF に送信します。この要求には、T-RAN SM N3 転送情報リストと、間接転送用に DL 転送トンネルを割り当てる指示が含まれます。 |
| 11c | T-UPF はトンネル情報を割り当て、N4 セッション変更応答メッセージを SMF に返します。T-UPF SM N3 転送情報リストには、データを転送するための T-UPF N3 アドレス、T-UPF N3 トンネル識別子が含まれます。 |
| 11d | SMF は S-UPF に N4 セッション変更要求を送信します。この要求には、T-RAN SM N3 転送情報リストまたは T-UPF SM N3 転送情報リストと、間接転送用に DL 転送トンネルを割り当てる指示が含まれます。 |

| ステップ | 説明 |
|---|---|
| 11e | S-UPF はトンネル情報を割り当て、N4 セッション確立応答メッセージを SMF に返します。<br>S-UPF SM N3 転送情報リストには、DL データ転送用の S-UPF N3 アドレスと S-UPF N3 トンネル識別子が含まれます。 |
| 11f | SMF は、PDU セッションごとに Nsmf_PDUSession_UpdateSMContext Response メッセージを T-AMF に送信します。<br>SMF は、引き継ぎコマンドで DRB レベルの転送の **qosFlowToBeForwardedList** を入力しません。ただし、セッション レベルの転送の場合、SMF は、転送用に選択された QFI を使用して **qosFlowToBeForwardedList** を送信します（ハンドオーバー確認応答の dataForwardingAccepted 指示に基づく）。 |
| 12 | AMF は、関係する SMF からの Nsmf_PDUSession_UpdateSMContext Response メッセージを監視します。最大待機時間の期限切れ時、またはすべての Nsmf_PDUSession_UpdateSMContext 応答メッセージを受信した時点で、T-AMF は Name_Communication_CreateUEContext 応答を S-AMF に送信します。 |

### IDFT でのセッション レベルのデータ転送

N2セットアップ応答を取得すると、SMFはハンドオーバー要求の応答確認転送をデコードし、既存のフローのメッセージ内にデータ転送承認済み IE が存在するかどうかを検証します。IE が少なくとも 1 つのフローに存在する場合、SMF は、DL 転送 UP TNL 情報 IE で受信したターゲット gNB TEID を持つフローごとに、送信元 gNB から転送されたパケットを受信するためにアップリンク PDR を作成し、パケットをターゲット gNB に転送するために作成します。SMF が引き継ぎ要求の確認応答で QoS フロー セットアップ応答リストを受信しなくても、DL 転送 UP TNL 情報 IE が存在すれば、SMF はセッション レベルの転送を続行します。SMF は、フローまたは転送を有効にする必要がある転送（QoS フローの転送項目）、およびパケットを転送するための UPF TEID（DL 転送 UP TNL 情報 IE）を示すハンドオーバー コマンドを送信元 gNB に送信します。

### IDFT での DRB レベルのデータ転送

引き継ぎ要求の確認応答を受信した SMF が、セッション レベル転送の条件が満たされていないことを検出し、**データ転送応答 DRB リスト** IE が存在する場合、SMF は DRB レベル転送を続行します。

SMF は N4 セッション変更要求をトリガーして、DRB リストに存在する各 DRB（データ無線ベアラー）のアップリンク PDR（パケット検出ルール）を作成します。PDR は QFI（QoS フロー識別子）に関連付けられません。各 DRB では、送信元 gNB から転送されたデータを受信するためのトンネルが作成され、各 PDR は FAR（転送アクション ルール）に関連付けられて、それらのパケットをターゲット gNB に送信します。各 FAR は、対応する DRB で受信した **DL データ転送 UP TNL 情報を**受信したターゲット gNB TEID に関連付けられます。

SMF には、ハンドオーバー コマンド転送での対応する DRB の UPF TEID を持つ **データ転送応答 DRB リスト** IE が含まれます。

次の図は、N2 ベースの NG-RAN 間ハンドオーバー手順の実行フェーズのコール フローを示しています。

**図 *105 : NG-RAN* ノード間 *N2* ベースのハンドオーバー：実行フェーズ**

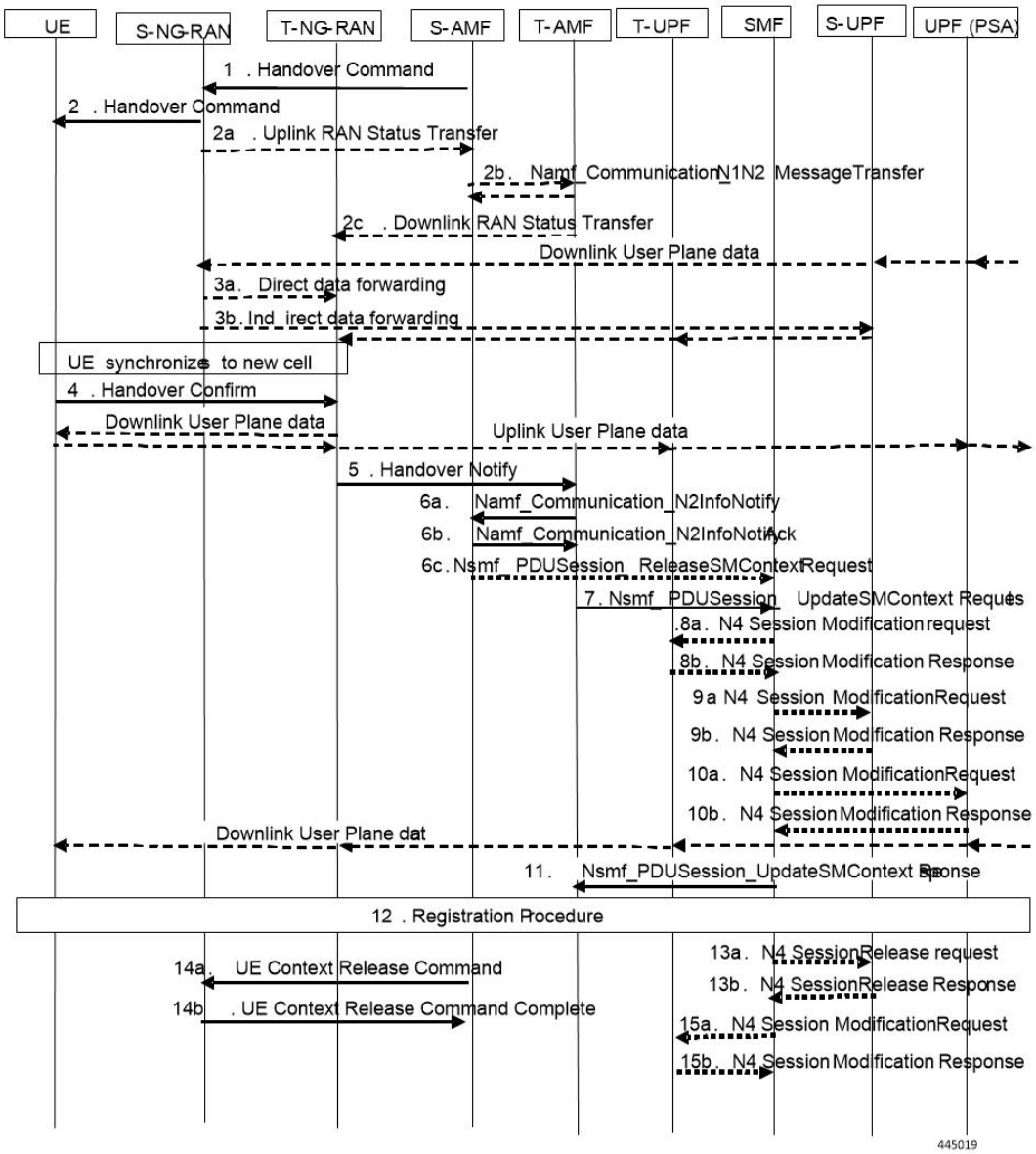


表 *179 : NG-RAN* ノードの *N2* ベースのハンドオーバー コール フローの説明：実行フェーズ

| ステップ | 説明 |
|---|---|
| 1 | 送信元 AMF（S-AMF）は、ハンドオーバー コマンドを送信元 NG-RAN（S-RAN）に送信します。<br>ハンドオーバーコマンドには、ターゲットから送信元への透過コンテナ、ハンドオーバーの準備段階中に T-RAN から受信した情報を含む N2 SM 情報でハンドオーバーされる PDU セッションのリスト、およびセットアップに失敗した PDU セッションのリストが含まれます。<br>SM 転送情報リストには、直接転送の T-RAN SM N3 転送情報リストまたは間接データ転送の S-UPF SM N3 転送情報リストが含まれます。<br>S-RAN は、PDU セッションのセットアップに失敗したリストと、示されている失敗の理由を使用して、N2 ハンドオーバー手順を続行するかどうかを判断します。 |
| 2 | S-RANはハンドオーバー コマンド（UE コンテナ）を UE に送信します。<br>UE コンテナは、ターゲットから送信元への透過コンテナのUE部分であり、AMF を介して T-RAN から S-RAN に透過的に送信され、S-RAN によってUEに提供されます。 |
| 2a ～ 2c | S-RAN は、アップリンク RAN ステータス転送メッセージをS-AMFに送信します。S-RANは、UEのいずれの無線ベアラーがパケット データ コンバージェンス プロトコル（PDCP）ステータスの維持で処理されない場合、このメッセージの送信を控えます。 |
| 3 | T-RANは、アップリンク パケットをT-UPFおよびUPF（PSA）に送信します。UPF（PSA）は、S-UPF を介して S-RAN にダウンリンク パケットを送信します。<br>S-RAN は、データ転送の対象となる QoS フローまたはデータ無線ベアラー（DRB）のために、T-RAN にダウンリンク データを転送します。データ転送パスは、直接（ステップ 3a）または間接転送（ステップ 3b）のいずれかです。 |
| 3a | 直接データ転送は、セッション レベルおよびDRB レベルのデータ転送によってサポートされます。 |
| 3b | 間接的なデータ転送も、セッション レベルおよび DRB レベルのデータ転送によってサポートされています。 |
| 4 | UE はターゲット セルと正常に同期した後、T-RAN にハンドオーバー確認メッセージを送信します。 |
| 5 | T-RANは、T-AMFにハンドオーバー通知メッセージを送信します。このメッセージは、ハンドオーバーが成功したことを示すために送信されます。 |

| ステップ | 説明 |
|---|---|
| 6a. | T-AMF は、Namef_Communication_N2InfoNotify を呼び出すことにより、T-RAN から受信した N2 ハンドオーバー通知について S-AMF に通知します。<br>S-AMF はタイマーを使用して S-RAN 内のリソースの解放を監視します。 |
| 6b | S-AMF は、Namef_Communication_N2InfoNotify ACK を T-AMF に送信して承認します。 |
| 6c | S-AMF は、Nsmf_PDUSession_ReleaseSMContext 要求を SMF に送信します。この要求には、SUPI、PDU セッション ID、および N2 SM 情報（セカンダリ RAT 使用状況データ）が含まれます。<br>T-AMF が PDU セッションを承認しない場合、S-AMF は N2 ハンドオーバー通知の受信後に PDU セッションのリリース手順をトリガーします。 |
| 7 | T-AMF は、Nsmf_PDUSession_UpdateSMContext 要求を SMF に送信します。この要求には、PDU セッション ID のハンドオーバー完了の表示、LADN サービス エリア内の UE プレゼンス、および N2 SM 情報（セカンダリ RAT 使用状況データ）が含まれます。<br>T-AMF は、各 PDU セッションごとに対応する SMF にハンドオーバー完了通知を送信して、N2 ハンドオーバーが成功したことを示します。 |
| 8a | 新しい T-UPF が挿入されるか、既存の中間 S-UPF が再割り当てされると、SMF は T-RAN の DL AN トンネル情報を示す N4 セッション変更要求を T-UPF に送信します。 |
| 8b | T-UPF は、N4 セッション変更応答メッセージを SMF に送信することで承認します。 |
| 9a | UPF が再割り当てされていない場合、SMF は、T-RAN の DL AN トンネル情報を示す N4 セッション変更要求を S-UPF に送信します。 |
| 9b | S-UPF は、N4 セッション変更応答メッセージを SMF に送信することで承認します。 |
| 10a | 非ローミングまたはローカル ブレークアウト ローミングのシナリオの場合、SMF は N4 セッション変更要求メッセージを PDU セッション アンカー UPF、UPF（PSA）に送信します。新しい T-UPF が挿入されるか、既存の中間 S-UPF が再割り当てされると、SMF は T-RAN の N3 AN トンネル情報 または T-UPF の DL CN トンネル情報 を提供します。<br>T-UPF が挿入されていないか、既存の中間 S-UPF が再割り当てされていない場合は、ステップ 10a とステップ 10b をスキップします。 |
| 10b | UPF（PSA）は、N4 セッション変更応答メッセージを SMF に送信します。<br>複数の UPF（PSA）がある場合は、各 UPF（PSA）に対してステップ 10a とステップ 10b を実行します。 |

| ステップ | 説明 |
|---|---|
| 11 | SMF は、Nsmf_PDUSession_UpdateSMContext 応答（PDU セッション ID）を T-AMF に送信します。SMF は Handover Complete の受信を確認します。 |
| 12 | UEは、*3GPP TS 23.502*で定義されているモビリティ登録の更新手順を開始します。 |
| 13a | 送信元中間 UPF がある場合、SMF は N4 セッション リリース要求（リリース原因）を送信元UPF に送信して、リソースの解放を開始します。このメッセージは、S-UPF の間接データ転送リソースを解放するためにも使用されます。 |
| 13b | S-UPF は N4 セッション リリース応答メッセージで確認応答し、リソースのリリースを確認します。<br>間接的なデータ転送の場合、間接的なデータ転送のリソースも解放されます。 |
| 14a | タイマーの期限切れ（手順 6a で定義）の後、AMF は UE コンテキスト リリース コマンドを送信します。 |
| 14b | 送信元 NG-RAN は、UE に関連するリソースを解放し、UE コンテキスト リリース完了 () メッセージで応答します。 |
| 15a | 間接転送が適用され、UPF が再割り当てされた場合、間接データ転送のタイマーが期限切れになった後、SMF は N4 セッション変更要求を T-UPF に送信します。その後、T-UPF は間接データ転送リソースを解放します。 |
| 15b | T-UPF は N4 セッション変更応答メッセージで承認し、間接データ転送リソースのリリースを確認します。 |

## 制限事項

UPF 再割り当てを使用した Xn ベースのハンドオーバーは、現在サポートされていません。

# OAM サポート

ここでは、この機能の操作、管理、およびメンテナンスに関して説明します。

## 統計情報サポート

「smf_ran_failed_flows」メトリックは、Xn および N2 ハンドオーバー手順を含むさまざまなコール フロー手順の一部として RAN によって解放された QoS フローの数を識別するために追加されています。

SMF は、Xn 引き継ぎを考慮して「xn_handover」ラベルを使用します。同様に、N2 ハンドオーバーの場合、SMF は「n2_handover」ラベルを使用します。

# Wi-Fi ハンドオーバー

## 機能説明

重要 この章で使用されている PGW-C という用語は、SMF でサポートされている EPS インターワーキング機能を意味しており、LTE ネットワークで使用されるスタンドアロン P-GW として想定してはなりません。

SMF＋PGW-C 製品は、Wi-Fi ハンドオーバーをサポートしています。クラウドベースのアーキテクチャにより、5GS または EPS での次の Wi-Fi ハンドオーバーと、non-3GPP の信頼できないアクセスがサポートされます。

- EPC から non-3GPP 信頼できない Wi-Fi ハンドオーバーへ
- Non-3GPP 信頼できない Wi-Fi から EPC ハンドオーバーへ
- EPS フォールバックによる非 3GPP 信頼できない Wi-Fi から 5GS へのハンドオーバー
- Non-3GPP 信頼できない Wi-Fi から 5GS ハンドオーバーへ
- 5GS から non-3GPP 信頼できない Wi-Fi ハンドオーバーへ

### ハンドオーバー説明サポート

SMF＋IWF は、セッションが存在しない場合でも、ハンドオーバー（HO）指示で受信したセッション作成要求を拒否します。このサポートは、4G および Wi-Fi セッションにのみ適用されます。

アクセスプロファイルの下にある **gtpc message-handling create-session-request ho-ind new-call-reject** CLI コマンドは、「Context Not Found」というメッセージと共に通話を拒否します。

詳細については、ハンドオーバー通知を伴うコールの構成（587ページ）を参照してください。

### Wi-Fi 向けの代替 RAT トンネルの作成

SMF は、Wi-Fi 接続手順中に代替 RAT トンネルを作成します。このトンネルは、サブスクライバが移行中に別の RAT に移動するときに再利用されます。

（注） 代替 RAT トンネルの作成は、PLMN 間ハンドオーバー サポートの前提条件です。

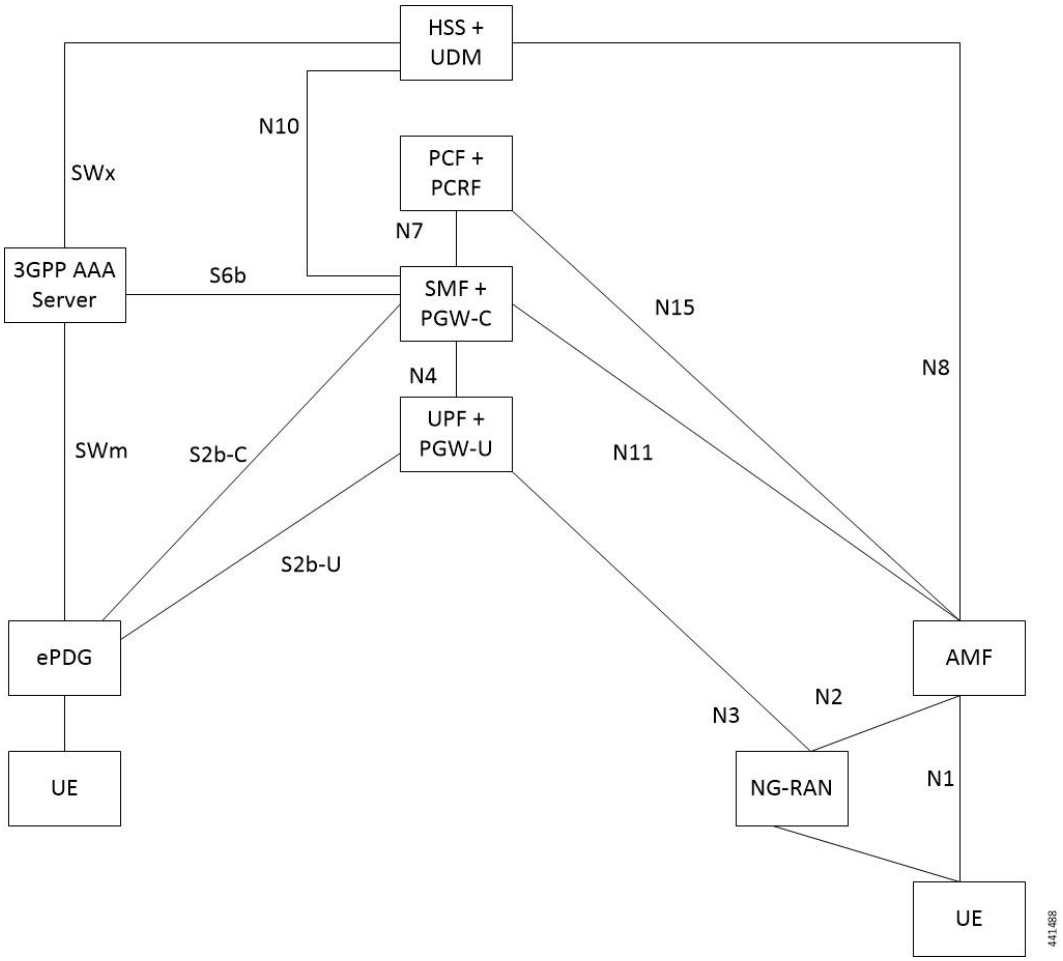
# アーキテクチャ

次のセクションでは、S5 および S2b インターフェイスを使用した ePDG または EPC と 5GS 間のインターワーキング、および EPS 内の非ローミング アーキテクチャについて説明します。

## ハンドオーバーのための ePDG と 5GS のインターワーキング

次の図は、ePDG または EPC と 5GS 間のインターワーキングの非ローミング アーキテクチャを示しています。

**図 *106 : ePDG* または *EPC* と *5GS* 間のインターワーキングの非ローミング アーキテクチャ**




ePDG と 5GS の間のインターワーキングは、N26 インターフェイスを使用しない EPC と 5GS 間のインターワーキングに似ています。このインターワーキングでは、IP アドレスの保存はシステム間モビリティの UE で行われます。HSS と UDM を介して PGW-C と SMF および対応する APN と DNN の情報を取得して保存すると、インターワーキングが可能になります。このようなネットワークでは、AMF は、5GC での初期登録時にN26 インターフェイスを使用しない UE とのインターワーキングもサポートします。AMF は、5GS の接続手順で N26 なしの UE とのインターワーキングをサポートする場合があります。非 3GPP 信頼できない Wi-Fi アクセスの場合、N26 インターフェイスが存在しないため、ePDG は AMF と通信しません。

5GS はネットワーク スライスをサポートし、その PLMN または他の PLMN で EPS とインターワーキングできます。SMF + PGW-C は、PGW-C FQDN および NSSAI 値を持つ各 UE に対して UDM 登録を実行します。この登録により、AMF または ePDG は、UE 承認が完了した後、サブスクリプション情報の一部として UDM または HSS から PGW-C の IP アドレスを識別します。

5GC から EPC へのモビリティによって、すべてのアクティブな PDU セッションを EPC に転送できるという保証はありません。EPC での PDN 接続の確立中に、UE は PDU セッション ID を割り当て、PCO を介して PGW-C + SMF に送信します。

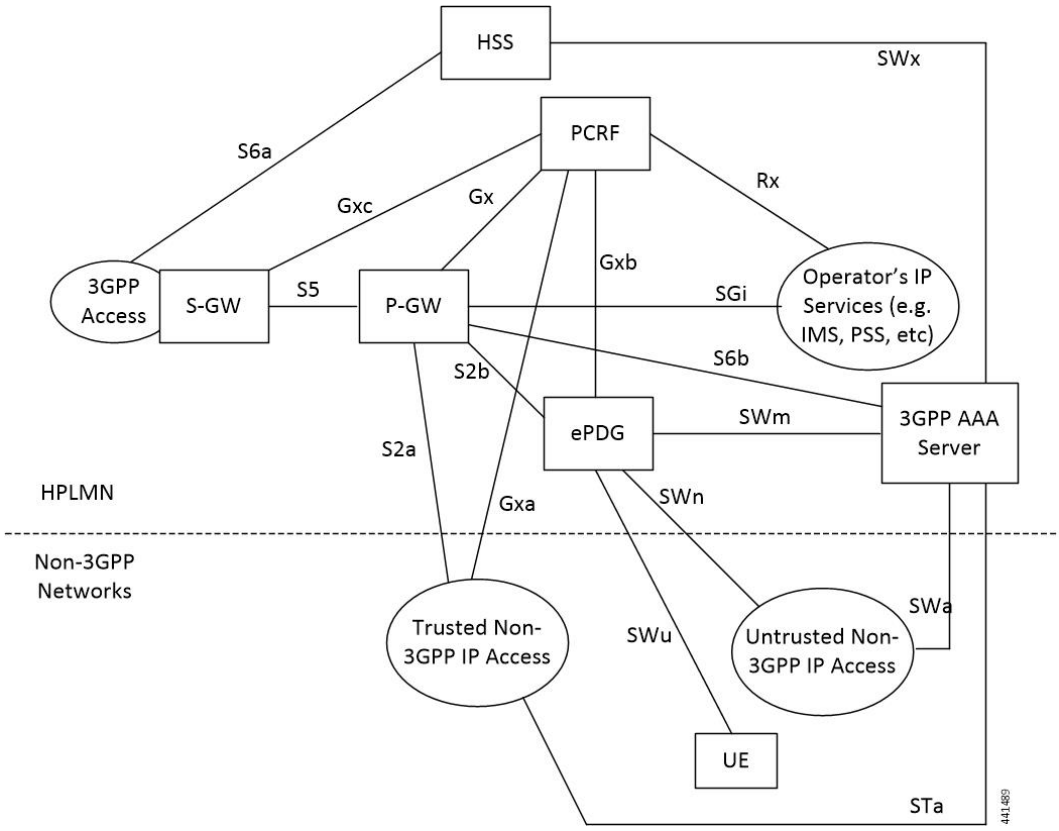
PDN 接続と関連付けられている S-NSSAI は、PGW-C+SMF によるオペレータ ポリシーに基づいて決定されます。たとえば、PGW-C + SMF アドレスと APN の組み合わせが、S-NSSAI が関連する PLMN ID とともに PCO の UE に送信されます。PGW-C+SMF が複数の S-NSSAI をサポートし、APN が複数の S-NSSAI に対して有効である場合、PGW-C+SMF は、UE の登録済み S-NSSAI にマッピングされている S-NSSAI のみを選択します。

UE は、PDN 接続に関連付けられている S-NSSAI および PLMN ID を保存します。UE は、受信した PLMN ID から要求された NSSAI を取得します。NAS 登録要求メッセージには、要求された NSSAI が含まれます。RRC は、UE が 5GC に登録するときに登録要求を伝送します。このシナリオは、UE が非ローミングであるか、またはローミング時に VPLMN に対して NSSAI を構成している場合に適用できます。

## ハンドオーバーのための EPS と ePDG のインターワーキング

次の図は、S5 と S2b インターフェイス使用して EPS 内の非ローミング アーキテクチャを示しています。

図 *107 : S5*、*S2a*、および *S2b* インターフェイスを使用した *EPS* 内の非ローミングアーキテクチャ




非 3GPP アクセスへの信頼できない Wi-Fi ハンドオーバーへの 3GPP アクセスと非 3GPP アクセスへの信頼できない Wi-Fi から 3GPP アクセスへのハンドオーバーで、UE が送信元アクセスの異なる APN への複数の PDN 接続を持ち、UE が異なる同時アクティブ URI をルーティングできる場合異なるアクセスネットワークを介した PDN 接続の場合、UE は、ハンドオーバー前にソース アクセスでアクティブだったすべての PDN 接続をソースからターゲットアクセスに転送するか、またはそれらのサブセットのみを転送できます。この転送では、同じ APN への複数の PDN 接続で 1 つのアクセスが制限される場合があります。

遷移プロセスは、次のシナリオで発生する可能性があります：

- 3GPP アクセスから非 3GPP アクセスへの信頼できない Wi-Fi ハンドオーバー
- 非 3GPP アクセス信頼できない Wi-Fi から 3GPP へのアクセスのハンドオーバー

UE は、次の条件が満たされている場合、ハンドオーバー前にソースアクセスでアクティブだったすべての PDN 接続をソースからターゲットアクセスに転送するか、またはそれらのサブセットのみを転送できます：

- UE に送信元アクセスの異なる APN への複数の PDN 接続がある
- UE は、異なるが同時にアクティブな PDN 接続を異なるアクセスネットワークでルーティングできます。

SMF は、エンドユーザーと ePDG の間の IPSec 接続が確立された後、ePDG を使用した S2b インターフェイスを介したエンドユーザーの信頼できない Wi-Fi アクセスをサポートします。

信頼できない Wi-Fi から EPC へのハンドオーバーの場合、SMF は UDM 登録中に PGW-C FQDN を提供し、サブスクリプション情報を取得します。

UE ハンドオーバー時に、MME は HSS から PGW-C FQDN をフェッチします。認証後、MME は引き継ぎを示す GTPv2 セッション作成要求を開始します。SMF + PGW-C は、ハンドオーバー要求の処理中に UDM 登録およびサブスクリプション手順を実行しません。SMF + PGW-C により、ハンドオーバーを示す GTPv2 MB 要求が送信され、信頼できない Wi-Fi から EPC へのデータ パス スイッチングが実行されます。

EPC から信頼できない Wi-Fi へのハンドオーバーの場合、HSS はサブスクライバの認証後に SMF + PGW-C FQDN を提供します。UE がハンドオーバーを実行する場合、認証後、HSS は SMF + PGW-C FQDN を提供します。ePDG は、IPSec トンネル確立後、PGW への引き継ぎを示す GTPv2 セッション作成要求を開始します。SMF + PGW-C は UDM 登録を実行し、引き継ぎ要求の処理中にサブスクリプション手順は存在しません。

## Wi-Fi ハンドオーバーの TFT 処理

4G および 5G の展開、3 者間での音声またはビデオのマルチパーティコール会議、および RCS メッセージの使用例では、PGW-C は UL と DL の両方向に対して 4 つ以上のフィルタ（最大 16 個のフィルタに対応）を持つことになります。SMF には、BearerContextList の GTPv2 CBReq または UBReq に含まれる「EPS ベアラ レベル トラフィック フロー テンプレート（Bearer TFT）」が含まれます。CBReq または UBReq は、ベアラーごとに最大 4 つの TFT を伝送します。

3 者間音声/ビデオおよびマルチパーティ コール会議の場合、PCF は、複数の「N7 ポリシー通知要求」メッセージに異なるサブスクライバ TFT を追加することで pccRules をプッシュしようとします。PGW-C は、GTPv2 CBReq または UBReq メッセージを開始することにより、専用ベアラーの確立で受信した「N7 更新通知要求」を処理します。SMF は、256 バイト（4 TFT）を超えないように、TFT で受信した SDF フィルタを調整します。

（注） PGW-C は、PCF「N7 ポリシー通知要求」から受信した 4TFT を超えるデータをサポートしません。

PCF は、「N7 Policy Notify Req」を送信することで、同じベアラーに対して複数の pccRules をプッシュし続け、その間、SMF はマルチパーティ コールの場合に 12 ～ 16 のフィルタを持つことになります。

サブスクライバが LTE から Wi-Fi または Wi-Fi から LTE または NR から Wi-Fi ハンドオーバーのコールモデルのケースに移行すると、SMF はまず、HO の一部としてデフォルトのベアラーの作成を確立します。SMF は次に、サブスクライバのベアラー コンテキスト リストの「EPS ベアラー レベル トラフィック フロー テンプレート（ベアラー TFT）」の 16 個のフィルタすべてに対応することで、専用ベアラ確立のために CBReq の送信を試みます。これらの制限のためにエンコードが失敗した場合、SMF は、HO タイプ、SGW、MME、または ePDG に基づ

いて、「EPS ベアラ レベル トラフィック フロー テンプレート（ベアラ TFT）」IE なしで CBReq を送信します。

SGW または ePDG から CBResp を受信した後、SMF はそれぞれの失敗したベアラーのポリシーまたは課金リソースを解放しないため、SMF と UPF でさらに古いエントリが発生し、そのサブスクライバの「EBI Mismatch - 408 Error Voice Call」によりシステムの不整合が発生します。Wi-Fi HOS の失敗）。

## 標準準拠

Wi-Fi ハンドオーバー機能は、以下の基準に準拠しています：

- 3GPP TS 23.502 V15.2.0（2018-09）
- 3GPP TS 23.402 V15.3.0（2018-03）
- 3GPP TS 29.214 V15.5.0（2018-03）

# 機能の仕組み

このセクションでは、Wi-Fi から LTE へのハンドオーバー、EPS フォールバックを使用した Wi-Fi ハンドオーバー、および Wi-Fi から 5GS へのハンドオーバーについて説明します。

## EPC から非 3GPP への信頼できない Wi-Fi ハンドオーバー コール フロー

このセクションでは、EPC から非 3GPP の信頼できない Wi-Fi ハンドオーバー コール フローについて説明します。

図 *108 : EPC* から非 *3GPP* への信頼できない *Wi-Fi* ハンドオーバー コール フロー

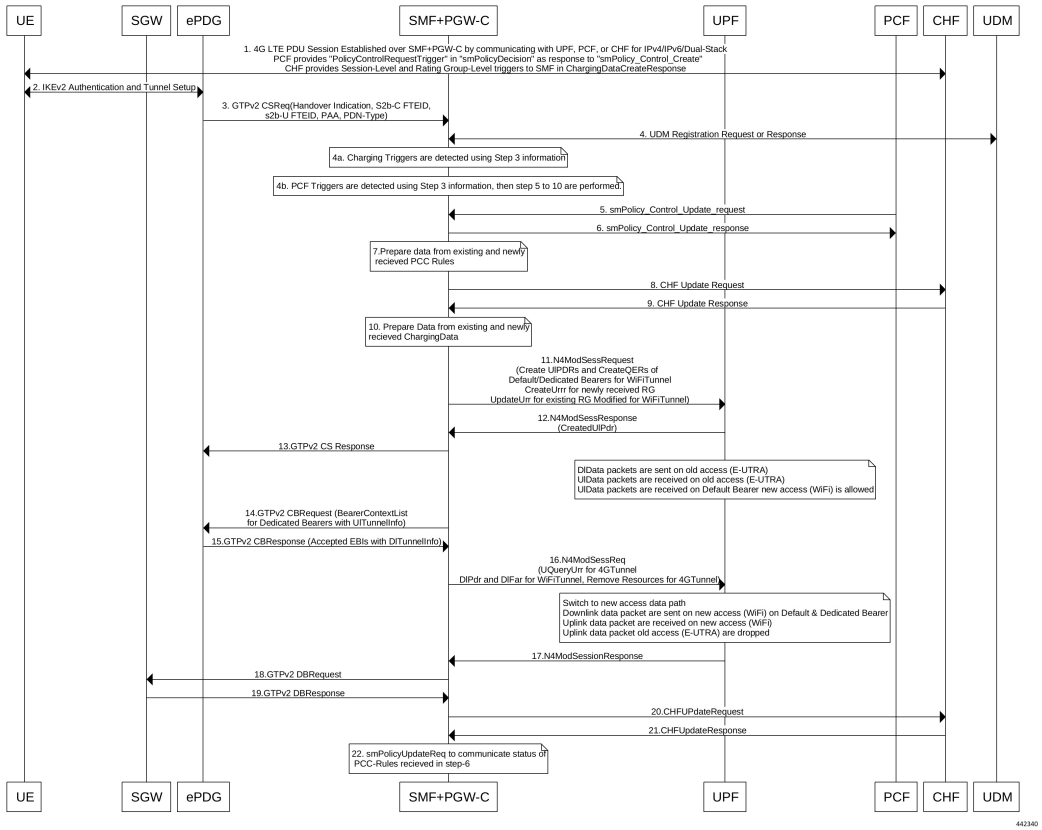



表 *180 : EPC* から非 *3GPP* への信頼できない *Wi-Fi* ハンドオーバー コール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | UE は 3GPP アクセス ネットワークに接続されています。<br><br>SMF + PGW-C は、IPv4、IPv6、またはデュアルスタックの UPF、PCF、および CHF と通信して、4G LTE PDU セッションを確立します。PCF は、SM ポリシー制御の作成に応答して、SM ポリシーの決定であるポリシー制御要求トリガーを送信します。CHF は、課金データ作成の応答で、SMF に対しセッション レベルまたは料金設定グループレベルのトリガーを提供します。 |
| 2 | UE は信頼できない非 3GPP アクセスに接続され、ePDG 選択プロセスで ePDG が選択されます。次に、UE は、3GPP TS 23.402（セクション 8.6.2.1）で定義されているハンドオーバー接続手順を開始します。UE と ePDG の間に IKE トンネルが確立され、UE が AAA サーバとの SWm インターフェイスを介して認証された後、UE は IKE 認証（IKE_AUTH）を開始します。IKE_AUTH には、EPC および P-CSCF と DNS のオプションで以前に割り当てられた IPv4 または IPv6 アドレスの構成パラメータが含まれます。 |

| ステップ | 説明 |
|---|---|
| 3 | ePDG はセッション作成要求を PGW-C に送信します。この要求には、次の詳細が含まれます。<br>• IMSI<br>• APN<br>• ハンドオーバー インジケータ<br>• RAT タイプ<br>• コントロール プレーンの ePDG TEID<br>• ユーザー プレーンの ePDG アドレス<br>• ユーザー プレーンの ePDG TEID<br>• EPS ベアラー ID<br>• ユーザーの現在地<br>RAT タイプは、非 3GPP アクセス テクノロジー タイプを示します。UE が IP アドレスの保持をサポートし、ポート アナライザ アダプタ（PAA）に含まれている場合、ePDG はセッション作成要求で引き継ぎの通知を構成し、PDN ゲートウェイが UE に割り当てられた同じ IP アドレスまたはプレフィックスを再割り当てできるようにします。 この IP アドレスまたはプレフィックスは、UE が 3GPP IP アクセスに接続され、PCF でポリシー変更手順を開始するときに割り当てられます。 |
| 4a | SMF は、UDM を使用して PGW-C FQDN を更新することにより、UDM 登録を実行します。<br>EPC とのセッション確立中に UDM 登録は行われません。 |
| 4b | SMF は、EPC セッションの確立中に受信した課金トリガーに対してステップ 3 で利用可能な情報を使用して、課金トリガーを検出します。 |
| 4c | SMF は、EPC セッション確立中に PCF との通信で受信した要求ポリシー制御トリガーに対してステップ 3 で利用可能な情報を使用して PCF トリガーを検出します。 |
| 5 | ステップ 4b で受信した検出されたアーム化されたポリシー制御トリガに基づいて、SMF は、ステップ 3 で検出されたアクセス パラメータを使用して PCF に SM ポリシー制御更新要求を送信します。 |
| 6 | PCF は、新しいまたは更新された PCC ルールを含み、SM ポリシー制御更新応答を送信します。更新応答には、SM ポリシー決定に関する情報が含まれています。 |
| 7 | ステップ 6 で受信した情報と EPC セッションの既存のポリシー データに基づいて、SMF は新しいまたは更新された PCC ルールの情報を準備します。 |

| ステップ | 説明 |
|---|---|
| 8 | クォータ情報を必要とする新しい料金設定グループを含む新しいPCCルールをステップ 6 で受信した場合、SMF は CHF に課金情報の更新要求を送信します。SMF には、PDU セッション情報の新しいアクセス パラメータも含まれます。 |
| 9 | CHF は、ステップ 8 で要求された料金設定グループのクォータ情報を含むマルチユニット情報とともに課金更新応答を SMF に送信します。CHF は、EPC セッションの既存の料金設定グループの新しいクォータ情報を送信することもできます。 |
| 10 | SMF は、CHF から課金更新応答として受信した情報を処理します。 |
| 11 | SMF は、Wi-Fi トンネルのために、N4 セッション変更要求を UPF に送信します。この要求には、アップリンク PDR の作成、QER の作成、受信した新しい料金設定グループ クォータ情報の URR の作成、および変更されたクォータ情報の URR の更新に関する詳細が含まれています。 |
| 12 | UPF は、N4 セッション変更応答として作成された PDR 内にある UL トンネル情報を SMF に送信します。 |
| 13 | SMF は GTPv2 セッション作成応答を S-GW に送信します。この応答では、承認された要求または部分的に承認された要求、PGW-C S2b F-TEID、PAA、APN-AMBR、ベアラー コンテキストの作成、課金ゲートウェイ アドレス、および APCO に関する詳細を示します。 |
| 14 | SMF は、S-GW に GTPv2 ベアラー作成要求を送信します。この要求には、作成されるエンドユーザーへの DL トンネル情報を含むベアラー コンテキスト リストに関する情報が含まれています。 |
| 15 | S-GW は SMF に GTPv2 ベアラー作成応答を送信します。応答には、承認された要求または部分的に承認された要求の詳細と、ベアラー コンテキストが含まれます。 |
| 16 | SMF はベアラー応答の作成を処理し、確立されたベアラーの DL トンネル情報と失敗した EBI リスト（ある場合）を取得します。SMF は、Wi-Fi トンネルのために、N4 セッション変更要求を UPF に送信します。この要求では、各ベアラーの DL トンネル情報、RAT 変更情報を使用して DL PDR および DL FAR を作成し、4G トンネルのリソースを削除します。SMF は、受信した失敗した EBI リストまたは失敗した QFI リストの Wi-Fi トンネルの N4 リソースも削除します。 |
| 17 | UPF は、N4 セッション変更応答として使用状況レポートを SMF に送信します。 |
| 18 | SMF + PGW-C は、S-GW に GTPv2 DB 要求を送信します。この要求には、EBI または EBI のリストが含まれます。 |
| 19 | S-GW は SMF + PGW-C に GTPv2 DB 応答を送信します。 |
| 20 | SMF は、課金更新要求を CHF に送信します。この要求には、ステップ 8 で受信した新しいアクセスパラメータと使用状況レポートの詳細を含む複数使用状況レポートを含む PDU セッション情報が含まれています。 |

| ステップ | 説明 |
|---|---|
| 21 | CHFは、SMFに課金更新応答としてマルチユニット情報を送信します。マルチユニット情報には、既存の料金設定グループの新しいクォータ情報が含まれている場合があります。 |
| 22 | SMFは、SMポリシー制御の更新要求をUPFに送信します。このリクエストには、ベアラー応答の作成の一部として AMF から受信した失敗した QFI リストの新しいアクセス パラメータとルール レポートが含まれています。<br>PCF は、SM ポリシー制御更新応答として SM ポリシー決定を送信します。<br>SMF は SM ポリシー決定を処理し、3GPP 23.502、セクション 4.3.3.2 で定義されている PCF 開始変更手順として処理します。 |

（注） 上記のコール フローは 3GPP 仕様に基づいており、Cisco の実装には独自の最適化が施されています。詳細については、シスコのアカウント担当者にお問い合わせください。

## 非 3GPP 信頼できない Wi-Fi から EPC へのハンドオーバー コール フロー

このセクションでは、非 3GPP の信頼できない Wi-Fi から EPC ハンドオーバー コール フローへのについて説明します。

図 *109* : 非 *3GPP* 信頼できない *Wi-Fi* から *EPC* へのハンドオーバー コール フロー

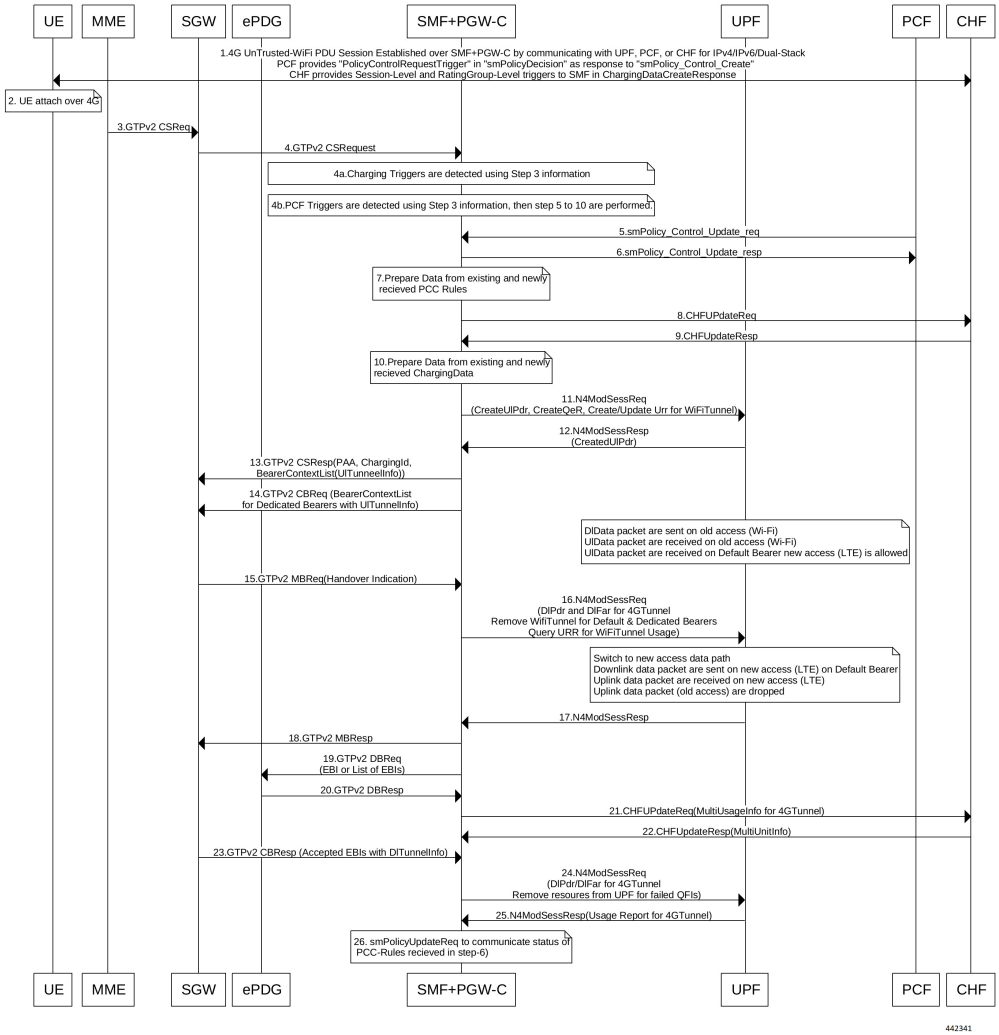



表 *181* : 非 *3GPP* 信頼できない *Wi-Fi* から *EPC* へのハンドオーバーコール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | 信頼できない非 3GPP アクセスを介して UE と ePDG 間で 1 つ以上の PDU セッションが確立されます。UE の 5G NAS 機能により、ePDG は PGW + SMF を組み合わせて選択します。UE が PDU セッション ID を PGW+SMF に送信します。 |

| ステップ | 説明 |
|---|---|
| 2 | UE は E-UTRAN アクセスを検出し、現在使用されている非 3GPP アクセス システムから E-UTRAN にセッションを引き継ぎます。3GPP アクセス システムの UE 検出の詳細については、3GPP TS 23.401、セクション 4.8 を参照してください。<br><br>UE はハンドオーバー接続要求タイプのアタッチ要求を MME に送信します。E-UTRAN は、3GPP TS 23.401 で定義されているように、UE から受信したメッセージを MME にルーティングします。UE には、送信元の非 3GPP アクセスの PDN 接続に対応する APN の 1 つが含まれます。APN は、3GPP TS 23.401 で定義されているように提供されます。 |
| 3 | MME と HSS が認証を実行します。次に、位置情報の更新手順とサブスクライバデータの取得によって APN 情報を受信します。<br><br>MME は、3GPP TS 23.401 で定義されているように APN、SGW、および PDN ゲートウェイを選択します。MME がセッション作成要求メッセージを SGW に送信します。この要求には、IMSI、MME コンテキスト ID、PDN-GW アドレス、「ハンドオーバー」要求タイプのハンドオーバー指示、および APN に関する情報が含まれます。 |
| 4 | SGW は、3GPP TS 23.401 で説明されているように、HPLMN の PDN-GW にセッション作成要求（ハンドオーバー通知）メッセージを送信します。MME はセッション要求作成メッセージにハンドオーバー指示情報を含めるため、SGW は GTPv2 セッション要求メッセージを PDN GW に送信します。このメッセージには、IMSI の詳細、APN、ハンドオーバーの表示、RAT タイプ、ユーザー プレーンの S5-C TEID、S5-U TEID、EBI、およびユーザー ロケーション情報に関する詳細が含まれます。RAT タイプは、3GPP IP アクセス E-UTRAN テクノロジー タイプを示します。UE が IP アドレスの保存をサポートしており、PAA に含まれている場合、SGW はセッション作成要求でハンドオーバー通知を構成します。この構成では、PDN GW は、UE が 3GPP IP アクセスに接続している間に UE に割り当てられていたのと同じ IP アドレスまたはプレフィックスを再割り当てします。この構成では、SGW は PCF に対してポリシー変更手順を開始します。<br><br>ハンドオーバー通知に含まれているため、PDN GW は、この時点で非 3GPP IP アクセスから 3GPP アクセス システムにトンネルを切り替えることはありません。<br><br>登録は Wi-Fi セッションの確立中に行われるため、SMF は UDM 登録を実行しません。 |
| 4a | SMF は、EPC セッションの確立中に受信した課金トリガに対してステップ 3 で利用可能な情報を使用して、課金トリガを検出します。 |
| 4b | SMF は、EPC セッション確立中に PCF との通信で受信した要求ポリシー制御トリガに対してステップ 3 で利用可能な情報を使用して PCF トリガを検出します。 |
| 5 | ステップ 4b で受信した検出されたアーム化されたポリシー制御トリガに基づいて、SMF は、ステップ 3 で検出されたアクセス パラメータを使用して PCF に SM ポリシー制御更新要求を送信します。 |

| ステップ | 説明 |
|---|---|
| 6 | PCF は、新規または更新された PCC ルールを含めることによって、SM ポリシーの決定である SM ポリシー制御更新応答を送信します。 |
| 7 | ステップ 6 で受信した情報と EPC セッションの既存のポリシー データに基づいて、SMF は新しいまたは更新された PCC ルールの情報を準備します。 |
| 8 | SMF はステップ 6 で新しい PCC ルールを受信した場合、課金更新要求を、クォータ情報を持つ新しい料金設定グループとともに CHF に送信します。この要求には、新しいアクセス パラメータを含む PDU セッション情報が含まれています。 |
| 9 | CHF は、SMF に課金更新応答としてマルチユニット情報を送信します。マルチユニット情報には、料金設定グループの新しいクォータ情報と、EPC セッションの既存の料金設定グループ（存在する場合）が含まれます。 |
| 10 | SMF は、CHF が送信した受信済みの課金更新応答の課金データを準備します。 |
| 11 | SMF は、N4 セッション変更要求を UPF に送信します。この要求には、UL および DL PDR の作成、QER の作成、受信した新しい料金設定グループ クォータ情報の URR の作成、変更されたクォータ情報の更新された URR、および FAR の作成に関する詳細が含まれています。 |
| 12 | UPF は、SMF への N4 セッション変更応答として、作成された PDR 内の UL トンネル情報を送信します。 |
| 13 | SMF は GTPv2 セッション作成応答を S-GW に送信します。この応答では、承認された要求または部分的に承認された要求、PGW-C S2b F-TEID、PAA、APN-AMBR、ベアラー コンテキストの作成、課金ゲートウェイ アドレス、および APCO に関する詳細を示します。 |
| 14 | SGW は、Wi-Fi トンネルから 4G トンネルへのデータ パス切り替えについて、ハンドオーバー通知を含む変更ベアラー要求を PGW に送信します。 |
| 15 | PGW は N4 セッション変更要求を送信して、Wi-Fi トンネルを削除し、ステップ 4 の 4G トンネルの GTPv2 セッション要求の作成で受信した DL トンネル情報を設定します。 |
| 16 | UPF が SMF に N4 セッション変更応答を送信します。 |
| 17 | SMF は、ベアラー コンテキスト リストを含む GTPv2 セッション作成要求を SGW に送信します。このリストには、エンドユーザー向けの DL トンネル情報が含まれています。 |
| 18 | SGW は GTPv2 セッション作成応答を SMF に送信します。この応答には、承認された要求または部分的に承認された要求の詳細と、ベアラー コンテキストが含まれます。 |
| 19 | ePDG は GTPv2 ベアラー要求の作成を送信します（DL トンネル情報を持つ EBI を SMF に |

| ステップ | 説明 |
|---|---|
| 20 | SMF はベアラー応答の作成を処理し、確立されたベアラーの DL トンネル情報と失敗した EBI リスト（ある場合）を取得します。SMF は、Wi-Fi トンネルのために、N4 セッション変更要求を UPF に送信します。この要求は、DL トンネル情報、RAT 変更情報を使用して DL FAR を更新し、4G トンネルのリソースを削除することです。SMF は、受信した失敗した EBI リストまたは失敗した QFI リストの Wi-Fi トンネルの N4 リソースも削除します。 |
| 21 | UPF は、使用状況レポートを含む N4 セッション変更応答を SMF に送信します。 |
| 22 | SMF は、課金更新要求を CHF に送信します。この要求には、新しいアクセス パラメータを含む PDU セッション情報と、ステップ 8 で受信した使用状況レポートで構成される複数使用状況レポートが含まれています。 |
| 23 | CHF は、既存の料金設定グループのクォータ情報を含むマルチユニット情報とともに、課金更新応答を SMF に送信します。 |
| 24 | SMF + PGW-C は、EBI または EBI リストを含めることで、SGW への GTPv2 DB 要求を開始します。 |
| 25 | SGW は、SMF + PGW-C に対して GTPv2 DB 応答を送信します。 |
| 26 | SMF は、SM ポリシー制御の更新要求を UPF に送信します。このリクエストには、ベアラー応答の作成の一部として AMF から受信した失敗した QFI リストの新しいアクセス パラメータとルール レポートが含まれています。<br>PCF は、SM ポリシー制御更新応答として SM ポリシー決定を送信します。<br>SMF は SM ポリシー決定を処理し、3GPP 23.502 セクション 4.3.3.2 で定義されている PCF 開始変更手順として処理します。 |

（注） 上記のコール フローは 3GPP 仕様に基づいており、Cisco の実装には独自の最適化が施されています。詳細については、シスコのアカウント担当者にお問い合わせください。

## EPS フォールバック コール フローによる非 3GPP 信頼できない Wi-Fi から 5GS へのハンドオーバー

このセクションでは、非 3GPP の信頼できない Wi-Fi から 5GS ハンドオーバー EPS フォールバック コール フローへのについて説明します。

図 *110 : EPS* フォールバック コール フローによる非 *3GPP* 信頼できない *Wi-Fi* から *5GS* へのハンドオーバー

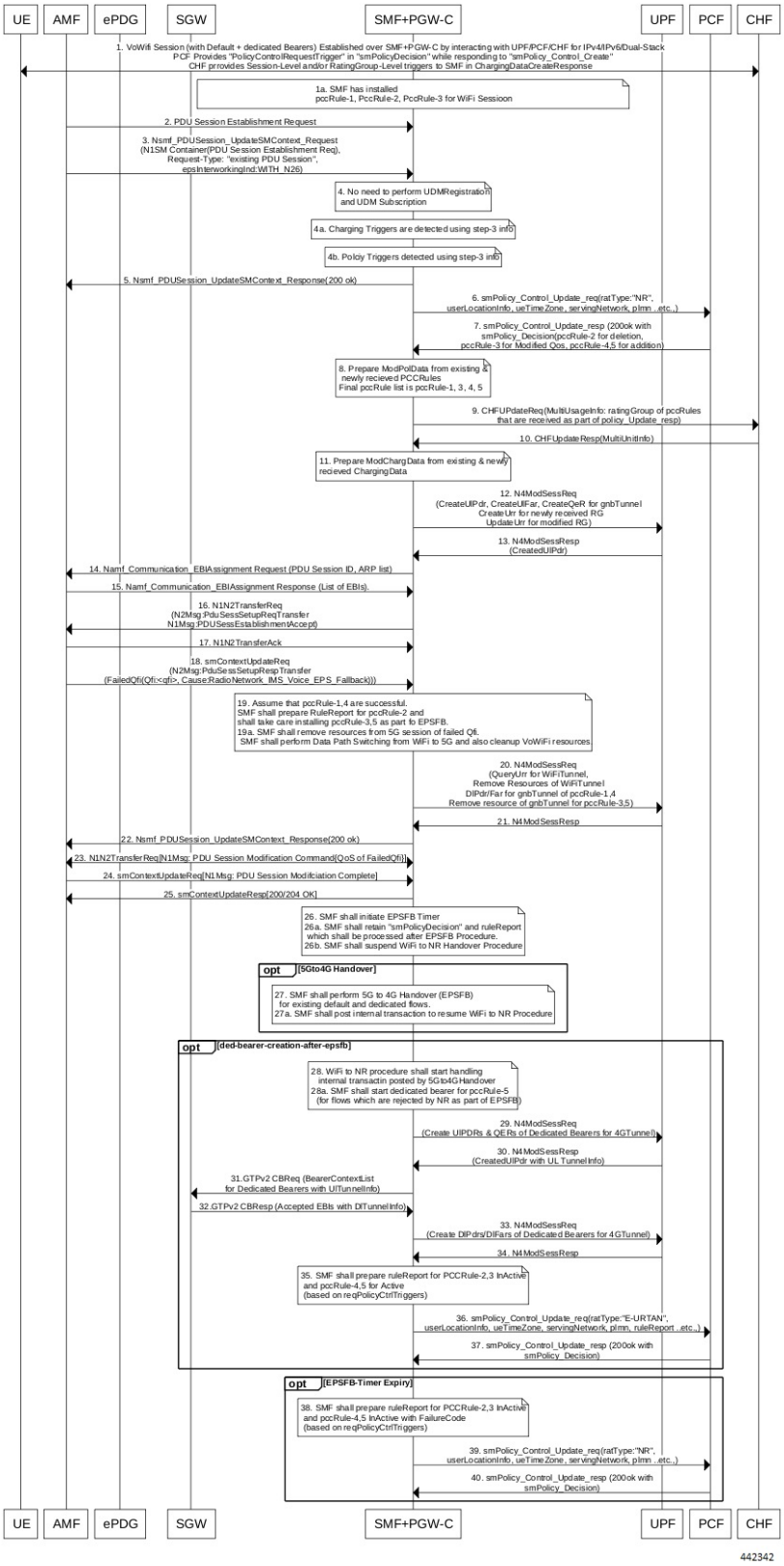

UE
AMF
ePDG
SGW
SMF+PGW-C
UPF
PCF
CHF
1. VoWifi Session (with Default + dedicated Bearers) Established over SMF+PGW-C by interacting with UPF/PCF/CHF for IPv4/IPv6/Dual-Stack
PCF Provides "PolicyControlRequestTrigger" in "smPolicyDecision" while responding to "smPolicy_Control_Create"
CHF provides Session-Level and/or RatingGroup-Level triggers to SMF in ChargingDataCreateResponse
1a. SMF has installed
pccRule-1, PccRule-2, PccRule-3 for WiFi Sessioon
2. PDU Session Establishment Request
3. Nsmf_PDUSession_UpdateSMContext_Request
(N1SM Container(PDU Session Establishment Req),
Request-Type: "existing PDU Session",
epsInterworkingInd:WITH_N26)
4. No need to perform UDMRegistration
and UDM Subscription
4a. Charging Triggers are detected using step-3 info
4b. Policy Triggers detected using step-3 info
5. Nsmf_PDUSession_UpdateSMContext_Response(200 ok)
6. smPolicy_Control_Update_req(ratType:"NR",
userLocationInfo, ueTimeZone, servingNetwork, plmn ..etc..)
7. smPolicy_Control_Update_resp (200ok with
smPolicy_Decision(pccRule-2 for deletion,
pccRule-3 for Modified Qos, pccRule-4,5 for addition)
8. Prepare ModPolData from existing &
newly recieved PCCRules
Final pccRule list is pccRule-1, 3, 4, 5
9. CHFUPdateReq(MultiUsageInfo: ratingGroup of pccRules
that are received as part of policy_Update_resp)
10. CHFUpdateResp(MultiUnitInfo)
11. Prepare ModChargData from existing & newly
recieved ChargingData
12. N4ModSessReq
(CreateUlPdr, CreateUlFar, CreateQeR for gnbTunnel
CreateUrr for newly received RG
UpdateUrr for modified RG)
13. N4ModSessResp
(CreatedUlPdr)
14. Namf_Communication_EBIAssignment Request (PDU Session ID, ARP list)
15. Namf_Communication_EBIAssignment Response (List of EBIs).
16. N1N2TransferReq
(N2Msg:PduSessSetupReqTransfer
N1Msg:PDUSessEstablishmentAccept)
17. N1N2TransferAck
18. smContextUpdateReq
(N2Msg:PduSessSetupRespTransfer
(FailedQfi(Qfi:<qfi>, Cause:RadioNetwork_IMS_Voice_EPS_Fallback)))
19. Assume that pccRule-1,4 are successful.
SMF shall prepare RuleReport for pccRule-2 and
shall take care installing pccRule-3,5 as part to EPSFB.
19a. SMF shall remove resources from 5G session of failed Qfi.
SMF shall perform Data Path Switching from WiFi to 5G and also cleanup VoWiFi resources
20. N4ModSessReq
(QueryUrr for WiFiTunnel,
Remove Resources of WiFiTunnel
DlPdr/Far for gnbTunnel of pccRule-1,4
Remove resource of gnbTunnel for pccRule-3,5)
21. N4ModSessResp
22. Nsmf_PDUSession_UpdateSMContext_Response(200 ok)
23. N1N2TransferReq(N1Msg: PDU Session Modification Command(QoS of FailedQfi))
24. smContextUpdateReq(N1Msg: PDU Session Modificiation Complete)
25. smContextUpdateResp(200/204 OK)
26. SMF shall initiate EPSFB Timer
26a. SMF shall retain "smPolicyDecision" and ruleReport
which shall be processed after EPSFB Procedure.
26b. SMF shall suspend WiFi to NR Handover Procedure
opt
[5Gto4G Handover]
27. SMF shall perform 5G to 4G Handover (EPSFB)
for existing default and dedicated flows.
27a. SMF shall post internal transaction to resume WiFi to NR Procedure
opt
[ded-bearer-creation-after-epsfb]
28. WiFi to NR procedure shall start handling
internal transactin posted by 5Gto4GHandover
28a. SMF shall start dedicated bearer for pccRule-5
(for flows which are rejected by NR as part of EPSFB)
29. N4ModSessReq
(Create UlPDRs & QERs of Dedicated Bearers for 4GTunnel)
30. N4ModSessResp
(CreatedUlPdr with UL TunnelInfo)
31.GTPv2 CBReq (BearerContextList
for Dedicated Bearers with UlTunnelInfo)
32.GTPv2 CBResp (Accepted EBIs with DlTunnelInfo)
33. N4ModSessReq
(Create DlPdrs/DlFars of Dedicated Bearers for 4GTunnel)
34. N4ModSessResp
35. SMF shall prepare ruleReport for PCCRule-2,3 InActive
and pccRule-4,5 for Active
(based on reqPolicyCtrlTriggers)
36. smPolicy_Control_Update_req(ratType:"E-URTAN",
userLocationInfo, ueTimeZone, servingNetwork, plmn, ruleReport ..etc..)
37. smPolicy_Control_Update_resp (200ok with
smPolicy_Decision)
opt
[EPSFB-Timer Expiry]
38. SMF shall prepare ruleReport for PCCRule-2,3 InActive
and pccRule-4,5 InActive with FailureCode
(based on reqPolicyCtrlTriggers)
39. smPolicy_Control_Update_req(ratType:"NR",
userLocationInfo, ueTimeZone, servingNetwork, plmn ..etc..)
40. smPolicy_Control_Update_resp (200ok with
smPolicy_Decision)
442342

表 *182 : EPS* フォールバック コール フロー詳細による非 *3GPP* 信頼できない *Wi-Fi* から *5GS* へのハンドオーバー

| ステップ | 説明 |
|---|---|
| 1 | UE と ePDG は、信頼できない非 3GPP アクセスを介して相互に通信し、1 つまたは複数の PDU セッションを確立します。UE の 5G NAS 機能により、ePDG は PGW-C と SMF を組み合わせて選択します。UE が PDU セッション ID を PGW と SMF の組み合わせに送信します。 |
| 1a | SMF は Wi-Fi セッションの PccRule-1、PccRule-2、PccRule-3 をインストールします。 |
| 2 | AMF は、SMF への 3GPP アクセス を通して PDU セッション確立要求を送信します。この要求には、次に関する詳細が含まれます：<br>• PDU セッション ID<br>• 要求された PDU セッション タイプ<br>• 要求された SSC モード<br>• 5GSM 機能 PCO<br>• SM PDU DN 要求コンテナ<br>• パケット フィルタ数<br>• オプションの要求常時 PDU セッション<br>既存 PDU セッション付きのリクエスト タイプは、3GPP アクセスと non-3GPP アクセスの間をスイッチまたは、EPC 内で既存の PDN 接続からの PDU セッション ハンドオーバーを示します。 |

| ステップ | 説明 |
| --- | --- |
| 3 | |

| ステップ | 説明 |
| --- | --- |
| | 要求タイプが「既存の PDU セッション」の場合、AMF は UDM から受信した SMF-ID に基づいて SMF を選択します。<br>この要求タイプでは、次の条件のいずれかを満たす場合にエラーが発生します。<br>• AMF が、登録中に AMF が UDM から受信した PDU セッション ID またはサブスクリプション コンテキストを識別しない場合。<br>• サブスクリプション プロファイルの更新通知手順に PDU セッション ID に対応する SMF ID が含まれていない場合。<br>次に、AMF は PDU セッション用に保存されているアクセスタイプを更新します。<br>既存の PDU セッションを持つ要求タイプが 3GPP アクセスと非 3GPP アクセスの間を移動する PDU セッションを参照しており、PDU セッションの S-NSSAI がターゲット アクセス タイプの許可された NSSAI で使用可能な場合、PDU セッション確立手順は、PDU セッション ID に対応する SMF ID および AMF が同じ PLMN の一部である場合に開始されます。<br>AMF は、要求タイプが「既存の PDU セッション」の NSMF PDU セッション作成 SM コンテキスト要求を SMF に送信します。この要求には、次の情報が含まれます：<br>• SUPI<br>• DNN<br>• S-NSSAI<br>• PDU セッション ID<br>• AMF ID<br>• リクエストタイプ<br>• PCF ID<br>• ベータ版への優先アクセス<br>• PDU セッション確立要求を含む N1 SM コンテナ<br>• ユーザー ロケーション情報<br>• アクセスタイプ<br>• PEI<br>• GPSI<br>• PDU セッション ステータス通知のサブスクリプション<br>• DNN 選択モード |

| ステップ | 説明 |
|---|---|
| | SMF は、SUPI + PDU セッション ID を使用して、PDU セッション確立要求からの既存の PDU セッションを分析します。SMF は受信した UE の IPv4 または IPv6 アドレスを取得した PDU セッションの IPv4 または IPv6 アドレスと比較します。セッションが取得されない場合、または IPv4 アドレスまたは IPv6 アドレスが一致しない場合、SMF は要求を拒否します。 |
| 4 | SMF は、WiFi セッションの確立中にすでに UDM に登録されているため、UDM 登録を実行しません。 |
| 4a | SMF は、WiFi セッションに受信した課金トリガーに対してステップ 3 で利用可能な情報を使用して、課金トリガーを検出します。 |
| 4b | SMF は、Wi-Fi セッション中に PCF との以前の通信で受信した要求ポリシー制御トリガーに対してステップ 3 で利用可能な情報を使用して PCF トリガーを検出します。 |
| 5 | SMF は、NSMF PDU セッション 作成 SM コンテキスト応答を AMF に送信します。この応答には、原因、SM コンテキスト ID、または PDU セッション拒否の原因を含む N1 SM コンテナが含まれます。 |
| 6 | ステップ 4a で受信した検出されたアーム化されたポリシー制御トリガに基づいて、SMF は、ステップ 3 で検出されたアクセス パラメータを使用して PCF に SM ポリシー制御更新要求を送信します。 |
| 7 | PCF は、新しいまたは更新された PCC ルールを含めて SM ポリシー制御更新応答を通して SM ポリシー判断を送信します。 |
| 8 | SMF は、ステップ 7 で受信した情報と Wi-Fi セッションの既存のポリシー データに基づいて、ModPolData を準備します。 |
| 9 | SMF はステップ 7 で新しい PCC ルールを受信した場合、課金更新要求を、クォータ情報の新しい料金設定グループを持つ CHF に送信します。この要求には、新しいアクセス パラメータを含む PDU セッション情報が含まれています。 |
| 10 | CHF は、SMF に課金更新応答としてマルチユニット情報を送信します。マルチユニット情報には、料金設定グループのクォータ情報と、Wi-Fi セッションの既存のステップ 9 で受信した料金設定グループが含まれます。 |
| 11 | SMF は、CHF から課金更新の応答内で受信した ModChargingData を処理します。 |

| ステップ | 説明 |
|---|---|
| 12 | SMF は、gNBトンネルのために、N4 セッション変更要求を UPF に送信します。この要求には、次に関する詳細が含まれます：<br>• アップリンク PDR を作成します。<br>• QER を作成。<br>• URRの作成（新しい料金設定グループ クォータ情報用）<br>• URR の更新（変更されたクォータ情報用）<br>• FAR の作成 |
| 13 | UPF は、SMF への N4 セッション変更応答として、作成された PDR 内の UL トンネル情報を送信します。 |
| 14 | SMF は EBI 割り当て要求を AMF に送信します。このリクエストは、PDU セッション ID の ARP リストを含みます。 |
| 15 | AMF は、SMF に EBI Assignment 応答として EBI のリストを送信します。 |
| 16 | SMF は、N1 N2 転送要求を AMF に送信します。この要求には、サポートされている QFI リストと gNB トンネルの UL トンネル情報を含む「PDU セッション リソース セットアップ要求転送」として N2 メッセージが含まれています。このリクエストは、承認済み QoS ルール、承認済み QoS 詳細、EPCO、PDN アドレス、およびセッション AMBR 値として「PDU セッション確立承認」として N1 メッセージを含みます。 |
| 17 | AMF は、N1 N2 Transfer 確認応答を SMF に送信します。 |
| 18 | AMF は、SM コンテキスト更新要求を SMF に次のいずれかで送信します：<br>• 「PDU セッション技術セットアップ失敗転送」N2 メッセージに「IMS 音声 EPS フォールバックまたは、RAT フォールバックがトリガーされました」の原因が表示されます。<br>• 「QoS Flow Flow Flow Setup List」の原因「PDU Session Resource Setup Response Transfer」で「IMS voice EPS fallback or RAT fallback triggered」のような原因が表示されます。 |
| 19 | pccRule-1 と pccRule-4 が成功したとの前提で、SMF は pccRule-2 のルール レポートを準備し、pccRule-3 と pccRule-5 を EPS フォールバックの一部としてインストールします。 |
| 19a | SMF は、失敗した QFI の 5G セッション、および VoWiFi リソースからリソースを削除します。さらに、SMF は Wi-Fi から 5G へのデータパスの切り替えを実行します。 |

| ステップ | 説明 |
|---|---|
| 20 | SMF は、次の操作を実行して、N4 セッション変更要求を UPF に送信します。<br>• WiFiTunnel の QueryUrr<br>• Wi-Fi トンネルのリソースを削除します。<br>• pccRule-1 および pccRule-4 の gNB トンネル用に DlPdr/Far を作成します。<br>• pccRule-3 および pccRule-5 の失敗した QFI の gNB トンネルのリソースを削除します。 |
| 21 | UPF は、Wi-Fi セッションの使用状況レポートとともに N4 セッション変更応答を SMF に送信します。 |
| 22 | SMF は、SM コンテキスト更新応答を AMF に送信します。 |
| （注）<br>SMF は、失敗した QFI がある場合、ステップ 23 からステップ 25 を実行します。 | |
| 23 | SMF は N1Msg：PDU セッション変更コマンド（FailedQfi の QoS）で N1 N2 転送要求を開始します。SMF は AMF から N1 N2 転送応答を受信します。 |
| 24 | SMF は AMF から N1Msg: PDU Session Modification Complete を含む SM コンテキスト更新要求を受信します。 |
| 25 | SMF は、SM コンテキスト更新応答内の 204 OK を AMF に送信します。 |
| 26 | SMF は、EPS フォールバック手順後に処理される「smPolicyDecision」と ruleReport を保持することにより、EPS フォールバック タイマーを開始します。また、SMF は、EPS フォールバック手順が実行されるか、EPS フォールバック タイマーが期限切れになるまで、WiFi から NR へのハンドオーバー手順を一時停止します。 |
| 27 | SMF は、既存のデフォルトフローと専用フローに対して 5G から 4G へのハンドオーバー（EPS フォールバック）を実行します。SMF は、内部トランザクションをポストして Wi-Fi から NR への手順を再開します。 |
| 28 | WiFi から NR への手順により、内部トランザクションの処理が開始されます。 |
| 28a | SMF は、pccRule-5（EPS フォールバックの一部として NR によって拒否されたフロー用）の専用ベアラ作成手順を開始します。 |
| 29 | SMF は、pccRules の Create UlPDR、QER、URR（存在する場合）を使用して N4 変更要求を開始します。これらは、EPS フォールバックの理由による Wi-Fi から NR へのハンドオーバーの一部として拒否されます。 |

| ステップ | 説明 |
|---|---|
| 30 | SMF は、専用ベアラーのアップリンク トンネル情報を含む CreatedUlPDR を使用して N4 変更応答を受信します。 |
| 31 | SMF は GTPv2 コンテキスト ベアラー要求（アップリンク トンネル情報を持つ専用ベアラのベアラー コンテキスト リスト）を開始します。 |
| 32 | SMF が GTPv2 コンテキスト ベアラー応答（承認された EBI とダウンリンク トンネル情報）を受信します。 |
| 33 | SMF は、UPF に向けて N4 変更セッション要求（4G トンネルの専用ベアラーの DlPdrs/DlFars の作成）を開始します。 |
| 34 | SMF は、UPF から N4 変更セッション応答を受信します。 |
| 35 | SMF は、要求ポリシー制御トリガーに基づいて、PCCRule-2、3 InActive および pccRule-4、5 for Active の ruleReport を準備します。 |
| 36 | SMF は、ratType:"E-URTAN"、userLocationInfo、ueTimeZone、servingNetwork、plmn、ruleReport などを含む SM ポリシー制御更新要求を送信します。 |
| 37 | SMF は、SM Policy Control Update 応答で SM Policy Decision で 200 OK を受信します。 |
| （注）<br>SMF は、ステップ 27 からステップ 37 が実行されない場合、つまり EPS フォールバック手順がトリガーされない場合にのみ、ステップ 38 ーステップ 40 を実行します。 | |
| 38 | SMF は、要求ポリシー制御トリガーに基づいて、FailureCode を持つ PCCRule-2、3 InActive および pccRule-4、5 InActive の ruleReport を作成します。 |
| 39 | SMF は、ratType:"NR"、userLocationInfo、ueTimeZone、servingNetwork、PLMN、ruleReport などを含む SM ポリシー制御の更新を送信します。 |
| 40 | PCF は、SM ポリシー制御更新応答の SM ポリシー決定を送信します。SMF は SM ポリシー決定を処理し、*3GPP TS 23.502*、セクション *4.3.3.2* で定義されている PCF 開始変更手順として処理します。 |

## 非 3GPP 信頼できない Wi-Fi から 5GS へのハンドオーバー コール フロー

このセクションでは、非 3GPP の信頼できない Wi-Fi から 5GS ハンドオーバー コール フローについて説明します。

図 *111* : 非 *3GPP* 信頼できない *Wi-Fi* から *5GS* へのハンドオーバー コール フロー

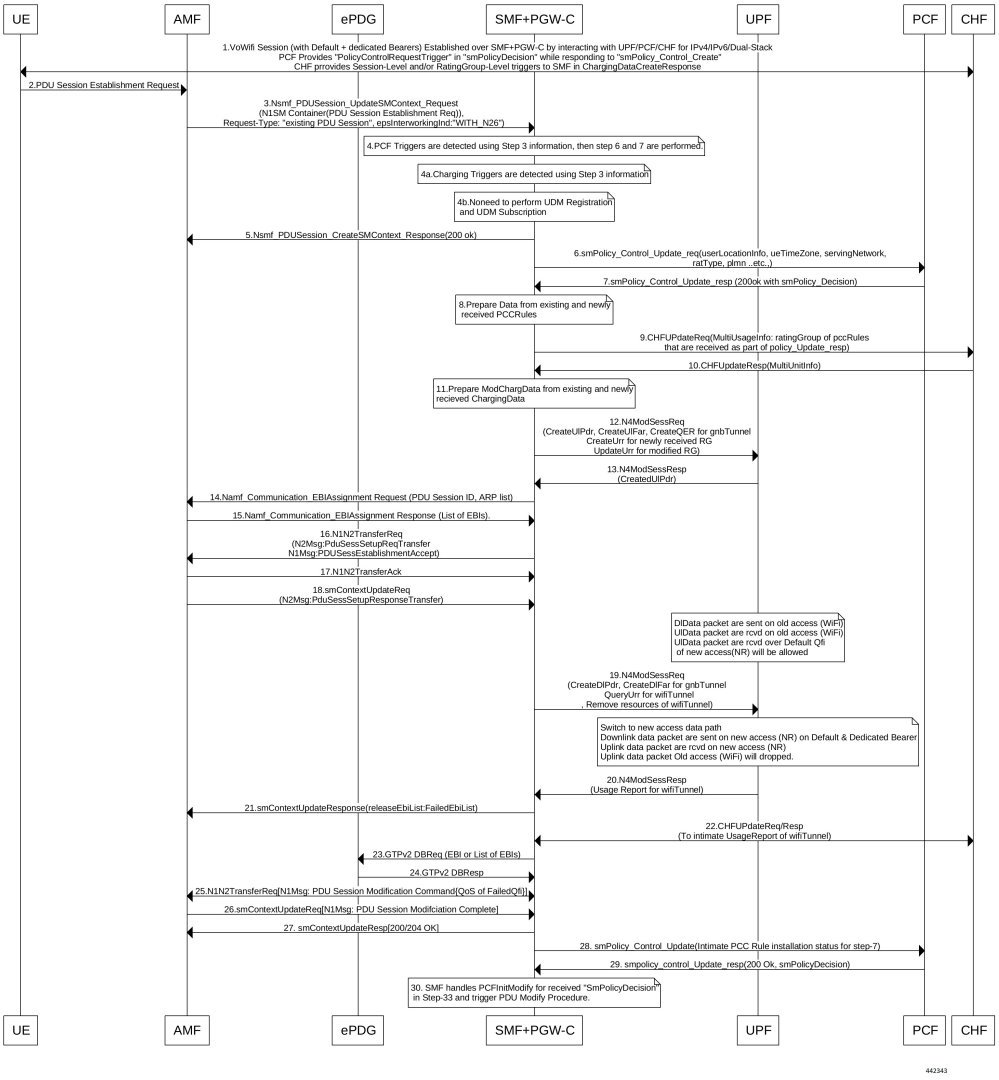



表 *183* : 非 *3GPP* 信頼できない *Wi-Fi* から *5GS* へのハンドオーバー コール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | 信頼できない非 3GPP アクセスを介して UE と ePDG 間で 1 つ以上の PDU セッションが確立されます。UE の 5G NAS 機能により、ePDG は PGW + SMF を組み合わせて選択します。UE が PDU セッション ID を PGW+SMF に送信します。 |

| ステップ | 説明 |
|---|---|
| 2 | UE は PDU セッション確立要求を AMF に送信します。この要求には、PDU セッション ID、要求された PDU セッションのタイプ、要求された SSC モード、5GSM 機能 PCO、SM PDU DN 要求コンテナ、パケット フィルタの数、およびオプションの要求常時 PDU セッションに関する詳細が含まれます。<br><br>既存 PDU セッション付きのリクエスト タイプは、3GPP アクセスと non-3GPP アクセスの間をスイッチまたは、EPC 内で既存の PDN 接続からの PDU セッション ハンドオーバーを示します。 |
| 3 | 要求タイプが「既存の PDU セッション」の場合、AMF は UDM から受信した SMF-ID に基づいて SMF を選択します。この要求タイプでは、AMF が登録中に AMF が UDM から受信した PDU セッション ID またはサブスクリプション コンテキストを識別しない場合、またはサブスクリプション プロファイルの更新通知手順に PDU セッション ID に対応する SMF ID が含まれていない場合、エラーが発生します。次に、AMF は PDU セッション用に保存されているアクセスタイプを更新します。<br><br>既存の PDU セッションを持つ要求タイプが 3GPP アクセスと非 3GPP アクセスの間を移動する PDU セッションを参照しており、PDU セッションの S-NSSAI がターゲット アクセス タイプの許可された NSSAI で使用可能な場合、PDU セッション確立手順は、PDU セッション ID に対応する SMF ID および AMF が同じ PLMN の一部である場合に実行されます。<br><br>AMF は、要求タイプが「Existing PDU Session」の NSMF PDU セッション作成 SM コンテキスト要求を SMF に送信します。この要求には、SUPI、DNN、S-NSSAI、PDU セッション ID、AMF ID、要求タイプ、PCF ID、優先アクセス、PDU セッション確立要求を含む N1 SM コンテナ、ユーザー位置情報、アクセス タイプ、PEI、GPSI、PDU セッション状態通知のサブスクリプション、DNN 選択モードに関する情報が含まれます。<br><br>SMF は、SUPI + PDU セッション ID を使用して、PDU セッション確立要求からの既存の PDU セッションを分析します。SMF は受信した UE の IPv4 または IPv6 アドレスを取得した PDU セッションの IPv4 または IPv6 アドレスと比較します。セッションが取得されない場合、または IPv4 または IPv6 アドレスが一致しない場合、SMF は要求を拒否します。 |
| 4 | SMF は、Wi-Fi セッション中に PCF との以前の通信で受信した要求ポリシー制御トリガに対してステップ 3 で利用可能な情報を使用して PCF トリガを検出します。 |
| 4a | SMF は、EPC セッションの確立中に受信した課金トリガに対してステップ 3 で利用可能な情報を使用して、課金トリガを検出します。 |
| 4b | SMF は、Wi-Fi セッション確立時に行われるような UDM 登録を実行しません。 |

| ステップ | 説明 |
|---|---|
| 5 | SMF は、NSMF PDU セッション 作成 SM コンテキスト応答を AMF に送信します。この応答には、原因、SM コンテキスト ID、または PDU セッション拒否の原因を含む N1 SM コンテナが含まれます。 |
| 6 | ステップ 4a で受信した検出されたアーム化されたポリシー制御トリガに基づいて、SMF は、ステップ 3 で検出されたアクセス パラメータを使用して PCF に SM ポリシー制御更新要求を送信します。 |
| 7 | PCF は、新規または更新された PCC ルールを含めることによって、SM ポリシーの決定である SM ポリシー制御更新応答を送信します。 |
| 8 | SMF は、ステップ 7 で受信した情報と Wi-Fi セッションの既存のポリシー データに基づいて、情報を準備します。 |
| 9 | SMF はステップ 7 で新しい PCC ルールを受信した場合、課金更新要求を、クォータ情報の新しい料金設定グループを持つ CHF に送信します。この要求には、新しいアクセス パラメータを含む PDU セッション情報が含まれています。 |
| 10 | CHF は、SMF に課金更新応答としてマルチユニット情報を送信します。マルチユニット情報には、料金設定グループのクォータ情報と、Wi-Fi セッションの既存のステップ 9 で受信した料金設定グループが含まれます。 |
| 11 | SMF は、CHF から課金更新応答を受信したデータを処理します。 |
| 12 | SMF は、gnb トンネルのために、N4 セッション変更要求を UPF に送信します。この要求には、アップリンク PDR の作成、QER の作成、受信した新しい料金設定グループ割当情報に対する URR の作成、変更されたクォータ情報に対する URR の更新、および FAR の作成に関する詳細が含まれます。 |
| 13 | UPF は、N4 セッション変更応答として作成された PDR 内にある UL トンネル情報を SMF に送信します。 |
| 14 | SMF は EBI 割り当て要求を AMF に送信します。この要求は、PDU セッションID の ARP リストを含みます。 |
| 15 | AMF は、SMF への応答として EBI のリストを送信します。 |
| 16 | SMF は、N1 N2 転送要求を AMF に向けて送信します。この要求には、サポートされている QFI リストおよび gnb トンネルの UL トンネル情報を含む「PDU セッション リソース セットアップ要求転送」として N2 メッセージが含まれています。この要求には、承認された QoS ルール、承認された QoS フローの説明、EPCO、PDN アドレス、およびセッション AMBR 値を含む N1 メッセージも「PDU セッション確立承認」として含まれています。 |
| 17 | AMF が SMF に N1 N2 転送確認応答を送信します。 |

| ステップ | 説明 |
|---|---|
| 18 | AMF は、失敗した QFI リストと DL トンネル情報を含む「PDU セッション リソース セットアップ応答転送」とともに、SM コンテキスト更新要求を SMF に送信します。 |
| 19 | SMF は、gnb トンネル リソースのために、N4 セッション変更要求を UPF に送信します。この要求は、DL PDR を作成し、DL トンネル情報を使用して DL FAR を作成し、RAT 変更の詳細を含め、Wi-Fi トンネルのリソースを削除することです。SMF は、受信した失敗した QFI リストの gnb トンネルの N4 リソースも削除します。 |
| 20 | UPF は、使用状況レポートを含む N4 セッション変更応答を SMF に送信します。 |
| 21 | SMF は、SM コンテキスト更新応答を AMF に送信します。 |
| 22 | SMF は、課金更新要求を PCF に送信します。この要求には、ステップ 18 で受信した古いアクセス パラメータと使用状況レポートを含む複数使用状況レポートに加え、新しいアクセス パラメータを含む PDU セッション情報が含まれます。<br>SMF は、既存の料金設定グループの新しいクォータ情報を含む課金更新応答を受信します。 |
| 23 | SMF + PGW-C は、EBI を含む GTPv2 DB 要求を ePDG に対して開始します。 |
| 24 | ePDG は SMF + PGW-C に GTPv2 DB 応答を送信します。 |
| 25 | SMF は、PDU セッション変更完了のための N1 メッセージを含む SM コンテキスト更新要求を AMF から受信します。 |
| 26 | SMF は AMF に「200/204 OK」として SM コンテキスト更新応答を送信します。 |
| 27 | SMF は、SM ポリシー制御更新応答として SM ポリシー決定を AMF に送信します。 |
| 28 | SMF は、SM ポリシー制御の更新要求を PCF に送信します。このリクエストには、N2 メッセージの一部として AMF から受信した失敗した QFI リストの新しいアクセス パラメータとルール レポートが含まれています。 |
| 29 | PCF は、SM ポリシー制御更新応答として SM ポリシー決定を SMF に送信します。 |
| 30 | SMF は SM ポリシー決定を処理し、3GPP 23.502 セクション 4.3.3.2 で定義されている PCF 開始変更手順として処理します。 |

## 5GS から非 3GPP への信頼できない Wi-Fi ハンドオーバー コール フロー

このセクションでは、5GS から非 3GPP の信頼できない Wi-Fi ハンドオーバー コール フローについて説明します。

図 *112 : 5GS* から非 *3GPP* への信頼できない *Wi-Fi* ハンドオーバー コール フロー

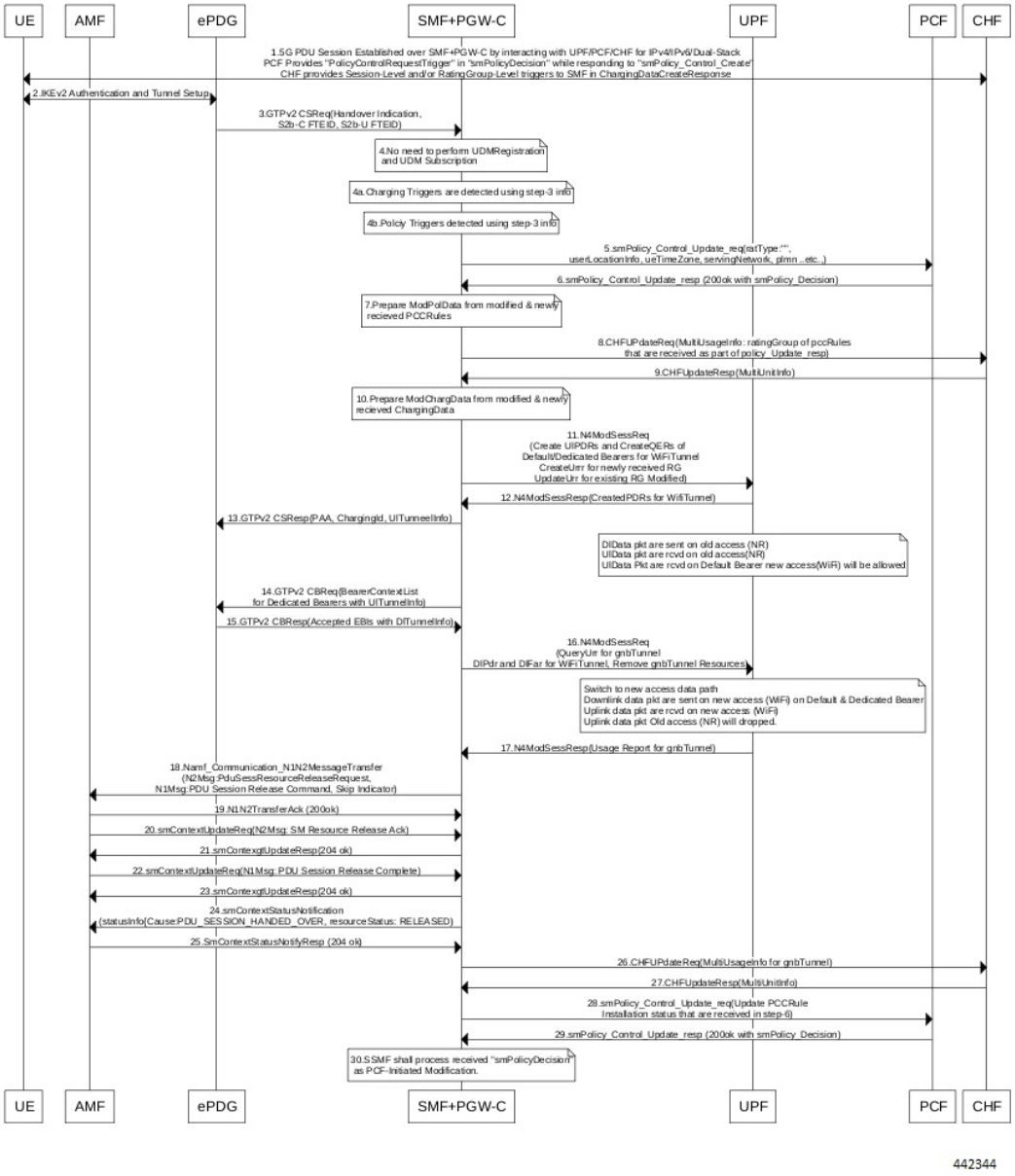



表 *184 : 5GS* から非 *3GPP* への信頼できない *Wi-Fi* ハンドオーバー コール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | UE と SMF または UPF は、NG-RAN を介して通信して、1 つまたは複数の PDU セッションを確立します。 |

| ステップ | 説明 |
|---|---|
| 2 | UE は信頼できない非 3GPP アクセスに接続され、ePDG を選択します。次に、UE は、3GPP TS 23.402（セクション 8.6.2.1）で定義されているハンドオーバー接続手順を開始します。UE と ePDG の間に IKE トンネルが確立され、UE が AAA サーバとの SWm インターフェイスを介して認証された後、UE は IKE_AUH を開始します。IKE_AUH には、5GS および P-CSCF と DNS のオプションで以前に割り当てられた IPv4 または IPv6 アドレスの cfg_params が含まれます。 |
| 3 | ePDG はセッション作成要求を PGW-C に送信します。この要求には、次の詳細が含まれます。<br>• IMSI<br>• APN<br>• ハンドオーバー インジケータ<br>• RAT タイプ<br>• コントロール プレーンの ePDG TEID<br>• ユーザー プレーンの ePDG アドレス<br>• ユーザー プレーンの ePDG TEID<br>• EPS ベアラー ID<br>• ユーザーの現在地<br><br>RAT タイプは、非 3GPP アクセス テクノロジー タイプを示します。UE が IP アドレス保持をサポートし、ポート アナライザ アダプタ（PAA）に含める場合、ePDG はセッション要求の作成においてハンドオーバー通知を構成します。この構成により、PGW-C は、UE に割り当てられたのと同じ IP アドレスまたはプレフィックスを再割り当てできます。IP アドレスまたはプレフィックスの割り当ては、UE が 3GPP IP アクセスに接続されているときに発生します。ポリシー変更手順は PCF から始まります。 |
| 4 | 登録は 5GS セッションの確立中に行われるため、SMF は UDM 登録を実行しません。 |
| 4a | SMF は、EPC セッションの確立中に受信した課金トリガに対してステップ 3 で利用可能な情報を使用して、課金トリガーを検出します。 |
| 4b | SMF は、Wi-Fi セッション確立中に PCF との通信で受信した要求ポリシー制御トリガに対してステップ 3 で利用可能な情報を使用してポリシー トリガを検出します。 |
| 5 | ステップ 4b で受信した検出されたアーム化されたポリシー制御トリガに基づいて、SMF は、検出されたアクセス パラメータを使用して PCF に SM ポリシー制御更新要求を送信します。 |

| ステップ | 説明 |
|---|---|
| 6 | PCF は、新規または更新された PCC ルールを含めることによって、SM ポリシーの決定である SM ポリシー制御更新応答を送信します。 |
| 7 | SMF は、ステップ 7 で受信した情報と 5GS セッションの既存のポリシー データに基づいて、「ModPolData」情報を準備します。 |
| 8 | SMF はステップ 6 で新しい PCC ルールを受信した場合、課金更新要求を、クォータ情報の新しい料金設定グループを持つ CHF に送信します。この要求には、新しいアクセス パラメータを含む PDU セッション情報が含まれています。 |
| 9 | CHF は、SMF に課金更新応答としてマルチユニット情報を送信します。マルチユニット情報には、料金設定グループのクォータ情報と、5GS セッションの既存のステップ 9 で受信した料金設定グループが含まれます。 |
| 10 | SMF は、CHF から受信した課金更新応答内の ModChargingData を処理します。 |
| 11 | SMF は、Wi-Fi トンネルのために、N4 セッション変更要求を UPF に送信します。この要求には、アップリンク FAR の作成、QER の作成、受信した新しい料金設定グループ クォータ情報の URR の作成、および変更されたクォータ情報の URR の更新に関する詳細が含まれています。 |
| 12 | UPF は、SMF への N4 セッション変更応答を、作成された PDR 内の UL トンネル情報とともに SMF に送信します。 |
| 13 | SMF は GTPv2 セッション作成応答を S-GW に送信します。この応答には、承認された要求または部分的に承認された要求の詳細、PGW-C S2b F-TEID、PAA、APN-AMBR、ベアラー コンテキストの作成、課金ゲートウェイ アドレス、および APCO が含まれます。 |
| 14 | SMF は、S-GW に GTPv2 ベアラー要求の作成を送信します。この要求には、エンドユーザー向けの各専用ベアラーに対する UL トンネル情報を含む、ベアラー コンテキスト リストに関する情報が含まれています。 |
| 15 | S-GW は SMF に GTPv2 ベアラー作成応答を送信します。応答には、要求を受け入れたか、要求を部分的に受け入れたか、 およびベアラー コンテキストの詳細が含まれます。 |
| 16 | SMF はベアラー応答の作成を処理し、確立されたベアラーの DL トンネル情報と失敗した EBI リスト（ある場合）を取得します。SMF は、Wi-Fi トンネルのために、N4 セッション変更要求を UPF に送信します。この要求では、検出された課金トリガの DL トンネル情報または課金説明 ID のリストを使用して DL PDR および DL FAR を作成します。<br>SMF は、失敗したベアラー コンテキスト リストの Wi-Fi トンネルの gnb トンネル リソースと N4 リソースを削除します。 |

| ステップ | 説明 |
|---|---|
| 17 | UPF は、N4 セッション変更応答として使用状況レポートを SMF に送信します。 |
| 18 | SMF は、S-GW への NAMF 通信 N1 および N2 メッセージ転送を開始します。この転送メッセージには、PDU セッション リソース解放要求 N2 メッセージが含まれています。 |
| 19 | AMF は、N1 N2 転送の確認応答を SMF に送信します。 |
| 20 | AMF は、SM コンテキスト更新要求を SMF に送信します。この要求には、SM リソース リリース確認応答 N2 メッセージが含まれます。 |
| 21 | SMF は、SM コンテキスト更新応答を「200/204 OK」として AMF に送信します。 |
| 22 | AMF は、SM コンテキスト更新要求を SMF に送信します。この要求には、PDU セッション リリース完了 N1 メッセージが含まれます。 |
| 23 | SMF は、SM コンテキスト更新応答を「200/204 OK」として AMF に送信します。 |
| 24 | SMF が 3GPP 仕様 23.502 の 2019 年 6 月の準拠バージョンをサポートしている場合、SMF は AMF にリリースの詳細を示します。SMF は、SM コンテキスト ステータス通知メッセージ（statusInfo;Cause: PDU_SESSION_HANDED_OVER, resourceStatus: RELEASED）を送信することでこの機能を実現します。SMF は、5GS から 3GPP 以外の信頼できない WiFi セッションへのハンドオーバーが成功した後に、この通知を送信します。<br><br>SMF は、対応するサービス用に構成されたコンプライアンス プロファイルに従ってメッセージが処理されます。コンプライアンスプロファイルの詳細については、「コンプライアンス プロファイルの構成 （586 ページ）」の項を参照してください。<br><br>**重要**<br>SMF が 3GPP 仕様の 2018 年 12 月準拠バージョンをサポートしている場合、ステップ 24 およびステップ 25 は適用されません。 |
| 25 | SMF は、SM コンテキスト ステータス通知応答として「204 OK」を SMF に送信します。<br><br>**重要**<br>SMF が 3GPP 仕様の 2018 年 12 月準拠バージョンをサポートしている場合、ステップ 24 およびステップ 25 は適用されません。 |
| 26 | SMF は、CHF に課金更新要求を送信します。この要求には、ステップ 17 で受信した古いアクセス パラメータと使用状況レポートの詳細を含む複数使用状況レポートを含む PDU セッション情報が含まれています。 |

| ステップ | 説明 |
|---|---|
| 27 | CHF は、SMF に課金更新応答としてマルチユニット情報を送信します。マルチユニット情報には、既存の料金設定グループの新しいクォータ情報が含まれています。 |
| 28 | SMF は PCF に SM ポリシー制御の更新を送信します。この更新には、ベアラー応答の作成の一部として AMF から受信した失敗した QFI リストの新しいアクセス パラメータとルール レポートが含まれています。 |
| 29 | PCF は、SM ポリシー決定である SM ポリシー制御更新応答を SMF に送信します。 |
| 30 | SMF は SM ポリシー決定を処理し、3GPP TS 23.502、セクション 4.3.3.2 で定義されている PCF 開始変更手順として処理します。 |

## 非信頼 3GPP LTE から WiFi へのハンドオーバー

このセクションでは、非 3GPP 信頼 LTE to WiFi ハンドオーバー コール フローについて説明します。

図 *113* : 専用ベアラーで *4* を超える *TFT* を使用した非 *3GPP* 信頼できない *LTE* から *WiFi* へのハンドオーバー

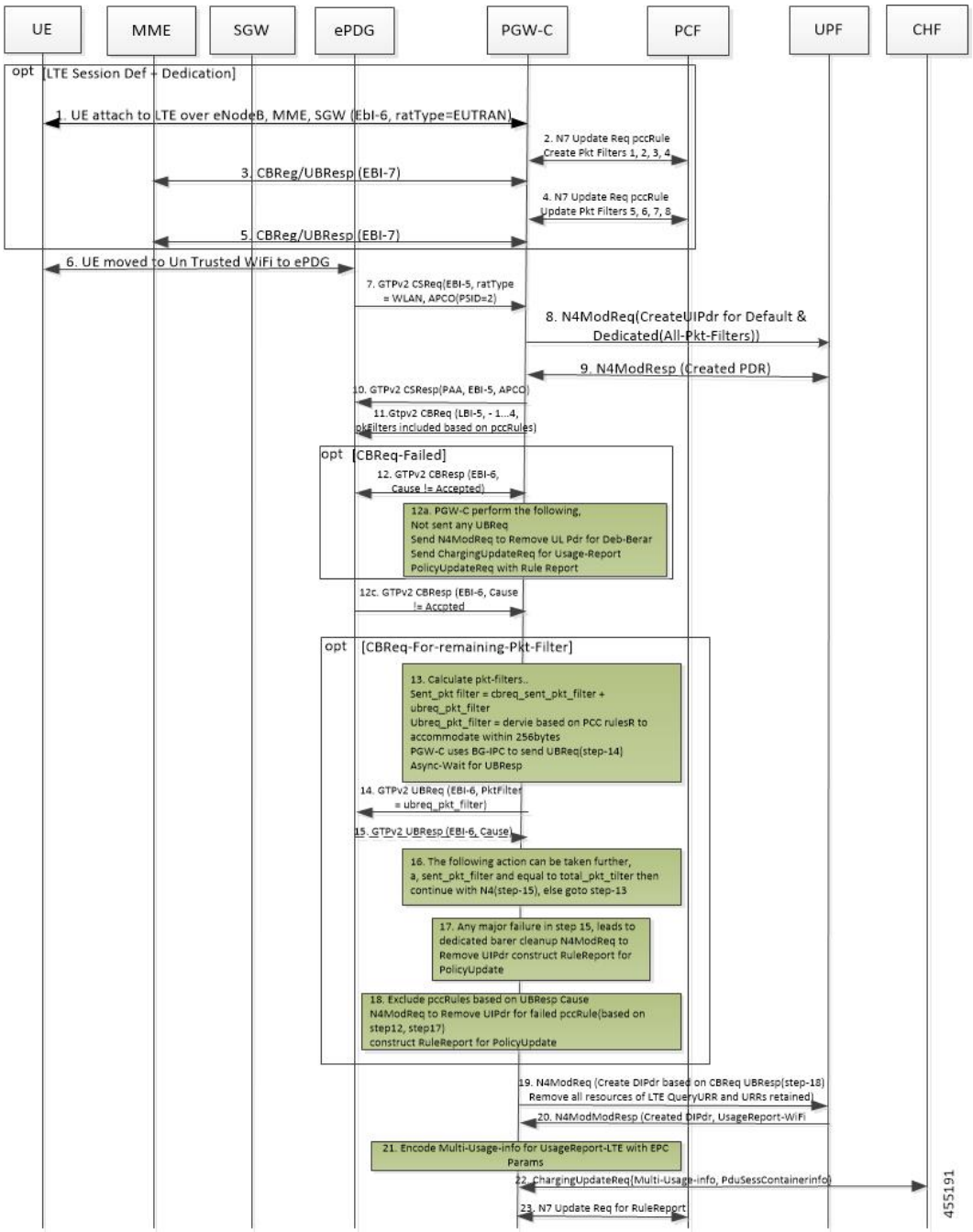


表 *185* : 非 *3GPP* 信頼できない *LTE* から *WiFi* へのハンドオーバー コール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | セッションは、デフォルトのベアラーと 8 TFT の専用ベアラーで LTE で確立されます。 |
| 2 | ePDG から Hi フラグが構成された CSReq を受信すると、LTE から Wi-Fi へのハンドオーバーがトリガーされます。 |
| 3 | CSReq が正常に処理された後、CSResp が ePDG に返され、デフォルトのベアラーが正常に引き渡されたことが示されます。 |
| 4 | 8 TFT を持つ専用ベアラーの場合、すべての TFT を CBReq で送信できないため、CBReq メッセージは ePDG に対する 4 TFT のみでトリガーされます。 |
| 5 | ePDG からの CBResponse が成功した後、SMF は残りの TFT を UBReq メッセージで送信します。 |
| 6 | ePDG からの UBResponse が成功した後、SMF は UPF へのベアラーの確立の完了に進みます。 |
| 7 | CBResponse で障害が発生した場合、またはステップ 5 またはステップ 6 で UBResponse で障害が発生した場合、SMF はそのベアラーを削除し、装備されている場合は、対応するルール情報を [非アクティブ（Inactive）] として PCF にルール レポートを送信します。 |

**重要** ステップ 4 ～ 7 は、専用ベアラーに 4 つ以上の TFT がある場合、LTE から Wi-Fi および NR から Wi-Fi に適用されます。

## GTPC の IE サポート

SMF は、GTPC メッセージで次の IE をサポートします。

表 *186* : *GTPC* メッセージでサポートされる *IE*

| IE | シナリオ |
|---|---|
| UE ローカル IP アドレス | SMF がセッション要求の作成、ベアラー応答の作成、ベアラー要求の変更、またはベアラー応答の削除の手順中に ePDG から UE ローカル IP アドレスを受信すると、トリガーが満たされた場合、SMF は PCF および CHF に n3gaLocation 属性を送信します。 |

| IE | シナリオ |
|---|---|
| UE UDP ポート | SMF がセッション要求の作成、ベアラー応答の作成、ベアラー要求の変更、またはベアラー応答の削除の手順中に ePDG から UE UDP ポートを受信すると、トリガーが満たされた場合、SMF は PCF および CHF に n3gaLocation 属性を送信します。 |

**例**

次に、 **show subscriber supi imsi-123456789012345 nf-service smf psid 5 full** コマンドの出力で n3GaLocation 属性を表示する例を示します。

```
"n3GaLocation": {
"PortNumber": 4661,
"UeIpv4Addr": "209.165.200.227",
"ueLocationTimestamp": "2021-03-09T12:34:02Z"
}
```

## 代替 RAT トンネル作成コール フローによる Wi-Fi から 5G へのハンドオーバー

このセクションでは、代替 RAT トンネルの作成による Wi-Fi から 5G へのハンドオーバーのコール フローについて説明します。

**図 *114*：代替 *RAT* トンネル作成コール フローによる *Wi-Fi* から *5G* へのハンドオーバー**

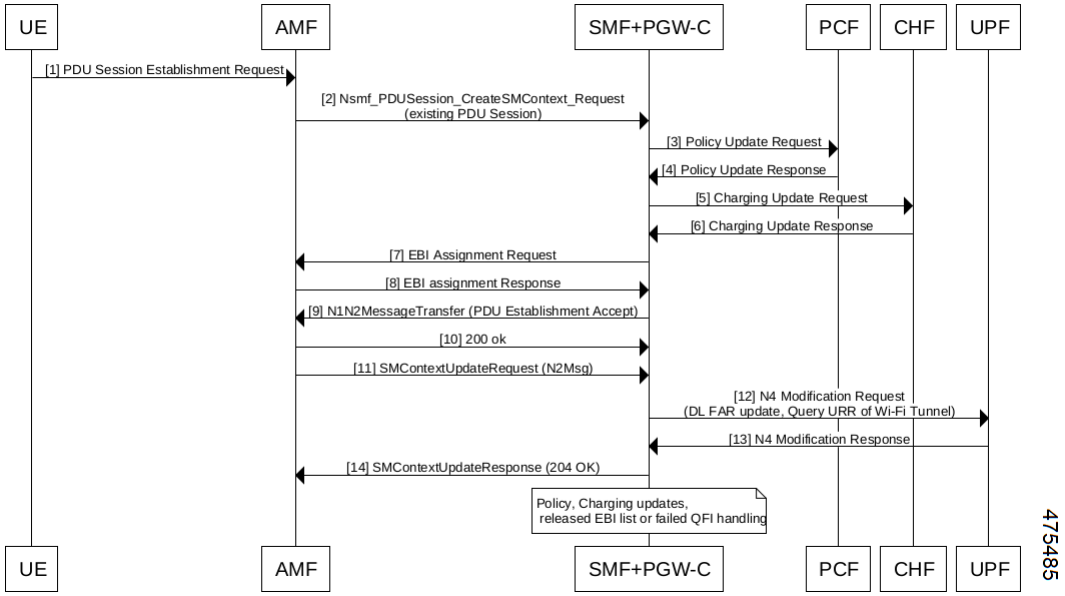


表 *187* : 代替 *RAT* トンネル作成による *Wi-Fi* から *5G* へのハンドオーバー コール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | UE は、PDU セッション確立要求を AMF に送信します。 |
| 2 | SMF+PGW-C に対する AMF Nsmf PDU Session Create SMContext 要求。この要求は既存の PDU セッションに対するものです。<br>SMF+PGW-C は 200 OK メッセージを送信します。 |
| 3 | SMF + PGW-C は PCF にポリシー更新要求を送信します。 |
| 4 | PCF は、SMF + PGW-C にポリシー更新応答を送信します。 |
| 5 | SMF + PGW-C は、CHF に課金更新要求を送信します。 |
| 6 | CHF は、課金更新応答を SMF+PGW-C に送信します。 |
| 7 | SMF + PGW-C は、EBI 割り当て要求を AMF に送信します。 |
| 8 | AMF は、EBI 割り当て応答を SMF + PGW-C に送信します。 |
| 9 | SMF + PGW-C は、N1N2 メッセージ転送（PDU 確立承認）メッセージを AMF に送信します。 |
| 10 | AMF は、200 OK 応答を SMF + PGW-C に送信します。 |
| 11 | AMF は、SMContext 更新要求（N2 メッセージ）を SMF + PGW-C に送信します。 |
| 12 | SMF + PGW-C は、UPF に N4 変更要求を送信します。この要求には、Wi-Fi トンネルの DL FAR アップデートとクエリ URR に関する詳細が含まれています。 |
| 13 | UPF が SMF+PGW-C に N4 変更応答を送信します。 |
| 14 | SMF + PGW-C は、 SMContext アップデート応答の 204 OK を AMF へ送信します。SMF+PGW-C<br>SMF + PGW-C には、ポリシー、課金更新、およびリリースされた EBI リストまたは失敗した QFI 処理情報に関する詳細が含まれます。 |

## 代替 RAT トンネル作成コール フローによる 5G から Wi-Fi へのハンドオーバー

このセクションでは、代替 RAT トンネルの作成による 5G から Wi-Fi へのハンドオーバーのコール フローについて説明します。

図 *115* : 代替 *RAT* トンネル作成コール フローによる *5G* から *Wi-Fi* へのハンドオーバー

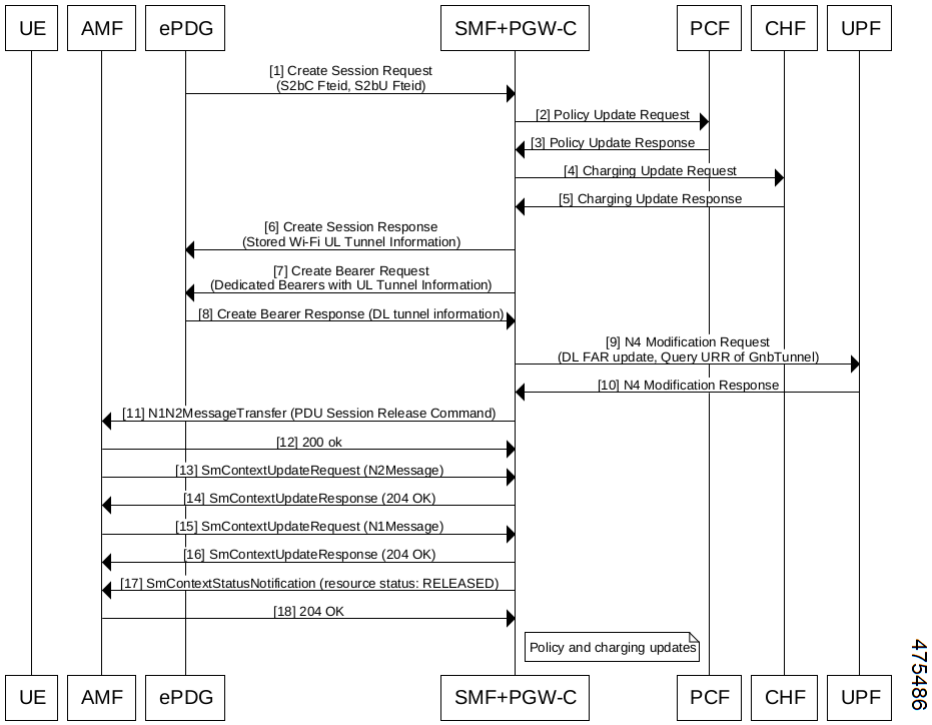



表 *188* : 代替 *RAT* トンネル作成による *5G* から *Wi-Fi* へのハンドオーバー コール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | ePDG は、SMF + PGW-C にセッション要求の作成を送信します。このリクエストには、S2bC F-TEID および S2bU F-TEID に関する詳細が含まれています。 |
| 2 | SMF + PGW-C は PCF にポリシー更新要求を送信します。 |
| 3 | PCF は、SMF + PGW-C にポリシー更新応答を送信します。 |
| 4 | SMF + PGW-C は、CHF に課金更新要求を送信します。 |
| 5 | CHF は、課金更新応答を SMF+PGW-C に送信します。 |
| 6 | SMF+PGW-C はセッション応答の作成を ePDG に送信します。この応答には、保存されている Wi-Fi UL トンネルの詳細が含まれます。 |
| 7 | SMF + PGW-C は、ePDG にベアラー作成要求を送信します。このリクエストには、UL トンネルの専用ベアラーに関する詳細が含まれています。 |
| 8 | ePDG は、Create Bearer Response（DL トンネル情報）を SMF + PGW-C に送信します。 |

| ステップ | 説明 |
|---|---|
| 9 | SMF + PGW-C は、UPF に N4 変更要求を送信します。この要求には、gNB トンネルの DL FAR アップデートとクエリ URR に関する情報が含まれています。 |
| 10 | UPF が SMF+PGW-C に N4 変更応答を送信します。 |
| 11 | SMF + PGW-C は、AMF に PDU セッション リリース コマンドである N1N2Message 転送を送信します。 |
| 12 | AMF は、200 OK 応答を SMF + PGW-C に送信します。 |
| 13 | AMF は、SMContext 更新要求（N2Message）を SMF + PGW-C に送信します。 |
| 14 | SMF + PGW-C は、SMContext Update Response（204 OK）を AMF に送信します。 |
| 15 | AMF は、SMContext 更新要求（N1Message）を SMF + PGW-C に送信します。 |
| 16 | SMF + PGW-C は、SMContext Update Response（204 OK）を AMF に送信します。 |
| 17 | SMF + PGW-C は、AMF に SM コンテキスト ステータス通知を送信します。この通知は、リソースの状態が RELEASED として示されていることを示します。 |
| 18 | AMF は、204 OK 応答を SMF + PGW-C に送信します。<br>次に、SMF + PGW-C で、ポリシーと課金の更新が行われます。 |

# Wi-Fi ハンドオーバーの構成

このセクションでは、Wi-Fi ハンドオーバー機能に関連する構成について説明します。

## コンプライアンス プロファイルの構成

SMF は、CLI 構成を介して 3GPP 仕様 23.502 のコンプライアンス プロファイル サポートを提供します。このコンプライアンス プロファイルは、5GS から非 3GPP への信頼できない Wi-Fi ハンドオーバーの手順中に使用されます。

3GPP 仕様に準拠して SMF を構成するには、次の構成を使用します。

```
config
   profile compliance profile_name
      service threegpp23502 version   spec  {  15.4.0 | 15.6.0 } spec_version
 full version_format
      uri_version uri_version
         range
         !
         !
```

**重要** コンプライアンス プロファイルの構成方法の詳細は、Cisco アカウント担当者にご連絡ください。

**注**：

- **full**：次の形式で完全バージョンを指定します。<Major-version> 。<Minor-version> 。<patch-version> .[alpha-<draft-number> ]
- **spec**：3GPP 仕様バージョン番号を指定します。次のいずれかの値を指定できます。
  - 15.4.0
  - 15.6.0

  3GPP 2018 年 12 月仕様に準拠するためには、仕様バージョンを 15.4.0 として設定します。デフォルトのバージョンは 15.4.0 です。

  3GPP 2019 年 6 月の仕様準拠をサポートするには、仕様のバージョンを 15.6.0 に構成します。
- **uri**：URI バージョンを番号と連結した「v」形式で指定します。バージョンは、v1 と v2 の両方、または v1 または v2 のいずれかです。

## ハンドオーバー通知を伴うコールの構成

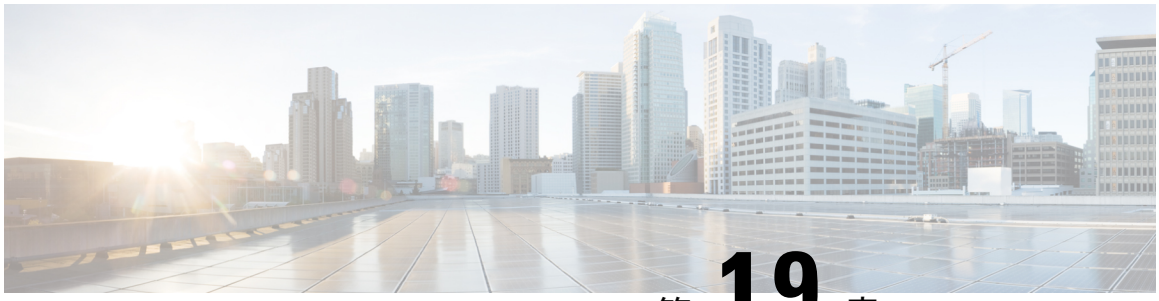
次の構成例を使用して、ハンドオーバー（HO）通知で着信するコールおよび既存のセッションがないコールを処理します。

```
config
  profile access access_profile_name
   gtpc message-handling create-session-request ho-ind new-call-reject

    exit
```

**注**：

- **ho-ind**：セッション要求の作成がハンドオーバーで受信されたことを示します。
- **new-call-reject**：セッションが存在しない場合、SMF は HO インジケータで受信したセッション作成要求を拒否します。



第 19 章

# 音声用の IMS PDU セッション


- 機能の概要と変更履歴, on page 589
- 機能説明 （590 ページ）
- LTE の音声サポート （590 ページ）
- VoLTE および VoNR の NPLI サポート （603 ページ）
- VoWi-Fi サポート （604 ページ）
- 音声の新しいラジオ （611 ページ）


## 機能の概要と変更履歴

### 要約データ

***Table 189:*** 要約データ

| | |
|---|---|
| 該当製品または機能エリア | SMF |
| 該当プラットフォーム | SMI |
| 機能のデフォルト設定 | 無効：設定が必要 |
| このリリースでの関連する変更点 | N/A |
| 関連資料 | 該当なし |

### 更新履歴

***Table 190:*** マニュアルの変更履歴

| 改訂の詳細 | リリース |
|---|---|
| VoLTE および緊急通話の優先順位付けのサポートを追加 | 2021.02.03 |

| 改訂の詳細 | リリース |
|---|---|
| VoLTE と VoNR の NPLI サポートを紹介 | 2021.02.0 |
| 最初の導入。 | 2020.02.0 より前 |

# 機能説明

この章では、SMF によって処理される IMS 手順の概要について説明します。

# LTE の音声サポート

## 機能説明

**Important** この章で使用されている PGW-C という用語は、SMF によってサポートされている EPS インターワーキング機能を意味しており、LTE ネットワークで使用されるスタンドアロン P-GW として想定してはなりません。

SMF は、Voice over Long-Term Evolution または LTE（VoLTE）をサポートします。VoLTE テクノロジーでは IP マルチメディア サブシステム（IMS）を利用して、LTE アクセス ネットワーク上でセルラー コールを実行できます。

SMF は、ICSR スイッチ オーバーおよびリカバリ時に、緊急コールと VoLTE コールの優先順位付けをサポートします。SMF は、アクティブな音声コールが含まれている IMS セッションを追跡するとともに UPF と通信します。次に、UPF は ICSR のスイッチ オーバーとリカバリ中に、緊急コールと VoLTE コールを優先します。SMF は、MP フラグが N4 で構成され、GTP ヘッダーが WPS 構成に基づいているワイヤレス プライオリティ サービス（WPS）コールの優先順位付けのみをサポートします。

### 機能の仕組み

LTE アクセスを備えた 5G モバイル デバイスは、S-GW および MME を介して PGW-C と通信するように音声サービスを要求します。その結果、PDU セッションが確立されます。PGW-C は、VoLTE セッションの QCI フローが 5 である非 GBR ベアラーをサポートします。このサポートにより、エンドユーザーの P-CSCF、DNS IPv4、または DNS IPv6 アドレスとともに IMS シグナリングが可能になります。モバイル発信（MO）コールまたはモバイル着信（MT）コールの場合、アプリケーション機能（AF）はポリシー許可の詳細を PCF に提供します。次に、PCF はこれらの詳細を GBR フローと PCC ルールに変換し、PGW-C に送信します。次に、PGW-C は、UE（ユーザー機器）で専用ベアラー作成手順を確立することにより、GBR フローを専用ベアラに変換します。PGW-C は、UPF への QCI フローを 1 として GBR をプロビジョ

ニングします。このプロビジョニングにより、UPFは、IMSネットワーク要素を介した発信側と着信側のデバイス間の音声通信をサポートします。

E-UTRAN 接続手順に従って、MME は S-GW 経由で PGW-C への GTPv2 セッション作成要求をトリガーします。この要求には、EPS ベアラー ID（EBI）値、P-CSCF および DNS IPv4 または DNS IPv6 コンテナの ePCO オプション、エンドユーザーに IPv4 または IPv6 で割り当てられたアドレスの PDN-Type、および PAA オプションが含まれています。PGW-C は、受信したセッション作成要求を処理し、さまざまなSBIインターフェイスと通信して次の情報を受信します。

- サブスクリプション要求に PGW-C FQDN を含めることによる UDM からのサブスクリプション データ。
- SM ポリシー作成要求の送信による PCF からのポリシー情報。ポリシー情報には、PCC ルールやセッション AMBR などの詳細が含まれます。
- 課金データ作成要求を送信して、CHF からのオンラインおよびオフラインの課金情報。

ローカル SMF プロファイルの構成に基づく SBI インターフェイスとの通信の後、PGW-C は、S-GW および MME を介してエンドユーザーに GTPv2 セッション作成応答を送信します。この応答には次の内容が含まれます：

- PGW-C IPAM モジュールが割り当てる IPv4 または IPv6 アドレスを持つ PAA
- P-CSCF を使用する ePCO オプション
- DNN プロファイル構成に基づく DNS IPv4 アドレスまたは DNS IPv6 アドレス
- IMS シグナリングの場合、QCI フローが 5 の非 GRB

MO または MT コールの場合、エンドユーザー向けの QCI フローが 1 として GBR 用に PCF がプロビジョニングされている場合、PGW-C はこれらの GBR フローを専用ベアラーの作成に変換します。GBR フローには、SM ポリシー更新通知要求にフロー情報と PCC ルールが含まれます。専用ベアラは、S-GW または MME を介して UE に GTPv2 ベアラー要求の作成を送信することによって作成されます。また、S-GW と PGW-C の間に別の S5-U トンネルが作成され、発信側と着信側のデバイス間の音声通信にGBEフローパケットが使用できるようになります。

ICSR スイッチオーバーおよびリカバリ中の緊急コールと VoLTE コールの優先順位付けのために、SMF は N4 メッセージおよび GTP メッセージに MP フラグ値を含めます。フラグの値を次の表に示します。

***Table 191: MP* フラグ値**

| コール タイプ | MP フラグ値 |
|---|---|
| 緊急（Emergency） | 1 |
| IMS アクティブ | 2 |
| IMS 非アクティブ | 3 |
| WPS | 1 |

**Note**

- **message-priority gtpc** がWPS プロファイルで構成されている場合、SMF は WPS セッションの MP フラグ値を 1 として送信します。以前の SMF は、WPS セッションの N4 および GTP ヘッダーで MP 値を 0 として送信するために使用されていました。
- コールが複数のコール タイプに一致する場合、SMF はより適切な優先順位（最小値）を送信します。コールが WPS と一致し、 **message-priority** が構成されていない場合、メッセージ優先順位は送信されません。
- SMF は、DNN プロファイルで IMS として構成された QCI の確立のために専用ベアラーまたは変更手順が開始され、セッションが IMS アクティブとしてマークされない場合に、セッションを IMS 非アクティブとしてマークします。
- SMF は、IMS QCI ベアラーまたはフローが確立された後、セッションを IMS アクティブ セッションとして更新します。
- SMF は、最後の IMS QCI ベアラーまたはフローが削除された後、IMS 非アクティブ セッションとしてセッションを更新します。
- SMF は、WPS プロファイルで構成されている ARP に対して専用ベアラーまたは変更手順が開始されたときに、セッションを WPS セッションとしてマークします。
- SMF は、WPS ベアラーまたはフローが確立された後、セッションを WPS セッションとして更新します。
- 最後の WPS ベアラーが削除されたときに IMS QCI ベアラーが存在している場合、SMF はセッションを IMS アクティブまたは IMS 非アクティブとして更新します。
- ハンドオーバー、パス切り替え、またはその他の手順中に IMS フローが削除された場合、SMF はセッションを IMS 非アクティブとして更新します。
- クリア サブスクライバの非 VoLTE CLI の実装は、IMS として構成されている QCI を使用するように変更されています。QCI が構成されていない場合は、非 VoLTE セッションを検出する以前の動作が使用されます。この動作は、セッションに QCI が 1 または 2 のベアラーまたはフローがないことを意味します。

## コール フロー

このセクションでは、次のコールフローについて説明します。

- VoLTE PDU セッションの作成コール フロー
- VoLTE モバイル発信（MO）コール作成コール フロー
- VoLTE モバイル着信（MT）コールの作成コール フロー

### *VoLTE PDU* セッションの作成コール フロー

5G コアを介した接続を有効にするために、E-UTRAN または EPS の最初のアタッチは、次のように定義された 3GPP 手順から逸脱します。

- この手順では、SMF + PGW-C が PGW-C の代わりになります。
- SM ポリシーの関連付けの確立手順は、IP-CAN セッションの確立と変更に代わるものです。
- CHF を使用した NCHF インターフェイス経由の統合課金は、Gy および Gz インターフェイスを使用したオンラインおよびオフラインの課金機能に代わるものです。
- ユーザー プレーン ノードとの通信は、Sxb インターフェイスではなく N4 インターフェイスを介して行われます。

**Note** マッピングされた PCC ルールに応じて、SMF + PGW-C は専用ベアラーの作成を開始できます。

以下のコール フローは、VoLTE PDU セッションの作成の流れを示しています。

*Figure 116: VoLTE PDU* セッションの作成コール フロー

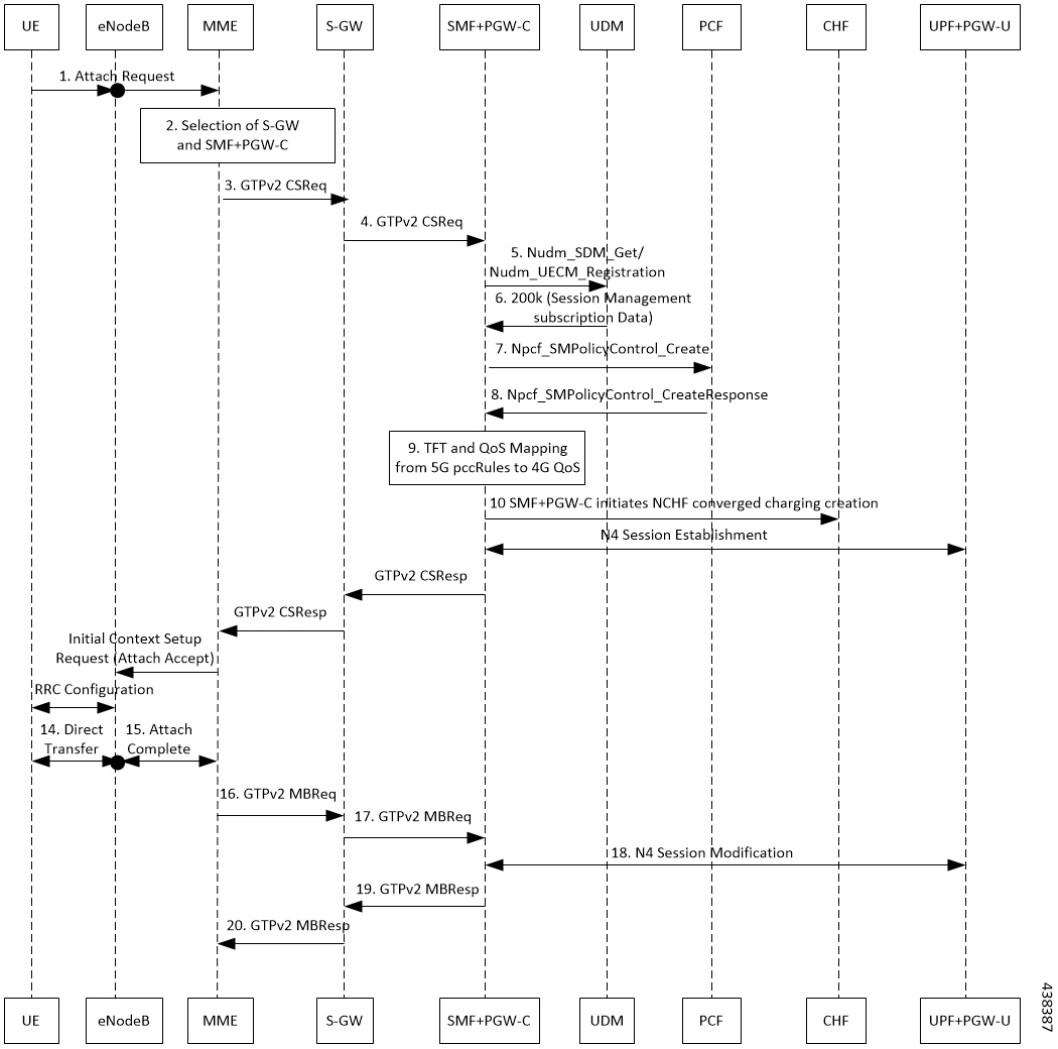



*Table 192: VoLTE PDU* セッション作成コール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | UE は、eNodeB を介して MME に接続要求を送信します。 |
| 2 | MME は、UE がアクティブであり、NR へのハンドオフをサブスクライブしているかどうかを判断します。次に、MME は PDU セッションの PGW-C として SMF+PGW-C ノードを選択します。 |
| 3 | MME は、選択した S-GW にセッション作成要求を送信し、選択した SMF + PGW-C アドレスを要求に含めます。 |

| ステップ | 説明 |
|---|---|
| 4 | S-GW は、拡張 PCO IE オプションに「P-CSCF IPv4 または IPv6 要求」コンテナ識別子を含めることで、SMF+PGW-C に対するセッション作成要求を開始します。<br>SMF + PGW-C は、UE が PCO オプションで送信する PDU セッション ID を抽出して保存します。次に、SMF + PGW-C は UDM 登録を実行し、N11 および S5 または S8 インターフェイス ID の両方を UDM に送信します。各 DNN の UDM から受信したローカル構成またはセッション管理サブスクリプション データに基づいて、SMF+PGW-C は「IMS Voice over PS」をサポートすることを決定します。 |
| 5 | SMF+PGW-C は、NPCF SM ポリシー制御作成要求を PCF に送信して、SM ポリシー関連付けの確立手順を開始します。この手順では、PGW-C+SMF は、セッションの作成要求メッセージで受信した情報要素を Npcf_SMPolicyControl_Create サービスに含めます。これらの要素は、次の情報で構成されます。<br>• SUPI には IMSI が含まれています。<br>• DNN には APN が含まれています。<br>• PEI には IMEI-SV が含まれます。<br>• セッション AMBR には APN-AMBR が含まれています。<br>• デフォルトの EPS ベアラー QoS を含むデフォルトの QoS 情報。QCI 値は 5QI 値にマッピングされます。 |
| 6 | PGW-C+SMF は、PCC ルール、PDU セッション ポリシー情報、および 5G QoS 情報を受信します。PCC ルールは EPS QoS 情報にマッピングされます。SMF+PGW-C は、PCC ルールで受信した SDF フィルタから TFT を作成します。次に、SMF+PGW-C は、それらを対応するデフォルトおよび専用のベアラーに関連付けます。 |
| 7 | PCF から受信した課金ポリシーに基づいて、SMF+PGW-C は、CHF に対して NCHF コンバージド課金の作成手順を開始します。この手順は、PCF から受信した課金ルールに基づきます。 |
| 8 | SMF+PGW-C は、UPF+PGW-U の選択と N4 セッションの確立手順を開始します。このセッションは、SMF+PGW-C に接続する 4G セッションであるため、ベアラーごとに個別の CN トンネルが作成されます。また、QoS フロー識別子（QFI）が QoS 適用ルール（QER）およびパケット検出ルール（PDR）で送信されません。 |
| 9 | SMF+PGW-C は、S-GW へセッション作成応答を送信します。この応答には、デフォルトのベアラーのベアラー情報と TEID が含まれています。また、SMF + PGW-C には、UE への PCO オプション 001CH（QoS ルール）、001DH（セッション AMBR）、001EH（PDU セッション アドレスの有効期間）、および 001FH（QoS フロー記述）に 5G QoS パラメータも含まれています。 |

| ステップ | 説明 |
|---|---|
| 10 | PCF から受信した課金ポリシーに基づいて、SMF + PGW-C は CHF に対する NCHF 統合課金の作成手順を開始します。この手順は、PCF から受信した課金ルールに基づいています。 |
| 11 | S-GW はセッション作成応答を MME に送信します。 |
| 12 | MME は、N1 Attach Accept メッセージとともに初期コンテキスト設定要求を eNodeB に送信します。 |
| 13 | eNodeB と UE は RRC 構成を実行します。 |
| 14 | UE は、直接転送メッセージを eNodeB に送信します。 |
| 15 | eNodeB は、初期コンテキスト設定応答で接続完了メッセージと、eNodeB の TEID を MME に送信します。 |
| 16 | MME は、ベアラー要求の変更を eNodeB TEID とともに S-GW に送信します。 |
| 17 | S-GW は、eNodeB TEID を使用して SMF + PGW-C にベアラー要求の変更を送信します。 |
| 18 | SMF+PGW-C は N4 セッションの変更を実行して、UPF+PGW-U へのデータ パス上の eNodeB TEID を更新します。 |
| 19 | SMF + PGW-C は、ベアラー変更応答を S-GW に送信します。 |
| 20 | S-GW が、ベアラー変更応答を MME に送信します。 |

## *VoLTE* モバイル発信（*MO*）コール作成コール フロー

このセクションでは、VoLTE MO コール作成コール フローを説明します。

*Figure 117: VoWi-Fi MO* コールの作成コール フロー

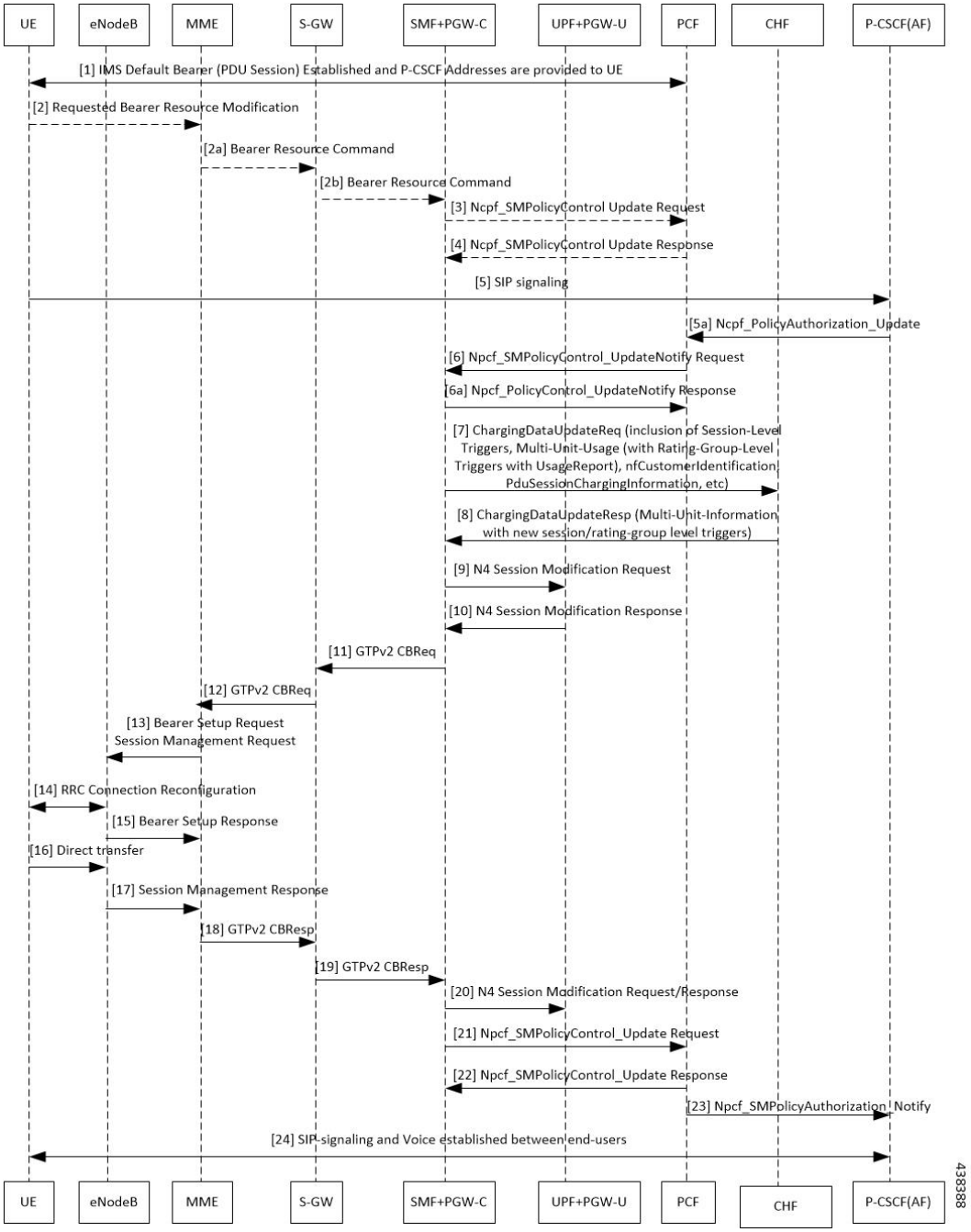


*Table 193: VoWi-Fi MO* コール作成コール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | UE は、PCF を介して IMS デフォルト ベアラーである PDU セッションの確立を要求します。セッションの確立後、UE は PCF から P-CSCF アドレスを受信します。 |
| 2 | UE は、要求されたベアラー リソースの変更情報を MME に送信します。 |
| 2a | MME は、S-GW にベアラー リソース コマンドを送信します。 |
| 2b | S-GW は、SMF + PGW-C にベアラー リソース コマンドを送信します。 |
| 3 | SMF+PGW-C は、NPCF SM ポリシー制御更新要求を PCF に送り返します。 |
| 4 | PCF は、NPCF SM ポリシー制御更新通知リクエストを SMF + PGW-C に送り返します。 |
| 5 | UE は P-CSCF（AF）への SIP シグナリングを開始します。 |
| 5a | P-CSCF は、CHF を介して NPCF ポリシー認可更新メッセージを PCF に送信します。 |
| 6 | PCF は、NPCF SM ポリシー制御更新通知要求を SMF + PGW-C に送信します。 |
| 6a | SMF + PGW-C は、NPCF SM ポリシー制御更新通知応答を PCF に送り返します。 |
| 7 | SMF は、Sm_PolicyControl_UpdateNotify_Request の Charging_Description の一部として受信した Rating-Group-Id を持つ Multi-Unit-Usage を含めて、ChargingDataUpdateReq を送信します。これにより、PCC ルールがインストールされます。 |
| 8 | CHF は、要求されたメッセージで受信した料金設定グループ値のマルチユニット情報を含む ChargingDataUpdateResp を提供します。CHF では、セッション レベルおよび評価グループ値のパラメータの変更も提供されます。 |
| 9 | SMF は、ULPDR の作成と ULFAR の作成を含む N4 セッション変更要求を UPF に送信します。PCC ルールインストールの一部として受け取った SDF と QER 情報を含む ULPDR を作成します。 |
| 10 | UPF は、作成済み ULPDR と作成済み ULFAR を含めて、SMF に対する N4 セッション変更応答で応答します。ULFAR の作成には、専用ベアラー作成のための UPF の UL トンネル情報が含まれます。 |
| 11 | SMF+PGW-C は、S-GW に GTPv2 ベアラー要求の作成を送信します。 |
| 12 | S-GW は、MME に GTPv2 ベアラー要求の作成を送信します。 |
| 13 | MME は、ベアラー セットアップ設定要求とセッション管理要求を eNodeB に送信します。 |
| 14 | RRC 接続再構成は、UE と eNodeB との間で始まります。 |
| 15 | eNodeB は、MME にベアラーのセットアップ応答を送信します。 |
| 16 | UE は、eNodeB へ直接転送を開始します。 |

| ステップ | 説明 |
|---|---|
| 17 | eNodeB が MME にセッション管理応答を送信します。 |
| 18 | MME が S-GW に GTPv2 作成ベアラー応答の更新を送信します。 |
| 19 | S-GW は SMF + PGW-C に GTPv2 ベアラー応答の作成を送信します。 |
| 20 | SMF + PGW-C は、N4 セッション変更要求または、応答を UPF+PGW-U に送信します。 |
| 21 | SMF+PGW-C は、NPCF SM ポリシー制御更新要求を PCF に送り返します。 |
| 22 | PCF は、NPCF SM ポリシー制御更新通知要求を SMF + PGW-C に送り返します。 |
| 23 | PCF は、NPCF ポリシー許可通知要求を P-CSCF（AF）に送信します。 |
| 24 | UE と P-CSCF（AF）を介したエンドユーザー間の SIP シグナリングと音声コールを確立します。 |

**Note**

- PCF が提供する PCC ルールは、新しい専用ベアラーの TFT にマッピングされます。関連付けられた QoS は 4G QoS にマッピングされます。
- NCLF コンバージド課金更新サービスの手順により、すべての Gy および Gz インターフェイス メッセージが置き換えられます。
- 専用ベアラーのユーザー プレーン リソースは、UPF に対する N4 セッション変更手順を通じて追加されます。新しい専用ベアラーの SDF フィルタに PDR、QER、FAR が追加されます。
- SMF + PGW-C は、ベアラー応答の作成で受信した専用ベアラの EBI を保存します。

## *VoLTE* モバイル着信（*MT*）コールの作成コール フロー

このセクションでは、VoLTE MT コール作成コール フローを説明します。

*Figure 118: VoLTE MT* コール作成コール フロー

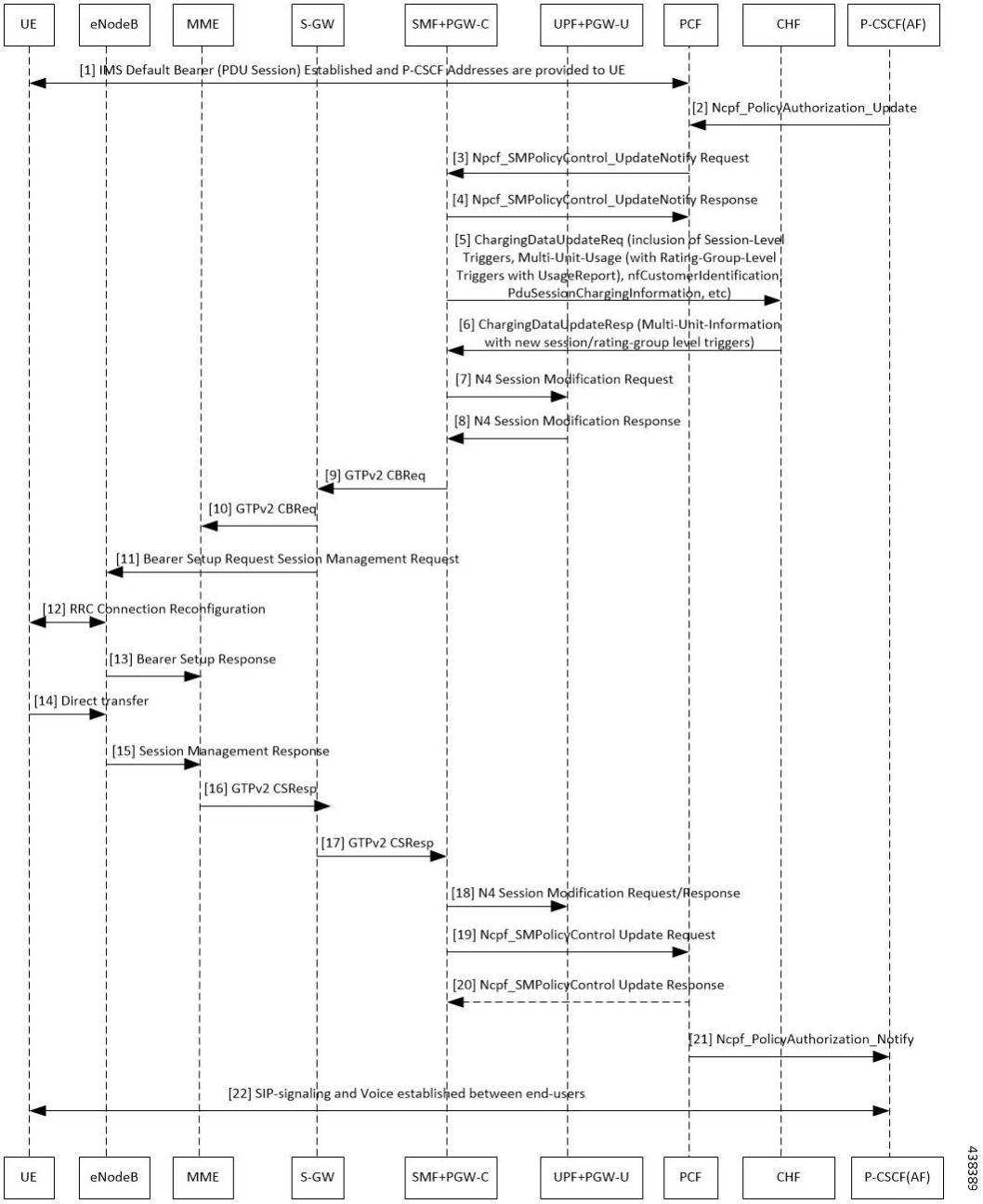



*Table 194: VoLTE MT* コール作成コール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | UE は、PCF を介して IMS デフォルト ベアラーである PDU セッションの確立を要求します。セッションの確立後、UE は PCF から P-CSCF アドレスを受信します。 |

| ステップ | 説明 |
|---|---|
| 2 | P-CSCF（AF）は、NPCF ポリシー許可アップデートを PCF に送信します。 |
| 3 | PCF は、NPCF SM ポリシー制御更新通知リクエストを SMF + PGW-C に送り返します。 |
| 4 | SMF+PGW-C は、NPCF SM ポリシー制御更新通知応答を PCF に送り返します。 |
| 5 | SMF は、Sm_PolicyControl_UpdateNotify_Request の Charging_Description の一部として受信した Rating-Group-Id を持つ Multi-Unit-Usage を含めて、ChargingDataUpdateReq を送信します。これにより、PCC ルールがインストールされます。 |
| 6 | CHF は、要求されたメッセージで受信した料金設定グループ値のマルチユニット情報を含む ChargingDataUpdateResp を提供します。CHF では、セッション レベルおよび評価グループ値のパラメータの変更も提供されます。 |
| 7 | SMF は、ULPDR の作成と ULFAR の作成を含む N4 セッション変更要求を UPF に送信します。PCC ルールインストールの一部として受け取った SDF と QER 情報を含む ULPDR を作成します。 |
| 8 | UPF は、作成済み ULPDR と作成済み ULFAR を含めて、SMF に対する N4 セッション変更応答で応答します。ULFAR の作成には、専用ベアラー作成のための UPF の UL トンネル情報が含まれます。 |
| 9 | SMF+PGW-C は、S-GW に GTPv2 ベアラー作成要求を送信します。 |
| 10 | S-GW は、MME に GTPv2 ベアラー作成要求を送信します。 |
| 11 | MME は、ベアラー セットアップ 設定要求とセッション管理要求を eNodeB に送信します。 |
| 12 | RRC 接続再構成は、UE と eNodeB との間で始まります。 |
| 13 | eNodeB は、MME にベアラーのセットアップ応答を送信します。 |
| 14 | UE は、eNodeB へ直接転送を開始します。 |
| 15 | eNodeB は、MME へセッション管理応答を送信します。 |
| 16 | MME が S-GW に GTPv2 作成ベアラー応答の更新を送信します。 |
| 17 | S-GW は SMF + PGW-C に GTPv2 作成ベアラー応答を送信します。 |
| 18 | SMF + PGW-C は、N4 セッション変更要求または、応答を UPF+PGW-U に送信します。 |
| 19 | SMF+PGW-C は、NPCF SM ポリシー制御更新要求を PCF に送り返します。 |
| 20 | PCF は、NPCF SM ポリシー制御更新通知リクエストを SMF + PGW-C に送り返します。 |
| 21 | PCF は、NPCF ポリシー許可通知要求を P-CSCF（AF）に送信します。 |

| ステップ | 説明 |
|---|---|
| 22 | UE と P-CSCF（AF）を介したエンドユーザー間の SIP シグナリングと音声コールを確立します。 |

# VoLTE および緊急コールの優先順位付けの構成

VoLTE と緊急通話の優先順位付けを設定するには、次の構成を使用します：

```
config
  profile dnn dnn_profile_name ims mark qci qci_value
  end
```

注：

- **mark**：IMS メディアとして標準 QCI 値を作成するために値を指定します。
- **qci** *qci_value*：標準の QoS クラス識別子を指定します。識別子の値は、1 ～ 9 の範囲にする必要があります。デフォルトでは、SMF は QCI 値を 1、2 として IMS と見なします。これらの値を使用して構成すると、デフォルトの動作が上書きされます。

## 設定例

次に設定例を示します。

```
config
  profile dnn dnn1 ims mark qci [1 2]
  end
```

## 設定の確認

IMS セッションの構成を確認するには、次の show running-config コマンドを使用します。

```
show running-config profile dnn dnn1 ims mark qci
```

# 標準準拠

VoLTE サポート機能は、以下の基準に準拠しています：

- *3GPP TS 23.502* バージョン *15.2.0*（*2018-09*）*-5G*、 *5G* システムの手順

# 制限事項

VoLTE サポート機能は、UE によって開始される専用ベアラーの作成をサポートしていません。

# VoLTE および VoNR の NPLI サポート

## 機能説明

SMF は、この 2021.02.0 リリースで VoNR および VoLTE サポート用の PCF に対して NetLoc ユーザーの位置情報、アクセス タイプ、UE タイムゾーンを提供します。

ローミング シナリオでは、hSMF が上記の機能を提供し、関連するコールフローをサポートします。

SMF は、SmPolicyContextData で PCF に NetLoc ビットを送信することにより、PCF へのアクセス ネットワーク情報レポートのサポートを通知します。

PCF は NetLoc 機能がサポートされていることを学習すると、PCC ルールのプロビジョニングを実行し、次のように要求されたアクセス ネットワーク情報の指定（ユーザーの場所やユーザーのタイムゾーン情報）も SMF に提供します。

1. PCF には、1 つ以上の値 MS_TIME_ZONE や USER_LOC_INFO を含む「reqData」属性と、関連する 1 つ以上のインストール済み/変更済み/削除済み PCC ルール識別子を含む「refPccRuleIds」属性を含む「lastReqRuleData」属性が含まれています。
2. 「policyCtrlReqTriggers」属性内で AN_INFO ポリシー制御要求リガーを提供します（まだ設定されていない場合）。
3. 3GPP TS 29.514 [17] または 3GPP TS 29.214 [18] に記載されている予備サービス情報に基づく PCC ルールの場合、PCF はデフォルトの QoS フローの 5QI および ARP を割り当てて、UE へのシグナリングを回避する場合があります。これらの PCC ルールは、「flowInfos」属性内で true に設定された「packetFilterUsage」属性には含まれていません。

PCFがAN_INFOポリシー制御要求トリガを設定し、「lastReqRuleData」属性と「reqData」属性（MS_TIME_ZONEおよび/またはUSER_LOC_INFOの1つ以上の値を含む）を受け取り、さらに「refPccRuleIds」属性に、インストール、変更、または削除が同時に実行された 1 つ以上の PCC ルールに対応する 1 つ以上の PCC ルール識別子を含む場合。

- ユーザーの位置情報が PCF によって要求され、SMF に提供された場合、SMF は「userLocationInfo」属性内のユーザー位置情報と、「userLocationInfoTime」属性内で最後に認識された時刻を提供します（使用可能な場合）。
- ユーザーの位置情報が PCF によって要求され、それが SMF に提供されていない場合、SMF は「servingNetwork」属性内でサービス提供 PLMN 識別子を提供します。
- タイムゾーンが PCF によって要求された場合、SMF は「ueTimeZone」属性を提供します。さらに、SMF は、「repPolicyCtrlReqTriggers」属性内で AN_INFO ポリシー制御要求のトリガも提供します。
- SMF にタイムゾーン情報がなく、PCF が reqData で MS TIME ZONE だけを要求し、AN INFO が policyCtrlReqTriggers でアクティブ化される唯一のトリガである場合、SMF は PCF 更新を開始しません。

SMFは、関連するPCCルールをさらにプロビジョニングまたは削除しない限り、RANから受信した後続のアクセス ネットワーク情報の更新は報告しません。SMF は、関連する QoS フローまたは PDU セッションが解放されない限り、アクセス ネットワーク情報を要求します。

## アーキテクチャ

### コール フロー

このセクションでは、次のコールフローについて説明します。

- VoLTE PDU セッションの作成コール フロー
- VoLTE モバイル発信（MO）コール作成コール フロー
- VoLTE モバイル着信（MT）コールの作成コール フロー

## 標準準拠

VoNR/VoLTE NPLI サポート機能は、次の基準に準拠しています：

- 3GP TS 29.518
- 3GP TS 29.512
- 3GP TS 29.502
- 3GPP TS 23.502

# VoWi-Fi サポート

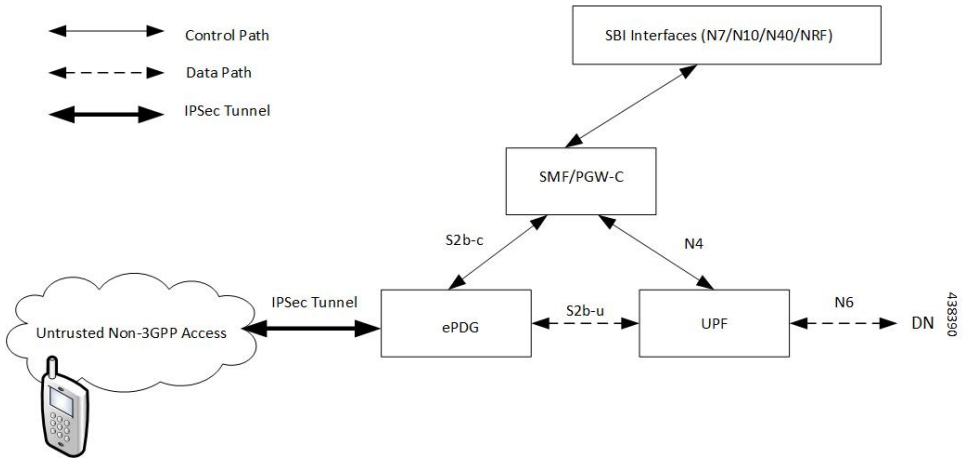
## 機能説明

SMF は Voice over Wi-Fi（VoWi-Fi）をサポートしています。VoWi-Fi テクノロジーは、Wi-Fi ネットワーク経由で接続されているモバイル デバイスから Voice over IP（VoIP）を使用してテレフォニー サービスを提供します。

## アーキテクチャ

ここでは、VoWi-Fi アーキテクチャについて説明します。

*Figure 119: VoWi-Fi アーキテクチャ*




# 機能の仕組み

5Gモバイルデバイスは、音声サービス用の信頼できないWi-Fiネットワークを介して接続し、PGW-CとのPDN接続を確立します。この接続は、UE と拡張パケット データ ゲートウェイ（ePDG）間のインターネット キー エクスチェンジ プロトコル バージョン 2（IKEv2）プロトコルを介して確立されます。PGW-C は、S2b インターフェイスを介して信頼できない Wi-Fi ePDG から GTPv2 セッション要求の作成を受信します。次に、PGW-C は SBI インターフェイスと通信して、デフォルトと専用のベアラーを作成します。SBI インターフェイスは、N7、N10、N40、または NRF インターフェイスにすることができます。

## コール フロー

このセクションでは、次のコールフローについて説明します。

- VoWi-Fi PDU セッション作成コール フロー
- VoWi-Fi モバイル発信（MO）コール作成コール フロー
- VoWi-Fi モバイル着信（MT）コールの作成コール フロー

### VoWi-Fi PDU セッション作成コール フロー

5G コアを介した接続を有効にするために、ePDG または EPS の最初のアタッチは、次のように定義された 3GPP 手順から逸脱します。

- この手順では、SMF + PGW-C が PGW-C の代わりになります。
- SM ポリシーの関連付けの確立手順は、IP-CAN セッションの確立と変更に代わるものです。
- CHF を使用した NCHF インターフェイス経由の統合課金は、Gy および Gz インターフェイスを使用したオンラインおよびオフラインの課金機能に代わるものです。

- ユーザー プレーン ノードとの通信は、Sxb インターフェイスではなく N4 インターフェイスを介して行われます。

以下のコール フローは、VoW-ifi PDU セッションの作成の流れを示しています。

***Figure 120: VoWi-Fi PDU* セッション作成コール フロー**

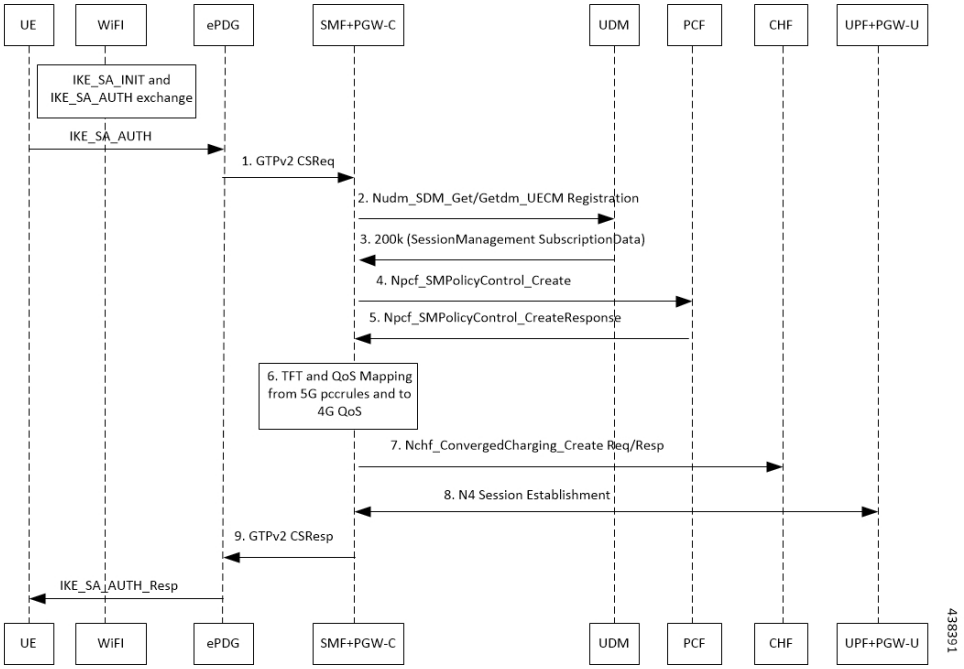



***Table 195: VoWi-Fi PDU* セッション作成コール フローの説明**

| ステップ | 説明 |
|---|---|
| 1 | UE は IKE_SA_INIT と IKE_SA_AUTH の交換を開始します。<br>次に、UE は IKE_SA_AUTH 交換メッセージを ePDG に送信して IPSec トンネルを作成します。 |
| 2 | UE は、APCO IE オプションに「P-CSCF IPv4 または IPv6 要求と DNS IPv4 または IPv6」コンテナ識別子を含めることで、GTP セッション要求の作成として SMF + PGW-C に IKE_SA_AUTH 交換メッセージを送信します。 |
| 3 | SMF + PGW-C は、UE が APCO IE オプションで送信する PDU セッション ID を抽出して保存します。次に、SMF + PGW-C は UDM 登録を実行し、N11 および S2b インターフェイス ID の両方を UDM に送信します。各 DNN の UDM から受信したローカル構成またはセッション管理サブスクリプションデータに基づいて、SMF+PGW-C は「IMS Voice over PS」をサポートすることを決定します。 |

| ステップ | 説明 |
|---|---|
| 4 | SMF+PGW-C は、NPCF SM ポリシー制御作成要求を PCF に送信して、SM ポリシー関連付けの確立手順を開始します。この手順では、PGW-C+SMF は、セッション要求の作成メッセージで受信した情報要素を Npcf_SMPolicyControl_Create サービスに含めます。これらの要素は、次の情報で構成されます。<br>• SUPI には IMSI が含まれています。<br>• DNN には APN が含まれています。<br>• PEI には IMEI-SV が含まれます。<br>• セッション AMBR には APN-AMBR が含まれています。<br>• デフォルトの EPS ベアラー QoS を含むデフォルトの QoS 情報。QCI 値は 5QI 値にマッピングされます。 |
| 5 | PGW-C+SMF は、PCC ルール、PDU セッション ポリシー情報、および 5G QoS 情報を受信します。PCC ルールは EPS QoS 情報にマッピングされます。SMF+PGW-C は、PCC ルールで受信した SDF フィルタから TFT を作成します。次に、SMF+PGW-C は、それらを対応するデフォルトおよび専用のベアラーに関連付けます。 |
| 6 | PCF から受信した課金ポリシーに基づいて、SMF + PGW-C は CHF に対する NCHF 統合課金の作成手順を開始します。この手順は、PCF から受信した課金ルールに基づきます。 |
| 7 | SMF+PGW-C は、UPF+PGW-U の選択と N4 セッションの確立手順を開始します。このセッションは、SMF+PGW-C に接続する 4G セッションであるため、ベアラーごとに個別の CN トンネルが作成されます。また、QoS フロー識別子（QFI）が QoS 適用ルール（QER）およびパケット検出ルール（PDR）で送信されません。 |
| 8 | eSMF+PGW-C はセッション応答の作成を ePDG に送信します。この応答には、デフォルトのベアラーのベアラー情報と TEID が含まれています。 |
| 9 | ePDG が IKE_SA_AUTH 応答を UE に送信します。<br>マッピングされた PCC ルールに応じて、SMF + PGW-C は専用ベアラーの作成を開始できます。 |

## VoWi-Fi モバイル発信（MO）コール作成コール フロー

このセクションでは、VoWi-Fi MO コール作成コール フローを説明します。

*Figure 121: VoWi-Fi MO* コールの作成コール フロー

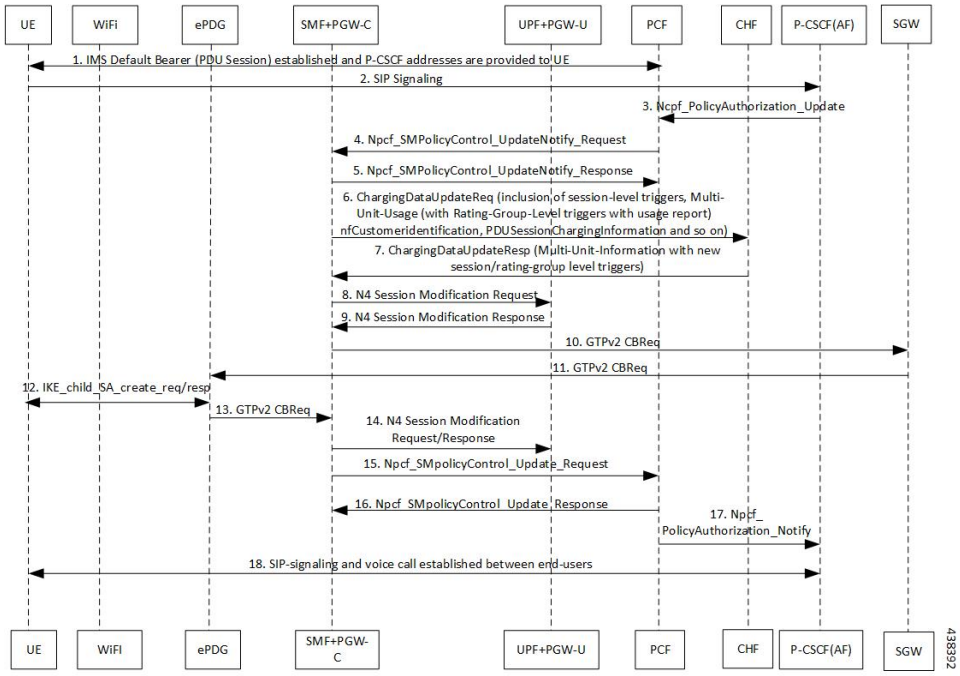



*Table 196: VoWi-Fi MO* コール作成コール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | UE は、PCF を介して IMS デフォルト ベアラーである PDU セッションの確立を要求します。セッションの確立後、UE は PCF から P-CSCF アドレスを受信します。 |
| 2 | UE は P-CSCF（AF）への SIP シグナリングを開始します。 |
| 3 | P-CSCF（AF）は、NPCF ポリシー認可更新メッセージを PCF に送信します。 |
| 4 | PCF は、NPCF SM ポリシー制御更新通知要求を SMF + PGW-C に送信します。 |
| 5 | SMF + PGW-C は、NPCF SM ポリシー制御更新通知応答を PCF に送り返します。 |
| 6 | SMF は、SM Policy Control UpdateNotify 要求の Charging_Description の一部として受信した Rating-Group-Id を持つ Multi-Unit-Usage を含めて、ChargingDataUpdateReq を送信します。これにより、PCC ルールがインストールされます。 |
| 7 | CHF は、要求されたメッセージで受信した料金設定グループ値のマルチユニット情報を含む ChargingDataUpdateResp を提供します。CHF では、セッション レベルおよび評価グループ値のパラメータの変更も提供されます。 |
| 8 | SMF は、ULPDR の作成と ULFAR の作成を含む N4 セッション変更要求を UPF に送信します。作成された ULPDR には、PCC ルールのインストールの一部として受信した SDF と QER 情報が含まれます。 |

| ステップ | 説明 |
|---|---|
| 9 | UPF は、作成済み ULPDR と作成済み ULFAR を含めて、SMF に対する N4 セッション変更応答で応答します。ULFARの作成には、専用ベアラー作成のためのUPFのULトンネル情報が含まれます。 |
| 10 | SMF+PGW-C は、S-GW に GTPv2 ベアラー要求の作成を送信します。 |
| 11 | S-GW は ePDG に GTPv2 ベアラー要求の作成を送信します。 |
| 12 | IKE_ChiLD_SA の交換は、UE と ePDG の間で行われます。 |
| 13 | ePDG は GTPv2 ベアラー応答の作成を SMF + PGW-C に送り返します。 |
| 14 | 確立された N4 セッションは、SMF + PGW-C および UPF + PGW-C の間で変更されます。 |
| 15 | SMF + PGW-C は、NPCF SM ポリシー制御更新要求を PCF に送信します。 |
| 16 | PCF は、NPCF SM ポリシー制御更新応答を SMF + PGW-C に送り返します。 |
| 17 | PCF は、NPCF ポリシー許可通知要求を P-CSCF（AF）に送信します。 |
| 18 | UE と P-CSCF（AF）を介したエンドユーザー間の SIP シグナリングと音声コールを確立します。 |

**Note**

- PCF が提供する PCC ルールは、新しい専用ベアラーの TFT にマッピングされます。関連付けられた QoS は 4G QoS にマッピングされます。
- NCLF コンバージド課金更新サービスの手順により、すべての Gy および Gz インターフェイス メッセージが置き換えられます。
- 専用ベアラーのユーザー プレーン リソースは、UPF に対する N4 セッション変更手順を通じて追加されます。新しい専用ベアラーの SDF フィルタに PDR、QER、FAR が追加されます。
- SMF + PGW-C は、ベアラー作成応答で受信した専用ベアラの EBI を保存します。

## VoWi-Fi モバイル着信（MT）コールの作成コール フロー

このセクションでは、モバイル着信（MT）コール フローについて説明します。

*Figure 122: VoWi-Fi MT* コール作成コール フロー

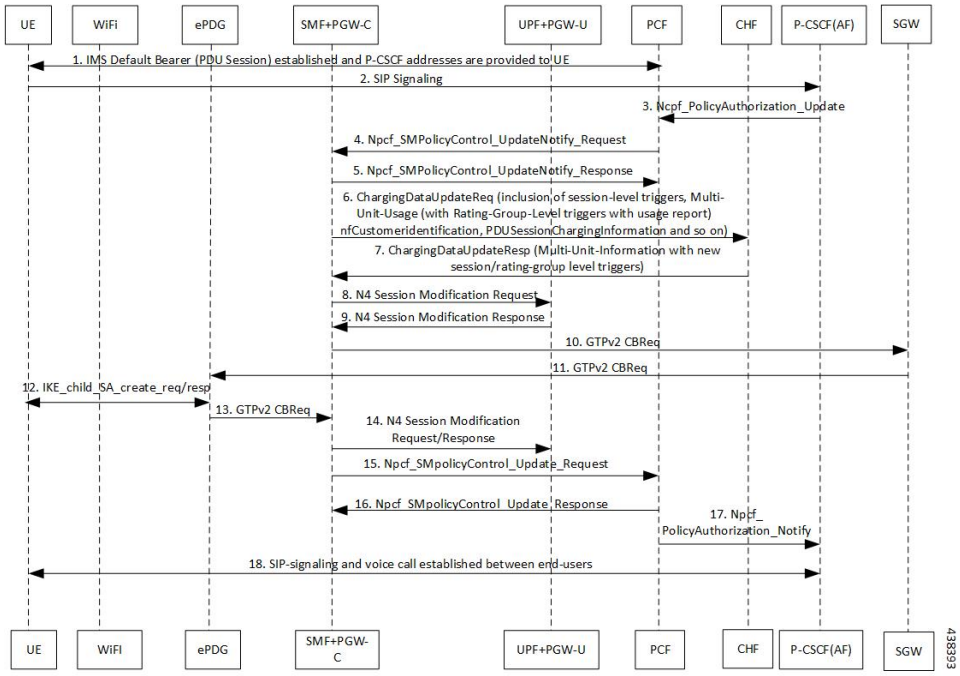



*Table 197: VoWi-Fi MT* コール作成コール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | UE は、PCF を介して IMS デフォルト ベアラーである PDU セッションの確立を要求します。セッションの確立後、UE は PCF から P-CSCF アドレスを受信します。 |
| 2 | UE は、P-CSCF（AF）への SIP シグナリングを開始します。 |
| 3 | P-CSCF（AF）は、NPCF ポリシー認可更新メッセージを PCF に送信します。 |
| 4 | PCF は、NPCF SM ポリシー制御更新通知要求を SMF + PGW-C に送信します。 |
| 5 | SMF + PGW-C は、NPCF SM ポリシー制御更新通知応答を PCF に送り返します。 |
| 6 | SMF は、SM Policy Control UpdateNotify 要求の Charging_Description の一部として受信した Rating-Group-Id を持つ Multi-Unit-Usage を含めて、ChargingDataUpdateReq を送信します。これにより、PCC ルールがインストールされます。 |
| 7 | CHF は、要求されたメッセージで受信した料金設定グループ値のマルチユニット情報を含む ChargingDataUpdateResp を提供します。CHF では、セッション レベルおよび評価グループ値のパラメータの変更も提供されます。 |
| 8 | SMF は、ULPDR の作成と ULFAR の作成を含む N4 セッション変更要求を UPF に送信します。PCC ルールインストールの一部として受け取った SDF と QER 情報を含む ULPDR を作成します。 |

| ステップ | 説明 |
|---|---|
| 9 | UPF は、作成済み ULPDR と作成済み ULFAR を含めて、SMF に対する N4 セッション変更応答で応答します。ULFARの作成には、専用ベアラー作成のためのUPFのULトンネル情報が含まれます。 |
| 10 | SMF+PGW-C は、S-GW に GTPv2 ベアラー要求の作成を送信します。 |
| 11 | S-GW は ePDG に GTPv2 ベアラー要求の作成を送信します。 |
| 12 | IKE_ChiLD_SA の交換は、UE と ePDG の間で行われます。 |
| 13 | ePDG は GTPv2 ベアラー応答の作成を SMF + PGW-C に送り返します。 |
| 14 | 確立された N4 セッションは、SMF + PGW-C および UPF + PGW-C の間で変更されます。 |
| 15 | SMF + PGW-C は、NPCF SM ポリシー制御更新要求を PCF に送信します。 |
| 16 | PCF は、NPCF SM ポリシー制御更新応答を SMF + PGW-C に送り返します。 |
| 17 | PCF は、NPCF ポリシー許可通知要求を P-CSCF（AF）に送信します。 |
| 18 | UE と P-CSCF（AF）を介したエンドユーザー間の SIP シグナリングと音声コールを確立します。 |

### 標準準拠

VoWi-Fi サポート機能は、以下の基準に準拠します：

- 3GPP TS 23.502 V15.2.0（2018-09）

### 制限事項

VoWi-Fi サポート機能には、次の制限があります：

- UE 開始の専用ベアラーの作成はサポートされていません。

# 音声の新しいラジオ

## 機能説明

New Radio (NR) は 5G 無線アクセス技術であり、Voice over NR (VoNR) は 5G ネットワークを介した音声またはビデオです。VoNRは、5Gネットワーク向けのターゲット音声またはビデオ通信ソリューションです。

5GS over NG-RAN の通話サービスは、引き続き Voice over LTE（VoLTE）などの IP マルチメディア サブシステム（IMS）に基づいています。VoNR は、5GS が IMS コアに接続されている場合にのみサポートされます。

**P-CSCF サーバ アドレスの解決**

SMF は、**DNS プロキシ**または P-CSCF プロファイルで定義された**ローカル構成**のいずれかを使用して、P-CSCF サーバのアドレスを解決します。SMF は、ドメイン名を解決、リモート DNS サーバから IP アドレスを受信、そしてサブスクライバに IP アドレスを送信するためのオプションを一つ使用します。

**Note** ローカル構成は、 4G と 5G の両方に適用されます。

## 標準準拠

この VoNR 機能は、以下の基準に準拠しています：

- *3GPP TS 23.228*、リリース *15.3.0*
- *3GPP TS 23.501*、リリース *15.4.0*
- *3GPP TS 23.502*、リリース *15.4.0*

# DNS プロキシを使用したアドレス解決

## 機能説明

ドメイン ネーム システム（DNS）は、数値の IP アドレスを読み取り可能な階層型のインターネット アドレスに（またはその逆に）変換するサーバーのネットワークです。ドメイン ネーム システム（DNS）プロキシを使用して、ホスト名を IP アドレスに解決するために 1 つ以上のプロキシ サーバーを構成できます。ドメイン ネーム システム（DNS）プロキシは SMF 内に配置されます。

ホスト名を照会すると、SMF はドメイン ネーム システム（DNS）プロキシ サーバーを介して構成済みの DNS サーバーに DNS クエリーを送信して、最大 2 つの P-CSCF IP アドレスを取得します。解決された IP アドレスがドメイン ネーム システム（DNS）クライアントに送り返されます。この操作は、P-CSCF の完全修飾ドメイン名（FQDN）の解決に役立ちます。SMF では、P-CSCF プロファイル内で FQDN を構成できます。

## アドレス解決のための DNS プロキシの構成

ここでは、P-CSCF アドレス解決のために DNS プロキシを構成する方法について説明します。

DNS プロキシの構成には、次の手順が含まれます：

1. P-CSCF FQDN の構成, on page 613

2. SMF での DNS プロキシ レプリカの構成
3. SMF での DNS プロキシの構成

## P-CSCF FQDN の構成

SMF では、P-CSCF プロファイルでドメイン名を構成できます。DNS は、ドメイン名を解決し、リモート DNS サーバから IP アドレスを取得し、その IP アドレスをサブスクライバに提供するために使用されます。

P-CSCF の FQDN を定義するには、次の構成例を使用します。

```
config
   profile pcscf pcscf_profile_name
      fqdn domain_name
      end
```

注：

- **pcscf-profile** *pccf_profile_name*：P-CSCF プロファイル名を指定し、P-CSCF プロファイル コンフィギュレーション モードを開始します。 *pccf_profile_name* は英数字の文字列である必要があります。
- **fqdn** *domain_name*：P-CSCF サーバの FQDN を指定します。 *domain_name* は英数字の文字列である必要があります。

機能の設定の確認

次の show コマンドを使用して P-CSCF FQDN 機能構成の詳細を認証します。

**show running-config**

次に、この show コマンドの出力例を示します：

```
profile pcscf pcscf1
 fqdn cisco.com
exit
```

## DNS プロキシ レプリカの構成

DNS プロキシ レプリカを構成するには、次の構成例を使用します。

```
config
   instance instance-id gr_instance_id
      endpoint dns-proxy replicas replica_value
      commit
```

注：

- **endpoint dns-proxy replicas** *replica_value*：ノードあたりの DNS プロキシポッドの複製数を指定します。

  *replica_value* が 整数である必要があります。
- **commit**：構成を保存します。

## DNS プロキシの構成

SMF の DNS プロキシ機能を構成するには、次の構成例を使用します。

```
config
   profile dns-proxy
      cache-ttl dns_response_ttl_value
      query-type { ipv4v6 | ipv4 | ipv6 }
      servers dns_server_name
         ip server_ip_address
         port server_port
         priority server_priority
         protocol { tcp | udp }
      timeout dns_timeout_value
      commit
```

注：

- **profile dns-proxy**：DNS プロキシ構成モードを開始します。
- **cache-ttl** *dns_response_ttl_value*：キャッシュ内の DNS 応答の TTL 値（秒単位）を指定します。 *dns_response_ttl_value* は 、60 ～ 86400 の範囲の整数である必要があります。
- **query-type**：DNS クエリ タイプを指定します。
- **servers** *dns_server_name*：DNS サーバーの名前を指定します。たとえば、serv1。
  - **ip** *server_ip_address*：DNS サーバーの IP アドレスを指定します。
  - **port** *server_port*：DNS サーバーのポートを指定します。

    *server_port* は 1 ～ 65535 の範囲の整数である必要があります。
  - **priority** *server_priority*：DNS サーバーの優先順位を指定します。

    13*server_priority* は、1 ～ 100 の範囲の整数である必要があります。
  - **protocol**：DNS サーバーのプロトコ ルタイプを TCP または UDP として指定します。
- **timeout** *dns_timeout_value*：DNS タイムアウト値（ミリ秒単位）を指定します。
  *dns_timeout_value* は 、200 ～ 10000 の範囲の整数である必要があります。

  *dns_timeout_value* は 整数である必要があります。
- **commit**：構成を保存します。

## DNS プロキシの構成の確認

この項では、DNS プロキシ機能構成を確認する方法について説明します。

**show running-config profile dns-proxy** コマンドを使用して、DNS プロキシ機能の構成を確認します。

次に、2 つの DNS サーバ（serv1 と serv2）を構成した **show running-config profile dns-proxy** コマンドの出力例を示します。

```
query-type ipv4
timeout 205
servers serv1
round-robin-answers
randomise-answers

servers serv1
 ip 209.165.200.240
 port 53
 protocol tcp
 priority 1
exit
servers serv2
 ip 209.165.200.241
 port 20
 protocol udp
 priority 2
exit
```

## DNS からの P-CSCF アドレスのランダム化

SMF サービスでは、解決されたホストのランダムな選択がサポートされています。DNS 解決でホストの IP アドレスのセットが得られ、 **randomize-answers** CLI が DNS プロキシ プロファイルの構成で有効になっている場合、DNS ルックアップはランダムに IP アドレスを選択します。アドレスの選択は、ランダム化を保証する整数の疑似ランダム順列に基づいています。

**randomize-answers** CLI が有効になっている場合、特定のホストのすべての DNS クエリが異なるセットの IP アドレスを返します。これは、IPv4 と IPv6 の両方のアドレスに適用されます。

DNSプロキシプロファイルの選択方法は、ラウンドロビンまたはランダム化のいずれかです。

例：

**randomize-answers** が有効になっている 5 つの IP アドレスのサブセットを取得する DNS ルックアップの場合。

Host1 = *{ "209.165.200.226", "209.165.201.2", "209.165.201.3", "209.165.201.4", "209.165.201.5", "209.165.201.6", "209.165.201.7", "209.165.201.8", "209.165.201.9", "209.165.201.10" }*

最初のルックアップ： *[209.165.201.5 209.165.200.226 209.165.201.9 209.165.201.2 209.165.201.7]*

2 番目のルックアップ： *[209.165.201.8 209.165.201.6 209.165.201.2 209.165.201.3 209.165.201.9]*

3 番目のルックアップ： *[209.165.201.7 209.165.201.5 209.165.201.2 209.165.201.4 209.165.201.9]*

### P-CSCF アドレスのランダム選択に DNS を構成する

SMF では、ランダム化またはラウンドロビン方式のいずれかで、解決されるホストの選択がサポートされます。

P-CSCF アドレスを選択するための DNS を構成するには、次の構成例を使用します：

```
config
   profile dns-proxy
      randomize-answers
      round-robin-answers
      end
```

注：

- **randomize-answers**：ランダム選択方式によってアドレスを取得するための DNS を有効にします。
- **round-robin-answers**：ラウンドロビン選択方式によるアドレス取得の DNS を有効にします。

# DNS テスト クエリ

## 機能説明

SMF は、完全修飾ドメイン名（FQDN）を使用して P-CSCF IP アドレスを照会および確認する DNS テスト クライアントをサポートしています。DNS テストクライアントは、VoNR 起動用のデバッグ ユーティリティとして使用できます。SMF は、SMF Ops Center CLI からの DNS テスト クエリの実行をサポートしています。DNS テスト クライアントは、DNS プロキシを介して DNS サーバと対話して、テスト クエリ結果を取得します。DNS クライアントは、取得した結果をユーザーに表示します。

テスト DNS クライアントは、次のエラー シナリオを管理し、ユーザーに適切な IPv4 または IPv6 応答を提供します。

- クエリ タイムアウト
- DNS プロキシの障害/エラー
- 無効な応答処理

## 機能の仕組み

DNS プロキシは DNS 要求を DNS サーバに送信します。DNS プロキシ サーバは DNS サーバから応答を受信し、OAM ポッドから実行されている DNS テスト クライアントに送信します。CLI に応答が表示されます。

タイムアウト値は、DNS プロキシと対話するときに使用されます。データの基本的な検証は、SMF Ops Center CLI に送信する前に、DNS クライアントで実行されます。

DNS 応答には、指定された FQDN のプライマリおよびセカンダリ IPv4 または IPv6 アドレスが含まれます。DNS クライアントは、これに応じて応答データを処理します。

**重要** DNS クライアントは、キャッシュなしでの DNS クエリの送信（ダイレクト ヒット DNS サーバ）をサポートしていません。DNS プロキシではサポートされません。

## DNS テスト クエリの構成

DNS テスト クライアントは、FQDN を使用して P-CSCF IP アドレスをクエリおよびチェックします。

DNS テストクエリを構成するには、次のコマンドを使用します。

**test dns-query [ fqdn** *fqdn_name* **| num-ipv4** *ipv4_address_num* **| num-ipv4v6** *ipv4v6_address_num* **| num-ipv6** *ipv6_address_num* **]**

**注**：

- **test dns-query**：テスト FQDN 解決を実行します。
- **fqdn** *fqdn_name*：DNS クエリを送信する必要があるノードの FQDN を指定します。

  *fqdn_name* は、1 ～ 30 文字の英数字の文字列である必要があります。
- **num-ipv4** *ipv4_address_num*：DNS クエリに使用する IPv4 アドレスの数を指定します。

  *ipv4_address_num* は 1 ～ 9 の範囲の整数である必要があります。
- **num-ipv4v6** *ipv4v6_address_num*：DNS クエリに使用される IPv4v6 アドレスの数を指定します。

  *ipv4v6_address_num* は 1 ～ 9 の範囲の整数である必要があります。
- **num-ipv6** *ipv6_address_num*：DNS クエリに使用される IPv6 アドレスの数を指定します。

  *ipv6_address_num* は 1 ～ 9 の範囲の整数である必要があります。

## 設定の確認

この項では、DNS テスト クエリの構成を確認する方法について説明します。

**show dns query** コマンドを使用して、DNS テスト クエリの構成を確認します。

**show dns query** コマンドの出力例を次に示します。

```
smf# show dns-query fqdn smf.com
dns-summary
Hostname : smf.com,
IPv4Addr : [209.165.200.228,
209.165.200.229,
209.165.200.230],
IPv6Addr : [::1,
::3,
::2]

smf# show dns-query fqdn smf.comnum-ipv4 1

dns-summary
Hostname : smf.com,
IPv4Addr : [209.165.200.228],
IPv6Addr : []

[smf] smf# show dns-query fqdn hello.comnum-ipv4v6 4
dns-summary
Hostname : hello.com,
IPv4Addr : [209.165.200.235,
209.165.200.236,
209.165.200.237,
209.165.200.238],
IPv6Addr : [2001:DB8::1,
2001:DB8::2,
2001:DB8::3,
2001:DB8::4]
```

# ローカル構成を使用したアドレス解決

UE が P-CSCF 検出を要求すると、SMF は DNN 構成から P-CSCF アドレスを取得します。これらは、IMS サポートおよび P-CSCF アドレスまたは P-CSCF FQDN のリストを使用する DNN の下でローカルにプロビジョニングされます。

現在、P-CSCF IPv4 アドレスと IPv6 アドレスの両方に対して最大 64 のアドレス リストのみを構成できます。

## P-CSCF アドレスの選択メカニズム

ローカル構成は、プライマリ、セカンダリ、およびターシャリ P-CSCF サーバの IP アドレスを含む P-CSCF アドレス セットで構成されます。このような複数の IPv4、IPv6、または混合 IP アドレス セットを構成できます。各アドレス セットには優先順位の値があります。

SMF は、P-CSCF アドレスの選択に関してラウンドロビン方式のみをサポートしています。通常のコールまたは緊急コールに基づいて選択されるアドレスの数を定義できます。

ローカル構成からアドレスを選択する場合、SMF はアドレス セットの優先順位値に従って P-CSCF サーバ アドレスを選択し、それらを UE に送信します。

選択されているアドレス セットに定義済みの数の P-CSCF サーバ アドレスが構成されていないか、一部がダウンとしてマークされている場合、SMF はそのセット内で構成されて機能するアドレスを同じ数だけ選択します。SMF は、後続のセットから残りのアドレス数を選択しません。

選択したセット内のアドレスが設定されていないか、ダウンとしてマークされている場合にのみ、SMF は次のアドレスが設定されているアドレス セットに移動します。

### SMF による P-CSCF アドレス選択の実行方法

サービス提供している PLMN AMF は、登録手順中に UE に対して通知を送信し、3GPP アクセス ネットワークで IMS Voice over PS セッションがサポートされているかどうかを示します。3GPP アクセスを介した「IMS voice over PS」音声機能を持つ UE は、音声ドメイン選択を実行するときに、この指示を考慮します。

UE は、AMF で P-CSCF コンテナ オプションを設定することにより、PDU セッション確立要求に拡張プロトコル構成オプション（ePCO）IE を含めます。さらに、AMF は、SM コンテキスト作成要求でこれらの ePCO IE オプションを SMF に転送します。SMF は、IMS 関連のデータを維持する DNN プロファイルに基づいて P-CSCF アドレスを取得します。SMF は、PDN タイプと要求された P-CSCF コンテナ値に従って、AMF への N1N2 メッセージ転送に P-CSCF IPv4 アドレスと IPv6 アドレスを含めます。

**Important** UE が ePCO IE の P-CSCF コンテナ オプションを設定していない場合、SMF には P-CSCF アドレスは含まれません。

### 通常コール中の P-CSCF アドレス選択

通常の通話中に、SMF は IMS DNN から P-CSCF アドレスを取得します。デフォルトでは、SMF はローカル構成から UE に 3 つの P-CSCF アドレスを送信します。

## アドレス解決のための P-CSCF サーバの構成

P-CSCF サーバの構成には、次の手順が含まれます：

手順

**ステップ 1** P-CSCF サーバ構成の P-CSCF プロファイルの作成
**ステップ 2** P-CSCF サーバ パラメータの定義
**ステップ 3** DNN プロファイル構成で P-CSCF プロファイルの定義 （621 ページ）

### P-CSCF プロファイルの作成

このタスクは、P-CSCF サーバを構成するための P-CSCF プロファイルを作成するのに役立ちます。

手順

**profile pcscf** *pccf_profile_name* コマンドを使用して、P-CSCF プロファイル インスタンスを作成します。

例：

```
[smf] smf# config
[smf] (config)# profile pcscf pcscf1
[smf] (config-pcscf-pcscf1)#
```

#### 次のタスク

P-CSCF プロファイルを作成したら、次のタスクを実行する必要があります。

- FQDN、サーバ選択方法、アドレス数、IPv4 または IPv6 P-CSCF アドレスのセットなどの P-CSCF サーバ パラメータを定義します。
- P-CSCF プロファイルと DNN プロファイルの関連付け。

### P-CSCF サーバ パラメータの定義

このタスクは、P-CSCF サーバを構成するためのパラメータを定義するのに役立ちます。

### 始める前に

P-CSCF プロファイル インスタンスを作成します。

### 手順

**ステップ 1** **fqdn** *domain_name* コマンドを使用して、P-CSCF サーバの完全修飾ドメイン名（FQDN）を指定します。

例：

```
[smf] (config-pcscf-pcscf1)# fqdn cisco.com
```

FQDN が構成されている場合、SMF は DNS プロキシから P-CSCF アドレスを選択します。FQDN が構成されていないか、DNS プロキシにアクセスできない場合、SMF はローカル構成から P-CSCF サーバ アドレスを選択します。

**ステップ 2** **pcscf-selection round-robin** コマンドを使用して、P-CSCF サーバの選択方法を構成します。

例：

```
[smf] (config-pcscf-pcscf1)# pcscf-selection round-robin
```

**ステップ 3** **v4-list | v6-list | v4v6-list** コマンドを使用して、構成された P-CSCF プロファイルの下に IPv4、IPv6 または IPv4v6 アドレス リストを構成します。

例：

```
[smf] (config-pcscf-pcscf1)# v4-list | v6-list | v4v6-list
```

**ステップ 4** **precedence** *precedence_value* コマンドを使用して、IP アドレスリストを選択するための優先順位を構成します。また、**{ primary** *server_ipv4_address* | *server_ipv6_address* | **secondary** *server_ipv4_address* | *server_ipv6_address* | **tertiary** *server_ipv4_address* | *server_ipv6_address* **}** コマンドを使用して、プライマリ、セカンダリ、およびターシャリの P-CSCF の IP アドレスを指定します。

例：

```
[smf] (config-pcscf-pcscf1)# v6-list
                             precedence 1
                             primary fd00:976a:c004:1938::5
                             secondary fd00:976a:b699:4901::5
                             tertiary fd00:976a:b699:4901::7
```

- **precedence** *precedence_value* の値は、1 ～ 64 の整数である必要があります。
- **{ primary** *server_ipv4_address* | *server_ipv6_address* | **secondary** *server_ipv4_address* | *server_ipv6_address* | **tertiary** *server_ipv4_address* | *server_ipv6_address* では **}**、プライマリ、セカンダリ、およびターシャリの IPv4/IPv6 アドレスを構成できます。

**ステップ 5** 現在のコンフィギュレーション モードを終了して、**exit** コマンドを使用して以前のコンフィギュレーション モードに戻ります。

例：

```
[smf] smf# config
[smf] (config)# profile pcscf pcscf1
```

```
[smf] (config-pcscf-pcscf1)# fqdn cisco.com
[smf] (config-pcscf-pcscf1)# server-cnt-ue 2
[smf] (config-pcscf-pcscf1)# pcscf-selection round-robin
[smf] (config-pcscf-pcscf1)# v6-list
                              precedence 1
                               primary fd00:976a:c004:1938::5
                               secondary fd00:976a:b699:4901::5
                               tertiary fd00:976a:b699:4901::7
[smf] (config-pcscf-pcscf1)# exit
```

### 次のタスク

P-CSCF サーバのパラメータを構成したら、P-CSCF プロファイルを DNN プロファイルに関連付けます。

## DNN プロファイル構成で P-CSCF プロファイルの定義

このタスクにより、P-CSCFプロファイルをDNNプロファイルに関連付けることができます。

### 始める前に

P-CSCFプロファイルをDNNプロファイルに関連付ける前に、次の手順を実行する必要があります：

- P-CSCF プロファイルを構成します。
- P-CSCF サーバ パラメータの定義

### 手順

**ステップ 1** **profile dnn** *dnn_profile_name* コマンドを使用して、グローバル構成モードで DNN プロファイル インスタンスを構成します。

例：

```
[smf] smf#config
[smf] (config)#profile dnn dnntst1
[smf] (config-dnn-dnntst1)#
```

**ステップ 2** コマンド **pcscf-profile** *pccf_profile_name*を使用して、設定済みのDNNプロファイルの下にP-CSCFプロファイルを定義します。

例：

```
[smf] (config-dnn-dnntst1)#pcscf-profile pcscf1
```

**ステップ 3** **exit** コマンドを使用して、DNN コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。

例：

```
[smf] (config-dnn-dnntst1)#exit
```

# P-CSCF アドレスの再選択と復元

表 *198 :* 機能の履歴

| 機能名 | リリース情報 | 説明 |
|---|---|---|
| P-CSCF アドレスの復元と再選択 | 2024.02.0 | SMF は、P-CSCF 障害イベントが発生した場合に、P-CSCF アドレスの復元と再選択をサポートします。P-CSCF アドレス再選択の構成には、CLI **pcscf-restoration trigger [ UDM ] [ action [ mark-down ] ]** を使用します。<br>この機能により、5G/4G/Wi-Fi RAT サブスクライバは、動作中の P-CSCF アドレスに接続することで、障害が発生した UE との IMS 接続を復元できます。<br>**デフォルト設定** 無効：有効にするには構成が必要です。 |

## 機能説明

SMF は、P-CSCF 障害イベントが発生した場合に、P-CSCF アドレスの復元と再選択を可能にします。このメカニズムは、UE がコールを受信したものの、P-CSCF アドレスの失敗によりそのコールが IMS に接続できない場合に実行されます。

SMF は、UE に P-CSCF アドレスを提供します。S-CSCF（Serving-CSCF）が P-CSCF の障害を検出した場合、UDM に通知します。UDM はその後、P-CSCF 復元指示を SMF に送信します。次に、IMS PDU セッションの更新手順または IMS PDU セッションの再確立を開始して、P-CSCF 再選択プロセスをトリガします。

## 機能の仕組み

このセクションでは、P-CSCF アドレス再選択プロセスに関する詳細について説明します。

### P-CSCF の復元と再選択のコール フロー

次のコール フローは、P-CSCF の復元と再選択のプロセスを示しています。

図 *123 : P-CSCF* の復元と再選択のコール フロー

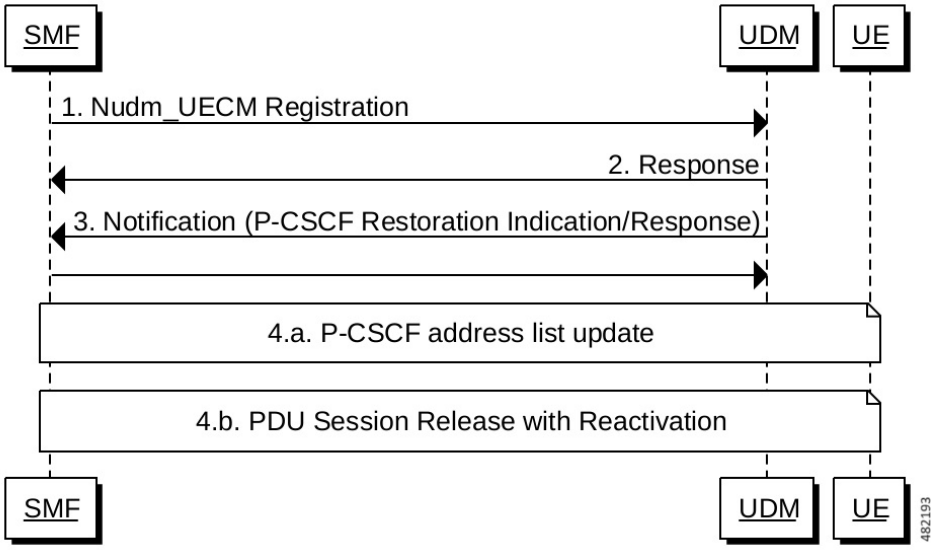



表 *199 : P-CSCF* の復元と再選択のコール フロー説明

| ステップ | 説明 |
|---|---|
| 1. | SMF は、UDM に対して Nudm_UECM 登録要求を開始します。SMF は、P-CSCF 再選択が構成によって有効になっている場合、DNN に関係なく、N10 登録要求に pccfRestorationCallbackUri IE を含めます。 |
| 2. | UDM は、Nudm_UECM 登録要求への応答として SMF に登録されます。 |
| 3. | UDM が P-CSCF の障害について学習すると、コールバック URI をトリガーして、障害イベントについて SMF に知らせます。UDM が、failedPcscf IE を含む P-CSCF 復元通知を SMF に送信します。<br>SMF は、セッション中の UE に送信された P-CSCF アドレスを保存します。SMF は、UDM からの P-CSCF 復元通知で受信した Mw インターフェイスアドレスから、機能不全な P-CSCF の Gm インターフェイス アドレスを取得します。<br>UE が ePCO で「P-CSCF 再選択のサポート」を示している場合、SMF は PDU セッションを変更します。それ以外の場合ははPDUセッションを解放します。 |

| ステップ | 説明 |
|---|---|
| 4.a. | SMF は、機能不全な P-CSCF アドレスをセッション中の P-CSCF アドレス リストと比較します。一致が見つかった場合、SMF は P-CSCF アドレスリストを再選択します。<br><br>P-CSCF アドレスがローカルに設定されている場合、SMF は、失敗した P-CSCF アドレスを除く、構成に基づいて新しい P-CSCF アドレスのセットを選択します。PCSCF FQDN がローカルに設定されている場合、SMF は DNS を使用して、失敗した P-CSCF アドレスを除く P-CSCF アドレスの新しいセットを取得します。<br><br>UE が EUTRA/Wi-Fi RAT にある場合、SMF は新しい P-CSCF リストを使用して UE に ePCO/aPCO を使用して UBR をトリガーします。UE が NR RAT にある場合、SMF は、新しい P-CSCF リストを含む UE への ePCO の N1 変更コマンドを使用した N11 インターフェイスで N1N2 メッセージをトリガーします。割り当てられたセットの下のすべての P-CSCF アドレス（プライマリ、セカンダリ、およびターシャリ）がダウンとマークされている場合にのみ、P-CSCF アドレスの代替セットが選択されます。<br><br>**action** が構成モードの P-CSCF プロファイルで **mark-down** として構成されている場合、SMF は、失敗した P-CSCF サーバーを到達不能としてマークして、このサーバーが新しいセッションに選択されないようにします。 |
| 4.b. | SMF は、次のシナリオで PDU セッションの解放をトリガーします：<br><br>• P-CSCF 復元通知が failedPcscf IE なしで受信された場合。<br><br>• UE に ePCO での「P-CSCF Re-selection」のサポートが示されていない場合。<br><br>SMF は、UE が NR RAT にある場合、すべてのリリース ケースで「再アクティブ化が必要」の理由で N1 リリースをトリガーします。SMF は、UETRA/Wi-Fi RAT の場合、すべてのリリース ケースに対して「再アクティブ化要求（reactivation requested）」という原因で DBR をトリガーします。 |

## P-CSCF の復元と再選択の構成

P-CSCF の復元と再選択を有効にするには、次の構成例を使用します。

```
config
  profile pcscf pcscf_profile_name
    pcscf-restoration trigger [ UDM ] [ action [ mark-down ] ]
    pcscf-selection round-robin
    fqdn domain_name
    v4-list  | v6-list
      precedence precedence_value
        primary server_ipv4_address | server_ipv6_address
        secondary server_ipv4_address | server_ipv6_address
        tertiary server_ipv4_address | server_ipv6_address
        end
```

```
    end
  end
```

注：

- **pcscf-restoration trigger [ UDM ] [ action [ mark-down ] ]**： UDM がトリガする P-CSCF の復元と再選択を有効にします。 **[ action [ mark-down ]** はオプションです。構成する場合、オプションとして指定できるのは**[ mark-down ]**のみです。アクションが「mark-down」として構成され、新しいセッションで選択されていない場合、SMF は失敗した P-CSCF を到達不能としてマークします。

### 設定例

次に、P-CSCF の復元と再選択の構成例を示します。

```
profile dnn ims1
    pcscf-profile PCSCF_restoration_fqdn_profile
    exit
profile pcscf PCSCF_restoration_fqdn_profile
    pcscf-selection round-robin
    fqdn ims1.com
    pcscf-restoration
    trigger UDM
    action mark-down
    exit
   exit
exit
```

## Gm および Mw インターフェイスのマッピング構成

P-CSCF 復元プロセスの Gm インターフェイスと Mw インターフェイスをマッピングするには、次の構成例を使用します。

```
config
  profile interface-mapping default
  interface [ GM ] [ ipv4  ipv4_address | ipv6 ipv6_address ] interface [ MW
 ] [ ipv4  ipv4_address | ipv6 ipv6_address ]
  end
```

注：

- **profile interface-mapping default**：Gm および Mw インターフェイスのマッピングを有効にします。
- **interface [ GM ] [ ipv4** *ipv4_address* **| ipv6** *ipv6_address* **] interface [ MW ] [ ipv4** *ipv4_address* **| ipv6** *ipv6_address* **]**：Gm IPv4/IPv6 アドレスを Mw IPv4/IPv6 アドレスにマッピングします。

### 設定例

次に、Gm および Mw インターフェイスをマッピングするための構成例を示します：

```
profile pcscf-interface-mapping default
    interface GM ipv4 209.165.200.220 interface MW ipv4 209.165.200.222
```

```
    interface GM ipv4 209.165.200.221 interface MW ipv4 209.165.200.223
    interface GM ipv6 fd00:976a::9 interface MW ipv6 fd00:976a::10
exit
```

# 失敗した P-CSCF をオンラインにマークする構成

失敗した P-CSCF アドレスをオンラインとしてマークするには、次の構成例を使用します。

**pcscf mark-online [ all | fqdn** *fqdn* **| mw-ipv4** *IPv4_address* **| mw-ipv6** *IPv6_address* **]**

- **pcscf mark-online [ all | fqdn** *fqdn* **| mw-ipv4** *IPv4_address* **| mw-ipv6** *IPv6_address* **]**：失敗した P-CSCF アドレスをオンラインとしてマークできます。次の 4 つの値が考えられます：
  - **all**：このコマンドは、すべての P-CSCF アドレスをオンラインにマークします。
  - **fqdn** *fqdn*：このコマンドは、オンラインとしてマークする FQDN を指定します。
  - **mw-ipv4** *IPv4_address*：このコマンドは、オンラインとしてマークする失敗した P-CSCF IPv4 アドレスを指定します。
  - **mw-ipv6** *IPv6_address*：このコマンドは、オンラインとしてマークする失敗した P-CSCF IPv6 アドレスを指定します。

### 設定例

次に、失敗した P-CSCF アドレスをオンラインとしてマークする構成例を示します：

```
[smf] smf# pcscf mark-online mw-ipv4 "209.165.200.220"
Thu Feb 15 18:44:27.257 UTC+00:00
result
Failed IP is marked online
209.165.200.220
[smf] smf# pcscf mark-online mw-ipv6 "fd00:976a::9"
Thu Feb 15 18:44:27.297 UTC+00:00
result
Failed IP is marked online
fd00:976a::9
```

# OAM サポート

この項では、P-CSCF の復元および再選択機能でサポートされているメトリックスと統計情報について説明します。

### バルク統計

次の新しいラベルが **smf_service_stats**に追加されました。

- **pccf_restoration_init_mod**：このラベルは、5G、4G または Wi-Fi セッション変更手順中の P-CSCF 復元を示します。
- **smf_req_pccf_restoration_rel**：このラベルは、5G セッション中の P-CSCF リリースを示します。

- **pccf_restore_pdn_sess_rel**：このラベルは、4G および Wi-Fi セッション中の P-CSCF リリースを示します。
- **PcscfAddressNotFound**：このラベルは、P-CSCF 復元手順の失敗の理由を示しています。

次の新しい統計情報が SMF ノード マネージャ統計カテゴリに追加されました。

**nodemgr_pccf_cache_stats**：この統計情報は、P-CSCF キャッシュ管理を示します。

- **pccf_address_req_type**：このラベルは、アドレスがオンライン/オフラインとしてマークされているかどうかを示す P-CSCF アドレスを示します。
- **pccf_mw**： このラベルは、P-CSCF アドレスの IP アドレスを示します。

次の新しいラベルがSMF 切断統計カテゴリの下に追加されます：

- **disk_pccf_restoration**：このラベルは、コールの切断に関連付けられている理由を示しています。

### show コマンドの出力

次の show コマンドを使用して、失敗した P-CSCF アドレスを表示します。

```
[smf] smf# show pcscf failed-address peers

["209.165.200.220","209.165.200.221","fd00:976a::9"]
```

# VoNR MO と MT コール サポート

## 機能説明

SMF は、IMS PDU セッション作成後の UE の保証ビットレート（GBR）フローとして、5G QoS 識別子（5QI）を使用したモバイル発信（MO）およびモバイル着信（MT）VoNR をサポートします。SMF は、次のモビリティ（gNB 間、AMF 間）シナリオで VoNR コールをさらにサポートします。

- アイドル モード UE の MO および MT コール
- UE が引き継いでいるときの MO と MT の通話

VoNR MO および MT コールのモビリティ シナリオでは、次の点を考慮してください：

- VoNR GBR フローは、UE およびネットワーク サービス要求手順中、Xn および N2 ベースのハンドオーバー中にサポートされます。

### コール フロー

ここでは、この機能に関連したコール フローについて説明します。

## *VoNR MO* コールの処理手順

このセクションでは、UE がアイドル モードの場合の VoNR MO コールの処理手順について説明します。

***Figure 124: VoNR MO* コールの処理手順**

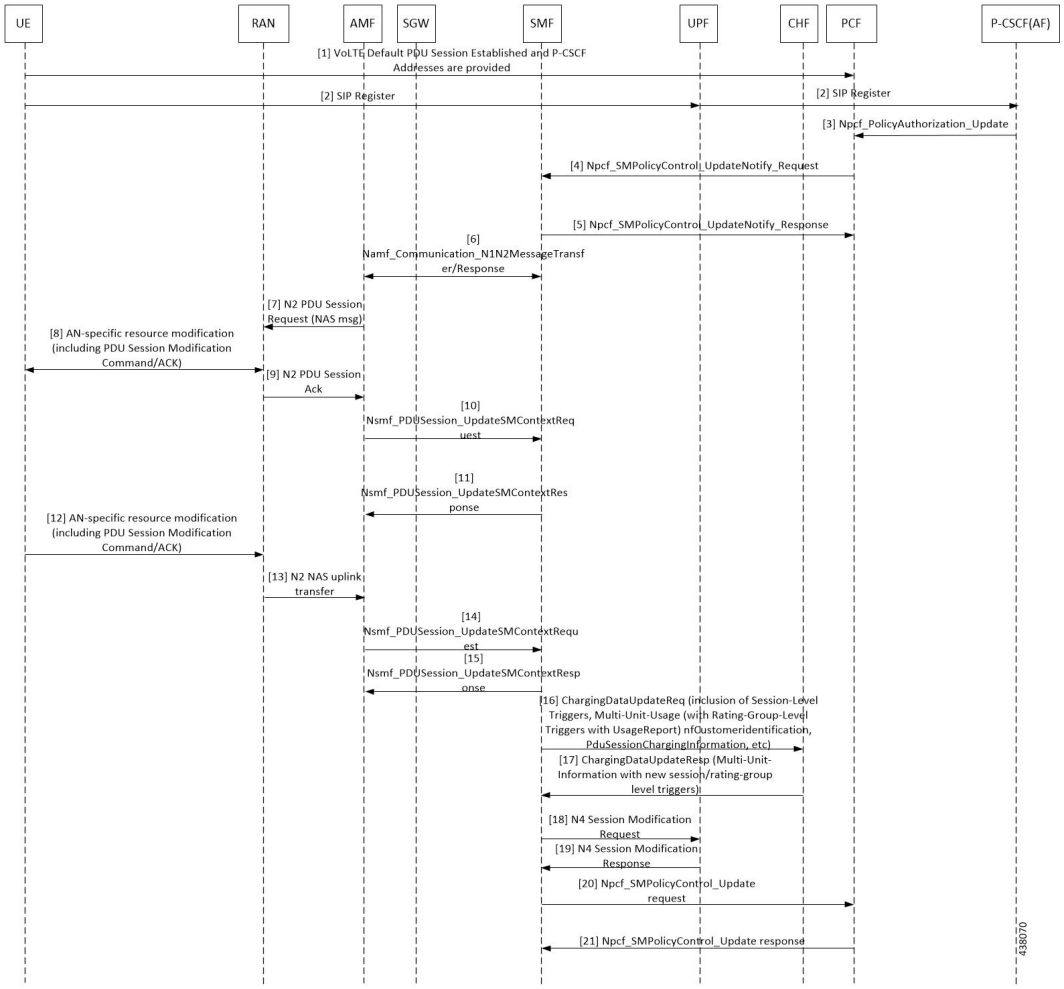



***Table 200: VoNR MO* コール処理フローの説明**

| ステップ | 説明 |
|---|---|
| 1 | SMF は、3GPP TS 23.502 で定義されている PDU セッション確立手順を実行します。 |
| 2 | UE は、バックアップされた IMS コア ネットワーク経由で UPF、P-CSCF を介して、着信側に対して SIP 登録を開始します。 |

| ステップ | 説明 |
|---|---|
| 3 | P-CSCF は「Npcf_PolicyAuthorization_Update」を PCF に送信し、ポリシーの適用、サービス情報の変更、ゲート制御、SDF 通知/非アクティブ化のサブスクリプションの変更、トラフィック ルーティング情報の更新などを行います（*3GPP TS 29.514*で定義されています）。このサービスでは、NF コンシューマはイベント通知（アクセスタイプ、RAT タイプの変更、または PLMN 識別子の変更など）の通知をサブスクライブおよびサブスクライブ解除できます。 |
| 4 | PCF は、Npcf_SMPolicyControl_UpdateNotify 要求を送信し、SMF およびポリシー制御要求トリガー情報で PCC ルール PDU セッション関連のポリシー コンテキストを更新または削除します。これにより、PCC ルール、ポリシー制御要求トリガ、SDF、課金関連情報が適用されます。 |
| 5 | SMF では、受信した PCC ルールが処理され、成功シナリオの場合は 200 OK メッセージが送信されます。コンテンツの処理が失敗すると、SMF は「Npcf_SMPolicyControl_UpdateNotify リクエスト」に「400 Bad Request」を含め、*3GPP TS 29.512*で定義されている適切な原因値とともに送信します。 |
| 6 | SMF は、Namef_Communication_\nN1N2MessageTransfer/Response（PDU セッション ID、QFI、QoS プロファイル、セッション AMBR）、N1 SM コンテナ（PDU セッション変更コマンド（PDU セッション ID、QoS ルール）、QoS フロー レベル パラメータを送信します。 QoS ルール、QoS ルール操作、および QoS フロー レベルの QoS パラメータ操作（セッション AMBR）に関連付けられた QoS フローに必要です）。<br><br>UE が CM-IDLE 状態またはモビリティ ハンドオーバー（HO）状態である場合は、アイドル モードでの UE の VoNR MO コール フロー, on page 633 の手順を参照してください。 |
| 7 | AMF は、N2 PDU セッション要求（SMF から受信した N2 SM 情報、NAS メッセージ（PDU セッション ID、N1 SM コンテナ（PDU 変更コマンド））メッセージを (R)AN に送信します。 |
| 8 | (R)AN は、SMF から受信した情報に関連する UE との特定のシグナリング交換を発行します。たとえば、 NG-RAN 内で RRC 接続再構成は、UE が PDU セッションに関連した必要な（R）AN 技術情報の変更をして行われます。 |

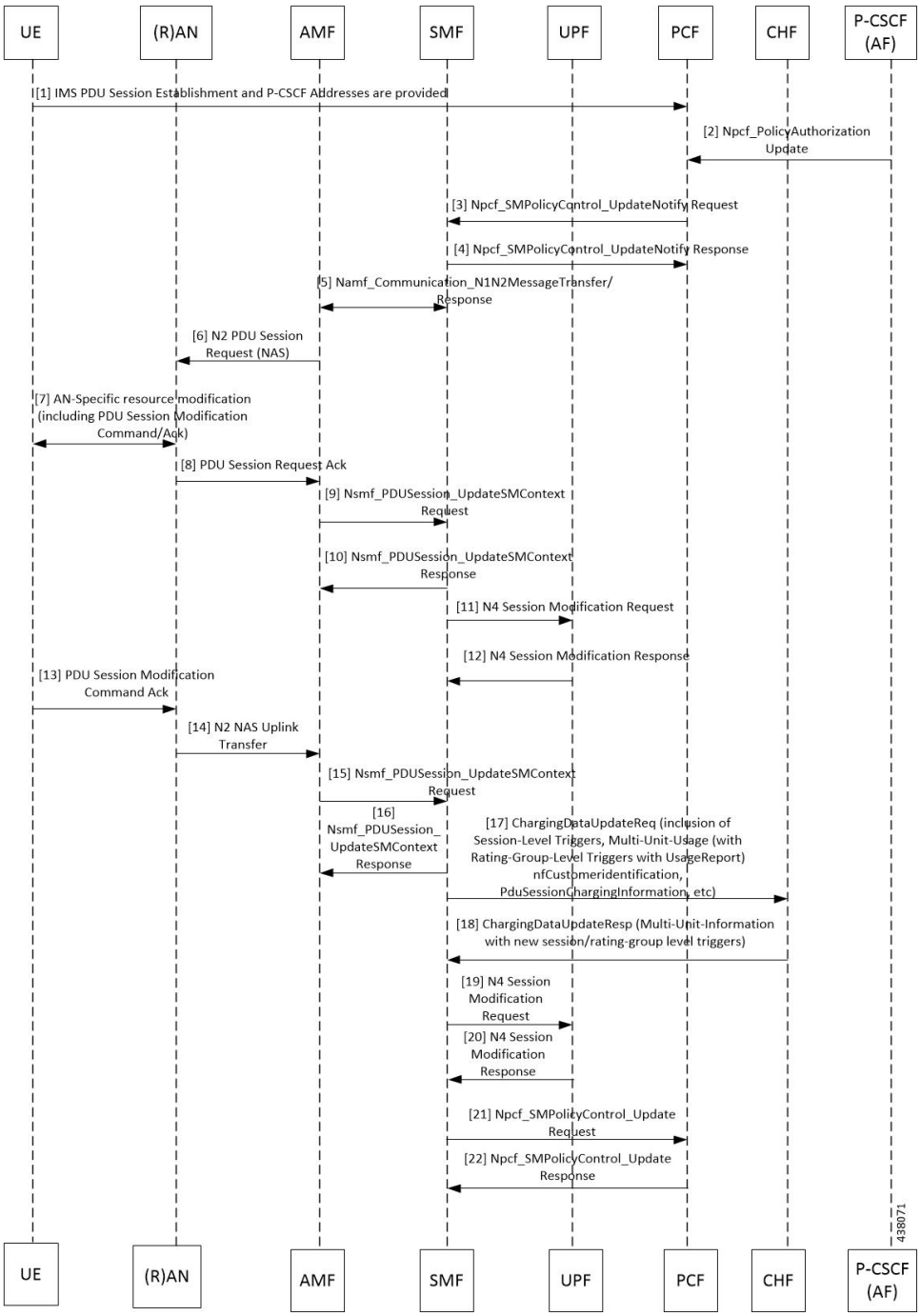
| ステップ | 説明 |
|---|---|
| 9 | (R)AN は、N2 PDU セッション ACK（N2 SM 情報（承認/拒否された QFI のリスト、AN 情報、PDU セッション ID、セカンダリ RAT 使用状況データ）、ユーザー ロケーション情報）メッセージを送信して N2 PDU セッション要求を AMF。デュアル接続の場合、1 つ以上の QFI が PDU セッションに追加されると、プライマリ RAN ノードは、これらの QFI のうちの1つ以上を、以前 PDU セッションに関与しなかった NG-RAN ノードに割り当てます。この場合、AN トンネル情報には、新しい NG-RAN ノードに割り当てられた QFI の新しい N3 トンネル エンドポイントが含まれます。同様に、1 つ以上の QFI が PDU セッションから削除されると、(R)AN ノードは PDU セッションに関与しなくなる可能性があり、対応するトンネルエンドポイントが AN トンネル情報から削除されます。NG-RAN は、対応する QoS プロファイルのユーザー プレーン セキュリティ適用情報を満たすことができない場合（たとえば、UE 整合性保護の最大データ レートを超えているため）、QFI を拒否します。 |
| 10 | AMF は、Nsmf_PDUSession_UpdateSMContext サービス操作を介して、(R)AN から受信した N2 SM 情報とユーザーの場所の情報を SMF に転送します。<br>(R)AN が QFI を拒否した場合、SMF は QoS ルールと QoS パラメータを必要に応じて、UE の QoS ルールに関連付けられた QoS フローに必要に応じて更新します。 |
| 11 | SMF は Nsmf_PDUSession_UpdateSMContext 応答を送信します。N2 SM 情報には、セカンダリ RAT 使用状況のデータが含まれます。 |
| 12 | UE は、NAS メッセージ（PDU セッション ID、N1 SM コンテナ（PDU セッション変更コマンド ACK））メッセージを送信して PDU セッション変更コマンドを確認します。 |
| 13 | (R)AN は NAS メッセージを AMF に転送します。 |
| 14 | AMF は、Nsmf_PDUSession_UpdateSMContext サービス操作を介して (R)AN から受信した N1 SM コンテナ（PDU セッション変更コマンド ACK）とユーザーの場所情報を SMF に転送します。 |
| 15 | SMF は Nsmf_PDUSession_UpdateSMContext 応答を送信します。<br>SMF によって開始された変更で、デフォルトの QoS ルールに関連付けられた QoS フローが含まれていない（PCF によってトリガされたなどの）QoS フローを削除することで、SMF が UE からの応答を受信しない場合、SMF は それらのステータスを QoS フローは UE と同期されます。 |
| 16 | SMF は、Sm_PolicyControl_UpdateNotify_Request の Charging_Description の一部として受信した Rating-Group-Id を持つ Multi-Unit-Usage を含めて、ChargingDataUpdateReq を送信します。これにより、PCC ルールがインストールされます。 |

| ステップ | 説明 |
|---|---|
| 17 | CHF は、要求されたメッセージで受信した料金設定グループ値のマルチユニット情報を含む ChargingDataUpdateResp を提供します。CHF では、セッション レベルおよび評価グループ値のパラメータの変更も提供されます。 |
| 18 | SMF は、N4 セッション変更要求（N4 セッション ID）メッセージを UPF に送信することにより、PDU セッション変更に含まれている UPF の N4 セッションを更新します。イーサネット PDU セッション タイプの PDU セッションの場合、SMF は PCF にイーサネットパケットフィルタセットと転送ルールの追加または削除を通知します。<br>PDU セッション変更手順で影響を受ける UPF は、変更された QoS パラメータと展開によって異なります。たとえば、UL CL が変更された PDU セッションのセッション AMBR が変更された場合は、UL フロー分類（CL）だけが関係します。 |
| 19 | UPF は、受信した制御情報に応じて PCF が SMF に提供する必要がある情報を含む N4 セッション変更応答メッセージを送信します。 |
| 20 | PCF を開始したポリシー変更ケースの場合、SMF は、*3GPP TS 23.502*、セクション 4.16.5.1 で定義されている SMF によって開始される SM ポリシー関連付けの変更手順を実行することによって、PCC の決定を適用できるかどうかを PCF に通知します。SMF は、PDU セッションの変更に関連するユーザーの場所情報を登録しているすべてのエンティティに通知します。 |
| 21 | PCF は、PDU セッションに関する更新されたポリシー情報を含む Npcf_SMPolicyControl_Update 応答を送信します。 |

## *VoNR MT* コールの処理手順

このセクションでは、VoNR MT コールの処理手順について説明します。

*Figure 125: VoNR MT* コールの処理フロー

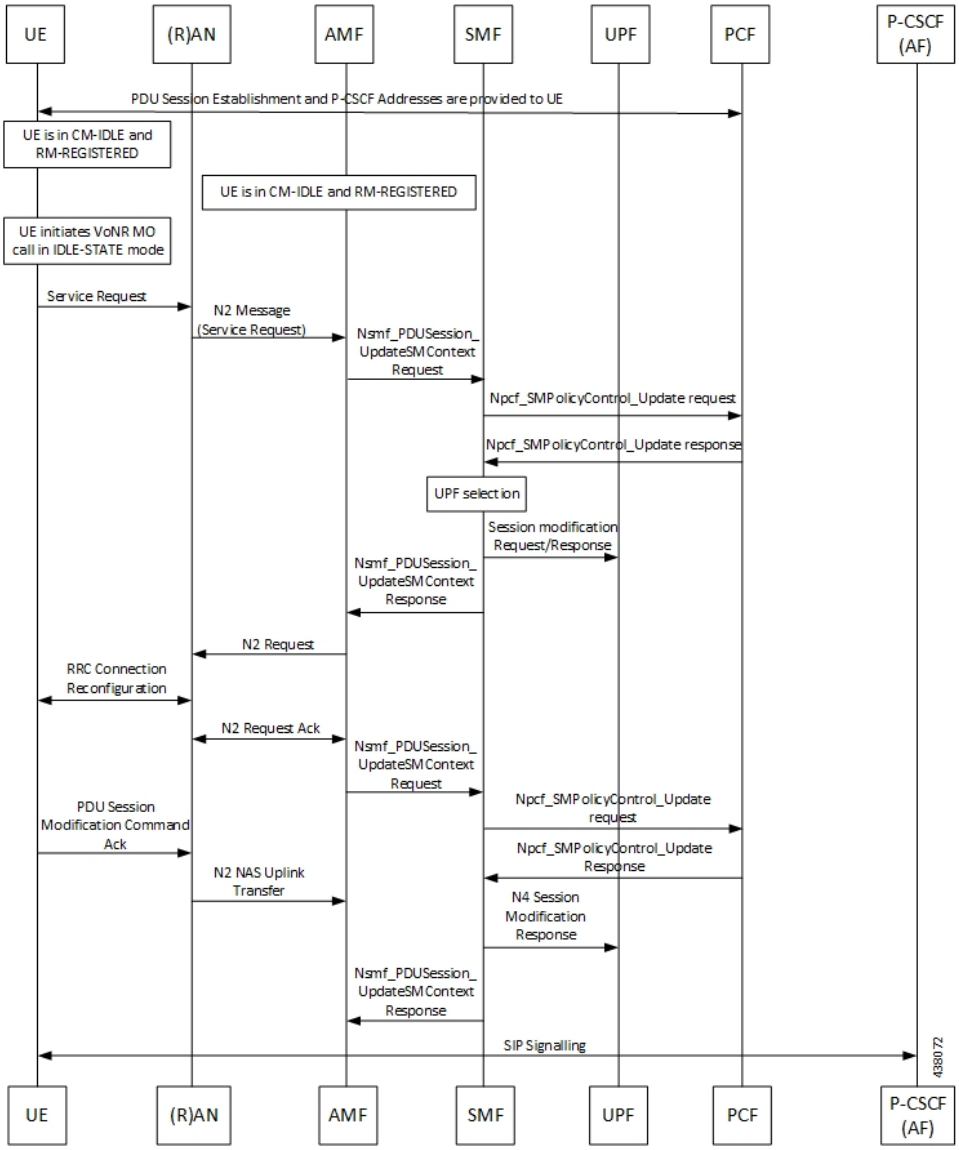



VoNR MT コールの処理手順は、UPF を介して UE から P-CSCF(AF) に開始される SIP 登録要求を除き、VoNR MO コールの処理手順と同じです。

## アイドル モードでの *UE* の *VoNR MO* コール フロー

このセクションでは、UE がアイドル モードの場合の VoNR MO コールの処理手順について説明します。

***Figure 126:*** アイドル モードでの ***UE*** の ***VoNR MO*** コール処理フロー



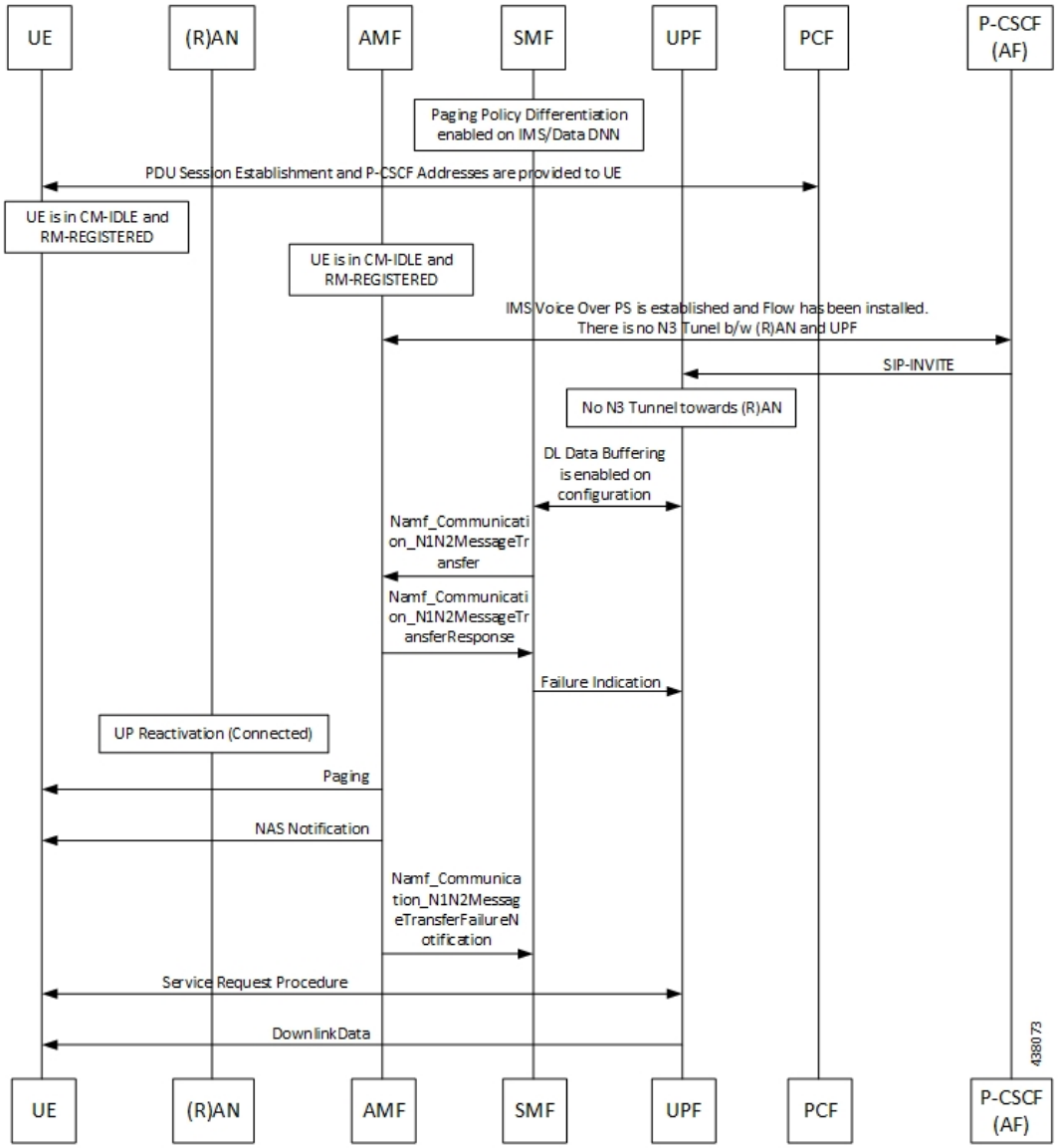
| ステップ | 説明 |
|---|---|
| 1 | SMF は、3GPP TS 23.502 で定義されている PDU セッション確立手順を実行し、UE に送信するために P-CSCF アドレスを取得します。SMF は、フローと各 PDR のトラフィック検出情報をプロビジョニングすることにより、N4 インターフェイスの一部として、それぞれの PDU セッションのページング ポリシー差別化（PPD）を使用して UPF をプログラムします。 |
| 2 | UE はその状態を CM-IDLE および RM-REGISTERED で維持します。 |
| 3 | UPF は、UE を CM-IDLE および RM-REGISTERED 状態に維持します。 |
| 4 | UE は CM-IDLE 状態で VoNR コールを開始します。 |
| 5 | UE は、*3GPP TS 23.502*で定義されているサービス要求手順を実行します。 |
| 6 | RAN は、N2 メッセージ（サービス要求）をAMFに送信します。 |
| 7 | AMF は、Nsmf_PDUSession_UpdateSMContext 要求（PDU セッション ID、操作タイプ、UE ロケーション情報、アクセス タイプ、RAT タイプ、LADN サービス エリア内の UE プレゼンス、アクセス タイプの表示は変更可能）を SMF に送信します。 |
| 8 | AMF が PDU セッションのアクセス タイプを変更できることを SMF に通知し、PCC が展開されている場合、SMF は、*3GPP TS 23.502* のセクション 4.16.5.1 に定義されている SMF によって開始される SM ポリシー関連付け変更手順を実行します。 |
| 9 | PCF は、更新された PCC ルールを SMF に提供します。 |
| 10 | SMF は UPF に対して N4 セッション変更要求を開始します。SMF は、(R)ANトンネル情報と対応する転送ルールをUPFに提供します。UPF は、SMF に N4 セッション変更応答を提供します。 |
| 11 | SMF は、Nsmf_PDUSession_UpdateSMContext Response（N2 SM 情報（PDU セッション ID、QFI（複数可）、QoS プロファイル（複数可）、CN N3 トンネル情報、S-NSSAI、ユーザー プレーン セキュリティ適用、UE インテグリティ保護最大データレート）、N1 SM コンテナ、原因）を AMF に送信します。SMF は、該当する場合、N1 SM コンテナおよび/または N2 SM 情報をAMFに送信します。 |
| 12 | AMF は、N2 要求を送信します（SMF から受信した N2 SM 情報、セキュリティ コンテキスト、モビリティ制限リスト、登録済みUE-AMBR、MM NAS サービス承認、推奨セルのリスト、TA、NG-RAN ノード識別子、UE 無線機能、コア ネットワーク サポート情報、トレーシング要件）を (R)AN に追加します。 |
| 13 | NG-RAN は、UP 接続がアクティブ化されている PDU セッションのすべての QoS フローとデータ無線ベアラーの QoS 情報に応じて、UE との RRC 接続の再構成を実行します。 |

| ステップ | 説明 |
|---|---|
| 14 | (R)AN は N2 要求の確認応答メッセージ（N2 SM 情報（AN トンネル情報、UP 接続がアクティブになっている PDU セッションで承認された QoS フローのリスト、UP 接続がアクティブになっている PDU セッションで拒否された QoS フローのリスト）を送信します。PDU セッション ID を AMF に送信します。<br>N2 要求 ACK メッセージには、N2 SM 情報（AN トンネル情報など）が含まれます。AMF が別の N2 メッセージを送信した場合、NG-RAN は別の N2 メッセージ（N2 トンネル セットアップ応答など）でN2 SM情報に応答します。 |
| 15 | AMF は、PDU セッションごとに Nsmf_PDUSession_UpdateSMContext 要求（N2 SM 情報、RAT タイプ、アクセス タイプ）を SMF に送信します。AMF は、N2 インターフェイスに関連付けられたグローバルRANノードIDに基づいて、アクセス タイプと RAT タイプを決定します。AMF が N2 SM 情報（1 つまたは複数）を受信した場合、AMF は N2 SM 情報を PDU セッション ID ごとに関連する SMF に転送します。UE タイムゾーンが最後にレポートされた UE タイムゾーンと比較して変更されている場合、AMF はこのメッセージに UE タイムゾーン IE を含めます。 |
| 16 | SMF は、*3GPP TS 23.502*、セクション 4.16.5.1 で定義されている SMF によって開始される SM ポリシー関連付けの変更手順を実行することによって、PCC の決定を適用できるかどうかを PCF に通知します。SMF は、PDU セッションの変更に関連するユーザーの場所情報を登録しているすべてのエンティティに通知します。 |
| 17 | PCF は、PDU セッションに関する更新されたポリシー情報を含む Npcf_SMPolicyControl_Update 応答を送信します。 |
| 18 | SMF は、N4 セッション変更要求（N4 セッション ID）メッセージを UPF に送信することにより、PDU セッション変更に含まれている UPF の N4 セッションを更新します。イーサネット PDU セッション タイプの PDU セッションの場合、SMF は UPF にイーサネットパケットフィルタセットと転送ルールの追加または削除を通知します。<br>PDU セッション変更手順で影響を受ける UPF は、変更された QoS パラメータと展開によって異なります。たとえば、UL CL が変更された PDU セッションのセッション AMBR が変更された場合は、UL CL だけが関係します。<br>UPF は、受信した制御情報に応じて UPF が SMF に提供する必要がある情報を含む N4 セッション変更応答メッセージを送信します。 |
| 19 | SMF は Nsmf_PDUSession_UpdateSMContext 応答を送信します。N2 SM 情報には、セカンダリ RAT 使用状況のデータが含まれます。 |

## アイドル モードでの *UE* の *VoNR MT* コールフロー

このセクションでは、UE がアイドル モードの場合の VoNR MT コールの処理手順について説明します。

*Figure 127:* アイドル モードでの *UE* の *VoNR MT* コールフロー




VoNR MT コール フローは、次を除き、UE が CM-IDLE 状態の場合のサービス要求の VoNR MO コール フローと同じです。

- P-CSCF が受信した SIP-INVITE
- PCF から SMF に対してトリガされた PCC ルールの適用。

**Note** PCC ルール、QoS、PDR、およびトラフィック検出ルールの適用は、 VoNR MT コールの処理手順, on page 631 VoNR MT コール処理の手順で定義されている VoNR MT コール処理の手順と同じです。

AMF が Namef_Communication_N1N2MessageTransfer 要求（N2 SM 情報（PDU セッション ID、QFI（s）、QoS プロファイル、セッション AMBR）、N1 SM コンテナ（PDU セッション変更コマンド（PDU セッション ID、QoS ルール）、 UE が CM-IDLE 状態の場合の QoS フローレベルのパラメータ（QoS ルール動作、QoS フロー レベル パラメータ動作、セッション AMBR）に関連付けられた QoS フローに必要な場合。UE が CM-IDLE 状態で、非同期タイプの通信（ATC）がアクティブになっている場合、AMF は Namef_Communication_N1N2MessageTransfer に基づいて UE コンテキストを更新および保存します。

AMF は UE に対してページング操作を実行し、UE はサービス要求手順をトリガします。ページングが確立されると、AMF はNamf_Communication_N1N2MessageTransfer Request で受信される QoS フロー、QoS ルール、および Session-AMBR のうち、受け入れが必要なものを決定し、AMF は SMF に対して Nsmf_PDUSession_UpdateSMContext 操作を実行して、QoS フロー、QoS ルール、session-AMBR などの受け入れを通知します。

# VoNR ページング ポリシー差別化

## 機能説明

SMF は、UE のデータおよび IMS DNN セッションに PLMN、DNN、および 5QI レベルで構成を提供することにより、ページング ポリシー差別化機能をサポートします。SMF は、UPF データに基づいてページング ポリシー インジケータを提供します。SMF は、N11 インターフェイスを介した AMF への QoS フロー（PPI、ARP、および 5QI）もサポートしています。

### コール フロー

ここでは、この機能に関連したコール フローについて説明します。

#### *VoNR* ページング ポリシーの差別化手順

このセクションでは、VoNR ページング ポリシーの区別手順について説明します。

*Figure 128: VoNR* ページング ポリシー差別化コール フロー

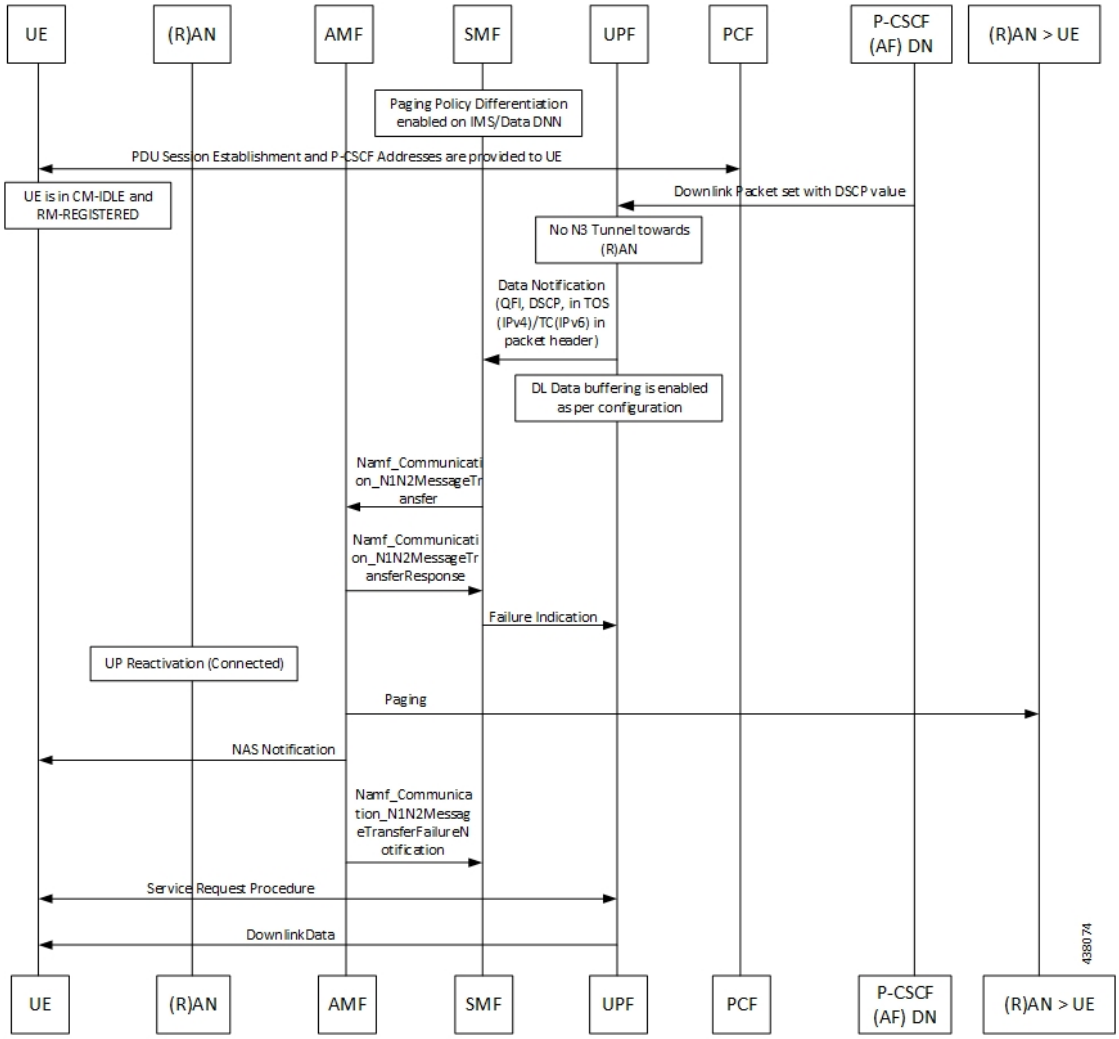



*Table 201: VoNR* ページング ポリシーの差別化コール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | SMF は、DNN、5QI、および PLMN に基づく DNN プロファイルの下でページング ポリシー差別化（PPD）を有効にします。 |
| 2 | SMF は、3GPP TS 23.502 で定義されている PDU セッション確立手順を実行し、UE に送信するために P-CSCF アドレスを取得します。SMF は、各 PDR のフローおよびトラフィック検出情報をプロビジョニングすることにより、N4 インターフェイスの一部として、それぞれの PDU セッションの PPD を使用して UPF をプログラムします。 |

| ステップ | 説明 |
|---|---|
| 3 | UPF は、PDU セッションで PPD が有効になっているときに、いずれかのダウンリンク（DL）パケットが DSCP 値（IPv4 の TOS または IPv6 の TC）で設定されているかどうかを検出します。 |
| 4 | UPF は、DSP マーク付き DL パケット用の N3 トンネルがないため、転送パスがないことを検出します。 |
| 5 | UPF は、パケットヘッダー内でデータ通知（QFI、DSCP in TOS（IPv4）/TC（IPv6））を送信します。 |
| 6 | UPF は、バッファリング構成に基づいて DL データ バッファリングを有効にします。UPF は、データ通知（N4 セッション ID、DL データ パケットの QoS フローを識別する情報、DSCP）メッセージを SMF に送信します。<br>**1.** QoS フローの最初の DL データパケットが到着すると、SMF が以前に UPF に通知していない場合、UPF はデータ通知メッセージを SMF に送信します（その場合、次の手順はスキップされます）。<br>**2.** UPF が同じ PDU セッションで別の QoS フローの DL データ パケットを受信すると、UPF は別のデータ通知メッセージを SMF に送信します。<br>**3.** ページング ポリシー差別化機能（*3GPP TS 23.501*、セクション *5.4.3*で指定）が UPF でサポートされており、PDU セッション タイプが IP の場合、UPF の TOS（IPv4）/TC（IPv6）値には DSCP が含まれます。 DL データ パケットの IP ヘッダーと DL データパケットの QoS フローを識別する情報です。<br>**4.** SMF は、データ通知確認応答メッセージを UPF に送信します。<br>**5.** UPF は、要求に応じて DL データ パケットを SMF に転送します。SMF はデータパケットをバッファリングします。 |

| ステップ | 説明 |
|---|---|
| 7 | SMF は AMF を決定し、N4 セッション ID に基づく PDU セッション ID を含む AMF に対する Namef_Communication_N1N2MessageTransfer を呼び出します。ユーザー プレーン接続がアクティブになるのを待っているときに、SMFは追加のデータ通知メッセージを受信します。<br>SMF は、追加のデータ通知またはデータ パケットの DSCP に従って、異なるページング ポリシー インジケータを取得します。SMF は新しい Namef_Communication_N1N2MessageTransfer を呼び出し、AMF に対してより高い優先順位または別のページング ポリシー インジケータを示します。<br>ページング ポリシーの差別化をサポートしている場合、SMF は 、*3GPP TS 23.501*、セクション *5.4.3* に記載されているように、*DSCP* に基づいて *UPF* から受信した、またはデータ通知メッセージをトリガしたダウンリンク データに関連するページング ポリシー インジケータを決定します。SMF は、Namef_Communication_N1N2MessageTransfer のページング ポリシー インジケータを示します。 |
| 8 | AMF は、UE が CM_IDLE 状態の場合、Namef_Communication_N1N2MessageTransfer 応答を「Attempting to reach UE」という理由で SMF に送信します。UE が CM-CONNECTED 状態の場合、AMF は「N1/N2 transfer success」の理由とともに Namef_Communication_N1N2MessageTransfer 応答を SMF にただちに送信します。 |
| 9 | SMF は、AMF から否定応答を受信すると、障害通知を UPF に送信します。 |
| 10 | AMF は、（R）AN を介して UE へのページングを開始します。 |
| 11 | AMF は UE に対する NAS 通知を開始します。 |
| 12 | AMFは、UEがページングに応答しない場合、SMFによって提供された通知ターゲット アドレスに Namef_Communications_N1N2MessageTransfer Failure Notification を送信してSMFに通知します。AMFは、UEの応答を妨げる進行中のモビリティ管理（MM）手順を認識していません。AMF は、UE が別の AMF を使用して登録手順を実行することを示す N14 コンテキスト要求メッセージを受信します。 |
| 13 | UE が CM-IDLE 状態の場合、3GPP アクセスに関連付けられた PDU セッションのページング要求を受信すると、UE は、 *3GPP TS 23.502*、セクション *4.2.3.2*に定義されているように、UE トリガー サービス要求手順を開始します。 |

## VoNR ページング プロファイル差別化の構成

ここでは、VoNR ページング プロファイル差別化機能を構成する方法について説明します。

VoNR ページング プロファイル差別化機能を構成するには、次の手順を実行します：

1. PDD プロファイルの作成

2. RLAN プロファイル パラメータの設定
3. DNN プロファイル構成での PPD の有効化

## PDD プロファイルの作成

次の構成を使用して、PPD プロファイルのインスタンスを作成します：

```
config
   profile ppd ppd_profile_name
   end
```

注：

- **ppd** *ppd_profile_name*：PPD プロファイルを指定します。このコマンドは、PPD プロファイルを作成し、PPD プロファイル コンフィギュレーション モードにアクセスできるようにします。このモードでサポートされているコマンドの詳細については、『*Ultra Cloud Core 5G* セッション管理機能、*CLI* コマンド リファレンス ガイド』を参照してください。*ppd_profile_name* の値は英数字の文字列である必要があります。

## RLAN プロファイル パラメータの設定

次の構成を使用して、PPD プロファイルパラメータを定義します：

```
config
   profile ppd ppd_profile_name
      5qi 5qi_value
      dscp dscp_value { ppi ppi_value }
      end
```

注：

- **5qi**：このルートのプライオリティ レベルを指定します。*5qi_value* は 0 ～ 127 の範囲の整数である必要があります。さまざまな優先度レベルをリストするには、必要に応じてカンマとハイフンを使用します。たとえば、5QI 3、10-15、65 です。
- **dscp** *dscp_value*：DSCP 値を指定します。 *dscp_value* は 、0 ～ 63 の範囲の整数である必要があります。
- **ppi** *ppi_value*： ページング ポリシー インジケータの値を指定します。 *ppi_value* は 0 ～ 7 の範囲の整数である必要があります。

## DNN プロファイル構成での PPD の有効化

既存の DNN プロファイル構成内の PPD 機能を有効にするには、次の構成例を使用します。

```
config
   profile dnn dnn_profile_name
      ppd-profile ppd_profile_name
      end
```

注：

- **ppd-profile** *ppd_profile_name*：このコマンドは、DNN プロファイルに関連付ける PPD プロファイルを定義します。 *pdd_profile_name* は 、構成済みの PPD プロファイルの名前である必要があります。
- このコマンドは、DNN、5QI、および PLMN の構成値に基づいて、DNN プロファイルの PPD 機能を有効にします。

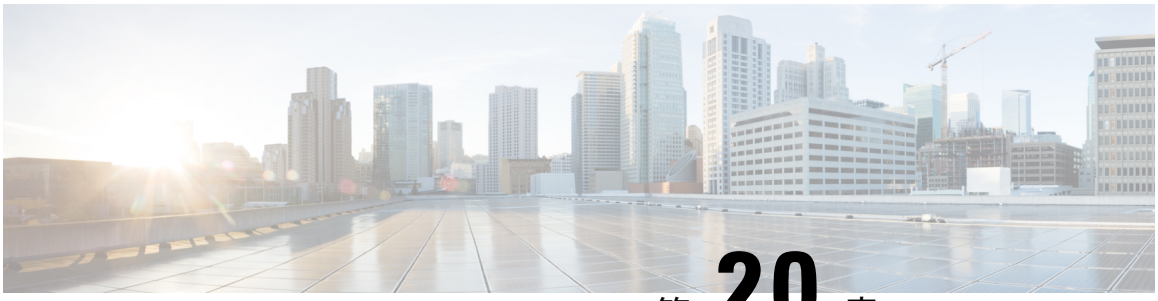
## 機能の設定の確認

次の表示コマンドを使用して機能構成の詳細を認証します。

**show running-config**

次に、この show コマンドの出力例を示します：

```
product smf# show running-config
profile dnn dnntst1
pcscf-profile pcscf1
!
```



第 20 章

# インターフェイス サポート


- 機能の概要と変更履歴, on page 643
- 機能説明 （647 ページ）
- SMF インターフェイスの 3GPP 仕様コンプライアンス （649 ページ）
- サポートされている SMF インターフェイス （655 ページ）
- FQDN の概要 （881 ページ）
- インターフェイスの設定 （887 ページ）
- OAM サポート （891 ページ）


## 機能の概要と変更履歴

### 要約データ

**表 *202 :* 要約データ**

| | |
|---|---|
| 該当製品または機能エリア | SMF |
| 該当プラットフォーム | SMI |
| デフォルト設定 | 有効：常時オン |
| このリリースでの関連する変更点 | N/A |
| 関連資料 | 該当なし |

# 更新履歴

表 *203 :* マニュアルの変更履歴

| 改訂の詳細 | リリース |
|---|---|
| 次に対するサポートが追加されました：<br>• オフライン ベアラー再計算の非同期および同期使用状況レポート<br>• Gzインターフェイスでのベアラー要求トリガーの変更の処理<br>• Gz 通知変更<br>• APN-AMBR および Qci の変更に基づくデフォルトのベアラーの変更<br>• セカンダリ RAT 使用状況の定期レポートの処理：<br>• EGCDR 最終レコード構成<br>• ゼロCDR抑制<br>• 後続の CCR-U における最終ユニット表示<br>• FHT 継続の機能強化（FHT Continue Enhancement）<br>• 直径クレジット制御障害処理 AVP | 2023.04.0 |
| 次に対するサポートが追加されました：<br>• SMF インターフェイスの複数の 3GPP 仕様に準拠。<br>• Gz インターフェイスおよび関連機能：<br>  • Gzインターフェイスと一緒に PDN を付加と切断<br>  • Gz 使用状況レポート<br>• SCP モデル D を介した NF の間接的な通信。<br>• NRF メッセージで地域性のオプションの IE を除外する。 | 2023.03.0 |

| 改訂の詳細 | リリース |
| --- | --- |
| 次に対するサポートが追加されました：<br>• Gx インターフェイスとその関連機能：<br>• Gx の初期アタッチとデタッチ<br>• ダイナミックおよび事前定義済みのルール<br>• Gy インターフェイスとその関連機能：<br>• Gy 使用状況レポート<br>• Gy 障害処理<br>• Gy MSCC レベルの失敗結果コード<br>• Gy QVT と QHT<br>• Gy tarrift時間<br>• データ インターフェイスでの IPv6 | 2023.02.0 |
| 次に対するサポートが追加されました：<br>• IPsec 経由の N4 インターフェイス<br>• すべての SMF インターフェイスの IPv6 アドレス<br>• ユーザー プレーン整合性保護<br>• SBI インターフェイスの相互 TLS<br>• CHF サーバーの 3GPP 仕様バージョン準拠の構成 | 2022.04.0 |
| UDM および PCF メッセージの構成ベースの制御のサポートが追加されました。 | 2021.02.3.t3 |
| N2 原因および診断 IE のサポートが追加されました。 | 2021.02.3 |

| 改訂の詳細 | リリース |
| --- | --- |
| 次に対するサポートが追加されました：<br>• N11 インターフェイスで IE を発生させる。<br>• NAS メッセージが無効なプロトコル データの処理に準拠しています。<br>• N11 インターフェイス上の ProblemDetails JSON オブジェクト。<br>• HTTP エラーコードによるエラー処理。<br>• SBA インターフェイスでは HTTP/2 TLS をサポートします。 | 2021.02.0 |
| 最初の導入。 | 2020.02.0 より前 |

# 機能説明

表 *204 :* 機能の履歴

| 機能名 | リリース情報 | 説明 |
|---|---|---|
| レガシー インターフェイスを使用した SMF の IPv6 接続の有効化 | 2024.01.1 | レガシー インターフェイスを使用する SMF により、IPv6 アドレス構成が GTP、N4、Gx、および Gy インターフェイスとの通信を可能にします。このサポートにより、IPv4 アドレスと IPv6 アドレスの両方をピア接続に使用できます。1 つのピア接続で IPv4 または IPv6 アドレスのいずれかを使用できます。<br>IPv6 接続を有効にするには、SMF で既存の **endpoint { bgpspeaker \| diameter \| dns-proxy \| geo \| gtp \| gtpprime \| li \| nodemgr \| pfcp \| protocol \| radius \| radius-dns \| sbi \| service \| sgw-service }** および **dual-stack-transport { false \| true }** CLI コマンドを使用します。<br>**デフォルト設定**：無効：構成が必要 |
| N3 のデュアル スタックのサポート | 2024.01 | SMF は、UPF ネットワーク プロファイルで **dual-stack-transport { false \| true }** CLI コマンドを使用して、N3 トンネルのデュアル スタック トランスポートを有効にします。<br>**デフォルト設定**：無効：構成が必要 |

**重要** この章で使用されている PGW-C という用語は、SMF によってサポートされている EPS インターワーキング機能を意味しており、LTE ネットワークで使用されるスタンドアロン P-GW として想定してはなりません。

5G システム アーキテクチャでは、SMF は、4G モビリティ管理エンティティ（MME）、サービング ゲートウェイ コントロール プレーン機能（SGW-C）、および PDN ゲートウェイ コントロールプレーン機能（PGW-C）が処理するセッション管理機能を実行します。SMF は、サービスベース アーキテクチャ（SBA）を構成する要素の 1 つです。SMF は、分離されたデータ プレーンと通信し、プロトコル データ ユニット（PDU）セッションを作成、更新、および削除します。SMF は、ユーザー プレーン機能（UPF）を使用してセッション コンテキストも管理します。セッション管理関連の機能の場合、SMF は N1、N4、N10 などのさまざまなインターフェイスと通信します。

特定の時点で、SBI インターフェイス（N7、N10、N11、および N40）は、IPv4 または IPv6 アドレスのみをサポートします。ただし、N3、N4 、および GTPC インターフェイスは、IPv4 または IPv6 アドレスのいずれか 、または両方をサポートします。IP アドレスをサポートするには、エンドポイントとインターフェイスの両方の構成に一意の VIP IP とポートが含まれている必要があります。構成詳細については、インターフェイスの設定（887 ページ）セクションを参照してください。

SMF は、N4 インターフェイスでメッセージを開始するときに、IPv4 アドレスよりも IPv6 を優先します。ピア GTPC が IPv4 アドレスと IPv6 アドレスの両方を使用する場合、SMF は、新しいメッセージを開始する一方で、その特定のセッションの GTPC ピアから最後のメッセージを受信したのと同じ IP アドレス タイプを使用します。

SMF が CSR または MBR メッセージの一部として IPv4 アドレスと IPv6 アドレスの両方を受信した場合、SMF は GTPC インターフェイス上の IPv4 アドレスと IPv6 アドレスを使用してエコーを送信します。ピアは、両方のインターフェイスでエコーが失敗した場合にのみ、ダウンしていると見なされます。SMF はパス障害として判断し、セッションをクリアします。

SBI インターフェイスの場合、検出された NF プロファイルに IPv4 アドレスと IPv6 アドレスの両方が含まれている場合、SMF は、その特定のインターフェイスの SBI エンドポイントレベルまたはインターフェイス レベルでの IP タイプ構成に基づいて、ピア NF と通信するための IP を選択します。

SMF は、IPv6 エンドポイント識別子情報とトンネル情報を交換することで、UPF トンネルと RAN の間をネゴシエートします。

HO 中に、SMF はターゲット ピアから受信したトンネル情報に基づいてトンネルを作成し、UPF とターゲット ピアの間でトンネル情報を交換します。

各インターフェイスとエンドポイントは、現在のサポートに基づいて、IPv4 または IPv6、またはその両方に対して個別に構成できます。

UPF の関連付けのセットアップ時に、SMF はセットアップ要求のトランスポート タイプが構成済みのアドレスと同じかどうかを確認します。SMF は、関連付け要求を処理するか、検証結果に基づいて要求を拒否します。

同様に、NRF 検出時に、トランスポート タイプは、エンドポイント レベルまたはインターフェイス レベルのいずれかで静的に設定されたトランスポート タイプと一致する必要があります。SMF は、IP アドレスの一致基準に基づいて NF 選択を実行します。

レガシー インターフェイスを使用する 4G コールの場合、ピア SGW IPv4、IPv6、または IPv4v6 データ アドレスがサポートされます。

（注） DNS、RADIUS、およびローミング インターフェイスは、現在 IPv6 アドレスをサポートしていません。

# SMF インターフェイスの 3GPP 仕様コンプライアンス

## 機能説明

SMF は、SMF インターフェイス N1、N2、N4、N7、N10、N11、N40、および Nnrf の 2 つの 3GPP 仕様準拠バージョン 15.x（2018 年 12 月および 2019 年 6 月）の構成をサポートしています。これは、対応するサービスの構成されたプロファイルに準拠したピア インターフェイスから着信メッセージをプロセスします。

サポートされているさまざまな仕様バージョンとさまざまなインターフェイスの対応するマッピングされた URI バージョンの詳細については、「規格準拠」の 項を参照してください。

コンプライアンス プロファイルの設定の詳細については、インターフェイスの 3GPP 仕様コンプライアンスの構成, on page 652 セクションを参照してください。

SMF は、IE エンコーディングおよびデコーディング機能のみをサポートしています。既存の機能は、2019 年 6 月の仕様バージョンで動作します。2019 年 6 月のバージョンの追加機能はサポートされていません。

**Note** SMF では、古いバージョンの 3GPP 仕様が引き続きサポートされ、コンプライアンス プロファイル構成によって、SMF インターフェイスの同一性が制御されます。

### URI バージョン選択ロジック

2 つの異なる 3GPP コンプライアンス バージョンが構成されている場合、Nnrf_NFDiscovery サービスにより、SMF は、ローカル NRF（ネットワーク リポジトリ機能）、つまり CHF、AMF、PCF をクエリして、それらが提供するサービスを持つ他の NF（ネットワーク機能）インスタンスを検出できます。

ディスカバリ応答の SearchResult 本体には、検索フィルタ条件を満たす NF プロファイル オブジェクトの配列が含まれています。属性データ タイプ **NFServiceVersion** は、さまざまなピア NF によってサポートされているバージョンをキャプチャします。

SMF プロファイルの構成バージョンと、Discovery SearchResult で受信したバージョンに基づいて、SMF は後続のメッセージのピア NF のバージョンを選択します。

SMF がピア NF のバージョンを選択するためのロジックは、URI バージョン選択ロジックと呼ばれます。ピア NF の最上位バージョンを選択します。

次の表に、ディスカバリ応答の結果として NFServiceVersion を受信したときに、URI バージョン選択ロジックがピアに適したバージョンを選択する方法を示します。

**表 *205 : URI* 選択ロジック**

| SMF コンプライアンス構成バージョン | ディスカバリ検索結果バージョン | ピア NF の選択バージョン |
|---|---|---|
| V2、V1 | V2、V1 | V2 |
| V2、V1 | V1 | V1 |
| V1 | V2、V1 | V1 |

ピア NF のバージョンが選択されると、後続のメッセージは選択されたバージョンを使用して送信されます。最初のメッセージ交換中に、選択したピア NF がダウンした場合、SMF は、NF バージョンが同じまたは次に高い別のピアを選択します。

最初のメッセージ交換後に、選択したピア NF がダウンした場合、SMF はセッション用に同じバージョンまたは異なるバージョンを持つ別のピアを選択しません。

## 標準準拠

SMF は、5G コアネットワークのコントロールプレーン（CP）NF の 1 つです。SMF はさまざまなインターフェイスを使用して他の NF またはノードと通信します。

たとえば、SMF とユーザープレーン機能（UPF）の間に N4 インターフェイスが存在します。各 SMF インターフェイスは、サポートされているコンプライアンスバージョンに応じて、3GPP 仕様の特定のバージョンに準拠します。

次の表を使用して、各 SMF インターフェイスと 3GPP 標準規格バージョンのコンプライアンスマッピングを確認します。

***Table 206: SMF* インターフェイスと *3GPP* 標準仕様バージョンのマップ**

| Interface | 関係 | 3GPP 仕様 | バージョン |
|---|---|---|---|
| N1/NAS | UE と AMF 間 | *24.501* | 2018 年 12 月のコンプライアンス サポート： *15.2.0*<br>2019 年 6 月のコンプライアンス サポート： *15.4.0*<br>サポートされている仕様： *15.2.0*、***15.4.0***<br>マッピング済み URI： *V1* |

| Interface | 関係 | 3GPP 仕様 | バージョン |
|---|---|---|---|
| N2/NGAP | RANとAMFの間 | *38.413* | 2018年12月のコンプライアンス サポート： *15.2.0*<br>2019年6月のコンプライアンス サポート： *15.4.0*<br>サポートされている仕様： *15.0.0*、*15.2.0*、***15.4.0***<br>マッピング済み URI： *V1* |
| N4 | UPF と SMF 間 | *29.244* | 2018年12月のコンプライアンスサポート： *15.2.0*<br>2019年6月のコンプライアンスサポート： *15.4.0* |
| N7 | PCF と SMF の間 | *29.512* | 2018年12月のコンプライアンスサポート： *15.2.0*<br>2019年6月のコンプライアンスサポート： *15.4.0*<br>サポートされている仕様： *15.0.0*、*15.2.0*、***15.4.0***<br>マッピング済み URI： *V1* |
| N10 | UDM と SMF の間 | *29.503* | 2018年12月のコンプライアンスサポート： *15.2.1*<br>2019年6月のコンプライアンスサポート： *15.4.0*<br>サポートされている仕様： *15.1.0*、*15.2.1*、***15.4.0***<br>マッピング済みURI：<br>• *V1*：*15.1.0, 1 5.2.1*<br>• *V2*：*15.4.0* |

| Interface | 関係 | 3GPP 仕様 | バージョン |
|---|---|---|---|
| N11 | AMF と SMF 間 | *29.518*<br>*29.502* | 2018 年 12 月のコンプライアンスサポート： *15.2.0*<br>2019 年 6 月のコンプライアンスサポート： *15.4.0*<br>サポートされている仕様：15.0.0、15.2.0、**15.4.0**<br>マッピング済み URI： *V1* |
| N40 | SMF と CHF の間 | *32.291* | 2018 年 12 月のコンプライアンスサポート： *15.1.0*<br>2019 年 6 月のコンプライアンスサポート： *15.3.0*<br>サポートされている仕様：*15.0.0,15.1.0*、*15.2.1*、***15.3.0***、*15.3.0.custom*、*15.3.0.std*<br>マッピング済み URI：<br>• *V1*：*15.0.0*、*15.1.0*<br>• *V2 15.2.1*、*15.3.0*、*15.3.0 std*、*15.3.0 custom* |
| Nnrf | NRF と SMF の間 | *29.510* | 2018 年 12 月のコンプライアンス サポート： *15.0.0*<br>2019 年 6 月のコンプライアンス サポート： *15.4.0*<br>サポートされている仕様： *15.0.0*、*15.2.0*、***15.4.0***<br>マッピング済み URI： *V1* |

# インターフェイスの 3GPP 仕様コンプライアンスの構成

3GPP 仕様に準拠して SMF インターフェイスを構成するには、次の構成例を使用します。

```
config
   profile compliance profile_name
      service { n1 | n2 | namf-comm | nchf-convergedcharging | nnrf-disc
 | nnrf-nfm | npcf-smpolicycontrol | nsmf-pdusession | nudm-sdm |
nudm-uecm | threegpp23502 }
          version { full version_format| spec spec_version| uri uri_version }
          version-list version  version_name { full version_format | mode {
```

```
active | offline } | spec  spec_version | uri  uri_version }
          end
       end
    end
```

**Important** サービスの選択は、仕様バージョンにのみ基づいています。将来のリリースでは、完全なAPIバージョンが使用されます。

注：

- **service { n1 | n2 | namf-comm | nchf-convergedcharging | nnrf-disc | nnrf-nfm | npcf-smpolicycontrol | nsmf-pdusession | nudm-sdm | nudm-uecm | threegpp23502 }**： *3GPP TS 29.510*、バージョン *15.2.0*、セクション *6.1.6.3.11*に記載されているサービス名を指定します。

**Note** **nchf-convergedcharging** サービスのコンプライアンス プロファイル構成は 、*3GPP TS 29.510* バージョン *15.4.0* 仕様をサポートしています。この構成済みバージョンでは、SMF は次の形式の subscriberIdentifier を CHF に送信します：

"subscriberIdentifier":"imsi-123456789"

- **version**：構成するコンプライアンス バージョン名を指定します。一度に構成できるバージョンは 1 つのみです。
- **full** *version_format*：次の形式で、各サービスの API 完全バージョンを指定します。

  <Major-version>.<Minor-version>.<patch-version>.[alpha-<draft-number>]

  フォーマットは 、*3GPP TS 29.501* バージョン *15.2.0*、セクション *4.3.1.1*で規定されています。
- **spec** *spec_version*：次のいずれかの値で 3GPP 仕様のバージョン番号を指定します：
  - 15.0.0
  - 15.1.0
  - 15.2.0
  - 15.2.1
  - 15.3.0
  - 15.3.0.custom
  - 15.3.0.std
  - 15.4.0
  - 16.8.1

たとえば、N7（PCF）インターフェイスの 3GPP 2019 年 6 月仕様準拠をサポートするには、仕様バージョンを *15.4.0* として構成します。

デフォルトのバージョン番号は、SMF インターフェイスによって異なります。たとえば、N7 インターフェイスのデフォルトのバージョンは *15.2.0* です。同様に、N10 インターフェイスの場合、デフォルトのバージョンは *15.2.1* です。

- **uri** *uri_version*：各サービスの API バージョン URI を次の形式で指定します。

  v：数字で連結。値は v1 と v2 の両方、または v1 か v2 のいずれかです。

  例：

  ：サービスタイプ nudm-sdm の NRF 構成のコンプライアンスバージョン 15.4.0 では、バージョンの uri-version の構成を v2 に必須にします。コンプライアンスバージョン 15.2.1 の場合、この構成はオプションです。

  —version v1: (- url: '{apiRoot}/nsmf-pdusession/v1').

- **version-list version** *version_name*：3GPP 仕様のコンプライアンス バージョンのリストを指定します。 **version-list version** が1 つのバージョンのみで構成されている場合、 **version** と **version-list version** の両方の CLI がピア NF のバージョン選択ロジックで考慮されます。CLI **version** と **version-list version** の両方が同じ属性のセットを構成できます。

**Note** **version-list version** は N1、N2、N7、N10、N11、N40、および Nnrf インターフェイスでのみサポートされます。

- **mode { active | offline }**：構成した 3GPP コンプライアンス バージョンのステータスを指定します。 **mode** は、CLI **version-list version** でのオプションの構成です。 **mode** のデフォルト値は **active** です。 **version-list version** が2 つのバージョンで構成されている場合、少なくとも 1 つのバージョンは **active** である必要があります。

**Important** 3GPP 仕様バージョン値の構成は、SMF インターフェイスに依存します。前述のすべてのバージョンが SMF インターフェイスのオプションになるわけではありません。3GPP バージョン コンプライアンス構成のオプションとして、上記のバージョンの組み合わせのみが存在します。準拠バージョンの詳細については、標準準拠, on page 650 セクションを参照してください。

**Important** 15.3.0.custom 仕様バージョンはお客様に固有であり、 **nchf-convergedcharging** サービスにのみ適用されます。詳細については、Cisco アカウント担当者にご連絡ください。

この仕様バージョンでは、MultipleUnitUsage 属性は usedUnitContainer フィールドを大文字で送信します。15.3.0 以降の他のすべての仕様バージョンでは、MultipleUnitUsage 属性は UsedUnitContainer フィールドを小文字で送信します。

**Important** リリース バージョン 2023.03.0 は、 **version** と **version-list version** CLI の両方をサポートしています。ただし、 **version** CLI は将来のリリースで廃止されます。

## 設定の確認

UDM メッセージ処理プロファイルが構成されているかどうかを確認するには、次の **show full-configuration profile smf** コマンドを使用します：

```
[smf] smf(config)# show full-configuration profile smf
profile smf smf1
 locality      LOC1
 instances 1 allowed-nssai [ slice1 ]
 instances 1 fqdn cisco.com.apn.epc.mnc456.mcc123 node-id abcdef
 plmn-list mcc 123 mnc 456
 exit
 plmn-list mcc 242 mnc 01
 exit
 plmn-list mcc 310 mnc 210
 exit
 plmn-list mcc 310 mnc 220
 exit
 plmn-list mcc 310 mnc 260
 exit
 plmn-list mcc 310 mnc 310
 exit
 plmn-list mcc 440 mnc 550
 exit
 service name nsmf-pdu
  type               pdu-session
  schema             http
  service-id         1
  version            1.Rn.0.0
  http-endpoint base-url http://smf-service
  icmpv6-profile     icmpprf1
  compliance-profile comp1
  access-profile     access1
  subscriber-policy  polSub
 exit
exit
```

構成を確認するには、3GPP仕様プロファイルコンプライアンスコンフィギュレーションモードで **show full** コマンドを使用します。

```
product smf(config-compliance-comp1)# show full
profile compliance comp1
   service nsmf-pdusession
      version uri v1
      version full 1.0.0
      version spec 15.2.0
```

# サポートされている SMF インターフェイス

このセクションでは、他のネットワーク機能との通信を容易にするために SMF が使用するさまざまなインターフェイスについて説明します。

# GTP インターフェイス

General Packet Radio Service（GPRS）Tunneling Protocol（GTP）は、3G、4G、または 5G ネットワークを介した GPRS コア ネットワークで使用されるプライマリ プロトコルです。GTP は、コア ネットワーク内のモバイル データのシグナリングおよび転送を担います。

GTP は、2 つのコア ユーザー プレーン機能（UPF）間の基準ポイントとして N9 インターフェイスを使用します。

## GTP 原因コードの処理

### 機能説明

SMF は、IE で障害を検出した場合、4G プロシージャの GTP 原因コード処理をサポートします。

セッション要求の作成

SMF では、セッション要求の作成メッセージで次の原因がサポートされます。

**表 *207 :* セッション要求の作成でサポートされる原因**

| 原因 | SMF の動作 |
|---|---|
| Missing or unknown APN | 設定された DNN がセッション作成要求で受信した DNN と一致しない場合、SMF はセッション作成応答内のこの原因値を持つメッセージを拒否し、適切な切断理由を設定します。 |
| User authentication failed | SMF は、RADIUS から失敗した AAA セカンダリ認証応答を受信すると、セッション作成応答でこの原因値を持つメッセージを拒否します。この原因は、認証またはセキュリティ手順の失敗によって要求が拒否されたことを示し、適切な切断理由を設定します。 |
| APN アクセスが拒否されました - サブスクリプションなし | SMF が UDM からサブスクリプション取得失敗応答を受信すると、SMF はセッション作成応答でこの原因値を持つメッセージを拒否します。この原因は、サブスクライバが必要なサブスクリプションを持っていないため、SMF が APN へのユーザーアクセスを拒否したことを示します。SMF では適切な切断理由も設定されます。 |

| 原因 | SMF の動作 |
|---|---|
| 単一のアドレスベアラーのみによる新しい PDN タイプ | デュアル アドレス ベアラー フラグ（DAF）表示が設定されておらず、要求された PDN タイプがセッション作成要求メッセージで IPV4V6 である場合、SMF はセッション作成応答でこの原因値を持つメッセージを拒否します。SMF では適切な切断理由も設定されます。 |
| Late Overlapping Request | セッション作成要求メッセージには、要求が開始された絶対時間を示す発信タイムスタンプが含まれています（13.2.2、TS29.274 で指定されているとおり）。<br>SMF が異なる S-GW から後続の CSR を受信し、「発信タイムスタンプ」のタイムスタンプが既存のセッションに保存されているタイムスタンプよりも古いシーケンス番号になると、SMF はセッション作成の応答のこの原因値を持つ新しい CSR を拒否します。この原因は、着信要求が、新しい要求のタイム スタンプよりも最近のタイム スタンプを持たない既存のセッションと競合することを示します。<br>タイムスタンプの方が新しい場合、SMF は現在の手順を中止し、最新のタイムスタンプで新しい CSR 要求を処理します。 |
| リクエストのタイムアウト | 着信 CSR が origination-time-stamp および maximum-wait-time IE を受信した場合、SMF は Create 手順の開始時に maximum-wait-time 値を使用して SLA タイマーを起動し、タイマーの期限切れ時に Create 手順を中止します。その後、SMF は CSR 応答のこの原因値で拒否します。 |
| ネットワーク設定による新しい PDN タイプ | プロファイル dnn で設定されたセッション タイプが IPv4 または IPv6 であり、セッション作成要求で要求された PDN タイプが IPv4v6 である場合、SMF はセッション作成応答でこの原因値を持つメッセージを拒否します。 |

## ベアラー要求の削除

SMF では、ベアラー要求の削除メッセージで次の原因がサポートされます。

表 *208 :* ベアラー要求の削除でサポートされる原因

| 原因 | シナリオ |
|---|---|
| 再アクティベーションが必要です | SMF は、次の場合にデフォルト ベアラーにこの原因値を付けてベアラー応答の削除を送信します。<br>• CHF 調整<br>• PCF 調整<br>• 内部 DB 競合<br>• セッション レポート（SRSR/GTER/SRIR/SPTER/ERIR） |
| PDN 接続非アクティブ タイマーの期限切れ | SMF は、次の場合にデフォルト ベアラーにこの原因値を付けてベアラー応答の削除を送信します。<br>• CP-IDLE タイマーの期限切れ<br>• UPIR でのセッション レポート<br>• 絶対タイマーの期限切れ |

## *RAN-NAS* 原因 *IE*

SMF は、QoS フローの終了または PDU セッションの終了により、GTP メッセージでアクセスネットワークから RAN/NAS 原因 IE を受信します。SMF は、RuleReport の ranNasRelCauses 属性で受信した原因を PCF に提供します。この原因の詳細については、「3GPP TS 29.274 バージョン 15.4.0」を参照してください。

RAN/NAS 原因 IE は、次の GTP メッセージをサポートしています。

- ベアラー作成応答
- ベアラー更新応答
- ベアラー削除コマンド
- セッション要求の削除

## 指定から導出された原因コードのマッピング

SMF は、UDM および PCF インターフェイスに対する 5G メッセージの原因コード マッピングに基づいた仕様（TS 29.524）をサポートしています。

表 *209 : HTTP* から *5GSM* 原因値へのマッピング：*N10* の障害により、要求が *UDM* によって拒否された

| **N10** での **HTTP** ステータス コード | プロトコルまたはアプリケーションのエラー | **UE** への **5GSM** 原因 |
|---|---|---|
| 403 Forbidden | ROAMING_NOT_ALLOWED | 原因#29：ユーザー認証または承認の失敗 |
| | DNN_NOT_ALLOWED | 原因 #27：DNN の欠落または不明 |
| 404 Not Found | ユーザーが見つかりません | 原因#29：ユーザー認証または承認の失敗 |

表 *210 : HTTP* から *5GSM* への原因値のマッピング：*PCF* による要求が拒否される

| **N7** での **HTTP** ステータス コード | プロトコルまたはアプリケーションのエラー | **UE** への **5GSM** 原因 |
|---|---|---|
| 400 Bad Request | USER_UNKNOWN | 原因#29：ユーザー認証または承認の失敗 |
| | ERROR_INITIAL_PARAMETERS | 原因#31：要求が拒否された、未指定 |
| | ERROR_TRIGGER_EVENT | 原因#31：要求が拒否された、未指定 |
| 403 Forbidden | ERROR_TRAFFIC_MAPPING_INFO_REJECTED | 原因#29：ユーザー認証または承認の失敗 |
| | ERROR_CONFLICTING_REQUEST | 原因 #67：特定のスライスと DNN のリソースが不足している |
| | POLICY_CONTEXT_DENIED | 原因#29：ユーザー認証または承認の失敗 |
| | VALIDATION_CONDITION_NOT_MET | 原因#29：ユーザー認証または承認の失敗 |

## 標準準拠

サポートされる GTP 原因コードは、次の標準に準拠しています：

- 3GPP TS 29.274、バージョン 15.4.0
- 3GPP TS 29.524

## GTP 原因コードの構成

ここでは、原因からクラスへのマッピングおよびクラスから原因へのマッピングを構成する方法について説明します。

送信元インターフェイスの障害の場合、 **cause-map-class** プロファイルは、対応するターゲット インターフェイスに適用する必要がある **class-map-cause** プロファイルを決定します（ただし、アクセス プロファイルでプロファイルが構成されている場合のみ）。それぞれの CLI 構成は、送信元インターフェイスの障害と原因の値に基づいて、ターゲットインターフェイスにユーザー定義の原因の値を送信します。CLI コマンドが構成されていない場合、ターゲットインターフェイスは、指定駆動の原因値をデフォルト値として送信します。

GTP 原因コードの構成には、次の手順が含まれます：

- 原因からクラスへのマッピング構成 （660 ページ）
  - cause-map-class プロファイルでの Cause-to-Class マップの構成 （660 ページ）
  - ネットワーク イーサネット プロファイル下の原因からクラスへのマッピングの構成（661 ページ）
- マッピング構成を原因とするクラス （662 ページ）
  - class-map-cause プロファイルでの Class-to-Cause マップの構成 （662 ページ）
  - アクセス プロファイルでのクラス/ケースマップの構成 （663 ページ）

### 原因からクラスへのマッピング構成

このセクションでは、SMF でクラスへのマッピングを構成する方法を説明します。

#### cause-map-class プロファイルでの Cause-to-Class マップの構成

cause-map-class プロファイル下の cause-to-class マッピングを構成するには、次の構成例を使用します：

```
config
  profile cause-map-class nf-type [ udm | pcf ] cmc_profile_name
    source { status-code httpv2_code cause cause_value } fail-class
failclass_string
    exit
```

**注**：

- **profile cause-map-class nf-type [ udm | pcf ]** *nfprofile_name*：NF プロファイル名を指名して、cause-map-class プロファイルを構成します。
- **source { status-code** *httpv2_code* **cause** *cause_value* **} fail-class** *failclass_string*
  - **status-code** *httpv2_code*：送信元インターフェイスの HTTPv2 ステータス コードを指定します。
  - **cause** *cause_value*：原因の値を文字列として指定します。

- **fail-class** *failclass_string*：障害クラスを文字列として指定します。

- **profile cause-map-class** は、ネットワーク要素のプロファイルに関連付けられます。
- **status-code** および **cause** キーワードはオプションです。両方が構成されている場合、対応する **fail-class** がより高い優先順位になり、**status-code** と **cause**が続きます。

**例**

次に、UDM インターフェイスの構成例を示します：

```
profile cause-map-class nf-type udm UDM-CMC
     source status-code 403 cause DNN_NOT ALLOWED fail-class congestion
```

ネットワーク イーサネット プロファイル下の原因からクラスへのマッピングの構成

ネットワーク要素プロファイルの下で原因からクラスへのマッピングを構成するには、次の構成例を使用します：

```
config
  profile network-element [ udm | pcf ] nfprofile_name
     cause-map-class-profile cmcp_name
     exit
```

**注**：

- **profile network-element [ udm | pcf ]** *nfprofile_name*：ネットワーク要素のプロファイルを構成する NF プロファイル名を指定します。
- **cause-map-class-profile** *cmcp_name*：原因からクラスマップのプロファイル名を指定します。

**例**

次に、UDM インターフェイスの構成例を示します：

```
profile network-element udm nfprf-udm
     cause-map-class UDM-CMC
```

設定例

```
[smf] smf# show running-config profile cause-map-class
profile cause-map-class nf-type udm CMC-UDM-1
 source status-code 500 cause CAUSE2 fail-class failClass2
 source status-code 500 cause CAUSE3 fail-class failClass3
 source status-code 501 cause CAUSE1 fail-class failClass1
 source status-code 502 cause CAUSE2 fail-class failClass1
 source status-code 504 cause CAUSE4 fail-class failClass4
 source status-code 505 cause CAUSE4 fail-class failClass5
exit
profile cause-map-class nf-type udm CMC-UDM-2
 source status-code 501 cause CAUSE1 fail-class failClass6
 source status-code 501 cause any fail-class failClass6
 source status-code 502 cause CAUSE1 fail-class failClass6
 source status-code 502 cause CAUSE2 fail-class failClass6
 source status-code 502 cause any fail-class failClass6
 source status-code any cause CAUSE1 fail-class failClass6
```

```
 source status-code any cause CAUSE2 fail-class failClass6
exit
profile cause-map-class nf-type udm CMC-UDM-3
 source status-code 504 cause CAUSE4 fail-class failClass4
 source status-code 505 cause CAUSE4 fail-class failClass5
exit
profile cause-map-class nf-type pcf PCF-CMC-1
 source status-code 500 cause CAUSE2 fail-class failClass2
 source status-code 500 cause CAUSE3 fail-class failClass3
 source status-code 501 cause CAUSE1 fail-class failClass1
 source status-code 502 cause CAUSE2 fail-class failClass1
 source status-code 504 cause CAUSE4 fail-class failClass4
 source status-code 505 cause CAUSE4 fail-class failClass5
exit
profile cause-map-class nf-type pcf PCF-CMC-2
 source status-code 500 cause any fail-class failClass2
 source status-code 501 cause any fail-class failClass3
 source status-code any cause CAUSE2 fail-class failClass2
 source status-code any cause CAUSE3 fail-class failClass3
exit
[smf] smf#
```

## マッピング構成を原因とするクラス

このセクションでは、SMF でマッピングを原因とするクラスを構成する方法を説明します。

### class-map-cause プロファイルでの Class-to-Cause マップの構成

class-map-cause プロファイルでクラスと原因のマッピングを設定するには、次のサンプル設定を使用します。

```
config
  profile class-map-cause cmc_profile_name
    fail-class failclass_string
      target n11 { status-code  httpv2_code cause cause_value } | [ n1 |
n2 | gtp ] { cause cause_value }
      exit
```

**注**：

- **profile class-map-cause** *cmc_profile_name*：class-map-cause を設定するプロファイル名を指定します。
- **fail-class** *failclass_string*：文字列として障害クラスを指定します。
- **target n11 { status-code** *httpv2_code*：**cause** *cause_value* **} | [ n1 | n2 | gtp ] { cause** *cause_value* **}**：
  - **target**：ターゲット インターフェイスを指定します。
  - **status-code** *httpv2_code*：ターゲット インターフェイスの HTTPv2 ステータス コードを指定します。
  - **cause** *cause_value*：ターゲット インターフェイスの原因の値を指定します。
- **profile class-map-cause** は、アクセス プロファイルに関連付けられています。
- **status-code** キーワードは、GTP、N1、および N2 インターフェイスには適用されません。

**例**

CLI 設定の例を次に示します。

```
profile class-map-cause cmc1
    fail-class congestion
         target gtp cause 72
```

アクセス プロファイルでのクラス/ケースマップの構成

アクセスプロファイルの下で原因からクラスへのマッピングを構成するには、次の構成例を使用します：

```
config
  profile access access_profile_name
     [ gtpc | n1 | n2 | n11 ] class-map-cause-profile cmc_profile_name
     exit
```

**注**：

- **profile access** *access_profile_name*：アクセス プロファイルを構成するプロファイル名を指定します。
- **class-map-cause-profile** *cmc_profile_name*：クラス/原因マップ プロファイルを構成するプロファイル名を指定します。

**例**

CLI 構成の例を次に示します。

```
profile access access1
       n11 class-map-cause cmc1
```

設定例

```
[smf] smf# show running-config profile class-map-cause
profile class-map-cause CMC
 fail-class failClass1
  target n11 status-code 403 cause CA1
  target n1 cause CA_N1
  target n2 cause CA_n2
  target gtp cause 75
 exit
 fail-class failClass2
  target n11 status-code 402 cause CAUSE4
  target n1 cause CAUSE3
  target n2 cause CAUSE2
  target gtp cause 95
 exit
exit
[smf] smf#
```

## GTP 原因コードの処理 OAM サポート

ここでは、この機能の操作、管理、およびメンテナンスに関して説明します。

統計情報サポート

送信元インターフェイスの障害では、次の切断理由が考えられます。

- disk_new_pdn_type_due_to_single_addr_bearer_only：セッション作成応答で原因値「New PDN type due to single address Bearer only」というセッション作成要求の失敗数。
- disk_new_pdn_type_due_to_network_preference：セッション作成応答で、原因値が「New PDN type due to network preference」で失敗したセッション要求の作成数。
- disk_pdnsetup_dnn_missing_or_unknown：セッション作成応答で、原因値が「Missing or unknown APN」で失敗したセッション作成要求の数。
- disk_request_timeout_at_origin_entry：セッション作成応答の「Timed Out Request」という原因値で、失敗したセッション要求の作成数。

# GTPv2 IE および原因コード

## 機能説明

このセクションでは、4G および 5G の手順における GPRS トンネリング プロトコル バージョン 2（GTPv2）の IE と原因コードについて説明します。

原因ソース エラー

原因ソース（CS）ビットは、セッション応答の作成、ベアラー応答の変更、ベアラー障害表示の変更（MBFI）、またはベアラー障害表示の削除（DBFI）で次の原因値をサポートしています。

**表 *211 : CS* ビットの原因**

| 原因値 | シナリオ |
|---|---|
| Context Not Found | サブスクライバが SMF に存在せず、引き継ぎ通知を含むセッション作成応答を受信すると、SMF はこの原因を送信します。 |
| 欠落したまたは不明な APN | [セッション作成応答（Create Session Response）] が欠落している APN または不明な APN を受信すると、SMF はこの原因を送信します。 |
| コンテキストを持つ DBFI が見つかりません | サブスクライバが SMF に存在せず、ベアラーコマンドの削除を受信すると、SMF はこの原因を送信します。 |
| コンテキストが見つからないセッション応答を削除 | サブスクライバが SMF に存在せず、古い TEID でセッション要求の削除を受信すると、SMF はこの原因を送信します。 |

### ベアラー コンテキスト *IE* エラー

Bearer Context IE Error（BCE）ビットは、削除セッション応答、ベアラー変更応答、ベアラー障害表示の変更（MBFI）、またはベアラー障害表示の削除（DBFI）で次の原因値をサポートしています。

**表 *212 : BCE* ビットの原因**

| 原因値 | SMF の動作またはシナリオ |
|---|---|
| コンテキストが検出されない MBFI | SMF は、ベアラー コンテキストで EBI が正しくないベアラー要求の変更を受信すると、この原因を送信します。 |
| コンテキストが検出されない DBFI | SMF は、ベアラー コンテキストで誤った EBI を持つベアラーの削除コマンドを受信すると、この原因を送信します。 |

### リモート ノード エラー

SMF は次のリモート ノード エラーをサポートしています：

- コンテキストが見つかりません
- Missing or unknown APN
- PduSessionType
- 必須 IE の不足
- 不正なメッセージ エラー

## 統計情報サポート

この機能は、GTPC メッセージに関連する次の統計をサポートしています：

**smf_gtpc_msg_stats**

説明：GTPC インターフェイス メッセージの統計

サンプル クエリ：`'smf_gtpc_msg_stats{message_type="modify_bearer_request"}'`

ラベル

- ラベル： `message_type`

  ラベルの説明：GTPC メッセージ タイプ

  例：modify_bearer_request, delete_bearer_request, delete_session_request

- ラベル：`status`

  ラベルの説明：GTPC メッセージ ステータス

  例：試行、成功、失敗

- ラベル：`reason`

  ラベルの説明：失敗に関連付けられた理由。

  Example: ipc_failed, sgw_failure, EGTP_CAUSE_LOCAL_DETACH,
  EGTP_CAUSE_RAT_CHANGED_FROM_3GPP_TO_NON_3GPP,
  EGTP_CAUSE_COMPLETE_DETACH, EGTP_CAUSE_ISR_DEACTIVATION,
  EGTP_CAUSE_ERROR_IND_RCVD_RNC_ENODE, EGTP_CAUSE_IMSI_DETACH_ONLY,
  EGTP_CAUSE_REACTIVATION_REQUESTED,
  EGTP_CAUSE_PDN_RECONNECTION_TO_THIS_APN_DISALLOWED,
  EGTP_CAUSE_ACCESS_CHANGED_FROM_NON_3GPP_TO_3GPP,
  EGTP_CAUSE_PDN_CONN_INACTIVITY_TIMER_EXPIRED,
  EGTP_CAUSE_PGW_NOT_RESPONDING, EGTP_CAUSE_NETWORK_FAILURE,
  EGTP_CAUSE_QOS_PARAMETER_MISMATCH, EGTP_CAUSE_REQ_ACCEPTED,
  EGTP_CAUSE_REQ_ACCEPTED_PARTIALLY,
  EGTP_CAUSE_NEW_PDN_TYPE_NETWORK_PREFERENCE,
  EGTP_CAUSE_NEW_PDN_TYPE_SINGLE_ADDR_BEARER_ONLY,
  EGTP_CAUSE_CONTEXT_NOT_FOUND, EGTP_CAUSE_INVALID_MESSAGE_FORMAT,
  EGTP_CAUSE_VERSION_NOT_SUPPORTED_BY_NEXT_PEER,
  EGTP_CAUSE_INVALID_LENGTH, EGTP_CAUSE_SERVICE_NOT_SUPPORTED,
  EGTP_CAUSE_MANDATORY_IE_INCORRECT, EGTP_CAUSE_MANDATORY_IE_MISSING,
  EGTP_CAUSE_SYSTEM_FAILURE, EGTP_CAUSE_NO_RESOURCES_AVAILABLE,
  EGTP_CAUSE_SEMANTIC_ERROR_IN_TFT_OPERATION,
  EGTP_CAUSE_SYNTACTIC_ERROR_IN_TFT_OPERATION,
  EGTP_CAUSE_SEMANTIC_ERROR_IN_PKT_FILTERS,
  EGTP_CAUSE_SYNTACTIC_ERROR_IN_PKT_FILTERS,
  EGTP_CAUSE_MISSING_OR_UNKNOWN_APN,
  EGTP_CAUSE_UNEXPECTED_REPEATED_IE, EGTP_CAUSE_GRE_KEY_NOT_FOUND,
  EGTP_CAUSE_REALLOCATION_FAILURE, EGTP_CAUSE_DENIED_IN_RAT,
  EGTP_CAUSE_PREFERRED_PDN_TYPE_UNSUPPORTED,
  EGTP_CAUSE_ALL_DYNAMIC_ADDR_OCCPUPIED,
  EGTP_CAUSE_UE_CTX_WO_TFT_ALREADY_ACTIVATED,
  EGTP_CAUSE_PROTOCOL_TYPE_NOT_SUPPORTED,
  EGTP_CAUSE_UE_NOT_RESPONDING, EGTP_CAUSE_UE_REFUSES,
  EGTP_CAUSE_SERVICE_DENIED, EGTP_CAUSE_UNABLE_TO_PAGE_UE,
  EGTP_CAUSE_NO_MEMORY_AVAILABLE,
  EGTP_CAUSE_USER_AUTHENTICATION_FAILED,
  EGTP_CAUSE_APN_DENIED_NO_SUBSCRIPTION, EGTP_CAUSE_REQUEST_REJECTED,
  EGTP_CAUSE_PTMSI_SIGNATURE_MISMATCH, EGTP_CAUSE_IMSI_IMEI_NOT_KNOWN,
  EGTP_CAUSE_SEMANTIC_ERROR_IN_TAD_OPERATION,
  EGTP_CAUSE_SYNTACTIC_ERROR_IN_TAD_OPERATION,
  EGTP_CAUSE_RESERVED_MESSAGE_VALUE_RECEIVED,
  EGTP_CAUSE_PEER_NOT_RESPONDING,
  EGTP_CAUSE_COLLISION_WITH_NETWORK_INIT_REQUEST,
  EGTP_CAUSE_UNABLE_TO_PAGE_UE_DUE_TO_SUSPENSION,
  EGTP_CAUSE_CONDITIONAL_IE_MISSING,
  EGTP_CAUSE_INCOMPATIBLE_APN_REST_TYPE,
  EGTP_CAUSE_INVALID_LENGTH_WITH_PIGGYBACK_MSG,
  EGTP_CAUSE_DATA_FORWARDING_NOT_SUPPORTED,
  EGTP_CAUSE_INVALID_REPLY_FROM_REMOTE_PEER,
  EGTP_CAUSE_FALLBACK_TO_GTPV1, EGTP_CAUSE_INVALID_PEER,
  EGTP_CAUSE_TEMP_REJECTED_DUE_TO_HANDOVER_IN_PROGRESS,

EGTP_CAUSE_REQ_REJECTED_FOR_PMIPV6_REASON, EGTP_CAUSE_APN_CONGESTION, EGTP_CAUSE_BEARER_HANDLING_NOT_SUPPORTED, EGTP_CAUSE_UE_ALREADY_REATTACHED, EGTP_CAUSE_MULTI_PDN_CONNECTION_FOR_APN_NOT_ALLOWED, EGTP_CAUSE_MME_SGSN_REFUSES_DUE_TO_VPLMN_POLICY, EGTP_CAUSE_GTPC_ENTITY_CONGESTION, EGTP_CAUSE_TARGET_ACCESS_RESTRICTED_FOR_THE_SUBSCRIBER, EGTP_CAUSE_UE_TEMP_NOT_REACHABLE_DUE_TO_POWER_SAVING, EGTP_CAUSE_RELOC_FAILURE_DUE_TO_NAS_MSG_REDIRECTION, EGTP_CAUSE_MISSING_TIMESTAMP_OPTION, EGTP_CAUSE_MULTIPLE_HNP_NOT_ALLOWED, EGTP_CAUSE_SN_MALFORMED_MSG, EGTP_CAUSE_INT_TIMEOUT

- ラベル： `qos_5qi`

  ラベルの説明：QoS フローに適用される 5Qi

  例: 1、2、5

- ラベル： `rat_type`

  ラベル説明：要求に関連付けられた無線アクセスのタイプ

  例：EUTRA、NR、WLAN、rat_type_unknown

- ラベル：`smf_current_procedure`

  ラベルの説明：メッセージレベル統計の現在のプロシージャ名

  例：nr_to_untrusted_wifi_handover, eps_fb_ded_brr, PdnDisconnectProcedure, enb_to_untrusted_wifi_handover, pcf_req_ded_brr_create, pcf_req_ded_brr_delete, pcf_req_ded_brr_mod, smf_initiated_pdn_detach, untrusted_wifi_to_enb_handover, upf_sess_report_srir_sess_rel, utn3gpp_to_5g_handover

# Gx インターフェイス

Gx インターフェイスは、SMF とポリシーおよび課金ルール機能（PCRF）間のインターフェイスです。

ここでは、SMF での Gx サポートについて説明します。これには、Gx インターフェイスでサポートされているすべての AVP の詳細が含まれます。

## 機能説明

ポリシー制御および課金（PCC）アーキテクチャにより、オペレータはサービスベースの QoS ポリシーとフローベースの課金制御を実行できます。PCC は、アクセス制御、リソース制御、QoS 制御を提供します。

## 機能の仕組み

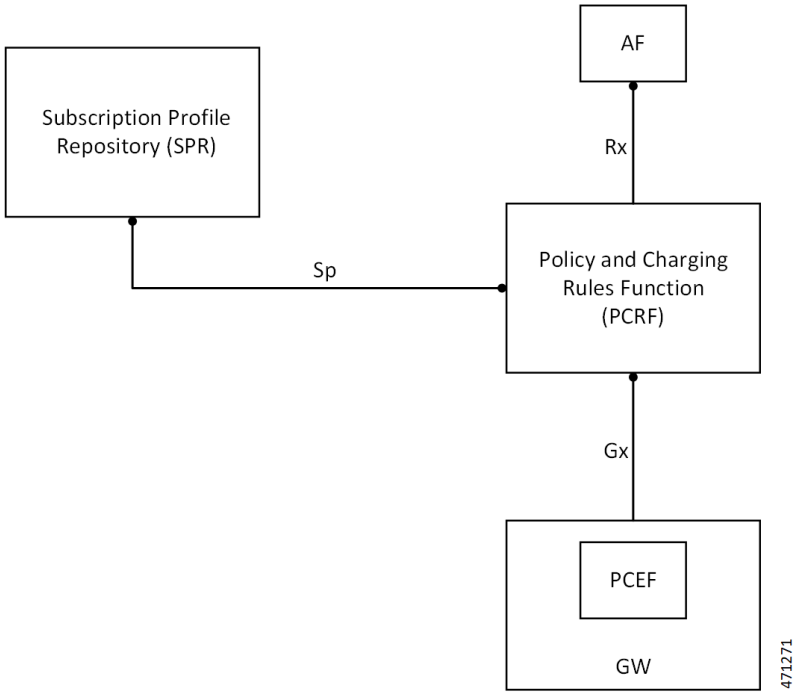
SMF の Gx サポートは、PCC アーキテクチャの次の 2 つの主要な要素を使用します。

- PCEF（SMF 内のポリシー施行機能）

• PCRF（ポリシーおよび課金設定ルール機能の）

Gx 参照点は PCRF と SMF の間にあります。Gx 参照ポイントを使用すると、PCC ルールをプロビジョニングおよび削除できます。次の図は、ポリシーインフラストラクチャに関連するさまざまな要素間の参照ポイントを示しています。

**図 *129 : Gx* インターフェイス**




Gx インターフェイスの実装は、Diameter 接続の一部です。Gx メッセージには、通常、ダイナミック ルールのインストール/削除、事前定義されたルールのアクティブ化/非アクティブ化、および APN-AMBR とデフォルトのベアラー QoS の変更が含まれます。

ルールをベアラーに関連付けるのは、「ベアラー バインディング」のタスクです。PCEF は SMF でこのタスクを実行します。バインド メカニズムは、サービス データ フローを関連付ける手順です。フローは、IP-CAN ベアラーへの SDF テンプレートによって PCC ルールで定義されます（サービス データ フローを転送すると見なされます）。

- **PCEF ベアラー バインド**：PCEF はルールをベアラーにバインドします。このルールは、ベアラーのアクティブ化または更新の実行を必要とする場合があります。SMF サービスは、新しいベアラーを更新または作成するタスクを実行します。この更新は、SGW/MME に対して UBR または CBR 要求を呼び出すことによって発生します。

（注） 現在のリリースでは、デフォルトのベアラーに対してのみ PCEF バインディングがサポートされています。

# Gx 初期接続とデタッチ サポート

次に、SMF の Gx 初期アタッチおよびデタッチのサポートに関連付けられているさまざまなタイプのルールを示します。

- **PCC ルール**：初期アタッチの一部として。PCEF は以下をサポートします。
  - Charging-Rule-Definition AVP を使用したダイナミック ルールのインストール
  - Charging-Rule-Name AVP を使用する事前定義済みルール
  - デフォルト ベアラーにバインドされているベアラー

（注） デフォルトのベアラーでの TFT アップデートの CBR 手順と UBR は、現在のリリースではサポートされていません。

- **ルールベースの選択**：PCEF は、Charging-Rule-Base-Name AVP の処理をサポートします。処理は CCA-I の一部として行われ、ECS ルールベース名の構成が DNN の一部として上書きされます。
- **APN-AMBR**：CCA-I/CCA-U/RAR が処理され、コールに適用される際に PCRF によって QoS-Information AVP の一部となる APN-AMBR 値。
- **[デフォルトベアラー QoS（Default Bearer QoS）]**：CCA-I/CCA-U/RAR 中に Default-EPS-Bearer-QoS AVP を使用して PCRF によって承認された値が処理され、コールに適用されます。

SMF の Gx（CCR/CCA/RAR/RAA）インターフェイスでサポートされる AVP は次のとおりです。

- Origin-Host
- Origin-Realm
- Destination-Realm
- CC-Request-Type
- CC-Request-Number
- Destination-Host
- Subscription-Id
  - Subscription-Id-Type
  - Subscription-Id-Data
- Supported-Features
  - Vendor-Id
  - Feature-List-ID

    - Feature-List
- Network-Request-Support
- Framed-IP-Address
- Framed-IPv6-Prefix
- IP-CAN-Type
- 3GPP-RAT-Type
- Termination-Cause
- User-Equipment-Info
    - User-Equipment-Info-Type
    - User-Equipment -Info-Value
- QoS-Information
    - APN-Aggregate-Max-Bitrate-UL
    - APN-Aggregate-Max-Bitrate-DL
- Default-EPS-Bearer-QoS
    - QoS-Class-Identifier
    - Allocation-Retention-Priority
        - Priority-Level
        - Pre-Emption-Capability
        - Pre-Emption-Vulnerability
- AN-GW-Address
- 3GPP-SGSN-MCC-MNC
- 3GPP-User-Location-Info
- 3GPP-MS-TimeZone
- Called-Station-Id
- Bearer-Usage
- オンライン
- オフライン
- Charging-Rule-Report
    - Charging-Rule-Name
    - Charging-Rule-Base-Name

    - PCC-Rule-Status
    - Rule-Failure-Code
- Event-Trigger
- Access-Network-Charging-Address
- Access-Network-Charging-Identifier-Gx
    - Access-Network-Charging-Identifier-Value
- 課金ルールインストール
    - Charging-Rule-Definition
        - Charging-Rule-Name
        - Service-Identifier
        - Rating-Group
        - Flow-Information
            - Flow-Description
            - ToS-Traffic-Class
            - Security-Parameter-Index
            - Flow-Label
        - フロー ステータス
        - QoS-Information
        - Reporting-Level
        - オンライン
        - オフライン
        - 優先順位
    - Charging-Rule-Name
    - Charging-Rule-Base-Name
- 課金ルール削除
    - Charging-Rule-Name
    - Charging-Rule-Base-Name

SMFは、サポートされている次の機能をGxインターフェイスを介してポリシーサーバ（PCRF）にアドバタイズします。

表 *213 : Feature-List-ID 1* のサポート対象機能

| 機能ビット | 機能 |
|---|---|
| 0 | Rel8 |
| 5 | ADC |

表 *214 :* 機能リスト *ID 2* のサポート対象機能

| 機能ビット | 機能 |
|---|---|
| 7 | Extended-BW-NR |

## Gx の発信元ホストと発信元レルム

各サブスクライバについて、SMF は、Diameter メッセージを介して PCRF から送信された Origin-Realm および Origin-Host 属性情報のレコードを保持します。Origin-Host 属性および Origin-Realm 属性の値が変更された場合、SMF は最新の値を更新し、対応する宛先ホストと対話します。その後、SMF は属性値の変更ごとに policy_pcf_dest_host_change の統計情報を増加させます。

## ダイナミックおよび事前定義済みのルール サポート

### ダイナミック ルール

この機能では、「課金ルールの定義」AVP を使用して、SMF のダイナミックなルールのインストールをサポートします。Charging-Rule-Definition の一部としてサポートされる AVP のリストについては、Gx 初期接続とデタッチ サポート （669 ページ） を参照してください。

（注） ダイナミック ルールのインストールのサポートは、現在のリリースのデフォルトのベアラーでのみ使用できます。

### 定義済みルール

この機能は、「課金ルール名」AVP を使用した SMF の事前定義されたルール（課金ルール名）のインストールをサポートします。

（注） 事前定義されたルールのインストールのサポートは、現在のリリースのデフォルト ベアラーでのみ使用できます。

### 課金ルール ベース名（CRBN）

PCEF は PCRF から「Charging-Rule-Base-Name」AVP を受信すると、AVP を ECS ルールベースまたは ruledef のグループのインストールとして扱います。この動作は、アクティブな課金サービス構成に存在する CLI によって異なります。

```
config
  active-charging service  service_name
    policy-control charging-rule-base-name gor
    end
```

（注） デフォルトでは、「Charging-Rule-Base-Name」AVP がコールの ECS ルールベースです。

### 初期アタッチ/デタッチのための N4 サポート

ユーザープレーンとコントロールプレーンが統合することで、EPC ネットワーク内の他の要素に対してもノードの機能が提供されます。SMF は、UP への N4 インターフェイスをサポートします。

- **初期接続サポート（N4 セッション確立要求）**：

  SMF は、ダイナミック ルールおよび事前定義済みルールに必要な PDR、FAR、QER、URR の送信をサポートしています。

  このサポートは、UPF への N4 確立要求のデフォルト ベアラーにのみ適用されます。

  この機能は、ルールベースの PDR、デフォルトの QoS、APN-AMBR 値の UPF への送信もサポートしています。

- **サポートの分離（N4セッション削除要求）**：

  SMF は、デタッチ手順の一部として N4 セッション削除要求を送信することをサポートしています。

### PCRF に対する CCR の一部としてのサブスクリプション ID

次の CLI は、SMF から PCRF への CCR メッセージのサブスクリプション ID 値を制御します。デフォルト値は none です。

構成オプションは、次のようにアクセス プロファイルで使用できます。

```
config
  profile network-element   network_element_name
    subscription-id id_number
    description id_description
      possible completions { e164 | imsi | nai }
      end
```

### オンラインおよびオフライン AVP

CCR - 初期要求メッセージで PCRF に送信されるオンラインおよびオフラインの AVP 値は、次の方法で制御されます：

- **オンライン AVP が CCR-I で PCRF に送信される**：network-profile-element OCS が構成されており、構成されたルールベースの静的ルールの課金アクションのいずれかに `ccacharge-credit` CLI が含まれている場合、オンライン AVP から PCRF へは次のように送信されますENABLE_ONLINE の場合、それ以外の場合は DISABLE_ONLINE として送信されます。
- **オフライン AVP を CCR-I で PCRF に送信**：network-profile-element OFCS が構成され、構成されたルールベースに `billing-action egcdr` CLI が構成されている場合、オフライン AVP から PCRF へは ENABLE_OFFLINE として送信されます。それ以外の場合は DISABLE_OFFLINE のように送信されます。

### Charging-Rule-Name AVP による事前定義済み Group-of-Ruledef のインストール

この機能は、PCRF からのcharge-rule-name インストールを使用した、事前定義された group-of-ruledefのインストールをサポートします。これは、デフォルト機能で構成は必要ありません。

# Gy インターフェイス

Gy インターフェイスは、SMF 課金トリガー機能（CTF）とオンライン課金システム（OCS）課金データ機能（CDF）間のオンライン課金インターフェイスです。このインターフェイスは、3GPP 標準規格に基づいており、クォータ割り当てに依存しています。OCS は、Diameter クレジット制御サーバーです。これは、SMF にオンライン充電データを提供します。Gy インターフェイスでお客様トラフィックは、ゲートウェイに送りオンラインまたは前払いスタイルで課金されます。SMF は時間ベースと使用量ベースの課金モデルをサポートします。

## Gy 使用状況レポート

### 機能説明

P-GW ユーザープレーンは、さまざまなトリガーの使用状況レポートを送信します。たとえば、ボリューム、時間クォータ、しきい値、有効時間、クォータ保持時間、トラフィック開始（SoT）などです。それ以外の場合、SMF は、課金状態イベントを検出した後、または SMF での PCC ルール削除の一環として使用状況レポートルール（URR）の削除を検出した後、クエリ使用状況レポートを送信します。

使用状況レポートを受信すると、コントロール プレーンは URR を対応する Charging Multiple-Service Credit Control（MSCC）にマッピングします。そして、コントロール プレーンは、それぞれの MSCC のクレジット制御更新要求を開始します。使用状況レポートは、同期または非同期のいずれかです。SMF は、N4 変更応答または N4 削除応答メッセージを介して同期使用状況レポートを受信します。SMF は、N4 セッション レポート要求メッセージを介して非同期使用状況レポートを受信します。

## 機能の仕組み

Gy インターフェイスの使用状況レポートには、次の使用状況レポート手順が含まれます。

- クレジット制御要求のトラフィック開始（SoT）-最初の（CCR-I）要求が最初のアタッチまたはベアラーの作成中に送信されません。
- SoT を含む使用状況レポート：初期接続またはベアラーの作成中にクォータ要求なしで CCRI が送信される
- 事前定義済みルールおよび静的ルール用の SoT
- N4 クエリ URR の応答を変更します。
- N4 セッション レポート リクエスト。
- URR を削除するための N4 変更応答。
- N4 削除セッション応答。

## コール フロー

***SoT*** - 初期接続またはベアラーの作成時に ***CCR-I*** メッセージが送信されない使用状況レポート

このセクションでは、最初の接続またはベアラーの作成中にCCR-Iメッセージが送信されない場合の、SoT での使用状況レポートについて詳しく説明します。

**図 *130 : SoT* - 初期接続またはベアラーの作成時に *CCR-I* メッセージが送信されない使用状況レポート**

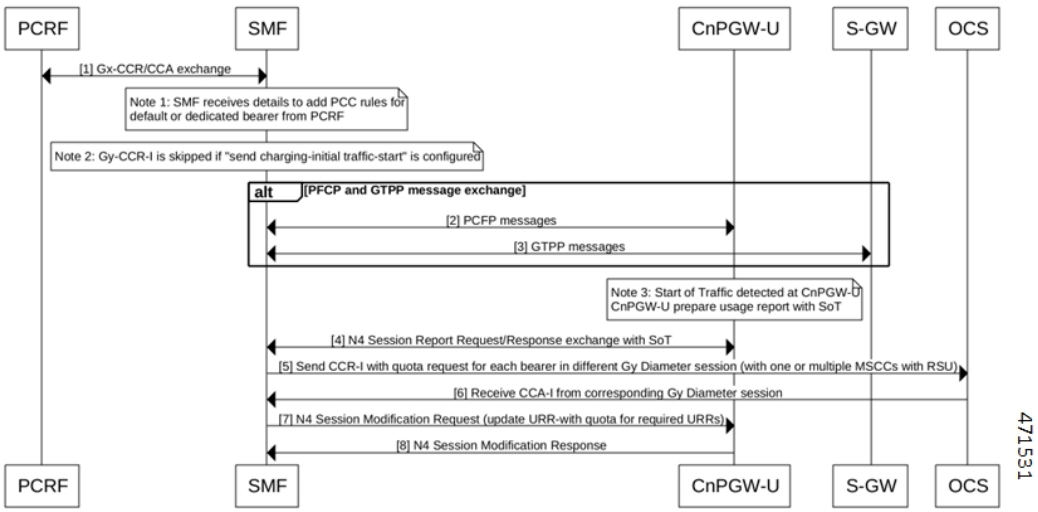


表 *215 : SoT* - 初期接続またはベアラーの作成コール フローの説明で *CCR-I* メッセージが送信されない使用状況レポート

| ステップ | 説明 |
|---|---|
| 1 | PCRF と SMF の両方が、Gx クレジット制御要求（CCR）およびクレジット制御応答（CCA）メッセージを相互に送受信します。<br>（注）<br>• SMF は、PCRF からデフォルトまたは専用ベアラーの PCC ルールを追加するための詳細を受信します。<br>• sendcharge-initial traffic-start 値を構成している場合、PCRF は Gy Credit Control Request-Initial（CCR-I）メッセージを SMF に送信しません。 |
| 2 および 3 | PFCP と GTPP のメッセージ交換が行われます。SMF は PCFP メッセージを CnPGW-U に、GTPP メッセージを S-GW に送信します。<br>（注）<br>CnPGW-U でトラフィックが検出された場合、CnPGW-UはSoTとともに使用レポートを作成します。 |
| 4 | CnPGW-U F は、SoT の詳細とともに N4 セッション レポート要求を SMF に送信します。SMF は N4 セッション レポート レスポンスを CnPGW-U に送信します。 |
| 5 | SMF は、異なる Gy Diameter セッションの各ベアラーに対するクォータ要求を含む CCR-I メッセージを OCS に送信します。これらのセッションには、各料金設定グループおよびサービス ID に対して 1 つずつ、要求されたサービスユニット (RSU) の AVP を 1 つまたは複数の MSCC を含めることができます。 |
| 6 | OCS は、対応する Gy Diameter セッションから SMF に CCA-I メッセージを送信します。Diameter セッションには、各料金設定グループおよびサービス ID のクォータやトリガーなどの詳細が含まれます。 |
| 7 | SMF は N4 セッション変更要求を CnPGW-U に送信します。この要求には、クォータで必要な URR に関する詳細が含まれています。 |
| 8 | CnPGW-U は、N4 セッション変更応答を SMF に送信します。 |

## *SoT* を含む使用状況レポート：初期接続またはベアラーの作成中にクォータ要求なしで *CCR-I* が送信される

このセクションでは、最初の接続またはベアラーの作成中にクォータ要求なしで CCR-I メッセージが送信された場合の SoT での使用状況レポートについて詳しく説明します。

図 *131 : SoT* を含む使用状況レポート：初期接続またはベアラーの作成中にクォータ要求なしで *CCR-I* が送信される

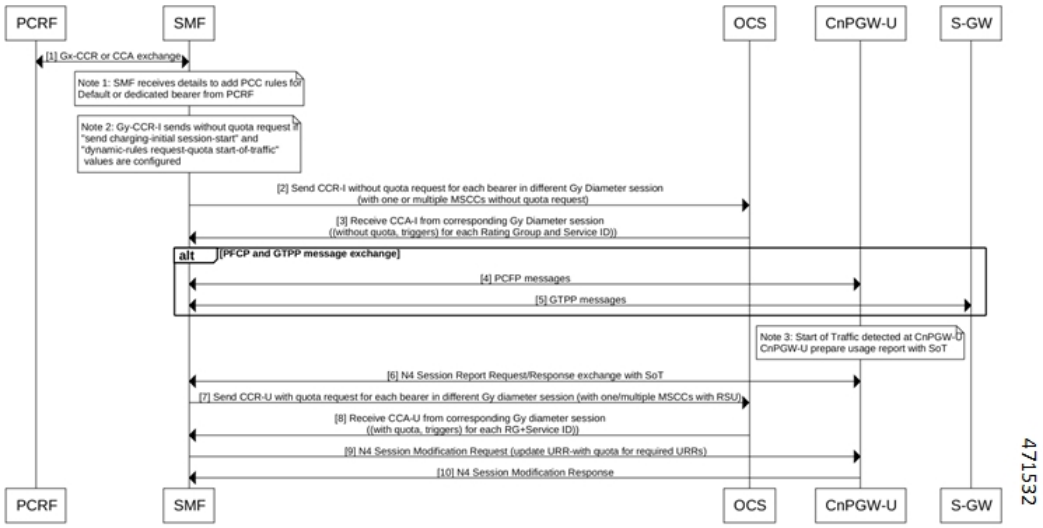



表 *216 : SoT* を含む使用状況レポート：初期接続またはベアラーの作成中にクォータ要求なしで *CCR-I* が送信される

| ステップ | 説明 |
|---|---|
| 1 | PCRF と SMF は相互に Gx クレジット制御要求（CCR）とクレジット制御応答（CCA）メッセージを交換します。<br>（注）<br>• SMF は、PCRF からデフォルトまたは専用ベアラーの PCC ルールを追加するための詳細を受信します。<br>• **send charging-initial session-start** および **dynamic rules request-quota start-of-traffic** 値を設定した場合、PCRF はクォータ要求なしで SMF に Gy CCR-I メッセージを送信します。 |
| 2 | SMF は、様々な Gy Diameter セッションの各ベアラーに対するクォータ要求を含まない CCR-I を OCS に送信します。これらのセッションには、各料金設定グループとサービス ID に 1 つずつ、クォータ リクエストを含まない 1 つまたは複数の MSCC を含めることができます。 |
| 3 | OCS は、対応する Gy Diameter セッションから SMF に CCA-I メッセージを送信します。Diameter セッションはクォータとトリガーなし。 |
| 4 および 5 | PFCP と GTPP のメッセージ交換が行われます。<br>（注）<br>CnPGW-U でトラフィックが検出された場合、CnPGW-UはSoTとともに使用レポートを作成します。 |

| ステップ | 説明 |
|---|---|
| 6 | CnPGW-U は、SoT の詳細とともに N4 セッション レポート要求を SMF に送信します。SMF は N4 セッション レポート レスポンスを CnPGW-U に送信します。 |
| 7 | SMF は、異なる Gy Diameter セッションの各ベアラーに対するクォータ要求を含む CCR-I メッセージを OCS に送信します。これらのセッションでは、Requested-Service-Unit（RSU）AVP を使用して 1 つまたは複数の MSCC を使用できます。 |
| 8 | OCS は、対応する Gy Diameter セッションから SMF にクレジット制御要求：アップデート（CCA-U）メッセージを送信します。Diameter セッションには、各料金設定グループおよびサービス ID のクォータやトリガーなどの詳細が含まれます。 |
| 9 | SMF は N4 セッション変更要求を CnPGW-U に送信します。この要求には、クォータで必要な URR に関する詳細が含まれています。 |
| 10 | CnPGW-U は、N4 セッション変更応答を SMF に送信します。 |

## 事前定義済みルールおよび静的ルール用の *SoT* を含む使用状況レポート

このセクションでは、事前定義済みルールおよび静的ルールの SoT を使用した使用状況レポートについて説明します。

**図 *132 :* 事前定義済みルールおよび静的ルール用の *SoT* を含む使用状況レポート**

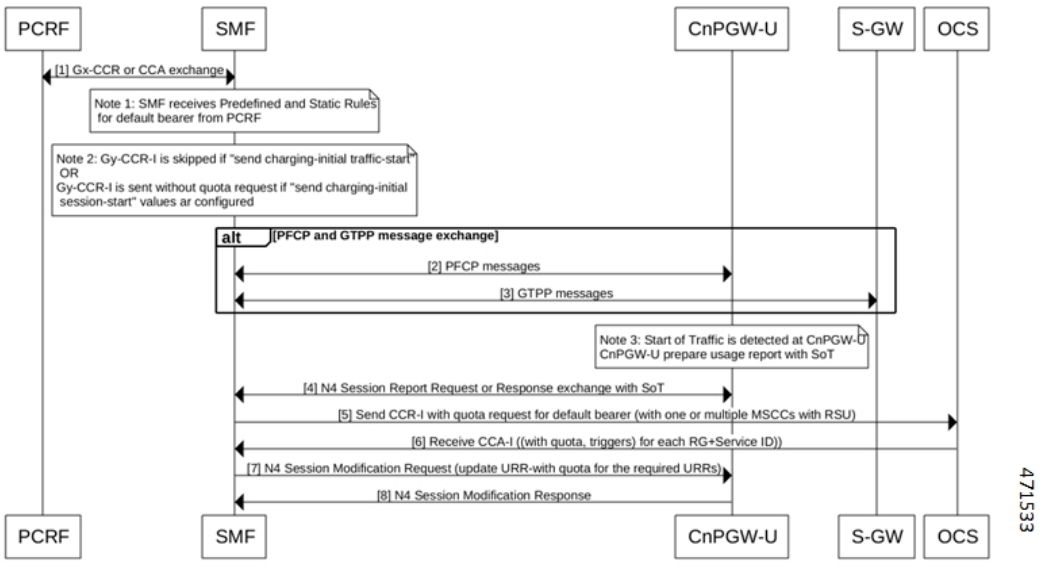


表 *217:* 事前定義済みルールおよび静的ルール用の *SoT* を含む使用状況レポート コール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | PCRF と SMF は相互に Gx CCR と CCA メッセージを交換します。<br>（注）<br>SMF はデフォルトのベアラーの定義済みルールと静的ルールを PCRF から受信します。 |
| 2 および 3 | PFCP と GTPP のメッセージ交換が行われます。SMF は PFCP メッセージを CnPGW-U に、GTPP メッセージを S-GW に送信します。<br>（注）<br>CnPGW-U でトラフィックが検出された場合、CnPGW-UはSoTとともに使用レポートを作成します。 |
| 4 | CnPGW-U は、SoT の詳細とともに N4 セッション レポート要求を SMF に送信します。SMF は N4 セッション レポート レスポンスを CnPGW-U に送信します。 |
| 5 | SMF は、Gy Diameter セッションでデフォルト ベアラーのクォータ要求を含む CCR-I メッセージを OCS に送信します。このセッションでは、各料金設定グループおよびサービス ID に対して 1 つである、要求サービス ユニット（RSU）の AVP を 1 つまたは複数の MSCC に含めることができます。 |
| 6 | OCS は、Gy Diameter セッションの CCA-I メッセージを SMF に送信します。Diameter セッションには、各料金設定グループおよびサービス ID のクォータやトリガーなどの詳細が含まれます。 |
| 7 | SMF は N4 セッション変更要求を CnPGW-U に送信します。この要求には、クォータで必要な URR に関する詳細が含まれています。 |
| 8 | CnPGW-U は、N4 セッション変更応答を SMF に送信します。 |

## *N4* 応答の変更（*URR* クエリ シナリオ）の使用状況レポート

このセクションでは、URR のトリガー イベント、クエリ URR シナリオ内の N4 応答の変更の使用状況レポートの詳細について説明します。

図 *133 : N4* 応答の変更（*URR* クエリ シナリオ）の使用状況レポート

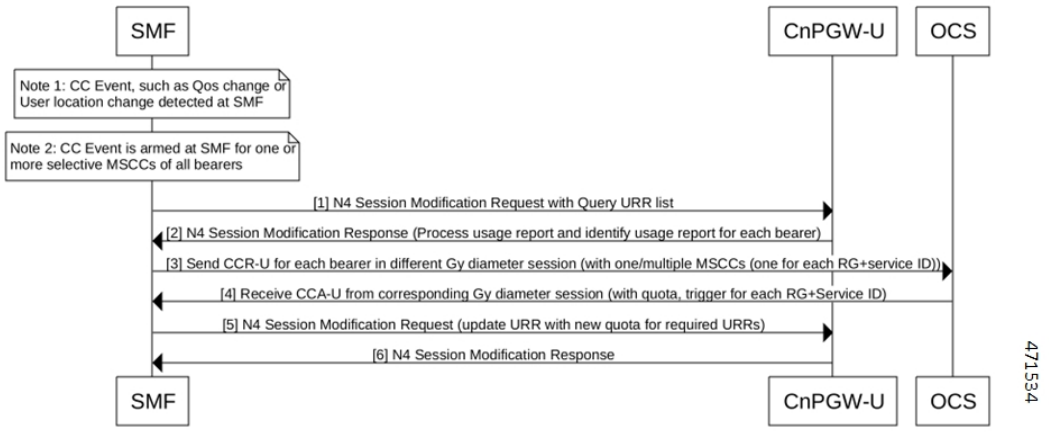



表 *218 : N4* 応答の変更（クエリ *URR* シナリオ）コール フローの説明の使用状況レポート

| ステップ | 説明 |
|---|---|
| 1 | SMF は課金条件イベントを検出し、すべてのベアラーの 1 つ以上の特定の MSCC に対応します。次に、SMF は、装備されているベアラーのクエリ URR のリストを作成します。このリストの作成後、SMF はクエリ URR リストを含む N4 セッション変更要求を CnPGW-U に送信します。 |
| 2 | CnPGW-U は、使用状況レポートとともに N4 セッション変更応答を SMF に送信します。SMF は各ベアラーの使用状況レポートを処理して識別します。 |
| 3 | SMF は、異なる Gy Diameter セッションの各ベアラーの CCR-U メッセージを OCS に送信します。これらのセッションには、各料金設定グループとサービス ID に 1 つずつ、1 つまたは複数の MSCC を含めることができます。 |
| 4 | OCS は、対応する Gy Diameter セッションから SMF に CCA-U メッセージを送信します。Diameter セッションには、各料金設定グループおよびサービス ID のクォータやトリガーなどの詳細が含まれます。 |
| 5 | SMF は N4 セッション変更要求を CnPGW-U に送信します。この要求には、クォータで必要な URR に関する詳細が含まれています。 |
| 6 | CnPGW-U は、N4 セッション変更応答を SMF に送信します。 |

## *N4* セッション レポート

このセクションでは、N4 セッション レポートの詳細について説明します。

図 *134 : N4* セッション レポート

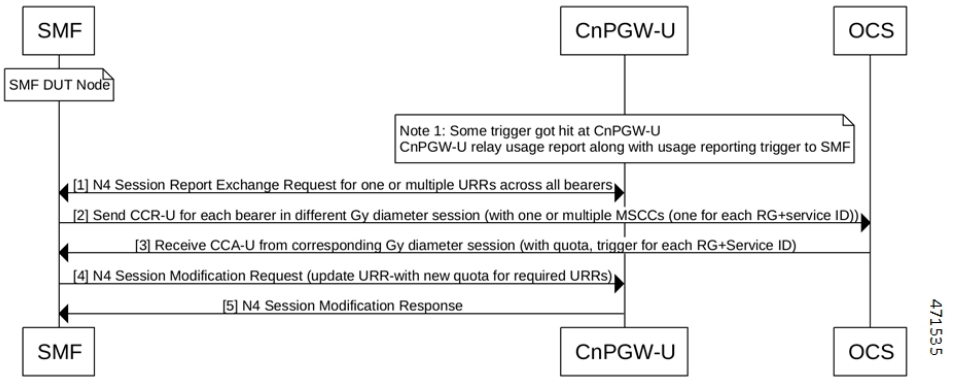



表 *219 : N4* セッション レポートのコール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | テスト対象デバイス（DUT）ノードが SMF 上にあります。<br>（注）<br>CnPGW-Uには、しきい値、クォータ、トリガーなどの値を持つさまざまなURRが含まれています。一部のトリガーは、特定の URR の CnPGW-U でヒットします。CnPGW-U は、使用状況レポート トリガーとともに使用状況レポートを SMF に送信します。<br><br>CnPGw-U は、ベアラー全体で 1 つまたは複数の URR に関する N4 セッションレポートを SMF に送信します。 |
| 2 | SMF は、異なる Gy Diameter セッションの各ベアラーの CCR-U メッセージを OCS に送信します。これらのセッションには、各料金設定グループとサービス ID に 1 つずつ、1 つまたは複数の MSCC を含めることができます。 |
| 3 | OCS は、対応する Gy Diameter セッションから SMF に CCA-U メッセージを送信します。Diameterセッションには、各料金設定グループおよびサービスIDのクォータやトリガーなどの詳細が含まれます。 |
| 4 | SMF は N4 セッション変更要求を CnPGW-U に送信します。このリクエストには、新しいクォータで必要な URR に関する詳細が含まれています。 |
| 5 | CnPGW-U は、N4 セッション変更応答を SMF に送信します。 |

## *N4* 応答の変更（*URR* 削除シナリオ）の使用状況レポート

このセクションでは、URRの削除シナリオのN4応答の変更の使用状況レポートの詳細について説明します。

図 *135 : N4* 応答の変更（*URR* 削除シナリオ）の使用状況レポート

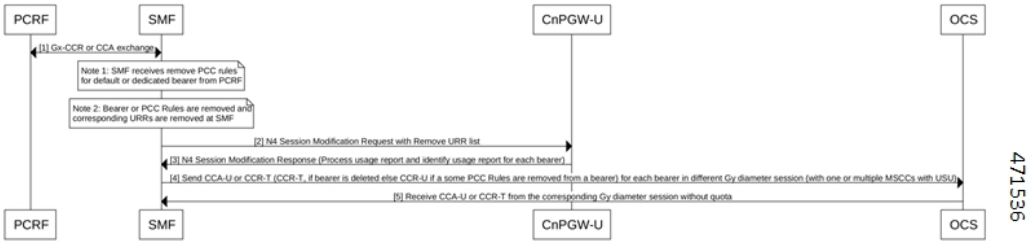



表 *220 : N4* 応答の変更（*URR* シナリオ削除）コール フローの説明の使用状況レポート

| ステップ | 説明 |
|---|---|
| 1 | PCRF と SMF は両方とも、Gx CCR と CCA メッセージを交換します。<br>（注）<br>• SMF は PCRF から、削除 URR リストを含む N4 セッション変更要求を受信します。<br>• SMF により、ベアラー ルールまたは PCC ルールと対応する URR が削除されます。 |
| 2 | SMF は、URR リストの削除を含む N4 セッション変更要求を CnPGW-U に送信します。 |
| 3 | CnPGW-U は、N4 セッション変更応答を SMF に送信します。SMF は各ベアラーの使用状況レポートを処理して識別します。 |
| 4 | SMF が 1 つのベアラーから 1 つまたは複数の PCC ルールを削除する場合、SMF は OCS に異なる Gy Diameter セッションの各ベアラーの CCA-U または credit Control Answer - Terminate (CCR-T) メッセージを送信します。これらのセッションには、Used Service Unit（USU）を割り当てて 1 つまたは複数の MSCC を含めることができます。 |
| 5 | OCS は、対応する Gy Diameter セッションからの CCA-U または CCA-T メッセージをクォータなしで SMF に送信します。 |

## *N4* 削除セッション応答の使用レポート

このセクションでは、N4 削除セッション応答の使用状況レポートに関する情報を提供します。

図 *136 : N4* 削除セッションの使用状況レポート

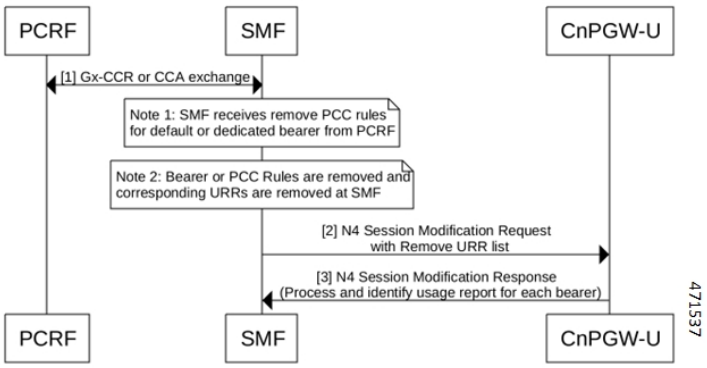



表 *221 : N4* セッション削除コール フローの説明の使用状況レポート

| ステップ | 説明 |
|---|---|
| 1 | （注）<br>SMF が UE またはネットワークが開始した削除セッションを検出します。<br><br>SMF は、N4 セッション要求を CnPGW-U に送信してセッションを削除します。<br>CnPGW-U は、N4 セッション削除応答で使用状況レポートを SMF に送信します。 |
| 2 | SMF は、異なる Gy Diameter セッションの各ベアラーの CCR-T メッセージを OCS に送信します。これらのセッションでは、USU を使用して 1 つまたは複数の MSCC を使用できます。 |
| 3 | OCS は、対応する Gy Diameter セッションから SMF に CCA-T メッセージを送信します。 |

# Gy 障害処理

## 機能説明

Diameter 障害処理テンプレートは、さまざまな Diameter サービスに関連付けられています。Diameter エンドポイント ポッドが、OCS から Gy メッセージのコマンド レベルの障害を受信します。次に、Diameter エンドポイント ポッドがエラー処理設定を処理します。

## サポートされるアクションとサブアクション

次の表に、Gy インターフェイスでサポートされている失敗処理テンプレートのアクションとサブアクションを示します。

表 *222 :* サポートされる失敗処理テンプレートのアクションとサブアクション

| 操作 | サブアクション |
|---|---|
| 続行（Continue） | • FHSubActionEnum_UNKNOWN<br>• FHSubActionEnum_DISCARD_TRAFFIC |
| Terminate | • FHSubActionEnum_WITH_TERM_REQUEST<br>• FHSubActionEnum_WITHOUT_TERM_REQUEST |

## 使用例

テンプレート アクションの失敗処理に対する課金動作

次の表に、失敗処理テンプレート アクションの課金動作を示します。

表 *223 :* テンプレート アクションの失敗処理に対する課金動作

| 手順 | 失敗処理テンプレート（アクションとサブアクション） | SMF の動作 |
|---|---|---|
| CCR-I（PDN セットアップ） | 続行 + 不明/なし | 課金の無効化<br>URR は作成されていません。<br>切断手順中に Gy CCR-T を使用できません。<br>トリガまたは更新中の Gy CCR-U はありません。<br>Gy オフライン課金「「Charging-params」で有効（デフォルト ベアラーのみ） |
| | 続行 + 破棄 | 転送アクション ルール(FAR)のドロップ<br>ドロップ FAR ID を使用して URR を送信します。<br>切断手順中に Gy CCR-T を使用できません。<br>トリガまたは更新中の Gy CCR-U はありません。<br>Gy オフライン課金「「Charging-params」で有効（デフォルト ベアラーのみ） |
| | 用語なしで + を終了 | Gy CCR-T メッセージなしでセッションを終了する |
| | 用語ありで + を終了 | Gy CCR-T メッセージでセッションを終了する |

| 手順 | 失敗処理テンプレート（アクションとサブアクション） | SMF の動作 |
|---|---|---|
| CCR-I（トラフィックの開始） | 続行 + 不明/なし | **既知の URR**：<br>高クォータを割り当てる<br>切断中に Gy CCR-T がありません。<br>トリガまたは更新中の Gy CCR-U はありません。<br>Gy オフライン課金「「Charging-params」で有効（デフォルト ベアラーのみ）<br>**不明な URR**：<br>OCS 課金の無効化<br>URR は作成されていません。<br>切断中に Gy CCR-T がありません。<br>トリガまたは更新中の Gy CCR-U はありません。<br>Gy オフライン課金「「Charging-params」で有効（デフォルト ベアラーのみ） |
| | 続行 + 破棄 | FAR のドロップ<br>ドロップ FAR ID で URR を送信します<br>切断中に Gy CCR-T がありません。<br>トリガまたは更新中の Gy CCR-U はありません。<br>Gy オフライン課金「「Charging-params」で有効（デフォルト ベアラーのみ） |
| | 用語なしで + を終了 | Gy CCR-T メッセージなしでセッションを終了する |
| | 用語ありで + を終了 | Gy CCR-T メッセージでセッションを終了する |

| 手順 | 失敗処理テンプレート（アクションとサブアクション） | SMF の動作 |
|---|---|---|
| MBR の手順：<br>**シナリオ**：<br>N4 の変更（クエリ URR）<br>Gy CCR-U（使用量）<br>Gy CCA-U（失敗） | 続行 + なし | 高クォータを割り当てる<br>送信済み CCR-T がデタッチされました<br>"Charging-params" で Gy オフライン充電「有効」に設定（デフォルトの ebarer のみ） |
| | 続行 + 破棄 | FAR のドロップ<br>URR をドロップ FAR にリンクします。<br>送信済み CCR-T をデタッチしました<br>GyOffline 課金は、「Charging-params」で「Enabled」になっています（デフォルト ベアラーのみ）。 |
| | 用語なしで + を終了 | デフォルトベアラーの場合は、Gy CCR-T を使用せずにセッションを終了します。 |
| | 用語ありで + を終了 | デフォルトベアラーの場合は、Gy CCR-T でセッションを終了します。 |

| 手順 | 失敗処理テンプレート（アクションとサブアクション） | SMF の動作 |
|---|---|---|
| デフォルトベアラー手順（UBR）：<br>**シナリオ**：<br>UBR（QoS の変更）<br>N4 の変更<br>Gy CCR-U<br>Gy CCA-U が失敗 | 続行 + なし | 高クォータを割り当てる<br>送信済み CCR-T をデタッチ<br>Gy オフライン課金「「Charging-params」で有効（デフォルト ベアラーのみ） |
| | 続行 + 破棄 | FAR のドロップ<br>FAR をドロップするための URR がリンクで作成されました。<br>送信済み CCR-T をデタッチ<br>Gy オフライン課金「「Charging-params」で有効（デフォルト ベアラーのみ） |
| | 用語なしで + を終了 | デフォルトベアラーの場合は、Gy CCR-T を使用せずにセッションを終了します。 |
| | 用語ありで + を終了 | デフォルト ベアラーの場合は、CCR-T でセッションを終了します。 |

| 手順 | 失敗処理テンプレート（アクションとサブアクション） | SMF の動作 |
|---|---|---|
| デフォルトベアラーの使用状況レポート：<br>シナリオ：<br>セッション レポート（デフォルト ベアラー URR の場合）<br>Gy CCR-U<br>Gy CCA-U（失敗） | 続行 + なし | 高クォータを割り当てる<br>送信済み CCR-T をデタッチ<br>Gy オフライン課金「「Charging-params」で有効（デフォルト ベアラーのみ） |
| | 続行 + 破棄 | FAR のドロップ<br>FAR をドロップするための URR がリンクで作成されました<br>送信済み CCR-T をデタッチ<br>Gy オフライン課金「「Charging-params」で有効（デフォルト ベアラーのみ） |
| | 用語なしで + を終了 | デフォルトベアラーの場合は、Gy CCR-T を使用せずにセッションを終了します。 |
| | 用語ありで + を終了 | デフォルトベアラーの場合は、Gy CCR-T でセッションを終了します。 |

### *BGIPC* の障害

Gy インターフェイスは、BGIPC タイムアウトおよび障害処理テンプレートを考慮します。この動作は、Gx インターフェイスにも適用されます。

### 非 *Gy* 障害の課金動作の課金

次の表に、Gy 以外の障害の課金動作を示します。

**表 *224* : 非 *Gy* 障害の課金動作の課金**

| 手順 | 手順 | 失敗 |
|---|---|---|
| 1 | PDN セットアップ | N4 の障害 |
| 2 | PDN 変更（MBR） | |

| 手順 | 手順 | 失敗 |
|---|---|---|
| 2.1 | フロー：<br>• N4 変更要求（クエリ URR）<br>N4変更応答（使用状況）：<br>• Gy CCR-U（使用とトリガー）<br>• Gy CCA-U（クォータ）<br>N4 変更（クォータ）<br>• Gx CCR-U | 最初の N4（クエリ URR 用 |
| 2.2 | | CCA-U 後の 2 番目の N4（ |
| 3 | アクセス失敗 | UBR |

## Diameter セッション フェールオーバー

機能説明

このセクションでは、Diameter インターフェイス上で 4G セッション障害を処理する際の SMF の動作について説明します。

機能の仕組み

この機能の一部として、次の機能が追加されました：

- SMF は、OCS から CCA-I および CCA-U で受信した CC-Session-Failover AVP を処理します。
- SMF は、CC-Session-Failover AVP を受信すると、Diameter セッションの最新の AVP 情報を上書きして保存します。
- 構成および CC セッション フェールオーバー AVP 情報に基づいて、SMF サービスは、Diameterエンドポイントへの CCR-U または CCR-T の次の後続の要求で、セッション フェールオーバー フラグ表示を送信します。
- セッション フェールオーバー CLI が有効になっており、OCS が CC セッション フェールオーバー AVP を送信した場合、失敗の処理テンプレートでプロビジョニングされていると、SMF はセカンダリ サーバへの要求を再試行します。
- フェールオーバーは、応答メッセージ内のサーバによって上書きされ、SMF サービス通知フラグよりも優先されます。

セッション フェールオーバーの構成

高速フェールオーバーを構成するには、このコマンドを使用します。

```
config
  profile charging charging_profile_name
     [ default | no ] session failover
     exit
```

注：

- **profile charging** *charge_profile_name*：課金プロファイル名を指定します。 *charge_profile_name* は 英数字の文字列である必要があります。
- **default session failover**：デフォルト設定でこのコマンドを構成します。

（注） デフォルト設定は、失敗処理の構成によって異なります。

- **no session failover**：プライマリ サーバに到達できない場合は、フェールオーバーはトリガされず、セッションが破棄されます。フェールオーバー アクションは実行されません。
- **session failover**：SMF は、失敗処理テンプレートに基づいてプロビジョニングされている場合、セカンダリ サーバに要求を再試行します。

### 設定の確認

UDM セッション フェールオーバー処理プロファイルが構成されているかどうかを確認するには、次のコマンドを使用します：

```
smf# show running-config profile charging chp
profile charging chp
  session failover
exit
```

## Diameter クレジット制御障害の処理

**表 *225*：機能の履歴**

| 機能名 | リリース情報 | 説明 |
|---|---|---|
| Gy 要求失敗処理に対する credit-Control-Failure-Handling AVP の使用 | 2023.04 | SMF は、credit-Control-Failure-Handling AVP の値を使用して、ネットワークの問題によって要求が阻止される場合に、Gy要求の失敗処理動作を導き出します。 |

機能説明

課金の一環として、SMF サービス ポッドと Diameter エンドポイントの間でメッセージ交換が行われます。障害処理の動作を定義するには、オンライン課金サーバ（OCS）が、

Credit-Control-Failure-Handling 属性値ペア（AVP）を Diameter エンドポイントに送信します。Diameter エンドポイントは、受信した Gy Credit Control Answer - Initial（CCA-I）または Gy Credit Control Answer - Update（CCA-U）メッセージを Credit-Control-Failure-Handling AVP とともに転送します。SMF サービス ポッドは、CCA-I または CCA-U OCS 応答メッセージからこの AVP を保存し、後続の Credit-Control-Failure-Handling AVP を後続の Credit Control Response - Update (CCR-U) メッセージに含めます。次に、Diameter エンドポイントはこの AVP 値を使用して、OCS から応答を受信しなかった場合、またはコマンド レベルの障害結果コードを受信した場合の Gy 障害処理動作を導き出します。

SMF は既存の AVP 値を上書きし、Diameter セッションごとに最新の値を課金サブスクライバ データに保存します。SMF サービスは、後続のクレジット制御要求更新メッセージにクレジット制御機能不全の処理 AVP の保存された値を含めます。このメッセージを受信した後、Diameter エンドポイントはこの AVP の値を抽出し、OCS に送信します。

（注） Diameter クレジット制御の障害処理は、Diameter セッション フェールオーバーよりも優先され、クレジット制御障害処理 AVP の受信値に基づいてアクションとサブアクションを適用します。

機能の仕組み

Diameter エンドポイントは、CSR-U メッセージの Credit-Control-Failure-Handling AVP の次の値を SMF に送信します。

- Terminate：Diameter エンドポイントは、アクションを Termination、サブアクションを without-termination として SMF サービスポッドに送信します。
- Continue：Diameter エンドポイントは、アクションを continue として、サブアクションを none として SMF サービスポッドに送信します。
- [Retry-AND-Terminate]：Diameter エンドポイントは、成功メッセージを受信するか、再試行回数を超えるまで、アクションを再試行として送信します。再試行回数を超えた後、Diameter エンドポイントは、アクションを terminate として、サブアクションを without-termination として SMF サービスポッドに送信します。

（注） 再試行回数の値は、失敗処理テンプレートから導出されます。

次の表は、OCS が SMF サービスに送信する Credit-Control-Failure-Handling AVP 値のリストの例です。SMF サービスは、後続の CCR-U メッセージの受信した値を保存します。

表 *226 : OCS* から *SMF* へのクレジット制御障害処理 *AVP* 値

| | 以前の **CCA-I** または **CCA-U** メッセージの **OCS AVP** 値 | **CCR-U** メッセージでの **Diameter** エンドポイントへの **Smf-service** 通知 |
|---|---|---|
| 1 | CreditControl<br>FailureHandling AVP（終了） | CreditControl<br>FailureHandling AVP（終了） |
| 2 | CreditControl<br>FailureHandling AVP（続行） | CreditControl<br>FailureHandling AVP（続行） |
| 3 | CreditControl<br>FailureHandling AVP<br>（Retry-AND-Terminate） | CreditControl<br>FailureHandling AVP（Retry-AND<br>-Terminate） |

# Gy MSCC レベルの失敗結果コード

## 機能説明

このセクションでは、一時的な障害（4xxx）および永続的な障害（5xxx）の結果コードを「MSCC レベルで受信した障害結果コード」を受信した場合の SMF の動作について説明します。

表 *227 :* 一時的な障害（*4XXX*）

| 結果コード | 説明 |
|---|---|
| 4010 | DIAMETER_END_USER_SERVICE_DENIED |
| 4011 | DIAMETER_CREDIT_CONTROL_NOT_APPLICABLE |
| 4012 | DIAMETER_CREDIT_LIMIT_REACHED |

表 *228 :* 恒久的なエラー（*5XXX*）

| 結果コード | 説明 |
|---|---|
| 5003 | DIAMETER_AUTHORIZATION_REJECTED |
| 5012 | DIAMETER_UNABLE_TO_COMPLY |
| 5030 | DIAMETER_USER_UNKNOWN |
| 5031 | DIAMETER_RATING_FAILED |

## 機能の仕組み

次の表では、さまざまな SMF の一時的および永続的な障害結果コードについて説明します。

| 障害コード | 説明 |
|---|---|
| SMF は、CCAI のすべての永続的な障害結果コードと一時的な障害結果コード4010および4012 を受信します。 | SMF が PFCP_SESSION_ESTABLISHMENT_REQUEST でゼロの時間とボリューム クォータを送信します |
| SMF は CCAU のすべての永続的な障害結果コードと一時的な障害結果コード4010および4012 を受信します | SMF が PFCP_SESSION_MODIFICATION_REQUEST でゼロの時間とボリュームク ォータを送信します |
| SMF が CCAI で一時的な障害結果コード 4011 を受信します | SMF が PFCP_SESSION_ESTABLISHMENT_REQUEST で高い（最大）時間とボリュームクォータを送信します |
| SMF が CCAU で一時的な障害結果コード 4011 を受信します | SMF が PFCP_SESSION_ESTABLISHMENT_REQUEST で高い（最大）時間とボリュームクォータを送信します |
| SMF が CCAU で一時的な障害結果コード 4011 を受信します | PFCP_SESSION_MODIFICATION_REQUEST で SMF の最大時間およびボリュームクォータが高（最大）になります |
| SMF は、PFCP_SESSION_DELETION_RESPONSE メッセージで「**termr**」トリガを使用して使用状況レポートを受信します。 | • SMF が、4010 および 4012 の MSCC 障害コードを受信した URR に対して、3GPP レポートの理由が「FINAL」の CCRT メッセージを送信します<br>• SMF が、MSCC 障害コード 4011 を受信した URR に対して MSCC なしの CCRT メッセージを送信します<br>• SMF は、すべての永続的障害結果コードを受信した URR に対して、USU(時間(0) + ボリューム(0))および 3GPP レポートの理由に「FINAL」の CCRT メッセージを送信します |

SMF は CCAI のすべての永続的な障害結果コードと一時的な障害結果コード 4010 および 4012 を受信します。

- SMF は PFCP_SESSION_ESTABLISHMENT_REQUEST でゼロの時間とボリュームのクォータを送信します。SMF は、CCAU の永続的な障害結果コードと一時的な障害結果コード 4010 および 4012 をすべて受信します。

- SMF が PFCP_SESSION_MODIFICATION_REQUEST でゼロの時間とボリュームのクォータを送信する：SMF は、CCAI で一時的な障害結果コードを 4011 として受信します。
- SMF が PFCP_SESSION_ESTABLISHMENT_REQUEST で高い（最大の）時間とボリュームのクォータを送信する：SMF は、CCAU で一時的な障害結果コードを 4011 として受信します。

## アーキテクチャ

このセクションでは、Gy インターフェイスから受信したクレジット制御アプリケーション（CCA）メッセージでの、MSCC レベルでの複数サービス クレジット制御（MSCC）失敗結果コードの処理に関連する詳細のキャプチャについて説明します。この機能により、SMF は、**CCAI** および **CCAU** メッセージの Gy インターフェイスから MSCC レベルで一時的な障害（4xxx）と永続的な障害（5xxx）を処理できます。

## 結果コード

次の表に、一時的な障害（4xxx）および永続的な障害（5xxx）の結果コードのさまざまな結果コードと動作を示します。

**表 *229 :* 結果コード**

| 結果コード | Behaviour |
|---|---|
| 4010/4012 (CCAI) | 1. **CCAI** は **4010/4012**で受信します<br>2. **PFCP_SESSION_ESTABLISHMENT_REQUEST** goes with **CREATE FAR** with APPLY ACTION as DROP:1, **CREATE URR** with REPORTING_TRIGGERS as "volqu, timqu" and VOLUME_QUOTA as 'volume_quota' : {'dlvol': 1, 'ulvol': 1, 'tovol': 1, 'total_vol': 0, 'up_vol': 0, 'down_vol': 0}, TIME_QUOTA as 'tm_quta' : 0 |
| 4010/4012（CCAU） | 1. **CCAU** が **4010/4012**で受信されました<br>2. **PFCP_SESSION_MODIFICATION_REQUEST** goes with **UPDATE FAR** with APPLY ACTION as DROP:1, **UPDATE URR** with REPORTING_TRIGGERS as "volqu, timqu" and VOLUME_QUOTA as 'volume_quota' : {'dlvol': 1, 'ulvol': 1, 'tovol': 1, 'total_vol': 0, 'up_vol': 0, 'down_vol': 0}, TIME_QUOTA as 'tm_quta' : 0 |

| 結果コード | Behaviour |
|---|---|
| 4010/4012 (CCRT) | 1. **TMQ** トリガを使用して使用状況レポートで受信した **PFCP_SESSION_DELETION_REQUEST**<br>2. **CCRT** は 3GPP レポートの理由を「FINAL」にする必要があります |
| 4011（CCAI） | 1. **CCAI** が **4011**で受信しました<br>2. **PFCP_SESSION_ESTABLISHMENT_REQUEST** goes with **CREATE FAR** APPLY ACTION as DROP:1, **CREATE URR** with REPORTING_TRIGGERS as "volqu, timqu" and VOLUME_QUOTA as 'volume_quota' : {'dlvol': 1, 'ulvol': 1, 'tovol': 1, 'total_vol': 9223372036854775807, 'up_vol': 9223372036854775807, 'down_vol': 9223372036854775807}, TIME_QUOTA as 'tm_quta' : 2147483647, TIME_THRESHOLD as 'time_treshold' : 10 |
| 4011（CCAU） | 1. **CCAU** が **4011**で受信しました<br>2. **PFCP_SESSION_MODIFICATION_REQUEST** should go with **UPDATE FAR** APPLY ACTION as DROP:1, **UPDATE URR** with REPORTING_TRIGGERS as "volqu, timqu" and VOLUME_QUOTA as 'volume_quota' : {'dlvol': 1, 'ulvol': 1, 'tovol': 1, 'total_vol': 9223372036854775807, 'up_vol': 9223372036854775807, 'down_vol': 9223372036854775807}, TIME_QUOTA as 'tm_quta' : 2147483647, TIME_THRESHOLD as 'time_treshold' : 10 |
| 4011（CCRT） | 1. **TMQ** トリガを使用して使用状況レポートで受信した **PFCP_SESSION_DELETION_REQUEST**<br>2. **CCRT** には MSCC なし |

| 結果コード | Behaviour |
|---|---|
| 5003/5012/5030/5031<br>CCA-I | 1. **CCAI** は **5003/5012/5030/5031** で受信します<br>2. **PFCP_SESSION_ESTABLISHMENT_REQUEST** goes with **CREATE FAR** with APPLY ACTION as DROP:1, **CREATE URR** with REPORTING_TRIGGERS as "volqu, timqu" and VOLUME_QUOTA as 'volume_quota' : {'dlvol': 1, 'ulvol': 1, 'tovol': 1, 'total_vol': 0, 'up_vol': 0, 'down_vol': 0}, TIME_QUOTA as 'tm_quta' : 0 |
| 5003/5012/5030/5031<br>CCA-U | 1. **CCAU** が **5003/5012/5030/5031** で受信しました<br>2. **PFCP_SESSION_MODIFICATION_REQUEST** goes with **UPDATE FAR** with APPLY ACTION as DROP:1, **UPDATE URR** with REPORTING_TRIGGERS as "volqu, timqu" and VOLUME_QUOTA as 'volume_quota' : {'dlvol': 1, 'ulvol': 1, 'tovol': 1, 'total_vol': 0, 'up_vol': 0, 'down_vol': 0}, TIME_QUOTA as 'tm_quta' : 0 |
| 5003/5012/5030/5031<br>(CCRT) | 1. **TMQ** トリガを使用して使用状況レポートで受信した **PFCP_SESSION_DELETION_REQUEST**<br>2. **CCRT** では USU(時間(0)+ボリューム(0)) および 3GPP-Reporting-Reason が「FINAL」になります |

（注） SMF が URRS でサポートされている障害コードを受信します。ローカル トリガの構成または OCS から受信したトリガに基づいて、URR に対して操作が実行されることはありません。

## Gy Quota Validity Time（QVT）と Quota Holding Time（QHT）

### 機能説明

この機能の一部として、次の機能が SMF に追加されます。

- SMF は、 **CCAI** および **CCAU** メッセージの Gy インターフェイスから **クォータ有効期間** を受信できます。処理後、SMF は、「**timq** 」をトリガとしてこの情報をメッセージ

**PFCP_SESSION_ESTABLISHMENT_REQUEST** および **PFCP_SESSION_MODIFICATION_REQUEST**で UPF に送信します。

PFCP_SESSION_REPORT_REQUEST メッセージが「**timq**」トリガを使用した使用状況レポートを受信した場合、SMF は時間クォータ情報を含む USU を含む **CCRU** メッセージを送信し、TGPPReportingReason を「**VALIDITY_TIME**」として追加します。

- SMF は、 **CCAI** および **CCAU** メッセージの Gy インターフェイスから **クォータ保持時間** を受信できます。処理後、SMF はこの情報を「**quehti** 」としてトリガするメッセージ **PFCP_SESSION_ESTABLISHMENT_REQUEST** および **PFCP_SESSION_MODIFICATION_REQUEST**で UPF に送信します。

  **PFCP_SESSION_ESTABLISHMENT_REQUEST PFCP_SESSION_MODIFICATION_REQUEST**

  **PFCP_SESSION_REPORT_REQUEST** メッセージが「**quihti**」トリガで使用状況レポートを受信した場合。SMF は、USU に時間クォータ情報を含む **CCRU** メッセージを送信し、TGPPReportingReason を「**QHT**」として追加します。

### Quota-Validity-Time

これはオプションの AVP であり、CCA コマンドでのみ発生する可能性があります。これは、Multiple Services-Credit-Control AVP に含まれています。このフィールドは、特定のカテゴリ インスタンスに対して付与されたクォータの有効性を制限する時間を定義します。

SMF では、次の要件がサポートされています：

- Gy CCAI/CCAU メッセージの確立または変更で受信した「**有効期間**」を受信しました
- SMF プロセスが有効時間を受け取りました（UPF に情報を送信できる場合）。

  SMF は、PFCP_IE_TIME_QUOTA に有効時間を「**tm_quata**」として送信し、PFCP_IE_REPORTING_TRIGGERS の: `PFCP_SESSION_ESTABLISHMENT_REQUEST` および `PFCP_SESSION_MODIFICATION_REQUEST` にトリガーを **tmq**として設定します。

- SMF は、PFCP_SESSION_REPORT_REQUEST メッセージの「**durton_msrt** 」のトリガーおよび期間として **timq** を使用して、PFCP_IE_USAGE_REPORT_REP_REQ を受信できます。
- SMF プロセス使用状況レポートは、Used-Service-Unit および CCRU の Multiple-Services-Credit-Control AVP で VALIDITY_TIME として追加された **3GPP-Reporting-Reason** 内で、受け取った「**durton_msrt**」を「**CC-Time**」として送信します。
- SMF が「**durton_msrt**」とともに「**volume_msrmt**」を受信した場合、Used-Service-Unit 内の「**CC-Time**」とともに「**CC-Total-Octets**」、「CC-Input-**Octets**」、「**CC-Output-Octets**」が入力され、および **3GPP-Reporting-Reason** が CCRU の Multiple-Services-Credit-Control AVP に VALIDITY_TIME として追加されました。
- cnPGW が Gy CCAI/CCAU メッセージで「**有効期間**」を受信しない場合、課金プロファイル構成から読み取り、適用します。

#### Quota-Holding-Time

これはオプションの AVP であり、CCA コマンドでのみ発生する可能性があります。これは、Multiple Services-Credit-Control AVP に含まれています。これは、付与された時間クォータと付与されたボリューム クォータに等しく適用されます。

SMF では、次の要件がサポートされています：

- Gy CCAI/CCAU メッセージの確立または変更で「**3GPP-Quota-Holding-Time**」を受信しました
- SMF は PFCP_IE_QUOTA_HOLDING_TIME 内で「**quma_hldg_tm**」として保持時間を送信し、PFCP_IE_REPORTING_TRIGGERS の PFCP_SESSION_ESTABLISHMENT_REQUEST および PFCP_SESSION_MODIFICATION_REQUEST の PFCP_IE_REPORTING_TRIGGERS でトリガーを **qhti** として構成します。
- SMF は、 **qhti** をトリガーとして使用して PFCP_IE_USAGE_REPORT_REP_REQ を受信できます。
- CCRU の Multiple-Services-Credit-Control AVP で SMF プロセス使用状況レポート **3GPP-Reporting-Reason が** QHT として追加されました。

#### Volume-Quota-Threshold

これはオプションの AVP であり、CCA コマンドでのみ発生する可能性があります。これは、Multiple Services-Credit-Control AVP に含まれています。cnPGW が Gy CCAI/CCAU メッセージで「3GPP-Volume-Quota-Threshold」を受信していない場合、課金プロファイル構成から情報を読み取り、適用します。

## 機能の仕組み

SMF は、PFCP_IE_TIME_QUOTA IE の「tm_quata」で N4 に対してクォータの有効時間を送信します。SMF が CCAI/CCAU からクォータの有効時間のみを受信する場合、または cc-Time と validity-time の両方を受信する場合、有効時間は短くなります。両方の値が等しい場合、SMF は tm_quata で cc-Time 値を送信します。クォータの有効期間が選択されている場合、SMF は 3GPP-Time-Quota-Threshold を N4 に転送しません。

受信したクォータ保持時間が有効な場合、SMF はクォータ保持時間を N4 に送信します。

（注）

- **ゼロ有効期間**：

  SMF では、CCRI/CCRU から受信した有効時間または保持時間の値が 0 の場合、有効時間または保持時間の値が N4 に転送されます。0 が UPF でアームド タイマーを無効化するメカニズムであるため、SMF は 0 をリレーします。CCRI/CCRU から受信した有効時間または保持時間の値が 0 の場合、QVT および QHT の実装は SMF と連携します。

- **QHTトリガーを受信しました。**

  SMF では、volume_msrmt、duration_msrmt が quehti トリガーとともに受信され、CCRU は USU 内で volume_msrmt、duration_msrmt を送信し、レポートの理由を MSCC レベルの QHT として更新して、「Requested-Service-Unit」も送信します。volume_msrmt、duration_msrmt が qhti トリガーと共に受信される場合、QHT の実装は SMF と連携します。

### ロギング

次のデバッグ ログは、Gy インターフェイスから有効時間が受信された場合、さまざまなシナリオで存在します。

- validity-Time のみを受信しました：

  **「有効期限があり、時間クォータではありません」**

- Validity-Time と cc-Time を受信しました：

  **「時間クォータが有効時間よりも小さい」**

  **「時間クォータが有効時間よりも大きくなっています」**

  **「時間クォータは有効時間と等しくなります」**

## Gy Tarif 時間のサポート

### 機能説明

タリフ切り替え時間機能は、サブスクライバがあるタリフ プランから別のタリフ プランに切り替わるときに適用されます。Tariff-Time-Change AVP はタリフ切り替え時間を決定するために使用され、Monitoring-Time IE はタリフ時間サポート機能をサポートするために使用されます。

タリフタイマーが終了すると、ゲートウェイは別途、使用量を課金バケットに累積し、引き続き元のクォータ値から消費します。次回のレポート時（クォータの枯渇またはその他の制御イベント発生時）に、ゲートウェイはこの課金バケットの 2 つの使用量（タリフ時間変更の前後）をレポートします。

### 機能の仕組み

SMF は、CCAI メッセージと CCAU メッセージの Gy インターフェイスからの付与されたサービス ユニット（GSU）レベルの Tariff-Time-Change AVP を処理します。SMF では、UPF から

使用状況レポートを受信すると、CCRU および CCRT メッセージの Used-Service-Unit（USU）内に Tariff-Change-Usage AVP が含まれます。

以下のシナリオがサポートされています：

- Tariff-Time-Change with Quota-Holding-Time Expired Trigger
- Tariff-Time-Change with Validity-Time Expired Trigger
- Tariff-Time-Change with Volume/Time-Quota Exhausted Trigger
- Tariff-Time-Change with Volume/Time-Quota Exhausted Trigger
- Tariff-Time-Change with Immediate Reporting Trigger
- Tariff-Time-Change with Terminate Reporting Trigger

この SMF の機能の一部として、次の機能が追加されました：

- OCS は、CCAI/CCAU メッセージで「Tariff-Time-Change」AVP を提供します。処理後、SMF は、PFCP_IE_MONITORING_TIME IE を使用して、PFCP セッション確立要求および PFCP セッション変更要求で UPF にこの情報を送信します。
- SMF は、URR ごとに次の 2 つの使用状況レポートを受信します：
  - 1 つは、「Usage Report Trigger」は「MONIT」として、「PFCP_IE_USAGE_INFORMATION」は、「PFCP_IE_VOLUME_MEASUREMENT」と「PFCP_IE_DURATION_MEASUREMENT」と一緒の「bef」としてです。
  - 他の使用レポートは、「Usage Report Trigger」は「TIMQU」として、「PFCP_IE_USAGE_INFORMATION」は、「PFCP_IE_VOLUME_MEASUREMENT」と「PFCP_IE_DURATION_MEASUREMENT」と一緒の「aft」としてです。
- SMF は異なる USU を使用して、MSCC 内の両方の使用状況レポートを CCRU/CCRT メッセージの OCS に転送します。

  .
  - 最初の使用状況レポート。これは「MONIT」トリガーがあるものは、「Tariff-Change-Usage: UNIT_BEFORE_TARIF_CHANGE」で USU1 に転送されます。
  - そして 2 番目の使用状況レポート。これは「TIMQU」トリガーで、「Tariff-Change-Usage: UNIT_AFTER_TARIFF_CHANGE」と共に USU2 に転送されます。

## Gy の発信元ホストと発信元レルム

各サブスクライバについて、SMF は、Diameter メッセージを介して OCS から送信された Origin-Realm および Origin-Host 属性情報のレコードを保持します。Origin-Host 属性および Origin-Realm 属性の値が変更された場合、SMF は最新の値を更新し、対応する宛先ホストと対話します。その後、SMF は属性値の変更ごとに ocs_dest_host_change_stats の統計情報を増加させます。

# Diameter インターフェイスを介した保留中のトラフィック処理

SMF は、プリペイド サブスクライバ用の Evolved Packet System（EPS）と Diameter インターフェイス（オンライン課金システム（OCS）用の Gy など）のインターワーキングに関する 3GPP の推奨事項を実装しており、クォータ更新手順中に保留中のトラフィック管理をサポートします。

保留中のトラフィック処理（PTT）により、P-GW からのクォータ情報を待機している間に、ユーザープレーン機能（UPF）で流れるトラフィックのパスまたはドロップの処理が可能になります。トラフィックは、UPF のアクティブな課金サービスのクレジット制御グループでサポートされている次の構成に基づいて処理されます：

- pending-traffic-treatment noquota pass
- pending-traffic-treatment noquota drop
- pending-traffic-treatment noquota limited-pass volume < in bytes, ranging from 1 to 4294967295>
- pending-traffic-treatment quota-exhausted pass
- pending-traffic-treatment quota-exhausted drop

（注） Diameterインターフェイス上で保留中のトラフィック処理を有効にするために、SMF での構成は不要です。

詳細については、『*UCC 5G UPF* 構成および管理ガイド』の「*UPF* の構成例」の章および『コマンド ライン インターフェイス リファレンス、モード *C - D* 』の「クレジット コントロール構成モードのコマンド」の章を参照してください。

# ルーティング データのサポート

## 機能説明

ルーティング データ サポート機能により、SMF は次のことが可能になります。

- OCS から CCA-I/CCA-U で受信したルーティングデータの処理
- Diameter セッションごとに ChargingSubData にルーティングデータ情報を上書きして保存します。Smf-service には、次の後続の CCR-U または CCR-T メッセージに格納されたルーティング データ値が含まれます。SMF は常に OCS からの CCA-I/CCA-U のルーティングデータを想定しています。

### モニタリングおよびトラブルシューティング

このセクションには、機能操作時に発生する可能性がある問題のトラブルシューティングに関する情報が記載されています。

次に、サブスクライバの Gy Diameter セッションごとのルーティングデータの出力例を示します。

```
"gyDiamSession": {
                                "brrId": 1,
                                "sessionID": ":2:69:ocs-prof:64c37b62:1",
                                "originHost": "dummyOriginHost",
                                "originRealm": "dummyOriginRealm.com",
                                "destRealm": "dummyGyDestRealm.com",
                                "destHost": "Gy-server",
                                "RoutingData": {
                                    "primaryHost": "10.105.34.14",
                                    "primaryRealm": "dummyGyDestRealm.com",
                                    "boundPeer": "Gy-server"
                                }
                            },
```

# Gz インターフェイス

**表 *230 :* 機能の履歴**

| 機能名 | リリース情報 | 説明 |
|---|---|---|
| オフライン ベアラー再計算の非同期および同期使用状況レポート | 2023.04 | Gz 使用状況レポートの一部として、SMF はオフライン ベアラー再計算のための非同期および同期使用状況レポートを受信します。 |
| ベアラー要求トリガの変更の処理 | 2023.04 | SMF は、ユーザーの場所とタイムゾーンの変更、変更通知について、S-GW からベアラー要求の変更を受信します。SMF は、N4 クエリ インターフェイスとルールベースの変更、セカンダリ RAT 使用制限、およびレコード終了トリガについてのインターフェイス IE の再計算をサポートします。<br>**デフォルト設定** 無効：有効にするには構成が必要です。 |

| 機能名 | リリース情報 | 説明 |
|---|---|---|
| Gzデフォルト ベアラーの変更 | 2023.04 | この機能により、Gx CCR-UおよびGx RAR を介してデフォルトのベアラーのPCRFによって開始された変更が可能になります。次の機能を実行できます。<br>• デフォルトのベアラーにルールを追加する<br>• デフォルトのベアラーからルールを削除する<br>• ルールベースの変更<br>• デフォルト ベアラー QoS の変更<br>• APN-AMBR の変更 |

# Gz インターフェイスを使用した PDN 接続および接続解除

## 機能説明

レガシー インターフェイスを使用した SMF は、オフライン アカウンティング機能を有効にするために、デフォルトのベアラーの Gz インターフェイスを使用したパケット データ ネットワーク（PDN）接続をサポートします。

### 動作

Gx CCA-I を介して PCRF からオフライン ルールを受信すると、Diameter インターフェイスを備えた SMF はオフライン URR を作成し、対応する課金バケット（SDF）にマッピングし、レガシー インターフェイスを使用して SMF に N4EstablishmentRequest を送信します。

オフライン SDF/ベアラーレベルの URR の使用状況レポートを受信すると、UPF からの N4 セッション削除応答で、GTPP データレコード転送要求を GTPP に送信します。Gz 通信量レポートの詳細については、「回線の課金」 > 「*GTPP* での *Gz* 通信量レポートの取り扱い」の セクションを参照してください。

Gz インターフェイス機能を備えた PDN のアタッチとデタッチを使用して、次のことを行います。

- アタッチ手順:
  - オフライン ルールのみ（Gx + Gz）
  - オフライン ルールとオンライン ルール（Gx + Gy + Gz）

- 次による切断手順:
  - オフライン ルールのみ（Gx + Gz）
  - オフライン ルールとオンライン ルール（Gx + Gy + Gz）

## 情報要素および AVP サポート

PDN 接続および切断機能は、次の情報要素（IE）をサポートします。

- **オフライン ルールのレポート レベル IE**：ダイナミック ルールの ReportingLevel は、Gx CCA-I の PCRF から受信されます。その他の条件は次のとおりです：
  - ダイナミック オフライ ンルールで ReportingLevel が存在しない場合、SMF は、受信した RG とサービス ID に基づいてレポート レベルを考慮します：
    - RG のみを受信した場合は、レポート レベルは RatingGroupLevel になります。
    - RG と ServiceID の両方を受信した場合のレポート レベルは ServiceIdentifierLevel です。
  - 動的オフライン ルールに ReportingLevel が存在する場合、同じものと見なされます。

（注） デフォルトの offlineReportingLevel 構成は Gz には適用できません。

### 動的ルールのオフライン AVP の処理

次の表は、ダイナミック ルールのオフライン AVP の機能について説明します。

**表 *231 :* ルール レベルおよびコマンド レベルの *AVP***

| AVP | 説明 |
|---|---|
| Gx CCR-I のオフライン AVP | Gx CCR-I に存在するオフライン AVP は、オフライン充電方式のデフォルト構成を示します。Gz が有効になっている場合、オフライン AVP は Gx CCR-I で有効に設定されます。そうでない場合は、無効に設定されます。 |

| AVP | 説明 |
|---|---|
| Gx CCA -I/ CCA-U/ RAR のオフライン AVP | RULE レベルのオフライン AVP が課金ルール定義内に存在する場合、対応する動的ルールのオフライン課金方式を定義します。有効にすると、対応する動的ルールに対してオフライン課金が行われます。無効化されている場合、対応するダイナミック ルールに対してオフライン課金は行われません。 |
| | RULE レベルのオフライン AVP が課金ルールの定義内に存在しない場合、COMMAND レベルのオフライン AVP は、動的ルールのオフライン課金方式が有効か無効かを判断するために考慮されます。 |
| | オフライン AVP が RULE および COMMAND レベルで存在しない場合、デフォルトのオフライン課金方式が動的ルールに適用されます。Gz が有効になっている場合、動的ルールのデフォルトのオフライン課金方式が有効になります。そうでない場合、デフォルトのオフライン課金方式は無効になります。 |

### Gz が無効になっている場合のオフライン ダイナミック ルールの処理

ルールベースで Gz が無効になっている場合、オフラインのダイナミック ルールに対して SDF およびベアラー レベルの URR は作成されません。次の表に、入力値の可能な組み合わせを示します。

**表 *232 :* 入力値の組み合わせ**

| ルールベース プロファイルで GZ が有効になりました | ダイナミック ルール オフラインが有効になっています | オフライン URR N4 で作成 |
|---|---|---|
| TRUE | TRUE | TRUE |
| TRUE | FALSE | FALSE |
| FALSE | TRUE | FALSE |
| FALSE | FALSE | FALSE |

## GTPP レコードの異常終了

コントロール プレーンまたはユーザー プレーンのいずれかからパス障害が発生した場合、次のいずれかの理由により、異常なリリースを含む GTPP レコード終了メッセージが送信されます。

- UPF セッション レポート ERIR
- UPF セッション レポート SRIR
- GTPU ピア パス障害
- UPF リカバリ リリース
- UPF パス ピアの障害

- GTPC ピア パスのリリース失敗
- GTPC ピア再起動リリース

## オフライン ルールのみによる PDN 接続

次のコール フローと手順では、オフラインを含むダイナミック ルールが Gx および Gz インターフェイスを介して有効になっている場合の PDN アタッチについて説明します。

**図 *137 :* オフライン ルールのみによる *PDN* 接続のコール フロー**

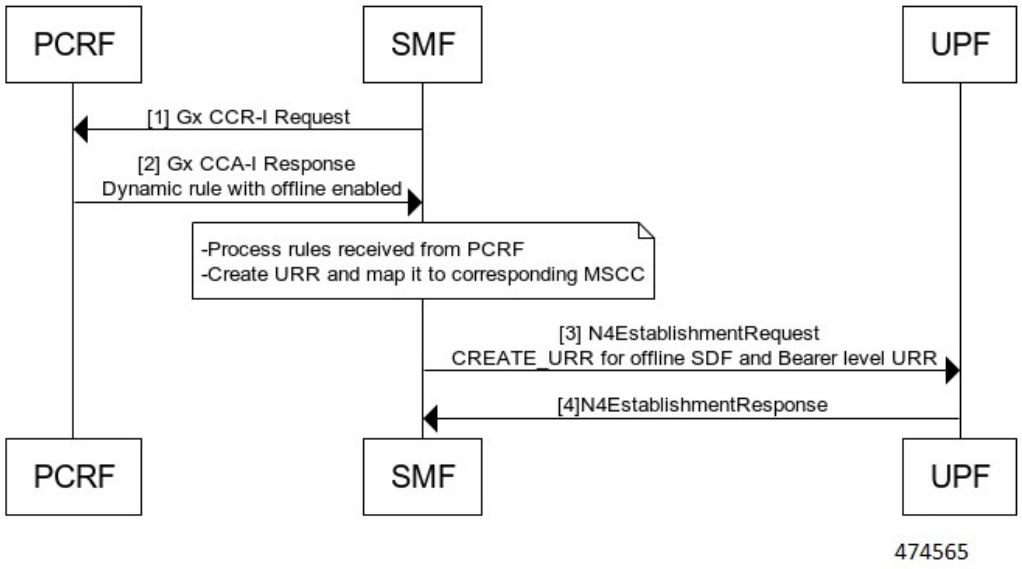



**表 *233 : PDN* 接続のコール フロー説明**

| 手順 | 説明 |
|---|---|
| 1 | SMF は PCRF に Gx CCR-I を送信します。 |
| 2 | PCRF は、OFFLINE_ENABLED が True に設定されたダイナミックルールを持つデフォルトのベアラーを使用して、SMF に Gx CCA-I を送信します。 |

| 手順 | 説明 |
|---|---|
| 3 | N4 確立要求は、次の条件に基づいて UPF に送信されます。<br>• 次の場合、デフォルトのベアラー レベル URR に対して CREATE_URR を設定します：<br>• デフォルトのベアラ レベル URR の PFCP_IE_URR_ID が 0x80000002 に設定されています。<br>• PFCP_IE_VOLUME_THRESHOLD および PFCP_IE_TIME_THRESHOLD には、ルールベース プロファイルで構成された egcdr しきい値があります。<br>• PFCP_IE_MEASUREMENT_METHOD には、ボリュームと期間の両方のビットが設定されています。<br>• 次の場合は、オフライン SDF レベルの URR に対して CREATE_URR を使用します。<br>• PFCP_IE_URR_ID に一意のオンライン UrrId がある<br>• PFCP_IE_VOLUME_THRESHOLD および PFCP_IE_TIME_THRESHOLD には、GTPP プロファイルで構成された egcdr しきい値があります。<br>• PFCP_IE_MEASUREMENT_METHOD には、ボリュームと期間の両方のビットが設定されています。<br>• すべての SDF レベルのオフライン URR は、ベアラー レベルの URR にリンクされます。つまり、PFCP_IE_LINKED_URR_ID は、リンクされた URRId が BearerLevel URR に設定されています。<br>• ダイナミック ルール（オンライン + オフライン）のために作成された PDR は、オンライン、オフライン SDF およびベアラー レベル URR にマッピングされます。 |
| 4 | UPF は N4Establishment 応答を送信します。 |

## オフライン ルールとオンライン ルールを使用した PDN アタッチ

次のコール フローと手順では、オンラインとオフラインの両方を含むダイナミック ルールが Gx、Gy、および Gz インターフェイスを介して有効になっている場合の PDN アタッチについて説明します。

図 *138 :* コール フロー

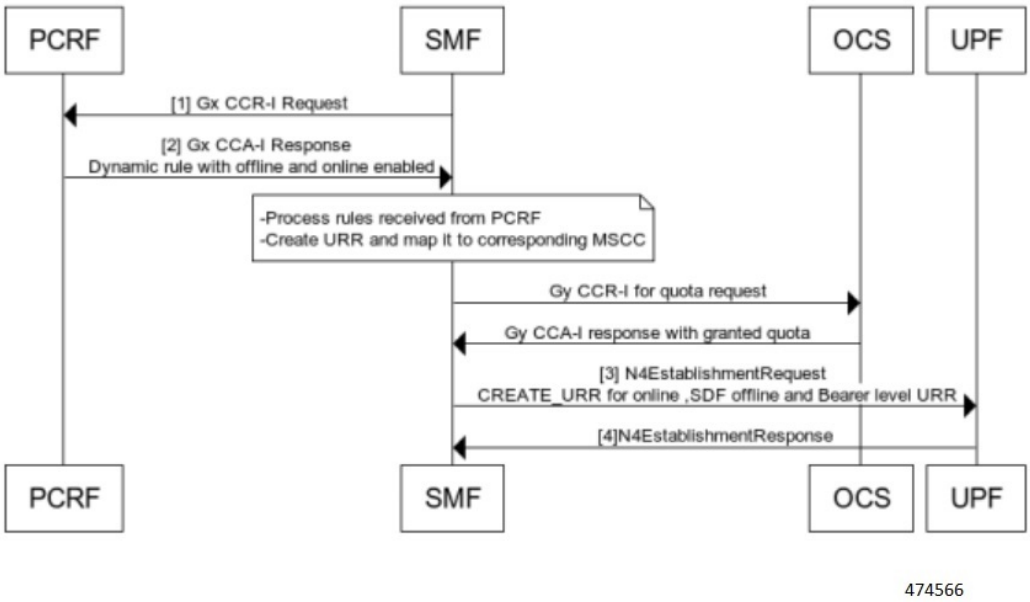



表 *234 :* オフライン ルールとオンライン ルールを使用した *PDN* 接続のコール フローの説明

| 手順 | 説明 |
|---|---|
| 1 | SMF は PCRF に Gx CCR-I を送信します。 |
| 2 | PCRF は、OFFLINE_ENABLED が True に設定されたダイナミックルールを持つデフォルトのベアラーを使用して、SMF に Gx CCA-I を送信します。 |

| 手順 | 説明 |
|---|---|
| 3 | N4 確立要求は、次の条件に基づいて UPF に送信されます。<br>• 次の場合、デフォルトのベアラー レベル URR に対して CREATE_URR を設定します：<br>• デフォルトのベアラ レベル URR の PFCP_IE_URR_ID が 0x80000002 に設定されています。<br>• 次の場合は、オフライン SDF レベルの URR に対して CREATE_URR を使用します。<br>• PFCP_IE_VOLUME_THRESHOLD および PFCP_IE_TIME_THRESHOLD には、GTPP プロファイルで構成された egcdr しきい値があります。<br>• オンライン URR の CREATE_URR。<br>• PFCP_IE_URR_ID に一意のオンライン UrrId がある<br>• PFCP_IE_VOLUME_THRESHOLD および PFCP_IE_TIME_THRESHOLD には OCS から受信したしきい値があります。<br>• PFCP_IE_MEASUREMENT_METHOD は、OCS から受信したクォータに基づいて設定されます。<br>• ダイナミック ルール（オンライン + オフライン）のために作成された PDR は、オンライン、オフライン SDF およびベアラレベル URR にマッピングされます。 |
| 4 | UPF は N4Establishment 応答を送信します。 |

## オフライン ルールとオンライン ルールによる PDN の接続解除

以下のコールフローと手順は、セッション削除応答における使用状況レポートを説明しています。

図 *139 : N4* セッション削除応答の一部としての使用状況レポートのコール フロー

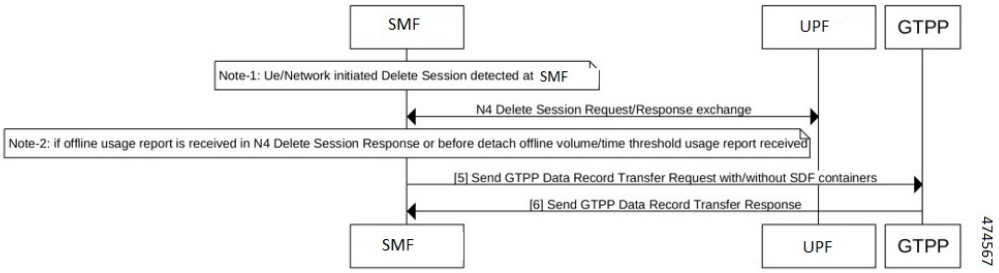


表 *235 : N4* セッション削除の応答のコール フローの説明

| 手順 | 説明 |
|---|---|
| UE/ネットワークによって開始された削除セッションが SMF で検出されました。 | |
| 1 | N4 セッション削除要求または応答が交換されてセッションが削除され、N4 削除セッション応答で使用状況レポートが受信されます。 |
| 3 | SMF は、SDF コンテナを使用してもしくは使用しないで GTPP データ転送要求を送信します。<br>• N4 セッション削除応答でオフラインの使用状況レポートを受信した場合、SMF は、最大課金条件がヒットした場合にのみ、SDF コンテナ（ボリューム使用率と serviceConditionChange を各 RG + サービス ID に 1 つずつ加えて）を使用してデフォルトで GTPP データ レコード転送要求を送信します。<br>• オフラインの使用状況レポートが N4 セッション削除の応答の測定なしで受信され、デタッチする前にオフラインのボリューム/時間しきい値の使用レポートが受信されない場合、GTPP サーバによる GTPP データ レコード転送メッセージ。<br>• デタッチ前にオフラインのボリューム/時間しきい値の使用レポートを受信し、受信した N4 削除セッション応答にオフラインの使用状況レポートがない場合、GTPP データ レコード転送はレコード クローズのために SDF コンテナなしで交換されます。 |
| 4 | SMF は、GTPP サーバから GTPP データ レコード転送応答を受信します。 |

## GZ インターフェイスの有効化

Gz インターフェイスを有効にするために構成コマンドを使用します。オフライン AVP がルールおよびコマンド レベルで存在しない場合、デフォルトのオフライン課金方式が動的ルールに適用されます。Gz インターフェイスが有効になっている場合、動的ルールのデフォルトのオフライン課金方式が有効になります。それ以外の場合、デフォルトのオフライン課金は無効になります。

```
config
   active-charging service service_name
      rulebase rulebase_name
         billing-records egcdr value
   profile gtpp-profile   profile_name  gtpp dictionary dictionary_num
   profile network-element ofcs  ofcs_name  gtpp-profile profile_name
   profile dnn intershat network-element-profiles ofcs ofcs_name |
end
```

注：

- **rulebase** *rulebase_name*：ACS ルールベースの名前を指定します。 *rulebase_name* は 、1 ～ 63 文字の英数字の文字列である必要があります。

（注） ルールベースは、フローと一致するプロトコル ルール、および一致したフローに対して実行される関連アクションのコレクションです。

- **billing-records egcdr** *value* ：eG-CDR 請求を有効にする場合に True に指定します。これにより、対応するルールベース プロファイルの Gz インターフェイスに CnPGW-C が関連付けられます。さらに、PCRF が Gx CCA-I で別のルールベースを送信すると、Gz インターフェイスは、新しいルールベースで受信した billingRecord EGCDR 構成に従って有効または無効になります。
- **profile gtpp-profile** *profile_name* **gtpp dictionary** *dictionary_num* ：ディクショナリを使用して gtpp プロファイルを構成します。正しいディクショナリは gtpp dictionary *custom24*です。*profile_name* は 、セッションのラウンド ロビン方式で使用される関連 GTPP プロファイル名のリストを指定します。最大 gtpp プロファイル数は 4 です。
- **profile network-element ofcs** *ofcs_nameprofile_name* **gtpp-profile** ： ネットワーク プロファイル ofcs を構成します。OFCS プロファイル構成では、複数の gtpp プロファイルを構成することができます。

（注） **network profile ofcs** を構成する前に **gtpp-profile.**を構成してください

## ベアラー レベルの URR しきい値の設定

構成コマンドを使用して、ベアラー レベルのしきい値を設定します。

```
config
   active-charging service service_name
      rulebase rulebase_name
         egcdr threshold volume { downlink | total | uplink }  bytes
end
```

注：

- **rulebase** *rulebase_name*：ACS ルールベースの名前を指定します。 *rulebase_name* は 、1 ～ 63 文字の英数字の文字列である必要があります。
- **egcdr threshold volume { downlink | total | uplink }** *bytes* ：ベアラー レベルの URR しきい値を指定します。ダウンリンク、合計、またはアップリンクのオクテットの数の制限は、100000 ～ 4000000000 の範囲の整数である必要があります。例： `egcdr threshold volume downlink 100000 uplink 100000 total 200000`

## SDF レベルのオフライン URR しきい値の構成

サービス データ フロー（SDF）レベルのしきい値を設定するには、 構成コマンドを使用します。

```
config
   active-charging service service_name
     charging-action charging_action
       egcdr service-data-flow threshold volume { downlink | total |
uplink } bytes
        egcdr service-data-flow threshold interval interval  60
   end
```

注：

- **charging-action** *charge_action_name*: 課金アクションの名前を指定します。 *charge_action_name* は 、1 ～ 63 文字の英数字の文字列である必要があります。また、句読点を含めることができます。各家禽アクションには一意の名前が必要です。
- **egcdr service-data-flow threshold volume { downlink | total | uplink }** *bytes* ：SDF レベルのオフライン URR しきい値を指定します。ダウンリンク、合計、またはアップリンクのオクテットの数の制限は、100000 ～ 4000000000 の範囲の整数である必要があります。
- **egcdr service-data-flow threshold interval** *interval* ：オフライン充電のしきい値を構成します。60 ～ 40000000 の範囲の整数である必要があります。

## max-losdv 値の構成

コンフィギュレーション コマンドを使用して、構成した maxlosdv 値に相当する数のサービス データ フロー（SDF）コンテナの数で GTPP データ レコードを作成します。maxlosdv が構成されていない場合、デフォルト値は 1 です。

```
config
   active-charging service service_name
     charging-action charging_action
       egcdr losdv-max-containers container_num
   end
```

注：

- **charging-action** *charge_action_name*: 課金アクションの名前を指定します。 *charge_action_name* は 、1 ～ 63 文字の英数字の文字列である必要があります。また、句読点を含めることができます。各家禽アクションには一意の名前が必要です。
- **egcdr losdv-max-containers** *container_num* ：GTPP データ レコードを作成するサービス データ コンテナ（LOSDV）の最大リストを指定します。

## close-reason の構成

次のコマンドを使用して、GTPP データ レコードで送信する終了理由を構成します。終了理由は、管理介入または通常のリリースです。デフォルトの終了理由は mgmt-intervention です。

```
config
   active-charging service service_name
     charging-action charging_action
       egcdr closure-reason { admin-disconnect | normal-release |  }

   end
```

注：

- **charging-action** *charge_action_name*: 課金アクションの名前を指定します。 *charge_action_name* は 、1 ～ 63 文字の英数字の文字列である必要があります。また、句読点を含めることができます。各家禽アクションには一意の名前が必要です。
- **egcdr closure-reason { admin-disconnect | normal-release | }** ：終了理由を構成します。

# Gz 使用状況レポート

## 機能説明

統合ユーザープレーン機能の実行時に、P-GW（ユーザープレーン）は、オフライン課金のボリュームまたは時間しきい値などのトリガに関する使用状況レポートを送信します。統合型コントロール プレーン機能中に、P-GW（コントロール プレーン）は、SMF でのポリシー制御および課金（PCC）ルールの削除の一環として課金状態イベントが検出された場合、または URR が削除された場合に、使用状況レポートをクエリします。

使用状況レポートを受信すると、コントロール プレーンは URR を対応するオフライン課金パラメータにマッピングします。オフラインの課金パラメータが使用できない場合は、静的ルールまたは事前定義されたルールに対してサービス データ フロー（SDF）またはベアラー レベルの課金パラメータが作成され、それぞれの SDF に対して GTPP データ レコード転送要求が開始されます。つまり、N4 変更応答または N4 削除応答メッセージを介して同期使用状況レポートを受信します。N4 セッション レポート要求メッセージを介して非同期使用状況レポートを受信します。

詳細については、『UCC 5G cnSGWc 構成および管理ガイド』>「インターフェイス サポート」の章を参照してください。

## 機能の仕組み

Gz インターフェイスの使用状況レポートには、次の使用状況レポート手順が含まれます。

- オフライン ベアラーまたはオフライン ベアラーと SDF レベル、またはダイナミック ルールの SDF レベルの URR
- オフライン ベアラーまたはオフライン ベアラーと SDF レベル、またはスタティック/事前定義済みルールの SDF レベルの URR
- オンラインまたはオフライン URR
- N4 削除セッション応答。

## *N4* セッション レポートの使用状況レポート

次のコールフローと手順では、ボリュームまたは時間のしきい値を含むN4セッション レポートの使用状況レポートについて説明します。

### ダイナミック ルールのオフライン ベアラーと SDF レベルまたは SDF レベルの URR

次のコール フローと手順では、オフライン ベアラーまたはSDF レベルのボリューム/時間しきい値、またはダイナミック ルールの SDF レベル URR を含む N4 セッション レポートの使用状況レポートについて説明します。

（注） URR がしきい値などの値とともに UPF に存在することを確認します。ボリュームまたは時間しきい値が、ベアラー/SDF または SDF レベルの URR の UPF でヒットします。UPF は、使用状況レポートのトリガ情報とともに、使用状況をSMF にリレーします。

**図 *140* : オフライン *N4* セッション レポートの使用状況レポートのコール フロー**

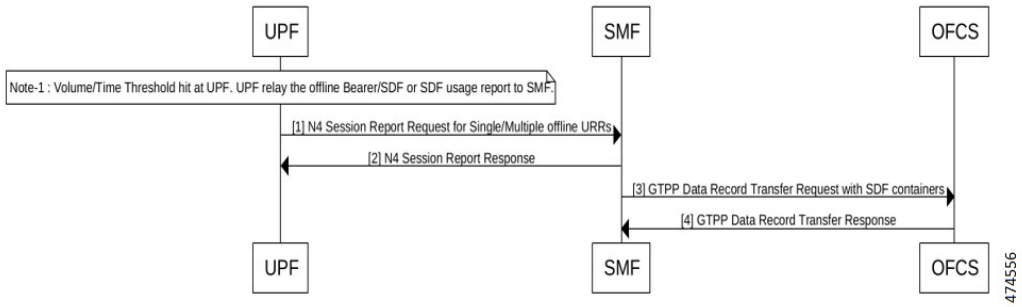



**表 *236* : *N4* セッション レポートのオフライン使用状況レポートのコール フローの説明**

| 手順 | 説明 |
|---|---|
| 1 | UPF は、オフライン ベアラーの使用率と SDF の使用率または SDF の使用率のみに対する N4 セッション レポート要求を SMF に送信します。 |
| 2 | SMF が N4 セッション レポート応答を送信します。 |

| 手順 | 説明 |
|---|---|
| 3 | SMF は、SDF コンテナを使用して GTPP データ レコード転送要求をオフライン課金システム（OFCS）に送信します。この要求は、ボリューム使用率と serviceConditionChange を含む 1 つまたは複数の SDF（RG + サービス ID ごとに 1 つ）とともに送信されます。<br>（注）<br>このアルゴリズムは、次のいずれかの条件に基づいて動作します：<br>• オフライン ベアラー使用率レポートを受信した SDF または SDF 使用状況レポートとともに受信し、最大課金条件がヒットした場合（**max-losdv** CLI 構成値。デフォルト値は 1）。<br>• 受信したオフライン使用状況レポートが N4 セッション レポート要求のベアラー レベルの時間しきい値の測定値なしの場合、recordClosureReason「TimeLimit」を持つ GTPP データ レコード転送メッセージが、SDF コンテナを含まず、OFCS と交換されます。<br>• 受信したオフライン使用状況レポートに N4 セッション レポート要求の SDF レベルの時間しきい値の測定がない場合、GTPP データ レコード転送メッセージは OFCS と交換されません。 |
| 4 | OFCS は、GTPP データ レコード転送応答を送信します。 |

### 構成サンプル

次に、ダイナミック ルール SDF レベル URR のメッセージ出力例を示します。

```
URR ID:
                Type: 81   Length: 4
                Value: 0x000000021.
            USAGE REPORT TRIGGER:
                Type: 63   Length: 2
                Time Threshold
            VOLUME MEASUREMENT:
                Type: 66   Length: 25
                Total Volume: 450
                Uplink Volume: 250
                Downlink Volume: 200
            DURATION MEASUREMENT:
                Type: 67   Length: 4
                Value: 100

        accessPointNameNi                   cisco.com
        ratingGroup                         10
        chargingRuleBaseName                cisco
        resultCode                          2001
        localSequenceNumber                 1
        timeOfFirstUsage                    220829173906-0400
        timeOfLastUsage                     220829173907-0400
        timeUsage                           1
        serviceConditionChange              Time Exhaust
         qCI                                 5
         maxRequestedBandwithUL              0
```

```
 maxRequestedBandwithDL                0
 guaranteedBitrateUL                   0
 guaranteedBitrateDL                   0
 aRP                                   5
servingNodeAddress                     2002::2:61
datavolumeFBCUplink                    250
datavolumeFBCDownlink                  200
timeOfReport                           220829173907-0400
userLocationInformation
 Location Type                      TAI
  MCC                                  214
  MNC                                  365
  TAC                                  0x6789
  Location Type                     ECGI
  MCC                                  214
  MNC                                  365
  ECI                                  0x1234567
```

オフラインの静的ルールまたは事前定義済みルール

次のコール フローと手順では、オフライン ベアラーまたはSDF レベルのボリューム/時間しきい値、または事前定義ルールとスタティック ルールの SDF レベル URR を含む N4 セッション レポートの使用状況レポートについて説明します。

**図 *141*：オンライン スタティックまたは事前定義ルールの *N4* セッション レポートの使用状況レポートのコール フロー**

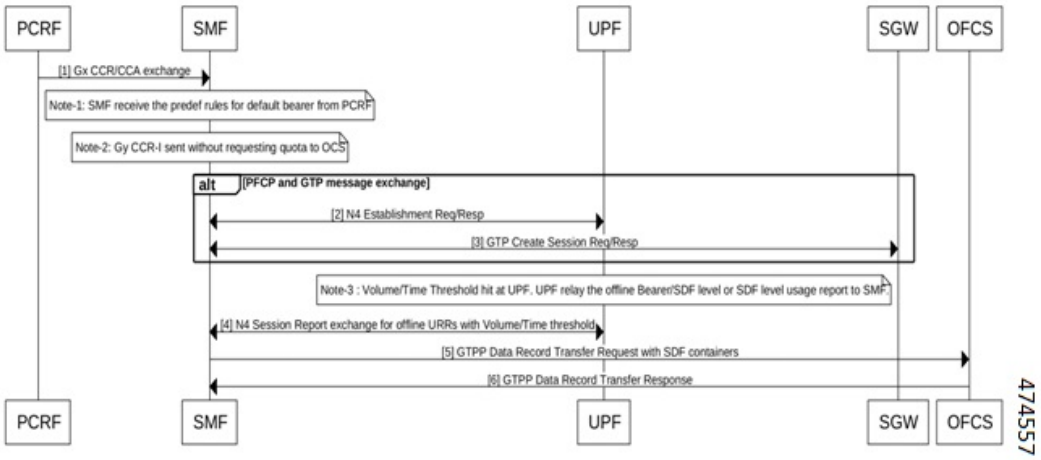



**表 *237*：オフラインのスタティック ルールまたは事前定義済みルールのコール フローの説明**

| 手順 | 説明 |
|---|---|
| 1 | PCRF は SMF と Gx-CCR または CCA 交換を実行します。この交換では、SMF は PCRF からデフォルトのベアラーのダイナミック ルールを受信します。 |
| 2 | SMF は、UPF との N4 セッション確立要求交換を開始します。同じ要求内で UPF は、応答として PFCP メッセージ交換をリレーします。 |
| 3 | SMF はセッション作成要求を S-GW に送信し、GTPP 応答メッセージが交換されます。 |

| 手順 | 説明 |
|---|---|
| （注）<br>UPF および UPF で検出されたボリューム/時間しきい値は、オフラインのベアラー/SDF レベルまたは SDF レベルの URR の VOLTH/TIMTH を使用した使用状況レポートを作成します。 | |
| 4 | SMF は、オフラインのボリューム/時間しきい値とともに N4 セッション レポート要求/応答交換を送信します。<br>SMF がスタティック/事前定義済みルールの LOTH/TIMTH を含む SDF レベルまたはベアラー/SDF レベルの使用レポートを受信すると、SMF でベアラー/SDF レベルの URR が作成され（存在しない場合）、SDF レベルの URR はベアラー レベルの URR にリンクされます。 |
| 5 | SMF は、SDF コンテナを使用して GTPP データ レコード転送要求をオフライン課金サーバ（OFCS）に送信します。この要求は、ボリューム使用率と serviceConditionChange を含む 1 つまたは複数の SDF（RG + サービス ID ごとに 1 つ）とともに送信されます。<br>（注）<br>このアルゴリズムは、次のいずれかの条件に基づいて動作します：<br>• オフライン ベアラー使用率レポートを受信した SDF または SDF 使用状況レポートとともに受信し、最大課金条件がヒットした場合（**max-losdv** CLI 構成値。デフォルト値は 1）。<br>• 受信したオフライン使用状況レポートが N4 セッション レポート要求のベアラー レベルの時間しきい値の測定値なしの場合、recordClosureReason「TimeLimit」を持つ GTPP データ レコード転送メッセージが、SDF コンテナを含まず、OFCS と交換されます。<br>• 受信したオフライン使用状況レポートに N4 セッション レポート要求の SDF レベルの時間しきい値の測定がない場合、GTPP データ レコード転送メッセージは OFCS と交換されません。 |
| 6 | OFCS は、GTPP データ レコード転送応答を SMF に送信します。 |

### 構成サンプル

次に、スタティック ルールの使用状況レポートのオフライン SDF レベルの URR ID のメッセージ出力の例を示します。

```
URR ID:
                Type: 81   Length: 4
                Value: 0x80000021.
            USAGE REPORT TRIGGER:
                Type: 63
                Vol Threshold
            VOLUME MEASUREMENT:
                Type: 66
                Total Volume: 400
                Uplink Volume: 200
```

```
        Downlink Volume: 200


accessPointNameNi                    cisco.com
ratingGroup                          101
chargingRuleBaseName                 prepaid
resultCode                           2001
localSequenceNumber                  1
timeOfFirstUsage                     220920093554-0400
timeOfLastUsage                      220920093558-0400
timeUsage                            4
serviceConditionChange               Volume Exhaust
 qCI                                  5
 maxRequestedBandwithUL               512000
 maxRequestedBandwithDL               512000
 guaranteedBitrateUL                  0
 guaranteedBitrateDL                  0
 aRP                                  84
servingNodeAddress                   192.60.7.31
datavolumeFBCUplink                  200
datavolumeFBCDownlink                200
timeOfReport                         220920093601-0400
userLocationInformation
 Location Type                   CGI
  MCC                                404
  MNC                                43
  LAC                                0x84C
  CI                                 0x4F0A
```

## オンライン URR とオフライン URR

次のコール フローと手順では、オンライン URR とオフライン URR の N4 セッション レポートの使用状況レポートについて説明します。

**図 *142 :* オンラインおよびオフラインの *N4* セッション レポートの使用状況レポートのコール フロー**

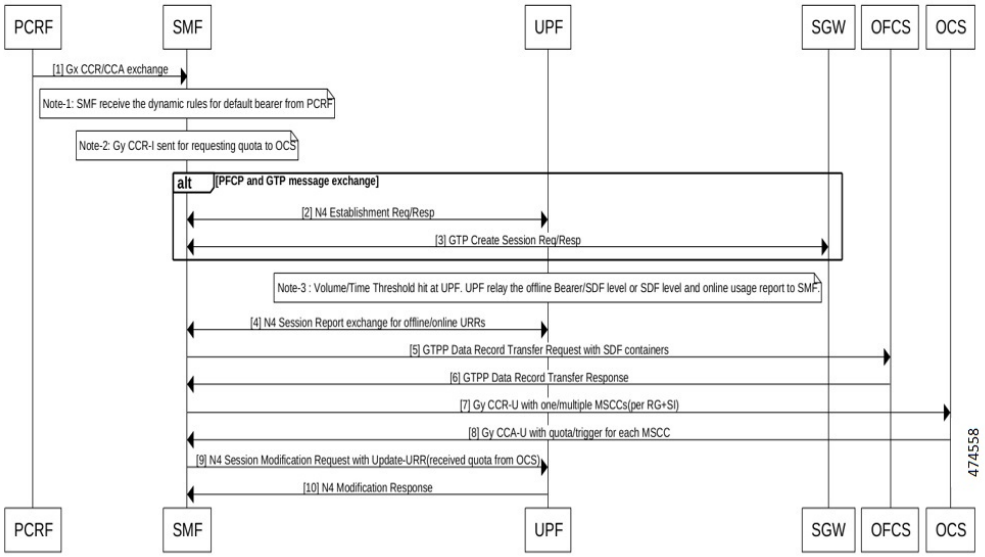


表 *238* : オンライン *URR* とオフライン *URR* 向けコール フローの説明

| 手順 | 説明 |
|---|---|
| 1 | PCRF は SMF と Gx-CCR または CCA 交換を実行します。この交換では、SMF は PCRF からデフォルトのベアラーのダイナミック ルールを受信します。 |
| 2 | SMF は、UPF と N4 セッション確立要求の交換を開始します。同じ要求内で UPF は、応答として PFCP メッセージ交換をリレーします。 |
| 3 | SMF はセッション作成要求を S-GW に送信し、GTPP 応答メッセージが交換されます。 |
| （注）<br>UPF および UPF で検出されたボリューム/時間しきい値は、オンライン URR およびオフラインのベアラー/SDF レベルまたは SDF レベルの URR の VOLTH/TIMTH を使用した使用状況レポートを作成します。 | |
| 4 | SMF は、オンラインおよびオフラインのボリューム/時間しきい値とともに N4 セッション レポート要求/応答交換を送信します。<br>SMF が SDF レベルまたはベアラー/SDF レベルの使用レポートを受信します。このレポートには、オンライン URR およびオフラインベアラー/SDF レベルの URR の VOLTH/TIMTH が含まれています。 |
| 5 | SMF は、SDF コンテナを使用して GTPP データ レコード転送要求をオフライン課金サーバ（OFCS）に送信します。この要求は、ボリューム使用率と serviceConditionChange を含む 1 つまたは複数の SDF（RG + サービス ID ごとに 1 つ）とともに送信されます。<br>（注）<br>このアルゴリズムは、次のいずれかの条件に基づいて動作します：<br>• オフライン ベアラー使用率レポートを受信した SDF または SDF 使用状況レポートとともに受信し、最大課金条件がヒットした場合（**max-losdv** CLI 構成値。デフォルト値は 1）。<br>• 受信したオフライン使用状況レポートが N4 セッション レポート要求のベアラーレベルの時間しきい値の測定値なしの場合、recordClosureReason「TimeLimit」を持つ GTPP データ レコード転送メッセージが、SDF コンテナを含まず、OFCS と交換されます。<br>• 受信したオフライン使用状況レポートに N4 セッション レポート要求の SDF レベルの時間しきい値の測定がない場合、GTPP データ レコード転送メッセージは OFCS と交換されません。 |
| 6 | OFCS は、GTPP データ レコード転送応答を SMF に送信します。 |
| 7 | SMF は、RG+SID ごとに 1 つまたは複数の MSCC を含む Gy CCR-U を送信します。 |

| 手順 | 説明 |
|---|---|
| 8 | SMF は、クォータを使用して Gy CCA-I を受信し、各 RG + サービス ID に対してトリガーします。 |
| 9 | SMF は、更新 URR を使用して N4 セッション変更要求を UPF に送信します。必要なオンライン URR のクォータを OCS から受け取ります。 |
| 10 | UPF が N4 セッション変更応答を送信します。 |

### 構成サンプル

次に、オフラインのベアラー レベル URR のメッセージ出力の例を示します。

```
URR ID:
                Type: 81   Length: 4
                Value: 0x80000002   --- Offline Bearer level URR Id
            USAGE REPORT TRIGGER:
                Type: 63   Length: 2
                Volume Threshold
            VOLUME MEASUREMENT:
                Type: 66   Length: 25
                Total Volume: 101096
                Uplink Volume: 896
                Downlink Volume: 100200
            DURATION MEASUREMENT:
                Type: 67   Length: 4
                Value: 16

            URR ID:
                Type: 81   Length: 4
                Value: 0x80000021.
            USAGE REPORT TRIGGER:
                Type: 63   Length: 2
                Linked Usage Reporting
            VOLUME MEASUREMENT:
                Type: 66   Length: 25
                Total Volume: 101096
                Uplink Volume: 896
                Downlink Volume: 100200
        DURATION MEASUREMENT:
                Type: 67   Length: 4
                Value: 1


         accessPointNameNi                    cisco.com
         ratingGroup                          10
         chargingRuleBaseName                 cisco
         resultCode                           2001
         localSequenceNumber                  1
         timeOfFirstUsage                     220829173906-0400
         timeOfLastUsage                      220829173907-0400
         timeUsage                            1
         serviceConditionChange               Volume Limit
          qCI                                  5
          maxRequestedBandwithUL               0
          maxRequestedBandwithDL               0
          guaranteedBitrateUL                  0
          guaranteedBitrateDL                  0
          aRP                                  5
```

```
servingNodeAddress                    2002::2:61
datavolumeFBCUplink                   896
datavolumeFBCDownlink                 100200
timeOfReport                          220829173907-0400
userLocationInformation
 Location Type                      TAI
  MCC                                 214
  MNC                                 365
  TAC                                 0x6789
  Location Type                     ECGI
  MCC                                 214
  MNC                                 365
  ECI                                 0x1234567
```

N4 セッション削除の応答のオフライン使用状況レポート

以下のコールフローと手順は、セッション削除応答における使用状況レポートを説明しています。

（注） UE またはネットワークが開始した削除セッションが SMF で検出されることを確認してください。

**図 *143 : N4* 削除セッション応答の使用レポートのコール フロー**

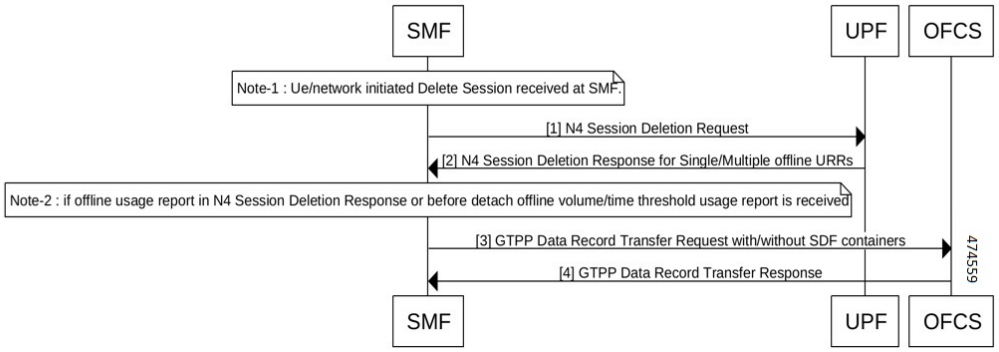



**表 *239 :* セッション削除応答のコール フローの説明**

| 手順 | 説明 |
|---|---|
| 1 | SMF は、UPF へのセッションを削除するために N4 セッション削除要求を開始します。 |
| 2 | UPF は、N4 セッション削除の応答をオフライン使用状況レポートとともに送信します。 |

| 手順 | 説明 |
|---|---|
| 3 | SMF は、SDF コンテナを使用してもしくは使用しないで GTPP データ転送要求を送信します。<br>• N4 セッション削除応答でオフラインの使用状況レポートを受信した場合、SMF は、最大課金条件がヒットした場合にのみ、SDF コンテナ（ボリューム使用率と serviceConditionChange を各 RG + サービス ID に 1 つずつ加えて）を使用してデフォルトで GTPP データ レコード転送要求を送信します。<br>• 受信したオフライン使用状況レポートが N4 セッション レポート要求のベアラー レベルの時間しきい値の測定値なしの場合、GTPP データ レコード転送メッセージで、recordClosureReason が「NormalRelease」であり、SDF コンテナを含まないものが、OFCS と交換されます。<br>• デタッチ前にオフラインのボリューム/時間しきい値の使用レポートを受信し、受信した N4 削除セッション応答にオフラインの使用状況レポートがない場合、GTPP データ レコード転送はレコード クローズのために SDF コンテナなしで交換されます。 |
| 4 | SMF は OFCS から GTPP データ レコード転送応答を受信します。 |

N4 セッション レポートのオフライン SDF 使用状況レポート

オフライン SDF または、ベアラー URR は、しきい値などの値とともに UPF に存在します。SDF ボリューム/時間のしきい値が、SDF レベルの URR の UPF でヒットします。UPF は、使用状況レポートのトリガー情報とともに、使用状況をSMFにリレーします。次のコールフローと手順では、オフラインのベアラー再計算の非同期使用状況レポートについて説明します。

**図 *144*：オフライン ベアラー再計算の非同期使用状況レポートのコール フロー**

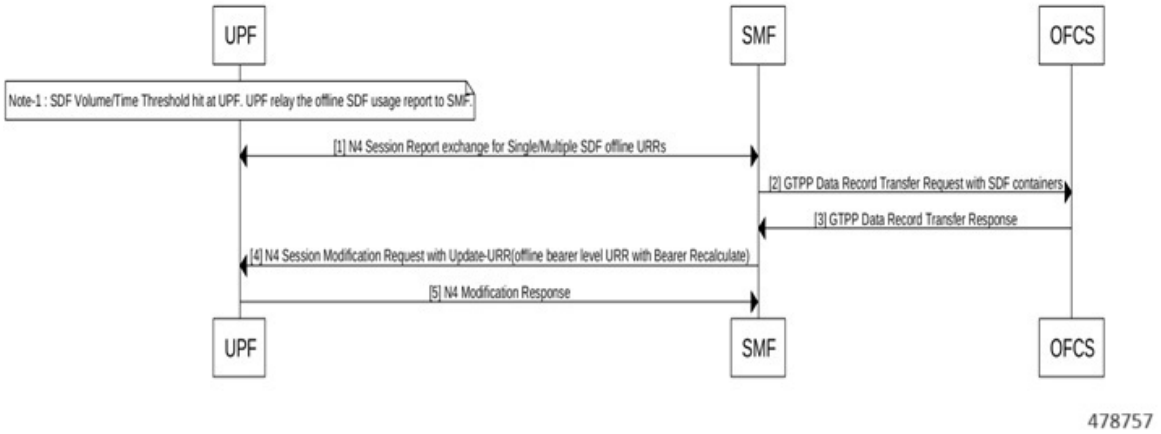


表 *240 :* 非同期使用状況レポートのオフラインのベアラー再計算のコール フローの説明

| 手順 | 説明 |
|---|---|
| 1 | UPF は、SMF との N4 セッション レポート交換を開始します。 |
| 2 | SMF は、SDF コンテナを使用して GTPP データ転送要求を送信します。<br>• N4 セッション レポート要求でオフラインの使用状況レポートを受信した場合、SMF は、最大課金条件がリーチした場合にのみ、SDF コンテナ（ボリューム使用率と serviceConditionChange を各 RG + サービス ID に 1 つずつ加えて）を使用して GTPP データ記録転送要求を送信します。<br>• 受信したオフライン使用状況レポートに N4 セッション レポート要求の SDF レベルの時間しきい値の測定がない場合、GTPP データ レコード転送メッセージは OFCS と交換されません。 |
| 3 | SMF は OFCS から GTPP データ レコード転送応答を受信します。 |
| 4 | オフライン SDF 使用量を受信した後、最大課金状態により SMF が GTPP データ レコード転送要求を送信すると、ベアラー レベルの更新 URR（ベアラーの再計算）を含む N4 変更要求が UPF に送信されます。 |
| 5 | UPF が N4 変更応答を送信します。 |

オフライン SDF またはオンライン URR の使用状況レポート

UPF で検出されたボリューム/時間しきい値の場合、UPF はオンライン URR またはオフライン SDF レベル URR の VOLTH/TIMTH を使用した使用状況レポートを作成します。次のコール フローと手順では、オンラインまたはオフラインのベアラー再計算の非同期使用状況レポートについて説明します。

図 *145 :* 非同期使用状況レポートのオンラインまたはオフライン ベアラー再計算のコール フロー

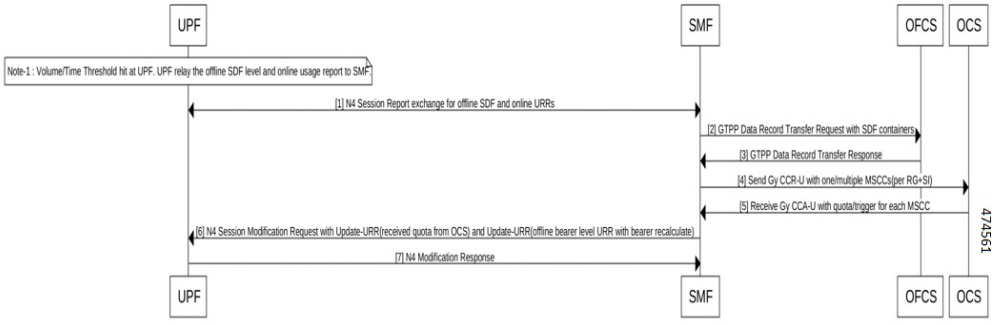


表 *241 :* 非同期使用状況レポートのオンラインまたはオフラインのベアラー再計算のコール フローの説明

| 手順 | 説明 |
|---|---|
| 1 | UPFは、オンライン/オフラインのボリューム/時間しきい値を使用して、N4セッション レポート要求/応答の交換を開始します。 |
| 2 | SMF は、SDF コンテナを使用して GTPP データ転送要求を送信します。<br>• N4 セッション レポート要求でオフラインの使用状況レポートを受信した場合、SMFは、最大課金条件がヒットした場合にのみ、SDFコンテナ（ボリューム使用率と serviceConditionChange を各 RG + サービス ID に 1 つずつ加えて）を使用して GTPP データ記録転送要求を送信します。<br>• 受信したオフライン使用状況レポートがN4セッション レポート要求のSDF レベル時間しきい値の測定値なしの場合、GTPP データ レコード転送メッセージは OFCS と交換されません。 |
| 3 | SMF は OFCS から GTPP データ レコード転送応答を受信します。 |
| 4 | SMF は、1 つまたは複数の MSCC（RG + サービス ID ごと）を含む Gy CCR-U を OCS に送信します。 |
| 5 | SMF は RG+Service ID ごとにトリガーとクォータを持つ Gy CCA-I を受信します。 |
| 6 | SMF は N4 セッション変更要求を UPF に送信します。<br>（注）<br>必要なオンライン URR の更新 URR-with クォータと、オフライン ベアラー レベル URR のベアラー再計算付きの更新 URR-with ベアラー再計算が送信されます。 |
| 7 | UPF が SMF に N4 セッション変更応答を送信します。 |

オフライン ベアラー使用状況レポート

オフライン SDF または、ベアラー URR は、しきい値などの値とともに UPF に存在します。SDF ボリューム/時間のしきい値が、ベアラーの URR の UPF でヒットします。UPF は、使用状況レポートのトリガー情報とともに、使用状況をSMF にリレーします。次のコール フローと手順では、N4 セッション レポート（非ベアラー再計算なし）のオフライン ベアラー使用状況レポートについて説明します。

図 *146 :* 非同期オフライン ベアラー使用状況レポート

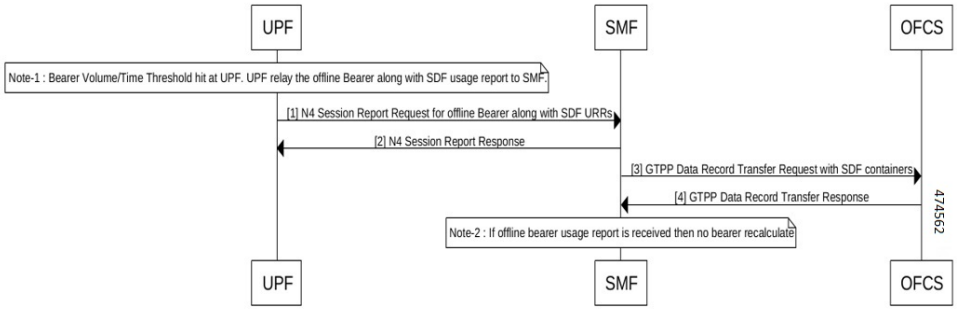



表 *242 :* ベアラー再計算なしの非同期オフライン ベアラー使用レポートのコール フローの説明

| 手順 | 説明 |
|---|---|
| 1 | UPF は、オフライン ベアラーと SMF への SDF 使用状況とともにN4 セッション レポート リクエストを送信します。 |
| 2 | SMF が N4 セッション レポート応答を UPF に送信します。 |
| 3 | SMF は、最大課金条件がヒットした場合にのみ、SDF コンテナ（ボリューム使用率と serviceConditionChange を各 RG + サービス ID に 1 つずつ加えて）を使用して GTPP データ記録転送要求を送信します。<br>受信したオフライン使用状況レポートにN4 セッション レポート要求のベアラー レベルの時間しきい値の測定がない場合、GTPP データ レコード転送メッセージは OFCS とともに SDF コンテナなしで送信されます。 |
| 4 | SMF は OFCS から GTPP データ レコード転送応答を受信します。 |
| （注）<br>ボリューム測定なしでベアラー使用状況レポートを受信した場合、SMF はベアラーの再計算を UPF に送信しません。 | |

オフライン SDF の使用状況レポート

次のコール フローと手順では、N4 セッション レポート（非ベアラー再計算なし）のオフライン ベアラー使用状況レポートについて説明します。

図 *147 :* ベアラー再計算なしの非同期使用状況レポート オフラインのコール フロー

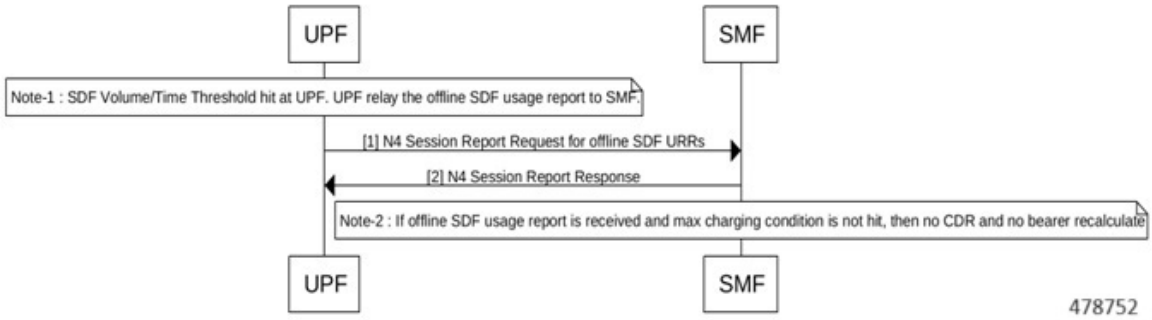



表 *243 :* ベアラー再計算なしの非同期オフライン ベアラー使用レポートのコール フローの説明

| 手順 | 説明 |
|---|---|
| （注）<br>オフライン SDF /ベアラー URR は、しきい値などの値とともに UPF に存在します。SDF ボリュームまたは時間しきい値が、SDF レベルの URR の UPF でヒットします。UPF は、使用状況レポートのトリガー情報とともに、使用状況をSMF にリレーする必要があります。 | |
| 1 | UPF は、オフライン SDF の使用状況を含む N4 セッション レポート要求を SMF に送信します。 |
| 2 | SMF が N4 セッション レポート応答を UPF に送信します。 |
| （注）<br>SDF 使用率レポートを受信し、最大充電条件に達していない場合、SMF は CDR を OFCS に送信し、ベアラーは UPF に再計算します。<br>max-losdv CLI 値が 2 に構成されており、1 つの SDF 使用状況レポートのみを受信します。2 番目の SDF レベルの使用量が受信され、最大課金条件に達すると、CDR が GTPP に送信され、ベアラーが UPF に再計算します。 | |

オフラインのベアラー再計算のための同期オンラインおよびオフライン使用状況レポート

次のコール フローと手順では、即時トリガを使用した N4 セッション変更要求でのオフライン SDF とオンライン URR の使用状況レポートについて説明します。

図 *148 :* 同期使用状況レポートのコール フロー

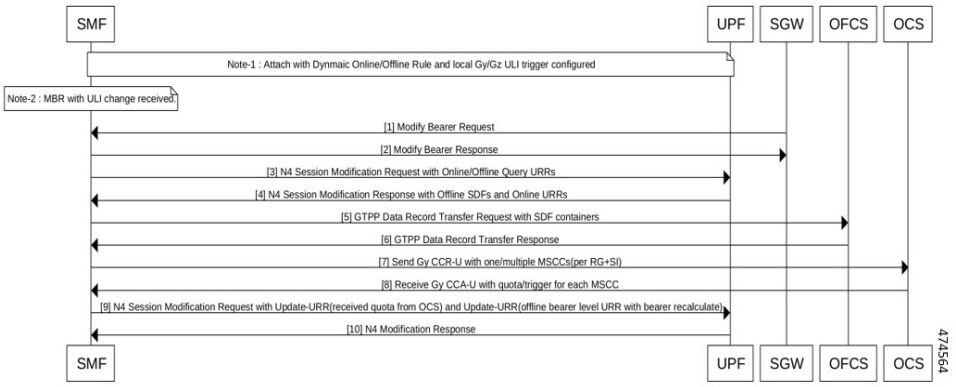



表 *244 :* オフラインのベアラー再計算のための同期オンラインおよびオフライン使用状況レポートのコール フロー説明

| 手順 | 説明 |
|---|---|
| （注）<br>デフォルト ベアラーは、1 つの動的なオンライン ルールとオフライン ルールを使用して作成されます。ULI トリガは、OFCS および OCS の課金プロファイルでローカルに構成されます。ULI 変更によるベアラー要求の変更を受信しました。 | |
| 1 | S-GW が新しい ULI を使用してベアラー要求の変更を送信します。 |
| 2 | SMF は、ベアラー応答の変更を S-GW に送信します。 |
| 3 | SMF は、オンラインのクエリ URR およびオフライン URR のクエリインターフェイスを含む UPF に N4 セッション変更要求を送信します。<br>SMF は、オンライン URR のクエリ URR およびクエリ インターフェイスを使用して、N4 セッション変更要求を UPF に送信し、オフライン URR のオフライン ビットが 1 に設定されたインターフェイスの再計算を実行します。 |
| 4 | UPF は、オフライン SDF およびオンライン URR の N4 セッション変更応答をレポート トリガ Immediate とともに送信します。 |
| 5 | SMF は、SDF コンテナを使用して GTPP データ転送要求を送信します。<br>• N4 セッション変更応答でオフラインの使用状況レポートを受信した場合、SMF は、最大課金条件がヒットした場合にのみ、SDF コンテナ（ボリューム使用率と serviceConditionChange を各 RG + サービス ID に 1 つずつ加えて）を使用して GTPP データ記録転送要求を送信します。<br>• 受信したオフライン使用状況レポートに N4 セッション変更応答の SDF レベルの時間しきい値の測定がない場合、GTPP データ レコード転送メッセージは OFCS と交換されません。 |
| 6 | SMF は OFCS から GTPP データ レコード転送応答を受信します。 |

| 手順 | 説明 |
|---|---|
| 7 | SMF は、1 つまたは複数の MSCC（RG + SID ごと）を含む Gy CCR-U を OCS に送信します。 |
| 8 | SMF は、クォータを使用して Gy CCA-I を受信し、各 RG + サービス ID に対してトリガーします。 |
| 9 | SMF は、オンライン URR 用の受け取ったクォータを含む更新 *URR* と、オフラインのベアラー レベル URR 用のベアラー再計算を含む更新 URR を伴う N4 セッション変更要求を送信します。 |
| 10 | UPF が SMF に N4 セッション変更応答を送信します。 |

### 構成サンプル

次に、オフラインのベアラー レベル URR のメッセージ出力の例を示します。

```
URR ID:
                Type: 81   Length: 4
                Value: 0x80000002
            USAGE REPORT TRIGGER:
                Type: 63   Length: 2
                Time Threshold
            VOLUME MEASUREMENT:
                Type: 66   Length: 25
                Total Volume: 450
                Uplink Volume: 250
                Downlink Volume: 200
            DURATION MEASUREMENT:
                Type: 67   Length: 4
                Value: 100

            URR ID:
                Type: 81   Length: 4
                Value: 0x00000021.
            USAGE REPORT TRIGGER:
                Type: 63   Length: 2
                Linked Usage Reporting
            VOLUME MEASUREMENT:
                Type: 66   Length: 25
                Total Volume: 450
                Uplink Volume: 250
                Downlink Volume: 200
            DURATION MEASUREMENT:
                Type: 67   Length: 4
                Value: 87

        accessPointNameNi                   cisco.com
        ratingGroup                         10
        chargingRuleBaseName                cisco
        resultCode                          2001
        localSequenceNumber                 1
        timeOfFirstUsage                    220822005641-0400
        timeOfLastUsage                     220822005646-0400
        timeUsage                           5
        serviceConditionChange              Time Limit
         qCI                                 5
         maxRequestedBandwithUL              0
```

```
 maxRequestedBandwithDL                0
 guaranteedBitrateUL                   0
 guaranteedBitrateDL                   0
 aRP                                   5
servingNodeAddress                     2002::2:61
datavolumeFBCUplink                    250
datavolumeFBCDownlink                  200
timeOfReport                           220822005818-0400
userLocationInformation
 Location Type                       TAI
  MCC                                  214
  MNC                                  365
  TAC                                  0x6789
  Location Type                     ECGI
  MCC                                  214
  MNC                                  365
  ECI                                  0x1234567
```

## OAM サポート

ここでは、SFMのインターフェイスのサポートに関する操作、管理、およびメンテナンスに関して説明します。

バルク統計サポート

Gz 充電機能用に、次のカウンタが追加されました：

- ofcs_cdr_message_stats：カウンタは、CGF に向かうすべての CDR に対して増加します。次のラベルが追加されます：
  - **gtpp_profile** *gtpp_profile_name*：このメトリックは、GTPP プロファイルを表示します。
  - **RuleBase** *RuleBase Name*：このメトリックは、ルール ベースの名前を表示します。
  - **record_closure_reason***record_closure_reason* ：このメトリックは、レコードがクローズされた理由のいずれかを表示します：
    - normalRelease
    - abnormalRelease
    - cAMELInitCallRelease
    - volumeLimit
    - timeLimit
    - servingNodeChange
    - maxChangeCond
    - managementIntervention
    - intraSGSNIntersystemChange
    - rATChange
    - mSTimeZoneChange

- sGSNPLMNIDChange
- **dnn** *dnn_name* ：このメトリックは、DNN 名を表示します。
- **TriggerType** *[Trigger_name]* ：このメトリックには、次のトリガー タイプの GZ_SECONDARY_RAT_USAGE_LIMIT_REACHED が表示されます。

- ofcs_sdf_container_stats：カウンタは、CGF への CDR のすべての SDF コンテナで増加します。次のラベルが追加されます。
- **service_condition_change** *service_condition_change_value* ：service_condition_change ラベル値は、各 SDF コンテナの複数のサービス条件変更値の場合にカンマで区切られます。このメトリックには、サービス条件の変化に応じた値が表示されます：
  - QoSChange
  - PdpContextRelease
  - ConfigurationChange
  - ServiceStop
  - DccaTimeExhausted
  - DccaVolumeExhausted
- ofcs_cdr_drop_stats：OFCS に対するゼロ抑制により、抑制されるすべての CDR のカウンタが増加します。次のラベルが追加されます：
  - **procedure_type** *procedure_name*：このメトリックは、抑制基準が満たされたトリガー名とともに SMF 手順名が表示されます。
  - **TriggerType** *[Trigger_name]* ：このメトリックには、次のトリガー名のいずれかが表示されます。
    - 最終 CDR
    - 外部トリガー CDR
    - intrenal-trigger-cdr
  - **dnn** *dnn_name* ：このメトリックは、DNN 名を表示します。

## ベアラー要求トリガの変更の処理

### 機能説明

SMFは、ユーザーの場所とタイムゾーンの変更、変更通知について、S-GWからベアラー要求の変更を受信します。次の機能は、トリガによってサポートされます。

- タイムゾーン トリガ：CHANGE_IN_UE_TIMEZONE トリガを使用して、タイムゾーンの変更を特定します

- ULI トリガ：CHANGE_IN_LOCATION、CHANGEINLOCATION_TAC、および CHANGEINLOCATION_ECGI を使用してロケーションの変更を特定します。

制限事項

次の制限事項があります。

- SMF は、Gz オフライン URR に対してのみ QueryInterface と RecalculateInterface をサポートしています。Gy onlineURR および RADIUS URR ではサポートされません。
- RecalculateInterface value(264) IE タイプが仕様で指定されているベンダー タイプ範囲内にありません。RecalculateInterface value (264) IE タイプへの更新は、UPF でサポートが利用可能な場合に必要です。
- 専用ベアラーのトリガ処理はサポートされていません。

## タイムゾーンの変更

タイムゾーン情報は、CDR レベルでのみ送信されます。次のコール フローは、SMF のタイムゾーンの変更を示しています。

**図 *149 :* タイムゾーンの変更によるベアラー変更要求**

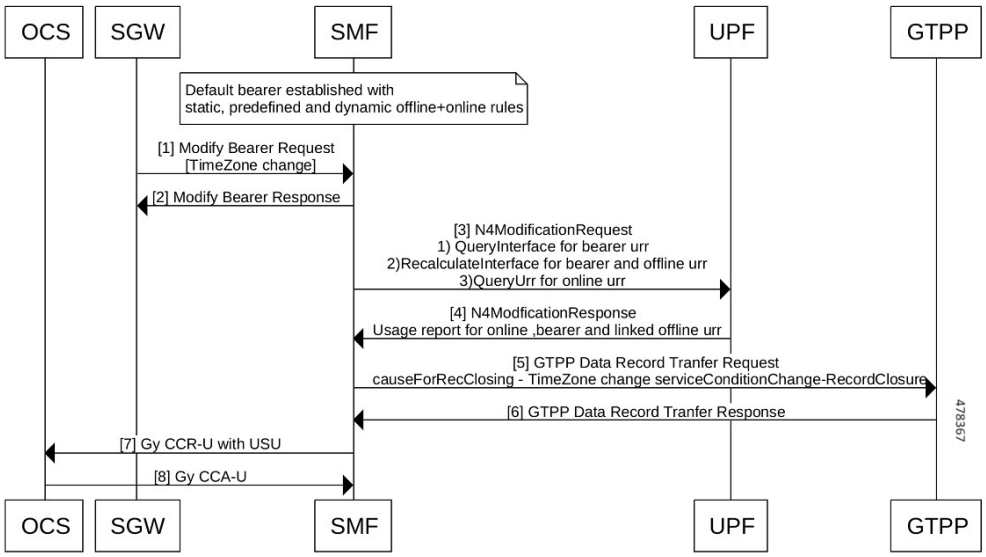



**表 *245 :* タイムゾーンの変更のコール フローの説明**

| ステップ | 説明 |
|---|---|
| デフォルトのベアラーが正常に確立され、最初の接続は動的、静的、および事前定義されたルールで行われます。 | |

| ステップ | 説明 |
|---|---|
| 1 | SMF は、タイムゾーンの変更を含む S-GW からのベアラー要求の変更を受信します。 |
| 2 | SMF はベアラー応答の変更を送信します。 |
| 3 | N4 変更要求は、次の詳細とともに送信されます：<br>• オンライン URR の QueryUrr<br>• ベアラー URR に **bearer_urr** が設定されたクエリ インターフェイス<br>• SDF URR の **offline_urr** および **bearer_urr** を使用してインターフェイスを再計算します。<br>（注）<br>**bearer_urr** がクエリ インターフェイスでクエリされると、再計算インターフェイスでベアラーとオフライン/SDF URR の両方の再計算が要求されます。 |
| 4 | SMF は、UPF から次の詳細を含む N4 変更応答を受信します。<br>• ベアラー URR とリンクされた SDF URR の使用状況レポート<br>• オンライン URR の UsageReport |
| 5 | SMF は、レコード終了理由タイムゾーンの変更を含む GTPP データ レコード転送要求を GTPP に送信します。<br>（注）<br>タイムゾーンの変更は、仕様に従ってレコードクローズイベントです。したがって、ベアラーの URR が照会され、続いて CDR が送信されます。 |
| 6 | SMF が GTPP データ レコード転送応答を受信します。 |
| 7 | UPF は、受信した使用状況を含む Gy CCR-U メッセージを OCS に送信します。 |
| 8 | SMF は OCS から Gy CCA-U を受信します。 |

### N4 変更要求例

```
PFCP_SESSION_MODIFICATION_REQUEST (52)
'Retransmit flag'  : 0
'Seid'             : 17293822569102704642
'Length'           : 71
'Sequence Number'  : 3
'Number of IEs'    : 5
    PFCP_IE_SUB_PARAMS (226)
      'sub_params' : {'rat_type': 6, 'sgsn_v4': '10.105.38.134', 'uli_len': 13, 'uli':
{'spare': 0, 'ecgi': 1, 'tai': 1, 'nrtai': 0, 'nrcgi': 0, 'tai-mcc': 123, 'tai-mnc':
456, 'tai-tac': 2347, 'ecgi-mcc': 123, 'ecgi-mnc': 456, 'ecgi-spare': 0, 'ecgi-eci':
1234567}, 'ggsn_v4': '10.21.82.217'}
```

```
    PFCP_IE_QUERY_URR (77)

            PFCP_IE_URR_ID (81)
                  'urr_id' : 55

    PFCP_IE_PFCPSMREQFLAGS (49)
           'spare' : 0
           'qaurr' : 1
           'sndem' : 0
           'drobu' : 0

    PFCP_IE_QUERY_INTERFACE (253)
   'query_interface' : {'spare_3bit': 0, 'offline_urr': 0, 'online_urr': 0, 'radius_urr':
 0, 'bearer_urr': 1, 'sess_urr': 0}

    PFCP_IE_RECALCULATE_INTERFACE (264)
    'recalculate_interface' : {'spare_3bit': 0, 'offline_urr': 1, 'online_urr': 0,
'radius_urr': 0, 'bearer_urr': 1, 'sess_urr': 0}


        MESSAGE BUFFER:
                2134 0047 F000 0000 0000 0002 0000 0304
                00E2 001C 0100 012A 060A 6926 860D 1821
                6354 092B 2163 5400 12D6 870A 1552 D904
                004D 0008 0051 0004 0000 0037 0031 0001
                0400 FD00 0110 0108 0001 10
```

## *CDR* レベルでタイムゾーン情報が送信されました

次の表に、CDR レベルで送信されるタイムゾーン情報を示します。

| PreCondition | シナリオ | Expected Behaviour |
|---|---|---|

| | | |
|---|---|---|
| Maxlosdv 1<br>MSTimeZone でのCSR<br>ベアラーしきい値 60 秒（Bearer threshold 60 seconds）<br>**タイムゾーン** トリガの有効化 | **TimeZone1** を使用したアタッチ<br>時間しきい値でベアラー使用率を受信しました<br>**TimeZone2** でのMBR<br>時間しきい値でベアラー使用率を受信しました<br>**TimeZone3** でのMBR<br>時間しきい値でベアラー使用率を受信しました<br>トラフィック データとの接続を解除する | N4 インターフェイスでは、**ベアラー**ビットがオフラインに設定された状態で、タイムゾーン変更のクエリが実行されます。<br>最初のベアラー使用率を受信した後、CDR は **TimeZone1** で送信されます<br>最初の **MBR** のベアラー使用状況を受信した後、CDR は**TimeZone1** で送信されます<br>2 番目のベアラー使用を受信した後、CDR は **TimeZone2** で送信されます<br>2 番目の **MBR**のベアラー使用状況を受信した後、CDR は**TimeZone2** で送信されます<br>3番目のベアラーの使用を受信すると、CDR は **TimeZone3** で送信されます<br>**デタッチ**中に使用状況レポートを終了する場合、CDR は**TimeZone3** で送信されます |
| Maxlosdv 1<br>**MSTimeZone** のないCSR<br>ベアラーしきい値 60 秒（Bearer threshold 60 seconds）<br>**TimeZone** トリガの有効化 | **TimeZone なしで**アタッチ<br>時間しきい値でベアラー使用率を受信しました<br>**TimeZone1** でのMBR<br>時間しきい値でベアラー使用率を受信しました<br>**TimeZone2** でのMBR<br>時間しきい値でベアラー使用率を受信しました<br>トラフィック データとの接続を解除する | N4 インターフェイスでは、**ベアラー**ビットがオフラインに設定された状態で、タイムゾーン変更のクエリが実行されます。<br>最初のベアラー使用率を受信した後、CDR は**タイムゾーンなしで**送信されます<br>最初の **MBR** のベアラー使用率を受信した後、CDR が **TimeZone なしで**送信されます<br>2 番目のベアラー使用を受信した後、CDR は **TimeZone1** で送信されます。<br>2 番目の **MBR**のベアラー使用率を受信した後、CDR が **TimeZone1** で送信されます。<br>3番目のベアラーの使用状況を受信した後、CDR は**TimeZone2** で送信されます<br>**デタッチ**中に使用状況レポートを終了する場合、CDR は**TimeZone2** で送信されます |

| | | |
|---|---|---|
| Maxlosdv 1<br>**MSTimeZone** でのCSR<br>ベアラーしきい値 60 秒<br>**Suppress zero cdrs**<br>**TimeZone** トリガの有効化 | **TimeZone1**を使用したアタッチ<br>**TimeZone2 で使用量がゼロ（トラフィックなし、ボリュームなし）の MBR を受信**<br>**TimeZone3 で使用量がゼロ（トラフィックなし、ボリュームなし）の MBR を受信**<br>トラフィックなしで時間しきい値の使用量がゼロ（トラフィックなし、ボリュームなし）を受信しました<br>トラフィック データとの接続を解除する | N4 インターフェイスでは、**ベアラー**ビットがオフラインに設定された状態で、タイムゾーン変更のクエリが実行されます。<br>切断中に使用状況レポートを終了する場合、CDRは**TimeZone2** で送信されます |
| Maxlosdv 1<br>MSTimeZone でのCSR<br>ベアラーしきい値 60 秒（Bearer threshold 60 seconds）<br>**TimeZone** トリガの**無効化** | **TimeZone1** を使用したアタッチ<br>時間しきい値でベアラー使用率を受信しました<br>**TimeZone2** での MBR<br>時間しきい値でベアラー使用率を受信しました<br>**TimeZone3** での MBR<br>時間しきい値でベアラー使用率を受信しました<br>切断 | TimeZone の N4 クエリでは、オフラインの場合、変更は発生しない。<br>すべての CDR が **TimeZone1**で送信されます |
| Maxlosdv 1<br>MSTimeZone のない CSR<br>ベアラーしきい値 60 秒（Bearer threshold 60 seconds）<br>**TimeZone** トリガの**無効化** | **TimeZone1**を使用したアタッチ<br>時間しきい値でベアラー使用率を受信しました<br>**TimeZone2** での MBR<br>時間しきい値でベアラー使用率を受信しました<br>**TimeZone3** での MBR<br>時間しきい値でベアラー使用率を受信しました<br>切断 | N4 クエリでは、タイムゾーンの変更はオフラインで発生しないようにする必要があります。<br>すべての CDR は **TimeZone なしで**送信されます。 |

## ユーザー ロケーション情報の変更

ユーザーの位置情報は、CDR と SDF の両方のコンテナ レベルで送信されます。接続が実行されると、1 つの CDR が現在のレコード開始時刻と現在の ULI で開かれます。CDR が生成されると、現在のレコード開始時刻と最後のユーザーの位置情報で別の CDR が開かれます。

次のコール フローは、SMF のユーザロケーション情報（ULI）の変更を示しています。

**図 *150 : ULI* 変更によるベアラー要求の変更**

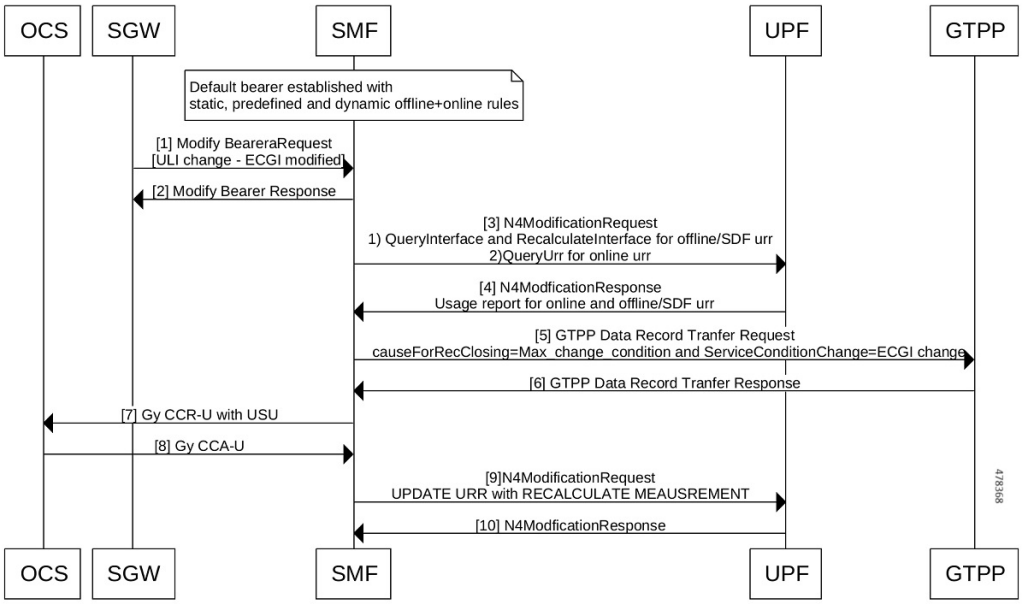



**表 *246 : ULI* 変更のコール フローの説明**

| ステップ | 説明 |
|---|---|
| 1 | デフォルトのベアラーが正常に確立され、最初の接続はダイナミック、静的、および事前定義されたルールで行われます。 |
| 2 | SMF は、ULI で変更された ECGI を使用して S-GW からベアラー要求の変更を受信します。 |
| 3 | SMF はベアラー応答の変更を送信します |

| ステップ | 説明 |
|---|---|
| 4 | N4 変更要求は、次の詳細とともに送信されます：<br>• オンライン URR の QueryUrr。<br>• SDF URR に **offline_urr** が設定されたクエリ インターフェイス。<br>• SDF URR に設定された **offline_urr** を使用してインターフェイスを再計算します。<br>（注）<br>**offline_urr** がクエリ インターフェイスでクエリされると、再計算インターフェイスでオフライン/SDF URR のみの再計算が要求されます。 |
| 5 | SMF は、次の詳細とともに UPF から N4 変更応答を受信します。<br>• SDF URR の使用状況レポート<br>• オンライン URR の使用状況レポート |
| 6 | SMF は、Max_change_condition として終了理由を記録し、ECGI の変更として serviceConditionChange を記録する GTPP データ記録転送要求を送信します。<br>（注）<br>ULI の変更は、仕様上、クローズ イベント レコードではありません。したがって、SDF URR がクエリされます。同じものに対する使用状況レポートを受信すると、MaxLosDv がヒットした場合、対応する理由とともに CDR が送信されます。 |
| 6 | SMF が GTPP データ レコード転送応答を受信します。 |
| 7 | UPF は、受信した使用状況を含む Gy CCR-U メッセージを OCS に送信します。 |
| 8 | SMF は OCS から Gy CCA-U を受信します。 |

### N4 変更要求例

```
PFCP_SESSION_MODIFICATION_REQUEST (52)
'Retransmit flag'  : 0
'Seid'             : 17293822569102704642
'Length'           : 71
'Sequence Number'  : 3
'Number of IEs'    : 5
    PFCP_IE_SUB_PARAMS (226)
      'sub_params' : {'rat_type': 6, 'sgsn_v4': '10.105.38.134', 'uli_len': 13, 'uli':
{'spare': 0, 'ecgi': 1, 'tai': 1, 'nrtai': 0, 'nrcgi': 0, 'tai-mcc': 123, 'tai-mnc':
456, 'tai-tac': 2347, 'ecgi-mcc': 123, 'ecgi-mnc': 456, 'ecgi-spare': 0, 'ecgi-eci':
1234567}, 'ggsn_v4': '10.21.82.217'}

    PFCP_IE_QUERY_URR (77)

            PFCP_IE_URR_ID (81)
                  'urr_id' : 55
```

```
    PFCP_IE_PFCPSMREQFLAGS (49)
           'spare' : 0
           'qaurr' : 1
           'sndem' : 0
           'drobu' : 0

    PFCP_IE_QUERY_INTERFACE (253)
   'query_interface' : {'spare_3bit': 0, 'offline_urr': 1, 'online_urr': 0, 'radius_urr':
 0, 'bearer_urr': 0, 'sess_urr': 0}

    PFCP_IE_RECALCULATE_INTERFACE (264)
    'recalculate_interface' : {'spare_3bit': 0, 'offline_urr': 1, 'online_urr': 0,
'radius_urr': 0, 'bearer_urr': 0, 'sess_urr': 0}


        MESSAGE BUFFER:
                2134 0047 F000 0000 0000 0002 0000 0304
                00E2 001C 0100 012A 060A 6926 860D 1821
                6354 092B 2163 5400 12D6 870A 1552 D904
                004D 0008 0051 0004 0000 0037 0031 0001
                0400 FD00 0110 0108 0001 10
```

### サービス条件変更の理由

ULI 変更のサービス条件変更理由は次のとおりです。

- TAI が ULI で変更された場合、CDR の ServiceConditionChange の理由は「tailChange」です。
- ECGI が ULI で変更された場合、CDR の ServiceConditionChange の理由は「EcgiChange」です。
- TAI と ECGI の両方が ULI で変更された場合、CDR の ServiceConditionChange の理由は一般的な「UserLocationChange」です

## *CDR* および *SDF* コンテナ レベルで送信される *ULI* 情報

次の表では、CDR および SDF コンテナ レベルで送信される ULI 情報のシナリオとその動作について説明します。

| PreCondition | シナリオ | Expected Behaviour |
|---|---|---|

| | | |
|---|---|---|
| Maxlosdv 1<br>ULI を含む CSR<br>ベアラーしきい値 60 秒<br>ULI トリガーの 有効化 | ULI1でのアタッチ<br>時間しきい値でベアラー使用率を受信しました<br>ULI 2を使用した MBR<br>時間しきい値でベアラー使用率を受信しました<br>ULI3を使用した MBR<br>時間しきい値でベアラー使用率を受信しました<br>切断 | N4 クエリで ULI 情報の変更が発生すると、オフラインに対して オフライン ビットが設定されます。<br>最初のベアラーの使用状況を受信した後、CDR および SDF コンテナが ULI1 で送信されます。<br>1 番目の MBRの SDF 使用量を受信した後、CDR および SDF コンテナが ULI1 で送信されます。<br>2 番目のベアラーの使用を受信すると、URI1 を持つ CDR と ULI2 を持つ SDF コンテナが送信されます。<br>2 番目の MBRの SDF 使用率を受信した後、CDR および SDF コンテナが ULI2 で送信されます。<br>3 番目のベアラーの使用を受信すると、URI2 を持つ CDR と ULI3 を持つ SDF コンテナが送信されます。<br>切断中に使用状況レポートを終了する場合、CDR および SDF コンテナは ULI3で送信されます。 |

| | | |
|---|---|---|
| Maxlosdv 1<br>**ULI なしの**CSR<br>ベアラーしきい値 60 秒（Bearer threshold 60 seconds）<br>**ULI** トリガーの **有効化** | **ULI なしで**アタッチ<br>時間しきい値でベアラー使用率を受信しました<br>**ULI1**を使用した MBR<br>時間しきい値でベアラー使用率を受信しました<br>**ULI 2**を使用した MBR<br>時間しきい値でベアラー使用率を受信しました<br>切断 | N4 クエリで ULI 情報の変更が発生すると、オフラインに対して **オフライン** ビットが設定されます。<br>1 番目のベアラーの使用状況を受信した後、CDR および SDF コンテナは **ULI なしで**送信されます。<br>**1 番目の MBR**の SDF 使用率を受信した後、CDR および SDF コンテナが **ULI なしで**送信される<br>2 回目のベアラー使用を受信した後、**URI のない** CDR と **ULI1** のある SDF コンテナが送信されます。<br>2 番目の **MBR**の SDF 使用量を受信した後、CDR および SDF コンテナが **ULI1** で送信されます。<br>3回目のベアラーの使用を受信すると、**URI1** を持つ CDR と **ULI2** を持つ SDF コンテナが送信されます。<br>**切断**中に使用状況レポートを終了する場合、CDR および SDF コンテナが **ULI2**で送信されます。 |
| Maxlosdv 1<br>ULI **を含む CSR**<br>ベアラーしきい値 60 秒<br>**Suppress zero cdrs**<br>**ULI** トリガーの **有効化** | **ULI1** でのアタッチ<br>**ULI2 で使用量がゼロ（トラフィックなし、ボリュームなし）の MBR を受信**<br>**ULI3 で使用量がゼロ（トラフィックなし、ボリュームなし）の MBR を受信**<br>**時間しきい値**の使用量がゼロ（トラフィックなし、ボリュームなし）を受信しました<br>**トラフィック データ**との接続を解除する | N4 クエリで ULI 情報の変更が発生すると、オフラインに対して **オフライン** ビットが設定されます。<br>**切断**中に使用状況レポートを終了する場合、 **URI1** を持つ CDR と **ULI3** を持つ SDF コンテナが送信されます。 |

| | | |
|---|---|---|
| **Maxlosdv 3**<br>ULI を含む CSR<br>ベアラーしきい値 60 秒<br>**ULI** トリガーの **有効化** | **ULI1** でのアタッチ<br>**ULI2** を使用する MBR と SDF の **使用量はゼロ**（トラフィックなし、ボリュームなし）<br>**ULI3** と SDF の **使用量がゼロの** MBR（トラフィックなし、ボリュームなし）<br>**ULI4** を使用した MBR と **2 SDF の使用**<br>**ULI5** を使用した MBR と **3 SDF の使用**を受信<br>2 つの SDF の使用によるデタッチ | N4 では、URI 情報の変更のクエリで、オフラインに設定された **オフライン** ビットが使用されます。<br>**4 番目の MBR の SDF の使用量**を受信した後、 **URI1** と 3 つの SDF コンテナ（**SDF1** の **ULI3**、 **SDF2** の **ULI3** 、**SDF3** の **ULI4**） を持つ 1 つの CDR が送信されます。<br>**終了の** 使用状況を受信すると、SDF コンテナを含む **2 つの CDR**が送信されます。<br>**ULI4 を** 含む **1 番目の CDR** と 3 つの SDF コンテナ（**SDF4** は **ULI4**、 **SDF5** は **ULI4** 、 **SDF6** は **ULI5**）<br>**ULI5** と 1 つの SDF コンテナを含む **2 番目の CDR** （ **URI5** を使用する **SDF7**）。 |
| Maxlosdv 1<br>**ULI を含む**CSR<br>ベアラーしきい値 60 秒（Bearer threshold 60 seconds）<br>**ULI** トリガーの **無効化** | **ULI1**でのアタッチ<br>時間しきい値でベアラー使用率を受信しました<br>**ULI 2**を使用した MBR<br>時間しきい値でベアラー使用率を受信しました<br>**ULI3**を使用した MBR<br>時間しきい値でベアラー使用率を受信しました<br>切断 | ユーザーの場所情報の N4 クエリでは、オフラインの場合、変更は発生しない。<br>すべての CDR および SDF コンテナが **ULI1**で送信されます。 |

| | | |
|---|---|---|
| Maxlosdv 1<br>**ULI なしの**CSR<br>ベアラーしきい値 60 秒（Bearer threshold 60 seconds）<br>**ULI** トリガーの **無効化** | **ULI なしで**アタッチ<br>時間しきい値でベアラー使用率を受信しました<br>**ULI1**を使用した MBR<br>時間しきい値でベアラー使用率を受信しました<br>**ULI 2**を使用した MBR<br>時間しきい値でベアラー使用率を受信しました<br>切断 | ユーザーの場所情報の N4 クエリでは、オフラインの場合、変更は発生しない。<br>すべての CDR および SDF コンテナは **ULIなしで**送信されます。 |

## 変更通知

次のコール フローと手順では、SMF での変更通知について説明します。

**図 *151 :* 変更通知のコール フロー**

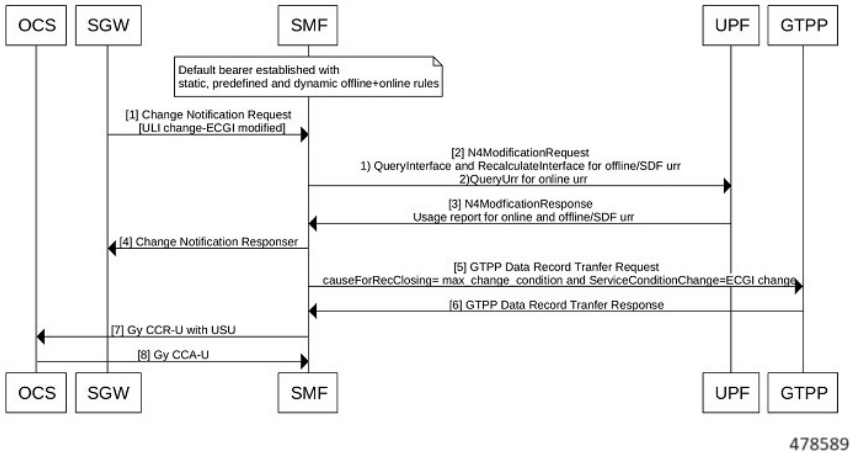



**表 *247 :* 変更通知の変更のコール フロー説明**

| ステップ | 説明 |
|---|---|
| （注）<br>デフォルトのベアラーが正常に確立され、最初の接続はダイナミック、静的、および事前定義されたルールで行われます。 | |
| 1 | S-GW が変更通知要求を SMF に送信します。たとえば、変更通知は ULI 変更 ECGI が変更されて送信されます。 |

| ステップ | 説明 |
|---|---|
| 3 | N4 変更要求は、次の詳細とともに送信されます：<br>• オンライン URR の QueryUrr<br>• オフライン/SDF URL の QueryInterface および RecalculateInterface |
| 5 | SMF は、次の詳細とともに UPF から N4 変更応答を受信します。<br>• SDF URR の使用状況レポート<br>• オフラインおよびオンライン URR の使用状況レポート |
| 6 | SMF は、max-change_condition を使用して GTPP データ レコード転送要求を GTPP に送信します。 |
| 6 | SMF が GTPP データ レコード転送応答を受信します。 |
| 7 | UPF は、受信した使用状況を含む Gy CCR-U メッセージを OCS に送信します。 |
| 8 | SMF は OCS から Gy CCA-U を受信します |

## インターフェイスのクエリとインターフェイス IE の再計算

次の表では、クエリ インターフェイスと再計算インターフェイス IE について説明します。

| トリガー | **N4 クエリ インターフェイス** | **N4 インターフェイス再計算** | **N4 クエリ URR** |
|---|---|---|---|
| ルールベースの変更 | クエリ インターフェイス - たとえば、**bearer_urr': 1**<br>"offline_urr": 0<br>“online_urr”:0<br>“radius_urr”:0<br>UPF は、SDF レベルの使用状況とともにベアラー レベルの使用状況を報告します。 | インターフェイスの再計算<br>**-"bearer_urr": 1**<br>**"offline_urr"** : **1**<br>“online_urr”:0<br>“radius_urr”:0 | **北米** |

| | | | |
|---|---|---|---|
| セカンダリ RAT の使用制限 | クエリ インターフェイス - たとえば、**bearer_urr': 1**<br>"offline_urr": 0<br>“online_urr”:0<br>“radius_urr”:0<br>UPF は、SDF レベルの使用状況とともにベアラー レベルの使用状況を報告します。 | インターフェイスの再計算 - **"bearer_urr": 1**<br>**"offline_urr"** : **1**<br>“online_urr”:0<br>“radius_urr”:0 | |
| レコード終了トリガー：例：タイムゾーンの変更 | クエリ インターフェイス - たとえば、**bearer_urr': 1**<br>"offline_urr": 0<br>“online_urr”:0<br>“radius_urr”:0<br>UPF は、SDF レベルの使用状況とともにベアラー レベルの使用状況を報告します。 | インターフェイスの再計算：**"Bearer_urr": 1**<br>**"offline_urr": 1**<br>“online_urr”:0<br>“radius_urr”:0 | online および radius |
| SDFレベルクエリ：例: QOSの変更 | -bearer_urr': 0 でのクエリ インターフェイス<br>**"offline_urr"** : **1**<br>“online_urr”:0<br>“radius_urr”:0<br>UPF は、すべての SDF レベルの使用状況を報告します。SMF は、SDF レベル URR のしきい値をリセットするために同じ N4 で再計算を送信する必要があります。 | インターフェイスの再計算:<br>"bearer_urr": 0<br>**"offline_urr": 1**<br>“online_urr”:0<br>“radius_urr”:0 | オンラインおよび RADIUS |

| | | | |
|---|---|---|---|
| レコードクローズ - 最大変更条件によるベアラー レベル制限の再計算 | **北米** | URR の更新：<br>タイプ：13<br>Value：<br>URR ID：<br>タイプ：81 値：0x80000002<br>測定値の再計算:<br>タイプ：216<br>RCVOL：1<br>RCDUR：1 | NA |
| 個別のURRクエリ：現在、将来のユースケースはこれを必要としません。 | クエリ URR：<br>**値：<XYZ>** | URR の更新：<br>タイプ：13<br>Value：<br>URR ID：<br>タイプ：81 **値：XYZ**<br>測定値の再計算:<br>タイプ：216<br>RCVOL：1<br>RCDUR：1 | N/A |

## Gzトリガーの構成

Gz トリガーを構成するには、次の構成例を使用します。

```
config
   active-charging service service_name
      charging-action charging_action
        egcdr  losdv-max-containers   service-data-flow triggers {
ms-timezone-change [ true | false ] | qos-change [ true | false ] |
uli-change [ true | false ] }
   end
```

注：

- **egcdr losdv-max-containers** ：1 つの EGCDR 内の LoSDV コンテナの最大数を構成します。**losdv-max-containers** value は1ー255の範囲の整数である必要があります。デフォルト値は 1 です。
- **egcdr service-data-flow** ：サービス データフ ローを構成します。
- **egcdr triggers { ms-timezone-change [ true | false ] | qos-change [ true | false ] | uli-change [ true | false ] }**

- **egcdr triggers**：CDR のトリガーのリストを構成します。デフォルトでは、次のトリガーが有効になっています：
  - **triggers ms-timezone-change [ true | false ]**：CDR デフォルトの MS タイム ゾーン トリガーを有効または無効にします。
  - **triggers qos-change [ true | false ]**：CDR のデフォルトの QoS 変更トリガーを有効または無効にします。
  - **triggers uli-change [ true | false ]**：CDR のデフォルトのユーザーの場所の変更トリガーを有効または無効にします。

# Gz デフォルト ベアラーの変更

## 機能説明

SMF は、Gx CCR-U および Gx RAR を介してデフォルトのベアラーの PCRF によって開始される変更をサポートしています。次の機能を実行できます。

- デフォルトのベアラーにルールを追加する
- デフォルトのベアラーからルールを削除する
- ルールベースの変更
- デフォルト ベアラー QoS の変更
- APN-AMBR の変更

## 機能の仕組み

このセクションでは、SMF での Gz デフォルト ベアラー変更機能に関連するコール フローについて説明します。

コール フロー

デフォルト ベアラーへのオフライン ルールの追加

ベアラー レベルの URR ID は、ベアラーごとに 1 回だけ作成されます。次のコール フローと手順で、さまざまなダイナミック ルールの追加シナリオについて説明します。

図 *152 :* デフォルト ベアラーへのオフライン ルールの追加

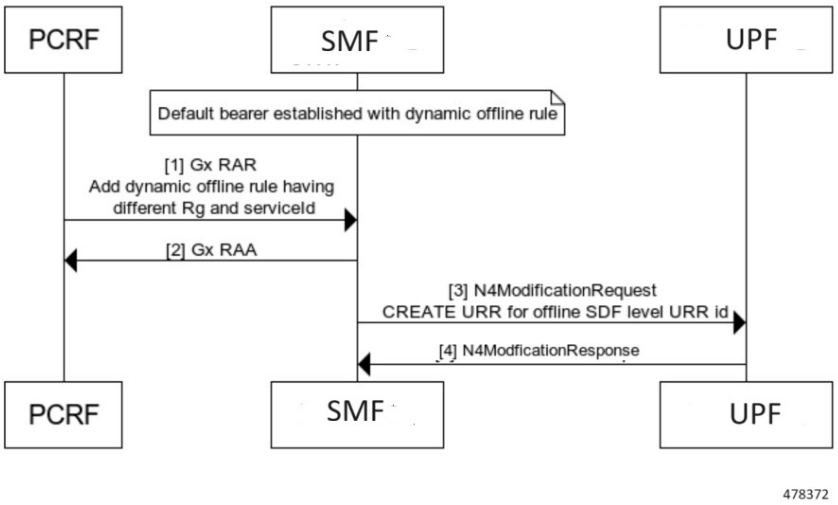



表 *248 :* デフォルトのベアラーにオフライン ルールを追加するコール フローの説明

| ステップ | 説明 |
|---|---|
| （注）<br>初期接続がダイナミック オフライン ルールで正常に完了したことを確認します。 | |
| 1 | PCRF は、Gx RAR を介して、異なる RG とサービス ID を持つ新しいダイナミック オフライン ルールを追加します。 |
| 2 | SMF は Gx RAA を PCRF に送信します。 |
| 3 | SMF は、オフライン SDF URR の CREATE_URR を含む N4 変更要求を UPF に送信します。そのためには、次の条件を満たす必要があります。<br>• PFCP_IE_URR_ID には一意のオフライン URR ID が必要です<br>• PFCP_IE_VOLUME_THRESHOLD および PFCP_IE_TIME_THRESHOLD には、GTPP プロファイルで構成された eG-CDR しきい値があるはずです。<br>• PFCP_IE_MEASUREMENT_METHOD には、ボリュームと期間の両方のビットが設定されています。<br>• PFCP_IE_REPORTING_TRIGGERS には *lisua* ビットが設定されています。<br>• ベアラー URR ID にリンクされています。 |
| 4 | UPF が N4 変更応答を送信します。 |

## 最初のダイナミック ルールの追加

図 ***153 :*** 最初の動的ルール追加のコール フロー

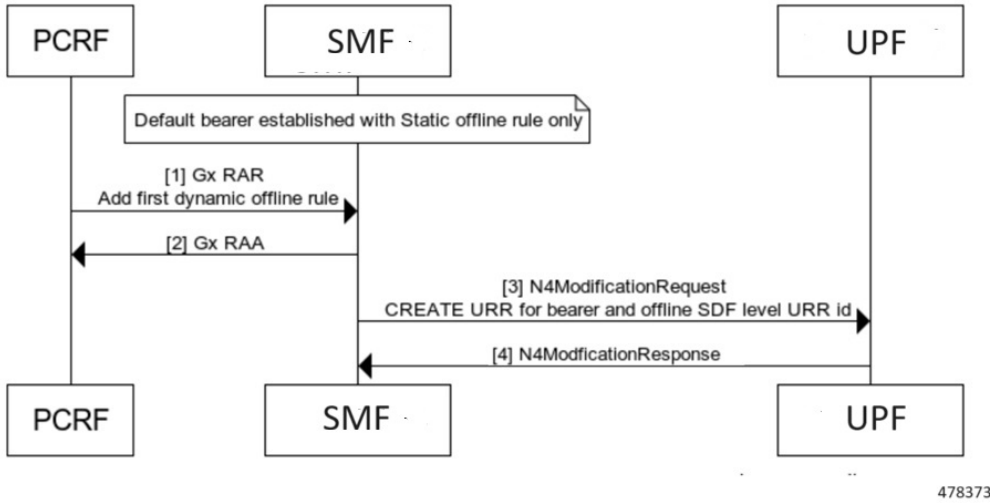



表 ***249 :*** 最初のダイナミック ルールを追加するためのコール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | 単一の静的オフライン ルールを持つデフォルトのベアラーで最初の接続が正常に完了したことを確認します。 |
| 2 | PCRF は、Gx RAR を介して最初のダイナミック オフライン ルールを追加します。 |
| 3 | SMF は Gx RAA を PCRF に送信します。 |

| ステップ | 説明 |
|---|---|
| 3 | SMF は N4 変更要求を UPF に送信します：<br>• デフォルトのベアラー レベル URR に対して CREATE_URR を設定します：<br>• デフォルトのベアラ レベル URR の PFCP_IE_URR_ID が 0x80000002 に設定されています。<br>• PFCP_IE_VOLUME_THRESHOLD および PFCP_IE_TIME_THRESHOLD には、ルールベース プロファイルで構成された eG-CDR しきい値があります。<br>• PFCP_IE_MEASUREMENT_METHOD には、ボリュームと期間の両方のビットが設定されています。<br>• オフライン SDF レベルの URR に対して CREATE_URR を使用します：<br>• PFCP_IE_URR_ID には一意のオフライン URR ID があります。<br>• PFCP_IE_VOLUME_THRESHOLD および PFCP_IE_TIME_THRESHOLD には、GTPP プロファイルで構成された egcdr しきい値があります。<br>• PFCP_IE_MEASUREMENT_METHOD には、ボリュームと期間の両方のビットが設定されています。<br>• PFCP_IE_REPORTING_TRIGGERS には *lisua* ビットが設定されています。<br>• ベアラー URR ID にリンクされています。 |
| 4 | UPF が N4 変更応答を送信します。 |

## 使用状況レポートの後の最初の動的ルールの追加

図 *154 :* 使用状況レポート後に最初の動的ルールを追加するためのコール フロー

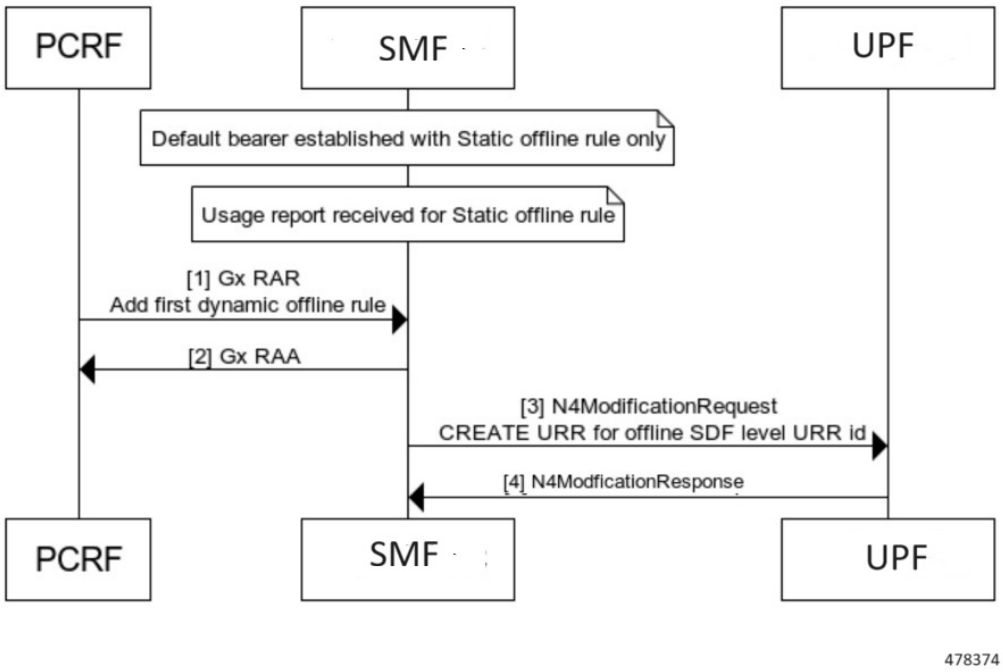



表 *250 :* 使用状況レポート後に最初のダイナミック ルールを追加するためのコール フローの説明

| ステップ | 説明 |
|---|---|
| 単一の静的オフライン ルールを持つデフォルトのベアラーを使用して、最初の接続が正常に完了したことを確認します。静的オフライン ルールの使用状況レポートが正常に処理されました。 | |
| 2 | PCRF は、Gx RAR を介して最初のダイナミック オフライン ルールを追加します。 |
| 3 | SMF は Gx RAA を PCRF に送信します。 |

| ステップ | 説明 |
|---|---|
| 3 | SMF は N4 変更要求を UPF に送信します：<br>• オフライン SDF レベルの URR に対して CREATE_URR を使用します：<br>• PFCP_IE_URR_ID には一意のオフライン URR ID があります。<br>• PFCP_IE_VOLUME_THRESHOLD および PFCP_IE_TIME_THRESHOLD には、GTPP プロファイルで構成された egcdr しきい値があります。<br>• PFCP_IE_MEASUREMENT_METHOD には、ボリュームと期間の両方のビットが設定されています。<br>• PFCP_IE_REPORTING_TRIGGERS には *lisua* ビットが設定されています。<br>• ベアラー URR ID にリンクされています。 |
| 4 | UPF が N4 変更応答を送信します。 |

デフォルト ベアラーからのルールの削除

次のコール フローと手順では、デフォルトのベアラーからのルールの削除について説明します。

**図 *155* : デフォルト ベアラーからのルールの削除のコール フロー**

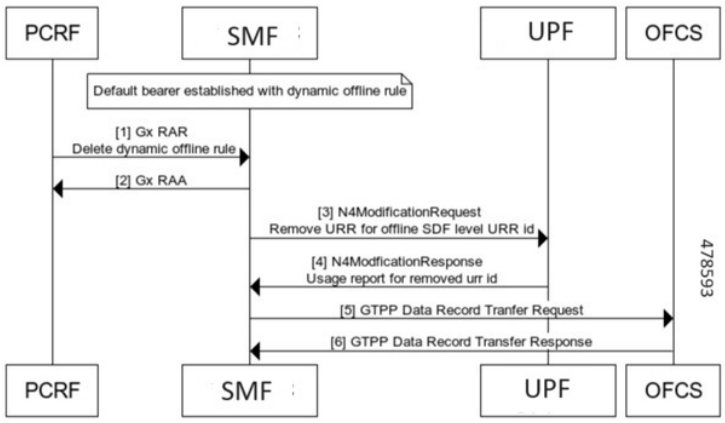


表 *251 :* デフォルトのベアラーからルールを削除するコール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | 初期接続がダイナミック オフライン ルールで正常に完了したことを確認します。 |
| 2 | PCRF は、Gx RAR を介してダイナミック オフライン ルールを削除します。 |
| 3 | CnPGW-C は Gx RAA を PCRF に送信します。 |
| 4 | オフライン SDF URR の REMOVE_URR を含む N4 変更要求は、CnPGW-U に送信されます。 |
| 5 | CnPGW-U は、次の N4 変更応答を送信します。<br>• 削除された URR の PFCP_IE_USAGE_REPORT_MOD_RES を受信しました。<br>• 「termr」が設定された PFCP_IE_USAGE_REPORT_MOD_RES |
| 6 | OFCS は、GTPP レコード転送応答を SMF に送信します。次に例を示します。<br>`Maxlosdvcontainer: 1.GTPP データ レコード転送要求は、削除された URR causeForRecClosing: 最大変更条件 serviceConditionChange:ServiceStop の単一のサービス レコードで送信されます` |

## QoS および APN-AMBR でのデフォルト ベアラーの変更

ここでは、デフォルト ベアラーの QoS および APN-AMBR の変更について説明します。

図 *156 :* オフライン ルール変更のみの *QoS/APN-AMBR* のコール フロー

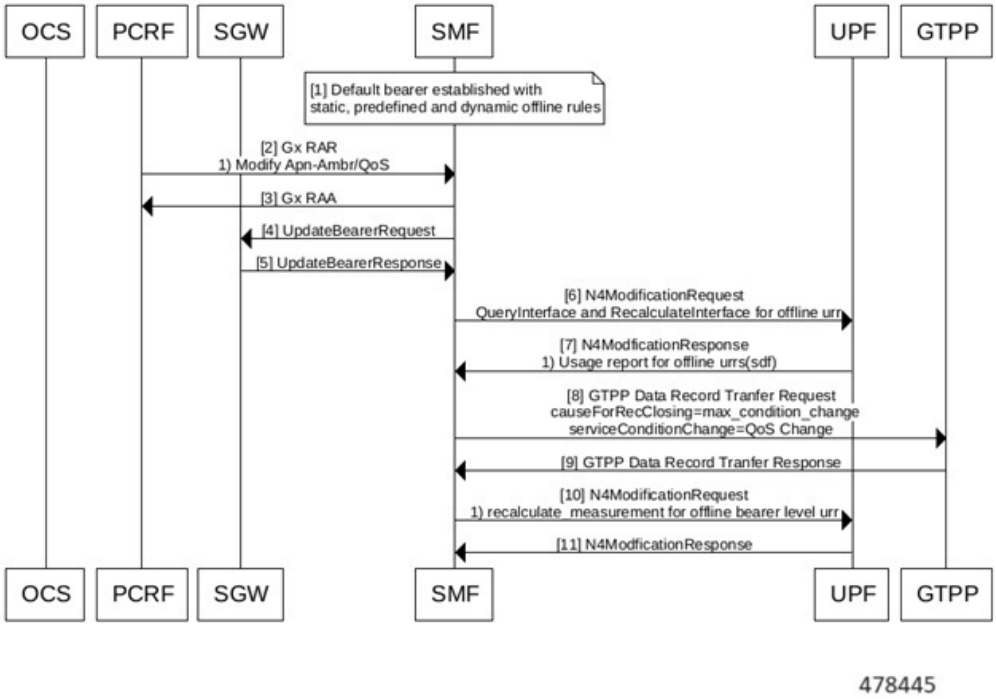



表 *252 :* オフライン ルールの変更のみによる *QoS/APN-AMBR* のコール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | ダイナミック、静的、および事前定義されたオフラインルールを使用して、デフォルトのベアラー接続を確立します。SMF には、CHANGE_IN_QOS、CHANGEINQOS_APN_AGGREGATE_MAXIMUM_BIT_RATE トリガーの構成が必要です。 |
| 2 | PCRF は Apn-Ambr または QoS の変更を伴う GxReAuthRequest を送信します。たとえば、変更要求は次のデバイスに送信できます：<br>• デフォルト ベアラー QoS（QCI、ARP）<br>• Apn-Ambr（アップリンクまたはダウンリンク） |
| 3 | SMF は PCRF に GxReAuthAnswer を送信します。 |
| 4 | SMF は、S-GWにベアラー要求を送信します。 |
| 5 | S-GW は、SMF にベアラー応答の更新を送信します。 |

| ステップ | 説明 |
|---|---|
| 6 | UPF は、SMF から次の N4 変更要求を受信します。<br>• SDF URR に offline_urr が設定された QueryInterface<br>• SDF URR に offline_urr が設定されたインターフェイスを再計算する |
| 7 | SMF は UPF から N4Modification 応答を受信します。たとえば、SMF は SDF URR の UsageReport 応答を受信します。 |
| 8 | SMF は、Maxlosdvcontainer が構成された制限ヒットがある場合にのみ、GTPP データ レコード転送要求を送信します。 |
| 9 | SMF が GTPP データ レコード転送応答を受信します。 |
| 10 | SMF は、オフラインのベアラー レベル URR の Recalculate_measurement を含む N4 変更要求を UPF に送信します。 |
| 11 | UPF が SMF に N4 変更応答を送信します。 |

図 *157* : オフラインおよびオンラインでのルール変更のコール フロー

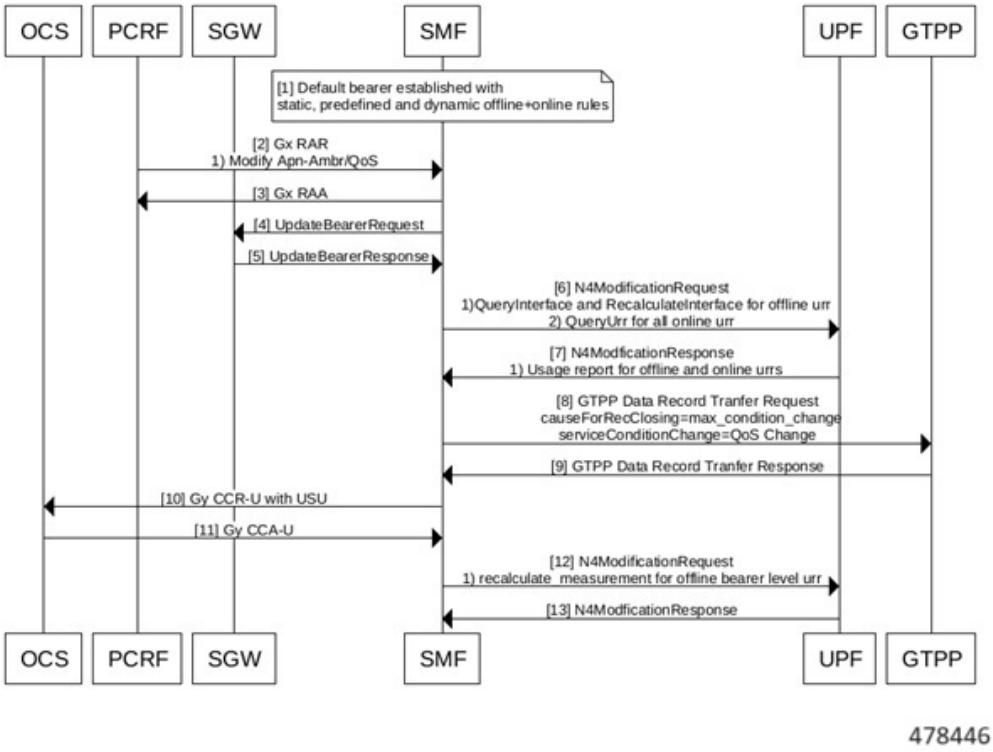



表 *253* : オフライン ルールとオンライン ルールが変更された *QoS/APN-AMBR* のコール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | 次のダイナミック、スタティック、および事前定義されたオフライン ルールを使用して、デフォルトのベアラー接続を確立します。<br>• オンライン ルールの CHANGE_IN_QOS、CHANGEINQOS_APN_AGGREGATE_MAXIMUM_BIT_RATE などの OCS アームの Gy-trigger。<br>• SMF には CHANGEINQOS_APN_AGGREGATE_MAXIMUM_BIT_RATE トリガ構成が必要です |
| 2 | PCRF は APN-AMBR または QoS の変更を伴う GxReAuthRequest を送信します。たとえば、変更要求は次のデバイスに送信できます。<br>• デフォルト ベアラー QoS（QCI、ARP）<br>• Apn-Ambr（アップリンクまたはダウンリンク） |

| ステップ | 説明 |
|---|---|
| 3 | SMF は PCRF に GxReAuthAnswer を送信します。 |
| 4 | SMF は、S-GWにベアラー要求を送信します。 |
| 5 | S-GW は、SMF にベアラー応答の更新を送信します。 |
| 6 | UPF は、SMF から次の N4 変更要求を受信します。<br>• SDF URR に offline_urr が設定された QueryInterface<br>• SDF URR に offline_urr が設定されたインターフェイスを再計算する |
| 7 | SMF は UPF から N4Modification 応答を受信します。たとえば、SMF は SDF URR の UsageReport 応答を受信します。 |
| 8 | SMF は、Maxlosdvcontainer が構成された制限ヒットがある場合にのみ、GTPP データ レコード転送要求を送信します。 |
| 9 | SMF が GTPP データ レコード転送応答を受信します。 |
| 10 | SMF は、USU の UPF から受信した使用状況とともに Gy CCR-U を OCS に送信します。次に例を示します。<br>`QoS Change  => Reporting-Reason with RATING_CONDITION_CHANGE (6), Trigger - CHANGEINQOS_ANY (2).`<br>`Apn-Ambr Change => Reporting-Reason with RATING_CONDITION_CHANGE (6), Trigger - CHANGEINQOS_APN_AGGREGATE_MAXIMUM_BIT_RATE (24).` |
| 11 | SMF は、OCS から Gy CCA-U を受信します。 |
| 12 | SMF は、オフライン ベアラー レベルの URR の Recalculate_measurement を含む N4 変更要求を UPF に送信します。 |
| 13 | UPF が SMF に N4 変更応答を送信します。 |

CDR で送信された QoS

すべての QoS 情報は、SDF コンテナレベルでのみ送信されます。APN-AMBR 値は、maxRequestedBandwithUL または maxRequestedBandwithDL CDR SDF コンテナで **ゼロ** として送信されます。

| **PreCondition** | シナリオ | 予想される動作 |
|---|---|---|

| | | |
|---|---|---|
| Maxlosdv 1<br>**Gx** による接続<br>SDF しきい値 60 秒（Bearer threshold 60 seconds）<br>**QoS** トリガー の有効化 | Gx で接続（QoS 情報 - **QoS1**）<br>時間しきい値で SDF 使用率を受信しました<br>QoS 変更のための Gx RAR：**QoS2**<br>時間しきい値でベアラー使用率を受信しました<br>QoS 変更のための Gx RAR：**QoS3**<br>時間しきい値でベアラー使用率を受信しました<br>切断 | N4 クエリで QoS 情報の変更が発生すると、オフラインに対して **オフライン** ビットが設定されます。<br>1st SDF 使用量を受信した後、CDR SDF コンテナは、**QoS1**で送信されます。<br>**1st RAR** の SDF 使用量を受信した後、CDR SDF コンテナは、**QoS1** で送信されます。<br>2nd SDF 使用量を受信した後、CDR SDF コンテナは、**QoS2**で送信されます。<br>**2nd RAR** の SDF 使用量を受信した後、CDR SDF コンテナは、**QoS2** で送信されます。<br>3 番目の SDF の使用量を受信した後、CDR SDF コンテナが **QoS3**で送信される<br>切断中に使用状況レポートを終了する場合、CDR SDF コンテナが **QoS3** で送信されます。 |
| Maxlosdv 1<br>**Gx なしで**接続<br>ベアラーしきい値 60 秒（Bearer threshold 60 seconds）<br>**QoS** トリガー の有効化 | **Gx なしで接続（デフォルトの QoS ルール**）<br>時間しきい値でベアラー使用率を受信しました<br>音量しきい値でベアラー使用率を受信しました<br>切断 | すべての CDR SDF コンテナが、接続時間の **デフォルト** ルール QoS 情報とともに送信されます。 |

| | | |
|---|---|---|
| Maxlosdv 1<br>**Gx** による接続<br>SDF しきい値 60 秒（Bearer threshold 60 seconds）<br>**QoS** トリガー **の無効化** | Gx で接続（QoS 情報 - **QoS1**）<br>時間しきい値でベアラー使用率を受信しました<br>QoS 変更のための Gx RAR：**QoS2**<br>時間しきい値でベアラー使用率を受信しました<br>QoS 変更のための Gx RAR：**QoS3**<br>時間しきい値でベアラー使用率を受信しました<br>切断 | オフラインの場合 QoS 情報の N4 クエリ上で変更は、発生しません。<br>すべての CDR SDF コンテナが接続時間 QoS 情報（**QoS1**）とともに送信されます。 |
| Maxlosdv 1<br>**Gx なしで**接続<br>ベアラーしきい値 60 秒（Bearer threshold 60 seconds）<br>**QoS** トリガー **の無効化** | **Gx なしで接続（デフォルトの QoS ルール**）<br>時間しきい値でベアラー使用率を受信しました<br>音量しきい値でベアラー使用率を受信しました<br>切断 | すべての CDR および SDF コンテナが、接続時間 **のデフォルトの** ルール QoS 情報とともに送信されます。 |

ルールベースの変更

次のコール フローと手順では、ルール ベースの変更について説明します。

図 *158 :* ルールベースの変更のコール フロー

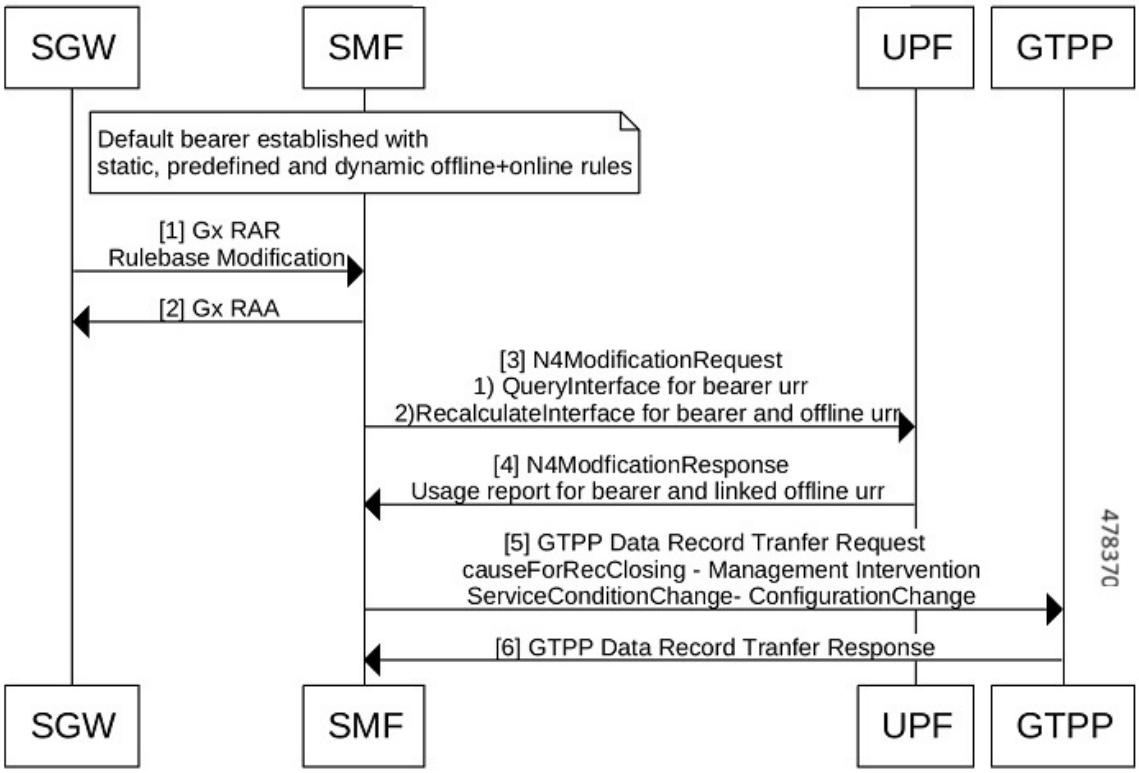



表 *254 :* ルールベースの変更を伴うコール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | 初期接続が、静的、事前定義、およびダイナミック ルールで正常に完了したことを確認します。 |
| 2 | S-GW は、Gx RAR を介して SMF にルールベースを変更します。 |
| 3 | SMF は Gx RAA を S-GW に送信します。 |
| 4 | SMF は以下の N4 変更要求を UPF に次のように送信します：<br>• 新しいルールベースの PDR を作成する<br>• 古いルールベースと事前定義されたルールの PDR の削除<br>• bearer_urr ビット設定を持つでのクエリ インターフェイス<br>• Bearer_urr と offline_urr ビットが設定されたインターフェイスを再計算します |

| ステップ | 説明 |
|---|---|
| 5 | UPF が SMF に以下の N4 変更応答を送信します。<br>• 「ima」フラグが設定されたベアラー レベル URR の PFCP_IE_USAGE_REPORT_MOD_RES<br>• 「liusa」フラグが設定されたすべての SDF オフライン URR の PFCP_IE_USAGE_REPORT_MOD_RES |
| 6 | SMF は、GTPP データ レコード転送要求を SMF に送信します。<br>たとえば、GTPP データ レコード転送要求は ForRecClosing: Management Intervention serviceConditionChange:Configuration change とともに送信されます。 |
| 7 | GTPP は、SMF に GTPP データ レコード転送応答を受信したことを確認します。 |

（注） 請求レコードがルールベースの変更によって変更されると、少なくとも1つのオフラインルール（ダイナミック、スタティック、またはアクティブ化された事前定義済みルール）が現在インストールされている場合、ベアラー URR が照会されます。次に例を示します。

- 課金レコードを無効にして、オフラインルールが存在しない状態で接続が終了した場合。ルールベースの変更によって請求レコードが変更されて有効になると、システムにオフライン ルールが存在していないため、ベアラー URL はクエリされません。
- 新しいルールベースで EGCDR 課金レコードが無効になっている場合、既存のダイナミック オフライン ルールは削除されず、同じルールの使用状況レポートが続行されます。ただし、新しいオフライン ルールが追加されると、同じものに対してオフライン URR は作成されず、課金記録の無効化により検証失敗としてマークされます。

# セカンダリ RAT の使用状況に関する定期レポートの処理

表 *255 :* 機能の履歴

| 機能名 | リリース情報 | 説明 |
|---|---|---|
| セカンダリ RATの使用状況の定期レポート | 2023.04 | この機能により、SMF は、ベアラー要求の変更、通知要求、セッションの削除要求、およびベアラー応答の削除で、S5 または S8 インターフェイスを介して MME から定期的に送信されるセカンダリ RAT データ ボリューム レポート メッセージを処理できます。<br>**デフォルト設定** 無効：有効にするには構成が必要です。 |

## 機能説明

SMF と UPF は、eNB の通信量を追跡して、NSA デバイスの NR 通信量と LTE 通信量を区別します。SMF は、S5 インターフェイスに関するさまざまなメッセージで使用状況データ レポートを受信し、オフラインの使用状況レポートとともに OFCS サーバーに対する使用状況を報告します。

SMF は、Intended Receiver PGW-C（IPGW）フラグに基づいて、ベアラー要求の変更、通知要求、セッションの削除要求、およびベアラー応答の削除の S5 または S8 インターフェイスを介して MME から定期的に送信されるセカンダリ RAT データ ボリューム レポート メッセージを処理します。 SMF は、IRGW = 1 の場合に使用状況レポートを保持します。

SMF は、Secondary RAT Usage Data レポート IE の複数のインスタンスをサポートしています。トリガーに基づいて OFCS に送信されるまで、レポートを保存します。SMF は、課金トリガーのいずれかが満たされると、保存されているセカンダリ RAT 使用量データ レポートを gtpp-ep エンドポイントを介して送信します。課金プロファイルで、保存されるセカンダリ RAT 使用レポートの最大数を構成できます。SMF は、オフライン使用状況レポートが原因で CDR が閉じられた場合、保存されているセカンダリ RAT 使用状況データ レポートをオフライン使用状況レポートとともに送信します。

## 機能の仕組み

次の図は、定期的なセカンダリ RAT 使用状況レポートのコール フローを示しています。

図 *159* : 定期的なセカンダリ *RAT* の使用におけるコール フロー

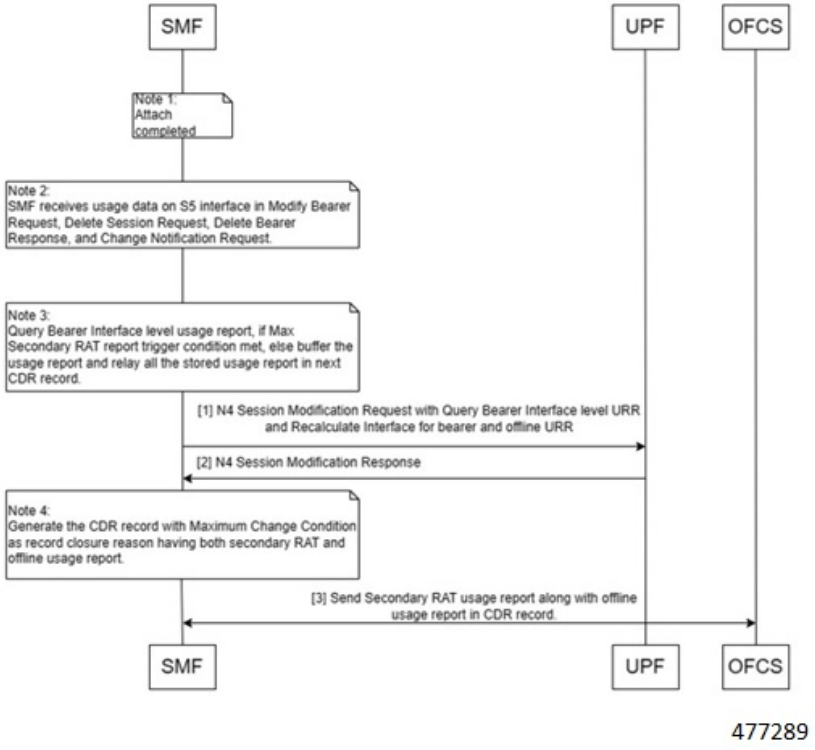



表 *256* : 定期的なセカンダリ *RAT* の使用におけるコール フローの説明

| ステップ | 説明 |
|---|---|
| （注）<br>次の条件が満たされていることを確認します。<br>• 接続手順が完了しました。<br>• SMF は、Modify-Bearer-Request、Delete-Session-Request、Delete-Bearer-Response、および Change-Notification-Request において S5 インターフェイスで使用状況データを受信します。詳細については、CDR の出力例 （765 ページ） を参照してください。<br>• Max Secondary RAT レポート トリガ条件が満たされた場合に、クエリベアラー インターフェイス レベルの使用状況レポートを処理します。そうでない場合、 は通信量レポートをバッファし、保存されているすべての通信量レポートを次の CDR レコードに中継します。 | |

| ステップ | 説明 |
|---|---|
| 1 | SMF はクエリのベアラー インターフェイス レベルの URR を使用して N4 セッション変更要求を送信し、ベアラーとオフライン URR のインターフェイスを再計算します。<br>次のパラメータが送信されます。<br>• ベアラー URR に **bearer_urr** が設定されたクエリ インターフェイス次に例を示します。<br>`PFCP_IE_QUERY_INTERFACE (253)`<br>`'query_interface' : {'spare_3bit': 0, 'offline_urr': 0, 'online_urr': 0, 'radius_urr': 0, 'bearer_urr': 1, 'sess_urr': 0}`<br>• **offline_urr** と **bearer_urr** との再計算インターフェイスが SDF URR に設定されています。<br>`PFCP_IE_RECALCULATE_INTERFACE (264)`<br>`'recalculate_interface' : {'spare_3bit': 0, 'offline_urr': 1, 'online_urr': 0, 'radius_urr': 0, 'bearer_urr': 1, 'sess_urr': 0}` |
| 2 | UPFは、ベアラーおよび関連する SDF 使用レポートと共に、N4 セッション変更応答を送信します。 |
| 3 | CDR レコード終了理由 （764 ページ） として最大変更条件を使用し、セカンダリ RAT とオフライン使用状況レポートの両方が含まれる CDR レコードを生成します。 |
| 4 | SMF は、オフライン使用状況レポートで OFCS に CDR レコードを送信します。 |

## *CDR* レコード終了理由

次の表では、セカンダリ レートの使用量のさまざまな使用例における CDR レコードの終了理由とサービス条件の理由について説明しています。

**表 *257 : CDR* レコード終了理由**

| トリガータイプ | セカンダリ RAT 制限ヒット | N4 でのクエリ | SDF 終了理由 | レコード終了理由 | メトリックの増加 |
|---|---|---|---|---|---|
| SDF レベル クエリ<br>例：URI 変更トリガー | TRUE | ベアラー レベル クエリ<br>例：URI 変更のトリガー理由 | トリガー理由 | 状態の最大変更 | ○ |

| トリガータイプ | セカンダリ RAT 制限ヒット | N4 でのクエリ | SDF 終了理由 | レコード終了理由 | メトリックの増加 |
|---|---|---|---|---|---|
| ベアラー レベル クエリ<br>例：タイムゾーン トリガー | TRUE | ベアラー レベル クエリ | トリガー理由<br>例：タイムゾーン トリガーの理由 | トリガー理由<br>例：タイムゾーン トリガーの理由 | 非対応 |
| トリガー ヒットなし | TRUE | ベアラー レベル クエリ | サービス固有のユニット制限 | 状態の最大変更 | はい |

## セカンダリ RAT 使用状況制限の構成

OFCS に送信する前に、次の構成例を使用して、セカンダリ RAT 使用状況レポートを構成します。

```
config
  profile charging profile_name
    max-secondary-rat-reports report_range
    exit
```

注：

- **profile charging** *profile_name*：課金プロファイル コンフィギュレーション モードを開始します。
- **max-secondary-rat-reports** *report_range*：GTPP（Gz）更新をトリガするセカンダリ RAT 使用率レポートの最大数を構成します。 *report_range* は 、0 ～ 50 の範囲の整数である必要があります。 **max-secondary-rat-reports** のセカンダリ RAT 使用制限の推奨値は 25 です。

（注） 累積セカンダリ RAT 使用量が構成された制限を超えると、制限を超えたセカンダリ RAT 使用量の数が 1 回の使用にまとめられます。

### *CDR* の出力例

次に、変更通知要求の [セカンダリ RAT データ使用量（Secondary RAT Data Usage）] の出力例を示します。

```
CHANGE NOTIFICATION REQUEST" (38)
'Teid'             : 0x4
'Length'           : 86
'Sequence Number'  : 3
'Number of IEs'    : 6
    "GTPV2_IE_IMSI" (1)
          'Length' : 8
            'inst' : 0
            'imsi' : 123456789012345

       IE BUFFER:
                0100 0800 2143 6587 0921 43F5
    "GTPV2_IE_RAT_TYPE" (82)
          'Length' : 1
            'inst' : 0
        'rat_type' : E-Utran (6)
       IE BUFFER:
                5200 0100 06
    "GTPV2_IE_ULI" (86)
          'Length' : 13
            'inst' : 0
             'uli' : {'spare': 0, 'lai': 0, 'ecgi': 1, 'tai': 1, 'rai': 0, 'sai': 0,
'cgi': 0, 'tai-mcc': 123, 'tai-mnc': 456, 'tai-tac': 2346, 'ecgi-mcc': 123, 'ecgi-mnc':
 456, 'ecgi-spare': 0, 'ecgi-eci': 1234567}
       IE BUFFER:
                5600 0D00 1821 6354 092A 2163 5400 12D6
                87
    "GTPV2_IE_PGW_S5/8_GTPC_IP_ADDR" (74)
          'Length' : 4
            'inst' : 0
      'ip_address' : 10.11.12.13
       IE BUFFER:
                4A00 0400 0A0B 0C0D
    "GTPV2_IE_LBI" (73)
          'Length' : 1
            'inst' : 0
           'spare' : 0
          'eps_id' : 5
       IE BUFFER:
                4900 0100 05
    "GTPV2_IE_SECONDARY_RAT_USAGE_DATA_REPORT" (201)
          'Length' : 27
            'inst' : 0
    'secondary_rat_usage_data_report' : {'irsgw': 0, 'irpgw': 1, 'sec_rat_type': 0,
'ebi': 5, 'start_timestamp': 3890790208, 'end_timestamp': 3890790218, 'usage_data_dl':
100, 'usage_data_ul': 100}
       IE BUFFER:
                C900 1B00 0100 05E7 E8BF 40E7 E8BF 4A00
                0000 0000 0000 6400 0000 0000 0000 64
        MESSAGE BUFFER:
                4826 0056 0000 0004 0000 0300 0100 0800
                2143 6587 0921 43F5 5200 0100 0656 000D
                0018 2163 5409 2A21 6354 0012 D687 4A00
                0400 0A0B 0C0D 4900 0100 05C9 001B 0001
                0005 E7E8 BF40 E7E8 BF4A 0000 0000 0000
                0064 0000 0000 0000 0064
```

次に、セカンダリ RAT 使用量を含む GTPP レコードの出力例を示します。

```
CDR ELEMENTS FOLLOW
  recordType                          PGWRECORD
  servedIMSI                          123456789012345
  p_GWAddress                         10.0.2.15
```

```
  chargingID                          4
  servingNodeAddress                  10.105.34.80
  accessPointNameNI                   intershat
  pdpPDNType                          IPV4
  servedPDPPDNAddress                 1.1.4.3
  dynamicAddressFlag                  TRUE
  recordOpeningTime                   230608091158+0000
  duration                            2
  causeForRecClosing                  Maximum Change Condition
  recordSequenceNumber                1
  nodeID                              1000acs1
  localSequenceNumber                 7
  apnSelectionMode                    MS Provided Subscription Not Verified
  servedMSISDN                        223310101010101
  chargingCharacteristics             Flat (0x1234)
  chChSelectionMode                   SGSN Supplied
  servingNodePLMNIdentifier           121, 100
  rATType                             eUTRAN
  mSTimeZone                          +04:30 - Daylight savings +2
  userLocationInformation
    Location Type                   TAI
    MCC                               123
    MNC                               456
    TAC                               0x92A
    Location Type                   ECGI
    MCC                               123
    MNC                               456
    ECI                               0x012D687

    ratingGroup                         10
    chargingRuleBaseName                RULE-BASE-1
    localSequenceNumber                 1
    timeUsage                           70
    serviceConditionChange              Service specific Unit Limit
     qCI                                 5
     maxRequestedBandwithUL              0
     maxRequestedBandwithDL              0
     guaranteedBitrateUL                 0
     guaranteedBitrateDL                 0
     aRP                                 8
    servingNodeAddress                  10.105.34.80
    datavolumeFBCUplink                 1001
    datavolumeFBCDownlink               1001
    timeOfReport                        230608091200+0000
    userLocationInformation
      Location Type                   TAI
      MCC                               123
      MNC                               456
      TAC                               0x92A
      Location Type                   ECGI
      MCC                               123
      MNC                               456
      ECI                               0x012D687

  servingNodeType                     GTPSGW
  subscriptionIDType                  3
  subscriptionIDData
0123456789012345@nai.epc.mnc456.mcc123.3gppnetwork.org
  p_GWPLMNIdentifier                  123, 456
  startTime                           230608091158+0000
  pDNConnectionID                     4

 listOfRANSecondaryRATUsageReports
```

```
RANSecondaryRATUsageReport
 dataVolumeUplink                    100
 dataVolumeDownlink                  100
 rANStartTime                        230418070328+0000
 rANEndTime                          230418070338+0000
 secondaryRATType                    New Radio 5G

RANSecondaryRATUsageReport
 dataVolumeUplink                    400
 dataVolumeDownlink                  500
 rANStartTime                        230418070455+0000
 rANEndTime                          230418070615+0000
 secondaryRATType                    New Radio 5G
```

## DCNR の構成

SMF が DNN プロファイルを使用して処理されるセッションの DCNR 機能をサポートできるようにするには、次の構成例を使用します：

```
config
   profile dnn profile_name  intershat dcnr
      dcnr { false | true }
      exit
```

注：

- **profile dnn** *profile_name*：DNN プロファイル名を指定します。 *profile_name* は 英数字の文字列である必要があります。
- **intershat dcnr**：新しい無線とのデュアル接続のサポートを有効にします。

（注） DCNR 構成が有効になっており、UE のセッション作成要求に「UP プレーン インジケータ IE」がある場合、セカンダリ RAT 使用レポートの処理が実行されます。

- **dcnr { false | true }**:
  - **false**：DCNR フラグが false に設定されるように DNN プロファイルを構成します。デフォルトでは、この DCNR 構成は無効になっています。
  - **true**：DCNR フラグが true に設定されるように DNN プロファイルを構成します。

    この構成により、SMF が DCNR 機能をサポートできるようになります。DCNR 機能が有効になっている場合、UE は DCNR フラグを送信してデュアル接続をサポートしていることを示します。

# EGCDR 最終レコード終了原因のサポート

表 *258 :* 機能の履歴

| 機能名 | リリース情報 | 説明 |
|---|---|---|
| EGCDR最終レコード終了原因 | 2023.04 | この機能を使用すると、CLI構成を介して最終CDRの一意のレコード終了理由を送信できます。 |

## 機能説明

デフォルトでは、サブスクライバ セッションの終了に対して複数の CDR が生成された場合、すべての CDR でレコード クロージャの原因が同じになります。

SMF は、CLI オプションの closing-cause を介して、最終的な CDR でレコードが閉じられる原因を制御します。サブスクライバ セッションの終了時に複数の CDR が生成された場合、最終的な CDR レコード クロージャ理由は NormalRelease に設定され、他のすべての CDR レコード クロージャ理由は MaxChangeConditionに設定されます。

最終レコード クローズの構成

次のコマンドを使用して、final-record closing-cause を構成します。

```
config
   active-charging service service_name
      charging-action charging_action
        egcdr-final-record
           closing-cause [ same-in-all-partials | unique ]
  end
```

注：

- **egcdr-final-record** ：最終 CDR を構成します。
- **closing-cause** ：最終 CDR の場合の終了原因を構成します。
  - **same-in-all-partials** ：値は、同じ終了原因が複数の最終CDRに含まれることを指定します。
  - **unique**：値は、最終 CDR の終了原因が一意であることを指定します。

# ゼロ ボリュームで CDR を抑制

表 *259 :* 機能の履歴

| 機能名 | リリース情報 | 説明 |
|---|---|---|
| Gzインターフェイスでのゼロ CDR 抑制のサポート | 2023.04 | この機能により、 **egcdr suppress-cdrs zero-volume** CLI に基づいてCDR レコードを抑制できます。 |

## 機能説明

次のシナリオで CDR レコードを抑制できます :

- CLI 構成に基づいてボリューム使用率がない場合
- CDR のボリュームがゼロで、構成されたトリガーと一致している場合。
- CDR のボリュームがゼロで、構成されたトリガーと一致しない場合。 egcdr suppress-cdrs zero-volume CLI が構成されていない場合、SDF コンテナのない CDR が送信されます。

（注） UPF からのセッション使用状況レポートにボリュームがゼロの SDF レベルの使用状況が含まれている場合、SDF コンテナはデフォルトで抑制されます。

egcdr suppress-cdrs zero-volume CLI は、通話終了の使用状況レポートまたはベアラー レベルの使用例にのみ適用されます。たとえば、コールがゼロ ボリューム レポートで終了した場合、またはボリュームがゼロのベアラー レベルの同期または非同期使用レポートがある場合、CDR が送信されるかどうかは CLI 構成に基づいて決定されます。

## ゼロ抑制 CDR の構成

CDR がボリューム使用状況を報告しない場合に CDR レコードを抑制するには、次の CLI 構成を使用します。

```
config
   active-charging service service_name
      charging-action charging_action
       egcdr suppress-cdrs zero-volume   triggers [ internal-trigger-cdr
 |  final-cdr | external-trigger-cdr ]
  end
```

注 :

- **egcdr suppress-cdrs zero-volume** ：CDR を抑制
- **triggers** ：ゼロ ボリュームで CDR を抑制するために使用できるトリガーのリストの 1 つを構成します。

- **egcdr suppress-cdrs zero-volume trigger internal-trigger-cdr** ：非同期ボリューム使用率レポートが PFCP セッション使用状況レポートを介して UPF から取得されるように指定します。
- **egcdr suppress-cdrs zero-volume trigger final-cdr** ：通話が終了することを指定します。
- **egcdr suppress-cdrs zero-volume trigger external-trigger-cdr** ：同期ボリュームの使用状況レポートがクエリ URR を介して UPF から取得されることを指定します。

# N1/NAS インターフェイス

N1 インターフェイスは、ユーザー機器（UE）とアクセスおよびモビリティ管理機能（AMF）間の基準ポイントです。このインターフェイスは、接続、モビリティ、およびセッションに関連する UE 情報を AMF に転送するために使用されます。

セッション管理のために、PDU セッションは UE の要求時に確立され、UE と 5GC の要求で変更され、UE と 5GC の要求で NAS SM シグナリングを介して解放されます。このシグナリングは、UE と SMF 間の N1 インターフェイスを介して交換されます。

## 無効なプロトコル データの処理に対する NAS メッセージのコンプライアンス

### 機能説明

SMF は、このリリースの 3GPP TS 24.501 に定義されているように、無効なプロトコル データ処理に準拠する NAS メッセージです。

### 機能の仕組み

無効なプロトコル データ処理機能に準拠する NAS メッセージの動作は次のとおりです。

- SMF は、完全なメッセージ タイプ情報要素（IE）を含むには短すぎる NAS メッセージを無視します。
- SMF は、3GPP 仕様で定義されている最大制限よりも長い NAS メッセージを無視します。
- SMF は NAS メッセージ内の不明な IE を無視します。
- SMF は、NAS メッセージ内のシーケンスが正しくない IE を無視します。
- T、TV、TLV、または TLV-E フォーマットの情報要素が、IE の繰り返しが指定されていないメッセージ内で繰り返される場合、SMF は、最初に表示される情報要素の内容だけを処理します。さらに、SMF は後続の情報要素の繰り返しを無視します。
- SMF は、メッセージの構文が正しくないオプションの IE を使用できないメッセージと見なします。
- ネットワークは次のメッセージのいずれも無視し、原因 #100 「条件付き IE エラー」のステータス メッセージを返します。
  - SMF が NAS メッセージを受信し、条件付き IE エラーが欠落している場合

- SMF が予期しない条件付き IE エラーを受信した場合
- SMF が、少なくとも 1 つの構文的に正しくない条件付き IE を含むメッセージを受信した場合

## *NAS* メッセージ コンプライアンスと無効なプロトコル データの処理

SMF は、無効なプロトコル データ処理機能への NAS メッセージの準拠の次の 3GPP の仕様のセクションに準拠します：

### 短すぎるメッセージ

SMF は、サイズが最小制限を満たしていないサイズの NAS メッセージを破棄します。

次の表に、SMF が UE から受信する NAS メッセージの最小制限を示します。

**表 *260 : NAS* メッセージの最小制限**

| 番号 | NAS メッセージ | 最小制限 |
|---|---|---|
| 1 | PDU セッション確立リクエスト | 6 オクテット |
| 2 | PDU セッション認証の完了 | 4 オクテット |
| 3 | PDU セッション変更要求 | 4 オクテット |
| 4 | PDU セッション変更要求 | 4 オクテット |
| 5 | PDU セッション変更コマンド拒否 | 5 オクテット |
| 6 | PDU セッション解放要求 | 4 オクテット |
| 7 | PDU セッションの解放 | 4 オクテット |

### メッセージが長すぎます

SMF は、サイズが上限を満たさない NAS メッセージを破棄します。

5G コアネットワークに接続されている NR の NAS メッセージの最大サイズは 9000 バイトです。

### 不明な IE

SMF は NAS メッセージ内の不明な IE を無視します。

（注） SMF は、特定の NAS メッセージ タイプに関連する IE のみを処理します。SMF は、メッセージ タイプに対して不明な別の IE を無視します。

#### シーケンス外のIE

SMF は、NAS メッセージ内で必須 IE の正しくないシーケンスを持つ IE を無視します。

#### 反復的な IE

SMF は、IE の繰り返しに関する情報がない NAS メッセージで IE を複数回受信することがあります。このような場合、SMF は繰り返される IE の最初の発生だけを考慮し、その後の IE のその後の発生はすべて無視します。

#### 構文的に正しくない IE

SMF は NAS メッセージの構文的に不正なオプションの IE を無視します。

#### 欠落または予期しない条件付きIE

SMF は、次の条件付き IE エラーを含む受信済み NAS メッセージを無視します。

- 予期される条件付き IE がありません
- 予期しない条件付き IE
- 構文的に正しくない条件付き IE

標準準拠

無効なプロトコル データ処理機能への NAS メッセージの準拠は、次の基準に準拠します。

- *3GPP TS 24.501 – 5G 5G* システム（*5GS*）用の *Non-Access-Stratum*（*NAS*）プロトコル第*3*段階
- *3GPP TS 38.323 – 5G NR* パケット データ コンバージェンス プロトコル（*PDCP*）

## 5GSM 原因コードの処理

### 機能説明

SMF または vSMF では、UE によって開始された手順とネットワークによって開始された手順の 5G セッション管理（5GSM）の原因処理をサポートしています。

サポートされている手順は次のとおりです。

- PDU セッション確立
- PDU セッション変更
- PDU セッションの解放

## *PDU* セッション確立拒否原因値

要求されたデータ ネットワーク（DN）との接続がネットワークによって拒否された場合、SMF は、PDU セッション確立拒否メッセージの 5GSM 原因 IE を設定して、PDU セッション確立手順を拒否する理由を示します。

次の表では、PDU セッション確立拒否メッセージでサポートされている 5GSM の原因について説明します。

**表 *261 : 5GSM* の原因：*PDU* セッション確立拒否**

| **5GSM 拒否の原因** | **SMF の動作（SMF Behavior）** |
|---|---|
| 原因 #26：リソース不足 | SMF では、次の N2 の原因のいずれかとともに、「PDU_RES_SETUP_FAIL」と共に N2SmInfoType を受信すると、この原因が含まれます。<br>• RadioNetwork/Radio_resources_not_available<br>• RadioNetwork/Failure_in_the_radio_interface_procedure<br>• Misc/Not_enough_user_plane_processing_resources |
| 原因 #27：DNN の欠落または不明 | DNN が必須であり、SMF で構成されていないために、SmContextCreateData で DNN が使用できない場合、SMF にはこの原因が含まれます。 |
| 原因 #28：不明な PDU セッション タイプ | SMF では、PDU セッション確立要求メッセージに SMF でサポートされていない PDU セッション タイプが含まれている場合に、この原因が含まれます。 |
| 原因 #29：ユーザー認証または承認の失敗 | SMF には、UE の DNN 認証が失敗した（RADIUS 認証のタイムアウト）ときに、この原因が含まれます。 |
| 原因 #32：サービス オプションがサポートされていない | SMF では、受信した S-NSSAI の検証が S-NSSAI の許可リストと照合して失敗した場合に、この原因が使用されます。 |
| 原因 #33：リクエスト済みのサービス オプションがサブスクライブされていない | SMF には、UE がサブスクリプションのないサービス オプションを要求した場合に、この原因が含まれます。 |
| 原因 #38：ネットワーク障害 | ネットワークのエラーが原因で要求されたサービスが拒否された場合、SMF にはこの原因が表示されます。これには、内部障害、または PDN セットアップ手順中の外部 NF からの応答がないことが含まれます。 |

| 5GSM 拒否の原因 | SMF の動作（SMF Behavior） |
|---|---|
| 原因 #54：PDU セッションが存在しません | SMF には、3GPP アクセスと非 3GPP アクセス間、または EPS から 5GS への転送を UE によって要求された PDUセッションに関する情報がない場合、この原因が含まれます。 |
| 原因 #70：スライス内の DNN が欠落しているか、または不明である | SMF には、スライス構成は存在するものの、要求された DNN が SMF のスライスで構成されていない場合に、この原因が含まれます。 |
| プロトコル エラー | |
| 原因 #95：意味的に不適切なメッセージ | この 5GSM により、意味的に不適切なコンテンツを含むメッセージの受信が報告されます。<br>**重要**<br>SMF は、PDU セッション ID や手順トランザクション アイデンティティなどの非セマンティック エラーを含む必須パラメータに対しても、この原因を送信します。 |

## *PDU* セッション変更拒否

SMF が PDU セッションの変更要求を受け入れない場合、SMF は PDU セッション リリース拒否メッセージの 5GSM Cause IE を設定して、PDU セッションの変更を拒否する理由を示します。

次の表では、PDU セッション変更拒否メッセージでサポートされている 5GSM の原因について説明します。

**表 *262 : 5GSM* の原因：*PDU* セッション変更拒否**

| 5GSM 拒否の原因 | SMF の動作（SMF Behavior） |
|---|---|
| 原因 #43：無効な PDU セッション ID | SMF では、SMF セッションが存在しない場合に、この原因が送信されます。 |
| プロトコル エラー | |
| 原因 #95：意味的に不適切なメッセージ | この 5GSM により、意味的に不適切なコンテンツを含むメッセージの受信が報告されます。<br>**重要**<br>SMF は、PDU セッション ID や手順トランザクション アイデンティティなどの非セマンティック エラーを含む必須パラメータに対しても、この原因を送信します。 |

### *PDU*セッション リリース拒否

SMF が PDU セッションの解放要求を受け入れない場合、SMF は PDU セッション リリース拒否メッセージの 5GSM Cause IE を設定して、PDU セッションの解放を拒否する理由を示します。

SMF では、PDU セッション リリース拒否メッセージで次の原因がサポートされます。

**表 *263 : 5GSM* の原因：*PDU* セッションの解放拒否**

| **5GSM 拒否の原因** | **SMF の動作（SMF Behavior）** |
|---|---|
| 原因 #43：無効な PDU セッション ID | SMF では、SMF セッションが存在しない場合に、この原因がサポートされます。 |
| プロトコル エラー | |
| 原因 #95：意味的に不適切なメッセージ | この 5GSM により、意味的に不適切なコンテンツを含むメッセージの受信が報告されます。<br>**重要**<br>SMF は、PDU セッション ID や手順トランザクション アイデンティティなどの非セマンティック エラーを含む必須パラメータに対しても、この原因を送信します。 |

### *PDU* セッション解放要求

UE が要求した PDU セッション リリース手順を開始するために、UE は、5GSM Cause IE を含む PDU セッション リリース要求メッセージを送信して、PDU セッションを解放する理由を示します。

SMF では、PDU セッション リリース要求メッセージで次の原因がサポートされます。

| **拒否の原因/ 5GSM の原因** | **SMF の動作（SMF Behavior）** |
|---|---|
| 原因 #36：通常の非アクティブ化 | SMF は原因に基づいて統計情報を保持し、リリース手順を続行します。 |
| 原因 # 41：TFT 操作のセマンティック エラー | SMF は原因に基づいて統計情報を保持し、リリース手順を続行します。 |
| 原因 # 42：TFT 操作の構文エラー | SMF は原因に基づいて統計情報を保持し、リリース手順を続行します。 |
| 原因 #44：パケット フィルタのセマンティック エラー | SMF は原因に基づいて統計情報を保持し、リリース手順を続行します。 |
| 原因 # 45：パケット フィルタの構文エラー | SMF は原因に基づいて統計情報を保持し、リリース手順を続行します。 |

*PDU* セッション変更コマンド拒否

UE が PDU-Session-Modification-Command を拒否した場合、UE は PDU セッション変更拒否メッセージの 5GSM 原因 IE を設定して、PDU セッション変更を拒否する理由を示します。

SMF は、次の 5GPP タイマーをサポートしています。

**表 *264*：サポートされる *PDU* セッション変更拒否メッセージ**

| **5GSM の原因** | **SMF の動作** |
|---|---|
| 原因 #26：リソース不足 | SMF では、原因に基づいて統計情報が保持されます。 |
| 原因 #43：無効な PDU セッション ID | SMF は原因に基づいて統計情報を保持し、既存の PDU セッションをリリースします。 |
| 原因 #44：パケット フィルタのセマンティック エラー | SMF では、原因に基づいて統計情報が保持されます。 |
| 原因 #45：パケット フィルタの構文エラー | SMF では、原因に基づいて統計情報が保持されます。 |
| 原因 #83：QoS 操作のセマンティック エラー | SMF では、原因に基づいて統計情報が保持されます。 |
| 原因 #85：QoS 操作の構文エラー | SMF では、原因に基づいて統計情報が保持されます。 |

## 機能の仕組み

SMF は、PDU セッション確立、PDU セッション変更、および PDU セッション リリースの手順に関する 5GSM の原因処理をサポートします。適切な SM 原因が N1 メッセージを介して UE に送信されます。

vSMF は、前述のシナリオですべてのセッション クリーンアップのために PDU セッションと関連技術情報を解放するように指示を hSMF に送信します。

標準準拠

5GSM 原因処理機能は 、*5G* システム（*5GS*）ステージ *3* 向けの *3GPP TS 24.501* リリース *15* *Non-Access-Stratum*（*NAS*）プロトコルに準拠しています。

## 5GSM 原因処理 OAM

ここでは、この機能の操作、管理、およびメンテナンスに関して説明します。

統計

5GSM 原因処理機能では、以下の統計情報をサポートしており、5GSM の原因に基づいて障害の数を追跡できます。

**SMF N1 メッセージ統計情報**

**PDU セッション確立 - 拒否**：

- NETWORK_FAILURE：SMF から送信された、N1 原因が「NETWORK_FAILURE」である PDU-Session-Establishment-Reject メッセージの数。
- UNKNOWN_PDU_SESSION_TYPE：SMF から送信された、N1 原因「UNKNOWN_PDU_SESSION_TYPE」の PDU-Session-Establishment-Reject メッセージの数。
- USER_AUTHENTICATION_OR_AUTHORIZATION_FAILED：SMF から送信された、N1 原因「USER_AUTHENTICATION_OR_AUTHORIZATION_FAILED」の PDU-Session-Establishment-Reject メッセージの数。
- REQUESTED_SERVICE_OPTION_NOT_SUBSCRIBED：SMF から送信された、N1 原因「REQUESTED_SERVICE_OPTION_NOT_SUBSCRIBED」の PDU-Session-Establishment-Reject メッセージの数。
- MISSING_OR_UNKNOWN_DNN：SMF から送信された、N1 原因「MISSING_OR_UNKNOWN_DNN」の PDU-Session-Establishment-Reject メッセージの数。
- SERVICE_OPTION_NOT_SUPPORTED：SMF から送信された、N1 原因「SERVICE_OPTION_NOT_SUPPORTED」の PDU-Session-Establishment-Reject メッセージの数。
- INSUFFICIENT_RESOURCES：SMF から送信された、N1 原因「INSUFFICIENT_RESOURCES」の PDU-Session-Establishment-Reject メッセージの数。
- MISSING_OR_UNKNOWN_DNN_IN_A_SLICE：N1 原因「MISSING_OR_UNKNOWN_DNN_IN_A_SLICE」により SMF から送信された PDU-Session-Establishment-Reject メッセージの数。
- PDU_SESSION_DOES_NOT_EXIST：SMF から送信された、N1 原因「PDU_SESSION_DOES_NOT_EXIST」の PDU-Session-Establishment-Reject メッセージの数。

**PDU セッション変更拒否**：

- INVALID_PDU_SESSION_IDENTITY：SMF から送信された、N1 原因「INVALID_PDU_SESSION_IDENTITY」の PDU-Session-Modification-Reject メッセージの数。

**PDU-セッション-リリース-拒否**：

- INVALID_PDU_SESSION_IDENTITY：SMF から送信された、N1 原因「INVALID_PDU_SESSION_IDENTITY」の PDU-Session-Release-Reject メッセージの数。

**PDU-Session-Release-Request**：

- REGULAR_DEACTIVATION：SMF で受信した、N1 原因が「REGULAR_DEACTIVATION」の PDU-Session-Release-Request メッセージの数。

- SEMANTIC_ERRORS_IN_PACKET_FILTER：SMF で受信した、N1 原因「SEMANTIC_ERRORS_IN_PACKET_FILTER」の PDU PDU-Session-Release-Request メッセージの数。
- SYNTACTICAL_ERROR_IN_PACKET_FILTER：SMF で受信した、N1 原因「SYNTACICAL_ERROR_IN_PACKET_FILTER」の PDU-Session-Release-Request メッセージの数。
- SEMANTIC_ERROR_IN_THE_TFT_OPERATION：SMF で受信した、N1 原因「SEMANTIC_ERROR_IN_THE_TFT_OPERATION」の PDU-Session-Release-Request メッセージの数。
- SYNTACTICAL_ERROR_IN_THE_TFT_OPERATION：SMF で受信した、N1 原因「SYNTACICAL_ERROR_IN_THE_TFT_OPERATION」の PDU-Session-Release-Request メッセージの数。

**PDU-Session-Modification-Command-Reject**：

- INSUFFICIENT_RESOURCES：SMF で受信した、N1 原因「INSUFFICIENT_RESOURCES」の PDU-Session-Modification-Command-Reject メッセージの数。
- INVALID_PDU_SESSION_IDENTITY：SMF で受信した、N1 原因「INVALID_PDU_SESSION_IDENTITY」の PDU-Session-Modification-Command-Reject メッセージの数。
- SEMANTIC_ERRORS_IN_PACKET_FILTER：SMF で受信した、N1 原因「SEMANTIC_ERRORS_IN_PACKET_FILTER」の PDU-Session-Modification-Command-Reject メッセージの数。
- SYNTACTICAL_ERROR_IN_PACKET_FILTER：SMF で受信した、N1 原因「SYNTACICAL_ERROR_IN_PACKET_FILTER」の PDU-Session-Modification-Command-Reject メッセージの数。
- SEMANTIC_ERROR_IN_THE_QOS_OPERATION：SMF で受信した、N1 原因「SEMANTIC_ERROR_IN_THE_QOS_OPERATION」の PDU-Session-Modification-Command-Reject メッセージの数。
- SYNTACTICAL_ERROR_IN_THE_TFT_OPERATION：SMF で受信した、N1 原因「SYNTACICAL_ERROR_IN_THE_TFT_OPERATION」の PDU-Session-Modification-Command-Reject メッセージの数。

# N2/NGAP インターフェイス

N2インターフェイスは、RANとAMF間の参照ポイントです。このインターフェイスはgNodeBをAMFに接続し、コントロール プレーンとユーザー プレーンの分離（CUPS）のために必要です。

サービスにアクセスする前に、UEをネットワークに接続する必要があるため、N2インターフェイスが必要です。SMFはセッション制御を処理し、AMFはUEコンテキストを処理しま

す。そのため、トラフィックまたはセッションを開始する前に、UE コンテキストなどの情報を取得する必要があります。

N2インターフェイスはコントロールプレーンシグナリングを処理します。そのため、SMF は N2 を使用してユーザー トラフィックを生成および検証します。

# N2 原因および診断 IE サポート

## 機能説明

SMF は、NG 無線アクセス ネットワーク（NG-RAN）との間で N2 メッセージを介して受信される N2 原因および重要度診断 IE の処理をサポートします。

## 機能の仕組み

この機能のために、SMF は次の IE および原因の値をサポートしています。

- SMF が次の N2 メッセージの一部として受信する「Criticality Diagnostics」IE をデコードします。
  - PDU セッション リソースのセットアップに失敗した転送
  - PDU セッション リソースの変更に失敗した転送
- 以下の N2 原因値を PDU セッション リソース設定の転送失敗で処理してください：
  - 無線ネットワーク層の原因値：
    - 未指定
    - 複数の PDU セッション ID インスタンス
    - NG システム内ハンドオーバーがトリガーされました
    - NGのシステム間ハンドオーバーがトリガーされました
    - XN ハンドオーバーがトリガーされました
    - UP 整合性保護は実行できない
    - アップの機密性保護は不可能
    - UE 最大完全性保護データ レートの理由
  - プロトコル原因値：
    - 転送構文エラー
    - 抽象構文エラー（拒否）
    - 抽象構文エラー（無視および通知）
    - メッセージに受信状態との互換性がありません。
    - 構文エラー

- 抽象構文エラー（誤って作成されたメッセージ）
- 未指定

- その他の原因値：
  - ユーザー プレーンの処理リソースが不足しています

- 以下の N2 原因値を PDU セッション リソース変更の転送失敗で処理してください：
  - 無線ネットワーク層の原因値：
    - 未指定
    - 不明な PDU セッション ID
    - 複数の PDU セッション ID インスタンス
    - IMS 音声 EPS フォールバックまたは RAT フォールバックがトリガされました
    - NG システム内ハンドオーバーがトリガーされました
    - NGのシステム間ハンドオーバーがトリガーされました
    - XN ハンドオーバーがトリガーされました
  - プロトコル原因値：
    - 転送構文エラー
    - 抽象構文エラー（拒否）
    - 抽象構文エラー（無視および通知）
    - メッセージに受信状態との互換性がありません。
    - 構文エラー
    - 抽象構文エラー（誤って作成されたメッセージ）
    - 未指定
  - その他の原因値：
    - ハードウェア障害
    - 不明な PLMN

- PDU セッション リソース リリース コマンド転送で次の N2 原因値を送信します。
  - 無線ネットワーク層の原因値：
    - 未指定
    - 5GC 生成が原因でリリース

- NAS 原因値：
  - 通常リリース
  - 認証の失敗
  - 登録解除
  - 未指定

- 以下の N2 原因値をパス スイッチ要求のセットアップの失敗転送で処理してください
  - 無線ネットワーク層の原因値：
    - 未指定
    - ターゲット セルに使用可能な無線リソースがありません
    - 無線リソースが使用できません
    - スライスはサポートされていません
    - スライスのリソースが使用できません
    - UP 整合性保護は実行できない
    - アップの機密性保護は不可能
    - サポートされていない 5QI 値
    - 暗号化や整合性保護アルゴリズムがサポートされていない
    - ターゲット セルに使用可能な無線リソースがありません

- SMF が失敗の原因の N2 原因と成功の原因のデバッグ レベルのログを受信した後、エラー レベルのログを生成します。
- SMF が PDU セッション リソース セットアップ失敗転送、PDU セッション リソース変更失敗転送、およびパス スイッチ要求セットアップ失敗転送メッセージを受信する N2 原因に基づいて統計を維持します。
- PDU セッション リソース リリース コマンド転送メッセージで送信された N2 の原因に基づいて統計を維持します。

### *N2* 原因処理

SMF は、次の IE を使用して N2 原因を処理します。

- PDU セッション リソースのセットアップの失敗転送 IE
- PDU セッション リソースの変更に失敗した転送 IE
- PDU セッションリソース リリース コマンド転送 IE

- パス スイッチ要求のセットアップ機能不全転送 IE

PDU セッション リソースのセットアップに失敗した転送 IE

失敗した構成の各PDUセッション リソースについては、NG-RANにはPDUセッション リソース セットアップ要求メッセージの PDU セッション リソース セットアップ失敗転送 IE が含まれます。このメッセージには、SMFの確立に失敗した原因の詳細とともに、原因値が含まれています。

サービス提供の NG-RAN が PDU セッションの部分的な QoS フローの失敗を受け入れない場合、SMF は PDU セッション変更手順を開始します。この手順では、PDU セットアップ手順の完了後に、受け入れられない QoS フローを PDU セッションから削除します。

（注） SMF は、N2 メッセージの一部としてのみ受信する「重要度診断」IE のデコードをサポートします。たとえば、PDU セッション リソースのセットアップ失敗転送メッセージや PDU セッション リソース変更失敗転送メッセージです。SMF は、他のメッセージの「重要度診断」IE を完全にはサポートしていません。

PDU セッション リソースのセットアップの失敗転送 IE には、次の原因とその原因の値が含まれます。

表 *265 : PDU* セッション リソースのセットアップ失敗の転送 *IE* の原因と原因の値

| 原因 | 原因値 | 説明 |
|---|---|---|
| 無線ネットワーク層 | 複数の PDU セッション ID インスタンス | NG-RAN は、PDU セッション リソース セットアップ要求メッセージの受信後に、この原因値を含めます。このメッセージには、同じ値に構成されている PDU セッション リソース セットアップ要求リスト IE のさまざまな PDU セッション ID IE が含まれています。 |
| | ユーザー プレーン セキュリティ強化 | ユーザープレーンセキュリティ適用情報が満たされていない場合、NG-RAN には次の原因値が含まれます。これらの原因の値には、必須または優先のいずれかの値が含まれています。<br>• UP 整合性保護は実行できない<br>• アップの機密性保護は不可能<br>• UE 最大完全性保護データ レートの理由 |
| | ハンドオーバーとのコリジョン | NG-RANでは、ハンドオーバー要求を受信した後、次の原因値が含まれ、ハンドオーバーの準備手順を続行します。<br>• NG システム内ハンドオーバーがトリガーされました<br>• NGのシステム間ハンドオーバーがトリガーされました<br>• XN ハンドオーバーがトリガーされました<br>（注）<br>PDUセッションのリソースのセットアップ手順中に、ハンドオーバー要求が必要です。 |
| | （注）<br>前述の原因の値については、障害検出の場合、NG-RAN が N1 メッセージを UE に転送せず、セッションの解放が続行される場合、SMF は N1 メッセージを介して UE に PDU セッション確立拒否メッセージを送信します。NG-RAN は、N2 メッセージ タイプの N2 原因ベースの統計を維持します。 | |

| 原因 | 原因値 | 説明 |
|---|---|---|
| | 未指定 | NG-RAN の障害が特定されていない場合、SMF はこの PDU セッションの解放をトリガーします。NG-RANは、N2 メッセージタイプのN2原因ベース統計を維持します。 |
| プロトコルグループ | プロトコル データの誤ったエラー | 受信したメッセージをデコードできなかった場合、NG-RAN には次の原因値が含まれます。<br>• 転送構文エラー<br>• 抽象構文エラー（拒否）<br>• 抽象構文エラー（誤って作成されたメッセージ）<br>• 構文エラー<br>（注）<br>NG-RAN が N1 メッセージを UE に転送せず、セッションの解放を続行する場合、SMF は N1 メッセージを介して UE に PDU セッション確立拒否メッセージを送信します。NG-RANは、N2 メッセージ タイプの N2 原因ベースの統計を維持します。 |
| | プロトコル データの予期しない、または不明な情報 | 受信したメッセージをデコードできない場合、NG-RAN には次の原因値が含まれます。<br>• メッセージに受信状態との互換性がありません。<br>• 未指定<br>• 抽象構文エラー（無視および通知）<br>NG-RAN がメッセージを復号化できない場合、SMF は PDU セッションの解放をトリガします。NG-RANは、N2 メッセージ タイプの N2 原因ベースの統計を維持します。 |

| 原因 | 原因値 | 説明 |
|---|---|---|
| トランスポート グループ | アクセスできないトランスポート リソース | 必要なトランスポート リソースが使用できない場合、NG-RAN には次の原因値が含まれます。<br>• リソースが使用できません<br>• 未指定<br>NG-RAN がトランスポート リソースにアクセスできない場合、SMF は PDU セッションの解放をトリガします。NG-RAN は、N2 メッセージ タイプの N2 原因ベースの統計を維持します。 |
| その他 | ユーザー プレーンの処理リソースが不足しています | NG-RAN は、ユーザー プレーン処理に使用できるリソースが不足している場合に、この原因値を含めます。<br>NG-RAN がユーザー プレーンの処理リソースにアクセスできない場合、SMF は PDU セッションの解放をトリガーします。NG-RAN は、N2 メッセージ タイプの N2 原因ベースの統計を維持します。 |

PDU セッション リソースの変更に失敗した転送 IE

変更が失敗した各 PDU セッション リソースについて、NG-RAN には PDU セッション リソース変更要求メッセージの PDU セッション リソース変更失敗転送 IE が含まれます。このメッセージには、SMF の失敗した変更の原因の詳細とともに、原因値が含まれています。

PDU セッション リソース変更の失敗の転送 IE には、次の原因とその原因の値が含まれます。

表 *266 : PDU* セッション リソース変更の失敗の転送 *IE* の原因と原因値

| 原因 | 原因値 | 詳細 |
|---|---|---|
| 無線ネットワーク層 | 複数の PDU セッション ID インスタンス | NG-RAN は、PDU セッション リソース変更要求メッセージの受信後に、この原因値を含めます。このメッセージには、同じ構成値を持つ PDU セッション リソース変更要求リスト IE のさまざまな PDU セッション ID IE が含まれています。 |
| | ハンドオーバーとのコリジョン | NG-RANでは、ハンドオーバー要求を受信した後、次の原因値を設定し、ハンドオーバーの準備手順を続行します。<br>• NG システム内ハンドオーバーがトリガーされました<br>• NGのシステム間ハンドオーバーがトリガーされました<br>• XN ハンドオーバーがトリガーされました<br>（注）<br>ハンドオーバー要求は、PDUセッションのリソース変更手順中に必要です。 |
| | 未指定 | |
| | （注）<br>上記の原因値の場合、SMF は PDU セッション変更手順を停止し、以前の変更手順で存在していたすべてのフィールドで同じ値を引き続き使用します。SMF は、N2 メッセージ タイプの下にある N2 原因ベースの統計情報を維持します。 | |
| | 不明な PDU セッション ID | |

| 原因 | 原因値 | 詳細 |
|---|---|---|
| | | NG-RAN は、PDU セッション リソース変更要求メッセージの受信後に、この原因値を含めます。このメッセージには、NG-RAN が識別できなかった PDU セッション リソース変更要求リスト IE からの PDU セッション ID IE が含まれています。これらのセッションは無効な PDU セッションです。<br><br>SMF は、NG-RAN が無効または不明としてマークした PDU セッション ID の PDU セッションを解放します。NG-RANは、N2メッセージ タイプのN2原因ベース統計を維持します。 |
| トランスポート グループ | | 必要なトランスポート リソースが使用できない場合、NG-RAN にはトランスポート原因値が含まれます。<br><br>SMF は PDU セッション変更手順を停止し、以前の変更手順に存在していたものと同じ値をすべてのフィールドに使用し続けます。SMF は、N2 メッセージ タイプの N2 原因ベース統計情報を維持します。 |
| NAS | | SMF は PDU セッション変更手順を停止し、以前の変更手順に存在していたものと同じ値をすべてのフィールドに使用し続けます。SMF は、N2 メッセージ タイプの N2 原因ベース統計情報を維持します。 |
| プロトコル グループ | | |

| 原因 | 原因値 | 詳細 |
|---|---|---|
| その他 | | SMF は、PDU セッション リソース変更要求メッセージを受信した後、PDU セッションのリリースをトリガーします。このメッセージには、N2 SM 情報に次のその他の原因が含まれています。SMF は、N2 メッセージ タイプの N2 原因ベース統計情報を維持します。<br>• ハードウェア障害<br>• 不明な PLMN<br>前述の原因の原因値を除き、SMF は PDU セッション変更手順を停止し、以前の変更手順で存在していたものと同じすべてのフィールドに同じ値を引き続き使用します。SMF は、N2 メッセージ タイプの N2 原因ベース統計情報を維持します。 |

PDU セッションリソース リリース コマンド転送 IE

解放される各 PDU セッション リソースに対して、SMF には原因値を含む PDU セッション リソースのリリース コマンド転送 IE が含まれます。この値には、NG-RAN へのリリースの原因に関する詳細が含まれています。

PDU セッション リソースのリリース コマンド転送 IE には、次の原因とその原因の値が含まれます：

**表 *267 : PDU* セッション リソース リリース コマンド転送 *IE* の原因と原因値**

| 原因 | 原因値 | 詳細 |
|---|---|---|
| NAS | 通常リリース | SMF では、UE によって開始された PDU セッション解放のためにこの原因が含まれます。 |
| | 登録解除 | SMF には、UDM によって開始された PDU セッションの解放のためにこの原因が含まれます。 |

| 原因 | 原因値 | 詳細 |
|---|---|---|
| 無線ネットワーク層 | 5GC 生成が原因でリリース | SMF では、ネットワークによって開始された PDU セッションの解放と内部障害ケースの両方に対して、この原因が挿入されます。 |
| | （注）<br>SMF は、N2 メッセージ タイプの N2 原因ベース統計情報を維持します。 | |

パス スイッチ要求のセットアップの失敗転送 IE

スイッチングに失敗した各 PDU セッション リソースについては、NG-RAN にはパス スイッチ要求メッセージのパス スイッチ要求のセットアップの失敗転送 IE が含まれます。このメッセージには、ターゲット NG-RAN への切り替えが失敗した原因の詳細とともに、cause 値が含まれています。

（注） SMF は、N2 Cause IE のデコードのみをサポートします。

パス スイッチ要求のセットアップの失敗転送 IE には、次の原因とその原因の値が含まれます。

表 *268 :* パス スイッチ要求のセットアップの失敗転送 *IE* の原因と原因の値

| 原因 | 原因値 | 説明 |
|---|---|---|
| 無線ネットワーク層 | ユーザー プレーン セキュリティ強化 | ユーザープレーンセキュリティ適用情報が満たされていない場合、NG-RAN には次の原因値が含まれます。これらの原因の値には、必須または優先のいずれかの値が含まれています。<br>• UP 整合性保護は実行できない<br>• アップの機密性保護は不可能<br>• UE 最大完全性保護データ レートの理由<br>• 暗号化や整合性保護アルゴリズムがサポートされていない |
| | サポートされていない 5QI 値 | ターゲット NG-RAN が PDU セッションの QoS フローを受け入れない場合、NG-RAN にはこの原因値が含まれます。 |
| | スライスはサポートされていません | 対応するネットワーク スライスがターゲットの NG-RAN でサポートされていない場合、NG-RAN には次の原因値が含まれます。<br>• スライスはサポートされていません<br>• スライスのリソースが使用できません |
| | リソースが使用できません | ターゲットの NG-RAN でスイッチに使用できるリソースが不足している場合、NG-RAN には次の原因値が含まれます。<br>• ターゲットセルに使用可能な無線リソースがありません<br>• 無線リソースが使用できません |
| | 未指定 | |
| | （注）<br>前述のすべての原因値について、SMF は、ターゲット RAN のスイッチングに失敗した QoS フローの UPF N3 トンネルを非アクティブにします。SMF は、N2 メッセージ タイプの N2 原因ベースの統計情報を保持しています。 | |

### 標準準拠

N2 原因と診断 IE サポート機能は、以下の基準に準拠しています：

- *3GPP TS 38.413* バージョン *15.4.0* リリース *15—5G NG-RAN NG*アプリケーション プロトコル（*NGAP*）
- *3GPP TS 23.502* バージョン *15.6.0*、リリース *15—5G*、*5G* システム、セッション管理サービス、第 *3* 段階

# N4 インターフェイス

SMF は、パケット転送制御プロトコル（PFCP）を使用して、N4 インターフェイスを介してユーザー プレーン機能（UPF）にメッセージを送信します。SMF は N4 インターフェイスを使用してさまざまなセッション管理手順を実行します。管理手順の例は、UPF が、SMF から受信したセッション管理データに基づいて、ユーザー プレーン トラフィック情報とフローを識別して転送する場合です。

## N4 Over IPSec

SMF は、セキュアなネットワークトラフィックのために N4 インターフェイス上でインターネット プロトコル セキュリティ（IPSec）をサポートします。

N4/Sx Over IPSec 機能では、SMF、UPF、および SMI でいくつかの基本的な構成を有効にする必要があります。この機能の詳細については、リリースに該当する『*UCC 5G UPF* 構成および管理ガイド』を参照してください。

### SMI StrongSwan 構成

SMI StrongSwan ポッドを生成するには、次の構成例を使用します。

```
SMI:
addons strongswan enabled
strongswan connections N4_IPSec_RCM3
  auto add
  keyexchange ikev2
  type tunnel
  left 192.12.31.202
  right 50.50.29.5
  leftsubnet 192.12.31.202/24
  rightsubnet 50.50.29.4/32
  leftauth psk
  rightauth psk
  leftsendcert never
  psk starent
  esp aes128-sha1,aes128-sha256-prfsha256
  ike aes128-sha1-modp1024,aes128-sha256-modp1536
  reauth no
  dpdaction clear
  dpddelay 300
  dpdtimeout 60
  closeaction none
  server-cert "-----BEGIN CERTIFICATE-----MIIDjTCCAnWgAwIBAgIUF6njegbcarj2oq
/x9c2+utqPThUwDQYJKoZIhvcNAQELBQAwRTELMAkGA1UEBhMCQVUxEzARBgNVBAgMClNvbWUtU3R
hdGUxITAfBgNVBAoMGEludGVybmV0IFdpZGdpdHMgUHR5IEx0ZDAeFw0yMjA5MDcwOTQ0MDdaFw0zM
```

```
jA5MDQwOTQ0MDdaMEUxCzAJBgNVBAYTAkFVMRMwEQYDVQQIDApTb211LVN0YXRlMSEwHwYDVQQKDBh
JbnRlcm5ldCBXaWRnaXRzIFB0eSBMdGQwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDkKA
vGj94OWcFV8j7Enpr5HHqQxakb7hD0fETPByMIb9lPA73AM/3g7YjyIuAFhhs/fx4ZbFQJKDUVjiK/
PE7Mq/Opw5vIsUAgyhors2goa3YvBEPCmTk4fPz21hkWLHZgTARKq3XkgdCAO7kB7UsJpxVBSGg0A
52bIy3bB5C8YNa4rTrafVqzzFdYrQfAama2lpLrfxI7TzoZ6qK1LUDe8U7K/Ln/LJOeqxXClGSEzz
GRBqG41FeU18u3mpJ1pDINUJj7E7r+UN58aTwMoW3/ThCL/2ou+vjTVN7TDzva6XdJPNBCMA5dKEh
0EF10rMo8nmtLzo4UW9NBKMbiv7KPAgMBAAGjdTBzMB8GA1UdIwQYMBaAFC/Lvz0LAowgIkydSpKNUwy/
wHzJMAkGA1UdEwQCMAAwCwYDVR0PBAQDAgTwMDgGA1UdEQQxMC+CFWNuZHAtbmFybWFkYS1tYXN0ZXIt
M4cEwAwfyocQIAFIiAGSEjEAAAAAAAACAjANBgkqhkiG9w0BAQsFAAOCAQEAB6WUQI4qgEHQ8E5sYwzP
zw5KC/zGP2WZIkBfcs8ReiGmLJlC8n8uceWH12ZbFwY75j3EBFfqkmnNXftQGmuU8oGyZsuPDpmEySo+
nE28xnQDZDGzABLZWLSZqqeR6obnYUKvDho14kd40o1hnVlaONw1mrwc/QyFvn3tOwoYnXgaktGM01Fu
cQY1Kc33DvJx3n7fOsdoOLRm9jEENYT3Dv8b6/Ezr2mMHRhAwuoaFpvOSc/eLJy0QO7RpQLpHcRmnh9n
XO+gccB+e0YzvuBS5PONt8wjNSCKl46ZW4F9jpvehR8P/rvH/3VbwDaa8c6xARHNxzNcfq5S4tK/f58RSA
=======END CERTIFICATE-----"
  server-priv-key "$8$gFVXFkFlJplgshiCqWs222+/vkNL5suwjGgqQVwhm1HEIvNp5ViKE8Stz7NK
jubZL1uXIDuy\nTbZmSPp8gIyWFTAJadMNjSoJswWhFYHX+aYoliCIdWQEUFSnJTz2Gofjgex3kM7g8iFkw
BNb\nB6qnSOV2WwMHown1ZfIGEZQAZ6B6iNnQbIHVrOgsyAY6akkyoNzIuc1gFdijQ2W56wW6tQR1\n5EpV
5zweW/Nr0RoOma+ZjpKY8L2VDW30SZ+VwbeTWexrVVfTbYifYYURekyIr6SbK4wFwt+3\nLhBUIr/6zvOlV
QBh4GVEheB5IJid0vHSI3N91sxX+VRaBodSKyw22HpC5BgWanarhkd1KfCT\nmoLzQ7+Nw0X0UfbKTLM5G8
IhXGxqccjl8Jb8nZf490MGx+XrYMkNcFNJ7ua7bxNhl1goTyUs\n4Wbw9hcviv9ZD4leTwnSlqnv5Yfr0ED
GJVrkW2zFv808fKdkJ2rO9T843u9DOrKrFo6XMPT2\n3JU9RL6zlI6bUMTHRqy2xLDfTtDBrD5jg3joJdD7
nkQfCW6cS79cXTBSLTc79p8otX8Jy56n\nkg1uDmQvdY+PgmbByvjQLrPkFr1BQ0C/g5F1uTPSiy2bNGr9l
QF8LfV8kakQMsi+FT0BJbil\nXHxw9pMu2p9srsZRmiBUw4PMq5nQ69jqDJweoNwzjqcJKBvIV1mvKIzHll
Ha0jOqA/FqASn0\nXzmKuZwG49c8qJaE5JBTLTjxeD7tG6A5XuewKynAYWnynT/0xP0mMDMcwEPdOt4e/L4
WJUOJ\nUn4EVo9EMOeG/eRzqILwAbeo2faQtY3HR7c5qMGgnBk903zIVsxl7SP4ujR0HuRw3zq7co5y\n6O
GSmu5Q79EeHezgxn+uiCsPSBwD3gkjvCerdBi8lKPptp//J+XyFA6MdgTbjzb+MxsDXszt\nyXaojBhn9t1
RxwVepAyVesm511JdH/IeDGIYY21Q2DT/k3RT490yKQSu2U2J3n49PCsEtHTQ\nbJo0WmoBVzkysE5kkL2R
MMD6PN+oV8eSqXJHkc1lAFhTpB+TqXcUI+QM0DsLdC1KOr7I5a6P\nl7jdyFFKlbPW8bOe2BB+bKA+5lOQ0
ygb9hlM76WdKmr8hhaimIuH6covaqISrFJJ0IvXcaWS\nhiatKxAq/KhkdczeM0WS6Z8PFlUwRoqgL8X8tn
v1C6tvJbUNLOPgTbHYjkflOyEeFHgXVlXi\nnzE4iAADsRTaMT/3G5YuPjk7+0lmtiZRKHXUPy7LyRwJHNZ
vkaEY+LALhA0ukMpH4DcdDibh\n16kPVUPvWZNZ2Mw3kILH5raqICdGYDDuW1SwCLBeV2pqMuaTzFiSPpLt
5AFXKtF5u9vA+VIC\nJcWP77XVbPTkbsnSBtxFy32RlZY5rx6hLEf/XsMnPAOJvprZvWuc7F+KzrexMmYAY
bJbKE3S\n8POaPet9r8+mPkQf+F5NQD7r3iz0iZ7Hj4IVzm5cvlo9yfatvm03cDplBhVAvsa5dTRuJCq+\
n0UMpf6PbcZI3vhVjIGm7iR+SVSVrq27+lGW76MpnpGwffm/gnyVvg97wl21LmPuool6vKljs\nc9DBybr
dOIwf6gkHkfwDPITGZEbc0SiH3AnIc8Z6HPiCqm1jLJ+2PfC6xnJdLRgkB8sJA1UC\n1VikR2YOvSR26Z6
PI5x7Nhq73jlRMr2N7cvrbBgfjmQyluHa0H/fnOYh4/D6Va8ROWCM4Ca3\nGOPeGn/oJAY1qogLSad33OI
DLsExvyh52x8KvrhdBCRRY5EabXa97XG0TtRTgt6NDd9NwZZ0\n2xxE06VUMS307UBAmyQn7vuezVqcHtv
3H9NnDFPRVLsnyreNo04VjZN6PHtqqOei/sLfL1GK\nVzvleeNGfSAvh1kmFh13f9p1jXgnTwt4iFErpaR
1lvk5K1RoF/+Sjo0HYhETvJFxA/yd/2I0\nZQe3ob/W4hBqI069yQjHbk+9L6kGWzQl3Tl8Lw1/YU/2AXS
zW8V9wCV0OhNLwQezt7a8EBm4\nX3CsPNVhhixhdvC/rSrXFPJnXy0mrcuCXhqLitWRA5VO6883Yry7ldP
uHzcVTyLCxYm0PWaT\nif4TQ6BxvT/gz7Ic6F3dO/QwMKoyeA7RoRR3XpnFcN1QMNTrF17jg17hDFjJwBO
dsq1gfau5\nUDeG6HihvcggYwnbkTprwaHflK/tsTCReNi+j/+ei+4DIe0f2vFgqaGjHdaa6qGkpSXks4L
R\nhyVd9/y+"
  nodes master-3
  exit
 exit
strongswan connections N4_IPSec_V6
  auto add
  keyexchange ikev2
  type tunnel
  left 2001:4888:192:1231::202
  right 2001:4888:50:50::22
  leftsubnet 2001:4888:192:1231::202/64
  rightsubnet 2001:4888:50:50::21/128
  leftauth psk
  rightauth psk
  leftsendcert never
  psk starent
  esp aes128-sha1,aes128-sha256-prfsha256
  ike aes128-sha1-modp1024,aes128-sha256-modp1536
  reauth no
  dpdaction clear
  dpddelay 300
  dpdtimeout 60
```

```
  closeaction none
  server-cert "-----BEGIN CERTIFICATE-----MIIDjTCCAnWgAwIBAgIUF6njegbcarj2oq
/x9c2+utqPThUwDQYJKoZIhvcNAQELBQAwRTELMAkGA1UEBhMCQVUxEzARBgNVBAgMClNvbWUtU3R
hdGUxITAfBgNVBAoMGEludGVybmV0IFdpZGdpdHMgUHR5IEx0ZDAeFw0yMjA5MDcwOTQ0MDdaFw0zM
jA5MDQwOTQ0MDdaMEUxCzAJBgNVBAYTAkFVMRMwEQYDVQQIDApTb211LVN0YXRlMSEwHwYDVQQKDBh
JbnRlcm5ldCBXaWRnaXRzIFB0eSBMdGQwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDkKA
vGj94OWcFV8j7Enpr5HHqQxakb7hD0fETPByMIb9lPA73AM/3g7YjyIuAFhhs/fx4ZbFQJKDUVjiK/
PE7Mq/Opw5vIsUAgyhors2goa3YvBEPCmTk4fPz21hkWLHZgTARKq3XkgdCAO7kB7UsJpxVBSGg0A
52bIy3bB5C8YNa4rTrafVqzzFdYrQfAama2lpLrfxI7TzoZ6qK1LUDe8U7K/Ln/LJOeqxXClGSEzz
GRBqG41FeU18u3mpJ1pDINUJj7E7r+UN58aTwMoW3/ThCL/2ou+vjTVN7TDzva6XdJPNBCMA5dKEh
0EF10rMo8nmtLzo4UW9NBKMbiv7KPAgMBAAGjdTBzMB8GA1UdIwQYMBaAFC/Lvz0LAowgIkydSpKNUwy/
wHzJMAkGA1UdEwQCMAAwCwYDVR0PBAQDAgTwMDgGA1UdEQQxMC+CFWNuZHAtbmFybWFkYS1tYXN0ZXIt
M4cEwAwfyocQIAFIiAGSEjEAAAAAAAACAjANBgkqhkiG9w0BAQsFAAOCAQEAB6WUQI4qgEHQ8E5sYwzP
zw5KC/zGP2WZIkBfcs8ReiGmLJlC8n8uceWH12ZbFwY75j3EBFfqkmnNXftQGmuU8oGyZsuPDpmEySo+
nE28xnQDZDGzABLZWLSZqqeR6obnYUKvDho14kd40o1hnVlaONw1mrwc/QyFvn3tOwoYnXgaktGM01Fu
cQY1Kc33DvJx3n7fOsdoOLRm9jEENYT3Dv8b6/Ezr2mMHRhAwuoaFpvOSc/eLJy0QO7RpQLpHcRmnh9n
XO+gccB+e0YzvuBS5PONt8wjNSCKl46ZW4F9jpvehR8P/rvH/3VbwDaa8c6xARHNxzNcfq5S4tK/f58RSA
==-----END CERTIFICATE-----"
  server-priv-key "$8$jW1TFB0/rJW4V6NrVjk4+1KE7Dw6ynkP3Bqtiwp2k+GQDrI4bX2n+a6Yvyeq
zzKdQ+EQLuy6\ncj9xOrxtNflmzaptNF9Ku786m934ID9hzmC8ISya6/4f2Xu+WdG6uIJl2jDhB/3B2PIc
b6VQ\nV7c4GmwPRNBlIZTVMvTS/2xiUx9bdXIQTVzl2Sc3bZqwLJ6ho/qr4r++T7blVZ16j5sYxUI6\nat
ZKNMMk8+0aoH4UaOd5vtoSkhXCLXkfyrGYagx4KceKxPxSciSEptAzM36py7hDqazW5epU\nFaAnw3PMhq
Ut1r790CaG3VZR5WpcJVkHbdpf0iMCt6pJjNeNlL7BTvns+vo16Mcgt0pyi6Rj\nBAo5lSzog9max0EiRk
spb4a91DFX8mV4tzTy0RCzbgkuzdZ3ecbB9OOvrkWOv7dLiWsZe66Q\nrQA4SLH7eOkgRQvDzqmx3DpqXP
7rebptkLAGXAxZV5uvUuyivdal0EPiB6fu3OwP+gJweZIg\nLjIVbJsREgN7YdukihOmk/xbSMK25Eu3X3
yI1Y55vvQfsY08WEfKBO+Alzjrvz4ABydVJcEE\nqywkSUK/j0VksGvN4lzgely07tpz22VjMTrxJvoWB+
5j9j183T/C1Wgf53miFz2z8ak0NYYe\n2AEP9NNs4tFkB9bY9JQsFv6zY3J+2hQ8iyCiYIROd5ItRyLenO
Bt1fKGp5FHg7dlPuOz0VoI\nUm7GlEexMIycNEr9rzOqzBbMiH5c53htY4iQWFvOARHhw2f5GWPZOIe8Z8
uTq4k5iUjWmaLa\nfhNMXIGX2QNgoduZwXiX6yv3gCpK8WDgF4dlvPjFB+f+iA+QyBlc5AYZuE/2yjYRCr
aaPkzx\ndrWm+Uh18d1YdmQq4ss/rUY4Q0DxDblv94Xx64NIq8dbnY7Zehjs9LXXHk2X6daSTC/FYIY+\n
J/Sks+tmnZ489Tojo/F5dS9iVVstP68MdKOl4OC53lDkqcNl0xhniu2nneS6HTlzUrKFSi4I\n3eRW0FwK
ONKrePxKdObZFB+FvV+xOa2UKnXBbpIh/ENFE0XnADP7Ljox3YsZZpvnXTcz7OcE\nq1b8ggtLt6KyWDb0
tdZljLAb4posj1NioJQzyxHT0gsdfkZxtWiqgt65gqXS/iDo9XXdFEj1\n1Gr07SoE+HwoJIPzAG/8fNhm
27CCYaUW1uWJAOUt9I5UCbER+2kFaVC+odEY2W5/Hfc/gWAy\nSRd6/46kvjN/SzabIdb1yqr68G4LIrHg
1kEBoAf9hXSkD7WY2SMSjl950Co4Cq6zVbk6PAcX\n2ET02FhFewiq+TamVNr0/ruyPohyr1Cpgjqzvx6s
+s7EMWOPJh+XEh8PPBKY+DcDEr2RBIcZ\n4O9uAzwiYTm1x4u8dw5kKRd+H8HFobgaQ18i3IfCdZ4DXyrq
mMrxOw52fGIuAd3Ln2j/AitZ\nQP61dlQlwWPHX7ykvXqCP6oZnfbMUVW3iIdFauZLiCDZkX98UXY3IZUi
Eq13GL6KZtKwFAbu\nqHYEtb5OJRiHRZnqmoOf7BQjC3cdDTBpmPd/s9JCSejqSahlSaSl4Qghbba35HIG
o9PVyks3\nGny6P6twYnDCHLdXbmfE+HE71MnRRPd63CNp+SeX/pP5nBhu6RU/K61ovPrSqcsmo8GiytZB
\ndtVH7nYk3ZUWan04us/bd5zNZfrQ1mCF4rS4KGprQ0N7xWSCilMI49aIxSCNM9WkYl8HAEWA\n1IceEZ
RxHxeltl3JMNTxwFlkP4i4IEalf//Tidrd13jka0NnnjOsboUgn7lay3LvsC6zsIGN\nkP0sTGI1hHj9OL
1iKkw6IhTS1Py5Bjof+XPE844QwOY6Qj6GTd5F/GQJOOD3rL2J/S651TvJ\nsnKM5roovBVb1dUANC/Eay
frpC/2w8wjqPQ/O02SzVNSbZOIPn8P8BV3Ql+NC8rEWL1FZMkI\nkM1AsZTx8BQ0Z1Haf4uhtV5+/29ula
EqEiTH1x2QDV9idWPekqr7eC3009YoGESWHuIH/JE/\n76Rr2zi4wK0JVecxbCGDOynIRFE3I3gRdxgtTi
GrOMe2WdqsUDvDkcijCVpHo0JS3jFVONR8\nxbEo7RpxdrQJ5Zr/u/vx1jnQV/bXTzwlkqoy1g9C3V1m4m
NrqYz62taNTF7+NEVyWC/cp5CU\n5SDuAs3JmFyLaRvyU5SsmDbzlyj+z3DUaByHWlWtC5+klwXYoZOKIy
8zNj+1Kzxosk1wiVX1\nqT4CoAKX"
  nodes master-3
  exit
 exit
```

最新の strongSwan 構成については、『*Ultra Cloud Core* サブスクライバ マイクロサービス インフラストラクチャ操作ガイド』を参照してください。

### SMI StrongSwan 検証

特定のノードで生成されたポッドを確認するには、次のコマンドを使用します。

**kubectl get pods -o wide -n smi-strongswan**

```
NAME              READY   STATUS    RESTARTS   AGE     IP          NODE    NOMINATED NODE
 READINESS GATES
```

```
strongswan-d7zzp   1/1   Running     0      4h57m   10.1.27.7  master-3    <none>
    <none>
```

次に、SMF プロトコル ポッドで IPSec トンネル CLI を検証するための SMI StrongSwan 構成の例を示します。

```
cloud-user@cndp-narmada-master-1:~$ kubectl exec -ti strongswan-d7zzp -n smi-strongswan
 -- ipsec statusall
Status of IKE charon daemon (strongSwan 5.9.3, Linux 5.4.0-122-generic, x86_64):
uptime: 14 days, since Sep 19 16:36:02 2022
malloc: sbrk 6221824, mmap 0, used 3867536, free 2354288
worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 15
loaded plugins: charon aesni aes des rc2 sha2 sha1 md5 mgf1 random nonce x509 revocation
 constraints pubkey pkcs1 pkcs7 pkcs8 pkcs12 pgp dnskey sshkey pem openssl af-alg fips-prf
 gmp curve25519 xcbc cmac hmac ccm gcm drbg curl files attr kernel-netlink resolve
socket-default stroke vici updown eap-identity eap-dynamic eap-tls xauth-generic counters
Listening IP addresses:
10.105.90.166
2001:420:5504:2004::90:18
71.71.71.15
71.71.71.70
71.71.71.72
71.71.71.73
192.12.31.21
2001:4888:192:1231:42a6:b7ff:fe3b:7161
2001:4888:192:1231::21
192.12.31.203
192.12.31.206
192.12.31.207
192.12.31.208
192.12.31.209
192.12.31.210
192.12.31.211
192.12.31.213
192.12.31.214
192.12.31.215
2001:4888:192:1231::203
2001:4888:192:1231::206
2001:4888:192:1231::207
2001:4888:192:1231::208
2001:4888:192:1231::209
2001:4888:192:1231::210
2001:4888:192:1231::211
2001:4888:192:1231::213
2001:4888:192:1231::214
2001:4888:192:1231::215
2001:4888:192:1231::121
192.12.31.121
192.12.31.205
192.12.31.212
2001:4888:192:1231::205
2001:4888:192:1231::212
192.12.31.202
192.12.31.221
192.12.31.222
2001:4888:192:1231::202
2001:4888:192:1231::221
2001:4888:192:1231::222
192.50.0.1
fd00::1
192.115.3.37
Connections:
N4_IPSec_RCM1: 192.12.31.202...50.50.27.5 IKEv2, dpddelay=300s
N4_IPSec_RCM1: local: [192.12.31.202] uses pre-shared key authentication
```

```
N4_IPSec_RCM1: remote: [50.50.27.5] uses pre-shared key authentication
N4_IPSec_RCM1: child: 192.12.31.0/24 === 50.50.27.4/32 TUNNEL, dpdaction=clear
N4_IPSec_RCM2: 192.12.31.202...50.50.28.5 IKEv2, dpddelay=300s
N4_IPSec_RCM2: local: [192.12.31.202] uses pre-shared key authentication
N4_IPSec_RCM2: remote: [50.50.28.5] uses pre-shared key authentication
N4_IPSec_RCM2: child: 192.12.31.0/24 === 50.50.28.4/32 TUNNEL, dpdaction=clear
N4_IPSec_RCM3: 192.12.31.202...50.50.29.5 IKEv2, dpddelay=300s
N4_IPSec_RCM3: local: [192.12.31.202] uses pre-shared key authentication
N4_IPSec_RCM3: remote: [50.50.29.5] uses pre-shared key authentication
N4_IPSec_RCM3: child: 192.12.31.0/24 === 50.50.29.4/32 TUNNEL, dpdaction=clear
N4_IPSec_V6: 2001:4888:192:1231::202...2001:4888:50:50::22 IKEv2, dpddelay=300s
N4_IPSec_V6: local: [2001:4888:192:1231::202] uses pre-shared key authentication
N4_IPSec_V6: remote: [2001:4888:50:50::22] uses pre-shared key authentication
N4_IPSec_V6: child: 2001:4888:192:1231::/64 === 2001:4888:50:50::21/128 TUNNEL,
dpdaction=clear
N4_IPSec: 192.12.31.202...50.50.21.5 IKEv2, dpddelay=300s
N4_IPSec: local: [192.12.31.202] uses pre-shared key authentication
N4_IPSec: remote: [50.50.21.5] uses pre-shared key authentication
N4_IPSec: child: 192.12.31.0/24 === 50.50.21.4/32 TUNNEL, dpdaction=clear
Security Associations (5 up, 0 connecting):
N4_IPSec_RCM1[1345]: ESTABLISHED 96 minutes ago,
192.12.31.202[192.12.31.202]...50.50.27.5[50.50.27.5]
N4_IPSec_RCM1[1345]: IKEv2 SPIs: bc79a16793c7d7eb_i 087bb5cd20fd2f34_r*, rekeying in 72
 minutes
N4_IPSec_RCM1[1345]: IKE proposal:
AES_CBC_128/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_1536
N4_IPSec_RCM1{2501}: INSTALLED, TUNNEL, reqid 2, ESP SPIs: cd664851_i 13009213_o
N4_IPSec_RCM1{2501}: AES_CBC_128/HMAC_SHA2_256_128, 900 bytes_i (17 pkts, 16s ago), 829
 bytes_o (17 pkts, 16s ago), rekeying in 36 minutes
N4_IPSec_RCM1{2501}: 192.12.31.202/32 === 50.50.27.4/32
N4_IPSec_RCM3[1343]: ESTABLISHED 97 minutes ago,
192.12.31.202[192.12.31.202]...50.50.29.5[50.50.29.5]
N4_IPSec_RCM3[1343]: IKEv2 SPIs: 1a50e1d11dfeacb7_i 7be50275473937a3_r*, rekeying in 65
 minutes
N4_IPSec_RCM3[1343]: IKE proposal:
AES_CBC_128/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_1536
N4_IPSec_RCM3{2499}: INSTALLED, TUNNEL, reqid 5, ESP SPIs: cd6f47ec_i 13009213_o
N4_IPSec_RCM3{2499}: AES_CBC_128/HMAC_SHA2_256_128, 1328 bytes_i (25 pkts, 26s ago),
1217 bytes_o (25 pkts, 26s ago), rekeying in 30 minutes
N4_IPSec_RCM3{2499}: 192.12.31.202/32 === 50.50.29.4/32
N4_IPSec_RCM2[1341]: ESTABLISHED 103 minutes ago,
192.12.31.202[192.12.31.202]...50.50.28.5[50.50.28.5]
N4_IPSec_RCM2[1341]: IKEv2 SPIs: 26fd8455c09927ab_i 78c5379f6559be4b_r*, rekeying in 60
 minutes
N4_IPSec_RCM2[1341]: IKE proposal:
AES_CBC_128/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_1536
N4_IPSec_RCM2{2500}: INSTALLED, TUNNEL, reqid 1, ESP SPIs: c6f5243c_i 13009213_o
N4_IPSec_RCM2{2500}: AES_CBC_128/HMAC_SHA2_256_128, 1026 bytes_i (19 pkts, 0s ago), 917
 bytes_o (19 pkts, 0s ago), rekeying in 34 minutes
N4_IPSec_RCM2{2500}: 192.12.31.202/32 === 50.50.28.4/32
N4_IPSec_V6[1339]: ESTABLISHED 2 hours ago,
2001:4888:192:1231::202[2001:4888:192:1231::202]...2001:4888:50:50::22[2001:4888:50:50::22]
N4_IPSec_V6[1339]: IKEv2 SPIs: 64e5d5e102e885e7_i 9062914577d9eb95_r*, rekeying in 36
minutes
N4_IPSec_V6[1339]: IKE proposal: AES_CBC_128/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_1536
N4_IPSec_V6{2498}: INSTALLED, TUNNEL, reqid 3, ESP SPIs: c25a2531_i 0f009d13_o
N4_IPSec_V6{2498}: AES_CBC_128/HMAC_SHA2_256_128, 6817 bytes_i (89 pkts, 17s ago), 6326
 bytes_o (89 pkts, 17s ago), rekeying in 17 minutes
N4_IPSec_V6{2498}: 2001:4888:192:1231::202/128 === 2001:4888:50:50::21/128
N4_IPSec[1337]: ESTABLISHED 2 hours ago,
192.12.31.202[192.12.31.202]...50.50.21.5[50.50.21.5]
N4_IPSec[1337]: IKEv2 SPIs: 9af4e1f24dcc0edb_i 6fcea88758803d37_r*, rekeying in 26 minutes
N4_IPSec[1337]: IKE proposal: AES_CBC_128/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_1536
N4_IPSec{2497}: INSTALLED, TUNNEL, reqid 4, ESP SPIs: cc7c3bf1_i 0f009c13_o
```

```
N4_IPSec{2497}: AES_CBC_128/HMAC_SHA2_256_128, 6844 bytes_i (121 pkts, 19s ago), 5693
bytes_o (121 pkts, 19s ago), rekeying in 4 minutes
N4_IPSec{2497}: 192.12.31.202/32 === 50.50.21.4/32
cloud-user@cndp-narmada-master-1:~$
```

次に、SMF で *ipsec.yaml* ファイルを検証するための SMI StrongSwan 構成の例を示します。

```
cloud-user@cndp-narmada-master-1:~$ kubectl exec -ti strongswan-d7zzp -n smi-strongswan
 -- cat /etc/ipsec.conf
conn N4_IPSec_RCM1
leftcert=/etc/ipsec.d/certs/N4_IPSec_RCM1.cert.pem
auto=add
closeaction=none
compress=no
dpdaction=clear
dpddelay=300
dpdtimeout=60
esp=aes128-sha1,aes128-sha256-prfsha256
ike=aes128-sha1-modp1024,aes128-sha256-modp1536
ikedscp=000000
ikelifetime=3h
keyexchange=ikev2
left=192.12.31.202
leftallowany=no
leftauth=psk
leftsendcert=never
leftsubnet=192.12.31.202/24
lifetime=1h
mobike=yes
reauth=no
rekey=yes
right=50.50.27.5
rightallowany=no
rightauth=psk
rightsubnet=50.50.27.4/32
sha256_96=no
type=tunnel
```

# ユーザー プレーン整合性保護

## 機能説明

SMF は、UE と gNB の間で交換されるユーザー データ パケットの完全性保護をサポートしています。3GPP 仕様では UE と gNB の両方で完全性保護機能を必須としていますが、パケットサイズのオーバーヘッドのため、この機能の使用はオプションのままです。

SMF は UDM から整合性保護ステータスを学習し、gNB でユーザー プレーン整合性保護を適用するかどうかを決定します。UDM からのステータス情報がない場合、SMF はそのローカルの構成データを使用します。

SMF は、UE によって要求され、SMF でローカルに構成されたデータ レート値を比較して、最大整合性データ レートを決定します。データ レートのローカル構成がない場合、UE に要求されたデータ レートが適用されます。

たとえば、整合性保護されたトラフィックの最大データ レートとして UE が 64 kbps を指定した場合、ネットワークはデータ レートが 64 kbps を超えることが予想されない UP 接続に対してのみ整合性保護をオンにします。

## 機能の仕組み

このセクションでは、UE と gNB 間のユーザー データ パケットの完全性がどのように保護されるかについて説明します。

SMF は、5G セッションの作成中に UDM から DNN ごとに UP セキュリティ サブスクリプションを取得し、UDM から受信した UPIP ステータス（UP 完全性値）をローカル構成よりも優先します。

SMF は、UP セキュリティ サブスクリプション、ローカル構成、および UE から受信した UPIP データ レート値に基づいて、UPIP 適用ステータスと UPIP 適用データ レートを決定します。次に、SMF は、PDU 確立手順中に PDU セッション リソース設定要求メッセージを介して、適切な UPIP 適用ステータスとデータレートを gNB に送信します。

SMF は、N2 セットアップ要求メッセージのセキュリティ通知に次の情報を含めます。

- UPIP 適用ステータスを含む完全性保護表示 IE
- UPIP 適用データ レートでの最大整合性保護データ レート アップリンクまたはダウンリンク IE
- UPCP 機能の構成に基づいて、値が「not-needed」の機密保持表示 IE が送信されます。

gNB が UPIP 適用データ レートを満たすことができず、整合性保護表示 IE が「必須」に設定されている場合、gNB は「up-integrity-protection-not-possible」という理由で PDU セッション リソース セットアップ要求を拒否します。その後、SMF はコールをクリアし、N1 リリースを UE に送信します。

gNB が適用データレートを満たすことができず、整合性保護表示 IE が「preferred」に設定されている場合は、PDU セッション リソース セットアップ応答メッセージに、整合性保護結果が「未実行」に設定されたセキュリティ結果が含まれます。

gNB が UPIP データレートを適用でき、整合性保護表示 IE が「preferred」に設定されている場合、PDU セッション リソース セットアップ応答メッセージに、整合性保護結果が「実行済み」に設定されたセキュリティ結果が含まれます。

SMF は、次の表で指定されたアルゴリズムに基づいて、N2 メッセージに UPIP 適用値を入力します。

**表 *269 : UDM* サブスクリプションとローカル構成に基づいて交渉された *UPIP* ステータス**

| UPIP サブスクリプション | ローカル設定 | UPIP ステータス |
|---|---|---|
| 必須 | N/A | 必須 |
| 優先（Preferred） | N/A | 優先（Preferred） |
| 不要 | N/A | 不要 |
| 未受信 | 必須 | 必須 |
| 未受信 | 優先（Preferred） | 優先（Preferred） |

| UPIP サブスクリプション | ローカル設定 | UPIP ステータス |
|---|---|---|
| 未受信 | 不要 | 不要 |
| 未受信 | 未設定 | なし |

表 *270 : UE* でサポートされる値とローカル構成に基づいてネゴシエートされた *UPIP* データ レート

| UE 要求データ レート | ローカル設定 | UPIP データ レート |
|---|---|---|
| 64 kbps | 未設定 | 64 kbps |
| Null | 未設定 | Null |
| Null | 設定済み（Configured） | Null |
| フルレート | 未設定 | フルレート |
| 64 kbps | 64 kbps | 64 kbps |
| フルレート | 64 kbps | 64 kbps |
| 64 kbps | Null | Null |
| フルレート | Null | Null |
| 64 kbps | フルレート | Null |
| フルレート | フルレート | フルレート |

表 *271 : UPIP* ステータスおよび *UPIP* データ レート出力に基づく *N2 UPIP*

| UPIP ステータス | UPIP データ レート | N2 UPIP の表示 | N2 セキュリティ データ レート | N2 セキュリティの結果 | コメント |
|---|---|---|---|---|---|
| 必須 | 64 kbps | 必須 | 64 kbps | N/A | 次のいずれかの理由により N2 障害を受信した場合、コールはクリアされます：<br>• 暗号化および整合性保護アルゴリズムはサポートされていません。<br>• UP 整合性保護は実行できません。 |

| UPIP ステータス | UPIP データレート | N2 UPIP の表示 | N2 セキュリティ データレート | N2 セキュリティの結果 | コメント |
|---|---|---|---|---|---|
| 必須 | Null | N/A | N/A | N/A | コールは N1 cause=#82「ユーザー プレーン整合性保護の UE あたりの最大データレートが低すぎます」でクリアされます。<br>N11 SmContextCreate エラーは、INTTEGRITY_PROTECTION_MDR_NOT_ACCEPTABLE（forbidden）の理由で送信されます。 |
| 必須 | フルレート | 必須 | フルレート | N/A | 次のいずれかの理由により N2 障害を受信した場合、コールはクリアされます：<br>• 暗号化および整合性保護アルゴリズムはサポートされていません。<br>• UP 整合性保護は実行できません。 |
| 優先（Preferred） | 64 kbps | 優先（Preferred） | 64 kbps | 実行済みまたは未実行 | |
| 優先（Preferred） | Null | IEは含まれていません | IE は含まれていません | N/A | |
| 優先（Preferred） | フルレート | 優先（Preferred） | フルレート | 実行済みまたは未実行 | |
| 不要またはなし | N/A | IEは含まれていません | IE は含まれていません | N/A | |

| UPIP ステータス | UPIP データ レート | N2 UPIP の表示 | N2 セキュリティ データ レート | N2 セキュリティの結果 | コメント |
|---|---|---|---|---|---|
| 不要またはなし | N/A | IEは含まれていません | IE は含まれていません | N/A | |
| 不要またはなし | N/A | IEは含まれていません | IE は含まれていません | N/A | |

SMF でローカルに構成されたデータ レートが UE 要求値よりも小さい場合、ローカルに構成された値が null でない限り、SMF は UE 要求値を gNB に送信します。

SMF は、N1 PDU セッション確立要求でユーザー プレーン整合性保護の UE ごとに最大データ レートを受信します。UP セキュリティ サブスクリプションが UPIP が必要であることを示している場合、SMF は UE が要求したデータ レートを構成されたデータ レートと比較します。UE 要求データ レートが低い場合、SMF は 5GSM 原因値 #82「ユーザー プレーンの完全性保護の UE あたりの最大データ レートが低すぎます」により PDU の確立を拒否します。SMF は、403 forbidden-- INTEGRITY_PROTECTED_MDR_NOT_ACCEPTABLE 障害メッセージで SmContextCreateError を含む N11 応答をトリガーします。

UPIP ステータスとデータレートの構成の詳細については、UP Integrity 保護の構成 （803 ページ） のセクションを参照してください。

CLI コマンド で続行するように構成されている場合は、UPIP を有効にしなくてもコールは続行されます。この CLI は、UPIP ステータスが「REQUIRED」にのみ適用されます。

SMF は、PDU セッションの確立中に、N2 セットアップ要求で UPIP 表示が N2 セキュリティ通知で「必須」として送信された場合、インターワーキング機能（IWK）を無効としてマークします。このようなセッションでは、EBI 割り当て手順はトリガーされず、MappedEpsbearerContext は ePCO に含まれません。

IWK が無効としてマークされている場合、SMF は「**403 禁止：サブスクリプション拒否**」という原因で N11 取得メッセージを拒否します。表示が「required」に設定されている NR で UPIP がアクティブな場合、NR から Wi-Fi HO への は拒否されます。HI=1 の Wi-Fi RAT からの CSR が「RAT で拒否されました（Denied in RAT）」という理由で拒否される

UDM サブスクリプションで UPIP が「必須」であることが示されている場合、または構成で UPIP が「必須」であると示されている場合は、4G または Wi-Fi RAT でのセッション作成要求が「RAT で拒否されました」という理由で拒否されます。

UDM サブスクリプションまたはローカル構成で UPIP が「優先」であることが示されている場合、4G または Wi-Fi RAT でのセッション作成要求が受け入れられます。

「preferred」で UPIP アクティブ セッションの 4G から 5G へのハンドオーバー（HO）は受け入れられますが、UE 対応データ レートが使用できない場合、UPIP は有効になりません。

UE は N1 の変更をトリガーしてデータ レートを更新し、SMF は後続の N2 セットアップ中に UPIP を有効にします（つまり、アイドル モードの終了または後続の 5G への H接続）。

UPIP の適用ステータスが次のいずれかの値を示している場合、SMF には、UE トリガーのサービス要求手順中に、UPIP 通知および UPIP データ レートを含む N2 セキュリティ通知が含まれます：

- 必須
- preferred:performed
- preferred:not-performed

### ハンドオーバーおよびその他の手順での UPIP ステータスの処理

このセクションでは、さまざまな引き継ぎシナリオおよびその他の手順中に UPIP の適用値が計算され、UPIP が交渉される方法について説明します。

EUTRA から NR への最初の HO の場合、hSMF は UPIP データ レートを抽出し、アルゴリズムを適用して UPIP の適用値を決定します。

UPIP 適用値が優先され、gNB がデータ レートを満たせない場合、vSMF は通知原因が UP_SEC_NOT_FULFILLED に設定された HSMFUpdateData に NotifyList を含め、gNB から受信したセキュリティ結果を N16 HSMFUpdateData の securityResult IE の hSMF に転送します。

#### XN ハンドオーバー中の UPIP 交渉

パス スイッチ要求のパス スイッチ転送 IE に、セキュリティ結果とセキュリティ表示を含むユーザープレーンセキュリティ情報が含まれています。ローカルに格納された値がパス スイッチで受信した値と異なる場合、SMF は、パス スイッチ確認転送メッセージのセキュリティ痕跡にローカル値を含めます。SMF は、このイベントを警告として記録します。パス スイッチ確認応答で受信したセキュリティ通知がすでに適用されているものと異なる場合、ターゲット gNB は値を修正し、N2 変更通知を送信します。

Xn hanover 中に、ターゲット gNB が「UPIP Required」の場合に多くのアクティブ セッションの中の特定のセッションに UPIP を適用できなかった場合、ターゲット gNB はパス切り替え要求で、対応する PDU セッション ID とともの「pdu session resource failed to setup list」というエラー メッセージを含めることにより、特定の PDU セッションのリリースをトリガーします。ターゲット gNB がアクティブセッションのいずれにも UPIP を適用できない場合、ハンドオーバー試行のリリースがトリガーされ、送信元 gNB はセッションのリリースを決定します。ターゲット gNB から「up-integrity-protection-not-possible」が原因の障害応答を受信した後、SMF はセッションを解放します。

送信元 gNB が HO の前に要求された UPIP をサポートできないことを示し、パス スイッチのセキュリティ結果が「実行済み」を示している場合、SMF は Xn HO 中に UPIP ステータスを [未実行（not-performed）] から [実行済み（performed）] に変更します。

#### 4G または Wi-Fi から 5G へのハンドオーバー中の UPIP 交渉

5G または 4G または Wi-Fi への HO 中に UPIP が無効になることを推奨します。同様に、UPIP は、4G または Wi-Fi から 5G への HO中に有効になります。

#### アイドルからアクティブへの移行中の UPIP 交渉

「UE 最大完全性保護データ レートが理由」の N2 セットアップエラーを受信した場合、SMF はセッションの解放をトリガーします。アイドル モードの終了時に UPIP ステータスが有効（実行済み）または無効（未実行）になり、UPIP ステータスが CDL で更新されます。

#### N2 ハンドオーバー中の UPIP 交渉

SMF は、ターゲット AMF を介してターゲット gNB に UE の UP セキュリティ ポリシーを送信します。ターゲット gNB は、対応する UP セキュリティ ポリシーに準拠できない場合、すべての PDU セッションを拒否し、ターゲット AMF を介して SMF に拒否の原因を示します。他のすべての PDU セッションでは、ターゲット gNB は、UP セキュリティ ポリシーに従って、DRB ごとに UP 整合性保護をアクティブにします。「UE 最大完全性保護データ レートが原因」という理由で N2 障害を受信した場合、SMF はセッションの解放をトリガーします。

SMF は、セキュリティ結果を PDU リソース変更通知転送メッセージに含めることで、gNB から整合性保護レート機能に関する指示を受信します。SMF は、整合性保護レート機能に基づいて「優先」ケースで UPIP 適用アクション（実行済みまたは未実行）を更新します。SMF は、これを受信しても他のアクションを実行しません。これは優先ケースにのみ適用されます。

#### ローミング時の UPIP 交渉シナリオ

#### 訪問者のローカル ブレークアウト

訪問者のローカルブレークアウトシナリオの UPIP 交渉は、ホームのシナリオと同じように機能します。ただし、ビジター LBO では、SMF は UDM から受信した UPIP ステータスよりもローカルに構成された UPIP ステータスを優先します。

標準準拠

ユーザー プレーン完全性保護機能は、次の基準に準拠しています：

- *3GPP* 仕様 *24.501*、バージョン *15.4.0*
- *3GPP* 仕様 *38.413*、バージョン *15.4.0*
- *3GPP* 仕様 *29.503*、バージョン *15.4.0*
- *3GPP* 仕様 *29.502*、バージョン *15.4.0*

## UP Integrity 保護の構成

SMF は、UP 整合性保護パラメータに基づいて gNB で UP Integrity Protection を適用します。

UP 整合性保護パラメータを構成するには、次の構成例を使用します：

```
config
    profile dnn dnn_profile_name
        upip status { required | preferred | not-needed }
        upip data-rate dl { 64kbps | max-ue-rate | null } ul { 64kbps
| max-ue-rate | null } restrict-action { continue | terminate } }
        end
```

注：

- **upip status { required | preferred | not-needed }**：UDM からサブスクリプションで受信されない場合は、UPIP のローカル構成を指定します。
- **upip data-rate dl { 64kbps | max-ue-rate | null } ul { 64kbps | max-ue-rate | null } restrict-action { continue | terminate } }**：ダウンリンクおよびアップリンク トラフィックの UPIP データ レートを構成します。

  構成されたデータ レートおよびUE対応データ レートに基づいて実行するアクションを、次の中から 1 つ指定します。

  - 次へ
  - terminate

  デフォルト アクションは、UPIP status=required の場合は終了し、その他の UPIP ステータスの場合は続行されます。

  続行が構成されている場合、コールは UPIP を有効にせずに続行されます。restrict-action の構成は、UPIP ステータスが「REQUIRED」にのみ適用されることに注意してください。

次に、UP 完全性保護の構成例を示します。

```
profile dnn intershat
 network-element-profiles chf chf1
 network-element-profiles amf amf1
 network-element-profiles pcf pcf1
 network-element-profiles udm udm1
 charging-profile chgprf1
 virtual-mac      b6:6d:47:47:47:47
 ssc-mode 2 allowed [ 3 ]
 session type IPV4 allowed [ IPV6 IPV4V6 ]
 upf apn intershat
 dcnr true
 upip status required
 upip data-rate dl max-ue-rate ul max-ue-rate restrict-action terminate
 exit
```

### UP Integrity Protection の構成の確認

UPIP適用ステータスおよびUPIP適用データレートを表示するには、グローバル構成レベルで **show subscriber** コマンドを使用します。

**show subscriber** コマンドの出力を次に示します。

```
Upip-enforcement-status: [required|preferred]: [performed|not-perfomed]

Upip-enforcement-datarate-dl: 64kbps/max-ue-rate
Upip-enforcement-datarate-ul: 64kbps/max-ue-rate
```

（注） 実行された/実行されていない詳細は、gNB 応答に基づいて更新される「優先される」UPIP ステータスにのみ適用されます。データ レートは、UPIP が有効になっている場合にのみ表示されます（必須/優先：実行済み）。

UPIP 適用がアクティブなサブスクライバの数を表示するには、 **show subscriber count** コマンドを使用します。この出力は、履行または未完了の N2 変更指示を受信すると更新されます。

UPIP でアクティブなセッションの数を表示するには、 **subscriber namespace smf count upip true** コマンドを使用します。

## OAM サポート

ここでは、この機能の操作、管理、およびメンテナンス サポートについて説明します。

バルク統計サポート

UP Integrity Protection 機能のサポートにおいて、次の統計情報を使用できます。

- smf_service_stats：この統計には、セッションで UPIP がアクティブになっているかどうかを示す「upip_active」ラベルが含まれます。

  この統計には、次のシナリオの新しい障害理由も含まれます：

  - ステータスが REQUIRED で UPIP が 5G で有効になっている場合、5G から 4G への HO エラーが発生する - "upip_req_denied_in_rat"
  - ステータスが REQUIRED（「nr_to_untrusted_wifi_upip_status_req_denied_in_rat」）で 5G で UPIP が有効になっている場合の NR から WIFI HO への失敗。

- smf_disconnect_stats：この統計情報には、次の障害シナリオの新しい障害理由が含まれます。
  - UE 要求データ レートが、ステータスが REQUIRED（「disc_pdusetup_integrity_protected _mdr_not_acceptable」）で UPIP を有効にするためにサポートされている SMF のデータ レート未満の場合、5G コールが失敗します。
  - UDM サブスクリプション応答が UPIP status=REQUIRED（「disc_pdnsetup_upip_ status_req_denied_in_rat」）の場合の 4G または Wi-Fi 通話の失敗。
  - ステータスが REQUIRED（「upip_ req_denied_in_rat」）で 5G で UPIP が有効になっている場合の 5G から 4G への HO エラー。
  - ステータス = REQUIRED（「nr_to_untrusted_wifi_upip_status _req_denied_in_rat」）で 5G で UPIP が有効になっている場合の NR から Wi-Fi HO への失敗。

- smf_n2_message_stats：この統計には、ステータス = QUIRED の UPIP の有効化を示す N2 セットアップ要求に対して gNB から障害応答を受信した場合、「n2_cause」、「_UP_integrity_protection_not_possible」または「_Encryption_and_or_integrity_ protection_algorithms_not_supported」という原因値が含まれます。

### *show running-config profile smf*

show コマンド **show running-config profile smf** の出力は、UPIP の非アクティブ化機能が SMF で構成されているかどうかを確認するために強化されています。

```
[smf] smf# show running-config profile smf
profile smf smf1
```

```
 locality LOC1
 instances 1 fqdn   cisco.com.apn.epc.mnc456.mcc123
 instances 1 inter-plmn-fqdn cisco.com.apn.5g.mnc456.mcc123
 instances 1 deactivate-features upip
 instances 1 supported-features [ vsmf dtssa acscr ]
 instances 1 node-id abcdef
 instances 1 allowed-nssai [ slice1 ]
 plmn-list mcc 123 mnc 456
 exit
 plmn-list mcc 242 mnc 01
 exit
 plmn-list mcc 310 mnc 210
 exit
 plmn-list mcc 310 mnc 220
 exit
 plmn-list mcc 310 mnc 260
 exit
 plmn-list mcc 310 mnc 310
 exit
 plmn-list mcc 440 mnc 550
 exit
 service name nsmf-pdu
  type               pdu-session
  schema             http
  service-id         1
  version            1.Rn.0.0
  http-endpoint base-url http://smf-service
  icmpv6-profile     icmpprf1
  compliance-profile comp1
  access-profile     access1
  subscriber-policy  polSub
 exit
exit
```

# ユーザー プレーンの機密性保護

表 *272 :* 機能の履歴

| 機能名 | リリース情報 | 説明 |
|---|---|---|
| ユーザー プレーンの機密性保護の有効化 | 2025.01.0 | ユーザー プレーン機密保持保護（UPCP）は、UE と gNB の間のユーザー データの暗号化を可能にするユーザー プレーン セキュリティ メカニズムです。<br>UDMサブスクリプションデータとローカル構成に基づいて、SMF は PDU セッション確立プロセス中に PDU セッションの UPCP ステータスを判断します。SMF は、PDU セッション確立手順中に gNB に PDU セッション向けのこのセキュリティ ポリシーを提供します。gNB は、受け取った UP セキュリティ ポリシーに応じて、UP 機密性をアクティブにするものとします。<br>**導入されたコマンド**：<br>• UPCP ステータスをローカルで構成するための CLI が導入されました：**[ no ] upcp status { required \| preferred \| not-needed }**<br>• SMF プロファイルの UPCP 機能を非アクティブにするために、新しい CLI が導入されました：**[ no ] instances** *instance_id* **deactivate-features { upcp \| upip }**<br>**デフォルト設定**：有効：常時オン |

### UPCP とは？

ユーザー プレーン機密保持保護（UPCP）は、UE と gNB の間のユーザー データの暗号化を可能にするユーザー プレーン セキュリティ メカニズムです。

この機能では、SMF が UDM サブスクリプション データとローカル構成に基づいて PDU セッションの UPCP ステータスを判断します。SMF は、PDU セッション確立プロセス中に gNB にこの UP セキュリティ ポリシーを提供します。

gNB は、受信した UP セキュリティ ポリシーに基づいて UP 機密性をアクティブ化するものとします。

### SMF での UPCP 適用ステータスの選択

UP セキュリティ ポリシーは、次の 3 つの UPCP 適用ステータスのいずれかを示します。

- **[必須（Required）]**： PDUセッションのすべてのトラフィックにUPCPが適用されます。
- **[優先（Preferred）]**： PDU セッションのすべてのトラフィックに UPCP を適用する必要があります。

- **[不要（Not Needed）]**：UPCP は PDU セッションに適用されません。

SMF は 2 つのソースから PDU セッションの UPCP 適用ステータスを受信します。

- UDM から送信されるUPセキュリティ ポリシー
- ローカル DNNの構成

SMF は、UDM から受信した UPCP の適用ステータスを、ローカルに構成された UPCP の適用ステータスと比較します。デフォルトでは、SMF は常にローカル DNN 構成よりも UDM から受信した UPCP 適用ステータスを優先します。SMF が UDM から UPCP 適用ステータスを受信しない場合、ローカル DNN 構成で定義されている UPCP 適用ステータスが適用されます。

UPCP の適用ステータスをローカルで構成するには、「UPCP の適用ステータスのローカルな構成」の トピックを参照してください。

UPCP の非アクティブ化機能が有効になっている場合、UPCP 機能は **不要** と見なされ、UDM サブスクリプションまたはローカル DNN 構成は無視されます。

SMF は、UPCP 適用ステータス選択ロジックに従って、gNB に送信される UPCP 適用ステータスを決定します。最終的な UPCP 適用ステータスは、その PDU セッションのすべてのメッセージに適用されます。

次の表に、UDM が受信した UPCP 適用ステータスとローカルに設定された UPCP 適用ステータス間のネゴシエーション後のさまざまなシナリオで、SMF が最終的な UPCP 適用ステータスを導出する方法を示します。

| UDM から UPCP 適用ステータスを受信しました | ローカル構成での UPCP 適用ステータス | gNB に送信される最終的な UPCP 適用ステータス |
|---|---|---|
| 必須 | N/A | 必須 |
| 優先（Preferred） | N/A | 優先（Preferred） |
| 不要 | N/A | 不要 |
| 未受信 | 必須 | 必須 |
| 未受信 | 優先（Preferred） | 優先（Preferred） |
| 未受信 | 不要 | 不要 |
| 未受信 | 未設定 | なし |

（注） UPCP がセキュリティ通知 IE を送信するように構成されている場合、SMF は、ローカル DNN 構成とサブスクリプションがない場合、セキュリティ通知 IE に [機密保持表示（Confidentiality Protection Indication）] を **[不要（Not needed ）]**として入力します。

## UPCP の仕組み

### UPCP を有効にするプロセス

SMF が gNB で UPCP をアクティブにする方法は次のとおりです。

1. UE は SMF に PDU セッションの確立を要求します。
2. SMF は、UDM から DNN ごとに UE の UP セキュリティ サブスクリプション情報を受信します。このセキュリティ ポリシーは、gNB で UPCP 機能をアクティブにするか、その PDU セッションの UPCP 適用ステータスを使用しないかを示します。
3. SMF では、オペレータは UP セキュリティ ポリシーをローカルで構成することもできます。受信したセキュリティ ポリシーに基づいて、SMF は、受信した UP セキュリティ ポリシーとローカルに構成されたポリシーに基づく最終的な UPCP 適用ステータスを決定します。

   SMF は、ローカル DNN 構成を介して、UDM から受信した UP セキュリティ ポリシーを常に優先します。ただし、ローミング サブスクライバの場合、ローカル ポリシーの優先順位が高くなります。

   UPCP を非アクティブ化する CLI は、UDM サブスクリプションとローカル DNN 構成の両方よりも優先されます。つまり、非アクティブ化 CLI が設定されている場合、UPCP の適用ステータスは**不要**と見なされ、UPCP 機能は無効になります。

   SMF が UPCP 適用ステータスを選択する方法の詳細については、「SMF での UPCP 適用ステータスの選択」の トピックを参照してください。
4. SMF は、gNB に送信された N2 メッセージのセキュリティ表示 IE で、機密性保護表示 IE のネゴシエートされた UP セキュリティ ポリシーを入力します。
5. gNB からの SecurityResult IE は、Security Indication IE で「**preferred**」と示されているセキュリティ ポリシーが実行されているかどうかを示します。UP セキュリティ ポリシーが「**必須**」または「**不要**」の場合、SecurityResult IE は適用されません。必須の場合に SecurityResult IE を受信しても、SMF は何の処理も行いません。

   gNB が UPCP 機能の有効化を受け入れるか拒否するかに基づいて、次のアクションが実行されます。

| **SMF からの UPCP 適用ステータス** | **gNB による承認/拒否** | **実行されたアクション** |
|---|---|---|
| 必須 | Accepted | コールは正常に続行されます。 |
| | 拒否 | gNB は、PDU セッション リソース設定応答で **機密性保護が不可能であるという** 原因を送信します。SMF がセッションを解放します。 |

| SMF からの UPCP 適用ステータス | gNB による承認/拒否 | 実行されたアクション |
|---|---|---|
| 優先（Preferred） | Accepted | gNB には、機密性保護の結果を含む SecurityResult IE が含まれており、PDU セッション リソース セットアップ応答メッセージで「**実行**」に設定されています。SMF は、gNB からの SecurityResult IE に基づいて「**実行済み**」としてステータスを更新します。 |
| | 拒否 | gNB には、PDU セッション リソース セットアップ応答メッセージで機密保持の結果が「**実行されていない**」に設定されている SecurityResult IE が含まれています。SMF は、gNB からの SecurityResult IE に基づいてステータスを「**実行していません**」として更新します。 |
| 不要 | Accepted | アクションは実行されませんでした。 |
| | 拒否シナリオは適用されません。 | |

（注）

- SMF では、RAT 間、RAT 内、および PLMN 間ハンドオーバーの各プロセスにおける UPCP 機能もサポートされます。
- PDU セッションの確立中に SMF が UPCP の適用ステータスを選択すると、その PDU セッションが終了するまで同じままです。つまり、ランタイム構成の更新は、既存のアクティブな PDU セッションには適用されません。

### アイドルからアクティブへの移行中の UPCP ネゴシエーション

SMF は、アイドルからアクティブへの移行の一環として開始された N2 セットアップ要求の UP セキュリティ ポリシーに UPCP 適用ステータスを含めます。**UP 機密保持が不可能な**場合に N2 セットアップエラーを受信した場合、SMF は PDU セッションの解放をトリガします。UPCP ステータスは SMF でも更新されます。

### N2 変更通知中の UPCP 処理

PDU セッション リソース変更通知メッセージで SecurityResult IE を受信した場合は、SMF によって PDU セッションの新しい UPCP ステータスと見なされます。これは「**優先**」のケースにのみ適用されます。SMF はこれ以外のアクションを実行しません。

UPCP 適用ステータスが「**必須**」の場合、gNB が **not-performed** として通知を送信しても、SMF はアクションを実行しません。

# 移行手順中の *UPCP* ステータス処理

## XN ハンドオーバー時の UPCP サポート

SMF は Xn ハンドオーバー中に UPCP をサポートする方法を次に示します。

1. Xn ベースの RAN 間ハンドオーバー シナリオ中、N2 パス スイッチ要求にはパス スイッチ転送 IE が含まれ、これにはユーザー プレーン セキュリティ情報が含まれます。ユーザープレーン セキュリティ情報には、SecurityResult と SecurityIndication が含まれています。
2. ターゲット gNB が、**[UPCP が必要（UPCP Required）]** ステータスのサブスクライバの Xn ハンドオーバー前にソース gNB でアクティブであった UPCP を提供できない場合、その PDU セッションは、パス スイッチ要求で対応する PDU セッション ID を **持つリストのセットアップに失敗しました。**

   ターゲット gNB から UPCP 値を受信すると、SMF はそれをローカルに構成された値と比較します。パス スイッチ要求で受け取った値と異なる場合、ローカルに構成された値は、パス スイッチ要求承認転送のセキュリティ指標 IE に含まれます。SMF は、このイベントを警告として記録します。

   その後、ターゲット gNB は N2 変更通知を送信して、SecurityIndication の不一致を修正します。

   不一致の場合、hSMF は UP セキュリティ フィールドを送信します。hSMF は、Xn ハンドオーバー中にパス スイッチ要求で「upSecurityInfo」IE を受信した場合、HsmfUpdatedData の upSecurity フィールドを vSMF に送信します。vSMF は、PDU の確立中に hsmf から受信した UpSecurity 情報をすでに持っているため、その情報を使用して、パス スイッチ確認転送で送信されるセキュリティ表示を取得します。
3. 送信元のの gNB がハンドオーバー前に要求された UPCP をサポートできないことを示した場合でも、、パス スイッチのセキュリティ結果が「**実行済み**」を示している場合、SMF は Xn HO 中に UPIP ステータスを **[未実行（not-performed）]** から **[実行済み（performed）]** に変更します。
4. PDU セッションがターゲットの NG-RAN によって拒否されたとして示され、ユーザー プレーン セキュリティ適用が原因で PDU セッションが拒否されたことが示され、ターゲットの NG-RAN ではサポートされていないものの、ユーザープレーン適用ポリシーには「必須」と表示されている場合、 SMF がその PDU セッションの解放をトリガーします。

   ターゲット gNB は、このようなシナリオでは原因として **UP 不可能な機密性保護を**送信します。

## N2 ハンドオーバー中の UPCP サポート

N2ハンドオーバー中に、SMF はターゲット AMF を介して UE の UP セキュリティ ポリシーをターゲット gNB に送信します。ターゲット gNB は、受信した対応する UP セキュリティ ポリシーに準拠できないすべての PDU セッションを拒否します（**[必須（Required ）]** ステータスの UPCP サブスクリプションのみ）。これらの PDU セッションでは、ターゲット gNB はターゲット AMF を介して SMF に拒否原因を示します。

他のすべての PDU セッションにおいて、ターゲットの ng-eNB/gNB は、受信した UE の UP セキュリティ ポリシーに従い、DRB ごとに UP 機密保護を有効化します。

### 5G、4G、または Wi-Fi ハンドオーバー中の UPCP サポート

4G または Wi-Fi から 5G へのハンドオーバー時に、SMF は [セキュリティ表示（Security Indication）] で UPCP 適用ステータスを送信します。SMF は GNB からの SecurityResult に基づいてセッションの UPCP ステータスを更新します。ターゲット gNB が UPCP を提供できない場合、UPCP **が必要な** 場合、SMF は PDU セッションの解放をトリガします。

UPCP は、Wi-Fi から 5G へのハンドオーバー時に処理されます。ローミング シナリオでの Wi-Fi から 5G へのハンドオーバーは、現在 SMF ではサポートされていないため、これらのケースでは UPCP は処理されません。

## *N16* インターフェイスでのユーザー プレーン機密保持のサポート

SMF は、N16 インターフェイスを介したホームルーティング ローミング ネットワークでの UP 機密性保護をサポートしています。このプロセスでは、hSMF が UDM から UPCP サブスクリプションの詳細を受信します。次に、hSMF は受信した UPCP 値をローカルに構成された UPCP 値と比較し、N16 作成応答（upSecurity）の最終値を vSMF に送信します。

vSMFは、hSMFからの応答で受信したUPCP値をvSMFのローカル構成に基づいて上書きする場合があります。これは、vSMFでのローカル設定がローミング サブスクライバに対して優先されるためです。

gNB が UPCP サポートを適用できるかどうかに基づいて、次の 2 つのシナリオが発生します。

- gNB が UPCP サポートを適用できる場合、プロセスで securityResult IE を vSMF に送信します。vSMF は、この IE を含めて、機密性保護の結果を hSMF に伝達します。
- gNB が UPCP の **[要求（Required）]** ステータスのサブスクライバに UPCP サポートを適用できない場合、vSMF は **[up-confidentiality-protection-not-possible]** を原因とする N2 セットアップ応答を受信します。次に、vSMF は PDU セッションの解放をトリガします。vSMF はまた、原因「REL_DUE_TO_UP_SEC」と「UP 機密保持保護が不可能」を示す NgapCause により hSMF に対して解放をトリガします。

（注）

- gNB から PDU セッション リソース変更通知の SecurityResult IE で受信した UPCP ステータスの処理は、優先される場合にのみサポートされます。ローミング サブスクライバの場合、UPCP ステータスは vSMF で更新されます。ただし、変更された UPCP ステータスを持つ hSMF に対する更新の送信はサポートされていません。
- この機能は、nsmf-pdusession の 3GPP リリース 16.9.0 に準拠する必要があります。このサポートは、ローミング サブスクライバの N16 シナリオに UP セキュリティ関連のパラメータを組み込むために必要です。

## ローカルでの UPCP ステータスの構成

このタスクにより、オペレータはローカル構成で PDU セッションの UPCP ステータスを手動で構成できます。

（注） UDM から UPCP ステータスを受信しているにもかかわらず、SMF の UPCP 機能を非アクティブ化する場合は、「SMF での UPCP サポートの非アクティブ化」のトピックを参照してください。

### 手順

**ステップ 1** コマンド **profile dnn** *dnn_profile_name*を使用して、DNN プロファイルのインスタンスを作成します。

**例**：

```
[smf] smf# Config
[smf] smf(config)# profile dnn dnnprof
[smf] smf(config-dnn-dnnprof)#
```

**ステップ 2** コマンド **[ no ] upcp status { required | preferred | not-needed }**を使用して、UPCP のパラメータをローカルで構成します。

**例**：

```
[smf] smf(config-dnn-dnnprof)# upcp status required
[smf] smf(config-dnn-dnnprof)# no upcp status
```

- **upcp status**：UPCP ステータスをローカルで構成します。次の 3 つのオプションがあります：
  - **required**
  - **preferred**
  - **not-needed**
- **[ no ]**：これは任意のコマンドです。UPCP ステータスのローカル構成を削除します。

**ステップ 3** **commit** コマンドを使用して、構成を保存しコミットします。

**例**：

```
[smf] smf(config-dnn-dnnprof)#commit
[smf] smf(config-dnn-dnnprof)#
```

## 制限事項

この機能には次の既知の制限事項があります。

- SMF は、PDU SESSION RESOURCE Modify REQUEST メッセージで gNB に UPCP 適用の詳細を送信することをサポートしていません。
- ローミングの場合、SMF は、gNB から N2 変更指示を受信した場合、通知 Cause= UP_SEC_NOT_FULFILLED/UP_SEC_NOT_FULFILLED を含む通知リストを含む NotifyList とともに HSMFUpdate を送信しません。

  vSMF は、HSMFUpdatedData を受信する upSecurity を処理しません。
- UPCP は、Wi-Fi から 5G へのハンドオーバー時に処理されます。ただし、ローミング シナリオでは処理されません。

## モニタリングおよびトラブルシューティング

この項では、この機能のモニタリングとトラブルシューティングに使用されるバルク統計情報と show コマンドについて説明します。

### バルク統計

この機能をサポートするために、次の統計が拡張または追加されました。

- 統計情報 **SMF サービス統計（smf_service_stats）** が 新しいラベル **upcp_active** をサポートするように拡張され、UPCPがセッションでアクティブになっているかどうかを示します。このラベルの値は [True] または [False] です。
- 統計情報 **SMF サービス統計情報（smf_n2_message_stats）** が、新しい N2 障害原因 **UP_confidentiality_protection_not_posible**で拡張されています。
- 切断統計（smf_disconnect_stats）は、2 つの新しい切断理由（**disc_pdurel_upcp_not_possible** と **disk_pdusetup_upcp_not_possible**）で強化されています。これらの新しいラベルは、UPCP ステータスが REQUIRED の場合、 **UP_confidentiality_protection_not_possible**を示す gNB により、5G コールの切断が SMF によってトリガされることを示しています。
- hSMF のシナリオでは、切断統計（smf_disconnect_stats） **disc_pdurel_upcp_not_possible が**、原因 **REL_DUE_TO_UP_SEC** および Ngap の原因が **UP_confidentiality_protection_not_possible** を示している vSMF リリースを受信すると更新されます。

### コマンドと出力の表示

この項では、この機能の確認に使用する show コマンドとその出力について説明します。

#### Show subscriber count nf-service smf upcp true

UPIP でアクティブなセッションの数を表示するには、show command **Show subscriber count nf-service smf upcp true** コマンドを使用します。この CLI は、5G セッションにのみ適用されます。

```
[command=show subscriber count nf-service smf upcp true | exclude subscriber-details,
timeout=NA, ]]> for SMF ops-center instance [SMF]
----------------------------------------------------------------------------------------
{
```

```
  "sessionCount": 1
}
```

show subscriber supi imsi nf-service smf full

show コマンド **show subscriber supi imsi** *imsi_value* **nf-service smf full** の出力が強化され、UPCP の適用ステータス（必須または優先）が表示されるようになりました。この CLI では UPCP のステータス（実行済みまたは未実行）も表示されます。この CLI は、5G セッションにのみ適用されます。

```
[smf] smf# show subscriber supi imsi-123456789012345 nf-service smf full
{
  "subResponses": [
    {
      "status": true,
      "genericInfo": {
        "pduState": "pduState_None",
        "supi": "imsi-123456789012345",
        "pei": "imei-123456786666660",
        "pduSessionId": 5,
        "pduSesstype": "Ipv6PduSession",
        "accessType": "3GPP_ACCESS",
        "dnn": "intershat",
        "plmnId": {
          "mcc": "123",
          "mnc": "456"
        },
        "sScMode": 1,
        "uetimeZone": "UTC+12:00",
        "allocatedIpv6": "2001:db0::",
        "allocatedIntfid": "tG1H//5HR0c=",
        "nrLocation": {
          "ncgi": {
            "mcc": "123",
            "mnc": "456",
            "nrCellId": "123456789"
          },
          "tai": {
            "mcc": "123",
            "mnc": "456",
            "tac": "1820"
          }
        },
        "alwaysOn": "None",
        "dcnr": "None",
        "wps": "Non-Wps Session",
        "ratType": "NR",
        "ueType": "NR Capable UE",
        "sessTimeStamp": "2025-01-07 10:19:35.974140891 +0000 UTC",
        "callDuration": "12.693001211s",
        "ipv6Pool": "poolv6",
        "commonId": 2,
        "snssai": {
          "sd": "Abf123",
          "sst": 2
        },
        "authStatus": "Unauthenticated",
        "roamingStatus": "Homer",
        "uePlmnId": {
          "mcc": "123",
          "mnc": "456"
        },
        "upipEnforcementStatus": "required",
```

```
"upipEnforcementDataRateDl": "max-ue-rate",
"upipEnforcementDataRateUl": "max-ue-rate",
"ipAllocationBy": "Dynamic",
"anType": "3GPP_ACCESS",
"upcpEnforcementStatus": "required"
```

（注） 実行されたかどうかの詳細は、gNB 応答に基づいて更新される「優先される」UPCP ステータスにのみ適用されます。

## SMF での UPCP および UPIP 機能の非アクティブ化

このタスクは、SMF の UPCP および UPIP 機能を非アクティブ化して、UDM から受信したセキュリティ ポリシーをオーバーライドするのに役立ちます。この構成は、UDM から受信した UPCP および UPIP ステータスとローカル DNN 構成よりも優先されます。

### 手順

**ステップ 1** コマンド **profile smf** *smf_profile_name*を使用して、SMF プロファイルのインスタンスを作成します。

例：

```
[smf] smf# config
[smf] smf(config)# profile smf smf1
[smf] smf(config-smf-smf1)#
```

**ステップ 2** コマンド **[ no ] instances** *instance_id* **deactivate-features { upcp | upip }**を使用して、SMF 上の UPCP および UPCP 機能を非アクティブにします。

例：

```
[smf] smf(config-smf-smf1)# instances 1 deactivate-features upcp
[smf] smf(config-smf-smf1)# instances 1 deactivate-features upip
[smf] smf(config-smf-smf1)# no instances 1 deactivate-features upcp
[smf] smf(config-smf-smf1)# no instances 1 deactivate-features upip
```

- **instances** *instance_id*：このコマンドは、SMF の GR インスタンス ID を指定します。
- **deactivate-features { upcp | upip }**：SMF の UP セキュリティ メカニズムを非アクティブにします。次の 2 つのオプションがあります：
  - **upcp**：ユーザー プレーンの機密性保護を非アクティブにします。
  - **upip**：ユーザー プレーン整合性保護を無効にします。
- **[ no ]**：これは任意のコマンドです。SMF の UPCP および UPIP 機能を有効にし、UDM の指示を再度尊重します。

**ステップ 3** **commit** コマンドを使用して、構成を保存しコミットします。

例：

```
[smf] smf(config-smf-smf1)# commit
[smf] smf(config-smf-smf1)#
```

# N7 インターフェイス

N7 インターフェイスは、セッションの確立または変更時の SMF とポリシー制御機能（PCF）間の参照ポイントです。

PCF は、セッション管理にポリシー制御を使用します。このネットワーク機能は、SMF に対するセッション管理ポリシーをトリガーする N7 インターフェイスを実装しています。SMF はユーザー プレーン機能（UPF）を制御し、PCF から受信したポリシーを UPF が理解できる情報に変換し、UPF に転送します。

## HTTP エラー コードによるエラー処理

### 機能説明

SMF は、このリリースでの PCF に対する SM ポリシー更新通知サービスのエラー応答および関連する HTTP エラー コードをサポートします。この機能では、SMF は 3GPP TS 29.512、セクション 4.2.3.2 の「SM ポリシー関連付け更新要求」に準拠しています。

### 機能の仕組み

SMF は、エラーの詳細と HTTP エラー コードで PCF からの SM ポリシー更新通知サービスに応答します。

コール フロー

このセクションでは、PCF からの SM ポリシー更新通知サービスのコール フローについて説明します。

図 *160 : PCF* からの *SM* ポリシー更新通知サービス

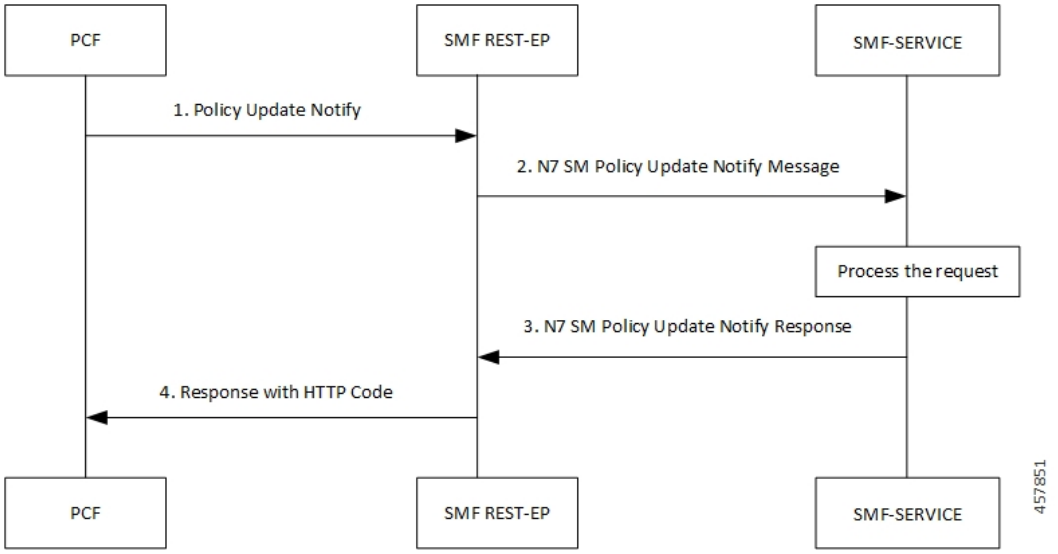



表 *273 : PCF* コール フローからの *SM* ポリシー更新通知サービス

| ステップ | 説明 |
|---|---|
| 1 | PCF は、SMF REST-EP にポリシー更新通知要求を送信します。 |
| 2 | SMF REST-EP は、処理のために N7 SM ポリシー更新通知メッセージを SMF サービスに送信します。 |
| 3 | SMF サービスは要求を処理し、成功の詳細または失敗の詳細のいずれかを含む応答を PCF に送信します。 |
| 4 | SMF-RESTEP は、HTTP コードおよび必要なデータ構造を含む応答を処理した後、その応答を PCF に送信します。 |

## *SMF* エラー処理

SMF は、次の検証を通じて PCF に対する HTTP エラーコードを処理します。

- SMF は、RuleReport データ構造の RuleStatus 列挙を処理します。このデータ構造は、次のガイドラインに従って機能します：
  - PDU セッションのインストール済みまたはアクティブ化されたポリシーと課金制御（PCC）ルールを検証します。検証が失敗した場合、RuleStatus 列挙は設定を「inactive」として表示します。
  - PDU セッションで更新された PCC ルールを検証します。検証が失敗した場合、RuleStatus の列挙には構成が「アクティブ」であると表示されます。

- SMF は、SessRuleReport データ構造内の RuleStatus 列挙を処理します。このデータ構造は、次のガイドラインに従って機能します：
  - インストール済みまたはアクティブ化済みのセッションルールが PDU セッションに存在することを検証します。検証が失敗した場合、SessionRuleStatus 属性は設定を「inactive」と表示します。
  - PDUセッションでのアクティブ化またはインストールの後に、更新されたセッションルールが存在することを確認します。検証が失敗すると、SessRuleStatus 属性は設定を「active」と表示します。
- 検証が原因で PCC ルールが失敗した場合、SMF は ProblemDetails の FailureCause 列挙を使用して原因を処理します。
  - SMF との接続を再試行するには、PCF の PCC_RULE_EVENT を使用します。「InvalidParams」属性でエラーの詳細を表示できます。
- 検証が原因で SessionRule が失敗した場合、SMF は ProblemDetails の FailureCause 列挙を使用して原因を処理します。
  - PCF の RULE_PERMANENT_ERROR を使用して、SMF との接続を再試行します。「InvalidParams」属性でエラーの詳細を表示できます。
- SMF は SessionRuleReport データ構造の SessionRuleFailureCode を処理します。これは次のガイドラインに従って機能します：
  - このリリースでサポートされている値としては、UNSUCC_QOS_VAL のみを使用してください。
- SMF は SessionRuleReport データ構造の SessionRuleFailureCode を処理します。これは次のガイドラインに従って機能します：
  - サポートされる値として、UNSUCC_QOS_VAL を使用します。
- SMF は、HTTP 応答本文にエラーの詳細を表示する ProblemDetails JSON オブジェクトをサポートしています。このオブジェクトを使用すると、SMF サービスには、「application/problem+json」に構成された「Content-Type」ヘッダー フィールドが含まれます。

## エラー コード

次の表は、SMF がエラー処理に使用するエラー コードのリストです。

表 *274 :* エラー コードと詳細

| 番号 | 列挙体 | 詳細 | SMF サポート |
|---|---|---|---|
| 1 | UNK_RULE_ID | 事前にプロビジョニングされた PCC ルールがアクティブ化されていないことを示します。このエラーは、SMF に PCC ルール識別子の情報がない場合に発生します。 | はい |
| 2 | RA_GR_ERR | PCC ルールがアクティブ化または適用されていないことを示します。このエラーは、課金データポリシーの決定で、指定された料金設定グループを参照している PCC ルールが不明であるか無効である場合に発生します。 | はい |
| 3 | SER_ID_ERR | PCC ルールがアクティブ化または適用されていないことを示します。このエラーは、課金データポリシーの決定で、指定されたサービス ID を参照する PCC ルールが、課金対象のサービスに無効、不明、または適用されない場合に発生します。 | はい |
| 4 | NF_MAL | SMF または UPF の機能の問題により、PCC ルールがインストール、アクティブ化、または適用されていないことを示します。PCC ルールのインストールは PCF からプロビジョニングされたルール用です。PCC ルールのアクティブ化は、SMF で事前定義されたルール用です。PCC ルールの適用は、インストールされたルールを対象としています。 | 非対応 |
| 5 | RES_LIM | SMF または UPF のリソースの制限により、PCC ルールがインストール、アクティブ化、または適用されていないことを示します。 | いいえ |

| 番号 | 列挙体 | 詳細 | SMF サポート |
|---|---|---|---|
| 6 | MAX_NR_QoS_FLOW | PDU セッションが QoS フローの最大数に達したことを示します。 | はい |
| 7 | MISS_FLOW_INFO | PCC ルールがインストールされていないことを示します。このエラーは、PCC ルールの最初のインストール要求時に、PCF が PccRule データ構造で「flowInfos」属性または「appId」属性を指定できない場合に発生します。 | はい |
| 8 | RES_ALLO_FAIL | PCC ルールがインストールまたは維持されていないことを示します。このエラーは、QoS フローの確立、変更の失敗、または QoS フローのリリースが原因で発生します。 | はい |
| 9 | UNSUCC_QOS_VAL | QoS 検証の失敗、または保証帯域幅が要求された最大帯域幅を超える場合を示します。 | はい |
| 10 | INCOR_FLOW_INFO | PCC ルールが SMF でインストールまたは変更されていないことを示します。このエラーは、IP アドレスや IPv6 プレフィックスが PDU セッションの該当する IP バージョンに対応していないなど、ネットワークがフロー情報をサポートしていない場合に発生します。 | はい |
| 11 | PS_TO_CS_HAN | パケット交換（PS）から回線交換（CS）へのハンドオーバーにより、PCC ルールが維持されないことを示します。 | いいえ |

| 番号 | 列挙体 | 詳細 | SMF サポート |
|---|---|---|---|
| 12 | APP_ID_ERR | PCC ルールがインストールまたは適用されていないことを示します。このエラーは、アプリケーションが検出するために必要なアプリケーション識別子が無効、不明、または適用不可能な場合に発生します。 | いいえ |
| 13 | NO_QOS_FLOW_BOUND | PCC ルールを関連付ける SMF の QoS フローが存在しないことを示します。 | 対応 |
| 14 | FILTER_RES | SMF が「flowInfos」のフロー情報を処理できないことを示します。このエラーは、3GPP TS 29.212 [23] の第 5.4.2 節で定義された制限が満たされていない場合に発生します。 | あり |
| 15 | MISS_REDI_SER_ADDR | PCC ルールが SMF にインストールまたは適用されていないことを示します。このエラーは、PCF が PCC ルールのトラフィック制御データ ポリシーの決定で有効なリダイレクト サーバ アドレスを提供せず、この PCC ルールの事前構成されたリダイレクト アドレスが SMF に存在しない場合に発生します。 | 非対応 |
| 16 | CM_END_USER_SER_DENIED | 課金システムがサービス制限によりサービス要求を拒否したことを示します。たとえば、エンドユーザー アカウントに要求されたサービスが含まれていないなど、料金設定グループまたはエンドユーザーに関連する制限が終了するとします。 | 非対応 |

| 番号 | 列挙体 | 詳細 | SMF サポート |
|---|---|---|---|
| 17 | CM_CREDIT_CON_NOT_APP | 課金システムがサービスをエンドユーザーに付与できると判断したことを示します。ただし、クレジット制御はサービスには適用されません。たとえば、サービスが無料であるか、オフラインで課金できる場合に利用できます。 | 非対応 |
| 18 | CM_AUTH_REJ | 課金システムが、エンドユーザーがクレジットを要求したサービスを終了するサービス要求を拒否したことを示します。 | 非対応 |
| 19 | CM_USER_UNK | 課金システムでエンドユーザー情報を利用できないことを示します。 | 非対応 |
| 20 | CM_RAT_FAILED | 課金システムがサービス要求を評価できないことを示します。このエラーは、レーティング入力が不十分である、AVP の組み合わせが正しくない、またはレーティングに認識されない、またはサポートされない属性値があるために発生します。 | 非対応 |
| 21 | UE_STA_SUSP | UE が中断状態であることを示します。<br>（注）<br>このエラーは、3GPP 仕様の Annex B で定義されているインターワーキング シナリオにのみ該当します。 | 非対応 |

# 構成ベースの PCF メッセージの制御

## 機能説明

SMF は、PCF メッセージに特定のオプション情報要素（IE）を含めたり除外したりできる柔軟性をオペレータに提供します。オペレータは、CLI 構成コマンドを使用して IE を選択できます。

特定のピア NF が PCF メッセージのオプションの IE をサポートしていない場合があります。この場合、SMF は PCF メッセージ処理プロファイル構成で **skip optional-ies** CLI コマンドを構成します。SMF は常に、N7 インターフェイスを介してオプションの IE を PCF に送信します。

**重要** 制御される IE の包含は、userLocationInfoTime IE のみに制限されます。

PCF メッセージは、次のメッセージの組み合わせです。

- smPolicyControlCreate
- smPolicyControlUpdate
- smPolicyControlDelete

構成コマンドの詳細については、オプションの IE に対する制御の構成 （825 ページ） セクションを参照してください。

## 機能の仕組み

SMF は PCF メッセージ処理プロファイル構成をサポートしています。この構成では、オプションの IE を制御できます。SMF は、 SM ポリシー制御の作成、SM ポリシー制御の更新、および SM ポリシー制御の削除メッセージでこれらの IE を PCF に送信します。

## 機能設定

PCF メッセージを構成ベースで制御する機能には、次の手順が含まれます：

1. メッセージ処理プロファイルの構成 （824 ページ）
2. オプションの IE に対する制御の構成 （825 ページ）

### メッセージ処理プロファイルの構成

PCF メッセージ処理プロファイルを構成するには、次の構成例を使用します。

```
config
  profile network-element pcf pcf_profile_name
    nf-client-profile profile_name
    message-handling-profile message_handling_profile_name
    end
```

**注**：

- **nf-client-profile** *profile_name*：PCF クライアントプロファイルを指定します。 *profile_name* は 、対応する PCF プロファイル名を表す英数字の文字列である必要があります。
- **message-handling-profile** *message_handling_profile_name*：PCF メッセージのメッセージ処理プロファイル名を指定します。

### 設定の確認

UDM メッセージ処理プロファイルが構成されているかどうかを確認するには、次のコマンドを使用します。

**show running-config profile message-handling nf-type pcf mh-profile**

メッセージ処理プロファイルが構成されている場合、この値は、 **message-handling-profile** 構成の一部として次の出力に表示されます。

```
smf(config)# show running-config profile message-handling nf-type pcf mh-profile
 profile network-element pcf nfprf-pcf1
 nf-client-profile udm-profile
 message-handling-profile MHPCF
 exit
```

## オプションの *IE* に対する制御の構成

オプションの IE をスキップするように制御を構成するには、次の構成例を使用します：

```
config
  profile message-handling message_handling_name
    nf-type pcf
      mh-profile mh_profile_name
        service name type npcf-smpolicycontrol
          message type { PcfSmpolicycontrolCreate |
PcfSmpolicycontrolDelete | PcfSmpolicycontrolUpdate }
            skip optional-ies [ userLocationInfoTime ]
            end
```

**注**：

- **mh-profile** *mh_profile_name* ：PCF メッセージ処理プロファイル構成を指定します。
- **service name type npcf-smpolicycontrol**：ポリシー制御サービス名のタイプを指定します。
- **message type { PcfSmpolicycontrolCreate | PcfSmpolicycontrolDelete | PcfSmpolicycontrolUpdate }**：メッセージ タイプを [PCF SM ポリシー コントロール作成（PCF SM Policy Control Create）]、[PCF SM ポリシーコントロール削除（PCF SM Policy Control Delete）]、または [PCF SM ポリシー コントロール アップデート（PCF SM Policy Control Update）] として指定します。
- **skip optional-ies [ userLocationInfoTime ]**：選択した PCF メッセージでスキップするパラメータを指定します。

**重要** 制御される IE の包含は、userLocationInfoTime IE のみに制限されます。

## 設定の確認

オプションの IE をスキップする制御が構成されているかどうかを確認するには、Exec モードで次のコマンドを使用します。

**show running-config profile message-handling nf-type pcf**

また、グローバル構成モードで次の show コマンドを使用して機能構成を確認することもできます。

**show full-configuration profile message-handling nf-type pcf**

**show running-config profile message-handling nf-type pcf** コマンドの出力例を次に示します。

```
[smf] smf# show running-config profile message-handling nf-type pcf
profile message-handling nf-type pcf
 mh-profile mh1
  service name type npcf-smpolicycontrol
   message type PcfSmpolicycontrolCreate
    skip optional-ies [ userLocationInfoTime ]
   exit
   message type PcfSmpolicycontrolUpdate
    skip optional-ies [ userLocationInfoTime ]
   exit
   message type PcfSmpolicycontrolDelete
    skip optional-ies [ userLocationInfoTime ]
   exit
  exit
 exit
exit
```

**show full-configuration profile message-handling nf-type pcf** コマンドの出力例を次に示します。

```
[smf] smf(config)# show full-configuration profile message-handling nf-type pcf
profile message-handling nf-type pcf
 mh-profile mh1
  service name type npcf-smpolicycontrol
   message type PcfSmpolicycontrolCreate
    skip optional-ies [ userLocationInfoTime ]
   exit
   message type PcfSmpolicycontrolUpdate
    skip optional-ies [ userLocationInfoTime ]
   exit
   message type PcfSmpolicycontrolDelete
    skip optional-ies [ userLocationInfoTime ]
   exit
  exit
 exit
exit
```

前の例で、**skip optional-ies** 構成を確認して、オプションの IE がスキップされているかどうか、およびこの構成が有効になっているメッセージ タイプを確認してください。

# N10 インターフェイス

セッションの確立または変更中に、SMF は N7 インターフェイスを介して PCF と、および N10 インターフェイスのユニファイド データ管理 (UDM) 機能に保存されているサブスクライバ プロファイル情報と通信します。

## 構成ベースの UDM メッセージの制御

### 機能説明

SMF を使用すると、オペレータは、CLI 構成コマンドを使用して特定の URI クエリ パラメータを UDM メッセージに含めたり除外したりできます。

特定のクエリ パラメータが UDM メッセージ（N10 Get サブスクリプション要求メッセージ）に含まれない場合があります。この場合、SMF は UDM メッセージ処理プロファイル構成で **skip uri-query-params** CLI コマンドを構成します。デフォルトでは、SMFはN10 Get サブスクリプション取得要求メッセージを介してすべてのクエリ パラメータを UDM に送信します。

構成コマンドの詳細については、URI パラメータの制御の構成 （828 ページ） セクションを参照してください。

## 機能設定

UDM メッセージを構成ベースで制御する機能には、次の手順が含まれます：

1. メッセージ処理プロファイルの構成 （827 ページ）
2. URI パラメータの制御の構成 （828 ページ）

### メッセージ処理プロファイルの構成

UDM メッセージ処理プロファイルを構成するには、次の構成例を使用します。

```
config
  profile network-element udm udm_profile_name
    nf-client-profile profile_name
    message-handling-profile message_handling_profile_name
    end
```

**注**：

- **nf-client-profile** *profile_name*：UDM クライアントプロファイルを指定します。 *profile_name* は 、対応する UDM プロファイル名を表す英数字の文字列である必要があります。
- **message-handling-profile** *message_handling_profile_name*：UDM メッセージのメッセージ処理プロファイル名を指定します。

### 設定の確認

UDM メッセージ処理プロファイルが構成されているかどうかを確認するには、次のコマンドを使用します：

**show running-config profile network-element udm**

メッセージ処理プロファイルが構成されている場合、この値は、 **message-handling-profile** 構成の一部として次の出力に表示されます。

```
[smf] smf# show running-config profile network-element udm
profile network-element udm udm1
 nf-client-profile udm12
 failure-handling-profile fh1
 query-params [ dnn ]
 message-handling-profile MHUDM
 response-timeout 5000
exit
```

## *URI* パラメータの制御の構成

URI クエリ パラメータをスキップするようにコントロールを構成するには、次の構成例を使用します：

```
config
  profile message-handling message_handling_name
    nf-type udm
      mh-profile mh_profile_name
        service name type nudm-sdm
          message type UdmSdmGetUESMSubscriptionData
            skip uri-query-params
            end
```

注：

- **mh-profile** *mh_profile_name* ：UDM メッセージ処理プロファイル構成を指定します。
- **service name type nudm-sdm**：UDM で使用可能なオプションからサービス名タイプを nudm-sdm として指定します。
- **message type UdmSdmGetUESMSubscriptionData**：メッセージ タイプを UDM SDM Get UE SM Subscription Data として指定します。
- **skip uri-query-params**：選択した UDM メッセージをスキップするパラメータを指定します。

## 設定の確認

URI パラメータをスキップする構成が有効になっているかどうかを確認するには、次のコマンドを使用します。

**show running-config profile message-handling nf-type udm**

**show running-config profile message-handling nf-type udm** コマンドの出力例を次に示します。

```
[smf] smf# show running-config profile message-handling nf-type udm
profile message-handling nf-type udm
 mh-profile MHUDM
  service name type nudm-sdm
   message type UdmSdmGetUESMSubscriptionData
    skip uri-query-params [ snssai dnn plmnid ]
   exit
  exit
 exit
exit
```

前の例で、**skip uri-query-params** 構成を確認して、N10 取得サブスクリプション要求メッセージで除外するように構成されている URI クエリ パラメータを特定します。

# 3GPP リリース 16 準拠の N10 属性

表 *275 :* 機能の履歴

| 機能名 | リリース情報 | 説明 |
|---|---|---|
| 3GPP リリース 16 準拠の汎用 UDM の機能強化 | 2024.01 | SMF は、3GPP 29.503、リリース 16 に準拠した次の拡張機能をサポートしています。<br>• サブスクリプション レベル 3GPP 課金特性：この属性が DNN 構成で使用可能な場合、この属性は SessionManagementSubscriptionData で受信される属性よりも優先されます。<br>• ePDG 表示および NF 登録時間：UDM メッセージ処理構成には、N10 登録要求の ePDG Indication アクセス情報と NF 登録時間を許可または無視する追加のキーワードオプションが含まれています。<br>**デフォルト設定**：該当なし |

ePDG 表示（epdgInd）属性と NF 登録時間（registrationTime）属性が N10 登録要求メッセージに追加され、3GPP TS 29.503 リリース 16 に準拠します。

これらの属性を無効にするには、UDM 構成で **skip optional-ies** コマンドを使用します。構成の詳細については、「オプションの IE を無効にする構成」の項 を参照してください。

# UDM サブスクリプション S-NSSAI に対する S-NSSAI の検証

SMF は、UDM サブスクリプション応答のシングル ネットワーク スライス選択支援情報（S-NSSAI）を使用して、サブスクライバ ポリシーを再選択します。SMF では、Slice or Service Type（SST）および Slice Differentiator（SD）パラメータに基づいて S-NSSAI が照合されます。

S-NSSAI サブスクリプションの選択は、次の基準に基づいています。

- 両方のパラメータが一致する場合、SMF は、SST と SD の両方が一致（完全に一致）する S-NSSAI サブスクリプションを選択します。
- SST のみが一致し、SD が要求された S-NSSAI または UDM サブスクリプション S-NSSAI のいずれかで使用できない場合、SMF は SST のみが一致した（部分的に一致した）サブスクリプションを選択します。

- 要求された S-NSSAI が SMF ローカル コンフィギュレーション S-NSSAI（SMF プロファイルで sus高）と部分的に一致する場合、ローカル コンフィギュレーション S-NSSAI を使用して UDM サブスクリプション応答を検証します。この条件は、5G 通話に適用されます。

次の表に、UDM N10 サブスクリプションからサブスクリプションを選択するための検証基準を示します。

表 *276 : UDM N10* サブスクリプション応答からのサブスクリプション選択の検証基準

| RAT の処理 | N10サブスクリプション前の選択された S-NSSAI | サブスクリプションの S-NSSAI | N10 サブスクリプション後の最終的な S-NSSAI |
|---|---|---|---|
| 5G | 作成メッセージで受信した要求済みの S-NSSAI | サブスクリプション内の単一の S-NSSAI | 要求された S-NSSAI と一致する登録済み S-NSSAI。 |
| 5G | 作成メッセージで受信した要求済みの S-NSSAI | サブスクリプション内の複数の S-NSSAI | 要求された S-NSSAI と一致する登録済み S-NSSAI。 |
| 4G または Wi-Fi | 要求された S-NSSAI（DNN プロファイルで構成されているデフォルトの S-NSSAI）デフォルトの S-NSSAI が使用できない場合は、SMF プロファイルで使用可能な許可された S-NSSAI のいずれかが選択されます。 | サブスクリプション内の単一の S-NSSAI | 登録済みの S-NSSAI。要求された S-NSSAI または要求された DNN またはセッション作成要求（CSR）で利用可能な APN と一致します。 |
| 4G または Wi-Fi | 要求された S-NSSAI（DNN プロファイルで構成されているデフォルトの S-NSSAI）デフォルトの S-NSSAI が使用できない場合は、SMF プロファイルで使用可能な許可された S-NSSAI のいずれかが選択されます。 | サブスクリプション内の複数の S-NSSAI | 登録済みの S-NSSAI。要求された S-NSSAI または要求された DNN またはセッション作成要求（CSR）で利用可能な APN と一致します。 |

次の表に、N10 サブスクリプション要求メッセージでのクエリ パラメータの可用性に基づく SMF および UDM の動作の詳細を示します。

表 *277 : UDM N10 Get* サブスクリプション要求の *URI* クエリ パラメータ

| 設定（Configuration） | N10サブスクリプションの URI パラメータ | UDM の動作 | SMF N10 サブスクリプション応答処理 |
|---|---|---|---|
| デフォルトまたは構成なし | PLMN、選択した SNSSAI、DNN | UDM は、要求された PLMN を使用して、S-NSSAI と DNN に一致するサブスクリプションを送信します。 | SMF は、要求された S-NSSAI に一致する S-NSSAI サブスクリプションを選択し、選択したサブスクリプションから要求された DNN と一致する DNN 構成を選択します。 |
| PLMN のスキップ | 選択された S-NSSAI、DNN | UDM は、ホーム PLMN を使用して、S-NSSAI と DNN に一致するサブスクリプションを送信します。 | SMF は、要求された S-NSSAI と一致する S-NSSAI サブスクリプションを選択し、選択したサブスクリプションから要求された DNN と一致する DNN 構成を選択します。 |
| S-NSSAI をスキップ | PLMN、DNN | UDM は、要求された PLMN を使用し、DNN に一致する S-NSSAI サブスクリプションで応答します。 | SMF は、要求された S-NSSAI と一致する S-NSSAI サブスクリプションを選択し、選択したサブスクリプションから要求された DNN と一致する DNN 構成を選択します。 |
| DNN のスキップ | 選択された S-NSSAI、PLMN | UDM は、要求された PLMN を使用して、S-NSSAI に一致する S-NSSAI サブスクリプションを送信します。 | SMF は、要求された S-NSSAI と一致する S-NSSAI サブスクリプションを選択し、選択したサブスクリプションから要求された DNN と一致する DNN 構成を選択します。 |
| PLMN、S-NSSAI をスキップ | DNN | UDM はホーム PLMN を使用して、DNN に一致するすべての S-NSSAI サブスクリプションを送信します。 | SMF は、要求された S-NSSAI と一致する S-NSSAI サブスクリプションを選択し、選択したサブスクリプションから要求された DNN と一致する DNN 構成を選択します。 |

| 設定（Configuration） | N10サブスクリプションの URI パラメータ | UDM の動作 | SMF N10 サブスクリプション応答処理 |
|---|---|---|---|
| PLMN のスキップ、DNN | S_NSSAI | UDM は、ホーム PLMN を使用して、S-NSSAI に一致する S-NSSAI サブスクリプションを送信します。 | SMF は、要求された S-NSSAI と一致する S-NSSAI サブスクリプションを選択し、選択したサブスクリプションから要求された DNN と一致する DNN 構成を選択します。 |
| S-NSSAI のスキップ、DNN | PLMN | UDM は要求された PLMN を使用し、すべての S-NSSAI サブスクリプションを送信します。 | SMF は、要求された S-NSSAI と一致する S-NSSAI サブスクリプションを選択し、選択したサブスクリプションから要求された DNN と一致する DNN 構成を選択します。 |
| PLMN、S-NSSAI、DNN のスキップ | なし | UDM はホーム PLMN を使用し、すべての S-NSSAI サブスクリプションを送信します。 | SMF は、要求された S-NSSAI と一致する S-NSSAI サブスクリプションを選択し、選択したサブスクリプションから要求された DNN と一致する DNN 構成を選択します。 |

# N11 インターフェイス

N11 インターフェイスは、アクセスとモビリティ管理（AMF）と SMF 間の基準ポイントです。

新しいセッションを要求するには、UE と gNB の両方が次世代アプリケーション プロトコル（NGAP）を使用して、N1 または N2 インターフェイスを介して Non Access Stratum（NAS）メッセージを伝送します。AMF はこれらの要求を受信し、接続およびモビリティ管理を処理します。次に、AMF は、N11 インターフェイスを介してセッション管理関連の要件を SMF に転送します。AMF は、ネットワーク リポジトリ機能（NRF）にクエリを実行することで、接続要求を処理できる SMF を識別します。

SMF が N11 インターフェイスを介して受信するメッセージは、ユーザー プレーン全体で PDU セッションを追加、変更、または削除するための要求です。

## ProblemDetails JSON オブジェクト

### 機能説明

SMF は N11 インターフェイス上での ProblemDetails JSON オブジェクトの送受信をサポートし、ローミングをサポートします。

アプリケーション エラーは、HTTP サーバとして機能する SMF サービスが HTTP 要求を完了できない場合があります。この場合、SMF サービスはアプリケーション エラーを類似の 4xx または 5xx HTTP ステータスにマップします。

HTTP ステータス コードにより、エラーの原因が分かります。ただし、これらのステータス コードにはエラーに関する十分な情報がない場合があります。この場合、HTTP サーバとして動作している SMF サービスは、HTTP クライアントとして動作している SMF サービスに、より多くのアプリケーション関連のエラー情報を提供します。この SMF サービスは、応答本文に「ProblemDetails」データ構造の表現を含めることによって、追加情報を提供します。

3GPP 仕様では、ドキュメント形式の 1 つとして JSON が定義されています。HTTP API はこの形式を再利用して、要件に基づいてさまざまな問題のタイプを特定します。

N11 インターフェイスに指定された ProblemDetails 構造は、hSMF でのローミング コール フローのために N16 インターフェイスに送信されます。hSMF から問題の詳細を受信した後、vSMF は AMF からの対応するメッセージを拒否し、vSMF が hSMF から受信した問題の詳細を保存します。

サポートされる属性

この機能のために、SMF は次の属性をサポートしています。

- status：問題発生の HTTP ステータス コードを指定します。HTTP ステータスは、403 や 504 など、4xx と 5xx の形式になります。
- cause：問題の発生に基づいて、マシンが読み取り可能なアプリケーション エラーの原因を指定します。5G コア SBI API 仕様で、アプリケーション エラーの原因が定義されています。仕様に従い、この属性では、UNSPECIFIED_NF_FAILURE","DNN_NOT_SUPPORTED などの UPPER_WITH_UNDERSCORE ケース形式を使用します。
- title：問題の種類の概要を表示します。この属性は、問題の 1 つの発生が別の発生においても同じままです。この属性には、無効なパラメータ、ネットワーク障害、必須、オプション、または条件付きの IE が欠落しているなどのサマリーが含まれます。
- detail：問題の発生に固有の人間が判読可能な情報を提供します。この属性には、UDM 登録の失敗、UDM サブスクリプションの失敗、SM コンテキスト作成での無効なパラメータの送信などの情報が含まれます。

（注）
- この機能では、SMF は title 属性と detail 属性をサポートしています。
- この機能では、SMF は invalidParams 属性をサポートしていません。

## 機能の仕組み

ここでは、この機能の仕組みを説明します。

応答に ProblemDetails データ構造のペイロード本文が含まれている場合、SMF サービスには、「application/problem+json」に構成された「Content-Type」ヘッダー フィールドが含まれます。SMF サービスが HTTP 応答を生成します。

問題の詳細の送信

SMF は、次の N11 メッセージで問題の詳細を AMF に送信します。

- SM コンテキスト作成エラー
- SM コンテキストの更新エラー
- SM コンテキスト リリースへの POST 応答
- SM コンテキスト取得への POST 応答

問題の詳細処理

SMF は、SMF が AMF から受信する問題の詳細構造を処理し、他の SMF にローミング サポートを提供します。

EBI 割り当てエラーと問題の詳細

SMF は、EBI 割り当てに失敗した ARP 値の EBI を保存しないことによって、この N11 メッセージを処理します。たとえば、SMF は、問題の詳細と「EBI_EXAUSTED」の原因および障害の詳細を含む AMF からの EBI 割り当てエラーを処理します。

問題の詳細を含む N1N2 転送の確認

SMF は、問題の詳細の HTTP ステータスと原因の値に従って、確認応答 N11 メッセージを処理します。たとえば、SMF は、HTTP ステータスが 404、原因が AMF からの「CONTEXT_NOT_FOUND」である N1N2 確認応答メッセージを処理します。

SMF 間のローミング

ホーム SMF（hSMF）と訪問先 SMF（vSMF）が N16 インターフェイスを介して相互に通信します。次のセクションでは、hSMF および vSMF のローミング コール フローのために、N11 インターフェイスに指定された ProblemDetails 構造が N16 インターフェイスにどのように送信されるかについて説明します。

コール フロー

このセクションでは、次のコールフローについて説明します。

- hSMF コール フローでのサービス操作の作成
- vSMF コール フローでのサービス操作の作成
- hSMF コール フローに対するサービス操作の更新
- vSMF コール フローに対するサービス操作の更新

hSMF コール フローでのサービス操作の作成

作成サービス操作は、hSMF においてホームルーティング ローミング シナリオ用の PDU セッションを作成します。vSMF などの NF サービス コンシューマは、HTTP POST メソッドを使用して PDU コンテキストを作成します。

このセクションでは、hSMF でサービス オペレーションの作成のコール フローについて説明します。

**図 *161 : hSMF* コール フローでのサービス操作の作成**

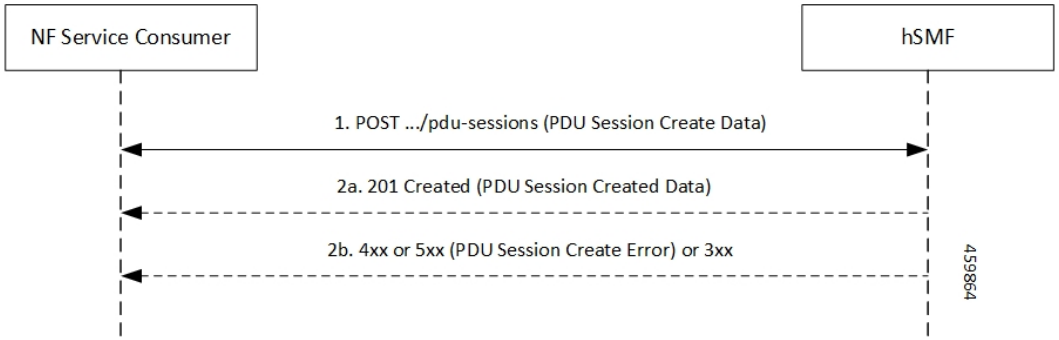



**表 *278 : vSMF* コール フローの説明にサービス操作を作成**

| ステップ | 説明 |
|---|---|
| 1 | vSMF などの NF サービス コンシューマが POST 要求を送信して、hSMF で PDU セッションを作成します。 |
| 2 | PDU セッションの作成が成功すると、hSMF は「201 Created」を NF サービス コンシューマに送信します。 |
| 3 | PDU セッションの確立が失敗した場合、hSMF は、「PDU セッション作成エラーの HTTP ステータス コード」の表にリストされているように、HTTP ステータス コードを送信します。4xx または 5xx 応答の場合、メッセージ本文には「cause」属性を持つ ProblemDetails 構造を含む PDU セッション作成エラー構造が含まれています。 |

**表 *279 : PDU* セッション作成エラーの *HTTP* ステータス コード**

| データ タイプ | HTTPS ステータス コード | 原因 | 詳細 | タイトル（Title） |
|---|---|---|---|---|
| PDU セッション作成エラー | 403 | サブスクリプション_DENIED | UDM_Subscription_Fetch_Failed | ネットワーク_Failure |
| PDU セッション作成エラー | 403 | SNSSAI_DENIED | SNSSAI_Not_Supported_By_SMF | ネットワーク_Failure |

| データ タイプ | HTTPS ステータス コード | 原因 | 詳細 | タイトル（Title） |
|---|---|---|---|---|
| PDU セッション作成エラー | 500 | 未指定 _NF_FAILURE | UDM_Notification _Failed | ネットワーク _Failure |
| PDU セッション作成エラー | 404 | サブスクリプション _NOT_FOUND | UDM_Subscription _Failed | ネットワーク _Failure |
| PDU セッション作成エラー | 504 | NETWORK_ 障害 | SLA_Txn _Timeout | ネットワーク _Failure |
| PDU セッション作成エラー | 403 | DNN_DENIED | DNN_Not_Subscribed | ネットワーク _Failure |
| PDU セッション作成エラー | 403 | SSC_NOT_ サポート対象 | SSC_Mode_Not _Supported_By_SMF | ネットワーク _Failure |
| PDU セッション作成エラー | 403 | SSC_DENIED | SSC_Mode_Denied _From_UDM | ネットワーク _Failure |
| PDU セッション作成エラー | 403 | PDUTYPE_DENIED | UDM_Rejected _PDU_Type | ネットワーク _Failure |

vSMF コール フローでのサービス操作の作成

Create SM Context service 操作を行うと、ホーム ルーティング ローミングの場合に、SMF または vSMF のいずれかで PDU セッションの SM コンテキストが作成されます。AMF などの NF サービス コンシューマは、HTTP POST メソッドを使用して SM コンテキストを作成します。

このセクションでは、vSMF でサービス オペレーションの作成のコール フローについて説明します。

図 *162 : vSMF* コール フローでのサービス操作の作成

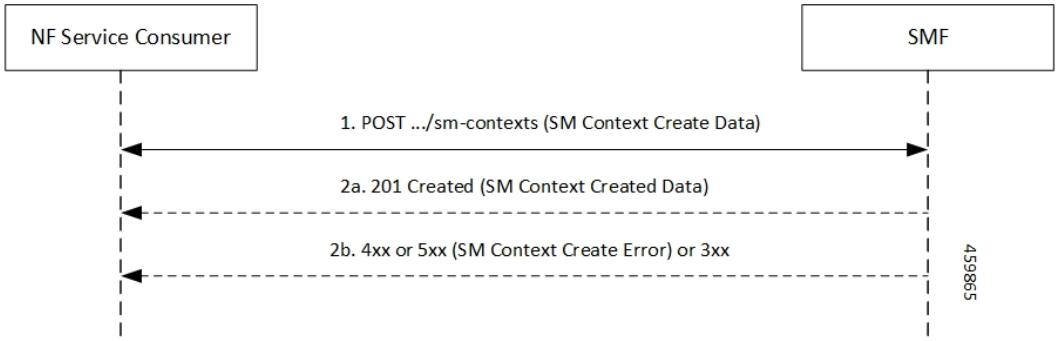



表 *280 : vSMF* コール フローの説明にサービス操作を作成

| ステップ | 説明 |
|---|---|
| 1 | AMF などの NF サービス コンシューマは、vSMF の SM コンテキスト収集リソースを表すリソースに SM コンテキストを作成するための POST 要求を送信します。 |
| 2 | PDU セッションの作成が成功すると、SMF は「201 Created」を NF サービス コンシューマに送信します。 |
| 3 | PDU セッションの確立が失敗した場合、SMF は、「SM コンテキスト作成エラーの HTTP ステータス コード」の表にリストされているように、HTTP ステータス コードを送信します。NF サービス コンシューマへの 4xx 応答または 5xx 応答では、メッセージ本文には「cause」属性を持つ ProblemDetails 構造を含む SM コンテキスト作成エラー構造が含まれます。 |

表 *281 : SM* コンテキスト作成エラーの *HTTP* ステータス コード

| データ タイプ | HTTPS ステータス コード | 原因 | 詳細 | タイトル（Title） |
|---|---|---|---|---|
| SM コンテキスト作成エラー | 403 | PDUTYPE_ NOT_SUPPORTED | PDU_Type_Not _Supported_ By_SMF | ネットワーク _Failure |
| SM コンテキスト作成エラー | 500 | REQUEST_ REJECTED_ 未指定 | Charging_Response _Failure | ネットワーク _Failure |
| SM コンテキスト作成エラー | 504 | NETWORK_ 障害 | SLA_txn _timeout | ネットワーク _Failure |

| データ タイプ | HTTPS ステータス コード | 原因 | 詳細 | タイトル（Title） |
|---|---|---|---|---|
| SM コンテキスト作成エラー | 400 | MANDTORY_IE _MISSING | PDU_Session_ ID_Not_Sent | Mandatory_IE _Missing |

hSMF コール フローに対するサービス操作の更新

NF サービス コンシューマ（vSMF など）は、hSMF の PDU セッションを更新します。また、NF サービス コンシューマは、NF サービス コンシューマが UE からの N1 SM シグナリングで vSMF から受信する情報を hSMF に提供します。NF サービス コンシューマは、HTTP POST メソッドを使用してこの情報を受信します。

ここでは、hSMF コール フローに対する更新サービス操作について説明します。

**図 *163 : hSMF* コール フローに対するサービス操作の更新**

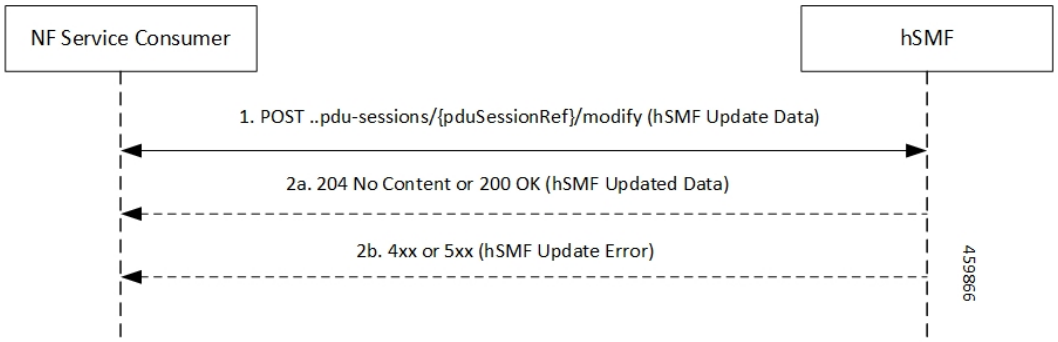



**表 *282 : hSMF* コール フローの説明に対するサービス操作の更新**

| ステップ | 説明 |
|---|---|
| 1 | vSMF などの NF サービス コンシューマは、hSMF の PDU セッション リソースを表すリソースに PDU セッションを変更するための POST 要求を送信します。 |
| 2 | PDU セッションの更新が成功した場合、hSMF は「204 No Content」または「200 OK」を NF サービス コンシューマに送信します。 |
| 3 | PDU セッションの更新が失敗した場合、hSMF は「hSMF 更新エラーの HTTP ステータス コード」の表にリストされているように、HTTP ステータス コードを送信します。4xx または 5xx 応答の場合、メッセージ本文には「cause」属性を持つ ProblemDetails 構造を含む hSMF 更新エラー構造が含まれています。 |

表 *283 : hSMF* 更新エラーの *HTTP* ステータス コード

| データ タイプ | HTTPS ステータス コード | 原因 | 詳細 | タイトル（Title） |
|---|---|---|---|---|
| hSMF アップデート エラー | 404 | CONTEXT_NOT _FOUND | PDU_Context _Not_Found | ネットワーク _Failure |

vSMF コール フローに対するサービス操作の更新

NF サービス コンシューマ（hSMF など）は、vSMF の PDU セッションを更新します。また、NF サービス コンシューマは、V-SMF が HTTP POST メソッドを使用して N1 SM シグナリングを UE に送信するために必要な情報も提供します。

ここでは、vSMF コール フローに対する更新サービス操作について説明します。

図 *164 : vSMF* コール フローに対するサービス操作の更新

表 *284 : vSMF* コール フローの説明に対するサービス操作の更新

| ステップ | 説明 |
|---|---|
| 1 | NF サービス コンシューマ（hSMF など）は、vSMF の PDU セッション リソースを表すリソースに PDU セッションを変更するための POST 要求を送信します。 |
| 2 | PDU セッションの更新が成功した場合、vSMF は「204 No Content」または「200 OK」を NF サービス コンシューマに送信します。 |
| 3 | PDU セッションの更新が失敗した場合、vSMF は「vSMF 更新エラーの HTTP ステータス コード」の表にリストされているように、HTTP ステータス コードを送信します。4xx または 5xx 応答の場合、メッセージ本文には「cause」属性を持つ ProblemDetails 構造を含む vSMF 更新エラー構造が含まれています。 |

表 *285 : vSMF* 更新エラーの *HTTP* ステータス コード

| データ タイプ | **HTTPS** ステータス コード | 原因 | 詳細 | タイトル（**Title**） |
|---|---|---|---|---|
| vSMF 更新エラー | 400 | 未指定 _NF_FAILURE | Ngap_Decode _failed | Invalid_Param |
| vSMF 更新エラー | 500 | 未指定 _NF_FAILURE | Failure_N4 _Response | ネットワーク _Failure |
| vSMF 更新エラー | 500 | SYSTEM_ 障害 | 手順 _Aborted | ネットワーク _Failure |
| vSMF 更新エラー | 500 | INSUFFICIENT_ リソース | Failed_Due_ To_Insufficient_ Resounces_At_Gnb | ネットワーク _Failure |
| vSMF 更新エラー | 400 | UNSPECIFIED_ NF_FAILURE | Qfi_Failed _List_Invalid | ネットワーク _Failure |

サポートされるステータスおよび原因コード

次の表に、この機能でサポートされているステータスと原因コードを示します。

表 *286* : サポートされるステータスおよび原因コード

| タイトル | 詳細 | HTTP ステータス | 原因 | メッセージ |
|---|---|---|---|---|
| ネットワーク障害 | UDM_Registration _Failed | 403 | SUBSCRIPTION_ DENIED | SMContext CreateError |
| ネットワーク障害 | SNSSAI_Not_ Supported_By_SMF | 403 | SNSSAI_ DENIED | |
| ネットワーク障害 | UDM_Subscription _Failed | 404 | SUBSCRIPTION_ NOT_FOUND | |
| ネットワーク障害 | SLA_Txn_Timeout | 504 | NETWORK_ 障害 | |
| ネットワーク障害 | PDU_Type_ Not_Supported _By_SMF | 403 | PDUTYPE _NOT _SUPPORTED | |
| ネットワーク障害 | UDM_Rejected _PDUTYPE | 403 | PDUTYPE _DENIED | |
| ネットワーク障害 | DDN_Not_Supported _By_SMF | 403 | DNN_NOT _SUPPORTED | |
| ネットワーク障害 | DDN_Denied_By _UDM_Or_UDM Sent_Different_ DNN | 403 | DDN_DENIED | |
| ネットワーク障害 | SSC_Not_Supported _By_SMF | 403 | SSC_NOT _SUPPORTED | |
| ネットワーク障害 | SSC_Denied_ From_UDM | 403 | SSC_DENIED | |
| ネットワーク障害 | N26_HO_Failure _N4_Response | 504 | NETWORK_ 障害 | |
| Mandatory_IE _Missing | PDU_Session_ID _Not_Sent | 400 | 必須 _IE _MISSING | |

| タイトル | 詳細 | HTTP ステータス | 原因 | メッセージ |
|---|---|---|---|---|
| ネットワーク障害 | N26_HO_Movement _Default_Bearer _Inactive | 403 | DEFAULT_EPS_ BEARER_ 非アクティブ | |
| ネットワーク障害 | Failed_Due_To _Insufficient_ Resources_At _Gnb | 500 | INSUFFICIENT _RESOURCES | SMContext UpdateError |
| ネットワーク障害 | No_Resource_Is_ Allocated_By_The _Target_NGRAN | 403 | HANDOVER_ RESOURCE_ ALLOCATION_ 障害 | |
| ネットワーク障害 | SLA_Txn_Timeout | 500 | UNSPECIFIED_ NF_FAILURE | |
| ネットワーク障害 | N2HO_N4 _Reject | 500 | UNSPECIFIED_ NF_FAILURE | |
| ネットワーク障害 | XNHO_N4_Reject | 500 | UNSPECIFIED_ NF_FAILURE | |
| ネットワーク障害 | SLA_Txn_Timeout | 500 | UNSPECIFIED_ NF_FAILURE | POST 応答 SMContext リリース |
| ネットワーク障害 | SLA_Txn_Timeout | 504 | NETWORK_ 障害 | SMContext への POST 応答 保留解除 |

## 標準準拠

ProblemDetails JSON オブジェクトのサポート機能は、次の標準に準拠しています。

- *3GPP TS 29.502-5G* システム セッション管理サービス
- *3GPP TS 29.518-5G* システム アクセスおよびモビリティ管理サービス
- *3GPP TS 29.571-5G* システム サービス ベースのインターフェイスの一般的なデータ型
- *3GPP TS 29.501-5G* システム サービス定義の原則と注意事項

# 原因情報要素

## 機能説明

SMF は、N11 インターフェイスメッセージの原因 IE をサポートしています。この機能の目的は次のとおりです。

- SMF は、受信した原因の送信と処理をサポートしています。これらは [原因 IE（Cause IE）] で使用できます。このサポートでは、SMF は 3GPP TS 29.502 バージョン 15.4.0.0、セクション 6.1.6.3.8 に準拠しています。
- SMF は、3GPP 仕様に従って、次の変更要求（CR）をサポートします。
  - 3GPP TS 29.502, CR 0097 により、新しい「INSUFFICIENT_UP_RESOURCES」原因情報を送信。
  - S3GPP TS 29.518 CR 161 は、AMF からの N1N2 メッセージ転送エラーの UE_IN_NON_ALLOWED_AREA の原因をサポートしていません。
- SMF は、N11 インターフェイスメッセージの原因に関する統計情報をサポートしています。

## 機能の仕組み

この機能は、次のサポートと連携します。

- 原因の送信と処理のサポート
- CR0097 および CR 161 の 3GPP CR サポート
- 統計のサポート

### 原因の送信と処理

SMF は、次の受信原因の送信と処理をサポートしています：

- REL_DUE_TO_HO
- EPS_FALLBACK
- REL_DUE_TO_UP_SEC
- DNN_CONGESTION
- S_NSSAI_CONGESTION
- REL_DUE_TO_REACTIVATION
- 5G_AN_NOT_RESPONDING
- REL_DUE_TO_SLICE_NOT_AVAILABLE
- REL_DUE_TO_DUPLICATE_SESSION_ID
- PDU_SESSION_STATUS_MISMATCH

- HO_FAILURE
- [INSUFFICIENT_UP_RESOURCES
- PDU_SESSION_HANDED_OVER

原因の説明とシナリオ

このセクションでは、SMF が N11 インターフェイス メッセージを介して AMF から受信する原因と、それらの原因に関連するシナリオに関する情報を提供します。

### REL_DUE_TO_HO

次の表では、引き継ぎの原因とシナリオによるリリースについて説明します。

**表 *287 :* 引き継ぎの原因とシナリオによるリリース**

| 原因 | REL_DUE_TO_HO |
|---|---|
| 3GPP TS 29.502 からの原因の説明 | 引き継ぎによるリリース |
| 発生シナリオ | ローミング中に 5GS から EPG または ePDG にハンドオーバー |
| 使用されるメッセージ | vsmfUpdateData |
| メッセージの方向 | H-SMF から V-SMF |
| コメントと仕様の参照 | 3GP TS 29.502<br>• 5.2.2.8.3v V-SMF に対するサービス操作の更新<br>• 5.2.2.8.3.4 3GPP と信頼できない非 3GPP アクセス間のハンドオーバー（5GC-N3IWF から EPS へ、または 5GS から EPC/ePDG へ）<br><br>要求の要求表示が NW_REQ_PDU_SES_REL に構成され、原因 IE がハンドオーバー原因による解放を示している場合、V-SMF は PDU セッション用に予約されている RAN リソース（存在する場合）の解放を開始します。ただし、SMF は UE に PDU セッションのリリースコマンドを送信しません。<br><br>V-SMF は PDU セッションの SM コンテキストを解放しません。<br><br>（注）<br>• SMF は、この原因に対するローミング機能をサポートしていません。<br>• この原因は、N2 の引き継ぎ後の SmContext リリース要求で利用可能です。SMF は、このシナリオをサポートします。 |

### EPS_FALLBACK

次の表に、IP マルチメディア サブシステム（IMS）音声原因の EPS フォールバックによるモビリティと、原因の発生シナリオについて示します。

**表 *288 : EPS* フォールバックによるリリース 原因とシナリオ**

| | |
|---|---|
| 原因 | EPS_FALLBACK |
| 3GPP TS 29.502 からの原因の説明 | IMS 音声に対する進行中の EPS フォールバックによるモビリティ。 |
| 発生シナリオ | ローミング シナリオにおける IMS 音声の構成 |
| 使用されるメッセージ | VsmfUpdatedData<br>このメッセージは、QosFlowItem の原因 IE である qosFlowsFailedtoAddModList 属性で使用されます。 |
| メッセージの方向 | V-SMF から H-SMF |
| コメントと仕様の参照 | SMF は、仕様に従ってこの原因について次のシナリオをサポートしています。<br>• IMS 音声の EPS フォールバックに関する 3GPP TS 23.502、Section 4.13.6.1。<br>SMF への PDU セッション応答メッセージは、AMF を介して IMS 音声の QoS フローを受信します。ローミング シナリオの場合、このメッセージは V-SMF を介して H-SMF に送信されます。NG-RAN は、IMS 音声のフォールバックによる進行中のモビリティを示す IMS 音声の QoS フローを構成するため、PDU セッションの変更を拒否します。<br>• 3GPP TS 23.502<br>3GPP TS 23.502 [3] の 4.13 項に定義されているように、IMS 音声の EPS フォールバックが原因で NG-RAN が音声 QoS フローの確立を拒否した場合、V-SMF は原因を返します。V-SMF は、qosFlowsFailedtoAddModifyList IE の対応するフローに対する IMS 音声の EPS フォールバックが原因で、原因が継続的なモビリティとして示されます。<br>（注）<br>このシナリオはローミングをサポートしていません。 |

### REL_DUE_TO_UP_SEC

次の表では、ユーザープレーンの原因と原因の発生シナリオからセキュリティ要件を満たしていないことによるリリースについて説明します。

**表 *289 :* ユーザー プレーンの原因とシナリオによるリリース**

| | |
|---|---|
| 原因 | REL_DUE_TO_UP_SEC |
| 3GPP TS 29.502 からの原因の説明 | ユーザープレーンのセキュリティ要件が満たされなかったためのリリース。 |
| 発生シナリオ | NG-RAN が必要なユーザー プレーンのセキュリティ施行を満たすことができない場合に、AMF によって開始されるリリース。 |
| 使用されるメッセージ | SM コンテキスト サービスのリリース操作 |
| メッセージの方向 | AMF から SMF へ |
| コメントまたは仕様の参照 | 3GPP 29.502、セクション 5.2.2.4、SM コンテキスト サービスのリリース<br>REL_DUE_TO_UP_SEC の原因は、NG-RAN が必要なユーザー プレーンのセキュリティ施行を履行できない場合の SM コンテキスト リリース要求で使用できます。 |

### DNN_CONGESTION

次の表では、DNN ベースの輻輳制御の原因によるリリースと、原因の発生シナリオについて説明します。

**表 *290 : DNN* 輻輳によるリリース の原因とシナリオ**

| | |
|---|---|
| 原因 | DNN_CONGESTION |
| 3GPP TS 29.502 からの原因の説明 | DNN ベースの輻輳制御によるリリース。 |
| 発生シナリオ | SMF は、要求された DNN の輻輳を検出し、PDU セッションの確立を制限する DNN の過負荷制御を実行します。 |
| 使用されるメッセージ | SM コンテキスト作成エラーおよび SM コンテキスト更新エラー |
| メッセージの方向 | SMF から AMF |
| コメントまたは仕様の参照 | 未サポート |

### S_NSSAI_CONGESTION

次の表に、S-NSSAIベースの輻輳制御の原因によるリリースと、原因の発生シナリオを示します。

**表 *291 : S NSSAI* によるリリース 原因とシナリオ**

| | |
|---|---|
| 原因 | S_NSSAI_CONGESTION |
| 3GPP TS 29.502 からの原因の説明 | S-NSSAI ベースの輻輳制御によるリリース。 |
| 発生シナリオ | SMF は、要求された S-NSSAI の輻輳を検出し、PDU セッションの確立を制限する S-NSSAI の過負荷制御を実行します。 |
| 使用されるメッセージ | SM コンテキスト作成エラーおよび SM コンテキスト更新エラー |
| メッセージの方向 | SMF から AMF |
| コメントまたは仕様の参照 | 未サポート |

### REL_DUE_TO_REACTIVATION

次の表に、PDU セッションの再アクティブ化によるリリースと、その発生シナリオを示します。

**表 *292 :* 再アクティブ化の原因とシナリオによるリリース**

| | |
|---|---|
| 原因 | REL_DUE_TO_REACTIVATION |
| 3GPP TS 29.502 からの原因の説明 | PDU セッションが再アクティブ化されたため、リリースされました。 |
| 発生シナリオ | 3GPP TS 29.502、セクション 5.2.2.3.10、AMF を介した P-CSCF 復元手順。<br>POST 要求には、True に構成されたリリース IE と REL_DUE_TO_REACTIVATION に構成された原因 IE が含まれます。 |
| 使用されるメッセージ | SM コンテキスト サービス操作の更新 |
| メッセージの方向 | AMF から SMF へ |
| コメントまたは仕様の参照 | AMF から原因を受信した後、SMF は 5GSM 原因を再アクティブ化必須として UE に送信します。 |

### 5G_AN_NOT_RESPONDING

次の表では、5Gアクセス ネットワーク（AN）がネットワークによって開始された要求に応答しない場合の原因と、原因の発生シナリオについて説明します。

表 *293 : 5G AN* が応答しないことによるリリース 原因とシナリオ

| | |
|---|---|
| 原因 | 5G_AN_NOT_RESPONDING |
| 3GPP TS 29.502 からの原因の説明 | 5G の AN は、ネットワークによって開始された要求に応答しません。 |
| 発生シナリオ | なし。 |
| 使用されるメッセージ | SM コンテキスト ステータス通知（SM Context Status Notification）またはステータス通知（SM Context Status Notification） |
| メッセージの方向 | SMF から AMF |
| コメントまたは仕様の参照 | SMF は、この原因について次のシナリオをサポートしています。<br>• ネットワークでUEがアクティブ化されると、SMF は、UE またはネットワークが開始した PDU セッションの解放中に、statusInfo の原因で SM コンテキスト ステータス通知またはステータス通知メッセージを送信します。<br>• UE PDU セッションが非アクティブ化された状態からアクティブ化されている間、SMF は gNB からの PDU RES STP RES を待ちます。GNB が AMF または SMF に応答しない場合、AMF はこの原因で DEACTIVATED として、SM コンテキスト更新を送信します。AMF は、SM コンテキストの更新サービス操作を SMF に送信します。 |

### REL_DUE_TO_SLICE_NOT_AVAILABLE

次の表に、関連する S-NSSAI 原因が利用できないことによるリリースと、原因発生のシナリオを示します。

表 *294 :* スライスが利用できないことによるリリース 原因とシナリオ

| | |
|---|---|
| 原因 | REL_DUE_TO_SLICE_NOT_AVAILABLE |
| 3GPP TS 29.502 からの原因の説明 | 関連付けられたS-NSSAIが原因でリリースできません。 |
| 発生シナリオ | 原因が発生するケースのシナリオは次のとおりです。<br>• シナリオ 1：PDU がアクティブになったときに、UDM が開始したスライス情報変更通知。<br>• シナリオ2：PDUが非アクティブ化されたときに、UDM が開始したスライス情報変更の AMF への通知。 |

| | |
|---|---|
| 使用されるメッセージ | 以下のシナリオで使用されるメッセージは以下の通りです：<br>• シナリオ1：SM コンテキスト サービス操作を更新します。<br>• シナリオ2：SM コンテキスト サービスのリリース操作。 |
| メッセージの方向 | AMF から SMF へ |
| コメントまたは仕様の参照 | SMF は、仕様に従ってこの原因について次のシナリオをサポートしています。<br>• 3GPP TS 29.502 のセクション 5.2.2.3.12 AMF は、スライスを利用できないため、PDU セッションのリリースを要求しました。<br>POST 要求には、True に構成されたリリース IE と REL_DUE_TO_SLICE_NOT_AVAILABLE に構成された原因 IE が含まれます。<br>• 3GPP TS 29.502、セクション 5.2.2.4、SM コンテキスト サービスのリリース<br>3GPP TS 23.501 [2] の 5.15.5.2.2 項で定義されているように、ネットワーク スライス インスタンスが使用できず、PDU セッションがアクティブ化されていない UE では、ネットワーク スライスのセットの変更が発生します。 |

### REL_DUE_TO_DUPLICATE_SESSION_ID

次の表に、新しい PDU セッション確立の原因の UE 要求によるリリースと、原因の発生のシナリオについて示します。

**表 *295*：セッション *ID* の重複によるリリース 原因とシナリオ**

| | |
|---|---|
| 原因 | REL_DUE_TO_DUPLICATE_SESSION_ID |
| 3GPP TS 29.502 からの原因の説明 | 同一の PDU セッション ID を使用して新しい PDU セッションを確立する UE 要求によるリリース。 |
| 発生シナリオ | PDU セッション ID が重複しているため、AMF が PDU セッションの解放を要求しました。 |
| 使用されるメッセージ | SM コンテキスト サービス操作の更新 |
| メッセージの方向 | AMF から SMF へ |

| | |
|---|---|
| コメントまたは仕様の参照 | SMF では、次のシナリオがサポートされています：<br>3GPP TS 24.501 [7] の 5.4.5.2.5 項で定義されているように、AMF が UE の PDU セッション コンテキストの既存の PDU セッション ID を持つ最初の要求を受信すると、AMF は SMF に既存の PDU セッションを解放するように要求します。SMF の SM コンテキストの削除を示す SM コンテキスト ステータス通知を受信した後、AMF は PDU セッション用に保存されているコンテキストを解放します。次に、AMF は PDU セッション ID を含む最初の要求を送信します。<br>POST 要求には、True に構成されたリリース IE と、REL_DUE_TO_DUPLICATE_SESSION_ID に構成された原因 IE が含まれます。<br>（注）<br>この手順では、SMF は PDU セッションの解放のために NAS シグナリングを UE に送信しません。 |

### PDU_SESSION_STATUS_MISMATCH

次の表に、UE と AMF 間の PDU セッション ステータスの不一致によるリリースと、原因の発生シナリオを示します。

**表 *296 : PDU* セッション ステータスの不一致によるリリースの原因とシナリオ**

| | |
|---|---|
| 原因 | PDU_SESSION_STATUS_MISMATCH |
| 3GPP TS 29.502 からの原因の説明 | UE と AMF 間の PDU セッション ステータスの不一致によるリリース。 |
| 発生シナリオ | UE サービス要求手順。 |
| 使用されるメッセージ | SM コンテキストのリリース データ |
| メッセージの方向 | AMF から SMF へ |
| コメントまたは仕様の参照 | SMF では、次のシナリオがサポートされています：<br>3GPP TS 24.501 のセクション 5.2.2.4 の「SM コンテキスト サービスのリリース」で定義されているように、UE と AMF の間で PDU セッション ステータスが一致しない場合、AMF は SMF へのリリース操作を開始して、ネットワークから PDU コンテキストを解放します。 |

### HO_FAILURE

次の表に、引き継ぎの準備が失敗する原因と、原因の発生シナリオを示します。

表 *297 : HO* 障害の原因とシナリオによるリリース

| | |
|---|---|
| 原因 | HO_FAILURE |
| 3GPP TS 29.502 からの原因の説明 | ハンドオーバーの準備に失敗しました。 |
| 発生シナリオ | N26 インターフェイスを介した 5GS から EPS へのハンドオーバーであり、試行された PDU セッションのハンドオーバーに EPS でリソースを割り当てることができない場合。 |
| 使用されるメッセージ | SM コンテキストの更新 |
| メッセージの方向 | AMF から SMF へ |
| コメントまたは仕様の参照 | SMF では、次のシナリオがサポートされています：<br>AMF は、原因属性を HO_FAILURE に構成し、EPS ベアラー コンテキストの空のリストを使用して POST 要求を送信することにより、ハンドオーバーの準備が失敗したという情報で SMF を更新します。この手順には、dataForwarding IE は含まれません。次に、SMF はハンドオーバー用に準備されたリソースを解放し、PDU セッションを続行します。 |

### [INSUFFICIENT_UP_RESOURCES

次の表に、リソース不足によるユーザープレーン接続のアクティベーションの失敗の原因と、原因の発生シナリオを示します。

表 *298 :* 稼働リソース不足によるリリース 原因とシナリオ

| | |
|---|---|
| 原因 | [INSUFFICIENT_UP_RESOURCES |
| 3GPP TS 29.502 からの原因の説明 | ユーザー プレーン リソースが不足しているため、PDU セッションのユーザー プレーン接続をアクティブ化できませんでした。 |
| 発生シナリオ | アイドル モード終了手順の実行中。 |
| 使用されるメッセージ | SM コンテキスト更新データ |
| メッセージの方向 | SMF から AMF |

| | |
|---|---|
| コメントまたは仕様の参照 | 3GPP TS 129.502、セクション 5.2.2.3.2.2、「PDU セッションのユーザー プレーン接続のアクティブ化」<br>SMF では、次のシナリオがサポートされています：<br>3GPP TS 38.413 [9] の9.3.4.16 条項で定義されているように、5G-AN は、障害の原因またはリソースが PDU セッションの確立に失敗したかどうかを含む N2 SM 情報を SMF に送信します。<br>SMF がこの情報を受信した後、SMF はユーザープレーン接続のアクティベーションが失敗したと判断し、upCnxState 属性を DEACTIVATED に構成します。<br>リソース不足が原因でユーザープレーン接続のアクティブ化が失敗した場合、原因は問題の詳細の応答に含まれ、ステータス コード 500 で INSUFFICIENT_UP_RESOURCES に構成されます。 |

### PDU_SESSION_HANDED_OVER

次の表に、PDU セッション原因の引き継ぎと原因発生のシナリオを示します。

**表 *299 : PDU* セッションのハンドオーバーによるリリース 原因とシナリオ**

| | |
|---|---|
| 原因 | PDU_SESSION_HANDED_OVER |
| 3GPP TS 29.502 からの原因の説明 | PDU セッションは別のシステムまたはアクセスに渡されました。 |
| 発生シナリオ | N26 インターフェイスを使用しない 5GC から EPS へのモビリティ<br>5GS から EPC または ePDG へのハンドオーバー |
| 使用されるメッセージ | SM コンテキスト ステータス通知 |
| メッセージの方向 | SMF から AMF |

| | |
|---|---|
| コメントまたは仕様の参照 | SMF は、この原因に対して次の仕様をサポートしています。<br>• 3GPP TS 23.502 で定義されているように、SMF はセクション 4.11.2.2 5GC から EPS モビリティへの対応をサポートしています（N26 インターフェイスなし、5GS から EPC または ePDG への 4.11.4.2 ハンドオーバー）。<br>• 3GPP TS 29.502 のセクション 5.2.2.5 SM コンテキスト ステータス通知サービス操作で定義されているように、SMF は、この通知のサブスクリプション中に NF サービス コンシューマが提供する SM コンテキスト ステータスのコールバック リファレンスに POST 要求を送信します。POST 要求のペイロード本文には、通知ペイロードが含まれています。PDU セッションのハンドオーバーによって通知がトリガされた場合、通知ペイロードには PDU_SESSION_HANDED_OVER 値を含む原因 IE が含まれます。<br>（注）<br>• SMF は、N26 インターフェイスなしの 5GC から EPS へのモビリティをサポートしていません。<br>• SMF は、5GS から EPC または ePDG へのハンドオーバー中の、この原因による SM コンテキスト ステータス通知の送信をサポートしています。 |

## *3GPP* 変更要求

SMF は、3GPP 仕様に従って、次の変更要求（CR）をサポートします。

- SMF は、3GPP TS 29.502 CR 0097 に準拠しており、AMF への「INSUFFICIENT_UP_RESOURCES」の原因の送信をサポートしています。INSUFFICIENT_UP_RESOURCES テーブルは、この原因とシナリオについて説明しています。
- SMF は、3GPP TS 29.518 CR 161 に準拠しており、AMF からの N1N2 メッセージ転送エラーの UE_IN_NON_ALLOWED_AREA の原因をサポートしていません。この転送エラーは、ゲートウェイのタイムアウトが原因で発生します。

## 統計

SMF は、AMF から受信する N11 インターフェイス メッセージに関する次の原因に関する統計情報をサポートします。

SMコンテキストのリリース要求：

- REL_DUE_TO_UP_SEC
- PDU_SESSION_STATUS_MISMATCH

SM コンテキスト更新要求（Release フラグを True に構成した場合）

- REL_DUE_TO_SLICE_NOT_AVAILABLE
- REL_DUE_TO_REACTIVATION
- REL_DUE_TO_DUPLICATE_SESSION_ID

次に、REL_DUE_TO_SLICE_NOT_AVAILABLE 原因の統計を表示する例を示します：

```
smf_service_amf_msg_total{app_name="smf",cause_code=
"REL_DUE_TO_SLICE_NOT_AVAILABLE",cluster="smf",
data_center="smf",direction="inbound",instance_id="1",message_type="pdu_session_release_request_amf",
procedure_type="PDU Session Release - AMF initiated Mod Req",service_name="smf-service"}
2
```

### 標準準拠

N11 インターフェイス機能の原因 IE サポートは、次の標準に準拠しています：

- *3GPP TS 29.502* バージョン *15.4.0.0*（セクション *6.1.6.3.8*）：*5G*。*5G* システム セッション管理サービス第 *3* 段階
- *3GPP TS 29.502*（*CR 0097*）：*5G*。*5G* システム セッション管理サービス第 *3* 段階
- *3GPP TS 29.518*（*CR 161*）：*5G*。*5G* システム アクセスおよびモビリティ管理サービス第 *3* 段階

# N16 インターフェイス

N16 インターフェイスは、ローミング シナリオにおける 2 つの SMF 間の参照ポイントです。一方の SMF は訪問先ネットワークにあり、もう一方の SMF はホーム ネットワークにあります。

SMF 間のローミングの詳細については、SMF 間のローミング （834 ページ） を参照してください。

## ProblemDetails JSON オブジェクト

### 機能説明

SMF は N11 インターフェイス上での ProblemDetails JSON オブジェクトの送受信をサポートし、ローミングをサポートします。

アプリケーション エラーは、HTTP サーバとして機能する SMF サービスが HTTP 要求を完了できない場合があります。この場合、SMF サービスはアプリケーション エラーを類似の 4xx または 5xx HTTP ステータスにマップします。

HTTP ステータス コードにより、エラーの原因が分かります。ただし、これらのステータス コードにはエラーに関する十分な情報がない場合があります。この場合、HTTP サーバとして動作している SMF サービスは、HTTP クライアントとして動作している SMF サービスに、より多くのアプリケーション関連のエラー情報を提供します。この SMF サービスは、応答本文に「ProblemDetails」データ構造の表現を含めることによって、追加情報を提供します。

3GPP 仕様では、ドキュメント形式の 1 つとして JSON が定義されています。HTTP API はこの形式を再利用して、要件に基づいてさまざまな問題のタイプを特定します。

N11 インターフェイスに指定された ProblemDetails 構造は、hSMF でのローミング コール フローのために N16 インターフェイスに送信されます。hSMF から問題の詳細を受信した後、vSMF は AMF からの対応するメッセージを拒否し、vSMF が hSMF から受信した問題の詳細を保存します。

## 機能の仕組み

ここでは、この機能の仕組みを説明します。

応答に ProblemDetails データ構造のペイロード本文が含まれている場合、SMF サービスには、「application/problem+json」に構成された「Content-Type」ヘッダー フィールドが含まれます。SMF サービスが HTTP 応答を生成します。

### 問題の詳細処理

SMF は、SMF が AMF から受信する問題の詳細構造を処理し、他の SMF にローミング サポートを提供します。

### SMF 間のローミング

ホーム SMF（hSMF）と訪問先 SMF（vSMF）が N16 インターフェイスを介して相互に通信します。次のセクションでは、hSMF および vSMF のローミング コール フローのために、N11 インターフェイスに指定された ProblemDetails 構造が N16 インターフェイスにどのように送信されるかについて説明します。

### コール フロー

このセクションでは、次のコールフローについて説明します。

- hSMF コール フローでのサービス操作の作成
- vSMF コール フローでのサービス操作の作成
- hSMF コール フローに対するサービス操作の更新
- vSMF コール フローに対するサービス操作の更新

#### hSMF コール フローでのサービス操作の作成

作成サービス操作は、hSMF においてホームルーティング ローミング シナリオ用の PDU セッションを作成します。vSMF などの NF サービス コンシューマは、HTTP POST メソッドを使用して PDU コンテキストを作成します。

このセクションでは、hSMF でサービス オペレーションの作成のコール フローについて説明します。

**図 *165 : hSMF* コール フローでのサービス操作の作成**

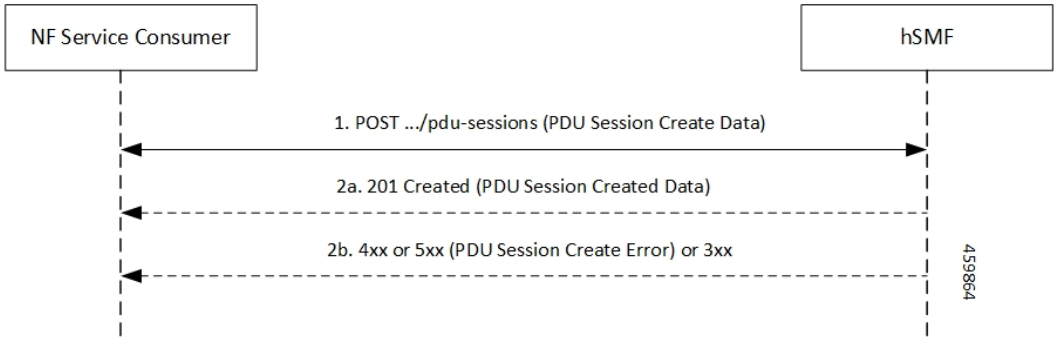



**表 *300 : vSMF* コール フローの説明にサービス操作を作成**

| ステップ | 説明 |
|---|---|
| 1 | vSMF などの NF サービス コンシューマが POST 要求を送信して、hSMF で PDU セッションを作成します。 |
| 2 | PDU セッションの作成が成功すると、hSMF は「201 Created」を NF サービス コンシューマに送信します。 |
| 3 | PDU セッションの確立が失敗した場合、hSMF は、「PDU セッション作成エラーの HTTP ステータス コード」の表にリストされているように、HTTP ステータス コードを送信します。4xx または 5xx 応答の場合、メッセージ本文には「cause」属性を持つ ProblemDetails 構造を含む PDU セッション作成エラー構造が含まれています。 |

**表 *301 : PDU* セッション作成エラーの *HTTP* ステータス コード**

| データ タイプ | HTTPS ステータス コード | 原因 | 詳細 | タイトル（Title） |
|---|---|---|---|---|
| PDU セッション作成エラー | 403 | サブスクリプション _DENIED | UDM_Subscription _Fetch_Failed | ネットワーク _Failure |
| PDU セッション作成エラー | 403 | SNSSAI_ DENIED | SNSSAI_Not_ Supported_By_SMF | ネットワーク _Failure |

| データ タイプ | HTTPS ステータス コード | 原因 | 詳細 | タイトル（Title） |
|---|---|---|---|---|
| PDU セッション作成エラー | 500 | 未指定 _NF_FAILURE | UDM_Notification _Failed | ネットワーク _Failure |
| PDU セッション作成エラー | 404 | サブスクリプション _NOT_FOUND | UDM_Subscription _Failed | ネットワーク _Failure |
| PDU セッション作成エラー | 504 | NETWORK_ 障害 | SLA_Txn _Timeout | ネットワーク _Failure |
| PDU セッション作成エラー | 403 | DNN_DENIED | DNN_Not_Subscribed | ネットワーク _Failure |
| PDU セッション作成エラー | 403 | SSC_NOT_ サポート対象 | SSC_Mode_Not _Supported_By_SMF | ネットワーク _Failure |
| PDU セッション作成エラー | 403 | SSC_DENIED | SSC_Mode_Denied _From_UDM | ネットワーク _Failure |
| PDU セッション作成エラー | 403 | PDUTYPE_DENIED | UDM_Rejected _PDU_Type | ネットワーク _Failure |

## vSMF コール フローでのサービス操作の作成

Create SM Context service 操作を行うと、ホーム ルーティング ローミングの場合に、SMF または vSMF のいずれかで PDU セッションの SM コンテキストが作成されます。AMF などの NF サービス コンシューマは、HTTP POST メソッドを使用して SM コンテキストを作成します。

このセクションでは、vSMF でサービス オペレーションの作成のコール フローについて説明します。

図 *166 : vSMF* コール フローでのサービス操作の作成

表 *302 : vSMF* コール フローの説明にサービス操作を作成

| ステップ | 説明 |
|---|---|
| 1 | AMF などの NF サービス コンシューマは、vSMF の SM コンテキスト収集リソースを表すリソースに SM コンテキストを作成するための POST 要求を送信します。 |
| 2 | PDU セッションの作成が成功すると、SMF は「201 Created」を NF サービス コンシューマに送信します。 |
| 3 | PDU セッションの確立が失敗した場合、SMF は、「SM コンテキスト作成エラーの HTTP ステータス コード」の表にリストされているように、HTTP ステータス コードを送信します。NF サービス コンシューマへの 4xx 応答または 5xx 応答では、メッセージ本文には「cause」属性を持つ ProblemDetails 構造を含む SM コンテキスト作成エラー構造が含まれます。 |

表 *303 : SM* コンテキスト作成エラーの *HTTP* ステータス コード

| データ タイプ | HTTPS ステータス コード | 原因 | 詳細 | タイトル（Title） |
|---|---|---|---|---|
| SM コンテキスト作成エラー | 403 | PDUTYPE_ NOT_SUPPORTED | PDU_Type_Not _Supported_ By_SMF | ネットワーク _Failure |
| SM コンテキスト作成エラー | 500 | REQUEST_ REJECTED_ 未指定 | Charging_Response _Failure | ネットワーク _Failure |
| SM コンテキスト作成エラー | 504 | NETWORK_ 障害 | SLA_txn _timeout | ネットワーク _Failure |

| データ タイプ | HTTPS ステータス コード | 原因 | 詳細 | タイトル（Title） |
|---|---|---|---|---|
| SM コンテキスト作成エラー | 400 | MANDTORY_IE _MISSING | PDU_Session_ ID_Not_Sent | Mandatory_IE _Missing |

hSMF コール フローに対するサービス操作の更新

NF サービス コンシューマ（vSMF など）は、hSMF の PDU セッションを更新します。また、NF サービス コンシューマは、NF サービス コンシューマが UE からの N1 SM シグナリングで vSMF から受信する情報を hSMF に提供します。NF サービス コンシューマは、HTTP POST メソッドを使用してこの情報を受信します。

ここでは、hSMF コール フローに対する更新サービス操作について説明します。

**図 *167 : hSMF* コール フローに対するサービス操作の更新**

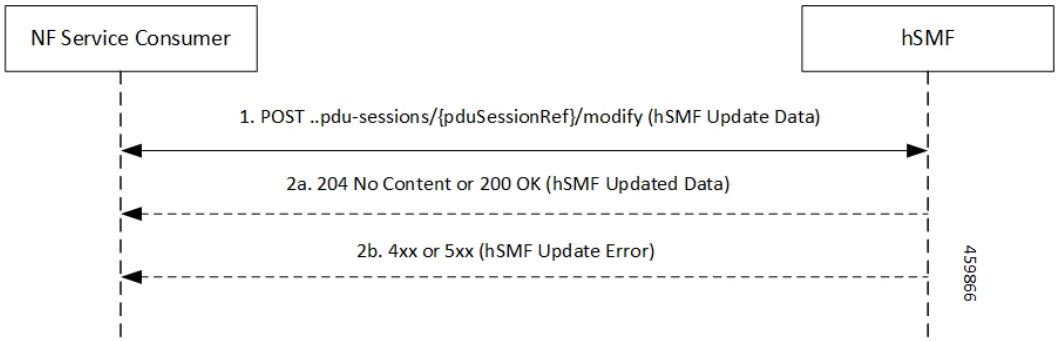



**表 *304 : hSMF* コール フローの説明に対するサービス操作の更新**

| ステップ | 説明 |
|---|---|
| 1 | vSMF などの NF サービス コンシューマは、hSMF の PDU セッション リソースを表すリソースに PDU セッションを変更するための POST 要求を送信します。 |
| 2 | PDU セッションの更新が成功した場合、hSMF は「204 No Content」または「200 OK」を NF サービス コンシューマに送信します。 |
| 3 | PDU セッションの更新が失敗した場合、hSMF は「hSMF 更新エラーの HTTP ステータス コード」の表にリストされているように、HTTP ステータス コードを送信します。4xx または 5xx 応答の場合、メッセージ本文には「cause」属性を持つ ProblemDetails 構造を含む hSMF 更新エラー構造が含まれています。 |

表 *305 : hSMF* 更新エラーの *HTTP* ステータス コード

| データ タイプ | HTTPS ステータス コード | 原因 | 詳細 | タイトル（Title） |
|---|---|---|---|---|
| hSMF アップデート エラー | 404 | CONTEXT_NOT_FOUND | PDU_Context_Not_Found | ネットワーク_Failure |

vSMF コール フローに対するサービス操作の更新

NF サービス コンシューマ（hSMF など）は、vSMF の PDU セッションを更新します。また、NF サービス コンシューマは、V-SMF が HTTP POST メソッドを使用して N1 SM シグナリングを UE に送信するために必要な情報も提供します。

ここでは、vSMF コール フローに対する更新サービス操作について説明します。

図 *168 : vSMF* コール フローに対するサービス操作の更新

表 *306 : vSMF* コール フローの説明に対するサービス操作の更新

| ステップ | 説明 |
|---|---|
| 1 | NF サービス コンシューマ（hSMF など）は、vSMF の PDU セッション リソースを表すリソースに PDU セッションを変更するための POST 要求を送信します。 |
| 2 | PDU セッションの更新が成功した場合、vSMF は「204 No Content」または「200 OK」を NF サービス コンシューマに送信します。 |
| 3 | PDU セッションの更新が失敗した場合、vSMF は「vSMF 更新エラーの HTTP ステータス コード」の表にリストされているように、HTTP ステータス コードを送信します。4xx または 5xx 応答の場合、メッセージ本文には「cause」属性を持つ ProblemDetails 構造を含む vSMF 更新エラー構造が含まれています。 |

表 *307 : vSMF* 更新エラーの *HTTP* ステータス コード

| データ タイプ | HTTPS ステータス コード | 原因 | 詳細 | タイトル（Title） |
|---|---|---|---|---|
| vSMF 更新エラー | 400 | 未指定<br>_NF_FAILURE | Ngap_Decode<br>_failed | Invalid_Param |
| vSMF 更新エラー | 500 | 未指定<br>_NF_FAILURE | Failure_N4<br>_Response | ネットワーク<br>_Failure |
| vSMF 更新エラー | 500 | SYSTEM_<br>障害 | 手順<br>_Aborted | ネットワーク<br>_Failure |
| vSMF 更新エラー | 500 | INSUFFICIENT_<br>リソース | Failed_Due_<br>To_Insufficient_<br>Resounces_At_Gnb | ネットワーク<br>_Failure |
| vSMF 更新エラー | 400 | UNSPECIFIED_<br>NF_FAILURE | Qfi_Failed<br>_List_Invalid | ネットワーク<br>_Failure |

# N40 インターフェイス

N40 インターフェイスは、SMF と課金機能（CHF）間の参照ポイントです。SMF と CHF 間の通信により、オンラインおよびオフラインでの充電が可能になります。

N40 インターフェイスは HPLMN の SMF と CHF の間に配置されているため、ホーム ルーティング ローミングと非ローミングのシナリオは同じ方法でサポートされます。

# Nnrf インターフェイス

NF 管理の場合、ネットワーク リポジトリ機能（NRF）システムは、HTTP2 ベースの Nnrf サービスベースのインターフェイス（SBI）を介してサービス処理機能を提供します。Nnrf インターフェイスは、3GPP 5G システム アーキテクチャ上の NRF によって表示されます。NRF は、次のサービス処理機能を提供します：

- NFサービス登録：NFインスタンスが提供する 5G コア サービス情報を管理します。
- NF サービス検出：5G コア SBI をサポートする NF インスタンス情報を提供します。
- アクセス トークン：5G コア サービスを使用するための認証および承認トークンを提供します。

# NRF メッセージの構成ベースの制御

## 機能説明

SMFは、オペレータが NRF メッセージにオプションの情報要素（IE）を包含するか除外するかを選択する柔軟性を提供します（例：NRF メッセージの地域情報など）オペレータは、CLI 構成コマンドを使用して IE を選択できます。

SMF は、NRF メッセージ処理プロファイル構成で **skip optional-ies locality** CLI コマンドを送信して、NRF 登録メッセージと NRF 更新メッセージで地理情報パラメータを送信しないようにします。

NRF メッセージは、次のメッセージの組み合わせです。

- nf-deregister
- nf-list-retrieval
- nf-profile-retrieval
- nf-register
- nf-status-notify
- nf-status-subscribe
- nf-status-unsubscribe
- nf-update

構成コマンドの詳細については、オプションの IE に対する制御の構成 （863 ページ） セクションを参照してください。

## 機能設定

NRF メッセージを構成ベースで制御する機能には、次の手順が含まれます：

1. メッセージ処理プロファイルの構成 （862 ページ）
2. オプションの IE に対する制御の構成 （863 ページ）

### メッセージ処理プロファイルの構成

NRF メッセージ処理プロファイルを構成するには、次の構成例を使用します。

```
config
  profile message-handling message_handling_profile_name
    nf-type nf_type_name
    mh-profile message_handling_profile_name
    end
```

注：

- **nf-type** *nf_type_name*：NRF として NF タイプを指定します。 *profile_name* は、対応する NRF プロファイル名を表す英数字の文字列を指定する必要があります。

- **mh-profile** *message_handling_profile_name*：NRF メッセージのメッセージ処理プロファイル名を指定します。

## 設定の確認

UDM メッセージ処理プロファイルが構成されているかどうかを確認するには、次のコマンドを使用します。

**show running-config profile message-handling nf-type nrf mh-profile**

メッセージ処理プロファイルが構成されている場合、この値は、 **message-handling-profile** 構成の一部として次の出力に表示されます。

```
smf(config)# show running-config profile message-handling nf-type nrf mh-profile
 message-handling-profile mhnrf
 exit
```

## オプションの *IE* に対する制御の構成

オプションの IE をスキップするように制御を構成するには、次の構成例を使用します：

```
config
  profile message-handling message_handling_name
    nf-type nrf
      mh-profile mh_profile_name
        service name type { nnrf-at | nnrf-bs | nnrf-nfd | nnrf-nfm
}
          message type { nf-deregister | nf-list-retrieval |
nf-profile-retrieval | nf-register | nf-status-notify |
nf-status-subscribe | nf-status-unsubscribe | nf-updatenf-register }
            skip optional-ies locality
            end
```

**注**：

- **mh-profile** *mh_profile_name* ：NRFメッセージ処理プロファイル構成を指定します。
- **service name type { nnrf-at | nnrf-bs | nnrf-nfd | nnrf-nfm }**：NRF サービス名のタイプを、nnrf-at、nnrf-bs、nnrf-nfd、および nnrf-nfm と指定します。
- **message type { nf-deregister | nf-list-retrieval | nf-profile-retrieval | nf-register | nf-status-notify | nf-status-subscribe | nf-status-unsubscribe | nf-update | nf-register }**：メッセージ タイプを NF 登録解除、NF リスト取得、NF プロファイル取得、NF 登録、NF ステータス通知、NF ステータス サブスクライブ、NF ステータス登録解除、NF 更新、および NF 登録として指定します。
- **skip optional-ies locality**：選択した NRF メッセージに対してスキップする locality パラメータを指定します。

（注） デフォルトでは、SMF はNRF 登録または更新メッセージで**locality** パラメータを送信します。 **profile message-handling** *message_handing_name* CLI コマンドは、NRF メッセージで**locality** パラメータの送信をスキップするプロビジョニングを提供します。

設定の確認

オプションの IE をスキップする制御が構成されているかどうかを確認するには、Exec モードで次のコマンドを使用します。

**show running-config profile message-handling nf-type nrf**

また、グローバル構成モードで次の show コマンドを使用して機能構成を確認することもできます。

**show full-configuration profile message-handling nf-type nrf**

**show running-config profile message-handling nf-type nrf** コマンドの出力例を次に示します。

```
[smf] smf# show running-config profile message-handling nf-type pcf
profile message-handling nf-type nrf
 mh-profile mhnrf
  service name type nnrf-nf
   message type nf-register
    skip optional-ies locality
   exit
exit
```

上記の例では、SMF の **skip optional-ies locality** 構成が有効になっており、NRF メッセージの局元性に関するオプションの IE をスキップしています。

# RADIUS インターフェイス

Remote Authentication Dial-In User ServiceRADIUS）は、ネットワーク アクセスを管理するプロトコルです。このプロトコルは、ネットワーク サービスに接続し使用するユーザー向けに、一元化された認証、認可、およびアカウンティング（AAA）管理を提供します。

認証と認可の場合、アクセス ログイン情報を使用してネットワーク リソースにアクセスする要求をユーザが NAS に送信すると、クレデンシャルがリンク層プロトコルを介して NAS デバイスに渡されます。たとえば、Point-to-Point Protocol（PPP）：その後、NAS から RADIUS サーバに RADIUS アクセス要求メッセージが送信され、RADIUS プロトコルを介してアクセスを許可できるように要求されます。

アカウンティングの場合、NAS がユーザーにネットワーク アクセスを許可すると、NAS から RADIUS サーバーにアカウンティング開始パケットが送信され、ユーザーのネットワーク アクセスの開始が通知されます。

# S2b インターフェイス

ワイヤレス アプリケーションでは、S2b インターフェイスはパケット データ ネットワーク ゲートウェイ（PGW）と Evolved Packet Data Gateway（ePDG）間の 4G インターフェイスです。このインターフェイスは UE と PGW の間に WLAN セッションを確立するために PMIPv6 プロトコルを使用します。

# S5 インターフェイス

S5 インターフェイスは、サービング ゲートウェイ（SGW）と PDN ゲートウェイ間のユーザープレーン トンネリングとトンネル管理を提供します。これは、UE モビリティによる SGW の再配置に使用され、また、SGW が必要な PDN 接続のために非コロケーション PDN ゲートウェイに接続する必要がある場合に使用されます。

### S5 および S8 インターフェイス

S5 インターフェイスと S8 インターフェイスの両方が LTE の Evolved Packet Core（EPC）内で使用され、SGW と PGW の間に存在します。機能に基づいて、S5 と S8 はどちらも同じインターフェイスですが、S5 インターフェイスがネットワークの内部であるのに対して、S8 インターフェイスは異なるオペレータ間をローミングするときに使用されます。

# SBA インターフェイス

5G アーキテクチャは、サービスベース アーキテクチャ（SBA）に基づいています。このアーキテクチャは、複数のソースおよびサプライヤのコンポーネントを使用して共通のアプリケーションを展開できるモジュラ フレームワークを提供します。3GPP は、SMF などの相互接続されたネットワーク機能（NF）のセットによって提供される 5G コア ネットワークの SBA を定義します。ネットワーク機能は、他のネットワーク機能のサービスにアクセスできます。

NF は、サービスベースのインターフェイス（SBI）を介して相互に通信します。SBI は、HTTP/2 プロトコルを使用するアプリケーションプログラミング インターフェイス（API）ベースの通信（REST インターフェイス）です。

## TLS を使用した HTTP/2

### 機能説明

SBA インターフェイスの HTTP/2 TLS サポート機能により、PCF、AMF など、他の NF へのすべての SBA インターフェイスに対して TLS セキュア チャネルを介した SMF のサポートが可能になります。

この機能は、次の機能をサポートしています。

- SBA インターフェイスで HTTPS（Hypertext Transfer Protocol Secure）ポートを構成するための CLI サポート。

- SMF では、トランスポート層保護とすべてのインバウンドおよびアウトバウンド HTTP/2 トランスポートに TLS バージョン 1.2 が使用されます。
- 各 SBA インターフェイスの TLS 証明書を入力するための CLI サポート。
- 他の NF へのすべての SBA インターフェイス用の TLS セキュア チャネルを介した HTTP/2。

**Note** SMF では、下位互換性のために TLS なしの HTTP もサポートされています。これはデフォルトの動作です。

- SMF のサーバーおよびクライアント HTTPS 要求。
- 署名付き証明書が使用できない場合、デフォルトの動作では、自己署名証明書がサポートされます。

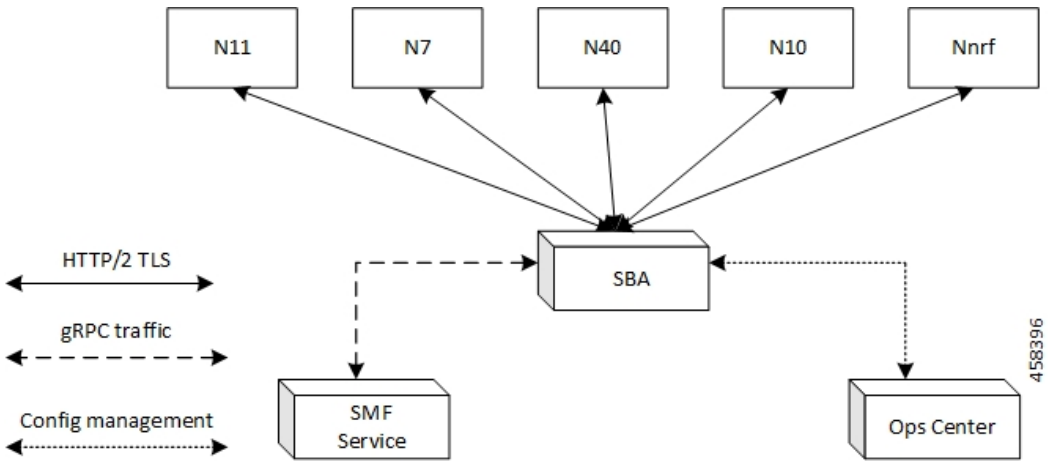
**Note** 現在、構成された証明書の保持はサポートされていません。

- 証明書の有効期限が近づいたら、適切なアラームを生成します。

## アーキテクチャ

SMF Ops Center では、すべてのアウトバウンドインターフェイス（N7、N10、N11、N40、Nnrf など）で TLS が有効になっている HTTP/2 REST エンドポイントがサポートされています。マルチベンダー サポートが必要な場合、各 NF エンドポイントは個別に TLS 証明書を選択できます。

***Figure 169: SBA インターフェイスでの SMF HTTP2 TLS サポート***



## SBA インターフェイスの HTTP/2 TLS の構成

このセクションでは、SBA インターフェイスの HTTP/2 TLS サポートを構成するためのコマンドについて説明します。

### CA 証明書の構成

CA 証明書を構成するには、次の構成例を使用します：

```
config
   nf-tls ca-certificates certificate_name
      cert-data certificate_data
   exit
exit
```

注：

- **nf-tls ca-certificates** *certificate_name*：CA 証明書名を指定します。
- **cert-data** *certificate_data*：CA 証明書データを PEM 形式で指定します。

### サーバーまたはクライアント証明書の構成

次の構成例を使用して、サーバーまたはクライアント証明書を構成します。

```
config
   nf-tls certificates certificate_name
      cert-data certificate_data
      private-key certificate_private_key
   exit
exit
```

注：

- **nf-tls ca-certificates** *certificate_name*：CA 証明書名を指定します。
- **cert-data** *certificate data*：CA 証明書データを PEM 形式で指定します。
- **private-key** *certificate_private_key*：PKCS 8 形式で CA 証明書の秘密キーを指定します。

証明書から秘密キーを取得するには、次の手順を実行します：

1. PEM から PKCS12 形式に変換する必要があります。

   ```
   openssl pkcs12 -export -out pkcscertificate.p12 -inkey certificatekey.pem
   in inputcertificate.pem
   ```

2. 前のステップで作成した PKCS12 証明書から秘密キーを抽出します。

   ```
   openssl pkcs12 -in pkcscertificate.p12 nocerts -nodes -out privatekey.pem
   ```

3. 秘密キーを PKCS8 キーに変換します。

   ```
   openssl pkcs8 -in privatekey.pem -topk8 -nocrypt -out privatekey.p8
   ```

HTTPS を有効にするには、rest-endpoint uri-scheme を HTTPS に構成します。uri-scheme のデフォルト値は HTTP です。uri-scheme が HTTPS として構成されている場合、SMF にはサーバー証明書名が必要です。

### インターフェイスへの構成済み証明書の関連付け

インターフェイスに構成された証明書を関連付けるには、次の構成例を使用します。構成された証明書名は、 **nf-tls certificates** CLI コマンドを使用して表示できます。

```
config
  endpoint sbi certificate-name configured_certificate_name
  exit
exit
```

注：

- **endpoint sbi certificate-name** *configured_certificate_name*：構成されている証明書名のリストを表示します。

SMF は、SBI メッセージにサーバー証明書名を使用します。これらの証明書は、smf-rest-ep ポッドの起動時に使用され、REST SBI サーバーの SSL コンテキストを構成します。クライアントとしての SMF が N7、N10、nNRF 要求などの要求を開始すると、エンドポイントプロファイルにプロトコルが記述されます。

### SBI インターフェイスの相互 TLS の構成

SBI インターフェイスの相互 TLS を構成するには、次の構成例を使用します：

```
config
  instance instance-id instance_id
    endpoint sbi
      interface [ bfd | bgp | coa-nas | geo-external | geo-internal
| gtpu | n4 | n7 | n10 | n11 | n16 | n40 | nrf | s2b | s5 | s5e | s8 |
 s11 | sxa | x1 | x2 ]
        mtls-enable [ true | false ]
         certificate name [ clientCert | prem-server-cert | serverCert
 | x1client | x1server ]
        end
```

注：

- **endpoint sbi**：LI インターフェイスのエンドポイントを構成します。
- **interface [ bfd | bgp | coa-nas | geo-external | geo-internal | gtpu | n4 | n7 | n10 | n11 | n16 | n40 | nrf | s2b | s5 | s5e | s8 | s11 | sxa | x1 | x2 ]** ：設定されたエンドポイントの SBI インターフェイスを指定します。
- **mtls-enable [ true | false ]** ：セキュリティ コンプライアンスを目的として、ノード間にトランスポート層の暗号化を提供するように mTLS を設定します。デフォルトでは、 の値 **mtls-enable** は に構成されています **false** 。
- **certificate name [ clientCert | prem-server-cert | serverCert | x1client | x1server ]**：使用可能なオプションから証明書のエイリアス名を指定します。SMF では、HTTPS メッセージに

証明書名が使用されます。証明書名は、REST-EP ポッドの起動時に使用され、SBI インターフェイスでメッセージが交換されるときに SSL コンテキストと TLS ハンドシェイクを構成します。

### 構成した証明書の確認

**show running-config endpoint sbi** コマンドを使用して、SBA インターフェイスで構成された証明書を確認します。

**show running-config endpoint sbi** コマンドの出力例を次に示します。

```
smf# show running-config endpoint sbi
  endpoint sbi
    replicas         2
    uri-scheme       https
    certificate-name smf-server
    vip-ip 209.165.200.225
  exit
```

### モニタリングおよびトラブルシューティング

このセクションには、機能操作時に発生する可能性がある問題のトラブルシューティングに関する情報が記載されています。

SMF は、トレース ログ、イベント ログなどのさまざまなログを保持します。メッセージ ルーティングの障害に関連する問題については、データストア ポッドの正常性とログを確認します。この機能の問題をデバッグするには、diameter-ep-rx およびデータストアまたはセッション DB ポッドのログの情報を使用します。

#### show nf-tls certificate-status

構成されている証明書のリストと残りの有効期間（日数）を表示するには、次のコマンドを使用します：

```
show nf-tls certificate-status
```

出力の例を以下に示します。

```
CERTIFICATE
NAME         DAYS
--------------------
ca           3631
smf-server   355
smfclient    355
```

# SCP インターフェイス

サービス通信プロキシ（SCP）は、ネットワーク コアですべてのシグナリングとコントロール プレーン メッセージを仲介するルーティング コントロール ポイントです。SCP はネットワーク リポジトリ機能（NRF）への NF ディスカバリ要求のルーティングの最適化、ロードバランシング、トラフィックの優先順位付け、およびメッセージ管理を行います。

### NF および NF サービスの連携動作の通信モデル

3GPP 5GC 拡張 SBA（eSBA）ネットワークの場合、3GPP は NF サービスと NF サービス（コンシューマ NF とプロデューサー NF）が相互に作用するために使用できる 4 つの通信モデルを定義します。これらの通信モデルは、モデル A、B、C、および D です。

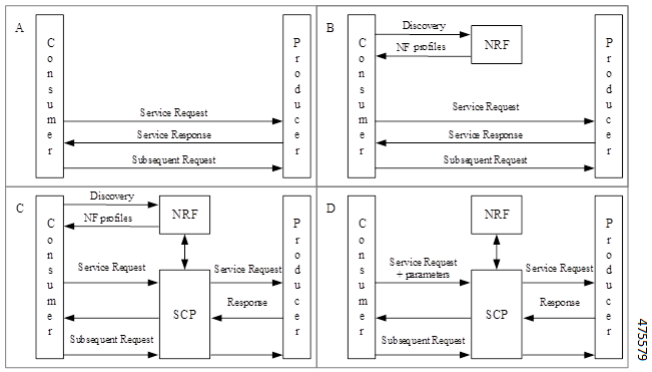
（注） SMF は、モデル A、B、および D をサポートします。

次の表に、通信モデル、それらの使用法、および SCP の使用法との関連性を示します。

**表 *308 : NF* および *NF* サービスの連携動作の通信モデル**

| コンシューマ NF とプロデューサ NF 間の通信 | サービスの発見と要求のルーティング | コミュニケーション モデル |
|---|---|---|
| ダイレクト通信 | NRF または SCP なし。ダイレクト ルーティング | A |
| | NRF サービスを使用した検出（SCP なし）。ダイレクト ルーティング | B |
| 間接的な通信 | NRF サービスを使用した検出。セットから特定のインスタンスの選択を SCP に委任できます。ルーティングは SCP を介して行われます。 | C |
| | サービス要求の検出および選択パラメータを使用して SCP に委任された検出と関連する選択。ルーティングは SCP を介して行われます。 | D |

**図 *170 : NF* および *NF* サービスの連携動作の通信モデル**



モデル A では、NRF の相互作用のない直接通信があります。NRF または SCP は使用されません。コンシューマはプロデューサ NF プロファイルを使用して構成され、任意のプロデューサと直接通信します。

モデル B では、NRF 相互作用による直接通信があります。コンシューマは、NRF をクエリして検出を実行します。検出結果に基づいて、コンシューマが選択を行います。コンシューマは、選択したプロデューサにリクエストを送信します。

モデル C では、委任されたディスカバリを使用しない間接的な通信があります。コンシューマは、NRF をクエリして検出を実行します。検出結果に基づいて、コンシューマは NF セットまたは NF セットの特定の NF インスタンスを選択します。コンシューマは、NF サービス インスタンスまたは NF サービス インスタンスのセットを指す選択されたサービス プロデューサのアドレスを含む要求を SCP に送信します。SCP は、選択した NF サービス プロデューサ インスタンスに要求をルーティングします。

モデル D では、委任されたディスカバリとの間接的な通信があります。コンシューマは、検出または選択を実行しません。コンシューマは、必要な発見および選択パラメータを追加して、サービス要求に適切なプロデューサを見つけます。SCP は、要求メッセージの要求アドレスと検出および選択パラメータを使用して、要求を適切なプロデューサ インスタンスにルーティングします。SCP は NRF を使用して検出を実行し、検出結果を取得できます。

# SCP モデル D による NF の間接通信

## 機能説明

表 *309 :* 機能の履歴

| 機能名 | リリース情報 | 説明 |
|---|---|---|
| ピア ノード通信用サービス通信プロキシ（SCP）モデル D | 2025.01.0 | SCP は、ネットワーク コアですべてのシグナリングとコントロール プレーン メッセージを仲介するルーティング コントロール ポイントです。SCP はネットワーク リポジトリ機能（NRF）への NF ディスカバリ要求のルーティングの最適化、ロード バランシング、トラフィックの優先順位付け、およびメッセージ管理を行います。<br>導入されたコマンド：<br>**nf-selection-model** *nf_model_priority* **[ local \| nrf-query \| scp ]** ：NF ピア通信の NF モデルとその優先順位の選択に使用されます。<br>**デフォルト設定**：無効：構成が必要 |

SMF はモデル D を介してネットワーク機能（NF）の間接通信を実行します。デフォルトでは、SMF は NF ピア（PCF、CHF、AMF など）を選択するために NRF 探索を実行します。NRF 検出が失敗し、ローカル構成がピアに対して使用可能な場合、SMF はローカルに設定されたピアを選択します。

（注） ネットワークでは、SMF は理論上 12 個の SCP をサポートし、実際のシナリオでは最大 5 個の SCP をサポートします。

## 機能の仕組み

SCP モデル D のサポートにより、SMF は SCP エンドポイントに要求を送信します。SCP は NRF ディスカバリを実行して正しいピア NF を見つけ、要求を NF に送信します。NRF ディスカバリの場合、HTTP ヘッダーでディスカバリ パラメータが送信されます。

モデル D による間接通信は、ピア タイプごと、および優先順位ごとに構成できます。モデル A、B、D の優先順位は構成できます。

標準準拠

SCP モデル D 機能による NF の間接通信は、次の標準に準拠しています：

- *3GPP TS 29.500*、バージョン *16.9.0*。

### サポートされる HTTP ヘッダー

*3gpp-Sbi-Discovery* ヘッダー

モデル D を構成した場合、SMF は NF 検出をトリガーせず、ピア選択のために検出パラメータを含むメッセージを SCP に送信します。

デフォルトでは、SUPI とターゲット NF タイプが追加されます。SMF には、次の形式でネットワーク要素プロファイルに構成されている各クエリ パラメータの 3gpp-Sbi-Discovery HTTP ヘッダーが含まれます。

```
3gpp-Sbi-Discovery-<query-param>
```

次に、3gpp-Sbi-Discovery ヘッダーの例を示します：

```
3gpp-Sbi-Discovery-dnn: internet
3gpp-Sbi-Discovery-snssais: [{"sst": 1, "sd": "A08923"}, {"sst": 1, "sd": "0023F1"}]
```

（注）
- **3gpp-Sbi-Discovery-target-plmn** と **3gpp-Sbi-Discovery-source-plmn** の両方が常に PLMN 間ディスカバリに含まれます。しかし、このパラメータはサポートされていません。
- 3gpp-Sbi-Discovery-supi ヘッダーをすべてのメッセージに追加する必要がある。

認証局ヘッダー

SMF は、SCP へのメッセージに authority HTTPP ヘッダーを含めます。このヘッダーは、次の場合に入力されます：

- スキームが構成から「https」である場合、権限ヘッダーはエンドポイント名の構成から FQDN を伝送します。
- スキームが「http」の場合、認証局は FQDN または IP アドレスを伝送します。IP アドレス構成が優先されます。

*3gpp-Sbi-Target-apiRoot* ヘッダー

SMF はピア NF に通知を送信する際に、「target api」の「api root」を「scp api root」に置き換え、「3gpp-sbi-target-apiRoot」ヘッダーに「target api root」を含めます。

たとえば、SMF が「POST *https://scp.com/a/b/c/notification*」という通知を SCP に送信する場合、「3gpp-sbi-target-apiRoot」ヘッダーは「*https://*「POST https://example.com/a/b/c/notification 」の

際に、SCP は「3gpp-sbi-target-apiRoot」ヘッダーを含めずに、要求「POST https://example.com/a/b/c/notification」を NF サービス プロデューサーに送信します。

（注） SMF は SCP「apiPrefix」をサポートしていません。

SMF は、特定のセッションに関するピア NF への最初の要求に、「3gpp-sbi-target-apiRoot」ヘッダーを含めません。SMF は、応答の「location」ヘッダーからリソースの「target api」プレフィックスを抽出します。次に、SMF は、同じセッションのピア NF への後続のメッセージの「3gpp-sbi-target-apiRoot」ヘッダーにこのプレフィックスを含めます。

たとえば、SMF が N7 作成応答で次の「location」ヘッダーを受信した場合、

*http://209.165.200.230:9082/npcf-smpolicycontrol/v1/sm-policies/ism.14.imsi-310260157090153.1660028704.43993.7129768994171956185*

その後、SMF は次の SMPolicy 更新メッセージを送信します。

*http://scpIP:port/npcf-smpolicycontrol/v1/sm-policies/ism.14.imsi-310260157090153.1660028704.43993.7129768994171956185*

ここで、

「authority header」は「scpIP」です

「3gpp-sbi-target-apiRoot」は 209.165.200.230:9082 です

（注） SMF ではまた、ピアがすでに作成したリソースで動作することを目的としたメッセージに、「3gpp-sbi-target-apiRoot」ヘッダーが含まれます。たとえば、SMF が N10 登録解除メッセージを UDM に送信する場合、SMF は、N10 登録応答で受信する「location」ヘッダーを使用して、「3gpp-sbi-target-apiRoot」ヘッダーを設定します。

### *3gpp-Sbi-Callback* ヘッダー

SMF は、コールバック要求内の「3gpp-Sbi-Callback」ヘッダーに SCP のコールバック サービス名を入力し、差別化されたサービスを提供します。

次に、このヘッダーの形式を示します：

「N<NF>_<service name>_<name of the callback service operation in the corresponding OpenAPI specification file>」

例の一部を次に示します：

- AMFへの通知は「Nsmf_PDUSession_smContextStatusNotification」として送信されます
- vSMF への通知は「Nsmf_PDUSession_StatusNotify」として送信されます

### サーバー ヘッダー

SMF は、エラーの原因に関する情報のために、ピア NF へのすべてのエラー応答に「Server」ヘッダーを含めます。次に、このヘッダーの形式を示します。

UDM：「nf-instance-id」

例：UDM："54804518-4191-46b3-955c-ac631f953ed8"

エラー応答を受信すると、クライアントとしての SMF は「Server」ヘッダーから NFType を抽出し、SCP 障害処理をトリガーします。モデル D が構成されていて、「Server」ヘッダーが NF ピアを示している場合、SMF は「再試行」失敗処理アクションを無視します。SCP 障害処理として「再試行フォールバック」を設定している場合、SMF は再試行アクションなしでローカル構成にフォールバックします。SMF フォールバックの後、障害が NF 障害処理の構成に従って処理されます。

（注）

- 「サーバー」ヘッダーが受信されなかった場合、またはタイムアウトが発生した場合は、SCP の失敗の処理が適用されます。
- ピアからタイムアウトする場合、SCP は「Server」ヘッダーに独自の FQDN を入力し、「504」エラーコードが原因を含む問題の詳細とともに返されます。これは「TARGET_NF_NOT_REACHABLE」に設定されます。この場合も、SCP 失敗処理が適用されます。構成に基づいて、SCP は使用可能なすべてのピア NF を試行します。SCP が使用可能なピア NF を見つけられない場合、SCP は「504」エラーコードと「TARGET_NF_NOT_REACHABLE」の原因で応答します。ただし、他の SCP がピアに到達できる可能性があります。このような場合に別の SCP を試行しないユースケースが存在する場合、オペレータは再試行値を 0 に構成できます。
- SCP と NRF 間の NF 検出エラーの場合、SCP は原因を「NRF_NOT_REACHABLE」または「NF_DISCOVERY_ERROR」に設定できます。このような場合、SMF はモデル A にフォールバックします（構成されている場合）。

*3gpp-Producer-id Header*

SMF は、NF ピアからの応答で受信した「3gpp-Producer-id」ヘッダーを保存します。次に、SMF は、このヘッダーを、同じセッションの同じサービスに対するピア NF への後続のメッセージに含めます。

### SCP モデル D フォールバック

「再試行」アクションを使用して SCP 障害の処理を構成している場合、SMF は、SCP 構成と再試行回数の構成に基づいて、代替 SCP を試みます。構成された再試行回数が完了するか、再試行に代替 SCP を再試行に使用できなくなると、SMF は次のシナリオでモデル D からモデル A にフォールバックします。

- SCP はエラーをトリガーし、「Server」ヘッダーに「scp」が表示されます。
- 「retry-and-fallback」アクションが構成されています。
- ピアの NF クライアント構成を使用できます。

## *SCP* モデル *D* の有効化

SCP モデル D 機能を有効にする

- NF 選択モデルの構成
- SCP プロファイルの構成

### NF 選択モデルの構成

ネットワーク要素プロファイルで SCP モデル D 機能を有効にするには、NF 選択モデルを構成する必要があります。SCP モデル D を有効にするには、次の構成例を使用します。

```
config
  profile network-element network_element_name
    nf-client-profile client_profile_name
    failure-handling-profile failure_handling_profile_name
    nf-selection-model 1 model1_name
    nf-selection-model 2 model2_name
  exit
```

注：

- **nf-selection-model 1** *model1_name*：最初の NF 選択モデルとして SCP を指定します。
- **nf-selection-model 2** *model2_name*：2 番目の NF 選択モデルに、ローカルなどの別の NF 選択モデルを指定します。

### SCP プロファイルの構成

SCP モデル D の機能を有効にするには、DNN プロファイルの下で SCP プロファイルを構成する必要があります。DNN プロファイルで SCP プロファイルを有効にするには、次の構成例を使用します。

```
config
  profile dnn dnn_name
    network-element-profiles udm udm_profile_name
    network-element-profiles scp scp_profile_
  exit
```

注：

- **network-element-profiles udm** *udm_profile_name*：UDM プロファイル名を指定します。
- **network-element-profiles scp** *scp_profile_*：特定の UDM プロファイルの下で構成する SCP プロファイル名を指定します。

## 設定例

次は、ネットワーク要素プロファイルで SCP モデル D を有効にする構成例です：

```
profile network-element pcf pcf1
 nf-client-profile PP1
 failure-handling-profile FHPCF
exit
```

```
profile network-element pcf pcf1-scp
 nf-client-profile PP1
 failure-handling-profile FHPCF
 nf-selection-model 1 scp
 nf-selection-model 2 local
exit
```

次は、DN プロファイルの下に SCP プロファイルを追加して SCP モデル D を有効にする構成例です：

```
profile dnn ims
 network-element-profiles udm udm-scp
 network-element-profiles scp scp-udm
exit
```

### *SCP* 障害処理プロファイルの構成

NF の構成と同様に、SMF で 1 つまたは複数の SCP を構成できます。SCP プロファイルでサービス単位の SCP エンドポイントを構成できます。SCP 失敗処理プロファイルを構成するには、次の構成例を使用します：

```
config
  profile network-element scp scp_profile_name
    nf-client-profile scp_client_profile_name
    failure-handling-profile failure_handling_scp_profile_name
    end
```

**注**：

- **profile network-element scp** *scp_profile_name*：SCP をネットワーク要素プロファイルとして指定します。 *scp_profile_name* には、対応するネットワーク要素のプロファイル名を表す英数字の文字列を指定する必要があります。
- **nf-client-profile** *scp_client_profile_name*：SCP クライアント プロファイルを指定します。 *scp_client_profile_name* には、対応する NF クライアント プロファイル名を表す英数字の文字列を指定する必要があります。
- **failure-handling-profile** *failure_handling_scp_profile_name*：構成された SCP の SCP 障害処理ネットワーク プロファイルを指定します。 *failure_handling_scp_profile_name* には、対応する SCP 障害処理ネットワーク プロファイル名を表す英数字の文字列を含める必要があります。

### 設定例

次に、SCP 障害処理プロファイルの構成例を示します：

```
profile network-element scp scp1
    nf-client-profile scp_profile1
    failure-handling-profile FHSCP
 exit
```

### *NF* 通信用の *SCP* の構成

NF 通信用に SCP を構成するには、次の構成例を使用します：

```
config
  profile nf-client nf-type scp
```

```
scp-profile scp_profile_name
   locality locality_name
      priority priority_value
      service name type service_name_type_value
         responsetimeout  responsetimeout_value
         endpoint-profile endpoint-profile_name
            capacity capacity_value
            priority priority_value
            uri-scheme uri_scheme_value
            endpoint-name endpoint_name/* FQDN */
               priority priority_value
               capacity endpoint-profile_name
               primary ip-address ipv4 ipv4_address
               primary ip-address port port_number
               end
```

注：

- **scp-profile** *scp_profile_name*：SCP プロファイルの名前を指定します。
- **locality** *locality_name*：SCP の地域を指定します。
- **priority***priority_value*：優先順位の値を指定します。
- **service name type** *service_name_type_value*：サービス名のタイプを指定します。
- **responsetimeout** *responsetimeout_value*：応答タイムアウト値を指定します。
- **endpoint-profile** *endpoint-profile_name*：SCP エンドポイント プロファイル名を指定します。
- **primary ip-address ipv4** *ipv4_address*：プライマリ エンドポイントの IPv4 アドレスを指定します。
- **primary ip-address port** *primary_port_number*：プライマリ エンドポイントのポート番号を指定します。

設定例

次に、NF 通信用の SCP の構成例を示します：

```
profile nf-client nf-type scp
 scp-profile scp-profile1
  locality LOC1
   priority 30
   service name type <>
    responsetimeout 4000
    endpoint-profile EP1
     capacity 30
     priority 10
     uri-scheme http
     endpoint-name <> /* FQDN */
      priority 10
      capacity 50
      primary ip-address ipv4 209.165.202.133
      primary ip-address port 8080
     exit
    exit
```

```
   exit
  exit
 exit
exit
```

## *SCP* モデル *D* フォールバックの構成

SCP モデル D のフォールバックを構成するには、次の構成例を使用します：

```
config
  profile nf-client-failure nf-type scp
    profile failure-handling failure_handling_name
    service name type npcf-smpolicycontrol
      responsetimeout response_timeout_value
      message type { PcfSmpolicycontrolCreate }
      status-code httpv2 status_code
      retry retry_value
      action [ retry-and-fallback | retry-and-continue | continue |
terminate { nfaction terminate } | retry-and-terminate { nfaction
terminate } ]
    exit
  exit
```

**注**：

- **profile nf-client-failure nf-type scp** ：NF クライアントの障害後に必要な SCP として NF タイプを指定します。
- **service name type npcf-smpolicycontrol**：サービス名タイプを npcf-smpolicycontrol として指定します。
- **responsetimeout** *response_timeout_value*：応答タイムアウト値を秒単位で指定します。
- **message type { PcfSmpolicycontrolCreate }**：メッセージ タイプを **PcfSmpolicycontrolCreate** として指定します。
- **status-code httpv2** *status_code* ：サービスのステータス コードを指定します。 *status_code* は 0 ～ 599 の範囲の整数である必要があります。
- **retry** *retry_value*：使用可能な別のエンドポイントへの再試行回数を指定します。 *retry_value* は、1 ー 10 の範囲の整数である必要があります。
- **action [ retry-and-fallback | retry-and-continue | continue | terminate { nfaction terminate } | retry-and-terminate { nfaction terminate } ]**：SCP モデル D からモデル A へのフォールバックのアクションを、再試行-フォールバック、再試行-継続、続行、終了、または再試行-終了を指定します。NF ピアからのアクションだとサーバーヘッダーが示している場合にNF障害アクションが使用されます。障害の原因が SCP にある場合、アクションが使用されます。

（注）

- フォールバック後は、同じリソースに対する後続のメッセージでは、フォールバックの一部として選択されたピアが使用されます。たとえば、N10 の登録中に SCP モデル A へのフォールバックが発生した場合、SMF は、後続の N10 の登録解除をフォールバックの一部として選択された UDM に送信します。
- 現在、 **action [ retry-and-fallback ]** は、SCP NF クライアントの障害処理テンプレートにのみ推奨されます。

設定例

次に、SCP モデル D フォールバックの構成例を示します：

```
config
  profile nf-client-failure nf-type scp
    profile failure-handling FHSCP
    service name type npcf-smpolicycontrol
      responsetimeout 1800
      message type PcfSmpolicycontrolCreate
      status-code httpv2 504
        retry 1
        action retry-and-fallback
      exit
    exit
```

### デッド SCP 検出

SMF の既存のデッドピア検出フレームワークが、デッド SCP を検出するように拡張されています。

# FQDN の概要

表 *310* : 機能の履歴

| 機能名 | リリース情報 | 説明 |
|---|---|---|
| ピア通信用 FQDN | 2025.01.0 | SMF では、NRF およびピア NF と通信するための FQDN を構成できます。<br>導入されたコマンド：<br>• **fqdn** *fqdn_value* ：エンドポイント、インターフェイス、および NF クライアント レベルで FQDN を構成するために使用されます。<br>**デフォルト設定**：無効：構成が必要<br>• **smf-fqdn** *fqdn_value* ：各インスタンスの SMF プロファイルで SMF の FQDN を構成するために使用されます。<br>**デフォルト設定**：無効：構成が必要 |

FQDN 機能により、SMF はピア NF との通信に FQDN を使用できます。FQDN のサポートにより、NF 間の通信に IP アドレスではなくドメイン名を使用することで、ネットワーク管理が簡素化され、セキュリティが強化されます。

検出プロセスで FQDN を選択すると、使用されているプロトコルに基づいて適切なポートが自動的に割り当てられます。プロトコルが HTTPS の場合、ポートは 443 に設定されます。プロトコルが HTTP の場合、ポートは 80 に設定されます。

SMF が DNS 解決を実行して、ピア IP アドレスを取得します。次の表に、IP アドレスと FQDN の存在に基づいて NF URI を処理するためのシナリオと構成、および使用する適切なスキームと権限ヘッダーの概要を示します。

| シナリオ | スキーム | IP の有無 | FQDN が存在します | IP ヘッダー | URI スキーム | 認証局ヘッダー（NF URI） |
|---|---|---|---|---|---|---|
| スタティック/ディスカバリ | http | Y | Y/N | IP | http | IP アドレス |
| スタティック/ディスカバリ | http | N | Y | FQDN の IP | http | [FQDN] |
| 静的/ディスカバリ | https | Y | Y | IP | https | [FQDN] |
| 静的/ディスカバリ | https | N | Y | FQDN の IP | https | [FQDN] |
| 静的/ディスカバリ | https | Y | N | IP | https | IP address |

# FQDN：制限事項

ポッドの再起動時に、NF は、スタティックに構成された FQDN と検出された FQDN の両方に対して DNS クエリを再試行します。このプロセスにより、初期化中の DNS 検出で遅延が発生します。この期間中に、最初の試行でそれらの FQDN の DNS 解決が成功しなかった場合、一部のコールでポッドを介して送信されたメッセージが失敗する可能性があります。

# FQDN の構成

エンドポイントレベルまたはインターフェイス レベルで FQDN を構成できます。

### エンドポイントレベルで FQDN を構成する

エンドポイントレベルで FQDN を構成するには、次の構成を使用します。

```
config
  instance instance-id  instance-id
    endpoint  endpoint_name
      fqdn  fqdn_value
      exit
```

注：

- **instance instance-id** *instance_id*：インスタンス識別子を指定します。
- **endpoint** *endpoint_name*：インスタンス内のエンドポイント タイプを指定します。例：SBI インターフェイス。
- **fqdn** *fqdn_value*：指定されたエンドポイントの FQDN 値を指定します。FQDN 値は文字列である必要があります。

### インターフェイス レベルでの FQDN の構成

インターフェイス レベルで FQDN を構成するには、次の構成を使用します。

```
config
  instance instance-id  instance-id
    endpoint  endpoint_name
      interface  interface_name
        fqdn  fqdn_value
        exit
```

注：

- **instance instance-id** *instance_id*：インスタンス識別子を指定します。
- **endpoint** *endpoint_name*：インスタンス内のエンドポイント タイプを指定します。例：SBI インターフェイス。
- **interface** *interface_name*：FQDN を構成するインターフェイスを指定します。例：N7、N10、または N11 インターフェイス。
- **fqdn** *fqdn_value*：指定されたエンドポイントの FQDN 値を指定します。FQDN 値は文字列である必要があります。

## ピア通信用 FQDN の構成

ピア NF 通信の FQDN 静的構成を構成するには、次の構成例を使用します。

```
config
  profile nf-client nf-type udm
    udm-profile   udm_profile_name
      locality   locality_name
        priority   priority_value
        service name type   service_name_type
          endpoint-profile   endpoint-profile_name
            capacity   capacity_value
            priority   priority_value
            uri-scheme   uri_scheme_value
            endpoint-name   endpoint_name
              fqdn name   fqdn_name
              fqdn port  fqdn_port
              end
```

NRF の構成も拡張されて、NF クライアントの構成と同様にエンドポイント名レベルでの FQDN のサポートが含まれるため、NRF の手順が容易になります。

注：

- **locality** *locality_name*：プロファイルの場所を指定します。
- **priority** *priority_value*：優先順位の値を指定します。
- **service name type** *service_name_type*：サービス名のタイプを指定します。

- **uri-scheme** *uri_scheme_value*：uri-scheme に http または https を指定します。
- **fqdn name** *fqdn_name*： FQDN 名を指定します。
- **fqdn port** *fqdn_port*：fqdn ポート番号を指定します。ポートが構成されていない場合、SMF は FQDN の標準ポートを使用します。これにより、URI スキーム http では 80、URI スキーム https では 443 が使用されます。

# 障害処理の構成

選択したエンドポイント プロファイルで FQDN の IP アドレスを解決できない場合、ピア NF にメッセージを送信するときにエラー処理が開始されます。未解決の FQDN を持つエンドポイント プロファイルは、解決済みの FQDN を持つエンドポイント プロファイルまたは IP アドレスを持つエンドポイントプロファイルと比較して、優先順位が低いと見なされます。構成されたアクションに再試行アクションが含まれている場合、システムは次の未解決 FQDN で再試行を試みます。FQDN が正常に解決されると、再試行回数がリセットされます。再試行プロセスがリセットされ、後続の FQDN を解決するときに再起動されます。再試行回数を終了すると、システムは構成されたアクションをアプリケーションに返します。

未解決の FQDN の場合、SMF はこれらの FQDN を追跡し、DNS サーバにこれらの FQDN の解決済み IP アドレスを取得するように照会します。

障害処理テンプレートを構成するには、次の構成例を使用します。

```
profile nf-client-failure nf-type  nf_type
  profile failure-handling   failure_handling_profile
     service name type  service-name_type
       message type message-type
          status-code dns   any
             retry  retry_count
            action [ terminate | retry-and-continue | retry-and-ignore
 | retry-and-fallback ]
             exit
```

注：

- **profile nf-client-failure nf-type** *nf_type*：特定の NF タイプの障害処理テンプレートを構成します。*nf-type* を udm などのネットワーク機能タイプに置き換えます。
- **profile failure-handling** *failure_handling_name*：障害処理プロファイル名を指定します。*failure-handling-profile* を FH4 などのプロファイル識別子に置き換えます。
- **service name type** *service-name_type*：サービス名のタイプを指定します。*service-name-type* を nudm-sdm などの関連するサービス タイプに置き換えます。
- **message type** *message-type*：障害処理を構成するメッセージタイプを設定します。*message-type* を UdmSdmSubscribeToNotification などのメッセージ タイプに置き換えます。
- **status-code dns** *any*：DNS ステータス コードを構成します。現在、サポートされているのは any のみです。

- **retry** *retry_count*：再試行の回数を指定します。 *retry-count* を 1 などの整数に置き換えます。
- **action [ terminate | retry-and-continue | retry-and-ignore | retry-and-fallback ]**：障害発生時に実行するアクションを定義します。次のいずれかのオプションを選択します。
  - **terminate**：操作を終了します。
  - **retry-and-continue**：操作を再試行して続行します。
  - **retry-and-ignore**：操作を再試行して無視します。
  - **retry-and-fallback**：再試行とフォールバック。SCP にのみ適用されます。

# SMF FQDN の構成

SMF FQDN を構成するには、次の構成例を使用します：

```
config
profile smf   profile_name
   instances instance_id  smf-fqdn   fqdn
   exit
```

注：

- **profile smf** *profile_name*：構成する SMF プロファイルを指定します。 *profile-name* を プロファイル名（smf1 など）に置き換えます。
- **instances** *instance_id* ：SMF のインスタンス ID を指定します。 *instance-id* を 1 などの適切なインスタンス番号に置き換えます。
- **smf-fqdn** *fqdn*：SMF の FQDN を設定します。 *fqdn* を topon.abc.mncxxx.mccyyy.3gppnetwork.org などの目的の FQDN に置き換えます。

# OAM サポート

ここでは、SFM の FQDN 機能に関する操作、管理、およびメンテナンスに関して説明します。

## バルク統計サポート

- **FQDN 統計情報**

  「fqdn_dns_msg_total」統計は、アプリケーションが試行、正常に解決、または解決に失敗した FQDN の数を追跡するように設計された、新しく導入されたメトリックです。このメトリックは、次のコマンドを使用して制御できます。

```
infra metrics verbose application
metrics fqdn_dns_msg_total
granular-labels [ fqdn ]
exit
```

  - **DNS 解決のために CoreDNS に送信される要求のメトリック**：

- dns_request_total：CoreDNS に送信された要求の数をモニターします。
- dns_response_total：CoreDNS から受信した成功応答と失敗応答の数をモニターします。

  例：「dns_request_total」および「dns_responseq_total」統計情報の例を次に示します。

```
dns_request_total{app_name="SMF", attempt="first",
cluster="clu1", data_center="dc1", fqdn="cisco.udm.scp.org",
instance_id="1", method_name="get", service_name="smf-rest-ep", type="ipv6"}
 27
dns_request_total {app_name="SMF", attempt="retry",
cluster="clu1", data_center="dc1",fqdn="cisco.udm.scp.org",
instance_id="1", method_name="unresolved-get",
service_name="smf-rest-ep",type="ipv4"} 937
dns_request_total{app_name="SMF",attempt="second",
cluster="clu1",data_center="dc1", fqdn="cisco.udm.scp.org",
instance_id="1", method_name="get", service_name="smf-rest-ep", type="ipv4"}
 5
dns_request_total{app_name="SMF" ,attempt="third",
cluster="clu1" ,data_center="dc1", fqdn="cisco.udm.scp.org", instance_id="1",
method_name="get", service_name="smf-rest-ep", type="ipv4"} 5

dns_response_total{app_name="SMF",attempt="first",
cluster="clu1",data_center="dc1",fadn="cisco.udm.scp.org",
instance_id="0",method_name="get",service_name="smf-rest-ep" ,
status="success" , status_code="",type="ipv4"} 22
dns_response_total {app_name="SMF",attempt="retry",
cluster="clu1", data_center="dc1",fadn="cisco.udm.scp.org",
instance_id="0",method_name="unresolved-get" ,
service_name="smf-rest-ep" ,status="error",
status_code="Ipv6NotFound",type="ipv6"} 933
dns_response_total {app_name="SMF", attempt="retry",
Cluster="clu1",data_center="dc1",fadn="cisco.udm.scp.org",
instance_id="0", method_name="unresolved-get" , service_name="smf-rest-ep"
,
status="error", status_code="read udp 192.168.12.42:55049->10.96.0.10:53:
i/o timeout",type="ipv4"} 1
dns_response_total{app_name="SMF",attempt="third",
cluster="clu1",data_center="dc1",fadn="cisco.udm.scp.org",
instance_id="0", method_name="get",service_name="smf-rest-ep" ,
status="success" , status_code="",type="ipv4"} 3
```

- **サービス レベルでのDNS解決統計**：
  - fqdn_dns_msg_total：アプリケーションによる FQDN の試行/成功/失敗ステータスを追跡します。

    ステータスが「attempted」または「success」の場合、エラー統計フィールドは空です。ステータスが「失敗」の場合にのみコードが含まれます。

    次に、サンプル メトリックの例を示します：

```
fqdn_dns_msg_total{app_name="SMF",cluster="SMF",data_center="DC",
error="",fqdn="host1.satya-test.com",instance_id="1",nf_type="SCP",req="resolution",
service_name="rest-ep",status="attempted",svc_name="nudm-sdm"} 1

fqdn_dns_msg_total{app_name="SMF",cluster="SMF",data_center="DC",
error="",fqdn="host1.satya-test.com",instance_id="1",nf_type="SCP",
req="resolution",service_name="rest-ep",status="success",svc_name="nudm-sdm"}
 1
```

```
fqdn_dns_msg_total{app_name="SMF",cluster="SMF",data_center="DC",
error="8312",fqdn="seth.com",instance_id="1",nf_type="SCP",req="resolution",
service_name="rest-ep",status="failure",svc_name="nudm-uecm"} 1
```

# インターフェイスの設定

SMFサービスのエンドポイントと、他のネットワーク機能との通信を容易にするインターフェイスを構成するには、次の構成例を使用します：

```
config
  instance instance-id instance_id
    endpoint { bgpspeaker | diameter | dns-proxy | geo | gtp | gtpprime
 | li | nodemgr | pfcp | protocol | radius | radius-dns | sbi | service
 | sgw-service }
       replicas replica_id
       instancetype Dual
       nodes node_id
       interface { bfd | bgp | coa-nas | geo-external | geo-internal
| gtpu | n4 | n7 | n10 | n11 | n16 | n40 | nrf | s2b | s5 | s5e | s8 |
 s11 | sxa }
          loopbackPort port_number
          vip-ip ipv4_address vip-port ipv4_port_number
          vip-ip6 ipv6_address vip-ipv6-port ipv6_port_number
          end
```

注：

- **endpoint { bgpspeaker | diameter | dns-proxy | geo | gtp | gtpprime | li | nodemgr | pfcp | protocol | radius | radius-dns | sbi | service | sgw-service }**：目的のサービスに基づいてエンドポイントを構成します。
- **interface { bfd | bgp | coa-nas | geo-external | geo-internal | gtpu | n4 | n7 | n10 | n11 | n16 | n40 | nrf | s2b | s5 | s5e | s8 | s11 | sxa }**：構成されたエンドポイントのインターフェイスを指定します。
- **vip-ip** *ipv4_address* **vip-port***ipv4_port_number*：インターフェイスの IPv4 アドレスとポートを指定します。

  *ipv4_address* は、ドット付き 10 進表記の IPv4 アドレスである必要があります。
- **vip-ip6** *ipv6_address* **vip-ipv6-port***ipv6_port_number*：インターフェイスの IPv6 アドレスとポートを指定します。

  *ipv6_address* は、コロンで区切った 16 進数表記の IPv6 アドレスである必要があります。

  特定の時点で、SBI インターフェイス（N7、N10、N11、および N40）は、IPv4 または IPv6 アドレスのみをサポートします。ただし、N3、N4 、および GTPC インターフェイスは、IPv4 または IPv6 アドレスのいずれか 、または両方をサポートします。

（注） レガシー インターフェイスを使用する 4G コールの場合、ピア SGW IPv4、IPv6、または IPv4v6 データ アドレスがサポートされます。

重要 IPv4 または IPv6、または IPv4 と IPv6 の両方を同時にサポートするインターフェイスに関係なく、任意のインターフェイスの IPv6 を構成するには、インスタンス タイプを Dual として構成する必要があります。これは、エンドポイント レベルでのみ構成する必要があります。そのエンドポイントで構成されたすべてのインターフェイスは、暗黙的にデュアル タイプ インスタンスとして構成されます。

SBI インターフェイスで構成された VIP IP または VIP IPv6 は、エンド ポイント レベルで構成された VIP IP および VIP IPv6 を常にオーバーライドします。

N4 インターフェイスと GTPC インターフェイスの場合、インターフェイスで構成された IP アドレス（IPv4 または IPv6、あるいはその両方）は、エンドポイントで構成されている同じタイプの IP アドレスのみをオーバーライドします。

- SBI インターフェイスでは、同時の IPv4 アドレスと IPv6 アドレスはサポートされていないため、検出アドレスの転送タイプは、エンドポイントまたはインターフェイス構成で構成された転送タイプと同じである必要があります。
- エンドポイントとインターフェイスの両方のレベルでポート、IPv4、および IPv6 アドレスを構成します。VIP IP とポートの組み合わせは、インターフェイス全体で一意にする必要があります。インターフェイス レベルの構成が使用できない場合は、エンドポイント レベルの構成が考慮されます。

# 設定例

インターフェイスの IPv4 または IPv6 構成の例を次に示します。

```
config
 instance instance-id 1
  endpoint sbi
   replicas     1
   instancetype Dual
   nodes        1
   loopbackPort 7091
   vip-ip 209.165.200.225 vip-port 1234
   vip-ipv6 2001:DB8:1::1 vip-ipv6-port 2345
  interface nrf
   loopbackPort 7096
   vip-ip 209.165.200.226 vip-port 1235
```

```
  interface n11
   loopbackPort 7094
   vip-ip6 2001:DB8:0:ABCD::1 vip-ipv6-port 1212
   exit
  interface n7
   loopbackPort 7092
   vip-ip6 2001:DB8:1::FFFF vip-ipv6-port 1233
   exit
  interface n10
   loopbackPort 7093
   vip-ip 209.165.200.227 vip-port 4321
   exit
  interface n40
   loopbackPort 7095
   vip-ip 209.165.200.228 vip-port 4231
   end
```

デュアル スタックはサポートされていないため、NRF 検出アドレスのトランスポート タイプは、エンドポイントまたはインターフェイス レベルの構成で構成されたトランスポート タイプと同じである必要があります。

上記の構成例では、PCF は PCF プロファイル内で構成されているものと同じトランスポート タイプである IPv6 アドレスを使用しています。

```
config
 profile nf-client nf-type pcf
  pcf-profile PP100
   locality LOC1
    priority 30
    service name type npcf-smpolicycontrol
     endpoint-profile EP1
      capacity   30
      uri-scheme http
      endpoint-name EP1
       priority 56
       primary ip-address ipv6 2001:DB8:1::FEFF
       primary ip-address port 2223
      exit
      endpoint-name exit
      exit
     exit
    exit
 exit
exit
```

次に、N4 インターフェイスの UPF プロファイル内の IPv6 構成の例を示します。

```
config
 profile network-element upf UPF1
  node-id           SSI-UPF1
  n4-peer-address ipv6 2001:DB8:0:ACBD::1
  n4-peer-port      8805
  upf-group-profile upg1
  dnn-list          [ emergency intershat test ]
  capacity          1
  priority          100
  exit
 exit
exit
```

# 設定の確認

インターフェイス構成を認証するには、次のコマンドを使用します：

**show running-config instance instance-id** *instance_id* **endpoint** *endpoint_name* **interface** *interface_name*

```
[smf] smf# show running-config instance instance-id 1 endpoint sbi interface nrf
instance instance-id 1
 endpoint sbi
  interface nrf
   loopbackPort 9050
   dscp         24
   vip-ip 209.165.200.232 vip-port 8095
  exit
 exit
exit
[smf] smf#
```

次に、NRF インターフェイスの構成例を示します。 **vip-ip** コマンドの 値は、IPv4 アドレスが NRF インターフェイスに構成されていることを示します。

**show peer**

```
Thu Jul  7  07:53:23.422 UTC+00:00
GR                                                                                  POD
      CONNECTED                                                                      INTERFACE
INSTANCE  ENDPOINT      LOCAL ADDRESS    PEER ADDRESS          DIRECTION  INSTANCE
TYPE  TIME        RPC     ADDITIONAL DETAILS                    NAME       VRF
-------------------------------------------------------------------------------------------------------
0         RadiusServer  -                10.1.4.72:1812        Outbound   radius-ep-0
Udp   6 days      Radius  Status: Init,Type: Auth               <none>     NA
0         RadiusServer  -                10.1.4.72:1813        Outbound   radius-ep-0
Udp   6 days      Radius  Status: Init,Type: Acct               <none>     NA
1         <none>        192.168.47.245   10.1.4.72:9014        Outbound   rest-ep-0
Rest  6 days      CHF     <none>                                 n40        NA
1         <none>        192.168.47.245   10.1.4.72:9024        Outbound   rest-ep-0
Rest  6 days      CHF     <none>                                 n40        NA
1         <none>        192.168.47.235   10.1.4.72:9011        Outbound   rest-ep-1
Rest  6 days      UDM     <none>                                 n10        NA
1         <none>        192.168.47.235   10.1.4.72:9012        Outbound   rest-ep-1
Rest  6 days      AMF     <none>                                 n11        NA
1         <none>        192.168.47.235   10.1.4.72:9060        Outbound   rest-ep-1
Rest  6 days      SEPP    <none>                                 n32        NA
1         <none>        192.168.47.235   10.1.4.72:9010        Outbound   rest-ep-1
Rest  6 days      NRF     <none>                                 nrf        NA
1         <none>        192.168.47.235   10.1.4.72:9013        Outbound   rest-ep-1
Rest  6 days      PCF     <none>                                 n7         NA
1         <none>        192.168.47.245   10.1.4.72:9010        Outbound   rest-ep-0
Rest  6 days      NRF     <none>                                 nrf        NA
1         <none>        192.168.47.245   10.1.4.72:9011        Outbound   rest-ep-0
Rest  16 minutes  UDM     <none>                                 n10        NA
1         <none>        192.168.47.245   10.1.4.72:9012        Outbound   rest-ep-0
Rest  6 days      AMF     <none>                                 n11        NA
1         <none>        192.168.47.245   10.1.4.72:9060        Outbound   rest-ep-0
Rest  6 days      SEPP    <none>                                 n32        NA
1         <none>        192.168.47.235   10.1.4.72:9024        Outbound   rest-ep-1
Rest  6 days      CHF     <none>                                 n40        NA
1         <none>        192.168.47.235   10.1.4.72:9014        Outbound   rest-ep-1
Rest  6 days      CHF     <none>                                 n40        NA
1         <none>        192.168.47.245   10.1.4.72:9013        Outbound   rest-ep-0
Rest  6 days      PCF     <none>                                 n7         NA
1         S2B           10.1.3.236:2123  172.31.4.72:2123      Inbound    nodemgr-0
```

```
Udp   6 days      ePDG    MaxRemoteRcChange: N/A,Recovery: 100  S2B        NA
1         S2B           [1111::10:1:3:236]:2123       [1111::10:1:4:72]:2123  Inbound
  nodemgr-0    Udp   6 days      ePDG    MaxRemoteRcChange: N/A,Recovery: N/A  S2B
   NA
1         S2B           [1111::10:1:3:236]:2123       [1111::10:1:4:72]:2123  Inbound
  nodemgr-1    Udp   6 days      ePDG    MaxRemoteRcChange: N/A,Recovery: N/A  S2B
   NA
```

# OAM サポート

ここでは、SFMのインターフェイスのサポートに関する操作、管理、およびメンテナンスに関して説明します。

## バルク統計サポート

次のラベルが既存の統計情報 **smf_restep_http_msg_total**に追加されます：

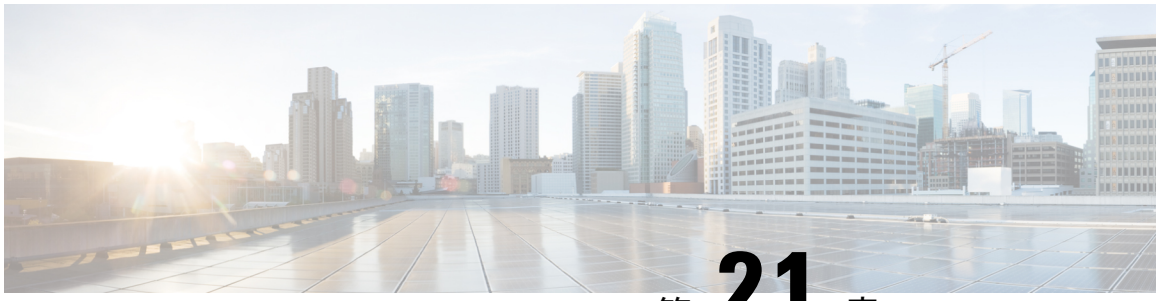
**uri_version_mismatch**：このメトリックスは、着信メッセージのURIバージョンが、SMF で構成された URI バージョンで見つからない場合に含まれます。

**OFCS_CDR_DROP_STATS** ：このメトリックスは、ゼロ抑制によってCDRが抑制されるたびに、カウンタ値をキャプチャするために追加されます。

抑制基準が満たされた場合、トリガー名とともに SMF 手順名が表示されます。

トリガー名の値は次のいずれかになります：

- 最終 CDR
- 外部トリガー CDR
- 内部トリガー CDR



第 21 章

# IP アドレス管理


- 機能の概要と変更履歴, on page 894
- 機能説明 （896 ページ）
- 機能の仕組み （897 ページ）
- SMF 内の IPAM 統合 （897 ページ）
- 静的 IP サポート （918 ページ）
- IPAM によるデュアルスタック静的 IP サポート （933 ページ）
- IPAM オフライン モードのサポート （935 ページ）
- UPF ごとの IPAM 冗長性サポート （938 ページ）
- IPAM 隔離タイマー（IPAM Quarantine Timer） （939 ページ）
- IPAM 隔離タイマーの構成 （940 ページ）
- IPAM データの照合 （941 ページ）
- IPv6 プレフィックス委任 （945 ページ）
- IPAM の隔離 Qsize の構成 （952 ページ）
- IP アドレス プールをオーバーラップ （953 ページ）
- 使用率の低い IP チャンクの自動再利用 （954 ページ）
- UPF の一意の IP プール （957 ページ）
- SMF と UPF の間での IP チャンクの調整 （961 ページ）
- IP チャンク スロットリング （963 ページ）
- IPAM キャッシュ データ シャーディング （969 ページ）
- IP の割り当てと再利用 （971 ページ）
- スイッチ制限を処理するためのルート集約 （980 ページ）
- NAT のサポート （988 ページ）
- トラブルシューティング情報 （999 ページ）

# 機能の概要と変更履歴

## 要約データ

***Table 311:*** 要約データ

| | |
|---|---|
| 該当製品または機能エリア | SMF |
| 該当プラットフォーム | SMI |
| 機能のデフォルト設定 | • IPAM：有効：常時オン<br>• UPF 無効化用固有 IP プール：有効化するには構成が必要です<br>• 使用率の低い IP チャンクの自動再利用：無効 - 有効に必要な構成が必要です<br>• 破損したチャンクの識別：無効 - 有効にするには構成が必要です。<br>• SMF と UPF 間の IP チャンクの照合：無効 - 有効にするには構成が必要です。<br>• IP チャンク自動スロットルおよび ToD チャンク クリアランス：無効：有効にするには構成が必要です。<br>• スイッチ制限を処理するためのルート集約：無効：有効にするには構成が必要です。<br>• NAT サポート：無効 - 有効化するには構成が必要です。 |
| このリリースでの関連する変更点 | N/A |
| 関連資料 | 該当なし |

# 更新履歴

***Table 312:*** マニュアルの変更履歴

| 改訂の詳細 | リリース |
|---|---|
| 次の機能に対して追加サポート：<br>• CLI を使用した N4 技術情報の解放<br>• SMF での NAT バインディング更新の送信に使用するネットワーク アドレス変換（NAT）。 | 2023.04.0 |
| 次の機能に対して追加サポート：<br>• 使用率の低い IP チャンクの自動再利用。<br>• 破損したチャンクの識別。<br>• SMF と UPF の間の IP チャンクの調整。<br>• IP チャンク オートスロットルおよび ToD チャンク クリアランス。<br>• スイッチ制限を処理するためのルート集約 | 2023.03.0 |
| IPv6 アドレス範囲とプレフィックス範囲に追加されたネクスト ホップ転送アドレス設定。 | 2023.01.4 |
| 次の機能に対して追加サポート：<br>• IPAM の定期的調整<br>• UPF フォールバック機能 | 2023.01.0 |
| 次の機能に対して追加サポート：<br>• IPAM 強化のための IPAM 調整 CLI コマンド。<br>• スライスおよび DNN 機能ごとの IP プールの割り当て。<br>• 一意の IP プールを持つ UPF を割り当てるための SMF。 | 2022.04.0 |

| 改訂の詳細 | リリース |
| --- | --- |
| 次の機能に対して追加サポート：<br>• 静的 IP アドレスを使用した新しいコール。<br>• 隔離キュー サイズ。<br>• CDL 構成と統計による IP アドレスの検証。 | 2021.02.0 |
| CDL 構成による IP アドレス検証が導入されました。 | 2021.02.0 |
| 隔離時間の範囲を 3600 秒に更新しました。 | 2021.02.0 |
| VRF サポートが導入されました。 | 2020.02.5 |
| 最初の導入。 | 2020.02.0 より前 |

# 機能説明

IP アドレス管理（IPAM）は、ネットワークの IP アドレスを追跡および管理する方法です。IPAM は、サブスクライバ管理システムのコア コンポーネントの 1 つです。従来の IPAM 機能では、クラウドネイティブのネットワーク環境では不十分です。したがって、IPAM には、クラウドネイティブのサブスクライバ管理システムと連携するための追加の機能が必要です。クラウド ネイティブ IPAM システムは、SMF や PCF などさまざまなネットワーク機能で使用されます。

IPAM システムには、クラウドネイティブとコントロールとユーザープレーンの分離（CUPS）アーキテクチャにサービスを提供する次の機能が含まれています：

- **中央集中型 IP リソース管理**：インターネット サービス プロバイダー（ISP）の需要に基づいて、コントロールプレーン（CP）は単一の（集中型）クラスタまたは複数（分散型）クラスタのいずれかに展開されます。マルチ クラスタ展開の場合、IPAM は、分散環境に展開されている複数の CP 間で単一の IP アドレス空間を自動的に管理します。
- **ユーザー プレーンごとの IP アドレス範囲予約**：インターネット コアに接続するサブスクライバの場合、ユーザー プレーン（UP）は物理的な接続を提供します。UP はサマリー ルートを使用して、サブスクライバルートをインターネット コアにアドバタイズします。複数の UP を管理している CP の場合、CP は統合された IP サブネットを UP に予約します。このようなシナリオでは、IPAM は使用可能なアドレス空間をより小さなアドレス範囲に分割し、異なる UP に割り当てます。
- **[事前予約されたアドレス範囲からの IP アドレスの割り当て（IP Address Assignment from Pre-Reserved Address Ranges）]**：サブスクライバが IP アドレスを要求すると、IPAM はそれぞれの UP の事前予約されたアドレス範囲からアドレスを割り当てます。

- **IPv4 および IPv6 プールのネクスト ホップ アドレス範囲**：SMF は、アドレス範囲とプレフィックス範囲とともに、IPv4 および IPv6 プールのネクスト ホップ構成をサポートします。

（注） 統一された互換性のために、 **nexthop-forwarding-address** 構成オプションは、Internet Assigned Numbers Authority（IANA）と Identity Association for Prefix Delegation（IAPD）の両方の IPv6 構成プロファイルで使用できます。SMF は IANA 構成を使用せず、IAPD 構成のみを使用します。BNG は IANA IPv6 構成を使用します。

# 機能の仕組み

IPAMは、クラウドネイティブサブスクライバ管理システムに次のサブモジュールを使用します：

- [IPAMサーバー（IPAM Server）]：このモジュールは、プールとアドレス空間構成の完全なリストを管理します。IPAM サーバーは、構成されたアドレス範囲をより小さなアドレス範囲に静的または動的に分割して、それらを IPAM キャッシュ モジュールに配布します。IPAMサーバーは、クラウドネイティブクラスタのグループにサービスを提供する集中型エンティティとして展開されますが、単一のクラスタ内の統合エンティティにすることもできます。
- [IPAM キャッシュ（IPAM Cache）]：このモジュールは、IPAM サーバーからフリー アドレス範囲を受信し、個々のIPアドレスをIPAMクライアントに割り当てます。通常、IPAM キャッシュは、同じ場所またはリモートにある IPAM サーバと通信するために、各クラスタ内で実行される分散モードで展開されます。IPAM キャッシュは、UP およびプールしきい値のモニタリングごとにアドレス範囲予約も処理します。IPAMサーバーとキャッシュモジュールは、統合モードとして実行できます。
- IPAM クライアント：このモジュールは、各 IP の管理対象エンドデバイスの IPAM キャッシュからの個々のIPアドレスの要求とリリースを処理します。IPAM クライアントは、それぞれのネットワーク機能と緊密に結合されています。

# SMF 内の IPAM 統合

## 機能説明

IP アドレス管理（IPAM）は、ネットワークの IP アドレス スペースを追跡および管理するための技術です。サブスクライバ管理システムの核心的な構成要素であるIPAMは、クラウドネイティブのサブスクライバ管理システムと連携するために必要なすべての機能を提供します。

また、IPAM は、SMF およびポリシー制御機能（PCF）など、さまざまなネットワーク機能の汎用 IP アドレス管理システムとして機能します。

## アーキテクチャ

このセクションでは、SMF アーキテクチャでの IPAM の統合について説明します。

## IPAMの統合

IPAM と SMF は、アプリケーション サービス レイヤーに存在します。

- SMF ノードマネージャ アプリケーション：SMF ノードマネージャ アプリケーションは、UPF、ID リソース、および IP アドレス管理を処理します。したがって、SMF ノード マネージャ アプリケーションは、IPAM キャッシュ モジュールと IPAM クライアント モジュールを統合します。UPF マネージャは、UPF ごとにアドレス範囲予約に IPAM クライアント モジュールを使用します。
- SMF サービス アプリケーション：SMF サービス アプリケーションは、PDU セッション サービスを提供します。セッションの確立と終了時に、IP アドレスが要求されて解放されます。SMF サービス アプリケーションは、ノード マネージャのリソース マネージャ（RMGR）に対して IPC を呼び出し、IPAM モジュールから IP を（解放）します。
- IPAM サーバー アプリケーション：導入モデルに基づいて、IPAM サーバー アプリケーションは、独立したマイクロサービスとして、同じクラスタの一部として、またはリモート クラスタ内で実行できます。スタンドアロン展開の場合、IPAM サーバーは IPAM キャッシュの不可欠な部分です。

## IP 割り当ての送信元

UE が SMF に IP アドレスを要求するたびに、SMF は 2 つのソースから UE に IP アドレスを割り当てます。

| **IPAM ソースが構成されている場合...** | **IP の割り当ては...** |
|---|---|
| ローカルとして | ローカル IPAM プール。これはデフォルトの動作です。<br>ローカル IPAM ベースの IP 割り当ての詳細については、「SMF における IPAM 統合」 トピックを参照してください。 |
| DHCP として | DHCP サーバDHCP ベースの IP 割り当ての詳細については、「DHCP サーバによる IP 割り当て」 のトピックを参照してください。 |

## コンポーネント

このセクションでは、IPAM システムのさまざまなコンポーネントについて説明します。

### IPAM サブモジュール

IPAM システムには、次のサブモジュールが含まれています：

- **IPAM サーバー** ：IPAM サーバー モジュールは、プールとアドレス空間構成の完全なリストを管理します。設定されたアドレス範囲をより小さなアドレス範囲（静的および動的）に分割し、IPAM キャッシュ モジュールに配布します。IPAM サーバーは、クラウド ネイティブ クラスタのグループにサービスを提供する一元化されたエンティティとして、または単一クラスタ内の統合エンティティとして展開できます。
- **IPAM キャッシュ** ：IPAM キャッシュは、IPAM サーバーからフリー アドレス範囲を取得し、個々の IP アドレスを IPAM クライアントに割り当てます。IPAM キャッシュは各クラスタ内で実行される分散モードで展開され、同じ場所またはリモートにある IPAM サーバと通信します。さらに、IPAM キャッシュは、データ プレーンおよびプールのしきい値モニタリングごとにアドレス範囲予約を処理します。
- **IPAM クライアント** ：IPAM クライアントモジュールは、各 IP 管理対象エンドデバイスの IPAM キャッシュからの個々の IP アドレスの要求とリリースを処理します。IPAM クライアントモジュールは、使用例に基づいて、特定のネットワーク機能（SMF、PCF など）のニーズに対応します。

# 機能の仕組み

このセクションでは、SMF での IPAM の統合に関連するコール フローについて説明します。

## コール フロー

次のコール フローは、SMF の IPAM 統合を示しています。

*Figure 171: IPAM* 統合コール フロー

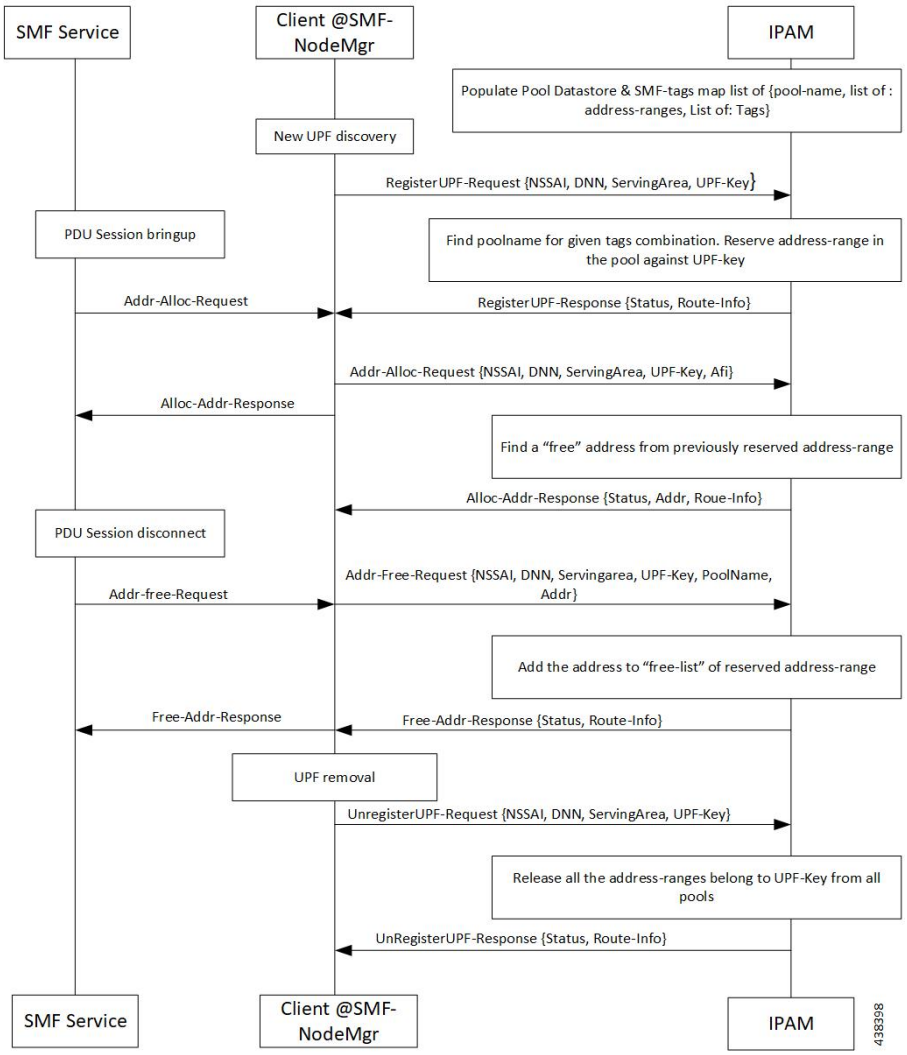



*Table 313: IPAM* 統合コール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | IPAM は、IPAM プール構成で構成されたデータをローカル キャッシュとキャッシュ ポッドに入力します。アドレス範囲で構成された分割サイズに従って、アドレス範囲を分割します。 |
| 2 | ノード マネージャ（NM）が UPF の検出要求または登録要求を受け取ります。 |
| 3 | NM は、特定の DNN またはアドレス タイプの IPAM に UPF 登録要求を転送します。 |
| 4 | IPAM は、指定されたタグとアドレス タイプのプールを検索し、指定された UPF キーに対して空きアドレス範囲を割り当てます。 |

| ステップ | 説明 |
|---|---|
| 5 | UPF 応答、ステータス、およびルート情報を登録します。 |
| 6 | SMF サービスは PDU セッションの起動を実行します。NM は、アドレス割り当て要求のために要求を IPAM に転送します。 |
| 7 | IPAM は、タグ、UPF キー、権威およびフォーマット識別子（AFI）、およびグループ識別子（GrID）のアドレス割り当ての要求を受信します。 |
| 8 | IPAM は、以前に割り当てられたアドレス範囲から空きアドレスを割り当て、ステータスと割り当てられたアドレス、およびルート情報で応答します。 |
| 9 | SMF サービスが PDU セッションの停止を行います。NM は、アドレス リリース要求のために IPAM に要求を転送します。 |
| 10 | IPAM は、プール名、UPF キー、AFI、および GrID のアドレス解放要求を受信します。 |
| 11 | IPAM は、予約済みアドレス範囲のフリー リストにアドレスを追加し、ステータスとルート情報で応答します。 |
| 12 | IPAM は、タグ、UPF キー、および AFI を持つ UPF 登録解除要求を受信します。 |
| 13 | タグ、UPF キー、および AFI に関連付けられているプールからすべてのアドレス範囲を解放します。次に、アドレス範囲をフリー リストに移動します。 |
| 14 | IPAM は、ステータスおよびルート情報とともに UPF 登録解除応答を送信します。 |

# IPAM の構成

このセクションでは、SMF で IPAM を構成する方法を説明します。

SMF の IPAM 構成には、次の手順が含まれます。

1. IPv4 アドレス範囲の構成, on page 902
2. IPv6 アドレス範囲の構成, on page 903
3. IPv6 プレフィックス範囲の構成, on page 904
4. SMF タグの構成, on page 908
5. IPv4 アドレス範囲のしきい値の構成, on page 909
6. IPv6 アドレス範囲のしきい値の構成, on page 910
7. IPv6 プレフィックス範囲のしきい値の構成, on page 910
8. IPv4 アドレス範囲分割の構成, on page 911

9. IPv6 アドレス範囲分割の構成, on page 912
10. グローバルなしきい値の構成, on page 913
11. IPAM 送信元の構成, on page 914

**Note** リリース 2021.02 以降では、IPAM プールを地理的冗長性（GR）インスタンスに関連付ける必要があります。つまり、IPAM 構成モードで GR インスタンス ID を構成する必要があります。この構成は、バックワードと互換性はありません。SMF を 2021.02 以前のリリースから 2021.02 以降のリリースにアップグレードする場合は、まず古い IPAM の構成を削除し、Ops Center にアクセスできるようになった後に新しい構成を適用してください。

## IPv4 アドレス範囲の構成

IPv4 アドレス範囲を構成するには、次の構成例を使用します：

```
config
   ipam
      instance gr_instance_id
         address-pool pool_name
            vrf-name vrf_name
            ipv4
               address-range start_ipv4_address end_ipv4_address
               commit
```

注：

- **ipam**：IPAM 構成モードを開始します。
- **address-pool** *pool_name*：アドレス プールの名前を指定します。 *pool_name* は 文字列である必要があります。
- **vrf-name** *vrf_name*：プールの仮想ルーティング名と転送（VRF）名を指定します。
- **ipv4**：プールの IPv4 モードを開始します。
- **address-range** *start_ipv4_address end_ipv4_address*：IPv4 アドレス範囲の開始アドレスと終了アドレスをドット付き 10 進表記で指定します。

次に、設定例を示します。

```
config
   ipam
      instance 1
         address-pool p1
                  vrf-name one
                  ipv4
                     address-range 209.165.200.225 209.165.200.253
                     address-range 209.165.201.1 209.165.201.30
                     end
```

### プールの IPv4 アドレス範囲の確認

指定したプール名の IPv4 アドレス範囲を表示するには、 **show ipam** *pool_name* **ipv4-addr** コマンドを使用します。構成に基づいて、アドレス範囲はダイナミックに分割されます。このコマンドを使用して、アドレス範囲が解放されているか、データ プレーン（ユーザー プレーン）に割り当てられているかを表示することもできます。

次に、 **show ipam** *pool_name* **ipv4-addr** コマンドの出力例を示します。

```
show ipam pool p1 ipv4-addr
=====================================================================
Flag Indication: S(Static) O(Offline)
=====================================================================
StartAddress          EndAddress    AllocContext     Flag
=====================================================================
209.165.200.225    209.165.200.253  Upf-100
209.165.201.1      209.165.201.30   Upf-200
209.165.202.129    209.165.202.158  Free:NM1









=====================================================================
```

## IPv6 アドレス範囲の構成

IPv6 アドレス範囲を構成するには、次の構成例を使用します：

```
config
   ipam
      instance gr_instance_id
         address-pool pool_name
            vrf-name vrf_name
            ipv6
               address-range start_ipv6_address end_ipv6_address
               commit
```

注：

- **address-pool** *pool_name*：アドレス プールの名前を指定します。 *pool_name* は 文字列である必要があります。
- **vrf-name** *vrf_name*：プールの VRF 名を指定します。
- **ipv6**：プールの IPv6 モードを開始します。
- **address-range** *start_ipv6_address end_ipv6_address*：IPv6 アドレス範囲の開始アドレスと終了アドレスを、コロンで区切った 16 進数表記で指定します。

次に、設定例を示します。

```
config
   ipam
      instance 1
         address-pool p1
                  vrf-name one
```

```
ipv6
   address-range 1::1 1::1000
   address-range 2::1 2::1000
   end
```

## IPv6 プレフィックス範囲の構成

IPv6 プレフィックス範囲を構成するには、次の構成例を使用します：

```
config
   ipam
      instance instance_id
         address-pool pool_name
            vrf-name vrf_name
            ipv6
               prefix-ranges
                  prefix-range prefix_value prefix-length length
                  commit
```

注：

- **address-pool** *pool_name*：アドレス プールの名前を指定します。 *pool_name* は文字列である必要があります。
- **vrf-name** *vrf_name*：プールの VRF 名を指定します。*vrf_name* は文字列である必要があります。
- **ipv6**：プールの IPv6 モードを開始します。
- **prefix-ranges**：プレフィックス範囲モードを入力します。
- **prefix-range** *prefix_value* **prefix-length** *length* ：IPv6 プレフィックス範囲と IPv6 プレフィックス長を指定します。

次に、設定例を示します。

```
config
   ipam
      instance 1
         address-pool p3
                  vrf-name three
                  ipv6
                     prefix-ranges
                        prefix-range 1:1:: prefix-length 48
                        prefix-range 2:1:: prefix-length 48
                        end
```

### プールの IPv6 アドレス プレフィックス範囲の確認

特定のプール名のプレフィックス範囲を表示するには、 **show ipam pool** *pool_name* **ipv6-prefix** コマンドを使用します。構成に基づいて、アドレス範囲はダイナミックに分割されます。このコマンドを使用して、アドレス範囲が解放されているか、データ プレーン（ユーザー プレーン）に割り当てられているかを表示することもできます。

次に、 **show ipam pool** *pool_name* **ipv6-prefix** コマンドの出力例を示します。

```
show ipam pool p1 ipv6-prefix
=================================================================================
Flag Indication: S(Static) O(Offline)
=================================================================================
StartAddress                EndAddress                  AllocContext         Flag
=================================================================================
aaaa:bbbb:ccc0::/64    aaaa:bbbb:ccc4::/64          Upf-100
aaaa:bbbb:dd00::/64    aaaa:bbbb:dd12::/64          Upf-200
bbbb:cccc:ee00::/64    bbbb:cccc:ee12::/64          Free:NM1
bbbb:cccc:ff00::/64    bbbb:cccc:ff12::/64          Free:NM0
xxxx:yyyy:zz00::/64    xxxx:yyyy:zz12::/64          Free:CP
```

## ネクスト ホップ転送アドレスを使用した IPv4 アドレスとプレフィックス範囲の設定

IPv4 プール/アドレス範囲のネクストホップ構成で IPv4 アドレスを構成するには、次の構成例を使用します。

```
configure
  ipam
    instance instance_id
      address-pool pool_name
        ipv4
        address-ranges
          address-range start_ipv4_address end_ipv4_address
nexthop-forwarding-address nexthop_forwarding_address
          prefix-range prefix_value length  prefix_length
nexthop-forwarding-address nexthop_forwarding_address
          split-size per-cache number_of_addresses
          split-size per-dp number_of_addresses
          commit
```

注：

- **address-pool** *pool_name*：アドレス プールの名前を指定します。 *pool_name* は 文字列である必要があります。
- **ipv4**：プールの IPv4 モードを開始します。
- **address-ranges**：IPv4 アドレス範囲の開始アドレスを指定します。ネクスト ホップ転送アドレスを使用して IPv4 アドレス範囲とプレフィックス範囲のアドレスを入力します。
  - **address-range** *start_ipv4_address end_ipv4_address* **nexthop-forwarding-address** *nexthop_forwarding_address*：ネクスト ホップ転送アドレスで IPv4 アドレス範囲の開始アドレスと終了アドレスを指定します。
  - **prefix-range** *prefix_value* **length** *prefix_length*：IPv4 アドレス内のプレフィックス値と長さを指定します。
  - **nexthop-forwarding-address** *nexthop_forwarding_address*：ネクスト ホップ転送アドレスを指定します。
- **split-size per-cache** *number_of_addresses*：IPAM キャッシュを割り当てるチャンクあたりの IPv4 アドレスの数を指定します。2 の累乗で指定します。IPAM サーバーは、この構成を使用します。 *number_of_addresses* は 、2 ～ 262144 の範囲の整数である必要があります。

- **split-size-per-dp** *number_of_addresses*：データ プレーンに割り当てるチャンクあたりの IPv4 アドレスの数を指定します。2 の累乗で を指定します。IPAM キャッシュは、この構成を使用します。

  *number_of_addresses* は 、2 ～ 262144 の範囲の整数である必要があります。

### 設定例

次に、設定例を示します。

```
config
   ipam
      instance 1
         address-pool p1
                  ipv4
                     split-size per-cache 1024
                     split-size per-dp 256
                     end
```

## ネクスト ホップ転送アドレスでの IPv6 アドレス範囲の構成

IPv6 プールおよびアドレス範囲のネクスト ホップ構成で IPv6 アドレスを構成するには、次の構成例を使用します。

```
configure
   ipam
      instance instance_id
         address-pool pool_name
            ipv6
            address-ranges
               address-range start_ipv6_address end_ipv6_address
nexthop-forwarding-address nexthop_forwarding_address
              prefix-range prefix_value length prefix_length
nexthop-forwarding-address nexthop_forwarding_address
                split-size per-cache number_of_addresses
                split-size per-dp number_of_addresses
                exit
                prefix-range prefix_value length prefix_length
nexthop-forwarding-address nexthop_forwarding_address
              commit
```

注：

- **address-pool** *pool_name*：アドレス プールの名前を指定します。 *pool_name* は 文字列である必要があります。
- **ipv6**：プールの IPv6 モードを開始します。
- **address-ranges**：ネクスト ホップ転送アドレスを使用して、IPv6 アドレス範囲とプレフィックス範囲のアドレスを指定します。

（注） IANA IPv6 構成は BNG により使用されます。

- **address-range** *start_ipv6_address end_ipv6_address* ：IPv6 アドレス範囲の開始アドレスと終了アドレスを指定します。
- **nexthop-forwarding-address** *nexthop_forwarding_address*：ネクストホップ転送アドレスを指定します。
- **prefix-range** *prefix_value* **length** *prefix_length*：IPv6 アドレス内のプレフィックス値と長さを指定します。
- **nexthop-forwarding-address** *nexthop_forwarding_address*：ネクスト ホップ転送アドレスを指定します。

• **prefix-ranges** ：IPv6 アドレスのプレフィックス範囲を指定します。

（注） SMF は、IAPD IPv6 構成のみをサポートしています。

- **split-size per-cache** *number_of_addresses*：IPAM キャッシュを割り当てるチャンクあたりの IPv6 アドレスの数を指定します。
- **split-size-per-dp** *number_of_addresses*：データプレーンに割り当てるチャンクあたりの IPv6 アドレスの数を指定します。
- **prefix-range** *prefix_value* **length** *prefix_lengthnexthop_forwardng_address* **nexthop-forwarding-address** ：ネクスト ホップ転送アドレスで IPv6 アドレス内のプレフィックス値と長さを指定します。

### 設定例

次に、設定例を示します。

```
ipam
 instance 1
  address-pool ISE-Pool1
   vrf-name ISP
   tags
    dnn cisco_vlan400.com
   exit
   ipv6
    address-ranges
      address-range 1000::1 1000::ffff nexthop-forwarding-address :9001::3
      prefix-range 2607:fc20:1010:: length 98 nexthop-forwarding-address :9001::3
    prefix-ranges
       split-size
         per-cache 32768
         per-dp    32768
       exit
       prefix-range 2607:fc20:1010:: length 44 nexthop-forwarding-address :9001::3
  exit
 exit
```

# SMF タグの構成

SMF タグを構成するには、次の構成例を使用します：

```
config
   ipam
      instance gr_instance_id
         address-pool pool_name
            tags
               nssai nssai_value
               dnn dnn_name
               serving-area serving_area_value
               commit
```

注：

- **address-pool** *pool_name*：アドレス プールの名前を指定します。 *pool_name* は 文字列である必要があります。
- **tags**：プールの追加プロパティを一般的な方法で設定するには、プール タグを指定します。
  - **nssai** *sains_value*：プールの NSSAI タグを指定します。*ns_value* は文字列である必要があります。
  - **dnn** *dnn_value*：プールの ロケーション DNN または DNN タグを指定します。 *dnn_value* は 文字列である必要があります。

**Note**

- **pool-selection nssai** 構成に基づいて、SMF はタグとして「slice + dnn」を IPAM に送信します。
- NSAI 値は、SMF スライスの設定名と一致している必要があります。

  - **serving-area** *serving_area_value*：プールのサービスエリア タグを指定します。 *serving_area_value* は 文字列である必要があります。

### SMF タグの構成例

次に、設定例を示します。

```
config
   ipam
      instance 1
         address-pool
                  tags
                     nssai one
                     dnn two
                     serving-area three
                     end
```

### 同じ SMF スライス構成名を持つ IPAM タグの構成例

```
ipam
 instance 1
  address-pool p1
   tags
    nssai slice1
    dnn   dnn1

  address-pool p2
   tags
    nssai slice1
    dnn   dnn2
```

## IPv4 アドレス範囲のしきい値の構成

IPAMは、プール使用のしきい値をモニタリングし続けます。構成されたしきい値に基づいて、IPAM は次の空きアドレス範囲を要求するか、アドレス範囲を解放します。

IPv4 しきい値を構成するには、次の構成例を使用します：

```
config
   ipam
      instance gr_instance_id
         address-pool pool_name
            ipv4
               threshold
                  upper-threshold percentage
                  commit
```

注：

- **address-pool** *pool_name*：アドレス プールの名前を指定します。 *pool_name* は 文字列である必要があります。
- **ipv4**：プールの IPv4 モードを開始します。
- **threshold**：しきい値サブモードに入ります。
- **upper-threshold** *percentage*：IPv4 上限しきい値をパーセンテージで指定します。

以下に設定例を示します。

```
config
   ipam
      instance 1
         address-pool p1
                  ipv4
                     threshold
                        upper-threshold 80
                        end
```

### プールのしきい値の確認

各プールの現在のしきい値の概要を表示するには **show ipam pool** コマンドを使用します。

**show ipam pool** コマンドの出力例を次に示します。

```
show ipam pool
================================================================
PoolName   Ipv4Utilization  Ipv6AddrUtilization  Ipv6PrefixUtilization
```

```
============================================================
  p1                80%             80%              0%
  p2                75%             0%               70%
============================================================
```

## IPv6 アドレス範囲のしきい値の構成

IPv6 アドレス範囲のしきい値を構成するには、次の構成例を使用します。

```
config
   ipam
      instance gr_instance_id
         address-pool pool_name
            ipv6
               address-ranges
                  threshold
                     upper-threshold percentage
                     commit
```

注：

- **address-pool** *pool_name*：アドレス プールの名前を指定します。 *pool_name* は 文字列である必要があります。
- **ipv6**：プールの IPv6 モードを開始します。
- **address-ranges**：IPv6 アドレス範囲サブモードを入力します。
- **threshold**：しきい値サブモードを開始します。
- **upper-threshold** *percentage*：IPv6 上限しきい値を指定します（%）

次に、設定例を示します。

```
config
   ipam
      instance 1
         address-pool p2
                  ipv6
                     address-ranges
                        threshold
                           upper-threshold 75
                           end
```

## IPv6 プレフィックス範囲のしきい値の構成

IPv6 プレフィックス範囲のしきい値を構成するには、次の構成例を使用します：

```
config
   ipam
      instance gr_instance_id
         address-pool pool_name
            ipv6
               prefix-ranges
                  threshold
                     upper-threshold percentage
                     commit
```

注：

- **address-pool** *pool_name*：アドレス プールの名前を指定します。 *pool_name* は 文字列である必要があります。
- **ipv6**：プールの IPv6 モードを開始します。
- **prefix-ranges**：IPv6 プレフィックス範囲サブモードを入力します。
- **threshold**：しきい値サブモードを開始します。
- **upper-threshold** *percentage*：IPv6 上限しきい値を指定します（%）

次に、設定例を示します。

```
config
   ipam
      instance 1
         address-pool p3
                  ipv6
                     prefix-ranges
                        threshold
                           upper-threshold 78
                           end
```

## IPv4 アドレス範囲分割の構成

IPv4 アドレス範囲分割を構成するには、次の構成例を使用します：

```
config
   ipam
      instance gr_instance_id
         address-pool pool_name
            ipv4
               split-size per-cache number_of_addresses
               split-size per-dp number_of_addresses
               commit
```

注：

- **address-pool** *pool_name*：アドレス プールの名前を指定します。 *pool_name* は 文字列である必要があります。
- **ipv4**：プールの IPv4 モードを開始します。
- **split-size per-cache** *number_of_addresses*：IPAM キャッシュを割り当てるチャンクあたりの IPv4 アドレスの数を指定します。2 の累乗で指定します。IPAM サーバは、この構成を使用します。

  *number_of_addresses* は 、2 ～ 262144 の範囲の整数である必要があります。
- **split-size-per-dp** *number_of_addresses*：データ プレーンに割り当てるチャンクあたりの IPv4 アドレスの数を指定します。2 の累乗で を指定します。IPAM キャッシュは、この構成を使用します。

  *number_of_addresses* は 、2 ～ 262144 の範囲の整数である必要があります。

次に、設定例を示します。

```
config
   ipam
      instance 1
         address-pool p1
                  ipv4
                     split-size per-cache 1024
                     split-size per-dp 256
                     end
```

## IPv6 アドレス範囲分割の構成

IPv6 アドレスとプレフィックス アドレスの範囲分割を構成するには、次の構成例を使用します：

```
config
   ipam
      instance gr_instance_id
         address-pool pool_name
            ipv6
               address-ranges
                  split-size per-cache number_of_addresses
                  split-size per-dp number_of_addresses
                  exit
               prefix-ranges
                  split-size per-cache number_of_addresses
                  split-size per-dp number_of_addresses
                  commit
```

注：

- **address-pool** *pool_name*：アドレス プールの名前を指定します。 *pool_name* は 文字列である必要があります。
- **ipv6**：プールの IPv6 モードを開始します。
- **address-ranges**：IPv6 アドレス範囲サブモードを入力します。
- **split-size per-cache** *number_of_addresses*：IPAM キャッシュを割り当てるチャンクあたりの IPv4 アドレスの数を指定します。2 の累乗で指定します。IPAM サーバは、この構成を使用します。

  *number_of_addresses* は 、2 ～ 262144 の範囲の整数である必要があります。
- **split-size-per-dp** *number_of_addresses*：データ プレーンに割り当てるチャンクあたりの IPv4 アドレスの数を指定します。2 の累乗で を指定します。IPAM キャッシュは、この構成を使用します。

  *number_of_addresses* は 、2 ～ 262144 の範囲の整数である必要があります。
- **prefix-ranges**：IPv6 プレフィックス範囲サブモードを入力します。

次に、設定例を示します。

```
config
   ipam
      instance 1
         address-pool p1
                  ipv6
                     address-ranges
                        split-size per-cache 4096
                        split-size per-dp 1024
                        exit
                     prefix-ranges
                        split-size per-cache 8192
                        split-size per-dp 2048
                        end
```

## グローバルなしきい値の構成

グローバルしきい値を構成するには、次の構成例を使用します：

```
config
   ipam
      instance gr_instance_id
         threshold
            ipv4-addr percentage
            ipv6-addr percentage
            ipv6-prefix percentage
            commit
```

注：

- **threshold**：しきい値サブモードを開始します。
- **ipv4-addr** *percentage*：IPv4 しきい値をパーセンテージで指定します。
- **ipv6-addr** *percentage*：IPv6 しきい値を指定します（%）
- **ipv6-prefix** *percentage*：IPv6 プレフィックス しきい値をパーセンテージで指定します。

次に、設定例を示します。

```
config
   ipam
      instance 1
         threshold
                  ipv4-addr 80
                  ipv6-addr 75
                  ipv6-prefix 70
                  end
```

### プールの詳細の確認

このセクションは、SMF 内にある IPAM の統合確認を説明します。

特定のプール名の詳細を表示するには、 **show ipam pool** *pool_name* コマンドを使用します。

次に、 **show ipam pool** *pool_name* コマンドの出力例を示します。

```
show ipam pool p1
-----------------------------------------------------------
Ipv4Addr   [Total/Used/Threshold] = 7680 / 7680 / 80%
Ipv6Addr   [Total/Used/Threshold] = 0 / 0 / 0.00%
```

```
Ipv6Prefix [Total/Used/Threshold] = 512 / 512 / 80%
Instance ID = 1
------------------------------------------------------------
```

## IPAM 送信元の構成

IPAM ソースを構成するには、次の構成例を使用します。

```
config
   ipam
      instance gr_instance_id
         source local
            source external ipam
               host ip_address
               port port_number
               vendor type
               commit
```

注：

- **source local**：プールのソースとしてローカル データ ストアを入力します。
- **source external ipam** ：プールのソースとして外部 IPAM サーバを入力します。
- **host** *ip_address* ：外部 IPAM サーバのホスト名を指定します。
- **port** *port_number* ：外部 IPAM サーバのポートを指定します。
- **vendor** *type*：外部 IPAM サーバのベンダー タイプを指定します。

次に、設定例を示します。

```
config
   ipam
      instance 1
         source external ipam
            host 209.165.200.225
            port 10000
            vendor cisco
            end
```

## IPAM 統合構成の確認

このセクションでは、SMF での IPAM の統合を確認する方法について説明します。

## データ プレーンの詳細の確認

特定のデータ プレーン（ユーザー プレーン）の詳細を表示するには、 **show ipam dp** *data_plane_name* コマンドを使用します。

**show ipam dp** *data_plane_name* コマンドの出力例を次に示します。

```
show ipam dp UPF-100
------------------------------------------------------------
Ipv4Addr   [Total/Used/Threshold] = 512 / 100 / 20%
Ipv6Addr   [Total/Used/Threshold] = 0 / 0 / 0.00%
Ipv6Prefix [Total/Used/Threshold] = 512 / 300 / 70%
```

```
Instance ID = 1
------------------------------------------------------
```

## データ プレーンのしきい値の確認

各データ プレーン（ユーザー プレーン）の現在のしきい値の概要を表示するには **show ipam dp** 、 コマンドを使用します。

**show ipam dp** コマンドの出力例を次に示します。

```
show ipam dp
==================================================================
DpName     Ipv4Utilization  Ipv6AddrUtilization  Ipv6PrefixUtilization
==================================================================
UPF-100           20%              40%                70%
UPF-200           40%              20%                20%
==================================================================
```

## データ プレーンに割り当てられた IPv4 アドレス範囲の確認

**show ipam dp** *data_plane_name* **ipv4-addr** コマンドを使用して、データ プレーンに割り当てられている IPv4 アドレスの範囲を表示します。

**show ipam dp** *data_plane_name* **ipv4-addr** コマンドの出力例を次に示します。

```
show ipam dp UPF-100 ipv4-addr
=============================================================================================================
Flag  Indication: S(Static) O(Offline) R(For Remote Instance)
G:N/P Indication: G(Cluster InstId) N(Native NM InstId) P(Peer NM InstId)
=============================================================================================================
StartAddress          EndAddress       AllocContext   Route              G:N/P
Utilization   Flag
=============================================================================================================
209.165.200.225  209.165.200.253  Pool-1        209.165.200.224/27 1:1/0     99.60%

209.165.201.1    209.165.201.30   Pool-2        209.165.201.0/27   1:1/0     99.60%
    R
=============================================================================================================
```

## データ プレーンに割り当てられた IPv6 アドレス範囲の確認

**show ipam dp** *data_plane_name* **ipv6-prefix** コマンドを使用して、データ プレーンに割り当てられている IPv6 アドレスの範囲を表示します。

**show ipam dp** *data_plane_name* **ipv6-prefix** コマンドの出力例を次に示します。

```
show ipam dp UPF-100 ipv6-prefix
=============================================================================================================
Flag  Indication: S(Static) O(Offline) R(For Remote Instance)
G:N/P Indication: G(Cluster InstId) N(Native NM InstId) P(Peer NM InstId)
=============================================================================================================
StartAddress                  EndAddress                AllocContext       Route
           G:N/P    Utilization   Flag
=============================================================================================================
2001:DB80:8f20::              2001:fc20:8f20:ffff::     ims-ipv6-pool1(n6)
2001:fc20:8f20::/48      1:1/0    99.60%
2001:fc20:8f21::              2001:fc20:8f21:ffff::     ims-ipv6-pool1(n6)
2001:fc20:8f21::/48      1:0/1    99.80%
2001:fc20:8f22::              2001:fc20:8f22:ffff::     ims-ipv6-pool1(n6)
2001:fc20:8f22::/48      1:0/1    0.00%         R
```

```
2001:fc20:8f23::              2001:fc20:8f23:ffff::     ims-ipv6-pool1(n6)
2001:fc20:8f23::/48      1:1/0    0.00%         R
2001:fc20:8f49::              2001:fc20:8f49:ffff::     ims-ipv6-pool1(n6)
2001:fc20:8f49::/48      1:1/0    34.42%
2001:fc20:8f4f::              2001:fc20:8f4f:ffff::     ims-ipv6-pool1(n6)
2001:fc20:8f4f::/48      1:0/1    33.58%
==========================================================================================
```

## IP プール選択方法の構成

次の構成を使用して、IP プールの選択方法を構成します。

```
config
nssai name nssai_name
    dnn dnn
    pool-selection [ pool_selection_method  ]
    sdt sdt_value
    sst sst_value
    tai-group-list tai_group_list
    end
```

注：

- **pool-selection [** *pool_selection_method* **]**：IP プールの選択方法を DNN または NSSSAI に構成します。 **pool-selection** のデフォルト値は *dnn*です。スライスの **pool-selection [** *nsnai* **]** を構成する場合、その UPF のすべての DNN の IPAM 構成で、「slice1+dnn」を構成します。

（注） スライスベースのプールの選択はサポートされていません。

### 設定例

次に、IP プール選択方法の構成例を示します。

```
nssai name slice1
pool-selection [nssai]
exit

nssai name slice2
pool-selection [nssai dnn]
exit

nssai name slice3
exit
```

（注） プール選択方法が構成されていない場合、デフォルト値の **pool-selection [** *dnn* **]** が使用されます。

## UPF グループ プロファイルの IP プール 選択の構成

IP プール選択用の UPF グループ プロファイルを構成するには、次の構成例を使用します。

（注） この構成は、スライス ベースの IP プールをサポートするために必要です。

```
config
  profile network-element upf upf_name
    upf-group-profile upf_group_profile_name
    dnn-list dnn_list_value
    end
```

注：

- **profile network-element upf** *upf_name*：UPF のプロファイル名を指定します。
- **upf-group-profile** *upf-group_profile_name* ：UPF グループ プロファイル名を指定します。*upf_group_profile_name* の 値は文字列である必要があります。
- **dnn-list** *dnn_list_value*：UPF ノードがサポートする DNN のリストを指定します。*dnn_list_value* 値は、DNN リスト値の範囲を含む文字列である必要があります。

**設定例**

次に、設定例を示します。

```
profile network-element upf upf1
   upf-group-profile group1
   dnn-list [dnn1, dnn2]
```

## IP プール選択用のスライス グループ リストの構成

IP プール選択用のスライス グループ リストを構成するには、次の構成例を使用します。

（注） この構成は、スライス ベースの IP プールをサポートするために必要です。

```
config
  profile upf-group upf_group_profile_name
    slice-group-list slice_group_list_name
    end
```

注：

- **profile upf-group** *upf_group_profile_name*：指定された UPF ネットワーク構成に関連付ける必要がある UPF グループ名を指定します。 *upf_group_profile_name* の 値は英数字の文字列である必要があります。
- **slice-group-list** *slice_group_list_name*：UPF ノードがサポートするスライス グループのリストを指定します。 *slice_group_list_name* の値は、スライス グループの範囲を含む文字列である必要があります。

**設定例**

次に、設定例を示します。

```
profile upf-group group1
 slice-group-list [ slice1 ]
exit
```

（注） IP プール選択の NSSAI 構成に基づいて、SMF はタグとして「slice + dnn」を IPAM に送信します。

**例**

```
profile network-element upf upf1
upf-group-profile group1
 dnn-list [dnn1, dnn2, dnn3]

profile upf-group group1
 slice-group-list [slice1, slice2 slice3]
exit
```

# 静的 IP サポート

## 機能説明

***Table 314:*** **機能の履歴**

| 機能 | リリース | 説明 |
|---|---|---|
| 重複スタティック IP の検出と解決 | 2024.03.4 | この機能は、同じ静的 IP が 2 つの異なる UE または同じ UE または DNN に属する 2 つの異なる PDU セッションに割り当てられるエラーシナリオを処理するメカニズムを提供します。<br>この機能により、そのような重複する IP 割り当てが検出され、競合を防ぐための適切なアクションが実行されます。<br>導入されたコマンド：<br>**condition duplicate-ip** ：このコマンドは、ポリシールール管理構成で使用して、重複するスタティック IP 割り当てを検出し、そのようなセッション要求を拒否または終了します。 |

IPAM は、サブスクライバ管理システムのコア コンポーネントです。従来の IPAM 機能では、クラウド ネイティブのネットワーク環境では不十分であることを証明しています。したがって、IPAM には、クラウド ネイティブのサブスクライバ管理システムと連携するための追加の機能が必要です。

スタティック IP サポート機能により、IPAM を使用した SMF でのスタティック IP のサポートが可能になります。この機能は、次の機能をサポートしています。

- スタティック プールの構成：システムの稼働中にスタティック IP プールまたはスタティック IP アドレス範囲をダイナミックに追加および削除します。
- スタティック アドレス範囲をより小さなチャンクに分割し、設定された UPF に関連付けます。
- UPF 関連付け時に、静的アドレス範囲の予約に従ってプログラムルートを有効にします。
- DNN プロファイルでセカンダリ認証を有効にする。
- 予約済みアドレス範囲と認証応答から受信した Framed-IP に基づいて UPF を選択します。
- UPF の追加、削除、および Sx パスの失敗の処理
- 既存の UPF に DNN を追加する

### スタティック IP アドレスを使用したコール

SMF はスタティック IP アドレスを使用したコールをサポートしており、IP アドレスがスタティック プールに属しているかどうかを検証します。

SMF は、スタティック IP アドレスを使用してセッション要求の作成をサポートし、PAA で受信したセッション要求の作成も処理します。SMF は、要求された IP アドレスがスタティック プールで構成されているかどうかを確認し、セッションに同じ IP アドレスを割り当てます。IP アドレスがスタティック プールで構成されていない場合、SMF はセッションを拒否します。

**Important** リリース 2021.02 では、SMF は動的な IP 割り当てへのフォールバックをサポートしていません。

次の動作は、スタティック IP アドレスを持つセッションにのみ適用されます。

- SMF は、5G セッション作成手順中に UDM からのサブスクリプション応答でスタティック IP を受信すると、IP がスタティック プールの下で構成されている場合は、同じ IP アドレスを UE セッションに割り当てます。IP アドレスがスタティック プールで構成されていない場合、SMF はセッションを拒否します。
- RADIUS インターフェイスが有効で、RADIUS サーバがスタティック IP アドレスを返す場合、SMF はセッション作成要求またはサブスクリプション応答で受信した IP アドレスを無視します。

構成の誤りにより、複数の UE に同じスタティック IP アドレスが割り当てられる可能性があります。これは、同じ UE または DNN に属する 2 つの PDU セッションでも発生する可能性があり、ネットワークの競合が発生し、予期しない動作が発生する可能性があります。

後続の接続中に重複する IP アドレスが検出されると、SMF はサブスクライバ セッションを終了してネットワークの競合を防ぎます。

標準的な 5G ネットワークの実装では、UDM がスタティック IP アドレスの割り当てにおいて最も高い優先順位を持ちます。ただし、セカンダリ認証が有効になっていて、サブスクライバがネットワークに再接続すると、AAA サーバが UDM よりも優先されます。

重複するスタティック IP 割り当てを検出する利点は次のとおりです。

- IP の競合を防止する：スタティック IP が一意に割り当てられるようにし、IP の競合によって引き起こされるネットワークの問題を防止します。
- ネットワークの信頼性の向上：重複するIP割り当てを検出して処理することにより、ネットワークの全体的な信頼性を向上させます。
- エラー処理の自動化：IP が重複するセッションを自動的に終了し、手動による介入の必要性を軽減します。

# 機能の仕組み

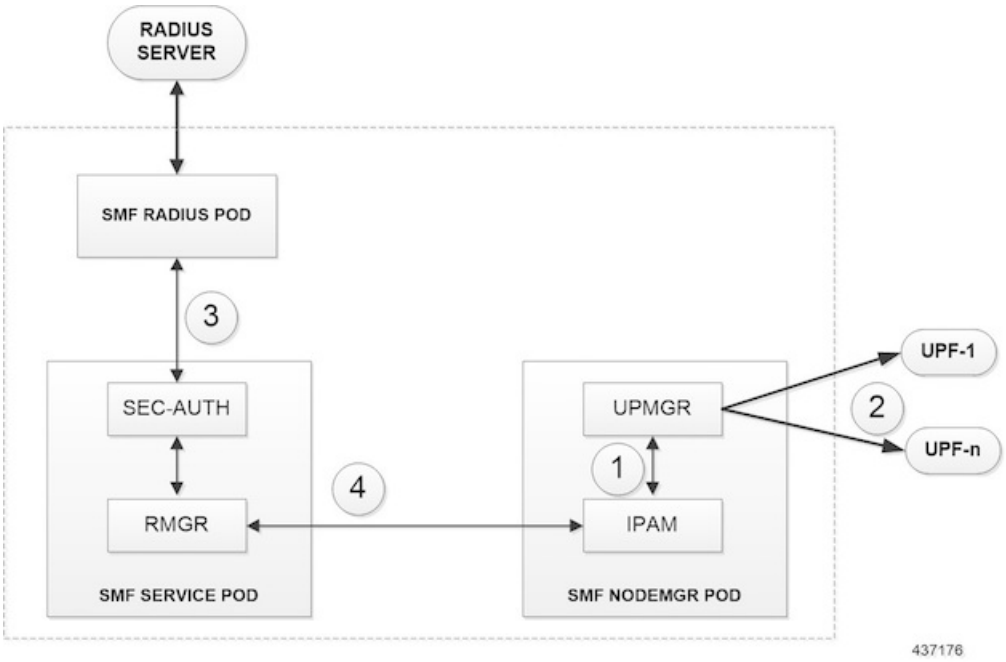
この項では、静的 IP のサポート機能の仕組みについて簡単に説明します。

SMF は、RADIUS などの外部 AAA サーバーからサブスクライバのフレーム化された IP アドレスを受信します。このシナリオでは、IPAM は個々の IP アドレス管理には関与しませんが、静的アドレス範囲のルート管理と UPF 管理は引き続き処理します。

IPAM は、SMF 構成に存在する UPF の数に従って、「静的」アドレス範囲を均等に分割します。ダイナミック IP とは異なり、IPAM はすべての静的 IP アドレス範囲を分割し、構成されたすべての UPF にそれらを割り当てます。IPAM は、外部 AAA サーバーがサブスクライバのフレーム化された IP を返すときに、UPF を関与させて選択します。IPAM は、この静的 IP を含むルートを検索し、ルートがすでに構成されている UPF を選択します。

次の図は、構成された UPF に静的 IP アドレスを割り当てる方法を示しています。

図 *172 :* 静的 *IP* アドレス管理手順




1. IPAM は、構成された UPF の数に基づいて、静的範囲を等しい数のアドレス範囲に分割します。
2. UPMGR は、関連付けられた UPF で対応する静的ルートをプログラムします。
3. サブスクライバは、RADIUS サーバーの承認応答から静的 IP を取得します。
4. SMF サービスは、アドレス範囲とノード マネージャからの UPF マップ割り当てに基づいて適切な UPF を選択します。

### アドレス範囲スプリット

特定のアドレス範囲をより小さなアドレス範囲に分割することは、IPAM サーバーおよびIPAM キャッシュの重要な機能です。次のガイドラインは、アドレス範囲の分割に関するものです：

- スプリット アドレス範囲のサイズは、認証局およびフォーマット識別子（AFI）タイプに応じた構成値またはデフォルト値によって異なります。
- 分割アドレス範囲のサイズは、2の累乗またはその最小値までにする必要があります。つまり、必要に応じてデータ プレーン（ユーザープレーン）にルートを追加できるように、サブネット/マスク表記で分割範囲を表すことができる必要があります。
- 構成されるアドレス範囲またはデフォルトのアドレス範囲サイズは2 の累乗にする必要があります。

アドレス範囲は、構成または最初の起動時に、すぐにさらに小さな範囲に分割する必要があります。これにより、サイズに基づいてアドレス範囲をより適切にソートし、実際のアドレス範

囲割り当て要求時の割り当てを高速化できます。モジュール間のアドレス範囲交換は、常に指示されたサイズ内にあります。

表 *315 : IPv4* アドレス範囲分割の例

| アドレス範囲 | スプリットサイズ（範囲あたりのアドレス数） | 範囲の分割<br>（* 奇数サイズの範囲） | ルート表記 |
|---|---|---|---|
| 209.165.200.225 - 209.165.200.254 | 128 | [1] 209.165.200.225 – 209.165.200.254<br>[2] 209.165.202.129 – 209.165.202.158 | [1] 209.165.200.224/27<br>[2] 209.165.202.128/27 |
| 209.165.201.1 – 209.165.201.30 | 256 | [1] 209.165.200.224 – 209.165.200.254<br>[2] 209.165.201.0 – 209.165.201.30<br>[3] 209.165.202.128 – 209.165.202.158<br>...<br>[n] 209.165.200.225 – 209.165.200.253 | [1] 209.165.201.1/27<br>[2] 209.165.200.224/27<br>[3] 209.165.202.128/27<br>...<br>[n] 209.165.201.0/27 |
| 209.165.200.229 – 209.165.200.253 | 256 | [1] 209.165.201.1 – 209.165.201.30 *<br>[2] 209.165.202.129 – 209.165.202.158<br>[3] 209.165.200.225 – 209.165.200.253 * | [1] 209.165.201.0/27<br>[2] 209.165.200.224/27<br>[3] 209.165.202.128/27 |

表 *316 : IPv6* アドレス範囲分割の例

| アドレス範囲 | スプリットサイズ（範囲あたりのアドレス数） | 範囲の分割<br>（* 奇数サイズの範囲） | ルート表記 |
|---|---|---|---|
| 1:: - 1::1000 | 1024 | [1] 1:: – 1::3FF<br>[2] 1::400 – 1::7FF<br>[3] 1::800 – 1::BFF<br>[4] 1::C00 – 1::FFF | [1] 1::/118<br>[2] 1::400/118<br>[3] 1::800/118<br>[4] 1::C00/118 |

| | | | |
|---|---|---|---|
| 1::3 - 1::1DEF | 1024 | [1] 1::3 – 1::3FF *<br>[2] 1::400 – 1::7FF<br>[3] 1::800 – 1::BFF<br>…<br>[n] 1::1C00 – 1::1DEF * | [1] 1::/118<br>[2] 1::400/118<br>[3] 1::800/118<br>…<br>[n] 1::1C00/118 |

**IPv6 アドレス範囲分割の例**

プレフィックス分割では、分割を実行するために 2 つの長さフィールドが必要です。

- ネットワークの長さ
- ホストの長さ

プレフィックスはこれら2つの長さフィールド間で分割され、新しいルートが計算されます。

例 1：network-length = 48、prefix-length = 64

合計（64-48）= 16 ビット（つまり、65536 個のプレフィックスが分割に使用可能）

例 2：network-length = 32、prefix-length = 56

合計（56-32）= 24 ビット（つまり、スプリットに使用可能な 1,600 万プレフィックス）

（注） SMF の場合、ホスト長は「64」としてハードコードされています。CLI を使用して構成できるのは network-length だけです。

表 *317 : IPv6* アドレス範囲分割の例

| プレフィックス範囲 | スプリットサイズ（範囲あたりのアドレス数） | 範囲の分割<br>（* 奇数サイズの範囲） | ルート表記 |
|---|---|---|---|
| 1:2:3::<br>Nw-len = 48<br>Host-len = 64 | 8192 | [1]1:2:3:: ... 1:2:3:1fff<br>[2]1:2:3:2000:: ... 1:2:3:2fff::<br>[3]1:2:3:3000:: ... 1:2:3:3fff::<br>... | [1]1:2:3::/51<br>[2]1:2:3:2000/51<br>[3]1:2:3:3000/51<br>... |

## コール フロー

ここでは、静的 IP コール フローについて説明します。

次の図は、スタティック IP アドレスの割り当てのコール フローを示しています。

*Figure 173:* スタティック *IP* コール フロー

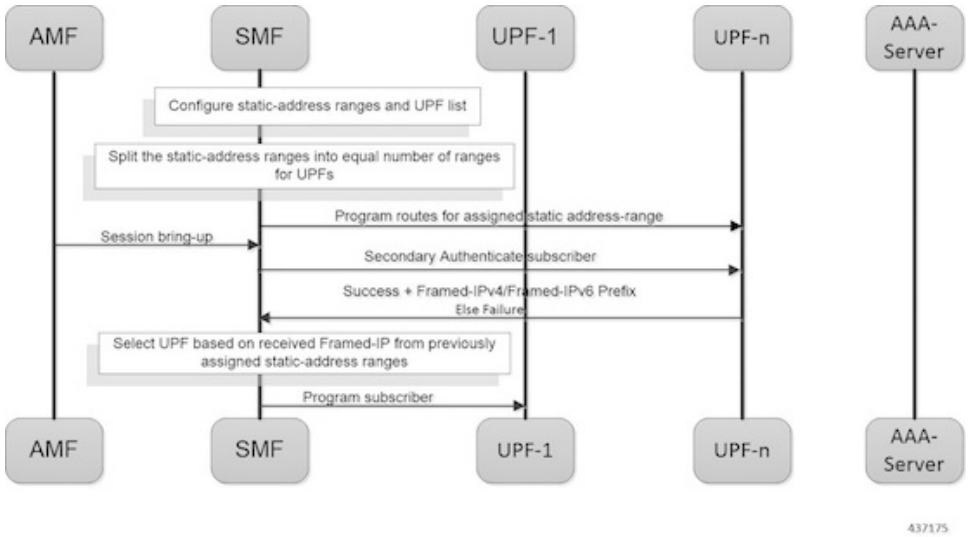



*Table 318:* 静的 *IP* コール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | 静的アドレス範囲と UPF リストを構成します。 |
| 2 | 静的アドレス範囲を UPF の同じ数の範囲に分割します。 |
| 3 | 割り当てられた静的アドレス範囲のプログラム ルートを有効にします。 |
| 4 | セッションを起動します。 |
| 5 | DNN プロファイルでセカンダリ認証を有効にする。 |
| 6 | SMF は、認証要求を RADIUS サーバーに送信します。<br>RADIUS サーバーは、サブスクライバの静的 IP を使用して認証応答を送信します。SMF は静的 IP に基づいて UPF を選択し、プログラミングを続行します。 |
| 7 | サブスクライバのプログラミングを完了します。 |

# DNN の追加

この項では、DNN 追加の一連の操作について説明します。

1. 対応する DNN を使用して IPAM で静的 IP プールを作成します。
2. DNN プロファイルの追加します。
3. 該当する場合は、UPF を追加します。

4. DNN の IP アドレス範囲を使用可能な UPF に関連付けます。

（注） ルートは、明示的な Sx 関連付け時に RegisterUpf 要求の一部として追加されます。

## 静的 IP アドレス範囲の追加

このセクションでは、SMF で静的IPアドレス範囲を追加する一連の操作について説明します。

- 新しい静的 IP アドレス範囲が単一のスタック IP プールに追加されると、IP アドレス範囲は構成に従って分割され、負荷分散方式で使用可能な UPF に関連付けられます。
  1. 最初の関連付けと同様に、中間関連付けも、構成された UPF の数に対する IP アドレスの数に基づいて行われます。
  2. UPF がすでに IPAM に登録されている場合：
     - ルートの追加がトリガーされるか、または
     - 即時対処なし

- デュアル スタック プールが構成されている場合、すべての IP アドレス範囲（IPv4 と IPv6 の両方）が、負荷が最も少ない UPF に関連付けられます。
  - UPF がすでに IPAM に登録されている場合：
    - ルートの追加がトリガーされるか、または
    - 即時対処なし

## 静的 IP プールの追加

このセクションでは、SMF で静的 IP プールを追加する一連の操作を説明します。

- 単一のスタック IP プールが設定されている場合、IP アドレス範囲は設定に従って分割され、負荷分散方式で利用可能な UPF に関連付けられます。
  1. 最初の関連付けと同様に、中間関連付けも、構成された UPF の数に対する IP アドレスの数に基づいて行われます。
  2. UPF がすでに IPAM に登録されている場合：
     - ルートの追加がトリガーされるか、または
     - 即時対処なし

- デュアル スタック プールが構成されている場合、すべての IP アドレス範囲（IPv4 と IPv6 の両方）が、負荷が最も少ない UPF に関連付けられます。

- UPF がすでに IPAM に登録されている場合：
  - ルートの追加がトリガーされるか、または
  - 即時対処なし

## UPF の追加

この項では、UPF 追加の一連の操作について説明します。

1. UPF が追加されると、NodeMgr は IP のリストを IPAM に送信します。
2. 新しい静的IPプールまたは静的IPアドレス範囲が設定されている場合、この機能により、ロード バランシング モデルに基づいた UPF のルート アソシエーションが有効になります。

（注） 新しいまたは既存の DNN がそれぞれ新しいまたは既存の UPF に追加される場合も、同じ手順が適用されます。

3. 既存の静的IPプールまたは範囲を新しいUPFに再配布するには、次の手順を実行します。
   - プール/範囲をオフラインとしてマークする
   - サブスクライバをクリア
   - IP プールまたは範囲の削除
   - IP プールまたは範囲を再度追加します。

     この手順により、チャンクが新しい UPF に割り当てられます。

## UPF の削除

このセクションでは、既存の UPF を削除する一連の操作を説明します。

1. 既存の UPF を削除するには、まずその UPF を「オフライン」とマークします。

   適切な CLI コマンドを実行して、セッションを手動でクリアします。
2. NodeMgr は、UPF の削除について IPAM に通知します。
3. IPAM は、削除された UPF のすべての DNN から他の使用可能な UPF にスタティック アドレス範囲を移動します。
4. Nodemgr は IPAM への ReleaseUpf を開始します。IPAM は、ダイナミック アドレス範囲をフリーリストに解放します。
5. Nodemgr は、N4 関連付けリリース メッセージを UPF に送信し、キャッシュから UPF をクリーンアップします。

（注） UPFがオフラインとしてマークされておらず、取り外す前に手動クリーンアップが実行されていない場合、システムの動作が異常になる可能性があります。

## 静的 IP アドレス範囲の削除

このセクションでは、SMF でスタティック IP アドレス範囲を削除する一連の操作について説明します。

1. スタティック IP プールから IP アドレス範囲を削除するには、まずプールを「オフライン」とマークします。
2. オフライン IP アドレス範囲から割り当てられた IP アドレスを持つ新しいコールを拒否します。
3. 既存のサブスクライバを削除します。既存のサブスクライバを削除するには、次の CLI コマンドを実行します。

   ```
   clear subscriber ipv4-range { pool_name | start_of_range }
   clear subscriber ipv6-range { pool_name | start_of_range }
   ```

4. スタティック IP アドレス範囲の構成を削除し、登録済みの UPF へのルートの削除をトリガします。

## 静的 IP プールの削除

このセクションでは、SMF で静的 IP プールを削除する一連の操作を説明します。

1. 静的 IP プールを削除するには、まずプールを「オフライン」とマークします。
2. オフライン IP プールから割り当てられた IP アドレスを持つ新しいコールを拒否します。
3. 既存のサブスクライバを削除します。既存のサブスクライバを削除するには、次の CLI コマンドを実行します。

   ```
   clear subscriber ipv4-pool pool_name
   clear subscriber ipv6-pool pool_name
   ```

4. すべてのサブスクライバが削除されたら、IP プール構成を削除し、登録済みの UPF へのルートの削除をトリガーします。

## オフライン UPF との Sx の関連付けの削除

ここでは、オフライン UPF との関連付けを削除する一連の操作について説明します。

1. **profile-network-element-upf** 構成で UPF をオフラインとして構成します。

   SMF は、新しいセッションの特定の UPF へのダイナミック IP の選択と関連付けを停止します。

2. NodeMgr がオフライン UPF に関する構成変更通知を受信します。

SMF は、新しいセッションまたは関連付けの特定の UPF へのスタティック IP の選択と関連付けを停止します。

3. NodeMgr は、すでに関連付けられている UPF のハートビート メッセージを確認します。
4. NodeMgr は、リリース指示で UPF からの N4 関連付け更新を確認応答します。

   この手順は、IPAM のスタティックおよびダイナミック チャンク割り当てには影響しません。

   IPAM モジュールは、UPF のオフライン ステータスを認識していません。新しい IP プールまたはアドレス範囲を追加するためのオフライン UPF が含まれる場合があります。

## UPF の Sx パス障害

このセクションでは、UPF における Sx パス障害の一連の操作を説明します。

1. NodeMgr は **clear subscriber** コマンドを開始します。
2. NodeMgr は UnRegisterUpf を IPAM に送信します。
3. IPAM は、ダイナミック IP アドレス範囲を解放し、自由範囲リストに移動します。
4. IPAM は、UPF の静的 IP アドレス範囲を保持します。Sx パスの障害は、静的 IP アドレス マッピングには影響しません。

## 制限事項

静的 IP サポート機能には、次の制限があります：

- システムが実行されている場合、
  - ダイナミックから静的、およびスタティックからダイナミックへのプールの変更はサポートされていません。
  - UPF の追加または削除はサポートされていません。
  - DNN は UPF から削除できません。
- SMF は、プレフィックス長が付加された IPv6 アドレスをサポートしていません。
- アドレスの範囲の分割は、UPF の数と範囲内のアドレスの数に基づいて最適にする必要があります。

  **次に例を示します。**

  範囲内に 2 つの UPF と 1024 のアドレスが指定されている場合は、per-dp-split-size を 512 に指定します。

  3 つの UPF と 1024 のアドレスがある場合は、per-dp-split-size を 256 に指定します。
- デュアルス タック IPAM プールをシングル スタックに変更、またはシングル スタック IPAM プールをデュアル スタックに変更することはサポートされていません。

- SMF はできません
  - 構成ミスにより、異なる SMF でホストされている異なる UE への重複 IP 割り当てを検出します。
  - DHCP IPAM が有効になっていて、重複する IP が割り当てられているシナリオを処理します。

# 静的 IP の構成

## スタティック IP プールの構成

スタティック IP サポート機能を構成するには、次の構成例を使用します。

```
config
  ipam
    instance gr_instance_id
      address-pool pool_name
        static
        end
```

注：

- **ipam**：IPAM 構成モードを開始します。
- **address-pool** *pool_name*：プールの構成を開始するプールの名前を指定します。*pool_name* は 文字列である必要があります。
- **static**：スタティック IP モードを有効にします。

## 重複静的 IP 検出の構成

UDM と AAA サーバによって割り当てられた重複する静的 IP アドレスを検出して解決するには、次の手順に従います。

### 始める前に

- DNNプロファイルをイベント管理ポリシーに関連付けます。詳細については、QoS プロファイルとイベント管理ポリシーを DNN プロファイルに関連付ける構成 （1278 ページ）のセクションを参照してください。

### 手順

**ステップ 1** イベント管理ポリシーの構成 （930 ページ）

**ステップ 2** セッション終了に対処するためのルールと条件の定義 （930 ページ）

**ステップ 3** アクション定義ポリシーでの終了アクションの構成 （931 ページ）

## イベント管理ポリシーの構成

優先度ベースのイベント処理を構成するには、次の手順を実行します。この構成により、DNN プロファイルに関連するイベントを管理するためのポリシーが設定されます。

### 手順

**ステップ 1** イベント イベント ポリシー構成モードを開始します。

**policy eventnmgmt** *policy_eventmgmt_name*

例：

```
[smf] smf# config
[smf] smf(config)# policy eventmgmt emp
```

**ステップ 2** イベント管理ポリシーの優先順位を定義し、実行する新しいコール、ルール、およびアクション名としてイベント タイプを構成します。

**priority** *priority_number* **event new-call ruledef** *ruledef_name* **actiondef** *actiondef_name*

例：

```
[smf] smf(config-eventmgmt-emp)# priority 2 event new-call ruledef rd1 actiondef ad1
```

有効な優先範囲は 1 ～ 65535 です。 *ruledef_name* と *actiondef_name* は、いずれも 1 ～ 63 文字の英数字文字列です。

**ステップ 3** 構成を保存してコミットします。

例：

```
[smf] smf(config-eventmgmt-emp))# end
```

## セッション終了に対処するためのルールと条件の定義

セッション終了を処理するためのルールと条件を定義するには、次の手順に従います。

### 手順

**ステップ 1** ルール定義ポリシー構成モードを開始します。

**policy rulemgmt** *policy_rulemgmt_name*

例：

```
[smf] smf# config
[smf] smf(config)# policy rulemgmt rm1
```

**ステップ 2** ruledef の名前を指定して、ポリシーに追加します。

**ruledef** *ruledef_name*

例：

```
[smf] smf(config-rulemgmt-rm1)# ruledef rd1
```

**ステップ 3** **duplicate-ip is true ip-type is static** として条件を定義します。

例：

```
[smf] smf(config-ruledef-rd1)# condition duplicate-ip is true ip-type is static
```

この条件を構成することで、SMF は再接続シナリオ中に重複する静的 IP アドレスを検出できます。

**ステップ 4** 構成を保存してコミットします。

例：

```
[smf] smf(config-ruledef-rd1))# end
```

## アクション定義ポリシーでの終了アクションの構成

重複する静的 IP アドレスを持つ新しいコールに対するセッション終了アクションを構成するには、次の手順を実行します。

### 手順

**ステップ 1** アクション管理ポリシー コンフィギュレーション モードを開始します。

**policy actionmgmt** *policy_actionmgmt_name*

例：

```
[smf] smf# config
[smf] smf(config)# policy actionmgmt act1
```

**ステップ 2** アクション定義ポリシーを指定します。

**actiondef** *actiondef_name*

例：

```
[smf] smf(config-actionmgmt-act1)# actiondef ad1
```

**ステップ 3** アクションを実行する優先順位を指定します。次に、セッションを終了するアクションを構成します。

**priority** *priority_number* **action terminate-session**

例：

```
[smf] smf(config-actiondef-ad1)# priority 1 action terminate-session
```

**ステップ 4** 構成を保存してコミットします。

例：

```
[smf] smf(config-actiondef-ad1)# end
```

**ステップ 5** （オプション） **show running-config policy actionmgmt** コマンドを使用して、重複するスタティック IP アドレスを持つ新しいコールに対して PDU セッションの終了が有効になっているかどうかを確認します。

**例：**

```
[[smf] smf# show running-config policy actionmgmt act1
Thu Jun 20 18:50:12.888 UTC+00:00
policy actionmgmt act1
actiondef ad1
priority 1 action terminate-session
```

**bold** 内のテキストは、SMF でセッション終了が有効になっていることを示しています。

### 重複静的 IP 検出の構成例

このセクションでは、重複静的 IP 検出を有効にする構成例を示します。

```
profile dnn internet
    eventmgmt-policy em1
exit

policy eventmgmt em1
   priority 2 event new-call ruledef rd1 actiondef ad1
exit

policy rulemgmt rm1
    ruledef rd1
        condition duplicate-ip is true ip-type is static
        exit
exit

policy actionmgmt am1
    actiondef ad1
        priority 1 action terminate-session
    exit
exit
```

# 統計情報サポート

smf_service_resource_mgmt_stats および smf_service_node_mgr_stats は、静的 IP 割り当てタイプ情報の詳細を提供します。

これらの統計情報の ip_req_type 属性は、次のラベルをサポートします。

- ip-static-subscription：サブスクリプションに基づく静的 IP 割り当て情報。
- ip-static-radius：RADIUS に基づくスタティック IP 割り当て情報。

これらの統計は、重複する静的 IP 割り当てが原因で切断されたセッションのモニタリングに使用します。

- disk_pdusetup_static_duplicate_ip：重複する静的 IP が検出されたために SMF によって拒否された 5G セッションの総数。

- disk_pdnsetup_static_duplicate_ip：重複する静的 IP の検出が原因で SMF によって拒否された 4G セッションまたは Wi-Fi セッションの総数。

# IPAM によるデュアルスタック静的 IP サポート

## 機能説明

SMF は、IPAM を使用してデュアル スタック静的 IP をサポートしています。デュアルスタック セッションの場合、AAA サーバーは、Access-Accept メッセージの一部として IPv4 と IPv6 の両方のアドレス プレフィックスを送信します。SMF-IPAM 構成では、IPv4 と IPv6 の両方のアドレス プレフィックスが同じプールに追加されます。IPAM は、IPv4 ルートと IPv6 ルートの両方を単一の UPF に割り当てます。

UPF の選択中、ノード マネージャ アプリケーションは IPAM からの IPv4 アドレスと IPv6 アドレスの両方の UPF を使用して、それらを適切に処理します。

## 機能の仕組み

SMF は、次の方法で IPAM を介してデュアル スタック スタティック IP をサポートします。

- プールから UPF へのマッピング：使用可能な UPF の数に基づいて、IPv4 アドレス範囲と IPv6 プレフィックス範囲がより小さいチャンクに分割されます。次に、ペア（チャンク）が同じ IPAM プールに構成されます。

  IPAM は、1 つのデュアルスタック プールで構成されているすべてのアドレスとプレフィックスを、受信した方法で UPF に割り当てます。AAA サーバは、同じペアからデュアルスタック アドレスを返します。これらのアドレスから、SMF はデュアルスタック プログラミング用に 1 つの UPF を選択します。

  アドレス数とプレフィックス数のロードバランシングが管理されている。IPAM は、デュアルスタック スタティックプールから UPF へのマッピングのみを実行します。

- アドレス範囲非分割構成：IPAM は「非分割」構成を使用して、アドレス範囲がより小さなチャンクに分割されるのを防ぎます。この構成は、特定の範囲に対して複数のルートがプログラミングされるのを防ぐのに役立ちます。

次の表に、エラーまたは例外とその処理方法を示します。

*Table 319:* エラーと例外処理

| エラーまたは例外 | 例外処理 |
|---|---|
| IPv4 UPF と IPv6 UPF の構成が正しくない | 1. アクティブなUPFを選択します。両方のUPFがアクティブの場合は、IPv4アドレスを含むUPF を選択します。<br>2. その他のスタックの IP 情報をリセットし、それに応じて PDU セッションタイプを更新します。 |
| IPv4 アドレスが無効または null です | IPv4 アドレスを使用した UPF を選択し、それに応じて PDU セッションタイプを更新します。 |
| IPv6 プレフィックスが無効であるか null です | IPv6 アドレスを使用した UPF を選択し、それに応じて PDU セッション タイプを更新します。 |
| IPv4アドレス、IPv6プレフィックスが無効です | IPv4 アドレスと IPv6 プレフィックスの両方を拒否する。 |

## 制限事項

デュアル スタック静的 IP サポート機能には、次の制限があります。

- システムが実行モードの場合、「no-split」構成の変更はサポートされません。

# デュアル スタック 静的 IP の構成

このセクションでは、IPAM を使用してデュアル スタック静的 IP サポートを構成する方法について説明します。

## IPAM 分割なしの構成

IPAM 非分割を設定するには、次の構成例を使用します。

```
config
   ipam
      instance gr_instance_id
         address-pool pool_name
         ipv4
            split-size no-split
            exit
         ipv6 prefix_ranges
            split-size no-split
            exit
         exit
```

注：

- **split-size no-split**：IPv4 アドレス範囲または IPv6 プレフィックス範囲がより小さいチャンクに分割されないようにします。

# IPAM オフライン モードのサポート

## 機能説明

SMF では、デフォルトで、ダイナミック プール、IPv4、または IPv6 アドレス範囲のダイナミック プールへの追加がサポートされています。新しいチャンクは、DNN などのそれぞれのタグに追加され、同じプールから割り当てられます。

## 機能の仕組み

### 前提条件

プールまたは IPv4/IPv6 アドレス範囲をオフラインにする必要があります。また、アドレス範囲の使用率をゼロにしてから、構成から削除する必要があります。

ダイナミック プール、またはダイナミック プールから IPv4 または IPv6 のアドレス範囲を削除するプロセスを次に示します。

1. プールまたはアドレス範囲をオフラインとして構成します。その後、IPAM は、それぞれのプールまたはアドレス範囲からのアドレスの割り当てを停止します。
2. 次の **clear subscriber** CLI コマンドを使用して、オフライン モードに構成されているそれぞれのプールまたはアドレス範囲に基づいてサブスクライバを削除します。
   - **clear subscriber ipv4-pool** *pool_name*
   - **clear subscriber ipv4-range** *pool_name/start_of_range*
   - **clear subscriber ipv6-pool** *pool_name*
   - **clear subscriber ipv6-range** *pool_name/start_of_range*
3. 次の **cdl show** CLI コマンドを使用し、すべてのサブスクライバが削除されるまで待ちます。
   - **cdl show sessions count summary filter { key ipv4-pool:** *pool_name* **condition match }**
   - **cdl show sessions count summary filter { key ipv4-range:** *pool_name/start_of_range* **condition match }**
   - **cdl show sessions count summary filter { key ipv6-pool:** *pool_name* **condition match }**
   - **cdl show sessions count summary filter { key ipv6-range:** *pool_name/start_of_range* **condition match }**
   - **cdl show sessions count summary slice-name** *slice_name*

4. 次の **show ipam** コマンドを使用して、削除したプールまたはアドレス範囲に対応するすべてのアドレス範囲/チャンクが使用率を示していないことを確認します。
   - **show ipam pool** *pool-name*
   - **show ipam pool** *pool-name* **ipv4-addr | ipv6-prefix**
   - **show ipam dp** *dp-key* **ipv4-addr | ipv6-prefix**

**Note** 一致するプールまたはアドレス範囲を削除するためにサブスクライバがすべてクリアされていても、対応するチャンクが **show ipam** コマンドで使用率を示している場合は、IPAM の調整を使用してそのような古い IP のリリースをトリガします。検疫期間が満了した後にのみ、古い IP が解放されます。

IPAM 調整の詳細については、「*IPAM データ調整*」セクションを参照してください。

5. すべてのサブスクライバが削除されたら、IPAM 設定からプールまたはアドレス範囲を削除します。

# IPAM オフライン モードに構成

このセクションでは、プール、IPv4 アドレス範囲、および IPv6 プレフィックス範囲の IPAM オフライン機能を構成する方法について説明します。

## オフライン モードにプールを構成

プール全体をオフライン モードに構成するには、次の構成例を使用します：

```
config
   ipam
      instance gr_instance_id
         address-pool pool_name
            offline
            end
```

注：

- **address-pool** *pool_name*：プールの構成を開始するプールの名前を指定します。*pool_name* は 文字列である必要があります。
- **offline**：プールをオフライン モードに構成

## IPv4 アドレス範囲をオフライン モードに設定

IPv4 アドレスの範囲をオフライン モードに構成するには、次の構成例を使用します：

```
config
   ipam
      instance gr_instance_id
```

```
address-pool pool_name
   vrf-name vrf_name
   ipv4
      address-range start_ipv4_address end_ipv4_address offline
      end
```

注：

- **address-pool** *pool_name*：プールの構成を開始するプールの名前を指定します。*pool_name* は 文字列である必要があります。
- **ipv4**：IPv4 モードに入ります。
- **address-range** *start_ipv4_address end_ipv4_address* **offline**：IPv4 アドレス範囲の開始と終了の IP アドレスを指定します。
  - **offline**：選択したアドレス範囲をオフライン モードに設定します。

## オフライン モードへの IPv6 プレフィックス範囲の設定

IPv6 プレフィックスの範囲をオフライン モードに構成するには、次の構成例を使用します：

```
config
   ipam
      instance gr_instance_id
         address-pool pool_name
         vrf-name vrf_name
            ipv6
               prefix-ranges
                  prefix-range prefix_valuelength prefix_lengthoffline
                  end
```

注：

- **address-pool** *pool_name*：プールの構成を開始するプールの名前を指定します。*pool_name* は 文字列である必要があります。
- **ipv6**： IPv6 モードを開始します。
- **prefix-ranges**：プレフィックス範囲モードを入力します。
- **prefix-range** *prefix_value* **length** *prefix_length* **offline**：IPv6 プレフィックス範囲のプレフィックス範囲とプレフィックス長を指定します。
  - **offline**：選択したアドレス範囲をオフライン モードに設定します。

# UPF ごとの IPAM 冗長性サポート

## 機能説明

SMF は、各 UPF の IPAM 冗長性とロード バランシングをサポートしています。ノード マネージャ マイクロサービスで実行されている IPAM には、各 UPF に関連付けられた 2 つの IPAM インスタンスがあります。1 つの IPAM インスタンスが非アクティブになると、もう 1 つの IPAM インスタンスが UPF のアドレス割り当て要求を管理します。

## 機能の仕組み

このセクションでは、UPF 機能ごとの IPAM 冗長性サポートの動作の簡単な説明を行います。

- ピア選択：ノード マネージャ ピアは UPF 関連付け中に選択されます。
- ピア IPAM への UPF 登録：UPF コールの登録中に、IPAM に UPF のピアのインスタンス ID が通知されます。IPAM は、特定の DNN のローカル データからルータを割り当て、ピア IPAM インスタンスがアクティブまたは非アクティブ状態かどうかを確認します。

  ピア IPAM インスタンスがアクティブな場合、ローカル インスタンス内の同じ UPF に登録し、応答としてルートを受信するために、REST コールがピア IPAM インスタンスに送信されます。

  ピア IPAM インスタンスが非アクティブの場合、ローカル インスタンスがリモート インスタンスの IPAM コンテキストを引き継ぎます。次に、ローカル インスタンスは UPF に登録され、ルートを受信して、データをキャッシュ ポッドに戻します。ピア インスタンスがアクティブになると、キャッシュ ポッドから同じデータを復元します。

  両方のインスタンスからのルートは、両方のインスタンスからのロードバランシングされたアドレス割り当てのために UPF に送信されます。
- 負荷分散モデルでのアドレス割り当て：1 つの UPF が 2 つの IPAM サーバに登録されると、SMF は負荷分散された任意のピアにアドレス割り当て要求を送信します。各 IPAM インスタンスは、ローカル アドレス ビットマップから新しいアドレスを割り当てます。1 つのピア インスタンスが非アクティブである場合、もう 1 つのピア インスタンスがすべての要求を処理します。
- アドレス リリース要求の処理：IPAM では、最初に IP を割り当てたインスタンスにアドレス リリース要求が送信されます。そのピアが非アクティブの場合、アドレス リリース要求がピア IPAM に送信されます。

  リモート インスタンスのアドレスの解放を受信する IPAM インスタンスは、これらのインスタンスをローカルでバッファし続け、キャッシュ ポッドを定期的に更新します。リモート ピアがアクティブになると、バッファに格納されたアドレスの解放要求が処理されます。

- UPF のリリース：UPF のリリース中にピア IPAM がアクティブになると、データをクリアするために REST コールが送信されます。ピア IPAM が非アクティブの場合、既存の IPAM インスタンスはリモート IPAM の動作データを引き継ぎ、UPF 情報をクリアして、キャッシュ ポッドを更新します。

# IPAM 隔離タイマー（IPAM Quarantine Timer）

## 機能説明

IPAM 隔離タイマーのサポート機能は、IP プール アドレスの IPAM 検疫タイマーをサポートします。この機能は、解放された IP アドレスを検疫タイマーが期限切れになるまでビジー状態に保ち、その IP アドレスが再利用されないようにします。各 IP プールにはタイマー値を構成する必要があります。この値は、最近解放されたアドレスが、割り当てに使用可能になる前に検疫状態である期間を決定します。タイマーの期限が切れた後、その IP アドレスは、サブスクライバによる割り当てのためのフリーアドレスのリストで使用可能になります。アドレス検疫タイマーのない解放された IP アドレスは、割り当てに使用中と見なされます。同じサブスクライバ ID であっても、アドレス検疫タイマーが作動するときにサブスクライバが再接続しようとすると、そのサブスクライバは同じ IP アドレスを受信しません。

## IPAM 隔離タイマーの構成

このセクションでは、IPAM 隔離タイマーの構成方法について説明します。

### IPAM 隔離タイマーの構成

このセクションでは、IPAM 隔離タイマーの構成方法について説明します。

```
config
   ipam instance instance_id
      address-pool pool_name
         address-quarantine-timer quarantine_timer_value




         end
```

注：

- **address-pool** *pool_name*：プールの構成を開始するプールの名前を指定します。 *pool_name* は 、アドレス プールの名前である必要があります。
- **address-quarantine-timer** *quarantine_timer_value*：隔離タイマーの値を秒単位で指定します。 *quarantine_timer_value* は 4 ～ 3600 秒の範囲である必要があります。デフォルト値は 4 です。

# IPAM 隔離タイマーの構成

このセクションでは、CDL 構成で IP アドレスを検証する方法について説明します。

## システム診断の IP 検証

このセクションでは、システム診断の IP 検証を有効または無効にする方法について説明します。

```
config
   system-diagnostics ip-validation enable ignore-mismatch-responses
   exit
```

注：

**system-diagnostics ip-validation ignore-mismatch-responses** ：アドレス検証中に CDL の不整合を無視します。

IP 検証の不一致応答は、IP の重複を避けるためにあります。この機能が有効になっている場合、SMF Nodemgr は、現在の IP が CDL 内の他のいずれかのレコードによってすでに使用されているかどうかをチェックします。レコードが見つからない場合は、IP アドレスが UE に割り当てられます。CDL レコードが見つかった場合は、新しい IP が UE に割り当てられます。

**重要** 検証での不一致への応答を無視することを有効にすると、パフォーマンスに一定の影響を与える可能性があります。

## 統計

**nodemgr_diag_ip_verify**

説明：Nodemgr to CDL IP 検証クエリ関連の統計を表示します

Metrics-Type：カウンタ

クエリ：sum(nodemgr_diag_ip_verify(namespace="$namespace") by (status)）

ラベル

ラベル：status

Value: success | duplicate_record_found | cdl_ipc_failure | ipv4_alloc_failed | ipv6_alloc_failed | unknown

- CDL で成功レコードが見つかりませんでした
- duplicate_record_found CDL で重複レコードが見つかりました
- cdl_ipc_failure CDL への検索 IPC 要求が失敗しました
- ipv4_alloc_failed IPV4 アドレス要求が失敗し、空き IP を 2 回取得できない

- ipv6_alloc_failed IPV6 プレフィックス要求が失敗し、空き IP を 2 回取得できない
- CDL への不明な IPC 要求が 2 回失敗し、放棄と IP の smf-service が返されました

**IPAM_Quarantine_Statistics**

説明：IPAM 検疫 IP バッチ関連の統計を表示します

Metrics-Type：カウンタ

クエリ：sum(IPAM_Quarantine_Statistics(namespace="$namespace") by (addressType, type)

ラベル

ラベル： pool

値：<name-of-pool>

ラベル：upf

値：<name-of-upf>

ラベル： addressType

値： IPv4 | IPv6PD

ラベル：タイプ

値： start_batch_qsize | end_batch_qsize pop_count_qtime | pop_count_qsize | avg_qtime_secs

- start_batch_qsize：バッチ処理の開始時の QT キュー内の IP の数
- end_batch_qsize：バッチ処理の終了時の QT キュー内の IP の数
- pop_count_qsize：qsize 制限により QT キューから削除された IP の数
- pop_count_qtime：qtime 制限により QT キューから削除された IP の数
- avg_qtime_secs：削除する前に IP が QT キューにあった平均時間（秒）

# IPAM データの照合

## 機能説明

SMF は、IPAM データを CDL レコードと調整するための IPAM データ調整機能をサポートしています。この機能は、EXEC モード CLI を介してトリガされます。IPAM 調整では、インスタンス レベル、プール レベル、およびチャンク レベルでトリガされます。

## IPAM 調整のトリガー

このセクションでは、インスタンス レベル、プール レベル、およびチャンク レベルで IPAM 調整をトリガーする方法について説明します。

## インスタンス レベルでの IPAM 調整のトリガ

インスタンス レベルで IPAM 調整をトリガーするには、次の CLI コマンドを使用します。

**reconcile ipam instance** *instance_id*

注：

- **reconcile ipam instance** *instance_id*：特定の GR インスタンス ID の IPAM 調整をトリガーします。

## プール レベルでの IPAM 調整のトリガ

プール レベルで IPAM 調整をトリガーするには、次の CLI コマンドを使用します。

**reconcile ipam instance** *instance_id* **pool-name** *pool_name*

注：

- **pool-name** *pool_name* ：特定のアドレス プールの IPAM 調整をトリガーします。

## チャンク レベルでの IPAM 調整のトリガー

チャンク レベルで IPAM 調整をトリガーするには、次の CLI コマンドを使用します：

**reconcile ipam instance** *instance_id* **pool-name** *pool_name* **chunk-start-ip** *chunk_start_ip_address*

注：

- **chunk-start-ip** *chunk_start_ip_address* ：IPAM 調整チャンクの開始 IP アドレスを指定します。

# IPAMの定期的調整

IPAM の調整は、CLI を介して手動でトリガーできます。また、 nodemgr の 起動時または GR ロールの切り替え後にもトリガーされます。

このプロセスでは、システムまたはソフトウェアに依存する手順のアップグレードが必要です。IPAM 調整設定を提供し、バックグラウンドで定期的に時間駆動型アクティビティを実行するには、サポートが必要です。

次の CLI 構成フレームワークを使用して、毎日の IPAM 調整アクティビティを実行するようにスケジュールできます：

- 特定の GR インスタンス ID
- GR インスタンス ID の下の特定のアドレス プール

IPAM 調整プロセスは、CDL に対して複数のクエリを実行し、サブスクライバセッションを取得して IPAM キャッシュデータ データを同期または更新します。

## 制限事項

この機能には、次の制限事項があります。

- システムのトラフィック負荷管理が少ない時間中に、定期的な IPAM 調整をスケジュールします。
- 1 日の同じ時間に複数の調整をスケジュールすることはサポートされていません。
- nodemgr は 、一度に 1 つの調整プロセスのインスタンスのみをトリガーできます。
- 複数の調整スケジュールをプール間で設定するには、2 つのトリガーの間に少なくとも 5 分の間隔を確保する必要があります。
- IPAM の調整は、非静的プールでのみサポートされます。

## 機能設定

更新された IPAM 構成 CLI フレーム ワークは、次をサポートします：

- GR インスタンス ID の調整のスケジュール
- 特定のアドレス プールのサポート

この機能を構成するには、次の構成を使用します。

```
config
   ipam
      instance <gr_instance_id>
         reconcile-schedule
            tod-hour <time_of_day_hour_value>
            tod-minute <time_of_day_minute_value>
…
      address-pool <pool_name>
         reconcile-schedule
            tod-hour <time_of_day_hour_value>
            tod-minute <time_of_day_minute_value>
            end
```

**注**：

- **ipam**：IPAM 構成を入力します。
- **instance** <*gr_instance_id*>：特定の GR インスタンス ID の IPAM 調整を指定します。
- **address-pool** <*pool_name*>：プールの名前を指定して、プールの構成を開始します。<*pool_name*> はアドレス プールの名前である必要があります。
- **reconcile-schedule**：調整に必要なスケジュールを指定します。time-of-day の値を時間と分で設定して、指定された時刻に毎日の調整をトリガする時間を設定できます。
- **tod-hour** <*time_of_day_hour_value*>：一日の必要な時間を時間単位で指定します。指定した時間を 0 ～ 23 の 24 時間形式で構成できます。

- **tod-minute** <*time_of_day_minute_value*>：一日の必要な時間を分単位で指定します。指定した分は、60 分の形式（0 ～ 59）で構成できます。

## 設定例

次の構成例では、IPAM が午前 00:00 に gr-instance-id 1 の調整をトリガする日次スケジュールを構成できます。

```
config
 ipam
  instance 1
   reconcile-schedule
    tod-hour   0
    tod-minute 0
   exit
```

次の構成例では、IPAM が毎日午後 10:30 に gr-instance-id 1 の testPool1 の調整をトリガする日次スケジュールを構成できます。

```
config
 ipam
  instance 1
   address-pool testPool1
    reconcile-schedule
     tod-hour   22
     tod-minute 30
    exit
    ipv4
     split-size
      per-cache 8192
      per-dp    1024
     exit
     address-range 209.165.200.225 209.165.200.254
    exit
   exit
  exit
```

# IPv6 プレフィックス委任

表 *320 :* 機能の履歴

| 機能名 | リリース情報 | 説明 |
|---|---|---|
| ローカル プールからの IPv6 プレフィックス委任 | 2024.04.0 | SMF は IPv6 プレフィックス委任をサポートしており、ユーザー機器（UE）および顧客宅内機器（CPE）がルータまたはセルラー ゲートウェイ デバイスを構成するために追加の IPv6 プレフィックスを要求できるようにしています。<br><br>委任されたプレフィックスの長さの許容範囲は 48 から 62 です。<br><br>この IPv6 プレフィックス委任は、サブスクライバの内部ネットワークとコア ネットワーク間のルータとして機能する CPE デバイスにプレフィックスを割り当てることで、サブスクライバ ネットワークをより効果的に管理できるため、サービス プロバイダにとって特に役立ちます。<br><br>**コマンドの導入**：次のコマンドがプロファイル DNN に導入されました。<br><br>**ipv6-prefix-delegation prefix length** *prefix_length*<br><br>**dnn prefix-delegation** *vdnn*<br><br>**デフォルト設定**：[Disabled]：有効にするには設定が必要。 |

SMF を介してネットワークを設定する場合、ルータにプレフィックスを委任できる柔軟性があります。SMF は、3GPP で定義されている手順を使用してルータまたはセルラー ゲートウェイ デバイスに IPv6 アドレス範囲を割り当て、プレフィックス委任を使用してルータの背後にある多くのデバイスに IP アドレスを割り当てます。

IPv6 プレフィックス委任機能により、ユーザー機器（UE）および顧客宅内機器（CPE）は、ルータまたはセルラー ゲートウェイ デバイスを構成するための追加の IPv6 プレフィックスを要求できます。

これらのルータまたはセルラーゲートウェイは、4g/5Gネットワークに対して一意の APN/DNN を使用して PDU セッションを作成する必要があります。

### IPv6 プレフィックス委任の主な機能

IPv6 プレフィックス委任機能の機能は次のとおりです。

- **DNN ごとの 1 つのプレフィックス長**：SMF は、データ ネットワーク名（DNN）ごとに 1 つのプレフィックス長のみをサポートします。許可されるプレフィックス長の範囲は 48 ー 62 です。
- **ローカル プール（IPAM）から委任されたプレフィックス**：SMF はローカル プールから委任されたプレフィックスを取得します（IP アドレス管理）。
- **委任されたプレフィックスの割り当て（Allocation of Delegated prefix）**：SMF は、DNN 構成に従って委任されたプレフィックスを割り当て、UPF に送信します。

次のコマンドを使用して、委任されたプレフィックスを持つセッションを確認およびクリアできます。

- Show subscriber コマンド：
  - show subscriber nf-service smf delg-prefix { starts-with dp }
  - show subscriber nf-service smf delg-prefix { starts-with dp-$prefixLength }
  - show subscriber count nf-service smf delg-prefix { starts-with dp-$prefixLength }
- Clear subscriber コマンド：
  - clear subscriber nf-service smf delg-prefix { starts-with dp }
  - clear subscriber nf-service smf delg-prefix { starts-with dp-$prefixLength }

（注） 上記のコマンドで **starts-with** の横に指定された値は、委任されたプレフィックス セッション キー **dp:dp-$prefixLength/$ipPool/$delegatedPrefix** と照合され、 **dp:<starts-with-val>**を含むすべてのセッションが含まれます。

たとえば、プレフィックス長が 61 および 62 のセッションが存在する場合、 **{starts-with dp-6}** にはキーが であるすべてのセッションが含まれます **dp:dp-61* & dp:dp-62***。

### SMF での IPv6 プレフィックス委任の前提条件

プレフィックス委任のサポートは UPF で必要です。

（注） IPv6 委任機能をサポートしていない古い UPF バージョンでは、実装の変更によってデコードエラーが発生しました。そのため、SMF でこの機能を有効にする前に UPF をアップグレードする必要があります。

# IPv6 プレフィックス委任の仕組み

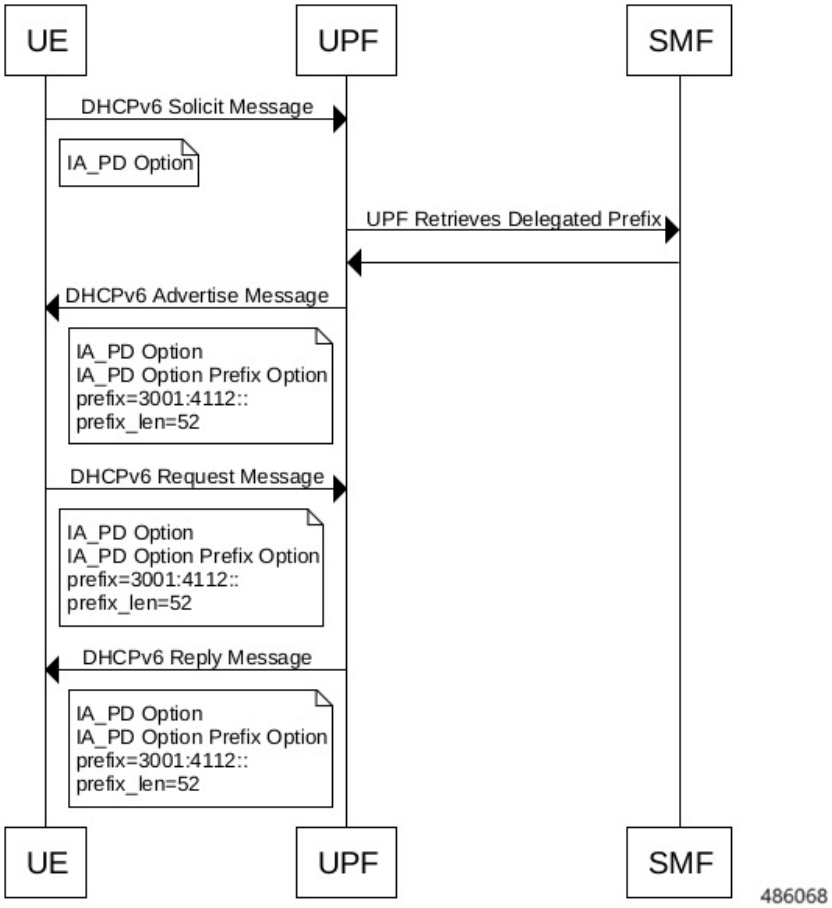
IPv6 プレフィックスの委任の段階は次のとおりです。

- [プロファイル DNN（Profile DNN）] と [プレフィックス長（Prefix length）] を構成して、ローカル プールからのプレフィックス委任を有効にします。構成手順については、「プロファイル DNN の構成」 および 「プレフィックス長の構成」 セクションを参照してください。

## IPv6 プレフィックス委任の割り当て

このセクションでは、IPv6 プレフィックス委任の割り当てにおけるコール フローとステージについて説明します。

図 *174 : IPv6* プレフィックスの割り当て




次の段階では、委任されたプレフィックスの割り当てと管理のための SMF（セッション管理機能）と UPF（ユーザー プレーン機能）間の相互作用について説明します。

1. UE/CPE は DHCPv6 要請メッセージを UPF に送信します。UE/CPE では、IA_PD プレフィックス オプションにプレフィックス長を含めることができます。
2. UPF は、UE の PDN セッションが確立されたときに作成された GTPU トンネル上の N3 または S1U/S5U インターフェイスを介して要求されたメッセージを受信します。UPF は IP プールをローカルで管理しないため、UPF はプロキシ DHCP サーバとして機能し、SMF からプレフィックスを受信します。SMF は、DNN 構成に従って委任されたプレフィックスを提供します。構成されたプレフィックス長の値とは異なるプレフィックス長で DHCP 請求を受信した場合、SMF は要求を拒否します。プレフィックス長が受信されない場合、SMF は構成されたプレフィックス長に従って割り当てます。
3. UPF は、IA_PD オプションに委任されたプレフィックスを含む DHCP アドバタイズ メッセージを使用して、DHCPv6 要請メッセージに応答を送信します。

   SMF は、ローカル IPAM プールから委任されたプレフィックスを割り当てます。

# プロファイル DNN を構成

次の手順を使用して、ローカル プールからプレフィックス委任を有効にするための DNN プロファイルを構成します：

## 手順

**ステップ 1** グローバル構成モードにログインします。

**ステップ 2** **profile dnn** *dnn_profile_name* コマンドを入力します。 **ipv6-prefix-delegation** は、このDNNのプレフィックス委任機能を有効にします。プレフィックス委任には、個別のDNNプロファイルが必要です。プレフィックスの委任では、DNN ごとに 1 つのプレフィックス長のみがサポートされます。

**例**：

```
config
      profile dnn dnn_profile_name
              ipv6-prefix-delegation prefix length prefix_length
              dnn prefix-delegation vdnn
      exit
```

**ステップ 3** **ipv6-prefix-delegation prefix length** *prefix_ length* コマンドを入力します。これは、この dnn にサポートされている委任されたプレフィックス長を示し、サポートされている範囲は 48 ～ 62 です。要求されたプレフィックス長のない DHCP 要請メッセージを UE が送信すると、SMF はこれをプレフィックス長として使用します。

**例**：

```
config
      profile dnn dnn_profile_name
              ipv6-prefix-delegation prefix length prefix_length
              dnn prefix-delegation vdnn
      exit
```

**ステップ 4** **dnn prefix-delegation** *vdnn* コマンドを入力して、プレフィックス委任（PD）vDNN を構成します。委任されたプレフィックスには個別の IP プールが必要であるため、この構成は必須です。

**例**：

```
config
      profile dnn dnn_profile_name
              ipv6-prefix-delegation prefix length prefix_length
              dnn prefix-delegation vdnn
      exit
```

（注）
PD vDNN は専用 UPF に関連付けられます。関連付けられていない場合、動作は未定義です。PD DNNはUPF選択には使用されません。 SMF と UPF が正しく構成されていることが想定されます。

UPF が異なる場合に PD IP プールが複数のチャンクに分割されるのを避けるために、PDDNN に専用の UPF を関連付けることを推奨します。

SMF は、委任されたプレフィックスと非委任されたプレフィックスを割り当てるためにコントロール プレーンで構成されているのと同じ UE IP プールの使用をサポートしていません。

**ステップ 5** **exit** コマンドを入力して現在の構成モードを終了します。

# IPAM の構成

次の手順を使用して、プレフィックス委任用に SMF IPAM を構成します。

### 手順

**ステップ 1** IPAM 構成モードを開始します。

```
ipam
 instance 1
  address-pool poolv6_pfx62
   vrf-name ISP1
   tags
    dnn pd_vdnn
   exit
   ipv6
    prefix-ranges
     split-size
      per-cache 256
      per-dp    256
     exit
     prefix-length 62
     prefix-range 2607:fb91:8a00:: length 52
    exit
   exit
  exit
 exi
```

**ステップ 2** IP 割り当てのプレフィックス長を指定するには、 **prefix-length** *prefix_value* コマンドを入力します。2 から 64 までの整数である必要があります。プールから割り当てられるIPは、常に指定されたプレフィックスのみになります。DNNタグは、DNNプロファイルの構成で設定されている **pd_vdnn** と一致する必要があります。

**例**：

```
ipam
 instance 1
  address-pool poolv6_pfx62
   vrf-name ISP1
   tags
    dnn pd_vdnn
   exit
   ipv6
    prefix-ranges
```

```
    split-size
     per-cache 256
     per-dp    256
    exit
    prefix-length 62
    prefix-range 2607:fb91:8a00:: length 52
   exit
  exit
 exit
exi
```

（注）
UPF でのデコードエラーを回避するために、SMF で IPv6 プレフィックス委任機能を有効にする前に UPF をアップグレードする必要があります。

（注）
IPAM のプレフィックス長は、プロファイル DNN で設定されたプレフィックス長と一致する必要があります。

PD プールの IP プールサイズと設定は、UPF ごとに必要なチャンク数とチャンク サイズの制限を考慮して計画する必要があります。

### 次のタスク

ローカル プールからのプレフィックス委任を確認

# ローカル プールからのプレフィックス委任を確認

ローカル プールからのチャンクの作成を確認するには、次の **show ipam pool** コマンドを使用しま：

## ipam pool を表示

次の出力は、プールでのチャンクの作成を示しています。

```
[smf] smf# show ipam pool poolv6_pfx62
-------------------------------------------------------
 Ipv4Addr   [Total/Used/Utilization] = 0 / 0 / 0.00%
 Ipv6Addr   [Total/Used/Utilization] = 0 / 0 / 0.00%
 Ipv6Prefix [Total/Used/Utilization] = 1024 / 0 / 0.00%
 Instance ID                         = 1
-------------------------------------------------------

[smf] smf# show ipam pool poolv6_pfx62 ipv6-prefix
=============================================================================
Flag Indication: S(Static) O(Offline)
=============================================================================
StartAddress               EndAddress               AllocContext   Flag  GroupId
=============================================================================
2607:fb91:8a00::/62        2607:fb91:8a00:3fc::/62   Free:CP
2607:fb91:8a00:400::/62    2607:fb91:8a00:7fc::/62   Free:CP
2607:fb91:8a00:800::/62    2607:fb91:8a00:bfc::/62   Free:CP
2607:fb91:8a00:c00::/62    2607:fb91:8a00:ffc::/62   Free:CP
=======================
```

## メトリック

このセクションでは、IPv6プレフィックス委任について収集および報告されるメトリックについて説明します。これらのメトリックは、プレフィックスの委任の数（プレフィックス長ごと）を示すために必要です。

次のメトリックは、次のラベルで強化されます。

- **smf_service_resource_mgmt_stats**：このカウンタは、SMF サービス リソース管理統計の合計数を追跡します。既存の「ip_req_type」ラベルは「pd_alloc」と「pd_dealloc」で拡張されます。
- **nodemgr_resource_mgmt_resp_stats** ：このカウンタは、ノードマネージャのリソース管理応答統計情報の総数を追跡します。既存の「req_type」ラベルは「pd_req_alloc」と「pd_req_rel」で拡張されます。
- 「**smf_sess_report_stats**」は 、新しいレポート タイプ用に機能強化されています。

# IPAM の隔離 Qsize の構成

このセクションでは、IPAM隔離検疫キューサイズサポート機能の構成方法について説明します。

## IPAM 隔離キュー サイズの構成

このセクションでは、IPAM 隔離タイマーの構成方法について説明します。

```
config
   ipam instance instance_id
      address-pool pool_name
         address-quarantine-qsize quarantine_queue_size
         exit
        exit
```

注：

- **ipam**：IPAM 構成を入力します。
- **address-pool** *pool_name*：プールの構成を開始するプールの名前を指定します。 *pool_name* は 、アドレス プールの名前である必要があります。
- **address-quarantine-qsize** *quarantine_queue_size*：隔離キューのサイズの値を指定します。デフォルト値は 0 です。

  QT 処理中に、隔離タイマーの期限切れに関わらず、隔離キュー内の過剰な IP アドレスが強制的に解放されます。

# IP アドレス プールをオーバーラップ

## 機能説明

重複する IP アドレス プール機能により、IP アドレスをダイナミックに割り当てる柔軟性が向上します。この機能を使用すると、重複 IP アドレス プール グループを設定して、異なるアドレス空間を作成し、異なるアドレス空間で同じ IP アドレスを同時に使用できます。

一意の DNN と VRF タイプを使用して、異なるプール間で重複する IP アドレス範囲を構成できます。

## 重複する IP アドレス プールの構成

重複するスタティック IP アドレス プールを構成するには、次の構成例を使用します。

```
config
ipam instance instance_id 1
source local
address-pool pool1
  static
  vrf-name vrf1@ISP
  tags
   dnn dnn1
  exit
  ipv4
   split-size
    per-cache 256
    per-dp    256
   exit
   address-range 209.165.200.225 209.165.200.254
  exit
exit
address-pool pool2
  static
  vrf-name vrf2@ISP
  tags
   dnn dnn2
  exit
  ipv4
   split-size
    per-cache 256
    per-dp    256
   exit
   address-range 209.165.200.225 209.165.200.254
  exit
exit
exit
```

次に、重複する IP アドレス プールの構成例を示します。

```
config
ipam instance instance_id 1
source local
address-pool pool1
  vrf-name vrf1@ISP1
  tags
```

```
   dnn dnn1
  exit
  ipv4
   split-size
    per-cache 256
    per-dp    256
   exit
   address-range 209.165.200.225 209.165.200.254
  exit
exit
address-pool pool2
  vrf-name vrf2@ISP2
  tags
   dnn dnn2
  exit
  ipv4
   split-size
    per-cache 256
    per-dp    256
   exit
   address-range 209.165.200.225 209.165.200.254
  exit
exit
exit
```

# 使用率の低い IP チャンクの自動再利用

## 機能説明

SMF は、さまざまな UPF ノードに割り当てられている十分に活用されていない IP チャンクの自動再利用をサポートしています。[使用率のしきい値（Utilization Threshold）] と [非アクティブのしきい値（Inactivity Threshold）] を構成することにより、SMF は自動再利用プロセスを定期的にまたは即座にトリガできます。

IP チャンクの十分な使用率と非アクティブは、非アクティブ タイマーの構成に基づいて検出されます。非アクティブで低使用率が検出されると、SMF は IP チャンクを使用してすべてのサブスクライバをクリアすることによって IP チャンクの再利用をトリガします。SMF は UPF へのルート削除もトリガします。

## 制限事項

次に、SMF での十分に活用されていない IP チャンクの自動再利用に関する既知の制限を示します。

- 十分に活用されていない IP チャンクの再利用中に、解放されたすべての IP は、構成されたアドレス プール レベルの隔離時間（QT）を実行する必要があります。
- 再利用された IP チャンクからの IP がアクティブなサブスクライバ セッションに関連付けられている場合、SMF はサブスクライバ セッションを切断し、セッションの切断を確認することが期待されます。
- スケジュール済みの再利用手順中は、ローリング更新を避ける必要があります。

# 十分に活用されていないIPチャンクのインスタント再利用プロセスの構成

次の構成を使用して、IP チャンクの十分でない使用率の瞬時に再利用を実行します。

**exec-ipam reclaim-chunk { utilization-threshold** *utilization_threshold* **inactivity-threshold** *inactivity_threshold* **[ instance** *grInstance* **] [ pool-name** *poolName* **] [ chunk-start-ip** *ip* **] }**

注：

- **exec-ipam**：このコマンドは、IPAM コマンドを実行します。
- **reclaim-chunk**：この CLI は IP チャンクの再利用手順を実行します。
- **utilization-threshold** *utilization_threshold*：この CLI は、修復の使用率のしきい値を構成するために使用されます。
- **inactivity-threshold** *inactivity_threshold*：この CLI は、修復の非アクティブしきい値を構成するために使用されます。
- **instance** *grInstance*：この CLI では、GR インスタンス ID を設定できます。
- **pool-name** *poolName*：この CLI では、プール名を定義できます。
- **chunk-start-ip** *ip*：この CLI では、特定のプールのチャンク スタート IP を定義できます。

## 設定例

次に、インスタント IP チャンク再利用プロセスの構成例を示します：

```
exec-ipam reclaim-chunk utilization-threshold 2 inactivity-threshold 180 instance 1
pool-name poolv4 chunk-start-ip 209.165.201.1
```

# 十分に活用されていない IP チャンクの定期再利用プロセスの構成

次の構成を使用して、IP チャンクの十分でない使用率の定期的な再利用をトリガーします。

```
config
   ipam
      instance instance_id
         chunk-reclamation { schedule tod-hour tod_hour_value schedule
tod-minute tod_min_value utilization-threshold utilization_threshold
inactivity-threshold inactivity_threshold }
         exit
      exit
   exit
```

注：

- **chunk-reclamation**：この CLI は、定期的な IP チャンクの再利用を構成するために使用されます。

- **schedule**：この CLI は、チャンクの再利用プロセスの時刻値を構成するために使用されます。
- **tod-hour** *tod_hour_value*：この CLI は、チャンクの再利用プロセスの時刻の値を構成するために使用されます。 **tod-hour** の値の範囲は <0-23> です。
- **tod-minute** *tod_min_value*：この CLI は、チャンクの再利用プロセスの時刻（Time-of-day）の分の値を構成するために使用されます。 **tod-minute** の値の範囲は <0-59> です。
- **utilization-threshold** *utilization_threshold*：この CLI は、修復の使用率のしきい値を構成するために使用されます。 **utilization-threshold** の値の範囲は <0-20> です。デフォルト値は 2 です。
- **inactivity-threshold** *inactivity_threshold*：この CLI は、修復の非アクティブしきい値を構成するために使用されます。 **inactivity-threshold** の値の範囲は <0 ー 3600> です。デフォルト値は 1800 です。

（注） トラフィックが少ないことが予想される場合は、Time-of-Day を構成することをお勧めします。

## 設定例

次に、定期的な IP チャンクの再利用プロセスの構成例を示します：

```
config
  ipam
    instance <instance>
      chunk-reclamation
        schedule tod-hour <0..23> tod-minute <0..59>
        utilization-threshold <0..20>
        inactivity-threshold  <0..3600>
      exit
    exit
  exit
exit
```

## 設定の確認

構成を確認するために次の show コマンドを使用する必要があります：

```
[smf] smf# show running-config ipam instance 1 chunk-reclamation
Tue May  16 20:36:58.887 UTC+00:00
ipam
instance 1
  chunk-reclamation
   schedule tod-hour 22
   schedule tod-minute 10
   utilization-threshold 5
   inactivity-threshold  600
  exit
exit
exit
```

# OAM サポート

このセクションでは、この機能でサポートされているメトリックスについて説明します。

## バルク統計

チャンク再利用プロセスの一部として、次のカウンタがサポートされます。

**IPAM_chunk_reclamation_count**：再要求された IP チャンクの合計数を指定するカウンタです。IP チャンクが再要求されたときにトリガされます。このメトリックは、GR インスタンス、IP プール、アドレス タイプ、UPF、リモート インスタンス、およびトリガ状態のレベルで維持する必要があります。

**disk_ip_chunk_reclamation**：このカウンタが理由として **smf_active_call_disconnect_stats** および **smf_disconnect_stats** 統計の下に追加されます。このメトリックは、チャンクの再評価によってクリアされたセッションに導入されます。

# UPF の一意の IP プール

## 機能説明

この機能を使用すると、SMF で次のタスクを実行できます。

- UPF が同じ IP プールを共有しないように、エッジ UPF に特定の IP プールのセットを割り当てる
- エッジ UPF がダウンしている場合、中央に配置された UPF にフォールバックする

UPF への一意の IP プールを割り当てるために、SMF はロケーション DNN に基づいて、IPAM 構成で IP アドレス プールを持つタグを使用します。次に、SMF は、各 DNN の UPF の選択を構成するときに、このタグ名を関連付けます。

中央の UPF へのフォールバックを実装するために、SMF にはエッジ UPF がダウンした場合に中央の UPF を構成するオプションがあります。

## 一意の IP プールの SMF の構成

このセクションでは、UPF への IP アドレス割り当てをキュー解除するために必要な構成について説明します。

この機能の構成には、次の手順が含まれます。

- ロケーション DNN に基づくタグの構成 （958 ページ）
- UPF フォールバックの有効化 （958 ページ）

# ロケーション DNN に基づくタグの構成

ロケーションベースの DNN プロファイルを定義するには、次の構成例を使用します：

```
config
   profile location-dnn location_dnn_name
       location-area-group la_group_name profile dnn_profile_name
       end
```

注：

- **profile location-dnn** *location_dnn_name*：ロケーションベースの DNN プロファイルの名前を指定します。
- **location-area-group** *la_group_namednn_profile_name* **profile** ：サブスクライバが属するロケーション エリア グループの名前と DNN プロファイルを指定します。

  このプロファイルで定義されたロケーションに基づいて、SMF は IP プールにタグを付け、各 DNN の UPF を選択します。

# UPF フォールバックの有効化

一意の IP プールを使用して UPF フォールバック機能を有効にするには、次の設定例を使用します：

```
config
   profile dnn dnn_profile_name
       dnn rmgr dnn_name fallback secondary_dnn_name
       end
```

注：

- **profile dnn** *dnn_profile_name*：DNN プロファイルの名前を指定します。
- **dnn rmgr** *dnn_name* **fallback** *secondary_dnn_name*：プライマリおよびセカンダリ DNN の名前を指定します。

  SMF は、次の条件のいずれかが満たされている場合に、DNN に基づいて中央に配置された UPF へのフォールバックを有効にします：

  - ロケーションに基づいて選択された IP プールと UPF が失敗します。
  - 構成された DNN の UPF がダウンしています。
  - UEの場所は構成されていません。

# 設定例

次に、一意の IP プールの割り当てに使用される構成の例を示します。

```
config
profile location-area-group lag1
 tai-group tai-grp
exit
profile location-area-group lag2
```

```
 tai-group tai-grp2
exit
profile location-dnn dnnloc-1
 location-area-group  lag1 profile dnnprof-ims-1
 location-area-group  lag2 profile dnnprof-ims-2
exit
policy dnn polDnn
 dnn ims profile dnnprof-ims //fallback dnn profile
 dnn ims location-dnn-profile  dnnloc-1 //location-based dnn profile
exit
profile upf-group upf-group1
 location-area-group-list [ lag1 ] //grouping upf based on location
 failure-profile FHUP
exit
profile upf-group upf-group2
 location-area-group-list [ lag2 ] //grouping upf based on location
 failure-profile FHUP
exit
profile upf-group upf-group3 // central upf group - no location tag
 failure-profile FHUP
exit

profile network-element upf nfprf-upf1
 node-id           n4-peer-DAUI0301
 n4-peer-address ipv4 209.165.201.3
 n4-peer-port      8805
 upf-group-profile upf-group1//ims-lag1 picks upf-group1, based on location
 dnn-list          [ ims-lag1 magenta-ims-dnn sos-pool-ipv6 ]
 capacity          10
 priority          1
exit
profile network-element upf nfprf-upf3
 node-id           n4-peer-DAUI0303
 n4-peer-address ipv4 209.165.201.4
 n4-peer-port      8805
 upf-group-profile upf-group1//ims-lag1 picks upf-group1, based on location
 dnn-list          [ ims-lag1 magenta-ims-dnn sos-pool-ipv6 ]
 capacity          10
 priority          1
exit
profile network-element upf nfprf-upf5
 node-id           n4-peer-DAUI0305
 n4-peer-address ipv4 209.165.201.5
 n4-peer-port      8805
 upf-group-profile upf-group2//ims-lag2 picks upf-group2, based on location
 dnn-list          [ ims-lag2 magenta-ims-dnn sos-pool-ipv6 ]
 capacity          10
 priority          1
exit
profile network-element upf nfprf-upf7
 node-id           n4-peer-DAUI0307
 n4-peer-address ipv4 209.165.201.6
 n4-peer-port      8805
 upf-group-profile upf-group2//ims-lag2 picks upf-group2, based on location
 dnn-list          [ ims-lag2 magenta-ims-dnn sos-pool-ipv6 ]
 capacity          10
 priority          1
exit
profile network-element upf nfprf-upf8
 node-id           n4-peer-DAUI0308
 n4-peer-address ipv4 209.165.201.7
 n4-peer-port      8805
 upf-group-profile upf-group3//ims-central picks upf-group3, if location is not available
```

```
 dnn-list          [ ims-central magenta-ims-dnn sos-pool-ipv6 ]
 capacity          10
 priority          1
exit

profile dnn dnnprof-ims-1//dnn profile, where ip pool and upf is selected based on
location
dnn ims-lag1 network-function-list [ upf ]
dnn rmgr ims-lag1 fallback ims-central
timeout up-idle 3600 cp-idle 7320
.
.
.
session skip-ind false
upf apn ims-lag1
qos-profile 5qi-to-dscp-mapping-table-IMS
.
.
.

profile dnn dnnprof-ims-2//dnn profile, where ip pool and upf is selected based on
location
dns primary ipv4 209.165.200.225
dns primary ipv6 fd00:976a::9
dns secondary ipv4 209.165.200.226
dns secondary ipv6 fd00:976a::10
dnn ims-lag1 network-function-list [ upf ]
dnn rmgr ims-lag1 fallback ims-central
timeout up-idle 3600 cp-idle 7320
.
.
.
profile dnn dnnprof-ims//dnn profile, where ip pool and upf selected based on location
fails but falls back based on dnn based on precedence
dns primary ipv4 209.165.200.227
dns primary ipv6 fd00:976a::9
dns secondary ipv4 209.165.200.228
dns secondary ipv6 fd00:976a::10
dnn ims-central network-function-list [upf ]
dnn rmgr ims-central
timeout up-idle 3600 cp-idle 7320
.
.
.


config
 ipam
  instance 1
   source local
   address-pool ims-ipv6-pool1
   address-quarantine-timer 3600
    vrf-name                 n6
    tags
     dnn ims-lag1//ip pool for upf-group1 and dnn profile dnnprof-ims-1
    exit
    ipv4
    address-range 1.1.1.0 1.1.10.254
    exit
    ipv6
    prefix-ranges
     split-size
      per-cache 65536
      per-dp    65536
     exit
```

```
 exit
exit
address-pool ims-ipv6-pool2
address-quarantine-timer 3600
 vrf-name                 n6
 tags
  dnn ims-lag2//ip pool for upf-group2 and dnn profile dnnprof-ims-2
 exit
 ipv4
 address-range 2.1.1.0 2.1.10.254
 exit
ipv6
 prefix-ranges
 split-size
 per-cache 65536
 per-dp    65536
exit
 prefix-range 2607:fc20:8aa0:: length 44
exit
exit
address-pool ims-ipv6-pool3
address-quarantine-timer 3600
 vrf-name                 n6
 tags
 dnn ims-central//ip pool for upf-group3 and dnn profile dnnprof-ims
 exit
ipv4
address-range 3.1.1.0 3.1.10.254
exit
ipv6
prefix-ranges
 split-size
 per-cache 65536
 per-dp    65536
exit
prefix-range 3607:fc20:8aa0:: length 44
exit
exit
exit
```

# SMF と UPF の間での IP チャンクの調整

## 機能説明

予期しないシナリオでは、SMF と UPF で割り当てられた DP チャンクのリスト間で不一致が発生する可能性があります。これにより、ネットワーク内で重複した IP が割り当てられる可能性があります。

SMF は、IP 割り当ての重複を回避できる IP チャンクの調整をサポートしています。

## 機能の仕組み

UPF への新しい DP チャンク割り当ての一部として、次のメカニズムに従う必要があります。

1. 空き DP チャンクを UPF に割り当てます。

2. ノード マネージャから CDL へのサブスクライバをクリアして、次の条件に一致するサブスクライバ セッションを解放します。
   - 新しく割り当てられた DP チャンク（セッションを解放するための一意でないキーとしての ipv4-startrange / ipv6-startrange）。
   - 現在のシステム時刻より前に作成されたセッション。
3. 新しいチャンク割り当ての一部として選択された UPF を除き、特定の DNN を提供する他のすべての UPF へのルート削除要求で N4 関連付けの更新をトリガーします。

（注） これらのステップはすべて、並行してトリガーされる必要があります。

4. **clear subscriber** トリガー中に、新しい相関 ID を CorrelationIdDpchunkAuditLocal（0xFF0D）として使用します。これは、セッションの削除中にメトリックの一部として使用する必要があります。
5. DNNは、リソース マネージャDNN/着信DNNです。

（注） 日曜日のシナリオでは、ノード マネージャから CDL への **clear subscriber** は、CDL 内のどのセッションとも一致しないはずです。また、ルート削除要求による N4 関連付けの更新は、このチャンクまたはルートを使用していないため、UPF に影響を与えることはありません。

# IP チャンクの調整を有効または無効にするための構成

SMF と UPF の間の IP チャンクの調整機能を有効または無効にするには、次の構成を使用します。

```
config
   ipam
      instance gr_instance_id
         audit chunk [ local | none ]
           end
```

注：

- **audit chunk** *[ local | none ]* ：IPAM で監査アクティビティを構成します。 **audit chunk** には、次の 2 つの可能な値があります：
  - *local*： 機能を有効にします。
  - *none* ：機能を無効にします。

  デフォルト値は、*none*です。

## 設定例

次に設定例を示します。

```
[smf] smf(config)# ipam instance 1 audit chunk
Possible completions:
  local   Enable local audit
  none    Disable audit
[smf] smf(config)# ipam instance 1 audit chunk local
```

# OAM サポート

この機能では、次のメトリクスと統計がサポートされます：

## バルク統計

既存のバルク統計情報 **smf_disconnect_stats** の理由に次のラベルが追加されました。

- **dp_chunk_audit_local**：IPAM ローカル監査によりセッションが切断されました。

# IP チャンク スロットリング

## 機能説明

**表 *321 :* 機能の履歴**

| 機能名 | リリース | 機能説明 |
|---|---|---|
| IPAMパフォーマンスと拡張性を最適化 | 2024.03.0 | IP チャンク割り当てスロットル機能は、サポートされている最大 UPF セッションに基づいてスロットリング チェックをトリガします。ただし、最大 UPF セッションが構成されていない場合でもスロットリング チェックが発生し、不要な処理オーバーヘッドが発生します。<br>これに対処するため、SMF には GR-Instance レベルで、IP チャンク スロットリングを明示的に無効にする新しいコマンド **chunk-throttling false** が導入されています。 |

SMF は、IP プールの使用率を最適化し、複数の UPF での IP アドレスチャンクの割り当てを管理するための IP チャンク スロットリング機能をサポートしています。この機能は、UPF によってアドバタイズされる UPF キャパシティ、または SMF でのローカル構成に基づいて新しい IP チャンクの割り当てを調整することにより、負荷を分散するのに役立ちます。スロットリングがトリガされると、新しいチャンクは割り当てられませんが、既存のチャンクがなくなるまで使用され続けます。

UPF キャパシティを決定するために、SMF は次の構成を評価します。

- ネットワーク要素（UPF）レベルで構成された **max-upf-sessions** コマンド。
- vDNN レベルで構成された **max-upf-sessions** コマンド（UPF レベルごとにも適用可能）。
- UPF のユーザー プレーン サービス レベルで構成された **load-control capacity** コマンド。

3 つの設定がすべて存在する場合、SMF は値を比較し、UPF の IP チャンク割り当てを制御するために最小の構成を選択します。ただし、SMF は、UPF セッションの最大数が UPF で構成されていない場合でもスロットリング チェックを開始するため、不要な処理オーバーヘッドが発生します。

意図しないスロットリング チェックを軽減するために、SMF では IP チャンク スロットリングを明示的に無効にする新しい構成コマンド **chunk-throttling false** を GR-Instance レベルで導入しました。

# 機能の仕組み

この IP チャンク スロットリング プロセスには次の手順が含まれます。

1. SMF は、UPF の最大セッション容量を伝送する UPF からの PFCP アソシエーション設定要求で、新しい独自の IE をサポートします。

   UPF 側からのこの IE のサポートの詳細については、『*UCC 5G UPF 構成および管理ガイド、リリース 2023.03*』を参照してください。

2. SMF の UPF ごとの最大セッション キャパシティを構成します。この構成は、UPF 構成ごと、または UPF ごと、DNN ごとに適用できます。
3. PFCP アソシエーションの一部として、SMF はノードマネージャごとに IP チャンクを UPF に割り当てます。
4. UPF ごとの IP 使用率が、割り当てられた合計 IP の 80% に達すると、SMF は追加のチャンクの割り当てを試みます。プール構成の変更やプールのしきい値のヒットなどの内部変更に基づいて追加の割り当てを行うこともできます。
5. SMF は、UPF の IP 使用率（アクティブ セッションと検疫内の IP による現在の IP 使用率を含む）を UPF の最大セッション キャパシティと比較します。
6. 現在の使用量が最大セッション キャパシティを超える場合、SMF はチャンクの割り当てをスロットリングします。

## 制限事項

この機能には次の既知の制限事項があります。

- 最初のチャンクが UPF 関連付けの各ノード マネージャ インスタンスに割り当てられている場合、スロットリングは適用されません。
- 分割サイズ構成は、SMF/UPF で構成されたセッション制限よりも小さくする必要があります。理想的には、最初のチャンクがネイティブ ノードマネージャインスタンスとリモート nodemgr インスタンス（GR 展開用）の両方に割り当てられることを考慮すると、半分未満にする必要があります。
- セッション制限がより低い値で構成されている場合、適用される実際の最小値は、チャンク サイズ（キャッシュ スプリットおよび dp スプリット）の構成と関連します。

# SMF での UPF の最大サポート セッションの構成

次の CLI は、UPF ごとにサポートされる最大セッションを構成します。

```
config
  profile network-element upf upf_profile_name
     max-upf-sessions max_upf_sessions_count
    n4-peer-address {  ipv4-address ipv4_address | ipv6-address ipv6_address
}
     n4-peer-port  port_number
     dnn-list dnn_list_value
     capacity lb_capacity
     priority lb_priority
     end
```

注：

**max-upf-sessions** *max_upf_sessions_count*：特定の UPF でサポートされる最大セッション数。

## 設定例

次に、UPF でサポートされる最大セッション数を定義するための構成例を示します。

```
profile network-element upf upf1
 max-upf-sessions 2000
 n4-peer-address ipv4 10.1.8.48
 n4-peer-port 8805
 dnn-list    [ intershat intershat1 intershat2 intershat3 intershat4 intershat5 intershat6
 intershat7 intershat_hrt intershatipex spectrum ]
 capacity     65535
 priority     65535
exit
```

# UPF ごとの vDNN ごとにサポートされる最大セッション数の構成

SMF は、UPF ごとに vDNN ごとに最大セッションの構成をサポートします。最初の DNN プロファイルの選択は、UEDNN に基づいて行われます。SMF は、最初の DNN プロファイルでの

DNN RMGR 構成に基づいて vDNN を選択します。この vDNN には追加の DNN プロファイルを構成でき、この vDNN ベースの DNN プロファイルの下で CLI **max-upf-sessions** を構成できます。

（注）
- **max-upf-sessions** は、ユース ケースに基づいて、初期 DNN プロファイルでも構成できます。
- DNN RMGR は **max-upf-sessions** 、を構成できる DNN プロファイルとして構成する必要があります。

```
config
  profile dnn dnn_profile_name
    network-element-profiles { amf | chf | pcf | sepp | udm } profile_name
 | ipv6 ipv6_address }
     dnn  ims network-function-list [ chf | pcf | udm | upf ]
     timeout  up-idle up_idle_duration cp-idle cp_idle_duration
     charging-profile  charging_profile_name
     pcscf-profile  profile_name
     ppd-profile  profile_name
     ssc-mode  [ 1 | 2 | 3 ] allowed [ 1 | 2 | 3 ]
     session type  default_session_type
     max-upf-sessions max_upf_sessions_count
     end
```

## 設定例

次に、SMF で UPF ごとに vDNN あたりのサポートされる最大セッション数を定義するための構成例を示します。

```
profile dnn dnnprof-ims
 dns primary ipv4 10.177.0.34
 dns primary ipv6 fd00:976a::9
 dns secondary ipv4 10.177.0.210
 dns secondary ipv6 fd00:976a::10
 dnn rmgr ims-pool-ipv6
 wps-profile dynamic-wps
 upf apn ims
exit

profile dnn dnnprof-ims.epdg.prod
 dns primary ipv4 10.177.0.35
 dns primary ipv6 fd00:976a::8
 dns secondary ipv4 10.177.0.211
 dns secondary ipv6 fd00:976a::11
 dnn rmgr ims-pool-ipv6
 upf apn ims.epdg.prod
exit

profile dnn ims-pool-ipv6
 network-element-profiles chf nfprf-chf1
 network-element-profiles amf nfprf-amf1
 network-element-profiles pcf nfprf-pcf1
 network-element-profiles udm nfprf-udm1
 dnn ims network-function-list [ chf pcf udm upf ]
```

```
 timeout up-idle 3600 cp-idle 7320
 charging-profile           chgprof-1
 pcscf-profile              pcscf1
 ppd-profile                ppd-prof1
 ssc-mode 1 allowed [ 2 ]
 session type IPV6
 max-upf-sessions 10000
exit
```

# IP チャンク スロットリングの無効化

この手順を使用して、IP チャンク割り当てスロットリングを無効にします。

**手順**

**ステップ 1** IPAM 構成モードを開始します。

**例**：

```
[smf] smf# config
[smf] smf(config)# ipam
```

**ステップ 2** GR インスタンス番号を指定します。*instance_id* の有効な範囲は 1 ～ 8 です。

**instance** *instance_id*

**例**：

```
[smf] smf(config-ipam)# instance 1
```

**ステップ 3** 値を false に設定して、IP チャンク割り当てスロットリングを無効にします。デフォルト値は true です。

**chunk-throttling { false | true }**

**例**：

```
[smf] smf(config-instance-instance_id)# chunk-throttling false
```

**ステップ 4** 構成を保存してコミットします。

**例**：

```
[smf] smf(config-instance-instance_id)# end
```

このコマンドを使用すると、構成をコミットまたは無視することができます。**[はい（Yes）]** と入力すると、構成を保存または変更できます。

# OAM サポート

このセクションでは、この機能でサポートされているメトリックについて説明します。

# メトリック

新しいチャンクの割り当てがスロットルされた場合のイベントをキャプチャするために、次の新しいメトリックが導入されました。

**メトリック名**： IPAM_DP_chunk_allocation_throttled

**説明**： このメトリックは、特定のアドレスタイプと DNN の UPF に対して新しいチャンク割り当て要求がスロットリングされたときにイベントをキャプチャします。新しいチャンク割り当て要求は、通常、特定のアドレスタイプと DNN の上限しきい値（80%）に達した後、すべてのアドレス割り当て要求でトリガーされます。

このメトリックには、次のラベルが追加されます：

- **grInstId**： GR インスタンス ID
- **upf**： UPF キー
- **addressType**：アドレス タイプ（IPv4/IPv6）
- **dnn**： DNN タグ名
- **chunkAllocTrigger**： 新しいチャンクの割り当てをトリガーする
  - **Threshold_Hit_Addr_Alloc**：新しいアドレスの割り当て後にしきい値がヒットします。
  - **Threshold_Hit_DP_Monitoring**：その UPF のプールモニタリング後のしきい値ヒット。
  - **Insufficient_Addr_Space**：IP 割り当て中に十分なアドレスを使用できない場合。

# IPAM キャッシュ データ シャーディング

表 *322 :* 機能の履歴

| 機能名 | リリース | 機能説明 |
|---|---|---|
| IPAMパフォーマンスと拡張性を最適化 | 2024.03.0 | SMF は、処理およびストレージのキャパシティのボトルネックを克服するために、適切な数のシャードで IPAM データ シャーディングを構成することを可能にします。<br><br>データシャーディングにより、IPAMのパフォーマンスとスケーラビリティが向上し、高い TPS と多数の IP プール、プールタグ、UPF のサポートが可能になります。<br><br>導入されたコマンド：**data-sharding num-shards** *ipam_data_shards* |

ネットワーク展開でのDNN、IPプール、およびUPFの需要が高まっているため、IPAMキャッシュのデータ サイズが大幅に増加します。現在の IPAM システムは、IP アドレスの割り当て中にシングル キャッシュ コンテキスト構造で動作するため、1秒あたりの高いトランザクション数（TPS）と大規模な展開という課題に直面しています。応答時間とバックプレッシャが長くなります。IPAM キャッシュデータのシャーディングでは、IP 割り当て要求とリリース要求の並列処理を可能にすることで、これらの問題に対処します。

シャーディングは、IPAMキャッシュ データを複数の部分（シャード）にフラグメント化するプロセスです。シャード キーとは、UPF ID、プールタグ文字列、またはプール名の組み合わせです。各シャードは独立して動作し、独自のキャッシュ コンテキスト フラグメントを制御します。シャーディングは、GR インスタンスレベルでCLI コマンド**data-sharding** を使用して有効または無効にすることができます。シャードの数は構成可能であり、展開される IP プール、UPF、およびアドレス タイプの数に基づいて拡張性を確保できます。

データ シャーディングは

- IPAM 操作でより高い TPS をサポートするためのパフォーマンスのスケーリングをサポートします。
- 大きなキャッシュ データをより効率的に管理できます。

# データ シャーディングの制限事項

IPAM キャッシュ データ シャーディングを実装する場合は、これらの制限を考慮してください。

- シャーディングを有効または無効にする際に、既存の IPAM キャッシュ データの移行はサポートされません。
- シャーディング構成を変更するには、SMF を新規に起動する必要があります。

# IPAMデータ シャーディングの有効化

この手順を使用して、IPAM キャッシュ データのシャーディングを有効にします。

**手順**

**ステップ 1** IPAM 構成モードを開始します。

**例**：

```
[smf] smf# config
[smf] smf(config)# ipam
```

**ステップ 2** GR インスタンス番号を指定します。*instance_id* の有効な範囲は 1 ～ 8 です。

**instance** *instance_id*

**例**：

```
[smf] smf(config-ipam)# instance 1
```

**ステップ 3** IPAM キャッシュ データ シャーディングを有効にし、シャードの数を指定します。 *shards_number* の値は、2 ～ 16 の整数である必要があります。データ シャーディングを無効にするには、 **no data-sharding** コマンドを使用します。

デフォルトでは、テレメトリ データは無効になっています。

**data-sharding num-shards** *chassis_number*

**例**：

```
[smf] smf(config-instance-instance_id)#data-sharding num-shards 4
```

**重要**
PC を再起動して構成を有効にします。

**ステップ 4** 構成を保存してコミットします。

**例**：

```
[smf] smf(config-instance-instance_id)# end
```

このコマンドを使用すると、構成をコミットまたは無視することができます。**[はい（Yes）]** と入力すると、構成を保存または変更できます。

# IP の割り当てと再利用

IP 割り当ての最初の手順では、UE が PDU セッション確立要求をネットワークに送信して IP アドレスを取得する必要があります。SMF は、UE からこの IP 割り当て要求を受信します。その後、ネットワークは必要なリソースを他のネットワーク コンポーネントに割り当て、割り当てられた IP アドレスを PDU セッション確立承認メッセージを介して UE に伝達します。

ネットワークから切断された後に同じ IP アドレスを保持するために、SMF には、IP の再利用のホールドタイマー機能を有効にする設定オプションが用意されています。ホールドタイマー期間は、統合コア プロファイル レベルまたは DNN レベルのいずれかで設定できます。

**session hold-duration** CLI コマンドが構成され、アクティブ サブスクライバが切断されると、IP アドレスは保持され、まだ使用中であると見なされます。この IP アドレスは、セッション ホールド タイマーの期限が切れるまで、空き状態に戻りません。

この機能により、指定された期間内に再接続したサブスクライバは IP プールの同じ IP アドレスを保持でき、IP アドレスの最適な再利用が保証されます。

**表 *323* : 機能の履歴**

| 機能名 | リリース | 機能説明 |
|---|---|---|
| UE IP アドレスの保持と再利用のサポート | 2024.03.1 | この機能により、セッション解放後、設定可能なセッション ホールド タイマー内にユーザーが再接続した場合に、SMF がユーザーセッションに同じ IP アドレスとセッション ID を割り当てることができます。<br>この機能により、ユーザー エクスペリエンスが向上し、ユーザーが頻繁に接続と切断を行うシナリオで IP アドレスを枯渇させることが減少します。<br>**新しいコマンド**：統合コア プロファイルおよび DNN プロファイル構成の **session-hold duration** |

# UE IP アドレスの保持および再利用の利点

このセクションでは、この機能を使用してユーザーが体験できる肯定的な結果を示します。

- **最適化された IP アドレス管理**：この機能により、IP アドレスの効率的な再利用を可能にします。これは、持続可能なスケーラブルなネットワーク インフラストラクチャを維持するために重要です。
- **セッション継続性の改善**：ホールドタイマー機能により、ネットワークの中断またはアップグレード後、指定された期間内にユーザーセッションを再接続できるようになり、シームレスなユーザー エクスペリエンスが提供されます。
- **包括的なカバレッジ**: この機能は、ユーザー セッションのリリース、ホールド タイマーの期限切れ内およびホールドタイマーの期限切れ後の再アタッチ、さまざまな障害シナリオなど、幅広いシナリオを処理するように設計されています。この包括的なカバレッジにより、ネットワークがさまざまな状況に対応できるようになり、さまざまな運用ニーズに適応できる汎用ソリューションが提供されます。

# ローリング アップグレードおよびダウングレード中の IP 再利用に関する注意事項

ローリングアップグレードの手順を実行する際、これらの重要な注意事項を必ず確認してください。

- ローリング アップグレードが完了した後にのみ、 **session-hold** CLI を有効にします。
- **clear subscriber session-state hold** コマンドを使用して、保留状態になっているユーザー セッションをクリアします。

ローリング ダウングレードを開始する前に、次の点を確認します。

- IP 再利用機能を無効にする
- IP 再利用状態にあるユーザー セッションのクリア

# UE IP アドレスの保持と再利用に関する制限事項

再接続シナリオ中に同じ IP アドレスを要求する場合は、次の潜在的な制限に注意してください。

- ID のみの再利用はサポートされていないため、ID と IP アドレスの両方を再利用する必要があります。
- この機能は、静的 IP 割り当ておよび DHCP IP 割り当ての間の遷移も、ダイナミック IP 割り当てと静的 IP 割り当ての間の移行もサポートしていません。このような場合、SMF は古い IP を解放し、新しい IP を割り当てます。

- コンバージド コア セッションの場合、cnSGWc は最初に UPF を選択し、cnPGW は同じ UPF の再利用を試みます。再接続中に UPF コンバージェンスを維持するには、cnSGW は前のセッションで使用されたのと同じ UPF を提供する必要があります。cnSGW が同じ UPF を提供しない場合、UPF セッションのコンバージェンスを維持できません。
- 前のコールが収束できなかった場合、新しいコールの IP の再利用は発生しません。これは、新しいコンバージド コールの cnSGW に選択された UPF にプライオリティが渡されます。
- 緊急通報中に未認証の IMSI と認証済みの IMSI の間で移行（またはその逆）が発生した場合、IP と ID は再利用されません。
- IPアドレスは、次の場合に再利用されません
  - ハーフ作成を介した作成の開始
  - 4G 専用 UE が Wi-Fi 接続を 4G 経由で実行、またはその逆
  - 4G 専用 UE が 5G 対応 UE として再接続
- この機能は、以前のセッションと現在のセッションの間で、PDN タイプ、スライス、DNN、UPF、または vDNN の不一致の場合は機能しません。

# 保留状態時の接続または PDU セットアップの失敗の処理

保留状態にある間に接続または PDU セットアップ処理が失敗した場合、SMF は表に示す特定のアクションを実行します。

| 接続または PDU のセットアップの処理中に期限切れになったホールド タイマー | N10 または N7 作成処理で発生する接続エラー | N7 更新、N40、N11、または N4 処理で接続エラーが発生する | 操作 |
|---|---|---|---|
| 非対応 | はい | N/A | • ホールド タイマーを停止しないでください<br>• 保留状態のままになる |
| × | N/A | はい (IP は再利用されません) | • IP をリリース<br>• ピア NF に削除/リリースを送信する<br>• CDL からセッションを削除しました |

| 接続または PDU のセットアップの処理中に期限切れになったホールドタイマー | N10 または N7 作成処理で発生する接続エラー | N7 更新、N40、N11、または N4 処理で接続エラーが発生する | 操作 |
|---|---|---|---|
| × | N/A | はい（IP が再利用されます） | • ホールドタイマーを停止しないでください<br>• 保留状態のままになる |
| はい | はい | N/A | • IP をリリース<br>• ピア NF に削除/リリースを送信する<br>• CDL からセッションを削除しました |
| ○ | N/A | はい | |

# IP 再利用の基準

次のシナリオは、保留状態のセッションの IP の再利用を防ぎます。

1. pdnType の不整合
2. スライス内の不一致
3. dnn と Vdnn のバリエーション
4. SGW から発信される UPF 不一致
5. UPF の不一致
6. UPF の停止
7. ロケーションベースの UPF 選択のアクティブ化

これらの条件は、作成要求の最初の処理中に、および再利用が失敗した場合に検証されます（シナリオ 4 を除く）。再利用が失敗すると、IP の解放がリソース マネージャ（R-MGR）に対してトリガされ、IP 割り当て後に UPF が割り当てられます。

以前の PDU セットアップまたは接続の UPF アドレスが優先 UPF として使用されるため、将来のコールで同じ UPF が選択される可能性が高くなります。

SGW との UPF の不一致（シナリオ 4）は、SGW がこの機能をサポートしていない場合、またはコールが新しい SGW から発信されている場合に発生する可能性があります。これは、リリース前にセッションが NR または Wi-Fi にあった場合にも発生する可能性があります。

新しいコンバージド コールの場合は、cnSGW によって選択された UPF が優先されます。したがって、前のコールが収束できなかった場合、IP の再利用は発生しません。ただし、前のコー

ルも集約されており、cnSGWc がこの機能をサポートしている場合、このシナリオは発生しない可能性があります。新しいコールが収束しなかった場合、IP アドレス、ID、UPF が再利用されます。

# SMF が UE IP アドレスの再利用を許可する仕組み

SMF は、統合コア プロファイルまたは DNN プロファイルでホールド タイマー機能が有効になっているかどうか、およびホールド タイマー値が有効かどうかを確認します。SMF はこれらの条件に基づいて適切なアクションを実行します。

**表 *324 : IP* 再利用のシナリオ**

| Condition 1 | Condition 2 | 操作 |
|---|---|---|
| 同じ PDU セッション ID と同じ SMF インスタンスでユーザー セッションが存在する場合 | ホールド タイマーの期限切れ前にユーザーが再接続し、再利用の条件が一致する場合 | SMF では、セッションに対し同じ IP と ID が再利用されます。 |
| | ユーザーがホールド タイマーの期限内に再接続しなかった場合 | SMF は IP と ID を解放し、セッションまたは PDU コンテキストの詳細を削除します。 |
| | 再利用条件が一致しない場合 | SMF はセッションに新しい IP および ID を割り当て、古い IP および ID を解放します。 |
| 同じ PDU セッション ID と同じ SMF インスタンスのセッションが存在しない場合 | | SMF がセッションに新しい IP と ID を割り当てます。 |

SMF はセッションを保留状態に移行し、IP および ID の再利用データを保持します。

# UE IP アドレスの保持と再利用の前提条件

SMF では、これらの条件が満たされている場合にのみ、IP アドレスを再利用できます。

- ユーザー セッションは、再接続のシナリオと同じ PDU セッション ID である必要があります。この機能は、IP および ID 割り当ての詳細へのユーザー セッションのマッピングに依存しています。
- IMSI と EBI は、再接続シナリオ中に 4G セッションと一致する必要があります。
- ユーザー セッションに対して同じ UPF を選択する必要があります。UPF の選択がロケーションに基づいているか、cnSGW によって決定されている場合、この機能は意図したとおりに機能しない可能性があります。

# IP再利用機能の有効化

統合コア プロファイル、DNNプロファイル、または両方のプロファイルでホールドタイマー期間を設定することで、IP 再利用機能を有効にできます。

### 手順

このセクションの手順に従ってください。

- コンバージド コアでのホールド タイマーの構成
- DNN でのホールド タイマーの構成

## コンバージド コアでのセッション ホールド タイマーの構成

統合コア プロファイル レベルでセッション ホールド タイマーを設定するには、次の手順を使用します。

### 始める前に

- このドキュメントの注意事項と制限事項セクションを確認します。
- SMF Ops Center に接続して構成を実行していることを確認します。

### 手順

**ステップ 1** コンバージドコア プロファイル構成モードを開始します。

**profile converged-core** *ccg_profile_name*

例：

```
[smf] smf# config
[smf] smf(config)# profile converged-core ccg1
```

**ステップ 2** 再利用のためにユーザーの IP アドレスを保持する期間を秒単位で指定します。ホールド タイマーの有効な値の範囲は 30 ～ 300 秒です。

**session-hold duration** *hold_timer*

例：

```
[smf] smf(config-converged-core-ccg1)# session-hold duration 120
```

セッション ホールド タイマーが統合コア プロファイルと DNN プロファイルの両方で構成されている場合、DNN で構成されたタイマー値により、統合コア プロファイルのタイマーの値が上書きされます。

（注）

SMF は、進行中のセッションのセッション ホールド タイマーの構成のダイナミックな変更をサポートしていません。タイマー値の変更は、新しいセッションにのみ適用されます。

**no session-hold** コマンドを使用して、ホールド タイマー機能を無効にします。

**ステップ 3** 構成を保存してコミットします。

**例**：

```
[smf] smf(config-converged-core-ccg1)# end
```

このコマンドを使用すると、構成をコミットまたは無視することができます。**[はい（Yes）]** と入力すると、構成を保存または変更できます。

## DNN でのセッション ホールド タイマーの構成

このタスクを使用して、DNN レベルでセッション保留タイマー期間を設定します。

### 始める前に

- このドキュメントの注意事項と制限事項セクションを確認します。
- SMF Ops Center に接続して構成を実行していることを確認します。

### 手順

**ステップ 1** DNN プロファイル構成モードを開始します。

**profile converged-core** *dnn_profile_name*

**例**：

```
[smf] smf# config
[smf] smf(config)# profile dnn dnn_test
```

**ステップ 2** 再利用のためにユーザーの IP アドレスを保持する期間を秒単位で指定します。ホールド タイマーの有効な値の範囲は 30 ～ 300 秒です。

**session-hold duration** *hold_timer*

**例**：

```
[smf] smf(config-dnn-dnn_test)# session-hold duration 140
```

セッション ホールド タイマーが統合コア プロファイルと DNN プロファイルの両方で構成されている場合、DNN で構成されたタイマー値により、統合コア プロファイルの値が上書きされます。SMF は、セッションの解放後 140 秒間 UE IP アドレスを保持します。

（注）
SMF は、進行中のセッションのセッション ホールド タイマーの構成のダイナミックな変更をサポートしていません。タイマー値の変更は、新しいセッションにのみ適用されます。

**no session-hold** コマンドを使用して、ホールド タイマー機能を無効にします。

**ステップ 3** 構成を保存してコミットします。

例：

```
[smf] smf(config-dnn-dnn_test)# end
```

このコマンドを使用すると、構成をコミットまたは無視することができます。**[はい（Yes）]** と入力すると、構成を保存または変更できます。

# IP 再利用機能のトラブルシューティング情報

このセクションでは、問題のトラブルシューティングに使用できる show コマンド、clear コマンド、およびバルク統計情報の出力を提供します。

## コマンドの表示

ユーザー セッションの状態を表示するには、 **show subscriber** コマンドを使用します。

```
[smf] smf# show subscriber supi imsi-123456789012345 nf-service smf full
subscriber-details
{
"subResponses": [
{
"status": true,
"genericInfo": {
"pduState": "pduState_hold",
"pduSesstype": "UnknownPduSessionType",
"alwaysOn": "None",
"dcnr": "None",
"wps": "Non-Wps Session",
"ueType": "NR Capable UE",
"authStatus": "Unauthenticated",
"ipAllocationBy": "Dynamic",
"anType": "3GPP_ACCESS",
"holdTime": "2024-08-19T18:50:53Z"
},
"policySubData": {
"supportedFeatureList": {}
},
"upfServData": {},
"access4GSubData": {}
}
]
}
```

アクティブ状態のユーザー セッションの数を確認するには、次のコマンドを使用します：

- **show subscriber count nf-service smf all**
- **cdl show sessions count summary slice-name 1 filter { condition not match key "1#/#sessState:Hold" }**

保留状態のユーザー セッションの数を確認するには、次のコマンドを使用します：

- **show subscriber count nf-service smf session-state hold**

- **cdl show sessions count summary slice-name 1 filter { condition match key "1#/#sessState:Hold" }**

（注） show コマンドは、この機能が有効になっている場合にのみ、アクティブ セッションとホールド セッションの数を表示します。

## clear コマンド

デフォルトでは、IP プールのオフライン、プールの削除、GTP-U または GTP-C パスの障害発生時などのすべてのコールクリアリングまたはリリースアクション中に、サブスクライバセッションが保留状態に移行します。これらのシナリオでは、保留状態のセッションをクリアするために、 **clear subscriber** コマンド（ **clear subscriber upf | upf-list**コマンドを使用）を使用します。

サブスクライバセッションは、IP チャンクの再利用またはパスの障害、再アソシエーション、再起動/回復のケースなどの UPF 関連のリリース中に、保留状態に移行することなく、完全にクリーンアップされます。このような場合、新しい CLI キーワード **no-session-hold** と既存の **clear subscriber** コマンド オプションを使用して、セッションを完全にクリアします。

## バルク統計情報出力

この機能では、次の新しいバルク統計が紹介されています：

- **smf_disconnect_session_hold_stats**：この統計は、ホールドタイマーの期限切れによる保留状態のコールのクリーンアップと、管理者が保留状態のセッションをクリアするために導入されています。
- **smf_ip_reuse_stats**：この統計情報は、IP 再利用数を決定するために導入されています。次のラベルが含まれます：
  - reason
  - rat_type

この機能により、バルク統計情報に次の更新が導入されました。

- **db_records_total**：この統計には、CDL レコードが保留状態かどうかを識別する新しいラベル「session-hold」が含まれています。
- **smf_disconnect_stats**：この統計情報には、セッションが保留状態に移行したかどうかを示す新しいラベル「hold=true/false」が含まれています。
- **smf_service_stats**：この統計情報には、IP 再利用機能が有効かどうかを示す新しいラベル「ipreuse=true/false」が含まれています。

# スイッチ制限を処理するためのルート集約

## 機能説明

SMF が UPF に割り当てるすべての IP チャンクについて、UPF はデータ ネットワークに IP アドレス サブネットをアドバタイズするためのルート レコードをアップストリーム ルータに公開します。ただし、一部のルータでは許可できるルート レコード数に制限があります。

SMF が UPF に割り当てることができる IP チャンクの数を制限し、より大きなチャンク（32K / 16K）を使用するように強制されます。ただし、より大きな IP チャンクを使用すると、割り当てられた IP チャンクが十分に活用されないため、それらのチャンクはネイティブ インスタンスでは使用できません。

SMF では、より小さいチャンク サイズを定義できるため、ルート レコードの最適化を使用して、公開されるルート レコードの数を制限できます。

## 機能の仕組み

チャンク サイズの定義とルート集約は、連続する IP チャンクを UPF に割り当て、連続するチャンクのサブネットに従って単一または集約されたルート レコードを公開することによって行われます。この機能は、次のプロセスで機能します：

- 連続的な方法での 4K などのより小さいチャンク サイズは定義されます。
- 割り当て中、IPAM は完全なグループを UPF に割り当て、チャンク グループの範囲に従って、単一のルートレコードが UPF に送信されます。
- チャンク グループ内には 2、4、または 8 つのチャンクがあります。このように、1 つのグループは 8K、16K、または 32K のサイズで構成され、それに応じてそのサイズのルート レコードが UPF に送信されます。
- ノード マネージャ インスタンスは、より小さい IP チャンクでのみ動作します。
- 最初の UPF 登録時に、リモート ノード マネージャのチャンクも同じグループから割り当てられます。
- チャンクの解放が開始されると、グループ内のすべてのチャンクが解放されたときにのみ、チャンクはフリー プールに戻ります。
- UPF に送信されるルートをさらに最適化するには、 **reserve-contiguous-groups** オプションを有効にすることもできます。この SMF を使用すると、（UPF/vDNN 用に構成された **max-session-size** に従って）複数の連続するチャンク グループが UPF に予約され、1 つのルート レコードのみが UPF にプッシュされます。オプション **reserve-contiguous-groups** の構成は、完全なアドレス プールの構成とともに有効にする必要があります。有効になっている場合、無効にするオプションはサポートされていません。ユーザーがプールの動作を変更したい場合は、プールに関連付けられているサブスクライバをクリアし、アドレス プールの構成を削除して、 オプションを使用せずに再設定する必要があります。

- チャンク グループがアドレス プールに対して有効になる場合は、cache-split と dp-split の値を同じにする必要があります。dp-split と cache-split の値が異なる場合、ノード マネージャはより多くのチャンクをプルします。

## チャンク グループのない古いプールからチャンク グループのあるプールへの移行

IP プールの移行は、次のプロセスで実行されます：

1. 同じ vDNN の chunkGroupSize 構成を持つ新しいプールを追加します（IP 範囲はシステム内のプール全体で一意であり、新しいプールのアドレス範囲のサブネットは標準の IP サブネットに準拠している必要があります）。ここで、 **reserve-contiguous-groups** は、使用または計画に基づいて有効または無効にすることができます。
2. **show ipam pool の** 出力から新しいプールが表示されているかどうかを確認します。

   構成例：

   ```
   [smf-m6-cndp-rack2/data] smf# show ipam pool Mon Jul 24 08:34:36.617 UTC+00:00
   ================================================================================================
   PoolName Ipv4Utilization Ipv6AddrUtilization Ipv6PrefixUtilization
   ================================================================================================
   data-ipv6-pool2 92.23% 0.00% 97.66%
   data-ipv6-pool1 59.42% 0.00% 34.40%
   data-ipv6-pool4 0.00% 0.00% 0.00%
   data-ipv6-pool3 1.70% 0.00% 1.10%
   ================================================================================================
   [smf-m6-cndp-rack2/data] smf#
   ```

3. 新しく追加されたプールが **show ipam pool の** 出力に表示されている場合は、新しいプールがアクティブであり、グループごとのチャンクの構成に従って、チャンク グループごとの割り当てを行います。これは、**show ipam pool <newly added pool> ipv4-addr/ ipv6-prefix** コマンドを使用して実行できます。

   構成例：

   ```
   show ipam pool data-ipv6-pool4 ipv4-addr/ ipv6-prefix
   ```

4. チャンク グループのない古いプールをオフラインとしてマークします。古いプールから新しい IP をさらに割り当てることはできません。
5. 進行中のトラフィックについては、新しいプールのチャンクがチャンク グループの構成に従って割り当てられます。これは、同じ CLI を使用して確認できます。

   **show ipam dp <DP association> show ipam pool <new pool> ipv4-addr/ ipv6-prefix**
6. 古いプールの IP に関連付けられたセッションが終了すると、古いプールから IP が解放され、さらにそのチャンクが解放されます。
7. 古いプールからすべてのチャンクが解放されるまで待ちます。

（注） 古いプールでさらに IP がスタックしたり古い場合は、admin-clear CLI を使用してサブスクライバをクリアできます。例： **show subscriber count nf-service smf dnn** <dnn> **show subscriber count nf-service smf ipv4-pool/ ipv6-pool**<old pool> 、および **clear subscriber nf-service smf ipv4-pool/ ipv6-pool**。この CLI ですべてのサブスクライバが古いプールからクリアされるのを待ち、UPF への対応する古いルートも削除される必要があります。

8. すべてのサブスクライバがチャンク グループで新しいプールに戻されているかどうかを確認します。

   **show subscriber count nf-service smf ipv4-pool/ ipv6-pool<new pool>**

9. すべてのサブスクライバが新しいプールに戻ったら、古いプールの構成を IPAM から削除します。

```
[smf-m6-cndp-rack2/data] smf(config)# ipam instance 1
Mon Jul 24 08:43:19.875 UTC+00:00
[smf-m6-cndp-rack2/data] smf(config-instance-1)# no address-pool data-ipv6-pool2
```

（注） トラフィックの少ない時間帯やメンテナンス ウィンドウで、チャンク グループのない古いプールをチャンク グループのあるプールに移行することをお勧めします。

## 制限事項

この機能には次の既知の制限事項があります。

- チャンク グループは、小さいアドレス プールではなく、大きなアドレス プールを管理するために使用する必要があります。
- チャンク サイズ（dp-split）は、2K、4K、8K などにする必要があります。dp-split が 256 未満の場合には適していません。
- チャンク グループがアドレス プールに対して有効になる場合は、cache-split と dp-split の値を同じにする必要があります。

# チャンク グループ サイズを定義する IPv4 アドレス範囲の構成

IPv4 アドレス範囲の小さいチャンクグループのサイズを定義するには、次の構成を使用します：

```
config
  ipam
    instance gr_instance_id
      address-pool pool_name
           ipv4
           address-range start_ipv4_address end_ipv4_address
```

```
chunk-group chunks-per-group { 2 | 4| 8 }
exit
```

注：

- **address-range** *start_ipv4_address end_ipv4_address*：この CLI は、開始アドレスと終了アドレスで構成される IPv4 アドレス範囲の範囲を指定します。ドット付き 10 進表記のアドレス範囲。

  **chunk-group** が有効になっている場合、アドレス範囲内の IP の数は 2 の累乗にする必要があります。つまり、IP の数は偶数にする必要があります。アドレス範囲の IP の数が奇数である場合、次のエラー メッセージが表示されます。

  **"address range from " + startAddr +" to "+ endAddr + " is odd"**

（注） このチェックは、**chunk-group** が有効になっており、IPv4 アドレスにのみ適用可能な場合にのみ適用されます。

- **chunk-group**：この CLI は、プールのチャンク グループを構成します。
- **chunks-per-group** *{ 2 | 4| 8 }*：この CLI は、チャンク グループ内のチャンクの数を定義します。値は 2、4、または 8 のいずれかです。したがって、チャンク グループは次のように計算できます。

  **Chunk Group= Chunk Size * 2K or 4K or 8K**

（注） この機能では、グループごとの奇数のチャンクの構成はサポートも推奨もされていません。

## 設定例

次に、IPv4 アドレスの範囲のチャンク グループ サイズを定義する構成例を示します：

```
config
ipam
 instance 1
  address-pool poolv4
   vrf-name ISP
   tags
    dnn intershat
   exit
   ipv4
    split-size
     per-cache 256
     per-dp    256
    exit
    chunk-group
     chunks-per-group 4
    exit
    address-range 10.0.0.1 10.0.10.254
   exit
  exit
```

```
 exit
exit
```

## 設定の確認

次に、IPv4 アドレスの範囲のチャンク グループ サイズを定義する構成出力を示します：

```
[smf] smf# show ipam pool poolv4 ipv4-addr

=================================================================================================
Flag Indication: S(Static) O(Offline)
=================================================================================================
StartAddress          EndAddress          AllocContext                    Flag  GroupId
=================================================================================================
10.0.0.1              10.0.0.255          Free:CP                               1
10.0.1.0              10.0.1.255          Free:CP                               1
10.0.2.0              10.0.2.255          Free:CP                               1
10.0.3.0              10.0.3.255          Free:CP                               1
10.0.4.0              10.0.4.255          10.1.13.52:10.1.8.184                 2
10.0.5.0              10.0.5.255          10.1.13.52:10.1.8.184                 2
10.0.6.0              10.0.6.255          Free:CP                               2
10.0.7.0              10.0.7.255          Free:CP                               2
10.0.8.0              10.0.8.255          Free:CP                               3
10.0.9.0              10.0.9.255          Free:CP                               3
10.0.10.0             10.0.10.254         Free:CP                               3
```

（注） CLI **show ipam pool <pool-name> <ipv4-addr|ipv6-prefix|ipv6-addr>** 出力が更新され、チャンク グループ ID を示す追加の列 *GroupId* が 追加されました。同じグループに属するチャンクは、同じチャンク グループ ID に反映されます。

# チャンクグループを定義するための IPv6 プレフィックス範囲の構成

IPv6 アドレス範囲の小さいチャンク グループのサイズを定義するには、次の構成を使用します：

```
config
  ipam
    instance instance_id
      address-pool pool_name
        ipv6
          prefix-ranges
            prefix-range Prefix-range
            chunk-group chunks-per-group { 2 | 4| 8 }
            exit
```

## 設定例

次に、IPv6 プレフィックス範囲のチャンク グループ サイズを定義する構成例を示します。

```
ipam
 instance 1
  address-pool poolv6
   vrf-name ISP
```

```
   tags
    dnn intershat
   exit
   ipv6
    prefix-ranges
     split-size
      per-cache 8192
      per-dp    1024
     exit
     chunk-group
      chunks-per-group 4
     exit
     prefix-range 2001:db0:: length 48
    exit
   exit
  exit
 exit
exit
```

# チャンク グループを定義するための IPv6 アドレス範囲の設定

IPv6 アドレス範囲の小さいチャンク グループのサイズを定義するには、次の構成を使用します：

```
config
   ipam
      instance gr_instance_id
         address-pool pool_name
            vrf-name vrf_name
            ipv6
               address-range start_ipv6_address end_ipv6_address
               chunk-group chunks-per-group { 2 | 4| 8 }
               exit
```

## 設定例

次に、IPv6 アドレスの範囲のチャンク グループ サイズを定義する構成例を示します：

```
ipam
 instance 1
  address-pool poolv6DNN2
   vrf-name ISP
   tags
    dnn intershat1
   exit
   ipv6
    address-ranges
     split-size
      per-cache 1024
      per-dp    1024
     exit
     chunk-group
      chunks-per-group 4
     exit
     address-range 64:ff9b:: 64:ff9b::ffff:ffff
    exit
   exit
  exit
```

```
 exit
exit
```

# IPv6 プレフィックス範囲とアドレス範囲の構成の確認

IPv6 プレフィックス範囲とアドレス範囲の構成は、次の show コマンドを使用して確認できます：

```
[smf-m6-cndp-rack2/data] smf# show ipam dp 100.105.64.10:10.210.184.49 ipv6-p
Tue Jul  11 12:08:36.232 UTC+00:00

=============================================================================================
Flag  Indication: S(Static) O(Offline) R(For Remote Instance) RF(Route Sync Failed)
G:N/P Indication: G(Cluster InstId) N(Native NM InstId) P(Peer NM InstId)
=============================================================================================
StartAddress                  EndAddress                Route                     G:N/P
   Utilization   Flag      AllocContext
=============================================================================================
2607:fb90:8700::              2607:fb90:8700:fff::      2607:fb90:8700::/52       1:0/1
   100.00%                 data-ipv6-pool1(ISP)
2607:fb90:8700:1000::         2607:fb90:8700:1fff::     2607:fb90:8700:1000::/52 1:1/0
   100.00%                 data-ipv6-pool1(ISP)
=============================================================================================
```

IPv6 のチャンク グループごとに割り当てられたコンテキストは、次のコマンドを使用して確認できます：

**show ipam pool data-ipv6-pool2 ipv6-prefix | include（DP-Name）**

次に、出力/形式の例を示します：

```
[smf-m6-cndp-rack2/data] smf# show ipam pool data-ipv6-pool2 ipv6-prefix | include
100.105.64.80:10.210.184.49
Mon Jul 17 07:43:20.510 UTC+00:00
2607:fb90:8732:400::/64 2607:fb90:8732:7ff::/64 100.105.64.80:10.210.184.49 33
2607:fb90:8732:800::/64 2607:fb90:8732:bff::/64 100.105.64.80:10.210.184.49 33
2607:fb90:8732:1000::/64 2607:fb90:8732:13ff::/64 100.105.64.80:10.210.184.49 34
2607:fb90:8732:1800::/64 2607:fb90:8732:1bff::/64 100.105.64.80:10.210.184.49 34
2607:fb90:8732:2000::/64 2607:fb90:8732:23ff::/64 100.105.64.80:10.210.184.49 35
2607:fb90:8732:2800::/64 2607:fb90:8732:2bff::/64 100.105.64.80:10.210.184.49 35
2607:fb90:8732:3000::/64 2607:fb90:8732:33ff::/64 100.105.64.80:10.210.184.49 36
2607:fb90:8732:3800::/64 2607:fb90:8732:3bff::/64 100.105.64.80:10.210.184.49 36
2607:fb90:8732:4000::/64 2607:fb90:8732:43ff::/64 100.105.64.80:10.210.184.49 37
2607:fb90:8732:4800::/64 2607:fb90:8732:4bff::/64 100.105.64.80:10.210.184.49 37
2607:fb90:8732:5000::/64 2607:fb90:8732:53ff::/64 100.105.64.80:10.210.184.49 38
2607:fb90:8732:5800::/64 2607:fb90:8732:5bff::/64 100.105.64.80:10.210.184.49 38
2607:fb90:8732:6000::/64 2607:fb90:8732:63ff::/64 100.105.64.80:10.210.184.49 39
2607:fb90:8732:6800::/64 2607:fb90:8732:6bff::/64 100.105.64.80:10.210.184.49 39
2607:fb90:8732:7000::/64 2607:fb90:8732:73ff::/64 100.105.64.80:10.210.184.49 40
2607:fb90:8732:7800::/64 2607:fb90:8732:7bff::/64 100.105.64.80:10.210.184.49 40
2607:fb90:8732::/64 2607:fb90:8732:3ff::/64 100.105.64.80:10.210.184.49 33
2607:fb90:8732:c00::/64 2607:fb90:8732:fff::/64 100.105.64.80:10.210.184.49 33
2607:fb90:8732:1400::/64 2607:fb90:8732:17ff::/64 100.105.64.80:10.210.184.49 34
2607:fb90:8732:1c00::/64 2607:fb90:8732:1fff::/64 100.105.64.80:10.210.184.49 34
2607:fb90:8732:2400::/64 2607:fb90:8732:27ff::/64 100.105.64.80:10.210.184.49 35
2607:fb90:8732:2c00::/64 2607:fb90:8732:2fff::/64 100.105.64.80:10.210.184.49 35
2607:fb90:8732:3400::/64 2607:fb90:8732:37ff::/64 100.105.64.80:10.210.184.49 36
2607:fb90:8732:3c00::/64 2607:fb90:8732:3fff::/64 100.105.64.80:10.210.184.49 36
2607:fb90:8732:4400::/64 2607:fb90:8732:47ff::/64 100.105.64.80:10.210.184.49 37
2607:fb90:8732:4c00::/64 2607:fb90:8732:4fff::/64 100.105.64.80:10.210.184.49 37
2607:fb90:8732:5400::/64 2607:fb90:8732:57ff::/64 100.105.64.80:10.210.184.49 38
2607:fb90:8732:5c00::/64 2607:fb90:8732:5fff::/64 100.105.64.80:10.210.184.49 38
```

```
2607:fb90:8732:6400::/64 2607:fb90:8732:67ff::/64 100.105.64.80:10.210.184.49 39
2607:fb90:8732:6c00::/64 2607:fb90:8732:6fff::/64 100.105.64.80:10.210.184.49 39
2607:fb90:8732:7400::/64 2607:fb90:8732:77ff::/64 100.105.64.80:10.210.184.49 40
```

# 最大セッション サイズに基づく IP チャンクの事前割り当て

IPv6 アドレス範囲の小さいチャンク グループのサイズを定義するには、次の構成を使用します：

```
config
  ipam
    instance instance_id
      address-pool pool_name
        ipv4
          chunk-group chunks-per-group { 2 | 4| 8 }
          reserve-contiguous-groups
            exit
```

注：

- **reserve-contiguous-groups**： **reserve-contiguous-groups** が有効で、 **max-upf-sessions** が構成されている場合、IPAM は、**max-upf-sessions** の値をカバーするために、2 の累乗でチャンク グループとチャンクを予約します。

  たとえば、 **max-upf-sessions** が 60000 で、 **reserve-contiguous-groups** が DP サイズ 8192 で有効になっており、 **chunks-per-group** が 4 の場合、IPAM は 65536（2 の 16 乗）の IP を持つ 2 つのチャンク グループを予約し、UPF に向けてシングル ルートを発行します。

## 設定例

次に、UPF/vDNN に構成された最大セッションサイズに従って、複数の連続するチャンクを事前に割り当てるための構成例を示します。

```
[smf] smf# show running-config ipam instance 1 address-pool poolv4
Sun Jun  18 20:00:19.226 UTC+00:00
ipam
 instance 1
  address-pool poolv4
   vrf-name ISP
   tags
    dnn intershat
   exit
   ipv4
    split-size
     per-cache 256
     per-dp    256
    exit
    chunk-group
     chunks-per-group          4
     reserve-contiguous-groups
    exit
    address-range 10.0.0.1 10.0.10.254
   exit
  exit
 exit
exit
```

# OAM サポート

このセクションでは、この機能でサポートされているメトリックの詳細について説明します。

## メトリック

この機能により、次の 2 つのメトリックに新しいラベル **グループ ID** が追加されます。

1. **IPAM_chunk_events_total**
2. **IPAM_chunk_allocations_current**

**groupID**：このラベルは、UPF 用にチャンクが割り当て/解放されるチャンク グループ ID に関する追加情報をキャプチャします。次の構成は、このラベルを表示するのに役立ちます：

```
config
   infra metrics verbose application metrics IPAM_chunk_allocations_current level
production granular-labels [ groupID ]
   infra metrics verbose application metrics IPAM_chunk_events_total level production
granular-labels [ groupID ]
```

（注） **groupID** は詳細なラベルであり、このラベルの値の基数が高いため、デフォルトでは有効になりません。

# NAT のサポート

表 *325 :* 機能の履歴

| 機能名 | リリース情報 | 説明 |
|---|---|---|
| ネットワーク アドレス変換バインディング更新 | 2023.04 | SMF は、NAT バインディング レコ ード機能をサポートしています。この機能では、UPF から SMF に NAT バインディング レコード情報を提供するために N4 セッション レポート要求メッセージが使用されます。SMF は UPF から NAT バインディング レコード情報を受信した後、対応する NAT バインディング更新をRADIUS インターフェイスを介して AAA サーバに送信します。<br>**デフォルト設定** 無効：有効にするには構成が必要です。 |

# 機能説明

ネットワーク アドレス変換（NAT）は、プライベート IP ネットワークがインターネットとクラウドを使用できるようにするサービスです。NAT では、パケットを外部ネットワークに送信する前に、内部ネットワークのプライベート IP アドレスがパブリック IP アドレスに変換されます。これにより、IP アドレスを保存してセキュリティを向上させることができます。

NAT が UPF で有効になっている場合、外部プラットフォームはリアルタイム NAT バインディングの更新を必要とします。これにより、Gi インターフェイスで使用されるプライベート IP アドレスからパブリック IP アドレスへのマッピングを外部プラットフォームに提供できます。

SMF は、NAT バインディングレコ ード機能をサポートしています。この機能では、UPF から SMF に NAT バインディング レコード情報を提供するために N4 セッション レポート要求メッセージが使用されます。SMF は UPF から NAT バインディング レコード情報を受信した後、対応する NAT バインディング更新を RADIUS インターフェイスを介して AAA サーバに送信します。

詳細については、[UCC 5G SMF 構成およびアドミニストレーション ガイド（UCC 5G SMF Configuration and Administration Guide）] > [IP アドレス管理（IP Address Management）] の章を参照してください。

# 機能の仕組み

ここでは、SMF でのネットワーク アドレス変換バインド更新に関連するコール フローと手順について説明します。

ネットワーク アドレス変換バインド更新機能は、次の機能をサポートしています。

- ポート チャンクの割り当てとリリースの NAT バインディングの更新
- 有効な NAT IP によるセッションの削除
- SMF での NAT バインディング レコードの処理

## コール フロー

次のコール フローは、SMF で NAT バインディング更新を送信することを示しています。

### ポート チャンクの割り当て

ポート チャンク割り当てのための NAT バインディングの更新は、サブスクライバがネットワーク アドレス変換 IP アドレスを共有するときに発生します。これは、割り当てモードに基づいて、コール セットアップ時またはデータ フロー中に実行されます。NBU は、1 対 1 と多対 1 の両方のネットワーク アドレス変換 IP モードをサポートします。

このセクションでは、SMF でのポートチャンクの割り当てのためのネットワーク アドレス変換バインド更新に関連するコール フローについて説明します。

図 *175 :* ポート チャンク割り当てのコール フロー

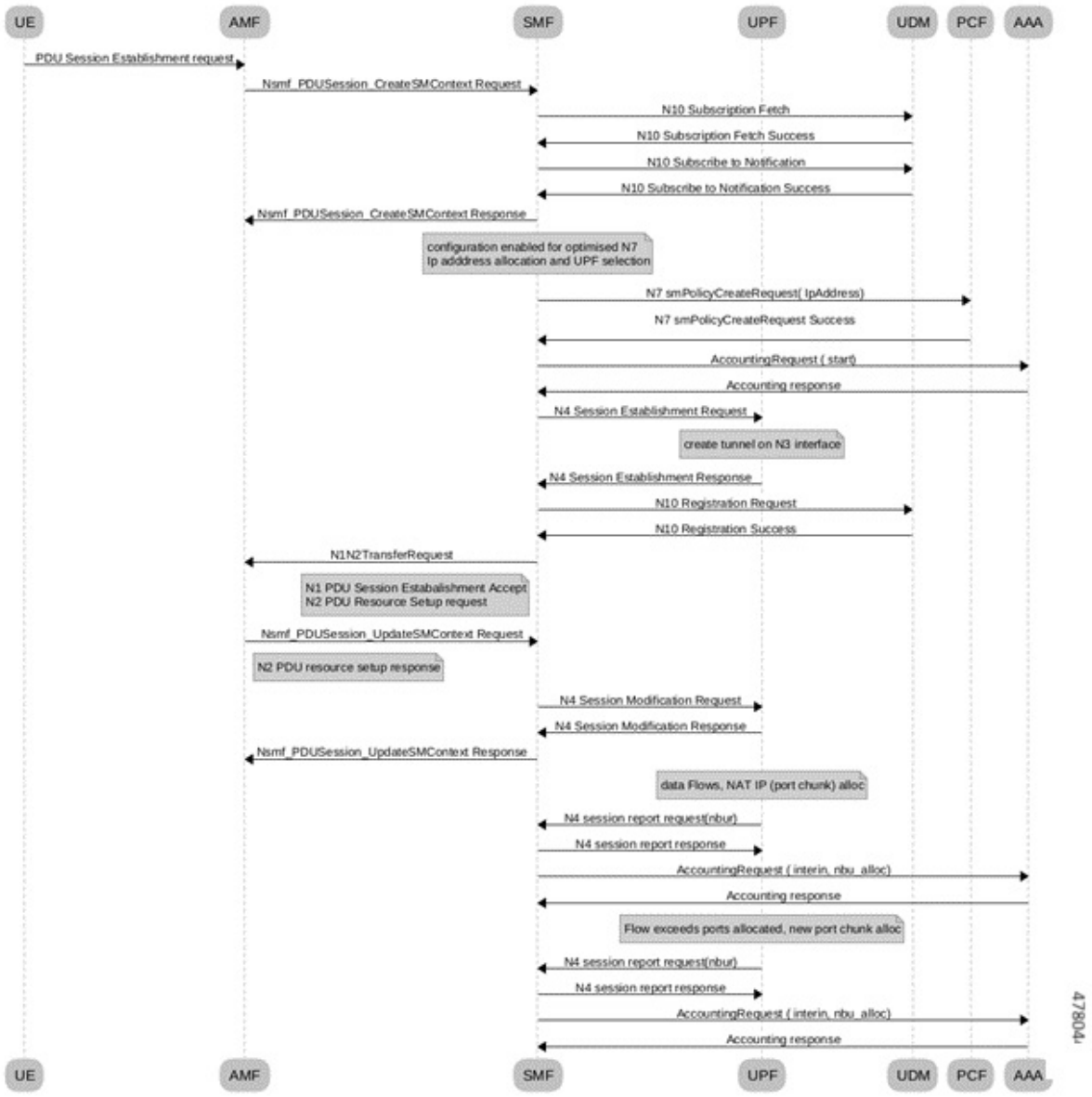



表 *326 :* ポート チャンクの割り当てコール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | 5G セッションの作成中に、RADIUS アカウンティング要求の開始メッセージが AAA サーバに送信されます。<br><br>。 |

| ステップ | 説明 |
|---|---|
| 2 | サブスクライバに対してデータ フローが発生すると、NAT IP とポート チャンクが割り当てられます。その後、UPF は、NBR 情報を含む新しい N4 セッション レポート要求を SMF に送信します。 |
| 3 | SMF は、RADIUS アカウンティング要求の中間更新として、NAT バインディング更新を NAT 関連の AVP とともに AAA に送信します。 |
| 4 | フローの数がすでに割り当てられているポートを通過すると、UPF は新しいポート チャンクを割り当てます。ポート チャンクが割り当てられるたびに、UPF は新しい N4 セッション レポート要求を SMF に送信し、SMF は RADIUS アカウンティングの中間更新として NAT バインディング更新を AAA サーバに送信します。 |

## ポート チャンクのリリース手順

このセクションでは、SMF でのポート チャンク リリースのネットワーク アドレス変換バインド更新に関連するコール フローについて説明します。

図 *176 :* ポート チャンク リリースのコール フロー

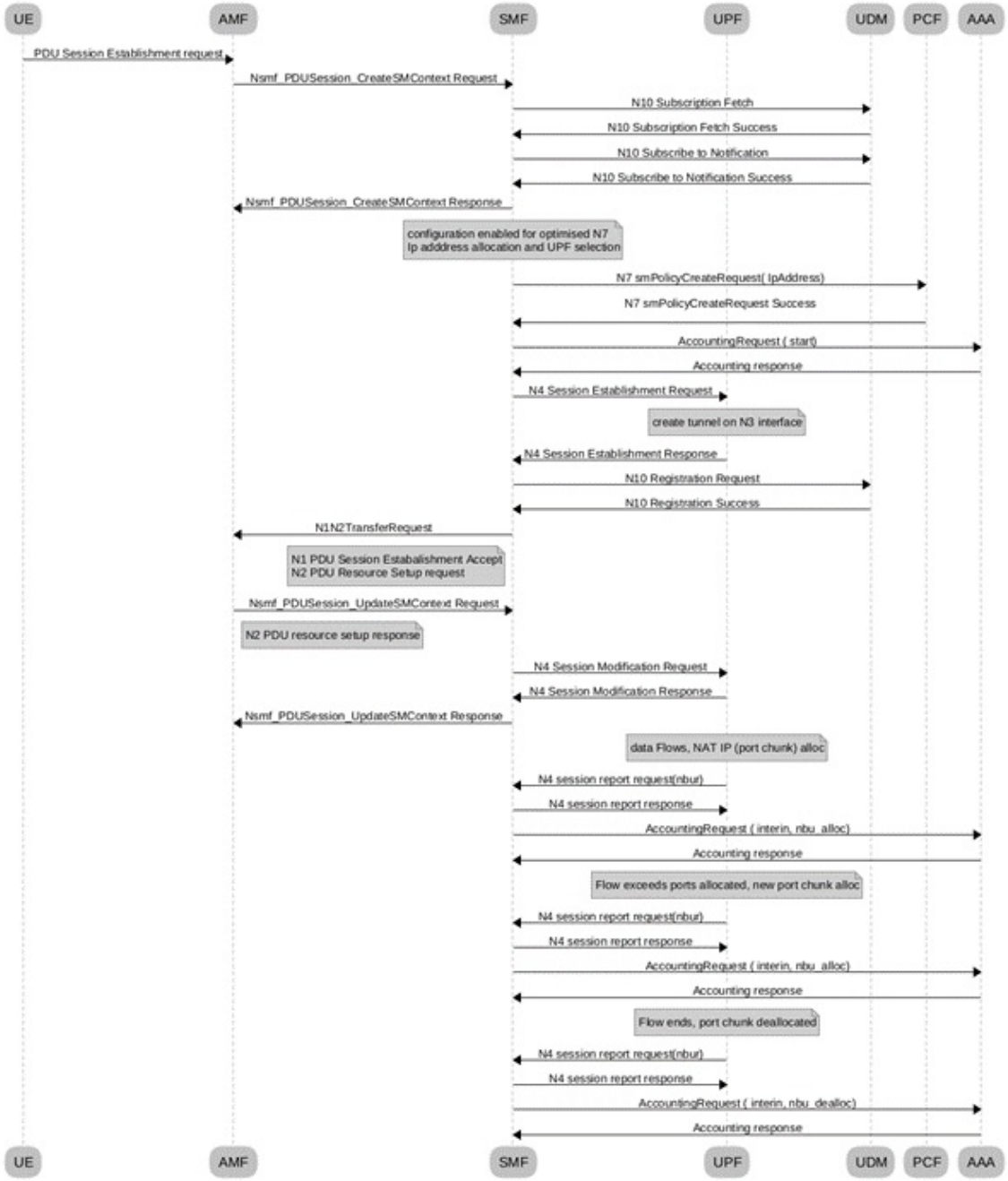


表 *327:* ポート チャンクのリリース コール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | 5G セッションの作成中に、RADIUS アカウンティング要求の開始メッセージが AAA サーバに送信されます。<br><br>。 |
| 2 | サブスクライバに対してデータ フローが発生すると、NAT IP とポート チャンクが割り当てられます。その後、UPF は、NBR 情報を含む新しい N4 セッション レポート要求を SMF に送信します。 |
| 3 | SMF は RADIUS アカウンティング要求の中間更新として NAT バインディング更新を NAT 関連 AVP とともに AAA サーバに送信します。 |
| 4 | フローの数がすでに割り当てられているポートを通過すると、UPF は新しいポート チャンクを割り当てます。ポート チャンクが割り当てられるたびに、UPF は新しい N4 セッション レポート要求を SMF に送信し、SMF は RADIUS アカウンティングの中間更新として NAT バインディング更新を AAA サーバに送信します。 |
| 5 | ポートチャンクが使用されていなければ、UPFはポートチャンクを解放します。ポート チャンクリリースごとに、N4 セッション レポート要求が SMF に送信されます。SMF は、NAT バインディング更新を RADIUS アカウンティング暫定更新として AAA サーバに送信します。 |
| （注）<br>ポートチャンクが割り当てられるか解放されるたびに、NAT バインディング更新がポート チャンク割り当てまたはポート チャンク リリースの RADIUS アカウンティング暫定更新として AAA サーバに送信されます。 | |

## 有効な NAT IP によるセッションの削除

次のコール フローは、SMF での有効な NAT IP によるセッション削除を示しています。

図 *177 :* セッション削除のコール フロー

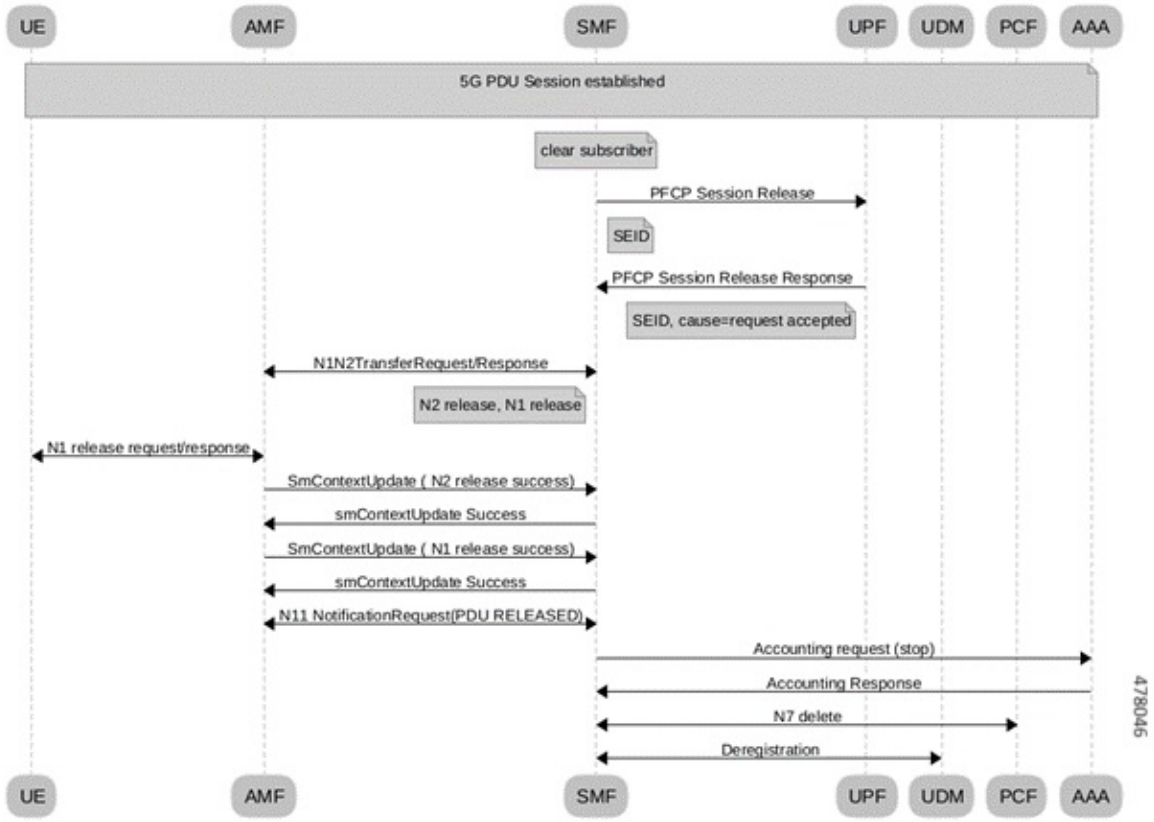



表 *328 :* セッション削除のコール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | 5G セッションの作成中に、RADIUS アカウンティング要求の開始メッセージが AAA サーバに送信されます。 |
| 2 | サブスクライバに対してデータ フローが発生すると、NAT IP とポート チャンクが割り当てられます。その後、UPF は、NBR 情報を含む新しい N4 セッション レポート要求を SMF に送信します。 |
| 3 | SMF は RADIUS アカウンティング要求の中間更新として NAT バインディング更新を AAA サーバに送信します。 |

セッション削除手順中には、ポートチャンクのリリースを示す明示的なメッセージは送信されません。通常のセッション削除手順の一環として、SMF は Radius Accounting STOP メッセージを AAA サーバに送信します。およびこの Radius STOP メッセージは、以前に送信した、サブスクライバのポートチャンク割り当てに関する NAT バインディング更新をクリアする必要があります。

# NAT バインディング手順の PFCP IE

次の表に、NAT バインディング情報を伝送する PFCP セッション レポート メッセージの IE を示します。

**表 *329 : NAT* バインド更新のセッション レポート要求**

| 情報要素 | 優先順位 | 条件/コメント | IE タイプ |
|---|---|---|---|
| レポート タイプ | M | この IE は、レポートのタイプが NBUR であることを示すものとします。 | レポート タイプ |
| NBR 情報 | M | NBR 情報 IE は、NAT バインド更新の情報を伝送するものとします | NBR 情報 |

次の表では、レポート タイプ IE のエンコーディングについて説明します。UPF 機能が SMF で送信するレポートのタイプを示します。NBR 情報を送信するには、レポート タイプを NBUR に設定します。

**図 *178 :* レポート タイプ**

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1–2 | Type = 39 (decimal) | | | | | | | |
| 3–4 | Length = n | | | | | | | |
| 5 | Spare | UISR | SESR | TMIR | UPIR | ERIR | USAR | DLDR |
| 6 | Spare | Spare | Sparte | Spare | Spare | NBUR | SPTER | MSUR |

478608

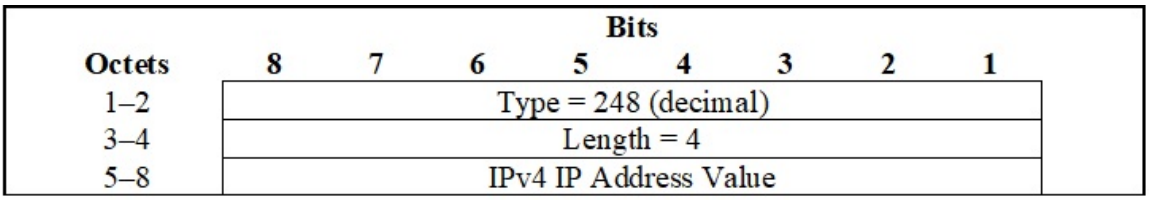
以下の表は、NBR 情報をグループ化した IE について記述したものです。

**図 *179 : NBR* 情報**

| Octet 1 and | NBR Info IE Type = 247 (decimal) | | | | | | |
|---|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | | **IE Type** |
| | | | **Sxa** | **Sxb** | **Sxc** | **N4** | |
| NAT IP | M | This IE shall identify NAT IP allocated or released | - | X | - | X | NAT IP |
| Port Chunk Info | M | Port Chunk Info IE carries Port Chunk that is allocated or released.<br>Several IEs within the same IE type may be present to represent a list of Port Chunks. | - | X | - | X | Port Chunk Info |
| Allocation Flag | M | Allocation Flag shall indicate that NBR Info is for Allocation or for Release | - | X | - | X | Allocation Flag |
| NAPT Number of Users Per IP | M | This IE carries Number of Users allowed to share the same NAT IP | - | X | - | X | NAPT Number of Users Per IP |
| Release Timer | M | Release Timer is the Release Timer configure for the realm from which NAT IP was allocated or released | - | X | - | X | Release Timer |

次の表で、NAT IP IE のエンコーディングについて説明します。

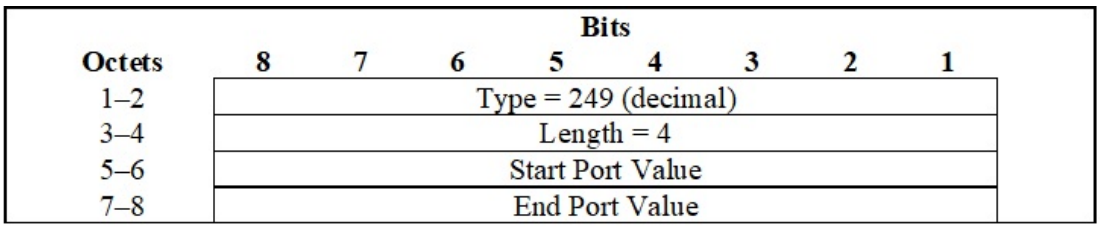
図 *180 : NAT IP*



| Octets | Bits 8 7 6 5 4 3 2 1 |
|---|---|
| 1–2 | Type = 248 (decimal) |
| 3–4 | Length = 4 |
| 5–8 | IPv4 IP Address Value |

次の表で、ポート チャンク情報 IE のエンコーディングについて説明します。

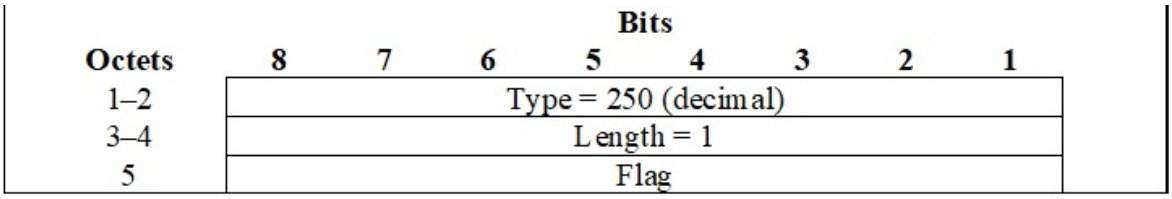
図 *181 :* ポート チャンク情報



| Octets | Bits 8 7 6 5 4 3 2 1 |
|---|---|
| 1–2 | Type = 249 (decimal) |
| 3–4 | Length = 4 |
| 5–6 | Start Port Value |
| 7–8 | End Port Value |

次の表では、割り当てフラグ IE のエンコードについて説明します。

図 *182 :* 割り当てフラグ

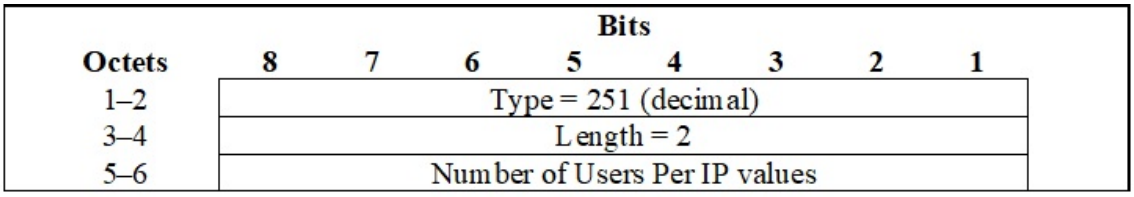


| Octets | Bits 8 7 6 5 4 3 2 1 |
|---|---|
| 1–2 | Type = 250 (decimal) |
| 3–4 | Length = 1 |
| 5 | Flag |

フラグ値 1 は割り当てを示し、フラグ値 0 はリリースを示します。

次の表に、IP IE ごとの NAPT ユーザー数のエンコーディングについて示します。

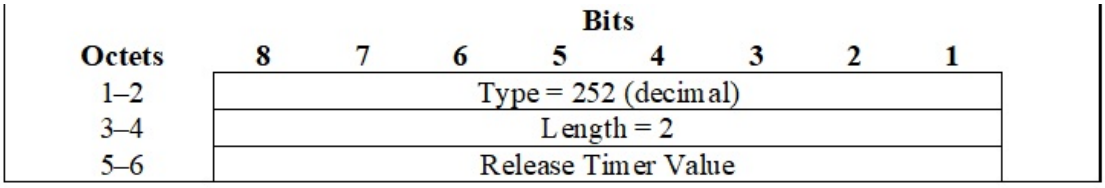
図 *183 : IP* ごとの *NAPT* ユーザー数



| Octets | Bits 8 7 6 5 4 3 2 1 |
|---|---|
| 1–2 | Type = 251 (decimal) |
| 3–4 | Length = 2 |
| 5–6 | Number of Users Per IP values |

次の表では、リリース タイマー IE のエンコーディングについて説明します。

図 *184 :* リリース タイマー



| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1–2 | Type = 252 (decimal) | | | | | | | |
| 3–4 | Length = 2 | | | | | | | |
| 5–6 | Release Timer Value | | | | | | | |

リリース タイマーの値は秒単位です。

## SMF でのネットワーク アドレス変換バインディング レコードの処理

SMF は、Non-State Handler プロセスでセッション レポートを処理します。応答はすぐに返され、要求を処理するために内部イベントが投稿されます。

通常、NAT バインド レポートは優先順位が高いと見なされ、それらを使用状況レポートの手順に追加すると、時間がかかります。これは、使用状況レポート手順が、引き継ぎ、変更、アイドル モード手順などの他の手順と比較して優先順位が低いためです。

適切な優先順位で処理するために、SMF は非状態ハンドラの一部として NBU の NIntSelfTxnN4SessRptReq を処理します。これにより、他の手順が進行中の場合でもメッセージを処理できます。これにより、NAT バインドの更新処理が現在の手順を完了するまで待機する必要がなくなります。

通常のセッション レポートの処理に関する変更はありません（非 NBU）。

（注） 作成およびリリースの手順中、NAT バインディング レポートは完全に処理されません。N4 成功応答のみが送信され、メッセージは無視されます。

## NAT バインド手順の Radius AVP

NBU は、RADIUS アカウンティング暫定更新メッセージの一部として送信されます。標準の RADIUS アカウンティング属性に加えて、次の新しい RADIUS 属性（AVP）が NBU メッセージの一部として送信されます。

- NAT-IP-Address：ネットワーク アドレス変換 IP アドレスの割り当てまたはサブスクライバ フローへの解放。
- NAT-Port-Block-Start：割り当てまたは解放されたポート チャンクの開始ポート。
- NAT-Port-Block-End：割り当てまたは解放されたポート チャンクの終了ポート。
- Alloc-Flag：フラグは、NBU が割り当てまたはリリース用であることを示します。1 は割り当て、0 は解放の場合です。
- 負荷係数：IP あたりのユーザー数
- Binding-Timer：ネットワーク アドレス変換バインディング リリース タイマー

## 制限事項

次の制限事項があります。

- IP を解放する前にバッテリが低下した場合など、アングレース フル終了が原因でコールがクリアされた場合は、ネットワーク アドレス変換のバインド更新は実行されません。
- ネットワーク アドレス変換バインド更新機能が有効になっている場合、UPF から SMF へ、および SMF から AAA サーバーへの追加のシグナリングにより、SMF へのパフォーマンス上の影響が最小限になる可能性があります。
- NBU を AAA サーバーに送信するための追加のホップ（UPF から SMF への更新）があるため、NBU が送信される前に遅延が発生する可能性があります。したがって、これらの更新のリアルタイム配信を実現することが保証されていません。

# NAT バインディング更新の設定

次の CLI は、SMF で NAT バインドの更新を構成します。

```
config
  profile dnn intershat dnn_intershat
    supported-features   [ inter-plmn-ho nat-binding-update  ]
  exit
```

注

- **supported-features** ：DNN レベルの SMF で有効または無効にできるサポートされている機能のリスト。このフラグは、*plmn* 間のローミング ハンドオーバーを有効にします
- **inter-plmn-ho** ：PLMN ローミングのハンドオーバーを有効にします。
- **nat-binding-update** ：NAT バインディング更新手順のサポートを有効にします。

。

# OAM サポート

## バルク統計

NAT バインディング更新（NBU）機能をサポートするために、次のメトリックの詳細が変更されました。

- smf_sess_report_stats ：この既存のメトリックには、新しいラベル値 sess_report_type_nbur が追加されたラベル sess_report_type が含まれています。NBU での PFCP セッション レポートの処理にメトリックを使用します。

  **メトリック例**：

  ```
  smf_sess_report_stats{app_name="SMF",cluster="SMF",data_center="DC",gr_instance_id="1",
  instance_id="0",rat_type="NR",reason="success",
  service_name="smf-service",sess_report_type="sess_report_type_nbur"} 3
  ```

- radius_accounting_message_stats：この既存のメトリックには、新しいラベルの trigger_reason と新しいラベル値 nat_binding_updateが含まれています。NBU での PFCP セッション レポートの処理にメトリックを使用します。

  **メトリック例**：

```
Attempt:
radius_accounting_message_stats{app_name="SMF",cluster="SMF",data_center="DC",
dnn="",gr_instance_id="1",instance_id="0",procedure_type="radius_update",
rat_type="NR",reason="",service_name="smf-service",status="attempted",
trigger_reason="nat_binding_update"} 3

Successful Response:
radius_accounting_message_stats{app_name="SMF",cluster="SMF",data_center="DC",
dnn="",gr_instance_id="1",instance_id="0",procedure_type="radius_update",
rat_type="NR",reason="",service_name="smf-service",status="success",
trigger_reason="nat_binding_update"} 2

Failure Response:
radius_accounting_message_stats{app_name="SMF",cluster="SMF",data_center="DC",
dnn="",gr_instance_id="1",instance_id="0",procedure_type="radius_update",
rat_type="NR",reason="",service_name="smf-service",status="failures",
trigger_reason="nat_binding_update"} 1
```

# トラブルシューティング情報

このセクションでは、システムの動作中に発生する可能性のある問題をトラブルシューティングするために、コマンド ライン インターフェイス（CLI）コマンド、アラート、ログとメトリックスの使用に関する情報について説明します。

## UPF に割り当てられる IPv6 の範囲

**show ipam dp** *dp_name* **ipv6-prefix** CLI コマンドは、UPF に割り当てられた IP プール チャンクを表示します。このプールチャンクには、VRF タグ情報と、定義されているプールが静的プールまたはダイナミック プールのどちらであるかなどの詳細が含まれます。

```
[unknown] smf# show ipam dp 198.18.1.3 ipv6-prefix

================================================================================
Flag Indication: S(Static) O(Offline)
N/P  Indication: N(Native InstId) P(Peer InstId)
================================================================================
StartAddress          EndAddress            AllocContext       Route
  N/P    Utilization   Flag
================================================================================
3001:db0::            3001:db0:0:3fff::     v6pool4(vrf4@ISP)  3001:db0::/50
  -                    S
3001:db0::            3001:db0:0:3fff::     v6pool3(vrf3@ISP)  3001:db0::/50
  -                    S
3001:db0:0:4000::     3001:db0:0:7fff::     v6pool4(vrf4@ISP)  3001:db0:0:4000::/50
  -                    S
3001:db0:0:4000::     3001:db0:0:7fff::     v6pool3(vrf3@ISP)  3001:db0:0:4000::/50
  -                    S
================================================================================
[unknown] smf#
```

# UPF に割り当てられる IPv4 の範囲

**show ipam dp** *dp_name* **ipv4-addr** CLI コマンドは、UPF に割り当てられた IP プール チャンクを表示します。このプール チャンクには、VRF タグ情報と、定義されているプールが静的プールまたはダイナミック プールのどちらであるかなどの詳細が含まれます。

```
[unknown] smf# show ipam dp 209.165.201.3 ipv4-addr
```

```
==============================================================================================
Flag Indication: S(Static) O(Offline)
N/P  Indication: N(Native InstId) P(Peer InstId)
==============================================================================================
StartAddress     EndAddress         AllocContext       Route               N/P
Utilization   Flag
==============================================================================================
209.165.200.129  209.165.202.131    v4pool3(vrf3@ISP)209.165.200.129/27      -
         -S
209.165.200.129  209.165.202.131    v4pool4(vrf4@ISP)209.165.200.129/27      -
         -S
209.165.200.253  209.165.202.153    v4pool3(vrf3@ISP)209.165.200.253/27      -
         -S
209.165.200.253  209.165.202.153    v4pool4(vrf4@ISP)209.165.200.253/27      -
         -S
209.165.202.154  209.165.202.155    v4pool3(vrf3@ISP)209.165.202.154/27      -
         -S
209.165.202.154  209.165.202.155    v4pool4(vrf4@ISP)209.165.202.154/27      -
         -S
209.165.202.156  209.165.202.156    v4pool3(vrf3@ISP)209.165.202.156/27      -
         -S
209.165.202.156  209.165.202.156    v4pool4(vrf4@ISP)209.165.202.156/27      -
         -S
209.165.202.128  209.165.202.158    v4pool4(vrf4@ISP)209.165.202.128/27      -
         -S
209.165.202.129  209.165.202.158    v4pool4(vrf4@ISP)209.165.202.129/27      -
         -S
209.165.200.225  209.165.200.253    v4pool4(vrf4@ISP)209.165.200.225/27      -
         -S
209.165.201.134  209.165.201.30     v4pool4(vrf4@ISP)209.165.201.134/27      -
         -S
==============================================================================================
```

# IP プール マッピング エラー ログ

次に、静的 IP からプールへのマッピングが正しくない場合、または RADIUS から受信した静的 IP が UPF で見つからない場合のエラー ログの例を示します。

```
[smf-service-n0-0] 2020/09/23 07:42:25.969 smf-service [DEBUG] [rmgrutil.go:501]
[smf-service.smf-app.resource] [imsi-123456789012345:5] [imsi-123456789012345:5] [16]
response received for message NmgrRersourceMgmtResponse
[smf-service-n0-0] 2020/09/23 07:42:25.969 smf-service [INFO] [upmgrCacheApi.go:450]
[misc-lib.upmgrcache.gen] Cache doesnot have entry for UpfEpKey:
[smf-service-n0-0] 2020/09/23 07:42:25.969 smf-service [ERROR] [rmgrutil.go:73]
[smf-service.smf-app.resource] [imsi-123456789012345:5] [imsi-123456789012345:5] [16]
Both the associated nodemgr instances for upfEpKey:  is down
[smf-service-n0-0] *errors.errorString Both the associated nodemgr instances for upfEpKey:
  is down
[smf-service-n0-0]
/opt/workspace/smf-service/src/smf-service/vendor/wwwin-github.cisco.com/
mobile-cnat-golang-lib/app-infra.git/src/app-infra/infra/Transaction.go:621 (0xd8b29e)
```

```
[smf-service-n0-0]
/opt/workspace/smf-service/src/smf-service/procedures/generic/rmgrutil.go:73 (0x14dbd61)
```

# N4 リソースまたは関連付けをリリース

表 *330 :* 機能の履歴

| 機能名 | リリース情報 | 説明 |
|---|---|---|
| N4 リソースまたは関連付けのリリース | 2023.04 | SMF は、CLI **release-resource**を使用した、SMF からの特定の UPF に関するリソースのクリアをサポートしています。 |

## 機能説明

ネットワークが IP プールの状態に関して異常な状態（SMF と UPF 間のプールの不一致など）になっている場合は常に、特定の UPF に関するサブスクライバ セッション、IP プール/チャンクなどのリソースを SMF。

この機能により、SMF からのリソース解放プロセスをトリガーして自動化する CLI が導入されます。リソース リリース プロセスがトリガーされると、SMF は次の 2 つの処理を行います。

1. ピアに関連付けられているすべての IP プールがクリアされます。これにより、プールを使用してコールがクリアされ、ルートも削除されます。

（注） 静的 IP チャンクは、リソース解放操作の一部としてクリアされません。

2. 新しいコール切断理由が SMF 切断統計に追加されました。また、ルートは 2 分の隔離時間の後に UPF に再登録されます。

**注意** この機能は、SMF が異常な状態の場合にのみ実行されます。正常な SMF で実行すると、コールのクリアが必要になるため、アクティブなサブスクライバに影響します。十分に注意してください。

## 機能の仕組み

N4 リソースまたはアソシエーションのリリース プロセスは、次の手順に従います。

1. UPF の優先順位を 0 に設定する。これにより、新しいコールがこの UPF をピックアップしないようにします。
2. N4 インターフェイスに対して コマンドを実行し、リソースをクリーンアップします。

3. コールがクリアされているかどうかを確認してください。
4. UPFの優先順位をバックに設定します。

## N4 リソースまたは関連付けのリリースの構成

次の構成は、SMF と UPF 間の N4 リソースまたは関連付けを解放するために使用されます。

**mode debug exec action release-resource attributes { interface n4 peer { ip** *upf_ip* **} } condition { dnn matches** *dnn-name* **}**

注：

- **debug**：このキーワードは、動作 CLI がデバッグ モードであることを示します。
- **exec**：このコマンドは、SMF から UPF ごとに N4 リリースをトリガするコマンドを実行します。
- **action** ：このコマンドは、実行するアクションを示します。
- **release-resource**： **release-resource**を実行すると、SMF は指定されたピアに対してサブスクライバ/プール リソースのクリーンアップをトリガします。
- **attributes**：このコマンドは、アクションを実行する属性を定義します。
- **peer**：UPF ピアは、UPF IP アドレスを使用して定義できます。
- **interface** ：このコマンドは、操作をトリガするインターフェイス名を指定します。
- **condition**：この CLI は、選択した操作のデータをフィルタリングするための追加の条件を指定します。これはオプションのフィルタです。
- **dnn**：この dnn-name に関連付けられているプールは、指定された演算子に基づいてクリアされます。ここでは、IP プールが割り当てられている DNN 名を使用する必要があります。
- **matches**：このコマンドは、出力修飾子に一致する DNN を確認します。

### 設定例

以下は、N4 リソースまたは関連付けを解放するための構成例です。

```
mode debug exec action release-resource attributes { interface n4 peer { ip <upf_ip> }
} condition { dnn matches dnn1 }
```

### 設定の確認

次のコマンドは、UPF および SMF ごとに N4 リソースおよびアソシエーションを解放するための構成を確認します。

```
[smf] smf# show ipam pool poolv4 ipv4-addr
Wed Aug  23 07:04:48.511 UTC+00:00

================================================================================
Flag Indication: S(Static) O(Offline)
================================================================================
```

```
StartAddress          EndAddress         AllocContext                  Flag  GroupId
================================================================================================
209.165.200.225       209.165.200.231    QT:NM1
209.165.200.232       209.165.200.239    Free:CP
209.165.200.240       209.165.200.247    Free:CP
209.165.200.248       209.165.200.254    Free:NM1
================================================================================================
```

## OAM サポート

このセクションでは、この機能でサポートされているメトリックの詳細について説明します。

### メトリック

次の理由が **smf_disconnect_stats** カウンタに追加されます。

**disk_rel_upf_admin_clear**：管理者によってトリガーされた特定の UPF の IP チャンクがクリアされるため、セッションが終了する。

# 破損した IP チャンクの識別

## 機能説明

SMF では、構成された IP プールとそのデータをキャッシュポッドおよび IPAM の内部状態で監査することにより、欠落しているか破損した IP チャンクを特定できます。

（注） 欠落または破損した IP チャンクを特定するための SMF の構成に関するご質問については、Cisco のアカウント担当者またはサポート担当者にお問い合わせください。

## 機能の仕組み

SMFは、次のシナリオによるIPAMデータの破損を確認できるデバッグ情報をキャプチャできます。

- チャンク エントリが IPAM キャッシュポッド データから欠落しています。
- チャンク エントリは存在しますが、プール名、アドレスタイプ、gr-instance-id などの必須の非固有キーがいくつか欠落しています。
- チャンクは、キャッシュポッドに割り当て済み（ロック済み）に表示されますが、ノードマネージャによって UPF に割り当てられません。
- チャンクはキャッシュポッドで空きとして示されていますが、ノードマネージャがIPチャンクを UPF（DP）に割り当てています。

# OAM サポート

このセクションでは、この機能でサポートされているメトリックスと統計について説明します。

## バルク統計

次のメトリックは、新しいカテゴリ **[SMF IPAM プール チャンクの合計カウンタ カテゴリ（SMF IPAM Pool Total Chunks Counter Category）]**でサポートされます：

**[IPAM_pool_total_chunks]**：プールの合計チャンク数をキャプチャします。

- **[Metrics-Type]**：ゲージ

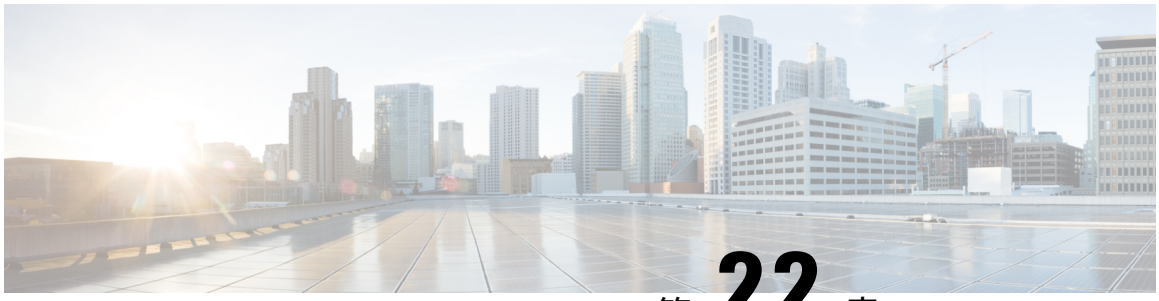
次のラベルは、このメトリックの一部としてサポートされています：

- **[grInstId]**：GR インスタンス ID
- **[プール（pool）]**：IP アドレス プール名
- **[addressType]**：Address-Type（ipv4/ipv6）
- **[IPAM_chunk_Alloc_Type]**：チャンクの割り当て状態

  次の値のいずれかになります：

  - **[FreeCP]**：cache-pod でチャンクが解放される
  - **[FreeNM]**：ノード マネージャ インスタンスでチャンクが解放されている
  - **[AllocatedUPF]**: UPFに割り当てられたチャンク

（注） パラメータ FreeCP ラベルは、キャッシュポッドで使用可能な空きチャンクの合計数をキャプチャします。この値はノード マネージャ インスタンスに共通であるため、ノード マネージャ インスタンスの1つ（リーダー）によってのみキャプチャされます。このようにして、Grafana 合計クエリは正しい合計チャンク数を表示します。



第 22 章

# IPv6 PDU セッション


- 機能の概要と変更履歴, on page 1005
- 機能説明, on page 1006
- ルータ要請とルータ アドバタイズメントの構成, on page 1007


## 機能の概要と変更履歴

### 要約データ

***Table 331:*** 要約データ

| | |
|---|---|
| 該当製品または機能エリア | SMF |
| 該当プラットフォーム | SMI |
| 機能のデフォルト設定 | 有効：常時オン |
| このリリースでの関連する変更点 | N/A |
| 関連資料 | 該当なし |

### 更新履歴

***Table 332:*** マニュアルの変更履歴

| 改訂の詳細 | リリース |
|---|---|
| ICMPv6 プロファイル構成オプションで次のコマンドの許容範囲の値を追加しました。<br>• **mtu**<br>• **reachable-time**<br>• **retrans-timer** | 2021.02.1 |

| 改訂の詳細 | リリース |
|---|---|
| 最初の導入。 | 2020.02.0 より前 |

# 機能説明

SMF は、IPv6 のステートレス自動構成に準拠するため、ICMPv6 のルータ要求とアドバタイズメントをサポートしています。

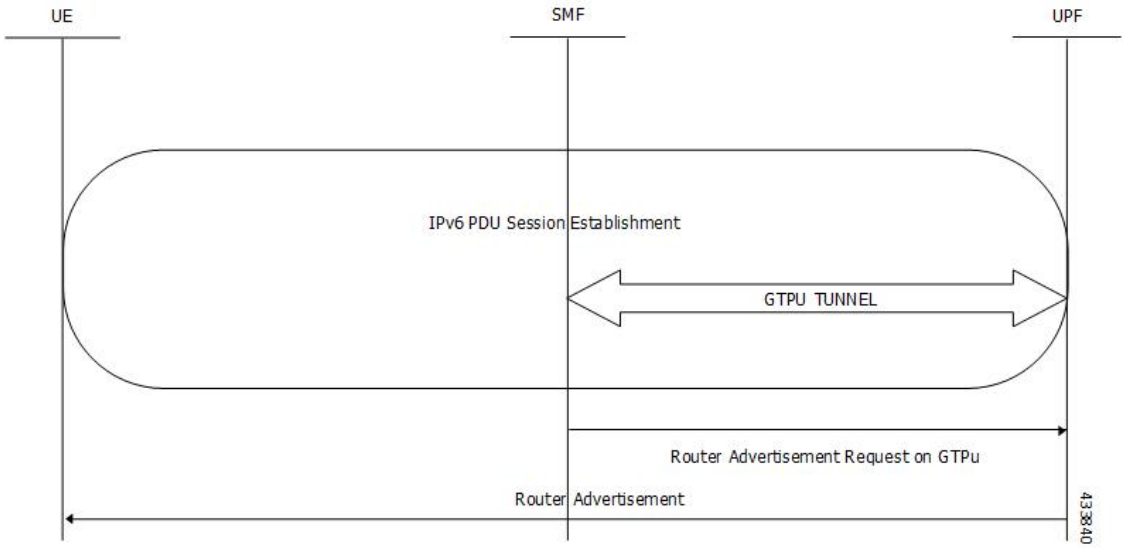
ルータ アドバタイズメントは、次の ICMPv6 オプションをサポートしています。

- プレフィックス情報：割り当てられた UE IPv6 プレフィックスを送信します。
- MTU：構成から MTU サイズを取得します。デフォルト値は1500 です。
- 送信元リンク層アドレス：構成されたローカル仮想 MAC から値を取得します。

# 未承諾のルータ アドバタイズメント

SMF は、正常な PDU セッション確立時に非送信請求ルータ アドバタイズメントを送信して、割り当てられた IPv6 プレフィックスを UE に共有します。RA メッセージは、セッション確立手順中に SMF と UPF の間で作成される GTPU トンネルを介して送信されます。また、SMF は UPF に PDR および FAR をインストールして、RS および RA メッセージのルーティングを有効にします。

***Figure 185:*** ルータ アドバタイズメント メッセージ処理コール フロー

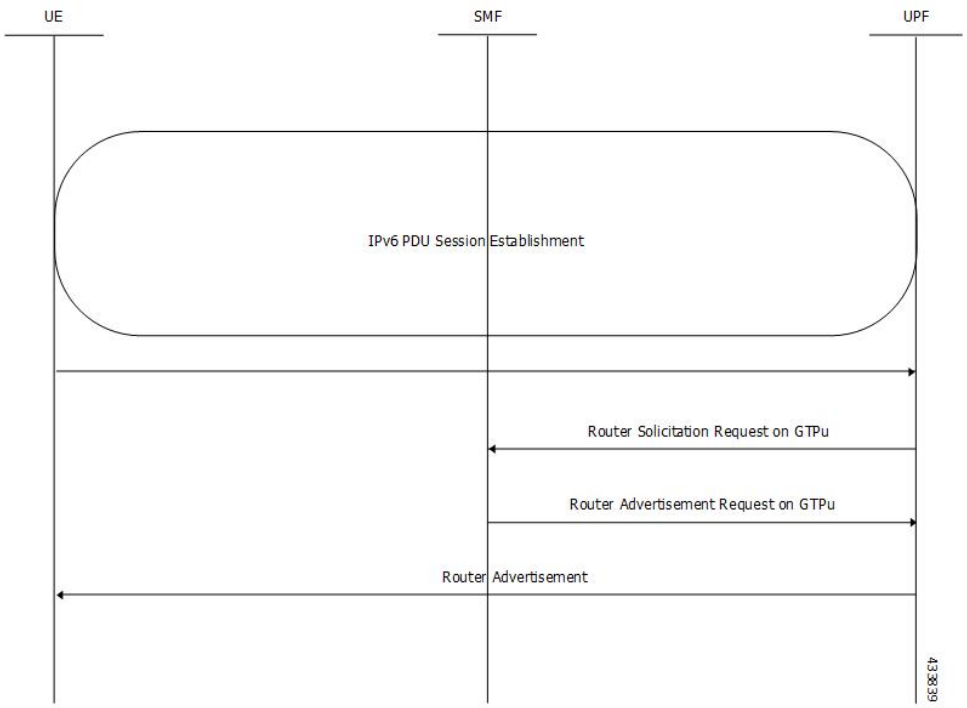


**Note** IPv6 プレフィックスの割り当ては SMF によって実行されるため、UPF は非要請ルータ アドバタイズメントを生成したり、UE に送信したりできません。

# 要請ルータ アドバタイズメント

割り当てられた IPv6 プレフィックスを取得するために、UE はルータ要請メッセージを送信します。ルータ要請メッセージを受信すると、SMF は、割り当てられた UE IPv6 プレフィックスを含むルータ アドバタイズメント メッセージを UE に送信します。

***Figure 186:*** ルータ要請とアドバタイズメント メッセージ処理コール フロー




# ルータ要請とルータ アドバタイズメントの構成

ここでは、ルータ送信要求およびルータ アドバタイズメント機能を構成する方法について説明します。

ルータ送信要求およびルータ アドバタイズメント機能の設定には、次の作業が含まれます：

- ルータ アドバタイズメントのパラメータの構成, on page 1008
- 仮想 MAC アドレスの構成, on page 1009
- ICMPv6 プロファイルと SMF サービス プロファイルの関連付け, on page 1010

# ルータ アドバタイズメントのパラメータの構成

ルータ アドバタイズメントのパラメータを構成するには、次の構成例を使用します：

```
config
  profile icmpv6 icmpv6profile_name
    options { hop-limit hop_limit | mtu mtu_size | reachable-time
reachable_time | retrans-timer retrans_timer | router-lifetime router_lifetime
 | virtual-mac virtual_mac }
    ra trigger handover { false | true }
    end
```

注：

- **profile icmpv6** *icmpv6profile_name*：ICMPv6 プロファイル名を指定します。*icmpv6profile_name* は 英数字の文字列である必要があります。
- **options { hop-limit** *hop_limit* **| mtu** *mtu_size* **| reachable-time** *reachable_time* **| retrans-timer** *retrans_timer* **| router-lifetime** *router_lifetime* **| virtual-mac** *virtual_mac* **}**：ICMPv6 オプションを構成します。
  - **hop-limit** *hop_limit*：ホップ リミットを構成します。 *hop_limit* は 0 ー 255 の範囲の整数である必要があります。デフォルト：255。
  - **mtu** *mtu_size*：MTU サイズを構成します。デフォルト：1,500。

    *mtu_size* は 、1280 ～ 1500 の範囲の整数である必要があります。
  - **reachable-time** *reachable_time*：到達可能時間をミリ秒単位で構成します。デフォルト：[0]。

    *reachable_time* は、0 ～ 3600 の範囲の整数である必要があります。
  - **retrans-timer** *retrans_timer*：再送信タイマーをミリ秒単位で構成します。デフォルト：[0]。

    *retrans_timer* は 、0 ～ 4294968 の範囲の整数である必要があります。
  - **router-lifetime** *router_lifetime*：ルータのライフタイムを秒単位で構成します。*router_lifetime* は 0 ～ 65535 の範囲の整数である必要があります。デフォルト：65535。
  - **virtual-mac** *virtual_mac*：ローカル仮想 MAC アドレスを設定します。
- **ra trigger handover { false | true }**：Wi-Fi ハンドオーバーのルータ アドバタイズメントを送信するトリガーを構成します。

### 設定の確認

**show running-config profile icmpv6** コマンドを使用して、ルータ アドバタイズメントの構成を確認します。

次の構成は、コマンドの出力例です：

```
[unknown] smf(config)# show running-config profile icmpv6
profile icmpv6 icmpprf1
 options hop-limit 255
 options mtu   1500
 options reachable-time 0
 options retrans-timer 0
 options router-lifetime 65535
 options virtual-mac b6:6d:57:45:45:45
 ra trigger handover true
exit
```

# 仮想 MAC アドレスの構成

DNNプロファイルでリモート仮想MACアドレスを構成するには、次の構成例を使用します：

```
config
  profile dnn dnnprofile_name
    virtual-mac mac_address
    exit
```

注：

- **profile dnn** *dnnprofile_name*：DNN プロファイル名を指定します。*dnnprofile_name*は英数字の文字列である必要があります。
- **virtual-mac** *mac_address*：UE のインターフェイス ID の生成に使用するリモート仮想 MAC アドレスを指定します。 *mac_address* は MAC アドレス パターンの文字列である必要があります。

リリース 2021.01 以降では、SMF は SBI VIP アドレスとサブスクライバの CommonId を使用して、非 EUI-64 形式である一意の 64 ビットのインターフェイス ID を生成します。

つまり、IPv6 インターフェイス ID = VIP-IP（4 バイト）+ CommonId（4 バイト）です。

デフォルトでは、 **virtual-mac** CLI コマンドは DNN 構成で無効になっています。

**表 *333*：各種メッセージのインターフェイス *ID***

| コール モデル | PDU セッション確立の承認 | セッション応答の作成 |
|---|---|---|
| 5G | N11-SBI-VIP+CommonID | — |
| 4G | — | GTP-VIP + CommonID |
| Wi-Fi | — | GTP-VIP + CommonID |
| 5G->4G | — | —（N26 HO - ハンドオーバー中に NAS コンテンツが存在します） |
| 4G->5G | —（N26 HO - ハンドオーバー中に NAS コンテンツが存在します） | — |

| コール モデル | PDU セッション確立の承認 | セッション応答の作成 |
|---|---|---|
| 4G->WiFi | — | GTP-VIP + CommonID（4G と同じ） |
| WiFi->4G | — | GTP-VIP + CommonID（4G と同じ） |
| 5G->WiFi | — | N11-SBI-VIP+CommonID（5G と同じ） |
| WiFi->5G | GTP-VIP + CommonID（WiFi と同じ） | — |

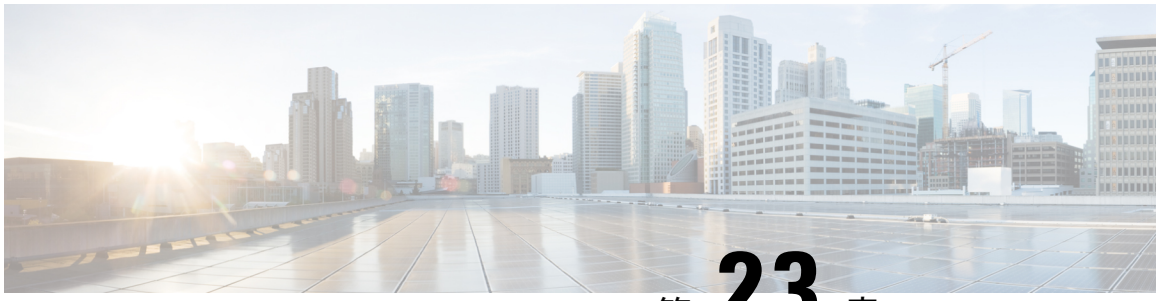
# ICMPv6 プロファイルと SMF サービス プロファイルの関連付け

次の構成例を使用して、ICMPv6プロファイルをSMFサービスプロファイルに関連付けます。

```
config
  profile smf smfprofile_name
    service name svc_name
      icmpv6-profile icmpv6profile_name
      exit
```

注：

- **profile smf** *smfprofile_name*：SMF サービス プロファイル名を指定します。 *smfprofile_name* 英数字の文字列である必要があります。
- **service name** *svc_name*：SMF ネットワーク機能サービスの名前を指定します。*svc_name* は英数字の文字列である必要があります。
- **icmpv6-profile** *icmpv6profile_name*：ロード プロファイル名を指定して、SMF サービス プロファイルを関連付けます。*icmpv6profile_name* は英数字の文字列である必要があります。



第 23 章

# MBR 短回線の最適化


- 機能の概要と変更履歴 （1011 ページ）
- 機能説明 （1012 ページ）
- 機能の仕組み （1012 ページ）
- 制限事項 （1013 ページ）
- MBR 短回線最適化のサポート （1013 ページ）


## 機能の概要と変更履歴

### 要約データ

| | |
|---|---|
| 該当製品または機能エリア | SMF |
| 該当プラットフォーム | SMI |
| 機能のデフォルト設定 | 有効：常時オン |
| このリリースでの関連する変更点 | N/A |
| 関連資料 | 該当なし |

### 更新履歴

**表 *334* : マニュアルの変更履歴**

| 改訂の詳細 | リリース |
|---|---|
| 導入リリース | 2021.02.x |

# 機能説明

gtpc-ep ポッドでのベアラー応答の変更メッセージの生成は、MBR 短絡と呼ばれます。SMF は、gtpc-ep ポッドでベアラー応答の変更メッセージを生成して、smf-service ポッドでの成功原因を持つベアラー応答の変更メッセージを送信するベアラー要求の変更の影響を制限するようになりました。ベアラー応答の変更メッセージは、gtpc-ep ポッドで生成されます。

# 機能の仕組み

**重要** GTPv2 CEP を使用した CEPS 最適化は、システム モードのシャットダウンと再起動でのみ機能します。システムの不整合につながる可能性があるため、ローリング ソフトウェア アップデートでこれを使用することは推奨されません。

### キャッシュ

udp-proxy ポッドで、キャッシュが維持されます。このキャッシュには、ネットワーク内の他のノードとの対話に GTP プロトコルを必要とするセッションに対応するエントリが含まれています。各キャッシュ エントリは、SMF によって対応するセッションに割り当てられた TEID にマッピングされます。キャッシュ エントリには、詳細なリモート セッション TEID、EBI、SMF によって割り当てられた TEID、および最後のシーケンス番号が含まれます。

キャッシュに追加できるキャッシュ エントリの数には制限があります。制限は、約 100 万キャッシュ エントリです。古い（1 時間使用されないキャッシュ エントリ）キャッシュ エントリはキャッシュから定期的に削除されます。

### 短絡

着信 UDP パケットを受信すると、SMF はメッセージが要求メッセージかどうかを識別します。キャッシュを検索して、対応するキャッシュ エントリがあるかどうかを確認します。

キャッシュ エントリが存在し、要求が MBR であり、それが短絡している場合、MBR 応答は完全な処理なしで生成されます。

MBR の短絡の条件は次のとおりです。

- サービング ネットワーク IE のみで構成される MBR
- サービス ネットワーク IE と EBI のみを使用するベアラー コンテキストで構成される MBR
- HO（ハンドオーバー）ビットセット以外を含むサービング ネットワーク IE とインジケーション IE で構成される MBR

# 制限事項

MBR 短回線機能には、次の制限があります。

- Wi-Fi セッションの場合、SMF はキャッシュ エントリを作成しません。
- 4G から 5G HO の場合、SMF はキャッシュ エントリをクリーンアップできず、古いエントリを残すことができず、エントリはキャッシュエントリのタイムアウト後に自動的に削除されます。
- SMF は、最大 100 万エントリと最大 60 分のキャッシュ エントリ タイムアウトをサポートします。キャッシュ エントリは、アクセス権がない場合は削除されます。

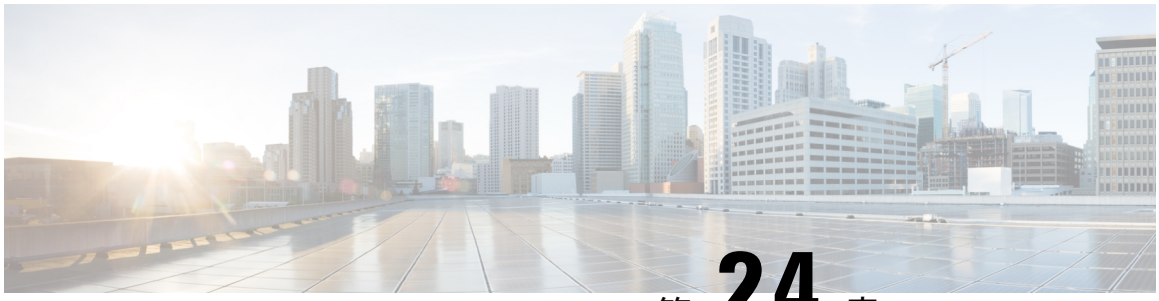
# MBR 短回線最適化のサポート

ここでは、この機能の操作、管理、およびメンテナンスに関して説明します。

## 統計

次の統計情報で MBR 短回線機能がサポートされます。

- gtpc_msg_short_circuit_stats：ショート回線のメッセージの数をキャプチャします。メッセージがスキップされたか、またはショートされたかどうか、およびメッセージがショートされたという条件が表示されます。
- gtpc_short_circuit_map_count：キャッシュ内で追加/削除/更新されたエントリの数をキャプチャします。削除されたエントリと更新エントリの追加エントリを個別に表示します。
- smf_service_gtpc_cache_stats：追加/削除された操作を含む、Smf-Service から送信されたキャッシュエントリの数をキャプチャします。各キャッシュエントリと手順タイプ、メッセージタイプ、操作（追加/削除）を表示します。



第 24 章

# すべての UPF へのメッシュ接続


- 機能の概要と変更履歴 （1015 ページ）
- 機能説明 （1015 ページ）


## 機能の概要と変更履歴

### 要約データ

| | |
|---|---|
| 該当製品または機能エリア | SMF |
| 該当プラットフォーム | SMI |
| 機能のデフォルト設定 | 有効：常時オン |
| このリリースでの関連する変更点 | N/A |
| 関連資料 | 該当なし |

### 更新履歴

**表 *335*：マニュアルの変更履歴**

| 改訂の詳細 | リリース |
|---|---|
| 最初の導入。 | 2021.02.1 |

## 機能説明

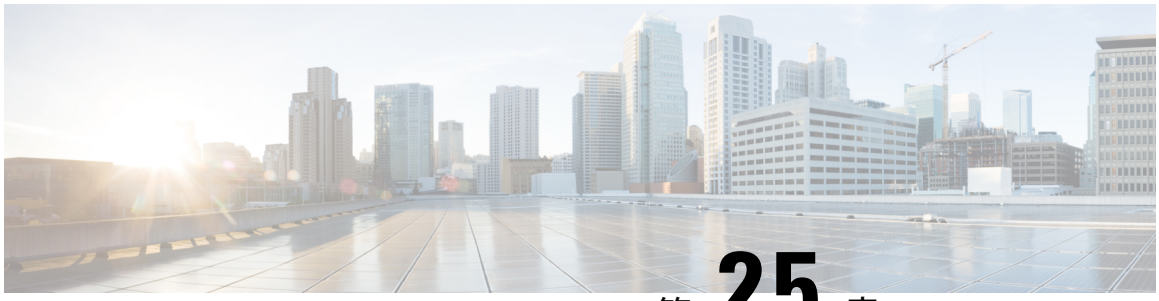
リリース 2021.02.01 では、リージョン内のすべての UPF への SMF メッシュ接続が導入されています。

メッシュ接続により、UPF は特定のリージョン内のすべての SMF に接続できます。ただし、サブスクライバは 1 つの UPF でのみホストされます。リージョン内のすべての UPF は、そのリージョン内のすべての SMF に接続する必要があります。

理想的には、SMF は最大 1024 の UPF に接続できます。UPFは、最大4つのピア(SMF/SGWC/CN-SGW)をサポートできます。

**重要** メッシュ接続のサポートは、SMF の地理的冗長性サポート機能の前提条件です。

詳細については、『UCC 5G SMF 構成およびアドミニストレーション ガイド』の「すべての UPF へのメッシュ接続」の 章を参照してください。



第 25 章

# PCO での MTU サポート


- 機能の概要と変更履歴 （1017 ページ）
- 機能説明 （1018 ページ）
- IPv4 リンク MTU の構成 （1018 ページ）


## 機能の概要と変更履歴

### 要約データ

***Table 336:*** 要約データ

| | |
|---|---|
| 該当製品または機能エリア | SMF |
| 該当プラットフォーム | SMI |
| 機能のデフォルト設定 | 有効：常時オン |
| このリリースでの関連する変更点 | N/A |
| 関連資料 | 該当なし |

### 更新履歴

**表 *337*：マニュアルの変更履歴**

| 改訂の詳細 | リリース |
|---|---|
| 最初の導入。 | 2021.02.0 |

# 機能説明

この機能を使用すると、設定を変更したり、フラグメンテーションの回避やトラフィックのブロックといったタスクを実行するために、最大伝送ユニット（MTU）値をサブスクライバ デバイスに送信できます。UE が要求した場合、構成はプロトコル構成オプション（PCO）IE で MTU をリンクします。CSR に IPv4 リンク MTU を要求する PCO が付属している場合、SMF は、ネットワーク機能ポリシーに基づいて構成されたリンク MTU を含む PCO とともにセッション応答の作成を送信します。N1 PDU セッション確立要求に IPv4 リンク MTU を要求する PCO が含まれている場合、SMF は、ネットワーク機能ポリシーで構成されたリンク MTU を含む PCO を含む N1 PDU セッション確立応答を送信します。

CSR に MTU を要求する PCO、EPCO、または APCO が付属している場合、ネットワーク機能ポリシーがオペレータ ポリシーに関連付けられていると、SMF は CSR 応答で構成済みの IPv4 MTU を送信します。

MTU を要求する PCO を使用して 5G PDU セッション確立要求を受信すると、ネットワーク機能ポリシーがオペレータ ポリシーに関連付けられている場合、SMF は PDU セッション確立承認で構成された IPv4 MTU を送信します。

PGW-C が最初のアタッチ中に拡張プロトコル構成オプション（ePCO）を UE に返すことを決定した場合、UE が要求した PDN 接続手順が開始されます。PGW-C が ePCO をサポートしており、セッション要求作成メッセージで EPCOSI フラグが 1 に設定されている場合、PGW-C は S-GW に ePCO を送信します。S-GW は、ePCO IE を受信すると、それを MME に転送します。

ローミング シナリオでは、vSMF は入力 N1 メッセージをデコードし、N1 メッセージで n1SmInfoFromUE IE を PDU セッション要求の作成または要求の更新を埋めてエンコードします。同様に、hSMF が MTU の要求を含む ePCO を受信し、ポリシーのネットワーク機能がリンク MTU 値で構成されている場合、リンク MTU 値を n1SmInfoToUE IE に送信します。それ以外の場合、hSMF はデフォルトの MTU 値である 1500 を送信します。

ネットワークによって開始されたセッション変更であり、セッションが ePCO を使用して確立された場合、hSMF はセッション要求の更新に ePCO を含めます。

# IPv4 リンク MTU の構成

ここでは、UE に送信される PCO IE に含める MTU を構成する方法について説明します。

IPv4 MTU を構成するには、次の構成例を使用します：

```
config
   policy network-capability network_capability_name
      link-mtu link_mtu_range
      end
```

注：

- **link-mtu** *link_mtu_range* ：UE に要求された場合は、PCO IE にリンク MTU を含めるようにネットワーク機能ポリシーを構成します。

  *link_mtu_range* は、1280 ～ 2000 の範囲の整数で指定する必要があります。デフォルト値は 1500 バイトです。

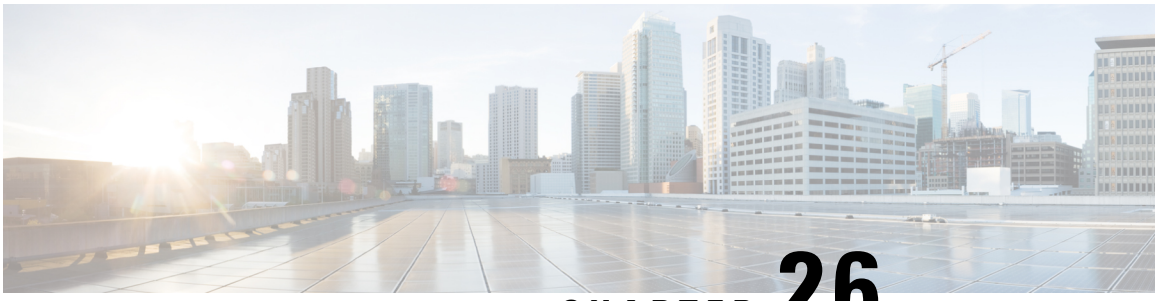
# 設定の確認

構成を確認するには、次の show コマンドを使用します。

**show running-config policy network-capability**

IPv4 MTU が構成されている場合、その値は、次の出力の **link-mtu** 構成の一部として表示されます。

```
[unknown] smf# show running-config policy network-capability
policy network-capability nc1
 link-mtu 1500
 max-supported-pkt-filter 20
 nw-support-local-address-tft true
exit
```



CHAPTER 26

# DNN のサポート


- 機能の概要と変更履歴, on page 1021
- 機能説明, on page 1022
- 機能の仕組み, on page 1023
- 仮想 DNN の構成, on page 1024
- SMF インスタンスに基づくネットワーク機能の選択 （1031 ページ）
- 動的構成更新中に DNN プロファイルをオフライン モードに切り替える （1033 ページ）
- DNN 継承 （1037 ページ）
- DNN ごとの IP プールの割り当て （1042 ページ）
- スライス および DNN ごとの IP プール割り当て （1045 ページ）


## 機能の概要と変更履歴

### 要約データ

***Table 338:*** 要約データ

| | |
|---|---|
| 該当製品または機能エリア | SMF |
| 該当プラットフォーム | SMI |
| 機能のデフォルト設定 | 無効：設定が必要 |
| このリリースでの関連する変更点 | N/A |
| 関連資料 | 該当なし |

# 更新履歴

*Table 339:* マニュアルの変更履歴

| 改訂の詳細 | リリース |
|---|---|
| DNN プロファイルのダイナミック構成変更のサポートが追加されました。 | 2023.03.0 |
| RADIUS サーバからの仮想 DNN をサポートするために、CLI に override キーワードが追加されました。 | 2023.02.0 |
| スライスおよびDNN ごとの IP プール割り当てのサポートが追加されました。 | 2022.04.0 |
| 次に対するサポートが追加されました。<br>• サブスクライバ ポリシー構成の課金特性ルックアップ パラメータ。<br>• 課金特性 ID の範囲値の拡張。 | 2021.02.3.t3 |
| SBI VIP アドレスとサブスクライバの CommonId に基づく IPv6 インターフェイス ID 生成のサポートが追加されました。 | 2021.01.1 |
| SMF では、次の構成に対し最大 2048 がサポートされます。<br>• 優先順位<br>• オペレータ ポリシー<br>• DNN ポリシー<br>• DNN プロファイル | 2021.01.0 |
| SMF は、大文字と小文字を区別しない DNN 構成をサポートします。 | 2020.02.5.t1 |
| 最初の導入。 | 2020.02.0 より前 |

# 機能説明

**Important** この章で使用されている PGW-C という用語は、SMF でサポートされている EPS インターワーキング機能を意味しており、LTE ネットワークで使用されるスタンドアロン P-GW として想定してはなりません。

マルチ DNN のサポートにより、SMF はエンドユーザーに複数の PDN 接続を提供し、インターネットや VoNR サービスなどのさまざまなサービスを提供できます。

SMF は、AMF から PDU セッション確立要求で、ローカルに構成されたプロファイル ベースのデータ ネットワーク名（DNN）を取得します。次に、SMF は SUPI と PDU セッション ID を使用して PDN 接続を維持します。SMF は、受信した DNN をすべての SBI インターフェイスに含めて、エンドユーザーがサブスクリプション情報、ポリシー、および課金関連情報を取得することを許可します。SMF は、転送パス情報を UPF にプロビジョニングします。SMF はマルチ DNN サポートを IP アドレス管理（IPAM）モジュールと統合し、受信した DNN に基づいてエンド ユーザーにアドレスを割り当てます。SMF は、サブスクライバ ポリシーから取得した DNN プロファイルをマッピングします。また、SMF は、IPAM プール構成に基づいて DNN および IPv4 および IPv6 パス情報を取得し、ノード アソシエーションの相互作用の一部として UPF を更新します。

**Note** 複数のDNNは5GSの手順でのみサポートされており、SBIインターフェイスを使用したEPSセッションには適していません。

SMF は、サブスクライバ プロファイルに基づく仮想 DNN（vDNN）マッピングをサポートします。UE要求のDNNから構成済みのDNNへのマッピングをサポートし、選択したDNNプロファイルを構成済みのネットワーク インターフェイスに送信します。

5G サブスクライバの場合、SMF では、スライスベースの vDNN 選択により、より多くの vDNN を使用できます。ただし、5G サブスクライバが 4G アクセス ネットワークから接続する場合、SMF が UDM から UE サブスクリプション データを取得するまでスライス情報は使用できません。このようなシナリオでは、SMF は CC ルックアップ パラメータに基づいて最初の vDNN 選択を実行します。サブスクリプション データが取得された後、SMF はスライス ID 情報に基づいて vDNN を再選択し、新しい vDNN プロファイルを使用します。このアプローチは、Wi-Fi 通話でも同じです。

SMF は、課金特性を使用するか、CLI 構成をスライスすることで、柔軟な vDNN の選択を可能にします。構成の一部の詳細については、「サブスクライバ ポリシーの構成, on page 1025」セクションを参照してください。

**Note** DNN プロファイルはオペレータ ポリシーの下にあるため、vDNN プロファイルの再選択は、オペレータ ポリシーの再選択も意味します。SMF は、再選択がオペレータ ポリシーの他のパラメータに関連付けられている既存の機能に影響を与えないように、構成をサポートします。

# 機能の仕組み

PGW-C での DNN プロファイルのルックアップは、サブスクライバ ポリシーまたは DNN ポリシーに基づいています。SMF プロファイル構成でこれらのポリシーを関連付けることができま

す。両方の構成が利用可能な場合、サブスクライバ ポリシーは DNN ポリシーよりも高い優先順位を持ちます。

サブスクライバ ポリシーは、優先順位の値のリストで構成されます。優先順位の選択は、さまざまな値に基づきます。たとえば、サブスクライバの SUPI、GPSI、サービス提供 PLMN、NSSAI、課金特性、IMSI などです。各優先順位には関連付けられたオペレータ ポリシーがあり、DNN ポリシーは選択したオペレータ ポリシーから選択されます。

DNN ポリシーには、UE が要求した DNN ごとに DNN プロファイルを設定できます。DNN プロファイルには、インターフェイスのリストを含む仮想 DNN またはマッピング DNN があります。

仮想 DNN の選択順序は次のとおりです。

- サブスクライバ ポリシーに基づいて、選択の順序は次のとおりです。smf-profile > smf-service > subscriber-policy > precedence > operator-policy > dnn-policy > dnn-profile（UE 要求の DNN に基づく） > 仮想 DNN マッピング。
- DNN ポリシーに基づいて、選択の順序は次のとおりです。smf-profile > dnn-policy > dnn-profile（UE 要求の DNN に基づく） > Virtual DNN マッピング。

PCF、CHF、UDM、UPF、および Resource Manager（RMGR）は、仮想 DNN マッピングでサポートされているインターフェイスです。

仮想 DNN マッピングが構成されていない場合、UE 要求の DNN がすべてのインターフェイスで使用されます。

## 制限事項

この機能には、次の制限があります：

- SMF は、NFR への登録時に、最初に構成された DNN プロファイルを NFProfile の「dnnSmfInfoList」に含めます。

# 仮想 DNN の構成

ここでは、仮想 DNN 機能の構成方法について説明します。

仮想 DNN 機能の構成には、次の手順が含まれます：

1. サブスクライバ ポリシーの構成, on page 1025
2. オペレータ ポリシーの構成と DNN ポリシーの関連付け, on page 1027
3. DNN ポリシーの構成, on page 1027
4. DNN プロファイルでの 仮想 DNNの構成, on page 1028
5. SMF サービスでのサブスクライバ ポリシーの関連付け, on page 1030

# サブスクライバ ポリシーの構成

サブスクライバポリシーを構成するには、次の構成例を使用します：

```
config
   policy subscriber subscriber_policy_name
      precedence precedence_value
         cc-start-range cc_start_range_value
         cc-stop-range cc_stop_range_value
         gpsi-start-range gpsi_start_range_value
         gpsi-stop-range gpsi_stop_range_value
         imsi { mcc mcc_value | mnc mnc_value | msin  msin_value }
         imsi-start-range imsi_start_value
         imsi-stop-range imsi_stop_value
         operator-policy operator_policy_name
         pei-start-range pei_start_range_value
         pei-stop-range pei_stop_range_value
         sdt sdt_value
        serving-plmn { mcc mcc_value | mnc mnc_value | mnc-list  mnc_list_value
}
         serving-plmn  serving_plmn_value
         sst sst_value
         supi-start-range supi_start_range_value
         supi-stop-range supi_stop_range_value
         instance-start-range start_range_value
         instance-stop-range stop_range_value
         end
```

注：

- **precedence** *precedence_value*：サブスクライバ ポリシーに関連付けられた優先順位の値を指定します。

  precedence の最大制限は 2048 です。

- **cc-start-range** *cc_start_range_value*：サブスクライバ ポリシーに関連付けられた課金特性開始範囲の値を指定します。 *cc_start_range_value* は 、0x1 から 0xffff の範囲の 1 ー 4 桁の 16 進文字列である必要があります。たとえば、0001 とします。

- **cc-stop-range** *cc_stop_range_value*：サブスクライバポリシーに関連付けられた課金特性の終了範囲の値を指定します。 *cc_stop_range_value* は 、0x1 ー 0xffff の範囲の 1 ー 4 桁の 16 進文字列である必要があります。たとえば、12AB です。

- **gpsi-start-range** *gpsi_start_range_value*：サブスクライバ ポリシーに関連付ける GPSI 開始範囲の値を指定します。 *gpsi_start_range_value* は 、1000000000 ～ 999999999999999 の範囲の整数である必要があります。

- **gpsi-stop-range** *gpsi_stop_range_value*：サブスクライバ ポリシーに関連付ける GPSI 停止範囲の値を指定します。 *gpsi_stop_range_value* は 、1000000000 ～ 999999999999999 の範囲の整数である必要があります。

- **imsi { mcc** *mcc_valuemnc_value* **| mnc** *msin_value* **| msin** ：**}**サブスクライバ ポリシーに関連付けられる MCC、MNC、または MSIN 値を提供して、IMSI 値を指定します。
- **imsi-start-range** *imsi_start_value*：IMSI 開始範囲の値を指定します。 *imsi_start_value* は 、1000000000 ～ 999999999999999 の範囲の整数である必要があります。
- **imsi-stop-range** *imsi_stop_value*：IMSI 停止範囲値を指定します。 *imsi_stop_value* は 、1000000000 ～ 999999999999999 の範囲の整数である必要があります。
- **operator-policy** *operator_policy_name*：サブスクライバ ポリシーに関連付けるオペレータ ポリシーを指定します。

  オペレータ ポリシーの最大制限は 2048 です。
- **pei-start-range** *pei_start_range_value*：PEI 開始範囲の値を指定します。 *pe_start_range_value* は 、1000000000 ～ 999999999999999 の範囲の整数である必要があります。
- **pei-stop-range** *pei_stop_range_value*：PEI 停止範囲の値を指定します。 *pey_stop_range_value* は 、1000000000 ～ 999999999999999 の範囲の整数である必要があります。
- **sdt** *sdt_value*：サブスクライバ ポリシーに関連付ける SDT 値を指定します。 *sdt_value* は [0-9a-fA-F](6) - 000000 - ffffff 形式の 6 桁のオクテット文字列である必要があります。たとえば、1A2B3c です。
- **serving-plmn { mcc** *mcc_valuemnc_valuemnc_list_values* **mnc** ： **mnc-list** *3***}** 桁のモバイル国コード（MCC）、2 桁または 3 桁のモバイル ネットワーク コード（MNC）、またはサービスを提供している PLMN の MNC 値のリストを指定します。 *mcc_value* と *mnc_value* は文字列である必要があります。 *mnc_list_values* は 、[580 660] などの文字列である必要があります。
- **sst** *ssst_value*：スライス/サービス タイプ（SST）値を指定します。 *sst_value* は 、[0-9a-fA-F](2) - 00 ～ FF 形式の 2 桁のオクテット文字列である必要があります。たとえば、A8 です。
- **supi-start-range** *supi_start_range_value*：SUPI 開始範囲の値を指定します。 *supi_start_range_value* は 、1000000000 から 999999999999999 までの範囲の整数である必要があります。
- **supi-stop-range** *supi_stop_range_value*：SUPI 停止範囲の値を指定します。 *supi_stop_range_value* は 、1000000000 から 999999999999999 までの範囲の整数である必要があります。
- **instance-start-range** *start_range_value*：SMF インスタンスの開始範囲の値を指定します。 *start_range_value* は 、1 ～ 8 の範囲の整数である必要があります。
- **instance-stop-range** *stop_range_value*：SMF インスタンスの停止範囲の値を指定します。 *stop_range_value* は 、1 ～ 8 の範囲の整数である必要があります。

## 設定の確認

ポリシー関連の構成の詳細を確認するには、次のコマンドのいずれかを使用します：

ポリシー構成モード内の **show subscriber policy** *policy_name* または **show full**

次は、表示コマンドの出力例です：

サブスクライバポリシーの構成に課金特性パラメータが含まれている場合、この値は次の出力で **cc-start-range** と **cc-stop-range** の一部として表示されます。

```
smf(config-subscriber-polSub)# show full
policy smf polSmf
precedence 1
  sst              22
  sdt              232322
  serving-plmn mcc 210
  serving-plmn mnc 90
  supi-start-range 100000000000001
  supi-stop-range  100000000000010
  gpsi-start-range 1000000000
  gpsi-stop-range  9999999999
  cc-start-range 0001
  cc-stop-range 0005
  operator-policy  opPol1
!
!
```

# オペレータ ポリシーの構成と DNN ポリシーの関連付け

オペレータ ポリシーを構成するには、以下の構成例を使用します：

```
config
   policy operator operator_policy_name
      policy dnn dnn_policy_name [ [ secondary secondary_dnn_policy_name ] [
network-capability network_capability ] ]
      end
```

注：

- **policy dnn** *dnn_policy_name* **[ [ secondary** *secondary_dnn_policy_name* **] [ network-capability** *network_capability***] ]**：オペレータ ポリシーに関連付ける primary DNN ポリシーのパラメータを指定します。 *dnn_policy_name* は 文字列である必要があります。
  - **secondary** *secondary_dnn_policy_name*：オペレータ ポリシーに関連付ける DNN ポリシーのパラメータがプライマリ ポリシーと一致しない場合は、フォールバック用のセカンダリ DNN ポリシーを指定します。*secondary_dnn_policy_name* は文字列である必要があります。
  - **network-capability** *network_capability*：選択したそれぞれのオペレータ ポリシーのネットワーク機能構成の詳細を指定します。*network_capability* 値は文字列である必要があります。

# DNN ポリシーの構成

DNN ポリシーを構成するには、次の構成を使用します。

```
config
   policy dnn dnn_policy_name
      dnn dnn_name profile dnn_profile_name dnn-list dnn_list
   exit
exit
```

注：

- **policy dnn** *dnn_policy_name*：DNN 名を指定します。*dnn_policy_name* 英数字の文字列である必要があります。

  DNN ポリシーの最大制限は 2048 です。

- **dnn** *dnn_name*：指定したネットワーク DNN プロファイルにマッピングする仮想 DNN プロファイルを指定します。 *dnn_name* は 英数字の文字列である必要があります。

  DNN 構成は、1 ～ 62 文字の英数字文字列を受け入れます（大文字と小文字は区別されません）。ドット（.）やダッシュ（-）を含めることもできます。

- **profile** *profile_name*：ネットワーク DNN プロファイルを指定します。 *profile_name* は 英数字の文字列である必要があります。

  DNN プロファイルの最大制限が 512 から 2048 に引き上げられました。

- **dnn-list** *dnn_list*：UPF ノードでサポートされている DNN リストを指定します。

# DNN プロファイルでの 仮想 DNNの構成

SMF は、すべてのノースバウンドインターフェイスで仮想 DNN 値を送信できる柔軟性を提供します。各インターフェイスで送信する仮想 DNN は、次のように構成できます。リソース マネージャ（RMGR）仮想 DNN は、IP プールを DNN にマッピングするために使用されます。

DNN プロファイルで仮想 DNN を構成するには、次の構成例を使用します。

```
config
   profile dnn profile_name
     dnn dnn_name network-function-list [ chf | ocs | pcf | pcrf | radius
 | upf | cgf ]
   profile profile_name
   end
```

注：

- **dnn** *dnn_name*：DNN 名を指定します。 *dnn_name* は 英数字の文字列である必要があります。

- **network-function-list**：ネットワーク機能を指定します。DNN プロファイルはこれらのネットワーク機能にアクセスします。**CHF, OCS, PCF, PCRF, RADIUS, UPF, and CGF.** の値をサポートしています。

### オーバーライド コマンドの構成

上記の CLI に加えて、SMF には、RADIUS サーバから受信した vDNN でアクセス DNN をオーバーライドする機能があります。

RADIUS-ep は、Starent VSA 属性「SN-Virtual-APN-Name（タイプ：94）」をデコードするようにアップグレードされ、この属性をサポートするようにアプリケーションが拡張されています。

RADIUS サーバはアクセス承認で SMF に vDNN を送信し、SMF は UPF への N4 メッセージにこの DNN を含めます。特定のインターフェイスで送信された DNN を RADIUS サーバから受信した値でオーバーライドするかどうかを決定するために、新しい構成が SMF に追加されます。

Radius サーバから仮想 DNN をサポートするためのオーバーライド キーワードが追加されます。

```
config
   profile dnn profile_name
      dnn override network-function-list [ chf | ocs | pcf | pcrf |
radius | upf | cgf ]
      dnn override rmgr
      end
```

RADIUS インターフェイスで仮想 DNN を受信するために使用される属性の詳細は次のとおりです。

- **SN**: Virtual-APN-Name
- **構文**：Opaque Value
- **長さ**：1-64
- **タイプ**：26
- **ベンダー ID**：8164
- **VSA タイプ**：94
- 上書きキーワードは、ローカルに構成された値よりも優先されます。
- オーバーライド キーワードは存在しますが、RADIUS は vDNN を提供しないため、SMF はローカルに構成された値（存在する場合）または gnDNN を使用します。
- インターフェイスの場合、構成（オーバーライドまたは local-dnn-nameI）がない場合、gnDNN を使用します。

  vDNN のオーバーライドは、UDM ネットワーク機能には適用されません。
- RADIUS サーバから受信した framed-ip は、 RADIUS サーバから受信した vDNN に関連付けられた IP プールの一部である必要があります。不一致の場合、セッションの作成は失敗します。

- ダイナミックおよび静的IP割り当てケースで、同じDNNに対する同じUEに異なるRMGR vDNNを割り当てることができるため、IPはダイナミックまたは静的プールから割り当てることができます。

# SMF サービスでのサブスクライバ ポリシーの関連付け

SMF サービスでサブスクライバ ポリシーを関連付けるには、次の構成例を使用します：

```
config
  profile smf smf_profile_name
    service name service_name
      subscriber-policy subscriber_policy_name
      end
```

注：

- **subscriber-policy** *subscriber_policy_name*：サブスクライバ ポリシー名を指定します。*subscriber_policy_name* は 英数字の文字列である必要があります。

# SMF インスタンスに基づくネットワーク機能の選択

表 *340 :* 機能の履歴

| 機能名 | リリース情報 | 説明 |
|---|---|---|
| SMF インスタンスに基づく UPF の選択 | 2024.01.2 | この機能を使用すると、サブスクライバ ポリシー構成で SMF インスタンスをカスタマイズしたり、サイト間 GR 展開モデルで SMF インスタンスを共存 UPF にバインドしたりできます。<br>ユーザーがオペレータ ポリシーを選択すると、SMF インスタンスがフィルタとして機能し、SMF が特定の DNN プロファイルを選択できるようにします。DNN の選択は、最も近くアクティブなネットワーク機能（UPF など）を見つけるのに役立ち、ユーザー トラフィックを同じ場所にある UPF にのみルーティングできるようになります。これを実装することで、待ち時間が減り、ユーザー エクスペリエンスが向上します。<br>この機能を実装するには、policy subscriber コマンドの下に次のキーワードを追加します。<br>• **instance-start-range**<br>• **instance-stop-range**<br>**デフォルト設定** 無効：有効にするには構成が必要です。 |

**インスタンスベースのネットワーク機能の選択**

## 機能説明

サブスクライバ セッションの作成中に、SMF は、サブスクライバ ポリシー構成モードで構成された SMF インスタンス ID に基づいてオペレータ ポリシーを選択します。SMF は、サブス

クライバごとに、選択されたオペレータ ポリシーをさまざまなDNNプロファイル、仮想DNN、IP プール、および UPF プロファイルに関連付けます。

SMF では、SMF インスタンスに対応する適切な DNN プロファイルを柔軟に選択できます。

たとえば、アクティブ/スタンバイ Geo 冗長性（GR）の展開シナリオで、各ラックが 2 つのリージョン（リージョン 1 とリージョン 2）、2 つのアクティブとスタンバイの SMF インスタンス（SMF インスタンス 1 および SMF インスタンス 2）、IP プール（プール 1 とプール 2）、仮想 DNN（vdnn 1 と vdnn 2）、および 2 つの UPF セット（UPF セット 1（UPF 1 と UPF 3）と UPF セット 2（UPF 2 および UPF 4）の 2 つのラック（ラック 1 とラック 2）があることを想定します。

SMF は、vdnn 1 が SMF インスタンス 1、プール 1、および UPF セット 1 に関連付けられ、vdnn 2 が SMF インスタンス 2、プール 2、および UPF セット 2 に関連付けられるように構成されます。サブスクライバが PDU 接続の確立を試みると、到達したセッションの仮想 IP（VIP）に基づいて SMF インスタンスが選択されます。1 つのリージョンの SMF インスタンス 1 がアクティブで選択されている場合、両方のリージョンで SMF インスタンスが同じ DNN を持っていても、SMF は vdnn1、プール 1、および UPF セット 1 を選択します。

その後、SMF は IP プールをプール 1 から UPF セット 1 の UPF にのみ配布します。SMF インスタンス ID が構成されていない場合、SMF は両方の SMF インスタンスに関連付けられた UPF に使用可能な IP アドレスを割り当てます。

# SMF インスタンスの構成

SMF インスタンスを構成するには、次の構成例を使用します：

（注） 実行時にこの構成を追加することを推奨します。構成変更後の新しいオペレータ ポリシーの選択では、新しい構成が使用されます。

```
config
   policy subscriber subscriber_policy_name
      precedence precedence_value
         instance-start-range start_range_value
         instance-stop-range stop_range_value
         operator-policy operator_policy_name
         end
```

注：

- **precedence** *precedence_value*：サブスクライバ ポリシーに関連付けられた優先順位の値を指定します。

  precedence の最大制限は 2048 です。

- **instance-start-range** *start_range_value*：SMF インスタンスの開始範囲の値を指定します。*start_range_value* は 、1 ～ 8 の範囲の整数である必要があります。

- **instance-stop-range** *stop_range_value*：SMF インスタンスの停止範囲の値を指定します。*stop_range_value* は 、1 ～ 8 の範囲の整数である必要があります。

### 設定例

次に、DNN プロファイル選択用の SMF インスタンスを記述する構成 **show running-config policy subscriber** コマンドの例を示します。

```
 [smf] smf# show running-config policy subscriber
Wed Mar  6  05:09:45.143 UTC+00:00
policy subscriber polSub
 precedence 1
  sst                   02
  sdt                   Abf123
  serving-plmn mcc 123
  serving-plmn mnc 456
  supi-start-range      100000000000001
  supi-stop-range       999999999999999
  gpsi-start-range      100000000000001
  gpsi-stop-range       999999999999999
  instance-start-range 1
  instance-stop-range  1
  operator-policy       opPolHomer
 exit
```

# 動的構成更新中に DNN プロファイルをオフライン モードに切り替える

## 機能説明

この機能により、SMF は DNN をオフライン モードに切り替えて、構成の動的な更新をサポートできます。SMF では、DNN プロファイルがオフライン モードに変更された場合にのみ、一部の DNN プロファイル パラメータの動的な構成の更新ができます。

DNNがオフラインモードの場合、新しいセッションまたは既存のセッションの後続のメッセージは、更新された構成値を使用します。

**重要** 動的変更が許可されていない構成を変更するときに、DNN をオフラインモードに切り替える前に、サブスクライバ セッションをクリアする必要があります。DNN がオンライン モードに戻るまで、新しいセッション要求は拒否されます。

## 機能の仕組み

このセクションでは、この機能がサポートされている SMF 構成に対してどのように機能するのかについて説明します。

# DNN ポリシー

DNNポリシーの構成は、DNN との DNN プロファイルマッピングを定義します。DNN からプロファイルへのマッピングが変更された後、同じ DNN の新しいサブスクライバは、更新された DNN プロファイルを使用します。したがって、既存の回線には影響ありません。

# DNN プロファイル

DNN プロファイルは、特定の DNN 用に様々なパラメータを定義します。

次のテーブルは、ダイナミック構成変更が許可されているかどうかまたは、DNN がオフライン モードに設定される必要があるかどうかを説明します。

**表 *341 : DNN* プロファイル構成と動的更新時の影響**

| 設定パラメータ | ダイナミックな変更 | 既存のセッションへの影響 |
|---|---|---|
| DnsServers | 許可 | 影響なし |
| DnnInfo | 許可 | セッションのデータベースリロード後には、新しい値が使用されます。 |
| NetworkElementProfile | 推奨されていません（注意事項を参照） | |
| タイムアウト（Timeout） | 許可 | 影響なし |
| ChargingProfile | 推奨されていません（注意事項を参照） | |
| RemoteVmac | 許可 | 影響なし |
| PcscfProfile | 許可 | 影響なし |
| PpdProfile | 許可 | 即時（新しい値が使用されます） |
| DefaultSscMode | 許可 | 影響なし |
| DefaultPduSession | 許可 | 影響なし |
| AllowedPduSession | 許可 | 影響なし |
| QosProfile | 許可 | 即時（新しい値が使用されます） |
| UpfApn | 許可 | 影響なし |
| SecondaryAuthen | 許可 | 影響なし |
| LocalAuthorization | 許可 | 影響なし |
| NetworkCapability | 許可 | 影響なし |
| PolicyProfile | 許可 | 影響なし |

注：

- NetworkElementProfile および ChargingProfile の構成パラメータは変更または削除しないことをお勧めします。パラメータが変更されている場合、次の動作に影響があります：
  - NetworkElementProfile：既存セッションのメッセージは、新しいサーバーに送信される場合があります。
  - ChargingProfile：SMF と UPF 間の使用状況レポート ルール（URR）に関連する不整合がある場合があります。
- DNN プロファイル マッピングを変更するには、DNN プロファイルは、オフライン モードである必要があります。
- CLI コマンドを実行する前に、ヘルプ文字列に表示されるメッセージを確認することが推奨されています。
- パラメータを動的に構成するときに DNN プロファイルをオフライン モードにスイッチします。このステップは、構成変更によってネットワーク影響を回避します。

## サブスクライバ ポリシー

SMF は、サブスクライバポリシーを使用して、次のオプションに基づいてオペレータポリシーを選択します：

- SUPI 範囲
- SST（スライス/サービス タイプ）
- IMSI 範囲
- GPSI
- PEI
- SDT（スライス差別化要因）
- S_NSSAI
- PLMN ID
- CC（課金特性）範囲
- SMF インスタンス範囲

サブスクライバポリシー構成の変更は、既存のセッションには影響しないため、ダイナミックに適用できます。SMF は、更新された構成に基づいて、新しいセッションのオペレータ ポリシーを選択します。

## 制限事項

DNN がオフライン モードの場合、次の制限が適用されます：

- オフライン DNN の後続の 5G コールは、HTTP の原因（HTTP_STATUS_CODE_503_SERVICE_UNABLE）で拒否され、5GSMCause として「サービス オプションが一時的に無効になっています」と表示されます。
- オフライン DNN の後続の 4G コールは、GTP の原因「リソースがありません」で拒否されます。

# オフライン DNN プロファイルを構成

このセクションでは、DNN プロファイルのオフライン モードを有効にする方法について説明します。

## DNNプロファイルをオフライン モードに切り替える

DNN プロファイルをオフライン モードに変更するには、次の構成例を使用します。

```
config
  profile dnn dnn_profile_name
    mode dnn_mode
    end
```

注：

- **profile dnn** *dnn_profile_name*：DNN プロファイルを指定します。
- **mode** *dnn_mode*：動作の DNN モードを指定します。DNN モードが **offline** に構成されると、新しいセッションは拒否されます。デフォルト値は **online** です。

## DNN プロファイルのオフライン モード構成の確認

このセクションでは、DNN プロファイルがオフライン モードに設定されているかどうかを確認する方法について説明します。

次に、 **show running-config profile dnn** *profile_name* コマンドの出力例を示します。

```
show running-config profile dnn intershat
 profile dnn intershat
      mode offline
      network-element-profiles chf chf1
      network-element-profiles amf amf1
      network-element-profiles pcf pcf1
      network-element-profiles udm udm1
      charging-profile chgprf1
      virtual-mac b6:6d:47:47:47:47
      ssc-mode 2 allowed [ 3 ]
      session type IPV4 allowed [ IPV6 IPV4V6 ]
      upf apn intershat
      dcnr true
  exit
```

# DNN プロファイルのオフライン モード設定の OAM サポート

ここでは、この機能の操作、管理、およびメンテナンスに関して説明します。

## バルク統計サポート

この機能の一部として、次のラベルが導入されています：

- LABEL_DISC_PDUSETUP_DNN_OFFLINE：このラベルは、DNN がオフライン モードであるためにコールが拒否されることを示すために定義されます。

# DNN 継承

## 機能説明

**表 *342 :* 機能の履歴**

| 機能名 | リリース情報 | 説明 |
|---|---|---|
| レガシー インターフェイスでの 4G セッションの DNN 継承 | 2024.02.0 | レガシー インターフェイスを持つ SMF は、DNN 継承機能をサポートしています。 |

SMF では、親DNNプロファイルテンプレートで共通の属性を構成し、必要に応じて他のDNNプロファイル（子 DNN プロファイルなど）で再利用できます。この機能により、DNN プロファイル構成が最適化され、運用効率が向上します。

（注） 現在、DNN継承機能はSMF（レガシーインターフェイスを含む）でのみ認定され、cnSGW-Cでは認定されていません。

## 機能の仕組み

このセクションでは、ネットワーク事業者が親 DNN プロファイルを継承または再利用するために DNN プロファイル構成を実行する方法について詳しく説明します。

**表 *343 :* 親 *DNN* プロファイルを構成する準備**

| ステップ | 説明 |
|---|---|
| 1 | 共通の属性を持つ親DNNプロファイルを構成します。 |

| ステップ | 説明 |
| --- | --- |
| 2 | 構成された親 DNN プロファイルを子 DNN プロファイルに継承します。<br>次の条件が適用されます。<br>• 子プロファイルが存在しない DNN プロファイルを継承しようとすると、変更のコミット中に SMF CLI にエラーが表示されます。<br>• 親 DNN プロファイルが削除されていても子プロファイルで見つかった場合、変更のコミット中に SMF CLI にエラーが表示されます。<br>（注）<br>親 DNN プロファイルを削除するには、子 DNN プロファイルから親プロファイルのリンク解除を行います。<br>• 子 DNN プロファイルで構成された属性が親 DNN プロファイルに属していない場合、オペレータは個々の子 DNN プロファイルでそれらの属性を変更できます。 |

| ステップ | 説明 |
| --- | --- |
| 3 | |

| ステップ | 説明 |
| --- | --- |
| | SMF が子 DNN プロファイルの要求を受信します。子 DNN プロファイルに 継承 属性がある場合、SMF は次の条件に基づいて継承/親プロファイルを解決します。<br>• 親プロファイルが見つかり、子プロファイルが親属性をオーバーライドしていない場合、SMF は継承した属性で子プロファイルを更新します。<br>• 親プロファイルが見つかり、子プロファイルが親属性の一部またはすべてを上書きする場合、SMF は親プロファイルよりも上書きされた属性を優先し、子プロファイルから上書きされた属性を取得し、残りの属性を親プロファイルから取得して子プロファイルを更新します。<br>• 親プロファイルに配列またはスライスの形式の属性があり、子プロファイルにも同じ属性が設定されている場合、結果として得られる DNN プロファイルは、子プロファイルからその属性を完全にオーバーライドします。つまり、結合されたプロファイルには子プロファイルの値が含まれます。属性のみを一覧表示します。<br>**DNNプロファイルの例**：<br>`profile dnn intershat_Parent // parent dnn profile`<br>`ims mark qci [ 83 128 ]`<br>`network-element-profiles chf chf1`<br>`network-element-profiles amf amf1`<br>`network-element-profiles pcf pcf1`<br>`network-element-profiles udm udm1`<br>`charging-profile chgprfFBC`<br>`override [ charging-profile charging-characteristics-id ]`<br>`virtual-mac b6:6d:47:47:47:47`<br>`session type IPV4 allowed [ IPV6 IPV4V6 ]`<br>`dcnr true`<br>`exit`<br>`profile dnn intershatRoamer // child dnn profile`<br>`inherit intershat_Parent`<br>`override [ charging-characteristics-id charging-qbc-profile ]`<br>`exit`<br>**結果のプロファイルの例**：<br>`profile dnn intershatRoamer // Resultant dnn profile`<br>`ims mark qci [ 83 128 ]`<br>`network-element-profiles chf chf1`<br>`network-element-profiles amf amf1`<br>`network-element-profiles pcf pcf1`<br>`network-element-profiles udm udm1`<br>`charging-profile chgprfFBC`<br>`override [charging-characteristics-id charging-qbc-profile ]`<br>`virtual-mac b6:6d:47:47:47:47`<br>`session type IPV4 allowed [ IPV6 IPV4V6 ]`<br>`dcnr true`<br>`exit`<br>• 親プロファイルに構造体の形式の属性があり、子プロファイルにも同じ属性が構成されている場合、結果として得られる DNN プロファイルは、その属性を子か |

| ステップ | 説明 |
|---|---|
| | ら完全にオーバーライドします。つまり、結合されたプロファイルには子属性の値が含まれます。<br>**DNNプロファイルの例：**<br>`profile dnn intershat_Parent // parent dnn profile`<br>`charging-profile chgprfFBC`<br>`virtual-mac b6:6d:47:47:47:47`<br>`dcnr true`<br>`network-element-profiles chf chf1`<br>`network-element-profiles amf amf1`<br>`network-element-profiles udm udm1`<br>`exit`<br>`profile dnn intershatRoamer // child dnn profile`<br>`inherit intershat_Parent`<br>`network-element-profiles pcf pcf1`<br>`exit`<br>**結果のプロファイルの例：**<br>`profile dnn intershatRoamer // Resultant dnn profile`<br>`charging-profile chgprfFBC`<br>`virtual-mac b6:6d:47:47:47:47`<br>`dcnr true`<br>`network-element-profiles pcf pcf1`<br>`exit`<br>（注）<br>SMF が子 DNN プロファイルの要求を受信し、子 DNN プロファイルに継承属性がない場合、SMF は子 DNN プロファイルからすべての属性を返します。 |
| 4 | 実行時に親と子の DNN プロファイルを更新します。変更がコミットされると、SMF は子と親のプロファイルから最新の属性を選択します。 |

# DNN継承の構成

個別のDNNプロファイルですべての共通属性を定義し、CLI構成を使用して、この親プロファイルを他の DNN プロファイルで使用できます。

共通の属性を持つ親 DNN プロファイルを継承するには、次の設定例を使用します。

```
config
  profile dnn dnn_profile_name
    inherit dnn_template_name
     dnn rmgr  ims_pool_ipv6
    end
```

注：

- **inherit** *dnn_template_name*：子プロファイルに継承する親 DNN プロファイルの名前を指定します。

### 設定例

親 DNN プロファイルから属性を継承し、子プロファイルで使用する構成の例を以下に示します。

```
// Parent DNN profile
profile dnn dnnprof-ims.epdg.prod
  dns primary ipv4 10.177.0.34
  dns primary ipv6 fd00:976a::9
  dns secondary ipv4 10.177.0.210
  dns secondary ipv6 fd00:976a::10
  network-element-profiles chf nfprf-chf1
  network-element-profiles amf nfprf-amf1
  network-element-profiles pcf nfprf-pcf1
  network-element-profiles udm nfprf-udm1
  dnn ims.epdg.prod network-function-list [ chf pcf udm upf ]
  timeout up-idle 3600 cp-idle 7320
  charging-profile           chgprof-1
  pcscf-profile              pcscf1
  ppd-profile                ppd-prof1
  ssc-mode 1 allowed [ 2 ]
  session type IPV6
  session skip-ind false
  upf apn ims.epdg.prod
  qos-profile                5qi-to-dscp-mapping-table-IMS
  always-on                  true
  dcnr                       true
  userplane-inactivity-timer 3600
  only-nr-capable-ue         false
exit

// Child DNN profile
profile dnn dnnprof-ims.prod
  inherit dnnprof-ims.epdg.prod
  dnn rmgr ims-pool-ipv6
exit
```

# DNN ごとの IP プールの割り当て

## 機能説明

IPプール割り当て機能は、IPプールの選択のために、UEが要求したDNNから構成済みのDNNへのマッピングをサポートします。この機能は、5Gおよび4GのSMFおよびPGW-Cでサポートされています。

SMF は次の機能をサポートしています。

- DNN プロファイルでの構成をサポートして、UE 要求の DNN から IP プールに関連付けられている DNN へのマッピングを有効にします。

- マップされた DNN をリモート プロシージャ コール（gRPC）を介してノード マネージャ サービスのリソース マネージャ機能に送信して、IP 割り当てを行います。
- 冗長マネージャを使用した仮想 DNN を介した IP プール DNN の構成をサポートします（利用可能な場合）。
- IP プールの構成と仮想 DNN の両方が利用できない場合に、UE 要求の DNN を送信します。

# 機能の仕組み

このセクションは、IP プール割り当て機能の仕組みの概要を提供します。

- DNN プロファイルのルックアップは、サブスクライバ ポリシーまたは DNN ポリシーに基づいています。DNN プロファイルは、SMF プロファイル構成で関連付けられます。両方の構成が存在する場合、サブスクライバ ポリシーは DNN ポリシーよりも優先されます。
- サブスクライバポリシーには、precedence 値のリストが含まれています。優先順位の選択は、サブスクライバの SUPI、GPSI、サービング PLMN、および NSSAI の値に基づいて行われます。
- 各優先順位には、オペレータ ポリシーが関連付けられます。DNNポリシーは、選択したオペレータポリシーから選択されます。
- DNN ポリシーには、UE が要求した DNN ごとに DNN プロファイルを設定できます。
- DNN プロファイルには、仮想またはマッピングされた DNN とインターフェイスのリストが含まれています。これは既存の設定であり、Redundancy Manager もインターフェイスのリストにあります。詳細については、DNN プロファイルでの 仮想 DNNの構成（1028 ページ）を参照してください。
- DNNプロファイルの下の設定には、UE要求されたDNNからIPプールDNNへのマッピングが含まれています。
- DNN プロファイルの選択は、次の順序で行われます。
  - サブスクライバ ポリシーに基づいて、選択の順番は、次のとおりです：smf-profile > smf-service > subscriber-policy > 優先順位 > operator-policy > dnn-policy > dnn-profile（UE-requested DNN に基づく）> 仮想 DNN マッピング。
  - DNN ポリシーに基づいて、選択の順序は次のとおりです：sf-profile > dnn-policy > dnn-profile（UE が要求した Dnn に基づく） > 仮想 DNN マッピング。

（注）

- 冗長マネージャの構成が存在する場合、IP プール DNN マッピングは既存の仮想 DNN 構成よりも優先されます。
- 冗長性管理の両方の構成が存在しない場合は、UE 要求の DNN を使用して IP プールが選択されます。
- マップされた DNN で IP プールが構成されていない場合、IP の割り当ては失敗し、コールは削除されます。
- EPS コールと 5G コールの両方が、DNN の IP 割り当てに関する同じ原則に従います。

# IP プールの割り当ての構成

ここでは、IP プール割り当て機能の構成方法について説明します。

IP プール割り当てを構成するには、次のいずれかの手順を実行します。

1. DNN プロファイルでの 仮想 DNN の構成詳細については、DNN プロファイルでの 仮想 DNNの構成, on page 1028を参照してください。

**Note** これは、オプションとしての他のインターフェイスと同様の汎用構成です。

2. DNN ごとの IP プールの割り当て

**Note** この構成は IP 割り当て専用です。

## DNN ごとの IP プールの割り当て

DNN ごとに IP プールを割り当てるには、次の構成例を使用します：

```
config
  profile dnn dnn_profile_name
    dnn rmgr rmgr_name
    end
```

注：

- **profile dnn** *dnn_profile_name*：仮想 DNN プロファイルを指定したネットワーク DNN プロファイルにマッピングします。 *dnn_profile_name* は 英数字の文字列である必要があります。
- **dnn rmgr** *rmgr_name*：DNN プロファイルの送信先となる冗長マネージャを指定します。 *rmgr_name* は 英数字の文字列である必要があります。

## IP プール割り当ての構成の確認

この項では、IP プールの割り当て構成を確認する方法について説明します。

DNN プロファイル構成モードで **show full** CLI コマンドを使用して、DNN ごとに IP プールの割り当てに関連する構成を確認します。

以下は、この show コマンドの出力例です。

```
[unknown] smf(config-dnn-cisco123)# show full
profile dnn intershat
dns primary ipv4 209.165.200.231
dns primary ipv6 2001:DB8:1::1
dns secondary ipv4 209.165.200.232
dns secondary ipv6 2001:DB8:1::2
network-element-profile-list chf [ chgser1 ]
dnn starent.com network-function-list [ upf chf rmgr ]
dnn rmgr cisco.com
charging-profile chgprf1
virtual-mac      01-00-5E-90-10-00
pcscf-profile    pcscf1
ppd-profile      ppd1
ssc-mode 1
session type IPV4
.
.
.
```

# スライス および DNN ごとの IP プール割り当て

## 機能説明

SMF は、同じ DNN を使用したスライスごとの IP プールの割り当てをサポートします。スライスは、ダイナミックに作成される論理的なエンドツーエンドネットワークです。ユーザー機器（UE）は、同じ無線インターフェイスなど、1 つのアクセス ネットワークを介して複数のスライスにアクセスできます。

SMF は次のタスクを実行します。

- スライス ID に基づいて、すべての外部 NF を登録、検出、サブスクライブして、トラフィックを送信します。
- スライスベースの手順とセッション統計を提供します。
- EDR に関するスライス情報を入力します。
- ログに関するスライス情報を提供します。
- SMF でサポートされるスライスの最大数を 512 に制限します。

# 機能の仕組み

SMF は、スタティック構成または NRF ベースのダイナミック選択を通じて、PCF、CHF、UDM、AMF などの NF を選択します。これらの両方のオプションで、メッセージングにはそれらのインターフェイスで使用されるスライス情報が含まれます。

SMF は次のタスクを実行します。

- スライスを NRF に登録します。
- N11 および N10 インターフェイスでスライス情報を受信します。
- ピア NF 検出と UPF の選択にスライスを使用します。
- N7 および N40 インターフェイスでスライス情報を送信します。

## 制限事項

スライスおよび DNN 機能ごとの IP プール割り当てには、次の制限があります：

- 手順とセッション統計にのみスライス情報があります。その他の統計は NF レベルにあります。
- スライス情報に基づくロギングの有効化または無効化はサポートされていません。

# 機能設定

このセクションでは、スライスおよび DNN ごとに IP プールの割り当てを構成する方法について説明します。

この機能の構成には、次の手順が含まれます。

1. タグを構成します。詳細は、「SMF タグの構成 （908 ページ）」を参照してください。
2. 次のタスクを使用して、スライスでのダイナミック ノード選択を実行します。
   - NRF を登録します。詳細については、「NRF の登録」を参照してください。
   - 許可された NSSAI 値を構成します。詳細については、「許可される NSSAI 値の構成」を参照してください。
   - NRF を検出します。詳細については、「NRF の検出」を参照してください。
3. 手順とセッション統計のスライス情報に、smf_service_stats メトリックの NSSAI ラベルを構成します。詳細については、「メトリック収集の設定 （2097 ページ）」を参照してください。

## 許可 NSSAI 値の構成

スライスに対して許可される NSSAI 値を構成するには、次の構成例を使用します：

```
config
   profile smf smf_profile_name
      instances instance_id
         allowed-nssai allowed_nssai_values
         end
```

注：

- **allowed-nssai** *allowed_nsai_values* ：スライシングの許可 NSSAI の 1 つまたは複数の値を指定します。

## スライスベースの IP プール割り当ての構成

スライスに基づいたプール割り当てを構成するには、次のサンプル構成を使用します。

```
config
nssai name nssai_name
    sst sst_value
    sdt sdt_value
    dnn dnn_name_value
    pool-selection pool_selection_value
    end
```

注：

- **pool-selection** *pool_selection_value* ：IP プールの選択方法を DNN または NSSAI に構成します。デフォルトのプール選択方法は DNN です。プールの選択方法がスライスまたはスライス DNN のみの場合、スライスと DNN に基づいて IP プールが選択されます。

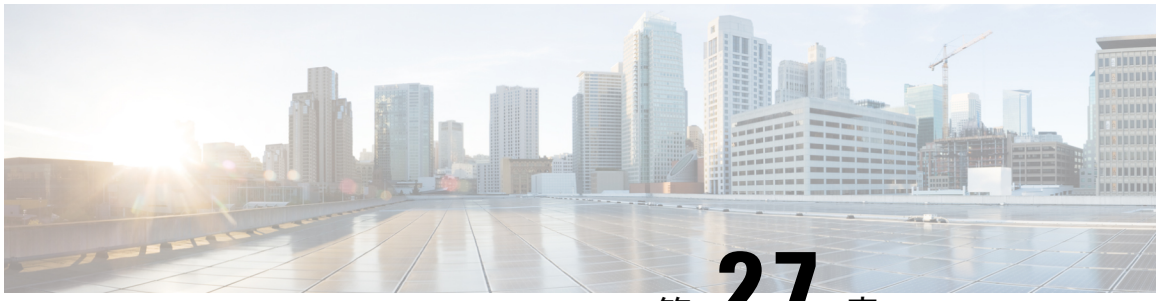
（注）

- スライスのプール選択方法を NSAI として構成する場合、その UPF のすべての DNN の IPAM 構成で、「slice1」と「dnn」を値として構成する必要があります。
- IPAM では、タグ「nsai」は文字列であり、SMF スライスの構成名と一致する必要があります。

### 設定例

次に、スライス ベースのプール割り当ての構成例を示します。

```
nssai name slice1
 sst 02
 sdt  Abf123
 pool-selection [ dnn nssai ]
exit
```



第 27 章

# 複数 PLMN のサポート


- 機能の概要と変更履歴 （1049 ページ）
- 機能説明 （1050 ページ）
- 機能の仕組み （1050 ページ）
- 複数の PLMN の構成 （1051 ページ）
- 複数の PLMN の OAM サポート （1054 ページ）


## 機能の概要と変更履歴

### 要約データ

表 *344* : 要約データ

| | |
|---|---|
| 該当製品または機能エリア | SMF |
| 該当プラットフォーム | SMI |
| 機能のデフォルト設定 | 無効：設定が必要 |
| このリリースでの関連する変更点 | N/A |
| 関連資料 | 該当なし |

### 更新履歴

表 *345* : マニュアルの変更履歴

| 改訂の詳細 | リリース |
|---|---|
| 非標準 PLMN リストの構成を追加しました。 | 2023.04.0 |

| 改訂の詳細 | リリース |
|---|---|
| オペレータ ポリシーの構成から **visitor-hrt** CLI キーワードを削除しました。 | 2021.02.3 |
| 最初の導入。 | 2021.01.0 |

# 機能説明

マルチ PLMN 機能は、ホーマー ネットワークとローマー ネットワークの複数の PLMN をサポートします。最大 32 の PLMN を構成できます。

SMFは、プロファイル DNN で構成されたプライマリ PLMN をピア検出に使用します。この機能は、さまざまなセッション タイプ構成のホーマー ネットワークとローマー ネットワークをサポートします。IPv6 セッション タイプ構成のホーマーと、IPv4 または IPv6 セッション タイプ構成のローマーは一般的な構成です。

この機能は、SIM (非認証IMSI) および SIM なしのローマー UE からの 4G および 5G RAT からの緊急通話をサポートします。IMSI を使用しない緊急通話の場合、プライマリ PLMN が構成されていない場合（PLMN ID がなく、プロファイル DNN にプライマリ PLMN がない場合）、PLMN リストの PLMN の 1 つが外部メッセージ用のプライマリ PLMN として使用されます。

SMF は、SmContextCreate または CreateSessionRequest メッセージを受信して UE PLMN を検証し、外部メッセージングに PLMN を入力します。

ローミング機能の詳細については、「ローミングのサポート （1643 ページ）」の章を参照してください。

# 機能の仕組み

PLMN リストの下に構成されたオペレータ PLMN には、すべての UE PLMN およびサービス提供 PLMN が含まれます。

4G または 5G RAT から要求の作成（SmContextCreate またはセッション要求の作成」）を受信すると、SMF は SUPI から UE PLMN を抽出します。SMF は、UE PLMN およびサービス PLMN を構成済みの PLMN リストと比較し、外部メッセージングに PLMN を入力します。SMF は、HPLMN 値に基づいて加入者のローミング状態を決定します。

UE PLMN とサービング PLMN の両方が、SMF に構成された PLMN リストに属している場合、その PLMN はホーム サブスクライバです。UE の PLMN が構成された PLMN リストに属しておらず、サービス提供 PLMN が構成された PLMN リストに属している場合、その UE はビジター状態です。UE の PLMN が構成された PLMN リストに属しており、サービス提供 PLMN が構成された PLMN リストに属していない場合、その UE はローミング状態です。

# 複数の PLMN の構成

このセクションでは、マルチ PLMN 機能を構成する方法について説明します。

## 構成ベースのピア NF の選択

ここでは、ピアネットワーク機能を選択するための NRF 検出またはローカル構成の使用を設定する方法について説明します。

プロファイルのネットワーク要素での構成により、ユーザーはサブスクライバポリシーに異なる選択ロジックを使用できます。たとえば、ユーザーはホーム、ローミング、またはビジター用にピア NF の選択ロジックを構成できます。

NF 検出の構成を選択するには、次の構成例を使用します：

```
config
  profile network-element amf amf_profile_name
    discovery local
    end
```

注：

- **discovery local**：NF 検出にローカル構成を使用するように指定します。

## PLMN ID の構成

このセクションでは、PLMN ID を構成する方法について説明します。

1 つまたは複数の PLMN ID を構成するには、次の構成例を使用します：

```
config
  profile smf smf_profile_name
    plmn-id mcc mcc_value mnc mnc_value
   plmn-list { mcc mcc_value mnc mnc_value | range mcc mcc_value mnc mnc_value
}
    end
```

注：

- **plmn-id mcc** *mcc_value* **mnc** *mnc_value*：PLMN ID の 3 桁のモバイル国コード（MCC）と 2 桁または 3 桁のモバイル ネットワーク コード（MNC）を指定します。 *mcc_value* と *mnc_value* は 文字列である必要があります。
- **plmn-list { mcc** *mcc_valuemnc_valuemcc_valuemnc_value* **mnc** ： **mnc** 複数 **| range mcc** の **}**PLMN の 3 桁のモバイル国コード（MCC）と 2 桁または 3 桁のモバイル ネットワーク コード（MNC）のリストを指定します。 *mcc_value* と *mnc_value* は 文字列である必要があります。

（注）
- 最大 32 の PLMN を構成できます。
- すべてのオペレータ PLMN は、すべての UE-PLMN とサービス PLMN を含む PLMN リストの下で構成されます。

# 非標準 PLMN リストの構成

この項では、非標準 PLMN リストを構成する方法について説明します。

1 つまたは複数の非標準 PLMN リストを構成るには、次の構成例を使用します：

```
config
  profile smf smf_profile_name
     non-standard-plmn-list mcc mcc_value mnc mnc_value
     end
```

注：

- **non-standard-plmn-list mcc** *mcc_value* **mnc** *mnc_value* ：UE PLMN ID を取得するためにサポートされている非標準 PLMN のリストを指定します。 *mcc_value* と *mnc_value* は整数である必要があります。

## 非標準 PLMN リストの確認

この項では、非標準 PLMN リスト機能構成を確認する方法について説明します。

構成されている非標準の PLMN のリストを表示するには、次の show コマンドを使用します。

**show running-config profile smf plmn-list**

以下は、この show コマンドの出力例です。

```
[smf] smf# show running-config profile smf smf1 non-standard-plmn-list
   profile smf smf1
       non-standard-plmn-list mcc 200 mnc 111
       exit
       non-standard-plmn-list mcc 100 mnc 100
       exit
exit
```

# プライマリ PLMN の構成

このセクションでは、DNN プロファイルの下のプライマリ PLMN の構成方法を説明します。

ピア検出用にプライマリPLMNを構成するには、次の構成例を使用します。

```
config
  profile dnn dnn_profile_name
     primary-plmn mcc mcc_value mnc mnc_value
     exit
```

注：

- **primary-plmn mcc** *mcc_value* **mnc** *mnc_value*：プライマリ PLMN の 3 桁のモバイル国コード（MCC）と 2 桁または 3 桁のモバイル ネットワーク コード（MNC）を指定します。*mcc_value* と *mnc_value* は 文字列である必要があります。

# NRF 検出での PLMN の構成

このセクションでは、NRF 検出での PLMN を構成する方法について説明します。

PLMN クエリ パラメータを構成するには、次の構成例を使用します：

```
config
  profile network-element pcf pcf_profile_name
    query-target-plmn { primary | serving | ue }
    exit
```

注：

- **query-target-plmn { primary | serving | ue }**：NRF 検出で使用するクエリ パラメータ target-plmn を指定します。次のいずれかを指定できます。
  - **primary**: ターゲット PLMN で送信されるプライマリ PLMN を構成します。
  - **serving**：ターゲット PLMN で送信されるサービング PLMN を構成します。
  - **ue**: ターゲット PLMN で送信される UE PLMN を構成します。

# サービング PLMN MNC リストの構成

このセクションでは、PLMN を提供する MNC リストを構成する方法について説明します。

サービス提供 PLMN 情報を構成するには、次の構成を使用します。

```
config
  policy subscriber policy_name
    precedence precedence_value
    serving-plmn { mcc mcc_value | mnc mnc_value | mnc-list mnc_list_values
}
    exit
```

注：

- **serving-plmn { mcc** *mcc_value* **| mnc** *mnc_value* **| mnc-list** *mnc_list_values* **}**：3 桁のモバイル国コード（MCC）、2 桁または 3 桁のモバイル ネットワーク コード（MNC）、またはサービスを提供している PLMN の MNC 値のリストを指定します。*mcc_value* and *mnc_value* は文字列である必要があります。

  *mnc_list_values* は 文字列である必要があります。例：[580 660]

- この構成は、バックワードと互換性はありません。 **mnc** と **mnc-list** の両方が構成されている場合、オペレータ ポリシーの選択時に両方が考慮されます。

# オペレータ ポリシーのローマを構成

ここでは、オペレータ ポリシーのローマ ネットワークの構成方法について説明します。

オペレータ ポリシー固有のローミング構成を構成するには、次の構成例を使用します：

```
config
  policy operator operator_policy_name
    roaming-status { roamer | visitor-lbo }
    exit
```

注：

- **roaming-status { roamer | visitor-lbo }**：ローミング ステータスを指定します。次のいずれかを指定できます。
  - **roamer**：ホーム ネットワークのローマのステータスを指定します。
  - **visitor-lbo**：ローカル ブレークアウト セッションでのローマのステータスを指定します。
- ローミング ステータスが設定されていない場合、SMF は PLMN と SUPI の値を使用してサブスクライバのローミング ステータスを判断します。

# 複数の PLMN の OAM サポート

ここでは、この機能の操作、管理、およびメンテナンス サポートについて説明します。

## バルク統計サポート

複数の PLMN 機能をサポートするために、次の統計情報が更新されています。

- smf_service_stats：この統計には、サブスクライバ セッションのローミング ステータスを示す roaming_status ラベルが含まれます。
- smf_service_counters：この統計には、サブスクライバセッションのローミング ステータスを示す roaming_status ラベルが含まれます。
- smf_session_counters：この統計には、サブスクライバセッションのローミング ステータスを示す roaming_status ラベルが含まれます。
- smf_session_stats：この統計には、サブスクライバ セッションのローミング ステータスを示す roaming_status ラベルが含まれます。

第 28 章

# 非 3GPP アクセスのための N3IWF

表 *346* : 機能の履歴

| 機能名 | リリース情報 | 説明 |
|---|---|---|
| 信頼できない非 3GPP アクセス ネットワークの N3IWF | 2024.01 | SMF は、5G コアと信頼できない非 3GPP ネットワーク間のインターワーキングのために N3IWF インターフェイスをサポートします。<br><br>N3IWF は、ユーザーが異なるネットワーク タイプに移行するときに、シームレスなハンドオーバーと中断のない接続を促進します。<br><br>**デフォルト設定**：無効：構成が必要 |


- 機能説明 （1056 ページ）
- N3IWF の UE アイドル モード エントリ （1058 ページ）
- 機能の仕組み （1059 ページ）
- N3GA ロケーション パラメータ （1080 ページ）
- アクティブなベアラー機能を使用した N3IWF および HO サポートを使用した Wi-Fi 経由の音声またはビデオ通話 （1082 ページ）
- N3IWF セッションの RAT タイプの処理 （1082 ページ）
- 標準準拠 （1082 ページ）
- OAM サポート （1083 ページ）

# 機能説明

表 *347 :* 機能の履歴

| 機能名 | リリース情報 | 説明 |
|---|---|---|
| N3IWF の機能強化：ネットワーク開始型サービス リクエスト、PLMN 間ハンドオーバー、およびコアに依存しないロケーション パラメータ | 2024.04.1 | 次に、Wi-Fi ネットワークとセルラー ネットワーク間でシームレスな通信を実現するための N3IWF の追加の機能拡張を示します。<br>• N3IWF を通してネットワークによって開始されたサービス要求<br>• PLMN Wi-FiからNRへのハンドオーバー<br>• PLMN NR から Wi-Fi へのハンドオーバー間<br>• Wi-Fi（N3IWF）から進化したユニバーサル地上波無線アクセス（EUTRA）HO<br>• EUTRA から Wi-Fi（N3IWF）HO へ<br>• 次世代コアに依存しない（N3GA）ロケーション パラメータ |

| 機能名 | リリース情報 | 説明 |
| --- | --- | --- |
| N3IWF の機能強化：サービス要求、ハンドオーバー手順、アイドル モード管理、および音声/ビデオ通話サポート | 2024.03.0 | 次に、Wi-Fi ネットワークとセルラー ネットワーク間でシームレスな通信を実現するための N3IWF の追加の機能拡張を示します。<br>• N3IWF を介して UE が開始したサービス要求<br>• N3IWF を介した NR ハンド オーバー（HO）への Wi-Fi<br>• NR から N3IWF Wi-Fi HO へ<br>• アイドル モードの開始と終了の手順を UE が開始しました。<br>• アクティブ ベアラーを使用した N3IWF および HO サポートを使用した Wi-Fi 経由の音声またはビデオ通話、SMF は、ハンドオーバー中の Evolved Packet System（EPS）フォールバックもサポートしています。<br>• N3IWF セッションの RAT タイプの処理 |

5G SBA（サービス ベース アーキテクチャ）の非 3GPP インターワーキング機能（N3IWF）は、信頼できない非 3GPP ネットワークと 5G コア間のインターワーキングを担当します。したがって、N3IWF は、デバイスへの IPSec 接続をサポートしながら、コアへの N2 ベースの接続と N3 ベースの接続の両方をサポートします。N3IWF は、N2 および N3 インターフェイスを有効にすることにより、非 3GPP Wi-Fi ネットワークから 5G コア ネットワークとシームレスにインターフェイスするためのアクセスおよび認証プロトコルを提供します。

このインターフェイスは、レイヤ 2 アクセス レベル（WPA2）で実装されているセキュリティ対策に関係なく、ユーザー機器（UE）と N3IWF との間のエンドツーエンド セキュリティ アソシエーションを確立します。

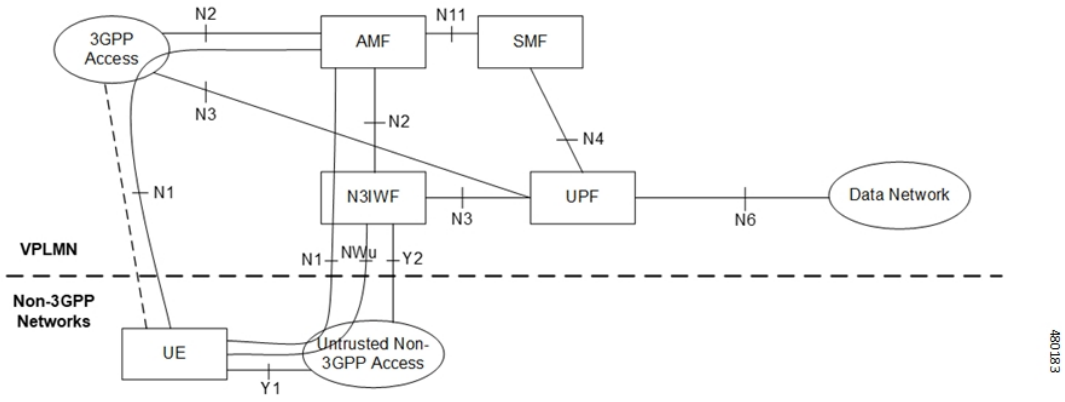
SMF では、次の手順がサポートされています：

- N3IWF を介した PDU セッションの確立

- N3IWF を介した PDU セッションのリリース
- N3IWF を通して UE によって開始されたサービス要求
- N3IWF を介した NR HO への内部 PLMN Wi-Fi
- 内部 PLMN NR から N3IWF Wi-Fi HO へ
- N3IWF を通してネットワークによって開始されたサービス要求
- PLMN Wi-FiからNRへのハンドオーバー
- PLMN NR から Wi-Fi へのハンドオーバー間
- Wi-Fi（N3IWF）から進化したユニバーサル地上波無線アクセス（EUTRA）HO
- EUTRA から Wi-Fi（N3IWF）HO へ
- 次世代コアに依存しない（N3GA）ロケーション パラメータ

## アーキテクチャ

次の図は、信頼できない非 3GPP アクセス ネットワークを使用した 5G コアネットワークの非ローミング アーキテクチャを表しています。




# N3IWF の UE アイドル モード エントリ

SMF は、UP 接続を非アクティブ化するための UE/アクセスが開始したアイドルモード開始手順をサポートしています。UP 接続の非アクティブ化には、CM-CONNECTED 状態の UE の確立された PDU セッションのデータ無線ベアラーと N3 トンネルが含まれます。

（注） 5G PDU IM の開始手順中に、UE と N3IWF 間の IPSEC 接続が解放されます。これにより、SMF での今後のページングの試行が失敗する可能性があります。

### アイドル モード時のサービス要求処理

次に、UE がアイドル モードの場合の 2 種類のサービス要求を示します。

- **UEが開始したサービス要求**:

  アイドル モードの UE は、3GPP アクセスを介した信頼できない非 3GPP アクセスによるサービス要求手順を使用します。このサービス要求は、NAS シグナリング接続の再確立、および非 3GPP アクセスに関連付けられたすべてまたは一部の PDU セッション用のユーザー プレーンの再確立のためのものです。

  接続モードの UE は、3GPP アクセスを介した信頼できない非 3GPP アクセスによるサービス要求手順を使用します。このサービス要求は、非 3GPP アクセスに関連付けられている 1 つ以上の PDU セッションのユーザー プレーンを再確立するためのものです。

  非 3GPP アクセスで CM-IDLE 状態になっている UE は、UE トリガーのサービス要求手順を使用して既存の PDU セッションの UP 接続を再アクティブ化し、既存の PDU セッションの UP 接続を個別にアクティブにすることもできます。

- **ネットワークによって開始されたサービス要求**:

  SMF は、UE と N3IWF 間の接続が解放されたアイドル状態の N3IWF セッションに対してページング信号を送信します。このような場合、N2 セットアップ要求が失敗することがあります。

# 機能の仕組み

N3IWF は、サービス プロバイダのインフラストラクチャ内のネットワーク機能として展開されます。アクセス モビリティ管理機能（AMF）、セッション管理機能（SMF）、ユーザー プレーン機能（UPF）など、5G ネットワーク アーキテクチャのさまざまなコンポーネントと相互作用します。

# コール フロー

ここでは、N3IWF に関連するコール フローについて説明します。

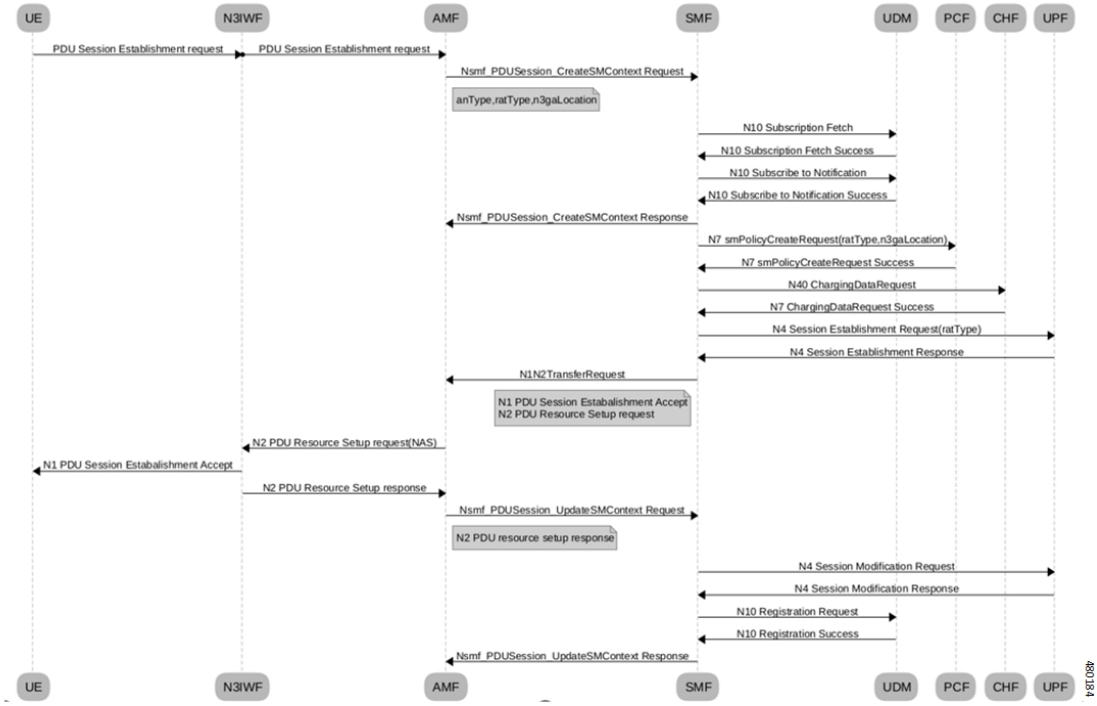
### N3IWF を介した PDU セッションの確立

UE は N3IWF を使用して 5G コア ネットワークで初期登録と認証を実行します。N3IWF を介した 5G PDU セッションの作成は、5G PDU 作成要求メッセージに以下の追加属性が含まれることを除いて、5G NR PDU の作成と同じです。

- ratType
- anType
- n3gaLocation

（注）
- N3IWF を介した 5G PDU セッションの作成では、EBI 割り当てを実行する必要はありません。
- N3GPP TAI 情報を伝送する n3gaLocation 属性は 3GPP-User-Location-Info AVP に含まれ、anType 属性が Non-3GPP Access の場合は RADIUS サーバーに送信されます。
- N3GaLocation 情報は PCF と CHF とのみ共有されます。

次のコール フローでは、N3IWF を介した PDU 確立の開始について説明します。




### N3IWF を介した PDU セッションのリリース

N3IWF を介した PDU セッションの解放手順は、次の 5G NR PDU セッションの解放手順と同じです。

- トリガーされたリリースへのアクセス
- ネットワーク トリガー リリース
  - PCF 開始
  - 管理者が開始
  - CHF のトリガー
  - IDLE タイムアウトベース

• N4 パス障害によるリリース

### N3IWF を介して UE が開始したサービス要求

SMF は、N3IWF を介して接続された Wi-Fi セッションの PDU アイドル モードの参加/終了手順を処理するようになりました。

**図 *187 : N3IWF* を介して *UE* が開始したサービス要求**

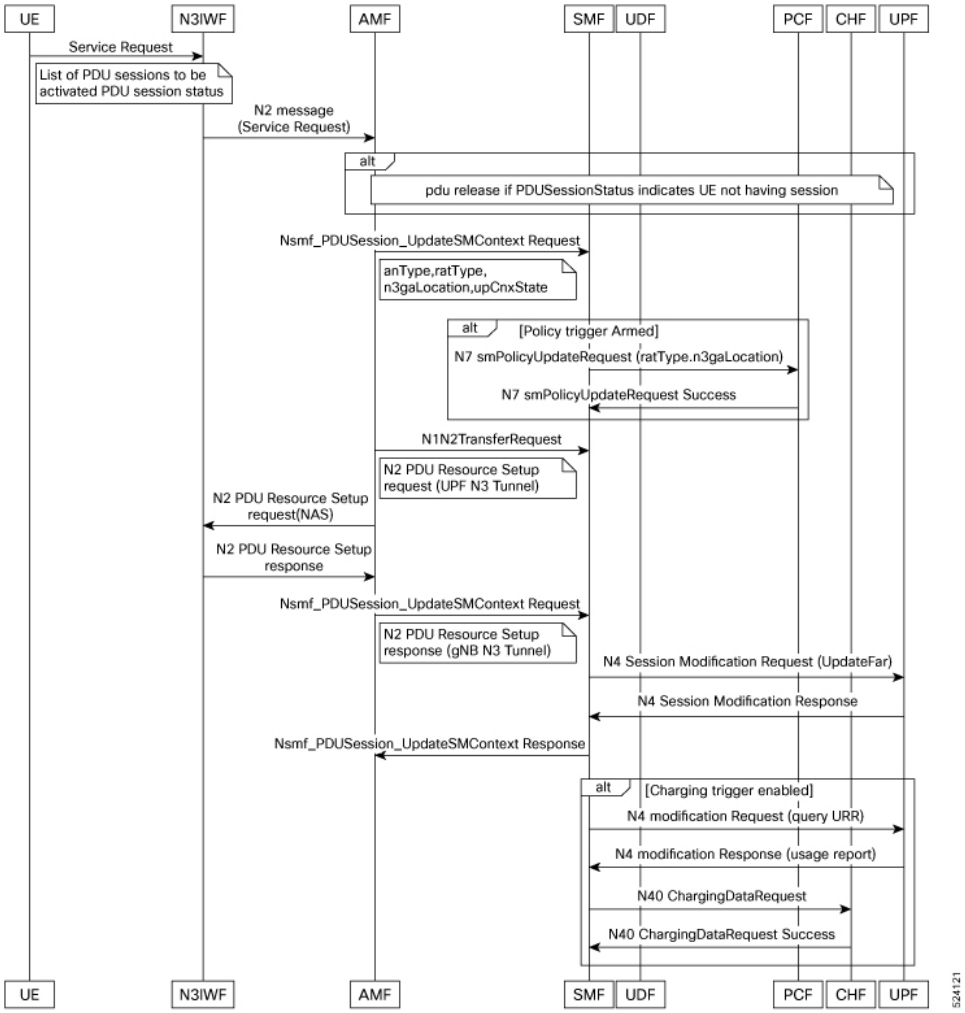



**表 *348 : N3IWF* コール フローの説明を介して *UE* が開始したサービス要求**

| ステップ | 説明 |
|---|---|
| 1 | UE は、アクティブにされる PDU セッションのリストと現在の PDU セッション ステータスとともに N3IWF にサービス要求を送信します。 |
| 2 | N3IWF は、N2 メッセージ サービス要求を AMF に転送します。 |

| ステップ | 説明 |
|---|---|
| 3 | AMF は、anType、ratType、n3gaLocation、upCnxState などのパラメータを含む Nsmf_PDUSession_UpdateSMContextRequest を SMF（セッション管理機能）に送信します。 |
| 4 | SMF は、PDUSessionStatus が UE にアクティブなセッションがないことを示しているかどうかを確認します。その場合、セッションの解放がトリガーされます。 |
| 5 | 必要に応じて、SMF は、ratType と n3gaLocation を使用して N7 SmPolicyUpdateRequest を PCF に送信します。 |
| 6 | PCF は成功の N7 SmPolicyUpdateResponse で応答します。 |
| 7 | SMF が N1N2TransferRequest を AMF に送信します。 |
| 8 | AMF は N1N2TransferRequest を N3IWF に転送します。 |
| 9 | N3IWF は、AMF への N2 PDU 技術情報セットアップ応答で応答します。 |
| 10 | AMF は、N3IWF に N2 PDU 技術情報セットアップ応答で応答します。 |
| 11 | AMF は、別の Nsmf_PDUSession_UpdateSMContextRequest を SMF に送信し、UPF N3 トンネルのセットアップを示します。 |
| 12 | SMF は、転送アクション ルールを更新するために、N4 セッション変更要求を UPF に送信します。 |
| 13 | UPF は、N4 セッション変更応答で応答します。 |
| 14 | SMF は Nsmf_PDUSession_UpdateSMContextResponse を AMF に送信します。 |
| 15 | 課金トリガーが有効になっている場合、SMF は N4 変更要求を UPF に送信し、使用状況レポート ルール（URR）を照会します。 |
| 16 | UPF は、使用状況レポートを含む N4 変更応答で応答します。 |
| 17 | SMF は CHF に N40 ChargingDataRequest を送信します。 |
| 18 | CHF は正常な N40 ChargingDataRequest で応答します。 |

### N3IWF を介した NR HO への Wi-Fi

次のコール フローでは、同じ AMF または同じ PLMN 内の古い AMF と新しい AMF に対する NR HO へのイントラ PLMN Wi-Fi について説明します。このコール フロー図は、5G ネットワークでの Wi-Fi（N3IWF 経由）から新無線（NR）カバレッジへのセッション移行に関連する一連の手順を示しています。

図 *188 : N3IWF* を介した *NR HO* への *Wi-Fi*

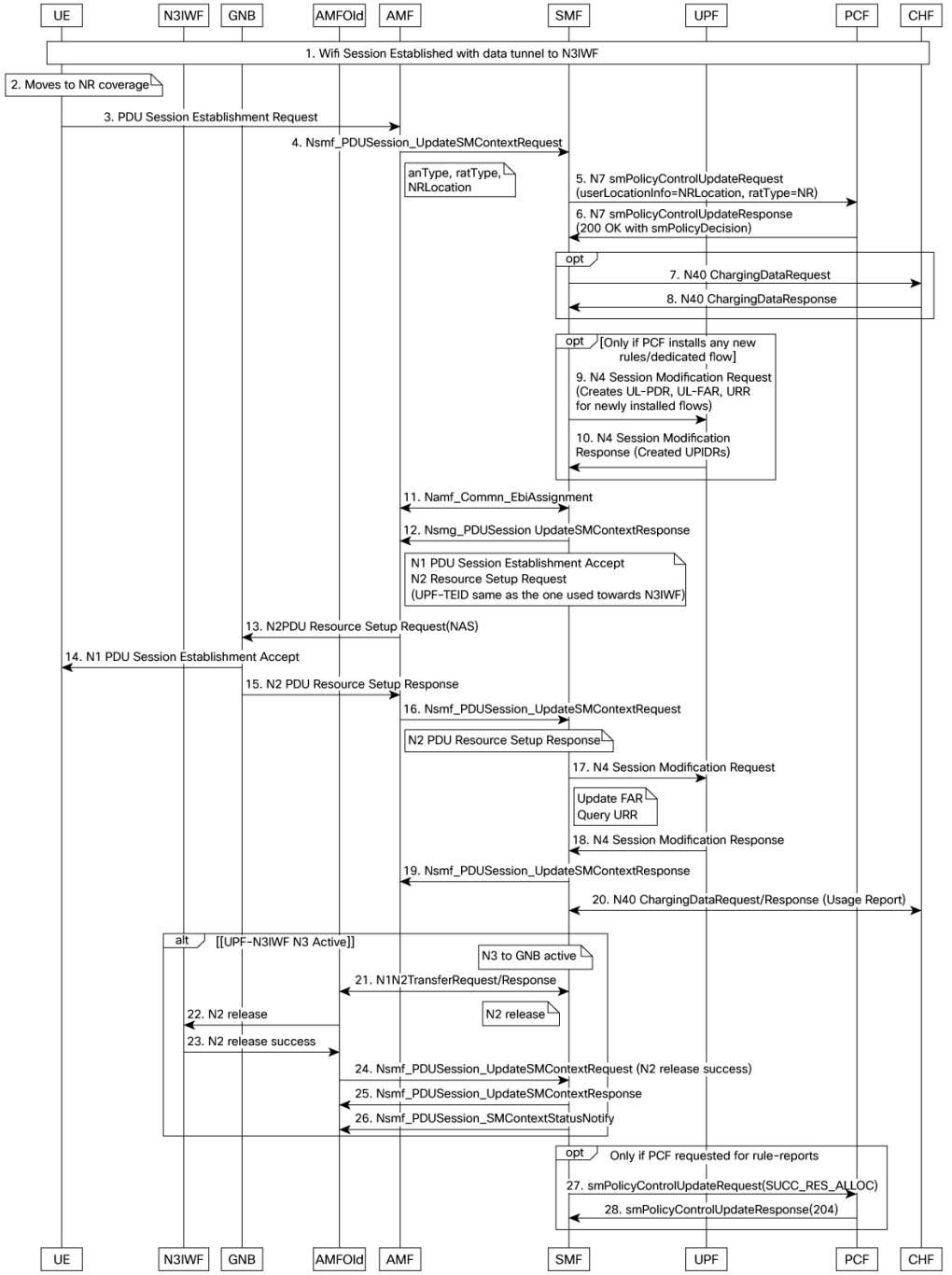



表 *349 : Wi-Fi* から *NR HO* への *N3IWF* コール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | N3IWF にトンネリングされたデータを使用して Wi-Fi セッションが確立されます。 |

| ステップ | 説明 |
|---|---|
| 2 | UE が NR カバレッジ エリアに移動します。 |
| 3 | UE は、Existing-PDU-Session を使用して PDU セッション確立要求を AMF に送信します。 |
| 4 | AMF は、Type=3GPP-ACCESS、ratType=NR、NR Location などのパラメータを使用して Nsmf_PDUSession_UpdateSMContextRequest を SMF に送信します。 |
| 5 | SMF は、userLocationInfo=NRLocation、ratType = NR を含む情報 SmPolicyContextData を使用して、N7 smPolicyControlUpdateRequest を PCF に送信します。 |
| 6 | PCF は 200 OK および SmPolicyDecision（ある場合）で応答します。 |
| 7 | オプションで、SMF はステップ 6 で PCF から受信した情報に基づいて N40 ChargingDataRequest を送信します。 |
| 8 | N40 ChargingDataRequest が送信されると、CHF は N40 ChargingDataResponse で応答します。 |
| 9 | ステップ 6 で、PCF が新しいルールのインストールを試行すると、SMF はフロー作成のために UPF に対して N4SessionModificationRequest を送信します（新しくインストールされたフローの PDR、FAR、URR を作成します）。 |
| 10 | ステップ 9 が送信された場合 UPF は、N4SessionModificationResponse で応答します。 |
| 11 | epsInterworking が有効になっている場合、SMF は EBI を割り当てるために Namef_Commn_EbiAssignmentRequest を開始し、AMF は Namef_Commn_EbiAssignmentResponse に EBI の割り当てられたリストを返します。 |
| 12 | SMF は N1PDUSessionEstablishmentAccept を UE に、N2PDUResourceSetupRequestTransfer を gNB に（UPF-TEID は N3IWF に対して使用されるものと同じ） の両方を伝送する Nsmf_PDUSession_UpdateSMContextResponse を送信します。 |
| 13 | AMF は N2PDUResourceSetupRequestTransfer および NAS PDU（N1PDUSessionEstablishmentAccept）を gNB に転送します。 |
| 14 | gNB は N1PDUSessionEstablishmentAccept を UE に転送します。 |
| 15 | gNB は、TEID を持つ N2PDUResourceSetupTransferResponse で応答します。 |

| ステップ | 説明 |
|---|---|
| 16 | AMF は、N2PDUResourceSetupTransferResponse を持つ SMF に Nsmf_PDUSession_UpdateSMContextRequest を送信します。 |
| 17 | SMF は、Update FAR を使用して N4SessionModificationRequest を送信して転送パラメータと QueryURR を更新し、使用状況レポートがあれば取得します。 |
| 18 | UPF が N4SessionModificationResponse で応答します。UPF と gNB 間のトンネルがアクティブになる。 |
| 19 | SMF は Nsmf_PDUSession_UpdateSMContextResponse で AMF に応答します。 |
| 20 | ステップ 18 で UPF から使用状況レポートを受信した場合、SMF は N40ChargingDataRequest を使用情報とともに CHF に送信し、CHF は N40ChargingDataResponse で応答します。 |
| 21 | 異なる AMF の場合、SMF は N1N2TransferRequest を N2ResourceReleaseTransferRequest で送信元 AMF（古い）に開始し、AMF は N1N2TransferAck で応答します。 |
| 22 | 送信元 AMF は N2ResourceReleaseTransferRequest を N3IWF に転送します。 |
| 23 | N3IWF は N2ResourceReleaseTransferResponse で送信元 AMF に応答します。 |
| 24 | AMF は Nsmf_PDUSession_UpdateSMContextRequest を SMF に送信し、N2Release が成功したことを示します。 |
| 25 | SMF は、送信元 AMF に対する Nsmf_PDUSession_UpdateSMContextResponse で応答します。 |
| 26 | SMF は、Nsmf_PDUSession_SMContextStatusNotify を送信元 AMF に送信して、ハンドオーバーのステータスを示します。この手順は、コンプライアンス プロファイルで 3GPP 23 502 のバージョン仕様が 15.6.0 に設定されている場合にのみ適用されます。 |
| 27 | 手順 6 で成功したインストールのルール レポートを PCF が要求した場合、SMF は N7smPolicyControlUpdateRequest を PCF に送信します。 |
| 28 | ステップ 25 が送信されると、PCF は SMF に N7 smPolicyControlUpdateResponse で応答します。 |

## NR から N3IWF Wi-Fi HO へ

次のコール フローでは、同じ AMF または同じ PLMN 内の古い AMF と新しい AMF に対する Wi-Fi HO に対するイントラ PLMN NR について説明します。コール フロー図は、5G ネットワークで新無線（NR）カバレッジから N3IWF を介した Wi-Fi カバレッジにセッションを移行する際の一連の手順を示しています。

**図 *189 : NR から N3IWF Wi-Fi HO へ***

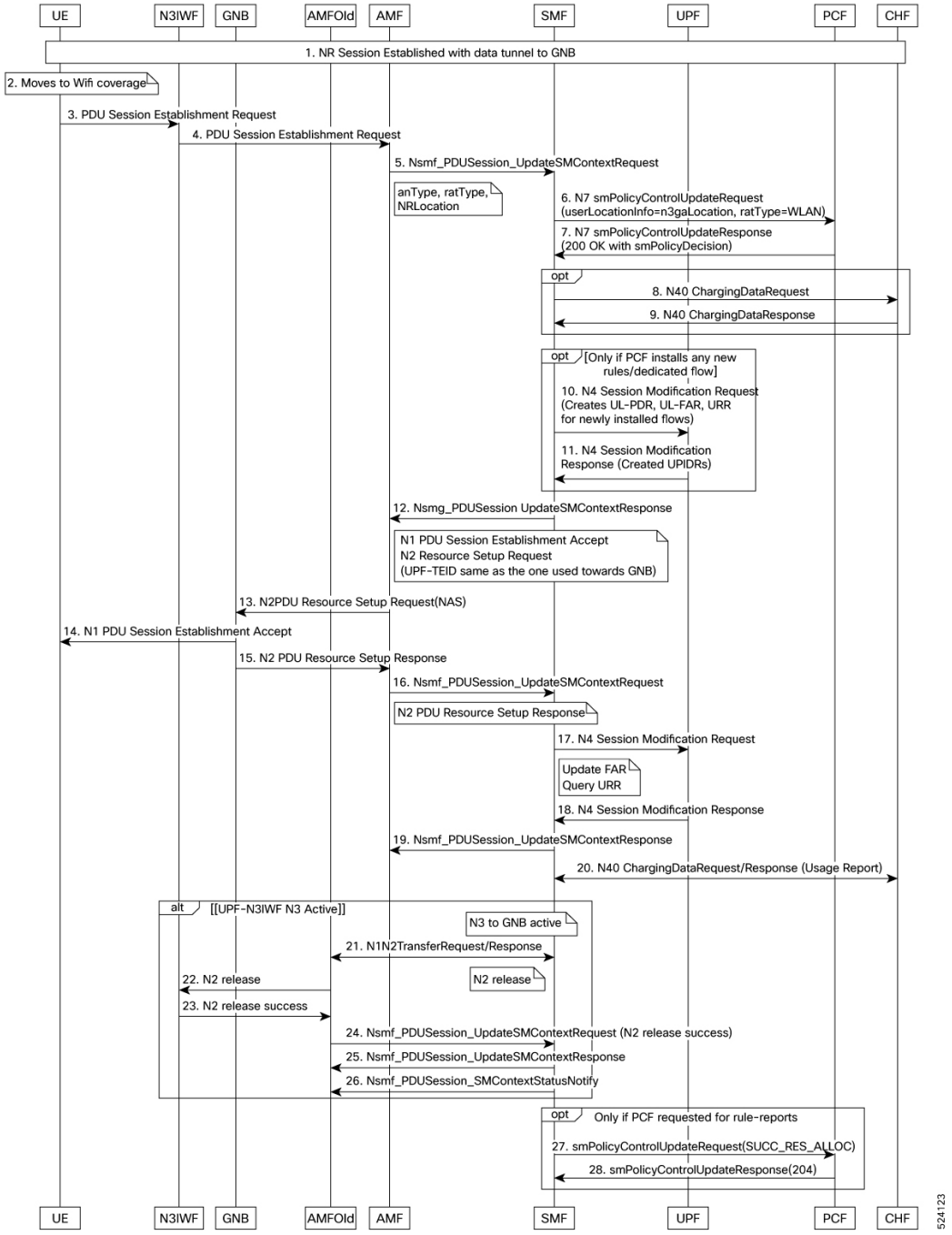


表 *350 : NR* から *N3IWF* 用 *Wi-Fi HO* へのコール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | セッションは、gNB にトンネリングされたデータを使用して NR を介して確立される。 |
| 2 | UE が Wi-Fi カバレッジがあるエリアに移動します。 |
| 3 | UE は、N1PDUSessionEstablishmentRequest を Existing-PDU-Session と共に N3IWF に送信します。 |
| 4 | N3IWF は N1PDUSessionEstablishmentRequest を Existing-PDU-Session で AMF に転送します。 |
| 5 | AMF は、Type=NON-3GPP-ACCESS、ratType=WLAN、N3GA Location などのパラメータを指定して、Nsmf_PDUSession_UpdateSMContextRequest を SMF に送信します。 |
| 6 | SMF は、userLocationInfo=N3GA-Location、ratType = WLAN を含む情報 SmPolicyContextData を使用して、N7 smPolicyControlUpdateRequest を PCF に送信します。 |
| 7 | PCF は 200 OK および SmPolicyDecision（ある場合）で応答します。 |
| 8 | オプションで、SMF はステップ 6 で PCF から受信した情報に基づいて N40ChargingDataRequest を送信します。 |
| 9 | ステップ 7 が送信されると、CHF は N40 ChargingDataResponse で応答します。 |
| 10 | ステップ 7 で、PCF が新しいルールのインストールを試みると、SMF はフロー作成のために UPF に対して N4SessionModificationRequest を送信します（新しくインストールされたフローの QER、PDR、FAR、URR を作成します）。 |
| 11 | ステップ 10 が送信された場合 UPF は、N4SessionModificationResponse で応答します。 |
| 12 | SMF は、N1PDUSessionEstablishmentAcceptをUEに、N2PDUResourceSetupRequestTransfer to N3IWF（UPF-TEIDはgNBに対して使用されるものと同じ）の両方を伝送する Nsmf_PDUSession_UpdateSMContextResponseを送信します。 |
| 13 | AMF は、N2PDUResourceSetupRequestTransfer および NAS PDU（N1PDUSessionEstablishmentAccept）を N3IWF に転送します。 |
| 14 | N3IWF は N1PDUSessionEstablishmentAccept を UE に転送します。 |

| ステップ | 説明 |
|---|---|
| 15 | N3IWF は、TEID を持つ N2PDUResourceSetupTransferResponse で応答します。 |
| 16 | AMF は、N2PDUResourceSetupTransferResponse を持つ SMF に Nsmf_PDUSession_UpdateSMContextRequest を送信します。 |
| 17 | SMF は、Update FAR を使用して N4SessionModificationRequest を送信して転送パラメータと QueryURR を更新し、使用状況レポートがあれば取得します。 |
| 18 | UPF が N4SessionModificationResponse で応答します。UPF と N3IWF 間のトンネルがアクティブになります。 |
| 19 | EPS インターワーキングが NR で有効になっている場合、SMF からの Nsmf_PDUSession_UpdateSMContextResponse メッセージには、AMF に対して解放される EBI のリストを含む releaseEbiList が含まれます。 |
| 20 | ステップ 18 で UPF から使用状況レポートを受信した場合、SMF は N40ChargingDataRequest を使用情報とともに CHF に送信し、CHF は N40ChargingDataResponse で応答します。 |
| 21 | 異なる AMF の場合、SMF は N1N2TransferRequest を N2ResourceReleaseTransferRequest で送信元 AMF（古い）に開始し、AMF は N1N2TransferAck で応答します。 |
| 22 | 送信元 AMF は、N2ResourceReleaseTransferRequest を gNB に転送します。 |
| 23 | gNB は N2ResourceReleaseTransferResponse で送信元 AMF に応答します。 |
| 24 | AMF は Nsmf_PDUSession_UpdateSMContextRequest を SMF に送信し、N2Release が成功したことを示します。 |
| 25 | SMF は、送信元 AMF に対する Nsmf_PDUSession_UpdateSMContextResponse で応答します。 |
| 26 | SMF は、Nsmf_PDUSession_SMContextStatusNotify を送信元 AMF に送信して、ハンドオーバーのステータスを示します。この手順は、コンプライアンス プロファイルで 3GPP 23502 のバージョン仕様が 15.6.0 に設定されている場合にのみ適用されます。 |
| 27 | 手順 6 で成功したインストールのルール レポートを PCF が要求した場合、SMF は N7smPolicyControlUpdateRequest を PCF に送信します。 |
| 28 | ステップ 25 が送信されると、PCF は SMF に N7 smPolicyControlUpdateResponse で応答します。 |

## PLMN Wi-FiからNRへのハンドオーバー

次のコールフローでは、PLMN 間 Wi-Fi から NR へのハンドオーバーに関連するさまざまな手順について説明します。

**図 *190 : PLMN Wi-Fiから*NR*へのハンドオーバー***

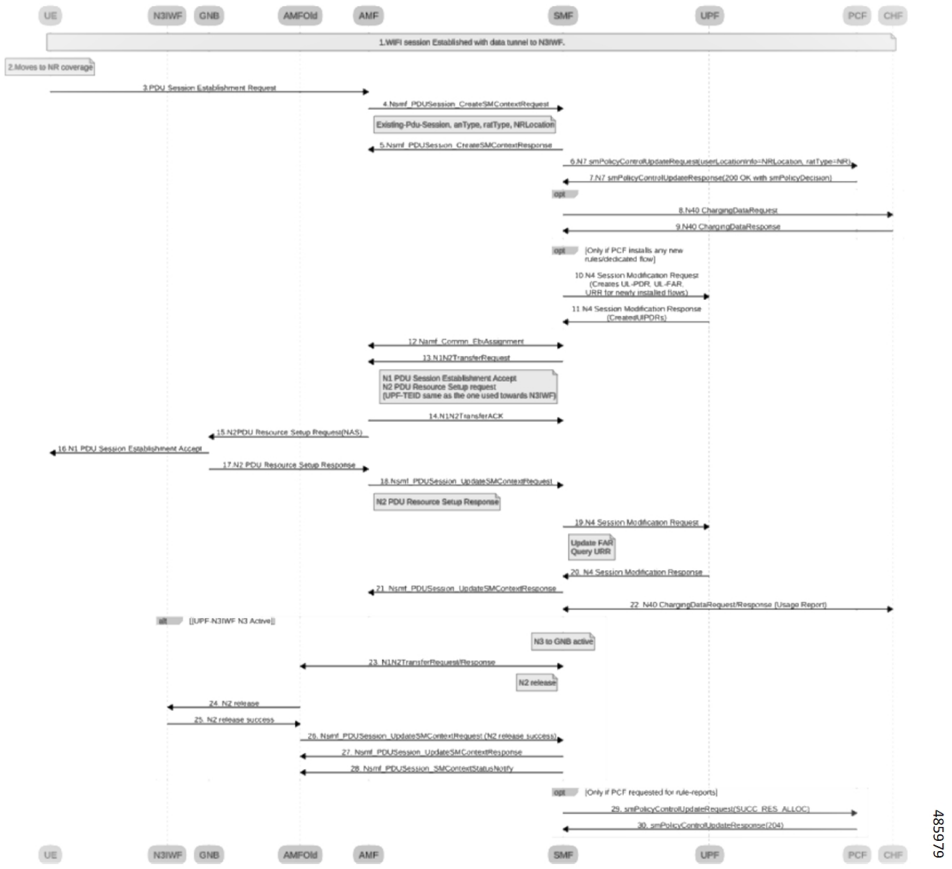



**表 *351 : PLMN Wi-Fiから*NR*へのハンドオーバー***

| ステップ | 説明 |
|---|---|
| 1 | N3IWF へのデータ トンネルで Wi-Fi セッションが確立されます。 |
| 2 | UE が NR カバレッジ エリアに移動します。 |
| 3 | UEは、既存の PDU セッションで PDU セッション確立要求を AMF に送信します。 |
| 4 | AMF は、AnType = 3GPP-ACCESS、ratType = NR、NR Location などのパラメータを使用して、Nsmf_PDUSession_CreateSMContextRequest を SMF に送信します。 |
| 5 | SMF は Nsmf_PDUSession_CreateSMContextResponse を送信します。 |

| ステップ | 説明 |
|---|---|
| 6 | SMF は、userLocationInfo=NRLocation、ratType = NR を含む情報 SmPolicyContextData を使用して、N7 smPolicyControlUpdateRequest を PCF に送信します。 |
| 7 | PCF は 200 OK および SmPolicyDecision（ある場合）で応答します。 |
| 8 | オプションで、SMF はステップ 6 で PCF から受信した情報に基づいて N40ChargingDataRequest を送信します。 |
| 9 | ステップ 8 が送信されると、CHF は N40 ChargingDataResponse で応答します。 |
| 10 | ステップ 7 で、PCF が新しいルールのインストールを試みると、SMF はフロー作成のために UPF に対して N4SessionModificationRequest を送信します（新しくインストールされたフローの QER、PDR、FAR、URR を作成します）。 |
| 11 | ステップ 10 が送信された場合 UPF は、N4SessionModificationResponse で応答します。 |
| 12 | epsInterworking が有効になっている場合、SMF は EBI を割り当てるために Namef_Commn_EbiAssignmentRequest を開始し、AMF は Namef_Commn_EbiAssignmentResponse に EBI の割り当てられたリストを返します。 |
| 13 | SMF は、UE への N1PDUSessionEstablishmentAccept と gNB への N2PDUResourceSetupRequestTransfer の両方を伝送する N1N2TransferRequest を送信します（N3IWF に対して使用されるものと同じ UPF-TEID）。 |
| 14 | AMF は SMF に N1N2TransferACK で応答します。 |
| 15 | AMF は N2PDUResourceSetupRequestTransfer および NAS PDU（N1PDUSessionEstablishmentAccept）を gNB に転送します。 |
| 16 | gNB は N1PDUSessionEstablishmentAccept を UE に転送します。 |
| 17 | gNB は、TEID を持つ N2PDUResourceSetupTransferResponse で応答します。 |
| 18 | AMF は、N2PDUResourceSetupTransferResponse を持つ SMF に Nsmf_PDUSession_UpdateSMContextRequest を送信します。 |
| 19 | SMF は、Update FAR を使用して N4SessionModificationRequest を送信して転送パラメータと QueryURR を更新し、使用状況レポートがあれば取得します。 |
| 20 | UPF が N4SessionModificationResponse で応答します。UPF と gNB 間のトンネルがアクティブになる。 |

| ステップ | 説明 |
|---|---|
| 21 | SMF は Nsmf_PDUSession_UpdateSMContextResponse で AMF に応答します。 |
| 22 | ステップ 20 で UPF から使用状況レポートを受信した場合、SMF は N40ChargingDataRequest を使用情報とともに CHF に送信し、CHF は N40ChargingDataResponse で応答します。 |
| 23 | 異なる AMF の場合、SMF は N1N2TransferRequest を N2ResourceReleaseTransferRequest で送信元 AMF（古い）に開始し、AMF は N1N2TransferAck で応答します。 |
| 24 | 送信元 AMF は N2ResourceReleaseTransferRequest を N3IWF に転送します。 |
| 25 | N3IWF は N2ResourceReleaseTransferResponse で送信元 AMF に応答します。 |
| 26 | AMF は Nsmf_PDUSession_UpdateSMContextRequest を SMF に送信し、N2Release が成功したことを示します。 |
| 27 | SMF は、送信元 AMF に対する Nsmf_PDUSession_UpdateSMContextResponse で応答します。 |
| 28 | SMF は、Nsmf_PDUSession_SMContextStatusNotify を送信元 AMF に送信して、ハンドオーバーのステータスを示します。この手順は、コンプライアンス プロファイルで 3GPP 23502 のバージョン仕様が 15.6.0 に設定されている場合にのみ適用されます。 |
| 29 | 手順 7 で PCF が正常なインストールまたは技術情報解放のルールレポートを要求した場合、SMF は N7smPolicyControlUpdateRequest を PCF に送信します。 |
| 30 | ステップ 29 が送信されると、PCF は SMF に N7 smPolicyControlUpdateResponse で応答します。 |

SMF は、アクティブなベアラーから 5G へのハンドオーバーをサポートしており、いずれかのフローが失敗した場合に「EPS-FB が必要です」という原因が表示された場合に、EPS-FB を開始できます。

### PLMN NR から Wi-Fi へのハンドオーバー間

次のコール フローでは、PLMN NR から Wi-Fi へのハンドオーバーに関連するさまざまな手順について説明します。

図 *191 : PLMN NR* から *Wi-Fi* へのハンドオーバー間

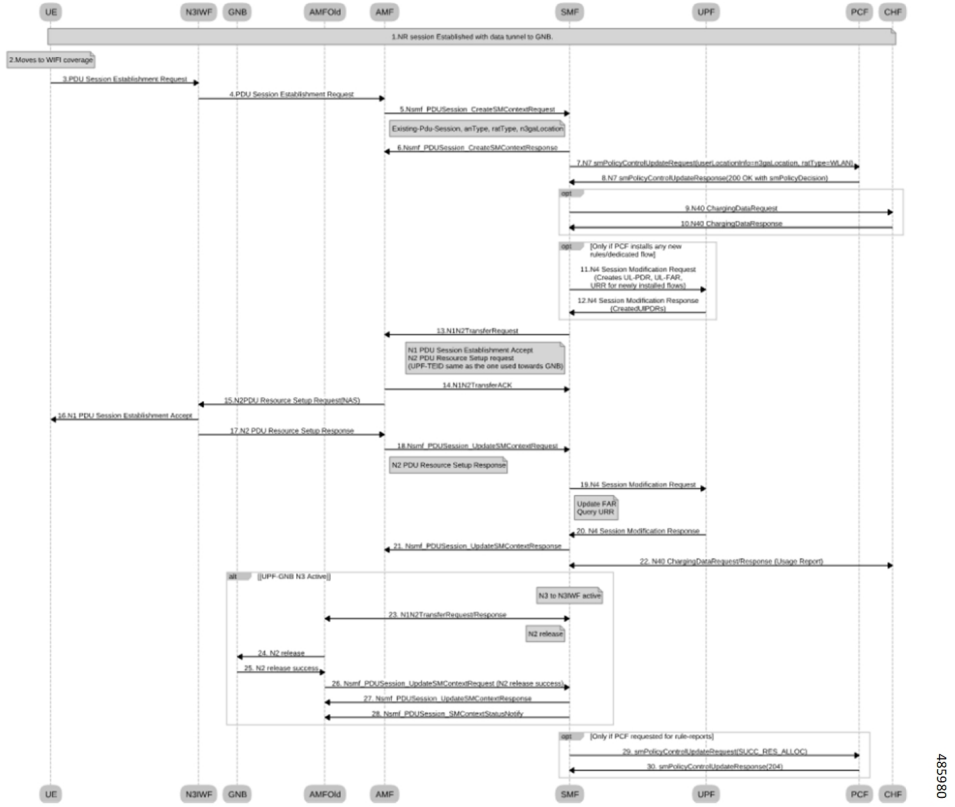



表 *352 : PLMN NR* から *Wi-Fi* へのハンドオーバー間

| ステップ | 説明 |
|---|---|
| 1 | セッションは、gNB にトンネリングされたデータを使用して NR を介して確立される。 |
| 2 | UE が Wi-Fi カバレッジがあるエリアに移動します。 |
| 3 | UE は、既存の PDU セッションで N1PDUSessionEstablishmentRequest を N3IWF に送信します。 |
| 4 | N3IWF は N1PDUSessionEstablishmentRequest を既存の PDU セッションで AMF に転送します。 |
| 5 | AMF は、Type=NON-3GPP-ACCESS、ratType=WLAN、N3GA Location などのパラメータを指定して、Nsmf_PDUSession_CreateSMContextRequest を SMF に送信します。 |
| 6 | SMF は Nsmf_PDUSession_UpdateSMContextResponse を AMF に送信します。 |

| ステップ | 説明 |
|---|---|
| 7 | SMF は、userLocationInfo=N3GA-Location、ratType = WLAN を含む情報 SmPolicyContextData を使用して、N7 smPolicyControlUpdateRequest を PCF に送信します。 |
| 8 | PCF は 200 OK および SmPolicyDecision（ある場合）で応答します。 |
| 9 | オプションで、SMF はステップ 8 で PCF から受信した情報に基づいて N40ChargingDataRequest を送信します。 |
| 10 | ステップ 9 が送信されると、CHF は N40 ChargingDataResponse で応答します。 |
| 11 | ステップ 8 で、PCF が新しいルールのインストールを試行すると、SMF はフロー作成のために UPF に対して N4SessionModificationRequest を送信します（新しくインストールされたフローの PDR、FAR、URR を作成します）。 |
| 12 | ステップ 11 が送信された場合 UPF は、N4SessionModificationResponse で応答します。 |
| 13 | SMF は、UE への N1PDUSessionEstablishmentAccept と N3IWF への N2PDUResourceSetupRequestTransfer の両方を伝送する N1N2TransferRequest を送信します（gNB に対して使用されるものと同じ UPF-TEID）。 |
| 14 | AMF は SMF に N1N2TransferACK で応答します。 |
| 15 | AMF は、N2PDUResourceSetupRequestTransfer および NAS PDU（N1PDUSessionEstablishmentAccept）を N3IWF に転送します。 |
| 16 | N3IWF は N1PDUSessionEstablishmentAccept を UE に転送します。 |
| 17 | N3IWF は、TEID を持つ N2PDUResourceSetupTransferResponse で応答します。 |
| 18 | AMF は、N2PDUResourceSetupTransferResponse を持つ SMF に Nsmf_PDUSession_UpdateSMContextRequest を送信します。 |
| 19 | SMF は、Update FAR を使用して N4SessionModificationRequest を送信して転送パラメータと QueryURR を更新し、使用状況レポートがあれば取得します。 |
| 20 | UPF が N4SessionModificationResponse で応答します。UPF と N3IWF 間のトンネルがアクティブになります。 |
| 21 | SMF は Nsmf_PDUSession_UpdateSMContextResponse で AMF に応答します。 |
| 22 | ステップ 20 で UPF から使用状況レポートを受信した場合、SMF は N40ChargingDataRequest を使用情報とともに CHF に送信し、CHF は N40ChargingDataResponse で応答します。 |

| ステップ | 説明 |
|---|---|
| 23 | 異なる AMF の場合、SMF は N1N2TransferRequest を N2ResourceReleaseTransferRequest で送信元 AMF（古い）に開始し、AMF は N1N2TransferAck で応答します。 |
| 24 | 送信元 AMF は、N2ResourceReleaseTransferRequest を gNB に転送します。 |
| 25 | gNB は N2ResourceReleaseTransferResponse で送信元 AMF に応答します。 |
| 26 | AMF は Nsmf_PDUSession_UpdateSMContextRequest を SMF に送信し、N2Release が成功したことを示します。 |
| 27 | SMF は、送信元 AMF に対する Nsmf_PDUSession_UpdateSMContextResponse で応答します。 |
| 28 | SMF は、Nsmf_PDUSession_SMContextStatusNotify を送信元AMF に送信して、ハンドオーバーのステータスを示します。この手順は、コンプライアンス プロファイルで 3 GPP 23502 のバージョン仕様が 15.6.0 に設定されている場合にのみ適用されます。 |
| 29 | 手順 8 で成功したインストールのルールレポートを PCF が要求した場合、SMF は N7smPolicyControlUpdateRequest を PCF に送信します。 |
| 30 | ステップ 29 が送信されると、PCF は SMF に N7 smPolicyControlUpdateResponse で応答します。 |

### Wi-Fi から EUTRA へのハンドオーバー

次のコール フローでは、Wi-Fi から EUTRA へのハンドオーバーに関連するさまざまな手順について説明します。

図 *192 : Wi-Fi* から *EUTRA* へのハンドオーバー

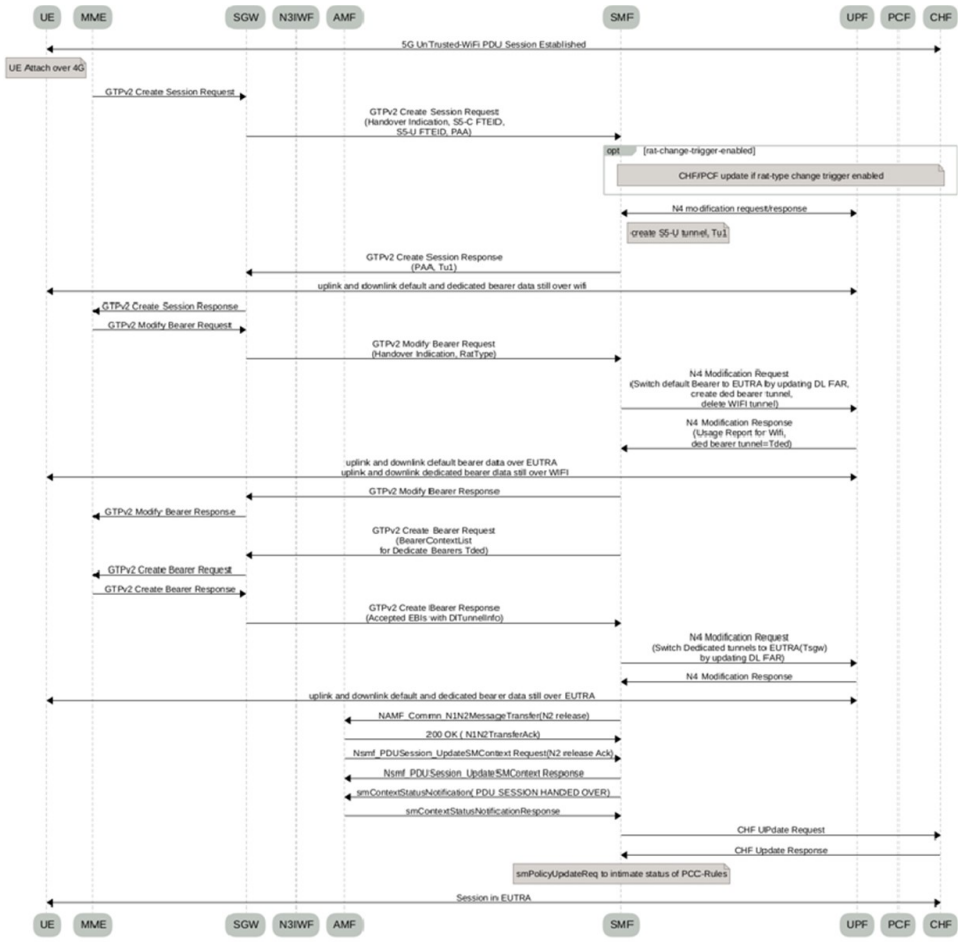



表 *353 : Wi-Fi* から *EUTRA* へのハンドオーバー

| ステップ | 説明 |
|---|---|
| 1 | N3IWF へのデータ トンネルで Wi-Fi セッションが確立されます。 |
| 2 | UE が 4G/LTE のカバレッジ エリアに移動します。 |
| 3 | MME は GTPv2CreateSessionRequest を S-GW に送信します。 |
| 4 | S-GW は、デフォルトのベアラー F-TEID 情報とともにハンドオーバー指示を設定した GTPv2CreateSessionRequest を送信します。 |
| 5 | SMF は、userLocationInfo=EutraLocation、ratType = EUTRA を含む情報 SmPolicyContextData とともに N7 smPolicyControlUpdateRequest を PCF に送信します。 |
| 6 | PCF は 200 OK および SmPolicyDecision（ある場合）で応答します。 |

| ステップ | 説明 |
|---|---|
| 7 | オプションで、SMF はステップ 6 で PCF から受信した情報に基づいて N40 ChargingDataRequest を送信します。 |
| 8 | ステップ 7 が送信されると、CHF は N40 ChargingDataResponse で応答します。 |
| 9 | ステップ 6 で、PCF が新しいルールまたはルールベースの変更をインストールしようとすると、SMF はフロー作成のために UPF に対して N4SessionModificationRequest を送信します（新しくインストールされたフローの PDR、FAR、URR を作成します）。 |
| 10 | ステップ 9 が送信された場合 UPF は、N4SessionModificationResponse で応答します。 |
| 11 | SMF は、GTPv2CreateSessionResponse を SGW に送信します。この場合も、デフォルトと専用のベアラーのアップリンクとダウンリンクのデータは Wi-Fi を介して流れます。 |
| 12 | S-GW は、GTpv2CreateSessionResponse を MME に転送します。 |
| 13 | MME は GTPv2ModifyBearerRequest を S-GW に送信します。 |
| 14 | S-GW は、ハンドオーバー通知が設定された GTPv2ModifyBearerRequest を送信します。 |
| 15 | SMF は、Update FAR を使用して N4SessionModificationRequest を送信し、デフォルトのベアラーの転送パラメータを更新します。クエリ URR を使用して使用レポート（ある場合）を取得し、変更されたルールの PDR を更新（存在する場合）し、削除されたルールの PDR を削除します。 |
| 16 | UPF が N4SessionModificationResponse で応答します。UPF と SGW 間のトンネルが、デフォルトのベアラーに対してアクティブになります。ここでは、デフォルト ベアラーのアップリンクおよびダウンリンク データは EUTRA を経由して流れ、専用ベアラーのデータは今まで Wi-Fi を経由して流れます。 |
| 17 | SMF は GTPv2ModifyBearerResponse を S-GW に送信します。 |
| 18 | S-GW は、GTpv2ModifyBearerResponse を MME に転送します。 |
| 19 | SMF は、専用ベアラーのベアラー コンテキストのリストを持つ S-GW に GTPv2CreateBearerRequest を送信します。 |
| 20 | S-GW が MME に GTPv2CreateBearerRequest を送信します。 |
| 21 | MME が GTPv2CreateBearerResponse を S-GW に送信します。 |

| ステップ | 説明 |
|---|---|
| 22 | S-GW は、GTPv2CreateBearerResponse を、受け入れられたベアラー コンテキストのリストとともに、EBIs および DlTunnelInformation（TEID など）とともに SMF に送信します。 |
| 23 | SMF は Update FAR を使用して N4SessionModificationRequest を送信し、専用ベアラの転送パラメータを更新します。 |
| 24 | UPF が N4SessionModificationResponse で応答します。UPF と S-GW 間のトンネルが専用ベアラーに対してアクティブになります。ここでは、デフォルトと専用の両方のベアラーのアップリンクとダウンリンクのデータが EUTRA を経由して流れます。 |
| 25 | SMF は N1N2TransferRequest を N2ResourceReleaseTransferRequest で送信元 AMF に開始し、AMF は N1N2TransferAck で応答します。 |
| 26 | AMF は N2ResourceReleaseTransferRequest を N3IWF に転送します。 |
| 27 | N3IWF は AMF への N2ResourceReleaseTransferResponse で応答します。 |
| 28 | AMF は Nsmf_PDUSession_UpdateSMContextRequest を SMF に送信し、N2Release が成功したことを示します。 |
| 29 | SMF は、AMF へのNsmf_PDUSession_UpdateSMContextResponse で応答します。 |
| 30 | SMF は、Nsmf_PDUSession_SMContextStatusNotify を AMF に送信して、ハンドオーバーのステータスを示します。この手順は、コンプライアンス プロファイルで 3GPP 23502 のバージョン仕様が 15.6.0 に設定されている場合にのみ適用されます。 |
| 31 | ステップ 16 で UPF から使用状況レポートを受信した場合、SMF は N40ChargingDataRequest を使用情報とともに CHF に送信し、CHF は N40ChargingDataResponse で応答します。 |
| 32 | 手順 6 で成功したインストールのルール レポートを PCF が要求した場合、SMF は N7smPolicyControlUpdateRequest を PCF に送信します。 |
| 33 | ステップ 32 が送信されると、PCF は SMF に N7 smPolicyControlUpdateResponse で応答します。 |

### EUTRA から Wi-Fi へのハンドオーバー

次のコール フローでは、EUTRA から Wi-Fi へのハンドオーバーに関連するさまざまな手順について説明します。

図 *193 : EUTRA* から *Wi-Fi* へのハンドオーバー

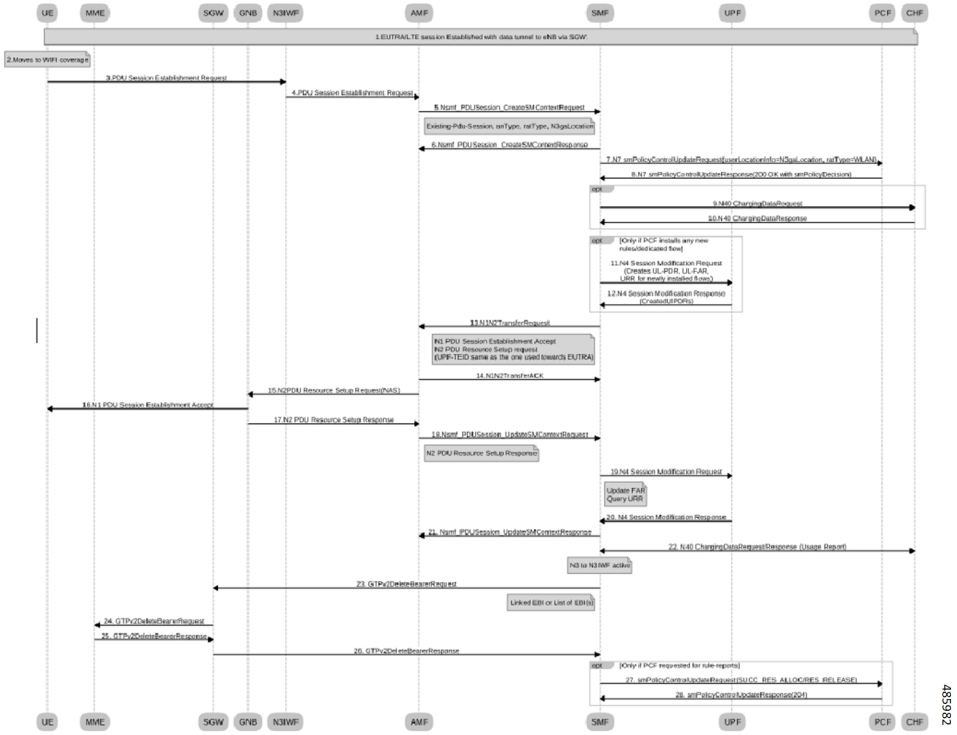



表 *354 : EUTRA* から *Wi-Fi* へのハンドオーバー

| ステップ | 説明 |
|---|---|
| 1 | セッションは、SGW を介して eNB にトンネリングされたデータを使用して EUTRA 経由で確立されます。 |
| 2 | UE が Wi-Fi カバレッジがあるエリアに移動します。 |
| 3 | UE は N1PDUSessionEstablishmentRequest を N3IWF に送信します。 |
| 4 | N3IWF は N1PDUSessionEstablishmentRequest を AMF に転送します。 |
| 5 | AMF は、Type=NON-3GPP-ACCESS、ratType=WLAN、N3GA Location などのパラメータを指定して、Nsmf_PDUSession_CreateSMContextRequest を SMF に送信します。 |
| 6 | SMF は、Nsmf_PDUSession_CreateSMContextResponse を AMF に送信します。 |
| 7 | SMF は、userLocationInfo=N3GA-Location、ratType = WLAN を含む情報 SmPolicyContextData を使用して、N7 smPolicyControlUpdateRequest を PCF に送信します。 |
| 8 | PCF は 200 OK および SmPolicyDecision（ある場合）で応答します。 |

| ステップ | 説明 |
|---|---|
| 9 | オプションで、SMF はステップ 8 で PCF から受信した情報に基づいて N40ChargingDataRequest を送信します。 |
| 10 | ステップ 9 が送信されると、CHF は N40 ChargingDataResponse で応答します。 |
| 11 | ステップ 8 で、PCF が新しいルールのインストールを試行すると、SMF はフロー作成のために UPF に対して N4SessionModificationRequest を送信します（新しくインストールされたフローの PDR、FAR、URR を作成します）。 |
| 12 | ステップ 11 が送信された場合 UPF は、N4SessionModificationResponse で応答します。 |
| 13 | SMF は、UE への N1PDUSessionEstablishmentAccept と N3IWF への N2PDUResourceSetupRequestTransfer の両方を伝送する N1N2TransferRequest を送信します（EUTRA に対して使用されるものと同じ UPF-TEID）。 |
| 14 | AMF は SMF に N1N2TransferACK で応答します。 |
| 15 | AMF は、N2PDUResourceSetupRequestTransfer および NAS PDU（N1PDUSessionEstablishmentAccept）を N3IWF に転送します。 |
| 16 | N3IWF は N1PDUSessionEstablishmentAccept を UE に転送します。 |
| 17 | N3IWF は、TEID を持つ N2PDUResourceSetupTransferResponse で応答します。 |
| 18 | AMF は、N2PDUResourceSetupTransferResponse を持つ SMF に Nsmf_PDUSession_UpdateSMContextRequest を送信します。 |
| 19 | SMF は、Update FAR を使用して N4SessionModificationRequest を送信して転送パラメータと QueryURR を更新し、使用状況レポートがあれば取得します。 |
| 20 | UPF が N4SessionModificationResponse で応答します。UPF と N3IWF 間のトンネルがアクティブになります。 |
| 21 | SMF は Nsmf_PDUSession_UpdateSMContextResponse で AMF に応答します。 |
| 22 | ステップ #20 で UPF から使用状況レポートを受信した場合、SMF は N40ChargingDataRequest を使用情報とともに CHF に送信し、CHF は N40ChargingDataResponse で応答します。 |
| 23 | SMF は、技術情報をクリーンアップするために、SGW への GTPv2DeleteBearerRequest を開始します。 |
| 24 | SGW は GTPv2DeleteBearerRequest を MME に転送します。 |

| ステップ | 説明 |
|---|---|
| 25 | MME は SGW への GTPv2DeleteBearerResponse で応答します。 |
| 26 | SGW は、GTPv2DeleteBearerResponse を SMF に送信し、ベアラーの削除が成功したことを示します。 |
| 27 | 手順 8 で PCF が正常なインストールまたは技術情報解放のルールレポートを要求した場合、SMF は N7smPolicyControlUpdateRequest を PCF に送信します。 |
| 28 | ステップ 27 が送信されると、PCF は SMF に N7 smPolicyControlUpdateResponse で応答します。 |

# N3GA ロケーション パラメータ

SMF は、3GPP TS 29.571 リリース 16.4.0 に従って N3GALocation パラメータをサポートします。AMF が N3GA ロケーションを送信する場合、SMF は、適切なコンプライアンス バージョンを構成した後、N7（PCF）や N40（CHF）などのピア インターフェイスに送信される N3GALocation に次の属性を含めます。」

| **Attribute name** | 説明 |
|---|---|
| n3gppTai | PLMN で使用される一意の非 3GPP TAI。3GPP PLMN 内部インターフェイスには存在しますが、N5 インターフェイスには存在しません。 |
| n3IwfId | この IE には、NGAP を介して受信した N3IWF 識別子が含まれ、16 進数文字列としてエンコードされます。文字列内の各文字の値は「0」～「9」または「A」～「F」になり、4 ビットを表します。N3IWF ID の 4 つの最上位ビットを表す最上位文字が文字列の最初に表示され、N3IWF ID の最下位 4 ビットを表す文字が文字列の最後に表示されます。<br>パターン：'^[A-Fa-f0-9]+$'<br>例：<br>N3IWF Id 0x5BD6 は「5BD6」としてエンコードされます。<br>UE が信頼できない非 3GPP アクセスを介して 5GC にアクセスしている場合、この番号が 3GPP PLMN 内部インターフェイスに存在するが、N5 インターフェイスには存在しない。 |

| | |
|---|---|
| ueIpv4Addr | UE/N5CW デバイスのローカル IPv4 アドレス（N3IWF、TNGF、または TWIF に到達するために使用）。<br>ueIPv4Addr または ueIPv6Addr は、信頼または信頼できない非 3GPP アクセスを介して UE が 5GC にアクセスしており、情報が利用可能な場合に存在します。 |
| ueIpv6Addr | UE/N5CW デバイスのローカル IPv6 アドレス（N3IWF、TNGF、または TWIF に到達するために使用）。<br>ueIPv4Addr または ueIPv6Addr は、信頼または信頼できない非 3GPP アクセスを介して UE が 5GC にアクセスしており、情報が利用可能な場合に存在します。 |
| portNumber | UDP または TCP 送信元ポート番号。信頼または信頼できない非 3GPP アクセスを介して UE が 5GC にアクセスしており、NAT が検出された場合に存在します。 |
| tnapID | この IE には、信頼できる非 3GPP アクセスポイント（TNAP）の識別子が含まれます。 |
| hfcNodeId | この IE には、NGAP を介して受信した HFC ノード識別子が含まれています。有線アクセスネットワークを介して 5GC にアクセスする 5G-CRG/FN-CRG に対して存在します。 |
| gli | この IE には、グローバル回線 ID が含まれています。有線アクセスネットワークを介して 5GC にアクセスする 5G-BRG/FN-BRG 用に存在します。 |
| w5gbanLineType | この IE は、有線アクセス ネットワークを介して 5GC にアクセスする 5G-BRG/FN-BRG のために存在する可能性があります。存在する場合は、有線のタイプ（DSL または PON）を示します。 |
| twap ID | この IE には、信頼された WLAN アクセス ポイント（TWAP）識別子が含まれます。 |

（注）

- ePDG を介した接続の場合、システムは IP アドレス、ポート、およびプロトコル（使用可能な場合）のみを入力します。SMF は、オプションのパラメータが使用できない場合、それらのパラメータを入力しません。
- SMF は、すべての N4 メッセージの SUB_PARAMS IE の下で ULI の一部として N3GPPTAI のみを送信します。
- SMF は、3GPP TS 29.571 リリース 16.4.0 に従って、N3GA の場所で次のパラメータをサポートします。
  - tnapID
  - hfcNodeId
  - gli
  - w5gbanLineType
  - twap ID

# アクティブなベアラー機能を使用した N3IWF および HO サポートを使用した Wi-Fi 経由の音声またはビデオ通話

この機能は、ユーザーが 1 つのネットワークから別のネットワークに移動する際に（たとえば、Wi-Fi からセルラーへ、またはその逆に）通話の継続性を維持するために重要です。「アクティブなベアラー」とは、進行中のデータ セッションまたはコールを指します。したがって、「アクティブベアラーの HO サポート」とは、システムが接続を切断せずに、あるネットワークから別のネットワークへの進行中の通話またはデータ セッションの移行を処理できることを意味します。

# N3IWF セッションの RAT タイプの処理

リリース 2024.03 より前は、SMF は、RAT タイプが NR に設定された N3IWF ベースのセッションに対して受信された PDU セッション確立要求を処理するために使用されていました。

リリース 2024.03 以降、SMF は、RAT タイプが NR に設定された N3IWF ベースのセッションの PDU セッション確立要求を拒否し、RAT タイプが WLAN に設定された場合にのみ要求を処理するようになりました（3GPP 仕様 23.501 のリリース 16.4.0 に従って）。

# 標準準拠

N3IWF 機能は、次の標準規格に準拠しています：

• 3GPP 23.501 リリース 15 バージョン

# OAM サポート

### バルク統計サポート

この機能は、smf サービス統計情報の一部として新しいラベル「anType」をサポートします。このラベルは、アクセス ネットワーク タイプを 3GPP アクセスまたは非 3GPP アクセスとして定義します。

バルク統計のサポートの詳細については、このリリースに該当する *UCC 5G SMF* メトリック リファレンス ドキュメント を参照してください。

SMF は、smf_service_stats の プロシージャタイプに関する次の新しい値のセットをサポートしています。

- pduim_ran_req_active_to_idle_non3gpp：RAN によって開始されたアイドルモードエントリ
- pduim_nw_req_active_to_idle_non3gpp：NW がアイドル モード エントリを開始しました。
- pduim_ue_req_idle_to_active_non3gpp - UE がアイドル モードの終了を開始した

SMF では、「an-type」ラベルとともに既存の手順タイプ ラベルを使用して、NR セッションと N3IWF セッションを区別します。

- nr_to_untrusted_wifi_handover：NR から N3IWF へのハンドオーバー
- utn3gpp_to_5g_handover：N3IWF から NR へのハンドオーバー
- ue_req_pdu_sess_mod：UE が PDU の変更を開始した
- amf_req_pdu_sess_mod：AMF が PDU の変更を開始した
- smf_req_pdu_sess_mod：SMF によって PDU の変更が開始された
- pcf_req_pdu_sess_mod：PCF が PDU の変更を開始した
- udm_req_pdu_sess_mod：UDM が PDU の変更を開始した
- gnb_req_pdu_sess_mod：GNB が PDU の変更を開始した
- pccf_restoration_init_mod：PCSCF 復元で PDU の変更が開始した
- enb_to_n3iwf_handover：enodeB から N3IWF へのハンドオーバー
- n3iwf_wifi_to_enb_handover：N3IWF から enodeB へのハンドオーバー
- pduim_ran_req_active_to_idle_non3gpp：非 3GPP アクセスで UE がアクティブから待機中になる

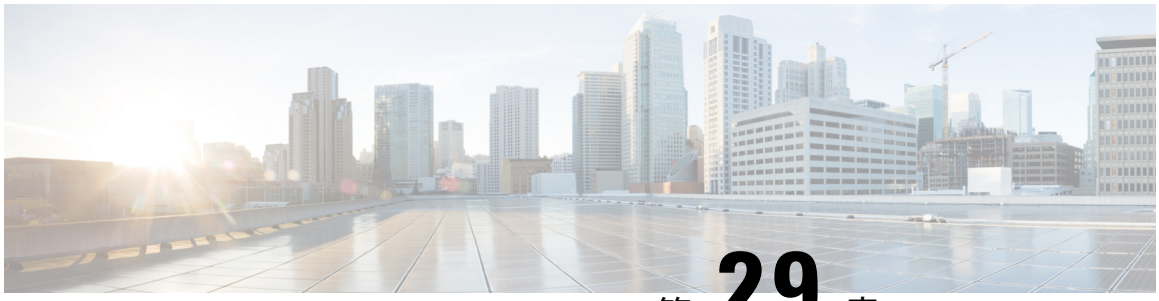
### Monitoring Support

既存の show subscriber コマンドおよび clear subscriber コマンドの 1 つには、サブスクライバのアクセス タイプを示す新しいフィルタ オプション「an-type」があります。show subscriber コマンドの出力には、N3Ga の場所に関する情報も表示されます。

UE が Wi-Fi アクセス ポイントに接続し、ePDG を介して接続しようとした場合、アクセスタイプは非 3GPP アクセスとして分類されます。AMF を介して接続する N3IWF セッションの場合、アクセス タイプは 3GPP アクセスで、アクセス タイプは非 3gpp アクセスです。

### 『PSF Administration guide』

この機能は、手順失敗ログでのアクセス ネットワーク タイプ情報のサポートを提供します。



第 29 章

# ネットワーク開始型セッション変更手順


- 機能の概要と変更履歴, on page 1085
- 機能説明, on page 1086
- 機能の仕組み, on page 1086
- OAM サポート （1091 ページ）


## 機能の概要と変更履歴

### 要約データ

***Table 355:*** 要約データ

| | |
|---|---|
| 該当製品または機能エリア | SMF |
| 該当プラットフォーム | SMI |
| 機能のデフォルト設定 | 有効：常時オン |
| このリリースでの関連する変更点 | N/A |
| 関連資料 | 該当なし |

### 更新履歴

***Table 356:*** マニュアルの変更履歴

| 改訂の詳細 | リリース |
|---|---|
| VoNR 関連の強化の修正を追加。 | 2022.04.0 |
| 最初の導入。 | 2020.02.0 より前 |

# 機能説明

PDU セッション変更手順の目的は、UE 専用の QoS フローを作成することです。UE のデフォルト QoS フローに対して異なる QoS 特性を持つ専用 QoS フローを作成するには、次の 2 つの方法があります。

- UE が開始した PDU セッションの変更
- ネットワークによって開始された PDU セッションの変更

**Note** ポリシー更新応答にポリシー パラメータが含まれている場合は、PDU 変更手順がトリガーされます。

ネットワークは AN、AMF、または PCF です。

SMF は、UE が開始したセッション変更要求またはネットワークが開始したセッション変更要求を受信して、UE の PDU セッションを拡張し、既存の QoS フローを変更するか、ユーザ トラフィックに適した新しい QoS フローを作成します。

**Note** PCF によって開始されたフローの削除手順中にエラーが発生した場合、SMF は PCC ルールを削除し、削除された PCC ルールの詳細を UPF および PCF に伝達します。

# 機能の仕組み

ここでは、この機能の仕組みを説明します。

## コール フロー

このセクションでは、次のコールフローについて説明します。

- CM 接続状態のアクティブなユーザー プレーンと UE のネットワーク開始の変更コール フロー, on page 1087
- CM 接続状態の非アクティブなユーザー プレーンと UE に対してネットワークが開始した変更コール フロー, on page 1088
- 非アクティブなユーザー プレーンと CM-Idle 状態の UE に対してネットワークが開始した変更コール フロー, on page 1089

# CM 接続状態のアクティブなユーザー プレーンと UE のネットワーク開始の変更コール フロー

このセクションでは、UE が CM 接続状態にあり、ユーザー プレーンがアクティブ化されている場合の、ネットワークの開始後に N4 セッション変更がどのように機能するかについて説明します。ネットワークは PCF、UDM、または SMF です。

次の図は、UE が CM 接続状態で、ユーザー プレーンがアクティブになっている場合の、ネットワークによって開始される変更のコール フローを示しています。

***Figure 194: CM** 接続状態での **UE** とアクティブ化されたユーザー プレーンでのネットワーク開始の変更コール フロー*

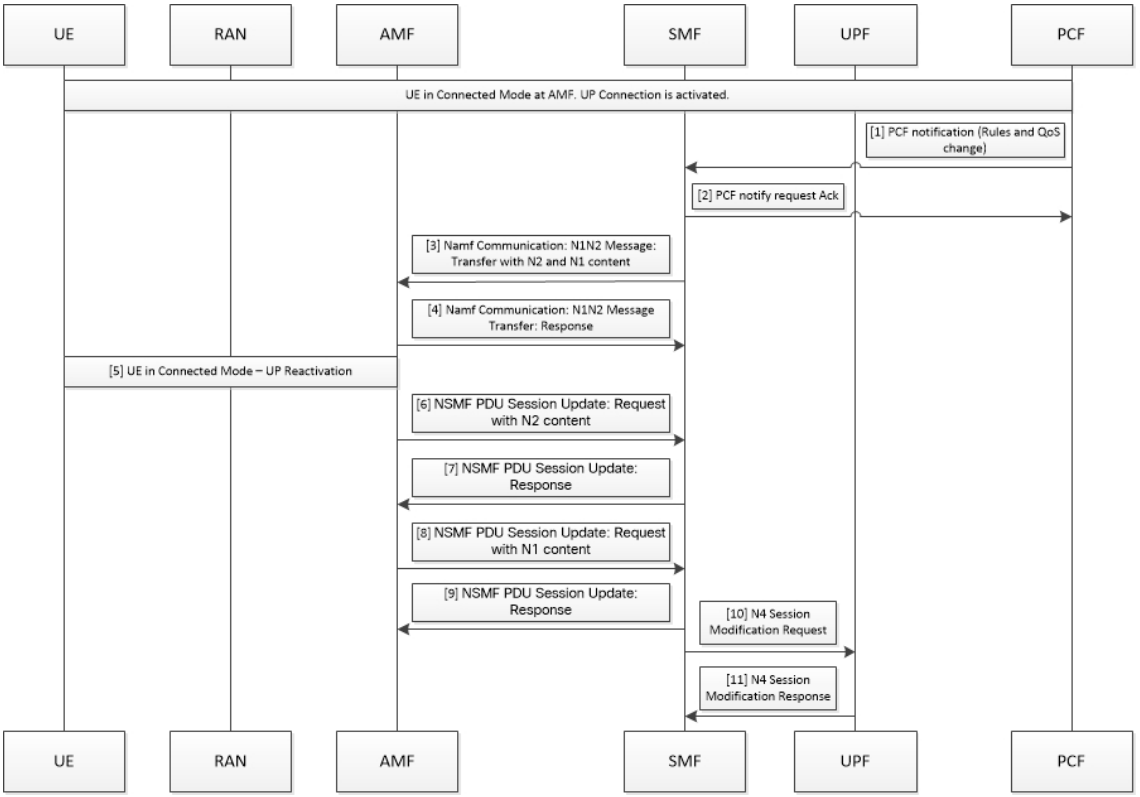



***Table 357: CM** 接続状態でアクティブ化されたユーザー プレーンの **UE** のネットワーク開始型変更コール フローの説明*

| ステップ | 説明 |
|---|---|
| 1 | PCF は、適用するポリシー決定とともに SMF に通知を送信します。 |
| 2 | SMF は、ポリシー通知の確認応答を PCF に送信します。 |

| ステップ | 説明 |
|---|---|
| 3 | SMF は、ポリシー決定が原因で発生した QoS モデルの変更を識別し、NAMF 通信 N1 および N2 メッセージを AMF に転送するようトリガします。このメッセージ転送には、以下の詳細が含まれます：<br>• PDU セッション ID<br>• N2 SM 情報<br>• N1 SM 情報<br>• N1 および N2 転送機能通知ターゲット アドレス<br>N2 には PDU セッション リソース変更要求転送 IE が含まれ、N1 には PDU セッション変更要求が含まれます。 |
| 4 | UE が CM 接続状態であるため、AMF は N1 および N2 転送応答を開始します。この応答には、「200 OK」のステータス コードと「N1_N2_TRANSFER_INITIATED」の原因が含まれています。 |
| 5 | ユーザー プレーンの変更手順は、RANとUEの両方に対して開始されます。 |
| 6 | RAN からの応答を受信した後、AMF は、NSMF PDU セッション更新 SM コンテキスト要求を SMF に送信します。この要求には、N2 インターフェイスの SM 情報を含みます。 |
| 7 | SMF は、NSMF PDU セッション更新 SM コンテキスト要求のステータス コード「200 OK」で AMF に応答します。 |
| 8 | UE からの応答を受信した後、AMF は SMF に NSMF PDU セッション更新 SM コンテキスト要求を送信します。この要求には、N1 インターフェイスの SM 情報が含まれています。 |
| 9 | SMF は AMF に「NSMF PDU セッション更新 SM コンテキスト要求」のステータス コード「200 OK」で応答します。 |
| 10 | 新しい QoS 情報に基づいて、SMF は UPF に対して N4 変更手順を開始し、セッションを変更します。 |
| 11 | UPF はセッションを変更し、変更の確認応答を SMF に送信します。 |

## CM接続状態の非アクティブなユーザープレーンとUEに対してネットワークが開始した変更コール フロー

このセクションでは、UE が CM 接続状態にあり、ユーザープレーン（UP）コンテキストが非アクティブになった場合のネットワークによって開始される変更手順について説明します。

1. PCF は、ルールおよびQoSが変更されたPDUセッションのポリシー更新通知をSMFに送信します。PCF からの通知として受信されたアップデートされたポリシー ルールを SMF は、処理します。
2. SMF により「200 OK」ステータス コードが PCF に返されます。
3. SMF は、AMF への NAMF 通信 N1 N2 メッセージ転送サービス操作を使用して、変更されたルールと QoS の変更を含む N1 メッセージ PDU セッション変更コマンドのみを UE に送信します。
4. AMF は、NAMF Communication N1 N2 Message Transfer 応答を SMF に送信します。この応答には、「200 OK」のステータス コードと「N1N2_TRANSFER_INITIATED」の原因が含まれています。
5. SMF は AMF からの Nsmf_PDUSession_UpdateSMContext メッセージを待機します。
6. SMF は、UE からの応答を受信した後、変更されたパラメータ値で UPF 内のサブスクライバ セッションを更新し、UP コンテキスト状態は Deactivated のまま残ります。
7. SMF は、N4 セッション変更リクエストを UPF に送信し、ユーザー プレーン トンネルの変更されたルールと QoS の詳細を更新します。
8. UPF は PDU セッションの N4 セッション変更応答を送信します。
9. SMF は、ダウンリンクまたはアップリンク データを送信するトリガーの結果として、UP 接続をアクティブにします。

## 非アクティブなユーザー プレーンと CM-Idle 状態の UE に対してネットワークが開始した変更コール フロー

このセクションでは、UE が CM アイドル状態で、ユーザープレーン（UP）コンテキストが非アクティブになった場合のネットワークによって開始された変更手順について説明します。

SMF では、ネットワークによって開始された PDU セッション変更手順で次の使用例がサポートされます：

- PDN アクティベーションのサービス リクエストで UE がアクティブに切り替わるとき
- 制御サービス リクエストで UE がアクティブになったとき

### ユース ケース 1：PDN アクティベーションのサービス要求で UE がアクティブになる場合

1. PCF は、ルールおよびQoSが変更されたPDUセッションのポリシー更新通知をSMFに送信します。PCF からの通知として受信されたアップデートされたポリシー ルールを SMF は、処理します。
2. SMF により「200 OK」ステータス コードが PCF に返されます。
3. SMF は、AMF への NAMF 通信 N1 N2 メッセージ転送サービス操作を使用して、変更されたルールと QoS の変更を含む N1 メッセージ PDU セッション変更コマンドのみを UE に送信します。

4. AMF は、NAMF Communication N1 N2 Message Transfer 応答を SMF に送信します。この応答には、「200 OK」のステータス コードおよび「ATTEMPTING_TO_REACH_UE」の原因が含まれます。
5. SMF は、UE への N1 - PDU セッション変更応答メッセージの再送信を停止します。さらに、N1 PDU 変更コマンド再送信タイマーを停止し、UE からの応答を待ちます。

（注） N1 PDU 変更コマンド再送信タイマーを構成できます。N1 PDU 変更コマンドの再送信のタイムアウト値と最大試行回数を構成するには、アクセス プロファイル構成モードで **n1 t3591-pdu-mod-cmd timeout** *timeout* **max-retry** *retry_count* コマンドを使用します。デフォルトのタイムアウト値は 2 秒、デフォルトの再試行回数は 2 回です。

6. UE は、AMF からページング要求を受信し、要求されたサービスを開始して PDU セッションをアクティブにします。UE は、UP コンテキストをアクティブにする必要がある場合にのみ、PDU Session-to-Activate リストに PDU セッション ID を含めます。

   SMF は、アイドルからアクティブへの PDU セッション移行手順を開始し、現在の変更手順を一時停止します。
7. アイドルからアクティブへの手順が完了すると、SMF は変更手順を再開し、N1 N2 転送メッセージで N1 と N2 の両方のコンテンツを送信し、それぞれ UE と gNB からの N1 と N2 の両方の応答を待ちます。
8. SMF は gNB から N2 応答を受信し、UE から N1 応答をそれぞれ受信します。
9. SMF は、N4 セッション変更リクエストを UPF に送信し、ユーザー プレーン トンネルの変更されたルールと QoS の詳細を更新します。
10. UPF は PDU セッションの N4 セッション変更応答を送信します。

**ユースケース 2：コントロール サービス要求で UE がアクティブになる場合。**

1. PCF は、ルールおよび QoS が変更された PDU セッションのポリシー更新通知を SMF に送信します。PCF からの通知として受信されたアップデートされたポリシー ルールを SMF は、処理します。
2. SMF により「200 OK」ステータス コードが PCF に返されます。
3. SMF は、AMF への NAMF 通信 N1 N2 メッセージ転送サービス操作を使用して、変更されたルールと QoS の変更を含む N1 メッセージ PDU セッション変更コマンドのみを UE に送信します。
4. AMF は、NAMF Communication N1 N2 Message Transfer 応答を SMF に送信します。この応答には、「200 OK」のステータス コードおよび「ATTEMPTING_TO_REACH_UE」の原因が含まれます。
5. SMF は、UE への N1 - PDU セッション変更応答メッセージの再送信を停止します。さらに、N1 PDU 変更コマンド再送信タイマーを停止し、UE からの応答を待ちます。

6. AMF は UE に対するページング手順を開始し、UE は制御のサービス リクエスト メッセージでアクティブになります。
7. SMF は UE から N1 応答を受信します。
8. SMF は、N4 セッション変更リクエストを UPF に送信し、ユーザー プレーン トンネルの変更されたルールと QoS の詳細を更新します。その後、SMF は新しいルールの転送アクション ルール（FAR）アクションを「ドロップ」に設定します。
9. UPF は PDU セッションの N4 セッション変更リクエストを送信します。

## 標準準拠

CM アイドル状態または CM 接続状態の UE に対するネットワーク開始メッセージのサポートは 、*3GPP TS 23.502, V15.6.0 (2019-10)*に準拠しています。

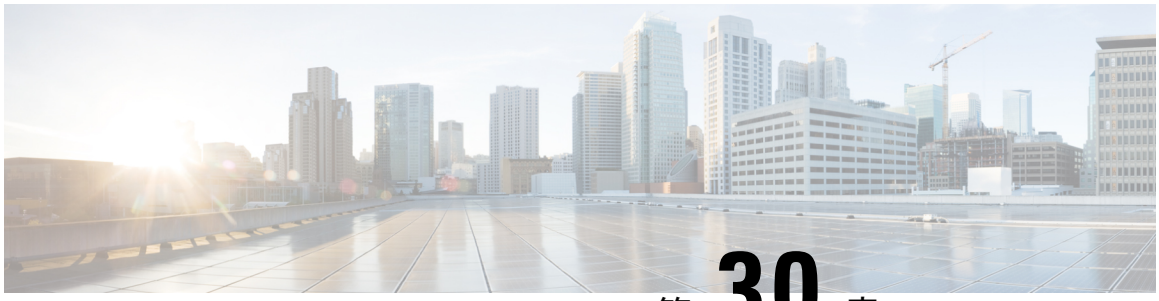
# OAM サポート

ここでは、この機能の操作、管理、およびメンテナンスに関して説明します。

## バルク統計サポート

SMFは、ネットワークによって開始された変更手順中にトリガーされる次の統計情報を保持します。

- UP コンテキストが非アクティブになったときにトリガーされた、ネットワークによって開始された変更の試行の合計数。
- UP コンテキストが非アクティブになったときにトリガーされた、ネットワークによって開始された変更の成功の合計数。
- UP コンテキストが非アクティブになったときにトリガーされた、ネットワークによって開始された変更の失敗の合計数。
- ネットワークによって開始された変更手順がトリガーされ、UPコンテキストが非アクティブ化されたときに受信された「ATTEMPTING_TO_REACH_UE」ステータスの総数。
- ネットワークによって開始された変更手順がトリガーされ、UPコンテキストが非アクティブになったときに受信された「N1N2_TRANSFER_INITIATED」ステータスの総数。



第 30 章

# 新しい無線デュアル接続


- 機能の概要と変更履歴 （1093 ページ）
- 機能説明 （1093 ページ）


# 機能の概要と変更履歴

## 要約データ

表 *358* : 要約データ

| | |
|---|---|
| 該当製品または機能エリア | SMF |
| 該当プラットフォーム | SMI |
| 機能のデフォルト設定 | 有効：常時オン |
| このリリースでの関連する変更点 | N/A |
| 関連資料 | 該当なし |

## 更新履歴

表 *359* : マニュアルの変更履歴

| 改訂の詳細 | リリース |
|---|---|
| 最初の導入。 | 2021.02.0 |

# 機能説明

新しい無線デュアル接続（NR-DC）は、5Gスタンドアロン コアを使用したデュアル接続構成です。この構成では、プライマリRANノードとセカンダリ RAN ノードの両方が5G gNBです。

SMF は NR-DC とともに 5G アグリゲーションをサポートし、より高い 5G データ レートを実現します。

この機能には、以下の重要なポイントがあります：

- データ トラフィックにのみ NR-DC を使用する
- データ トラフィックにはデフォルト フローのみを使用する
- トンネルは1つで十分です
- SMF には構成は不要です

NR-DC の機能は、ローミングと非ローミングの両方のシナリオに適用できます。

# 機能の仕組み

RAN が開始した QoS フローは、プライマリ ノード（PN）からセカンダリ ノード（SN）にオフロードされます。フローが作成された後、PN はトラフィックを SN に切り替える場合があります。SN は新しい DL TEID を割り当て、PN に送信します。次に、PN はその DL TEID で PDU セッションのリソース変更要求を開始します。SMF は DL FAR のみを更新して、トラフィックを SN に切り替えます。SN から PN への切り替えが発生する可能性があります。ただし、SMF の動作に変更はありません。

## コール フロー

このセクションでは、PN から SN への RAN 開始 QoS フロー オフロードのコール フローについて説明します。

### RAN が開始した QoS フローのオフロード コール フロー

このセクションでは、PN から SN への RAN 開始 QoS フロー オフロードのコール フローについて説明します。

図 *195 : RAN* が開始した *QoS* フローのオフロード コール フロー

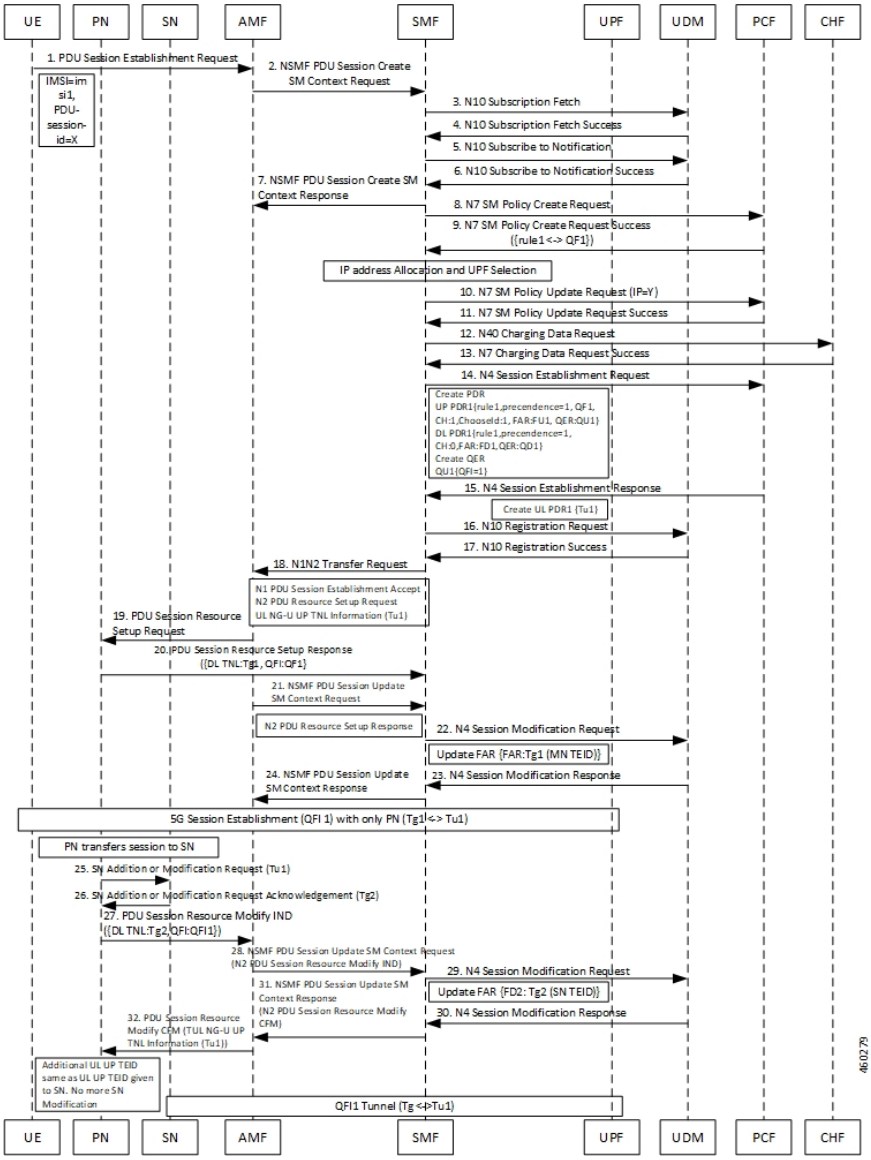
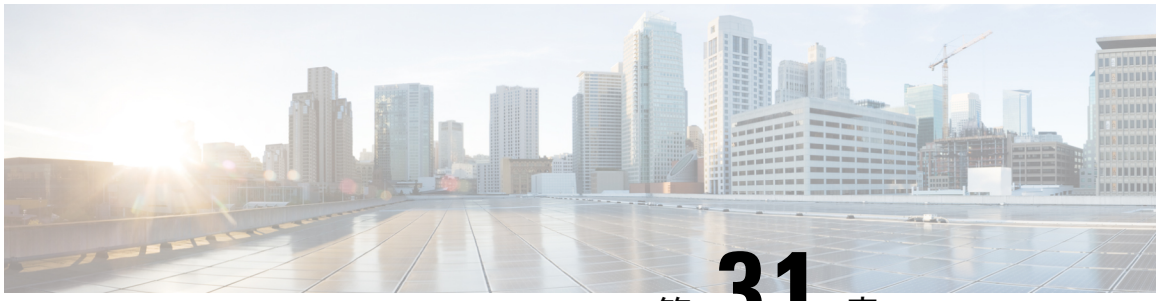



表 *360 : RAN* が開始した *QoS* フロー オフロード コール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | UE は、PDU セッション確立要求を AMF に送信します。 |
| 2 | AMF は、NSMF PDU セッション SM 作成コンテキスト要求を SMF に送信します。 |
| 3 | SMF は、N10 登録要求を UDM に送信します。 |
| 4 | UDM が SMF に N10 登録の成功通告を送信します。 |

| ステップ | 説明 |
|---|---|
| 5 | SMF は N10 サブスクリプション取得メッセージを UDM に送信します。 |
| 6 | UDM は SMF に N10 サブスクリプション取得成功の確認応答を送信します。 |
| 7 | SMF は、N10 Subscribe to Notification メッセージを UDM に送信します。 |
| 8 | UDM が SMF に N10 通告への登録の成功通告を送信します。 |
| 9 | SMF は、NSMF PDU セッション 作成 SM コンテキスト応答を AMF に送信します。 |
| 10 | SMF は、N7 SM ポリシー作成要求を PCF に送信します。 |
| 11 | PCF は、N7 SM ポリシー作成要求成功の通告を SMF に送信します。 |
| 12 | IP アドレスの割り当てと UPF の選択に基づいて、SMF は N7 SM ポリシー更新要求を PCF に送信します。 |
| 13 | PCF は、N7 SM ポリシー アップデート要求の成功通告を SMF に送信します。 |
| 14 | SMF は N40 課金データ要求を CHF に送信します。 |
| 15 | CHF は、N7 課金データ要求成功の応答を SMF に送信します。 |
| 16 | SMF は、N4 セッション確立要求を UPF に送信します。 |
| 17 | UPF は N4 セッション確立応答を SMF に送信します。 |
| 18 | SMF は、N1N2 転送要求を AMF に送信します。 |
| 19 | AMF は、PN に PDU セッション リソースセットアップ要求を送信します。 |
| 20 | PN は、DL トンネルおよび QFI 情報とともに、PDU セッション リソース設定応答通知を SMF に送信します。 |
| 21 | AMF は、NSMF PDU セッション更新 SM コンテキスト要求を SMF に送信します。 |
| 22 | SMF は、N4 セッション変更要求を UPF に送信します。 |
| 23 | UPF が SMF に N4 セッション変更応答メッセージを送信します。 |
| 24 | SMF は、NSMF PDU セッション アップデート SM コンテキスト応答を AMF に送信します。 |
| 25 | 5G セッションが PN のみで確立された後、PN はセッションを SN に転送します。次に、PN は追加要求または変更要求を SN に送信します。 |
| 26 | SN は追加または変更要求の確認応答を PN に送信します。 |
| 27 | PN は、PDU セッション リソース変更指示メッセージを AMF に送信します。 |

| ステップ | 説明 |
|---|---|
| 28 | AMF は、NSMF PDU セッション更新 SM コンテキスト要求を SMF に送信します。 |
| 29 | SMF は、N4 セッション変更要求を UPF に送信します。 |
| 30 | UPF が SMF に N4 セッション変更応答メッセージを送信します。 |
| 31 | SMF は、NSMF PDU セッション アップデート SM コンテキスト応答を AMF に送信します。 |
| 32 | AMF は、PN に PDU セッション リソース変更 CFM 要求を送信します。別の UL UP TEID は SN に提供される UL UP TEID と同じままであり、SN を変更する必要はありません。QFI1 トンネルは SN から UPF へ使用できます。 |



第 31 章

# NF の検出と管理


- 機能の概要と変更履歴, on page 1099
- 機能説明 （1100 ページ）
- NF 管理 （1101 ページ）
- NF ディスカバリ （1123 ページ）
- 代替 AMF の選択 （1145 ページ）
- ピア NF 管理の静的構成 （1147 ページ）
- NRF 障害の処理, on page 1153


## 機能の概要と変更履歴

### 要約データ

***Table 361:*** 要約データ

| | |
|---|---|
| 該当製品または機能エリア | SMF |
| 該当プラットフォーム | SMI |
| 機能のデフォルト設定 | 有効：常時オン |
| このリリースでの関連する変更点 | N/A |
| 関連資料 | 該当なし |

# 更新履歴

*Table 362:* マニュアルの変更履歴

| 改訂の詳細 | リリース |
|---|---|
| NRF 管理と SMF ローカリティを NRF エンドポイントに関連付ける一環として、NRFのメッセージ処理プロファイルが追加されました。 | 2023.03.0 |
| 分割および DNN 機能ごとの IP プール割り当ての一部として、NRF 登録および検出の構成手順を追加しました。 | 2022.04.0 |
| 次の機能のサポートが追加されました。<br>• 特定のエラー コードに対して構成可能な再試行アクション。<br>• エラー コードに関連付けられた再試行アクションの柔軟なオプション。<br>• NF の失敗処理テンプレートの Httpv2 ステータス コード範囲。 | 2021.02.0 |
| NRF 通知による個々の NF プロファイル メンバーの変更のサポートが導入されました。<br>NRF 検出クエリの一部として、次の新しいパラメータが追加されました。<br>• limit<br>• 最大ペイロード サイズ<br>• リクエスタの VRF | 2020.03.0 |
| 最初の導入。 | 2020.02.0 より前 |

# 機能説明

ネットワーク機能（NF）リポジトリ機能（NRF）は、次の機能をサポートしています。

- 使用可能な NF インスタンスとサポートされているサービスの NF プロファイルを維持します。
- 他の NF インスタンスが、特定のタイプの新しい NF インスタンスの NRF で登録し、その登録に関する通知を取得できるようにします。

- サービス検出機能をサポートします。NF インスタンスから NF 検出要求を受信し、特定の基準を満たす（特定のサービスのサポートなど）使用可能な NF インスタンスの情報を提供します。

# NF 管理

## 機能説明

ここでは、SMF がサポートする NF 管理の手順とその構成について説明します。これらの手順は、NF 登録、NF 登録解除、NF ハートビート、および NF 更新です。NF 登録、更新、およびハートビートは、選択されたプライマリ ノードである rest-ep ポッドの 1 つだけから送信されます。このノードが選択されると、ポッドがクラッシュまたは削除されるまで、インスタンスは NF 管理アクティビティのプライマリ ノードのままになります。

NF 管理はダイナミックな構成変更をサポートします。したがって、トランザクション/手順の途中で構成が変更されると、進行中のトランザクションが影響を受けます。

ダイナミックな構成変更機能は、次をサポートします。

- NRF トランザクション/プロシージャは構成バージョン（v1）を選択し、NRF トランザクション/プロシージャが完了するまで同じバージョンを使用します。
- 継続されている NRF トランザクション中に構成を変更した場合、新しい構成バージョン（v2）が作成されます。ただし、新しい構成は新しいトランザクションに適用されます。

ダイナミック構成変更は、次のデータ構造に適用します：

- NrfFailureProfileSt
- NrfClntProfileSt
- NrfGrpSt
- NrfPairProfileSt
- NrfMgmtGrpSt

## 登録

SMF が NRF に登録されます。NRF への登録中に、SMF は NF プロファイルに FQDN、IPv4 または IPv6 アドレスなどのアドレッシング パラメータのうち少なくとも 1 つを含めます。NF プロファイル登録には、少なくとも 1 つのアドレッシング パラメータを含める必要があります。SMF が「https」uri スキームをサポートしている場合、SMF は NFProfile または NFService で FQDN を提供します。

# NF 管理用の NRF エンドポイント プロファイル パラメータの構成

SMF は、**nnrf-nfm**（NF 管理）の NRF エンドポイントを構成するための CLI を提供します。

**Note** NF 管理では、 **nnrf-nfm** サービスのみを構成できます。

CLI設定では、各エンドポイントプロファイルの下で複数のエンドポイントを構成できます。SMFは、優先順位とキャパシティのパラメータを使用して、これらのエンドポイント間でロードバランシングを行います。各エンドポイント内にプライマリ、セカンダリ、およびターシャリ ホスト [ip:port] を構成できます。IPv4 アドレスと IPv6 アドレスの両方を指定できます。両方が指定されている場合は、IPv4 アドレスが優先されます。

URI はリソースを一意に識別します。5GC SBI API では、リソース URI が絶対 URI の場合、その構造は次のように指定されます。

```
{apiRoot}/{apiName}/{apiVersion}/{apiSpecificResourceUriPart}
```

**Note** このリリースの仕様では、HTTP と HTTPS の両方のスキーム URI が許可されています。サービスベースのインターフェイスのセキュリティの詳細については、*3GPP TS 33.501* の *13.1* 項を参照してください。

「apiRoot」 は、schema（「http」または「https」）の連結です。

- 固定文字列「://」
- IETF RFC 3986 で定義されている権限（ホストおよびオプションのポート）
- 「/」文字で始まるオプションの展開固有の文字列（APIプレフィックス）（CLIのapi-root）

NRF でサポートされているさまざまなサービスの NRF エンドポイントを構成するには、次の構成例を使用します。

```
config
  group nrf mgmt mgmt_name
    service type nrf nnrf-nfm
      endpoint-profile epprofile_name
        priority priority_value
        capacity capacity
        api-root api_string
        api-uri-prefix uri_prefix_string
        uri-scheme { http | https }
        endpoint-name ep_name { capacity capacity | primary ip-address
        { ipv4 ipv4_address | ipv6 ipv6_address | port port_num}
        | secondary ip-address { ipv4 ipv4_address | ipv6 ipv6_address
        | port port_num } | tertiary ip-address { ipv4 ipv4_address
        | ipv6ipv6_address | port port_num } }
        version [ uri-version version_num full version version_num ]
        end
```

注：

- **group nrf mgmt** *mgmt_name* ：NRF 自己管理グループの構成を表示します。
- **api-root** *api_string*：: apiRoot 内で使用される展開固有のサービス API プレフィックスを指定します。
- **api-uri-prefix** *uri_prefix_string*：6apiName を指定します。構成されていない場合は、仕様に従ってサービスの標準 API 名を使用します。
- **capacity** *[capacity]*：プロファイルの容量を指定します。
- **endpoint-name** *ep_name* **{ capacity** *capacity* **| primary ip-address { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **| port** *port_num* **} | secondary ip-address { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **| port** *port_num* **} | tertiary ip-address { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **| port** *port_num* **} }**：エンドポイント名を指定します。NF サーバのフェールオーバー処理のために、各エンドポイント内のプライマリ ホスト、セカンダリ ホスト、およびターシャリ ホスト（IP：ポート）を構成できます。サーバ フェールオーバー構成は、IPv4 アドレスと IPv6 アドレスの両方を受け入れます。ただし、SMF では IPv4 アドレスが優先されます。
- **capacity***capacity*：エンドポイントのノード キャパシティを指定します。 *capacity* は 0 ～ 65535 の範囲の整数である必要があります。
- メッセージを送信するためのエンドポイントの選択は、優先順位およびキャパシティのパラメータを使用する確率論的ロード バランシング アルゴリズム（IETF RFC 2782）に基づいています。
- **primary ip-address { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **| port** *port_num* **}**：プライマリ エンドポイントの IPv4 アドレス、IPv6 アドレス、またはポートを指定します。
- **secondary ip-address { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **| port** *port_num* **}**：セカンダリ エンドポイントの IPv4 アドレス、IPv6 アドレス、またはポートを指定します。
- **tertiary ip-address { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **| port** *port_num* **}**：ターシャリ エンドポイン トの IPv4 アドレス、IPv6 アドレス、またはポートを指定します。
- **priority***priority_value*：サービスがロードバランシング ロジックを使用して適切なプロファイルを選択するための優先順位を指定します。 *priority* は 0 ～ 65535 の範囲の整数である必要があります。
- **uri-scheme { http | https }**： **http** または **https**として URI スキームを指定します。
- **version [ uri-version** *version_num* **full version** *version_num* **]**：API/バージョンを指定します。完全バージョンの形式は次のとおりです。
  <Major-version>.<Minor-version>.<patch-version>.[alpha-<draft-number>].

## NF 管理用の NF エンドポイント プロファイル パラメータの確認

**show running-config group nrf** コマンドを使用して、NF 管理用の NF エンドポイント プロファイル パラメータを確認します。

```
show running-config group nrf
group nrf mgmt mgmt_group
```

```
 service type nrf nnrf-nfm
  endpoint-profile epprof
  uri-scheme http
   endpoint-name EP1
   priority       2
   primary ip-address ipv4 209.165.200.231
   primary ip-address port 8082
   secondary ip-address ipv4 209.165.200.232
   secondary ip-address port 8082
 exit
   endpoint-name EP2
      priority 10
       primary ip-address ipv4 209.165.200.231
       primary ip-address port 8082
       secondary ip-address ipv4 209.165.200.232
       secondary ip-address port 8082
     exit
   exit
 exit
exit
```

# 最適化された NRF 登録要求メッセージを使用したスライス使用率の向上

**表 *363 :* 機能の履歴**

| 機能名 | リリース情報 | 説明 |
|---|---|---|
| 最適化された NRF 登録要求メッセージ | 2024.02.1 | NRF 登録要求メッセージの **smfInfoList** 属性のサイズは、TAC グループに基づいてそのサブ属性をグループ化することによって縮小されます。<br>メッセージ属性をグループ化することにより、サービス プロバイダ スライスの展開をスケールアップして追加のサービスを提供できます。<br>**smfInfoList の** 最適化は、 **ie smfinfolist tac-based** コマンドを NRF メッセージ処理プロファイル コンフィギュレーション モードで使用して有効にします。 |

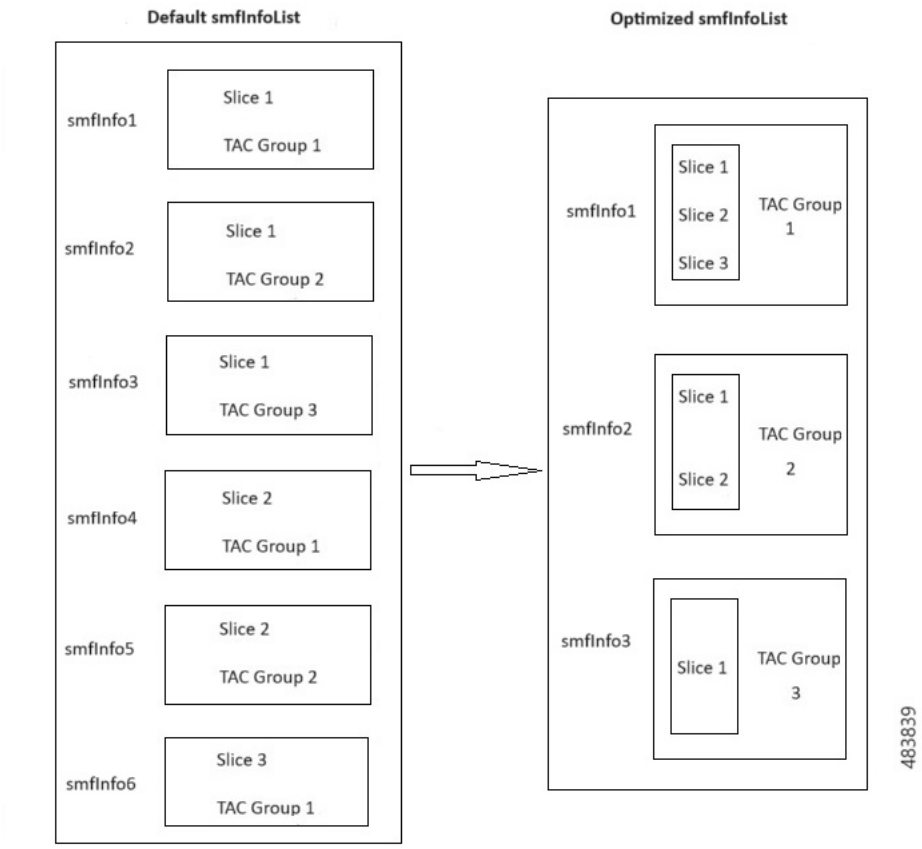
## 概要

SMF は、 **smfInfo** の複数のエントリを含む **smfInfoList**属性を使用して、NRF に登録要求メッセージを送信します。各**smfInfo** 属性には、スライス、DNN、TAC グループなどに関する情報を伝送するサブ属性が含まれます。

デフォルトでは、1 つの **smfInfo** 属性に、単一のスライスと単一の **TAC グループ** 情報が含まれます。スライス、DNN、TAC グループは共有属性ですが、すべての共有メッセージ情報に対応するには複数の **smfInfo** エントリが必要です。

この機能は、TAC グループに基づいて **smfInfo** 属性をグループ化します。1 つの TAC グループに対応するすべての共通要素が 1 つの **smfInfo** エントリに入るように属性が分類されます。共通メッセージ属性をグループ化すると、既存のメッセージ属性をより少ない **smfInfo** 要素に収容できます。

図 *196 : NRF* 登録要求での *smfInfoList* の最適化




**smfInfoList** を最適化すると、同じメッセージ情報を収容するのに必要な **smfInfo** エントリの数が減少します。これにより、NRF 登録要求で送信される **smfInfoList** のサイズが削減され、**smfInfoList** 内の制限された数の **smfInfo**エントリ内に追加のスライスの詳細を追加できるようになります。

（注） この機能は下位互換性があります。

## TAC グループに基づく smfInfoList グループ化の有効化

TAC グループに基づいて smfInfoList グループ化を有効にするには、次の構成例を使用します：

```
config
  profile message-handling message_handling_name
    nf-type nrf
      mh-profile mh_profile_name
        service name type { nnrf-at | nnrf-bs | nnrf-nfd | nnrf-nfm
}
```

```
            message type { nf-deregister | nf-list-retrieval |
nf-profile-retrieval | nf-register | nf-status-notify |
nf-status-subscribe | nf-status-unsubscribe | nf-updatenf-register }
                ie smfinfolist tac-based
                end
```

注：

- **ie smfinfolist**：グループ化される **smfInfoList** 情報要素を指定します。

  **tac-based**：TAC グループに基づいて **smfInfoList** 情報要素をグループ化します。

（注） この構成は、新しいスライスまたは TAC グループ情報を追加する場合にのみ使用することをお勧めします。

# NRF による SMF の登録解除

## 機能説明

SMF は、ネットワーク機能（NF）リポジトリ機能（NRF）の登録解除をサポートしています。SMF の NF 登録解除サービス操作により、NRF に登録されているネットワーク機能のプロファイルが削除されます。

SMF 、次のシナリオで NF 登録解除サービス操作を開始します。

- サービス ベースのインターフェイス (SBI) エンドポイントが構成されておらず、残りのすべてのエンドポイントが機能を停止している場合。
- 構成されたすべての SBI エンドポイントの VIP IP と N11 VIP IP がオフラインの場合。

**Note** すべての REST エンドポイントが機能を突然停止した場合、SMF は NRF の登録解除を実行できません。REST エンドポイントのみが NRF の登録または登録解除を実行できます。

## 機能の仕組み

NF 登録解除操作では、NF インスタンス ID に基づいて特定のリソースを削除します。NF の登録解除は、Uniform Resource Identifier（URI）が特定の NF インスタンスを削除する要求を受信すると開始されます。

推奨される SMF シャットダウン プロセスには、次のステップが含まれます。

1. すべての N11 および SBI VIP IP がオフラインとしてマークされます。これらのエンドポイントがオフラインで表示されると、NF 登録解除要求が NRF に送信されます。NRF は、SMFシャットダウンとトラフィックでのその使用不可について、ピア NF（AMF など）に通知します。

2. コンバージェンスを許可するまでの猶予期間を待ち、「システム モードシャットダウン」を実行してすべてのポッドを停止します。

エンドポイント SBI が構成されていない場合、システムは rest-ep ポッドをすぐに削除し、適切なコンバージェンスを回避します。SBI および N11 VIP IP をオフラインにせずにシステム モードのシャットダウンを実施しても、コンバージェンスを回避できます。

## コール フロー

このセクションでは、次のコールフローについて説明します。

- NRF 登録解除コール フロー
- NRF 登録解除トリガー イベントのコール フロー

### *NRF* 登録解除コール フロー

ここでは、NF の登録解除 コール フローについて説明します。

***Figure 197: NRF* 登録解除コール フロー**

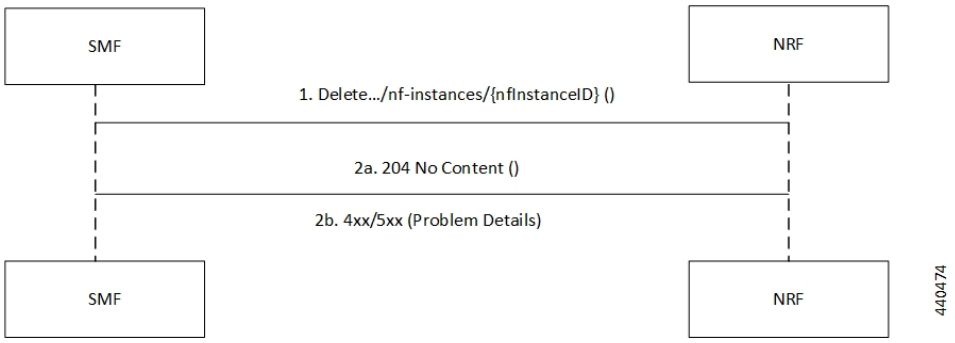



***Table 364: NRF* 登録解除コール フロー詳細**

| ステップ | 説明 |
|---|---|
| 1 | SMF は、NF インスタンスを示す技術情報 URI に削除要求を送信します。リクエスト本文が空です。 |
| 2a | 指定されたリソースの削除に成功すると、「204 No Content」というメッセージが表示されます。応答本文は空のままです。 |
| 2b | 「nfInstanceID」で識別される NF インスタンスが NRF のデータベースの登録済み NF インスタンスのリストで見つからない場合、NRF は「404 Not Found」ステータス コードを返して ProblemDetails IE にエラーの詳細を示します。 |

### *NF* 登録解除トリガー イベント コール フロー

ここでは、NF の登録解除トリガー イベント コール フローについて説明します。

*Figure 198: NF 登録解除トリガー イベント コール フロー*

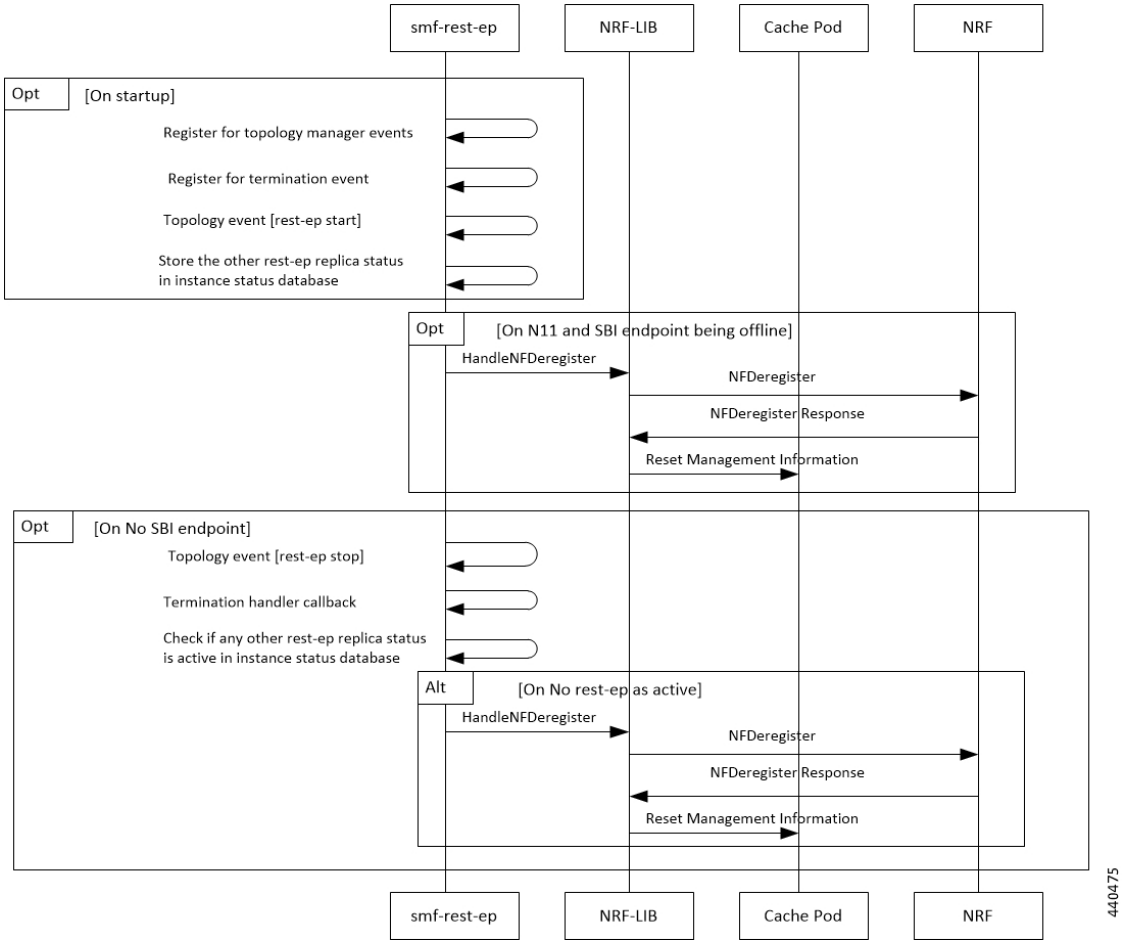



*Table 365: NF 登録解除トリガー イベント コール フローの説明*

| ステップ | 説明 |
|---|---|
| 起動時 | |
| 1 | SMF rest-ep は、トポロジ マネージャ イベントを登録して他の rest-ep インスタンスの状態を識別し、インスタンス状態データベースにこれらのインスタンスを追跡します。 |
| 2 | SMF rest-ep は、アプリケーション インフラストラクチャが機能を停止したときに通知を受信するための終了ハンドラのために、アプリケーションインフラストラクチャに登録します。終了ハンドラの一部として、SMF rest-ep は他の動作している rest-ep のインスタンス状態データベースをモニターします。 |
| 3 | SMF rest-ep はトポロジ イベントを開始します。 |

| ステップ | 説明 |
|---|---|
| 4 | SMF rest-ep は、他の rest-ep レプリカのステータスをインスタンス状態データベースに保存します。 |
| N11 と SBI エンドポイントがオフラインの場合 | |
| 5 | SMF rest-ep は Handle NF deregister メッセージを NRF-Lib に送信します。 |
| 6 | すべての SBI および N11 VIP IP エンドポイントがオフラインの場合、SMF rest-ep は登録解除要求を NRF に送信します。 |
| 7 | NRF は、NF 登録解除応答を NRF-Lib に送信します。 |
| 8 | NRF-Lib は、キャッシュ ポッドで構成されているすべての管理情報をリセットします。 |
| SBI エンドポイントが存在しない場合 | |
| 9 | SMF rest-ep はトポロジ イベントを開始して、他の rest-ep を停止します。 |
| 10 | SMF rest-ep は終了ハンドラのコールバックを開始します。 |
| 11 | AMF rest-ep は、他の動作している SMF rest-ep のインスタンス ステータス データベースをチェックします。 |
| rest-ep が機能していない場合 | |
| 12 | SMF rest-ep は Handle NF deregister メッセージを NRF-Lib に送信します。 |
| 13 | SMF rest-ep は登録解除要求を NRF に送信します。 |
| 14 | NRF は、NF 登録解除応答を NRF-Lib に送信します。 |
| 15 | NRF-Lib は、キャッシュ ポッドで構成されているすべての管理情報をリセットします。 |

## 標準準拠

NRF 機能付き SMF 登録解除は、以下の基準に準拠しています：

- *3GPP TS 29.510* バージョン *15.4.0*。*5G* システム ネットワーク機能リポジトリ サービス。第 *3* 段階

## 制限事項

NRF 機能を使用した SMF 登録解除には、次の制限があります。

- N11 および SBI VIP IP がオフラインとマークされていない場合、ポッドを削除するための特定の順序が存在しないため、NF 登録解除はシステム モード シャットダウンで送信されません。さらに、rest-ep ポッドが機能しているかどうかを確認するためのモニタリング手順は存在しません。

# NF ハートビート

## 機能説明

NF ハートビート機能は、NF は NRF に対して NF が正常に動作していることを通知できます。NRF に登録されている各 NF は、NF 更新サービス操作を呼び出すことによって、定期的に NRF と接続します。NRF が連絡を受ける時間間隔は展開固有であり、NRF は登録が成功した結果として、その時間間隔を SMF に返します。

SMF は 、NF ハートビートの一部として NF ステータスと負荷パラメータを NRF に送信します。SMF は、 定期的な NF ハートビートの間隔を構成する CLI を提供します。NF 登録応答でハートビート値が構成されている場合、同じ値が別の構成値の代わりに使用されます。

### NF ハートビート間隔

SMF NF ハートビート機能は、SMF が動作していることを NRF に通知します。デフォルトのハートビート間隔は 10 秒です。 **heartbeat interval** CLI コマンドを使用して、ハートビートの間隔（秒単位）を構成できます。NRF が NF 登録応答またはハートビート応答の一部として別のハートビート時間値を返す場合、後続のハートビートには同じ間隔が使用されます。ハートビートの一部として、NRF は NF インスタンスを表す技術情報 URI に HTTP パッチ要求を送信します。PATCH 要求のペイロード本文には、NF インスタンスの NF プロファイルの「nfStatus」属性に対する「置換」操作が含まれており、「REGISTERED」値に構成されます。このリリースは、負荷や容量などのパラメータをサポートしていません。

（注） SMF は構成されたハートビートを使用します。ハートビートが構成されていない場合、SMF はローカルに構成されたハートビートを使用します。

## 機能の仕組み

### コール フロー

*NF* ハートビートのコール フロー

次の図は、NF ハートビートのフローを示しています。

*Figure 199: NF* ハートビートのコールフロー

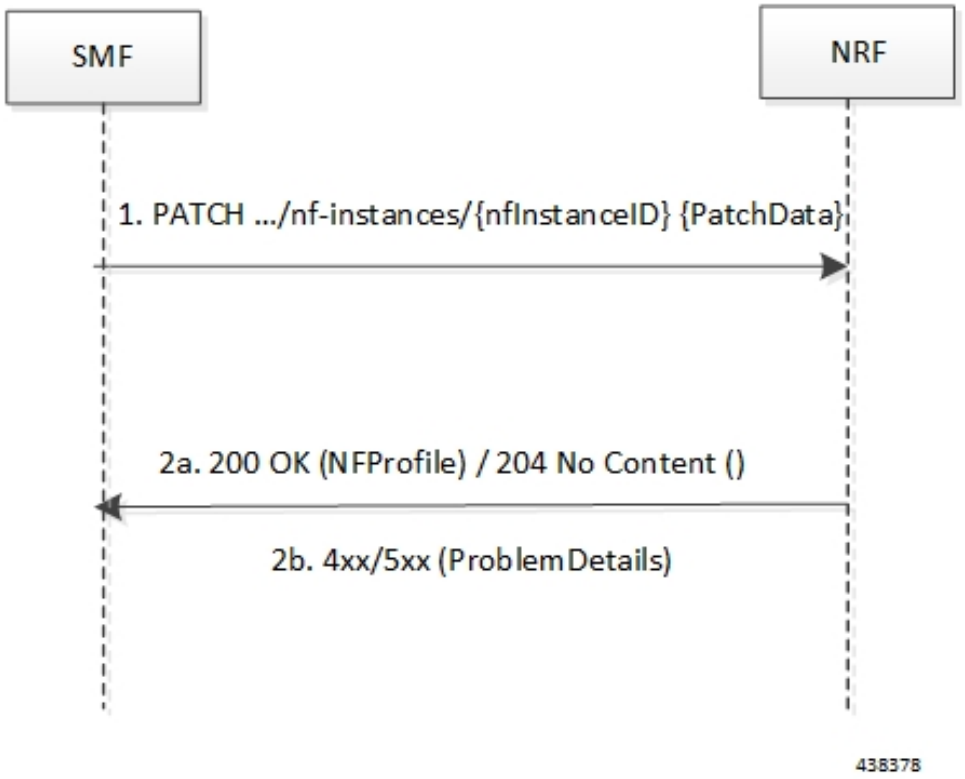



*Table 366: NF* ハートビートのコールフロー説明

| ステップ | 説明 |
|---|---|
| 1 | NF サービス コンシューマは、NF インスタンスを表すリソース URI に PATCH 要求を送信します。PATCH 要求のペイロード本文には、NF インスタンスの NF プロファイルの nfStatus 属性に対する置換操作が含まれており、REGISTERED の値に設定されています。 |
| 2 | 成功すると、NF プロファイルが変更されると、NRF は、応答本文で完全な NF プロファイル データとともに「200 OK」を返します。それ以外の場合は、「204 No Content」が返されます。 |

| ステップ | 説明 |
|---|---|
| 3 | 「nfInstanceID」で識別される NF インスタンスが NRF のデータベースの登録済み NF インスタンスのリストで見つからない場合、NRF は「404 Not Found」ステータス コードを返して ProblemDetails IE にエラーの詳細を示します。例：<br>**PATCH .../nf-instances/4947a69a-f61b-4bc1-b9da-47c9c5d14b64**<br>**Content-Type: application/json-patch+json**<br>**[**<br>**{"op": "replace", "path": "/nfStatus", "value": "REGISTERED"}**<br>**]**<br>**HTTP/2 204 No Content**<br>**Content-Location:**<br>**.../nf-instances/4947a69a-f61b-4bc1-b9da-47c9c5d14b64** |

### 標準準拠

NF ハートビート機能は、次の標準規格に準拠しています：

- *3GPP TS 29.510*、バージョン *15.4.0*（*2019* 年 *7* 月）：*5G* システム ネットワーク機能リポジトリ サービス第 *3* 段階

## NRF ハートビート 間隔を構成

ここでは、NRF ハートビート間隔の構成方法について説明します。

```
config
  group nf-mgmt nf_mgt_name
    hearbeat interval  hearbeat_interval
  end
```

注：

- **group nf-mgmt** *nf_mgt_name*：NF 管理のグループ名を指定します。
- **hearbeat interval** *Heartbeat_interval*：ハートビート間のハートビートの間隔を指定します。ハートビート間隔（秒）の値。

（注） NRF が NF 登録応答またはハートビート応答の一部として別のハートビート間隔値を返す場合、後続のハートビートには同じ値が使用されます。

# SMF サブスクリプションおよび通知の NRF サポート

## 機能説明

SMF は、NFR が提供するサブスクライブ サービスを使用して、NF が検出応答として受信する NF インスタンスのステータスの変更をサブスクライブします。この機能は、キャッシュされた NF 検出応答の更新に役立ちます。

SMF 、NF レベルおよびサービス レベルでの負荷、容量、ステータスの通知変更のみを受け入れます。通知内のその他のパラメータの変更はすべて無視されます。

通知サービスのサブスクリプションが成功すると、 SMF NF インスタンスの登録および登録解除の通知、または指定された NF インスタンスの NF プロファイル変更の通知を受信します。

SMF 、「NotificationData」の「NFProfile」フィールドと「ChangeItem」フィールドをサポートします。通知イベントタイプが「NF_PROFILE_CHANGED」に設定されている場合、 SMF 、プロファイル レベルの変更に関する通知、または NFProfile パラメータの個々の変更項目のリストを nfInstanceUri と共に受信します。

「ChangeItem」フィールドには、次のパラメータが含まれます：

- op：リソースに発生する変更のタイプを示します。
- path：リソース内のターゲット場所を示す JSON ポインタ値が含まれます。
- from：「path」属性で示される場所に移動またはコピーされる JSON 要素のパスを示します。「op」属性の値が「MOVE」の場合に存在します。
- origValue：「パス」属性で指定されたリソース内のターゲット位置での元の値を示します。
- newValue：「パス」属性で指定されたリソース内のターゲットロケーションの新しい値を示します。

**Note** SMF 現在、「op」パラメータの一部として、ADD、REPLACE、および REMOVE 操作のみをサポートしています。

次に、最初の NF サービスの最初のエンドポイントの IP アドレス値と TCP ポートを更新して、NF インスタンスがそのプロファイルを変更した場合に、NRF から送信される通知ペイロードの例を示します。

例 1：

```
{
  "event": "NF_PROFILE_CHANGED",
  "nfInstanceUri": ".../nf-instances/4947a69a-f61b-4bc1-b9da-47c9c5d14b64",
  "profileChanges": [
    {
      "op": "REPLACE",
     "path": "/nfServices/0/ipEndPoints/0/ipAddress", ===> Change ipAddress to ipv4Address
```

```
      "newValue": "209.165.201.10"
    },
    {
      "op": "REPLACE",
      "path": "/nfServices/0/ipEndPoints/0/port",
      "newValue": 8080
    }
  ]
```

例 2：

```
{
"event": "NF_PROFILE_CHANGED",
"nfInstanceUri": ".../nf-instances/4947a69a-f61b-4bc1-b9da-47c9c5d14b64",
"nfProfile": <Newly updated complete profile>
}
```

## 機能の仕組み

この機能は、NF サブスクライブ サービスを使用して、NF が検出応答として受信する NF インスタンスのステータスの変更をサブスクライブします。SMF は、検出応答で受信する各 NF プロファイルの応答有効期間のサブスクリプションを送信します。SMF は、現在の応答時間の有効性に応じて、既存の NF インスタンスのサブスクリプション時間に延長が必要かどうかを確認します。サブスクリプションに拡張が必要な場合は、拡張された有効期間が設定されたサブスクリプション PATCH が送信されます。

サブスクリプション中に、NRF は変更された有効期間で応答する場合があります。この有効時間は、SMF の有効時間リクエストとは異なる場合があります。このようなシナリオでは、SMF は、必要なサブスクリプション時間と、NRF によって返される実際のサブスクリプション時間を追跡します。

SMF は、実際のサブスクリプション期間がすぐに終了するが（次の5分で終了）、必要な有効期間が実際の有効期間よりも長いサブスクリプションがあるかどうかを定期的に（2分ごとに）データベースにチェックします。この場合、SMF は PATCH サブスクリプションを送信してサブスクリプションの有効時間を延長します。

SMF は、構成で指定されたインターフェイス NRF の構成に基づいてステータス通知 URI を入力します。通知 VIP IP および VIP ポートは、ステータス通知 URI をフレーム化するために使用されます。

```
http://{nrfinterface.vip-ip}:{ nrfinterface.vip-port}/{notifResourceURI}
```

ステータス通知時に、SMF は変更された属性でローカル キャッシュと外部キャッシュ（キャッシュ ポッド）を更新します。

### コール フロー

ここでは、SMF サブスクリプションと通知機能の主要なコール フローについて説明します。

サブスクリプション（*PATCH*）コール フロー

NRF は、指定された期間の有効期限が切れる場合に、NF インスタンスの通知へのサブスクリプションを更新して有効時間をリフレッシュします。SMF は、NRF に対して新しい有効期間

を要求できます。操作が成功した場合、NRF は新しい有効時間を NF に割り当て、提供できます。

「subscriptionID」リソースを更新すると、サブスクリプション（PATCH）操作が開始されます。操作は、個々のリソースを表す URI で HTTP PATCH 要求を発行することにより開始されます。

次の図は、同じ PLMN 内の NF インスタンスにサブスクリプションするためのコール フローを示しています。

***Figure 200:*** サブスクリプション（***PATCH***）コール フロー

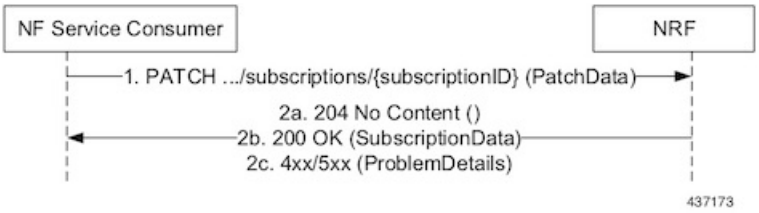



***Table 367:*** サブスクリプション（***PATCH***）コール フロー

| ステップ | 説明 |
|---|---|
| 1 | SMF は、個々のサブスクリプション リソースを識別するリソース URI に PATCH 要求を送信します。PATCH 要求のペイロード本文には、SubscriptionData 構造の「validityTime」属性に対する「replace」操作が含まれています。要求には、「validityTime」属性の新しい推奨値も含まれています。この置換操作によってリソースの他の属性が置き換えられることはありません。 |
| 2a | サブスクリプションが成功すると、NRF は「204 No Content」応答を送信します。この応答は、NRF が以下を受け入れることを示します。<br>• サブスクリプション期間の延長<br>• 「validityTime」属性の値 |
| 2b | 要求本文の JSON パッチ オブジェクトのエラーが原因でサブスクリプションが失敗した場合、NRF は、問題の詳細を含む「400 Bad Request」ステータス コードを返します。 |
| 2c | NRF の内部エラーが原因でサブスクリプションが失敗した場合、NRF は問題の詳細とともに「500 Internal Server Error」を返します。<br>例：<br>`PATCH .../subscriptions/2a58bf47`<br>`Content-Type: application/json-patch+json`<br>`[`<br>`{ "op": "replace", "path": "/validityTime", "value": "2018-12-30T23:20:50Z" },`<br>`]` |

## サブスクリプション（*POST*）コール フロー

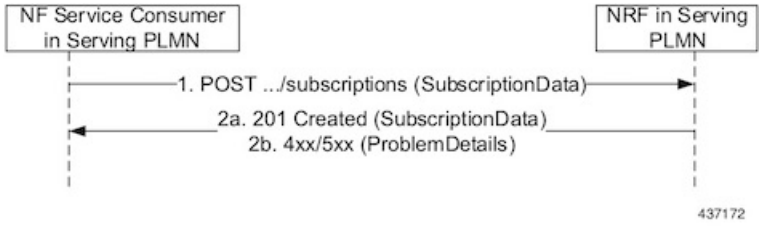
サブスクリプション サービスの操作により、次のことが可能になります：

- 次のようなシナリオで、SMF が（特定のフィルタに応じて）通知を要求できるようにサブスクリプションを作成します。
  - NRF での登録または登録解除がある場合。
  - プロファイルに変更があった場合。
- SMF が次のシナリオで通知を要求できるように、特定の NF インスタンスへのサブスクリプションを作成します：
  - NF インスタンスに変更がある場合。
  - NF インスタンスの登録解除があった場合。

**Important** 現在、SMF は、NF が検出応答として受信する NF インスタンスのサブスクリプションのみをサポートしています。

次の図は、同じ PLMN 内の NF インスタンスにサブスクリプションするためのコール フローを示しています。

***Figure 201:*** サブスクリプション（***POST***）コール フロー




NF インスタンスでの通知へのサブスクリプションを実装すると、収集リソース「subscriptions」の下に新しい個別のリソースが作成されます。POST 要求を発行すると、「サブスクリプション」リソースを表す Uniform Resource Identifier（URI）の操作が開始されます。

*Table 368:* サブスクリプション（*POST*）コール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | NF サービス コンシューマは、「サブスクリプション」収集リソースを表すリソース URI に POST 要求を送信します。<br>要求本文には、SMF が受信するようサブスクライブしている通知のタイプを示すデータを含めます。また、SMF が NRF から実際の通知を受信するための準備を行うコールバック URI も含まれています。通知には、SMF が推奨する有効期間が含まれます。これは、サブスクリプションがアクティブであり続ける期間を表します。<br>サブスクリプション要求には、モニタする（またはモニタリングから除外する）NF プロファイルの属性のリストを示す追加のパラメータも含まれる場合があります。この要求は、プロファイルのいずれかの属性に変更があった場合に、NRF が通知を送信する必要があるかどうかを決定します。<br>サブスクリプション データには、サブスクリプションの作成を要求する NF サービス コンシューマの NF タイプを含む **reqNfType** 属性も含まれます。NRF は要求を許可するためにこれを使用します。 |
| 2a | サブスクリプションが成功すると、NRF は「201 Created」応答を送信します。この応答には、サブスクリプションが無効になる、NRF で決定された有効期間を含む、新しく作成されたサブスクリプション データが含まれています。サブスクリプションが期限切れになると、SMF は NRF に新しいサブスクリプションを作成して、ステータス通知を引き続き受信します。 |
| 2b | サブスクリプション データのエラーが原因でサブスクリプションが失敗した場合、NRF は、問題の詳細とともに「400 Bad Request」ステータス コードを返します。<br>NRF の内部エラーが原因でサブスクリプションが失敗した場合、NRF は問題の詳細とともに「500 Internal Server Error」を返します。 |

## *NFStatus* 通知のコール フロー

サブスクライブされたさまざまな NF インスタンスの各コールバック URI に対して POST 要求が発行されると、 SMF NFStatus Notify オペレータを開始します。

次の図は、NFStatus Notify コール フローを示しています。

*Figure 202: NFStatus* 通知のコール フロー

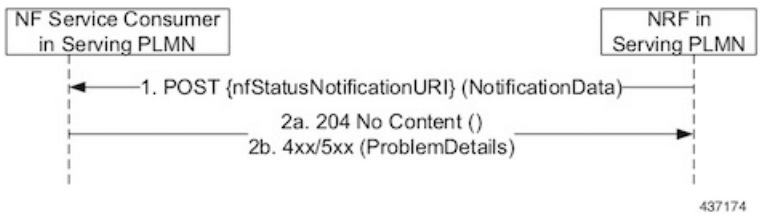


*Table 369: NFStatus Notify* コール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | NRF は、コールバック URI に POST 要求を送信します。<br>プロファイル変更通知要求の要求本文には、次のものが含まれます。<br>• **event**：この属性は、通知タイプを示します。次のいずれかを指定できます。<br>• NF_REGISTERED<br>• NF_DEREGISTERED<br>• NF_PROFILE_CHANGED<br>• **nfInstanceUri**：通知イベントに関連付けられている NF インスタンスの Uniform Resource Identifier（URI）。<br>• **nfProfile**：新しい NF プロファイルまたは更新された NF プロファイルを示します。<br>• **profileChanges**：この属性は、通知イベントに関連付けられた NF インスタンスのプロファイルの変更を識別します。この属性は、イベント通知タイプが「NF_PROFILE_CHANGED」の場合に使用できます。 |
| 2a | 通知が成功すると、NRF は「204 No Content」応答を送信します。 |
| 2b | SMF 有効な通知 URI として「nfStatusNotificationURI」を無視する場合、SMF は 問題の詳細とともに「404 Not Found」というステータス コードを返します。たとえば、URI が SMF が NRF で作成した既存のサブスクリプションのいずれにも属していない場合です。 |

## 制限事項

この機能には、次の制限事項があります。

- NF ステータス通知は、NF プロファイルの負荷、NF プロファイルのキャパシティ、NF プロファイルのステータス、サービスの負荷、サービスのキャパシティ、サービス ステータス パラメータの変更のみをサポートします。
- SMF 、「NotificationData」 の NFPofiile フィールドのみをサポートします。「項目の変更（Change item）」フィールドはサポートされていません。
- SMF は 、次のパラメータ変更の通知をサポートしています：
  - nfProfile
    - nfStatus
    - ipv4Address

- ipv6Address
- priority
- 容量
- 負荷

- nfService
  - version

**Note** 新しいバージョンへの変更は許可されていますが、既存のバージョンの削除や変更は許可されていません。

- スキーム

**Note** 現在、http のみがサポートされています

- nfServiceStatus
- ipEndPoints
- apiPrefix
- 容量
- 負荷
- priority

- SMF現在、「ChangeItem」フィールドの「op」パラメータの一部として、ADD、REPLACE、および REMOVE 操作のみをサポートしています。

## サブスクリプションおよび通知の NRF の構成

ここでは、サブスクリプションおよび通知用に NRF を構成する方法について説明します。

**Note** サブスクリプションと通知を機能させるには、SBIインターフェイス内にNRFインターフェイスを構成する必要があります。

NRF で検出を行うと、検出されたNFインスタンスのサブスクリプション メッセージが送信されます。SMF は、構成で指定された NRF インターフェイス構成に基づいてステータス通知 URL を入力します。通知 VIP IP と VIP ポートは、ステータス通知 URL をフレーム化するため

に使用されます。SMF は、ステータス通知のサブスクリプション要求メッセージに含まれている URL を使用します。

NF ステータス通知のためにサーバ エンドポイントを開くように NRF インターフェイス、vip-ip、vip-port、およびループバック ポートを構成するには、次の構成例を使用します。

```
config
  instance instance-id gr_instance_id
    endpoint sbi
      replicas replica_num
        vip-ip ip_address
      interface nrf
        vip-ip ip_address
        vip-port port_number
        loopbackPort port_number
        end
```

注：

- **interface nrf**：インターフェイスを NRF として指定します。
- **vip-ip** *ip_address*：仮想ホストの仮想 IP アドレスを指定します。SMF は、これをステータス通知のリスニング IP アドレスとして使用します。
- **vip-port** *port_number*：仮想ホストのポート番号を指定します。SMF はこれをステータス通知のリスニング ポートとして使用します。
- **loopbackPort** *port_number*：ループバック ホストの内部ポート番号を指定します。SMF はこのポートを NF ステータス通知に使用します。

## 標準準拠

本機能は、*3GPP TS 29.510*、バージョン *16.4.0*に準拠しています。

# NF プロファイルの更新

## 機能説明

SMF プロファイルの構成の変更によって NF 登録パラメータに変更があった場合、 SMF は NF 更新サービス操作を呼び出します。

NF 更新サービスは、要求元の NF の更新されたプロファイルを NRF に提供することによって、以前に NRF に登録されている NF プロファイルを更新します。

更新操作は次のいずれかになります：

- NF プロファイル全体の更新（既存のプロファイルを新しいプロファイルに完全に置き換える）
- NF プロファイル パラメータのサブセットのみの更新（NF プロファイルへのサービスの追加、削除、または置換）

# 機能の仕組み

このセクションでは、NF プロファイル更新手順を説明します。

## コール フロー

このセクションでは、次のコールフローについて説明します。

- NF プロファイルの完全な交換コール フロー （1121 ページ）
- NF 登録と NF 更新のコール フロー （1122 ページ）

### *NF*プロファイルの完全な交換コール フロー

次の図は、完全な NF プロファイルの交換を表すコール フローを示しています。

**図 *203 : NF* プロファイルの完全な置換**

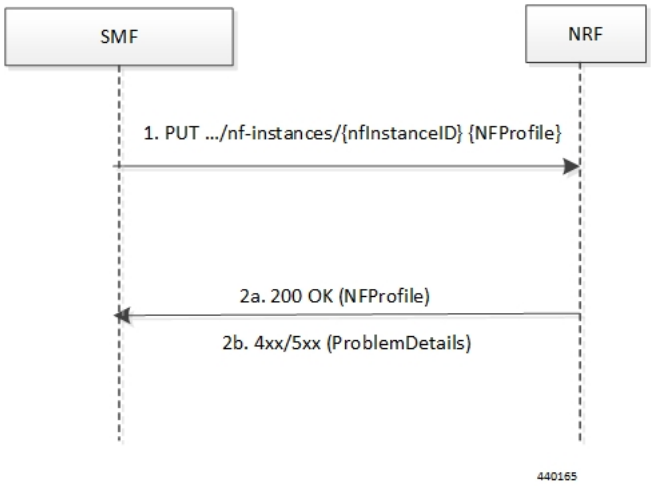


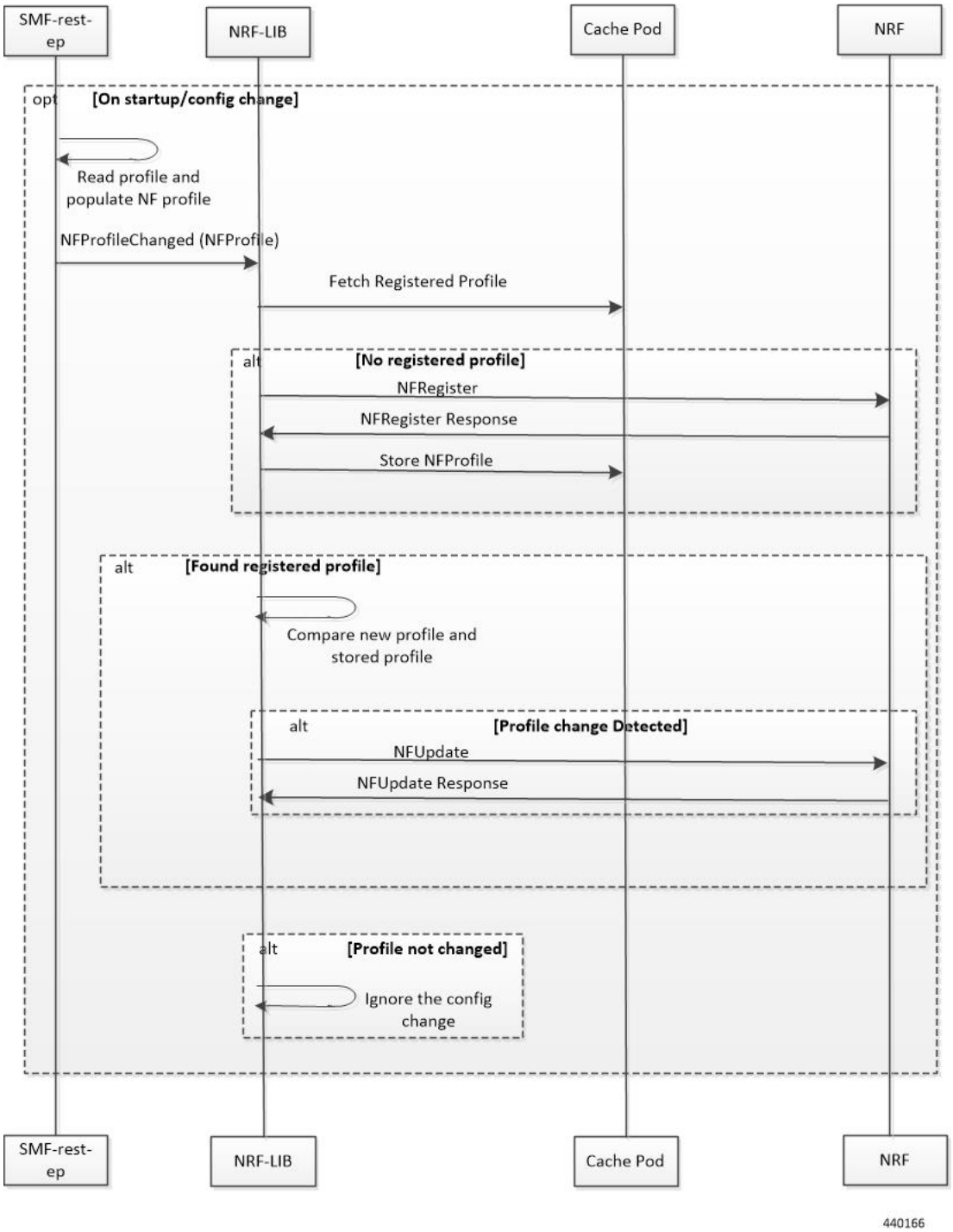

**表 *370 : NF* プロファイル完全な交換コール フローの説明**

| ステップ | 説明 |
|---|---|
| 1 | SMF は、NF インスタンスを表す技術情報 URI に PUT 要求を送信します。PUT 要求のペイロード本文には、NF インスタンスの NF プロファイルに対する更新操作が含まれています。 |
| 2a | 成功し、NF プロファイルが変更されると、NRF は、応答本文で完全な NF プロファイルデータとともに「200 OK」を返します。 |
| 2b | 「nfInstanceID」で識別される NF インスタンスが、NRF データベースの登録済み NF インスタンスのリストにない場合、NRF は、エラーの詳細を提供する ProblemDetails IE とともに 4xx または 5xx ステータス コードを返します。 |

## *NF* 登録と *NF* 更新のコール フロー

次の図は、REST-EP からの NF プロファイル変更トリガーでの、SMF からの NF 登録および NF 更新メッセージングを表すコールフローを示しています。

**図 *204 : NF* 登録と *NF* 更新のコール フロー**



1. SMF REST-EP は起動時に SMF プロファイル設定を読み取り、それに応じて NF 管理プロファイルを入力します。次に、REST-EP は SMF をトリガーして、NF プロファイルの変更を示します。
2. SMF は NF 登録ステータスと登録済みプロファイルを外部キャッシュポッドに保持します。SMF は、NRF を使用した NF 登録が完了しているかどうかを検出します。NF プロファイル変更の処理中に登録が完了していないことを SMF が検出した場合は、ステップ 3 を実行します。NF 登録が完了している場合は、ステップ 4 を実行します。
3. SMF は NF 登録を NRF に送信します。これにより、NF インスタンスはその NF プロファイルを NRF に登録できます。これには、NF インスタンスによって公開されるサービスのリストとともに、NF インスタンスの一般パラメータの登録が含まれます。
4. SMF は登録済みの NF プロファイルを取得し、新しいプロファイルと比較します。
5. SMF プロファイル設定の変更により、NF 管理プロファイルのいずれかのパラメータが変更されると、SMF は NF 更新 (PUT) 要求を NRF に送信します。

   負荷パラメータは PUT メッセージの一部として設定されません。ハートビートは、現在アクティブなハートビート間隔として設定されます。
6. 変更が検出されない場合、SMF はトリガーを無視します。

**重要** NF 更新は、選択された SMF からのみ送信されます。

### 標準準拠

NF プロファイル更新機能は、次の標準規格に準拠しています：

- *3GPP TS 29.510*、バージョン *15.4.0*（*2019* 年 *7* 月）：*5G* システム ネットワーク機能リポジトリ サービス第*3*段階

### 制限事項

NF プロファイル更新機能には、次の制限があります：

- NF プロファイルの完全な置換のみをサポートします。
- キャパシティはサポートされません。

# NF ディスカバリ

## 機能説明

SMF は NRF が提供する NF 検出サービスを使用して、アクセスおよびモバイル機能（AMF）、Unified Data Management（UDM）、ポリシー制御機能（PCF）などのネットワーク機能（NF）

を検出します。SMFは、ディスカバリ クエリのネットワーク リポジトリ機能（NRF）の「profile nf-pair」構成で提供される優先順位を構成します。

NF ごとに、クエリ パラメータ（フィルタとも呼ばれる）を構成できます。これらのパラメータに基づいて、NRF は NF プロファイルを検出するための SMF のクエリ条件に一致するすべての NF を返します。

**Note** NF 検出とロード バランシングは、UDM、PCF、CHF、AMF でのみ使用できます。

NF ディスカバリはダイナミックな構成変更をサポートします。したがって、トランザクション/手順の途中で構成が変更されると、進行中のトランザクションが影響を受けます。

ダイナミックな構成変更機能は、次をサポートします。

- NRF トランザクション/プロシージャは構成バージョン（v1）を選択し、NRF トランザクション/プロシージャが完了するまで同じバージョンを使用します。
- 継続されている NRF トランザクション中に構成を変更した場合、新しい構成バージョン（v2）が作成されます。ただし、新しい構成は新しいトランザクションに適用されます。

ダイナミック構成変更は、次のデータ構造に適用します：

- NrfFailureProfileSt
- NrfClntProfileSt
- NrfGrpSt
- NrfPairProfileSt
- NrfMgmtGrpSt

# 機能の仕組み

このサービス操作は、「nf-instances」リソースをクエリすることによって実行されます。リクエストは、SMF の同じ PLMN 内の NRF に送信されます。

## コール フロー

ここでは、この機能に関連したコール フローについて説明します。

### サービス検出要求のコール フロー

このセクションでは、サービス検出要求のコール フローについて説明します。

*Figure 205:* サービス検出要求のコール フロー

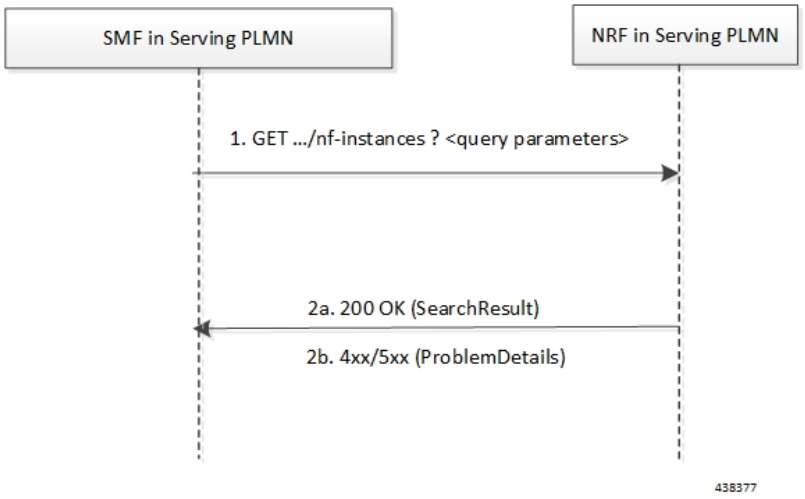



*Table 371:* サービス検出要求のコール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | SMF はリソース URI「nf-instances」収集リソースに HTTP GET 要求を送信します。検出要求の入力フィルタ条件は、クエリパラメータにあります。 |
| 2a | 成功すると、「200 OK」が返されます。応答本文には、SMF が検索結果をキャッシュする有効期間と、検索フィルタ基準を満たす NF プロファイル オブジェクトの配列が含まれます。たとえば、特定の NF サービス名を表示するすべての NF インスタンスです。 |
| 2b | SMF がクエリ パラメータで指定された要求された NF タイプの NF サービスを検出できない場合、NRF は「403 Forbidden」という応答を返します。<br>URI クエリ パラメータの入力データのエラーが原因で NRF で検出要求が失敗した場合、NRF は、エラーの詳細を提供する「ProblemDetails」IE を使用して「400 Bad Request」ステータスコードを返します。<br>NRF 内部エラーが原因で検出要求が NRF で失敗した場合、NRF は、「500 Internal Server Error」ステータス コードと、エラーの詳細を提供する「ProblemDetails」IE を返します。 |

正常な結果として返される NF プロファイル オブジェクトには、任意の NF タイプに適用可能な、各 NF インスタンスの汎用データが含まれます。これらのオブジェクトには、特定のタイプに属する NF インスタンスの NF 固有のデータを含めることもできます（たとえば、NF インスタンスのタイプが「UDR」値の場合、属性「udrInfo」は NF プロファイルに存在します）。また、カスタム NF タイプを持つ NF インスタンスの NF プロファイルに属性「customInfo」が

存在します。NF インスタンスの場合、NRF は、検出応答で返される NF プロファイルの一部として、「customInfo」属性を返します（使用可能な場合）。

SMF サービスは、セッションがアクティブな場合、UDM、AMF、PCF、CHF などのさまざまな NF と通信します。NF 検出は、セッションに関連付けられている一連のフィルタ（クエリパラメータとも呼ばれる）に基づいています。SMF サービスは、セッションのフィルタ条件と一致する NF を検出し、NF にメッセージを送信します。

SMF は次のフィルタをサポートしています：

- Dnn
- Tai
- TargetNfFqdn
- TargetPlmnList
- TargetNfInstanceId
- Snssais
- 優先地名

検出された NF は、フィルタをキーとしてキャッシュされます。メッセージを送信するためのエンドポイントの選択は、優先順位とキャパシティのパラメータを使用する確率論的ロードバランシングアルゴリズム（IETF RFC 2782）に基づいています。NF 検出応答には、キャッシュの有効期間を決定する有効期間が含まれています。

SMF は NF に送信された最初のメッセージへの応答として、Location ヘッダー URL に基づいてメッセージをターゲットに送信します。

SMF は、送信されるメッセージの選択されたエンドポイントのエンドポイント、サービス インスタンス、および NF インスタンスの詳細がアプリケーションまたは REST-EP に提供される定着度をサポートし、後続のメッセージ(検出フィルターの代わりに) で同じものを指定できるようになります。この操作は、選択した NF へのセッションの定着度を維持するのに役立ちます。

## 標準準拠

NF 検出機能は、次の標準規格に準拠しています：

- *3GPP TS 29.510*、バージョン *15.4.0*（*2019* 年 *7* 月）：*5G* システム ネットワーク機能リポジトリ サービス第 *3* 段階

## 制限事項

NRF 検出機能には、次の制限があります：

- 維持されるキャッシュはライブラリに対してローカルです。REST-EP の複数のレプリカを使用した展開では、同じ検出フィルタを持つ 2 つの検出または送信メッセージが異なるポッドにある場合、両方のポッドが NF 検出をトリガーします。

- この機能は、UDM、PCF、CHF、AMF の検出とロード バランシングのみをサポートします。UPF 検出はサポートしていません。

# 検出のために NRF を構成

このセクションでは、NF 検出を実行するために必要な構成について説明します。

## NRF を登録

NRF を登録するには、次の構成例を使用します。

```
config
nssai name nssai_name
    sst sst ssd ssd
    dnn dnn_name_value
    end
```

注：

- **nssai name** *mains_name*：スライスの NSSAI 名の値を構成します。*nsnai_name* 値は文字列である必要があります。

（注） SMF は、NRF に送信される最大 512 のスライスをサポートします。

### 設定例

次に、NRF 登録の構成例を示します。

```
nssai name slice1
 sst 02
 sdt Abf123
 dnn [ dnn1 intershat intershat1 intershat2 intershat3 intershat4 intershat5 intershat6
 intershat7 starosupf ]
exit

nssai name slice2
 sst 02
 sdt Abf124
 dnn [ dnn1 intershat intershat1 intershat2 intershat3 intershat4 intershat5 intershat6
 intershat7 starosupf ]
exit
```

## NRF の検出

NRF 検出を構成するには、次の構成例を使用します：

```
config
  profile network-element [ amf amf_profile_name| chf chf_profile_name | pcf
 pcf_profile_name | udm udm_profile_name | upf upf_profile_name ]
     query-params requester-snssais
     exit
```

注：

- **query-params requester-snssais**：NRF への NF 検出要求のクエリ パラメータとしてシングル ネットワーク スライス選択アシスタンス情報（S-NSSAI）のリストを指定します。

### 設定例

次に、設定例を示します。

```
config
   profile network-element udm udm1
      query-params requester-snssais
      exit
   profile network-element pcf pcf1
      query-params requester-snssais
      exit
   profile network-element chf chf1
      query-params requester-snssais
      exit
   profile network-element upf upf1
      query-params requester-snssais
      exit
   profile network-element amf amf1
      query-params requester-snssais
      exit
```

## NF クライアント プロファイルを構成

AMF、CHF、PCF、および UDM の NF エンドポイントを構成するには、次の構成例を使用します：

```
config
  profile nf-client { nf-type { amf amf-profile | chf chf-profile |
pcf pcf-profile | udm udm-profile } nf_profile_name }
  end
```

注：

- **profile nf-client { nf-type { amf amf-profile | chf chf-profile | pcf pcf-profile | udm udm-profile } *nf_profile_name* }**：必要な NF クライアントプロファイルを指定し、次の構成済み NF のいずれかのローカル構成を指定します：
  - **amf**：AMF ローカル構成を有効にします。
  - **chf**：CHF ローカル構成を有効にします。
  - **pcf**：PCF ローカル 構成を有効にします。
  - **udm**：UDM ローカル 構成を有効にします。

    たとえば、 **amf amf-profile** キーワードを構成する場合、このコマンドは AMF ローカル構成を有効にします。同じアプローチが他の構成済み NF にも適用されます。

    *nf_profile_name* は 、対応する NF クライアント プロファイル名を表す英数字の文字列である必要があります。

- 特定のサービス内に複数の NF プロファイルを構成できます。

- 構成を無効にするには、**no profile nf-client { nf-type { amf amf-profile | chf chf-profile | pcf pcf-profile | udm udm-profile }** *nf_profile_name* **}** コマンドを使用します。

### 設定例

次に、設定例を示します。

```
profile nf-client nf-type pcf
pcf-profile pcf-profile
  locality LOC1
   priority 1
   service name type npcf-smpolicycontrol
    endpoint-profile epprof
     capacity   10
     priority   1
     uri-scheme http
     endpoint-name ep1
      priority 1
      capacity 10
      primary ip-address ipv4 209.165.202.133
      primary ip-address port 8080
     exit
     endpoint-name ep2
      priority 1
      capacity 10
      primary ip-address ipv4 209.165.201.1
      primary ip-address port 8080
     exit
    exit
   exit
  exit
exit
exit
profile nf-client nf-type pcf
pcf-profile pcf-profile
  locality LOC1
   priority 1
   service name type npcf-smpolicycontrol
    endpoint-profile epprof
     capacity   10
     priority   1
     uri-scheme http
     endpoint-name ep1
      priority 1
      capacity 10
      primary ip-address ipv4 209.165.201.2
      primary ip-address port 8080
     exit
```

## 検出グループと NF タイプの関連付け

検出グループを NF タイプとペアリングするには、次の構成例を使用します。

```
config
  profile nf-pair nf-type nf_type
    nrf-discovery-group nrfdisc_group_name
    end
```

注：

- **nf-type** *nf_type*：NF クライアント タイプの値を SMFとして指定します。

- **nrf-discovery-group** *nrfdisc_group_name*：NRF 検出グループ名を指定します。検出グループは、NRF エンドポイント グループ（nrf-group）への論理リンクです。NF タイプごとに、検出グループとローカリティ情報を関連付けることができます。

## NF ディスカバリ用の NRF エンドポイント プロファイル パラメータの構成

SMF は、**nnrf-nfd**（NF ディスカバリ）の NRF エンドポイントを構成するための CLI を提供します。

（注） 検出グループについては、 **nnrf-disc** サービスのみを構成できます。

CLI設定では、各エンドポイントプロファイルの下で複数のエンドポイントを構成できます。SMFは、優先順位とキャパシティのパラメータを使用して、これらのエンドポイント間でロード バランシングを行います。エンドポイント プロファイルの下のすべてのエンドポイントがセッション コンテキストを共有します。つまり、セッションの最初のメッセージにエンドポイント プロファイルを選択すると、SMF は、セッションの後続のメッセージ（update、delete など）をエンドポイント プロファイル内の任意のエンドポイントに送信します。

各エンドポイント内にプライマリ、セカンダリ、およびターシャリ ホスト[ip:port]を構成できます。IPv4 アドレスと IPv6 アドレスの両方を指定できます。両方が指定されている場合は、IPv4 アドレスが優先されます。

SMF は、フィルタ パラメータのセットに一致するメッセージを検出して NF に送信する API を提供します。

URI はリソースを一意に識別します。5GC SBI API では、リソース URI が絶対 URI の場合、構造は次のように指定されます：

```
{apiRoot}/{apiName}/{apiVersion}/{apiSpecificResourceUriPart}
```

apiRoot は、次の部分の連結です：

- スキーム（「http」または「https」）

（注） HTTP と HTTPS スキーム URI の両方を使用できます。サービスベースのインターフェイスのセキュリティの詳細については、*3GPP TS 33.501* の *13.1* 項を参照してください。

- 固定文字列「://」
- IETF RFC 3986 で定義されている権限（ホストおよびオプションのポート）
- 「/」文字で始まるオプションの展開固有の文字列（APIプレフィックス）（CLIのapi-root）

NRF でサポートされているさまざまなサービスの NRF エンドポイントを構成するには、次の構成例を使用します。

```
config
  group nrf discovery discovery_name
    service type nrf nnrf-disc
      endpoint-profile
        name  epprofile_name
        api-root api_string
        api-uri-prefix uri_prefix_string
        uri-scheme { http | https }
        endpoint-name ep_name { capacity capacity | primary ip-address {
 ipv4 ipv4_address | ipv6 ipv6_address | port port_num } | secondary ip-address
 { ipv4 ipv4_address | ipv6 ipv6_address| port  port_num } | tertiary ip-address
 { ipv4 ipv4_address| ipv6 ipv6_address | port port_num } }
        version [ uri-version version_num full version version_num ]
        end
```

注：

- **group nrf discovery** *discovery_name* ：NRF 検出グループを構成します。
- **api-root** *api_string*：: apiRoot 内で使用される展開固有のサービス API プレフィックスを指定します。
- **api-uri-prefix** *uri_prefix_string*：6apiName を指定します。構成されていない場合は、仕様に従ってサービスの標準 API 名を使用します。
- **endpoint-name** *ep_name* **{ capacity** *capacity* **| primary ip-address { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **| port** *port_num* **} | secondary ip-address { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **| port** *port_num* **} | tertiary ip-address { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **| port** *port_num* **} }**：エンドポイント名を指定します。NF サーバのフェールオーバー処理のために、各エンドポイント内のプライマリ ホスト、セカンダリ ホスト、およびターシャリ ホスト（IP：ポート）を構成できます。サーバ フェールオーバー構成は、IPv4 アドレスと IPv6 アドレスの両方を受け入れます。ただし、AMF では IPv4 アドレスが優先されます。
  - **capacity***capacity*：エンドポイントのノード キャパシティを指定します。 *capacity* は 0 ～ 65535 の範囲の整数である必要があります。
  - メッセージを送信するためのエンドポイントの選択は、優先順位およびキャパシティのパラメータを使用する確率論的ロードバランシング アルゴリズム（IETF RFC 2782）に基づいています。
  - **primary ip-address { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **| port** *port_num* **}**：プライマリ エンドポイントの IPv4 アドレス、IPv6 アドレス、またはポートを指定します。
  - **secondary ip-address { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **| port** *port_num* **}**：セカンダリ エンドポイントの IPv4 アドレス、IPv6 アドレス、またはポートを指定します。
  - **tertiary ip-address { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **| port** *port_num* **}**：ターシャリ エンドポイント の IPv4 アドレス、IPv6 アドレス、またはポートを指定します。
  - **priority***priority_value*：サービスがロードバランシング ロジックを使用して適切なプロファイルを選択するための優先順位を指定します。 *priority* は 0 ～ 65535 の範囲の整数である必要があります。

- **uri-scheme { http | https }**： **http** または **https**として URI スキームを指定します。
- **version [ uri-version***version_num* **full version***version_num* **]**：API URI バージョンを指定します。完全バージョンの形式は次のとおりです。<Major-version>.<Minor-version>.<patch-version>.[alpha-<draft-number>].

### NF 検出用の NRF エンドポイント プロファイル パラメータの確認

このセクションでは、NRF エンドポイントのプロファイル パラメータの構成を確認する方法を説明します。

```
show running-config group nrf
group nrf discovery udmdiscovery
 service type nrf nnrf-disc
  endpoint-profile epprof
   capacity       10
   priority       1
   api-uri-prefix nudm-sdm
   api-root       root
   uri-scheme     http
   version
    uri-version v1
     full-version 209.165.200.225
    exit
   exit
   endpoint-name endpointName
    priority 1
    capacity 100
    primary ip-address ipv4 209.165.200.237
    primary ip-address port 3021
   exit
  exit
 exit
exit
```

## NF タイプの局所性の構成

SMF は地域対応の NF 検出を提供します。

ペアプロファイルには、NF タイプが SMF として構成された地域値があります。ローカリティには、次の値があります：

- client：クライアントの地域情報を指定します。
- geo-server：地理サービス地域情報を指定します。
- preferred-server：優先サーバの地域情報を指定します。

プロファイルの選択では、preferred-server および geo-server の地域値のみが考慮されます。次に、これらの地域の値を構成するシナリオを示します：

- preferred-server および geo-server の両方の地域値が構成されている場合、検出応答内に存在し、これらの地域値に一致するプロファイルが選択されます。さらに、地域値が空のプロファイルが選択されます。preferred-server および geo-server の地域値以外の地域を持つ他のプロファイルは考慮されません。

- 優先サーバのローカリティ値のみが構成されている場合は、この値に一致する検出応答内に存在するプロファイルが選択されます。さらに、地域値が空のプロファイルが選択されます。優先サーバの地域値以外の地域を持つ他のプロファイルは考慮されません。
- geo-server 地域値のみが構成されている場合、この geo-server 地域値に一致する検出応答内に存在するプロファイルが選択されます。さらに、地域値が空のプロファイルが選択されます。地理的なサーバの地域の値以外の地域を持つ、他のプロファイルは考慮されません。
- 優先サーバーと地域の値の両方が設定されていない場合は、検出応答に存在するすべてのプロファイルが選択されます。

NF タイプのローカリティを設定構成するには、次の構成例を使用します。

```
config
  profile nf-pair nf-type nf_type
    locality { client client_name | geo-server geoserver_name |
preferred-server prefserver_name }
    end
```

注：

- **client** *client_name*：クライアントの地域情報を指定します。クライアント地域は SMF の地域であり、必須パラメータです。
- **preferred-server** *prefserver_name*：優先されるサーバの地域情報を指定します。優先サーバの地域は、対応する NF 検出中に優先の地域と見なされる必要がある地域です。
- **geo-server** *geoserver_name*：地域サーバの地域情報を指定します。地理的なサーバ ローカリティは、優先ローカリティの地理的冗長サイトであり、通常、NF ディスカバリ中に、優先ローカリティの次に最適なサーバ ローカリティとして使用されます。

**Note** **geo-server** *geoserver_name* は完全修飾されていません。

### 検出グループと地域構成の関連付けの確認

ここでは、NF の検出グループの関連付けと地域の構成を確認する方法について説明します。

```
show running-config profile nf-pair
profile nf-pair nf-type UDM
 nrf-discovery-group DISC1
 locality client LOC1
 locality preferred-server PREF_LOC
 locality geo-server GEO
exit
```

## SMF の地域の構成

SMF の地域を構成するには、次の構成例を使用します。

SMF が NRF を使用して NF の検出を実行する場合、これは必須の構成です。

```
config
  profile SMF SMF_profile_name
    locality value
    end
```

注：

- **locality** *value*：AMF の地域を指定します。 値は 、展開された AMF の地域を表す英数字の文字列である必要があります。デフォルトでは、この CLI は無効になっています。
- この構成を無効にするには、**no locality** *value* コマンドを使用します。

## DNN の NF プロファイルの構成

構成済み DNN（データ ネットワーク名）の NF プロファイルを構成するには、次のサンプル構成を使用します。

```
config
  profile dnn dnn_profile_name
    network-element-profiles { amf | chf | pcf | udm } nf_profile_name
    end
```

注：

- **network-element-profiles { amf | chf | pcf | udm }** *nf_profile_name*：AMF、CHF、PCF および UDM などの NF タイプを 1 つ以上ネットワーク要素プロファイルとして指定します。 *nf_profile_name* は、対応するネットワーク要素のプロファイル名を表す英数字の文字列を指定する必要があります。
- この設定は、オプションです。デフォルトでは、この CLI は無効になっています。
- 特定のサービス内に複数プロファイルを構成できます。
- 構成を無効にするには、 **no network-element-profiles { amf | chf | pcf | udm }** *nf_profile_name* コマンドを使用します。

## NF プロファイル内での局在性の定義

このセクションでは、NFエンドポイントのローカリティを定義する方法について説明します。NF エンドポイントの選択については、 SMF**profile nf-pair** CLI コマンドで構成されている優先順位を最初に考慮します。管理者は、地域とネットワーク機能の近接性に基づいて、優先される地域を決定します。 SMF 、NF 検出の次の優先ローカリティとして、Geo サーバーのローカリティ構成を使用します。**profile nf-pair** コマンドに関する詳細は、「ピア NF タイプごとの NRF の選択, on page 1137」セクション内の NF タイプの局所性の構成, on page 1132 を参照してください。

**profile nf-pair** CLI コマンドで優先サーバーのローカリティ構成が含まれていない場合、または **profile nf-client** CLI コマンドで優先サーバーまたは Geo-server ローカリティで構成されたエンドポイントが含まれていない場合、 SMF は他のローカリティエンドポイントを選択します。他の地域のエンドポイントの選択では、 SMF**locality** CLI コマンド内の **priority** 構成を使用します。

NF エンドポイントのローカリティを定義するには、次の構成例を使用します。

```
config
  profile nf-client { nf-type { amf amf-profile | chf chf-profile |
pcf pcf-profile | udm udm-profile } nf_profile_name }
     locality locality_name [ priority priority | service name type
service_types { endpoint-profile epprofile_name } ]
     end
```

注：

- **locality** *locality_name*：NF エンドポイントの場所を指定します。 SMF 、ローカリティ構成（つまり、優先サーバーローカリティと Geo サーバーローカリティ）を使用して、適切な NF エンドポイントを選択します。
- **priority** *priority*：ローカリティ構成の優先順位を指定します。
- **service name type** *service_types*：構成された NF サービス タイプを指定します。サービス タイプは、構成されたサービスによって異なります。
  - AMF サービスは、ピア通信タイプとして 「namf-comm」、 をサポートします。
  - PCF サービスは、ピア通信タイプとして「npcf-am-policy-control」をサポートします。
  - UDM サービスは、ピア通信タイプとして「nudm-sdm」と「nudm-uecm」をサポートしています。
  - SMF サービスは、ピア通信タイプとして「nsmf-pdusession」をサポートします。
  - EIR サービスは、ピア通信タイプとして「n5g-eir-eic」をサポートします。
  - NSSF サービスは、ピア通信タイプとして「nnssf-nsselection」をサポートしています。
  - SMSF サービスでは、ピア通信タイプとして「nsmsf-sms」がサポートされています。
  - LMF サービスは、ピア通信タイプとして「nlmf-loc」をサポートします。
  - GMLC サービスは、ピア通信タイプとして「ngmlc-loc」をサポートしています。
  - AUSF サービスは、ピア通信タイプとして「nausf-auth」をサポートしています。
- **endpoint-profile** *epprofile_name*：NF サービス レベルごとにエンドポイントを指定します。NF 固有のサービスは、ローカリティ構成内で使用できます。
- 構成された NF のプロファイル名ごとに複数のエンドポイントを構成できます。

## NF クライアント プロファイルの NF エンドポイント プロファイル パラメータの構成

ここでは、サービス内の NF エンドポイント プロファイルとその関連パラメータを構成する方法について説明します。

CLI 設定では、各エンドポイント プロファイルの下で複数のエンドポイントを構成できます。SMF は、優先順位とキャパシティのパラメータを使用して、これらのエンドポイント間でロード バランシングを行います。エンドポイント プロファイルの下のすべてのエンドポイントが

セッション コンテキストを共有します。つまり、セッションの最初のメッセージにエンドポイント プロファイルを選択すると、SMF は、セッションの後続のメッセージ（update、delete など）をエンドポイント プロファイル内の任意のエンドポイントに送信します。

SMF は、フィルタ パラメータのセットに一致するメッセージを検出して NF に送信する API を提供します。

URI はリソースを一意に識別します。5GC SBI API では、リソース URI が絶対 URI の場合、構造は次のように指定されます：

```
{apiRoot}/{apiName}/{apiVersion}/{apiSpecificResourceUriPart}
```

apiRoot は、次の部分の連結です：

- スキーム（「http」または「https」）

**Important** HTTP と HTTPS スキーム URI の両方を使用できます。サービス ベースのインターフェイスのセキュリティの詳細については、*3GPP TS 33.501* の *13.1* 項を 参照してください。

- 固定文字列「://」
- *IETF RFC 3986* で定義されている権限（ホストおよびオプションのポート）
- 「/」文字で始まるオプションの展開固有の文字列（APIプレフィックス）（CLIのapi-root）

サービス内の NF エンドポイントプロファイルと関連パラメータを構成するには、次の構成例を使用します：

```
config
  profile nf-client { nf-type { amf amf-profile | chf chf-profile |
pcf pcf-profile | udm udm-profile }  nf_profile_name }
    locality locality_name [ priority priority | service name type service_type
 ]
        endpoint-profile epprofile_name
           api-root api_string
           api-uri-prefix uri_prefix_string
           capacity capacity
           endpoint-name ep_name { capacity capacity | primary ip-address {
 ipv4 ipv4_address | ipv6 ipv6_address | port port_num }| secondary ip-address
 { ipv4 ipv4_address | ipv6 ipv6_address| port  port_num } | tertiary ip-address
 { ipv4 ipv4_address| ipv6 ipv6_address | port port_num } }
           priority priority_value
           uri-scheme { http | https }
           version [ uri-version version_num full version version_num ]
           end
```

注：

- **api-root** *api_string*：: apiRoot 内で使用される展開固有のサービス API プレフィックスを指定します。

- **api-uri-prefix** *uri_prefix_string*：6apiName を指定します。構成されていない場合は、仕様に従ってサービスの標準 API 名を使用します。
- **capacity** *[capacity]*：プロファイルの容量を指定します。
- **endpoint-name** *ep_name* **{ capacity** *capacity* **| primary ip-address { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **| port** *port_num* **} | secondary ip-address { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **| port** *port_num* **} | tertiary ip-address { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **| port** *port_num* **} }**：エンドポイント名を指定します。NF サーバのフェールオーバー処理のために、各エンドポイント内のプライマリ ホスト、セカンダリ ホスト、およびターシャリ ホスト（IP：ポート）を構成できます。サーバ フェールオーバー構成は、IPv4 アドレスと IPv6 アドレスの両方を受け入れます。ただし、SMF では IPv4 アドレスが優先されます。
  - **capacity** *capacity*：エンドポイントのノード キャパシティを指定します。 *capacity* は 0 ～ 65535 の範囲の整数である必要があります。

    メッセージを送信するためのエンドポイントの選択は、優先順位およびキャパシティのパラメータを使用する確率論的ロードバランシング アルゴリズム（*IETF RFC 2782*）に基づいています。
  - **primary ip-address { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **| port** *port_num* **}**：プライマリ エンドポイントの IPv4 アドレス、IPv6 アドレス、またはポートを指定します。
  - **secondary ip-address { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **| port** *port_num* **}**：セカンダリ エンドポイントの IPv4 アドレス、IPv6 アドレス、またはポートを指定します。
  - **tertiary ip-address { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **| port** *port_num* **}**：ターシャリ エンドポイン トの IPv4 アドレス、IPv6 アドレス、またはポートを指定します。
- **priority** *priority_value*：サービスがロードバランシング ロジックを使用して適切なプロファイルを選択するための優先順位を指定します。 *priority* は 0 ～ 65535 の範囲の整数である必要があります。
- **uri-scheme { http | https }**： **http** または **https** として URI スキームを指定します。
- **version [ uri-version** *version_num* **full version** *version_num* **]**：API URI バージョンを指定します。完全バージョンの形式は次のとおりです。
  <Major-version>.<Minor-version>.<patch-version>.[alpha-<draft-number>].

# ピア NF タイプごとの NRF の選択

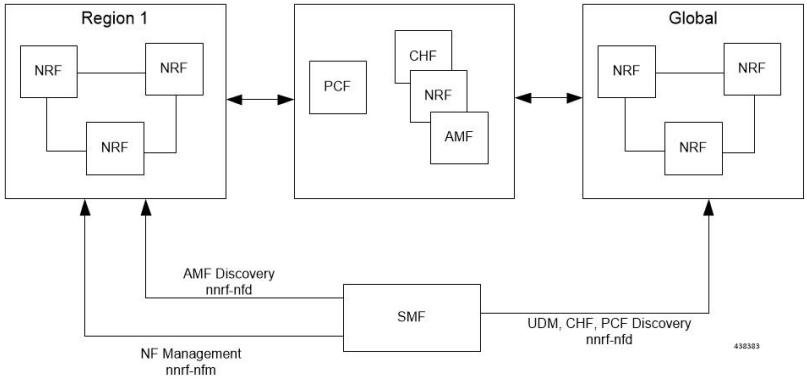
## 機能説明

ネットワーク リポジトリ機能（NRF）の導入は、グローバル、リージョンなどとして論理的にセグメント化して、信頼性の高いネットワーク管理を実現できます。このセグメンテーションを実現するには、さまざまなネットワーク機能の検出に対してさまざまな NRF エンドポイント グループを指定します。

たとえば、SMF は、管理および SMF 検出のためにリージョン 1 の NRF エンドポイントと対話します。UDM、CHF、PCF 検出の場合、SMF はグローバル NRF エンドポイントと通信します。

以下の図は、NRF 展開を説明しています。

***Figure 206: NRF* の展開**




### 標準準拠

この機能は、以下の基準に準拠しています。

- *3GPP TS 29.510* バージョン *15.4.0*。*5G* システム ネットワーク機能リポジトリ サービス。第 *3* 段階

## ピア NF タイプごとの NRF の選択の構成

ここでは、ピア NF タイプごとに NRF 選択を構成する方法について説明します。

### NRF エンドポイントへの NRF 管理と SMF 同一性の関連付け

NRF 管理（nrf-group）と SMF の局所性を構成し、それらを NRF エンドポイントに関連付けるには、次の構成例を使用します。

```
config
  group nf-mgmt mgmt_name
    nrf-mgmt-group nrf_group_name
    locality locality_name
    message-handling-profile message_handling_profile_name
    end
```

注：

- **nrf-mgmt-group** *nrf_group_name*：NRF 管理グループを指定します。
- **locality** *locality_name*：地域情報を指定します。
- **message-handling-profile** *message_handling_profile_name*：NRF のメッセージ処理プロファイルを指定します。

## *NRF* エンドポイントに対する 管理および *SMF* 同一性の関連付けの確認

このセクションでは、NRF 管理と SMF ローカリティを NRF エンドポイントに関連付ける構成を確認する方法について説明します。

```
show running-config group nf-mgmt
group nf-mgmt NFMGMT1
 nrf-mgmt-group MGMT
 locality       LOC1
exit
```

### SMF の局元性の構成

SMF のローカリティを構成するには、次の構成例を使用します。

SMF が NRF を使用して NF 検出を実行する場合、これは必須の構成です。

```
config
   profile SMF SMF_profile_name
      locality value
      end
```

注：

- **locality** *value*：SMF の地域を指定します。 値は 、展開された SMF の地域を表す英数字の文字列である必要があります。デフォルトでは、この CLI は無効になっています。
- 構成を無効にするには、**no locality** *value* コマンドを使用します。

### DNN の NF プロファイルの構成

構成済みデータネットワーク名（DNN）に使用される NF プロファイルを構成するには、次の構成例を使用します。

```
config
   profile dnn dnn_profile_name
      network-element-profiles { amf | chf | pcf | udm } nf_profile_name

      end
```

注：

- **network-element-profiles { amf | chf | pcf | udm }** *nf_profile_name*：AMF、CHF、PCF および UDM などの NF タイプを 1 つ以上ネットワーク要素プロファイルとして指定します。*nf_profile_name* は、対応するネットワーク要素のプロファイル名を表す英数字の文字列を指定する必要があります。
- この設定は、オプションです。デフォルトでは、この CLI は無効になっています。
- 特定のサービス内に複数プロファイルを構成できます。
- 構成を無効にするには、**no network-element-profiles { amf | chf | pcf | udm }** *nf_profile_name* コマンドを使用します。

## NFネットワーク要素プロファイル パラメータの構成

構成済み NF のネットワーク エレメント プロファイル パラメータを構成するには、次のサンプル構成を使用します。

```
config
  profile network-element { { amf | chf | pcf | udm } nf_profile_name }

    nf-client-profile profile_name
    query-params { dnn | limit | max-payload-size | requester-snssais
 | supi | tai | target-nf-instance-id | target-plmn }
    end
```

注：

- **nf-client-profile** *profile_name*：クライアント プロファイルを指定します。 *profile_name* は、対応する NF クライアント プロファイル名を表す英数字の文字列を指定する必要があります。
- **query-params { dnn | limit | max-payload-size | requester-snssais | supi | tai | target-nf-instance-id | target-plmn }**：NRF へ NF デスカバリ要求に含めるために次のいずれかのクエリ パラメータを指定します。
  - **dnn**：NRF への NF 検出要求のクエリ パラメータとして DNN を指定します。
  - **limit**：NRF が NF ディスカバリ応答で送信するプロファイルの最大数の制限を指定します。
  - **max-payload-size**：NRF への NF 検出要求のクエリ パラメータとして最大ペイロード サイズを指定します。
  - **requester-snssais**：NRF への NF デスカバリ要求のクエリ パラメータとしてシングル ネットワーク スライス選択アシスタンス情報（S-NSSAI）のリストを指定します。
  - **supi**：NRF への NF 検出要求のクエリ パラメータとして SUPI を指定します。
  - **tai**：NRF への NF 検出要求のクエリ パラメータとして TAI を指定します。
  - **target-nf-instance-id**：NRF への NF 検出要求のクエリ パラメータとしてターゲット NF インスタンス識別子を指定します。
  - **target-plmn**：NRF への NF 検出要求のクエリ パラメータとしてターゲット PLMN を指定します。
- この設定は、オプションです。デフォルトでは、CLI コマンドは無効になっています。
- 構成を無効にするには、これらのコマンドの **no** バリエーションを使用します。例えば、**no nf-client-profile** CLI コマンド。

### エンドポイントごとの *NRF* インターフェイスのローカル構成の確認

このセクションでは、エンドポイントごとの NRF インターフェイスの構成を確認する方法を説明します。

次に、NRF エンドポイントの構成例を示します。

```
show running-config profile dnn cisco
profile dnn cisco
 network-element-profiles chf chf1
 network-element-profiles amf amf1
 network-element-profiles pcf pcf1
 network-element-profiles udm udm1
 ssc-mode 2 allowed [ 3 ]
 session type IPV4 allowed [ IPV4V6 ]
 upf apn intershat
exit

profile smf smf1
 node-id          12b888e1-8e7d-49fd-9eb5-e2622a57722
 locality         LOC1
 bind-address ipv4 209.165.200.227
 bind-port        8008
instances 1 fqdn cisco.com.apn.epc.mnc456.mcc123
 plmn-id mcc 123
 plmn-id mnc 456
exit

profile network-element amf amf1
 nf-client-profile        AMF-L1
 failure-handling-profile FH1
 query-params [ target-nf-instance-id ]
exit
profile network-element pcf pcf1
 nf-client-profile        PCF-L1
 failure-handling-profile FH1
exit
profile network-element udm udm1
 nf-client-profile        UDM-L1
 failure-handling-profile FH1
exit
profile network-element chf chf1
 nf-client-profile        CHF-L1
 failure-handling-profile FH2
exit
end
```

# 検出された NF プロファイルのキャッシング

## 機能説明

SMF は、検出されたキャッシング プロファイルのキャッシング サポートを提供します。NF 検出（nnrf-disc）機能を使用して、AMF、UDM、PCF、CHF などのプロファイルを検出します。受信した検出応答は、有効期間に関連付けられています。SMF は検出応答をキャッシュし、キャッシュが有効になるまで将来の NF の選択に同じ応答を使用します。このキャッシング サポートは、進行中のセッション中の NRF 対話数の削減に役立ちます。

### 関係

NF 検出のキャッシング サポートには、次の機能と機能的な関係があります。

- SMF サブスクリプションおよび通知の NRF サポート

- ピア NF タイプごとの NRF の選択

## 機能の仕組み

SMF 、キャッシュポッドにキャッシュデータを保持します。キャッシュ ポッドを使用して、SBI ポッドの複数のインスタンス間で NF 検出キャッシュを共有します。SBI ポッドは、NF ディスカバリ応答を受信すると、キャッシュ ポッドを定期的に更新します。すべての SBI ポッドは、キャッシュ ポッドを利用してキャッシュ データを定期的に更新します。

特定の基準を満たす NF にメッセージが送信されると、 SMF は さらに処理するためにキャッシュ データを検索します。キャッシュ ルックアップ中の場合：

- 期限切れのエントリのないキャッシュ ヒットが発生した場合、選択されたキャッシュ済み NF 応答はエンドポイント選択のメッセージを送信します。
- 期限切れのエントリのキャッシュがヒットすると、 SMF は NF ディスカバリ要求を NRF に送信して、NF ディスカバリ応答の新しいリストを取得します。
- キャッシュミスがある場合、 SMF は NF 検出要求を NRF に送信し、NF 検出応答の新しいリストを取得します。

### コール フロー

キャッシュ ルックアップのコール フロー

ここでは、キャッシュ ルックアップのコール フローについて説明します。

SMF ローカル キャッシュを維持し、外部キャッシュ（cache-pod）を更新します。キャッシュのキーは nfType と filter の組み合わせで、複数のフィルタ パラメータから「key1=value, key2=value2」という形式で作成された文字列です。

起動時に、SMF、エポック以降に変更されたすべてのキャッシュ エントリをキャッシュ ポッドから取得して、ローカル キャッシュを構築できるようにします。ローカル キャッシュが構築されると、同じキャッシュが検索のためにメッセージの送信フローで使用されます。キャッシュ ポッドを使用してローカル キャッシュを更新するため、定期的な更新ルーチンが開始されます。ローカルキャッシュは、最後の更新以降に変更されたすべてのレコードをキャッシュ ポッドから取得することにより、定期的に更新されます。結果のレコードのリストがトラバースされ、ローカル キャッシュが更新されます。

SMF-rest-ep（SBI）が UDM へのメッセージの送信をトリガすると、SMFnfType とフィルタ キーを使用してローカル キャッシュを検索します。NF プロファイルはロードバランシングされ、選択したエンドポイントにメッセージが送信されます。

### 標準準拠

この機能は、以下の基準に準拠しています。

- *3GPP TS 29.510* バージョン *15.4.0*。*5G* システム ネットワーク機能リポジトリ サービス。第 *3* 段階

# NF 検出キャッシュの無効化（NF Discovery Cache Invalidation）

## 機能説明

SMF は、ローカルに構成された NF よりも、NRF から検出された NF をより高く優先します。SMF は、NRF エンドポイントが構成されていない場合、または NF 検出応答の一部として使用できる NF がない場合にのみ、ローカルに構成された NF を使用します。この応答は、クエリ フィルタ条件が満たされた後に表示されます。各 NF 検出応答には関連付けられた有効期間があり、SMF は NF 検出応答をキャッシュし、そのキャッシュを後続のセッションのアクティブ化に使用します。SMF は、その NF 検出応答キャッシュ内のクエリ フィルタに一致するエントリがない場合、またはキャッシュ内にエントリがあるが有効期限切れで存在する場合にのみ、NF 検出を実行します。

## 機能の仕組み

SMF は、NRF が到達不能で、期限切れのキャッシュ エントリがある場合の動作を決定する設定を提供します。CLI には、判断を実行するための次のオプションが用意されています。

- キャッシュ エントリを有効期限時に無効にする必要がある場合。
- キャッシュ エントリを無効にする必要がある場合、および有効期限の切れ後にキャッシュ エントリを保持する期間。

これらのオプションは、NRF が非アクティブの場合にのみ適用されます。構成は nf-pair プロファイルに準拠しています。構成は、NRF が非アクティブになった場合に SMF が期限切れのキャッシュを使用する必要があるかどうか、期限切れのキャッシュを使用するかどうか、および有効期限の切れた後にキャッシュ エントリを保持する期間を決定します。

## NF 検出キャッシュの無効化（消去）の構成

NF 検出キャッシュのキャッシュ エントリの無効化（消去）を構成するには、次の構成例を使用します。

```
config
  profile nf-pair nf-type { amf | chf | pcf | udm }

     cache invalidation { false | true [ timeout integer ] }
     end
```

注：

- **cache invalidation { false | true [ timeout** *integer* **] }**：間隔およびキャッシュ無効化ルールを構成します。デフォルト値は false です。
  - **false**：キャッシュ エントリが無効にならないように指定します。
  - **true timeout** *integer* ：キャッシュ エントリを無効にすることを指定します。**timeout***integer* は 、期限切れのキャッシュ エントリの使用を制御する期間をミリ秒単位で指定します（NRF が到達不能の場合）。デフォルト値は 0 ミリ秒です。

次の構成は、UDM 検出のキャッシュの無効化を false に設定する例です：

```
profile nf-pair nf-type UDM
  cache invalidation false
 end
```

次の構成は、UDM 検出のキャッシュの無効化を true に設定する例です：

```
profile nf-pair nf-type UDM
  cache invalidation true timeout 10
 end
```

# 代替 AMF の選択

表 *372 :* 機能の履歴

| 機能名 | リリース情報 | 説明 |
|---|---|---|
| 代替 AMF の選択 | 2024.02.0 | この機能により SMF は、UE に接続された AMF が障害を体験した場合、セットから使用可能な AMF の選択をすることがでみます。SMF は、NRF クエリ パラメータまたは、 NRF クエリ応答ローカリフィルタの構成に基づいて AMF 選択を実行します。<br><br>この機能は、AMF が使用できなくなった場合でも中断のないサービス継続性のニーズに対応します。<br><br>この機能では、次の新しいCLI コマンドが導入されます：<br><br>• **filter-discovery-response filter match { all \| any } attributes { target-nf-instance-id }**<br><br>• **filter-discovery-response filter failure-action { use-discovery-response }**<br><br>これらの構成により、SMF は受信した NRF 検出応答をローカルにフィルタ処理し、構成されたフィルタと一致する適切な応答を選択することができます。<br><br>この機能は、NRF クエリ パラメータの一部としてリージョンとセット ID の構成をさらにサポートします。<br><br>**デフォルト設定** 無効：有効にするには構成が必要です。 |

# 機能説明

AMF の選択機能は、AMF が使用できなくなった場合でも、サービスを中断させないという重要なニーズに対応します。この機能により SMF は、UE に接続された AMF が障害を体験した場合、セットから使用可能な AMF の選択をすることがでみます。SMF は、NRF クエリ パラメータまたは、NRF クエリ応答ローカリフィルタの構成に基づいて AMF 選択を実行します。

# AMF クエリ パラメータの検出応答フィルタの構成

AMF クエリ パラメータの検出応答フィルタを構成するには、次の構成例を使用します：

```
config
  profile network-element amf amf_profile_name
     query-params [ target-nf-instance-id | region-set ]
     filter-discovery-response filter match { all | any } attributes {
 target-nf-instance-id }
     filter-discovery-response filter failure-action {
use-discovery-response }
     end
```

注：

- **query-params [ target-nf-instance-id | region-set ]**：ターゲット NF インスタンス ID またはリージョン セットをクエリ パラメータとして指定します。 **region-set** は、リージョン ID とセット ID の組み合わせです。

  **region-set** クエリ パラメータを構成する場合。SMF は、**amf-set-id** および **amf-region-id**を使用して NF Discovery を行います。AMF は、AMF から N11 の作成または N11 の更新要求で受信した GUAMI から **set-id** と **region-id** を学習します。

- **filter-discovery-response filter match { all | any } attributes { target-nf-instance-id }**：このフィルタは、指定された属性の「すべて」または「任意」の属性を一致させることで検出応答を制御します。

  **match all** オプションを使用してローカル応答フィルタ パラメータを構成した場合。SMF は、優先パラメータを使用して NRF から検出されたプロファイルをフィルタリングしようとします。SMF は、パラメータと一致するプロファイルのうちの 1 つを選択します。一致しない場合、AMFの選択は失敗します。

  ローカル クエリ パラメータとして target-nf-instance-id を構成する場合。SMF はクエリ パラメータを使用して NF ディスカバリを行います。SMF は、検出されたプロファイルリストを target-nf-instance-id = AMF の最新の既知 nf インスタンス ID でフィルタリングして、最終的な AMF を選択します。

- **filter-discovery-response filter failure-action { use-discovery-response }**：フィルタが失敗した場合に実行するアクションを決定します。

  ローカル応答フィルタ パラメータを設定すると、SMF はローカル パラメータを使用して NRF から検出されたプロファイルをフィルタリングし、最終的なピア インスタンスを選択します。パラメータが一致しない場合、SMF は NRF から検出されたプロファイルの 1

つを選択します。SMF は、failure-action 構成が **use-discovery-response** オプションで使用できるかどうかを確認します。 AMFの選択に失敗します。

# ピア NF 管理の静的構成

## 静的 IP アドレス サポートへのフォールバック

### 機能説明

SMF、さまざまなNF選択オプションの優先順位に従います。SMF、ローカル構成よりもNRFから検出された NF を優先します。SMF 、NF 検出応答に有効な NF がない場合、ローカルに構成された NF を使用します。

展開に応じて、優先サーバと地理的位置性サーバが NF ごとに構成されます。原則として、優先サーバNFが失敗した場合に備えて、優先サーバ地理情報内のNF、続いてgeo地理情報サーバ内の NF を選択します。

各 NF に対して、 SMF **profile nf-pair** パラメータを介して優先サーバーおよび Geo サーバの地理情報を構成するオプションを提供します。（詳細については、ピア NF タイプごとの NRF の選択, on page 1137 セクションの NF タイプの局所性の構成, on page 1132 を参照してください。）

また、各 NF 検出応答には有効時間が関連付けられています。SMF この NF 検出応答をキャッシュし、後続のセッションを取得するために使用します。

SMF 、次の条件で NF 検出を実行します。

- NF 検出応答キャッシュに一致するエントリがありません。
- NF 検出応答キャッシュに一致するエントリがありますが、有効期限が切れています。

#### 関係

スタティック IP アドレスへのフォールバック機能には、次の機能との機能関係があります。

- NF 検出のキャッシング サポート
- NF 検出、NF 選択、およびロード バランシング
- ピア NF タイプごとの NRF の選択

### 機能の仕組み

NRF 検出グループが構成されている場合、SMF は NF 選択のために次のシーケンスに従います：

1. NF のローカル キャッシュ（NF 検出応答キャッシュ）を検索します。

2. NF が有効なエントリ（期限切れでない）である場合は、そのエントリが使用されます。それ以外の場合、SMF はステップ 3 に進みます。
3. SMF は検出のために NRF に到達します（「NRF 検出（優先度 1）」を参照）。それ以外の場合、SMF はステップ 4 に進みます。
4. SMF が検出に NRF を使用できない場合、AMF は期限切れの NF キャッシュを使用します（「期限切れの NF キャッシュ（優先順位 2）（Expired NF Cache ( Priority 2)）」を参照）。期限切れの NF キャッシュが使用できない場合、SMF はステップ 5 に進みます。
5. SMF がローカル キャッシュで NF を見つけられず、NRF 検出応答で NF を取得することもできない場合、AMF はローカルで構成された NF を使用します（「NF ローカルの構成（優先度 3）」を参照してください）。

NF 選択の優先順位は次のとおりです：

1. **NRFディスカバリ（優先順位 1）**

   SMS は、NRF が提供する NF 検出サービスを使用して、SMF、UDM、PCF などの NF を検出します。SMF は、検出クエリの「**profile nf-pair**」構成で指定された優先地理情報を構成します。（**profile nf-pair nf-type**CLI 構成の詳細については、NF タイプの局所性の構成, on page 1132 の ピア NF タイプごとの NRF の選択, on page 1137 セクションを参照してください）。NF ごとに、クエリ パラメータを構成できます。（詳細については、ピア NF タイプごとの NRF の選択, on page 1137セクションのNFネットワーク要素プロファイル パラメータの構成, on page 1140を参照してください。）NRF は、クエリ基準に一致するすべての NF を返します。使用可能な場合、NRF は preferred-locality と一致するローカリティ属性を持つ NF プロファイルを優先します。NRF は、優先されるターゲット NF の場所と一致しない追加の NF を応答で返す可能性があります。これは、優先ターゲット NF の場所と一致する NF プロファイルが見つからない場合に発生します。これを回避するために、NRF は、応答の優先ターゲット NF の場所に一致しない追加の NF に、優先ターゲット NF の場所に一致するものよりも低い優先順位を設定できます。SMF の地理情報対応 NF 選択ロジックは次のとおりです。

   a. NF に優先サーバー構成と地理的ローカリティサーバー構成の両方がある場合、これらに一致する応答内のすべての NF がキャッシュされます。SMF はバランス NF を無視します。ロード バランシング ロジックは、最初に優先されるローカリティ NF を選択します。優先される地理情報 NF が失敗した場合、SMF は再試行対象の geo 地理情報 NF を選択します。N 回の再試行が許可されている場合、N-1 回の再試行が優先ローカリティで行われ、最後の再試行が地理的ローカリティ NF で行われます。N-1 エンドポイントが優先地理情報で利用できない場合、SMF は優先地理情報のすべてのエンドポイントを試行します。それ以外の場合、SMF は残りの再試行の geo 地理情報エンドポイントを選択します。同じホスト（ポート）での複数回の再試行は行われません。

   b. NF に優先ローカリティ構成のみがある場合は、応答内の優先ローカリティに一致するすべての NF がキャッシュされます。ロードバランシング ロジックは、これらの NF からエンドポイントを選択します。

c. NF に優先ローカリティまたは地理的ローカリティ構成がない場合、SMS はすべての検出応答 NF をキャッシュします。ロードバランシング ロジックは、これらの NF から選択します。

**Note**

- ロードバランシング ロジックは、優先順位、キャパシティ、および負荷に基づいています。このロジックは、IETF RFC 2782 で定義されているサーバ選択と同様です。ただし、重量は「キャパシティ * (100 - 負荷)」と見なされます。
- SMF が NRF で検出された NF を選択した場合（3 つのケースのいずれかで）、優先および geo 地理情報に到達する試みがすべて失敗した場合でも、SMF は再試行のためにローカル構成 NF にフォールバックしません。

2. **期限切れの NF キャッシュ（優先度 2）**

SMF は、次のシナリオでのみ NF 検出を実行します。

- NF 検出キャッシュのクエリ フィルタで一致エントリを使用できない場合
- 一致するエントリが NF 検出キャッシュで使用可能な場合。ただし、これらのエントリは有効期限が切れています。

  期限切れのキャッシュ エントリの保持は、設定に基づいています。期限切れのキャッシュ エントリが使用可能で、NRF が到達不能であるか、エラーを返した場合、SMF は NF の選択に期限切れのキャッシュ エントリを使用します。以下のオプションを使用して、キャッシュ エントリの使用を制御するように SMF を構成できます：

  - 有効期限でキャッシュ エントリを無効にします。
  - 無効化されたキャッシュ エントリを構成可能な期間（タイムアウト）の間使用し、タイムアウトが経過した後に静的構成にフォールバックする。

**Note**

SMF は、これらのオプションを通じてキャッシュ エントリの使用を制御します（NRF がダウンしている場合のみ）。構成は、**profile nf-pair**に基づいています。さらに、SMF は、さまざまな NF に対してさまざまなキャッシュ使用ルールを構成できる柔軟性を提供します。たとえば、SMF は NRF がダウンしている場合、常に期限切れのキャッシュを使用して PCF を検出します。ただし、UDM を検出するために、SMF は、NRF がダウンしている場合、10 ミリ秒（ms）のタイムアウト期間の間、期限切れのキャッシュを使用します。

3. **NF ローカル構成（優先度 3）**

ローカルに構成されたNFは、NFエンドポイントの選択の最後のオプションになります。ローカル構成でも、NF の選択のために優先される地域と地理的なサーバーの地域が考慮されます。優先順位は次のとおりです：

**a.** 優先サーバーが NF [ in **profile nf-pair** ] 向けに構成されている場合、SMF はまず優先地理情報の下の NF エンドポイントを選択します。ロードバランシング ロジックは、構成された優先順位とキャパシティの値に従って、エンドポイントのプロファイルと地域内のエンドポイントに適用できます。

**b.** 地理情報が NF [ **profile nf-pair** ] に構成されている場合、SMF はフォールバック オプションとして、地理的局在性の下の NF エンドポイントを選択します。つまり、優先サーバー ローカリティ NF エンドポイントに障害が発生した場合、または優先サーバー ローカリティ エンドポイントが構成されていない場合です。ロードバランシング ロジックは、構成された優先順位とキャパシティの値に従って、エンドポイントのプロファイルと地域内のエンドポイントに適用できます。

**c.** 優先サーバと地理情報別サーバが適用されない場合、SMF は、ローカル NF 構成の各地域に構成されている優先順位に基づいて地域を選択します。ロードバランシング ロジックは、構成された優先順位とキャパシティの値に従って、エンドポイントのプロファイルと地域内のエンドポイントに適用できます。

**Note** ローカリティの優先順位は、優先サーバーと地理的ローカリティサーバーが適用されない場合にのみ適用されます。

障害テンプレートは、NF ごとに構成できます。また、テンプレートのメッセージ タイプは、考えられる HTTP 戻りコードの再試行回数とアクションを設定できます。

### 標準準拠

静的 IP アドレスへのフォールバック機能は、以下の基準に準拠しています：

- *3GPP TS 29.510* バージョン *15.4.0*（*2019* 年 *7* 月）：*5G* システム ネットワーク機能リポジトリ サービス第 *3* 段階

## フォールバックから静的 IP アドレスへの構成

このセクションでは、静的 IP アドレスへのフォールバックのサポートを構成する方法について説明します。

### NF クライアント プロファイルを構成

AMF、CHF、PCF、および UDM の NF エンドポイントを構成するには、次の構成例を使用します：

```
config
  profile nf-client { nf-type { amf amf-profile | chf chf-profile |
```

**pcf pcf-profile | udm udm-profile }** *nf_profile_name* **}**
**end**

注：

- **profile nf-client { nf-type { amf amf-profile | chf chf-profile | pcf pcf-profile | udm udm-profile } *nf_profile_name* }**：必要な NF クライアントプロファイルを指定し、次の構成済み NF のいずれかのローカル構成を指定します：
  - **amf**：AMF ローカル構成を有効にします。
  - **chf**：CHF ローカル構成を有効にします。
  - **pcf**：PCF ローカル 構成を有効にします。
  - **udm**：UDM ローカル 構成を有効にします。

  たとえば、 **amf amf-profile** キーワードを構成する場合、このコマンドは AMF ローカル構成を有効にします。同じアプローチが他の構成済み NF にも適用されます。

  *nf_profile_name* は、対応する NF クライアント プロファイル名を表す英数字の文字列である必要があります。
- 特定のサービス内に複数の NF プロファイルを構成できます。
- 構成を無効にするには、**no profile nf-client { nf-type { amf amf-profile | chf chf-profile | pcf pcf-profile | udm udm-profile }** *nf_profile_name* **}** コマンドを使用します。

## 設定例

次に、設定例を示します。

```
profile nf-client nf-type pcf
pcf-profile pcf-profile
  locality LOC1
   priority 1
   service name type npcf-smpolicycontrol
    endpoint-profile epprof
     capacity   10
     priority   1
     uri-scheme http
     endpoint-name ep1
      priority 1
      capacity 10
      primary ip-address ipv4 209.165.202.133
      primary ip-address port 8080
     exit
     endpoint-name ep2
      priority 1
      capacity 10
      primary ip-address ipv4 209.165.201.1
      primary ip-address port 8080
     exit
    exit
   exit
  exit
exit
exit
profile nf-client nf-type pcf
```

```
pcf-profile pcf-profile
  locality LOC1
   priority 1
   service name type npcf-smpolicycontrol
    endpoint-profile epprof
     capacity   10
     priority   1
     uri-scheme http
     endpoint-name ep1
      priority 1
      capacity 10
      primary ip-address ipv4 209.165.201.2
      primary ip-address port 8080
     exit
```

## NFネットワーク要素プロファイル パラメータの構成

構成済み NF のネットワーク エレメント プロファイル パラメータを構成するには、次のサンプル構成を使用します。

```
config
  network-element-profiles { { amf | chf | pcf | udm } nf_profile_name }

     nf-client-profile profile_name
    query-params { dnn  | limit | max-payload-size | requester-snssais
 | supi | tai | target-nf-instance-id | target-plmn }
     end
```

注：

- **nf-client-profile** *profile_name*：クライアント プロファイルを指定します。 *profile_name* は、対応する NF クライアント プロファイル名を表す英数字の文字列を指定する必要があります。
- **query-params { dnn | limit | max-payload-size | requester-snssais | supi | tai | target-nf-instance-id | target-plmn }**：NRF へ NF デスカバリ要求に含めるために次のいずれかのクエリ パラメータを指定します。
  - **dnn**：NRF への NF 検出要求のクエリ パラメータとして DNN を指定します。
  - **limit**：NRF が NF ディスカバリ応答で送信するプロファイルの最大数の制限を指定します。
  - **max-payload-size**：NRF への NF 検出要求のクエリ パラメータとして最大ペイロード サイズを指定します。
  - **requester-snssais**：NRF への NF デスカバリ要求のクエリ パラメータとしてシングル ネットワーク スライス選択アシスタンス情報（S-NSSAI）のリストを指定します。
  - **supi**：NRF への NF 検出要求のクエリ パラメータとして SUPI を指定します。
  - **tai**：NRF への NF ディスカバリ要求のクエリ パラメータとして TAI を指定します。
  - **target-nf-instance-id**：NRF への NF ディスカバリ要求のクエリ パラメータとしてターゲット NF インスタンス識別子を指定します。

- **target-plmn**：NRF への NF Discovery 要求のクエリ パラメータとしてターゲット PLMN を指定します。

- この設定は、オプションです。デフォルトでは、CLI コマンドは無効になっています。
- 構成を無効にするには、これらのコマンドの **no** バリエーションを使用します。例えば、**no nf-client-profile** CLI コマンド。

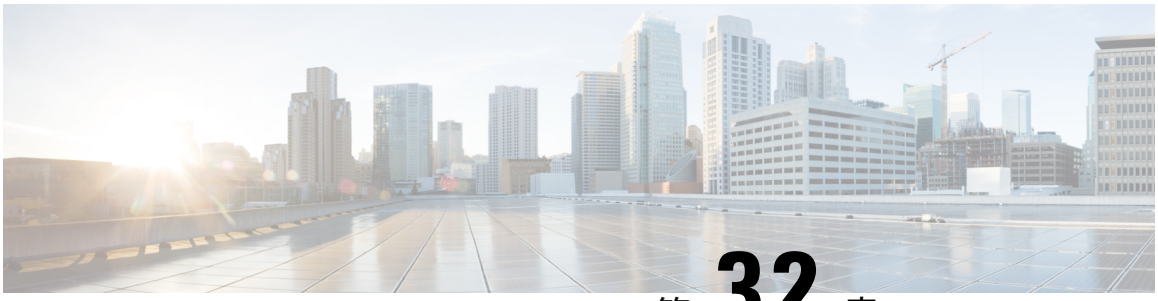
# NRF 障害の処理

## 機能説明

SMF は、NF 登録メッセージを使用して、管理 NRF グループの活性を追跡します。SMF が管理グループ内のいずれかの NRF で障害を検出すると、NRF 障害処理メカニズムを使用します。

各 NF とそのメッセージタイプに失敗処理テンプレートを使用して、再試行回数とアクションを設定して、考えられる HTTP 戻りコードを定義できます。

障害処理の詳細については、障害処理サポート, on page 411 の章を参照してください。



第 32 章

# 負荷および過負荷管理


- 機能の概要と変更履歴, on page 1155
- 機能説明 （1157 ページ）
- SBA インターフェイス過負荷制御 （1158 ページ）
- GTP-C ロードおよびオーバーロード制御 （1165 ページ）
- N4 インターフェイス負荷および過負荷制御 （1173 ページ）
- SMF での負荷および過負荷制御の構成 （1177 ページ）
- ノード過負荷, on page 1186
- モニタリングおよびトラブルシューティング, on page 1188


## 機能の概要と変更履歴

### 要約データ

***Table 373:*** 要約データ

| | |
|---|---|
| 該当製品または機能エリア | SMF |
| 該当プラットフォーム | SMI |
| 機能のデフォルト設定 | 無効：設定が必要 |
| このリリースでの関連する変更点 | N/A |
| 関連資料 | 該当なし |

# 更新履歴

***Table 374:*** マニュアルの変更履歴

| 改訂の詳細 | リリース |
|---|---|
| GTPC ピア過負荷制御のサポートが追加されました。 | 2021.02.3 |
| GTP-C 負荷および過負荷制御のサポートが追加されました。 | 2021.02.0 |
| メッセージ優先順位構成のサポートが追加されました。 | 2020.04.0 |
| 最初の導入。 | 2020.03.0 |

# 機能説明

表 *375 :* 機能の履歴

| 機能名 | リリース情報 | 説明 |
|---|---|---|
| SBI、GTP-C、および N4 インターフェイスを介した負荷と過負荷の制御 | 2024.04.1 | この機能は、GTP-C、N4、およびSBAインターフェイスの負荷と過負荷の制御メカニズムを処理します。<br>この機能は、セルフ ノードとピア ノードの負荷と過負荷の状態を考慮することでネットワークの堅牢性を向上させます。<br>**コマンドの拡張**：<br>• **profile overload-exclude** *overload_exclude_profile_name* **message-priority [ n4 \| n7 \| n10 \| n11 \| n16 \| n40 \| s5 ] upto** *message_priority*<br>• **profile overload-exclude** *overload_exclude_profile_name* **procedure-list [ session-delete \| new-call \| xnho \| modify \| chf-reauth \| inter-rat-ho \| intra-rat-ho \| imexit-nw \| imexit-ue \| usar ]**<br>**デフォルト設定**：無効：有効にするには構成が必要です |

SMF は、SMF およびサービスベース アーキテクチャ（SBA）で発生する過負荷と輻輳を管理するためのメカニズムを提供します。SMFは、設計されたキャパシティよりも高いレートで入力メッセージを受信します。SMF の内部キューの使用率が、構成レベルよりも高くなる場合があります。このシナリオは、ネットワークまたは SMF からの過負荷トラフィックが原因で、SBA サーバで、直接的または間接的に発生する可能性があります。

**重要** この章で使用されている PGW-C という用語は、SMF でサポートされている EPS インターワーキング機能を意味しており、LTE ネットワークで使用されるスタンドアロン P-GW として想定してはなりません。

# SBA インターフェイス過負荷制御

## 機能説明

インターフェイスは、指定された数の着信要求のみを処理します。着信要求が指定の数を超えると、インターフェイスが過負荷状態になります。たとえば、次の場合にインターフェイスが過負荷になります。

- ネットワーク要素の障害が原因で多数の再接続が発生している
- 複数のユーザーが、位置更新またはアイドル モードからアクティブ モードへの移行を頻繁に実行する

過負荷になると、インターフェイスは要求をドロップするか、要求の処理を遅らせる可能性があります。インターフェイスでの過負荷により、ネットワーク全体のパフォーマンスが低下します。このシナリオでは、ノードの輻輳、障害、または折りたたみが発生し、他のノードの負荷が増加する可能性があります。

SMFはさまざまなリソースを測定し、それらの測定に基づいて負荷を定義します。また、SMFは負荷に関するNRFを更新します。現在、SMFでは着信メッセージに過負荷保護を適用しています。過負荷保護がインバウンドインターフェイス（SBAインターフェイス）に適用されている場合、外部ノードはSMFに向けてスロットリングし、輻輳から抜け出します。

**Note** この機能の範囲は、SBAインターフェイスでのインバウンド要求による過負荷のみです。

## 機能の仕組み

SMFは、エンドポイントおよびアプリケーション レベルでのオーバーロードから着信リクエストを保護します。

- [エンドポイント レベル（Endpoint Level）]：保護は、メッセージ タイプを考慮せずに、HTTP要求メソッドに基づいています。
- [アプリケーション レベル（Application Level）]：保護はメッセージ タイプに基づいています。

### メッセージの優先順位

SMFは、要求を処理するためのリソースの可用性とメッセージの優先度を評価した後、着信要求メッセージに過負荷保護を適用します。優先順位の高いメッセージには、スロットリングに対する優先順位が低くなり、優先順位の低いメッセージにはより高い優先順位が高くなります。オーバーロードされたNFは、オーバーロード状態のときに、着信メッセージにメッセー

ジの優先順位付けスキームを適用します。このような状況では、NFは最も優先順位の高いメッセージを過負荷保護メカニズムから除外します。

メッセージの優先度を構成すると、SMFは優先度に基づいてメッセージの分類を開始します。この設定は任意です。この構成を使用しないことを選択した場合、SMFはメッセージの優先順位を考慮せずに過負荷保護技術を適用します。

# エンドポイントでオーバーロード保護

エンドポイントの場合、SMFはエンドポイントレベルとクライアントレベルの両方でオーバーロード保護を提供します。SMFは、着信要求メッセージの過負荷しきい値制限を定義します。しきい値の範囲に基づいて、SMF は着信要求メッセージを拒否できます。SMF は構成されたステータスとともに HTTP 応答をリクエストイニシエータに返します。

次に、SMF で定義されている過負荷のしきい値の制限を示します：

- **[低（Low）]**：このしきい値に達すると、POST 方式（リソース割り当てに寄与する汎用 URI）のみが拒否されます。
- **[高（High）]**：このしきい値に達すると、構成された（拒否）ステータスのすべてのメッセージが拒否されます。
- **[クリティカル（Critical）]**：このしきい値に達すると、構成された（拒否）ステータスのすべてのメッセージが拒否されます。

# オーバーロードの防止の設定

このセクションでは、インバウンド要求メッセージのオーバーロード保護の構成に関連する構成手順について説明します。

## エンドポイント レベルで過負荷の防止の構成

次の構成例を使用して、クライアント レベルで過負荷保護を構成します。

```
config
   instance instance-id gr_instance_id
     endpoint sbi
        overload-control threshold threshold_limit threshold_range action
action_status action_code range
        commit
        end
```

注：

- **overload-control**：エンドポイント レベルでの過負荷制御を指定します。
- **threshold** ：しきい値の制限と範囲を指定します。
- *threshold_limit*：しきい値の上限を指定します。 *threshold_limit* は 、次のいずれかである必要があります。

- *low*：オーバーロード保護の下限しきい値制限を指定します。
- *high*：オーバーロード保護の上限しきい値制限を指定します。
- *critical*：オーバーロード保護のクリティカルしきい値制限を指定します。

- *thershold_range*：しきい値の範囲を指定します。 *threshold_range* は 10 ～ 100000 の範囲の整数である必要があります。
- **action** ：しきい値制限に対して実行するアクションを指定します。
- *action_status*：しきい値制限のアクションを指定します。 *action_status* は次のように指定する必要があります：
  - **reject**：指定したしきい値の範囲が満たされた場合に着信メッセージを拒否します。
- *action_code*：アクション ステータス コードを指定します。 *action_code* は次の必要があります：
  - **reject-code**：拒否ステータス コードを指定します。
- *range*：アクション コードの範囲を指定します。 *range* は 100 ー 600 の範囲の整数である必要があります。

次に設定例を示します。

```
overload-control threshold low 500 action reject reject-code 501
overload-control threshold critical 10000 action reject reject-code 329
```

## クライアント レベルでオーバーロードの防止の構成

次の構成例を使用して、クライアント レベルで過負荷保護を構成します。

```
config
   instance instance-id gr_instance_id
      endpoint sbi
         overload-control client threshold threshold_limit threshold_range
action action_status action_code range
         commit
         end
```

注：

- **overload-control client**：クライアント レベルでのオーバーロード制御を指定します。
- **threshold** ：しきい値の制限と範囲を指定します。
- *threshold_limit*：しきい値の上限を指定します。 *threshold_limit* は 、次のいずれかである必要があります。
  - *low*：オーバーロード保護の下限しきい値制限を指定します。

- *high*：オーバーロード保護の上限しきい値制限を指定します。
- *critical*：オーバーロード保護のクリティカルしきい値制限を指定します。

- *thershold_range*：しきい値の範囲を指定します。 *thershold_range* は 10 ～ 100000 の範囲の整数である必要があります。
- **action** ：しきい値制限に対して実行するアクションを指定します。
- *action_status*：しきい値制限のアクションを指定します。 *action_status* は次のように指定する必要があります：
  - **reject**：指定したしきい値の範囲が満たされた場合に着信メッセージを拒否します。
- *action_code*：アクション ステータス コードを指定します。 *action_code* は次の必要があります：
  - **reject-code**：拒否ステータス コードを指定します。
- *range*：アクション コードの範囲を指定します。 *range* は 100 ー 600 の範囲の整数である必要があります。

次に設定例を示します。

```
overload-control client threshold low 50 action reject reject-code 329
overload-control client threshold critical 20000 action reject reject-code
 501
```

## 過負荷保護の構成の確認

**show running-config** コマンドを使用して、SMF Ops Center で過負荷保護の構成を表示します。次に、**show running-config** コマンドの出力例を示します。

```
[cluster1/data] example# show running-config
instance instance-id 1
 endpoint sbi
  overload-control threshold low 5000 action reject reject-code 555
  overload-control threshold high 7000 action reject reject-code 329
  overload-control threshold critical 10000 action reject reject-code 503
  overload-control client threshold low 750 action reject reject-code 329
  overload-control client threshold high 500 action reject reject-code 329
  overload-control client threshold critical 1000 action reject reject-code 503
  interface n11
  overload-control threshold low 4000 action reject reject-code 555
  overload-control threshold high 6000 action reject reject-code 329
  overload-control threshold critical 7000 action reject reject-code 503
  overload-control client threshold low 500 action reject reject-code 329
  overload-control client threshold high 700 action reject reject-code 329
  overload-control client threshold critical 800 action reject reject-code 503
 exit
exit
```

# メッセージの優先順位の構成

次の構成を使用して、インバウンド要求メッセージのメッセージ優先順位を構成します。

```
config
  overload-control threshold threshold_limit threshold_range action reject
reject-code range exclude message-priority priority_value
  end
```

注：

- **overload-control**：エンドポイント レベルでの過負荷制御を指定します。
- **threshold***threshold_limit* ：しきい値の制限と範囲を指定します。
- ：しきい値の上限を指定します。 *threshold_limit* は 、次のいずれかである必要があります。
  - low：過負荷保護の下限しきい値制限を指定します。
  - high：過負荷保護の上限しきい値制限を指定します。
  - critical：過負荷保護のクリティカルしきい値制限を指定します。
- *thershold_range* ：しきい値の範囲を指定します。 *thershold_range* は 10 ～ 100000 の範囲の整数である必要があります。
- **action** ：しきい値制限に対して実行するアクションを指定します。
- *action_status* ：しきい値制限のアクションを指定します。*action_status* は 次のように構成する必要があります。
  - **reject** ：指定したしきい値範囲が満たされた場合、着信メッセージを拒否します。
- **exclude message-priority** ：割り当てられた優先順位に応じて、過負荷保護メカニズムからメッセージを除外します。
- *priority_value* ：優先順位の値を指定します。

次に設定例を示します。

```
overload-control threshold low 1000 action reject reject-code 100 exclude
 message-priority 8
overload-control threshold high 2000 action reject reject-code 100 exclude
 message-priority 5
```

優先度の値が 8 の場合、優先度 8 以上で受信されるメッセージはスロットリングされません。これは、システムしきい値が優先順位値より低い場合でも適用されます。3GPP で定義されるメッセージの優先順位は、*3GPP TS 29.500* バージョン *15.4.0*により 0 ～ 31 です。

# SBA インターフェイス メッセージの自己過負荷処理

SMF は、app-infra からシステムの負荷係数情報を定期的に取得します。次に、SMF はこの負荷係数を過負荷プロファイルで構成されたしきい値と比較します。負荷ステータスに基づいて、SMF は SBA インターフェイス メッセージに対する負荷または過負荷の制御メカニズムをトリガします。

構成されたしきい値に従って、次の 3 つの負荷および過負荷の状態が考えられます。

| 負荷または過負荷の状態 | SMF アクション |
|---|---|
| 標準 | システムは通常の負荷状態です。構成に従って適用される負荷制御 |
| 過負荷状態 | システムが過負荷になっています。構成ごとに適用される過負荷制御。 |
| 自己保護状態 | 負荷ステータスが過負荷のしきい値を超えました。自己保護する必要があります。SMF は、構成に従ってメッセージのスロットリングまたは除外を適用します。 |

## NRF への自己負荷情報の伝達

負荷係数の計算に加えて、SMF は、OAM ポッドによって導出された負荷係数の変更を検出すると、負荷情報を NRF に送信します。SMF は、負荷構成が有効になっていない場合でも、負荷情報を計算して共有します。

SMF は、HTTP パッチ要求を使用して **NF 更新パッチ API** を送信し、部分的な NF プロファイルの更新を実行します。この部分的な更新は、NF インスタンスによって提供されるサービスの追加、削除、または置換に使用されます。

NF 更新パッチには、次の 2 つのパラメータが含まれています。

- **load**： NF の現在の負荷の割合を示します。値の範囲は 0 ～ 100 です。
- **loadTimeStamp**： NF インスタンスで最新の負荷情報が生成された時点を示します。

## SBI メッセージの自己過負荷スロットリングと除外

SMF は、着信する SBI メッセージに対してのみ、自己過負荷制御と除外処理を実行します。自己保護モードでは、サブスクライバが過負荷除外プロファイルで構成されていない限り、SMF はすべての着信 SBI メッセージをスロットリングします。

SBI インターフェイスの過負荷除外プロファイルを構成するには、「過負荷除外プロファイルの構成」の項を参照してください。

SMF が過負荷状態にあり、HTTP 要求を拒否する必要がある場合、HTTPS ステータス コード **503 Service Unavailable**で着信 SBI メッセージを拒否します。このコードを受信すると、受信側 NF は、拒否およびタイムアウトになったトラフィックを受け入れられたトラフィックと比

較します。この分析に基づいて、受信側 NF は SMF に送信されたトラフィックを迂回またはスロットリングします。

### SBI メッセージのバックオフ タイマー

自己保護状態で、バックオフ タイマーが構成されていて、SMF が **N11 SM Context Create** および **N11smcontextModify** メッセージを拒否する場合、SMF は、N1msgtypes の下の N1 コンテナの DNN プロファイルレベルに構成されたバックオフ間隔を含めます。

- PDU セッション確立拒否
- PDU セッション変更拒否

PDU セッションの確立および変更メッセージのバックオフ タイマーを設定するには、「メッセージレベルのバックオフ タイマーの有効化」の項を参照してください。

N11、N16、N40、および N10 応答メッセージをスロットリングすると、応答メッセージに次の原因コードのいずれかが含まれます。

- DNN_CONGESTION
- NF_CONGESTION
- 失敗の通知
- 取得失敗

（注） N11N1N2MessageTransferFailNotificationReq メッセージは、どのような状況でもスロットルされません。

## 制限事項

次に、SBA インターフェイス メッセージの負荷および過負荷サポートの既知の制限を示します。

- PDU セッションの解放とフローの解放を開始するすべての着信 SBI 要求または clearsub 要求は、スロットルされません。
- 自己保護処理は、Gx、Gy、Gz、Radius、Diameter（AAA）メッセージではサポートされません。
- 現在、SMF は、SBA インターフェイスを介したピアへの負荷または過負荷情報のアドバタイズをサポートしていません。

# GTP-C ロードおよびオーバーロード制御

## 機能説明

**重要** GTP-C ロードおよびオーバーロード制御はオプションの機能です。

SMF は、システム負荷情報を使用して GTP-C エンティティ リソースの動作ステータスを判別します。この情報が GTP-C ピアに送信されると、有効負荷に基づいて、同じ機能をサポートするエンティティ間でセッション負荷を適応的にバランスするのに役立ちます。

GTP-C オーバーロードは、着信要求の数が受信側の GTP-C エンティティでサポートされている最大要求スループットを超えると発生します。GTP-C は UDP トランスポートを介したものであり、確認応答されていない要求の再送信に依存しています。GTP-C エンティティがオーバーロード（または重大なオーバーロード）になると、確認応答されていない GTP-C メッセージの数が指数関数的に増加し、ノードの輻輳またはクラッシュが発生します。過負荷またはノードの障害により、ネットワーク内の他のノードの負荷が増加します。

ネットワーク内のコア ネットワーク ノードの過負荷は、サービスの低下につながります。ネットワーク全体の負荷分散を改善することで、過負荷の問題に対処できます。

オーバーロード状態は、さまざまなネットワーク シナリオで発生する可能性があります。次に、GTP-C オーバーロードにつながる GTP-C シグナリング ベースのシナリオの例を示します。

- ネットワーク要素の障害に起因するトラフィック フラッディングで、シグナリング スパイクが引き起こされます。
- TAU または RAU を実行している多数のユーザー、またはアイドル モードと接続モードの間の頻繁な移行によって発生するトラフィック フラッディング。
- 多数のコール（および専用ベアラ）がほぼ同時にセットアップされているなど、トラフィック スパイクをローカルに発生させる例外的なイベント。
- 3GPP 以外のカバレッジ（たとえば、Wi-Fi）の分散、または 3GPP と非 3GPP カバレッジ間の大規模なモビリティによる頻繁な RAT の再選択。この操作により、頻繁または大規模なシステム間変更アクティビティが発生する可能性があります。

GTP-C のオーバーロードにより、次のいずれかのサービスの影響が発生する可能性があります：

- 緊急コール ドロップ
- PDN 接続（IMS、インターネットなど）および関連するサービスの損失。
- サービスをサポートするために必要な無線およびコア ネットワーク ベアラー（GBR ベアラーなど）をセットアップおよびリリースする機能の喪失。

- 次の変更を報告する能力が失われる：
  - ユーザー情報（たとえば、緊急サービスの位置情報や合法的傍受の位置情報）
  - RAT または QoS
- 収益損失につながる請求エラー。

GTP-C ロードおよびオーバーロード制御は標準規格の機能です。標準準拠の詳細については、標準準拠 （1171 ページ）の項のこの機能の章を参照してください。

GTP-C ロード制御とオーバーロード制御は、ネットワーク上で個別にサポートおよびアクティブ化できる補完的な概念です。

この機能は、SMF のスタンドアロン展開と、cnSGWc との統合展開の両方で機能します。

（注） この機能は、SMF が PGW-C（つまり、EPS ネットワーク）とインターワーキングする場合にのみ機能します。この章で使用される「SMF」という用語は、SMF と PGW-C の両方の組み合わせを示します。

## GTP-C 負荷制御

この機能により、cnSGWc と PGW-C が負荷制御情報（LCI）を収集して GTP-C ピアに送信できます（たとえば、cnSGWc を介した MME、および ePDG）。概して、GTP-C 負荷制御は予防アクションを示し、GTP-C 過負荷制御は修正アクションを示します。

GTP-C 負荷制御を有効にする利点は次のとおりです。

- 負荷制御により、セッションの負荷をより適切に分散できます。このメカニズムにより、GTP-C 過負荷シナリオが防止されます。
- LCI は、有効負荷に応じて、同じ機能をサポートするエンティティ間でセッション負荷を適応的にバランスするのに役立ちます。
- 負荷制御は、GTP-Cエンティティが高い負荷を報告した場合でも、過負荷の緩和アクションをトリガしません。

## GTP-C 過負荷制御

この機能により、cnSGWc と PGW-C が過負荷制御情報（OCI）を収集して GTP-C ピアに送信できます（たとえば、cnSGWc を介した MME、および ePDG）。GTP-C エンティティがそのシグナリング容量を超えて動作すると過負荷状態になり、パフォーマンスが低下します。

GTP-C 過負荷制御を有効にする利点は次のとおりです。

- GTP-C エンティティの過負荷を回避します。
- SMF および cnSGWc の負荷分散が改善され、SMF 過負荷の発生が減少します。

- 過負荷が発生したときに着信トラフィックをできるだけ多く制限することを目的としています。

# メッセージ スロットリング

### 入力メッセージ

GTP-Cエンティティは、メッセージスロットリングのために、オーバーロード制御情報（OCI）のトラフィック削減メトリック情報を使用します。過負荷のシナリオを軽減するために、GTP-Cエンティティは、メトリック情報に基づいて、過負荷のピアへの入力メッセージフローを削減します。

ノードが自己保護モードの場合、SMF はメッセージ スロットリング除外構成に基づいて、入力 GTP-C メッセージを拒否します。除外プロファイル構成の詳細については、除外プロファイルの作成 （1179 ページ） セクションを参照してください。

### 出力メッセージ

GTP-C の過負荷のシナリオを軽減するために、SMF は、OCI 内で受信した情報に基づいて、過負荷の GTP-C ピアへの出力メッセージ フローを制御します。

SMF は、除外プロファイルの構成に基づいて GTP-C ピアへの出力メッセージを拒否します。除外プロファイルには、スロットリングから除外されるメッセージに対応する DNN リスト、5QI リスト、ARP リスト、および優先順位が含まれます。

GTP-C インターフェイスのピア オーバーロード制御は **profile overload** 、 *profile-name* **peer-level interface gtpc action throttle** コマンドを使用して構成できます。

**重要** メッセージ スロットリングは最初のメッセージにだけ適用されます。SMF は、対応する要求メッセージの再送信が発生する可能性があるため、トリガーされた要求または応答メッセージをスロットルしません。

スロットリングの場合、SMF は 3GPP 29.274 で指定されている損失アルゴリズムを使用します。

メッセージ グループは、3GPP 29.274、セクション 12.3.9.3.2 に記載されている手順のカテゴリに基づいて作成されます。次に、メッセージ スロットリング用のピア オーバーロード グループを示します。

- グループ 1 は、既存のリソースの更新に対応します。このグループには、Update Bearer Request メッセージが含まれます。
- グループ 2 は、新しいリソースの作成に対応します。このグループには、Create Bearer Request メッセージが含まれます。

メッセージ グループを使用すると、SMF が各メッセージ グループで生成する予定のメッセージの数をパーセンテージで構成できます。両方のグループのデフォルト値は50%です。デフォ

ルト値の 50% は、100 個の発信メッセージのうち、50 個のメッセージがベアラーの更新要求（グループ 1）で、50 個がベアラーの作成要求（グループ 2）であることを意味します。

ピアが過負荷となり、過負荷削減マトリックスが 30% である場合、SMF スロットル 30 はベアラー要求メッセージを作成し、残りのすべてのメッセージを送信します。

ピアが過負荷となり、過負荷削減マトリックスが 70% である場合、SMF は 50 の作成ベアラー要求メッセージと 20 の更新ベアラー要求メッセージをスロットルし、残りの 30 の更新ベアラー メッセージを送信します。

## 過負荷ピア検出

SMF は、次の GTP-C メッセージのいずれかで受信したオーバーロード制御情報（OCI）IE 情報に基づいて、GTP-C ピア エンティティがオーバーロードされているかどうかを判断します。

- セッション作成要求
- ベアラー作成応答
- ベアラー変更要求
- ベアラー更新応答
- セッション削除要求
- ベアラー削除応答
- ベアラー変更コマンド
- ベアラー削除コマンド
- ベアラーリソースコマンド

すべての GTP-C メッセージに、Delete Bearer Command メッセージおよび Bearer Resource Command メッセージを除き、cnSGWc、MME または S4-SGSN、および TWAN または ePDG の OCI が含まれることに注意してください。

SMF は、1 つのメッセージで複数の GTP-C エンティティに対応する OCI（たとえば、cnSGWc と MME または S4-SGSN の OCI）を受信します。SMF サービスポッドは、1 つのメッセージで受信したそのようなすべての OCI IE を解析して保存します。

SMF は、次のいずれかの条件が満たされた場合に、GTP-C ピアが過負荷であると見なします。

- OCI の有効期限が切れました
- OCI が 0 として受信されます

地理的冗長性（GR）の場合、新しいメッセージから受信した OCI に基づく時間を持つ新しいキャッシュ レコードが新しいインスタンスによって構築されることが期待されます。

プライマリ キャッシュ ポッドが非アクティブである場合、セカンダリ キャッシュ ポッドがアクティブになり、すべてのキャッシュ要求を処理します。

# 機能の仕組み

ここでは、この機能の動作メカニズムを説明します。

1. SMF は、アプリケーション インフラストラクチャからシステム負荷を定期的に取得します。詳細については、本章の「ノード過負荷（1186ページ）」セクションを参照してください。
2. SMFは、過負荷プロファイルで構成されたしきい値とシステム負荷値に基づいて、現在のノードの過負荷状態を識別します。
3. SMFは、ノードの過負荷状態に基づいて、着信要求メッセージに過負荷制御メカニズムを適用します。

| ノード過負荷状態 | 定義（Definition） | 基準 | 過負荷制御アクション |
|---|---|---|---|
| 標準 | システムは過負荷状態になっていません。 | 負荷<最小許容度未満 | GTP-C 負荷制御の適用 |
| 過負荷状態 | システムが過負荷状態かどうかを確認します。 | 最小許容値 <= 負荷 < 最大許容値 | GTP-C 過負荷制御の適用 |
| 自己保護状態 | システムが過負荷の限界に達しました。 | 負荷>=最大許容度 | メッセージスロットリングの適用 |

### GTP-C 負荷制御のメカニズム

SMF は、次の条件を満たすと、LCI を GTP-C ピア（MME や ePDG など）に伝達します。

- **profile load** *load_profile_name* **interface gtpc action advertise** コマンドを使用して機能が有効になっている場合
- 負荷プロファイルと過負荷プロファイルが SMF プロファイルに関連付けられている場合
- LCI がピアに送信されない場合
- **profile load** *load_profile_name* **advertise interval** *lci_broadcast_interval* の構成に従って定期的に送信
- 現在の負荷値と最後に示された負荷値との差が、構成された変更係数 **profile load** *load_profile_name* **advertise change-factor** *load_value_change_factor* よりも大きい場合

（注） SMF は、追加のシグナリングをトリガすることなく、GTP-C 要求および応答メッセージを介して LCI を交換します。

SMF は、次のメッセージで LCI を含みます。

- セッション応答の作成

- ベアラー要求の作成
- ベアラー変更応答
- ベアラー要求の削除
- N4 セッション応答
- ベアラー更新の要求

メッセージ形式および LCI IE の詳細については、3GPP TS 29.274 仕様のバージョン 15.4.0 を参照してください。

### GTP-C 過負荷制御メカニズム

SMFは、負荷の値と過負荷の削減メトリック構成に基づいて過負荷メトリックを計算して送信します。SMF は、次の条件を満たすと、OCI を GTP-C ピアに伝達します。

- 機能が **profile overload** *overload_profile_name* **node-level interface gtpc action advertise** コマンドによって有効になっている場合
- OCI がピアに送信されない場合
- **profile overload** *overload_profile_name* **node-level advertise interval** *oci_broadcast_interval* の構成に従って定期的に送信
- 現在の削減メトリックと最後に示された削減メトリックの差が、構成された変更係数**profile overload** *overload_profile_name* **node-level advertise change-factor** *overload_value_change_factor* より大きい場合
- 有効タイマーが期限切れになり、SMF がまだ過負荷状態の場合

（注） SMF は、追加のシグナリングをトリガすることなく、GTP-C 要求および応答メッセージを介して OCI を交換します。

SMF は、次のメッセージで OCI を含みます。

- セッション応答の作成
- ベアラー要求の作成
- ベアラー変更応答
- ベアラー要求の削除
- N4 セッション応答
- ベアラー障害表示の変更
- ベアラー更新の要求
- ベアラー障害表示の削除

メッセージ形式と OCI IE の詳細については、 *3GPP TS 29.274* 仕様のバージョン *15.8.0* を参照してください。

#### メッセージ スロットリング

自己保護モードでは、SMF は自己保護除外構成に従って、障害原因が「GTP-C エンティティ輻輳」に設定された入力 GTP-C メッセージを拒否します。

## 標準準拠

GTP-C ロードおよびオーバーロード制御機能には、次の制限があります。

- *3GPP TS 29.807*、バージョン *12.2.0*
- *3GPP TS 29.274*、バージョン *15.8.0*

## 制限事項

GTP-C ロードおよびオーバーロード制御機能には、次の制限があります。

- 1 つの負荷プロファイルと 1 つのオーバーロード プロファイルのみの構成が可能

# GTP-C ロードおよびオーバーロード制御の OAM サポート

ここでは、この機能の操作、管理、およびメンテナンスに関して説明します。

## バルク統計サポート

SMF は、この機能の一部として次のメトリックを維持します。

- **node_lci_metric**

  説明：このカウンタは、ノード レベル、つまり PGW-C を使用する SMF での現在の負荷（LCI）値を示します。

  メトリック タイプ：ゲージ

  ラベル

  - app_name
  - cluster
  - data_center
  - instance_id

- **node_oci_metric**

  説明：このカウンタは、ノード レベルでの現在のオーバー ロード（OCI）値を示します。

  メトリック タイプ：ゲージ

ラベル

- app_name
- cluster
- data_center
- instance_id

- **node_overload_status**

  説明：このカウンタは、ノード レベルでの現在の過負荷ステータスを示します。

  - 0：標準
  - 1：OverLoaded
  - 2：SelfProtection

  メトリック タイプ：ゲージ

  ラベル

  - app_name
  - cluster
  - data_center
  - instance_id

- **smf_inc_msg_throttled_stats**

  説明：このカウンタは、自己保護モードで各インターフェイスでスロットルされた受信メッセージの数を示します。

  メトリック タイプ：カウンタ

  ラベル

  - app_name
  - cluster
  - data_center
  - instance_id
  - インターフェイス
  - message_type
  - cause

- **smf_og_msg_throttling_stats**

  説明：このカウンタは、ピアエンティティが過負荷になっている場合に、各インターフェイスでスロットルされた発信メッセージの数を示します。

メトリック タイプ：カウンタ

ラベル

- app_name
- cluster
- data_center
- gr_instance_id
- instance_id
- インターフェイス
- message_type
- service_name
- throttled_target_peer_type
- cause

# N4 インターフェイス負荷および過負荷制御

SMF は、関連付けられた UPF ノードの負荷と過負荷の状態に基づいて、着信または発信 N4 メッセージを処理します。SMF は、N4 インターフェイスを介した負荷および過負荷のシナリオを制御するために次の機能を実行します。

- **自己過負荷スロットリングおよび N4 メッセージ**：自己保護状態では、SMF は、構成に従って、着信または発信メッセージをスロットリングするか、またはスロットリングから除外します。
- **N4 メッセージのピアの負荷およびオーバーロードの処理**：N4 発信メッセージは、ピアの負荷または過負荷の状態に基づいて処理またはスロットリングされます。

## N4 インターフェイスの負荷と過負荷のレポート

SMF は、SMF プロファイルの下で関連付けられたプロファイルに基づいて、次のアクションを実行します。

| プロファイルが関連付けられました | 行われるアクション |
|---|---|
| 負荷プロファイル | SMF はキャッシュ POD から負荷係数を定期的にフェッチします。SMF は CP 機能負荷を UPF に向けて送信します。 |

| プロファイルが関連付けられました | 行われるアクション |
|---|---|
| 過負荷プロファイル | SMF は、定期的にオーバーロードパラメータ（システムのオーバーロード削減値やオーバーロード状態など）をキャッシュ POD からフェッチします。SMF は CP FunctionOVRL を UPF に送信します。 |

# N4 メッセージの自己過負荷スロットリングと除外

SMF は、次のタイプのメッセージに対して、自己過負荷スロットリングおよびN4 メッセージの除外を実行します。

- 着信メッセージ（Incoming Messages）
- 発信メッセージ（Outgoing Messages）
- セッション レポート DLDR

### 着信 N4 メッセージに対する自己過負荷制御と除外機能

自己保護状態では、デフォルトの動作として、SMF は次の輻輳原因コードを使用してすべての着信 N4 メッセージをスロットリングします。

| 拒否原因コード | 説明 |
|---|---|
| PFCP_ENTITY_IN_CONGESTION | SMF は、PFCP エンティティがノード レベルの輻輳を検出し、過負荷制御を実行すると、この原因コードを返します。この原因コードでは、要求を処理できません。 |

またこの機能により、SMF は過負荷除外プロファイルで構成されたメッセージの優先順位に基づいて、スロットリングから N4 メッセージを除外できます。メッセージの優先順位が N4 インターフェイスに構成されている場合、メッセージは過負荷シナリオでも処理されます。

過負荷除外プロファイルが構成されている場合、自己保護モードにおいて、SMFは受信するすべてのN4メッセージを、構成されたパラメータ（DNN、5QI、ARP、メッセージ優先順位、およびメッセージのカテゴリなど）と比較します。一致した場合、メッセージはSMF でのスロットリングから除外されます。

N4 メッセージの過負荷除外プロファイルを構成するには、「過負荷除外プロファイルの構成」を参照してください。

### 発信 N4 メッセージの自己過負荷スロットリングと除外

自己過負荷状態では、SBI および GTPC インターフェイスでのトリガ メッセージにスロットリングが適用されるため、SMF からの N4 インターフェイスの発信メッセージが間接的にスロットルされます。SMF は、トリガ NF でのスロットリングから除外されたメッセージを処理します。

### DLDR メッセージの自己過負荷スロットリング

図 *207 : SMF* 過負荷中の *N4 DLDR* を処理するためのコール フロー

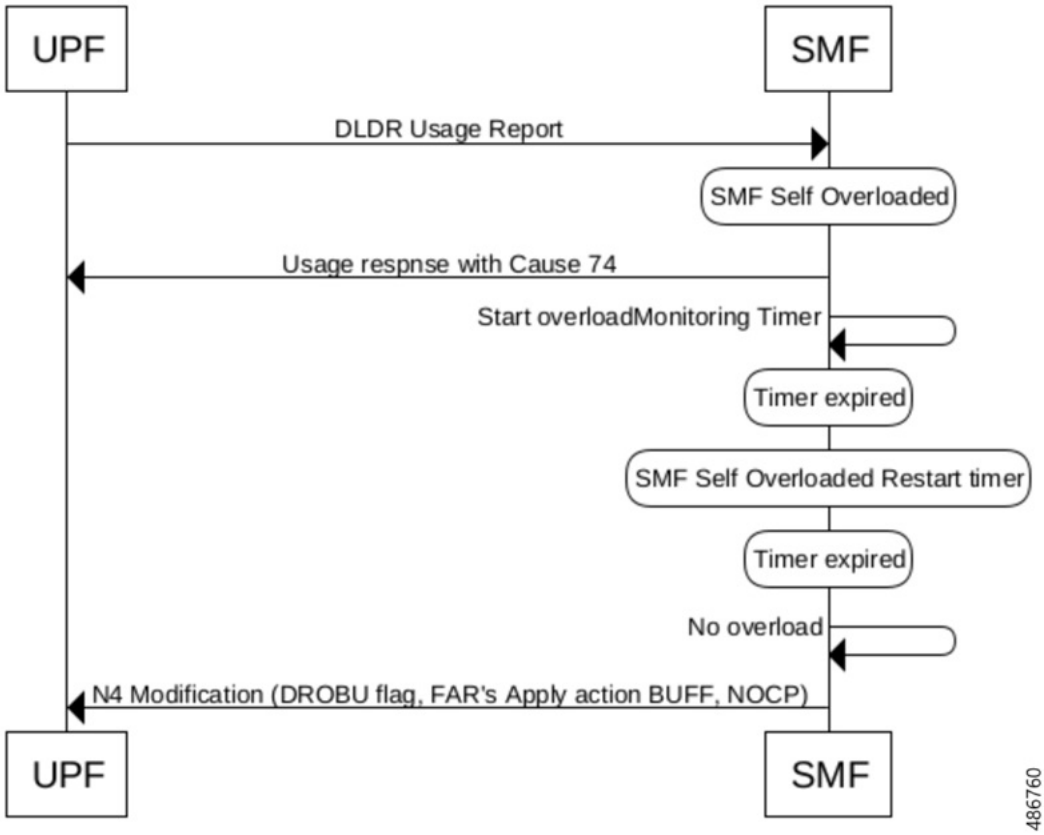



表 *376 : SMF* 過負荷中の *N4 DLDR* の処理コール フローの説明

| ステップ | 説明 |
|---|---|
| 1. | SMF は UPF から DLDR 使用状況レポートを受信します。 |
| 2. | SMF が過負荷（自己保護）状態にある場合、SMF は着信 DLDR メッセージをスロットリングし、 **輻輳原因コード 74 PFCP_ENTITY_IN_CONGESTION** を含む使用応答メッセージを UPF に送信します。 |
| 3. | その後、SMF は、過負荷モニタリング タイマーを開始します。 |
| 4. | タイマーが期限切れになった後も SMF が過負荷状態のままの場合、SMF は過負荷モニタリング タイマーを再開します。 |

| ステップ | 説明 |
|---|---|
| 5. | タイマーの期限が切れた後、SMF が過負荷状態でない場合、SMF は N4 変更メッセージを UPF に向けて送信します。このメッセージには DROBU フラグが含まれており、ダウンリンク FAR に対する BUFF、NOCP として適用アクションを送信します。<br>タイマーの期限が切れる前に、SMF がアイドル モードを終了すると、過負荷モニタリング タイマーは停止し、N4 変更は DROBU フラグとともに送信されません。 |

# N4 インターフェイスのピア負荷とオーバーロードの処理

コントロール プレーン（CP）は、SMF に関連付けられた負荷または過負荷のプロファイルについてユーザープレーン（UP）に通知します。この情報に基づいて、UPは負荷または、過負荷情報を CP ピアに送信するかを決定します。

SMF は、LCI および OCI IE のすべての着信 N4 メッセージと N4 応答を解析します。SMF はピア ノードから LCI IE または OCI IE を受信するたびに、そのノードの負荷と過負荷のパラメータについて学習します。SMF は、N4 メッセージのいずれかで OCI IE を受信した場合、そのピア ノードを過負荷と見なします。

UPF から受信した負荷値は、CP からのセッション負荷を制御するために使用されます。この負荷情報は、UPF 間でセッションのバランスをとるために UPF を選択するために使用されます。オーバーロード情報は、UPF の選択と UPF へのメッセージのスロットリングに使用されます。

SMF は、次の 2 つのメッセージ タイプについてピアの負荷と過負荷を処理します：

- 発信メッセージ
- 受信メッセージ

### 発信 N4 メッセージのピア ロードとオーバーロードの処理

ピアがセッション確立またはセッション変更のために選択された場合、OCI IE のピア/UPF ノードによって伝達される OCI 削減係数に基づいてスロットリングが適用されます。セッションがピア除外プロファイルに基づく除外基準を満たす場合、発信 N4 メッセージはピア ノードによってスロットルされません。

除外プロファイルには、スロットリングから除外されるメッセージに対応する、DNNリスト、5QI リスト、ARP リスト、およびメッセージ優先度のパラメータを含めることができます。

（注） N4 確立要求と N4 変更要求はスロットルされますが、N4 削除要求はスロットルされません。

### ピアの負荷に基づく UPF の選択

SMF は、UPF から受信した LCI 値に基づいて UPF を選択します。受信した負荷の値に従って、UPF のキャパシティが変更されます。これにより、UPF 全体の負荷係数に基づいてセッションが分散されます。UPF 選択プロセスは、各サービス ポッドで個別に適用されます。

（注） UPF 選択プロセスは、各サービス ポッドで個別に適用されます。

### ユーザー プレーンが開始したセッションの終了

自己保護モード中に、UP の負荷状態の改善が確認されない場合、UP は SMF/PGW-C に対するセッション終了要求を開始します。この要求は、UPF が過負荷状態にあることを示すセッション レポート要求メッセージを介して送信されます。SMF/PGW-C は、このセッション レポートに基づいて対応するセッションのリリースを開始します。

Self Protection Termination Request (SPTER）は、自己保護に基づく終了を開始するために、ユーザープレーンからコントロールプレーンに対して設定されます。SMF/PGW-C は、Disc-Reason が **userplane_requested_termination** としてセッションを解放します。

SPTER メッセージ ビットの設定は、SMF と UPF の間で EPFAR 機能がネゴシエートされているかどうかによって異なります。

EPFAR 機能の詳細については、『*UCC 5G UPF* 構成および管理ガイド、リリース *2024.04*』を参照してください。

## 輻輳中のピアの N4 障害処理

ピア UPF ノードがオーバー ロード状態にあり、OCI で受信したピア オーバーロード削減のために発信 N4 メッセージがドロップされると、N4 障害処理メカニズムが開始されます。セッションをクリアするために、SMF では原因コード **peer-overload-resolution** を追加できます。

障害処理プロファイルでこの原因コードを構成するには、」UPF障害処理を有効にする （457 ページ）セクションを参照してください。

SMF が UPF から原因コード **74-PFCP ENTITY IN CONGESTION** を受信し、原因コード 74 **アクション終了**が N4 障害処理プロファイルで構成されている場合、SMF はセッションを削除します。

# SMF での負荷および過負荷制御の構成

SMF での負荷と過負荷の制御の構成には、次の手順が含まれます：

1. 負荷プロファイルの作成 （1178 ページ）
2. 除外プロファイルの作成 （1179 ページ）
3. 過負荷プロファイルの作成 （1180 ページ）

4. 負荷プロファイルと過負荷プロファイルの関連付け （1184 ページ）
5. 負荷係数の構成

（注） 現在、SMF は、SBA インターフェイスを介したピアへの負荷または過負荷情報のアドバタイズをサポートしていません。

# 負荷プロファイルの作成

負荷プロファイルを作成するには、次の構成例を使用します。このプロファイルは、SMF の負荷を計算するために必要なパラメータを定義します。

```
config
   profile load load_profile_name
      load-calc-frequency load_calculation_interval
      load-fetch-frequency load_fetching_time
      advertise [ interval lci_broadcast_interval | change-factor
lci_change_factor ]
      interface gtpc action advertise
      end
```

注：

- **profile load** *load_profile_name*：負荷プロファイル名を指定します。 *load_profile_name* は英数字の文字列である必要があります。

  システム負荷計算と LCI ブロードキャストには負荷プロファイルを使用します。

- **load-calc-frequency** *load_calculation_interval*：システム負荷計算間隔を秒単位で指定します。

  *load_calculation_interval* は、5 ～ 3600 の範囲の整数である必要があります。デフォルト値は 10 秒です。

- **load-fetch-frequency** *load_fetching_time*：サービス ポッドがキャッシュ ポッドから負荷を取得する時間間隔を指定します。

  *load_fetching_time* は、5 ～ 3600 の範囲の整数である必要があります。デフォルト値は 10 秒です。

- **advertise interval** *lci_broadcast_interval*：GTP-C ピアに LCI を送信するための定期的な間隔を指定します。

  *lci_broadcast_interval* は、0 ～ 3600 の範囲の整数で指定する必要があります。値 0 は、すべてのメッセージで LCI が送信されることを示します。デフォルト値は 300 秒です。

- **advertise change-factor** *lci_change_factor*：アドバタイズが発生するまでの、現在の LCI と最後に指定された LCI 間の最小変更を指定します。

*lci_change_factor* は、1 ～ 20 の範囲の整数で指定する必要があります。デフォルト値は 5 です。

- **interface gtpc action advertise**：GTP-C インターフェイスでの LCI パブリッシュまたはブロードキャストを有効にする場合に指定します。デフォルトでは、このオプションは無効になっています。

## 負荷プロファイルの構成の確認

負荷制御プロファイル構成構成を表示するには、次のコマンドを使用します。

**show running-config**

次に、**show running-config** コマンドの出力を示します。

```
#show running-config
.
.
.
profile load loadprofile
load-calc-frequency  10
load-fetch-frequency 10
advertise interval 300
advertise change-factor 5
interface gtpc
  action advertise
exit
exit
```

# 除外プロファイルの作成

自己保護状態時に使用する除外プロファイルを作成するには、次の構成例を使用します。このプロファイルは、スロットリングの決定から除外されるべきセッション関連のメッセージを決定します。

```
config
   profile overload-exclude overload_exclude_profile_name
      arp-list list_of_arps
      dnn-list list_of_dnns
      message-priority { n4 | n7 | n10 | n11 | n16 | n40 | s5 | any }
upto  message_priority
      procedure-list [ session-delete | new-call | xnho | modify |
chf-reauth | inter-rat-ho | intra-rat-ho | imexit-nw | imexit-ue | usar
 ]
      qi5-list list_of_qos_identifiers
      end
```

注：

- **profile overload-exclude** *overload_exclude_profile_name*：除外プロファイル名を指定します。*overload_exclude_profile_name* は 英数字の文字列である必要があります。

  このコマンドで複数の除外プロファイルを構成できます。必ず [過負荷制御（Overload Control）] 構成で除外プロファイル名を参照してください。

- **arp-list** *list_of_arps*：スロットリングの決定から除外する必要がある割り当てと保持の優先順位（ARP）のリストを指定します。

  *list_of_arps* は、1-15 の範囲の整数である必要があります。

  最大 21 のエントリを構成できます。

- **dnn-list** *list_of_dnns*：スロットリングの決定から除外する必要がある DNN のリストを指定します。

  最大 3 つのエントリを構成できます。

- **message-priority [ n4 | n7 | n10 | n11 | n16 | n40 | s5 ] upto** *message_priority*：メッセージをスロットリングから除外する必要があるインターフェイスを指定します。コマンド **upto** は、メッセージの優先順位の範囲を指定します。メッセージの優先順位の範囲は（0 ～ 31）（SBI インターフェイス）、GTPC および PFCP インターフェイス（0 ～ 15）です。

- **procedure-list [ session-delete | new-call | xnho | modify | chf-reauth | inter-rat-ho | intra-rat-ho | imexit-nw | imexit-ue | usar ]**：除外に対して実行する手順を指定します。

- **qi5-list** *list_of_qos_identifiers*：スロットリング決定から除外する必要がある 5G QoS 識別子を指定します。

  *list_of_qos_identifiers* は、1-15 の範囲の整数である必要があります。

## 除外プロファイルの構成の確認

除外プロファイル構成設定を表示するには、次のコマンドを使用します。

**show running-config**

次に、**show running-config** コマンドの出力を示します。

```
#show running-config
.
.
.
profile overload-exclude excludeProfile
dnn-list       [ starent.com.mnc456.mcc123.gprs ]
qi5-list        [ 1 2 ]
arp-list       [ 1 2 ]
procedure-list [ session-delete ]
message-priority s5
  upto 1
exit
exit
```

# 過負荷プロファイルの作成

過負荷プロファイルは、過負荷制御のさまざまな状態と、生じるスロットリングの判断を決定します。

過負荷プロファイルを作成するには、次の構成例を使用します。

```
config
   profile overload overload_profile_name
```

```
overload-exclude-profile self-protection overload_exclude_profile_name

node-level
   tolerance minimum min_percentage maximum max_percentage
   reduction-metric minimum min_percentage maximum max_percentage
   advertise [ interval oci_broadcast_interval | change-factor
oci_change_factor | validity-period oci_validity_period ]
   interface [ gtpc | any] overloaded-action [ advertise ]
peer-level interface gtpc
   message-prioritization group1 weight group2 weight
   interface gtpc
      action throttle
   end
```

**注**：

- **profile overload** *overload_profile_name*：過負荷プロファイル名を指定します。*overload_profile_name* は、英数字の文字列である必要があります。

**重要** このコマンドで構成できる過負荷プロファイルは 1 つだけです。過負荷プロファイルを構成する前に除外プロファイルを作成します。

- **overload-exclude-profile self-protection** *overload_exclude_profile_name*：過負荷自己保護モード中に使用する除外プロファイル名を指定します。

  *overload_exclude_profile_name* は 英数字の文字列である必要があります。

- **node-level**：過負荷の SMF ノードにのみ構成を適用するように指定します。

- **tolerance minimum** *min_percentagemax_percentage* **maximum** ：システム負荷許容の最小と最大のパーセンテージを指定します。 *min_percentage* および *max_percentage* は 、1 ～ 100 の範囲の整数である必要があります。

  *min_percentage*：この値は、システムが正常状態とみなされるしきい値です。デフォルト値は 80 です。

  *max_percentage*：システムが通常状態とみなされるになる最低許容レベルを指定します。デフォルト値は 95 です。

  値が、構成した最小許容値と最大許容値の間にある場合、システムは過負荷状態になっています。

- **reduction-metric minimum** *min_percentagemax_percentage* **maximum** ：トラフィック削減係数の最小と最大のパーセンテージを指定します。 *min_percentage* および *max_percentage* は 、1 ～ 100 の範囲の整数である必要があります。

  *min_percentage*：この値は、最小許容構成と組み合わせたトラフィック削減のパーセンテージです。デフォルト値は 10 です。

*max_percentage*：この値は、最大許容度の設定と組み合わせたトラフィック削減のパーセンテージです。デフォルト値は 100 です。

- **advertise interval** *oci_broadcast_interval*：GTP-C ピアに OCI を送信するための定期的な間隔を指定します。

  *oci_broadcast_interval*は、0 ～ 3600 の範囲の整数で指定する必要があります。値 0 は、すべてのメッセージで OCI が送信されることを示します。デフォルト値は 300 秒です。

- **advertise change-factor** *lci_change_factor*：現在の OCI と最後に指定された OCI との最小変更値を指定します。この値を超えると、OCI によりアドバタイズが行われます。

  *oci_change_factor* は、1 ～ 20 の範囲の整数で指定する必要があります。デフォルト値は 5 です。

- **advertise validity-period** *oci_validity_period*：アドバタイズされた OCI 値の有効期間を指定します。

  *oci_validity_period* は、1 ～ 3600 の範囲の整数で指定する必要があります。デフォルト値は600秒です。

- **interface [ gtpc | any] overloaded-action [ advertise ]** ：ノードが過負荷された場合のアクションを複数のインターフェイスで指定します。これらのインターフェイスの過負荷アクションは、アドバタイズです。

- **peer-level interface gtpc**：GTPC インターフェイスを介して過負荷になっているピアにのみ構成を適用するように指定します。

- **message-prioritization group1** *weight* **group2** *weight*：両方のメッセージ グループのメッセージをスロットリングする必要がある比率を指定します。各グループには、すべての SMF インターフェイスからの定義済みメッセージのセットが含まれています。

  *weight* は、1 ～ 100 の範囲の整数である必要があります。デフォルト値は 50 です。

- **interface gtpc action throttle** ：S6、S8、および S2b インターフェイスを介したスロットリング アクションを有効にします。

（注）

- 過負荷状態では、SMF は入力メッセージを拒否すると、応答で OCI 値を送信します。
- SMF は、期限切れのピア OCI 値と、SMF 内の関連付けられたエントリを識別して削除します。ピアから新しい OCI 値を受信すると、SMF は、以前の OCI と同じシーケンス番号であるかどうかに関係なく、この新しい値を使用します。

## 過負荷プロファイルの構成の確認

過負荷制御プロファイルの構成設定を表示するには、以下のコマンドを使用します。

```
show running-config
```

次に、**show running-config** コマンドの出力を示します。

```
#show running-config
.
.
.
profile overload overloadprofile
overload-exclude-profile self-protection excludeProfile
node-level tolerance minimum 80
node-level tolerance maximum 95
node-level reduction-metric minimum 10
node-level reduction-metric maximum 80
node-level advertise interval 300
node-level advertise change-factor 5
node-level advertise validity-period 600
node-level interface gtpc
  overloaded-action [ advertise ]
exit
exit
```

すべてのピアの過負荷情報を表示するには、次のコマンドを使用します。

**show overload-info peer all**

次に、**show overload-info peer all** コマンドの出力を示します。

```
[smf] smf# show overload-info peer all
                               OVERLOAD

                               CONTROL     OVERLOAD

PEER                           SEQUENCE    REDUCTION                              INSTANCE

TYPE  INTERFACE  PEER IP       NUMBER      METRIC     PERIOD OF VALIDITY          ID

-------------------------------------------------------------------------------------------
SGW   S5         10.1.45.151  1632888403  50         2024-11-08 11:46:03 UTC  1

MME   S5         10.1.2.30    1632888403  60         2024-11-08 11:46:03 UTC  1
```

このコマンドは、すべてのピアの過負荷情報を表示します。

特定のピアの過負荷情報を表示するには、次のコマンドを使用します：

**show overload-info peer all** *peer-type*

次に、**show overload-info peer all SGW** コマンドの出力を示します。

```
[smf] smf# show overload-info peer all SGW
                               OVERLOAD
                               CONTROL     OVERLOAD
PEER                           SEQUENCE    REDUCTION
TYPE  INTERFACE  PEER IP       NUMBER      METRIC     PERIOD OF VALIDITY
-------------------------------------------------------------------------------
SGW   S5         209.165.201.1    1632888445     5        2021-12-01 00:04:02 UTC
```

このコマンドは、S-GW の過負荷情報を表示します。

インターフェイス レベルでピアの過負荷情報を表示するには、次のコマンドを使用します：

**show overload-info peer all interface S5**

次に、**show overload-info peer all interface S5** コマンドの出力を示します。

```
[smf] smf# show overload-info peer all interface S5
                               OVERLOAD
```

```
                              CONTROL     OVERLOAD
PEER                          SEQUENCE    REDUCTION
TYPE  INTERFACE  PEER IP      NUMBER      METRIC     PERIOD OF VALIDITY
-------------------------------------------------------------------------------
SGW   S5         209.165.201.1    1632888445     5        2021-12-01 00:04:02 UTC
MME   S5         209.165.201.2    1632888445     6        2021-12-01 05:04:02 UTC
```

このコマンドは、S5 インターフェイスのすべてのピアの過負荷情報を表示します。

ピアの IP アドレス別に過負荷情報を表示するには、次のコマンドを使用します：

**show overload-info peer all peerIP** *ip_address*

次に、**show overload-info peer all peerIP 209.165.201.2** コマンドの出力を示します。

```
[smf] smf# show overload-info peer all peerIP 209.165.201.2
                              OVERLOAD
                              CONTROL     OVERLOAD
PEER                          SEQUENCE    REDUCTION
TYPE  INTERFACE  PEER IP      NUMBER      METRIC     PERIOD OF VALIDITY
-------------------------------------------------------------------------------
MME   S5         209.165.201.2    1632888445     6        2021-12-01 05:04:02 UTC
```

# 負荷プロファイルと過負荷プロファイルの関連付け

SMF サービス プロファイルにロードコントロールプロファイルとオーバーロードプロファイルを関連付けるには、次の設定例を使用します。

```
config
   profile smf smf_profile_name
      load-profile load_profile_name
      overload-profile overload_profile_name
      end
```

注：

- **profile smf** *smf_profile_name*：既存の SMF サービス プロファイル名を指定します。

  *smf_profile_name* は 英数字の文字列である必要があります。

- **load-profile** *load_profile_name*：SMF サービス プロファイルに関連付ける負荷のプロファイル名を指定します。

  *load_profile_name* は 英数字の文字列である必要があります。

- **overload-profile** *overload_profile_name*：SMF サービス プロファイルに関連付けるオーバーロード プロファイル名を指定します。

  *overload_profile_name* は英数字の文字列である必要があります。

- オーバーロード プロファイルと SMF プロファイルとのリンクは、負荷プロファイルがリンクされている場合にのみ機能します。

## 負荷と過負荷プロファイルの関連付けの確認

負荷および過負荷プロファイルと SMF サービス プロファイルとの関連付けを表示するには、次のコマンドを使用します。

**show running-config**

次に、**show running-config** コマンドの出力を示します。

```
#show running-config
.
.
.
profile smf smf1
<……..>
load-profile  loadprofile
overload-profile overloadprofile
<……..>
exit
```

# 負荷係数の構成

この設定により、ユーザーは特定の時間間隔での負荷係数の計算とサービス ポッドの除外を設定できます。

**手順**

**ステップ 1** コマンド **load factor**を使用して、負荷係数の周波数計算を構成します

**例**：

```
[smf] smf(config)# load factor
```

**ステップ 2** コマンド **[ no ] load factor { calc-frequency** *calc_frequency_time* **| exclude-pods** *exclude_pod_name***}** を使用して、負荷係数計算の頻度または除外するサービス ポッドを定義します。

**例**：

```
[smf] smf(config)# load factor calc-frequency 15
[smf] smf(config)# load factor exclude-pods bgpspeaker-pod
```

- CLI **calc-frequency** のデフォルト値は 30 です。
- CLI **exclude-pods** は、次のサービス ポッドを除外します：
  - **bfdmgr**
  - **bgpspeaker-pod**
  - **cache-pod**
  - **edr-monitor**
  - **georeplication-pod**
- CLI **calc-frequency** と **exclude-pods** の両方に下位互換性があります。

**ステップ 3** コマンド **exit** を使用してグローバル構成モードを閉じます。

**例**：

```
[smf] smf(config)#exit
```

## 設定の確認

**show resources** コマンドは、負荷係数の構成パラメータを表示します。

```
[smf] smf# show resources
Thu Oct  10 09:32:52.900 UTC+00:00
                                TOTAL    USED     DISK
                                NODE     POD      USAGE   GO                GC
                          CPU   MEMORY   MEMORY   IN      ROUTINES  GC      PAUSE   LOAD
POD INSTANCE              USAGE IN MB    IN MB    KBPS    COUNT     COUNT   IN NS   FACTOR
-------------------------------------------------------------------------------------------
cache-pod-1               3     32096    99       0       438       672     99      0.438
cache-pod-2               2     32097    87       0       438       671     87      0.438
diameter-ep-gx-client-0   2     32096    92       0       217       670     92      0.19999881
diameter-ep-gy-client-0   2     32096    83       0       173       670     83      0.18888578
dns-proxy-0               0     32096    64       0       86        672     64      0.39150715
gtpc-ep1-0                2     32096    112      0       293       672     112     0.24416667
gtpp-ep-0                 2     32096    109      0       208       669     109     0.22245248
gtpp-ep-1                 2     32097    110      0       202       669     110     0.22777763
```

# ノード過負荷

ノード過負荷は、NF 展開内のすべての SMF ポッドのリソース使用率データを参照します。SMFは、これらのポッドの現在のリソース使用率データを定期的に収集します。リソース使用率データを読み取るデフォルトの頻度は 5 秒です。SMF は CPU、メモリ使用率、go-routing を監視し、ポッドの現在、過去 5 分間、および 15 分間の平均値を保存します。

### ポッド レベルの負荷係数

ポッドの CPU、メモリ使用率、および Go ルーチンの現在の値に対する最大値は、その負荷係数の計算に使用されます。GOMAXPROCS 環境変数は、ポッドのキャパシティを計算するために使用されます。コアあたりの最大値は定数値で定義され、CPU、メモリ、および Go ルートのキャパシティを派生させるために使用されます。

コアあたりの最大値の例を以下に示します。

MAX_CPU_PERCENTAGE_PER_CORE = 100

MAX_MEMORY_PER_CORE = 4 GB

MAX_GO_ROUTINE_PER_CORE = 10,000

**NewApplicationWithOptions** は最大値を取得するために使用されます。アプリケーションによって値が提供されない場合は、デフォルト値が使用されます。

ポッドの負荷係数は次のように計算されます。

- CPU load factor = Current load percentage / Maximum load percentage at pod x 100
- Memory load factor = Current memory usage / Maximum memory at pod x 100

- Go-routine load factor = Go-routine count / Maximum Go-routine count at pod x 100

CPU、メモリ、および Go ルートの負荷係数の最大値は、最終的な負荷係数と見なされます。

### OAM ポッドからのセルフ NF 負荷係数

OAM ポッドは、各 SMF ポッドから負荷係数データを定期的に収集し、キャッシュ ポッドを更新します。また、OAM ポッドは、CDL からセッション負荷係数を受け取り、同時にキャッシュ ポッドを更新します。

システム API は、次のロジックに基づいて負荷係数のデータを提供します。

- **ポッド レベルの負荷係数** ：アプリケーションが SMF でリソース使用率データを取得するためにポッドの負荷係数をクエリしている場合、応答には、そのクラスタ内のすべてのポッド タイプ カテゴリの最大負荷係数が含まれます。
- **システム レベルの負荷係数** ：アプリケーションがシステム レベルで負荷係数をクエリしている場合、応答には、そのクラスタ内のすべてのポッドの最大負荷係数とセッション負荷係数データが含まれます。
- **カテゴリに基づく負荷係数** ：アプリケーションが特定のタイプのサービス（smf-service、smf-rest-ep など）の負荷係数をクエリする場合、次の条件が満たされます。
  - **アクティブ-アクティブ展開** ：クエリ応答に負荷係数の平均値が含まれています。
  - **アクティブ-スタンバイ展開** ：クエリ応答に負荷係数の最大値が含まれています。

セッション数を処理するシステム レベルのキャパシティは、SMF で構成されます。各セッションの負荷係数は、OAM ポッドで現在のセッション数 / セッションの最大数として計算されます。

### 最大セッション数

データストア構成は、サポートされている名前空間のセッション負荷係数を含めるために使用されます。値は、セッションデータベースの登録時にアプリケーションから設定する必要があります。値が設定されていない場合は、デフォルトの 1,000,000 がセッション負荷係数の計算に使用されます。

### OAM に対するアプリケーション レベルの ConfigMap サポート

OAM インフラ チャートは、次の方法で OAM アプリケーションから configmaps をマウントします。

- **Infra-OAM**
  - テンプレートを更新して、render.yaml から構成マップのボリュームを追加します。
  - volumeMounts を使用して、render.yaml からボリュームをマウントするようにテンプレートを更新します。
- **Application-OAM**

- アプリケーション構成チャート内と同じ構成マップを追加します。
- 構成マップに Values.yaml または CLI から値を指定します。

# モニタリングおよびトラブルシューティング

このセクションでは、機能のモニタリングとトラブルシューティングに使用できるバルク統計に関する情報を説明します。

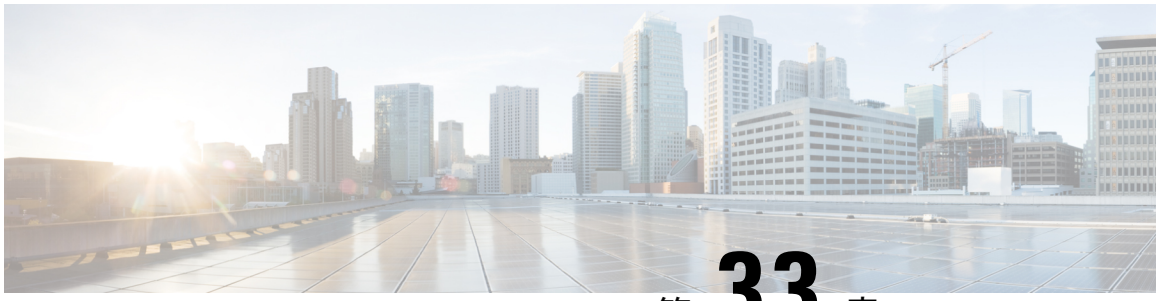
## 統計

次の統計情報は、過負荷制御のサポートで使用できます。

| バルク統計 | 統計情報の種類 | 説明 |
|---|---|---|
| endpoint_overload_status | ゲージ | Endpoint-Name、Interface-Name、および Overload-Level がラベルとして含まれます。いずれかのレベル（低/高/重大）がヒットすると、ゲージ値は 1 に設定されます。通常の状態では、値は 0 に設定されます。 |
| endpoint_client_overload_status | ゲージ | エンドポイント名、インターフェイス名、ピア ホスト名、および過負荷レベルがラベルとして含まれます。いずれかのレベル（低/高/重大）がヒットすると、ゲージ値は 1 に設定されます。通常の状態では、値は 0 に設定されます。 |
| endpoint_pending | ゲージ | エンドポイントに対する現在の未処理の要求を表示します。エンドポイント名とインターフェイス名がラベルとして含まれています。 |
| endpoint_client_pending_request | ゲージ | エンドポイントに接続されているピアに対する現在の未処理の要求を表示します。これには、エンドポイント名、インターフェイス名、およびエンドポイントにラベルとして接続されたピア ホスト アドレスが含まれます。 |
| endpoint_overload_exclude | カウンタ | 過負荷制御メカニズムから除外されたメッセージと優先度の詳細を表示します。メトリックはメッセージごとに増分され、過負荷制御メカニズムがバイパスされます。 |

SBA、N4、および GTPC インターフェイスの負荷および過負荷処理の一環として、次のメトリックが拡張されています。

- **自己過負荷状態**： SMF が過負荷状態になると、統計 **smf_inc_msg_throttling_stats** は、ドロップされた着信メッセージの数だけ増加します。次の新しいメッセージが、label **message_type**の一部として追加されています。
  - **SBI インターフェイス**：
    - N7SmPolicyUpdateNotifyReq
    - N7SmPolicyUpdateSuccess
    - N7SmPolicyTerminateNotifyReq
    - N11SmContextCreateReq
    - N11SmContextRetrieveReq
    - N11SmContextStatusNotifyReq
    - N16PduSessionHsmfUpdateReq
    - N16PduSessionHsmfUpdateReqClient
    - N16PduSessionVsmfUpdateReq
    - N16PduSessionVsmfUpdateReqClient
    - N16VsmfPduSessionCreateReq
    - N16HsmfSmContextRetrieveReq
    - N10UpdateNotifyReq
    - N10PcscfRestorationNotifyReq
  - **GTPC インターフェイス**：
    - S5S8CreateSessReq
    - S5S8ModifyBearerCmd
    - S5S8ModifyBearerReq
    - S5S8CreateBearerRsp
    - S5S8UpdateBearerRsp
  - **N4 インターフェイス**：
    - N4SessionEstablishmentReq
    - N4SessionModificationReq
- **ピア過負荷状態**： ピア ノードが過負荷状態になると、統計 **smf_og_msg_throttling_stats** は、ドロップされた発信メッセージの数だけ増加します。



第 33 章

# 実行最適化サポート


- 機能の概要と変更履歴 （1191 ページ）
- 機能説明 （1194 ページ）
- バッチ ID の割り当て、リリース、および調整のサポート （1194 ページ）
- キャッシュ ポッドの最適化 （1197 ページ）
- CDL フラッシュ間隔およびセッション有効期限のチューニング構成 （1197 ページ）
- Ops センターを使用したドメインベースのユーザー認可 （1198 ページ）
- エッジ エコーの実装 （1201 ページ）
- GTPC エンドポイント ポッドのエンコーダとデコーダの最適化 （1203 ページ）
- ETCD ピア最適化サポート （1204 ページ）
- ローミング ピア最適化 （1204 ページ）
- ETCD トラフィックの最適化 （1207 ページ）
- ETCD クライアントのフォールバック （1209 ページ）
- フラグ DB データベースの更新 （1210 ページ）
- RRC 非アクティブ原因コードに基づく PDU セッション変更の処理 （1211 ページ）
- K8 活性プローブを使用したポッド障害検出 （1220 ページ）
- 復元力の処理 （1221 ページ）
- IoT 展開でのサブスクライバ セッションのスケーリング （1226 ページ）


# 機能の概要と変更履歴

## 要約データ

**表 *377*: 要約データ**

| | |
|---|---|
| 該当製品または機能エリア | SMF |
| 該当するプラットフォーム | SMI |

| | |
|---|---|
| 機能のデフォルト設定 | バッチ ID の割り当て、リリース、調整のサポート：無効：有効にするには構成が必要<br>キャッシュ ポッドの最適化<br>CDL フラッシュ間隔およびセッション有効期限のチューニング構成：有効：無効にするには構成が必要<br>Opsセンターを使用したドメインベースのユーザー認可<br>エッジ エコーの実装：有効：常時オン<br>GTPC エンドポイント ポッドのエンコーダとデコーダの最適化：無効：有効にするには構成が必要<br>ETCD ピア最適化のサポート：有効：常時オン<br>ETCD トラフィックの最適化：有効：常時オン<br>ローミングピアの最適化：無効：有効にするには構成が必要<br>DB データベース更新へのフラグの設定：有効：常時オン<br>GTPC IPC クロスラックのサポート：無効：有効にするには構成が必要<br>RRC 非アクティブ原因コードに基づく PDU セッション変更の処理：無効：有効にするには構成が必要<br>サービス間ポッド通信：無効：有効にするには構成が必要<br>復元力の処理：無効：有効にするには構成が必要 |
| 関連資料 | 該当なし |

# 更新履歴

表 *378 :* マニュアルの変更履歴

| 改訂の詳細 | リリース |
|---|---|
| 次のサポートが追加されました：<br>• ETCD トラフィックの最適化<br>• ETCD クライアントのフォールバック<br>• K8 ポッドの稼働状態チェックの改善<br>• 復元力の処理における Diameter サービス ポッド<br>• ローミング ピア最適化 | 2023.03.0 |
| 次のサポートが追加されました<br>• キャッシュ ポッドの最適化<br>• GTPC エンドポイント ポッドのエンコーダとデコーダの最適化<br>• フラグ DB データベースの更新<br>• 復元力処理 | 2023.01.0 |
| 最初の導入。<br>次のサポートが追加されました。<br>• バッチIDの割り当て、リリース、および調整のサポート<br>• CDL フラッシュ間隔およびセッション有効期限のチューニング構成<br>• Ops センターを使用したドメインベースのユーザー認可<br>• エッジ エコーの実装<br>• ETCD ピア最適化サポート<br>• GTPC IPC クロスラック サポート<br>• RRC 非アクティブ原因コードに基づく PDU セッション変更の処理 | 2022.04.0 |

# 機能説明

この章では、パフォーマンス最適化機能について説明します。

一部のパフォーマンス最適化機能は、cnSGW-C と SMF に共通です。

cnSGW-C 機能の詳細については、『*UCC 5G cnSGWc* 構成および管理ガイド』を参照してください。

# バッチ ID の割り当て、リリース、および調整のサポート

## 機能説明

nodemgr は、接続状態にあるサブスクライバに一意の ID を割り当てます。サブスクライバが接続解除されると、一意の ID が nodemgr に解放されます。割り当てと割り当て解除の手順が増えると、nodemgr のパフォーマンスが影響を受け、sgw-service はこれらの手順を完了するために長時間待機し続けます。

バッチ ID の割り当て、リリース、および調整サポート機能は、sgw-service と nodemgr 間の対話を削減し、nodemgr のパフォーマンスを最適化するメカニズムを提供します。

## 機能の仕組み

ここでは、この機能の仕組みを説明します。

**バッチ ID の割り当て**：

バッチ ID の割り当てには、次の手順が含まれます。

- sgw-service では、フリー ID をサブスクライバに割り当てることで ID ストアが管理されます。ID がストアで利用できない場合、sgw-service はバッチ ID 割り当て要求を nodemgr に送信します。
- nodemgr は応答で、ID 予約レポート間隔で 128 の ID を一括で返します。sgw-service は、nodemgr から受信した ID で ID ストアを更新し、ID 予約レポート間隔のタイマーを開始します。
- [ID予約レポート間隔（ID Reserve Report Interval）] で構成された期間の前にすべての ID が使用されている場合、sgw-service は、以前の要求からすべての ID を予約する通知とともに、ID 割り当て要求のバッチを nodemgr に送信します。
- sgw-service がすべての ID を割り当てる前に ID 予約レポート間隔タイマーが期限切れになった場合、sgw-service は予約レポート バッチ操作を介して未使用の ID を nodemgr に返します。

**バッチ ID のリリース**：

バッチ ID のリリースには、次の手順が含まれます。

- sgw-service は ID ストアが各ノードマネージャに対して解放する ID を管理します。
- sgw-service は、ID の割り当てが解除されるたびに ID を ID ストアに返します。ID ストアがいっぱいの場合、sgw-service はバッチ ID リリース要求とリリースされた ID をそれぞれのノード マネージャに送信します。
- sgw-service が ID ストアへの ID の追加を開始すると、ID リリース タイマーがスタートします。
- バッチ ID がリリースされる前、またはバッチがいっぱいになる前に ID リリースタイマーが期限切れになった場合、sgw-service はリリースされた ID を nodemgr に送信します。

### バッチ ID の調整

バッチ ID の調整は、サービス ポッドと nodemgr ポッドの再起動時に発生します。

サービス ポッドの再起動時：

1. サービス ポッドがバッチ ID を受信し、ID を割り当てる前に応答しなくなった場合、nodemgr はバッチ ID 予約要求を取得できず、ID 予約手順がタイムアウトします。このようなシナリオでは、nodemgr は予約されていないか、割り当てられていない ID を CDL と調整します。サブスクライバに割り当てられていない ID は ID ストアに解放されます。
2. サービス ポッドは、解放された ID を収集し、無応答になった場合 ID は nodemgr に解放します。このシナリオでは、ID はドロップされます。

nodemgr のポッドの再起動時に、次のように動作します。

1. 実行中のバッチ ID 予約要求とバッチ ID リリース要求に存在する ID はドロップされます。
2. nodemgr は、割り当てられた ID をバッチで cachemgr に通知します。ID を cachemgr に通知する前に nodemgr が応答しなくなった場合、nodemgr は再起動後に新しい ID の割り当てを開始します。nodemgr は、最後に割り当てられた ID とバッチ サイズに基づいて ID を割り当てます。

# 機能設定

この機能を構成するには、次の構成を使用します。

```
config
   sgw sgw_name
      resmgr-batch-operation [ disable | enable ]
      end
```

注：

**resmgr-batch-operation [ disable | enable ]**：バッチ操作を構成します。デフォルトでは、**resmgr-batch-operation** は無効です。

# OAM サポート

ここでは、この機能の操作、管理、およびメンテナンス サポートについて説明します。

## バルク統計

バッチ ID の割り当ておよびリリースのサポート機能では、次の統計情報がサポートされています。

- sgw_resource_mgmt_stats：cnSGW-C リソース管理統計情報の合計数をキャプチャします。

  サンプル クエリ：

```
sgw_resource_mgmt_stats{app_name="smf",cluster="Local",data_center="DC",gr_instance_id="1",
id_req_type="id_batch_alloc",instance_id="0",service_name="sgw-service",status="attempted"}
 3
:sgw_resource_mgmt_stats{app_name="smf",cluster="Local",data_center="DC",gr_instance_id="1",
id_req_type="id_batch_alloc",instance_id="0",service_name="sgw-service",status="success"}
 3
```

```
sgw_resource_mgmt_stats{app_name="smf",cluster="Local",data_center="DC",gr_instance_id="1"
,id_req_type="id_batch_dealloc",instance_id="0",service_name="sgw-service",status="attempted"}
 2
sgw_resource_mgmt_stats{app_name="smf",cluster="Local",data_center="DC",gr_instance_id="1",id_req_type=
"id_batch_dealloc",instance_id="0",service_name="sgw-service",status="success"}
 2
```

```
sgw_resource_mgmt_stats{app_name="smf",cluster="Local",data_center="DC",gr_instance_id="1",
id_req_type="id_batch_dealloc_timeout",instance_id="0",service_name="sgw-service",status="attempted"}
 1
:sgw_resource_mgmt_stats{app_name="smf",cluster="Local",data_center="DC",gr_instance_id="1",id_req_type
="id_batch_dealloc_timeout",instance_id="0",service_name="sgw-service",status="success"}
 1
```

```
sgw_resource_mgmt_stats{app_name="smf",cluster="Local",data_center="DC",gr_instance_id="1",
id_req_type="id_batch_release_timeout",instance_id="0",service_name="sgw-service",status="attempted"}
 1
-:sgw_resource_mgmt_stats{app_name="smf",cluster="Local",d-ata_center="DC",gr_instance_id="1",id_req_type
="id_batch_release_timeout",instance_id="0",service_name="sgw-service",status="success"}
 1
```

- nodemgr_rmgr_batch_reconcile_stats：調整のために送信されるバッチの総数をキャプチャします。

  サンプル クエリ：

```
nodemgr_rmgr_batch_reconcile_stats{app_name="smf",cluster="Local",data_center="DC",instance_id="0",
 service_name="nodemgr",status="success"} 1
```

- nodemgr_resource_mgmt_resp_stats：調整のために解放されたIDの合計数をキャプチャします。

  サンプル クエリ：

```
nodemgr_resource_mgmt_resp_stats{app_name="smf",cluster="Local",data_center="DC",error="",

gr_instance_id="0",instance_id="0",ip_ver_type="IP_TYPE_NONE",req_type="ID_REQ_REL_RECONCILE",
 service_name="nodemgr",status="success"} 16
```

バルク統計のサポートの詳細については、「*UCC* サービング ゲートウェイ コントロール プレーン機能メトリック リファレンス」を参照してください。

# キャッシュ ポッドの最適化

## 機能説明

cnSGW-Cは、GTPCエンドポイントでのキャッシュ ポッドクエリを削減するためのキャッシュ ポッドの最適化をサポートしています。アフィニティの取得クエリは、GTPCエンドポイントへの発信要求または応答メッセージでアフィニティ情報を受信するために使用されます。この最適化により、GTPCエンドポイントポッドは、今後の要求メッセージのキャッシュポッドにクエリを送信しません。

# CDL フラッシュ間隔およびセッション有効期限のチューニング構成

## 機能説明

デフォルトのサービスポッド パラメータを変更して、スループット パフォーマンスを微調整し、負荷パフォーマンスを最適化できます。

## 機能設定

この機能を構成するには、次の構成を使用します。

```
config
   profile sgw sgw_name
      timers [ session-expiration-in-secs session_expiration |
affinity-expiration-in-secs affinity_expiration |
```

```
session-dbsync-interval-in-ms database_sync ]
      end
```

注：

- **session-expiration-in-secs** *session_expiration* ：セッションがサービス ポッドにキャッシュされる期間を指定します。 *session_expiration* は 、1 ～ 600 ミリ秒の範囲の値を受け入れます。デフォルト値は 30 ミリ秒です。
- **affinity-expiration-in-secs** *affinity_expiration*：サービス ポッドやその他のポッドでセッション アフィニティ キーが有効である期間を指定します。 *affinity_expiration* は 、1 ～ 1200 秒の範囲の値を受け入れます。デフォルトは 80 秒です。
- **session-dbsync-interval-in-ms** *database_sync* ：セッションがデータベースで同期されるまでの期間を指定します。 *database_sync* は、1 ～ 10000 ミリ秒の値を受け入れます。デフォルトのタイムアウト値は 500 ミリ秒です。

# Ops センターを使用したドメインベースのユーザー認可

## 機能説明

SMF と cnSGW-C は、Ops Center を使用したドメインベースのユーザー認証をサポートしています。ユーザー単位でアクセスを制御するには、Ops Center AAA で TACACS プロトコルを使用します。このプロトコルを使用すると、ルータまたは NAS へのアクセスを試みるユーザーを集中的に検証できます。

ルール リストで NETCONF アクセス制御（NACM）ルールを構成します。構成したルールを Ops Center の構成にマッピングして、グループを適切な運用許可にマッピングします。次の基準と製品に基づいた構成を使用します。

- NACM ルールと SMF ドメインベースのグループを使用して、SMF ベースの構成にアクセスのみ、または更新を許可するように Ops Center を構成します。
- NACM ルールと cSGW-C ドメインベースのグループを使用して、cSGW-C ベースの構成にアクセスのみ、または更新を許可するように Ops Center を構成します。
- NACM ルールと cSGW-C ドメインベースのグループを使用して、CCG ベースの構成にアクセスのみ、または更新を許可するように Ops Center を構成します。

（注） NSO サービス アカウントは、構成全体にアクセスできます。

# 機能の仕組み

Ops センターでこの機能構成をサポートするために、domain-based-services 構成が TACACS セキュリティ構成に追加されます。TACACS フローの変更は次のように機能します。

- **domain-based-services** パラメータを構成している場合、TACACS プロセスに送信される構成済みのユーザー名は、ユーザー ID をユーザー ID と ドメインに分割します。ドメインデリミタである分割文字は、domain-based-services で構成されます。これらの分割文字は「@」、「/」、または「\」であり、ドメインおよびユーザー ID 情報を取得するために次の形式で使用されます。
  - @ — <user id>@<domain>
  - / — <domain>/<user id>
  - \ — <domain>\<user id>
- TACACS は、既存のフローに従って認証および認可します。ただし、domain-based-services 機能が有効になっていて、TACACS がユーザーを認証および認可する場合、次のステップが TACACS フロー手順に追加されます。
  - Network Services Orchestrator（NSO）が NSO サービス アカウントとしてログインすると、そのセッションは、**domain-based-services nso-service-account group** *group-name* で設定した特定の NACM グループを受け取ります。これは、機能的には NSO の動作と同じです。
  - 指定したドメインがグループ マッピングに存在する場合は、**domain-based-services domain-service** *domain* **group** *group-name* で構成した NACM グループが適用されます。
  - ユーザーにドメインがない場合、またはドメインがドメインからグループへのマッピングに存在しない場合、**domain-based-services no-domain group** *group-name* で構成した **no-domain** NACM グループが適用されます。**no-domain** 構成が存在しない場合、ユーザー値は拒否されます。

この機能を有効にするには、次のオプションを指定して **domain-based-services** CLI コマンドを構成する必要があります。

- NSO サービス アカウント
- ドメイン サービス
- ドメイン デリミタ
- ドメインなし

# 機能設定

Ops センターを使用してドメインベースのユーザー認証を有効にするには、次の構成例を使用します。

```
config
  tacacs-security domain-based-services [ domain-delimiter delimiter_option
 | domain-service domain_service_name [ group service_group_name  ] | no-domain
 group service_group_name | nso-service-account [ group service_group_name |
id service_account_id ] ]
  end
```

注：

- **domain-based-services [ domain-delimiter** *delimiter_option* **| domain-service** *domain_service_name* **[ group** *service_group_name* **] | no-domain group** *service_group_name* **| nso-service-account [ group** *service_group_name* **| id** *service_account_id* **] ]**: Configure the required domain-based-services value.**domain-based-services** には次のオプションが含まれます。
  - **domain-delimiter**：ドメインの決定に使用するデリミタを指定します。このオプションは必須であり、次の値を使用できます。
    - @：ドメインデリミタが「@」の場合、ユーザー値は <user> @<domain> 形式になります。
    - / : ドメインデリミタが「/」の場合、ユーザー値は次の形式になります。<domain> /<user> 。
    - \ : ドメインデリミタが「\」の場合、ユーザー値は<domain>\<user> 形式になります。
  - **domain-service**：ドメインおよびそのドメインのグループ マッピングのリストを指定します。キーはドメインの名前で、グループはドメインに割り当てられたグループです。このリストの少なくとも 1 つのオプションを構成する必要があります。
  - **no-domain**：ドメインを持たないグループを指定します。またはドメインがドメインサービスマッピングで使用できない場合、このグループが受け入れ応答で送信されます。
  - **nso-service-account**：ID とグループを持つNSO サービスアカウントを指定します。このパラメータを構成する場合は、ID フィールドとグループ フィールドを構成する必要があります。ID とグループには文字列値が必要です。

## 設定例

次に、tacacs セキュリティ モードでのドメインベースのユーザー認証の例を示します。

```
config
   tacacs-security domain-based-services nso-service-account id nsid
      tacacs-security domain-based-services nso-service-account group nso-group
   tacacs-security domain-based-services no-domain group read-operational
   tacacs-security domain-based-services domain-delimiter @
   tacacs-security domain-based-services domain-service etcd
      group etcd
exit
tacacs-security domain-based-services domain-service sgw
   group sgw_1
exit
tacacs-security domain-based-services domain-service smf
```

```
   group smf
exit
```

## 設定の確認

構成を確認するには、次の show コマンドを使用します。

**show running-config tacacs-security**

この show コマンドの出力には、TACACS セキュリティ内のドメインベースのサービスのすべての構成が表示されます。

```
[smf] smf# show running-config tacacs-security
tacacs-security service smf
tacacs-security server 1
address 209.165.200.234
key $8$+twbdL2ZCgmjVswgp7kFJp8+SMXDjQRTZgoPVa3oEwY=
exit
tacacs-security domain-based-services nso-service-account id nsid
tacacs-security domain-based-services nso-service-account group nso-group
tacacs-security domain-based-services no-domain group read-operational
tacacs-security domain-based-services domain-delimiter @
tacacs-security domain-based-services domain-service etcd
group etcd
exit
tacacs-security domain-based-services domain-service sgw
group sgw_1
exit
tacacs-security domain-based-services domain-service smf
group smf
exit
```

# エッジ エコーの実装

## 機能説明

非マージモードでは、udp-proxy ポッドはエンドポイントとして機能し、gtpc-ep はピア ノードからのエコー要求に応答します。

gtpc-ep では、システムが CEPS を大量に受信した場合にトラフィックが発生し、gtpc-ep が udp-proxy からメッセージをピックアップするレートと、udp-proxy がメッセージを取得するれ一pとに不一致が生じるとき、トラフィックが発生します。

gtpc-ep がロードされると、udp-proxy と gtpc-ep の間のキューがいっぱいになり、udp-proxy の一部のメッセージがドロップされることがあります。これらがエコー要求メッセージである場合、エコー応答を受信していないため、ピアはパス障害を検出します。さらに、ピアは sgw サービスに送信されたすべてのセッションをクリアします。

## 機能の仕組み

ここでは、この機能の仕組みを説明します。

nodemgr は次の手順でエコー要求を処理します。

- nodemgr には、各 GR インスタンス ID と GTPC ピアの自己再起動カウンタキャッシュが保持されます。
- UDP プロキシ ポッドがピアからエコー要求を受信し、自己再起動カウンタ値が自己再起動カウンタ キャッシュで利用できない場合、UDP プロキシポッドがエコー要求を GTPC-EP に転送します。
- GTPC-EP が UDP プロキシ メッセージ メタデータの一部としてエコー応答で自己再起動カウンタを送信します。UDP プロキシが自己再起動カウンタを自己再起動カウンタ キャッシュに保存します。UDP プロキシは、ピアからエコー要求を受信し、自己再起動カウンタ値が自己再起動カウンタ キャッシュで利用可能な場合、再起動カウンタとともにエコー応答を送信します。
- UDP プロキシがエコー要求メッセージを GTPC-EP に転送します。GTPC-EP がエコー要求を処理し、必要に応じて nodemgr に転送します。
- ピア再起動カウンタ値が変更されると、nodemgr はパス障害を検出します。
- エコー応答では、GTPC-EP が UDP プロキシ メッセージ メタデータの自己再起動カウンタを UDP-Proxy に送信します。自己再起動カウンタが自己再起動カウンタ キャッシュに保存されているカウンタとは異なる場合、UDP プロキシはキャッシュ内の自己再起動カウンタを更新し、GTPC-EP から受信したエコー応答をドロップします。

（注） GTPC-EP がマージ モードで開始された場合、エッジ エコー機能はサポートされません。

#### Heartbeat

GTPV2インターフェイスのエコー要求メッセージとエコー応答メッセージを処理するために、GTPC-EP と UDP プロキシ ポッドの間にハートビート キューが実装されます。ハートビート キューは、PFCP インターフェイスのプロトコルと UDP プロキシ ポッド間のハートビート要求およびハートビート応答メッセージに関与します。

# OAM サポート

ここでは、この機能の操作、管理、およびメンテナンス サポートについて説明します。

## バルク統計サポート

エッジ エコー実装機能では、次の統計情報がサポートされています。

- ハートビート キュー ステータス：

```
sum(irate(ipc_response_total{rpc_name~=".ipc_stream_hb."}[10s])) by
(service_name, instance_id, status, status_code, rpc_name, dest_host)
```

• EdgeEcho メッセージを確認します。

```
sum(irate(udp_proxy_msg_total{ message_name ="edge_echo"}[30s])) by
(message_name, message_direction, status)
```

ハートビートキューおよび EdgeEcho メッセージを有効にするには、以下を使用して udp_proxy_msg_total のトレースレベル統計を構成します。

```
infra metrics verbose application
   metrics udp_proxy_msg_total level trace
   exit
```

（注） ハートビートおよびEdgeEcho統計を有効にすると、udp-proxyポッドのパフォーマンスが低下する可能性があります。

# GTPC エンドポイント ポッドのエンコーダとデコーダの最適化

## 機能説明

SMF は **enable-direct-encdec** CLI コマンドを使用して、GTPC エンドポイント ポッドに関連付けられている IE のエンコードとデコードを最適化します。この最適化により、メモリ管理が向上し、ガベージ コレクション時間が短縮されます。

## 機能設定

この機能は、実行時に有効にすることができます。デフォルトでは、この機能は無効になっています。

この機能を構成するには、次の構成例を使用します。

```
config
  instance instance-id instance_id
    endpoint gtp
    interface s5e
      enable-direct-encdec true | false
    interface s11
      enable-direct-encdec true | false
    exit
  exit
```

注：

- **enable-direct-encdec true | false**: エンコーダとデコーダを有効にするには、値を **true** として選択します。デフォルトでは、このフィールドの値は **false**です。

# ETCD ピア最適化サポート

## 機能説明

多数の GTPC ピアが SMF または cnSGW-C に接続されている場合、ETCD のパフォーマンスに影響が出ます。各ピアは ETCD のレコードと見なされ、タイムスタンプはピア単位で 30 秒ごとに更新されるため、ETCD が継続的に更新され、システム全体のパフォーマンスに影響を与える大量のトラフィックが生成されます。

ETCD ピア最適化機能は、ピア管理の最適化を促進し、ETCD に対するパフォーマンスの影響の軽減を可能にします。

## 機能の仕組み

ここでは、この機能の仕組みを説明します。

各ピアをETCD レコードエントリと見なさず、各ピアの IP アドレスのハッシュ値に基づいて、複数のピアをピア グループとしてグループ化します。これにより、ETCD のエントリの数が減少します。デフォルトでは、最大 200 のピア グループを作成できます。ピア グループ内のピアに関連する変更の場合：

- 新しいピアの場合、ピア グループはETCDですぐに保持されます。
- 既存のピアのタイムスタンプの変更の場合、ピア グループは 3 秒ごとに 1 回更新されます。次の更新：
  - 各ピア グループ内でタイムスタンプが変更された多くのピアの累積的なグループ更新が発生します。
  - etcd の頻繁な更新を削減します。

# ローミング ピア最適化

## 機能説明

SMF は、次の 2 つの方法でピア ノードをローミングとして識別します。

- **インターフェイスに基づくローミング ピア検出**：S8 インターフェイスを構成し、CSR、MBR、およびエコー要求を S8 経由で送信してローミング ピアとして識別します。

- **アプリケーションによるローミングピア検出**：サービスネットワークをローミングPLMNとして構成し、S5インターフェイス経由でメッセージが送信されるようにします。次に、タイプが「ローミング」としてリストに表示されている場合は、ピアをローミングとして識別します。

# 機能の仕組み

このセクションでは、SMFがローミングピアを検出して最適化する方法について説明します。

## インターフェイスに基づくローミング ピア検出

SMFは、エンドポイントGTPでのS8 VIPの構成をサポートしています。ピアからのセッション要求/変更ベアラー要求/エコー要求（CSR/MBR）がS8 VIPに到達すると、SMFはピアをROAMING SGWとしてマークし、ピアタイプも更新します。

## アプリケーションによるローミング ピア検出

SMFは、SMFプロファイルでのPLMNリストの構成をサポートします。SMFは、サービングとUE-PLMNを構成されたplmnsと比較して、セッションがホーマーかローマーかを判断します。

UE-PLMNが構成済みPLMNリストで見つかり、サービングPLMNが構成済みPLMNリストで見つからない場合、そのセッションはローマー（発信ローマー）としてマークされます。

新しいセッション作成のCSR、またはハンドオフ用のMBRを取得すると、SMFサービスはセッションがローマー セッションであることを検出します。

（注） SMFからパートナーSGWへの最初のダウンリンク制御メッセージは、セッション応答の作成または変更されたベアラー応答であると想定されています。

## ピア最適化

S8インターフェイスを介してピアからCSR/MBR/エコー要求を取得すると、SMFはピアをローミングSGWとしてマークし、S8インターフェイスに対して行われたパス管理関連の構成を使用します。

パートナーSGWのパス障害検出ロジックに違いはありません。S5インターフェイスを介したローミングセッションとしてセッションを検出すると、SMFはピアをローミングSGWとしてマークし、S8インターフェイスに対して行われたパス管理関連の構成を更新します。

SMFには、S8インターフェイスのエコーを無効にすることで、パス管理を無効にするオプションがあります。エコーを無効にするには、エコー間隔を0に構成します。この場合、ローミングSGWのSMFからエコーは開始されません。

SMF は、デフォルトでは、VIP インターフェイスに VRF アソシエーションがない場合、ローミング SGW のためのルートを追加します。VRF の関連付けが存在する場合、SMF はルートをインストールしません。

（注） ピア再起動の影響を最小限に抑えるために、ローマ セッションの cp-idle/up-idle タイムアウトを小さくすることが推奨されます。ピアパス障害またはピア再起動の（古いセッション）検出されないを最小限に抑えることができます。

## 制限事項

SMF でのローミング ピア最適化の既知の制限を次に示します。

- ローミング SGW に対してエコーが無効になっている場合、SMF は再起動カウンタに基づくピア パス管理を行いません。

# 機能設定

SMF は次の構成を使用してローミングピアを最適化します：

```
config
   instance instance-id gr_instance_id
   endpoint gtp
      interface { s2b | s5 | s5e | s8 | s11 }
      echo interval echo_interval
      echo retransmission-timeout retransmission_timeout_value
      echo max-retransmissions max_retry_count
      end
```

注：

- **interval** *echo_interval*：エコー間隔の範囲は <300 ～ 3600> 秒です。デフォルト値はデフォルト 300 秒です。エコー間隔を 0 秒に構成すると、アウトバウンドエコーが無効になります。この変更は、インターフェイスのタイプに関係なく適用されます。s2b、s5e、s5e、s11 などの他のインターフェイスの場合、エコー間隔の範囲は <60-3600> 秒です。
- **retransmission-timeout** *retransmission_timeout_value*：S8 インターフェイスの再送信タイムアウトの範囲は <60 ー 180> 秒です。デフォルト値は 60 秒です。s2b、s5e、s5e、s11 などの他のインターフェイスの場合、再送信のタイムアウトの範囲は <1 ー 20> 秒です。
- **max-retransmissions** *max_retry_count*：GTP エコー要求の最大再試行回数の値の範囲は 0 ～ 4 です。デフォルト値は 4 です。s2b、s5e、s5e、s11 などの他のインターフェイスの場合、最大再送信回数の範囲は <0 ー 10> です。

（注） これらのパラメータは、S8 インターフェイスにのみ適用されます。他のインターフェイスについては、既存の構成が適用されます。

## 設定例

S8 インターフェイスの構成例：

```
[unknown] smf# config
Entering configuration mode terminal
[smf] smf(config-instance-id-1)# endpoint gtp
[smf] smf(config-endpoint-gtp)# interface s8
[smf] smf(config-interface-s8)# vip-ip 192.0.2.1 vip-interface bd2.pgs5.3051
echo interval          300
   echo retransmission-timeout 60
   echo max-retransmissions 4
  exit
```

## 設定の確認

`show peers all` コマンドは、すべてのローミング SGW とそのノード情報を表示します。

```
[smf] smf# show peers all
GR INSTANCE ENDPOINT LOCAL ADDRESS PEER ADDRESS DIRECTION POD INSTANCE TYPE CONNECTED
TIME RPC ADDITIONAL DETAILS INTERFACE NAME VRF
```

---

```
1 N4 10.1.3.185:8805 10.1.3.234:8805 Inbound nodemgr-1 Udp 4 hours UPF Capacity:
65535,LoadMetric: 0,LoadSeqNo: 0,Mode: Online,OverloadMetric: 0,OverloadSeqNo: 0,Priority:
 65535  N4 NA
1 S5/S8 10.1.3.248:2123 10.1.3.245:2123 Inbound nodemgr-0 Udp 4 hours SGW
MaxRemoteRcChange: N/A,Recovery: 100 S8 NA
1 S5/S8 10.1.1.23:2123  10.1.3.245:2123 Inbound nodemgr-0 Udp 4 hours SGW
MaxRemoteRcChange: N/A,PeerType: Roaming,Recovery: 100 S5 NA
```

# ETCD トラフィックの最適化

拡張分散キー値（ETCD）は、分散システムで使用される構成データ、状態データ、およびその他のデータを格納するために使用される分散 key-value ストアです。

## 機能説明

拡張分散キー値（ETCD）のトポロジデータの現在の実装では、内部データと外部データの両方が特定のプレフィックスとともに保存され、アプリケーションはすべてのデータのコンテキストを作成し、ETCD データのすべての変更を処理します。この動作により、各ポッドから ETCD に大量のトラフィックが発生します。これには、これらの通知とレコードに関心のない一部のポッドが含まれます。

この問題に対処するために、この機能により、ポッドはこれらの通知とリロードをオプトイン/アウトできます。この「制限付き通知」および「リロード」機能はオプションです。この機能を使用すると、サブスクリプション サービスとピア データの通知のみを受信します。

（注） アップグレード中に既存の実稼働環境に影響を与えないよう、現在のキー構造を保持することが重要です。

ETCDのトラフィック最適化は、構成管理とサービス検出にetcdに依存する分散システムの信頼性、パフォーマンス、スケーラビリティ、およびセキュリティを向上させます。

# 機能の仕組み

ETCD には、次の 2 つの主要なデータ カテゴリが保存されます：

1. 内部トポロジデータ、ETCDのインスタンス情報、エンドポイント情報とリーダー情報が含まれます。
2. アプリケーションによって追加された外部ピアの情報。

これらのデータ カテゴリは両方とも ETCD に保存され、内部トポロジ データと外部ピア情報データの保存と通知に使用されます。トポロジデータと通知の現在の実装により、ETCDへのトラフィックが増加します。ポッドがこれらの通知とリロードをオプトインできるようにする、制限付きの通知とリロード機能を実装することで、トラフィックを削減できます。

現在のトポロジデータは、これらのエントリに関係のないポッドを含む、すべてのアプリケーション インフラ ベースのポッドにブロードキャストされます。これにより、ETCD からの不要な通知が発生しますが、これを回避できます。

さらに、すべてのデータが 10 秒ごとにリロードされます。つまり、ETCD とローカル キャッシュからのレコードが調整されます。不一致の場合は、通知が表示されます。このアプローチでは、ETCD とローカル キャッシュ間の一貫性が確保されますが、ETCD へのトラフィックが過剰になる可能性があります。

このプロセスを最適化するために、新しい実装では、通知とリロードに選択的なアプローチを適用し、すべてのポッドにブロードキャストするのではなく、特定のエントリまたは変更を必要とするポッドのみが通知されます。また、10秒ごとにすべてのデータをリロードする代わりに、サブスクライブされたデータのみをリロードすると効率的です。この選択的なアプローチにより、さまざまなポッドとETCD間のデータ量を削減し、システムの全体的なパフォーマンスを向上させることができます。その結果、ETCDとすべてのポッド間のトラフィックが減少します。

次のポッドは外部ピア データを受信しなくなるため、トラフィックが減少します：

- cache-pod
- rest-ep
- UDP プロキシ
- radius-ep
- li-ep
- dns-proxy
- gtpp-ep
- georeplication-pod
- oam-pod

# ETCD クライアントのフォールバック

## 機能説明

ETCD クライアントでは、次のコンポーネントが実装されています：

- ETCD クラスタへの gRPC 接続を確立するバランサ。
- ETCD サーバーに RPC を送信する API クライアント。
- 失敗した要求を再試行するか、エンドポイントを切り替えるかを決定するエラー ハンドラ。

5G のメモリ キャッシュを使用するアプリインフラベースのポッドは、ETCD サーバーと通信します。この通信は、ETCD クライアント ロードバランサを介して分散システムに重要なデータを保存するためのものです。メモリ キャッシュは、clientv3-grpc1.7 ライブラリを実装する ETCD クライアント 3.3 バージョンを使用します。

## ETCD クライアント ロード バランサ

SMF は、clientv3-grpc1.14 ライブラリを実装する ETCD クライアント バージョン 3.4.21 をサポートしています。このライブラリには下位互換性があります。

clientv3-grpc1.14 ライブラリには、次の重要なポイントがあります。

- 異常なエンドポイントのリストを維持するのではなく、バランサーのフェールオーバー ロジックを簡素化します。
- 複数のエンドポイントが使用可能な場合は、複数のサブ接続を作成します。これは、エンドポイントごとに 1 つのサブ接続を意味します。たとえば、5 ノードクラスタでは、clientv3-grpc1.14 バランサーには 5 つの TCP 接続が必要です。
- TCP 接続のプールを保持することで、より優れたフェールオーバー パフォーマンスと柔軟なロードバランサを提供します。
- デフォルトのラウンドロビン負荷分散ポリシーを拡張し、パワーオブツーやピックリーダーなどの他の種類の負荷分散方式をサポートするようにします。
- gRPC リゾルバ グループを使用し、バランサー ピッカー ポリシーを実装して、複雑なバランシング作業をアップストリーム gRPC に委任します。
- gRPC 内部エラーを自動的に処理し、バックオフなどの高度な再試行ポリシーを有効にする gRPC インターセプタ チェーンに再試行を導入します。

# ETCD のクライアントの再試行メカニズム

PUT 要求のエラーを受信すると、ETCD クライアントはこの要求を 3 回再試行します。ETCD クライアントは、各再試行を 1 秒のタイムアウト後に実行します。ETCD クライアントは、3 回の再試行すべてを 3 秒以内に完了し、アプリケーションの既存の SLA を満たします。3 回の再試行の後、ETCD クライアントは結果をアプリケーションに返します。

# フラグ DB データベースの更新

## 機能説明

SMF は、サブスクライバの状態がアイドルからアクティブに変わり、URI、UeTz、またはサービング ネットワークが変更される時に、CDL を更新します。

CDL に向けられたトランザクション要求が増加すると、SMF による CPU 使用率が高くなります。不要な CPU 使用率を防ぐために、 SMF は 変更された属性で CDL のサブセットのみを更新します。

フラグ DB データベースは、次の SMF プロシージャのために更新されます：

- ULI 変更のみの MBR：SMF は、応答を送信するステートレスな方法で、URI 変更のみの MBR を処理します。応答の送信後、smf サービスは CDL を更新します。これは、CPU 使用率に影響します。CPU 使用率を最適化するために、ULI については、部分的な更新でのみ SMF が CDL に通知します。
- 4G RAT ハンドオーバー：S-GW 間ハンドオーバー中に、smf サービスは ULI の変更と TEID の変更を含む MBR を受信します。CPU 使用率を最適化するために、SMF は、すべてのベアラーの引き継ぎが成功した場合、部分的なアップデートのみを使用してピア TEID と ULI について CDL に通知します。
- N2 ハンドオーバー：N2 ハンドオーバー手順が終了すると、smf-service は CPU 使用率に影響を与える CDL を更新します。CPU 使用率を最適化するために、SMF は既存のすべての QFI の引き継ぎが成功した場合、部分的なアップデートで ULI と TEID のみについて CDL に通知します。

# RRC 非アクティブ原因コードに基づく PDU セッション変更の処理

## 機能説明

無線リソース制御（RRC）は、5G NR プロトコル スタック内のレイヤです。コントロール プレーン、UE、gNB にのみ存在します。PDU セッションの既存の状態により、RRC の動作と機能が制御されます。

PCF によって開始された変更中に、AMF は、次の条件で、SmContextUpdate メッセージの N2 コンテンツに含まれる受信した失敗した転送無線ネットワーク原因コードを SMF に送信します。

- XN ハンドオーバーが進行中の場合。
- AN が解放された場合。
- UE が RRC 非アクティブ状態の場合。
- UE が到達不能な場合。

N2 原因コードを含む SmContextUpdate メッセージは、AMF から SMF、または SMF から AMF へのブリッジとコンバータとして機能します。

## 機能の仕組み

ここでは、この機能の仕組みを説明します。

PCF によって開始された変更中に、Xn ハンドオーバーが進行中の場合、次のシナリオが通知されます。

- AN が解放されるか、UE が RRC 非アクティブ状態になっていて到達不能になっています。
- AMF は、 **SmContextUpdate** メッセージの N2 コンテンツで、受信した転送に失敗した無線ネットワークの原因コードを SMF にリレーします。
- これらの原因コードは、標準の無線ネットワークの原因である可能性もありますが、gNB から送信されたカスタマイズされた無線ネットワーク原因コードの可能性もあります。

以前は、これらの原因コードは SMF によって拒否され、PCF は同じ PCF の変更を複数回試行していました。SMF はすぐに拒否されず、PCF からの複数の再試行を回避するために、新しい N2 トリガー構成に基づいて、さまざまな原因コードに対して異なる動作をするようになりました。

受信した N2 原因コードに基づいて、PDU 変更手順の SMF では次のシナリオがサポートされます：

- 原因コードが Xn ハンドオーバーが進行中であることを示しているか、AN が解放された場合、次のアクティビティが発生します。
  - SMF は進行中の PDU セッションの変更を一時停止します。
  - Xn ハンドオーバーまたは AN リリース後に再開されます。
- 原因コードが、UE が RRC 非アクティブで到達不能であることを示している場合、次のアクティビティが発生します。
  - SMF が PDU セッションの変更を拒否します。
  - ルール違反を PCF に報告する。

デフォルトでは、この機能は、デフォルトのガードタイムアウトと最大再試行がゼロのいくつかの標準 RRC 非アクティブ原因コードに対してアクティブになります。

次の原因コードの場合、SMF はセッション変更を一時停止し、Xn-handover アクティビティが終了した後にのみセッション変更を再開します。

- **_RadioNetwork_NG_intra_system_handover_triggers**
- **_RadioNetwork_NG_inter_system_handover_triggers**

次の原因コードの場合、SMF はセッション変更を拒否します。

- **_RadioNetwork_UE_in_RRC_INACTIVE_state_not_reachable**

標準の原因コードとともに、新しい N2 トリガー CLI が導入され、さまざまなカスタマイズされた無線ネットワーク原因コードと対応する SMF アクションを構成できるようになりました。

（注） 非ローミング PCF によって開始された変更シナリオは、この機能の一部としてサポートされています。

## コール フロー

ここでは、この機能の主要なコール フローについて説明します。

### PCF によって開始された gNB 転送状態の変更

このセクションでは、PCF によって開始された変更コール フロー手順における gNB 転送状態のアクティビティについて説明します。

次の図は、PCF によって開始される gNB 転送状態のコール フローの変更を示しています。

図 *208 : PCF* によって開始された *gNB* 転送状態の変更でのコール フロー

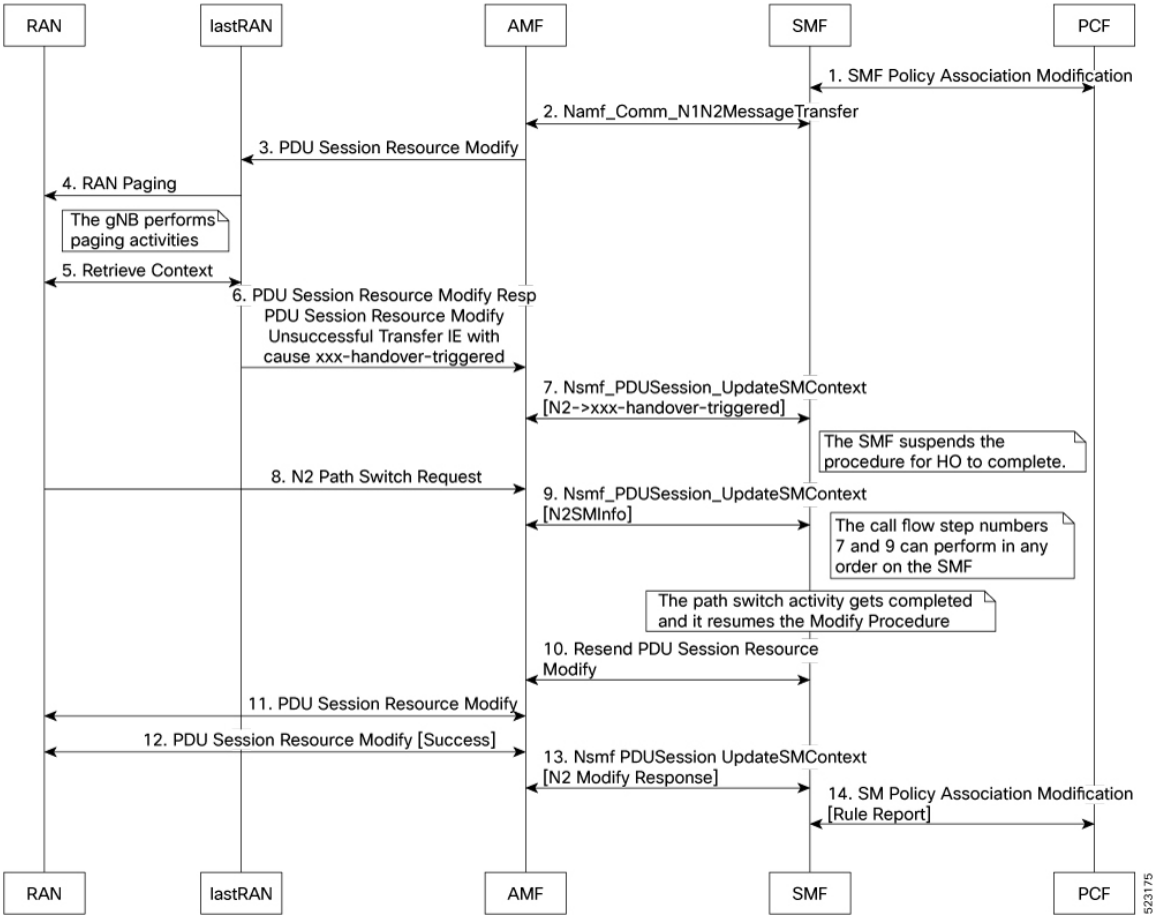



表 *379 : PCF* によって開始された *gNB* 転送状態の変更でのコール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | PCF は、SMF に SMF ポリシー関連付け変更要求を送信します。<br>これは、SMFからも同じメッセージを受信するため、相互に交換可能なアクションです。 |
| 2 | SMF が AMF に Name Comm N1N2MessageTransfer 要求を送信します。<br>これは、AMFからも同じメッセージを受信するため、交換可能なアクションです。 |
| 3 | AMF は、lastRAN に PDU セッション リソース変更要求を送信します。 |
| 4 | lastRAN は、RAN にページング アクティビティを要求します。 |

| ステップ | 説明 |
|---|---|
| 5 | gNB はページング アクティビティを実行し、RAN と lastRAN 間のコンテキストを取得します。<br>lastRAN は、Retrieve Context メッセージを RAN に送信します。<br>これは、RAN から同じメッセージも受信するため、相互に交換可能なアクションです。 |
| 6 | lastRAN は、AMF に PDU セッション リソース変更応答を送信します。<br>また、PDU セッション リソース変更の失敗の転送 IE（cause xxx-handover-triggered メッセージ）も含まれます。 |
| 7 | AMF は Nsmf PDUSession UpdateSMContext メッセージ（N2 から xxx-handover-triggered）を処理して SMF に送信します。<br>これは、SMF からも同じメッセージを受信するため、相互に交換可能なアクションです。<br>（注）<br>このステップの間、SMF はそれ以降の手順を一時停止し、HO を開始して完了します。 |
| 8 | RAN は、N2 パス切り替え要求を AMF に送信します。 |
| 9 | AMF は、Nsmf PDUSession UpdateSMContext（N2SMInfo）応答メッセージを SMF に送信します。<br>（注）<br>ステップ番号 7 と 9 は、SMF に向けて、または AMF から任意の順序で進めることができます。 |
| 10 | SMF が AMF に PDU セッション リソース変更メッセージを再送信します。<br>これは、AMF からも同じメッセージを受信するため、交換可能なアクションです。<br>（注）<br>このステップ中にパスの切り替えが完了し、変更手順が再開されます。 |
| 11 | AMF は、PDU セッション リソース変更メッセージを RAN に送信します。<br>これは、RAN から同じメッセージも受信するため、相互に交換可能なアクションです。 |
| 12 | RAN は、成功通知の PDU セッション リソース変更（成功）メッセージを AMF に送信します。<br>これは、AMF からも同じメッセージを受信するため、交換可能なアクションです。 |

| ステップ | 説明 |
|---|---|
| 13 | AMF は、変更された応答 Nsmf PDUSession UpdateSMContext（N2 変更応答）メッセージを SMF に送信します。<br>これは、AMF からも同じメッセージを受信するため、交換可能なアクションです。 |
| 14 | SMF は PCF に、レポートの SM ポリシー関連付け変更（ルール レポート）メッセージを送信します。<br>これは、PCF からも同じメッセージを受信するため、相互に交換可能なアクションです。 |

## PCF によって開始された UE 到達不能状態に関する変更

このセクションでは、PCF によって開始された変更コール フロー手順での UE 到達不能状態のアクティビティについて説明します。

次の図は、PCF によって開始された UE 到達不能状態の変更を示しています。

**図 *209 : PCF* によって開始された *UE* の到達不能状態に対する変更のコール フロー**

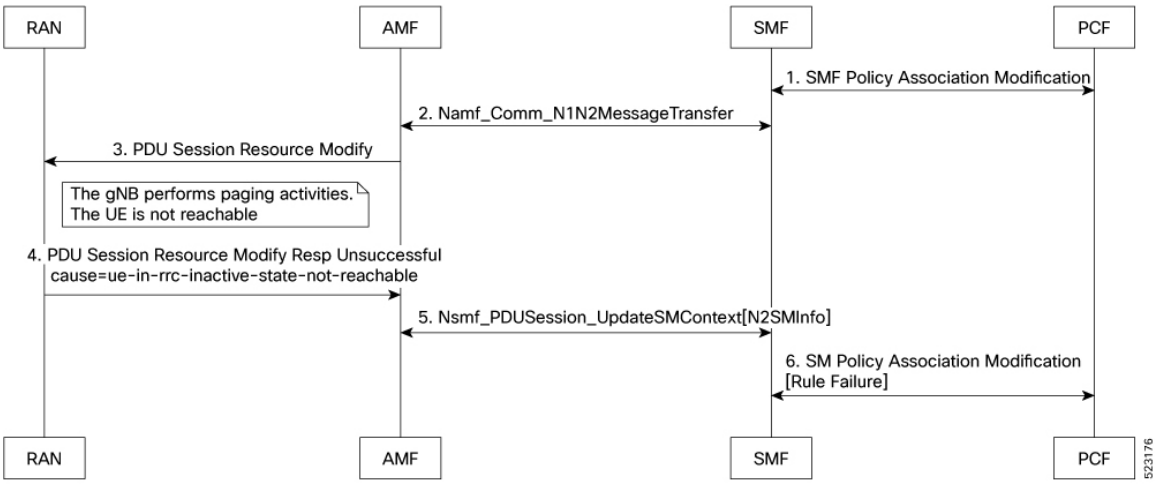



**表 *380 : PCF* によって開始された *UE* 到達不能状態に対する変更のコール フローの説明**

| ステップ | 説明 |
|---|---|
| 1 | PCF は、SMF に SMF ポリシー関連付け変更要求を送信します。<br>これは、SMF からも同じメッセージを受信するため、相互に交換可能なアクションです。 |

| ステップ | 説明 |
|---|---|
| 2 | SMF が AMF に Name Comm N1N2MessageTransfer 要求を送信します。<br>これは、AMFからも同じメッセージを受信するため、交換可能なアクションです。 |
| 3 | AMF は、RAN に PDU セッション リソース変更要求を送信します。<br>（注）<br>このステップ中に、UE が到達不能であるため、gNB はページングアクティビティを実行します。 |
| 4 | RAN は、PDU セッション リソース変更応答失敗メッセージを AMF に送信します。<br>また、障害原因である ue-in-rrc-inactive-state-not-reachable メッセージも含まれます。 |
| 5 | AMF は、Nsmf PDUSession UpdateSMContext（N2SMInfo）応答メッセージを SMF に送信します。<br>これは、SMFからも同じメッセージを受信するため、相互に交換可能なアクションです。 |
| 6 | SMFは、失敗したレポートのSMポリシーの関連付けの変更（ルール失敗レポート）メッセージを PCF に送信します。<br>これは、PCFからも同じメッセージを受信するため、相互に交換可能なアクションです。 |

## PCFによって開始された非アクティブからアイドルへの状態に関する変更

このセクションでは、PCF によって開始された変更コール フロー手順での非アクティブからアイドルへの状態のアクティビティについて説明します。

次の図は、PCF によって開始される非アクティブからアイドルへの状態のコール フローの変更を示しています。

図 *210 : PCF* によって開始された非アクティブからアイドルへの状態に対する変更のコール フロー

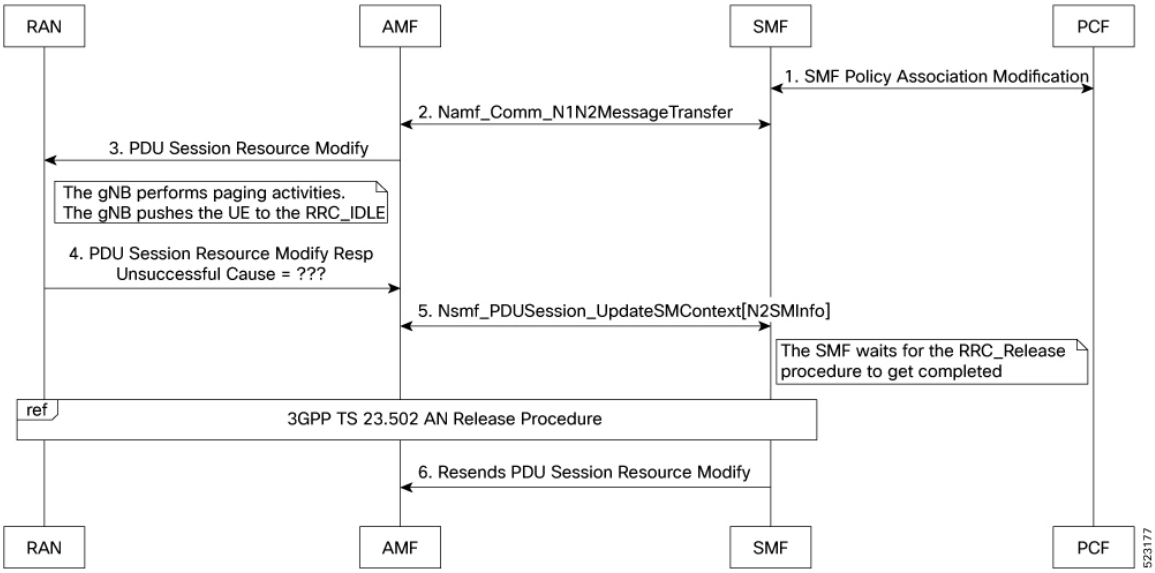



表 *381 : PCF* によって開始された非アクティブからアイドルへの状態に対する変更のコール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | PCF は、SMF に SMF ポリシー関連付け変更要求を送信します。<br>これは、SMFからも同じメッセージを受信するため、相互に交換可能なアクションです。 |
| 2 | SMF が AMF に Name Comm N1N2MessageTransfer 要求を送信します。<br>これは、AMFからも同じメッセージを受信するため、交換可能なアクションです。 |
| 3 | AMF は、RAN に PDU セッション リソース変更要求を送信します。<br>（注）<br>このステップ中に、gNB は、gNBは、UE を RRC_IDLE モードへプッシュする時にページング アクティビティを実行します。 |
| 4 | RAN は、PDU セッション リソース変更応答失敗メッセージを AMF に送信します。<br>また、障害原因不明のメッセージも含まれます。 |

| ステップ | 説明 |
|---|---|
| 5 | AMF は、Nsmf PDUSession UpdateSMContext（N2SMInfo）応答メッセージを SMF に送信します。<br>これは、SMF からも同じメッセージを受信するため、相互に交換可能なアクションです。<br>（注）<br>このステップの間、SMF は RRC_Release 手順が完了するのを待ちます。 |
| 6 | SMF が AMF に PDU セッション リソース変更メッセージを再送信します。<br>（注）<br>この手順は、3GPP TS 23.502 AN リリース手順に従います。 |

# 機能設定

この機能を構成するには、次の構成例を使用します。

```
config
profile access access_profile_name
   n2 trigger { ho-in-progress | temp-not-reachable } { guard-timeout
timeout | max-retry retry_count | value retry_count_range }
   n2 trigger ue-not-reachable value notreachable_count_range
   end
```

注：

- **profile access** *access_profile_name*：アクセス プロファイルの名前を選択します。
- **n2 trigger**：N2 トリガ タイプを指定します。[トリガ（Trigger）] はトラフィック タイプです。以下のいずれかである必要があります。
  - **ho-in-progress**：原因コードのハンドオーバー進行中トリガ構成リストを指定します。
  - **temp-not-reachable**：原因コードの一時的な到達不能トリガ構成リストを指定します。
  - **ue-not-reachable**：原因コードの UE 到達不能トリガ構成リストを指定します。
- **guard-timeout** *timeout*：Handover in progress ガードのタイムアウトを 500 ～ 30000 ミリ秒の範囲で指定します（ミリ秒単位）。デフォルト値は、10000 ミリ秒です。
- **max-retry** *retry_count*：進行中のハンドオーバーまたは一時的に到達不能なオプションの最大再試行回数を 0 ～ 64 の範囲で指定します。デフォルト値は 0 です。
- **value** { *notreachable_count_range* } | { *retry_count_range* }：最大再試行範囲の UE カウントの範囲の数値。

（注） 定義された構成は、受信した失敗した転送（無線ネットワーク標準およびカスタマイズ状態）を照合するために使用され、コードが RRC 非アクティブアクションを決定するようになります。シナリオは次のとおりです。

- **ue-not-reachable**、 **ho-in-progress**、および **temp-not-reachable** の場合、PCF によって開始された変更は拒否されます。ANリリースにおける xn ハンドオーバー処理の後、一時停止され、その後再開されます。
- RRC 非アクティブ アクションが **ho-in-progress** または **temp-not-reachable** トリガ プロファイルのいずれかにある場合、ガード タイマーが開始されます。進行中の PCF によって開始された変更が一時停止するのを待ちます。指定された時間内に AN リリースの xn ハンドオーバー アクティビティを再開します。このアクションが失敗すると、PCF によって開始された変更は拒否されます。その結果、このアクションはルール失敗メモとして PCF に報告されました。
- 最大再試行回数により、最初の試行が失敗した後、最大連続再試行回数を再試行できます。これは、試行ごとに同じトリガ カテゴリの原因コードを繰り返し受信した結果です。このアクションが失敗すると、PCF によって開始された変更は拒否されます。その結果、このアクションは、最大再試行回数に達した後、PCF にルール失敗メモとして報告されました。
- この機能は、デフォルトのガードタイムアウトと最大再試行がゼロの標準RRC非アクティブ原因コードに対してアクティブになります。

## 設定例

次に、設定例を示します。

```
config
smf(config)# profile access access1
 smf(config-access-access1)# n2 trigger [ ho-in-progress | temp-not-reachable ] [ value
 1 ] [ guard-timeout 10000 ] [ max-retry 10 ]
 smf(config-access-access1)# n2 trigger ue-not-reachable value [10]
 exit
exit
```

## 設定の確認

設定を確認するには、次のコマンドを実行します。

```
[smf] smf# show running-config profile access access1 n2
profile access access1
  n2 trigger ho-in-progress value [ 50 51 52 53 ] guard-timeout 12000 max-retry 3
  n2 trigger temp-not-reachable value [ 54 55 56 57 ] guard-timeout 11000 max-retry 2
  n2 trigger ue-not-reachable value [ 58 59 60 61 ]
exit
```

# K8 活性プローブを使用したポッド障害検出

Kubernetes は、活性プローブを使用して、すべてのポッドの正常性を定期的に監視します。このメカニズムにより、ポッドの障害を簡単に検出できます。活性プローブの K8 構成パラメータ値が調整され、ポッド障害をより迅速に検出し、障害のあるポッドを適切なタイミングで再起動できるようになりました。

構成の変更は、次のポッドに適用されます：

- bgpspeaker-pod
- cache-pod
- diameter-ep
- dns-proxy
- edr-monitor
- georeplication-pod
- gtpc-ep
- gtpc-ep-s11
- gtpp-ep
- li-ep
- nodemgr
- oam-pod (infra-oam)
- protocol
- radius-ep
- rest-ep
- sgw-service
- smf-service
- UDP プロキシ

K8 によるポッド障害の早期検出により、バックアップ ポッドまたはスタンバイ ポッドがメッセージ処理を引き継ぎ、シームレスな通信を実現します。

# 復元力の処理

## 機能説明

復元力処理機能により、CLI 制御のフレームワークが導入され、システム障害を確認した場合、またはクラッシュが報告された場合に、サービス ポッドのリカバリがサポートされるため、次のいずれかのサービス ポッドのリカバリに役立ちます。

- sgw-service ポッド
- smf-service ポッド
- gtpc-ep ポッド
- protocol ポッド
- diameter-ep ポッド

これらのサービス ポッドは、複数のセッションメッセージを処理するロジックを含むソフトウェア モジュールです。サービス ポッドは、次のいずれかのシナリオ、または複数のシナリオの組み合わせが原因で障害が発生しやすくなります。

- 複雑なコール フローおよびコリジョン処理
- セッション状態に整合性がありません
- セッション状態に対する着信メッセージの不適切な処理
- 受信メッセージ内の予期しないコンテンツや未処理のコンテンツ

システム障害やクラッシュを確認するたびに、障害の動作によってサービス ポッドが強制的に再起動され、他のセッションの進行中のトランザクション処理に影響を及ぼします。ポッドの再起動後でもクラッシュは再発します。

このリスクを軽減するには、アクションが定義されている CLI ベースのフレームワークを使用し、サブスクライバ セッションをクリーンアップするか、現在の処理を終了します。

## 機能の仕組み

このセクションでは、障害リカバリ フレームワークを使用してクラッシュに対するアクションを定義する方法について説明します。フレームワークでは、次のアクションのいずれかを定義できます。

- 終了：障害が発生すると、このアクションは障害が発生したトランザクションを終了し、サブスクライバ セッション キャッシュをクリアします。これは、 smf-service ポッドおよび sgw-service ポッドに適用されます。

（注） ポッドは再起動されません。このアクション中にデータベースはクリアされません。

- クリーンアップ：障害が発生した場合、このアクションでは障害が発生しているサブスクライバ セッションをクリアし、コールを解放します。これは、 smf-service ポッドおよび sgw-service ポッドに適用されます。
- グレースフル リロード：障害が発生すると、このアクションはポッドを再起動します。これは、 gtpc-ep、 protocol、および diameter-ep ポッドに適用されます。障害信号を処理して、キープアライブ ポートなどのリソースをクリーンアップし、早期に閉じます。また、checkport スクリプトはポッドの状態を検出し、対応するポッドの VIP スイッチ処理を開始できます。
- リロード：ポッドがクラッシュすると、リロード アクティビティが開始されます。これは、すべてのポッドに適用されるデフォルトの設定または値です。

# 機能設定

この機能を構成し、システムの障害回復を有効にするには、次の構成例を使用します。

```
config
   system-diagnostics { diameter |  gtp | pfcp | service | sgw-service
 }
       fault
          action { abort | cleanup { file-detail | interval | num |
skip { ims | emergency | wps } } | graceful-Reload | reload }
          end
```

注：

- **system-diagnostics { diameter | gtp | pfcp | service | sgw-service }**：システム診断に必要なサービス ポッドのタイプを指定します。使用可能なポッド オプションは、diameter、gtp、pfcp、smf-service、および sgw-service です。
- **fault**：セッションの処理中に障害回復を有効にします。
- **action { abort | cleanup | graceful-Reload | reload }**：障害発生時に実行するアクションを次から 1 つ指定します。デフォルト アクションはリロードです。
  - **abort**：障害のあるトランザクションを削除し、そのセッション キャッシュをクリアします。データベースはクリアされません。

（注） これは、smf-service ポッドに対する排他的オプションです。

- **cleanup { file-detail | interval | num | skip }**：クリーンアップ アクティビティを有効にします。障害を軽減するためのアクションとして次の選択肢があります。

- **file-detail**：ファイル名に行番号を付けて一覧表示します。リカバリからファイル名の詳細を除外します。
- **interval**：間隔を分単位で指定します。この期間に、障害の最大数を許可する許容間隔を指定します。1 ～ 3600 の範囲の整数で指定する必要があります。
- **num**：1 つの間隔内で許容可能な障害の最大数を指定します。0 ～ 50 の範囲の整数で指定する必要があります。
- **skip { ims | emergency | wps }**：アクティブ音声コール、WPS、または緊急コールに対するサブスクライバ セッションのクリーンアップのスキップを有効にします。
  - アクティブ音声コールを検出するには、次のコマンドを使用します。

    **profile dnn** *dnn_name* **ims mark qci** *qos_class_id*

  - クリーンアップのスキップ構成を有効にすると、SMF は問題のあるトランザクションを削除し、そのセッション キャッシュをクリアします。
  - セッションのセットアップ中またはリリース状態の間に障害が発生すると、SMF は次の処理を実行します。

    ：セッション終了時にトランザクションを削除します。

    ：これらの状態の間、構成済みの障害アクションをオーバーライドします。

    ：障害のあるトランザクションのセッションキャッシュおよびデータベース エントリをクリアします。
  - これにより、ダイナミックな構成変更が可能になります。

（注） これは、smf-service および sgw-service ポッドの排他的オプションです。

- **graceful-Reload**：ポッドの正常なリロードのためのオプションを指定します。サービス ポッドは、障害信号を処理してキープアライブ ポートなどのリソースをクリーンアップし、クラッシュ処理（ポッド再起動処理）を続行します。

（注） これは、diameter-ep、gtpc-ep、および protocol サービス ポッドに対する排他的なオプションです。

- **reload**：障害動作が原因でポッドがクラッシュした場合に、ポッドをリロードします。これは、すべてのサービス ポッドに適用できるオプションです。これはデフォルトのオプションでもあります。

## 設定例

次の構成例では、障害発生アクションをサブスクライバのクリーンアップとして、10分間隔以内で smf-service または sgw-service ポッドの 3 回のクラッシュが許可されます。

```
config
    system-diagnostics { service | sgw-service }
        fault
            num 3 interval 10
            action cleanup
            end
```

次の構成例では、diameter または gtpc-ep ポッド、あるいは protocol ポッドのグレースフル障害処理で、障害信号の受信時にキープアライブポートを閉じることができます。

```
config
    system-diagnostics { diameter | gtp | pfcp }
        fault
            action graceful-Reload
            end
```

## 設定の確認

設定を確認するには、次のコマンドを実行します。

```
smf# show running-config system-diagnostics service
 fault num 3
 fault interval 10
 fault action cleanup
exit

show running-config system-diagnostics sgw-service
 fault num 3
 fault interval 10
 fault action cleanup
exit

show running-config system-diagnostics gtp
 fault action graceful-Reload
exit

show running-config system-diagnostics pfcp
 fault action graceful-Reload
exit

show running-config system-diagnostics diameter
 fault action graceful-Reload
exit
```

# OAM サポート

ここでは、この機能の操作、管理、およびメンテナンス サポートについて説明します。

## バルク統計サポート

復元力処理機能では、次のバルク統計情報がサポートされています。

**recover_request_total**：この統計情報には、次の新しいラベルが含まれています。

- **action**：障害アクションを定義します。
- **reason**：障害の理由を定義します。
- **status**：障害ステータスを定義します。

次に、復元力処理機能のバルク統計情報の例を示します。

```
recover_request_total{action="panic_recovery_cleanup",
app_name="SMF",cluster="Local",data_center="DC",instance_id="0", reason="creating
 panic",service_name="sgw-service",status="success"} 1
```

SMF のバルク統計情報のサポートの詳細については、「*UCC 5G SMF* メトリック リファレンス」を参照してください。

cnSGW-C のバルク統計情報のサポートの詳細については、「*UCC 5G cnSGW-C* メトリック リファレンス」を参照してください。

## Monitoring Support

システム障害をモニタし、複数のポッドに適用する障害復旧アクションを決定するには、次のトランザクション エラーを含むエラー ログを使用します：

- クリーンアップ アクションの Txn エラー タイプ 10003（`ErrorPanicRecovery`）
- クリーンアップをスキップしてアクションを中止するための、Txn エラー タイプが 1802（`ErrorAffinityAddEntryFailed`）。

（注） 復元力処理機能のモニタリングのサポートは、SMF でのみ適用されます。

# IoT 展開でのサブスクライバ セッションのスケーリング

表 *382 :* 表 *1* 機能の履歴

| 機能名 | リリース | 説明 |
|---|---|---|
| UCS 220 M7 プラットフォームで 700 万のセッションをサポート | 2024.04.0 | この機能には、UCS 220 M7 プラットフォームで最大 700 万の IoT コールセッションをサポートするために SMF インフラストラクチャを最適化することが含まれます。最適化には、radius-ep および GTPC-ep コンポーネントと、CDL コンポーネントとの通信の改善が含まれています。<br>この最適化により、システムの信頼性と拡張性が向上し、大規模な IoT 展開の効率的な処理が保証されます。<br>CLI コンソールの変更：<br>2024.04.0 より前のリリースでは、**detect-dead-server consecutive-failures** のヘルプ文字列には、デフォルト値として 10 が表示されていました。<br>リリース 2024.04.0 以降では、 **detect-dead-server consecutive-failures** のヘルプ文字列が更新され、デフォルト値が無効になっていることを反映しています。<br>導入されたコマンド：<br>• **enable-async { false \| true }** RADIUS エンドポイント設定モードで を設定して、RADIUS 認証、アカウンティング、および CoA 要求メッセージのために RADIUS エンドポイントからの非同期通信を有効にします。デフォルト値は **false** です。<br>• **overload-control msg-type create-session-request** Create Session Request メッセージのレート制限を適用するには、S5 インターフェイス設定モードで を入力します。 |

この最適化機能の目的は、IoT コール制御用の UCS M6 サーバーで適切に実装されたのと同じ展開戦略を使用して、Cisco UCS M7 C220 サーバー上の 700 万のユーザー デバイスをサポートすることです。これには、負荷の増加に対応するようにインフラストラクチャを最適化し、一般的な IoT 環境で多数の接続とデータ ストリームを効率的に管理することが含まれます。

これを実現するには、次のパフォーマンスの最適化と拡張を実装する必要があります。

- RADIUS エンドポイント（radius-ep）：RADIUS 認証、アカウンティング、および CoA 要求メッセージに非同期通信を使用します。
- GTPC エンドポイント（GTPC-ep）：セッション要求作成メッセージのレート制限を適用します。受信された Create Session Request メッセージの数が設定されているレートを超えた場合、要求はドロップされるか、または「No resources available (73)」という応答で拒否されます。

また、この機能により、発信タイム スタンプと最大待機時間の AVP が、Gx CCR-I メッセージで PCRF サーバに送信されます。これらの AVP の組み合わせが、セッション作成要求メッセージを受信した現在のタイムスタンプより小さい場合は常に、これらの AVP 値が Gx CCR-I メッセージで PCRF サーバに送信されます。

# SMF インフラストラクチャの最適化の利点

- 高い拡張性：最大 700 万の IoT 通話セッションをサポートし、大規模な IoT の導入に適しています。
- パフォーマンスの最適化：RADIUS エンドポイントの非同期通信を有効にすると、システムは即時の応答を待つことなく複数の要求を同時に処理できるため、スループットが向上し、遅延が減少します。
- 信頼性の向上：GTPC エンドポイントにレート制限を適用することで、大量のセッション要求の作成メッセージによってシステムが過負荷になるのを防ぎ、システムの安定性と信頼性を維持します。
- データの整合性と精度：発信タイムスタンプと最大待機時間の AVP を PCRF サーバに送信することで、課金、分析、コンプライアンスに重要な正確なセッションデータを維持できます。

# RADIUS および GTPC エンドポイントのパフォーマンス最適化の構成

このセクションでは、M7 プラットフォームで 700 万の IoT コール セッションを有効にするためのこれらの構成手順について説明します。

**手順**

**ステップ 1** RADIUS エンドポイントの非同期通信の有効化 （1228 ページ）
**ステップ 2** セッション要求の作成に対するレート制限の有効化 （1228 ページ）

# RADIUS エンドポイントの非同期通信の有効化

RADIUSエンドポイントに対して非同期通信が有効になっている場合、SMFは即時応答を待たずに、認証、アカウンティング、およびCoA要求を送信します。これにより、大量の要求を同時に処理するシステムの能力が向上します。

RADIUS エンドポイントで非同期通信を有効にするには、次の手順に従う必要があります。

**手順**

**ステップ1** インスタンス ID を指定します。

**instance instance-id** *instance_id*

**例：**

```
[smf] smf# config
[smf] smf(config)# instance instance-id 1
```

**ステップ2** RADIUS エンドポイントを構成します。

**endpoint radius**

**ステップ3** 非同期通信を有効にして、UDP プロキシに RADIUS 認証およびアカウンティング メッセージを送信し、CoA メッセージを SMF サービスに送信します。デフォルト値は **false** です。

**enable-async true**

**（注）**
この構成を変更するには、radius-ep ポッドを再起動する必要があります。

# セッション要求の作成に対するレート制限の有効化

トラフィックの多いモバイルネットワークで、GTPCエンドポイントは、特にピーク時や人が密集するエリアに、多数のセッション要求の作成メッセージを受信する可能性があります。

レート制限構成を使用すると、GTPC エンドポイントへの着信セッション要求の作成メッセージのフローを制御できるため、GTPC エンドポイントで大量のトラフィックを効果的に処理できます。

**重要** レート制限構成が有効になっている場合、緊急コールと WPS セッションにも適用され、これらのコールのセッション要求の作成メッセージが拒否またはドロップされる可能性があります。

GTPC エンドポイントでセッション作成要求メッセージのレート制限を有効にするには、以下の手順に従う必要があります。

手順

**ステップ 1** インスタンス ID を指定します。

**instance instance-id** *instance_id*

例：

```
[smf] smf# config
[smf] smf(config)# instance instance-id 1
```

**ステップ 2** GTP エンドポイントを構成します。

**endpoint gtp**

**ステップ 3** インターフェイスを指定します。

**interface s5**

**ステップ 4** セッション要求の作成メッセージの過負荷制御を有効化します。

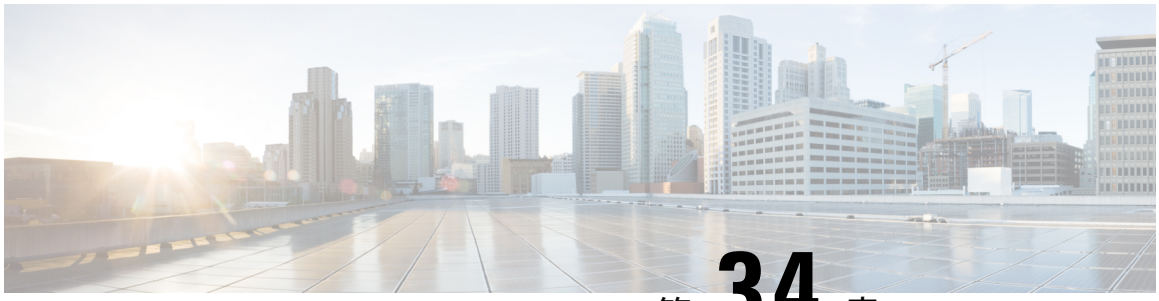
**overload-control msg-type create-session-request**

**ステップ 5** 必要に応じて、レート制限およびその他のパラメータを設定します。

**rate-limit** *rate_limit* **queue-size** *queue_size* **reject-threshold** *reject_threshold* **pending-request** *pending_requests* **reject-action { drop-req | reject-req }**

例：

```
[smf] smf(config-interface-s5)# rate-limit 3000 queue-size 8000 reject-threshold 100
pending-request 5000 reject-action drop-req
```



第 34 章

# ポッドとサービスの参考資料


- 機能の概要と変更履歴 （1231 ページ）
- 機能説明 （1232 ページ）
- ノードへのポッドの割り当て （1244 ページ）
- ポッドの詳細とステータスの表示 （1244 ページ）
- UDP プロキシバイパスを使用した PFCP プロトコルエンドポイントマージ （1246 ページ）
- プロトコル マイクロサービスに統合された UDP プロキシ機能 （1247 ページ）


## 機能の概要と変更履歴

### 要約データ

**表 *383* : 要約データ**

| | |
|---|---|
| 該当製品または機能エリア | SMF |
| 該当プラットフォーム | SMI |
| 機能のデフォルト設定 | 有効：常時オン |
| このリリースでの関連する変更点 | N/A |
| 関連資料 | 該当なし |

# 更新履歴

表 *384 :* マニュアルの変更履歴

| 改訂の詳細 | リリース |
|---|---|
| node-monitor ポッドは、すべての K8 ポッドのモニタリングを有効にするためにサポートされています。 | 2021.02.0 |
| grafana-dashboard-app-infra ポッドが削除されました。 | 2021.02.3.t3 |
| 最初の導入。 | 2020.02.0 より前 |

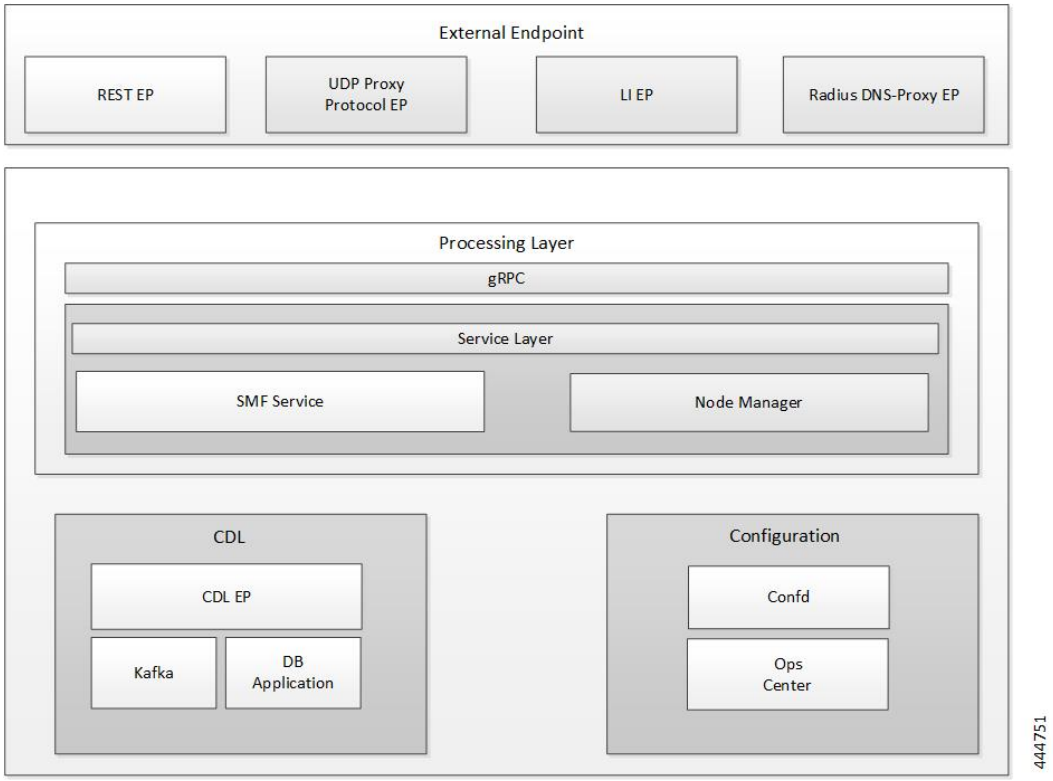
# 機能説明

Kubernetes クラスタ戦略に SMF は、構築されています。これは、コンテナ化、高可用性、拡張性、モジュラ性、および展開の容易さというネイティブの概念を採用していることを示します。Kubernetes に提供された利点を達成するために SMF は、ポッドやサービスなどのコンポーネントを含む構造を使用します。

展開環境に応じて、SMF は、仮想マシンにポッドを展開します。ポッドは、ポッド内通信を担当するサービスによって動作します。ポッドをホストするマシンに障害が発生した場合、またはネットワークの中断が発生した場合、ポッドは終了または削除されます。ただし、この状況は一時的なものであり、Kubernetes は新しいポッドを回転して無効なポッドを置き換えます。

次のワークフローは、ホストマシン、および関連するポッドとサービスへの高度な可視性を提供します。また、ポッドが相互に通信する方法も表します。展開インフラストラクチャに基づいて、表示が異なる場合があります。

図 *211* : ポッドの通信ワークフロー




Kubernetes の展開には、クラスタ内の Kubernetes リソースを管理するための kubectl コマンドラインツールが含まれています。ポッド、ノード、およびサービスを管理できます。

Kubernetes の概念に関する情報については、Kubernetes のドキュメントを参照してください。

SMF の Kubernetes コンポーネントの詳細については、次を参照してください：

- ポッド
- サービス

# ポッド

ポッドは、Kubernetes クラスタで実行されるプロセスです。ポッドは、コンテナと呼ばれる細かなユニットをカプセル化します。各ポッドには、1 つ以上のコンテナを含めることができます。

Kubernetes は、物理マシンまたは仮想マシンである単一ノードに 1 つまたは複数のポッドを展開します。各ポッドには、内部 IP アドレスとポートスペースを持つ個別の ID があります。ただし、ポッド内のコンテナは、ストレージリソースとネットワークリソースを共有できます。

次の表に、SMF ポッドの名前と、割り当てたラベルに応じてそれらが展開されるホストを示します。ラベルの割り当て方法については、「ノードへのポッドの関連付け」を参照してください。

表 *385 : SMF* ポッド

| ポッド名 | 説明 | Virtual Machine Name |
|---|---|---|
| api-smf-ops-center | SMF Ops センターの *confD* API ポッドとして機能します。 | OAM |
| base-entitlement-smf | スマート ライセンス 機能をサポートします。 | OAM |
| cache-pod | 他のポッドが適宜使用するあらゆる種類のシステム情報をキャッシュするポッドとして動作します。 | プロトコル |
| cdl-ep-session | CDL へのインターフェイスを提供します。 | セッション |
| cdl-index-session | セッション ポッドへのキーのマッピングを保持します。 | セッション |
| cdl-slot-session | セッションデータを保存する CDL セッション ポッドとして動作します。 | セッション |
| dns-proxy | SMF の DNS エンドポイントとして動作 | プロトコル |
| diameter-ep-gx-client | Diameter エンドポイントとして動作し、Gx インターフェイスを介した SMF と PCRF 間の通信を可能にします。 | プロトコル |
| diameter-ep-gy-client | Diameter エンドポイントとして動作し、Gy インターフェイスを介した SMF と PCRF 間の通信を可能にします | プロトコル |
| マニュアル | ドキュメントが含まれています。 | OAM |
| edr-monitor pod | 永続ボリュームに維持されている EDR ファイルが含まれています。 | OAM |
| etcd-smf-etcd-cluster | ポッドインスタンス、リーダー情報、NF-UUID エンドポイントなどの情報を保存する SMF アプリケーションの etcd をホストします。 | OAM |
| grafana-dashboard-cdl | Grafana の CDL メトリックのデフォルト ダッシュボードが含まれます。 | OAM |
| grafana-dashboard-smf | Grafana の SMF サービス メトリックのデフォルト ダッシュボードが含まれます。 | OAM |
| gtpc-ep | SMF の GTPC エンドポイントとして動作します。 | プロトコル |
| kafka | CDL レプリケーションの Kafka の詳細をホストします。 | プロトコル |
| li-ep | SMF の合法的傍受エンドポイントとして動作します。 | プロトコル |

| ポッド名 | 説明 | Virtual Machine Name |
|---|---|---|
| nodemgr | N4 リンクの確立と管理（ハートビート）など、ノードレベルの連携動作を実行します。また、UE IP アドレス、SEID、CHF-ID、リソース URI などの一意の識別子を生成します。 | サービス |
| node-monitor pod | すべての K8 ノードを監視し、問題が発生するとセルフリブートを実行します。これにより、他のラックへの GR がトリガーされます。 | NA |
| oam-pod | show コマンド、configuration コマンド、モニタ プロトコル モニタ サブスクライバなど、Ops センターのアクションを促進するためのポッドとして動作します。 | OAM |
| ops-center-smf-ops-center | SMF Ops センターとして機能します。 | OAM |
| protocol | アプリケーション プロトコル（PFCP、GTP、RADIUS など。その基礎となるトランスポート プロトコルは UDP）のエンコーダおよびデコーダとして動作します。 | プロトコル |
| Radius-ep | SMF の RADIUS エンドポイントとして動作 | プロトコル |
| rest-ep | HTTP2 通信用の SMF の REST エンドポイントとして動作します。 | プロトコル |
| サービス | SMF のメインのビジネス ロジックが含まれています。 | サービス |
| smart-agent-smf-ops-center | SMF Ops センターのユーティリティ ポッドとして機能します。 | OAM |
| UDP プロキシ | すべての UDP メッセージのプロキシとして動作します。UDP クライアントおよびサーバの機能を所有しています。 | プロトコル |
| swift-smf-ops-center | SMF Ops センターのユーティリティ ポッドとして機能します。 | OAM |
| zookeeper | トポロジ管理のために Kafka を支援します。 | OAM |

UDP プロキシの詳細は、「UDP プロキシ ポッド（1236 ページ）」のセクションを参照してください。

これらの SMF ポッドは、共通実行環境（CEE）ポッドと通信します。CEE ポッドの完全なリストについては、『*UCC CEE* 構成および管理ガイド』を参照してください。

# レプリカ

各ポッドは、アプリケーションの1つのインスタンスで実行されます。より多くのインスタンスを実行してより多くのリソースを提供する場合は、インスタンスごとに1つずつ複数のポッドを使用できます。この概念は、Kubernetes ではレプリケーションと呼ばれます。複製されたポッドまたはレプリカは通常、ワークロードリソースとそのコントローラによってグループとして作成および管理されます。

複数のレプリカがある場合、Kubernetes はそれらの間で負荷を分散できます。ノード障害時に、レプリカを使用できます。

（注） レプリカは、ハードウェアと展開されたコール モデルに基づいています。

# UDP プロキシ ポッド

## 機能説明

SMF には、UPF（N4）および SGW（EPS インターワーキング用の s5 または s8）への UDP インターフェイスがあります。プロトコル レイヤ ポッド（smf-protocol and gtp-ep）を利用して、これらの UDP インターフェイス上でメッセージのエンコード、デコード、および交換が行われます。

3GPP 仕様に記載されている機能を使用するには、次の手順を実行します。

- プロトコル レイヤ ポッドが元の送信元と宛先の IP アドレスおよびポート番号を受け取ることは必須です。ただし、着信パケットが Kubernetes（K8s）クラスタの UDP サービスに到着した後、元の IP および UDP ヘッダーは保持されません。
- 同様に、発信メッセージの場合、（ピア ノードに公開される）UDP サービスの外部 IP アドレスに設定された送信元 IP が必須です。ただし、プロトコル レイヤ ポッドのさまざまなインスタンスが K8s クラスタのさまざまなノードから発信メッセージを送信する場合、送信元 IP は出力インターフェイスに従って選択されます。

プロトコル レイヤ ポッドは、前述の条件を満たすために外部 IP アドレスを構成された物理インターフェイスを持つノードで生成されます。ただし、プロトコル レイヤ ポッドを生成すると、次の結果が発生します。

- プロトコル ポッドは K8s クラスタの同じノードで生成されるため、ノード レベルの HA（高可用性）を実現することはできません。そのノードに障害が発生すると、サービスが失われる可能性があります。
- プロトコル ポッド（smf-protocol、gtp-ep および radius-ep）には、独自の UDP クライアントおよびサーバ機能が含まれている必要があります。さらに、各プロトコル レイヤ ポッドには、アフィニティ ルールに基づいて K8s ノードにラベル付けを行う必要がある場合があります。これにより、プロトコル レイヤポッドのスケーリング要件が制限されます。

SMF では、「udp-proxy」と呼ばれる新しい K8s ポッドを導入することで、これらの問題に対処します。このポッドの主な目的は次のとおりです。

- 「udp-proxy」ポッドは、あらゆる種類の UDP メッセージのプロキシとして機能します。また、UDP クライアントおよびサーバの機能も備えています。
- プロトコルポッドは、個々のプロトコル（PFCP、GTP、Radius）のエンコーディングと復号化を実行し、「udp-proxy」ポッドに UDP ペイロードを提供します。「udp-proxy」ポッドは、プロトコル ポッドからペイロードを受信した後、UDP ペイロードを送信します。
- 「udp-proxy」ポッドは、物理 IP の代わりに仮想 IP（VIP）で UDP ソケットを開きます。これにより、「udp-proxy」ポッドが特定の K8s ノード（VM）に対して厳密なアフィニティを持ちません。したがって、UDPプロキシに対してノードレベルのHAが有効になります。

**Note** 「udp-proxy」ポッドの 1 つのインスタンスは、デフォルトで、K8s クラスタ内のすべてのワーカー ノードで生成されます。

SMF 向けの UDP プロキシ機能は、仮想 IP アドレス機能と機能的な関連性があります。

## アーキテクチャ

udp-proxy ポッドは、K8s クラスタのワーカー ノードに配置されます。

1. 各 K8s ワーカー ノードには、udp-proxy ポッドのインスタンスが 1 つ含まれています。ただし、仮想 IP を所有するのは K8s ワーカー ノードの 1 つだけです。仮想 IP を所有するワーカー ノードはアクティブ モードのままで、他のすべてのワーカー ノードはスタンバイ モードのままです。
2. アクティブな udp-proxy ポッドは、仮想 IP および指定されたポートにバインドされて、ピア ノード（UPF および SGW）からの UDP メッセージをリッスンします。
3. ピア ノードから受信した UDP ペイロードは、プロトコルの 1 つのインスタンス、gtp-ep、または radius-ep ポッドに転送されます。ペイロードは、さらに処理するために同じノードまたは異なるノードのいずれかで転送されます。
4. protocol、gtp-ep、または radius-ep ポッドからの応答メッセージは、udp-proxy ポッドのアクティブなインスタンスに転送されます。udp-proxy ポッドは、対応するピア ノードに応答メッセージを送り返します。
5. SMF によって開始されたメッセージは、protocol、gtp-ep、または radius-ep ポッドでエンコードされます。さらに、UDP ペイロードが udp-proxy ポッドに送信されます。最終的に、udp-proxy ポッドは完全な IP ペイロードで構成され、メッセージをピアに送信します。ピアからの応答を受信すると、メッセージを送信したのと同じ smf-protocol、gtp-ep、または radius-ep ポッドに UDP ペイロードが送り返されます。

### ピアによって開始されたメッセージのプロトコル ポッドの選択

udp-proxy ポッドは、ピア ノード（UPF など）によって開始されたメッセージを受信すると、プロトコル インスタンス間で負荷分散して、プロトコル ポッドの任意のインスタンスを選択します。このインスタンス番号のエントリが、ピア ノードの送信元 IP および送信元ポート番号とともに保存されます。同じ送信元 IP および送信元ポートからのメッセージが、以前に選択されたインスタンスと同じインスタンスに送信されます。

### UDP プロキシの高可用性

UDP プロキシの HA モデルは、キープアライブ仮想 IP の概念に基づいています。VIP は、展開中に N4 インターフェイスに指定されます。また、キープアライブ インスタンスは VIP を管理し、VIP の IP アドレスが K8s クラスタのワーカー ノードのいずれかにあるインターフェイスのセカンダリ アドレスとして作成されるようにします。

このワーカー ノードの「udp-proxy」インスタンスは VIP にバインドされ、アクティブな「udp-proxy」ポッドのロールを担います。他のワーカー ノードのすべての「udp-proxy」インスタンスはスタンバイ モードのままです。

# ノード モニタリング ポッド

ノード モニタ ポッドは、マスター ノードとワーカー ノードなどすべての Kubernetes ノードで実行され、他のノードの動作状態を定期的にチェックします。ネットワークの問題またはハードウェアの一時的な問題により、ノードが到達不能になる可能性があります。

ノードの動作状態に応じて、ノードモニタ ポッドはさまざまなモードに切り替わります。SMF は、グローバル コンフィギュレーション モードで CLI コマンド **nodemonitor** を使用してモードを切り替えます。

次の構成セクションでは、コマンドとモードに関する詳細について説明します。

## ノード モニタリング ポッドの構成

ノードモニタリング ポッドは、ハードウェアの一時的な問題を解決するためにさまざまなモードに切り替わります。

モードを切り替えるには、次の構成例を使用します。

```
config
   nodemonitor mode { 0 | 1 | 2 | 3 interval wait_time }
   end
```

注：

- **nodemonitor mode { 0 | 1 | 2 | 3 interval** *wait_time* **}**
  - **mode 0**：モニタリング機能を無効にします。
  - **mode 1**：2 つ以上のノードに到達できない場合に、ノードのモニタリングを有効にし、ハードコードされた値の 2 秒に達した後にのみ自己再起動を実行します。これがデフォルトの設定です。

- **mode 2**：すべてのノードではなく、2 つ以上のノードに到達できない場合に、ノードのモニタリングを有効にし、自己リブートを実行します。
- **mode 3 interval** *wait_time*：2 つ以上のノードに到達できない場合に、ノード モニタリング ポッドが再起動されるまでの時間間隔を秒単位で指定します。

  *wait_time*は、 5 ～ 300 の範囲の整数である必要があります。

### 設定例

次に、ノード モニタリング ポッド構成の例を示します。

```
config
   nodemonitor mode 3 interval 15
   end
```

この例に従って、ノード モニタリング ポッドは 15 秒待機してから、2 つまたは ノードに到達できない場合、セルフリブートを実行します。

### 設定の確認

構成を確認するために、この **show running-config nodemonitor** コマンドを使用します。

この show コマンドの出力には、ノードモニタリング ポッドのモードに関する構成が表示されます。

```
smf# show running-config nodemonitor
nodemonitor mode 3 interval 15
```

# サービス

SMF の構成は、一連の個別のポッドで実行される複数のマイクロサービスが含まれています。マイクロサービスは、SMF の展開時に展開されます。SMF はこれらのサービスを使用して、ポッド間の通信を可能にします。別のポッドと対話する場合、サービスはポッドの IP アドレスを識別してトランザクションを開始し、ポッドのエンドポイントとして機能します。

次の表では、SMF サービスと、それらが実行されるポッドについて説明します。

**表 *386 : SMF* サービスとポッド**

| Service Name | ポッド名 | 説明 |
|---|---|---|
| base-entitlement-smf | base-entitlement-smf | スマートライセンス機能をサポート |
| datastore-ep-session | cdl-ep-session | CDL セッションを担当します。 |
| datastore-notification-ep | smf-rest-ep | *smf-rest-ep* を介して CDL から *smf-ser* 知を送信します。 |
| datastore-tls-ep-session | cdl-ep-session | セキュアな CDL 接続を担います。 |

| Service Name | ポッド名 | 説明 |
|---|---|---|
| diameter-ep-gx-client | diameter-ep-gx-client | クレジット制御メッセージのために、g<br>メッセージをDiameterエンドポイントに<br>します。これは、Diameterエンドポイン<br>よってDiameter CCRメッセージに変換さ<br>Gx サーバーに送信されます。 |
| diameter-ep-gy-client | diameter-ep-gy-client | クレジット制御メッセージのために gRI<br>メッセージをDiameterエンドポイントに<br>します。これは、Diameterエンドポイン<br>よってDiameter CCRメッセージに変換さ<br>Gy サーバーに送信されます。 |
| マニュアル | マニュアル | SMF ドキュメントを担当します。 |
| edr-monitor | edr-monitor | 永続ボリューム内の EDR ファイルのメ<br>ナンスを担当します |
| etcd | etcd-smf-etcd-cluster-0、<br>etcd-smf-etcd-cluster-1、<br>etcd-smf-etcd-cluster-2 | 名前空間内のポッド検出を担当します。 |
| etcd-smf-etcd-cluster-0 | etcd-smf-etcd-cluster-0 | *etcd* クラスタ間のデータの同期を担当し<br>す。 |
| etcd-smf-etcd-cluster-1 | etcd-smf-etcd-cluster-1 | *etcd* クラスタ間のデータの同期を担当し<br>す。 |
| etcd-smf-etcd-cluster-2 | etcd-smf-etcd-cluster-2 | *etcd* クラスタ間のデータの同期を担当し<br>す。 |
| grafana-dashboard-app-infra | grafana-dashboard-app-infra | Grafana のアプリ インフラ メトリックの<br>フォルト ダッシュボードを担当します。 |
| grafana-dashboard-cdl | grafana-dashboard-cdl | GrafanaのCDLメトリックのデフォルト<br>シュボードを担当します。 |
| grafana-dashboard-smf | grafana-dashboard-smf | GrafanaのSMF-serviceメトリックのデフ<br>ト ダッシュボードを担当します。 |
| gtpc-ep | gtpc-ep | GTP-C ポッドとのポッド間通信を担当し<br>す。 |
| helm-api-smf-ops-center | api-smf-ops-center | Ops センター API を管理します。 |
| kafka | kafka | Kafka メッセージを処理します。 |
| li-ep | li-ep | 合法的傍受の相互作用を担います。 |
| local-ldap-proxy-smf-ops-center | ops-center-smf-ops-center | Grafana などの他のアプリケーションに<br>てOpsセンターのログイン情報を活用す<br>任があります。 |

| Service Name | ポッド名 | 説明 |
|---|---|---|
| oam-pod | oam-pod | Ops センターでの Exec コマンドの促進<br>します。 |
| ops-center-smf-ops-center | ops-center-smf-ops-center | SMF Ops センター を管理します。 |
| ops-center-smf-ops-center-expose-cli | ops-center-smf-ops-center | 外部 IP アドレスで SMF Ops センター<br>セスする。 |
| smart-agent-smf-ops-center | smart-agent-smf-ops-center | SMF Ops センター API に対応します |
| smf-sbi-service | smf-rest-ep | REST-EP ポッドへの着信 HTTP2 メッ<br>のルーティングを担当します。 |
| smf-n10-service | smf-rest-ep | REST-EP ポッドへの着信 N10 メッセ<br>ルーティングを担当します。 |
| smf-n11-service | smf-rest-ep | REST-EP ポッドへの着信 N11 メッセ<br>ルーティングを担当します。 |
| smf-n40-service | smf-rest-ep | REST-EP ポッドへの着信 N40 メッセ<br>ルーティングを担当します。 |
| smf-n7-service | smf-rest-ep | REST-EP ポッドへの着信 N7 メッセー<br>ルーティングを担当します。 |
| smf-nrf-service | smf-rest-ep | REST-EP ポッドへの着信 NRF メッセ<br>ルーティングを担当します。 |
| smf-nodemgr | smf-nodemgr | *smf-nodemgr* ポッドとのポッド間通信<br>します。 |
| smf-protocol | smf-protocol | smf-protocol ポッドとのポッド間通信<br>します |
| smf-radius-dns | smf-radius-dns | smf-radius-dns ポッドとのポッド間通信<br>します |
| smf-rest-ep | smf-rest-ep | smf-rest-ep ポッドとのポッド間通信を<br>ます |
| smf-service | smf-service | smf-service ポッドとのポッド間通信を<br>ます。 |
| swift-smf-ops-center | swift | SMF Ops センターのユーティリティ<br>として機能します |
| zookeeper | zookeeper | トポロジ管理のために Kafka を支援 |
| zookeeper-service | zookeeper | トポロジ管理のために Kafka を支援 |

# オープン ポートおよびサービス

SMF は、通信目的で異なるポートを使用します。次の表に、デフォルトのオープン ポートおよび関連するサービスを示します。

**表 *387*: オープン ポートおよびサービス**

| ポート | サービス | 使用方法 |
|---|---|---|
| 9003 | gRPC | これは、ホストネットワークを使用していないすべてのアプリケーション ポッドのデフォルトの gRPC ポートです。 |
| 8080 | TCP/HTTP | これは、ホストネットワークを使用していないすべてのアプリケーション ポッドのデフォルトの prometheus サーバー ポートです。 |
| 8090 | TCP/HTTP | SMF は、SBI インターフェイス エンドポイントの HTTP2 REST エンドポイントを使用します。 |
| 2024 | SSH | SMF Ops Center はこのポートを使用して ConfD CLI アクセスを提供します。 |
| 2379-2380 | TCP | SMF は etcd サーバー クライアント エンドポイントを使用して、システム データを保存および取得します。 |
| 8882 | gRPC | これは、他のすべてのアプリケーション ポッドで使用される CDL セッション DB エンドポイントです。 |
| 8890 | gRPC | アプリケーション REST エンドポイントはこのポートを使用して、CDL からコールバック タイマーまたは通知を受信します。 |
| 8883 | gRPC | これは、他のすべてのアプリケーションポッドで使用される TLS - CDL セッション DB エンドポイントです。 |
| 2123 | UDP | SMF は、GTP-C プロトコル メッセージ（制御パス）のシグナリングに 3GPP 標準の GTP-C ポートを使用します。 |
| 2152 | UDP | SMF は、GTP-U プロトコル メッセージ（データパス）のシグナリングに 3GPP 標準 GTP-U ポートを使用します。 |
| 8805 | UDP | SMF は、PFCP プロトコル メッセージのシグナリングに 3GPP 標準 PFCP ポートを使用します。 |
| 8765 | TCP6 | SMF は、このポートを UDP プロキシポッドの準備プローブ ポートとして使用します。 |
| 7179、7189 | TCP/HTTP | Pprof サーバー エンドポイントは、S11 や S5 などの GTP-C エンドポイント インターフェイス固有のポッドからのランタイム プロファイリング データを提供します。 |
| 23300, 23310 | TCP/gRPC | SMF は、GTP-C エンドポイント インターフェイス固有のポッドに TLS GRPC IPC サーバー エンドポイントを使用します。 |

| ポート | サービス | 使用方法 |
|---|---|---|
| 9005、9015 | TCP/gRPC | GTP-C エンドポイント インターフェイス固有のポッドの非 TLS GRPC IPC サーバー ポート。 |
| 27000、27010 | TCP | SMF は、GTP-C エンドポイント インターフェイス固有のポッドに KeepAliveD エンドポイントを使用します。 |
| 7279、7289 | TCP | このポートは、GTP-C エンドポイント インターフェイス固有のポッドで使用される管理エンドポイントの内部ポートです。このポートは、稼働状態および準備状態プローブに使用されます。 |
| 7079、7089 | TCP/HTTP | SMF は、GTP-C エンドポイント インターフェイス固有のポッドに prometheus サーバーポートを使用します。 |
| 8083 | TCP/HTTP | SMF は、プロトコル ポッドに prometheus サーバー ポートを使用します。 |
| 9006 | TCP/gRPC | SMF は、プロトコル ポッドの非 TLS GRPC IPC サーバー エンドポイントを使用します。 |
| 8003 | TCP/HTTP | SMF は、プロトコル ポッドに prometheus サーバー ポートを使用します。 |
| 23100 | TCP/gRPC | SMF は、プロトコル ポッドの TLS GRPC IPC サーバー エンドポイントを使用します。 |
| 7679 | TCP/HTTP | Pprof サーバー エンドポイントは、プロトコル ポッドからのランタイム プロファイリング データを提供します。 |
| 7879 | TCP | このポートは、プロトコル ポッドで使用される管理エンドポイントの内部ポートです。このポートは、稼働状態および準備状態プローブに使用されます。 |
| 27500 | TCP | SMF は、プロトコル ポッドにこの KeepAliveD エンドポイントを使用します。 |
| 28000 | TCP | SMF は、UDP プロキシ ポッドのこのキープアライブ エンドポイントを使用します。 |
| 23200 | TCP/gRPC | SMF は、UDP プロキシ ポッドの TLS GRPC IPC サーバー エンドポイントを使用します。 |
| 9004 | TCP/gRPC | UDP プロキシ ポッドの非 TLS GRPC IPC サーバーエンドポイント。 |
| 7879 | TCP | このポートは、UDP プロキシ ポッドで使用される管理エンドポイントの内部ポートです。このポートは、稼働状態および準備状態プローブに使用されます。 |
| 8850 | TCP/HTTP | Pprof サーバー エンドポイントは、UDP プロキシ ポッドからのランタイム プロファイリング データを提供します。 |

上記のポートに加えて、SMF は SMI 宛てのポートを使用して、ホスト間の情報をルーティングします。SMI ポートについては、『 *Ultra Cloud Core Subscriber Microservices Infrastructure Operations Guide*』を参照してください。

# ノードへのポッドの割り当て

ここでは、ラベルに基づきポッドをノードに関連付ける方法について説明します。

クラスタを構成したら、ラベルを使用してポッドをノードに関連付けることができます。この関連付けにより、キーと値のペアに基づいて、ポッドを適切なノードに展開できます。

ラベルは、展開する必要があるノードを識別し、サービスを実行するために ポッドに必要です。たとえば、必要なキーと値のペアを使用してプロトコル層のラベルを構成すると、そのキーと値のペアに一致するノードに ポッドが展開されます。

ラベルを介してポッドをノードに関連付けるには、次の構成例を使用します。

```
config
  k8 label vm_group key label_key value label_value
  end
```

注：

- **k8 label** *vm_group* **key** *label_key* **value** *label_value*：K8 ノード アフィニティ ラベルのパラメータを構成します。
  - *vm_group*：VM グループを指定します。次のいずれかである必要があります。
    - cdl-layer
    - oam-layer
    - protocol-layer
    - service-layer
  - **key** *label_key*：ラベル キーを指定します。 *label_key* は文字列である必要があります。
  - **value** *label_value*：ラベル値を指定します。 *label_value* は 文字列である必要があります。
- ラベルを構成しない場合、SMF ではデフォルトのキー値のペアを含むラベルが想定されます。

# ポッドの詳細とステータスの表示

サービスに追加のポッドが必要な場合、SMF はポッドを作成して展開します。展開内でポッドのリストは、SMF Ops Center で確認できます。

マスター ノードから **kubectl** コマンドを実行して、Kubernetes リソースを管理できます。

ポッドの詳細は、YAML 形式で利用できます。

次のサンプル構成を使用して、包括的なポッドの詳細を表示するには：

**kubectl get pods -n smf** *pod_name* **-o yaml**

このコマンドの出力には、次の情報の列が表示されます。

- ポッドが展開されているホストの IP アドレス。
- ポッドで実行されているサービスとアプリケーション。
- ポッド内のコンテナの ID と名前。
- ポッドの IP アドレス。
- ポッドの現在の状態とフェーズ。
- ポッドが現在の状態になった時刻からの開始時刻。

SMF 名前空間内のすべてのポッドを表示するには、次の構成例を使用します：

**kp get pods -n** *smf_namespace* **-o wide**

# 状態

ポッドの状態を理解することで、現在の正常性を判断し、潜在的なリスクを防ぐことができます。以下のテーブルでは、ポッドの状態を説明します。

**表 *388*：ポッドの状態**

| 状態 | 説明 |
|---|---|
| Running | ポッドは正常であり、ノードに展開されています。<br>1 つ以上のコンテナが含まれている。 |
| Pending | アプリケーションは、ポッドのコンテナ イメージを作成中です。 |
| 成功 | ポッド内のすべてのコンテナが正常に終了したことを示します。これらのポッドは再起動できません。 |
| 失敗しました（Failed） | ポッド内の 1 つ以上のコンテナが終了プロセスに失敗しました。障害は、コンテナがゼロ以外のステータスで終了したか、システムによってコンテナが終了されたために発生しました。 |
| 不明 | ポッドの状態を特定できませんでした。通常、これは、ポッドが存在するノードに到達できないために発生する可能性があります。 |

# UDP プロキシ バイパスを使用した PFCP プロトコル エンドポイント マージ

## 機能説明

バイパス プロキシは、この GTP パケットが gtpc-ep ポッドに直接到着できるようにするために導入されました。これにより、udp-proxy での処理が回避され、パケット転送での 1 ホップが減少します。

既存の gtpc-ep と udp-proxy でサポートされているすべての機能が、新しくマージされたパスに統合されます

次の機能は udp-proxy から統合されています。

- トランザクション SLA
- GTP パケットの DSCP マーキング
- ローミング サブスクライバの BGP ルートのオン ザ フライを追加
- ディスパッチャ機能と着信再送信のサポート
- DDN の SGW キャッシュの統合
- MBR キャッシュ統合

次の機能は gtpc-ep から統合：

- アウトバウンド要求の n3t3 構成に基づく再送信
- プロトコルをモニタし、サブスクライバをモニタする
- エコー メッセージ処理

### GR スプリットを使用した GTPC エンドポイント

スケーリングされた GTP トラフィックを処理し、CPU を最適に使用するために、GTPC-EP の複数のアクティブ インスタンスが開始され、GR インスタンスに基づいてトラフィック分割が行われます。

# プロトコルマイクロサービスに統合されたUDPプロキシ機能

## 機能説明

UDP プロキシ マイクロサービスは、UDP を必要とするプロトコル（PFCP、GTPC、および RADIUS）の UDP トランスポート終端を提供します。UDP プロキシは、ユーザー空間パケット転送と IPC 通信をプロトコル マイクロサービスへ提供します。また、送信元 IP アドレスのオブザーバビリティのためにホスト ネットワーキングを使用し、アクティブ/スタンバイ モードで動作します。

複数のプロトコル マイクロ サービスが UDP 転送の UDP プロキシに依存しているため、UDP プロキシはスケールのボトルネックと単一の障害発生時点になります。UDPプロキシ機能をそれぞれのプロトコルのマイクロサービスに統合することで、シグナリング パス内のマイクロサービス間での1ホップを減らすことにより、スケールのボトルネックを軽減し、CPUの使用率を向上させることができます。

## 機能の仕組み

### UDP プロキシ バイパスを使用した PFCP プロトコル エンドポイント

プロトコル エンドポイントは UDP プロキシをバイパスし、N4/Sxa メッセージを UPF に直接送信します。UPF からの着信 N4/Sxa メッセージも UDP プロキシをバイパスして、プロトコル ポッドに到達します。（ハートビート要求メッセージでの送信元 IP アドレス IE の UPF サポートの対象となります）。プロトコル ポッドは、非ホスト ネットワーキング モードの動作を使用し続けます。

Kubernetes サービスが構成された VIP IP アドレスおよび標準ポートでリッスンを開始し、着信 N4/Sxa UDP パケットがプロトコル ポッドに送信されるようにします。着信メッセージ/パケットに関連付けられたインターフェイスを識別するための個別のターゲット ポートを使用して、N4 および Sx 用に作成された個別の Kubernetes サービス。Kubernetes クライアント IP アドレス アフィニティは、UPF からの再送信パケットが同じプロトコル ポッド インスタンスに送信されて再送信キャッシュに正常にヒットするようにするために利用されます。

### 現在のモード（バイパスなし）

この動作モードでは、N4、Sxa、GTP-U のメッセージ交換は UDP プロキシを介して行われます。UDP プロキシは、UPF との接続または受信を行います。

すべての PFCP に関連するノード関連のメッセージやセッション サービスまたは UPF から開始され、その応答は UDP プロキシを通過します。

### アウトバウンド バイパス プロキシ モード

この操作モードは、S-GW または SMF サービスによって開始され、システムが Kubernetes Pod 環境変数「OUTBOUND_PROXY_BYPASS」を介して PFCP を使用して UPF に送信するすべてのメッセージに対してデフォルトで有効になっています。SMF（プロトコルポッド）によって UPF に直接送信されるメッセージは、関連するセッションで、次のようになります。

1. PFCP セッション確立要求
2. PFCP セッション変更要求
3. PFCP セッション削除要求

このモードでは、UPF から、またはサービスによって開始された UPF への GTP-U メッセージは、引き続き UDP プロキシを介して交換されます。このモードでは、セッション関連のメッセージ（つまり、SMF サービスによって開始されたメッセージ）のみが、プロトコルから UPF に直接流れます。

プロトコル ポッドは、サービスから UPF IP アドレスを受信します。これは、UPF との接続の設定に使用され、その後、セッション関連のメッセージ交換に同じアドレスを使用します。ノードに関連するメッセージは、UDP プロキシからプロトコルまたはノード マネージャへのパスを継続して取り続けます。

### 完全なバイパス モード（インバウンドおよびアウトバウンド）

このモードでは、着信メッセージと発信メッセージの両方が、UDP プロキシをバイパスするプロトコル ポッドによって送受信されます。プロトコル ポッドは、構成された VIP に基づいて N4 および GTPu または Sxa ポートでリッスンします。プロトコル ポッドは Kubernetes サービス ネットワーク上に存在しなくなり、ホスト ベースのネットワーキング モードのままになります。プロトコル ポッドは、それが存在するノードまたは VM の IP を取得します。この条件は、プロトコルおよび UDP プロキシ ポッドの両方に存在するか、または使用可能な環境変数（UDP_PROXY_BYPASS）に基づいてトリガーされます。デフォルトでは、この変数は false で、UDP プロキシとプロトコルは、UPF とメッセージを交換する UDP プロキシの現在のように続行されます。

UDP_PROXY_BYPASS は、次の両方の条件が満たされた場合にのみ true に設定されます：

1. VIP は、エンドポイント PFCP インターフェイス N4 またはインターフェイス Sxa で構成されます。
2. エンドポイント プロトコル インターフェイス N4 またはインターフェイス Sxa で構成された VIP はありません。

UDP_PROXY_BYPASS 変数の値を変更すると、UDP プロキシとプロトコル ポッドの両方が再起動され、この新しい動作モードが有効になるか、UDP プロキシを介してメッセージ交換の以前のモードにフォールバックします。

CLI を使用したバイパス モードのトリガー

バイパス モードまたはプロトコル プロキシ マージの機能をトリガーするには、次に示すように、エンドポイント PFCP で VIP-IP を構成する必要があります。

```
no instance instance-id 1 endpoint protocol interface n4
no instance instance-id 1 endpoint protocol interface gtpu
instance instance-id 1 endpoint pfcp interface n4 vip-ip X.X.X.X
instance instance-id 1 endpoint pfcp interface gtpu vip-ip X.X.X.X
```

**重要** 上記の構成で、環境変数 UDP_PROXY_BYPASS の値が変更されます。これにより、ポッドの UDP プロキシとプロトコルの両方の再起動がトリガーされます。

endpoint+ protocol に存在するすべての機能は、対応するように endpoint+PFCP で構成する必要があります。これには、DSCP、SLA、ディスパッチャ関連の構成などの機能が含まれている必要があります。すべての機能の設定は、内部 VIP-IP がエンドポイント = PFCP およびインターフェイス N4 またはインターフェイス Sxa で構成されている場合にのみ有効になります。エンドポイント プロトコルの下に、インターフェイス N4 と VIP-IP、またはインターフェイス Sxa と VIP-IP が存在する必要があります。

### CLI 値のレンダリング

N4 および Sxa VIP の構成に基づいて、レンダリング ロジックはエンドポイント プロトコルで公開する値を計算します。構成は、「endpointIp」というキーを持つポッドでレンダリングされます。個々のポッドの構成パスは、/config/AppName/vip-ip/endpointIp.yaml にあります。影響を受けるポッドは次のとおりです：

1. プロトコル
2. Node Mgr
3. SMF-Service
4. SGW サービス。

エンドポイント - pfcp 構成がエンドポイント - プロトコルの下でレンダリングされるようにすると、バックグラウンド構成読み取りロジックへの変更を回避できます

### ノード管理

この場合、プロトコルはピアが接続するために PFCP エンドポイントを開始します。同時に、アプリ サービスが UPF に向けて PFCP メッセージを開始すると、UPF との接続も確立します。次のメッセージが含まれます：

1. PFCP 関連付けのセットアップ要求/応答
2. PFCP 関連付け更新要求/応答
3. PFCP セッション レポート要求/応答
4. PFCP ノード レポート要求/応答
5. ハートビート要求/応答
6. PFCP PFD 管理要求/応答

### セッション管理

サービスによって開始され、プロトコル ポッドを介して UPF に直接送信されるセッション管理メッセージ。プロトコル ポッドは UPF との接続を開始してこれらのメッセージを送信します。これが、プロトコル ポッドが存在するノードの IP アドレスを取得するために「ホスト ネットワーキング」にある必要がある理由です。

### 標準化されたポート番号

「マージ」モードをトリガーしている間、プロトコル ポッドはホスト ベースのネットワーキングに移行します。プロトコル ポッドは、既存の UDP プロキシ ポッドと同様にホストまたはノードの IP アドレスを取得します。UDP プロキシ、GTPC-EP、およびプロトコルが同じポートを共有しないことが重要です。ポート計算のための経験的なルールは次のとおりです。

```
Port_Value = Base_Port _Value + (Gr_Instance_Id_index *50) + (Logical_Instance_id mod
50)
```

Gr_Instance_id：CLI を使用して構成で提供される GR インスタンス ID。

Logical_Instance_id：論理 SMF インスタンスの識別子。

**Prometheus ポート**：

完全な UDP プロキシ バイパスでは、Prometheus ポート 8080 は使用されず、代わりにインスタンス 1 の Prometheus 8004 の開始ポートが使用されます。8003 で追加される「instance-Id」はポート番号である必要があります。

**プロキシ キープアライブ ポート**:

プロキシ キープアライブ ポートは、27500+ 「Instance-Id」から始まります。

1. GR インスタンス 1 & 論理インスタンス ID 0：- 27500 +（0 * 50）+（0 % 50）= 27500
2. GR インスタンス 2 & 論理インスタンス ID 0：- 27500 +（1 * 50）+（0 % 50）= 27550

**キープアライブおよび活性プローブの管理ポート**:

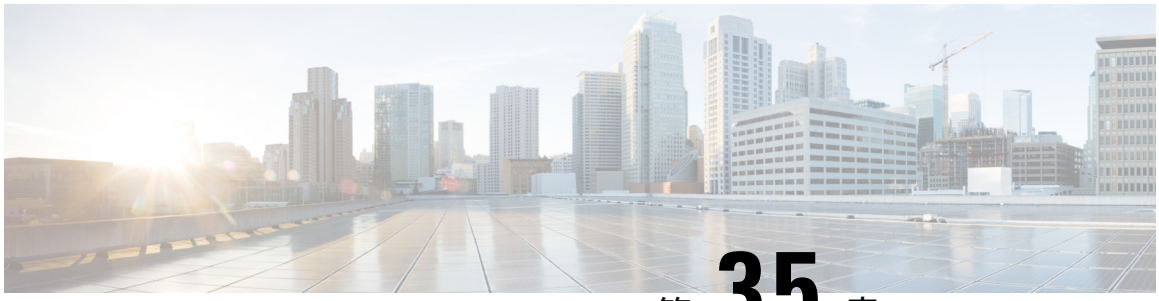
管理ポートは 7879 + (Gr_Instance_Id_index * 50) + (Logical_Instance_id mod 50) になります。

**インフラ診断ポート**:

Infra Diag ポートは、7779 + (Gr_Instance_Id_index * 50) + (Logical_Instance_id mod 50) になります。

**PProf ポート**:

PProf プロファイリング ポートは 7679 +（Gr_Instance_Id_index * 50）+（Logical_Instance_id mod 50）になります



第 35 章

# ポリシーおよびユーザー プレーンの管理


- 機能の概要と変更履歴, on page 1252
- 機能説明, on page 1254
- SMF での QoS 管理, on page 1255
- ビットレートマッピングのサポート （1265 ページ）
- デフォルト ベアラの許可された QoS の処理 （1268 ページ）
- ローカル ポリシーに基づく GBR ベアラーの作成 （1272 ページ）
- UPF での EDR 生成の SMF トリガーされたメタデータ, on page 1282
- 構成の動的な更新 （1282 ページ）
- ダイナミック PCC ルールの適用 （1285 ページ）
- ダイナミック QOS フローベースのアプリケーション検出および制御 （1308 ページ）
- Gx を介したダイナミック ADC ルールの適用 （1311 ページ）
- 静的 PCC ルールのサポート, on page 1322
- 定義済み PCC ルール, on page 1339
- ベアラー QCI サポート （1340 ページ）
- ダイナミック PCC およびセッション ルールの非標準 QCI サポート （1343 ページ）
- 帯域幅 ID の構成のサポート （1345 ページ）
- PCF の UE キャンペーン レポートの生成 （1347 ページ）
- UPF ノード選択, on page 1348
- UPF ノード レポートと独自のセッション レポートのサポート （1372 ページ）
- 外部ヘッダー形式 （1378 ページ）
- グレースフルセッション終了の拡張された PFCP 関連付けのリリース手順 （1381 ページ）
- PCF を介した使用状況監視 （1386 ページ）
- N7 上の Ruledefs の QoS グループのサポート （1394 ページ）

# 機能の概要と変更履歴

## 要約データ

***Table 389:*** 要約データ

| | |
|---|---|
| 該当製品または機能エリア | SMF |
| 該当プラットフォーム | SMI |
| 機能のデフォルト設定 | 無効：設定が必要 |
| このリリースでの関連する変更点 | N/A |
| 関連資料 | 該当なし |

## 更新履歴

***Table 390:*** マニュアルの変更履歴

| 改訂の詳細 | リリース |
|---|---|
| PTTサービスなどの専用UEサービスをサポートするためのパケットの優先順位付けに関するサポートが追加されました。 | 2024.01.1 |
| • 4G および 5G 向けの PCF 連携なしでの GBR ベアラー作成のサポートが追加されました。<br>• N7最適化のサポートが追加されました。<br>• ローカル ポリシー構成にオプションの PCF または PCRF 構成のサポートが追加されました。 | 2023.04.0 |
| 次の機能に対して追加サポート：<br>• N7 上の Ruledefs の QoS グループ<br>• UPF での N3 インターフェイスの IPv6 サポート | 2023.01.0 |

| 改訂の詳細 | リリース |
| --- | --- |
| 一意のIPプールを持つUPFを割り当てるための<br>• SMF のサポートが追加されました。<br>• （PDNタイプに基づいてUPFを選択するため） | 2022.04.0 |
| PCF との相互作用中に、Diff-Serv-CodePoint（DSCP）または Type of Service（ToS）QoS 機能のサポートが導入されました。 | 2021.02.3.t3 |
| 次の機能のサポートが追加されました。<br>• PCF を介した使用状況監視<br>• N4 QoS 不一致の修正<br>• ダイナミック QOS フローベースのアプリケーション検出および制御<br>• IP しきい値ベースの UPF の選択 | 2021.02.3 |
| ダイナミックPCCおよびセッションルールの非標準 QCI サポートが導入されました | 2021.02.2 |
| 次の機能のサポートが追加されました。<br>• ビット レート マッピング<br>• スライスとロケーションに基づく UPF の選択<br>• UP 最適化 | 2021.02.0 |
| 次のサポートが追加されました。<br>• 共存 UPF 選択<br>• 帯域幅ポリシー構成における最大グループ数の拡張制限<br>• セッション レポート拒否手順<br>• 外部ヘッダー情報要素（IE）の新しい形式 | 2021.01.0 |

| 改訂の詳細 | リリース |
| --- | --- |
| 次のサポートが追加されました。<br>• DNN および PDU セッション タイプに基づく UPF ノードの選択<br>• 認定デフォルト QoS の変更<br>• 追加のセッション レポートおよび UPF ノードレポート要求 | 2020.03.0 |
| 最初の導入。 | 2020.02.0 より前 |

# 機能説明

**Important** この章で使用されている PGW-C という用語は、SMF でサポートされている EPS インターワーキング機能を意味しており、LTE ネットワークで使用されるスタンドアロン P-GW として想定してはなりません。

SMF は、5G コア ネットワークでセッション管理サービスを提供するコントロール プレーン NF の 1 つです。SMF は、次のセッション管理手順を通じて PDU セッションのライフサイクルを管理します：

- PDU セッション確立
- PDU セッション変更拒否
- PDU セッションの解放

この章では、ポリシーおよびユーザー プレーンの管理機能について説明します。

- ポリシー管理：ポリシー制御機能（PCF）またはローカル設定は、SMF で管理されるポリシーを制御します。PCF は、該当する QoS および課金情報とともに、ポリシーおよび課金制御（PCC）ルールを SMF に送信します。SMF はこの情報を使用して QoS フローを定義し、QoS の適用を行います（ユーザープレーン機能（UPF）および課金機能（CHF）への課金）。PCC ルールは、ローカルで構成することもできます。ローカルで構成されたポリシー ルールは、静的または、定義済みルールとしてラベルされます。
- ユーザー プレーン管理：SMF でのユーザー プレーン管理には、UPF の選択と、セッションごとおよびノード レベルのユーザー プレーン データの維持が含まれます。SMF は、UPF ノードのパス管理を実行します。セッション レベルごとに、SMF はパケット検出ルール（PDR）、QoS 適用ルール（QER）、転送アクション ルール（FAR）、および使用状況レポートルール（URR）を UPF に公開します。次に、SMF は、PCF から受信した、またはローカルに構成されたポリシー ルールを適用します。

# SMF での QoS 管理

## 機能説明

SMF の主な機能は、フローベースの QoS モデルを管理することです。SMF は、統合データ管理（UDM）およびポリシー制御機能（PCF）と相互作用して、GBR および非 GBR フローの登録および承認された QoS パラメータを取得し、関連情報を UE（NAS）、gNB（NGAP）、およびUPF（PFCP）。これにより、ネットワーク上のすべてのノードが PDU セッションに必要な QoS を提供します。

## 使用例

このセクションでは、QoS プロファイルの作成、変更、および削除につながるさまざまな使用例のシナリオと、それに対応するアクションについて説明します。

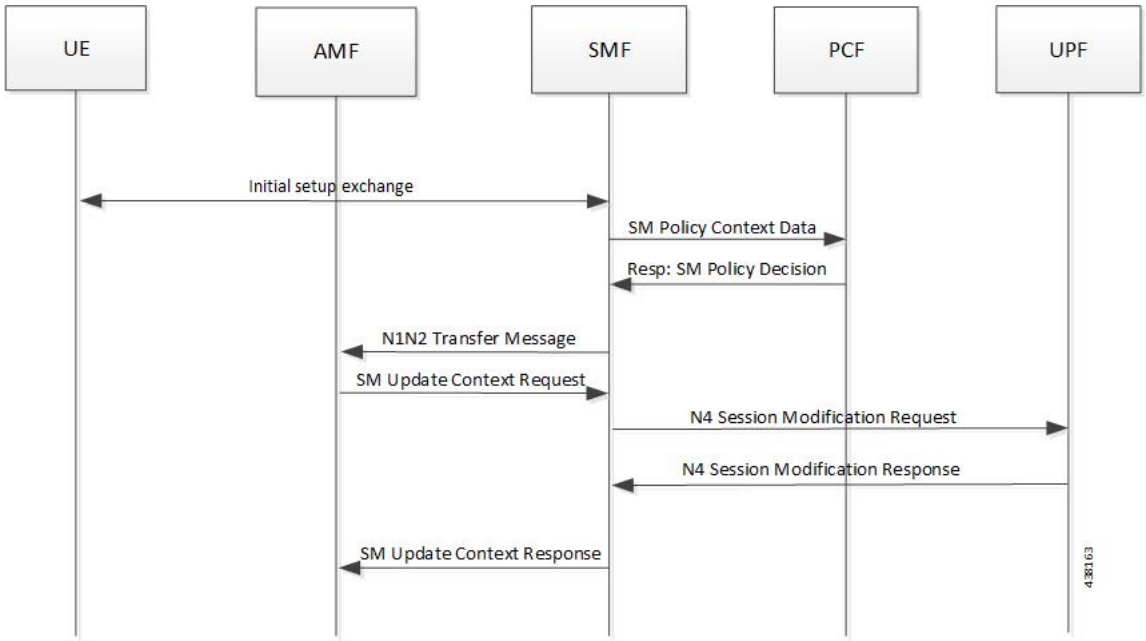
PDU コンテキストに関連付けられた QoS プロファイルは、次のシナリオで変更されます：

- SMPolicyContextData に対する PCF からの応答
- PCF からの更新通知
- SMF から最初に送信される更新要求に代わって PCF から応答を更新
- SMF からの更新要求は、次の場合にトリガーされます：
  - UEによって変更要求がトリガーされました
  - AN トリガー変更要求
  - UDM によって変更要求がトリガーされました

### セットアップの作成

次の図は、セットアップ作成のコール フローを示しています。

*Figure 212:* セットアップ作成コール フロー



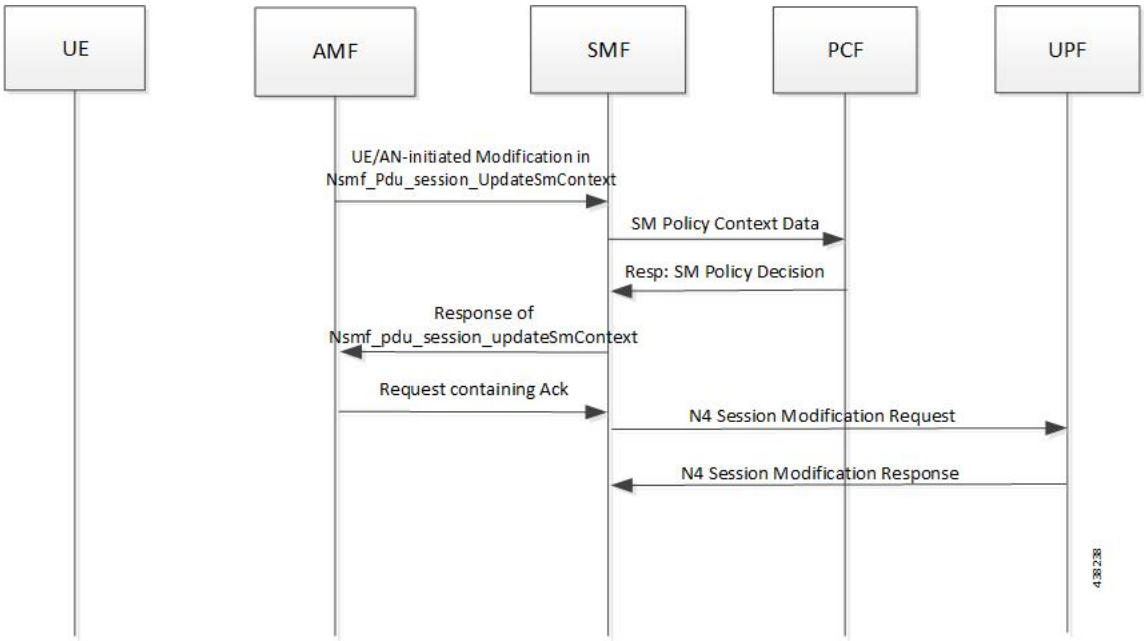

SM ポリシー決定で受信したコンテンツに基づいて、SMF はさまざまなインターフェイスに次をプッシュします。

- UPF:
  - PCC ルールから派生した一連の PDR
  - QoS フローから派生した QER のセットです。これは、PCF から QosDescription/QosCharacteristics から派生します。
  - SessRules から派生した 1 つの追加の QER
- N1：
  - QosFlow から派生した QoS ルールのセット
  - 各 QosRule にはパケットフィルタが関連付けられます。
- N2:
  - QoS フロー情報のセット

## UE/AN によって開始された変更

次の図は、UE/AN によって開始された変更コール フローを示しています。

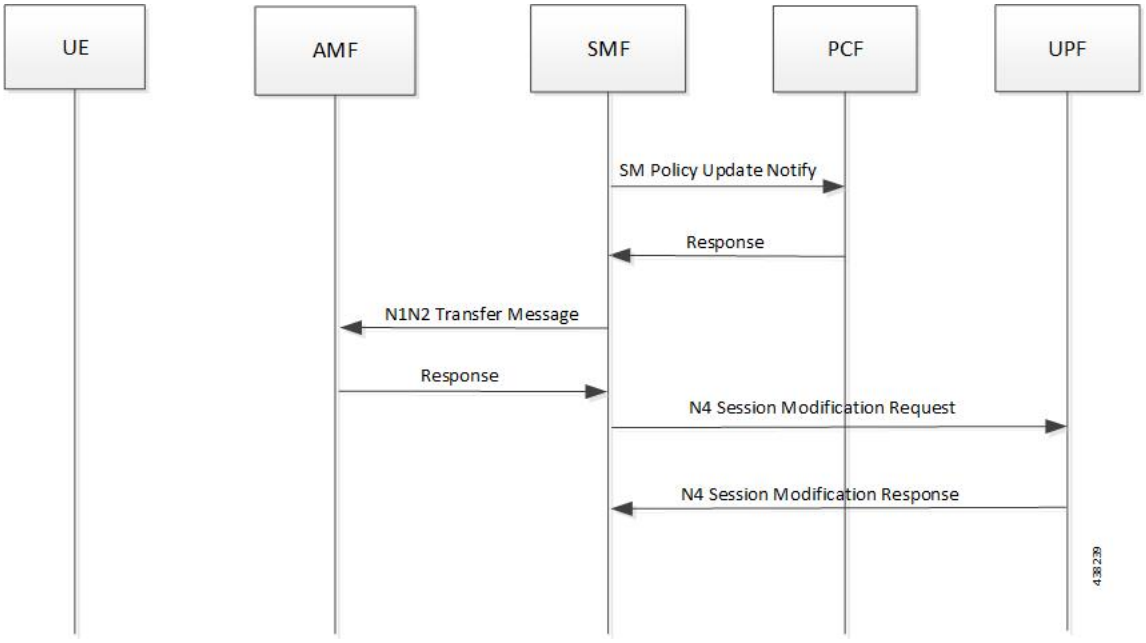
*Figure 213: UE/AN* によって開始された変更コール フロー




## UDM/PCF によって開始された変更

次の図は、UDM/PCF によって開始される変更コールフローを示しています。

*Figure 214: UDM/PCF* によって開始された変更




- N1：

- PDU セッション変更コマンドが SMF からトリガーされます。セッション AMBR ルールと QoS ルールを変更できます。
- PDU セッション変更要求は、UE からトリガーされます。QoS ルールと、サポートされているパケットフィルタの最大数が変更される可能性があります。

  いずれの場合も、QoS ルールの変更は次から発生する可能性があります。

  - パケット フィルタの追加/削除/置換
  - QoS ルールの優先順位の設定
  - QoS パラメータ：5QI/MBR/GBR

- N2：
  - PDUセッションリソース変更要求はSMFからトリガーされます。インストールされている既存の QoS フローを変更したり、すでにインストールされている QoS フローを削除したりできます。変更要求を受信すると、パラメータ（ARP、GBR/MBR、優先度レベルなど）が変更される可能性があります。
  - PDUセッションリソース通知はANからトリガーされます。これは、特定のフローがリリースされ、これ以上履行されず、再度履行された場合に発生します。

## 登録済み QoS

UDM NF は、セッション管理サブスクリプション データで UE のサブスクライブされた QoS を維持します。PDU のセットアップ手順中に、SMF はリソース URI「/(supi)/sm-data」の HTTP2 GET 要求（*3GPP TS 29.503*を参照）を投稿して、セッション管理サブスクリプション データを取得します。サブスクリプション データには、サブスクライバがアクセスできる DNN ごとに 1 つずつの DNN 構成があります。各DNN構成は、次のパラメータで構成されます：

- セッションAMBR：各 PDU セッションのすべての非 GBR QoS フローで共有される、アップリンクおよびダウンリンク ビット レートの合計の最大値。
- 5gQosProfile：デフォルトの 5G QoS インジケータ（5QI）とデフォルトの ARP 値は、DNN 構成のこの属性でセッション管理サブスクリプション データ内の SMF に提供されます。

SMF は、サブスクライブされた QoS パラメータを保存し、SM ポリシーの関連付けの確立手順中にこれを PCF に送信します。

## QoS 交渉力

SMF は、*3GPP TS 23.502*、セクション *4.16.4*で定義されているポリシーの関連付けの確立手順を開始することにより、PCF と QoS をネゴシエートします。サブスクリプションから受信した sessionAMBR および 5gQosProfile のパラメータは、PCF への Npcf_SMPolicyControl_Create 要求に含まれます。PCF からの応答には、次のものが含まれる場合があります。

- セッションルール：セッションルールは、PDUセッションに関連付けられているポリシー情報要素で構成されます。QoS 関連情報は、承認されたセッション AMBR および承認されたデフォルト QoS です。
  - ポリシーの課金と制御（PCC）ルール：PCC ルールには、FlowDescription、FlowDirection、および RefQosData パラメータが含まれます。PCF からの応答に 1 つ以上の PCC ルールが含まれている場合があります。
    - FlowDescription：このパラメータには、IP フローのパケット フィルタが含まれます。IP PDU セッション タイプの場合、パケット フィルタ セットは、少なくとも次のいずれかの組み合わせに基づいてパケット フィルタリングをサポートします。

      ：送信元/宛先 IP アドレスまたは IPv6 プレフィックス

      ：送信元/宛先ポート番号

      ：IP/Next ヘッダー タイプの上のプロトコルのプロトコル ID

      - Type of Service（TOS）（IPv4）/トラフィッククラス（IPv6）とマスク

      ：フロー ラベル（IPv6）

      ：セキュリティ パラメータ インデックス

    - FlowDirection：このパラメータは、ルールを適用する必要があるデータ トラフィックの方向を示します。これは、UPLINK、DOWNLINK、または BIDIRECTIONAL のいずれかです。
    - RefQosData：このパラメータは、この PCC ルールに適用される QoS の説明を参照します。これは、PCF からの応答の QoS 説明エントリの少なくとも 1 つの QosId と一致します。

  - QoS 特性：QoS 特性には、次のパラメータが含まれます。
    - リソース タイプ（GBR、遅延クリティカル GBR、または非 GBR）
    - プライオリティレベル
    - パケット遅延バジェット
    - パケットエラーレート
    - ウィンドウの平均化
    - 最大データ バースト ボリューム（遅延クリティカル GBR リソース タイプのみ）

      PCF からの応答のこの属性は、非標準 5QI 値にのみ使用することを目的としています。標準 5QI 値の場合、特性はすでに *3GPP TS 23.501*、セクション *5.7.4* に定義されています。

  - QoS の説明：[QoS の説明（QoS Description）] パラメータは、次の各パラメータで構成されます。

- 5QI：QoS 特性属性からの標準または非標準
- アップリンクおよびダウンリンク GBR
- アップリンクおよびダウンリンク MBR
- 最大パケット損失レート
- QosId：PCC ルールで参照
- デフォルトの QoS 表示

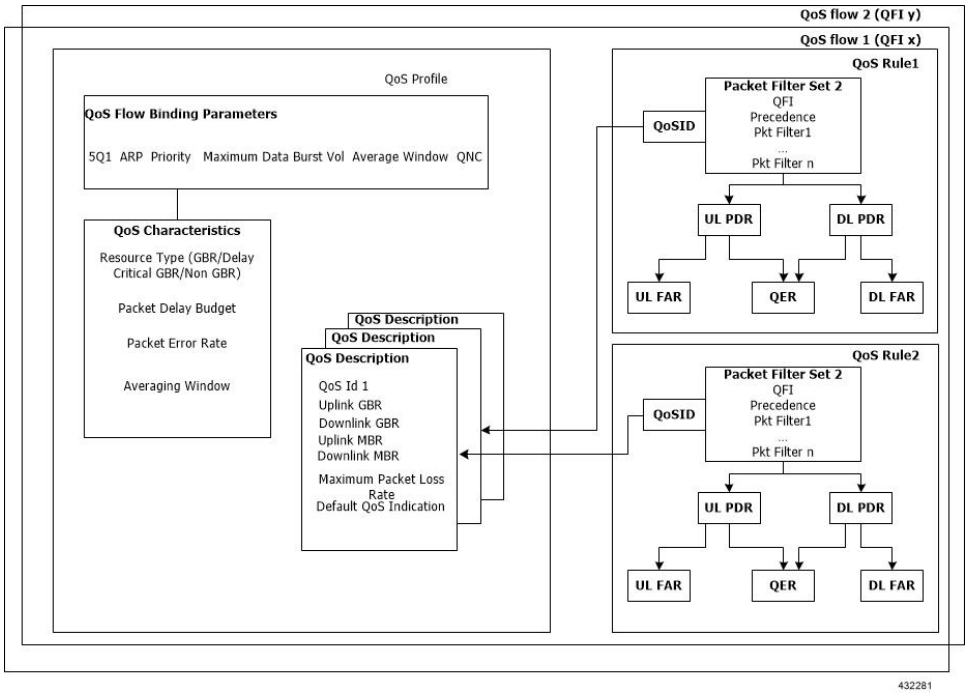
  PCF からの応答に複数の QoS の説明属性が含まれている場合があります。

## QoS フロー管理

Npcf_SMPolicyControl_Create 応答で PCF から受信した情報は、SMF で QoS フローを作成および更新するために使用されます。各 QoS フローには一意の QoS フロー ID（QFI）があり、1 つ以上の PCC ルールが単一の QoS フローにマップされます。

次の図は、SMF で QoS 情報を管理する方法を示しています。

***Figure 215: SMF での QoS 情報管理***




SMF の各 QoS フローは、次の 3 セットの情報の組み合わせです。

- QoS プロファイル：QoS プロファイルには、特定の QoS フローのすべての QoS 属性が保存されます。

- QoS フロー バインディング パラメータと呼ばれる一部の QoS パラメータは、1 つの PDU セッションの 1 つの QoS フローに一意の組み合わせを行います。つまり、PDU セッションでは、これらのパラメータの一意の組み合わせごとに個別の QoS フローを表すことになります。これらのパラメータは、5QI、ARP、優先順位、最大データ バースト ボリューム、平均ウィンドウ、および QNC です。
- QoS フローの QoS プロファイルの 5QI が非標準の場合、リソース タイプ、パケット遅延バジェット、パケット エラー率、平均ウィンドウなどの追加の QoS 特性も QoS プロファイルに保存されます。
- QoS プロファイルは複数の QoS の説明を維持し、それぞれが特定の PDU セッションに固有の QoSId を持ちます。各 QoS 説明には、アップリンクとダウンリンクの GBR、アップリンクとダウンリンクの MBR、最大パケット損失率、およびデフォルトの QoS 表示が含まれています。

- QoS ルール：QoS ルールは、QoS フローの QoS プロファイル内の特定の QoS の説明に関連付けられているパケット フィルタのコレクションです。パケット フィルタは、PCF からの Npcf_SMPolicyControl_Create 応答の PCC ルールで受信したフロー記述に直接マッピングされます。QoS ルールには、そのルールが関連付けられている QoS の説明の QoSId への参照が含まれています。
- PDR：各 QoS ルールは、UPF に送信される 2 つのパケット検出ルール（PDR）にマッピングされます。1 つの PDR はアップリンク方向用で、もう 1 つの PDR はダウンリンク方向用です。PDR マップ内のパケット検出情報（PDI）属性でのサービス データ フロー（SDF）フィルタは、QoS ルールのパケット フィルタをマップします。各 PDR は、SDF フィルタに一致するパケットの転送アクションを決定する転送アクション ルール（FAR）にマッピングされます。各 PDR は、QoS 情報を伝送する QoS 適用ルール（QER）にも関連付けられ、QoS ルールに関連付けられた QoS の説明にマッピングされます。

## 3GPP インターフェイスでの QoS 通信

ネゴシエートされた QoS は主に UE（NAS プロトコルを使用した N1 インターフェイス）、gNB（NGAP プロトコルを使用した N2 インターフェイス）、および UPF（PFCP プロトコルを使用した N4 インターフェイス）と通信する必要があります。

- N1 Interface：N1 インターフェイスでは、AMF を介して UE と SMF の間でセッション管理メッセージが交換されます。NAS メッセージは N1 コンテナにエンコードされ、SMF に送信されるか、SMF から受信されます。
  - UE に送信する必要があるネゴシエート済みおよび認可済み QoS 関連情報はすべて、PDU セッションの確立時に、N1 コンテナ内の PDU SESSION ESTABLISH ACCEPT メッセージの認可 QoS ルールおよびセッション AMBR 属性で見つかります（*3GPP TS 24.501*、セクション *8.3.2* を参照）。
  - UE からの PDU セッション変更要求メッセージには、UE が開始した QoS 変更中に要求された QoS ルールが含まれています。

- 認定 QoS ルールとセッション AMBR 属性は、PCF/SMF によって開始された QoS 変更中に SMF から UE に送信される PDU セッション変更コマンドメッセージにも存在します。
- QoS ルール NAS 属性の形式は 、*3GPP TS 24.501*、セクション *9.10.4.9*に定義されています。この属性は主に、パケット フィルタ リスト、QFI、および QoS パラメータ（個々の QoS ルール ベース）で構成されます。この情報は、QoS フロー内の QoS ルールで使用できます。

- N2 インターフェイス： N2 インターフェイスでは、SMF は AMF を介して N2 コンテナを gNB に送信します。N2 コンテナは ASN.1 エンコードデータであり、NGAP メッセージの特定の情報要素で構成されています。gNB へのすべての QoS 関連情報はエンコードされ、N2 コンテナで SMF との間で送受信されます。AMF から gNB に IE を最終的に伝送する NGAP IE および対応する NGAP メッセージは 、*3GPP TS 29.502*、セクション *6.1.6.4.3*に記載されています。
  - PDUセッションのセットアップ中に、SMFはPDUセッション再送信元セットアップ要求転送IEのN2コンテナでN1N2MessageTransferをAMFに送信します。この IE には、PDU セッション集約最大ビットレートと QoS フロー設定要求リストが含まれています。QoS フロー設定要求リストには、QoS フローレベルの QoS パラメータ（GBR フロー情報、5QI など）が含まれます。これらは 、*3GPP TS 38.413*、セクション *9.3.1*で定義されています。
  - 同様の情報（QoS フローレベルの QoS パラメータ）も、PCF/SMF によって開始された QoS 変更手順中に、N2 コンテナの PDU セッションリソース変更要求転送 IE で SMF によって送信されます。

    SMF で N2 コンテナを作成するために必要な情報は、前のセクションで説明したように、QoS フローの QoS プロファイルにあります。

- [N4 インターフェイス（N4 Interface）]： N4 インターフェイスでは、SMF は QoS 情報をパケット検出ルール（PDR）、転送アクションルール（FAR）、および QoS 適用ルール（QER）の形式で送信します。
  - PDR には、PDI IE の SDF フィルタが含まれます。これらの SDF フィルタは、QoS フローの QoS ルールで設定されたパケットフィルタです。
  - QER には、QoS ルールが関連付けられている QoS の説明に従って、QoS パラメータが含まれています。

    PDR、FAR、QER の内容は 、*3GPP TS 29.244*で定義されています。

## QoS 変更内容

QoS の変更により、次のシナリオのいずれかが発生する可能性があります：

- QoS フローの追加：UE が開始した変更、または PCF が開始した QoS の変更のいずれかとして、ネゴシエートされた QoS を PCF から受信するたびに、SMF は受信した QoS フロー バインド パラメータ（5QI、ARP、優先順位、最大データ バースト ボリューム、QNC）

を抽出します。フロー バインディング パラメータの受信の組み合わせを持つ QoS フローがない場合、SMF は新しい QoS フローを追加し、受信した PCC ルールは新しい QoS フローに対してマッピングされます。その結果、新しい QoS フロー ルール/QoS の説明/PDR/QER が作成され、対応するインターフェイス（N1、N2、および N4）が新しいフローの作成によって更新されます。

- QoS フロー変更：UE が開始した変更、または PCF が開始した QoS の変更のいずれかとして、ネゴシエートされた QoS を PCF から受信するたびに、SMF は受信した QoS フロー バインディング パラメータ（5QI、ARP、優先順位、最大データ バースト ボリューム、QNC）を抽出します。バインディング パラメータの組み合わせが同じ QoS フローがある場合、その QoS フローの QoS プロファイル、QoS ルール、PDR、および QER が N1、N2、および N4 インターフェイスで更新されます。

## PCF および SMF 相互作用の QoS 機能のサポート

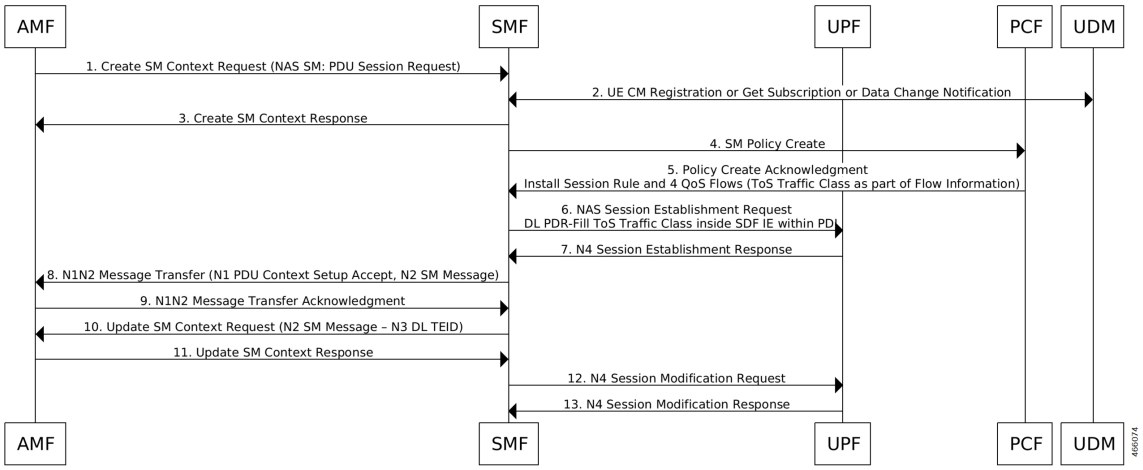
SMF は、PCF との相互作用中に、Diff-Serv-Code-Point（DSCP）またはタイプオブサービス（ToS）QoS 機能をサポートします。SMF で定義されたトラフィックは、SMF が PCF から受信する `tosTrafficClass` 値に基づいて優先順位を付けることができます。指定された ToS 値を使用して、UPF はダウンリンク方向で DSCP パケット マッチングを実行し、UE はアップリンク方向で DSCP パケット マッチングを実行します。この機能により、`FlowDescription` 値が存在しない場合でも、ToS 値を使用したパケット照合が可能です。

次の機能により、この機能が有効になります。

- PCF は、PCF からの PCC ルール内の `FlowInformation` の一部である `sTrafficClass` IE をに送信します。SMF はそれをデコードし、それぞれの QoS フローの一部として保存します。
- SMF は、ダウンリンク PDR の作成中に、PDI 内の SDF IE 内の `tosTrafficClass` で PCF から受信した `tosTrafficClass` IE 値を入力します。
- UE への `tosTrafficClass` をサポートします。

次のコール フローでは、`tosTrafficClass` IE をサポートするための PCF から SMF へのフローについて説明します。

図 *216 :* サポート *tosTrafficClass IE* へのコール フロー




- 最小限の機能をサポートする基本的な PCF を展開できます。PCF はノースバウンド インターフェイスをサポートする必要がなく、ローカル構成に基づいた専用フローがインストールされます。
- UE は、データ、音声、およびビデオをサポートする単一のセッション（デフォルトのベアラー）のみを作成します。PCF は、PDU セッションの作成時に 4 つのフローをトリガします。1 つずつ、音声、ビデオ、データ、ネットワーク管理用です。
- ローカル構成に基づいた PCF は、N7 作成応答で `sTrafficClass` IE に伝送される `FlowInformation` をそれぞれ含む 4 つの PCC ルールを送信します。
- SMF は、`tosTrafficClass` のみを持ち、 `FlowDescription` を 持たない `FlowInformation`にマッピングされた PCC ルールのフロー作成をサポートします。
- PCF は、`any から any への IP の許可`、または `any から any への IP の許可`など、フィルタを使用して `FlowInformation` 内に `FlowDescription` を含めることができます。
- PCF は、関連付けられた QCI を示す各 pcc ルールの `smPolicyDecision` に QoS データを含みます。SMF は QCI ごとに QoS フローを作成します。
- SMF は、 `sTrafficClass` にマップされた PCF からルールをインストールする際に、`N4SessionEstablishmentReq` のダウンリンク PDR の SDF IE 内に `tosTrafficClass`を UPF に含めます。
- SMF は PCF に N1 PDU 確立応答を送信します。この応答には、PCF から受信した情報に基づいて、サービス タイプまたはトラフィック クラス タイプで構成されたパケット フィルタを含む QoS ルールなどの詳細が含まれています。SMF が PCF からフロー方向を受信しない場合、パケット フィルタの方向は双方向として入力され、パケット フィルタ コンポーネント タイプ識別子は `[タイプオブサービス（Type of service）]` または `[トラフィック クラス タイプ（Traffic class type）]`として入力されます。

（注） `FlowDirection` はオプションのパラメータで、そのデフォルト値は**`bidirectional`**です。

# ビットレートマッピングのサポート

## 機能説明

### 5G コアネットワークのビットレートマッピングのサポート

SMF は PCF からアップリンク トラフィックとダウンリンク トラフィックの QoS 値（ビット/秒（bps））を受信します。

GTPv2インターフェイス以外のインターフェイスがアクセスポイント名の集約最大ビット レート（APN-AMBR）を送信すると、SMF は受信した値をキロビット/秒（kbps）に変換します。この変換により、小数部分が最も近い整数（フロア値）に切り捨てられ、その結果、情報が失われます。

帯域幅損失を最小限に抑えるために、CLI コマンド **bitrates rounded-up** が導入され、小数の QoS 値の上限値またはフロア値への丸めを制御します。この動作は、3GPP 29.274 仕様のバージョン 12 に準拠しています。CLI コマンドが **profile network-element pcf** 構成内で有効になっている場合、SMFはN1、N4、S5、またはS8インターフェイスを介して上限値を送信します。

ローミング シナリオでは、SMF が hSMF として機能し、ビット レート マッピングのサポート機能が有効になっている場合、hSMF はN16およびN4経由で、qosFlowDescription で丸められたビット レートを送信します。

SMF がvSMF として機能し、この機能が有効になっている場合、vSMF はN16インターフェイスを介して受信した qosFlowDescription を転送し、N1 および N4 インターフェイスを介して送信する前にセッション AMBR 値を切り上げます。

（注） vSMF は PCF と通信しません。この機能をサポートするには、vSMF に機能を有効にして構成された network-element-profiles pcf が必要です。

（注） **bitrates rounded-up** コマンドは、ローミングと非ローミングの両方のシナリオに適用できます。

デフォルトでは、SMF は変換中にビット レートをフロア値に丸めます。

この機能は、次の手順に影響します：

- 5G セッションの確立

- 専用ベアラーによる 4G セッション確立
- WiFi コールの確立
- ハンドオーバー シナリオ
  - NR から Wi-Fi
  - Wi-Fi から NR
  - Wi-Fi から 4G
  - 4G から Wi-Fi
  - 4G から NR
  - NR から 4G
- 異なるデータ ネットワーク名（DNN）による PDU セッションの確立

**重要** PCF が 4.2 Gbps を超えるビット レートで応答する場合、SMF は、4G 対応 UE のデュアル接続新規無線（DCNR）が無効になっている場合にのみ、ビット レートを 4.2 Gbps に制限します。

# 機能の仕組み

この機能は **bitrates rounded-up** 、 CLI コマンドが **profile network-element pcf** 構成内で有効になっている場合にのみ機能します。この機能を有効にすると、SMF は QoS 値を切り上げます。

たとえば、SMF が N7 インターフェイス上で 123,456 bps のビットレートを受信した場合、123,456 bps を 123 kbps に変換し、小数値を失います。この機能を有効にすると、SMF は 123,456 bps を 124 kbps に変換します。

## 標準準拠

この ビット レート マッピング機能は、以下の基準に準拠しています：

- *3GPP TS 29.274*、リリース *12*：*3GPP Evolved Packet System*（*EPS*）、*Evolved General Packet Radio Service*（*GPRS*）*Tunnelling Protocol for Control plane*（*GTPv2-C*）、ステージ *3*

# ビット レート マッピングの構成

ビットレート マッピング機能を有効にするには、次の構成例を使用します。

```
config
  profile network-element pcf profile_name
    bitrates rounded-up
    exit
```

注：

- **profile network-element pcf** *profile_name*：PCF のプロファイル名を指定します。
- **bitrates rounded-up**：このキーワードを構成して、小数の QoS 値を天井値に丸めます。SMF は、目的のネットワーク インターフェイスを介して上限値を送信します。

  デフォルトでは、SMF は変換中にビット レートをフロア値に丸めます。

## 機能の設定の確認

次のコマンドを使用して、ビット レート マッピング機能を確認します。

**show full-configuration profile network-element pcf**

PCF プロファイル内でビット レートの切り上げが有効になっている場合、 **bitrates round-up** という文字列が表示されます。それ以外の場合、文字列は表示されません。

以下の構成は、show コマンドの出力例です。

```
show full-configuration profile network-element pcf
profile network-element pcf pcf1
nf-client-profile PP1
failure-handling-profile FH1
query-params [ dnn ]
rulebase-prefix cbn#
predefined-rule-prefix crn#
bitrates rounded-up
exit
```

# Diameter インターフェイス間のビットレート マッピング

SMF は PCRF からアップリンク トラフィックとダウンリンク トラフィックの QoS 値（ビット/秒（bps））を受信します。

アップリンク用の APN-AMBR とダウンリンク用の APN-AMBR を GTPv2 インターフェイス以外のインターフェイスから受信した場合、SMF はアップリンク用の APN-AMBR とビット/秒単位のダウンリンク値をキロビット/秒に変換します。この変換の結果が小数になった場合、アップリンクの APN-AMBR とダウンリンクの APN-AMBR の値は切り上げられます。

デフォルトでは、構成が構成されていない場合、SMF は変換中にビット レートを CEIL 値に丸めます。

この機能は、次の手順に影響します：

- 4Gセッションの確立
- RAR/CCA-U を介したデフォルトのベアラーの更新

## Diameter インターフェイスとのビット レート マッピングの構成

Diameter インターフェイスと GTPv2 インターフェイス間でビットレート マッピングを有効にするには、次の構成例を使用します。

（注） MBR/GBR/APN-AMBR などの専用ベアラー ビット レート変換にも同じ構成を使用します。

```
config
  profile network-element pcrf profile_name
    bitrates rounded-down
    diameter-client-profile Diameter Client_Profile Name
    subscription-idsubscription-id
    exit
```

注：

- **profile network-element pcrf** *profile_name*：PCRF のプロファイル名を指定します。
- **bitrates rounded-down**：ビット レートの切り捨てを構成します。SMF は、目的のネットワーク インターフェイスを介してフロア値を送信します。

  デフォルトでは、SMF は変換中にビット レートを CEIL 値に丸め、ビット レートは切り上げられます。

# デフォルト ベアラの許可された QoS の処理

## 機能説明

CHF サーバーは PCF と対話して、ユーザー クォータの枯渇を報告します。次に、PCF は SMF に対してポリシー更新要求を開始し、セッションルールの承認されたデフォルトの Quality of Service（QoS）を変更します。QoS は QoS クラス ID（QCI）または 5G QoS インジケータ（5QI）、セッション集約最大ビットレート（AMBR）、または QCI/5QI とセッション AMBR の両方です。

ユーザーのクォータが枯渇するたびに、この QoS の変更によってダウングレードが実行されます。

- セッションのデータ パケットの DSCP マーキング
- セッションの AMBR

クォータを補足すると、PCF はデフォルトのベアラーに対して以前に承認された QoS に戻ります。

デフォルトのフローまたはベアラーの QCI/5QI が変更されるたびに、次の変更に注意してください。

- QCI/5QI 情報は、そのセッションに対して生成されたイベントデータレコード（EDR）で更新されます。次に、SMF は、パケット転送制御プロトコル（PFCP）メッセージを介して更新されたベアラー レベル情報を送信して、EDR 機能をサポートします。

- データ パケットの DSCP マーキングは、デフォルトのベアラーまたはフローに関連するすべてのパケット検出ルール（PDR）で更新されます。
- LI パケットで送信される QCI 情報が更新されます。
- ルールベースの変更および Ruledef のアクティブ化または非アクティブ化は、5QI の変更およびセッション AMBR の変更とともに、予想どおりに機能します。
- 変更された QoS は、課金データ要求（更新）メッセージで CHF に送信されます。また、承認された QoS の QCI/5QI の変更は、課金の QoS 変更トリガーとして扱われ、CDR-U が送信されます。

# 機能の仕組み

このセクションでは、PDU セッションが確立された後に、承認 QoS の QCI/5QI 値の変更をサポートするための SMF の変更について詳しく説明します。

## 4G および Wi-Fi セッションのデフォルトのベアラー QoS 処理

次の手順では、SMF が 4G および Wi-Fi セッションでの承認されたデフォルト QoS の変更を処理する方法について説明します。

1. SMF は、AuthorizedDefaultQoS の変更された QCI/5QI や異なるセッション AMBR 値を持つ PCF から SmPolicyUpdateNotify を受信します。
2. SMF は、デフォルトのベアラーの S-GW に向けてベアラー要求の更新を開始します。
    1. ベアラーの更新要求では、デフォルトのベアラーにベアラー コンテキスト IE が含まれ、対応するベアラー QoS が変更された QCI 値で更新されます。
    2. 4G セッションでは、拡張プロトコル構成オプション（ePCO）がサポートされている場合は、Update Bearer Request メッセージに含まれます。ePCO には、セッションでインターワーキング（IWF）が有効になっている場合、デフォルトフローの更新された QCI 値を含む 5G 認定 QoS フロー情報が含まれます。それ以外の場合、PCO IE は同じ詳細とともに送信されます。
    3. Wi-Fi セッションでは、Update Bearer Request メッセージに追加のプロトコル構成オプション（APCO）が含まれています。APCO には、デフォルトフローの QCI 値が更新された 5G 認定 QoS フロー情報が含まれています。
3. SMF は、S-GW からのベアラー応答の更新を受け入れます。
4. N4 インターフェイスでは、次の変更が行われます。
    1. BearerLvlInfo IE の新しいインスタンスは、デフォルトのベアラートンネルの変更された QCI 値に含まれています。
    2. 更新 PDR は、デフォルトフローの一部であるすべての PDR に送信され、新しい BearerLvlInfo IE との関連付けを反映します。

3. デフォルトフロー内のすべての PDR に関連付けられた FAR は、5QI-DSCP マッピング構成に、変更された 5QI の異なる値がある場合、新しい DSCP マーキング値で更新されます。

## 5G セッションのデフォルト ベアラー QoS 処理

次の手順では、SMF が 5G セッションのデフォルト ベアラの承認済み QoS の変更を処理する方法について説明します。

1. SMF は、AuthorizedDefaultQoS の変更された 5QI や異なるセッション AMBR 値を持つ PCF から SmPolicyUpdateNotify を受信します。
2. SMF は、AMF を使用して N1N2MessageTransfer 手順を開始し、このメッセージで N1 PDU セッション変更コマンドおよび N2 PDU セッションリソース変更要求転送 IE を送信します。
    1. N1 メッセージでは、デフォルト QoS フローが許可された QoS フローの説明 IE で変更され、5QI 値が更新されます。
    2. N1 メッセージでは、デフォルトのベアラの QCI を更新するように、マッピングされた EPS ベアラーコンテキスト IE が変更されます。
    3. N2 メッセージでは、デフォルト フローの QoS フロー レベルの QoS パラメータが変更され、5QI 値が更新されます。
3. SMF は、N1N2Message Transfer メッセージで送信された N1 および N2 要求に対する応答とともに、AMF からの SMContextUpdate 要求を受け入れます。
4. N4 インターフェイスでは、次の変更が行われます。
    1. BearerLvlInfo IE の新しいインスタンスは、変更された 5QI から QFI へのマッピングに含まれています。
    2. 更新 PDR は、デフォルトフローの一部であるすべての PDR に送信され、新しい BearerLvlInfo IE との関連付けを反映します。
    3. デフォルトフロー内のすべての PDR に関連付けられた転送アクション ルール（FAR）は、5QI-DSCP マッピング構成に、変更された 5QI の異なる値がある場合、新しい DSCP マーキング値で更新されます。

## WiFi ハンドオーバー中のデフォルト ベアラー QoS 処理

次の手順では、SMF が Wi-Fi ハンドオーバーおよびその他のハンドオーバー時に、承認されたデフォルトの QoS 変更をどのように処理するかを説明します。

1. SMF は、各引き継ぎ手順の最後に SMPolicy 更新要求を PCF に送信します。たとえば、PCF アームで異なるポリシーがトリガされると、SMF は SMPolicy 更新要求を PCF に送信します。PCF からの応答には、セッション ルール（承認されたデフォルト QoS）で変更された

QCI が含まれています。SMF は、RAN/UE に対する変更手順を開始し、N1、N2、N4、および S5 インターフェイスで同じ情報を伝達します。

2. すべてのハンドオーバー（Wi-Fi-NR/EPS および NR/EPS-WiFi を除く）の場合、SMF は SMPolicy 更新要求を PCF に送信し、RAT タイプの変更を示します。PCF からの応答には、セッション ルール（承認されたデフォルト QoS）で変更された QCI が含まれています。SMF は、RAN/UE に対する変更手順を開始し、N1、N2、N4、および S5 インターフェイスで同じ情報を伝達します。

Wi-Fi を含むハンドオーバーは、他のハンドオーバーとは異なります。SMF は、引き継ぎ後ではなく引き継ぎ中に、PCF に対して SMPolicy 更新要求をトリガします。WiFi を含むハンドオーバーの場合、ターゲット RAN は、更新ではなく、新規としてフローとベアラーをインストールします。SMF は、ハンドオーバー時にデフォルトのフローとベアラーをインストールする際に、PCF からの応答で受信した最新の QCI を送信します。

## 障害処理中のデフォルト ベアラー QoS の変更

5G セッションの場合、デフォルト フローは非 GBR フローであり、QCI/5QI の変更にリソース予約は必要ないため、通常は N1 または N2 インターフェイスでの QCI/5QI の変更は失敗しません。ただし、AMF からの N1 または N2 応答がないために変更手順が失敗した場合、変更はロールバックされ、セッションは古い QCI/5QI およびセッション AMBR 値で続行されます。N2 がフロー変更を拒否すると、デフォルト フローなしではセッションを維持できないため、セッションは削除されます。

4G セッションの場合、デフォルトのベアラーの変更に対するベアラーの更新応答は失敗しません。ただし、ベアラー応答の更新が欠落しているか、または失敗した場合、変更はロールバックされ、セッションは古い 5QI およびセッション AMBR 値で続行されます。

4G と 5G の両方のセッションで、N4 更新が失敗するか、応答が受信されない場合、SMF は UPF 障害処理テンプレートの構成に従ってアクションを実行します。4G および Wi-Fi セッションでは、N4 インターフェイスに障害があると、別のベアラー要求が古い 5QI および AMBR 値とともに S-GW および ePDG に送信されます。

障害処理メカニズムは、PCF によって開始される変更手順でも同じです。

## 制限事項

デフォルトのベアラーに関する認可された QoS の処理機能には、次の制限があります。

- 承認された QoS の QoS フロー バインディング パラメータ（5QI や ARP など）の組み合わせは、専用ベアラーまたはフローと同じになることはありません。つまり、QCI/5QI を変更しても、デフォルト フローのバインディング パラメータが別のフローと類似することはありません。
- SMF は、セッション ルールの割り当て/保持優先順位（ARP）および QCI/5QI（セッション AMBR の有無にかかわらず）を除き、すべてのバインディング パラメータの変更をサポートしていません。

- QCI/5QI が変更されると、既存のデフォルト ベアラー フローが N1、N2、および N4 インターフェイスに向けて変更されます。この場合、SMF は新しいフローを作成する代わりに、既存のフローを削除しません。

## 承認された QoS 処理の OAM サポート

ここでは、この機能の操作、管理、およびメンテナンスに関して説明します。

### 統計情報サポート

SMF は、「SESSRULE_CHANGE」というラベルを維持して、AMBR 値、QCI/5QI 値、または AMBR 値と QCI/5QI 値の両方の組み合わせに対する変更を示します。

# ローカル ポリシーに基づく GBR ベアラーの作成

## 機能説明

最小ビットレート保証が必要な場合は、GBR ベアラーを作成する必要があります。N7 インターフェイスでは、GBR ベアラーは PCF からの要求を受信したときに作成されます。ただし、PCF がない場合、SMF で設定されたローカル ポリシーを使用して、セッションの作成直後に GBR ベアラーを作成できます。

SMF では、4G および 5G RAT のローカル ポリシーに基づいて GBR ベアラーを作成できます。

## 機能の仕組み

このアプローチでは、次の 2 つのベアラーが作成されます：

1. **デフォルトの非 GBR ベアラー**：デフォルトの非 GBR ベアラー/フローは、UDM から受信した QoS または新しい無線（NR）の場合はローカル構成に基づいて作成され、MME から受信した QoS は EUTRA の場合に使用されます。
2. **専用 GBR ベアラー**：専用 GBR フロー/ベアラーは、ローカル ポリシー構成に基づいて追加的に作成されます。

### PCF を使用しないデフォルトの非 GBR ベアラと専用 GBR ベアラーの作成

デフォルトのベアラーとフローを作成するために、ネゴシエートされた QoS プロファイルが選択されます。

- 4G セッションで、N7 インタラクションが無効になっている場合、MME によって提供される QoS が使用されます。
- 5G セッションで N7 と N10 の連携が無効になっている場合、DNN プロファイルに関連付けられているローカル定義の QoS プロファイルが使用されます。

PCF の介入を使用せずに専用ベアラー/フローを作成するには、イベント管理ポリシーが必要です。イベント管理ポリシーとDNNプロファイルの関連付けは、構成を利用して行われます。イベントがトリガされるたびに、その DNN に関連付けられたイベント管理ポリシーが実行されます。イベント管理ポリシーで構成された各イベントポリシーは、イベントおよびルールに基づいて一致が見つかるまで、優先順位の順に実行されます。

新しい構成では、イベント管理ポリシーを定義できます。複数の優先順位ベースのイベント処理ポリシーをイベント管理ポリシー下で構成できます。構成された各イベントポリシーは、イベントとルールに基づいて一致が検索されるまで、優先順位の高い順に実行されます。

NR の場合、専用およびデフォルトのフロー パラメータは、N1 PDU セッション確立承認で UE に、N2 セットアップ要求で gNB に送信されます。E-UTRA の場合、デフォルトベアラーの作成はセッション作成応答の一部として実行され、GBR 専用ベアラーはセッション応答の作成送信直後にベアラー要求の作成（CBR）をトリガーすることによって作成されます。これは、SMF ですでにサポートされている PCF によってトリガーされるピギーバックされた CBR に似ています。

（注） この機能は、CBR と CSR 応答が同じメッセージで送信される実際のピギーバック CBR をサポートしていません。

## 専用GBRベアラーの作成による5G接続

次のコール フローは、専用 GBR ベアラーの作成による 5G 接続のプロセスを示しています：

図 *217 :* 専用 *GBR* ベアラーを作成した *5G* 接続のコール フロー（*PCF* インタラクションなし）

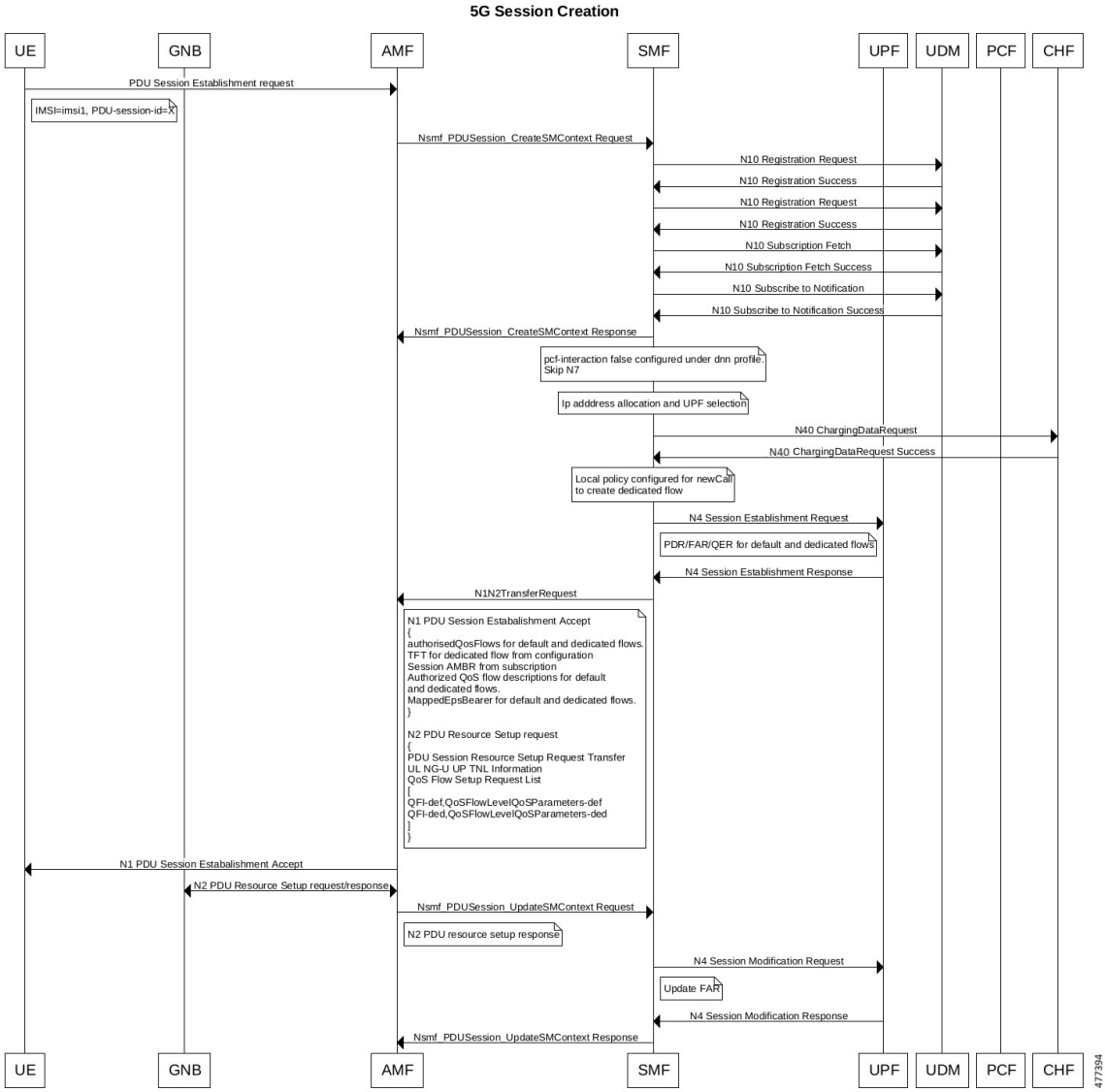



表 *391 :* 専用 *GBR* ベアラーを作成した *5G* 接続のコール フローの説明（*PCF* 連携なし）

| ステップ | 説明 |
|---|---|
| 1. | UE は、N1 SM コンテナ内の PDU セッション確立要求を含む NAS メッセージを AMF に送信することで PDU セッション確立手順を開始します。PDU セッション確立要求には、PDU セッション ID と IMSI が含まれます。 |
| 2. | AMF が、UE によって提供された PDU セッション ID の SMF との関連付けを持っていない場合、AMF は Nsmf_PDUSession_CreateSMContext 要求を呼び出します。AMF は、UE から受信した PDU セッション確立要求を含む N1 SM コンテナとともに PDU セッション ID を転送します。 |

| ステップ | 説明 |
|---|---|
| 3. | SMF は、N10 登録要求を UDM に送信します。次に、UDM は、N10 の登録応答を SMF に送信します。 |
| 4. | SMF は、N10 サブスクリプションフェッチ要求を UDM に送信します。その後、UDM は SMF に N10 サブスクリプション取得応答を送信します。 |
| 5. | SMF は、N10 サブスクライブ通知要求を UDM に送信します。次に、UDM は、通知成功の応答に N10 サブスクライブを SMF に送信します。 |
| 6. | SMF が PDU セッション確立要求を処理できる場合、SMF は SM コンテキストを作成します。次に、SMF は、Nsmf PDU Session CreateSMContext Response を AMF に送信します。<br>PCF が展開されていない場合は、SMF で **pcf-interaction false を** 構成する必要があります。したがって、SMF はローカル構成を適用して、PCC ルールと 5G QoS パラメータのマッピングを実行します。<br>この段階で、SMF は 1 つ以上の UPF も選択します。 |
| 7. | （オプション）SMF は N40 インターフェイス経由で CHF に課金データ要求を送信します。次に、CHF は N40 ChargingDataRequest 成功応答で SMF に応答します。 |
| 8. | この段階で、ローカルポリシーを使用して新しいコールを構成し、専用フローを作成します。<br>事前定義されたルールが専用フロー/ベアラーにマッピングされている場合、SMF は N4 セッション確立要求を UPF に送信します。SMF は、デフォルト フローと専用フローの両方の PDR/FAR/QER/URR 要求の作成も UPF に送信します。 |
| 9 です。 | UPF は N4 セッション確立応答で SMF に応答します。 |
| 10. | SMF は、NamefCommunication N1N2 メッセージ転送要求を AMF に送信します。このメッセージには、デフォルト フローと専用フローの両方に対する承認された QoS フロー、構成からの専用ベアラの TFT、サブスクリプションからのセッション AMBR、デフォルトと専用フローの承認された QoS フローの説明、デフォルトと専用フローにマッピングされた EPS ベアラーを含む N1 PDU セッション確立の承認が含まれます。<br>NamefCommunication N1N2 メッセージ転送要求には、PDU セッション リソース設定要求転送、UL NG-U UP TNL 情報、および QoS フロー設定要求リストを含む N2 PDU リソース設定要求も含まれます。 |
| 11 . | N1 PDU セッション確立承認は、AMF から UE に送信されます。 |
| 12. | N2 PDU リソース セットアップ要求が AMF から gNB に送信されます。応答として、gNBはN2 PDUリソース設定応答をAMFに送信します。 |

| ステップ | 説明 |
|---|---|
| 13. | AMF は、Nsmf PDU Session UpdateSMContext 要求（N2 PDU Resource Setup 応答）を SMF に送信します。このメッセージには、N2 PDU リソースのセットアップ要求が含まれています。 |
| 14. | SMF は、N4 セッション変更要求を UPF に送信します。この要求は、GNB トンネル情報を使用して FAR を更新することです。 |
| 15. | UPF が SMF に N4 セッション変更応答を送信します。 |
| 16. | SMF は、Nsmf PDU セッション UpdateSMContext 応答を AMF に送信します。 |

## 専用 GBR ベアラーの作成による 4G 接続

専用 GBR ベアラーを作成した 4G 接続のプロセスは、次の手順に従います：

**図 *218* : 専用 *GBR* ベアラーの作成による *4G* 接続のコール フロー**

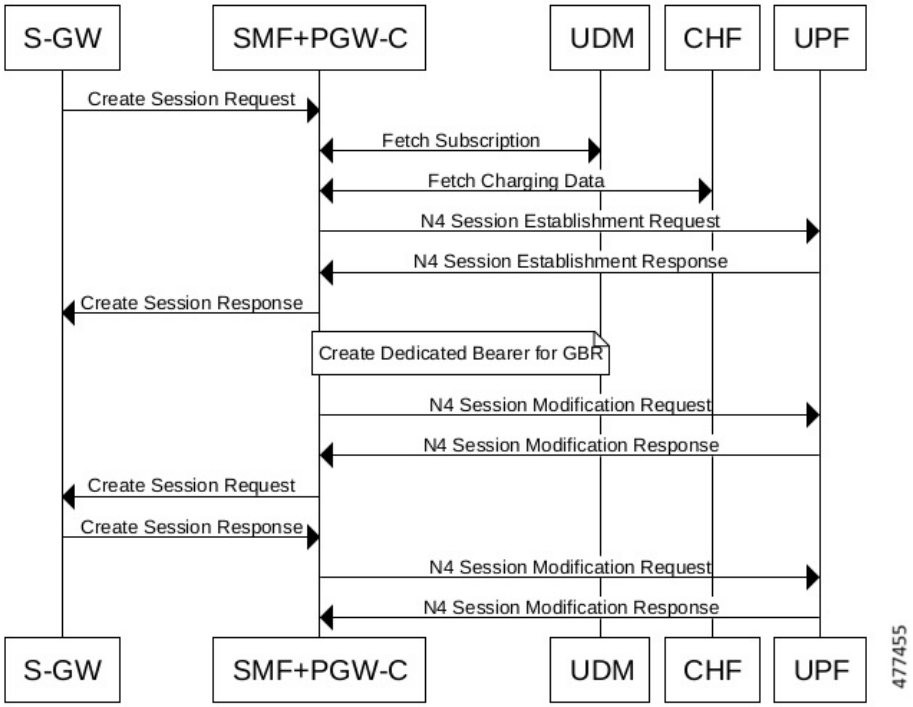



**表 *392* : 専用 *GBR* ベアラーの作成による *4G* 接続のコール フローの説明**

| ステップ | 説明 |
|---|---|
| 1. | S-GW は SMF にセッション要求の作成を送信します。 |

| ステップ | 説明 |
|---|---|
| 2. | SMFはサブスクリプション取得要求をUDMに送信します。その後、UDM はサブスクリプション取得応答を SMF に送信します。 |
| 3. | SMF は課金データ要求を CHF に送信します。その後、CHF は N40 課金データ応答を SMF に送信します。 |
| 4. | SMF は、N4 セッション確立要求を UPF に送信します。 |
| 5. | トンネルの作成後、UPF は N4 セッション確立応答を SMF に送信します。 |
| 6. | SMF は、セッション応答の作成を S-GW に送信します。この応答には、4G デフォルト ベアラー トンネル情報を含みます。 |
| 7. | 専用 GBR ベアラーの作成は、ローカル ポリシーの構成に基づいて開始されます。この段階で、SMF は N4 セッション変更要求を UPF に送信します。このメッセージには、専用 GBR ベアラーの作成要求が含まれています。 |
| 8. | UPF が SMF に N4 セッション変更応答を送信します。 |
| 9 です。 | SMF は、S-GWにベアラー作成要求を送信します。<br>この要求には、QOS、TFT、および UPF FTEID に関する情報を含むベアラー コンテキスト リストに関する情報が含まれています。 |
| 10. | SGW は、SMF にベアラー応答の作成を送信します。応答には、要求を受け入れたか、要求を部分的に受け入れたか、およびベアラー コンテキストの詳細が含まれます。 |
| 11 . | SMF は、N4 セッション変更要求を UPF に送信します。この要求は、各ベアラーの SGW-U トンネル情報で FAR を更新することです。 |
| 12. | UPF は SMF への N4 セッション変更応答で応答し、ベアラーは SMF で確立されます。 |

## 制限事項

この機能には次の既知の制限事項があります。

- この機能は、PCRF なしではなく、PCF なしの 4G コールをサポートしています。

# PCF を使用せずにデフォルトの非 GBR ベアラと専用 GBR ベアラを作成するための設定

デフォルトの非 GBR ベアラーと専用 GBR ベアラーを作成するには、次の段階的な設定が必要です。

1. QoS プロファイルとイベント管理ポリシーを DNN プロファイルに関連付けます。この構成には、新しい CLI が導入されています。
2. デフォルトのフロー/ベアラーの QoS 構成を作成します。これは既存の構成です。詳細については、「QoS パラメータの構成」を参照してください。
3. 優先順位、実行するイベント、ルール、および（ルールの一致がある場合に）実行するアクションを定義することによって、イベント管理構成を追加します。
4. ルールの条件を指定して、ルール定義ポリシーを追加します。
5. アクション定義ポリシーを追加します。アクションは、ルールベースをアクティブ化して GBRベアラー/フローを作成することになります。
6. ルールベース、事前定義されたルール、課金アクションを構成します。これは既存の構成です。詳細については、ACS 構成モードで ACS ルールベースの構成を参照します。
7. 専用ベアラ/フロー QCI/ARP ごとに QoS を構成します。これは既存の構成です。詳細については、「帯域幅 ID の構成」を参照してください。

## QoS プロファイルとイベント管理ポリシーを DNN プロファイルに関連付ける構成

QoS プロファイルとイベント管理ポリシーの DNN プロファイルへの関連付けは、次の構成で行うことができます。

```
config
  profile dnn dnn_profile_name
    qos-profile qos_profile_name
    eventmgmt-policy eventmgmt_policy_name
    exit
```

注：

- **eventmgmt-policy** *eventmgmt_policy_name*：この CLI では、DNN に関連付けられた優先順位ベースのイベント処理を構成できます。 **eventmgmt-policy** で構成された各イベント ポリシーは、イベントおよびルールに基づいて一致が見つかるまで、優先順位順に実行されます。
- **qos-profile** *qos_profile_name*：この CLI を使用すると、QoS プロファイルとイベント管理ポリシーを DNN プロファイルに関連付けることができます。この QoS プロファイルは、UDM が提供しない場合、5G のデフォルト フローの QoS 値を読み取るために使用されます。

## イベント管理ポリシーを追加するための構成

イベント管理ポリシーの追加は、次の構成によって行われます。

```
config
  policy eventmgmt policy_eventmgmt_name
    priority event_priority [ event event_name ] ruledef ruledef_name actiondef
 actiondef_name
    exit
```

注：

- **eventmgmt** *policy_eventmgmt_name*：この CLI では、イベント管理ポリシーを構成し、属性を定義できます。
- **priority** *event_priority*：特定のイベント管理ポリシーの優先順位を定義できます。
- **event** *event_name*：特定のアクションが実行されるイベントを定義するオプションの CLI です。イベント名として **new-call** のみをサポートします。セマンティックおよびシンタックス エラー処理シナリオでは、イベント名として **cbr-resp** がサポートされます。

  **event** が構成されていない場合、ルールが一致すると、すべての定義済みイベントに対して **actiondef** が実行されます。
- **ruledef** *ruledef_name*：一致した場合にアクションを実行するローカル ポリシーのルールを定義します。
- **actiondef** *actiondef_name*：実行されるアクション名を構成します。

## ルール定義ポリシーを追加するための構成

次の構成では、ルール定義ポリシーを追加できます：

```
config
  policy rulemgmt policy_rulemgmt_name
    ruledef rule_def condition condition_string
    exit
```

- **rulemgmt** *policy_rulemgmt_name*：ポリシーに追加するルールを定義します。
- **ruledef** *rule_def*：ルール属性を構成します。ruledef は、条件が一致したときに宣言されます。
- **condition** *condition_string*：ルールの使用例を定義します。 **any** および **cause matches “cause”** 条件のみサポートしています。

## アクション定義ポリシーを追加するための構成

次の構成では、アクション定義ポリシーを追加します：

```
config
  policy actionmgmt policy_actionmgmt_name
    actiondef actiondef_name
      priority priority_number action action_name [ attributes { rulebase
rulebase_name [ rules rules_name ] } ]
      exit
```

注：

- **actionmgmt** *policy_actionmgmt_name*：実行されるアクションを構成します。
- **actiondef** *actiondef_name*：実行されるアクション属性を定義します。現在、アクションとして **activate-rulebase** のみがサポートされています。

意味的および構文エラーの処理では、UE が 4G または 5G RAT にある場合のアクションは異なります。

- **priority** *priority_number*：アクションが実行される優先順位を定義します。
- **action** *action_name*：actiondef に関連付けられたアクションを優先順に定義します。GBR の作成が失敗した場合、SMF は **release-session** アクションをサポートします。
- **attributes** ：特定のアクションの属性を定義します。これは任意のコマンドです。
- **rulebase** *rulebase_name*：フローと一致させるプロトコルルールのコレクションと、フローと一致するために実行する関連アクションを定義します。
- **rules** *rules_name*：実行されるルールのリストを定義します。

（注） 課金アクション、帯域幅ポリシー、およびパケットフィルタの既存の構成が、各ルールの QoS パラメータの構成に使用されます。

# 設定例

次に、QoS プロファイルとイベント管理ポリシーを DNN プロファイルに関連付ける設定例を示します。

```
config
profile dnn dnnprof-data
qos-profile qos camera_profile
eventmgmt-policy emp
end
```

次のサンプル構成では、イベント管理ポリシーを追加します：

```
policy eventmgmt emp
 priority 1 event new-call ruledef rd1 actiondef ad1
end
```

次に、 **any** および **cause matches “cause”** ルール定義ポリシーを追加するための構成例を示します。

```
policy rulemgmt rm1
  ruledef rd1
    condition “any”
    end
```

```
policy rulemgmt rm1
ruledef rd1
condition cause matches [ 83 ] source ue
```

アクション定義ポリシーを追加するための構成例を次に示します：

```
policy actionmgmt am1
  actiondef ad1
    priority 1 action activate-rulebase  attributes rulebase rb1 rules [r1,r2]
    exit
end
```

```
active-charging service olympics
rulebase rb1
bandwidth default-policy bw_policy1
action priority 1 dynamic-only ruledef r1 charging-action ca1
action priority 2 dynamic-only ruledef r2 charging-action ca2
exit

charging-action ca1
allocation-retention-priority 1
qos-class-identifier 6
tft packet-filter tft1
flow limit-for-bandwidth id 1
end

packet-filter tft1
direction bi-directional
ip protocol 6
ip remote-port range start 1002 end 1005
end

active-charging service acs1
bandwidth-policy bw_policy1
flow limit-for-bandwidth id 1 group-id 1
group-id 1 direction uplink peak-data-rate 1000000000 peak-burst-size 100 violate-action
 discard committed-data-rate 1000 committed-burst-size 100 exceed-action discard
group-id 1 direction downlink peak-data-rate 2000000000 peak-burst-size 100 violate-action
 discard committed-data-rate 1000 committed-burst-size 100 exceed-action discard
```

専用ベアラーの作成が失敗した場合の処理のために、次の構成を行うことを推奨します：

```
policy eventmgmt emp
  priority 2 event cb-resp ruledef rd3 actiondef ad3
      exit

policy rulemgmt rm1
      ruledef rd3
               condition cause matches “cause”
            exit
     exit

policy actionmgmt am1
      actiondef ad3
priority 1 action release-session
            exit
exit
```

# OAM サポート

このセクションでは、この機能でサポートされているメトリックスと統計について説明します。

## メトリック

この機能の一部として、次のラベルが **smf_service_stats** に追加されています。

- **policy_status**：このメトリックは、構成されているローカル ポリシーに関連付けられます。

# UPF での EDR 生成の SMF トリガーされたメタデータ

SMF は、EDR の生成を可能にするために、次のメタデータをユーザー プレーン機能（UPF）に提供します。

- Called-Station-ID：セッションの DNN を指定します
- Calling-Station-ID：UE の電話番号を指定します。
- RATタイプ（RAT Type）：現在のセッションの RAT タイプ（NR または EUTRAN）
- ULI：現在のセッションのユーザーの場所

UPF は、PFCP セッション確立要求メッセージの「サブスクライバパラメータ」IE で先行データを受け取ります。RAT タイプと ULI は、セッションの存続期間中に変更される場合があります（5G から 4G へのハンドオーバーなどのイベントの場合）。UPF は、PFCP セッション変更要求メッセージでこれらのパラメータの変更された値を受信します。

**Note**

- EDR 構成が使用可能かどうかに関係なく、すべてのパラメータは常に SMF から UPF に送信されます。これらのパラメータを使用すると、セッション作成後の設定変更がただちに UPF に適用されます。
- SMF は、EDR 関連の構成をサポートしています。しかし、SMF では、その機能のこれらの構成は必要ありません。これらの構成は、UPF に送信されます。

UPF EDR の詳細については、『*UCC 5G UPF* 構成および管理ガイド』を参照してください。

# 構成の動的な更新

## 機能説明

SMF では、SMF プロファイルおよびSMF サービス プロファイルの構成をダイナミックに変更できます。

特定の SMF プロファイルまたはサービス プロファイルの構成パラメータを変更するには、次のメンテナンス操作手順を実行する必要があります。このメンテナンス操作手順は、新しいセッションを拒否してシステムに影響を与えないように、SMF システムをメンテナンス モードに保つのに役立ちます。また、このメンテナンス手順により、オペレータは**clear subscriber all** コマンドを実行してサブスクライバを手動でクリアできるようになります。

SMF は、PUT メソッドを使用して「NFUPdate」を送信することで、構成パラメータの変更を NRF に更新します。

# 機能の仕組み

ここでは、メンテナンス操作手順と、サポートされている SMF 構成の動的な構成変更の仕組みについて説明します。

### メンテナンス運用の手順

必須の運用保守を必要とする構成パラメータの変更については、次の手順を実行します。

1. SMF プロファイルで **mode offline** CLI コマンドを実行して SMF をシャットダウン（オフライン）します。

   SMF は、メソッド PUT と NFStatus を「UNDISCOVERABLE」として NFUpdate を送信します。

（注） オンラインからオフラインへの移行期間中、SMF はどの新しい要求も受け入れません。

2. **clear subscriber sess all** CLI コマンドを使用してセッションをクリーンアップします。
3. 構成を変更し、**mode offline** CLI コマンドを削除します。

   SMF は、メソッド PUT と NFStatus を "Registered" として指定して NFUpdate を送信します。

### SMF プロファイルと SMF サービス プロファイル

次の表では、サポートされている SMF 構成に対する構成のダイナミックな変更がどのように機能するかを示します。

表 *393 : SMF* プロファイルおよび *SMF* サービス プロファイルの動的な変更

| 設定パラメータ | ダイナミックな変更 | 既存のセッションへの影響 | NRF の更新 | メンテナンス運用の手順 |
|---|---|---|---|---|
| locality | 許可 | セッションは新しい値を使用して開始されます。 | 不要 | 必須 |
| node-id | N/A | 影響なし | N/A | N/A |
| fqdn | 許可 | SMF は、UDM との対話中に常にセッションの最新の FQDN 値を取得します。 | 必須 | 必須 |
| allowed-nssai | 許可 | セッションは新しい値を使用して開始されます。 | 必須 | 必須 |

| 設定パラメータ | ダイナミックな変更 | 既存のセッションへの影響 | NRF の更新 | メンテナンス運用の手順 |
|---|---|---|---|---|
| plmn-id | 許可 | セッションは新しい値を使用して開始されます。 | 必須 | 必須 |
| サービス名、スキーマ、サービス ID、バージョン | 許可 | セッションは新しい値を使用して開始されます。 | 必須 | 必須 |
| http-endpoint | 許可 | セッションは新しい値を使用して開始されます。 | 必須 | 必須 |
| icmpv6-profile | 許可 | セッションは新しい値を使用して開始されます。 | 不要 | 不要 |
| compliance-profile | 許可 | SMF は、さまざまな SBI インターフェイスの SMF と他の NF 間の非互換性の問題により、解析の失敗を実行する場合があります。 | 不要 | 不要 |
| access-profile | 許可 | セッションは新しい値を使用して開始されます。 | 不要 | 不要 |
| subscriber-policy | 許可 | セッションは新しい値を使用して開始されます。 | 不要 | 不要 |

# 動的な構成変更のサポートの構成

SMF プロファイルでオフライン動作モードを有効にするには、次の設定例を使用します。

```
config
  profile smf profile_name
    mode offline
    exit
```

注：

- **mode**：動作モードを指定します。
- **offline**：モードをオフラインに指定し、新しいセッションを拒否します。

## 動的な構成変更のサポート構成の確認

この機能が有効になっているかどうかを確認するには、**show running-config profile smf** CLI コマンドを使用します。有効にすると、show コマンド出力の一部として次のフィールドが表示されます。

- mode offline

# ダイナミック PCC ルールの適用

## 機能説明

SMF は、ポリシー制御機能（PCF）のポリシーおよび課金制御（PCC）ルール、またはローカルに構成されたポリシー ルールのいずれかを使用して、ポリシー管理を制御します。PCF は、該当する QoS および課金情報とともに PCC ルールを SMF に送信します。SMF はこの情報を使用して QoS フローを定義し、QoS の適用（UPF 経由）と CHF に対する課金を適用します。

PCC ルールは、ローカルで構成することもできます。ローカルで構成されたポリシー ルールは、静的または、定義済みルールとしてラベルされます。

次のセクションでは、ダイナミックなポリシー管理のために実装されている機能について説明します。

### サポートされる機能の交渉

SMF と PCF は、ポリシー コンテキストの作成中および PDU セッションの確立中に、サポートされている機能を交渉します。交渉された機能に基づいて、PCF は関連情報を提供します。

次の表は、3GPP 仕様 29.512 で定義されているネゴシエート可能な機能を示しています。

***Table 394:*** サポートされるネゴシエートされた機能

| 機能番号 | 機能名 | 説明 |
|---|---|---|
| 1 | TSC | この機能は、（S）Gi-LAN でのトラフィック ステアリング制御、またはアプリケーション機能ごとの DNAI によって識別されるローカル データ ネットワークへのユーザー トラフィックのルーティングのサポートを示します。SMF がこの機能をサポートする場合、PCF は 3GPP 仕様 29.512 の 4.2.6.2.20 項で説明されている機能を実行します。 |
| 2 | ResShare | この機能は、リソースを共有するサービス データ フローのサポートを示します。SMF がこの機能をサポートする場合、PCF は 3GPP 仕様 29.512 の 4.2.7.4 項で説明されている機能を実行します。 |
| 4 | ADC | この機能により、アプリケーションの検出と制御がサポートされます。 |

| 機能番号 | 機能名 | 説明 |
|---|---|---|
| 6 | ネットワーク（NetLoc） | この機能は、5GS のアクセスネットワーク情報レポートのサポートを示します。 |
| 7 | RAN-NAS-Cause | この機能は、アクセス ネットワークからの詳細なリリース原因コードのサポートを示しています。 |
| 8 | EPSFフォールバック レポート | EPS フォールバックが発生し、EPS フォールバック後にルール レポートのルールに対応するリソースが正常にセットアップされたことを示します。SMF は、3GP 仕様リリース 16.10.0、23.502/29.512 で説明されている機能を実行します。 |

SMF は、Npcf_SMPolicyControl_Create メッセージで supportedFeatures 属性を送信し、さらにサポートされている機能を示すビットマップを含めます。PCF は、応答メッセージで supportedFeatures 属性も送信します。応答は、要求と一致するか、要求のサブセットである必要があります。

この文字列には、サポートされている機能を16進形式で示すビットマスクが含まれています。文字列内の各文字は「0」～「9」または「A」～「F」の値をとり、前の表に記載されている機能のサポートを表します。最も大きい番号の機能を表す最上位文字がストリングの最初に表示され、機能 1 ～ 4 を表す文字がストリングの最後に表示されます。機能のリストとそれらの機能の番号付け（1 から始まる）は、各 API に対して個別に定義されます。

## セッション AMBR とデフォルト QoS のプロビジョニングと管理

N4 インターフェイスの場合、SMF は QoS 情報を次の形式で送信します。

- パケット検出ルール（PDR）
- 転送アクション ルール（FAR）のドロップ
- QoS 適用ルール（QER）

SessionAMBR には、各 PDU セッションのすべての非 GBR QoS フローで共有される、アップリンクおよびダウンリンク ビット レートの合計の最大値を含みます。SMF は、既存の QER とともに、非 GBR フローのセッション レベル QER を UPF に送信します。

SMF は、PDU セッションの作成中に SmPolicyDecision 内の PCF から sessionRule を受信します。sessionRule は、authSessAmbr と authDefQos で構成されます。承認された AMBR は、セッション レベルのアップリンク（UL）とダウンリンク（DL）の MBR で構成され、authDefQos にはデフォルト QoS フローの 5Qi、ARP、およびその他の QoS バインド パラメータが含まれています。

SMF は次のステップを実行します：

- authDefQoS で受信したものと同じバインディング パラメータを持つ QoS Desc が関連付けられている PCF から受信した PCC ルールは、デフォルトの QoS フローでタグ付けされます。

- N4 インターフェイスでは、デフォルトの QoS フローに関連付けられた各 PCC ルールに対して UL および DL パケット検出ルール（PDR）が作成されます。セッション AMBR の適用の場合、SMF は適切な AMBR を使用して QoS 適用ルール（QER）を作成し、非 GBR ルールのすべての PDR にそれを関連付けます。
- N1 インターフェイスでは、PDU SESSION ESTABLISHMENT ACCEPT メッセージの「QoS フロー説明」属性に、QFI、MFBR、5Qi の各値が含まれています。このメッセージには、セッション AMBR も送信されます。
- N2 インターフェイスでは、PDU セッション リソース セットアップ転送要求 IE に AMBR と「QoS フロー レベルの QoS パラメータ」（5Qi、ARP など）および QFI が含まれます。
- SMF は、UDM によって開始されたセッション AMBR の変更をサポートしています。この場合、次のように計算します。
  - SMF は、Npcf_SMPolicyControl_Update を、「subsSessAmbr」属性内の新しい登録されたセッション AMBR および「repPolicyCtrlReqTriggers」内の SE_AMBR_CH ポリシー制御要求トリガとともに PCF に送信します。セッション AMBR の変更を受信すると、PCF は、応答内で新しく承認されたセッション AMBR を SMF にプロビジョニングします。
  - セッション AMBR 適用のために、N4 インターフェイスの QER を更新します。
  - N1N2MessageTransfer を、N1 インターフェイスの PDU セッション変更コマンド メッセージの AMF および新しい AMBR を持つ N2 コンテナ内の PDU セッション リソース変更要求の転送 IE に対して AMF に対して開始します。

## ポリシー再検証時間のプロビジョニング

### 機能説明

PCF は SMF に PCF 連携動作をトリガーし、PCF にまだ対応していない場合は PCC ルールを要求するように指示します。PCF は、「revalidationTime」属性内に再検証時間を提供し、SmPolicyDecision の「policyCtrlReqTriggers」属性内に RE_TIMEOUT ポリシー制御要求トリガーを提供することにより、この操作を実行します。PCF は、「revalidationTime」属性に新しい値を含めることで、再検証時間を変更できます。PCF は、RE_TIMEOUT ポリシー制御要求トリガーが提供されている場合は、削除することで再検証機能を無効にすることもできます。

SMF は、既存の再検証時間または新しい再検証時間を受信すると、受信した値を保存し、その値に基づいてタイマーを開始します。次に、SMF は、指定された再検証時間の前に PCC ルール要求を送信します。RE_TIMEOUT ポリシー制御要求のトリガーが削除されると、SMF は再検証のためのタイマーを停止します。

**Note** RE_TIMEOUT が削除されると、以前 SMF に提供されていた再検証時間の値は適用されなくなります。

### 機能の仕組み

再検証時間は、OpenAPI 仕様で定義されている「date-time」形式の文字列です。SMF は、「revalidationTime」属性で再検証時間を受信し、「policyCtrlReqTriggers」属性で RE_TIMEOUT トリガーを受信すると、差分期間（revalidationTime - currentTime - 5 秒バッファ）のタイマーを開始します。タイマーが期限切れになると、SMF は PCC ルールを要求するために PCF との連携を開始します。

標準準拠

ポリシー再検証時間機能は 、*3GPP TS 29.512*、*v15.2.0*に準拠しています。

## 追加 QoS フローのプロビジョニングと管理

PCF は、複数の GBR ルールと非 GBR PCC ルールを作成、変更、または削除できます。

次のシナリオが可能です。

1. PDU セッションの確立中に複数の非 GBR および GBR PCC ルールがアクティブ化されます。この場合、次のように計算します。
   a. SMF は「QoS 管理」の項で説明されている QoS フロー バインドの原則に従って QoS フローを作成します。
   b. N4 インターフェイスでは、すべてのフローに関連付けられた PCC ルールごとに UL および DL PDR が作成されます。フローレベルの QoS 適用では、SMF は MFBR および GFBR（GBR フローの場合）の値を使用して QER を作成し、フローの各 PDR に関連付けます。
   c. N1 インターフェイスでは、PDU SESSION ESTABLISHMENT ACCEPT メッセージの「QoS ふろーの説明」属性に、QFI と MFBR、GFBR、および 5Qi の値が含まれます。各 QoS ルールに関連付けられたパケット フィルタは、「認証 QoS ルール」属性で N1 インターフェイスに送信されます。
   d. N4 インターフェイスと N1 インターフェイスの両方で、さまざまなタイプのパケット フィルタがサポートされています。このリストには、次のオプションが含まれています。

```
Packet filter component type identifier
Bits
8 7 6 5 4 3 2 1
0 0 0 0 0 0 0 1 Match-all type
0 0 0 1 0 0 0 0 IPv4 remote address type
0 0 0 1 0 0 0 1 IPv4 local address type
0 0 1 0 0 0 0 1 IPv6 remote address/prefix length type
0 0 1 0 0 0 1 1 IPv6 local address/prefix length type
0 0 1 1 0 0 0 0 Protocol identifier/Next header type
0 1 0 0 0 0 0 0 Single local port type
0 1 0 0 0 0 0 1 Local port range type
0 1 0 1 0 0 0 0 Single remote port type
0 1 0 1 0 0 0 1 Remote port range type
```

   e. N2 インターフェイスでは、PDU セッション リソース セットアップの転送要求 IE に、各フローの「QoS フロー レベルの QoS パラメータ」（5Qi、ARP など）と QFI が含ま

れます。IE の「GBR QoS フロー情報」フィールドには、GBR フローの MFBR と GFBR が含まれています。

2. PDU セッション確立後の PCC ルールの変更。このシナリオでは、次のシナリオが見られます。

   a. 1 つまたは複数の PCC ルールのパケット フィルタの変更、追加、および削除：

      1. この場合、N4 セッション変更を呼び出すことにより、N4 インターフェイス上の PDR の SDF フィルタが変更されます。

      2. SMF は、N1 インターフェイスの PDU セッション変更コマンド メッセージの「認可 QoS ルール」属性を使用して AMF に対して N1N2MessageTransfer を開始します。この属性のルール操作コードは、次のいずれかです。

```
0 1 1 Modify existing QoS rule and add packet filters
1 0 0 Modify existing QoS rule and replace all packet filters
1 0 1 Modify existing QoS rule and delete packet filter
```

   b. 1 つ以上の PCC ルールに関連付けられた QoS の変更：

      1. SMF は QoS フロー バインド評価を実行し、次の操作が行われます。

         1. 新しい QoS フローが追加されると、一部の PDR の N4 インターフェイスの QFI が変更されます。

         2. ある QoS フローから別の QoS フローへの PCC ルールの移動。この場合、影響を受ける PCC ルールの PDR/QER が変更され、QFI が更新されます。

         3. フローの最後の PCC ルールが別の QoS フローに移動された場合の QoS フローの削除。この場合、影響を受ける PCC ルールの PDR/QER が変更され、QFI が更新されます。

      2. 上記の場合、N1 インターフェイスでは、認定 QoS ルールおよび認定 QoS 記述子が次のいずれかの動作コードとともに送信されます。

```
0 0 1 Create new QoS flow description
0 1 0 Delete existing QoS flow description
0 1 1 Modify existing QoS flow description
```

      3. N2 インターフェイスでは、PDU セッション リソース変更要求転送 IE の QoS フロー レベルの QoS パラメータにより、変更された GFBR、MFBR、5Qi などを伝送します。フロー削除の場合、再リースする QoS フロー リストがこの IE に含まれます。

   c. PCC ルールの削除：

      1. この場合、SMF は N4 インターフェイス上の QoS フローに関連付けられているすべての PDR を削除します。

      2. N1 インターフェイスでは、認定 QoS ルールおよび認定 QoS 記述子が次のいずれかの動作コードとともに送信されます。

```
0 1 0 Delete existing QoS flow description
```

3. N2 インターフェイスでは、PDU セッション リソース変更要求転送 IE が QoS フローをリリース リストに伝送します。

## QoS 適用

SMF は、次のように 1 つの QER を作成することで、PCC ルール（SDF）レベル、QoS フローレベル、およびセッション レベルで QoS を適用します。

- PCC ルールレベルごとに、PCF によって提供され、特定の PCC ルールに関連付けられている関連する QoS Desc に従って MBR/GBR を適用する場合。
- QFI に関連付けられたすべての PCC ルールの MBR/GBR を集約した QoS フロー レベルでの実行。
- セッション レベルで、GBR 以外のすべての QoS フローにセッション AMBR を適用します。

これらの QER が作成されると、SMF は以下を関連付けます。

- GBR 以外の QoS カテゴリに属するすべての PDR にセッション レベル QER を実行します。
- SDF レベルの QER を個別の PCC ルールにマッピングします。

あるフローから別のフローへの PCC ルールの移動およびフロー内の QoS の変更を含む QoS の変更の場合、SMF は GFBR/MF BR（またはセッション AMBR）を変更し、それに応じて N4 インターフェイスで QER を更新します。

## ポリシー制御要求のトリガー

PCF は、SmPolicyDecision データ構造内の「policyCtrlReqTriggers」属性にトリガーを含めることで、1 つまたは複数のポリシー制御要求のトリガーを提供します。

PDU セッションの存続期間中、PCF はポリシー制御要求のトリガーを更新または削除します。トリガーを更新するために、PCF は「policyCtrlReqTriggers」属性にトリガーを含めることで、該当するポリシー制御要求のトリガーの新しい完全なリストを提供します。

PCF は、「policyCtrlReqTriggers」属性を NULL 値に設定して、以前に提供されたすべてのトリガーを削除します。この値を持つポリシー制御要求のトリガーを受信すると、SMF は、常に報告されるトリガーを除き、PCF にトリガーを通知せず、PCF からのプロビジョニングを必要としません。

PCF がトリガーをプロビジョニングするたびに、トリガーの値定義で指定されていない限り、SMF は、HTTP POST メッセージに応答として対応する現在適用可能な値（たとえば、アクセスタイプ、RAT タイプ、ユーザーの場所情報など）をUECampingRep データ構造内の PCF に送信します。この場合、「repPolicyCtrlReqTriggers」属性は含まれません。

サポートされているトリガーのリストは次のとおりです：

| トリガー | 説明 |
|---|---|
| RES_MO_RE | リソース変更の要求がSMFで受信されました。これは必須のトリガーです。<br>**Note**<br>この要求は、UE/AMF が要求した QoS 変更がトリガーされたときに、SMF から PCF に送信されます。 |
| UE_IP_CH | UE IP アドレスの変更。これは必須のトリガーです。 |
| DEF_QOS_CH | デフォルト QoS の変更。これは必須のトリガーです。 |
| SE_AMBR_CH | セッションAMBRの変更。これは必須のトリガーです。 |
| SAREA_CH | N11 アップデートのサービスエリアに関する場所の変更。 |
| SCNN_CH | サービングCNノードに関するロケーションの変更。さまざまな引き継ぎシナリオ中に SMF がこのトリガーをサポートする方法の詳細については、次のセクションを参照してください。 |
| [RE_TIMEOUT] | PCC 再検証タイムアウト（つまり、*3GPP TS 29.503*の表 6.1.3.5.-1 で定義されている適用された PCC ルール要求）があったため、SMF が要求を生成したことを示します。 |
| EPS_FALLBACK | SMF が、PCF によって EPS_FALLBACK トリガーが送信された pccRules の EPS フォールバック レポート機能をサポートしていることを示します。 |

### ハンドオーバーでの SCNN_CH トリガーのサポート

SMF は、次のハンドオーバーでのサービス ネットワークの変更トリガーをサポートしています。

- **Inter AMF ハンドオーバー**：「SCNN_CH」がプロビジョニングされている場合、SMF はサービスネットワーク機能（AMF など）の変更を検出すると、SMF は「repPolicyCtrlReqTriggers」属性内と現在のサービスネットワーク機能「servNfId」属性。サービス提供ネットワーク機能が AMF の場合、SMF は、「servNfInstId」属性内に AMF ネットワーク機能インスタンス識別子を含め、「guami」属性内にグローバルに一意の AMF 識別子を含めます。
- **5G から 4G へのハンドオーバー**：UE が 5GS から EPC/E-UTRAN にハンドオーバーされた場合、「SCNN_CH」ポリシー制御要求トリガーがプロビジョニングされて満たされている場合、SMF には、内部の S-GW ID を含む「servNfId」属性が含まれます。 "anGwAddr" 属性。
- **4G から 5G へのハンドオーバー**：SMF では、「servNfInstId」属性内に AMF ネットワーク機能インスタンス識別子が含まれ、「guami」属性内にグローバルに一意の AMF 識別子が含まれます。
- **WiFi から 5G ハンドオーバー**：SMF では、「servNfInstId」属性内に AMF ネットワーク機能インスタンス識別子が含まれ、「guami」属性内にグローバルに一意の AMF 識別子が含まれます。

- **5G から WiFi ハンドオーバーへの**5GS から EPC への 3GPP 以外のアクセスが引き渡されると、SMF には、「SCNN_CH」ポリシー制御要求トリガーがプロビジョニングされて満たされている場合、「servNfId」属性内の「anGwAddr」属性内の ePDG 識別子が含まれています。

# ゲート制御

## 機能説明

ゲート制御は、PCF による決定に基づいて、特定の IP フローに属する IP パケットをブロックまたは許可する機能です。たとえば、PCF は、AF によって報告されたセッション イベント（サービスの開始と停止）に基づいてゲートウェイ決定を行うことができます。

AF は、アップリンクまたはダウンリンク方向、または両方向で特定の PCC ルールに対応するユーザー トラフィックを一時的にブロックするように PCF に指示します。

PCF ゲートウェイ制御の決定を有効にするために、AF は PCF にセッション イベント（セッションの終了、変更など）を報告します。たとえば、セッションの終了により、ゲートウェイ制御でパケットのブロック、つまり「ゲートのクローズ」がトリガーされます。

**Note** ゲートウェイ制御は、IP タイプのサービス データ フローにのみ適用されます。

## 機能の仕組み

ゲート制御機能は次のように動作します。

1. PCF は、PCC ルールによって参照される TrafficControlData で flowStatus 属性を送信します。この属性の値は、PCF の決定に基づいて、「enabled」、「disabled」、「enable_uplink」、または「enable_downlink」に設定されます。
2. この属性を受信すると、SMF は UPF に、UL または DL パケット検出ルール（PDR）の GATE を開閉するよう指示するか、関連付けられた PCC ルールの UL と DL の両方の PDR をオープンまたはクローズします。PDR に関連付けられている Create QoS Enhancement Rule（QER）または QER の更新のゲート ステータス情報要素（IE）が OPEN または CLOSED に設定されている。
3. その後の変更がある場合、PCF は N4 変更要求をトリガーして GATE ステータスを変更します。

標準準拠

この Gating Control 機能は、以下の基準に準拠しています：

- *3GPP TS 29.512*、バージョン *15.2.0*

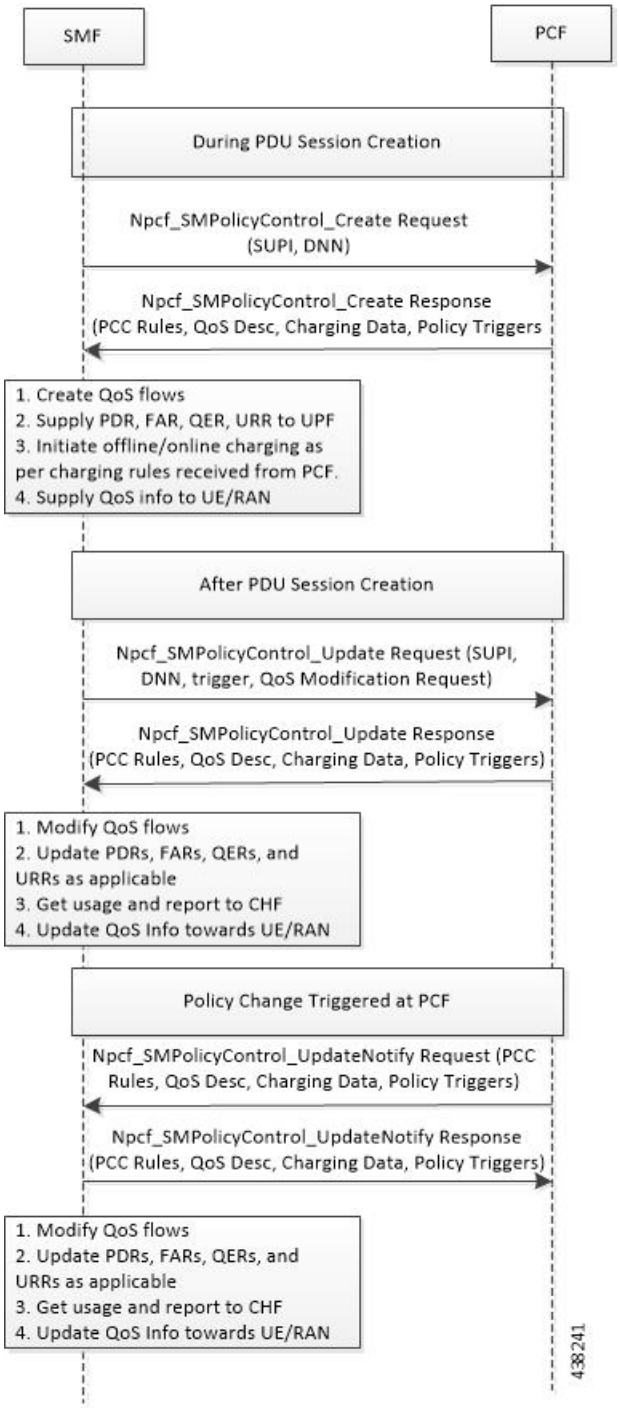
# 機能の仕組み

SMF は PCF からポリシー情報を要求します。PCF は、PDU セッションの作成中および作成後に、動的なポリシーの適用を有効にするためのポリシー規則を提供します。ダイナミック ポリシー管理には、次の操作が含まれます。

- ポリシーコンテキストの作成：この操作は、PDU セッションの作成時に実行され、PCF は応答メッセージで PCC ルールおよび関連する QoS、課金情報、およびその他のポリシー データを送信します。
- ポリシー コンテキストの更新：RAN によって開始されたポリシー更新または UE によって開始されたポリシーの更新およびトリガーイベントの通知の場合、SMF はポリシー コンテキストの更新を開始します。応答で、PCF は QoS と課金に影響する変更されたポリシー データを送信します。
- ポリシー コンテキスト更新通知：PDU セッションのライフサイクル中に、PCF は AF との対話または PCF でのローカル構成の変更に基づいてポリシーの更新を開始できます。PCF からの通知として受信されたアップデートされたポリシー ルールを SMF は、処理します。
- ポリシー コンテキストの削除：PDU セッションの終了時に、SMF は PCF を使用してポリシー コンテキストを終了します。

次の図に、PDU セッションに対するダイナミック ポリシーの管理の手順を示します。

*Figure 219:* ダイナミック ポリシー管理のコール フロー




## 標準準拠

ダイナミック PCC ルールの適用機能は、次の規格に準拠しています。

- *3GPP TS 29.512* バージョン *15.4.0 - 5G 5G* システム。セッション管理ポリシー制御サービス。第 *3* 段階

## 制限事項

ダイナミック PCC ルールの適用機能は、次の制限があります。

- SMF は次の操作の組み合わせのみをサポートします。
  - 新しい QoS フローを作成するための新しい QoS 記述子を使用した新しい PCC ルールの作成
  - 既存の QoS フローへの新しい PCC ルールの追加
  - PCC ルールの削除
  - ルールに関連付けられている GBR/MBR パラメータの更新
  - セッション AMBR の変更

# 動的 PCC ルール適用機能の構成

ここでは、ダイナミック PCC ルール適用機能の構成方法について説明します。

ダイナミック PCC ルール適用機能の構成には、次の手順が含まれます：

1. QoS プロファイルの作成, on page 1295
2. QoS パラメータの構成, on page 1295
3. DNN プロファイル構成での QoS プロファイルの定義, on page 1296

## QoS プロファイルの作成

Quality of Service（QoS）プロファイルのインスタンスを作成するには、次の構成例を使用します。

```
config
  profile qos qos_profile_name
  exit
```

**注**：

- **qos** *qos_profile_name*：QoS プロファイルを作成し、QoS パラメータを構成する [QoS プロファイル コンフィギュレーション（QoS Profile Configuration）] モードへのアクセス権を付与します。 *qos_profile_name* は、QoS プロファイルを一意に識別する英数字の文字列である必要があります。

## QoS パラメータの構成

QoS パラメータを構成するには、次の構成例を使用します。

```
config
  profile qos qos_profile_name
    ambr { ul uplink_ambr | dl downlink_ambr }
    arp { preempt-cap preemption_capability |
    preempt-vuln preemption_vulnerability |
    priority-level priority_level }
    max data-burst burst_volume
    priority qos_priority
    qi5 5qi_value
    exit
```

注：

- **ambr { ul** *uplink_ambr* **| dl** *downlink_ambr* **}**：アップリンク（サブスクライバからネットワーク）およびダウンリンク（ネットワークからサブスクライバ）トラフィックの集約最大ビットレート（AMBR）を定義します。
- **arp preempt-cap** *preemption_capability*：プリエンプション機能フラグを指定します。次のオプションがあります。
  - MAY_PREMPT：ベアラーがプリエンプション処理される可能性がある。
  - NOT_PREMPT：ベアラーをプリエンプトできない。
- **arp preempt-vuln** *preemption_ulnerability*：プリエンプション脆弱性フラグを指定します。次のオプションがあります。
  - PREMPTABLE：ベアラーがプリエンプション処理される可能性があります。
  - NOT_PREMPTABLE：ベアラーをプリエンプトできません。
- **arp priority-level** *priority_level*：サービス データの割り当てと保持の優先順位（ARP）を定義します。 *priority_level* のデフォルト値は 8 です。
- **max data-burst** *burst_volume*：最大データ バースト ボリュームを定義します。 *burst_volume* は 1 ～ 4095 の範囲の整数である必要があります。
- **priority** *qos_priority*：5QI 優先順位レベルを指定します。 *qos_priority* は 、1 ー 127 の範囲の整数である必要があります。
- **qi5** *5qi_value*：承認された QoS パラメータの 5G QoS 識別子（5QI）を指定します。*5qi_value* は 0 ～ 255 の範囲の整数である必要があります。

## DNN プロファイル構成での QoS プロファイルの定義

既存の DNN プロファイル内のQoS プロファイルを構成するには、次のサンプル構成を使用します。

```
config
  profile dnn dnn_profile_name
    qos-profile qos_profile_name
    exit
```

注：

- **qos-profile** *qos_profile_name*：ローカルに構成されたデフォルトの QoS プロファイルを定義します。このプロファイルは、既存のDNNプロファイル設定の下で構成されます。*qos_profile_name* は 、構成された QoS プロファイルの名前である必要があります。

## ダイナミック PCC ルール適用機能の構成の確認

ここでは、ダイナミック PCC ルール適用機能構成の認証方法について説明します。

次の表示コマンドを使用して機能構成の詳細を認証します。

**show full-configuration**

次に、この show コマンドの出力例を示します。

```
show full-configuration
profile dnn dnn1
qos-profile qos1
!
profile qos qos1
ambr ul 1024
ambr dl 1024
qi5 128
arp priority-level 8
arp preempt-cap NOT_PREEMPT
arp preempt-vuln NOT_PREEMPTABLE
priority 9
max data-burst 2048
exit
```

# PCF および SMF インタラクションの制御

サブスクライバ コールの PCF と SMF の連携動作は、デフォルトで有効になっています。SMF との PCF の相互作用を無効にするには、次の構成例を使用します。

```
config
  profile dnn dnn_profile_name
    pcf-interaction { false | true }
    end
```

注：

- **profile dnn** *dnn_profile_name*:：DNN プロファイル名を指定します。 *dnn_profile_name* 英数字の文字列である必要があります。
- **pcf-interaction { false | true }**：PCF とのやり取りを有効または、無効にします。
  - **false**：SMF は PCF と対話しません。
  - **true**：SMF は、すべてのコールフローの一部として可能な場合はPCF と対話します。これはデフォルトの設定です。

（注） **pcf-interaction { false | true }** CLI コマンドは、将来のリリースでは廃止される予定です。

### 設定例

次に、設定例を示します。

```
config
profile dnn intershat1
pcf-interaction false
end
```

### 設定の確認

**pcf-interaction** の構成を確認して、PCF と SMF の相互作用が有効か無効かを判断します。構成を確認するには、 EXEC コマンドを使用します。

**show running-config profile dnn intershat1**

また、グローバル構成モードで次の show コマンドを使用して機能構成を確認することもできます。

**show full-configuration profile dnn intershat1**

**show running-config profile dnn intershat1** コマンドの出力例を次に示します。

```
[smf] smf# show running-config profile dnn intershat1
profile dnn intershat1
 dns primary ipv4 209.165.200.239
 dns primary ipv6 fd01:976a::9
 dns secondary ipv6 fd01:976a:c002:1:fd95:6218:825e:f867
 network-element-profiles chf chf1
 network-element-profiles amf amf1
 network-element-profiles pcf pcf1
 network-element-profiles udm udm1
 charging-profile chgprf1
 virtual-mac      b6:6d:47:47:47:48
 pcscf-profile    PCSCF_Prof_2
 ssc-mode 1
 session type IPV4 allowed [ IPV6 IPV4V6 ]
 upf apn intershat1
 pcf-interaction  false
exit
```

**show full-configuration profile dnn intershat1** コマンドの出力例を次に示します。

```
[smf] smf(config)# show full-configuration profile dnn intershat1
profile dnn intershat1
 dns primary ipv4 209.165.200.239
 dns primary ipv6 fd01:976a::9
 dns secondary ipv6 fd01:976a:c002:1:fd95:6218:825e:f867
 network-element-profiles chf chf1
 network-element-profiles amf amf1
 network-element-profiles pcf pcf1
 network-element-profiles udm udm1
 charging-profile chgprf1
 virtual-mac      b6:6d:47:47:47:48
```

```
 pcscf-profile    PCSCF_Prof_2
 ssc-mode 1
 session type IPV4 allowed [ IPV6 IPV4V6 ]
 upf apn intershat1
 pcf-interaction  false
exit
```

上記の例では、**pcf-interaction false** が表示され、SMF が PCF と対話しないことを示しています。

# 専用 UE サービスのトラフィック フローの処理

**表 *395 :* 機能の履歴**

| 機能名 | リリース情報 | 説明 |
|---|---|---|
| 専用 UE サービスのトラフィック フローの処理 | 2024.01.2 | この機能により、PTT などの特定の UE が特定の TFT を使用して 5G RAT で接続できます。この機能を有効にするには、PCF はダイナミック PCC ルールで **PacketFilterUsage** IE 属性の値を **true** に設定します。このルールにより、SMF は IP「Any-Any」の代わりに PCC ルール TFT のみを送信します。この機能は、デフォルトのフローにのみ適用されます。<br>**デフォルト設定**： 有効 - 常時オン |

## 機能説明

サービスが制限された特定の UE（PTT デバイスなど）が 5G RAT に接続すると、PCF は、デフォルト フローに関連付けられたダイナミック PCC ルールを SMF に送信します。PCF が動的 PCC ルールで **true** に設定された値を持つ **PacketFilterUsage** IE を送信し、PCC ルールがデフォルト フローに関連付けられている場合、SMF はフロー情報を含む QoS ルールを追加し、TFT（トラフィック フロー テンプレート）を UE に送信します。

**packetFilterUsage** IE が false に設定されている場合、SMF は「**Any-Any**」フィルタを使用して QoS ルールを追加し、UE に送信します。パケットフィルタ「**Any-Any**」は、UEが任意のIPと通信して任意のサービスを利用できるようにするデフォルトのフィルタです。この機能の目的は、PTT サービスなどの専用 UE サービスをサポートするためのパケットの優先順位付けを可能にすることです。

この機能はダイナミック ルールにのみ対応しており、静的ルールや定義済みルールには対応しています。この機能も専用ベアラーには適用されません。

（注） N4 インターフェイスには影響がないため、すべてのルールとフィルタは PCF から受信されたとおりに UPF に送信されます。

# 機能の仕組み

UE へのデフォルト フローに関連付けられた TFT パラメータの送信は、次の手順で行われます。

1. **[PCC ルールの識別（PCC Rule Identification）]**：デフォルトフローに関連付けられた PCC ルールを識別するために、次の 2 つの条件が使用されます。
   - PCC ルールが、authDefQos と同じバインディング パラメータ（5QI、arp）で QoS データに関連付けられている場合（authDefQos には、デフォルト QoS フローの 5QI、ARP、および他の QoS バインディング パラメータが含まれています）。

（注） デフォルト フローに関連付けられている PCC ルールの場合、**authDefQos** パラメータのみが考慮され、他のすべての QoS パラメータは無視されます。

   - PCF から受信した PCC ルールに **defQosFlowIndication** IE が **true**に設定されている場合。

2. **[TFT 更新（TFT Update）]**：SMF は、次の条件に基づいて、対応する TFT パラメータを UE に送信します。

| 条件 | 予期される動作 | 説明 |
|---|---|---|
| **packetFilterUsage IE** が **true**に設定されている PCC ルール。 | その PCC ルールに関連付けられている TFT が、N1 インターフェイスを介して UE に送信されます。 | |
| **packetFilterUsage IE** が **false**に設定されている PCC ルール。 | "**Any-Any**" TFT が UE に送信されます。 | |
| 「**Any-Any**」フィルタ + **packetFilterUsage** IE を **true**に設定した新しいルールを使用した既存の TFT。 | SMF は PCF から受信した新しいパケット フィルタで TFT を更新します。 | 以前の QoS ルールが削除され、新しい QoS ルールが UE に対して作成されます。 |
| TFT **packetFilterUsage = true** を持つ最後のルールが削除されます。 | SMF は、現在のルールを削除し、「**Any-Any**」フィルタを使用して新しいルールを追加することで、更新 TFT をプッシュします。 | |

| 条件 | 予期される動作 | 説明 |
|---|---|---|
| **packetFilterUsage=true**のデフォルト フローに対する複数の PCC ルール。 | SMF は、 **packetFilterUsage** IE が **true**になっているルールを 1 つだけ選択します。 | SMF は、**packetFilterUsage** IE が **true**に設定されている他のすべてのルールを拒否します。 |
| SMF には **packetFilterUsage=true** の PCC ルールがすでにあり、PCF は **packetFilterUsage=true**の新しいルールを送信します。 | SMF は新しいルールを拒否します。 | |

（注）
- SMF は、DQR（デフォルトの QoS ルール）= 1 およびパケットフィルタを「**Any-Any**」または特定の TFT として N1 インターフェイスを介してデフォルト フローに対して 1 つの QoS ルールのみを送信します。SMF は、FBR IE の PCC ルールの QoS 説明でビットレートを送信または追加しません。UE の MBR は、セッション AMBR から取得する必要があります。
- SMF は、N4 インターフェイスを介して PCC ルールの QoS 記述の CREATE_QER を送信しません。PCC ルールの PDR の QER ID は、セッション ルールの QER ID に設定されます。SMF では PCC ルールの PDR に追加の QER が含まれており、ゲート ステータスのみが有効または無効になっています。QER には MBR 情報は含まれません。

### 標準準拠

本機能は、*3GPP TS 29.512* バージョン *15.6.0* に準拠しています。セッション管理ポリシー制御サービス。ステージ *3* 標準。

# N7 最適化

**表 *396 :* 機能の履歴**

| 機能名 | リリース情報 | 説明 |
|---|---|---|
| N7インターフェイスでの SMF と PCF の相互作用の最小化 | 2023.04 | N7 最適化サポートの場合、SMF は N7 作成メッセージに UE IP アドレスを送信することで、N7 更新メッセージをスキップします。 |

# 機能説明

N7 最適化サポートの場合、SMF は N7 作成メッセージで UE IP アドレスを送信することで、N7 更新メッセージをスキップします。CLI コマンドを使用してこの機能を有効にすると、SMF は IP アドレスを割り当て、UPF の選択を実行してから PCF との連携を開始します。IP の再割り当てが必要な代替 UPF を選択するように SMF を構成している場合、N4 の障害時に、SMF は N4 成功メッセージの後に N7 更新メッセージを送信して新しい IP アドレスを示します。

# 機能の仕組み

## コール フロー

ここでは、この機能に関連したコール フローについて説明します。

- N7 最適化コール フローによる 5G セッションの作成 （1302 ページ）
- N7 最適化コールフ ローによる N4 セッション確立失敗時の 5G セッションの作成 （1304 ページ）

### *N7* 最適化コール フローによる *5G* セッションの作成

次のコール フローは、N7 最適化を有効にした場合の 5G セッション作成のコール フローを示しています。

図 *220 : N7* 最適化コール フローによる *5G* セッションの作成

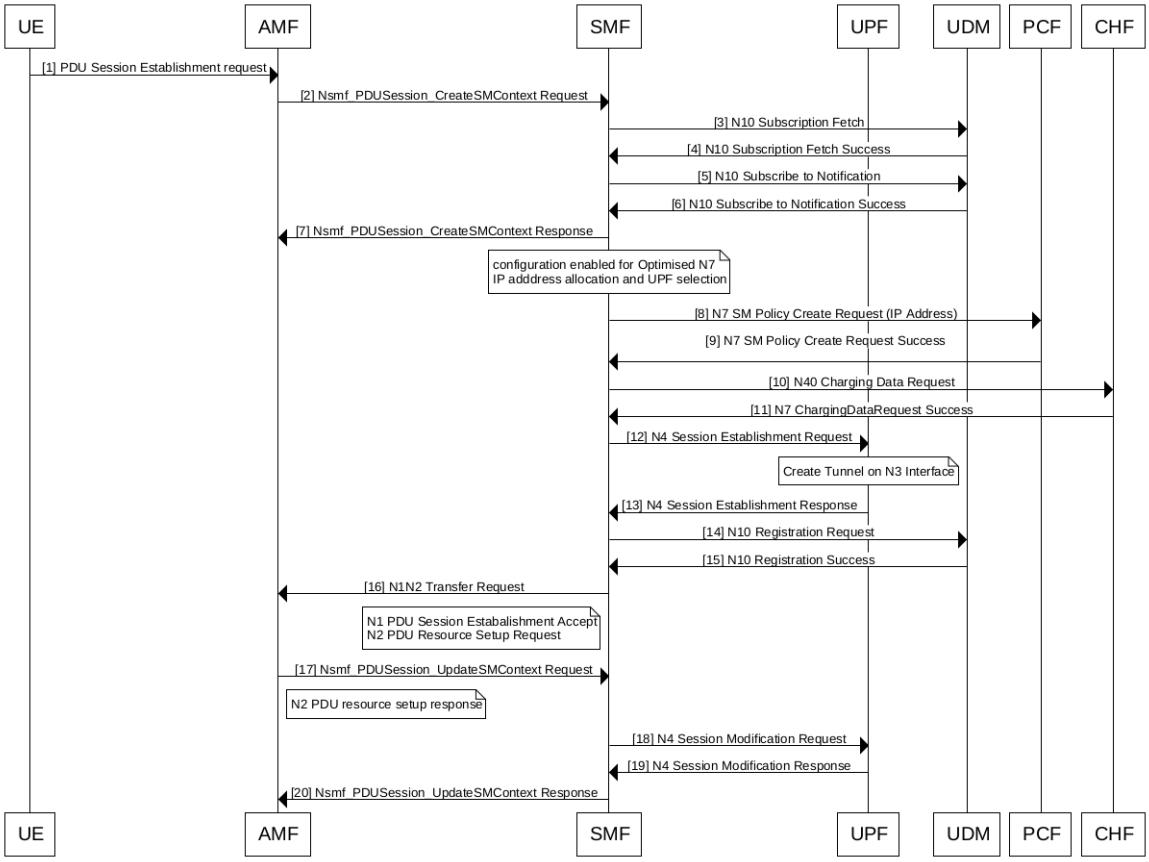



表 *397 : N7* 最適化での *5G* セッション作成のためのコール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | UE は、PDU セッション確立要求メッセージを AMF に送信します。 |
| 2 | AMF は、Nsmf_PDUSession_CreateSMContext 要求メッセージを SMF に送信します。 |
| 3 | SMF は N10 サブスクリプション取得要求を UDM に送信します。 |
| 4 | UDM は SMF に N10 サブスクリプション取得成功応答を送信します。 |
| 5 | SMF は、N10 Subscribe to Notification メッセージを UDM に送信します。 |
| 6 | UDM が SMF に N10 Subscribe to Notification Success 応答を送信します。 |
| 7 | SMFは、Nsmf_PDUSession_CreateSMContext応答をAMFに送信します。 |

| ステップ | 説明 |
|---|---|
| 8 | SMF では、最適化された N7 IP アドレス割り当てと UPF 選択の構成が有効になります。<br>SMF は、IP アドレスとともに N7 SM ポリシー作成要求メッセージを PCF に送信します。 |
| 9 | PCF は、N7 SM ポリシー作成要求の成功応答を SMF に送信します。 |
| 10 | SMF は CHF に N40 課金データ要求メッセージを送信します。 |
| 11 | CHF は、N7 Charging Data Request Success 応答を SMF に送信します。 |
| 12 | SMF は、N4 セッション確立要求を UPF に送信します。 |
| 13 | N3 インターフェイス上にトンネルが作成されます。次に、UPF は N4 セッション確立応答を SMF に送信します。 |
| 14 | SMF は N10 登録要求メッセージを UDM に送信します。 |
| 15 | UDM が SMF に N10 登録成功応答を送信します。 |
| 16 | SMF は、N1N2 転送要求メッセージを AMF に送信します。 |
| 17 | N1 PDU セッション確立要求が受け入れられ、N2 PDU リソース セットアップ要求が送信されます。<br>AMF は、Nsmf_PDUSession_UpdateSMContext Request メッセージを SMF に送信します。 |
| 18 | AMF は N2 PDU リソースのセットアップ応答を送信します。<br>SMF は、N4 セッション変更要求メッセージを UPF に送信します。 |
| 19 | UPF が SMF に N4 セッション変更応答を送信します。 |
| 20 | SMF は、Nsmf_PDUSession_UpdateSMContext 応答を AMF に送信します。 |

### *N7* 最適化コールフ ローによる *N4* セッション確立失敗時の *5G* セッションの作成

次のコール フローは、N7 最適化を有効にしてメッセージ失敗の場合の 5G セッション作成のコール フローを示しています。

図 *221 : N7* 最適化コール フローによる *N4* セッション確立失敗時の *5G* セッションの作成

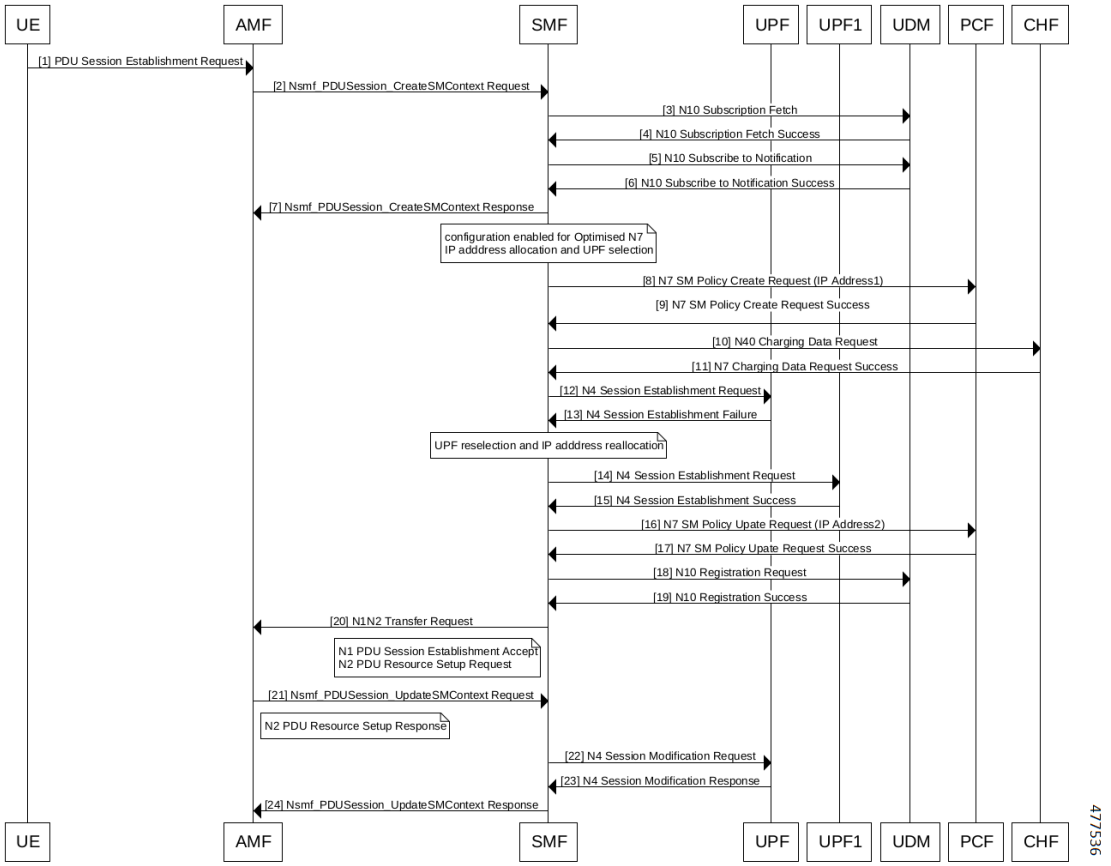



表 *398 : N7* 最適化での *5G* セッション作成のためのコール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | UE は、PDU セッション確立要求メッセージを AMF に送信します。 |
| 2 | AMF は、Nsmf_PDUSession_CreateSMContext 要求メッセージを SMF に送信します。 |
| 3 | SMF は N10 サブスクリプション取得要求メッセージを UDM に送信します。 |
| 4 | UDM は SMF に N10 サブスクリプション取得成功応答を送信します。 |
| 5 | SMF は、N10 Subscribe to Notification メッセージを UDM に送信します。 |
| 6 | UDM が SMF に N10 Subscribe to Notification Success 応答を送信します。 |
| 7 | SMFは、Nsmf_PDUSession_CreateSMContext応答をAMFに送信します。 |

| ステップ | 説明 |
|---|---|
| 8 | SMF では、最適化された N7 IP アドレス割り当てと UPF 選択の構成が有効になります。<br>SMF は、IP アドレスとともに N7 SM ポリシー作成要求メッセージを PCF に送信します。 |
| 9 | PCF は、N7 SM ポリシー作成要求成功メッセージを SMF に送信します。 |
| 10 | SMF は CHF に N40 課金データ要求メッセージを送信します。 |
| 11 | CHF は、N7 Charging Data Request Success 応答メッセージを SMF に送信します。 |
| 12 | SMF は、N4 セッション確立要求メッセージを UPF に送信します。 |
| 13 | 次に、UPF は N4 セッション確立障害メッセージを SMF に送信します。 |
| 14 | UPF の再選択と IP アドレスの再割り当てが行われます。<br>SMF は、N4 セッション確立要求メッセージを UPF1 に送信します。 |
| 15 | UPF1 は SMF に N4 セッション確立成功メッセージを送信します。 |
| 16 | SMF は、IP アドレスとともに N7 SM ポリシー更新要求を PCF に送信します。 |
| 17 | PCF は、N7 SM ポリシー更新要求成功メッセージを SMF に送信します。 |
| 18 | SMF は N10 登録要求メッセージを UDM に送信します。 |
| 19 | UDM が SMF に N10 登録成功応答を送信します。 |
| 20 | SMF は、N1N2 転送要求メッセージを AMF に送信します。 |
| 21 | N1 PDU セッション確立が受け入れられ、N2 PDU リソース セットアップ要求メッセージが送信されます。<br>AMF は、Nsmf_PDUSession_UpdateSMContext Request メッセージを SMF に送信します。 |
| 22 | N2 PDU リソース設定応答メッセージを受信しました。<br>SMF は、N4 セッション変更要求メッセージを UPF に送信します。 |
| 23 | UPF が SMF に N4 セッション変更応答メッセージを送信します。 |
| 24 | SMF は、Nsmf_PDUSession_UpdateSMContext 応答を AMF に送信します。 |

## N7 最適化の構成

N7 最適化を構成するには、次の構成例を使用します：

```
config
  profile dnn dnn_profile_name
    policy [ local | optimized ]
      rat-type [ nr | wlan | eutra ]
    end
```

注：

- **profile dnn** *dnn_profile_name*:：DNN プロファイル名を指定します。 *dnn_profile_name* 英数字の文字列である必要があります。
- **policy [ local | optimized ]**：PCF とのやり取りを有効または、無効にします。
  - **local**：SMF は UPF と対話しません。

（注）
- このパラメータは、セッションの作成時にのみ適用され、引き継ぎ中は変更されません。
- **policy local**を構成する場合、PCF または PCRF の構成は必須ではありません。

  - **optimized**：SMF は、N7 作成メッセージで UE IP アドレスを送信することで、N7 更新をスキップします。

（注） **policy local** と **policy optimized** の両方を同時に構成した場合は、**policy local** が優先されます。

- **rat-type [ nr | wlan | eutra ]**：このキーワードは、指定された RAT タイプについて PCF と交換されるメッセージの数を減らします。

（注） このキーワードは任意です。 **rat-type** が構成されていない場合、**policy local** または **policy optimized** は、NR、WLAN、および EUTRA の 3 つの RAT タイプすべてに対して有効です。

# OAM サポート

## バルク統計サポート

SMF は、この機能の一部として次のメトリックを維持します。

- smf-service-stats

  説明：この統計には、最適化された N7 でセットアップされたセッションの数を示す policy_type ラベルが含まれます。

ラベル

- policy_type

- 値：
  - pcf
  - pcrf
  - local-policy
  - pcf_optimized

smf-service-stats は、詳細ラベル構成の一部として有効にする必要があります。有効になっている場合、smf-service-stats は policy_type ラベルの最適化された N7 で設定されたセッションの数を示します。

smf-service-stats 統計情報を有効にするには、次を使用して pcf_optimized の詳細ラベル統計情報を構成します。

```
infra metrics verbose application
  metrics smf_service_stats
    granular-labels [ policy_type ]
  exit
```

# ダイナミック QOS フローベースのアプリケーション検出および制御

## 機能説明

QCI 80（QoS クラス識別子）で専用ベアラーをサポートするには、SMF がアプリケーション検出および制御（ADC）機能をサポートしている必要があります。

アプリケーションの検出と制御の PCC ルールを受信すると、Policy-control-request-trigger にプロビジョニングされた application-Id と APP_STA/APP_STO を使用して、SMF は UPF にアプリケーショントラフィックを検出するように指示します。アプリケーショントラフィックが UPF から受信したアプリケーション識別子によって識別されると、SMF はアプリケーションの開始を PCF に報告します。次に、PCF は受信した情報に基づいてポリシーを決定し、QCI 80 を使用する新しい専用 PCC ルールを SMF にインストールします。

SMF は次の機能をサポートしています。

- PCF から ADC を有効または無効にします。
- UPF でのアプリケーショントラフィック検出に基づいて、PCF に APP_START および APP_STOP を報告します。
- アプリケーション検出をミュートします。

- セッションレポートの UPF からのアプリケーションの START、STOP および PCF への APP_STA/APP_STO のトリガを処理します。
- L3、L4、および L7 ルールのアプリケーションを検出する。

ダイナミック QoS フローベースのアプリケーションの検出と制御は、ローミングと非ローミングの両方のシナリオに適用できます。

# 機能の仕組み

この項では、ダイナミック QoS フロー ベースのアプリケーション検出および制御機能の仕組みについて説明します。

## インターフェイスの詳細

**PCF および SMF インターフェイス：PCF は SMF で ADC を有効にします**

PCF から SMF への ADC 関連の IE：

**appId**：PCC-Rule 内で PCF によって提供されるアプリケーション識別子。

**APP_STA および APP_STO**：PCF は、ポリシー制御要求トリガでこれらのトリガをプロビジョニングします。

**muteNotif** ：ミュート通知PCF は、IE を「traffContDecs」に含め、PCC ルール内のトラフィック制御データ決定を参照する「refTcData」属性を含めることで、特定の検出されたアプリケーションに関する通知をミュートする場合があります。

例：

```
{  'sessRules': {'SessRule-1': {…}}},
    'pccRules': {
         'PccRule-1': {…},
         'crn#rda1': {'pccRuleId': 'crn#rda1', 'appId': 'x', reftcdata:”TCD-2”}},
    'qosDecs': {'QoS-1': {…}}
   'traffContDecs':{'TCD-2':{'tcId':'TCD-2','flowStatus':'DISABLED','muteNotif':true}},

    'policyCtrlReqTriggers':['PLMN_CH','AC_TY_CH','APP_STA','APP_STO'] }
}
```

**重要** 定義済みルールのミュート解除はサポートされていません。

ミュート機能はポリシー作成中にのみサポートされ、ポリシー更新中はサポートされません。

**SMF では PCF は PCF に開始または停止のトリガを提供しません**

SMF は、「repPolicyCtrlReqTriggers」属性内の「appDetectionInfo」と「APP_STA」/「APP_STO」の検出されたアプリケーション情報を含む SMPolicyControl_Update を送信します。

UPF 最適化が有効になっている場合、SMF は APP_STA または APP_STO トリガをフィルタ処理せず、UPF によってトリガされたすべての APP_STA または APP_STO トリガを PCF に送信

します。SMF セットアップで環境変数 UPF_ADC_OPTIMIZED を true に設定することにより、UPF の最適化を有効にします。

**表 *399 : AppDetectioninfo* タイプの定義**

| 属性名 | データタイプ | L | 基数 | 説明 |
|---|---|---|---|---|
| appid | 文字列 | M | 1 | UPF で構成されたアプリケーション検出フィルタへの参照 |
| InstanceId | 文字列 | O | 1 | サービスデータ フローの説明が推測可能な場合、特定のサービス データ フローの説明にアプリケーションの開始イベントと停止イベントを関連付けることを可能にするために、SMF によってダイナミックに割り当てられる識別子。 |
| sdfDescriptions | 配列（フロー情報） | O | 1...N | 推論可能である場合、推論されたサービスデータ フローの説明が含まれます。 |

# 制限事項

ダイナミック QoS フロー ベースのアプリケーション検出および制御機能には、次の制限があります。

- ADC の開始または停止と非 ADC の使用状況レポート（ボリューム/時間のしきい値）の両方が同じセッション レポート内の UPF から送信されている場合、どのような気象の最初の ADC レポートまたは非 ADC レポートが処理されるかは最初にわかりません。ADC レポートと非 ADC レポートの両方がセッション レポートに送信される場合、smf-service ポッドは 2 つの内部イベント ADC イベントと非 ADC 使用レポート イベントを送信します。インフラでは、2 つの個別の導入ルートを作成して、両方のイベントを処理することができます。ただし、この制限により、非 ADC 使用状況レポートが ADC レポートよりも前に処理されることがあるため、その逆の場合、どの問題が最初にスケジュールされるかが決定論的ではありません。
- 2 つの個別の App-Id の APP-Start イベントと App-Stop イベントが同じセッションレポート要求で UPF から受信されると、SMF は同じ SmPolicyUpdateReq の両方の（開始と停止）イベントを PCF に通知します。APP_STA と APP_STO は、repPolicyCtrlReqTriggersIE、\、で送信されます。これはグローバルな IE です。PCF には APP_STA と APP_STO を受信した履歴があるため、APP_STO を APP_STA をすでに受信している appId にリンクできます。APP_STA トリガーは、PCF が開始通知を受信していない appId に適用できます。

# Gx を介したダイナミック ADC ルールの適用

表 *400 :* 機能の履歴

| 機能名 | リリース情報 | 説明 |
|---|---|---|
| ダイナミック ADC ルールのフローに基づくトラフィックの優先順位付け | 2025.01.0 | SMF は、PCRF のダイナミック ADC ルールの TosTrafficClass フィールドを使用して、ネットワークの輻輳時に IoT アプリケーションに関連付けられたトラフィック フローに優先順位を付けます。 |
| QCI、ARP、オンライン/オフライン課金属性の変更 | 2024.03.0 | このリリースでは、SMF は、ダイナミック ADC ルールに含まれる次の追加 AVP の変更をサポートします。<br>• QCI<br>• ARP<br>• オンライン<br>• オフライン<br>これらの変更によって、サービス プロバイダーはトラフィックをより効率的に分類できます。 |
| Gx インターフェイスを介したダイナミック ADC ルール | 2024.02.0 | SMF では、ユーザーはダイナミック ADC ルールをインストール、変更、または削除できます。SMF は、新しいルールまたは更新されたルールをトラフィック分類のために UPF に転送します。<br>この機能により、通信事業者はコネクテッド カーなどの IoT デバイスを管理し、SMF/UPF で分類されたトラフィック フローに基づいて回線に請求できます。このトラフィック分類により、サービスプロバイダーはサービスの収益化を可能にします。<br>**デフォルト設定**：有効 - 常にオン |

## 機能説明

SMF は、Gx インターフェイスを介したダイナミック ADC ルールの追加、変更、および削除をサポートします。PCRF から TDF-App-Identifier AVP（アプリケーション ID）と TosTrafficClass AVP を含む新しいダイナミック ADC ルールを受信すると、SMF はダイナミック ADC ルールを処理し、ADC ルールをインストールするための TDF-App-Identifier および TosTrafficClass とともに N4 メッセージを UPF に送信します。

PCRF からダイナミック ルールで受信した TosTrafficClass フィールドは、ネットワーク輻輳時のトラフィック フローの優先順位付けをサポートします。UPF が TosTrafficClass フィールドを受信すると、ADC ルールに一致するフローのすべてのアップリンクとダウンリンクのパケットの IP ヘッダーに ToS が適用されます。

UPF は、ダイナミック ADC ルールをさらに処理するために、構成された TDF-App-Identifier とダイナミック ADC ルールを照合します。

この機能により、ポリシー サーバは各サブスクライバの料金設定グループとサービス ID をダイナミックに制御できます。

（注） SMF は、デフォルトのベアラーにのみ関連付けられたダイナミック ADC ルールを処理します。

# 機能の仕組み

Gx を介したダイナミック ADC ルールを有効にするには、SMF および PCRF サーバーは、サポートされている機能ビットを使用して、CCR-I/CCA-I メッセージでサポートしている機能に関する情報を交換します。このため、SMF および PCRF サーバーは、セッションで有効になるサポート対象の機能を交渉します。

サポートされている機能ビットの交渉が成功すると、SMF は PCRF からダイナミック ADC ルールを受信します。その後、SMF は、ダイナミック ADC ルールのインストール、変更、または削除を開始します。

SMF は、Gx インターフェイスを介したダイナミック ADC ルールの次の操作をサポートします。

- ダイナミック ADC ルールのインストール
- ダイナミック ADC ルールの変更
- ダイナミック ADC ルールの削除

## ダイナミック ADC ルールのインストール

次のコール フローでは、ダイナミック ADC ルールをインストールするプロセスについて説明します。

図 *222 :* ダイナミック *ADC* ルールのインストール コール フロー

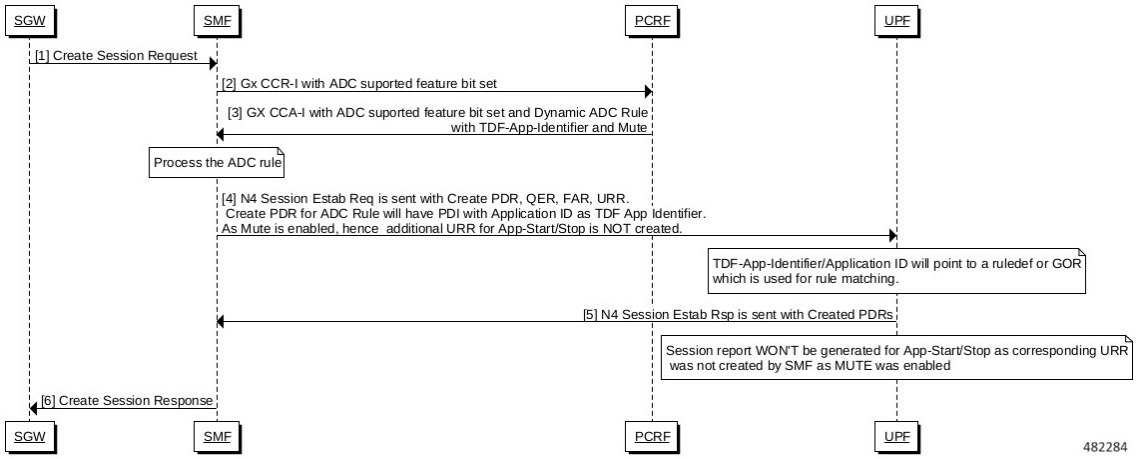



表 *401 :* ダイナミック *ADC* ルール インストール コール フローの説明

| ステップ | 説明 |
|---|---|
| 1. | SMF は SGW からセッション要求の作成を受信します。 |
| 2. | SMF は、ADC がサポートする機能ビットを含む CCR-I を PCRF に送信します。<br>（注）<br>ADC のサポートされている機能ビットは、PCRF と SMF の間でネゴシエートする必要があります。 |
| 3. | SMF は、CCA-I メッセージを介して PCRF から TDF-App-Identifier および Mute を含むダイナミック ADC ルールを受信します。<br>TosTrafficClass は CCA-I メッセージで受信されるオプションの値です。 |

| ステップ | 説明 |
|---|---|
| 4. | SMF はルールをインストールし、N4セッション確立要求を UPF に送信して、パケット検出ルール（PDR）、QoS適用ルール（QER）、転送アクションルール（FAR）、および使用状況レポートルール（URR）を作成します。この ADC ルールの PDR 要求を作成します。このルールには TDF-App-Identifier と TosTrafficClass が含まれています<br><br>受信した TOS 値が、作成されたベアラー レベル FAR と異なる場合、ダイナミックルールに対して新しい UL/DL FAR が作成されます。<br><br>TOS 値と対応するマスクは、N4 Establishment 要求の DL FAR の TRANSPORT LEVEL MARRING IE と UL FAR の INNER PACKET MARCMING IE にそれぞれ入力されます。<br><br>（注）<br>SMF は、Mute AVP が有効になっているダイナミック ADC ルールのみをサポートします。したがって、APP-START および APP-STOP 通知用の追加 URR は作成されません。 |
| 5. | UPF は、ADC ルール用に作成された PDR を使用して N4 セッション確立応答を送信します。<br><br>UPF は、ミュートが有効になっている ADC ルールを受信するため、APP-START および APP-STOP のセッション レポートを生成しません。 |
| 6. | SMF は、セッション応答の作成を SGW から送信します。 |

## ダイナミック ADC ルールの変更

次の段階では、ダイナミック ADC ルールを変更するプロセスについて説明します。

図 *223 :* ダイナミック *ADC* ルール変更のコール フロー

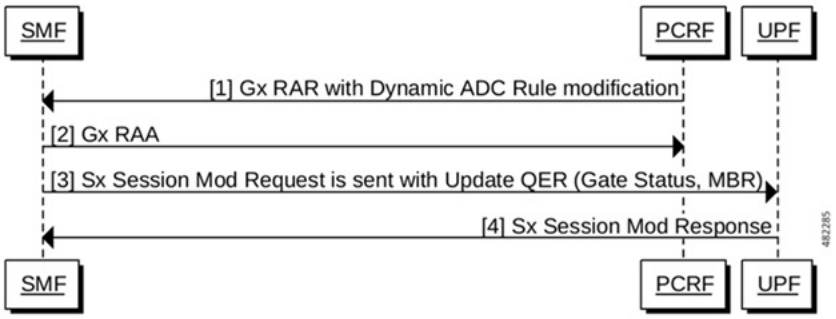


表 *402 :* ダイナミック *ADC* ルール変更コール フローの説明

| ステップ | 説明 |
|---|---|
| 1. | SMF は、PCRF からのダイナミック ADC ルール変更要求とともに、再許可要求（RAR）を受信します。<br>SMF は、ダイナミック ADC ルールでの次の AVP の変更をサポートします。<br>• フロー ステータス<br>• Max-Requested-Bandwidth-UL<br>• Max-Requested-Bandwidth-DL<br>• QCI<br>• ARP<br>• オンライン<br>• オフライン<br>（注）<br>デフォルトのベアラーの QCI と ARP も調整されている場合にのみ、ダイナミック ルールの QCI と ARP を変更できます。 |
| 2. | SMF は、再認証応答（RAA）を PCRF に送信します。 |
| 3. | SMF は、更新 QER IE を含む N4 セッション変更要求を UPF に送信します。この Update QER IE には、ゲート ステータス IE と最大ビット レート（MBR）IE の両方が含まれます。 |
| 4. | UPF が SMF に N4 セッション変更応答を送信します。 |

## インストールされたダイナミック ADC ルールの課金データの変更

SMF は、次の 2 つのダイナミック ADC ルールの課金属性の変更をサポートします：

- **オフライン**：可能な値は ENABLE_OFFLINE（1）および DISABLE_OFFLINE（0）です。
- **オンライン**：使用可能な値は ENABLE_ONLINE（1）および DISABLE_ONLINE（0）です。

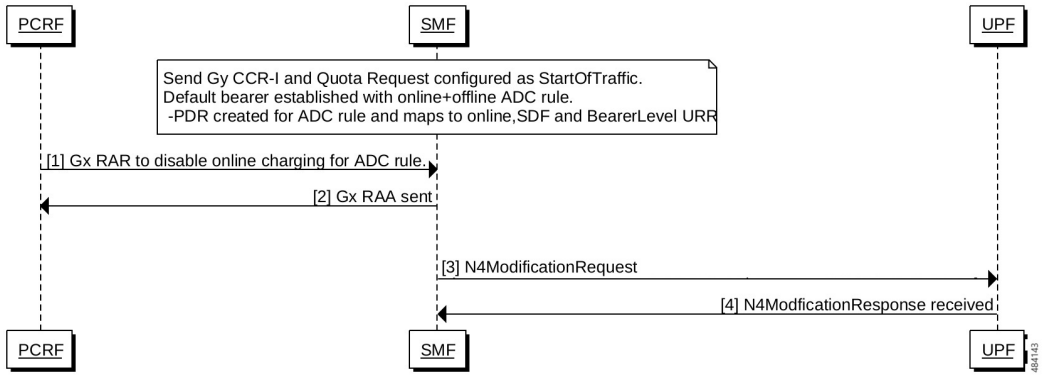
ダイナミック ADC ルールの課金属性を変更するための組み合わせは複数あります。主な組み合わせは次の 2 つです：

- オンラインおよびオフラインからオフラインのみ
- オフラインのみからオンラインとオフライン

## オフラインおよびオンラインの両方からオフラインのみに課金属性を変更する

次の段階では、オフラインとオンラインの両方からオフラインのみに課金属性を変更するプロセスについて説明します：

**図 *224*：オフラインおよびオンラインの両方からオフラインのみに課金を変更する場合のコール フロー**



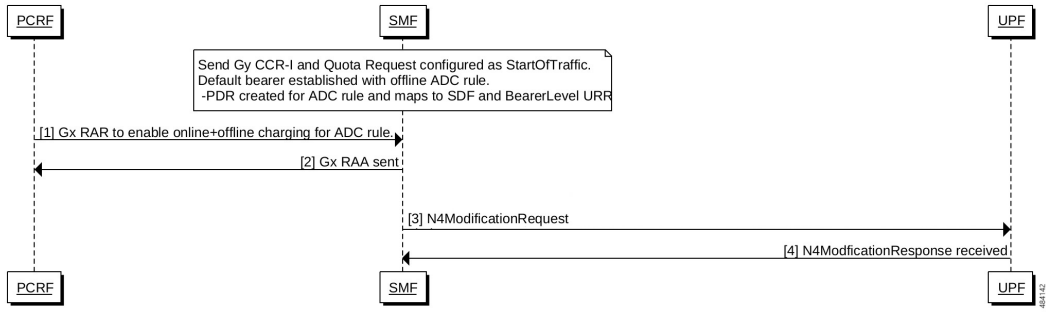

PDN 接続が成功すると、ダイナミック ADC ルールがデフォルトのベアラーにオンライン ルールとオフライン ルールの両方とともにインストールされます。この時点で、PDR が作成され、オンライン、サービス データ フロー（SDF）レベル、およびベアラー レベルの URR にマッピングされます。

1. PCRF は、Gx RAR を SMF に送信し、ダイナミック ADC ルールでオンライン課金を無効にします。PCRF は DISABLE_ONLINE（0）を送信して、ルールをオフラインのみに変更します。
2. SMF は Gx RAA を PCRF に送信します。
3. SMF は、次の 2 つの指示とともに N4 変更要求を UPF に送信します：
    1. オンライン課金に関連付けられている URR を削除します。
    2. SDF およびベアラーレベル URR にマッピングするようにダイナミック ADC ルールの PDR を更新します。
4. UPF が SMF に N4 変更応答を送信します。

## 課金属性をオフラインのみからオフラインとオンラインの両方に変更する

次の段階では、オフラインのみからオフラインとオンラインの両方に課金属性を変更するプロセスについて説明します：

図 *225 :* オフラインのみからオフラインおよびオンラインの両方に課金を変更する場合のコール フロー



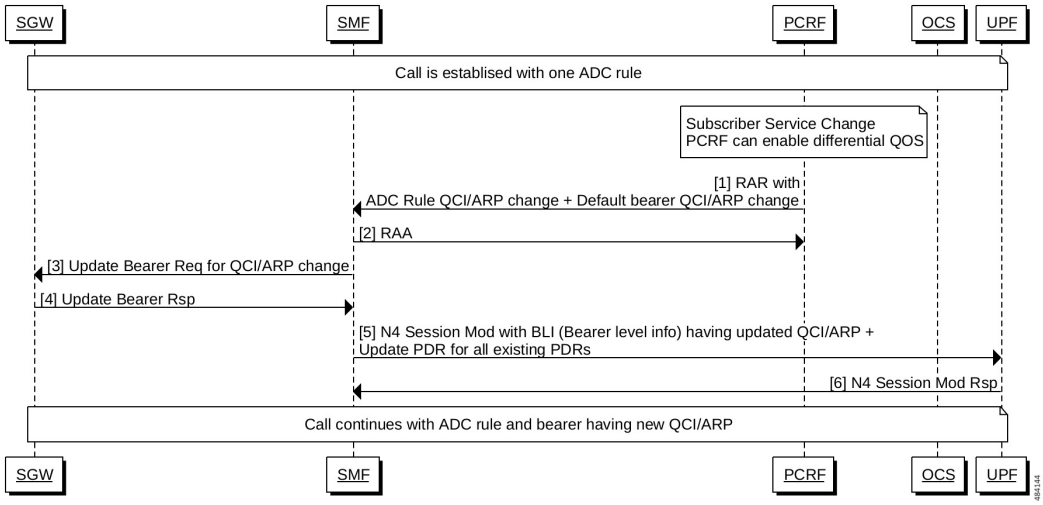

PDN 接続が正常に完了すると、ダイナミック ADC ルールがオフライン課金機能が有効化されたデフォルトのベアラーにインストールされます。この時点で、ダイナミック ADC ルール用に PDR が作成され、SDF URR とベアラー レベル URR にマッピングされます。

1. PCRF は、Gx RAR を SMF に送信し、ダイナミック ADC ルールでオフラインおよびオンライン課金の両方を有効にします。PCRF は ENABLE_ONLINE(1) を送信して、オフラインでのみルールをオンラインとオフラインの両方の課金に変更します。
2. SMF は Gx RAA を PCRF に送信します。
3. SMF は、次の 2 つの指示とともに N4 変更要求を UPF に送信します：
    1. オンライン URR を作成し、トラフィック開始（SoT）が設定されたオンライン課金を有効にします。
    2. オンラインの SDF レベルおよびベアラー レベル URR にマッピングするようにダイナミック ADC ルールの PDR を更新します。
4. UPF が SMF に N4 変更応答を送信します。

## インストールされたダイナミック ADC ルールの QCI および ARP の変更

次の段階では、インストールされたダイナミック ADC ルールの QCI および ARP を変更するプロセスについて説明します。

図 *226* : インストールされたダイナミック *ADC* ルールの *QCI* および *ARP* を変更するためのコール フロー




1. PCRF は、ダイナミック ADC ルールとデフォルトのベアラーの QCI と ARP の変更を含む Gx RAR を SMF に送信します。
2. SMF は Gx RAA を PCRF に送信します。
3. SMF は、デフォルトのベアラーの QCI と ARP を変更するために、SGW にベアラー更新要求を送信します。
4. SGW は、SMF にベアラー応答の更新を送信します。
5. SMF は、更新された QCI と ARP を含むベアラー レベル情報（BLI）とともに N4 セッション変更要求を送信します。N4 セッション変更要求には、既存のすべての PDR に対する PDR の更新命令も含まれています。
6. UPF が SMF に N4 変更応答を送信します。
7. セッションは、新しい QCI と ARP を持つ ADC ルールとベアラーで続行されます。

## ダイナミック ADC ルールの削除

次のコール フローは、ダイナミック ADC ルールを削除するプロセスについて説明しています。

図 *227 :* ダイナミック *ADC* ルールの削除のコール フロー

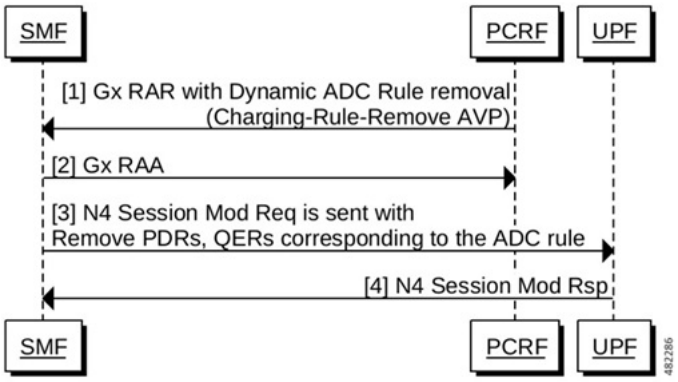



表 *403 :* ダイナミック *ADC* ルールの削除コール フローの説明

| ステップ | 説明 |
|---|---|
| 1. | SMF は、PCRF から課金ルール削除 AVP とともに、再許可要求（RAR）を受信します。 |
| 2. | SMF は、再認証応答（RAA）を PCRF に送信します。 |
| 3. | SMF は、ADC ルールに対応する削除 PDR、QER、FAR とともに、N4 セッション変更要求を UPF に送信します。 |
| 4. | UPF が SMF に N4 セッション変更応答を送信します。 |

（注） REMOVE_FAR は、ルールが削除され、他のルール PDR がこれらの FAR に関連付けられていない場合にのみ送信されます。

# 制限事項

この機能には次の既知の制限事項があります。

- 現在、ADC ルールのインストールと変更の失敗は PCRF に報告されません。
- Rating-Group および Service-Identifier の AVP は、ダイナミック ADC ルールと静的ルールの間で共有できません。ただし、これらの AVP は、複数のダイナミック ADC ルールにわたって共有できます。
- ダイナミック ADC ルール名の先頭を「adc」という文字列にすることはできません。
- この機能は、ミュート通知が有効になっているダイナミック ADC ルールのみをサポートします。

- 課金状態（オンライン、オフライン、または両方の URR にマッピングされた PDR）から課金状態なし（URR にマップされていない PDR）へのダイナミック ADC ルールの変更はサポートされていません。
- Gy インターフェイス障害処理では、ADC ルールをオフライン専用の課金からオフラインとオンラインの両方の課金に変更することがサポートされています。他のタイプの課金変更では現在サポートされていません。
- すべてのダイナミック ADC ルールの QCI および ARP は、常にデフォルトのベアラーの QCI および ARP と一致する必要があります。

# OAM サポート

ここでは、この機能の操作、管理、およびメンテナンス サポートについて説明します。

## バルク統計サポート

Gx を介したダイナミック ADC ルールの適用機能では、次の統計情報がサポートされています。

- **policy_adc_total**：このメトリックは、インストールされているダイナミック ADC ルールの合計数を反映します。このメトリックは、デバッグ レベルで有効になります。この機能をサポートするために、次の新しいラベルが追加されました。
  - **mute**：このラベルは、ダイナミック ADC ルールに対してミュート AVP が有効になっているかどうかを指定します。このラベルに表示されるフィールド値は [TRUE] または [FALSE] です。
- **policy_dynamic_pcc_rules_total**：このメトリックは、PCF からプッシュされたダイナミック ルールの総数を表示します。次に、この機能をサポートするために追加された新しいラベルを示します。
  - **is_adc**：このラベルは、ダイナミック ルールが ADC ルールであるかどうかを指定します。このラベルに表示されるフィールド値は [TRUE] または [FALSE] です。
  - **mute**：このラベルは、ダイナミック ルールに対してミュート AVP が有効になっているかどうかを指定します。このラベルに表示されるフィールド値は [TRUE] または [FALSE] です。

## show コマンドの出力

このセクションでは、ダイナミック ADC ルールに関連する構成を表示するために使用できる show コマンドと出力について説明します。

### show subscriber nf-service smf supi *supi_id* full

次の show subscriber コマンドが拡張され、ADC ダイナミックルールの **ミュート** と **appId** 、およびすべてのダイナミック ルールの **ToSTrafficClass** と **flowstatus の** 情報が表示されるようになりました。

```
[unknown] smf# show subscriber nf-service smf supi imsi-123456789012345 full

pccRuleId": "rd1-adc",
   "qfi": 1,
   "mbrDl": 2000,
   "mbrUl": 2000,
   "chargingInformation": {
   "chargingId": "rd1-adc",
   "meteringMethod": "Duration and Volume",
   "Type": "Offline",
   "ratingGroup": 10,
   "serviceId": "20"
  },
  "appId": "adc",
  "mute": "Required",
  "flowStatus": "Enabled (2)"
   ToSTrafficClass: 20fe
```

## Monitoring Support

次の monitor subscriber コマンドが拡張され、Gx インターフェイスと N4 インターフェイスの両方の ADC ダイナミック ルールの TDF App ID、TosTraffic AVP、ミュート AVP の情報が表示されるようになりました。

```
[unknown] smf# monitor subscriber supi imsi-* capture-duration 1000 internal-messages
yes

ChargingRuleInstall:
                            ChargingRuleInstall[0]:
                                ChargingRuleDefinition:
                                    ChargingRuleDefinition[0]:
                                        ChargingRuleName: dynamicAdc1
                                        RatingGroup:
                                            Value: 40
                                        ServiceIdentifier:
                                            Value: 30
                                        Precedence:
                                            Value: 70
                                        QoSInformation:
                                            QoSClassIdentifier:
                                                Value: QCI_7(7)
                                            MaxRequestedBandwidthUL:
                                                Value: 2000
                                            MaxRequestedBandwidthDL:
                                                Value: 2000
                                            GuaranteedBitrateUL:
                                                Value: 1000
                                            GuaranteedBitrateDL:
                                                Value: 1000
                                            AllocationRetentionPriority:
                                                PriorityLevel: 5
                                                PreEmptionCapability:
                                                    Value:
PREEMPTION_CAPABILITY_DISABLED(1)
                                                PreEmptionVulnerability:
```

```
                                                Value:
PREEMPTION_VULNERABILITY_ENABLED(0)
                                            ReportingLevel:
                                                Value: RATING_GROUP_LEVEL(1)
                                            Online:
                                                Value: ENABLE_ONLINE(1)
                                            Offline:
                                                Value: DISABLE_OFFLINE(0)
                                            MeteringMethod:
                                                Value: DURATION_VOLUME(2)
                                            MuteNotification:
                                                Value: MUTE_REQUIRED(0)
                                            FlowStatus:
                                                Value: ENABLED(2)
                                            TdfApplicationIdentifier: qci7
                                            ToSTrafficClass: 20fe
```

# 静的 PCC ルールのサポート

## 機能説明

静的 PCC ルールは SMF で構成されます。これらのルールは、PDU セッションの確立時に即座にアクティブ化できます。静的ルールは、 **action priority** CLI コマンドを使用した ruledef 構成によって識別されます。

SMF のローカル構成は、セッションの確立中に UPF に送信されるルールベースを表します。SMF は、PCF から受信した PCC ルール、QoS Desc、および課金データを表す構成を使用して、QoS フロー バインドを実行します。この構成は、UPF にも存在します。SMF は PDR、QER、FAR を送信せず、代わりにデフォルトの PDR（ルールベース PDR と呼ぶ）のルールベース名だけを N4 インターフェイス経由で送信します。UPF は、ルールベースの構成に基づいて、定義済みルールの PDR、FAR、QER、および URR を生成します。

**Important** SMF での静的 PCC ルールのサポートは、4G コールと 5G コールの両方に適用されます。

## 関係

この機能は、PDU セッション ライフサイクル機能によって提供される機能を利用します。

## 機能の仕組み

PCF は、SMF で静的 PCC ルールのサポートを有効にするためにルールベース名を送信する必要があります。

PCF がルールベース名を提供すると、SMF は PDU セッションの作成中に次の手順を実行します：

1. SMF が Npcf_SMPolicycontrolCreate メッセージを PCF に送信します。このメッセージに応答して、PCF は SMPolicyDecision を PccRule とともに送信できます。PccRule のルール ID が cbn# ルールベース名の形式である場合、SMF はルール ID がルールベース名を表していると見なします。
2. SMF は、Create PDR IE 内の独自の IE の PFCP セッション確立要求で UPF にルールベース名を送信します。

**Note** SMF は、SDF フィルタを持たないデフォルトの PDR でのみこの名前を送信します。静的ルールの場合、他の PDR、FAR、QER、および URR は UPF に送信されません。UPF は、ルールベース名から同じものを派生させることができます。

## 構成時の前処理

アクティブな課金サービスの構成（ルールベース、関連するルール定義、課金アクションを含む）が完了すると、SMF は構成された値を処理し、構成された値から PCC ルール、QoSData、および ChargingData を導出します。これらのエンティティを作成するには、次の原則が使用されます。

1. QoSデータ：
   a. 設定された課金アクションごとに QoSDesc が作成されます。
   b. 課金アクションで構成される **flow-limit-bandwidth** は、QoSData の GBR/MBR を提供します。
   c. 課金アクションで構成された QCI と ARP は、QoS データの 5QI と ARP を構成します。QCI と ARP が構成されていない場合は、デフォルトの QoS フローの 5QI と ARP がこの QoS データに関連付けられます。
2. ChargingData：
   a. 課金アクションの下の **billing-action** 構成により、作成された ChargingData でオフライン課金を有効にするかどうかが決まります。
   b. 課金アクションの下の **cca charging credit** 構成により、作成された ChargingData でオンライン課金を有効にするかどうかが決まります。
   c. ChargingData の料金設定グループとサービス ID は、課金アクションのコンテンツ ID とサービス識別子を構成することで提供されます。
3. PCCR ルール：
   a. ルールベースの下にある各 ruledef は、PCCRule で作成されます。
   b. 課金アクションで構成された **packet-filter** は、PCCRule の FlowInformation に使用されます。

c. ルールベース構成定でこの ruledef に関連付けられている QoSData と ChargingData は、この PCCrule の refQoS と refChg を形成します。

作成されたすべての PCCRules、QoSData、および ChargingData は、ルールベースごとに保存されます。

## PDU セッションの作成時

1. PDU セッションの作成中に、PCF はルールベース名（PCF が送信しない場合は upf-apn で設定された値）を PCCRule として送信します。このとき、ID が cbn# 構成済みルールベース名に設定されています。また、ID が crn# 設定済みルール定義名に設定された別の PCCRule としてアクティブ化される事前定義済みルールを送信する場合もあります。このような PCC ルールにはすべて、RuleId 属性のみが存在します。
2. このような要求を受信すると、SMF は、受信したルールベースおよびルール定義名に対応する作成済みの PCCRules、QoSData、および ChargingData を選択し、これらを使用して QoSModel で QoS フローを作成します。
3. N4 インターフェイスでは、SMF は、「rulebase」という名前の Cisco 独自の IW の CreatePDR IE でルールベース名を送信します。
4. すべてのアクティブ化された事前定義ルールについて、SMF は「事前定義されたルールのアクティブ化」IE の ruledef 名を含む 1 つのアップリンクと 1 つのダウンリンク PDR を送信します。
5. UPF にも、アクティブ課金サービス用の同様の構成があります。ルールベース名とルール定義名から、対応する QER と URR を作成できます。
6. N1 および N2 インターフェイスでは、事前定義された静的ルールの処理はダイナミックルールの処理と同じです。
7. すべての静的ルールおよびアクティブ化された事前定義ルールについて、パケットフィルタが構成されている場合、QoSR ルールは N1 インターフェイスに送信されます。
8. フローの GFBR および MFBR は、任意の時点ですべての静的およびアクティブ化済みの事前定義済みルールに関連付けられた QoSData の GBR/MBR を使用して計算され、同じものが N2 インターフェイスの AuthorizedQoSDescription IE で N1 インターフェイスに送信されます。

## PDU セッションの変更時

1. PDU セッションの変更中に、PCF はルールベース名を PCCRule として、cbn#configured rulebase name に設定された ID とともに送信します。事前定義されたルールの場合、PCF は新しいルール crn#configured ruledef 名をアクティブにするか、既存のルール（crn#"nil"）を削除できます。このような PCC ルールにはすべて、RuleId 属性のみが存在します。
2. 新しいルール追加要求を受信すると、SMF は、受信したルールベースおよびルール定義名に対応する作成済みの PCCRules、QoSData、および ChargingData を選択し、これらを使用して QoSModel で QoS フローを作成します。

3. 既存のルールの削除要求を受信したときに、SMF が既存のものとは異なる値（nil 値）またはルールベース名を持つ ruledef 名を受け取った場合、SMF は QoSModel の以前のルールベース名または ruledef に対応する QoS フローを削除します。
4. N4 インターフェースにおいて、SMF は Cisco 独自の IW「rulebase」内の CreatePDR IE に新しいルールベース名を送信し、古いルールベース名に対応する PDR ID を伴う RemovePDR を送信します。
5. すべてのアクティブ化された事前定義ルールについて、SMF は「事前定義されたルールのアクティブ化」IE の ruledef 名を含む 1 つのアップリンクと 1 つのダウンリンク PDR を送信します。
6. 非アクティブ化されたすべての事前定義済みルールに対して、SMF は、事前定義済みルールに対応する PDR ID とともに RemovePDR を送信します。
7. UPF にも、アクティブ課金サービス用の同様の構成があります。ルールベース名とルール定義名から、対応する QER と URR を作成または削除できます。
8. N1 および N2 インターフェイスでは、事前定義された静的ルールの処理はダイナミックルールの処理と同じです。
9. すべてのスタティック ルールおよびアクティブ化/非アクティブ化された事前定義ルールについて、パケット フィルタが構成されている場合、QoSR ルールは N1 インターフェイスに送信されます。
10. フローの GFBR および MFBR は、任意の時点ですべてのスタティックおよびアクティブ化/非アクティブ化済みの事前定義済みルールに関連付けられた QoSData の GBR/MBR を使用して計算され、同じものが N2 インターフェイスの AuthorizedQoSDescription IE で N1 インターフェイスに送信されます。

# スタティック PCC ルールの構成

この項では、SMF におけるスタティック PCC ルールの構成方法について説明します。

スタティックルールと事前定義済みルールの構成は、StarOS ベースの PGW-C の ECS 構成に基づいています。これは、UPF が SMF とシームレスに連携できるようにするためです。

スタティック PCC ルールの構成に進む前に、必ず、まずアクティブ課金サービス（ACS）を構成してください。ACS は、バックエンド課金仲介システムとの統合機能を備えたレイヤ 3 からレイヤ 7 のパケット インスペクション（DPI）を使用して、サブスクライバに柔軟で差別化された詳細な課金情報を提供します。

**Note** システムごとに構成できるアクティブな課金サービスは 1 つのみです。

スタティック PCC ルール サポートの構成には、次の手順が含まれます。

1. 課金アクションでの構成, on page 1326

2. パケット フィルタの構成, on page 1328
3. ACS ルールデフの構成, on page 1329
4. ルール定義の ACS グループの構成, on page 1331
5. ルールベースおよび事前定義済みルールプレフィックスの構成, on page 1331
6. ACS ルールベースの構成（ACS 構成モード）, on page 1334
7. URR ID の構成, on page 1332
8. GTPP グループの構成, on page 1333
9. APN の構成, on page 1333
10. GTPP グループと APN の関連付け, on page 1333
11. ACS ルールベースの構成（APN 構成モード）, on page 1332
12. DNN プロファイル構成での UPF APN プロファイルの定義, on page 1336
13. QoS パラメータの構成, on page 1295

# 課金アクションでの構成

このセクションでは、課金アクションの構成方法を説明します。課金アクションは、構成されたルールに一致したときに実行されるアクションを意味します。アクションの範囲として、アカウンティング レコード（例：EDR）の生成から IP パケットのドロップなどまでが含まれます。また、課金アクションによって、使用量計算の原則を規定します。再送信されたパケットをカウントするかどうか、および課金情報にどのプロトコルフィールド（L3/L4/L7など）を使用するかがこれに当たります。

ruledef に関連付けられた QoS および課金関連パラメータを定義するには、次の構成例を使用します。

```
config
   active-charging service service_name
     charging-action charging_action
        allocation-retention-priority priority  [ pci pci_value
        | pvi pvi_value billing-action egcdr cca
        charging credit [ rating-group coupon_ id
        ] [ preemptively-request ]
        content-id content_id
        flow action { discard [ downlink | uplink ] | redirect-url
        redirect_url | terminate-flow }
        flow limit-for-bandwidth { { direction { downlink | uplink }
        peak-data-rate bps peak-burst-size bytes violate-action
        { discard | lower-ip-precedence } [ committed-data-rate
        bps committed-burst-size bytes
        [ exceed-action { discard | lower-ip-precedence
        } ] ] } | { id id } }
        nexthop-forwarding-address ipv4_address/ipv6_address
```

```
qos-class-identifier qos_class_identifier
service-identifier service_id
tft packet-filter packet_filter_name
tft-notify-ue
tos { af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32
| af33 | af41 | af42 | af43 | be | ef | lower-bits tos_value
} [ downlink | uplink ]
end
```

注：

- **charging-action** *charge_action_name*: 課金アクションの名前を指定します。 *charge_action_name* は 、1 ～ 63 文字の英数字の文字列である必要があります。また、句読点を含めることができます。各家禽アクションには一意の名前が必要です。
- 指定された課金アクションが存在しない場合は作成され、CLI モードは課金アクションを構成できる ACS 課金アクション構成モードに変わります。
- 指定された課金アクションが存在する場合、CLI モードはその課金アクションの ACS 課金アクション構成モードに変更されます。
- **allocation-retention-priority** *priority* **[ pci***pci_value* **| pvi** *pvi_value* ：割り当て保持優先順位（ARP）を構成します。 *priority* は 1 ～ 15 の範囲の整数値である必要があります。
  - **pci** *pci_value* ：プリエンプション機能表示（PCI）値を指定します。次のオプションがあります。
    - MAY_PREEMPT：フローをプリエンプション処理できます。これはデフォルト値です。
    - NOT_PREEMPT：フローをプリエンプション処理できません。
  - **pvi** *pvi_value*：プリエンプション脆弱性の兆候（PVI）の値を指定します。次のオプションがあります。
    - NOT_PREEMPTABLE：フローをプリエンプション処理できません。これはデフォルト値です。
    - PREMPTABLE：フローをプリエンプション処理できます。
- **billing-action**：特定のルール定義に一致するパケットの課金アクションを構成します。
- **cca charging credit**：クレジット制御アプリケーション（CCA）を有効または無効にし、RADIUS/Diameter のプリペイド課金動作を構成します。
- **content-id**：料金設定グループを構成します。
- **flow action**：ルール定義に一致するパケットで実行するアクションを指定します。
- **flow limit-for-bandwidth**：MBR や GBR などの QoS パラメータを構成します。
  - Peakdatarate（MBR）：デフォルトは 3000 bps です

- Peakburstsize：デフォルトは 3,000 バイトです
- [committedDataRate（GBR）]：デフォルトは 144000 bps です
- commitedBurstSize：デフォルトは 3000 バイト

- **nexthop-forwarding-address** *ipv4v6_address* | *ipv4_address* | *ipv6_address* ：この APN のネクストホップ転送アドレスを構成します。
- **qos-class-identifier** *qos_class_identifier*：課金アクションの QoS クラス識別子（QCI）を構成します。 *qos_class_identifier*は 、1 ～ 9 または 128 ～ 254 の範囲の整数である必要があります（演算子固有）。
- **service_identifier** *service_id*：生成された課金レコードで使用するサービス ID を構成します。 *service_id* は 、1 ～ 2147483647 の範囲の整数である必要があります。
- **tft packet-filter** *packet_filter_name*：現在の課金アクションに追加する、またはアクションから削除するパケットフィルタを指定します。 *packet_filter_name* は 、1 ～ 63 文字の英数字の文字列である必要があります。
- **tft-notify-ue**：特定のトリガ条件に基づいて UE に対する TFT 更新を制御します。
- **tos**：Type of Service（ToS）オクテットを構成します。

## パケット フィルタの構成

パケット フィルタを構成するには、次の構成例を使用します。

```
config
  active-charging service service_name
    packet-filter packet_filter_name
      direction { bi-directional | downlink | uplink }
      ip local-port { = port_number | range start_port_number to
      end_port_number }
      ip protocol = protocol_number
      ip remote-port { = port_number | range start_port_number to
      end_port_number }
      ip tos-traffic-class = { type-of-service | traffic class }
      mask { = mask-value}
      priority priority
      end
```

注：

- **packet-filter** *packet_filter_name*：UE に送信するパケットフィルタを構成します。 *packet_filter_name* は 、1 ～ 15 文字の英数字の文字列である必要があります。
- **direction { bi-directional | downlink | uplink }**：パケット フィルタを適用する必要がある方向を設定します。デフォルト値は **bi-directional** です。
- **ip local-port**：現在のパケット フィルタの IP 5 タプル ローカル ポートを構成します。
- **ip protocol**：現在のパケット フィルタの IP プロトコルを構成します。

- **ip remote-address**：現在のパケット フィルタの IP リモート アドレスを構成します。
- **ip remote-port**：現在のパケット フィルタの IP リモート ポートを構成します。
- **ip tos-traffic-class**：パケット フィルタ モードで、課金アクションのサービス（TOS）/トラフィック クラスのタイプを構成します。
- **priority** *priority*：現在のパケット フィルタの優先順位を構成します。

## ACS ルールデフの構成

は、プロトコル フィールドと状態情報に基づいた複数の L3 ～ L7 プロトコルにおける一連の一致条件を表します。各 ruledef は、アクティブな課金サービス内の複数のルールベースで使用できます。

ACS ルール定義を作成、設定、または削除するには、次の設定例を使用します。

```
config
  active-charging service service_name
    ruledef ruledef_name
      ip any-match [ = | != ] [ TRUE | FALSE ]
      ip dst-address { operator { { ipv4_address | ipv6_address
      } | { ipv4_address/mask | ipv6_address/mask} |
      address-group ipv6_address } | { !range | range }

      rule-application { charging | post-processing | routing }
      end
```

注：

- **ruledef** *ruledef_name*：追加、設定、または削除する ruledef を指定します。 *ruledef_name* は ACS ルールデ の名前である必要があります。また、1 ～ 63 文字の英数字の文字列である必要があり、句読点を含めることができます。各 ruledef には一意の名前を付ける必要があります。ホストプール、ポートマップ、IMSI プール、ファイアウォール、ルーティング、および課金のルール定義には一意の名前を付ける必要があります。
- 指定された ruledef が存在しない場合は作成され、CLI モードは ruledef を設定できる ACS ルールデ コンフィギュレーション モードに変わります。
- 指定された ruledef がすでに存在する場合、CLI モードはその ruledef の ACS ルールデ コンフィギュレーション モードに変わります。ACS ルール定義コンフィギュレーション モードを使用して、個々のルール定義（ruledef）でルール式を作成および管理します。
- **ip any-match [= | !=] [TRUE | FALSE**：IPv4/IPv6 パケットに一致するルール式を定義します。コマンドの 演算子 と 条件 は、次を指定します。
  - *operator*
    - != : 等しくない
    - <=: 等しい
  - 条件

- FALSE
- TRUE

- **ip dst-address {** *operator* **{ {** *ipv4_address* **|** *ipv6_address* **} | {** *ipv4_address/mask* **|***ipv6_address/mask* **} | address-group** *ipv6_address* **} | { !range | range } host-pool** *host_pool_name* **}**：IP ヘッダー内の IP 宛先アドレスフィールドに一致するルール式を定義します。
  - *ipv4_address* **|** *ipv6_address*：発信トラフィックの宛先ノードの IP アドレスを指定します。 *ipv4_address* **|** *ipv6_address* は、 IPv4 ドット付き 10 進表記または IPv6 コロン区切り 16 進表記の IP アドレスである必要があります。
  - *ipv4_address/mask* **|** *ipv6_address/mask*：発信トラフィックの宛先ノードの IP アドレスを指定します。 *ipv4_address/mask* **|** *ipv6_address/mask* は、 サブネットマスクビットを含む IPv4 ドット付き 10 進表記または IPv6 コロン区切り 16 進表記の IP アドレスである必要があります。マスク ビットは、サブネット マスクのビット数に対応する数値です。
  - *address-group ipv6_address*：ワイルドカード入力や特殊な範囲入力で設定された IPv6 アドレスのグループを指定します。複数のワイルドカード文字を入力として受け入れることができますが、入力できるのは 1 つの 2 バイト範囲入力だけです。ワイルドカード文字の入力と 2 バイトの範囲の入力の両方を、特定の IPv6 アドレス内で一緒に設定できます。
  - コマンドの 演算子 は、次を指定します。
    - != : 等しくない
    - < : 次の値以下
    - = : 等しい
    - >=: 次の値以上

- **multi-line-or all-lines**：単一の ruledef で複数の URL 式を指定できます。ruledef が評価されるときに、multi-line-or all-lines コマンドが設定されていると、論理 OR 演算子が ruledef 内のすべてのルール式に適用され、ruledef が一致するかどうかが判断されます。multi-line-or all-lines コマンドが設定されていない場合、論理 AND 演算子がすべてのルール式に適用されます。
- **rule-application { charging | post-processing | routing }**：ルール定義のルール適用を指定します。
  - **charging**：現在の ruledef が課金目的であることを指定します。
  - **post-processing**：現在の ruledef が後処理用であることを指定します。これにより、パケットのルール照合が無効になっている場合でも、パケットを処理できます。
  - **routing**：現在の ruledef がルーティング用であると指定します。アクティブな課金サービスでのルーティングには、最大 256 のルール定義を定義できます。デフォルトで、ディセーブルになっています。

## ルール定義の ACS グループの構成

group-of-ruledefs には最適化可能な ruledef を含めることができます。Ruledef グループの最適化は、ruledef のグループの ruledef の最適化機能と、ルールベースのグループの最適化の設定に依存します。

新しい ruledef を追加すると、次のチェックが行われます。

- 新しい ruledef が既存の ruledef グループの一部であるかどうかを判別します。
- 新しい ruledef が最適化を必要としているかどうかを識別します

ruledef のセットを組み合わせて同じ課金アクションを適用するには、次の設定例を使用します。

```
config
  active-charging service service_name
    group-of-ruledefs ruledef_group_name
      add-ruledef priority ruledef_priority ruledef ruledef_name
      exit
```

注：

- **group-of-ruledefs** *ruledef_group_name* ：追加、設定、または削除の対象となる ruledef グループ名を指定します。このコマンドでは、最大 128 個の ruledef 設定グループを指定できます。
- **add-ruledef**：このコマンドを使用すると、ruledef のグループに ruledef を追加または削除できます。このコマンドでは、最大 128 個の ruledef 設定が可能です。
- **priority**：ruledef の現在のグループでの ruledef の優先順位を指定します。 *ruledef_priority* は 、1 ～ 10000 の範囲の整数である必要があります。
- **ruledef** *ruledef_name*：現在のルール定義のグループに追加するルール定義の名前を指定します。*ruledef_name* は 1 ～ 63 文字の英数字の文字列である必要があります。

## ルールベースおよび事前定義済みルールプレフィックスの構成

ルールベースおよび事前定義されたルールのプレフィックス構成は、PCF からの静的ルールのインストールに必須です。SMF は、プレフィックス付きおよびプレフィックスなしの事前定義ルールのインストールをサポートします。SMF は、事前に定義されたルールと静的ルールの両方で group-of-ruledef のインストールもサポートしています。

ルールベースのプレフィックスと事前定義されたルールのプレフィックスを構成するには、次の構成例を使用します。

```
config
  profile network-element pcf pcf_service_name
    predefined-rule-prefix predef_rule_prefix
    rulebase-prefix rulebase_prefix
    end
```

注：

- **predefined-rule-prefix** *predef_rule_prefix*：追加する事前定義されたルールのプレフィックスを指定します。たとえば、事前に定義されたルールのプレフィックスは **cbr** です。
- これは、事前定義済みルールのオプションの構成です。PCF ネットワーク要素プロファイル内に定義されたプレフィックスがない場合、事前定義されたルールの適用は *3GPP TS 29.244* 仕様で定義されているように動作します。
- **rulebase-prefix** *rulebase_prefix*：追加するルールベースのプレフィックスを指定します。たとえば、ルールベースのプレフィックスは **rbn**です。これは、静的ルールの必須構成です。

## ACS ルールベースの構成（APN 構成モード）

構成された APN を使用するサブスクライバに使用される ACS ルールベースを有効にして構成するには、次の構成例を使用します。

```
config
  apn apn_name
    active-charging rulebase rulebase_name
    end
```

注：

- **active-charging rulebase** *rulebase_name*：ACS ルールベースの名前を指定します。 *rulebase_name* は 、1 ～ 63 文字の英数字の文字列である必要があります。

## URR ID の構成

このセクションでは、料金設定およびサービスグループの通信量レポートルール（URR）IDを構成する方法について説明します。

```
config
  active-charging service service_name
    urr-list list_name
      rating-group rating_id service-identifier service_id_value
      urr-id urr_id_value
      end
```

注：

- **urr-list** *list_name*：URR リストの名前を指定します。 *list_name* は 、1 ～ 63 文字の英数字の文字列である必要があります。
- **rating-group** *Rating_id*：課金に使用される料金設定 ID を指定します。 *Rating_id* は 、0 ～ 2147483647 の範囲の整数である必要があります。
- **service-identifier** *service_id_value*：サービス識別子の値を構成します。 *service_id_value* は 、0 ～ 2147483647 の範囲の整数である必要があります。
- **urr-id** *urr_id_value*：料金設定/サービス グループの URR 識別子を構成します。 *urr_id_value* は 、1 ～ 8388607 の範囲の整数である必要があります。

• URR ID の構成は、料金設定グループおよびサービス ID ごとです。異なる料金設定グループとサービス ID の組み合わせについては、URR ID 構成を必要な回数だけ使用します。

## GTPP グループの構成

GTPP グループの構成するには、次のサンプル構成を使用します。

```
config
  gtpp group group_name
    gtpp trigger { time-limit | volume-limit }
    end
```

注：

• **gtpp group** *group_name*：GTPP グループ名を指定します。 *group_name* は 、1 ～ 63 文字の英数字の文字列である必要があります。

• **gtpp trigger { time-limit | volume-limit }**：CDR のトリガーを構成します。

  • **time-limit**：CDR の時間制限トリガーを有効にします。

  • **volume-limit**：CDR のボリューム制限トリガーを有効にします。

## APN の構成

このセクションでは、アクセス ポイント名（APN）テンプレートを作成する方法について説明します。この APN 構成は UPF 内のアクセスポイント構成を表し、その内でのルールベース名の構成をさらに容易にします。

APN を構成するには、次の構成例を使用します。

```
config
  apn apn_name
  end
```

注：

• **apn** *apn_name*：APN テンプレートの名前を 1 ～ 62 文字の英数字の文字列として指定します。名前は、大文字と小文字が区別されません。

## GTPP グループと APN の関連付け

構成された APN に GTTP グループを関連付けるには、次のサンプル構成を使用します。

```
config
  apn apn_name
    gtpp group group_name
    end
```

注：

• **gtpp group** *group_name*：定義済みの GTPP グループを構成済みの APN に関連付けます。

# ACS ルールベースの構成（ACS 構成モード）

このセクションでは、ACSルールベースを作成、設定、または削除する方法について説明します。ルールベースは、フローと一致するプロトコルルール、および一致したフローに対して実行される関連アクションのコレクションです。サブスクライバ/APN に使用する特定のルールベースが設定されていない場合、デフォルトのルールベースが使用されます。

ルールベースの設定は、指定されたすべての設定を組み合わせて静的および事前定義された PCC ルールを構築する設定です。

ACS ルールベースを構成するには、次の構成例を使用します。

```
config
   active-charging service service_name
      rulebase rulebase_name
         action priority action_priority { [ dynamic-only ]
         | static-and-dynamic | timedef timedef_name ]
         { group-of-ruledefs ruledefs_group_name |
         ruledef ruledef_name } charging-action charging_action_name
         [ monitoring-key monitoring_key ] [ description description ] }
         cca quota { holding-time holding_time content-id content_id
         | retry-time retry_time [ max-retries retries ] }
         cca quota time-duration algorithm { consumed-time seconds
         [ plus-idle ] | continuous-time-periods seconds |
         parking-meter seconds} [ content-id content_id]
         credit-control-group cc_group_name
         dynamic-rule order { always-first | first-if-tied }
         egcdr threshold { interval interval
         [ regardless-of-other-triggers ] | volume { downlink | total
|
         uplink } bytes }
         route priority route_priority ruledef ruledef_name
        analyzer { dns | file-transfer | ftp-control | ftp-data | h323

         | http | imap | mipv6 | mms | pop3 | pptp | radius | rtcp |
rtp
       | rtsp | sdp | secure-http | sip [ advanced | basic-and-advanced

         ]
         | smtp | tftp | wsp-connection-less | wsp-connection-oriented
 }
         [ description description ]
         tcp check-window-size
         tcp mss tcp_mss { add-if-not-present | limit-if-present }
         tcp packets-out-of-order { timeout timeout_duration|
         transmit [ after-reordering | immediately ] }
         end
```

注：

- **rulebase** *rulebase_name*：ACS ルールベースの名前を指定します。 *rulebase_name* は 、1 ～ 63 文字の英数字の文字列である必要があります。

- **action priority** *action_priority* **{ [ dynamic-only ] | static-and-dynamic | timedef** *timedef_name* **] { group-of-ruledefs** *ruledefs_group_name* **| ruledef** *ruledef_nameCharging_action_namemonitoring_key* **} charging-action** 説明 **] [ description** ： **[ monitoring-key** *ruledef* **] }**が一致する優先順位と、関連する課金アクションを構成します。
  - 優先度は 1ー65535 の範囲の整数である必要があります
  - *monitoring_key* は、100000 ～ 4000000000 の範囲の整数である必要があります。

  設定した ruledef、group-of-ruledefs、Charging アクションを削除するには、 **no action priority** *action_priority* コマンドを使用します。

**Important** 現在、SMF は、ruledef、group-of-ruledefs、および課金アクションの個別の削除をサポートしていません。

- **cca quota { holding-time** *hold_time* **content-id** *content_id* **| retry-time** *retry_time* **[ max-retries** *retries* **] }**：オンライン課金のクォータを構成します。
  - *holding_time* は 1 ～ 4000000000 までの整数である必要があります。
  - *content_id* は 、1 ～ 2147483647 の範囲の整数である必要があります
  - *retry_time* は、0 ～ 86400 の範囲の整数である必要があります。
  - *retries* は 1 ～ 65535 の範囲の整数である必要があります。
- **cca quota time-duration algorithm { consumed-time** *consumed_time* **[ plus-idle ] | continuous-time-periods** *continuous_time* **| parking-meter** *parking_meter* **} [ content-id** *content_id* **]**
  - *consumed_time* は、1 ～ 4294967295 秒の範囲の整数である必要があります
  - *content-id* は 1 ～ 2147483647 の範囲の整数である必要があります
  - *continuous_time* は、1 ～ 4294967295 秒の範囲の整数である必要があります
  - *parking_meter* は、1 ー 4294967295 秒の範囲の整数である必要があります
- **credit-control-group** *cc_group_name*：このルールベースで使用されるオンライン課金のパラメータを設定します。 *cc_group_name* は 、1 ～ 63 文字の英数字の文字列である必要があります。
- **dynamic-rule order**：ルールベース内のスタティックルールに対するダイナミックルールの照合の順序を構成します。
- **egcdr threshold { interval** *interval* **[ regardless-of-other-triggers ] | volume { downlink | total | uplink } bytes }**：オフライン充電のしきい値を構成します。
  - *interval* は、60 ～ 40000000 の範囲の整数である必要があります。

- **downlink** は、100000 ～ 4000000000 の範囲の整数である必要があります。デフォルト：4000000000。
- **uplink** は、100000 ～ 4000000000 の範囲の整数である必要があります。デフォルト：4000000000。
- **total** は、100000 ～ 4000000000 の範囲の整数である必要があります。

- **route priority** *route_priority* **ruledef** *ruledef_name* **analyzer { dns | file-transfer | ftp-control | ftp-data | h323 | http | imap | mipv6 | mms | pop3 | pptp | radius | rtcp | rtp | rtsp | sdp | secure-http | sip [ advanced | basic-and-advanced ] | smtp | tftp | wsp-connection-less | wsp-connection-oriented } [ description** 説明 **]**：このコマンドは UPF でのみ使用されます。
  - *route_priority* は、0 ー 65535 の範囲の整数である必要があります。
  - *ruledef_name* は、1 ～ 63 文字の英数字の文字列である必要があります。
- **tcp check-window-size**：このコマンドは UPF でのみ使用されます。
- **tcp mss** *tcp_mss*：このコマンドは UPF でのみ使用されます。 *tcp_mss* は 496 ～ 65535 の範囲の整数である必要があります。
- **tcp packets-out-of-order { timeout** *timeout_duration* **| transmit [ after-reordering | immediately ] }**：このコマンドは UPF でのみ使用されます。
  - *timeout_duration* は 100 ～ 30000 の範囲の整数である必要があります。デフォルト値は 5000 です。

## DNN プロファイル構成での UPF APN プロファイルの定義

既存の DNN プロファイルで UPF APN プロファイルを構成するには、次の構成例を使用します。

```
config
  profile dnn dnn_profile_name
    upf apn apn_name
    end
```

注：

- **upf apn** *apn_name*：UPF APN プロファイル構成を有効にします。このプロファイルは、既存の DNN プロファイル構成で構成されます。 *apn_name* は 、1 ～ 62 文字の英数字の文字列である必要があります。

## QoS パラメータの構成

QoS パラメータを構成するには、次の構成例を使用します。

```
config
  profile qos qos_profile_name
    ambr { ul uplink_ambr | dl downlink_ambr }
```

```
arp { preempt-cap preemption_capability |
preempt-vuln preemption_vulnerability |
priority-level priority_level }
max data-burst burst_volume
priority qos_priority
qi5 5qi_value
exit
```

注：

- **ambr { ul** *uplink_ambr* **| dl** *downlink_ambr* **}**：アップリンク（サブスクライバからネットワーク）およびダウンリンク（ネットワークからサブスクライバ）トラフィックの集約最大ビットレート（AMBR）を定義します。
- **arp preempt-cap** *preemption_capability*：プリエンプション機能フラグを指定します。次のオプションがあります。
  - MAY_PREMPT：ベアラーがプリエンプション処理される可能性がある。
  - NOT_PREMPT：ベアラーをプリエンプトできない。
- **arp preempt-vuln** *preemption_ulnerability*：プリエンプション脆弱性フラグを指定します。次のオプションがあります。
  - PREMPTABLE：ベアラーがプリエンプション処理される可能性があります。
  - NOT_PREMPTABLE：ベアラーをプリエンプトできません。
- **arp priority-level** *priority_level*：サービス データの割り当てと保持の優先順位（ARP）を定義します。 *priority_level* のデフォルト値は 8 です。
- **max data-burst** *burst_volume*：最大データ バースト ボリュームを定義します。 *burst_volume* は 1 ～ 4095 の範囲の整数である必要があります。
- **priority** *qos_priority*：5QI 優先順位レベルを指定します。 *qos_priority* は 、1 ー 127 の範囲の整数である必要があります。
- **qi5** *5qi_value*：承認された QoS パラメータの 5G QoS 識別子（5QI）を指定します。*5qi_value* は 0 ～ 255 の範囲の整数である必要があります。

## 静的 PCC ルールのサポート機能構成の確認

この項では、静的 PCC ルール サポート構成を確認する方法について説明します。

機能構成の詳細を確認するには、以下のコマンドを使用します。

**show full-configuration**

次に、この show コマンドの出力例を示します。

```
active-charging service acs
charging-action ca1
  arp priority-level 15 preempt-cap MAY_PREEMPT preempt-vuln PREEMPTABLE
  cca charging credit preemptively-request
  content-id 320001
```

```
  flow limit-for-bandwidth direction uplink peak-data-rate 1000000 peak-burst-size 1000000
 violate-action discard committedDataRate 2000000 committed-burst-size 2000000
exceed-action lower-ip-precedence
  nexthop-forwarding-address fa00:965a:c263:25::16/128
  qos-class-identifier 9
  service-identifier 32000
  tft packet-filter pf1
  tft-notify-ue
  tos af11 downlink
rulebase rb1
  cca quota time-duration algorithm parking-meter 1000 content-id 18000
  credit-control-group cg1
  dynamic-rule order first-if-tied
  egcdr threshold volume total 400000
  tcp packets-out-of-order transmit immediately
  action priority 95 timedef ruledef rd6 charging-action ca6 description ruledef
  action priority 96 ruledef rd3 charging-action ca5
  action priority 97 group-of-ruledefs grd3 charging-action ca4 monitoring-key 200000
  action priority 98 static-and-dynamic group-of-ruledefs grd2 charging-action ca2
  action priority 99 dynamic-only ruledef rd1 charging-action ca1 monitoring-key 100000
  action priority 100 dynamic-only group-of-ruledefs grd1 charging-action ca1
monitoring-key 100000 description gruledefs
  route priority 1 ruledef rd1 analyzer dns description dns
exit
packet-filter pk1
  direction uplink
  ip local-port = 23
  ip protocol = 23
  ip remote-address = 209.165.201.0/27
  ip remote-port = 23
  ip tos-traffic-class = 23 mask = 10
  priority  4
exit
ruledef prepaidBgl
  multi-line-or all-lines
  rule-application charging
  ip any-match = TRUE
  ip server-ip-address range host-pool 12
  ip dst-address = 209.165.201.10
exit
urr-list urrlocal
  rating-group 1 service-identifier 1 urr-id 2
  rating-group 1 service-identifier 3 urr-id 2
exit
exit
```

group-of-ruledefs の構成の詳細を確認するには、次のコマンドを使用します。

**show running-config**

次に、この show コマンドの出力例を示します。

```
show running-config
profile network-element pcf pcf1
rulebase-prefix   rbn
predefined-rule-prefix cbr
!
active-charging service acs1
group-of-ruledefs IPV6-whtlst-https_2300
  add-ruledef priority 1 ruledef IPV6-whtlst-https_2300_01
  add-ruledef priority 2 ruledef IPV6-whtlst-https_2300_02
  add-ruledef priority 3 ruledef IPV6-whtlst-https_2300_03
  add-ruledef priority 4 ruledef IPV6-whtlst-https_2300_04
  add-ruledef priority 5 ruledef IPV6-whtlst-https_2300_05
```

```
  add-ruledef priority 6 ruledef IPV6-whtlst-https_2300_06
  add-ruledef priority 7 ruledef IPV6-whtlst-https_2300_07
  add-ruledef priority 8 ruledef IPV6-whtlst-https_2300_08
  add-ruledef priority 9 ruledef IPV6-whtlst-https_2300_09
  add-ruledef priority 10 ruledef IPV6-whtlst-https_2300_10
  add-ruledef priority 11 ruledef IPV6-2dns-whtlst-https_2300_01
  add-ruledef priority 12 ruledef IPV6-2dns-whtlst-https_2300_02
  add-ruledef priority 13 ruledef IPV6-2dns-whtlst-https_2300_03
exit
group-of-ruledefs rdg1
  add-ruledef priority 10 ruledef rd2
  add-ruledef priority 12 ruledef rd1
exit
exit
```

# 定義済み PCC ルール

## 機能説明

静的 ルールに適用される概念のほとんどが、事前定義されたルールにも適用されます。構成セット、QoS バインディングのメカニズム、および事前構築された QoS モデルは同じままです。

**Important** 事前定義された PCC ルールは、4G コールと 5G コールの両方に適用できます。

### 定義済みルール vs 静的ルール

この項では、事前定義済みルールとスタティック ルールの相違点を示します。

- 定義済みルールは、ルールベース構成の下の ruledef に関連付けられたアクション優先順位の **dynamic-only** キーワードで識別されます。
- 事前定義されたルールは自動的にアクティブになりませんが、ルールごとに PCF によって有効または無効にされます。PCF は、事前定義されたルールをアクティブにするために、ruledef 名だけで、または ruledef とルールベース名をルール ID として一緒に持つ PCC ルールを送信し、以前にアクティブになった ruledef の null エントリを含む PCC ルールマップを送信して、事前定義されたルールを非アクティブにします。
- 静的ルールとは異なり、構成時に定義済みルールに対して QoS バインディングおよびモデリングは行われません。代わりに、PDUセッションのアクティブ化または変更中に、アクティブ化された ruledef の ECS 構成がセッションに適用可能な QoS モデルを作成または変更するために考慮されます。
- N4インターフェイスでは、PCF によってアクティブ化されたルール定義ごとに 1 つの PDR および対応する FAR が、事前定義されたルール IE のアクティブ化とルールベース名を使用して UPF に送信され、デフォルト PDR のルールベース IE で送信されます。ルールの削除時には、対応する PDR が削除されます。

**Note** PCF は事前定義されたルールを送信し、UPF APN に「ルールベース」名が構成されている場合にのみこれらのルールをアクティブにします。それ以外の場合、PCF はルール名を「ルールベース」名とともに送信する必要があります。

### 静的ルール、事前定義済みルール、動的なルールの組み合わせアプリケーション

3 つの静的ルール、事前定義済みルール、ダイナミック ルールはすべてセッションで共存できます。このような場合は、次の手順に従います。

- 事前構築された QoS モデルは、静的ルール専用に準備されています。PDU セッションのアクティブ化/変更中に、ダイナミックな事前定義されたルールが QoS モデルを変更するために評価され、それに応じて N1、N2、および N4 インターフェイスで変更が行われます。
- ダイナミック ルールのレーティング グループとサービス ID が、構成済みの事前定義済みルールと静的ルールのものと同じである場合、静的ルールと事前定義済みルールの URR ID は、ダイナミックルールに対しても保持されます。

# ベアラー QCI サポート

## 機能説明

インライン サービスをサポートするためにユーザープレーン機能（UPF）には、5G の QFI や 4G のベアラー ID、5G QoS 識別子（5QI）の割り当てと保持の優先順位（ARP）、および課金 ID など、各 QoS フローのベアラーレベル情報（BLI）が必要です。ベアラー QCI サポート機能は、SMF でこの要件を満たします。

**Note** ベアラー QCI サポート機能には、「PDR の作成」メッセージの Bli_ID と QFI 値のサポートも含まれています。

SMF は、PFCP セッション確立要求および PFCP セッション変更要求で、シスコ独自の IE であるベアラー QoS クラス識別子（QCI）情報要素（IE）を送信します。UPF は削除指示を暗黙的に提示します。BLI ID がどの PDR にも関連付けられなくなった場合、UPF はその ID を PFCP セッション コンテキストから削除します。UPF は、EDR に 5QI または QCI 値を追加します。現在、5G では [ベアラー QCI（Bearer QCI）] フィールドを使用して 5QI を追加します。

BLI は、次の表に示すように、UPF に報告されます。これらの IE の形式およびエンコーディングとデコーディングは、 *TS 29.244*で説明されている他の 3GPP IE と同じです。

| 情報<br>要素 | 必須<br>またはオプション | データ型 | 説明 |
|---|---|---|---|
| valid | | guint8 | ベアラー レベル情報 IE の有効性 |
| bli_id | 必須 | PfcpBliId | 5G またはベアラー ID（4G）の QoS フロー識別子（QFI） |
| qci | オプション | PfcpQci | PGW-C で使用され、SMF とは関連性がありません |
| _5qi | オプション | Pfcp5qi | QoS フローに関連付けられた 5QI |
| arp | 必須 | PfcpArp | ARP は、プリエンプション機能、プリエンプション脆弱性、および優先度レベルで構成されます。 |
| charging_id | オプション | PfcpChargingId | QoS フローまたはベアラー（またはその両方）に関連付けられている課金 ID。 |

### ベアラーレベル 情報 ID

SMF から送信された各ベアラー レベル情報の固有 ID。この IE の推奨値は QFI（5G 単位）または Bearer-id（4G 単位）です。IE の形式は次のとおりです：

| | ビット | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Octets** | **8** | **7** | **6** | **5** | **4** | **3** | **2** | **1** |
| 1 ～ 2 | タイプ = 232（10 進数） | | | | | | | |
| 3 ～ 4 | 長さ = 1 | | | | | | | |
| 5 | BLI_ID 値 | | | | | | | |
| 6 ～ n+4 | これらのオクテットは、明示的に指定されている場合にのみ存在します。 | | | | | | | |

**QCI**： 5G には適用されません。必要に応じて CUPS で使用されます。

| | ビット |
|---|---|

| Octets | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 ～ 2 | タイプ = 233（10 進数） | | | | | | | |
| 3 ～ 4 | 長さ = 1 | | | | | | | |
| 5 | QCI 値 | | | | | | | |
| 6 ～ n+4 | これらのオクテットは、明示的に指定されている場合にのみ存在します。 | | | | | | | |

**5QI**： SMF はこの IE を使用して 5QI 値を送信します。

| | ビット | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Octets | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
| 1 ～ 2 | Type = 234（10 進数） | | | | | | | |
| 3 ～ 4 | 長さ = 1 | | | | | | | |
| 5 | 5QI 値 | | | | | | | |
| 6 ～ n+4 | これらのオクテットは、明示的に指定されている場合にのみ存在します。 | | | | | | | |

**ARP**： ARP 値はこの IE とともに送信されます。

**Note** SMF から、ARP 値は arp->pci)<<4) | arp->pl)<< 2)| arp->pvi)

| | ビット | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Octets | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
| 1 ～ 2 | タイプ = 235（10 進数） | | | | | | | |
| 3 ～ 4 | 長さ = 1 | | | | | | | |
| 5 | ARP 値 | | | | | | | |
| 6 ～ n+4 | これらのオクテットは、明示的に指定されている場合にのみ存在します。 | | | | | | | |

**[Charging ID]**： Charging IE はこの IE とともに送信されます。

| | ビット | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Octets | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
| 1 ～ 2 | タイプ = 236（10 進数） | | | | | | | |
| 3 ～ 4 | 長さ = 1 | | | | | | | |

| | |
|---|---|
| 5 | 課金 ID 値 |
| 6 ～ n+4 | これらのオクテットは、明示的に指定されている場合にのみ存在します。 |

**ベアラー レベル情報 IE のトリガー**

PFCP メッセージで BLI IE を送信するためのトリガーは次のとおりです。

**PFCP セッション確立メッセージ**

ベアラーレベル情報 IE は、一意の QFI ID を持つ新しい QoS フローごとに送信されます。この IE は、PCF からの N7 ポリシー制御作成応答メッセージのポリシー決定で追加されます。したがって、SMF は、単一の PFCP メッセージで、この IE の複数のインスタンスを送信します。

**PFCP セッション変更メッセージ**：

新しい QoS フローが追加されたか、既存の QoS フローを参照する新しい PCC ルールにより、一意の QFI ID ごとに新しいベアラー レベル情報 IE を持つ新しい QER または PDR IE が生成されます。

変更が IDFT トンネルに対するものである場合、BLI IE は PFCP セッション変更メッセージに含まれません。

# ダイナミック PCC およびセッション ルールの非標準 QCI サポート

## 機能説明

SMF は、標準 QCI 値とともに、ダイナミック PCC およびセッション ルールで非標準 QCI 値をサポートします。

非標準 QCI は、1 から 255 までの値であり、3GPP 23.203 仕様のセクション 6.1.7.2 で定義されている標準 QCI 値の一部ではありません。

SMF は、セッションのデータ パケットの DSCP マーキングに非標準 QCI をサポートします。

**重要** SMF は、静的ルールおよび事前に定義されたルールの非標準 QCI 値の CLI ベースの構成をサポートしていません。PCF が非標準 QCI を使用してセッションルールを送信すると、SMF は、デフォルトフローに属する静的ルールおよび事前定義済みルール用に非標準 QCI 値を予約します。

# 機能の仕組み

SMF は、SmPolicyCreateResponse、SmPolicyUpdateResponse、または SmPolicyUpdateNotify メッセージを介して、PCF から QoS の非標準および標準 QCI を受信します。

PCF がセッション ルール情報を送信しない場合、または PCF が無効な QCI 値を送信する場合、SMF は UDM によって提供される非標準の QCI 値を使用し、PCF によって送信された場合と同じ方法で QCI 情報を処理します。PCF も UDM も非標準 QCI 情報を送信しない場合、SMF は QoS プロファイル内でローカルに構成された QCI 情報を使用します。構成詳細については、QoS パラメータの構成 （1295 ページ） セクションを参照してください。

PCF が非標準 QCI を使用して PCC ルールを送信すると、SMF は（UL および DL）GBR QoS 情報が関連付けられた QoS 記述子で使用可能な場合は GBR フローを作成します。そうでない場合、SMF は非 GBR フローを作成します。

デフォルトのセッション ルールの場合、SMF は PCF から受信する非標準 QCI 情報に関係なく、非 GBR フローと見なします。

SMF は、RAN または UE に対するセッションの確立または変更手順を開始し、N1、N2、N4、および S5 インターフェイスで同じ QCI 情報を伝達します。

（注） SMF は、非標準 QCI の PCF によって送信された QoS 特性を処理しません。

PCF からの QCI 入力に不一致またはあいまいさが生じた場合、SMF は次の検証を実行します。

- SMF は QCI 値が 1 ～ 255 の範囲内であるかどうかを確認します。SMF では、指定された範囲外の非標準 QCI 値は処理されません。
- PCF が、次の例に示すように、GBR UL および DL 情報とともに、同じバインディング パラメータと非標準 QCI を使用してセッションルールと PCC ルールを送信すると、SMF は「PccRule1」PCC ルールを拒否します。

```
sessRule1=>AuthDefQos{arp1, qci128}+ authSessAmbr{UL=20mbps,DL=20mbps}
PccRule1=>QosDesc{arp1, qci128, gbrUL=10mbps, gbrDL=10mbps}
```

## 制限事項

非標準 QCI サポート機能には次の制限があります。

- SMF は、セッション ルール フローを非標準 QCI の非 GBR フローと見なします。
- SMF は、非標準 QCI の PCF によって送信された QoS 特性を処理しません。

# OAM サポート

ここでは、この機能の操作、管理、およびメンテナンスに関して説明します。

### 統計情報サポート

SMF では、非標準 QCI の既存のポリシー統計情報が使用されます。標準 QCI 値を表示する QCI ラベルには、非標準 QCI 値も表示されます。

## トラブルシューティング情報

非標準 QCI 値に関連付けられたフロー情報を表示するには、標準 QCI 値に使用されるものと同じ **show subscriber 5qi** CLI コマンドを使用します。

既存の **clear subscriber 5qi** CLI コマンドを使用して、非標準 QCI 値を持つフローも削除します。

# 帯域幅 ID の構成のサポート

## 機能説明

SMF は、帯域幅制限設定がすべての課金アクションで同じであっても、すべての課金アクションで、ユーザがダウンリンク パケットとアップリンク パケットの両方に帯域幅制限を設定することを想定しています。

これらの設定を最適化するために、SMF では、ユーザーが帯域幅 ID を定義してすべての帯域幅関連の設定を含め、課金アクションで帯域幅 ID を関連付けることができます。

帯域幅の値が変更されると、新しいサブスクライバは設定された帯域幅の値を使用し、既存のサブスクライバは古い値を使用し続けます。

## 制限事項

SMF では、bandwidth-policy の構成に関連する次の制限があります。

- 帯域幅ポリシー内で最大 64,000 のフロー ID を構成可能
- 最大 64 個の帯域幅ポリシーを構成可能
- 構成できる電話機の最大数は 1000 です。
- 帯域幅ポリシーごとに構成できる帯域幅 ID の最大数は 1000 です。

## 帯域幅 ID の構成

課金アクション内で帯域幅 ID を定義するには、次の構成例を使用します。

```
config
  active-charging service service_name
    bandwidth-policy policy_name
```

```
    flow limit-for-bandwidth id bandwidth_id group-id group_id
    group-id group_id direction { downlink | uplink }
    peak-data-rate peak_data_rate peak-burst-size
    peak_burst_size violate-action { discard | lower-ip-precedence }
    [ committed-data-rate committed_data_rate committed-burst-size
    committed_burst_size [ exceed-action { discard | lower-ip-precedence
    } ] ]
    exit
active-charging service service_name
charging-action charging_action_name
    flow limit-for-bandwidth bandwidth_id
    end
```

- **bandwidth-policy** *policy_name*：帯域幅ポリシーの名前を指定します。この CLI オプションでは、最大 64 の帯域幅ポリシーを構成できます。
- **flow limit-for-bandwidth id** *bandwidth_id*：事前定義されたルールとスタティック ルールの課金アクションにすべての帯域幅関連の構成を含めるように帯域幅 ID を定義します。

  *bandwidth_id* は 1 ～ 65535 の範囲の整数である必要があります。

（注） 帯域幅ポリシーごとに構成できる帯域幅 ID の最大数は 1000 です。

- 帯域幅 ID が構成され、個々のアップリンクおよびダウンリンクの帯域幅制限も課金アクションで構成されている場合、帯域幅 ID の構成が優先されます。
- **group-id** *group_id*：グループ ID を指定します。 *group_id* は 、1 ～ 65535 の範囲の整数である必要があります。

  グループ ID は、MBR や GBR などの QoS パラメータを識別します。各グループ ID は特定の帯域幅 ID にマッピングされます。
- 帯域幅ポリシーごとに構成できるグループの最大数は 1000 です。

## BGP リンク帯域幅構成の確認

帯域幅 ID 構成を確認するには、次の show コマンドを使用します：

**show config**

この show コマンドは、削除されている構成済みの帯域幅 ID などの無効な構成を特定するのに役立ちますが、課金アクションではまだ定義されています。このような無効な構成の場合、この show コマンドは次の出力例に示すように適切なエラーを表示します：

```
ERROR COMPONENT      ERROR DESCRIPTION
--------------------------------------------------------------------------------------------------
RuleBase        Default bandwidth policy does not exist in rulebase <rba1> for charging
 action <ca1> .Dropping ruleDef <rda1>
RuleBase        Default bandwidth policy does not exist in rulebase <rba6> for charging
```

```
 action <ca1>.Dropping ruleDef <rda60>
RuleBase        Default bandwidth policy does not exist in rulebase <rba6> for charging
 action <ca1>.Dropping ruleDef <rda61>
ChargingAction  Packet filter <pkt1234> configured for charging action <ca4> associated
 with rulebase <rb1> does not exist
BandWidthPolicy Uplink peak data rate less than commited data rate in charging action
<ca6>Dropping ruleDef <rd6>
```

# PCF の UE キャンペーン レポートの生成

## 機能説明

PCF は、PDU セッションのライフサイクル中に関連するポリシーをプロビジョニングするために、UE の場所、RAT タイプ、アクセス タイプ、およびその他の詳細を認識する必要があります。これを容易にするために、PCF が開始したポリシー更新手順中に、SMF は、PCF によって有効になったトリガに基づいて、応答メッセージで「UeCampingRep」属性を送信します。

SMF は、3GPP 仕様 29.512 で定義されている表 5.5.2.2-2 に従って、UeCampingRep を PCF に送信します。PCF で提供されたすべてのルールの検証が成功すると、SMF は更新応答メッセージで UeCampingRep を PCF に送信します。

いずれかのルールの検証が失敗した場合、SMF は、3GPP 仕様 29.512 の 4.2.3.2 セクションで定義されている「PartialSuccessReport」で ueCampingRep を送信します。

「UeCampingRep」IE のフィールドは、PCF によって設定された次のトリガに基づいて入力されます。

- アクセス タイプ（AC_TY_CH）
- RAT 変更（RAT_TY_CH）
- ユーザー ロケーションの変更（SAREA_CH）
- PLMN の変更（PLMN_CH）

SMF は、次の 3GPP タイマーをサポートしています：

- accessType
- ratType
- servingNetwork
- userLocationInfo

**重要** SMF は現在、ueTimeZone 属性をサポートしていません。

# UPF ノード選択

UPF 選択機能により、5GS および EPS コア ネットワークは UPF を選択して、ユーザー プレーンの遅延を軽減し、優先ベースの有用性を実現できます。

SMF は、PDU セッションのセットアップ中に適切な UPF を選択します。UPF の選択は、次のクエリ パラメータに依存します。

- DNN
- サブスクライバの場所
- ネットワーク スライス情報
- PDU セッション タイプ
- PDU サブスクリプション タイプ
- 優先順位
- 負荷
- 新しい無線（DCNR）とのデュアル接続

複数の UPF が UPF 選択基準を満たす場合、UPF 選択は優先順位と負荷に基づきます。負荷メトリック情報の場合、SMF は N4 インターフェイスを介して UPF からパケット転送制御プロトコル（PFCP）IE を取得します。障害処理サポートが存在し、N4 セッション確立が失敗した場合、SMF は次に負荷の少ない UPF を選択します。

ネットワーク オペレータは、この機能を活用して、優先順位、PDU セッション タイプなどに基づいてユーザー プレーン トラフィックを効率的に処理します。この機能は、複数の UPF にわたるユーザー プレーン接続の効果的なロード バランシングにも使用されます。

特定のサブスクリプション永久識別子（SUPI）に複数の UPF を使用できるシナリオでは、SMF は各 SUPI に複数の UP アドレスを構成する機能を提供します。SMF は SUPI 優先構成に基づいて特定の PDU セッションの UPF の選択を実行します。構成詳細については、UPF アドレスの構成, on page 1364 セクションを参照してください。

つまり、SMF は構成された SUPI 値のいずれかが現在の SUPI と一致するかどうかをチェックします。一致が成功した場合、SMF は使用可能なユーザー プレーン ノードに関する情報を使用し、IP アドレスが SUPI に構成された値のいずれかと一致するかどうかを確認します。SMF は、UPF 選択のために次の検証を実行します。

- 稼働ノードが有効でアクティブであるかどうかを確認します
- 位置情報ベースの DNN または サービスから受信した DNN が、UPノードでサポートされている DNN のリストにあるか確認します
- 構成したユーザー プレーンで PDU セッション タイプがサポートされているかどうかを確認します。この検証では、SMF はネットワーク プロファイル UPF 内で構成された UP プロファイル名と UPF グループを取得します。次に、SMF は UPF グループが空であるかど

うか、またはサポートされている PDU セッション タイプで使用可能な PDU セッション タイプがグループにあるかどうかを確認します。

すべての検証が成功すると、SMF は、クエリパラメータを含む既存の UPF 選択ロジックをスキップし、SUPI によって選択された UPF を使用します。SUPI に UPF アドレスが構成されていない場合、または前述の検証チェックが失敗した場合、SMF はデフォルトの UPF 選択メカニズムを使用します。共存 UPF 選択の場合、cnSGW-C 構成は SMF と同じままです。

# クエリ パラメータに基づく UPF の選択

このセクションでは、SMF が特定の選択パラメータに基づいて UPF を選択する方法について説明します。

## 機能説明

SMF は、事前定義されたクエリ パラメータに基づいて、すべてのアクティブな UPF のリストから UPF を選択します。

5GS および EPS コアネットワークは、サブスクライバ セッションの作成中に、選択メカニズムを適用して UPF ノードを選択します。

UPF の選択が UPF の負荷に基づいている場合、SMF は、SMF に関連付けられたアクティブな UPF 間でコールを分散します。3GPP では、N4 リファレンス ポイントにおけるオプション機能として、負荷制御機能が指定されています。この機能により、UPF はその負荷情報を CP 機能に送信できます。

負荷ベースの UPF 選択をサポートするために、SMF は次の Packet Forwarding Control Protocol（PFCP）メッセージで UPF が提供する負荷制御情報を使用します。

- セッション確立応答
- セッションの変更応答
- セッション削除応答
- セッション レポート要求

負荷制御手順の詳細については 、*3GPP TS 29.244*、リリース *14* の *6.2.3* 項を参照してください。SMF は CP 機能に準拠しています。

## 機能の仕組み

UPF は、SMF との関連付けを設定するために、N4 関連付けセットアップ要求を開始します。

次に、SMF がコア ネットワークの UPF ノードを選択する方法の概要を示します：

- SMF は、DNN プロファイル構成で構成された UPF 選択ポリシーに基づいて、EPS および 5GS セッションの UPF ノードを選択します。UPF 選択ポリシーは、次のパラメータの組み合わせを定義します：
  - DNN

- ネットワーク スライス
- サブスクライバ ロケーション
- DCNR（EPS コールのみ）
- サブスクリプション タイプ
- PDN/PDU セッション タイプ

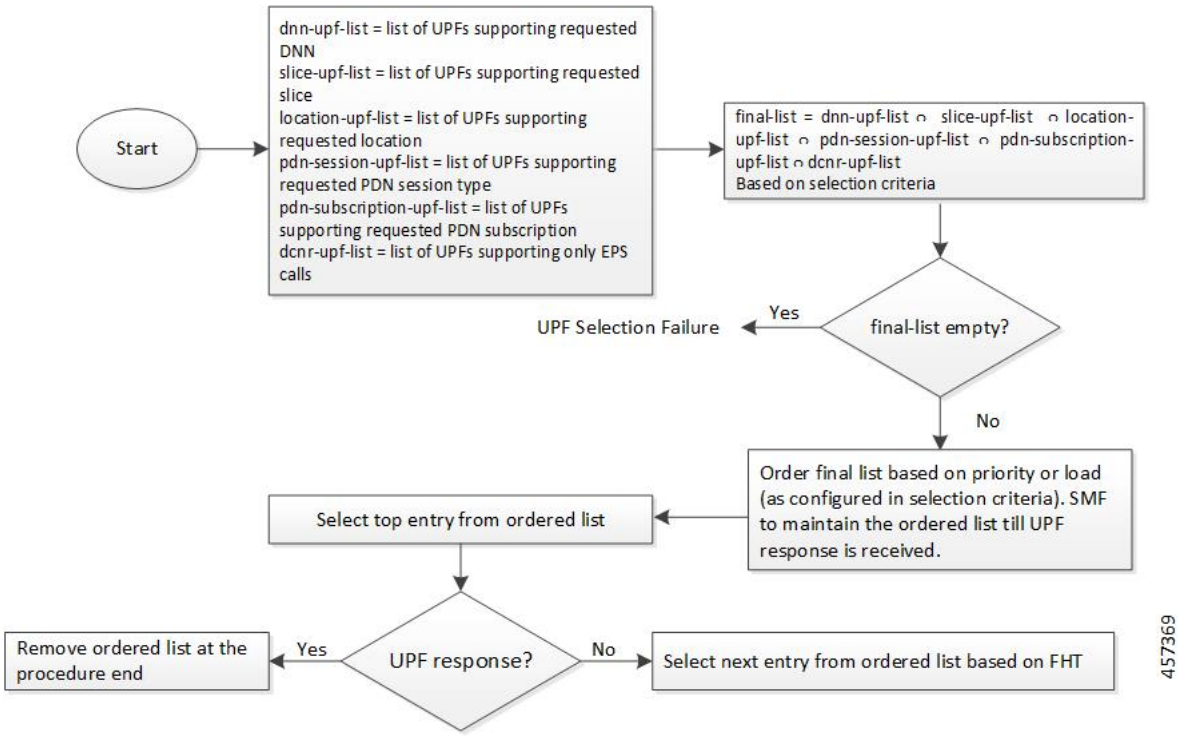
- UPF 選択ポリシーが DNN プロファイルの構成で定義されていない場合、SMF は取得したロケーションの DNN または 要求された DNN に基づいて UPF を選択します。
- SMF では、適切なノードをクエリするために使用する UPF 選択基準を定義できます。
- 複数の UPF が選択基準に一致する場合、SMF はアクティブな UPF を選択し、優先順位と負荷情報に基づいてそれらをソートします。次に、SMF は N4 セッション確立が成功するまで、UPF へのアクセスを 1 つずつ試行します。
- SMF は、UPF によって提供された負荷情報を保存し、新しいセッションの UPF の選択に使用します。SMF は、（DNN ベースの）アクティブ UPF 候補の中から負荷の少ない UPF を選択します。
- SMF は、各 UPF に対して静的に構成された優先順位とキャパシティを考慮します。UPF が負荷情報を静的に送信しない場合、SMF は構成された容量を使用して UPF を選択します。
- SMF は、特定の場所でより優先される UPF を選択します。UPF の最終的なプライオリティは、UPF のプライオリティと UPF グループのプライオリティの両方を使用して決定されます。UPF グループの優先順位の構成については、UPF グループへの優先順位の割り当て, on page 1361 セクションを参照してください。

## UPF 選択アルゴリズム

SMF は、アルゴリズムに基づいて UPF ノードを決定します。

次の図は、UPF ノードの選択ワークフローを示しています。

*Figure 228: UPF* ノード選択ワークフロー




SMF は、ノードに割り当てられた優先順位に基づいて UPF ノードをリストします。同じ優先順位値を持つ複数のノードがある場合、SMF は負荷レベルが最も低い UPF を選択します。負荷パラメータは、同じ優先順位を持つ UPF にのみ適用されます。

負荷を選択基準として使用できない場合、同じ優先順位を持つ複数の UPF がある場合、SMF はランダムな UPF を選択します。

SMF は、優先順位に基づいて UPF の順序リストを保存します。障害が発生すると、SMF は障害処理テンプレート（FHT）の設定に基づいて、リスト内の次のエントリを選択します。

優先順位が選択基準として使用できず、負荷が選択基準として使用可能な場合、SMF は、選択された UPF のリストから最も負荷の小さい UPF を選択します。

**Important** SMF は、最初のコールの確立および引き継ぎ手順の実行時に UPF の選択を実行します。

サブスクライバの場所が UPF 選択パラメータとして使用される場合、SMF は UPF および UPF グループに設定された優先順位を使用して最適な UPF を選択します。

次に、UPF の選択ロジックを理解する例を示します。

次の構成で、2 つの UPF グループと 2 つの UPF を想定します。

- UPF グループ：
  - UpfGrp1：

- ロケーション エリア グループ リスト：TAI1
- スライス リスト
- PDN タイプのリスト

- UpfGrp2：
  - ロケーション エリア グループ リスト：TAI2
  - スライス リスト
  - PDN タイプのリスト

- UPF
  - Upf1：
    - 優先順位：500
    - キャパシティ：1000
    - Upf Grp リスト：（UpfGrp1、優先順位：10）、（UpfGrp2、優先順位：30）
  - Upf2：
    - 優先順位：500
    - キャパシティ：1000
    - Upf Grp リスト：（UpfGrp1、優先順位：20）、（UpfGrp2、優先順位：5））

UPF グループの優先順位と UPF の優先順位の組み合わせは、特定の場所で優先度の高い（優先度の低い）UPF を選択するために使用されます。

SMF は、upf1 の優先順位が低いため、ロケーション TAI1 に upf1 を選択します。同様に、UPF 優先順位と UPF グループ優先順位に基づいて、TAI2 には upf2 が選択されます。

SMF は、UE ロケーション、つまり TAI または ECGI に基づいて DNN プロファイルを構成する機能も提供します。ロケーションベースの DNN プロファイルにより、ロケーション エリア グループが TAI または ECGI グループを指定する DNN プロファイルとロケーション エリア グループをマッピングできます。

TAI ベースの UPF の選択では、最初に location-dnn-profile 構成を介して UE ロケーションに基づいて DNN プロファイルを選択する必要があります。次に、選択した DNN プロファイルで定義されている UPF 選択ポリシー（DNN やスライスの選択基準など）を使用します。

構成詳細については、ロケーションベースの DNN プロファイルの選択, on page 1362 セクションを参照してください。

## 標準準拠

ロードベース UPF 選択機能は、以下の基準に準拠しています。

- *3GPP TS 29.244* リリース *14*：*LTE*。*EPC* ノードの制御プレーンとユーザー プレーン間のインターフェイス

### 制限事項

ロードベースの UPF 選択機能には、次の制限があります：

- nodemgr POD の再起動後、後続の PDU セッションの確立を正常に行うには、UPF アソシエーションを再確立する必要があります。

## UPF 選択機能の構成

ここでは、UPF 選択方法の構成方法について説明します。

UPF の選択は、クエリ パラメータによって異なります。選択したクエリ パラメータに基づいて、次の構成を使用します。

- EPS の ECGI グループ プロファイルの作成, on page 1353
- 5GS の NCGI グループ プロファイルの作成, on page 1354
- トラッキング エリア ID グループの構成, on page 1355
- ロケーション エリア グループ プロファイルの作成, on page 1356
- UPF グループの定義, on page 1357
- UPF グループと UPF ネットワーク要素との関連付け, on page 1358
- UPF 選択クエリ パラメータの定義, on page 1359
- UPF 選択クエリ パラメータと DNN プロファイルの関連付け, on page 1360
- UPF アドレスの構成, on page 1364

### EPS の ECGI グループ プロファイルの作成

このセクションでは、ECGI グループ プロファイルのインスタンスを作成する方法について説明します。

ECGI グループ プロファイルを使用すると、個々の ECGI 値と範囲のリストを設定できます。

ECGI グループを作成するには、次の設定例を使用します。

```
config
  profile ecgi-group profile_name
    mcc mcc_value mnc mnc_value
    ecgi list [ ecgi_value1 ecgi_value2 ecgi_valueN ]
    ecgi range start start_value end end_value
    end
```

注：

- **profile ecgi-group** *profile_name* ：プロファイル構成を入力するロケーション エリア グループの名前を指定します。ECGI グループプロファイルでは、最大 16 の PLMN がサポートされます。
- **mcc** *mcc_value* **mnc** *mnc_value*：MCC および MNC 値を指定します。
- **ecgi list [** *ecgi_value1 ecgi_value2 ecgi_valueN* **]**：設定する ECGI 値のリストを指定します。受け入れられる値は、7 桁の 16 進文字列の E-UTRAN セル ID です。SMF では、PLMN で最大 64 の ECGI 値がサポートされています。
- **ecgi range start** *start_value***end** *end_value* ： ECGI 範囲の開始値と終了値を指定します。ECGI で指定できる開始と終了の範囲は、7 桁の 16 進文字列の E-UTRAN セル ID です。 **ecgi range** はオプション属性です。複数の ECGI 範囲値を構成できます。SMF は、PLMN の下で最大 64 の ECGI 範囲をサポートします。

**Important** 範囲開始値が終了範囲値より大きい場合、SMF は ECGI 範囲値を無視します。

### *ECGI* グループ プロファイルの作成の確認

このセクションでは、ECGI グループ プロファイルが作成されているかどうかを確認する方法について説明します。

次に、**show running-config profile ecgi-group** コマンドの出力例を示します。

```
profile ecgi-group e1
mcc 123 mnc 45
  ecgi list [ 1234567 abcdef0 ]
  ecgi range start 1111111 end fffffff
  exit
exit
exit
```

## 5GS の NCGI グループ プロファイルの作成

このセクションでは、NCGI グループ プロファイルのインスタンスを作成する方法について説明します。

NCGI グループ プロファイルを使用すると、個々の NCGI 値と範囲のリストを構成できます。

GTPP グループの構成するには、次の構成例を使用します。

```
config
  profile ncgi-group profile_name
    mcc mcc_value mnc mnc_value
    ncgi list [ ncgi_value1 ncgi_value2 ncgi_valueN ]
    ncgi range start start_value end end_value
    end
```

注：

- **profile ncgi-group** *profile_name* ：プロファイル構成を入力する NCGI グループ プロファイルの名前を指定します。NCGI グループ プロファイルでは、最大 16 の PLMN がサポートされます。
- **mcc** *mcc_valuemnc_value* **mnc** ：MCC と MNC の値を指定します。
- **ncgi list [** *ncgi_value1 ncgi_value2 ncgi_valueN* **]**：構成する NCGI 値のリストを構成します。受け入れられる値は、9 桁の 16 進文字列の NR セル ID です。SMF では、PLMN の下で最大 64 の NCGI 値をサポートしています。
- **ncgi range start** *start_value* **end** *end_value*：特定の NCGI 範囲または複数の NCGI 範囲のリストを構成します。許容される開始と終了の範囲は、9 桁の 16 進文字列 NR Cell ID です。**ncgi range** はオプション属性です。複数の NCGI 範囲値を構成できます。SMF は、PLMN の下で最大 64 の NCGI 範囲をサポートします。

**Important** 開始範囲の値が終了範囲の値より大きい場合、SMF は NCGI 範囲の値を無視します。

### *NCGI* グループ プロファイルの作成の確認

このセクションでは、NCGI-Group プロファイルが作成されているかどうかを確認する方法について説明します。

次に、**show running-config profile ncgi-group** コマンドの出力例を示します。

```
profile ncgi-group n1
mcc 123 mnc 45
  ncgi list [ 123456789 12ab34CD9 ]
  ncgi range start 111111111 end FFFFFFFFF
  exit
exit
exit
```

## トラッキング エリア ID グループの構成

SMF は、PLMN のトラッキング エリアとトラッキングエリア範囲のサポート対象リストを定義するための構成を提供します。この構成を有効にすると、SMF は、SMF サービス登録時に、構成されたトラッキング エリア ID（TAI）を NRF に送信します。

異なる名前で複数の TAI グループを定義するには、次の構成例を使用します。

```
config
  profile tai-group tai_group_name
    mcc mcc mnc mnc
    tac list [ tac_value1 tac_value2 tac_valueN ]
    tac range start tac_start_value end tac_end_value
    end
```

注：

- **profile tai-group** *tai_group_name*：プロファイル構成を入力する TAI グループの名前を指定します。

- **mcc** *mcc_value*：モバイル国コードを指定します。
- **mnc** *mnc_value*：モバイル ネットワーク コードを指定します。
- **tac list [** *tac_value1 tac_value2 tac_valueN* **]**：このキーワードを使用すると、次の構成を行うことができます。
  - 指定された TAI グループ内の複数の PLMN と TAC 値
  - 指定された TAI グループ内の最大 16 の PLMN
  - PLMN の TAC 値の最大数は 64 です
- **tac range start** *tac_start_value* **end** *tac_end_value*：このキーワードを使用すると、次を構成できます。
  - 複数の TAC 範囲値
  - PLMN の TAC 範囲の最大数は 64 です。

**重要** SMF は、範囲開始の値が終了範囲の値より大きい場合、TAC 範囲の値を無視します。

- SMF は、TAI グループまたは NCGI グループの構成から TAC リストと TAC 範囲を取得します。NCGI リストに TAC がすでに含まれている場合は、TAI グループの下の TAC 構成をスキップできます。ただし、TAC が別の UPF に関連付けられている場合、この動作は適用されません。

## ロケーション エリア グループ プロファイルの作成

SMF は、1 つ以上のサービス ロケーションの詳細をピア UPF に関連付けます。ロケーションの詳細には、オプションのサポートされているセルの詳細とともに、個々のトラッキング エリアおよび/またはトラッキング エリアの範囲が含まれます。

ecgi-group および ncgi-group に追加されるロケーション エリア グループ プロファイルのインスタンスを作成するには、次の構成例を使用します。

```
config
   profile location-area-group profile_name
      tai-group tai_group_name
      ecgi-group ecgi_group_name
      ncgi-group ncgi_group_name
      end
```

注：

- **profile location-area-group** *profile_name* ：プロファイル構成を入力するロケーション エリア グループの名前を指定します。
- **tai-group** *group_name*: TAI グループの名を指定します。

- **ecgi-group** *group_name*: ECGI グループの名を指定します。この設定は任意です。
- **ncgi-group** *group_name*：NCGI グループの名前を指定します。この設定は任意です。

ロケーション エリア グループ プロファイル作成の確認

このセクションでは、ロケーション エリア グループ プロファイルが作成されているかどうかを確認する方法について説明します。

次の構成は 、**show running-config profile location-area-group** コマンドの出力例です：

```
profile location-area-group la1
tai-group  t1
ecgi-group e1
ncgi-group n1
exit
```

## UPF グループの定義

ここでは、UPF グループを構成し、UPF グループ プロファイルの pdn-session-type、slice-group およびその他のパラメータを定義する方法について説明します。

UPF グループ プロファイルを定義するには、次の構成例を使用します。

```
config
  profile upf-group upfgroup_name
    pdn-session-type [ ipv4 | ipv4v6 | ipv6 ]
    dcnr { false | true }
    slice-group-list [ slice1 slice2 sliceN ]
    location-area-group-list [ la1 la2 laN ]
    end
```

注：

- **profile upf-group** *upfgroup_name*：指定された UPF ネットワーク構成に関連付ける必要がある UPF グループの名前を指定します。
- **pdn-session-type [ ipv4 | ipv4v6 | ipv4v6 ]**：UPF でサポートされる PDN セッション タイプを構成します。pdn-session-type のクエリパラメータは、「pdn-type-subscription」および「pdn-type-session」を受け入れます。このパラメータは、UDM で返されたサブスクリプションまたは UE セッションからそれぞれ pdn-type を選択します。

**Note** 「pdn-type-subscription」と「pdn-type-session」パラメータの両方が構成されている場合、SMF は、「pdn-type-subscription」が考慮されます。

SMF は、IPv4、IPv6、IPv4v6 などのさまざまな PDN セッションタイプにサービスを提供するように UPF を関連付ける次の CLI オプションを提供します。UPF は、複数の PDN セッション タイプにサービスを提供します。

- **slice-group-list [** *slice1 slice2 sliceN* **]**：構成されたネットワーク スライスの選択支援情報（NSSAI）リストを指定します。スライス値は、smf-profiles の allowedNsnai と同じである

必要があります。スライス グループには NSSAI 情報と DNN 情報の両方が含まれます。NSSAI UPF リストを取得するときは、スライス グループで構成されている DNN リストを考慮してください。ネットワーク要素の下にある既存の dnn-list は、upf-profile グループに移動されません。

- **dcnr { true | false }**：新しい無線（DCNR）機能を備えたデュアル接続を構成します。デフォルト構成は、false です。

**Note** DCNR 機能は、4G コールにのみ適用されます。

- **location-area-group-list [** *la1 la2 laN* **]**：異なる名前のロケーション エリア グループのリストを構成します。

### *UPF* グループ プロファイルの構成の確認

このセクションでは、UPF グループ プロファイルが構成されているかどうかを確認する方法について説明します。

以下の構成は、 **show running-config profile upf-group** *upfgroup_name* コマンドの出力例です：

```
profile upf-group ug1
pdn-session-type ipv4v6
slice-group-list [ slice1 ]
location-area-group-list [ loc1 ]
dcnr true
exit
```

### UPF グループと UPF ネットワーク要素との関連付け

定義された UPF グループを UPF ネットワーク要素に関連付けするには、次のサンプル構成を使用します。

UPF プロファイルには、SMF に設定されている UPF のリストが含まれています。

```
config
  profile network-element upf upf_name
     upf-group-profile upfgroup_name
     capacity service_capacity
     priority priority_value
     dnn-list dnn_list
     end
```

注：

- **profile network-element upf** *upf_name*：定義された UPF グループが関連付けられている UPF ネットワーク構成を構成します。
- **upf-group-profile** *upf_group*：指定された UPF ネットワーク構成に関連付ける必要がある UPF グループ名を構成します。

- **capacity** *service_capacity*：同じタイプの他の UPF に対する静的な重みを構成します。*server_capacity* は 、0 ～ 65535 の範囲の整数である必要があります。デフォルトは 10 です。
- **priority** *priority_value*：同じタイプの他の UPF に相対する静的優先順位を構成します。*priority_value* は 、0 ～ 65535 の範囲の整数である必要があります。デフォルトは 1 です。
- **dnn-list** *dnn_list*：UPF ノードでサポートされているロケーション DNN または、DNN を指定します。

### *UPF* 構成の確認

ここでは、UPF 構成と UPF グループと UPF ネットワーク要素との関連付けを確認する方法について説明します。

以下の構成は、 **show configuration** コマンドの出力例です：

```
profile network-element nrf nrf1
http-endpoint base-url http://209.165.200.253:8082
…
profile network-element upf upf2
upf-group-profile ug1
capacity 10
priority 1
n4-peer-address ipv4 209.165.200.234
n4-peer-port 8805
keepalive 60
dnn-list [ dnn1 intershat cisco.com ]
…
```

## UPF 選択クエリ パラメータの定義

このセクションでは、SMF が選択クエリを使用して UPF を選択できるようにするパラメータの構成方法について説明します。

UPF 選択ポリシー固有の構成を定義するには、次の構成例を使用します：

```
config
  policy upf-selection upfpolicy_name
    precedence priority_value [ dcnr | dnn | location | pdn-type-session
 | pdn-type-subscription | slice ]
    end
```

**注**：

- **policy upf-selection** *upfpolicy_name*：DNN プロファイルに関連付ける必要がある UPF ポリシーの名前を指定します。

  SMF は、優先順位値が最も低い UPF ノードを選択します。SMF は、以前の下位の優先順位の基準が UPF を返さない場合、優先順位の選択基準が最も高いノードを選択します。設定された基準がすべて使用され、ノードが選択されていない場合、UPF 選択ポリシーは失敗します。

  precedence 値内で、各基準の UPF の交差が実行されて UPF リストが取得されます。

- **precedence** *priority_value* **[ dcnr | dnn | location | pdn-type-subscription | pdn-type-session | slice ]**：precedence 値を UPF ポリシーに割り当てます。UPF 選択のための DNN およびその他のパラメータを指定します。

  **precedence** キーワードを使用すると、UPF 選択ポリシーの下で最大 4 つの precedence 値を構成できます。

  DNN プロファイルに UPF 選択ポリシーが関連付けられていない場合、SMF はロケーション DNN または DNN、優先度、および負荷情報を使用して UPF 選択を実行します。

### *UPF* 選択ポリシー構成の確認

このセクションは、UPF 選択ポリシーが構成されていることを確認する方法を説明します。

以下の構成は、 **show running-config policy upf-selection** コマンドの出力例です：

```
#show running-config policy upf-selection
policy upf-selection polUpf1
   precedence 1
         [dnn location pdn-type-subscription]
   exit
   precedence 2
         [dnn pdn-type-session slice]
   exit
   precedence 3
          [dnn]
   exit
exit
```

### UPF 選択クエリ パラメータと DNN プロファイルの関連付け

このセクションでは、UPF 選択クエリ パラメータを DNN プロファイルに関連付ける方法について説明します。

UPF 選択ポリシーを DNN プロファイルに関連付けるには、次の構成を使用します：

```
config
   profile dnn profile_name
      upf-selection-policy upfpolicy_name
      end
```

注：

- **profile dnn** *profile_name*：DNN プロファイル名を指定します。 *profile_name* は 英数字の文字列である必要があります。
- **upf-selection-policy** *upfpolicy_name*：DNN プロファイルに関連付ける必要がある UPF 選択ポリシーの名前を指定します。

### *UPF* 選択ポリシーと *DNN* プロファイルの関連付けの確認

このセクションでは、DNN プロファイルとの UPF 選択ポリシーの関連付けが確立されているかどうかを確認する方法について説明します。

以下の構成は、**show running-config profile dnn** *profile_name* コマンドの出力例です。

```
profile dnn intershat
upf-selection-policy upfPol1
end
```

## UPF グループへの優先順位の割り当て

ここでは、UPF グループ リストを構成し、UPF グループに優先順位を割り当てる方法について説明します。

UPF グループには、ロケーション、スライスなどのセットがリストされます。グループに存在する各 UPF には、その UPF の最終的な優先順位を決定する優先順位が与えられます。

UPF グループ 優先順位を割り当てるには、次の構成例を使用します。

```
config
  profile network-element upf upf_profile_name
    upf-group-profile-list upf_group_name
      priority priority_value
      end
```

注：

- **upf-group-profile-list** *group_name*：UPF グループ プロファイル名を指定します。
- **priority** *priority_value*：UPF グループに優先順位を割り当てます。

  UPF グループの優先順位は、同じロケーション（TAI）を持つ 2 つ以上の UPF があるシナリオで使用されます。

### 設定の確認

機能構成の詳細を確認するには、**show running-config profile network-element upf** コマンドを使用します。

**show running-config profile network-element upf** コマンドの出力例を次に示します。

```
[smf] smf# show running-config profile network-element upf
profile network-element upf upf1
 n4-peer-address ipv4 209.165.200.231
 n4-peer-port 8805
 dnn-list    [ intershat intershat1 intershat2 intershat3 intershat4 intershat5 intershat6
 intershat7 intershat_hrt intershatipex ]
 capacity     65535
 priority     65535
 upf-group-profile-list group1 priority 10
 upf-group-profile-list group2 priority 20
exit
```

上記の出力で、 **upf-group-profile-list group1 priority 10** および **upf-group-profile-list group2 priority 20** の行を確認して、UPF グループの構成と UPF グループの優先順位を表示します。

構成済みのすべての UPF グループを表示するには、 **show running-config profile upf-group** コマンドを使用します。

**show running-config profile upf-group** コマンドの出力例を次に示します。

```
[smf] smf# show running-config profile upf-group
profile upf-group group1
 failure-profile FH1
```

```
exit
profile upf-group group2
 failure-profile FH2
exit
```

## ロケーション ベースの DNN プロファイルの選択

DNN ポリシーには、UE が要求した各 DNN の UE ロケーションに基づいた DNN プロファイル構成を含めることができます。DNN プロファイルには、インターフェイスのリストを持つ仮想またはマッピングされた DNN があります。

ロケーションベースの DNN プロファイルを構成するには、次の構成例を使用します：

```
config
  policy dnn dnn_policy_name
    dnn dnn_name location-dnn-profile location_dnn_profile_name
    end
```

注：

- **dnn** *dnn_name* **location-dnn-profile** *location_dnn_profile_name*：UE ロケーションに基づいて定義される DNN プロファイルの名前を指定します。

  この構成により、UE 要求の DNN が DNN ポリシーのロケーションベースの DNN プロファイルにマッピングされます。

## ロケーション エリア グループと DNN プロファイルの関連付け

ロケーションエリア グループとロケーションベースの DNN プロファイルを関連付けるには、次の構成例を使用します：

```
config
  profile location-dnn location_dnn_profile_name
    location-area-group lag_name profile dnn_profile_name
    end
```

注：

- **profile location-dnn** *location_dnn_profile_name*：構成済みの DNN プロファイルの名前を指定します。
- **location-area-group** *lag_namednn_profile_name* **profile** ：ロケーション エリア グループと DNN プロファイルの名前を指定します。

  この構成により、ロケーションエリア グループが DNN プロファイルにマッピングされます。

設定例

次に、設定例を示します。

```
config
 policy dnn polDnn
  profile default-profile
  dnn ims location-dnn-profile loc1
```

```
exit
profile location-dnn loc1
 location-area-group lag1 profile dnnprof-imslag1
 location-area-group lag2 profile dnnprof-imslag2
 exit
profile location-area-group lag1
 tai-group tai1
 ecgi-group ecgi1
 exit
profile location-area-group lag2
 tai-group tai2
 ecgi-group ecgi2
 exit
profile tai-group tai1
 mcc 123 mnc 456
 tac range start 4455 end 5566
 exit
profile tai-group tai2
 mcc 123 mnc 456
 tac range start 3355 end 3366
 exit
exit
profile ecgi-group ecgi1
 mcc 123 mnc 456
 ecgi range start A123451 end A234567
 exit
exit
profile ecgi-group ecgi2
 mcc 123 mnc 456
 ecgi range start B123451 end B234567
 exit
exit
profile location-dnn loc1
 location-area-group lag1 profile dnnprof-imslag1
 location-area-group lag2 profile dnnprof-imslag2
 exit
profile dnn dnnprof-imslag1
 dns primary ipv4 209.165.201.10
 dns primary ipv6 fd00:976a::9
 dns secondary ipv4 209.165.201.12
 dns secondary ipv6 fd00:976a::10
 dnn imslag1 network-function-list [ upf ]
 dnn rmgr imslag1
 upf-selection-policy       upfsecpol1
 timeout up-idle 3600 cp-idle 7320
 pcscf-profile pcscf1
 session type IPV4V6
 upf apn ims
 dcnr true
 userplane-inactivity-timer 3600
 exit
profile dnn dnnprof-imslag2
 dns primary ipv4 209.165.201.13
 dns primary ipv6 fd00:976a::9
 dns secondary ipv4 209.165.201.14
 dns secondary ipv6 fd00:976a::10
 dnn imslag2 network-function-list [ upf ]
 dnn rmgr imslag2
 upf-selection-policy       upfsecpol2
 timeout up-idle 3600 cp-idle 7320
 pcscf-profile pcscf1
 session type IPV4V6
 upf apn ims
 dcnr true
```

```
   userplane-inactivity-timer 3600
   exit
  exit
 exit
exit
```

上記の例では、構成された DNN の名前は「ims」、location-dnn-profile は「loc1」、location-area-group は「lag1」および「lag2」、dnn-profile は「dnnprof-imslag1」および「dnnprof-imslag2」です。

SMF は、PDU セッション要求で受信した "ims" DNN に対して location-dnn-profile "loc1" を選択します。loc1 プロファイルは、location-area-group を dnn-profile にマップします。SMF は PDU セッション要求からの TAI および ECGI 情報を使用して、設定された location-area-group "lag1" を見つけます。次に、対応する dnn-profile "dnnprof-imslag1" を選択します。

"dnnprof-imslag1" の dnn プロファイルが選択されると、SMF は UPF 選択ポリシーで指定された選択基準に基づいて適切な UPF を選択します。

### UPF アドレスの構成

このセクションは、SUPI と UPF ノード情報を構成する方法を説明します。

SUPI 値と UPF アドレスを構成するには、次の構成例を使用します：

```
config
  system-diagnostics supi supi_value
    preferred-up node-id upf_address
    end
```

注：

- **system-diagnostics supi** *supi_value*：SUPI 値またはコンマで区切られた SUPI 値のリストを指定します。 *supi_value* は 15 桁の文字列である必要があります。
- **preferred-up node-id** *upf_address*：構成された SUPI の UPF アドレスをコンマで区切って指定します。 *upf_address* は 、IPv4 アドレス パターンの文字列である必要があります。

  複数の UPF が SUPI に構成されている場合、SMF は SUPI 優先構成に基づいて特定の PDU セッションの UPF の選択を実行します。

### 設定の確認

構成を確認するために、この **show running-config system-diagnostics supi** コマンドを使用します。

以下は、show コマンドの出力例です。

```
[smf] smf# show running-config system-diagnostics supi
system-diagnostics supi [ 123456789012345 ]
 preferred-up node-id [ 209.165.200.230 209.165.200.236 ]
exit
```

## UPF 選択 OA&M サポート

ここでは、この機能の操作、管理、およびメンテナンスに関して説明します。

### 統計

DNN、pdn-type-session、 ネットワーク スライス、 優先度、および負荷に基づく UPF ノード選択をサポートするために、次の統計が追加されました。

- upf-selector

  req_type="upf-selector",

  status="Precedence:2 Dnn-Upf-List:3 Pdn-Type-Upf-List:2 Slice-Upf-List:2 Dcnr-Upf-List:0"

  status="upf_selector_empty_upf_list"

  status="upf_selector_invalid_upf_selection_policy"

  例：

```
smf_service_resource_mgmt_stats{app_name="SMF",cluster="Local",
data_center="DC",dnn="intershat",emergency_call="",instance_id="0",ip_req_type
="upf-selector",pdu_type="ipv4",procedure_type="PDU Session Establishment",
rat_type="NR", service_name="smf-service", status="Precedence:2 Dnn-Upf-List:3
 Pdn-Type-Upf-List:2 Slice-Upf-List:2 Dcnr-Upf-List:0"} 1
```

# IP しきい値ベースの UPF の選択

## 機能説明

この機能は、過負荷状態の UPF 間のロード バランシングに対処します。各 IP プールには、既存の使用可能なしきい値構成があります。この構成では、特定の UPF のしきい値ヒットと見なされる IP アドレスの割合を指定できます。IPAM は、UPF の特定の DNN でしきい値がヒットすると SMF に通知します。SMF は、UPF がしきい値条件にヒットするまで、そのような UPF に低い優先順位を与えます。

### ユースケース

同じ DNN を提供し、異なる優先順位を持つ UPF は IP アドレスを均等に消費します。このような場合、特定の UPF では IP アドレスがすぐに不足し、しきい値に達することがあります。このような場合、SMF はまず新しいセッションの割り当て中にしきい値に達していない UPF を優先します。

フィールドでの非線形アクティビティにより、SMF による UPF への初期セッションの分布が均一である可能性があります。後続のセッションでは、1 つの特定の UPF がより長く残り、別の UPF がクリアされる場合があります。このような場合、新しいセッションは UPF の優先順位に基づいて配信を継続します。より長くコールが続くと、しきい値に達する可能性があり、UPF で IP アドレスが不足する場合があります。このような状況に対応するために、UPF のしきい値の優先順位は低くなります。

## 機能の仕組み

ここでは、IP しきい値 SMF と IPAM の統合の仕組みについて説明します。

**IPAM から SMF へのしきい値ヒット状態の推測**：UPF の DNN の IP アドレスが、IPAM モジュールの「しきい値」で構成された数の IP アドレスを残した場合、リソース管理応答を使用して SMF に情報を提供します。

**しきい値ヒットを受信したときの SMF の動作**：SMF は、特定の UPF に対して使用可能なしきい値ヒットをマークします。IPAM プールの配布はノードマネージャごとに個別に行われるため、SMF はプライマリ ノードマネージャとセカンダリ ノードマネージャに対して個別にしきい値をマークします。

**しきい値がとマークされている場合の新しいセッションの UPF を選択する SMF の動作**：SMF は次のチェックを実行します。

- プライマリ ノードマネージャとセカンダリ ノードマネージャのしきい値がヒットしていない場合、IP 割り当て要求がセカンダリ ノードマネージャに送信されます。
- しきい値がプライマリ ノードマネージャとセカンダリ ノードマネージャの両方に一致する場合、現在の UPF は優先順位の低いノードマネージャを選択します（他の UPF が構成されていてヒットしていない場合）。しきい値が最初に選択されます。
- すべての UPF がしきい値に達した場合、動作は優先順位と既存の動作である負荷ベースにフォールバックします。これは、非存在しきい値ヒットの動作に似ています。

**重要** 構成の詳細については、IP アドレス管理 （893 ページ） の章を参照してください。

**しきい値ヒットからのリカバリ動作**：UPF がしきい値ヒット状態から抜けた場合、IPAM から定期的に実行されます。（各 DNN および各 UPF について）しきい値ヒットから抜け出すのに十分な空きアドレスが UPF にある場合、IPAM は（コールバックを通じて）SMF の情報を提供します。SMF がしきい値ヒットとして UPF のマークを解除します。

IPAM モジュールで（各 DNN および各 UPF の）プール内の IP アドレスが、IPAM モジュールで「しきい値」として構成された数の IP アドレスの状態で残っている場合、リソース管理応答を使用して SMF に情報を提供します。

# IP しきい値ベースの UPF 選択の OAM サポート

ここでは、この機能の操作、管理、およびメンテナンスに関して説明します。

## バルク統計サポート

次の統計情報をキャプチャするために導入された新しい統計：

ラベル：

- ラベル：up_ep_key

  ラベルの説明（Label Description）：IP アドレスの使用で特定の IP アドレスプールのしきい値に達すると、この統計が記録されます

  例：209.165.200.241:209.165.200.242

- ラベル：dnn

  ラベルの説明：構成されたしきい値 usgae に達した IP プールの DNN

  例：sampleDNN

- ラベル：threshold_hit

  ラベルの説明：しきい値ヒットが [はい（yes）] か [いいえ（no）] かを示します。

  例：yes

- ラベル：threshold_clear

  ラベルの説明：しきい値ヒットがクリアされたかどうかを示します。

  例：yes

- ラベル： nodemgr_id

  ラベルの説明：しきい値に達したノード マネージャのインスタンスを示します。

  例 1

## ユーザー プレーンをすべて表示

ここでは、問題のデバッグに役立つ show コマンドについて説明します。

### ユーザー プレーンをすべて表示

- ノード IP とエンドポイント
- キャパシティと優先順位
- サービス提供 DNN のリスト
- プライマリおよびピア ノード マネージャ インスタンス
- 負荷 seq およびロード メトリック
- Connected time
- プライマリおよびセカンダリ ノード マネージャの使用可能なしきい値ヒット

以下は、show コマンドの出力例を示しています。

```
[smf] smf# show userplane all
result
{
  "209.165.200.230:209.165.200.244": {
    "NodeIdType": 1,
    "NodeId": "209.165.200.228",
    "NodePort": 8805,
    "NodeStatus": 2,
    "Capacity": 65535,
    "Priority": 65535,
    "DnnList": [
      "intershat",
      "intershat1",
      "intershat2",
```

```
      "intershat3"
    ],
    "PrimaryNodeMgrInst": {
      "InstanceId": 1,
      "IsActive": true
    },
    "PeerNodeMgrInst": {
      "IsActive": true
    },
    "EpIp": "209.165.200.244",
    "EpPort": 8805,
    "UpEpKey": "209.165.200.230:209.165.200.244",
    "recoveryInfo": {
      "SvcRecoveryTime": 3820194022,
      "PeerRecoveryTime": 3817503651
    },
    "ConnectedTime": 3820194461,
    "IntfType": 1,
    "UpProfName": "upf1",
    "OverloadTimer": {},
    "NegotiatedCPFeatures": 2147483648
  }
}
```


# 初期 EPS 接続中の共存 UPF の選択

このセクションでは、最初の EPS 接続手順中に SMF が UPF の選択を実行する方法について説明します。

## 機能説明

cnSGWc および SMF を備えたコンバージド コア ゲートウェイは、コンバージェンスを実現するためのコンバージド UP ノードの選択をサポートします。この機能により、UE 向けに最適化されたデータ パスを作成できます。

SMF は、セッション作成要求（CSR）メッセージで受信した SGW-U ノード名に基づいて、同じ場所に配置された UPF の選択を実行します。

## 機能の仕組み

このセクションでは、4G ネットワークでの PDN セッションの確立中に SMF が同じ場所にある UPF の選択を処理する方法について説明します。

SGW-U ノード名が CSR で使用可能な場合、SMF はノード名に基づいて設定から UPF を取得します。

次に、SMF は既存の UPF 選択ロジックを使用し、それに応じて UPF のリストを取得します。SMF は、SGW-C が選択した UPF が派生した UPF リストに存在するかどうかを確認します。

SGW-C で選択された UPF が導出 UPF リストに存在し、その優先順位が導出 UPF リスト内の最も高い優先順位と一致する場合、SGW-C 選択 UPF が選択されます。それ以外の場合は、派生リストの優先順位 UPF が選択されます。

SGW-U ノード名がない場合、SMF は既存の UPF 選択アルゴリズムに従います。

# ノード ID の構成

共存 UPF を選択するには、次の構成例を使用します。

```
config
  profile network-element upf upf_name
    node-id value
    end
```

注：

- **profile network-element upf** *upf_name*：UPF のプロファイル名を指定します。
- **node-id** *value*：このキーワードは、UPF のノード ID の構成を支援します。SMF は、このノード名を SGW-U ノード名と比較して、共存 UPF を選択します。 *value* は英数字の文字列です。

# 統計情報サポート

SMF は、この機能のサポートで、以下の統計情報を保持します。

**upf_selection_stats**

説明：同じ共存 UPF が SMF によって選択された合計回数を表示します。

Metrics-Type：カウンタ

ラベル

- upf_selection_type
- upf_fqdn
- Preferred
- upf_not_associated
- upf_profile_not_found
- upf_not_active
- n4_failed
- pdu_session_type
- pdu_subscription_type
- snssai

Status:

- attempted
- failure

理由：ステータスが失敗の場合、値は次のいずれかになります。

- upf_not_associated

- upf_profile_not_found
- upf_not_active
- n4_failed

# ハンドオーバー中の共存 UPF の選択

このセクションでは、5G から 4G へのハンドオーバーおよび EPS フォールバック シナリオ中に、SMF による UPF の選択を実行する方法について説明します。

## 機能説明

5G コア ネットワークでの UE セッションの確立中に、SMF は既存の UPF 選択ロジックを使用し、選択された UPF のインデックスを PGW-C 制御トンネルのエンドポイント識別子（TEID）に記録します。

MME からセッション作成要求（CSR）を受信すると、cnSGWc は TEID 値がゼロかどうかをチェックします。ゼロの場合、cnSGWc はリモート手順コール（gRPC）メッセージを SMF に送信し、UP ID と UPF IP をフェッチします。

TEID がゼロ以外の場合、SMF は制御 TEID 値の 21 ー 30 のビットをチェックし、UPF インデックスを抽出します。SMF は、抽出された UPF インデックスを使用して、優先される UPF を選択します。

SGW-C は、UE セッションが EPS ネットワークに引き渡されるときに、優先 UPF としてこれを使用します。UPF 選択アルゴリズムによって返されたリストに優先される UPF が存在する場合、cnSGWc は優先順位が最も高い UPF を選択します。つまり、cnSGWc は SMF によって選択されたのと同じ UPF を選択します。この操作により、UE の最適化されたデータ パスを作成できます。

優先される UPF が返されたリストに存在しない場合、cnSGWc は別の UPF を選択します。

## 共存 UPF 選択のパラメータの構成

このセクションでは、ハンドオーバー シナリオ中に同じ場所に UPF の選択を実行する方法について説明します。

共存 UPF 選択 グループの選択のパラメータを構成するには、次の手順を実行します：

- 共存 UPF 選択を有効にします （1370 ページ）
- UPF 選択のためのインデックスの構成 （1371 ページ）

### 共存 UPF 選択を有効にします

共存 UPF の選択を有効または無効にするには、次の構成例を使用します。

```
config
  profile converged-core cc_profile_name
```

```
    up-selection { disable | enable }
    end
```

注：

- **profile converged-core** *cc_profile_name*：コンバージド コア プロファイルの名前を指定します。このキーワードを使用すると、コンバージド コア プロファイル構成モードを開始できます。
- **up-selection { disable | enable }**：共存 UPF 選択を有効または無効にします。デフォルトでは、構成は有効化されています。

## UPF 選択のためのインデックスの構成

共存 UPF 選択の UPF インデックス値と最大セッション数を定義するには、次の構成例を使用します。

```
config
  profile converged-core cc_profile_name
    max-upf-index upf_index_value
    max-session-count up_session_count
    end
```

注：

- **profile converged-core** *cc_profile_name*：コンバージド コア プロファイルの名前を指定します。このキーワードを使用すると、コンバージド コア プロファイル構成モードを開始できます。
- **max-upf-index** *upf_index_value*：UPF 選択でサポートされる UPF インデックス値の最大数を指定します。

  *upf_index_value* は 、0 ～ 1023 の範囲の整数である必要があります。

  SMF は、UPF から N4 関連付け設定要求で受信した UP ID に対して構成された UPF インデックス値を検証します。検証が失敗した場合、SMFは該当する要求を拒否します。検証が成功すると、SMF は要求を確認し、他の UPF の詳細とともに UP ID を保存します。
- **max-session-count** *up_session_count*:：サポートされる UP セッションの最大数を指定します。

  *up_session_count* は、1000000 ～ 12000000 の範囲の整数である必要があります。デフォルト値は 1,000,000 です。

  SMF は、構成されたセッション数を使用して、UP セッションを IdMgr コンテキストに関連付けます。IdMgr は、100 万の UP セッションごとに個別のコンテキストを維持することに注意してください。

# UPF ノード レポートと独自のセッション レポートのサポート

## 機能説明

SMF は、*3GPP TS 29.244*、セクション *6.2.9*に従って、Packet Forwarding Control Protocol（PFCP）ノード レポート手順をトリガーします。UPF はこのレポートを送信して、リモート GTP-U ピアに向かうすべての PFCP セッションに影響を与えるユーザープレーンパス障害を示します。UPF は、この障害をユーザープレーン パス障害レポート（UPFR）経由で SMF に通知します。UPF が GTP-U パスの障害を検出すると、SMF は GTP-U ピアおよび UPF ノード ID に属する PDU セッションをクリアします。

既存の UPF セッション レポートに加えて、SMF は次の独自のレポート タイプをサポートします。

- グレースフル終了レポート（GTER）：このタイプのレポートは、セッション リカバリ（SR）またはシャーシ間セッション リカバリ（ICSR）中に UPF が PDU セッションを回復できない場合に送信されます。
- セッション置換レポート（SRIR）：このタイプのレポートは、gNB によって割り当てられた同一の GTP-U トンネル エンドポイント識別子（TEID）が原因でセッションを置換するために送信されます。これは、gNB の再起動で可能です。この場合、同じ TEID を持つ古いセッションが削除されます。
- 自己保護終了レポート（SPTER）：このタイプのレポートは、過負荷シナリオ中に PFCP セッションを終了するために送信されます。

## 機能の仕組み

このセクションでは、SMF が UPF ノード レポートと独自のセッション レポートをサポートする方法について説明します。

### PFCP ノード レポートの処理

PFCP ノード レポートを適切に処理するために、GTP-U ピア アドレスには一意でないセカンダリ セッション キーが含まれている必要があります。Common Data Layer（CDL）には、セッションの詳細とともにピア アドレスと UPF IP アドレスが保存されます。アイドルからアクティブへの移行手順、N2 ハンドオーバー（HO）、5G から 4G HO、または 4G から 5G HO 中に GTP-U ピア アドレスが変更された場合、CDL データベースは古いキーを削除し、新しいキーを追加します。

1. UPF は、失敗した GTP-U ピアの IP アドレスとともに、PFCP ノード レポート要求を SMF に送信します。

2. SMF プロトコルは、ノード ID、つまり要求に含まれる UPF IP アドレスをチェックします。ノード ID が見つからない場合、またはノード ID が関連付けられた状態にない場合、SMF プロトコルは失敗応答を送信します。
3. ノード ID が見つかった場合、ノード マネージャは GTP-U ピアの IP アドレスとノード ID を使用して EPS セッションの CDL をクエリします。ノード マネージャは、対応するセッションをクリアするための一括通知を CDL に送信します。
4. CDL は REST エンドポイント（REST-EP）ポッドに通知を送信して、セッションをクリアします。
5. REST-EP ポッドは、アフィニティに基づいて、サブスクライバのクリア通知を SMF サービスに送信します。SMF サービスは、すべてのインターフェイスのセッションをクリアします。

## PFCP セッション レポートの処理

UPF は、GTER、SRIR、および SPTER とともに PFCP セッション レポートを SMF に送信します。セッションが見つかった場合、SMF は正常な PFCP セッション レポート応答を送信します。その後、SMF は PDU セッションのリリース手順をトリガし、すべてのインターフェイスでセッションを削除します。

## コリジョン処理

新しくサポートされるメッセージ（ノード レポートとセッション レポート）の場合、SMF は PDU セッションの解放手順をトリガします。PDU セッションの解放手順が HO 手順と競合した場合、SMF は HO 中に GTP-U ピア IP が変更されるため、HO 手順を中止しません。これを実現するために、PDU リリース手順では、リリース要求で受信した GTP-U ピア IP アドレスを PDU セッションに存在するアドレスと比較します。2 つのアドレスが異なる場合、SMF はリリース手順を中止します。

**重要** コリジョン処理は、ノード レポートによってトリガーされる着信 HO メッセージと **clear subscriber** コマンドの到着時刻によって異なります。

## 復元力の処理

SMF は再試行タイマーを使用して、GTP-U ピアの保留中のセッションの削除をチェックし、報告します。SMF ノード マネージャの再起動後、セッションが削除されていない場合、これらのセッションはそのまま残ります。

## 標準準拠

VoWi-Fi サポート機能は、以下の基準に準拠します：

- *3GPP TS 29.244 バージョン 15.6.0：LTE、Interface between the Control Plane and the User Plane nodes*

## 制限事項

この機能には、次の制限事項があります。

- CDL 通知が失われ、セッションがクリアされない場合、SMF ノードマネージャは 10 分後に 1 回だけ一括削除操作を再試行します。
- ノード レポート要求が到着し、システムが過負荷状態になると、一部の CDL 通知がドロップされます。この場合、SMF は UPF からのエラー通知レポート要求に基づいてセッションのクリーンアップを実行します。
- UPF は現在、ノード レポート要求で 1 つのリモート GTP-U ピアのみを送信しています。そのため、SMF は 1 つのリモート GTP-U ピアだけを検証できます。

# OAM サポート

ここでは、この機能の操作、管理、およびメンテナンスに関して説明します。

## Monitoring Support

CEE Ops-Center で次の構成が実行されると、アラームが追加されます。このアラームは、特定の UPF の GTP-U ピアがダウンしたことを示しています。アラーム データには、GTP-U ピア IP アドレスと UPF IP アドレスが含まれます。

次に、UPF ノード レポート要求に関連するアラート ルールを構成するために CEE Ops-Center で実行される構成の例を示します。

```
config
   alerts rules group alert_group_name
   interval-seconds seconds
   rule rule_name
      expression promql_expression
      severity severity_level
      type alert-type
      annotationannotation_name
      value annotation_value
      exit
   exit
```

注：

- **alerts rules**：Prometheus アラート ルールを指定します。
- **group** *alert_group_name*：Prometheus アラート ルール グループを指定します。1 つのアラート グループにルールの複数のリストを含めることができます。 *alert-group-name* はアラート グループの名前です。*alert-group-name* は、0 ～ 64 文字の範囲の文字列にする必要があります。
- **interval-seconds** *seconds*：ルール グループの評価間隔を秒単位で指定します。
- **rule** *rule_name*：アラート ルール定義を指定します。 *rule_name* はルールの名前です。

アラートの構成例を次に示します。

```
config
   alerts rules group NodeReportGTPURemotePeer
   interval-seconds 300
   rule NodeReportGTPURemotePeerDown
      expression smf_protocol_udp_res_msg_total{message_name=\"n4_node_report_req\",
 message_direction= \“inbound\”, status=\“accepted\”}”
       severity major
       type "Communications Alarm"
       annotation summary
       value “This alert is fired when the UPF Sends Node Report Request to SMF”
       exit
   exit
```

## show コマンドのサポート

**show subscriber all** コマンドを使用して、GTP-U ピア IP アドレスと GTP-U ピア エンドポイント キーに関連する構成を表示します。この構成データは、失敗したセッションまたは手順の衝突を特定するのに役立ちます。

次に出力例があります。

```
[unknown] smf# show subscriber all nf-service smf
subscriber-details
{
  "subResponses": [
    [
      "supi:imsi-123456789012345",
      "gpsi:msisdn-223310101010101",
      "pei:imei-123456786666660",
      "psid:5",
      "dnn:intershat",
      "emergency:false",
      "rat:e-utran",
      "access:3gpp access",
      "connectivity:4g",
      "udm-sdm:10.84.17.111",
      "pcfGroupId:PCF-dnn=;",
      "policy:2",
      "pcf:10.84.17.111",
      "upf:10.84.17.111",
      "upfEpKey:10.84.17.111:10.84.17.112",
      "ipv4-addr:poolv4/209.165.202.129",
      "ipv4-pool:poolv4",
      "ipv4-range:poolv4/209.165.202.129",
      "ipv4-startrange:poolv4/209.165.202.129",
      "gtp-peer:10.84.17.112",
      "peerGtpuEpKey:10.84.17.111:10.84.17.111",
      "namespace:smf"
    ]
  ]
}
```

**show subscriber count peerGtpuEpKey** コマンドを使用して、指定した GTP-U ピアと UPF ノードに関連付けられているセッション数を表示します。

重要 **show subscriber count peerGtpuEpKey** コマンドは、システム パフォーマンスに影響を与える可能性があるため、慎重に、かつ慎重に考えてください。

**show subscriber count peerGtpuEpKey** コマンドの出力例を次に示します。

```
smf# show subscriber count peerGtpuEpKey 30.30.30.63:50.50.0.58
  subscriber-details
  {
    "sessionCount": 12568
  }
```

# 統計情報サポート

SMF は、試行、成功、および失敗したノード レベルとセッション レベルの要求の合計数を追跡するために、次の統計情報を保持します。

- SMF_SERVICE_STATS には、次の手順タイプがあります：
  - upf_node_report_pdu_sess_rel

    [試行（attempted）]：ノード レポートがトリガーされた PDU セッションの解放要求の試行回数。

    [成功（successful）]：ノード レポートが原因でトリガーされた、成功した PDU セッションの解放要求の合計数。

    [失敗（failure）]：ノード レポートが原因でトリガーされた、失敗した PDU セッションの解放要求の合計数。

  - upf_sess_report_gter_pdu_sess_rel

    [試行（attempted）]：セッション レポート「GTER」がトリガーされた PDU セッションの解放要求の試行回数。

    [成功（successful）]：セッション レポート「GTER」によりトリガーされた、成功した PDU セッション リリース要求の合計数。

    [失敗（failure）]：セッション レポート「GTER」がトリガーされた、失敗した PDU セッション リリース要求の合計数。

- SMF_PROTOCOL_UDP_REQ_MSG_TOTAL（次のメッセージタイプの場合）。
  - n4_node_report_req

    [試行（attempted）]：ノード レポートがトリガーである試行された N4 要求の合計数。

    [成功（successful）]：ノード レポートが原因でトリガーされた成功した N4 リクエストの合計数。

    [失敗（failure）]：ノード レポートが原因でトリガーされた失敗した N4 要求の合計数。

  - n4_session_report_req

[試行（attempted）]：セッション レポートが原因でトリガーされた試行された N4 リクエストの合計数。

[成功（successed）]：セッション レポートが原因でトリガーされた、成功した N4 リクエストの合計数。

[失敗（failure）]：セッション レポートが原因でトリガーされた失敗した N4 リクエストの合計数。

- 次のメッセージ タイプの SMF_PROTOCOL_UDP_RES_MSG_TOTAL。
  - n4_node_report_res

    [試行（attempted）]：ノード レポートがトリガーされた試行された N4 応答の合計数。

    [成功（successful）]：ノード レポートがトリガーされた成功した N4 応答の合計数。

    [失敗（failure）]：ノード レポートが原因で失敗した N4 応答の合計数。

  - n4_session_report_res

    [試行（attempted）]：セッション レポートがトリガーされた試行された N4 応答の合計数。

    [成功（successful）]：セッション レポートがトリガーされた成功した N4 応答の合計数。

    [失敗（failure）]：セッション レポートが原因で失敗した N4 応答の合計数。

- SMF_DISCONNECT_STATS が次の切断理由でトリガーされます。

  gtpu_peer_path_failure：この統計情報は、ノード レポートが原因でセッションが削除された場合にトリガーされます。

  upf_sess_report_gter_pdu_sess_rel：この統計は、セッション レポートが原因でセッションが削除された場合にトリガーされます。

統計情報の例を次に示します：

ノード レポート SMF サービスの統計:

```
smf_service_stats{app_name="SMF",cluster="Local",data_center="DC",dnn="intershat",
emergency_call="false",instance_id="0",pdu_type="ipv4",
procedure_type="upf_node_report_pdu_sess_rel",qos_5qi="",rat_type="NR",
reason="",service_name="smf-service",status="attempted",up_state=""}

smf_service_stats{app_name="SMF",cluster="Local",data_center="DC",dnn="intershat",
emergency_call="false",instance_id="0",pdu_type="ipv4",
procedure_type="upf_node_report_pdu_sess_rel",qos_5qi="",rat_type="NR",
reason="",service_name="smf-service",status="success",up_state=""} 1
```

セッション レポート SMF サービスの統計:

```
smf_service_stats{always_on="",app_name="smf",cluster="smf",data_center="unknown",
dcnr="",dnn="intershat",emergency_call="false",instance_id="0",pdu_type="ipv4",
procedure_type="upf_sess_report_gter_pdu_sess_rel",qos_5qi="",rat_type="NR",
reason="",service_name="smf-service",status="attempted",up_state=""} 1

smf_service_stats{always_on="",app_name="smf",cluster="smf",data_center="unknown",
dcnr="",dnn="intershat",emergency_call="false",instance_id="0",pdu_type="ipv4",
```

```
procedure_type="upf_sess_report_gter_pdu_sess_rel",qos_5qi="",rat_type="NR",
reason="",service_name="smf-service",status="success",up_state=""} 1
```

ノード レポート SMF プロトコル統計：

```
smf_proto_udp_req_msg_total{app_name="smf",cluster="smf",data_center="unknown",
instance_id="0",message_direction="inbound",message_name="n4_node_report_req",
msgpriority="",service_name="smf-protocol",status="accepted",
transport_type="origin"} 15

smf_proto_udp_res_msg_total{app_name="smf",cause="1",cluster="smf",
data_center="unknown",instance_id="0",message_direction="outbound",
message_name="n4_node_report_res",msgpriority="",service_name="smf-protocol",
status="accepted",transport_type="origin"} 15
```

セッション レポート SMF プロトコル統計：

```
smf_proto_udp_req_msg_total{app_name="smf",cluster="smf",data_center="unknown",
instance_id="1",message_direction="inbound",message_name="n4_session_report_req",
msgpriority="",service_name="smf-protocol",status="accepted",
transport_type="origin"} 43

smf_proto_udp_res_msg_total{app_name="smf",cause="1",cluster="smf",
data_center="unknown",instance_id="1",message_direction="outbound",
message_name="n4_session_report_res",msgpriority="",service_name="smf-protocol",
status="accepted",transport_type="origin”}
```

SMF は、ノード レポートとセッション レポート タイプ（GTER、SRIR、SPTER）が原因でセッション削除された数を追跡するためのラベルも維持します。

たとえば、ラベル「LABEL_DISC_PDNREL_GTER_SESSION_REP」が追加され、GTER の存在によるセッションの削除が追跡されます。

# 外部ヘッダー形式

**表 *404 :* 機能の履歴**

| 機能名 | リリース情報 | 説明 |
|---|---|---|
| N3 のデュアル スタックのサポート | 2024.01 | SMF は、UPF ネットワーク プロファイルで **dual-stack-transport { false \| true }** CLI コマンドを使用して、N3 トンネルのデュアル スタック トランスポートを有効にします。<br>**デフォルト設定**：無効：構成が必要 |

SMF は、PFCP セッションのパケット検出ルール（PDR）で UPF に外部ヘッダー IE を送信します。外部ヘッダー IE は、Sx インターフェイスを介して送信される N4 セッション確立要求メッセージで使用できます。この IE の形式は、3GPP TS 29.244 仕様のバージョン 16.4.0 で定義されています。

次の表に、外部ヘッダー作成（OHC）の説明フィールドのエンコーディング形式を示します。これはビットマスクの形式になり、各ビットは発信パケットに追加される外部ヘッダーを示します。SMF はスペア ビットを無視します。

**表 *405*：ヘッダー エンコーディング フォーマット**

| オクテット/ビット | 発信パケットで作成された外部ヘッダー |
|---|---|
| 5/1 | GTP-U/UDP/IPv4 |
| 5/2 | GTP-U/UDP/IPv6 |
| 5/3 | UDP/IPv4 |
| 5/4 | UDP/IPv6 |
| 5/5 | IPv4 |
| 5/6 | IPv6 |
| 5/7 | C-TAG |
| 5/8 | S-TAG |
| 6/1 | N19 の兆候 |
| 6/2 | N6 の兆候 |
| 6/3 | TCP/IPv4 |
| 6/4 | TCP/IPv6 |

**注**：

- 現在、UPF は外部ヘッダー作成の説明の次の値をサポートしていません。
  - IPv4
  - IPv6
  - C-TAG
  - S-TAG
  - N19 の兆候
  - N6 の兆候
- 6 番目のオクテットの 3 番目と 4 番目のビット（つまり、6/3 と 6/4）は、LI over TCP に使用されるスペアビット（つまり、3GPP TS 29.244、バージョン 16.4.0 の一部ではありません）。

**重要** セッションを正常に確立するには、SMF および UPF が外部ヘッダー IE の同じ形式をサポートしている必要があります。

# 外部ヘッダー IE の機能構成

SMF により、UPF プロファイルでのデュアル スタック接続が有効になります。デュアル スタックが構成されている場合、IPv4 および IPv6 アドレスの GTP-U または UDP または IP ヘッダーを削除するために、OHR IE の [外部ヘッダー削除（OHR）の説明（Outer Header Removal (OHR) Description）] フィールドが 6 に設定されます。

N3 インターフェイスでデュアル スタックを有効にするには、次の構成例を使用します。

```
config
   profile network-element upf upf_profile_name
       dual-stack-transport { true | false }
       end
```

注：

- **dual-stack-transport { true | false }**：N3 インターフェイスでデュアル スタック トランスポートを有効または無効にします。
  - **dual-stack-transport true** コマンドが構成されている場合、SMF は、サポートされているインターフェイス上で、IPv6 アドレスの値 6 を使用して OHR IE を送信します。
  - SMF はセッション確立中に構成されたデュアル スタック値を保存します。SMF は、セッションが切断されるまで、後続の N4 メッセージで同じデュアル スタック値を使用します。

（注） この CLI 構成は、レガシーのインターフェイスを使用する SMF にも適用できます。

# グレースフル セッション終了の拡張された PFCP 関連付けのリリース手順

表 *406 :* 機能の履歴

| 機能名 | リリース | 説明 |
|---|---|---|
| UPF によって開始された PFCP の関連付けの解除に関する痕跡 | 2024.03.0 | この機能により、SMF は UPF によって開始された PFCP 関連付けリリースの手順についての通知を受信できます。この通知は、UPF と SMF でセッションと関連付けを同時にクリアすることを示しています。<br>SMF に通知されない場合、UPF が SMF から次のセッション変更要求を受信するまで、コールは接続されたままになります。これにより、回線の使用状況レポートが失われます。ここで、拡張 PFCP 関連付けリリース（EPFAR）機能により、シグナリングの効率と、SMF による使用状況レポートの効果的な処理が向上します。<br>**デフォルト設定**： 無効：有効にするには構成が必要 |

UPF がエラーまたは部分的な障害によりコールをクリアすることを決定すると、UPF はコールのクリアについて SMF に通知せずに、コールをローカルでクリアします。UPF が SMF から次のセッション変更要求を受信するまで、コールは接続されたままになります。

コール クリア中の使用状況レポートの損失を防ぎ、シグナリング効率を向上させるために、UPF に拡張 PFCP 関連付けリリース（EPFAR）機能を適用し、セッション レポート要求を開始して、UPF と SMF または、UPF と cnSGWc び間のセッションを同時に正常にクリアします。この機能は、3GPP TS 29.244 のリリース 16.9.0、セクション 5.18.1 およびセクション 5.18.2 に準拠しています。

### EPFAR 交渉

EPFAR 機能の交渉は、SMF と UPF 間の集約通信です。SMF と UPFの両方が EPFAR 機能をサポートしている場合、セッションと関連付けリリースアクションが実行されます。UPF が SMF との関連付けをリリースする必要がある場合は、構成コマンドを使用して EPFAR 機能を有効にすることができます。

SMF は、UPF への PFCP 関連付け設定応答で CP Function Features IE の EPFAR ビットを設定することで、EPFAR 機能のサポートを示します。

ローリング アップグレードの場合、シャーシがアクティブになるたびに、EPFAR 機能が再度交渉できるように、UPF または SMF は UP または CP 機能による PFCP 関連付けの更新を送信します。

UPF によって開始されたリリースは、次の手順を使用してトリガされます。

1. UPF が開始した PFCP セッションのリリース
2. UPF によって開始された拡張 PFCP 関連付けのリリース

# UPF が開始した PFCP セッションのリリース

UPF によって開始された PFCP セッション リリースは、次の一連のアクションで構成されます。

1. UPF は、関連付けセットアップまたは変更手順中にネゴシエートされた場合にのみ、ピア ノードの機能を有効にします。UPF は、エラーまたは部分的な障害により PFCP セッションを削除する必要がある場合、影響を受けるセッションの PFCP セッション レポート要求を開始します。SMF は、レポート タイプとユーザー レポート トリガ IE とともに UPF から PFCP セッション レポート要求を受信します。
   - PFCP セッションの使用状況がゼロ以外のレポートがある場合、レポート タイプは USAR（使用状況レポート）に設定され、送信する使用状況レポートがない場合は UISR（UP 開始セッション要求）に設定されます。

     レポート タイプ IE のオクテット 6 の 5 番目のビットは、PFCP セッション レポート要求の UISR を示すために使用される独自の IE ビットです。
   - ユーザー レポート トリガは、ゼロ以外の使用状況レポートの TEBUR（UP 機能による終了レポート）に設定されます。

   UPF が PSDBU（PFCP セッションが UP 機能によって削除されました）フラグを 1 に設定して、PFCP セッションの削除を示します。
2. UPF は、PFCP セッション レポート要求メッセージでピア ノードに原因 IE を送信します。Cause IE は、次の値を使用してセッション削除の原因を伝達します。
   - 201：サブスクライバによるクリア
   - 202：UP によって開始された関連付けのリリース
   - 203：復元失敗

- 204：IP ソース違反
- 205：PFCP 原因自己保護での終了

次の表に、レガシー インターフェイスで SMF に送信される原因を示します。

| UPF からの原因 | Gx Termination-Cause | Gy Termination-Cause | RADIUS アカウンティングが停止 Acct-Terminate-Cause | Gtpc 原因 | Gz CauseForRecClosing |
|---|---|---|---|---|---|
| サブスクライバによるクリア（201） | Diameter ログアウト | Diameterログアウト | NAS 要求 | 再アクティブ化の要求 | 管理介入 |
| UP によって開始された関連付けのリリース（202） | Diameter ログアウト | Diameter ログアウト | NAS 要求 | 再アクティブ化の要求 | 管理介入 |
| 復元失敗（203） | Diameter 管理 | Diameter 管理 | NAS 要求 | 再アクティブ化の要求 | 異常なリリース |
| IP 送信元違反（204） | Diameter 管理 | Diameter 管理 | NAS 要求 | 再アクティブ化の要求 | 異常なリリース |
| 自己保護の終了（205） | Diameter 管理 | Diameter 管理 | NAS 要求 | 再アクティブ化の要求 | 異常なリリース |

3. SMF が、リリース手順の一部として次の使用状況レポートを処理します。
   - PSDBU を使用しない TEBUR
   - PSDBU を使用する TEBUR
   - UISR および PSDBU のセッション レポート
4. 使用状況レポートは、セッション リリース時に CHF にまとめて報告されます。

（注） SMF でサポートされているクリアサブスクライバの最大レートは 500 セッション/秒です。したがって、セッション レポートのスロットル レートは UPF で 1 秒あたり 500 に維持されます。複数の UPF からのセッション レポートの合計レートがサポートされている最大レートを超えている場合でも、SMF とその後の再送信でスロットリングが発生する可能性があります。

# UPF によって開始された拡張 PFCP 関連付けの解除

UPF によって開始された PFCP の関連付け解除は、次の一連のアクションで構成されます。

1. SMF と UPF の両方が EPFAR 機能をサポートしている場合、UPF は PFCP の関連付けの解除を開始します。SMF は、PFCP 関連付けリリースの UPF から PARPS（PFCP 関連付けリリース準備開始）フラグが設定された PFCP 関連付け更新要求を受信し、cnSGWc は UPF の選択を停止します。
2. SMF は、UPF から次のフラグが設定された使用状況レポートを受信します。
   - ゼロ以外の最終使用状況レポートが存在するすべてのセッションに対する PSDBU を使用しない TEBUR と PSDBU を使用した TEBUR。
   - 使用状況レポートがないすべてのセッションの UISR および PSDBU フラグを含むセッション レポート。
3. SMF は、影響を受ける PFCP セッションのゼロ以外のすべての使用状況レポートが送信されることを示す URSS フラグが 1 に設定された状態で、UPF から PFCP 関連付け更新要求を受信します。 cnSGWc は、この UPF の残りのすべてのセッションを削除します。SMF は、この UPF の残りのすべてのセッションを削除します。
4. UPF のすべてのセッションがクリアされると、SMF は UPF に対して PFCP 関連付け解除手順をトリガして、PFCP 関連付けをクリアします。

# EPFAR 機能の有効化

**[smf] smf(config)# profile converged-core cc supported-features [ epfar ]** CLI コマンドを使用して、SMF で EPFAR 機能を有効にします。

## 手順

**ステップ 1** コンテキスト構成モードを開始します。**profile converged-core cc supported-features**

例：

```
[smf] smf(config)# profile converged-core cc supported-features [ epfar ]
```

（注）
eppar：拡張 PFCP アソシエーション リリースのサポートを有効にします。

**ステップ 2** **show running-config profile converged-core** show コマンドを使用して、EPFAR 機能が有効か無効かを確認できます。

例：

```
[smf] smf# show running-config profile converged-core
Mon May  6  03:09:36.813 UTC+00:00
profile converged-core cc
 supported-features [ epfar ]
```

```
exit
[smf] smf#
```

# バルク統計

既存の統計に対するこの機能の一部として、新しいラベルが追加されています。

- smf_disconnect_stats

**クエリの例 1**：

```
smf_disconnect_stats {an_type=""app_name ="SMF",cluster="SMF",
data_center="DC",gr_instance_id="1",instance_id="0",rat_type=
 "EUTRA"reason=" disc_subscriber_clear",roaming_status="homer",
service_name="smf-service",severity="normal",snssai=""} 1
```

**クエリの例 2**：

```
smf_disconnect_stats {an_type="3GPP_ACCESS", app_name="SMF",
cluster="SMF",data_center="DC",gr_instance_id="1",instance_id="0",
rat_type="NR",reason="disc_pdurel_upf_urss_init_ association_release",
roaming_status="homer",service_name="smf-service",severity="normal",
snssai=""} 1
```

**クエリの例 3**：

```
smf_disconnect_stats {an_type="",app_name="SMF",cluster="SMF",
data_center="DC",gr_instance_id="1",instance_id="0",rat_type="EUTRA",
reason=" disc_pdn_upf_urss_init_release",roaming_status="homer",
service_name="smf-service",severity="normal",snssai=""} 1
```

**ラベル**：

- disc_subscriber_clear
- disc_association_release_initiated_by_up
- disc_recovery_failure
- disk_ip_source_violation
- disc_psdbu_timer_expiry
- disc_pdurel_upf_urss_init_association_release

- smf_sess_report_stats

**クエリの例 1**：

```
smf_sess_report_stats {app_name="SMF",cluster="SMF",
data_center= "DC",gr_instance_id="1",instance_id="0",
rat_type="EUTRA",reason="psdbu",service_name="smf-service",
sess_report_type="sess_report_type_uisr"} 1
```

**クエリの例 2**：

```
smf_sess_report_stats {app_name="SMF",cluster="SMF",
data_center="DC",gr_instance_id="1",instance_id="0",
rat_type="EUTRA",reason="psdbu",service_name="smf-service",
sess_report_type="sess_report_type_usar"} 2
```

**ラベル：**

report_type と reason には、統計に次のラベルがあります。

- sess_report_type_uisr
- sess_report_type_usar
- psdbu

- smf_pfcp_usar_rpt_type_stats

**クエリの例：**

```
smf_pfcp_usar_rpt_type_stats {app_name="SMF",
charging_trigger_type="TEBUR,",cluster="SMF",
data_center="DC",instance_id="0",service_name=
"smf-service",status="validated"} 2
```

**Label:**

- charge_trigger_type = "TEBUR"

- nodemgr_up_pathfail_reasons

**クエリの例：**

```
nodemgr_up_pathfail_reasons {app_name="SMF",
 cluster="SMF",data_center="DC",gr_instance_id="1",
instance_id="0",service_name="nodemgr",
up_pathfail_reason="up_urss_reason_association_release"} 1
```

**Label:**

- up_urss_reason_association_release

# PCF を介した使用状況監視

## 機能説明

SMF は、4G および 5G PDU セッションの PCF N7 インターフェイスを介した使用状況監視機能をサポートします。SMF が使用状況データを PCF に報告した後、SMF は、合計ボリューム、アップリンク ボリューム、またはダウンリンク ボリュームのしきい値などの使用状況モニタリング パラメータの変更、および PCF からの使用状況モニタリングしきい値または関連するトリガを受信しないことに基づく使用状況モニタリングの無効化をサポートします。

## 機能の仕組み

このセクションでは、PCF N7 インターフェイスを介した SMF 使用率モニタリングの仕組みについて説明します。

# 使用状況レポート

UPF は、PDU セッションまたは対応するサービス データ フローのすべてのトラフィックの量と使用時間を測定します。UPF は、PFCP セッション レポート要求または PFCP セッション変更応答のいずれかで累積使用レポートを SMF に送信します。次に、SMF は、PCF への次のいずれかのメッセージの「accuUsageReports」属性に 1 つまたは複数の累積使用状況レポートを含めます。

- HTTP POSTメッセージ

（注） また、このメッセージでは、「repPolicyCtrlReqTriggers」属性に「US_RE」値も含まれています。

- 終了手順中に SM ポリシー削除データ構造を含めるメッセージ。

各 AccuUsageReport データ構造には、1 つまたは 2 つの通信量レポート情報要素内に累積通信量が含まれます。これらの要素は、PCF が要求した使用状況モニタリング制御インスタンスに対応しています。PCF がボリュームと時間の両方のしきい値を提供し、いずれかの測定値のしきい値が到達すると、UPF は、累積されたボリュームと時間の測定値とともにこのイベントを SMF に通知します。次に、SMF は両方の測定について、最後のレポート以降の累積使用量を PCF に送信します。

SMF は、PFCP セッション レポート要求で UPF から累積使用状況レポートを受信します。このレポートを受信した後、SMF は使用状況モニタリング制御インスタンスに対応する使用状況レポートのリストを識別します。次に、SMF は PDU 変更または PDU 専用ベアラー手順をポストします。この手順には、新しいイベント タイプ、使用状況レポートのリスト、およびそれらを処理する URR のリストが含まれています。

## 累積通信量レポート

次の表に、累積通信量レポートで利用可能な情報を示します。

**表 *407 :* 累積通信量レポート**

| 属性名 | データタイプ | L | 基数 | 説明 |
|---|---|---|---|---|
| refUmId | 文字列 | M | 1 | 通信量レポートに関連付けられている UsageMonitoringData オブジェクトの参照 ID を示します。 |
| volUsage | 音量 | O | 0.1 | 累積ボリューム使用量の合計を示します。 |

| 属性名 | データタイプ | L | 基数 | 説明 |
|---|---|---|---|---|
| volUsageUplink | 音量 | O | 0.1 | アップリンクでの累積ボリューム使用量を示します。 |
| volUsageDownlink | 音量 | O | 0.1 | ダウンリンクでの累積ボリューム使用量を示します。 |
| 時間 | DurationSec | O | 0.1 | 累積時間の使用量を示します。 |
| nextVolUsage | 音量 | C | 0.1 | モニタリング時間の後の累積ボリューム使用量を示します。 |
| nextVolUsageUplink | 音量 | O | 0.1 | モニタリング時間後のアップリンクの累積ボリューム使用量を示します。 |
| nextVolUsageDownlink | 音量 | O | 0.1 | モニタリング時間後のダウンリンクの累積ボリューム使用量を示します。 |
| nextTimeUsage | DurationSec | C | 0.1 | モニタリング後に累積時間の使用量を示します。 |

## 通信内容管理データの変更

以下は、PCF を介した使用状況モニタリングに使用可能なデータ変更シナリオです。

- PCFが1つまたは複数のモニタリング キーのしきい値レベルを削除する必要がある場合、PCFは、対応する属性にNULL値を、対応する使用状況モニタリング制御インスタンスに提供します。
- PCF が HTTP POST メッセージで累積使用量を受信すると、PCF は、次の使用状況モニタリング制御インスタンスの使用状況モニタリングが継続しているかどうかを SMF に通知します。
  - 特定のレベルの監視が続く場合、PCF は HTTP POST メッセージの応答でそのレベルの新しいしきい値を提供します。このメッセージには、「volumeThreshold」、「volumeThresholdUplink」、「volumeThresholdDownlink」などの既存の属性が含まれます。
  - PCF が特定のレベルのモニタリングを停止した場合、PCF は停止したレベルの HTTP POST メッセージの応答に更新されたしきい値を含めません。これは、PCF に「umDecs」属性のエントリに対応する属性が含まれていないことを意味します。属性

は、「volumeThreshold」、「volumeThresholdUplink」、「volumeThresholdDownlink」、「timeThreshold」、「nextVolThreshold」、「nextVolThresholdUplink」、「nextVolThresholdDownlink」、および「nextTimeThreshold」です。

PCF が使用状況モニタリング制御インスタンスの監視を停止する場合、PCF は HTTP POST メッセージの応答に使用状況モニタリング制御インスタンスのしきい値を含めません。また、PCF は、ダイナミック PCC ルールまたはセッション ルールから使用状況モニタリング制御インスタンスの参照を削除しません。

次のシナリオに基づいて、SMF は PFCP セッション変更要求を PCF に送信します。

- 既存のしきい値を変更する場合、SMF は新しいしきい値で URR を更新し、PFCP セッション変更要求で UPF に対する URR の更新を開始します。
- 使用状況監視制御インスタンスのモニタリングが停止されている場合、SMF は URR を削除し、PFCP セッション変更要求で UPF に対して URR の削除を開始します。
- 新しい使用状況モニタリング制御インスタンスの場合、SMF はしきい値を持つ新しい URR を作成します。また、SMF は URR を対応する PDR に関連付け、PFCP セッション変更要求で UPF に対する PDR の更新とともに URR の作成を開始します。

## エラー処理

SMF とそのアクションでの使用状況モニタリングのプロビジョニング中に、次のエラーが発生する可能性があります：

- PCF が無効なしきい値を定義している場合、セッション ルールまたは PCC ルールに無効なしきい値を含むモニタリング キー（UmId）の参照がある場合、SMF は PCC ルールを失敗または無効としてマークします。
- PCF が SMF で使用状況モニタリングがアクティブであるメッセージ交換間の US_RE フラグを削除するか、構成しない場合、SMF は、N7 インターフェイス用に作成された使用可能な URR を使用して、変更要求で UPF に URR 削除要求を送信します。

## コール フロー

このセクションでは、次のコール フローについて説明します。

- 通信量監視のアクティベーション通話フロー
- 使用状況レポートのコール フロー

### 通信量監視のアクティベーション コール フロー

ここでは、通信量モニタリングのアクティベーションのコール フローについて説明します。

図 *229 :* 通信量監視のアクティベーション コール フロー

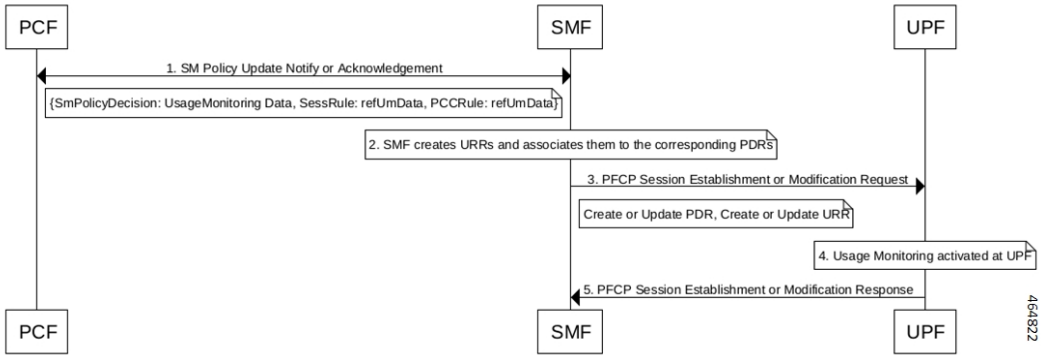



表 *408 :* 通信量モニタリングのアクティベーション コール フロー

| ステップ | 説明 |
|---|---|
| 1 | PCF は、使用状況モニタリング データのリストを、モニタリング対象のしきい値と、セッションまたは PCC ルール レベルのいずれかへのしきい値の関連付けとともに送信します。 |
| 2 | SMF は、各モニタリング データの URR を作成し、対応する PDR に関連付けます。 |
| 3 | SMF は、URR の作成または更新要求を送信し、PFCP セッションの確立または変更要求内の対応する PDR に URR をリンクします。 |
| 4 | UPF は、受信した URR のモニタリングをアクティブにします。 |
| 5 | UPF は、対応する原因コードとともに SMF に応答を送信します。 |

## 使用状況レポートのコールフロー

ここでは、使用状況レポートのコール フローについて説明します。

図 *230 :* 使用状況レポートのコールフロー

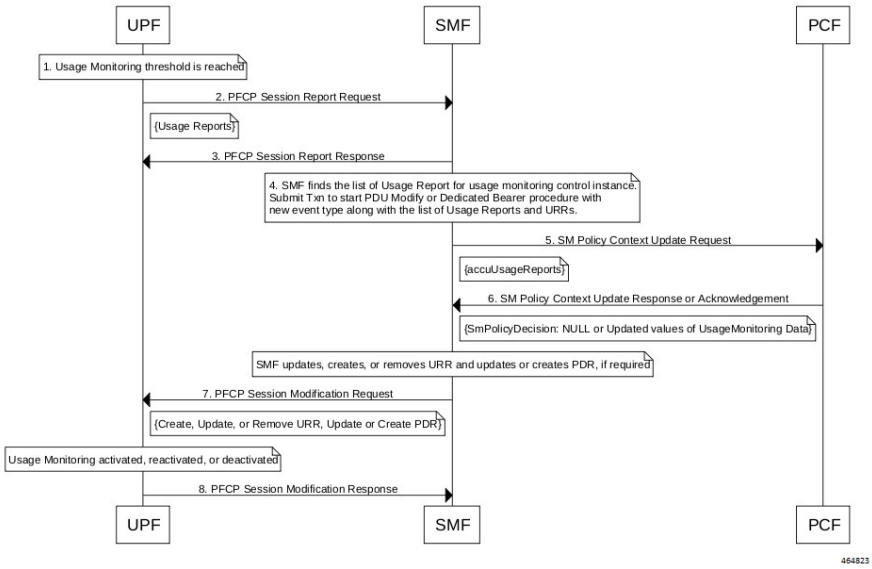



表 *409 :* 使用状況レポートのコール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | UPF で、構成された使用状況のモニタリングしきい値の制限に達します。 |
| 2 | UPF は、URR の使用情報とともに PFCP セッション レポート要求を SMF に送信します。 |
| 3 | SMF は、原因：「PFCP Cause Request Accepted」の PFCP セッション レポート応答を送信します。 |
| 4 | SMF は、受信した使用状況情報をポリシー要求の更新で PCF に送信します。 |
| 5 | PCF は、SMF に対するモニタリングの更新されたしきい値またはしきい値なしを確認します。なしの場合、SMF へのモニタリングは無効です。 |
| 6 | SMF は対応する URR を削除または更新し、変更要求を UPF に送信します。 |
| 7 | UPF は、受信した情報に基づいてモニタリングを非アクティブ化または再アクティブ化します。 |
| 8 | UPF は、対応する原因コードを含む確認応答を SMF に送信します。 |

## 標準準拠

PC F機能を使用した使用状況モニタリングは、以下の規格に準拠しています。

- *3GPP TS 29.512* バージョン *16.5.0* リリース *16 - 5G*。*5G* システム。セッション管理ポリシー制御サービス

## 制限事項

この機能には、次の制限事項があります。

- PCC ルール レベルのモニタリングを有効にすると、デフォルトでは、このモニタリングはPCCルールおよびセッション レベルのURR（存在する場合）に関連付けられたrefUmDataの URR にリンクされます。リンクは、PCF が「exUsagePccRuleId」のセッション レベルのモニタリングから除外するまで存在します。
- 使用状況監視の進行中に、refUmData を使用せずにセッション ルールまたは PCC ルールのパラメータを PCF から更新すると、そのルールの使用状況監視が無効になるか削除されることを意味します。このルールは、変更がない場合でも、常にrefUmDataを含める必要があります。
- SMF は、SMF が使用状況レポートを PCF に通知し、PCF が 204 - No Content で応答した後、UPFから受信した使用状況レポートを受け入れません（PCFは使用状況のモニタリングを無効にします）。この場合、SMF は無効化された UmId の削除 URR を UPF にのみ通知し、受信した使用状況レポートをローカルで破棄します。
- デフォルトでは、SMF は、セッション レベルの URR（存在する場合）を、セッションの一部としてすべてのアクティブな静的ルールにリンクします。SMF と UPF 間の静的ルールでは URR 情報の交換が行われないため、UPF は PDU およびセッション レベルのモニタリングの一環として静的ルールのデータ使用状況をモニタリングします。次に、UPFは使用状況レポートを使用して SMF に応答を送信します。

# 事前定義されたルールの使用状況モニタリング キーの構成

事前定義されたルールの使用状況モニタリング キーを構成するには、次の構成例を使用します。

```
config
   active-charging service  service_name
      rulebase  rulebase_name
         action priority  priority_name dynamic-only ruledef  ruledef_name
charging-action  charging-action_name umid  usage-monitoring_identifier
         end
```

注：

- **umid** *usage-monitoring_identifier*：使用状況モニタリング識別子を指定します。*usage-monitoring_identifier* は 文字列である必要があります。

（注） **action priority** *priority_name* **dynamic-only ruledef** *ruledef_name* コマンドのローカル構成によって、事前定義されたルールの使用状況のモニタリング識別子を関連付けることができます。PCF がこのルールをアクティブにすると、SMF は PCF から SMF を受信する使用状況のモニタリングしきい値を取得します。SMF は URR を作成し、それを事前定義されたルールの作成済み PDR に関連付けてから、それらを UPF に送信します。次に、UPF はこれらの URR を尊重し、使用状況を SMF に報告します。

## 設定の確認

構成を確認するには、次のコマンドを使用します：

**show running-config active-charging service** *active-charging_service_name* **rulebase** *rulebase_name* **action priority** *action_priority* **dynamic-only ruledef**

使用状況モニタリングキーが構成されている場合、その値は、次の出力の **umid** 構成の一部として表示されます。

```
show running-config active-charging service acs1 rulebase rba1
   active-charging service acs1
      rulebase rba1
         action priority 1 dynamic-only ruledef rda1 charging-action ca1 description
myrule1
         action priority 2 dynamic-only ruledef rda1 charging-action ca1 description
myrule2 umid 54
         action priority 3 dynamic-only ruledef rda3 charging-action ca3 description
myrule3
       exit
      exit
```

# OAM サポート

ここでは、この機能の操作、管理、およびメンテナンスに関して説明します。

## 使用率モニタリング統計情報

SMF サービス（smf-service）ポッドは、次の統計情報をサポートしています：

**PolicyPcfUpdatesTotal**

- 説明：PCF に対して使用状況レポートが送信された回数を表示します。
- Metrics-Type：統計情報
- ラベル
  - ラベル：**smf_current_procedure**
    - 説明：現在実行中の手順を表示します。

- 値：PDU セッションの変更 - PCF によって開始された、または PDN セッションの変更：ベアラーの追加、削除、または変更

- ラベル
  - ラベル： **trigger**
    - 説明：SMF で開始された手順のトリガーを表示します。
    - 値： usage_report

# N7 上の Ruledefs の QoS グループのサポート

## 機能説明

Ruledef の QoS グループ機能により、PCF はサブスクライバごとに Fair-Usage-Policy（FUP）を定義して適用できます。この機能により、個々のサブスクライバセッションごとに、特定の課金アクション パラメータとすべての QoS-of-ruledefs パラメータを変更できます。

Ruledef の QoS グループは、QGR とも呼ばれます。

次の QoS-group-of-ruledefs の属性がサポートされます。

- 優先順位：QoS-group-of-ruledefs の優先順位は、QoS-group-of-ruledefs の QoS パラメータを着信データ パケットに適用する優先順位を意味します。パケットが、セッションでアクティブ化された複数の QoS グループの一部である ruledef と一致すると、優先順位が最も高い QoS-group-of-ruledefs の QoS パラメータがパケットに適用されます。優先順位番号が小さいほど、そのグループの QoS パラメータ適用の優先順位が高くなります。
  QoS-group-of-ruledefs の優先順位は、各サブスクライバ セッションの PCF によって設定されます。
- フロー ステータス：IP フローが有効か無効かを示します。値は以下のとおりです。
  - アップリンクを有効化
  - ダウンリンクを有効化
  - 有効
  - 無効
  - 削除済み

  デフォルト値は [有効（Enabled）] です。

（注） QosGroupRuleDefs IE の属性は、CLI コマンドを使用して定義することはできません。これらの属性は、PCF でのみ設定および変更できます。

N7 インターフェイス経由で受信した定義済みの QoS-group-of-ruledefs で、個別のルール定義をダイナミックに追加または削除することはできません。

# 機能の仕組み

この項では、Ruledef の QoS グループ機能が実装されている方法について説明します。

UPF は、アクティブ課金サービス（ACS）で QoS-group-of-ruledefs の構成をプロビジョニングします。CLI では、名前付きの QoS ルール定義のグループにチャージング ルールおよびダイナミック ルールを追加または削除できます。単一の ruledef は複数の QoS-group-of-ruledef の一部にすることができます。このシナリオでは、優先順位の高い QGR が強制または考慮され、優先順位は N7 インターフェイスを介した PCF によって優先順位 IE を介して通信されます。

PCF は、SMF で構成されたすべての QoS-group-of-ruledef の名前と、それらに関連する ruledef の名前を認識します。PCF は、N7 メッセージで独自の AVP を使用して、サブスクライバ セッションの QoS-group-of-ruledefs をアクティブにして削除します。この AVP は、アクティブ化または削除する QoS-group-of-ruledefs の名前を指定します。

サブスクライバでは、QoS-group-of-ruledefs がアクティブになっていない可能性があります。着信トラフィックが、そのサブスクライバ セッションに関連付けられた QoS-group-of-ruledef を持たない ruledef と一致する可能性があります。その場合、アクションはそのルール定義の構成に基づいてのみ実行されます。

## QGR の処理フロー

次に、UPF での QGR 処理ロジックを示します。

- IE「Qos-Group-Of-Ruledef」の受信時に、スタティック構成で QGR を検索します。QGR の ruledef または group-of-ruledef ごとに、対応する PDR を検索し、受信した QGR FAR および QER ID で FAR および QER リストを更新します。
- UPlane の ruledef または group-of-ruledef PDR ごとに、優先順位の高い QGR の FAR-ID および QER-ID を関連付けます。
- SMF と UPF の両方で QGR マップを維持します。これは、QGR 名、優先順位、QER-ID、および FAR-ID で構成されます。必要に応じて、リカバリとルックアップに QGR マップを使用します。

## QGR パラメータ

SMF は、N4 インターフェイスを介して UPF にセッション確立または変更要求の QGR パラメータを送信します。

QGR 名と優先順位は、カスタム IE「QGR-INFO-LIST」で送信されます。フローアクションおよび帯域幅パラメータによって、新しい FAR および QER を個別に作成します。

QGR のダイナミック パラメータを変更すると、FAR および QER の更新がトリガーされます。

IE は、セッション確立または変更要求で送信されます。

**QGR IE**

```
Qos-Group-Of-Ruledef:
Name:
Operation:  (0 - Add  1 - Modify 2 - Delete)
Precedence:
FAR ID:
QER ID:
```

## UPF でのカスタム IE

このセクションでは、UPF で使用可能なカスタム IE を示します。

### Extended Apply Action

[拡張適用アクション（Extended Apply Action）] IE は、UPF がパケットに適用する必要があるアクションを示します。次の図のようにコードが書かれています。

**図 *231 :* 拡張適用アクション *IE***

| Octets | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = **200** (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | Spare | Spare | Spare | Spare | TERMFLOW | DL DROP | UL DROP |

523029

オクテット 5 は次のように符号化されます :

- ビット 1 : UL DROP（ドロップアップリンク）：1 に設定すると、アップリンク パケットのドロップ要求を示します。
- ビット 2 : DL DROP（Drop Downlink）：1 に設定すると、ダウンリンク パケットのドロップ要求を示します。
- ビット 3 : TERMFLOW（フローの終了/強制終了）：1 に設定されている場合、フローを終了する要求を示します。
- ビット 4 ～ 8 : 今後使用する場合のスペア（0 に設定）。

### QGR-INFO リスト

QGR-INFO リスト IE は、PCF から UPF に受信した QoS グループに関する情報を示します。UPF はフローを識別し、受信したパラメータを適用します。次の図のようにコードが書かれています。

図 *232 : QGR-INFO* リスト *IE*

| Octets | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = **241** (decimal) | | | | | | | |
| 3 to 4 | Length - n | | | | | | | |
| 5 to 6 | Number of QGR | | | | | | | |
| 7 | Spare | Spare | Spare | Spare | QER | FAR | QGRN | PRECED |
| 8 | QGR Operation (ADD = 0/MODIFY = 1/REMOVE = 2) | | | | | | | |
| 9 to 12 | QGR Precedence | | | | | | | |
| 13 | Length of QGR Name | | | | | | | |
| 14 to n | QGR Name | | | | | | | |
| n+1 to n+4 | FAR ID | | | | | | | |
| n+5 to n+8 | QER ID | | | | | | | |
| Same as 7 to n+8 | Next QGR Details (if any) | | | | | | | |

523030

オクテット 7（QGR 情報のビットベクトル）は次のようにエンコードされます。

- ビット 1 - PRECED（優先順位）：1 に設定すると、優先順位が存在することを示します。
- ビット 2 - QGRN（QGR 名）：1 に設定すると、QGRN 名が存在することを示します。
- ビット 3：FAR：1 に設定すると、FAR ID が存在することを示します。
- ビット 4：QER：1 に設定すると、QER ID が存在することを示します。
- ビット 5 ～ 8：今後使用する場合のスペア（0 に設定）。

SMF は、このビット ベクトル フィールドに基づいて QGR 情報をエンコードします。

### バースト サイズ

バーストサイズ IE は、MBR から UPF への UL およびDL バースト サイズに関する情報を示します。次の図のようにコードが書かれています。

図 *233 :* バースト サイズ *IE*

| Octets | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = **176** (decimal) | | | | | | | |
| 3 to 4 | Length - n | | | | | | | |
| 5 to 8 | UL Burst Size | | | | | | | |
| 9 to 12 | DL Burst Size | | | | | | | |

523031

### 適合アクション

適合アクション IE は、UL と DL の両方のパケットに適用する必要がある UPF のアクションを示します。次の図のようにコードが書かれています。

図 *234 :* 適合アクション *IE*

| Octets | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = **177** (decimal) | | | | | | | |
| 3 to 4 | Length - n | | | | | | | |
| 5 | Spare | Spare | Spare | Spare | Spare | MARK-DSCP | DROP | ALLOW |
| 6 | Spare | Spare | Spare | Spare | Spare | MARK-DSCP | DROP | ALLOW |
| 7 | UL Tos | | | | | | | |
| 8 | DL Tos | | | | | | | |

523032

## 超過アクション

超過アクション IE は、UL と DL の両方のパケットに適用する必要がある UPF のアクションを示します。次の図のようにコードが書かれています。

図 *235 :* 超過アクション *IE*

| Octets | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = **178** (decimal) | | | | | | | |
| 3 to 4 | Length - n | | | | | | | |
| 5 | Spare | Spare | Spare | Spare | Spare | MARK-DSCP | DROP | ALLOW |
| 6 | Spare | Spare | Spare | Spare | Spare | MARK-DSCP | DROP | ALLOW |
| 7 | UL Tos | | | | | | | |
| 8 | DL Tos | | | | | | | |

523033

次の表に、N4 メッセージに含まれるカスタム IE に関する情報を示します。

表 *410 : FAR* 形式

| **FAR ID** | 固有 **ID** |
|---|---|
| 拡張適用アクション | プライベート IE には、フローアクション許可、破棄アップリンク、破棄ダウンリンクと終了フローが含まれます。<br>拡張適用アクションの値は、PCF から QosGroupOfRuledef IE で受信した FlowStatus IE 値から派生します。 |

表 *411 : QER* 形式

| **QER ID** | 固有 **ID** |
|---|---|
| 最大ビットレート: | QGR の MBR（Kbps）。<br>• UL MBR<br>• DL MBR |

| QER ID | 固有 ID |
|---|---|
| バースト サイズ | バースト サイズを指定するプライベート IE。<br>• UL Burst<br>• DL バースト |
| 適合アクション | 適合アクションを構成するプライベート IE：<br>• アップリンク アクション<br>• アップリンク ToS<br>• ダウンリンク アクション<br>• ダウンリンク ToS |
| 超過アクション | 超過アクションを設定するプライベート IE。<br>• アップリンク アクション<br>• アップリンク ToS<br>• ダウンリンク アクション<br>• ダウンリンク ToS |

## PCF でのカスタム IE

PCF は、SmPolicyDecision 属性のカスタム IE「QosGroupRuleDefinition」を SMF に送信します。この IE は、QosGroupRuleName、refQosGroupQosData、FlowStatus、および Precedence 属性で構成されます。

PCF は、QGRDefs マップで QosGroupRuleName をキーとして、QosGroupRuleDefinition を値として（すべての属性とともに）送信することにより、「QGR の追加/更新」をトリガーします。

QGR の削除の場合、PCF は QosGroupRuleName をキーとして送信することで「Remove QGR」をトリガーし、値が NULL に設定されます。

次の表に、PCF によって送信されるカスタム IE を示します。

表 *412 : SmPolicyDecision* 属性

| Attribute name | データ型 | L | 基数 | 説明 | 適用性 |
|---|---|---|---|---|---|
| qosGroupQosData | マップ（QosGroupQosData） | O | 1..N | コンテンツが QosGroupQosData である qosGroupQosInfo のマップ。 | qosGroupQosInfo |

| Attribute name | データ型 | L | 基数 | 説明 | 適用性 |
|---|---|---|---|---|---|
| qosGroupRuleDefs | マップ（QosGroupRuleDef） | O | 1..N | QosGroupOfRuledefs のマップで、その内容が QosGroupRule 定義です。 | |

表 *413 : QosGroupRuleDef* 属性

| Attribute name | データ型 | L | 基数 | 説明 | 適用性 |
|---|---|---|---|---|---|
| qosGroupRuleId | string | M | 1 | SMF で構成された QoS Group of Ruledef（QGR）を一意に識別します | |
| refQosGroupQosData | string | M | 1 | QosGroupQosData への参照 | |
| flowStatus | FlowStatus | O | 0..1 | IP フローが有効か無効かを示します。<br>使用可能な値：アップリンクの有効化、ダウンリンクの有効化、有効化、無効化、削除<br>デフォルト値の「有効」が適用されます。 | |
| precedence | 単位数 | M | 0..1 | QosGroupRuleName で識別される Ruledef の QoS グループの優先順位を説明します。 | |

表 *414 : QosGroupQoSData* 属性

| 属性名 | データ型 | L | 基数 | 説明 | 適用性 |
|---|---|---|---|---|---|
| qos Id | 文字列 | M | 1 | QoSGroupQosData を一意に識別します。 | |
| maxbrDL | BitRateRm | M | | ダウンリンクの最大帯域幅を示します。 | |
| maxbrUL | BitRateRm | M | | アップリンクの最大帯域幅を示します。 | |

| | | | | | |
|---|---|---|---|---|---|
| mbrBurstSizeUL | MaxDataBurstVol | O | | アップリンクのピークレートで送信できるデータの量を表します。 | |
| mbrBurstSizeDL | MaxDataBurstVol | O | | ダウンリンクのピークレートで送信できるデータの量を表します。 | |
| mbrConformActionUL | RateLimitAction | O | | トラフィックがアップリンクの最大ビットレート内に留まる限り、実行されるレート制限アクションを説明します。 | |
| mbrConformActionDL | RateLimitAction | O | | トラフィックがダウンリンクの最大ビットレート内に留まる限り、実行されるレート制限アクションを説明します。 | |
| mbrExceedActionUL | RateLimitAction | O | | アップリンクでトラフィックが最大ビットレートを超えた場合に実行するレート制限アクションを説明します。 | |
| mbrExceedActionDL | RateLimitAction | O | | ダウンリンクでトラフィックが最大ビットレートを超えた場合に実行するレート制限アクションを説明します。 | |

表 *415 : RateLimitAction* 属性

| 属性名 | データ型 | L | 基数 | 説明 | 適用性 |
|---|---|---|---|---|---|
| action | アクション | M | | レート制限アクションを説明します。<br>列挙型アクション（値は ALLOW、DROP、MARK_DSCP） | |

| | | | | | |
|---|---|---|---|---|---|
| tosTrafficClass | string | C | | IPv4 サービス タイプとマスク フィールド、または IPv6 トラフィック クラス フィールドとマスク フィールドが含まれます。<br>tosTrafficClass IE は、アクション IE の値が MARK_DSCP である場合にのみ存在します。 | |

## データパスの適用

次に、UPF で実行されるデータ トラフィックの適用のシーケンスを示します。

1. 着信データ トラフィックが http ruledef と一致するかどうかを確認します。
2. 一致する ruledef または ruledef のグループを持つ QGR があるかどうかを確認します。優先順位が一番高い QGR が返されます。

（注） ruledef または ruledef のグループは、スタティックまたは事前定義のいずれかです。

3. QGR が一致した場合、フローアクションの適用は最初に課金アクション レベルで実行されてから QGR レベルで実行され、課金アクションでパケットが許可されたと見なされます。パケットがドロップされた場合、QGR レベル フローアクションの適用はスキップされます。
4. QGR のフローアクションによってパケットの通過が許可される場合、帯域幅制限または QoS 適用ルール（QER）制限がデータ パケットに適用されます。QGR でパケットがドロップされた場合、QER の制限はスキップされます。
5. フローアクションの適用と同様に、QER の制限は実行され、最初に課金アクション レベルで実行され、次に QGR でパケット対象が課金アクションで許可されます。

## コール フロー

ここでは、この機能の主要なコール フローについて説明します。

### Ruledef アクティベーション コール フローの QoS グループ

このセクションでは、ルール定義の QoS グループのアクティブ化に関連するコール フローについて説明します。

図 *236 : Qos-Group-of-Ruledef* のアクティブ化コール フロー

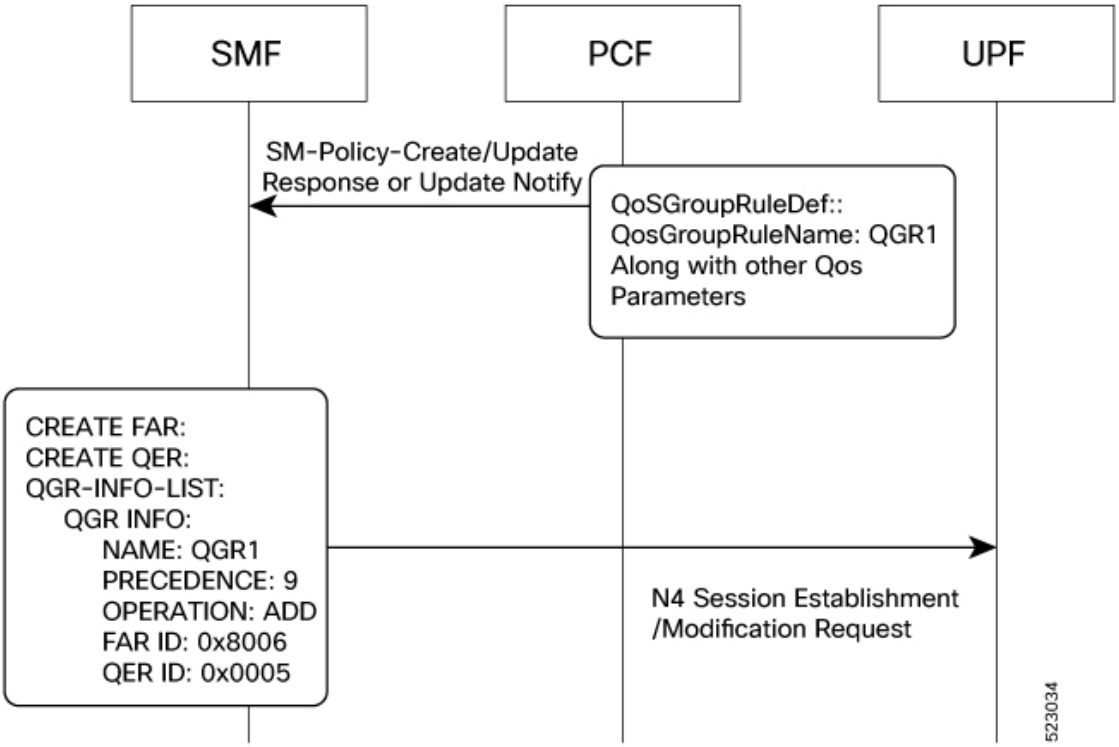



表 *416 :* ルール定義の *QoS* グループをアクティブ化するコール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | PCF は、N7 メッセージで受信したカスタム IE「QosGroupRuleDefs」を介して qos-group-of-ruledefs をアクティブにします。QosGroupRuleDefs IE は、QosGroupRuleName、refQosGroupQosData、FlowStatus、および precedence から構成されます。<br><br>PCF は、QGRDef マップで QosGroupRuleName をキーとして、QosGroupRuleDef を値として（すべての属性とともに）送信することにより、「QGR の追加」をトリガーします。<br><br>PCF は、N7 ポリシー関連付け確立応答またはポリシー関連付け更新要求メッセージを介して QosGroupRuleDefs IE を SMF に送信します。 |
| 2 | SMF は、PCF から受信した各 QGR に対して Create FAR および QER を準備し、QoS グループ名を対応する FAR ID および QER ID とともに QGR-INFO-LIST IE でエンコードして、N4 インターフェイス セッションの確立または変更要求時に送信されます。 |

## Ruledef 変更コール フローの QoS グループ

このセクションでは、ルール定義の QoS グループの変更に関連するコール フローについて説明します。

図 *237 : Qos-Group-of-Ruledef* 変更コール フロー

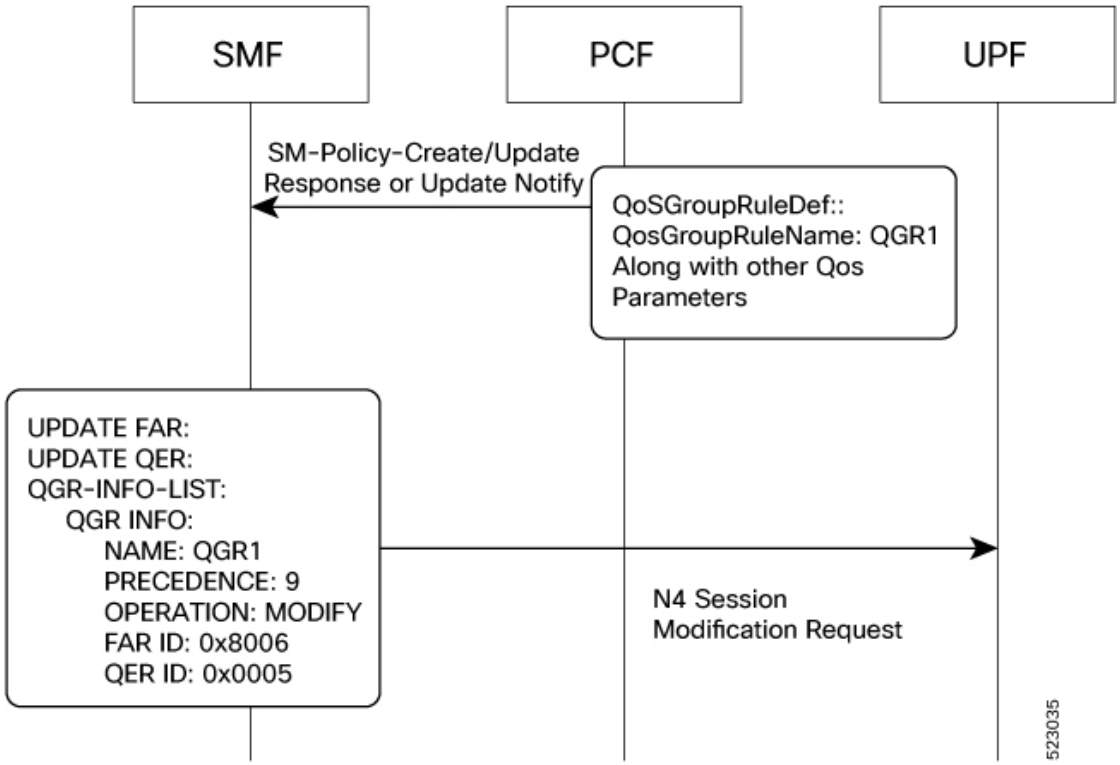



表 *417 :* ルール定義の *QoS* グループを変更するコール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | qos-group-of-ruledefs がアクティブになると、PCF は N7 メッセージからの SM ポリシー関連付け確立応答および SM ポリシー関連付け更新要求で送信される「QoSGroupRuleName」IE を介して QoS パラメータを変更します。<br>PCF は、QGRDef マップで QosGroupRuleName をキーとして、QosGroupRuleDef を値として（すべての属性とともに）送信することにより、「QGR の変更」をトリガします。<br>PCF は、N7 ポリシー関連付け確立応答またはポリシー関連付け更新要求メッセージを介して QosGroupRuleDefs IE を SMF に送信します。 |

| ステップ | 説明 |
|---|---|
| 2 | SMF は、変更に対して受信した各 QGR に対して FAR および QER の更新を準備し、アクティブ化した QoS グループ名を対応する FAR ID および QER ID とともに QGR-INFO-LIST IE でエンコードして、N4 セッションの確立または変更要求時に送信されます。 |

### ルールデフ非アクティブ化コール フローの QoS グループ

このセクションでは、ルール定義の QoS グループの非アクティブ化に関連付けられているコール フローについて説明します。

**図 *238 : Qos-Group-of-Ruledef* の非アクティブ化コール フロー**

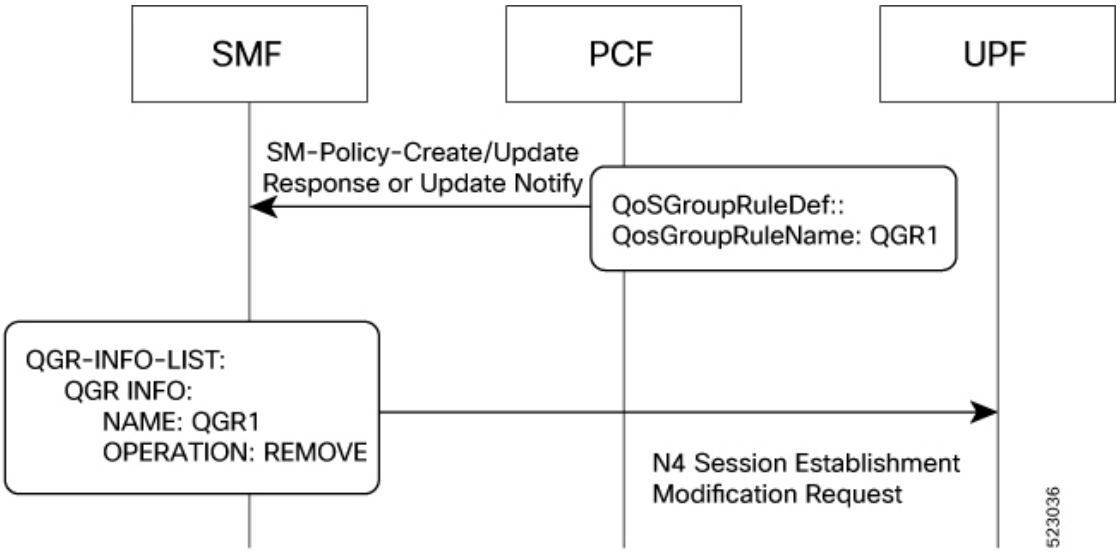


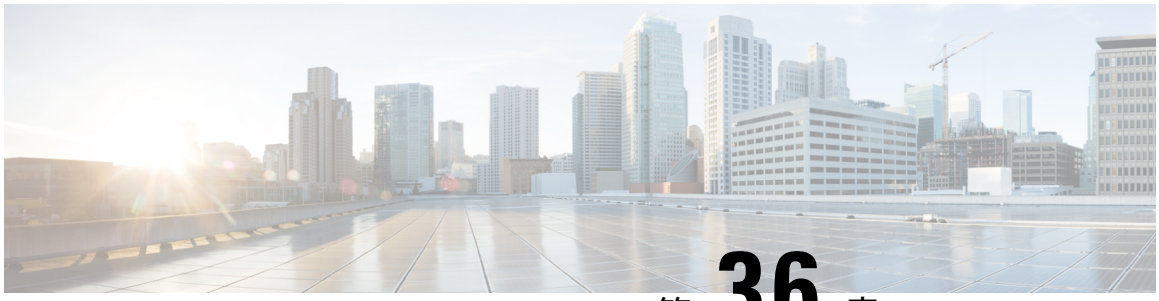

**表 *418 :* ルール定義の *QoS* グループの非アクティブ化のコール フローの説明**

| ステップ | 説明 |
|---|---|
| 1 | PCF は、値が NULL の QosGroupRuledefName であるマップ キーのみを送信することにより、「QosGroupRuleDefs」IE を介して qos-group-of-ruledefs を非アクティブにします。 |
| 2 | SMF は、N4 セッション変更要求で送信される QGR-INFO-LIST で、ruledef 名の非アクティブ化された QoS グループを QGR-INFO-LIST でエンコードします。 |

## 制限事項

QoS Group of Ruledefs（QGR）サポート機能には、次の制限があります。

- [モニタリング（Monitoring）]：QGR に関連付けられたキーの使用状況はモニタリングされません。URR の作成および適用はサポートされません。
- PCF は QosGroupRuleDef IE を個別に送信しません。PCC ルールとともに送信されます。
- SMF では、最大 20 個の QosGroupRuleDef をサポートします。つまり、SMF は PCF から最初の 20 個の QosGroupRuleDef のみを受け入れます。
- FlowStatus 属性に無効な値が受信された場合、PCF の QosGroupRuleDef 属性は無視されません。FlowStatus は、属性のデフォルト値である ENABLED と見なされます。



第 36 章

# RADIUS 認証およびアカウンティング


- 機能の概要と変更履歴, on page 1407
- 機能説明, on page 1409
- 機能の仕組み, on page 1415
- RADIUS クライアントの構成, on page 1441
- RADIUS クライアント OA & M サポート, on page 1461
- トラブルシューティング情報 （1469 ページ）


## 機能の概要と変更履歴

### 要約データ

***Table 419:*** 要約データ

| | |
|---|---|
| 該当製品または機能エリア | SMF |
| 該当プラットフォーム | SMI |
| 機能のデフォルト設定 | 無効：設定が必要 |
| このリリースでの関連する変更点 | N/A |
| 関連資料 | 該当なし |

### 更新履歴

***Table 420:*** マニュアルの変更履歴

| 改訂の詳細 | リリース |
|---|---|
| RADIUS エンドポイントの動的な構成変更のサポートが追加されました。 | 2023.03.0 |

| 改訂の詳細 | リリース |
| --- | --- |
| RADIUS アクセス応答属性のセキュリティ グループ タグのサポートが追加されました。 | 2023.01.4 |
| 次に対するサポートが追加されました。<br>• 3GPP ディクショナリ<br>• Allow-auth<br>• 連続的障害<br>• 最大転送数 | 2023.03.0 |
| ISE とのインターワーキングのサポートが追加されました。 | 2021.02.2.t1.0 |
| TFT の変更時に RADIUS アカウンティング トリガーを生成するために、課金プロファイルに新しい CLI オプションが導入されました。 | 2021.02.0 |
| RADIUS でのインスタンス認識をサポートするために、SMF では次の作業が可能です。<br>• RADIUS プロファイルでのインスタンス レベルの設定<br>• NAS-IP-Address および NAS-Identifier 属性は、RADIUS プロファイル構成で instance-id ごとに構成できます。<br>• RADIUS エンドポイント設定のインスタンス ID ごとの RADIUS 切断要求 VIP 設定 | 2021.02.0 |
| 次のサポートが追加されました<br>• PAP、CHAP および MSCHAP ベースの RADIUS 認証<br>• 複数の RADIUS NAS-IP 送信元アドレス<br>• RADIUS 切断および CoA 要求の処理<br>• SMF の RADIUS アカウンティング<br>• RADIUS アクセス応答メッセージの新しい属性 | 2020.02.5.t1 |
| 最初の導入。 | 2020.02.0 より前 |

# 機能説明

リモート認証ダイヤルインユーザーサービス（RADIUS）は、クライアントとサーバのプロトコルです。通常、RADIUS クライアントはネットワーク アクセス サーバ（NAS）で、RADIUS サーバは UNIX または Windows NT マシンで実行されているデーモン プロセスです。クライアントは指定された RADIUS サーバにユーザ情報を渡し、返された応答に応じた動作をします。RADIUS サーバはユーザ接続要求を受信し、ユーザを認証してから、このユーザへのサービス提供にクライアントが必要とする設定情報を返します。

RADIUS は、ユーザーに認証サービスとアカウンティング サービスを提供します。SMF では、次の構成に対し最大 2048 がサポートされます。

- RADIUS サーバの詳細を追加します。
- RADIUS アカウンティングおよび認証を有効にします。
- DNN プロファイル内で仮想 APN 構成のオプションとして RADIUS インターフェイスを追加します。
- CC トリガ レポートを有効にします。
- ボリュームと時間の制限を定義します。

RADIUS クライアントは、次の機能をサポートしています。

- **サーバの選択**

  RADIUS サーバは、キーとして [IP: Port] を使用して設定されています。 **algorithm** CLI は、認証またはアカウンティング要求を送信する RADIUS サーバを選択するためのフェールオーバーまたはロード バランシング アルゴリズムを指定します。「デッド」とマークされたサーバは、「アライブ」とマークされるまで選択対象として考慮されません。サポートされているアルゴリズムは、ファーストサーバとラウンドロビンです。

  - ファーストサーバ：要求を最も優先順位の高い RADIUS サーバに送信する必要があることを指定します。サーバが到達不能になった場合、要求は構成されている次に高い優先順位を持つサーバに送信されます。これはデフォルトのアルゴリズムです。
  - ラウンドロビン：要求を循環キュー方式のロードバランシングに基づいて送信する必要があることを指定します。最後に使用されたサーバが保存され、ラウンドロビン選択が維持されます。リストの順序は、構成シーケンスにのみ基づいています。

- **サーバ検出とデッドサーバ検出の監視**

  AAA Dead-Server Detection 機能を使用すると、RADIUS サーバをデッド状態と指定するための条件を構成できます。デッドサーバを識別するために設定できる 2 種類のパラメータは次のとおりです。

  - **Response-timeout**：モニタ サーバはサーバデータベースを再アクセスし、最初の要求が送信された後、構成されている「response-timeout」値を超える応答を受信していないサーバをマークします。サーバは「デッド」とマークされ、「デッドタイム」とし

て構成された分数の間デッド状態のままになります。「デッドタイム」の時間が経過すると、サーバのデッド変数が再度リセットされ、要求を処理する準備ができているとマークされます。それでもサーバに到達できない場合は、次の要求応答タイムアウトの一部として「デッド」とマークされます。

- **連続した失敗**：RADIUS サーバがデッド状態と指定されるまでにコントローラで発生する必要がある連続タイムアウト回数を構成することもできます。要求が再試行要求か通常の要求かにかかわらず、サーバが応答を返さない場合（つまり、要求のタイムアウト）、失敗数は増加します。サーバの障害数が連続障害のしきい値に達すると、当該サーバはデッド サーバとして宣言されます。

- **タイムアウトと再試行**

  サーバが選択され、要求がサーバに送信されると、RADIUS サーバから応答が受信されるまで、またはタイムアウトが発生するまで、エントリは要求キューに保持されます。[要求のモニタ（Monitor Requests）] が呼び出されると、要求キューの応答タイムアウトがチェックされ、再試行されます。すべてのエントリを順を追って調べ、「タイムアウト」として構成された要求タイムアウト値がヒットしているかどうかをチェックします。このような要求では、再試行回数が構成された「max-retries」値未満の場合、要求は RADIUS サーバに再送信されます。または、「max-retries」カウントに達すると、要求は要求キューから削除されます。要求が削除されると、その要求に対する応答があった場合でも、応答は破棄され、ユーザーに送信されません。

- **最大伝送**

  最大伝送では、使用可能なすべてのサーバの伝送パラメータを構成できます。この機能は、要求の再試行サイクルが終了した後に、送信回数が再試行回数を超えているかどうかをクロスチェックするのに役立ちます。その場合、使用可能な時は別のサーバーで後続の再試行サイクルが開始されます。サーバが利用できない場合、または maxtransimissions 制限に達した場合、タイムアウト応答が送信されます。

  **例**：max-transmissions 値が 5 に設定されている場合、最大再試行値は 2 であり、使用可能なサーバが 2 つあります。したがって、最初のサーバで 3 回の試行（実際の試行が 1 回、再試行が 2 回）、残りの 2 回（実際の試行が 1 回、再試行が 1 回）が 2 番目のサーバにあります。

# RADIUS 認証

認証とキー管理は、ユーザーとネットワークの間に相互認証を提供するため、モバイルネットワークのセキュリティの基本です。

5G では、ユーザーを認証するためのさまざまな認証方法が定義されています。5G アーキテクチャでは、サービスを提供するネットワークは、プライマリ認証メカニズムを使用してサブスクリプション永久識別子（SUPI）を認証し、UE とネットワーク間のキー契約を認証します。

RADIUS クライアント機能をイネーブルにする方法については、RADIUS クライアントの構成（1441 ページ）を参照してください。

### アイデンティティ サービス エンジン

Identity Services Engine（ISE）は、5Gおよびその他のエンタープライズデバイスのポリシー定義の共通ポイントです。5G as a Service（5GaaS）アーキテクチャでは、ISE は認証とアカウンティングのみを実行します。Control Center は 5G 認証を処理します。RADIUS Authorize-Only フローを使用して 5G 認証を実装できます。

SMF は、Cisco private 5G の ISE との通信をサポートしています。SMF が ISE から受信するポリシーに基づいて、Cisco Private 5G はエンタープライズ側でのさまざまな動作をサポートします。ISEは、サブスクライバの識別、サブスクライバのグループの定義、ポリシーの割り当てなどのタスクを実行するためのメカニズムをエンタープライズ カスタマーに提供します。

### Allow-auth

構成で allow-auth が有効になっている場合、認証の成功、タイムアウト、またはエラー メッセージの受信に関係なく、進行中のコールを続行できます。デフォルト値は false ですが、allow-auth を有効にするには構成が必要です。

## スループットの制限

SMF でセカンダリ認証を構成している場合、SMF は、構成されている RADIUS サーバ アドレスに基づいて RADIUS アクセス要求を ISE に送信します。SMF はアクセス要求に PEI を追加します（可能な場合）。構成された IMEI ベースの ISE には、スループット制限を実現するためにプライベート 5G ネットワークに適用されるルールの名前が含まれています。

（注） スループット制限では、IMEI または IMSI のいずれかを使用できます。

ISE は、アクセス承認要求の 3GPP-Policy-Reference 属性にルール名を入力します。このルールベースは SMF で構成できます。SMF は、3GPP-Policy-Reference 属性に含まれるオクテット文字列から ASCII 値を派生させます。次に、SMF はこの値を構成済みのルールベースと照合します。

次の表に、3GPP-Policy-Reference AVP のオクテット値を示します。

***表 421 : 3GPP-Policy-Reference AVP***

| | ビット | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Octets** | **8** | **7** | **6** | **5** | **4** | **3** | **2** | **1** |
| 1 | 3GPP Type = 113 | | | | | | | |
| 2 | 3GPP Length = m | | | | | | | |
| 3-m | ポリシー データ参照先（オクテット文字列）<br>（注）<br>DN AAA はポリシー データ参照値を送信します。SMF はこの値を使用して、PCF の SM および QoS ポリシー データを取得します。 | | | | | | | |

ISE はルールベースを SMF に送信します。SMF は、構成されていないルールベースを受信しても無視します。SMF でデフォルトの帯域幅ポリシーを設定していない場合、帯域幅ポリシーは無視されます。

UE が 4G RAT または 5G RAT を介して接続する場合、SMF で帯域幅制限を構成できます。4G RAT によって構成された帯域幅制限に基づいて、SMF はセッション応答の作成に BearerQoS 値を入力します。5G RAT によって構成された帯域幅制限に基づいて、SMF は N1 PDU Establishment Accept 要求の QosFlowDescription 値を入力します。

帯域幅制限は、SMF から送信される事前定義済みのルールに基づいて、UPF 上でローカルに構成されます。

# RADIUS アカウンティング

アカウンティングは、請求、監査、および報告のために使用される加入者の利用状況およびアクセス情報を収集し、送信します。たとえば、ユーザーは開始時刻と終了時刻、実行されたアクション、パケット数、バイト数を識別します。アカウンティングを使用すると、オペレータはユーザーが利用するサービスと、そのサービスが消費するネットワーク リソースの量を分析することができます。アカウンティング レコードは、アカウンティング属性値ペア（AVP）で構成され、アカウンティング サーバに格納されます。このアカウンティング情報を分析すると、ネットワーク管理、クライアント課金、監査の3つすべて、または監査に利用できます。

SMF は CLI 構成を使用して RADIUS アカウンティング機能を実装します。構成の詳細については、「RADIUS クライアントの構成 （1441 ページ）」を参照してください。

RADIUS アカウンティングが有効で、DNN プロファイル内でサーバ グループが構成されている場合、SMF は N4 セッション確立要求の課金パラメータでサーバ グループを AAA グループとして送信します。SMF が UPF に存在しない AAA グループを送信すると、RADIUS URR の静的ルールと事前定義済みルールのトラフィックが考慮されず、レポートに失敗します。このシナリオでは、SMF は RADIUS URR のアカウンティングでダイナミック ルール トラフィックのみを考慮します。

# RADIUS 切断要求メッセージの処理

動的認可クライアント（DAC）は、UDP ポートを介して RADIUS エンドポイント（radius-ep）に接続解除要求パケットを送信します。DAC は、このパケットを送信して、ネットワーク アクセス サーバ（NAS）上のユーザー セッションを終了させます。また、関連付けられているすべてのセッション コンテキストが破棄されます。

切断要求パケットには、終了するセッションを識別する次のセッション識別属性が含まれます。

- 3GPP-IMSI + 3GPP-NSAPI
- ACCT-SESSION-ID
- CALLED-STATION-ID (DNN) + FRAMED-IP-ADDR
- CALLED-STATION-ID (DNN) + FRAMED-IPV6-PREFIX

RADIUS エンドポイントは、Disconnect-Request パケットを検証します。検証が失敗した場合、エンドポイントはパケットを拒否し、適切な原因コードを含む Disconnect-NAK メッセージを DAC に送信します。検証が成功すると、エンドポイントはセッション識別キーまたは属性に基づいてアフィニティ検索を実行します。その後、エンドポイントは切断要求パケットを特定の SMF サービス インスタンスに転送します。SMF はパケットを処理し、PDU リリースまたは PDN 切断手順をトリガします。セッションが識別され、削除され、無効になった場合、SMF は適切な原因コードを含む切断 ACK 応答を送信します。セッション コンテキストが見つからない場合、SMF は適切な原因コードを含む Disconnect-NAK メッセージを送信します。SMF は、切断 ACK または NAK 応答を送信するための解放手順の完了を待機しません。

ローミング シナリオでは、ローミング ステータスがローミングの場合、ホームルーティング サブスクライバに対して RADIUS 接続解除要求がサポートされます。hSMF は SMF サービスとして機能し、セッションの解放手順を開始します。

（注） 4G および EpsInterworkingIndication でのローミングはサポートされていません。そのため、IMSI キーと NSAPI キーの組み合わせはサポートされていません。

この機能は、セッション識別キーまたは属性の組み合わせを使用して、終了すべきセッションを識別します。

**重要** 複数のキーの組み合わせが同じセッションに対して指定された場合、それは受け入れられます。ただし、複数のキーの組み合わせが複数のセッション コンテキストまたは存在しないセッション コンテキストになる場合、動作は非決定的です。

SMF は、Disconnect-Message（DM）要求ごとに 1 つのセッション コンテキストだけをサポートします。SMF では、DM 要求で次の属性を使用して、終了する NAS およびユーザーセッションを特定できます。

| 属性 | 参考仕様 | エンコード タイプ |
|---|---|---|
| 3GPP-IMSI | 3GPP 29.061 - 16.4.7.2-1 | 文字列 |
| 3GPP-NSAPI | 3GPP 29.061 - 16.4.7.2-10<br>3GPP 29.561 – 11.3 | 文字列 |
| Accounting-Session-Id | RFC 2866 | 文字列 |
| FRAMED-IP | RFC 2865 - 5.1 | IPv4 アドレス（IPv4 Address） |
| FRAMED-IPV6-PREFIX | RFC 3162 | PrefixLen および String |
| CALLED-STATION-ID (DNN) | RFC 2865 - 5.30 | 文字列 |
| NAS-IP-Address | RFC 2865 – 5.4 (optional) | 文字列 |

| 属性 | 参考仕様 | エンコード タイプ |
|---|---|---|
| NAS-Identifier | RFC 2864 – 5.32 (optional) | 文字列 |

パケットのデコードが成功すると、SMF は DM 要求に存在する他の属性をサイレントに廃棄します。

SMF は、DM ACK または NAK 応答で次の属性をサポートします。

| 属性 | 参考仕様 | エンコード タイプ |
|---|---|---|
| ERROR-CAUSE | RFC 5176 – 3.5 | 整数（Integer） |
| REPLY-MESSAGE | RFC 2865 – 5.18 | 文字列 |

切断要求が radius-ep によって拒否された場合、RADIUS エンドポイント ポッドは次のエラーコードをサポートします。

- 402（属性の欠落）：無効なキーの組み合わせが原因でトリガされます。
- 403（NAS IDの不一致）：DM 要求の NAS-IP 属性がエンドポイントの COA-NAS VIP-IP と一致しない場合、または要求の NAS-Identifier 属性が RADIUS ダイナミック認可内または CoA 構成内で NAS 識別子構成を行う場合にトリガされます。
- 407（無効な属性）：フォーマットエラー、エンコードエラーなどが原因でトリガされます。
- 405（サポートされていないサービス）：要求が接続解除要求でない場合にトリガされます。
- 503（見つかっていないセッション コンテキスト）：セッションが見つからない場合にトリガされます。

この機能の構成の詳細については、セッション切断機能の構成 （1459ページ） のセクションを参照してください。

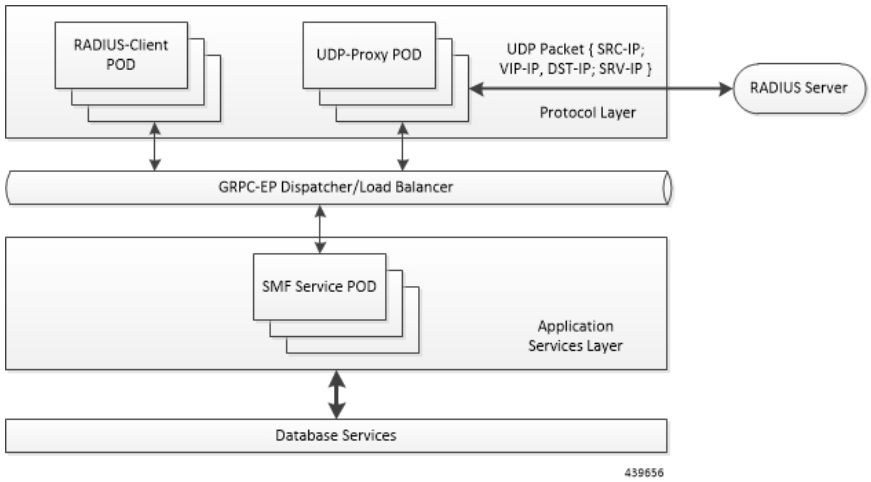
# アーキテクチャ

## SMF での RADIUS クライアント統合

RADIUS クライアントポッドは、5G アーキテクチャのプロトコル層に存在します。

次の図は、SMF での RADIUS クライアントの統合を示しています。

*Figure 239: RADIUS* クライアントの統合




**Radius-EP アプリ（RADIUS-Client Pod）**：RADIUS クライアント機能が新しいポッドに追加されました。認証やアカウンティングなど、RADIUS プロトコル固有の機能を処理します。

**SMF サービス アプリ（SMF サービスポッド）**：SMF サービス アプリは、PDU セッション サービスを提供します。SMF サービスは、セッションの確立中にセカンダリ認証が必要かどうかを判断し、それに応じて動作します。

**UDP プロキシ アプリケーション（UDP-Proxy Pod）**：UDP プロキシ アプリケーションは、ホスト ネットワーキングで有効になっており、外部仮想 IP を使用してパケットを通信します。すべての RADIUS パケットは、このアプリケーションを使用して外部クラスタと送受信されます。

# 機能の仕組み

このセクションでは、SMF が RADIUS 認証およびアカウンティングの機能をサポートする方法について説明します。

## 認証のための RADIUS インタラクション

RADIUS サーバがユーザーを認証するために、さまざまな方法をサポートします。サーバがユーザーのユーザー名と元のパスワードを受け取った場合、ポイントツーポイントプロトコル（PPP）、パスワード認証プロトコル（PAP）、チャレンジハンドシェイク認証プロトコル（CHAP）、またはMicrosoft CHAP（MSCHAP）、UNIX ログイン、その他の認証方式をサポートできます。

SMF は、PAP、CHAP、または MSCHAP プロトコルを使用したユーザー認証をサポートしています。SMF の構成は、ユーザー認証のプロトコルの選択に役立ちます。DNN プロファイルでセカンダリ認証が有効になっている場合、SMF は RADIUS サーバと対話して RADIUS 認証を実行します。認証を実装するために、SMF 内に存在する RADIUS クライアントは、

Access-Request メッセージで User-Name 属性と User-Password 属性を RADIUS サーバに送信します。

SMF は、RADIUS 認証機能を容易にするために、より多くの属性を使用します。サポートされている属性の完全なリストについては、RADIUS 属性定義, on page 1431 セクションを参照してください。

RADIUS サーバは、認証情報を使用してユーザーを検証します。検証が成功すると、サーバは Access-Accept 応答を SMF に送信します。

### PAP、CHAP、または MSCHAP ベースの認証の構成

SMF は、UE から受信したプロトコル コンフィギュレーション オプション（PCO）、拡張 PCO（ePCO）、または追加 PCO（APCO）IE をデコードします。次に、SMF は IE から PAP（ユーザー名とパスワード）、CHAP（チャレンジ/レスポンス）、または MSCHAP（チャレンジ/レスポンス）に関連する値を取得します。いずれかのプロトコルの DNN での構成優先順位が高い場合、SMF は RADIUS Access-Request メッセージで受信した値を RADIUS サーバに送信します。

**Note** SMF は、プライオリティが構成されていない場合、UE から受信した認証情報を RADIUS Access-Request メッセージに含めません。

デフォルトでは、SMF は PCO、ePCO、または APCO で受信したパスワードを使用するように追加の構成が有効になるまで、DNN の下で構成されたホストパスワードを認証に使用します。SMF を使用すると、オペレータは DNN プロファイルのホスト パスワードをプレーンテキストまたは暗号化形式のいずれかで構成でき、可能な場合は常に同じ暗号化形式でのみ表示されます。

SMF は、UE が PAP ベースの認証のために PCO IE で明示的にユーザー名を提供しない場合、ユーザー名として MSISDN を送信します。

CHAP ベースの認証の場合、**convert-to-mschap** コマンド オプションが有効で、CHAP が有効で、受信した CHAP 応答の長さが 49 バイトの場合、SMF は、受信した CHAP チャレンジと応答を MSCHAP に変換します。デフォルトでは、SMF は認証アルゴリズムとして MSCHAPv1 を使用します。

MSCHAP ベースの認証において、プロトコル ID が LCP であり、かつ LCP コンテナが RFC 2433 に基づく CHAP/MSCHAPv1 (128) または RFC 2795 に基づく CHAP/MSCHAPv2 (129) をアルゴリズムとして指定している場合、SMF は PCO で受信したユーザー名、チャレンジ、および応答を RADIUS サーバに送信します。

SMF は、4G/Wi-Fi セッションの場合は Create-Session-Response PCO/EPCO/APCO IE、5G セッションの場合は N1 Container EPCO IE で、RADIUS サーバから UE に認証情報を転送します。

RADIUS 認証機能を実装する場合は、次の重要な点を考慮してください。

- RFC 2865 に基づいて、この機能に適用可能なさまざまな AVP の長さ検証を実行します。また、違反が識別された場合、認証を拒否します。

- CHAP チャレンジの最小長は 5 バイトです（ただし、RFC 1334 および RFC 1994 で 1 バイトです）。

- SMF は、構成された認証アルゴリズムに基づいて、DNN レベルで受信した認証情報を UE から RADIUS サーバに送信します。SMF は UE から受信したデータを操作せず、情報を RADIUS サーバに送信する前に、認証に関連する構成のみを適用します。
- SMF は IPv4 または IPv6 アドレスをセッションに割り当て、RADIUS アカウンティング メッセージを介して RADIUS サーバに FRAMED-IP または FRAMED-IPv6-PREFIX 属性を送信します。RADIUS サーバは、この属性情報を使用して電話番号と IP アドレスを関連付けます。
- SMF では、PDU セッションのライフタイム中に複数の認証を許可しないため、すべての認証の ID 値を増加させるユースケースを検証しません。
- SMF は、UE から空のパスワードを受信し、SMF で構成されたホスト レベルのパスワードが構成されていない場合、または **password-use-pco** オプションが有効になっていない場合、Access-Request で暗号化された NULL（空の）パスワードを送信します。
- SMF は、次のシナリオで、Access-Request が構成されたサーバ シークレットをユーザー パスワードとして伝送するデフォルト認証にフォールバックします。
  - アルゴリズム設定のいずれも優先順位とともに有効になっていない場合
  - UE によって提供された情報が、構成されたアルゴリズムの構成に適用できない場合（存在する場合）
  - UE がデータなしで空の PAP または CHAP コンテナを送信した場合（コンテナの長さは 0）
- SMF は、次のシナリオで認証を拒否します。
  - 他の認証アルゴリズムが構成されていない場合
  - CHAP チャレンジ コンテナと CHAP 応答コンテナの両方で受信した CHAP 識別子に不一致がある場合（SMF は現在、CHAP チャレンジ コンテナから CHAP ID をコピーします）
    - CHAP パスワードの CHAP-ID は、RFC 2865 に従って CHAP 応答から取得する必要があります。
    - 応答識別子は、RFC 1334 に従ってチャレンジ応答の [識別子（Identifier）] フィールドからコピーする必要があります。
    - 現在のアルゴリズムの検証基準が失敗したとき
- 明示的に 0 を構成すると構成が無効になるため、SMF では、CLI を通して異なるアルゴリズムに対して同じ優先順位を構成できます。このシナリオでは、アルゴリズムのいずれかが考慮され、選択は純粋に実装に依存します。UE が SMF に複数の認証コンテナを送信す

るたびに、競合を解決するために、異なるアルゴリズムに異なる優先順位を構成するのは、オペレータの責任です。

- SMF では、YANG 定義の構文形式の制限により、PAP を設定せずに **password-use-pco** オプションを構成できます。同じことが **convert-to-mschap** オプションにも適用されます。ただし、この機能は、対応するアルゴリズムが有効な優先順位で有効になっている場合にのみ機能します。
- デフォルトでは、SMF はオペレータがホスト レベルで設定したパスワードを、平文の場合 AES-128-CFB 暗号化アルゴリズムを用いて暗号化します。オペレータが AES-128-CFB 暗号化標準を満たす必要があるすでに暗号化されたパスワードを指定した場合、暗号化は無視されます。
- デフォルトでは、受信した CHAP 応答の長さが 49 バイトで、 **convert-to-mschap** オプションが有効の場合、SMF は受信した CHAP チャレンジと応答が MSCHAP に変換されるたびに、認証アルゴリズムを MSCHAPv1(128) と見なします。
- 以下は、SMF でサポートされる MSCHAP 固有の AVP とその RFC リファレンスのリストです。
  - MSCHAP-CHALLENGE（MSCHAP）（RFC2548 セクション 2.1.2）
  - MSCHAP-RESPONSE（RFC2548 セクション 2.1.3）
  - MSCHAP2-RESPONSE（RFC2548 セクション 2.3.2）
  - MSCHAP-ERROR RFC2548（セクション 2.1.5）
  - MS-CHAP2-Success（RFC 2548、セクション 2.3.3）は、RFC 2548 に v1 の MS-CHAP 成功 AVP に関する明確な情報がないため、サポートされていません。
- RADIUS サーバが Access-Reject メッセージで MSCHAP-Error と Reply-Message AVP の両方を送信すると、PCO/APCO/EPCO で NACK の CHAP コンテナを埋めるときに、MSCHAP-ERROR が優先されます。MSCHAP-Error は、MSCHAPv1 アルゴリズムと MSCHAPv2 アルゴリズムの両方に共通であり、CHAP Failure コンテナの [メッセージ（Message）] フィールドにカプセル化されます。
- MSCHAP では、認証機能だけがサポートされています。

**Important** SMF は、組み込みの暗号化アルゴリズム「AES-128-CFB」を使用して、NETCONF-YANG データ モデルによって提供されるホスト レベルのパスワード（アウトバウンド パスワード）を暗号化します。SMF Ops Center は、AES-128-CFB 暗号化のグローバル キーを作成します。これは、プレーン テキスト パスワードが与えられたオペレータの暗号化に使用されます。それぞれのポッドで暗号化されたデータを復号化するために、SSH を介してすべてのポッドとキーを共有します。キーは、SMF-SERVICE ポッドに ENV 変数「CONFD_AES_KEY」としてエクスポートされます。オペレータがすでに暗号化されたパスワードを構成する場合は、AES-CFB-128 暗号化文字列の先頭に「$8$」を「$8$<encrypted-data> 」のように追加する必要があります。指定された入力がすでに NETCONF-YANG モデルに対する AES-128-CFB 暗号化文字列であることを示します。

認証に関連する CLI の詳細については、RADIUS クライアントの構成, on page 1441 の項を参照してください。

# RADIUS 認証属性

### RADIUS アクセス リクエスト属性

次のテーブルは、RADIUS アクセス リクエスト メッセージでサポートされている属性をリストします。

| 属性 | 参考仕様 | エンコード タイプ |
|---|---|---|
| USER-NAME | RFC2865 - 5.1 | 文字列 |
| PASSWORD | RFC2865 - 5.2 | 暗号化された文字列 |
| CALLING-STATION-ID | RFC2865 - 5.31 | 文字列 |
| CALLED-STATION-ID | RFC2865 - 5.30 | 文字列 |
| NAS-IP-ADDRESS | RFC2865 - 5.4 | IPv4 アドレス（IPv4 Address） |
| NAS-IDENTIFIER | RFC2865 - 5.32 | 文字列 |
| SERVICE-TYPE | RFC2865 - 5.6 | オクテット - 4 バイト |
| FRAMED-PROTOCOL | RFC2865 - 5.7 | オクテット - 4 バイト |
| NAS-PORT-TYPE | RFC2865 - 5.41 | オクテット - 4 バイト |
| NAS-PORT | RFC2865 - 5.5 | オクテット - 4 バイト |
| SERVING-NETWORK-NAME | 3GPP TS 29.561 - 16.4.0、RFC2865 | 文字列 |
| 3GPP-IMSI | 3GPP 29.061 - 16.4.7.2-1 | 文字列 |
| 3GPP-CHARGING-ID | 3GPP 29.061 - 16.4.7.2-2 | オクテット - 4 バイト |
| 3GPP-PDP-TYPE | 3GPP 29.061 - 16.4.7.2-3 | オクテット - 4 バイト |

| 属性 | 参考仕様 | エンコード タイプ |
|---|---|---|
| 3GPP-CHARGING-GATEWAY-ADDR | 3GPP 29.061 - 16.4.7.2-4 | IPv4 アドレス（IPv4 Address） |
| 3GPP-GPRS-NEG-QOS-PROFILE | 3GPP 29.061 - 16.4.7.2-5<br>3GPP 29.274 - 8.7 | 特別エンコード オクテット |
| 3GPP-SGSN-ADDRESS | 3GPP 29.061 - 16.4.7.2-6 | IPv4 アドレス（IPv4 Address） |
| 3GPP-GGSN-ADDRESS | 3GPP 29.061 - 16.4.7.2-7 | IPv4 アドレス（IPv4 Address） |
| 3GPP-IMSI-MCC-MNC | 3GPP 29.061 - 16.4.7.2-8 | 文字列 |
| 3GP-GGSN-MCC-MNC | 3GPP 29.061 - 16.4.7.2-9 | 文字列 |
| 3GPP-NSAPI | 3GPP 29.061 - 16.4.7.2-10<br>3GPP 29.561 – 11.3 | 文字列 |
| 3GPP-SELECTION-MODE | 3GPP 29.061 - 16.4.7.2-12 | 文字列 |
| 3GPP-CHARGING-CHARACTERISTICS | 3GPP 29.061 - 16.4.7.2-13 | 文字列 |
| 3GPP-SGSN-MCC-MNC | 3GPP 29.061 - 16.4.7.2-18 | 文字列 |
| 3GPP-IMEISV | 3GPP 29.061 - 16.4.7.2-20 | 文字列 |
| 3GPP-RAT-TYPE | 3GPP 29.061 - 16.4.7.2-21 | オクテット - 1 バイト |
| 3GPP-USER-LOCATION | 3GPP 29.061 - 16.4.7.2-22<br>3GPP 29.274 - 8.21-4、8.21-5<br>3GPP 38.413 – 9.3.1.7、9.3.3.10 | 特別エンコード オクテット |
| 3GPP-MS-TIMEZONE | 3GPP 29.061 - 16.4.7.2-23<br>3GPP 29.274 - 8.44 | 特別エンコード オクテット |
| 3GP-NEGOTIATED-DSCP | 3GPP 29.061 - 16.4.7.2-26 | オクテット - 1 バイト |
| CHAP-PASSWORD（CHAP） | RFC2865 – 5.3 | 文字列 |
| CHAP-CHALLENGE（CHAP） | RFC2865 – 5.40 | 文字列 |
| MSCHAP-CHALLENGE（MSCHAP） | RFC2548 - 2.1.2 | 文字列 |
| MSCHAP-RESPONSE | RFC2548 - 2.1.3 | オクテット |
| MSCHAP2-RESPONSE | RFC2548 - 2.3.2 | オクテット |
| MSCHAP-ERROR | RFC2548 - 2.1.5 | 文字列 |

| 属性 | 参考仕様 | エンコード タイプ |
|---|---|---|
| REPLY-MESSAGE | RFC2865 – 5.18 | 文字列 |

（注） Wi-Fi 通話の属性は、4G 通話と同じです。

### RADIUS アクセス応答属性

次のテーブルは、RADIUS アクセス応答メッセージでサポートされている属性をリストします。

| 属性 | 参考仕様 | エンコード タイプ |
|---|---|---|
| クラス | RFC 2865 | 文字列 |
| FRAMED-IP | RFC2865 - 5.1 | IPv4 アドレス（IPv4 Address） |
| FRAMED-IPv6-PREFIX | RFC3162 | PrefixLen および String |
| Framed-IP-Netmask | RFC 2865 | オクテット |
| IDLE-TIMEOUT | RFC2865 - 5.28 | 整数（Integer） |
| 3GPP-POLICY-REFERENCE | 3GP TS 29.061 | オクテット |
| MS プライマリ DNS サーバー | RFC 2548 | オクテット |
| MS-Secondary-DNS-Server | RFC 2548 | オクテット |
| SN-VIRTUAL-APN-NAME | Starent ディクショナリ | 不透明 |
| SESSION-TIMEOUT | RFC2865 - 5.27 | 整数（Integer） |
| cts :security-group-tag | Cisco ディクショナリ | 不透明 |

（注） Wi-Fi 通話の属性は、4G 通話と同じです。

RADIUS認証属性の詳細については、このガイドのRADIUS 属性定義 （1431 ページ） の項を参照してください。

# コール フロー

## RADIUS 認証 コール フロー

次の図は、SMF サーバと RADIUS エンドポイント間のエンドツーエンドのコール フローを示しています。

***Figure 240: RADIUS* 認証 コール フロー**

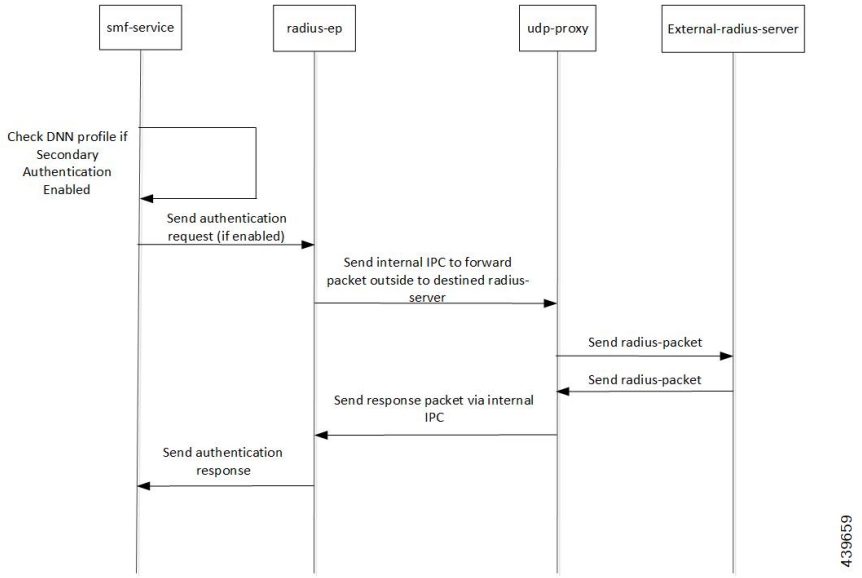



***Table 422: RADIUS* 認証コール フローの説明**

| ステップ | 説明 |
|---|---|
| 1 | RADIUS ポッドの起動：プロトコル EP VIP-IP と同様の VIP-IP で、それぞれのエンドポイント構成を追加します。RADIUS サーバ情報を RADIUS プロファイル構成に追加します。 |
| 2 | 必要な DNN プロファイルにセカンダリ認証構成を追加します。 |
| 3 | セッションの起動中、DNN プロファイルは、UDM 検証が成功した後、セカンダリ認証が有効になっているかどうかを確認します。<br>• 認証が有効になっていない場合は、PCF で続行します。<br>• 認証が有効になっている場合は、プロセス間通信（IPC）メッセージを RADIUS ポッドに送信して、サブスクライバを認証します。 |
| 4 | RADIUS ポッドは、構成された RADIUS サーバ宛てのアクセス要求パケットを準備し、そのパケットを UDP プロキシ ポッドに送信してパケットをプロキシします。 |

| ステップ | 説明 |
|---|---|
| 6 | UPDプロキシポッドはソケットを作成し（まだ存在しない場合）、パケットをRADIUSサーバに送信します。 |
| 7 | RADIUSサーバはアクセス要求を検証します。受け入れられると、アクセス承認メッセージで応答されます。それ以外の場合は、アクセス拒否メッセージで応答します。 |
| 8 | UDP プロキシは、それぞれの RADIUS-EP インスタンスに応答します。 |
| 9 | RADIUS-EP インスタンスは応答を検証し、Framed-IP（存在する場合）を取得して、SMF サービスを更新します。 |
| 10 | SMF サービスは、RADIUS-EP からの正常な応答時に PCF フローを続行します。そうでない場合、SMF サービスはサブスクライバから切断されます。 |

# アカウンティングのための RADIUS 相互作用

SMF は、RADIUS クライアント RADIUS-EP を介して RADIUS サーバと次のメッセージを交換します。

- Accounting-Request：このメッセージは、次のいずれかのパケットを伝送して、RADIUS サーバにアカウンティング情報をリレーします。
  - **アカウンティング開始パケット**：このパケットは、配信されるサービスのタイプと配信先であるユーザーが記述されています。

    SMF は、セッション確立手順中にアカウンティング開始パケットを送信します。RADIUS アカウンティング サーバは、accounting-start パケットを受信すると、確認応答を返します。

    RADIUS アカウンティングの構成の詳細については、RADIUS クライアントの構成（1441 ページ） の項を参照してください。
  - **アカウンティング終了パケット**：このパケットは、配信されたサービスのタイプと、必要に応じて経過時間、入力および出力オクテット、または入出力パケットなどの統計情報を記述します。

    サービス提供の最後に、SMFは、すべてのセッション削除シナリオについて、およびコール設定中にRADIUSアカウンティングが有効になった場合に、アカウンティング停止パケットを送信します。
  - **Accounting-Request Interim-Update**： セッション中、SMF は更新された累積使用率レポートを RADIUS アカウンティング サーバに送信します。
- Accounting-Response：正常に処理されたアカウンティング要求ごとに、RADIUS サーバは情報の受信を確認するアカウンティング確認応答を返します。

アカウンティングに関連付けられているCLIの詳細については、「RADIUS クライアントの構成 （1441 ページ）」セクションを参照してください。

## RADIUS アカウンティング属性

次の表に、アカウンティング要求メッセージでサポートされるRADIUSアカウンティング属性を示します。

| [Attribute] | 参考仕様 | エンコード タイプ（Encoding Type） | サポートされるアカウンティング タイプ |
|---|---|---|---|
| USER-NAME | RFC 2865 - 5.1 | 文字列 | 開始、停止、暫定アップデート |
| CALLING-STATION-ID | RFC 2865 - 5.31 | 文字列 | 開始、停止、暫定アップデート |
| CALLED-STATION-ID | RFC 2865 - 5.30 | 文字列 | 開始、停止、暫定アップデート |
| クラス | RFC 2865 - 5.25 | 文字列 | 開始、停止、暫定アップデート |
| NAS-IP-ADDRESS | RFC 2865 - 5.4 | IPv4 アドレス | 開始、停止、暫定アップデート |
| NAS-IDENTIFIER | RFC 2865 - 5.32 | 文字列 | 開始、停止、暫定アップデート |
| SERVICE-TYPE | RFC 2865 - 5.6 | オクテット - 4 バイト | 開始、停止、暫定アップデート |
| FRAMED-PROTOCOL | RFC 2865 - 5.7 | オクテット - 4 バイト | 開始、停止、暫定アップデート |
| FRAMED-IP | RFC2865 - 5.1 | IPv4 アドレス（IPv4 Address） | 開始、停止、暫定アップデート |
| FRAMED-IPv6-PREFIX | RFC3162 | PrefixLen および String | 開始、停止、暫定アップデート |
| Framed-IP-Netmask | RFC 2865 - 5.9 | オクテット - 4 バイト | 開始、停止、暫定アップデート |
| NAS-PORT-TYPE | RFC 2865 - 5.41 | オクテット - 4 バイト | 開始、停止、暫定アップデート |
| NAS-PORT | RFC 2865 - 5.5 | オクテット - 4 バイト | 開始、停止、暫定アップデート |

| [Attribute] | 参考仕様 | エンコード タイプ（Encoding Type） | サポートされるアカウンティング タイプ |
|---|---|---|---|
| 3GPP-IMSI | 3GPP 29.061 - 16.4.7.2-1 | 文字列 | 開始、停止、暫定アップデート |
| 3GPP-CHARGING-ID | 3GPP 29.061 - 16.4.7.2-2 | オクテット - 4 バイト | 開始、停止、暫定アップデート |
| 3GPP-PDP-TYPE | 3GPP 29.061 - 16.4.7.2-3 | オクテット - 4 バイト | 開始、停止、暫定アップデート |
| 3GPP-CHARGING-GATEWAY-ADDR | 3GPP 29.061 - 16.4.7.2-4 | IPv4 アドレス | 開始、停止、暫定アップデート |
| 3GPP-GPRS-NEG-QOS-PROFILE | 3GPP 29.061 - 16.4.7.2-5<br>3GPP 29.274 - 8.7 | 特別エンコード オクテット | 開始、停止、暫定アップデート |
| 3GPP-SGSN-ADDRESS | 3GPP 29.061 - 16.4.7.2-6 | IPv4 アドレス | 開始、停止、暫定アップデート<br>この属性は、5Gアカウンティング開始メッセージには含まれません。 |
| 3GPP-GGSN-ADDRESS | 3GPP 29.061 - 16.4.7.2-7 | IPv4 アドレス | 開始、停止、暫定アップデート |
| 3GPP-IMSI-MCC-MNC | 3GPP 29.061 - 16.4.7.2-8 | 文字列 | 開始、停止、暫定アップデート |
| 3GPP-GGSN-MCC-MNC | 3GPP 29.061 - 16.4.7.2-9 | 文字列 | 開始、停止、暫定アップデート |
| 3GPP-NSAPI | 3GPP 29.061 - 16.4.7.2-10 | 文字列 | 開始、停止、暫定アップデート |
| 3GPP-SELECTION-MODE | 3GPP 29.061 - 16.4.7.2-12 | 文字列 | 開始、停止、暫定アップデート |
| 3GPP-CHARGING-CHARACTERISTICS | 3GPP 29.061 - 16.4.7.2-13 | 文字列 | 開始、停止、暫定アップデート |
| 3GPP-SGSN - MCC - MNC | 3GPP 29.061 - 16.4.7.2-18 | 文字列 | 開始、停止、暫定アップデート |

| [Attribute] | 参考仕様 | エンコード タイプ（Encoding Type） | サポートされるアカウンティング タイプ |
|---|---|---|---|
| 3GPP-IMEISV | 3GPP 29.061 - 16.4.7.2-20 | 文字列 | 開始、停止、暫定アップデート |
| 3GPP-RAT-TYPE | 3GPP 29.061 - 16.4.7.2-21 | オクテット - 1 バイト | 開始、停止、暫定アップデート |
| 3GP-USER<br>-LOCATION | 3GPP 29.061 - 16.4.7.2-22<br>3GPP 29.274 - 8.21-4<br>3GPP 29.274 - 8.21-5 | 特別エンコード オクテット | 開始、停止、暫定アップデート |
| 3GPP-MS-TIMEZONE | 3GPP 29.061 - 16.4.7.2-23<br>3GPP 29.274 - 8.44 | 特別エンコード オクテット | 開始、停止、暫定アップデート |
| 3GP-NEGOTIATED<br>-DSCP | 3GPP 29.061 – 16.4.7.2-26 | オクテット：1 バイト | 開始、停止、暫定アップデート<br>この属性は、関連する構成が存在する場合にのみ送信されます。 |
| Acct-Status-Type | RFC 2866 | 開始/停止/暫定 | 開始、停止、暫定アップデート |
| Accounting-Session-Id | RFC 2866 | 文字列 | 開始、停止、暫定アップデート |
| Acct-Delay-time | RFC 2866 | オクテット | 開始、停止、暫定アップデート |
| Acct-Input-Octets | RFC 2866 | 整数（Integer） | 開始、停止、暫定アップデート |
| Acct-Output-Octets | RFC 2866 | 整数（Integer） | 開始、停止、暫定アップデート |
| Acct-Input-Gigawords | RFC 2869 | 整数（Integer） | 開始、停止、暫定アップデート |
| Acct-Output-Gigawords | RFC 2869 | 整数（Integer） | 開始、停止、暫定アップデート |
| Acct-Input-packets | RFC 2866 | 整数（Integer） | 開始、停止、暫定アップデート |

| [Attribute] | 参考仕様 | エンコード タイプ（Encoding Type） | サポートされるアカウンティング タイプ |
|---|---|---|---|
| Acct-Output-Packets | RFC 2866 | 整数（Integer） | 開始、停止、暫定アップデート |
| Acct-Session-Time | RFC 2866 | 整数（Integer） | 開始、停止、暫定アップデート |
| Acct-Terminate-Cause | RFC 2866 | 文字列 | 停止 |
| Framed-MTU | RFC 2866 | 文字列 | 開始、停止、暫定アップデート |
| 3GPP-Session -Stop-Indicator | 3GPP 29.061 | ビット文字列 | 停止 |
| Framed-Ip-Addr | RFC 2866 | IPv4 アドレス | 開始、停止、暫定アップデート |
| Acct-Authentic | RFC 2866 | 文字列 | 開始、停止、暫定アップデート |
| EventTimeStamp | RFC 2869 | 文字列 | 開始、停止、暫定アップデート |

（注） WiFi 通話の属性は、4G 通話と同じです。

RADIUSアカウンティング属性の詳細については、このガイドのRADIUS属性定義 （1431ページ） の項を参照してください。

## コール フロー

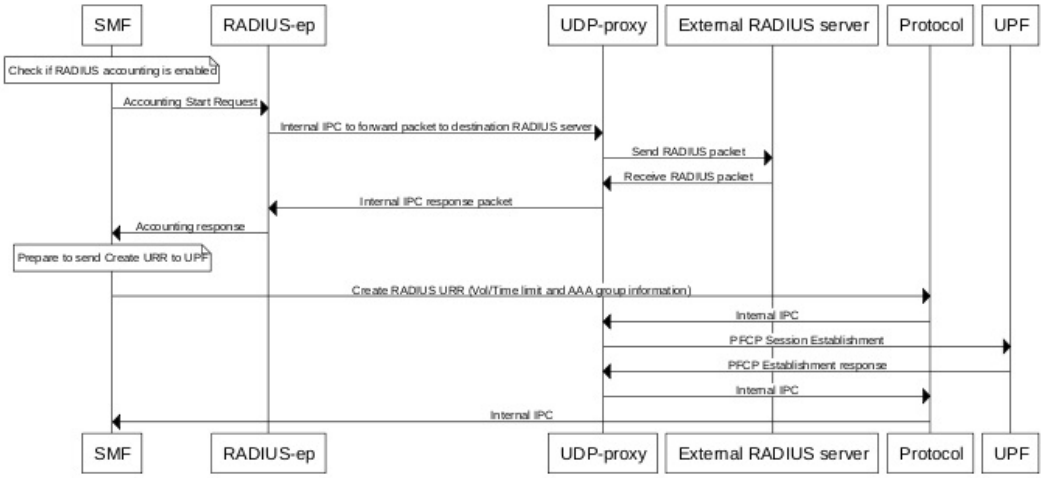
このセクションでは、次のコールフローについて説明します。

- RADIUS アカウンティング開始コール フロー
- RADIUS アカウンティング終了コール フロー
- RADIUS アカウンティングの暫定更新非同期コール フロー
- 同期アカウンティング暫定更新コール フロー （1429 ページ）

### RADIUS アカウンティング開始コール フロー

ここでは、RADIUS アカウンティング手順の開始に関連するコール フローについて説明します。

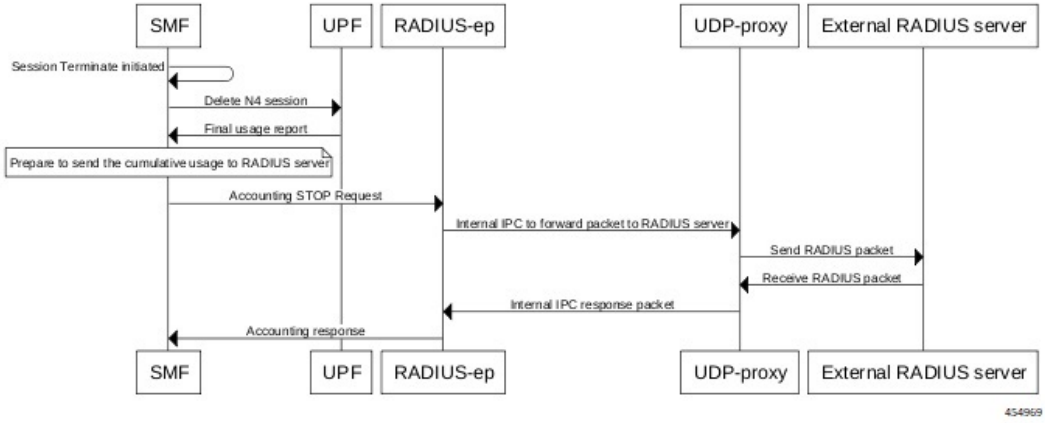
図 *241 : RADIUS* アカウンティング開始コール フロー




## RADIUS アカウンティング終了コール フロー

ここでは、RADIUS アカウンティング手順の終了に関連するコール フローについて説明します。

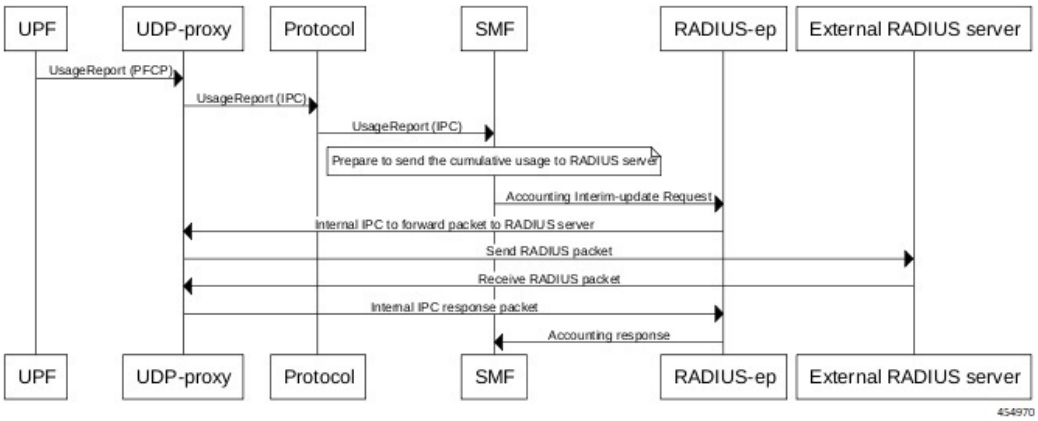
図 *242 : RADIUS* アカウンティング終了コール フロー




## 非同期アカウンティングの暫定更新コール フロー

ここでは、非同期の中間更新要求に関連付けられたコール フローについて説明します。

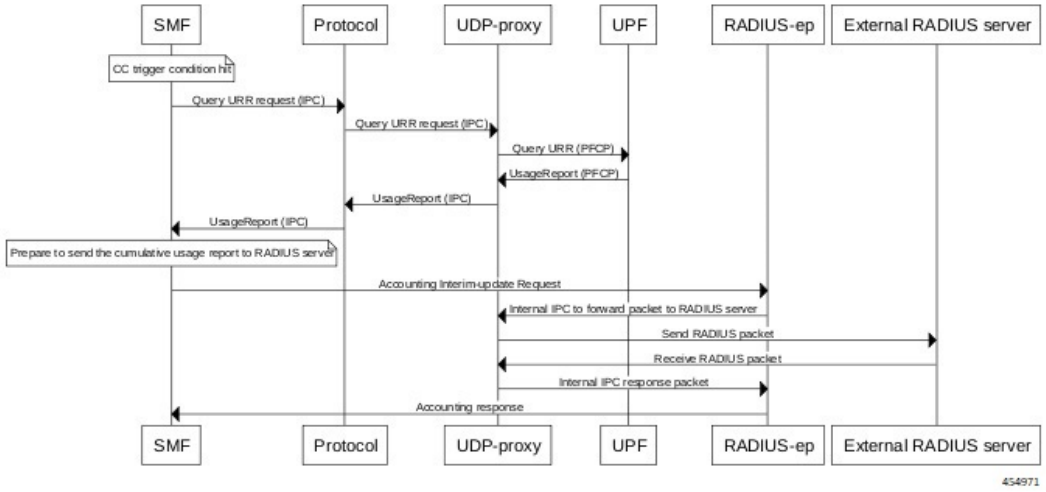
図 *243 :* 非同期アカウンティングの暫定更新コール フロー




## 同期アカウンティング暫定更新コール フロー

ここでは、同期中間アップデート要求に関連付けられたコール フローについて説明します。

図 *244 :* 同期アカウンティング暫定更新コール フロー




# ご利用明細レポートルールの処理

RADIUS アカウンティングを有効にすると、SMF は使用状況レポートルール（URR）を作成し、Create URR 情報要素（IE）を介して UPF にルールをリレーします。Create URR IE は N4 セッション確立要求内に存在し、構成に従ってボリュームと時間制限が含まれます。

SMF では、RADIUS URR が動的なパケット検出ルール（PDR）にのみ関連付けられ、静的ルールや定義済みのルールには関連付けられません。N4 セッション確立要求の AAA グループ名により、UPF は静的で事前定義された PDR を RADIUS URR に関連付けます。ボリューム制限または時間制限に達すると、UPF は RADIUS URR の使用状況レポートを送信します。次に、SMF は、中間アカウンティング要求メッセージの使用状況を RADIUS サーバーに送信します。

SMFは、次の条件のいずれかが満たされた場合に、N4変更応答またはN4削除応答でRADIUS URR の使用状況レポートを受信します：

- CC イベント条件がヒットし、SMF がクエリ URR を実行します
- セッション削除応答は、送信されました

SMFは、前のセッションで報告されたボリュームと時間のしきい値の値を保存し、保存されている値に現在報告された値を加算することによって累積使用量をレポートします。SMF は、Accounting-Request Interim-Update およびAccounting-Stop メッセージで累積使用状況レポートを送信します。

UPF から使用状況レポートを受信すると、SMF は CHF サーバーと RADIUS サーバーに送信する URR ID を識別します。たとえば、URR ID が「0x80 00 00 09」に関連付けられている場合、SMF はこの URR ID を RADIUS サーバーに送信し、他の URR ID を CHF サーバーに送信します。

## 構成の動的な更新

SMFを使用すると、既存のセッションに影響を与えずに、RADIUSアカウンティング構成を動的に変更できます。

次の表に、さまざまな RADIUS アカウンティング構成に対するダイナミック アップデートの影響を示します。

**表 *423 : RADIUS* アカウンティング構成の動的な更新**

| 設定（Configuration） | ダイナミックな変更 | 既存のセッションへの影響 |
|---|---|---|
| RADIUS アカウンティング構成の有効化と無効化 | システム レベルで許可 | 既存のセッションは古い値を引き続き使用します。 |
| CC トリガー更新 | 現在のポッド レプリカごとに許可 | 既存のセッションは新しい値を使用します。 |
| ボリュームと時間制限の変更 | システム レベルで許可 | 既存のセッションは古い値を引き続き使用します。 |
| グローバル レベルとグループ レベルの構成<br>（注）<br>グループレベルの構成を使用できない場合、デフォルトでは、グローバルレベルの構成が考慮されます。 | システム レベルで許可 | 既存の要求は、引き続き古い値を使用します。新しい要求には、新しく構成された値が使用されます。 |

# RADIUS 属性定義

次のセクションでは、各属性について詳しく説明します。属性値の大部分は、ISE ディクショナリと 3GPP ディクショナリに共通です。この値は、特に、ISE および 3GPP ディクショナリの異なる属性値を持つ属性の属性説明セクションに含まれています：

- USER-NAME

  **説明**：RFC 2865 に従ってエンコードされる文字列値。

  - 5G 通話：「msidn-」を削除した GPSI 値が使用される
  - 4G コール：電話番号の値が使用され、「msidn-」が削除されます。
  - 3GPP ディクショナリの属性値は imsi@apn です。

**Note** 2020.02.x より前のリリースでは、PAP、CHAP、および MSCHAP の認証方法はサポートされていません。

リリース 2020.02.x 以降では、PAP、CHAP、および MSCHAP 認証方式がサポートされています。

- PASSWORD

  **説明**：RFC 2865 に従ってエンコードされた暗号化された文字列値。

  5G コールと 4G コールの両方で、選択した RADIUS サーバーの「シークレット」がユーザー パスワードとして設定されます。

- CALLING-STATION-ID

  **説明**：RFC 2865 に従ってエンコードされる文字列値。

  5G 通話：「msidn-」を削除した GPSI 値が使用されます

  4G コール：「msidn-」を削除した電話番号値が使用されます。

- CALLED-STATION-ID

  **説明**：RFC 2865 に従ってエンコードされる文字列値。

  5G コールと 4G コールの両方で、DNN 値は called-station-id に設定されます。

- NAS-IP-ADDRESS

  **説明**：RFC 2865 に従ってエンコードされた IPv4 アドレス値。

  5G コールと 4G コールの両方で、ユーザー構成の RADIUS クライアント インターフェイス タイプの VIP-IP が使用されます。

- NAS-IDENTIFIER

  **説明**：RFC 2865 に従ってエンコードされる文字列値。

  5G コールと 4G コールの両方で、ユーザー構成の nas-identifier 属性値が使用されます。

- SERVICE-TYPE

  **説明**：RFC 2865 に従ってエンコードされる 4 バイト オクテット（int）値。

  5G コールと 4G コールの両方で「FRAMED (2)」の値が設定されます。

- FRAMED-PROTOCOL

  **説明**：RFC 2865 に従ってエンコードされる 4 バイト オクテット（int）値。

  5G コールと 4G コールの両方で「GPRS-PDP-CONTEXT (7)」の値が設定されます。

- NAS-PORT-TYPE

  **説明**：RFC 2865 に従ってエンコードされる 4 バイト オクテット（int）値。

  5G コールと 4G コールの両方で「WIRELESS-OTHER（18）」の値が設定されます。

- NAS-PORT

  **説明**：RFC 2865 に従ってエンコードされる 4 バイト オクテット（int）値。

  5G コールと 4G コールの両方で、それぞれのインスタンスのベース値が使用されます。つまり、以下のようになります。

  0x4000... 0x407F は replica-0 に設定されます

  0x4080... 0x40FF が replica-1 に設定される

- 3GPP-IMSI

  **説明**： *3GPP TS 29.061*に従ってエンコードされた文字列値。

  5G コール：SUPI 値が使用されます。

  4G コール：IMSI 値が使用されます。

- 3GPP-CHARGING-ID

  **説明**： *3GPP TS 29.061*に従ってエンコードされた 4 バイトオクテット（int）値。

  5G コールと 4G コールの両方に、Charging-ID が設定されます。

- 3GPP-PDP-TYPE

  **説明**： *3GPP TS 29.061*に従ってエンコードされた 4 バイトオクテット（int）値。

  5G コールと 4G コールの両方の場合、pdp-type は次のように設定されます：

  - 0 = IPv4
  - 2 = IPv6
  - 3 = IPv4v6

- 3GPP-CHARGING-GATEWAY-ADDR

  **説明**： *3GPP TS 29.061*に従ってエンコードされた 4 バイト オクテット（IPv4 アドレス）値。

  5G コールと 4G コールの両方に対して、課金ゲートウェイアドレスが設定されます。

• 3GPP-GPRS-NEG-QOS-PROFILE

**説明**： *3GPP TS 29.061* および *29.274* に従ってエンコードされたオクテット（特殊エンコーディング）値。

5G コールの場合、システムの default-qos プロファイルの値が使用され、エンコードは次のように実行されます。

***Table 424: Non-GBR case***

| | |
|---|---|
| 1 ～ 2 | <Release indicator>- = "15" (UTF-8 encoded) |
| 3 | "-" (UTF-8 encoded) |
| 4 ～ 5 | ARP (UTF-8 encoded) |
| （6 ～ 7 ページ）を参照 | 5QI (UTF-8 encoded) |
| 8 ～ 9 | UL Session-AMBR length (UTF-8 encoded) |
| 10-m | UL Session-AMBR (UTF-8 encoded) |
| (m+1) - (m+2) | DL Session-AMBR length (UTF-8 encoded) |
| (m+3) – n | DL Session-AMBR (UTF-8 encoded) |

***Table 425: GBR case***

| | |
|---|---|
| 1 ～ 2 | <Release indicator> = "15" (UTF-8 encoded) |
| 3 | "-" (UTF-8 encoded) |
| 4 ～ 5 | ARP (UTF-8 encoded) |
| （6 ～ 7 ページ）を参照 | 5QI (UTF-8 encoded) |
| 8 ～ 9 | UL MFBR length (UTF-8 encoded) |
| 10-m | UL MFBR (UTF-8 encoded) |
| (m+1)-(m+2) | DL MFBR length (UTF-8 encoded) |
| (m+3)-n | DL MFBR (UTF-8 encoded) |
| (n+1)-(n+2) | UL GFBR length (UTF-8 encoded) |
| (n+3)-o | UL GFBR (UTF-8 encoded) |
| (o+1) – (o+2) | UL GFBR length (UTF-8 encoded) |
| (o+3) - p | DL GFBR (UTF-8 encoded) |

4G コールの場合、システムの default-qos プロファイルの値が使用され、エンコードは次のように実行されます：

***Table 426: Non-GBR case***

| | |
|---|---|
| 1 ～ 2 | <Release indicator>- = "08" (UTF-8 encoded) |
| 3 | "-" (UTF-8 encoded) |
| 4 ～ 5 | ARP (UTF-8 encoded) |
| （6 ～ 7 ページ）を参照 | 5QI (UTF-8 encoded) |
| 8-11 | UL Session-AMBR (UTF-8 encoded) |
| 12-15 | DL Session-AMBR (UTF-8 encoded) |

***Table 427: GBR case***

| | |
|---|---|
| 1 ～ 2 | <Release indicator> = "08" (UTF-8 encoded) |
| 3 | "-" (UTF-8 encoded) |
| 4 ～ 5 | ARP (UTF-8 encoded) |
| （6 ～ 7 ページ）を参照 | 5QI (UTF-8 encoded) |
| 8-11 | UL MBR (UTF-8 encoded) |
| 12-15 | DL MBR (UTF-8 encoded) |
| 16-19 | UL GBR (UTF-8 encoded) |
| 20-23 | DL GBR (UTF-8 encoded) |

- 3GPP-SGSN-ADDRESS

  **説明**： *3GPP TS 29.061*に従ってエンコードされた 4 バイト オクテット（IPv4 アドレス）値。

  5G通話の場合、AMF アドレスが設定されます。

  4G コールの場合、S-GW アドレスが設定されます。

- 3GPP-GGSN-ADDRESS

  **説明**： *3GPP TS 29.061*に従ってエンコードされた 4 バイト オクテット（IPv4 アドレス）値。

  5G と 4G の両方のコールに対して、SMF サービス IP が設定されます。

  3GPP ディクショナリの場合、CSRsp で送信された PGW 制御 IP アドレス。

- 3GPP-IMSI-MCC-MNC

  **説明**： *3GPP TS 29.061*に従ってエンコードされた文字列値。

  5G コールの場合、SUPI の MCC と MNC の値が設定されます。

  4G コールの場合、IMSI MCC と MNC の値が設定されます。

MCC は最初の 3 バイト、MNC は次の 2 バイトまたは 3 バイトです。

MCC 値が次のいずれかの場合、MNC は 3 バイトになります。それ以外の場合は MNC は 2 バイトになります。

300 302 310 311 312 313 316 334 338 342 344 346 348 354 356 358 360 365 376 405 708 722 732

- 3GP-GGSN-MCC-MNC

  **説明**： *3GPP TS 29.061*に従ってエンコードされた文字列値。

  5G コールと 4G コールの両方で、SMF の構成された MCC および MNC 値が使用されます。

  MCC は最初の 3 バイトで、MNC は次の 2 バイトまたは 3 バイトです。

- 3GPP-SGSN-MCC-MNC

  **説明**： *3GPP TS 29.061*に従ってエンコードされた文字列値。

  5G コールの場合、AMF の MCC と MNC の値が設定されます。

  4G コールの場合、SGW の MCC と MNC の値が設定されます。

  MCC は最初の 3 バイトで、MNC は次の 2 バイトまたは 3 バイトです。

- 3GPP-NSAPI

  **説明**： *3GPP TS 29.061*に従ってエンコードされた文字列値。

  5G コールの場合、defaultQos プロファイルの QFI 値が設定されます。

  4G コールの場合、EPS ベアラー ID が設定されます。

- 3GPP-SELECTION-MODE

  **説明**： *3GPP TS 29.061*に従ってエンコードされた文字列値。

  4G コールと 5G コールの両方で、値は「0」に設定されます。

  3GPP ディクショナリの場合、選択モード値は CSReq で受信されます。

- 3GPP-CHARGING-CHARACTERISTICS

  **説明**： *3GPP TS 29.061*に従ってエンコードされた文字列値。

  4G コールと 5G コールの両方で、一般的な課金の文字が設定されます。

- 3GPP-IMEISV

  **説明**： *3GPP TS 29.061*に従ってエンコードされた文字列値。

  5G コールの場合、PEI 値は設定されます。

  4G コールの場合、IMEI 値が設定されます。

- 3GPP-RAT-TYPE

  **説明**： *3GPP TS 29.061*に従ってエンコードされた 1 バイトのオクテット。

  5G コールの場合、値「NR（51）」が設定されます。

4G コールの場合、値「EUTRAN (6)」が設定されます。

WLAN コールの場合、値「WLAN(3)」が設定されます。

- 3GPP-USER-LOCATION

**説明**：*3GPP TS 29.061*に従ってエンコードされた特別なオクテット値。

5G コールの場合、次のエンコーディング ロジックが使用されます。

| | |
|---|---|
| 1 | Location-Type<br>Only TAI = 136<br>Only NCGI = 135<br>Both TAI + NCGI =137 |
| 2-7 | TAI エンコーディング（存在する場合） |
| 8 ～ 15 | NCGI エンコーディング（存在する場合） |

TAI エンコーディング ヘッダー:

| | | |
|---|---|---|
| 1 | MCC 桁 2 | MCC 桁 1 |
| 2 | MNC 桁 3 | MCC 桁 3 |
| 3 | MNC 桁 2 | MNC 桁 1 |
| 4-6 | TAC 値 | |

NCGI エンコーディング ヘッダー：

| | | |
|---|---|---|
| 1 | MCC 桁 2 | MCC 桁 1 |
| 2 | MNC 桁 3 | MCC 桁 3 |
| 3 | MNC 桁 2 | MNC 桁 1 |
| 4 | SPARE | NCI |
| 5 ～ 8 | NR セル識別子（NCI） | |

4G コールの場合、次のエンコーディング ロジックが使用されます。

| | |
|---|---|
| 1 | Location-Type |
| | Only TAI = 128 |
| | Only ECGI = 129 |
| | Both TAI + ECGI =130 |
| 2 ～ 6 | TAI エンコーディング（存在する場合） |
| 7-13 | ECGI 7-13（存在する場合） |

TAI エンコーディング ヘッダー:

| | | |
|---|---|---|
| 1 | MCC 桁 2 | MCC 桁 1 |
| 2 | MNC 桁 3 | MCC 桁 3 |
| 3 | MNC 桁 2 | MNC 桁 1 |
| 4 ～ 5 | TAC 値 | |

ECGI エンコーディング ヘッダー：

| | | |
|---|---|---|
| 1 | MCC 桁 2 | MCC 桁 1 |
| 2 | MNC 桁 3 | MCC 桁 3 |
| 3 | MNC 桁 2 | MNC 桁 1 |
| 4 | 予備 | ECI |
| 5-7 | EUTRAN セル識別子（ECI） | |

- 3GPP-MS-TIMEZONE

  **説明**： *3GPP TS 29.061*に従ってエンコードされた特別なオクテット値。

  タイムゾーン文字列（例：-07:00+1）は、次の表に示すように、2バイト値としてエンコードされます。

| | |
|---|---|
| 1 | タイムゾーン<br>最初のバイトのタイムゾーンは、3GPP 29.061、3GPP 29.274、3GPP 24.008、および 3GPP 23.040（セクション 9.2.3.11）に従ってエンコードされます。 |
| 2 | 夏時間 0、または、+1 あるいは、+2<br>第2バイトのデイライトは、使用される2ビット（00-0、01-+1、10-+2、11：未使用）で構成されます。 |

- 3GP-NEGOTIATED-DSCP

  **説明**： *3GPP TS 29.061*に従ってエンコードされた 1 バイトのオクテット。

  5G コールと 4G コールの両方で、DNN qos-profile 構成の DSCP 構成が使用されます。

  サブ -> DNNプロファイル -> QosProfile -> DSCPMap -> Qi5 値チェック -> ARP 優先順位チェック

- Acct-Status-Type

  **説明**：RFC 2866 に従ってエンコードされる列挙値。この属性の値は次のいずれかになります。

  - 1 - 開始

- 2 - 停止
- 3 - 暫定アップデート

- Acct-Delay-Time

  **説明**：RFC 2866 に従ってエンコードされる整数値。この属性は、クライアントがアカウンティング レコードを送信しようとしている時間を表します。

- Acct-Input-Octets

  **説明**：RFC 2866 に従ってエンコードされる整数値。この属性は、受信したバイト数を表します。この属性には 4 バイトが含まれています。

  SMF では、数値が最大値を超えると、値がラップされます。

- Acct-Output-Octets

  **説明**：RFC 2866 に従ってエンコードされる整数値。この属性は、送信されたバイト数を表します。この属性には 4 バイトが含まれています。

  SMF では、数値が最大値を超えると、値がラップされます。

- Acct-Input-Packets

  **説明**：RFC 2866 に従ってエンコードされる整数値。この属性は、受信されたパケットの量を表します。この属性には 4 バイトが含まれています。

  SMF では、数値が最大値を超えると、値がラップされます。

- Acct-Output-Packets

  **説明**：RFC 2866 に従ってエンコードされる整数値。この属性は、送信されたパケットの量を表します。この属性には 4 バイトが含まれています。

  SMF では、数値が最大値を超えると、値がラップされます。

- Acct-Input-Gigawords

  **説明**：RFC 2869 に従ってエンコードされる整数値。この属性は、このサービスの提供中に Acct-Input-Octets カウンタが一周（2 の 32 乗）した回数を示します。この値は、Acct-Input-Octets がラップされるたびに増分されます。

- Acct-Output-Gigawords

  **説明**：RFC 2869 に従ってエンコードされる整数値。この属性は、このサービスの提供中に Acct-Output-Octets カウンタが一周（2 の 32 乗）した回数を示します。この値は、Acct-Output-Octets がラップされるたびに増加します。

- Acct-Session-Id

  **説明**：RFC 2866 に従ってエンコードされる文字列値。この属性は、サブスクライバの一意のアカウンティング ID を表します。アカウンティング ID は、一意であり、ログ ファイル内の開始レコードと停止レコードを簡単に対応付けることができるようにします。あるセッションの開始レコードと停止レコードには同じ same Acct-Session-Id があるはずです。Accounting-Request パケットには、Acct-Session-Id が必要です。

Access-Request パケットには Acct-Session-Id が含むことができますが、含まれている場合、NAS はこのセッションの Accounting-Request パケットで同じ Acct-Session-Id を使用しなければなりません。Acct-Session-Id には UTF-8 エンコードされた 10646 文字が含まれます。

- Acct-Session-Time

  **説明**：RFC 2866 に従ってエンコードされる整数値。この属性は、サブスクライバがアクティブである合計時間を表します。

- Framed-MTU

  **説明**：他の手段（PPP など）で交渉されていない場合、この属性は、ユーザーのために構成されるべき最大伝送ユニット（MTU）示します。デフォルト値は 1500 です

  It MAY be used in Access-Accept packets. これは、その値を優先する NAS がサーバーにヒントとしてアクセスリクエストパケットに使用される場合があります。しかしサーバーは、ヒントを受け入れる必要はありません。

- Acct-Terminate-Cause

  **説明**：RFC 2866 に従ってエンコードされる列挙値。この属性は、サブスクライバの終了理由を表します。

- FRAMED-IP

  RFC 2865 に従ってデコードされた IPv4 アドレス値。

  4G コールと 5G コールの両方で、受信した値はサブスクライバの IPv4 アドレスとして設定されます。

- FRAMED-IPv6-PREFIX

  RFC 3162 に従ってデコードされた IPv6 プレフィックス + 長さの値。

  4G コールと 5G コールの両方で、受信した値はサブスクライバの IPv6 プレフィックスとして設定されます。

**Important** 受信した prefix-length が !=64 の場合、SMF は 64 にオーバーライドします。

- IDLE-TIMEOUT

  RFC 2865 に従ってエンコードされる 4 バイト オクテット（整数）値。この属性は、着信 RADIUS パケットでサポートされています。

  4G コールと 5G コールの両方で、受信された値が、NAS によって切断される前にユーザに許可されるアイドル時間の最大連続秒数として使用されます。

- SESSION-TIMEOUT

  RFC 2865 に従ってエンコードされる 4 バイト オクテット（整数）値。この属性は、着信 RADIUS パケットでサポートされています。

4G コールと 5G コールの両方で、受信済みの値が、NAS がユーザの接続を維持できる最大秒数として使用されます。

- 3GPP ネゴシエート QoS プロファイル
  - Access-request

    ISE またはデフォルトのディクショナリの場合：ARP PCI と ARP PVI が誤って送信され、CSReq で受信した値と一致しませんでした。また、APN AMBR が Kbps ではなく bps で送信されました。

    3GPP ディクショナリの場合：ARP PCI および ARP PVI 値は固定され、CSReq で受信したものと同期します。また、APN AMBR は Kbps で送信されます。

  - アカウンティング要求

    ISE またはデフォルトのディクショナリの場合：ARP PCI および ARP PVI が誤って送信され、CSReq/Gx CCA-I で受信した値と一致しませんでした。また、APN AMBR が Kbps ではなく bps で送信されました。

  - 3GPP ディクショナリの場合：ARP PCI および ARP PVI 値は固定され、CSReq/Gx-CCA-I で受信されるものと同期します。また、APN AMBR は Kbps で送信されます。

- 3GPP-IMEI-SV
  - Access-request

    ISEまたはデフォルトディクショナリの場合: 16 ビットIMEIの場合：imisv-1122334455667788、15 ビットIMEIの場合：112233445566778。

    3GPP ディクショナリの場合：16 ビット IMEI では 1122334455667788、15 ビット IMEI では 112233445566778。

  - アカウンティング要求

    ISEまたはデフォルトディクショナリの場合：16ビットIMEIの場合: 1122334455667788、15ビットIMEIの場合：112233445566778。

  - 3GPP ディクショナリの場合：16 ビット IMEI では 1122334455667788、15 ビット IMEI では 112233445566778。

- 3GPP-UE-Location
  - Access-request

    ISE またはデフォルト ディクショナリの場合：ECI 値は 0 になります。

    3GPP ディクショナリの場合：値は CSReq で受信されます。

  - アカウンティング要求

    ISEまたはデフォルトディクショナリの場合：16ビットIMEIの場合: 1122334455667788、15ビットIMEIの場合：112233445566778。

  - 3GPP ディクショナリの場合：16 ビット IMEI では 1122334455667788、15 ビット IMEI では 112233445566778。

**Note** WiFi 通話の属性は、4G 通話と同じです。

## 標準準拠

RADIUS クライアント機能は、以下の基準に準拠しています：

- RFC 2865：RADIUS
- RFC 2866：RADIUS アカウンティング
- RFC 3162：RADIUS および IPv6
- 3GP TS 29.061
- 3GPP TS 29.274
- 3GPP TS 29.561、バージョン 16.4.0

## 制限事項と制約事項

SMF には次の制限があります。

- SMF は、1 つの RADIUS 属性プロファイルのみをサポートし、ディクショナリの選択をサポートしません。
- RADIUS アカウンティングが有効で、DNN プロファイル内でサーバー グループが構成されている場合、SMF は N4 セッション確立の課金パラメータでサーバー グループを AAA グループとして送信します。SMF と UPF の間にサーバー グループの不一致があると、UPF はエラーを表示します。

  このシナリオでは、静的および事前定義された使用法は RADIUS URR に考慮されません。ただし、ダイナミック ルール トラフィックは RADIUS URR で考慮されます。

# RADIUS クライアントの構成

RADIUS クライアントは、RADIUS 認証機能とアカウンティング機能の両方を提供します。これらの機能を使用するには、関連付けられた CLI 構成を介して RADIUS 認証およびアカウンティング フレームワークを有効にすることが重要です。

ここでは、RADIUS クライアントの構成方法について説明します。

**Important** RADIUS クライアントが動作するには、RADIUS クライアント インターフェイスの VIP-IP の構成が必須です。また、VIP-IP は UDP プロキシ ポッドの IP と同じである必要があります。

RADIUS クライアントの構成には、次の作業が含まれます：


- RADIUS サーバーの構成, on page 1442
- RADIUS サーバー選択ロジックの構成, on page 1444
- RADIUS 属性の構成, on page 1444
- RADIUS 検出デッド サーバの構成, on page 1447
- RADIUS デッド タイムの構成, on page 1448
- RADIUS DTLS 接続再試行回数の設定, on page 1449
- RADIUS タイムアウトの構成, on page 1450
- RADIUS POD の構成, on page 1451
- セカンダリ認証メソッドの構成, on page 1454
- PAP、CHAP、または MSCHAP ベースの認証の構成, on page 1455
- RADIUS アカウンティングの有効化, on page 1456
- DNN プロファイルでの RADIUS サーバー グループの定義, on page 1457
- RADIUS アカウンティング オプションの構成, on page 1457
- RADIUS アカウンティング サーバー グループの構成, on page 1459
- セッション切断機能の構成, on page 1459
- RADIUS 認証許可パラメータの有効化, on page 1445
- 連続的障害の構成, on page 1446
- 最大送信数の構成, on page 1449
- プロトコル エンド ポイントの内部仮想 IP の構成, on page 1446


# RADIUS サーバーの構成

RADIUS サーバーを構成するには、次の構成例を使用します。

```
config
  profile radius
     server ipv4_address port_num
        secret secret_key
        priority priority_value
        type { acct | auth }
        commit
```

注：

- **profile radius**：RADIUS 構成モードに入ります。

- **server** *ipv4_address port_num*: インターフェイスの IPv4 アドレスと RADIUS サーバーのポートを指定します。
- secret_key：<<Secret_Key>>**secret**
- **priority** *priority_value*：サーバー優先順位の値を指定します。
- **type { acct | auth }**：RADIUS サーバーのタイプを指定します。サーバーは次のいずれかになります。
  - **acct**：アカウンティング要求に使用される RADIUS サーバー
  - **auth**認証要求を使用する RADIUS サーバー
- **commit**：次の構成をコミットします。

**例**

次に、RADIUS サーバーの設定例を示します。

```
profile radius
 server 209.165.200.238 1812
  secret   $8$73a0i4G3ILj0Np+8tn2QOoWDj3QkB+oefPc2ZK6RE6A=
  priority 1
 exit
 server 209.165.200.240 1812
  secret   $8$VccEEUVou7m5ptA9WZRPR7KDmxQ/L3KlJ3QqgHjexkk=
  priority 2
 exit
exit
```

## RADIUS 設定の確認

**show radius** コマンドを使用して、システムに構成されている RADIUS サーバー（アカウンティングと認証の両方）に関する情報を表示します。

以下の構成は、 **show radius** コマンドの出力例です：

```
bng# show radius
radius
-------------------------------------------------------
 Server: 209.165.200.231, port: 1812, status: up, port-type: Auth
 2 requests, 0 pending, 0 retransmits
 1 accepts, 1 rejects, 0 timeouts
 0 bad responses, 0 bad authenticators
 0 unknown types, 0 dropped, 4 ms latest rtt
-------------------------------------------------------
-------------------------------------------------------
 Server: 209.165.200.231, port: 1813, status: up, port-type: Acct
 3 requests, 0 pending, 0 retransmits
 3 responses, 0 timeouts
 0 bad responses, 0 bad authenticators
 0 unknown types, 0 dropped, 1 ms latest rtt
-------------------------------------------------------
```

# RADIUS サーバー選択ロジックの構成

RADIUS サーバ選択ロジックを構成するには、次の構成例を使用します。

```
config
  profile radius
    algorithm { first-server | round-robin }
    commit
```

注：

- **profile radius**：RADIUS 構成モードに入ります。
- **algorithm { first-server | round-robin }**：RADIUS サーバを選択するためのアルゴリズムを定義します。
  - **first-server**：選択ロジックを最初に最も高い優先順位に設定します。これはデフォルトの動作です。
  - **round-robin**：選択ロジックをサーバのラウンドロビン順に設定します。
- **commit**：次の構成をコミットします。

例

RADIUS サーバ選択ロジックの構成例を次に示します。

```
config
   profile radius
      algorithm round-robin
      exit
```

# RADIUS 属性の構成

認証およびアカウンティングの RADIUS 属性を構成するには、次の構成例を使用します：

```
config
   profile radius
      attribute [ [ instance gr_instance_id ]  [ nas-identifier nas_id ] [
 nas-ip ipv4_address ] ]
      end
```

注：

- **profile radius**：RADIUS 構成モードに入ります。
- **attribute [ [ instance** *gr_instance_id* **] [ nas-identifier** *nas_id* **] [ nas-ip** *ipv4_address* **] ]**：RADIUS 識別パラメータを構成します。
  - **instance** *gr_instance_id*：地理的冗長性（GR）インスタンス ID を指定します。*gr_instance_id* は 整数である必要があります。
  - **nas-identifier** *nas_id*：アカウンティング要求メッセージでシステムを識別する属性名を指定します。 *nas_id* は 英数字の文字列である必要があります。

- **nas-ip** *ipv4_address*：NAS の IPv4 アドレスを指定します。 *ipv4_address* は 、ドット付き 10 進表記の IPv4 アドレスである必要があります。

- NAS-IP-Address および NAS-Identifier 属性は、RADIUS プロファイル構成で instance-id ごとに構成できます。この場合、インスタンス構成下の NAS-IP-Address および NAS-Identifier 属性は、非インスタンス ベースの属性構成よりも高い優先順位として扱われます。

**例**

次に、RADIUS 属性の構成例を示します。

```
config
   profile radius
      attribute
         instance 1
            nas-identifier CiscoSmf
         exit
      exit
   exit
exit
```

# RADIUS 認証許可パラメータの有効化

次の構成を使用して、RADIUS サーバーで allow-auth を有効にします。

```
config
  profile radius
     enable-allow-auth
     end
```

**注**：

- **profile radius**：RADIUS 構成モードに入ります。

- **enable-allow-auth** ： 構成で allow-auth が有効になっている場合、認証の成功、タイムアウト、またはエラーメッセージの受信に関係なく、進行中のコールを続行できます。デフォルト値は false ですが、allow-auth を有効にするには構成が必要です。

次の構成を使用して、RADIUS サーバー グループで allow-auth を有効にします。

```
config
  profile radius
     server-group group_name
        enable-allow-auth
        end
```

**注**：

- **profile radius**：RADIUS 構成モードに入ります。

- **server-group** *group_name*：allow-auth を有効にするサーバー グループを入力します。

- **enable-allow-auth** ： 構成で allow-auth が有効になっている場合、認証の成功、タイムアウト、またはエラーメッセージの受信に関係なく、進行中のコールを続行できます。デフォルト値は false です。allow-auth を有効にするには構成が必要です。

# 連続的障害の構成

RADIUS サーバで連続する障害を構成するには、次の構成を使用します。dead-server-detection のオプションがない場合でも、consecutive-failure はデフォルトで有効になっており、そのデフォルト値は 10 です。オフにするには、ユーザーは値を 0 に設定する必要があります。

```
config
  profile radius
    detect-dead-server consecutive-failures value
    end
```

注：

- **profile radius**：RADIUS 構成モードに入ります。
- **detect-dead-server consecutive-failures** *value*：サーバの障害数が連続障害のしきい値に達すると、当該サーバはデッド サーバとして宣言されます。

  *value*：1 ～ 1000 の範囲の整数である必要があります。デフォルトは 10 です。
- セットアップでは、要求の maxTransmissions 値よりも大きい値を連続エラー値に構成することを推奨します。

  例：maxRetry = 2 および maxTransmissions = 6 の場合、maxtransmissions が原因でサーバ スイッチに影響を与えないように、連続障害数が 6 より大きくなる場合があります。さらに、同じサーバに対して連続した要求が行われると、連続失敗と呼ばれるサーバ レベルの値が増加します。

# プロトコル エンド ポイントの内部仮想 IP の構成

プロトコルエンドポイントは、UDP-Proxy ポッドの構成です。UDP-Proxy ポッドは、RADIUS-EP ポッドから UDP メッセージを送信するための IPC 要求を受信します。UDP-Proxy ポッドは、メッセージを適切な UDP パケットに変換し、RADIUS サーバに送信します。RADIUS サーバが UDP パケットを SMF に送信している場合、UDP-Proxy ポッドは TCP 接続でパケットを受信して RADIUS-EP ポッドに転送します。

```
config
  instance instance-idgr_instance_id
    endpoint protocol
      replicasreplica_id
      nodesnode_id
      internal-vip{ SMF_UDP_PROXY_INTERNAL_VIP }
      vip-ip{ client_ipv4_address }
    exit
  exit
```

注：

- **instance instance-id***gr_instance_id*：GR インスタンス ID を指定します。
- **endpoint protocol**：GTP エンドポイント構成を入力します。
- **replicas***replica_id*：レプリカ サーバの ID を指定します。
- **nodes***node_id*：SMF ピア ノードのノード ID を指定します。値は文字列である必要があります。
- **internal-VIP**\n *SMF_UDP_PROXY_INTERNAL_VIP*：内部 SMF 通信用の UDP プロキシの IP アドレスを指定します。Radius-ep はこの IP アドレスを使用して、発信 AAA メッセージの UDP プロキシに到達します。
- **VIP-ip***client_ipv4_address )*：ダイナミック認証クライアントの IP アドレスを指定します。*ipv4_address* は 、標準の IPv4 ドット付き 10 進表記にする必要があります。

**例**

次に、設定例を示します。

```
config
   instance instance-id 1
      endpoint protocol
         replicas 1
         nodes 2
         internal-vip {SMF_UDP_PROXY_INTERNAL_VIP}
         vip-ip { client_ipv4_address}
      exit
   exit
```

# RADIUS 検出デッド サーバの構成

次の構成例を使用して、RADIUS 検出デッド サーバを構成します。

```
config
  profile radius
    detect-dead-server response-timeout value
    commit
```

注：

- **profile radius**：RADIUS 構成モードに入ります。
- **detect-dead-server response-timeout** *value*：パケットが指定された秒数の間受信されなかった場合にサーバーを「デッド」とマークするタイムアウト値を設定します。

  *value* は 1 ～ 65535 の範囲の整数である必要があります。デフォルト：10 秒
- **commit**：次の構成をコミットします。

例

次に、RADIUS 検出デッド サーバ構成の例を示します。

```
config
   profile radius
      detect-dead-server response-timeout 100
      exit
```

# RADIUS デッド タイムの構成

次の構成例を使用して、RADIUS デッドタイムを構成します。

```
config
  profile radius
     deadtime value
     commit
```

注：

- **profile radius**：RADIUS 構成モードに入ります。
- **deadtime** *value*：RADIUSサーバーが到達不能とマークされてから、再び接続を試みることができるよ うになるまでの経過時間を設定します。

  *value* は 1 ～ 65535 の範囲の整数である必要があります。デフォルト: 10分。
- **commit**：次の構成をコミットします。

例

次に、RADIUS デッド タイムの構成例を示します。

```
config
   profile radius
     deadtime 15
     exit
```

# RADIUS ディクショナリの構成

次の構成例を使用して、RADIUS ディクショナリを構成します。

```
config
  profile radius
     dictionary { ISE dictionary | 3GPP dictionary }
     commit
```

注：

- **profile radius**：RADIUS 構成モードに入ります。
- **dictionary { ISE dictionary | 3GPP dictionary }**：SMF サービスは RADIUS 構成をレンダリングし、選択された ISE または 3GPP 固有のパラメータを含む要求メッセージを入力します。

- **commit**：次の構成をコミットします。

**例**

RADIUS ディクショナリの構成例を次に示します。

```
config
   profile radius
      dictionary { ISE dictionary | 3GPP dictionary }
      exit
```

# RADIUS DTLS 接続再試行回数の設定

次の構成例を使用して、最大 RADIUS 再試行数を構成します。

```
config
   profile radius
      max-retry value
      commit
```

**注**：

- **profile radius**：RADIUS 構成モードに入ります。
- **max-retry** *value*：システムが RADIUS サーバとの接続を再試行する最大回数を設定します。

  *value*：0 ー 65535 の範囲の整数である必要があります。デフォルト：2

- **commit**：次の構成をコミットします。

**例**

次に、RADIUS 再試行構成の例を示します。

```
config
   profile radius
      max-retry 2
      exit
```

# 最大送信数の構成

RADIUS サーバーの最大伝送数を構成するには、次の構成を使用します。

```
config
   profile radius
      max-transmissions value
      end
```

**注**：

- **profile radius**：RADIUS 構成モードに入ります。

- **max-transmissions** *value*：最大伝送では、使用可能なすべてのサーバーの伝送パラメータを構成できます。この機能は、要求の再試行サイクルが終了した後に、送信回数が再試行回数を超えているかどうかをクロスチェックするのに役立ちます。その場合、使用可能な時は別のサーバーで後続の再試行サイクルが開始されます。使用可能なサーバーがない場合、またはmaxtransimissionsの制限に達した場合、サーバーデータベースはタイムアウト応答を送信します。

  *value*：0 ー 65535 の範囲の整数である必要があります。デフォルト: 6。

- 最大伝送値は、最大再試行回数 + 1 よりも常に高い値にする必要があります。maxTransmissions の数値を（maxRetries + 1）の倍数として使用することを推奨します。
- maxTransmissions に基づいて、単一の要求に費やされる時間が増加し、他のサーバーで再試行しても応答が提供されないままシステムに残ります。その結果、システムリソースが使用され、パフォーマンスが低下する可能性があります。

RADIUS サーバー グループの最大伝送数を構成するには、次の構成を使用します。

```
config
  profile radius
    server-group group_name
      max-transmissions value
      end
```

注：

- **profile radius**：RADIUS 構成モードに入ります。
- **server-group** *group_name*：最大転送数を構成するサーバーグループを入力します。
- **max-transmissions** *value*：最大伝送では、使用可能なすべてのサーバーの伝送パラメータを構成できます。この機能は、要求の再試行サイクルが終了した後に、送信回数が再試行回数を超えているかどうかをクロスチェックするのに役立ちます。その場合、使用可能な時は別のサーバーで後続の再試行サイクルが開始されます。使用可能なサーバーがない場合、またはmaxtransimissionsの制限に達した場合、サーバーデータベースはタイムアウト応答を送信します。

  *value*：0 ー 65535 の範囲の整数である必要があります。デフォルト: 6。

- 最大伝送値は、最大再試行回数 + 1 よりも常に高い値にする必要があります。maxTransmissions の数値を（maxRetries + 1）の倍数として使用することを推奨します。
- maxTransmissions に基づいて、単一の要求に費やされる時間が増加し、他のサーバーで再試行しても応答が提供されないままシステムに残ります。その結果、システムリソースが使用され、パフォーマンスが低下する可能性があります。

# RADIUS タイムアウトの構成

次の構成例を使用して、RADIUS タイムアウトを構成します。

```
config
  profile radius
     timeout value_in_seconds
     commit
```

注：

- **profile radius**：RADIUS 構成モードに入ります。
- **timeout** *value_in_seconds*：再送信する前に RADIUS サーバからの応答を待機する時間を設定します。

  *value_in_seconds* は 1 ～ 65535 の範囲の整数である必要があります。デフォルト：2 秒。
- **commit**：次の構成をコミットします。

例

次に、RADIUS タイムアウトの構成例を示します。

```
config
   profile radius
      timeout 4
      exit
```

# RADIUS POD の構成

次の構成例を使用して、RADIUS ディクショナリを構成します。

```
config
   instance instance-id gr_instance_id
      endpoint radius
         replicas number_of_replicas
         commit
```

注：

- **endpoint radius**：RADIUS エンドポイント構成モードに入ります。
- **replicas** *number_of_replicas*：必要なレプリカの数を設定します。
- **commit**：次の構成をコミットします。

例

RADIUS ポッドの構成例を次に示します。

```
config
   instance instance-id 1
      endpoint radius
         replicas 3
         exit
```

# RADIUS NAS-IP の構成

ここでは、RADIUS NAS-IP の構成方法について説明します。

### 複数の RADIUS NAS-IP 構成

**Note** NAS-Identifier 属性の構成は、RADIUS プロファイル構成の instance-id ごとに定義できます。この場合、インスタンス構成の下の NAS-Identifier 属性は、非インスタンス ベースの NAS-Identifier 属性構成よりも高い優先順位として扱われます。

複数の RADIUS NAS-IP アドレスをさまざまなレベルで構成するには、次の構成例を使用します。

```
config
  profile radius
     attribute [[ instance gr_instance_id ] [ nas-ip ipv4_address ] ]
     accounting attribute [[ instance gr_instance_id ] [ nas-ip ipv4_address
] ]
     server-group group_name attribute [[ instance gr_instance_id ] [ nas-ip
ipv4_address ] ]
     server-group group_name accounting attribute [[ instance gr_instance_id
] [ nas-ip ipv4_address ] ]
     end
```

注：

- **profile radius**：RADIUS 構成モードに入ります。
- **attribute [[ instance** *gr_instance_id* **] [ nas-ip** *ipv4_address* **] ]**：グローバル NAS-IP アドレス値を設定します。
  - **instance** *gr_instance_id*：地理的冗長性（GR）インスタンス ID を指定します。*gr_instance_id* は 整数である必要があります。
  - **nas-ip** *ipv4_address*：NAS の IPv4 アドレスを指定します。 *ipv4_address* は 、ドット付き 10 進表記の IPv4 アドレスである必要があります。
- **accounting attribute [[ instance** *gr_instance_id* **] [ nas-ip** *ipv4_address* **] ]**：グローバル アカウンティング NAS-IP アドレス値を設定します。
  - **instance** *gr_instance_id*：地理的冗長性（GR）インスタンス ID を指定します。*gr_instance_id* は 整数である必要があります。
  - **nas-ip** *ipv4_address*：NAS の IPv4 アドレスを指定します。 *ipv4_address* は 、ドット付き 10 進表記の IPv4 アドレスである必要があります。
- **server-group** *group_name* **attribute [[ instance** *gr_instance_id* **] [ nas-ip** *ipv4_address* **] ]**：サーバーグループごとの共通 NAS-IP アドレス値を設定します。

- **instance** *gr_instance_id*：地理的冗長性（GR）インスタンス ID を指定します。*gr_instance_id* は 整数である必要があります。
- **nas-ip** *ipv4_address*：NAS の IPv4 アドレスを指定します。 *ipv4_address* は 、ドット付き 10 進表記の IPv4 アドレスである必要があります。

- **server-group** *group_name* **accounting attribute [[ instance** *gr_instance_id* **] [ nas-ip** *ipv4_address* **] ]**：サーバ グループごとのアカウンティング NAS-IP アドレス値を設定します。
  - **instance** *gr_instance_id*：地理的冗長性（GR）インスタンス ID を指定します。*gr_instance_id* は 整数である必要があります。
  - **nas-ip** *ipv4_address*：NAS の IPv4 アドレスを指定します。 *ipv4_address* は 、ドット付き 10 進表記の IPv4 アドレスである必要があります。

**例**：

次に、複数 RADIUS NAS-IP の構成例を示します。

```
config
 profile radius
  attribute
   instance 1
    nas-ip 209.165.200.225
    nas-identifier  smf1
   exit
   instance 2
    nas-ip 209.165.201.2

    nas-identifier  smf2
   exit
  exit
  accounting
   attribute
    instance 1
     nas-ip 209.165.200.225
     nas-identifier  smf1
    exit
    instance 2
     nas-ip 209.165.201.2

     nas-identifier  smf2
    exit
   exit
  exit
 exit
 server-group g1
  attribute
   instance 1
    nas-ip 209.165.200.225
    nas-identifier  smf1
   exit
   instance 2
    nas-ip 209.165.201.2

    nas-identifier  smf2
   exit
  exit
 exit
```

```
 accounting
  attribute
   instance 1
    nas-ip 209.165.200.225
    nas-identifier  smf1
   exit
   instance 2
    nas-ip 209.165.201.2

    nas-identifier  smf2
   exit
  exit
 exit
exit
```

# セカンダリ認証メソッドの構成

次の構成例を使用して、セカンダリ認証方式を構成します。

```
config
  profile dnn dnn_name
     authentication secondary radius [ group group_name ]
     commit
```

注：

- **profile dnn** *dnn_name*：DNN プロファイル構成モードを開始します。
- **authentication secondary radius [ group** *group_name* **]**：DNN プロファイルでセカンダリ認証を有効にし、方式を RADIUS に設定します。

  **group** *group_name*：このキーワードはオプションです。このキーワードは RADIUS サーバー グループ名を定義します。
- **commit**：次の構成をコミットします。

**例**

次に、セカンダリ認証方式の構成例を示します：

```
config
   profile dnn intershat
   ...
   authentication secondary radius
   exit
```

## RADIUS 認証構成の確認

RADIUS 認証サーバおよびポートの詳細な統計情報を表示するには、 **show radius auth-server** コマンドを使用します。

以下の構成は、 **show radius auth-server** コマンドの出力例です：

```
bng# show radius auth-server
-------------------------------------------------------
 Server: 209.165.200.232, port: 1812, status: up, port-type: Auth
 2 requests, 0 pending, 0 retransmits
 1 accepts, 1 rejects, 0 timeouts
```

```
 0 bad responses, 0 bad authenticators
 0 unknown types, 0 dropped, 4 ms latest rtt
---------------------------------------------------------
```

# PAP、CHAP、または MSCHAP ベースの認証の構成

このセクションでは、PAP、CHAP、および MSCHAP ベースの RADIUS 認証を有効にするための構成について説明します。この構成は、PCO IE で受信した CHAP チャレンジ/レスポンスを MSCHAP チャレンジ/レスポンスとして変換するのに役立ちます。

## 認証アルゴリズムの優先順位の定義

次の構成例を使用して、SMF の RADIUS ベースの認証のさまざまな認証アルゴリズム（PAP、CHAP、または MSCHAP）の優先順位を定義します。

```
config
   profile dnn profile_name
      authentication { { secondary radius [ group group_name  ] | {
algorithm { pap priority_value [ password-use-pco ] | chap priority_value [
convert-to-mschap ] | mschap priority_value } }
      end
```

注：

- **password-use-pco**：このキーワードは、DNN で構成されたパスワードを PCO パスワードで上書きします。デフォルト設定では無効になっています。

  ホストレベルのパスワードが DNN で構成されていない場合、SMF は、この構成が無効になっていても、PAP ベースの認証に UE が指定したパスワードを使用します。

- **convert-to-mschap**：このキーワードは、CHAP 応答の長さが 49 バイトの場合に、受信した CHAP チャレンジと応答を MSCHAP に変換します。それ以外の場合は、この構成が明示的に有効になっている場合でも、SMF は CHAP として送信します。

- PAP、CHAP、および MSCHAP アルゴリズムのデフォルトの優先順位は 0 であり、構成が無効であることを意味します。有効な値は 1、2、3 です。値が小さいほど、優先順位が高くなります。UE が PCO、EPCO、または APCO IE で複数の認証パラメータを送信する場合に、競合を解決するために使用されます。

## ホスト パスワードの構成

次の構成例を使用して、PAP ベースの認証のパスワードとして使用される DNN レベルでホスト パスワードを指定します。

```
config
   profile dnn profile_name
      outbound password password
      end
```

注：

- **profile dnn** *profile_name*：DNN コンフィギュレーション モードを開始する英数字の文字列として DNN プロファイル名を指定します。
- **outbound password** *password*：認証用の DNN ホスト パスワードを指定します。デフォルトでは、**password-use-pco** オプションを使用して明示的に上書きされていない場合、SMF は PAP ユーザー パスワードでこのパスワードを送信します。

  デフォルトでは、SMF は AES-128-CFB 暗号化アルゴリズムを使用して指定されたパスワードを暗号化します。

# RADIUS アカウンティングの有効化

次の構成例を使用して、SMF で RADIUS アカウンティングを有効にし、RADIUS アカウンティング固有のパラメータを構成します。

```
config
  profile charging charging_profile_name
     accounting limit { duration value | volume { downlink value | total
 value | uplink value } }
     accounting triggers [ ambr-change | plmn-change | qos-change |
rat-change | serv-node-change | tft-change | ue-time-change |
user-loc-change ]
     commit
```

注：

- **profile charging** *charge_profile_name*：課金プロファイル名を指定します。 *charge_profile_name* は 英数字の文字列である必要があります。
- **accounting**：このオプションを指定すると、サブスクライバの SMF で RADIUS アカウンティングが有効になります。
- **limit { duration** *value* **| volume { downlink** *value* **| total** *value* **| uplink** *value* **} }**：RADIUS アカウンティングのボリュームと時間の上限を指定します。

  **duration** *value*：継続時間の値を 0 ～ 2147483647 の範囲の整数で指定します。

  **downlink** *value*：中間生成のダウンリンク ボリューム制限をバイト単位で 100000 ～ 4000000000 の範囲の整数で指定します。

  **total** *value*：中間生成の合計ボリューム制限を 100000 ～ 4000000000 の範囲の整数で指定します（バイト単位）。

  **uplink** *value*：中間生成のアップリンクボリューム制限を 100000 ～ 4000000000 の範囲の整数でバイト単位で指定します。
- **accounting triggers [ ambr-change | plmn-change | qos-change | rat-change | serv-node-change | tft-change | ue-time-change | user-loc-change ]**：次の条件に従って、適切な RADIUS アカウンティング トリガーをイネーブルにします。
  - AMBR の変更
  - PLMN の変更

- Quality of Service（QoS）の変更
- ルーティング エリア情報の変更
- サービング ノードの変更
- トラフィック フロー テンプレート（TFT）の変更
- UE 時間の変更
- ユーザーの場所情報の変更：PGW-C および GGSN にのみ適用されます。

**重要** これらのトリガーのいずれかを有効にすると、残りのトリガーがオフになります。

- **commit**：次の構成をコミットします。

# DNN プロファイルでの RADIUS サーバー グループの定義

次の構成例を使用して、DNN プロファイルのアカウンティングに使用する RADIUS サーバグループを設定します。

指定された DNN のすべてのサブスクライバで、RADIUS アカウンティングが有効になります。

```
config
  profile dnn dnn_profile_name
    accounting server-group group_name
    commit
```

注：

- **profile dnn** *profile_name*：DNN コンフィギュレーション モードを開始する DNN プロファイル名を指定します。*dnn_profile_name* は英数字の文字列である必要があります。
- **accounting server-group** *group_name*：構成済みの DNN プロファイルのアカウンティングで使用する RADIUS サーバ グループの名前を指定します。 *group_name* は 英数字の文字列である必要があります。
- **commit**：次の構成をコミットします。

# RADIUS アカウンティング オプションの構成

RADIUS アカウンティング オプションを構成するには、次の構成例を使用します：

```
config
  profile radius accounting
    algorithm { first-server | round-robin }
    attribute [ [ instance gr_instance_id ]  [ nas-identifier nas_id ] [
nas-ip ipv4_address ] ]
```

```
deadtime value
detect-dead-server response-timeout value
max-retry value
timeout value
end
```

注：

- **profile radius accounting**：RADIUS アカウンティング構成モードを開始します。
- **algorithm { first-server | round-robin }**：RADIUS サーバを選択するためのアルゴリズムを定義します。
  - **first-server**：選択ロジックを最初に最も高い優先順位に設定します。これはデフォルトの動作です。
  - **round-robin**：選択ロジックをサーバのラウンドロビン順に設定します。
- **attribute [ [ instance** *gr_instance_id* **] [ nas-identifier** *nas_id* **] [ nas-ip** *ipv4_address* **] ]**：RADIUS 識別パラメータを構成します。
  - **instance** *gr_instance_id*：地理的冗長性（GR）インスタンス ID を指定します。 *gr_instance_id* は 整数である必要があります。
  - **nas-identifier** *nas_id*：アカウンティング要求メッセージでシステムを識別する属性名を指定します。 *nas_id* は 英数字の文字列である必要があります。
  - **nas-ip** *ipv4_address*：NAS の IPv4 アドレスを指定します。 *ipv4_address* は 、ドット付き 10 進表記の IPv4 アドレスである必要があります。
- **deadtime** *value*：RADIUS サーバが到達不能とマークされてから、再び接続を試みることができるようになるまでの経過時間を設定します。

  *value* は 0 ～ 65535 の整数である必要があります。デフォルト: 10分。
- **detect-dead-server response-timeout** *value*：パケットが指定された秒数の間受信されなかった場合にサーバーを「デッド」とマークするタイムアウト値を設定します。

  *value* は 1 から 65535 までの整数値です。デフォルト：10 秒
- **max-retry** *value*：システムが RADIUS サーバとの接続を再試行する最大回数を設定します。

  *value* は 0 ー 65535 の範囲の整数である必要があります。デフォルト：2
- **timeout** *value*：再送信する前に RADIUS サーバからの応答を待機する時間を設定します。

  *value* は 1 ～ 65535 の範囲の整数である必要があります。デフォルト：2 秒。
- RADIUS アカウンティング コンフィギュレーション モードのすべての キーワード オプションは、RADIUS コンフィギュレーション モードでも使用できます。

# RADIUS アカウンティング サーバー グループの構成

RADIUS サーバー グループを構成するには、次の構成例を使用します。

```
config
  profile radius
    server-group group_name
    commit
```

注：

- **profile radius**：RADIUS 構成モードに入ります。
- **server group** *group_name*：RADIUS アカウンティングで使用するサーバーグループの名前を指定します。 *group_name* は 英数字の文字列である必要があります。
- **commit**：次の構成をコミットします。

## RADIUS アカウンティング 構成の確認

RADIUS アカウンティング サーバおよびポートの統計情報を表示するには、 **show radius acct-server** コマンドを使用します。

以下の構成は、 **show radius acct-server** コマンドの出力例です：

```
bng# show radius acct-server
----------------------------------------------------------
 Server: 209.165.200.228, port: 1813, status: up, port-type: Acct
 3 requests, 0 pending, 0 retransmits
 3 responses, 0 timeouts
 0 bad responses, 0 bad authenticators
 0 unknown types, 0 dropped, 1 ms latest rtt
----------------------------------------------------------
```

# セッション切断機能の構成

ここでは、セッション切断機能の構成方法について説明します。

SMF のセッション切断機能の構成には、次の手順が含まれます：

- 動的認可サービスの構成 （1459 ページ）
- CoA-NAS インターフェイスの構成 （1461 ページ）

## 動的認可サービスの構成

次の構成例を使用して、NAS をダイナミック認証サービスの認証、承認、および会計（AAA）サーバとして有効にします。このサービスは、RADIUS 切断および認可変更（CoA）機能をサポートしています。

```
config
   profile radius-dynamic-author
      client ipv4_address [ secret shared_secret ]
      nas-identifier value
```

```
secret shared_secret
end
```

注：

- **profile radius-dynamic-author**：パッケージ承認コンフィギュレーション モードを開始します。
- **client** *ipv4_address* **[ secret** *shared_secret* **]**：ダイナミック認証クライアントの IP アドレスを指定します。*ipv4_address* は、標準の IPv4 ドット付き 10 進表記にする必要があります。

  切断メッセージが受け入れられるクライアント IP のリストを追加できます。

  **secret** *shared_secret*：これはオプションのキーワードです。クライアント レベルで秘密キーを指定します。

重要 クライアント レベルでサーバー キーを設定すると、グローバル レベルで設定されたサーバー キーが上書きされます。

- **nas-identifier** *value*：ダイナミック認可固有の NAS-Identifier の値を指定します。 *value* は、1 ～ 64 文字の英数字の文字列である必要があります。

  このキーワードが構成されると、DM 要求で受信した値に対して検証されます。このキーワードが構成されていない場合、入力値はサイレントに無視されます。つまり、リストされていないクライアントまたは認証されていないクライアントからの DM 要求は、サイレントに廃棄されます。

- **secret** *shared_secret*：サーバのグローバル共有秘密キーを指定します。

## セッション切断機能構成の確認

ここでは、セッション切断機能の構成方法について説明します。

システムに構成されている RADIUS ダイナミック認可クライアントに関する情報を表示するには、 **show radius-dyn-auth** コマンドを使用します。

次に、**show radius-dyn-auth** コマンドの出力例を示します。

```
[unknown] smf# show radius-dyn-auth
radius-dyn-auth
------------------------------------------------------------
 IP: 209.165.200.227
 ------------------
 COA:
 0 total-requests     0 inprocess-requests
     0 retry-request-drops  0 invalid-requests
     0 bad-authenticators   0 internal-errors
 0 ack-sent             0 nak-sent
 ------------------
 DISCONNECT:
 0 total-requests     0 inprocess-requests
     0 retry-request-drops  0 invalid-requests
     0 bad-authenticators   0 internal-errors
 0 ack-sent             0 nak-sent
 ------------------
```

```
 UnknownTypesRcvd: 0
-------------------------------------------------------
```

## CoA-NAS インターフェイスの構成

次の構成例を使用して、RADIUSエンドポイントで認可変更（CoA）NASインターフェイスを定義します。

```
config
   instance instance-id gr_instance_id
      endpoint radius
         interface coa-nas
            vip-ip ipv4_address vip-port port_number
            end
```

注：

- **endpoint radius**：RADIUS エンドポイント構成モードを開始します。
- **interface coa-nas**：インターフェイス コンフィギュレーション モードを開始します。このキーワードは、新しいインターフェイス「coa-nas」を定義します。
- **vip-ip** *ipv4_address* **vip-port** *port_number*：ホストの IP アドレスを指定します。*ipv4_address* は、標準的なドット付き 10 進表記の IPv4 アドレスである必要があります。

  インバウンド CoA 要求または DM 要求をリッスンするための VIP-IP のリストを構成できます。

  **vip-port** *port_number*：仮想ホストのポート番号を指定します。デフォルトでは、ポート番号は3799です。このデフォルト値は、VIP-IPが指定されている場合にのみ使用されます。

重要　この構成では、IP ごとにポートのみを指定できます。

SMF（udp-pxy）は、これらのポートで着信 CoA または DM 要求メッセージをリッスンし、それぞれの送信元 IP とポートで送信された ACK または NAK メッセージをリッスンします。

# RADIUS クライアント OA＆M サポート

ここでは、この機能の操作、管理、およびメンテナンスに関して説明します。

## 統計情報サポート

### RADIUS 認証統計

この機能は、RADIUS 認証に関連する次の統計をサポートしています：

- SMF-Service：

- 送信されたセカンダリ認証要求の数
- 受信されたセカンダリ認証応答の数

- RADIUS-EP：
  - 送信されたセカンダリ認証要求の数
  - 受信されたセカンダリ認証応答の数
  - 送信された RADIUS パケットの数
  - 受信された RADIUS パケットの数。

### RADIUS 統計情報

SMF は次の統計情報を保持して、試行された、成功した、または失敗した RADIUS アカウンティングの開始、アカウンティングの更新の中間、およびアカウンティングの終了の要求と応答の合計数を追跡します。

- SMF_SERVICE_STATS（次の手順タイプの場合）。
  - radius_initial：このカウンタは、アカウンティング開始要求と応答で増分されます。
  - radius_update：このカウンタは、アカウンティングの中間更新要求と応答に対して増加します。
  - radius_terminate：このカウンタは、アカウンティング終了要求と応答に対して増分されます。

### RADIUS アクセス管理

次の統計情報は、SMF で RADIUS Access-Accept メッセージで AVP を受信した回数を追跡します。

- SmfRadiusMessageStats

  着信：
  - radius_access_accept
    - radius_avp_session_timeout
    - radius_avp_idle_timeout

### PAP、CHAP、または MSCHAP ベースの認証統計

SMF は、AVP が Access-Request メッセージで送信した回数を追跡するために、次の統計情報をサポートします。

**Group:** smf_radius_message_stats

**Format:** {app_name, cluster, data_center, direction, instance_id, message_type, radius_avp_type, rat_type, service_name}

**message_type:** radius_access_request

**radius_avp_type:**

- radius_avp_pap_user_password
- radius_avp_pap_username
- radius_avp_chap_challenge
- radius_avp_chap_response
- radius_avp_mschap_challenge
- radius_avp_mschap_response

例：

```
smf_radius_message_stats{app_name="SMF",cluster="Local",data_center="DC",direction="outbound",
instance_id="0",message_type="radius_access_request",radius_avp_type="radius_avp_pap_user_password",
rat_type="NR",service_name="smf-service"} 1

smf_radius_message_stats{app_name="SMF",cluster="Local",data_center="DC",
direction="outbound",instance_id="0",message_type="radius_access_request",
radius_avp_type="radius_avp_pap_username",rat_type="NR",service_name="smf-service"} 1
```

SMF はこれらの追加の統計情報をサポートして、PAP、CHAP、および MSCHAP 認証によって受信された、試行された応答、成功した応答、および失敗した応答の数を追跡します。

**Group:** radius_authentication_message_stats

**Format:** {app_name, cluster, data_center, dnn, instance_id, radius_auth_algorithm, rat_type, reason, service_name, status}

**radius_auth_algorithm:**

- radius_auth_algorithm_default
- radius_auth_algorithm_pap
- radius_auth_algorithm_chap
- radius_auth_algorithm_mschap

**rat_type:**

- NR
- EUTRA
- WLAN

**status:**

- decode_failed
- encode_failed
- attempted

- success
- 失敗しました
- タイムアウト

**reason:**

- parse_error
- invalid_code
- invalid_option
- invalid_pco
- invalid_epco
- invalid_apco
- write_error

例：

```
radius_authentication_message_stats{app_name="SMF",cluster="Local",
data_center="DC",dnn="intershat2",instance_id="0",
radius_auth_algorithm="radius_auth_algorithm_default",rat_type="NR",reason="",
service_name="smf-service",status="attempted"} 2

 radius_authentication_message_stats{app_name="SMF",cluster="Local",
data_center="DC",dnn="intershat2",instance_id="0",radius_auth_algorithm="radius_auth_algorithm_default",
rat_type="NR",reason="",service_name="smf-service",status="success"} 2

radius_authentication_message_stats{app_name="SMF",cluster="Local",data_center="DC",
dnn="intershat",instance_id="0",radius_auth_algorithm="radius_auth_algorithm_chap",
rat_type="EUTRA",reason="",service_name="smf-service",status="attempted"} 2

radius_authentication_message_stats{app_name="SMF",cluster="Local",
data_center="DC",dnn="intershat",instance_id="0",radius_auth_algorithm="radius_auth_algorithm_chap",

rat_type="EUTRA",reason="",service_name="smf-service",status="failed"} 2
```

### RADIUS 切断と CoA 要求に関連する統計情報

RADIUS エンドポイント (radius-ep) ポッドは、次の統計情報をサポートしています。

**Radius_Server_Status**

説明：RADIUS サーバのアクティブまたは非アクティブ ステータスを表示します。

Metrics-Type: Gauge

Metrics-値： 1 – ActiveServer, 0 – Inactive Server

ラベル

- ラベル： radSvrIP
  - 説明：サーバ IP アドレス
  - 値： <any-ip-address>

- ラベル： radSvrPort
  - 説明：サーバ ポート
  - 値： <any-port>
- ラベル： radSvrPortType
  - 説明：認証またはアカウンティング タイプ
  - 値： Auth, Acct

**Radius_Requests_Current**

説明：未処理の認証およびアカウンティング要求を表示します。

Metrics-Type: Gauge

ラベル

- ラベル： radMsgCode
  - 説明：RADIUS メッセージ タイプ
  - Values: SecondaryAuthenReq, RadiusAcctReq, TestAuth, TestAcct
- ラベル： radSvrIP
  - 説明：サーバ IP アドレス
  - 値： <any-ip-address>
- ラベル： radSvrPort
  - 説明：サーバ ポート
  - 値： <any-port>
- ラベル： radSvrPortType
  - 説明：認証またはアカウンティング タイプ
  - 値： Auth, Acct
- ラベル：dnn
  - 説明：サブスクライバの DNN
  - 値：<string>
- ラベル：procType
  - 説明：Procedure-type
  - 値： <string>

- ラベル： ratType
  - 説明：サブスクライバの RAT タイプ
  - 値：<string>
- ラベル： sessType
  - 説明：サブスクライバのセッション タイプ
  - 値：<string>
- ラベル：grInstId
  - 説明：地理的冗長性（GR）インスタンス ID
  - 値：<string>

**Radius_Requests_Statistics**

説明：送信、再送信、および受信された応答の総数を表示します。

Metrics-Type：カウンタ

ラベル

- ラベル: radMsgCode
  - 説明：Radius メッセージ タイプ
  - 値：SecondaryAuthenReq、RadiusAcctReq、TestAuth、TestAcct
- ラベル：radPacketType
  - 説明：パケットの方向
  - 値：Tx、Rx、Retry_Tx
- ラベル：radResult
  - 説明：操作の結果
  - 値：Success, Failed, Timeout, Failure_Reject, ...
- ラベル：radSvrIP
  - 説明：サーバ IP アドレス
  - 値：<any-ip-address>
- ラベル：radSvrPort
  - 説明：サーバ ポート
  - 値：<any-port>

- ラベル：radSvrPortType
  - 説明：認証またはアカウンティング タイプ
  - 値：Auth, Acct
- ラベル：dnn
  - 説明：サブスクライバの DNN
  - 値：<string>
- ラベル：procType
  - 説明：Procedure-type
  - 値：<string>
- ラベル： rat_type
  - 説明：サブスクライバの RAT タイプ
  - 値：<string>
- ラベル： sessType
  - 説明：サブスクライバのセッションタイプ
  - 値：<string>
- ラベル：grInstId
  - 説明：地理的冗長性（GR）インスタンス ID
  - 値：<string>

**Radius_CoaDM_Requests_Current**

説明：処理中の未処理の CoA 要求と DM 要求を表示します。

Metrics-Type: Gauge

ラベル

- ラベル：radMsgCode
  - 説明：RADIUS メッセージ タイプ
  - 値：DisconnectRequest、CoARequest
- ラベル：radSvrIP
  - 説明：サーバ IP アドレス
  - 値：<any-ip-address>

- ラベル：grInstId
  - 説明：地理的冗長性（GR）インスタンス ID
  - 値：<string>

**Radius_CoaDM_Requests_Statistics**

説明：受信および処理された CoA および DM 要求の総数を表示します。

Metrics-Type：カウンタ

ラベル

- ラベル：radMsgCode
  - 説明：Radius メッセージ タイプ
  - 値：DisconnectRequest、DisconnectACK、DisconnectNAK、CoARequest、CoaDMReq、CoAACK
- ラベル：radPacketType
  - 説明：パケットの方向
  - 値：Tx、Rx
- ラベル：radResult
  - 説明：操作の結果
  - 値：Success, Failure_Invalid_Request, Failure_Drop_Retry_Coa, Failure_Unknown_Error...
- ラベル：radSvrIP
  - 説明：サーバ IP アドレス
  - 値：<any-ip-address>
- ラベル：nakErrorCause
  - 説明：COA-NAK / DM-NAK 中に設定されたエラー原因（他のケースには適用されません）
  - 値：Missing-Attribute、NAS-Identification-Mismatch、Unsupported-Service、Invalid-Attribute-Value、Session-Context-Not-Found、Internal-Error
- ラベル：grInstId
  - 説明：地理的冗長性（GR）インスタンス ID
  - 値：<string>

# トラブルシューティング情報

このセクションでは、システムの動作中に発生する可能性のあるRADIUS関連の問題をトラブルシューティングするために、コマンドライン インターフェイス（CLI）コマンド、アラート、ログとメトリックスの使用に関する情報について説明します。

## RADIUS バルク統計情報

次のバルク統計情報を使用して、RADIUS認証、RADIUSアカウンティング、および切断メッセージ要求に関連する障害または問題をモニターします。

表 *428 : RADIUS* アカウンティング メッセージ（エンドポイントごと）

| バルク統計名 | 説明 |
| --- | --- |
| [illegible] | セッションの確立中にMサブスクライバによって試行されたアカウンティング要求の合計数。 |

| 説明 | バルク統計名 |
| --- | --- |
| セッションの確立中にMサブスクライバから成功したアカウンティング要求の合計数。 | [illegible] |

| バルク統計名 | 説明 |
| --- | --- |
| [illegible] | セッション確立中にMサブスクライバから送信された失敗したアカウンティング要求の合計数 |

| 説明 | バルク統計名 |
| --- | --- |
| セッション解放中にMWサブスクライバによって試行されたアカウンティング要求の合計数。 | [illegible] |

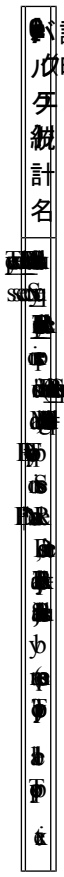
| 説明 | 名前 |
| --- | --- |
| セッション解放中にMサブスクライバから成功したアカウンティング要求の合計数 | [illegible] |

| 説明 | バルク統計名 |
| --- | --- |
| セッション解放中にMサブスクライバから送信された失敗したアカウンティング要求の合計数。 | [illegible] |

説明
統計名

| バルク統計名 | 説明 |
| --- | --- |
| ONM | 特定のリソースタイプに対してONMサブスクライバによって試行されたアカウンティング要求の |

| バルク統計名 | 説明 |
| --- | --- |
| | 合計数 |


説明
バルク統計名

| バルク統計名 | 説明 |
| --- | --- |
| QNVM | 特定のリソースタイプに対するVMサブスクライバからの成功したアカウンティング要求の合 |

| バルク統計名 | 説明 |
| --- | --- |
| | 計数。 |

| 説明 | 名前 |
| --- | --- |
| [illegible] | [illegible] |

| バルク統計名 | 説明 |
| --- | --- |
| ONM | 特定のリザスタイプに対するONMサブスクライバからの失敗したアカウンティング要求の合 |

| バルク統計名 | 説明 |
| --- | --- |
| | 計数 |

| 説明 | バルク統計名 |
| --- | --- |
| セッション確立中にSMサブスクライバによって試行されたアカウンティング再試行要求の合計数。 | [illegible] |

説明
名

| バルク統計名 | 説明 |
| --- | --- |
| ONM | セッションの解放中にNMサブスクライバによって試行されたアカウンティング再試行要求の合計 |

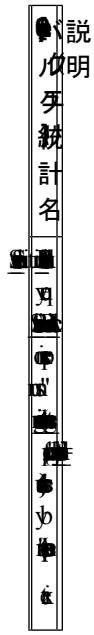
| バルク統計名 | 説明 |
| --- | --- |
| | 数 |

表 *429 : RADIUS* アカウンティング メッセージ（*SMF* サービスごと）

| バルク統計名 | 説明 |
|---|---|
| | |
| | |
| | |

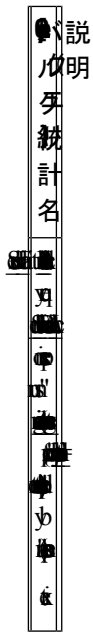
| バルク統計名 | 説明 |
| --- | --- |
| / | サービスエンドポイントからの RADIUS アカウンティングの初期開始試行を伴うサブスクライバの |

| バルク統計名 | 説明 |
| --- | --- |
| | 合計数 |


説明
統計名

| バルク統計名 | 説明 |
| --- | --- |
| / | サービスエンドポイントからアカウンティングの初期開始が成功したサブスクライバの合 |

| バルク統計名 | 説明 |
| --- | --- |
| | 計数。 |


説明

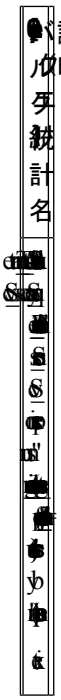
| バルク統計名 | 説明 |
| --- | --- |
| SIR | サービスエンドポイントからのアカウンティングの初期開始失敗が発生したサブスクライ |

| バルク統計名 | 説明 |
| --- | --- |
| | バの合計数。 |

| 説明 | 名前 |
| --- | --- |
| [illegible] | [illegible] |

| 統計名 | 説明 |
| --- | --- |
| sessstart | サービスエンドポイントからのRADIUSアカウンティング終了停止試行を使用したサブスクライバ |

| 説明 |
| --- |
| <バルク統計名> の合計数。 |


説明
名

| バルク統計名 | 説明 |
| --- | --- |
| SIR | サービスエンドポイントからのアカウンティング終了停止が成功したサブスクライバの合 |

| バルク統計名 | 説明 |
| --- | --- |
| | 計数。 |

| 説明 | 名 |
| --- | --- |
| [illegible] | [illegible] |

| バルク統計名 | 説明 |
| --- | --- |
| / | サービスエンドポイントからの RADIUS アカウンティング終了停止失敗を伴うサブスクライバの合 |

| バルク統計名 | 説明 |
| --- | --- |
| | 計数。 |

| 説明 |
| --- |
| バルク統計名 |
| [illegible] |

| 統計名 | 説明 |
| --- | --- |
| SIR | サービスエンドポイントからのアカウンティング更新中間試行を使用したサブスクライバ |

| バルク統計名 | 説明 |
| --- | --- |
| | の合計数。 |

| 説明 | バルク統計名 |
| --- | --- |
| サービスエンドポイントからの RADIUS アカウンティング更新中間成功のサブスクライバの合計数。 | [illegible] |

説明

| 統計名 | 説明 |
| --- | --- |
| SIR | サービスエンドポイントからのアカウンティング更新中間失敗があるサブスクライバの合 |

| バルク統計名 | 説明 |
| --- | --- |
| | 計数。 |

表 *430 :* 切断メッセージ

| バルク統計名 | 説明 |
| --- | --- |
| [illegible] | 切断メッセージ試行の合計数 |
| [illegible] | 成功した切断メッセージの合計数 |

| バルク統計名 | 説明 |
| --- | --- |
| [illegible] | 失敗した[illegible]切断メッセージの合計数 |

表 *431 : RADIUS* アクセス要求（セカンダリ認証）

| バルク統計名 | 説明 |
| --- | --- |
| [illegible] | アクセス要求セ(カンダリ認証が試行された ONM サブスクライバの合計数 |

| バルク統計名 | 説明 |
| --- | --- |
| [illegible] | アクセス要求に成功したMサブスクライバの合計数セ(カンダリ認証 |

| ルク統計名 | 説明 |
| --- | --- |
| [illegible] | アクセス要求に失敗したSMサブスクライバの総数セ(カンダリ認証 |

# RADIUS 固有の情報のサブスクライバの詳細

**show subscriber supi** *supi_id* **nf-service smf full** CLI コマンドは、RADIUS 固有の使用例のサブスクライバの詳細を表示します。

```
[unknown] smf# show subscriber supi imsi-123456789012345 nf-service smf
 full
subscriber-details
{
…
```

```
"alwaysOn": "None",
        "dcnr": "None",
        "wps": "Wps Session",
        "ratType": "NR",
        "idleTimeout": 600,      << can be overwritten from Radius in Auth
Resp
        "sessTimeout": 1200,     << can be overwritten from Radius in Auth
Resp
        "radiusEpInfo": "209.165.200.228:1812",
        "authAlg": "pap-default",
        "authStatus": "Authenticated"
…
…
        "accountingEnabled": "true",
        "n40ChargingEnabled": "true",
        "acctSessId": "198.15.1.40016777221"
…
…
"upfServData": {
        "numberOfTunnels": 2,
        "smfSeid": 72057615828912656,
        "UPState": "Activated",
        "urrInfo": [
          {
            "id": 2147483657,
            "chgName": "radiusurr",
            "method": {
              "duration": "false",
              "volume": "true",
              "event": "false"
            },
```

# RADIUS エンドポイントの認証とアカウンティングの統計情報

**show radius** CLI コマンドは、RADIUS エンドポイントからの RADIUS 認証とアカウンティングの統計情報を表示します。

```
[unknown] smf# show radius
radius
------------------------------------------------------
 Server: 209.165.200.240, port: 1812, status: up, port-type: Auth
 3 requests, 0 pending, 0 retransmits
 2 accepts, 0 rejects, 1 timeouts
 0 bad responses, 0 bad authenticators
 0 unknown types, 0 dropped, 1 ms latest rtt
------------------------------------------------------
------------------------------------------------------
 Server: 209.165.200.234, port: 1813, status: up, port-type: Acct
 3 requests, 0 pending, 6 retransmits
 0 responses, 3 timeouts
 0 bad responses, 0 bad authenticators
 0 unknown types, 0 dropped, 0 ms latest rtt
------------------------------------------------------
 Server: 209.165.200.245, port: 1813, status: up, port-type: Acct
 5 requests, 0 pending, 3 retransmits
 3 responses, 2 timeouts
 0 bad responses, 0 bad authenticators
 0 unknown types, 0 dropped, 6 ms latest rtt
------------------------------------------------------
[unknown] smf#
```

```
[unknown] smf# show radius acct-server
----------------------------------------------------------
 Server: 209.165.200.234, port: 1813, status: up, port-type: Acct
 3 requests, 0 pending, 6 retransmits
 0 responses, 3 timeouts
 0 bad responses, 0 bad authenticators
 0 unknown types, 0 dropped, 0 ms latest rtt
----------------------------------------------------------
 Server: 209.165.200.240, port: 1813, status: up, port-type: Acct
 5 requests, 0 pending, 3 retransmits
 3 responses, 2 timeouts
 0 bad responses, 0 bad authenticators
 0 unknown types, 0 dropped, 6 ms latest rtt
----------------------------------------------------------
[unknown] smf#
[unknown] smf# show radius auth-server
----------------------------------------------------------
 Server: 209.165.200.243, port: 1812, status: up, port-type: Auth
 3 requests, 0 pending, 0 retransmits
 2 accepts, 0 rejects, 1 timeouts
 0 bad responses, 0 bad authenticators
 0 unknown types, 0 dropped, 1 ms latest rtt
----------------------------------------------------------
[unknown] smf#
```

# RADIUS エンドポイント切断メッセージおよび CoA 統計情報

**show radius-dyn-auth** CLI コマンドは、RADIUS エンドポイントからの RADIUS 切断メッセージと CoA の統計を表示します。

```
[unknown] smf# show radius-dyn-auth
radius-dyn-auth
----------------------------------------------------------
 IP: 209.165.201.20
 ------------------
 COA:
 0 total-requests       0 inprocess-requests
     0 retry-request-drops  0 invalid-requests
     0 bad-authenticators   0 internal-errors
 0 ack-sent             0 nak-sent
 ------------------
 DISCONNECT:
 2 total-requests       0 inprocess-requests
     0 retry-request-drops  0 invalid-requests
     0 bad-authenticators   0 internal-errors
 1 ack-sent             1 nak-sent
 ------------------
 UnknownTypesRcvd: 0
----------------------------------------------------------
[unknown] smf#
```

# 外部インバウンドおよびアウトバウンド接続

**show peers all** CLI コマンドは、SMF によって確立された外部の着信および発信接続のリストを取得します。

```
[unknown] smf# show peers all | include radius
RadiusServer  -     209.165.202.145:1813   Outbound   radius-ep-0    Udp   18 hours
```

```
Radius  Status: Active,Type: Acct  1
RadiusServer  -     209.165.201.20:1812    Outbound   radius-ep-0    Udp   17 hours
Radius  Status: Active,Type: Auth  1
RadiusServer  -     209.165.201.20:1813    Outbound   radius-ep-0    Udp   17 hours
Radius  Status: Active,Type: Acct  1
[unknown] smf#
```

**重要** アプリケーションのスタートアップ中または構成の更新中に、RADIUS エンドポイントはテスト認証およびアカウンティング要求を送信して、RADIUS サーバー ピアのステータスを確認します。 **show peers** コマンドの出力に、ピア ステータスの結果が表示されます。

それらのダミー要求の結果は、実際の認証要求とアカウンティング要求の結果によって上書きされます。

# 内部および外部の接続

**show endpoint info** CLI コマンドは、SMF によって確立された内部および外部の接続のリストを取得します。

```
[unknown] smf# show endpoint all | include radius
Radius:209.165.201.4:     209.165.201.1:3799     Udp   Started  RADIUS     false     18
 hours  <none>   1
[unknown] smf#
```

# ポッドのステータス

**show running-status** CLI コマンドは、ポッドの現在のステータスを取得します。この機能は、K8 **kubectl get pods –n <>** CLI コマンドに似ています。

```
[unknown] smf# show running-status | include radius
radius-ep-0      Started      19 hours
[unknown] smf#
```

# 設定エラー

**show config-error** CLI コマンドは、検証基準（成功または失敗）を表示します。エントリがない場合は、[Pass] 基準が表示されます。

```
[unknown] smf# show config-error | include radius
[unknown] smf#
```

# アラートの表示

このセクションでは **show alerts** 、 CLI コマンドのさまざまな変数の出力例を示します。

**show alerts | include radius**

```
alerts history radius_test cfb253587397
alerts history radius_test 911f84aff47c
```

```
alerts history radius_test 3ed7a5112905
alerts history radius_test 292af807b299
 source      radius-ep-n0-0
 labels      [ "namespace: smf" "pod: radius-ep-n0-0" ]
 annotations [ "summary: Container:  of pod: radius-ep-n0-0 in namespace: smf has been
restarted." ]
 source      radius-ep-n0-0
 labels      [ "name:
k8s_radius-ep_radius-ep-n0-0_smf_7f9e968a-39dc-11eb-ba84-0050569cb367_0" "namespace:
smf" "pod: radius-ep-n0-0" ]
 annotations [ "summary: Container:
k8s_radius-ep_radius-ep-n0-0_smf_7f9e968a-39dc-11eb-ba84-0050569cb367_0 of pod:
radius-ep-n0-0 in namespace: smf has been restarted." ]
 source      radius-ep-n0-0
 labels     [ "name: k8s_POD_radius-ep-n0-0_smf_7f9e968a-39dc-11eb-ba84-0050569cb367_0"
 "namespace: smf" "pod: radius-ep-n0-0" ]
 annotations [ "summary: Container:
k8s_POD_radius-ep-n0-0_smf_7f9e968a-39dc-11eb-ba84-0050569cb367_0 of pod: radius-ep-n0-0
 in namespace: smf has been restarted." ]
alerts history radius_test 1c17e31c13f9
alerts history radius_test ffaabfce0929
 source      radius-ep-n0-0
 labels     [ "name: k8s_POD_radius-ep-n0-0_smf_cd16807a-2f0b-11eb-ba84-0050569cb367_0"
 "namespace: smf" "pod: radius-ep-n0-0" ]
 annotations [ "summary: Container:
k8s_POD_radius-ep-n0-0_smf_cd16807a-2f0b-11eb-ba84-0050569cb367_0 of pod: radius-ep-n0-0
 in namespace: smf has been restarted." ]
 source      radius-ep-n0-0
 labels      [ "namespace: smf" "pod: radius-ep-n0-0" ]
 annotations [ "summary: Container:  of pod: radius-ep-n0-0 in namespace: smf has been
restarted." ]
 source      radius-ep-n0-0
 labels      [ "name:
k8s_radius-ep_radius-ep-n0-0_smf_cd16807a-2f0b-11eb-ba84-0050569cb367_0" "namespace:
smf" "pod: radius-ep-n0-0" ]
 annotations [ "summary: Container:
k8s_radius-ep_radius-ep-n0-0_smf_cd16807a-2f0b-11eb-ba84-0050569cb367_0 of pod:
radius-ep-n0-0 in namespace: smf has been restarted." ]
[unknown] cee#
```

### show alerts active detail | include radius

```
alerts active detail Radius_Server_Down 0fe030aba3ce
 summary  "Radius Server: 209.165.201.20, Port: 1813 in namespace: smf is DOWN for more
 than 15min."
alerts active detail Radius_Server_Down 6f41c340311c
 summary  "Radius Server: 209.165.202.145, Port: 1813 in namespace: smf is DOWN for more
 than 15min."
alerts active detail Radius_Server_Down 8a290c5ed1de
 summary  "Radius Server: 209.165.201.20, Port: 1812 in namespace: smf is DOWN for more
 than 15min."
[unknown] cee#
[unknown] cee#
alerts active detail Radius_Server_Down 0fe030aba3ce
 severity major
 type     "Processing Error Alarm"
 startsAt 2020-12-11T13:30:16.874Z
 source   System
 summary  "Radius Server: 209.165.201.20, Port: 1813 in namespace: smf is DOWN for more
 than 15min."
 labels   [ "namespace: smf" "radSvrIP: 209.165.201.20" "radSvrPort: 1813" ]
alerts active detail Radius_Server_Down 6f41c340311c
 severity major
 type     "Processing Error Alarm"
```

```
 startsAt 2020-12-11T13:30:16.874Z
 source   System
 summary  "Radius Server: 209.165.202.145, Port: 1813 in namespace: smf is DOWN for more
 than 15min."
 labels   [ "namespace: smf" "radSvrIP: 209.165.202.145" "radSvrPort: 1813" ]
alerts active detail Radius_Server_Down 8a290c5ed1de
 severity major
 type     "Processing Error Alarm"
 startsAt 2020-12-11T13:30:16.874Z
 source   System
 summary  "Radius Server: 209.165.201.20, Port: 1812 in namespace: smf is DOWN for more
 than 15min."
 labels   [ "namespace: smf" "radSvrIP: 209.165.201.20" "radSvrPort: 1812" ]

[unknown] cee# show alerts active summary | include RTT
Radius_Server_RTT      1d0353b3db82  major     12-11T15:10:16  System   RTT for Radius
Server: 209.165.201.20, Port: 1812 in namespace: smf is more than 5 ms.
[unknown] cee#
```

### show alerts active summary | include RTT

```
Radius_Server_RTT      1d0353b3db82  major     12-11T15:10:16  System RTT for Radius
Server: 209.165.201.20, Port: 1812 in namespace: smf is more than 5 ms.
[unknown] cee#
```

### show alerts active summary | include radius

```
Radius_Server_RTT      1d0353b3db82  major     12-11T15:10:16  System
RTT for Radius Server: 209.165.201.20, Port: 1812 in namespace: smf is more than 5 ms.
Radius_Acct_Establish  520d9943d53f  major     12-11T15:05:16  System
This alert is fired when the percentage of successful Radius Accounting Establish responses
 received is lesser than threshold
Radius_Server_Down     0fe030aba3ce  major     12-11T13:30:16  System
Radius Server: 209.165.201.20, Port: 1813 in namespace: smf is DOWN for more than 15min.
Radius_Server_Down     6f41c340311c  major     12-11T13:30:16  System
Radius Server: 209.165.202.145, Port: 1813 in namespace: smf is DOWN for more than 15min.
Radius_Server_Down     8a290c5ed1de  major     12-11T13:30:16  System
Radius Server: 209.165.201.20, Port: 1812 in namespace: smf is DOWN for more than 15min.
```

# RADIUS アラート

MVNO または PAPN フローの RADIUS エンドポイントは、新しいアラートをサポートします。次の項では、いくつかの基本的なアラートについて説明します。これらのアラートは、RAT に基づいて、またはユーザーの必要性に応じて強化できます。

**重要** これらのアラートは、CEE Ops-center CLI を介してのみ構成できます。

## RADIUS EP ダウン アラート

次の例を使用して、RADIUS EP ダウンに関連するアラートを構成します。

```
alerts rules group RadiusEP
 rule Radius_Server_Down
  expression "sum by (namespace, radSvrIP, radSvrPort)
(Radius_Server_Status{radSvrPortType=~\"Auth|Acct\"} < 1)"
```

```
  duration   15m
  severity   major
  type       "Processing Error Alarm"
  annotation summary
  value "\"Radius Server: {{ $labels.radSvrIP }}, Port: {{ $labels.radSvrPort }} in
namespace: {{ $labels.namespace }} is DOWN for more than 15min.\""
  exit
 exit
```

## RADIUS アカウンティング確立の失敗しきい値アラート

RADIUSアカウンティングの確立の失敗しきい値に関連するアラートを構成するには、次の例を使用します。

```
alerts rules group RadiusEP
 rule Radius_Acct_Establish_SR
   expression "sum by (namespace)
(increase(Radius_Requests_Statistics{radMsgCode=\"RadiusAcctReq\", procType=\"PDU Session
 Establishment\", radPacketType=\"Rx\", radResult=\"Success\"}[5m])) / sum by (namespace)
 (increase(Radius_Requests_Statistics{radMsgCode=\"RadiusAcctReq\", procType=\"PDU Session
 Establishment\", radPacketType=\"Tx\"}[5m])) < 0.80"
   severity   major
   type       "Communications Alarm"
   annotation summary
     value "This alert is fired when the percentage of successful Radius Accounting
Establish responses received is lesser than threshold"
   exit
  exit
```

## RADIUS アカウンティングのリリースの失敗しきい値アラート

RADIUSアカウンティングのリリース失敗しきい値に関連するアラートを構成するには、次の例を使用します。

```
rule Radius_Acct_Release_SR
   expression "sum by (namespace)
(increase(Radius_Requests_Statistics{radMsgCode=\"RadiusAcctReq\", procType=\"PDU Session
 Release\", radPacketType=\"Rx\", radResult=\"Success\"}[5m])) / sum by (namespace)
(increase(Radius_Requests_Statistics{radMsgCode=\"RadiusAcctReq\", procType=\"PDU Session
 Release\", radPacketType=\"Tx\"}[5m])) < 0.80"
   severity   major
   type       "Communications Alarm"
   annotation summary
     value "This alert is fired when the percentage of successful Radius Accounting
Release responses received is lesser than threshold"
   exit
  exit
```

## RADIUS 認証失敗しきい値アラート

次の例を使用して、RADIUS 認証失敗しきい値に関連するアラートを構成します。

```
rule Radius_Auth_SR
   expression "sum by (namespace)
(increase(Radius_Requests_Statistics{radMsgCode=\"SecondaryAuthenReq\", procType=\"PDU
Session Establishment\", radPacketType=\"Rx\", radResult=\"Success\"}[5m])) / sum by
(namespace) (increase(Radius_Requests_Statistics{radMsgCode=\"SecondaryAuthenReq\",
procType=\"PDU Session Establishment\", radPacketType=\"Tx\"}[5m])) < 0.80"
   severity   major
   type       "Communications Alarm"
```

```
   annotation summary
     value "This alert is fired when the percentage of successful Radius Authentication
 Request responses received is lesser than threshold"
   exit
  exit
```

## RADIUS 接続解除メッセージの失敗しきい値アラート

RADIUS切断メッセージ障害しきい値に関連するアラートを構成するには、次の例を使用します。

```
rule Radius_Disconnect_Message_SR
   expression "sum by (namespace)
(increase(Radius_CoaDM_Requests_Statistics{radMsgCode=\"DisconnectACK\",
radPacketType=\"Tx\", radResult=\"Success\"}[5m])) / sum by
(namespace)(increase(Radius_CoaDM_Requests_Statistics{radMsgCode=\"DisconnectRequest\",
 radPacketType=\"Rx\"}[5m])) < 0.80"
   severity   major
   type       "Communications Alarm"
   annotation summary
     value "This alert is fired when the percentage of successful Disconnect Message
(DM) responses sent is lesser than threshold"
   exit
  exit
exit
```

## RADIUS サーバ RTT アラート

次の例を使用して、RADIUS サーバ RTT に関連するアラートを構成します。

```
rule Radius_Server_RTT
  expression "sum by (namespace, radSvrIP, radSvrPort)
(Radius_Server_Rtt_ms{radSvrPortType=~\"Auth|Acct\"} > 5)"
duration   15m
  severity   warning
  type       "Communications Alarm"
  annotation summary
   value "\"RTT for Radius Server: {{ $labels.radSvrIP }}, Port: {{ $labels.radSvrPort
}} in namespace: {{ $labels.namespace }} is more than 5 ms.\""
  exit
 exit
```

## RADIUS アカウンティング開始初期メッセージの失敗しきい値アラート

次の例を使用して、RADIUSアカウンティングの開始初期メッセージの失敗しきい値に関連するアラートを構成します。

```
rule Radius_Acct_Start_SR
   expression "sum by (namespace)
(increase(radius_accounting_message_stats{procedure_type=\"radius_initial\",
status=\"success\"}[5m])) / sum by (namespace)
(increase(radius_accounting_message_stats{procedure_type=\"radius_initial\",
status=\"attempted\"}[5m])) < 0.80"
   severity   major
   type       "Processing Error Alarm"
   annotation summary
     value "This service based alert is fired when the percentage of successful Radius
Accounting Start successful response received is lesser than threshold"
```

```
   exit
  exit
```

## RADIUS アカウンティング暫定/更新メッセージ失敗しきい値アラート

次の例を使用して、RADIUSアカウンティングの中間/更新メッセージの失敗しきい値に関連するアラートを構成します。

```
rule Radius_Acct_Interim_SR
   expression "sum by (namespace)
(increase(radius_accounting_message_stats{procedure_type=\"radius_update\",
status=\"success\"}[5m])) / sum by (namespace)
(increase(radius_accounting_message_stats{procedure_type=\"radius_update\",
status=\"attempted\"}[5m])) < 0.80"
   severity   major
   type       "Processing Error Alarm"
   annotation summary
     value "This service based alert is fired when the percentage of successful Radius
Accounting Interim Update successful response received is lesser than threshold"
   exit
  exit
```

## RADIUS アカウンティングの停止/終了メッセージの失敗しきい値アラート

次の例を使用して、RADIUSアカウンティングの停止/終了メッセージの失敗しきい値に関連するアラートを構成します。

```
rule Radius_Acct_Stop_SR
   expression "sum by (namespace)
(increase(radius_accounting_message_stats{procedure_type=\"radius_terminate\",
status=\"success\"}[5m])) / sum by (namespace)
(increase(radius_accounting_message_stats{procedure_type=\"radius_terminate\",
status=\"attempted\"}[5m])) < 0.80"
   severity   major
   type       "Processing Error Alarm"
   annotation summary
     value "This service based alert is fired when the percentage of successful Radius
Accounting Stop successful response received is lesser than threshold"
   exit
  exit
```

## RADIUS 認証タイプ メッセージ失敗しきい値アラート

次の例を使用して、RADIUS認証タイプのメッセージ失敗しきい値に関連するアラートを構成します。

```
rule Radius_Auth_Type_SR
   expression "sum by (namespace, radius_auth_algorithm)
(increase(radius_authentication_message_stats{radius_auth_algorithm=\"radius_auth_algorithm_.*\",
 status=\"success\"}[1m])) / sum by (namespace)
(increase(radius_authentication_message_stats{radius_auth_algorithm=\"radius_auth_algorithm_.*\",
 status=\"attempted\"}[1m])) < 0.80"
   severity   major
   type       "Processing Error Alarm"
   annotation summary
     value "This alert is fired when the percentage of successful Radius Auth Type
response received is lesser than threshold"
   exit
  exit
```

# Grafana チャート

Grafana チャートは、RADIUS エンドポイントまたはサービス エンドポイントに基づくモニタリングに使用されます。

- RADIUS 認証、アカウンティング、および接続解除メッセージを含むコール フロー用の RADIUS エンドポイント。
- アカウンティング初期、中間、または終了パケットに固有のアカウンティング フローのサービス エンドポイント。

# エラー ログ

このセクションでは、基本的なエラー状態と、障害をデバッグするための関連ログについて説明します。

## RADIUS 認証

### サーバが認証要求に応答しませんでした

次に、RADIUS サーバーによって応答されなかった RADIUS 認証要求に関するエラー ログを示します。

```
[smf-service-n0-0] 2020/09/17 07:14:52.921 smf-service [ERROR] [GenericAAA.go:786]
[smf-service0.smf-app.aaa] [imsi-123456789012345:5] [imsi-123456789012345:5] [16] Secondary
 Authentication Failed: TIMEOUT
[smf-service-n0-0] *errors.errorString Secondary Authentication Failed: TIMEOUT
[smf-service-n0-0]
/opt/workspace/smf-service/src/smf-service/vendor/wwwin-github.cisco.com/
mobile-cnat-golang-lib/app-infra.git/src/app-infra/infra/Transaction.go:621 (0xd89cae)
[smf-service-n0-0]
/opt/workspace/smf-service/src/smf-service/procedures/generic/GenericAAA.go:786 (0x144fa52)
```

### 認証段階でのコールの失敗

次に、RADIUS 認証段階でのコール失敗のエラー ログの例を示します。

```
[smf-service-n0-0]
[smf-service-n0-0] 2020/09/17 07:14:52.921 smf-service [ERROR] [idlestate.go:504]
[smf-service0.smf-app.aaa] [imsi-123456789012345:5] [imsi-123456789012345:5] [16]
USER_AUTHENTICATION_OR_AUTHORIZATION_FAILED
[smf-service-n0-0] *errors.errorString USER_AUTHENTICATION_OR_AUTHORIZATION_FAILED
[smf-service-n0-0]
/opt/workspace/smf-service/src/smf-service/vendor/wwwin-github.cisco.com/
mobile-cnat-golang-lib/app-infra.git/src/app-infra/infra/Transaction.go:621 (0xd89cae)
[smf-service-n0-0]
/opt/workspace/smf-service/src/smf-service/vendor/wwwin-github.cisco.com/
mobile-cnat-golang-lib/app-infra.git/src/app-infra/infra/Transaction.go:580 (0x15d7ddc)

[smf-service-n0-0]
/opt/workspace/smf-service/src/smf-service/procedures/4g/pdnsetup/idlestate.go:537
(0x15bc4f5)
```

## RADIUS サーバーが認証要求を拒否しました

次に、RADIUS サーバーによって拒否された RADIUS 認証要求に関するエラー ログを示します。

```
[smf-service-n0-0] 2020/12/09 09:20:14.047 smf-service [INFO] [idlestate.go:649]
[smf-service.smf-app.aaa] [imsi-123456789012345:5] [imsi-123456789012345:5] [1] Processing
 Secondary Authentication Response
[smf-service-n0-0] 2020/12/09 09:20:14.047 smf-service [ERROR] [GenericAAA.go:1173]
[smf-service.smf-app.aaa] [imsi-123456789012345:5] [imsi-123456789012345:5] [1] Secondary
 Authentication Failed: REJECT
[smf-service-n0-0] 2020/12/09 09:20:14.047 smf-service [DEBUG] [Genericutil.go:681]
[smf-service.smf-app.gen] Internal Transaction Submit with BP for MessageType: 118, SLA:
 0
[smf-service-n0-0] 2020/12/09 09:20:14.047 smf-service [DEBUG] [idlestate.go:169]
[smf-service.smf-app.gen] inCallStatus:9

**********************************************
Transaction Log received from Instance: smf.radius-ep.ajay-smf1.smf.0
************* TRANSACTION: 00004 *************
TRANSACTION SUCCESS:
    Txn Type             : SecondaryAuthenReq(2004)
    Priority             : 1
    Session State        : No_Session
LOG MESSAGES:
    2020/12/09 09:20:13.756 [TRACE] [infra.message_log.core] >>>>>>>>

    2020/12/09 09:20:13.757 [DEBUG] [Radius.smf.AAA] Starting smf AccessRequest
    2020/12/09 09:20:13.757 [DEBUG] [Radius.smf.AAA] Starting smf AccessRequest for User
 [msisdn-9884886688]
    2020/12/09 09:20:13.757 [DEBUG] [Radius.smf.AAA] Created new Radius Message for smf
 AccessRequest
    2020/12/09 09:20:13.757 [DEBUG] [Radius.smf.AAA] Selected server: 209.165.200.229:1812
 , nasIP: 209.165.200.237 PID: 4194304
    2020/12/09 09:20:13.757 [DEBUG] [Radius.smf.AAA] Sending an IPC Message to UDP proxy
 [198.18.1.4]
    2020/12/09 09:20:13.763 [DEBUG] [Radius.smf.AAA] PID: 4194304 - Response received
on channel
    2020/12/09 09:20:13.763 [DEBUG] [Radius.smf.AAA] Authentication Result for user
[8899776655] = [REJECT]
    2020/12/09 09:20:13.764 [TRACE] [infra.message_log.core] <<<<<<<<

**********************************************
```

## 不正な認証者による認証応答

以下の内容は、不正な認証者を使用した RADIUS 認証応答のエラー ログです。

```
[radius-ep-n0-0] ************* TRANSACTION: 00044 *************
[radius-ep-n0-0] TRANSACTION SUCCESS:
[radius-ep-n0-0]     Txn Type             : RadiusUdpProxyMsg(2002)
[radius-ep-n0-0]     Priority             : 1
[radius-ep-n0-0]     Session State        : No_Session
[radius-ep-n0-0] LOG MESSAGES:
[radius-ep-n0-0]     2020/12/09 13:20:38.874 [TRACE] [infra.message_log.core] >>>>>>>>
[radius-ep-n0-0]
[radius-ep-n0-0]     2020/12/09 13:20:38.874 [DEBUG] [Radius.smf.AAA] Response received
 from udp proxy
[radius-ep-n0-0]    2020/12/09 13:20:38.874 [DEBUG] [Radius.smf.AAA] SrcIp: 209.165.201.20
 SrcPort: 1812 DestIp: 209.165.201.4 DestPort: 16384
[radius-ep-n0-0]     2020/12/09 13:20:38.874 [ERROR] [Radius.smf.AAA] PID: 4194310 -
Packet dropped due to invalid authenticator
[radius-ep-n0-0]     2020/12/09 13:20:38.874 [TRACE] [infra.message_log.core] <<<<<<<<
```

```
[radius-ep-n0-0]
[radius-ep-n0-0] ***********************************************
```

# RADIUS アカウンティング

## アカウンティング要求タイムアウト

次に、RADIUS アカウンティング要求タイムアウトのエラー ログを示します。

```
[radius-ep-n0-0] ************* TRANSACTION: 00027 *************
[radius-ep-n0-0] TRANSACTION SUCCESS:
[radius-ep-n0-0]     Txn Type             : IntSmfAcctReqMsg(3)
[radius-ep-n0-0]     Priority             : 1
[radius-ep-n0-0]     Session State        : No_Session
[radius-ep-n0-0] LOG MESSAGES:
[radius-ep-n0-0]     2020/12/09 13:09:10.247 [TRACE] [infra.message_log.core] >>>>>>>>
[radius-ep-n0-0]
[radius-ep-n0-0]     2020/12/09 13:09:10.247 [DEBUG] [Radius.smf.AAA] Starting smf
AccountingRequest
[radius-ep-n0-0]     2020/12/09 13:09:10.247 [DEBUG] [Radius.smf.AAA] Starting smf
AccountingRequest for User [msisdn-9884886688]
[radius-ep-n0-0]    2020/12/09 13:09:10.247 [DEBUG] [Radius.smf.AAA] Created new Radius
 Message for smf AccountingRequest
[radius-ep-n0-0]     2020/12/09 13:09:10.247 [DEBUG] [Radius.smf.AAA] Selected server:
209.165.201.20:1813 , nasIP: 209.165.201.4 PID: 4194304
[radius-ep-n0-0]     2020/12/09 13:09:10.247 [DEBUG] [Radius.smf.AAA] Sending an IPC
Message to UDP proxy [209.165.201.4]
[radius-ep-n0-0]     2020/12/09 13:09:15.091 [DEBUG] [Radius.smf.AAA] PID: 4194304 -
Response received on channel
[radius-ep-n0-0]     2020/12/09 13:09:15.091 [ERROR] [Radius.smf.AAA] Retried MaxNumber
 of times without success
[radius-ep-n0-0]    2020/12/09 13:09:15.092 [DEBUG] [Radius.smf.AAA] Int-txn Accounting
 Result for user [9884886688] = [TIMEOUT]
[radius-ep-n0-0]     2020/12/09 13:09:15.092 [TRACE] [infra.message_log.core] <<<<<<<<
[radius-ep-n0-0]
[radius-ep-n0-0] ***********************************************
```

# アイドル タイムアウトに基づくリリース

## RADIUS から受信したアイドル タイムアウト

次に、RADIUS から受信したアイドル タイムアウトのエラー ログの例を示します。

```
[smf-service-n0-0] 2020/09/23 16:10:11.965 smf-service [DEBUG]
[Genericutil.go:7158] [smf-service.smf-app.gen] Idle timeout value received from Radius:
 10
[smf-service-n0-0] 2020/09/23 16:10:11.965 smf-service [DEBUG]
[Genericutil.go:7168] [smf-service.smf-app.gen] Starting cp idle timer with timeout
value: 10
```

## RADIUS から絶対セッション タイムアウトを受信しました

次に、RADIUS から受信した絶対セッション タイムアウトのエラー ログの例を示します。

```
[smf-service-n0-0] 2020/09/23 16:10:11.964 smf-service [DEBUG]
[Genericutil.go:7200] [smf-service.smf-app.gen] Session absolute timeout value
received from Radius: 200
```

### セッション クリーンアップ

セッション クリーンアップのエラー ログの例を次に示します。

```
[smf-service-n0-0] 2020/09/23 16:10:21.966 smf-service [WARN] [stateHandler.go:187]
[smf-service.smf-app.gen] [imsi-123456789012345:5] [imsi-123456789012345:5] [21]
TIMEOUT -- Cp Idle Session Timer Expired, Triggering release
```

## 切断メッセージ

### 不明なクライアントから受信した切断メッセージ

次に、不明なクライアントから切断メッセージを受信した場合のエラー ログの例を示します。

```
[radius-ep-n0-0] 2020/11/25 10:30:02.960 radius-ep [INFO] [processor.go:157]
[Radius.smf.Ipc] Process continue - 2003
[radius-ep-n0-0] 2020/11/25 10:30:02.960 radius-ep [DEBUG] [coa.go:23] [Radius.smf.AAA]
 [] [] [11] Coa/Disconnect Req received from udp proxy
[radius-ep-n0-0] 2020/11/25 10:30:02.960 radius-ep [DEBUG] [coa.go:43] [Radius.smf.AAA]
 [] [] [11] SrcIp: 209.165.201.20 SrcPort: 3799 DestIp: 209.165.201.4 DestPort: 3799
[radius-ep-n0-0] 2020/11/25 10:30:02.960 radius-ep [ERROR] [coa.go:253] [Radius.smf.Ipc]
 Bng Coa/Disconnect req failed - Invalid Coa Client 209.165.201.20
.
.
.
[radius-ep-n0-0] LOG MESSAGES:
[radius-ep-n0-0] 2020/11/25 10:30:02.960 [TRACE] [infra.message_log.core] >>>>>>>>
[radius-ep-n0-0]
[radius-ep-n0-0] 2020/11/25 10:30:02.960 [DEBUG] [Radius.smf.AAA] Coa/Disconnect Req
received from udp proxy
[radius-ep-n0-0] 2020/11/25 10:30:02.960 [DEBUG] [Radius.smf.AAA] SrcIp: 209.165.201.20
 SrcPort: 3799 DestIp: 209.165.201.4 DestPort: 3799
[radius-ep-n0-0] 2020/11/25 10:30:02.960 [ERROR] [Radius.smf.AAA] Unable to process
Coa/Disconnect request - Error during init of Radius Message Invalid Coa Client
209.165.201.20
[radius-ep-n0-0] 2020/11/25 10:30:02.960 [TRACE] [infra.message_log.core] <<<<<<<<
[radius-ep-n0-0]
[radius-ep-n0-0] ********************************************
```

### 無効なセッション ID キーを含む切断メッセージを受信しました

次に、無効なセッション ID キーが指定された切断メッセージを受信した場合のサンプル エラー ログを示します。

```
[radius-ep-n0-0] ************* TRANSACTION: 00009 *************
[radius-ep-n0-0] TRANSACTION SUCCESS:
[radius-ep-n0-0]     Txn Type             : RadiusUdpProxyCoaMsg(2003)
[radius-ep-n0-0]     Priority             : 1
[radius-ep-n0-0]     Session State        : No_Session
[radius-ep-n0-0] LOG MESSAGES:
[radius-ep-n0-0]     2020/11/25 10:49:43.942 [TRACE] [infra.message_log.core] >>>>>>>>
[radius-ep-n0-0]
[radius-ep-n0-0]    2020/11/25 10:49:43.942 [DEBUG] [Radius.smf.AAA] Coa/Disconnect Req
 received from udp proxy
[radius-ep-n0-0]    2020/11/25 10:49:43.942 [DEBUG] [Radius.smf.AAA] SrcIp: 209.165.201.20
 SrcPort: 3799 DestIp: 209.165.201.4 DestPort: 3799
[radius-ep-n0-0]    2020/11/25 10:49:43.942 [DEBUG] [Radius.smf.AAA] Decoded coa message
 type is DisconnectRequest
[radius-ep-n0-0]     2020/11/25 10:49:43.942 [ERROR] [Radius.smf.AAA] Unable to process
 DisconnectRequest - Error during construct Invalid DNN/IPv4Addr/IPv6Pfx value
[radius-ep-n0-0]     2020/11/25 10:49:43.942 [TRACE] [infra.message_log.core] <<<<<<<<
```

```
[radius-ep-n0-0]
[radius-ep-n0-0] ********************************************
```

# RADIUS テスト CLI サポート

**RADIUS テスト** CLI には、RADIUS 認証およびアカウンティング サーバとのネットワーク接続と、それらのサーバの構成をテストするためのメカニズムが用意されています。

この機能は、システムの RADIUS 構成の精度、RADIUS サーバ上のサブスクライバ プロファイルの構成、サーバの応答時間のトラブルシューティングに役立ちます。

## RADIUS アカウンティング サーバのテスト

RADIUSアカウンティング サーバーのテストに使用される場合、このツールは特定のユーザー名のアカウンティング要求メッセージを生成します。

（注） テストを実行する前に、RADIUS認証サーバーでユーザー名を構成しておく必要があります。

RADIUS 認証テスト ツールを実行するには、次のコマンドを入力します。

**test-radius accounting { all | server-group** *group_name* **| server** *server_ip_address* **port** *server_port* **} { client-nas** *client_nas_ip_address* **| grinstanceid** *gr_instanceID* **| username** *user_name* **}**

注：

- **all**：構成されているすべての RADIUS アカウンティング サーバーをテストするように指定します。
- **server-group** *group_name*：サーバーグループ機能用に、*group_name* という名前の RADIUS サーバーグループに構成された RADIUS 認証サーバーを指定します。
- **server** *server_ip_address*：テストする特定の RADIUS アカウンティングサーバーの IP アドレスを指定します。
- *server_port*：システムがテストするRADIUSアカウンティング サーバーとの通信時に使用する必要がある TCP ポートを指定します。
- **username** *user_name*：アカウンティング用にRADIUSサーバーに提供されるユーザー名を指定します。
- **client-nas** *client_nas_ip_address*：アカウンティング用に RADIUS サーバーに提供される送信元 NAS の IP アドレスを指定します。
- **grinstanceid** *gr_instanceID*：GR インスタンス ID を指定します。デフォルト値はローカル インスタンス ID です。

重要 **grinstanceid** は、非ネイティブ インスタンスには必須です。

**例**

次のコマンドは、すべての RADIUS サーバーを確認します。

```
test-radius accounting all
```

次のコマンドは、IP アドレスが *192.0.2.0* の RADIUS サーバーについて、user *user1*の RADIUS アカウンティングを確認します。

```
test-radius accounting server 192.0.2.0 port 5000 username user1
```

次のコマンドは、ユーザー *user1* の RADIUS アカウンティング サーバー グループ *star1* を確認します。

```
test-radius accounting server-group star1 username user1
```

## RADIUS 認証サーバのテスト

RADIUS 認証サーバのテストに使用される場合、このツールは特定のユーザー名の認証要求メッセージを生成します。

（注） テストを実行する前に、RADIUS認証サーバーでユーザー名を構成しておく必要があります。

RADIUS 認証テスト ツールを実行するには、Exec モードで、次のコマンドを入力します。

**test-radius authentication { all | server-group** *group_name* **| server** *server_ip_address* **port** *server_port* **} { client-nas** *client_nas_ip_address* **| grinstanceid** *gr_instanceID* **| username** *user_name* **| password** *password* **}**

**注**：

- **all**：構成されているすべての RADIUS 認証サーバをテストするように指定します。
- **server-group** *group_name*：サーバーグループ機能用に、*group_name* という名前の RADIUS サーバーグループに構成された RADIUS 認証サーバーを指定します。
- **server** *server_ip_address*：テストする特定の RADIUS 認証サーバの IP アドレスを指定します。
- *server_port*：システムがテストする RADIUS 認証サーバとの通信時に使用する必要がある TCP ポートを指定します。
- **username** *user_name*：認証用に RADIUS サーバに提供されるユーザー名を指定します。デフォルトのユーザー名は *test* です。
- **password** *password*：認証のために RADIUS サーバに提供されるユーザー名に関連付けるパスワードを指定します。デフォルトのパスワードは *test*です。
- **client-nas** *client_nas_ip_address*：アカウンティング用に RADIUS サーバーに提供される送信元 NAS の IP アドレスを指定します。

- **grinstanceid** *gr_instanceID*：GR インスタンス ID を指定します。デフォルト値はローカル インスタンス ID です。

重要 **grinstanceid** は、非ネイティブ インスタンスには必須です。

**例**

次のコマンドは、すべての RADIUS サーバーを確認します。

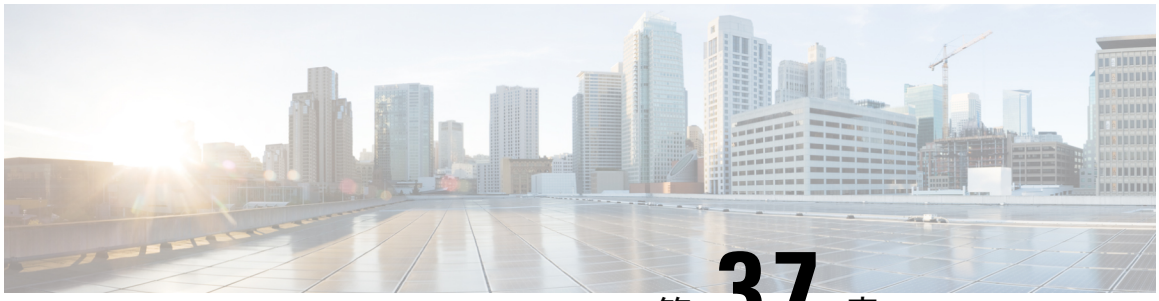
```
test-radius authentication all
```

次のコマンドは、IP アドレスが *192.0.2.0* の RADIUS サーバーについて、user *user1*の RADIUS アカウンティングを確認します。

```
test-radius authentication server 192.0.2.0 port 5000 username user1
password dummyPwd
```

次のコマンドは、ユーザー *user1* の RADIUS 認証サーバー グループ *star1* を「確認します。

```
test-radius authentication server-group star1 username user1
```



第 37 章

# 冗長性サポート


- 機能の概要と変更履歴 （1533 ページ）
- 機能説明 （1534 ページ）
- サポートされる冗長性のタイプ （1534 ページ）
- 高可用性のサポート （1535 ページ）
- ラック間冗長性サポート （1544 ページ）
- サイト間の地理的冗長性 （1627 ページ）


## 機能の概要と変更履歴

### 要約データ

表 *432* : 要約データ

| | |
|---|---|
| 該当製品または機能エリア | SMF |
| 該当するプラットフォーム | SMI |
| 機能のデフォルト設定 | • 冗長性サポート：有効の構成を無効にする必要があります。<br>• アクティブインスタンスの L2 VIP でのトラフィック モニタリング：無効の構成を有効にする必要があります。<br>• 地理強化：有効の構成を無効にする必要があります。<br>• アプリケーション VIP スイッチ オーバー時のセッション損失の最小化：該当なし。 |
| 関連資料 | 該当なし |

# 更新履歴

表 *433 :* マニュアルの変更履歴

| 改訂の詳細 | リリース |
|---|---|
| 高可用性冗長性のサポートが強化され、マスター ノード間のアプリケーション VIP スイッチオーバー時のセッション損失を最小限に抑えました。 | 2023.04.0 |
| 次のサブ機能のサポートが追加されました。<br>• アクティブ インスタンスの L2 VIP でのトラフィック モニタリング<br>• サイト間の冗長性<br>• GR の強化： | 2023.03.0 |
| メンテナンス モードのサポートが追加されました。 | 2021.04.0 |
| 地理的冗長（GR）サポートが導入されました。 | 2021.02.0 |
| 最初の導入。 | 2020.02.0 より前 |

# 機能説明

この章では、フェールオーバー シナリオの機能を達成するために必要な冗長性機能、アーキテクチャ、および構成の概要を示します。

# サポートされる冗長性のタイプ

SMF は、次のタイプの冗長性をサポートしています：

| 冗長タイプ | 説明 |
|---|---|
| [サーバ（Server）] | このソリューションは、サーバ障害を持続させ、クラスタ内の別のサーバにワークロードを分散するように設計されています。<br>このシナリオでは、Essential ポッドおよびサービス クリティカルなポッドのほとんどがアクティブ モードとスタンバイ モードで実行されており、ハードウェア障害が発生した場合の影響を最小限に抑えるために、異なるサーバーに存在します。 |

| 冗長タイプ | 説明 |
|---|---|
| ラック | このシナリオでは、Kubernetesクラスタが同じデータセンター内で異なるラックにミラーリングされます。<br>複数のサーバ障害、ソフトウェア障害、または隣接ルーティング層の問題が発生した場合、セッションは他のラックに切り替えられます。このようにして、新しいラックと同じレベルのサービスを確実に達成できるようになります。 |
| サイト | このシナリオでは、Kubernetes クラスタは異なる地理的なデータセンターにミラーリングされます。<br>データセンター全体がダウンタイムしている場合、セッションは別のデータセンターの他のラックに切り替えられます。これにより、新しいラックと同じレベルのサービスを確実に実現できます。 |

# 高可用性のサポート

**表 *434 :* 機能の履歴**

| 機能名 | リリース情報 | 説明 |
|---|---|---|
| アプリケーションVIPスイッチオーバー時のセッション損失の最小化 | 2023.04 | 高可用性の冗長性サポートは、gRPC IPC ストリームが中断すると、App-Infra ライブラリがただちに再試行し、gRPC エンドポイント間で IPC 接続を数ミリ秒以内に再確立する方法で SMF で強化されています。 |

## 機能説明

SMFは Kubernetes クラスタ戦略に基づいて構築されているため、K8 クラスタ展開の高可用性の側面を継承します。SMF は、ポッドやサービスなどのコンポーネントを含む構造を使用します。

各ポッドには、次に対して高可用性を確保するために少なくとも2つのインスタンスがあります

- ポッド インスタンスの再起動または障害
- ノードの再起動または障害によりポッドが失われました

ポッドとサービスの詳細については、このガイドの「ポッドとサービスの参考資料（1231 ページ）」の章を参照してください。

## UDP プロキシの高可用性

SMF は、UDP プロキシの高可用性（HA）をサポートしています。UDP プロキシの HA モデルは、キープアライブ仮想 IP の概念に基づいています。

UDPプロキシ冗長性に関する情報について、「ポッドとサービスの参考資料（1231ページ）」章の「UDP プロキシの高可用性 （1238 ページ）」セクションを参照してください。

## ノード マネージャの高可用性

SMF は、各 UPF の IPAM 冗長性とロード バランシングをサポートしています。ノード マネージャ マイクロサービスで実行されている IPAM には、各 UPF に関連付けられた 2 つの IPAM インスタンスがあります。1 つの IPAM インスタンスが非アクティブになると、もう 1 つの IPAM インスタンスが UPF のアドレス割り当て要求を管理します。

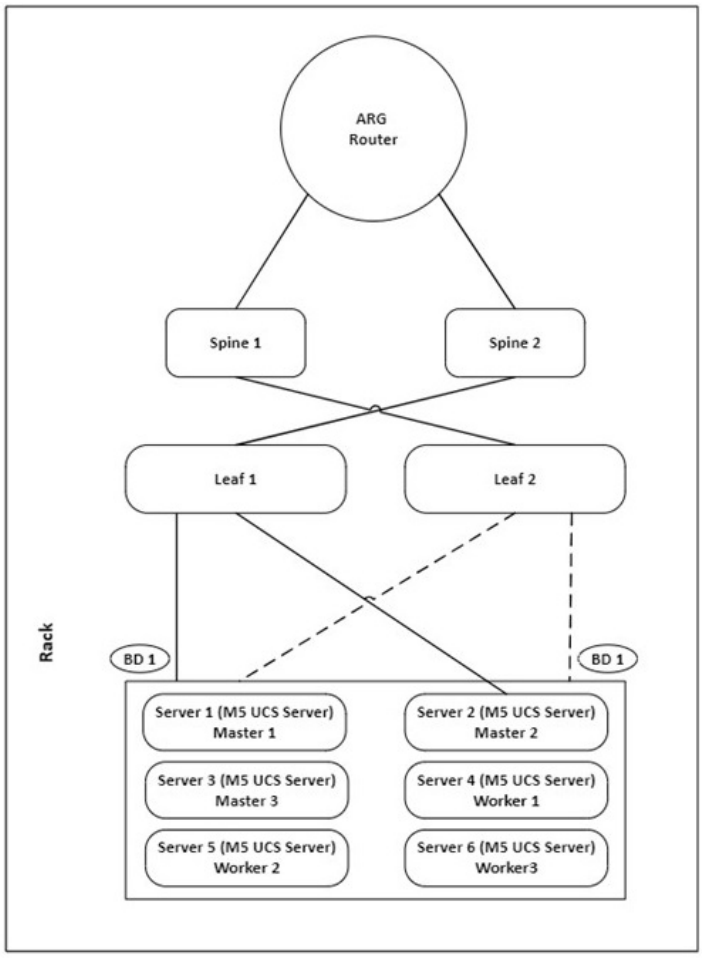
ノード マネージャ冗長性に関する情報については、「IP アドレス管理 （893 ページ）」章の「UPF ごとの IPAM 冗長性サポート （938 ページ）」セクションを参照してください。

## 内部ラックの高可用性

ラック内の高可用性は、サーバ レベルの冗長性を処理する配置です。このソリューションでは、1つのサーバで障害が発生した場合、設計に応じたいくつかのポッドが利用可能な別のサーバに分散される場合があります。一方、他のポッドは、サーバが復帰するまで保留状態のままです。

このシナリオでは、外部トラフィックを処理する重要なポッドが、別のサーバのアクティブ/スタンバイ ペアで実行されます。ルーティング レイヤでの冗長性サポートは、リーフおよびスパイン レイヤによって提供されます。

図 *245 :* 高可用性レイアウト




# アーキテクチャ

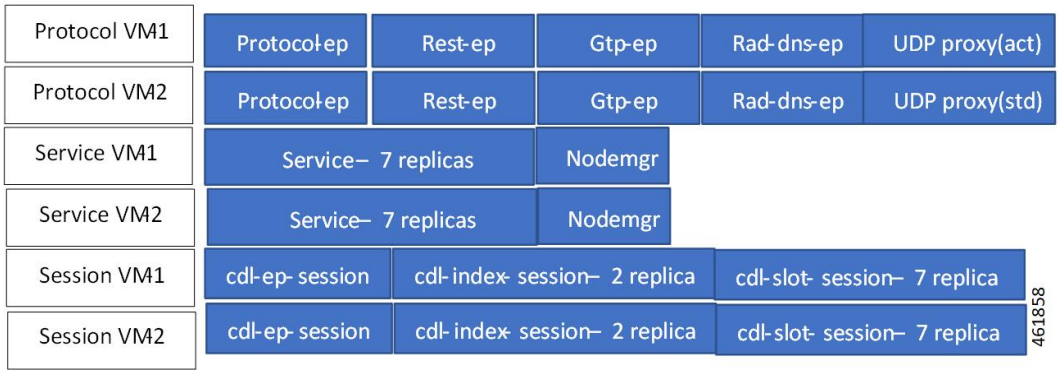
このセクションでは、SMF ポッドと VM の推奨レイアウトについて説明します。

## SMF ポッドおよび VM の展開レイアウト

ここでは、SMF ポッドとそのマイクロサービスの展開について説明します。

次の図は、SMF における 6 つの VM の導入モデルを示しています。

図 *246 : VM* 導入モデル




このモデルでは、ポッドはVMペアに展開されます。各プロトコルポッド（rest-ep、protocol-ep、gtp-ep など）に対して 2 つのレプリカを使用できます。各プロトコル VM に 1 つのインスタンスが展開されます。

同様に、サービス ポッドとセッション ポッドは、サービス VM とセッション VM の両方に均等に分散されます。このような分散は、VMにラベルを付け、ポッドのスケジューリング中に K8 アフィニティ ルールとアンチアフィニティルールを実装することによって制御されます。

このモデルにより、VM の再起動シナリオ中に、各 ポッドタイプの少なくとも 50% のレプリカがユーザー シグナリングの処理に使用可能になります。

ポッドのグレースフル再起動により、ポッドは進行中の処理を30秒以内に完了できます。ポッドの突然の再起動は、PDUセッションに影響を与えずに、進行中のトランザクションに影響を与えます。

# 機能の仕組み

ここでは、復元力と HA を実現する方法について説明します。

SMF は、ポッドの障害中または再起動中にポッド間通信を可能にします。

ポッドのグレースフル再起動中：

- 進行中の処理は影響を受けません。
- 新しいメッセージは、Kubernetes サービスを介してポッドに送信されません。
- セッション アフィニティを持つメッセージは、引き続きポッドで受信されます。
- 既存のコール フローは 30 秒以内に完了することが予想されます。

ポッドの再起動後：

- ポッドのすべての Prometheus メトリックがリセットされます。
- 内部ポッド診断に合格すると、ポッドのステータスが準備完了に変更されます。
- ポッドは新しいメッセージを処理する準備ができています。

SMF VM が再起動するか、VM が使用できない場合：

- VM 上のすべてのポッドが失われます。
- 使用可能な他の VM 上のポッドは処理を継続するため、高可用性が提供されます。
- VIP（存在する場合）は、他の使用可能なノードに切り替えられます。
- Kubernetes がノードをダウン状態として検出するには、ノードが到達不能になってから約 5 分間かかります。
- その後、ノード上のポッドは、Kubernetes サービスでは検出できません。

ポッドが再起動すると、VM 上のポッドが順次スケジュールされます。この操作は、ポッドの再起動に似ています。

VIP と VM の再起動中に、仮想 IP は単一の VM に関連付けられます。UDP プロキシは、UPF との通信のために N4 VIP アドレスにバインドします。UDP プロキシは、cnSGW との通信用に S5 VIP アドレスにバインドします。

アクティブな VIP で VM を再起動すると、VIP は他のプロトコルの VM に切り替わります。アクティブな UDP プロキシに障害が発生すると、VIP は他のプロトコル VM に切り替わります。

サブスクライバ マイクロサービス インフラストラクチャ（SMI）が VIP のモニタリングとスイッチオーバーを処理する前に、SMI デプロイメントで適切な VIP 構成が使用可能であることを確認してください。また、ポートが 28000 に設定されており、ホストの優先順位が同じであるかどうかを確認します。

BGP スピーカーは、そのノードでの IP アドレスの変更をモニタします。サービス IP アドレスが追加または削除されると、ネットリンクによる「IP モニタ」サポートを使用して、適切な Med 値でそれらをすぐにアドバタイズします。

VIP スイッチオーバー中に、gRPC IPC ストリームが中断すると、App-Infra ライブラリはすぐに再試行し、ミリ秒以内に gRPC エンドポイント間で IPC 接続が再確立されます。

BGP POD のグレースフル シャットダウン中、すべての VIP は他のマスターにフェールオーバーし、トラフィックは他のノードによってすぐに処理される必要があります。ピア ポッド/ノードの即時トラフィックを取得するために、ポッドをシャットダウンすると Med の優先順位（1217/1218）が低下します。

BFD リンクが両方のリーフからダウンしていると検出された場合、BGP スピーカーは VIP を他のマスターにすぐに移動する必要があります。これは、BGP スピーカーからのキープアライブ インターフェイスのモニタリングを再開し、BFD リンクがダウンしたときに特定することで実現されます。

# ポッドレベルのラベル付けとレプリカの構成

ノード ラベルは、SMI クラスタ デプロイヤで構成されます。構成コマンドに関する詳細は、「」章の構成コマンドを参照してください。

## 設定例

次に、VM のラベル付けとレプリカの構成例を示します。

```
k8 label protocol-layer key smi.cisco.com/node-type value smf-proto
exit
k8 label service-layer key vm-type value smf-svc
exit
k8 label cdl-layer key smi.cisco.com/node-type value smf-cdl
exit
k8 label oam-layer key smi.cisco.com/node-type value oam
exit

endpoint pfcp
 replicas 1
 nodes    2
exit
endpoint service
 replicas 1
 nodes    2
exit
endpoint protocol
 replicas 1
 nodes    2
 vip-ip 209.165.201.28
exit
endpoint sbi
 replicas 1
 nodes    2
```

## 設定の確認

構成を確認するには、次の show コマンドを使用します。

**show running-config instance instance-id** *instance_id* **endpoint**

以下は、この show コマンドの出力例です。

```
[unknown] smf# show running-config instance instance-id 1 endpoint
instance instance-id 1
 endpoint nodemgr
  replicas 1
  nodes    2
 exit
 endpoint gtp
  replicas 1
  vip-ip 209.165.202.149
 exit
 endpoint pfcp
  replicas                2
  enable-cpu-optimization true
  interface n4
   heartbeat
    interval               0
    retransmission-timeout 3
    max-retransmissions    5
   exit
  exit
 exit
 endpoint service
  replicas 2
 exit
 endpoint protocol
```

```
  replicas 1
  vip-ip 209.165.202.149
 exit
exit
```

このコマンド出力には、エンドポイント名、ポッドレプリカ、ノードなど、複数のエンドポイントに関連する構成が表示されます。

# アクティブ インスタンスの L2 VIP でのトラフィック モニタリング

## 機能説明

SMF は、トラフィックがないプロトコル ノード上のアクティブな L2 VIP を識別します。アクティブな L2 VIP の場合、ネットワーク接続の問題など、さまざまな理由によりトラフィックが存在しない場合があります。

アクティブな L2 VIP でトラフィックがないシナリオを検出すると、SMF はポッドの再起動を試みるか、CLI 構成アクションに基づいて GR をトリガーします。トラフィックの復元を容易にし、セッションの損失を最小限に抑えます。

この機能は、CLI を使用して有効または無効にすることができます。

## 機能の仕組み

- IPC L2 VIP でのトラフィックのモニタリングは定期的に行われ、構成可能な **no-traffic-duration** 時間と一致しています。
- 構成された時間内にアクティブ IPC L2 VIP にトラフィックがない場合、構成されたアクションに応じて、GR トリガーが発生し、他のラックがトラフィックを処理できるようにするか、ポッドが再起動され、VIP が他のポッドに切り替わります。トラフィックを復元します。
- ポッド再起動アクションが設定され、VIP スイッチオーバー後でもトラフィックが復元されない場合、IPC 接続モニタリング機能は、影響を最小限に抑えるように構成されていれば、GR シナリオをトリガーします。
- 次のチェックは定期的にモニターされます。チェックが条件を満たしている場合、トラフィックはモニターされます。
  - CLI 構成 **no-traffic-duration** は 10 秒より長くする必要があります。
  - CLI 構成 **session-threshold** は1000以上にする必要があります。デフォルト値は 1000 です。
  - GR インスタンス ID ロールのいずれかが PRIMARY であるかどうか。
  - 内部 VIP がプロトコル ノードに存在するかどうか。
  - セッション数が CLI を使用して設定したセッションしきい値以上の場合、トラフィック モニタリングがトリガーされます。ただし、セッション数が 1000 未満の場合、トラフィックの監視は停止します。

- 単一の IPC エンドポイントは、GR モードで両方の GR インスタンス ID のトラフィックを処理します。IPC エンドポイントでのトラフィック モニタリングは、GR インスタンス ID 固有ではありません。ただし、両方の GR インスタンス ID に対してチェックが実行されます。

## HA および GR シナリオの構成

HA（ポッド再起動）シナリオまたは GR（トリガ スイッチオーバー）シナリオをトリガするには、次の構成を使用します。

```
config
   monitor
      active-instance-traffic {  no-traffic-duration no_traffic_duration
session-threshold session_threshold action { pod-restart | trigger-switch-over
} }
```

注：

- **active-instance-traffic**：このキーワードを指定して、アクティブ トラフィック モニタリングを有効または無効にします。
- **no-traffic-duration** *no_traffic_duration*：アクティブ インスタンスでトラフィックが発生しない場合の最大許容時間（秒単位）。値の範囲は 10 ～ 300 です。この CLI に設定されているデフォルト値はありません。 **no-traffic-duration** の値は、**max-conn-downtime** の値よりも小さい値にする必要があります。
- **session-threshold** *session_threshold*：アクティブ インスタンス トラフィック モニタリングを開始するために必要な最小セッション数。値の範囲は 10 ～ 10000000 です。デフォルト値は 1000 です。
- **action {** *pod-restart* | *trigger-switch-over* **}**：条件を満たす際に実行するアクション。このコマンドに使用できる値は 、*pod-restart* および *trigger-switch-over*です。デフォルト値は *pod-restart*です。

### 設定例

次の例は、この機能の構成を示したものです：

```
smf(config)# monitor active-instance-traffic no-traffic-duration 15 session-threshold
1000 action pod-restart
```

### 設定の確認

次のコマンドは、この機能の出力を表示します：

```
smf# show running-config monitor active-instance-traffic
monitor active-instance-traffic no-traffic-duration 15 session-threshold 1000 action
pod-restart
```

## OAM サポート

このセクションでは、この機能でサポートされているさまざまな統計情報を定義します。

## KPI

次の KPI じゃ、この機能の一部としてサポートされいています：

### アクティブ インスタンスのトラフィック モニター サービス KPI

| KPI 名 | 説明 | ラベル |
|---|---|---|
| active_instance_traffic_monitor_services | この統計情報には、トラフィックモニタリングのために登録されているサービスが表示されます。 | interface_name<br>internal_vip_ip |

### アクティブ インスタンスのトラフィック モニターのステータス KPI

| KPI 名 | 説明 | ラベル | 有効な値 |
|---|---|---|---|
| active_instance_traffic_monitor_status | この統計には、アクティブ インスタンスのトラフィックモニタリングのステータスが表示されます。 | interface_name<br>internal_vip_ip | 0 ：モニタリングしません<br>1：モニタリング |

### アクティブ インスタンスのトラフィック モニタの理由 KPI

| KPI 名 | 説明 | ラベル | 有効な値 |
|---|---|---|---|
| active_instance_traffic_monitor_reason | この統計には、モニタリング状態または非モニタリング状態でのアクティブ インスタンス トラフィックのモニタリングの条件が一致しない場合の理由が表示されます。 | interface_name<br>internal_vip_ip | 1：GRインスタンスIDがプライマリではありません<br>2：現在のセッション数は、セッションしきい値数未満です<br>3：内部 VIP がアクティブでない<br>4：アクティブ インスタンス トラフィック モニターが設定されていない |

### アクティブ インスタンスのトラフィック モニターのセッション数 KPI

| KPI 名 | 説明 | ラベル |
|---|---|---|
| active_instance_traffic_monitor_session_count | この統計情報には、現在のセッション数が表示されます。 | interface_name<br>internal_vip_ip |

（注） 表示される数は、アフィニティ キャッシュから取得されます。

**アクティブ インスタンスのトラフィック モニターの最後の受信トラフィック KPI**

| KPI 名 | 説明 | ラベル |
|---|---|---|
| active_instance_traffic_monitor_last_recv_traffic | この統計情報には、トラフィックの最終受信時間が秒単位で表示されます。 | interface_name<br>internal_vip_ip |

（注） この統計は、**アクティブインスタンス トラフィック モニター**のすべての条件が満たされている場合にのみ計算されます。

# ラック間冗長性サポート

ラック間冗長性サポートとは、1 つのラックで障害や停止が発生した場合でも、システムまたはサービスがその機能と可用性を維持する機能を意味します。これは、同じ地理的な場所にある別のラックに操作を移動することで軽減できます。

## 機能説明

SMF は、アクティブ-アクティブ モードのラック間冗長性をサポートします。ラック間の冗長性は、リモート ラックへのサービスのシームレスなフェールオーバーとフェールバックに必要なセッション、構成、およびその他のデータのレプリケーションによって実現されます。

## 機能の仕組み

SMF （CNF）を同じデータセンターに展開して、SMF SMF クラスタをホストするラックにローカライズされた致命的な障害にサービスを提供できます。

各 CNF インスタンス サービスは、MME/SGW の DNS エントリのために NRF および S11/S5 に登録されます。ローカル HA 冗長性により、インスタンスは、同じデータセンター内の K8 クラスタ レベルの障害に加えて、ラック レベルの冗長性を実現したり、障害のあるコンテナがタイプ 2 < *n*ごとである場合に、同じ K8 クラスタ内でローカルに処理したりできます。

*n* は値です。コンテナ障害の 50% 未満の場合は、HA で障害を処理する必要があります。コンテナ障害の 50% を超えると、ラック間スイッチオーバーがトリガされます。

### 概要

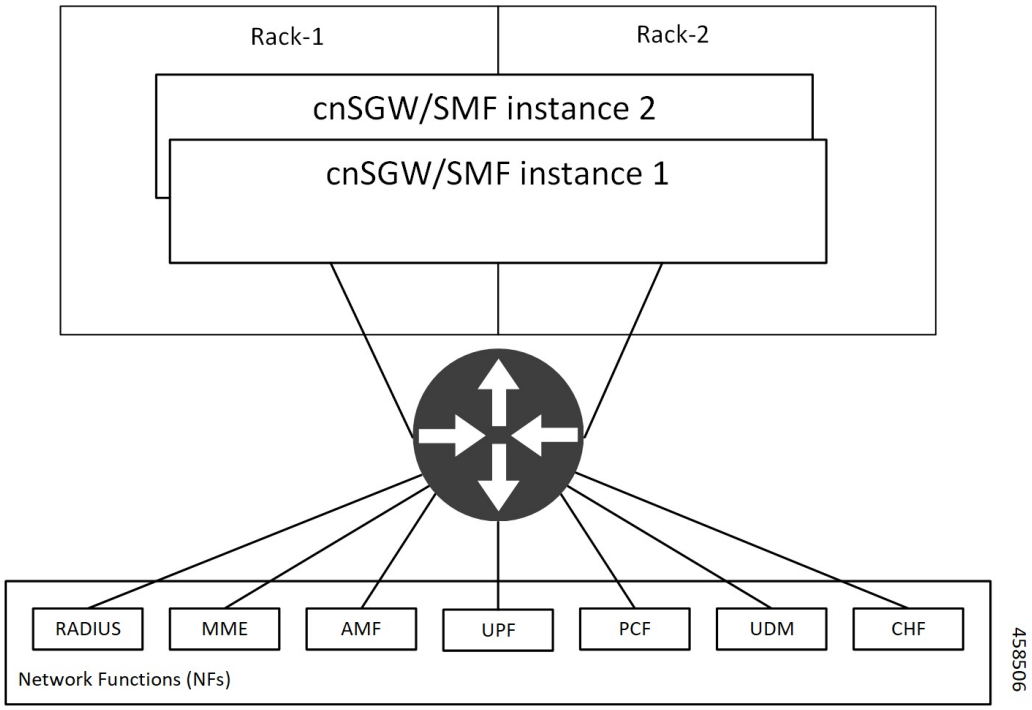
アクティブ - アクティブモード

- ラック間展開は、隣接する NF に対して透過的です。
- ラック間の展開には CCG 機能の 2 つのインスタンスが含まれ、各インスタンスは一連のインターフェイス IP で識別されます。
- 各インスタンスは一連のセッションをサポートし、セッションの一貫性のために同じ IP を使用し続けます。
- 特定の期間において、1つのCCGインスタンスは一方のラックでのみプライマリとして動作し、もう一方のラックではスタンバイとして動作します。
- CCG インスタンスに関連付けられている一連のインターフェイス IP は、インスタンスのプライマリ ラックにダイナミックにルーティングされます。

SMF は、データがプライマリからスタンバイ インスタンスに複製されるプライマリ/スタンバイ冗長性をサポートします。通常の動作では、プライマリ インスタンスがサービスを提供します。プライマリ インスタンスで障害が発生すると、スタンバイ インスタンスがプライマリになり、動作を引き継ぎます。ラック間の冗長性を実現するために、2つのプライマリ/スタンバイペアを設定できます。この場合は各ラックがアクティブにトラフィックを処理し、スタンバイ側がリモートラックのバックアップとして機能します。

アクティブ-アクティブのラック間冗長性展開で、同じデータセンターに 2 つのラックがあるとします（Rack-1 と Rack-2）。すべての NF が instance-1 と instance-2 に到達しようとしています。

**図 *247*: アクティブ-アクティブラック間冗長性展開**



NF の場合、両方のインスタンスがアクティブになります。しかし実際には、instance-1 と instance-2 はラックにまたがって分割されます。

Rack-1 には instance-1 と instance-2 があります。トリガー前のシナリオでは、instance-1 はローカルでプライマリとして機能し、instance-2 はスタンバイ モードになります。

Rack-2 には instance-1 と instance-2 も含まれています。トリガー前のシナリオでは、instance-2 はローカルでプライマリとして機能し、instance-1 はスタンバイ モードす。

Rack-1 がダウンすると、トラフィックは Rack-2 に移動します。ラック 2 では、instance-1 と instance-2 の両方がプライマリとして機能します。

# ラック間冗長性トリガ

ラック間冗長性は、次のトリガをサポートしています。

- **CLI ベースのスイッチオーバー**： 手動の CLI コマンドを使用して、ロールを切り替え、ラック間冗長性フェールオーバーをトリガします。
- **BFD リンク フェールオーバー検出**： 接続されたラックとリーフ間の両方の BFD リンクがダウンすると、ラック間冗長性フェールオーバーがトリガされます。
- **ローカル ラック POD 障害検出**： ポッド レプリカ セットの障害のしきい値パーセンテージが、構成されたしきい値より大きい場合、ラック間冗長性フェールオーバーがトリガされます。
- **リモート ラック ポッド障害検出**： リモート POD モニタリングで障害しきい値パーセンテージが検出されると、POD はそのインスタンスに対してセルフプライマリになります。
- **リモート ラック ロール モニタリング**： リモート ロール モニタリングで、ラックが Standy_error 状態であることが検出されると、そのラックはセルフプライマリになります。
- **マルチコンピューティング障害**：2 つ以上のサーバの電源がオフになると、ラック間冗長性フェールオーバーがトリガされます。

# ラック NF ロール

次に、適用可能なラック NF ロールのリストを示します。

（注）
- **Cachepod/etcd**および**CDL レプリケーション**は、次のセクションで説明されているすべてのロール中に発生します。
- ラック間リンクがダウンしているか、定期的なハートビートに失敗すると、これらのラック間冗長性トリガが一時停止します。

- **PRIMARY**：このロールでは、ラックは準備完了状態で、特定のインスタンスのトラフィックをアクティブに取得しています。

- **[スタンバイ（STANDBY）]**：このロールでは、ラックはスタンバイ モードであり、トラフィックを取得する準備ができていますが、特定のインスタンスのトラフィックを取得しません。
- **STANDBY_ERROR**：このロールでは、ラックは問題のある状態で、アクティブではなく、特定のインスタンスのトラフィックを取得する準備ができていません。

（注） インスタンス ロールが **STANDBY_ERROR** の状態の場合、データの複製は停止します。この状態では、**show georeplication-status** コマンドは常に失敗します。ただし、インスタンスのロールが **STANDBY** に移行されると、データの複製が自動的に再開され、 コマンドは結果が **pass** であると表示します。

- **FAILOVER_INIT**：このロールでは、ラックはフェールオーバーを開始し、トラフィックを取得する状態ではありません。アプリケーションがアクティビティを完了するまでのバッファ時間は 2 秒です。

新規インストールの場合、ラックは次のロールでブートアップします。

- **PRIMARY**：このロールでは、ラックはローカルインスタンス用です（各ラックには、ローカル**インスタンスを識別するように構成されたローカル インスタンス ID**があります）。新規インストール中は、ポッドをモニタリング用に構成しないことをお勧めします。セットアップの準備ができたら、モニタリング用にポッドを構成できます。
- **STANDBY**：このロールでは、ラックは他のインスタンスの にあります。

アップグレードの場合、ラックは次のロールでブートアップします。

- **STANDBY_ERROR**：このロールでは、アップグレード後にトラフィックを移動させるには手動の介入が必要なため、すべてのインスタンスがラックになります。

# 一般的なガイドライン

ラック間冗長性展開を構成する前に、一般的な注意事項を次に示します。

- 両方のラックのソフトウェア バージョンが同じである必要があります。
- 両方のラックの構成を同じにする必要があります。
- インスタンス 1 とインスタンス 2 のループバック ポートは異なる必要があります。そうしないと、K8 IP/ポートの競合が原因で REST-EP POD は起動しません。
- 両方のラックのそれぞれのインターフェイスは、同じ VLAN 上にある必要があります。たとえば、インスタンス 1 とインスタンス 2 の N4 VLAN は、同じ VLAN 上にある必要があります。そうでない場合、BGP ポリシーを適用しているときに、カーネルでルートの競合が発生します。

- 適切なロールが割り当てられていることを確認するには、Cisco のテクニカル担当者に問い合わせて、次の手順を実行してください。

  詳細については、GR ペアのソフトウェア アップデート （1586 ページ）を参照してください。

- フェールオーバー後、ラックが正常であることを確認してから、フェールバックを手動で実行します。自律フェールバックはサポートされていません。

  詳細については、回復手順 （1610 ページ）を参照してください。

- BGP ピアリングには、BGP スピーカー POD で非結合インターフェイスを使用します。
- Proto ノードごとの BGP ピアリングは、2 つの BGP ルータ/リーフのみでサポートされます。2 つの Proto ノードを考慮すると、最大 4 つの BGP ネイバーシップを設定できます。
- サービス トラフィックには結合インターフェイスを使用します。
- Geo ポッドでは、次の 2 つの VIP を使用します。
  - ポッド間通信用の内部 VIP（ラック内）
  - ラック間 Geo ポッド通信用の外部 VIP。L2 サブネットの Proto ノードでのみ構成します。これはラック間の通信に使用されます。このノードには他のラックへの外部接続があります。
- ラック内のすべてのノードに到達可能な Geo 内部 IP。
- Geo 外部 IP：
- CDL/Kafka VIP：L2 サブネット上の CDL ラベル付きノードで構成します。
- 両方のラックで LI タップを有効にします。
- MDF サーバは、両方のラックから到達可能である必要があります。

# インスタンス認識

SMF でのインスタンス認識構成は、ローカル ラック インスタンスとリモート ラック インスタンスを区別するのに役立ちます。

## ラック間冗長性インスタンスの構成

この設定は、複数ラックのラック間冗長性構成を提供するために必要です。インスタンス ID を使用して、ラックごとにエンドポイントを構成する必要があります。

### 構成例 1

以下は、1 つのインスタンスにおけるエンドポイント VIP 構成の構成例です。

```
config
  instance instance-id gr_instanceId
```

```
    endpoint endpoint_name
        vip-ip vip_ip_address
  exit
exit
```

例：

```
config
instance instance-id 1
 endpoint sbi
  vip-ip 209.165.201.21
 exit
exit
```

### 構成例 2

次に、インスタンスのシステム ID、クラスタ ID、スライス名に関する情報を提供する構成例を示します。

```
config
  instances instance instance_id
   system-id system_id
   cluster-id cluster_id
   slice-name cdl_slice_name
  exit
exit
```

例：

```
config
 instances instance 1
  system-id smf
  cluster-id smf
  slice-name 1
 exit
exit
```

（注） インスタンスの *system-id*、 *cluster-id* 、および展開の *app-name*、 *cluster-name* に同じ値を使用することをお勧めします。

## エンドポイント インスタンス認識の構成

ローカル ラックとリモート ラックごとに 2 つの インスタンスのみを構成でき、対応するエンドポイントをインスタンス化できます。

ローカルインスタンスIDは、ラックが冗長かどうかに関係なく、ローカルラックのIDです。

### ローカル インスタンス ID の構成

ローカル インスタンスは、 local-instance コマンドを使用して構成されます。

```
local-instance instance 1
```

エンドポイント構成は、各一意のインスタンス ID で指定されたインスタンスの下にある必要があります。

### エンドポイントの構成例

次の構成例を参照してください。

（注） 次の例では、 *instance-id* "**1**" がローカ ルインスタンス ID であり、その下に構成されたエンドポイントはローカル サイトに属しています。

必要に応じて、リモート ラック インスタンス *ID* 「**2**」をラックに属するエンドポイントに構成できます。

```
instance instance-id 1
 endpoint li
  replicas 1
  nodes    2
  vip-ip 209.165.201.6
  vip-ip 209.165.201.13
 exit
 endpoint gtp
  replicas 1
  nodes    2
  retransmission timeout 5 max-retry 4
  vip-ip 209.165.201.6
  vip-ip 209.165.201.4
  interface s5
   echo interval          60
   echo retransmission-timeout 5
   echo max-retransmissions 4
  exit
  interface s2b
   echo interval 60
   echo retransmission-timeout 5
   echo max-retransmissions 4
  exit
 exit
exit
instance instance-id 2
 endpoint li
  replicas 1
  nodes    2
  vip-ip 209.165.201.6
  vip-ip 209.165.201.13
 exit
exit
endpoint gtp
  replicas 1
  nodes    2
  retransmission timeout 5 max-retry 4
  vip-ip 209.165.201.6
  vip-ip 209.165.201.5
  interface s5
   echo interval 60
   echo retransmission-timeout 5
   echo max-retransmissions 4
  exit
  interface s2b
```

```
   echo interval 60
   echo retransmission-timeout 5
   echo max-retransmissions 4
  exit
 exit
exit
```

## プロファイル SMF インスタンス認識の構成

ローカルおよびリモート インスタンスに対応する PGW FQDN のインスタンスを追加します。

**例**

次に、構成例を示します。

（注） 次の例では、 *instance-id* 「**1**」がローカル インスタンス ID であり、その下に構成された SMF プロファイルがローカル ラックに属しています。

必要に応じて、リモート ラック インスタンス *ID* 「**2**」をラック間に属する FQDN に構成できます。

```
profile smf smf1
locality LOC1
allowed-nssai [ slice1 ]
instances 1 fqdn cisco.com.apn.epc.mnc456.mcc123
instances 2 fqdn cisco.com.apn.epc.mnc567.mcc123
```

# ダイナミック ルーティング

ボーダー ゲートウェイ プロトコル（BGP）では、自律システム（AS）間にループフリーのドメイン間ルーティングを作成可能です。AS は、単一の技術管理に基づくルータのまとまりです。ルータは、外部ゲートウェイ プロトコルを使用して AS の外部にパケットをルーティングできます。BGP を使用したダイナミック ルーティング機能を使用すると、優先順位とルートとともに IP アドレスにサービスを提供する代替ローカル アドレスを持つ BGP ルータのネクストホップ属性を構成できます。App-Infra BGP スピーカー ポッドは、BGP を使用してポッド ルートをサービス VIP にアドバタイズすることにより、トラフィックのダイナミック ルーティングを可能にします。

この機能は、次の機能をサポートしています。

- BGP を使用したダイナミック ルーティングによる着信トラフィックのサービス IP アドレスのアドバタイズ。
- 発信トラフィックのルートの学習。
- BGP ポッド フェールオーバーの処理。
- プロトコル ポッド フェールオーバーの処理。
- BGP スピーカーの統計と KPI。

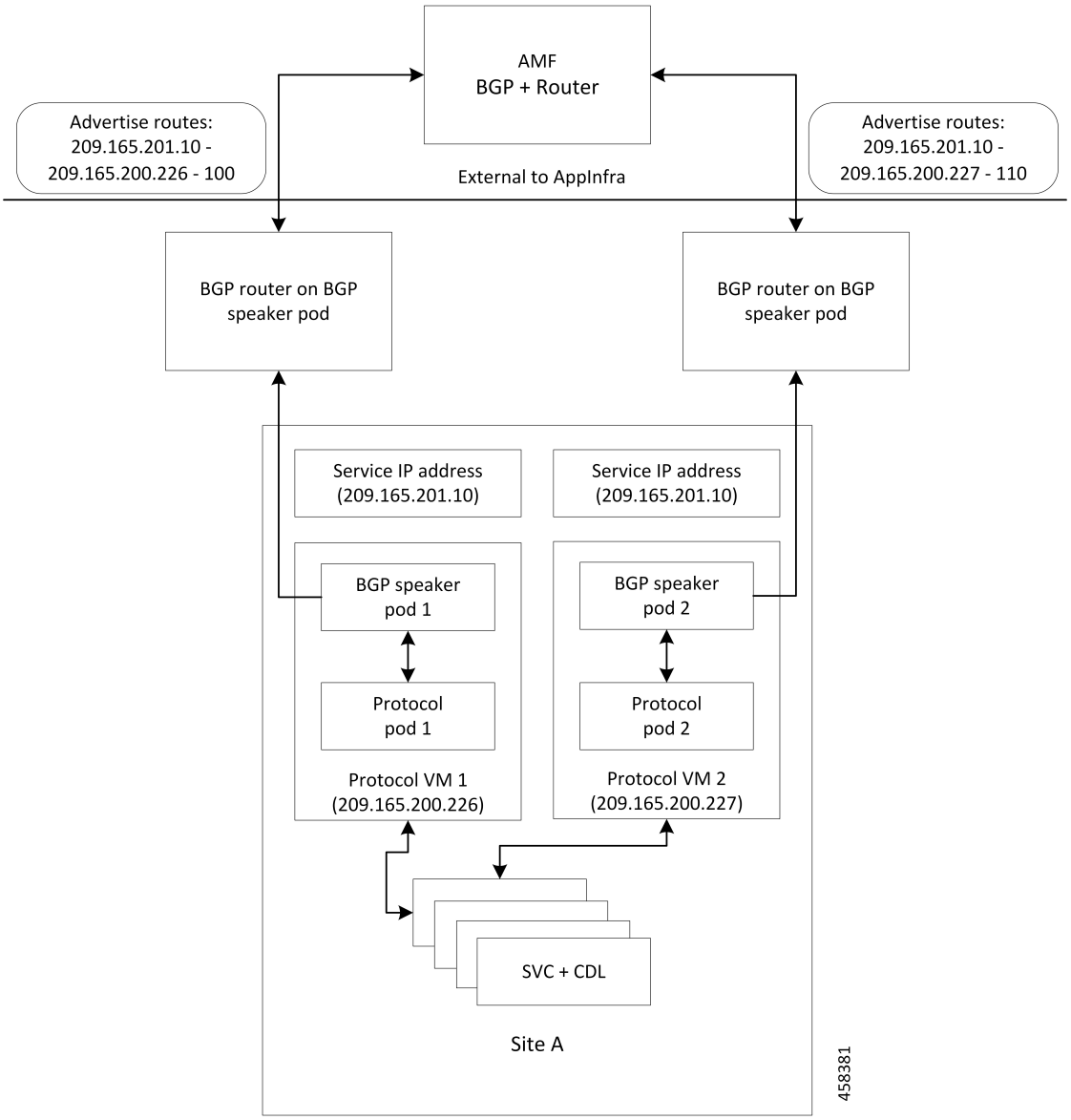
- BGP スピーカーをデバッグするためのログ メッセージ。
- BGP スピーカー ポッドを有効または無効にします。
- BGP を構成するための新しい CLI コマンド。

### 着信トラフィック

BGP は、ポート 179 でトランスポートプロトコルとして TCP を使用します。2 台の BGP ルータは相互に TCP 接続を形成し、各ルータはピアルータです。ピアルータはメッセージを交換し、接続パラメータを開いて確認します。

BGP スピーカーは、アクティブ/スタンバイ モードで着信トラフィックのプロトコル ポッドのルーティング情報を公開します。次の図を例として使用して、ダイナミック ルーティングの機能を理解してください。pod1 と pod2 の 2 つのプロトコル ポッドがあります。pod1 はアクティブで、pod2 はスタンバイ モードになっています。サービス IP アドレス 209.165.200.225 は、209.165.200.226 と 209.165.200.227 の両方のノードで構成されています。 pod1 はホスト 209.165.200.226 で、pod2 はホスト 209.165.200.227 で実行されています。ホスト IP アドレスはポッドサービスを公開します。BGP スピーカーは、ルート 209.165.200.225、209.165.200.226 および 209.165.200.227 に公開します。また、ポッドの優先順位を決定するために、プリファレンス値 110 と 100 を公開します。

図 *248 :* アクティブ/スタンバイ トポロジでの着信トラフィックのダイナミック ルーティング




高可用性を実現するため、各クラスタにはアクティブ/スタンバイ トポロジを備えた2つのBGP スピーカー ポッドがあります。カーネルルートの変更は、プロトコル ポッドが実行されているホスト/ネットワーク レベルで実行されます。

## MED 値

ローカル プリファレンスはIGP ネイバーでのみ使用され、MED 属性はEGP ネイバーでのみ使用されます。BGP では、より低い MED 値が推奨されます。

表 *435 : MED* 値

| ボンディングインターフェイスがアクティブ | VIP の存在 | MED 値 | Local Preference |
|---|---|---|---|
| はい | はい | 1210 | 2220 |
| はい | 非対応 | 1220 | 2210 |
| 非対応 | はい | 1215 | 2215 |
| いいえ | 非対応 | 1225 | 2205 |

### BGP スピーカー ポッドのブートストラップ

次の一連の手順で、BGP スピーカー ポッドをセットアップします。

1. BGP スピーカー ポッドは、ポート 179 でトランスポート プロトコルとして TCP を使用し、これらのポッドは、Ops Center CLI で構成された AS 番号を使用します。
2. Topology Manager を登録します。
3. リーダー ポッドを選択します。アクティブなスピーカー ポッドがデフォルトの選択肢です。
4. Ops Center CLI によって提供されるすべての BGP ピアへの接続を確立します。
5. ETCD から既存のすべてのルートを公開します。
6. CLI 構成を使用して、ルーティングのインポート ポリシーを構成します。
7. 両方のスピーカー ポッドで gRPC ストリーム サーバを開始します。
8. キャッシュ ポッドと同様に、各名前空間で 2 つの BGP スピーカー ポッドを実行する必要があります。

## 外部ネットワーク障害

NF インスタンスの起動により、BGP スピーカー K8s ポッドは、優先順位とルートとともに IP アドレスにサービスを提供するための代替ローカル アドレスを使用して、BGP ルータのネクストホップ属性を構成します。

地理的 HA がトリガされると、宛先サービスの IP アドレス、パスの接続性、および優先度の値に基づいてパスが選択されます。

**Note** ポッド間の透過的な移行により、サブスクライバ セッションは影響を受けません。

## Geo スイッチオーバー

SMF は、サービス IP アドレスを、対応するピア K8s クラスタ、コロケーションされたラック、または地理的に配置されたラックに透過的に移行することで、Geo スイッチオーバーを実現します。NF の起動時に、すべての K8s クラスタ名前空間はネクストホップの BGP ルータに登録し、サービス IP アドレスとローカル IP アドレス、優先順位とルート修飾値をアドバタイズします。

各論理 NF は、NRF または DNS に対する個別の NF インスタンス、個別の構成、および名前空間の個別 LCM を公開する。

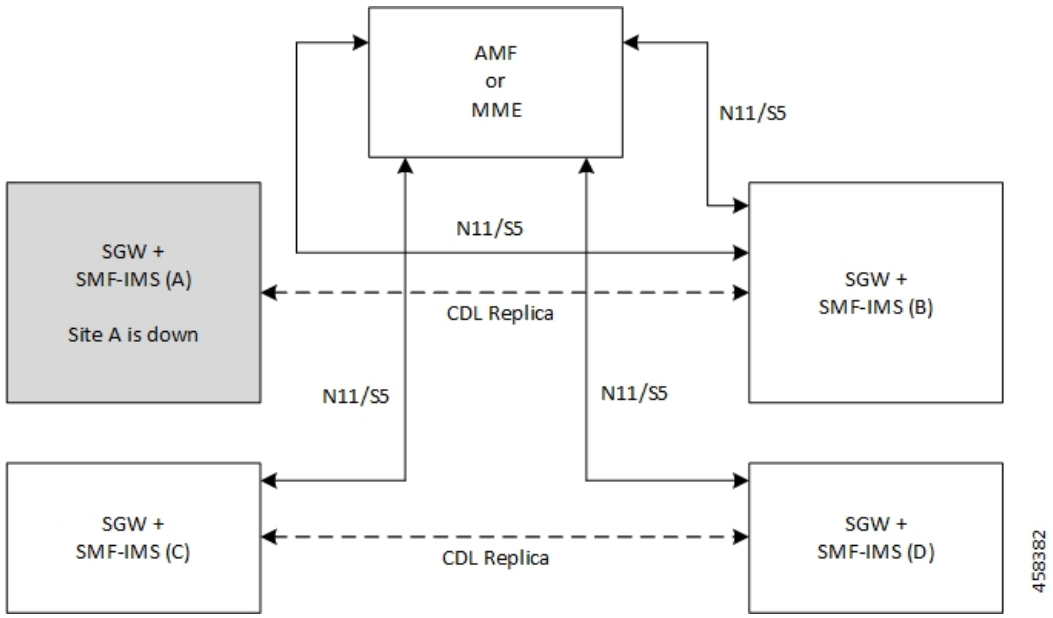
## 内部ネットワーク障害

マスター ノードとのサーバ通信の中断、BFD の障害、または K8s ポッドのネットワークの問題が原因で、機能している K8s クラスタに内部ネットワーク障害が発生した場合、K8s の稼働状態の障害に基づく K8s の依存関係チェックにより、Geo HA がトリガされます。

次の図に示した例では、AMF または MME が透過的に代替ラック サーバの使用を開始しています。N11/S11/S5 および N4/Sxa サービスアドレスはサイト B のラック B に移行されます。システムはラック A のラック B からのシグナリングを継続します。ラック B では、既存のサブスクライバ セッションに影響を与えることなくセッションが続行されます。

**Note** UE が再接続する前にコールが終了される状態によっては、接続中のコールがほとんど失敗する場合があります。

***Figure 249:*** 内部ネットワーク障害に対する ***Geo HA***



# ローカル スイッチオーバー

SMF は、同じデータセンター内に配置されたピア K8s クラスタまたはラックにサービス IP アドレスを透過的に移行することで、Geo スイッチオーバーを実現します。NF の起動時に、すべての K8s クラスタ名前空間はネクストホップの BGP ルータに登録し、サービス IP アドレスとローカル IP アドレス、優先順位とルート修飾値をアドバタイズします。各論理 NF は、NRF または DNS に対する個別の NF インスタンス、個別の構成、および名前空間の個別 LCM を公開する。

# リカバリとフェールバック

シームレスなフェールオーバーとフェールバックのために、UE セッションと対応するサービス IP アドレスがグループ化されます。

次のシナリオでは、UE セッションのシームレスなフェールオーバーとフェールバックのメカニズムについて説明します。

- **通常**：UE セッション セットは、最初のラックから作成、更新、または削除され、2 番目のラックに複製されます。
- **失敗**：UE セッション セットは、2 番目のラックから作成、更新、または削除されますが、可用性が低いため、最初のラックには複製されません。
- **リカバリ**：すべての UE セッション データをリカバリするために、最初のラックの CDL が 2 番目のラックの CDL と自動同期を実行します。リカバリ中は、2 番目のラックはセッション セットからのトラフィックを処理し続けます。

# コール フロー

ここでは、BGP を使用したダイナミック ルーティングの主要なコール フローについて説明します。

## アクティブ/スタンバイ モードでの着信トラフィックのルートの公開

ここでは、アクティブ/スタンバイ モードでのコントロール プレーンとデータ プレーンのコール フローについて説明します。

### コントロール プレーンのコール フロー

ここでは、コントロール プレーンのコール フローについて説明します。

***Figure 250:*** コントロール プレーンのコール フロー

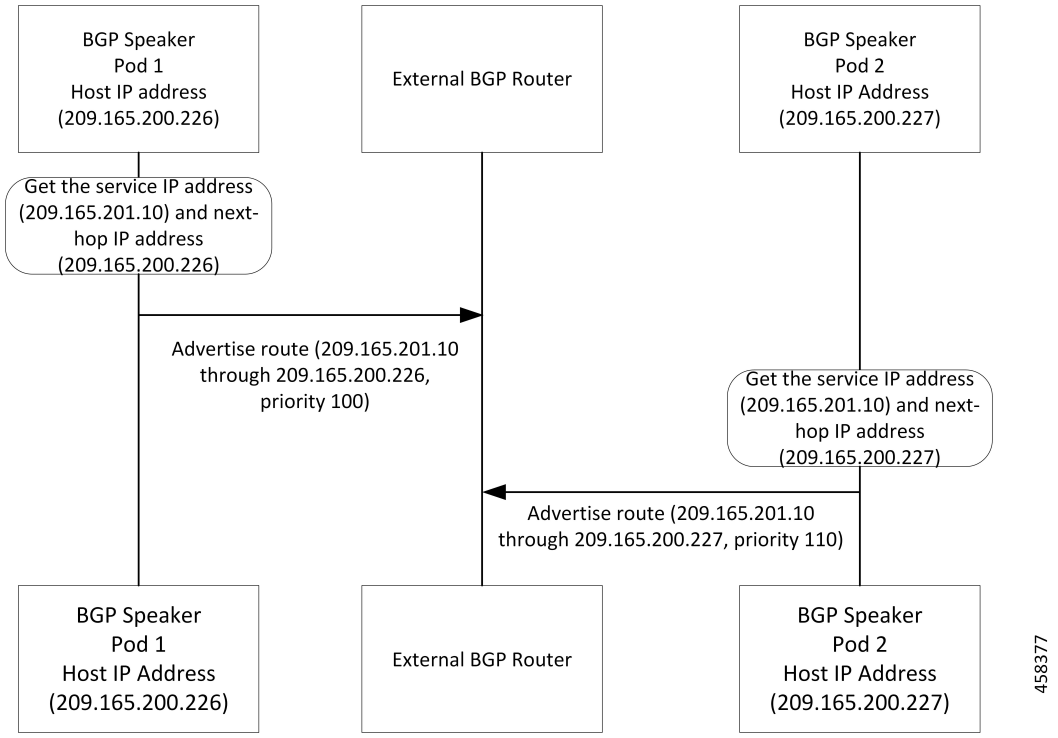



***Table 436:*** コントロール プレーンのコール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | BGP スピーカーポッドが起動し、サービス IP アドレス、ネクストホップ IP アドレス（ホスト IP または loopbackEth）、および BGP スピーカー ポッドのインスタンス ID を取得します。<br>ポッド サービスは、ホスト IP または構成された loopbackEth を介して公開されます。<br>NF インスタンス ID は、ルートの優先順位やプリファレンスを検索するために使用されます。 |
| 2 | BGP スピーカー ポッドは、Ops Center から vip-ip（サービス IP アドレス）を取得してルートをアドバタイズします。 |

## データ プレーンのコール フロー

ここでは、データ プレーンのコール フローについて説明します。

***Figure 251:*** データ プレーンのコール フロー

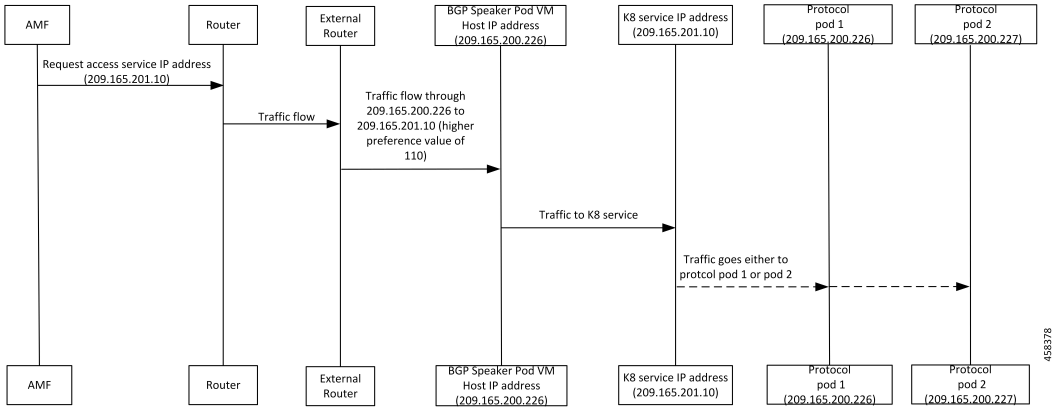



***Table 437:*** データ プレーンのコール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | サービス IP アドレスの AMF 要求。要求は、複数の外部ルータを介して、接続された最も近いルータに送信されます。次に、ルータは優先順位が最も高いBGP スピーカーポッドに要求を送信します。 |
| 2 | BGP ルータは、プリファレンス値に基づいてデータ プレーン フローを設定します。前述のコール フローの例では、ルータは、プリファレンス値がより高いため、サービス要求をホスト 209.165.200.226 を介してポッド 1 にルーティングします。<br>ホスト（209.165.200.226）からのトラフィックは K8 サービス IP アドレス（209.165.201.10）に転送され、プロトコルポッド 1（209.165.200.226）またはポッド 2（209.165.200.227）に送信されます。 |

## シングル プロトコル ポッド障害コール フロー

ここでは、シングル プロトコル ポッド障害コール フローについて説明します。

***Figure 252:*** シングル プロトコル ポッド障害コール フロー

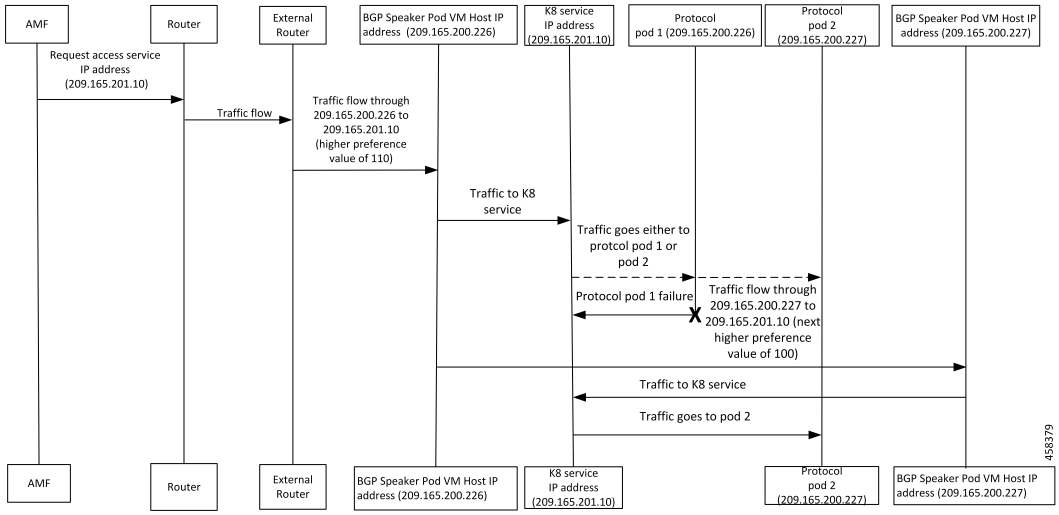


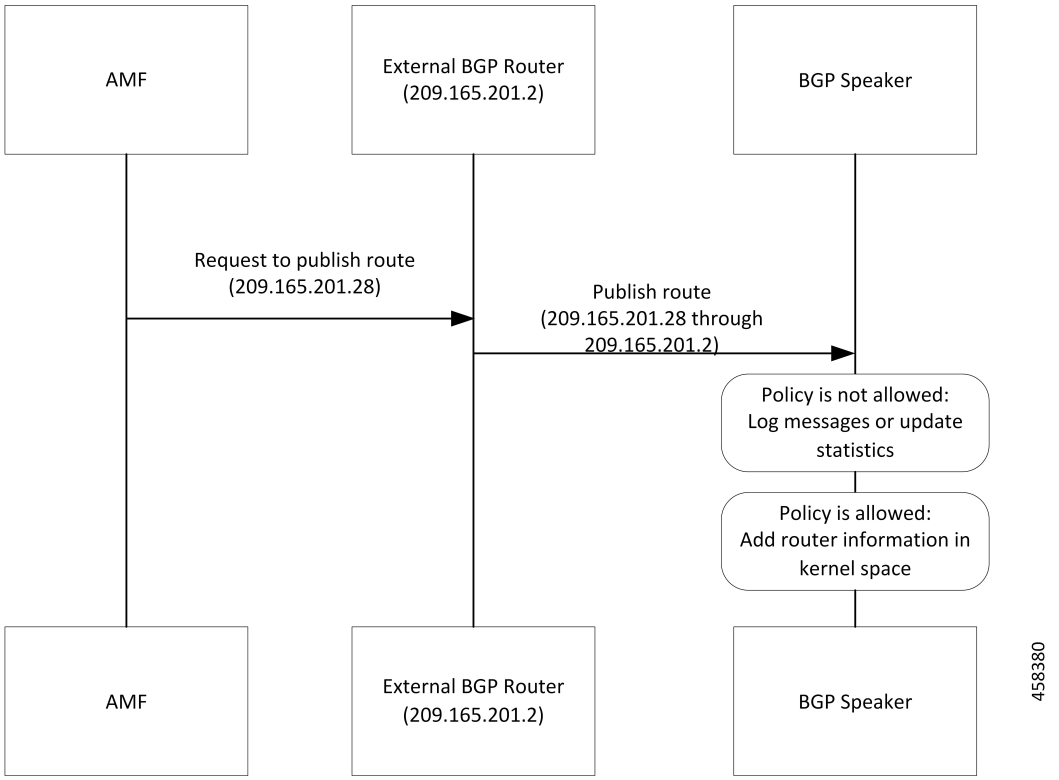

***Table 438:*** シングル プロトコル ポッド障害コール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | サービス IP アドレスの AMF 要求。要求は、次に高いプリファレンス値に基づいて、複数の外部ルータを介して、最も近く接続された BGP ルータに送信されます。 |
| 2 | BGP ルータは、プリファレンス値に基づいてデータ プレーン フローを設定します。最も高いプリファレンス値を持つポッドが使用できない場合、要求は K8 サービス ポッドを介して次に高いプリファレンス値を持つポッドにルーティングされます。<br>前述のコール フローの図に示した例では、IP アドレスの 209.165.200.227 を持つポッド 2 が、より高いプリファレンス値のために要求を処理します。 |

## 発信トラフィック コール フローのルートの学習

ここでは、発信トラフィックのルートの学習コール フローについて説明します。

***Figure 253:*** 発信トラフィックのルートの学習コール フロー




AMF などのシステムが外部BGPルートにルートをアドバタイズします。次に、外部BGPルータがBGP を介してそのサービスのルートをアドバタイズします。

***Table 439:*** 発信トラフィックのルートの学習コール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | BGP スピーカーがルーティング情報を受信します。 |
| 2 | BGP プロトコルを使用してルートを学習します。 |
| 3 | 構成ポリシーに基づいて、システムはルーティング情報を確認するか、無視します。 |
| 4 | ポリシーが許可されていない場合、システムはメッセージをログに記録し、統計情報を更新します。 |
| 5 | プロトコル ポッドは、netlink go API を介してホスト上のカーネル スペースでルートを構成します。 |

# BGP を使用したダイナミック ルーティングの構成

ここでは、BGP を使用してダイナミック ルーティングを構成する方法について説明します。

### AS と BGP ルータの IP アドレスの構成

BGP ルータの AS と IP アドレスを構成するには、次のコマンドを使用します。

```
config
   router bgp local_as_number
   exit
exit
```

注：

- **router bgp** *local_as_number*：BGP ルータの AS の ID 番号を指定します。

### BGP サービス リスニング IP アドレスの構成

BGP サービス リスニング IP アドレスを構成するには、次のコマンドを使用します。

```
config
   router bgp local_as_number
      interface interface_name
   exit
exit
```

注：

- **router bgp** *local_as_number*：BGP ルータの AS の ID 番号を指定します。
- **interface** *interface_name*：インターフェイスの名前を指定します。

### BGP ネイバーの構成

BGP ネイバーを構成するには、次のコマンドを使用します。

```
config
   router bgp local_as_number
      interface interface_name
      neighbor neighbor_ip_address remote-as as_number
   exit
exit
```

注：

- **router bgp** *local_as_number*：BGP ルータの AS の ID 番号を指定します。
- **interface** *interface_name*：インターフェイスの名前を指定します。
- **neighbor** *neighbor_ip_address*：ネイバー BGP ルータの IP アドレスを指定します。
- **remote-as** *as_number*：AS の ID 番号を指定します。

### ボンディング インターフェイスの構成

インターフェイスに関連するボンディングインターフェイスを構成するには、次のコマンドを使用します。

```
config
  router bgp local_as_number
    interface interface_name
    bondingInterface interface_name
  exit
exit
```

注：

- **router bgp** *local_as_number*：BGP ルータの AS の ID 番号を指定します。
- **interface** *interface_name*：インターフェイスの名前を指定します。
- **bondingInterface** *interface_name*：インターフェイスに関連するボンディングインターフェイスを指定します。ボンディング インターフェイスがアクティブである場合、BGP は、より低い MED 値を提供することで、インターフェイス サービスに高いプリファレンスを与えます。

### 学習デフォルト ルートの構成

システム上に特定のルートを構成し、すべてのルートをサポートする必要があるユーザーは、**learnDefaultRoute** を **true** に設定する必要があります。

**Note** この設定は任意です。

デフォルト ルートの学習を構成するには、次のコマンドを使用します。

```
config
  router bgp local_as_number
    learnDefaultRoute true/false
  exit
exit
```

注：

- **router bgp** *local_as_number*：BGP ルータの AS の ID 番号を指定します。
- **learnDefaultRoute** *true/false*： **learnDefaultRoute** パラメータを有効または無効にするオプションを指定します。true に設定すると、BGP はデフォルト ルートを学習し、カーネルスペースに追加します。デフォルトは False です。

### BGP ポートの構成

BGP サービスのポート番号を構成するには、次のコマンドを使用します。

```
config
  router bgp local_as_number
    loopbackPort port_number
  exit
exit
```

注：

- **router bgp** *local_as_number*：BGP ルータの AS の ID 番号を指定します。
- **loopbackPort** *port_number*：BGP サービスのポート番号を指定します。デフォルト値は 179 です。

### ポリシーの追加

BGP スピーカー ポッドは、ネイバーから多くのルート情報を学習します。ただし、発信トラフィックのサポートに使用されるのはそのうちのごく一部です。これは、 SMF が 外部の AMF/PCF に情報を送信している場合、出力トラフィックの処理にのみ必要です。ルートは、BGP スピーカーでインポート ポリシーを構成することでフィルタリングされ、学習したルートをプロトコルポッドに送信するために使用されます。

ポリシー追加用のサンプル CLI コードと、各パラメータに対応する説明を以下に示します。

```
$bgp policy <policy_Name> ip-prefix 209.165.200.225 subnet 16 masklength-range 21..24
as-path-set "^65100"
```

***Table 440:*** インポート ポリシーのパラメータ

| 要素 | 説明 | 例 | オプション |
|---|---|---|---|
| **as-path-set** | AS パス値 | “^65100” | 対応 |
| **ip-prefix** | プレフィックス値 | “209.165.200.225/16” | 対応 |
| **masklength-range** | 長さの範囲 | “21..24” | はい |
| **interface** | 送信元 IP として設定するインターフェイス（デフォルトは VM IP） | eth0 | 対応 |
| **gateWay** | 着信ルートのゲートウェイを変更します | 209.165.201.30 | 対応 |
| **modifySourceIp** | 着信ルートの送信元IPの変更<br>デフォルト値は False です。 | true | はい |
| **isStaticRoute** | カーネルルートにスタティック IP アドレスを追加するフラグ<br>デフォルト値は False です。 | true | はい |

# BGP スピーカーの構成

この構成は、展開内の BGP スピーカーポッドの数を制御します。BGP スピーカーは、両方のラックからの着信トラフィックのサービス IP 情報をアドバタイズします。

（注）
- BGP ピアリングには、BGP スピーカーポッドで非結合インターフェイスを使用します。
- Proto ノードごとの BGP ピアリングは、2 つの BGP ルータ/リーフのみでサポートされます。2 つの Proto ノードを考慮すると、最大 4 つの BGP ネイバーシップを設定できます。

```
instance instance-id  instance_id endpoint bgpspeaker interface { bgp |
bfd } internal base-port start base_port_number
```

```
config
instance instance-id instance_id
 endpoint bgpspeaker
   replicas replica_id
   nodes node_id
   interface bgp
     internal base-port start base_port_number
   exit
   interface bfd
     internal base-port start base_port_number
  exit
exit
```

注：

- **instance instance-id** *instance_id*：GR インスタンス ID を指定します。
- *base_port_number*：論理 NF が構成されている場合にのみ、ポート範囲を指定します。この範囲は、展開によって異なります。

例

次に、設定例を示します。

```
instance instance-id 1
endpoint bgpspeaker
   replicas 1
   nodes    2
   interface bgp
     internal base-port start {24000}
   exit
   interface bfd
     internal base-port start {25000}
 exit
```

# モニタリングおよびトラブルシューティング

この項では、BGP を使用したダイナミック ルーティング機能でサポートされている show コマンドについて説明します。

### show bgp-kernel-route

BGP ルータのカーネル レベルのすべてのルートを表示するには、 **show bgp-kernel-route** コマンドを使用します。

以下の構成は、**show bgp-kernel-route** コマンドの出力例です。

```
kernel-route

-----bgpspeaker-pod-1 ----

 DestinationIP       SourceIP        Gateway

 209.165.200.235     209.165.200.239   209.165.200.239

-----bgpspeaker-pod-2 ----

 DestinationIP       SourceIP        Gateway

 209.165.200.235     209.165.200.229   209.165.200.244
```

### show bgp-global

すべての BGP グローバル コンフィギュレーションを表示するには、 **show bgp-global** コマンドを使用します。

以下の構成は、**show bgp-global** コマンドの出力例です。

```
global-details

-----bgpspeaker-pod-1 ----
AS:        65000
Router-ID: 209.165.200.239
Listening Port: 179, Addresses: 209.165.200.239
AS:        65000
Router-ID: 209.165.200.232
Listening Port: 179, Addresses: 209.165.200.232

-----bgpspeaker-pod-2 ----
AS:        65000
Router-ID: 209.165.200.235
Listening Port: 179, Addresses: 209.165.200.235
AS:        65000
Router-ID: 209.165.200.246
Listening Port: 179, Addresses: 209.165.200.246
```

### show bgp-neighbors

BGP ルータのすべての BGP ネイバーを表示するには、**show bgp-neighbors** コマンドを使用します。

以下の構成は、**show bgp-neighbors** コマンドの出力例です。

```
neighbor-details

-----bgpspeaker-pod-2 ----
Peer              AS  Up/Down State       |#Received  Accepted
209.165.200.244 60000 00:34:20 Establ      |       10        10
Peer            AS  Up/Down State       |#Received  Accepted
209.165.200.250 60000 00:34:16 Establ      |        3         3

-----bgpspeaker-pod-1 ----
```

```
Peer             AS  Up/Down State       |#Received  Accepted
209.165.200.244 60000 00:33:53 Establ      |       10        10
Peer           AS  Up/Down State       |#Received  Accepted
209.165.200.250 60000 00:33:53 Establ      |        3         3
```

### show bgp-neighbors *ip*

BGP ルータのネイバーの詳細を表示するには、**show bgp-neighbors** *ip* コマンドを使用します。

以下の構成は、**show bgp-neighbors** *ip* コマンドの出力例です。

```
neighbor-details

-----bgpspeaker-pod-1 ----
BGP neighbor is 209.165.200.244, remote AS 60000
  BGP version 4, remote router ID 209.165.200.244
  BGP state = ESTABLISHED, up for 00:34:50
  BGP OutQ = 0, Flops = 0
  Hold time is 90, keepalive interval is 30 seconds
  Configured hold time is 90, keepalive interval is 30 seconds

  Neighbor capabilities:
    multiprotocol:
        ipv4-unicast:   advertised and received
    route-refresh:      advertised and received
    extended-nexthop:   advertised
        Local:  nlri: ipv4-unicast, nexthop: ipv6
    4-octet-as: advertised and received
  Message statistics:
                         Sent       Rcvd
    Opens:                  1          1
    Notifications:          0          0
    Updates:                1          2
    Keepalives:            70         70
    Route Refresh:          0          0
    Discarded:              0          0
    Total:                 72         73
  Route statistics:
    Advertised:             0
    Received:              10
    Accepted:              10

-----bgpspeaker-pod-2 ----
BGP neighbor is 209.165.200.244, remote AS 60000
  BGP version 4, remote router ID 209.165.200.244
  BGP state = ESTABLISHED, up for 00:35:17
  BGP OutQ = 0, Flops = 0
  Hold time is 90, keepalive interval is 30 seconds
  Configured hold time is 90, keepalive interval is 30 seconds

  Neighbor capabilities:
    multiprotocol:
        ipv4-unicast:   advertised and received
    route-refresh:      advertised and received
    extended-nexthop:   advertised
        Local:  nlri: ipv4-unicast, nexthop: ipv6
    4-octet-as: advertised and received
  Message statistics:
                         Sent       Rcvd
    Opens:                  1          1
    Notifications:          0          0
    Updates:                1          2
    Keepalives:            71         71
    Route Refresh:          0          0
```

```
    Discarded:              0          0
    Total:                 73         74
  Route statistics:
    Advertised:             0
    Received:              10
    Accepted:              10
```

### show bgp-route-summary

BGP ルータのすべてのルートの詳細を表示するには、**show bgp-route-summary** コマンドを使用します。

以下の構成は、**show bgp-route-summary** コマンドの出力例です。

```
route-details

-----bgpspeaker-pod-1 ----
Table afi:AFI_IP safi:SAFI_UNICAST
Destination: 5, Path: 5

-----bgpspeaker-pod-2 ----
Table afi:AFI_IP safi:SAFI_UNICAST
Destination: 5, Path: 5
```

### show bgp-routes

BGP ルータのすべてのルートを表示するには、**show bgp-routes** コマンドを使用します。

以下の構成は、**show bgp-routes** コマンドの出力例です。

```
bgp-route

-----bgpspeaker-pod-1 ----
   Network              Next Hop             AS_PATH       Age        Attrs
*> 209.165.200.235/24   209.165.200.250      60000         00:36:39   [{Origin: i} {Med:
 0}]
*> 209.165.200.227/32   209.165.200.232                     00:36:44   [{Origin: e}
{LocalPref: 220} {Med: 3220}]
*> 209.165.200.247/24   209.165.200.250      60000         00:36:39   [{Origin: i} {Med:
 0}]
*> 209.165.200.251/24   209.165.200.250      60000         00:36:39   [{Origin: i} {Med:
 0}]
*> 209.165.200.252/32   209.165.200.232                     00:36:44   [{Origin: e}
{LocalPref: 220} {Med: 3220}]

-----bgpspeaker-pod-2 ----
   Network              Next Hop             AS_PATH        Age        Attrs
*> 209.165.200.235/24   209.165.200.250      60000          00:37:02   [{Origin: i} {Med:
 0}]
*> 209.165.200.227/32   209.165.200.246                      00:37:11   [{Origin: e}
{LocalPref: 220} {Med: 3220}]
*> 209.165.200.228/24   209.165.200.234      60000          00:37:02   [{Origin: i} {Med:
 0}]
*> 209.165.200.229/24   209.165.200.234      60000          00:37:02   [{Origin: i} {Med:
 0}]
*> 209.165.200.230/32   209.165.200.246                      00:37:11   [{Origin: e}
{LocalPref: 220} {Med: 3220}]
```

### KPI

以下の KPI は、この機能でサポートされます。

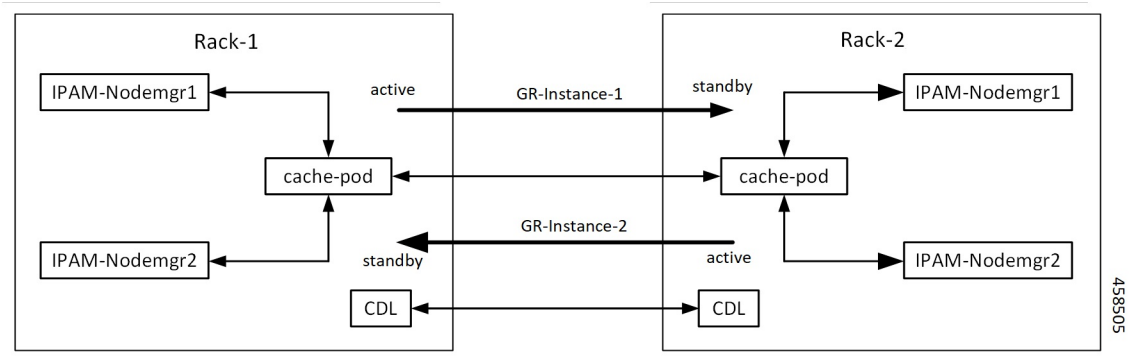
*Table 441: BGP* を使用したダイナミック ルーティングの統計情報

| KPI 名 | タイプ | 説明/式 | ラベル |
|---|---|---|---|
| bgp_outgoing_route request_total | カウンタ | 受信ルートの総数。 | local_pref、med、next_hope、service_IP |
| bgp_outgoing_failed route request_total | カウンタ | 障害の発生した受信ルートの総数。 | local_pref、med、next_hope、service_IP |
| bgp_incoming_route request_total | カウンタ | 着信ルートの総数。 | interface、next_hope、service_IP |
| bgp_incoming_failedroute request_total | カウンタ | 障害の発生した着信ルートの総数。 | interface、next_hope、service_IP |
| bgp_peers_total | カウンタ | 追加されたピアの総数。 | peer_ip、as_path |
| bgp_failed_peertotal | カウンタ | 障害が発生したピアの総数。 | peer_ip、as_path、error |

# IPAM

ここでは、ラック レベルでの IP アドレス管理（IPAM）について説明します。

**図 *254 : IPAM***




UPF 登録時、アクティブな IPAM インスタンスは、各 DNN の UPF ごとに 4 つのアドレス範囲を予約します。

- 範囲 1：アクティブ クラスタ、nodemgr-1
- 範囲 2：アクティブ クラスタ、nodemgr-2
- 範囲 3：スタンバイ クラスタ、nomgr-1

- 範囲-4：スタンバイ クラスタ、nodemgr-2

通常の動作中、Rack-1 は GR-instance-1 で起動するサブスクライバの UPF 登録/リリース、アドレス割り当て/リリースを処理します。

Rack-2 がダウンすると、Rack-1 が GR-Instance-2 のロール変更トリガを取得します。

- Rack-1 の IPAM は、local-cache-pod（すでに同期されている）から GR-Instance-2 のコンテンツを復元します。
- Rack-1 の IPAM は、GR-Instance-1 の処理に加えて、復元されたコンテンツを使用して GR-Instance-2 で起動するサブスクライバの UPF-Register/Release および address-allocate/release を処理します。

各 IPAM プールは、次のように GR インスタンスに関連付けられます。

- プール名は、すべての インスタンスで一意です。
- アドレス範囲は、VRF 内およびすべてのインスタンスにわたって一意です。

特定の インスタンスのアクティブとスタンバイの両方の SMF クラスタで、同じプールを構成する必要があります。

アドレス割り当て中に、アクティブ インスタンスは UPF 用に予約されたアドレス範囲から空き IP を割り当てます。

新しいアドレス範囲を使用できない場合は、スタンバイのアドレス範囲の所有権を現在のアクティブ インスタンスに変更し、そこからアドレス範囲の割り当てを続行します。

## IPAM の構成

次のセクションでは、IPAM の構成例を示します。

### SMF-1 の例

SMF-1 の構成例を次に示します。

```
ipam
 instance 1
  address-pool pool-1
  vrf-name ISP
   tags
   dnn dnn-1
  exit
  ipv4
    address-range 209.165.201.1 209.165.201.31
 exit
instance 2
 address-pool pool-2
  vrf-name ISP
  tags
   dnn dnn-2
  exit
  ipv4
    address-range 209.165.202.129 209.165.202.159
```

```
 exit
exit
```

### SMF-2 の例

次に、 SMF-2の構成例を示します。

```
ipam
 instance 1
 address-pool pool-1
  vrf-name ISP
  tags
   dnn dnn-1
  exit
  ipv4
    address-range 209.165.201.1 209.165.201.31
 exit
 instance 2
 address-pool pool-2
  vrf-name ISP
   tags
   dnn dnn-2
  exit
  ipv4
    address-range 209.165.202.129 209.165.202.159
 exit
exit
```

# Geo レプリケーション

Geo レプリケーションはラック間通信で、ラック内のPOD、VIP、またはBFDのモニタリングで使用されます。地理的冗長性は、次で構成されます。

- ラックごとに Geo ポッドの 2 つのインスタンスが実行されていること。
- 2 つの Geo ポッドがアクティブ/スタンバイモードで機能する。
- 各 Geo ポッド インスタンスは、異なる Proto ノードまたは VM で生成されます。
- Proto ノードまたは VIP を持つ VM で実行されている Geo ポッドがアクティブな Geo ポッドです。
- アクティブな Geo ポッドが再起動した場合、VIP は他の Proto ノードまたは VM に切り替えられ、他の Proto ノードまたは VM で実行されているスタンバイ Geo ポッドがアクティブになります。
- 地理ポッドは、ホスト ネットワーキング モードを使用します（UDP プロキシと同様）。
- Geo ポッドでは、次の 2 つの VIP を使用します。
  - **内部**：POD 間通信用の VIP（ラック内）
  - **外部**：ラック間 Geo ポッド通信の VIP

    L2 サブネット上の Proto ノードでのみ構成されます。ラック間の通信に使用されます。このノードは他のラックに外部接続されています。

- Logical-NF-InstanceID は、GR-Pair の両方の SMF で同じに設定する必要があります。
- KeepAliveD モニタリングの場合：
  - 地理ポッドは、15000+（Logical-NF-InstanceID * 32）+4 としてベース ポートを使用します。

    Geo ポッドのベース ポートは、BGP スピーカーのポッド ポートとは異なる必要があります。

    - デフォルト ポート（論理 SMFなし）：15004
    - Logical-nf-instance-id が 1 に構成され、ポートが 15036 に構成された論理 SMF の場合
  - UDP プロキシ ポッドは、ベースポートを 28000+Logical-NF-InstanceID として使用します。
    - デフォルト ポート（論理 SMFなし）：28000
    - Logical-nf-instance-id が 1 に構成され、ポートが 28001 に構成された論理 SMF の場合
  - BGP スピーカー ポッドは、デフォルトのベース ポートを 20000+(Logical-NF-InstanceID * 32)+4 として使用します。
    - デフォルト ポート（論理 SMFなし）：20004
    - 論理的 SMF の場合、logical-nf-instance-id が 1 に構成され、ポートが 20036 に設定される

（注） ETCD およびキャッシュ ポッド データのみがスタンバイ ラックに複製されます。

## ETCD/CachePod レプリケーションの構成

エンドポイントは、インスタンス下で構成する必要があります。各ラックには2つのGeo冗長ポッドが必要です。また、ETCD/CachePodレプリケーショのために、内部および外部の地理的インターフェイスに VIP を構成する必要があります。

```
instance instance-id  instance_id endpoint geo interface { geo-internal
| geo-external } vip-ip { vip_ip_address } vip-port { vip_port_number }
```

```
config
instance instance-id instance_id
 endpoint geo
  replicas replica_id
  nodes node_id
  internal base-port start base_port_number
  interface geo-internal
```

```
   vip-ip vip_ip_address vip-port vip_port_number
  exit
  interface geo-external
   vip-ip vip_ip_address vip-port vip_port_number
  exit
exit
exit
```

注：

- **instance instance-id** *instance_id*：GR インスタンス ID を指定します。1 つのインスタンス ID はローカル ラック用、もう 1 つは別のラック用です。
- **vip-ip** *vip_ip_address*：内部/外部の地理的インターフェイスの VIP IP アドレスを指定します。
- **vip-port** *vip_port_number*：VIP ポート番号を指定します。
- **internal base-port start** *base_port_number*：論理 NF が構成されている場合にのみ、ポート範囲を指定します。

**例**

次に、設定例を示します。

```
instance instance-id 1
endpoint geo
  replicas 1
  nodes 2
  internal base-port start 25000
  interface geo-internal
   vip-ip 209.165.201.8 vip-port 7001
  exit
  interface geo-external
   vip-ip 209.165.201.8 vip-port 7002
  exit
exit
```

# Geo モニタリング

このセクションでは、Geo モニタリングについて説明します。

## ポッド モニタリング

ラック間セットアップでポッド モニタリングおよびフェールオーバーしきい値を設定するには、次の構成例を使用します。地理ポッドは、構成されたポッド名をモニタします。

```
config
 geomonitor
  podmonitor pods pod_name
   retryCount value
   retryInterval interval_value
   retryFailOverInterval failover_interval
   failedReplicaPercent percent_value
```

```
  exit
 exit
```

注：

- **pods** *pod_name*：モニタされるポッドの名前を指定します。たとえば、Cache-pod、rest-epなどです。
- **retryCount** *value*：ポッドがpingに失敗した場合に再試行する再試行カウンタ値を指定します。その後、ポッドはダウンとしてマークされます。1ー10の範囲の整数である必要があります。
- **retryInterval** *interval_value*：ポッドが ping に成功した場合の再試行間隔をミリ秒単位で指定します。200 ～ 10000 の範囲の整数である必要があります。
- **retryFailOverInterval** *failover_interval*：ポッドが ping に失敗した場合の再試行間隔をミリ秒単位で指定します。200 ～ 10000 の範囲の整数である必要があります。
- **failedReplicaPercent** *percent_value*：ラック間冗長性フェールオーバーがトリガされるまでの、失敗したレプリカのパーセント値を指定します。10～100の範囲の整数である必要があります。

### 設定例

次に、設定例を示します。

```
geomonitor podmonitor pods cache-pod
 retryCount 3
 retryInterval 5
 retryFailOverInterval 1
 failedReplicaPercent 40
exit
```

## リモート クラスタ モニタリング

リモート クラスタ モニタリングは、トラフィックのトラフィックフローが中断されないように、ロール（リモート ラックが **STANDBY_ERROR** 状態の場合はセルフ プライマリになります）を自動修正します。ただし、このロールの自動修正は、特定のロールに対してのみ実行されます。

この機能を構成するには、次の構成例を使用します。

```
config
   geomonitor
      remoteclustermonitor
         retryCount value
         retryInterval interval_value
         end
```

注：

- **retryCount** *value*：現在のラックを **PRIMARY** にする前の再試行回数を指定します。1ー10の範囲の整数で指定する必要があります。デフォルト値は 3 です。

- **retryInterval** *interval_value*：リモートラックのステータスが取得されるまでの再試行間隔をミリ秒単位で指定します。200 ～ 50000 の範囲の整数である必要があります。デフォルト値は 3000 です。

### 設定例

次に構成例を示します。

```
geomonitor remoteclustermonitor
retryCount 3
retryInterval 3000
```

## トラフィック モニタリング

次のコマンドを使用して、トラフィックをモニタします。

```
config
 geomonitor
  trafficMonitor
   thresholdCount value
   thresholdInterval interval_value
  exit
 exit
```

注：

- **thresholdCount** *value*：スタンバイ インスタンスの受信コール数を指定します。0 ー 10000 の範囲の整数である必要があります。デフォルト値は0です。カウンタ値として、UDPプロキシと REST-EP の両方を考慮する必要があります。
- **thresholdInterval** *interval_value*：しきい値カウント値に達するまでの最長時間をミリ秒単位で指定します。100 ー 10000 の範囲の整数である必要があります。デフォルト値は3000です。

### 設定例

次に構成例を示します。

```
geomonitor trafficmonitor
thresholdCount 3
thresholdInterval 3000
```

# Geo 冗長性の強化

Geo冗長性強化アクティビティは、次のようなさまざまなシナリオに起因する複数の問題に対処します。

- ハードウェア障害
- Network failure
- プロセスの失敗

- 異常な状態
- コード ウォークスルー

これらの失敗したシナリオは、Geo レプリケーション ポッドの機能に影響を与え、システムの誤動作を引き起こします。これらの問題に対処するには、Geo レプリケーション ポッドのさまざまな領域を強化する必要があります。

## 機能の仕組み

強化された Geo レプリケーション ポッドの次の領域は、地理的冗長性強化機能の一部です。

- システムは、正常に動作すると、GRPC レプリケーションと管理ストリームを使用できるようになります。
- システムは、すべてのシナリオで両方のインスタンスに正しいロールがあることを保証します。
- システムは、ラック 1 とラック 2 の Geo レプリケーション ポッド間のデータ レプリケーションを同期状態に維持します。
- システムは、チェックサムとチェックポイントデータが両方のラックで常に正しいことを確認して、データの整合性を確保します。
- システムは、レプリケーションデータが同期されなくなったときにユーザーが同期するメカニズムを提供しますが、手動による介入が必要です。

  このコマンドの詳細については、「Geo レプリケーションのプルデータ」セクションを参照してください。
- システムは、Geo レプリケーション ポッド間での Geo VIP 移動が機能に影響しないようにします。
- システムは、依存するプロセスの障害がユーザーの機能に影響を与えないようにするための対策を講じています。

### 制限事項

この機能の既知の制限の一部は次のとおりです：

- **レプリケーション データの損失**：両方のキャッシュ ポッドがパートナー ラックでダウンしているため、スイッチオーバーが発生すると発生する可能性があります。

## OAM サポート

ここでは、この機能の操作、管理、およびメンテナンス サポートについて説明します。

### KPI のサポート

次の一連の統計は、地理的冗長性の強化とセキュア化機能をサポートしています：

1. KPI 名：**geo_replication_finalpull_total**

次の表に、**geo_replication_finalpull_total** KPI の詳細を示します。

| 説明 | 機能 | ラベル名 | 有効な値 |
|---|---|---|---|
| この KPI には、機能メッセージの最終取得時点で存在する Geo レプリケーションの総数が表示されます。 | **geo_replication_finalpull_total**：機能の出力です。 | **MessageType** | これは要求または応答のメッセージタイプです。 |
| | | **TotalTimeTaken** | これは、リクエストの処理にかかった合計時間です。 |
| | | **GRInstanceNumber** | これは、次のリストにある GR インスタンス ID の番号です。<br>• 1<br>• 2<br>• Instance.1<br>• Instance.2 |

# BFD モニタリング

双方向フォワーディング検出（BFD）プロトコルは、迅速なネットワーク障害検出のために BGP とともに使用されます。クラスタ（NF）との BGP ピアリングの間に接続障害が発生するたびに、フェールオーバーがトリガされ、トラフィック障害の影響が最小限に抑えられます。

```
config
  router bgp as
    bfd interval interval min_rx min_rx multiplier multiplier
    loopbackPort loopbackPort loopbackBFDPort loopbackBFDPort
  interface interface_id (BGP on non-bonded interface <-- loopbackEth)
    bondingInterface bondingInterface (leaf6-nic)
    bondingInterface bondingInterface (leaf6-nic)
    neighbor neighbor_ip_address remote-as remote_as fail-over fail_over_type
  exit
  interface interface_id (BGP on non-bonded interface <-- loopbackEth)
    bondingInterface bondingInterface (leaf7-nic)
    bondingInterface bondingInterface (leaf7-nic)
    neighbor bondingInterface remote-as remote_as fail-over fail_over_type
  exit
  policy-name policy_name
   as-path-set as_path_set
   gateWay gateWay_address
   interface interface_id_source
   ip-prefix ip_prefix_value
   isStaticRoute false | true
```

```
   mask-range mask_range
   modifySourceIp false | true
  exit
exit
```

注：

- **bgp** *as*：自律システム（AS）パスセットを指定します。
- **bfd**：BFD 構成を指定します。
  - **interval** *interval* ：BFD 間隔をミリ秒単位で指定します。
  - **min_rx** *min_rx*：BFD の最小 RX をミリ秒単位で指定します。
  - **multiplier** *multiplier*：BFD 間隔の乗数を指定します。
- **interface** *interface_id*：BGP ローカル インターフェイスを指定します。
  - **bondingInterface** *bondingInterface*：リンクされたボンディング インターフェイスを指定します。
  - **neighbor** *neighbor_ip_address*：ネイバーの IP アドレスを指定します。
    - **fail-over** *fail_over_type*：フェールオーバー タイプを指定します。
    - **remote-as** *remote_as*：BGP ネイバーの自律システム（AS）番号を指定します。
- **learnDefaultRoute**：デフォルト ルートを学習し、カーネル スペースに追加します
- **loopbackBFDPort** *loopbackBFDPort*：BFD ローカル ポートを指定します。
- **loopbackPort** *loopbackPort*：BGP ローカル ポートを指定します。
- **policy-name** *policy_name*：ポリシー名を指定します。
  - **as-path-set** *as_path_set*：自律システム（AS）パスセットを指定します。
  - **gateWay** *gateWay_address*：ゲートウェイ アドレスを指定します。
  - **interface** *interface_id_source*：送信元 IP として設定するインターフェイスを指定します。
  - **ip-prefix** *ip_prefix_value*：IP プレフィックス値を指定します。
  - **isStaticRoute** *false* | *true*：カーネル スペースでスタティック ルートを追加するかどうかを指定します。デフォルト値は false です。
  - **mask-range** *mask_range*：マスク範囲を指定します。
  - **modifySourceIp** *false* | *true*：着信ルートの送信元 IP を変更します。デフォルト値は false です。

**true**：このオプションは、UDP 関連でない VIP に使用されます。特定のインターフェイスの送信元 IP は、SMF からパケットを送信するときに送信元 IP として使用されます。

**false**：このオプションは、UDP 関連のすべての VIP に使用されます。VIP は、SMF からパケットを送信するときに送信元 IP として使用されます。

### 例

構成例は次のとおりです。

```
router bgp 65000
  bfd interval 250000 min_rx 250000 multiplier 3
  loopbackPort 179 loopbackBFDPort 3784
interface ens160 (BGP on non-bonded interface <-- loopbackEth)
  bondingInterface enp216s0f0 (leaf6-nic)
  bondingInterface enp216s0f1 (leaf6-nic)
  neighbor leaf6-ip remote-as 60000 fail-over bfd
exit
interface ens192 (BGP on non-bonded interface <-- loopbackEth)
  bondingInterface enp94s0f1 (leaf7-nic)
  bondingInterface enp94s0f0 (leaf7-nic)
  neighbor leaf7-ip remote-as 60000 fail-over bfd
exit
policy-name allow-all ip-prefix 209.165.201.30/0 mask-range 0...32
exit
```

BFD を使用した BGP ルータ構成

```
show running-config router
router bgp 65142
 learnDefaultRoute false
 bfd interval 250000 min_rx 250000 multiplier 3
 interface enp94s0f0.3921
  bondingInterface enp216s0f0
  bondingInterface enp94s0f0
  neighbor 209.165.201.24 remote-as 65141 fail-over bfd
 exit
 interface enp94s0f1.3922
  bondingInterface enp216s0f1
  bondingInterface enp94s0f1
  neighbor 209.165.202.24 remote-as 65141 fail-over bfd
```

ネイバーの BFD ステータスを表示

```
show bfd-neigbor
status-details

----- bgpspeaker-pod-1----

Peer             Status

209.165.202.142  STATE_DOWN
----- bgpspeaker-pod-2----

Peer             Status

209.165.202.142  STATE_UP
```

```
policy-name allow-n11 ip-prefix 209.165.200.225/54 mask-range 25..32 interface bd1.n11.2271
 modifySourceIp true isStaticRoute true gateWay 209.165.201.14
```

上記の例では、*modifySourceIp* は true に設定されています。

- AMF サブネット：209.165.200.225/54

  N11 Svc ボンド物理インターフェイス：bd1.n11.2271（IP アドレス：209.165.201.23）

  N11 Svc ボンド VxLAN Anycast GW：209.165.201.14

  N11 VIP アドレス：209.165.201.7

- SMF アウトバウンド パケット（送信元 IP は 209.165.201.23 になります）

  SMF へのインバウンド パケット（宛先 IP は 209.165.201.7 になります）

```
policy-name allow-n4-1 ip-prefix 209.165.201.17/41 mask-range 24..32 interface bd2.n4.2274
 gateWay 209.165.201.17
```

上記の例では、*modifySourceIp* は false（デフォルト）に設定されています。

- UPF N4 インターフェイス IP：209.165.201.17/41

  N4 Svc ボンド物理インターフェイス：bd2.n4.2274（IP アドレス：209.165.201.23）

  N4 Svc ボンド VxLAN Anycast GW：209.165.201.17

  N4 VIP アドレス：209.165.201.14

- SMF アウトバウンド パケット（送信元 IP は 209.165.201.14 になります）

  SMF へのインバウンド パケット（宛先 IP は 209.165.201.14 になります）

# CDL GR の展開

デフォルトでは、CDL は db-ep の 2 つのレプリカ、1 つのスロット マップ（マップごとに 2 つのレプリカ）、および 1 つのインデックス マップ（マップごとに 2 つのレプリカ）で展開されます。

（注） YANG の CDL コンテナを構成することを推奨します。

## CDL GR の前提条件

CDL GR を展開する前に、ユーザーは次を構成する必要があります。

- CDL セッション データベースを削除し、基本構成を定義します。
- CDL 用の Kafka。
- CDL 用の Zookeeper。

# CDL インスタンス認識とレプリケーション

CDL では、既存の GR 関連パラメータとともに、すべてのラックで機能フラグを使用して GR インスタンス認識を有効にする必要があります。また、この機能をすべてのラックで機能させるには、システム ID からスライス名へのマッピングも提供する必要があります。

CDL には Geo レプリケーション（GR）フェールオーバー通知も用意されていているため、セッションデータのタイマーの期限切れ、および現在アクティブなラックへの一括通知を通知できます。CDL は GR フェールオーバー通知のために、App-Infra を介してボーダー ゲートウェイ プロトコル（BGP）を使用します。

CDL は両方の GR ラックのキー値を登録します。登録したキー値に変更があると、App-Infra は CDL に通知を送信します。キー値は、CDL システム ID または GR インスタンスの状態を示します。GR インスタンスは、 キーの CDL システム ID または GR インスタンス ID を使用して CDL スライスにマップされます。

システム ID は両方のラックで必須です。NF 構成の GR インスタンス ID が CDL システム ID と一致している必要があります。

CDL には、インスタンス固有のデータ スライスがあります。また、ユーザーは起動時にインスタンス固有のスライス情報を構成できます。

- CDL は、有効期限切れ時またはアクティブなスライスからの一括通知要求時にデータを通知します。
- CDL は、app-infra memory-cache からの通知に基づいてアクティブインスタンスを決定します。
- CDL スライスは、異なる種類のデータを保存する CDL インスタンス内のパーティションです。この場合、NF はデータの別のインスタンスを保存します。

（注） CDL スライス名は、GR で構成されているスライス名と一致する必要があります。

## CDL インスタンス認識の構成

CDL インスタンス認識を構成するには、次のコマンドを使用します。

```
config
cdl
 datastore datastore_session_name
   features
    instance-aware-notification
     enable [ true | false ]
     system-id system_id
      slice-names slice_names
  end
```

注：

- **datastore** *datastore_session_name*：データストア名を指定します。

- **enable [ true | false ]**：スライスの GR インスタンス状態チェックを有効にします。
- **system-id** *system_id*：システム ID からスライス名へのマッピング。
- **slice-names** *slice_names*：システム ID に関連付けられているスライス名のリストを指定します。CDL スライス名は、GR で構成されたスライス名と一致する必要があります。

**例**

次に、設定例を示します。

```
cdl datastore session
 features instance-aware-notification enable true
 features instance-aware-notification system-id 1
  slice-names [ sgw1 smf1 ]
 exit
 features instance-aware-notification system-id 2
  slice-names [ sgw2 smf2 ]
 end
```

## CDL レプリケーションの構成

ここでは、CDL レプリケーションの構成について説明します。

1. Geo HA 関連の構成パラメータを使用せずに、Rack-1 CDL HA システムを構成します。
   1. 構成でシステム ID を 1 に設定します。
   2. 要件に従って、スロット マップ/レプリカとインデックスマップ/レプリカと Kafka レプリカを設定します。

   以下に設定例を示します。

   ```
   cdl system-id 1
   cdl node-type session
   cdl datastore session
   endpoint replica replica_id
     slot map 4
     slot replica 2
     index map 1
     index replica 2
   cdl kafka replica 2
   ```

1. Rack-2 から Rack-1 への通信用に、Rack-1 で外部 IP を構成します。
   1. Rack-1 で Geo レプリケーションを有効にし、リモートラックを Rack-1 の 2 として構成します。

      ```
      cdl enable-geo-replication true
      ```
   2. Rack-2 からアクセスできるように CDL エンドポイントの外部 IP を構成します。

      ```
      cdl datastore session endpoint external-ip site-1_external_ip
      ```
   3. すべての Kafka レプリカの外部 IP とポートを構成します。

したがって、Kafka 用に 2 つのレプリカ（デフォルト）が構成されている場合、ユーザーは異なる <*ip*>+ <*port*> ペアでサポートされます。

**cdl kafka external-ip** *site-1_external_ip port1* **cdl kafka external-ip** *site-1_external_ip port2*

2. Rack-2 のリモートラック情報を追加します。
   - Rack-2 でのリモートラック cdl-ep の構成：

     **cdl remote-site 1 db-endpoint host** *site-1_cdl_ep_ip*

     **cdl remote-site 1 db-endpoint port** *site-1_cdl_ep_port*

     （ポートの例：8882）
   - Rack-2 のリモートラック Kafka 構成：

     cdl remote-site *1* kafka-server *site-1_kafka1_ip site-1_kafka1_port*

     cdl remote-site *1* kafka-server *site-1_kafka2_ip site-1_kafka2_port*
   - セッション データストア構成をリモート Rack-2 構成に誘導します。

     cdl datastore session geo-remote-site *1*
   - （任意）SSL 証明書を構成して、Rack-1 のリモートラックとのセキュアな接続を確立します。証明書はすべて、複数行の生のテキスト形式です。証明書が有効でない場合、サーバの接続は非セキュアな接続のままです。

     **cdl ssl-config certs** *site-2_external_ip* **ssl-key**<ssl_key>

     **cdl ssl-config certs** *site-2_external_ip* **ssl-crt**<ssl_crt>
3. Rack-2 で GR 構成をコミットします。
   - 構成をコミットし、ポッドを Rack-2 に展開します。
   - すべてのポッドが実行状態であることを確認します。
   - 両方のラックを展開したら、両方のラックのミラー メーカー ポッドが実行中で、準備完了状態であることを確認します。

**例**

**HA**：

```
cdl node-type db-ims

cdl datastore session
 endpoint replica 2
 index map    1
 index write-factor 1
 slot replica 2
 slot map     4
 slot write-factor 1
exit
```

```
k8 label cdl-layer key smi.cisco.com/node-type value smf-ims-session
```

**Rack-1** :

```
cdl system-id          1
cdl node-type          session
cdl enable-geo-replication true
cdl zookeeper replica 1

cdl remote-site 2
 db-endpoint host 209.165.201.21 >> Rack-2 external CDL IP
 db-endpoint port 8882
 kafka-server 209.165.201.21 10092 >> Rack-2 external CDL IP
 exit
exit

cdl label-config session
 endpoint key smi.cisco.com/node-type1
 endpoint value smf-cdl
 slot map 1
  key   smi.cisco.com/node-type1
  value smf-cdl
 exit
 index map 1
  key   smi.cisco.com/node-type1
  value smf-cdl
 exit
exit
cdl logging default-log-level debug

cdl datastore session
 label-config    session
 geo-remote-site [ 2 ]
 slice-names     [ 1 2 ]
 endpoint cpu-request 100
 endpoint replica 2
 endpoint external-ip 209.165.201.25 >> Rack-1 external CDL IP
 endpoint external-port 8882
 index cpu-request 100
 index replica 2
 index map   1
 slot cpu-request 100
 slot replica 2
 slot map    1
exit

cdl kafka replica 1
cdl kafka label-config key smi.cisco.com/node-type1
cdl kafka label-config value smf-cdl
cdl kafka external-ip 209.165.201.25 10092 >> Rack-1 external CDL IP
```

**Rack-2** :

```
cdl system-id          2
cdl node-type          session
cdl enable-geo-replication true
cdl zookeeper replica 1

cdl remote-site 1
 db-endpoint host 209.165.201.25 >> Rack-1 external CDL IP
 db-endpoint port 8882
 kafka-server 209.165.201.25 10092 >> Rack-1 external CDL IP
 exit
exit
```

```
cdl label-config session
 endpoint key smi.cisco.com/node-type12
 endpoint value smf-cdl
 slot map 1
  key   smi.cisco.com/node-type12
  value smf-cdl
 exit
 index map 1
  key   smi.cisco.com/node-type12
  value smf-cdl
 exit
exit

cdl datastore session
 label-config    session
 geo-remote-site [ 1 ]
 slice-names     [ 1 2 ]
 endpoint cpu-request 100
 endpoint replica 2
 endpoint external-ip 209.165.201.21 >> Rack-2 external CDL IP
 endpoint external-port 8882
 index cpu-request 100
 index replica 2
 index map   1
 slot cpu-request 100
 slot replica 2
 slot map    1
exit

cdl kafka replica 1
cdl kafka label-config key smi.cisco.com/node-type12
cdl kafka label-config value smf-cdl
cdl kafka external-ip 209.165.201.21 10092 >> Rack-2 external CDL IP
```

# 合法的傍受

合法的傍受（LI）機能を使用すると、法執行機関（LEA）がサブスクライバの通信を傍受できます。LI機能を使用すると、ネットワーク オペレータは、対象のモバイルユーザーの制御メッセージとデータ メッセージを傍受できるようになります。このサポートを呼び出すため、LEA はネットワーク オペレータに特定のモバイル ユーザーの傍受を開始するように要求します。法的な承認がこの要求をサポートします。

1. 合法的傍受（LI）タップは、すべてのラックで構成/有効にする必要があります。1 つのラックでLI構成に失敗した場合、特定のサブスクライバのタップをすべてのラックで有効にするようにLEA を再構成する必要があります。

（注） LI タップ構成はラック間で同期されません。

したがって、LI タップ構成はすべてのラックに必須です。

LI タップ構成の詳細については、Cisco のテクニカル担当者にお問い合わせください。

2. GR インスタンス認識は、合法的傍受 src-address にのみ適用されます。

例：

```
lawful-intercept instance 1 src-addr 209.165.200.225
```

または

```
lawful-intercept
  instance 1
    src-addr 209.165.200.225
```

3. `show` コマンドはインスタンスを認識しません。特定のクラスタで構成されているすべてのタップを表示します。

   LI `show` コマンドの詳細については、Cisco のテクニカル担当者にお問い合わせください。

4. すべての GR インスタンスがクラスタでスタンバイ状態にあり、アクティブな LI タップが失敗し、CLI メッセージ「ラックがスタンバイ モードにあるため、アクティブなタップは許可されません。`camp on` を試行してください」が表示された場合、同じサブスクライバで camp-on タップを構成します。

# RADIUS 設定

NAS-IP と NAS-Identifier はインスタンス対応です。プロファイル RADIUS 構成では、instance-id ごとに異なる NAS-IP と NAS-Identifier を構成できます。既存の非インスタンス NAS-IP および NAS-Identifier 構成が、ラックのローカル インスタンスのデフォルト nas-ip およびデフォルト nas-id として使用されます。

### 例

次の構成例を参照してください。

```
profile radius
 attribute
  instance 1
   nas-ip 209.165.200.225  --> Instance-1 specific NAS-IP, used for common AUTH & ACCT
   nas-identifier  smf1    --> Instance-1 specific NAS-Identifier, used for common AUTH
 & ACCT
  exit
  instance 2
   nas-ip 209.165.200.230  --> Instance-2 specific NAS-IP, used for common AUTH & ACCT
   nas-identifier  smf2    --> Instance-2 specific NAS-Identifier, used for common AUTH
 & ACCT
  exit
 exit
 accounting
  attribute
   instance 1
    nas-ip 209.165.200.225  --> Instance-1 specific NAS-IP, used for common ACCT
    nas-identifier  smf1    --> Instance-1 specific NAS-Identifier , used for common
ACCT
   exit
   instance 2
    nas-ip 209.165.200.230  --> Instance-2 specific NAS-IP, used for common ACCT
    nas-identifier  smf2    --> Instance-2 specific NAS-Identifier , used for common
ACCT
   exit
  exit
 exit
 server-group g1
  attribute
```

```
   instance 1
    nas-ip 209.165.200.225  --> Instance-1 specific NAS-IP, used for server-group <g1>
AUTH & ACCT
    nas-identifier  smf1    --> Instance-1 specific NAS-ID, used for server-group <g1>
Auth &Acct
   exit
   instance 2
    nas-ip 209.165.200.230  --> Instance-2 specific NAS-IP, used for server-group <g1>
AUTH & ACCT
    nas-identifier  smf2    --> Instance-2 specific NAS-ID,used for server-group
<g1>AUTH&ACCT
   exit
  exit
  accounting
   attribute
    instance 1
     nas-ip 209.165.200.225 --> Instance-1 specific NAS-IP, used for server-group <g1>
ACCT
     nas-identifier  smf1   --> Instance-1 specific NAS-ID, used for server-group <g1>
ACCT
    exit
    instance 2
     nas-ip 209.165.200.230 --> Instance-2 specific NAS-IP, used for server-group <g1>
ACCT
     nas-identifier  smf2   --> Instance-2 specific NAS-ID, used for server-group <g1>
ACCT
    exit
   exit
  exit
 exit
exit
```

**endpoint** ポッド構成が特定のインスタンスの下に移動するため、Radius Disconnect-Request VIP もインスタンス対応になります。

```
instance instance-id 1
 endpoint radius
  replicas 1
  interface coa-nas
   vip-ip 209.165.202.130 vip-port 3799  --> Instance-1 specific Radius-Disconnect-Msg-VIP
 & PORT
  exit
 exit
exit
instance instance-id 2
 endpoint radius
  replicas 1
  interface coa-nas
   vip-ip 209.165.202.129 vip-port 3799  --> Instance-2 specific Radius-Disconnect-Msg-VIP
 & PORT
  exit
 exit
exit
```

# GR ペアのソフトウェア アップデート

`config commit` を基準として考慮してください。同じチェックリストは、他のアップグレードシナリオにも適用できます。

### チェックリスト

（注） 両方のラック（Rack-1 とRack-2）で `cluster sync` を同時に実行しないでください。Rack-1 のアップグレードを続行する前に、Rack-1 で手動スイッチオーバーをトリガしてください。

- 両方のラックで同時に `config commit` を実行しないでください。各ラックで個別に `config commit` を実行してください。
- Rack-1 で `config commit` を実行する前に、Rack-1 で CLI ベースのスイッチオーバーを開始し、Rack-2 に両方のインスタンス（instance-id 1 と instance-id 2）のプライマリ所有権があることを確認してください。
- Rack-1 で `config commit` を実行します。`config commit` が成功し、ポッドが再起動し、実行状態に戻って最新の helm チャートを取得するのを待ちます（該当する場合）。
- Rack-1 のロールを Primary に戻します（両方のラックのロールを切り替え / リセットします）。
- Rack-1（Primary）と Rack-2（Standby）の使用可能なロールが、予期されるステータスになっていることを確認します。
- Rack-2 についても前述のチェックリストを繰り返します。

### ソフトウェア アップグレード

**GR が有効な場合の Rack-1 のアップグレード**：

1. Rack-1 の両方のインスタンスで使用可能なロールが PRIMARY/STANDBY であることを確認します。

```
show role instance-id 1
result "PRIMARY"

show role instance-id 2
result "STANDBY"
```

2. Rack-1 の両方のインスタンスのロールの切り替えを開始し、フェールバック間隔を 0 秒にして STANDBY に移行します。このステップにより、ロールが PRIMARY/STANDBY から STANDBY_ERROR/STANDBY_ERROR に移行します。

```
geo switch-role instance-id 1 role standby [failback-interval 0]
geo switch-role instance-id 2 role standby [failback-interval 0]
```

（注）
- 両方のラック間のハートビートが正常である必要があります。
- CLI **failback-interval** は、リリース間のアップグレードの下位互換性を提供するオプションのコマンドです。 **failback-interval** の値は 0 です。現在のリリースでは廃止され、後続のリリースでは廃止されます。

3. 両方のインスタンスの使用可能なロールが Rack-1 の STANDBY_ERROR に移動したことを確認します。

```
show role instance-id 1
result "STANDBY_ERROR"

show role instance-id 2
result "STANDBY_ERROR"
```

4. 両方のインスタンスの使用可能なロールが Rack-2 の PRIMARY に移動したことを確認します。

```
show role instance-id 1
result "PRIMARY"

show role instance-id 2
result "PRIMARY"
```

5. Rack-1 の要件に従って、システム モードのシャットダウン/実行を使用して、ローリング アップグレード（または）非グレースフル アップグレードを実行します。レプリケーションが完了するまで、GR のスイッチオーバーと SMF のシャットダウンの間に 5 分の間隔を設けます。

6. アップグレード手順の完了後に次の手順を実行します。Rack-1 で正常性チェックを実行し、POD が起動し、Rack-1 が正常であることを確認します。

7. 両方のインスタンスで使用可能なロールが Rack-1 の STANDBY_ERROR モードのままであることを確認します。

```
show role instance-id 1
result "STANDBY_ERROR"

show role instance-id 2
result "STANDBY_ERROR"
```

8. Rack-1 の両方のインスタンスのロールの STANDBY へのリセットを開始します。このステップにより、ロールが STANDBY_ERROR/STANDBY_ERROR から STANDBY/STANDBY に移行します。

```
geo reset-role instance-id 1 role standby
geo reset-role instance-id 2 role standby
```

9. 両方のインスタンスのロールが Rack-1 の STANDBY に移動したことを確認します。

```
show role instance-id 1
result "STANDBY"

show role instance-id 2
result "STANDBY"
```

10. Rack-2 の instance-id 1 のロールの STANDBY への切り替えを開始します。この手順により、Rack-2 の使用可能なロールが PRIMARY/PRIMARY から STANDBY_ERROR/PRIMARY に、Rack-1 の使用可能なロールが STANDBY/STANDBY から PRIMARY/STANDBY に移行します。

```
geo switch-role instance-id 1 role standby [failback-interval 0]
```

11. Rack-2 の インスタンスで使用可能なロールが STANDBY_ERROR/PRIMARY であることを確認します。

```
show role instance-id 1
result "STANDBY_ERROR"

show role instance-id 2
result "PRIMARY"
```

**12.** Rack-1 の両方のインスタンスで使用可能なロールが PRIMARY/STANDBY であることを確認します。

```
show role instance-id 1
 result "PRIMARY"

show role instance-id 2
 result "STANDBY"
```

**13.** STANDBY への Rack-2 の instance-id 1 のロールのリセットを開始します。このステップにより、Rack-2 のロールが STANDBY_ERROR/PRIMARY から STANDBY/PRIMARY に移行します。

```
geo reset-role instance-id 1 role standby
```

**14.** Rack-2 の両方のインスタンスで使用可能なロールが STANDBY/PRIMARY のロールであることを確認します。

```
show role instance-id 1
result "STANDBY"

show role instance-id 2
 result "PRIMARY"
```

**GR が有効な場合の Rack-2 のアップグレード**：

**1.** Rack-2 の両方のインスタンスで使用可能なロールが STANDBY/PRIMARY のロールであることを確認します。

```
show role instance-id 1
result "STANDBY"

show role instance-id 2
result "PRIMARY"
```

**2.** Rack-2 の両方のインスタンスのロールの切り替えを開始し、フェールバック間隔を 0 秒にして STANDBY に移行します。このステップにより、ロールが STANDBY/PRIMARY から STANDBY_ERROR/STANDBY_ERROR に移行します。

```
geo switch-role instance-id 1 role standby [failback-interval 0]
geo switch-role instance-id 2 role standby [failback-interval 0]
```

**3.** 両方のインスタンスの使用可能なロールが Rack-2 の STANDBY_ERROR に移動することを確認します。

```
show role instance-id 1
result "STANDBY_ERROR"

show role instance-id 2
result "STANDBY_ERROR"
```

**4.** 両方のインスタンスで使用可能なロールが Rack-1 の PRIMARY に移動していることを確認します。

```
show role instance-id 1
 result "PRIMARY"
```

```
show role instance-id 2
 result "PRIMARY"
```

5. Rack-2 の要件に従って、システム モードのシャットダウン/実行を介して、ローリング アップグレード（または）非グレースフル アップグレードを実行します。
6. アップグレード手順の完了後に後続の手順を実行します。Rack-2 で正常性チェックを実行し、ポッドが起動し、Rack-2 が正常であることを確認します。
7. 両方のインスタンスで使用可能なロールが Rack-2 の STANDBY_ERROR のままであることを確認します。

```
show role instance-id 1
result "STANDBY_ERROR"

show role instance-id 2
result "STANDBY_ERROR"
```

8. Rack-2 の両方のインスタンスのロールの STANDBY へのリセットを開始します。このステップにより、ロールが STANDBY_ERROR/STANDBY_ERROR から STANDBY/STANDBY に移行します。

```
geo reset-role instance-id 1 role standby
geo reset-role instance-id 2 role standby
```

9. 両方のインスタンスで使用可能なロールが Rack-2 の STANDBY に移動することを確認します。

```
show role instance-id 1
result "STANDBY"

show role instance-id 2
result "STANDBY"
```

10. Rack-1 の instance-id 2 のロールを STANDBY に切り替えて開始します。この手順では、Rack-1 の使用可能なロールを PRIMARY/PRIMARY から PRIMARY/STANDBY_ERROR に、Rack-2 の使用可能なロールを STANDBY/STANDBY から STANDBY/PRIMARY に移行します。

```
geo switch-role instance-id 2 role standby [failback-interval 0]
```

11. Rack-1 の両方のインスタンスで使用可能なロールが PRIMARY/STANDBY_ERROR であることを確認します。

```
show role instance-id 1
result "PRIMARY"

show role instance-id 2
result "STANDBY_ERROR"
```

12. Rack-2 の両方のインスタンスで使用可能なロールが STANDBY/PRIMARY のロールであることを確認します。

```
show role instance-id 1
result "STANDBY"

show role instance-id 2
result "PRIMARY"
```

13. Rack-1 の instance-id 2 の STANDBY へのロールのリセットを開始します。この手順では、Rack-1 のロールを PRIMARY/STANDBY_ERROR から PRIMARY/STANDBY に移行します。

```
geo reset-role instance-id 2 role standby
```

14. Rack-1 の両方のインスタンスで使用可能なロールが PRIMARY/STANDBY であることを確認します。

```
show role instance-id 1
result "PRIMARY"

show role instance-id 2
result "STANDBY"
```

# GR CLI

次のセクションでは、GR CLI ベースのコマンドについて説明します。

## Geo レプリケーション プル データ

次のサンプル構成では、Geo レプリケーションのプルデータを設定します。これらのコマンドは、誤動作シナリオが発生した場合に、レプリケーションデータ同期アクティビティを支援および実行します。GR ロールに移行し、システムでのレプリケーションデータの不一致を最小限に抑えるためには、次のコマンドを開始して、アクセス可能なすべてのラック間でデータを同期することができます。

**geo replication-pull instance-id** *gr_instanceId*

**注**：

- **geo replication-pull**：ピア ラックからレプリケーションデータをプルして、ローカル ラックと同期します。
- **instance-id** *gr_instanceId*：GR インスタンス ID を指定します。

## Geo ロールのリセット

GR インスタンスのロール（たとえば、 **STANDBY_ERROR** から **STANDBY** 、 **PRIMARY**のロール）をリセットするには、次のコマンド例を使用します。

**geo reset-role role** *role* **instance-id** *gr_instanceId*

**注**：

- **role** *role*：指定のラックの新しいロールを指定します。

  ロールは **PRIMARY** または **STANDBY**です。

- **instance-id** *gr_instanceId*：GR インスタンス ID を指定します。

重要 **geo reset-role** コマンドは、ローカル ラックの特定のインスタンスのロールの変更をトリガします。リモート ラックは、同じコマンドのメッセージを受信しません。指定されたインスタンス ID のロールを **STANDBY_ERROR** から **STANDBY** に、および **STANDBY** から **PRIMARY**に変更することのみが可能です。別のロールの変更はできません。

## Geo スイッチ ロール

GR ロールを切り替えるには、プライマリ ラックで コマンドを開始し（たとえば、ロール **PRIMARY** を **STANDBY** のみに）、次のコマンドを使用します。

**geo switch-role { role** *primary | standby* **instance-id** *gr_instanceId* **[ failback-interval** *failback_interval* **] }**

注：

- **role** *role*：指定のラックの新しいロールを指定します。

  ロールは、 *primary* または *standby*にできます。特定の GR インスタンス ID のプライマリ ロールから手動スイッチオーバーをトリガする必要があります。

- **instance-id** *gr_instanceId*：GR インスタンス ID を指定します。
- **failback-interval** は、リリース間のアップグレードの後方互換性を提供するオプションのコマンドです。 **failback-interval** の推奨値は 0 です。

重要 **geo switch-role** コマンドは、特定のインスタンス ID について、あるラックから別のラックへの手動フェールオーバーをトリガします。フェールオーバーをトリガするラックが**PRIMARY** ロールから **STANDBY_ERROR** ロールに変更されます。その間、フェールオーバーをトリガしたラックは、別のラックにフェールオーバー（Trigger GR）メッセージを送信します。フェールオーバー メッセージを受信した他のラックは、 **STANDBY** ロールから **PRIMARY** ロールに変更されます。

（注） **failback-interval** は現在のリリースで廃止され、後続のリリースでは廃止されます。

# 障害対応

ここでは、さまざまな該当するトラブルシューティングのシナリオについて説明します。

## show/clear コマンド

ここでは、問題のデバッグに役立つ show/clear コマンドについて説明します。

### clear subscriber

gr-instance 対応サブスクライバをクリアするには、次のコマンドを使用します。

**clear subscriber all gr-instance** *gr_instanceId*

（注） **gr-instance** はオプションのパラメータです。**gr-instance** が指定されていない場合、`show subscriber all` ではそのラックのローカル インスタンス ID が考慮されます。

**例**

次に、設定例を示します。

```
clear subscriber all gr-instance 1
result
ClearSubscriber Request submitted
```

### BFD ステータスの表示

ネイバーの BFD ステータスを表示するには、次のコマンドを使用します。

**show bfd-neighbor**

**例**

次に、いくつか構成例を示します。

```
show bfd-neighbor
status-details

-----example-bgp-ep-1 ----

Peer             Status

 209.165.202.142  STATE_DOWN
-----example-bgp-ep-2 ----

Peer             Status

 209.165.202.142  STATE_DOWN

show bfd-neigbor
status-details

-----bgpspeaker-pod-1 ----

Peer             Status

 209.165.202.131
-----bgpspeaker-pod-2 ----

Peer             Status

 209.165.202.131   STATE_UP
```

### BGP グローバルの表示

BGP グローバル構成を表示するには、次のコマンドを使用します。

**show bgp-global**

例

次に、いくつか構成例を示します。

```
show bgp-global
global-details
-----example-bgp-ep-2 ----
AS:        65000
Router-ID: 209.165.202.149
Listening Port: 179, Addresses: 209.165.202.149
-----example-bgp-ep-1 ----
AS:        65000
Router-ID: 209.165.202.148
Listening Port: 179, Addresses: 209.165.202.148
```

```
show bgp-global
global-details

-----bgpspeaker-pod-2 ----
AS:        65061
Router-ID: 209.165.202.132
Listening Port: 179, Addresses: 209.165.202.132
```

## show bgp kernel route

BGP カーネル構成ルートを表示するには、次のコマンドを使用します。

**show bgp-kernel-route kernel-route**

例

次に、いくつか構成例を示します。

```
show bgp-kernel-route
kernel-route

-----example-bgp-ep-2 ----

 DestinationIP  SourceIP        Gateway

-----example-bgp-ep-1 ----

 DestinationIP      SourceIP          Gateway
 209.165.202.133    209.165.202.148   209.165.202.142
 209.165.202.134    209.165.202.148   209.165.202.142
```

```
show bgp-kernel-route
kernel-route

-----bgpspeaker-pod-2 ----

 DestinationIP        SourceIP            Gateway

 209.165.202.135    209.165.202.132    209.165.202.131

-----bgpspeaker-pod-1 ----

 DestinationIP  SourceIP        Gateway
```

## show bgp neighbors

BGP ネイバーのステータスを表示するには、次のコマンドを使用します。

**show bgp-neighbors neighbor-details**
**show bgp-neighbors ip** *ip_address* **neighbor-details**

### 例

次に、いくつか構成例を示します。

```
show bgp-neighbors neighbor-details
-----example-bgp-ep-1 ----
Peer             AS  Up/Down State       |#Received  Accepted
209.165.202.142 60000 00:25:06 Establ      |        3         3
-----example-bgp-ep-2 ----
Peer             AS Up/Down State       |#Received  Accepted
209.165.202.142 60000   never Idle        |        0         0

show bgp-neighbors ip 209.165.202.142 neighbor-details
-----example-bgp-ep-2 ----
BGP neighbor is 209.165.202.142, remote AS 60000
  BGP version 4, remote router ID unknown
  BGP state = ACTIVE
  BGP OutQ = 0, Flops = 0
  Hold time is 0, keepalive interval is 0 seconds
  Configured hold time is 90, keepalive interval is 30 seconds

  Neighbor capabilities:
    multiprotocol:
        ipv4-unicast:   advertised
    route-refresh:      advertised
    extended-nexthop:   advertised
        Local:  nlri: ipv4-unicast, nexthop: ipv6
    4-octet-as: advertised
  Message statistics:
                        Sent       Rcvd
    Opens:               130          0
    Notifications:         0          0
    Updates:               0          0
    Keepalives:            0          0
    Route Refresh:         0          0
    Discarded:             0          0
    Total:               130          0
  Route statistics:
    Advertised:            0
    Received:              0
    Accepted:              0

-----example-bgp-ep-1 ----
BGP neighbor is 209.165.202.142, remote AS 60000
  BGP version 4, remote router ID 209.165.202.136
  BGP state = ESTABLISHED, up for 00:25:20
  BGP OutQ = 0, Flops = 0
  Hold time is 90, keepalive interval is 30 seconds
  Configured hold time is 90, keepalive interval is 30 seconds

  Neighbor capabilities:
    multiprotocol:
        ipv4-unicast:   advertised and received
    route-refresh:      advertised and received
    extended-nexthop:   advertised
        Local:  nlri: ipv4-unicast, nexthop: ipv6
    4-octet-as: advertised and received
```

```
  Message statistics:
                        Sent       Rcvd
    Opens:                 1          1
    Notifications:         0          0
    Updates:               1          1
    Keepalives:           51         51
    Route Refresh:         0          0
    Discarded:             0          0
    Total:                53         53
  Route statistics:
    Advertised:            0
    Received:              3
    Accepted:              3
```

## show bgp route サマリ

BGP ルート サマリを表示するには、以下のコマンドを使用します。

**show bgp-route-summary**

### 例

次に、設定例を示します。

```
show bgp-route-summary
route-details
-----example-bgp-ep-1 ----
Table afi:AFI_IP safi:SAFI_UNICAST
Destination: 5, Path: 5
-----example-bgp-ep-2 ----
Table afi:AFI_IP safi:SAFI_UNICAST
Destination: 2, Path: 2
```

## BGP ルートの表示

BGP ルート情報を表示するには、次のコマンドを使用します。

**show bgp-routes**

### 例

次に、設定例を示します。

```
show bgp-routes
bgp-route

-----example-bgp-ep-1 ----
   Network              Next Hop             AS_PATH      Age        Attrs
*> 209.165.202.133/24   209.165.202.142        60000      00:25:55   [{Origin: i} {Med:
 0}]
*> 209.165.200.225/32   209.165.202.148                   00:26:00   [{Origin: e}
{LocalPref: 100} {Med: 600}]
*> 209.165.202.134/24   209.165.202.142        60000      00:25:55   [{Origin: i} {Med:
 0}]
*> 209.165.202.140/24   209.165.202.142        60000      00:25:55   [{Origin: i} {Med:
 0}]
*> 209.165.202.146/32   209.165.202.148                   00:26:00   [{Origin: e}
{LocalPref: 100} {Med: 600}]

-----example-bgp-ep-2 ----
   Network              Next Hop             AS_PATH      Age        Attrs
*> 209.165.200.225/32   209.165.202.149                   00:26:24   [{Origin: e}
```

```
{LocalPref: 100} {Med: 600}]
*> 209.165.202.146/32   209.165.202.149                  00:26:24   [{Origin: e}
{LocalPref: 100} {Med: 600}]
```

## show endpoint

gr-instance 対応になったエンドポイントを表示するには、次のコマンドを使用します。

**show endpoint all grInstance** *gr_instanceId*

（注） **grInstance** はオプションのパラメータです。**grInstance** が指定されていない場合、`show subscriber all` ではそのラックのローカル インスタンス ID が考慮されます。

### 例

次に、設定例を示します。

```
show endpoint all grInstance 1
                                                                                                    START
  STOPPED  GR
ENDPOINT                          ADDRESS        TYPE  STATUS   INTERFACE  INTERNAL
TIME      TIME     INSTANCE
-------------------------------------------------------------------------------------------------------
209.165.202.137:2123       209.165.202.137:2123  Udp   Started             false     10
 hours  <none>   1
Gtpu:209.165.202.137:2152  209.165.202.137:2152  Udp   Started  GTPU       false     10
 hours  <none>   1
N4:209.165.202.137:8806    209.165.202.137:8806  Udp   Started  N4         false     10
 hours  <none>   1
S2B-GTP                    209.165.202.138:2124  Udp   Started  s2b        false     10
 hours  <none>   1
S5-GTP                     209.165.202.138:2125  Udp   Started  s5         false     10
 hours  <none>   1
S5S8S2B-GTP                209.165.202.138:2123  Udp   Started  s5s8s2b    false     10
 hours  <none>   1
Sxa:209.165.202.137:8805   209.165.202.137:8805  Udp   Started  SXA        false     10
 hours  <none>   1
n10-1                      209.165.202.139:9010  Rest  Started  N10-1      false     10
 hours  <none>   1
n11-1                      209.165.202.139:9011  Rest  Started  N11-1      false     10
 hours  <none>   1
n40-1                      209.165.202.139:9040  Rest  Started  N40-1      false     10
 hours  <none>   1
n7-1                       209.165.202.139:9007  Rest  Started  N7-1       false     10
 hours  <none>   1
sbi-1                      209.165.202.139:8090  Rest  Started  SBI-1      false     10
 hours  <none>   1
```

## ETCD/キャッシュポッドのレプリケーションの表示

etcd および cache-pod データのレプリケーションの詳細を表示するには、次のコマンドを使用します。

**show georeplication checksum instance-id** *gr_instanceId*

例

次に、設定例を示します。

```
show georeplication checksum instance-id
Value for 'instance-id' (<string>): 1
checksum-details
--              ----    --------
 ID             Type    Checksum
 --             ----    --------
 1              ETCD    1617984439
 IPAM           CACHE   1617984439
 NRFCache       CACHE   1617984439
 NRFSubs        CACHE   1617984439
 IDMGR          CACHE   1617984439
 NRFMgmt        CACHE   1617984439
```

## show role

GR インスタンスの現在のロールを表示するには、次のコマンドを使用します。

**show role instance-id** *gr_instanceId*

（注） ロールで使用可能な値のリストは次のとおりです。

- プライマリ
- **STANDBY**
- **INIT**
- **FAILOVER_INIT**
- **STANDBY_ERROR**

例

次に、いくつか構成例を示します。

```
show role instance-id 1
result
"PRIMARY"

show role instance-id 2
result
"STANDBY"
```

## show ipam dp with type and address

インスタンス ID とリモート インスタンスのチャンクを示すフラグを表示するには、次のコマンドを使用します。

**show ipam dp { *dp_type* } { *addr_type* }**

注：

- **dp** *dp_type*：DP タイプを指定します。

• *addr_type*：IPv4/IPv6 アドレス タイプを指定します。

**例**

次に、設定例を示します。

```
show ipam dp 209.165.202.145:209.165.202.144  ipv4-addr
=====================================================================
Flag Indication: S(Static) O(Offline) R(For Remote Instance)
G:N/P Indication: G(GR InstId) N(Native NM InstId) P(Peer NM InstId)
=====================================================================
StartAddress    EndAddress      AllocContext                    Route              G:N/P
 Utilization Flag
=====================================================================
209.165.200.240 209.165.200.243 209.165.202.145:209.165.202.144 209.165.200.240/24 1:0/1
 0.00%        R
=====================================================================
```

## ipam dp を表示

この DP のチャンクを持つすべてのインスタンスを表示するには、次のコマンドを使用します。

**show ipam dp** *dp_name*

**注**：

• **dp** *dp_name*：データ プレーン割り当て名を指定します。

**例**

次に、設定例を示します。

```
show ipam dp 209.165.202.145:209.165.202.144
-----------------------------------------------------------
Ipv4Addr [Total/Used/Utilization] = 257 / 1 / 0.39%
Ipv6Addr [Total/Used/Utilization] = 0 / 0 / 0.00%
Ipv6Prefix [Total/Used/Utilization] = 2048 / 0 / 0.00%
Instance ID = 1
-----------------------------------------------------------
```

## ipam pool を表示

プールが構成されているインスタンス ID 情報を表示するには、次のコマンドを使用します。

**show ipam pool** *pool_name*

**注**：

• **pool** *pool_name*：プール名を指定します。

**例**

次に、いくつか構成例を示します。

```
show ipam pool

=============================================================================================
```

```
PoolName                     Ipv4Utilization  Ipv6AddrUtilization  Ipv6PrefixUtilization
=============================================================================================
poolv6DNN2                     0.00%            0.00%                0.00%
poolv6                         0.00%            0.00%                0.00%
poolv4vDNN                     0.00%            0.00%                0.00%
poolv4DNN2                     0.00%            0.00%                0.00%
poolv4                         0.00%            0.00%                0.00%
poolv6vDNN                     0.00%            0.00%                0.00%
poolv4DNN3                     -                -                    -
=============================================================================================

show ipam pool poolv4DNN3
----------------------------------------------------------
Ipv4Addr [Total/Used/Utilization] = 2814 / 0 / -
Ipv6Addr [Total/Used/Utilization] = 0 / 0 / -
Ipv6Prefix [Total/Used/Utilization] = 65536 / 0 / -
Instance ID = 1
isStatic = true
----------------------------------------------------------

show ipam pool poolv4
----------------------------------------------------------
 Ipv4Addr   [Total/Used/Utilization] = 2814 / 0 / 0.00%
 Ipv6Addr   [Total/Used/Utilization] = 0 / 0 / 0.00%
 Ipv6Prefix [Total/Used/Utilization] = 0 / 0 / 0.00%
 Instance ID                         = 1
----------------------------------------------------------
```

### show nrf discovery-info discovery-filter

GR インスタンス ID 情報を表示して、検出フィルタ情報が属する GR インスタンスを判別するには、次のコマンドを使用します。

**show nrf discovery-info** *nf_type* **discovery-filter**

#### 例

次に、設定例を示します。

```
=======================================================
-------------------------------------------------------
Discovery Filter: dnn=intershat;
Expiry Time: 1580146356
GR Instance ID: 1
-------------------------------------------------------
=======================================================================
```

### show nrf discovery-info

GR インスタンス ID 情報を表示して、検出情報が属する GR インスタンスを判別するには、次のコマンドを使用します。

**show nrf discovery-info**

#### 例

次に、設定例を示します。

```
show nrf discovery-info
=======================================================
------Discovered NFs:-------
    NF Type: AMF
```

```
    Number of Discovery Filters: 15
    Number of NF Profiles: 15
    GR Instance ID: 1
------Discovered NFs:-------
    NF Type: UDM
    Number of Discovery Filters: 1
    Number of NF Profiles: 3
    GR Instance ID: 2
=====================================================
```

## show nrf 登録情報

GR インスタンス ID 情報を表示して、登録情報が属する GR インスタンスを特定するには、次のコマンドを使用します。

**show nrf registration-info**

### 例

次に、設定例を示します。

```
show nrf registration-info
==========================================================================
 NF Status: Not Registered
 Registration Time:
 Active MgmtEP Name:
 Heartbeat Duration: 0
 GR Instance ID: 1
========
```

```
show nrf registration-info

==========================================================================
 Gr-instance:
 NF Status: Not Registered
 Registration Time:
 Active MgmtEP Name:
 Heartbeat Duration: 0
 Uri:
 Host Type:

==========================================================================
 Gr-instance:
 NF Status: Not Registered
 Registration Time:
 Active MgmtEP Name:
 Heartbeat Duration: 0
 Uri:
 Host Type:

==========================================================================
```

## show nrf subscription-info

サブスクリプション情報が属する GR インスタンスを判別するために GR インスタンス ID 情報を表示するには、次のコマンドを使用します。

**show nrf subscription-info**

**例**

次に、設定例を示します。

```
show nrf subscription-info
=====================================================================
NF Instance Id: f9882966-a253-32d1-8b82-c785b34a7cc9
SubscriptionID : subs123459
Actual Validity Time : 2020-01-21 12:39:45 +0000 UTC
Requested Validity Time : 2020-01-21 12:39:45 +0000 UTC
GR Instance ID: 1
=====================================================================
```

## show peers

gr-instance 対応になったピアを表示するには、次のコマンドを使用します。

**show peers all grInstance** *gr_instanceId*

（注） **grInstance** はオプションのパラメータです。**grInstance** が指定されていない場合、`show subscriber all` ではそのラックのローカル インスタンス ID が考慮されます。

**例**

次に、設定例を示します。

```
show peers all grInstance 1
                                                                    POD                CONNECTED
 ADDITIONAL  INTERFACE  GR
ENDPOINT  LOCAL ADDRESS   PEER ADDRESS     DIRECTION  INSTANCE TYPE TIME     RPC DETAILS
 NAME       INSTANCE
_____________________________________________________________________________________________
<none>  209.165.202.139 209.165.201.22:8001 Outbound rest-ep-0 Rest 10 hours UDM <none>
  n10        1
<none>  209.165.202.139 209.165.201.22:8002 Outbound rest-ep-0 Rest 10 hours AMF <none>
  n11        1
<none>  209.165.202.139 209.165.201.22:8003 Outbound rest-ep-0 Rest 10 hours PCF <none>
  n7         1
<none>  209.165.202.139 209.165.201.22:8004 Outbound rest-ep-0 Rest 10 hours CHF <none>
  n40        1
<none>  209.165.202.139 209.165.201.22:9040 Outbound rest-ep-0 Rest 10 hours CHF <none>
  n40
```

## show subscriber

gr-instance 対応にするサブスクライバの詳細を表示するには、次のコマンドを使用します。

**show subscriber { all | gr-instance** *gr_instanceId* **}**

（注） `show subscriber all` は、 ローカル インスタンス サブスクライバの詳細のみを表示します。

**gr-instance** はオプションのパラメータです。**gr-instance** が指定されていない場合、`show subscriber all` ではそのラックのローカル インスタンス ID が考慮されます。

### 例

次に、設定例を示します。

```
show subscriber gr-instance 1 all
subscriber-details
{
"subResponses": [
[
""
],
[
""
],
[
"roaming-status:homer",
"supi:imsi-123456789300001",
"gpsi:msisdn-22331010301010",
"psid:1",
"dnn:intershat",
"emergency:false",
"rat:nr",
"access:3gpp access",
"connectivity:5g",
"udm-uecm:209.165.202.150",
"udm-sdm:209.165.202.150",
"auth-status:unauthenticated",
"pcfGroupId:PCF-*",
"policy:2",
"pcf:209.165.202.152",
"upf:209.165.202.154",
"upfEpKey:209.165.202.154:209.165.202.158",
"ipv4-addr:v4pool1/209.165.200.250",
"ipv4-pool:v4pool1",
"ipv4-range:v4pool1/209.165.200.249",
"ipv4-startrange:v4pool1/209.165.200.250",
"id-index:1:0:0:32768",
"id-value:8",
"chfGroupId:CHF-*",
"chf:209.165.202.151",
"amf:209.165.202.153",
"peerGtpuEpKey:209.165.202.154:209.165.202.155",
"namespace:smf",
"nf-service:smf"
]
]
}
```

## モニタ サブスクライバ

サブスクライバのメッセージをキャプチャするには（GR インスタンス対応）、次のコマンドを使用します。

**monitor subscriber [ capture-duration** *duration* **| gr-instance** *gr_instance_id* **| imei** *imei_id* **| imsi** *imsi_value* **| internal-messages [ yes ] | namespace [ sgw | smf ] | nf-service [ sgw | smf ] | supi** *supi_id* **| transaction-logs [ yes ] ]**

（注） 2021.02 以降のリリースでは、 **namespace** キーワードは廃止され、 **nf-service** キーワードに置き換えられました。

注：

- **capture-duration** *duration*：モニタ サブスクライバを有効にする期間を秒単位で指定します。デフォルトは 300 秒（5 分）です。これは省略可能なパラメータです。
- **gr-instance** *gr_instance_id*：GR インスタンス ID を指定します。インスタンス ID 1 はローカル インスタンス ID を示しています。
- **imei** *imi_id*：サブスクライバ IMEI を指定します。例：123456789012345、*
- **imsi** *imsi_value*：サブスクライバ IMSI を指定します。たとえば、123456789、* などです。
- **internal-messages [ yes ]**：**yes** に設定されている場合、内部メッセージを有効にします。デフォルトでは、無効になっています。これは省略可能なパラメータです。
- **namespace [ sgw | smf ]**：指定した名前空間を有効にします。デフォルトでは、名前空間は none に設定されています。これは省略可能なパラメータです。

重要 このキーワードはリリース 2021.02.0 で廃止され、 **nf-service** キーワードに置き換えられました。

- **nf-service [ sgw | smf ]**：指定した NF サービスを有効にします。デフォルトでは、nf-service は none に設定されています。これは必須パラメータです。

重要 **nf-service** キーワードは、リリース 2021.02 以降では **namespace** キーワードに置き換わります。

- **supi** *supi_id*：サブスクライバ ID を指定します。例：imsi-123456789、imsi-123*
- **transaction-logs [ yes ]**：**yes** に設定されている場合はトランザクション ログを有効にします。デフォルトでは、無効になっています。これは省略可能なパラメータです。

  トランザクション履歴ログを表示するには、**dump transactionhistory** コマンドを使用します。

（注） 最新のトランザクション ログは、トランザクション ログ サイズが 1024 の循環キューに保存されます。

**例**

次に、設定例を示します。

```
monitor subscriber imsi 123456789 gr-instance 1
supi: imsi-123456789
captureDuration: 300
enableInternalMsg: false
enableTxnLog: false
namespace(deprecated. Use nf-service instead.): none
nf-service: none
gr-instance: 1
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   295  100    98  100   197  10888  21888 --:--:-- --:--:-- --:--:-- 29500
Command: --header Content-type:application/json --request POST --data
{"commandname":"mon_sub","parameters":{"supi":"imsi-123456789","duration":300,
"enableTxnLog":false,"enableInternalMsg":false,"action":"start","namespace":"none",
"nf-service":"none","grInstance":1}} http://oam-pod:8879/commands
Result start mon_sub, fileName
->logs/monsublogs/none.imsi-123456789_TS_2021-04-09T09:59:59.964148895.txt
Starting to tail the monsub messages from file:
logs/monsublogs/none.imsi-123456789_TS_2021-04-09T09:59:59.964148895.txt
Defaulting container name to oam-pod.
Use 'kubectl describe pod/oam-pod-0 -n smf' to see all the containers in this pod.
```

## モニタープロトコル

異なるインターフェイスでパケットをキャプチャするには（grインスタンス対応）、次のコマンドを使用します。

**monitor protocol { interface** *interface_name* **[ capture-duration** *duration* **| gr-instance***gr_instance* **| pcacp yes | | ] | list [ | ] }**

**注**：

- **interface** *interface_name*：PCAPがキャプチャされるインターフェイス名を指定します。このCLIでは、1つのCLIコマンドで複数のインターフェイス名を設定できます。
- **capture-duration** *duration*：pcapがキャプチャされる期間を秒単位で指定します。デフォルトは300秒（5分）です。
- 構成されたインターフェイス名は**show endpoint**、CLIコマンドを使用して取得できます。
- **gr-instance** *gr_instance_id*：GRインスタンスIDを指定します。インスタンスID 1はローカルインスタンスIDを示しています。
- **pcap yes**：このオプションを構成すると、PCAPファイルの生成が有効になります。デフォルトでは、このオプションは無効になっています。
- **list**：プロトコルリストファイルをモニタします。

**例**

次に、設定例を示します。

```
monitor protocol interface sbi gr-instance 1
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   220  100    95  100   125   8636  11363 --:--:-- --:--:-- --:--:-- 20000
Command: --header Content-type:application/json --request POST --data
{"commandname":"mon_pro","parameters":{"interface":"sbi","duration":300,"action":
"start","enable_pcap":false,"grInstance":1}} http://oam-pod:8879/commands
Result start mon_pro, fileName
->logs/monprologs/sessintfname_sbi_at_2021-04-30T05:26:22.712229347.txt
Starting to tail the monpro messages from file:
logs/monprologs/sessintfname_sbi_at_2021-04-30T05:26:22.712229347.txt
Defaulting container name to oam-pod.
Use 'kubectl describe pod/oam-pod-0 -n cn' to see all of the containers in this pod.
```

# 地理的冗長 OAM サポート

ここでは、この機能の操作、管理、およびメンテナンスに関して説明します。

## ヘルス チェック

次のセクションでは、GR セットアップの正常性チェックに関する情報を提供します。

- すべての重要なポッドは、ユーザー トラフィックを処理できる良好な状態です。

  GR および CDL に関連するポッドが実行状態にあるかどうかを確認するには、次のコマンドを使用します。

  ```
  kubectl get pods -n cn-cn1 -o wide | grep georeplication-pod
  kubectl get pods -n cn-cn1 -o wide | grep cdl
  kubectl get pods -n cn-cn1 -o wide | grep mirror-maker
  ```

- キープアライブ ポッドは正常な状態になり、check-interface/check-port 用に構成されたすべての VIP をモニタリングします。

  次のコマンドを使用して、「smi-vips」名前空間のキープアライブ ポッドが「実行」状態であるかどうかを確認します。

  ```
  kubectl get pods -n smi-vips
  ```

- CDL に関連するポッドの正常性チェック：CDL DB エンドポイント、スロット、およびインデックスのステータスを確認します。システム ID 1 と 2 の両方で、すべてのが STARTED または ONLINE 状態になっている必要があります。

  ```
  cdl show status
  message params: {cmd:status mode:cli dbName:session sessionIn:{mapId:0 limit:500
  key: purgeOnEval:0 filters:[] nextEvalTsStart:0 nextEvalTsEnd:0 allReplicas:false
  maxDataSize:4096} sliceName:}
  db-endpoint {
      endpoint-site {
          system-id 1
          state STARTED
          total-sessions 4
          site-session-count 2
          total-reconciliation 0
          remote-connection-time 66h37m31.36054781s
          remote-connection-last-failure-time 2021-07-13 11:24:10.233825924 +0000 UTC

          slot-geo-replication-delay 2.025396ms
      }
  ```

```
    endpoint-site {
        system-id 2
        state STARTED
        total-sessions 4
        site-session-count 2
        total-reconciliation 0
        remote-connection-time 66h58m49.83449066s
        remote-connection-last-failure-time 2021-07-13 11:02:51.759971655 +0000 UTC

        slot-geo-replication-delay 1.561816ms
    }
}
slot {
    map {
        map-id 1
        instance {
            system-id 1
            instance-id 1
            records 4
            capacity 2500000
            state ONLINE
            avg-record-size-bytes 1
            up-time 89h38m37.335813523s
            sync-duration 9.298061ms
        }
        instance {
            system-id 1
            instance-id 2
            records 4
            capacity 2500000
            state ONLINE
            avg-record-size-bytes 1
            up-time 89h39m11.1268024s
            sync-duration 8.852556ms
        }
        instance {
            system-id 2
            instance-id 1
            records 4
            capacity 2500000
            state ONLINE
            avg-record-size-bytes 1
            up-time 89h28m38.274713022s
            sync-duration 8.37766ms
        }
        instance {
            system-id 2
            instance-id 2
            records 4
            capacity 2500000
            state ONLINE
            avg-record-size-bytes 1
            up-time 89h29m37.934345015s
            sync-duration 8.877442ms
        }
    }
}
index {
    map {
        map-id 1
        instance {
            system-id 1
            instance-id 1
            records 4
```

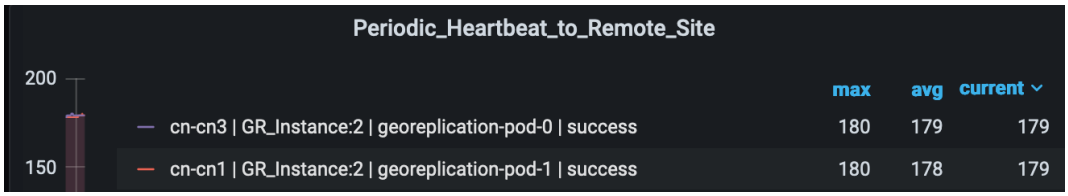
```
            capacity 60000000
            state ONLINE
            up-time 89h38m16.119032086s
            sync-duration 2.012281769s
            leader false
            geo-replication-delay 10.529821ms
        }
        instance {
            system-id 1
            instance-id 2
            records 4
            capacity 60000000
            state ONLINE
            up-time 89h39m8.47664588s
            sync-duration 2.011171261s
            leader true
            leader-time 89h38m53.761213379s
            geo-replication-delay 10.252683ms
        }
        instance {
            system-id 2
            instance-id 1
            records 4
            capacity 60000000
            state ONLINE
            up-time 89h28m29.5479133s
            sync-duration 2.012101957s
            leader false
            geo-replication-delay 15.974538ms
        }
        instance {
            system-id 2
            instance-id 2
            records 4
            capacity 60000000
            state ONLINE
            up-time 89h29m11.633496562s
            sync-duration 2.011566639s
            leader true
            leader-time 89h28m51.29928233s
            geo-replication-delay 16.213323ms
        }
    }
}
```

- CDL レプリケーション ステータス

  **[CDLレプリケーション統計（CDL Replication Stats）]** Grafana ダッシュボードの **[GRPC_Connections_to_RemoteSite]** パネルのラック全体で、（各名前空間の）CDL EP セッションポッド間で 4 つの gRPC 接続が確立されているかどうかを確認します。両方のラックで Grafana をチェックします。

- Geo レプリケーション用のラック間の管理ポート ステータス。

  **[GR 統計情報（GR Statistics）]** Grafana ダッシュボードの **[Periodic_Heartbeat_to_Remote_Site]** パネルで、ラック全体の Geo レプリケーション ポッド間のハートビート メッセージを確認します。



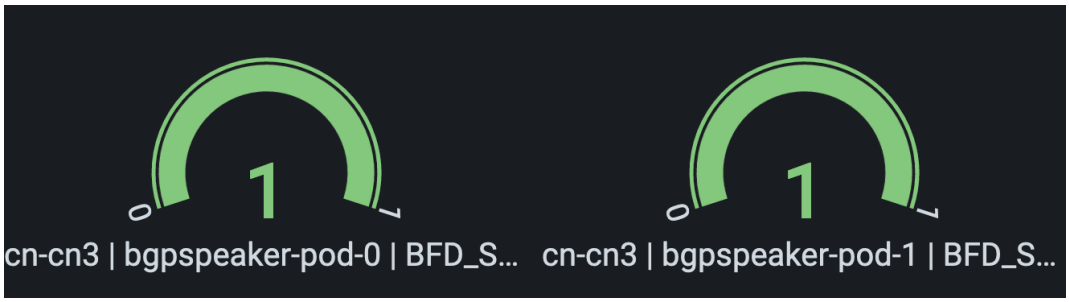

- ラック上の BGP/BFD リンク ステータス

  BGP ピアとの隣接関係が確立されているかどうかを、 **[BGP、BFD 統計情報（BGP, BFD Statistics）]** Grafan ダッシュボードの **[BGP ピア（BGP Peers）]** パネルで確立しているかどうかを確認します。

BGP Peers

| Time | as_path | namespace 1 | peer_ip | pod | Value |
|---|---|---|---|---|---|
| 2021-07-16 06:29:18 | 3333 | cn-cn1 | 192.204.10.6 | bgpspeaker-pod-0 | 1 |
| 2021-07-16 06:29:18 | 3333 | cn-cn1 | 192.204.10.6 | bgpspeaker-pod-1 | 1 |
| 2021-07-16 06:29:18 | 3333 | cn-cn3 | 192.204.18.6 | bgpspeaker-pod-0 | 1 |
| 2021-07-16 06:29:18 | 3333 | cn-cn3 | 192.204.18.6 | bgpspeaker-pod-1 | 1 |

BFD リンクが接続状態であるかどうかを、**[BGP、BFD 統計情報（BGP, BFD Statistics）]** Grafana ダッシュボードの **[BFD リンク ステータス（BFD Link Status）]** パネルで確認します。




- 各インスタンスのロールが正常な状態である

  各ラックのロールがどの時点においても STANDBY_ERROR 状態でないことを確認します。

  - **アクティブ/スタンバイ モデル**：ロールは各ラックで次の状態である必要があります。

    **Rack-1**：

    ```
    show role instance-id 1
    result "PRIMARY"
    show role instance-id 2
    result "PRIMARY"
    ```

    **Rack-2**：

    ```
    show role instance-id 1
    result "STANDBY"
    show role instance-id 2
    result "STANDBY"
    ```

  - **アクティブ/アクティブ モデル**：ロールは、各ラックで次の状態になっている必要があります。

    **Rack-1**：

    ```
    show role instance-id 1
    result "PRIMARY"
    show role instance-id 2
    result "STANDBY"
    ```

    **Rack-2**：

    ```
    show role instance-id 1
    result "STANDBY"
    show role instance-id 2
    result "PRIMARY"
    ```

# 回復手順

### Rack-1 上

1. Rack-1 の両方のインスタンスのロールが STANDBY_ERROR であることを確認します。

   ```
   show role instance-id 1
   result "STANDBY_ERROR"

   show role instance-id 2
   result "STANDBY_ERROR"
   ```

2. Rack-1 の両方のインスタンスのロールの STANDBY へのリセットを開始します。このステップにより、ロールが STANDBY_ERROR/STANDBY_ERROR から STANDBY/STANDBY に移行します。

```
geo reset-role instance-id 1 role standby
geo reset-role instance-id 2 role standby
```

3. ラック 1 両方のインスタンスのロールがの STANDBY に変わったことを確認します。

```
show role instance-id 1
result "STANDBY"

show role instance-id 2
result "STANDBY"
```

4. フェールバック間隔を 0 秒にして、Rack-2 で instance-id 1 のインスタンスのロールの STANDBY への切り替えを開始します。このステップにより、Rack-2 のロールが PRIMARY/PRIMARY から STANDBY_ERROR/PRIMARY に、Rack-1 のロールが STANDBY/STANDBY から PRIMARY/STANDBY に移行します。

```
geo switch-role instance-id 1 role standby [failback-interval 0]
```

5. Rack-2 の両方のインスタンスのロールが STANDBY_ERROR/PRIMARY にあることを確認します。

```
show role instance-id 1
result "STANDBY_ERROR"

show role instance-id 2
result "PRIMARY"
```

6. Rack-1 の両方のインスタンスのロールが PRIMARY/STANDBY であることを確認します。

```
show role instance-id 1
result "PRIMARY"

show role instance-id 2
result "STANDBY"
```

7. STANDBY への Rack-2 の instance-id 1 のロールのリセットを開始します。このステップにより、Rack-2 のロールが STANDBY_ERROR/PRIMARY から STANDBY/PRIMARY に移行します。

```
geo reset-role instance-id 1 role standby
```

8. Rack-2 のロールが STANDBY/PRIMARY であることを確認します。

```
show role instance-id 1
result "STANDBY"

show role instance-id 2
result "PRIMARY"
```

### Rack-2 上

1. Rack-2 の両方のインスタンスのロールが STANDBY_ERROR であることを確認します。

```
show role instance-id 1
result "STANDBY_ERROR"

show role instance-id 2
result "STANDBY_ERROR"
```

2. Rack-2 の両方のインスタンスのロールの STANDBY へのリセットを開始します。このステップにより、ロールが STANDBY_ERROR/STANDBY_ERROR から STANDBY/STANDBY に移行します。

```
geo reset-role instance-id 1 role standby
geo reset-role instance-id 2 role standby
```

3. 両方のインスタンスのロールが Rack-2 の STANDBY に移動することを確認します。

```
show role instance-id 1
result "STANDBY"

show role instance-id 2
result "STANDBY"
```

4. ラック 1 の instance-id 2 のロールの STANDBY への切り替えを開始します。このステップでは、Rack-1 のロールを PRIMARY/PRIMARY から PRIMARY/STANDBY_ERROR に、Rack-2 のロールを STANDBY/STANDBY から STANDBY/PRIMARY に移行します。

```
geo switch-role instance-id 2 role standby [failback-interval 0]
```

5. Rack-1 のインスタンスのロールが PRIMARY/STANDBY_ERROR モードであることを確認します。

```
show role instance-id 1
result "PRIMARY"

show role instance-id 2
result "STANDBY_ERROR"
```

6. Rack-2 のインスタンスのロールが STANDBY/PRIMARY モードであることを確認します。

```
show role instance-id 1
result "STANDBY"

show role instance-id 2
result "PRIMARY"
```

7. Rack-1 の instance-id 2 の STANDBY へのロールのリセットを開始します。この手順では、Rack-1 のロールを PRIMARY/STANDBY_ERROR から PRIMARY/STANDBY に移行します。

```
geo reset-role instance-id 2 role standby
```

8. Rack-1 のインスタンスのロールが PRIMARY/STANDBY であることを確認します。

```
show role instance-id 1
result "PRIMARY"

show role instance-id 2
result "STANDBY"
```

# 主要業績評価指標（KPI）

次の項では、KPI について説明します。

### ETCD/Cachepod の複製 KPI

次の表に、ETCD/Cachepod 複製 KPI のリストを記載します。

表 *442 : geo_replication_total KPI*

| KPI 名 | 説明 | ラベル | 有効な値 |
|---|---|---|---|
| geo_replication _total | このKPIには、さまざまな同期タイプと複製タイプの複製要求/応答の総数が表示されます。 | ReplicationRequest タイプ | 要求/応答 |
| | | ReplicationSync タイプ | 即時/遅延/プル |
| | | ReplicationNode | ETCD / CACHE_POD / PEER |
| | | ReplicationReceiver | ローカル/リモート |
| | | status | True/False |
| | | status_code | エラーコード/説明 |

### 地理的なロール変更拒否の KPI

次の表に、地理的なロール変更拒否の KPI のリストを記載します。

表 *443 :* 地理的なロール変更拒否の *KPI*

| KPI 名 | 説明 | ラベル | 有効な値 |
|---|---|---|---|
| geo_RejectedRole Changed_total | このKPIには、スタンバイインスタンスの拒否された要求や受信したコールの合計数が表示されます。カウントの後、同じインスタンスがPRIMARYに移行されます。 | RejectedCount | スタンバイインスタンスに対して受信された拒否されたコール/要求を示す数の値。 |
| | | GRInstance 番号 | 1/2 |

### KPI のモニタリング

次の表に、KPI のモニタリングを示します。

表 *444 : geo_monitoring_total KPI*

| KPI 名 | 説明 | ラベル | 有効な値 |
|---|---|---|---|
| geo_monitoring_total | このKPIには、ハートビート/リモート通知/トリガーGRなど、さまざまな種類の成功/失敗メッセージの総数が表示されます。 | ControlAction タイプ | AdminMonitoring<br>ActionType / AdminRemote<br>MessageAction<br>タイプ/AdminRole<br>ChangeActionType |
| | | ControlAction NameType | MonitorPod/MonitorBfd/<br>RemoteMsgHeartbeat/<br>RemoteMsgNotifyFailover/<br>RemoteMsgNotify<br>PrepareFailover /<br>RemoteMsgGetSiteStatus /<br>RemoteClusterPodFailure /<br>RemoteSiteRole<br>Monitoring /<br>TriggerGRApi /<br>ResetRoleApi |
| | | 管理者ノード | 任意の文字列値。例：GRインスタンス ID またはインスタンスキー/ポッド名 |
| | | ステータス コード | 0/1001/1002/1003/<br>1004 / 1005 / 1006 / 1007 /<br>1008/受信エラー コード（1206, 1219, 2404, ...） |
| | | ステータス メッセージ | |

| KPI 名 | 説明 | ラベル | 有効な値 |
|---|---|---|---|
| | | | 成功 (0) /<br>STANDBY_ERROR => ANDBY/STANDBY STANDBY => PRIMARY (0) / Pod Failure (0) /<br>CLI (0) / BFD Failure (0) /<br>デコード失敗 (1001) /<br>リモート ステータスが使用不可（1002）/<br>ターゲット ロールは (1002) をサポートしていません /<br>ポッド障害（1002）/<br>CLI (1002) / BFD の障害 (1002) /<br>サイトがダウンしています(1003) / ポッド障害(1003) /<br>CLI (1003) / BFD の障害 (1003) /<br>トラフィック ヒット（1004）/<br>ポッドエラー(1004) / CLI(1004) /<br>BFD の障害 (1004) /現在のロールは以下ではありません<br>STANDBY_ERROR/<br>STANDBY（リセットによりスタンバイ）<br>role (1005) / resetRole：<br>etcd でキーが見つかりませんでした (1006) /<br>ポッドあたりの<br>ポッド侵害（1007）/<br>ハートビートの再試行<br>障害(1008) /<br>エラーメッセージを受信しました(この要求に使用可能なリモートホストがありません/選択されたリモートホスト<remotehostname>クライアント接続がありません/ SLA がトランザクションに対して期限切れです / ...） |

表 *445 : geo_replication_finalpull_total KPI*

| KPI 名 | 説明 | ラベル名 | 有効な値 |
|---|---|---|---|
| geo_replication _finalpulld_total | この KPI には、機能メッセージの最終取得時点で存在する Geo レプリケーションの総数が表示されます。 | **MessageType** | これは要求または応答のメッセージタイプです。 |
| | | **TotalTimeTaken** | これは、リクエストの処理にかかった合計時間です。 |
| | | **GRInstanceNumber** | これは、次のリストにある GR インスタンス ID の番号です。<br>• 1<br>• 2<br>• Instance.1<br>• Instance.2 |

## BFD KPI

次の表に、BFD KPI を示します。

表 *446 : BFD KPI - 1*

| KPI 名 | 説明 | ラベル | 有効な値 |
|---|---|---|---|
| bgp_speaker _bfd_status | この KPI には、BGP スピーカーの BFD リンクステータスが表示されます。 | status | STATE_UP / STATE_DOWN |
| geo_bfd_ status | この KPI には、Geo POD の BFD リンク ステータスが表示されます。 | status | STATE_UP / STATE_DOWN |

表 *447 : BFD KPI - 2*

| KPI 名 | 説明 | ゲージ |
|---|---|---|
| bgp_speaker _bfd_status | この KPI には、BGP スピーカーの BFD リンクステータスが表示されます。 | 1（UP）または 0（DOWN） |

| KPI 名 | 説明 | ゲージ |
|---|---|---|
| geo_bfd_<br>status | この KPI には、Geo POD の BFD リンク ステータスが表示されます。 | 1（UP）または 0（DOWN） |

### GR インスタンス情報

**表 *448 : GR* インスタンス情報 *KPI***

| KPI 名 | 説明 | ラベル | 有効な値 |
|---|---|---|---|
| gr_instance_<br>information (Type – Guage) | この KPI には、アプリケーションでの GR インスタンスの現在のロールが表示されます。 | gr_instance_id | 設定された GR インスタンス値（数値） |

### Geo メンテナンス モード

**表 *449 : Geo* メンテナンス モードの *KPI***

| KPI 名 | 説明 | ラベル | 有効な値 |
|---|---|---|---|
| geo_MaintenanceMode<br>info（Type -Ugage） | この KPI には、ラックのメンテナンスモードの現在の状態が表示されます。 | MaintenanceMode | 0 = False<br>1 = True |

## バルク統計

次のセクションでは、GR 固有のバルク統計情報について詳しく説明します。

```
bulk-stats query GR-BGP-Incoming-Failed-Routes
 expression "sum(bgp_incoming_failedrouterequest_total) by (namespace, interface,
service_IP, next_hop, instance_id)"
 labels     [ instance_id interface next_hop service_IP ]
 alias      gr-bgp-routes-in
exit
bulk-stats query GR-Geo-Monitoring-Failure
 expression
"sum(geo_monitoring_total{ControlActionNameType=~'MonitorPod|RemoteMsgHeartbeat|
RemoteMsgGetSiteStatus|RemoteSiteRoleMonitoring|RemoteClusterPodFailure|RemoteMsgNotifyFailover|
RemoteMsgNotifyPrepareFailover|MonitorVip',status!~'success|monitoring.*'}) by (namespace,

AdminNode, ControlActionType, ControlActionNameType,  pod, status, status_code)"
 labels     [ pod AdminNode ControlActionNameType status status_code ]
 alias      gr-geo-monitoring-failure
exit
bulk-stats query GR-Geo-Monitoring-Success
 expression
"sum(geo_monitoring_total{ControlActionNameType=~'MonitorPod|RemoteMsgHeartbeat|
```

```
RemoteMsgGetSiteStatus|RemoteSiteRoleMonitoring|RemoteClusterPodFailure|RemoteMsgNotifyFailover|
RemoteMsgNotifyPrepareFailover',status=~'success|monitoring.*'}) by (namespace, AdminNode,

ControlActionType, ControlActionNameType,  pod, status)"
 labels     [ pod AdminNode ControlActionNameType status ]
 alias      gr-geo-monitoring
exit
bulk-stats query GR-Geo-Monitoring-Total
 expression
"sum(geo_monitoring_total{ControlActionNameType=~'MonitorPod|RemoteMsgHeartbeat|
RemoteMsgGetSiteStatus|RemoteSiteRoleMonitoring|RemoteClusterPodFailure|RemoteMsgNotifyFailover
|RemoteMsgNotifyPrepareFailover|MonitorVip'})
by (namespace, AdminNode, ControlActionType, ControlActionNameType,  pod, status)"
 labels     [ pod AdminNode ControlActionNameType status ]
 alias      gr-geo-monitoring
exit
bulk-stats query GR-Geo-Replication-Failure
 expression
"sum(geo_replication_total{ReplicationNode=~'CACHE_POD|ETCD|PEER',status!='success',
ReplicationRequestType='Response'}) by (namespace, ReplicationNode, ReplicationSyncType,
ReplicationReceiver,ReplicationRequestType,status,status_code)"
 labels     [ pod ReplicationNode ReplicationReceiver ReplicationRequestType
ReplicationSyncType status status_code ]
 alias      gr-geo-replication-failure
exit
bulk-stats query GR-Geo-Replication-Success
 expression "sum(geo_replication_total{ReplicationNode=~'CACHE_POD|ETCD|PEER',
status='success',ReplicationRequestType='Response'}) by (namespace, ReplicationNode,
ReplicationSyncType,ReplicationReceiver,ReplicationRequestType,status)"
 labels     [ pod ReplicationNode ReplicationReceiver ReplicationRequestType
ReplicationSyncType status ]
 alias      gr-geo-replication-success
exit
bulk-stats query GR-Geo-Replication-Total
 expression "sum(geo_replication_total{ReplicationNode=~'CACHE_POD|ETCD|PEER'})
by (namespace, ReplicationNode, ReplicationSyncType,ReplicationReceiver,
ReplicationRequestType,pod)"
 labels     [ pod ReplicationNode ReplicationReceiver ReplicationRequestType
ReplicationSyncType ]
 alias      gr-geo-replication-total
exit
bulk-stats query GR-Trigger-ResetRole-Api
 expression "sum(geo_monitoring_total{ControlActionNameType=~'TriggerGRApi|ResetRoleApi'})

by (namespace, AdminNode, ControlActionType, ControlActionNameType,  pod, status,
status_code)"
 labels     [ pod AdminNode ControlActionNameType status status_code ]
 alias      gr-api
exit
bulk-stats query GR-CDL-Index-Replication
 expression "sum(consumer_kafka_records_total) by (pod, origin_instance_id)"
 labels     [ origin_instance_id pod ]
 alias      gr-cdl-index-replication
exit
bulk-stats query GR-CDL-Inter-Rack-Replications-Failures
 expression "sum(datastore_requests_total{local_request='0',errorCode!='0'}) by
(operation,sliceName,errorCode)"
 labels     [ sliceName operation errorCode ]
 alias      gr-cdl-inter-rack-replications
exit
bulk-stats query GR-CDL-Inter-Rack-Replications-Success
 expression "sum(datastore_requests_total{local_request='0',errorCode='0'}) by
(operation,sliceName,errorCode)"
 labels     [ sliceName operation errorCode ]
```

```
 alias      gr-cdl-inter-rack-replications
exit
bulk-stats query GR-CDL-Inter-Rack-Replications-Total
 expression "sum(datastore_requests_total{local_request='0'}) by
(operation,sliceName,errorCode)"
 labels     [ sliceName operation errorCode ]
 alias      gr-cdl-inter-rack-replications
exit
bulk-stats query GR-CDL-Intra-Rack-Operations-Failures
 expression "sum(datastore_requests_total{local_request='1',errorCode!='0'}) by
(operation,sliceName,errorCode)"
 labels     [ sliceName operation errorCode ]
 alias      gr-cdl-intra-rack-operations
exit
bulk-stats query GR-CDL-Intra-Rack-Operations-Success
 expression "sum(datastore_requests_total{local_request='1',errorCode='0'}) by
(operation,sliceName,errorCode)"
 labels     [ sliceName operation errorCode ]
 alias      gr-cdl-intra-rack-operations
exit
bulk-stats query GR-CDL-Intra-Rack-Operations-Total
 expression "sum(datastore_requests_total{local_request='1'}) by
(operation,sliceName,errorCode)"
 labels     [ errorCode operation sliceName ]
 alias      gr-cdl-intra-rack-operations
exit
bulk-stats query GR-CDL-Session-Count-Per-Slice
 expression
sum(avg(db_records_total{namespace=~'$namespace',session_type='total'})by(systemId,sliceName))by(sliceName)

 labels     [ sliceName ]
 alias      gr-cdl-session-count-per-slice
exit
bulk-stats query GR-CDL-Session-Count-Per-System-ID
 expression sum(avg(db_records_total{namespace=~'$namespace',session_type='total'})
by(systemId,sliceName))by(systemId)
 labels     [ systemId ]
 alias      gr-cdl-session-count-per-system-id
exit
bulk-stats query GR-CDL-Slot-Records-Per-Slice
 expression "sum(slot_records_total{pod=~'.*',systemId!=''}) by (pod, sliceName)"
 labels     [ pod sliceName ]
 alias      gr-cdl-slot-records-per-slice
exit
bulk-stats query GR-CDL-Slot-Records-Per-System-ID
 expression "sum(slot_records_total{pod=~'.*',systemId!=''}) by (pod, systemId)"
 labels     [ pod systemId ]
 alias      gr-cdl-slot-records-per-system-id
exit
bulk-stats query GR-CDL-Total-Session-Count
 expression "sum(db_records_total{namespace=~'$namespace',session_type='total'}) by
(systemId,sliceName)"
 labels     [ sliceName systemId ]
 alias      gr-cdl-total-session-count
exit
```

GR 関連の統計の詳細については、次を参照してください。

- RADIUS統計では、grInstIdラベルを使用してGR固有の統計をフィルタリングできます。

  詳細については、「*UCC5G*セッション管理機能 - メトリック参照」を参照してください。

- GTP エンドポイント統計情報で、gr_instance_id ラベルを使用して GR 固有の統計情報をフィルタリングできます。

詳細については、「*UCC 5G*セッション管理機能 - メトリック参照」を参照してください。

- SMF 統計では、gr_instance_id label を使用して GR 固有の統計をフィルタリングできます。

  詳細については、「*UCC 5G*セッション管理機能 - メトリック参照」を参照してください。

- REST エンドポイント統計情報で、gr_instance_id ラベルを使用して GR 固有の統計情報をフィルタリングできます。

  詳細については、「*UCC 5G*セッション管理機能 - メトリック参照」を参照してください。

- IPAM 関連の統計では、grInstId ラベルを使用して GR 固有の統計をフィルタリングできます。

  詳細については、「*UCC 5G*セッション管理機能 - メトリック参照」を参照してください。

# アラート

ここでは、GR アラートについて詳しく説明します。

### BFD アラート

次の表に、 *interval-seconds* が 60 に設定されたルールグループ BFD のアラートを示します。

**表 *450* : アラートルールグループ : *BFD***

| アラートルール | 重大度 | 期間（分単位） | タイプ |
|---|---|---|---|
| BFD-Link-Fail | critical | 1 | 通信アラーム |
| | **Expression:**sum by (namespace,pod,status)<br>(bgp_speaker_bfd_status{status='BFD_STATUS'}) == 0<br>**説明**：このアラートは、BGP ピアリングに関連付けられた BFD リンクがダウンしている場合に生成されます。 | | |

### GR アラート

次の表に、interval-seconds が 60 に設定されているルールグループ GR のアラートを示します。

表 *451 :* アラートルールグループ：*GR*

| アラートルール | 重大度 | 期間（分単位） | タイプ |
|---|---|---|---|
| Cache-POD-Replication-Immediate-Local | critical | 1 | 通信アラーム |
| | **Expression:** (sum by (namespace)<br>(increase(geo_replication_total{ReplicationNode='CACHE_POD',<br>ReplicationSyncType='Immediate',ReplicationReceiver='local',<br>ReplicationRequestType = 'Response',status='success' ([1m]))/sum by (namespace)<br>(increase(geo_replication_total{ReplicationNode='CACHE_POD',<br>ReplicationSyncType='Immediate',ReplicationReceiver='local',<br>ReplicationRequestType='Request'}[1m]))*100 < 90<br>**説明**：このアラートは、CACHE_POD sync type:Immediate および replication receiver:Local の成功率がしきい値未満の場合に生成されます。 | | |
| Cache-POD-Replication-Immediate-Remote | critical | 1 | 通信アラーム |
| | **Expression:** (sum by (namespace)<br>(increase(geo_replication_total{ReplicationNode='CACHE_POD',<br>ReplicationSyncType='Immediate',ReplicationReceiver='remote',<br>ReplicationRequestType = 'Response',status='success' ([1m]))/sum by (namespace)<br>(increase(geo_replication_total{ReplicationNode='CACHE_POD',<br>ReplicationSyncType='Immediate',ReplicationReceiver='remote',<br>ReplicationRequestType='Request'}[1m]))*100 < 90<br>**説明**：このアラートは、CACHE_POD sync type:Immediate および replication receiver:Remote の成功率がしきい値未満の場合に生成されます。 | | |

| アラートルール | 重大度 | 期間（分単位） | タイプ |
|---|---|---|---|
| Cache-POD-Replication-PULL-Remote | critical | 1 | 通信アラーム |
| | **Expression:** (sum by (namespace)<br>(increase(geo_replication_total{ReplicationNode='CACHE_POD',<br>ReplicationSyncType='PULL',ReplicationReceiver='remote',<br>ReplicationRequestType = 'Response',status='success' ([1m]))/sum by (namespace)<br>(increase(geo_replication_total{ReplicationNode='CACHE_POD',<br>ReplicationSyncType='PULL',ReplicationReceiver='remote',<br>ReplicationRequestType='Request'}[1m]))*100 < 90<br>**説明**：このアラートは、CACHE_POD sync type:PULL および replication receiver:Remote の成功率がしきい値未満の場合に生成されます。 | | |
| ETCD-Replication-Immediate-Local | critical | 1 | 通信アラーム |
| | **Expression:** (sum by (namespace)<br>(increase(geo_replication_total{ReplicationNode='ETCD',<br>ReplicationSyncType='Immediate',ReplicationReceiver='local',<br>ReplicationRequestType='Response',status='success'}[1m]))/sum by (namespace)<br>(increase(geo_replication_total{ReplicationNode='ETCD',<br>ReplicationSyncType='Immediate',ReplicationReceiver='local',<br>ReplicationRequestType='Request'}[1m]))*100 < 90<br>**説明**：このアラートは、ETCD 同期タイプ：Immediate およびレプリケーションレシーバ：Local の成功率がしきい値未満の場合に生成されます。 | | |

| アラートルール | 重大度 | 期間（分単位） | タイプ |
|---|---|---|---|
| ETCD-Replication-Immediate-Remote | critical | 1 | 通信アラーム |
| | **Expression:** (sum by (namespace) (increase(geo_replication_total{ReplicationNode='ETCD', ReplicationSyncType='Immediate',ReplicationReceiver='remote', ReplicationRequestType = 'Response',status='success' ([1m]))/sum by (namespace) (increase(geo_replication_total{ReplicationNode='ETCD', ReplicationSyncType='Immediate',ReplicationReceiver='remote', ReplicationRequestType='Request'}[1m])))*100 < 90<br>**説明**： このアラートは、ETCD 同期タイプ：Immediate およびレプリケーションレシーバ：リモートの成功率がしきい値未満の場合に生成されます。 | | |
| ETCD-Replication-PULL-Remote | critical | 1 | 通信アラーム |
| | **Expression:**(sum by (namespace) (increase(geo_replication_total{ReplicationNode='ETCD', ReplicationSyncType='PULL',ReplicationReceiver='remote', ReplicationRequestType = 'Response',status='success')/ sum by (namespace) (increase(geo_replication_total {ReplicationNode='ETCD',ReplicationSyncType='PULL', ReplicationReceiver='remote',ReplicationRequestType= 'Request'}[1m])))*100 < 90<br>**説明**： このアラートは、ETCD 同期タイプ：PULL およびレプリケーションレシーバ：リモートの成功率がしきい値未満の場合に生成されます。 | | |
| Heartbeat-Remote-Site | critical | - | 通信アラーム |
| | **Expression:** sum by (namespace) (increase(geo_monitoring_total{ControlActionNameType= 'RemoteMsgHeartbeat',status!='success'}[1m])) > 0<br>**説明**： このアラートは、リモートサイトへの定期的なハートビートが失敗するとトリガーされます。 | | |

| アラートルール | 重大度 | 期間（分単位） | タイプ |
|---|---|---|---|
| Local-Site-POD-Monitoring | critical | - | 通信アラーム |
| | **Expression:** sum by (namespace,AdminNode) (increase(geo_monitoring_total{ControlActionNameType ='MonitorPod'}[1m])) > 0<br>**説明**： このアラートは、ローカルサイトのポッドモニタリングに障害が発生した場合、ラベルにラベルで示されているポッドの設定済みしきい値を超えた場合にトリガーされます。 | | |
| PEER-Replication-Immediate-ローカル | critical | 1 | 通信アラーム |
| | **Expression:** (sum by (namespace) (increase(geo_replication_total{ReplicationNode='PEER', ReplicationSyncType='Immediate',ReplicationReceiver='local', ReplicationRequestType='Response',status='success'} [1m]))/sum by (namespace) (increase(geo_replication_total {ReplicationNode='PEER',ReplicationSyncType= 'Immediate',ReplicationReceiver='local', ReplicationRequestType='Request'}[1m])))*100 < 90<br>**説明**： このアラートは、PEER 同期タイプ：Immediate およびレプリケーション レシーバ：Local の成功率がしきい値未満の場合に生成されます。 | | |
| PEER-Replication-Immediate-リモート | critical | 1 | 通信アラーム |
| | **Expression:** (sum by (namespace) (increase(geo_replication_total{ReplicationNode='PEER', ReplicationSyncType='Immediate',ReplicationReceiver='remote', ReplicationRequestType='Response',status='success'} [1m]))/sum by (namespace) (increase(geo_replication_total {ReplicationNode='PEER',ReplicationSyncType='Immediate', ReplicationReceiver='remote',ReplicationRequestType= 'Request'}[1m])))*100 < 90<br>**説明**： このアラートは、PEER 同期タイプ：Immediate およびレプリケーションレシーバ：Remote の成功率がしきい値未満の場合に生成されます。 | | |

| アラートルール | 重大度 | 期間（分単位） | タイプ |
|---|---|---|---|
| RemoteCluster-PODFailure | critical | - | 通信アラーム |
| | **Expression:** sum by (namespace,AdminNode) (increase(geo_monitoring_total{ControlActionNameType ='RemoteClusterPodFailure'}[1m])) > 0<br>**説明**： このアラートは、ラベルに記載されているポッドのリモートサイトでポッド障害が検出された場合に生成されます。 | | |
| RemoteMsg NotifyFailover | critical | 1 | 通信アラーム |
| | **Expression:** sum by (namespace,status) (increase(geo_monitoring_total{ControlActionNameType ='RemoteMsgNotifyFailover',status!='success'}[1m])) > 0<br>**説明**： このアラートは、ラベルに記載されている理由で一時的なロール RemoteMsgNotifyFailover が失敗した場合に生成されます。 | | |
| RemoteMsg NotifyPrepare フェールオーバー | critical | 1 | 通信アラーム |
| | **Expression:** sum by (namespace,status) (increase(geo_monitoring_total{ControlActionNameType ='RemoteMsgNotifyPrepareFailover',status!='success'}[1m])) > 0<br>**説明**： このアラートは、ラベルに記載されている理由で一時的なロール RemoteMsgNotifyPrepareFailover が失敗した場合に生成されます。ライセンスは次のようになります。 | | |
| RemoteSite-RoleMonitoring | critical | - | 通信アラーム |
| | **Expression:** sum by (namespace,AdminNode) (increase(geo_monitoring_total{ControlActionNameType ='RemoteSiteRoleMonitoring'}[1m])) > 0<br>**説明**： このアラートは、RemoteSiteRoleMonitoring がパートナーラックのインスタンスのロールの不整合を検出し、それに応じてローカルラックのそれぞれのインスタンスのロールをプライマリに変更した場合に生成されます。影響を受けるインスタンスは Label:{{$labels.AdminNode}} にあります。 | | |

| アラートルール | 重大度 | 期間（分単位） | タイプ |
|---|---|---|---|
| ResetRoleApi -Initiated | critical | - | 通信アラーム |
| | **Expression:** sum by (namespace,status) (increase(geo_monitoring_total{ControlActionNameType ='ResetRoleApi'}[1m])) > 0<br>**説明**： このアラートは、Label::$labels.status)] で言及されているロールの状態遷移で ResetRoleApi が開始されたときに生成されます。 | | |
| TriggerGRApi -Initiated | critical | - | 通信アラーム |
| | **Expression:** sum by (namespace,status) (increase(geo_monitoring_total{ControlActionNameType ='TriggerGRApi'}[1m])) > 0<br>**説明**： このアラートは、ラベルに記載されている理由でTriggerGRApiが開始されたときに生成されます。 | | |
| VIP-Monitoring -Failures | critical | - | 通信アラーム |
| | **Expression:** sum by (namespace,AdminNode) (increase(geo_monitoring_total{ControlActionNameType ='MonitorVip'}[1m])) > 0<br>**説明**： このアラートは、ラベル（$$labels.AdminNode））に記載されているVIPとインスタンスのVIPモニタリング障害を検出してGRが生成されたときに生成されます。 | | |

### CDL アラート

次の表に、 *interval-seconds* が 60 に設定されたルールグループ CDL のアラートを示します。

**表 *452 : Alert Rule Group - CDL***

| アラートルール | 重大度 | 期間（分単位） | タイプ |
|---|---|---|---|
| GRPC-Connections-Remote-Site | critical | 1 | 通信アラーム |
| | **Expression:** sum by (namespace, pod, systemId) (remote_site_connection_status) !=4<br>**説明**： このアラートは、リモートサイトへの GRPC 接続が 4 に等しくない場合に生成されます。 | | |

| アラートルール | 重大度 | 期間（分単位） | タイプ |
|---|---|---|---|
| Inter-Rack<br>-CDL-Replication | critical | 1 | 通信アラーム |
| | **Expression:** (sum by (namespace)<br>(increase(datastore_requests_total{local_request=\"0\",<br>errorCode=\"0\"}[1m]))/sum by (namespace)<br>(increase(datastore_requests_total{local_request=\"0\"}<br>[1m])))*100 < 90<br>**説明**： このアラートは、ラック間 CDL レプリケーションの成功率がしきい値を下回った場合に生成されます。 | | |
| Intra-Rack<br>-CDL-Replication | critical | 1 | 通信アラーム |
| | **Expression:** (sum by (namespace)<br>(increase(datastore_requests_total{local_request=\"1\",<br>errorCode=\"0\"}[1m]))/sum by (namespace)<br>(increase(datastore_requests_total{local_request=\"1\"}<br>[1m])))*100 < 90<br>**説明**： このアラートは、ラック内 CDL レプリケーションの成功率がしきい値を下回った場合に生成されます。 | | |

# サイト間の地理的冗長性

サイト間の地理的冗長性は、複数のサイトまたは場所にまたがる冗長性とフェールオーバーメカニズムを実装する方法です。サイト間冗長性の目的は、1 つのサイトで致命的な障害が発生した場合でも、重要なサービスとアプリケーションを利用できるようにすることです。

## 機能説明

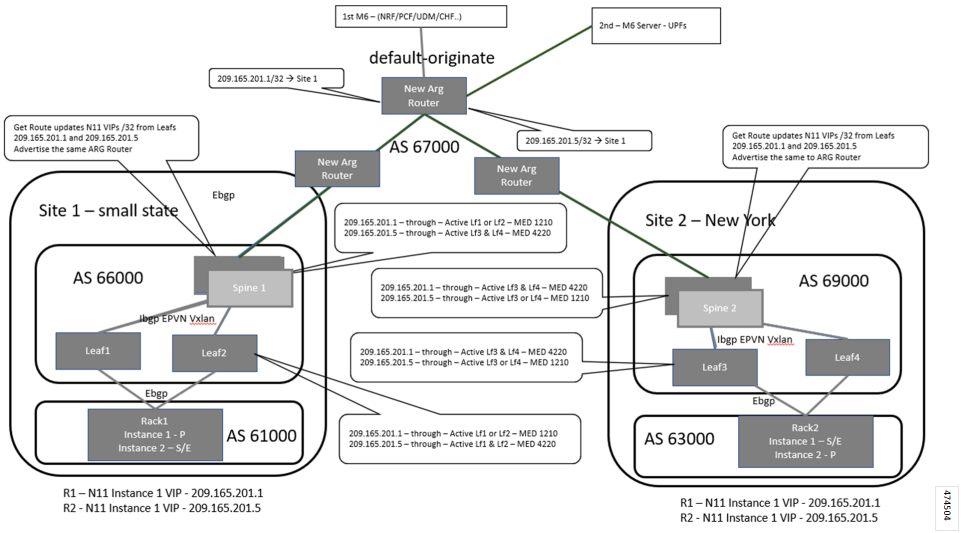
通信事業者は、地理的に異なる場所に冗長データ センターを設置し、1つのデータ センターがダウンした場合にもう1つのデータ センターが引き継ぐことができるようにします。この機能により、は既存のラック間ソリューションをサイト間ソリューションに拡張できます。ラック内の HA の現在の表記は、サイト間冗長性と連動して、より包括的な高可用性ソリューションを提供し続けます。

（注） サイト間ソリューションとラック間ソリューションは共存できないため、お客様はいずれかのソリューションを選択する必要があります。

# アーキテクチャ

SMF は、アクティブ：アクティブ モデルとも呼ばれる、サイト間冗長性の 1：1 モデルを実装します。このモデルは、ネットワーク内のすべてのサイトがトラフィックを同時にアクティブに処理し、各サイトが他のサイトで障害が発生した場合にネットワークの全負荷を引き継ぐことができる冗長構成の一種です。

次のトポロジ図は、サイト間冗長性の展開アーキテクチャについて説明しています。




# 前提条件

各サイトの 1:1 展開モデルの最小サイト要件のリストを次に示します。

- 2 つのリーフ
- 2 つのスパイン
- 2 つの GR インスタンスを含む論理 SMF を持つ 1 つの K8 クラスタ

（注） 各 GR インスタンスは、両方のサイトで同じ構成を持つ一意の EPC、RADIUS、および N11 エンドポイントのセットです。

- UPFは1: 1の構成で展開されます

（注） アクティブおよびスタンバイ UPF インスタンスは GR インスタンスに関連付けられ、UPF はコントロール プレーン プロファイルで両方の GR インスタンスの N4 アドレスのみを伝送します。

# 一般的なガイドライン

サイト間冗長性のさまざまなモジュールの構成は、ラック間冗長性と同じままです。各種モジュール構成の詳細については、次を参照してください。

- BGP スピーカーの構成 （1564 ページ）
- エンドポイント インスタンス認識の構成 （1549 ページ）
- ETCD/CachePod レプリケーションの構成 （1571 ページ）
- ラック間冗長性インスタンスの構成 （1548 ページ）
- IPAM の構成 （1569 ページ）
- ポッド モニタリング （1572 ページ）

# 機能の仕組み

冗長性イベントの管理とモニタリング、およびサイト間でのセッションの複製に必要な構成を除いて、ラック間およびサイト間のほとんどの構成は同じです。

サイト間冗長性の実装でサイト間でシームレスな通信を実現するためのガイドラインを次に示します。

- BGP（ボーダー ゲートウェイ プロトコル）ルート アドバタイズメント構成の先頭に自律システム（AS）パスを付加します。詳細については、サイト間展開の構成 （1632ページ）を参照してください。
- ジオポッド、CDL-EP（）、CDL-Kafka サーバーの L3 ルーティング。

## BGP ルート アドバタイズメント

サイト間冗長性展開では、非推移的な BGP 属性である Multi-Exit Discriminator（MED）属性を使用して、アクティブなサービス VIP に到達するための最適なパスを隣接ルータに通知します。ただし、MED 値は、隣接ルータとその eBGP ピア間では共有されません。

ラック間導入モデルでは、AS パス前に付加する技術が BGP で使用され、他の BGP ルータにアドバタイズされるルートのパス選択に影響を与えます。AS パス プリペンド技術では、BGP ルート アドバタイズメントで AS パスを操作することにより、特定のルートを他のルートよりも推奨します。ソフトウェア ロジックによって先頭に追加される AS パスの数の違いは、アップストリーム ルータが最適なルーティング可能なパスを選択するためのガイダンスを提供するのに役立ちます。

次の表に、サービス VIP とインターフェイス ボンディング ステータスのさまざまな組み合わせに必要な AS パスプリペンドの数を示します。

| GR ロール | ボンディング インターフェイスがアクティブ | VIP の存在 | MED 値 | Local Preference | AS パス プリペンド（回数） |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| 主要な役割（アクティブ） | はい | はい | 1210 | 2220 | 3 |
| | はい | 非対応 | 1220 | 2210 | 3 |
| | 非対応 | はい | 1215 | 2215 | 3 |
| | いいえ | 非対応 | 1225 | 2205 | 3 |
| スタンバイロール | はい | はい | 2210 | 1220 | 6 |
| | はい | 非対応 | 2220 | 1210 | 6 |
| | 非対応 | はい | 2215 | 1215 | 6 |
| | いいえ | 非対応 | 2225 | 1205 | 6 |
| Standby-error ロール | 該当なし | 該当なし | 3220 | 220 | 9 |

## KPI

prepend_as_path_count」ラベルが次の既存のメトリックに追加されます。

- bgp_outgoing_failedrouterequest_total
- bgp_outgoing_routerequest_total

上記のメトリックは、ルートがアドバタイズされるときに入力されます。

**BGP 発信失敗ルート要求 KPI**

| KPI 名 | 説明 | ラベル | 有効な値 |
|---|---|---|---|
| **bgp_outgoing_failedrouterequest_total** | この重要業績評価指標（KPI）は、失敗した発信ルートの合計数を表します。 | app_name | アプリケーション |
| | | cluster | ローカル（Local） |
| | | data_center | DC |
| | | インスタンス | 1 |
| | | instance_id | 1 |
| | | インターフェイス | bd2.nrf.2275 |
| | | local_pref | 320 |
| | | med | 3220 |
| | | next_hop | 50.50.50.50 |
| | | prepend_as_path_count | "9->STANDBY_ERROR" |
| | | service_IP | 10.10.10.10 |
| | | service_name | bgpspeaker-pod |
| | | vrf | デフォルト |

**BGP 発信ルート要求合計 KPI**

| KPI 名 | 説明 | ラベル | 有効な値 |
|---|---|---|---|
| **bgp_outgoing_routerequest_total** | この重要業績評価指標（KPI）は、発信ルートの総数を表します。 | app_name | アプリケーション |
| | | cluster | ローカル（Local） |
| | | data_center | DC |
| | | インスタンス | 1 |
| | | instance_id | 1 |
| | | インターフェイス | bd2.nrf.2275 |
| | | local_pref | 320 |
| | | med | 3220 |
| | | next_hop | 50.50.50.50 |
| | | prepend_as_path_count | "9->STANDBY_ERROR" |
| | | service_IP | 10.10.10.10 |
| | | service_name | bgpspeaker-pod |
| | | vrf | デフォルト |

（注） 上記のメトリックは、ルートがアドバタイズされるときに入力されます。

**As-Path メトリックの値**：

新しいラベル「prepend_as_path_count」には、RoleInfo に基づく次の値が含まれます。

- Rack/Prepend CLI 間で無効：
  - prepend_as_path_count="Not-Applicable"
- CLI 有効化/プライマリ、Traffic_Hit 理由：
  - prepend_as_path_count="0->PRIMARY,TRAFFIC_HIT"
- CLI 有効化/プライマリ、Traffic_Hit 以外の理由：
  - prepend_as_path_count="3->PRIMARY"
- CLI 有効化/スタンバイ：
  - prepend_as_path_count="6->STANDBY"
- CLI 有効化/ STANDBY_ERROR：

• prepend_as_path_count="9->STANDBY_ERROR"

# サイト間展開の構成

サイト間展開を有効にするには、BGP 構成で AS パス前に付加フラグを構成する必要があります。

いかに構成例を示します。

```
config
  router local_as_number
    bfd bfd_configuration
    interface bgp_local_interface
    prepend as-path { false | true }
    exit
   exit
```

注：

- **interface** *bgp_local_interface*：BGP ローカル インターフェイスを指定します。
- **prepend as-path { false | true }**： **true** を選択して、サイト間展開を有効にします。デフォルトでは、このオプションは無効になっています。

  このオプションが **false**に設定されている場合、論理 SMF の展開はラック間モデルに従います。

## 設定の確認

構成を確認するには、次の show コマンドを使用します。

```
smf# show running-config router
router bgp 63200
 learnDefaultRoute false
 prepend as-path true  ———————————————> as-path
 bfd interval 250000 min_rx 250000 multiplier 3
 interface enp216s0f0.2119
  bondingInterface enp216s0f0
  bondingInterface enp94s0f0
  neighbor 101.101.172.254 remote-as 63100 fail-over bfd
 exit
 interface enp216s0f0.2129
  vrf vrf_papn1
  bondingInterface enp216s0f0
  bondingInterface enp94s0f1
  neighbor 101.101.174.254 remote-as 63100 fail-over bfd
 exit
 interface enp216s0f0.2139
  vrf vrf_papn2
  bondingInterface enp216s0f0
  bondingInterface enp94s0f0
  neighbor 101.101.178.254 remote-as 63100 fail-over bfd
 exit
```

次に、GR ロールに対応する bgp でアドバタイズされたルートの出力例を示します。

```
[smf] smf# show role instance-id 1
result "PRIMARY"
```

```
[smf] smf# show bgp-advertised-routes
bgp-route

-----bgpspeaker-pod-0 ----
   Network              Next Hop                 AS_PATH          Age        Interface
       Vrf                          Attrs
*> 209.165.200.228    209.165.200.229       63000 63000 63000   00:00:47      ens161
      Default      [{Origin: e} {LocalPref: 2205} {Med: 1225}]
```

## ポッドの L3 ルーティング

ラック間ソリューションでは、リーフ サーバーとスパイン サーバーが同じ AS パスに組み込まれ、VxLAN 技術の利用が可能になりました。この展開モデルでは、ラック間の到達可能性を維持しながら、さまざまなポッド間での冗長性データとイベントのサポート、監視、および交換が可能です。具体的には、両方のラックの Geo ポッドの外部 IP アドレスが共通のサブネットに統合され、同じ VLAN を共有しているため、ルート検出を必要とせずにデータ交換を行えるようになりました。さらに、ラック間の通信はリーフ サーバーとスパイン サーバーの境界内に残り、パケットがそれらを超えて通過する必要はありませんでした。

次のポッドには、サイト間の外部接続が必要です：

- ジオポッド
- CDL-ep（秒）
- CDL-Kafka-server

サービス VIP とは異なり、これらの IP アドレスはサイト間でのフローティングを必要としません。ルーティングの決定は、実稼働展開中に 1 回だけ行う必要があります。したがって、これらの外部 IP アドレスを BGP を介してアドバタイズする代わりに、スタティック ルーティングが使用されました。

静的ルートは、リモート CDL/Kafka/Geo ネットワークに到達するために、ローカル K8S クラスタ プロトコル ノードに追加されます。リーフは、接続されているすべてのローカル CDL/Kafka/Geo ネットワークをスパインに自動的にアドバタイズします。スパインはこれらのルートを Arg ルータに再配布します。Arg ルータは、両方のサイトの CDL/Kafka/Geo ネットワークに到達する方法を認識しています。パケットの宛先がリモート CDL/Kafka/Geo ネットワークの場合、ローカル K8S プロトコル ノードには、ローカル リーフを指すスタティック ルートがあります。その後、パケットはスパインに送られます。スパインには、Arg ルータを指すデフォルトルートがあります。Arg ルータには、パケットをリモートサイトに送信するための適切なルートがあります。

さらに、Arg ルータは「default-originate」キーワードを使用して構成されます。これは、ARG ルータをスパインのデフォルト ゲートウェイとして指定します。その結果、スパインはルーティング パスがスパインで利用できないすべてのトラフィックを Arg ルータにリダイレクトします。

## サイト間の冗長性シナリオ

このセクションでは、サイト間冗長性の展開がさまざまなシナリオでどのように機能するかについて説明します。

2 つのサイトがあり、両方が動作しているシナリオでは、各サイトに 1 つのプライマリ/アクティブ GR（ゲートウェイ ルータ）インスタンスがあります。各サイトに構成されたエンドポイントは、アクティブなインスタンスに対応するトラフィックを伝送します。集約ルータ（ARG）がサイトに直接接続されていない可能性があり、ARG とサイトの間に複数の自律システムが存在する可能性があります。ARG ルータは、両方のサイトからのルートをまとめます。

サイトの冗長性に関するさまざまなシナリオを次に示します：

- 設定された気象条件では、サイト A は GR1 の最適なルートと、GR2 に関連付けられたエンドポイントのあまり好ましくないルートをアドバタイズします。

  ARG では、ルートは次のようになります：

  - サイト A からのルート
    - 209.165.200.225 AS-Path 65000 65000 65000 65000
    - 209.165.200.235 AS-Path 65000 65000 65000 65000 65000 65000 65000

  - サイト B からのルート
    - 209.165.200.225 AS-Path 64000 64000 64000 64000 64000 64000
    - 209.165.200.235 AS-Path 64000 64000 64000 64000

  - ベスト パス：
    - Site-A 209.165.200.225 AS-path 65000 65000 65000 65000
    - Site -B 209.165.200.235 AS-path 64000 64000 64000 64000

ここで、サイト A がダウンした場合は次のようになります：

ARG ルータの BGP セッションは BGP コンバージェンス時間後にダウンし、サイト A から学習したルートが取り消されます。ARG でのルートの現在の状態は次のとおりです。

- サイト B からのルート：
  - 209.165.200.225 AS-Path 64000 64000 64000 64000 64000 64000 64000
  - 209.165.200.235 AS-Path 64000 64000 64000 64000

  これで、エンドポイントの 209.165.200.225 と 209.165.200.225 の両方のトラフィックがサイト B に向けて送信されます。

- サイト B のトラフィック モニタリング機能は、IP アドレス 209.165.200.225 のトラフィックを識別しています。この IP アドレスのパケットしきい値を超えると、GeoReplication ポッドは、スタンバイ モードからアクティブ モードへの GR-1 インスタンスの移行をトリガーします。

- Geo-pod が GR1 のプライマリ インスタンスへの移行を BGPSpeaker-pod に通知した後、BGPSpeaker-pod は最も望ましいルーティング パスを使用して GR1 エンドポイントのルートを再アドバタイズします。

- これで、ARG 内のルートは次の情報で更新されます：
  - サイト B からのルート：
    - 209.165.200.225 AS-Path 64000 64000 64000 64000
    - 209.165.200.235 AS-Path 64000 64000 64000 64000

# スプリットブレイン

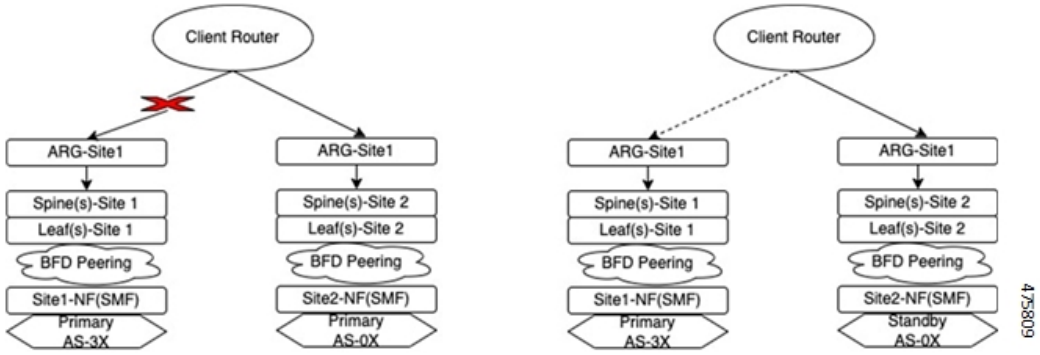
複数のサイトに展開すると、障害ドメインが拡大します。リーフ/スパイン アーキテクチャとラック内で発生する障害は適切に管理され、これらの障害時の GR インスタンスの状態は明確に定義され、ラック間ソリューションと同じメカニズムに従います。ただし、外部ルータのリンクの変動など、データ センターの外部に障害がある場合、ピアラックとの通信が失われた場合、アクティブな GR インスタンスを備えたラックのメカニズムはありません。

クライアント ルータとデータセンター ルータ間のリンクがダウンすると、ラック間の接続が失われます。クライアント ルータは、着信データ トラフィックを次の優先サイト（この場合はサイト 2）に送信します。サイト 2 ではトラフィック モニタリングが有効になっており、トラフィックが検出されます。着信トラフィックのしきい値が満たされると、GR インスタンスがスタンバイからプライマリに移行します。この時点で、サイト 1 とサイト 2 の両方がこの GR インスタンスに対してアクティブです。ARG-Site1 とクライアント ルータ間のリンクが復元されると、デュアルアクティブまたはスプリットブレイン シナリオが発生します。

その結果、以下のシナリオが考えられます：

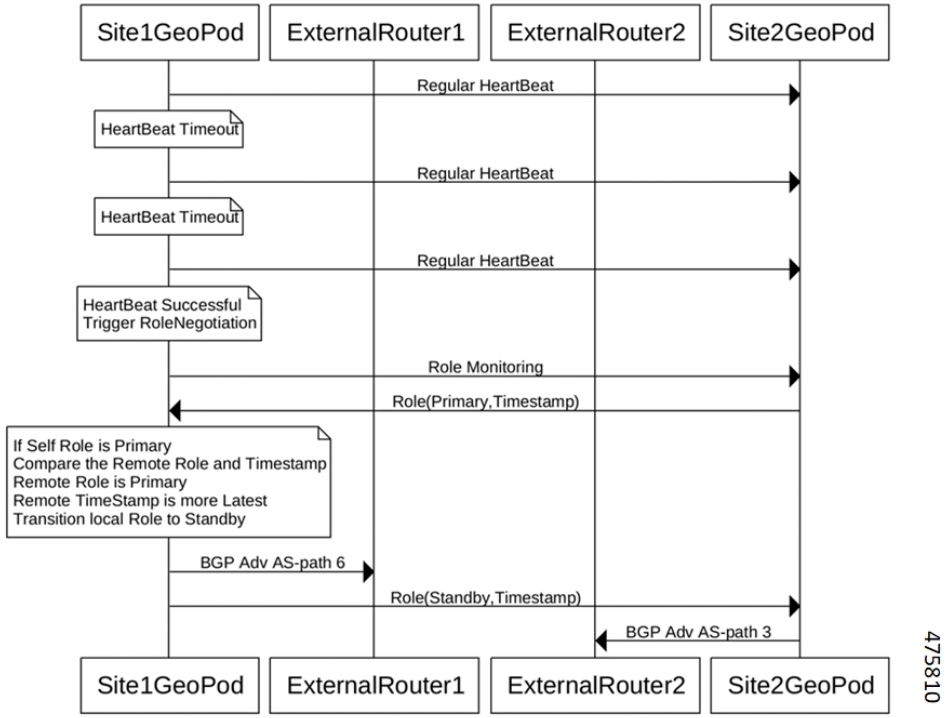
1. クライアント ルータが ARG-Site1 と ARG-Site2 の間にトラフィックを分散すると、コールが失われ、お客様サービスが中断します。
2. 外部リンク リカバリをポストし、プライマリと見なすサイトと他のサイトをスタンバイに移行する方法を指定します。

2 つのサイト間で分散されるトラフィックの問題に対処するための解決策は、トラフィック モニタリングによって GR インスタンスがスタンバイからプライマリに移行するときに、AS パスを付加しないことです。新しいプライマリ サイトは、明示的なローカル AS パスの付加なしで BGP 再アドバタイジングを実行し、ピアサイトがオンラインに戻った場合でもこのサイトを最も優先されるサイトにします。このアプローチにより、セカンダリ サイトが復元して完全に動作するまで、トラフィックがプライマリ サイトに確実に送信されます。




外部リンク リカバリ後のサイトロール移行の問題に対処するための解決策は、すべてのロール移行のタイムスタンプを保持することです。リンクが復元されると、Site-1/Geo-Pod と Site-2/Geo-Pod の間で通信が発生し、その間に両方のポッドが遷移が発生したロール状態とタイムスタンプを交換します。その後、タイムスタンプが古いサイトがプライマリからスタンバイに移行し、リンクの復元後も最新のプライマリ サイトがその役割を維持します。

（注） タイムスタンプの更新は、ロールに変更があった場合にのみ行われます。理由に変更があると、タイムスタンプは変更されません。最初のスプリットブレインを検出した場合、ロールが primary でトラフィックヒットが原因のサイト/ラックの組み合わせが優先されます。



# KPI

この機能の一部として、次の重要業績評価指標（KPI）がスプリットブレインのサポートに関連付けられます。

**Geoスプリット ブレイン検出合計KPI**

| KPI 名 | 説明 | ラベル | 有効な値 |
|---|---|---|---|
| **geo_split_brain_detection_合計** | この重要業績評価指標（KPI）は、スプリット ブレイン検出インスタンスの全体的な数を表します。 | GRInstanceNumber | これは GR インスタンス ID であり、値は次のいずれかになります。<br>• instance.1<br>• instance2. |
| | | LocalSiteRole | これは、数字としてのローカル サイトのロールです。次のいずれかの値を指定できます：<br>• 2（主要な役割用）<br>• 3（スタンバイ ロール用）<br>• 6（Standby-error ロールの場合） |
| | | LocalSiteReason | これはローカル サイトの理由の文字列値です：<br>•「CLI」<br>•「BFD 障害」<br>•「POD 障害」<br>•「トラフィック ヒット」<br>•「アップグレード」<br>•「スタートアップ」<br>•「スタックされたロール」<br>•「サイト通知」<br>•「リモートモニタリング」<br>• "スプリット ブレイン Recover"<br>• 通知の削除<br>•「HEARTBEAT 回復」 |
| | | LocalSiteTimeStamp | ロールが最後に更新されたときのローカル サイトのタイムスタンプ。 |
| | | RemoteSiteRole | |

| KPI 名 | 説明 | ラベル | 有効な値 |
|---|---|---|---|
| | | | これは、数字としてのリモート サイトのロールです。次のいずれかの値を指定できます：<br>• 2（主要な役割用）<br>• 3（スタンバイ ロール用）<br>• 6（Standby-error ロールの場合） |
| | | RemoteSiteReason | これはリモート サイトの理由の文字列値です：<br>• 「CLI」<br>• 「BFD 障害」<br>• 「POD 障害」<br>• 「トラフィック ヒット」<br>• 「アップグレード」<br>• 「スタートアップ」<br>• 「スタックされたロール」<br>• 「サイト通知」<br>• 「リモートモニタリング」<br>• "スプリット ブレイン Recover"<br>• 通知の削除<br>• 「HEARTBEAT 回復」 |
| | | RemoteSiteTimeStamp | ロールが最後に更新されたときのリモート サイトのタイムスタンプ。 |

**Geo スプリット ブレイン解決の合計**

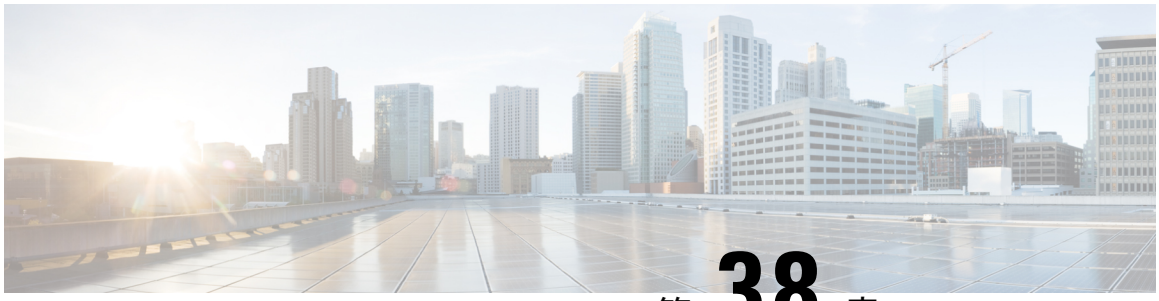
| KPI 名 | 説明 | ラベル | 有効な値 |
|---|---|---|---|
| **geo_split_brain_resolution_total** | この重要業績評価指標（KPI）は、スプリットブレイン解決インスタンスの全体的な数を表します。 | GRInstanceNumber | これは GR インスタンス ID であり、値は次のいずれかになります。<br>• instance.1<br>• instance2. |
| | | LocalSiteRole | これは、数字としてのローカルサイトのロールです。次のいずれかの値を指定できます：<br>• 2（主要な役割用）<br>• 3（スタンバイ ロール用）<br>• 6（Standby-error ロールの場合） |
| | | LocalSiteReason | これはローカル サイトの理由の文字列値です：<br>• 「CLI」<br>• 「BFD 障害」<br>• 「POD 障害」<br>• 「トラフィック ヒット」<br>• 「アップグレード」<br>• 「スタートアップ」<br>• 「スタックされたロール」<br>• 「サイト通知」<br>• 「リモートモニタリング」<br>• "スプリット ブレイン Recover"<br>• 通知の削除<br>• 「HEARTBEAT 回復」 |
| | | LocalSiteTimeStamp | ロールが最後に更新されたときのローカル サイトのタイムスタンプ。 |
| | | RemoteSiteRole | |

| KPI 名 | 説明 | ラベル | 有効な値 |
|---|---|---|---|
| | | | これは、数字としてのリモートサイトのロールです。次のいずれかの値を指定できます：<br>• 2（主要な役割用）<br>• 3（スタンバイ ロール用） |
| | | RemoteSiteReason | これはリモート サイトの理由の文字列値です：<br>•「CLI」<br>•「BFD 障害」<br>•「POD 障害」<br>•「トラフィック ヒット」<br>•「アップグレード」<br>•「スタートアップ」<br>•「スタックされたロール」<br>•「サイト通知」<br>•「リモートモニタリング」<br>• "スプリット ブレイン Recover"<br>• 通知の削除<br>•「HEARTBEAT 回復」 |
| | | RemoteSiteTimeStamp | ロールが最後に更新されたときのリモート サイトのタイムスタンプ。 |
| | | OldRole | スプリットブレイン解決前のロール。次のいずれかの値を指定できます：<br>• 2（主要な役割用）<br>• 3（スタンバイ ロール用） |
| | | NewRole | |

| KPI 名 | 説明 | ラベル | 有効な値 |
|---|---|---|---|
| | | | スプリット ブレイン解決後の新しいロール。次のいずれかの値を指定できます：<br>• 3（スタンバイ ロール用）<br>• 6（Standby-error ロールの場合） |

地域ロール理由変更の合計

| KPI 名 | 説明 | ラベル | 有効な値 |
|---|---|---|---|
| **geo_role_reason_change_total** | この重要業績評価指標（KPI）は、ロールの理由が HEARTBEAT リカバリに変更された合計回数の全体数を表します。 | GRInstanceNumber | これは GR インスタンス ID であり、値は次のいずれかになります。<br>• instance.1<br>• instance2. |
| | | LocalSiteRole | これは、数字としてのローカル サイトのロールです。次のいずれかの値を指定できます：<br>• 2（主要な役割用）<br>• 3（スタンバイ ロール用）<br>• 6（Standby-error ロールの場合） |
| | | oldReason | これは、HEARTBEAT リカバリ前のローカル サイトの理由の文字列値です：<br>• 「HEARTBEAT 回復」 |
| | | NewReason | これはローカル サイトの理由の文字列値です：<br>• 「HEARTBEAT 回復」<br>（注）<br>現在、この移行はトラフィック ヒットのみに基づいて発生します。 |



第 38 章

# ローミングのサポート


- 機能の概要と変更履歴 （1643 ページ）
- 機能説明 （1644 ページ）
- ローカル ブレークアウト ローミングのサポート （1645 ページ）
- 自宅ルート ローミングのサポート （1654 ページ）
- N3 および N9 ユーザー プレーンの分離 （1697 ページ）
- 許可された PLMN リストのサポート （1701 ページ）
- PLMN ローミング モビリティのサポート （1702 ページ）
- N4 インターフェイスのローミング ステータス （1714 ページ）
- トラブルシューティング情報 （1714 ページ）


## 機能の概要と変更履歴

### 要約データ

| | |
|---|---|
| 該当製品または機能エリア | SMF |
| 該当プラットフォーム | SMI |
| 機能のデフォルト設定 | 有効：常時オン |
| このリリースでの関連する変更点 | N/A |
| 関連資料 | 該当なし |

# 更新履歴

表 *453 :* マニュアルの変更履歴

| 改訂の詳細 | リリース |
|---|---|
| SMF は次のローミング機能をサポートしています。<br>• ホーム コールとローム コールの N3 と N9 の分離<br>• CLI 構成による許可 PLMN リストと要求送信者 PLMN リストのサポート<br>• N4 メッセージのローミング ステータス<br>• SMF は、N16 hSMF または vSMF および SEPP の障害処理をサポートしています。 | 2023.03.0 |
| 次の拡張機能が導入されました。<br>• ホーム ルーテッド（HR）ローミング サポート<br>• セキュリティ エッジ保護プロキシ（SEPP）サポート<br>• 人事ローミングにおける引き継ぎサポート | 2021.02.3 |
| 最初の導入。 | 2021.01.0 |

# 機能説明

この章では、SMF でサポートされるローミングの機能の概要について説明します。モバイル ネットワーク オペレーターは、ローミング パートナーシップを結び、ネットワークが到達しない地域の加入者にシームレスなサービスを提供します。PLMNは、オペレータ ネットワークの境界を指名します。 hPLMNは、サブスクライバのホーム ネットワークを示します。 vPLMNは、サービスのレンダリング元となる訪問ネットワークを示します。

SMF のローミング サポートは、次のように分類できます：

- LBO（ローカルブレークアウト）ローミング：vPLMNは、パケット コア サービスとデータ ネットワークへのアクセスをローカルに提供します。
- HR（ホーム ルーティング）ローミング：vPLMN はパケット コア サービスを提供し、hPLMN はデータ ネットワークへのアクセスを提供します。

# ローカル ブレークアウト ローミングのサポート

## 機能説明

**重要** この章で使用されている PGW-C という用語は、SMF でサポートされている EPS インターワーキング機能を意味しており、LTE ネットワークで使用されるスタンドアロン P-GW として想定してはなりません。

VPLMN はパケット コア サービスを提供し、データ ネットワークへのアクセスを提供します。この機能により、SMF はローカル ブレークアウト（LBO）ローミングと呼ばれるルーティングのフレーバをサポートできます。

この機能では、以下の機能を提供します：

- NR 経由で接続された 5G セッションのローミング
- E-UTRAN を介して接続された 4G および Wi-Fi セッションのローミング
- LI サポート
- SEPP を使用しない展開モデル

サービス PLMN の詳細については、複数 PLMN のサポート （1049 ページ） の章を参照してください。

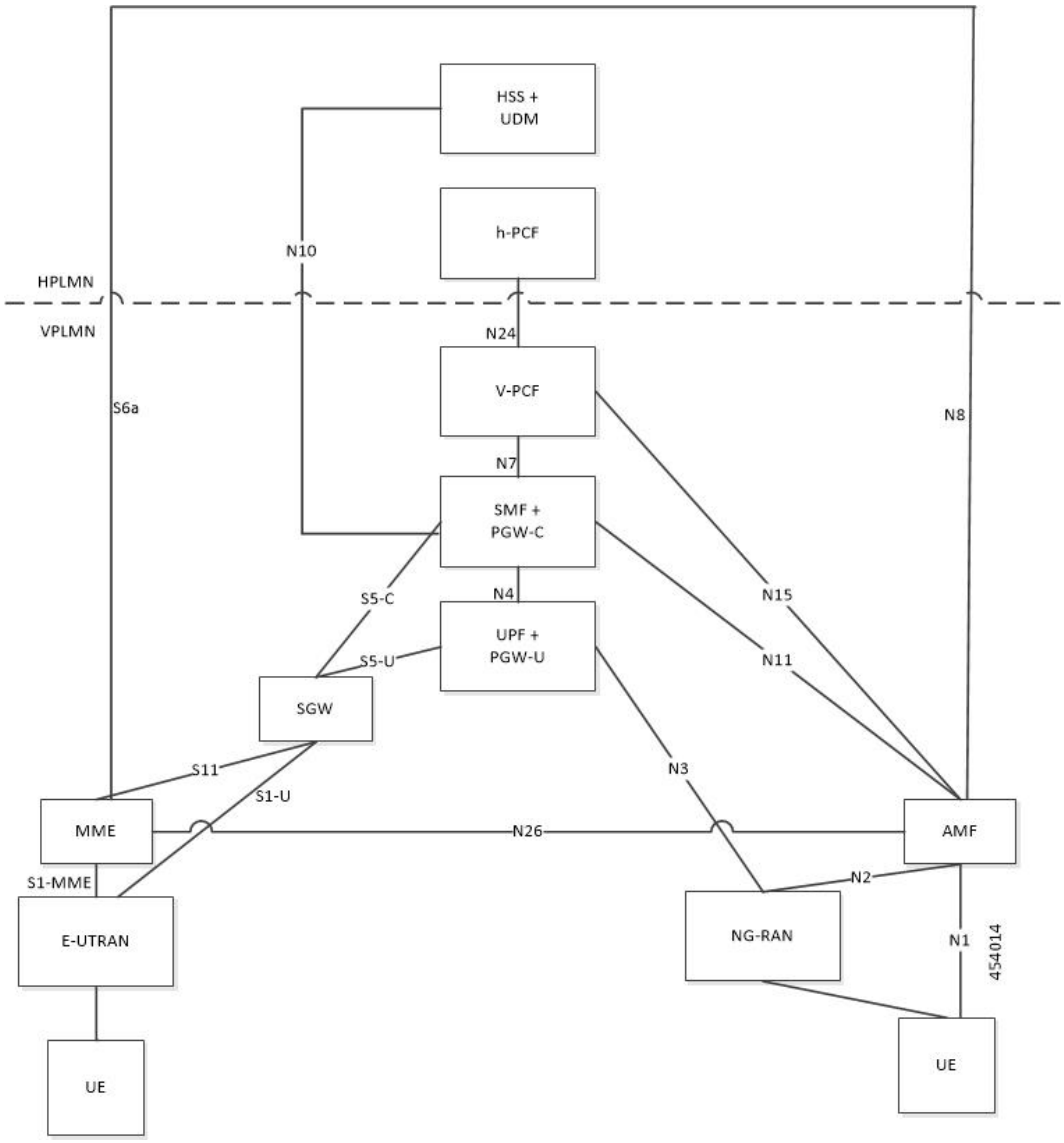
## アーキテクチャ

ここでは、LBO ローミング機能のアーキテクチャについて説明します。

### EPC LBO のシナリオ

次の図は、EPC の SMF と PGW-C に接続された 4G セッションの LBO ローミング アーキテクチャを示しています。

図 *255 : 4G*セッションのローカル ブレークアウト ローミング アーキテクチャ

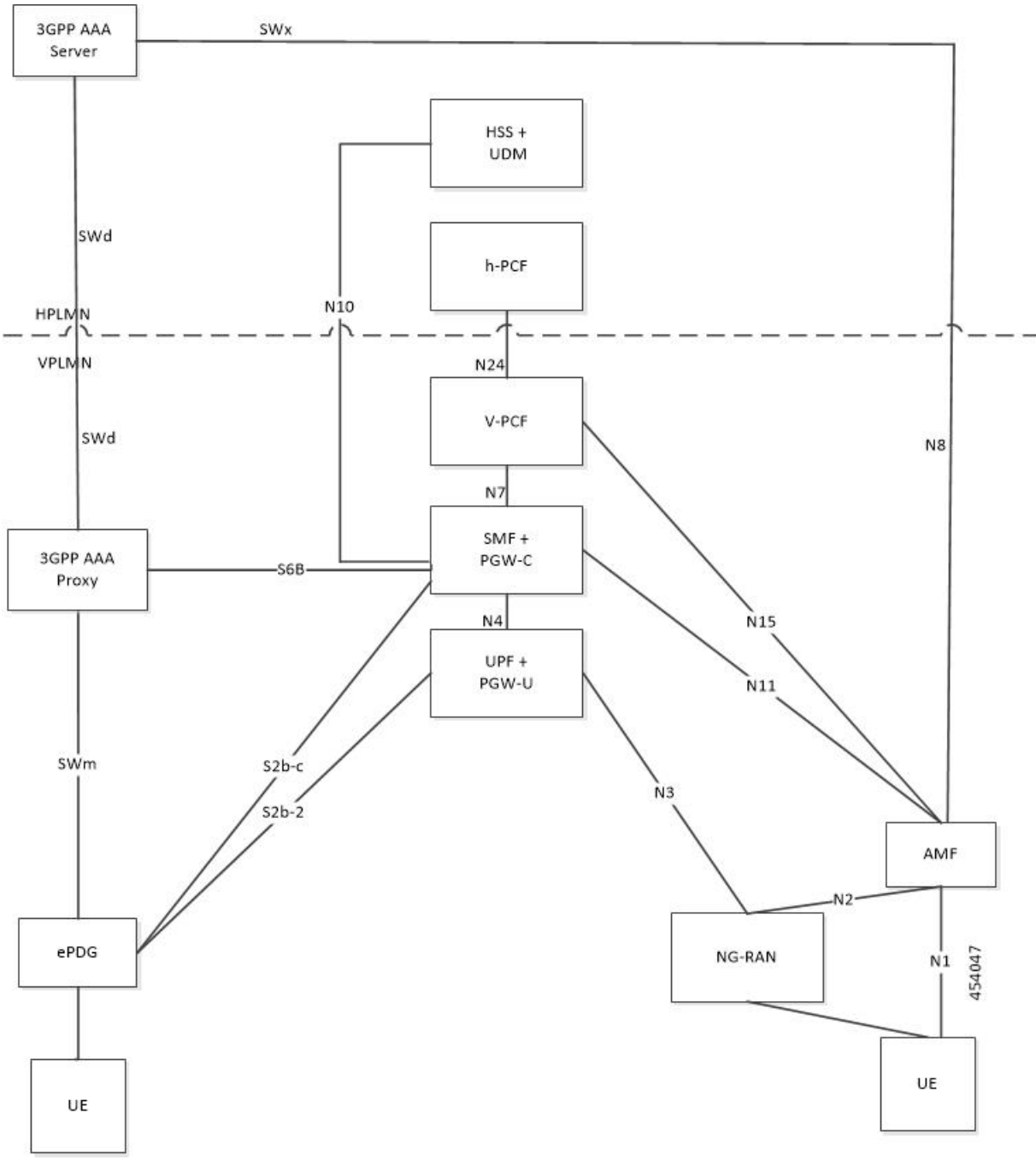



4G セッションの LBO ローミング中は、SGW と SMF の PGW-C が両方とも VPLMN に存在します。SGW と SMF は、S5-C インターフェイスを介してメッセージを交換します。すべてのノースバウンド SBI インターフェイスは、4G と 5G に共通です。SMF は、vPCF、vCHF、および UDM と情報をやりとりします。

### ePDG LBO シナリオ

次の図は、EPC の SMF および PGW-C に接続された Wi-Fi セッションの LBO ローミング アーキテクチャを示しています。

図 *256 : Wi-Fi* セッションのローカル ブレークアウト ローミング アーキテクチャ

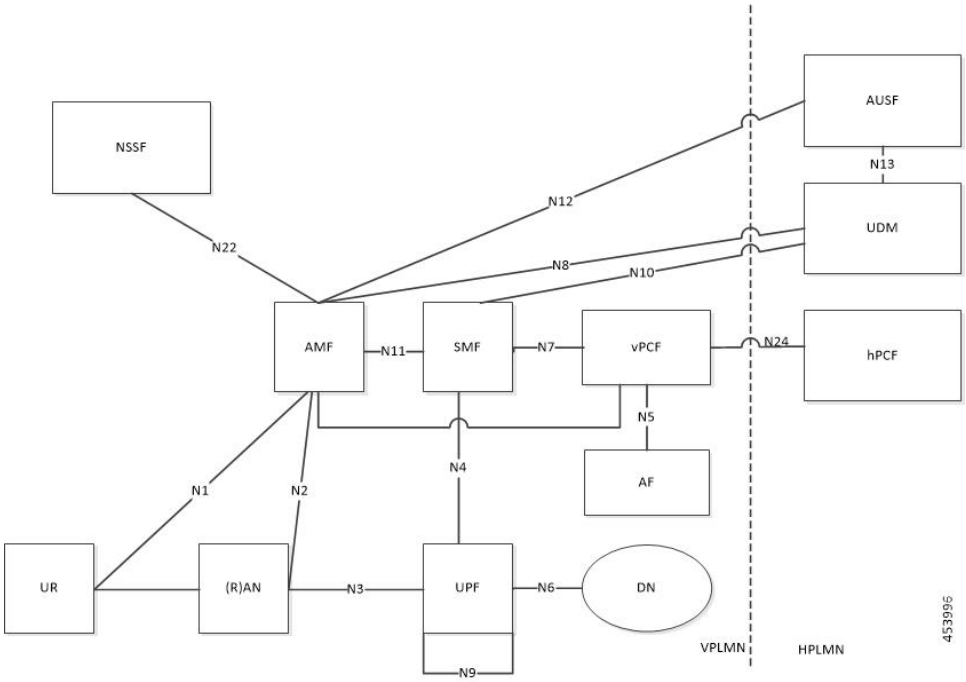



SMF は VPLMN に常駐し、vPCF、vCHF、UDM と相互作用します。SMF は 3GPP AAA サーバへの S6b をサポートしていませんが、N10 インターフェイスを使用します。

### 5G NR LBO シナリオ

次の図は、NR を介して接続された 5G セッションの LBO ローミング アーキテクチャを示しています。

図 *257 : 5G* セッション向けの *LBO* ローミング アーキテクチャ




前の図に示すように、SMF は VPLMN にあります。AUSF と UDM のみが HPLMN の NF です。VPLMN の PCF は、N24 インターフェイスを介して HPLMN の PCF と通信します。PCF は相互に通信して、サブスクライバ セッションに関連するポリシーを取得し、それらを SMF に渡します。

### LBO 中の SMF 機能

SMF は、インローマーの LBO に関連する次の機能をサポートしています。

- 受信した SUPI のローカル構成と MCC および MNC に基づくインローマーの検出
- N11
  - インローマーの LBO の決定
  - SMF が LBO をサポートしていない訪問者のセッション設定要求を受信した場合、SMF は AMF にエラーを送信します。次に、AMF はホーム ルーテッド（HR）ローミングをサポートする SMF とのセッションのセットアップを再試行します。
  - AMF からの vPCF である PCF ID のサポート
- N2

- SMF は、N2 SM 情報で VPLMN のシングル ネットワーク スライス選択支援情報（S-NSSAI）を提供します。

- N7
  - VPLMN での PCF の選択
  - vPCF は、PCC ルール生成のために HPLMN 内の AF と対話します（IMS など）。ただし、PCC ルールはローミング ポリシーを使用して生成され、HPLMN の登録済みポリシーには vPCF からアクセスできません。また、vPCF は支出制限のために CHF とやり取りしません。LBO の PCC ルールの機能は制限されています。
- N40
  - VPLMN での CHF の選択。 vSMF は、CHF が UE のローマー ステータス（インローマー）にサービスを提供する HPLMN ID の追加パラメータを考慮します。
- N10
  - HPLMN における UDM の選択
- NRF
  - SMF は、vCHF サービス HPLMN を検出する際に、**chf-supported-plmn** クエリパラメータを使用します。
  - EPS 手順中に、SMF が複数の S-NSSAI をサポートし、APN が複数の S-NSSAI に対して有効な場合、Nnssf_NSSelection_Get サービス操作を実行します。この操作は、SMF が S-NSSAI を UE に提供する前に有効になります。この操作は、サブスクライブ済みの S-NSSAI からサービング PLMN S-NSSAI 値へのマッピングを取得するのに役立ちます。
- SMF での緊急サービスは LBO モデルでのみサポートされます。LBO ローミングの場合、SMF は緊急セッション用に UDM に登録しません。

  緊急コールの場合、SMF は UE PLMN ID を無視し、すべてのインターフェイスでサービス提供中の PLMN ID リレーします。

### ネットワークスライシング

SMF は、以下のネットワーク スライシングに関連する機能をサポートします：

- SMF は、許可された NSSAI のリストで構成できます。
- SMF がローミング中に vSMF として機能する場合、VPLMN で使用される UE の S-NSSAI は、SMF で構成されている値である必要があります。
- LBO の場合、SMF は、UDM から受信した S-NSSAI のマッピングを、PDU 接続の構成中に受信した HPLMN の NSSAI にマッピングを実行します。受信した NSSAI は、サポートされている NSSAI として vSMF で構成する必要があります。

### ノード選択に関する考慮事項

LBO ローミングでのノードの選択には、次の基準が適用されます。

- ローミングが有効になっている場合、各 SMF は PLMN 間 FQDN 値を NRF に登録します。この操作により、AMF は別の PLMN の hSMF を選択できます。
- SMF は **target-plmn-list** と **requester-plmn-list** をクエリ パラメータとして扱います。
- サービス中 PLMN の NRF は、NF からのすべての発見リクエストを処理します。

### LBO 中の PDU 確立

LBO ローミングの場合、PDU セッションの確立には次の条件が考慮されます。

- SMF が LBO をサポートせずにビジターのセッション設定要求を受信した場合、SMF は SM コンテキスト作成エラーを AMF にHOME_ROUTED_ROAMING_REQUIRED の原因で送信します。次に、AMF はホーム ルーテッド（HR）ローミングをサポートする SMF とのセッションのセットアップを再試行します。シナリオ例は、NAS PDU セッション確立要求が SSC モード 3 を要求し、vSMF で許可される SSC モードが SSC モード 3 をサポートしていない場合です。
- SMF は HPLMN S-NSSAI と S-NSSAI の両方を受信します。SMF は S-NSSAI を使用して、vSMF でサポートされている NSSAI に対して NSSAI を検証します。
- N40 インターフェイス：
  - vSMF は、CDR メッセージを介して CHF に roamerInOut 属性を送信します。roamerInOut 属性には、PDUSessionChargingInformation と userInformation が含まれます。この属性値は、インローマーの場合は IN_BOUND、アウトローマーの場合は OUT_BOUND のいずれかです。
  - vSMF は、非ローミングおよびローミングの場合に適切な値（HOME_DEFAULT、ROAMING_DEFAULT、および VISITING_DEFAULT）を使用して PDUSessionInformation およびChargingCharacteristicsSelectionMode IE を送信します。
  - PDUSessionInformation IE の hPlmnId および ServingCNPlmnId フィールドには、UE のローミング ステータスに従って値が伝送されます。
- N1N2 メッセージの転送中に、N2 コンテンツで提供される S-NSSAI は VPLMN S-NSSAI と同じである必要があります。
- LBO ローミング シナリオでは、PDU セッション確立承認メッセージに、VPLMN に対して許可された NSSAI からの S-NSSAI が含まれます。また、SMF が AMF から受信した許可 NSSAI のマッピングから取得した HPLMN の対応する S-NSSAI も含まれます。
- SMF は LBO ローミング中の UDM 検出に HPLMN を使用します。

### LBO 中の PDN 確立

S-GW は、S-GW が属する PLMN ID とともに PGW-C にサービング ネットワーク IE を送信します。SMF は、その PLMN を VPLMN として使用して、検証、ノード選択、および他のノースバウンド インターフェイスへの VPLMN の受け渡しを行います。

5G セッションの作成に適用される N40 インターフェイス関連の要件と緊急セッション関連の要件は、4G および Wi-Fi セッションにも適用されます。

### PLMN の使用状況

次の表に、SMF サービス プロファイルで構成された PLMN 値が、すべてのインターフェイス間でどのようにリレーされるかを示します。

| インターフェイス | 属性 | Homer | インローマー（LBO） | アウトローミング（HR） | インローマー（HR） |
|---|---|---|---|---|---|
| | UE PLMN | 310-240 | 262-06 | 310-310 | 302-610 |
| NRF | UDM を検出するために nrf Discover の plmn-list（queryParam = target-plmn） | UE PLMN | UE PLMN | UE PLMN | N/A |
| NRF | PCF/CHF を検出するために nrf Discover の plmn-list（queryParam = target-plmn） | UE PLMN | サービング PLMN | UE PLMN | サービング PLMN |
| N10 | N10 登録における smfRegistration IE の PLMN | サービング PLMN | サービング PLMN | プライマリ ホーム PLMN | N/A |
| N10 | GET サブスクリプション URI の PLMN | サービング PLMN | サービング PLMN | プライマリ ホーム PLMN | N/A |

| インターフェイス | 属性 | Homer | インローマー（LBO） | アウトローミング（HR） | インローマー（HR） |
|---|---|---|---|---|---|
| N10 | N10 の sdmSubscription IE の PLMN が Notification To にサブスクライブ | サービング PLMN | サービング PLMN | プライマリ ホーム PLMN | N/A |
| N40 | N40 課金データ要求の NfConsumer 識別 IE の PLMN | プライマリ ホーム PLMN | プライマリ ホーム PLMN | プライマリ ホーム PLMN | プライマリ ホーム PLMN |
| N40 | pduSession の PDU の hPlmnId、IE の pduSession の課金情報の ChargingData 要求 | UE PLMN | UE PLMN | UE PLMN | UE PLMN |
| N40 | pduSession ChargingData リクエストの PDU セッション情報 IE での サービング PLMN | サービング PLMN | サービング PLMN | プライマリ ホーム PLMN | サービング PLMN |
| N7 | PCF 内の PLMN による AC_TY_CH/ SAREA_CH/ RAT_TY_CH トリガの通知 | サービング PLMN | サービング PLMN | プライマリ ホーム PLMN | N/A |
| N7 | PCF への作成要求の PLMN | サービング PLMN | サービング PLMN | プライマリ ホーム PLMN | N/A |

| インターフェイス | 属性 | Homer | インローマー（LBO） | アウトローミング（HR） | インローマー（HR） |
|---|---|---|---|---|---|
| RADIUS | 3GPP UE ロケーション IE RADIUS 認証の PLMN | サービング PLMN | サービング PLMN | N/A | |
| RADIUS | RADIUS 認証における 3GPP GGSN MCC MNC の PLMN | プライマリ ホーム PLMN | プライマリ ホーム PLMN | N/A | |
| N4 | N4 要求の X ヘッダー内の PLMN | サービング PLMN | サービング PLMN | プライマリ ホーム PLMN | N/A |

### ローミング ステータスの決定

SMF は SUPI から UE PLMN を抽出します。SMF は、UE PLMN およびサービング PLMN を構成済みの PLMN リストと比較します。SMF は、HPLMN 値に基づいて加入者のローミング状態を決定します。

UE PLMN とサービング PLMN の両方が、SMF に構成された PLMN リストに属している場合、その PLMN はホーム サブスクライバです。UE の PLMN が構成された PLMN リストに属しておらず、サービング PLMN が構成された PLMN リストに属している場合、その UE はビジター状態です。UE の PLMN が構成された PLMN リストに属しており、サービング PLMN が構成された PLMN リストに属していない場合、その UE はローミング状態です。

### ハンドオーバー シナリオ

ローミング ステータスが決定されると、引き継ぎ（HO）後に PLMN 値の構成が変更されても、ステータスは変更されません。

### ローカルポリシー

HO シナリオでは、vSMF はローカル ポリシーをサポートしています。これにより、vPLMN オペレータは、ローミング契約に従って、hPLMN ドメインからシグナリングされたパラメータをオーバーライドできます。SMF はローカル ポリシーを使用して以下を行います。

- 常時接続のセッション要求を許可します。
- ページング ポリシーの差別化
- HR モードまたは LBO モードでの PDU セッションのセットアップを許可します
- ローミング契約に従ってサブスクライバの QoS をサポートする

- HO ローミング セッションに ARP 優先順位レベル 1 ー 8 を許可します。

### その他の手順

#### ページング ポリシー差別化

SMF は、ローミング パートナーごとに異なる PPD プロファイルを使用できるように PLMN ごとに構成する必要があります。vSMF は HPLMN の適切な構成を選択し、ローミング セッションにも同じ構成を適用します。

#### PCF と UDM の選択

ローミング中に、AMFはvPCFとhPCFの両方を選択し、ポリシーの関連付け中に、vPCF IDとhPCF IDをそれぞれSMFとvPCFに送信します。SMF は、受信した vPCF ID を使用して PCF を選択します。AMF の再配置中に、ターゲット AMF は新しい vPCF と hPCF を選択します。SMF は、PDU セッションの既存の PCF から、PCF ID を含むリダイレクション通知を受信します。SMF は現在の SM ポリシー制御の関連付けを終了し、受信した PCF ID に基づいて PCF を再選択します。SMF は、再選択された PCF との SM ポリシー制御の関連付けを確立します。

ローカル構成に基づいて PCF と UDM を選択する場合、LBO ケースを使用したローミングでは PCF は VPLMN にあり、UDM は HPLMN にあるため、ローカルに構成されたアドレスはそれぞれ VPLMN と HPLMN にマッピングされます。

PCF および UDM の NRF ベースの検出の場合、クエリ基準には PCF 検出の VPLMN と UDM 検出の HPLMN が含まれます。AMF は、SMF が UDM を選択できるようにするために UDM グループ ID を送信します。SMF が PCF を選択するために使用する S-NSSAI は、AMF から受信した VPNLMN S-NSSAI である必要があります。

#### 合法的傍受

ローミング シナリオ中に、SMF は VPLMN の S-NSSAI を使用して IRI イベントを生成します。S-NSSAI 情報は、IRI イベント メッセージを介してメディエーション デバイスに送信されます。

# 自宅ルート ローミングのサポート

## 機能説明

VPLMN はパケット コアにアクセス ネットワーク サービスとパケットルーティングを提供し、HPLMN はサブスクライバにデータ ネットワーク アクセスを提供します。この機能により、SMF はホーム ルーテッド（HR）ローミングと呼ばれるルーティングのフレーバをサポートできます。

この機能では、以下の機能を提供します：

- NR を介して接続された 5G セッションのホーム ルーティング ローミング トラフィックをサポートします。
- UPF で QoS フロー ベースの課金（QBC）をサポートします。

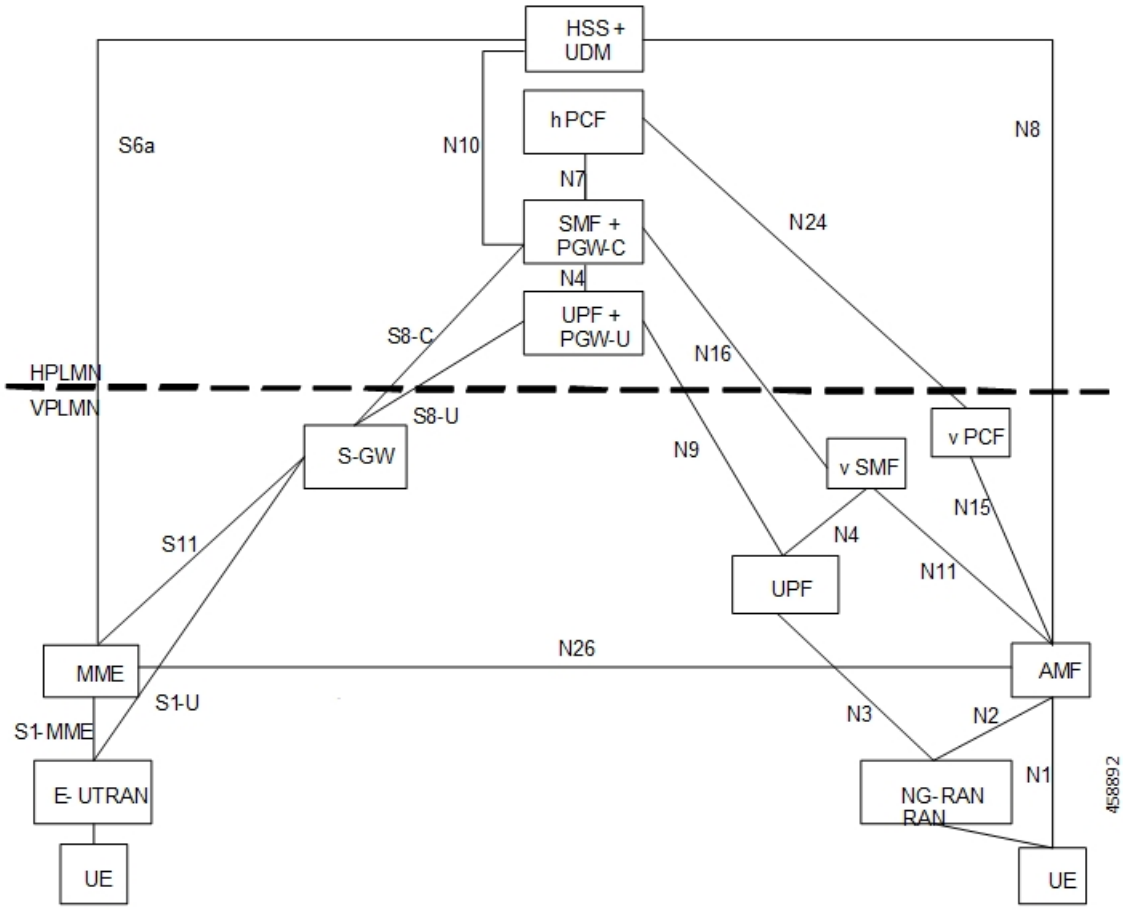
# アーキテクチャ

ここでは、HR ローミング サポート機能のアーキテクチャについて説明します。

## EPC HR ローミング シナリオ

次の図は、EPC HR ローミング シナリオのアーキテクチャを示しています。

***Figure 258: EPC HR* ローミング アーキテクチャ**



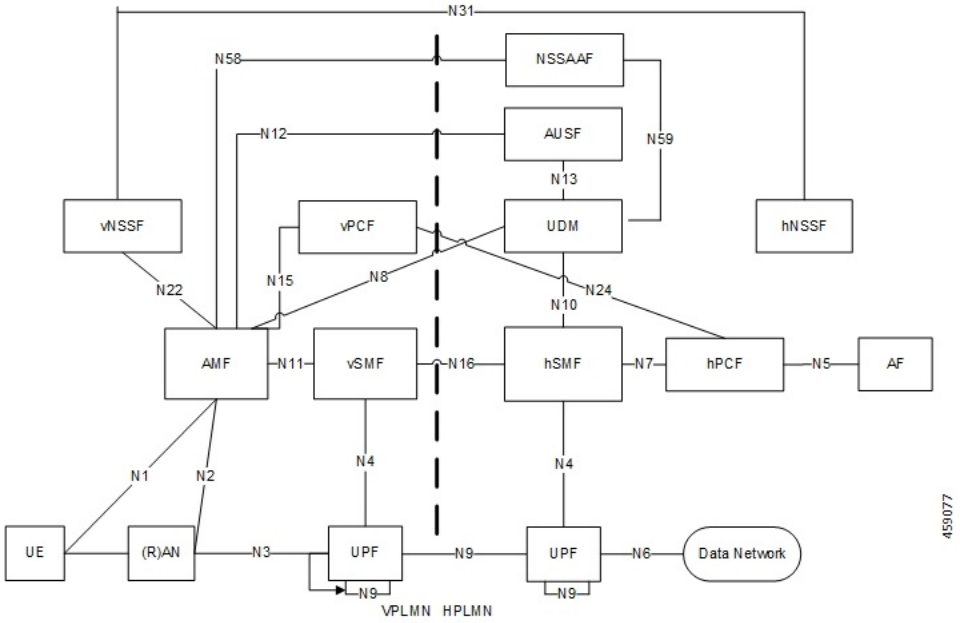

EPC HR ローミング シナリオの VPLMN および HPLMN のノードの 3GPP 参照ポイントは次のとおりです。

- SMF + IWK は HPLMN に存在します。
- SMF-IWK は、hPCF、hCHF、および UDM と情報をやりとりします。
- SMF-IWK は、（VPLMN）S-GW で S8-C をサポートします。
- vSMF は vCHF と対話します。

### 5G NR HR ローミング シナリオ

次の図は、5G NR HR ローミング シナリオのアーキテクチャを示しています。

***Figure 259: 5G NR HR* ローミング アーキテクチャ**




5G NR HR ローミング シナリオの VPLMN および HPLMN のノードの 3GPP 参照ポイントは次のとおりです。

- SMF は VPLMN と HPLMN の両方に存在します。
- vSMF および hSMF は N16 インターフェイスをサポートします。
- hSMF は、UDM、h-PCF、および h-CHF と相互作用します。
- vSMF は vCHF と対話します。
- SEPP がネットワーク内に出現すると、vSMF は hSMF メッセージングのために cSEPP と通信します。
- SCP がホームネットワークに表示されると、hSMF は UDM、hPCF、および hCHF メッセージングのために SCP と通信します。

### vSMF

SMF は、以下の訪問者の HR ローミングに関連する機能をサポートします：

- N1
  - NAS SM 情報は 2 つの部分から構成され、1 つは vSMF に表示されます（たとえば、PDU セッション タイプ、セッション AMBR、UE アドレス）。vSMF で認識されない

もう 1 つの機能（たとえば、SSC モード、PCO、QoS ルールなど）は、hSMF に透過的にリレーされます。

- vSMF は、vSMF に表示されない NAS シグナリング メッセージ情報をコンテナで hSMF に転送します。
- vSMF は、把握していない NAS シグナリング メッセージ情報を転送します。これらの情報は不明な IE、または vSMF が準拠するリリースに従って「予約済み」に設定されていない不明な値を持つ IE になります。
- vSMF は、UE に送信する NAS シグナリング メッセージの最後に、N16 コンテナで受信した不明な NAS シグナリング メッセージ情報を追加します。

- N40
  - hSMF への VPLMN の課金 ID の割り当てと転送。
  - ローミング課金プロファイルのネゴシエーション。
  - NRF が使用されている場合、vCHF は、インバウンド ローミングとして識別された UE および HPLMN の PLMN ID に基づいて選択されます。
- N4
  - V-CN-Tunnel ライフサイクル管理
- N16
  - N16 インターフェイスのサポート（vSMF と hSMF 間）。
  - 常時接続の PDU セッション許可の表示をサポートします。
- ホーム ルーティング ローミングの EPS インターワーキング手順は次のとおりです。
  - hSMF で受信した EPS ベアラー ID とマッピングされた QoS パラメータのキャッシング。AMF は、5G から 4G へのハンドオーバー中に vSMF から PDN コンテキストを取得します。また、vSMF はリリース PDN コンテキストをサポートしていますが、hSMF コンテキストへの転送はサポートしていません。
  - 4G から 5G へのハンドオーバー中。
  - 間接データ転送トンネル（IDFT）のサポート。
- PCF または UDM と対話しません。

### hSMF

SMF は、以下のローマーの HR ローミングに関連する機能をサポートします：

- N1
  - NAS SM 情報全体が hSMF によって解釈される必要があります。

- hSMF は、vSMF が 1 つのコンテナで解釈する必要がない NAS SM 情報を vSMF に向けて転送します。

- N10
  - HPLMNで定義されたS-NSSAI値を使用してUDMに登録します。
- N4
  - ユーザープレーンの非アクティブ検出はローミング中に実行されません（hUPF に非アクティブ タイマーを提供しません）。
  - ライフサイクル管理
- N40
  - 「ローミング課金プロファイル」のネゴシエーション。
  - 「ホーム提供の課金 ID」を生成します
  - NRF が使用されている場合、hCHF は、アウトバウンドローミングとして識別された UE および VPLMN の PLMN ID に基づいて選択されます。
- N7
  - hSMF の N7 インタラクションは、非ローミングの場合と同様です。
- N16
  - N16 インターフェイスのサポート（vSMF と hSMF 間）。
- UE が IPv6、IPv4v6 を使用している場合、ルータ アドバタイズメント セカンダリ認証または認証を生成します。

### ネットワークスライシング

SMF は、以下のネットワーク スライシングに関連する機能をサポートします：

- SMF は、許可された NSSAI のリストで構成できます。
- SMF がローミング中に vSMF として機能する場合、VPLMN で使用される UE が送信する S-NSSAI は、SMF で構成されている値である必要があります。
- HR では、vSMF が HPLMN で使用される NSSAI 値とともに、PDU セッション確立要求メッセージを hSMF に送信します。

### ノード選択の考慮事項

HR ローミングのノードの選択には、次の基準が適用されます。

- ローミングを有効にすると、各 SMF は interPlmnFqdn 値を NRF に登録します。これにより、AMF は別の PLMN の hSMF を選択できます。

- SMF は 、**target-plmn-list** および **requester-plmn-list** クエリ パラメータをサポートしています。
- サービス中 PLMN の NRF は、NF からのすべての発見リクエストを処理します。

### 合法的傍受

SMF は、次のネットワーク トポロジ ケースで IRI-POI 機能を提供します：

- 非ローミング ケース。
- ローミングのケース（VPLMN）。
- ローミングのケース（HPLMN）。

SMF は、ローミング シナリオ中に次の IRI イベントを生成します。

- PDU セッション確立
- PDU セッション変更
- PDU セッションの解放
- 確立された PDU セッションによる傍受の開始

### セッション管理

ローミングを考慮すると、SMF セッションは次の種類に分類されます：

- 非ローミング
- LBO
- vSMF-HO
- hSMF-HO

# 機能の仕組み

このセクションでは、セッションの作成、リリース、変更手順、および vSMF と hSMF の両方のさまざまなコール ハンドオーバー シナリオについて詳しく説明します。

## vSMF セッション作成手順

このセクションでは、vSMF のセッションの作成手順について詳しく説明します。

*Figure 260: vSMF セッション作成コール フロー*

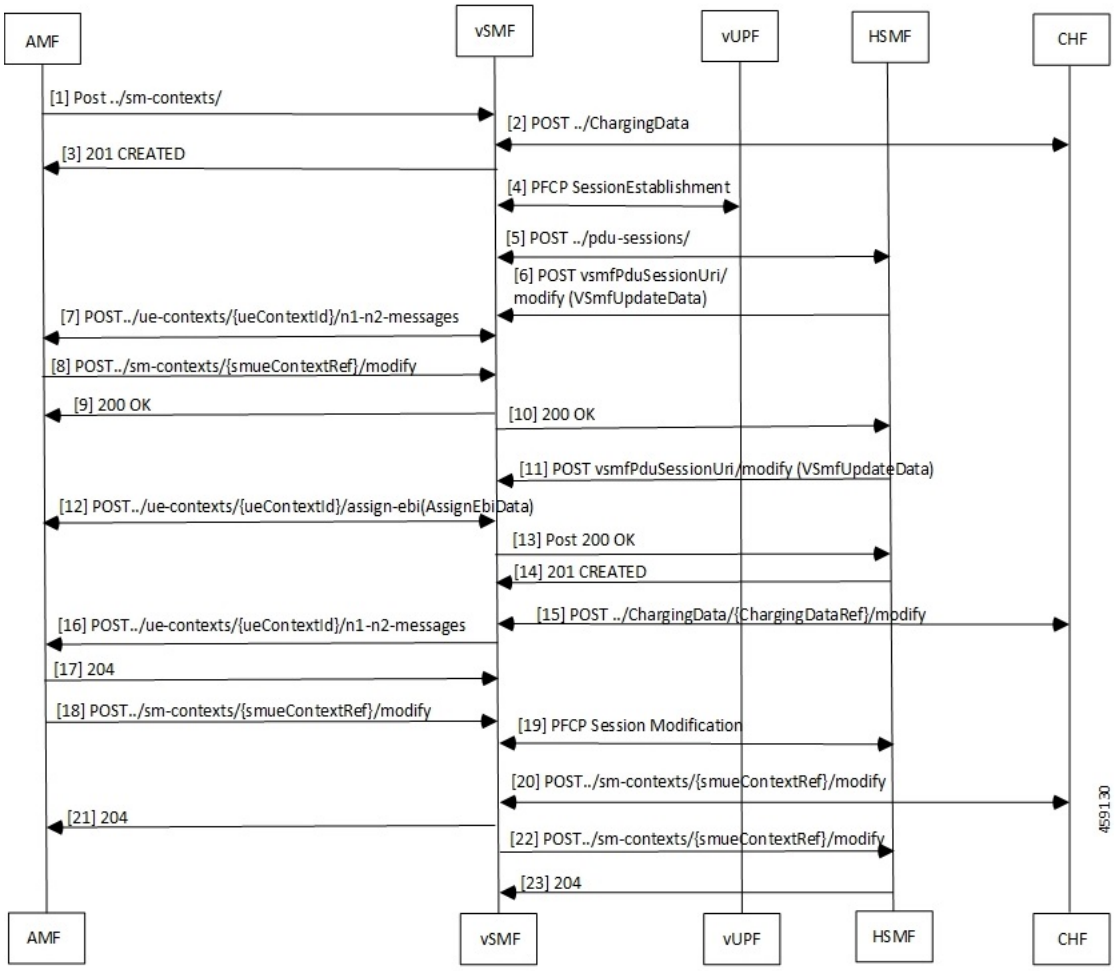



*Table 454: vSMF セッション作成コール フローの説明*

| ステップ | 説明 |
|---|---|
| 1 | AMF が UE から要求を受信します。ローカル構成に基づいて、AMF は vSMF と、UE 要求を処理する可能な hSMF のリストを見つけます。 **CreateSmContext** 要求を作成し、vSMF にメッセージを POST します。vSMF では、独自ではない hSMF URI の存在と、 の SUPI ポリシーの構成に基づいて、vSMF が有効な UE 要求の PDU コンテキストを作成します。 |
| 2 | vSMF は適切な CHF を見つけて課金アソシエーションを作成します。 |
| 3 | vSMF は、作成された PDU セッションを参照して AMF 要求に応答します。 |

| ステップ | 説明 |
|---|---|
| 4 | vSMF は、vUPF に PFCP セッションの作成要求を送信します。vUPF は、作成されたトンネルの CN トンネル情報で応答します。 |
| 5 | vSMF は、hSMF へ送信するための PDU セッション作成要求を作成します。vUPF の CN トンネル情報は、hSMF に送信される IE です。AMF からの要求パラメータのほとんどが hSMF への要求にコピーされます。N1 メッセージから次のパラメータは、hSMF に送信される前に要求から削除されます：<br>• **[常時接続の表示（Always-On Indication）]**：UE が常時接続 PDU セッションを要求し、ポリシーにより、vSMF がこのサービスを提供する準備が整っている場合、この表示は PDU セッション作成要求で設定されます。<br>• vSMF によって識別されない IE はメッセージから取り除かれ、異なるペイロードで hSMF に送信されます。<br><br>vSMF から hSMF への UE 要求は非同期に送信されます。この方法により、hSMF は、VSMF からの作成要求を処理するときに、vSMF を介して EBI 割り当て手順を開始できます。 |
| 6 | セカンダリ認証が必要な場合、hSMF は vSMF セッションのコールバック URI と変更メソッドを使用して、UE の認証要求ペイロードを送信します。 |
| 7 | vSMFはこのメッセージをAMFに送信し、AMFはvSMFに応答します。 |
| 8 | UE は、AMF によって vSMF に伝達される認証要求に応答します。 |
| 9 | vSMF は hSMF に更新を送信します。 |
| 10 | vSMF は AMF に対して変更要求に応答します。 |
| 11 | このセッションを EPC に移動できる場合、hSMF は、vSMF コールバック URI の modify メソッドを呼び出して EBI 割り当て手順を開始します。 |
| 12 | vSMF は AMF の assign-ebi メソッドを呼び出し、AMF は割り当てられた EPS ベアラー ID を vSMF に送り返します。 |
| 13 | vSMF が hSMF に応答します。 |
| 14 | 要求が hSMF で受け入れ可能な場合、GNB での PDU セッションのセットアップに必要なサブスクリプション情報を含む 201 Created 応答で応答します。この応答には N1 ペイロードも含まれています。 |
| 15 | SMF は、hSMF からの応答のパラメータを使用して CHF を更新します。このパラメータには、hSMF による課金プロファイルの設定が含まれます。 |

| ステップ | 説明 |
|---|---|
| 16 | vSMF は AMF への N1N2MessageTransferRequest を作成します。<br>• N2 ペイロードは、PDU セッション作成データで送信されたパラメータと、vUPF からの CN トンネル情報を使用して作成されます。<br>• N1 ペイロードは、hSMF からのバイナリ ペイロードを使用して作成されます。常時オンのインジケータは、PDU セッション作成データで受信される値に基づいて設定されます。 |
| 17 | AMF が N1N2MessageTransfer 要求に応答します。 |
| 18 | GNB は AMF に対する EARB RESOURCE SETUP REQUEST に N2 応答で応答します。AMF はこの AMF を SmContext Update メッセージで vSMF に送信します。 |
| 19 | vSMF は vUPF に、手順 6 で hSMF によって送信された GNB のトンネル情報、トンネル、およびその他の情報を更新するように要求します。vUPF が vSMF に応答します。 |
| 20 | 必要な場合、vSMF は CHF を追加情報で更新します。 |
| 21 | vSMFはAMFからの更新要求に応答します。 |
| 22 | 設定に失敗したフローがある場合、vSMF はその内容を hSMF に通知します。 |
| 23 | hSMF が vSMF に応答します。 |

## hSMF セッション作成手順

このセクションでは、hSMF のセッションの作成手順について詳しく説明します。

*Figure 261: hSMF セッション作成コール フロー*

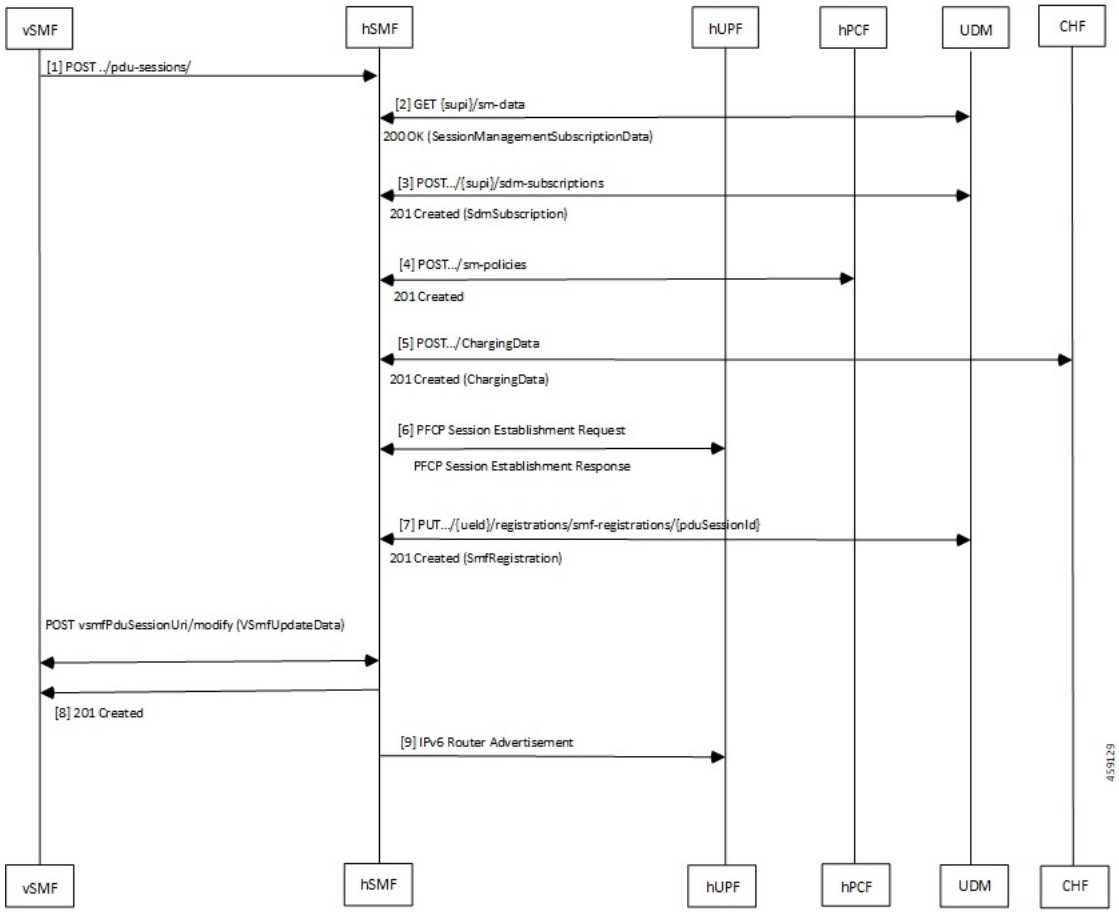



*Table 455: hSMF セッション作成コール フローの説明*

| ステップ | 説明 |
|---|---|
| 1 | hSMF は、vSMF から PDU セッションを作成する要求を受信します。要求には JSON 部分があり、vSMF が処理できなかった IE のリストが含まれるバイナリ部分もあります。 |
| 2 | hSMF は、UDM から UE のサブスクリプション データを取得します。 |
| 3 | サブスクリプションデータに基づいてセッションを確立できる場合、SMF はサブスクリプション データの変更を UDM にサブスクライブします。 |

| ステップ | 説明 |
|---|---|
| 4 | hSMF は PCF とのポリシーの関連付けを作成します。PCF は、AMF によって選択されて hSMF にシグナリングされたもの、または hSMF での NRF ベースまたはポリシーベースの選択のいずれかです。 |
| 5 | [課金データの関連付け]が CHF と作成されます。 |
| 6 | ステップ 1 で vSMF によって提供された CN トンネル情報を使用して、hSMF は hUPF に CN トンネルを作成します。hUPF は、hUPF 上の CN トンネル情報で応答します。 |
| 7 | hSMF は、この DNN での UE の通知について UDM に登録します。 |
| 8 | hSMF は、hUPF の CN トンネル情報と、UE に送信する必要がある N1 情報要素を使用して、vSMF からの要求に応答します。UE が常時接続のセッションを要求しており、これが hSMF で許容される場合は、応答で vSMF にそのことが示されます。 |
| 9 | IPV6 ルータ アドバタイズメントを送信する必要がある場合、hSMF は UPF にそのタスクを実行するように要求します。 |

## vSMF セッション変更手順

このセクションでは、vSMF のセッション変更手順について詳しく説明します。

*Figure 262: vSMF セッション変更コール フロー*

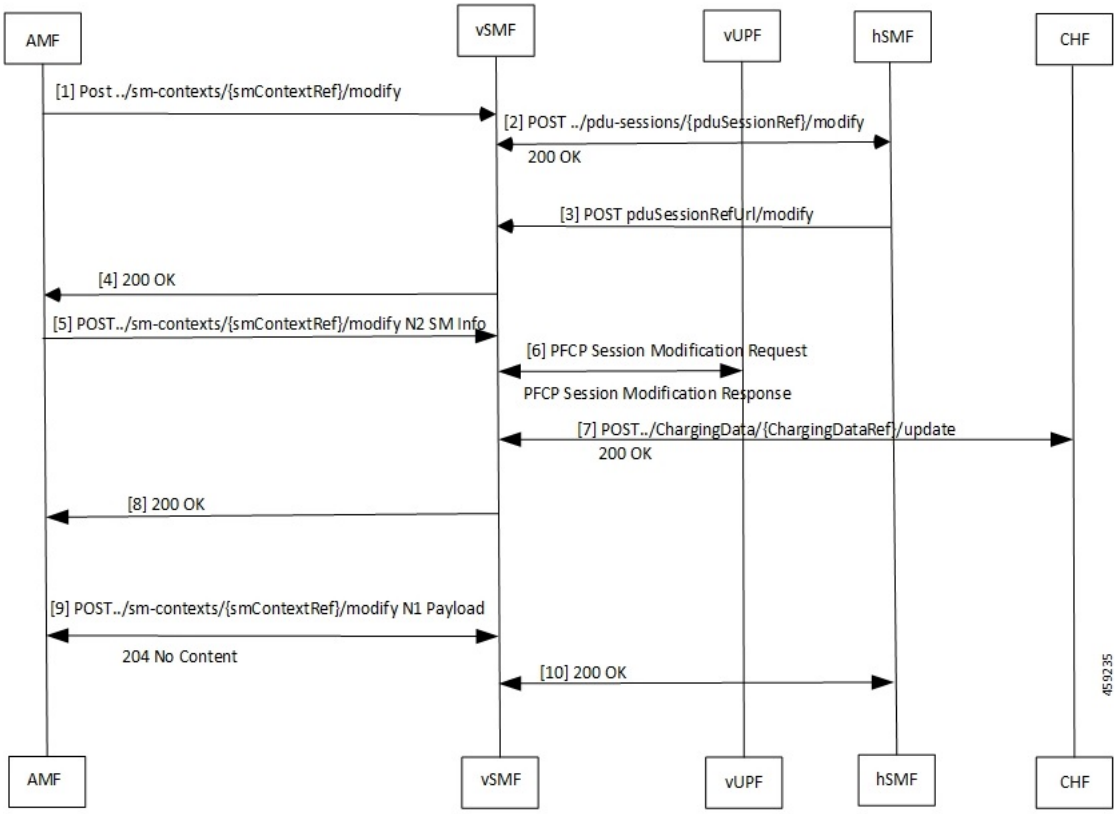



*Table 456: vSMF セッション変更コール フローの説明*

| ステップ | 説明 |
|---|---|
| 1 | AMF は、Sm コンテキスト更新メッセージとして UE からの要求を vSMF に送信します。 |
| 2 | vSMF は、メッセージの作成中に hSMF が返した参照を使用します。メッセージの関連部分を hSMF にポストします。hSMF がメッセージに応答します。 |
| 3 | hSMF は vSMF に更新要求を送信します。このメッセージには、要求メッセージの一部として gNB または UE に送信される N1 メッセージおよび N2 メッセージが含まれています。 |
| 4 | vSMF は hSMF からの情報を組み合わせ、UE と gNB の N1 および N2 ペイロードを作成します。次に、これらをAMFからの元の要求の応答に追加します。 |
| 5 | AMF は N2 応答を gNB にリレーします。 |

| ステップ | 説明 |
|---|---|
| 6 | UEによって要求され、ネットワークが承認した変更（たとえば、フローの追加または削除）が原因でUPFに変更がある場合、vSMFはこれらの変更でUPFを更新します。 |
| 7 | vSMF は、UPF に適用された変更に対する課金トリガーを CHF に通知します。 |
| 8 | vSMF は、200 OK メッセージで AMF からの N2 メッセージを確認します。 |
| 9 | AMF が UE から N1 ペイロードを転送し、vSMF がそれを確認します。 |
| 10 | vSMF は、hSMF からのセッション変更の要求に応答します。 |

# hSMF セッション変更手順

このセクションでは、hSMF のセッション変更手順について詳しく説明します。

***Figure 263: hSMF セッション変更コール フロー***

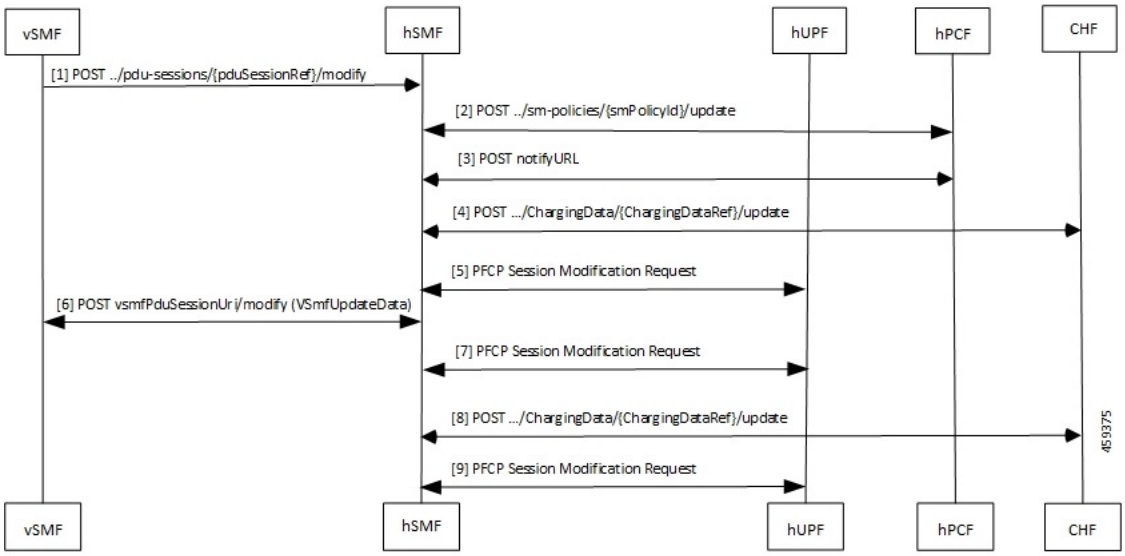



***Table 457: hSMF セッション コール フローの変更の説明***

| ステップ | 説明 |
|---|---|
| 1 | UE 要求が vSMF から hSMF に到達します。 |
| 2 | いずれかの hPCF トリガー基準が満たされると、hSMF は hPCF に更新要求を送信します。 |

| ステップ | 説明 |
|---|---|
| 3 | hSMF は UE 要求に応答し、例外を処理します。 |
| 4 | vSMF は、UPF に適用された変更の課金トリガーを CHF に通知します。 |
| 5 | UE が要求し、ネットワークが受け付けた変更（フローの追加や削除など）により UPF に 変更がある場合、vSMF はこれらの変更で UPF を更新します。 |
| 6 | PDU セッションを更新する UE 要求が、vSMF から hSMF に到達します。 |
| 7 | UE が要求し、ネットワークが受け付けた変更（フローの追加や削除など）により UPF に 変更がある場合、vSMF はこれらの変更で UPF を更新します。 |
| 8 | vSMF は、UPF に適用された変更の課金トリガーを CHF に通知および更新します。 |
| 9 | UE が要求し、ネットワークが受け付けた変更（フローの追加や削除など）により UPF に 変更がある場合、vSMF はこれらの変更で UPF を更新します。 |

## vSMF リリース セッションの手順

このセクションでは、vSMF のセッションの解放手順について詳しく説明します。

*Figure 264: vSMF リリース セッション コール フロー*

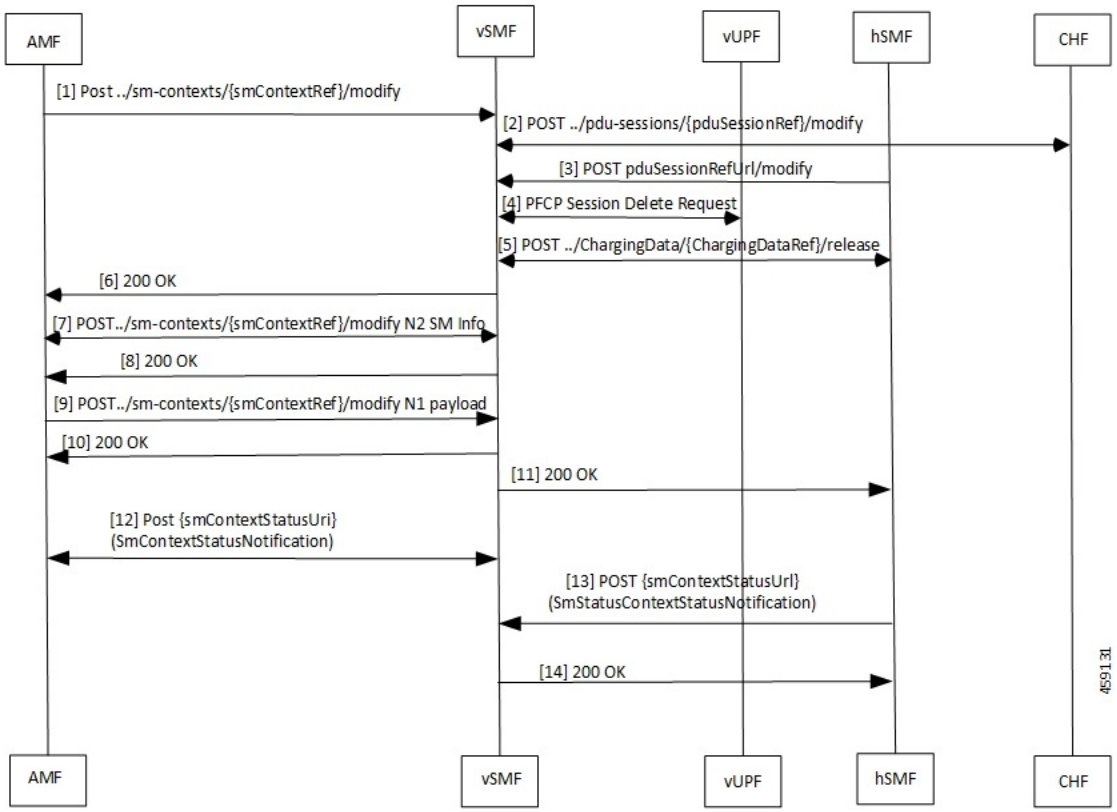



*Table 458: vSMF リリース セッション コール フローの説明*

| ステップ | 説明 |
|---|---|
| 1 | UE は PDU セッションのリリースを開始します。 |
| 2 | vSMF は、hSMF からリリース要求の応答を受信します。 |
| 3 | hSMF は、リリース表示を true に設定した変更要求の形式で要求をリリースするように要求に応答します。 |
| 4 | vSMF が PFCP セッションを解放します。 |
| 5 | vSMF が課金セッションを解放します。 |
| 6 | vSMF は 200 OK 応答メッセージで AMF に応答します。 |
| 7 | AMF は N2 変更要求で応答します。 |
| 8 | vSMF は 200 OK 応答メッセージで要求に応答します。 |

| ステップ | 説明 |
|---|---|
| 9 | AMF は N1 変更要求を vSMF に送信します。 |
| 10 | vSMF は 200 OK メッセージで応答します。 |
| 11 | vSMF は、hSMF PDU セッション変更要求に応答します。 |
| 12 | vSMF はこの通知を AMF に転送します。 |
| 13 | hSMFは、リリースが完了したことを示すSmコンテキストのステータス通知を送信します。 |
| 14 | vSMF は通知の受信を確認応答します。 |

## hSMF リリース セッションの手順

このセクションでは、hSMF のセッションの解放手順について詳しく説明します。

***Figure 265: hSMF*** リリース セッションのコール フロー

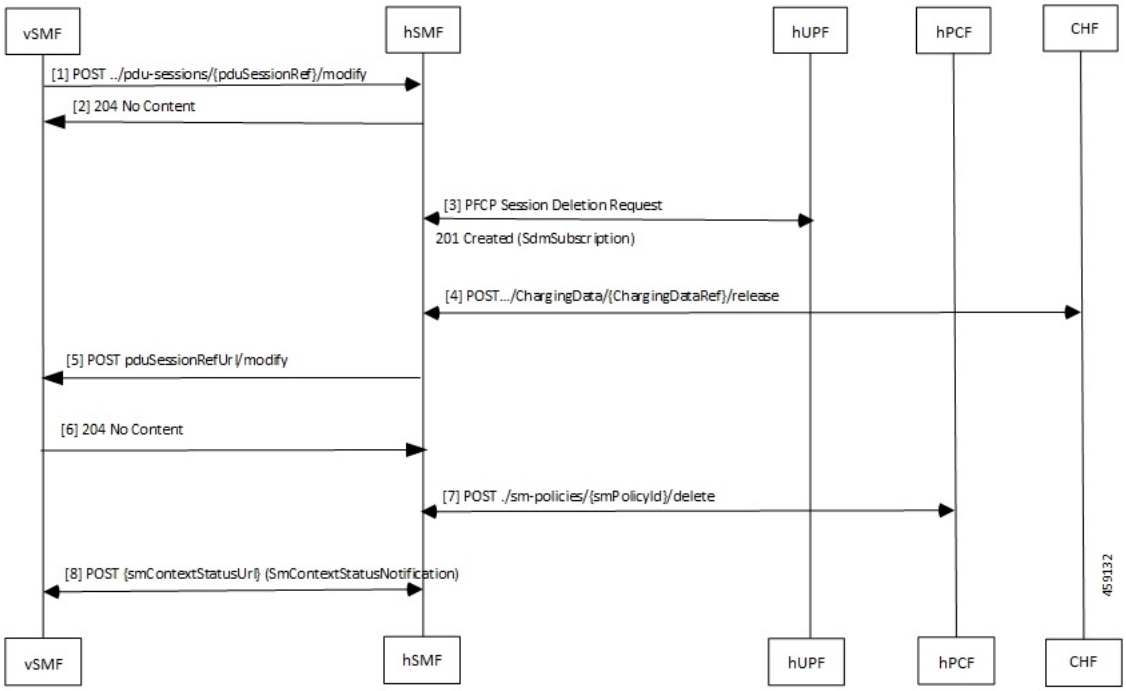


*Table 459: hSMF* リリース セッション コール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | vSMF は、hSMF にリリース要求を転送します。 |
| 2 | hSMF は 204 No Content メッセージで応答します。 |
| 3 | hSMF が PFCP セッションを解放します。 |
| 4 | hSMF が課金セッションを解放します。 |
| 5 | hSMF は、リリース表示を true に設定した変更要求の形式で要求をリリースするよう、vSMF に要求を送信します。 |
| 6 | vSMF は 204 No Content メッセージで応答します。 |
| 7 | hSMF は、関連付けられた Sm ポリシーを解放します。 |
| 8 | hSMF はこの通知を vSMF に転送します。 |

## vSMF クリア サブスクライバのリリースセッションの手順

このセクションでは、Ops Center を使用した vSMF のセッションの解放手順について詳しく説明します。

*Figure 266: vSMF クリア サブスクライバ リリース セッションのコール フロー*

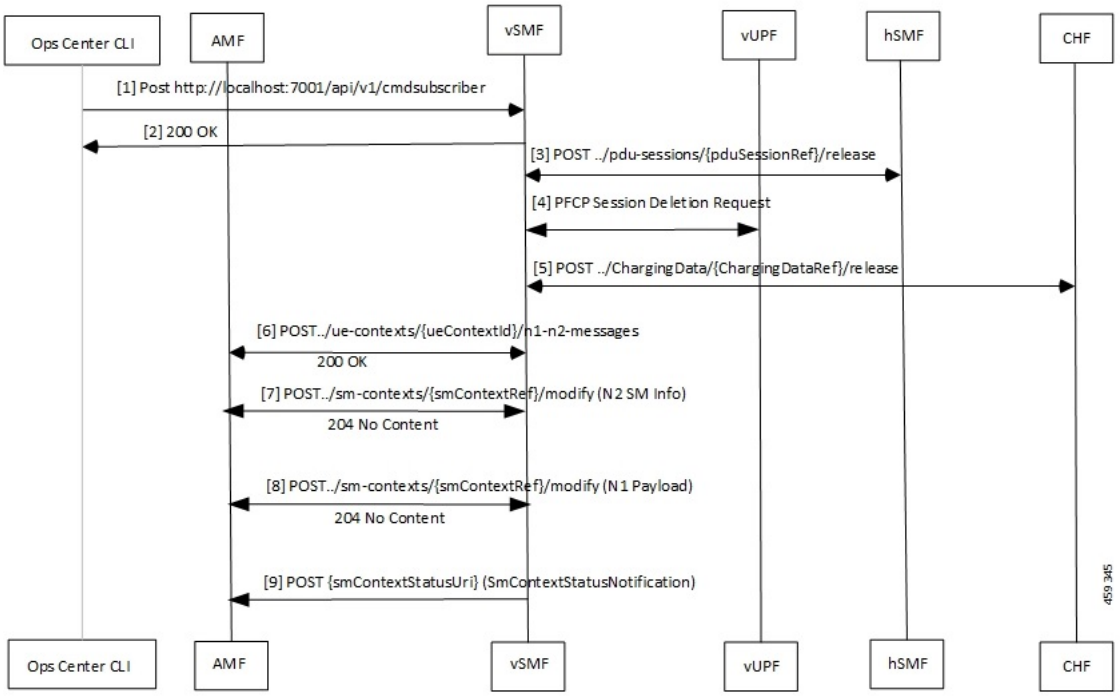



*Table 460: vSMF クリア サブスクライバ リリース セッションのコール フローの説明*

| ステップ | 説明 |
|---|---|
| 1 | Ops センターまたは vUPF は、明確なサブスクライバのリリース要求を発行します。 |
| 2 | vSMF はメッセージの受信を確認応答します。 |
| 3 | vSMF は、hSMF からリリース要求の応答を受信します。 |
| 4 | vSMF が vUPF の PFCP セッションをリリースします。 |
| 5 | vSMF は課金セッションを解放し、CHF を更新します。 |
| 6 | AMF が N1/N2 転送要求を受信します。 |
| 7 | vSMF は、N2 ステータスに関する情報を受信し、204 No Content メッセージで承認します。 |
| 8 | vSMF は AMF から N1 リリース完了通告を受信し、204 No コンテンツ メッセージで応答します。 |
| 9 | vSMF は、セッションが解放されたことを示す Sm コンテキスト ステータス通告メッセージで AMF を更新します。 |

# N26 インターフェイスを使用した EPS から 5G へのハンドオーバー

このセクションでは、N26 インターフェイスを使用した EPS から 5G へのハンドオーバー手順のコール フローについて説明します。

***Figure 267: N26** インターフェイスを使用した **EPS** から **5G** へのハンドオーバーのコール フロー*

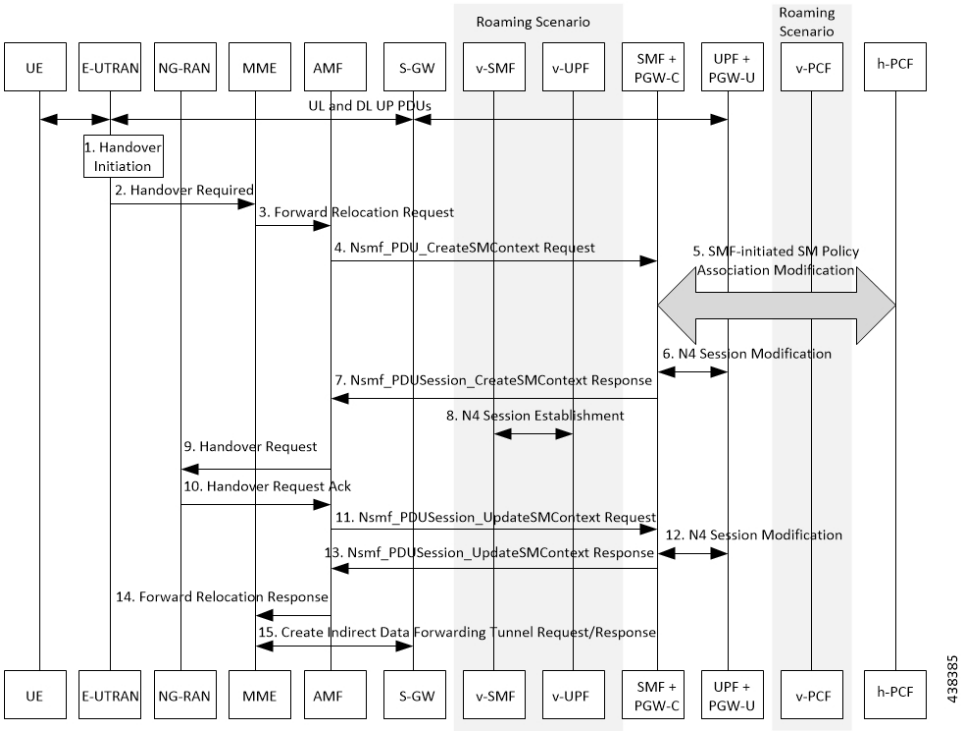



***Table 461: N26** インターフェイスを使用した **EPS** から **5G** へのハンドオーバーのコール フローの説明*

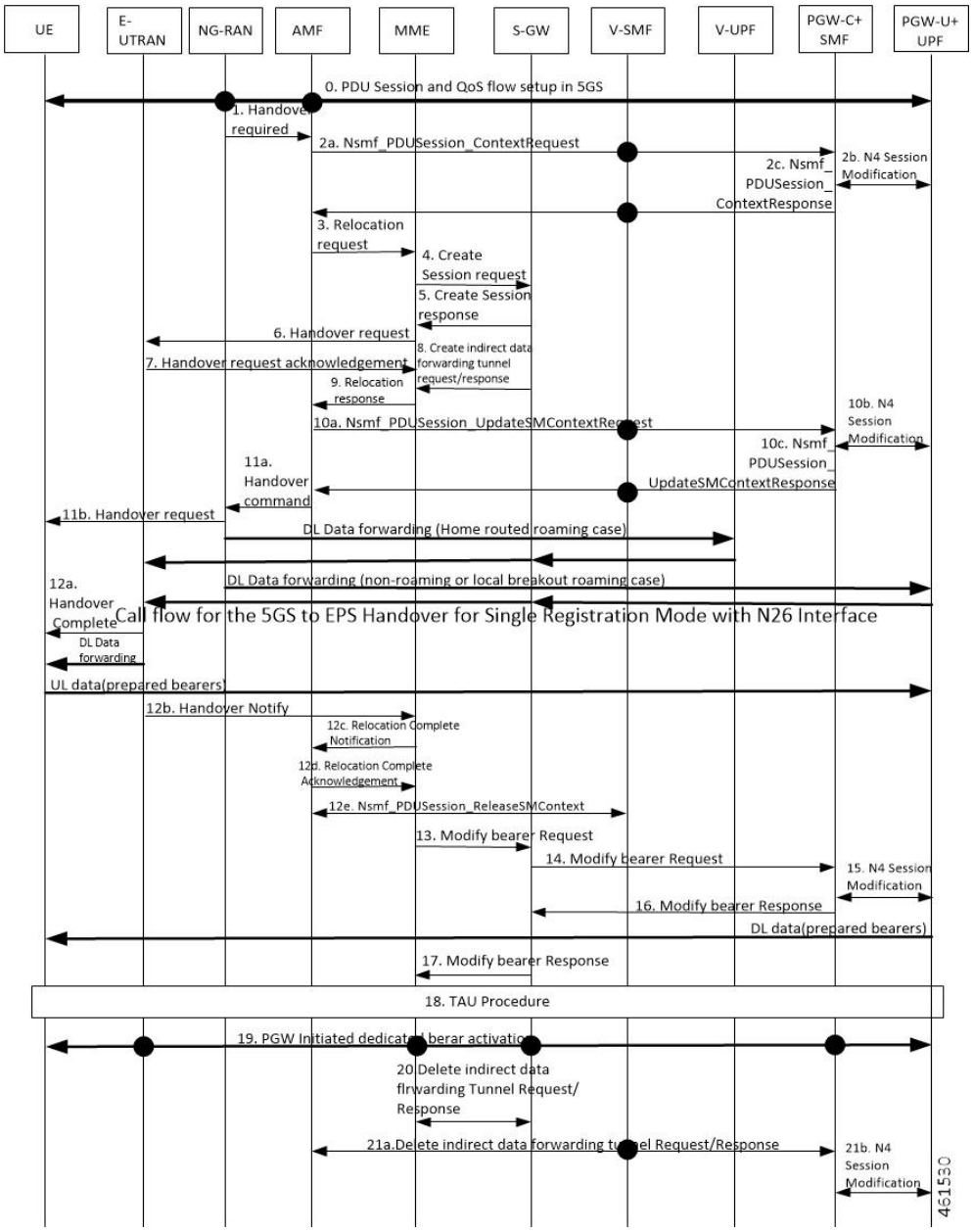
| ステップ | 説明 |
|---|---|
| 1 | コール ハンドオーバーの開始は、UE と E-UTRAN から相互に向けて開始され、E-UTRAN から S-GW へと進みます。次に、ローミング コールの場合、コール ハンドオーバーの開始は S-GW から UPF + P-GW-U に行われます。 |
| 2 | E-UTRAN が MME にハンドオーバー コール要求を送信します。 |
| 3 | MME は再配置要求を AMF に転送します。 |
| 4 | AMF は、SMF で NsmfPDUSessionCreateSMContext サービス操作を呼び出します。PGW-C+SMF アドレスは、このサービス操作を識別します。サービス操作は、[UE EPS PDN接続（UE EPS PDN Connection）]、[AMF ID]、または [ダイレクト転送フラグ（Direct Forwarding Flag）] です。AMFは、稼働パスの切り替えを回避するための引き継ぎの準備を示します。SMF は EPS ベアラー コンテキストに基づいて、対応する PDU セッションを検索します。AMF には、間接データ転送の適用可能性を SMF に通知するための Direct Forwarding Flag が含まれています。 |

| ステップ | 説明 |
|---|---|
| 5 | ダイナミック PCC を導入した場合、SMF + PGW-C は SMF によって開始される SM ポリシーの変更を PCF に対して開始します。 |
| 6 | PGW-C+SMF は PGW-U+UPF に N4 セッション変更を送信して、PDU セッションの CN トンネルを確立します。PGW-U + UPF は、NG-RAN からアップリンク パケットを受信します。この手順では、既存の 4G ベアラーからマッピングされた QFI とともに、5G セッションのアップリンク PDR および FAR を作成する必要があります。 |
| 7 | PGW-C+SMFは、NsmfPDUSessionCreateSMContext応答を AMF に送信します。この応答には、PDU セッション ID、S-NSSAI、および N2 SM の情報が含まれます。<br>N2 SM 情報には、PDU セッション ID、S-NSSAI、QFI、QoS プロファイル、EPS ベアラー セットアップ リスト、EBI と QFI の間のマッピング、CN トンネル情報、および原因コードの詳細が含まれます。<br>SMF には、EBI と QFI 間のマッピングが N2 SM 情報コンテナとして含まれています。P-GW-C+SMF が、PDU セッションで EPS から 5GS へのセッション継続性がサポートされていないと判断した場合、P-GW-C+SMF は、対応する PDU セッションのセッション マネージャ情報を提供しません。ただし、P-GW-C+SMF は、N2 SM 情報に PDU セッション転送を拒否する原因コードの詳細を含めます。 |
| 8 | V-SMF と V-UPF は、相互に N4 セッションを確立します。 |
| 9 | AMF は、NG-RAN にハンドオーバー要求を送信します。 |
| 10 | NG-RANは、受信したハンドオーバー要求の確認応答をAMFに送信します。 |
| 11 | AMF は、N3 トンネル情報を更新するために、NsmfPDUSessionUpdateSMContext 要求、T-RAN SM N3 転送情報リスト メッセージを SMF に送信します。<br>NsmfPDUSessionUpdateSMContext 要求には、PDU セッション ID、S-NSSAI、N2 SM の情報が含まれています。トンネル情報は、NG-RAN から受信したハンドオフ要求承認の NGAP IE DL 転送 UP TNL 情報に存在します。 |
| 12 | SMF + PGW-U に対する N4 セッション変更を実行し、eNodeB から NG-RAN に DL データを転送するための間接トンネルを作成します。この手順では、リダイレクトされた DL データの UL PDR を作成し、それらに FAR を関連付けて FAR を NG-RAN に転送することも含まれます。これらの PDR と FAR のマッピングは、QFI と対応するベアラー ID に基づいています。 |
| 13 | PGW-C+SMF は、NsmfPDUSessionUpdateSMContext 応答を AMF に送信します。この応答には、PDU セッション ID、EPS ベアラー セットアップ リスト、およびデータ転送用の CN トンネル情報が含まれます。この時点で、DL データ転送用の間接トンネルが確立されます。 |
| 14 | AMF が再配置応答を MME に送信します。 |

| ステップ | 説明 |
|---|---|
| 15 | MME は、間接データ転送トンネルの作成要求を S-GW に送信します。S-GW は、間接データ転送トンネルの応答を MME に送信します。 |

# N26 インターフェイスを使用したシングル登録モードでの 5GS から EPS へのハンドオーバー

図 *268 : N26* インターフェイスを使用したシングル登録モードでの *5GS* から *EPS* へのハンドオーバーのコール フロー




**重要** HPLMN の PGW-C+SMF でマッピングされた QoS パラメータが提供されない場合、IP アドレスの保持はサポートされません。

表 *462 : N26* インターフェイスを使用したシングル登録モードの *5GS* から *EPS* へのハンドオーバーのコール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | NG-RAN は、必要なハンドオーバー（ターゲット eNB ID、Source to Target Transparent Container、システム間ハンドオーバー指示）メッセージを AMF に送信します。 |
| 2a | AMF は Nsmf_PDUSession_ContextRequest を送信して、マッピングされた EPS ベアラー コンテキストも含む SM コンテキストを提供するように V-SMF に要求します。<br>（注）<br>AMF は、ローカル構成を通じて、非 IP PDN タイプをサポートするかどうかを認識します。<br>（注）<br>家庭用ルーティング ローミングのシナリオでは、UE の SM EPS コンテキストは V-SMF から取得されます。 |
| 2b | PGW-C + SMF は、N4 セッション変更を PGW-U + UPF に送信して、各 EPS ベアラーの CN トンネルを確立し、EPS ベアラー コンテキストを AMF に提供します。 |
| 2c | PGC+SMF は Nsmf_PDUSession_ContextResponse を送信して、マッピングされた EPS ベアラー コンテキストも含む SM コンテキストを提供するように V-SMF に要求します。 |
| 3 | AMF は、変更および明確化された転送再配置要求を送信します。 |
| 4 | MME が Create_Session_Request を S-GW に送信します。 |
| 5 | S-GW は、Create_Session_Response を MME に送信します。 |
| 6 | MME はハンドオーバー要求（PLMN IDに関する情報を含むハンドオーバー制限リストの情報が含まれている場合があります）を E-UTRAN に送信します。 |
| 7 | E-UTRAN が MME にハンドオーバー要求の承認を送信します。 |
| 8 | MME と S-GW 間で間接データ転送トンネル要求または応答を作成します。 |
| 9 | MME が再配置応答を AMF に送信します。 |
| 10a | AMF は、間接データ転送トンネルを作成するために、Nsmf_PDUSession_UpdateSMContext 要求（サービング GW アドレスおよびデータ転送用のサービング GW DL TEID）を PGW-C+SMF に送信します。 |
| 10b | N4 セッション変更要求は PGW-C+SMF と PGW-U+UPF 間で送信されます。 |

| ステップ | 説明 |
|---|---|
| 10c | PGW-C+SMF は、間接データ転送を作成するために、Nsmf_PDUSession_UpdateSMContext Response（原因、データ転送の CN トンネル情報、データ転送の QoS フロー）を AMF に返します。QFI と、データ転送用のサービング GW アドレスと TEID との相関に基づいて、PGW-U + UPF は、QoS フローを EPC のデータ転送トンネルにマッピングします。 |
| 11a | AMF は、送信元の NG-RAN にハンドオーバー コマンドを送信します。 |
| 11b | NG-RAN は送信元 UE にハンドオーバー コマンドを送信します。 |
| 12a | UE はハンドオーバー完了コマンドを送信元の UE NG-RAN に送信します。 |
| 12 b | E-UTRAN は、送信元 UE MME にハンドオーバー通知を送信します。 |
| 12C | MME が再配置完了通知を AMF に送信します。 |
| 12 d | AMF は、Relocation Complete Acknowledge メッセージで MME に確認応答します。NG-RAN および PGW-C+SMF のリソースが解放されるタイミングを監視するために、AMFのタイマーが開始されます。 |
| 13 | MME が、ベアラー要求の変更を S-GW に送信します。 |
| 14 | S-GW はベアラーの変更を PGW-C+SMF に送信します。 |
| 15 | PGW-C＋SMF は、UPF＋PGW-U の方向で N4 セッション変更手順を開始し、ユーザープレーン パスのダウンリンク ユーザープレーンを更新します。これにより、指定された PDU セッションが E-UTRAN に切り替えられます。PGW-C + SMF は、UPF + PGW-U の PDU セッションの CN トンネルのリソースを解放します。 |
| 16 | PGW-C+SMF は、ベアラー応答の変更を S-GW に送信します。 |
| 17 | S-GW が、ベアラー応答の変更を MME に送信します。 |
| 18 | UE はトラッキング エリア更新手順（TAU）を開始します。 |
| 19 | PGW-C+SMF は、非 GBR QoS フローに対して専用ベアラーのアクティベーション手順を開始します。 |
| 20 | 間接データ転送トンネルの要求と応答が MME と S-GW で削除される |
| 21a | 間接データ転送トンネルの要求と応答がAMFおよびPGW-C+SMF で削除されました。 |
| 21b | N4 セッション変更要求は PGW-C+SMF と PGW-U+UPF 間で送信されます。 |

# N26 インターフェイスを使用しない EPS から 5G へのハンドオーバー

このセクションでは、N26 インターフェイスを使用しない EPS から 5G へのハンドオーバー手順のコール フローについて説明します。

***Figure 269: N26** インターフェイスを使用しない **EPS** から **5G** へのハンドオーバーのコール フロー*

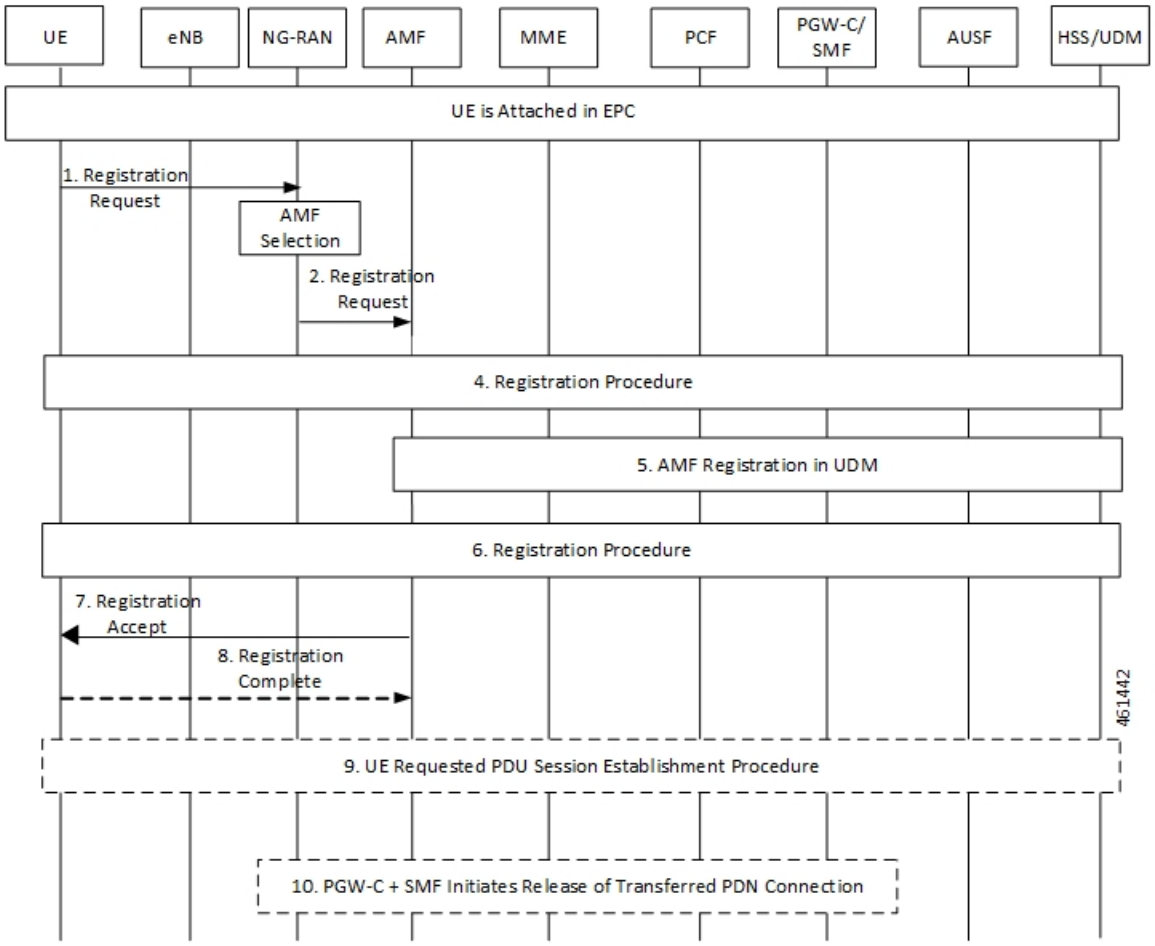



***Table 463: N26** インターフェイスを使用しない **EPS** から **5G** へのハンドオーバーのコール フローの説明*

| ステップ | 説明 |
|---|---|
| 1 | UE は NG-RAN への登録要求を開始します。 |
| 2 | NG-RAN は AMF を選択します。 |
| 3 | NG-RANは、N2 メッセージパラメータを含む登録要求を新しいAMFに転送します。 |

| ステップ | 説明 |
|---|---|
| 4 | TS 23.502 の「一般的な登録」の手順を参照してください。 |
| 5 | 新しいAMFは、アクセスを登録するためにNudm_UECM_Registrationを使用してUDMに登録します。 |
| 6 | TS 23.502 の「一般的な登録」の手順を参照してください。 |
| 7 | 新しい AMF は、Registration Accept メッセージを UE に送信します。<br>AMF には、UE への「Interworking without N26」インジケータが含まれています。 |
| 8 | UE は、新しい AMF に対して登録完了メッセージで応答します。 |
| 9 | UE は PDU セッション確立手順を開始します。 |
| 10 | PGW-C+SMF は、PDN GW によって開始されたベアラーの非アクティブ化手順を実行することにより、5GS に転送された PDN 接続の EPC 内のリソースの解放を実行します。 |

## N26 インターフェイスを使用しない 5G から EPS へのハンドオーバー

このセクションでは、N26 インターフェイスを使用した 5G から EPS へのハンドオーバー手順のコール フローについて説明します。

*Figure 270: N26* インターフェイスを使用した *5G* から *EPS* へのハンドオーバーのコール フロー

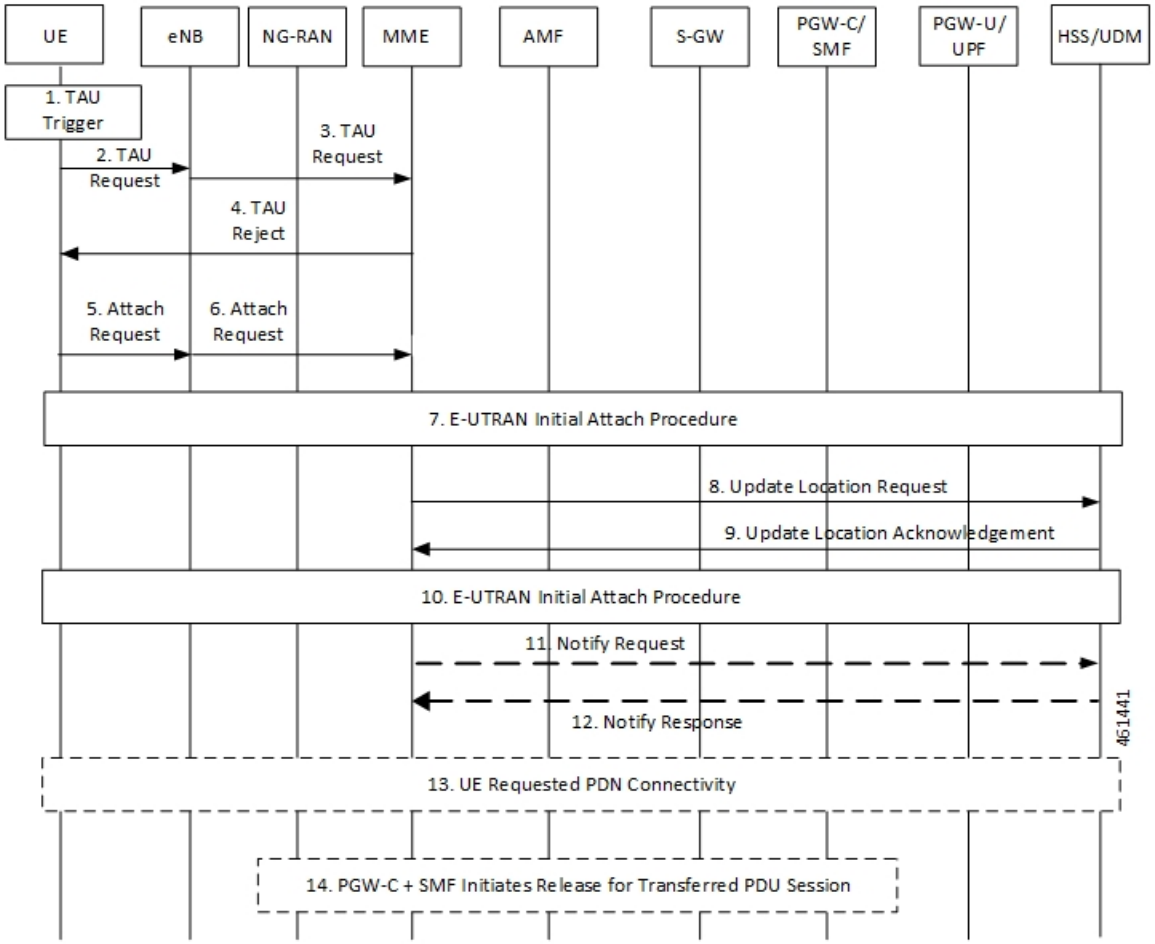



*Table 464: N26* インターフェイスを使用した *5G* から *EPS* へのハンドオーバーのコール フローの説明

| ステップ | 説明 |
|---|---|
| 1 - 2 | UE は、eNodeB へ TAU リクエスト を送信することで TAU 手順を初期化します。 |
| 3 | eNodeB は、新しい MME に TAU リクエスト メッセージを転送します。 |
| 4 | 古いノードが 5G-GUTI からマッピングされた UE の GUTI に基づいて AMF であり、かつ MME が N26 手順なしで 5GS-EPS インターワーキングをサポートするように構成されている場合、MME は UE に TAU 拒否を送信します。 |
| 5 | UE は eNodeB への接続要求を開始します。 |

| ステップ | 説明 |
|---|---|
| 6 | eNodeB は、接続要求を新しい MME にリレーします。 |
| 7 | TS 23.401 の E-UTRAN 初期接続の手順を参照してください。 |
| 8 | MME が最後のデタッチ以降に変更された場合、MME に UE の有効なサブスクリプション コンテキストがない場合、または UE が IMSI を提供するか、UE がまたは、eNodeB によって提供される TAI の PLMN-ID が UE のコンテキストでの GUTI の PLMN-ID と異なる場合、MME はロケーション更新要求メッセージを HSS に送信します。 |
| 9 | HSS は、更新ロケーション ACK（IMSI、サブスクリプションデータ）を新しい MME に送信することにより、更新ロケーション メッセージを確認応答します。 |
| 10 | TS 23.401 の E-UTRAN 初期接続の手順を参照してください。 |
| 11 | MME は、ベアラー応答の変更（EPS ベアラー ID）メッセージを受信すると、非 3GPP アクセスによるモビリティのために、APN および PDN GW ID を含む通知要求を HSS に送信します。メッセージには、PDN GW がある PLMN を識別する情報が含まれます。 |
| 12 | 緊急事態以外のサービスの場合、HSS は APN と PDN GW の ID のペアを保存します。緊急サービスの場合、HSS は「緊急サービスで現在使用されている PDN GW」を保存します。次に、HSS は、通知応答を MME に送信します。 |
| 13 | UE に EPS に転送して同じ IP アドレス/プレフィックスを維持する必要がある残りの PDU セッションが 5GS にある場合、UE は UE 要求の PDN 接続手順を実行し、要求タイプを「ハンドオーバー」に設定します。UE は、EPS に転送する PDU セッションに対応する APN と PDU セッション ID を提供します。 |
| 14 | PGW-C+SMF は、EPS に転送された 5GS で PDU セッションのリリースを開始します。 |

## 標準準拠

ホーム ルーティング ローミング サポート機能は、次の規格に準拠しています。

- *3GPP TS 23.501 v 15.4.0*
- *3GPP TS 23.502 v 15.4.0*
- *3GPP TS 23.503 v 15.4.0*
- *3GPP TS 33.501 v 15.4.0*
- *3GPP TS 33.128 v15.4.0*
- *3GPP TS 33.127 v15.4.0*
- *3GPP TS 32.240 v 15.4.0*
- *3GPP TS 29.244 v15.4.0*

- *3GPP TS 32.291 v 15.3.0*
- *3GPP TS 29.500*、バージョン *16.8.0*
- *3GPP TS 29.502*、リリース *16*
- *3GPP TS 29.502 v15.7.0*（*2020* 年 *4* 月）

## 制限事項

このリリースでは、ホーム ルーティング ローミングのサポート機能に次の制限があります。

- 不明な NAS SM 情報（不明な IE）はサポートされていません。
- VPLMN-ID は、Charging-ID 内に埋め込まれません。

# HR ローミングの課金サポート

***Table 465:*** **機能の履歴**

このセクションでは、HR ローミング機能の課金サポートについて説明しています。

この機能は、次の機能をサポートしています。

1. **QBC 課金およびプロファイル管理**
   - QBC 課金をサポートします。
   - ローミング QBC プロファイルを設定します。
   - ローミング QBC プロファイルを CHF にリレーします。
   - CHF からローミング QBC プロファイルを受信します。
2. **SMF 間の QBC プロファイルの連携動作**
   - ローミング QBC プロファイルをリレーします。
     - vSMF から hSMF の間で使用。
     - hSMF から hCHF の間。
     - vSMF から vCHF の間で使用。
3. **vSMF での QBC 処理**
   - vSMF で、UPServ は次への課金と連携します。
     - N4 インターフェイスで QFI の PDR を作成します。
     - ローミング QBC プロファイルから派生した関連 URR を生成します。

- QBC プロファイルから派生した URR 使用状況レポートを、QoS フローレポートのために QFi コンテナ内のそれぞれの CHF にリレーします。

**4. エラー処理と特別な条件**

- 対応する QBC 課金プロファイルを識別できないセッションの QBC を無効にします。
- CHF からのフェールオープン動作をサポートします。

**5. 設定のサポート**

- 次の場合に QBC を有効にする設定を可能にします。
  - ホーム SMF（hSMF）
  - 閲覧先 SMF（vSMF）
  - ローミングなし

### ローミング QBC プロファイルの使用

SMF は、ローカルインターフェイスに基づいて QBC プロファイルを決定します。QBC URR は、プロファイルに存在する制限に基づいて作成されます。

ホームからローミングへのシナリオ（5G ホームから 5G ローミングへ、または 4G ホームから 5G ローミングへなど）：

- hCHF から更新されたローミング QBC がある場合、SMF は QBC URR を UPF に対して更新します。
- ただし、hSMF は更新されたローミング QBC を vSMF に転送できないため、hSMF と vSMF 間の QBC データに不一致が発生します。

この問題を解決するには、3GPP 変更要求（CR）S5-234612 が必要です。

新しいルールのインストールに、ボリューム制限と時間制限の値が異なる CHF 更新応答が含まれている場合、既存の QBC URR は更新されません。新しいルールに対して新しい QBC URR が作成されます。更新されたボリュームと時間の制限が、新しい QBC URR に適用されます。

### トリガーとレポート

HR 課金には、次のトリガーが適用されます。

- セッション レベルで待機するトリガー
  - セッション レベル URR の QBC を報告します。
  - CC イベントの QBC を報告します。
- QBC プロファイルでトリガーが装備されます。

- 制限は QBC URR で使用されます。
- QBC プロファイルで装備されたイベントのすべての QBC URR を報告します。

次のサンプル コードは、さまざまなトリガーと対応する値を示しています。

```
Sess trigger []
Vol  100
time  100
RAT

Rg X trigger[]
Vol  10
time  10
PLMN

RoamignQbcprofile trigger[]
Vol    20
time  20
ULI


Sess URR
Vol 100
tim 100

RGX_URR
vol  10
tim 10

QBCURR1
Vol 20
tim 20

QBCURR2
Vol 20
tim 20



When RTA happens
Query all RG and all QBC urr

when PLMN change
Query RG X URR


when ULI changes
Query all QBC
```

### セッション レベル URR へのスタティック URR または定義済み URR の使用のアカウンティング

以前のリリースでは、CHF 主導のセッション制限は PCF によって制御され、その性質は動的で、オンラインおよびオフラインの課金サービスに適用されます。そのため、セッション レベルの URR が報告されたときに、すべてのダイナミック URR が報告されていました。また、別の URR が満たされたときに、静的または事前定義されたルールに関連付けられているオフライン URR が報告されました。

現在のリリースでは、次の URR を報告するセッション制限について、N4 インターフェイスでの報告メカニズムが合理化されています。

- ダイナミック ルールに関連付けられているオンライン URR とオフライン URR。
- 静的ルールまたは事前定義済みルールに関連付けられたオフライン URR。
- すべての QBC URR。

注：

- このリリースでは、セッション制限に達した場合、SMF はオンラインの静的 URR または事前定義済み URR を報告しません。
- このリリースでは、オフラインサービスの静的または事前定義された累積レポートを取得するためにルール ベースの ECGDR 構成は必要ありません。

  QBC が有効になっている場合、SMF はルール ベース名を伝送するデフォルトの UL または DL PDR に SessLevelUrr を関連付けます。UPF は、この URR をすべての静的事前定義ルールのすべての SDF PDR または URR に関連付けます。
- 設定中に、Sess Urr はデフォルトの PDR に関連付けられます。セッション レベル URR およびその後のポスト セットアップを作成するためのセットアップ時間中に SMF が入力を行わない場合、CHF は制限を設定します。これらの URR は適用されません。

### MaxChangeinCC、MaxDeferredUrr、OOO 構成

#### MaxChangeinCC

HR ローミング機能では、最大 CC に達した場合の QBC 使用状況データのレポートがサポートされます。

MaxCC 値は、CHF からの設定レベルとは別に設定レベルで制御できます。MaxCC 値を選択する優先順位は次のとおりです。

- CHF アームの MaxCC。
- セッションに関連付けられている場合の ChargingProfile。
- セッションで QBC 課金に対して有効になっている場合は、QbcProfile を使用します。

#### MaxDeferredUrr

ローカル設定は、Charging プロファイルに存在する MaxDefered 値を設定するために使用されます。これは、ChargingQbcProfile に拡張されます。選択の優先順位は次のとおりです：

- セッションに関連付けられている場合の ChargingProfile。
- セッションで QBC 課金に対して有効になっている場合は、QbcProfile を使用します。

UUC と QFICOntainer の合計値が設定されたしきい値を超えたときに、MaxDeferred 数が満たされます。

#### OOO Config

OOO 設定は、セッションに関連付けられた Charg-Profile から参照されます。.

セッションに関連付けられていない場合は、セッションで QBC 課金が有効になっていれば、QBC プロファイルから参照されます。

# HR ローミングの課金の構成

ここでは、HR ローミング機能の課金構成方法について説明します。

### QBC 課金プロファイルの構成

次のコード例を使用して、QBC 課金プロファイルを構成します。

```
[unknown] smf(config)# profile charging-qbc test
[unknown] smf(charging-qbc-test)# ?
Possible completions:
  limits       List of threshold
  triggers       List of Triggers to be configured

[unknown] smf(charging-qbc-test)# limits ?
Possible completions:
  duration       Duration threshold for Charging, range [60..40000000]
  volume         Volume threshold for Charging, range [10000..4000000000]

[unknown] smf(charging-qbc-test)#  limit duration ?
Description: Duration threshold for Charging, range [60..40000000]
Possible completions:
  <unsignedInt, 60 .. 40000000>

[unknown] smf(charging-qbc-test)#  limit volume ?
Possible completions:
  downlink    in bytes, range [10000..4000000000]
  total       in bytes, range [10000..4000000000]
  uplink      in bytes, range [10000..4000000000]

[unknown] smf(charging-qbc-test)#  triggers ?
Description: List of Triggers
Possible completions:
  3gpp-ps-change
  ambr-change
  max-number-of-changes-in-charging-conditions
  plmn-change
  qos-change
  rat-change
  serv-node-change
  ue-pra-change
  ue-time-change
user-loc-change
```

### 課金プロファイルへの QBC 課金プロファイルの関連付け

次のコード例を使用して、QBC 課金プロファイルを構成し、課金特性プロファイルに関連付けます。

```
[unknown] smf(config)# profile charging-characteristics 16
[unknown] smf(config-charging-characteristics-16)# ?
Possible completions:
  charging-profile                 Charging Profile configuration
  network-element-profile-list     Network element profile list
  charging-qbc-profile    Associate said QBC ChargignProfile

[unknown] smf(config-charging-characteristics-16)#associate-qbc-charg-profile test
```

### QBC 課金プロファイルを DNN プロファイルに関連付ける

次のコード例を使用して、QBC 課金プロファイルを構成し、DNN プロファイルに関連付けます。

```
unknown] smf(config)# profile dnn test
[unknown] smf(config-dnn-test)# ?
Possible completions:
  ---
  ---
  charging-profile                                              Charging Profile
configuration
  charging-qbc-profile                                       QBC ChargignProfile
```

### QoS プロファイルの構成

QoS プロファイルは、フロー パラメータ（MFBR および GFBR）の qi5 arp ごとの組み合わせを構成するように拡張されています。

QoS プロファイルを構成するには、次のコード例を使用します。

```
[smf] smf(config-qos-abc)# qosflow?
Possible completions:
  qosflow   Configure Qosflow params for 5QI/Arp values
[smf] smf(config-qos-abc)# qosflow ?
Possible completions:
  qi5   Standard 5QI value (range 1 to 255)
[smf] smf(config-qos-abc)# qosflow qi5 ?
Possible completions:
  <qci-value:unsignedInt, 1 .. 255>  range
[smf] smf(config-qos-abc)# qosflow qi5 1 ?
Possible completions:
  arp-priority-level   Configures the ARP Priority Level [1-255]
  flow-parameter
  <cr>
[smf] smf(config-qos-abc)# qosflow qi5 1 flow-parameter ?
Possible completions:
  gfbr   Guaranted Bit Rate (GFBR)
  mfbr   Maximum Bit Rate (MFBR)
[smf] smf(config-qos-abc)# qosflow qi5 1 flow-parameter gfbr ?
Possible completions:
  dl   GFBR Downlink threshold
  ul   GFBR Uplink threshold
[smf] smf(config-qos-abc)# qosflow qi5 1 flow-parameter gfbr dl ?
Description: GFBR Downlink threshold
Possible completions:
  <string>
[smf] smf(config-qos-abc)# qosflow qi5 1 flow-parameter mfbr ?
Possible completions:
  dl   MFBR Downlink threshold
  ul   MFBR Uplink threshold
[smf] smf(config-qos-abc)# qosflow qi5 1 flow-parameter mfbr

[smf] smf(config-qos-abc)# qosflow qi5 1 arp-priority-level 1 flow-parameter ?
Possible completions:
  gfbr   Guaranted Bit Rate (GFBR)
  mfbr   Maximum Bit Rate (MFBR)
[smf] smf(config-qos-abc)# qosflow qi5 1 arp-priority-level 1 flow-parameter
```

# 人事ローミングでのデフォルトの DNN サポート

HR ローミング シナリオでは、vSMF はデフォルトの DNN の使用をサポートしています。これにより、ローミング パートナーが使用するすべての DNN のリストまたは設定を回避できます。

vSMF が受信した visitor-hr コールの DNN 検証は無効になっています。デフォルトの DNN プロファイルから、仮想 DNN 構成は vCHF、vUPF、および vUPF 選択のための RMGR に対して使用されます。

デフォルトの DNN プロファイルを構成するには、次の CLI 構成を使用します：

```
config
  policy dnn policy_name
    profile profile_name
  exit
exit
```

仮想 DNN 名を構成するには、次の構成 CLI を使用します：

```
config
  profile dnn profile_name
    dnn virtual_dnn_name network-function-list [ chf | rmgr | upf ]
  exit
exit
```

# HR ローミングでの IPv6 RS/RA サポート

このリリースでは、ホーム ルーテッド ローミング機能は、*3GPP TS 29.502*、リリース *16*、*CR 202206*に従って、N16 インターフェイスを使用して vSMF が hSMF から IPv6 インターフェイス ID を受信するためのメカニズムをサポートしています。

HR ローミング シナリオでは、ルータ要請（RA）およびルータアドバタイズメント（RA）が hUPF または hSMF によって処理され、RA が適切に機能するよう両方向に vUPF がリレーします。CR 202206 では、hSMF が IPv6 インターフェイス ID を vSMF に送信し、vSMF がそれを N1 ペイロードで UE にリレーします。

相互運用性を確保するため、vSMF は N16 インターフェイスの hSMF から IPv6 インターフェイス ID を受信しない場合でも、DNN プロファイルの仮想 Mac 構成に基づいて UE にリレーします。

# SEPP サポート

## 機能説明

セキュリティ エッジ保護プロキシ(SEPP)は、異なる5G PLMN (パブリック ランド モバイル ネットワーク)間で交換されるコントロール プレーン トラフィックを保護するために使用されます。SEPP は、PLMN 境界ですべての API メッセージに対してメッセージ フィルタリング、ポリシング、およびトポロジ隠蔽を実行します。

SMF は、SEPP またはピアを介して障害の原因を特定するため、SEPP の障害処理テンプレートをサポートします。

## 機能の仕組み

SEPP は、通信パスを保護し、PLMN 間シグナリングですべてのコントロール プレーン メッセージに対してトポロジ隠蔽を実行し、実際のサービス プロデューサとサービス コンシューマ間のサービス リレーとして機能します。サービスプロデューサとコンシューマの両方にとって、サービス リレーの結果は直接的なサービスの相互作用と同等です。

HR ローミングの場合、各 SEPP は N16 インターフェイスを使用して VPLMN と HPLMN のそれぞれの SMF と通信します。

**Note** SEPP は PLMN 間境界でのみ使用され、ホーム ドメイン内のノード間（hSMF と hUDM 間など）では使用されません。

### SEPP の選択

SEPP はローカルの構成で選択されます。NF ノードの現在のセットが拡張され、SEPP を選択できるようになります。vSMF と hSMF は、同じ構成を使用して SEPP を選択します。

### SEPP および hSMF/vSMF の障害処理

SMF は、hSMF または vSMF および SEPP の障害処理（FH）をサポートしています。クライアント SMF は、HTTP 応答で受信した 3GPP ヘッダー メッセージに基づいて、失敗応答の発信元を検出します。発信元は、ピア SMF または SEPP のいずれかです。

ヘッダー メッセージ内の NF インスタンス値に応じて、SEPP FH プロファイルまたは N16 FH プロファイルのいずれかを選択します。

N16 FH プロファイルは、既存の N32 SEPP FH プロファイルと同様に機能します。ただし、N16 FH プロファイルは、他の NF で使用可能なエンドポイント（EP）構成の代わりに、AdditionalHsmfUri 属性を使用します。

**重要** AdditionalHsmfUri 属性は、セッションの作成手順でのみ使用されます。

SMF からのエラー応答がある場合、次の形式でサーバー ヘッダーが含まれます：

**SMF-nf-instance-id**

```
Example:
SMF-54804518-4191-46b3-955c-ac631f953ed8
 SEPP-35644518-9291-46b3-934c-ac5678f953ed
```

ヘッダーに SEPP NF インスタンス値が含まれている場合、エラーを受信したクライアント SMF は SEPP 障害処理構成を適用します。

（注） ヘッダーに 2 つの SEPP サーバ名がある場合、そのヘッダーは障害応答をピア SMF から発信されたものと見なします。

次に、PDU セッションの作成手順中に実行される一連の失敗処理手順を示します。

1. vSMF は、ローカルに構成された SEPP EP に基づいて最初の SEPP を選択し、「3gg-target-api-root」ヘッダーに hSMF URI を追加します。
2. 最初の SEPP EP が失敗した場合、vSMF は SEPP FHT を選択し、別の EP で手順を再試行する。
3. SEPP FHT がない場合、または再試行回数が枯渇した場合、SMF はセッションを終了します。
4. ピア SMF が失敗すると、vSMF は N16 FHT を使用して、AdditionalHsmfUri EP から次の EP を選択します。
5. AdditionalHsmfUri IE で定義されたすべての URI が失敗するか、再試行回数を超えた場合、vSMF は手順を終了します。

### SEPP および SMF 障害処理

PDU セッションのライフサイクル中に、SMF は NF インスタンス値を使用して hSMF と SEPP をチェックします。FH プロファイルに構成された HTTP ステータス コードに応じて、SMF は次のいずれかのアクションを実行します。

**表 *466 : SEPP* および *SMF FHT* でサポートされるアクション**

| N16 の手順 | SEPP FHT アクション（SEPP FHT Actions） | SMF FHT アクション（SMF FHT Actions） |
|---|---|---|
| 作成（Create） | terminate<br>retry-and-terminate | terminate<br>retry-and-terminate |
| リリース | terminate<br>retry-and-terminate | terminate |
| HsmfPduSessionNotify | terminate<br>retry-and-terminate | terminate |

（注） SMF は、他の構成された FH アクションをデフォルトの終了アクションで上書きします。

## コール フロー

ここでは、SEPP を選択して使用するためのコール フローについて説明します。

次のタイプの要求がクライアントからサーバに送信されます。

- **API ルートへの要求**：これらのリクエストは、YAML で定義されているように API ルートに送信されます。以下のヘッダーが要求に追加されます。
  - **3gpp-Sbi-Target-apiRoot**：このヘッダーの値は、要求を処理する NF の FQDN です。要求が hSMF に送信される場合、これは hSMF の FQDN です。
  - **Authority** ：このヘッダーの値は、クライアントによって要求が送信されるサーバ SEPP です。要求が vSMF によって送信される場合、値は vSEPP で、要求が hSMF によって送信される場合は hSEPP です。
- **コールバック リクエスト** ：これらのリクエストは、PLMN の境界を越えて呼び出されるコールバックです。このような要求のヘッダー フィールドの値は、*3GPP TS 29.500*、*Annex B*で定義されています。

***Figure 271: SEPP*** **を使用したコール フロー**

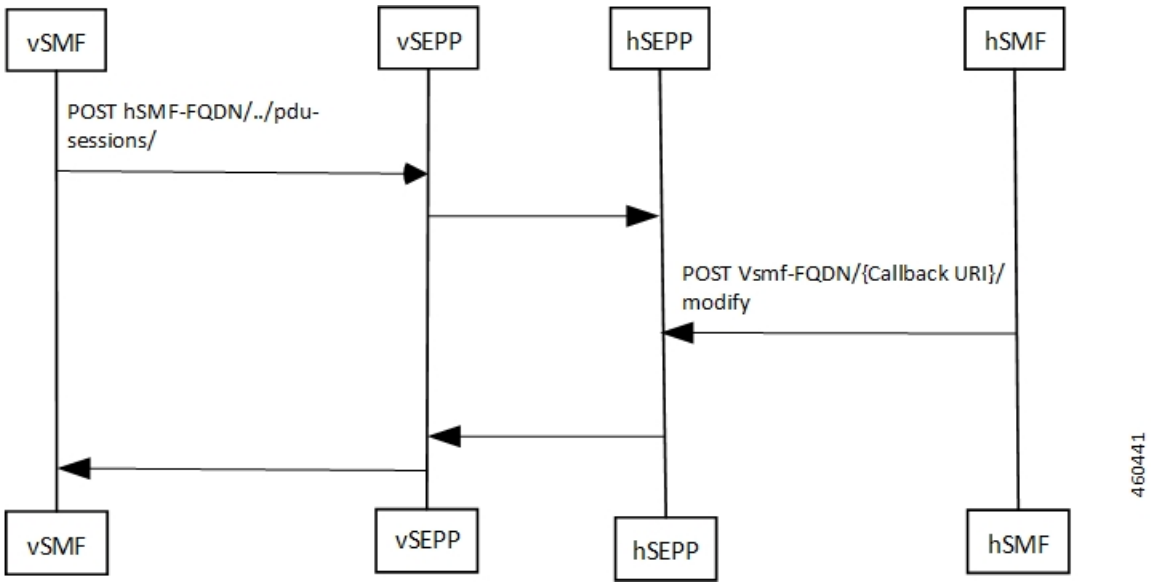


*Table 467: SEPP* を選択するためのコール フローの説明

| ステップ | 説明 |
|---|---|
| 1 - 2 | vSMF は、SEPP と SEPP のアドレスの使用に関する通知を hSMF に送信することにより、手順を開始します。この転送メッセージのコール フロー シーケンスは次のとおりです：<br>• vSEPP と hSEPP は、vSMF から hSMF に送信されるメッセージをそれぞれ暗号化と復号化を行います。<br>• AMF は hSMF FQDN を smf-service に送信し、次にすべてのメッセージで rest-ep に送信します。<br>• vSMF は、vSEPP にローカルに構成された IP アドレスとポート番号を読んで vSEPP を選択し、それを使用して hSMF にメッセージを送信します。<br>• rest-ep は、vSEPP の IP アドレスとポート番号を使用して hSMF URI と Authority ヘッダーを使用して 3gpp-Sbi-Target-apiRoot ヘッダーを更新し、その後、メッセージを vSEPP に送信します。vSEPP はさらに hSEPP と通信されます。<br>• hSEPP は、DNS を解決し（必要な場合）、メッセージを復号してから hSMF に送信します。 |
| 3 - 4 | hSMF は callback ヘッダー値で応答します。この返信メッセージのコール フロー シーケンスは次のとおりです。<br>• hSEPP と vSEPP は、hSMF から vSMF に送信されるメッセージをそれぞれ暗号化および復号化します。<br>• smf-service は、vSMF からメッセージの一部として受信した通知 URI から vSMF の FQDN を取得し、3gpp-Sbi-Target-apiRoot ヘッダーを更新します。smf-service は、すべてのメッセージ内の 3gpp-sbi-callback 列挙値を更新します。<br>• smf-service は、メッセージを rest-ep に転送します。rest-ep は、3gpp-sbi-callback ヘッダーと 3gpp-Sbi-Target-apiRoot ヘッダーの値を更新します。<br>• rest-ep は、hSEPP のローカルに構成された IP アドレスとポート番号で Authority（疑似ヘッダー）を更新し、hSEPP にメッセージを転送します。hSEPP はさらに vSEPP と通信します。<br>• vSEPP は DNS を解決し（必要な場合）、メッセージを復号してから vSMF に送信します。 |

## SEPP の構成

ここでは、SEPP の構成方法について説明します。

SEPP を構成する場合、次の条件が適用されます：

- これは、UDM、CHF、PCF などの他の NF と同じ方法で構成されます。
- エッジ プロキシであり、適切な NF ではないため、ピア SMF でサポートされているサービス リストが必要です。
- これは、他の NF と同様に、既存の nf クライアント障害テンプレートを使用した障害処理機能をサポートしています。

### SEPP nf-client の構成

SEPP nf-client を構成する場合、CLI 構成例は参考としてのみ使用してください。

```
profile nf-client nf-type sepp
 sepp-profile SEPP1
  locality LOC1
   service name type nsmf-pdusession
    endpoint-profile EP1
     capacity   50
     priority   50
     uri-scheme http
     endpoint-name sepp-ep-1
      priority 50
      capacity 50
      primary ip-address ipv4 xx.xx.xx.xx
      primary ip-address port xxxx
     exit
    exit
   exit
  exit
 exit
exit
```

### SEPP のネットワーク要素プロファイル パラメータの構成

SEPP nf-client にリンクされているネットワーク要素プロファイルを構成するには、CLI 構成例を使用します。

```
profile network-element sepp nrf-nf-sepp-1
 nf-client-profile SEPP1
exit
```

### SEPP の DNN プロファイルの構成

SEPP の DNN プロファイルを構成するには、CLI 構成例を参考としてのみ使用してください。

```
network-element-profile sepp nrf-nf-sepp-1 is linked to dnn

profile dnn intershatRoamer
 network-element-profiles sepp nrf-nf-sepp-1
exit
```

### SEPP の障害処理の構成

SEPP は、すべての HTTP エラー応答コードについて、既存の失敗処理テンプレートをサポートしています。SEPP の障害処理を構成するには、参照としてのみ構成例を使用してください。

```
profile nf-client-failure nf-type sepp
 profile failure-handling FH-SEPP
  service name type nsmf-pdusession
   message type VsmfPduSessionCreate
    status-code httpv2 504
     retry  2
     action retry-and-terminate
    exit
   exit
  exit
 exit
exit
```

**Note** 現在のリリースでは、すべてのメッセージで retry-terminate オプションのみがサポートされています。

### hSMF/vSMF および SEPP の障害処理テンプレートの構成

ピア SMF および SEPP は、すべての HTTP エラー応答コードの失敗処理テンプレートをサポートしています。ピア SMF メッセージの障害処理を構成するには、構成例を参照としてのみ使用してください。

以下に hSMF の構成例を示します：

```
profile nf-client-failure nf-type sepp
 profile failure-handling FHSEPP
  service name type nsmf-pdusession
   responsetimeout 4000
   message type VsmfPduSessionUpdate
    status-code httpv2 500-599
     retry  3
     action retry-and-terminate
    exit
   exit
   message type VsmfPduSessionNotify
    status-code httpv2 400-599
     retry  3
     action retry-and-terminate
    exit
   exit
  exit
 exit
exit
```

以下に vSMF の構成例を示します：

```
profile nf-client-failure nf-type sepp
 profile failure-handling sepp
  service name type nsmf-pdusession
   responsetimeout 4000
   message type HsmfPduSessionCreate
    status-code httpv2 400-599
     retry  3
     action retry-and-terminate
    exit
   exit
   message type HsmfPduSessionUpdate
    status-code httpv2 500-599
```

```
     retry  3
     action retry-and-terminate
    exit
   exit
   message type HsmfPduSessionRelease
    status-code httpv2 504
     retry  3
     action retry-and-terminate
    exit
   exit
  exit
 exit
exit
```

**Note** 構成例では、nf-type の SEPP を使用しています。Nf タイプの SMF にも同じものを使用できます。

### 代替 hSMF を使用した障害処理テンプレートの構成

プライマリ hSMF から障害が発生した場合、vSMF は代替 hSMF を試行します。SMF サービスは代替 hSMF の詳細を REST エンドポイント（rest-ep）に送信し、SMF は AMF から代替 HSM の詳細を取得します。N26 障害処理の構成に基づいて、代替 hSMF が選択されます。

代替 hSMF は、再試行が構成されている場合にのみ選択されます。**pduSessionCreate**

**Note** smf-service には、Rest エンドポイントへの **discoveryParams** にリスト**alternate-hsmf** が含まれています。

N26 障害処理の構成に基づいて、代替 hSMF が選択されます。

Rest-ep または NfLib は選択された代替 hSMF をサービスに送り返し、vSMF はこれを AMF に送り返します。 vSMF は、smContextCreatedData に **SelectedSmfId** を表示します。

**設定例**:

次に設定例を示します。

```
[smf] smf(config)# profile nf-client-failure nf-type n16smf
smf] smf(config-n16smf)# profile failure-handling fh
[smf] smf(config-failure-handling-fh)# service name type nsmf-pdusession
[smf] smf(config-type-nsmf-pdusession)# message type [ PduSessionCreate  ] status-code
httpv2 <0-599>
[smf] smf(config-httpv2-400)# action [continue  retry-and-continue  retry-and-ignore
retry-and-terminate  terminate]
[smf] smf(config-httpv2-400)# retry <1-10>
```

### SMF NRF 登録の構成

SMF NRF 登録を構成するには、構成例の参照としてのみ使用してください。

```
profile smf smf1 instances
            instances 1 fqdn 5gc.mnc456.mnc123.3gppnetwork.org
```

```
instances 1 inter-plmn-fqdn 5gc.mnc456.mnc123.3gppnetwork.org
instances 1 supported-features [ vsmf ]
```

**Note** 現在のリリースでは、SMF を NRF に登録するために、 **inter-plmn-fqdn** および vsmf でサポートされる IE が SMF ディスカバリに含まれています。 **vsmfSupportIndicator** の構成は 、**inter-plmn-fqdn**とともに vSMF に追加する必要があります。この構成は、vAMF がローミングをサポートする vSMF を検索するために必要です。

**vsmfSupportIndicator** の構成を元に戻すには、次の構成例を使用します：

```
smf] smf(config-smf-smf1)# no instances 1 supported-features
[smf] smf(config-smf-smf1)# commit
```

# OAM サポート

## バルク統計サポート

この機能により、「smf_restep_http_msg_total」統計に「failed_nf_type」ラベルが導入され、障害応答コードの送信元であるターゲット NF が示されます。

ピア SMF および SEPP 作成セッション失敗応答のクエリの例を次に示します。

- セッション手順の作成成功：

```
smf_restep_http_msg_total{api_name="smf_pdu_session_create",app_name="SMF",
cluster="SMF",data_center="DC",dnn="",gr_instance_id="1",
instance_id="0",message_direction="outbound",message_type="",
nf_type="smf",nf_uri="",proc_name="",rat_type="",req_cause="",response_cause="",
response_status="201",service_name="rest-ep",sess_type="", failed_nf_type=""} 1
```

- SMF からのセッション手順失敗応答を作成します：

```
smf_restep_http_msg_total{api_name="smf_pdu_session_create",app_name="SMF",
cluster="SMF",data_center="DC",dnn="",gr_instance_id="1",
instance_id="0",message_direction="outbound",message_type="",
nf_type="smf",nf_uri="",proc_name="",rat_type="",req_cause="",response_cause="",
response_status="400",service_name="rest-ep",sess_type="", failed_nf_type="smf"} 1
```

- SEPP からのセッション手順失敗応答を作成します：

```
smf_restep_http_msg_total{api_name="smf_pdu_session_create",app_name="SMF",
cluster="SMF",data_center="DC",dnn="",gr_instance_id="1",
instance_id="0",message_direction="outbound",message_type="",
nf_type="smf",nf_uri="",proc_name="",rat_type="",req_cause="",response_cause="",
response_status="400",service_name="rest-ep",sess_type="", failed_nf_type="sepp"} 1
```

バルク統計情報の詳細については、「*UCC 5G SMF* メトリック リファレンス」を参照してください。

# N3 および N9 ユーザー プレーンの分離

ユーザーは、非ローミング加入者とホーム ルーティング加入者の両方を処理する SMF または UPF 上の 5G ネットワークで N3 および N9 ネットワークを個別に保持することを希望します。

UPF が UE がアウトバウンド ローミングまたはホームのうちのいずれであるかを検出できない場合、SMF はサブスクライバに使用するインターフェイスに関する情報を UPF に渡します。このシナリオを克服するために、SMF は、あるネットワーク上で N3 インターフェイスを、別のネットワーク上で S5-U/S8-U と N9 インターフェイスを許可することにより、ユーザーが特にデータ パス上でコア ネットワークとは別の RAN ネットワークを維持できるようにします。

SMF は、適切なインターフェイス タイプを使用して PDR を作成しながら、N4 メッセージの PDI IE に送信元インターフェイス タイプ IE（3GPP インターフェイス タイプ）を入力します。IE の形式は次のとおりです：

| | ビット | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Octets** | **8** | **7** | **6** | **5** | **4** | **3** | **2** | **1** |
| 1 ～ 2 | タイプ = 160（10 進数） | | | | | | | |
| 3 ～ 4 | 長さ = n | | | | | | | |
| 5 | スペア | | | | インターフェイス タイプ値 | | | |
| 6 ～ n+4 | これらのオクテットは、明示的に指定されている場合にのみ存在します。 | | | | | | | |

次の表に、3GPP インターフェイスの種類とその値を示します。

| インターフェイス値 | 値（10進数） |
|---|---|
| S1-U | 0 |
| S5/S8U<br>（注）<br>ローミング トラフィックと非ローミング トラフィックが分離されている場合、この値は S5-U インターフェイスにのみ使用し、S8-U インターフェイスには「S8-U」（10 進数の 19）を使用する必要があります。 | 1 |
| S4-U | 2 |
| S11-U | 3 |
| S12 | 4 |

| | |
|---|---|
| Gn/Gp-U<br>（注）<br>ローミング トラフィックと非ローミング トラフィックが分離されている場合は、この値を Gn-U インターフェイスにのみ使用し、「Gp-U」（10 進数の 20）を Gp-U インターフェイスに使用する必要があります。 | 5 |
| S2a-U | 6 |
| S2b-U | 7 |
| DL データ転送用の eNodeB GTP-U インターフェイス | 8 |
| UL データ転送用の eNodeB GTP-U インターフェイス | 9 |
| DL データ転送用の SGW/UPF GTP-U インターフェイス | 10 |
| N3 3GPP アクセス | 11 |
| 3GPP 以外の信頼済みのアクセス | 12 |
| 3GPP 以外の信頼できないアクセス | 13 |
| データ転送用 N3 | 14 |
| N9（または非ローミングの場合はN9）<br>（注）<br>ローミング トラフィックと非ローミング トラフィックが分離されている場合、この値はN9非ローミングインターフェイスにのみ使用し、（10進数値「21」）はN9ローミングインターフェイスに使用する必要があります。 | 15 |
| SGi | 16 |
| N6 | 17 |
| N19 | 18 |
| S8-U | 19 |
| GPU | 20 |
| ローミング用 N9 | 21 |

| | |
|---|---|
| Iu-U | 22 |
| データ転送用の N9 | 23 |
| Sxa-U | 24 |
| Sxb-U | 25 |
| SXC-U | 26 |
| N4-U | 27 |
| UL データ転送用の SGW/UPF GTP-U インターフェイス | 28 |
| N6mb/Nmb9 | 29 |
| N3mb | 30 |
| N19mb | 31 |
| スペア | 32–63 |

### 提供内容の概要

N3 および N9 ユーザー プレーンの分離中に、次の機能が発生する可能性があります。

- SMF は以下を提供します。
  - 4G RAT を介して接続するホーマーのアップリンク PDR のパケット検出情報（PDI）で、送信元インターフェイス タイプとして S5-U を選択します。
  - 5G RAT を介して接続するホーマーのアップリンク PDR の PDI の送信元インターフェイス タイプとしての N3 3GPP アクセス。
  - Wi-Fi RAT を介して接続するホーマー ユーザーのアップリンク PDR の PDI のソースインターフェイス タイプとして S5-U。これは、4G < - > Wi-Fi ハンドオーバー中のトンネルの再作成を回避するための最適化として行われます。
- ハンドオーバー（HO）シナリオでは、次の手順を実行します。
  - **5G から 4G/Wi-Fi へ**：トンネルが再作成され、N4 変更は、S5-U に設定された送信元インターフェイス タイプを持つアップリンク PDR PDI を使用します。
  - **4G/Wi-Fi から 5G へ**：トンネルが再作成され、N4 の変更は、送信元のインターフェイスタイプが N3 に設定されたアップリンク PDR の PDI を使用します。
  - 同様に、専用フロー/ベアラーのアップリンク PDR は、RAT に応じて N3 または S5-U 送信元インターフェイス タイプで作成されます。

- UPF は送信元インターフェイス タイプのない N4 メッセージを処理し、インターフェイスからトンネルを割り当てます。インターフェイスには、下位互換性があるためどのインターフェイスにも関連付けられていません。

### インターフェイス タイプの構成

UPF 入力インターフェイス タイプを構成するには、次の構成を使用します。

```
configure
   context context_name
      user-plane-service service_name
         [ no ] associate gtpu-service gtpu_service_name upf-ingress
         end
```

注：

- **associate gtpu-service** *gtpu_service_name*：ユーザー プレーン サービスの GTP-U サービスを関連付けます。
- **upf-ingress**：インターフェイス タイプを S-GW 入力として構成します。

次に、例を示します。

```
associate gtpu-service n3-upf-in upf-ingress
associate gtpu-service n3-upf-in upf-ingress interface-type S5-U | S8-U | 3 3Gpp Access
 | n9-s5-s8
| N3 for data Forwarding | N9 | N6 | SGi
```

# N3 と N9 の分離での ホーマー コール

ホーム ルーティングされたコール中に次のコール フロー プロセスの変更が発生します。

- **vSMF セッション作成手順**：5G セッション作成手順中に、SMF は適切なインターフェイス タイプを使用して PDR を作成する際、N4 メッセージの PDI IE に送信元インターフェイス タイプ IE（3GPP インターフェイス タイプ）を含めます。たとえば、SMF は N4 メッセージの Create uplink PDR に source interface type= N3 3GPP Access を含め、UPF は構成に基づいてそのインターフェイスから TEID を割り当てます。GTPU サービスが N3 3GPP アクセスに関連付けられていない場合、TEID はデフォルト（インターフェイス構成のないもの）から割り当てられます。
- **4G アクセス登録**：4G アクセス登録時に、SMF は N4 メッセージのアップリンク PDR 作成に送信元インターフェイス タイプ = S5-U を含め、UPF は構成に基づいてそのインターフェイスから TEID を割り当てます。S5-U に GTPU サービスが関連付けられていない場合、TEID はデフォルト（インターフェイス構成なしで 1 つ）から割り当てられます。

## 専用ベアラー コール フロー

次の場合にコールフローの変更が発生します：

- **専用ベアラー フローの作成**：4G で専用ベアラーを作成しているときに、SMF は、アップリンク PDR 作成で S5-U として送信元インターフェイス タイプを持つ N4 変更を送信します。
- **追加の 5G コール フローの作成**：5G で追加のフローを作成している間、SMF は、アップリンク PDR 作成で、送信者インターフェイス タイプが「N3 3GPP Access」として N4 変更を送信します。

## N3 と N9 の分離でのローマ コール

ローマ コール中に次のコール フロー プロセスの変更が発生します。

- ローミングの場合、vSMF は、N9 トラフィックのダウンリンク（DL）PDR を作成するときに送信元インターフェイス タイプを N9 として送信し、N4 メッセージで N3 トラフィックのアップリンク（UL）PDR を作成するときに「N3 3GPP Access」として送信します。
- hSMF は、N9 トラフィックの UL PDR の作成時には N9 として、4G トラフィックの UL PDR（セカンダリ PDR）の作成時には S5-U として、送信元インターフェイス タイプを送信します。
- UPF は、NR および 4G のデフォルトのベアラー/フローに 2 つの異なるトンネルを割り当てます。

（注） さらなる最適化を実現するために、SMF は、UPF を変更することなく、必要に応じて 4G と 5G の両方の UL PDR を作成しながら、送信元インターフェイスタイプとして N9 を送信できます。

# 許可された PLMN リストのサポート

非ローミング SMF と hSMF が異なるノードにあるネットワークでは、AMF は、NSSAI、SUPI の PLMN-ID、DNN などのクエリ パラメータを使用して、NRF ディスカバリに基づいて SMF を選択できます。この選択では正しい結果が得られない場合があります。

このようなシナリオでは、SMF は NRF 検出サービスを使用して、許可された PLMN リストで NRF を登録します。非ローミング SMF はホームサービス PLMN のリストに登録でき、hSMF はパートナー サービス PLMN に登録できます。

SMF は、ネットワーク機能を NRF に登録するときに、ネットワーク プロファイルの allowedPlmns に構成された allowed-plmn-list を含めます。

AMF は、既存のクエリ パラメータに加えて、requester-plmn-list を使用して SMF を検出します。

許可された plmns が構成されている場合、SMF が service-plmn を持つ SmContextCreate または SmContextUpdate を受信し、これが構成された allowed-plmn と一致しない場合、コールは拒否されます。

NF 検出の詳細については、『 *UCC 5G SMF* 構成および管理ガイド』 の 「*NF* 検出」の章を参照してください。

### 許可済み PLMN リストの構成

SMF の許可済み PLMN リストを構成するには、次の構成例を使用します。

```
config
  profile smf smf_profile_name
    allowed-plmn-list  [ mcc-mnc ]
    end
```

注：

- **allowed-plmn-list [ mcc-mnc ]**：許可された plmn リストを構成します。

# PLMN ローミング モビリティのサポート

PLMN 間ローミング モビリティは、進行中のシームレスなデータ転送を維持しながら、UE がホーム ネットワーク（H-PLMN）からパートナー ネットワーク（V-PLMN）に、またはその逆に移動できるようにする機能です。

SMF は、UE がホーム ネットワークからビジター ネットワークに、またはその逆に移動する場合のホーム ルーティング ローミングの Inter-plmn シナリオをサポートします。

SMF は次の機能をサポートしています。

- H-PLMN から V-PMLN へのハンドオーバーとその逆。
- CLI による inter-plmn ハンドオーバー機能の有効化と無効化。
- N11 および N16 インターフェイスでサポートされている機能で、特定の SMF サービス エリア（DTSSA）を使用して展開トポロジをアドバタイズします。
- 効率的な Inter-RAT ハンドオフのために、ホーム コール用のセカンダリ RAT にセカンダリ PDR を作成します。

インターフェイス間モビリティの間、vSMF は次の動作を行います。

- 構成されたサブスクライバ ポリシーに基づいてオペレータ ポリシーを選択します。
- 構成に基づいて V-UPF と V-CHF を選択します。
- Operator ポリシーで構成されているローミング ステータスを使用して、HRT ローミング要求をオーバーライドして、UE をローカル ブレークアウト（LBO）として扱います。

### N4 の変更

SMF では、関連付けの変更ではなく、PDR の再作成がサポートされます。

- **5G ローミング**：5G ローミングでは、5G UE がホームピアからローミング サーバに、またはその逆に移動すると、N3 PDR が作成および削除されます。S5 および N9 のセカンダリ PDR は、既存の FTEID で再作成されます。
- **4G ローミング**：4G ローミングでは、4G UE がホームからローミングに、またはその逆に移動すると、S5 および N9 PDR が既存の FTEID で再作成されます。N3 PDR は新たに作成されて削除されます。
- **RAT 間ローミング**：SMF は古い RAT PDR を削除し、RAT 間シナリオ用に新しい RAT PDR を作成します。SMF では、既存の FTEID を使用して S5 および N9 PDR も再作成されます。

# 制限事項と制約事項

inter-plmn モビリティ中は、H-SMF または SMF に次の制限があります。

- オペレータ ポリシーと UPF を再選択しません。
- ノースバウンド NF の選択基準は変更されません。
- ローミング ステータスをホーマー/ローマーに変更

inter-plmn モビリティ中、V-SMF には次の制限があります。

- サブスクライバ ポリシー構成に基づいてオペレータ ポリシーを選択します。
- 構成に基づいて V-UPF と V-CHF を選択します。
- オペレータ ポリシーで構成されているローミングステータスを使用して、HRT ローミング要求をオーバーライドして、UE を LBO として扱います。

### [Restrictions（機能制限）]

SMF には次の制約事項があります。

- UE が V-SMF 内で別の V-SMF に移動する PLMN 内モビリティでは、V-SMF の変更はサポートされていません。
- IDFT は Inter-plmn HO ではサポートされていません。
- inter-plmn CLI が構成されていない場合、ビジター PLMN を持つ ModifyBearerRequest は拒否されます。
- inter-plmn シナリオでは、H-SMF で構成されたローミング QOS フローベースの課金プロファイルが優先され、V-SMF から受信した課金プロファイルは無視されます。

# 標準準拠

PLMn ローミング モビリティ機能は、次の標準に準拠しています。

- *3GPP TS 23.502*、バージョン *16.6*
- *3GPP TS 29.502*、バージョン *16.6*
- *3GPP TS 29.571*、バージョン *16.6*
- *3GPP TS 29.244*、バージョン *16.6*
- *3GPP TS 32.255*、バージョン *16.6*

# 機能の仕組み

ここでは、plmn 間ハンドオーバー機能のコール フローと手順について説明します。

## コール フロー

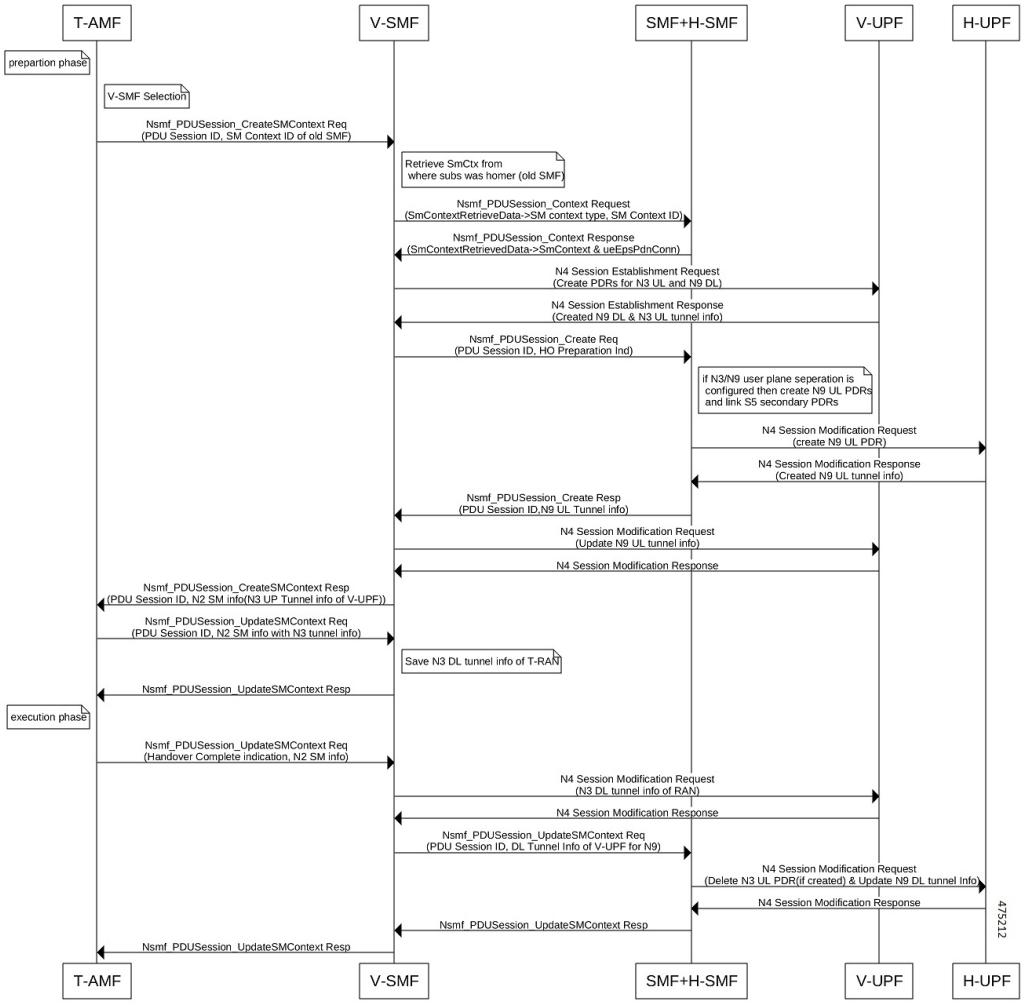
SMF では、さまざまな PLMM 間モビリティ機能の次のコール フローがサポートされます：

- 5G ホームから 5G ローマーへ
- 5g ローマーから 5g ホームへ
- 5G ローミング者から 4G ホーム/ローマーへ
- 4g ローマー/ホームから 5g ローマー
- 内部 PLMN ローミング

### Homer から Roamer への PLMN 5G ハンドオーバー

このセクションでは、v-SMF 挿入を使用した Inter-plmn N2 HO の手順に関するコール フローと詳細について説明します。

図 *272 : v-SMF* 挿入を使用した *Inter-plmn N2 HO* のコール フロー



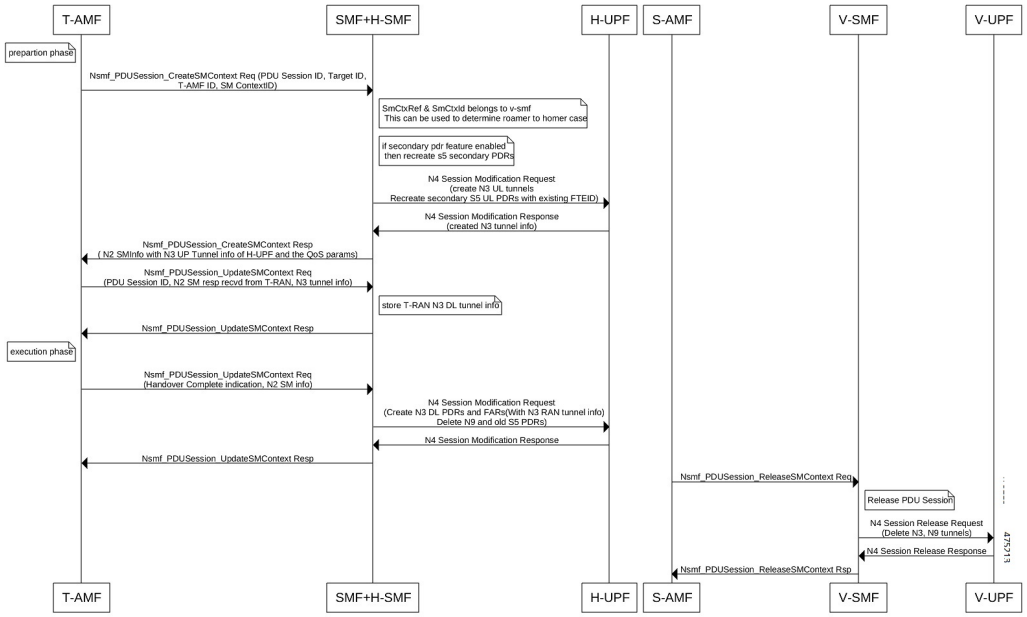

手順

- UE は H-PLMN のホームレイから V-PLMN のローマに移行します。
- V-SMF が追加されます。
- SMF は H-SMF に移行します。

## v-SMF 削除による 5G ローマーから 5G ホームマーへの PLMN 間ハンドオーバー

このセクションでは、v-SMF を削除した場合の Inter-plmn N2 HO の手順に関するコール フローと詳細について説明します。

図 *273 : v-SMF* 削除を使用した *Inter-plmn N2 HO* のコール フロー




**v-SMF 削除を使用した Inter-plmn N2 HO のコール フローの説明**：

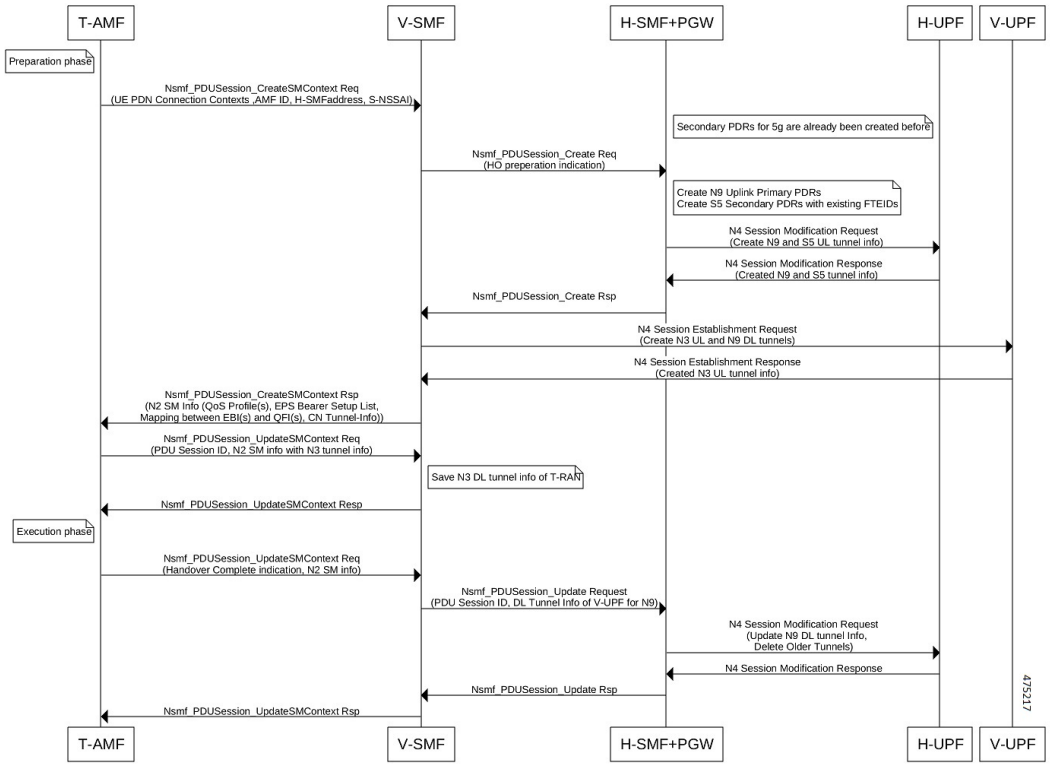
- UE は V-PLMN のローマから H-PLMN のホームレイに移行します。
- V-SMF を削除します。
- H-SMF から SMF へ移行します。

## PLMN 間および RAT 間シナリオ

### *4G* ホーマーから *5G* ローマーへの *PLMN N26* 間ハンドオーバー

このセクションでは、4G ホーマーから 5G ローマーへの Inter-plmn N2 HO に関するコール フローと詳細について説明します。

図 *274 : 4G* ホーマーから *5G* ローマーへの *Inter-plmn HO* のコール フロー

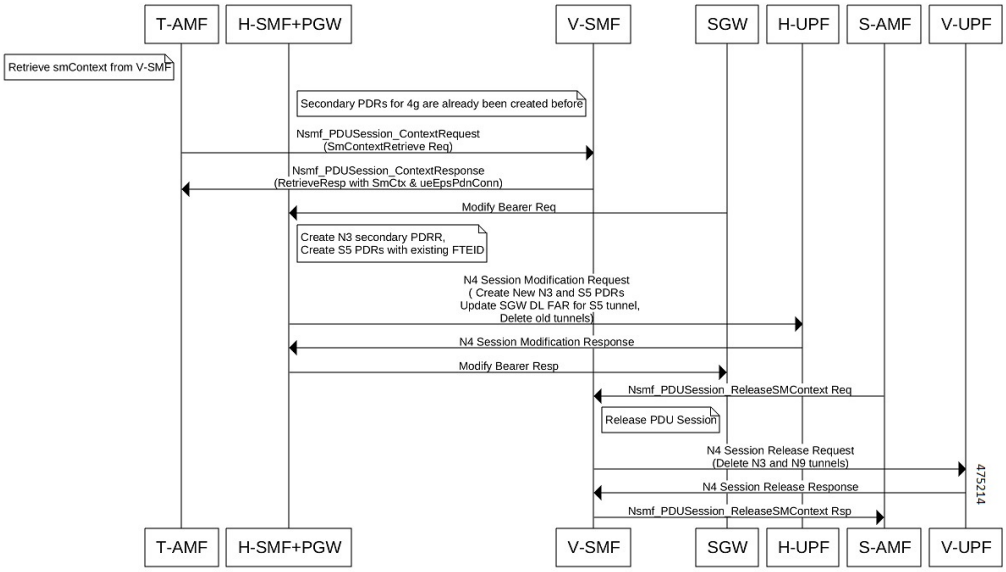



**4G ホーマーから 5G ローマーへの Inter-plmn N26 HO のコール フローの説明**：UE は、H-PLMN の 4G ホーマーまたは V-PLMN のローマーから V-PLMN の 5G ローマーグに移行します。

## *5G* ローマーから *4G* ホームまたはローミングへの *PLMN* 間ハンドオーバー

このセクションでは、5G ローマーから 4G ホームページへのインター PLMN HO に関するコールフローと詳細について説明します。

図 *275 : 5G* ローマーから *4G* ホームページでの *Inter-plmn HO* のコール フロー



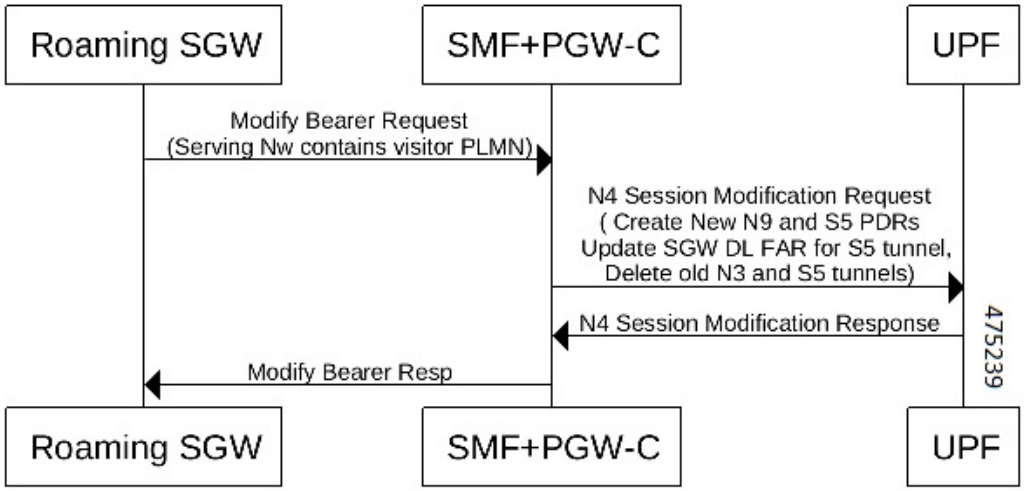

**5G ローマーから 4G ホームページへのインター PLMN HO のコール フローの説明**：

UE は、V-PLMN の 5G ローミングから H-PLMN の 4G ホームランまたは V-PLMN の 4G ローミングに移行します。

## *4G* ホーマーから *4G* ローマーへの *PLMN* 間ハンドオーバー

このセクションでは、4G ホーマーから 4G ローマーへの Inter-plmn ハンドオーバー（HO）の手順に関するコール フローと詳細について説明します。

図 *276 : 4G* ホーマーから *4G* ローマーへの *Inter-plmn HO* のコール フロー



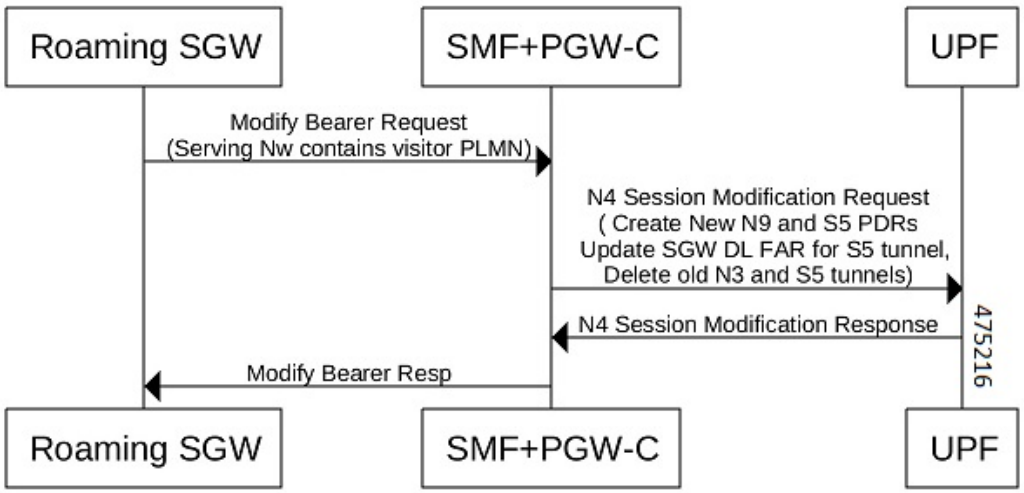

**4G ホーマーから 4G ローマーへのコール フローの説明**：

- 訪問者 S-GW から ModifyBearerRequest を受信します。
- ModifyBearerRequest 処理中のローミング ステータスを判別します。
- N3 を削除し、N9 セカンダリ PDR を作成します。
- 既存の FTEID を使用して S5 PDR を再作成します。

## *4G* ローマーから *4G Homer* への *PLMN* 間ハンドオーバー

このセクションでは、4G ローマから 4G ホームマへの Inter-plmn N2 HO の手順に関するコール フローと詳細について説明します。

図 *277 : 4G* ローマから *4G* ホームページへの *Inter-plmn N2 HO* のコール フロー



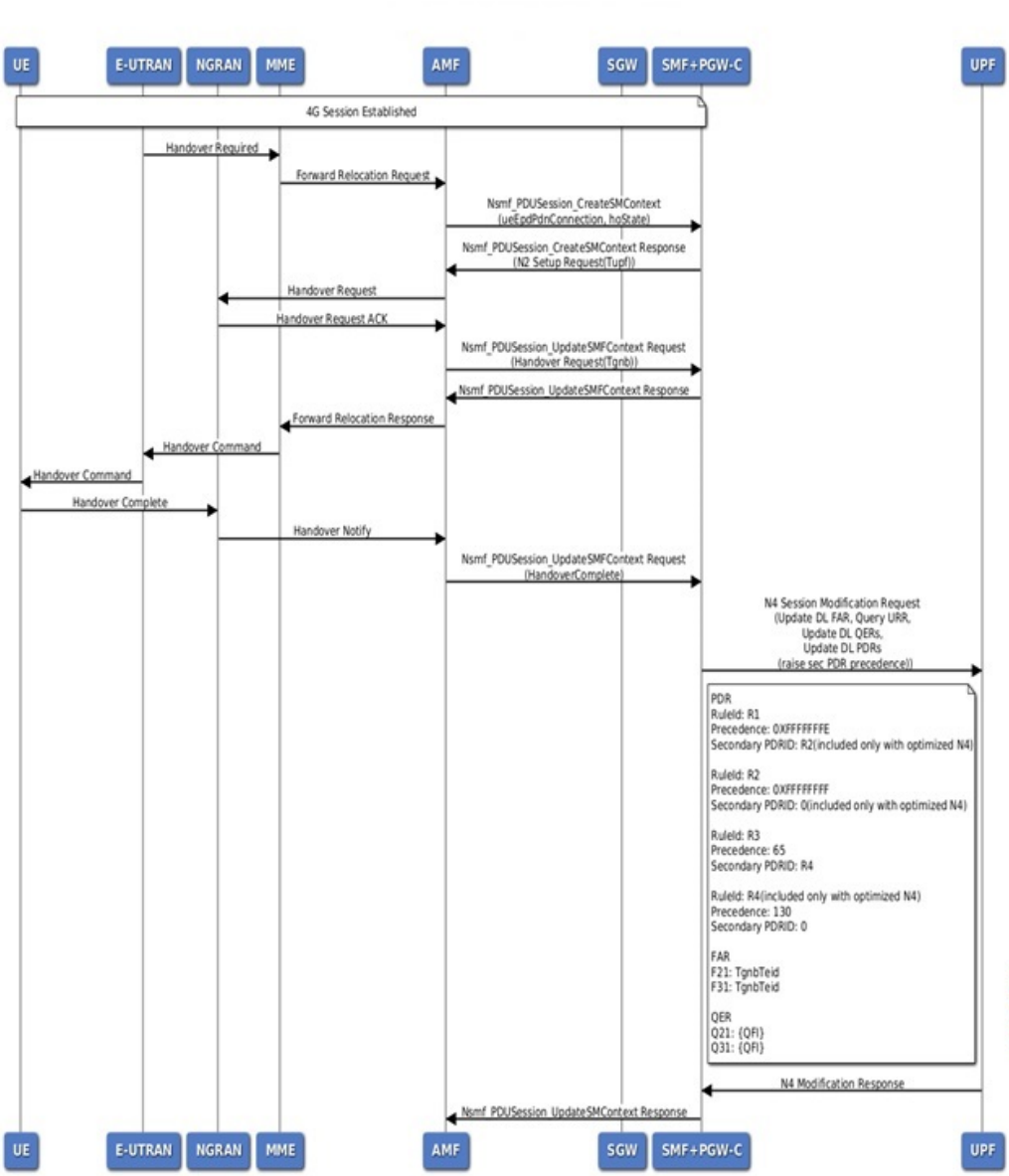

### 4G ローマーから 4G ホームページでの Inter-plmn N2 HO 手順のコール フローの説明

- サブスクライバがローミングの場合、SMF はホーム S-GW から ModifyBearerRequest を受信します。
- ModifyBearerRequest メッセージのローミング ステータスを判別します。
- N9 を削除し、N3 のセカンダリ PDR を作成
- 既存の FTEID を使用して S5 PDR を再作成します。

## *4G* ローマから *5G Homer* への *PLMN* 間ハンドオーバー

このセクションでは、4G ローマから 5G ホームへの Inter-plmn HO に関するコール フローと詳細について説明します。

図 *278 : 4G* ローマから *5G* ホームページへの *Inter-plmn HO* のコール フロー




**4G ローマから 5G ホームページへの Inter-plmn HO のコール フローの説明**

- N9 セカンダリを削除し、N3 プライマリ PDR を作成します。
- 既存の FTEID を使用して S5 PDR を再作成します。

# PLMN 間ハンドオーバーの構成

次の構成例を使用して、ローミングの inter-plmn ハンドオーバーを有効または無効にします。この構成を使用して、特定のDNNのInter-plmnローミングを無効にすることができます。

```
config
  profile dnn dnnprofile_name
    [ no ] supported-features [ inter-plmn-ho ]
```

注：

- **supported-features [ inter-plmn-ho ]**：ローミングの inter-plmn ハンドオーバーを有効にします。

（注） inter-plmn CLI が PGW-C+SMF で構成されていない場合、V-PLMN からの MBR は PGW-C+SMF によって拒否されます。V-PLMN からのハンドオーバーを処理するには、DNN プロファイルに inter-plmn-ho を構成することが必須です。

- **no**： 特定の DNN のローミング用の inter-plmn ハンドオーバーを無効にします。

### セカンダリ PDR 用の個別のトンネルを作成するための構成

サンプル設定を使用して、UPF で N3 および N9 インターフェイスの分離が有効になっているかどうかを確認します。n3-n9 インターフェイス分離が有効になっている場合、セカンダリ RAT PDR 用に別のトンネルが作成されます。そうでない場合は、同じトンネルがセカンダリ RAT に再利用されます。

```
config
  profile dnn dnnprofile_name
    [ no ] supported-features [ n3-interface-separation ]
```

注：

- **supported-features [ n3-interface-separation ]**：セカンダリ PDR 用に個別のトンネルを作成します。
- **no**：プライマリ PDR とセカンダリ PDR に同じトンネルを作成します。

（注） この構成が存在しない場合、SMF/PGW-C は、UPF で N3-N9 インターフェイスの分離が無効になっていると見なします。

# DTSSA および ACSCR の送信

SMF は、N11 および N16 インターフェイス上の SmContextCreated、SmContextUpdated、PduSessionCreated、および PduSessionUpdated IE のサポート対象機能で DTSSA および ACSCR を送信できます。

これにより、AMF は inter-plmn ローミングに適切な V-SMF および H-SMF を選択できます。

### DTSSA の構成

DTSSA または ACSCR を構成するには、構成例の参照として使用します。

```
config
  profile smf profile_name instances instance-id supported-features
      [ vsmf dtssa acscr]
```

注：

- **vsmf dtssa acscr**：サポートされている機能で DTSSA および ACSCR を送信します。

# OAM サポート

ここでは、SFM のインターフェイスのサポートに関する操作、管理、およびメンテナンスに関して説明します。

## バルク統計サポート

Inter-plmn モビリティ機能に、次のラベルが追加されました。

- interplmn_ho_not_configured
- dtssa_acscr_not_supported
- disc_vsmf_insert_dtssa_acscr_not_configured
- disc_vsmf_insert_interplmn_ho_not_configured
- disc_vsm_insert_hsmf_retrieve_failure
- disc_ro2ho_n2ho_interplmn_ho_not_configured
- disc_ro2ho_n4_modify_failed
- disc_ho2ro_n4_modify_failed
- disc_ho2ro_failure
- disc_ro2ho_failure
- ho2ro_invalid_state
- ro2ho_invalid_state
- disc_ro2ho_guard_timer_expiry
- disc_ho2ro_guard_timer_expiry
- disc_ro2ho_idft_timer_expiry
- smf_idft_inter_plmn_ro2ho_n2ho
- smf_dft_inter_plmn_ro2ho_n2ho
- smf_idft_inter_plmn_ho2ro_n2ho
- smf_dft_inter_plmn_ho2ro_n2ho

# N4 インターフェイスのローミング ステータス

**subscriber-params** N4 メッセージ内の独自の IE の下に **サブ IE** オプションが追加され、UPF がローミング ステータスを認識できるようになります。

```
SUBSCRIBER PARAMS:
Type: 226
    roaming-status: homer/roamer/visitor-hr/visitor-lbo
```

次の出力例は、ローミング ステータスを一覧表示したものです。

```
Homer- 1
Visitor-LBO - 2
Visitor-HR - 3
Roamer - 4
```

# トラブルシューティング情報

このセクションでは、システムの動作中に発生する可能性のあるローミング関連の問題をトラブルシューティングするために、コマンドライン インターフェイス（CLI）コマンド、アラート、ログとメトリックスの使用に関する情報について説明します。

## ローミング固有の情報の回線詳細

**show subscriber supi** *supi_id* **nf-service smf full** CLI コマンドは、UE のローミング ステータスを表示します。

（注） 2021.02 以降のリリースでは、 **namespace** キーワードは廃止され、 **nf-service** キーワードに置き換えられました。

```
[unknown-smf] smf# show subscriber supi imsi-123456789012345 nf-service smf full
subscriber-details
{
…
         "authStatus": "Unauthenticated",
         "roamingStatus": "Vistor LBO",    <<< In-Roamer UE Roaming Status
         "uePlmnId": {
           "mcc": "123",
           "mnc": "456"
         }

…
      "authStatus": "Unauthenticated",
         "roamingStatus": "Roamer",      <<< Out-Roamer UE Roaming Status
         "uePlmnId": {
           "mcc": "123",
           "mnc": "456"
         }
…
```

```
    "authStatus": "Unauthenticated",
    "roamingStatus": "Homer",
    "uePlmnId": {
      "mcc": "123",
      "mnc": "456"
    }
```

# hSMF に関するローミング固有の情報のサブスクライバの詳細

**show subscriber supi** *supi_id* **nf-service smf psid** *psid_value* **full** CLI コマンドは、hSMF としてローミング固有の使用例の詳細なサブスクライバ情報を表示します。

```
[unknown] smf# show subscriber supi imsi-123456789012345 nf-service smf
psid 5 full
subscriber-details
{
  "status": true,
  "genericInfo": {
    "supi": "imsi-310210789012346",
    "pei": "imei-123456786666660",
    "pduSessionId": 5,
    "pduSesstype": "Ipv4PduSession",
    "accessType": "3GPP_ACCESS",
    "dnn": "intershat",
    "plmnId": {
      "mcc": "310",
      "mnc": "560"
    },
    "sScMode": 1,
    "uetimeZone": "UTC+12:00",
    "allocatedIp": "209.165.200.229",
    "nrLocation": {
      "ncgi": {
        "mcc": "310",
        "mnc": "560",
        "nrCellId": "123456789"
      },
      "tai": {
        "mcc": "310",
        "mnc": "560",
        "tac": "1820"
      }
    },
    "alwaysOn": "None",
    "dcnr": "None",
    "wps": "Non-Wps Session",
    "ratType": "NR",
    "ueType": "NR Capable UE",
    "sessTimeStamp": "2021-06-18 18:49:28.266245111 +0000 UTC",
    "callDuration": "20.549700502s",
    "ipPool": "poolv4",
    "commonId": 2097158,
    "snssai": {
      "sd": "Abf123",
      "sst": 2
    },
    "authStatus": "Unauthenticated",
    "roamingStatus": "Roamer",
    "uePlmnId": {
      "mcc": "310",
      "mnc": "210"
    }
```

```
},
"accessSubData": {
  "amfID": "AFbe08",
  "amfPlmnId": {
    "mcc": "310",
    "mnc": "560"
  },
  "epsInterworkingIndication": "WITHOUT_N26"
},
"policySubData": {
  "TotalDynamicRules": 2,
  "TotalFlowCount": 2,
  "TotalNonGBRFlows": 1,
  "TotalGBRFlows": 1,
  "pccRuleList": [
    {
      "pccRuleId": "PccRule-1",
      "qfi": 2,
      "gbrDl": 2000000000,
      "gbrUl": 1000000000,
      "mbrDl": 4000000000,
      "mbrUl": 3000000000,
      "flowInformation": [
        {
          "flowLabel": "flow",
          "spi": "2",
          "flowDirection": 3,
          "flowDescription": "permit out ip from 209.165.200.225 to 209.165.200.254",
          "tosTrafficClass": "8"
        }
      ],
      "chargingInformation": {
        "chargingId": "ChargingData-1",
        "meteringMethod": "Duration and Volume",
        "Type": "Online",
        "ratingGroup": 10,
        "serviceId": "20"
      }
    },
    {
      "pccRuleId": "defaultrule",
      "qfi": 1,
      "mbrDl": 125000000,
      "mbrUl": 100000000,
      "flowInformation": [
        {
          "flowDirection": 3,
          "flowDescription": "permit out ip from any to any"
        }
      ]
    }
  ],
  "qosFlow": [
    {
      "qfi": 2,
      "GBRFlow": "True",
      "bindingParameters": {
        "x5Qi": 3,
        "arp": {
          "preemptCap": "NOT_PREEMPT",
          "preemptVuln": "PREEMPTABLE",
          "priorityLevel": 7
        }
      },
```

```
          "AggregatedULGFbr": 1000000000,
          "AggregatedDLGFbr": 2000000000,
          "AggregatedULMFbr": 3000000000,
          "AggregatedDLMFbr": 4000000000,
          "pccRuleList": "PccRule-1",
          "qosDescList": "QoS-1,"
        },
        {
          "qfi": 1,
          "GBRFlow": "False",
          "bindingParameters": {
            "x5Qi": 5,
            "arp": {
              "preemptCap": "NOT_PREEMPT",
              "preemptVuln": "NOT_PREEMPTABLE",
              "priorityLevel": 15
            },
            "priorityLevel": 1
          },
          "AggregatedULMFbr": 100000000,
          "AggregatedDLMFbr": 125000000,
          "pccRuleList": "defaultrule",
          "qosDescList": "default,"
        }
      ],
      "policyType": "Pcf",
      "pcfInteraction": "Pcf Interaction: ON",
      "ruleBase": "starent",
      "sessRuleList": [
        {
          "authDefaultQos": "&QosProfileKey{X5QI:5,Arp:{PreemptionCapability_NOT_PREEMPT
PreemptionVulnerability_NOT_PREEMPTABLE 15
true},Priority:1,MaxDataBurstVol:0,Qnc:false,AveragingWindow:,}",
          "authSessAmbr": {
            "downlink": 125000000,
            "uplink": 100000000
          },
          "sessRuleId": "default"
        }
      ],
      "presenceReporting": "Disabled"
    },
    "chargingData": {
      "invcSeqNo": 1,
      "pduChId": 2097158,
      "ccId": "1",
      "chargingIdRtgGrpMapInfo": {
        "rgId": "10",
        "chargingId": [
          "ChargingData-1",
          "l10of",
          "l10on"
        ]
      },
      "chargParmMapInfo": [
        {
          "ratingGrp": 10,
          "chargingId": "ChargingData-1",
          "online": "true",
          "offline": "true",
          "serviceID": 20,
          "pccRuleIds": [
            "PccRule-1"
          ],
```

```
    "linkedChrgId": [
      "l10of",
      "l10on",
      "sesslevelurr"
    ],
    "meteringMthd": "MeteringMethod_DURATION_VOLUME",
    "reportingLevelOnline": "ReportingLevel_RAT_GR_LEVEL",
    "reportingLevelOffline": "ReportingLevel_RAT_GR_LEVEL",
    "configured": "false",
    "tightInterworkingMode": "false",
    "parent": "true",
    "reportingParm": "false",
    "limitParm": "false",
    "limitsChrgParamOnline": "l10on",
    "limitsChrgParamOffline": "l10of",
    "qosIds": [
      "QoS-1"
    ],
    "qfi": 2,
    "offlineConverted": "false"
  },
  {
    "ratingGrp": 10,
    "chargingId": "l10of",
    "online": "false",
    "offline": "true",
    "pccRuleIds": [
      "PccRule-1"
    ],
    "linkedChrgId": [
      "sesslevelurr"
    ],
    "meteringMthd": "MeteringMethod_DURATION_VOLUME",
    "reportingLevelOnline": "ReportingLevel_Dummy",
    "reportingLevelOffline": "ReportingLevel_RAT_GR_LEVEL",
    "configured": "false",
    "tightInterworkingMode": "false",
    "parent": "false",
    "reportingParm": "true",
    "limitParm": "true",
    "qosIds": [
      "QoS-1"
    ],
    "qfi": 2,
    "offlineConverted": "false"
  },
  {
    "ratingGrp": 10,
    "chargingId": "l10on",
    "online": "true",
    "offline": "false",
    "pccRuleIds": [
      "PccRule-1"
    ],
    "linkedChrgId": [
      "sesslevelurr"
    ],
    "meteringMthd": "MeteringMethod_DURATION_VOLUME",
    "reportingLevelOnline": "ReportingLevel_RAT_GR_LEVEL",
    "reportingLevelOffline": "ReportingLevel_Dummy",
    "configured": "false",
    "tightInterworkingMode": "false",
    "parent": "false",
    "reportingParm": "true",
```

```
      "limitParm": "true",
      "qosIds": [
        "QoS-1"
      ],
      "qfi": 2,
      "offlineConverted": "false"
    },
    {
      "chargingId": "sesslevelurr",
      "online": "false",
      "offline": "true",
      "pccRuleIds": [
        "PccRule-1"
      ],
      "meteringMthd": "MeteringMethod_DURATION_VOLUME",
      "reportingLevelOnline": "ReportingLevel_Dummy",
      "reportingLevelOffline": "ReportingLevel_Dummy",
      "configured": "false",
      "tightInterworkingMode": "false",
      "parent": "false",
      "reportingParm": "false",
      "limitParm": "true",
      "offlineConverted": "false"
    }
  ],
  "chTriggerInfo": {
    "sessionTriggerInfo": [
      {
        "triggerType": "VOLUME_LIMIT",
        "triggerCategory": "IMMEDIATE_REPORT",
        "triglevel": 2
      },
      {
        "triggerType": "TIME_LIMIT",
        "triggerCategory": "IMMEDIATE_REPORT",
        "triglevel": 2
      },
      {
        "triggerType": "AMBR_CHANGE",
        "triggerCategory": "IMMEDIATE_REPORT",
        "triglevel": 2
      },
      {
        "triggerType": "QOS_CHANGE",
        "triggerCategory": "DEFERRED_REPORT",
        "triglevel": 2
      }
    ],
    "rgTrgrList": [
      {
        "ratingGroup": 10,
        "rgTriggerInfo": [
          {
            "triggerType": "QUOTA_THRESHOLD",
            "triggerCategory": "IMMEDIATE_REPORT",
            "triglevel": 1
          },
          {
            "triggerType": "VOLUME_LIMIT",
            "triggerCategory": "IMMEDIATE_REPORT",
            "triglevel": 1
          },
          {
            "triggerType": "TIME_LIMIT",
```

```
          "triggerCategory": "IMMEDIATE_REPORT",
          "triglevel": 1
        },
        {
          "triggerType": "QUOTA_EXHAUSTED",
          "triggerCategory": "IMMEDIATE_REPORT",
          "triglevel": 1
        }
      ]
    }
  ]
},
"chThresholdInfo": {
  "sessthresholdInformation": {
    "volumeThreshold": 45000,
    "durationThreshold": 90
  },
  "rgthresholdInformation": [
    {
      "volumeThreshold": 7000,
      "durationThreshold": 800
    }
  ],
  "quotaInformation": [
    {
      "quotaHoldingTime": -1,
      "timeQuotaThreshold": 10,
      "volQuotaThreshold": 1000,
      "downlinkVolume": 20000,
      "time": 100,
      "totalVolume": 35000,
      "uplinkVolume": 15000,
      "ratingGrp": 10
    }
  ]
},
"startTime": "2021-06-18T18:49:28Z",
"rulebase": "starent",
"chargingDisabled": "false",
"dropTraffic": "false",
"gtppGrp": "group1",
"profileName": "chgprf1",
"accountingEnabled": "false",
"n40ChargingEnabled": "true",
"QbcProfileName": "qbc_general",
"qbcChargingEnabled": "True",
"roamingQbcInfo": {
  "qfiTh": {
    "volTh": 30000,
    "durTh": 80
  },
  "qfis": {
    "rgTriggerInfo": [
      {
        "triggerType": "QOS_CHANGE",
        "triggerCategory": "IMMEDIATE_REPORT",
        "triglevel": 2
      },
      {
        "triggerType": "TIME_LIMIT",
        "triggerCategory": "IMMEDIATE_REPORT",
        "triglevel": 2
      },
      {
```

```
            "triggerType": "VOLUME_LIMIT",
            "triggerCategory": "IMMEDIATE_REPORT",
            "triglevel": 2
          }
        ]
      },
      "partialRecordMethod": "PartialRecordMethod_DEFAULT"
    },
    "qbcChargParam": [
      {
        "chargingId": "qfi1",
        "qfi": 1,
        "meteringMthd": "MeteringMethod_DURATION_VOLUME",
        "reportingParam": "True",
        "limitParam": "True",
        "parent": "True"
      },
      {
        "chargingId": "qfi2",
        "qfi": 2,
        "meteringMthd": "MeteringMethod_DURATION_VOLUME",
        "reportingParam": "True",
        "limitParam": "True",
        "parent": "True"
      }
    ],
    "chfGroupId": "CHF-dnn=intershat;",
    "fbcChargingEnabled": "True"
  },
  "upfServData": {
    "numberOfTunnels": 1,
    "smfSeid": 9007228892966842,
    "qerInfo": [
      {
        "qosId": "Sess#Level",
        "qerId": 1,
        "refcnt": 1
      },
      {
        "qosId": "QoS-1@def#TC",
        "qerId": 2,
        "refcnt": 1
      },
      {
        "qosId": "default@def#TC",
        "qerId": 3,
        "refcnt": 1
      }
    ],
    "urrInfo": [
      {
        "chargingId": "ChargingData-1",
        "urrId": 16
      },
      {
        "chargingId": "l10of",
        "urrId": 33
      },
      {
        "chargingId": "l10on",
        "urrId": 55
      },
      {
        "chargingId": "sesslevelurr",
```

```
        "urrId": 76
      },
      {
        "chargingId": "qfi1",
        "urrId": 82
      },
      {
        "chargingId": "qfi2",
        "urrId": 98
      }
    ],
    "mapping": {
      "tunnelMapping": [
        {
          "TunnelID": 1,
          "tunnelName": "gnbTunnel",
          "RemoteTeid": {
            "teID": 1001,
            "ipAddr": "209.165.200.241"
          }
        }
      ]
    },
    "upfSeid": "17293822569102704642",
    "TotalNumberOfPdrs": "4 (Ul:2 Dl:2)",
    "TotalNumberOfFars": 4,
    "TotalNumberOfQers": 3,
    "TotalNumberOfUrrs": 6
  }
}
```


# hSMF に関するローミング固有の情報のサブスクライバ セッションの詳細

**show subscriber supi** *supi_id* **nf-service smf psid** *psid_value* **summary** CLI コマンドは、hSMF としてローミング固有の使用例のサブスクライバ セッションに関する詳細情報を表示します。

```
[unknown] smf# show subscriber supi imsi-123456789012345 nf-service smfpsid
 5 summary
subscriber-details
{
  "status": true,
  "genericInfo": {
    "supi": "imsi-310210789012346",
    "pduSessionId": 5,
    "pduSesstype": "Ipv4PduSession",
    "accessType": "3GPP_ACCESS",
    "dnn": "intershat",
    "plmnId": {
      "mcc": "310",
      "mnc": "560"
    },
    "allocatedIp": "209.165.200.240",
    "ratType": "NR",
    "sessTimeStamp": "2021-06-18 18:49:28.266245111 +0000 UTC",
    "authStatus": "Unauthenticated",
    "roamingStatus": "Roamer",
    "uePlmnId": {
      "mcc": "310",
      "mnc": "210"
```

```
  }
},
"policySubData": {
  "TotalDynamicRules": 2,
  "TotalFlowCount": 2,
  "TotalNonGBRFlows": 1,
  "TotalGBRFlows": 1,
  "pcfInteraction": "Pcf Interaction: ON",
  "ruleBase": "starent"
},
"chargingData": {
  "chargParmMapInfo": [
    {
      "chargingId": "ChargingData-1",
      "offlineConverted": "false"
    },
    {
      "chargingId": "l10of",
      "offlineConverted": "false"
    },
    {
      "chargingId": "l10on",
      "offlineConverted": "false"
    },
    {
      "chargingId": "sesslevelurr",
      "offlineConverted": "false"
    }
  ],
  "chargingDisabled": "false",
  "dropTraffic": "false",
  "gtppGrp": "group1",
  "profileName": "chgprf1",
  "accountingEnabled": "false",
  "n40ChargingEnabled": "true",
  "QbcProfileName": "qbc_general",
  "qbcChargingEnabled": "True",
  "qbcChargParam": [
    {},
    {}
  ],
  "chfGroupId": "CHF-dnn=intershat;",
  "fbcChargingEnabled": "True"
},
"upfServData": {
  "smfSeid": 9007228892966842,
  "qerInfo": [
    {
      "qosId": "Sess#Level",
      "qerId": 1,
      "refcnt": 1
    },
    {
      "qosId": "QoS-1@def#TC",
      "qerId": 2,
      "refcnt": 1
    },
    {
      "qosId": "default@def#TC",
      "qerId": 3,
      "refcnt": 1
    }
  ],
  "urrInfo": [
```

```
      {
        "chargingId": "ChargingData-1",
        "urrId": 16
      },
      {
        "chargingId": "l10of",
        "urrId": 33
      },
      {
        "chargingId": "l10on",
        "urrId": 55
      },
      {
        "chargingId": "sesslevelurr",
        "urrId": 76
      },
      {
        "chargingId": "qfi1",
        "urrId": 82
      },
      {
        "chargingId": "qfi2",
        "urrId": 98
      }
    ],
    "mapping": {
      "tunnelMapping": [
        {
          "TunnelID": 1,
          "tunnelName": "gnbTunnel",
          "RemoteTeid": {
            "teID": 1001,
            "ipAddr": "209.165.200.231"
          }
        }
      ]
    },
    "upfSeid": "17293822569102704642",
    "TotalNumberOfPdrs": "4 (Ul:2 Dl:2)",
    "TotalNumberOfFars": 4,
    "TotalNumberOfQers": 3,
    "TotalNumberOfUrrs": 6
  }
}
```

# vSMFのローミング固有情報のサブスクライバの詳細

**show subscriber supi** *supi_id* **nf-service smf psid** *psid_value* **full** CLI コマンドは、vSMF としてローミング固有の使用例の詳細なサブスクライバ情報を表示します。

```
[unknown] smf# show subscriber supi imsi-123456789012345 nf-service smf
psid 5 full
subscriber-details
{
  "status": true,
  "genericInfo": {
    "supi": "imsi-310480789012346",
    "pei": "imei-123456786666660",
    "pduSessionId": 5,
    "pduSesstype": "Ipv4PduSession",
    "accessType": "3GPP_ACCESS",
    "dnn": "intershat",
```

```
  "plmnId": {
    "mcc": "310",
    "mnc": "260"
  },
  "uetimeZone": "UTC+12:00",
  "allocatedIp": "209.165.202.131",
  "nrLocation": {
    "ncgi": {
      "mcc": "310",
      "mnc": "260",
      "nrCellId": "123456789"
    },
    "tai": {
      "mcc": "310",
      "mnc": "260",
      "tac": "1820"
    }
  },
  "alwaysOn": "None",
  "dcnr": "None",
  "wps": "Non-Wps Session",
  "ratType": "NR",
  "ueType": "NR Capable UE",
  "sessTimeStamp": "2021-06-18 18:55:11.252750658 +0000 UTC",
  "callDuration": "42.336122162s",
  "commonId": 2097159,
  "snssai": {
    "sd": "Abf123",
    "sst": 2
  },
  "authStatus": "Unauthenticated",
  "roamingStatus": "Vistor HR",
  "uePlmnId": {
    "mcc": "310",
    "mnc": "480"
  }
},
"accessSubData": {
  "amfID": "AFbe08",
  "amfPlmnId": {
    "mcc": "310",
    "mnc": "260"
  },
  "ueCmStatus": "UeCMConnected",
  "amfNrfID": "76517361-338e-4d77-bc76-713a79779574",
  "epsInterworkingIndication": "WITHOUT_N26"
},
"policySubData": {
  "TotalFlowCount": 2,
  "TotalNonGBRFlows": 1,
  "TotalGBRFlows": 1,
  "qosFlow": [
    {
      "qfi": 1,
      "GBRFlow": "False",
      "bindingParameters": {
        "x5Qi": 5,
        "arp": {
          "preemptCap": "NOT_PREEMPT",
          "preemptVuln": "NOT_PREEMPTABLE",
          "priorityLevel": 1
        },
        "priorityLevel": 10,
        "maximumDataBurstVolume": 1,
```

```
          "averagingWindow": "2003"
        }
      },
      {
        "qfi": 4,
        "GBRFlow": "True",
        "bindingParameters": {
          "x5Qi": 4,
          "arp": {
            "preemptCap": "NOT_PREEMPT",
            "preemptVuln": "NOT_PREEMPTABLE",
            "priorityLevel": 1
          },
          "priorityLevel": 1,
          "maximumDataBurstVolume": 1,
          "averagingWindow": "1"
        },
        "AggregatedULGFbr": 10000000,
        "AggregatedDLGFbr": 10000000,
        "AggregatedULMFbr": 1000000000,
        "AggregatedDLMFbr": 1000000000,
        "ebi": 8
      }
    ],
    "SessAmbrUl": 200000000,
    "SessAmbrDl": 125000000
  },
  "chargingData": {
    "invcSeqNo": 3,
    "pduChId": 2097159,
    "ccId": "0",
    "chargingIdRtgGrpMapInfo": {},
    "chTriggerInfo": {},
    "chThresholdInfo": {
      "sessthresholdInformation": {}
    },
    "startTime": "2021-06-18T18:55:11Z",
    "chargingDisabled": "false",
    "dropTraffic": "false",
    "profileName": "chgprf1",
    "accountingEnabled": "false",
    "n40ChargingEnabled": "true",
    "QbcProfileName": "qbc_maxlimit",
    "qbcChargingEnabled": "True",
    "roamingQbcInfo": {
      "qfiTh": {
        "volTh": 40000,
        "durTh": 90
      },
      "qfis": {
        "rgTriggerInfo": [
          {
            "triggerType": "QOS_CHANGE",
            "triggerCategory": "IMMEDIATE_REPORT",
            "triglevel": 2
          },
          {
            "triggerType": "TIME_LIMIT",
            "triggerCategory": "IMMEDIATE_REPORT",
            "triglevel": 2
          },
          {
            "triggerType": "VOLUME_LIMIT",
            "triggerCategory": "IMMEDIATE_REPORT",
```

```
            "triglevel": 2
          }
        ]
      },
      "partialRecordMethod": "PartialRecordMethod_DEFAULT"
    },
    "qbcChargParam": [
      {
        "chargingId": "qfi1",
        "qfi": 1,
        "meteringMthd": "MeteringMethod_DURATION_VOLUME",
        "reportingParam": "True",
        "limitParam": "True",
        "parent": "True"
      },
      {
        "chargingId": "qfi4",
        "qfi": 4,
        "meteringMthd": "MeteringMethod_DURATION_VOLUME",
        "reportingParam": "True",
        "limitParam": "True",
        "parent": "True"
      }
    ],
    "chfGroupId": "CHF-dnn=intershat;",
    "fbcChargingEnabled": "False"
  },
  "upfServData": {
    "numberOfTunnels": 1,
    "smfSeid": 9007233406673128,
    "qerInfo": [
      {
        "qosId": "Sess#Level",
        "qerId": 1,
        "refcnt": 1
      },
      {
        "qosId": "BQF_1",
        "qerId": 2,
        "refcnt": 1
      },
      {
        "qosId": "BQF_4",
        "qerId": 4,
        "refcnt": 1
      }
    ],
    "urrInfo": [
      {
        "chargingId": "qfi1",
        "urrId": 18
      },
      {
        "chargingId": "qfi4",
        "urrId": 50
      }
    ],
    "mapping": {
      "tunnelMapping": [
        {
          "TunnelID": 1,
          "tunnelName": "gnbTunnel",
          "RemoteTeid": {
            "teID": 5555,
```

```
            "ipAddr": "209.165.200.242"
          }
        }
      ]
    },
    "upfSeid": "17293822569102704642",
    "TotalNumberOfPdrs": "4 (Ul:2 Dl:2)",
    "TotalNumberOfFars": 4,
    "TotalNumberOfQers": 3,
    "TotalNumberOfUrrs": 2
  }
}
```

# vSMFに関するローミング固有の情報のサブスクライバ セッションの詳細

**show subscriber supi** *supi_id* **nf-service smf psid** *psid_value* **summary** CLI コマンドは、vSMF としてローミング固有の使用例のサブスクライバ セッションに関する詳細情報を表示します。

```
[unknown] smf# show subscriber supi imsi-123456789012345 nf-service smf
psid 5 summary
subscriber-details
{
  "status": true,
  "genericInfo": {
    "supi": "imsi-310480789012346",
    "pduSessionId": 5,
    "pduSesstype": "Ipv4PduSession",
    "accessType": "3GPP_ACCESS",
    "dnn": "intershat",
    "plmnId": {
      "mcc": "310",
      "mnc": "260"
    },
    "allocatedIp": "209.165.200.231",
    "ratType": "NR",
    "sessTimeStamp": "2021-06-18 18:55:11.252750658 +0000 UTC",
    "authStatus": "Unauthenticated",
    "roamingStatus": "Vistor HR",
    "uePlmnId": {
      "mcc": "310",
      "mnc": "480"
    }
  },
  "policySubData": {
    "TotalFlowCount": 2,
    "TotalNonGBRFlows": 1,
    "TotalGBRFlows": 1,
    "SessAmbrUl": 200000000,
    "SessAmbrDl": 125000000
  },
  "chargingData": {
    "chargingDisabled": "false",
    "dropTraffic": "false",
    "profileName": "chgprf1",
    "accountingEnabled": "false",
    "n40ChargingEnabled": "true",
    "QbcProfileName": "qbc_maxlimit",
    "qbcChargingEnabled": "True",
```

```
    "qbcChargParam": [
      {},
      {}
    ],
    "chfGroupId": "CHF-dnn=intershat;",
    "fbcChargingEnabled": "False"
  },
  "upfServData": {
    "smfSeid": 9007233406673128,
    "qerInfo": [
      {
        "qosId": "Sess#Level",
        "qerId": 1,
        "refcnt": 1
      },
      {
        "qosId": "BQF_1",
        "qerId": 2,
        "refcnt": 1
      },
      {
        "qosId": "BQF_4",
        "qerId": 4,
        "refcnt": 1
      }
    ],
    "urrInfo": [
      {
        "chargingId": "qfi1",
        "urrId": 18
      },
      {
        "chargingId": "qfi4",
        "urrId": 50
      }
    ],
    "mapping": {
      "tunnelMapping": [
        {
          "TunnelID": 1,
          "tunnelName": "gnbTunnel",
          "RemoteTeid": {
            "teID": 5555,
            "ipAddr": "209.165.200.242"
          }
        }
      ]
    },
    "upfSeid": "17293822569102704642",
    "TotalNumberOfPdrs": "4 (Ul:2 Dl:2)",
    "TotalNumberOfFars": 4,
    "TotalNumberOfQers": 3,
    "TotalNumberOfUrrs": 2
  }
}
```


# ローマ UE アラート

ここでは、ローマ UE でサポートされているアラートについて説明します。これらのアラートは、RAT ベースまたはエンド ユーザーの意図に従って強化できます。

## ローマ内 UE 障害しきい値アラート

次の例を使用して、インローマ UE 障害しきい値に関連するアラートを構成します。

```
alerts rules group RoamerUEs
 rule In-Roamer_SR
  expression "sum by (namespace) (increase(smf_service_stats{app_name=\"smf\",
roaming_status=\"visitor-lbo\", rat_type!=\"\", status=\"Success\"}[5m])) / sum by
(namespace) (increase(smf_service_stats{app_name=\"smf\", roaming_status=\"visitor-lbo\",
 rat_type!=\"\", status=\"attempted\"}[5m])) < 0.10"
  severity major
  type "Communications Alarm"
  annotation summary
   value "This alert is fired when the percentage of successful InRoamer is lesser than
 threshold"
  exit
exit
```

## アウトローマ UE 障害しきい値アラート

次の例を使用して、アウトローマ UE 障害しきい値に関連するアラートを構成します。

```
rule Radius_Acct_Release_SR
   rule Out-Roamer_SR
  expression "sum by (namespace) (increase(smf_service_stats{app_name=\"smf\",
roaming_status=\"roamer\", rat_type!=\"\", status=\"Success\"}[5m])) / sum by (namespace)
 (increase(smf_service_stats{app_name=\"smf\", roaming_status=\"roamer\", rat_type!=\"\",
 status=\"attempted\"}[5m])) < 0.10"
  severity major
  type "Communications Alarm"
  annotation summary
   value "This alert is fired when the percentage of successful InRoamer is lesser than
 threshold"
  exit
exit
```

# ローマー UE バルク統計情報

次の SMF サービスのバルク統計情報を使用して、ローマ UE に関連する障害または問題を監視します。

**表 *468 :* ローマ *UE***

| バルク統計名 | [Query（クエリ）] | 説明 |
|---|---|---|
| 4G_In-Roamers_Attempted | bulk-stats query 4G_In-Roamers_Attempted expression "sum(smf_service_stats {roaming_status='visitor-lbo', status='attempted',rat_type='EUTRA'}) by (namespace)" exit | |
| 4G_In-Roamers_Success | bulk-stats query 4G_In-Roamers_Success expression "sum(smf_service_stats {roaming_status='visitor-lbo', status='success',rat_type='EUTRA'}) by (namespace)" exit | |
| 4G_Out-Roamers_Attempted | bulk-stats query 4G_Out-Roamers_Attempted expression "sum(smf_service_stats {roaming_status='roamer', status='attempted',rat_type='EUTRA'}) by (namespace)" exit | |

| バルク統計名 | [Query（クエリ）] | 説明 |
|---|---|---|
| 4G_Out-Roamer_Success | bulk-stats query 4G_Out-Roamers_Success expression "sum(smf_service_stats {roaming_status='roamer', status='success',rat_type='EUTRA'}) by (namespace)" exit | |
| 5G_In-Roamers_Attempted | bulk-stats query 5G_In-Roamers_Attempted expression "sum(smf_service_stats {roaming_status='visitor-lbo', status='attempted',rat_type='NR'}) by (namespace)" exit | |
| 5G_In-Roamers_Success | bulk-stats query 5G_In-Roamers_Success expression "sum(smf_service_stats {roaming_status='visitor-lbo', status='success',rat_type='NR'}) by (namespace)" exit | |
| 5G_Out-Roamers_Attempted | bulk-stats query 5G_Out-Roamers_Attempted expression "sum(smf_service_stats {roaming_status='roamer', status='attempted',rat_type='NR'}) by (namespace)" exit | |
| 5G_Out-Roamers_Success | bulk-stats query 5G_Out-Roamers_Success expression "sum(smf_service_stats {roaming_status='roamer', status='success',rat_type='NR'}) by (namespace)" exit | |
| WiFi_In-Roamers_Attempted | bulk-stats query WiFi_In-Roamers_Attempted expression "sum(smf_service_stats {roaming_status='visitor-lbo', status='attempted',rat_type='WLAN'}) by (namespace)" exit | |
| WiFi_In-Roamers_Success | bulk-stats query WiFi_In-Roamers_Success expression "sum(smf_service_stats {roaming_status='visitor-lbo', status='success',rat_type='WLAN'}) by (namespace)" exit | |
| WiFi_Out-Roamers_Attempted | bulk-stats query WiFi_Out-Roamers_Attempted expression "sum(smf_service_stats {roaming_status='roamer', status='attempted',rat_type='WLAN'}) by (namespace)" exit | |
| WiFi_Out-Roamers_Success | bulk-stats query WiFi_Out-Roamers_Success expression "sum(smf_service_stats {roaming_status='roamer', status='success',rat_type='WLAN'}) by (namespace)" exit | |

# ローミング エラー ログ

このセクションでは、基本的なエラー状態と、ローミング機能の障害をデバッグするためにキャプチャされるログを示します。

### PLMN 検証の失敗

次の例では、PLMN 検証の失敗に関するエラー ログが表示され、ローミング ステータスが「none」に設定されます。

```
2021/01/06 15:25:18.630 smf-service [DEBUG] [genericinfo.go:1597]
[smf-service.smf-app.subscriber] Set roaming status to 0
2021/01/06 15:25:18.630 smf-service [DEBUG] [genericinfo.go:2317]
[smf-service.smf-app.subscriber]  Subscriber is %!s(uint32=0)
2021/01/06 15:25:18.630 smf-service [ERROR] [genericinfo.go:1082]
```

```
[smf-service.smf-app.subscriber] PLMN validation failed
2021/01/06 15:25:18.630 smf-service [DEBUG] [subscriber_policy_config.go:187]
[misc-lib.config.subscriber-policy] LookupParameters - {imsi-123456789012345
msisdn-223310101010101 imei-123456786666660  0 123 456 intershat}
```

### ホーマー UE ステータス（ホーマー）

次に、UE ローミング ステータスの汎用ログの例を示します。

```
2021/01/06 15:04:39.146 smf-service [DEBUG] [genericinfo.go:1597]
[smf-service.smf-app.subscriber] Set roaming status to 1
2021/01/06 15:04:39.146 smf-service [DEBUG] [genericinfo.go:2317]
[smf-service.smf-app.subscriber]  Subscriber is %!s(uint32=1)
2021/01/06 15:04:39.146 smf-service [DEBUG] [subscriber_policy_config.go:187]
[misc-lib.config.subscriber-policy] LookupParameters - {imsi-123456789012345
msisdn-9999988888 imei-352099001761480 Abf123 2 310 310 intershat}
```

### アウトローマー UE ステータス（ローミング）

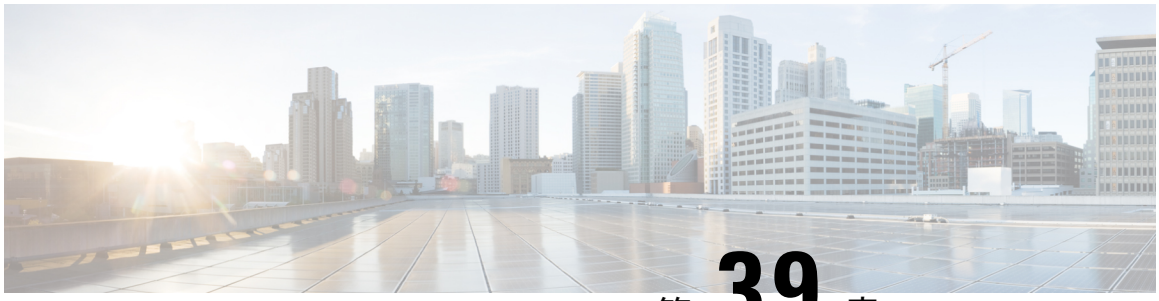
アウトローマー UE ステータスの汎用ログの例を次に示します。

```
2021/01/06 16:11:02.710 smf-service [DEBUG] [genericinfo.go:1597]
[smf-service.smf-app.subscriber] Set roaming status to 4
2021/01/06 16:11:02.710 smf-service [DEBUG] [genericinfo.go:2317]
[smf-service.smf-app.subscriber]  Subscriber is %!s(uint32=4)
2021/01/06 16:11:02.710 smf-service [DEBUG] [subscriber_policy_config.go:187]
[misc-lib.config.subscriber-policy] LookupParameters - {imsi-123456789012345
```

### ローミング中の UE ステータス（ビジター LBO）

次に、インローマ UE ステータスの汎用ログの例を示します。

```
2021/01/06 15:54:32.323 smf-service [DEBUG] [genericinfo.go:1597]
[smf-service.smf-app.subscriber] Set roaming status to 2
2021/01/06 15:54:32.323 smf-service [DEBUG] [genericinfo.go:2317]
[smf-service.smf-app.subscriber]  Subscriber is %!s(uint32=2)
2021/01/06 15:54:32.323 smf-service [DEBUG] [subscriber_policy_config.go:187]
[misc-lib.config.subscriber-policy] LookupParameters - {imsi-123456789012345
msisdn-223310101010101 imei-123456786666660  0 310 310 intershat}
```



第 39 章

# セッションおよびサービス継続性モード


- 機能の概要と変更履歴, on page 1733
- 機能説明, on page 1734
- SSC モードの構成, on page 1735


# 機能の概要と変更履歴

## 要約データ

***Table 469:*** 要約データ

| | |
|---|---|
| 該当製品または機能エリア | SMF |
| 該当プラットフォーム | SMI |
| 機能のデフォルト設定 | 有効：常時オン |
| このリリースでの関連する変更点 | N/A |
| 関連資料 | 該当なし |

## 更新履歴

***Table 470:*** マニュアルの変更履歴

| 改訂の詳細 | リリース |
|---|---|
| 最初の導入。 | 2020.02.0 より前 |

# 機能説明

5G システム アーキテクチャのセッションおよびサービス継続性（SSC）サポートは、ユーザー機器（UE）のさまざまなアプリケーションとサービスのさまざまな継続的な要件に対応します。5G システムは、さまざまな SSC モードをサポートします。PDU セッションに関連付けられている SSC モードは、PDU セッションの存続期間中は変更されません。SSC 機能は、次の 3 つのモードをサポートしています。

- SSC モード1：ネットワークは UE に提供される接続サービスを保持します。IPv4 または IPv6 または IPv4v6 タイプの PDU セッションの場合、IP アドレスは保持されます。
- SSC モード 2：ネットワークは、UE に配信された接続サービスを解放し、対応する PDU セッションも解放できます。IPv4 または IPv6 または IPv4v6 タイプの場合、PDU セッションが解放されると、UE に割り当てられた IP アドレスが解放されます。
- SSC モード 3：ユーザー プレーンの変更は、ネットワークによって、UE の接続が失われないようにしながら、UE に表示されます。サービスの継続性を向上させるため、前の接続が終了する前に、新しい PDU セッション アンカー ポイントを介した接続が確立されます。IPv4 または IPv6 または IPv4v6 タイプの場合、PDU セッション アンカーが変更されても、IP アドレスはこのモードでは保持されません。

## SSC モードの選択

SSC のモード選択ポリシーは、UE のアプリケーションまたはアプリケーション グループに関連付けられたモードのタイプを決定します。UDM からのサブスクリプション情報の一部として、SMF は、DNN および S-NSSAI ごとに、サポートされている SSC モードとデフォルトの SSC モードのリストを受信します。

SSC モードを選択するには、UE が PDU セッション確立要求で SSC モードを送信するときに、サブスクライバ データとローカル SMF 構成とを照合して許可される SSC モードが決定されます。

**Important** SMF は、SSC mode-1 のみをサポートします。

## SSC モードを選択するための優先順位

SSC モードを選択する際の優先順位は次のとおりです：

- 優先順位#1：UDMからのサブスクライバ データの優先順位が最も高くなります。UDM は、DefaultSscMode と AllowedSscMode を送信します。
- 優先度 #2：DNN プロファイルに存在するローカル SSC モード構成データには、ssc-mode と allowed-ssc-mode が含まれています。

# SSC モードの選択方法

SSC モードでは、次の選択方法をサポートしています。

- SMF は、UE が送信した SSC モードがデフォルトの SSC モードまたは許可された SSC モードのいずれかであるかどうかを、優先順位に従って確認します。見つかった場合は、PDU の確立手順が続行されます。それ以外の場合は、PDU セッション確立拒否メッセージが、拒否メッセージで許可された SSC モードで UE に送信されます。
- SMF が UE から SSC モードを受信しない場合、デフォルトの SSC モード（優先順位に従います）が選択され、PDU セッションの確立に使用されます。

UE が SSC モード 2 またはモード 3 を要求したときに、UE のサブスクリプション（優先順位：SMF での UDM またはローカル構成）が SSC モード 1 とモード 2 またはモード 3 を許可する場合、SMF は PDU セッション確立を送信します。 5GSM 原因 68（サポートされていない SSC モード）および許可された SSC モード 01 で拒否します。この方法を使用すると、UE は SSC mode-1 での再試行が可能になります。3GPP TS 24.501 に従い、要求された SSC モードがサブスクリプションでサポートされていない場合は、5GSM 原因 68 が送信されます。

PDU セッションの確立を優先するために、SMF は UDM サブスクリプションまたはローカル構成のいずれかで SSC モードになることを想定しています。SMF に UDM サブスクリプションまたはローカル構成の一部として SSC モードがない場合、SMF は 5GSM 原因 31（要求が拒否され、未指定）で PDU セッション確立を拒否します。

# SSC モードの構成

DNN プロファイルでセッションおよびサービス継続モードのパラメータを構成するには、次の構成例を使用します。

```
config
   profile dnn dnn_name
      ssc-mode sscmode_value [ allowed allowed_sscmode_value ]
      exit
```

注：

- **profile dnn** *dnn_name*：DNN プロファイル コンフィギュレーション モードを開始します。
- **ssc-mode** *sscmode_value* **[ allowed** *allowed_sscmode_value* **]**：SSC モード パラメータを構成します。
  - **ssc-mode** *sscmode_value*：デフォルトの SSC モードを指定します。 *sscmode_value* は、1 ～ 3 の範囲の整数である必要があります。

    SMF は、SSC mode-1 のみをサポートします。
  - **allowed** *allowed_sscmode_value*：許可される SSC モードを指定します。デフォルトの SSC モードに加え、最大 2 つのモードを構成できます。 *allowed_sscmode_value* は 、1 ー 3 の範囲の整数である必要があります。

**allowed** コマンドで定義された SSC モード値とともに UE が送信される場合、これらの値は、DNN プロファイルでサポートされるデフォルトの SSC モードとともにサポートされます。

- **no ssc-mode**：このコマンドを指定すると、DNN プロファイルから SSC モードを削除できます。
- UE が SSC モード 2 またはモード 3 を要求したときに、UE のサブスクリプション（優先順位：SMF での UDM またはローカル構成）が SSC モード 1 とモード 2 またはモード 3 を許可する場合、SMF は PDU セッション確立を送信します。 5GSM 原因 68（サポートされていない SSC モード）および許可された SSC モード 01 で拒否します。この方法を使用すると、UE は SSC mode-1 での再試行が可能になります。3GPP TS 24.501 に従い、要求された SSC モードがサブスクリプションでサポートされていない場合は、5GSM 原因 68 が送信されます。

  PDU セッションの確立を優先するために、SMF は UDM サブスクリプションまたはローカル構成のいずれかで SSC モードになることを想定しています。SMF に UDM サブスクリプションまたはローカル構成の一部として SSC モードがない場合、SMF は 5GSM 原因 31（要求が拒否され、未指定）で PDU セッション確立を拒否します。

第 40 章

# セッション タイマー


- 機能の概要と変更履歴, on page 1737
- 機能説明 （1738 ページ）
- 3GPP 準拠タイマー （1739 ページ）
- 非 3GPP 準拠タイマー （1752 ページ）


## 機能の概要と変更履歴

### 要約データ

***Table 471:*** 要約データ

| | |
|---|---|
| 該当製品または機能エリア | SMF |
| 該当プラットフォーム | SMI |
| 機能のデフォルト設定 | 無効：設定が必要 |
| このリリースでの関連する変更点 | N/A |
| 関連資料 | 該当なし |

### 更新履歴

***Table 472:*** マニュアルの変更履歴

| 改訂の詳細 | リリース |
|---|---|
| セッション アイドル タイマーのサポートが追加されました。 | 2023.03.0 |

| 改訂の詳細 | リリース |
| --- | --- |
| セッション セットアップ タイマーとバックオフ タイマーのサポートが追加されました。 | 2021.02.0 |
| 最初の導入。 | 2020.02.0 |

# 機能説明

この章では、タイマーの機能、動作、および構成について詳しく説明します。

SMF では、セッション タイマーまたは非 3GPP セッション イマーのいずれかの構成可能なタイマーがサポートされます。

- 非 3GPP セッション タイマー
  - 絶対タイマー
  - コントロール プレーン非アクティブ タイマー
  - ユーザー プレーン非アクティブ タイマー
  - セッション セットアップ タイマー
- 3GPP セッション タイマー
  - GTP タイマー
  - N11 タイマー
  - バックオフ タイマー
  - デフォルトのフロー専用タイマー
  - EPS フォールバック ガード タイマー
  - 間接データ転送トンネル タイマー
  - 専用ベアラー遅延および再試行タイマー
  - 専用ベアラー手順の失敗処理タイマー
  - 手順 SLA タイマー
  - ダイナミック構成変更サポートタイマー
  - IPAM 検疫タイマー
  - ポリシー再検証タイマーのプロビジョニング
  - ルータ アドバタイズメント パラメータ タイマー

GTP および N11 以外のタイマーの詳細については、次のセクションを参照してください。

• EPS フォールバック ガード タイマーのサポート （244 ページ）
• 間接データ転送トンネル（IDFT）タイマーのサポート （238 ページ）
• 専用ベアラの作成に対する遅延および再試行のサポート （301 ページ）
• IPAM 隔離タイマー（IPAM Quarantine Timer） （939 ページ）
• ポリシー再検証時間のプロビジョニング （1287 ページ）
• ルータ アドバタイズメントのパラメータの構成 （1008 ページ）

# 3GPP 準拠タイマー

## GTP および N11 タイマー

### 機能説明

SMF は GTP タイマーおよび N11 タイマーを介した再送信をサポートしています。このプロビジョニングにより、ピアがタイマー値で応答しない場合、SMF は GTP 要求と N11 要求を再送信します。最大再送信回数を構成します。

### 機能の仕組み

SMF は、次の 3GPP タイマーをサポートしています：

#### GTP 再送信タイマー

SMF または PGW-C が、T3-RESPONSE で示されるタイマーを開始します。このタイマーは、応答が期待されるシグナリング メッセージが送信されたときに呼び出されます。T3-RESPONSE タイマーが期限切れになる前に応答を受信しなかった場合、シグナリング メッセージまたはトリガーされたメッセージが失われる可能性があります。

T3-RESPONSE タイマーが期限切れになった後、再試行の合計回数が N3REQUESTS よりも少ない場合、T3-RESPONSE タイマーに対応するメッセージが再送信されます。

#### 5G N1N2 再試行タイマー

AMF が「一時的な登録拒否」または「一時的な拒否のハンドオーバー継続」の原因コードで N1N2 MessageTransfer を拒否した場合、SMF は N1N2 MessageTransfer を再試行するためのタイマーを開始します。

タイマーが期限切れになると、設定された再試行回数に基づいて N1N2 MessageTransfer に対応するメッセージが再試行されます。

# 標準準拠

3GPP サポート機能は、以下の基準に準拠しています：

- *3GPP TS 29.510 V15.2.0*（*2018-12*）*-5G 5G* システムネットワーク機能リポジトリ サービス 第 *3* 段階

# N11 タイマーおよび GTP タイマーの構成

このセクションでは、3GPP 準拠のタイマー（N11 タイマーおよび GTP タイマー）の構成方法について説明します。

## N11 タイマーの構成

N11 タイマーの構成は、AMF が「Temporary reject registrationp on」または「Temporary reject handover on」原因コードで N1N2 メッセージ転送を拒否するときに呼び出されます。次に、SMF はタイマーを考慮して、メッセージの転送を再試行します。タイマーが期限切れになると、構成された再試行回数に基づいて転送が再試行されます。

N11 タイマーを構成するには、次の構成例を使用します：

```
config
  profile failure-handling failure_handling_name
     interface [ gtpc | N11 ] message message_type
       cause-code [ temp-reject-register | temp-reject-handover ]
          action [ retry { timeout timeout_duration |
          max-retry retry_count } | clear | terminate ]
          end
```

注：

- **profile failure-handling** *failure_handling_name*：障害処理用のプロファイルの名前を入力します。
- **interface [ gtpc | N11 ]** ：メッセージ転送が行われるインターフェイスを構成します。
- **message** *message_type*：そのインターフェイスを介して転送するメッセージの種類を構成します。N11 インターフェイスは、N1N2Transfer としてメッセージ タイプをサポートします。
- **cause-code [ temp-reject-register | temp-reject-handover ]** ：HTTP 原因コードを構成します。1 つのメッセージに対して複数の原因コード値を構成できます。
- **action [ retry | clear | terminate ]**：メッセージ転送が失敗した場合に実行するアクションを構成します。
- **action [ retry { max-retry** *retry_count* **| timeout** *timeout_duration* **}** ：メッセージ転送の必要再試行回数と連続試行の間隔を指定します。

設定例

N11 タイマーの構成例を次に示します。

```
show running-config
profile failure-handling n11-fht
  interface n11 message n1n2transfer
    cause-code temp-reject-register
     action retry
       timeout 1000
         max-retry 2
```

### GTP タイマーの構成

GTP タイマーの構成は、応答が期待されるシグナリング メッセージまたはトリガーされたメッセージが、T3-RESPONSE タイマーの期限切れ前に応答を取得しなかったために失われた場合に導入されます。T3-RESPONSE タイマーが期限切れになった後、再試行の合計回数が N3-REQUESTS よりも少ない場合、T3-RESPONSE タイマーに対応するメッセージが再送信されます。

GTP タイマーを構成するには、次の構成例を使用します：

```
config
   instance instance-id gr_instance_id
      endpoint gtp
         retransmission { max-retry retry_count | timeout timeout_duration }
         end
```

注：

- **endpoint gtp**：GTP 再送信構成を入力します。
- **max-retry** *retry_count*：SMF へのシグナリング メッセージ要求を再試行する必要がある回数を指定します。指定できる範囲は 0 ～ 5 です。デフォルトの範囲は 3 です。 *retry_count* が「0」に設定されている場合、再送信機能は無効になります。
- **timeout** *timeout_duration*：GTP 再送信要求が再試行されるまでの時間間隔（ミリ秒単位）を設定します。指定できる範囲は 0 ～ 10 です。デフォルトの範囲は 2 です。 *timeout_duration* が「0」に設定されている場合は、再送信機能が無効になります。

設定例

次に、GTP タイマーの構成例を示します。

```
show running-config
instance instance-id 1
  endpoint gtp
   retransmission max-retry 2 timeout 5
```

# バックオフ タイマー サポート

## 機能説明

SMF は、ネットワークによって開始されたリリース後に再登録と新しい接続の試行を待機するように UE に通知する、構成可能なバックオフ タイマーをサポートしています。このタイマーは、システムを障害からの回復を支援します。

SMF は、次のシナリオで構成されたバックオフタイマー値を AMF に送信します：

- UPF スイッチオーバー中の N4 パス障害
- IP アドレスの枯渇

**重要** これらのシナリオは現在 、ホームルーティング ローミング セッションと 非ローミング セッションでのみサポートされています。

SMF は、IP アドレスの枯渇時にのみ、バックオフタイマー値を S-GW に送信します。

（注） バックオフ タイマーのサポートは、4G非ローミングセッションと5Gローミングおよび非ローミング セッションにのみ適用されます。

UPF が非アクティブであることを SMF が検出すると、N1 を介して送信される PDU セッション リリース コマンド メッセージにバックオフ タイマーと原因値が含められます。その後、SMF は PDU セッションをクリアします。

4G 接続の開始中に IP アドレスが枯渇すると、PGW-C はバックオフ タイマー IE と原因値をセッション作成応答メッセージに含めます。

5G 接続中に IP アドレスが枯渇した場合、SMF は N1 を介して送信される PDU セッション確立拒否メッセージにバックオフタイマー IE と原因値を含めます。

## 機能の仕組み

SMF には、障害条件と原因の値とともにバックオフ タイマー値を構成するオプションがあります。構成の詳細は、このガイドのバックオフ タイマーの構成 （1749 ページ） セクションを参照してください。

SMF は、N4 パス障害が原因で UPF がダウンしているかどうかを検出します。UPF がダウンしている場合、SMF は PDU セッションのクリア中に、N1 PDU セッション リリース コマンドに構成されたバックオフ タイマー値と原因値を含めます。

ホームルーティング ローミングのシナリオでは、vSMF は、次の条件のいずれかが満たされた場合に N1 を介して送信される PDU セッション リリース コマンド メッセージに、バックオフ タイマーと原因値を含めます。

- hSMF は、パス障害が原因で hUPF が非アクティブであることを検出します。
- vSMF は、パス障害が原因で vUPF が非アクティブであることを検出します。

SMF または PGW-C が IP アドレスが使い果たされたことを検出すると、SMF は RAT タイプに応じて、N1 PDU セッション確立拒否メッセージまたはセッション応答の作成メッセージにバックオフ タイマーと原因値を挿入します。

ローミング シナリオで、IP アドレスが使い果たされたことを hSMF が検出すると、バックオフ タイマーと原因値とともに PDU セッション作成エラーを vSMF に送信します。この値に基

づいて、vSMF は N1 PDU セッション確立拒否メッセージにバックオフ タイマーと原因値を含めます。

（注） PDU リリースコマンドおよび PDU 確立拒否におけるバックオフ タイマーのエンコーディングは 、*3GPP TS 24.008*（モバイル無線インターフェイスレイヤ *3* 仕様）コア ネットワーク プロトコル、ステージ *3* で定義されています。

セッション応答の作成でのバックオフ タイマーのエンコードは、*3GPP TS 29.274—3GPP* 進化型パケット システム（*EPS*）。コントロール プレーン用進化型一般パケット無線サービス（*GPRS*）トンネル プロトコル（*GTPv2-C*）、ステージ *3* に定義されているとおりです。

## コール フロー

このセクションでは、この機能のコール フローについて説明します。

### *N4* パス 障害処理コール フロー

ここでは、SMF が 非ローミングおよびローミングのシナリオで確認できるN4 パス障害を処理する方法について説明します。

#### 非ローミング セッションでの N4 パス障害の処理

次の図は 、非ローミング セッションの N4 パス障害処理コール フローを示しています。

**図 *279*：非ローミング セッションの *N4* パス障害処理コール フロー**

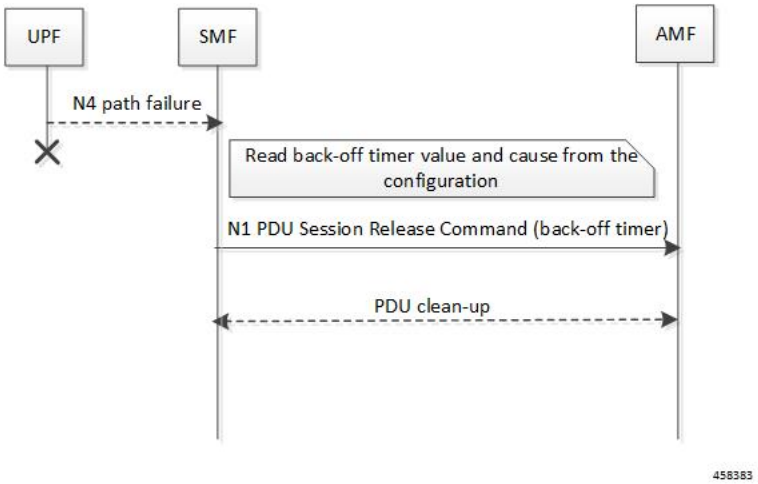



**表 *473*：非ローミング セッションの *N4* パス障害処理コール フローの説明**

| ステップ | 説明 |
|---|---|
| 1 | SMF は、N4 パス障害が原因で UPF が非アクティブであるかどうかを確認します。 |

| ステップ | 説明 |
|---|---|
| 2 | UPF が非アクティブであることを SMF が検出すると、バックオフ タイマーと原因値を DNN プロファイル構成から取得します。SMF は、N1 PDU セッション リリース コマンドのタイマーと原因の値を AMF に送信します。その後、SMF は PDU のクリーンアップを実行します。 |

### ローミング セッション中の vUPF での N4 パス障害の処理

次の図は、ローミング セッション中に vUPF で N4 パス障害を処理するコール フローを示しています。

図 *280 :* ローミング セッションの *vUPF* パス障害処理コール フロー

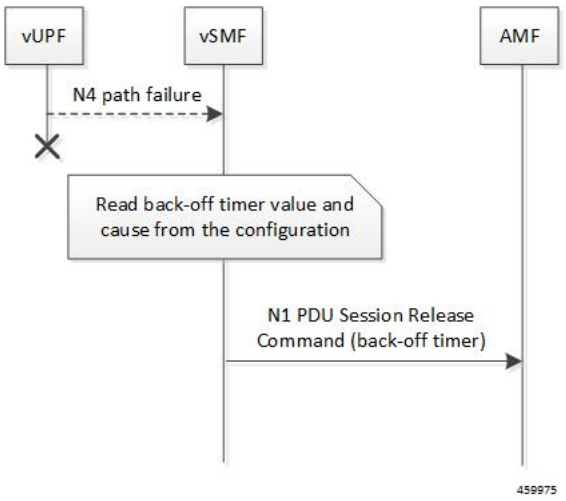



表 *474 :* ローミング セッションの *vUPF* パス障害処理コール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | vSMF は、N4 パス障害が原因で vUPF が非アクティブであるかどうかを確認します。 |
| 2 | vUPF が非アクティブであることを vSMF が検出すると、バックオフ タイマーの値と原因を DNN プロファイル構成から取得します。vSMF は、N1 PDU セッション リリース コマンドのタイマーと原因値を AMF に送信します。次に、vSMF が PDU のクリーンアップを実行します。 |

### ローミング セッション中の hUPF での N4 パス障害の処理

次の図は、ローミング セッション中に hUPF で N4 パス障害を処理するコール フローを示しています。

図 *281* : ローミング セッションの *hUPF* パス障害処理コール フロー

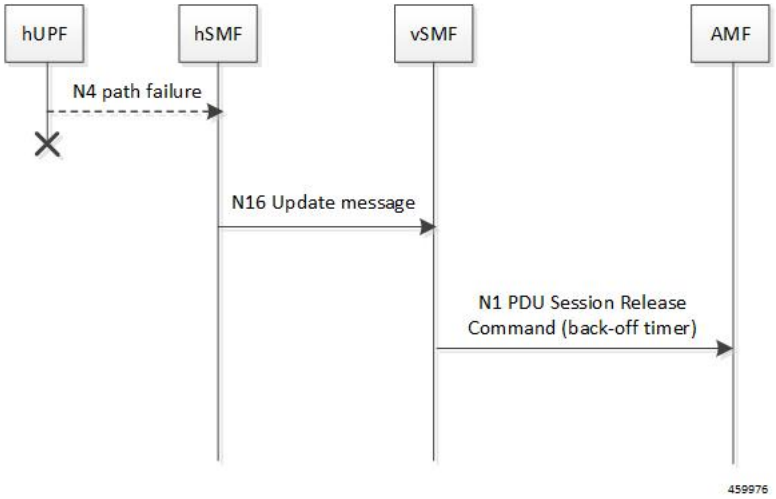



表 *475* : ローミング セッションの *hUPF* パス障害処理コール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | hSMF は、hUPF が N4 パス障害により非アクティブであるかどうかを確認します。 |
| 2 | hUPF が非アクティブの場合、hSMF は N16 更新要求を通じて、バックオフ タイマーと原因を vSMF に送信します。 |
| 3 | vSMF は、N1 PDU セッション リリース コマンド メッセージにバックオフ タイマーと原因値を含めます。 |

## *5G* セッションの *IP* アドレス枯渇処理コール フロー

このセクションでは、SMF が 5G セッションで IP アドレスが枯渇した場合の処理方法について説明します。

### 5G 非ローミング セッションでの IP アドレス枯渇の処理

次の図は、5G非ローミング セッションの IP アドレスの枯渇コールの処理フローを示しています。

図 *282 : 5G* 非ローミング セッションの *IP* アドレス枯渇処理コール フロー

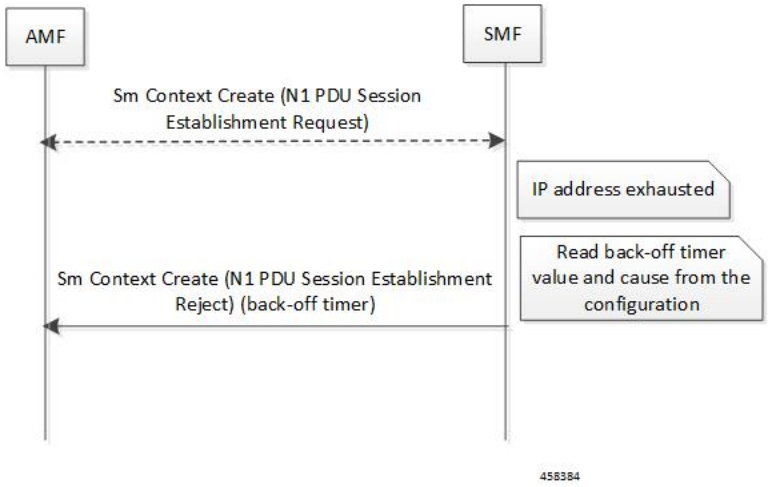



表 *476 : 5G* 非ローミング セッションの *IP* アドレス枯渇処理コール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | AMF は、N1 PDU セッション確立要求の SM コンテキスト作成メッセージを SMF に送信します。 |
| 2 | 5G 非ローミング コールで IP アドレスの枯渇が検出されると、SMF は構成されたバックオフ タイマーと原因値を読み取ります。次に、SMF は、N1 PDU セッション確立拒否メッセージでこのタイマーと原因値を AMF に送信します。 |

### 5G ローミング セッションでの IP アドレス枯渇の処理

次の図は、5G ローミング セッションの IP アドレスの枯渇コールの処理フローを示しています。

図 *283 : 5G* ローミング セッションの *IP* アドレス枯渇処理コール フロー

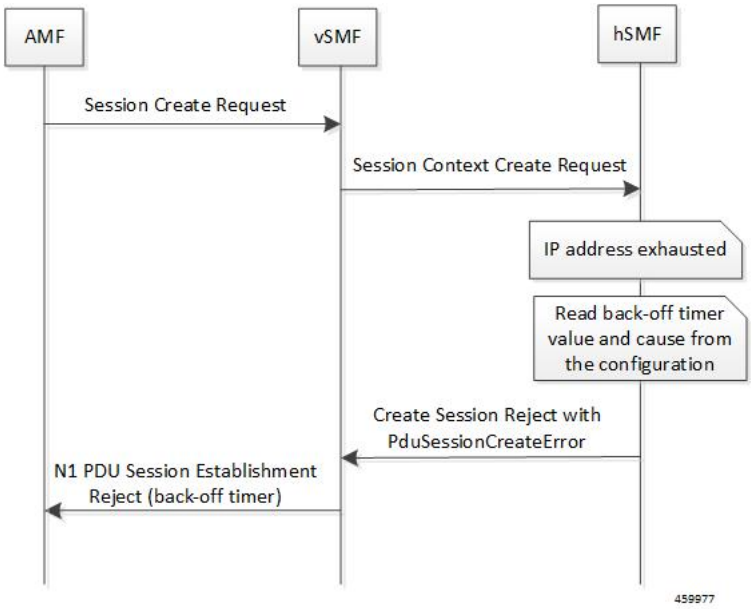



表 *477 : 5G* ローミング セッションの *IP* アドレス枯渇処理コール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | AMF は、N1 PDU セッション確立要求の SM コンテキスト作成メッセージを vSMF に送信します。 |
| 2 | vSMF は、セッション コンテキスト作成要求メッセージを hSMF に送信します。 |
| 3 | IP アドレスが使い果たされたことを hSMF が検出すると、hSMF の設定に基づいて、バックオフ タイマーと原因値とともに PduSessionCreateError を vSMF に送信します。<br>この値に基づいて、vSMF は N1 PDU セッション確立拒否メッセージにバックオフ タイマーと原因値を含めます。 |

## *4G* セッションの *IP* アドレス枯渇処理コール フロー

このセクションでは、SMF が 4G セッションで IP アドレスが枯渇した場合の処理方法について説明します。

次の図は、4G セッションの IP アドレスの枯渇コールの処理フローを示しています。

図 *284 : 4G* セッションの *IP* アドレス枯渇処理コール フロー

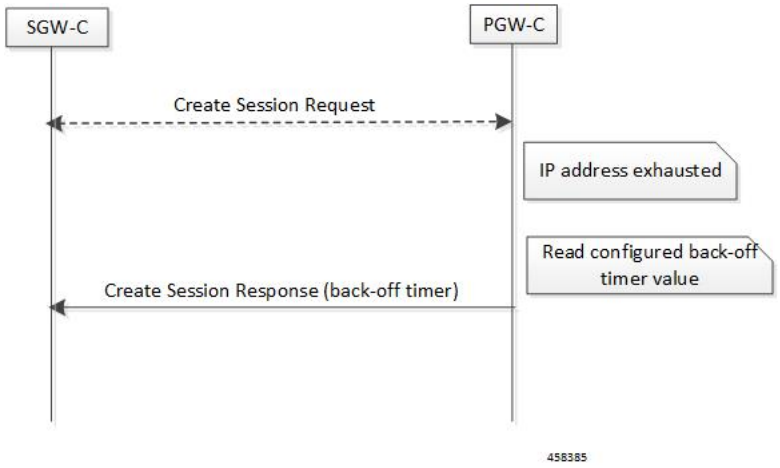



表 *478 : 4G* セッションの *IP* アドレス枯渇処理コール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | SGW-C は、PGW-C にセッション要求の作成を送信します。 |
| 2 | 4G コールで IP アドレスの枯渇が検出されると、PGW-C は構成されたバックオフ タイマー値と原因を読み取ります。次に、PGW-C は、セッション応答の作成メッセージでこのタイマー値と原因を SGW-C に送信します。 |

### 制限事項

この機能には、次の制限があります：

- 3GPP 29.274 仕様では削除されたベアラー要求メッセージでバックオフ タイマー IE がサポートされていないため、4G PDN セッションのクリア中はバックオフ タイマーのトリガはサポートされません。

（注） 前述の制限は、非ローミング シナリオにのみ適用されます。

## 標準準拠

バックオフ タイマー サポート機能は、以下の基準に準拠しています。

- *3GPP 29.274*、バージョン *15.9.0*、リリース *15*：ユニバーサル モバイル テレコミュニケーション システム（*UMTS*）*LTE 3GPP* 進化型パケット システム（*EPS*）進化型一般パケット無線サービス（*GPRS*）コントロール プレーンのトンネリング プロトコル（*GTPv2-C*）第 *3* 段階

- *3GPP 24.008*、バージョン *15.9.0*、リリース *15*：デジタル セルラー通信システム（フェーズ *2+*）（*GSM*）ユニバーサル モバイル テレコミュニケーション システム（*UMTS*） *LTE 5G* モバイル ラジオ インターフェイスのレイヤ *3* 仕様。コア ネットワーク プロトコル第 *3* 段階
- *3GPP 24.501*、バージョン *15.6.0*、リリース *15-5G 5G* システム（*5GS*）用の *Non-Access Stratum*（*NAS*）プロトコル第 *3* 段階
- *3GPP TS 29.502*、バージョン *15.6.0*、リリース *15-5G* セッション管理サービス第 *3* 段階

## バックオフ タイマーの構成

このセクションでは、バックオフ タイマーの構成方法について説明します。

このバックオフ タイマーの構成には、次の手順が含まれます：

- DNN プロファイルでのバックオフ タイマーとジッター タイマーの構成 （1749 ページ）
- メッセージレベル バックオフ タイマーの有効化 （1750 ページ）

（注） この機能は、バックオフタイマーと原因の両方が構成されている場合にのみ機能します。バックオフ タイマーの構成は、非ローミング コールとローミング コールの両方で同じままです。

### DNN プロファイルでのバックオフ タイマーとジッター タイマーの構成

DNN プロファイルでバックオフ タイマーとジッター タイマーの値を定義するには、次の設定例を使用します。

```
config
   profile dnn dnn_profile_name
      timeout backoff backoff_timer_value
      timeout jitter jitter_timer_value
      end
```

注：

- **timeout backoff** *backoff_timer_value*：バックオフタイマーの値（秒単位）を指定します。*backoff_timer_value* は 0 ～ 576000 の範囲の整数である必要があります。

  バックオフ タイマーは、IP の枯渇および N4 パスの障害発生時に使用される最大許容期間です。

- **timeout jitter** *jitter_timer_value*：バックオフ タイマー値にランダム性を導入するジッター値を指定します。 *jitter_timer_value* は 0 ～ 1000 の範囲の整数である必要があります。

  ジッターを使用すると、UE デバイスに異なるバックオフ タイマーを分散させて、次の再接続を試みる前に、すべてのデバイスが異なる時間に待機するようにできます。

  この設定は、バックオフ タイマーの期限切れ後のセッション ストームを防ぐのに役立ちます。

以下は、N4 パス障害のシナリオ中に使用される構成例です。

```
config
   profile dnn test
      timeout backoff 200 jitter 50
      end
```

## メッセージレベル バックオフ タイマーの有効化

次の構成例を使用して、GTP-C および N1 メッセージ レベルでバックオフ タイマーを有効にします。

```
config
   profile access access_profile_name
     gtpc message-handling create-session-response condition ip-exhaust
 action backoff cause cause_code_value
      n1 message-handling pdu-session-release condition n4-pathfail
action backoff cause cause_code_value
     n1 message-handling pdu-session-establishment condition ip-exhaust
 action backoff cause cause_code_value
      n1 message-handling pdu-modify condition self-protection action
backoff cause cause_code_value
     n1 message-handling pdu-establishment condition self-protection
action backoff cause cause_code_value
      end
```

注：

- **gtpc message-handling create-session-response condition ip-exhaust action backoff cause** *cause_code_value*：このコマンドを使用して、セッション応答作成（CSR）メッセージの GTP-C インターフェイス レベルでバックオフ タイマーを有効にします。つまり、CSR メッセージには、IP アドレスの枯渇時のバックオフタイマー IE とその原因コードが含まれます。
- **n1 message-handling pdu-session-release condition n4-pathfail action backoff cause** *cause_code_value*：このコマンドを使用して、PDU セッション リリース メッセージの N1 インターフェイス レベルでバックオフ タイマーを有効にします。つまり、PDU セッション リリース メッセージには、N4 パス障害が発生した場合のバックオフ タイマー IE とその原因コードが含まれます。
- **n1 message-handling pdu-session-establishment condition ip-exhaust action backoff cause** *cause_code_value*：このコマンドを使用して、PDU セッション確立メッセージの N1 インターフェイス レベルでバックオフ タイマーを有効にします。つまり、PDU セッション確立メッセージには、IP アドレスの枯渇時のバックオフ タイマー IE とその原因コードが含まれます。
- **n1 message-handling pdu-modify condition self-protection action backoff cause** *cause_code_value*：このコマンドを使用して、自己保護状態の間に PDU セッション変更メッセージの N1 インターフェイス レベルでバックオフ タイマーを有効にします。つまり、PDU セッション変更メッセージには、IP アドレスの枯渇時のバックオフ タイマー IE とその原因コードが含まれます。

- **n1 message-handling pdu-establishment condition self-protection action backoff cause** *cause_code_value*：このコマンドを使用して、自己保護状態の間に PDU セッション確立メッセージの N1 インターフェイス レベルでバックオフ タイマーを有効にします。つまり、PDU セッション確立メッセージには、IP アドレスの枯渇時のバックオフ タイマー IE とその原因コードが含まれます。

以下は、4G 接続および IP アドレスの枯渇中に使用される構成例です。

```
config
   profile access access1
     gtpc message-handling create-session-response condition ip-exhaust
 action backoff cause 73
      end
```

このシナリオでは、接続が失敗し、CSR がバックオフ タイマー IE と原因 73 で送信されます。

以下は、5G 接続および IP アドレスの枯渇中に使用される構成例です。

```
config
   profile access access1
     n1 message-handling pdu-establishment condition ip-exhaust action
 backoff cause 26
      end
```

このシナリオでは、接続が失敗し、PDUセッション確立がバックオフ タイマーおよび原因コード値が 26 に設定されて送信されます。

以下は、5G 接続および N4 パス障害のシナリオ中に使用される構成例です。

```
config
   profile access access1
      n1 message-handling pdu-session-release condition n4-pathfail
action backoff cause 26
      end
```

このシナリオでは、サブスクライバのクリアが内部的にトリガされ、PDU セッション リリース コマンドがバックオフ タイマー IE と原因 26 で送信されます。

## バックオフ タイマー構成の確認

このセクションでは、バックオフ タイマー構成を確認する方法について説明します。

**show running-config** コマンドを使用して、機能構成を確認します。

**show running-config profile access access1** コマンドの出力例を次に示します。

```
[unknown] smf# show running-config profile access access1
profile access access1
n1 message-handling pdu-establishment condition ip-exhaust action backoff cause 26
n1 message-handling pdu-release condition n4-pathfail action backoff cause 26
n26 idft enable timeout 15
n2 idft enable timeout 15
gtpc gtpc-failure-profile gtp1
gtpc message-handling create-session-response condition ip-exhaust action backoff cause
 76
exit
```

**show running-config profile dnn intershat** コマンドの出力例を次に示します。

```
[unknown] smf# show running-config profile dnn intershat
profile dnn intershat
network-element-profiles chf chf1
network-element-profiles amf amf1
network-element-profiles pcf pcf1
network-element-profiles udm udm1
timeout backoff 500 jitter 100
charging-profile chgprf1
virtual-mac b6:6d:47:47:47:47
ssc-mode 2 allowed [ 3 ]
session type IPV4 allowed [ IPV6 IPV4V6 ]
upf apn intershat
dcnr true
exit
```

# 非 3GPP 準拠タイマー

## 機能説明

SMF では、各 PDU セッションの非 3GPP セッション タイマーがサポートされます。ここでは、次のタイマーの機能、動作、および構成に関する詳細について説明します：

- 絶対タイマー
- コントロール プレーンおよびユーザー プレーン アイドル タイマー
- ユーザー プレーン非アクティブ タイマー
- セッション セットアップ タイマー

（注） このセクションは、Diameter インターフェイスを使用する 4G コールにも適用されます。

## 非 3GPP セッション タイマーの構成

DNN プロファイルで非 3GPP セッション タイマーを構成するには、次の構成例を使用します：

```
config
      profile dnn dnnprofile_name
            timeout absolute absolutetimer_value
            timeout { cp-idle timer_value | up-idle timer_value }
            timeout setup timeout_value
            userplane-inactivity-timer timer_value
            end
```

注：

- **timeout absolute** *absolutetimer_value*：システムがセッションを自動的に終了するまでの、セッションの最大継続時間（秒単位）を指定します。
  - デフォルト値は 0 で、機能が無効であることを示します。
  - *absolutetimer_value* は、0 ～ 2147483647 の範囲の整数である必要があります。
  - 絶対セッションタイマーは、セッションの作成中にトリガされます。そのセッションに対するアクセスおよびモビリティ手順の中間処理中に、タイマー値を変更することはできません。
  - タイマーの期限が切れると、SMF はすべての SBI インターフェイスと N4 インターフェイスに通知して、SMF によって開始された解放を実行します。これには、UE、UDM、PCF、CHF、および UPF のインターフェイスが含まれます。
  - レガシーインターフェイスを使用する 4G コールの場合、SMF によって開始されたリリースは、Diameter（Gx および Gy）、GTP、RADIUS、および N4 インターフェイスに通知することで実行されます。
- **timeout cp-idle** *timer_value*：CP アイドル状態への移行後、自動終了までの 4G セッションまたは 5G セッションの最大期間を指定します。
  - デフォルト値は 0 で、機能が無効であることを示します。
  - *timer_value* は 、0 ～ 2147483647 の範囲の整数である必要があります。
- **timeout up-idle** *timer_value*：UP アイドル状態への移行後、自動終了までの 5G セッションの最大期間を指定します。
  - デフォルト値は 0 で、機能が無効であることを示します。
  - *timer_value* は 、0 ～ 2147483647 の範囲の整数である必要があります。
- **cp-idle timer**：4G または 5G の手順の終了時に開始されます。新しい手順が開始されるとタイマーが停止します。タイマーが期限切れになると、SMF はセッションをクリアします。
- **up-idle timer**：AN によって開始されたか、またはネットワークによって開始された 5G セッションがアイドル モードになると開始されます。セッションがアイドル モードを終了するとタイマーは停止します。タイマーの期限切れ時に、SMF は 5G セッションをクリアします。
- **timeout setup** *timeout_value*：セッションのセットアップ タイムアウト値をミリ秒単位で指定します。
  - デフォルト値は、10000 ミリ秒です。
  - *timeout_value* は、5000 ～ 60000 の範囲の整数である必要があります。
  - 構成された時間内にコールが完了しない場合、SMF は作成手順を中止します。リクエストは PDU セッション確立拒否またはセッション拒否の作成を送信します。このタイマーは、4G、5G、および Wi-Fi セッションに適用されます。

- 4G 作成手順では、CSR が最大待機時間を受信すると、手順の SLA タイマーが最大待機時間を設定します。タイムアウト値に応じて、ガードタイマーまたはSLAタイマーのいずれかが最初に期限切れになります。

- **userplane-inactivity-timer** *timer_value*：タイマーの値を秒単位で指定します。
  - タイマーのデフォルト値は 0 で、機能が無効であることを示します。
  - タイマー値は、0 ～ 86400 の範囲の整数である必要があります。
  - SMF は、N4 PDUセッション確立要求を介して、構成された非アクティブ タイマーを UPF に送信します。セッションの確立後、構成値が変更されると、SMF は N4 変更要求を介して UPF の変更を報告します。
  - N3 /S5-U トンネルを介したアップリンクまたはダウンリンクのデータ送信がない場合、UPF は非アクティブ タイマーを開始します。N3 /S5-U トンネルを介したデータ送信が再開されると、タイマーが停止します。
  - タイマーの期限切れ時に、UPF は、ユーザー プレーン非アクティブ要求（UPIR）フラグをセットしてセッション レポートを SMF に送信します。
  - セッションのレポート通知を受信した後、SMF は 4G セッションの場合はセッションをクリアし、5G セッションの場合はアイドル モードの開始を開始します。

（注） **userplane-inactivity-timer** パラメータがそれぞれのDNNで無効になっている場合にのみ、5G コールの **always-on** パラメータを有効にします。

このパラメータを無効にするには、 **always-on** の値を *false* に構成します。

## 設定例

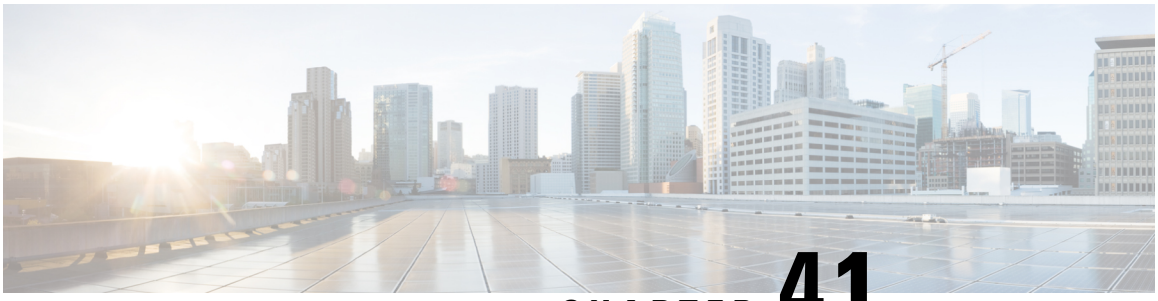
次に、設定例を示します。

```
smf(config)# profile dnn intershat timeout absolute 900
```

## 設定の確認

設定を確認するには、次のコマンドを実行します。

```
show running-config
 profile dnn intershat
 timeout absolute 900
 exit
```



CHAPTER 41

# 統合された SMF による複数世代のデバイス サポートの管理


- 機能の概要と変更履歴, on page 1755
- 機能説明, on page 1756
- 機能の仕組み, on page 1758
- 4G および 5G デバイスをサポートするためのパラメータの構成, on page 1760
- OAM サポート, on page 1764
- トラブルシューティング情報 （1768 ページ）
- SMF における 2G および 3G ネットワーク統合 （1772 ページ）


## 機能の概要と変更履歴

### 要約データ

***Table 479:*** 要約データ

| | |
|---|---|
| 該当製品または機能エリア | SMF |
| 該当プラットフォーム | SMI |
| 機能のデフォルト設定 | 有効：構成が必要 |
| このリリースでの関連する変更点 | N/A |
| 関連資料 | 該当なし |

# 更新履歴

*Table 480:* マニュアルの変更履歴

| 改訂の詳細 | リリース |
|---|---|
| 定期的な二次 RAT 使用データ報告は、MME 経由で S5/S8 インターフェースを介し、Modify-Bearer-Request、Delete-Session-Request、Delete-Bearer-Response、および Change-Notification-Request においてサポートされています。 | 2023.04.0 |
| レガシー インターフェイスを使用した SMF の拡張 QoS サポートが追加されました。 | 2023.02.0 |
| 4G-UE およびオプション 3x 機能のフェーズ 2 サポートには、以下が含まれます。<br>• DCNR ベースの UPF の選択<br>• S-GW/MME からのセカンダリ RAT データ使用状況レポートの処理と CHF へのリレー<br>• UE プレゼンス レポート<br>• 4G から 3G へのハンドオーバーのための GTPV1 メッセージの処理<br>• 4G および Wi-Fi ハンドオーバーへの SUPI + IP セッションとアフィニティ キー<br>• 4G 専用 UE での 5G QoS の送信の回避<br>• S-GW/MME からの 5GCNRS および 5GCNRI 通知フラグの処理 | 2021.01.0 |
| 最初の導入。 | 2020.03.0 |

# 機能説明

**Important** この章で使用されている PGW-C という用語は、SMF によってサポートされている EPS インターワーキング機能を意味しており、LTE ネットワークで使用されるスタンドアロン P-GW として想定してはなりません。

デュアル接続が有効になっている UE は、4G LTE と 5G NR をサポートします。このような UE は、4G コアネットワークに信号を送信して、デュアル接続対応デバイスであることを示します。

デュアル接続新規無線（DCNR）対応 UE が MME に登録しようとすると、MME はセッション作成要求メッセージで DCNR フラグを 1 に設定した「UP 機能選択表示フラグ」IE を設定します。S-GW は S11 を介してこの IE を受信した後、S5 を介して IE を PGW-C に送信します。この IE 送信は、SGW-C および PGW-C が SGW-U および UPF を選択するのに役立ち、NR とのデュアル接続をサポートします。

SMF および PGW-C は、4G 専用デバイスとオプション 3x 対応デバイス（EPC に接続された NR および LTE 無線）の両方からのパケット データ ユニット（PDU）セッションをサポートします。

SMF は、以下の機能と機能性をサポートします。

- DCNR ベースの UPF の選択, on page 1757
- セカンダリ RAT データ使用状況レポート, on page 1757
- #unique_2212 unique_2212_Connect_42_section_adw_rlv_5pb
- 4G から 2G または 3G へのハンドオーバー, on page 1758
- レガシーのインターフェイスでのサポート
- 4G から Wi-Fi ハンドオーバーへの SUPI + IP セッションとアフィニティ キー
- 4G 専用 UE での 5G QoS の送信の回避（QoS ルールと QoS フローの説明）
- S-GW および MME からの 5GCNRS および 5GCNRI 通知フラグの処理

### DCNR ベースの UPF の選択

DCNR がクエリ パラメータで構成されている場合、SMF は DCNR 対応セッションに対して DCNR がサポートする UPF を選択します。DCNR は、UPF 選択の必須クエリ パラメータではありません。UPF グループ プロファイルで DCNR を構成できます。

詳細については、「ポリシーとユーザープレーンの管理」 の章の「*UPF* ノードの選択」 セクションを参照してください。

### セカンダリ RAT データ使用状況レポート

SMF と UPF は、eNB の通信量を追跡して、NSA デバイスの NR 通信量と LTE 通信量を区別します。SMF は、S5 インターフェイスでさまざまなメッセージで使用状況データ ポートを受信し、CHF に対して使用状況を報告します。

SMF は、Intended Receiver PGW-C（IPGW）フラグに基づいて、ベアラー要求の変更、セッション要求の削除、ベアラー応答の削除、およびベアラー コマンドの削除で S5 または S8 インターフェイスを介して MME から定期的なセカンダリ RAT 使用状況データ レポートを処理します。SMF は、IRGW = 1 の場合に使用状況レポートを保持します。

SMF は、Secondary RAT Usage Data レポート IE の複数のインスタンスをサポートしています。トリガーに基づいて CHF に送信されるまで、レポートを保存します。SMF は、課金トリガーのいずれかが満たされると、保存されているセカンダリ RAT 使用量データ レポートを gtpp-ep エンドポイントを介して送信します。課金プロファイルで、保存されるセカンダリ RAT 使用レポートの最大数を構成できます。SMF は、オフライン使用状況レポートが原因で CDR が閉じられた場合、保存されているセカンダリ RAT 使用状況データ レポートをオフライン使用状況レポートとともに送信します。

### [Presence Reporting] エリア

Presence Reporting Area（PRA）は、ポリシー制御や課金理由でエリア内の UE プレゼンスをレポートするために、3GPP パケット ドメイン内で定義されるエリアです。E-UTRAN の場合、PRA はネイバーまたは非ネイバーのトラッキング エリア、eNB、および/またはセルのセットで構成されます。DNN プロファイルで PRA 機能を有効にできます。

MME プールに適用される Presence Reporting Area には、UE 専用の Presence Reporting Area とコア ネットワークの事前構成された Presence Reporting Area の 2 種類があります。SMF はコア ネットワークの事前設定済み PRA をサポートしています。

### 4G から 2G または 3G へのハンドオーバー

4G から 2G または 3G へのハンドオーバー中に、SMF は GTPv1 メッセージ要求を拒否し、中断のないサービスの継続性を確保するために 2G または 3G との再接続を行います。SMF が要求をドロップすると、ハンドオーバーの失敗とその後の 2G または 3G への接続が遅延します。

### レガシーのインターフェイスでの拡張 QoS サポート

DCNR が有効な 4G デバイスがレガシー インターフェイスを使用して SMF に接続し、Extended-BW-NR 機能が PCRF とネゴシエートされると、SMF は 4.2 Gbps を超える APN-AMBR 値を拡張ビットレートで PCRF に送信します。 AVP。

SMF が S-GW からの GTP-v2 メッセージで 4.2 Gbps を超える APN-AMBR 値を受信し、DCNR 機能が有効になっていない場合、SMF は APN-AMBR 値を 4.2 Gbps に制限します。

SMF が PCRF から拡張 QoS 値を受信し、セッションが DCNR 対応でない場合、SMF は APN-AMBR 値を 4.2 Gbps に制限します。

# 機能の仕組み

SMF は、4G 専用 UE からセッション作成要求を受信すると、PDU セッション ID（pdu-session-id）を生成します。SMF では、プロトコル構成オプションで PDU セッション ID を指定せずに、要求に EPS インターワーキング指示があるかどうかを検証します。UDM は、DNN ごとに SMF にインターワーキングの指示を提供します。SMF は、この表示を使用して UE が 5G に対応できるかどうかを判断しません。

SMF は、リンクされた EPS ベアラー ID（LBI）に基づいて pdu-session-id を生成します。4G セッションの場合、pdu-session-id は LBI+64 で、Wi-Fi セッションの場合、pdu-session-id は LBI+80 です。

SMF では、プロファイル DNN の下でデフォルト NSSAI を構成できます。NSSAI は、4G 専用 UE からのセッション作成時に PCF にポリシー作成要求で送信される sliceInfo IE の一部です。デフォルト スライスが構成されていない場合、SMF は構成されたスライスの 1 つを選択します。

UE が DCNR に対応していて、DCNR がセッションで有効になっている場合、SMF は UE がデュアル接続をサポートできると見なします。DNN および UPF などのその他の NF ごとに DCNR を構成できます。S-GW は、UPF 選択表示フラグ IE を介して、DCNR のサポートを PGW-C に通知します。

# 標準準拠

オプション 3x および 4G 専用デバイス機能は、以下の基準に準拠しています：

- *3GPP TS 23.003 [2]*
- *3GPP TS 24.301 [23]*
- *3GPP TS 29.272 [70]*
- *3GPP TS 29.274*
- *3GPP TS 29.212*

# 制限事項

この機能には、次の制限事項があります。

- 超低遅延 QCI はサポートされていません。
- PRA：
  - PRA は PCF に対してのみサポートされ、CHF に対してはサポートされません。
  - PRA は、デバイス タイプではなく、接続デバイスの RAT タイプにのみ基づいて適用されます。LTE から接続されている場合、4G デバイスと 5G デバイスの両方に適用されます。
  - 1 つの PCF 更新メッセージでは、最大 4 つの PRA-ID が処理されます。PCF アップデートに 4 つ以上の PRA-ID がある場合、他の PRA-ID は無視されます。
  - PRA-ID のみが S5 インターフェイスの「Presence Reporting Area Action」 IE で送信されます。ユーザー ロケーション情報は、送信されません。
  - PRA-ID のみが N7 インターフェイスの「repPraInfos」IE で送信されます。ユーザー ロケーション情報は、送信されません。
  - 「追加の PRA 情報」が S5 および N7 インターフェイスでサポートされていないため、PRA セットはサポートされていません。
- セカンダリ RAT データ使用状況レポート：

- S5 インターフェイスではオプション 3 およびオプション 3x（NR セカンダリ RAT）UE のみをサポートします。
- N2 インターフェイスでの E-UTRAN セカンダリ RAT はサポートされません。

# 4G および 5G デバイスをサポートするためのパラメータの構成

このセクションでは、4G および 5G デバイスをサポートする機能を SMF に構成する方法について説明します。

この機能の構成には、次の手順が含まれます。


- NSSAI の構成, on page 1760
- DNN プロファイルでの DCNR の有効化, on page 1761
- UPF 選択の構成, on page 1761
- セカンダリ RAT 使用状況レポートの構成, on page 1762
- プレゼンス レポートの構成, on page 1763


## NSSAI の構成

ここでは、ポリシー作成要求メッセージの sliceInfo IE に含めるデフォルト NSSAI を SMF で構成する方法について説明します。SMF は、4G 専用 UE からのセッション作成中に PCF にこのメッセージを送信します。

SMF でデフォルト NSSAI を構成するには、次の構成例を使用します：

```
config
  profile dnn profile_name
    nssai { sd sd_value | sst sst_value }
    exit
```

注：

- **profile dnn** *profile_name*：DNN プロファイル名を指定します。 *profile_name* は 英数字の文字列である必要があります。
- **nssai { sd** *sd_value* **| sst** *sst_value* **}**：デフォルトの NSSAI を構成します。
  - **sd** *sd_value*：スライス記述子（sd）を指定します。*sd_value* は 6 桁の 16 進文字列（[0-9a-fA-F]{6} - 000000 – ffffff）である必要があります。たとえば、1A2B3c です。
  - **sst** *sst_value*：スライス タイプ（sst）の値を指定します。 *sd_value* は 、0 ～ 255 の範囲の整数である必要があります。

# DNN プロファイルでの DCNR の有効化

SMF が DNN プロファイルを使用して処理されるセッションの DCNR 機能をサポートできるようにするには、次の構成例を使用します：

```
config
   profile dnn profile_name
      dcnr { false | true }
      exit
```

注：

- **profile dnn** *profile_name*：DNN プロファイル名を指定します。 *profile_name* は 英数字の文字列である必要があります。
- **dcnr { false | true }**:
  - **false**：DCNR フラグが false に設定されるように DNN プロファイルを構成します。デフォルトでは、この DCNR 構成は無効になっています。
  - **true**：DCNR フラグが true に設定されるように DNN プロファイルを構成します。

    この構成により、SMF が DCNR 機能をサポートできるようになります。DCNR 機能が有効になっている場合、UE は DCNR フラグを送信してデュアル接続をサポートしていることを示します。

# UPF 選択の構成

ここでは、DCNR フラグを有効にし、DCNR に適切な優先順位を構成する方法について説明します。

### UPF グループの定義

次の構成例を使用して、UPF グループを構成し、UPF グループ プロファイルで DCNR を定義します。

```
config
  profile upf-group profile_name
     dcnr { false | true }
     exit
```

注：

- **profile upf-group** *profile_name*：指定した UPF ネットワーク構成に関連付ける必要がある UPF グループ名を指定します。 *profile_name* は 英数字の文字列である必要があります。
- **dcnr { false | true }**：DCNR 機能を構成します。
  - **false**：DCNR のサポートを無効にします。これがデフォルトの設定です。
  - **true**：DCNR のサポートを有効にします。

### UPF 選択クエリ パラメータの関連付け

次の構成例を使用して、定義された UPF グループを DNN プロファイルの UPF ネットワーク要素に関連付けます。

```
config
  profile dnn profile_name
    upf-selection-policy  upfpolicy_name
    exit
```

注：

- **policy dnn** *profile_name*：DNN プロファイル構成モードを開始します。 *profile_name* は 英数字の文字列である必要があります。
- **upf-selection-policy** *upfpolicy_name*：DNN プロファイルに関連付ける必要がある UPF 選択ポリシーの名前を指定します。 *upfpolicy_name* は英数字の文字列である必要があります。

### DCNR の優先順位の構成

次の構成例を使用して、UPF 選択ポリシー プロファイルで DCNR の適切な優先順位を構成します。

```
config
  policy upf-selection upf_name
    precedence precedence_num
      dcnr
      exit
    exit
```

注：

- **policy upf-selection** *upf_name*：DNN プロファイルに関連付ける必要がある UPF ポリシー名を指定します。 *profile_name* は 英数字の文字列である必要があります。
- **precedence** *precedence_num*：upf ポリシーに precedence 値を割り当てます。 *precedence_num* は 1 ～ 4 の範囲の整数である必要があります。
- **dcnr**：DCNR 機能を構成します。

# セカンダリ RAT 使用状況レポートの構成

CHF に送信される前にセカンダリ RAT 使用レポートを構成するには、次の構成例を使用します。

```
config
  profile charging profile_name
    max-secondary-rat-reports report_range
    exit
```

注：

- **profile charging** *profile_name*：課金プロファイル コンフィギュレーション モードを開始します。
- **max-secondary-rat-reports** *report_range*：GTPP（Gz）またはCHFアップデートをトリガーするセカンダリ RAT 使用状況レポートの最大数を構成します。 *report_range* は 、0 ～ 50 の範囲の整数である必要があります。デフォルト値： 0 。

# プレゼンス レポートの構成

プレゼンス レポートを構成するには、次の構成例を使用します。

```
config
  profile dnn dnnprofile_name
    presence-reporting { false | true }
    exit
```

**注**：

- **profile dnn** *dnnprofile_name*：DNN プロファイル コンフィギュレーション モードを開始します。
- **presence-reporting { false | true }**：DNN のプレゼンス レポートを構成します。
  - **false**：プレゼンス レポートを無効化します。これがデフォルトの設定です。
  - **true**：プレゼンス レポートを有効にします。

# 設定の確認

構成を確認するには、次のコマンドを使用します：

**show subscriber supi** *supi_id* **nf-service smf**

上記の show コマンドの出力で、フィールド「dncr」に関連付けられている値を確認します。このフィールドには、次のいずれかの値が表示されます。

- 有効
- なし
- UE が要求され有効になりました

機能が構成されている場合、「dcnr」フィールドに「有効」と表示されます。

次の構成は、**show subscriber supinf-service smf** コマンドの出力例です：

```
unknown] smf# show subscriber supi imsi-123456789012345 nf-service smf
subscriber-details
{
"subResponses": [
{
"status": true,
"genericInfo": {
```

```
……
},
"sScMode": 1,
"chargEnabled": true,
"uetimeZone": "+00:15+1",
"allocatedIp": "209.165.201.12",
"eUtranLocation": {
"ecgi": {
"mcc": "123",
"mnc": "456",
"eutraCellId": "1234567"
},
"tai": {
"mcc": "123",
"mnc": "456",
"tac": "1820"
}
},
"alwaysOn": "None",
"dcnr": "Enabled",
……
"policySubData": {
 "TotalDynamicRules": 3,
……
Presence Information: "Enabled",
 "praIdList": [  -> list of all enabled PRA IDs
          "8388608",  Status = IN
          "8388618" Status = OUT
        ]
 },
```

# OAM サポート

ここでは、この機能の操作、管理、およびメンテナンスに関して説明します。

## 統計情報サポート

SMF は、DCNR セッション数を収集するために、セッションゲージの「smf_session_counter」および「smf_service_stats」の「dcnr」ラベルを使用します。SMF セッションが DCNR がサポートされている場合、「dcnr」ラベル値が有効になります。ラベルは非 DCNR セッションをサポートしていません。

次に、アクティブな DCNR SMF セッションをカウントするクエリの例を示します。

```
nts{action_type="rejected",app_name="smf",cluster="smf",data_center="unknown",
failure_type="hdr_decode_failure",hdr_decode_fail_reason="",instance_id="0",interface_type="
",message_type="",reject_cause="",service_name="gtpc-ep"} 2

smf_session_counter: sum (smf_session_counters{dcnr_on="enable"}) by (dcnr)

smf_service_stats: sum (smf_session_stats{dcnr_on="enable"}) by (dcnr, status, reason)

smf_session_counters{ presence-reporting ="enable"}) by (presence-reporting)
```

### DCNR セッション カウント

DCNR の場合、セッション数は既存のセッションゲージ「smf_session_counter」の「dcnr」ラベルをサポートします。SMF セッションが DCNR セッションの場合、「dcnr」ラベル値は「enable」になります。それ以外の場合は、DCNR セッションに対して「disable」になります。

次に、DCNR アクティブな SMF セッションをカウントするクエリの例を示します。

```
sum (smf_session_counters{dcnr_on="enable"}) by (dcnr)
```

DCNR 統計の場合、既存の「smf_service_stats」カウンタは「dcnr」ラベルをサポートします。DCNR セッションの場合、このカウンタは次のラベルと値をペインします。

- 試行統計：dcnr= "enable" および status= "attempted"
- 成功統計：dcnr= "enable" および status= "success"
- 障害統計：dcnr= "enable" および status= "failures"

次に、DCNR 統計のクエリの例を示します。

```
sum (smf_session_stats{dcnr_on="enable"}) by (dcnr, status, reason)
```

### セカンダリ RAT データ使用状況レポート

Secondary-Rat-Data-Usage-Reports は、「smf_secondary_rat_usage_report_stats」カウンタをサポートします。これらの統計情報のラベルには、ebi、qfi、rat_type、reason、service_name、および status が含まれます。このカウンタは、次のラベルと値とペグします。

- ebi=ebi-val
- qfi = qfi-val
- rat_type=NR
- reason=success/failure
- service_name=smf-service
- status=ReceivedFromSgw/SentToChf

次に、DCNR 統計のクエリの例を示します。

```
sum (smf_secondary_rat_usage_report_stats”) by (qfi, status, reason)
```

### プレゼンス レポート

プレゼンス レポートの場合、セッション数は既存のセッションゲージ「smf_session_counter」の「pra」ラベルをサポートします。SMF セッションでプレゼンス レポートが有効になっている場合、「presence-reporting」ラベルの値は「enable」になります。そうでない場合は、プレゼンス レポートが有効になっていない場合は「none」になります。

次に、DCNR アクティブな SMF セッションをカウントするクエリの例を示します。

```
sum (smf_session_counters{ pra ="enable"}) by (pra)
```

プレゼンス レポートの場合、統計は既存のカウンタ「smf_service_stats」の「presence-reporting」ラベルをサポートします。プレゼンス レポート セッションの場合、このカウンタは次のラベルと値をペインします。

- 試行統計：pra = "enable" および status= "attempted"
- 成功統計：pra = "enable" および status= "success"
- エラー統計：pra = "enable" および status= "failures"

次に、DCNR 統計のクエリの例を示します。

```
sum (smf_session_stats{ pra ="enable"}) by (pra, status, reason)
```

# バルク統計

オプション 3x および 4G 専用デバイス機能では、SMF スキーマで次のバルク統計がサポートされます。

| バルク統計名 | 統計情報の種類 | トリガー | 説明 |
|---|---|---|---|
| smf_session_counters | ゲージ | セッションのアタッチまたはデタッチの増減。 | 現在のアクティブ SMF セッションの総数を示します。DCNR セッション カウントの「dcnr=enable」などのラベルを使用して、アクティブ セッションをフィルタリングできます。 |
| smf_session_stats | カウンタ | コール フローの成功または失敗の増分。 | 試行、成功、失敗など、コール フロー状態の統計を示します。DCNR 統計情報のみを対象に「dcnr=enable」などのラベルを使用して統計情報をフィルタリングできます。 |
| セカンダリ RAT データ使用状況レポート機能は、次のバルク統計情報をサポートしています。 | | | |

| バルク統計名 | 統計情報の種類 | トリガー | 説明 |
|---|---|---|---|
| smf_secondary_rat_usage_report_stats | カウンタ | secondaryRatDataUsage レポート処理のステータスの増分。 | 「ReceivedFromSgw」や「SentToCHF」などのコール フロー ステータスに対する secondaryRatUsageReports 処理の統計を表示します。理由や QFI などのラベルを使用して統計をフィルタリングできます。 |
| OFCS_CDR_MESSAGE_STATS | カウンタ | | 新しいラベル「Trigger Type」は、構成されたセカンダリ RAT の使用制限に達したときにイベントをキャプチャします。トリガ タイプのラベルには「SECONDARY_RAT_USAGE_LIMIT_REACHED」の値が含まれています。 |
| PRA 機能では、次のバルク統計がサポートされています。 | | | |
| smf_session_counters | ゲージ | セッションのアタッチまたはデタッチの増減。 | 現在のアクティブセッションの総数。プレゼンス レポートが有効になったセッション カウントの「pri=enable」などのラベルを使用して、セッションをフィルタリングできます。 |
| smf_session_stats | カウンタ | コール フローの成功または失敗の増分。 | 試行、成功、失敗など、コール フロー状態の統計を示します。プレゼンス レポート統計情報に対してのみ「cra=enable」などのラベルを使用して統計情報をフィルタリングできます。 |

# トラブルシューティング情報

このセクションでは、システムの動作中に発生する可能性のある問題をトラブルシューティングするために、コマンド ライン インターフェイス（CLI）コマンド、アラート、ログとメトリックスの使用に関する情報について説明します。

## DCNR およびプレゼンス レポートが有効になっているサブスクライバの詳細

**show subscriber nf-service smf supi** *supi_id* **full** CLI コマンドは、オプション 3x 機能に対して有効になっているプレゼンス レポートが有効になっている DCNR アクティブ セッションを表示します。

（注） 2021.02 以降のリリースでは、 **namespace** キーワードは廃止され、 **nf-service** キーワードに置き換えられました。

```
[unknown] smf# show subscriber nf-service smf supi imsi-310260789012345 full

subscriber-details
{
  "subResponses": [
    {
      "status": true,
      "genericInfo": {
        "supi": "imsi-310260789012345",
        "pei": "imei-123456786666660",
        "pduSessionId": 5,
        "pduSesstype": "Ipv4PduSession",
        "accessType": "3GPP_ACCESS",
        "dnn": "fast.t-mobile.com",
        "plmnId": {
          "mcc": "123",
          "mnc": "456"
        },
…
        "alwaysOn": "None",
        "dcnr": "Enabled",
        "wps": "Non-Wps Session",
        "ratType": "EUTRA",
        "ueType": "NR Capable UE",
        "iwkEpsInd": true,
        "sessTimeStamp": "2021-01-12 12:40:39.931012285 +0000 UTC",
        "callDuration": "4m25.36784895s",
        "ipPool": "poolv4",
        "commonId": 16777223,
        "linkedEbi": 5,
        "smfIwkEpsInd": true,
        "snssai": {
          "sd": "Abf123",
          "sst": 1
        },
        "authStatus": "Unauthenticated",
```

```
        "roamingStatus": "Roamer",
        "uePlmnId": {
          "mcc": "310",
          "mnc": "260"
        }
      },
      "policySubData": {
        "TotalDynamicRules": 2,
        "TotalFlowCount": 2,
        "TotalNonGBRFlows": 1,
        "TotalGBRFlows": 1,
        …
        "presenceReporting": "Enabled",
        "praList": [
          {
            "praId": "0x80000b",
            "presenceState": "Inactive"
          },
          {
            "praId": "0x800000",
            "presenceState": "InArea"
          },
          {
            "praId": "0x80000a",
            "presenceState": "OutOfArea"
          }
        ]
      },
      …
      }
    }
  ]
}
```

# オプション 3x：DCNR 対応 UE アラート

このセクションでは、プレゼンス レポートが有効になっている DCNR 対応 UE に対してサポートされるアラートについて説明します。これらのアラートは、RAT ベースまたはエンド ユーザーの意図に従って強化できます。

DCNR 統計またはゲージの例は、pdn_sess_create、pdn_inter_sgw_handover、pdn_mbr、pcf_req_ded_brr_mod、pcf_req_ded_brr_create、pcf_req_ded_brr_delete、delete_session_request、smf_initiated_pdn_detach、ue_req_pdn_sess_rel などです。

## DCNR UE 接続失敗しきい値アラート

DCNR UE 接続障害しきい値に関連するアラートを構成するには、次の例を使用します。

```
alerts rules group DCNRUEs
 rule DCNR_UE_SR
  expression "sum by (namespace) (increase(smf_service_stats{app_name=\"smf\",
dcnr=\"enable\", rat_type!=\"EUTRA\", status=\"success\",
procedure_type=\"pdn_sess_create\"}[5m])) / sum by (namespace)
(increase(smf_service_stats{app_name=\"smf\", dcnr =\"enable\", rat_type!=\"EUTRA\",
status=\"attempted\", procedure_type=\"pdn_sess_create\"}[5m])) < 0.10"
  severity   major
  type       "Communications Alarm"
  annotation summary
   value "This alert is fired when attach success rate of DCNR enabled UE lesser than
```

```
threshold"
  exit
 exit
```

## プレゼンス レポートを使用した DCNR UE 接続失敗しきい値アラート

次の例を使用して、プレゼンス レポートを使用した DCNR UE 接続失敗しきい値に関連するアラートを構成します。

```
rule DCNR_UE_PRA_ENABLE_SR
  expression "sum by (namespace) (increase(smf_service_stats{app_name=\"smf\",
dcnr=\"enable\", rat_type!=\"EUTRA\", status=\"success\",
procedure_type=\"pdn_sess_create\", pra=\"enable\"}[5m])) / sum by (namespace)
(increase(smf_service_stats{app_name=\"smf\", dcnr =\"enable\", rat_type!=\"EUTRA\",
status=\"attempted\", procedure_type=\"pdn_sess_create\", pra=\"enable\"}[5m])) < 0.10"
  severity   major
  type       "Communications Alarm"
  annotation summary
   value "This alert is fired when attach success rate of DCNR enabled UE and presence
reporting enabled lesser than threshold "
  exit
 exit
```

# DCNR UE バルク統計情報

次の SMF サービスのバルク統計情報を使用して、DCNR UE に関連する障害または問題を監視します。

**表 *481 : DCNR UE***

| バルク統計名 | [Query（クエリ）] | 説明 |
|---|---|---|
| 4G_DCNRUE_Attempted | bulk-stats query 4G_DCNRUE_Attempted expression "sum(smf_service_stats {dcnr='enable',status='attempted', rat_type='EUTRA'}) by (namespace)" exit | |
| 4G_DCNRUE_Success | bulk-stats query 4G_DCNRUE_Success expression "sum(smf_service_stats {dcnr='enable',status='success', rat_type='EUTRA'}) by (namespace)" exit | |
| 4G_PRA_ENABLE_Attempted | bulk-stats query 4G_PRA_ENABLE_Attempted expression "sum(smf_service_stats {pra='enable',status='attempted', rat_type='EUTRA', procedure_type!='create_session_request'}) by (namespace)" exit | |
| 4G_PRA_ENABLE_Success | bulk-stats query 4G_PRA_ENABLE_Success expression "sum(smf_service_stats {pra='enable',status='success', rat_type='EUTRA', procedure_type!='create_session_request'}) by (namespace)" exit | |

# オプション - 3x デバイス固有のエラーログ

このセクションでは、基本的なエラー状態と、オプション 3x 機能の障害をデバッグするためにキャプチャされるログを示します。

### DCNR 無効化された UE または 4G 対応 UE のみ

次の例では、DCNR 無効化 UE または 4G 対応 UE のみのエラー ログを表示します。

```
2021/01/24 10:11:22.648 smf-service [ERROR] [GenericGtpMsg.go:1811]
[smf-service.smf-app.sgw] secRatUsageRpt recvd wrongly for DNCR disbled UE, ignoring
report

2020/12/19 13:17:17.834 smf-service [ERROR] [GenericGtpMsg.go:1834]
[smf-service.smf-app.sgw] secRatUsageRpt recvd wrongly for 4gOnly UE, ignoring report
```

### 無効な EBI によるセカンダリ RAT 使用状況

次の例では、無効な EBI でのセカンダリ RAT の使用のエラー ログを表示します。

```
2021/01/24 11:38:18.917 smf-service [DEBUG] [GenericGtpMsg.go:1824]
[smf-service.smf-app.sgw] Secondary Rat Data Usage Report Recvd
2021/01/24 11:38:18.917 smf-service [WARN] [IntMethods.go:137] [smf-service.Policy.gen]
 Qos Flow not found with EBI [8]
2021/01/24 11:38:18.917 smf-service [ERROR] [GenericGtpMsg.go:1853]
[smf-service.smf-app.sgw]  Qfi invalid in secRatUsageRpt
```

### セカンダリ RAT 使用無効な RAT タイプ

次に、無効な RAT タイプで使用されたセカンダリ RAT のエラー ログを表示する例を示します。

```
2021/01/24 11:42:21.474 smf-service [DEBUG] [GenericGtpMsg.go:1824]
[smf-service.smf-app.sgw] Secondary Rat Data Usage Report Recvd
2021/01/24 11:42:21.474 smf-service [ERROR] [GenericGtpMsg.go:1861]
[smf-service.smf-app.sgw]  Rat type invalid in secRatUsageRpt
```

### 意図した PGW がゼロに設定されたセカンダリ RAT 使用率

次に、意図された P-GW をゼロ（IRGW:0）に設定したセカンダリ RAT の使用状況のエラーログを表示する例を示します。

```
2021/01/24 11:33:10.390 smf-service [DEBUG] [GenericGtpMsg.go:1824]
[smf-service.smf-app.sgw] Secondary Rat Data Usage Report Recvd
2021/01/24 11:33:10.390 smf-service [ERROR] [GenericGtpMsg.go:1865]
[smf-service.smf-app.sgw]  secRatUsageRpt.IRPGW is false
```

### 4 を超える PRA ID を受信しました

次に、受信した PRA ID が 4 より大きい場合にエラー ログを表示する例を示します。

```
2021/01/24 14:48:26.085 smf-service [DEBUG] [policy_types.go:659] [smf-service.Policy.gen]
 praConfig:true for dnn:fast.t-mobile.com
2021/01/24 14:48:26.085 smf-service [DEBUG] [policy_pcf.go:1939] [smf-service.Policy.gen]
 Added PRA ID: 9388618
2021/01/24 14:48:26.085 smf-service [DEBUG] [policy_pcf.go:1939] [smf-service.Policy.gen]
 Added PRA ID: 9388608
2021/01/24 14:48:26.085 smf-service [DEBUG] [policy_pcf.go:1939] [smf-service.Policy.gen]
 Added PRA ID: 8388618
2021/01/24 14:48:26.085 smf-service [DEBUG] [policy_pcf.go:1939] [smf-service.Policy.gen]
 Added PRA ID: 9388619
2021/01/24 14:48:26.085 smf-service [WARN] [policy_pcf.go:1934] [smf-service.Policy.gen]
 Max 4 PRAs allowed, ignoring the PRA-ID (8388608) from PCF
2021/01/24 14:48:26.085 smf-service [WARN] [policy_pcf.go:1934] [smf-service.Policy.gen]
 Max 4 PRAs allowed, ignoring the PRA-ID (8388619) from PCF
```

# SMF における 2G および 3G ネットワーク統合

## 2G および 3G ネットワーク統合概要

表 *482 :* 機能の履歴（表）

| 機能 | リリース | 説明 |
|---|---|---|
| GTPv1 を介した 2G および 3G セッションの接続と切断の手順 | 2025.03.0 | この機能には、v1SGSN の SMF での 2G および 3G セッションのアタッチとデタッチのサポートに関する詳細が含まれています。これは、GTPv1 のメッセージ/手順、および同等の GTPv2 に変換される情報要素をキャプチャします。 |
| 2G および 3G セッションの QoS ネゴシエーション | 2025.03.0 | この機能により、SMF の S4-SGSN を利用する 2G および 3G サブスクライバの Quality of Service（QoS）ネゴシエーション機能が導入されています。これにより、ホーム ロケーション レジスタ (HLR) または PCF から発信されるトリガーに基づいて、デフォルト ベアラーの QoS パラメーターを動的に自動調整できます。<br>これにより、ネットワークは変化する条件とサブスクライバのニーズに適応し、リソースの使用率を最適化し、ユーザー エクスペリエンスを向上させることができます。 |

| 機能 | リリース | 説明 |
| --- | --- | --- |
| S4-SGSN セッションの引き継ぎと、2G および 3G ネットワークのモビリティ管理 | 2025.03.0 | この機能では、SMF の S4SGSN に対する 2G および 3G サポートのコンテキスト内での、ベアラー要求の変更（MBR）とハンドオーバーのシナリオの処理について詳しく説明します。ユーザー ロケーションの変更、RAT 間ハンドオーバー（4G から 3G/2G および 3G/2G から 4G）、RAT 内ハンドオーバー（3G SGW ハンドオーバー）、および専用ベアラーを含むハンドオーバーの手順について概説します。<br>これにより、ハンドオーバー中にセッションが維持されるため、ユーザー アプリケーションの中断が最小限に抑えられます。 |

| 機能 | リリース | 説明 |
| --- | --- | --- |
| S4-SGSN の 2G および 3G セッションの接続と切断の手順 | 2025.02.0 | この機能により、S4-SGSN（サービング GPRS サポートノード）から発信される接続およびデタッチ機能を管理するためのサポートが SMF に追加されます。これにより、2G/3G および 4G/5G のネットワーク制御を 1 つのコンバージド コアに統合できます。ネットワークを統合すると、ネットワーク管理を簡素化し、運用コストを削減できます。<br>**導入されたコマンド**：<br>**profile converged-core activated-features 2g3g**：この CLI コマンドは、SMF で 2G および 3G RAT タイプの S4-SGSN サポートを有効にします。<br>**デフォルト設定**無効：有効にするには構成が必要です。 |

コンバージドコア（CC）に 2G および 3G ネットワークの統合が含まれることにより、単一の環境で 2G、3G、4G、Wi-Fi および 5G ネットワークなどの無線アクセス技術の全範囲がサポートされます。これにより、無線アクセス タイプごとに個別のネットワークを維持する必要がなくなります。

S4-SGSN 機能の 2G および 3G セッションの接続および切断手順では、SBI インターフェイスの SMF のサポートを活用して、既存の SMF セットに 2G および 3G RAT タイプを含めます。4G 用の SMF でサポートされている機能は 2G および 3G ネットワークにまで拡張されています。

この機能の主な機能は次のとおりです：

- **GTPv2 プロトコルのサポート**： S4-SGSN ノードから発信されるアタッチおよびデタッチ シグナリング メッセージを処理するために、SMF 内で必要な GTPv2 プロトコル処理を実装します。
- **コンバージドコア統合**： 4G/5G サブスクライバと同じ SMF インスタンス内で 2G/3G サブスクライバを管理できます。これにより、ネットワーク管理が合理化され、個別のコントロールプレーンエンティティの必要性が軽減されます。

- **RAT 間モビリティ**： 2G/3G ネットワークと 4G/5G ネットワーク間のモビリティ シナリオをサポートし、異なる無線アクセス技術（RAT）間で一貫したユーザーエクスペリエンスを実現します。

### コンバージド コアとの 2G および 3G ネットワーク統合の標準規格に準拠

2G および 3G ネットワーク統合機能は、SMF での N7 および N40 インターフェイスと共通データ タイプの構成に関する次の 3GPP 標準に準拠しています。

- 3GPP TS 29.512、バージョン 17.3.0：N7 インターフェイス用
- 3GPP TS 32.291、バージョン 17.0.0：N40 インターフェイス用
- 3GPP TS 29.571、バージョン 17.3.0：一般的なデータ型の場合

### コンバージド コアとの 2G および 3G ネットワーク統合の前提条件

SMF の 2G および 3G ネットワーク統合機能の前提条件は次のとおりです。

- この機能を有効にする前に、PCF/CHF のユーザーは 3GPP リリース バージョン 17 以降にアップグレードする必要があります。
- 2G および 3G コールとインタラクションについては、Gx、Gy、および Gz インターフェイスから N7 または N40 インターフェイスに移行する必要があります。
- UE が 2G または 3G ネットワークに接続されている場合、5G ネットワークへのハンドオーバーは許可されないため、2G および 3G の接続中にセカンダリ PDR は作成されません。

### コンバージド コアとの 2G および 3G ネットワーク統合の制限事項

SMF の 2G および 3G ネットワーク統合機能には次の制限があります。

- この機能では、セカンダリ PDP コンテキスト（ネットワークまたは UE）はサポートされていません。
- 2G および 3G ネットワークは、4G ネットワークの SMF でサポートされていない DHCP/OC/VoGX 機能をサポートしていません。
- S4-SGSN ノードからの CSR 要求で、新しい無線（DCNR）とのデュアル接続が受信されません。したがって、SMF では DCNR サポートは必要ありません。
- S4-SGSN/SGSN は HSS/HLR からサブスクリプション データを取得するため、UTRAN/GERAN 接続の場合、N10 サブスクリプションのフェッチ、通知へのサブスクリプション、および登録機能はスキップされます。

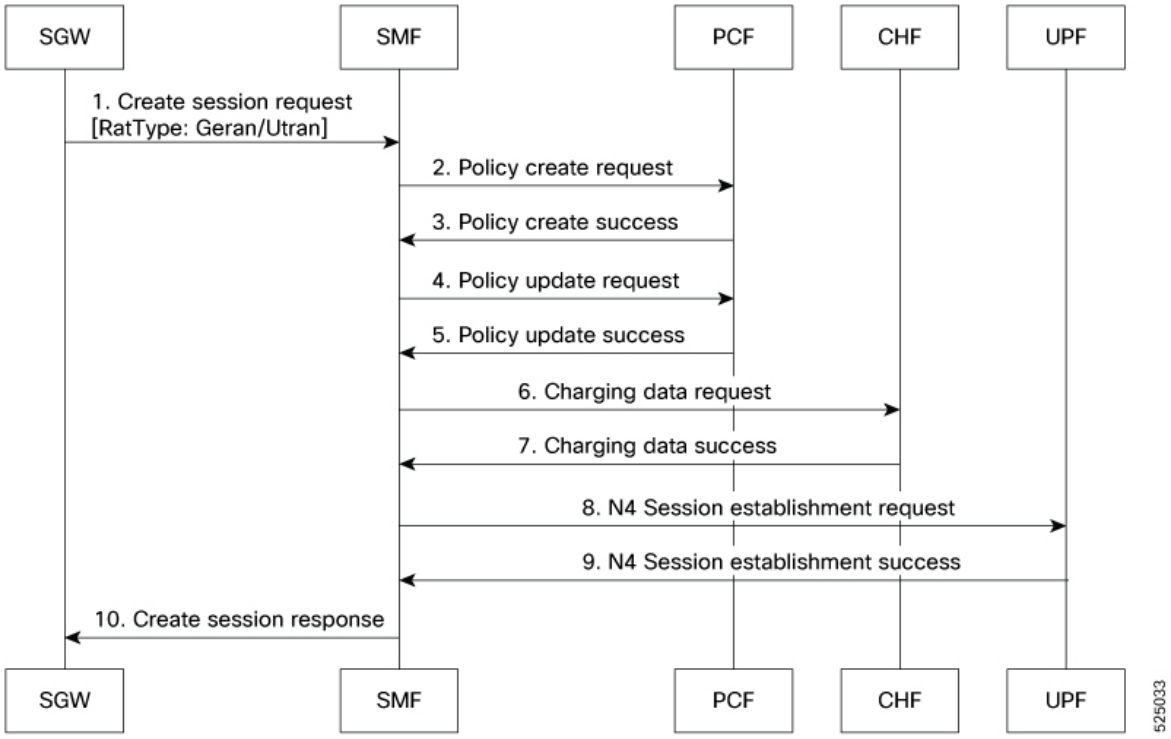
## S4-SGSN の接続と切断の手順コール フロー

接続と切断の手順については、S4-SGSN ネットワークを介した PDN 接続コール フローと PDN 切断コール フローを通じて説明します。

# S4-SGSN を介した PDN 切断

ここでは、S4-SGSN を介した PDN 接続でのコール フローとステージについて説明します。

図 *285 : S4-SGSN* を介した *PDN* 切断




特定の段階では、SMF を介した GERAN および UTRAN 上の初期アタッチでの SMF と他の NF 間の相互作用について説明します。

1. SMF は SGW から CreateSessionRequest 通知を受信します。CreateSessionRequest の RAT タイプは、2G 接続の場合は GERAN、3G 接続の場合は UTRAN です。

   ユーザー ロケーション情報（ULI）には、指定された値のいずれかが含まれます。

   - ルーティング エリア識別子（Rai）
   - サービング エリア識別子(Sai)
   - セル グローバル識別子（Cgi）
   - サービス エリア識別子 + ルーティング エリア識別子
   - セル グローバル識別子 + ルーティング エリア識別子

   さまざまな通知の IE および RAT タイプ値の詳細については 、「*S4-SGSN* をサポートするためのインターフェイス レベルの *IE* 情報」を参照してください。

2. SMF は PolicyCreateRequest メッセージを PCF に送信して、ポリシーの関連付けを確立します。

3. SMF は、ポリシー課金情報および制御情報を含む PolicyCreateSuccess メッセージを PCF から受信します。
4. UE IP アドレスが割り当てられ、SMF がトリガ `UE_IP_CH`を使用して PolicyUpdateRequest メッセージを PCF に送信します。
5. SMF は PCF から PolicyUpdateSuccess メッセージを受信します。
6. SMF は PCF から受信した課金ポリシーに基づいて、CHF に向けて ChargingDataRequest メッセージを開始します。
7. SMF は CHF から ChargingDataSuccess メッセージを受信し、次の通知を受信します。
   - セッションまたは RG レベルで CC がトリガーする
   - セッション レベルの時間またはボリュームの制限
   - RG レベルでの時間またはボリュームの制限
   - RG レベルのクォータ
8. SMF は、PDR、QER、FAR、URR に関連する情報を中継するために、UPF に向けて N4SessionEstablishmentRequest メッセージを送信します。
9. SMF は UPF から N4SessionEstablishmentSuccess メッセージを受信します。
10. SMF は S-GW に CreateSessionResponse メッセージを送信し、デフォルトのベアラーに関するベアラー情報とトンネル エンドポイント ID（TEID）を含めます。

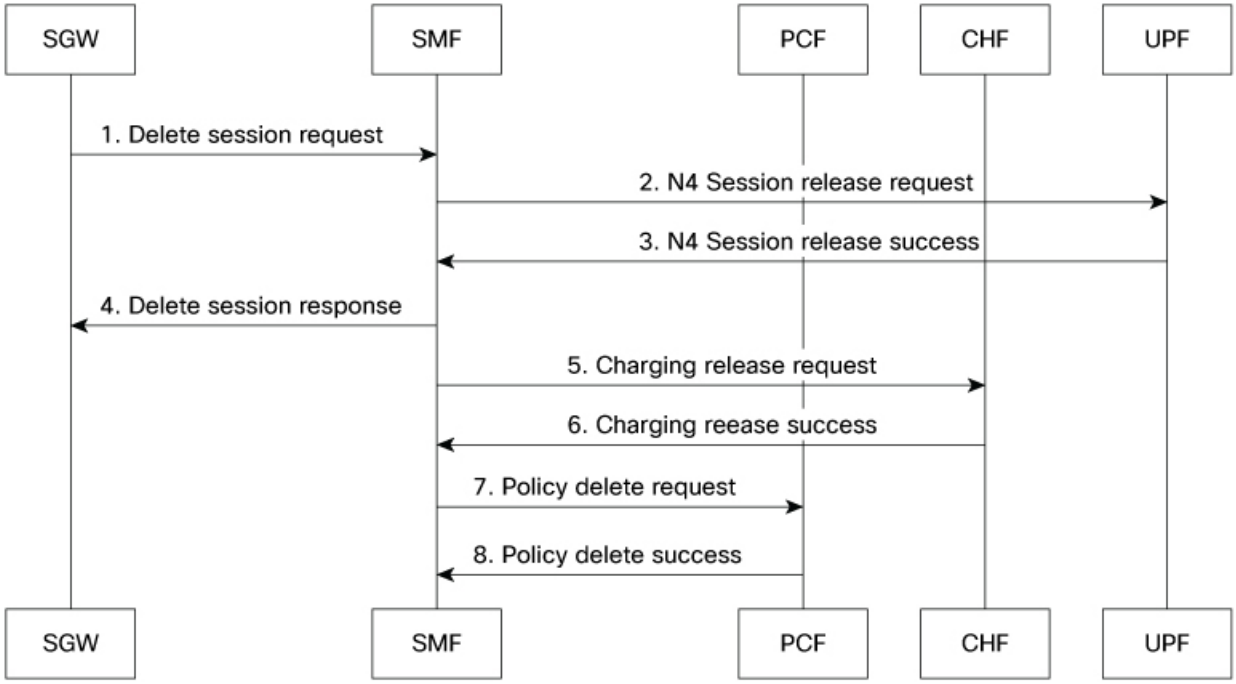
## S4-SGSN を介した PDN 切断

ここでは、SGSN を介した PDN 接続でのコール フローとステージについて説明します。

### UE で開始されたリリース

このコール フローは、S4-SGSN を介した PDN 切断のために UE が開始するリリースを示しています。

図 *286 : UE* が開始した *PDN* の切断



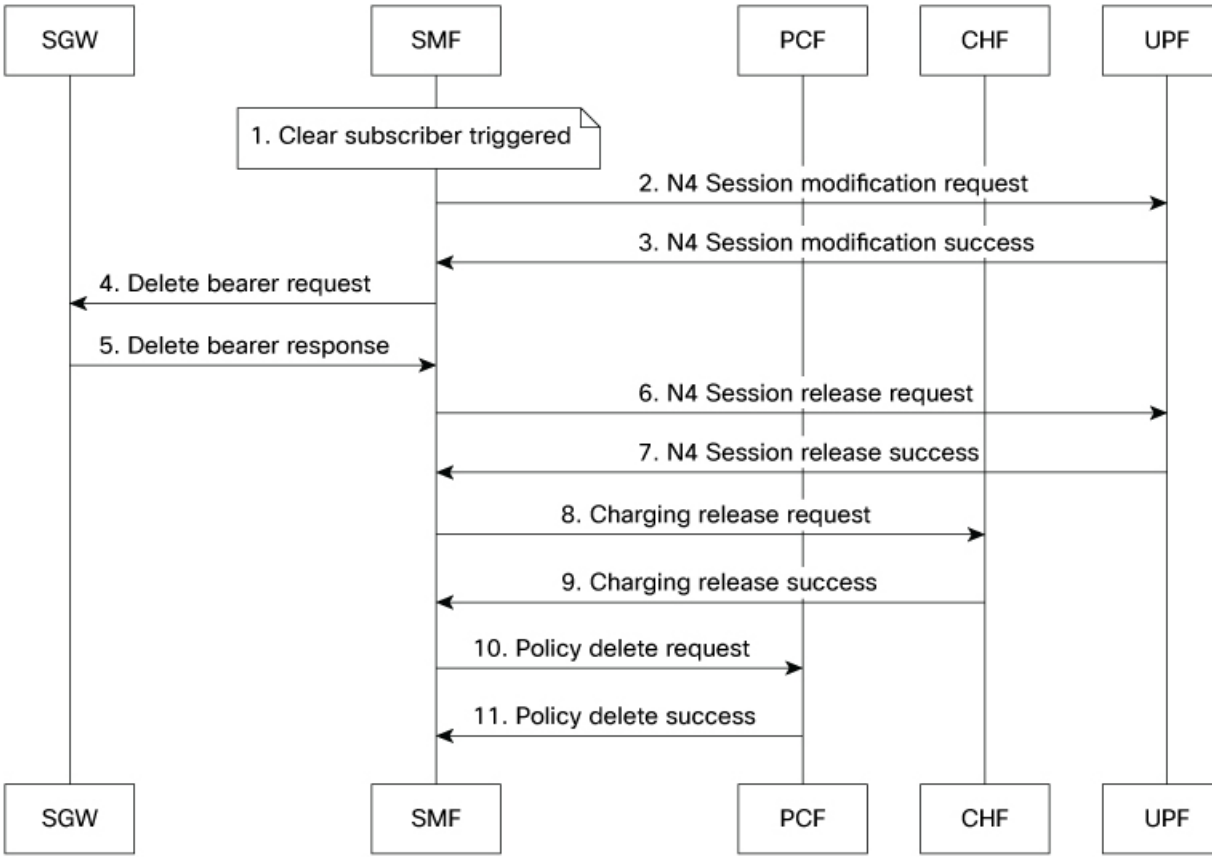

次の手順では、S4-SGSN を介した PDN 切断のために UE が開始するリリースについて説明します。

1. SMF は SGW から DeleteSessionRequest メッセージを受信します。
2. SMF が N4SessionReleaseRequest メッセージを送信して、ユーザー プレーン リソース UPF を削除します。
3. SMF は、UPF から最終的な使用状況を示す N4SessionReleaseSuccess メッセージを受信します。
4. SMF は、DeleteSessionResponse を SGW に送信します。
5. SMF は、最終的な使用状況を含む ChargingReleaseRequest メッセージを CHF に送信します。
6. SMF は、CHF から ChargingReleaseSuccess メッセージを受信します。
7. SMF は、PolicyDeleteRequest メッセージを PCF に送信して、PCF へのポリシーの関連付けを削除します。
8. SMF は PCF から PolicyDeleteSuccess メッセージを受信します。

## SMF によって開始されたリリース

このコールフローは、S4-SGSN を介した PDN 切断のために SMF が開始するリリースを示しています。

図 *287 : UE* が開始した *PDN* の切断




この手順では、PDN 切断のために SMF によって開始されるリリースについて説明します：

1. SMF によって開始されたリリースは、Clear subscriber コマンドを使用してトリガーされます。
2. SMF は、更新 FAR でドロップ アクションが設定された N4SessionModificationRequest メッセージを UPF に送信します。
3. SMF は UPF から N4SessionModificationSuccess メッセージを受信します。
4. SMF は、DeleteBearerRequest メッセージを SGW に送信して、ベアラー コンテキストを削除します。
5. SMF は SGW から DeleteBearerSuccess メッセージを受信します。
6. ユーザー プレーン リソースを削除するために SMF は、UPF に N4SessionReleaseRequest メッセージを送信します。
7. UPF からの最終使用とともに SMF は、N4SessionReleaseSuccess メッセージを受信します。
8. SMF は、最終的な使用状況の ChargingReleaseRequest メッセージを CHF に送信します。

9. SMF は、CHF から ChargingReleaseSuccess メッセージを受信します。
10. SMF は PolicyCreateRequest メッセージを PCF に送信して、ポリシーの関連付けを確立します。
11. SMF は PCF から PolicyUpdateSuccess メッセージを受信します。

## S4-SGSN をサポートするためのインターフェイス レベルの IE 情報

このセクションでは、S5/S8、N7、N40、および N4 インターフェイスからの通知の IE および RAT タイプの値に関する情報を提供します。

### S5/S8 インターフェイス

制御シグナリングがオペレータ ネットワークの S4-SGSN ノードから発信される場合に S5/S8 インターフェイスでサポートされる新しい enum と対応する値のセットを次に示します。

表 *483 : S5/S8* インターフェイス

| インターフェイス S5/S8 のメッセージ | IE | 詳細 |
|---|---|---|
| メッセージのセッション要求の作成/変更 | GTPV2_IE_RAT_TYPE | GERAN/UTRAN |
| セッション要求の作成/変更/削除 | GTPV2_IE_ULI | ユーザー ロケーション情報（ULI）に、次のリストされている値のいずれか 1 つが含まれている。<br>• Rai<br>• Sai<br>• Cgi<br>• Cgi + Rai<br>• Sai + Rai |

### N7 インターフェイス

N7 インターフェイス メッセージについては、次の IE 情報を参照してください。

表 *484 : N7* インターフェイス

| インターフェイス N7 メッセージ | IE | 詳細 |
|---|---|---|
| メッセージ :: N7 作成要求 | SmPolicyContextData ->ServNfId | GTPv2 2G/3G コール用の AnGwAddr および GTPv1 2G/3G コール用の SgsnAddr |
| | SmPolicyContextData->RatType | GERA/UTRA |
| | SmPolicyContextData->AccessType | 3GPP_ACCESS |
| | SmPolicyContextData-> PolicyCtrlReqTriggers | 'SCELL_CH', 'SAREA_CH', 'SCNN_CH' |
| | SmPolicyContextData-> UserLocationInfo-> GeraLocation/UtraLocation | GeraLocation または UtraLocation には、次の値のいずれかを含めることができます。<br>• Rai<br>• Sai<br>• Cgi<br>• Cgi + Rai<br>• Sai + Rai |
| | SmPolicyContextData->Suppfeat | PCF のリリース バージョンが 17.3.0 以上で、2g3g CLI が設定されている場合、2G3GIWK フラグ ビットは 1 に設定されます。 |

| インターフェイス N7 メッセージ | IE | 詳細 |
|---|---|---|
| メッセージ :: N7 更新要求 | SmPolicyUpdateContextData ->ServNfId | GTPv2 2G/3G コール用の AnGwAddr および GTPv1 2G/3G コール用の SgsnAddr |
| | SmPolicyUpdateContextData ->RatType | GERA/UTRA |
| | SmPolicyContextData-> PolicyCtrlReqTriggers | 'SCELL_CH', 'SAREA_CH', 'SCNN_CH' |
| | SmPolicyUpdateData->ServNfId<br>SmPolicyUpdateData-> UserLocationInfo-> GeraLocation/UtraLocation | GeraLocation または UtraLocation には、次の値のいずれかが含まれます。<br>• Rai<br>• Sai<br>• Cgi<br>• Cgi + Rai<br>• Sai + Rai |
| メッセージ :: N7 削除要求 | SmPolicyDeleteData-> UserLocationInfo-> GeraLocation/UtraLocation | GeraLocation または UtraLocation には、次の値のいずれかが含まれます。<br>• Rai<br>• Sai<br>• Cgi<br>• Cgi + Rai<br>• Sai + Rai |

### N40 インターフェイス

N40 インターフェイス メッセージについては、次の IE 情報を参照してください。

表 *485 : N40* インターフェイス：

| インターフェイス N40 メッセージ | IE | 詳細 |
|---|---|---|
| メッセージ：<br>ChargingDataRequest | PDUSessionInformation-><br>RatType | GERA/UTRA |
| | nfConsumerIdentification-><br>nodeFunctionality | SMF |
| | PDUSessionInformation<br>->servingNetworkFunctionID -><br>nodeFunctionality | GTPv2 2G/3G 用の SGW および GTPv1 2G/3G コール用の SGSN |
| | UserLocationInfo-><br>GeraLocation/UtraLocation | GeraLocation または UtraLocation には、次の値のいずれかを含めることができます。<br>• Rai<br>• Sai<br>• Cgi<br>• Cgi + Rai<br>• Sai + Rai |
| メッセージ：<br>ChargingDataResponse | []triggers | トリガ タイプ<br>CGI_SAI_CHANGE<br>RAI_CHANGE |
| | MultiUnitInformation-> []triggers | トリガ タイプ<br>CGI_SAI_CHANGE<br>RAI_CHANGE |

| インターフェイス N40 メッセージ | IE | 詳細 |
|---|---|---|
| メッセージ：<br>ChargingReleaseRequest | PDUContainerInformation-><br>RatType | GERA/UTRA |
| | PDUContainerInformation-><br>ServingNodeID-><br>nodeFunctionality | GTPv2 2G/3G 用の SGW および GTPv1 2G/3G コール用の SGSN |
| | PDUSessionInformation<br>->servingNetworkFunctionID -><br>nodeFunctionality | GTPv2 2G/3G 用の SGW および GTPv1 2G/3G コール用の SGSN |
| | PDUSessionInformation-><br>RatType | GERA/UTRA |
| | nfConsumerIdentification-><br>nodeFunctionality | SMF |
| | UserLocationInfo-><br>GeraLocation/UtraLocation | GeraLocation または UtraLocation には、次の値のいずれかを含めることができます。<br>• Rai<br>• Sai<br>• Cgi<br>• Cgi + Rai<br>• Sai + Rai |

### N4 インターフェイス

N4 インターフェイス メッセージについては、次の IE 情報を参照してください。

表 *486 : N4* インターフェイス

| インターフェイス N4 | IE | 詳細 |
|---|---|---|
| PFCP 確立要求<br>PFCP 変更要求 | Subscriber Params->Rat Type | [RAT タイプ（RAT Type）] の値は 1 または 2 のいずれかです。<br>1 - UTRAN<br>2 - GERAN |
| | Subscriber Params->Uli | ユーザー ロケーション情報（ULI）に、次のリストされている値のいずれか 1 つが含まれている。<br>• Rai<br>• Sai<br>• Cgi<br>• Cgi + Rai<br>• Sai + Rai |
| | Subscriber Params->Sgsn address | SGSN アドレスは、IPv4/IPv6 のいずれかになります。 |
| | Subscriber Params->Ggsn address | GGSN アドレスは、IPv4/IPv6 のいずれかになります。 |
| | Create_FAR ->Outer Header Creation ->Teid | TEID 値には、SGW GTP-U TEID が含まれています。 |

（注） ユーザー ロケーション情報 - ロケーション領域識別子（Lai）は、S5/S8、N7、N40、および N4 インターフェイスではサポートされていません。

## 2G と 3G RAT タイプの S4-SGSN を有効化

この設定により、SMF で 2G および 3G RAT タイプの S4-SGSN サポートを有効にすることができます。

### 手順

**ステップ 1** 構成モード内の統合コア プロファイル名 **converged-core <name>** を開始します。

```
config
profile converged-core <name>
```

**ステップ 2** **2g3g** フラグを入力して SMFでS4-SGSN を有効にし、コマンドを終了します。

```
config
   profile converged-core <name>
   activated-features 2g3g
end
```

構成例は、次のとおりです：

```
[smf] smf(config)# profile converged-core cc activated-features ?
Possible completions:
  2g3g               This flag enables the support for 2G 3G RAT on SMF
  upf-blocklisting   This flag enables upf blocklist feature
[smf] smf(config)# profile converged-core cc activated-features 2g3g
Tue Mar  4  13:28:27.850 UTC+00:00
[smf] smf(config-converged-core-cc)#
```

（注）
構成を無効にするには、指定された構文を使用します：

```
config
   profile converged-core <name>
   [no] activated-features 2g3g
end
```

設定が無効になっている場合、S4-SGSN（v2）メッセージは適切な **System Failure** エラーコードで拒否され、 **gtpc_app_total_unexpected_gtpc_msg_events** メトリックが増分されます。

**ステップ 3** オプション：**show running-config profile converged-core cc** CLI コマンドを実行して、2g3g フラグが有効になっているかどうかを確認します。

```
[smf] smf# show running-config profile converged-core cc
Tue Mar  4  13:30:51.799 UTC+00:00
profile converged-core cc
 supported-features [ rolling-upgrade-all ]
 activated-features 2g3g
exit
```

## N40 充電コンプライアンス バージョンの構成

この手順により、SMF の 2G および 3G セッションに対する N40 の 3GPP 仕様 TS 32.291（バージョン 17.0.0）を構成できます。

### 手順

**ステップ 1** コンフィギュレーション モードで **compliance profile name** を開始します。

```
config
profile compliance < compliance profile name>
```

**ステップ 2** **17.0.0** として **nchf-convergedcharging** を開始し、コマンドを終了します。

```
config
profile compliance < compliance profile name>
service nchf-convergedcharging version spec 17.0.0
end
```

構成例を示します。

```
[smf] smf(config-compliance-comp1)# service nchf-convergedcharging version spec ?
Description: 3gpp nchf-convergedcharging Spec version number - 15.0.0 [default]
Possible completions:
  [17.0.0] 15.0.0  15.1.0  15.2.1  15.3.0  15.3.0.custom  15.3.0.std  15.4.0  16.8.1  17.0.0
[smf] smf(config-compliance-comp1)# service nchf-convergedcharging version spec 17.0.0
Mon Oct  21 12:19:46.838 UTC+00:00
[smf] smf(config-service-nchf-convergedcharging)#
```

**ステップ 3** オプション：**show running-config profile compliance comp1 service nchf-convergedcharging** CLI コマンドを実行して、N40 インターフェイスの課金準拠バージョンを確認します。

```
[smf] smf# show running-config profile compliance comp1 service nchf-convergedcharging
Wed Oct  23 11:49:52.490 UTC+00:00
profile compliance comp1
 service nchf-convergedcharging
  version uri v1
  version full 1.0.0
  version spec 17.0.0
 exit
exit
[smf] smf#
```

## N7 ポリシー コンプライアンス バージョンの構成

この手順では、SMF での 2G および 3G セッションの N7 ポリシーのバージョン 17.3.0 の 3GPP 仕様 TS 29.512 を構成できます。

### 手順

**ステップ 1** コンフィギュレーション モードの **compliance profile name** を開始します。

```
config
profile compliance < compliance profile name>
```

**ステップ 2** **17.3.0** として **nchf- smpolicycontrol** を開始し、コマンドを終了します。

```
config
profile compliance < compliance profile name>
service nchf- smpolicycontrol version spec 17.3.0
end
```

構成例を示します。

```
[smf] smf(config-compliance-comp1)# service npcf-smpolicycontrol version spec ?
Description: 3gpp npcf-smpolicycontrol Spec version number - 15.2.0 [default]
Possible completions:
  [17.3.0]  15.0.0  15.2.0  15.4.0  16.10.0  17.3.0
[smf] smf(config-compliance-comp1)# service npcf-smpolicycontrol version spec 17.3.0
```

```
Mon Oct  21 12:21:22.960 UTC+00:00
[smf] smf(config-service-npcf-smpolicycontrol)
```

**ステップ 3** オプション： CLI コマンドの **show running-config profile compliance comp1 service npcf-smpolicycontrol** を実行して、N7 インターフェイスのポリシー コンプライアンス バージョンを確認します。

```
[smf] smf# show running-config profile compliance comp1 service npcf-smpolicycontrol
Wed Oct  23 11:49:01.841 UTC+00:00
profile compliance comp1
 service npcf-smpolicycontrol
  version uri v1
  version full 1.0.0
  version spec 17.3.0
 exit
exit
```

## 2G および 3G セッションの show コマンドと clear session コマンド

このセクションでは、SMF の 2G および 3G ネットワーク インターゲート機能に関連する show コマンドと clear session コマンドについて説明します。

### UTRAN RAT タイプの 3G セッションのサブスクライバ情報の表示

次に、UTRAN RAT タイプを指定した 3G セッションに対する **show subscriber** CLI コマンドの出力例を示します。

```
show subscriber nf-service smf supi imsi-123456789012345 full
```

```
  "subResponses": [
    {
      "status": true,
      "genericInfo": {
        "pduState": "pduState_None",
        "supi": "imsi-123456789012345",
        "pei": "imei-123456786666660",
        ...
       "uetimeZone": "+00:15+1",
        "allocatedIp": "12.0.0.1",
        "alwaysOn": "None",
        "dcnr": "None",
        "wps": "Non-Wps Session",
        "ratType": "UTRA",
        "ueType": "NR Capable UE",
        "sessTimeStamp": "2025-03-03 12:34:35.409932765 +0000 UTC",
        ...
     "ipAllocationBy": "Dynamic",
        "anType": "3GPP_ACCESS",
        "utranLocation": {
          "cgi": {
            "mcc": "123",
            "mnc": "456",
            "lac": "04d2",
            "cellId": "0004"
          },
          "ueLocationTimestamp": "2025-03-03T12:34:35Z"
        },
        "initialRatType": "UTRA"
      },
```

```
      "policySubData": {
        "TotalDynamicRules": 1,
        "TotalFlowCount": 1,
        "TotalNonGBRFlows": 1,

    },
    ...
     "access3GSubData": {
        "localTeid": 2097154,
        "lbi": 5,
        "bearerContexts": [
          {
            "ebi": 5,
            "defBrr": true,
            "dlFteid": {
              "teid": 1647,
              "ipaddr": "10.1.34.62"
            }
          }
        ],
   "AnGwAddr": { □ For GTPv2 3G call
    "anGwIpv4Addr": "10.1.0.227"
   }

   "sgsnAddr": { □ For GTPv1 3G call
   "sgsnIpv4Addr": "10.1.0.227"
  }
        "gtpVersion": "GtpV2"
      }
    }
  ]
}
```

2G セッションの出力は、GERAN が RAT タイプと同様です。

### セッション数の情報の表示

特定の RAT タイプのアクティブ セッションの数を表示するには、 **show subscriber count** CLI コマンドを使用します。次に例を示します。

```
show subscriber count nf-service smf rat utran

subscriber-details
{
  "sessionCount": 1
}
```

（注） RAT タイプ ベースの show および clear session オプションが、次に示すように、2G および 3G セッション向けに拡張されました。

- **show subscriber nf-service smf rat geran/utran**
- **clear subscriber nf-service smf rat utran/geran**

クリア セッションの場合、IMSI、MSID、ルールベースなどの 4G セッションに適用されるオプションは、2G および 3G セッションにも適用されます。

# 2G および 3G サポートのための S4-SGSN MBR およびハンドオーバー手順

この機能は、コンバージドコアを強化し、2G（GERAN）および 3G（UTRAN）ネットワークで動作する UE のモビリティとセッション継続性を提供します。ユーザーの場所の更新を管理するためのベアラー要求の変更（MBR）の処理に焦点を当てており、ユーザーが異なる RAT 間を移動するときに中断のないサービスを保証するためのさまざまな引き継ぎシナリオをサポートしています。

以下は、SMF での S4-SGSN の MBR および引き継ぎの手順のリストです。

- ユーザーの場所の更新処理（MBR）
- RAT 間ハンドオーバーのサポート（4G/LTE <=> 2G/3G）
- 専用ベアラーの処理
- RAT 内ハンドオーバーのサポート（2G/3G）

### 制限付き S4-SGSN ハンドオーバー

SMF での制限付き S4-SGSN ハンドオーバーサポートのリストを次に示します。

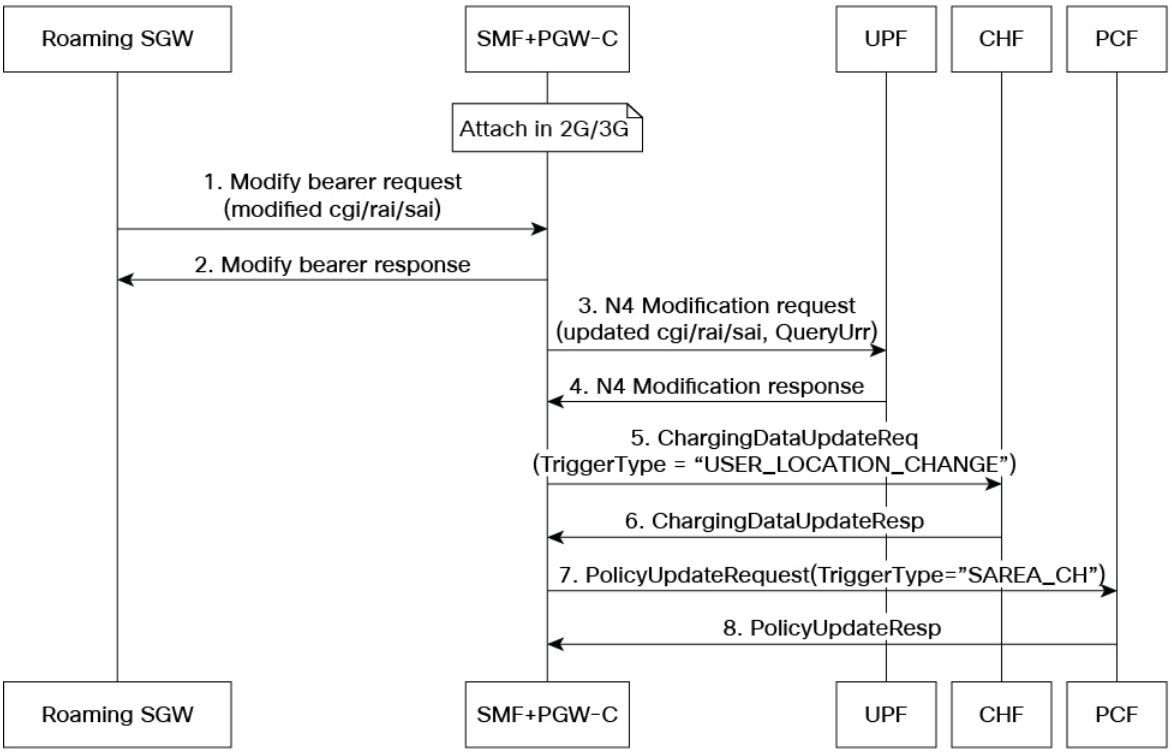
- UE 接続が 2G/3G アクセスタイプである場合、5G への直接および間接ハンドオーバーとその逆は、 サービスがサポートされていない という理由で拒否されます。指定されたハンドオーバーはサポートされていません。
  - 2G/3G -> 5G
  - 5G->2G/3G
  - 5G->4G->2G/3G
  - 2G/3G->4G->5G
- 2G/3GからWi-Fiおよびその逆の直接ハンドオーバーはサポートされていません。2G/3G->4G->Wi-Fiおよびその逆などの間接的なハンドオーバーがサポートされています。
- SMF は、2G/3G ハンドオーバーを処理するときに、ModifyBearerRequest 内のハンドオーバー通知フラグを無視します。
- 接続手順中に 2G/3G CLI が有効になっていない場合、2G/3G へのハンドオーバーは拒否されます。
- 以前のリリース 2025.2.0 バージョンで 4G セッションが確立されている場合、2G/3G へのハンドオーバーは拒否されます。

## ユーザーのロケーション変更のための MBR 手順

このコールフローは、S4-SGSN のユーザーの場所の変更に対する MBR 手順を示しています。

**process_workflow**

図 *288 : ULI* 変更に対する *MBR*




次の手順では、SMF での MBR のプロセスの段階的な説明を示します。

1. SMF で 2G/3G が正常にアタッチされると、SMF は、変更された `cgi/rai/rai` 値を含む ModifyBearerRequest メッセージを受信します。
2. SMF は、ベアラー応答の変更を S-GW に送信します。
3. SMF は次の値とともに N4ModificationRequest メッセージを送信します。
   - `cgi/rai/rai` を更新した`PFCP_IE_SUB_PARAMS`。
   - トリガーが設定された URR に送信される`PFCP_IE_QUERY_URR` 。
4. SMF は使用状況レポートを含む N4ModificationResponse メッセージを受信します。
5. SMF は、次の値を含む ChargingDataUpdateRequest メッセージを CHF に送信します。
   - RAT_CHANGE としての `TriggerType`。
   - E-UTRAN RAT タイプの `MultipleUnitUsage`。
   - UTRAN RAT タイプの `PDUSessionChargingInformation`。
6. SMF は CHF から ChargingDataUpdateResponse メッセージを受信します。
7. SMF は、SAREA_CH を含む PolicyUpdateRequest メッセージを送信します。

8. SMF は PCF から PolicyUpdateSuccess メッセージを受信します。

（注） コール フローは、2G RAT タイプと同様です。

## S4-SGSN RAT 間ハンドオーバーの手順

このセクションでは、ホームとローミングのシナリオでの 4G と 2G/3G 間のハンドオーバーについて説明します。

次の手順は、S4-SGSN での RAT 間ハンドオーバーの一部として説明されています。

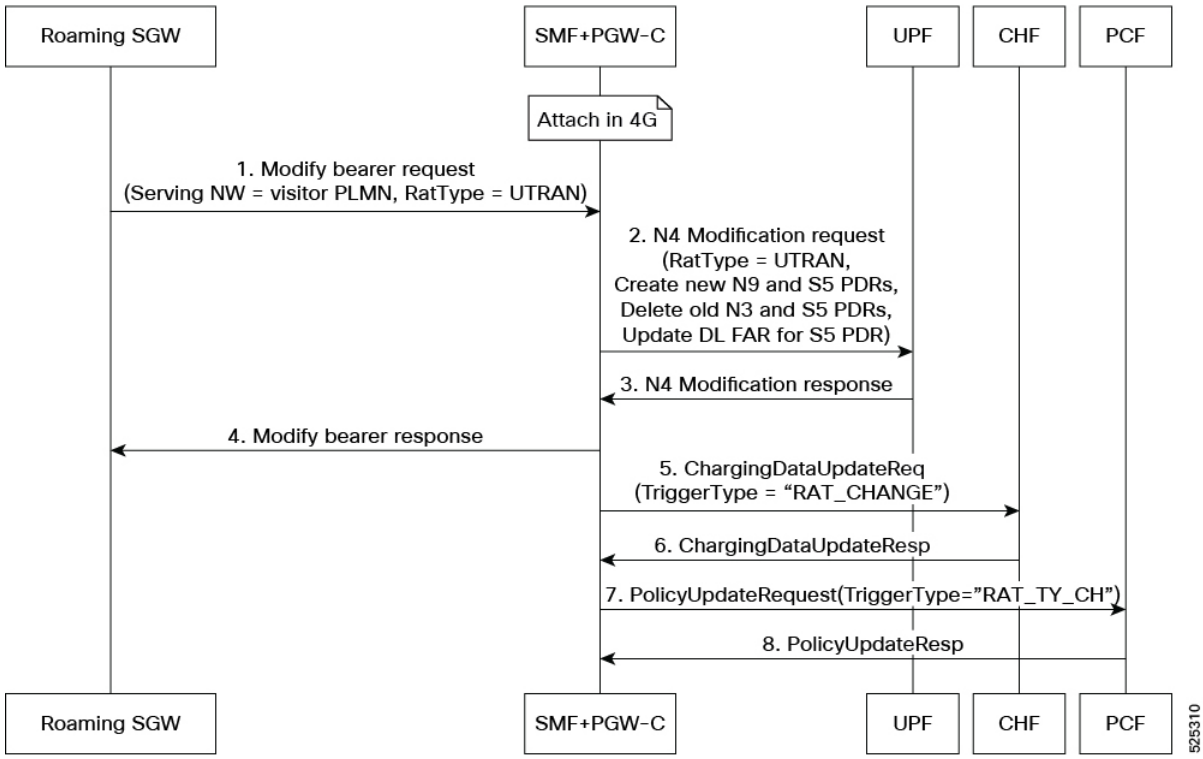
- 4G ホーマーから 3G ローマーへのハンドオーバー
- 3G ホーマーから 4G ローマーへのハンドオーバー
- 4G ローマーから 3G ホーマーへのハンドオーバー
- 3G ローマーから 4G ホーマーへのハンドオーバー

### 4G ホーマーから 3G ローマーへ

このコール フローは、S4-SGSN での 4G ホームから 3G ローミングへの inter-Rat ハンドオーバー シナリオを示しています。

### process_workflow

図 *289 : 4G* ホーマーから *3G* ローマーへ




次の手順では、SMF での 4G ホームから 3G ローマへの RAT 間ハンドオーバーのプロセスについて、順を追って説明します：

1. SMF で 4G が正常にアタッチされると、SMF は次の値の ModifyBearerRequest メッセージを受信します。
   - サービング NW 内のビジター PLMN
   - RAT タイプ UTRAN
   - 変更済みターゲットGTP-U TeID
2. SMF は次の値とともに N4ModificationRequest メッセージを送信します。
   - `ratType = 1(UTRAN)` と `roaming_status = 4(ROMER)` を伴う `PFCP_IE_SUB_PARAMS` 。
   - N9 および S5 PDR を作成します。
   - N3 および S5 PDR を削除します。
   - `external_header_creation` で `forw` アクションが設定され、ターゲット TeID になっている DL S5 FAR を更新します。
   - オンラインとオフライン URR の`Query_interface`。

3. SMF は使用状況レポートを含む N4ModificationResponse メッセージを受信します。
4. SMF は、次の値を含む ChargingDataUpdateRequest メッセージを CHF に送信します。
   - RAT_CHANGE としての `TriggerType`。
   - E-UTRAN RAT タイプの `MultipleUnitUsage`。
   - UTRAN RAT タイプの `PDUSessionChargingInformation`。
5. SMF は CHF から ChargingDataUpdateResponse メッセージを受信します。
6. SMF は、RAT_TY_CH および RAT タイプ UTRAN として `repPolicyCtrlReqTriggers` を含む PolicyUpdateRequest メッセージを送信します。
7. SMF は PCF から PolicyUpdateSuccess メッセージを受信します。

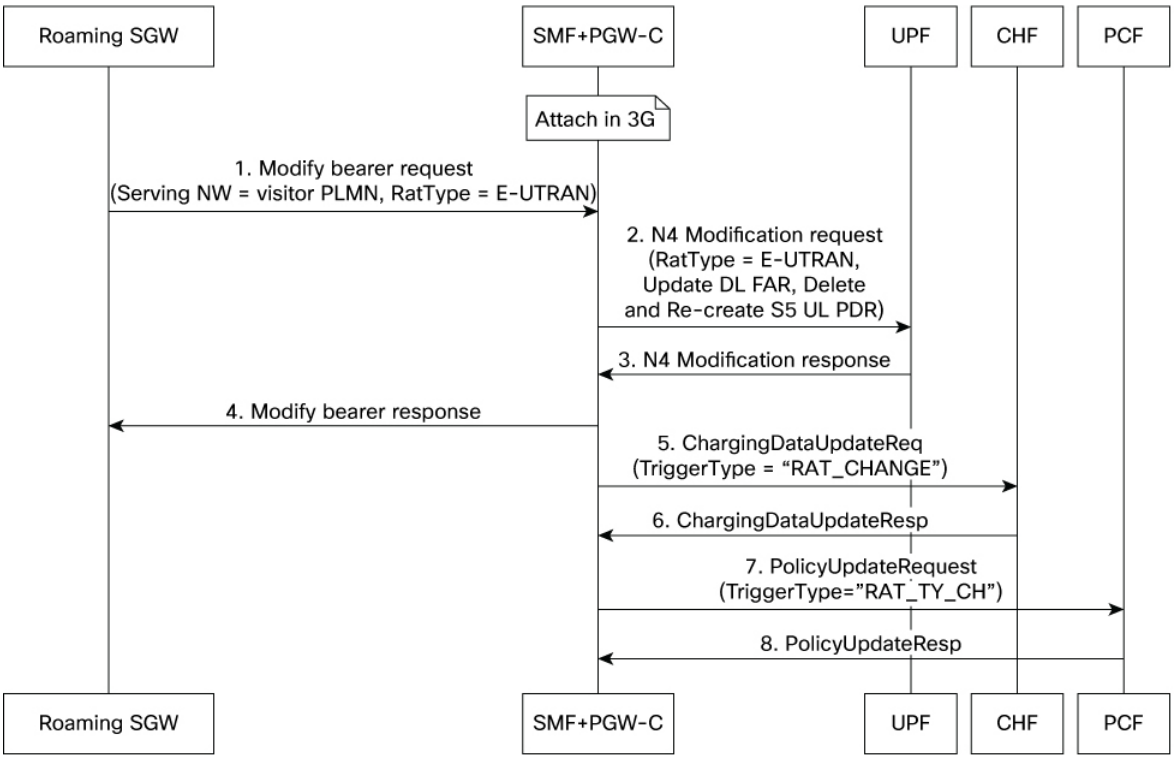
（注） コール フローは、RAT タイプが 2G ネットワークの GERAN になる 4G ホームと 2G ローミングのシナリオで似ています。

## 3G ホーマーから 4G ローマー

このコールフローは、S4-SGSN での 3G ホーマーから 4G ローマーへの inter-Rat ハンドオーバーシナリオを示しています。

### process_workflow

図 *290 : 3G* ホーマーから *4G* ローマー




次の手順では、SMF での 3G ホーマーから 4G ローマーへの RAT 間ハンドオーバーのプロセスについて、順を追って説明します。

1. SMF で 4G が正常にアタッチされると、SMF は次の値の ModifyBearerRequest メッセージを受信します。
   - サービング NW 内のビジター PLMN
   - RAT タイプ E-UTRAN
   - 変更済みターゲットGTP-U TeID
2. SMF は次の値とともに N4ModificationRequest メッセージを送信します。
   - `ratType = 1(UTRAN)` と `roaming_status = 4(ROMER)` を伴う `PFCP_IE_SUB_PARAMS` 。
   - S5 UL PDR の削除
   - S5 UL PDR の再作成
   - `external_header_creation` で `forw` アクションが設定され、ターゲット TeID になっている DL S5 FAR を更新します。
   - オンラインとオフライン URR の `Query_interface`。

3G 接続中にセカンダリ PDR が作成されません。

3. SMF は使用状況レポートを含む N4ModificationResponse メッセージを受信します。
4. SMF は、次の値を含む ChargingDataUpdateRequest メッセージを CHF に送信します。
   - RAT_CHANGE としての `TriggerType`。
   - E-UTRAN RAT タイプの `MultipleUnitUsage`。
   - UTRAN RAT タイプの `PDUSessionChargingInformation`。
5. SMF は CHF から ChargingDataUpdateResponse メッセージを受信します。
6. SMF は、RAT_TY_CH および RAT タイプ UTRAN として `repPolicyCtrlReqTriggers` を含む PolicyUpdateRequest メッセージを送信します。
7. SMF は PCF から PolicyUpdateSuccess メッセージを受信します。

（注） コール フローは、対応する RAT タイプとターゲットのローミング ステータスを持つ次のケースで同様です。

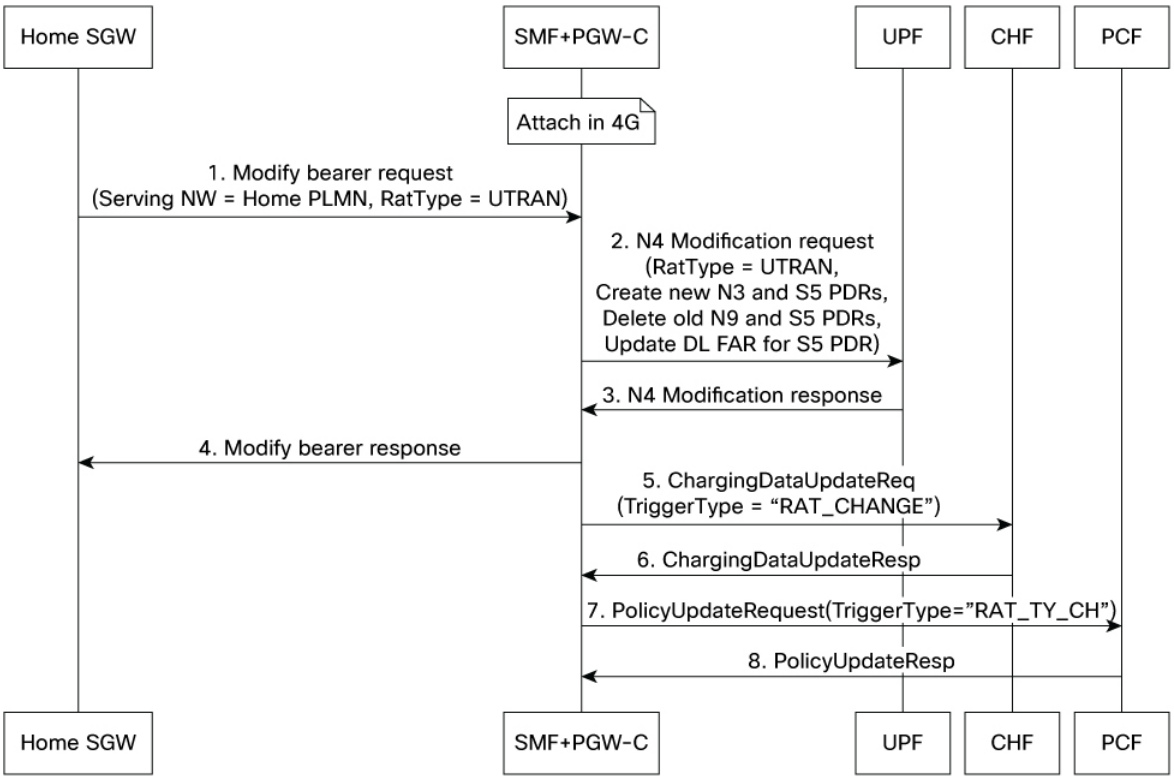
- 2G ホーマーから 4G ローマー
- 2G ホーマーから 3G ローマー
- 3G ローマーから 2G ホーマー

## 4G ローマーから 3G ホーマーへ

このコール フローは、S4-SGSN での 4G ローマーから 3G ホーマー シナリオへの Rad 間ハンドオーバーを示しています。

### process_workflow

図 *291 : 4G* ローマーから *3G* ホーマーへ




次の手順では、SMF での 4G ローマーから 3G ホーマーへの RAT 間ハンドオーバーのプロセスについて、順を追って説明します：

1. SMF で 4G の接続が正常に完了すると、SMF は次の値を含む ModifyBearerRequest メッセージを受信します：
   - サービング NW のホーマー PLMN
   - RAT タイプ UTRAN
   - 変更済みターゲットGTP-U TeID
2. SMF は次の値とともに N4ModificationRequest メッセージを送信します。
   - `PFCP_IE_SUB_PARAMS` with `ratType = 1(UTRAN)` and `roaming_status = 1(HOMER).`
   - N3 および S5 PDR を作成します。
   - N9 および S5 PDR を削除します。
   - `external_header_creation` で `forw` アクションが設定され、ターゲット TeID になっている DL S5 FAR を更新します。
   - オンラインとオフライン URR の`Query_interface`。

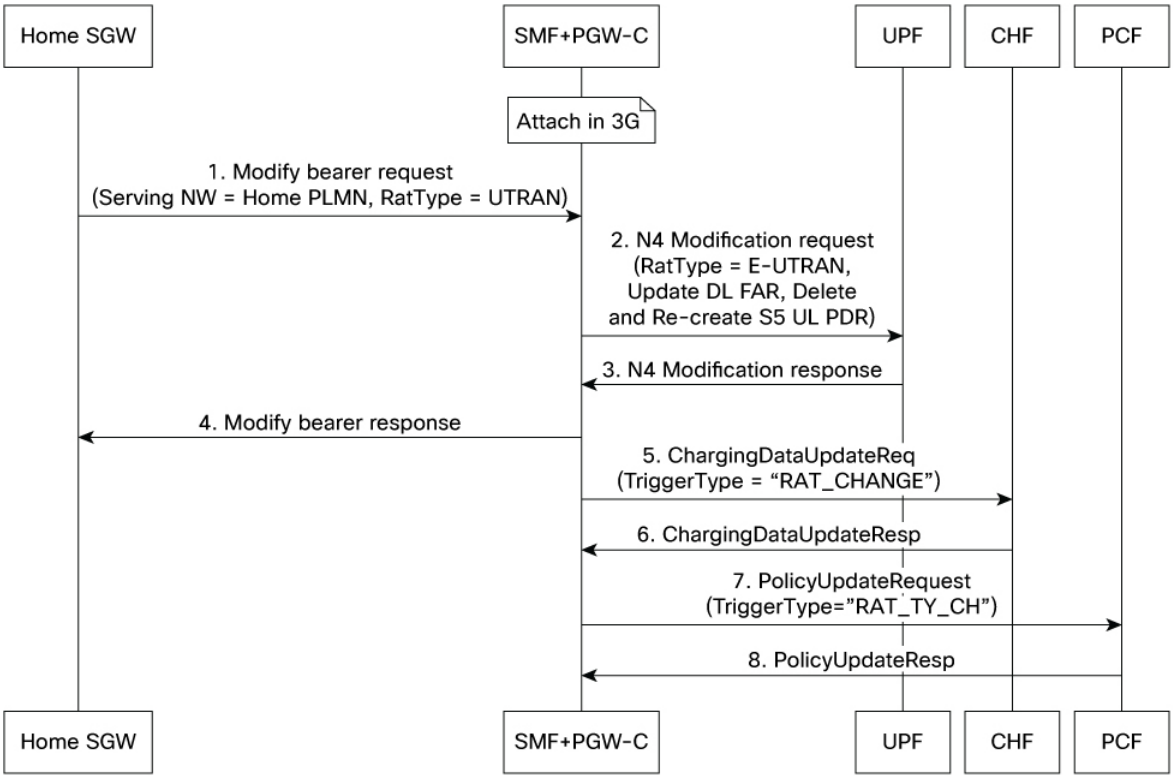
3. SMF は使用状況レポートを含む N4ModificationResponse メッセージを受信します。
4. SMF は、次の値を含む ChargingDataUpdateRequest メッセージを CHF に送信します。
   - RAT_CHANGE としての `TriggerType`。
   - E-UTRAN RAT タイプの `MultipleUnitUsage`。
   - UTRAN RAT タイプの `PDUSessionChargingInformation`。
5. SMF は CHF から ChargingDataUpdateResponse メッセージを受信します。
6. SMF は、RAT_TY_CH および RAT タイプ E-UTRAN として `repPolicyCtrlReqTriggers` とともに PolicyUpdateRequest を送信します。
7. SMF は PCF から PolicyUpdateSuccess メッセージを受信します。

（注） コール フローは、RAT タイプが 2G ネットワークの GERAN になる、4G ローマーと 2G ホーマー シナリオで同様です。

## 3G ローマーから 4G ホーマーへのハンドオーバー

このコールフローは、S4-SGSN での 3G ローマーから 4G ホーマーへの inter-Rat ハンドオーバー シナリオを示しています。

図 *292 : 3G* ローマーから *4H* ホーマー




次の手順では、SMF での 3G ローマーから 4G ホーマーへの RAT 間ハンドオーバーのプロセスについて、順を追って説明します。

1. SMF で 3G が正常にアタッチされると、SMF は次の値の ModifyBearerRequest メッセージを受信します。
   - サービング NW のホーマー PLMN
   - RAT タイプ E-UTRAN
   - 変更済みターゲットGTP-U TeID
2. SMF は次の値とともに N4ModificationRequest メッセージを送信します。
   - `ratType = 6(UTRAN)` および `roaming_status = 1(HOMER)` を持つ `PFCP_IE_SUB_PARAMS`。
   - S5 UL PDR を削除します。
   - S5 UL PDR の作成
   - `external_header_creation` で `forw` アクションが設定され、ターゲット TeID になっている DL S5 FAR を更新します。
   - オンラインとオフライン URR の`Query_interface`。
3. SMF は使用状況レポートを含む N4ModificationResponse メッセージを受信します。

4. SMF は、次の値を含む ChargingDataUpdateRequest メッセージを CHF に送信します。
   - RAT_CHANGE としての `TriggerType`。
   - E-UTRAN RAT タイプの `MultipleUnitUsage`。
   - UTRAN RAT タイプの `PDUSessionChargingInformation`。
5. SMF は CHF から ChargingDataUpdateResponse メッセージを受信します。
6. SMF は、RAT_TY_CH および RAT タイプ E-UTRAN として `repPolicyCtrlReqTriggers` とともに PolicyUpdateRequest を送信します。
7. SMF は PCF から PolicyUpdateSuccess メッセージを受信します。

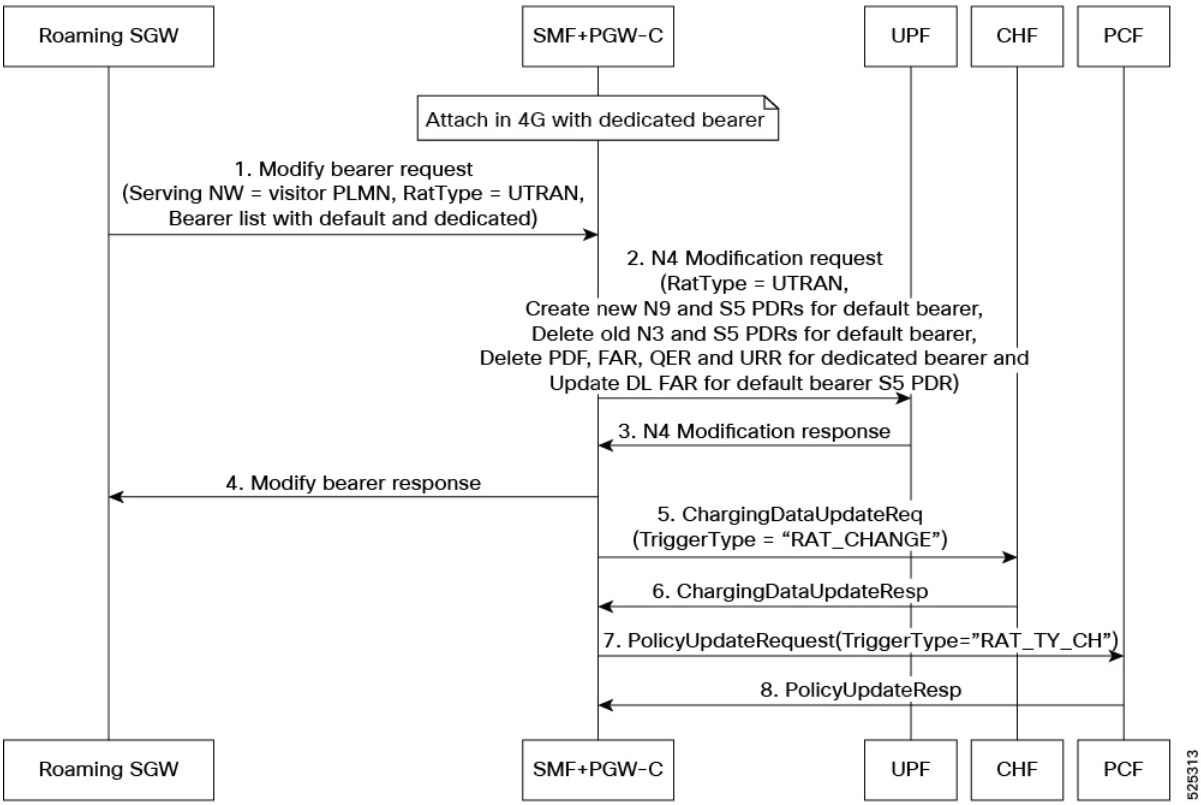
（注） コール フローは、RAT タイプが 2G ネットワークの GERAN になる 4G ローミングのシナリオと 4G ホームのシナリオで同様です。

## S4-SGSN での専用ベアラーによるハンドオーバー手順

このコール フローは、S4-SGSN での 4G ホームから 3G ローマーへのシナリオにおいて、専用ベアラを使用したハンドオーバー手順を示しています。

### process_workflow

図 *293 : 4G* ホームから *3G* ローマへの専用ベアラ ハンドオーバー




次の手順では、SMF での 4G ホームから 3G ローマへのシナリオにおいて、専用ベアラを使用したハンドオーバーの手順のプロセスを順を追って説明します。

1. SMF で 4G の専用ベアラとの接続が正常に完了すると、SMF は次の値を含む ModifyBearerRequest メッセージを受信します。
   - サービング NW 内のビジター PLMN
   - RAT タイプ UTRAN
   - 変更済みターゲットGTP-U TeID
   - デフォルトおよび専用ベアラによるベアラ リスト
2. SMF は次の値とともに N4ModificationRequest メッセージを送信します。
   - `ratType = 1(UTRAN)` と `roaming_status = 4(ROMER)` を伴う `PFCP_IE_SUB_PARAMS` 。
   - デフォルトのベアラ用に N9 および S5 PDR を作成します。
   - デフォルトのベアラの N3 および S5 PDR を削除します。
   - `external_header_creation` で `forw`アクションが設定され、ターゲット TeID になっているデフォルト ベアラの DL S5 FAR を更新します。

- オンラインとオフライン URR の`Query_interface`。

3. SMF は使用状況レポートを含む N4ModificationResponse メッセージを受信します。
4. SMF は、次の値を含む ChargingDataUpdateRequest メッセージを CHF に送信します。
   - RAT_CHANGE としての `TriggerType`。
   - E-UTRAN RAT タイプの `MultipleUnitUsage`。
   - UTRAN RAT タイプの `PDUSessionChargingInformation`。
5. SMF は CHF から ChargingDataUpdateResponse メッセージを受信します。
6. SMF は、RAT_TY_CH および RAT タイプ UTRAN として `repPolicyCtrlReqTriggers` を含む PolicyUpdateRequest メッセージを送信します。
7. SMF は PCF から PolicyUpdateSuccess メッセージを受信します。

（注） このコール フローでは、次のことが実行されます。

- ベアラ リストにデフォルトのベアラのみが含まれている ModifyBearerRequest メッセージを受信した場合、デフォルトのベアラは処理され、N4ModificationRequest メッセージで削除 PDR、QER、FAR、URR が送信され、専用ベアラが削除されます。
- 専用ベアラのみが受信された場合は、MBR は拒否されます。

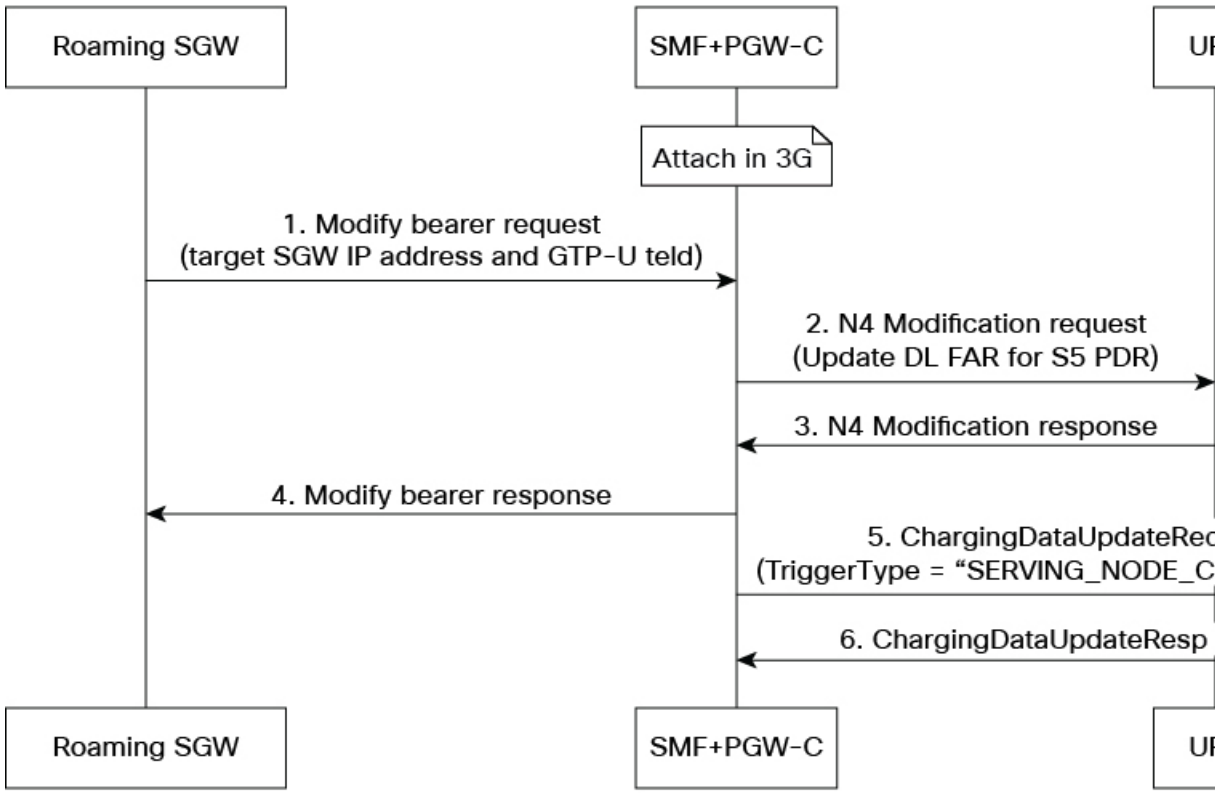
コール フローは、RAT タイプが 2G ネットワークの GERAN になる 2G ローミングの専用ベアラを使用する 4G ホームで同様です。

## S4-SGSN の RAT 内ハンドオーバー

このコール フローは、3G ネットワークでの SGW ハンドオーバーを示しています。

**process_workflow**

図 *294 : 3G* での *SGW* のハンドオーバー




次の手順では、SMF での 3G ネットワークの SGW ハンドオーバーのプロセスを段階的に説明します。

1. SMF で 3G が正常にアタッチされると、SMF は、ターゲット SGW GTP-U `teid` および IP アドレス値を含むベアラー要求の変更メッセージを受信します。
2. SMF は次の値とともに N4ModificationRequest メッセージを送信します。
   - `forw` アクションを設定し、 `outer_header_creation` でターゲット SGW `teid`と IP アドレスを使用して DL S5 FAR を更新します。
   - オンラインとオフライン URR の `Query_interface`。
3. SMF は使用状況レポートを含む N4ModificationResponse メッセージを受信します。
4. SMF は、次の値を含む ChargingDataUpdateRequest メッセージを CHF に送信します。
   - SERVING_NODE_CHANGE としての `TriggerType`。
   - E-UTRAN RAT タイプの `MultipleUnitUsage`。
   - UTRAN RAT タイプの `PDUSessionChargingInformation`。
5. SMF は CHF から ChargingDataUpdateResponse メッセージを受信します。

# コンバージド コアにおける S4-SGSN 向けのダイナミック QoS の変更

この機能により、コンバージド コア内で S4-SGSN を使用する 2G および 3G サブスクライバの QoS ネゴシエーション機能が導入されます。これにより、HLR または PCF から発信されるトリガに基づいて、デフォルトのベアラーの QoS パラメータをダイナミックかつ自動で調整できます。

QoS 変更機能の主な機能は次のとおりです。

- HSS によって開始される QoS の変更
- HSS によって開始される QoS の変更

### QoS ネゴシエーションの制限事項

デフォルト ベアラーの QoS ネゴシエーションの制限は次のとおりです。

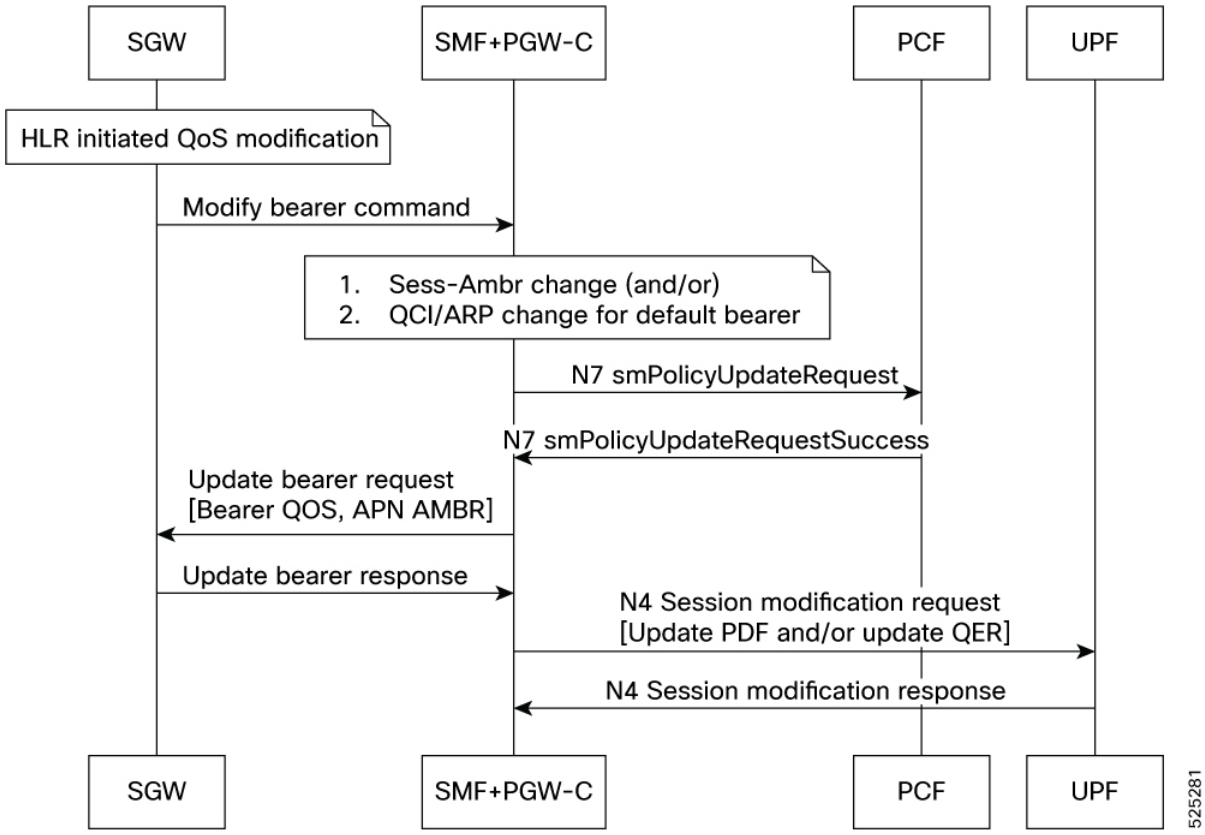
- デフォルト ベアラーの HLR または PCF が開始した QoS の変更は、QCI/ARP の変更または Sess-AMBR の変更に対してのみ許可されます。その他のパラメータは変更できません。
- 専用ベアラーは 2G/3G セッションではサポートされていないため、専用ベアラーの QoS ネゴシエーションは適用されません。
- HLR が開始した QoS 変更の一環として受信した [ベアラー コマンドの変更（Modify Bearer Command）] では、非標準 QCI のみがサポートされます。PCF から受信した非標準 QCI の既存のサポートは変わりません。

## HSS によって開始される QoS の変更

### process_summary

このコール フローは、SMF での HLR によって開始される QoS 変更プロセスを示しています。

図 *295 : HSS* によって開始される *QoS* の変更




**process_workflow**

以下の手順は、SMF での HLR によって開始される QoS 変更の段階的なプロセスから構成されます。

1. S4-SGSN は、HLR によって開始された QoS パラメータの更新に応答して、SGW にベアラーの変更コマンドを送信します。デフォルトのベアラー QoS の変更のサポートは制限されます。このプロセスでは、デフォルトのベアラー QoS の変更だけをサポートします。
2. SMF は、SESS_AMBR または QOS_CH 値を使用して Npcf_SMPolicyControl_Update メッセージを PCF に送信します。
   - QoS の変更の場合、SMF は DEF_QOS_CH 値を repPolicyCtrlReqTriggers 属性内に含め、新しいサブスクライブされたデフォルト QoS を subsDefQos 属性内に含めます。
   - Sess-AMBR の変更の場合、SMF は SE_AMBR_CH を repPolicyCtrlReqTriggers 属性内に含め、新しい Session-AMBR を subsSessAmbr 属性内に含めます。
3. PCF は、新しい承認されたセッション AMBR と承認されたデフォルト QoS を、応答の SMF にプロビジョニングします。
4. QCI/ARP 値が変更された場合、SMF は、変更された APN-AMBR および/または EPS ベアラー QoS とともに、ベアラー要求の更新メッセージを SGW に送信します。

5. S-GW から正常な [Update Bearer Response] メッセージを受信した後、SMF は [Update-PDR] や [Update-QER] の値で N4 変更をトリガーします。
6. ベアラーの変更が失敗した場合、SMF はエラー処理タイプ（FHT）に基づいてアクションを実行します。
7. このシナリオでは、4G セッションと同様に、procedure_type mme_req_ded_brr_mod および適切な rate_type を持つ既存の smf_service_stats メトリックがペグされます。

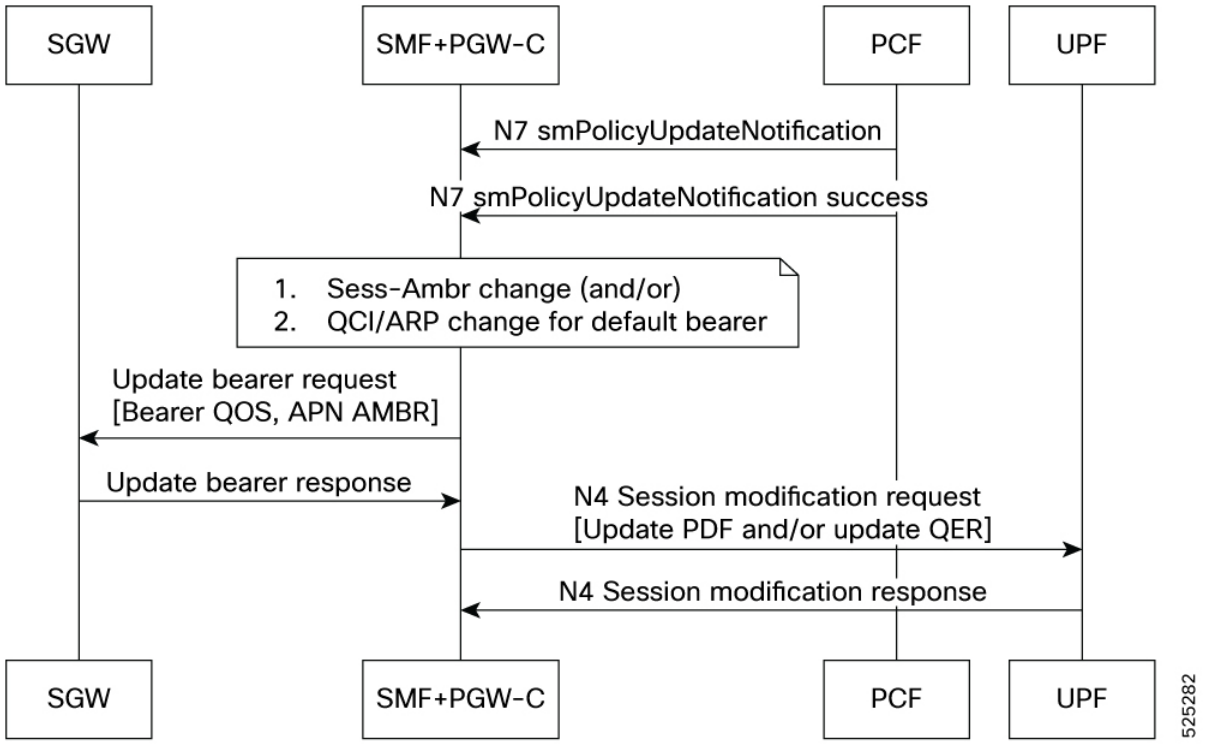
（注） 示されているように、HLR によって開始された QoS 変更時に DEF_QOS_CH および SE_AMBR_CH PCF トリガーが送信されます。ただし、他のシナリオではサポートされていません。

## HSS によって開始される QoS の変更

このコール フローは、SMF での PCF によって開始された QoS 変更プロセスを示しています。

**process_workflow**

図 *296 : HSS* によって開始される *QoS* の変更




次に、SMF での PCF によって開始される QoS 変更の段階的なプロセスの手順を示します。

1. QoS パラメータの PCF によって開始された通知の更新は、デフォルトのベアラーでサポートされます。

   SMF は PCF から通知更新を受信すると、QCI/ARP が変更された場合は、変更された APN-AMBR 値や EPS ベアラー QoS 値を使用して、ベアラー要求の更新メッセージを SGW に送信します。

2. S-GW から正常な [ベアラー応答の更新（Update Bearer Response）] メッセージを受信した後、SMF は [Update-PDR] や [Update-QER] の値で N4 変更をトリガします。

3. ベアラーの変更が失敗した場合、SMF はエラー処理タイプ（FHT）に基づいてアクションを実行します。

（注） 4G セッションの場合、SMF は UBR または N4 の障害時に PCF に通知を送信しません。同じ動作が、PCF によって開始された QoS 変更と HLR によって開始された QoS 変更の両方の 2G/3G セッションに適用されます。

## S4-SGSN PCF によって開始された変更

### process_workflow

S4-SGSN PCF によって開始された変更では、PCF によって開始された通知の更新は、既存の 4G 実装とともにデフォルトのベアラーに対してサポートされます。EventTrace の 2g/3g プロシージャに新しい ProcedureType が追加されました。専用ベアラー操作は 2g/3g ではサポートされていません

次の手順障害ログタグが追加されています。

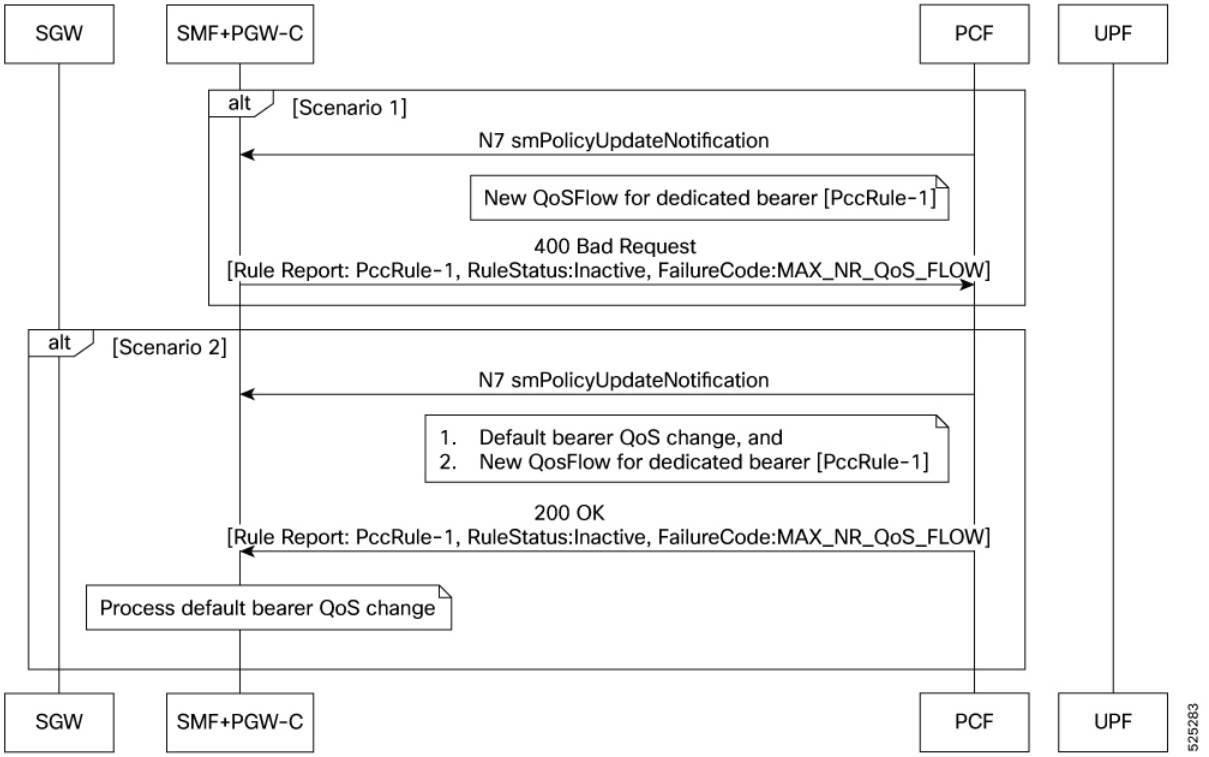
- 3gbrrmod-procfailure
- 2gbrrmod-procfailure

専用ベアラーの作成/変更/削除は、2G/3G セッションではサポートされていません。SMF は、次の図に示すように、専用ベアラの作成を必要とする PCC ルールの追加を拒否します。

### 専用ベアラー拒否の処理

このコール フローは、SMF での専用ベアラー拒否の処理を示しています。

図 *297 : S4-SGSN PCF* によって開始された変更




専用ベアラーの作成が拒否されると、HTTP ステータス コード 400 が MAX_NR_QoS_Flow として障害コードを含む RuleReport とともに送信されます。

（注）

1. 専用ベアラー拒否処理の所定のコール フローは、PCF からの SmPolicyUpdateNotification メッセージのシナリオを示しています。同様の拒否処理が、SmPolicyCreateResponse または SmPolicyUpdateResponse メッセージで、新しい専用ベアラーなどの新しい QoS フローの PccRules 値を送信する場合にも、同様の拒否処理が行われます。この場合、RuleReports 値を持つ SmPolicyUpdateReq メッセージがトリガされます。
   - PDN セットアップ時に SmPolicyCreateRsp/ SmPolicyUpdateResponse メッセージで新しい PccRule を受信すると（ピギーバック専用ベアラー シナリオ）、PDN セットアップ完了後にルール レポートがトリガされます。
2. SmPolicyUpdateNotification 中に、PCF 応答に対して Expedit CLI が有効になっている場合、これらの RuleReports は SmPolicyUpdateNotificationResp メッセージではなく、SmPolicyUpdateReq メッセージで送信されます。

手順タイプ pcf_req_ded_brr_create を持つ既存の smf_service_stats は、障害ステータスと理由が「oper_not_supported_in_rat」としてペグされます。QCI 値を含むラベル qos_5qi は、このような拒否シナリオでは入力されません。

# GTPv1 SGSN の接続と切断の手順コール フロー

この機能では、GTPv1 SGSN のアタッチおよびデタッチ手順のサポートについて説明します。GTPv1 メッセージおよび情報要素は、SMF で処理できるように同等の GTPv2 メッセージおよび情報要素に変換されます。

2G および 3G サポートの一環として、SMF には Gn インターフェイスをサポートする機能が必要です。SMF は、S5 として公開された同じインターフェイス（サービス IP）で GTPv1 メッセージを受信します。

この機能では、次の GTPv1 メッセージがサポートされています。

- PDP コンテキスト作成要求
- PDP コンテキスト応答の作成
- PDP コンテキスト削除要求
- PDP コンテキスト応答の削除

接続と切断の手順については、SGSN を介した PDN 接続のコール フローと PDN 切断のコール フローを通じて説明します。

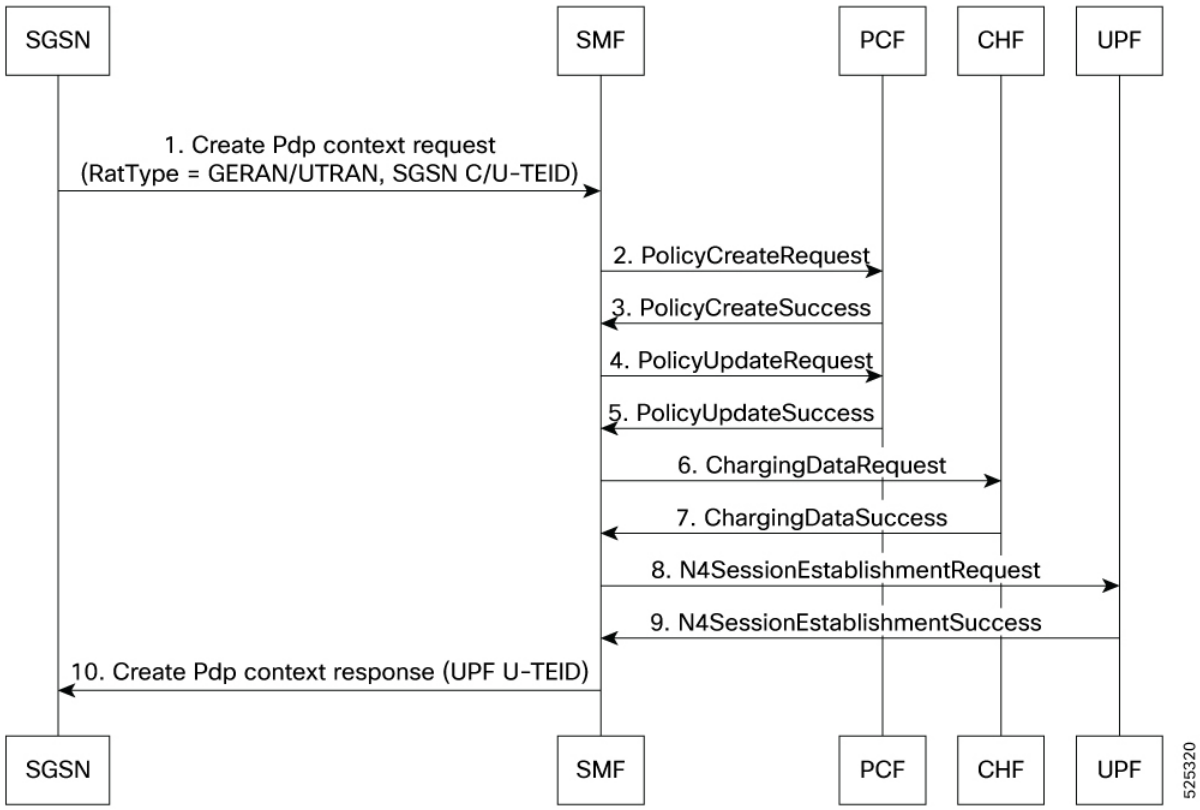
- PDN が SGSN 経由で切断
- PDN が SGSN 経由で切断

## PDN が SGSN 経由で切断

ここでは、SGSN を介した PDN 接続でのコールフローとステージについて説明します。

**process_workflow**

図 *298 : PDN* が *SGSN* 経由で切断




以下の段階は、SMF を介した GERAN および UTRAN への初期接続における SMF と他の NF 間の相互作用を説明しています。

1. SMF は、SGSN から次の値を持つ Create PDP Context Request メッセージを受信します。
   - RATタイプは、2G接続の場合はGERAN、3G接続の場合はUTRANです。
   - SGSN 制御
   - データTEID

   ULI には、次のいずれかの値が含まれます。
   - ルーティングエリア識別子（Rai）
   - サービスエリア識別子 (Sai)
   - セル グローバル識別子（Cgi）
   - サービス エリア識別子 + ルーティング エリア識別子
   - セル グローバル識別子 + ルーティング エリア識別子

2. SMF は PolicyCreateRequest メッセージを PCF に送信して、ポリシーの関連付けを確立します。
3. SMF は、ポリシー課金および制御情報を含む PolicyCreateSuccess メッセージを PCF から受信します。
4. UE IP アドレスが割り当てられ、SMF は、UE_IP_CH トリガーを使用して PolicyUpdateRequest を PCF に送信します。
5. SMF は PCF から PolicyUpdateSuccess メッセージを受信します。
6. SMF は PCF から受信した課金ポリシーに基づいて、CHF に向けて ChargingDataRequest メッセージを開始します。
7. SMF は CHF から ChargingDataSuccess メッセージを受信し、次の値を取得します。
   - セッションまたは RG レベルで CC がトリガーする
   - セッション レベルの時間またはボリュームの制限
   - RG レベルでの時間またはボリュームの制限
   - RG レベルのクォータ
8. SMF は、PDR、QER、FAR、URR に関連する情報を中継するために、UPF に向けて N4SessionEstablishmentRequest メッセージを送信します。
9. SMF は UPF から N4SessionEstablishmentSuccess メッセージを受信します。
10. SGSN は SMF から Create PDP Context Response（ベアラ制御モード値 2）を受信します。

## PDN が SGSN 経由で切断

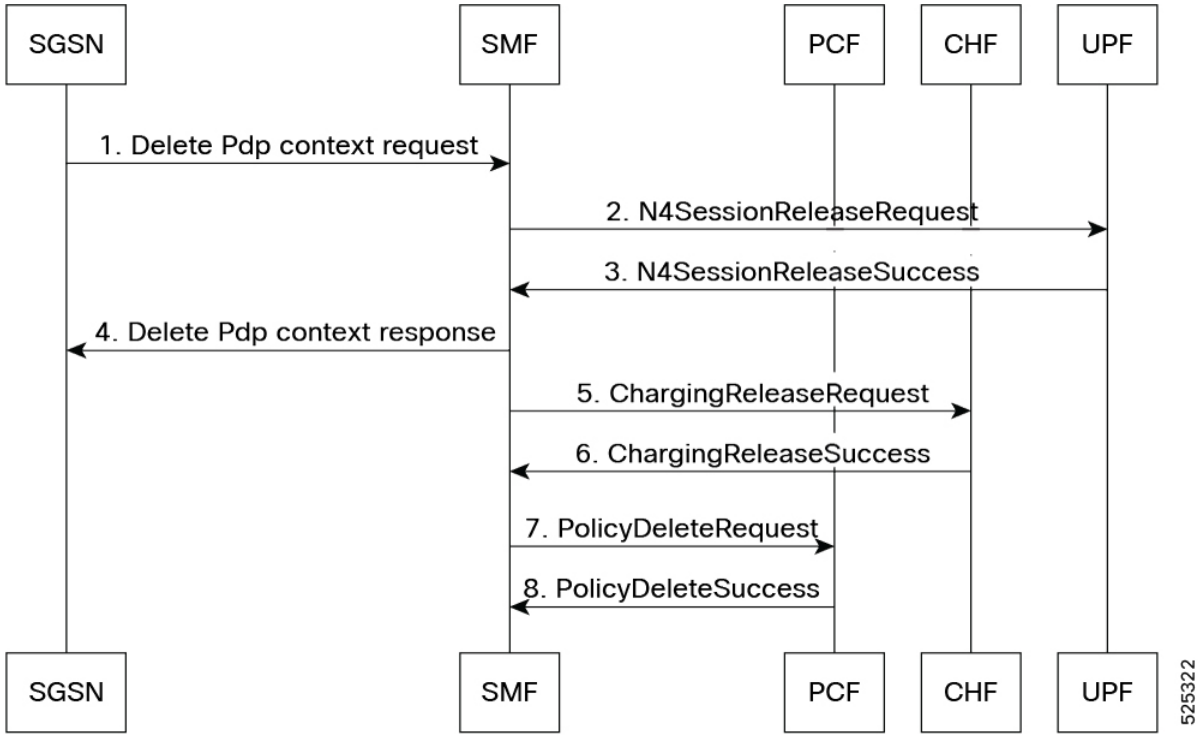
ここでは、SGSN を介した PDN 接続でのコール フローとステージについて説明します。

### SGSN の UE で開始されたリリース

このコール フローは、SGSN を介した PDN 切断のために UE が開始するリリースを示しています。

**process_workflow**

図 *299 : UE* が開始した *PDN* の切断




**process_summary**

次の手順では、SGSN を介した PDN 切断のために UE が開始したリリースについて説明します：

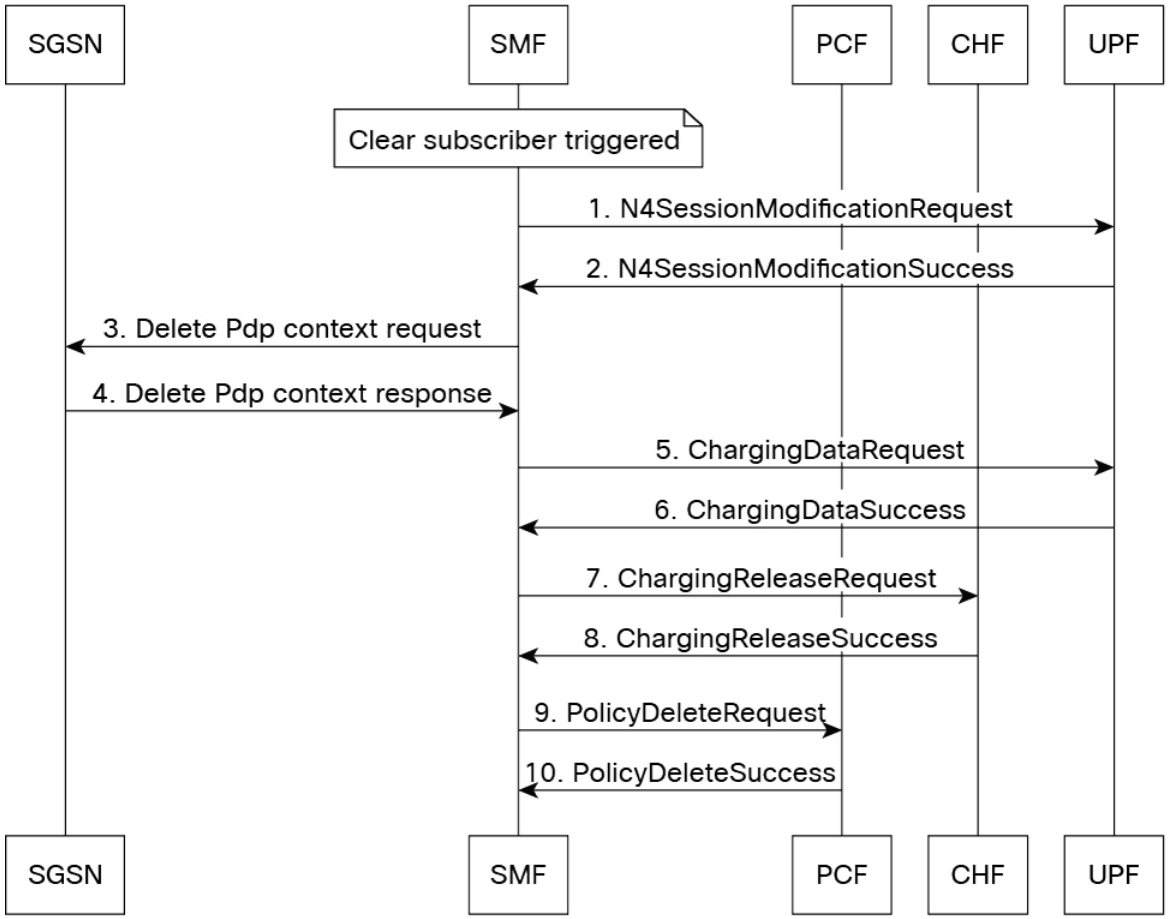
1. SMF は SGSN から「PDP コンテキストの削除要求」メッセージを受信します。
2. ユーザ プレーン リソースを削除するために SMF は、UPF に N4SessionReleaseRequest メッセージを送信します。
3. UPF からの最終使用とともに SMF は、N4SessionReleaseSuccess メッセージを受信します。
4. SGSN が SMF から Delete PDP Context Response メッセージを受信します。
5. SMF は、最終使用とともに CHF に ChargingReleaseRequest メッセージを送信します。
6. SMF は、CHF から ChargingReleaseSuccess メッセージを受信します。
7. SMF は、PolicyDeleteRequest メッセージを PCF に送信して、PCF へのポリシーの関連付けを削除します。
8. SMF は PCF から PolicyDeleteSuccess メッセージを受信します。

## SGSN の SMF で開始されたリリース

このコールフローは、SGSN を介した PDN 切断のために SMF が開始するリリースを示しています。

**process_workflow**

図 *300 : UE* が開始した *PDN* の切断




次の手順では、PDN 切断のために SMF によって開始されるリリースについて説明します。

1. SMF によって開始されたリリースは、Clear subscriber コマンドを使用してトリガーされます。SMF は、更新 FAR でドロップアクションが設定された N4SessionModificationRequest メッセージを送信します。
2. SMF が N4SessionModificationSuccess メッセージを受信します。
3. SMF は Delete PDP Context Request メッセージを SGSN に送信します。
4. SMF は SGSN から Delete PDP Context Response メッセージを受信します。
5. ユーザ プレーン リソースを削除するために SMF は、UPF に N4SessionReleaseRequest メッセージを送信します。

6. UPF からの最終使用とともに SMF は、N4SessionReleaseSuccess メッセージを受信します。
7. SMF は、最終使用とともに CHF に ChargingReleaseRequest メッセージを送信します。
8. SMF は、CHF から ChargingReleaseSuccess メッセージを受信します。
9. SMF は、PolicyDeleteRequest メッセージを PCF に送信して、PCF へのポリシーの関連付けを削除します。
10. SMF は PCF から PolicyDeleteSuccess メッセージを受信します。

# GTPv1 2G および 3G セッションの Show コマンド出力

## Show コマンドのサンプル出力

次に、GTPv1 メッセージ情報を含む **show subscriber** CLI コマンドの出力例を示します。

```
show subscriber supi imsi-123456789012345 nf-service smf full | exclude subscriber-details

{
  "subResponses": [
    {
      "status": true,
      "genericInfo": {
        "pduState": "pduState_None",
        "supi": "imsi-123456789012345",
        "pei": "imei-123456786666660",
        "pduSessionId": 69,
        "pduSesstype": "Ipv4PduSession",
        "accessType": "3GPP_ACCESS",
        "dnn": "intershat",
        "plmnId": {
          "mcc": "123",
          "mnc": "456"
        },
        "sScMode": 1,
        "uetimeZone": "+00:15",
        "allocatedIp": "12.0.4.0",
        "alwaysOn": "None",
        "dcnr": "Enabled",
        "wps": "Non-Wps Session",
        "ratType": "UTRA",
        "ueType": "4G Capable And NR Unknown UE",
        "sessTimeStamp": "2025-07-14 06:40:23.582495295 +0000 UTC",
        "callDuration": "5.743140999s",
        "ipPool": "poolv4",
        "commonId": 66,
        "linkedEbi": 5,
        "snssai": {
          "sd": "Abf123",
          "sst": 2
        },
        ...
        "ipAllocationBy": "Dynamic",
        "anType": "3GPP_ACCESS",
        "utranLocation": {
          "cgi": {
            "mcc": "123",
```

```
            "mnc": "456",
            "lac": "04d2",
            "cellId": "0004"
          },
          "rai": {
            "mcc": "123",
            "mnc": "456",
            "lac": "04d2",
            "rac": "22"
          },
          "ueLocationTimestamp": "2025-07-14T06:40:23Z"
        },
        "initialRatType": "UTRA"
      },
      ...    }
        ],
        "qosFlow": [
          {
            "qfi": 1,
            "GBRFlow": "False",
            "bindingParameters": {
              "x5Qi": 9,
              "arp": {
                "preemptCap": "NOT_PREEMPT",
                "preemptVuln": "PREEMPTABLE",
                "priorityLevel": 1
              },
              ...
            "startTime": "2025-07-14T06:40:23Z",
            "rulebase": "rba_charging_staticonly_offline",
            "chargingDisabled": "false",
            "dropTraffic": "false",
            "gtppGrp": "group1",
            "profileName": "chgprf1",
            "accountingEnabled": "false",
            "n40ChargingEnabled": "true",
            "qbcChargingEnabled": "false",
            "offlineConverted": "false",
            "chfGroupId": "CHF-dnn=intershat;",
            "chfChargDataRef": "1111",
            "bearerInctCharg": "false",
            "gyChargingEnabled": "false",
            "gzChargingEnabled": "false"
          }
        ]
      },
      ...
  "upfSeid": "17293822569102704642",
        "TotalNumberOfPdrs": "2 (Ul:1 Dl:1)",
        "TotalNumberOfFars": 2,
        "TotalNumberOfQers": 2
      },
      "access3GSubData": {
        "localTeid": 66,
        "lbi": 5,
        "bearerContexts": [
          {
            "ebi": 5,
            "defBrr": true,
            "dlFteid": {
              "teid": 1655,
              "ipaddr": "192.168.7.61"
            }
          }
```

```
        ],
        "sgsnAddr": {
          "sgsnIpv4Addr": "172.10.1.26"
        },
        "gtpVersion": "GtpV1"
      }
    }
  ]
}
```

# monitor subscriber CLI コマンドのサンプル出力

このセクションでは、SMF の GTPv1 メッセージに関連付けられた monitor subscriber CLI コマンドの出力例を示します。

## PDP コンテキスト要求メッセージ出力の作成

次に、monitor subscriber CLI コマンドの Create PDP Context Request メッセージ情報を表示する出力例を示します。

```
Subscriber Id: imsi-123456789012345
      Timestamp: 2025/02/27 11:37:03.690314
    Message: S5 S8 Create PDP Context Request
   Description: Create PDP Context Request Message displayed after decoding into Create
 Session Request Message Proto

      Source: 172.00.0.00

      Destination: 10.1.00.000

      PAYLOAD:
        S5 S8 Create PDP Context Request:

            S5 S8 Create PDP Context Request:

                Version: 1
      ...
                MsgType:
                   Create_Session_Request:
                       IMSI: 123456789012345
```

## PDP コンテキスト応答メッセージ出力の作成

次に、monitor subscriber CLI コマンドの Create PDP Context Response メッセージ情報を表示する出力例を示します。

```
Subscriber Id: imsi-123456789012345
         Timestamp: 2025/02/27 11:37:03.939684
      Message: S5 S8 Create PDP Context Response
      Description: Create PDP Context Response Message displayed after decoding into
Create Session Response Message Proto

      Source: 10.0.00.000
      Destination: 172.00.0.00
PAYLOAD:
       S5 S8 Create PDP Context Response:
          S5 S8 Create PDP Context Response:
                Version: 1
     ...
            MsgType:
```

```
                    Create_Session_Response:
                     Cause:
                         Cause_Value: 16
```

### PDP コンテキスト要求メッセージ出力の削除

次に、monitor subscriber CLI コマンドの Delete PDP Context Request メッセージ情報を表示する出力例を示します。

```
Subscriber Id: imsi-123456789012345
      Timestamp: 2025/02/27 11:37:14.149143
    Message: S5 S8 Delete PDP Context Request
    Description: SGSN Initiated Delete PDP Context Request Message
displayed after decoding into Delete Session Request Message Proto
      Source: 172.00.0.00

      Destination: 10.1.00.000

      PAYLOAD:
        S5 S8 Delete PDP Context Request:

            S5 S8 Delete PDP Context Request:

                Version: 1
      ...
                MsgType:
                   Delete_Session_Request:
                       Linked_EBI:
                            Value: 6
```

### PDP コンテキスト応答メッセージ出力の削除

次に、monitor subscriber CLI コマンドの Delete PDP Context Response メッセージ情報を表示する出力例を示します。

```
Subscriber Id: imsi-123456789012345
      Timestamp: 2025/02/27 11:37:14.187506
    Message: S5 S8 Delete PDP Context Response
    Description: SGSN Initiated Delete PDP Context Response Message
displayed after decoding into Delete Session Response Message Proto
      Source: 172.00.0.00

      Destination: 10.1.00.000

      PAYLOAD:
        S5 S8 Delete PDP Context Response:

            S5 S8 Delete PDP Context Response:

                Version: 1
      ...
                MsgType:
                   Delete_Session_Response:
                       Cause:
                           Cause_Value: 16
```

# 2G および 3G セッションの統計

これらのバルク統計情報を使用して、2Gおよび3Gセッションのモニタリング、分析、およびトラブルシューティングを行うことができます。

表 *487 : 2G* セッションおよび *3G* セッションのメトリック

| メトリック | ラベル情報 |
|---|---|
| smf_gtpc_msg_stats | このカウンタは、SGWからアクセス要求メッセージが受信されるたびに増加します。<br>• app_name < *app_name*><br>• cluster <*cluster*><br>• data_center <*data_center*><br>• dnn <*dnn*><br>• gr_instance_id < *gr_instance_id*><br>• instance_id <*instance_id*><br>• message_type <*message_name*><br>• qos_5qi <*qci*><br>• rat_type <*rat_type*><br>*rate_type* の 値は、2G/3G の Gera または UTRA のいずれかにする必要があります。 |
| • smf_service_stats<br>• smf_session_stats<br>• chf_message_stats<br>• chf_session_stats<br>• policy_msg_processing_status<br>• policy_pdu_flows_total<br>• smf_datacheck_stats<br>• smf_disconnect_stats<br>• smf_service_counters<br>• smf_service_resource_mgmt_stats<br>• smf_restep_http_msg_total | rat_type <*rat_type*><br>*rate_type* の値は、2G コールおよび 3G コールの場合、GEA または UTRA のいずれかです。 |

| メトリック | ラベル情報 |
|---|---|
| smf_session_counters | **fourg_only_ue** ラベルは、2G および 3G セッションの SessionID が 64 以上の場合、*fourg_only_ue:unknown* とマークされます。 |
| cdl show sessions summary | **fourg_only_ue** ラベルは、2G および 3G セッションの SessionID が 64 以上の場合、*fourg_only_ue:unknown* とマークされます。 |
| smf_service_stats | **fourg_only_ue** ラベルは、2G および 3G セッションの SessionID が 64 以上の場合、*fourg_only_ue:unknown* とマークされます。 |

2G および 3G セッションの GTPC メトリックは、次のとおりです。

表 ***488 : GTPC*** メトリック

| メトリック | ラベル情報 |
|---|---|
| gtpc_app_events | メトリックにバージョン（v1/v2）を追加しました。<br>*event_type* は、v1 メッセージを反映するように更新されます。 |
| gtpc_app_events_seconds | メトリックにバージョン（v1/v2）を追加しました。<br>*event_type* は、v1 メッセージを反映するように更新されます。 |
| gtpc_app_priority_events | メトリックにバージョン（v1/v2）を追加しました。<br>*event_type* は、v1 メッセージを反映するように更新されます。 |
| gtpc_app_total_unexpected_gtpc_msg_events | 失敗したメッセージのタイプとバージョンを追加しました。 |
| gtpc_msg_total | v1 メッセージ名をキャプチャします。 |
| gtpc_app_validation_events | v1 固有のメッセージ名、障害の種類、障害の理由、および拒否の原因をキャプチャします。 |
| gtpc_msg_seconds | v1 メッセージ名をキャプチャします。 |

| メトリック | ラベル情報 |
|---|---|
| gtpc_golang_enc_dec_stats | • *gtpc_msg_type* は v1 メッセージを反映するように更新されます。<br>• *gtpc_msg_status_cause* が更新され、v1 固有のエラーが表示されるようになりました。 |
| gtpc_echo_msg_stats | メトリックにバージョン（v1/v2）を追加しました |

ノード マネージャの GTPC メトリックを次に示します。

**表 *489 : GTPC* メトリック**

| メトリック | 説明 |
|---|---|
| nodemgr_gtpc_msg_stats | メトリックにバージョン（v1/v2）を追加しました |
| nodemgr_gtpc_peer_status | メトリックにバージョン（v1/v2）を追加しました |

メトリックの詳細については、『*UCC 5G SMF メトリック参照 2025.02.0* ガイド』以上のバージョンを参照してください。

第 42 章

# SMF の有用性


- ピア モニタリング （1822 ページ）
- ログ モニタリング （1823 ページ）

# ピア モニタリング

## Grafana を介したピア ステータスの表示

表 *490 :* 機能の履歴

| 機能名 | リリース情報 | 説明 |
|---|---|---|
| SMF メトリック：Grafana を介したピア ステータスの表示 | 2025.01.0 | このリリースでは、SMF は、Grafana クラウドで Grafana クエリを使用して、Diameter（Gx および Gy）、RADIUS、CGF、および N4 ピアの接続ステータスを表示する機能を提供します。<br>単一のペイン ビューで、さまざまな展開のピア ステータスを確認できるため、接続の問題をより迅速に特定して解決できます。<br>Grafana クエリでは、ピアの現在のステータスが表示され、接続されているかどうかのピア ステータスも表示されます。<br>SMF メトリックの詳細については、「SMF メトリック」を参照してください。 |

SMF は、次のメトリックを使用して Grafana のピア ステータスを表示します。

表 *491 : Grafana* クエリに使用されるメトリック

| ピア（**Peer**） | メトリック | 設定必須です |
|---|---|---|
| Diameter（Gx および Gy） | **rpc_host_status** | `infra metrics verbose protocol`<br>`metrics rpc_host_status`<br>`level debug`<br>`exit`<br>または<br>`infra metrics verbose protocol`<br>`level debug`<br>`exit`<br>（注）<br>この構成を追加した後、diameter-ep ポッドを再起動する必要があります。 |
| RADIUS | **Radius_Server_Status** | 設定は不要 |
| CGF（GTPP/Gz） | **nodemgr_gtpp_stats**<br>このメトリックは、このリリース（2025.01.0）で新しく追加されたものであることに注意してください。 | `infra metrics verbose application`<br>`metrics nodemgr_gtpp_stats`<br>`level debug`<br>`exit`<br>または<br>`infra metrics verbose application`<br>`level debug`<br>`exit` |
| N4 | **nodemgr_upf_link_status**<br>このメトリックは、このリリース（2025.01.0）で新しく追加されたものであることに注意してください。 | `infra metrics verbose application`<br>`metrics nodemgr_upf_link_status`<br>`level debug`<br>`exit`<br>または<br>`infra metrics verbose application`<br>`level debug`<br>`exit` |

# ログ モニタリング

## 機能の概要と変更履歴

### 要約データ

表 *492 :* 要約データ

| | |
|---|---|
| 該当製品または機能エリア | SMF |

| | |
|---|---|
| 該当プラットフォーム | SMI |
| 機能のデフォルト設定 | 有効：常時オン |
| このリリースでの関連する変更点 | N/A |
| 関連資料 | 該当なし |

## 更新履歴

**表 *493* : マニュアルの変更履歴**

| 改訂の詳細 | リリース |
|---|---|
| 最初の導入。 | 2023.01.0 |

# 機能説明

SMF ログとサービスアビリティ機能は、次のモードで実行されます。

- これは、トラブルシューティング ツールのチェーンを使用して、実稼働環境で制限付きのデバッグ ログを有効にすることを支援し、機能をキャプチャします。
- これらは、実稼働中に見つかった問題の根本原因を特定するためにかかる時間を短縮するのにさらに役立ちます。

この機能により、オペレータは特定の LogTag を有効にして、コールの失敗やプロシージャの失敗をデバッグし、実稼働のより良いRCA を促進できます。これには、次の特性があります：

- SMF は、問題のダウンロードと詳細な調査に役立つコアダンプを生成するためのツールまたはユーティリティを提供する必要がある。
- SMF は、ログにエラーの詳細とともに失敗したサブスクライバの SUPI を出力する必要があります。
- サブスクライバ情報 MonSub は 、特定のサブスクライバのデバッグに役立ちます。

## 関係

次のモジュールがこの機能に関連付けられています：

- コールの失敗ログ （1829 ページ）
- 手順失敗ログ （1831 ページ）
- 一般的なプロシージャ失敗ログ （1834 ページ）
- 追加のコールフロー失敗ログ （1835 ページ）
- イベント トレース ログ （1838 ページ）

- コール フロー統計ログ （1842 ページ）
- コア ダンプ ユーティリティ ログ （1843 ページ）
- サブスクライバ(MonSub)ログを監視 （1845 ページ）
- N40 追加のログと （1849 ページ）
- N7 の追加のログと統計情報 （1851 ページ）


# 機能の仕組み

ここでは、この機能の仕組みを説明します。

### ログ インスタンス

ログインスタンスは、問題、展開ステータス、およびパフォーマンスの調整の特定に使用されるメッセージを生成します。アプリケーションインフラストラクチャは、アプリケーション全体でログ メッセージを有効にする共通の方法を提供します。各ログ インスタンスには、次のログがあります。

- Timestamp
- ログメッセージ
- ログ レベル
- LogTag

### LogTag

LogTag は、特定のタイプのログ メッセージを有効または無効にするフィルタとして使用されます。これらは、ロギング セッションの前またはロギング セッション中に事前に作成され、評価されて除外されます。これは、次のタスクによって構成されます。

- モジュール名
- コンポーネント名
- インターフェイス名

### LogTag の作成

次に、LogTag の作成例を示します。

```
common.LogTagN7RestEp = appCtx.RegisterLogTag("rest_ep", "app", "n7")
```

### メッセージのロギング

次に、LogTag メッセージのロギングの例を示します。

```
appCtx.Info(common.LogTagN7RestEp, "Starting rest-ep app")
```

### ログ レベル

アプリケーションインフラストラクチャは、ログレベルの最大6つの変数を提供します。これは、LogTag とともにフィルタとして使用して、特定のログを有効または無効にすることができます。各レベルは、トラブルシューティング時に使用できるログ メッセージの重要度レベルを表します。次の表に、ログ レベルとその使用方法を示します。

**表 *494* : ログ レベル**

| ログ レベル | 利用 |
|---|---|
| エラー（Error） | 重大な問題につながる不当性がある場合に使用されます。 |
| 警告（warning） | 次のいずれかのシナリオが発生した場合に、通知および警告を行うために使用します。<br>• 重大なことが発生しようとしています。<br>• 誤って実行されているアクティビティがある場合<br>• エラーノートを継続的に表示する<br>• 不参加のシナリオ |
| 情報（info） | アプリケーションの起動や停止など、通常は予期される動作に使用されます。 |
| デバッグ | 問題をデバッグするために必要な詳細情報を提供するために使用されます。 |
| Trace | 広範な情報を提供するために使用されます。また、同じデバッグ ログが定期的に送信され続ける監視ルーチンにも使用されます。 |
| 消灯 | ロギング情報に意味がない場合に使用されます。ロギング アクティビティをオフまたはオンにするよう CLI で構成されます。 |

### ログ レベル順序

毎回、アプリケーション インフラストラクチャはログ メッセージをログに記録し、ログ レベル、および構成されたログ設定を持つ LogTag をログに記録する前に、ログに記録します。

表 *495 :* ログ レベル

| ログ レベル（順序） | 使用方法 |
|---|---|
| Error (0) | エラー ログと一致させます。 |
| Warn (1) | 警告ログとエラー ログを照合します。 |
| Info (2) | 情報、警告、およびエラーログを照合します。 |
| Debug (3) | デバッグ、情報、警告、およびエラー ログを照合します。 |
| Trace (4) | トレース、デバッグ、情報、警告、およびエラー ログを照合します。 |
| Off (5) | エラーを無効にするログと一致しません。 |

### SMF ログ

SMF は、特定の LogTag を有効にするオペレータをサポートしています。次に、この機能の実装をサポートするモジュールのリストを示します。

1. **コール失敗 ログ タグ:**
    - CLI モードでの有効化
    - SMF は、切断理由に基づいて次のログを有効にする必要があります。
        - エラー（Error）
        - 警告
        - デバッグ
    - 次のログ パラメータが出力されます。
        - Transaction ID
        - 切断理由
        - イベント トレース
        - セッション キー
        - エラー カテゴリ（重大な切断理由）

2. **手順失敗LogTag**：
    - CLI モードでの有効化
    - SMF は、切断理由に基づいて次のログを有効にする必要があります。
        - 警告（warning）

- 次のログ パラメータが出力されます。
  - Transaction ID
  - 手順名
  - イベント トレース
  - 詳細なエラー：次のような情報が含まれます。
    - 障害の理由または原因
    - 切断理由（該当する場合）
    - 失敗メトリック

3. **追加のコール フロー失敗LogTag**：
   - 特定の理由または条件で有効
   - 次のログ パラメータが出力されます。
     - Transaction ID
     - イベント トレース
     - コール フロー固有のエラー メッセージ
   - サポートされるログ レベル
     - エラー（Error）
     - 警告
     - 情報
     - デバッグ
4. **追加の汎用手順失敗 LogTag**:
   - CLI モードでの有効化
   - SMF では、切断理由に基づいてイベント トレースを有効にする必要があります。
   - オペレータがすべての手順の失敗ログを必要とする場合、オペレータはこの LogTag を有効にできます。

（注） 失敗したすべての手順のログを出力するため、オペレータは慎重にこのLogTagをアクティブにする必要があります。このアクションにより、サービス ログのオーバーフローが発生する可能性があります。

- 次のログ パラメータが出力されます。
  - Transaction ID
  - 手順名
  - 詳細なエラー：次のような情報が含まれます。
    - 障害の理由または原因
    - 切断理由（該当する場合）
    - 失敗メトリック

5. **コール フロー統計LogTag**：
   - このプロセスは、すべての手順の最後に一覧表示されます。
6. **コア ダンプ LogTag**：
   - このプロセスにより、コア ダンプ ユーティリティのデバッグ アクティビティが開始されます。
7. **サブスクライバ モニタリングLogTag**:
   - このプロセスは、あらゆる種類の障害のデバッグ アクティビティを開始します。また、サブスクライバのSUPIに基づいてサブスクライバのモニタリングも処理します。

**ワンポイント アドバイス**

詳細については、「トラブルシューティング情報」 > ログ （2100 ページ）を参照してください。

# コールの失敗ログ

次に、SMF に対するセッション管理ポリシーをトリガーするコール失敗ログの概要を示します。

- コールの失敗とコールの解放については、 切断理由ベースの 統計が定義され、添付されます。
- 切断の理由：次の 3 つのカテゴリに分類されます。
  - やや重大
  - 比較的重大でない
  - 通常

- コール失敗またはコール リリースのシナリオでは、メッセージは次のように記録されます。
  - メジャー（破棄）カテゴリの切断理由：エラー レベルのトランザクション ログには、エラー カテゴリ、切断理由、イベント トレース、セッション キーが表示されます。
  - マイナー（重大）カテゴリの切断理由：警告レベルのトランザクションログに、イベント トレースやセッション キーとともに切断理由をダンプします。
  - 通常のカテゴリの切断理由：デバッグ レベルのトランザクションログにより、イベント トレースとセッション キーと共に切断理由がダンプされます。
  - グレースフルコアダンプ：このトランザクション ログも、同じ LogTag およびレベルで実行されます。
- コール エラーをログに記録する新しい LogTag も定義されます。
- トランザクション ID は、ログおよびコール フローと一致するようにコール失敗ログに出力されます。
- 切断理由統計に基づいて、対応するログ レベルの callfailure タグを有効にして、セッションの詳細を収集できます。次に、例のリストを示します：
  - イベント トレース
  - セッション キー
  - コアダンプ

### コール失敗ログのサンプル ダンプ

次に、コール失敗ログのサンプル ダンプを示します。

例：手順の経過時間が2秒を超えると、イベント トレースに警告メッセージが記録されます。

```
2022/08/23 11:10:31.222 [警告] [smf-service.smf-app.callfailure-debug] 2sec Time Elapsed:
 EVENT TRACE SessionKeys[[imsi-123456789012345:5 (pk)]]
CurIndex:[ 2], CurProcInst:[0], CreateTimeStamp:[2022-08-23 11:10:31.204 +0530 IST],
BaseTimeStamp:[2022-08-23 11:10:31.204 +0530 IST]
|INDEX|EVENT NAME                          |EVENT TYPE           |PROC NAME
                              |PROC INST |TXN ID    |TIMESTAMP
 |
|1    |N11SmContextCreateReq               |INCOMING_EVENT       |PDU セッション確立
                      |1          |1          |2022-08-23 11:10:31.215 +0530 IST  |
|2    |N11SmContextCreateReq               |ENDPROC_EVENT        |PDU セッション確立
                      |1          |1          |2022-08-23 11:10:31.221 +0530 IST  |
```

## コール失敗ログの構成

この機能を構成するには、次の構成を使用します。

**logging name smf-service.smf-app.callfailure-debug level application/transaction <debug level>**

注：

- **Warning**：コール失敗についてサポートされるロギング レベル LogTags。
- 詳細については、「トラブルシューティング情報」>ログ（2100ページ）を参照してください。

### 設定例

次に、設定例を示します。

```
config
   logging name smf-service.smf-app.callfailure-debug level transaction warn
   logging name smf-service.smf-app.callfailure-debug level application error
exit
```

### 設定の確認

設定を確認するには、次のコマンドを実行します。

```
[smf] smf# show running-config logging name smf-service.smf-app.callfailure-debug
 logging name smf-service.smf-app.callfailure-debug level application error
 logging name smf-service.smf-app.callfailure-debug level transaction warn
```

# 手順失敗ログ

次に、SMF に対するセッション管理ポリシーをトリガーする的なプロシージャ障害ログの概要を示します。

- 終了のシナリオ中に、各 Procedure Failure ログが EndProcedureをオンにします。
- 失敗のシナリオ中に、手順が成功したか失敗したかを示すエラーコードが SMF インフラに戻ります。
- 失敗すると、レベル warning のトランザクション ログ（すべての手順に共通）が使用され、次のようにセッションの詳細がダンプされます。
  - イベント トレース
  - 手順名
  - エラーの詳細：失敗の理由または原因、切断理由（該当する場合）、および失敗メトリックが含まれます。
- プロシージャ失敗 ログタグは 、すべての手順に共通です。
- 手順固有の ログタグは 、各手順に対して構成され、特定の手順の失敗のログを有効にするために使用されます。
- トランザクション ID は、ログおよびコール フローと一致するように手順失敗ログに出力されます。

- 詳細なエラーメモは、手順失敗ログに出力されます。問題、実際のエラー原因、切断理由（該当する場合）、および障害メトリクスを理解するのに役立ちます。

### プロシージャ失敗ログのメッセージの記録

次に、プロシージャ障害ログの LogTag の例を示します。

```
2023/01/15 11:34:30.002 [WARN] [smf-service.smf-app.pdnsetup-procfailure]
[Txn :7]Procedure=[PDN Connect [LTE]], PduState=[IDLE], Rat-Type=[rat_type_unknown],
FailureReason=[udm_subscribe_notify_failure],
DisconnectReason=[disc_pdnsetup_udm_sub_notify_resp_failed]
2023/01/15 11:34:30.002 [WARN] [smf-service.smf-app.pdnsetup-procfailure] [Txn :7]EVENT
 TRACE
CurIndex:[8], CurProcInst:[0], CreateTimeStamp:[2022-09-13 11:34:27.942 +0000 UTC],
BaseTimeStamp:[2022-09-13 11:34:27.942 +0000 UTC]

|INDEX|EVENT NAME |EVENT TYPE |PROC NAME |PROC INST |TXN ID |TIMESTAMP |

|1 |S5S8CreateSessReq |INCOMING_EVENT |PDN Connect [LTE] |1 |7 |2022-09-13 11:34:27.942
 +0000 UTC |
|2 |N10RegistrationSuccess |INCOMING_EVENT |PDN Connect [LTE] |1 |7 |2022-09-13
11:34:27.943 +0000 UTC |
```

## 手順失敗ログの構成

この機能を構成するには、次の構成を使用します。

```
logging name smf-service.smf-app.pdusetup-procfailure level
  transaction <debug level>
logging name smf-service.smf-app.pdnsetup-procfailure level
transaction <debug level>
logging name smf-service.smf-app.pdurelease-procfailure
level transaction <debug level>
logging name smf-service.smf-app.pdndisconnect-procfailure level
  transaction <debug level>
logging name smf-service.smf-app.5gim-procfailure
   level transaction <debug level>
logging name smf-service.smf-app.xnho-procfailure
   level transaction <debug level>
logging name smf-service.smf-app.n2ho-procfailure
  level transaction <debug level>
logging name smf-service.smf-app.nrtowifiho-procfailure
level transaction <debug level>
logging name smf-service.smf-app.enbtowifiho-procfailure
 level transaction <debug level>
logging name smf-service.smf-app.wifitonrho-procfailure
  level transaction <debug level>
logging name smf-service.smf-app.wifitoenbho-procfailure
 level transaction <debug level>
logging name smf-service.smf-app.4gdedbrr-procfailure
  level transaction <debug level>
logging name smf-service.smf-app.pdnmodmbr-procfailure
```

```
level  transaction <debug level>
logging  name  smf-service.smf-app.5gmodify-procfailure
 level  transaction <debug level>
logging  name  smf-service.smf-app.5g4gho-procfailure
  level  transaction <debug level>
logging  name  smf-service.smf-app.n26ho-procfailure
   level          transaction <debug level>
```

注：

- **Warning**：手順の失敗でサポートされるロギング レベル LogTags。
- 詳細については、「トラブルシューティング情報」>ログ （2100ページ）を参照してください。

## 設定例

次に、設定例を示します。

```
config
  logging name smf-service.smf-app.4gdedbrr-procfailure level transaction warn
  logging name smf-service.smf-app.5g4gho-procfailure level transaction warn
  logging name smf-service.smf-app.5gim-procfailure level transaction warn
  logging name smf-service.smf-app.5gmodify-procfailure level transaction warn
  logging name smf-service.smf-app.enbtowifiho-procfailure level transaction warn
  logging name smf-service.smf-app.n26ho-procfailure level transaction warn
  logging name smf-service.smf-app.n2ho-procfailure level transaction warn
  logging name smf-service.smf-app.nrtowifiho-procfailure level transaction warn
  logging name smf-service.smf-app.pdndisconnect-procfailure level transaction warn
  logging name smf-service.smf-app.pdnmodmbr-procfailure level transaction warn
  logging name smf-service.smf-app.pdnsetup-procfailure level transaction warn
  logging name smf-service.smf-app.pdurelease-procfailure level transaction warn
  logging name smf-service.smf-app.pdusetup-procfailure level transaction warn
  logging name smf-service.smf-app.wifitoenbho-procfailure level transaction warn
  logging name smf-service.smf-app.wifitonrho-procfailure level transaction warn
  logging name smf-service.smf-app.xnho-procfailure level transaction warn
exit
```

## 設定の確認

設定を確認するには、次のコマンドを実行します。

```
[smf] smf# show running-config logging name
 logging name smf-service.smf-app.4gdedbrr-procfailure level transaction warn
 logging name smf-service.smf-app.5g4gho-procfailure level transaction warn
 logging name smf-service.smf-app.5gim-procfailure level transaction warn
 logging name smf-service.smf-app.5gmodify-procfailure level transaction warn
 logging name smf-service.smf-app.enbtowifiho-procfailure level transaction warn
 logging name smf-service.smf-app.n26ho-procfailure level transaction warn
 logging name smf-service.smf-app.n2ho-procfailure level transaction warn
 logging name smf-service.smf-app.nrtowifiho-procfailure level transaction warn
 logging name smf-service.smf-app.pdndisconnect-procfailure level transaction warn
 logging name smf-service.smf-app.pdnmodmbr-procfailure level transaction warn
 logging name smf-service.smf-app.pdnsetup-procfailure level transaction warn
 logging name smf-service.smf-app.pdurelease-procfailure level transaction warn
 logging name smf-service.smf-app.pdusetup-procfailure level transaction warn
 logging name smf-service.smf-app.wifitoenbho-procfailure level transaction warn
 logging name smf-service.smf-app.wifitonrho-procfailure level transaction warn
 logging name smf-service.smf-app.xnho-procfailure level transaction warn
```

# 一般的なプロシージャ失敗ログ

次に、SMFに対するセッション管理ポリシーをトリガーする一般的なプロシージャ障害ログの概要を示します。

- 終了のシナリオ中に、各 Procedure Failure ログが EndProcedureをオンにします。
- 失敗のシナリオ中に、手順が成功したか失敗したかを示すエラーコードが SMF インフラに戻ります。
- 失敗すると、警告レベルの汎用トランザクション ログ（すべての手順に共通）が使用され、次のようにセッションの詳細がダンプされます。
  - Transaction ID
  - 手順名
  - 詳細なエラー：失敗の理由または原因、切断理由（該当する場合）、および失敗メトリックが含まれます。
- 汎用プロシージャ失敗 ログ タグは 、すべての手順に共通です。
- 特定のプロシージャ失敗 ログタグ が無効になり、汎用プロシージャ失敗 ログ タグ が有効になっている場合、SMF はイベント トレースを出力しません。
- イベント トレースは、特定のプロシージャ失敗 ログ タグ が有効になった場合にのみ出力されます。
- トランザクション ID は、ログおよびコール フローと一致するように手順失敗ログに出力されます。
- 詳細なエラーのメモは、一般的なプロシージャ失敗ログに出力されます。問題、実際のエラー原因、切断理由（該当する場合）、および障害メトリクスを理解するのに役立ちます。

### 一般的なプロシージャ失敗ログのメッセージの記録

次に、汎用プロシージャ障害ログの LogTag の例を示します。

```
2023/01/15 10:58:01.171 [WARN] [smf-service.smf-app.procfailure] [Txn :1] Procedure=[PDN
 Connect [LTE]],
PduState=[IDLE], Rad-Type =[rat_type_unknown]、
FailureReason=[udm_subscribe_notify_failure]、
DisconnectReason=[disc_pdnsetup_udm_sub_notify_resp_failed]
```

## 一般的な手順失敗ログを構成

この機能を構成するには、次の構成を使用します。

**logging name smf-service.smf-app.procfailure level transaction <debug level>**

注：

- **Warning**：一般的な手順の失敗でサポートされるロギング レベル LogTags。
- 詳細については、「トラブルシューティング情報」>ログ（2100ページ）を参照してください。

### 設定例

次に、設定例を示します。

```
config
 logging name smf-service.smf-app.procfailure level transaction warn
exit
```

### 設定の確認

設定を確認するには、次のコマンドを実行します。

```
[smf] smf# show running-config logging name smf-service.smf-app.procfailure
logging name smf-service.smf-app.procfailure level transaction warn
```

## 追加のコールフロー失敗ログ

次に、SMF に対するセッション管理ポリシーをトリガーする追加のコール フロー失敗ログの概要を示します。

- 特定の手順に対して追加の LogTag が追加されています。
- これらの LogTag は 、手順フロー間の特定の条件に対して有効にできます。
- 追加のコールフロー失敗ログは、手順失効イベントを特定し、イベントトレースに記録された警告メッセージで応答するのに役立ちます。

### コール フロー失敗ログのサンプル ダンプ

次に、コール フロー失敗ログのサンプル ダンプを示します。

例：手順の経過時間が2秒を超えると、イベント トレースに警告メッセージが記録されます。

```
2022/08/23 11:10:31.222 [WARN] [smf-service.smf-app.5gmodify-failure] 2sec Time Elapsed:
 EVENT TRACE SessionKeys[[imsi-123456789012345:5 (pk)]]
CurIndex:[2], CurProcInst:[0], CreateTimeStamp:[2022-08-23 11:10:31.204 +0530 IST],
BaseTimeStamp:[2022-08-23 11:10:31.204 +0530 IST]
|INDEX|EVENT NAME                          |EVENT TYPE           |PROC NAME
                              |PROC INST |TXN ID    |TIMESTAMP
 |
```

### 追加のコール フロー失敗のログのメッセージのロギング

次に、追加のコール フロー 障害ログの LogTag の例を示します。

```
2022/08/23 11:10:31.222 [WARN] [smf-service.smf-app.5gmodify-failure] 2sec Time Elapsed:
 EVENT TRACE SessionKeys[[imsi-123456789012345:5 (pk)]]
CurIndex:[2], CurProcInst:[0], CreateTimeStamp:[2022-08-23 11:10:31.204 +0530 IST],
BaseTimeStamp:[2022-08-23 11:10:31.204 +0530 IST]
|INDEX|EVENT NAME                          |EVENT TYPE           |PROC NAME
                              |PROC INST |TXN ID    |TIMESTAMP
 |
```

# 追加のコールフロー失敗ログの構成

この機能を構成するには、次の構成を使用します。

```
Logging name smf-service.smf-app.4gdedbrr-failure level transaction
<debug level>
logging      name     smf-service.smf-app.pdnmodmbr-failure     level
    transaction     <debug level>
logging      name     smf-service.smf-app.5gmodify-failure
level     transaction     <debug level>
logging      name     smf-service.smf-app.5g4gho-failure
level     transaction     <debug level>
logging      name     smf-service.smf-app.n26ho-failure
level     transaction     <debug level>
logging      name     smf-service.smf-app.wifi-nr-ho
 level     transaction     <debug level>
logging      name     smf-service.smf-app.datacheck       level
transaction     <debug level>
logging      name     smf-service.smf-app.N16             level
transaction     <debug level>
logging      name     smf-service.smf-app.erir             level
transaction     <debug level>
logging      name     smf-service.smf-app.flagdb            level
transaction     <debug level>
logging      name     smf-service.smf-app.dcr          level
transaction     <debug level>
logging      name     smf-service.smf-app.dcr-ue        level
transaction     <debug level>
logging      name     smf-service.smf-app.dcr-brr-dup       level
transaction     <debug level>
logging      name     smf-service.smf-app.dcr-brr-mme       level
transaction     <debug level>
logging      name     smf-service.smf-app.dcr-brr-pcf       level
transaction     <debug level>
logging      name     smf-service.smf-app.dcr-brr-ubr       level
transaction     <debug level>
logging      name     smf-service.smf-app.dcr-brr-absent      level
  transaction     <debug level>
logging      name     smf-service.smf-app.dcr-brr-amf       level
transaction     <debug level>
logging      name     smf-service.smf-app.dcr-brr-chf      level
transaction     <debug level>
logging      name     smf-service.smf-app.dcr-brr-gnb       level
transaction     <debug level>
```

```
logging      name     smf-service.smf-app.dcr-brr-smf       level
transaction     <debug level>
logging      name     smf-service.smf-app.dcr-brr-udm       level
transaction     <debug level>
logging      name     smf-service.smf-app.dcr-brr-ue       level
transaction     <debug level>
logging      name     smf-service.smf-app.epsfb        level
transaction     <debug level>
```

注：

- **Warning**：コール フロー失敗 LogTags についてサポートされるロギング レベル。
- 詳細については、「トラブルシューティング情報」>ログ（2100ページ）を参照してください。

## 設定例

次に、設定例を示します。

```
config
  logging name smf-service.smf-app.4gdedbrr-failure level transaction warn
  logging name smf-service.smf-app.5g4gho-failure level transaction warn
  logging name smf-service.smf-app.5gmodify-failure level transaction warn
  logging name smf-service.smf-app.N16 level transaction warn
  logging name smf-service.smf-app.datacheck level transaction warn
  logging name smf-service.smf-app.dcr level transaction warn
  logging name smf-service.smf-app.dcr-brr-absent level transaction warn
  logging name smf-service.smf-app.dcr-brr-amf level transaction warn
  logging name smf-service.smf-app.dcr-brr-chf level transaction warn
  logging name smf-service.smf-app.dcr-brr-dup level transaction warn
  logging name smf-service.smf-app.dcr-brr-gnb level transaction warn
  logging name smf-service.smf-app.dcr-brr-mme level transaction warn
  logging name smf-service.smf-app.dcr-brr-pcf level transaction warn
  logging name smf-service.smf-app.dcr-brr-smf level transaction warn
  logging name smf-service.smf-app.dcr-brr-ubr level transaction warn
  logging name smf-service.smf-app.dcr-brr-udm level transaction warn
  logging name smf-service.smf-app.dcr-brr-ue level transaction warn
  logging name smf-service.smf-app.dcr-ue level transaction warn
  logging name smf-service.smf-app.epsfb level transaction warn
  logging name smf-service.smf-app.erir level transaction warn
  logging name smf-service.smf-app.flagdb level transaction warn
  logging name smf-service.smf-app.n26ho-failure level transaction warn
  logging name smf-service.smf-app.pdnmodmbr-failure level transaction warn
  logging name smf-service.smf-app.wifi-nr-ho level transaction warn
end
```

## 設定の確認

設定を確認するには、次のコマンドを実行します。

```
[smf] smf# show running-config logging name
 logging name smf-service.smf-app.4gdedbrr-failure level transaction warn
 logging name smf-service.smf-app.5g4gho-failure level transaction warn
 logging name smf-service.smf-app.5gmodify-failure level transaction warn
 logging name smf-service.smf-app.N16 level transaction warn
 logging name smf-service.smf-app.datacheck level transaction warn
 logging name smf-service.smf-app.dcr level transaction warn
 logging name smf-service.smf-app.dcr-brr-absent level transaction warn
 logging name smf-service.smf-app.dcr-brr-amf level transaction warn
```

```
logging name smf-service.smf-app.dcr-brr-chf level transaction warn
logging name smf-service.smf-app.dcr-brr-dup level transaction warn
logging name smf-service.smf-app.dcr-brr-gnb level transaction warn
logging name smf-service.smf-app.dcr-brr-mme level transaction warn
logging name smf-service.smf-app.dcr-brr-pcf level transaction warn
logging name smf-service.smf-app.dcr-brr-smf level transaction warn
logging name smf-service.smf-app.dcr-brr-ubr level transaction warn
logging name smf-service.smf-app.dcr-brr-udm level transaction warn
logging name smf-service.smf-app.dcr-brr-ue level transaction warn
logging name smf-service.smf-app.dcr-ue level transaction warn
logging name smf-service.smf-app.epsfb level transaction warn
logging name smf-service.smf-app.erir level transaction warn
logging name smf-service.smf-app.flagdb level transaction warn
logging name smf-service.smf-app.n26ho-failure level transaction warn
logging name smf-service.smf-app.pdnmodmbr-failure level transaction warn
logging name smf-service.smf-app.wifi-nr-ho level transaction warn
```

# イベント トレース ログ

次に、SMF に対するセッション管理ポリシーをトリガーするイベント トレース ログの概要を示します。

- イベント トレース ログは、セッションの実行シーケンスを提供します。これは、次を表します：
  - メッセージの種類
  - イベント タイプ：着信、発信、または内部送信されたイベント タイプ。
  - 手順タイプと手順インスタンス：メッセージが関連付けられている場所。
  - Txn ID：メッセージの関連付け先。
  - Timestamp：関連付けられている同じメッセージの場合
- イベント トレース ログは、次のように他のイベントも記述します：
  - Local2DB：セッションの詳細がプリミティブ構造に派生する場合。
  - DB2Local：セッション詳細が DB からセッション DS に派生しない場合。
  - プロシージャ イベント：END または SUSPEND または ABORT または CLEANUP イベントも伝送する場合。

### イベント トレース ログのサンプル ダンプ

次に、イベント トレース ログのダンプの例を示します。

```
2020/09/10 13:16:16.177 smf-service [DEBUG] [Genericutil.go:5739]
[smf-service0.smf-app.event-trace] EVENT TRACE SessionKeys[[imsi-123456789012345:5 (pk)]]
CurIndex:[31], CurProcInst:[1], CreateTimeStamp:[2020-09-10 13:16:15.503 +0000 UTC],
BaseTimeStamp:[2020-09-10 13:16:15.503 +0000 UTC]
|INDEX|EVENT NAME                          |EVENT TYPE           |PROC NAME
                               |PROC INST |TXN ID    |TIMESTAMP
```

```
 |
|1    |N11SmContextCreateReq             |INCOMING_EVENT      |PDU Session Establishment
                           |1          |1776      |2020-09-10 13:16:15.503 +0000 UTC  |
|2    |N10RegistrationRequest            |OUTGOING_EVENT      |PDU Session Establishment
                           |1          |1776      |2020-09-10 13:16:15.525 +0000 UTC  |
|3    |N10RegistrationSuccess            |INCOMING_EVENT      |PDU Session Establishment
                           |1          |1776      |2020-09-10 13:16:15.605 +0000 UTC  |
|4    |N10SubscriptionFetchReq           |OUTGOING_EVENT      |PDU Session Establishment
                           |1          |1776      |2020-09-10 13:16:15.606 +0000 UTC  |
|5    |N10SubscriptionFetchSuccess       |INCOMING_EVENT      |PDU Session Establishment
                           |1          |1776      |2020-09-10 13:16:15.644 +0000 UTC  |
|6    |N10SubscribeForNotificationReq    |OUTGOING_EVENT      |PDU Session Establishment
                           |1          |1776      |2020-09-10 13:16:15.65 +0000 UTC   |
|7    |N10SubscribeForNotificationSuccess |INCOMING_EVENT      |PDU Session Establishment
                           |1          |1776      |2020-09-10 13:16:15.67 +0000 UTC   |
|8    |NIntSelfTxnPduSetup               |INTERNAL_EVENT      |PDU Session Establishment
                           |1          |1777      |2020-09-10 13:16:15.67 +0000 UTC   |
|9    |Message Type None                   |LOCAL_2_DB          |Unknown
                              |0          |0         |2020-09-10 13:16:15.671 +0000 UTC
 |
|10   |N11SmContextCreateSuccess         |OUTGOING_EVENT      |PDU Session Establishment
                           |1          |1776      |2020-09-10 13:16:15.711 +0000 UTC  |
|11   |NIntSelfTxnPduSetup               |INCOMING_EVENT      |PDU Session Establishment
                           |1          |1777      |2020-09-10 13:16:15.712 +0000 UTC  |
|12   |N7SmPolicyCreateReq               |OUTGOING_EVENT      |PDU Session Establishment
                           |1          |1777      |2020-09-10 13:16:15.712 +0000 UTC  |
|13   |N7SmPolicyCreateSuccess           |INCOMING_EVENT      |PDU Session Establishment
                           |1          |1777      |2020-09-10 13:16:15.797 +0000 UTC  |
|14   |NmgrRersourceMgmtRequest          |OUTGOING_EVENT      |PDU Session Establishment
                           |1          |1777      |2020-09-10 13:16:15.805 +0000 UTC  |
|15   |NmgrRersourceMgmtResponse         |INCOMING_EVENT      |PDU Session Establishment
                           |1          |1777      |2020-09-10 13:16:15.814 +0000 UTC  |
|16   |N7SmPolicyUpdateReq               |OUTGOING_EVENT      |PDU Session Establishment
                           |1          |1777      |2020-09-10 13:16:15.823 +0000 UTC  |
|17   |N7SmPolicyUpdateSuccess           |INCOMING_EVENT      |PDU Session Establishment
                           |1          |1777      |2020-09-10 13:16:15.853 +0000 UTC  |
|18   |N40ChargingDataReq                |OUTGOING_EVENT      |PDU Session Establishment
                           |1          |1777      |2020-09-10 13:16:15.854 +0000 UTC  |
|19   |N40ChargingDataSuccess            |INCOMING_EVENT      |PDU Session Establishment
                           |1          |1777      |2020-09-10 13:16:15.912 +0000 UTC  |
|20   |N4SessionEstablishmentReq         |OUTGOING_EVENT      |PDU Session Establishment
                           |1          |1777      |2020-09-10 13:16:15.921 +0000 UTC  |
|21   |N4SessionEstablishmentSuccess     |INCOMING_EVENT      |PDU Session Establishment
                           |1          |1777      |2020-09-10 13:16:15.986 +0000 UTC  |
|22   |N11EbiAssignmentReq               |OUTGOING_EVENT      |PDU Session Establishment
                           |1          |1777      |2020-09-10 13:16:15.99 +0000 UTC   |
|23   |N11EbiAssignmentRsp               |INCOMING_EVENT      |PDU Session Establishment
                           |1          |1777      |2020-09-10 13:16:16.017 +0000 UTC  |
|24   |N11N1N2MessageTransferReq         |OUTGOING_EVENT      |PDU Session Establishment
                           |1          |1777      |2020-09-10 13:16:16.021 +0000 UTC  |
|25   |N11N1N2MessageTransferSuccess     |INCOMING_EVENT      |PDU Session Establishment
                           |1          |1777      |2020-09-10 13:16:16.096 +0000 UTC  |
|26   |Message Type None                   |LOCAL_2_DB          |Unknown
                              |0          |0         |2020-09-10 13:16:16.096 +0000 UTC
 |
|27   |N11SmContextUpdateReq             |INCOMING_EVENT      |PDU Session Establishment
```

```
                              |1          |1778       |2020-09-10 13:16:16.111 +0000 UTC   |
|28   |N4SessionModificationReq           |OUTGOING_EVENT       |PDU Session Establishment
                              |1          |1778       |2020-09-10 13:16:16.114 +0000 UTC   |
|29   |N4SessionModificationSuccess       |INCOMING_EVENT       |PDU Session Establishment
                              |1          |1778       |2020-09-10 13:16:16.155 +0000 UTC   |
|30   |N4GtpuRouterAdvertisementReq       |OUTGOING_EVENT       |PDU Session Establishment
                              |1          |1778       |2020-09-10 13:16:16.156 +0000 UTC   |
|31   |N4SessionModificationSuccess       |ENDPROC_EVENT        |PDU Session Establishment
                              |1          |1778       |2020-09-10 13:16:16.175 +0000 UTC   |
```

### イベント トレース ログへのメッセージの記録

次に、イベント トレース ログの LogTag の例を示します：

```
2020/09/10 13:16:16.177 smf-service [DEBUG] [Genericutil.go:5739]
[smf-service0.smf-app.event-trace] EVENT TRACE SessionKeys[[imsi-123456789012345:5 (pk)]]
CurIndex:[31], CurProcInst:[1], CreateTimeStamp:[2020-09-10 13:16:15.503 +0000 UTC],
BaseTimeStamp:[2020-09-10 13:16:15.503 +0000 UTC]
|INDEX|EVENT NAME                            |EVENT TYPE            |PROC NAME
                               |PROC INST |TXN ID    |TIMESTAMP
 |

|1    |N11SmContextCreateReq              |INCOMING_EVENT       |PDU Session Establishment
                              |1          |1776       |2020-09-10 13:16:15.503 +0000 UTC   |
|2    |N10RegistrationRequest             |OUTGOING_EVENT       |PDU Session Establishment
                              |1          |1776       |2020-09-10 13:16:15.525 +0000 UTC   |
|3    |N10RegistrationSuccess             |INCOMING_EVENT       |PDU Session Establishment
                              |1          |1776       |2020-09-10 13:16:15.605 +0000 UTC   |
|4    |N10SubscriptionFetchReq            |OUTGOING_EVENT       |PDU Session Establishment
                              |1          |1776       |2020-09-10 13:16:15.606 +0000 UTC   |
|5    |N10SubscriptionFetchSuccess        |INCOMING_EVENT       |PDU Session Establishment
                              |1          |1776       |2020-09-10 13:16:15.644 +0000 UTC   |
|6    |N10SubscribeForNotificationReq     |OUTGOING_EVENT       |PDU Session Establishment
                              |1          |1776       |2020-09-10 13:16:15.65 +0000 UTC    |
|7    |N10SubscribeForNotificationSuccess |INCOMING_EVENT       |PDU Session Establishment
                              |1          |1776       |2020-09-10 13:16:15.67 +0000 UTC    |
|8    |NIntSelfTxnPduSetup                |INTERNAL_EVENT       |PDU Session Establishment
                              |1          |1777       |2020-09-10 13:16:15.67 +0000 UTC    |
|9    |Message Type None                  |LOCAL_2_DB           |Unknown
                                 |0          |0          |2020-09-10 13:16:15.671 +0000 UTC
 |
|10   |N11SmContextCreateSuccess          |OUTGOING_EVENT       |PDU Session Establishment
                              |1          |1776       |2020-09-10 13:16:15.711 +0000 UTC   |
|11   |NIntSelfTxnPduSetup                |INCOMING_EVENT       |PDU Session Establishment
                              |1          |1777       |2020-09-10 13:16:15.712 +0000 UTC   |
|12   |N7SmPolicyCreateReq                |OUTGOING_EVENT       |PDU Session Establishment
                              |1          |1777       |2020-09-10 13:16:15.712 +0000 UTC   |
|13   |N7SmPolicyCreateSuccess            |INCOMING_EVENT       |PDU Session Establishment
                              |1          |1777       |2020-09-10 13:16:15.797 +0000 UTC   |
|14   |NmgrRersourceMgmtRequest           |OUTGOING_EVENT       |PDU Session Establishment
                              |1          |1777       |2020-09-10 13:16:15.805 +0000 UTC   |
|15   |NmgrRersourceMgmtResponse          |INCOMING_EVENT       |PDU Session Establishment
                              |1          |1777       |2020-09-10 13:16:15.814 +0000 UTC   |
|16   |N7SmPolicyUpdateReq                |OUTGOING_EVENT       |PDU Session Establishment
                              |1          |1777       |2020-09-10 13:16:15.823 +0000 UTC   |
```

```
|17   |N7SmPolicyUpdateSuccess           |INCOMING_EVENT      |PDU Session Establishment
                            |1          |1777      |2020-09-10 13:16:15.853 +0000 UTC  |
|18   |N40ChargingDataReq                |OUTGOING_EVENT      |PDU Session Establishment
                            |1          |1777      |2020-09-10 13:16:15.854 +0000 UTC  |
|19   |N40ChargingDataSuccess            |INCOMING_EVENT      |PDU Session Establishment
                            |1          |1777      |2020-09-10 13:16:15.912 +0000 UTC  |
|20   |N4SessionEstablishmentReq         |OUTGOING_EVENT      |PDU Session Establishment
                            |1          |1777      |2020-09-10 13:16:15.921 +0000 UTC  |
|21   |N4SessionEstablishmentSuccess     |INCOMING_EVENT      |PDU Session Establishment
                            |1          |1777      |2020-09-10 13:16:15.986 +0000 UTC  |
|22   |N11EbiAssignmentReq               |OUTGOING_EVENT      |PDU Session Establishment
                            |1          |1777      |2020-09-10 13:16:15.99 +0000 UTC   |
|23   |N11EbiAssignmentRsp               |INCOMING_EVENT      |PDU Session Establishment
                            |1          |1777      |2020-09-10 13:16:16.017 +0000 UTC  |
|24   |N11N1N2MessageTransferReq         |OUTGOING_EVENT      |PDU Session Establishment
                            |1          |1777      |2020-09-10 13:16:16.021 +0000 UTC  |
|25   |N11N1N2MessageTransferSuccess     |INCOMING_EVENT      |PDU Session Establishment
                            |1          |1777      |2020-09-10 13:16:16.096 +0000 UTC  |
|26   |Message Type None                 |LOCAL_2_DB          |Unknown
                               |0         |0         |2020-09-10 13:16:16.096 +0000 UTC
 |
|27   |N11SmContextUpdateReq             |INCOMING_EVENT      |PDU Session Establishment
                            |1          |1778      |2020-09-10 13:16:16.111 +0000 UTC  |
|28   |N4SessionModificationReq          |OUTGOING_EVENT      |PDU Session Establishment
                            |1          |1778      |2020-09-10 13:16:16.114 +0000 UTC  |
|29   |N4SessionModificationSuccess      |INCOMING_EVENT      |PDU Session Establishment
                            |1          |1778      |2020-09-10 13:16:16.155 +0000 UTC  |
|30   |N4GtpuRouterAdvertisementReq      |OUTGOING_EVENT      |PDU Session Establishment
                            |1          |1778      |2020-09-10 13:16:16.156 +0000 UTC  |
|31   |N4SessionModificationSuccess      |ENDPROC_EVENT       |PDU Session Establishment
                            |1          |1778      |2020-09-10 13:16:16.175 +0000 UTC  |
```

# イベント トレース ログの構成

この機能を構成するには、次の構成を使用します。

**logging name smf-service.smf-app.event-trace level transaction debug-level**

**注**：

- **Warning | Error**：イベント トレース ログ タグでサポートされているロギング レベル。
- **Session Keys | Procedure Name | Event Trace**：イベント トレース ログ タグでサポートされているロギング レベルのパラメータ。
- 詳細については、「トラブルシューティング情報」>ログ（2100ページ）を参照してください。

## 設定例

次に、設定例を示します。

```
logging name smf-service.smf-app.event-trace level transaction warn
```

### 設定の確認

設定を確認するには、次のコマンドを実行します。

```
[smf] smf# show running-config logging name smf-service.smf-app.event-trace
logging name smf-service.smf-app.event-trace level transaction warn
```

# コール フロー統計ログ

次に、SMF に対するセッション管理ポリシーをトリガーするコール フロー統計ログの概要を示します。

- 現在、各コールフローには、次の一般的なラベルと、その他の特定のラベルがあります。
  - 試行（Attempted）
  - Success
  - 障害 + 理由
- すべてのコールフロー統計が EndProcedureと統合されます。
- 手順でコールフローを終了するために使用される各 DispositionEnd は、成功または失敗シナリオのいずれかとして終了します。各障害シナリオには、統合の理由もあります。
- 障害原因はさまざまなレベルに分類できます。それらはさらにマッピングされ、次のように分類されます：
  - メジャーまたはエラー
    - 内部エラー：コールフローの失敗による内部エラーはすべてエラーに分類されます。
    - トランザクション タイムアウト エラー：インターフェイスでは、アウトバウンド応答タイムアウト（トランザクションタイムアウト）はエラーとして分類されます。
  - メジャーまたは警告
    - サーバ エラー：インターフェイスでは、http status code 5xx (server errors) のアウトバウンド応答は警告として分類されます。
    - クライアント エラー：インターフェイスでは、http status code 4xx (client errors) またはタイムアウトの着信応答は、警告として分類されます。
  - 標準
    - サーバ エラー：インターフェイスでは、http status code 5xx (server errors) のインバウンド応答は正常として分類されます。
    - クライアント エラー：インターフェイスでは、http status code 4xx (client errors) のアウトバウンド応答は正常として分類されます。

- 不明：コールフローが失敗したにもかかわらず、理由が入力されない場合は、不明な原因に分類されます。
- さらに、これらのシナリオは、ケース（統計の他の統計ラベル）にまで拡張でき、空のステータスに統合されます。

  例：RAT タイプは空として統合され、DNN タイプは統合されていないなど。

## コール フロー統計ログの構成

この機能を構成するには、次の構成を使用します。

**logging name smf-service.smf-app.stats-debug level transaction debug-level**

**注**：

- **Warning|Error**：コールフロー統計情報についてサポートされるロギング レベルLogTags。
- 詳細については、「トラブルシューティング情報」>ログ（2100ページ）を参照してください。

### 設定例

次に、設定例を示します。

```
logging name smf-service.smf-app.stats-debug level transaction warn
```

### 設定の確認

設定を確認するには、次のコマンドを実行します。

```
[smf] smf# show running-config logging name smf-service.smf-app.stats-debug
logging name smf-service.smf-app.stats-debug level transaction warn
```

# コア ダンプ ユーティリティ ログ

次に、SMF に対するセッション管理ポリシーをトリガーするコア ダンプ ユーティリティ ログの概要を示します：

- コア ダンプ ユーティリティのログには、デバッグ目的でコア ダンプを条件付きで生成する機能があります。
- コア ファイルの生成によってプロセスが強制終了されることはなく、通常どおり実行され続けます。
- コア ダンプ機能はデフォルトで無効になっており、適切な構成可能なパラメータを指定して有効にする必要があります。

**重要** コア ダンプの生成は、パフォーマンスに影響を与えるアクティビティです。そのため、コア ダンプを 15 分ごとに 1 つまたは 2 つのコア ダンプなどの最小数に制限することをお勧めします。その結果、パフォーマンスへの影響が見られる場合は、コア ダンプを微調整する必要があります。

### コア ダンプ ユーティリティ ログへのメッセージのロギング

次に、コア ダンプ ユーティリティ ログの LogTag の例を示します。

```
2022/10/14 09:14:38.809 [WARN] [smf-service.smf-app.pdusetup-procfailure] [Txn Id: 3]
{PDU Session Establishment} -> COREDUMP ->
Generating Core: current core count 1,
File:/opt/workspace/smf-service/src/smf-service/procedures/pdusetup/procedure.go:612
2022/10/14 09:15:38.817 [WARN] [smf-service.smf-app.pdusetup-procfailure] {PDU Session
Establishment} -> COREDUMP ->
Generating Core: current core count 2,
File:/opt/workspace/smf-service/src/smf-service/procedures/generic/CallFailureDebug.go:70
```

## コア ダンプ ユーティリティ ログの構成

この機能を構成するには、次の構成を使用します。

```
config
   dump core [ count count_number | interval interval_details | expires
expires_details | pod-name pod_name | file-detail file_detail ]
   end
```

注：

- **count** *count_number*：コア ダンプを取得できる最大回数を指定します。例：15 分間に 2 つのコア ダンプを取得できます。ここで、2 はカウントです。範囲：0～50
- **interval** *interval_details*：コア ダンプを取得する間隔の合計期間（分単位）を指定します。例：2 つのコアを 15 分で取得できます。この場合、2 つのコア ダンプを取得する合計間隔は 15 分です。範囲：1 ー 3600
- **expires** *expires_details*：コア エージェントがコア ダンプの生成を停止するまでの時間を指定します。フォーマット：CCYY-MM-DDTHH:MM:SS、例：2020-03-24T23:15:00+05:30 または 2022-10-17T19:00:00+00:00
- **pod-name** *pod_name*：コア ダンプのアクティビティを有効にするポッドの名前をリストします。
- **file-detail** *file_detail*：ファイル名、特定のコア ダンプの行番号をリストします。例：Procedures または PDUIM または process.go:1902 で、最大サイズは 10 です。
- 詳細については、「トラブルシューティング情報」>ログ （2100 ページ）を参照してください。

### 設定例

次に、設定例を示します。

```
dump core count 2 interval 15 expires pod-name [ smf-service-n0-0 smf-service-n0-1 ]
file-detail [ procedures/generic/CallFailureDebug.go:70
procedures/pdusetup/procedure.go:612 ]
```

### 設定の確認

設定を確認するには、次のコマンドを実行します。

```
[smf] smf# show running-config dump core
dump core
count 2 interval 15 expires 2023-01-18T18:00:00-00:00 pod-name [ smf-service-n0-0
smf-service-n0-1 ] file-detail [ procedures/generic/CallFailureDebug.go:70
procedures/pdusetup/procedure.go:612 ]
exit
```

# サブスクライバ(MonSub)ログを監視

次に、SMFに対するセッション管理ポリシーをトリガーするモニターサブスクライバ（MonSub）ログの概要を示します。

- ログは、モニター サブスクライバの CLI が有効になった場合に、トランザクションログのロギング レベルを制御するのに役立ちます。
- Monitor Subscriber CLI は、指定された SUPI または IMSI のトランザクション ログをキャプチャします。
- モニター サブスクライバロガーは、モニター サブスクライバの CLI がトリガーされるサブスクライバに使用される特定のロギング レベルを使用します。
- SMF は、サブスクライバ単位のモニタリング アクティビティをサポートしている必要があります。必要に応じて、SUPIやIMSIなどの適切な設定可能なパラメータに基づいて特定のサブスクライバをモニターするために使用する必要があります。
- デフォルト値では、モニターサブスクライバ機能は無効になっています。これは、適切な設定可能なパラメータを指定することにより、手動で有効になります。

### MonSub ログへのメッセージのロギング

次に、MonSub ログの LogTag の例を示します。

```
smf# monitor subscriber imsi 123456789012345 capture-duration 3600 transaction-logs yes

internal-messages yes
Fri Oct 14 09:05:53.902 UTC+00:00
supi: imsi-123456789012345
captureDuration: 3600
enableInternalMsg: true
enableTxnLog: true
namespace(deprecated. Use nf-service instead.): none
nf-service: none
```

```
gr-instance: 0
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 318 100 116 100 202 12888 22444 --:--:-- --:--:-- --:--:-- 35333
Command: --header Content-type:application/json --request POST --data

{"commandname":"mon_sub",
"parameters":{"supi":"imsi-123456789012345",
"duration":3600,"enableTxnLog":true,"enableInternalMsg":true,
"action":"start","namespace":"none","nf-service":"none",
"grInstance":0}} http://oam-pod:8879/commands
Result start mon_sub,
fileName
->logs/monsublogs/none.imsi-123456789012345_WithTxnLogs_TS_2022-10-14T09:05:53.926268924.txt
Starting to tail the monsub messages from
file:
logs/monsublogs/none.imsi-123456789012345_WithTxnLogs_TS_2022-10-14T09:05:53.926268924.txt
Defaulted container "oam-pod" out of: oam-pod, apache
Transaction Log received from Instance: SMF.nodemgr.DC.SMF.1
************* TRANSACTION: 00166 *************


TRANSACTION SUCCESS:
Start Time : 2022/10/14 09:07:24.449
GR Instance ID : 1
Txn Type : GtpcAssocEstReq(2114)
Priority : 1
Session Namespace : none(0)
CDL Slice Name : 1
LOG MESSAGES:
2022/10/14 09:07:24.449 [TRACE] [infra.message_log.core] >>>>>>>>
IPC message
Name: GtpcAssocEstReq
MessageType: GtpcAssocEstReq
Key:
--body--


{"IPv4address":167844075,"restart_counter":65535,
"nodemgr_instance_id":1,"timestamp":1665738444,
"gtpcPathStatus":2,"gtpcInterfaceType":4,"ddnInfo":{},
"gr_instance_id":1,"isNodeStarted":true}
2022/10/14 09:07:24.449 [DEBUG] [nodemgr1.app.Int] GetSessionNamespace for txn id: 166,
 Type: 2114
2022/10/14 09:07:24.449 [DEBUG] [nodemgr.gtpmgr.gtp] Received New GTP Peer info
[&GtpcAssocEstReq{IPv4Address:167844075,IPv6Address:[],SupportedFeatures:0,RestartCounter:65535,
NodemgrInstanceId:1,Timestamp:1665738444,OverloadControl:nil,GtpcPathStatus:GTPC_PATH_UP,
GtpcInterfaceType:4,DdnInfo:&DdnInfo{DelayValid:false,ThrottleValRcvd:false,ThrottleActive:false,
DelayValue:0,ThrottleDelayValue:0,ThrottleDelayUnit:0,ThrottleFactor:0,},GrInstanceId:1,
IsNodeStarted:true,SelfRCVal:0,PeerType:0,DeletedAt:0,}]
2022/10/14 09:07:24.449 [INFO] [nodemgr.gtpmgr.gtp] GTPC Path Mgmt Disabled for interface
 [4]
2022/10/14 09:07:24.449 [INFO] [nodemgr.gtpmgr.gtp] Rcvd timestamp 1665738444, stored
timestamp 1665738177
peer 10.1.24.235
2022/10/14 09:07:24.449 [DEBUG] [nodemgr.gtpmgr.gtp] Assoc req for already present peer
 [10.1.24.235]
```

```
2022/10/14 09:07:24.449 [DEBUG] [nodemgr.gtpmgr.gtp] stop timer for existing gtp-peer
[10.1.24.235]
2022/10/14 09:07:24.451 [TRACE] [infra.message_log.core] <<<<<<<<


**********************************************
Transaction Log received from Instance: SMF.nodemgr.DC.SMF.1
************* TRANSACTION: 00167 *************
TRANSACTION SUCCESS:
Start Time : 2022/10/14 09:07:34.061
GR Instance ID : 1
Txn Type : GtpcAssocEstReq(2114)
Priority : 1
Session Namespace : none(0)
CDL Slice Name : 1
LOG MESSAGES:
2022/10/14 09:07:34.062 [TRACE] [infra.message_log.core] >>>>>>>>
IPC message
Name: GtpcAssocEstReq
MessageType: GtpcAssocEstReq
Key:
--body--

{"IPv4address":167844075,"restart_counter":100,"timestamp":1665738454,"gtpcInterfaceType":4,
"ddnInfo":{},"isNodeStarted":true}
2022/10/14 09:07:34.062 [DEBUG] [nodemgr1.app.Int] GetSessionNamespace for txn id: 167,
 Type: 2114
2022/10/14 09:07:34.062 [DEBUG] [nodemgr.gtpmgr.gtp] Received New GTP Peer info
[&GtpcAssocEstReq{IPv4Address:167844075,IPv6Address:[],SupportedFeatures:0,RestartCounter:100,
NodemgrInstanceId:0,Timestamp:1665738454,OverloadControl:nil,GtpcPathStatus:GTP_PATH_INVALID,
GtpcInterfaceType:4,DdnInfo:&DdnInfo{DelayValid:false,ThrottleValRcvd:false,ThrottleActive:false,
DelayValue:0,ThrottleDelayValue:0,ThrottleDelayUnit:0,ThrottleFactor:0,},GrInstanceId:0,
IsNodeStarted:true,SelfRCVal:0,PeerType:0,DeletedAt:0,}]
2022/10/14 09:07:34.062 [INFO] [nodemgr.gtpmgr.gtp] GTPC Path Mgmt Disabled for interface
 [4]
2022/10/14 09:07:34.062 [INFO] [nodemgr.gtpmgr.gtp] Rcvd timestamp 1665738454,
stored timestamp 1665738444 peer 10.1.24.235
2022/10/14 09:07:34.062 [DEBUG] [nodemgr.gtpmgr.gtp] Assoc req for already present peer
 [10.1.24.235]
2022/10/14 09:07:34.062 [DEBUG] [nodemgr.gtpmgr.gtp] stop timer for existing gtp-peer
[10.1.24.235]
2022/10/14 09:07:34.065 [TRACE] [infra.message_log.core] <<<<<<<<

**********************************************
```

## モニタ サブスクライバ ログの構成

この機能を構成するには、次の構成を使用します。

```
config
   monitor subscriber [ supi supi_id | imsi imsi_value | imei imei_id |
capture-duration capture_duration | dump dump_name | gr-instance gr_instance_id
 | internal-messages internal_messages | list list_details | namespace
namespace_details | nf-service nf_service_details | transaction-logs
transaction_logs ]
   end
```

注：

- **supi** *supi_id*—サブスクライバ識別子を指定します。例えば、imsi-123456789、imsi-123*
- **imsi** *imsi_value*— サブスクライバ IMSI を指定します。たとえば、123456789、* などです。
- **imei** *imei_id*— サブスクライバ IMEI を指定します。例：123456789012345、*
- **capture-duration** *capture_duration*：モニタ サブスクライバアクティビティをキャプチャする期間を秒単位で指定します。デフォルトは 300 秒（5 分）です。これは省略可能なパラメータです。
- **dump** *dump_filename*：ダンプ ファイルの名前を指定します。例： monitor subscriber-dump [filename]
- **gr-instance** *gr_instance_id*：GR インスタンス ID を指定します。これは省略可能なパラメータです。これは、特定の gr-instance 専用のモニター サブスクライバです。インスタンス ID 1 はローカル インスタンス ID を示しています。
- **internal-messages** *internal_messages*：yes に設定すると、内部メッセージングが有効になります。デフォルトでは、無効な値 これはオプションのパラメータです。
- **list** *list_details*：リストの詳細を指定します。これには、モニター サブスクライバ リスト ファイルが含まれます。
- **namespace** *namespace_details*：指定した名前空間を有効にします。デフォルトでは、名前空間は none に設定されています。これは省略可能なパラメータです。

（注） リリース 2021.02.0 内の廃止キーワードと nf-service をキーワードとして置き換えられました。

- **nf-service** *nf_service_details*—指定した NF サービスを有効にします。デフォルトでは、nf-service は none に設定されています。これは必須パラメータです。可能な値：sgw、smf、pgw

（注） nf-service キーワードは、リリース 2021.02 以降では namespace キーワードに置き換わります。

- **transaction-logs** *transaction_logs*：yes に設定されている場合、トランザクションログを有効にします。デフォルトでは、無効な値です。これは省略可能なパラメータです。

（注） トランザクション履歴ログを表示するには、ダンプ トランザクション履歴コマンドを使用します。最新のトランザクション ログは、トランザクション ログ サイズが 1024 の循環キューに保存されます。

- 詳細については、「障害対応情報」 > ログ （2100 ページ）を参照してください。

**重要** MonSub には 、monitor subscriber コマンドでサブスクライバ SUPI または IMSI が必要です。重要なアクションは次のとおりです。

- 前提条件として、SMF はサブスクライバの SUPI または IMSI を ログに出力する必要があります。
- 現在、SMF トランザクション ログは、トランザクション ログにサブスクライバの SUPI または IMSI を含むサブスクライバ セッション キーを出力しています。
- オペレータは、これらのログからサブスクライバの SUPI または IMSI を選択できます。

### 設定例

次に、設定例を示します。

```
logging level monitor-subscriber info
logging name infra.message_log.core level monitor-subscriber debug
```

### 設定の確認

設定を確認するには、次のコマンドを実行します。

```
smf# show running-config logging
logging level monitor-subscriber info
logging name infra.message_log.core level monitor-subscriber debug
```

# N40 追加のログと

次に、SMF に対するセッション管理ポリシーをトリガーする N40 の追加のログと統計情報の概要を示します。

- 追加の LogTag またはラベルで構成される rest-ep の現在のメッセージ レベルの統計を次のように拡張します。
  - DNN タイプ
  - RAT タイプ
  - PDNタイプ
  - [プロシージャのタイプ（Procedure type）]
  - エラーがある場合のエラー原因のタイプ。
  - インターフェイスの障害
- 現在のメッセージレベルの統計情報が拡張されると、rest-epがすでに同じメッセージで構成されているため、メッセージ レベルの統計情報などの SMF サービスからの冗長な統計情報を削除できます。

- 次のように、CHF で開始されたすべてのメッセージについて問題とその詳細を更新できます。
  - 通知
  - 中止の場合
  - 再認証（Re-Auth）
- N40 の追加ログと統計のトランザクション ロギング レベルとログタグが 同期している必要があります。障害シナリオが発生した場合は、N40 に該当するログタグを 追加する必要があります。リストの内容は次のとおりです：
  - メジャー（エラー）
  - メジャー（警告）
  - 通常（情報）
- 対応するカテゴリでロギング レベルが有効になると、次のオプションが使用可能になります。
  - イベント トレース
  - コアダンプ

## N40 追加ログと統計情報の構成

この機能を構成するには、次の構成を使用します。

**logging name smf-service.smf-app.chf level transaction debug-level**

注：

- **Warning | Error**：N40 の追加ログおよび統計情報の LogTags でサポートされるロギング レベル。
- 詳細については、「トラブルシューティング情報」>ログ （2100 ページ）を参照してください。

### 設定例

次に、設定例を示します。

```
logging name smf-service.smf-app.chf level transaction warn
```

### 設定の確認

設定を確認するには、次のコマンドを実行します。

```
[smf] smf# show running-config logging name smf-service.smf-app.chf
logging name smf-service.smf-app.chf level transaction warn
```

# N7 の追加のログと統計情報

次に、SMF に対するセッション管理ポリシーをトリガーする N7 の追加のログと統計情報の概要を示します。

- PCF によって開始された更新通知の HTTP エラー コードを検出し、問題の詳細を含むメッセージを終了します。
- 追加の LogTag またはラベルで構成される rest-ep の現在のメッセージ レベルの統計を次のように拡張します。
  - DNN タイプ
  - RAT タイプ
  - PDNタイプ
  - [プロシージャのタイプ（Procedure type）]
  - エラーがある場合のエラー原因のタイプ。
  - インターフェイスの障害
- N7 の追加ログと統計のトランザクション ロギング レベルと LogTag が 同期している必要があります。リストの内容は次のとおりです：
  - エラー（Error）
  - 警告
  - 情報
- 対応するカテゴリでロギング レベルが有効になると、次のオプションが使用可能になります。
  - イベント トレース
  - コアダンプ

## N7 の追加ログと統計情報の構成

この機能を構成するには、次の構成を使用します。

```
logging name smf-service.smf-app.pcf level transaction debug-level
```

注：

- **Warning | Error**：N7 の追加ログおよび統計情報の LogTags でサポートされるロギング レベル。
- 詳細については、「トラブルシューティング情報」>ログ（2100 ページ）を参照してください。

## 設定例

次に、設定例を示します。

```
logging name smf-service.smf-app.pcf level transaction warn
```

## 設定の確認

設定を確認するには、次のコマンドを実行します。

```
[smf] smf# show running-config logging name smf-service.smf-app.pcf
logging name smf-service.smf-app.pcf level transaction warn
```

第 43 章

# サブスクライバの課金


- 機能の概要と変更履歴, on page 1853
- 機能説明, on page 1854
- さまざまなインターフェイスでの課金シナリオのマッピング （1885 ページ）
- 障害処理シナリオ （1893 ページ）
- 課金構成のダイナミックな更新 （1900 ページ）
- 静的ルールおよび事前定義済みルールを使用したプリエンプティブ クォータの取得 （1912 ページ）


## 機能の概要と変更履歴

### 要約データ

***Table 496:*** 要約データ

| | |
|---|---|
| 該当製品または機能エリア | SMF |
| 該当するプラットフォーム | SMI |
| 機能のデフォルト設定 | • サブスクライバの課金：無効：構成が必要です。<br>• Gyインターフェイスの最終単位の表示：無効：有効にするには構成が必要です。 |
| このリリースでの関連する変更点 | N/A |
| 関連資料 | 該当なし |

# 更新履歴

***Table 497:*** マニュアルの変更履歴

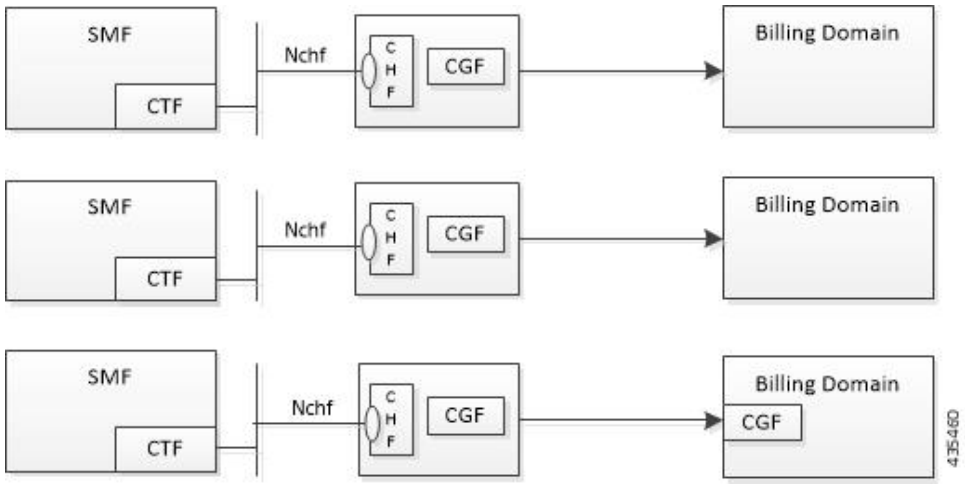
| 改訂の詳細 | リリース |
|---|---|
| サブスクライバの課金の Gz インターフェイスの詳細を追加しました。 | 2023.04.0 |
| 次の機能に対して追加サポート：<br>• APN、ECS、および課金プロファイルの構成のダイナミックな変更を追加しました。<br>• GTPP による GZ 使用率レポートの処理。<br>• Gyインターフェイスでの最終単位表示のサポートが追加されました。 | 2023.03.0 |
| 次の機能に対して追加サポート：<br>• 課金無効化機能<br>• スタティック ルールおよび事前定義済みルールの QoS 記述子の処理 | 2023.01.0 |
| 課金特性 ID の範囲値の拡張のサポートが追加さ」れました。 | 2021.02.3.t3 |
| クエリ インターフェイス IE のサポートが追加されました。 | 2021.02.0 |
| CHF が到達不能な場合の請求レコードの調整のサポートが導入されました。 | 2021.02.0 |
| N4 インターフェイスにセッション レベルの制限が追加されました。 | 2021.01.1 |
| 次のサポートが追加されました。<br>• ゼロ使用レポート抑制<br>• ダイナミックな ACS 構成変更 | 2021.01.0 |
| 最初の導入。 | 2020.02.0 より前 |

# 機能説明

SMF は、課金転送機能（CTF）として機能します。CTF は、課金データ レコード（CDR）の生成を担当する課金機能（CHF）に対して課金イベントを生成します。

このSMFは、N40、Gy、N4、N7、N10などのさまざまなインターフェイスと相互作用して、課金全体を促進します。SMFは、Nchf/N40、オンライン課金システム（OCS）/Gy、およびオフライン課金システム（OFCS）/Gzインターフェースを使用して課金イベントを生成します。

***Figure 301:*** 課金転送機能としての ***SMF***




SMF は、以下の機能と機能性をサポートします。

- オンライン課金とオフライン課金の統合。
- サービスベースのインターフェイスを使用した PDU セッションの課金。
- ネットワーク スライス インスタンスの課金。
- 3GPP および非 3GPP アクセス（信頼できない非 3GPP アクセス、信頼できる非 3GPP アクセス、および有線）で提供される UE の PDU セッションごとの課金情報の収集。

**Note** SMF 構成に OCS/OFCS のネットワーク要素プロファイルを持つ DNN プロファイルがある場合、OCS/OFCS課金動作は SMF 4G セッションに適用されます。

- 請求を目的とした PDU セッションごとの一意の ID 番号の割り当て。
- アップリンクとダウンリンクの両方向のデータボリュームを個別にカウントします。データ ボリュームは、ユーザーに配信または転送されたデータを反映します。
- PDU セッションが開始される日時情報を提供する課金メカニズム。
- サブスクリプションまたはサブスクリプション済みのDNNに固有の課金特性の処理。
- 個々のサービス データ フロー（フローベースの課金）のデータ量、経過時間、またはイベントの識別。1 つの PCC ルールは 1 つのサービス データ フローを識別します。

- 料金設定グループごと、または料金設定グループとサービスIDの組み合わせごとの、サービスの使用状況レポート、検出されたアプリケーション。このレポートレベルはPCCルールごとに有効化できます。
- N40の場合は料金設定グループ（RG）ごと、Gy/Gzの場合はRG/RG+SIDごとにPDUセッションごとにクォータを管理します。
- IP ベースの PDU セッション タイプの課金。

# コンバージド課金

5G システムは、オフラインおよびオンラインの充電シナリオでの統合型充電をサポートしています。

SMF は次のそれぞれに対して統合型課金を実行します。

- PDU セッションに関連する課金データ。
- PDU セッション内のサービスデータ フローに関連する課金データ。

この導入でのコンバージェント課金の範囲には、クォータ管理と使用状況レポートが含まれます。コンバージェント充電の場合、SMFはCHFまたはOCS/OFCSと連携して、PDUセッションに関連する課金データを取得します。課金データ要求メッセージおよび課金データ応答メッセージは、セッションベースの課金（SCUR シナリオ）に基づいて SMF と CHF の間で交換されます。課金データ要求は、課金対象イベントに関連する条件が満たされた場合にのみ、SMF によって発行されます。

## 課金対象イベント

PDU セッションのライフタイム中いつでも、PCC 課金ルールをアクティブ化、非アクティブ化、および変更できます。

PCFは、SMFでアクティブになっているダイナミックPCCルールの次の属性を変更できます。

- 課金キー
- Service Identifier
- 計測方法

**Note** Gy/Gz の変更はサポートされていません。

PCC ルールおよび QoS フローでのアクティビティは請求対象のイベントではありません。ただし、PCCルールの課金ルールの変更により、課金対象イベントが発生します。例の一部を次に示します。

- サービス データ フローの開始。
- 元のPCCルールの最後のサービスデータフローに関するサービスデータフローの終了。

課金キー（つまり、料金設定グループ）は、オンライン課金クォータを要求するために使用されます。

**Note** PCRF から受信したレポートレベルに応じて、次の手順を実行します。

- Gy の場合、クォータは料金設定グループ（RG）または料金設定グループとサービス ID（RG+SID）に基づいて要求されます。
- Gz の場合、クォータは RG または RG + SID に基づいて報告されます。

レポート レベルを受信しない場合、クォータは、PCRF から受信した料金設定グループまたはサービス ID の値から導出されます。

## 課金 ID

課金識別子は、PDU セッションの期間中に SMF と CHF または OCS /OFCS 間の課金情報を関連付けます。SMF は PDU セッションが確立されたときに課金 ID を生成して割り当てます。課金 ID は、その PDU セッションで一意であり、その PDU セッションで交換されるすべてのメッセージで使用されます。

## 請求情報

SMF は、オンライン課金とオフライン課金について次の課金情報を収集します。

- アクセスおよびコア ネットワーク リソースの使用状況：UE に配信および UE から転送されるデータの量を記述します。
- 使用期間：PDU セッションの確立から PDU セッションのリリースまでの時間間隔。
- ユーザー：PDU セッションのユーザーによって使用される UE 情報。
- データネットワーク：DNN によって決定されたデータネットワークアドレス。
- 開始時間：PDU セッションの開始時刻。
- ユーザの場所：HPLMN および VPLMN レポートエリア。

サービス データ フロー（フロー ベースの課金）の場合、SMF は次の情報を収集します。

- PDU セッションの説明。
- 料金設定グループ情報、またはボリュームベースの課金時に料金設定グループとサービス ID の組み合わせに基づいて、アップリンクおよびダウンリンク方向で送信されるデータ。
- 料金設定グループに基づくサービス データ フローの期間、またはイベントベースの課金における料金設定グループとサービス ID の組み合わせ。
- イベントベースの課金が適用される場合に、料金設定グループ、または料金設定グループとサービス ID の組み合わせによって分類されるイベントおよび対応するタイムスタンプの数。

SMF は、料金設定グループ、または料金設定グループとサービス ID の組み合わせに基づいて、PDU セッション内で UPF ごとにサービス データ フローの課金情報を収集します。

# 機能の仕組み

## 充電セッション

SMF は 、*3GPP TS 32.290*、セクション *5.3.2.3*で指定されているように、セッション ベースの統合型課金（SCUR）をサポートします。Gy が有効になっている場合、SMF では *3GPP TS32.299*、*12.9.0* セクション *6.4*で指定されているセッションベースの課金がサポートされます。Gz が有効になっている場合、SMF では*3GPP TS32.298*、*12.9.0*セクション *5.1.2.2*で指定されているセッションベースの課金がサポートされます。

SMF は課金データ要求/応答（初回）交換でCHF との課金セッションを確立します。PDUセッションの期間中は、課金データ要求または応答（更新）の交換で使用量が報告されます。セッションが解放されると、課金データの要求または応答（終了）メッセージが交換されます。

Gy が有効になっている 4G セッションの場合、SMF は、クレジット制御要求とクレジット制御応答（初期）メッセージ交換を送信することにより、OCS との課金セッションを確立します。PDUセッション中に、使用状況がクレジット制御要求およびクレジット制御応答（更新）メッセージとともに報告されます。セッションの解放後、クレジット制御要求メッセージとクレジット制御応答（終了）メッセージが交換されます。

Gz が有効になっている 4G セッションの場合、ダイナミック PCC ルールが受信されると、SMF はオフライン URR を作成します。次に、SMF は PCC ルールを対応する課金バケット（サービス データ フロー（SDF））にマッピングし、N4 確立要求を CnPGW-U に送信します。 PDU セッションの存続期間中、オフライン SDF またはベアラー レベルの URR の使用状況が N4 セッション レポートを介して報告されるか、UPF からの N4 削除セッション応答で、GTPP データ レコード転送要求を GTPP に送信する場合があります。

## オフライン充電とオンライン充電

***Table 498:*** **機能の履歴**

| 機能名 | リリース情報 | 説明 |
|---|---|---|
| サブスクライバの課金に対する GZ のサポート | 2023.04 | 4G セッションの Gz を有効にして、ダイナミック ルールの場合にデフォルトのベアラー レベル URR および SDF レベル URR を使用して SMF が N4 確立要求を送信できるようにすることができます。 |

PCF または PCRFから受信した入力に基づいて、セッションに対する課金が有効になります。

オフライン課金の場合、SMF は、SM ポリシー制御作成応答内の PCF からの smPolicyDecision メッセージで設定された課金記述子と refChgData フィールドの存在に基づいて、課金データ要求の初期を課金機能（CHF）に送信します。

初期セッションの確立時またはセッション後の確立時に課金が必要かどうかの決定時に、課金が PDU セッションに対して有効になります。課金が有効になると、SMF は課金データ要求（初期）メッセージを CHF に送信します。

SMF は、ボリューム/時間のしきい値をローカルに、または課金データ応答から決定します。これらの値は、URR のボリューム/時間しきい値 IE を更新し、それに応じてレポート トリガーを設定するために使用されます。URR で使用される測定方法は、課金データから導出されます。

オンライン課金の場合、SMF は CHF からボリューム/時間しきい値とクォータの値を受信します。これらの値は、課金データ応答（初回）で受信されるか、または PDU セッション確立時に課金データ要求（更新）を使用して受信されます。SMF は、これらのボリューム/時間のしきい値とクォータの値を対応する URR の UPF にリレーします。

SMF 4G セッションに対して Gy が有効になっている場合、セッションの SMF は、ボリューム/時間のしきい値とクォータ値を取得するために、クレジット制御要求（初期）を OCS に送信します。SMF はこれらの値を対応する URR の UPF にリレーします。SMF が OCS からボリュームしきい値を受信しない場合、SMF はローカル構成からボリュームしきい値を決定します。

SMF 4G セッションで Gz が有効になっている場合、SMF は、ダイナミック ルールの場合にデフォルトのベアラー レベル URR と SDF レベル URR を含む N4 確立要求を送信します。静的で事前に定義されたルールの場合、URR はトラフィックの開始（SoT）で受信した PFCP セッション レポートの後に作成されます。ベアラー レベルの URR TIME_THRESHOLD および VoLUME_THRESHOLD の値は、ルールベースのプロファイルで構成された egcdr のしきい値から受信されます。SDF レベル URR TIME_THRESHOLD および VoLUME_THRESHOLD の値は、課金プロファイルで構成された egcdr しきい値から受信されます。すべての SDF レベルの URR は、ベアラー レベルの URR にリンクされます。

**Note** CHF からのしきい値は、ローカルで構成された値を常にオーバーライドします。

次の表は、オンラインまたはオフラインの課金シナリオでの URR の作成または更新中に UPF と共有される IE のマッピングを示しています。

***Table 499:*** **オンラインおよびオフラインの課金シナリオの *IE* マッピング**

| IE | オンライン | オフライン | （N40）から派生 | Gy から派生 | Gz から派生 |
|---|---|---|---|---|---|
| Volume Limit | はい | はい | CHF 応答または ローカル構成 | OCS 応答または ローカル構成 | - |
| Time Limit | はい | はい | CHF 応答または ローカル構成 | OCS 応答 | - |

| IE | オンライン | オフライン | （N40）から派生 | Gy から派生 | Gz から派生 |
|---|---|---|---|---|---|
| ボリュームクォータ | はい | 非対応 | CHF 応答 | OCS 応答 | - |
| 時間クォータ | はい | 非対応 | CHF 応答 | OCS 応答 | - |
| クォータ保持時間 | ○ | — | CHF 応答 | OCS 応答 | - |
| モニタリング時間 | はい | はい | • オフライン充電用のローカル構成<br>• オンラインチャージングのCHF応答 | OCS 応答またはローカル構成 | - |
| レポートするトリガー | はい | はい | 設定されるそれぞれのトリガーが次の表に示されています。 | OCS 応答またはローカル構成 | ローカル設定 |
| 有効期間 | はい | - | - | OCS 応答またはローカル構成 | - |

次の表に、レポート トリガーとその派生した送信元を示します：

***Table 500:*** レポートするトリガーと派生した送信元

| レポートするトリガー | N40 から派生 | Gy から派生 | Gz から派生 |
|---|---|---|---|
| ボリュームしきい値トリガー | ボリュームしきい値が設定されている場合 | OCS応答またはローカル構成 | ボリュームしきい値が設定されている場合 |
| 時間しきい値トリガー | 時間しきい値が設定されている場合 | OCS応答またはローカル構成 | 時間しきい値が設定されている場合 |
| ボリューム クォータ トリガー | クォータを使い果たしたトリガーがCHFから設定されている場合 | OCS応答またはローカル構成 | - |
| 時間クォータ トリガー | クォータを使い果たしたトリガーがCHFから設定されている場合 | OCS応答またはローカル構成 | - |
| リンクされた使用状況レポート（LIUSA）トリガー | URR にリンクされたURRが含まれている場合 | - | URR にリンクされたURRが含まれている場合 |

## Quota Management

SMF は、次のいずれかの条件を満たすと、CHF にクォータを要求します。

- 料金設定グループ（RG）が初めてインストールされ、課金方法がダイナミック ルールに対してオンラインになります。
- スタティック ルールまたは事前定義済みルールの場合、トラフィック トリガの開始は、RG の UPF から開始されます。
- 3GPP 仕様 32.255 で定義されている特定のトリガ タイプは、オンライン課金サービスの使用状況レポートで UPF から受信されます。

SMF は **quota request always** CLI コマンドを使用して、常にクォータを要求します。この CLI コマンドは、課金プロファイル コンフィギュレーション モードで利用可能です。この CLI コマンドを構成すると、SMF はオンライン サービスの CHF に使用状況を報告するときに、常にクォータを要求します。クォータ要求は、課金サービスが停止したときに終了します。

**quota request [ always | standard ]** CLI の構成に関係なく、 **quota suppress triggers** CLI コマンドを使用して構成されたトリガ タイプ「qht」のクォータ要求は無効になります。

4G セッションで Gy が有効になっている場合、 **send charging-initial** CLI コマンドが **on-receving-rule** および **reqQuotaForDynRules** CLI として構成されている場合、SMF は、要求されたサービス ユニット（RSU）属性を含むクレジット制御要求イニシャル（CCR-I）メッセージを OCS に送信します。コマンドは **session-start** として構成されます。**send charging-initial** が使用可能な場合にのみ、CCR-I メッセージは RSU なしで送信されます。**charging-initial** および **reqQuotaForDynRules** CLI コマンドが **traffic-start** と構成されている場合、SMF はトラフィックの開始でセッション レポートを受信したときに、RSU とともに CCR-I メッセージを送信します。SMF は、PCRF から受信したレポート レベル、または課金プロファイルで利用可能なローカル構成（RG または RG + SID）に基づいて、クォータを要求します。

4G セッションで Gy が有効になっている場合、SMF は課金プロファイルで次の CLI コマンドを使用します。

- **send charging-initial [session-start | traffic-Start]**

（注） デフォルト値は **session-start** です。

- **dynamic-rules [request-quota on-receiving-rule | start-of-traffic]**

（注） デフォルト値は **on-receving-rule** です。

### クォータ管理のサービス ユニット

SMF は、課金機能（CHF）に課金データレコード（CDR）を送信して開始を許可し、ユニット数を予約します。CDR のトリガー中、SMF は VoLTE やその他の使用例をサポートするために、CHF にボリューム（アップリンク、ダウンリンク、合計）と時間クォータを要求します。

静的ルールの要求単位の値は、アクティブな課金サービスのDiameter構成から取得されます。動的オーディオまたはビデオ ルールの場合、要求されたサービスユニットの値は、課金プロファイル構成モードで **requested-service-unit** CLI コマンドを介して構成されます。

（注） Gz 対応 SMF が OFCS と連携して使用状況を報告する場合、ベアラー レベルと SDF レベルの値は、それぞれルールベースと課金プロファイルのローカル egcdr 構成から受信されます。

### 有効期間のサポート

SMFは、時間クォータ値とN4インターフェイス上の対応するトリガを使用して、SMFが有効時間の報告を必要とする時間についてUPFを支援します。

CHFは、validity_timeに関連付けられているタイマーが期限切れになったときに、SMFに料金設定グループの使用状況を報告するように準備します。

有効性クォータと時間クォータの存在に基づいて、SMFは次のように指定されているように動作します。

- CHF が時間クォータのみを送信し、有効クォータを送信しない場合、SMF は CDR-U を CHF にリレーし、UPF からの使用状況レポートを受信すると Quota_EXHAUSTED と報告します。
- CHF が時間クォータではなく有効性クォータのみを送信する場合、SMF はCDR-U を CHF にリレーし、UPF からの使用状況レポートを受信すると VALIDITY_TIME として報告します。
- CHF が有効性クォータと時間クォータの両方を送信すると、SMF は time_quota と validity_timeの小さい方の値を決定し、それに応じてCDR-U をCHFにリレーします。SMF は、validity_time が time_quota 値よりも小さい場合に、「VALIDITY_TIME」トリガを送信します。同様に、validity_time が time_quota 値より大きい場合、SMF は「Quota_EXHAUSTED」トリガを送信します。

上記の動作に加えて、SMF はボリュームと期間に関して 1 つの USU とともに Gy CCAU を送信します。Gy では、有効期間のボリュームと期間とともに使用状況レポートを受信すると、SMF はレポートを UPF に転送します。

## CHF の選択

CHF の選択は、次のいずれかのオプションで実行できます：

1. PCC ルールの一部として PCF が提供する 1 つ以上の CHF アドレス
2. UDM が提供する課金特性
3. NRF ベースの検出
4. SMF ローカル プロビジョニングの充電特性

**Important** SMF は、最後の 2 つのオプションのいずれかを使用して、CHF IP アドレスとポートの詳細を取得します。SMF は最初に NRF ベースの検出を実行して CHF サーバーを選択します。SMF がサーバーを識別できない場合、ローカルにプロビジョニングされた課金特性を使用します。Gy が有効になっている場合、SMF はローカルに構成された Diameter クライアント プロファイルを使用して OCS サーバーに接続します。同様に、Gz が有効になっている場合、SMF はローカルに構成された GTPP プロファイルを使用してオフライン課金システム（OFCS）サーバーに接続します。

# SMF での課金アクティビティ

N4 に向けた URR 生成

SMF は PCF から課金データと使用状況モニタリング データを受信します。この情報に基づいて、SMF は N4 に対する URR を導き出します。セッション レベルでボリューム/時間制限が SMF に構成されている場合、SMF はセッション レベルの URR を作成します。

## 課金コンポーネントの初期イベントの処理

SMF のセッション コンテキストは 、*3GPP TS 32.255*で説明されているデフォルトに従って、トリガー/しきい値を使用して設定されます。これは、課金プロファイルの構成に基づいて上書きされます。同じ値は、CHF Charging Data Response Initial によってさらにオーバーライドできます。現在、PDU 確立状態の場合、トリガー/しきい値をオーバーライドすることはできません。

課金プロファイルは、課金特性プロファイルから参照されます。CC プロファイルは、PDU セッションの UDM サブスクリプションから取得されます。CC プロファイルが UDM 応答に記載されていない場合は、DNN プロファイルから取得されます。

トリガー/しきい値/クォータが決定された後、Create URR のセットを含む SMF N4 セットアップ要求が 1 つのセッションレベルの URR を持つ課金データから派生します。

セッションレベルのレポートが決定されると、セッションレベルの URR は各 SDF URR に関連付けられます。

次のトリガーがサポートされています：

- Volume/Time trigger at session/RG level (N40) /RG or RG+SID level (Gy/Gz)
- AMBR の変更
- QoS の変更
- クォータしきい値とクォータを使い果たしました
- クォータ処理時間
- タリフ時間の変更

**Note** Gz は、QoS、URI、および MrsTimezone トリガーのみをサポートします。

## SMF でのしきい値の取得

オンライン課金中のしきい値は、常に CHF/OCS から取得されます。Gy の場合、OCS 応答でボリュームしきい値を使用できない場合、ボリュームしきい値はローカル構成から取得されます。一方、オフライン課金中のしきい値は、CHF または課金プロファイル構成のいずれかから取得されます。

課金プロファイルが PDU の確立時に決定されない場合、SMF は DNN プロファイルから課金プロファイルを参照します。課金プロファイルが決定されると、SMF は決定された課金プロファイルを使用してセッション/SDF URR のしきい値を取得します。

Gz の場合、しきい値はベアラー レベル URR のルールベースから、SDF レベル URR から課金プロファイルを受信します。

この構成には、セッション レベルまたは評価グループ レベルでのしきい値があります。1 つのレーティング グループ レベルのしきい値は汎用的なもので、1 つのレーティング グループに関するものではありません。これらのしきい値は、CHF 応答によって上書きされます。

Gz インターフェイスは、課金プロファイルから適用される SDF レベルの構成をサポートします。このインターフェイスは、料金設定グループ レベルの構成をサポートしていません。

**Note** CHF 応答にはさまざまなトリガーがあります。セッションレベルまたは料金設定グループ レベルで使用できるトリガがあり、ボリュームまたは時間のしきい値が使用できない場合、これらの値は対応するレベルで無効になっていると見なされます。

## SMF での決定のトリガー

SMF では、3GPP TS 32.255、セクション 5.2.1.4 で規定されているように、デフォルトでトリガーが有効になっています。

これらのトリガーは、課金プロファイルに存在するトリガー構成によって、セッション レベルで上書きできます。さらに、これらのトリガーは、CHF/OCS 応答によって上書きすることもできます。

課金プロファイルのトリガー構成は、セッション レベルにのみ適用されます。料金設定グループには適用されません。トリガーの構成は、SDF のレベルで適用されます。

Gz の場合、トリガー構成は SDF レベルの URR に適用できます。

## レポート カテゴリ

課金トリガは、即時と遅延の 2 つのレポート カテゴリのいずれかになります。即時カテゴリの使用状況レポートは、CHF にすぐに報告する必要があります。保留する必要があるレポート イベントの場合、SMF は使用状況レポートをローカルに保存し、即時カテゴリの次のトリガが呼び出されたとき、またはストレージ制限を超えたときに公開します。

保存された使用状況レポートを CHF に報告する場合、UsedUnitCategory のトリガ タイプにより使用状況レポートがトリガされ、ChargingDataRequest にあるトリガ タイプによりメッセージがトリガされます。

場合によっては、シナリオで2つのトリガが同時にヒットすることがあります。AMBR_Change と QoS の変更は同時に発生する可能性があります。この場合、RG レベルまたはセッション レベルで該当するすべてのトリガに複数のトリガ値が割り当てられます。OCS の場合、すべてのトリガが MSCC レベルで適用されます。Gz の場合、すべてのトリガを SDF レベルで適用できます。

トリガは RG レベルで有効にでき、一部の RG では即時レポートを、他の RG ではレポートを遅らせることができます。トリガイベントが発生すると、さまざまな使用状況レポートの対応するカテゴリが usedUnitContainer にそれぞれ入力されます。

遅延 CDR は、次のシナリオでリレーされます。

- 即時カテゴリ イベントが発生した場合。
- 課金条件の最大数を超えた場合。
- 構成された遅延レポートの最大数を超えました。

最大課金特性（CC）は、プッシュ CDR があるたびにリセットされます。これは、最大 CC 制限を超えたか、即時カテゴリ レポートが原因である可能性があります。

Gz の場合、CDR は課金プロファイルの maxlosdb 構成に基づいてリレーされます。

**Note** 現在、SMF は同じ料金設定グループを持つ 2 つの課金記述子をサポートしていません。

Gy の場合は、即時レポート カテゴリのみが適用されます。

## レポート レベルの処理

レポート カテゴリは、次のカテゴリに分類されます：

- 料金設定グループ（RG）レベル：このレベルでは RG は必須です。
- サービス ID レベル：このレベルでは、RG とサービス ID は必須です。
- スポンサー ID レベル：RG とスポンサー ID はこのレベルでは必須です。

PCF は、課金データ要求を介してレポート レベルを SMF に伝達します。レポート レベルが RG の場合、RG がプライマリ キーです。レポート レベルがサービス レベルまたはスポンサー レベルの場合は、RG とサービス ID、または RG とスポンサー ID がそれぞれプライマリ キーになります。SMF は、前述の要件が満たされていない場合、PCF から課金記述子をドロップします。

**Note** Gy または Gz の場合、PCRF はレポート レベルを SMF に伝達します。SMF が PCRF からレポート レベルを受信しない場合、レポート レベルは PCRF から受信した料金設定グループまたはサービス ID の値から導出されます。

## 再認証

CHF は Charging Notify 要求を使用して、課金記述子の再認証をトリガします。再認証は、オンライン課金とオフライン課金の両方に対し、セッションレベルまたは RG レベルで実装されます。

SMF は、CHF Notify で受信した再認証の詳細（RG、ServiceId、QuotaMgmtIndicator の配列を含む）を処理し、現在の PDU セッションに関連付けられている課金記述子を取得します。SMF は、一致しない再許可項目を無視します。

再認証のために識別された課金記述子について、SMF は UPF からの使用状況レポートを照会し、CHF に送信します。

CHF 応答の一部として、SMF はクォータまたはしきい値情報の変更を検出し、N4 セッション変更を実行して URR を更新します。

## N40 インターフェイスでの最終単位表示のサポート

SMF は、3GPP TS 32.291 のセクション 6.1.6.2.1.12 に記載されているように、CHF からの課金データの初期応答または更新応答で N40 の 最終ユニット識別（FUI）をサポートします。

FAA を受信すると、SMF は新しい FAR をインストールし、その FAR ID を FAR ID Quota Action IE で URR に関連付けます。同じパラメータを持つ FAR が存在する場合、SMF は、URR の作成または更新でその FAR-ID を使用します。UPF は、クォータを使い果たした後、FAR に設定された適切なアクションを開始します。

SMF は、OCS からの CCA-I または CCA-U メッセージで FUI をサポートしています。FAA を受信すると、SMF は新しい FAR をインストールし、その FAR-ID を URR に関連付けます。同じパラメータを持つ FAR が存在する場合、SMF はその FAR ID を使用して URR を作成または更新します。UPF は、クォータを使い果たした後、FAR で設定された適切なアクションを開始します。

デフォルトでは、セッションを終了するために終了構成はアクティブ化されず、SMF は追加のクォータを要求せずに、最終的な使用済みサービスユニットのみを OCS に報告します。クォータが枯渇すると、OCS が再認証によって新しいクォータを割り当てるまで、UPF はそれ以降のトラフィックをドロップします。

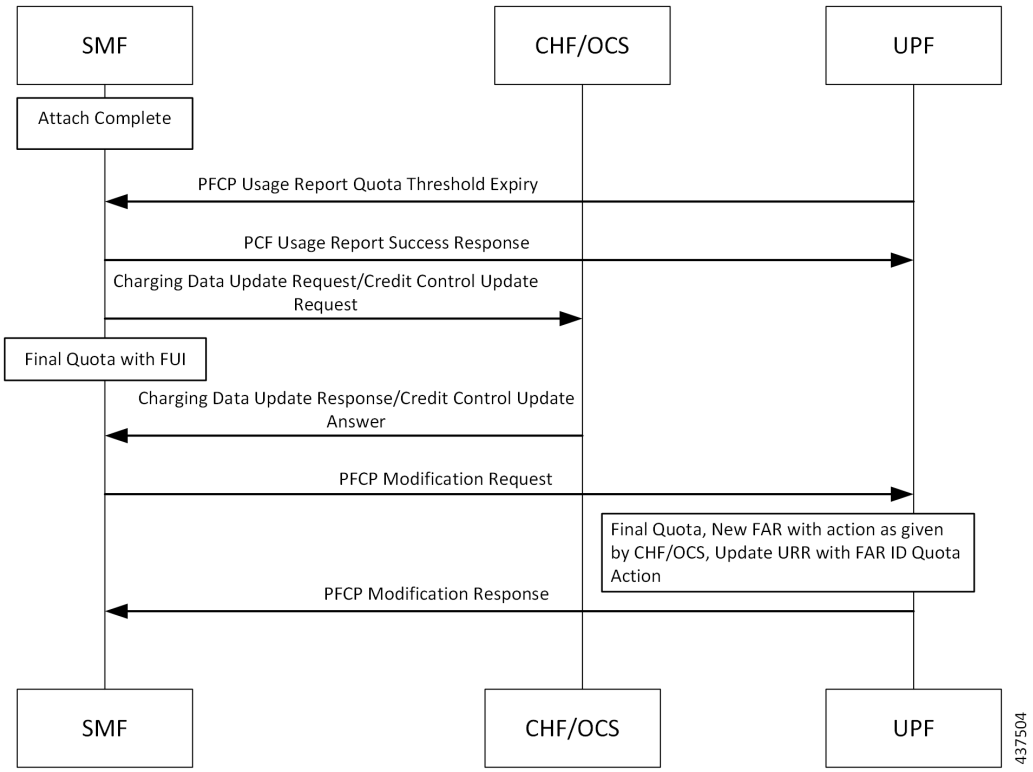
**Note** Gy では再認証がサポートされています。

MSCC レベルの FUI：MSCC レベルで FUI を受信し、セッションを終了するように FUI CLI が構成されている場合、クォータが使い果たされるか、使用可能なクォータがなければ、SMF はセッションを終了します。

コマンド レベルの FUI：FUI がコマンドレベルで受信された場合、SMF は、FUI CLI 構成に関係なく、クォータが使い果たされた後、または使用可能なクォータがなく FUI が受信された後にセッションを終了します。

現在、SMF は N40 の場合に[終了（Terminate）] アクションと [リダイレクト（Redirect）] FU アクションのみをサポートします。

***Figure 302: CHF からの課金データの初期応答または更新応答の FUI***




- いずれの場合も、CHF/OCS は FUI とともに SMF に付与ユニット（クォータ）を提供します。
- SMF は FUI を含む付与されたユニットを受信すると、SMF は N4 に対して FAR を作成し、クォータ情報を伝送する対応する URR にそれを関連付けます。
- UPF が URR に関連付けられた FAR を受信した後、クォータが使い果たされると、対応する FAR アクションが実装されます。

## Gy インターフェイスでの最終単位表示のサポート

表 *501* : 機能の履歴

| 機能名 | リリース情報 | 説明 |
|---|---|---|
| CCR-U での最終単位表示（FUI）のサポート | 2023.04 | Gy 使用状況レポートの一環として、SMF は OCS からの CCA-U の FUI をサポートします。FUI は、セッションの作成中または更新中に有効化またはアクティブ化されます。FUI のアクティブ化後、イベント トリガーまたは使用状況レポートによる更新トリガーが発生すると、SMF はそれ以上のクォータを要求せずに後続の CCR-U を OCS に送信し、CCA-U を受信します。 |

機能説明

SMF は、サーバーから与えられたクォータは最終的なクォータであること、そして AVP で指定された対応するアクションを行う必要があること示すためにオンライン課金システム（OCS）のクレジット制御応答：初期（CCA-I）/クレジット制御応答：更新（CCA-U）内の最終ユニット通知（FUI）をサポートします。

最終ユニットアクション（FUA）を受信すると、SMF は新しい転送アクションルール（FAR）をインストールし、その FAR-ID を使用状況レポートルール（URR）に関連付けます。同じパラメータを持つ FAR がすでに存在する場合、SMF は、URR の作成/更新でその FAR-ID を使用します。SMF は、クォータを使い果たした後、FAR で設定された適切なアクションをします。

最終ユニットアクションが終了する場合、SMF はアプリケーションアクション「ドロップ」を使用して新しい FAR をインストールし、その FAR-ID を URR に関連付けます。SMF は、セッションを終了するように設定されている場合は、プロトコル データユニット（PDU）を OCS に報告した後、追加のクォータを要求せずに、プロトコル データ ユニット（PDU）セッションを即時終了します。これは、セッションの終了が構成されている場合と他の MSCC の状態に関わらず、そのサービス/MSCC のクォータが消耗されている場合に行われます。

ボリューム/時間のしきい値または有効期間が原因で使用状況レポートを受信した場合、SMF は Gy-CCR-U を介してのみ使用状況レポートを報告し、追加のクォータを要求し続けます。

デフォルトでは、セッションを終了するために終了構成はアクティブ化されず、SMF は追加のクォータを要求せずに、最終的な使用済みサービスユニットのみを OCS に報告します。クォータが枯渇すると、OCS が再認証によって新しいクォータを割り当てるまで、SMF はそれ以降のトラフィックをドロップします。

FUI のアクティブ化後に OCS から追加のクォータを受信すると、以前の FUI が上書きされます。

（注） 現在、Gy インターフェイスを備えた SMF は Terminate FU アクションのみをサポートしています。

続行アクションを伴う FHT の場合、SMF は FUI URR のクォータ不足を受信した直後に PDU セッションを終了し、CLI がセッションを終了するように設定されている場合、またはコマンド レベル FUI を受信した場合には、Gy-CCRT を介して最終的な使用状況を OCS に報告します。SMF は、終了原因が「DIAMETER-ADMINISTRATIVE」、MSCC レポート理由が「FINAL」の Gy-CCRT を OCS に送信します。

時間クォータと有効時間の両方が受信され、時間クォータが有効時間を超えている場合、または時間クォータなしで有効時間のみを受信した場合、SMF は MSCC レポートの理由「VALIDITY-TIME」を含む Gy-CCRU を送信し、さらにクォータを要求します。

### FUI のレベル

FUI には、次の 2 つのレベルがあります：

- **MSCC レベルでの最終ユニット通知**：MSCC レベルで FUI が受信されている場合、FUI CLI はセッションの終了を構成している場合にのみ、SMF は、クォータが消耗した後にセッションを終了します。また、クォータがなく FUI を受信した場合、セッションを終了するように FUI CLI が構成されている場合に限り、SMF は即座にセッションを終了します。
- **コマンド レベルでの最終ユニット通知**：FUI がコマンド レベルで受信されている場合、SMF は、クォータが消耗した後、FUI CLI 構成とは無関係にセッションを終了します。また、クォータがなく FUI が受信された場合、SMF はセッションをただちに終了します。

### 提供内容の概要

FUI は、セッションの作成時または更新中に有効またはアクティブ化されます。FUI のアクティブ化後、イベント トリガーまたは使用状況レポートによる更新トリガーが発生すると、SMF はそれ以上のクォータを要求せずに後続の CCR-U を OCS に送信し、CCA-U を受信します。次のシナリオが起こる場合があります：

- **CCA-U はクォータありで FUI なしで受信**：SMF は FUI をリセットし、FAR の関連付けを解除して、更新 URR で新しいクォータを送信します。
- **CCA-U はクォータと FUI で受信**：SMF は更新 URR で新しいクォータを送信し、以前にドロップされた FAR を関連付け、更新なしで FUI を続行します。
- **CCA-U がクォータなしで FUI なしで受信する**：SMF は更新された URR を送信せず、更新なしで FUI を続行します。
- **CCA-U はクォータなしで FUI ありで受信します。**

  SMF によりセッションが即時終了されます。

  - FUI がコマンド レベルで受信され、クォータがない場合

- FUI が MSCC レベルで受信された場合、セッションを終了するように FUI CLI が構成され、クォータはありません。

- **CCA-U は、FHT アクションを Terminate として受信します**：SMF は、FHT によってすぐにセッションを終了します。
- **CCA-U は、FHT アクションを 続行とサブアクションをなし/不明として受信します**

  SMF は、FUI がコマンド レベルで受信されたか MSCC レベルで受信され たか、および **mscc-final-unit-action terminate session** CLI が構成されているかどうかに関係なく、最大クォータを FUI と非 FUI オンライン URR の両方に割り当てます。
- **CCA-U は MSCC レベル エラー を受信します**。SMF は失敗した MSCC をスキップし、更新せずに FUI を続行します。

## 制限事項

最終ユニット表示機能に関する既知の制限を次に示します。

- 現在、Gy インターフェイスを使用した SMF の FUI サポートでは、再認証はサポートされていません。
- リダイレクトは現在、Gy インターフェイスを使用した SMF の FUI サポートの一部としてはサポートされていません。

## 最終ユニット通知の構成

最終ユニット通知をアクティブにするには、次の構成例を使用します：

```
config
  profile charging profile_name
    mscc-final-unit-action terminate session
    end
```

注：

- **mscc-final-unit-action terminate session**：デフォルトでは、この構成は無効です。Final-Unit-Indication AVP に特定の MSCC に対するアクション TERMINATE が付属する場合、セッションは SMF によって終了されず、UPF はクォータの枯渇後に FAR に設定されたトラフィックに対して適切なアクションを実行する必要があります。特定の MSCC の FOA が TERMINATE に設定され、そのサービスのクォータが使い果たされると、他の MSCC の状態に関係なく、セッションがただちに終了します。

## 設定の確認

MSCC レベルで FUI のアクティブ化を確認するには、次の show コマンドを使用します：

```
product smf(config)# show running-config profile charging chp
product smf(config-charging-chp)#
mscc-final-unit-action terminate session
```

### *OAM* サポート

バルク統計サポート

SMF は、「**smf_disconnect_stats**」の一部として次の切断理由をサポートしています。

- **disk_fua_terminate**：最終ユニット表示の終端アクションによりセッションが終了します。

次の統計が **、SMF 課金最終ユニット表示統計カテゴリ**の一部として追加されました。

- **ocs_recived_fii_stats カウンタ**：OCS から受信した最終ユニット表示の総数。

### 課金情報レコードの照合

**重要** 請求レコードの調整はお客様固有の機能であり、SMF と CHF の両方にまたがる IE レベルのコンプライアンスが必要となります。

SMF と CHF の通信には、コンバージド CHF とオフライン CHF の両方が含まれます。すべての統合された CHF サーバが到達不能の場合、SMF は中断のない使用状況レポートのためにオフライン CHF にフォールバックします。その後、SMF はオフライン CHF に通信量を送信します。

オフライン CHF へのレポートには、オフライン サービスと変換されたオフライン サービスの使用済みユニット コンテナ（UUC）の差別化要因は含まれません。

SMF は、UUC に追加されたクォータ管理インジケータ（QMI）で新しい列挙値「CONVERTED_OFFLINE」をサポートします。SMF はこの列挙値を使用して、オフライン CHF に送信される変換済みのオフライン使用量レコードをマークします。

この機能により、オフライン CHF サーバは、通常のオフラインの使用記録と変換された使用記録を区別できます。

## 課金に関する静的ルールおよび事前定義済みルール

静的または事前定義されたルールの構成は、SMF および UPF の手順に似ています。設定のレイアウトは次のとおりです：

1. ルールベース：1 対多のルールベースを構成できます。単一の PDU セッションでは、1 つのルールベースをいつでもアクティブにできます。PCF は、PCC ルールでルールベース名を送信することにより、SMF でルールベースをアクティブ化できます。
2. Ruledef：各ルールベースは、1 対多の ruledef 構成を持つことができます。ruledef は、静的または事前定義済みのタイプのいずれかです。各 ruledef は課金アクションに割り当てられます。
3. 課金アクション：QoS と課金情報が含まれます。

SMF は、ルールベースの各課金アクションの課金データを取得します。ルールベースの静的ルールに関連付けられている課金アクションは、PDU コンテキストですぐに取得および更新さ

れます。事前定義されたルールに関連付けられている課金アクションは、PCF が SMF で特定の事前定義されたルールをアクティブにするときに取得され、更新されます。

課金アクションから派生した URR は、次の動作をします：

- オンライン課金は、課金アクションの「**cca charging credit**」構成によって識別されます。
- オフライン課金は、課金アクションの「**billing action egcdr**」構成によって識別されます。
- ボリューム制限と時間制限のアームトリガーは、APN の下の gtpp グループ設定の下にあります。UPF はこれらの値を自動的に検出し、それぞれの使用状況レポートを送信します。Gz は、課金プロファイルからのトリガーを使用します。
- 動的ケースとは異なり、SMF は構成されたルールから派生した課金データに対しては、Create URR をすぐに送信しません。
- オンライン課金方式を使用して、UPF は「開始」トリガーで使用状況レポートを送信します。SMF は CHF を使用して RG のクォータを取得し、Update URR メッセージで UPF に同じ情報をリレーします。Gz の場合 SMF は、ルールベースからベアラー レベル URR のしきい値を読み取り、課金プロファイルから SDF レベル URR のしきい値を読み取ります。
- ルールベース レベルで UPF しきい値を設定できます。ルールベース内のすべてのルール定義レベルの URR にリンクされたルールベース レベルの URR を作成します。

静的ルールの場合、SMF は実行時にアクティブな課金サービス設定を使用して、CHF にリレーされる QoS 記述子情報を取得します。

事前に定義されたルールでは、関連付けられた課金アクションにより、料金設定グループ（RG）、サービス ID、および帯域幅 ID の値を組み合わせたセッション データ内に QoS 記述子が作成されます。SMF は使用状況レポートを CHF にリレーするとき、RG およびサービス ID との一致を確認し、一致した課金アクションに適用可能な QoS を使用します。

**Important** 2 つの事前定義されたルールが同時にアクティブ化され、関連付けられた課金アクションが同じ RG とサービス ID を持つが、帯域幅 ID が異なる場合、SMF は RG とサービス ID との一致が見つかったかどうかを確認し、一致した課金アクションに適用可能な QoS を使用します。SMF は、さまざまな事前定義済みルールに関連付けられた課金アクションの 1 つから取得される QoS 記述子をランダムに選択します。

**Note** 前述の動作は、Gy にも適用できます。

## 課金の変更シナリオ

### PCF/PRCF 更新

変更シナリオでは、PCF は次のアクションを実行します。

- ダイナミック PCC ルールの追加
- 参照データの変更
- PCC ルールの削除
- 課金データのコンテンツ更新：測定方法を使用

### CHF/OCS 応答

交換中に、CHF応答は更新されたボリュームと時間のしきい値とクォータを送信します。SMFは更新された URR を N4 に向けてリレーします。

しきい値、トリガー、またはクォータの変更により、更新URRがトリガーされ、N4リレーが発生します。

SMF は、次のトリガーに基づいて更新 URR を送信します。

- ボリュームまたは時間のしきい値
- ボリュームまたは時間クォータ
- タリフ時間の変更
- クォータ保持時間など

### 即時 CC イベントの CDR 更新

QUERY_INTERFACE IE は、即時 CC イベントの CHF への CDR メッセージの送信をサポートしています。SMFでCCトリガーが発生し、トリガーがセッション レベルで監視される場合、SMFはUPFでオンラインURRとオフラインURRをクエリし、アカウンティングが有効になっている場合はRADIUS URR をクエリします。QUERY_INTERFACE IE により、SMF は UPF で使用可能な URR を検出できます。この IE は、N4 変更要求の送信時に QUARR フラグとともに構成されます。

QUARR フラグが構成されていない場合、UPF は QUERY_INTERFACE IE が構成されていても、すべての URR を報告しません。QUARR フラグが QUERY_INTERFACE IE で構成されている場合、クエリ URR は UPF にリレーされません。この機能は、課金プロファイル構成で **query-all-urr** CLI コマンドを使用して有効または無効にすることができます。デフォルトでは、構成は有効化されています。

QUERY_INTERFACE IE は、さまざまなインターフェイスのビットを持つ複合 IE です。

次のフラグが特定の URR にマップされます。

- [GZ_Offline]：インターフェイス 1 にマッピングされ、UPF はすべてのオフライン SDF URR を報告します。
- GY_Online：インターフェイス 7 にマッピングされ、UPF はすべてのオンライン SDF URR をレポートします。
- [Radius_URR]：インターフェイス 9 にマッピングされ、UPF は RADIUS URR を報告します。

- Bearer_URR：インターフェイス 2 にマッピングされ、UPF はすべての QBC URR を報告します。
- Sess_URR：インターフェイス 12 にマッピングされ、UPF はセッションレベルの URR を報告します。

（注） **query-all-urr** CLI は Gy または Gz には使用されません。

クエリ インターフェイスは、N40 の **query-all-urr** CLI に基づいて実行されます。ただし、クエリ インターフェイスは Gz の CLI 構成に関係なく実行され、クエリ インターフェイスは Gy には使用されません。

## URR のリンク

セッションレベルのボリュームまたは時間の値をローカルに構成したか、CHF からそれらを受け取った場合、SMF はセッションレベルの URR を作成し、それをオフラインの課金記述子に対応するすべての URR にリンクします。

PCF が同じ料金設定グループの複数の課金記述子を受信すると、SMF は追加の URR を作成し、同じ料金設定グループの課金記述子から派生したすべての URR にリンクします。

### URR 形式

次に、URR ID の形式を示します。

- URR ID は 32 ビットです。
- スタティック URR または事前定義済み URR の MSB（32 番目）ビットは 1 に構成され、ダイナミック URR の場合は 0 に構成されます。
- 最初の 4 つの LSB ビットは、インターフェイス タイプ用に構成されます。
  - オンラインの場合は 1
  - オンラインの場合は 7
- ビット 4 ～ 31 は URR ID 番号です。

  例：ID が 1 の場合の動的最初の URR：

  0x00 00 01 01 オフライン

  0x00 00 01 07 オンライン

  ID が 1 の場合の静的または事前定義済みの最初の URR：

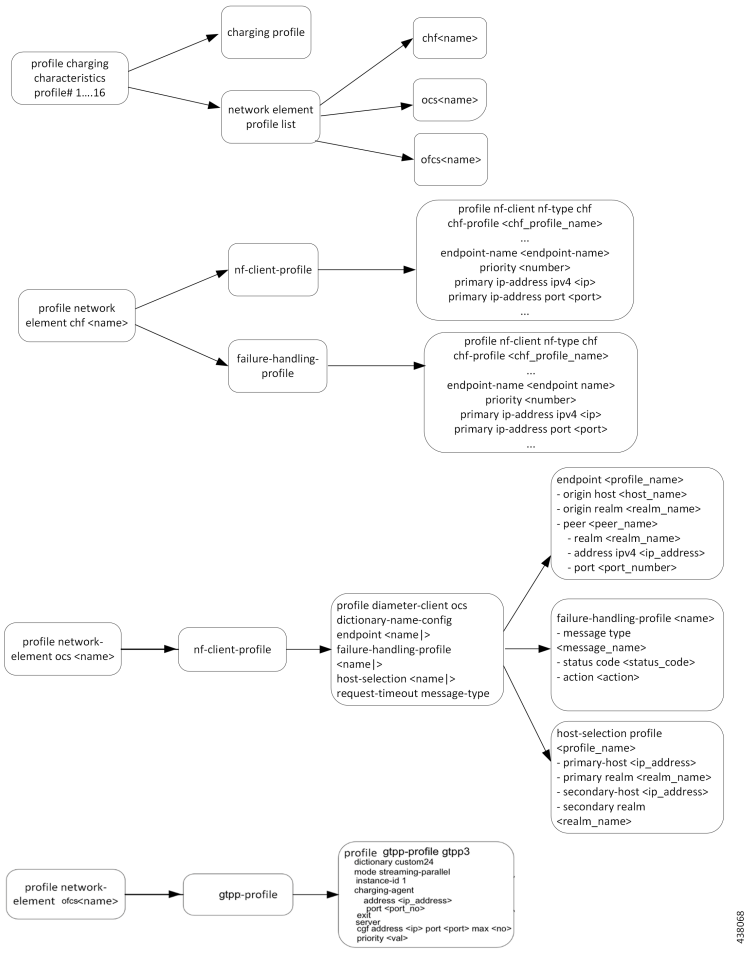
  0x80 00 01 01オフライン

  0x80 00 01 07 オンライン

# ローカル設定

次の図で、ローカル構成の動作について説明します：

***Figure 303:*** ローカル設定




- SMF は、最大 16 の充電特性プロファイルをサポートします。
- 各 CC プロファイルは、課金グループと課金プロファイルで構成されます。
- 課金サーバ グループと課金プロファイルは DNN プロファイルにリンクされています。現在、課金プロファイルはトリガーとしきい値の構成をサポートしています。

# ゼロ使用レポート抑制

SMF は、次の条件のいずれかが満たされた場合、オフライン リソース使用状況レポートを UPF から CHF にリレーします。

- レポート タイプは、immediate（即時）です。
- レポート タイプが遅延されており、遅延レポートの最大数を超えています。

使用状況レポートには、値がゼロの課金レコードも含まれます。これらのゼロ値レコード（UUC と CDR-U）は、CHF 上の不要なディスク領域を占有します。この問題を回避するために、SMF は新しい構成を利用して、ゼロ バイト データ カウントでオフラインの課金レコードを制御します。

課金プロファイル コンフィギュレーション モードで **offline zero-usage** CLI コマンドを構成すると、SMF は、UUC または CDR-U のオーバーロードを行うことなく、CHF に通信量をリレーします。

ユーザーは、CLI 構成に基づいて、抑制する UUC または CDR を選択できます。

**重要** **offline zero-usage drop cdr** コマンドが課金プロファイル コンフィギュレーション モードで構成されている場合でも、CDR リリースは抑制されません。

ゼロ抑制 CDR をサポートするには、Gz の **suppress-cdrs** CLI を有効にします。

構成についての詳細は、「課金プロファイルの構成（1880ページ）」セクションを参照してください。

## コール フロー

このセクションでは、次のコール フローについて説明します。

### PDU セッション確立

次の図に、PDU セッション確立のコール フローを示します。

*Figure 304: PDU* セッション確立コール フロー

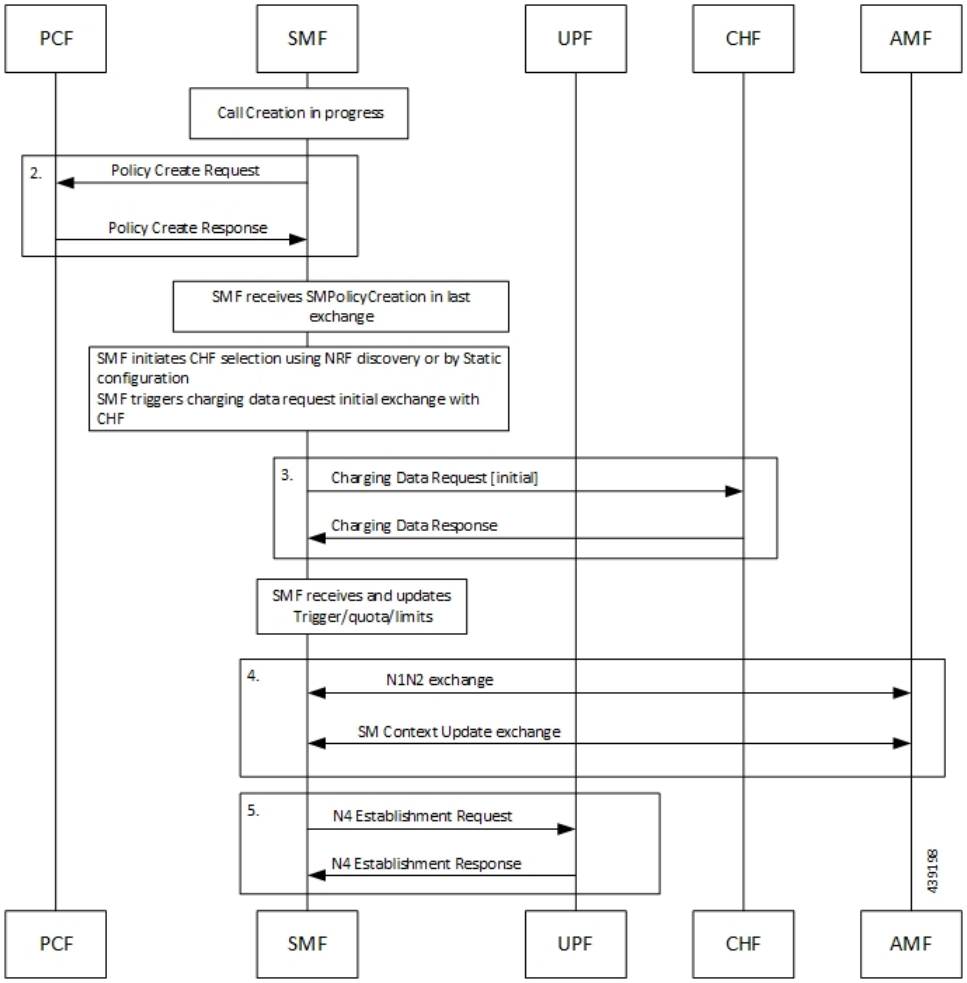



*Table 502: PDU* セッション確立コール フローの説明

| ステップ | 説明 |
|---|---|
| 1. | コールの作成は SMF で開始されます。 |
| 2. | SMF は PCF との Policy Create 交換を実行します。この交換で、SMF は PCC ルールに関連付けられている課金データを受信できます。この課金データは、進行中のセッションに対して課金が有効になっていることを示します。<br>PCF は、静的ルールまたは事前定義ルールを有効にすることができます。これらのルールは、構成に基づいて、課金で有効にすることもできます。 |

| ステップ | 説明 |
|---|---|
| 3. | 課金が SMF で検出された後、SMF は、CHF との課金データ要求の初期交換を開始します。この交換で、SMF は CHF から次の情報を受信できます。<br>• セッションまたは RG レベルで CC がトリガーする<br>• セッション レベルの時間またはボリュームの制限<br>• RG レベルでの時間またはボリュームの制限<br>• RG レベルのクォータ |
| 4. | SMF は、N1N2 交換と SM コンテキスト更新交換を AMF に送信します。 |
| 5. | SMF は、UPF との N4 セッション確立要求交換を開始します。同じ要求で、SMF は [URR 作成（Create URRs）] の課金に関する情報をリレーします。 |

## 制限事項

SMF 課金機能には、N4 インターフェイスに関する次の制限があります。

- セッション レベルの URR（CDR-I）が一度作成されると、セッション全体にわたってアクティブなままになります。この URR は、後続のセッション（CDR-U）で削除されません。
- セッションレベルの URR が作成されない場合、セッション制限が使用可能であっても、後続の CDR-U では作成されません。

# 標準準拠

この SMF 課金機能は、以下の基準に準拠しています：

- *3GPP TS 32.255*、バージョン *15.3.0*
- *3GP TS 32.290*
- *3GPP TS 32.299*、バージョン *12.9.0*
- *3GPP TS 32.298*、バージョン *12.9.0*

## 充電インターフェイスに関する 3GPP の 2019 年 6 月の適合規格

SMF は、2019 年 6 月の 3GPP 仕様 TS 32.290 バージョン 15.3.0 に準拠しています。

6 月リリースでは、メッセージは次の URI 形式に示されているようにバージョン「v2」を経由します。

```
nchf-convergedcharging/v2/chargingdata
```

コンプライアンス構成の CLI コマンド： **service nchf-convergedcharging**。この CLI コマンドまたは バージョンが構成されていない場合、3GPP のデフォルト バージョン（2018 年 12 月）が適用されます。

3GPP 2019 年 6 月準拠により、次の情報要素（IE）が追加されています。

- 認定 QoS
- 登録済み QoS
- QoSData の IE
- サービング ネットワーク機能 ID

# SMF 課金の構成

SMF 課金には、次の構成が含まれます。

- DNN プロファイルの構成, on page 1879
- 課金特性プロファイルの構成, on page 1879
- 課金プロファイルの構成

## DNN プロファイルの構成

次の構成を使用して、SMF 課金用の DNN プロファイルを構成します。

```
config
  profile dnn profile_name
    charging-profile profile_name
    network-element-profiles [ chf profile_name | ocs profile_name ]
    end
```

注：

- **charging-profile**：課金プロファイルの構成を指定します。
- **network-element-profiles**：ネットワーク要素プロファイルを指定します。ネットワーク要素プロファイルは、次のいずれかになります：

  **chf**：CHF ネットワーク要素プロファイルを指定します。

  **ocs**：OCS ネットワーク要素プロファイルを指定します。

- *profile_name*：選択したネットワーク要素プロファイルの名前を指定します。ネットワーク プロファイルを選択したら、文字列を入力します。

## 課金特性プロファイルの構成

以下の構成を使用して、SMF 課金の課金特性プロファイルを構成します。

```
config
  profile charging-characteristics cc_value
    charging-profile profile_name network-element-profile-list chf chf_name

     end
```

注：

- *cc_value*：課金特性値を指定します。値は、0x1 ～ 0xffff の範囲の 1 ～ 4 桁の 16 進文字列である必要があります。たとえば、11AB です。

## 課金特性 ID の構成

オフライン課金を有効にした場合、次の構成を使用して、課金プロファイルの選択に使用される課金特性 ID を構成します。

```
config
  profile dnn intershat charging-characteristics-id cc_id_value
     end
```

注：

- **profile dnn intershat charging-characteristics-id** *cc_id_value*：課金 ID 特性値を指定します。値は、0x1 ～ 0xffff の範囲の 1 ～ 4 桁の 16 進文字列である必要があります。たとえば、11AB です。

## 課金プロファイルの構成

SMF 課金用の課金プロファイル パラメータを構成するには、次の構成を使用します。

```
config
  profile charging profile_name
     limit [ rating-group ] { duration duration_value | volume volume_value
}
     max-charging-condition max_cc_value
     max-deferred-urr max_urr_value
     method { none | offline | online }
     offline zero-usage [ drop { cdr | uuc } | measurement { duration
| volume } | trigger { external | final | internal } ]
     query-all-urr { false | true }
     quota request [ always | standard ]
     quota suppress triggers [ qht ]
     reporting-level { offline | online { [rating-group]
     | rating-group | service-id }
     requested-service-unit time seconds volume downlink downlink_value
     uplink uplink_value total total_value
     tight-interworking-mode { false | true }
     triggers session session_level_triggers
     session-failover { false | true }
     send charging-initial  { session-start | traffic-start }
    dynamic-rules request-quota { on-receiving-rule | on-traffic-match
 }
```

```
     quota validity-time  validity_time
     quota volume-threshold percent  volume_threshold_percent
     usage-reporting quota-to-report based-on-grant {
report-only-granted-volume }
     mscc-final-unit-action terminate session
     max-secondary-rat-reports report_range
     egcdr losdv-max-containers container_num
    egcdr service-data-flow threshold { {volume | interval } { downlink
 | total | uplink }  bytes | {interval  <duration>}
     egcdr closure-reason { admin-disconnect | normal-release | }
     egcdr triggers {qos-change | uli-change | ms-timezone-change}
     egcdr suppress-cdrs zero-volume triggers { external-trigger-cdr
final-cdr  internal-trigger-cdr }
     egcdr-final-record closing-cause [ same-in-all-partials | unique
]
     end
```

注：

- **limit**：しきい値の制限を指定します。
- **duration**：課金の期間しきい値を指定します。しきい値の範囲は 0 ～ 2147483647 です。
- **volume**：課金のボリュームしきい値を指定します。しきい値の値の範囲は、0 ～ 9223372036854775807 です。
- **rating-group**：料金設定グループのボリュームと期間のしきい値を指定します。
- **max-charging-condition** *max_cc_value*：課金条件の変更の最大数を指定します。 *max_cc_value* は 0 ～ 500 の整数である必要があります。デフォルト値は 20 です。
- **max-deferred-urr** *max_urr_value*：遅延される USU コンテナの最大数を指定します。 *max_urr_value* は 、0 ～ 200 の整数である必要があります。デフォルト値は 50 です。
- **method**：課金方法を指定します。デフォルトの充電方法はオフラインです。
- **offline zero-usage { drop | measurement | trigger }** ：SMF は、ボリュームと期間がゼロのオフライン URR を抑止します。デフォルトでは、SMF のゼロ使用ドロップ構成は無効になっています。
  - **drop { cdr | uuc }**：SMF は、CDR または UUC をゼロの使用で抑止します。複数のレポートがある場合、SMF は使用状況がゼロのレポートのみをドロップします。オンライン レポートには影響がないことに注意してください。

    **drop** コマンドが構成されていない場合、SMF はオフライン使用状況レポートの UUC の送信を停止します。

  - **measurement { duration | volume }**：SMF は、抑制のネットワーク使用率の測定方法を指定します。測定方法は、ボリュームと期間に基づきます。

    **measurement** コマンドが構成されていない場合、SMF は、構成に応じて、ボリュームがゼロで期間がゼロのレコード、またはボリュームがゼロまたは期間がゼロのレコードを抑止します。

- **trigger { external | final | internal }**：抑制するトリーガのリストを指定します。
  - **external**：SMF は、QoS の変更、RAT の変更、ユーザーの場所の変更、PLMN の変更などの外部トリガーにより生成される使用状況レポートを抑止します。
  - **final**：SMF は、コンテキストの終了時に生成される使用状況レポートを抑制します。
  - **internal**：SMF は、ボリューム制限、時間制限、料金変更などの内部トリガーにより生成される使用レポートを抑制します。

- **query-all-urr { false | true }**：すべての URR をクエリする場合に を指定します。デフォルトでは、この構成は有効になっています（true に設定されています）。

  この CLI コマンドが無効になっている（false に設定されている）場合、または CC トリガーがセッション レベルでモニタされない場合、SMF は QUERY_URR を送信し、使用状況レポートとともに CC イベントを報告します。

- **quota request [ always | standard ]**：構成に基づき、オンライン課金サービスに対する CHF からのクォータ要求を制御します。 **quota request always** が構成定されている場合、SMF は常にクォータを要求します。 **no quota request** または **quota request standard** CLI コマンドが構成されている場合、SMF は、標準で定義されている特定のトリガータイプのクォータを要求します（これがデフォルトの動作です）。

- **quota suppress triggers [ qht ]**：使用状況レポート トリガー タイプ「qht」の構成時に、CHF からのクォータを抑制します。

- **reporting-level**：オフライン課金とオンライン課金に使用するレポート レベル構成を指定します。

  デフォルト値は [rating-group] レベルです。

- **requested-service-unit**：要求されたサービス ユニットの値を構成します。
  - **time** *seconds*：時間クォータ値を、1 ～ 4000000000 の秒単位で構成します。
  - **downlink** *downlink_value*：ダウンリンク ボリュームを 1 ～ 4000000000 のバイト単位で構成します。
  - **uplink** *uplink_value*：アップリンク ボリュームを 1 から 4000000000 までのバイト単位で構成します。
  - **total** *total_value*：合計ボリュームを 1 ～ 4000000000 のバイト単位で構成します。

- **tight-interworking-mode**：オンラインまたはオフラインの課金方式の厳格なインターワーキング モードを有効にする構成。

- **triggers**：構成するトリガのリストを指定します。

- **session** *session_level_triggers*：セッション レベルのトリガのリストを指定します。セッションレベルのトリガーのリストは次のとおりです：

- **repor3gpp-ps-change**
- **ambr-change**
- **max-number-of-changes-in-charging-conditions**
- **plmn-change**
- **qos-change**
- **rat-change**
- **serv-node-change**
- **tarrif-time-change**
- **ue-pra-change**
- **ue-time-change**
- **upf-add**
- **upf-rem**
- **user-loc-change**

- **session-failover { false | true }**：Gy の Diameter セッション フェールオーバーを有効にします。この構成のデフォルト値は、**false** です。
- **send charging-initial { session-start | traffic-start }**：ダイナミック ルールと事前定義済みルールを受信したときに、OCR-I メッセージを OCS に送信するかどうかを指定します。送信しない場合、CCR-I メッセージは、トラフィックの開始時に受信した使用状況レポートを送信します。デフォルト値は **session-start** です。
- **dynamic-rules request-quota { on-receiving-rule | on-traffic-match }**：ダイナミック ルールの受信時に RSU とともに CCR-I メッセージを送信するかどうかを指定します。送信しない場合、CCR-I メッセージは、トラフィックの開始時に受信した使用状況レポートを RSU とともに送信します。デフォルト値は **on-receiving-rule** です。
- **quota validity-time** *validity_time*：クォータの有効期間を 1 ～ 4000000 の秒数で指定します。
- **quota volume-threshold percent** *volume_threshold_percent*：ボリュームしきい値をボリュームクォータの割合（1 ～ 100）で指定します。
- **usage-reporting quota-to-report based-on-grant { report-only-granted-volume }**： **based-on-grant** オプションは、OCS サーバによって付与されたサービス ユニットでのみ付与される場合に、OCS に対する使用済みサービス ユニットのレポートの量または期間を指定します。**report-only-granted-volume** オプションは、OCS サーバによって付与された入力、出力、または合計オクテットに基づいて、使用済みボリューム クォータを OCS に送信するためのフィルタを指定します。
- **mscc-final-unit-action terminate session**：MSCC の最終ユニット アクションが終了するとセッションを終了します。

- **max-secondary-rat-reports** *report_range*：GTPP（Gz）更新をトリガするセカンダリ RAT 使用率レポートの最大数を構成します。 *report_range* は 0 ～ 50 の範囲内の整数である必要があります。max-secondary-rat-reports のセカンダリ RAT 使用制限の推奨値は 25 です。
- **egcdr losdv-max-containers** *container_num*：GTPP データ レコードを作成するサービス データ コンテナ（LOSDV）の最大リストを指定します。デフォルト値は 1 です。
- **egcdr service-data-flow threshold { {volume | interval } { downlink | total | uplink }** バイト**| {interval** <duration>：SDF レベルのオフライン URR しきい値を指定します。} ダウンリンク、合計、またはアップリンクのオクテット数の制限は、100000 ～ 4000000000 の範囲の整数である必要があります。
  - **egcdr service-data-flow threshold interval***duration*：オフライン充電のしきい値を構成します。しきい値間隔値は、60ー40000000の範囲の整数である必要があります。
- **egcdr closure-reason { admin-disconnect | normal-release | }**：終了理由を構成します。
- **egcdr triggers {qos-change | uli-change | ms-timezone-change}**：CDR のトリガーを有効にします。
- **egcdr suppress-cdrs zero-volume triggers { external-trigger-cdr final-cdr internal-trigger-cdr }**:
  - **egcdr suppress-cdrs zero-volume**：CDR を抑制します。
  - **triggers**：ボリュームがゼロの CDR を抑制するために使用できるトリガのリストの 1 つを構成します。
  - **egcdr suppress-cdrs zero-volume triggers internal-trigger-cdr**：非同期ボリューム使用レポートが PFCP セッションの使用レポートを介した UPF からのものであることを指定します。
  - **egcdr suppress-cdrs zero-volume triggers final-cdr internal-trigger-cdr**：通話が終了することを指定します。
  - **egcdr suppress-cdrs zero-volume triggers external-trigger-cdr**：同期ボリュームの使用状況レポートがクエリ URR を介して UPF から取得されるように指定します。
- **egcdr-final-record closing-cause [ same-in-all-partials | unique ]**
  - **egcdr-final-record**：最終 CDR を構成します。
  - **closing-cause [ same-in-all-partials | unique ]**：最後の CDR の場合の終了原因を構成します。 **same-in-all-partials** の値は、同じ終了原因が複数の最終 CDR に含まれることを指定します。 **unique** 値は、最終 CDR の終了原因が一意であることを指定します。

次に、SMF 課金の構成例を示します。

```
config
   profile dnn intershat1
   charging-profile chgprf1
   exit
   profile charging chgprf2
```

```
    limit volume 15000
    limit duration 90
    limit rating-group volume 12000
    limit rating-group duration 80
   triggers session [ ambr-change qos-change max-number-of-changes-in-charging-conditions
 ]
    max-charging-condition 1
    max-deferred-urr 3
    reporting-level online service-id
    reporting-level offline service-id
    session-failover   true
    quota validity-time 200
    quota volume-threshold percent 80
    dynamic-rules request-quota on-traffic-match
    send charging-initial traffic-start
    usage-reporting quotas-to-report based-on-grant
    mscc-final-unit-action terminate session
    max-secondary-rat-reports 25
    egcdr losdv-max-containers 2
    egcdr service-data-flow threshold volume downlink 100000
    cdr service-data-flow threshold interval 100
    egcdr closure-reason normal-release
    egcdr triggers ms-timezone-change
    egcdr suppress-cdrs zero-volume triggers
    egcdr-final-record closing-cause [ same-in-all-partials | unique ]

exit
```

# さまざまなインターフェイスでの課金シナリオのマッピング

## 機能説明

SMF の課金機能と動作は、N40、N7、および N4 インターフェイスの CHF、PCF、および UPF から受信したパラメータとメッセージの影響を受けます。SMF は、受信する課金データに基づいて、オンライン課金とオフライン課金のレポート レベルのサポートを提供します。

### 機能の仕組み

SMF は、次のルールに準拠したオンライン課金とオフライン課金の異なるレポート レベルを提供します。

- 構成されたルールは、スタティックまたは事前定義された課金アクションから派生します。
- セッションレベルの通信量レポートルール(URR)は、CHFトリガまたはローカル構成から導出されます。
- SMF は、オンラインおよびオフラインの課金説明のセッションレベルの URR を関連付けません。

- SMF では、セッションレベルの URR を構成済みの課金アクションの URR に関連付けません。
- ルールベースの URR は、オフラインで構成されている URR にのみ適用されます。
- 構成済みのオンラインまたはオフラインの課金方法で、[サービスID無視（Ignore Service ID）] 構成が存在する場合、URR リストには「rg x urr-id y」が含まれている必要があります。それ以外の場合、SMF は課金アクションを不正な形式としてドロップします。

**Important** SMF では、同じ料金設定グループ内の複数の課金方法がサポートされています。

## 充電マッピング

N7 インターフェイスは PCC ルールまたはローカル設定からの課金データを使用し、N4 インターフェイスは URR またはパケット検出ルール（PDR）を使用し、N40 インターフェイスは使用済みユニット コンテナ（UUC）を使用します。

さまざまな課金方式を持つ N7、N4、および N40 インターフェイスの SMF 課金マッピングを次に示します。

課金データが *1* つの *PCC* ルールから派生する場合のオフライン方式

レポート レベル：料金設定グループ レベルまたはサービス ID レベル

N4 インターフェイス：

- 最初の URR は最初の課金データから導出されます。料金設定グループ トリガまたはローカル構成によるデータ上限の請求。
- 2 番目の URR は CHF または、ローカル構成であるセッション制限から派生します。
- 2 番目の URR は最初の URR にリンクされています。
- 最初の PDR は最初の PCC ルールから導出されます。
- 最初の URR と 2 番目の URR は、最初の PDR にリンクされます。

N40 インターフェイス：

- 最初の UUC は、最初の URR の使用状況レポートから導出されます。
- 最初の UUC は、サービス識別子を持っている場合と、持っていない場合があります。

**Note**

- セッション レベルの URR は、構成済みの URR に関連付けられません。
- 構成されている場合、ルールベースの URR がセッション レベルの URR を置き換えます。
- 構成済みでルールベース URR が存在する場合は、最初の URR にリンクされます。

課金データが *1* つの *PCC* ルールから派生する場合のオンライン方式

レポート レベル: サービス IDレベルまたは料金設定グループ レベル

N4 インターフェイス：

- 最初の URR は、最初の課金データ、つまり料金設定グループの付与ユニットのしきい値またはクォータから導出されます。
- 2 番目の URR は CHF または、ローカル構成であるセッション制限から派生します。
- 2 番目の URR は最初の URR にリンクされています。
- 最初の PDR は最初の PCC ルールから導出されます。
- 最初の URR と 2 番目の URR は、最初の PDR にリンクされます。

N40 インターフェイス：

- 最初の UUC は、最初の URR の使用状況レポートから導出されます。
- 最初の UUC は、サービス識別子を持っている場合と、持っていない場合があります。

**Note**

- セッション レベルの URR は、構成済みの URR に関連付けられません。

課金データが *2* つの *PCC* ルールから派生する場合のオフライン方式

レポート レベル：サービス ID レベル

N4 インターフェイス：

- 最初の URR は最初の課金データから導出されます。課金データは制限がなく、評価トリガーは LIUSA である必要があります。
- 2 番目の URR は、課金データから派生します。課金データは制限がなく、評価トリガーは LIUSA である必要があります。
- 3 番目のURRは、料金設定グループ トリガーまたはローカル構成を制限する料金構成グループレベルから導出されます。
- 4 番目の URR は CHF または、ローカル構成であるセッション制限から派生します。
- 3 番目と 4 番目の URR は、 1 番目と 2 番目の URR にリンクされます。
- 最初の PDR は最初の PCC ルールから導出されます。
- 2 番目の PDR は 2 番目の PCC ルールから導出されます。
- 1 番目、3 番目と 4 番目の URRは、最初の PDR にリンクされています。
- 2 番目、3 番目と 4 番目の URRは、2 番目の PDR にリンクされています。

N40 インターフェイス：

- 最初の UUC は、最初の URR の使用状況レポートから導出されます。
- 2 番目の UUC は、2 番目の URR の使用状況レポートから導出されます。
- 1 番目と 2 番目の両方の UUC は、サービス識別子を持ちます。

**Note**

- セッションレベル URR は、構成済み URR に関連していません。
- 構成されている場合、ルールベースの URR は 1 番目と 2 番目の URR にリンクされます。

課金データが *2* つの *PCC* ルールから派生する場合のオンライン方式

レポート レベル：サービス ID レベル

N4 インターフェイス：

- 最初の URR は最初の課金データから導出されます。請求データに制限はなく、料金設定トリガーはリンクされた使用状況レポート（LIUSA）である必要があります。
- 2 番目の URR は、課金データから派生します。課金データは制限がなく、評価トリガーは LIUSA である必要があります。
- 3 番目の URR は、料金設定グループレベル、つまり料金設定グループの付与ユニットのしきい値またはクォータから導出されます。
- 4 番目の URR は CHF または、ローカル構成であるセッション制限から派生します。
- 3 番目と 4 番目の URR は、2 番目と 4 番目の URR にリンクされます。
- 一番目の PCC ルールから最初の PDR が派生します。
- 二番目の PCC ルールから二番目の PDR が派生します。
- 1 番目、3 番目と 4 番目の URRは、最初の PDR にリンクされています。
- 2 番目、3 番目と 4 番目の URRは、2 番目の PDR にリンクされています。

N40 インターフェイス：

- 最初の UUC は、最初の URR の使用状況レポートから導出されます。
- 2 番目の UUC は、2 番目の URR の使用状況レポートから導出されます。
- 1 番目と 2 番目の両方の UUC は、サービス識別子を持ちます。

**Note**

- セッションレベル URR は、構成済み URR に関連していません。
- [サービス ID を無視（Ignore Service ID）] が設定されている場合、この方法は無効です。

課金データが *1* つの *PCC* ルールから派生する場合のオフライン - オンライン方式

レポート レベル: サービス IDレベルまたは料金設定グループ レベル

N4 インターフェイス：

- オフラインURRは、最初の課金データから派生し、料金設定グループトリガーまたはローカル構成を制限します。
- オンライン URR は、付与されたユニットから制限される最初の課金データから派生します。
- 一番目の PCC ルールから最初の PDR が派生します。
- オフラインおよびオンラインの URR は、最初の PDR にリンクされます。

N40 インターフェイス：

- 最初の UUC は、オフライン URR の使用状況レポートから取得されます。
- 第 2 の UUC は、オンライン URR の使用状況レポートから取得されます。

課金データが *2* つの *PCC* ルールから取得される場合のオフライン - オンライン方式

レポート レベル：サービス ID レベル

N4 インターフェイス：

- 最初のオフライン URR は、最初の課金データから派生しました。課金データは制限がなく、評価トリガーは LIUSA である必要があります。課金データには、リンク済みの URR ID が URR_Off3 として含まれています。
  - 2 番目のオフライン URR は 2 番目の課金データから派生します。課金データは制限がなく、評価トリガーは LIUSA である必要があります。課金データには、リンク済みの URR ID が URR_Off3 として含まれています。
  - 3 番目のオフライン URR は、料金設定グループのトリガーまたはローカル設定を制限する料金設定グループレベルです。
  - 最初のオンライン URR は、最初の課金データから導出されます。課金データは制限がなく、評価トリガーは LIUSA である必要があります。課金データには、リンク済みの URR ID が URR_Online3 として含まれています。
  - 二番目のオンライン URR は、二番目の課金データから最初の課金データから派生します。課金データは制限がなく、評価トリガーは LIUSA である必要があります。課金データには、リンク済みの URR ID が URR_Online3 として含まれています。
  - 3 番目のオンライン URR は、付与されたユニットから制限する料金設定グループレベルです。
  - 一番目の PCC ルールから最初の PDR が派生します。
  - 二番目の PCC ルールから二番目の PDR が派生します。

- 最初のオフライン URR、最初のオンライン URR、3 番目のオフライン URR、および 3 番目のオンライン URR は、最初の PDR にリンクされます。
- 2 番目のオフライン URR、3 番目のオンライン URR、3 番目のオフライン URR、および 3 番目のオンライン URR は、2 番目の PDR にリンクされます。

N40 インターフェイス：

- 一番目の UUC は、最初のオフライン URR の使用レポートから派生し、サービス識別子を持ちます。
- 二番目の UUC は、二番目のオフライン URR の使用レポートから派生し、サービス識別子を持ちます。
- 3 番目の UUC は最初のオンライン URR の使用状況レポートから取得され、サービス識別子を持ちます。
- 4 番目の UUC は 2 番目のオンライン URR の使用状況レポートから取得され、サービス識別子を持ちます。

## 課金データがサービス *ID* のない *1* つの *PCC* ルールから派生する場合のオフライン - オンライン方式

オフラインおよびオンラインのレポート レベルは、それぞれサービス ID レベルと評価グループ レベルにあります。

前提条件：PCF からのレポート レベルがない

- CLI を使用して ROMmon ファイルを転送した場合の upgrade コマンドの例：
  - TAC インターワーキング モード
  - サービス識別子を無視
  - オフライン レポート: サービス識別子
  - オンライン レポート: 料金設定グループ

**Note**

- SMF は、料金設定グループレベルの CHF からのボリュームまたは時間制限のトリガを無視します。
- セッション レベルの URR は、最初の課金データから派生した URR に関連付けられません。

N4 インターフェイス：

- オフライン URR は、最初の課金データから派生します。課金データには制限がなく、料金設定トリガは LIUSA である必要があります。課金データには、リンク済みの URR ID が URR_Online としてあります。

- オンライン URR は、付与されたユニットから制限される最初の課金データから派生します。
- 一番目の PCC ルールから最初の PDR が派生します。
- オンライン URR とオフライン URR は、最初の PDR にリンクされています。

N40 インターフェイス：

- 最初の UUC はオフライン URR の使用状況レポートから取得され、サービス識別子を持ちます。
- 第 2 UUC はオンライン URR の使用状況レポートから取得され、サービス識別子はありません。

**Note**

- セッション レベルの URR は、構成済みの URR に関連付けられません。
- URR が構成されている場合、URR ルール ベースは eG-CDR から派生し、オフラインとオンラインの両方の URR にリンクされます。

### サービス *ID* のない *2* つの *PCC* ルールから課金データが派生する場合のオフライン - オンライン方式

オフラインおよびオンラインのレポート レベルは、それぞれサービス ID レベルと評価グループ レベルにあります。

前提条件：PCF からのレポート レベルがない

- CLI を使用して ROMmon ファイルを転送した場合の upgrade コマンドの例：
  - TAC インターワーキング モード
  - サービス識別子を無視
  - オフライン レポート: サービス識別子
  - オンライン レポート: 料金設定グループ

**Note**

- SMF は、料金設定グループレベルの CHF からのボリュームまたは時間制限のトリガを無視します。
- セッション レベルの URR は、最初の課金データから派生した URR に関連付けられません。

N4 インターフェイス：

- 最初のオフライン URR は、最初の課金データから派生しました。課金データには制限がなく、料金設定トリガは LIUSA である必要があります。課金データには、リンク済みの URR ID が URR_Online としてあります。
- 二番目のオンライン URR は、二番目の課金データから最初の課金データから派生します。課金データには制限がなく、料金設定トリガは LIUSA である必要があります。課金データには、リンク済みの URR ID が URR_Online としてあります。
- URR_Online は、付与されたユニットから制限される 2 番目の課金データから派生します。
- 一番目の PCC ルールから最初の PDR が派生します。
- 二番目の PCC ルールから二番目の PDR が派生します。
- 最初のオフライン URR と URR_Online は、最初の PDR にリンクされています。
- 2 番目のオフライン URR と URR_Online は、2 番目の PDR にリンクされています。

N40 インターフェイス：

- 一番目の UUC は、最初のオフライン URR の使用レポートから派生し、サービス識別子を持ちます。
- 二番目の UUC は、二番目のオフライン URR の使用レポートから派生し、サービス識別子を持ちます。
- 3 番目の UUC は、URR_Online の使用状況レポートから取得され、サービス識別子を持ちません。

**Note**

- セッションレベル URR は、構成済み URR に関連していません。
- URR が構成されている場合、URR ルールベースは egcdr から派生し、URR_Online とともに最初と 2 番目のオフライン URR の両方にリンクされます。

## 制限事項

この機能には、次の制限事項があります。

- 厳密なインターワーキング モードは、料金設定グループ レベルのサービスではサポートされません。
- 料金設定グループ レベルの 1 つのサービスとサービス ID レベルの別のサービスはサポートされていません。

## 標準準拠

オンライン課金とオフライン課金の異なるレポート レベルのサポート機能は、次の基準に準拠しています：

- 3GP TS 32.255
- 3GP TS 32.290

# 障害処理シナリオ

このセクションでは、SMF 課金中に発生するエラーに関連するさまざまな失敗処理シナリオについて説明します。

## アプリケーション エラーおよび結果コードの処理

SMF は、3GPP TS 32.291 仕様、バージョン 15.3.0、セクション 6.1.7.3 で定義されているように、コマンド レベルで CHF からのアプリケーション エラー コードをサポートします。SMF は、3GPP 32.291 仕様、バージョン 15.3.0 のセクション 6.1.6.3.14 で定義されている RG レベルの結果コードもサポートしています。

次のラベルは、アプリケーション レベルでの CHF 応答エラーを示すために「chf_appl_err_stats」カウンタで定義されています。

- http2_err_code：次の値が含まれます：
  - 403
  - 400
  - 404
- appl_err_code：次の値が含まれます：
  - END_USER_REQUEST_REJECTED
  - END_USER_SERVICE_DENIED
  - QUOTA_LIMIT_REACHED
  - CHARGING_NOT_APPLICABLE
- appl_err_action：次の値が含まれます：
  - drop_traffic
  - disable_charging
  - terminate
- appl_err_exchg_type：次の値が含まれます：
  - 初期
  - アップデート

# N40 アプリケーション エラー コード

次の表に、対応する SMF アクションを含むアプリケーション エラー コードの詳細を示します。

| アプリケーション エラー/セッション レベル | HTTP2 コード | SMF アクション | CHFの予期されるアクション | 制限事項 |
|---|---|---|---|---|
| CHARGING_FAILED | 400 | Terminate | なし | なし |
| RE_AUTHORIZATION_FAILED | 400 | なし | 是正措置の実施 | - |
| CHARGING_NOT_APPLICABLE | 403 | 課金なしで回線セッションを続行（オフライン課金もなし） | なし | なし |
| USER_UNKNOWN | 404 | Terminate | なし | なし |
| END_USER REQUEST_DENIED | 403 | Terminate | なし | なし |
| QUOTA_LIMIT_REACHED | 403 | オンラインサービスのトラフィックをドロップします。オフライン サービスは影響を受けません。 | セッションでこの状態が回復した後、CHF は通知（RAR）を送信します。 | |

（注）

- エラー コード 403 が失敗処理テンプレートで構成されていない。
- 静的ルールおよび事前定義ルールの CharGING_NOT_APPLICABLE（課金を無効にする）は、サブスクライバパラメータの独自の IE「課金無効」が N4 変更または確立要求で送信されたときに発生します。この要求は、UPF がアクティベーションを保留中の URR のトラフィック開始を生成しないようにするために送信されます。この IE は、2023.01.0 リリース以降では送信されなくなりました。詳細については、「課金の無効化機能の処理」セクションを参照してください。

# Gy アプリケーション エラー コード

Gy は、OCS サーバからの SMF によってサポートされる MSCC レベルとコマンドレベルのアプリケーションレベルのエラー コードをサポートします。

### MSCC レベルのエラー

次の表に、MSCC レベルの障害コードを示します。

表 *503 :* 一時的な障害（*4XXX*）

| 結果コード | 説明 |
|---|---|
| 4010 | DIAMETER_END_USER_SERVICE_DENIED |
| 4011 | DIAMETER_CREDIT_CONTROL_NOT_APPLICABLE |
| 4012 | DIAMETER_CREDIT_LIMIT_REACHED |

表 *504 :* 恒久的なエラー（*5XXX*）

| 結果コード | 説明 |
|---|---|
| 5003 | DIAMETER_AUTHORIZATION_REJECTED |
| 5012 | DIAMETER_UNABLE_TO_COMPLY |
| 5030 | DIAMETER_USER_UNKNOWN |
| 5031 | DIAMETER_RATING_FAILED |

表 *505 :* エラー コード

| ResultCode | Behaviour |
|---|---|
| 4010/4012(CCAI) | • CCAI は c4010/4012 とともに受信します。<br>• PFCP_SESSION_ESTABLISHMENT_REQUEST is sent with CREATE FAR with APPLY ACTION as DROP:1, CREATE URR is sent with REPORTING_TRIGGERS as "volqu, timqu" and VOLUME_QUOTA as 'volume_quota' : {'dlvol': 1, 'ulvol': 1, 'tovol': 1, 'total_vol': 0, 'up_vol': 0, 'down_vol': 0}, TIME_QUOTA as 'tm_quta' : 0 |
| 4010/4012(CCAU) | • CCAI は c4010/4012 とともに受信します。<br>• PFCP_SESSION_MODIFICATION_REQUEST is sent with UPDATE FAR with APPLY ACTION as DROP:1,UPDATE URR is sent with REPORTING_TRIGGERS as "volqu, timqu" and VOLUME_QUOTA as 'volume_quota' : {'dlvol': 1, 'ulvol': 1, 'tovol': 1, 'total_vol': 0, 'up_vol': 0, 'down_vol': 0}, TIME_QUOTA as 'tm_quta' : 0. |
| 4010/4012(CCRT) | • TMQ トリガを使用して使用状況レポートで受信した PFCP_SESSION_DELETION_REQUEST<br>• CCRT は、3GPP-Reporting-Reason が「FINAL」として送信されます。 |

| ResultCode | Behaviour |
|---|---|
| 4011(CCAI) | • CCAI が 4011で受信しました<br>• PFCP_SESSION_ESTABLISHMENT_REQUEST is sent with CREATE FAR APPLY ACTION as DROP:1, CREATE URR with REPORTING_TRIGGERS as "volqu, timqu" and VOLUME_QUOTA as 'volume_quota' : {'dlvol': 1, 'ulvol': 1, 'tovol': 1, 'total_vol': 9223372036854775807, 'up_vol': 9223372036854775807, 'down_vol': 9223372036854775807}, TIME_QUOTA as 'tm_quta' : 2147483647, TIME_THRESHOLD as 'time_treshold' : 10. |
| 4011(CCAU) | • CCAI が 4011で受信しました<br>• PFCP_SESSION_MODIFICATION_REQUEST is sent with UPDATE FAR APPLY ACTION as DROP:1, UPDATE URR with REPORTING_TRIGGERS as "volqu, timqu" and VOLUME_QUOTA as 'volume_quota' : {'dlvol': 1, 'ulvol': 1, 'tovol': 1, 'total_vol': 9223372036854775807, 'up_vol': 9223372036854775807, 'down_vol': 9223372036854775807}, TIME_QUOTA as 'tm_quta' : 2147483647, TIME_THRESHOLD as 'time_treshold' : 10. |
| 4011(CCRT) | • TMQ トリガを使用して使用状況レポートで受信した PFCP_SESSION_DELETION_REQUEST<br>• CCRT は MSCC なしで送信されます。 |
| 5003/5012/5030/5031<br>(CCAI) | • CCAI は 5003/5012/5030/5031 で受信します<br>• PFCP_SESSION_ESTABLISHMENT_REQUEST is ent with CREATE FAR with APPLY ACTION as DROP:1, CREATE URR with REPORTING_TRIGGERS as "volqu, timqu" and VOLUME_QUOTA as 'volume_quota' : {'dlvol': 1, 'ulvol': 1, 'tovol': 1, 'total_vol': 0, 'up_vol': 0, 'down_vol': 0}, TIME_QUOTA as 'tm_quta' : 0 |

| ResultCode | Behaviour |
|---|---|
| 5003/5012/5030/5031<br>(CCAU) | • CCAU は 5003/5012/5030/5031 で受信されます。<br>• PFCP_SESSION_MODIFICATION_REQUEST is sent with UPDATE FAR with APPLY ACTION as DROP:1, UPDATE URR with REPORTING_TRIGGERS as "volqu, timqu" and VOLUME_QUOTA as 'volume_quota' : {'dlvol': 1, 'ulvol': 1, 'tovol': 1, 'total_vol': 0, 'up_vol': 0, 'down_vol': 0}, TIME_QUOTA as 'tm_quta' : 0. |
| 5003/5012/5030/5031<br>(CCRT) | • TMQ トリガを使用して使用状況レポートで受信した PFCP_SESSION_DELETION_REQUEST<br>• CCRT は USU（時間（0）+ボリューム（0））および 3GPP-Reporting-Reason を「FINAL」として送信されます |

### コマンドレベルのエラー

Diameter エンドポイント ポッドは、OCS から Gy メッセージのコマンドレベルの障害を受信した後、障害処理構成を処理します。

Gy に適用されるアクションとサブアクションは次のとおりです。

- 続行（Continue）
  - FHSubActionEnum_UNKNOWN
  - FHSubActionEnum_DISCARD_TRAFFIC
- Terminate
  - FHSubActionEnum_WITH_TERM_REQUEST
  - FHSubActionEnum_WITHOUT_TERM_REQUEST

CCA-I、CCA-U、または CCA-T メッセージで受信した次の障害タイプに対して、先行するアクションおよびサブアクションを使用して障害処理プロファイルを構成できます。

- 任意
- Result-code

（注） 値の範囲は 3000 ～ 9999 です。

- Exp-result-code

（注） 値の範囲は 3000 ～ 9999 です。

- Local-error

## RG レベル結果コード

結果コードと対応する SMF アクションの詳細を次の表に示します。

| RG レベルの結果コード | HTTP ステータスコード | SMF 動作 | CHF 想定される動作 | 制限事項 |
|---|---|---|---|---|
| RATING_FAILED | 200 | 料金設定グループに一致するトラフィックをドロップする | なし | なし |
| QUOTA_MANAGEMENT_NOT_APPLICABLE | 200 | オフラインに変換 | なし | なし |
| USER_UNKNOWN | 200 | 無視（セッションレベルでのみサポート） | CHF からは予期していません | なし |
| END_USER SERVICE_DENIED | 200 | 料金設定グループに一致するトラフィックをドロップする | CHF は、料金設定グループのこの状態が回復した後、通知 (RAR) を送信します。 | オフラインサービスのトラフィックも、オンラインまたはオフラインのサービスでドロップされます。 |
| QUOTA_LIMIT_REACHED | 200 | 料金設定グループに一致するトラフィックをドロップする | セッションでこの状態が回復した後、CHF は通知（RAR）を送信します。 | なし |

| RG レベルの結果コード | HTTP ステータスコード | SMF 動作 | CHF 想定される動作 | 制限事項 |
|---|---|---|---|---|
| END_USER_SERVICE_REJECTED | 200 | 料金設定グループに一致するトラフィックをドロップする | セッションでこの状態が回復した後、CHF は通知（RAR）を送信します。 | なし |

## 課金無効化機能の処理

SMF は、N40 インターフェイスで課金トランザクションが無効になっている場合、次の機能を実行します。

- N4 ですでに作成されている使用レポート ルール（URR）を削除します。
- N4 の確立または変更要求を介して、サブスクライバ パラメータ属性で独自の IE「Charging Disabled」を送信します。

このカスタム N4 IE は、Radius アカウンティングなどの他の種類の課金に機能上の影響を及ぼします。

UPF で特定された課題を排除するために、SMF では課金プロセスを無効化する場合に、次の動作の変更が行われます。

- 新しくロードされたルールの場合、SMF は新しいダイナミック URR を構築しません。
- SMF が Charging Disabled IE の UPF への送信を停止します。UPF は、引き続き、使用状況レポート（USAR）を他の URR の SMF に送信します。
- その後、SMF は成功の応答メッセージで UPF を確認します。レポートで使用量のクォータが要求されている場合、SMF は N4 変更応答を通じて N40 の使用量の詳細を要求することなく、無限のクォータをリレーします。

# 課金サーバーの調整

NF 検出によって選択された NF に到達できない場合、SMF は最初に使用可能なオフライン CHF サーバーにフォールバックします。CHF 調整機能では、オフライン NF のセットに関連付けられている既存のサブスクライバ、およびオフライン フォールバック モードにあるサブスクライバを削除する必要があります。

（注） CHF の調整は、CHF エンドポイントが NF 検出サービスを介して NRF によって選択された場合にのみ適用されます。

CHF サーバーの調整は、次の 2 つの条件のいずれかが満たされたときに機能します：

1. オフライン CHF サーバーがアクティブであることを NRF が検出した場合。
2. オフライン変換セッションで CHF サーバーから RAR を受信した場合。

2 番目の条件の場合、セッションが直接削除されます。NF 検出では、この機能には次の手順が含まれます：

1. SMF は、Rest-EP の NF_LIB コンポーネントを介して NRF から NF インスタンス ID の通知をサブスクライブします。
2. NF 検出クエリですべての NF がダウンしていると判断された場合、NF_LIB コンポーネントはこれらの NF のセットをオフラインとして扱います。いずれかの NF が再度使用可能になると、NRF は SMF に対して同じ NF の通知をトリガーします。
3. SMF は再検証タイマーの後に NF ディスカバリを実行します。NRF が新しい NF を検出すると、SMF は NRF から対応する通知を受信します。
4. SMF は、必要なすべての NF ディスカバリ クエリ パラメータを使用して NF がオンラインであることを識別すると、CHF サーバーの調整を開始します。

この機能の一部として、次のラベルが導入されています：

- disk_pdurel_chf_reconciliation：このラベルは SMF_DISCONNECT_STATS の下で定義され、切断の理由を示します。
- chf_reconl_pdu_sess_rel：このラベルは、smf_service_stats メトリックの下で定義され、PDU セッションのリリース手順が開始された回数を示します。

# 課金構成のダイナミックな更新

## 機能説明

ダイナミック構成変更サポート機能により、SMF は構成エラーを最小限に抑えながら、課金パラメータの構成変更をダイナミックに処理できます。既存および新しい SMF 課金パラメータにより、ダイナミックな構成の更新を実装できます。この機能は、次の充電構成をサポートしています。

- アクティブ課金サービス（ACS）プロファイル
  - Rulebase
  - Ruledef

- Charging-Action
- Credit-Control-group

- 課金プロファイル
- 課金特性
- GTPP グループ
- UPF-APN 構成グループ

# 機能の仕組み

このセクションでは、サポートされている [障害処理プロファイル（Failure Handling Profile）] と [課金プロファイル（Charging Profile）] の構成に対するダイナミックな構成変更の仕組みについて説明します。

## ACS プロファイル

SMF では、実行時の ACS 構成の動的な変更がサポートされています。ACS プロファイル構成は、ACS プロファイルの様々なパラメータを定義します。

次の表に、さまざまなシナリオでの ACS 構成の動的な更新中の SMF および UPF の動作の変更を示します。

**表 *506 : ACS* プロファイルの構成と動的更新中の影響**

| 設定（Configuration） | SMF と UPF の両方に適用される構成 | SMF でのみ適用される構成 | 構成は UPF にのみ適用されます |
|---|---|---|---|
| ルールベースの追加 | **[既存のセッション（Existing Session）]**: 現在のルールベース値を引き続き使用します<br>**[新しいセッション（New Session）]**：新しいセッションの影響はありません。 | **[既存のセッション（Existing Session）]**：ルールベースの変更が UPF で拒否される<br>**[新しいセッション（New Session）]**：このルールベースの UPF でセッションの作成が失敗します | **[既存のセッション（Existing Session）]**：ルールベースの変更が SMF で拒否される<br>**[新しいセッション（New Session）]**：このルールベースの SMF でのセッション作成に失敗しました |

| | | | |
|---|---|---|---|
| ルールベースの削除 | **[既存のセッション（Existing Session）]**：ノードドレインなしでは許可されません<br>**[新しいセッション（New Session）]**：新しいセッションの影響はありません。 | **[既存のセッション（Existing Session）]**：ノードドレインなしでは許可されません<br>構成の変更後、UPF でのルールベースの削除を見逃した場合、ルールベースの構成は SMF で古いままです<br>**[新しいセッション（New Session）]**：新しいセッションの影響はありません。 | **[既存のセッション（Existing Session）]**：ノードドレインなしでは許可されません<br>構成の変更後、SMF でのルールベースの削除を見逃した場合、ルールベースの構成は UPF 上で古いままです<br>**[新しいセッション（New Session）]**：新しいセッションの影響はありません。 |
| Ruledef の追加 | **[既存のセッション（Existing Session）]**: 新しいルールが正常にアクティブ化されます<br>**[新しいセッション（New Session）]**：新しいセッションの影響はありません | **[既存のセッション - 静的ルール（Existing Session - Static Rule）]**：UPF はルールをアクティブ化しず、このルールのレポートを送信しません。<br>**[既存のセッション - 事前定義済みのルール（Existing Session - Predefined Rule）]**：UPF が新しいルールを受信するまで、新しいルールのアクティブ化に失敗します。<br>**[新しいセッション（New Session）]**：既存のセッションと同じです | **[既存のセッション - 静的ルール（Existing Session - Static Rule）]**：UPF はこのルールをアクティブにし、使用状況をレポートします。SMF には、この RG + ServID の課金データがあります。ダミーの ChargParam を作成し、それに URR を関連付けます。<br>**[既存のセッション - 事前定義済みのルール（Existing Session - Predefined Rule）]**：SMF が新しいルールを受信するまで、新しいルールのアクティブ化に失敗します。<br>**[新しいセッション（New Session）]**：既存のセッションと同じ |

| | | | |
|---|---|---|---|
| ルール定義の削除 | **[既存のセッション（Existing Session）]**：現在のフローはそのまま残ります。フローが作成されない場合、このセッションに対して作成されることはありません。SMF または UPF は、関連付けられた課金を削除しません。<br>**[新しいセッション（New Session）]**：新しいセッションの影響はありません | **[既存のセッション - 事前定義されたルール（Existing Session - Predefined rule）]**：SMF はこのルールの作成を拒否します。<br>**静的およびアクティブ化された事前定義ルール**：既存のフローはそのまま残ります。SMF または UPF は、関連付けられた課金を削除しません。受信した使用状況が正常にレポートされます。<br>SMF が最初の使用状況レポートを受信せず、最初のレポートが到着した場合、SMF は RG + ServID から chargParam/Urr コンテキストを作成します。<br>**[新しいセッション（New Session）]**：既存のセッションと同じです | **[既存のセッション - 事前定義されたルール（Existing Session - Predefined rule）]**：SMF は引き続きこのルールの作成を許可しますが、UPF で失敗します。<br>**静的およびアクティブ化された事前定義ルール**：UPF は、これらのフローに対して作成された URR で続行されます。SMF は問題なく使用状況を報告します。<br>**[新しいセッション（New Session）]**：既存のセッションと同じです |

| | | | |
|---|---|---|---|
| 新しい RG/Svc IDによる課金アクションの追加（その CA に関連付けられた新しいルールの追加） | **[既存のセッション - 静的ルール（Existing Session - Static Rule）]**：SMF は、最初の URR が受信されると、この RG の課金エントリを作成します。<br><br>**[既存のセッション - 事前定義されたルール（Existing Session - Predefined Rule）]**：SMF は PCF トリガーに基づいてルールをアクティブ化します。<br><br>**[新しいセッション（New Session）]**：新しいセッションの影響はありません。 | **[既存のセッション - 静的ルール（Existing Session - Static Rule）]**: UPFはこのフローをアクティブにしません。SMFは通信量を受信しません。<br><br>**[既存のセッション - 事前定義されたルール（Existing Session - Predefined Rule）]**：ruledef情報を使用できないため、UPFは事前定義されたルールのインストールに失敗します。<br><br>**[新しいセッション（New Session）]**：既存のセッションと同じ | **[既存のセッション - 静的ルール（Existing Session - Static Rule）]**：UPF はこのフローをアクティブにします。SMF は、最初の URR を受信すると、この RG の課金エントリを作成します。<br><br>この場合、SMF はこの RG + ServID を持つ Charging-action を検出しません。受信した RG + ServID でダミーの ChargParam を作成します。<br><br>**[既存のセッション - 事前定義されたルール（Existing Session - Predefined Rule）]**：静的ルールについて説明されているのと同じです。<br><br>**[新しいセッション（New Session）]**：既存のセッションと同じ |

| | | | |
|---|---|---|---|
| 請求アクション（および関連するルール）の削除 | **[既存のセッション - 静的ルール（Existing Session - Static Rules）]**：SMF および UPF は現在のフローを続行し、この RG の URR を報告します。<br>**[定義済みルール（Predefined Rules）]**：<br>SMF および UPF は現在のフローを続行し、この RG の URR を報告します。ルールが非アクティブ化されると、再度アクティブ化されることはありません。<br>**[新しいセッション（New Session）]**：新しいセッションの影響はありません。 | **[既存のセッション - 静的ルール（Existing Session - Static Rules）]**：SMF および UPF は現在のフローを続行し、この RG の URR を報告します。<br>**[定義済みルール（Predefined Rules）]**：<br>SMF および UPF は現在のフローを続行し、この RG の URR を報告します。ルールが非アクティブ化されると、再度アクティブ化されることはありません。<br>**[新しいセッション（New Session）]**：既存のセッションと同じ | **[既存のセッション - 静的ルール（Existing Session - Static Rules）]**：SMF および UPF は現在のフローを続行し、この RG の URR を報告します。<br>**[定義済みルール（Predefined Rules）]**：<br>SMF および UPF は現在のフローを続行し、この RG の URR を報告します。ルールが非アクティブ化されると、再度アクティブ化されることはありません。<br>**[新しいセッション（New Session）]**：既存のセッションと同じ |

| | | | |
|---|---|---|---|
| RG/Svc Id、CA 内でオンライン/オフライン構成が変更されました | **[静的ルールとすでにアクティブな事前定義済みルール（Static Rules and Already Active Predefined Rules）]**：UPF は新しい URR を作成し、それらを報告します。SMF は URR ID テーブルから調整し、レポートされた時点でこれらの URR の課金データを作成します。<br>**[事前定義されたルールの設定変更のアクティブ化後（Post config change activation of predefined rules）]**：問題はありません。SMF と UPF の両方が同期しています。<br>**[新しいセッション（New Session）]**：新しいセッションの影響はありません。 | **[スタティックルールとすでにアクティブな事前定義済みルール（Static Rules and Already Active Predefined Rules）]**：UPF は古い URR ID でレポートを継続し、SMF は問題なくレポートし続けます。<br>**[事前定義されたルールの構成変更のアクティブ化後（Post config change activation of predefined rules）]**：静的ルールと同じ<br>**[新規セッション（New Session）]**：事前定義されたルールがセッションの確立中にアクティブ化されると、UPF は確立要求を拒否します。 | **[静的ルールとすでにアクティブな事前定義済みルール（Static Rules and Already Active Predefined Rules）]**：UPF は新しい URR を作成し、それらを報告します。SMF は URR ID テーブルと照合し、ダミーの chargParam を作成して、URR を関連付けます。<br>**[事前定義されたルールの構成変更のアクティブ化後（Post config change activation of predefined rules）]**：静的ルールと同じ<br>**[新規セッション（New Session）]**：事前定義されたルールがセッションの確立中にアクティブ化されると、UPF は確立要求を拒否します。 |
| URR Id テーブルエントリの追加<br>（新しい RG の追加） | SMF の対処は不要です。 | SMF の対処は不要です。 | UPF は URR を作成します。 |
| URR Id テーブルエントリの削除 | 影響なし | 影響なし | UPF は URR を作成します。削除しても、作成された URR には影響しません。 |

| | | | |
|---|---|---|---|
| URR Id テーブルエントリの変更 | 影響なし | 影響なし | UPF は URR を作成します。削除しても、作成された URR には影響しません。<br>同じ URR-ID が異なる RG + ServID に割り当てられている場合、削除は URR に影響します。UPF が新しい RG + ServId の新しい URR を作成できませんでした。 |

**注**：

- オンライン レポートにサービス ID が含まれ、無視サービス ID がクレジット制御プロファイルで構成されていない場合、SMF はレポートをドロップします。
- 新しいオンライン URR に既存の URR と同じ RG が含まれている場合、SMF は使用状況レポートをドロップします。
- 新しいオフライン URR に既存の URR と同じ RG とサービス ID が含まれている場合、SMF は使用状況レポートをドロップします。
- 同じ使用状況レポートで、次のオンライン URR に同じ RG が含まれ、次のオフライン URR に同じ RG + サービス ID が含まれている場合、SMF は使用状況レポートを削除します。

## 課金プロファイル

課金プロファイルは、実行時に渡す値に基づく構成の動的な更新をサポートします。値の更新操作は、次のシナリオを考慮して行われます：

- **構成は、次のアクセス時に反映されます**： 操作の進行中に値が更新された場合、SMF は新しい値を無視して古い値を引き続き使用します。たとえば、[Charg-Profileの制限（Limits in Charg-Profile）] および [CC トリガー（CC triggers）]。
- **[設定が新しいセッションにのみ反映される（ConfigurationConfiguration only on a new session）]**： 構成がセッションに固有のものであり、そのセッションですでに値が考慮されている場合、SMF は新しい値を考慮しません。たとえば、PduContext（DB エントリ）。この場合は、設定を更新しても、すでに作成されているセッションには影響しないことを意味します。たとえば、[課金方法（Charging Method）] は [プロファイル（Profile）] で、[課金特性（Charging Characteristics）] の [課金プロファイル（Charg-Profile）] に変更できます。
- **設定が即座に反映**： 構成は、更新されるとすぐに動的な値を考慮します。SMF がすでに構成を使用していて、後で更新された場合は、最新の値が使用されます。

課金プロファイルを使用してセッションが作成され、のちに Ops センターから削除される場合、セッションは削除されたプロファイルの構成構造へのアクセスを試みる場合があります。

このような場合、Smf-Serviceポッドは、プロファイルが存在しないセッションにマッピングされたデフォルト プロファイルを維持します。

課金プロファイルは、SMF 課金パラメータの処理を担当します。

次の表に、動的な構成変更を含む構成パラメータと、既存のセッションへのその影響を示します。

***Table 507:*** 課金プロファイルのパラメータ

| 設定パラメータ | ダイナミックな変更 | 既存のセッションへの影響 |
|---|---|---|
| レーティンググループの期間の制限 | 許可 | 新しい値は、既存のセッションの新しい URR の作成または、以降の URR アップデート時に使用されます。<br>**Note**<br>動的な設定では、URRの更新は開始されません。 |
| max-charging-condition | 許可 | 影響なし |
| max-deferred-urr | 許可 | 影響なし |
| metering-method | 許可 | 新しい値は、既存のセッションの新しい URR の作成時に使用されます |
| method | 許可 | 影響なし |
| reporting-level | 許可 | 影響なし |
| requested-service-unit time | 許可 | 影響なし |
| tight-interworking-mode | 許可 | 影響なし |
| セッションのトリガー | 許可 | 影響なし |
| 要求クォータ | 許可 | 影響なし |
| session-failover | 許可 | 影響なし |
| dynamic-rules | 許可 | 影響なし |
| send charging-initial | 許可 | 影響なし |
| quota Validity-Time | 許可 | 影響なし |
| quota volume-threshold | 許可 | 影響なし |
| usage-reporting | 許可 | 影響なし |
| mscc-final-unit-action | 許可 | 影響なし |

| 設定パラメータ | ダイナミックな変更 | 既存のセッションへの影響 |
|---|---|---|
| max-secondary-rat-reports | 許可 | 影響 |
| egcdr losdv-max-containers | 許可 | 影響 |
| egcdr service-data-flow | 許可 | 影響なし |
| egcdr closure-reason | 許可 | 影響 |
| egcdr triggers | 許可 | 影響 |
| egcdr suppress-cdrs zero-volume | 許可 | 影響 |
| egcdr-final-record | 許可 | 影響 |

## 課金特性プロファイル

[課金特性プロファイル（Charging-Characteristics Profile）] 設定では、SMF 課金の課金特性を管理するためのさまざまなパラメータを定義します。

次の表に、構成パラメータで構成をダイナミックに変更できるかどうかを示します。

***Table 508:*** 課金特性プロファイル

| 設定パラメータ | ダイナミックな変更 | 既存のセッションへの影響 |
|---|---|---|
| 課金プロファイル | 不可 | 構成は、セッションの設定時に1回だけ使用されます。 |

## 課金アクション プロファイル

[課金アクション プロファイル（Charging-Action Profile）] 設定は、ルール定義に関連付けられた QoS および課金関連パラメータを定義します。

次の表に、構成パラメータで構成をダイナミックに変更できるかどうかを示します。

***Table 509:*** 課金アクション プロファイル パラメータ

| 設定パラメータ | ダイナミックな変更 | 既存のセッションへの影響 |
|---|---|---|
| 料金設定グループとサービス ID | 許可 | 影響なし |

## クレジット制御グループ プロファイル

credit-Control-Group の構成は、マップされたルールベースを使用するサブスクライバに使用されるパラメータを定義します。

次の表に、構成パラメータで構成をダイナミックに変更できるかどうかを示します。

***Table 510:*** クレジット制御グループ プロファイルのパラメータ

| 設定パラメータ | ダイナミックな変更 | 既存のセッションへの影響 |
|---|---|---|
| サービス ID を無視する | 許可 | 影響なし |

## ルールベースのプロファイル

Rulebaseの構成パラメータでは、フローを照合するプロトコルルールと、フローを照合するための関連アクションを定義します。

次の表に、構成パラメータで構成を動的に変更できるかどうかを示します。

***Table 511:*** ルールベースのプロファイル パラメータ

| 設定パラメータ | ダイナミックな変更 | 既存のセッションへの影響 |
|---|---|---|
| Charging-action への Ruledef の関連付け | 許可 | 影響なし |
| クレジット制御グループ | 許可 | 構成は、セッションの設定時に1回だけ使用されます |

## GTPP グループ プロファイル

GTPP グループ プロファイルの構成では、GTPP グループを作成するためのパラメータを指定します。

次の表に、構成パラメータで構成をダイナミックに変更できるかどうかを示します。

***Table 512: GTPP*** グループ プロファイル パラメータ

| 設定パラメータ | ダイナミックな変更 | 既存のセッションへの影響 |
|---|---|---|
| オフラインで構成されている URR の制限 | 許可 | 新しい値は、既存のセッションの新しい URR の作成時に使用されます。 |

## UPF-APN 構成プロファイル

[UPF-APN 構成プロファイル（UPF-APN Configuration Profile）] の構成では、UPF-APN プロファイルのさまざまなパラメータを定義します。

次の表に、構成パラメータで構成をダイナミックに変更できるかどうかを示します。

*Table 513: UPF-APN* 構成プロファイル パラメータ

| 設定パラメータ | ダイナミックな変更 | 既存のセッションへの影響 |
|---|---|---|
| GTPP グループの関連付け | 許可 | 構成は、セッションの設定時に1回だけ使用されます。 |

## ピア CHF のネットワーク プロファイル

ピア CHF 構成のネットワーク プロファイルは、さまざまなネットワーク構成を定義します。

次の表に、構成パラメータで構成をダイナミックに変更できるかどうかを示します。

*Table 514:* ピア *CHF* パラメータのネットワーク プロファイル

| 設定パラメータ | ダイナミックな変更 | 既存のセッションへの影響 |
|---|---|---|
| 構成された CHF のセット | 許可 | 影響なし |

## ピア OCS のネットワーク プロファイル

ピア OCS 構成のネットワーク プロファイルは、Gy インターフェイスを有効にします。

次の表に、構成パラメータでダイナミックな構成変更が可能かどうかを示します。

表 *515 :* ピア *OCS* パラメータのネットワーク プロファイル

| 設定パラメータ | ダイナミックな変更 | 既存のセッションへの影響 |
|---|---|---|
| 構成済みの一連の OCS サーバ | 許可 | 影響なし |

## ピア OFCS のネットワークプロファイル

ピア OCS 構成のネットワーク プロファイルは、Gy インターフェイスを有効にします。

次の表に、構成パラメータでダイナミックな構成変更が可能かどうかを示します。

表 *516 :* ピア *OFCS* パラメータのネットワーク プロファイル

| 設定パラメータ | ダイナミックな変更 | 既存のセッションへの影響 |
|---|---|---|
| 構成済みの OFCS サーバのセット | 許可 | 影響なし |

# 静的ルールおよび事前定義済みルールを使用したプリエンプティブ クォータの取得

表 *517 :* 機能の履歴

| 機能名 | リリース情報 | 説明 |
|---|---|---|
| 静的ルールおよび事前定義済みルールに対するプリエンプティブ クォータ要求 | 2024.02.0 | SMF では、プリエンプティブ クォータはダイナミック ルールに対してデフォルトで有効になっています。<br>この機能強化により、SMFは、最初の接続セッション作成プロセス中に、静的ルールと事前定義済みルールのプリエンプティブ クォータを要求できます。<br>プリエンプティブ クォータは、**preemptively-request-n-validate** コマンドを **Charging Action Configuration** モードで使用して構成できます。<br>**[デフォルト設定（Default Setting）]**：有効 – 常時オン |

## 機能説明

SMFは、オンライン課金システム（OCS）/Gyインターフェイスを使用して課金イベントを生成します。OCS は、Diameter クレジット制御サーバーとして機能します。これは、SMF にオンライン充電データを提供します。Gyインターフェイスでお客様トラフィックは、ゲートウェイに送りオンラインまたは前払いの方式で課金できます。SMFは時間ベースと使用量ベースの課金モデルをサポートします。

SMFでは、各PDUセッションの料金設定グループ（RG）ごとにクォータ管理が可能です。静的ルールおよび事前定義済みルールの場合、以前は、データ パケットがフローを開始し、「STARTOF TRAFFIC」通知が UPF から SMF に送信される場合にのみ、SMF が課金機能（CHF）からのクォータ フェッチを要求していました。

SMF は、 **preemptively-request-n-validate** CLI 構成を介して最初の接続セッションの作成プロセス中に、静的ルールと事前定義済みルールのプリエンプティブ クォータを要求できるようになりました。プリエンプティブ クォータ リクエストは、N11、N16、S5、S8、またはS2bの作成手順中にアタッチされ、送信されます。クォータ リクエストの CHF からエラーを受け取った場合、PDU のセットアップまたは接続は拒否されます。

拒否時に、SMF は次のシナリオで適切な通知を送信します。

- クォータが受信されない場合、SMFは「リソースなし」という理由でセッションの作成を拒否します。
- セッション作成がホームの NR RAT を介したものである場合、SMF は、N1 PDU 確立拒否を含む N11 N1N2 転送メッセージを送信します。原因は「リソース不足」であり、その後に原因が「REL_DUE_TO_UNSPECIFIED_REASON」である N11 ステータス通知が続きます。
- セッションの作成がローマの NR RAT を介して行われる場合、SMF は N16 PduSessionCreateError を N1 の原因 = "Insufficient resources" で送信します。
- セッション作成が EUTRA/WIFI 経由で行われる場合、SMF は「No resources available」という理由のセッション作成応答を送信します。

アクティブセッションに対して定義済みのルールまたはルールベースがランタイムで変更または追加されても、プリエンプティブ クォータは生成されません。クォータ要求は、UPF からトラフィック開始を受信した場合にのみ送信されます。

# 機能の仕組み

プリエンプティブ クォータは、接続手順または PDU 設定の検証にのみ使用されます。課金アクションが **cca charge credit preemptively-request-n-validate traffic-start-trigger** *trigger_type_name* で構成されている場合、SMF は選択された料金設定グループの CHF にクォータ要求を送信します。受信したクォータに基づいて、SMF は PDU セッションを承認または拒否します。PDU セッションの作成中にクォータ関連のエラーが発生した場合、またはクォータが受信されない場合、SMF は「リソースなし」という理由でセッションの作成を拒否します。

SMF はボリューム クォータを保存しません。UPF からトラフィックの開始メッセージを受信すると、SMF は再度 CHF に移動し、クォータを取得します。SMF は、CHF がクォータを再送信するための現在の使用率を 0 として示します。

SMFは、時間クォータ、時間しきい値、または保持時間を受信するとタイマーを開始します。

次の機能が発生します：

- タイマーの期限が切れる前に「トラフィックの開始」を受信すると、SMFはタイマーを停止し、usage=0 および trigger=configured またはデフォルトのトリガ MANAGEMENT_INTERVENTION とともに CHF にクォータ要求を送信します。
- タイマーが「トラフィックの開始」の前に期限切れになった場合、SMF は、使用率 = 0、トリガ = TIME_LIMIT およびクォータ要求で CHF に使用状況レポートを送信し、セッション作成中に受信されたクォータと同じ方法で処理します。

接続またはPDUのセットアップ中に、CHFの最初の要求が送信され、クォータを要求すると、START_OF_SERVICE_DATA_FLOW トリガが使用されます。

# コール フロー

このセクションでは、5G セッションのプリエンプティブ クォータ要求に関連付けられたコール フローについて説明します。

図 ***305 :*** プリエンプティブ クォータ要求のコールフロー：タイマー期限切れ前のトラフィック開始

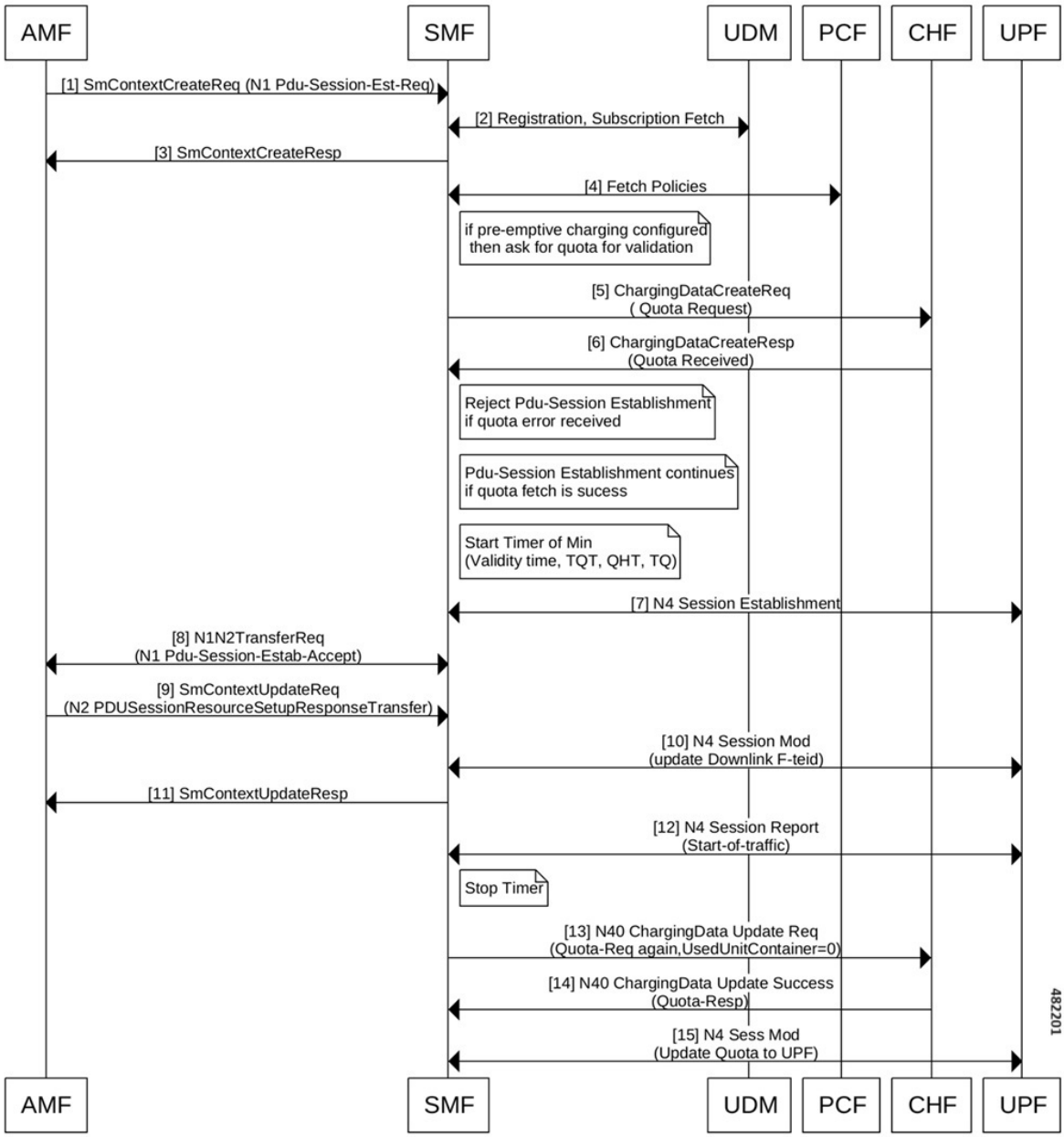


表 *518 :* プリエンプティブ クォータ要求コール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | AMF は N1 PDU セッション作成要求を SMF に送信します。 |
| 2 | SMF はサブスクリプション取得要求を UDM に送信します。次に、UDM は、サブスクリプション取得応答をSMFに送信します。 |
| 3 | SMF は、コンテキスト作成応答を AMF に送信します。 |
| 4 | SMF は PCF と取得ポリシーをネゴシエートします。<br>（注）<br>プリエンプティブ課金が構成されている場合、SMFはクォータの検証を要求します。 |
| 5 | プリエンプティブ課金が構成されている場合、SMF は、構成されている料金設定グループ、およびPCF対話中に受信した事前定義ルールの課金データ作成要求でクォータを要求します。 |
| 6 | CHF はクォータで SMF に応答します。<br>（注）<br>次のどちらかになります。<br>• クォータ エラーを受信した場合、SMF はPDUセッションの確立を拒否します。<br>• クォータ フェッチが成功した場合、SMF は PDU セッションの確立を続行します。<br><br>タイマーは、最小値（ValidityTime、TQT、QHT、TQ）で開始されます。この後に受信されたトラフィックが開始されると、CHF へのクォータ要求が発生します。<br>（注）<br>開始されたタイマーの値は、この値の最小値になります<br>• ValidityTime（VT）<br>• QuotaHoldingTime（QHT）<br>• TimeQuota から減算された TimeQuotaThreshold (TQ-TQT) |
| 7 | SMF は、UPF との N4 セッション確立要求交換を開始します。同じ要求で、SMF は [URR の作成（Create URRs）] で課金に関する情報をリレーします。 |
| 8 | SMF は N1N2 交換と SM Context Update Exchange を AMF に送信します。 |
| 9 | AMF は、SMContext 更新要求を SMF に送信し、PDU セッション リソースのセットアップについて通信します。 |
| 10 | SMF は N4 セッション変更を実行して、ダウンリンク FTEID を更新します。 |

| ステップ | 説明 |
|---|---|
| 11 | SMF は、SMContext Response を AMF に送信します。 |
| 12 | UPF は、N4 セッション レポートを介してトラフィックの開始メッセージを SMF に送信します。 |
| プリエンプティブ クォータ タイマーを停止します。タイマー（ステップ 6）が「トラフィックの開始」の前に期限切れになった場合、SMF は usage=0 で CHF に使用状況レポートを送信し、CHF がクォータを再度送信できるようにします。 | |
| 13 | SMF はクォータを要求する N40 課金データ要求を、使用量 0 で送信します。 |
| 14 | CHF は N40 課金データ更新成功応答メッセージで SMF に応答します。 |
| 15 | SMF は、クォータの更新を UPF に送信します。 |

プリエンプティブ クォータ要求のコール フロー：タイマー期限切れ後のトラフィック開始

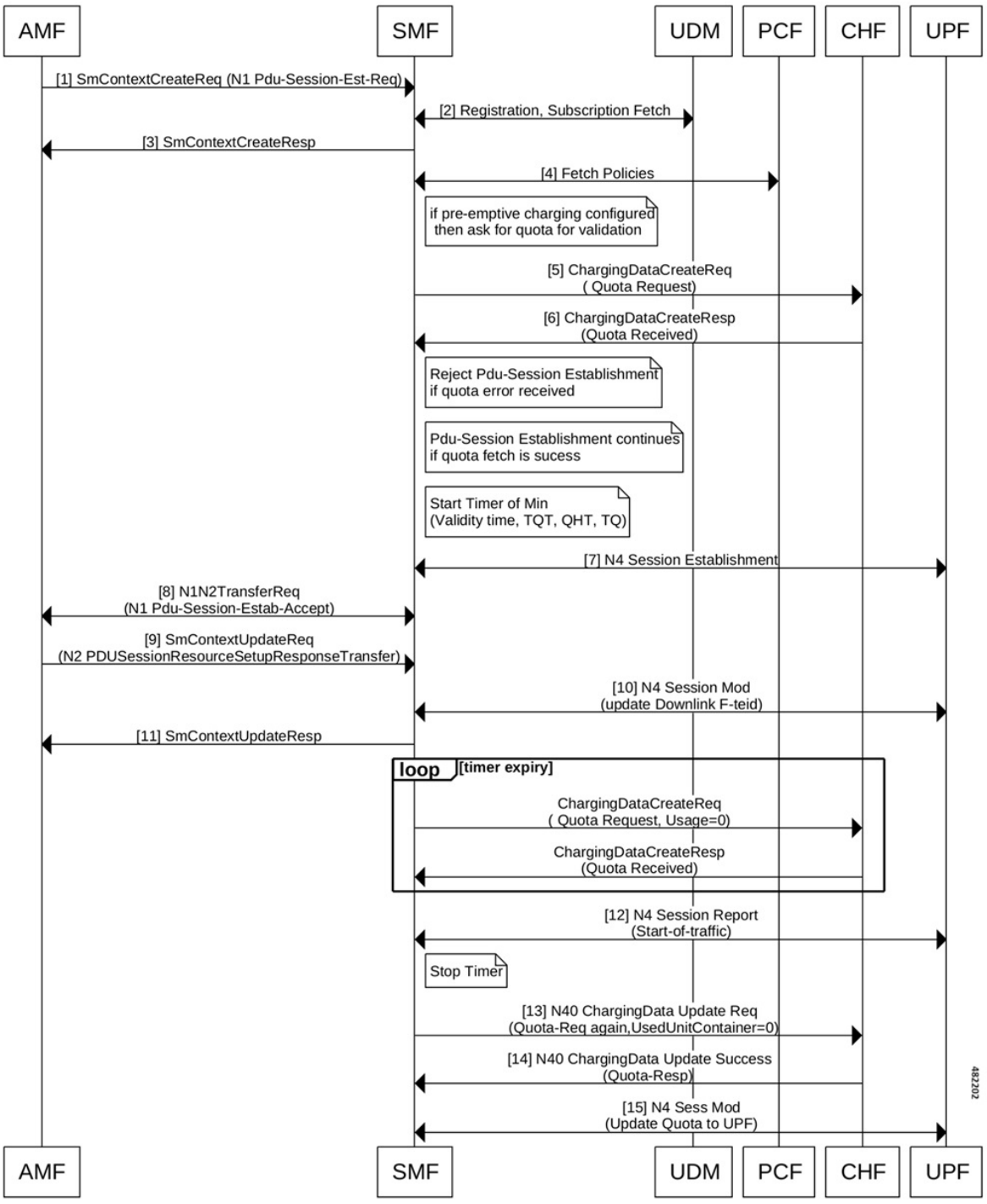


表 *519 :* プリエンプティブ クォータ要求コール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | AMF は N1 PDU セッション作成要求を SMF に送信します。 |
| 2 | SMF はサブスクリプション取得要求を UDM に送信します。次に、UDM は、サブスクリプション取得応答をSMFに送信します。 |
| 3 | SMF は、コンテキスト作成応答を AMF に送信します。 |
| 4 | SMF は PCF と取得ポリシーをネゴシエートします。 |
| 5 | プリエンプティブ課金が構成されている場合、SMF は、構成されている料金設定グループ、およびPCF対話中に受信した事前定義ルールの課金データ作成要求でクォータを要求します。 |
| 6 | CHF はクォータで SMF に応答します。<br>（注）<br>次のどちらかになります。<br>• クォータ エラーを受信した場合、SMF はPDUセッションの確立を拒否します。<br>• クォータ フェッチが成功した場合、SMF は PDU セッションの確立を続行します。<br><br>タイマーは、最小値（ValidityTime,TQT,QHT,TQ）で開始されます。この後に受信されたトラフィックが開始されると、CHF へのクォータ要求が発生します。<br>（注）<br>開始されたタイマーの値は、この値の最小値になります<br>• ValidityTime（VT）<br>• QuotaHoldingTime（QHT）<br>• TimeQuota から減算された TimeQuotaThreshold (TQ-TQT) |
| 7 | SMF は、UPF との N4 セッション確立要求交換を開始します。同じ要求で、SMF は [URR の作成（Create URRs）] で課金に関する情報をリレーします。 |
| 8 | SMF は N1N2 交換と SM Context Update Exchange を AMF に送信します。 |
| 9 | AMF は、SMContext 更新要求を SMF に送信し、PDU セッション リソースのセットアップについて通信します。 |
| 10 | SMF は N4 セッション変更を実行して、ダウンリンク FTEID を更新します。 |
| 11 | SMF は、SMContext Response を AMF に送信します。 |

| ステップ | 説明 |
|---|---|
| （ループ） ステップ 6 で開始されたプリエンプティブ クォータ タイマーが期限切れになります。SMF は使用状況 =0 の CHF に使用状況レポートを送信し、CHF がクォータを再送信できるようにします。 | |
| 12 | UPF は、N4 セッション レポートを介してトラフィックの開始メッセージを SMF に送信します。プリエンプティブ クォータ タイマーを停止します。 |
| 13 | SMF は、クォータを要求する課金データ要求を送信します。使用量は 0 です。 |
| 14 | 次に、CHF は N40 課金データ要求成功応答で SMF に応答します。 |
| 15 | SMF は、クォータの詳細を UPF に送信します。 |

# プリエンプティブ クォータ要求の構成

次の CLI コマンドを使用して、プリエンプティブ クォータ要求を構成します。

```
config
   active-charging service service_name
      charging-action charging_action
        cca charging credit [ preemptively-request-n-validate
traffic-start-trigger ]  trigger_type_name
        end
```

注：

- **charging-action** *charge_action_name*: 課金アクションの名前を指定します。 *charge_action_name* は 、1 ～ 63 文字の英数字の文字列である必要があります。また、句読点を含めることができます。各家禽アクションには一意の名前が必要です。
- 指定された課金アクションが存在しない場合は作成され、CLI モードは課金アクションを構成できる ACS 課金アクション構成モードに変わります。
- 指定された課金アクションが存在する場合、CLI モードはその課金アクションの ACS 課金アクション構成モードに変更されます。
- **cca charging credit**：クレジット制御アプリケーション（CCA）を有効または無効にし、RADIUS/Diameter のプリペイド課金動作を構成します。
- **preemptively-request-n-validate traffic-start-trigger** *trigger_type_name* ：クォータがプリエンプティブに要求され、検証のためにのみ使用されることを指定します。

  この **preemptively-request-n-validate** が料金構成グループ構成で有効になっている場合、SMF はその料金構成グループの CHF にクォータ要求を送信し、クォータは接続または PDU セットアップの検証にのみ使用されます。

**traffic-start-trigger** *trigger_type_name* は 、UPF からのトラフィック開始レポート中に、ChfUpdate で構成されたトリガー タイプを送信するために使用されます。この構成が使用できない場合、デフォルトで management_intervention トリガー タイプが使用されます。

### 設定例

次に、例を示します。

```
charging-action caOnline
  cca charging credit preemptively-request-n-validate traffic-start-trigger
other_quota_type
```

# OAM サポート

## バルク統計サポート

SMF は、プリエンプティブ クォータの一部として次のメトリックを維持します。

- disk_pdusetup_chf_rg_error：切断の理由がプリエンプティブ クォータ検証エラーによる pduSession-reject に対してペグされていることを示します。
- disk_pdnsetup_chf_rg_error：プリエンプティブ クォータ検証エラーにより、接続解除の理由が接続拒否のペグがあることを示します。

第 44 章

# AMF からの TAI 選択


- 機能の概要と変更履歴 （1921 ページ）
- 機能説明 （1922 ページ）
- 機能の仕組み （1922 ページ）
- TAI 選択機能の構成 （1925 ページ）


## 機能の概要と変更履歴

### 要約データ

| | |
|---|---|
| 該当製品または機能エリア | SMF |
| 該当プラットフォーム | SMI |
| 機能のデフォルト設定 | 有効：常時オン |
| このリリースでの関連する変更点 | N/A |
| 関連資料 | 該当なし |

### 更新履歴

**表 *520* : マニュアルの変更履歴**

| 改訂の詳細 | リリース |
|---|---|
| 最初の導入。 | 2021.01.0 |

# 機能説明

SMF では、トラッキングエリア ID（TAI）グループと優先順位に基づいてロケーションを構成するためのオプション構成が提供されています。この構成が使用可能な場合、SMF は SMF サービス登録中に、構成された TAI、つまり TAIList と TAIRRangeList をネットワーク機能（NF）リポジトリ機能（NRF）に送信します。SMF は、この TAI グループと優先順位を使用して NRF に登録できます。

**重要** 構成を変更すると、SMF サービスは新しく構成された TAIList および TAIRrangeList 値を使用して NRF に対して更新されます。

AMF が SMF のリストを NRF から要求すると、サポートされている場所と優先順位に基づいて選択できます。

NF 登録および NF 登録更新の詳細については、「NF の検出と管理 （1099 ページ）」の章の「NF プロファイルの更新 （1120 ページ）」セクションを参照してください。

# 機能の仕組み

SMF は、smfInfo データ型に追加された優先順位属性を使用して、SMF の検出と選択を可能にします。この機能は、異なる TAI リストを持つ異なる smfInfo エントリのターゲット SMF によって登録される相対的な優先順位に基づいています。

次の表に、NFProfile および SMFInfo データ型に含まれる機能固有の属性を示します。

***表 521 : NFProfile***

| | | | | |
|---|---|---|---|---|
| smfInfo | SmfInfo | O | 0..1 | SMF（DNN）の固有のデータ。 |
| smfInfoList | map(SmfInfo) | O | 1..N | SmfInfo の複数のエントリ。この属性は、smfInfo に追加情報を提供します。smfInfoListは、smfInfoが存在しない場合でも存在する可能性があります。<br>マップのキーは、IETF RFC 8259 の句 7 に基づく（一意の）有効な JSON 文字列で、最大 32 文字です。 |

（注）
SMF プロファイルに smfInfo 属性と smfInfoList 属性の両方がない場合は、S-NSSAI、DNN、TAI、およびアクセス タイプに対して SMF を選択できることを意味します。

表 *522 : SMFInfo*

| 属性名 | データタイプ | L | 基数 | 説明 |
|---|---|---|---|---|
| sNscliSmfInfoList | array(sNssaiSmfInfoItem) | M | 1..N | S-NSSAI ごとに SMF でサポートされるパラメータのリスト。 |
| taiList | array(Tai) | O | 1..N | SMF で対応できる TAI のリスト。非 3GPP アクセス TAI が含まれます。この属性と tailRangeList 属性がない場合は、サービングネットワーク内の任意の TAI に対して SMF を選択できます。 |
| taiRangeList | array(TaiRange) | O | 1..N | SMF で処理できる TAI の範囲。非 3GPP アクセス TAI が含まれます。この属性と tailList 属性がない場合は、サービスを提供しているネットワーク内の任意の TAI に対して SMF を選択できます。 |

| 属性名 | データタイプ | L | 基数 | 説明 |
|---|---|---|---|---|
| priority | integer | O | 0..1 | SmfInfoの属性と一致するサービス要求のNFの選択に使用される、0 ～ 65535 の範囲の（同じタイプの他のNFと比較した）優先順位。値が小さいほど、優先順位が高いことを示します。<br>Priority が nfServiceList パラメータまたはNFProfileにも存在する場合は、NFProfile の priority 属性の説明にある優先順位ルールを参照してください。<br>NRF は、Nnrf_NFDiscovery サービスにNFProfileを公開するときに、受信した優先度の値を上書きします。 |
| （注）<br>SMFプロファイルに複数のSmfInfoエントリを含めることができます。各エントリには異なるTAIのリストと異なる優先順位が含まれ、優先順位を区別してユーザーの場所に基づいてSMF を選択できます。SmfInfo の優先順位は最も低くなります。つまり、同じ優先順位のSMF または SMF サービス間に適用されます。 | | | | |

注：

- 構成に変更がない場合（すべての tai-groups データが優先順位なしで送信されます）、NFProfile の SmfInfo が送信されます。
- SmfInfoList マップは NFprofile の新しい要素です。
- 各 SmfInfoList エントリにすべての tail-group-list データが含まれていません。各要素には、NSSAI ごとに同じ優先順位の tai-groups のエントリが含まれます。

（注） スライスの下のすべての TA グループは、同じ優先順位であることが期待されます。

- tier-group-list にスライスの下で構成された異なる優先順位の TAI グループがある場合、TAI グループは優先順位に基づいて論理的にグループ化されます。SmfInfo には、SmfInfoList エントリのそれぞれに 1 つの優先順位の tai-group のデータと、後続の優先順位の tai-group データが含まれています。
- スライスに関連付けられている tai-group がない場合は、古い動作が優先されます。一部のスライスと TAI グループの関連付けがない場合、TAI グループのないスライスの smfinfolist エントリには TAI の詳細はありません。
- 優先順位が定義されていない tai-group では、優先順位が定義されていない場合、個別にグループ化され、SmfInfo エントリまたは別の SmfInfoList エントリとして送信されます。
- 各 SmfInfoList マップ要素のキーは、増分カウンタ文字列です。

# TAI 選択機能の構成

## TAI グループ リストの構成

TAI グループ リストを構成するには、次の構成を使用します。

```
config
nssai name nssai_name
    sst sst ssd ssd
    dnn dnn
    tai-group-list tai_group_list
    end
```

注：

- **tai-group-list** *tail_group_list* ：TAI グループ リストを構成します。

## TAI グループ リストの確認

次の show コマンドを使用して、TAI グループ リストを確認します。

```
show running-config nssai
```

```
nssai name slice1
sst 02
sdt Abf123
dnn [ dnn1 intershat intershat1 intershat2 ]
tai-group-list [ tai-group-1 tai-group-2 tai-group-3 ]
exit
nssai name slice2
sst 02
sdt abc456
dnn [ dnn1 intershat ]
tai-group-list [ tai-group-4 tai-group-5 tai-group-6 ]
exit
```

# TAI グループの構成

ここでは、TAI グループの構成方法について説明します。

次の手順を含む TAI グループの構成：

- TAC リストの構成 （1926 ページ）
- TAC 範囲リストの構成 （1926 ページ）

## TAC リストの構成

次の構成例を使用して、TAI プロファイル内の TAC リストを構成します。

```
config
   profile tai-group tai_group_name
      mcc mcc_value mnc mnc_value
      tac list [ tac_list_values ]
      end
```

注：

- **mcc** *mcc_value* **mnc** *mnc_value*：モバイル国コード（MCC）とモバイル ネットワーク コード（MNC）を構成します。
  - **mcc** *mcc_value*：モバイル国コード（MCC）を指定します。 *mcc_value* は、3 桁のパターンの文字列である必要があります。
  - **mnc** *mnc_value*：モバイル ネットワーク コード（MNC）を指定します。 *mnc_value* は、2 桁または 3 桁のパターンの文字列である必要があります。
- **tac list [** *tac_list_values* **]**：TAC 値のリストを構成します。例：[ 1111 2222 3333 ]

## TAC 範囲リストの構成

次の構成例を使用して、TAI プロファイル内の TAC 範囲リストを構成します。

```
config
   profile tai-group tai_group_name
      mcc mcc_value mnc mnc_value
      tac range start start_value end end_value
      end
```

注：

- **tac range start** *start_value* **end** *end_value*：特定の TAC 範囲または複数の TAC 範囲のリストを構成します。次に例を示します。 **tac range start DDDD end EEEE**

  範囲内で最大 16 個の値を構成できます。
- 特定の TAC 範囲または TAC 範囲を削除するには、 **no tac range start** *start_value* **end** *end_value* コマンドを使用します。

## TAI グループ構成の確認

TAI グループ構成を確認するには、次の show コマンドを使用します：

**show running-config profile tai-group** *tai_group_name*

次に、構成例を示します：

```
show running-config profile tai-group t1
profile tai-group t1
mcc 111 mnc 222
  tac list [ 1111 2222 3333 ]
  tac range start 4444 end 5555
  exit
exit
mcc 333 mnc 44
  tac list [ AAAA BBBB CCCC ]
  tac range start DDDD end EEEE
  exit
exit
exit
```

# プライオリティの設定

TAI グループを構成するには、次のサンプル構成を使用します。

```
config
profile tai-group tai_group_name
    priority priority
    end
```

注：

- **priority** *priority* ：TAI グループの優先順位を指定します。

# 優先順位構成の確認

TAI グループ優先順位に関連付けられている構成を確認するには、次の show コマンドを使用します。

**show running-config profile tai-group**

```
profile tai-group t1
mcc 123 mnc 456
priority 1
tac list [ 1234 789123 ]
tac range start 1234 end 1980
exit
exit
exit
profile tai-group t2
priority 1
mcc 456 mnc 123
tac list [ 0000 123456 ]
tac range start 3456 end 9000
exit
exit
exit
```

第 45 章

# UDM の統合


- 機能の概要と変更履歴 （1929 ページ）
- 機能説明 （1930 ページ）
- 機能の仕組み （1930 ページ）
- UDM を構成 （1931 ページ）
- 即時レポートによるサブスクリプション通知の構成ベースの制御 （1934 ページ）
- コンバージド コアで N10 フェール オープン （1938 ページ）
- サブスクリプション メッセージの構成ベースの制御 （1939 ページ）
- UDM 登録メッセージの構成ベースの制御 （1942 ページ）
- UDM データ変更通知に基づくセッション管理 （1944 ページ）


## 機能の概要と変更履歴

### 要約データ

**表 *523* : 要約データ**

| | |
|---|---|
| 該当製品または機能エリア | SMF |
| 該当製品または機能エリア | SMI |
| 機能のデフォルト設定 | 有効：常時オン |
| このリリースでの関連する変更点 | N/A |
| 関連資料 | 該当なし |

# 更新履歴

表 *524 :* マニュアルの変更履歴

| 改訂の詳細 | リリース |
|---|---|
| N10 フェール オープンのサポートが追加されました。 | 2023.04.0 |
| 最初の導入。 | 2020.02.2 |

# 機能説明

統合データ管理（UDM）は主にサブスクライバ データを保存する役割を果たし、SMF はネットワーク上のユーザー セッションを管理するためにこのデータにアクセスします。SMF は、セッション終了などのサブスクライバデータで発生したイベントに関する通知を受信するように明示的にサブスクライブします。

N10 インターフェイスは、ユニファイド データ管理（UDM）と SMF（セッション管理機能）の間にあります。UDM は、Nudm インターフェイスを介して SMF に次のサービスを提供します：

- Nudm_SubscriberDataManagement サービス
- Nudm_UEContextManagement サービス

# 機能の仕組み

ここでは、この機能の仕組みを説明します。

SMF が UDM サブスクリプションをスキップすると、次のメッセージの送信を停止します。

- セッション確立中にサブスクリプションを取得する
- セッション確立中の通知の登録
- セッションの解放中および UDCM が UECM メッセージを受信したときの Unsubscribe-to-Notification

SMF では、UDM サブスクリプションのスキップ構成に対する動的な変更が可能です。つまり、新しい値は、確立される新しいセッションに適用されます。既存のセッションは古い値を引き続き使用します。

# UDM を構成

このセクションでは、UDM に関連するすべての構成について説明します：

# SDM メッセージを制御するためのオプションの構成

ここでは、N10 インターフェイスでのサブスクリプション データ管理（SDM）メッセージの制御を構成する方法について説明します。

## RAT タイプの設定

DNN プロファイルでローカル承認を使用して RAT タイプを構成するには、次の構成例を使用します。

```
config
   profile dnn dnn_profile
      authorization local rat-type [ nr | eutra | wlan ]
      end
```

注：

- **authorization local**：このコマンドは、EPS セッションの SDM メッセージのみをスキップします。選択した DNN プロファイルでこのコマンドを構成すると、SMF はサブスクリプションを取得するための UDM 対話をスキップします。SMF では、セッション要求の作成メッセージで受信した値が使用されます。SMF は、UDM から「Subscribe-for-Notifications」への UDM 対話をスキップします。
- **rat-type [ nr | eutra | wlan ]**：このキーワードは、指定された RAT タイプに基づいて次の SDM メッセージをスキップします。
  - udm subscription-fetch
  - subscribe-to-notifications
  - unsubscribe-to-notifications

  選択した DNN プロファイルで **authorization local** コマンドを使用して RAT タイプを構成すると、その RAT タイプのセッションでは、SMF は次のメッセージの UDM 対話をスキップします。
  - udm subscription-fetch during session establishment
  - subscribe-for-notifications during session establishment
  - unsubscribe-for-notifications during session release
- **no authorization local rat-type [ nr | eutra | wlan ]**：DNN プロファイルに基づいてセカンダリ認証を無効にします。

### 設定の確認

構成を確認するために、この **show running-config profile dnn** *dnn_profile_name* コマンドを使用します。

この show コマンドの出力には、指定された DNN プロファイル内で構成されている RAT タイプ情報を含むすべての構成が表示されます。

```
[smf] smf# show running-config profile dnn intershat
profile dnn intershat
network-element-profiles chf chf1
network-element-profiles amf amf1
network-element-profiles pcf pcf1
network-element-profiles udm udm1
charging-profile chgprf1
virtual-mac b6:6d:47:47:47:47
ssc-mode 2 allowed [ 3 ]
session type IPV6 allowed [ IPV6 ]
authorization local rat-type nr
upf apn intershat
dcnr true
exit
```

## セッション タイプの構成

SMF は、UDM 応答からのサブスクリプション タイプ データと DNN プロファイルのセッションタイプ構成の両方を使用して、コールを許可または拒否します。SMF は、UDM サブスクリプション データ内の UE 要求の PDN タイプの最初のルックアップに基づいて、セッション タイプを選択します。次に、SMF は、選択したセッション タイプと DNN プロファイルで構成されたセッション タイプに基づいて、セッションのセッション タイプをプロビジョニングします。

DNN プロファイルで PDU セッション タイプを構成するには、次の構成例を使用します。

```
config
   profile dnn dnnprofile
      session type { IPV4 | IPV4V6 | IPV6 } allowed [ IPV4 | IPV4V6 |
IPV6 ]
      end
```

注：

- **session type { IPV4 | IPV4V6 | IPV6 } allowed [ IPV4 | IPV4V6 | IPV6 ]**：PDU セッションの IP タイプを指定します。 **allowed** キーワードを使用すると、デフォルトのセッション タイプ以外の 2 つの IP タイプを指定できます。
- SMF はこのセッション タイプ構成を使用して、コールを処理します。たとえば、UE 要求タイプが IPv4 で、UDM サブスクリプション タイプが IPv4v6 の場合、SMF は最初のパスで IPv4 を選択し、その後セッション タイプ構成に対してチェックします。構成されたセッション タイプが IPv6 の場合、SMF は「#51 - PDU session type IPv6 only= IPV4 allowed」という原因でコールを拒否します。
- IPAM 構成に、最後に選択された PDU セッション タイプと異なる IP アドレス プールが含まれている場合、SMF は、原因「#31 -request rejected, unspecified」でコールを拒否します。たとえば、この原因値は次の条件で生成されます：

- UeReq-PdnType = V4
- UdmSubscription-PdnType = V4V6
- SessionType-Config = V4V6
- IP-Pool = V6

### 設定の確認

構成を確認するために、この **show running-config profile dnn** *dnn_profile_name* コマンドを使用します。

この show コマンドの出力には、指定された DNN プロファイル内で構成されているセッション タイプ情報を含むすべての構成が表示されます。

```
[smf] smf# show running-config profile dnn intershat
profile dnn intershat
network-element-profiles chf chf1
network-element-profiles amf amf1
network-element-profiles pcf pcf1
network-element-profiles udm udm1
charging-profile chgprf1
virtual-mac b6:6d:47:47:47:47
ssc-mode 2 allowed [ 3 ]
session type IPV6 allowed [ IPV6 ]
upf apn intershat
dcnr true
exit
```

## オプションの IE を無効にする構成

N10 登録要求で、 **epdgInd** 属性や **registrationTime** 属性などのオプションの IE を無効にするには、次の構成例を使用します。

```
config
  profile message-handling nf-type nf_ype
     mh-profile mh_profile_name
     service name type { nudm-ee | nudm-pp | nudm-sdm | nudm-ueau |
nudm-uecm }
     message type { UdmRegistrationReq | UdmSdmGetUESMSubscriptionData
 | UdmSdmSubscribeToNotification | UdmSdmUnsubscribeToNotification |
UdmSubscriptionReq | UdmUecmRegisterSMF skip optional-ies [ epdgInd |
registrationTime ] | UdmUecmUnregisterSMF }
    exit
 exit
exit
```

注：

- **mh-profile** *mh_profile_name* ：NRF メッセージ処理プロファイル構成を指定します。
- **skip optional-ies [ epdgInd | registrationTime ]** ：登録要求内の ePDG 指示と登録時間をスキップします。

（注） **skip optional-ies [ epdgInd | registrationTime ]** コマンドは、UdmUecmRegisterSMF メッセージでのみ使用できます。

# 即時レポートによるサブスクリプション通知の構成ベースの制御

表 *525 :* 機能の履歴

| 機能名 | リリース情報 | 説明 |
|---|---|---|
| N10 インターフェイスでの即時レポート表示によるサブスクリプション通知の構成ベースの制御 | 2024.03.0 | UDM で「immediateReport」属性を有効にすると、SMF は UDM サブスクリプション fetch メッセージを無視してサブスクリプション通知要求を続行します。この場合、サブスクリプション管理データがサブスクリプション通知応答で受信されます。<br>即時レポートの表示を利用したこの制御された UDM 通知サブスクリプションにより、4G、5G、および Wi-Fi 接続手順中に N10 インターフェイスを介した SMF と UDM 間の連携動作が最小限に抑えられるため、メッセージの過負荷や障害が防止されます。<br>この機能により、DNN プロファイルに新しい CLI コマンド **subscription notify-immediate** が導入されます。<br>**デフォルト設定**：無効：構成が必要 |

# 機能説明

Nudm_SDM_Subscribe サービス操作要求で UDM の「immediateReport」属性が有効になっている場合、SMF は UDM サブスクリプション取得メッセージを無視し、サブスクリプション通知を継続します。UDM は、応答内のサブスクリプション データを SMF に送信します。「immediateReport」属性は、即時レポートが必要かどうかを示します。この属性はデフォルトでは無効になっています。

この機能を有効にすると、4G、5G、および Wi-Fi 接続手順中の N10 インターフェイスを介した SMF と UDM 間の相互作用が最小限に抑えられます。やりとりを最小限に抑えることにより、メッセージの過負荷や障害を防ぎます。この機能は、**subscription notify-immediate** CLI コマンドを使用して設定できます。

（注） UDM サブスクリプションの「immediateReport」属性は、*3GPP TS 29.503* バージョン *16.9.0*、リリース *16* でのみサポートされます。

# 機能の仕組み

即時レポート機能によるサブスクリプション通知が有効になっている場合、SMF は次のタスクを実行します：

- **subscription notify-immediate** CLI が構成されている場合、すべての UDM が即時レポート機能をサポートしていると見なされます。
- SMF は N10 サブスクリプションのフェッチをスキップして、N10 サブスクリプション通知を続行します。SMF は、Subscribe to Notify 要求に「immediateReport」属性を含めます。
- SMF は、Subscribe to Notify 応答でサブスクリプション データを受信しない場合、サブスクリプション取得手順をトリガーします。
- SMF は、サービス通信プロキシ（SCP）を介して UDM に「immediateReport」属性を使用してサブスクリプション通知をトリガーします。応答にサブスクリプションデータが含まれている場合、SMF はサブスクリプションの取得を再度実行しません。それ以外の場合、SMF はサブスクリプション フェッチをトリガーします。

（注） サブスクリプション通知が失敗した場合、SMF は失敗処理の構成に基づいてアクションを実行します。

- SMF は、同じ RAT タイプに対して **subscription local rat-type** と **subscription notify-immediate** の両方の CLI コマンドが構成されている場合にのみ **subscription local rat-type** 、 CLI 機能を有効にします。
- **authorization local** CLI が構成されている場合、SMF は **subscription [ local | notify-immediate ]** CLI 機能を無視します。

# 即時レポートによるサブスクリプション通知の構成

即時レポートを使用した UDM サブスクリプション通知メッセージを制御するには、次の構成例を使用します：

```
config
   profile dnn dnn_profile
      subscription [ local | notify-immediate ] rat-type [ nr | eutra
| wlan ]
      end
```

注：

- **subscription notify-immediate**：SMF はサブスクリプションの取得手順をスキップし、ImmediateReport を使用して「Subscribe to Notify」手順を続行します。

## 即時レポートによるサブスクリプション通知の確認

ここでは、「immediateReport」属性が有効になっている場合のサブスクリプション通知の確認方法について説明します。

**show running-config profile dnn** コマンドを使用して、さまざまな RAT タイプで「immediateReport」属性が有効になっている場合のサブスクリプション通知を確認します。

以下は、構成されている **subscription local rat-type** および **subscription notify-immediate rat-type** 値の **show running-config profile dnn** コマンドの出力例です。

```
show running-config profile dnn dnnprof-ims.prod
 profile dnn dnnprof-ims.prod
   subscription local rat-type [ wlan ]
   subscription notify-immediate rat-type [ nr wlan ]
exit
```

# OAM サポート

このセクションは、即時レポート機能付きのサブスクリプション通知の操作、管理、およびメンテナンスの情報を説明します。

## メトリック

この機能の一部として、次のラベルが追加されています。

- **UDM_LABEL_IMMEDIATE_RPT**：このラベルは、「immediateReport」属性が有効になっている PDU セッションの数を決定するために、RecordUdmMsgProcessingStats **udm_msg_processing_status** メトリックに追加されます。

次に、即時レポート機能が無効になっている場合のメトリックの例を示します。

```
udm_msg_processing_status{app_name="smf",cluster="Local",data_center="DC",
gr_instance_id="1",immediate_report="false",instance_id="0",msg_status="accepted",
rat_type="nr",service_name="smf-service",snssai="",udm_end_point="",udm_msg="UdmRegistration"}
 1
```

```
udm_msg_processing_status{app_name="smf",cluster="Local",data_center="DC",
gr_instance_id="1",immediate_report="false",instance_id="0",msg_status="accepted",
rat_type="nr",service_name="smf-service",snssai="",udm_end_point="",udm_msg="UdmSmSubscription"}
 1

udm_msg_processing_status{app_name="smf",cluster="Local",data_center="DC",
gr_instance_id="1",immediate_report="false",instance_id="0",msg_status="accepted",
rat_type="nr",service_name="smf-service",snssai="",udm_end_point="10.105.35.112:8001",
udm_msg="UdmSubscribeToNotify"} 1

udm_msg_processing_status{app_name="smf",cluster="Local",data_center="DC",
gr_instance_id="1",immediate_report="false",instance_id="0",msg_status="attempted",
rat_type="nr",service_name="smf-service",snssai="",udm_end_point="",udm_msg="UdmRegistration"}
 1

udm_msg_processing_status{app_name="smf",cluster="Local",data_center="DC",
gr_instance_id="1",immediate_report="false",instance_id="0",msg_status="attempted",
rat_type="nr",service_name="smf-service",snssai="",udm_end_point="",udm_msg="UdmSmSubscription"}
 1

udm_msg_processing_status{app_name="smf",cluster="Local",data_center="DC",
gr_instance_id="1",immediate_report="false",instance_id="0",msg_status="attempted",
rat_type="nr",service_name="smf-service",snssai="",udm_end_point="10.105.35.112:8001",
udm_msg="UdmDeregistration"} 1

udm_msg_processing_status{app_name="smf",cluster="Local",data_center="DC",
gr_instance_id="1",immediate_report="false",instance_id="0",msg_status="attempted",
rat_type="nr",service_name="smf-service",snssai="",udm_end_point="10.105.35.112:8001",
udm_msg="UdmSubscribeToNotify"} 1
```

次に、即時レポート機能が有効になっている場合のメトリックの例を示します。

```
udm_msg_processing_status{app_name="smf",cluster="Local",data_center="DC",
gr_instance_id="1",immediate_report="false",instance_id="0",msg_status="accepted",
rat_type="nr",service_name="smf-service",snssai="",udm_end_point="",udm_msg="UdmRegistration"}
 1

udm_msg_processing_status{app_name="smf",cluster="Local",data_center="DC",
gr_instance_id="1",immediate_report="true",instance_id="0",msg_status="accepted",
rat_type="nr",service_name="smf-service",snssai="",udm_end_point="",udm_msg="UdmSmSubscription"}
 1

udm_msg_processing_status{app_name="smf",cluster="Local",data_center="DC",
gr_instance_id="1",immediate_report="true",instance_id="0",msg_status="accepted",
rat_type="nr",service_name="smf-service",snssai="",udm_end_point="10.105.35.112:8001",
udm_msg="UdmSubscribeToNotify"} 1

udm_msg_processing_status{app_name="smf",cluster="Local",data_center="DC",
gr_instance_id="1",immediate_report="false",instance_id="0",msg_status="attempted",
rat_type="nr",service_name="smf-service",snssai="",udm_end_point="",udm_msg="UdmRegistration"}
 1

udm_msg_processing_status{app_name="smf",cluster="Local",data_center="DC",
gr_instance_id="1",immediate_report="true",instance_id="0",msg_status="attempted",
rat_type="nr",service_name="smf-service",snssai="",udm_end_point="",udm_msg="UdmSmSubscription"}
 1

udm_msg_processing_status{app_name="smf",cluster="Local",data_center="DC",
gr_instance_id="1",immediate_report="false",instance_id="0",msg_status="attempted",
rat_type="nr",service_name="smf-service",snssai="",udm_end_point="10.105.35.112:8001",
udm_msg="UdmDeregistration"} 1

udm_msg_processing_status{app_name="smf",cluster="Local",data_center="DC",
gr_instance_id="1",immediate_report="true",instance_id="0",msg_status="attempted",
```

```
rat_type="nr",service_name="smf-service",snssai="",udm_end_point="10.105.35.112:8001",
udm_msg="UdmSubscribeToNotify"} 1
```

# コンバージド コアで N10 フェール オープン

表 *526 :* 機能の履歴

| 機能名 | リリース情報 | 説明 |
|---|---|---|
| フェール オープン サポートによる N10 インターフェイスでの SMF と UDM の相互作用の最小化 | 2023.04 | フェール オープン機能により、SMF は N10 メッセージ エラー中のコールに対する無視および続行エラー処理アクションをサポートします。これらの障害には、すべての RAT タイプの UDM 登録、サブスクライバの取得、および通知へのサブスクライブが含まれます。 |

## 機能説明

この機能は次をサポートします：

- フェールオープン（Fail open）：SMF では、N10 メッセージエラーが発生しているときのコールに対して、無視および続行の障害処理アクションをサポートしています。これらの障害には、すべての RAT タイプ（LTE、NR、Wi-Fi）に対するUDM登録、回線取得、および通知へのサブスクライブが含まれます。

  セッションの作成中に登録が実行されないか、または失敗した場合、構成された障害処理アクションに基づいて、SMF は引き継ぎ中に N10 登録を実行します。障害処理アクションは、無視するか、続行することができます。セッションを終了するように障害アクションを構成しておらず、ハンドオーバー中に障害が発生した場合、SMF は障害を無視してハンドオーバー手順を続行します。

- SCP モデル D との相互作用：SCP 障害処理を「続行」または「無視」に構成している場合は、前述の障害処理を適用できます。SCP 障害処理をフォールバックとして設定し、フォールバック後に障害が発生した場合、UDM 障害処理で設定したアクションが適用されます。

# サブスクリプション メッセージの構成ベースの制御

## 機能説明

統合データ管理（UDM）は主にサブスクライバ データを保存する役割を果たし、SMF はネットワーク上のユーザー セッションを管理するためにこのデータにアクセスします。SMF は、セッション終了などのサブスクライバデータで発生したイベントに関する通知を受信するように明示的にサブスクライブします。SMF は通知の受信を停止する場合、Unsubscribe-to-Notification メッセージを UDM に対して開始します。これらのメッセージを受信すると、UDMは、登録済みセッションの通知サブスクリプションを削除して、サブスクリプションをキャンセルします。

（注） UDM によってトリガーされたサブスクリプションの変更が確認されても、SMF は通知を受信しません。ただし、UDM がトリガーしたセッション終了の場合、SMF は UDM から通知を受信します。

## 機能の仕組み

このセクションでは、Unsubscribe-to-Notifications メッセージを介した SMF および UDM の通信方法の概要を示します。

1. SMF などの NF は、UDM への URI で識別されるリソースに Unsubscribe-to-Notifications 要求を送信します。SMFは、N10インターフェイスを介して要求を UDM に変換します。Unscribe-to-Notifications 要求により、SMF は特定のサブスクライバセッションの通知をサブスクライブ解除できます。SMF は、サブスクリプション作成中に URI の詳細を受信します。

   Unsubscribe-to-Notifications リクエストには、URI に「SUPI」と「subscriptionId」が含まれています。

2. UDM が要求を処理し、その応答に基づきます。応答コードを SMF に送信します。たとえば、サブスクリプション解除が成功した場合、UDMは204コードを送信します。要求が処理されない場合、エラーを示す適切な HTTP ステータス コードが追加のエラー情報とともに応答本文で返されます。

3. SMF は、Unsubscribe-to-Notifications メッセージを UDM に送信するときに発生するタイムアウトと障害を処理します。Unsubscribe-to-Notifications 要求が失敗する場合、SMF は対応するセッションを消去し続けます。

   EUTRA ネットワークでホストされるセッションには、Unsubscribe-to-Notification メッセージが必要です。このネットワーク上にあることは、NR および WLAN ネットワークでリリースされるセッションの要件ではない場合があります。これらのアクセス タイプの場

合、SMF は、登録解除中に暗黙的なサブスクライブ解除による通知へのサブスクリプションを含む UDM 登録および登録解除メッセージを送信します。

## 標準準拠

通知への登録解除メッセージ機能へのサポートは、次の標準に準拠しています：

- *3GPP TS 29.503 - 5G* システム、統合データ管理サービス

## コール フロー

ここでは、Unsubscribe-To-Notifications メッセージ サポートのコール フローについて説明します。

### 通知への登録解除コール フロー

このセクションでは、データ変更の通知からのサブスクリプション解除に関する要求をSMFがUDMに送信する方法に関するコール フローについて説明します。

**図 *306 : UDM* との *Unsubscribe-to-Notifications* 通信**

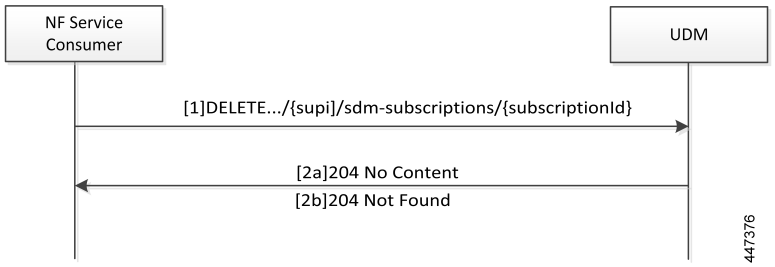



**表 *527 :* 通知への登録解除コール フローの説明**

| ステップ | 説明 |
|---|---|
| 1 | SMF などの NF サービス コンシューマは、UDM に通知のサブスクリプション解除要求を送信します。サブスクリプションを解除すると、各サブスクライバセッションでデータの変更が発生した場合に、UDM は SMF に通知を送信しなくなります。<br>NF サービス コンシューマは、URI によって識別されるリソースに DELETE 要求を送信します。NF サービス コンシューマは、サブスクリプションが作成されると、URI を受け取ります。 |
| 2a | 要求の削除が成功すると、UDMは「204 No Content」と応答します。 |

| ステップ | 説明 |
| --- | --- |
| 2b | サブスクリプションが無効である場合（不明な subscriptionId 値が原因である可能性がある）、HTTP ステータス コード「404 Not Found」が、応答本文の追加エラー情報とともに返されます（「ProblemDetails」要素の一部として）。<br>要求が処理されない場合、エラーを示す適切な HTTP ステータス コードが追加のエラー情報とともに DELETE 応答本文で返されます。 |

# サブスクライブ解除メッセージの OAM サポート

ここでは、この機能の操作、管理、およびメンテナンスに関して説明します。

## 統計情報サポート

SMF は、UDM に対して開始される [unsubscribe-to-notifications] メッセージの数をモニタリングするために、smf-rest-ep ポッドに次のラベルを維持します：

- nfType：「udm」
- messageDirection：「outbound」
- apiName：「sdm_unsubscription_req」
- nfUri：「nf_uri」
- respStatus：「response_status」
- rspCause：「response_cause」

# UDM 登録メッセージの構成ベースの制御

表 *528 :* 機能の履歴

| 機能名 | リリース情報 | 説明 |
|---|---|---|
| UDM 登録メッセージの構成ベースの制御 | 2024.01.2 | SMF を使用すると、ユーザーは PDU のセットアップと Wi-Fi 接続の手順中に、UDM 登録メッセージを無視できます。<br>この制御された UDM の登録により、N10 インターフェイスでの SMF と UDM 間の連携が最小限に抑えられ、N10 インターフェイスでのメッセージの過負荷と接続の失敗を処理するために最小限に抑えられます。<br>この機能により、DNN プロファイルに新しい CLI コマンド **skip-n10-registration rat-type [ NR \| WIFI \| ALL ]** が導入されます。<br>**デフォルト設定**：無効：構成が必要 |

## 機能説明

N10 インターフェイスでのメッセージの過負荷が UE 接続の失敗の原因である場合、SMF は、UE 登録メッセージが UDM に到達するのを無視します。この機能により、5G および Wi-Fi ネットワークでの N10 の連携動作が最適化されます。この機能は、**skip-n10-registration rat-type [ NR | WIFI | ALL ]** CLI コマンドを使用して設定できます。

## 機能の仕組み

**skip-n10-registration rat-type [ NR | WIFI | ALL ]** CLI コマンドを構成すると、SMF は 5G および Wi-Fi ネットワークでのセッションの作成中に UDM 登録を無視します。ePDG がセッションを処理していたターゲット SMF を検出できないため、5G と Wi-Fi 間のハンドオーバーが失敗します。5G または Wi-Fi 接続中に UE 登録が失敗し、UDM 障害処理テンプレート（FHT）

が続行または無視に構成されている場合、SMF は Wi-Fi から 5G および 5G から Wi-Fi へのハンドオーバー時に登録を再試行します。

# UDM 登録メッセージの制御の構成

UDM 登録メッセージを制御するには、次の構成例を使用します：

```
config
   profile dnn dnn_profile
      skip-n10-registration rat-type [ NR | WIFI | ALL ]
      exit
```

注：

- **skip-n10-registration rat-type [ NR | WIFI | ALL ]**：UDM 登録を無視する RAT タイプを指定します。

# UDM データ変更通知に基づくセッション管理

## UDM データ変更通知に基づくセッション管理

表 *529 :* 機能の履歴

| 機能名 | リリース情報 | 説明 |
|---|---|---|
| UDMデータ変更通知に基づくセッション管理 | 2025.01.0 | この機能により、SMF は、Unified Data Management（UDM）から REPLACE 操作を含むデータ変更通知を受信すると、セッションを終了または続行します。この機能により、ユーザー機器（UE）が新しいサブスクリプションの変更を利用できるようになります。<br>この機能により、既存のイベント管理ポリシー構成に新しいイベント **subscription-change** が導入されます。<br>**コマンドの拡張**：<br>**policy eventmgmt** *policy_eventmgmt_name* **priority** *priority_number* **event** *subscription-change*<br>**デフォルト設定**：無効：構成が必要 |

データ速度を 2 Mbps から 8 Mbps にアップグレードするなど、サブスクライバ データに変更がある場合、UDM は変更された属性を含むこのデータ変更通知を SMF に送信します。SMF がセッションを続行または終了します。SMFがセッションを終了すると、新しいサブスクリプション値が UE で更新されます。SMF がセッションを続行すると、UE でアクションは実行されません。

## SMF が UDM データ変更通知を使用してセッションを管理する方法

SMF は、UDM データ変更通知を受信すると、イベント管理ポリシー内のユーザー定義の構成またはシステム定義の構成に基づいてアクションを実行します。SMFがイベント管理ポリシーでサブスクリプションの変更に関するユーザー定義の構成を検出すると、SMFはその構成に基

づいてセッションを管理します。それ以外の場合、システム定義の構成に基づいてSMFがセッションを管理します。

UDMデータ変更通知には、NotifyItemsのリストを含むModificationNotificationが含まれます。NotifyItemsには、次の変更された属性を含むChangeItemフィールドが含まれます：

- Ambr
- 3gppChargingCharacteristics
- sscModes
- Snssai
- 登録済みデフォルトQoS
- staticIpAddress
- pduSessionTypes

[ChangeItem]フィールドには、次のパラメータが含まれます：

- op：リソースに対して行われる操作のタイプを示します。

（注） SMFは、op属性がREPLACE操作に設定されている場合にのみアクションを実行します。

- パス：変更が適用されるリソース内のターゲット位置を示すJSONポインタ値が含まれます。

（注） SMFは、UDM変更通知パスを空の（「」）としてサポートします。

- origValue：ターゲット位置の元の値を示します。この属性は、op属性の値がMOVE、REPLACE、またはREMOVEの場合に存在します。
- newValue：ターゲットロケーションの新しい値を示します。この属性は、op属性の値がADDまたはREPLACEの場合に存在します。

（注） hSMF（ホームSMF）では、SMFはUDM変更通知を受信するとコールを続行し、それ以外のアクションは実行しません。

## ユーザー定義の設定でセッションを管理

次の段階では、ユーザー定義の構成に基づいてSMFがセッションを管理する方法について説明します。

1. SMF が、OP 属性値が REPLACE に設定されたデータ変更通知を受信したときSMF は、policy eventmgmt CLI コマンドの *subscription-change* イベントのユーザー定義アクションに基づいてセッションを終了または続行します。
2. サブスクリプション変更イベントに対してアクション *terminate* が構成されている場合、SMF はセッションを終了し、Reactivation-Require メッセージとして N1 の原因を UE に送信します。新しいサブスクリプション値が UE で更新されます。サブスクリプション変更イベントに対してアクションの *continue* が構成されている場合、SMF はセッションを続行し、UE で変更は更新されません。

詳細については、「イベント管理ポリシー」の「サブスクリプション変更イベントの有効化」の項を参照してください。

## システム定義の構成によるセッションの管理

次の段階では、システム定義の構成に基づいて SMF がセッションを管理する方法について説明します。

1. SMF が、NotifyItem の ChangeItem フィールドにおいて REPLACE 操作に構成された origValue と newValue を含む UDM データ変更通知を受信すると、SMF はセッションを終了するか、続行します。
2. 通知で NotifyItems を受信すると、SMF は NotifyItem の originate 値をサブスクライブされたデータと比較します。
3. origValue がサブスクライブされたデータと一致する場合、SMF は関連する NotifyItem を選択します。選択した NotifyItem 内で、SMF は originate を属性の newValue と比較します。この比較により、変更された属性が特定されます。SMF は、origValue と newValue の比較で識別された変更された属性に基づいて、セッションを終了するか続行するかを決定します。SMF がセッションを終了すると、新しいサブスクリプション値が UE で更新されます。SMF がセッションを続行する場合、アクションは実行されません。

（注） SMF が NotifyItem の ChangeItem フィールドに originate 値を含まないデータ変更通知を受信すると、SMF はセッションを続行し、エラー応答 503 を UDM に送信します。

SMF は、次の表に示すようにセッションを管理します。

| 属性 | 状態（Condition） | 操作 |
|---|---|---|
| Ambr | SMF は Ambr の newValue と origin Value を比較しません。 | セッションを続行し、アクションは実行されません。 |

| 属性 | 状態（Condition） | 操作 |
|---|---|---|
| 3gppChargingCharacteristics | 条件 1：ChargingCharacteristics の newValue が ChargingCharacteristics の originValue と異なる場合。 | セッションを終了します。 |
| | 条件 2：ChargingCharacteristics の newValue が ChargingCharacteristics の originValue と同じである場合。 | セッションを続行し、アクションは実行されません。 |
| Snssai | 条件 1：Snsサイトの newValue に sst および sd との一致がない場合、または sst の一致がない場合（Snsnai に sst のみが含まれている場合）、origValue と一致することはありません。 | セッションを終了します。 |
| | 条件 2：Snsnai の newValue が sst と sd に一致するか、または sst match（Snsnai に sst のみが含まれる場合）が originate と一致する場合。 | セッションを続行し、アクションは実行されません。 |
| 登録済みデフォルト QoS | SMF では、SubscribedDefaultQos の newValue と originValue は比較されません。 | セッションを続行し、アクションは実行されません。 |
| sscModes | SMF では SSCmode1 のみがサポートされます。SSCmode1 が newValue にプリセットされていない場合、通話は切断されます。 | セッションを終了します。 |
| pduSessionTypes | 条件 1：pduSessionType の newValue が、origValue と同じまたはスーパーセットではない場合。 | セッションを終了します。 |
| | 条件 2：pduSessionType の newValue が originValue と同じ場合。 | セッションを続行し、アクションは実行されません。 |

| 属性 | 状態（Condition） | 操作 |
|---|---|---|
| staticIpAddress | 条件 1：staticIpAddress の newValue が originValue と同じでない場合。 | セッションを終了します。 |
| | 条件 2：staticIpAddress の newValue が originValue と同じ場合。 | セッションを続行し、アクションは実行されません。 |

# イベント管理ポリシーでサブスクリプション変更イベントを有効にします

イベント管理ポリシーでユーザー定義の構成を実行するには、次の手順を実行します：

**手順**

**ステップ 1** サブスクリプション変更イベントを構成します （1948 ページ）
**ステップ 2** サブスクリプション変更イベントのルールと条件の定義 （1949 ページ）
**ステップ 3** サブスクリプション変更イベントの構成アクション （1950 ページ）

## サブスクリプション変更イベントを構成します

サブスクリプション変更イベントを構成するには、次の手順を実行します：

**手順**

**ステップ 1** イベント イベント ポリシー構成モードを開始します。

**policy eventmgmt** *policy_eventmgmt_name*

例：

```
[smf] smf# config
[smf] smf(config)# policy eventmgmt em1
```

**ステップ 2** イベント管理ポリシーの優先順位を定義し、実行するサブスクリプション変更イベント、ルール、およびアクション名を構成します。

**priority** *priority_number* **event** *event_name* **ruledef** *ruledef_name* **actiondef** *actiondef_name*

例：

```
[smf] smf(config-eventmgmt-em1)# priority 16 event subscription change ruledef
rd-udmDataChangeNotif actiondef ad-udmDataChangeNotif
```

有効な優先範囲は 1 ～ 65535 です。 *ruledef_name* と *actiondef_name* は、いずれも 1 ～ 63 文字の英数字文字列です。

**ステップ 3** 構成を保存してコミットします。

**例**：

```
[smf] smf(config-eventmgmt-em1))# end
```

**ステップ 4** [オプション] **show running-config policy eventmgmt em1** コマンドを使用して、サブスクリプションの変更が有効かどうかを確認します。

**例**：

```
smf] smf# show running-config policy eventmgmt em1
Fri Dec  6  08:34:32.360 UTC+00:00
policy eventmgmt em1
priority 16 event subscription-change ruledef rd-udmDataChangeNotif actiondef ad-udmDataChangeNotif
exit
```

## サブスクリプション変更イベントのルールと条件の定義

サブスクリプション変更イベントのルールと条件を定義するには、次の手順に従います。

### 手順

**ステップ 1** ポリシー規則管理構成モードを開始します。

**policy rulemgmt** *policy_rulemgmt_name*

**例**：

```
[smf] smf# config
[smf] smf(config)# policy rulemgmt rm1
```

**ステップ 2** ruledef の名前を指定して、ポリシーに追加します。

**ruledef** *ruledef_name*

**例**：

```
[smf] smf(config-rulemgmt-rm1)# ruledef rd-udmDataChangeNotif
```

**ステップ 3** 任意として条件を定義します。

**例**：

```
[smf] smf(config-ruledef-rd-udmDataChangeNotif)# condition any
```

ruledef はこの条件**任意**で更新されます。

**ステップ 4** 構成を保存してコミットします。

**例**：

```
[smf] smf(config-ruledef-rm1))# end
```

**ステップ 5** [オプション]**show running-config policy rulemgmt rm1** コマンドを使用して、ルールと条件が定義されているかどうかを確認します。

**例**：

```
smf] smf# show running-config policy rulemgmt rm1
Fri Dec  6  08:34:32.360 UTC+00:00
policy rulemgmt rm1
 ruledef rd-udmDataChangeNotif
 condition any
 exit
```

## サブスクリプション変更イベントの構成アクション

アクションの構成の手順は、次のとおりです。

### 手順

**ステップ 1** アクション管理ポリシー コンフィギュレーション モードを開始します。

**policy actionmgmt** *policy_actionmgmt_name*

**例**：

```
[smf] smf# config
[smf] smf(config)# policy actionmgmt act1
```

**ステップ 2** アクション定義ポリシーを指定し、実行されるアクションの属性を定義します。

**actiondef** *actiondef_name*

**例**：

```
[smf] smf(config-actionmgmt-act1)# actiondef  ad-udmDataChangeNotif
```

**ステップ 3** アクションを実行する優先順位を指定します。その後、次のいずれかのアクションを構成します。

- 終了：セッションを終了するアクションを構成します。セッションを終了することで、UE で新しいサブスクリプションの変更を更新できます。
- 続行：セッションを続行する場合は、このアクションを構成します。

**priority** *priority_number* **action** *action_name*

**例**：

```
[smf] smf(config-actiondef-act1)# priority  12 action terminate-session
```

アクションが構成されています。このアクションを構成すると、SMF がセッションを終了するか続行するかを決定できます。

**ステップ 4** 構成を保存してコミットします。

**例**：

```
[smf] smf(config-actiondef-act1)# end
```

**ステップ 5** [オプション] **show running-config policy actionmgmt act1** コマンドを使用して、サブスクリプションの変更が有効かどうかを確認します。

**例**：

```
[smf] smf# show running-config policy actionmgmt act1
Fri Dec  6  08:34:32.360 UTC+00:00
policy actionmgmt act1
 actiondef ad-udmDataChangeNotif
  priority 1 action terminate-session
 exit
```

## サブスクリプション変更イベントの構成例

このセクションでは、適切なルールとアクションとともにイベント管理ポリシーでサブスクリプションの変更を有効にするための構成例を示します。

```
policy eventmgmt em1-SynAndSemError
      priority 16 event subscription-change ruledef rd-udmDataChangeNotif actiondef
ad-udmDataChangeNotif
exit
policy rulemgmt rm1
     ruledef rd-udmDataChangeNotif
     condition any
exit
policy actionmgmt act1
     actiondef ad-udmDataChangeNotif
     priority 1 action terminate-session
exit
```

# バルク統計情報を利用してセッションを管理する

これらのバルク統計情報は、UDM データ変更通知を使用してセッションを管理するために使用します。

- **UdmDataNotification**： このラベルはデータ変更通知メッセージを示します。
- **disk_udm_subscription_change**： このラベルは [切断統計（Disconnect Stats）] カテゴリの下に追加され、UDM データ変更通知に基づくセッション切断に関連付けられた理由を示します。

第 46 章

# UPセッションのアクティブ化と非アクティブ化のサービス要求手順


- 機能の概要と変更履歴, on page 1953
- 機能説明 （1954 ページ）
- UE 開始サービス要求の手順 （1954 ページ）
- ネットワーク開始型サービスのリクエスト手順 （1959 ページ）
- 常時接続の PDU セッションのサポート （1974 ページ）
- N3 接続再アクティブ化のための DLDR 処理 （1982 ページ）


## 機能の概要と変更履歴

### 要約データ

***Table 530:*** 要約データ

| | |
|---|---|
| 該当製品または機能エリア | SMF |
| 該当プラットフォーム | SMI |
| 機能のデフォルト設定 | N/A |
| このリリースでの関連する変更点 | N/A |
| 関連資料 | 該当なし |

# 更新履歴

***Table 531:*** マニュアルの変更履歴

| 改訂の詳細 | リリース |
|---|---|
| UPF トンネル エンド ポイント アドレスに導入された IPv6 アドレスのサポート。 | 2022.04.0 |
| DNN、ロケーション、PDU セッション タイプなどのクエリ パラメータに基づいて UPF ノードを選択できるようになりました。 | 2020.03.0 |
| 最初の導入。 | 2020.02.0 より前 |

# 機能説明

接続管理（CM）には、N1 インターフェイスを介して UE とアクセスおよびモビリティ管理機能（AMF）間の NAS シグナリング接続を確立および解放する機能が含まれます。このシグナリング接続により、UE とコア ネットワーク間の NAS シグナリング交換が可能になります。

5GS CM のステータスにより、UE と AMF との NAS シグナリング接続が決定されます。CM の状態は次のとおりです：

- **CM アイドル**：UE が CM アイドル状態のとき、UE には N1 インターフェイスを介して AMF との NAS シグナリング接続が確立されていません。この状態では、AN シグナリング接続、N2 接続、および N3 接続は存在しません。
- **CM-Connected**：UE が CM 接続状態のとき、UE には N1 インターフェイスを介して AMF との NAS シグナリング接続があります。NAS シグナリング接続では、3GPP アクセスのための、UE と NG-RAN 間の RRC 接続、および AN と AMF 間の NGAP UE 関連付けを使用します。

3GPP アクセスと非 3GPP アクセスの CM 状態は互いに独立しています。これは、両方のアクセスが同時に CM アイドル状態と CM 接続状態になる可能性があることを意味します。

SMF では、UE のアイドルからアクティブへの移行手順とアクティブからアイドルへの移行手順をサポートしています。

# UE 開始サービス要求の手順

CM-IDLE 状態の UE は、サービス要求手順を開始して、アップリンク シグナリング メッセージ、ユーザー データ、またはネットワーク ページング要求への応答として送信します。サービス要求メッセージを受信した後、AMF は認証を実行します。AMF へのシグナリング接続の確立後、UE またはネットワークは、AMF を介して、UE から SMF への PDU セッション確立などのシグナリング メッセージを送信します。

サービス要求手順は、CM-CONNECTEDのUEによって使用され、PDUセッションのユーザープレーン接続のアクティブ化を要求し、AMF からの NAS 通知メッセージに応答するために使用されます。PDU セッションのユーザー プレーン接続がアクティブになると、UE の AS レイヤが NAS レイヤにそれを示します。

# 機能説明

SMF は、PDU セッションのユーザー プレーン接続のアクティブ化および非アクティブ化をサポートしています。

アクティブ化または非アクティブ化のサービス要求手順は、CM-IDLE 状態または 5GC の状態のUEによって、AMFへのセキュアな接続の確立を要求するために使用されます。サービス要求手順は、UE が CM-IDLE および CM-CONNECTED の両方の場合に、確立された PDU セッションに対してユーザー プレーン接続をアクティブにするためにも使用されます。

**Note** 進行中のサービス要求手順がある場合、UE はサービス要求手順を開始しません。

# 機能の仕組み

ここでは、この機能の仕組みを説明します。

## PDU セッションのユーザープレーン接続の非アクティブ化

非アクティブ化手順により、論理 NG-AP シグナリング接続と関連する N3 ユーザー プレーン接続、および（R）AN RRC シグナリングとリソースが解放されます。

次の理由で AN リリースの開始がトリガされる可能性があります。

- （R）AN： 理由で開始

  例えば、O&M 介入、未指定の障害、(R)AN（例：ラジオ）リンク障害、ユーザーの不活動、システム間リダイレクト、IMS 音声用の QoS フローの確立要求、UE が生成したシグナリング接続の解放による解放、移動制限など。

- 原因がある AMF 開始

  たとえば、未指定のエラーです。

### 制限事項

ユーザー プレーンの非アクティブ化機能には、次の制限があります。

- SMF では、UE によって開始される非アクティブ化のみをサポートしています。
- ロケーションの更新はサポートされていません。

## 通話フロー

このセクションでは、PDU セッションのユーザー プレーンの非アクティブ化のコール フローについて説明します。

次の図は、ユーザー プレーンの非アクティブ化のコール フローを示しています。

***Figure 307:*** ユーザー プレーン接続コール フローの非アクティブ化

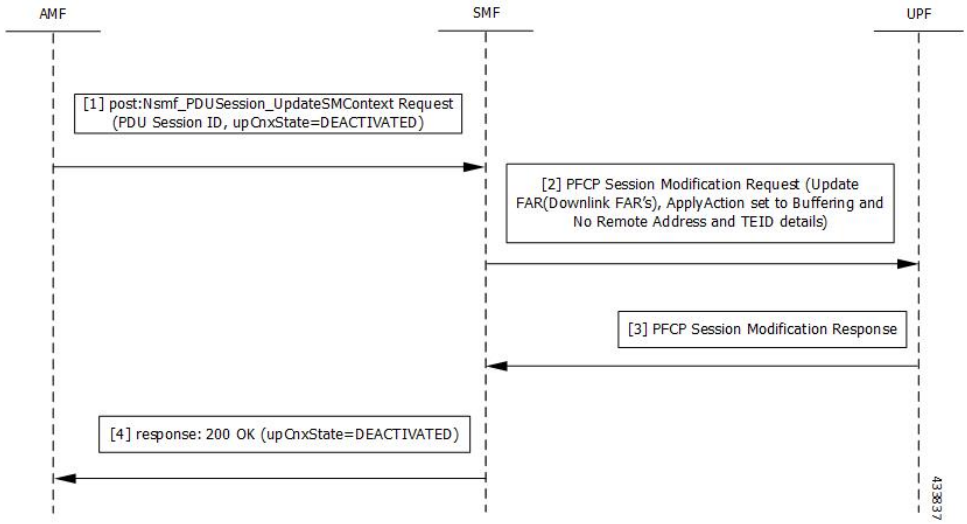



***Table 532:*** ユーザープレーン 接続コール フローの説明の非アクティブ化

| ステップ | 説明 |
|---|---|
| 1 | NF サービス コンシューマは、次の情報を含む POST 要求を送信して、PDU セッションのユーザー プレーン接続を非アクティブにするように SMF に要求します。<br>• DEACTIVATED に設定されている upCnxState 属性。<br>• ユーザーの場所とユーザーの場所のタイムスタンプ。<br>• ユーザー プレーン非アクティブ化の原因。原因は、5G-AN から受信した原因、または AMF 内部イベントによる原因を示している可能性があります。<br>• その他情報（必要であれば）。 |

| ステップ | 説明 |
|---|---|
| 2 | SMF はこのような要求を受信した後、PDU セッションの N3 トンネルを非アクティブにして解放します。SMF は、次のオプションで更新されたダウンリンク FAR を使用して、UPF に対する PFCP セッション変更手順を開始します。<br>• バッファリング アクションは、IP アドレスや GTP-U F-TEID などのリモート ノードの「転送パラメータ」の詳細なしで有効になります。<br>**Note**<br>NOCP（Notify the CP 機能）は有効になっていません。通知のサポートは、SMF ではサポートされません。 |
| 3 | SMF は、UPF ノードから正常な応答を受信した後、PDU セッションの upCnxState 属性を DEACTIVATED に設定します。 |
| 4 | SMF は、DEACTIVATED に設定された upCnxState 属性を含む AMF に対して 200 OK 応答を開始します。 |

## PDU セッションのユーザー プレーン接続のアクティブ化

サービス要求手順は、UE が CM-IDLE および CM CONNECTED 状態の場合に、確立された PDU セッションに対してユーザープレーン接続をアクティブにするために使用されます。CM IDLE 状態の UE は、サービス要求手順を開始して、アップリンク シグナリング メッセージ、ユーザー データ、またはネットワーク ページング要求への応答を送信します。

### 通話フロー

このセクションでは、PDU セッションのユーザー プレーンのアクティブ化のコール フローについて説明します。

次の図は、UE が開始したユーザープレーンのアクティブ化のコール フローを示しています。

***Figure 308:*** ユーザー プレーン接続アクティブ化コール フロー

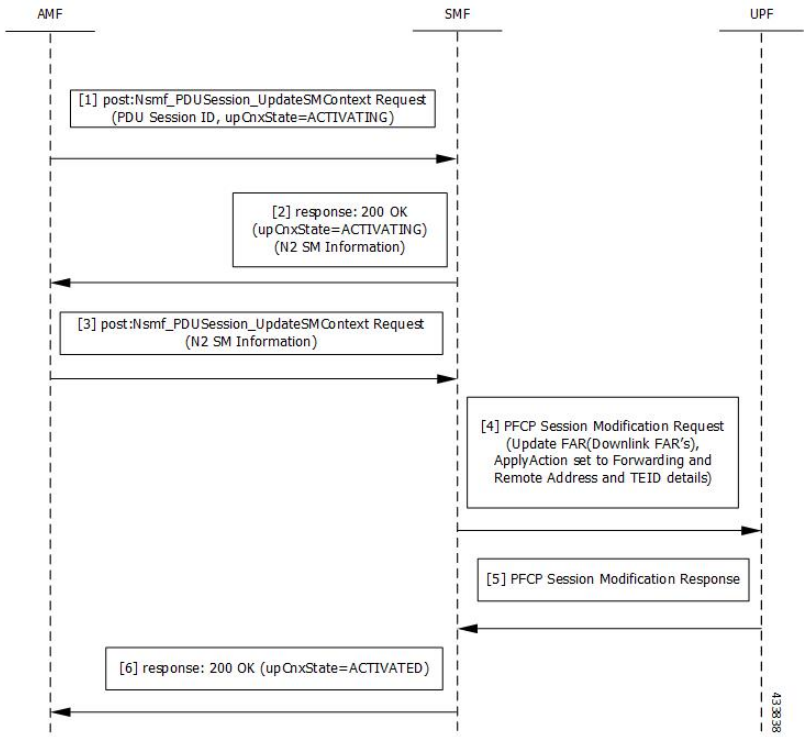



***Table 533: UE*** によって開始されたアイドルからアクティブへの移行コール フロー

| ステップ | 説明 |
|---|---|
| 1 | AMF は、次の情報を含む POST 要求を送信して、PDU セッションのユーザー プレーン接続をアクティブにするように SMF に要求します。<br>• ACTIVATING に設定されている upCnxState 属性。<br>• ユーザーの場所、ユーザーの場所のタイムスタンプ、および PDU セッションに関連付けられているアクセス タイプ（変更された場合）<br>• その他の情報（必要な場合） |

| ステップ | 説明 |
|---|---|
| 2 | 要求を受信すると、SMF は PDU セッションの N3 トンネルのアクティブ化を開始します。SMF は、次の情報を含む 200 OK 応答を返します。<br>• ACTIVATING に設定されている upCnxState 属性。<br>• 5G-AN にリソースを PDU セッションに割り当てるように要求する次の情報を含む N2 SM 情報。<br>• トランスポート層アドレス（UPF の IPv4 または IPv6 アドレス）<br>• 現在の PDU セッションの UP データのアップリンク終了ポイントのトンネル エンドポイント（つまり、アップリンク トラフィックの UPF の GTP-U F-TEID） |
| 3 | 次に、AMF は N2 SM 情報を含む POST 要求を送信して SMF を要求します。5G-AN が PDU セッションのリソースの確立に成功した場合、N2 SM 情報には次の情報が含まれます。<br>• トランスポート レイヤ アドレス<br>• 現在の PDU セッションのユーザー データのダウンリンク終端ポイントのトンネル エンドポイント。つまり、ダウンリンク トラフィックの 5G-AN の GTP-U F-TEID。 |
| 4 | SMF は、次のオプションで更新されたダウンリンク FAR を使用して、UPF に対する PFCP セッション変更手順を開始します。<br>• RAN の IPv4 または IPv6 アドレスや GTP-U F-TEID などのリモート ノード転送パラメータの詳細とともに有効になっている転送アクション。 |
| 5 | SMF は、UPF ノードから正常な応答を受信した後、PDU セッションの upCnxState 属性を ACTIVATED に設定します。 |
| 6 | SMF は、AMF に対する ACTIVATED に設定された upCnxState 属性を 200 OK 応答を開始します。 |

# ネットワーク開始型サービスのリクエスト手順

ネットワーク開始型サービス要求手順は、ピアネットワークが UE と通信する必要がある場合に使用されます（たとえば、PDU セッションに対するユーザー プレーン接続のアクティブ化で、モバイル終端ユーザー データを配信するなど）。UE が 3GPP アクセスで CM-IDLE 状態または CM-CONNECTED 状態である場合、ネットワークはネットワーク トリガー サービス要求手順を開始します。UE が CM-IDLE 状態で、非同期タイプの通信がアクティブになっていな

い場合、ネットワークは (R)AN または UE にページング要求を送信します。ページング要求は、UE で UE トリガー サービス要求手順をトリガーします。非同期タイプの通信がアクティブになっている場合、UE は CM-CONNECTED 状態を開始した時にネットワークは受信したメッセージを保存し、メッセージを（R）AN や UE に転送します（つまり、コンテキストを（R）AN や UE と同期させます）。

# 機能説明

SMF は、UE が CM アイドル状態のときに、ダウンリンクパケットを PDU セッションの UE に転送するように N3 トンネルを設定します。

N3 トンネルプロファイルは、アクティブからアイドルへの移行状態に移行する際に転送アクションルール（FAR）を定義するのに役立ちます。

N3 トンネルプロファイルの設定には、次のものが含まれます。

- コントロールプレーン通知（notify）の有効化
- UPF（バッファ UPF）でのパケット バッファリングの有効化

# 機能の仕組み

5G コアに接続されている場合、UE は RRC 非アクティブ状態でも CM 接続状態になる可能性があります。この状態は、CM アイドル状態と CM 接続状態の間です。

SMF は、UE CM と AMF の間にある場合、UE CM の状態を識別できません。SMF は、ユーザー プレーンの接続状態のみを識別します。この状態および N1 および N2 転送メッセージ応答ステータスは、ネットワークによって開始されたメッセージの SMF の動作を制御します。これらのメッセージは、シグナリングの変更、またはダウンリンク データ関連のユーザー プレーンのアクティブ化手順を示しています。

以下のコール フローでは、これらの手順の詳細について説明しています。

## コール フロー

このセクションでは、次のコールフローについて説明します。

- ネットワークによって開始されたアイドルからアクティブへの移行コール フロー, on page 1961
- ネットワーク開始型サービス要求の拒否コール フロー, on page 1964
- CM 接続状態の UE でのダウンリンク データ通知のユーザー プレーン アクティブ化コール フロー
- CM アイドル状態の UE でのダウンリンク データ通知ユーザープレーン アクティブ化コール フロー

## ネットワークによって開始されたアイドルからアクティブへの移行コール フロー

次の図に、ネットワークによって開始されるアイドルからアクティブへの遷移コールフローを示します。

***Figure 309:*** ネットワークによって開始されたアイドルからアクティブへの移行コール フロー

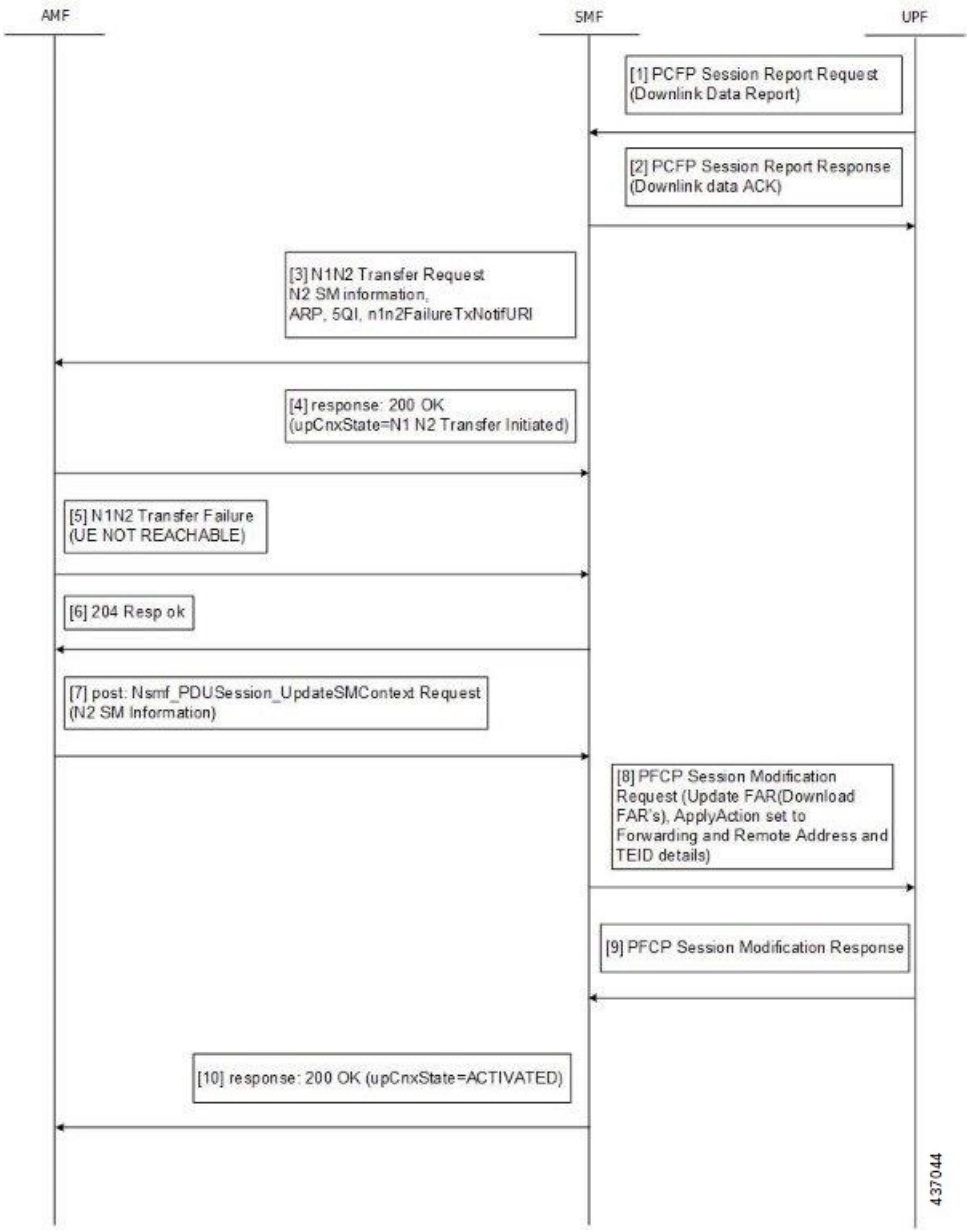


***Table 534:*** ネットワークによって開始されたアイドルからアクティブへの移行コール フロー

| ステップ | 説明 |
|---|---|
| 1 | UPF は SMF に PFCP セッションレポート要求を送信します。<br>• [レポートタイプ（Report Type）] : DLDR（ダウンリンク データ レポート）<br>• ダウンリンク データ レポート IE には、対応する PDR ID が含まれています。 |
| 2 | SMF は N4 セッション レポート レスポンスを送信します。 |
| 3 | SMFは、次の属性を使用してN1N2MessageTransferをAMFに送信します。<br>• SUPI、PDU セッション ID<br>• N2SMInformation as "ngapIeType":77 (id-PDUSessionResourceSetupListSUReq), "ngapMessageType":27 (id-PDUSessionResourceSetup)<br>• PDUSessionResourceSetupListSUReq には、次の情報が含まれます。<br>• PDU セッション ID<br>• QFI<br>• QoS プロファイル<br>• アップリンク トラフィックの UPF の GTP-U F-TEID<br>• QFI<br>• QoS プロファイル<br>• S_NSSAI<br>• ユーザー プレーン セキュリティ強化<br>• UE 整合性保護最大データ レート<br>• 原因<br>• N2 SM 情報の有効範囲<br>• ARP<br>• ページング ポリシー インジケータ<br>• 5QI<br>• N1N2TransferFailure 通知ターゲット アドレス（n1n2FailureTxfNotifURI） |

| ステップ | 説明 |
|---|---|
| 4 | SMF は、次のステータス コードを持つ N1N2 転送応答を受信します。<br>• 200/202 OK、原因は「N1_N2_TRANSFER_INITIATED」（ステップ 6 に進む）<br>• 409/504 で "UE_IN_NON_ALLOWED_AREA" を生成します（ステップ 7 に進みます） |
| 5 | AMF は、N1N2 転送失敗応答を送信します。UE が到達不能の場合は、ステップ 7 に進みます。 |
| 6 | AMFは、次の情報を含むPOST要求を送信することにより、SMF内のSMコンテキストを更新します：<br>• 5G-AN から受信した N2 SM 情報には、5G-AN が PDU セッションのリソースの確立に成功した場合、次の情報が含まれます。<br>• トランスポート層アドレス（UPF の IPv4 または IPv6 アドレス）<br>• 現在の PDU セッションのユーザー データのダウンリンク ターミネーション ポイントのトンネルエンドポイント（つまり、ダウンリンクトラフィックの 5G-AN の GTP-U F-TEID） |

| ステップ | 説明 |
|---|---|
| 7 | SMF は、次のオプションで更新されたダウンリンク FAR を使用して、UPF に対する PFCP セッション変更手順を開始します。<br>• N2 転送が成功した場合、転送アクションは、RAN の IPv4 または IPv6 アドレスや GTP-U F-TEID などのリモート ノード転送パラメータの詳細とともに有効になります。<br>• 転送失敗の原因が ATTEMPTING_TO_REACH_UE または UE_IN_NON_ALLOWED_AREA である場合：<br>• [FARの更新（Update FAR）]>[アクションの適用（Apply Action）]>[NOCP：1]<br>• [FARの更新（Update FAR）]>[アクションの適用（Apply Action）]>[DROP]を選択します。<br>• PFCPSMReq フラグ > DROBU：1<br>• 転送の失敗の原因が UE_NOT_REACHABLE である場合：<br>• [FARの更新（Update FAR）]>[アクションの適用（Apply Action）]>[NOCP：0（NOCP: 0）]<br>• [FARの更新（Update FAR）]>[アクションの適用（Apply Action）]>[DROP：1]<br>• PFCPSMReq フラグ > DROBU：1 |
| 8 | SMF は、UPF ノードから正常な応答を受信した後、PDU セッションの upCnxState 属性を ACTIVATED に設定します。 |
| 9 | SMF は、AMF に対して ACTIVATED に設定された upCnxState 属性を含む 200 OK 応答を開始します（ステップ6が完了し、ステップ8からの応答を受信した場合のみ）。 |

## ネットワーク開始型サービス要求の拒否コール フロー

ネットワークによって開始されたサービス要求中、SMF は、3GPP TS 23.502、セクション 4.2.3.3 に記載されているように、AMF からの N1N2 応答メッセージの一時的な拒否を処理します。

図 *310 :* ネットワーク トリガーのサービス要求の一時的な拒否コール フロー：*1*

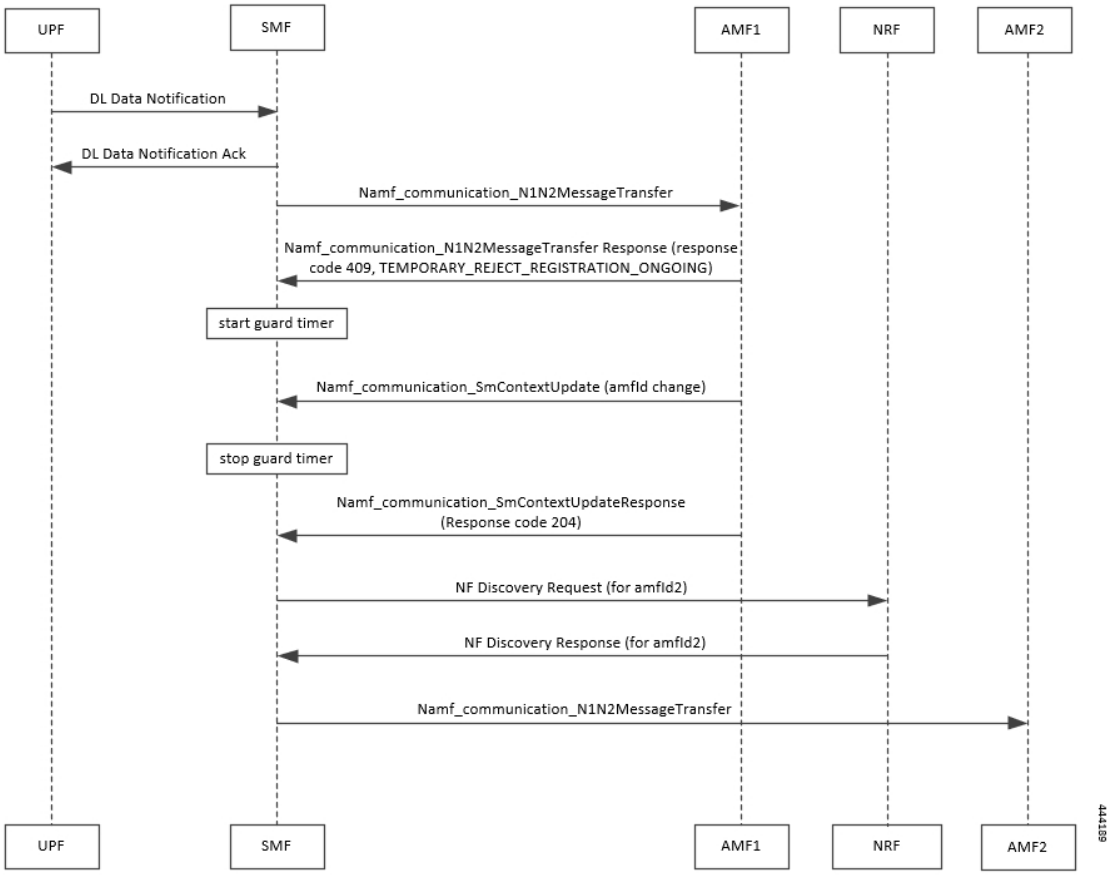



表 *535 :* ネットワーク トリガーのサービス要求における一時的な拒否コール フローの説明 - *1*

| ステップ | 説明 |
|---|---|
| 1 | UP IDLE セッション状態のサービス要求のトリガーを受信すると、SMF は、アイドル モード終了手順の一部として、AMF 向けに N1N2 メッセージを開始します。 |
| 2 | 新しい AMF を使用した UE 登録手順が進行中の場合、AMF は応答コード 409 で N1N2 メッセージの一時的な拒否で応答し、原因は TEMPORARY_REJECT_REGISTRATION_ONGING または TEMPORARY_REJECT_HANDOVER_ONGING SMF です。 |
| 3 | 応答を受信すると、SMF はローカルに構成された 2 秒のガードタイマーを開始します。 |
| 4 | ガード タイマーの実行中、SMF は AMF ID の変更を伴う SM コンテキスト更新または引き継ぎのための SM コンテキスト更新のいずれかを待ちます。 |

| ステップ | 説明 |
|---|---|
| 5 | AMF ID の変更を含む SM コンテキスト更新を受信すると、SMF は次の動作を行います。<br>**1.** ガイド タイマーを停止します。<br>**2.** 古い AMF の検出情報への参照を削除します。<br>**3.** 新しい UE ロケーション情報、PLMN 情報、AMF 情報を保存します。<br>**4.** コンテンツなしで SM コンテキスト更新の応答の成功を送信します。<br>**5.** 新しい AMF への N1N2 メッセージ転送を再開します。これには、NF検出とその後の新しいAMFへの送信が含まれます。 |
| 6 | N2 ハンドオーバーの SM コンテキスト更新を受信すると、SMF は次のように動作します。<br>**1.** ハンドオーバー手順を開始します。<br>**2.** アイドル モード終了手順を中断し、ガード タイマーを停止します。<br>**3.** 引き継ぎ手順完了の一環として、古い AMF の詳細を削除し、新しい AMF 情報を保存します。<br>**4.** 移行手順の完了後に、アイドル モードの終了手順を再開します。<br>**5.** 必要に応じて、新しいAMFへのN1N2メッセージ転送を再開します。これには、NF検出とその後の新しいAMFへの送信が含まれます。 |

図 *311 :* ネットワーク トリガーのサービス要求の一時的な拒否コールフロー：*2*

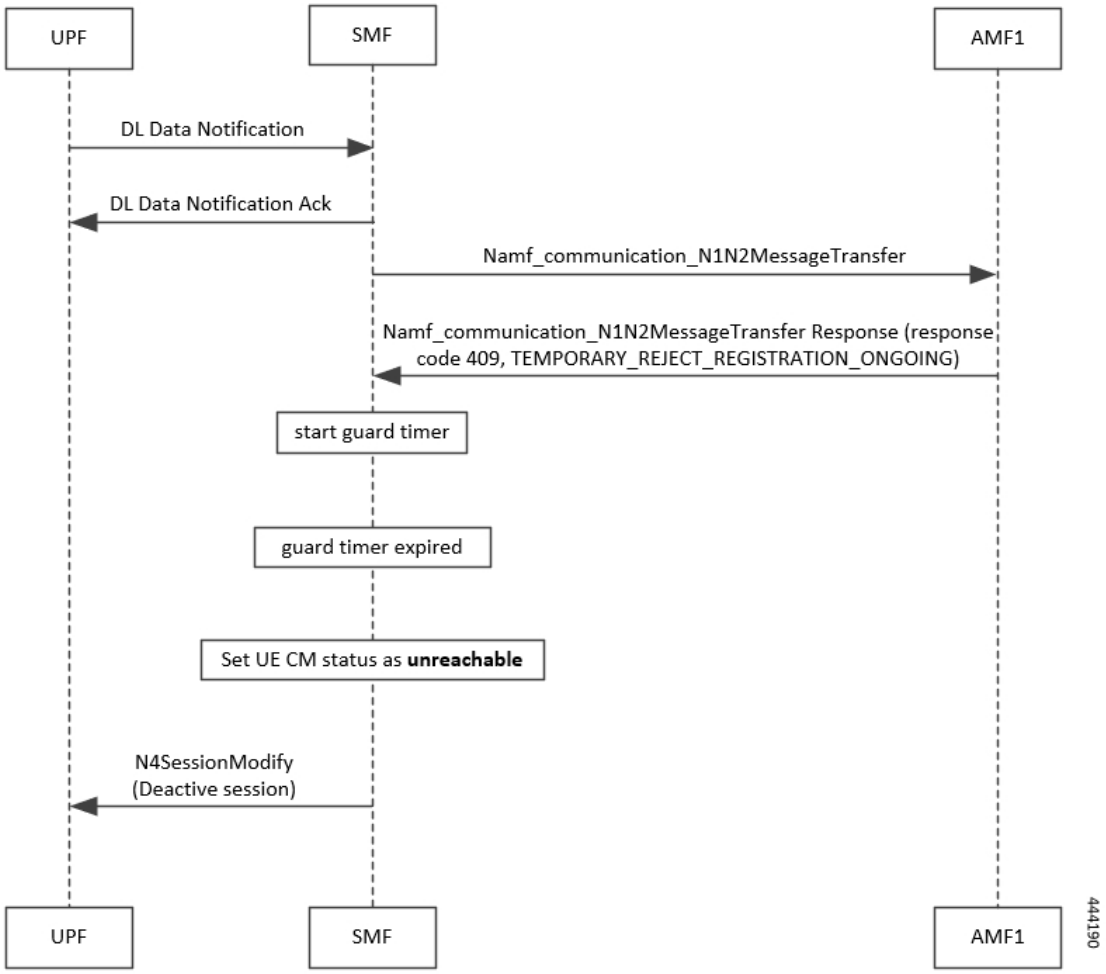



表 *536 :* ネットワーク トリガーのサービス要求の一時的な拒否コール フローの説明（*2*）

| ステップ | 説明 |
|---|---|
| 1 | UP IDLE セッション状態のサービス要求のトリガーを受信すると、SMF は、アイドル モード終了手順の一部として、AMF 向けに N1N2 メッセージを開始します。 |
| 2 | 新しい AMF を使用した UE 登録手順が進行中の場合、AMF は応答コード 409 で N1N2 メッセージの一時的な拒否で応答し、原因は TEMPORARY_REJECT_REGISTRATION_ONGING または TEMPORARY_REJECT_HANDOVER_ONGING SMF です。 |
| 3 | 応答を受信すると、SMF はローカルに構成された 2 秒のガードタイマーを開始します。 |

| ステップ | 説明 |
|---|---|
| 4 | ガード タイマーが期限切れになると、SMF は次の処理を行います：<br>**1.** UE CM ステータスを *NotReachable*に設定します。<br>**2.** UP セッション状態を非アクティブにします。 |

## CM 接続状態の UE でのダウンリンク データ通知のユーザー プレーン アクティブ化コール フロー

このセクションでは、UE が CM 接続状態にある場合のダウンリンク データの通知のためのユーザー プレーンのアクティブ化手順について説明します。

次の図は、UE が CM 接続状態の場合のダウンリンク データ通知のユーザー プレーンの有効化コール フローを示しています。

***Figure 312: CM** 接続状態の **UE** でのダウンリンク データ通知のユーザー プレーン アクティブ化コール フロー*

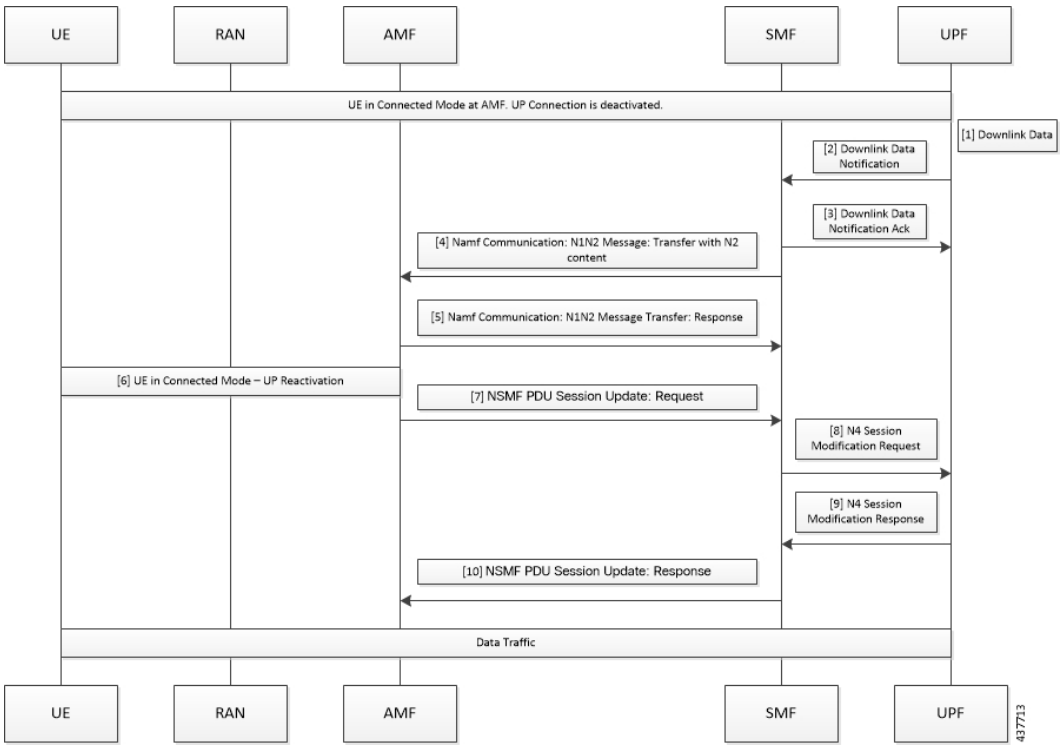



***Table 537: CM** 接続状態の **UE** のダウンリンク データ通知のユーザー プレーン アクティブ化コール フローの説明*

| ステップ | 説明 |
|---|---|
| 1 | UPF が PDU セッションのダウンリンク データを受信したときに、AN トンネル情報が PDU セッションの UPF に保存されていない場合、UPF はダウンリンク データをバッファリングします。バッファリングは、SMF からの指示に基づいて行われます。 |

| ステップ | 説明 |
|---|---|
| 2 | UPF は SMF にデータ通知を送信します。この通知には、N4 セッション ID、DL データ パケットの QoS フローを識別する情報、および DSCP の詳細が含まれます。 |
| 3 | SMF は、確認応答データ通知を UPF に送信します。 |
| 4 | SMF は、AMF への NAMF 通信 N1 および N2 メッセージ転送を開始します。<br>このメッセージ転送には、次の詳細が含まれます：<br>• PDU セッション ID<br>• N2 SM 情報（QFI、QoS プロファイル）<br>• CN N3 トンネル情報<br>• S_NSSAI<br>• ARP<br>• ページング ポリシー インジケータ<br>• 5QI<br>• N1 および N2 転送失敗通知ターゲット アドレス<br>• PDU セッション リソースのセットアップ要求 IE |
| 5 | UE が CM-Connected 状態であるため、AMF は N1 および N2 転送応答を開始します。この応答には、「200 OK」のステータス コードと「N1_N2_TRANSFER_INITIATED」の原因が含まれています。 |
| 6 | ユーザープレーンの再アクティブ化の手順が開始されます。再アクティブ化の手順では、無線リソースをセットアップし、ユーザープレーンをアクティブにしてN3トンネルを確立します。 |
| 7 | AMF は、NSMF PDU セッション更新 SM コンテキスト要求を SMF に送信します。この要求には、N2 インターフェイスの SM 情報が含まれています。ユーザー プレーンの接続状態はアクティブです。 |
| 8 | SMF は、セッションをアクティブ化し、AN トンネル情報（IP および TEID）を更新するために、N4 変更手順を UPF に送信します。セッションは、バッファの削除アクションと転送の設定アクションを実行することでアクティブ化されます。 |
| 9 | UPF はセッションを変更し、変更の確認応答を SMF に送信します。 |
| 10 | SMF は、ユーザープレーンの接続状態をアクティブとして、NSMF PDU セッション更新 SM コンテキスト要求の「200 OK」ステータス コードで AMF に応答します。 |

**注**：

次の N1 および N2 応答エラーケースが処理されます。

- 404 Context Not Found ステータスの場合は、PDU セッションが解放されます。
- 「UE_IN_NON_ALLOWED_AREA」および「NOT_REACHABLE」の原因を持つ 504 または 403 のステータスでは、バッファに格納されたパケットをドロップし、ダウンリンク データの CP 通知を除外するように N4 変更要求が送信されます。
- N1 および N2 の転送通知が失敗した場合は、N4 変更要求が送信され、バッファされたパケットがドロップされ、ダウンリンク データの CP 通知が除外されます。
- Retry After タイマーの値を持つ 409 ステータス コードの場合、N1 と N2 の転送はタイムアウト値の後に再開始されます。
- 原因が「HIGHER_PRIORITY_REQUEST_ONGOING」の 409 ステータス コードの場合、優先順位の低い N1 および N2 転送は許可されません。優先順位の高い転送のみが AMF に通信されます。

## CM アイドル状態の UE でのダウンリンク データ通知ユーザー プレーン アクティブ化コール フロー

このセクションでは、UE が CM アイドル状態にある場合のダウンリンク データの通知のためのユーザー プレーンのアクティブ化手順について説明します。

次の図は、UE が CM アイドル状態の場合のダウンリンク データ通知のユーザー プレーンの有効化コール フローを示しています。

*Figure 313: CM アイドル状態の UE でのダウンリンク データ通知ユーザー プレーン アクティブ化コール フロー*

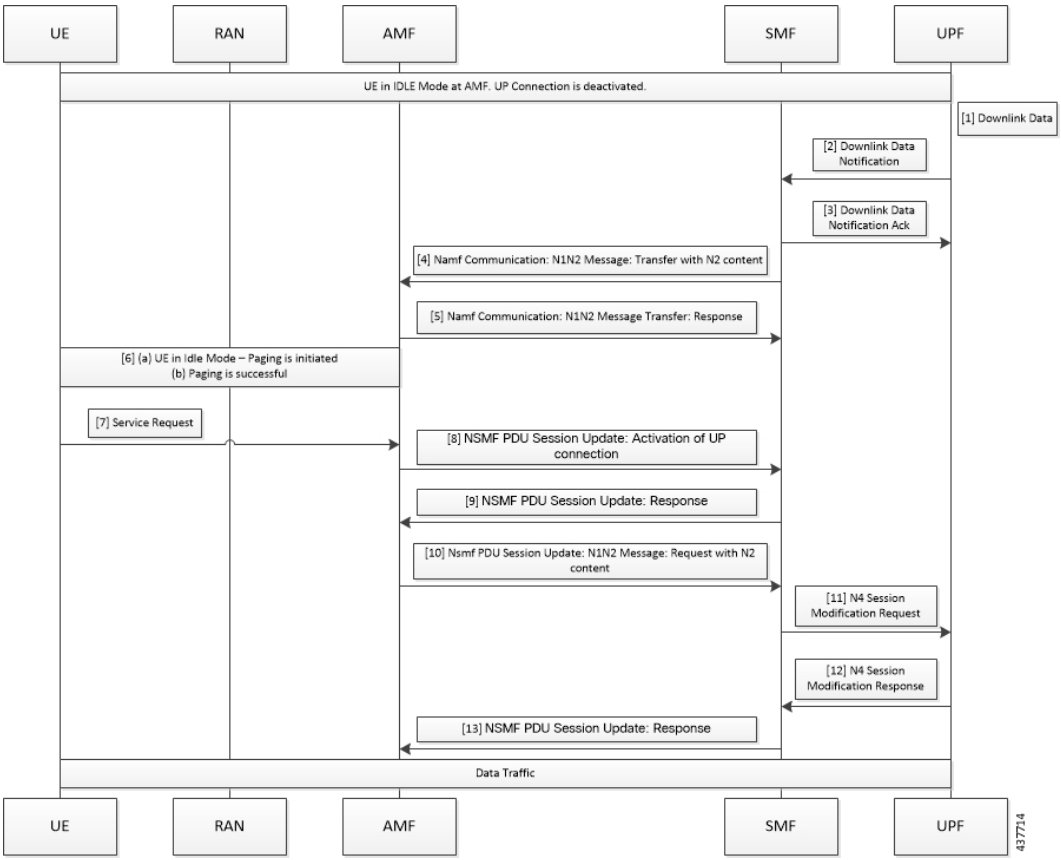



*Table 538: CM アイドル状態の UE でのダウンリンク データ通知ユーザー プレーン アクティブ化コール フローの説明*

| ステップ | 説明 |
|---|---|
| 1 | UPF が PDU セッションのダウンリンク データを受信したときに、AN トンネル情報が PDU セッションの UPF に保存されていない場合、SMF からの指示に基づき、UPF はダウンリンク データをバッファリングします。 |
| 2 | UPF は SMF にデータ通知を送信します。この通知には、N4 セッション ID、DL データ パケットの QoS フローを識別する情報、および DSCP の詳細が含まれます。 |
| 3 | SMF は、確認応答データ通知を UPF に送信します。 |

| ステップ | 説明 |
|---|---|
| 4 | SMF は、AMF への NAMF 通信 N1 および N2 メッセージ転送を開始します。このメッセージ転送には、次の詳細が含まれます：<br>• PDU セッション ID<br>• N2 SM 情報（QFI、QoS プロファイル）<br>• CN N3 トンネル情報<br>• S_NSSAI<br>• ARP<br>• ページング ポリシー インジケータ<br>• 5QI<br>• N1 および N2 転送失敗通知ターゲット アドレス |
| 5 | UE が CM-Connected 状態であるため、AMF は N1 および N2 転送応答を開始します。この応答には、「202 Accepted」のステータス コードおよび「ATTEMPTING_TO_REACH_UE」の原因が含まれます。 |
| 6 | AMF は、UE に対してページング手順をトリガします。 |
| 7 | UE は、ページング要求を受信し、要求されたサービスを開始してセッションをアクティブにします。 |
| 8 | AMF は、ユーザー プレーンの接続状態を Activating に構成した状態で、SMF に対して NSMF PDU セッション更新 SM コンテキスト要求を送信します。 |
| 9 | SMF は、NSMF PDU セッション更新 SM コンテキスト要求のステータス コード「200 OK」で AMF に応答します。この要求には、詳細が含まれています。<br>• N2 SM 情報（QFI、QoS プロファイル）<br>• CN N3 トンネル情報<br>• S_NSSAI<br>• ARP<br>• ページング ポリシー インジケータ<br>• 5QI<br>• N1 および N2 転送失敗通知ターゲット アドレス<br>• PDU セッション リソースのセットアップ要求 IE |

| ステップ | 説明 |
|---|---|
| 10 | AMF は、NSMF PDU セッション更新 SM コンテキスト要求を SMF に送信します。この要求には、N2 インターフェイスの SM 情報を含みます。ユーザー プレーンの接続状態はアクティブです。 |
| 11 | SMF は、セッションをアクティブ化し、AN トンネル情報（IP および TEID）を更新するために、N4 変更手順を UPF に開始します。セッションは、バッファの削除アクションと転送の設定アクションを実行することでアクティブ化されます。 |
| 12 | UPF はセッションを変更し、変更の確認応答を SMF に送信します。 |
| 13 | SMF は、ユーザー プレーンの接続状態をアクティブとして、NSMF PDU セッション更新 SM コンテキスト要求の「200 OK」ステータス コードで AMF に応答します。 |

## 標準準拠

ネットワーク開始型サービス要求機能は、3GPP TS 23.502、V 15.6.0（2019-10）に準拠しています。

## 制限事項

SMF は、ロケーションの更新とアクセス タイプの変更をサポートしていません。

# N3 トンネル プロファイルの構成

UPF がダウンリンクデータを受信し、N3 トンネルが使用できない場合、SMF に対するバッファリングまたは通知アクションに N3 トンネル プロファイルを使用します。N3 トンネル プロファイルを構成するには、次の構成例を使用します：

```
config
   profile n3-tunnel n3_profile_name
      buffer upf
      notify
      end
```

注：

- **profile n3-tunnel** *n3_profile_name*：N3 トンネル プロファイル名を指定します。*n3_profile_name* は 文字列である必要があります。
- **buffer** *upf*：ダウンリンク データのバッファリングを構成します。
- **notify**：UPF からのダウンリンク データ通知を有効にします。

# 常時接続の PDU セッションのサポート

## 機能説明

常時プロトコル データ ユニット（PDU）セッションとは、ユーザー プレーンが常にアクティブであることを意味します。IPマルチメディアサブシステム（IMS）などのアプリケーションには、常時接続の PDU セッションが必要です。

UE は、上位レイヤの要求表示に基づいて、常時接続の PDU セッションとして PDU セッションの確立を要求します。PDU セッションを常時接続の PDU セッションとして確立するかどうかを決定するのはネットワークです。

## 機能の仕組み

### コール フロー

このセクションでは、Always-On PDU セッション サポートのコール フローについて説明します。

#### PDU セッション確立コール フロー

このセクションでは、セッション作成要求に常時PDUセッションの開始の要求が含まれる PDU セッションの確立手順について説明します。

次の図に、PDU セッション確立のコール フローを示します。

図 *314 : PDU* セッション確立コール フロー

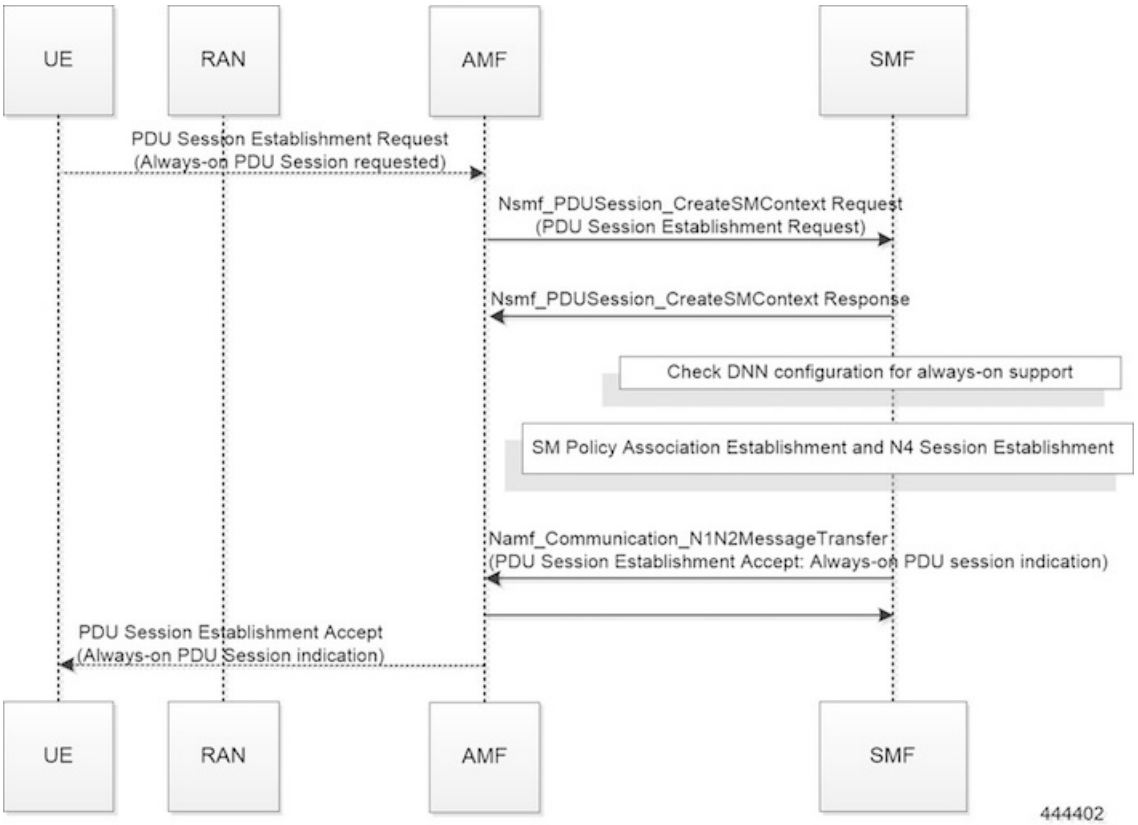



表 *539 : PDU* セッション確立コール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | UE が常時接続の PDU セッションの確立を要求する場合、UE は PDU セッション確立要求メッセージに「常時接続の PDU セッションが要求されました」という IE を含めます。 |
| 2 | SMF は DNN プロファイルをチェックして、常時接続のサポートが有効になっているかどうかを判断します。 |
| 3 | SMF は、次のいずれかに該当する場合、PDU セッション確立承認メッセージに「常時接続の PDU セッション表示」の IE を含めます。<br>• DNN プロファイルで常時接続の構成が有効になっている場合、「常時接続の PDU セッション表示」は「有効」という値と共に送信されます。<br>• 「常時接続の PDU セッション要求」IE が受信され、設定が無効になっている場合、「常時接続の PDU セッション表示」は「無効」の値と共に送信されます。 |

| ステップ | 説明 |
|---|---|
| 4 | SMF には、次の両方の条件が満たされる場合にのみ、「常時接続の PDU セッション表示」が含まれません。<br>• UE が「常時オン PDU セッション要求」 IE を送信しなかった場合。<br>• DNN プロファイルで常時オンの構成が無効になっている場合。 |

## UE 要求の PDU セッション変更のコール フロー

ここでは、常時接続 PDU セッション通知が送信される、UE 要求による PDU セッションの変更手順について説明します。

次の図は、UE 要求 PDU セッション変更のコール フローを示しています。

**図 *315 : UE* 要求の *PDU* セッション変更のコール フロー**

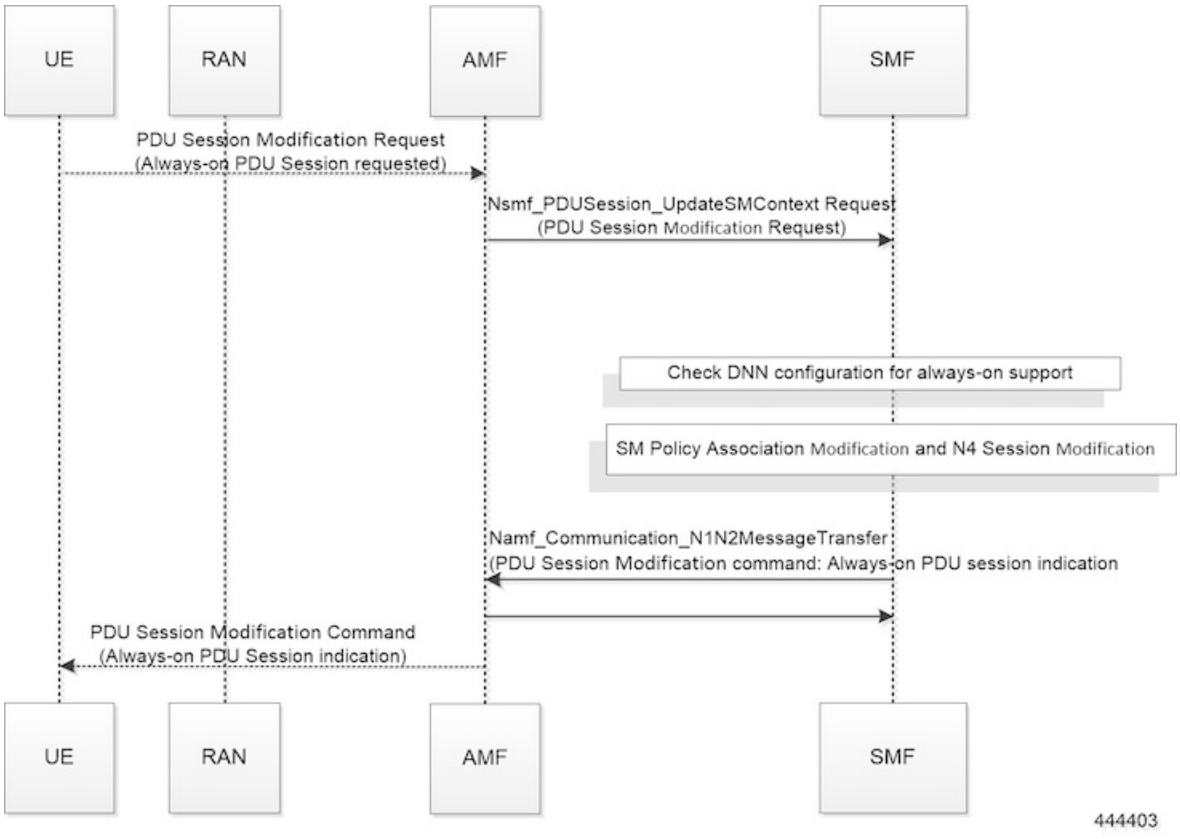


表 *540 : UE* 要求の *PDU* セッション変更のコール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | UE は、PDU セッション変更要求メッセージで「常時オン PDU セッション要求」という IE を送信します。 |
| 2 | SMF は DNN プロファイルをチェックして、常時接続のサポートが有効になっているかどうかを判断します。 |
| 3 | SMF は、次のいずれかに該当する場合、PDU セッション変更コマンドに「常時オン PDU セッションの表示」を含めます。<br>• DNN プロファイルで常時接続の設定が有効になっている場合、「常時オン PDU セッションの表示」は「有効」という値と共に送信されます。<br>• 「常時オン PDU セッション要求」IE が受信され、設定が無効になっている場合、「常時オン PDU セッションの表示」は「無効」の値と共に送信されます。 |
| 4 | SMF には、次の両方の条件が満たされる場合にのみ、「常時オン PDU セッションの表示」が含まれません。<br>• UE が「常時オン PDU セッション要求」 IE を送信しなかった場合。<br>• DNN プロファイルで常時オンの構成が無効になっている場合。<br>（注）<br>*3GPP TS 23502* に記載されているように、EPS で確立された PDU セッションの場合、UE が EPS から 5GS に初めて移動する際、 PDU セッションを「常にオン」の PDU セッションに変更する場合、UE は PDU セッション変更要求メッセージに「常時オン PDU セッション要求」という表示を含めます。 |

## ネットワーク要求による PDU セッション変更のコール フロー

ここでは、常時接続 PDU セッション通知が送信される、ネットワーク要求による PDU セッションの変更手順について説明します。

次の図は、ネットワーク要求 PDU セッション変更のコール フローを示しています。

図 *316 :* ネットワーク要求による *PDU* セッション変更のコール フロー

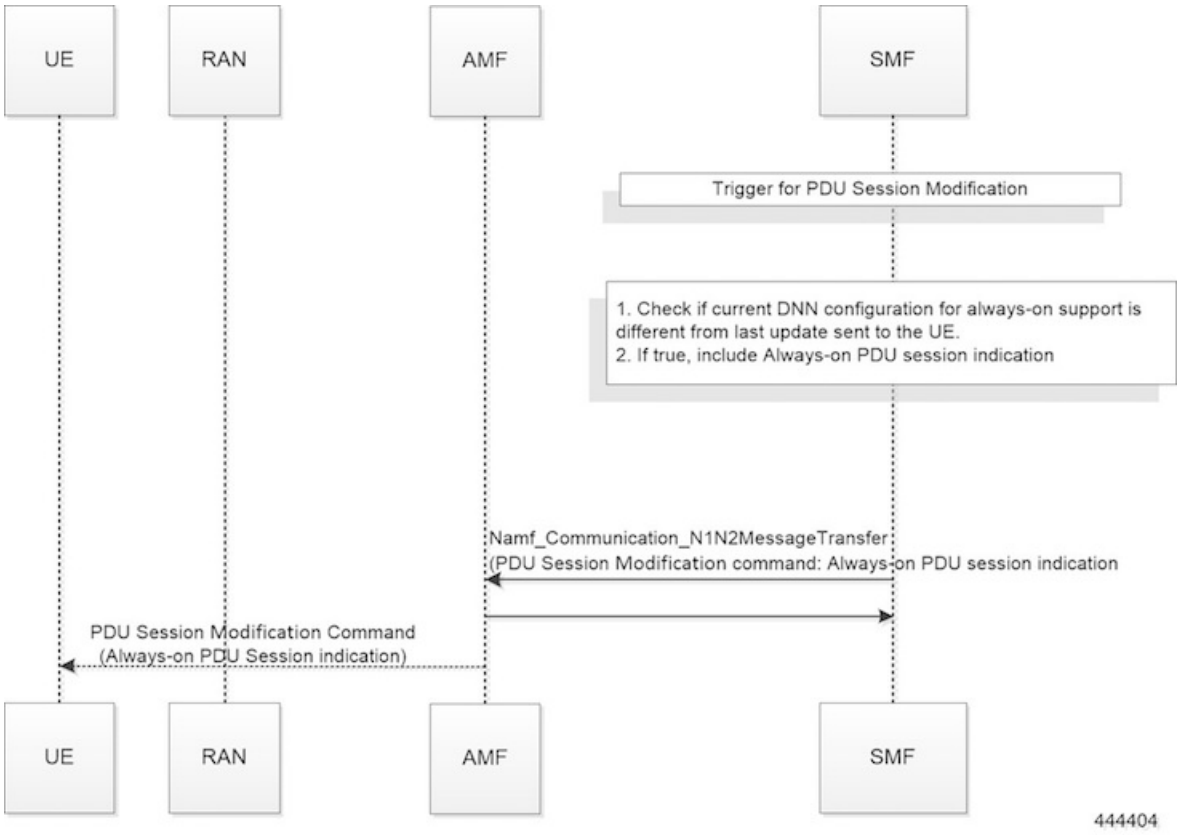



表 *541 :* ネットワーク要求の *PDU* セッション変更のコール フローの説明

| ステップ | 説明 |
|---|---|
| 1 | SMF は、PCF、UDM、または RAN によって開始された手順により、PDU のセッション変更をトリガーすることを決定しました。 |
| 2 | SMF は DNN プロファイルをチェックして、常時接続のサポートが有効になっているかどうかを判断します。 |
| 3 | SMF は、常時接続の現在の DNN 設定が UE に送信された最後の通知と異なるかどうかを判断します。異なる場合、SMF は、PDU セッション変更コマンド メッセージに「常時オン PDU セッションの表示」IE を含めます。 |

# 常時接続の PDU セッション サポートの構成

常時接続の PDU セッション サポートのパラメータを構成するには、次の構成例を使用します：

```
config
  profile dnn dnnprofile_name
    always-on { false | true }
    end
```

注：

- **always-on { false | true }**：常時接続の PDU セッションのサポートを構成します。
  - **false**：常時接続の PDU セッションのサポートを無効にします。
  - **true**：常時接続の PDU セッションのサポートを有効にします。
- PDU セッション確立承認メッセージで送信される「Always-on PDU Session Indication」IE の値は、DNN プロファイルの常時接続の構成に基づいています。つまり、DNN プロファイルの下で常時接続の構成が有効になっている場合、「Always-on PDU Session Indication」IE は「有効」という値で送信されます。

## 常時接続の PDU セッションサポートの確認

常時接続の PDU セッションのサポートを確認するには、 **show subscriber supi** *supi_id* **nf-service smf** CLI コマンドを使用します。

常時接続の PDU セッションサポートの show 出力に、次のいずれかのオプションが表示されます。

- “alwaysOn”: “UE Requested”
- “alwaysOn”: “Enabled”
- “alwaysOn”: “UE Requested & Enabled”

次に、 コマンドの出力例を示します。

```
show subscriber supi imsi-123456789012345 nf-service smf
subscriber-details
{
  "status": true,
  "genericInfo": {
    "supi": "imsi-123456789012345",
    "pei": "imei-123456786666660",
    "pduSessionId": 5,
    "pduSesstype": "Ipv4PduSession",
   "accessType": "ACCESS_5G",
    "dnn": "intershat",
    "plmnId": {
      "mcc": "123",
      "mnc": "456"
    },
    "sScMode": 1,
    "uetimeZone": "UTC+12:00",
    "allocatedIp": "209.165.201.4",
    "nrLocation": {
      "ncgi": {
        "mcc": "123",
        "mnc": "456",
        "nrCellId": "123456789"
      },
```

```
    "tai": {
      "mcc": "123",
      "mnc": "456",
      "tac": "1820"
    }
  }
  "alwaysOn":  "UE Requested"
},
"accessSubData": {
  "amfID": "AFbe08",
  "amfPlmnId": {
    "mcc": "123",
    "mnc": "456"
  },
  "ueCmStatus": "UeCMConnected",
  "amfNrfID": "76517361-338e-4d77-bc76-713a79779574"
},
"policySubData": {
  "TotalDynamicRules": 1,
  "TotalFlowCount": 1,
  "TotalNonGBRFlows": 1,
  "pccRuleList": [
    {
      "pccRuleId": "defaultrule",
      "qfi": 1,
      "mbrDl": 125000000,
      "mbrUl": 100000000,
      "flowInformation": [
        {
          "flowDirection": 3,
          "flowDescription": "permit out ip from any to any"
        }
      ]
    }
  ],
  "qosFlow": [
    {
      "qfi": 1,
      "GBRFlow": "False",
      "bindingParameters": {
        "x5Qi": 5,
        "arp": {
          "preemptCap": 1,
          "preemptVuln": 1,
          "priorityLevel": 15
        },
        "priorityLevel": 1
      },
      "AggregatedULMFbr": 100000000,
      "AggregatedDLMFbr": 125000000,
      "pccRuleList": "defaultrule"
    }
  ]
},
"chargingData": {},
"upfServData": {
  "numberOfTunnels": 1,
  "smfSeid": 21790984727,
  "UPState": "Activated",
  "mapping": {
    "tunnelMapping": [
      {
        "TunnelID": 1,
        "tunnelName": "gnbTunnel"
```

```
            }
          ]
        }
      }
    }
}
```

# 常時接続の PDU セッション OAM のサポート

ここでは、この機能の操作、管理、およびメンテナンスに関して説明します。

## バルク統計サポート

常時接続 PDU セッション機能では、次のバルク統計がサポートされています。

**表 *542*：常時接続 *PDU* セッションのバルク統計**

| バルク統計 | 説明 |
|---|---|
| always-on-pdu | 常時接続の PDU セッションの数を追跡します。 |
| Always-on-pdu-requested | 常時接続の PDU セッションを要求します。 |
| always-on-pdu-accepted | 常時接続の PDU セッション要求を受け入れます。 |
| Always-on-pdu-rejected | 常時接続の PDU セッション要求を拒否します。 |
| pdusetup_req_alwayson_requested | 「常時接続 PDU セッション要求済み」で受信したセッション確立要求メッセージの数。 |
| pdusetup_acc_alwayson_allowed | [常時接続 PDU セッションの通知（Always-On PDU Session Indication）] を有効にして送信したセッション確立承認メッセージの数。 |
| pdusetup_acc_alwayson_not_allowed | [常時接続 PDU セッションの通知（Always-On PDU Session Indication）] を無効にして送信したセッション確立承認メッセージの数。 |
| pdumod_req_alwayson_requested | 「常時接続 PDU セッション要求済み」で受信したセッション変更要求メッセージの数。 |
| pdumod_cmd_alwayson_allowed | [常時接続 PDU セッション指示（Always-On PDU Session Indication）] を有効にして送信したセッション変更コマンド メッセージの数。 |
| pdumod_cmd_alwayson_not_allowed | [常時接続 PDU セッション指示（Always-On PDU Session Indication）] を無効にして送信したセッション変更コマンドメッセージの数。 |

| | |
|---|---|
| pdumod_cmd_nw_init_alwayson_allowed | [常時接続 PDU セッション指示（Always-On PDU Session Indication）] を有効にして送信した、ネットワークによって開始されたセッション変更コマンドメッセージの数。 |
| smf_session_counters | アクティブな常時接続 PDU セッションの数を示すゲージ。 |

# N3 接続再アクティブ化のための DLDR 処理

## 機能説明

UPF がダウンリンク データ要求（DLDR）を受信したときに、SMF が N11 インターフェイスで N1N2 セットアップ要求をトリガーしない場合、SMF と UPF の upContext の状態の違いにより、UPF は DLDR をトリガーします。N3 が非アクティブ状態の場合、UPF はセッション レポート要求を SMF に送信するために使用されます。この機能により、DLDR が N3 をアクティブ化した状態で受信されると、SMF は N3 を再アクティブ化します。

## 機能の仕組み

**reactivate-n3-on-dupl-activation-dldr** CLI コマンドが SMF でサポートされている機能に追加され、DLDR が N3 でアクティブ化された状態で受信されたときに N3 を再アクティブ化します。この CLI が有効になり、ACTIVATED 状態の DLDR を受信すると、SMF は upState を DEACTIVATED に変更し、N3 接続を再度アクティブにします。

## N3 接続再アクティブ化の構成

N3 接続の再アクティブ化を構成するには、次の構成例を使用します。

```
config
  profile smf profile_name instances instance-id supported-features [
reactivate-n3-on-dupl-activation-dldr ]
     [ vsmf dtssa acscr]
```

注：

- **supported-features [ reactivate-n3-on-dupl-activation-dldr ]**：受信した DLDR がサポートされている機能で N3 でアクティブ化された状態になった場合に、N3 を再アクティブ化します。

第 47 章

# UPF パスの管理と復元


- 機能の概要と変更履歴, on page 1983
- 機能説明 （1984 ページ）
- 機能の仕組み （1984 ページ）
- UPF パス管理および復元の構成サポート （1985 ページ）
- OAM サポート （1990 ページ）


## 機能の概要と変更履歴

### 要約データ

***Table 543:*** 要約データ

| | |
|---|---|
| 該当製品または機能エリア | SMF |
| 該当プラットフォーム | SMI |
| 機能のデフォルト設定 | 無効：設定が必要 |
| このリリースでの関連する変更点 | N/A |
| 関連資料 | 該当なし |

### 更新履歴

***Table 544:*** マニュアルの変更履歴

| 改訂の詳細 | リリース |
|---|---|
| Sx でのハートビート | 2023.01.0 |
| 最初の導入。 | 2020.02.0 |

# 機能説明

ハートビートは、応答性の観点から UPF ノードのステータスをモニタします。SMF と UPF の間で要求と応答の双方向フローを開始します。次のアクションがあります。

- SMF は、登録済みの UPF ノードにハートビート要求の形式で定期的に信号を送信します。このアクションは、SMF がアクティブかどうかを判断するのに役立ちます。
- 再送信の試行が終了した後も SMF が UPF からの応答を受信しない場合、SMF は障害が発生したインスタンスを認識します。これにより、UPF ノードにマッピングされたサブスクライバがパージされます。

以下を制御できます。

- SMF が UPF に送信するハートビート要求の数。
- 連続した要求の間隔。
- SMF が応答を待機する期間。

ハートビート機能は、Diameter インターフェイスを使用した SMF にも適用できます。

# 標準準拠

SMF と UPF 間のハートビート伝送は、次の標準に準拠しています：

- *3GP TS 23.527*
- *3GPP TS 23.007*、バージョン *15.4.0*

# 機能の仕組み

ハートビート機能は、インターフェイス レベル、UPF プロファイル グループ レベル、またはその両方で構成できます。インターフェイスレベルの構成は必須です。インターフェイスレベルの構成が使用できない場合、ハートビートパラメータはデフォルト値で構成されます。プロファイルレベルの構成は、インターフェイスレベルの構成を上書きします。

ハートビート機能は、ノード マネージャの高可用性を実現するためにも拡張されます。

### インターフェイスおよびプロファイルレベルのハートビート

ハートビート メッセージを使用して UPF パス障害を検出するための SMF-UPF の相互作用には、次の手順が含まれます。

1. SMF は、構成されたスケジュールに基づいて、検出された UPF インスタンスまたはプロファイル グループにハートビート要求メッセージを送信します。

2. UPFインスタンスまたはプロファイルが動作している場合、スイッチが動作していることを示すハートビート応答を SMF に送信します。UPF がハートビート応答を送信しない場合、SMFはハートビート要求を再送信します。これは、構成されている間隔と、許可される試行回数に基づいています。
3. 構成されたハートビート メッセージの再試行回数を使い果たし、SMF が UPF からの応答を受信しない場合、SMF はその UPF に関連付けられているサブスクライバのセッションの解放手順を開始します。

### ノード マネージャでのハートビートと高可用性

各 UPF インスタンスは、プライマリおよびセカンダリ ノード マネージャに関連付けられています。セカンダリ ノード マネージャは、プライマリ マネージャがフェールオーバするスタンバイ システムとして機能します。プライマリ ノード マネージャは、IP 割り当てと、関連付け作成、更新、または削除要求などの関連付け固有のメッセージの管理を担当します。

# UPF パス管理および復元の構成サポート

この項では、UPF ステータスをモニタリングするためのサポートを構成する方法について説明します。

ハートビート機能を使用した UPF ステータス検出のサポートの構成には、次の手順が含まれます：

- UPF のハートビート パラメータの構成：インターフェイス レベルで UPF のハートビート パラメータの構成詳細をリストします。詳細については、インターフェイス レベルでハートビートの構成 （1985 ページ）を参照してください。
- UPF プロファイルのハートビート パラメータの構成：プロファイル レベルで UPF プロファイルのハートビート パラメータの構成詳細をリストします。詳細については、UPF グループ レベルでのハートビートの構成 （1987 ページ）を参照してください。
- [個々の UPF ネットワーク構成への UPF グループの関連付け（AssociatingUPF Group to Individual UPF Network Configuration）]：UPF グループを個々の UPF ネットワークに関連付けるための構成の詳細が一覧表示されます。詳細については、個々の UPF ネットワーク構成への UPF グループの関連付け （1988 ページ）を参照してください。
- Sx/N4 パス障害検出ポリシーの構成：Sx/N4 パス障害検出ポリシー パラメータの構成の詳細をリストします。詳細については、「Sx/N4 パス障害検出ポリシーの構成 （1988 ページ）」を参照してください。

# インターフェイス レベルでハートビートの構成

interface-level でハートビートを構成するには、以下の構成例を使用します：

```
config
   instance instance-id gr_instance_id
```

```
endpoint pfcp
   interface { n4 | sxa }
      heartbeat
         interval interval
            max-retransmissions max_retry_count
            retransmission-timeout retry_interval_count
            end
```

注：

- **instance instance-id** *gr_instance_id*：GR インスタンス ID を指定します。
- **endpoint pfcp**：エンドポイント コンフィギュレーション モードを指定します。
- **interface { n4 | sxa }**： SMF と UPF の間でハートビート メッセージが交換される N4 または Sxa インターフェイスを構成します。
- **Heartbeat**：ハートビート構成を指定します。
- **interval** *interval*：ハートビート間隔（秒）を指定します。許容範囲は 60 ー 360 です。デフォルト値は 60 秒です。

（注） *interval* を 0 に設定して、ハートビート機能を無効にします。

- **max-retransmissions** *max_retry_count*：Packet Forwarding Control Protocol（PFCP）のハートビート要求の最大再試行回数を指定します。0 ー 10 の範囲内である必要があります。デフォルト値は 3 です。
- **retransmission-timeout** *retry_interval_count*：ハートビート再送信タイムアウトを指定します（秒）。1 ー 20 の範囲内である必要があります。デフォルト値は 5 です。

## SMF のハートビート構成の確認

このセッションでは、SMF のハートビート構成を確認する方法を説明します。

**show running-config instance instance-id** *gr_instance_id* **endpoint pfcp** コマンドを使用して、機能構成を表示して確認します。

以下は show コマンドの出力例です。

```
show running-config instance instance-id 1  endpoint pfcp
 instance instance-id 1
  endpoint pfcp
   interface n4
    heartbeat
     interval               61
     retransmission-timeout 3
     max-retransmissions    5
     exit
    exit
   exit
 exit
exit
```

```
 interface sxa
  heartbeat
   interval               300
   retransmission-timeout 15
   max-retransmissions    0
   exit
  exit
exit
```

# UPF グループ レベルでのハートビートの構成

UPF グループ レベルでハートビートを構成するには、以下の構成例を使用します：

```
config
   profile upf-group group_name
      heartbeat
         interval interval
         retransmission-timeout max_retry
         max-retransmissions retry_count
         end
```

注：

- **profile upf-group** *group_name*：ハートビート機能を有効にする必要がある UPF グループを指定します。
- **interface**：SMF と UPF の間でハートビート メッセージが交換される N4 インターフェイスを構成します。
- **heartbeat** ：ハートビート構成を指定します。
- **interval** *interval*：ハートビート間隔（秒）を指定します。60 ー 360 の範囲内である必要があります。デフォルト値は 60 秒です。

  *interval* を 0 に設定して、ハートビート機能を無効にします。
- **max-retransmissions** *max_retry*：Packet Forwarding Control Protocol（PFCP）のハートビート要求の最大再試行回数を指定します。0 ー 10 の範囲内である必要があります。デフォルト値は 3 です。
- **retransmission-timeout** *retry_count*：ハートビート再送信タイムアウトを指定します（秒）。1 ー 20 の範囲内である必要があります。デフォルト値は 5 です。

## UPF グループ レベルのハートビート構成の確認

このセッションでは、UPF のハートビート構成を確認する方法を説明します。

**show running-config profile upf-group** コマンドを使用して、機能構成を表示して確認します。

以下は show コマンドの出力例です。

```
show running-config profile upf-group
 profile upf-group upfGroup1
  heartbeat
   interval               62
```

```
   retransmission-timeout 3
   max-retransmissions    2
   exit
  exit
 exit
```

# 個々の UPF ネットワーク構成への UPF グループの関連付け

ここでは、UPF グループを UPF 構成に関連付ける方法について説明します。

このシナリオでは、各 UPF ネットワーク構成に、すべての UPF インスタンスを UPF プロファイルに関連付ける UPF プロファイルが含まれます。

UPF グループプロファイルをネットワーク構成に関連付けるには、次の構成例を使用します。

```
config
   profile network-element upf upf_profile_name
      upf-group-profile upf_group_name
      end
```

注：

- **profile network-element upf** *upf_profile_name*：UPF ネットワーク構成を構成します。
- **upf-group-profile** *upf_group_name*：指定された UPF ネットワーク構成に関連付ける必要がある UPF グループ名を指定します。

## UPF グループと個々の UPF の関連付けの確認

ここでは、UPF グループと個別の UPF の関連付けを確認する方法について説明します。

**show running-config profile network-element upf** コマンドを使用して、機能構成を表示して確認します。

以下は show コマンドの出力例です。

```
profile network-element upf upf1
 n4-peer-address ipv4 209.165.200.238
 n4-peer-port      8805
 upf-group-profile upfGroup1
 dnn-list          [ intershat intershat1 intershat2 ]
 capacity          65535
 priority          65535
```

# Sx/N4 パス障害検出ポリシーの構成

Sx/N4 パス障害検出ポリシーを構成するには、次のサンプル構成を実行します：

次の構成例を使用して、Sx/N4 パス障害検出ポリシーを関連付けます。

```
config
   instance instance-id gr_instance_id
      endpoint pfcp
         sx-path-failure sx-detection-policy detection_policy_name
         end
```

Sx/N4 パス障害検出ポリシーのパラメータを設定するには、次の構成例を使用します：

```
config
   policy sx-path-failure-detection detection_policy_name
      ignore { heartbeat-retry-failure |
heartbeat-recovery-timestamp-change }
         end
```

注：

- **instance instance-id** *gr_instance_id*：GR インスタンス ID を指定します。インスタンス ID 1 はローカル インスタンス ID を示しています。
- **endpoint pfcp** *endpoint_name*：選択したインターフェイスのエンドポイント名とエンドポイント コンフィギュレーション モードを指定します。
- **sx-path-failure sx-detection-policy** *detection_policy_name*：ハートビート要求のタイムアウトの結果として Sx パスの障害が発生し、デフォルトの Sx アクションがクリーンアップ アクティビティを実行する場合に使用されるポリシーの名前を指定します。
- **policy sx-path-failure-detection** *detection_policy_name*：ハートビート要求タイムアウト検出の結果として Sx パス障害が発生した場合に使用されるポリシーの名前を指定します。
- **ignore { heartbeat-retry-failure | heartbeat-recovery-timestamp-change }**：ハートビート メッセージの再試行がタイムアウトになった場合、またはハートビート要求または応答メッセージのリカバリ タイムスタンプに変更があった場合は常に、パス障害モードを検出します。

## Sx/N4 パス障害検出ポリシーの確認

ここでは、Sx/N4 パス障害検出ポリシーを確認する方法について説明します。

**Sx/N4 パス障害検出ポリシーの関連付けの確認**：

**show running-config instance instance-id** *gr_instance_id* **endpoint pfcp** コマンドを使用して、機能構成の関連付けを表示および確認します。

以下は show コマンドの出力例です。

```
show running-config instance instance-id 1 endpoint pfcp
 instance    instance-id 1
  endpoint    pfcp
   replicas    1
   enable-cpu-optimization    true
   sx-path-failure sx-detection-policy sx1
   interface    n4
   heartbeat
    interval    0
    retransmission-timeout    3
    max-retransmissions    5
    exit
   vip-ip    209.165.201.24
   exit
  interface    gtpu
  vip-ip    209.165.201.24
  exit
```

```
 exit
exit
```

**Sx/N4 パス障害検出ポリシーのパラメータ設定の確認**：

Sx/N4 パス障害検出ポリシーの構成パラメータの設定を表示および確認するには、次のコマンドを使用します：

機能の構成パラメータ設定を表示および確認するには、**show running-config policy sx-path-failure-detection** *detection_policy_name* コマンドを使用します。

以下は show コマンドの出力例です。

```
show running-config policy sx-path-failure-detection
 policy sx-path-failure-detection sx1
 ignore heartbeat-retry-failure
 exit
exit
```

# OAM サポート

ここでは、この機能の操作、管理、およびメンテナンスに関して説明します。

## バルク統計

次の統計情報は、ハートビート関連 UPF パス管理機能でサポートされます。

- **nodemgr_upf_heartbeat_fail_stats**
- **nodemgr_upf_hb_msg_stats**

SMF は、ハートビート要求および応答の手順中にトリガされたこれらのバルク統計情報を保持します。

### nodemgr_upf_heartbeat_fail_stats

- 説明：

  ハートビート要求への応答が失敗した場合に UPF ごとに更新されるカウンタ。

- **`nodemgr_upf_heartbeat_fail_stats`** カウンタは、次のラベルをサポートしています。

  ラベル

  - ラベル： **upf_heartbeat_req_tx**

    ラベルの説明：SMF が送信するハートビート要求のラベル。

  - ラベル：**upf_heartbeat_req_retx**

    ラベルの説明：再送信されたハートビート要求のラベル

  - ラベル：**upf_heartbeat_rsp_rx**

    ラベルの説明：SMF が受信するハートビート応答のラベル。

**nodemgr_upf_hb_msg_stats**

- 説明：

  指定された UPF のすべてのハートビート メッセージのカウンタ

SMF のバルク統計情報のサポートの詳細については、「*UCC 5G SMF* メトリック リファレンス」を参照してください。

第 48 章

# 仮想ルーティングおよび転送


- 機能の概要と変更履歴, on page 1993
- 機能説明 （1994 ページ）
- 機能の仕組み （1995 ページ）
- 仮想ルーティングと転送の構成 （1996 ページ）
- OAM サポート （2001 ページ）


## 機能の概要と変更履歴

### 要約データ

***Table 545:*** 要約データ

| | |
|---|---|
| 該当製品または機能エリア | SMF |
| 該当プラットフォーム | SMI |
| 機能のデフォルト設定 | 無効：設定が必要 |
| このリリースでの関連する変更点 | N/A |
| 関連資料 | 該当なし |

### 更新履歴

***Table 546:*** マニュアルの変更履歴

| 改訂の詳細 | リリース |
|---|---|
| Diameter インターフェイスの VRF サポートが追加されました。 | 2023.04.0 |

| 改訂の詳細 | リリース |
|---|---|
| 次の拡張機能が導入されました。<br>• VRF の最大数を 129 に拡張<br>• スタティックおよびダイナミックなポリシーの削除 | 2023.01.0 |
| PAPN ユース ケースにおける AAA サーバ アドレスの重複のサポート | 2022.04.0 |
| 最初の導入。 | 2020.02.5 |

# 機能説明

仮想ルーティングおよびフォワーディング（VRF）は、同じルータ上で同時に複数のインスタンスのルーティング テーブルを共存させるためのテクノロジーです。ルーティング インスタンスは独立しているため、互いに競合することなく、同じ IP アドレスまたは重複する IP アドレスを使用できます。

プライベート APN（PAPN）の展開では、同じ SMF が複数の PAPN をサポートできます。この場合、エンタープライズ AAA サーバでの認証とアカウンティングが必要です。AAA サーバは異なるモバイル仮想ネットワーク事業者（MVNO）に属しているため、それらのアドレス範囲が重複する可能性があります。SMF は VRF を使用して、PAPN または MVNO での AAA サーバ アドレスの重複を許可します。

**重要** 現在、SMF は AAA クライアントの重複アドレスをサポートしていません。

SMF は VRF を使用して、VRF のデフォルト ルートを使用して最適化された UDP インターフェイスに基づくダイナミック ルートとスタティック ルートも削除します。このアクションにより、インターフェイスごとに1つのデフォルトルートでポリシーが置き換えられ、動作パフォーマンスが向上します。

SMF により、IP プールでの VRF の構成が可能になります。SMF は、構成された VRF 名とともに IP アドレスの詳細を UPF に送信します。UPF は、UPF 内で構成された VRF に IP アドレスをマッピングします。

SMFは、プライベート APN および DNN のために 2K TPS のスケールで最大 129 の VRF をサポートします。

SMF は、Diameter Gx および Gy インターフェイスのクライアント側 VRF をサポートします。プロファイルの Diameter エンドポイントは、Diameter エンドポイントから構成する VRF 名とインターフェイス名を参照します。Diameter エンドポイントは、VRF 名を使用して、Diameter クライアントから TCP 接続を作成します。

（注） この実装は、VRF を構成していない場合には下位互換性があります。このような場合、Diameter サーバに対する TCP ソケットの作成は、VRF 名の構成なしで適用できます。

# 機能の仕組み

このセクションは、次のユース ケースで SMF の VRF 技術の使用方法を説明します：

- PAPN
- 静的および動的なポリシーの削除

## VRF の作成

VRF を作成するには、次の手順を実行します：

1. CLI 構成により、ゲートウェイを使用して VRF を作成します。

   VRF は、VRF ルーティング テーブルのデフォルト ルートを使用して作成されます。

2. PAPN の使用例では、各 PAPN は、デフォルト ルートを持つ独自の VRF に関連付けられます。各 PAPN VRF は、SMF およびリーフ スイッチで定義する必要があります。
3. ダイナミックおよび静的なポリシー削除のユース ケースでは、デフォルト ルートを持つ VRF が SMF で作成され、VRF によって追加されたデフォルト ルートを介してアウトバウンド ルートを処理します。

   SMF は、リーフ スイッチへの L3 VIP アドバタイズメントに引き続きグローバル VRF を使用します。したがって、リーフでは、このユース ケースに特定の VRF は必要ありません。

## VRF 変更内容

既存の VRF でデバイスまたはゲートウェイを削除するには、次の手順を実行します。

1. 削除する VRF をエンドポイントとルータから関連付け解除する。
2. VRF を削除し、構成変更を適用します。

重要 実行中のシステムでのみ VRF を削除してください。

3. 変更したデバイスまたはゲートウェイで VRF を作成します。
4. 変更されたデバイスまたはゲートウェイで新しく作成された VRF をエンドポイントとルータに関連付けます。設定の変更を適用します。

## VRFの削除

既存の VRF でデバイスまたはゲートウェイを削除するには、次の手順を実行します。

1. 削除する VRF をエンドポイントとルータから関連付け解除する。
2. VRF を削除し、構成変更を適用します。

重要　実行中のシステムでのみ VRF を削除してください。

3. VRF が論理 SMF 間で共有されている場合は、すべての論理 SMF から VRF を削除して、インターフェイスから VRF 構成を完全に削除します。これは、静的および動的なユースケースにのみ適用されます。

## 制限事項

この機能には、次の制限事項があります。

- 認証およびアカウンティング要求の NAS-IP は、RADIUS エンドポイント CoA-NAS インターフェイス構成のインターフェイス CoA-NAS VIP-IP と同じである必要があります。
- RADIUS サーバ グループと RADIUS エンドポイントで構成されている VRF は同じである必要があります。
- メッセージ（DM）要求の切断では、クライアント VRF とサーバ VRF（CoA-NAS VIP VRF）が一致している必要があります。一致しなかった場合、DM 要求は廃棄されます。

# 仮想ルーティングと転送の構成

## VRF 設定

VRF の構成は、PAPN と静的および動的の両方のユース ケースに適用できます。

グローバル構成モードで VRF を構成するには、次のサンプル構成を使用します。

```
config
   vrf name vrf_name gateway gateway_ipv4_address gatewayIpv6 gateway_ipv6_address
 device interface_name linkDevice linked_device_name
   end
```

重要　VRF の作成および削除操作がサポートされています。既存の VRF を変更するには、VRF を削除してから再度追加する必要があります。

注：

- **vrf name** *vrf_name* ：VRF 名を指定します。サポートされる VRF の最大長は 15 です。
- **gateway** *gateway_ipv4_address*：ゲートウェイの IPv4 アドレスを指定します。
- **gatewayIpv6** *gateway_ipv6_address*：ゲートウェイの IPv6 アドレスを指定します。
- **device** *interface_name*：パブリック結合インターフェイスの名前を指定します。
- **linkDevice** *connectedDevice_name*：プライベート ボンディング インターフェイスの名前を指定します。このフィールドは、静的および動的なユース ケースにのみ適用されます。

## 設定例

次に、ゲートウェイを使用した VRF の構成例を示します：

```
vrf name papn_vrf_1 gateway 209.165.202.131 device bd2.radius.2161
vrf name papn_vrf_2  gateway 209.165.202.131 device bd2.radius.2162
vrf name vrf_s11 gateway 209.165.202.131 device bd1.s11.1692 linkDevice bd1.s11.1696
```

# エンドポイントの設定

エンドポイントを構成し、VRF に関連付けるには、次の構成例を使用します：

```
config
   instance instance-id instance_id
       endpoint { gtp | pfcp | radius | diameter  }
          interface { coa-nas | s5 | s5e | s2b | s11 | n4 | gx | gy  }

              vip-ip ip_address [ vip-interface  interface_name| vip-port
vip_port | vrf vrf_name ]
              end
```

注：

- **endpoint { gtp | pfcp | radius | diameter }**：エンドポイント名を指名します。GTP、PFCP プロトコル、RADIUS、または Diameter のいずれかです。

  PAPN サポートについては、RADIUS エンドポイントを使用します。スタティックおよびダイナミックなポリシー削除の使用例では、GTP または PFCP プロトコルを選択します。

- **interface { coa-nas | s5 | s5e | s2b | s11 | n4 | gx | gy }**：使用例に基づいてインターフェイスを指定します。PAPN サポートの場合は、**coa-nas** インターフェイスを選択します。ポリシー削除の使用例では、他の使用可能なインターフェイスのいずれかを使用します。Diameter エンドポイントの場合は、 **gx** または **gy** インターフェイスを選択します。
- **vip-ip** *ip_address*：構成されたエンドポイントの IPv4 アドレスを指定します。
- **vip-interface** *interface_name*：インターフェイス名を指定します。これは、VRF に関連付けられている結合インターフェイスであることに注意してください。
- **vip-port** *vip_port*：エンドポイントのポート番号を指定します。

- **vrf** *vrf_name*：グローバル VRF コンフィギュレーションを使用して定義された VRF 名を指定します。

## 設定例

次に構成例を示します；

```
instance instance-id 1 endpoint radius interface coa-nas vip-ip 209.165.202.131 vip-port
 8112 vip-interface bd2.radius.2161 vrf papn_vrf_1

instance instance-id 1 endpoint radius interface coa-nas vip-ip 209.165.202.133 vip-port
 8112 vip-interface bd2.radius.2162 vrf papn_vrf_2

instance instance-id 1 endpoint pfcp interface n4 vip-ip 209.165.202.134 vip-interface
bd2.n4.2105 vrf vrf_n4_ls1

instance instance-id 1 endpoint gtp interface s11 vip-ip 209.165.202.135 vip-interface
bd1.s11.1692 vrf vrf_s11

instance instance-id 1 endpoint diameter interface gx vip-ip 209.165.202.136 vip-interface
 d2.aaa.1212 vrf vrf_signaling
```

# RADIUS プロファイルにおける VRF 構成

RADIUS サーバ グループに VRF を構成するには、次の構成例を使用します：

```
config
   profile radius
      server-group group_name
         vrf vrf_name
         server-private { radius_server_ip_address port_number  | [ range ] }

            priority radius_server_priority
            secret radius_server_secret_key
            type { acct | auth }
            end
```

注：

- **server-private {** *radius_server_ip_address  port_number* **| [ range ] }** ：アカウンティングおよび認証要求に使用されるプライベート RADIUS サーバの IP アドレスとポート番号を指定します。このサーバーは、特定のサーバ グループに対してプライベートです。

  サーバ グループ内のプライベート サーバは、そのグループに関連付けられているグローバル サーバよりも優先されます。プライベート サーバが到達不能またはデッド状態の場合、認証要求またはアカウンティング要求を送信するためにグローバル サーバが選択されます。

- **priority** *radius_server_priority*：RADIUS サーバの優先順位を指定します。

- **secret** *radius_server_secret_key*：RADIUS サーバの共有秘密キーを指定します。

  文字列で指定する必要があります。

- **type { acct | auth }**：アカウンティングおよび認証要求に使用されるプライベート RADIUS サーバのタイプを指定します。

- **server-private {** *radius_server_ip_address port_number* **[ priority** *radius_server_priority* **| secret** *radius_server_secret* **| type { acct | auth } ] | [ range ] }**
- **range**：IP アドレス範囲を指定します。
- **vrf** *vrf_name*：AAA サーバ グループで構成する VRF 名を指定します。

  VRF が server-group で構成されている場合は、server-private を使用してサーバを構成し、グローバル サーバを関連付けないことをお勧めします。

RADIUS ダイナミック認証/COA 構成で VRF を定義するには、次の構成例を使用します。

```
config
   profile radius-dynamic-author
      client client_ip_address vrf vrf_name
         nas-identifier nas_identifier_port
         secret secret_key
         end
```

注：

- **client** *client_ip_address*：RADIUS ダイナミック認証クライアント構成を指定します。
- **vrf** *vrf_name*：AAA サーバ グループで構成する VRF 名を指定します。

  VRF が server-group で構成されている場合は、server-private を使用してサーバを構成し、グローバル サーバを関連付けないことをお勧めします。
- **nas-identifier** *nas_identifier_port*：ダイナミック認証 NAS 識別子を指定します。
- **secret** *secret_key*：ダイナミック認証サーバの共有秘密キーを指定します。

# BGP ピアリングの VRF 関連付け

BGP ピアリングのために VRF を BGP に関連付けるには、次の構成例を使用します：

```
config
   router bgp bgp_name
       interface interface_name
           vrf  vrf_name
           end
```

注：

- **interface** *interface_name*：ローカル BGP インターフェイスを指定します。
- **vrf** *`vrf_name*：BGP に関連付ける VRF の詳細を指定します。

## 設定例

次に、VRF 関連付けのない BGP ピアリング構成の例を示します。

```
interface enp94s0f0.3921
  bondingInterface enp216s0f0
```

```
  bondingInterface enp94s0f0
  neighbor 209.165.202.254 remote-as 65141 fail-over bfd
exit
interface enp94s0f1.3922
  bondingInterface enp216s0f1
  bondingInterface enp94s0f1
  neighbor 209.165.202.254 remote-as 65141 fail-over bfd
exit
```

次に、papn_vrf_1 との関連付けを使用した BGP ピアリング構成の例を示します。

```
interface enp94s0f0.3923  leaf1
  vrf papn_vrf_1
  bondingInterface enp216s0f0
  bondingInterface enp94s0f0
  neighbor 209.165.202.254 remote-as 65141 fail-over bfd
exit
interface enp94s0f1.3924  leaf2
  vrf papn_vrf_1
  bondingInterface enp216s0f1
  bondingInterface enp94s0f1
  neighbor 209.165.202.254 remote-as 65141 fail-over bfd
exit
```

次に、papn_vrf_2 との関連付けを使用した BGP ピアリング構成の例を示します。

```
interface enp94s0f0.3925
  vrf papn_vrf_2
  bondingInterface enp216s0f0
  bondingInterface enp94s0f0
  neighbor 209.165.202.254 remote-as 65141 fail-over bfd
exit
interface enp94s0f1.3926
  vrf papn_vrf_2
  bondingInterface enp216s0f1
  bondingInterface enp94s0f1
  neighbor 209.165.202.254 remote-as 65141 fail-over bfd
exit
```

## 設定の確認

VRF 情報を表示するには、**show vrf-info all** コマンドを使用します。

次に、**show vrf-info all** コマンドの出力例を示します。

```
                          GATEWAY                          TABLE
NAME        GATEWAY         IPV6    DEVICE      LINK DEVICE   ID     STATE  POD NAME
-------------------------------------------------------------------------------------------
npapn-vrf12 209.165.200.225      bd2.npv12.756               2516    true
bgpspeaker-pod-1
papn-vrf18  209.165.200.226      bd2.pv18.1236               2621    true
bgpspeaker-pod-1
vrf_s11     209.165.200.227      bd1.s11.1692  bd1.s11.1696  2631    true
bgpspeaker-pod-1
vrf_n4_ls1  209.165.200.228      bd2.n4.2105   bd2.n4.3915   2630    true
bgpspeaker-pod-1
```

VRF ルート情報を表示するには、**show vrf-route-info all** コマンドを使用します。

次に、**show vrf-route-info all** コマンドの出力例を示します。

```
Vrf TableId Route
papn-vrf11 2614 default via 209.165.200.225 dev bd2.pv11.1229 proto 217 metric 217
```

```
papn-vrf11 2614 broadcast 209.165.200.226 dev bd2.pv11.1229 proto kernel scope link src
 209.165.200.225
papn-vrf11 2614 209.165.200.227/29 dev bd2.pv11.1229 proto kernel scope link src
209.165.200.225
papn-vrf11 2614 local 209.165.200.225 dev bd2.pv11.1229 proto kernel scope host src
209.165.200.225
papn-vrf11 2614 broadcast 209.165.200.227 dev bd2.pv11.1229 proto kernel scope link src
 209.165.200.225
papn-vrf11 2614 anycast fe80:: dev bd2.pv11.1229 proto kernel
papn-vrf11 2614 local fe80::42a6:b7ff:fe37:38 dev bd2.pv11.1229 proto kernel
papn-vrf11 2614 fe80::/64 dev bd2.pv11.1229 proto kernel metric 256
papn-vrf11 2614 ff00::/8 dev bd2.pv11.1229 proto 3 metric 256

Vrf TableId Route
vrf_s5 2633 default via 209.165.200.225 dev bd1.s5.1691 proto 217 metric 217
vrf_s5 2633 local 209.165.200.226 dev bd1.s5.1691 proto kernel scope host src
209.165.200.225
vrf_s5 2633 broadcast 209.165.200.226 dev bd1.s5.1691 proto kernel scope link src
209.165.200.225
vrf_s5 2633 local 209.165.200.226 dev bd1.s5.1691 proto kernel scope host src
209.165.200.225
vrf_s5 2633 broadcast 209.165.200.226 dev bd1.s5.1691 proto kernel scope link src
209.165.200.225
vrf_s5 2633 broadcast 209.165.200.226 dev bd1.s5.1691 proto kernel scope link src
209.165.200.225
vrf_s5 2633 209.165.200.226/24 dev bd1.s5.1691 proto kernel scope link src 209.165.200.225
vrf_s5 2633 local 209.165.200.225 dev bd1.s5.1691 proto kernel scope host src
209.165.200.225
vrf_s5 2633 broadcast 209.165.200.226 dev bd1.s5.1691 proto kernel scope link src
209.165.200.225
vrf_s5 2633 broadcast 209.165.200.226 dev bd1.s5.1691 proto kernel scope link src
209.165.200.225
vrf_s5 2633 209.165.200.226/24 dev bd1.s5.1691 proto kernel scope link src 209.165.200.225
vrf_s5 2633 local 209.165.200.226 dev bd1.s5.1691 proto kernel scope host src
209.165.200.225
vrf_s5 2633 broadcast 209.165.200.226 dev bd1.s5.1691 proto kernel scope link src
209.165.200.225
vrf_s5 2633 anycast fe80:: dev bd1.s5.1691 proto kernel
vrf_s5 2633 anycast fe80:: dev bd1.s5.1691 proto kernel
vrf_s5 2633 local fe80::42a6:b7ff:fe37:39 dev bd1.s5.1691 proto kernel
vrf_s5 2633 local fe80::42a6:b7ff:fe37:39 dev bd1.s5.1691 proto kernel
vrf_s5 2633 fe80::/64 dev bd1.s5.1691 proto kernel metric 256
vrf_s5 2633 fe80::/64 dev bd1.s5.1691 proto kernel metric 256
vrf_s5 2633 ff00::/8 dev bd1.s5.1691 proto 3 metric 256
vrf_s5 2633 ff00::/8 dev bd1.s5.1691 proto 3 metric 256
```

# OAM サポート

## バルク統計サポート

VRF 機能をサポートするために、次の統計情報が更新されています。

- bgp_outgoing_routerequest_total：この統計には、VRF ごとの成功した BGP 発信ルートの総数を示す「vrf」ラベルが含まれています。
- bgp_outgoing_failedrouterequest_total：この統計には、VRF ごとの失敗した BGP 発信ルートの合計数を示す「vrf」ラベルが含まれています。

- [bgp_speaker_bfd_peer_status]：この統計には、BFD ピア ステータスを示す「vrf」ラベルが含まれています。

# 第 49 章

# ワイヤレス優先順位サービス

表 *547*: 機能の履歴

| 機能名 | リリース情報 | 説明 |
|---|---|---|
| SBI メッセージ優先順位の拡張 | 2023.04 | SBI メッセージ優先順位（SMP）メカニズムは、「3gpp-Sbi-Message-Priority」カスタム HTTP ヘッダーを使用して、クライアントとサーバ間のメッセージ優先順位を設定および伝送します。カスタム HTTP ヘッダーは、1 つ以上のプロキシを介して、クライアントとサーバ間でエンドツーエンドのメッセージの優先順位を適用します。<br>（注）<br>ストリーム優先順位メカニズムはサポートされていません。 |


- 機能の概要と変更履歴 （2004 ページ）
- 機能説明 （2005 ページ）
- 機能の仕組み （2014 ページ）
- 5QI マッピングのサポート （2015 ページ）
- ワイヤレス優先順位サービスの構成 （2016 ページ）
- 優先度の高いメッセージに対するメッセージ プライオリティのネゴシエーション （2027 ページ）
- WPS OAM サポート （2028 ページ）

# 機能の概要と変更履歴

## 要約データ

***Table 548:*** **要約データ**

| | |
|---|---|
| 該当製品または機能エリア | SMF |
| 該当プラットフォーム | SMI |
| 機能のデフォルト設定 | 無効：設定が必要 |
| このリリースでの関連する変更点 | N/A |
| 関連資料 | 該当なし |

## 更新履歴

***Table 549:*** **マニュアルの変更履歴**

| 改訂の詳細 | リリース |
|---|---|
| SBI メッセージ優先メカニズムと手順に基づくメッセージ優先順位付けの強化 | 2023.04.0 |
| 5QI マッピングのサポートが導入されました | 2023.03.0 |
| WPS ダイナミック ルール削除中の UPF の相互作用 | 2021.01.0 |
| SBI メッセージの優先順位メカニズムと手順に基づくメッセージの優先順位付けが導入されました。 | 2021.01.0 |
| ワイヤレス優先順位サービス機能は、このリリースで完全に認定されています。 | 2020.03.0 |
| 最初の導入。<br>この機能は、このリリースでは完全には認定されていません。詳細については、シスコのアカウント担当者にお問い合わせください。 | 2020.02.0 |

# 機能説明

ワイヤレス プライオリティ サービス（WPS）機能は、5GC を介した SMF でサポートされます。 SMF は 、セッションの作成または変更とさまざまなハンドオーバー シナリオでの WPS サービスの優先順位付けを検証します。 SMF では、ネットワーク トリガー サービス要求手順に対するページング ポリシーの差別化について、WPS サービスも評価します。

また、SMF ではローカル構成で ARP に基づいてプライオリティ コールを検出して、セッションを WPS として分類するため、ユーザは WPS コール用の ARP に加えて非標準 QCI を使用できます。

これらの非標準 QCI 値に対応する QoS プロパティは、gNB でローカルに構成されます。SMF は、データ パス上の非標準 QCI を DSCP 値にマップするために SMF に追加された値のみをサポートします。

**重要** リリース 2021.02.0 では、他の既存のルール ARP が wps-profile と一致しない場合、SMF はダイナミック ルールの削除中に N4 メッセージに MP フラグを設定しません。

# 使用例

WPS 機能は、5GS および EPS での次の使用例に対するワイヤレス優先順位のサポートに関する 3GPP 推奨事項を実装します。使用例は、3GPP TS 23.501（セクション 5.16.3、5.16.4、5.16.5、5.16.6、5.19、および 5.21）に従って定義されます。

WPS は次の使用例をサポートしています。

- マルチメディア優先サービス （2005 ページ）
- PFCP を介した N3、S5-U、または S2-B の DSCP マーキング （2011 ページ）

## マルチメディア優先サービス

マルチメディア優先サービス（MPS）では、サービス ユーザーがシステム リソースに優先的にアクセスできるため、優先度の高いセッションを提供または完了することが可能になります。サービス ユーザーとは、政府が承認した担当者、緊急管理当局、またはその他の承認ユーザーです。MPS は、「エンドツーエンド」のプライオリティ ベースでのプライオリティ セッションをサポートします。MPS には、シグナリングのプライオリティとメディアのプライオリティが含まれます。

MPS は、プライオリティを持つセッションを呼び出し、変更、維持、およびリリースする機能を提供します。また、ネットワークの輻輳状態では、プライオリティ メディア パケットを配信します。

すべての MPS サブスクライブ UE は、UDM の QoS プロファイルで MPS の適切な値を構成することによって、特定のサービス ユーザーに対して優先順位を持つように構成されている DN

に対して確立されると、QoSフロー（たとえば、IMSシグナリングに使用）が優先されます。サービス ユーザーは、地域または国の規制要件に基づいて、オンデマンド MPS 加入者ではなく、オンデマンド MPS 加入者として扱われます。オンデマンド サービスは、サービス ユーザーの明示的な呼び出しまたは呼び出しに基づいており、確立されているメディアQoSフローに適用されます。オンデマンドではない MPS サービスは呼び出しを必要とせず、5G ネットワークへの接続後に特定のサービスユーザーを優先するように構成されたDNにのみ、すべての QoS フローの優先処理を提供します。

MPS の優先順位処理には、モビリティ管理手順の優先順位メッセージの処理が含まれます。MPS セッションの優先処理には、オペレータのポリシーに従って、QoS フローに適切な ARP および 5QI を設定する必要があります。

MPS プライオリティ メカニズムは、サブスクリプション関連のメカニズムと呼び出し関連のメカニズムに分類できます。サブスクリプション関連のメカニズムは、「常に適用」および「条件付きで適用」として適用できます。

条件付きで適用されるサブスクリプション関連のメカニズムは次のとおりです。

- UDM：優先サービスまたは重要なサービスに対して、1 つまたは複数の ARP 優先レベルが割り当てられます。各 DN の優先順位付けされた QoS フローの ARP が、適切な ARP 優先順位レベルに構成されます。
- PCF：「IMSシグナリング優先順位」情報は、UDMでサブスクライバに対して構成され、PCF は IMS シグナリングに使用される QoS フローの ARP を変更します。

呼び出し関連のメカニズムは、モバイル発信 SIP コールまたはセッション、モバイル着信 SIP コールまたはセッション、および優先 PDU 接続サービスに適用できます。

## オンデマンド MPS サービス

優先順位付けされたサービスの呼び出し関連の優先順位メカニズムは、アプリケーション サーバーとの通信、およびアプリケーション サーバーと Rx または N5 インターフェイスを介した PCF 間の通信に基づいています（IMS を使用した MPS の場合は、3GPP TS 23.228、5.21 節で説明されています）。

モバイル発信の呼び出し関連のメカニズム（SIPやIMSなどを介した場合など）については、次のように説明されています：

- PCF：
  - セッションの指示が Rx または N5 インターフェイスに到達し、UE にシグナリング QoSフローの優先順位がない場合、PCFは、サービスプロバイダーのポリシーに従って（3GPP TS 23.503 の 6.1.3.11 節で指定されているように）ARP および 5QI パラメータと関連する QoS 特性を適切に取得します。
  - MPS セッションの場合、セッションの開始手順の一環として QoS フローを確立または変更するときに、PCF は ARP および 5QI パラメータ、および関連する QoS 特性を適宜選択して、QoS フローに優先順位を付けます。
  - 特定のDNに対するすべてのアクティブセッションが解放され、その特定のPDUセッションに対する優先処理の対象として UE が構成されていない場合、PCF は、必要に

応じて、ARP および 5QI パラメータの適切な設定と、関連する QoS 特性から IMS シグナリング QoS フローをダウングレードします。 ：サブスクリプションに基づいて UE が権限を有するものに。

モバイル終了（SIP や IMS などを介した）の呼び出し関連のメカニズムについては、次のように説明されています。

- PCF：セッションの指示が Rx または N5 インターフェイスを介して到達すると、上記のモバイル発信で説明されているメカニズムが適用されます。
- UPF：IP パケットが CM-IDLE の UE の UPF に到着した場合、UPF は、DL データ パケットの QoS フローを識別する情報を含む「データ通知」を SMF に送信します（3GPP TS 23.502 で指定されています）。を参照してください。
- SMF：SMF が、プライオリティの使用目的で ARP プライオリティレベル値に関連付けられた QoS フローの「データ通知」メッセージを受信した場合、N11 インターフェイスの「N1N2MessageTransfer」メッセージに ARP を含めることで、ページング手順中にプライオリティ表示が提供されます。 （3GPP TS 23.502 の 4.2.3.3 条で規定）。
- AMF：AMF は、プライオリティ使用のための ARP プライオリティレベル値を含む「N1N2MessageTransfer」メッセージを受信すると、プライオリティとともに要求を処理します。AMF には、より高い優先順位を必要とする UPF の既存の IP パケットについて示すように割り当てられた値に構成された N2 「Paging」メッセージの「Paging Priority」IE も含まれます（3GPP TS 23.502、4.2.3.3 節で規定）。
- SMF：プライオリティを高くするように設定されていない UE の場合、プライオリティを使用するための ARP プライオリティ レベルを持つ PCF から「N7 Session Management Policy Modification」メッセージを受信すると、SMF は「N1N2MessageTransfer」を送信して ARP をQoS フローのシグナリング（3GPP TS 23.502、4.3.3.2 項で規定）。
- AMF：プライオリティを使用するための ARP プライオリティレベルが含まれる SMF から「N1N2MessageTransfer」メッセージを受信した後、AMF はシグナリング QoS フローの ARP を更新します（3GPP TS 23.502、4.3.3.2 項で規定）。
- （R）AN：N2「Paging」メッセージに「Paging Priority」を含めると、（R）AN で輻輳時のページングの優先順位処理がトリガーされます（3GPP TS 23.502、4.2.3.3 節で規定）。

優先順位 PDU 接続サービスの呼び出し関連メカニズム：

- PCF：
  - 優先順位 PDU 接続サービスの状態が無効から有効に変更された場合、優先順位 PDU 接続サービスによって制御される QoS フローが確立または変更され、ARP および 5QI パラメータと関連する QoS 特性がPDU セッション変更手順（3GPP TS 23.502、4.3.3 節で規定）。
  - 優先順位 PDU 接続サービスの状態が有効から無効に変更された場合、優先順位 PDU 接続サービスによって制御される QoS フローは、ARP および 5QI パラメータと関連する QoS 特性のサービス適切な設定から、UE がPDU セッション変更手順（3GPP TS 23.502 第 4.3.3 条で規定）を使用。

## GTP-C を介したメッセージ優先順位の表示

過負荷ノードは、過負荷状態の間に着信メッセージを処理するときに、メッセージの優先順位付けを実行します。この条件は、GTP-C ヘッダーでシグナリングされる相対的な GTP-C メッセージ優先順位に基づいています。

メッセージ スロットリングが実行される場合、次の条件に従います：

- 優先順位トラフィック（3GPP TS 22.153 に記載されている eMPS）および緊急に関連する GTP 要求の優先度が最も高くなります。地域または、国の要件やネットワーク通信事業者のポリシーに応じて、これらの GTP 要求は、トラフィックの削減をする時に最後にスロットルされます。優先順位トラフィックは、プライオリティ トラフィックをスロットリングせずに要求されたトラフィック削減を達成できない時点まで、GTP 過負荷制御によりスロットリングから免除されます。
- 他のタイプのセッションでは、メッセージスロットリングでは、優先順位の低いメッセージが他のメッセージの前にスロットリング対象と見なされるように、メッセージの相対的な優先順位が考慮されます。メッセージの相対的な優先順位は、メッセージが送信される手順の相対的な優先順位（句 12.3.9.3.2 で指定されている）から、または APN や ARP などのセッション パラメータから派生します。

優先順位の高いメッセージにはより低いスロットルの優先順位が与えられ、優先順位の低いメッセージにはより高い優先順位が与えられます。過負荷状態のノードは、自己保護メカニズムの一部として、過負荷状態の間に最初の着信メッセージを処理するときに、これらのメッセージの優先順位付けスキームも適用します。

送信側の GTP-C エンティティは、手順ベースまたはセッションのパラメータに従って、メッセージでシグナリングする相対的なメッセージ優先順位を決定します。メッセージが複数のベアラーに影響する場合（たとえば、ベアラー要求の変更）、相対的なメッセージの優先順位は、すべてのベアラーの中で最高の優先順位の ARP を考慮します。

GTP-C エンティティは、対応する Initial メッセージまたは Triggered メッセージで受信したものと同じメッセージ優先順位を Triggered メッセージまたは Triggered Reply メッセージにそれぞれ設定します。GTP-C ヘッダーにメッセージ 優先順位がない着信 GTP-C メッセージの場合、受信側の GTP-C エンティティは次の処理を行います。

- 着信メッセージが初回メッセージである場合に、デフォルトの優先順位を適用します。
- 受信メッセージがトリガ メッセージまたはトリガ返信メッセージの場合に、初期メッセージまたはトリガ メッセージで送信されるメッセージ優先順位を適用します。

ネットワーク内のノードは、サポートされていないノードから受信した初期メッセージを過負荷のノードが処理するのを防ぐために、同種でこの機能をサポートしています。これらのメッセージは、デフォルトの優先順位に従って受信されます。過負荷のノードは、GTP-C メッセージでシグナリングされたメッセージ優先順位に従って、サポート ノードから受信した最初のメッセージを処理します。

### セッション パラメータに基づくメッセージの優先順位付け

また、メッセージの優先順位付けは、APN や ARP などのセッション パラメータに基づいて実行されます。優先順位の高いセッションに関連付けられた手順およびメッセージには、優先順位の低いセッションに関連付けられた手順およびメッセージよりも優先順位が低くなります。各セッションのグループ内では、メッセージは、メッセージが送信される手順のカテゴリに基づいてさらに優先順位付けされます。

## 手順に基づくメッセージの優先順位付け

メッセージの優先順位付けは、メッセージが送信される手順の相対的な優先度に基づいて実行されます。手順はさまざまなカテゴリに分類され、各カテゴリには優先順位が割り当てられます。さらに、特定の手順のカテゴリ内で、APN、QCI、ARP、LAAPI などのセッション パラメータに基づいてメッセージの優先順位をさらに高くすることができます。

優先順位が高いメッセージには、スロットリングに対してより低い優先順位が与えられ、優先順位が低いメッセージには、スロットルに対してより高い優先順位が与えられます。手順のグループ化は、個々の GTP-C エンティティに基づいて実行されるのではなく、一般的にすべての手順を考慮しながら実行されます。GTP-C エンティティは、自身に適用可能な手順を検討し、手順のカテゴリに基づいてメッセージ スロットリングに優先順位を付けます。カテゴリは、優先順位の高い順に表示され、カテゴリ 1 が最も優先順位が高くなります。カテゴリごとに、メッセージの重複しないリストが表示されます。今後の既存または新たに定義されたメッセージは、メッセージが送信される手順のカテゴリに基づいて考慮されます。手順のカテゴリを次に示します：

1. 3GPP アクセスまたは非 3GPP アクセス内および間の UE セッションモビリティ：アクティブまたはアイドル モードの UE モビリティを含む手順（関連する GTP-C シグナリングがこのカテゴリに分類されるなど）。たとえば、SGW の変更を伴うかどうかにかかわらず、X2 または S1 ベースのハンドオーバー、MME または SGSN の変更を伴う TAU または RAU（SGW の変更を行う/行わない）、および信頼できる非 3GPP アクセスのハンドオーバーへの 3GPP アクセスがあります。UE セッション モビリティに関連する手順中にこれらのメッセージをスロットリングすると、対応する手順が失敗します。この障害により、PDN の切断やサービスの中断が発生する可能性があります。その結果、このカテゴリに属する手順中に次のメッセージが送信される場合、優先度が最も高いと見なされる必要があります。したがって、これらのメッセージには、スロットリングの優先順位が最も低くなります。
   - セッション要求を作成する。
   - 「ハンドオーバー」指示ビットが設定されたセッション要求を作成する。
   - ベアラー要求を変更する。
   - 「ハンドオーバー」指示ビットが設定されたベアラ要求を変更します。
   - アクセス ベアラー要求を変更する。

2. PDN 接続またはベアラー リソースのリリース：既存の PDN 接続の非アクティブ化、ベアラーまたは UE のデータ転送トンネルの非アクティブ化により発生する手順は、過負荷状態のノードのリソースの解放につながります。これらの手順により、解放されたリソース

はUEの残りの部分へのサービス提供に使用できるため、過負荷の状況が緩和されます。したがって、このカテゴリに属し、PDN接続またはベアラーまたはデータ転送トンネルの非アクティブ化を引き起こす次のメッセージは、次に優先順位の高いレベルで処理する必要があります。したがって、これらのメッセージには、スロットリング中、対応する優先順位が与えられます：

- セッション要求を削除する。
- ベアラー要求を削除する。
- ベアラーコマンドを削除する。
- 間接データ転送トンネル要求の削除。

3. その他のセッション管理手順：このカテゴリは、PDN接続の作成およびベアラーの作成または変更手順を除くセッション管理手順で構成されます。いくつかの例として、他のモビリティ手順、およびサービス要求およびS1リリースの手順と組み合わせていない場合のロケーションレポートが挙げられます。これらの手順は、UEの進行中のサービスには影響しません。したがって、このカテゴリで特定された手順中に送信される次のメッセージは、次に優先順位の高いレベルで処理する必要があります。したがって、これらのメッセージには、スロットリング中、対応する優先順位が与えられます：
   - アクセス ベアラー要求をリリースします。
   - ベアラー要求を変更する。
   - 通知を変更。
   - 一時停止通知。
   - 再開通知。

4. 新しいPDN接続またはベアラー リソースまたは既存のベアラー リソースの変更の要求：このカテゴリは、PDN接続の作成、ベアラーの作成または変更、またはデータ転送トンネルの作成を要求する手順で構成されます。このカテゴリに属するメッセージを抑制すると、既存サービスは続行しながら新しいサービスが拒否されます。このオーバーロード状態では、リソース不足のためオーバーロードされたノードは、既存のサービスを維持しながら新しいサービスを提供できません。実行中に次のメッセージが送信されると、このカテゴリに属する手順は最も低い優先順位と見なされます。したがって、これらのメッセージには、スロットリングにおいて最も高い優先順位が与えられます。
   - PDN 接続要求中にセッション要求を作成します。
   - ベアラー要求の作成。
   - ベアラー要求の更新。
   - ベアラー 技術情報 コマンド。
   - ベアラー変更コマンド。
   - 間接データ転送トンネル要求の作成。

- クォータを使い果たす場合は、セッションのデータ パケットの DSCP マーキングをダウングレードします。

### PFCP の Message-Priority ヘッダー

メッセージ スロットリングが実行される場合：

- 優先トラフィック（つまり、3GPP TS 22.153 に記載されている eMPS）および緊急に関連する PFCP リクエストが最も優先されます。地域または、国の要件やネットワーク通信事業者のポリシーに応じて、これらの PFCP リクエストは、トラフィックの削減をする時に最後にスロットルされます。スロットリングでは、優先トラフィックをスロットリングしないとリクエストされたトラフィックの削減を達成できない時点まで、PFCP 過負荷制御によって優先トラフィックが免除されます。
- 他のタイプのセッションでは、メッセージスロットリングでは、メッセージの相対的な優先順位が考慮され、優先順位の低いメッセージが最初にスロットリングの対象になります。メッセージの相対的な優先順位は、メッセージが送信される手順の相対的な優先順位から導出されるか、APN や ARP などのセッション パラメータから導出されます。

PFCP エンティティは、オペレータ ポリシーに基づいて、PFCP シグナリングでメッセージ優先順位を構成および使用するかどうかを決定します。送信側 PFCP エンティティは、APN や ARP などのセッション パラメータから取得される、メッセージ内のシグナリングする相対的なメッセージの優先順位を決定します。メッセージが複数のベアラーに影響する場合、相対的なメッセージの優先順位は、すべてのベアラーの中で優先順位の最も高い ARP を考慮して決定されます。PFCP エンティティは、対応する要求メッセージで受信したものと同じ応答メッセージで構成する必要があります。

PFCP ヘッダーにメッセージの優先順位がない着信 PFCP メッセージの場合、受信側 PFCP エンティティは、次の処理を行います。

- 受信メッセージが要求メッセージである場合、デフォルトの優先順位を適用します。
- 受信メッセージが応答メッセージの場合に、要求メッセージで送信されるメッセージの優先順位を適用します。

ネットワークの SMF および UPF 機能は、過負荷状態のノードが、サポートしていないノードから受信した要求メッセージをデフォルトの優先順位に従って処理するのを防ぐために、同じようにこの機能をサポートしています。このサポートにより、過負荷ノードは、PFCP メッセージでシグナリングされたメッセージの優先順位に従って、サポート ノードから受信した要求メッセージを処理する必要がなくなります。

## PFCP を介した N3、S5-U、または S2-B の DSCP マーキング

### トランスポート レベル マーキング

トランスポート レベル マーキングは、QCI およびオプションの ARP プライオリティ レベルからローカルに構成されたマッピングに基づく DSCP 値でトラフィックをマーキングするプロセスです。EPC の場合、S-GW と PGW-C は、EPS ベアラーごとにトランスポート レベルのマー

キングを実行します。5GC の場合、S-GW と PGW-C は QoS フローごとにトランスポート レベル マーキングを実行します。

UPF は 5QI、優先度レベル（明示的にシグナリングされている場合）、およびオプションで SMF で構成された ARP 優先度レベルからのマッピングに基づいて、DSCP 値を使用してトランスポート レベルのマーキングを実行します。CP 機能は、（マーキングされるトラフィックと一致する PDR に関連付けられる）FAR 内のトランスポート レベル マーキング IE 内の ToS またはトラフィック クラスに DSCP を提供することにより、トランスポート レベル マーキングを制御します。

UP 機能は、検出されたトラフィックに対してトランスポート レベルのマーキングを実行し、マーキングされたパケットをピア エンティティに送信します。CP 機能は、関連する FAR のトランスポート レベル マーキング IE を変更することにより、トランスポート レベルのマーキングを変更します。

## WPS プロファイルのサポート

SMF + PGW-C では、GTP-C および PFCP プロトコル IP ヘッダーに構成される ARP および DSCP マーキング値で定義された WPS プロファイルがサポートされます。WPS プロファイルを使用して、GTP-C および PFCP プロトコルでのメッセージの優先順位を構成します。

SMF + PGW-C では、最大 64 の WPS プロファイルを使用でき、各 WPS プロファイルは DNN プロファイルに関連付けられます。詳細は、「ワイヤレス優先順位サービスの構成（2016 ページ）」の項を参照してください。

## SBI メッセージ優先メカニズム

SBI メッセージ優先順位（SMP）の主な用途は、過負荷制御に関連するスロットリングの決定をしながら、HTTP/2 クライアントまたはサーバとして機能する 5GC NF にガイダンスを提供することです。優先順位情報は、プロキシのルーティングに使用できます。最終的に、サーバは優先順位情報を使用して、優先順位の低い要求の前に優先順位の高い要求を処理します。SMP メカニズムは、「3gpp-Sbi-Message-Priority」カスタム HTTP ヘッダーを使用して、クライアントとサーバ間のメッセージ優先順位を設定および伝送します。カスタム HTTP ヘッダーは、1 つ以上のプロキシを介して、クライアントとサーバ間でエンドツーエンドのメッセージの優先順位を適用します。

（注） ストリーム優先順位メカニズムはサポートされていません。

ヘッダーには、HTTP/2 メッセージの優先度の値が含まれます。ヘッダーのエンコードは、IETF RFC 7230 [12] で定義されている ABNF に従います。

```
3gpp-Sbi-Message-Priority = "3gpp-Sbi-Message-Priority" ":" (DIGIT / %x31-32 DIGIT / "3"
 %x30-31)
```

メッセージ：

```
3gpp-Sbi-Message-Priority "0"
```

優先順位は 1 が最高です。

例：

```
3gpp-Sbi-Message-Priority: 10
```

## 仕組み

SBI メッセージ優先順位メカニズムの機能は次のとおりです：

- クライアント、プロキシ、およびサーバは、メッセージの優先順位を構成または評価するときに、**3gpp-Sbi-Message-Priority** 値を使用します。
- クライアントは、**3gpp-Sbi-Message-Priority** カスタム HTTP ヘッダーをメッセージに追加してその値を設定することにより、要求の優先度を割り当てます。
- サーバが応答メッセージに異なる優先順位を割り当てた場合、サーバは、**3gpp-Sbi-Message-Priority** カスタム HTTP ヘッダーをメッセージに追加し、その値を設定することにより、応答の優先順位を割り当てます。

構成の詳細については、「メッセージプライオリティプロファイルの構成」および「メッセージ優先順位プロファイルの関連付け」を 参照してください。

## WPS セッションの重要な情報

重要な WPS セッション クリティカルな情報を次に示します。

- SMF は確立中にセッションを WPS として識別しないため、SMF では確立に基づく優先順位のタグ付けはできません。SMF は、MCS および MPS のサブスクリプションまたは確立の原因を認識していません。
- SMF は、WPS セッション構成または WPS セッション モニタリングに対する特別なアクセス権の強制をサポートしていません。
- SMF では、WPS ユーザーと非 WPS ユーザー間のハードウェア分離はサポートされていません。
- N4 での IPSEC サポートは、WPS ではサポートされません。IPSEC は、インターフェイスまたはピア レベルで有効になります。
- SBI メッセージ優先順位機能がスムーズに動作するには、SMF の前に UPF をアップグレードします。それ以外の場合は、UPF がアップグレードされた後にのみ、SMF に新しい優先順位値を構成してください。UPF は、古いリリースのメッセージ優先順位（MP）値 1 ー 3 をサポートしています。最初に SMF がアップグレードされ、新しい構成が N4 インターフェイスに適用されると、UPF は新しい値を無視して、それらのセッションを通常のコールとして扱います。
- アップグレード後に新しい優先順位値が構成された場合、UPF では、古いセッションはアップグレード前に適用された古い MP 値を使用し、新しいセッションは新しい MP 値を使用します。このため、同じタイプのセッションの MP 値が競合する可能性があり、優先順位に基づくセッション リカバリは、古いセッションの MP 値が更新されるまで期待どおりに機能しません。古いセッションの MP 値は、SMF からの後続の N4 変更中に更新されます。

- メッセージ優先順位プロファイルが QoS プロファイル、DNN プロファイルまたは WPS プロファイルに関連付けられている場合、SMF はこの SBI メッセージ優先順位機能を有効にします。それ以外の場合、SBI メッセージ優先順位機能は無効のままになり、SMF は N4 および GTP インターフェイス上の以前と同様にハードコードされた値を送信します。

### SMF におけるセッション タイプ競合の解決

次の条件で、SMF でのセッション タイプの競合の解決を行うことができます：

- DNN が緊急にタグされている場合、またはセッションが自動に作成される場合 SMF タグは、セッションを緊急としてタグします。
- DNN プロファイルの下でベアラー/フローが IMS として構成された QCI と一緒に作成された時に SMF は、IMS としてセッションをタグします。
- SMF は、PCF から受信した ARP に基づいてセッションを WPS としてタグ付けします。

セッションが複数の条件を満たしている時、セッション タイプは次の基準に基づいてタグ付けされます。

`[WPS] > [緊急（Emergency）] > [IMS]`

SMF は UPF にセッション タイプを送信しません。UPF は、構成を通じてセッションを優先順位にマッピングします。詳細については、『*UPF* 構成ガイド』を参照してください。

### WPS セッション VLAN タギング

SMF は、セッションの確立中に WPS に別の VLAN を割り当てません。SMF は、IP プールのアドレス範囲ごとのネクストホップ アドレスの構成をサポートしています。UPF はネクストホップを VLAN にマッピングします。

# 機能の仕組み

ここでは、ワイヤレス プライオリティ サービス（WPS）機能の動作について説明します。

# 標準準拠

このワイヤレス優先順位サービス機能は、以下の基準に準拠しています：

- 3GPP TS 22.153
- 3GPP TS 23.228
- 3GPP TS 23.282
- 3GPP TS 23.379
- 3GPP TS 23.501
- 3GPP TS 23.502

- 3GPP TS 23.503
- 3GPP TS 24.301

# 5QI マッピングのサポート

## 機能説明

SMF は現在、ARP に基づいて優先順位コール（WPS）を検出します。WPS コールに ARP に加えて QCI を使用するために、SMF は 5QI リマッピング機能をサポートしており、UE が理解できる標準 QCI を使用した非標準 QCI のマッピングを可能にします。

SMF は、次の機能を実行します：

- **4G へのシームレスなハンドオーバー**：SMF は、マッピングされた EPS QoS パラメータで、マッピングされた EPS ベアラーコンテキストを含む QCI を構成値に再マッピングします。
- **5G へのシームレスなハンドオーバー**：SMF は、[セッション応答の作成（Create Session Response）]、[ベアラー要求の作成（Create Bearer Request）]、および [ベアラー要求の更新（Update Bearer Request）] のプロトコル構成オプションの QoS フローの説明で送信された QCI を再マッピングします。

## ダイナミック ルールの QCI 変更

特定のシナリオでは、既存のセッションを非 WPS から WPS にアップグレードしたり、WPS から非 WPS にダウングレードしたりできます。このような場合、PCF は新しい QCI/ARP（QoS クラス識別子/割り当ておよび保持優先順位）とともに N7 通知を SMF に送信します。

新しい QCI が NAS 再マッピングされるように設定されている場合 SMF は、5G RAT（無線アクセス技術）に接続されている場合、UE（ユーザー機器）に送信される N1 変更コマンドメッセージ内の QoS フロー詳細のパラメータ リスト内の再マッピングされた QCI を含みます。

4G または Wi-Fi RAT に接続されている UE の場合、再マッピングされた QCI は、ベアラー更新要求のプロトコル構成オプションの一部として QoS フローの説明内で送信されます。

Wi-Fi ハンドオーバー中に PCF が SMF が再マッピング構成のある時に非標準の QCI を送信した場合、構成で指定された再マッピングされた QCI は、N1 PDU（プロトコル データ ユニット）確立応答内、作成セッション応答内、または、ベアラー作成要求の UE に送信されます。

SMF は構成を再マッピングし、実行時の構成変更は、次の手順中にのみ適用されます：

- デフォルトのベアラーセッションの新規作成
- PCF からの新しい QoS フローまたはベアラーの作成リクエスト
- PCF からの QCI アップグレードまたはダウングレード

- Wi-Fi ハンドオーバー

詳細については、「非標準 QCI から標準 QCI への再マッピング （2019 ページ）」を参照してください。

## 元の QCI と再マッピングされた QCI の衝突

同じ QCI またはマッピングされた QCI を持つ新しいベアラーと既存のベアラーとの間で衝突が発生した場合、SMF は次の条件に基づいて一部の QoS フロー構成を拒否します。

- PCF が QCI を送信すると、フローまたはベアラーに関連付けられた既存の QCI に再マッピングされ、SMF はベアラーの作成または QCI アップグレードまたはダウングレード要求を拒否します。
- PCF が新しいベアラー/フローの作成のために QCI を送信し、同じ再マッピングされた QCI を持つ既存のフロー/ベアラーがすでに存在する場合、SMF は新しいベアラーの作成を要求する PCF の要求を拒否します。
- SMF が QCI=x を QCI=y に、QCI=z を QCI=y に再マッピングするように構成されている場合、PCF が QCI=x でルールを送信し、フロー/ベアラーが作成されると、 QCI = z の PCF は SMF によって拒否されます。

**例**：次の再マッピングの構成は、システムによって許可/受け入れられません。

- ```
  profile qos qosp-ims
      qosflow qi5 131 nas-remap 131
  ```
- ```
  profile qos qosp-ims
      qosflow qi5 131 nas-remap 132
      qosflow qi5 132 nas-remap 131
  ```
- ```
  profile qos qosp-ims
      qosflow qi5 131 nas-remap 132
      qosflow qi5 132 nas-remap 133
  ```

詳細については、「非標準 QCI から標準 QCI への再マッピング」を参照してください。

# ワイヤレス優先順位サービスの構成

ここでは、ワイヤレス優先順位サービス機能を構成する方法について説明します。

## DNN プロファイルの構成

次の構成例を使用して、WPS プロファイルを構成します。

```
config
  profile wps wps_profilename
    arp arp_value
```
```

```
    dscp [ n3 n3_value | message-priority { [ { gtpc | pfcp } [ arp |
dscp ] ] }
    end
```

注：

- **profile wps** *wps_profilename*：ワイヤレス プライオリティ サービス プロファイル構成にアクセスします。 *wps_profilename* は 、1 ～ 63 文字の英数字の文字列である必要があります。
- **arp** *arp_value*：ARP レベルの範囲を指定します。 *arp_value* は 、「,」または「-」のいずれかで区切られた 1 ～ 15 の整数である必要があります。

重要 SMF をリリース 2023.03.0 からそれ以降のリリースにアップグレードする場合は、アップグレードの完了後に WPS プロファイルの ARP パラメータを手動で再構成してください。

- **dscp [ n3** *n3_value* **]** ：N3 インターフェイスの DSCP マーキング値を指定します。N3 の値は、0 ～ 0x3F の範囲内の UP DSCP マーキング値を示します。
- **message-priority { gtpc pfcp }**：GTP-C および PFCP のメッセージの優先順位を指定します。

### WPS プロファイル構成の確認

この項では、WPS プロファイル構成を確認する方法について説明します。

**show running-config** コマンドを実行して構成を表示します。

次に、**show running-config** コマンドの出力を示します。

```
show running-config profile wps wps1
   profile wps wps1
   arp 1,4-6,9
   dscp n3 10
   message-priority [ pfcp gtpc ]
   exit
```

# DNN プロファイルでの WPS プロファイルの関連付け

次の構成例を使用して、WPS プロファイルを構成済みの DNN プロファイルに関連付けます。

```
config
   profile dnn profile_dnn_name
      wps-profile wps_profile_name
      end
```

注：

- **wps-profile** *wps_profile_name*：ワイヤレス プライオリティ サービス プロファイル構成を有効にします。このプロファイルは、既存の DNN プロファイル構成で構成されます。

### DNN プロファイルでの WPS プロファイルの確認

このセクションでは、DNN プロファイルの下の WPS プロファイル構成を確認する方法を説明します。

**show running-config** コマンドを実行して構成を表示します。

次に、**show running-config** コマンドの出力を示します。

```
show running-config profile dnn intershat
profile dnn intershat
network-element-profiles chf chf1
network-element-profiles amf amf1
network-element-profiles pcf pcf1
network-element-profiles udm udm1
charging-profile chgprf1
virtual-mac b6:6d:47:47:47:47
wps-profile wps1
ssc-mode 2 allowed [ 3 ]
session type IPV4 allowed [ IPV6 IPV4V6 ]
upf apn intershat
exit
```

# 設定の確認

サブスクライバセッションごとの WPS パラメータを表示するには、**show subscriber** コマンドを使用します。

**show subscriber** コマンドの出力例を次に示します。

```
show subscriber supi imsi-123456789012345 nf-service smf
subscriber-details
{
  "subResponses": [
    {
      "status": true,
      "genericInfo": {
        "supi": "imsi-123456789012345",
        "pei": "imei-123456786666660",
        "pduSessionId": 5,
        "pduSesstype": "Ipv4PduSession",
        "accessType": "3GPP_ACCESS",
        "dnn": "intershat",
        "plmnId": {
          "mcc": "123",
          "mnc": "456"
        },
        "sScMode": 1,
        "uetimeZone": "UTC+12:00",
        "allocatedIp": "209.165.200.233",
        "nrLocation": {
          "ncgi": {
            "mcc": "123",
            "mnc": "456",
            "nrCellId": "123456789"
          },
          "tai": {
            "mcc": "123",
            "mnc": "456",
            "tac": "1820"
          }
```

```
},
"alwaysOn": "None",
"dcnr": "None",
"wps": "Wps Session",
"ratType": "NR",
"ueType": "NR Capable UE",
"sessTimeStamp": "2021-05-28 12:46:11.165805357 +0000 UTC",
"callDuration": "2.925145554s",
"ipPool": "poolv4",
"commonId": 11,
"snssai": {
  "sd": "Abf123",
  "sst": 2
},
.
.
.
```

# 非標準 QCI から標準 QCI への再マッピング

次の設定例を使用して、QoS フロー パラメータmリストで送信された QCI を有効にし、必要な構成値に再マッピングします。この再マッピングプロセスは、N1 PDU 確立承認および PDU セッション変更手順に適用されます。

```
config
   profile qos qos_profile_name
      dscp-map qi5 qos_id
      qosflow qi5 nonstandard_value nas-remap standard_value
      arp-priority-level arp_value uplink user-datagram dscp-marking
dscp_marking_value
      arp-priority-level arp_value downlink { encsp-header { copy-inner
| dscp-marking dscp_marking_value } | user-datagram dscp-marking
dscp_marking_value } }
      commit
```

注：

- **dscp-map qi5** *qos_id*：承認された QoS パラメータの ID を指定します。 *qos_id* は 、1 ～ 255 の範囲の整数である必要があります。
- **qosflow qi5** *nonstandard_value* **nas-remap** *standard_value*：SMF は、QoS フローの説明のパラメータリストで送信される 5QI を構成された値に再マッピングします。 **nas-remap** *standard_value* は 、1ー255 の範囲のマッピング 5QI 値を受け入れます。たとえば、 **qosflow qi5** *131* **nas-remap***1*とします。
- **arp-priority-level** *arp_value* **uplink user-datagram dscp-marking** *dscp_marking_value*：ARP 優先度レベルを構成し、次にアップリンク方向の内部 IP ヘッダーに DSCP 値を設定します。この DSCP 値は、5QI 値が構成されているパケットに適用されます。

  *arp_value* は 1ー255 の範囲の整数である必要がありま。

  *dscp_marking_value* は、0x00 から 0x3F までの 16 進数である必要があります。

- **arp-priority-level** *arp_value* **downlink { encsp-header { copy-inner | dscp-marking** *dscp_marking_value* **} | user-datagram dscp-marking** *dscp_marking_value* **} }**：ARP 優先度レベルを設定し、カプセル化ヘッダーまたはユーザーデータグラムに適用する DSCP 値を構成します。

  **encsp-header** が構成されている場合は、ダウンリンク方向の外部 IP ヘッダーの DSCP を設定するか、内部 IP ヘッダーから外部 IP ヘッダーに DSCP 値をコピーします。

  **user-datagram** が構成されている場合は、ダウンリンク方向の内部 IP ヘッダーに DSCP を設定します。

  *arp_value* は 1ー255 の範囲の整数である必要がありま。

  *dscp_marking_value* は、0x00 から 0x3F までの 16 進数である必要があります。

次に、設定例を示します。

```
[smf] smf(config)# profile qos qos_A5972
[smf] smf(config-qos-qos_A5972)# qosflow qi5 1
Possible completions:
  arp-priority-level
  downlink
  gfbr
  mfbr
  nas-remap
  uplink
[smf] smf(config-qos-qos_A5972)# qosflow qi5 1 nas-remap 2
```

# メッセージの優先順位プロファイルの構成

すべてのインターフェイスにメッセージ優先順位を構成するには、次の構成例を使用します。

```
config
     profile message-priority msg_priority_profile_name
     interface [ any | pfcp | gtp | sbi [ { create | update | delete }
 ] ]
        priority value range
     exit
```

注：

- **interface [ any | pfcp | gtp | sbi [ { create | update | delete } ] ]**：
  - **interface [ any | pfcp | gtp | sbi ]**：インターフェイスごとに優先順位の値を指定します。たとえば、SBI インターフェイスの場合は、手順に従って構成します。手順が構成されていない場合、すべての手順に同じ値が適用されます。インターフェイスタイプは任意です。構成されていない場合は、すべてのインターフェイスに同じ値が適用されます。
  - **priority** *value*： sbi では 0 ～ 31 、pfcp、gtp、または anyでは 0 ～ 15 の優先度の範囲を指定します。0が最も高い優先度を示し、31 または15が最も低い優先度を示します。

（注） セルフトリガされる発信メッセージには、優先順位が設定されません。たとえば、タイマーの期限切れによってトリガされた発信メッセージです。

### メッセージの優先順位プロファイルの確認

**Show running-config for profile message-priority** コマンドの出力例を次に示します。

```
Show running-config for profile-> message-priority :

profile message-priority test

  interface pfcp,any priority value 15

 interface gtp priority value 10

 interface sbi priority value 20

 interface sbi procedure create priority value 0

 interface sbi procedure update priority value 10

 interface sbi procedure delete priority value 20

exit
```

# メッセージの優先順位プロファイルの関連付け

### WPS のメッセージの優先順位の関連付け

次の構成を使用して、WPS プロファイルを ARP およびメッセージ優先順位プロファイルに関連付けることができます。

```
config
  profile wps wps_profile_name
     arp  arp_value [ qci ] message-priority-profile profile_name
  exit
```

注

- **profile wps** *wps_profilename*：ワイヤレス優先順位サービス プロファイル構成にアクセスします。 *wps_profilename* は、1 ～ 63 文字の英数字の文字列である必要があります。
- **arp** *arp_value* **message-priority-profile** プロファイル名：1 ～ 15 の範囲で ARP 値を指定します。
- **qci message-priority-profile** *profile_name*：ワイヤレス優先セッションは、ARP および任意で QCI に基づいて決定されます。

- **message-priority-profile** *profile_name* ：このパラメータは、メッセージ優先順位プロファイルが関連付けられていない場合にのみ使用されます。例：**message-priority-profile** *[ pfcp gtpc ]*。

### WPS でのメッセージ優先順位プロファイルの確認

メッセージ優先順位プロファイルに基づいて WPS パラメータを表示するには、 **show full-configuration profile wps** コマンドを使用します。

**show full-configuration profile wps** コマンドの出力例を次に示します。

```
[smf] smf(config)# show full-configuration profile wps

profile wps test

  arp 1,8

  arp 5-7 message-priority-profile test

exit
```

### メッセージの優先順位プロファイルの関連付け

メッセージ優先順位プロファイルを SGW QoS プロファイルと、SGW QoS プロファイルの QoS、ARP に関連付けることができます。次の構成は、「sos」など、専用の DNN で着信する緊急通話に対して機能します。

```
config
  profile qos  qos-profile-name
      message-priority-profile profile_name
      qosflow qi5  nonstandard_value arp-priority-level arp_value
message-priority-profile profile_name
  exit
```

注：

- **message-priority-profile** *profile_name* ：メッセージ優先順位プロファイルを QoS プロファイルに関連付けます。
- **qosflow qi5** *nonstandard_value* ：QCI に関連付けられたメッセージ優先順位プロファイルと QoS プロファイルに関連付けられている優先順位プロファイル。
- **arp-priority-level** *arp_value* ：ARP に関連付けられたメッセージ優先順位プロファイル。1 ～ 255 の範囲で ARP 値を指定します。

  QCI、ARP、または QoS プロファイルに関連付けられたメッセージ優先順位プロファイル、または WPS に関連付けられたメッセージ優先順位プロファイルは、より高い優先順位を持つものを選択するために交渉されます。

（注） デフォルトのベアラー/フロー、QCI、またはARPに関連付けられたメッセージ優先順位プロファイルがない場合、メッセージ優先順位値は、IMSおよび緊急コールのQoSプロファイルに関連付けられたメッセージ優先順位プロファイルから考慮されます。専用ベアラー/フローが作成されると、構成に応じてQCIまたはARPに関連付けられたメッセージ優先順位プロファイルからメッセージ優先順位が考慮されます。

### QoS プロファイル構成の確認

メッセージ優先順位プロファイルに基づいたQoSフローを表示するには、**show full-configuration profile qos** コマンドを使用します。

**show full-configuration profile qos** コマンドの出力例を次に示します。

```
[smf] smf(config)# show full-configuration profile qos test

profile qos test

  message-priority-profile test

  qosflow qi5 5 arp-priority-level 5 message-priority-profile mpp1

exit
```

### 緊急用のメッセージ優先順位プロファイルの関連付け

「IMS」などの他のDNNとのPDUセッションの確立があり、セッションタイプが「致命的」に設定されている場合は、次の構成例を使用して、緊急コールに特定の優先順位を指定します。

```
config
  profile dnn dnn_profile_name
    emergency-message-priority-profile profile_name
  exit
```

注：

- **emergency-message-priority-profile** *profile_name* ：緊急メッセージ優先順位プロファイルとメッセージ優先順位ネゴシエーションを有効にします。

（注） IMS-Inactiveのメッセージ優先順位（MP）値は、IMS-Activeから導出されます。ここで、

$MP_{IMS\text{-}Active}$ = IMS専用ベアラー/フローに対してMPが選択されています。

$MP_{IMS\text{-}Inactive} = MP_{IMS\text{-}Active} + 1$

**DNN でのメッセージ優先順位の確認**

**Show running-config for profile dnn** コマンドの出力例を次に示します。

```
Show running-config for profile-> dnn :

profile dnn intershat

 emergency-message-priority-profile test

exit
```

# オーバーロード スロットリングから WPS セッションを除外するための SMF の構成

GTP インターフェイスのオーバーロード スロットリングから WPS セッションを除外するには、構成例を使用します。

（注） オーバーロードの除外は、ARP/5QI/DNN/MP のみに基づいており、DSCP には基づいていません。

```
config
  profile overload ovld_ctrl_prfl
    overload-exclude-profile self-protection ovld_exclude_wps
    node level
      tolerance minimum minimum_value
      tolerance maximum maximum_value
      reduction-metric minimum minimum_value
      reduction-metric maximum maximum_value
    advertise
      interval value
      change-factor value
      validity-period value
     exit
    interface interface_name
      overloaded-action [ advertise ]
     exit
   exit
  exit
profile overload-exclude ovld_exclude_wps
   dnn-list dnn_list
   arp-list arp_list
   qi5-list qi5_list
   message-priority priority_valuemessage-priority { n4 | n7 | n10 | n11
 | n16 | n40 | s5 } upto priority_val
exit
```

注：

- **overload-exclude-profile self-protection** *ovld_exclude_wps*：WPS セッションをオーバーロード スロットリングから除外します。
- **profile overload-exclude** *ovld_exclude_wps* **message-priority** *priority_value*：GTP オーバーロード除外のサポートを許可します。
- **message-priority { n4 | n7 | n10 | n11 | n16 | n40 | s5 } upto** *priority_val*：優先順位の値に従って、着信 SMF トラフィックをスロットリングから除外するインターフェイスを指定します。

# エンドポイント レベルでの過負荷除外の構成

SBIインターフェイスのエンドポイント レベルで過負荷除外を構成するには、次の構成を使用します。

```
config
   instance instance-id instance_id
     endpoint sbi
       overload-control threshold threshold_limit threshold_range action
action_status action_code range exclude message-priority value
       commit
     end
```

注：

- **overload-control** : エンドポイント レベルでの過負荷制御を指定します。
- **threshold** ：しきい値の制限と範囲を指定します。
- *threshold_limit*：しきい値の上限を指定します。 *threshold_limit* は 、次のいずれかである必要があります。
  - *low*：オーバーロード保護の下限しきい値制限を指定します。
  - *high*：オーバーロード保護の上限しきい値制限を指定します。
  - *critical*：オーバーロード保護のクリティカルしきい値制限を指定します。
- *thershold_range*：しきい値の範囲を指定します。 *threshold_range* は 10 ～ 100000 の範囲の整数である必要があります。
- **action** ：しきい値制限に対して実行するアクションを指定します。
- *action_status*：しきい値制限のアクションを指定します。 *action_status* は次のように指定する必要があります：
  - **reject**：指定したしきい値の範囲が満たされた場合に着信メッセージを拒否します。
- *action_code*：アクション ステータス コードを指定します。 *action_code* は次の必要があります：

- **reject-code**：拒否ステータス コードを指定します。

- *range*：アクション コードの範囲を指定します。 *range* は 100 ー 600 の範囲の整数である必要があります。
- **exclude message-priority** *value*：SBI MP 過負荷除外値を指定します。

次に設定例を示します。

```
profile overload ovld_ctrl_prfl
 overload-exclude-profile self-protection ovld_exclude_wps
 node-level
  tolerance minimum 80
  tolerance maximum 95
  reduction-metric minimum 10
  reduction-metric maximum 100
  advertise
   interval        60
   change-factor   5
   validity-period 600
  exit
  interface gtpc
   overloaded-action [ advertise ]
  exit
 exit
exit

profile overload-exclude ovld_exclude_wps
 dnn-list [ sos ]
 arp-list [ 2 3 4 ]
 qi5-list [ 1 2]
 message-priority s5 upto <unsignedInt, 0 .. 15>
exit

config
  instance instance-id 1
    endpoint sbi
      overload-control threshold high 10000 action reject reject-code 200 exclude
message-priority <value>
    exit
  exit
exit
```

# 優先度の高いメッセージに対するメッセージプライオリティのネゴシエーション

表 *550 :* 機能の履歴

| 機能名 | リリース情報 | 説明 |
|---|---|---|
| 優先度の高いメッセージに関するメッセージの優先順位ネゴシエーション | 2024.04.1 | SMF は、どのような状況でも、優先度の高いメッセージ（WPS、緊急など）が中断されないようにする必要があります。<br>SMFは、メッセージプライオリティ（MP）ネゴシエーションを使用して、SMF とピア ノード間の中断のない通信を保証します。このメカニズムにより、SMFは、着信メッセージに存在するメッセージプライオリティ値をローカル コンフィギュレーションに存在するメッセージプライオリティ値と比較できます。<br>これにより、WPSセッションにおける優先度の高い着信および発信メッセージが優先順位付けされ、SMF で処理されます。<br>**デフォルト設定**： 有効 - 常時オン |

## メッセージ プライオリティのネゴシエーション

SMF は、SBI、GTPC、および PFCP インターフェイスを介してメッセージを送受信します。SMF は PCF と接続して、ARP および QCI 値を収集します。これらの値に基づいて、対応するインターフェイスに設定されているメッセージの優先順位を取得します。このメッセージプライオリティ値は、発信メッセージの送信に対して設定されます。

ただし、このメッセージプライオリティ値は、メッセージのプライオリティ付けには不十分です。この場合、SMFは着信メッセージに存在するメッセージプライオリティを考慮しません。これにより、SMFは優先順位の高い着信メッセージでさえ優先順位を解除する可能性があります。

また、SMFはPCFと対話する前にメッセージ優先順位値を受信しません。この場合、送信メッセージにはメッセージ プライオリティ値は含まれません。これにより、SMF からの優先度の高い発信メッセージの優先度が、受信側ピア ノードで優先解除される可能性があります。

この機能により、メッセージのプライオリティ設定プロセスが強化されます。これにより、SMFは着信メッセージに存在するメッセージ優先順位値を抽出し、そのインターフェイスに設定されたメッセージ優先順位値とネゴシエートできます。SMF は、最も低いメッセージ プライオリティ値を選択し、そのセッションのすべての送受信メッセージに設定します。

これにより、SMF は、すべてのセッションでメッセージ プライオリティの高いメッセージをメッセージ プライオリティの低いメッセージよりも優先できます。これは、SMF が発信メッセージに高い優先順位を設定するのにも役立ちます。

特定の SMF インターフェイスからのメッセージの優先順位に基づくメッセージのスロットリングと除外の詳細については、「WPS セッションを除外するための SMF の設定」のセクションを参照してください。

# WPS OAM サポート

### SMF セッション ゲージ カウンタ

「wps」ラベルは、WPS および非 WPS 機能をサポートするセッション レベルのゲージ カウンタの SMF サービスで導入されます。

次に例を示します。

```
smf_session_counters{always_on="disable",app_name="smf",cluster="smf",data_center="unknown",dnn="intershat",
instance_id="0",pdu_type="ipv4",rat_type="NR",service_name="smf-service",ssc_mode="ssc_mode_1",wps="non_wps"}
 10
smf_session_counters{always_on="disable",app_name="smf",cluster="smf",data_center="unknown",dnn="intershat",
instance_id="0",pdu_type="ipv4",rat_type="NR",service_name="smf-service",ssc_mode="ssc_mode_1",wps="wps"}
 20
```

### N4 インターフェイス メトリック

メッセージの優先順位に関連する N4 インターフェイス カウンタには次のものがあります。

- SESSION_DELETION_REQUEST
- SESSION_ESTABLISHMENT_REQUEST
- SESSION_MODIFICATION_REQUEST

N4 インターフェイス メトリックの例：

```
proto_pfcp_msg_total{app_name="SMF",cluster="Local",data_center="DC",instance_id="0",
message_direction="outbound",message_name="SESSION_DELETION_REQUEST",msgpriority=true,
service_name="protocol",status="accepted",transport_type="origin"} 4
proto_pfcp_msg_total{app_name="SMF",cluster="Local",data_center="DC",instance_id="0",
message_direction="outbound",message_name="SESSION_ESTABLISHMENT_REQUEST",msgpriority=true,
service_name="protocol",status="accepted",transport_type="origin"} 6
proto_pfcp_msg_total{app_name="SMF",cluster="Local",data_center="DC",instance_id="0",
message_direction="outbound",message_name="SESSION_MODIFICATION_REQUEST",msgpriority=true,
service_name="protocol",status="accepted",transport_type="origin"} 20
```

### GTPv2 メトリック

メッセージ プライオリティに関連する GTPv2 カウンタには次のものがあります：

- NumCreate BearerSuccess
- NumRxCreateBearerRes
- NumTxCreateSessionReq

GTPv2 メトリックの例：

```
gtpc_app_priority_events{app_name="SMF",cluster="Local",data_center="DC",
event_type="NumCreateBearerSuccess",instance_id="0",interface_type="S5",priority_msg="true",service_name="gtpc-ep"}
 2
gtpc_app_priority_events{app_name="SMF",cluster="Local",data_center="DC",
event_type="NumRxCreateBearerRes",instance_id="0",interface_type="S5",priority_msg="true",service_name="gtpc-ep"}
 2
gtpc_app_priority_events{app_name="SMF",cluster="Local",data_center="DC",
event_type="NumTxCreateSessionReq",instance_id="0",interface_type="S5",priority_msg="true",service_name="gtpc-ep"}
 2
```

## KPI

次の KPI は、この機能でサポートされます：

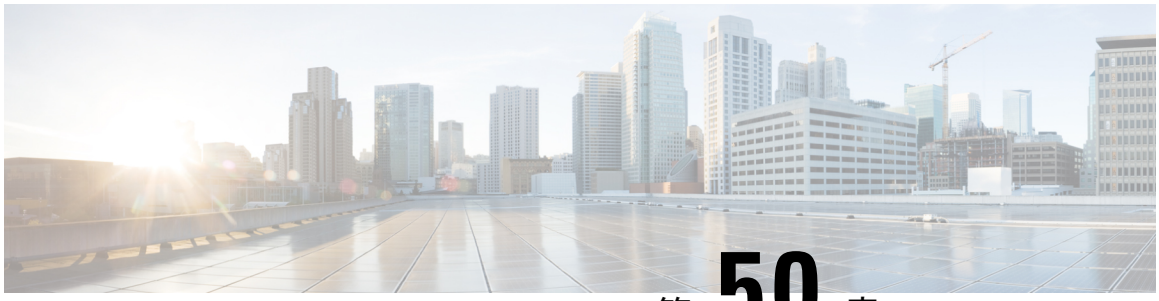
```
sum(policy_dynamic_pcc_rules_total{pccrule_change_type="binding_param_change",event="attempted"})
```

```
sum(policy_dynamic_pcc_rules_total{pccrule_change_type="binding_param_change",event="success"})
```

```
sum(policy_dynamic_pcc_rules_total{pccrule_change_type="binding_param_change",event="failure"})
```

**表 *551 : QCI* または *ARP* が変更された回数を追跡する統計情報**

| KPI 名 | タイプ | 説明または式 | ラベル（Label） |
|---|---|---|---|
| policy_dynamic_pcc_rules_total | counter | さまざまな手順の一環として追加、変更、または削除されたダイナミック PCC ルールの合計数。 | pccrule_change_type、ステータス |



第 50 章

# トラブルシューティング情報


- 機能の概要と変更履歴 （2031 ページ）
- 説明 （2033 ページ）
- CLI データの使用 （2033 ページ）
- アラート （2071 ページ）
- メトリック （2096 ページ）
- ログ （2100 ページ）
- ディスパッチャ （2112 ページ）


## 機能の概要と変更履歴

### 要約データ

***Table 552:*** 要約データ

| | |
|---|---|
| 該当製品または機能エリア | SMF |
| 該当プラットフォーム | SMI |
| 機能のデフォルト設定 | N/A |
| このリリースでの関連する変更点 | N/A |
| 関連資料 | 該当なし |

# 更新履歴

***Table 553:*** マニュアルの変更履歴

| 改訂の詳細 | リリース |
|---|---|
| 進行中の一括クリア サブスクライバ CLI の待機時間表示が追加され、連続した CLI がブロックされました。 | 2023.04.0 |
| 次のサポートが追加されました。<br>• SMF から UPF モニタ サブスクライバを有効にします。<br>• スライスごとのセッション数と NSSAI。 | 2023.03.0 |
| スライスおよびDNN機能ごとのIPプール割り当ての一部として、smf_service_stats メトリックの NSSAI ラベルを構成するための構成例を追加しました。 | 2022.04.0 |
| アプリケーション メトリックの分類と構成がサポートされるようになりました。 | 2021.02.3 |
| 次の機能強化のサポートが追加されました。<br>• vSMF または hSMF の IP アドレス値に基づいてサブスクライバの詳細を表示する **show subscriber nf-service smf** *smf_url* コマンド。<br>• vSMF または hSMF の IP アドレス値に基づいてサブスクライバの詳細をクリアする **clear subscriber nf-service smf** *smf_url* コマンド。<br>• vSMF または hSMF の IP アドレス値に基づいてサブスクライバの詳細をクリアする **clear subscriber nf-service smf** *smf_url* コマンド。<br>• **show subscriber supi** *supi_id* **nf-service smf psid** *psid_value* **full** コマンドは、hSMF および vSMF としてローミング固有の使用例の詳細なサブスクライバ情報を表示します。<br>• **show subscriber supi** *supi_id* **nf-service smf psid** *psid_value* **summary** コマンドは、hSMF および vSMF としてローミング固有の使用例のサブスクライバ セッションに関する詳細情報を表示します。 | 2021.02.2 |

| 改訂の詳細 | リリース |
| --- | --- |
| 次の機能強化のサポートが追加されました。<br>• サブスクライバ セッションに関する詳細情報を提供するには **show subscriber supi** 、 *supi_value* **nf-service smf psid** *psid_value* **summary** コマンド。<br>• **clear subscriber nf-service smf** および **show subscriber nf-service smf** コマンドと、サポートされているキーワードおよびフィルタ。<br>• **clear subscriber** および **clear subscriber nf-service smf** コマンドは、 **reactivation** キーワードをサポートし、再アクティブ化が必要というリリースの原因が構成されている場合にセッションをクリアします。この機能強化は、切断とリリースの理由もサポートします。<br>• **imeimonitor subscriber**、 **clear subscriber**、および **show subscriber** CLI コマンドのキーワード。 | 2021.02.0 |
| 最初の導入。 | 2020.02.0 より前 |

# 説明

この章では、システムの動作中に発生する可能性のある問題をトラブルシューティングするために、コマンド ライン インターフェイス（CLI）コマンド、アラート、メトリック、モニタ ツールとログの使用に関する情報について説明します。

# CLI データの使用

このセクションでは、トラブルシューティングに使用する show コマンドと clear コマンド、および monitor コマンドについて説明します。

## Show and Clear コマンド

### show コマンド

このセクションでは、問題のトラブルシューティングに使用できる主要な show コマンドの一部を示します。これらの show コマンドの出力には、特定の構成とステータス情報が示されます。

## show config-error

このコマンドを使用して、クラスタ内のすべてのポッドの構成エラー関連情報を表示します。次の出力例は、**show config-error** コマンドのためにあります：

```
[smf] smf# show config-error
ERROR
COMPONENT       ERROR DESCRIPTION
--------------------------------------------------------------------------------
RuleBase        Default bandwidth policy does not exist in rulebase <rba1> for charging
 action <ca1> .Dropping ruleDef <rda1>
RuleBase        Default bandwidth policy does not exist in rulebase <rba6> for charging
 action <ca1>.Dropping ruleDef <rda60>
RuleBase        Default bandwidth policy does not exist in rulebase <rba6> for charging
 action <ca1>.Dropping ruleDef <rda61>
ChargingAction  Packet filter <pkt1234> configured for charging action <ca4> associated
 with rulebase <rb1> does not exist
BandWidthPolicy Uplink peak data rate less than commited data rate in charging action
<ca6>Dropping ruleDef <rd6>
```

表 *554* : ***show config-error*** コマンドの出力フィールドの説明

| フィールド | 説明 |
|---|---|
| エラー コンポーネント | エラー コンポーネントを指定します。 |
| Error Description | エラーの説明を指定します。 |

## show diagnostics

このコマンドを使用して、診断情報を表示します。次の出力例は、**show diagnostics** コマンドのためにあります：

```
[smf] smf# show diagnostics
POD INSTANCE       DIAGNOSTIC            COMPONENT  START TIME               STATUS
RETRIES
--------------------------------------------------------------------------------------------
bgpspeaker-pod-1   Topology              AppInfra   2022/03/08 20:36:24.674  Success  0
bgpspeaker-pod-1   System Topology       AppInfra   2022/03/08 20:36:24.676  Success  0
sgw-service-0      Topology              AppInfra   2022/03/08 20:36:17.152  Success  0
sgw-service-0      System Topology       AppInfra   2022/03/08 20:36:17.154  Success  0
sgw-service-0      Cache Pod             AppInfra   2022/03/08 20:36:27.223  Success  0
sgw-service-0      SESSION_DB Datastore  AppInfra   2022/03/08 20:36:17.155  Success  0
li-ep-0            Topology              AppInfra   2022/03/08 20:36:20.743  Success  0
li-ep-0            System Topology       AppInfra   2022/03/08 20:36:20.741  Success  0
smf-service-1      Topology              AppInfra   2022/03/08 20:36:19.216  Success  0
smf-service-1      System Topology       AppInfra   2022/03/08 20:36:19.218  Success  0
smf-service-1      Cache Pod             AppInfra   2022/03/08 20:36:26.276  Success  0
smf-service-1      SESSION_DB Datastore  AppInfra   2022/03/08 20:36:19.220  Success  0
dns-proxy-0        Topology              AppInfra   2022/03/08 20:36:21.885  Success  0
dns-proxy-0        System Topology       AppInfra   2022/03/08 20:36:21.887  Success  0
protocol2-1        System Topology       AppInfra   2022/03/08 20:36:24.858  Success  0
protocol2-1        Cache Pod             AppInfra   2022/03/08 20:36:25.937  Success  0
protocol2-1        Topology              AppInfra   2022/03/08 20:36:24.856  Success  0
nodemgr-0          System Topology       AppInfra   2022/03/08 20:36:14.831  Success  0
nodemgr-0          Cache Pod             AppInfra   2022/03/08 20:36:26.485  Success  0
nodemgr-0          SESSION_DB Datastore  AppInfra   2022/03/08 20:36:14.833  Success  0
```

```
nodemgr-0          Topology             AppInfra   2022/03/08 20:36:14.835  Success  0
nodemgr-1          Topology             AppInfra   2022/03/08 20:36:23.068  Success  0
nodemgr-1          System Topology      AppInfra   2022/03/08 20:36:23.071  Success  0
nodemgr-1          Cache Pod            AppInfra   2022/03/08 20:36:26.690  Success  0
nodemgr-1          SESSION_DB Datastore AppInfra   2022/03/08 20:36:23.066  Success  0
```

表 *555* : ***show diagnostics*** コマンドの出力フィールドの説明

| フィールド | 説明 |
|---|---|
| コンポーネント | コンポーネント名を指定します。 |
| 診断 | 診断の詳細を指定します。 |
| ポッド インスタンス | ポッドのインスタンス情報を指定します。 |
| 再試行回数 | 再試行回数を指定します。 |
| 開始時刻 | アプリケーションの開始時刻を指定します。 |
| ステータス | 診断ステータスが成功かどうかを指定します。 |

## show endpoint all

このコマンドを使用して、クラスタ内のすべてのポッドで実行されているすべての内部および外部エンドポイントのリストを表示します。次の出力例は、**show endpoint all** コマンドのためにあります：

```
[smf] smf# show endpoint all
```

```
                          START    STOPPED
GR INSTANCE               ENDPOINT             ADDRESS  TYPE     STATUS
      INTERFACE  INTERNAL  TIME     TIME
-------------------------------------------------------------------------------
cache-pod                 xx.xx.xx.xx:0000     Grpc     Started  cache-pod
      true       4 weeks   <none>   0
cache-pod                 xx.xx.xx.xx:0000     Grpc     Started  cache-pod
      true       4 weeks   <none>   0
internal-admin-ep         xx.xx.xx.xx:0000     Rest     Started  internal-admin-ep
      true       4 weeks   4 weeks  0
internal-admin-ep         xx.xx.xx.xx:0000     Rest     Started  internal-admin-ep
      true       4 weeks   <none>   0
internal-admin-ep         xx.xx.xx.xx:0000     Rest     Started  internal-admin-ep
      true       4 weeks   <none>   0
:
:
keep-alived-ep            xx.xx.xx.xx:0000     Tcp      Started  keep-alived-ep
      true       2 weeks   <none>   0
keep-alived-ep            xx.xx.xx.xx:0000     Tcp      Started  keep-alived-ep
      true       2 weeks   <none>   0
oam-grpc-ep               xx.xx.xx.xx:0000     Grpc     Started  oam-grpc-ep
      true       4 weeks   <none>   0
oam-rest-ep               xx.xx.xx.xx:0000     Rest     Started  oam-rest-ep
      true       4 weeks   <none>   0
```

表 *556* : ***show endpoint all*** コマンドの出力フィールドの説明

| フィールド | 説明 |
|---|---|
| Address | エンドポイントのホストとポートを指定します。 |
| エンドポイント | エンドポイントの名前を指定します。 |
| GR インスタンス | GR インスタンスを指定します。 |
| Interface | エンドポイントのインスタンス名を指定します。 |
| 内線 | エンドポイントのタイプ（内部または外部）を指定します。 |
| 開始時刻 | エンドポイントの開始時間を指定します。 |
| ステータス | エンドポイントの現在のステータスを指定します。 |
| 停止時刻 | エンドポイントの終了時刻を指定します。 |
| タイプ | エンドポイントのタイプを指定します。 |

## show endpoint info

このコマンドを使用して、クラスタ内のすべてのポッドで実行されているエンドポイントのリストを表示します。次の出力例は、**show endpoint info** コマンドのためにあります：

```
[smf] smf# show endpoint info
                                                                                                    START
    STOPPED  GR
ENDPOINT                ADDRESS              TYPE  STATUS   INTERFACE  INTERNAL  TIME
    TIME     INSTANCE
-------------------------------------------------------------------------------------------------------
sbi                     xxx.xxx.xxx.xxx:0000  Rest  Started  rest       false     2 weeks
  <none>   0
sbi                     xxx.xxx.xxx.xxx:0000  Rest  Started  rest       false     2 weeks
  <none>   0
```

表 *557* : ***show endpoint all*** コマンドの出力フィールドの説明

| フィールド | 説明 |
|---|---|
| Address | エンドポイントのホストとポートを指定します。 |
| エンドポイント | エンドポイントの名前を指定します。 |
| GR インスタンス | GR インスタンスを指定します。 |
| Interface | エンドポイントのインスタンス名を指定します。 |

| フィールド | 説明 |
|---|---|
| 内線 | エンドポイントのタイプ（内部または外部）を指定します。 |
| 開始時刻 | エンドポイントの開始時間を指定します。 |
| ステータス | エンドポイントの現在のステータスを指定します。 |
| 停止時刻 | エンドポイントの終了時刻を指定します。 |
| タイプ | エンドポイントのタイプを指定します。 |

### show geo-maintenance-mode

このコマンドを活用と、この機能が有効か無効かどうかを表示できます。次のサンプル出力は、**show geo-maintenance-mode** コマンドのためにあります：

```
[smf] smf# show geo-maintenance-mode
result "geo-maintenance-mode is disabled"
```

```
[smf] smf# show geo-maintenance-mode
result "geo-maintenance-mode is enabled"
```

### show georeplication checksum instance-id

etcd および cache-pod データの複製の詳細を表示するには、このコマンドを使用します。次のサンプル出力は、**show georeplication checksum instance-id** コマンドのためにあります：

```
[smf] smf# show georeplication checksum instance-id
Value for 'instance-id' (<string>): 1
checksum-details
--       ----  --------
ID       Type  Checksum
--       ----  --------
1        ETCD  1646812528
IPAM     CACHE 1646812528
NRFMgmt CACHE 1646812528
```

### show georeplication-status

このコマンドを使用して、Geo セットアップの 2 つのラック間の重複ステータスを表示します。

接続が成功すると、次の出力例が表示されます。

```
[smf] smf# show georeplication-status
result "pass"
```

エラーがある場合、次の出力例が表示されます。

```
[smf] smf# show georeplication-status
result "fail: [424] checksum missmatch"
```

### show helm

**show helm** コマンドは、SMF システム イメージのバージョン情報を表示します。

## ipam pool を表示

| フィールド | 説明 |
|---|---|
| PoolName | アドレス プールの名前。 |
| Ipv4Utilization | このプールのIPv4アドレスの使用率（% 単位）。 |
| Ipv6AddrUtilization | このプールの IPv6 アドレスの使用率（% 単位）。 |
| Ipv6PrefixUtilization | このプールの IPv6 プレフィックス アドレスの使用率（% 単位）。 |

### show ipam pool <pool-name>

| フィールド | 説明 |
|---|---|
| Ipv4Addr [Total/Used/Utilization] | 使用可能な（このプールに構成されている）IPv4 アドレスの合計/使用済みアドレスの数/IPv4 アドレスの使用率。 |
| Ipv6Addr [Total/Used/Utilization] | 使用可能な（このプールに構成されている）IPv6 アドレスの合計/使用済みアドレスの数/IPv6 アドレスの使用率。 |
| Ipv6Prefix [Total/Used/Utilization] | 使用可能な（このプールに構成されている）IPv6プレフィックスアドレスの合計/使用済みアドレスの数/IPv6 プレフィックスの使用率 |

### show ipam pool <pool-name> ipv4-addr

| フィールド | 説明 |
|---|---|
| StartAddress | 範囲の開始アドレス。 |
| EndAddress | 範囲の終了アドレス。 |
| AllocContext | このアドレス範囲が割り当てられているデータ プレーンの名前。 |
| フラグ | フラグ：気象プールが静的か、オフラインかどうかを示します。 |

### show ipam pool <pool-name> ipv6-addr

| フィールド | 説明 |
|---|---|
| StartAddress | 範囲の開始アドレス。 |
| EndAddress | 範囲の終了アドレス。 |

| フィールド | 説明 |
|---|---|
| AllocContext | このアドレス範囲が割り当てられているデータ プレーンの名前。 |
| フラグ | フラグ：気象プールが静的か、オフラインかどうかを示します。 |

**show ipam pool <pool-name> ipv6-prefix**

| フィールド | 説明 |
|---|---|
| StartAddress | 範囲の開始アドレス。 |
| EndAddress | 範囲の終了アドレス。 |
| AllocContext | このアドレス範囲が割り当てられているデータ プレーンの名前。 |
| フラグ | フラグ プールが静的か、オフラインの場合はS（静的）およびO（オフライン）を示します。 |

**ipam dp を表示**

| フィールド | 説明 |
|---|---|
| dp-name | 登録されているデータプレーンの名前。 |
| Ipv4Utilization | このデータ プレーンによる IPv4 の使用率（%）。 |
| Ipv6AddrUtilization | このデータ プレーンの IPv6 アドレスの使用率（% 単位）。 |
| Ipv6PrefixUtilization | このデータ プレーンの IPv6 プレフィックス アドレスの使用率（% 単位）。 |

**show ipam dp <dataplane-name>**

| フィールド | 説明 |
|---|---|
| Ipv4Addr [Total/Used/Utilization] | 使用可能な（このデータ プレーンに構成された）IPv4 アドレスの合計 / 使用済みアドレスの数 / IPv4 の使用率。 |
| Ipv6Addr [Total/Used/Utilization] | 使用可能な（このデータプレーンに構成された）IPv6 アドレスの合計 / 使用済みアドレスの数 / IPv6 の使用率。 |

| フィールド | 説明 |
| --- | --- |
| Ipv6Prefix [Total/Used/Utilization] | 使用可能な（このデータ プレーンに構成された）IPv6 プレフィックス アドレスの合計 / 使用済みアドレスの数 / IPv6 プレフィックスの使用率。 |

**show ipam dp <dataplane-name> ipv4-address**

| フィールド | 説明 |
| --- | --- |
| StartAddress | 範囲の開始アドレス。 |
| EndAddress | 範囲の終了アドレス。 |
| ルート | このデータ プレーンに割り当てられたルートです。 |
| N/P | ルート フラグの表示 S（静的）および O（オフライン）を受信した NodeMgr インスタンス ID を表示します。 |

**show ipam pool <pool-name> ipv6-addr**

| フィールド | 説明 |
| --- | --- |
| StartAddress | 範囲の開始アドレス。 |
| EndAddress | 範囲の終了アドレス。 |
| AllocContext | このアドレス範囲が割り当てられているデータ プレーンの名前。 |
| フラグ | フラグ：気象プールが静的か、オフラインかどうかを示します。 |

**show ipam**

| フィールド | 説明 |
| --- | --- |
| PoolName | Ipv4Utilization、Ipv6AddrUtilization、および Ipv6PrefixUtilization を表示します。 |
| DpName | Ipv4Utilization、Ipv6AddrUtlization、および Ipv6PrefixUtlization を表示します。 |

## show nrf 登録情報

表 *558 : show nrf registration-info* コマンド出力の説明

| フィールド | 説明 |
|---|---|
| NF ステータス | NRF 登録情報を表示します。 |
| 登録時間 | NRF への登録の時刻を表示します。 |
| アクティブな MgmtEP 名 | アクティブな NRF 管理エンドポイント名を表示します。 |
| ハートビート期間 | ハートビート期間を表示します。 |
| Uri | URI 情報を表示します。 |
| ホスト タイプ（Host Type） | NRF ホスト タイプ情報を表示します。 |
| GR インスタンス ID | GR インスタンス ID を表示。 |

## show nrf subscription-info

表 *559 : show nrf subscription-info* コマンド出力の説明

| フィールド | 説明 |
|---|---|
| NF インスタンス ID | NF インスタンス ID を表示します。 |
| SubscriptionID | サブスクリプション識別情報を表示します。 |
| 実際の有効期間 | NRF サーバから受信した実際の有効時間を表示します。 |
| 要求された有効期間 | NF 要求された有効なサブスクリプション時間を表示します。 |
| GR インスタンス ID | GR インスタンス ID を表示。 |

## show nrf discovery info

表 *560 : show nrf discovery info* コマンド出力の説明

| フィールド | 説明 |
|---|---|
| NF タイプ | NF タイプ情報を表示します。 |
| 検出フィルタの数 | 検出フィルタの数を表示します。 |

| フィールド | 説明 |
|---|---|
| NFプロファイルの数 | NF プロファイルの数の表示 |
| GR インスタンス ID | GR インスタンス ID を表示。 |

### show nrf discovery-info AMF discovery-filter

表 *561 : show nrf discovery-info AMF discovery-filter* コマンド出力の説明

| ステップ | 説明 |
|---|---|
| 検出のフィルタ | 検出フィルタ情報を表示します。 |
| 期限切れ時間 | 検出フィルタの有効期限を表示します。 |
| GR インスタンス ID | GR インスタンス ID を表示。 |

### show nrf discovery-info AMF discovery-filter <discovery_filter>

表 *562 : nrf discovery-info AMF discovery-filter* を表示*<discovery_filter>*コマンドの説明

| フィールド | 説明 |
|---|---|
| NF InstanceId | NF インスタンス ID を表示します。 |
| NF タイプ | NF タイプ情報を表示します。 |
| 検出のフィルタ | 検出のフィルタ情報を表示します。 |
| NF ステータス | NF ステータス情報の表示 |
| 優先順位 | プライオリティ情報を表示します。 |
| キャパシティ | NF プロファイルのキャパシティ情報を表示します。 |
| 負荷 | ロード情報を表示します。 |
| 地域 | 地名情報を表示します。 |
| ipv4 address | この NF プロファイルの検出応答から受信した IPv4 アドレスを表示します。 |
| ipv6 address | この NF プロファイルの検出応答から受信した IPv6 アドレスを表示します。 |

### show nrf discovery-info AMF discovery-filter <discovery_name> nf-discovery-profile <nf_discovery_profile> nf-service

表 *563 : show nrf discovery-info AMF discovery-filter <discovery_name> nf-discovery-profile <nf_discovery_profile> nf-service Command Output Description*

| フィールド | 説明 |
|---|---|
| ServiceInstanceId | NF サービス インスタンス ID を表示します。 |
| ServiceName | NF サービス名を表示します。 |
| UriScheme | URI スキーム情報を表示します。 |

### show peers all

このコマンドを使用して、SMFによって確立されたすべての外部着信および発信接続のリストを表示します。キー情報だけが表示されます。次の出力例は、**show peers all** コマンドのためにあります：

```
[smf] smf# show peers all
GR                                                                                  POD
CONNECTED                                        INTERFACE
INSTANCE  ENDPOINT      LOCAL ADDRESS   PEER ADDRESS     DIRECTION  INSTANCE     TYPE
TIME       RPC     ADDITIONAL DETAILS       NAME       VRF
-------------------------------------------------------------------------------------------------------
1         <none>        xx.xx.xx.xx    xx.xx.xx.xx:0000  Outbound   rest-ep-0    Rest
25 hours   UDM     <none>                    n10
1         <none>        xx.xx.xx.xx    xx.xx.xx.xx:0000  Outbound   rest-ep-0    Rest
25 hours   UDM     <none>                    n10
1         <none>        xx.xx.xx.xx    xx.xx.xx.xx:0000  Outbound   rest-ep-0    Rest
25 hours   CHF     <none>                    n40
1         <none>        xx.xx.xx.xx    xx.xx.xx.xx:0000  Outbound   rest-ep-0    Rest
25 hours   PCF     <none>                    n7
1         <none>        xx.xx.xx.xx    xx.xx.xx.xx:0000  Outbound   rest-ep-0    Rest
25 hours   PCF     <none>                    n7
1         <none>        xx.xx.xx.xx    xx.xx.xx.xx:0000  Outbound   rest-ep-0    Rest
25 hours   AMF     <none>                    n11
```

表 *564 : show peers all* コマンドの出力フィールドの説明

| フィールド | 説明 |
|---|---|
| 詳細情報 | ステータスやタイプなど、ピアの追加の詳細を指定します。 |
| Connected Time | 接続されたピアの期間を指定します。 |
| 方向（Direction） | ピア接続方向がインバウンドかアウトバウンドかを指定します。 |
| エンドポイント | エンドポイントの名前を指定します。 |
| GR インスタンス | GR インスタンスを指定します。 |
| インターフェイス名（Interface Name） | エンドポイントのインスタンス名を指定します。 |

| フィールド | 説明 |
|---|---|
| Local Address | インスタンスのローカルIPアドレスとポートを指定します。エンドポイントの場合、エンドポイントのアドレスとポートです。RPCの場合は、インスタンス IP です。 |
| ピア アドレス\| | ピア アドレスのホストおよびポートを指定します。 |
| ポッド インスタンス | ピアのポッドを指定します。 |
| RPC | 特定のピアの rpc を指定します。 |
| タイプ | ピアのタイプを指定します。 |

## show resources

クラスタ内のすべてのポッドのリソース情報を一覧表示するには、このコマンドを使用します。次の出力例は、**show resources** コマンドのためにあります：

```
[smf] show resources
                          TOTAL    USED     DISK
                          NODE     POD      USAGE   GO                GC
                   CPU    MEMORY   MEMORY   IN      ROUTINES  GC      PAUSE
POD INSTANCE       USAGE  IN MB    IN MB    KBPS    COUNT     COUNT   IN NS
-------------------------------------------------------------------------------
bfdmgr-1           0      32117    56       0       56        1950    56
bfdmgr-2           0      32117    55       0       56        1935    55
bfdmgr-3           1      32117    54       0       56        2636    54
bfdmgr-4           0      32117    55       0       56        1946    55
bgpspeaker-pod-1   1      32117    104      0       94        9315    104
bgpspeaker-pod-2   1      32117    102      0       78        9300    102
cache-pod-1        4      7962     96       0       325       778     96
cache-pod-2        10     32117    91       0       325       778     91
gtpc-ep-0          2      32117    82       0       160       777     82
internal-gr-pod-1  2      32117    124      0       317       63      124
internal-gr-pod-2  1      32117    93       0       182       63      93
li-ep-0            0      32117    64       0       68        2723    64
nodemgr-0          3      32117    113      0       270       784     113
nodemgr-1          2      32117    115      0       252       784     115
oam-pod-0          3      7962     121      0       249       2110    121
protocol-0         2      32117    82       0       159       777     82
radius-ep-0        5      32117    76       0       145       782     76
rest-ep-0          3      32117    105      0       298       779     105
sgw-service-0      9      32117    138      0       262       779     138
smf-service-0      3      32117    228      0       347       2645    228
udp-proxy-0        0      32117    72       0       112       778     72
udp-proxy-1        0      32117    72       0       112       778     72
```

表 *565* : ***show resources*** コマンドの出力フィールドの説明

| フィールド | 説明 |
|---|---|
| CPU 使用率 | CPU 使用率を指定します。 |

| フィールド | 説明 |
|---|---|
| ディスク使用量（Kbps） | ディスク使用率（Kbps）を指定します。 |
| GC 数 | ガベージ コレクションのサイクル数を指定します。 |
| NS での GC 一時停止 | ガベージ コレクションの一時停止をナノ秒単位で指定します。 |
| Go ルート数 | go ルーチンの数を指定します。 |
| ポッド インスタンス | ポッドのインスタンス情報を指定します。 |
| 合計ノードメモリ（MB） | ノードの合計メモリ使用量を MB 単位で指定します。 |
| 使用済みポッド メモリ（MB） | ポッド メモリの消費量を MB 単位で指定します。 |

## show rpc all

**show rpc all** コマンドを使用して、RPC およびリモート ホスト情報を持つすべてのポッドからのすべての RPC のリストを表示します。

次の出力例は、**show rpc all** コマンドのためにあります：

```
[smf] smf# show rpc all | tab | nomore
```

```
     PROCESSING

                                                                CONNECTED  DISCONNECTED  MONITOR
  INSTANCE
POD INSTANCE       NAME                          REMOTE ADDRESS              REMOTE HOST
      TYPE                    SET NAME          STATUS    TIME       TIME          RPCHOST
  INFO                                               VERSION
-------------------------------------------------------------------------------------------------
cache-pod-1        cache-pod-affinity            xx.xx.xx.xx:0000           cache-pod_20
       Grpc                    cache-pod_2       Started   4 weeks    <none>        false
    <none>                                            <none>
cache-pod-1        cache-pod-affinity            xx.xx.xx.xx:0000           cache-pod_10
       Grpc                    cache-pod_1       Started   4 weeks    <none>        false
    <none>                                            <none>
cache-pod-1        stream_cache-pod-affinity     xx.xx.xx.xx:0000           cache-pod_10
       GrpcServerClientStream  cache-pod_1       Started   4 weeks    <none>        false
    <none>                                            <none>
cache-pod-1        stream_cache-pod-affinity     xx.xx.xx.xx:0000           cache-pod_20
       GrpcServerClientStream  cache-pod_2       Started   4 weeks    <none>        false
    <none>                                            <none>
cache-pod-1        oam-pod                       xx.xx.xx.xx:0000           oam-pod
       GrpcStream              <none>            Started   4 weeks    <none>        false
```

```
    <none>                                                  <none>
cache-pod-1        Replication                 xx.xx.xx.xx:0000          cachepod_1
       GrpcStream              <none>           Started   3 weeks    <none>        false
    <none>                                                  <none>
cache-pod-1        Replication                 xx.xx.xx.xx:0000          cachepod_2
       GrpcStream              <none>           Started   3 weeks    <none>        false
    <none>                                                  <none>
cache-pod-2        cache-pod-affinity          xx.xx.xx.xx:0000          cache-pod_10
       Grpc                    cache-pod_1      Started   4 weeks    <none>        false
    <none>                                                  <none>
:
:
cache-pod-2        cache-pod-affinity          xx.xx.xx.xx:0000          cache-pod_20
       Grpc                    cache-pod_2      Started   4 weeks    <none>        false
    <none>                                                  <none>
cache-pod-2        stream_cache-pod-affinity   xx.xx.xx.xx:0000          cache-pod_20
       GrpcServerClientStream  cache-pod_2      Started   4 weeks    <none>        false
    <none>                                                  <none>
cache-pod-2        stream_cache-pod-affinity   xx.xx.xx.xx:0000          cache-pod_10
       GrpcServerClientStream  cache-pod_1      Started   4 weeks    <none>        false
    <none>                                                  <none>
cache-pod-2        oam-pod                     xx.xx.xx.xx:0000          oam-pod
       GrpcStream              <none>           Started   4 weeks    <none>        false
    <none>                                                  <none>
cache-pod-2        Replication                 xx.xx.xx.xx:0000          cachepod_1
       GrpcStream              <none>           Started   3 weeks    <none>        false
    <none>                                                  <none>
cache-pod-2        Replication                 xx.xx.xx.xx:0000          cachepod_2
       GrpcStream              <none>           Started   3 weeks    <none>        false
    <none>                                                  <none>
example-rest-ep-1  example-service           example-service:0000      example-service0
    Grpc                    example-service  Started   2 weeks    <none>        true
  example.example-service.cluster1.example-data.12  <none>
```

**表 *566* : *show rpc* コマンドの出力フィールドの説明**

| フィールド | 説明 |
|---|---|
| Connected Time | RPC ホストが接続されている期間を指定します。 |
| 切断時刻 | RPC ホストが切断されている時間を指定します。 |
| RPC ホストのモニタリング | RPC ホストの接続ステータスをモニタしているかどうかを示します。 |
| 名前 | ポッドに登録されている RPC の名前を表示します。 |
| ポッド インスタンス | ポッドのインスタンス情報を表示します。 |
| インスタンス情報の処理 | 使用可能な場合、処理インスタンス名を示します。 |
| リモートアドレス | リモートエンドポイントの IP アドレスとポートを表示します。 |

| フィールド | 説明 |
|---|---|
| リモート ホスト | RPC ホストの名前が表示されます。 |
| セット名 | RPC ホストのグループの RPC セット名を表示します。 |
| ステータス | RPCホストの現在のステータスを表示します。ステータス値は、[開始済み（Started）]、[開始中（Starting）]、および [停止済み（Stopped）] です。 |
| タイプ | Rest、Grpc、GrpcStream などの接続のタイプを表示します。 |
| バージョン | RPCホストAPIのバージョンを表示します（該当する場合）。 |

### show running-status

このコマンドを使用して、システム内のすべてのポッドの実行中のステータス関連情報を表示します。次の出力例は、**show running-status** コマンドのためにあります：

```
[smf] smf# show running-status
                  RUNNING  SYSTEM  START
POD INSTANCE      STATUS   HEALTH  TIME
-----------------------------------------------
bfdmgr-1          Started  Normal  2 hours
bfdmgr-2          Started  Normal  2 hours
bgpspeaker-pod-1  Started  Normal  2 hours
bgpspeaker-pod-2  Started  Normal  2 hours
cache-pod-1       Started  Normal  2 hours
cache-pod-2       Started  Normal  2 hours
dns-proxy-0       Started  Normal  2 hours
dns-proxy-1       Started  Normal  2 hours
gtpc-ep1-1        Started  Normal  2 hours
gtpc-ep1-2        Started  Normal  2 hours
gtpc-ep2-1        Started  Normal  2 hours
gtpc-ep2-2        Started  Normal  2 hours
internal-gr-pod-1 Started  Normal  2 hours
internal-gr-pod-2 Started  Normal  2 hours
li-ep-0           Started  Normal  2 hours
li-ep-1           Started  Normal  2 hours
nodemgr-0         Started  Normal  2 hours
nodemgr-1         Started  Normal  2 hours
oam-pod-0         Started  Normal  2 hours
protocol1-1       Started  Normal  2 hours
protocol1-2       Started  Normal  2 hours
protocol2-1       Started  Normal  2 hours
protocol2-2       Started  Normal  2 hours
radius-ep-0       Started  Normal  2 hours
radius-ep-1       Started  Normal  2 hours
rest-ep-0         Started  Normal  2 hours
rest-ep-1         Started  Normal  2 hours
sgw-service-0     Started  Normal  2 hours
sgw-service-1     Started  Normal  2 hours
sgw-service-2     Started  Normal  2 hours
```

```
sgw-service-3      Started  Normal  2 hours
sgw-service-4      Started  Normal  2 hours
sgw-service-5      Started  Normal  2 hours
smf-service-0      Started  Normal  2 hours
smf-service-1      Started  Normal  2 hours
smf-service-2      Started  Normal  2 hours
smf-service-3      Started  Normal  2 hours
smf-service-4      Started  Normal  2 hours
smf-service-5      Started  Normal  2 hours
udp-proxy-0        Started  Normal  2 hours
udp-proxy-1        Started  Normal  2 hours
```

表 *567* : ***show running-status*** コマンドの出力フィールドの説明

| フィールド | 説明 |
|---|---|
| ポッド インスタンス | ポッドのインスタンス情報を指定します。 |
| 実行ステータス | システム実行ステータス（Starting、Started、Stopping、またはStopped）を指定します。 |
| 開始時刻 | アプリケーションの開始時刻を指定します。 |
| システムの状態（System Health） | アプリケーションの正常性ステータスを指定します。 |

## show sessions affinity

このコマンドを使用して、ポッドインスタンスに関するアフィニティ数を表示します。このアフィニティ数は、ポッドに対するセッションのアフィニティを定義します。次の出力例は、**show sessions affinity** コマンドのためにあります：

```
[smf] smf# show sessions affinity
POD
INSTANCE    COUNT
------------------
service-1   10
service-11  12
service-12  15
service-13  12
service-14  15
service-2   15
service-3   14
service-4   19
```

表 *568* : ***show sessions affinity*** コマンドの出力フィールドの説明

| フィールド | 説明 |
|---|---|
| Count | アフィニティ カウントを指定します。 |
| ポッド インスタンス | ポッドのインスタンス情報を指定します。 |

### show sessions commit-pending

このコマンドを使用して、ポッドごとの現在のセッション数と、データベース内のコミットが保留中のセッションを表示します。次の出力例は、**show sessions commit-pending** コマンドのためにあります：

```
[smf] smf# show sessions commit-pending
                                        DB
               GR                PENDING  BINARY  LAST DB SYNC
POD INSTANCE   INSTANCE  COUNT   COMMIT   SIZE    TIME
-------------------------------------------------------------------
sgw-service-1  1         0       0        0       Less than a second
sgw-service-1  2         0       0        0       Less than a second
sgw-service-2  1         0       0        0       Less than a second
sgw-service-2  2         0       0        0       Less than a second
sgw-service-4  1         0       0        0       Less than a second
sgw-service-4  2         0       0        0       Less than a second
sgw-service-5  1         0       0        0       Less than a second
sgw-service-5  2         0       0        0       Less than a second
smf-service-0  1         0       0        0       Less than a second
smf-service-0  2         0       0        0       Less than a second
smf-service-1  1         0       0        0       Less than a second
smf-service-1  2         0       0        0       Less than a second
smf-service-2  1         0       0        0       Less than a second
smf-service-2  2         0       0        0       Less than a second
smf-service-4  1         0       0        0       Less than a second
smf-service-4  2         0       0        0       Less than a second
smf-service-5  1         0       0        0       Less than a second
smf-service-5  2         0       0        0       Less than a second
```

表 *569* : ***show sessions commit-pending*** コマンドの出力フィールドの説明

| フィールド | 説明 |
|---|---|
| Count | カウントを指定します。 |
| DB バイナリサイズ | DB バイナリ サイズを指定します。 |
| GR インスタンス | GR インスタンス ID を指定します。 |
| 最終 DB 同期時刻 | 以前の DB 同期時刻を指定します。 |
| ポッド インスタンス | ポッドのインスタンス情報を指定します。 |

### show subscriber

このコマンドは、既存の show subscriber CLI 出力と新しく追加された CLI 出力を表示します。

*Table 570: show subscriber* コマンド出力の説明

| フィールド | 説明 |
|---|---|
| すべて | すべての SUPI または IMEI の情報を表示します。 |
| amf | AMF アドレスを表示します。 |
| chf | CHF アドレスを表示します。 |
| count | セッション数を表示します。 |
| debug | デバッグ情報を表示します。 |
| dnn | DNN 値を表示します。 |
| gr-instance | 地理的冗長性（GR）インスタンスを表示します。 |
| gtp-peer | GTP ピア アドレスを表示します。 |
| imei | 15 または 16 桁を含む IMEI を表示します。 |
| 名前空間 | **Important**<br>このキーワードはリリース 2021.02.0 で廃止され、 **nf-service** キーワードに置き換えられました。<br><br>検索対象の製品名前空間を表示します。デフォルト：なし。 |
| nf-service { none \| sgw \| smf } | 検索対象のネットワーク機能サービスを表示します。デフォルト：なし。 |
| pcf | PCF アドレスを表示します。 |
| ネズミ | RAT タイプを 4G または 5G として表示します。 |
| ローミング ステータス | UE ローミング ステータスを表示します：homer、visitor-lbo、visitor-hr、roamer。 |
| supi | SUPI 値を表示します。 |
| udm | UDM アドレスを表示します。 |
| upf | UPF アドレスを表示します。 |
| rulebase | ルールベースを使用してサブスクライバを表示します。 |
| \| | 出力修飾子。 |

## show subscriber all

このコマンドを使用して、すべての SUPI および NF サービスのすべてのセッションを表示します。次の出力例は、**show subscriber all** コマンドのためにあります：

```
[smf] smf# show subscriber all
subscriber-details
{
  "subResponses": [
    [
      ""
    ],
    [
      "id-index:1:0:32768",
      "id-value:16777505",
      "imsi:imsi-123456123456123",
      "msisdn:msisdn-123456123456123",
      "imei:imei-310220000000000",
      "upf:xx.xx.xx.xx",
      "upfEpKey: xx.xx.xx.xx: xx.xx.xx.xx ",
      "s5s8Ipv4: xx.xx.xx.xx ",
      "s11Ipv4: xx.xx.xx.xx",
      "namespace:sgw",
      "nf-service:sgw"
    ],
    [
      "roaming-status:roamer",
      "ue-type:4g-only",
      "supi:imsi-123456123456123",
      "gpsi:msisdn-123456123456123",
      "pei:imei-310220000000000",
      "psid:69",
      "dnn:papn1.com",
      "emergency:false",
      "rat:e-utran",
      "access:3gpp access",
      "connectivity:4g",
      "auth-status:authenticated",
      "pcfGroupId:PCF-*",
      "policy:2",
      "pcf: xx.xx.xx.xx",
      "ipv4-addr:pool-static1-v4/xx.xx.xx.xx",
      "ipv4-pool:pool-static1-v4",
      "ipv4-range:pool-static1-v4/xx.xx.xx.xx",
      "ipv4-startrange:pool-static1-v4/",
      "id-index:1:0:32768",
      "id-value:8/310",
      "upf:xx.xx.xx.xx",
      "chfGroupId:CHF-*",
      "chf:209.165.202.133",
      "gtp-peer:xx.xx.xx.xx",
      "peerGtpuEpKey:xx.xx.xx.xx:xx.xx.xx.xx",
      "namespace:smf",
      "nf-service:smf"
    ],
    [
      ""
    ]
  ]
}
```

*Table 571: show subscriber* コマンド出力の説明

| フィールド | 説明 |
|---|---|
| subscriber-details | すべてのサブスクライバの詳細を JSON 形式で表示します。 |

## show subscriber count

このコマンドは、count CLI コマンドの CLI オプションを表示します。

表 *572 : show subscriber* コマンド出力の説明

| フィールド | 説明 |
|---|---|
| すべて | すべての SUPI を表示します。 |
| amf | AMF アドレスを表示します。 |
| apn | APN 値を表示します。 |
| auth-status | RADIUS 認証ステータス（認証済みまたは未認証ステータス）を表示します。 |
| chf | CHF アドレスを表示します。 |
| 接続性 | 接続性（4g または 5g）を表示します。 |
| dnn | DNN 値を表示します。 |
| emergency | 緊急セッションの指示（true または false）を表示します。 |
| gpsi | GPSI 値を表示します。 |
| gr-instance | 指定された GR インスタンスからのサブスクライバの を表示します。 |
| gtp-peer | GTP ピア アドレスを表示します。 |
| ipv4-addr | 次の形式で IPv4 アドレスを表示します:-<poolName>または<ipv4-addr>。 |
| ipv4-pool | IPv4 プール名を表示します。 |
| ipv4-range | IPv4 アドレスの範囲を表示します。 |
| IPv6-pfx | 次の形式で IPv6 プレフィックスを表示します。<poolName>または<ipv6-pfx> |
| ipv6-pool | IPv6 プール名を表示します。 |
| ipv6-range | IPv6 プレフィックス範囲を表示します。 |
| msid | MSID 値を表示します。 |
| msisdn | MSISDN の値を表示します。 |

| フィールド | 説明 |
|---|---|
| 名前空間 | 廃止されたオプションを表示します。代わりに nf-service を使用してください（デフォルト：none）。 |
| nf-service | 検索対象のネットワーク機能サービス（SMF、S-GW）を表示します（デフォルト：none）。<br>このパラメータは、次の形式で、SMF のスライス名または NSSAI フィルタと併用できます。<br>**nf-service smf** *slice-name* または、**nf-service smf** *nssai*。 |
| pcf | PCF アドレスを表示します。 |
| peerGtpuEpKey | <upf_addr:gptu-peer-addr> 形式の GTPU ピア アドレスを表示します。 |
| pei | PEI（Permanent Equipment Identifier）を表示します。 |
| policy | サブスクライバ ポリシー情報を表示します。 |
| ネズミ | RAT タイプを 4G または 5G として表示します。 |
| ローミング ステータス | UE ローミング ステータス（homer/roamer/visitor-hr/lbo-visitor）を表示します。 |
| smf | SMF アドレスを表示します。 |
| Supi | 特定の SUPI 値を表示します。 |
| udm-sdm | UDM-SDM アドレスを表示します。 |
| udm-uecm | UDM-UECM アドレスを表示します。 |
| ue-type | デバイス機能（4g のみまたは nr 対応）を表示します。 |
| upf | UPF アドレスを表示します。 |
| rulebase | ルールベースを使用してサブスクライバを表示します。 |
| \| | 出力修飾子を表示します。 |

## show subscriber count all

このコマンドを使用して、すべてのSUPIのセッションの合計数を表示します。次の出力例は、**show subscriber count all** コマンドのためにあります：

```
[smf] smf# show subscriber count all
subscriber-details
{
  "sessionCount": 20
}
```

表 *573 : show subscriber count all* コマンドの出力フィールドの説明

| フィールド | 説明 |
|---|---|
| subscriber-details | すべてのサブスクライバの数が JSON 形式で表示されます。 |

## show subscriber debug-info

このコマンドは、PSID 値がオプションである特定の SUPI 値のデバッグ情報を表示します。

表 *574 : show subscriber debug-info* コマンド出力の説明

| フィールド | 説明 |
|---|---|
| gpsi | GPSI 値を表示します。 |
| gr-instance | 指定された GR インスタンスからのサブスクライバの を表示します。 |
| imsi | IMSI 値を表示します。 |
| msid | MSID 値を表示します。 |
| msisdn | MSISDN の値を表示します。 |
| 名前空間 | 廃止されたオプション。代わりに nf-service を使用してください（デフォルト： none）。 |
| nf-service | 検索対象のネットワーク機能サービス（SMF、SGW）を表示します（デフォルト：none）。 |
| pei | PEI または IMEI 値を表示します。 |
| Supi | SUPI 値を表示します。値には imsi- プレフィックスが含まれている必要があります。 |
| \| | 出力修飾子を表示します。 |

## show subscriber gpsi

表 *575 : show subscriber gpsi*

| フィールド | 説明 |
|---|---|
| policy | ポリシー情報を表示します。 |
| ipv4-addr | IPv4 プール名を表示します。 |
| dnn | DNN 値を表示します。 |
| pcf | PCF アドレスを表示します。 |

| フィールド | 説明 |
|---|---|
| ネズミ | RAT タイプ（nr、e-utran、または wlan）の情報を表示します。 |
| 接続性 | 接続性（4G または 5G）を表示します。 |
| ipv4-range | IPv4 アドレスの範囲を表示します。 |
| chf | CHF アドレスを表示します。 |
| pei | 永久機器 ID（PEI）を表示します。 |
| udm | UDM アドレスを表示します。 |
| upfEpKey | UPF アドレス EP キー情報を表示します。 |
| IPv6-pfx | IPv6 プレフィックス情報を表示します。 |
| ipv6-pool | IPv6 プール名を表示します。 |
| chfGroupId | CHF アドレス グループ ID 情報を表示します。 |
| gpsi | Generic Public Subscription Identifier（GPSI）を表示します。 |
| pcfGroupId | PCF アドレス グループ ID を指定します。 |
| upf | UPF アドレスを表示します。 |
| ipv4-pool | IPv4 プール名を表示します。 |
| ipv6-range | IPv4 アドレスの範囲を表示します。 |
| amf | AMF アドレスを表示します。 |
| supi | SUPI 値を表示します。 |
| アクセス | アクセス情報を表示します。 |
| gr-instance | GR インスタンスを表示します。 |

## show subscriber nf-service smf

重要　リストされているフィルタではワイルド カード入力はサポートされていません。

表 *576 : clear subscriber nf-service smf* コマンド出力の表示

| フィールド | 説明 |
|---|---|
| apn | APN 値を表示します。 |

| フィールド | 説明 |
|---|---|
| msid | MSID 値を表示します。 |
| msisdn | MSISDN の値を表示します。 |
| ローミングステータス | UE ローミングステータスを表示します：homer、visitor-lbo、visitor-hr、roamer。 |
| smf | vSMF または hSMF の IP アドレス値に基づいてサブスクライバ詳細を表示します。<br>次に例を示します。<br>`[smf] smf# show subscriber nf-service smf smf <smf_url> subscriber-details`<br>`{}` |
| rulebase | ルールベースを使用してサブスクライバを表示します。 |

## show subscriber pei

*表 577 : show subscriber pei*

| フィールド | 説明 |
|---|---|
| policy | ポリシー情報を表示します。 |
| ipv4-addr | IPv4 プール名を表示します。 |
| dnn | DNN 値を表示します。 |
| pcf | PCF アドレスを表示します。 |
| ネズミ | RAT タイプ（nr、e-utran、または wlan）の情報を表示します。 |
| 接続性 | 接続性（4G または 5G）を表示します。 |
| ipv4-range | IPv4 アドレスの範囲を表示します。 |
| chf | CHF アドレスを表示します。 |
| pei | 永久機器 ID（PEI）を表示します。 |
| udm | UDM アドレスを表示します。 |
| upfEpKey | UPF アドレス EP キー情報を表示します。 |
| IPv6-pfx | IPv6 プレフィックス情報を表示します。 |
| ipv6-pool | IPv6 プール名を表示します。 |
| chfGroupId | CHF アドレス グループ ID 情報を表示します。 |

| フィールド | 説明 |
|---|---|
| gpsi | Generic Public Subscription Identifier（GPSI）を表示します。 |
| pcfGroupId | PCF アドレス グループ ID を示します。 |
| upf | UPF アドレスを表示します。 |
| ipv4-pool | IPv4 プール名を表示します。 |
| ipv6-range | IPv4 アドレスの範囲を表示します。 |
| amf | AMF アドレスを表示します。 |
| supi | SUPI 値を表示します。 |
| アクセス | アクセス情報を表示します。 |
| gr-instance | GR インスタンスを表示します。 |
| rulebase | ルールベースを使用してサブスクライバを表示します。 |

### show subscriber supi <supi_value> nf-service smf psid <psid_value> full

このコマンドは、詳細サブスクライバ情報を表示します。

***表 578 : show subscriber supi <supi_value> nf-service smfpsid <psid_value> full Command Output Description***

| フィールド | 説明 |
|---|---|
| sessTimeStamp | セッションの接続時間を表示します。 |
| callDuration | 通話の継続時間が表示されます。 |
| commonId | 当該セッションに相当するコール ID（共通 ID）を表示します。 |
| ipPool、ipv6Pool | アドレスが割り当てられている IP プールを表示します。 |
| linkedEbi | セッションに対してリンクされた EBI を表示します。 |
| snssai | sNsai の詳細を表示します。 |
| smfIwkEpsInd | AMF および UDM データに基づいて SMF EPS IWK の決定を表示します。 |
| TotalNumberOfPdrs | 関連付けられた PDR の数を表示します。 |
| TotalNumberOfFars | 関連付けられた PDR の数を表示します。 |
| Qers の合計数 | 関連付けられた QER の数を表示します。 |

| フィールド | 説明 |
|---|---|
| TotalNumberOfUrrs | 関連付けられた URR の数を表示します。 |
| upfSeid | 特定の UPF セッションのリモート SEID を表示します。 |
| epsInterworking Indication | AMF の EPS インターワーキング指示ステータスを表示します。 |
| ebi | 各フローに割り当てられた EAB ID を表示します。 |
| revalidationTime | セッションの再検証タイマー情報を表示します。 |

### show subscriber supi <supi_value> nf-service smfpsid <psid_value> summary

このコマンドは、詳細なサブスクライバ情報を表示します。このコマンドは、使いやすさが向上し、デバッグ目的で使用できます。

*表 579 : show subscriber supi <supi_value> nf-service smf psid <psid_value> summary Command Output Description*

| フィールド | 説明 |
|---|---|
| Supi | 5G サブスクリプションの永久識別子を表示します。 |
| pduSessionId | PDU セッション ID を表示します。 |
| pduSesstype | PDU セッション タイプを表示します。 |
| accessType | アクセス タイプを表示します。 |
| dnn | DNN プロファイル名を表示します。 |
| allocatedIp/ allocatedIpv6 | 割り当てられた IP アドレスの詳細を表示します。 |
| ratType | RAT タイプを表示します。 |
| sessTimeStamp | セッションの接続時間を表示します。 |
| TotalDynamicRules/ TotalStaticRules/ TotalPredefinedRules | ダイナミック ルールまたはスタティック ルールまたは事前定義ルールの数が表示されます。 |
| TotalGBRFlows/TotalNonGBRflows | GBR フローまたは GBR 以外のフローの数が表示されます。 |
| pcfInteraction | PCF インタラクション ステータス |
| ruleBase | ルールベース名を表示します。 |
| chargingId | 課金記述子名を表示します。 |
| offlineConverted | オフラインに変換されたオンライン課金パラメータを表示します。 |

| フィールド | 説明 |
|---|---|
| chargingDisabled | 課金が無効な場合の課金パラメータを表示します。 |
| dropTraffic | トラフィックがドロップされた場合の課金パラメータを表示します。 |
| gtppGrp | GTPP 名の EGCDR 構成を表示します。 |
| profileName | 課金プロファイル名を表示します。 |
| deferredUsageCount | 遅延マルチユニット使用率の数が表示されます。 |
| smfSeid | 特定の UPF セッションのローカル SEID を表示します。 |
| upfSeid | 特定の UPF セッションのリモート SEID を表示します。 |
| TunnelID | GTPU ピア トンネル ID を表示します。 |
| TunnelName | GTPU ピア トンネル名を表示します。 |
| RemoteTeid (teid/ipAddr) | GTPU ピア TEID および IP アドレスを表示します。 |
| TotalNumberOfPdrs | 関連付けられた PDR の数を表示します。 |
| TotalNumberOfFars | 関連付けられた PDR の数を表示します。 |
| Qers の合計数 | 関連付けられた QER の数を表示します。 |
| TotalNumberOfUrrs | 関連付けられた URR の数を表示します。 |

## clear コマンド

このセクションでは、問題のトラブルシューティングに使用できる主要な clear コマンドの一部を示します。

**重要** SMF Ops センターでは、一度に 1 つの **clear subscriber all** コマンドのみを発行できます。Ops センターは、進行中の **clear subscriber all** コマンドが完了するまで、後続の **clear subscriber all** および **clear subscriber** コマンドの他のバリアントを制限します。

**（注）** Ops Center には、進行中の bulk **clear subscriber** CLI コマンドの予想待機時間が表示されます。さらに、以前の CLI の処理が進行している間、クリア サブスクライバ CLI がブロックされます。

## clear subscriber

"clear subscriber" コマンドは、サブスクライバ SMF フィールドのリストを表示します。

**表 *580 : clear subscriber* コマンド出力の説明**

| フィールド | 説明 |
|---|---|
| すべて | すべてのセッション情報をクリアします。 |
| amf | AMF アドレス情報に基づいてサブスクライバをクリアします。 |
| chf | CHF アドレス情報に基づいてサブスクライバをクリアします。 |
| dnn | DNN 値に基づいてサブスクライバをクリアします。 |
| gr-instance | 指定した地理的冗長性（GR）インスタンス情報に基づいてサブスクライバをクリアします。 |
| gtp-peer | GTP ピア アドレス情報に基づいてサブスクライバをクリアします。 |
| ipv4-pool | IPv4 プール名に基づいてサブスクライバをクリアします。 |
| ipv4-range | IPv4 アドレス範囲値に基づいてサブスクライバをクリアします。 |
| ipv6-pool | IPv6 プール名情報に基づいてサブスクライバをクリアします。 |
| ipv4-range | IPv4 プレフィックス範囲値に基づいてサブスクライバをクリアします。 |
| ipv6-range | プレフィックス範囲値に基づいてサブスクライバをクリアします。 |
| 名前空間 | **重要**<br>このキーワードはリリース 2021.02.0 で廃止され、**nf-service** キーワードに置き換えられました。<br><br>それぞれの名前空間に基づいてサブスクライバをクリアします。デフォルト：なし。 |
| nf-service { none \| sgw \| smf } | 指定されたネットワーク機能サービスに基づいてサブスクライバをクリアします。デフォルト：なし。 |
| pcf | PCF アドレス情報に基づいてサブスクライバをクリアします。 |
| policy | ポリシーに基づいてサブスクライバをクリアします。 |
| purge | ローカルで消去された場合は、サブスクライバ情報をクリアします。 |
| 再アクティブ化 [ true \| false] | 再アクティブ化が必要な原因値に基づいて、サブスクライバをクリアします。再アクティブ化が要求された場合、このオプションは true に設定されます。 |

| フィールド | 説明 |
|---|---|
| ローミングステータス | UE ローミング ステータス（homer、visitor-lbo、visitor-hr、roamer values）に基づいてサブスクライバをクリアします。 |
| sgw | S-GW アドレス情報に基づいてサブスクライバ情報をクリアします。 |
| smf | SMF アドレス情報に基づいてサブスクライバ情報をクリアします。 |
| Supi | SUPI 値に基づいてサブスクライバをクリアします。 |
| rulebase | ルールベースを使用してサブスクライバをクリアします。 |
| \| | 出力修飾子。」 |

## clear subscriber nf-service smf

**重要** リストされているフィルタではワイルド カード入力はサポートされていません。

`clear subscriber nf-service smf` コマンドを実行すると、nf-service SMF フィールドのリストが表示されます。

**表 *581 : clear subscriber nf-service smf* コマンド出力の説明**

| フィールド | 説明 |
|---|---|
| apn | APN 値に基づいてサブスクライバをクリアします。 |
| dnn | DNN 値に基づいてサブスクライバをクリアします。 |
| msid | MSID 値に基づいてサブスクライバをクリアします。 |
| msisdn | 電話番号の値に基づいてサブスクライバをクリアします。 |
| rate | レート値に基づいてサブスクライバをクリアします。rate の最大値は 1500 です。 |
| 再アクティブ化 [ true \| false] | 再アクティブ化が必要の原因に基づいて、サブスクライバをクリアします。再アクティブ化が要求された場合、このオプションは true に設定されます。 |
| ローミングステータス | UE ローミングステータス（homer、visitor-lbo、visitor-hr、roamer）に基づいてサブスクライバをクリアします。 |

| フィールド | 説明 |
|---|---|
| rulebase | rulebase 値に基づいてサブスクライバをクリアします。<br>このキーワードは、セカンダリ フィルタとして使用します。ルールベースの値にルールベースのプレフィックスが含まれていることを確認します。<br>次に例を示します。<br>`[smf] smf# clear subscriber nf-service smf dnn <dnn_val> rulebase <rulebase_value>`<br>`result`<br>`ClearSubscriber Request submitted` |
| rulename | rulename の値に基づいてセッションを変更します。<br>このキーワードは、セカンダリ フィルタとして使用します。ルール名の値にルール名プレフィックスが含まれていることを確認してください。<br>次に例を示します。<br>`[smf] smf# clear subscriber nf-service smf dnn <dnn_val> rulename <rulename_value>`<br>`result`<br>`ClearSubscriber Request submitted` |
| smf | vSMF または hSMF の IP アドレス値に基づいてサブスクライバをクリアします。<br>次に例を示します。<br>`[smf] smf# clear subscriber nf-service smf smf <smf_url>`<br>`result`<br>`ClearSubscriber Request submitted` |
| x5qi | 5G セッションの場合は 5QI、4G および WLAN セッションの場合は QCI に基づいてセッションを変更します。このキーワードは、セカンダリ フィルタとして使用します。<br>例：<br>`smf] smf# clear subscriber supi <supi_val> x5qi <x5qi_value>`<br>`result`<br>`ClearSubscriber Request submitted`<br>`[smf] smf# clear subscriber apn <apn_val> x5qi <x5qi_value>`<br>`result`<br>`ClearSubscriber Request submitted` |

## clear subscriber supi imsi <imsi_value>

`clear subscriber supi imsi` *`imsi_value`* コマンドは、サブスクライバ SUPI IMSI 値 SMF フィールドのリストを表示します。

表 *582 : clear subscriber supi imsi <imsi_value>* コマンド出力の説明

| フィールド | 説明 |
|---|---|
| ebi | EPS ベアラー ID 値に基づいてサブスクライバをクリアします。 |
| imsi | IMSI 情報に基づいてサブスクライバをクリアします。 |
| purge | ローカルで消去された場合は、true をクリアします。 |
| \| | 出力修飾子。 |

### clear subscriber supi imsi <imsi_value> psid <psid_value>

"`clear subscriber supi imsi imsi_value psid psid_value`" コマンドは、サブスクライバ SUPI IMSI 値 SMF フィールドのリストを表示します。

表 *583 : clear subscriber supi imsi <imsi_value> psid <psid_value>* コマンド出力の説明

| フィールド | 説明 |
|---|---|
| ebi | EPS ベアラー ID 値に基づいてサブスクライバをクリアします。 |
| imsi | IMSI 情報に基づいてサブスクライバをクリアします。 |
| psid | サービス ID 値に基づいてサブスクライバをクリアします。 |
| purge | ローカルで消去された場合は、true をクリアします。 |
| \| | 出力修飾子。 |

# サブスクライバのモニタリングとプロトコルのモニタリング

## 機能説明

SMF は、Kubernetes 環境でのモニタ サブスクライバとモニタプロトコルをサポートしています。モニター ツールを使用すると、サブスクライバおよびプロトコルのメッセージをキャプチャできます。

このセクションでは、SMF の正常性を監視するための CLI コマンドについて説明します。

## モニター サブスクライバおよびモニター プロトコル機能の構成

### サブスクライバ セッションのモニタリング

SMF でサブスクライバをモニターするには、次の CLI コマンドを使用します：

**monitor subscriber [ capture-duration** *duration* **| gr-instance** *gr_instance_id* **| imei** *imei_id* **| imsi** *imsi_value* **| internal-messages [ yes ] | namespace**

**[ sgw | smf ] | nf-service [ sgw | smf ] | supi** *supi_id* **| transaction-logs [ yes ] ]**

注：

- **capture-duration** *duration*：モニタ サブスクライバを有効にする期間を秒単位で指定します。デフォルトは 300 秒（5 分）です。これは省略可能なパラメータです。
- **gr-instance** *gr_instance_id*：GR インスタンス ID を指定します。インスタンス ID 1 はローカル インスタンス ID を示しています。
- **imei** *imi_id*：サブスクライバ IMEI を指定します。例：123456789012345、*
- **imsi** *imsi_value*：サブスクライバ IMSI を指定します。たとえば、123456789、* などです。
- **internal-messages [ yes ]**：**yes** に設定されている場合、内部メッセージを有効にします。デフォルトでは、無効になっています。これは省略可能なパラメータです。
- **namespace [ sgw | smf ]**：指定した名前空間を有効にします。デフォルトでは、名前空間は none に設定されています。これは省略可能なパラメータです。

重要　このキーワードはリリース 2021.02.0 で廃止され、**nf-service** キーワードに置き換えられました。

- **nf-service [ sgw | smf ]**：指定した NF サービスを有効にします。デフォルトでは、nf-service は none に設定されています。

重要　**nf-service** キーワードは、リリース 2021.02 以降では **namespace** キーワードに置き換わります。

- **supi** *supi_id*：サブスクライバ ID を指定します。例：imsi-123456789、imsi-123*
- **transaction-logs [ yes ]**：**yes** に設定されている場合はトランザクション ログを有効にします。デフォルトでは、無効になっています。これは省略可能なパラメータです。

  トランザクション履歴ログを表示するには、**dump transactionhistory** コマンドを使用します。

（注）　最新のトランザクション ログは、トランザクション ログ サイズが 1024 の循環キューに保存されます。

**monitor subscriber** CLI コマンドは、複数の端末で同時に実行できます。たとえば、2 つのサブスクライバ（たとえば、imsi-123456789012345 と imsi-456780123456789）の 2 つの SMF Ops Center ターミナルで CLI を同時に実行して、次を実装します：

- モニター サブスクライバが有効になっている場合に期間をモニターします

- 指定したサブスクライバの内部メッセージを表示します。
- 指定したサブスクライバのトランザクション ログを表示します

端末1：次のコマンドは、指定されたサブスクライバのサブスクライバメッセージをモニターおよび表示します。

```
monitor subscriber supi imsi-123456789012345 capture-duration 1000 internal-messages yes
```

ターミナル 2：次のコマンドは、指定されたサブスクライバのトランザクショ ンログを監視し、表示します。

```
monitor subscriber supi imsi-456780123456789 capture-duration 500 internal-messages yes
 transaction-logs yes
```

キャプチャ期間が完了した後、 **Ctrl+C** キーを使用して CLI を停止します。キャプチャされたメッセージは並べ替えられ、ファイルに保存されます。保存されたファイルの一覧を取得するには、 **monitor subscriber list** CLI コマンドを使用します。

例：

```
monitor subscriber list
RELEASE_NAMESPACE: 'smf'
'monsublogs/subscriberID_imsi-*_AT_2019-10-22T09:19:05.586237087.txt.sorted'
monsublogs/subscriberID_imsi-123456789012345_AT_2019-10-22T09:20:11.122225534.txt.sorted
```

## サブスクライバ ダンプのモニタリング

ソートされたファイルを [SMF Ops Center] 画面に表示するには、次の CLI コマンドを使用します。

**monitor subscriber dump filename** *filename*

例：

```
monitor subscriber dump filename
monsublogs/subscriberID_imsi-123456789012345_AT_2019-10-22T09:20:11.122225534.txt.sorted
```

## インターフェイス プロトコルのモニタリング

SMF 上のインターフェイスプロトコルをモニターするには、次の CLI コマンドを使用します：

**monitor protocol { interface** *interface_name* **[ capture-duration** *duration* **| gr-instance***gr_instance* **| pcacp yes | | ] | list [ | ] }**

**注**：

- **interface** *interface_name*：PCAP がキャプチャされるインターフェイス名を指定します。この CLI では、1 つの CLI コマンドで複数のインターフェイス名を設定できます。
- **capture-duration** *duration*：pcap がキャプチャされる期間を秒単位で指定します。デフォルトは 300 秒（5 分）です。
- 構成されたインターフェイス名は **show endpoint** 、 CLI コマンドを使用して取得できます。
- **gr-instance** *gr_instance_id*：GR インスタンス ID を指定します。インスタンス ID 1 はローカル インスタンス ID を示しています。

- **pcap yes**：このオプションを構成すると、PCAP ファイルの生成が有効になります。デフォルトでは、このオプションは無効になっています。
- **list**：プロトコル リスト ファイルをモニタします。

重要 Exec モードの **monitor protocol** コマンドは、グローバル コンフィギュレーション モードの **monitor protocol cpu-limit** *threshold_percentage* コマンドで構成されたポッドの CPU 使用率に基づいて制限されます。

**monitor protocol** CLI は、複数の端末で同時に実行できます。また、**interface** *interface_name* CLI では、1 つの CLI コマンドで複数のエンドポイント名を構成できます。

例：

```
monitor protocol interface sbi,N4:209.165.200.241:8805,gtpc
capture-duration 1000
```

# SMF から UPF モニター サブスクライバ

## 機能説明

SMF は、選択した UPF にトレース トリガを自動的に送信します。SMF からトリガを送信すると、コントロール プレーンとユーザー プレーン全体でトラブルシューティングに必要な最小限のファイルを解析できます。

（注）

- オペレータは、モニタリングのために SMF 上で一度に最大 5 つのサブスクライバを構成できます。
- データ トレースを有効にすると、使用可能な VPP、FCAP、および MEH が UPF PCAP でキャプチャされます。
- プロトコル トレースを有効にすると、UPF で次のオプションが有効になります。
  - ルールマッチ イベント
  - L3 データ
  - PFCP イベントのトレース
  - EDR
  - Sessmgr
  - コール切断後のサブスクライバ概要
- SMF GR スイッチオーバー後、モニタ対象サブスクライバの既存のセッションは UPF の影響を受けません。monitor nf CLI はコンフィギュレーション モードに存在するため、オペレータは両方の SMF インスタンスで CLI を構成する必要があります。

UPF のリロードとスイッチオーバーのシナリオについては、モニタ NF の UPF のトラブルシューティング ガイドを参照してください。

このセクションでは、SMF から UPF モニタ サブスクライバを構成するための CLI コマンドについて説明します。

## SMF からの UPF モニターサブスクライバの構成

SMF から UPF モニタ サブスクライバ プロトコルを有効または無効にするには、次の構成を使用します。

- SMF からの UPF モニターサブスクライバの有効化
- SMF からの UPF モニターサブスクライバの無効化

### SMF から UPF モニター サブスクライバを有効化

SMF から UPF モニター サブスクライバを有効にするには、次の構成を使用します。

```
config
   monitor nf subscriber  [ gpsi gpsi_value |imei imei_id|imsiimsi_value
control { true | false }  data { true | false } target-nf { sgwu | upf
 } ]
   end
```

注：

- **monitor nf** ：モニターする NF を指定します。
- **gpsi** *gpsi_value*：サブスクライバ GPSI を指定します。
- **imsi** *imsi_value*—サブスクライバ IMSI を指定します。たとえば、123456789、* などです。
- **imei** *imei_id*— サブスクライバ IMEI を指定します。例：123456789012345、*
- **control { true | false }**：制御イベント トレースを有効にするか無効にするかを指定します。
- **data { true | false }**：データ イベント トレースを有効にするか無効にするかを指定します。
- **target-nf { sgwu | upf }**：ターゲット NF を SGW-U または UPF として指定します。 **target-nf** はオプションのパラメータであり、オペレータがこのパラメータを構成しない場合、モニター サブスクライバは UPF と SGW-U の両方で有効になります。

### 設定例

次に、設定例を示します。

```
[smf] smf(config)# monitor nf subscriber
   imsi 234150999999999
      control true
      data true
      target-nf upf
exit
```

## SMF からの UPF モニターサブスクライバの無効化

SMF から UPF モニタ サブスクライバを無効にするには、次の構成を使用します。

```
config
   [ no ]monitor nf subscriber  [ gpsi gpsi_value |imei imei_id |
imsiimsi_value ]
   end
```

注：

- **monitor nf** ：モニターする NF を指定します。
- **gpsi** *gpsi_value*：サブスクライバ GPSI を指定します。
- **imsi** *imsi_value*—サブスクライバ IMSI を指定します。たとえば、123456789、* などです。
- **imei** *imei_id*— サブスクライバ IMEI を指定します。例：123456789012345、*

# GTP-C サービスのモニターとトラブルシューティング

表 *584 :* 機能の履歴

| 機能名 | リリース情報 | 説明 |
|---|---|---|
| GTP-C サービスのトラブルシューティング | 2024.02.0 | この機能により、cnSGW＋SMF＋PGW-C は GTPC テスト エコー コマンドをピア ノードに送信して、次のことを実行できます：<br>• ピア ノードの接続性のトラブルシューティングとモニタリングを行います。<br>• ピアのラウンド トリップ時間（RTT）をテストします。<br>• S11、S5E、S5、S2B、S8 GTPC インターフェイス、IPv4、IPv6 トランスポート タイプをサポートします。<br>**[デフォルト設定（Default Setting）]**：有効 – 常時オン |

## 機能説明

GTP-C テスト エコー CLI コマンド サービスを使用すると、ピア ノードの接続のトラブルシューティングとモニタリングができ、システム動作中のピアのラウンド トリップ時間（RTT）が提供されます。

## GTP-C テスト エコー コマンドの使用

システムは次のテストコマンドを使用して、GTP-C ピア ノードとの接続性を確認します。

**test gtpc echo instance-id** *id* **interface** *interface_type* **peer-address** *ip_address*

**注**：

- **instance-id** *id*：システム上に構成されている GR インスタンスのインスタンス ID を指定します。
- **interface** *interface_type*：s11、s5e、s5、s2b、s8 などの GTP-C インターフェイス タイプを指定します。
- **peer address** *ip_address*：GTP-C エコー要求が送信される特定のピアの IPv4 アドレスまたは IPv6 アドレスを指定します。

次の例では、出力例を示します。

```
Success Case
[sgw] smf# test gtpc echo instance-id 1 interface s11 peer-address 1.1.1.1
 result
{
  "testGtpcEchoResponse": {
    "rx": 1,
    "tx": 1,
    "rtt(ms)": 3,
    "recovery": "10 (0x0A)",
    "status": {
      "success": true
    }
  }
}

Timeout Case:
[sgw] smf# test gtpc echo instance-id 1 interface s5 peer-address 2.2.2.2

Wed Jan  10 13:38:51.415 UTC+00:00
result
{
  "testGtpcEchoResponse": {
    "tx": 4,
    "recovery": "NA",
    "status": {
      "errorMsg": "No Response Received, Timeout"
    }
  }
}
```

## GTPP テスト エコー コマンドの使用

システムは、次のテスト コマンドを使用して、GTPP プロファイルに構成されていない新しい CGF サーバ接続を確認します。

**test gtpp echo instance-id** *id* **ca-address** *ip_address* **[ ca-port** *port* **] [ cgf-address** *ip_address* **] [ cgf-port** *port* **]**

**注**：

- **instance-id** id：システム上に構成されている *GR* インスタンスのインスタンス *ID* を指定します。
- **ca-address** *ip_address*：gtpp プロファイル内で構成された課金エージェントの IPv4 アドレスを指定します。
- **ca-port** *port*：gtpp プロファイル内で構成された課金エージェント ポートを指定します。範囲は 1 ～ 65535 です。デフォルトのポートは 49999 です。
- **cgf-address** *ip_address*：GTPP エコー要求の送信先である特定の CGF サーバの IPv4 アドレスを指定します。
- **cgf-port** *port*: 1 ～ 65535 の範囲で特定の CGF サーバ ポートを指定します。デフォルトのポートは 3386 です。

以下の例では、GTPP Echo コマンド出力の例を表示します。

```
Success Case:
[sgw] smf# test gtpp echo instance-id 1 ca-address 10.0.0.1 ca-port 2222 cgf-address
11.0.0.1

Tue Jan  23 12:26:40.164 UTC+00:00
result
{
  "testGtppEchoResponse": {
    "rx": 1,
    "tx": 1,
    "rtt(ms)": 3,
    "recovery": "10 (0x0A)",
    "status": {
      "success": true
    }
  }
}

Timeout Case:

[sgw] smf# test gtpp echo instance-id 1 ca-address 10.0.0.1 ca-port 2222 cgf-address
11.0.0.2

Tue Jan  24 07:43:22.164 UTC+00:00
result
{
  "testGtppEchoResponse": {
    "tx": 4,
    "recovery": "NA",
    "status": {
      "errorMsg": "No Response Received, Timeout"
    }
  }
}
```

# アラート

## 機能説明

システムが異常を検出すると、CEE Opsセンターはアラート通知を生成します。システム統計情報は、これらのアラート通知の原因です。式がtrueになったときにアラートをトリガーするように式を設定できます。

## 機能の仕組み

共通実行環境（CEE）は、アラート操作にPrometheus Alert Managerを使用します。CEE YANGモデルでは、CLIまたはAPIを利用して、アクティブなアラート、サイレントにされたアラート、およびアラート履歴を表示できます。また、アプリケーションは、アラートAPIを直接呼び出して、アラートを追加またはクリアすることもできます。Prometheus Alert Manager API（v2）は、使用される標準 API です。

Prometheus アラート マネージャには、次のオプションが含まれています。

- **アラート ルールの定義**：このオプションは、アラート マネージャがトリガするアラートのタイプを定義します。Prometheus クエリ言語（PromQL）を使用してアラートを定義します。
- **アラート ルーティングの定義**：このオプションは、アラート マネージャがアラートを受信した後に実行するアクションを定義します。現在、SNMP トラッパーはアウトバウンド アラートとしてサポートされています。また、CEE は生成されたアラートを保存するためのアラート ロガーを提供します。

# アラート ルールの構成

次の構成例を使用して、アラート ルールを構成します。

```
config
   alerts rules group alert_group_name
   interval-seconds seconds
   rule rule_name
      expression promql_expression
      duration duration
      severity severity_level
      type alert-type
      annotation annotation_name
      value annotation_value
      exit
   exit
```

注：

- **alerts rules**：Prometheus アラート ルールを指定します。
- **group** *alert_group_name*：Prometheus アラート ルール グループを指定します。1 つのアラート グループにルールの複数のリストを含めることができます。 *alert-group-name* はアラート グループの名前です。アラート グループ名は、0 ～ 64 文字の範囲の文字列にする必要があります。
- **interval-seconds** *seconds*：ルール グループの評価間隔を秒単位で指定します。
- **rule** *rule_name*：アラート ルール定義を指定します。 *rule_name* はルールの名前です。
- **expression** *promql_expression*：PromQL アラート ルール式を指定します。 *promql_expression* は、PromQL 構文で表されるアラート ルール クエリです。
- **duration** *duration*：true と見なされる前の true 条件の期間を指定します。 *duration* は 、アラートがトリガされるまでの時間間隔です。
- **severity** *severity_level*：アラートの重大度を指定します。 *severity-level* は、 アラートの重大度レベルです。重大度レベルは、重大、主要、マイナー、警告です。
- **type** *alert_type*：アラートのタイプを指定します。 *alert_type* は、ユーザー定義のアラート タイプです。たとえば、通信アラーム、環境アラーム、機器アラーム、不特定の整合性違

反アラーム、運用違反アラーム、物理違反アラーム、処理エラー アラーム、QoS アラーム、セキュリティ サービス アラーム、メカニズム違反アラーム、または時間ドメイン違反アラームです。

- **annotation** *annotation_name*：アラートに添付する注釈を指定します。 *annotation_name* は、注釈の名前です。
- **value** *annotation_value*：注釈の値を指定します。 *annotation_value* は、注釈の値です。

次の例では、Unified Data Management（UDM）の応答の割合が指定されたしきい値限度を下回る場合にトリガーされるアラートを構成します。

**例**：

```
 config terminal
  alerts rules group SMFUDMchk_incr
  interval-seconds 300
  rule SMFUDMchk_incr
  expression "sum(increase(smf_restep_http_msg_total{nf_type=\"udm\",
message_direction=\"outbound\", response_status=~\"2..\"}[3m])) /
sum(increase(smf_restep_http_msg_total{nf_type=\"udm\",
message_direction=\"outbound\"}[3m])) < 0.95"
  severity major
  type "Communications Alarm"
  annotation summary
  value "This alert is fired when the percentage of UDM responses is less than threshold"

  exit
 exit
exit
```

**show running-config alerts** コマンドを使用して、構成されたアラートを表示できます。

**例**：

次の例では、実行コンフィギュレーションで構成されたアラートを表示します。

```
 show running-config alerts
  interval-seconds 300
  rule SMFUDMchk_incr
  expression "sum(increase(smf_restep_http_msg_total{nf_type=\"udm\",
message_direction=\"outbound\", response_status=~\"2..\"}[3m])) /
sum(increase(smf_restep_http_msg_total{nf_type=\"udm\",
message_direction=\"outbound\"}[3m])) < 0.95"
  severity major
  type "Communications Alarm"
  annotation summary
  value "This alert is fired when the percentage of UDM responses is less than threshold"

  exit
 exit
exit
```

## アラート ロガーの表示

デフォルトでは、アラートロガーは生成されたすべてのアラートを保存します。次のコマンドを使用して、保存されたアラートを表示できます。

**show alert history [ filtering ]**

次のフィルタリング オプションを使用して結果を絞り込むことができます：

- **annotations**：アラートの注釈を指定します。
- **endsAt**：アラートの終了時刻を指定します。
- **labels**：アラートの追加のラベルを指定します。
- **severity**：アラートの重大度を指定します。
- **source**：アラートの送信元を指定します。
- **startedAt**：アラートの開始時刻を指定します。
- **type**：アラートのタイプを指定します。

システムで構成されたアラートの次の例の表示例：

**例**：

```
show alerts history
alerts active SMFUDMchk_incr ac2a970ab621
state active
severity major
type "Communications Alarm"
startsAt 2019-11-15T08:26:48.283Z
source System
annotations [ "summary:This alert is fired when the percentage of UDM responses is less
 than threshold.” ]
```

**show alerts active** コマンドを使用して、アクティブおよびサイレントされたアラートを表示できます。

次のアクティブなアラートの例が表示されます。アラートは、評価された式が true である限り、アクティブのままです。

**例**：

```
show alerts active
alerts active SMFUDMchk_incr ac2a970ab621
state active
severity major
type "Communications Alarm"
startsAt 2019-11-15T08:26:48.283Z
source System
annotations [ "summary:This alert is fired when the percentage of UDM responses is less
 than threshold.” ]
```

## コール フロー手順に関するアラート

このセクションでは、さまざまなコールフロー手順に関連するアラートを構成するために必要なコマンドの詳細について説明します。

SMF に固有のアラートは、共通実行環境（CEE）で構成されます。式が開発され、新しいカウンタが作成されます。ユーザ要件に基づいて、コール フロー手順アラートは CEE で構成されます。これらのアラートは、ユーザーが指定した条件が満たされたときにトリガーされます。

### 4G PDN 変更

次の構成例を使用して、4G PDN の変更手順に関連するアラートを設定します：

```
alerts rules group SMFPDN
   interval-seconds 300
   rule SMFPDNModify
   expression "sum(smf_service_stats{procedure_type=~\"pdn_ho_location_changed|
pdn_ho_rat_type_changed|pdn_inter_sgw_handover|pdn_mbr\" ,
status=\"success\"})/sum(smf_service_stats{procedure_type=~
\"pdn_ho_location_changed|pdn_ho_rat_type_changed |pdn_inter_sgw_handover|pdn_mbr\" ,
status=\"attempted\"}) < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage successful 4G PDN Modify is below
threshold"
   exit
exit
```

### 4G PDN リリースの成功

次の構成例を使用して、4G PDN リリースの成功手順に関連するアラートを構成します：

```
alerts rules group SMFPDN
   interval-seconds 300
   rule SMFPDNRelease
   expression "sum(smf_service_stats{procedure_type=~\".*pdn_sess_rel\" ,
status=\"success\"}) / sum(smf_service_stats{procedure_type=~\".*pdn_sess_rel\" ,
status=\"attempted\"} < 0.95 "
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage successful 4G PDN Release is below
threshold."
   exit
exit
```

### 4G PDN セットアップの成功

次の構成例を使用して、4G PDN セットアップの成功手順に関連するアラートを構成します：

```
alerts rules group SMFPDN
   interval-seconds 300
   rule SMFPDNSetup
   expression "sum(smf_service_stats{procedure_type=\"pdn_sess_create\" ,
status=\"success\"}) / sum(smf_service_stats{procedure_type=\"pdn_sess_create\" ,
status=\"attempted\"} < 0.95 "
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage successful 4G PDN Setup is below
threshold."
   exit
exit
```

### 4G から 5G への HO 成功

次の構成を使用して、4G から 5G への HO 成功手順に関連するアラートを構成します：

```
alerts rules group Handover
   interval-seconds 300
   rule 4gTo5gHOSuccess
   expression
"sum(smf_service_stats{procedure_type=~\"n26_4g_to_5g_handover|n26_4g_to_5g_im_mobility\"
 , status=\"success\"}) /
sum(smf_service_stats{procedure_type=~\"n26_4g_to_5g_handover|n26_4g_to_5g_im_mobility\"
 , status=\"attempted\"}) < 0.95 "
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage successful 4G to 5G HO is below
threshold."
   exit
exit
```

### 4G から WiFi HO への成功

次の構成を使用して、4G から WiFi への HO 成功手順に関連するアラートを構成します：

```
alerts rules group Handover
   interval-seconds 300
   rule 4GtoWifiHOSuccess
  expression "sum(smf_service_stats{procedure_type=\"enb_to_untrusted_wifi_handover\"
 , status=\"success\"}) /
sum(smf_service_stats{procedure_type=\"enb_to_untrusted_wifi_handover\" ,
status=\"attempted\"}) < 0.95 "
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage of N4 responses sent is lesser than
 95 %."
   exit
exit
```

### 5G N2 HO 成功

次の構成を使用して、5G N2 HO 成功手順に関連するアラートを構成します：

```
alerts rules group Handover
   interval-seconds 300
   rule N2HOSuccess
   expression "sum(smf_service_stats{procedure_type=\"n2_handover\" ,
status=\"success\"}) / sum(smf_service_stats{procedure_type=\"n2_handover\" ,
status=\"attempted\"}) < 0.95 "
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage successful 5G N2 HO is below
threshold."
   exit
exit
```

### 5G PDU のアイドル成功

次の構成を使用して、5G PDU アイドル成功手順に関連するアラートを構成します：

```
alerts rules group SMFPDU
   interval-seconds 300
   rule SMFPDUIdleSuccess
  expression "sum(smf_service_stats{procedure_type=~\".*idle\" , status=\"success\"})
 / sum(smf_service_stats{procedure_type=~\".*idle\" , status=\"attempted\"}) < 0.95 "
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage successful 5G PDU Idle is below
threshold"
   exit
exit
```

### 5G PDU の変更に成功しました

次の構成を使用して、5G PDU 変更の成功手順に関連するアラートを構成します：

```
alerts rules group SMFPDU
   interval-seconds 300
   rule SMFSessionModifySuccess
   expression "sum(smf_service_stats{procedure_type=~\".*pdu_sess_mod\" ,
status=\"success\"}) / sum(smf_service_stats{procedure_type=~\".*pdu_sess_mod\" ,
status=\"attempted\"}) < 0.95 "
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage successful 5G PDU Modify is below
threshold"
   exit
exit
```

### 5G PDU のリリースの成功

次の構成を使用して、5G PDU リリース成功手順に関連するアラートを構成します：

```
alerts rules group SMFPDU
   interval-seconds 300
   rule SMFSessionReleaseFailure
   expression "sum(smf_service_stats{procedure_type=~\".*pdu_sess_rel\" ,
status=\"success\"}) / sum(smf_service_stats{procedure_type=~\".*pdu_sess_rel\" ,
status=\"attempted\"}) < 0.95 "
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage successful 5G PDU Setup is below
threshold"
   exit
exit
```

### 5G PDU のセットアップの成功

次の構成を使用して、5G PDU セットアップの成功手順に関連するアラートを構成します：

```
alerts rules group SMFPDU
   interval-seconds 300
   rule SMFSessionSetupFailure
   expression "sum(smf_service_stats{procedure_type=\"pdu_sess_create\" ,
status=\"success\"}) / sum(smf_service_stats{procedure_type=\"pdu_sess_create\" ,
status=\"attempted\"} < 0.95 "
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when failed to setup sessions is more than 5%"
   exit
exit
```

### 5G から 4G への HO 成功

次の構成を使用して、5G から 4G への HO 成功手順に関連するアラートを構成します：

```
alerts rules group Handover
   interval-seconds 300
   rule 5gTo4gHOSuccess
   expression "sum(smf_service_stats{procedure_type=~\"pdn_5g_4g_handover
|pdn_5g_4g_handover_dft|eps_fb_5g_4g_handover_dft|eps_fb_5g_4g_handover_idft
|pdn_5g_4g_handover_idft\" , status=\"success\"}) /
sum(smf_service_stats{procedure_type=~\"pdn_5g_4g_handover
|pdn_5g_4g_handover_dft|eps_fb_5g_4g_handover_dft|
eps_fb_5g_4g_handover_idft|pdn_5g_4g_handover_idft\" , status=\"attempted\"}) < 0.95 "
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage successful 5G to 4G HO is below
threshold."
   exit
exit
```

### 5G から WiFi HO への成功

次の構成例を使用して、5G から WiFi HO の成功手順に関連するアラートを構成します。

```
alerts rules group Handover
   interval-seconds 300
   rule 5GtoWifiHOSuccess
  expression "sum(smf_service_stats{procedure_type=\"nr_to_untrusted_wifi_handover\"
 , status=\"success\"}) /
sum(smf_service_stats{procedure_type=\"nr_to_untrusted_wifi_handover\" ,
status=\"attempted\"}) < 0.95 "
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage of N4 responses sent is lesser than
 95 %."
   exit
exit
```

### 5G Xn HO成功

次の構成例を使用して、5G Xn HO の成功手順に関連するアラートを構成します：

```
alerts rules group Handover
   interval-seconds 300
   rule XnHOSuccess
   expression "sum(smf_service_stats{procedure_type=\"xn_handover\" ,
status=\"success\"}) / sum(smf_service_stats{procedure_type=\"xn_handover\" ,
status=\"attempted\"}) < 0.95 "
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage successful 5G Xn HO is below
threshold."
   exit
exit
```

### PDN セッションの作成（PDN Session Create）

次の構成例を使用して、PDN セッションの作成手順に関連するアラートを構成します。

```
alerts rules group SMFProcStatus
   interval-seconds 300
   rule PDNSessCreate
   expression "sum(increase(smf_service_stats{app_name=\"SMF\",procedure_type=
/\"pdn_sess_create\",status=\"success\"}[5m])) /
sum(increase(smf_service_stats{app_name=\"SMF\
/",procedure_type=\"pdn_sess_create\",status=\"  /attempted\"}[5m])) < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the success percentage of pdn_sess_create procedure
 is lesser threshold."
   exit
exit
```

### PDU セッションの作成

次の構成例を使用して、PDU セッションの作成手順に関連するアラートを構成します。

```
alerts rules group SMFProcStatus
   interval-seconds 300
   rule PDUSessCreate
   expression "sum(increase(smf_service_stats{app_name=\"SMF\",procedure_type=
/\"pdu_sess_create\",status=\"success\"}[5m]))sum
/(increase(smf_service_stats{app_name=\"SMF\",
/procedure_type=\"pdu_sess_create\",status=\  /"attempted\"}[5m])) < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the success percentage of pdu_sess_create procedure
 is lesser threshold."
   exit
exit
```

### PDU セッション変更

次の構成例を使用して、PDU セッションの変更手順に関連するアラートを構成します。

```
alerts rules group SMFProcStatus
   interval-seconds 300
   rule PDUSessModify
   expression "sum(increase(smf_service_stats{app_name=\"SMF\",procedure_type=~\".
/*req_pdu_sess_mod\",status=\"success\"}[5m]))sum(increase
/(smf_service_stats{app_name=\"SMF\",procedure_type=~
/\".*req_pdu_sess_mod\",status=\"attempted\"}[5m]))  / < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
  value "This alert is fired when the success percentage of req_pdu_sess_mod procedure
 is lesser threshold."
   exit
exit
```

### PDU セッションの解放

次の構成例を使用して、PDU セッションのリリース手順に関連するアラートを構成します。

```
alerts rules group SMFProcStatus
   interval-seconds 300
   rule PDUSessRelease
   expression
"sum(increase(smf_service_stats{app_name=\"SMF\",procedure_type=~\".*req_pdu_sess_rel\",status=\
  /"success\"}[5m]))sum(increase(smf_service_stats{app_name=\"SMF
/\",procedure_type=~\".*req_pdu_sess_rel\",status=\  /"attempted\"}[5m])) < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
  value "This alert is fired when the success percentage of req_pdu_sess_rel procedure
 is lesser threshold."
   exit
exit
```

## インターフェイス固有のアラート

このセクションでは、さまざまなインターフェイスに関連するアラートを構成するために必要なコマンドの詳細について説明します。

### GTPC ピアの停止（GTPC Peer Down）

次のコマンドを使用して、GTPC ピア ダウン手順に関連するアラートを構成します。

```
alerts rules group GTPCPeerDown
   interval-seconds 300
   rule GTPCPeerDown
   expression nodemgr_gtpc_peer_status{gtpc_peer_status=\"gtpc_peer_path_down\"})
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the GTPC Path failure detected for peer crosses
```

```
threshold"
   exit
exit
```

### N4 メッセージの成功

N4 メッセージ成功手順に関連するアラートを構成するには、次のコマンドを使用します。

```
alerts rules group SMFSvcStatus
   interval-seconds 300
   rule SMFN4MessageSuccess
   expression "sum(protocol_udp_res_msg_total{message_direction=\"inbound\",
status=\"accepted\"}) / sum(protocol_udp_res_msg_total{message_direction=\"inbound\",
status=~\"accepted|denied\"}) < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage of N4 responses sent is lesser than
 95 %."
   exit
exit
```

### N4 UPF の関連付けがダウン

次のコマンドを使用して、N4 アドレスによる N4 UPF 関連付けダウン クエリに関連するアラートを構成します。

```
alerts rules group N4Association
   interval-seconds 300
   rule SMFAssociationRelease
  expression "proto_udp_res_msg_total{procedure_type=\"n4_association_release_res\",
 message_direction= \"inbound\", status=\"accepted\"}) "
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the N4 Association with UPF is released"
   exit
exit
```

### N4 UPF の関連付けが稼働

次のコマンドを使用して、N4 アドレスによる N4 UPF 関連付けアップ クエリに関連するアラートを構成します。

```
alerts rules group N4Association
   interval-seconds 300
   rule N4AssociationUP
   expression "proto_udp_res_msg_total{procedure_type=\"n4_association_setup_res\",
message_direction= \"inbound\", status=\"accepted\"}"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the N4 Association with UPF is established"
```

```
   exit
exit
```

### N7インターフェイス アウトバウンド

アウトバウンドN7インターフェイスに関連するアラートを構成するには、次のコマンドを使用します。

```
alerts rules group SMFSvcStatus
   interval-seconds 300
   rule SMFN7Outbound
   expression "sum(increase(smf_restep_http_msg_total{nf_type=\"pcf\",
message_direction=\"outbound\", response_status=~\"2..\"}[5m])) /
sum(increase(smf_restep_http_msg_total{nf_type=\"pcf\",
message_direction=\"outbound\"}[5m])) < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage of N7 responses received is lesser
threshold."
   exit
exit
```

### N7インターフェイス インバウンド

インバウンドN7インターフェイスに関連するアラートを構成するには、次のコマンドを使用します。

```
alerts rules group SMFSvcStatus
   interval-seconds 300
   rule SMFN7Inbound
   expression "sum(increase(smf_restep_http_msg_total{nf_type=\"pcf\",
message_direction=\"inbound\", response_status=~\"2..\"}[5m])) /
sum(increase(smf_restep_http_msg_total{nf_type=\"pcf\",
message_direction=\"inbound\"}[5m])) < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage of N7 responses sent is lesser
threshold."
   exit
exit
```

### N7メッセージがタイムアウトしました

N7メッセージ タイムアウト手順に関連するアラートを構成するには、次のコマンドを使用します。

```
alerts rules group MessageTimeout
   interval-seconds 300
   rule SMFN7Timeout
   expression "sum(irate(smf_restep_http_msg_total{nf_type=\"pcf\",
message_direction=\"inbound\", response_status=\"504\"}[5m])) > 5"
   severity major
   type "Communications Alarm"
```

```
   annotation summary
   value "This alert is fired when the increase in timeout for N7 messages toward PCF
 crosses threshold"
   exit
exit
```

## N10 インターフェイス

N10 インターフェイスに関連するアラートを構成するには、次のコマンドを使用します。

```
alerts rules group SMFSvcStatus
   interval-seconds 300
   rule SMFN10
   expression "sum(increase(smf_restep_http_msg_total{nf_type=\"udm\",
message_direction=\"outbound\", response_status=~\"2..\"}[5m])) /
sum(increase(smf_restep_http_msg_total{nf_type=\"udm\",
message_direction=\"outbound\"}[5m])) < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage of N10 responses received is lesser
 threshold."
   exit
exit
```

## N11 インターフェイス インバウンド

インバウンドN11インターフェイスに関連するアラートを構成するには、次のコマンドを使用します。

```
alerts rules group SMFSvcStatus
   interval-seconds 300
   rule SMFN11Inbound
   expression "sum(increase(smf_restep_http_msg_total{nf_type=\"amf\",
message_direction=\"inbound\", response_status=~\"2..\"}[5m])) /
sum(increase(smf_restep_http_msg_total{nf_type=\"amf\",
message_direction=\"inbound\"}[5m])) < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage of N11 responses sent is lesser
threshold."
   exit
exit
```

## N11インターフェイス アウトバウンド

アウトバウンドN11インターフェイスに関連するアラートを構成するには、次のコマンドを使用します。

```
alerts rules group SMFSvcStatus
   interval-seconds 60
   rule SMFN11Outbound
   expression "sum(increase(smf_restep_http_msg_total{nf_type=\"amf\",
message_direction=\"outbound\", response_status=~\"2..\"}[5m])) /
```

```
sum(increase(smf_restep_http_msg_total{nf_type=\"amf\",
message_direction=\"outbound\”}[5m])) < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage of N11 responses received is lesser
 threshold.”
   exit
exit
```

## N11メッセージがタイムアウトしました

N11メッセージのタイムアウト手順に関連するアラートを構成するには、次のコマンドを使用します。

```
alerts rules group MessageTimeout
   interval-seconds 300
   rule SMFN40Timeout
   expression ”sum(irate(smf_restep_http_msg_total{nf_type=\“chf\”,
message_direction=\”inbound\”, response_status=\”504\”}[5m])) > 5”
   severity major
   type "Communications Alarm"
   annotation summary
   value “This alert is fired when the increase in timeout for N11 messages toward AMF
 crosses threshold”
   exit
exit
```

## N40インターフェイス インバウンド

インバウンドN40インターフェイスに関連するアラートを構成するには、次のコマンドを使用します。

```
alerts rules group SMFSvcStatus
   interval-seconds 300
   rule SMFN40Inbound
   expression "sum(increase(smf_restep_http_msg_total{nf_type=\"chf\",
message_direction=\"inbound\", response_status=~\”2..\”}[5m])) /
sum(increase(smf_restep_http_msg_total{nf_type=\"chf\",
message_direction=\"inbound\”}[5m])) < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage of N40 responses sent is lesser
threshold.”
   exit
exit
```

## N40インターフェイスのアウトバウンド

アウトバウンドN40インターフェイスに関連するアラートを構成するには、次のコマンドを使用します。

```
alerts rules group SMFSvcStatus
   interval-seconds 300
```

```
   rule SMFN40Outbound
   expression "sum(increase(smf_restep_http_msg_total{nf_type=\"chf\",
message_direction=\"outbound\", response_status=~\"2..\"}[5m])) /
sum(increase(smf_restep_http_msg_total{nf_type=\"chf\",
message_direction=\"outbound\"}[5m])) < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage of N40 responses received is lesser
 threshold."
   exit
exit
```

## N40 メッセージがタイムアウト

N40 メッセージのタイムアウト手順に関連するアラートを構成するには、次のコマンドを使用します。

```
alerts rules group MessageTimeout
   interval-seconds 300
   rule SMFN11Timeout
   expression "sum(irate(smf_restep_http_msg_total{nf_type=\"chf\",
message_direction=\"inbound\", response_status=\"504\"}[5m])) > 5"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired the increase in timeout for N40 messages toward CHF
crosses threshold"
   exit
exit
```

## NRF ディスカバリ

次のコマンドを使用して、NRF ディスカバリ手順に関連するアラートを構成します。

```
alerts rules group NRF
   interval-seconds 300
   rule NRFDiscovery
   expression
"sum(nf_discover_messages_total{result=~\"success|failure\",svc_name=\"nnrf-disc\",
service_name=\"smf-rest-ep\"}) < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage of N4 responses sent is lesser than
 95 %."
   exit
exit
```

## SMF サービスの開始

次のコマンドを使用して、SMF サービス開始手順に関連するアラートを構成します。

```
alerts rules group SMFService
   interval-seconds 300
```

```
  rule SMFServiceStart
  expression "irate(outgoing_response_msg_total{msg_type=\"NrfNfmRegistration\"}[5m])"
  severity major
  type "Communications Alarm"
  annotation summary
  value "This alert is fired when SMF-Service starts upon registration with NRF"
  exit
exit
```

# IPプール

このセクションでは、IPプールに関連するアラートを構成するために必要なコマンドの詳細について説明します。

## IP プールを使用

次のコマンドを使用して、手順に使用される IP プールに関連するアラートを構成します。

```
alerts rules group IPPool
  interval-seconds 300
  rule IPPool
  expression "sum(IPAM_address_allocations_current) > THRESHOLD"
  severity major
  type "Communications Alarm"
  annotation summary
  value "This alert is fired when the percentage IP pool addresses used is above the
 threshold"
  exit
exit
```

# メッセージ レベル アラート

このセクションでは、さまざまなメッセージに関連するアラートを構成するために必要なコマンドの詳細について説明します。

## N11 SM の作成

N11 SM の作成に関連するアラートを構成するには、次のコマンドを使用します。

```
alerts rules group SMFSvcStatus
  interval-seconds 300
  rule SMFN11Success
  expression
"sum(increase(smf_restep_http_msg_total{api_name=\"amf_create_sm_context\",
message_direction=\"inbound\", response_status=\"201\"}[5m])) /
sum(increase(smf_restep_http_msg_total{api_name=\"amf_create_sm_context\",
message_direction=\"inbound\"}[5m])) < 0.95"
  severity major
  type "Communications Alarm"
  annotation summary
  value "This alert is fired when the percentage of amf_create_sm_context responses
sent is lesser threshold."
```

```
   exit
exit
```

### N11 SM 更新

N11 SM の更新に関連するアラートを構成するには、次のコマンドを使用します。

```
alerts rules group SMFSvcStatus
   interval-seconds 300
   rule SMFN11Update
   expression
"sum(increase(smf_restep_http_msg_total{api_name=\"amf_update_sm_context\",
message_direction=\"inbound\", response_status=\"200\"}[5m])) /
sum(increase(smf_restep_http_msg_total{api_name=\"amf_update_sm_context\",
message_direction=\"inbound\”}[5m])) < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage of amf_update_sm_context responses
sent is lesser threshold.”
   exit
exit
```

### N11 SM リリース

N11 SM リリースに関連するアラートを構成するには、次のコマンドを使用します。

```
alerts rules group SMFSvcStatus
   interval-seconds 300
   rule SMFN11Release
   expression
"sum(increase(smf_restep_http_msg_total{api_name=\"amf_release_sm_context\",
message_direction=\"inbound\", response_status=\"204\”}[5m])) /
sum(increase(smf_restep_http_msg_total{api_name=\"amf_release_sm_context\",
message_direction=\"inbound\”}[5m])) < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage of amf_release_sm_context responses
 sent is lesser threshold.”
   exit
exit
```

### N1 N2 メッセージ転送

N1 N2 メッセージ転送に関するアラートを構成するには、次のコマンドを使用します。

```
alerts rules group SMFSvcStatus
   interval-seconds 300
   rule SMFN1N2Transfer
  expression "sum(increase(smf_restep_http_msg_total{api_name=\"amf_n1_n2_transfer\",
 message_direction=\"outbound\", response_status=\"200\”}[5m])) /
sum(increase(smf_restep_http_msg_total{api_name=\"amf_n1_n2_transfer\",
message_direction=\"outbound\”}[5m])) < 0.95"
   severity major
   type "Communications Alarm"
```

```
   annotation summary
   value "This alert is fired when the percentage of amf_n1_n2_transfer responses
received is lesser threshold."
   exit
exit
```

### N11 EBI の割り当て

N11 EBI の割り当てに関連するアラートを構成するには、次のコマンドを使用します。

```
alerts rules group SMFSvcStatus
   interval-seconds 300
   rule SMFN11EBI
   expression "sum(increase(smf_restep_http_msg_total{api_name=\"amf_assign_ebi\",
message_direction=\"outbound\", response_status=\"200\"}[5m])) /
sum(increase(smf_restep_http_msg_total{api_name=\"amf_assign_ebi\",
message_direction=\"outbound\"}[5m])) < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage of amf_assign_ebi responses received
 is lesser threshold."
   exit
exit
```

### N11 SM ステータス通知

N11 SM ステータス通知に関連するアラートを構成するには、次のコマンドを使用します。

```
alerts rules group SMFSvcStatus
   interval-seconds 300
   rule SMFN11StatusNotify
  expression "sum(increase(smf_restep_http_msg_total{api_name=\"amf_status_notify\",
 message_direction=\"outbound\", response_status=\"201\"}[5m])) /
sum(increase(smf_restep_http_msg_total{api_name=\"amf_status_notify\",
message_direction=\"outbound\"}[5m])) < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
  value "This alert is fired when the percentage of amf_status_notify responses received
 is lesser threshold."
   exit
exit
```

### N11 SM コンテキストの取得

N11 SM コンテキスト取得に関連するアラートを構成するには、次のコマンドを使用します。

```
alerts rules group SMFSvcStatus
   interval-seconds 300
   rule SMFN11ContextRetrieve
   expression
"sum(increase(smf_restep_http_msg_total{api_name=\"amf_retrieve_sm_context\",
message_direction=\"inbound\", response_status=\"201\"}[5m])) /
sum(increase(smf_restep_http_msg_total{api_name=\"amf_retrieve_sm_context\",
message_direction=\"inbound\"}[5m])) < 0.95"
```

```
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage of amf_retrieve_sm_context responses
 sent is lesser threshold."
   exit
exit
```

## N7 SM ポリシーの作成

N7 SM ポリシーの作成に関連するアラートを構成するには、次のコマンドを使用します。

```
alerts rules group SMFSvcStatus
   interval-seconds 300
   rule SMFN7PolicyCreate
   expression
"sum(increase(smf_restep_http_msg_total{api_name=\"pcf_sm_policy_control_create\",
message_direction=\"outbound\", response_status=\"201\"}[5m])) /
sum(increase(smf_restep_http_msg_total{api_name=\"pcf_sm_policy_control_create\",
message_direction=\"outbound\"}[5m])) < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage of pcf_sm_policy_control_create
responses received is lesser threshold."
   exit
exit
```

## N7 SM ポリシーの更新

N7 SM ポリシーの更新に関連するアラートを構成するには、次のコマンドを使用します。

```
alerts rules group SMFSvcStatus
   interval-seconds 300
   rule SMFN7PolicyUpdate
   expression
"sum(increase(smf_restep_http_msg_total{api_name=\"pcf_sm_policy_control_update\",
message_direction=\"outbound\", response_status=\"200\"}[5m])) /
sum(increase(smf_restep_http_msg_total{api_name=\"pcf_sm_policy_control_update\",
message_direction=\"outbound\"}[5m])) < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage of pcf_sm_policy_control_update
responses received is lesser threshold."
   exit
exit
```

## N7 SM ポリシーの削除

N7 SM ポリシーの削除に関連するアラートを構成するには、次のコマンドを使用します。

```
alerts rules group SMFSvcStatus
   interval-seconds 300
   rule SMFN7PolicyDelete
   expression
```

```
"sum(increase(smf_restep_http_msg_total{api_name=\"pcf_sm_policy_control_delete\",
message_direction=\"outbound\", response_status=\"204\"}[5m])) /
sum(increase(smf_restep_http_msg_total{api_name=\"pcf_sm_policy_control_delete\",
message_direction=\"outbound\"}[5m])) < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage of pcf_sm_policy_control_delete
responses received is lesser threshold."
   exit
exit
```

## N7 SMポリシー通知の更新

N7 SMポリシー通知の更新に関連するアラートを構成するには、次のコマンドを使用します。

```
alerts rules group SMFSvcStatus
   interval-seconds 300
   rule SMFN7PolicyUpdateNotify
   expression
"sum(increase(smf_restep_http_msg_total{api_name=\"pcf_sm_policy_control_update_notify\",
 message_direction=\"inbound\", response_status=\"201\"}[5m])) /
sum(increase(smf_restep_http_msg_total{api_name=\"pcf_sm_policy_control_update_notify\",
 message_direction=\"inbound\"}[5m])) < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
  value "This alert is fired when the percentage of pcf_sm_policy_control_update_notify
 responses sent is lesser threshold."
   exit
exit
```

## N7 SM ポリシー通知終了

N7 SM ポリシーの終了に関連するアラートを構成するには、次のコマンドを使用します。

```
alerts rules group SMFSvcStatus
   interval-seconds 300
   rule SMFN7PolicyTerminateNotify
   expression
"sum(increase(smf_restep_http_msg_total{api_name=\"pcf_sm_policy_control_terminate_notify\",
 message_direction=\"inbound\", response_status=\"201\"}[5m])) /
sum(increase(smf_restep_http_msg_total{api_name=\"pcf_sm_policy_control_terminate_notify\",
 message_direction=\"inbound\"}[5m])) < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage of
pcf_sm_policy_control_terminate_notify responses sent is lesser threshold."
   exit
exit
```

## N10 UE レジスタ

N10 UE 登録に関するアラートを構成するには、次のコマンドを使用します。

```
alerts rules group SMFSvcStatus
   interval-seconds 300
   rule SMFN10UERegister
   expression "sum(increase(smf_restep_http_msg_total{api_name=\"register_ue\",
message_direction=\"outbound\", response_status=\"201\"}[5m])) /
sum(increase(smf_restep_http_msg_total{api_name=\"register_ue\",
message_direction=\"outbound\"}[5m])) < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage of register_ue responses received is
 lesser threshold."
   exit
exit
```

## N10 UE 登録解除

N10 UE DeRegister に関連するアラートを構成するには、次のコマンドを使用します。

```
alerts rules group SMFSvcStatus
   interval-seconds 300
   rule SMFN10UEDeRegister
   expression "sum(increase(smf_restep_http_msg_total{api_name=\"deregister_ue\",
message_direction=\"outbound\", response_status=\"201\"}[5m])) /
sum(increase(smf_restep_http_msg_total{api_name=\"deregister_ue\",
message_direction=\"outbound\"}[5m])) < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage of deregister_ue responses received
 is lesser threshold."
   exit
exit
```

## N10 SM サブスクリプションの取得

N10サブスクリプションフェッチに関連するアラートを構成するには、次のコマンドを使用します。

```
alerts rules group SMFSvcStatus
   interval-seconds 300
   rule SMFN10SubscriptionFetch
   expression "sum(increase(smf_restep_http_msg_total{api_name=\"subscription_req\",
 message_direction=\"outbound\", response_status=\"200\"}[5m])) /
sum(increase(smf_restep_http_msg_total{api_name=\"subscription_req\",
message_direction=\"outbound\"}[5m])) < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
  value "This alert is fired when the percentage of subscription_req responses received
 is lesser threshold."
   exit
exit
```

## 通知のための N10 SM 登録

通知のための N10 登録に関連するアラートを構成するには、次のコマンドを使用します。

```
alerts rules group SMFSvcStatus
   interval-seconds 300
   rule SMFN10SubscriptionNotification
  expression "sum(increase(smf_restep_http_msg_total{api_name=\"sdm_subscription_req\",
 message_direction=\"outbound\", response_status=\"201\"}[5m])) /
sum(increase(smf_restep_http_msg_total{api_name=\"sdm_subscription_req\",
message_direction=\"outbound\"}[5m])) < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage of sdm_subscription_req responses
received is lesser threshold."
   exit
exit
```

## N10 課金データ要求

次のコマンドを使用して、N10 課金データ要求に関連するアラートを構成します。

```
alerts rules group SMFSvcStatus
   interval-seconds 300
   rule SMFN10ChargingRequest
   expression
"sum(increase(smf_restep_http_msg_total{api_name=\"chf_charging_data_request\",
message_direction=\"outbound\", response_status=\"201\"}[5m])) /
sum(increase(smf_restep_http_msg_total{api_name=\"chf_charging_data_request\",
message_direction=\"outbound\"}[5m])) < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
  value "This alert is fired when the percentage of chf_charging_data_request responses
 received is lesser threshold."
   exit
exit
```

## N10 課金データ通知

次のコマンドを使用して、N10 課金データ通知に関連するアラートを構成します。

```
alerts rules group SMFSvcStatus
   interval-seconds 300
   rule SMFN10ChargingDataNotify
   expression "sum(increase(smf_restep_http_msg_total{api_name=\"chf_abort_notify\",
 message_direction=\"inbound\", response_status=\"201\"}[5m])) /
sum(increase(smf_restep_http_msg_total{api_name=\"chf_abort_notify\",
message_direction=\"inbound\"}[5m])) < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage of chf_abort_notify responses sent
is lesser threshold."
```

```
   exit
exit
```

# ポリシー ルール アラート

このセクションでは、さまざまなポリシールールに関連するアラートを構成するために必要なコマンドの詳細について説明します。

## ダイナミック PCC ルールの追加

ダイナミック PCC ルールの追加に関連するアラートを構成するには、次のコマンドを使用します。

```
alerts rules group SMFPolicyStatus
   interval-seconds 300
   rule AddPCCRule
   expression
"sum(increase(policy_dynamic_pcc_rules_total{app_name=\"SMF\",event=\"success\",operation=\"install\"}[5m]))
  /
sum(increase(policy_dynamic_pcc_rules_total{app_name=\"SMF\",event=\"attempted\",operation=\"install\"}[5m]))
 < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage of successful addition of dynamic
pcc rules is lesser threshold."
   exit
exit
```

## ダイナミック PCC ルールの変更

ダイナミック PCC ルールの変更に関連するアラートを構成するには、次のコマンドを使用します。

```
alerts rules group SMFPolicyStatus
   interval-seconds 300
   rule ModifyPCCRule
   expression
"sum(increase(policy_dynamic_pcc_rules_total{app_name=\"SMF\",event=\"success\",operation=\"modify\"}[5m]))
  /
sum(increase(policy_dynamic_pcc_rules_total{app_name=\"SMF\",event=\"attempted\",operation=\"modify\"}[5m]))
 < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
  value "This alert is fired when the percentage of successful modification of dynamic
 pcc rules is lesser threshold."
   exit
exit
```

## ダイナミック PCC ルールの削除

ダイナミック PCC ルールの削除に関連するアラートを構成するには、次のコマンドを使用します。

```
alerts rules group SMFPolicyStatus
   interval-seconds 300
   rule RemovePCCRule
   expression
"sum(increase(policy_dynamic_pcc_rules_total{app_name=\"SMF\",event=\"success\",operation=\"remove\"}[5m]))
  /
sum(increase(policy_dynamic_pcc_rules_total{app_name=\"SMF\",event=\"attempted\",operation=\"remove\"}[5m]))
 < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage of successful removal of dynamic pcc
 rules is lesser threshold."
   exit
exit
```

## SMF 過負荷/輻輳

このセクションでは、さまざまな SMF オーバーロード/輻輳に関連するアラートを構成するために必要なコマンドの詳細について説明します。

### SMF 過負荷

次のコマンドを使用して、SMF オーバーロード手順に関連するアラートを構成します。

```
alerts rules group SMFSvcStatus
   interval-seconds 300
   rule SMFOverload
   expression "sum by (component) (system_overload_status) == true"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when increase in events not processed due to system
overload"
   exit
exit
```

## SMF セッション

このセクションでは、さまざまな SMF セッションに関連するアラートを構成するために必要なコマンドの詳細について説明します。

### セッション リリース レート

次のコマンドを使用して、セッション リリース レート手順に関連するアラートを構成します。

```
alerts rules group SMFSession
   interval-seconds 300
   rule SMFSessionReleaseRate
   expression
"sum(rate(smf_service_stats{procedure_type=~\".*pdu_sess_rel|.*pdn_sess_rel\" ,
status=\"attempted\"}[5m])) >  THRESHOLD "
   severity major
   type "Communications Alarm"
```

```
   annotation summary
   value "This alert is fired when the session release rate exceeds the threshold"
   exit
exit
```

### セッション セットアップの失敗

次のコマンドを使用して、セッション セットアップ障害手順に関連するアラートを構成します。

```
alerts rules group SMFSession
   interval-seconds 300
   rule SMFSessionSetupFailure
  expression "sum(smf_service_stats{procedure_type=~\"pdu_sess_create|pdn_sess_create\"
 , status=\"failures\"}) /
sum(smf_service_stats{procedure_type=\"pdu_sess_create|pdn_sess_create\" ,
status=\"attempted\"}) >  0.05 "
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when failed to setup sessions is more than 5%"
   exit
exit
```

### セッション セットアップ レート

次のコマンドを使用して、セッション セットアップ レート手順に関連するアラートを構成します。

```
alerts rules group SMFSession
   interval-seconds 300
   rule SMFSessionSetupRate
   expression
"sum(rate(smf_service_stats{procedure_type=~\"pdu_sess_create|pdn_sess_create\" ,
status=\"attempted\"}[5m]))>  THRESHOLD "
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the session setup rate exceeds the threshold"
   exit
exit
```

### サブスクライバの制限

次のコマンドを使用して、サブスクライバ制限手順に関連するアラートを構成します。

```
alerts rules group SMFSession
   interval-seconds 300
   rule SMFSubscriberLimit
  expression "sum(smf_session_counters{pdu_type=~\"ipv4v6|ipv4|ipv6\"}) > THRESHOLD"

   severity major
   type "Communications Alarm"
   annotation summary
```

```
    value "This alert is fired when the max number of subscribers is more
    than the threshold"
    exit
exit
```

# メトリック

## 機能説明

幅広いアプリケーションとシステムの統計情報、および SMF インフラストラクチャ内の重要業績評価指標（KPI）をモニタできます。KPI は、SMF 環境の全体的な状態を把握するのに役立ちます。統計は、SMF 構成と使用率固有のデータを簡略化して表示します。

SMF は、パフォーマンス データをキャプチャして保持するためのサードパーティのモニタリングおよびアラート ソリューションである Prometheus と統合されます。このデータは統計として報告され、Web ベースのダッシュボードで表示できます。Grafana は、Prometheus データベースが収集する統計やカウンタをグラフィカルまたはテキストベースで表示します。Grafana ダッシュボードは、定量的定性的データの包括的なセットを投影し、選択したレポート ツールで SMF のメトリクスを分析し、情報に基づいた意思決定を行うことを促します。

デフォルトでは、モニタリング ソリューションが有効になっています。これは、Prometheus が SMF 環境を継続的にモニタし、Prometheus データソースが Grafana に関連付けられていることを示します。Grafana にアクセスするには、管理者権限が必要です。ただし、特定のダッシュボードを表示するには、Prometheus クエリを実行します。クエリは、組み込み形式とカスタム形式で使用できます。

次のスナップショットは、Grafana ダッシュボードの例です。

***Figure 317: Grafana ダッシュボード***

# 機能の仕組み

KPIは、統計情報やカウンタなどのメトリックを構成します。これらのメトリックは、パフォーマンスの向上または低下を表します。デフォルトでは、PrometheusはSMFが展開され、Grafanaで構成されているシステムで有効になっています。Prometheusは、システムで使用可能なデータ ソースのモニタリングを動的に開始します。新しいダッシュボード パネルは、Prometheusでクエリを実行します。

Prometheusの詳細については、 https://prometheus.io/docs/introduction/overview/にあるPrometheusのドキュメントを参照してください。

# メトリック収集の設定

各SMF メトリックのラベルは、次の3つのカテゴリに分類されます。

- 実稼働
- デバッグ
- きめ細かさ

すべてのSMF アプリケーション メトリックは、パフォーマンスの最適化のためにCLI コマンドを介して制御されます。

必要なSMF メトリックとラベルを収集するには、次の構成例を使用します。

```
config
   infra metrics verbose { service | protocol | load-balancer |
application } [ level { debug | off | production | trace } | metrics
metrics_name [ granular-labels label_name| level { debug | off | production
 | trace } | pod pod_name | level { debug | off | production | trace }
] ]
   end
```

注：

- メトリックの冗長性が構成されていない場合、ポッドタイプのデフォルトの冗長性レベルは次のようになります。
  - LoadBalancer = Production
  - Protocol = Trace
  - Service = Trace
  - Application = Debug
- 詳細メトリックのレベルの順序は、次の優先順位です。
  - **metrics [ [metrics_name] level [production|debug|trace|off]**: [Priority 1]
  - **pod [[pod_Name]] level [ production | debug | trace | off]]** [Priority 2]
  - **level [production | debug | trace | off]** [Priority 3]

- **infra metrics verbose { service | protocol | load-balancer | application }**：メトリック収集を有効にします。 この構成は、必要なアプリケーション メトリックとラベルを収集しやすくなります。デフォルトでは、このコマンドはメトリックのデバッグ ラベルをキャプチャします。
- **level { debug | off | production | trace }**：アプリケーション メトリックのカテゴリを指定して、必要なアプリケーション メトリックとラベルをキャプチャします。
  - **debug**：実稼働カテゴリおよびデバッグ カテゴリとして分類されるすべてのラベルをキャプチャします。デフォルトの構成オプション
  - **off**：アプリケーション レベルのメトリックの収集を無効にします。

    たとえば、 **infra metrics verbose application smf_service_stats level off** コマンドを構成すると、smf_service_stats アプリケーション メトリックが無効になります。
  - **production**：実稼働カテゴリとして分類されるラベルをキャプチャします。
  - **trace**：このオプションは、SMF アプリケーション メトリックではサポートされていません。このオプションが構成されている場合、SMF はこのオプションを **debug** として扱います。
- メトリックの実稼働およびデバッグの分類が空の場合、詳細ラベル（構成されている場合）を除くすべてのラベルがデバッグとして分類されます。
- **metrics** *metrics_name*：特定のメトリックに対応するラベルのみをキャプチャするメトリック名を指定します。メトリックレベルの構成は、アプリケーションレベルの構成よりも優先されます。メトリック レベルが構成されていない場合、ラベルはアプリケーション レベルでキャプチャされます。
- **granular-labels**：詳細なラベルのみをキャプチャします。デフォルトでは、このオプションは無効になっています。

  KPI に詳細なラベルが必要な場合は、そのラベルを構成する必要があります。たとえば、smf_service_stats メトリックの dnn ラベルをキャプチャするには、次の CLI コマンドを構成する必要があります。

  ```
  infra metrics verbose application metrics smf_service_stats level
  debug granular-labels [ dnn ]
  ```

## 設定例

以下は、すべてのアプリケーションメトリックで実稼働レベルのみを有効にする構成例です。

```
infra metrics verbose application level production
```

次に、smf_service_stats アプリケーションメトリックの実稼働レベルを有効にし、他のすべてのアプリケーションメトリックのデバッグレベルを有効にする構成例を示します。

```
infra metrics verbose application smf_service_stats level production
```

次に、smf_service_stats アプリケーション メトリックのデバッグ レベル、および他のすべてのアプリケーション メトリックの詳細なラベルと実稼働レベルを有効にする設定例を示します。

**infra metrics verbose application level production smf_service_stats level debug granular-labels [ dnn ]**

次に、smf_service_stats アプリケーション メトリックの実稼働レベルを有効にする構成例、および他のすべてのアプリケーション メトリックの詳細ラベルおよびデバッグ レベルを示します。

**infra metrics verbose application smf_service_stats level production granular-labels [ dnn ]**

次に、smf_service_stats アプリケーション メトリックと、他のすべてのアプリケーション メトリックのデバッグ レベルを無効にする構成例を示します。

**infra metrics verbose application smf_service_stats level off**

次に、smf_service_stats メトリックの NSSAI ラベルを構成する構成例を示します。

**infra metrics verbose application metrics smf_service_stats level debug granular-labels [ snssai ]**

（注） NSSAI 統計情報は、詳細ラベル構成で NSSAI ラベルを構成しないとペグされません。

## 設定の確認

構成を確認するには、次の show コマンドを使用します。

**show running-config infra metrics verbose application**

**show running-config infra metrics verbose application** コマンドの出力例を次に示します。

```
[smf] smf# show running-config infra metrics verbose application
infra metrics verbose application
 metrics smf_service_stats
  level production
  granular-labels [ dnn ]
 exit
exit
```

次に、smf_service_stats アプリケーション メトリック用の生産ラベルをキャプチャする構成が有効化されており、その他のすべてのアプリケーション メトリックの詳細ラベルとデバッグ レベルも含まれていることを示しています。

```
[smf] smf# show running-config infra metrics verbose application
 infra metrics verbose application
  level production
  metrics smf_service_stats
   level debug
   granular-labels [ [dnn] ]
  exit
exit
```

次に、smf_service_stats アプリケーション メトリック用のデバッグ ラベルをキャプチャする構成が有効化されており、その他のすべてのアプリケーション メトリックの詳細ラベルとデバッグ レベルも含まれていることを示しています。

手順とセッション統計のスライス情報を確認するには、次の show コマンドを使用します。

```
show running-config infra metrics verbose application
infra metrics verbose application
 metrics smf_service_stats
  level debug
  granular-labels [ snssai ]
 exit
```

# バルク統計情報と重要業績評価指標

## 機能説明

このセクションでは、SMF のパフォーマンス分析に使用されるバルク統計と重要業績評価指標（KPI）の詳細について説明します。

バルク統計情報には次の 2 種類があります：

- Gauge：レポートの時点での統計情報を示すスナップショット値（現在の PDP コンテキスト、同時アクティブ EPS ベアラーの数など）。ゲージの統計情報は連続的に増加または減少できます。
- [カウンタ（Counter）]：時間の経過とともに累積された統計を示す履歴値（受信された CSR リクエストの総数など）。次の 2 つの場合を除き、カウンタ値は増分のみ可能です。
  - ロールオーバー：カウンタが最大値を超過し、ゼロにロール オーバーする場合。
  - Reset：カウンタを手動でゼロにリセットする場合。

**Important** サポートされているバルク統計と KPI の完全なリストは、このリリースの対象の *[UCC 5G SMF メトリック参考資料（UCC 5G SMF Metrics Reference）]* を参照します。

# ログ

## 機能説明

システム ロギング機能は、アプリケーション間でログ メッセージをログに記録する共通の方法を提供します。各ログは以下のコンポーネントで構成されています。

- タイムスタンプ：ログ作成の日時を示します。
- ログ メッセージ：特定のログのメッセージを示します。
- ログ レベル：ログ メッセージの重要性レベルを示します。
- ログタグ：モジュール名、コンポーネント名、およびインターフェイス名の詳細を表示します。ログタグは事前に作成され、ロギング中に渡されます。

SMF には、メッセージを記録するためのさまざまなタイプのロギングが用意されています。ロギング タイプには、アプリケーション ロギング、トランザクション ロギング、モニタ サブスクライバ ロギング、およびトレース ロギングがあります。

SMF は、トレース ログやイベント ログなどのさまざまなログを保持します。**kubectl get pods -n** *namespace* CLI コマンドを使用して、現在実行されているすべてのポッドとサービスを確認します。次に、 **kubectl logs** *podname* **-n** *namespace* CLI コマンドを使用して、ポッド内のログを表示します。

この機能の動作中にエラーが発生した場合は、特定のサブスクライバ セッションの SMF サービス ログを使用して、問題を特定し、問題の解決策を決定します。

# OAM および EDR モニタ ポッド ファイルのダウンロード

## 機能説明

**monitor subscriber** コマンド、 **monitor protocol** コマンド、およびトランザクション ログを使用して生成されたファイルは、OAM ポッドに保存されます。OAM ポッドで生成されたファイルが収集され、内部の Apache サーバに保存されます。ユーザー認証後、Web ブラウザを使用してファイルを表示およびダウンロードできます。

**Note** ops-center と同じクレデンシャルを使用して、ブラウザを使用して oam-pod および edr-monitor pod に存在するファイルへのユーザー アクセスを認証します。

ファイルは、それぞれのコマンドが実行されると、個別のフォルダに作成されます。次の OAM および EDR ポッド ファイルをダウンロードできます。

- **サブスクライバ ファイルをモニタ**：これらのファイルは、 **monitor subscriber** CLI オプションを使用して生成され、指定されたサブスクライバに関連するメッセージをトレースします。 **monitor protocol** コマンド用に生成されるファイルは、`monsulogs/` ディレクトリに存在します。
- **モニタ プロトコル ファイル**：これらのファイルは、CLI コマンドで提供される特定のインターフェイスでパケットをキャプチャするために **monitor protocol** CLI オプションを使用しています。 **monitor protocol** コマンド用に生成されるファイルは、 `monprologs/` ディレクトリにあります。
- **トランザクション ログ**：トランザクション ロギングが有効になっている場合、トランザクション ログは oam-pod に送信され、そこからダウンロードできます。有効になっている場合、トランザクション ロギング用に生成されるファイルは、`transactionlogs/` ディレクトリに存在します。
- **EDR ファイル**：これらのファイルは smf サービス ポッドで生成され、edr-monitor ポッドに定期的にコピーされます。ファイルは /edr ディレクトリにあります。

# 機能の仕組み

このセクションでは、oam-pod および edr-monitor pod 内のログ ファイルを表示およびダウンロードする方法について説明します。

### OAM ポッド ファイルのダウンロード

ブラウザを開き、*https://oam-files.<ReleaseName>.<Ingress-host-name>.nip.io/* URL を使用して Apache サーバにログオンします。ops-center のユーザー ログイン情報を使用します。*<ReleaseName>* および *<Ingress-host-name>* を、それぞれリリース名と入力ホスト名に置換します。

oam-pod ディレクトリは、モニタ プロトコル ログ、モニタ サブスクライバ ログ、およびトランザクション ログをアーカイブするフォルダで構成されます。

ディレクトリ フォルダは、実行されたコマンドに従って表示されます。

モニタ プロトコル ファイルをダウンロードするには、次の URL を使用します。

*https://oam-files.<ReleaseName>.<Ingress-host-name>.nip.io/ monprologs/*

上記の URL で、モニタ サブスクライバ ファイルの monprologs を monsulogs に、トランザクション ログ ファイルの transactionlogs に置き換えます。

### EDR ファイルのダウンロード

EDR モニタ ポッドの永続ボリューム内の EDR ファイルにアクセスするには、必要なログイン情報で Ops センターにログオンし、edr-monitor ポッドの入力 URL を使用します。

入力 URL を決定するには、次のコマンドを使用します：

**kubectl get ingress -n** *namespace* **| grep edr**

例：

*cloud-user@svi-cndp-tb41-gr-setup-smf-cluster-2-cndp-server-1:~$* **kubectl get ingress -n smf-smf | grep edr**

# ログの構成

ここでは、ログの構成方法について説明します。

## トランザクション メッセージの有効化または無効化

トランザクション ログ内の要求応答メッセージの存在を有効または無効にするには、次の構成例を使用します。

```
config
  logging transaction message { disable | enable }
  commit
end
```

注：

- **logging transaction message { disable | enable }**：トランザクション ロギングのメッセージを有効にするか無効にするかを指定します。

## トランザクション履歴ログの表示

OAM ポッド シェルのトランザクション履歴を表示するには、SMF Ops センターで次の CLI コマンドを使用します。

**dump transactionhistory**

（注） 最新のトランザクション ログは、トランザクション ログ サイズが 1024 の循環キューに保存されます。

ポッド内のログを表示するには、Kubernetes マスター ノードで次のコマンドを使用します：

**kubectl logs -n** *<SMF namespace> podname*

## トランザクション ログの例

次に、SMF PDU セッションの確立中にモニタ サブスクライバで収集されたトランザクション ログの例を示します。

```
Transaction Log received from Instance: smf.smf-rest-ep.unknown.smf.0
************* TRANSACTION: 00010 *************
TRANSACTION SUCCESS:
    Txn Type             : N10RegistrationRequest(33)
    Priority             : 1
    Session State        : No_Session
LOG MESSAGES:
    2020/03/03 05:31:39.345 [DEBUG] [infra.transaction.core] Processing transaction Id:
 10 Type: 33 SubscriberID: imsi-123456789012345 Keys: []
    2020/03/03 05:31:39.345 [DEBUG] [infra.transaction.core] Trace is disabled
    2020/03/03 05:31:39.346 [TRACE] [infra.message_log.core] >>>>>>>
IPC message
Name: N10RegistrationRequest
MessageType: N10RegistrationRequest
Key:
--body--
{"regInfo":{"ueId":"imsi-123456789012345","pduSessionId":5},"regReq":{"dnn":"intershat",


"pduSessionId":5,"pgwFqdn":"cisco.com.apn.epc.mnc456.mcc123","plmnId":{"mcc":"123","mnc":"456"},


"smfInstanceId":"c388eec5-e2ff-4bda-8154-b5dd9f10ad97","supportedFeatures":"0","singleNssai":{"sd":"Abf123","sst":2}},


"msgReq":{"Type":2,"ServiceName":4,"Versions":["v1"],"ProfileName":"UP1","FailureProfile":"FH1","SvcMsgType":3,

  "Filter":{"Bitmapfeilds":2,"Dnn":"intershat"}}}
    2020/03/03 05:31:39.346 [DEBUG] [nrfClient.Discovery.nrf] Message send Metadata
[Type:UDM ServiceName:nudm-uecm
      ..
      ..
Request
Name: UdmRegistrationRequest
Host:
```

```
http://209.165.200.229:9020/nudm-uecm/v1/imsi-123456789012345/registrations/smf-registrations/5
Method: PUT
RequestURI:
--- Headers ---
Content-Type: application/json
Body:{"dnn":"intershat","pduSessionId":5,"pgwFqdn":"cisco.com.apn.epc.mnc456.mcc123",
"plmnId":{"mcc":"123","mnc":"456"},
"singleNssai":{"sd":"Abf123","sst":2},"smfInstanceId":"c388eec5-e2ff-4bda-8154-b5dd9f10ad97","supportedFeatures":"0"}

    2020/03/03 05:31:39.376 [TRACE] [infra.message_log.core] >>>>>>>
Response
Name:
Response Status 201
--- Headers ---
Location:
http://209.165.200.229:9020/nudm-uecm/v1/imsi-123456789012345/registrations/smf-registrations/5
Content-Length: 225
Content-Type: application/json
Body:{"pgwFqdn": "cisco.com.apn.epc.mnc456.mcc123", "plmnId": {"mcc": "123", "mnc":
"456"}, "dnn": "intershat",
  "smfInstanceId": "524f5f8a-b584-47b8-86f5-a5292eabcdef", "pduSessionId": 5,
"singleNssai": {"sd": "Abf123", "sst": 2}}
    ..
    ..
    ..
--body--
{"regRes":{"dnn":"intershat","pduSessionId":5,"pgwFqdn":"cisco.com.apn.epc.mnc456.mcc123",
"plmnId":{"mcc":"123","mnc":"456"},
  ..
  ..
**********************************************
Transaction Log received from Instance: smf.smf-rest-ep.unknown.smf.0
************* TRANSACTION: 00011 *************
TRANSACTION SUCCESS:
    Txn Type             : N10SubscriptionFetchReq(36)
    Priority             : 1
    Session State        : No_Session
LOG MESSAGES:
    2020/03/03 05:31:39.384 [DEBUG] [infra.transaction.core] Processing transaction Id:
 11 Type: 36 SubscriberID: imsi-123456789012345 Keys: []
    2020/03/03 05:31:39.384 [DEBUG] [infra.transaction.core] Trace is disabled
    2020/03/03 05:31:39.384 [TRACE] [infra.message_log.core] >>>>>>>
IPC message
Name: N10SubscriptionFetchReq
MessageType: N10SubscriptionFetchReq
Key:
--body--
  ..
  ..
Request
Name: UdmSubscriptionRequest
Host:
http://209.165.200.229:9020/nudm-sdm/v1/imsi-123456789012345/sm-data?dnn=intershat&plmn-id=%7B%22mcc%22%3A%22123%22%2C%22mnc%22%3A%2


2456%22%7D&single-nssai=%7B%22sd%22%3A%22Abf123%22%2C%22sst%22%3A2%7D&supported-features=0
Method: GET
RequestURI:
--- Headers ---
IPC message
Name: N10SubscriptionFetchSuccess
MessageType: N10SubscriptionFetchSuccess
Key:
  ..
```

```
  ..
--body--
  ..
  ..
```

## ロギング レベルを構成

ここでは、ロギング レベル パラメータの構成方法について説明します。

次の構成例を使用して、ロギング レベルを構成します：

```
config
  logging level { application | monitor-subscriber | tracing |transaction
 }
  end
```

注：

- **logging level { application | monitor-subscriber | tracing | transaction }**：トランザクション ログ コンフィギュレーション モードを開始します。
  - **application** ：オプションのアプリケーション ロギング レベルを構成します。
  - **monitor-subscriber** ：オプション モニタ サブスクライバのロギング レベルを構成します。
  - **tracing** ：オプションのロギング レベル トレースを構成します
  - **transaction** ：オプションのトランザクション ロギング レベルを構成します。

## 永続的なトランザクション ログの構成

このセクションでは、永続的なトランザクション ログのパラメータを構成する方法について説明します。

トランザクション ログは、OAM ポッドのトランザクション ログ ディレクトリにあるトランザクション ログ ファイルに保存されます。

構成例を使用して、永続トランザクション ログを構成します。

```
config
  logging transaction persist enable { max-file-size | max-rotation }
  end
```

注：

- **logging transaction**：トランザクション ログ コンフィギュレーション モードを開始します。
- **persist enable { max-file-size | max-rotation }** ：トランザクション ログ ファイルへのトランザクション ログの書き込みを有効にするオプションを構成します。
  - **max-file-size** *max_filesize*：ファイルに保持する必要があるトランザクション ログの最大サイズ（MB 単位）を指定します。デフォルトのサイズは 50 MB です。指定できる範囲は 1 ～ 10000 MB です。

- **max-rotation** *max_rotation*：フォルダに保存する必要があるファイルの最大数を指定します。指定された数に達すると、ファイルのローテーションが開始されます。このローテーションにより、最も古いファイルが削除され、最新のログ ファイルがフォルダに追加されます。たとえば、フォルダにファイル a1.txt-a.10.txt があり、a.11.txt が追加されると、a1.txt が削除されます。デフォルトの数は 10 です。許容範囲は 2 ～ 1000 です。

- **persist enable** ：トランザクション ログ ファイルへのトランザクション ログの書き込みを無効にします。

### 永続的なトランザクション ログの表示

このセクションでは、OAM ポッドに保存されているトランザクション ログを表示する方法について説明します。

永続的なトランザクション ログを表示するには、SMF Ops Center を介して次の構成を使用します。

**transaction file dump filename** *file_path*

**transaction log list** コマンドを使用して、ログ ファイルとそのパスのリストを表示できます。

次に、トランザクション ログの出力例を示します。

```
RELEASE_NAMESPACE: 'example-data'
Dumping file 'transactionlogs/transaction.log.20200907033433.4.gz'
InstanceInfo: example.example-rest-ep.cluster1.example-data.1
TimeStamp: 2020-09-09 00:25:18.379439773 +0000 UTC
************* TRANSACTION: 01371 *************
TRANSACTION SUCCESS:
    Txn Type             : MessageTypeExampleCreate(1)
    Priority             : 1
    Session Namespace    : none(0)
LOG MESSAGES:
    2020/09/09 00:25:18.339 [INFO] [rest_ep.app.n7] Message Example_Create decod
ed
    2020/09/09 00:25:18.339 [INFO] [rest_ep.app.n7] Process init
    2020/09/09 00:25:18.339 [DEBUG] [rest_ep.app.n7] Config from GetConfig is Ve
rsion: 783da2fc038c6bc961a95e2bf3dd6d93f282e36b30e0362698a1de369a2fd15c Services
: [Name: restServer Type: Rest Endpoint: sbi Name: tcpServer Type: Tcp Endpoint:
 tcp-protocol Name: udpServer Type: Udp Endpoint: udp-protocol]
    2020/09/09 00:25:18.339 [INFO] [rest_ep.app.n7] Process continue
    2020/09/09 00:25:18.339 [DEBUG] [rest_ep.app.n7] DerivedConfig from GetConfi
g is DerivedNameToBeTested_cb3383b95927a434d42cd9d5687ccf1b13e2de4b2faf4543287a3
4afb32518fe
    2020/09/09 00:25:18.339 [DEBUG] [rest_ep.udp.n5] Sending message Example_Cre
ate to example-service
    2020/09/09 00:25:18.342 [INFO] [infra.transaction.core] Calling RPC example-
service_ipc_stream on host example-service_1 proc-name example-service_ipc_strea
```

## JSON ロギングのイネーブル化またはディセーブル化

ポッド ログの JSON ロギングを有効または無効にするには、次の構成例を使用します。

```
config
  [no] logging json-logging [ application | monitor-subscriber |
```

```
transaction ]
end
```

注：

- **no**：ポッド ログの JSON ロギングを無効にします。
- **logging json-logging [ application | monitor-subscriber | transaction ]**：SMF ベースのアプリケーション ポッドが **application**、**monitor-subscriber**、および **transaction** ログ タイプの JSON 形式でのロギングを開始できるようにします。

# イベント障害のログ

表 *585 :* 機能の履歴

| 機能名 | リリース情報 | 説明 |
|---|---|---|
| セッション レポートの手順のイベント障害ログ | 2025.01.0 | この機能を使用すると、一貫性のあるイベント障害ログが拡張され、SMF、PGW、hSMF、および vSMF インターフェイスのセッション レポート手順をサポートします。 |
| vSMF インターフェイスのイベント障害ログ | 2024.04.0 | この機能を使用すると、一貫性のあるイベント障害ログが拡張され、vSMF インターフェイスの作成、挿入、リリース、および更新手順をサポートするようになります。 |
| リリース手順のイベント障害ログ | 2024.03.0 | この機能により、一貫したイベント障害ログが拡張され、SMF、4G、および hSMF インターフェイスのリリース手順がサポートされます。<br>**デフォルト設定**： 該当なし |

| 機能名 | リリース情報 | 説明 |
| --- | --- | --- |
| イベント障害ログ | 2024.02.0 | SMF は次のサポートを提供します。<br>• ポッド間で一貫したイベント障害ログ（作成、アイドル、またはアクティブ手順）<br>• ポッド タイプでの構成可能なログ<br>• 要求と応答の詳細を 1 行形式で含める<br><br>不要なシステム ログが大量に生成されると、メモリ消費が増加し、パフォーマンスが悪化し、ログの管理と使用が非効率的になります。これらの問題を防ぐために、さまざまなポッドで一貫したエラー ログ メッセージ形式が導入されました。SMF 手順の拡張エラー ロギングにより、メモリ使用量の削減、システム生成ログ数の最小化、詳細で一貫性のある構成可能なロギングが実現され、効果的なデバッグやシステム モニタリングに役立ちます。<br><br>**デフォルト設定**： 該当なし |

SMF 手順のエラー ロギング機能が強化され、詳細で一貫性のある構成可能なロギングが提供されます。これらの機能拡張は、効果的なデバッグとシステム モニタリングに役立ちます。拡張機能は次のとおりです。

- 一貫したログ形式：単一行のログ形式は、ログの記録および解釈方法を統一するために、REST エンドポイントやサービス ポッドなど、さまざまなポッド間で標準化されています。
- ロギングの有効化と無効化：ロギングを有効または無効にするオプションは、特定のポッド タイプで使用できます。このオプションを使用すると、ログストレージを柔軟に管理できます。

- 詳細なログコンテンツ：ログには、プライマリ キー、インターフェイス、手順の詳細、メッセージ要求と応答などの包括的な詳細が含まれます。このレベルの詳細は、デバッグと分析の詳細に役立ちます。
- ログ レベル管理：デフォルトでは、ログは INFO レベルで書き込まれます。必要に応じて、ログを有効にできます。ログを有効にすると、生成および保存されるログデータの量を制御できます。

  デフォルトでは、ログ レベルは WARN に設定され、ロギングはデフォルトで無効になります。必要に応じてロギングを有効にできます。
- 共通ロギング インターフェイス：イベント ロギング用に共通のインターフェイスが実装されます。すべてのコンポーネントで、同じロギング標準と形式に対してこのインターフェイスが使用されます。
- ログ タグ：ログタグが強化され、特定のポッド タイプまたはサービスのログを有効または無効にし、ロギングをきめ細かく制御できるようになりました。
- サポートされるログ：ロギングは、さまざまな手順、ポッド、およびインターフェイスでサポートされています。

## イベント障害ロギングの仕組み

各ポッド全体で一貫したログ形式を持つために、各コンポーネントはイベント ロギングに共通のインターフェイスを使用します。ログは JSON 形式を使用するため、すべてのデータが 1 行に表示されます。ログは INFO レベルで書き込まれるため、デフォルトではこのレベルを無効にして、必要な場合に有効にできます。

ログタグの形式は次のとおりです。

**transaction.event.<pod-type>**。**<pod-type>** は、ポッドが使用するサービス名です。たとえば、est-ep または、smf-service です。

ログ タグを使用すると、特定のポッド タイプまたはサービスのログを有効または無効にできます。

ログは、対応するログ レベルが INFO、DEBUG、または TRACE に設定されている場合に書き込まれます。ただし、メッセージの要求または応答フィールドは、ログ レベルが DEBUG または TRACE に設定されている場合にのみ入力されます。

ログの例：

### サンプル ログ

```
smf-service-1 [INFO] [Transaction.go:1576] [transaction.event.smf-service]
 {"TxnId":2,"StartTime":"2024-03-01T08:16:54Z","GRInstanceId":1,"TxnType":
"N7SmPolicyCreateReq","Priority": 33,"SessionNamespace":"smf(1)",
"CdlSliceName":"1","SubscriberId": "imsi-123456789012345", "SessionPrimaryKey":
"imsi-123456789012345:5","SessionKeys":"imsi-123456789012345:5 (pk)
roaming-status:homer (nuk) ue-type:nr-capable (nuk) supi:imsi-123456789012345 (nuk)
gpsi:msisdn-223310101010101 (nuk) pei:imei-123456786666660 (nuk) psid:5 (nuk)
snssai:002abf123 (nuk)
dnn:intershat (nuk) emergency:false (nuk) rat:e-utran (nuk) access:3gpp access (nuk)
connectivity:4g (nuk) udm-sdm:10.1.10.69 (nuk) auth-status:unauthenticated (nuk)
```

```
rulebase:starent (nuk)
policy:1(nuk)","SessionState":"Create_Session","ErrorMessage":"
{\"ErrType\":3,\"StatusCode\":500,
\"N1SmCause\":0,\"Detail\":\"\",\"InvalidParams\":null,\
"Title\":\"\",\"SourceDetails\":\"/opt
/workspace/smf-service/src/smf-service/procedures/4g/pdnsetup/idlestate.go:1318\"}",
"MessageRequest":{"smPolicyRequestPB": {"PolicyRequestPB":{"smPolicyCreateRequest":
{"smContextCreateData":{"accessType":1,"chargingcharacteristics":"1","dnn":
"intershat","gpsi":"msisdn-223310101010101","pduSessionId":5,"pduSessionType":1,
"pei":"imei-123456786666660","ratType":2,"servingNetwork":{"mcc":"123","mnc":
"456"},"sliceInfo": {"sd":"Abf123","sst":2},"subsDefQos":{"_5qi":5,"arp":
{"preemptCap":1,"preemptVuln":1,"priorityLevel":15},"priorityLevel":15},
"subsSessAmbr":{"downlink":"4096 Kbps","uplink":"4096 Kbps"},"supi":
"imsi-123456789012345","suppFeat":"407B","ueTimeZone":"+00:15+1",
"userLocationInfo":{"eutraLocation":{"ecgi":{"eutraCellId":"1234567","plmnId":
{"mcc":"123","mnc":"456"}},"tai":{"plmnId":{"mcc":"123","mnc":"456"},
"tac":"1820"},"ueLocationTimestamp":"2024-03-01T08:16:54Z"}},
"smPoliciesUpdateNotificationUrl":"http://10.1.8.54:8090/callbacks/v1/
smPoliciesUpdateNotification/imsi-123456789012345:5:1709281014408558981",
"recoveryTime":"2024-03-01T07:25:54Z","smfId":"94c78abd-ed68-49bb-b382-fd879504b702","servNfId":
{"anGwAddr":{"anGwIpv4Addr":"10.1.10.69"}}}}}, "commonApplMetaData":{"NFType":4,
"ApplData":{"smfApplData":{"Dnn":"intershat","ProcType":"PDN Connect [LTE]",
"RatType":"EUTRA","reason":1,"SessType":"ipv4","PduSessionId":"imsi-123456789012345:5"}}}},
"msgReq": "CAcYEkoCdjFiA1BQMWoNCAISCWludGVyc2hhdLoBA0ZIMcABCIgCApoCBAgCEAGaAgQIARACsAIg"},

"MessageResponse":{"PolicyResponsePB":null,"locationHeader": "http://10.1.10.69:9013
/npcf-smpolicycontrol/v1/sm-policies/imsi-123456789012345_5", "msgRsp":
"CAcYlAMwEmIDUFAxalFodHRwOi8vMTAuMS4xMC42OTo5MDEz L25wY2Ytc21wb2xpY3ljb250cm9s
L3YxL3NtLXBvbGljaWVzL2ltc2ktMTIzNDU2Nzg5MDEyMzQ1XzVwgxq
AAQKiAQNGSDGqARJQQ0YtZG5uPWludGVyc2hhdDs="}}
```


## サポートされるログ レベル

SMF では、次のログ レベルがサポートされています：

- デバッグ：このレベルは、アプリケーション動作とイベント（変数値、関数呼び出し、コンポーネント間の連携動作など）に関する詳細なメッセージを取得するために使用されます。この情報は、アプリケーションの開発およびデバッグ時に役立ちます。
- 情報：このレベルは、アプリケーションの進行状況に関する高レベルの情報の提供に使用されます。これらのメッセージはデバッグ メッセージよりも詳細度は低くなりますが、アプリケーションが期待どおりに機能しているかどうかを確認するために使用されます。このレベルは、重要なタスク、構成の設定、または操作の正常な完了などのアプリケーション マイルストーンをログに記録するために使用されます。

## サポートされているログ

次の表に、SMF でサポートされているロギングの手順、ポッド、およびインターフェイスを示します。

表 *586 :* サポーされるログ

| サポートされているロギングを使用する **SMF** 手順 | ロギングに関係するポッド | ポッドと関連付けられている **SMF** インターフェイスと手順 | ポッドと関連付けられている **P-GW** インターフェイス（**4G/Wi-Fi**）と手順 | ポッドと関連付けられている **hSMF** インターフェイスと手順 | ポッドと関連付けられている **vSMF** インターフェイスと手順 |
|---|---|---|---|---|---|
| 作成（Create） | REST-EP | N10、N40、N7、N11 | N10、N40、N7 | — | N16、N40、N11 |
| | SERVICE | N10、N40、N7、N11、N4、RMGR | N10、N40、N7、N4、RMGR | — | N40、N11、N4、RMGR |
| | PROTOCOL | N4 | N4、GTP | — | N4 |
| アイドル/アクティブ | REST-EP | N11 | — | — | — |
| | SERVICE | N11、N4 | — | — | — |
| | PROTOCOL | N4 | — | — | — |
| リリース | REST-EP | N10、N40、N7、N11 | N10、N40、N7、N16 | N10、N40、N7、N16 | N16、N40、N11 |
| | SERVICE | N10、N40、N7、N11、N4、RMGR | N10、N40、N7、N4、RMGR | N10、N40、N7、N16、N4、RMGR | N16、N40、N11、N4、RMGR |
| | PROTOCOL | N4 | N4、GTP | N4 | N4 |
| セッションレポート | REST-EP | N40 | N40 | N40 | N40 |
| | SERVICE | N40、N4 | N40、N4 | N40、N4 | N40、N4 |
| | PROTOCOL | N4 | N4 | N4 | N4 |
| 更新 | PROTOCOL | — | — | — | N4 |

## イベント ロギングの有効化

SMF サービスのイベント ログを有効または無効にするには、次の手順を使用します。CLI コマンドを使用して適切なログ レベル構成を行うことで、生成されるログ データの量とタイプを制御できます。したがって、この構成は効果的なモニタリング、トラブルシューティング、およびパフォーマンス管理に役立ちます。

手順

**ステップ 1** イベント ロギングのログ レベルを指定します。

**logging name transaction.event.**<*podname*> **level application** *application_log_level*

<pod-type> は、ポッドが使用するサービス名です。

例：

```
[smf] smf# config
[smf] smf(config)# logging name transaction.event.smf-service level application [ debug
 | error | info | off | trace | warn ]
```

例：

（注）
サポートされているデバッグ レベルと情報レベルについてのみ、ログを有効または無効にできます。

**ステップ 2** [オプション] show running-config loggingコマンドを使用して、構成されたアプリケーション イベント ロギング レベルを確認します。

例：

```
[[smf] smf# show running-config logging
Thu Jun  20 18:50:12.888 UTC+00:00
logging level tracing debug
logging name infra.config.core level application trace
logging name infra.config.core level transaction trace
logging name infra.config.core level tracing off
logging name infra.message_log.core level transaction trace
logging name transaction.event.smf-service level application debug
```

# ディスパッチャ

## 機能説明

ディスパッチャは、GTP および PFCP でのキューの数とキューのサイズを構成したアドミッション率の入力スロットリング構成です。

### S11 インターフェイスでのディスパッチャの構成制限

影響を受けると、IMS ベアラーは、入力プロトコル ディスパッチャで S11 インターフェイスと GTPv2 メッセージがドロップするため、音声コールが失敗します。

cnSGW での S11 プロトコル ディスパッチャの構成はスタティックであり、実稼働要件に基づいて調整する必要があります。構成がサービスされている MME プールに対して適切でない場

合、1 秒あたりのコール イベント数（CEPS）が高くなると、GTPv2 メッセージがドロップされます。

GTPv2-S11 は、入力でのディスパッチャ キューの制限が原因で廃棄またはドロップされます。これには、リリースアクセスベアラー（RAB）、ベアラー要求の変更（MBR）、DDN 確認応答などの要求または応答メッセージが含まれます。たとえば、既存の音声ベアラーを持つMMEからのMBRのドロップは、コールのドロップを発生させます。EPS フォールバック（EPSFB）の一部としての音声ベアラー転送による MME からの MBR のドロップにより、EPSFB コールのセットアップの失敗（音声アクセス失敗率（AFR））が発生します。

# S11 インターフェイス用のディスパッチャの構成

S11 インターフェイスのディスパッチャを構成するには、次の構成例を使用します：

```
config
   interface interface_name
      sla response response_time_value
      dispatcher
         count count_value
         capacity capacity_value
         outbound [ true | false ]
         cache [ true | false ]
         threshold threshold_value
         expiry expiry_time_value
         nonresponsive nonresponsive_time_value
     exit
```

注：

- **interface** *interface_name*：インターフェイス名を S11 として指定します。
- **sla response** *response_time_value*：SLA 応答時間を指定します。 *response_time_value* は 整数である必要があります。
- **count** *count_value*：ディスパッチャ キューの数を指定します。
- **capacity** *capacity_value*：各ディスパッチャ キューのキュー サイズを指定します。
- **outbound [ true | false ]**：この値を指定して、発信メッセージのキューサポートを有効または無効にします。
- **cache [ true | false ]**：キャッシュの再送信を有効または無効にするには、この値を指定します。
- **threshold** *threshold_value*：キュー キャッシュごとの未処理のリクエストのしきい値を指定します。
- **expiry** *expiry_time_value*：応答されたキャッシュ エントリの有効期限をミリ秒単位で指定します。

- **nonresponsive** *nonsensitive_time_value*：非応答キャッシュ エントリの有効期限のこの値をミリ秒単位で指定します。

## 設定例

次に、S11 インターフェイスのディスパッチャの構成例を示します。

```
interface s11
   sla response 5500
   dispatcher
    count         10
    capacity      100000
    outbound      true
    threshold     160000
    expiry        7000
    nonresponsive 6000
   exit
```

# OAM サポート

このセクションでは、ディスパッチャでサポートされているメトリックについて詳しく説明します。

## メトリック

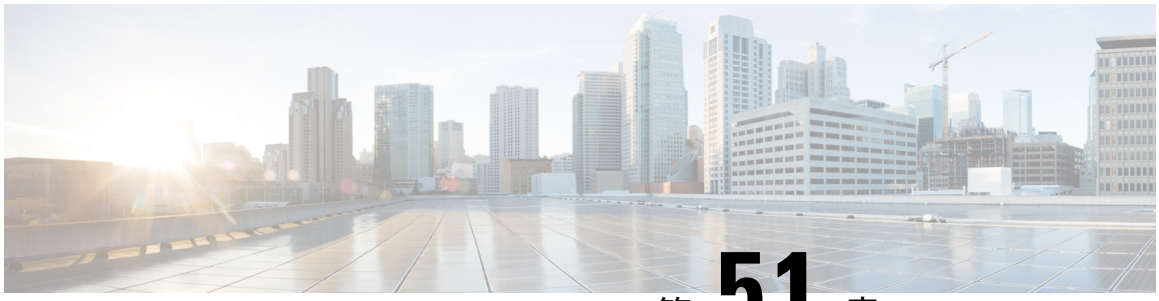
ディスパッチャ キューが構成されている場合に、特定のイベントをキャプチャするために、次の新しいメトリックが導入されました。

**メトリック名**： outgoing_drop_queued_total

**説明**： メトリックは、UDP クライアントで構成されたディスパッチャ キューがいっぱいで、構成されたキュー容量を超える数のメッセージがロードされている場合に、特定のイベントをキャプチャします。

このメトリックには、次のラベルが追加されます：

- **local_address**： UDP エンドポイントが開始されているローカル UDP アドレス。
- **interface**： エンドポイント構成で構成される UDP インターフェイスの名前。
- **protocol**： エンドポイント構成で構成されたプロトコルの名前。例：UDP
- **queue_id**： 送信元 IP アドレスに基づくキュー インデックス番号。
- **peer_address**： ピア エンドポイントの IP アドレス。
- **cause**： キューからメッセージがドロップされた理由。たとえば、理由の 1 つはディスパッチャ キューがいっぱいであることです。
- **queue_type**： ディスパッチャ構成で構成されたキューのタイプ。



第 51 章

# SMF 構成例


• 設定例 （2115 ページ）


## 設定例

以下は、選択に応じて個別に提供されたサンプルの構成ファイルです。展開の具体的なニーズに応じて、独自の構成ファイルを作成および変更する必要があります。

```
profile compliance comp1
 service nsmf-pdusession
  version uri v1
  version full 1.0.2
  version spec 15.4.0
 exit
 service namf-comm
  version uri v1
  version full 1.0.2
  version spec 15.4.0
 exit
 service n1
  version uri v1
  version full 1.0.0
  version spec 15.4.0
 exit
 service n2
  version uri v1
  version full 1.0.0
  version spec 15.4.0
 exit
 service nudm-sdm
  version uri v2
  version full 2.0.1
  version spec 15.4.0
 exit
 service nudm-uecm
  version uri v1
  version full 1.0.2
  version spec 15.4.0
 exit
 service nnrf-disc
  version uri v1
  version full 1.0.2
  version spec 15.4.0
 exit
```

```
 service nnrf-nfm
  version uri v1
  version full 1.0.2
  version spec 15.4.0
 exit
 service npcf-smpolicycontrol
  version uri v1
  version full 1.0.2
  version spec 15.4.0
 exit
 service nchf-convergedcharging
  version uri v2
  version full 2.0.1
  version spec 15.3.0
 exit
exit
profile network-element amf amf1
 nf-client-profile        AP1
 failure-handling-profile FH3
 query-params [ dnn target-nf-instance-id ]
exit
profile network-element udm udm1
 nf-client-profile        UP1
 failure-handling-profile FH1
 query-params [ target-plmn target-nf-instance-id ]
 query-target-plmn        primary
exit
profile network-element pcf pcf1
 nf-client-profile        PP1
 failure-handling-profile FH1
 query-params [ dnn target-plmn target-nf-instance-id requester-snssais ]
 rulebase-prefix          cbn#
 predefined-rule-prefix   crn#
 use-amf-provided-pcf     true
exit
profile network-element chf chf1
 nf-client-profile                CP1
 failure-handling-profile         FH2
 query-params [ dnn target-plmn chf-supported-plmn ]
 query-target-plmn                primary
 nf-client-profile-offline        CP2
 failure-handling-profile-offline FH2
exit
profile network-element chf chgser1
exit
profile network-element sepp sepp1
 nf-client-profile hsepp
exit
profile network-element upf upf1
 n4-peer-address ipv4 209.165.200.231
 n4-peer-port      8805
 upf-group-profile upfGroup1
 dnn-list          [ cisco intershat starent ]
 capacity          65535
 priority          1
exit
profile network-element upf upf2
 n4-peer-address ipv4 209.165.200.232
 n4-peer-port 8805
 dnn-list     [ cisco intershat starent ]
 capacity     65535
 priority     2
exit
profile network-element upf upf3
```

```
 node-id      toolsUPF
 n4-peer-address ipv4 209.165.200.233
 n4-peer-port 8805
 dnn-list     [ cisco intershat starent ]
 capacity     32768
 priority     10
exit
profile upf-group upfGroup1
 heartbeat
  interval               63
  retransmission-timeout 3
  max-retransmissions    5
 exit
 supported-features [ secondary-pdr ]
exit
profile wps wps1
 arp              1-15
 dscp n3 0x14
 dscp sxa 0x22
 dscp s5e 0x24
 dscp s11 0x26
 message-priority [ pfcp gtpc ]
exit
profile wps wps_F5972
 arp              1-4,14
 dscp n3 0x0F
 message-priority [ pfcp gtpc ]
exit
profile pcscf pcscf1
 v4-list
  precedence 3
   primary 209.165.201.1
   secondary 209.165.201.2
  exit
 exit
 v6-list
  precedence 3
   primary 33:33::1
   secondary 33:33::2
  exit
 exit
 v4v6-list
  precedence 3
   primary ipv4 209.165.200.225
   primary ipv6 fd01:976a:c305:9::5
   secondary ipv4 209.165.200.26
   secondary ipv6 46:46:33::2
  exit
 exit
exit
profile icmpv6 icmpprf1
 options virtual-mac b6:6d:57:45:45:45
exit
profile charging chgprf1
 method                  [ offline ]
 limit volume 10000000
 limit duration 7200
 accounting limit volume downlink 100000 total 100000 uplink 100000
 accounting triggers [ qos-change rat-change serv-node-change ambr-change ue-time-change
 plmn-change user-loc-change ]
 tight-interworking-mode true
 quota request always
 quota suppress triggers [ qht ]
 reporting-level online rating-group
```

```
 reporting-level offline service-id
exit
profile charging chgprf2
 method                  [ offline ]
 accounting limit volume downlink 100000 total 100000 uplink 100000
 accounting triggers [ qos-change rat-change serv-node-change ambr-change ue-time-change
 plmn-change user-loc-change ]
 tight-interworking-mode true
 quota request always
 quota suppress triggers [ qht ]
 reporting-level online rating-group
 reporting-level offline service-id
exit
profile charging chgprf3_roaming
 method [ offline ]
exit
profile charging-characteristics 1
 charging-profile     chgprf2
 charging-qbc-profile qbc_general
exit
profile charging-qbc qbc_general
 limit volume 20500
 limit duration 70
 max-charging-condition 1
 max-deferred-urr       2
 triggers               [ ambr-change qos-change user-loc-change ]
exit
profile charging-qbc qbc_hsmf1
 limit volume 40500
 limit duration 140
 triggers [ ambr-change qos-change serv-node-change user-loc-change ]
exit
profile failure-handling FH1
 interface pfcp
  message N4SessionEstablishmentReq
   cause-code pfcp-entity-in-congestion action retry-terminate max-retry 2
   cause-code system-failure action terminate
   cause-code service-not-supported action terminate
   cause-code no-resource-available action retry-terminate max-retry 3
   cause-code no-response-received action retry-terminate max-retry 1
   cause-code reject action terminate
  exit
  message N4SessionModificationReq
   cause-code mandatory-ie-incorrect action terminate
   cause-code session-ctx-not-found action terminate
   cause-code reject action terminate
  exit
 exit
 interface sxa
  message SessionEstablishmentReq
   cause-code 2-255 action retry-terminate max-retry 4
  exit
 exit
exit
profile failure-handling gtp1
 interface gtpc message S5S8CreateBearerReq
  cause-code temp-fail
   action retry timeout 1000 max-retry 2
  exit
 exit
 interface gtpc message S5S8UpdateBearerReq
  cause-code temp-fail
   action retry timeout 1000 max-retry 2
  exit
```

```
 exit
 interface gtpc message S5S8DeleteBearerReq
  cause-code temp-fail
   action retry timeout 1000 max-retry 2
  exit
 exit
exit
profile access access1
 n26 idft enable timeout 15
 n2 idft enable timeout 15
 gtpc gtpc-failure-profile gtp1
 erir delay 1
 eps-fallback cbr delay 3000 max-retry 1 timeout 1
exit
profile access idft
 n1 t3591-pdu-mod-cmd timeout 2 max-retry 1
 n1 t3592-pdu-rel-cmd timeout 2 max-retry 1
 n26 idft enable timeout 15
 n2 idft enable timeout 15
 erir delay 2000
exit
profile tai-group TA1
 mcc 123 mnc 456
  tac list [ 00092a 2346 2356 ]
 exit
 mcc 310 mnc 260
  tac list [ 00092a 2346 2356 ]
  tac range start 1234 end 7890
  exit
 exit
 mcc 310 mnc 310
  tac list [ 2346 2356 2378 ]
  tac range start 5676 end 5767
  exit
 exit
exit
profile tai-group TA2
 mcc 310 mnc 260
  tac list [ 2346 5676 ]
 exit
exit
profile tai-group tgp2
 mcc 091 mnc 05
 exit
exit
profile ecgi-group ECGI1
 mcc 122 mnc 234
  ecgi range start 1234567 end 1234577
  exit
 exit
 mcc 123 mnc 456
  ecgi range start 1234567 end 1234577
  exit
 exit
 mcc 310 mnc 260
  ecgi range start 1234567 end 1234577
  exit
 exit
 mcc 310 mnc 310
 exit
exit
profile ecgi-group ECGI2
exit
profile ncgi-group NCGI1
```

```
 mcc 123 mnc 456
  ncgi range start 123456788 end 133456789
  exit
 exit
 mcc 310 mnc 260
  ncgi list [ 123456789 ]
  ncgi range start 123456788 end 234567891
  exit
 exit
 mcc 310 mnc 310
  ncgi list [ 123456789 133456789 ]
  ncgi range start 234567891 end 244567891
  exit
 exit
exit
profile ncgi-group NCGI2
 mcc 123 mnc 456
  ncgi range start 123456789 end 133456789
  exit
  ncgi range start 234567891 end 244567891
  exit
 exit
 mcc 310 mnc 260
  ncgi range start 123456789 end 133456789
  exit
 exit
exit
profile location-area-group loc1
 tai-group  TA1
 ecgi-group ECGI1
 ncgi-group NCGI1
exit
profile location-area-group loc2
 tai-group  TA2
 ncgi-group NCGI1
exit
profile radius
 deadtime           2
 detect-dead-server response-timeout 2
 max-retry          2
 timeout            2
 enable-packet-dump
 server 209.165.200.248 1812
  type     auth
  secret   $8$j1Tgf1IvRvdywBgDZsP7q7FPzo87+/c1QV99bLxz6AY=
  priority 1
 exit
 server 209.165.200.248 1813
  type     acct
  secret   $8$bANgMCn/x7CspByC/q5Jm1sMo5d9TZMKdTbEq7543wc=
  priority 10
 exit
 attribute
  nas-identifier CISCO-SMF
 exit
 accounting
  algorithm first-server
  max-retry 3
  timeout   1
  attribute
   nas-identifier CISCO-ACCT-SMF
  exit
 exit
 server-group sg1
```

```
  server auth 209.165.200.248 1812
  exit
  server acct 209.165.200.248 1813
  exit
  attribute
   nas-ip 209.165.200.226
  exit
  accounting
   attribute
    nas-ip 209.165.200.226
   exit
  exit
 exit
exit
profile radius-dynamic-author
 client 209.165.200.248
  secret $8$G7fLQoqcBFPFpZNstAQUT/VtoxHqGqwPdLNB1PliHOI=
 exit
exit
profile dnn cisco
 dns primary ipv4 209.165.200.239
 dns primary ipv6 2001:4870:e00b:1a::3
 dns secondary ipv6 2001:4870:e00b:1a::5
 network-element-profiles chf chf1
 network-element-profiles amf amf1
 network-element-profiles pcf pcf1
 network-element-profiles udm udm1
 network-element-profiles sepp sepp1
 dnn cisco network-function-list [ upf upf2 ]
 dnn rmgr cisco
 timeout absolute 360000 up-idle 900 cp-idle 1500
 charging-profile           chgprf1
 charging-qbc-profile       qbc_hsmf1
 virtual-mac                b6:6d:47:47:47:47
 pcscf-profile              pcscf1
 wps-profile                wps1
 ssc-mode 1 allowed [ 3 ]
 session type IPV4 allowed [ IPV6 IPV4V6 ]
 upf apn cisco
 qos-profile                qos_nonStdQci
 authentication secondary radius group sg1
 authentication algorithm pap 1 password-use-pco chap 2 convert-to-mschap mschap 3
 always-on                  false
 userplane-inactivity-timer 300
 only-nr-capable-ue         true
exit
profile dnn intershat
 dns primary ipv4 209.165.200.239
 dns primary ipv6 2001:4870:e00b:1a::3
 dns secondary ipv6 2001:4870:e00b:1a::5
 network-element-profiles chf chf1
 network-element-profiles amf amf1
 network-element-profiles pcf pcf1
 network-element-profiles udm udm1
 network-element-profiles sepp sepp1
 timeout absolute 360000 up-idle 900 cp-idle 1500
 charging-profile           chgprf1
 charging-qbc-profile       qbc_hsmf1
 virtual-mac                b6:6d:47:47:47:47
 nexthop-forwarding-address ipv4 209.165.200.254
 nexthop-forwarding-address ipv6 8454:8454::8454
 pcscf-profile              pcscf1
 wps-profile                wps1
 ssc-mode 1
```

```
 session type IPV4 allowed [ IPV6 IPV4V6 ]
 qos-profile                qos_nonStdQci
 authentication secondary radius group sg1
 authentication algorithm pap 1 password-use-pco chap 2 convert-to-mschap mschap 3
 always-on                  false
 dcnr                       true
 userplane-inactivity-timer 1800
 only-nr-capable-ue         true
 emergency                  false
exit
profile dnn sos
 network-element-profiles chf chf1
 network-element-profiles amf amf1
 network-element-profiles pcf pcf1
 network-element-profiles udm udm1
 virtual-mac b6:6d:47:47:47:47
 ssc-mode 1
 session type IPV4 allowed [ IPV6 IPV4V6 ]
 authorization local
 emergency   true
exit
profile dnn starent
 dns primary ipv4 209.165.200.226
 dns primary ipv6 2001:4870:e00b:1a::3
 dns secondary ipv6 2001:4870:e00b:1a::5
 network-element-profiles chf chf1
 network-element-profiles amf amf1
 network-element-profiles pcf pcf1
 network-element-profiles udm udm1
 dnn cisco network-function-list [ upf upf2 ]
 timeout absolute 360000 up-idle 60 cp-idle 600
 charging-profile           chgprf1
 virtual-mac                b6:6d:47:47:47:47
 pcscf-profile              pcscf1
 wps-profile                wps2
 ssc-mode 1
 session type IPV4 allowed [ IPV6 IPV4V6 ]
 upf apn intershat
 qos-profile                qos_F5972
 always-on                  false
 userplane-inactivity-timer 300
 only-nr-capable-ue         true
 emergency                  false
exit
profile sgw-qos-profile sgw-non-standardqci
 dscp-map operator-defined-qci 128 non-gbr arp-priority-level 5 uplink user-datagram
dscp-marking 0x1e
 dscp-map operator-defined-qci 128 non-gbr arp-priority-level 5 downlink user-datagram
dscp-marking 0x22 encaps-header copy-inner
exit
profile qos 5qi-to-dscp-mapping-table
 dscp-map qi5 1 uplink user-datagram dscp-marking 0x2D
 dscp-map qi5 1 downlink encsp-header dscp-marking 0x2F
 dscp-map qi5 3 uplink user-datagram dscp-marking 0x0c
 dscp-map qi5 3 downlink encsp-header dscp-marking 0x0c
 dscp-map qi5 5 uplink user-datagram dscp-marking 0x3D
 dscp-map qi5 5 downlink encsp-header dscp-marking 0x3F
 dscp-map qi5 6 uplink user-datagram dscp-marking 0x0c
 dscp-map qi5 6 downlink encsp-header dscp-marking 0x0c
 dscp-map qi5 7 uplink user-datagram dscp-marking 0x0e
 dscp-map qi5 7 downlink encsp-header dscp-marking 0x0e
 dscp-map qi5 8 uplink user-datagram dscp-marking 0x0e
 dscp-map qi5 8 downlink encsp-header dscp-marking 0x0e
 dscp-map qi5 9 uplink user-datagram dscp-marking 0x0a
```

```
 dscp-map qi5 9 downlink encsp-header dscp-marking 0x0a
 dscp-map qi5 43 uplink user-datagram dscp-marking 0x1D
 dscp-map qi5 43 downlink encsp-header dscp-marking 0x1F
exit
profile qos abc
 ambr ul "250 Kbps"
 ambr dl "500 Kbps"
 qi5      7
 arp priority-level 14
 arp preempt-cap NOT_PREEMPT
 arp preempt-vuln PREEMPTABLE
 priority 120
 max data-burst 2000
 dscp-map qi5 1 arp-priority-level 12 uplink user-datagram dscp-marking 0x2e
 dscp-map qi5 1 arp-priority-level 12 downlink user-datagram dscp-marking 0x12 encsp-header
 copy-inner
 dscp-map qi5 1 uplink user-datagram dscp-marking 0x2e
 dscp-map qi5 1 downlink user-datagram dscp-marking 0x12 encsp-header copy-inner
 dscp-map qi5 2 uplink user-datagram dscp-marking 0x3f
 dscp-map qi5 2 downlink user-datagram dscp-marking 0x2a encsp-header dscp-marking 0x0a
 dscp-map qi5 3 uplink user-datagram dscp-marking 0x2e
 dscp-map qi5 3 downlink user-datagram dscp-marking 0x12 encsp-header copy-inner
 dscp-map qi5 4 uplink user-datagram dscp-marking 0x3f
 dscp-map qi5 4 downlink user-datagram dscp-marking 0x2a encsp-header dscp-marking 0x0a
 dscp-map qi5 5 uplink user-datagram dscp-marking 0x2e
 dscp-map qi5 5 downlink user-datagram dscp-marking 0x12 encsp-header copy-inner
 dscp-map qi5 6 uplink user-datagram dscp-marking 0x3f
 dscp-map qi5 6 downlink user-datagram dscp-marking 0x2a encsp-header dscp-marking 0x0a
 dscp-map qi5 7 uplink user-datagram dscp-marking 0x3f
 dscp-map qi5 7 downlink user-datagram dscp-marking 0x2a encsp-header dscp-marking 0x0a
 dscp-map qi5 8 uplink user-datagram dscp-marking 0x2e
 dscp-map qi5 8 downlink user-datagram dscp-marking 0x12 encsp-header copy-inner
 dscp-map qi5 9 uplink user-datagram dscp-marking 0x3f
 dscp-map qi5 9 downlink user-datagram dscp-marking 0x2a encsp-header dscp-marking 0x0a
 dscp-map qi5 65 uplink user-datagram dscp-marking 0x2e
 dscp-map qi5 65 downlink user-datagram dscp-marking 0x12 encsp-header copy-inner
 dscp-map qi5 66 uplink user-datagram dscp-marking 0x3f
 dscp-map qi5 66 downlink user-datagram dscp-marking 0x2a encsp-header dscp-marking 0x0a

 dscp-map qi5 69 uplink user-datagram dscp-marking 0x2e
 dscp-map qi5 69 downlink user-datagram dscp-marking 0x12 encsp-header copy-inner
 dscp-map qi5 70 uplink user-datagram dscp-marking 0x3f
 dscp-map qi5 70 downlink user-datagram dscp-marking 0x2a encsp-header dscp-marking 0x0a

 dscp-map qi5 80 uplink user-datagram dscp-marking 0x2e
 dscp-map qi5 80 downlink user-datagram dscp-marking 0x12 encsp-header copy-inner
 dscp-map qi5 82 uplink user-datagram dscp-marking 0x3f
 dscp-map qi5 82 downlink user-datagram dscp-marking 0x2a encsp-header dscp-marking 0x0a

 dscp-map qi5 83 uplink user-datagram dscp-marking 0x3f
 dscp-map qi5 83 downlink user-datagram dscp-marking 0x2a encsp-header dscp-marking 0x0a
exit
profile qos qos1
 qi5      128
 arp priority-level 8
 arp preempt-cap NOT_PREEMPT
 arp preempt-vuln NOT_PREEMPTABLE
 priority 9
 max data-burst 2048
exit
profile qos qos_F5972
 dscp-map qi5 1 arp-priority-level 5 uplink user-datagram dscp-marking 0x1e
 dscp-map qi5 1 arp-priority-level 5 downlink user-datagram dscp-marking 0x22 encsp-header
 copy-inner
```

```
exit
profile qos qos_nonStdQci
 ambr ul "250 Kbps"
 ambr dl "500 Kbps"
 qi5 128
 arp priority-level 12
 arp preempt-cap NOT_PREEMPT
 arp preempt-vuln PREEMPTABLE
 dscp-map qi5 1 arp-priority-level 5 uplink user-datagram dscp-marking 0x1e
 dscp-map qi5 1 arp-priority-level 5 downlink user-datagram dscp-marking 0x22 encsp-header
 copy-inner
 dscp-map qi5 2 arp-priority-level 6 uplink user-datagram dscp-marking 0x3e
 dscp-map qi5 2 arp-priority-level 6 downlink user-datagram dscp-marking 0x23 encsp-header
 copy-inner
 dscp-map qi5 3 arp-priority-level 12 uplink user-datagram dscp-marking 0x2f
 dscp-map qi5 3 arp-priority-level 12 downlink user-datagram dscp-marking 0x14 encsp-header
 copy-inner
 dscp-map qi5 6 downlink encsp-header copy-inner
 dscp-map qi5 7 downlink encsp-header dscp-marking 0x01
 dscp-map qi5 15 arp-priority-level 12 uplink user-datagram dscp-marking 0x2f
 dscp-map qi5 15 arp-priority-level 12 downlink user-datagram dscp-marking 0x14
encsp-header copy-inner
 dscp-map qi5 65 arp-priority-level 5 uplink user-datagram dscp-marking 0x1e
 dscp-map qi5 65 arp-priority-level 5 downlink user-datagram dscp-marking 0x22 encsp-header
 copy-inner
 dscp-map qi5 70 arp-priority-level 12 uplink user-datagram dscp-marking 0x2f
 dscp-map qi5 70 arp-priority-level 12 downlink user-datagram dscp-marking 0x14
encsp-header copy-inner
 dscp-map qi5 80 downlink encsp-header copy-inner
 dscp-map qi5 81 downlink encsp-header copy-inner
 dscp-map qi5 83 arp-priority-level 6 uplink user-datagram dscp-marking 0x3e
 dscp-map qi5 83 arp-priority-level 6 downlink user-datagram dscp-marking 0x23 encsp-header
 copy-inner
 dscp-map qi5 85 downlink encsp-header dscp-marking 0x01
 dscp-map qi5 128 arp-priority-level 5 uplink user-datagram dscp-marking 0x1e
 dscp-map qi5 128 arp-priority-level 5 downlink user-datagram dscp-marking 0x22
encsp-header copy-inner
 dscp-map qi5 230 arp-priority-level 6 uplink user-datagram dscp-marking 0x3e
 dscp-map qi5 230 arp-priority-level 6 downlink user-datagram dscp-marking 0x23
encsp-header copy-inner
 dscp-map qi5 254 downlink encsp-header dscp-marking 0x01
exit
profile ppd ppd1
 fqi 1,10-15,43,65
 dscp 0 ppi 3
 dscp 1 ppi 2
 dscp 43 ppi 3
exit
profile nf-client nf-type udm
 udm-profile UP1
  locality LOC1
   priority 30
   service name type nudm-sdm
    endpoint-profile EP1
     capacity   30
     uri-scheme http
     version
      uri-version v2
      exit
     exit
     endpoint-name EP1
      primary ip-address ipv4 209.165.200.248
      primary ip-address port 9001
     exit
```

```
    exit
   exit
   service name type nudm-uecm
    endpoint-profile EP1
     capacity   30
     uri-scheme http
     endpoint-name EP1
      primary ip-address ipv4 209.165.200.248
      primary ip-address port 9001
     exit
    exit
   exit
   service name type nudm-ee
    endpoint-profile EP1
     capacity       30
     api-uri-prefix PREFIX
     api-root       ROOT
     uri-scheme     http
     endpoint-name EP1
      priority 56
      primary ip-address ipv4 209.165.200.248
      primary ip-address port 9001
     exit
    exit
   exit
  exit
 exit
exit
profile nf-client nf-type pcf
 pcf-profile PP1
  locality LOC1
   priority 30
   service name type npcf-smpolicycontrol
    endpoint-profile EP1
     capacity   30
     uri-scheme http
     endpoint-name EP1
      priority 100
      primary ip-address ipv4 209.165.200.248
      primary ip-address port 9003
     exit
     endpoint-name realPCF
      priority 50
      primary ip-address ipv4 209.165.200.226
      primary ip-address port 9082
     exit
    exit
   exit
  exit
 exit
exit
profile nf-client nf-type amf
 amf-profile AP1
  locality LOC1
   priority 30
   service name type namf-comm
    endpoint-profile EP2
     capacity   30
     uri-scheme http
     endpoint-name EP1
      priority 56
      primary ip-address ipv4 209.165.200.248
      primary ip-address port 9002
     exit
```

```
     endpoint-name realAMF
      priority 100
      primary ip-address ipv4 209.165.202.138
      primary ip-address port 8090
     exit
    exit
   exit
  exit
 exit
exit
profile nf-client nf-type chf
 chf-profile CP1
  locality LOC1
   priority 30
   service name type nchf-convergedcharging
    endpoint-profile EP1
     capacity   30
     uri-scheme http
     version
      uri-version v2
      exit
     exit
     endpoint-name EP1
      priority 100
      primary ip-address ipv4 209.165.200.248
      primary ip-address port 9004
     exit
    exit
   exit
  exit
 exit
 chf-profile CP2
  locality LOC1
   priority 31
   service name type nchf-convergedcharging
    endpoint-profile EP1
     capacity   30
     uri-scheme http
     version
      uri-version v2
      exit
     exit
     endpoint-name EP1
      priority 56
      primary ip-address ipv4 209.165.200.248
      primary ip-address port 9005
     exit
    exit
   exit
  exit
 exit
exit
profile nf-client nf-type sepp
 sepp-profile hsepp
  locality LOC1
   priority 30
   service name type nsmf-pdusession
    endpoint-profile EP1
     capacity   30
     uri-scheme http
     endpoint-name EP1
      priority 56
      primary ip-address ipv4 209.165.200.250
      primary ip-address port 8090
```

```
     exit
     endpoint-name lfs-hsepp
      priority 10
      primary ip-address ipv4 209.165.200.248
      primary ip-address port 8888
      secondary ip-address ipv4 209.165.200.249
      secondary ip-address port 8889
     exit
    exit
   exit
  exit
 exit
exit
profile nf-pair nf-type UDM
 nrf-discovery-group DISC1
 locality client  LOC1
 locality preferred-server LOC1
 locality geo-server GEO
 cache invalidation true timeout 20000
exit
profile nf-pair nf-type AMF
 nrf-discovery-group DISC1
 locality client  LOC1
 locality preferred-server LOC1
 locality geo-server GEO
exit
profile nf-pair nf-type PCF
 nrf-discovery-group DISC1
 locality client  LOC1
 locality preferred-server LOC1
 locality geo-server GEO
exit
profile nf-pair nf-type SEPP
 nrf-discovery-group DISC1
 locality client  LOC1
 locality preferred-server LOC1
 locality geo-server GEO
exit
profile nf-pair nf-type UPF
 nrf-discovery-group DISC1
 locality client  LOC1
 locality preferred-server LOC1
 locality geo-server GEO
exit
profile nf-pair nf-type CHF
 nrf-discovery-group DISC1
 locality client  LOC1
 locality preferred-server LOC1
 locality geo-server GEO
 cache invalidation true timeout 20000
exit
profile nf-client-failure nf-type udm
 profile failure-handling FH1
  service name type nudm-sdm
   message type UdmSdmGetUESMSubscriptionData
    status-code httpv2 504
     retry  1
     action continue
    exit
   exit
   message type UdmSdmSubscribeToNotification
    status-code httpv2 504
     retry  1
     action continue
```

```
    exit
   exit
   message type UdmSubscriptionReq
    status-code httpv2 504
     retry  1
     action continue
    exit
   exit
  exit
  service name type nudm-uecm
   message type UdmUecmRegisterSMF
    status-code httpv2 504
     retry  1
     action continue
    exit
   exit
   message type UdmUecmUnregisterSMF
    status-code httpv2 504
     action continue
    exit
   exit
   message type UdmRegistrationReq
    status-code httpv2 504
     action continue
    exit
   exit
  exit
 exit
exit
profile nf-client-failure nf-type pcf
 profile failure-handling FH1
  service name type npcf-smpolicycontrol
   responsetimeout 4000
   message type PcfSmpolicycontrolCreate
    status-code httpv2 0,403
     action retry-and-ignore
    exit
    status-code httpv2 400,504
     action continue
    exit
    status-code httpv2 404
     action terminate
    exit
    status-code httpv2 500
     retry  2
     action retry-and-ignore
    exit
    status-code httpv2 503
     retry  2
     action retry-and-continue
    exit
   exit
   message type PcfSmpolicycontrolUpdate
    status-code httpv2 0,403
     action retry-and-ignore
    exit
    status-code httpv2 400,504
     action continue
    exit
    status-code httpv2 404
     action terminate
    exit
    status-code httpv2 500
     retry  2
```

```
      action retry-and-ignore
     exit
     status-code httpv2 503
      retry  2
      action retry-and-continue
     exit
    exit
    message type PcfSmpolicycontrolDelete
     status-code httpv2 0,403
      action retry-and-ignore
     exit
     status-code httpv2 400
      action continue
     exit
     status-code httpv2 404
      action terminate
     exit
     status-code httpv2 500
      retry  2
      action retry-and-ignore
     exit
     status-code httpv2 503
      retry  2
      action retry-and-continue
     exit
    exit
   exit
  exit
 exit
profile nf-client-failure nf-type chf
 profile failure-handling FH2
  service name type nchf-convergedcharging
   message type ChfConvergedchargingCreate
    status-code httpv2 0,500,504
     action continue
    exit
    status-code httpv2 400,404
     retry  3
     action retry-and-terminate
    exit
    status-code httpv2 403
     retry  3
     action retry-and-ignore
    exit
    status-code httpv2 503
     action terminate
    exit
   exit
   message type ChfConvergedchargingUpdate
    status-code httpv2 0,500,504
     action continue
    exit
    status-code httpv2 400,404
     retry  3
     action retry-and-terminate
    exit
    status-code httpv2 403
     retry  3
     action retry-and-ignore
    exit
    status-code httpv2 503
     action terminate
    exit
   exit
```

```
   message type ChfConvergedchargingDelete
    status-code httpv2 0,500,504
     action continue
    exit
    status-code httpv2 400,404
     retry  3
     action retry-and-terminate
    exit
    status-code httpv2 403
     retry  3
     action retry-and-ignore
    exit
    status-code httpv2 503
     action terminate
    exit
   exit
  exit
 exit
exit
profile nf-client-failure nf-type sepp
 profile failure-handling sepp
  service name type nsmf-pdusession
   responsetimeout 4000
   message type VsmfPduSessionCreate
    status-code httpv2 0
     retry  5
     action retry-and-terminate
    exit
    status-code httpv2 504
     retry  3
     action retry-and-terminate
    exit
   exit
   message type VsmfPduSessionUpdate
    status-code httpv2 0,401,404,503-504
     action retry-and-continue
    exit
    status-code httpv2 400
     action terminate
    exit
   exit
   message type VsmfPduSessionRelease
    status-code httpv2 0,504
     action retry-and-terminate
    exit
   exit
  exit
 exit
exit
profile smf smf1
 locality      LOC1
 instances 1 allowed-nssai [ slice1 slice2 ]
 load-profile  gtp-load1
 instances 1 fqdn   5gc.mnc456.mcc123.3gppnetwork.org
 instances 1 inter-plmn-fqdn 5gc.mnc210.mcc310.3gppnetwork.org
 instances 1 supported-features [ vsmf ]
 plmn-list mcc 123 mnc 456
 exit
 plmn-list mcc 310 mnc 310
 exit
 service name nsmf-pdu
  type               pdu-session
  schema             http
  service-id         1
```

```
  version            1.Rn.0.0
  http-endpoint base-url http://smf-service
  icmpv6-profile     icmpprf1
  compliance-profile comp1
  access-profile     access1
  subscriber-policy  polSub
 exit
exit
profile sgw sgw1
 locality          LOC1
 fqdn              cisco.com.apn.epc.mnc456.mcc123
 subscriber-policy polSub
 ddn failure-action-drop-timer 60
 ddn no-user-connect-retry-timer 60
 qci-qos-profile   sgw-non-standardqci
 wps-profile       wps1
 plmn-list mcc 123 mnc 456
 exit
 plmn-list mcc 310 mnc 260
 exit
exit
profile sgw-charging-threshold thre1
 cc profile value 1
  volume total 100000
  buckets  2
  duration 180
 exit
 cc profile value 2
  volume uplink 100000
  volume downlink 100000
  buckets  4
  duration 120
 exit
 cc profile value 4
  volume total 10000000
  buckets  4
  duration 300
 exit
 cc profile value 8
  volume total 100000
  buckets  2
  duration 3000
 exit
exit
profile overload gtp-overload1
 overload-exclude-profile self-protection gtp-overloadExclude1
 node-level
  tolerance minimum 15
  tolerance maximum 35
  reduction-metric minimum 20
  reduction-metric maximum 90
  advertise
   interval        300
   change-factor   15
   validity-period 60
  exit
  interface gtpc
   overloaded-action [ advertise ]
  exit
 exit
exit
profile overload-exclude gtp-overloadExclude1
 dnn-list       [ sos ]
 arp-list       [ 1 2 3 ]
```

```
 procedure-list [ session-delete ]
 message-priority s5
  upto 0
 exit
exit
profile load gtp-load1
 load-calc-frequency  30
 load-fetch-frequency 15
 advertise
  interval      30
  change-factor 5
 exit
 interface gtpc
  action advertise
 exit
exit
profile gtpp-profile pf1 gtpp
 local-storage
  file
   rotation
    volume        5
    cdr-count     1000
    time-interval 60
   exit
   name
    prefix               hSMF-cnsgw1
    format               .%Y-%m-%d%H-%M-%S.%4Q
    max-file-seq-num     9
    start-file-seq-num   1
    recover-file-seq-num true
   exit
   format custom1
  exit
 exit
 dictionary custom24
exit
profile gtpp-profile pf2 gtpp
 local-storage
  file
   rotation
    volume        5
    cdr-count     1000
    time-interval 60
   exit
   name
    prefix               hSMF-cnsgw1
    format               .%Y-%m-%d%H-%M-%S.%4Q
    max-file-seq-num     9
    start-file-seq-num   1
    recover-file-seq-num true
   exit
   format custom1
  exit
 exit
 dictionary custom24
exit
profile gtpp-profile pf4 gtpp
 local-storage
  file
   rotation
    volume        5
    cdr-count     1000
    time-interval 60
   exit
```

```
   name
    prefix               hSMF-cnsgw1
    format               .%Y-%m-%d%H-%M-%S.%4Q
    max-file-seq-num     9
    start-file-seq-num   1
    recover-file-seq-num true
   exit
   format custom1
  exit
 exit
 dictionary custom24
exit
profile dns-proxy
 timeout             6000
 round-robin-answers
 servers serv1
  ip       209.165.202.143
  port     53
  protocol tcp
 exit
 servers serv2
  ip       209.165.200.225
  port     53
  protocol tcp
 exit
exit
profile converged-core cc1
 max-upf-index 150
exit
nf-tls certificates cert1
 cert-data abc
 private_key k1
exit
active-charging service acs1
 bandwidth-policy BWP
  flow limit-for-bandwidth id 1 group-id 2
  flow limit-for-bandwidth id 2 group-id 3
  flow limit-for-bandwidth id 3 group-id 4
  group-id 2 direction uplink peak-data-rate 64000 peak-burst-size 8000 violate-action
discard
  group-id 2 direction downlink peak-data-rate 64000 peak-burst-size 8000 violate-action
 discard
  group-id 3 direction uplink peak-data-rate 128000 peak-burst-size 12000 violate-action
 discard
  group-id 3 direction downlink peak-data-rate 128000 peak-burst-size 12000 violate-action
 discard
  group-id 4 direction uplink peak-data-rate 3000000000 peak-burst-size 100 violate-action
 discard
  group-id 4 direction downlink peak-data-rate 3000000000 peak-burst-size 100
violate-action discard
 exit
 packet-filter pkt1
  ip local-port range 2 to 23
  ip protocol = 23
  ip remote-address = 209.165.201.0/27
  ip remote-port range 12 to 34
  ip tos-traffic-class = 23 mask = 23
  priority 23
 exit
 charging-action ca1
  billing-action egcdr
  content-id         51
  flow action redirect-url http://www.google.com
  flow limit-for-bandwidth id 1
```

```
  service-identifier 6000
  tft-notify-ue
  tos af11
  tft packet-filter pkt1
 exit
 charging-action caStaticOfflineOnline
  billing-action egcdr
  cca charging credit
  content-id         30
  flow limit-for-bandwidth direction uplink peak-data-rate 1000000000 peak-burst-size
100 violate-action discard committedDataRate 1000000000 committed-burst-size 100
exceed-action discard
  flow limit-for-bandwidth direction downlink peak-data-rate 1000000000 peak-burst-size
 100 violate-action discard committedDataRate 1000000000 committed-burst-size 100
exceed-action discard
  service-identifier 60
  tft-notify-ue
  tos af11
  tft packet-filter pkt1
 exit
 rulebase cisco
  billing-records egcdr
  edr transaction-complete http charging-edr http-edr
  dynamic-rule order first-if-tied
  egcdr threshold interval 1000
  action priority 1 ruledef ip-any-rule charging-action cisco
  route priority 1000 ruledef http-port-route analyzer http
 exit
 rulebase rba1
  action priority 1 dynamic-only ruledef rda1 charging-action ca1 description myrule1
  action priority 10 ruledef rda1 charging-action ca1
 exit
 urr-list urr_smf
  rating-group 10 urr-id 1
  rating-group 10 service-identifier 20 urr-id 2
  rating-group 10 service-identifier 21 urr-id 50
  rating-group 11 urr-id 3
  rating-group 11 service-identifier 21 urr-id 4
  rating-group 11 service-identifier 201 urr-id 11
  rating-group 12 urr-id 5
  rating-group 12 service-identifier 22 urr-id 6
  rating-group 13 urr-id 7
  rating-group 13 service-identifier 23 urr-id 8
  rating-group 30 urr-id 17
  rating-group 30 service-identifier 60 urr-id 18
  rating-group 30 service-identifier 61 urr-id 19
  rating-group 31 urr-id 20
  rating-group 31 service-identifier 61 urr-id 21
  rating-group 31 service-identifier 62 urr-id 22
  rating-group 32 urr-id 23
  rating-group 40 urr-id 24
  rating-group 51 service-identifier 6000 urr-id 32
  rating-group 100 urr-id 9
  rating-group 100 service-identifier 200 urr-id 10
  rating-group 100 service-identifier 201 urr-id 51
  rating-group 101 urr-id 11
  rating-group 101 service-identifier 201 urr-id 12
  rating-group 102 urr-id 13
  rating-group 102 service-identifier 202 urr-id 14
  rating-group 103 urr-id 15
  rating-group 103 service-identifier 203 urr-id 16
  rating-group 110 urr-id 25
  rating-group 199 urr-id 199
 exit
```

```
 ruledef adc_Youtube
  multi-line-or all-lines
 exit
 credit-control group onlineoffline
  diameter ignore-service-id true
 exit
 group-of-ruledefs adc_specific
  add-ruledef priority 1 ruledef adc_google
  add-ruledef priority 2 ruledef adc_facebook_https
  add-ruledef priority 3 ruledef adc_sni
 exit
gtpp group group1
 gtpp egcdr service-data-flow threshold interval 60
 gtpp egcdr service-data-flow threshold volume downlink 100000 uplink 100000 total 200000
exit
apn cisco
 gtpp group group1
 active-charging rulebase rba1
exit
apn intershat
 gtpp group group1
 active-charging rulebase rba1
exit
policy subscriber polSub
 precedence 1
  sst              22
  sdt              Abf123
  serving-plmn mcc 123
  serving-plmn mnc 456
  supi-start-range 100000000000001
  supi-stop-range  299999999999999
  gpsi-start-range 1000000000
  gpsi-stop-range  9999999999
  operator-policy  opPol1
 exit
 precedence 511
  operator-policy defOprPol1
 exit
exit
policy upf-selection up-policy1
 precedence 1
   [ dnn slice ]
 exit
 precedence 2
   [ dnn location ]
 exit
 precedence 3
   [ dnn pdn-type-session ]
 exit
 precedence 4
   [ dnn ]
 exit
exit
policy operator defOprPol1
 policy dnn         defPolDnn
 policy network-capability nc1
exit
policy operator opPol1
 policy dnn         polDnn
 policy network-capability nc1
exit
policy operator opPol2
 policy dnn         polDnn
 policy network-capability nc1
```

```
exit
policy dnn defPolDnn
 profile default-profile
 dnn cisco profile cisco
 dnn dnn2 profile profile2
 dnn intershat profile intershat
 dnn sos profile sos
 dnn starent profile abc.com
exit
policy dnn dnnPol1
 profile default
 dnn starent profile abc.com
exit
policy dnn polDnn
 profile default-profile
 dnn cisco profile cisco
 dnn dnn2 profile profile2
 dnn intershat profile intershat
 exit
policy network-capability nc1
 nw-support-local-address-tft true
exit
nssai name slice1
 sst 1
 dnn [ cisco intershat sos starent ]
exit
nssai name slice2
 sst 2
 sdt abf123
 dnn [ cisco intershat sos starent ]
exit
system-diagnostics session-consistency action monitor
ipam
 instance 1
  source local
  address-pool v4pool1
   vrf-name ISP
   tags
    dnn intershat
   exit
   ipv4
    split-size
     per-cache 65536
     per-dp    65536
    exit
    address-range 209.165.201.1 209.165.201.30
   exit
  exit
 exit
exit
group nf-mgmt NFMGMT1
 nrf-mgmt-group MGMT
 locality       LOC1
exit
group nrf discovery DISC1
 nrf-type PLMN
 service type nrf nnrf-disc
  endpoint-profile
   name       EP1
   uri-scheme http
   version
    uri-version v1
     full-version 209.165.200.224/27
    exit
```

```
   exit
   endpoint-name sauNRF
    priority 80
    capacity 56
    primary ip-address ipv4 209.165.201.4
    primary ip-address port 8095
   exit
  exit
 exit
exit
cdl system-id          2
cdl enable-geo-replication true
cdl zookeeper replica 1
cdl remote-site 1
 db-endpoint host 209.165.202.154
 db-endpoint port 8882
 kafka-server 209.165.200.226 10092
 exit
exit
cdl label-config session
 endpoint key smi.cisco.com/node-type
 endpoint value smf-cdl
 slot map 1
  key   smi.cisco.com/node-type
  value smf-cdl
 exit
 slot map 2
  key   smi.cisco.com/node-type
  value smf-cdl-1
 exit
 index map 1
  key   smi.cisco.com/node-type
  value smf-cdl-1
 exit
exit
cdl logging default-log-level error
cdl logging logger datastore.ep.session
 level debug
exit
cdl logging logger datastore.index.session
 level debug
exit
cdl logging logger datastore.slot.session
 level debug
exit
cdl datastore session
 label-config    session
 geo-remote-site [ 1 ]
 slice-names     [ 1 2 ]
 endpoint replica 1
 endpoint external-ip 209.165.202.158
 endpoint external-port 8882
 index replica 1
 index map    1
 index write-factor 1
 slot replica 1
 slot map     2
 slot write-factor 1
exit
cdl kafka replica 1
cdl kafka ssl-settings enable-ssl false
cdl kafka label-config key smi.cisco.com/pod-type
cdl kafka label-config value cdl-kafka-1
cdl kafka external-ip 209.165.202.158 10092
```

```
exit
etcd replicas 1
edr reporting disable
edr all subscribers
edr file transaction
 reporting enable
exit
edr file transaction-collision
 reporting enable
exit
instance instance-id 1
 endpoint li
  replicas 1
  nodes    1
  vip-ip 209.165.200.226
 exit
 endpoint nodemgr
  replicas 1
  nodes    2
 exit
 endpoint gtp
  replicas                1
  nodes                   2
  internal-vip            209.165.200.226
  mbr-optimization
   enable            true
   teid-cache-expiry 120000
   mbr-cache-expiry  50
  exit
  enable-gtpc-bypass      true
  retransmission timeout 5 max-retry 4
  enable-cpu-optimization true
  enable-go-encdec        true
  sla response 5000
  sla procedure 5000
  vip-ip 209.165.200.226
  interface s5
   sla procedure 5000
   echo interval          60
   echo retransmission-timeout 5
   echo max-retransmissions 4
   retransmission timeout 5 max-retry 4
   enable-go-encdec true
  exit
  interface s5e
   sla response 5000
   sla procedure 5000
   echo interval          60
   echo retransmission-timeout 5
   echo max-retransmissions 4
   path-failure detection-policy pol_egtp_path_failure
   retransmission timeout 5 max-retry 4
   enable-go-encdec true
  exit
  interface s2b
   echo interval          60
   echo retransmission-timeout 5
   echo max-retransmissions 4
  exit
  interface gtpu
  exit
  interface s11
   sla response 5500
   echo interval          60
```

```
  echo retransmission-timeout 5
  echo max-retransmissions 4
  path-failure detection-policy pol_egtp_path_failure
  retransmission timeout 5 max-retry 4
  enable-go-encdec true
  dscp             0x20
  vip-ip 209.165.200.226
 exit
exit
endpoint pfcp
 replicas               1
 nodes                  2
 internal-vip           209.165.200.226
 retransmission timeout 3 max-retry 2
 enable-cpu-optimization true
 vip-ip 209.165.200.226
 interface sxa
  sla response 4000
  heartbeat
   interval               60
   retransmission-timeout 9
   max-retransmissions    10
  exit
  retransmission timeout 5 max-retry 4
  vip-ip 209.165.200.226
  dispatcher
   count         25
   capacity      250
   outbound      true
   cache         true
   threshold     500
   expiry        60000
   nonresponsive 30500
  exit
 exit
 interface n4
  heartbeat
   interval               0
   retransmission-timeout 3
   max-retransmissions    5
  exit
  retransmission timeout 3 max-retry 2
  vip-ip 209.165.200.226
  dispatcher
   count         5
   capacity      1000
   outbound      true
   threshold     5000
   expiry        60000
   nonresponsive 30500
  exit
 exit
exit
endpoint service
 replicas 1
 nodes    1
exit
endpoint protocol
 replicas     1
 nodes        2
 internal-vip 209.165.200.226
 vip-ip 209.165.200.226
exit
endpoint radius
```

```
  replicas 1
  nodes    1
  vip-ip 209.165.200.226
  interface coa-nas
   vip-ip 209.165.200.226 vip-port 3799
  exit
 exit
 endpoint sgw-service
  replicas 1
  nodes    1
 exit
 endpoint dns-proxy
  replicas 1
 exit
 endpoint sbi
  replicas 1
  nodes    1
  vip-ip 209.165.200.226
  interface nrf
   vip-ip 209.165.200.226
  exit
 exit
exit
logging transaction message enable
logging transaction duplicate enable
logging level application trace
logging level transaction trace
logging level tracing debug
logging name infra.application.core level application warn
logging name infra.application.core level tracing warn
logging name infra.config.core level application trace
logging name infra.config.core level transaction trace
logging name infra.config.core level tracing off
logging name infra.dispatcher.core level application warn
logging name infra.dispatcher.core level transaction warn
logging name infra.dispatcher.core level tracing warn
logging name infra.heap_dump.core level application warn
logging name infra.ipcstream.core level application error
logging name infra.ipcstream.core level transaction warn
logging name infra.ipcstream.core level tracing warn
logging name infra.memory_cache.core level application error
logging name infra.memory_cache.core level transaction error
logging name infra.message_log.core level transaction trace
logging name infra.resource_monitor.core level application warn
logging name infra.resource_monitor.core level transaction warn
logging name infra.rest_server.core level application error
logging name infra.rest_server.core level tracing off
logging name infra.topology.core level application off
logging name infra.topology.core level transaction off
logging name infra.topology.core level tracing off
deployment
 app-name               cnsgw-smf-1
 cluster-name           Local
 dc-name                DC
 model                  small
 logical-nf-instance-id 1
exit
k8 label protocol-layer key smi.cisco.com/vm-type value smf-proto-1
exit
k8 label service-layer key smi.cisco.com/vm-type value smf-svc-1
exit
k8 label cdl-layer key smi.cisco.com/node-type value smf-cdl-1
exit
k8 label oam-layer key smi.cisco.com/node-type value oam
```

```
exit
instances instance 1
 system-id  smf
 cluster-id smf
 slice-name 1
exit
local-instance instance 1
system mode running
helm default-repository roaming-ph2
helm repository cnsgw-1
 access-token
dev-deployer.gen:AKCp5ekcXA7TknM9DbLASNBw4jwVEsx9Z9WpQwEvCvCQ2mJhLymcz6BfbH38YJiWC6fn1cKmw

 url
https://engci-maven-master.cisco.com/artifactory/smi-fuse-internal-snapshot/mobile-cnat-cn/cn-products/master/
exit
helm repository roaming-cx
 access-token
dev-deployer.gen:AKCp5ekcXA7TknM9DbLASNBw4jwVEsx9Z9WpQwEvCvCQ2mJhLymcz6BfbH38YJiWC6fn1cKmw

 url
https://engci-maven-master.cisco.com/artifactory/mobile-cnat-charts-release/relengbuilds/2021.03.m0.d4.0/ccg/2021.03.m0.d4.0.i77/ccg.2021.03.m0.d4.0.i77/
exit
helm repository roaming-ph2
 access-token
dev-deployer.gen:AKCp5ekcXA7TknM9DbLASNBw4jwVEsx9Z9WpQwEvCvCQ2mJhLymcz6BfbH38YJiWC6fn1cKmw

 url
https://engci-maven-master.cisco.com/artifactory/smi-fuse-internal-snapshot/mobile-cnat-cn/cn-products/dev-smf-amigos/
exit
k8s name          cnsgw-smf-1
k8s namespace     cnsgw-1
k8s nf-name       smf
k8s registry      dockerhub.cisco.com/smi-fuse-docker-internal
k8s single-node   true
k8s use-volume-claims false
k8s ingress-host-name 209.165.200.238.nip.io
aaa authentication users user admin
 uid        117
 gid        117
 password   $1$bQRuPxWc$ESF/KLDQBkmdQNtrReTJN1
 ssh_keydir /tmp/admin/.ssh
 homedir    /tmp/admin
exit
aaa authentication users user liadmin
 uid        201
 gid        2011
 password   $1$LugH/seF$hi4y0QnpOZoEiJDqGLd0L.
 ssh_keydir /tmp/liadmin/.ssh
 homedir    /tmp/liadmin
exit
aaa authentication users user liadmin2
 uid        202
 gid        2021
 password   $1$HBRlXp0W$pmaMFhDV9QIayXTxEZtxc0
 ssh_keydir /tmp/liadmin2/.ssh
 homedir    /tmp/liadmin2
exit
aaa authentication users user liadmin3
 uid        203
 gid        2031
 password   $1$kE6v4ZBD$sv97OlhMCmTtjm7Q35Esq1
 ssh_keydir /tmp/liadmin3/.ssh
 homedir    /tmp/liadmin3
```

```
exit
aaa ios level 0
 prompt "\h> "
exit
aaa ios level 15
 prompt "\h# "
exit
aaa ios privilege exec
 level 0
  command action
  exit
  command autowizard
  exit
  command enable
  exit
  command exit
  exit
  command help
  exit
  command startup
  exit
 exit
 level 15
  command configure
  exit
 exit
exit
nacm write-default deny
nacm groups group LI
 user-name [ liadmin ]
exit
nacm groups group LI2
 user-name [ liadmin2 ]
exit
nacm groups group LI3
 user-name [ liadmin3 ]
exit
nacm groups group admin
 user-name [ admin ]
exit
nacm rule-list admin
 group [ admin ]
 rule li-deny-tap
  module-name       lawful-intercept
  path              /lawful-intercept
  access-operations *
  action            deny
 exit
 rule li-deny-clear
  module-name       tailf-mobile-smf
  path              /clear/lawful-intercept
  access-operations *
  action            deny
 exit
 rule any-access
  action permit
 exit
exit
nacm rule-list confd-api-manager
 group [ confd-api-manager ]
 rule any-access
  action permit
 exit
exit
```

```
nacm rule-list ops-center-security
 group [ * ]
 rule change-self-password
  module-name       ops-center-security
  path              /smiuser/change-self-password
  access-operations exec
  action            permit
 exit
 rule smiuser
  module-name       ops-center-security
  path              /smiuser
  access-operations exec
  action            deny
 exit
exit
nacm rule-list lawful-intercept
 group [ LI LI2 LI3 ]
 rule li-accept-tap
  module-name       lawful-intercept
  path              /lawful-intercept
  access-operations *
  action            permit
 exit
 rule li-accept-clear
  module-name       tailf-mobile-smf
  path              /clear/lawful-intercept
  access-operations *
  action            permit
 exit
exit
```

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。