

概要

Evolved Packet Core（EPC）ネットワークは、ユーザープレーンとコントロールプレーンがP-GW、S-GW、およびTDF製品の個別のノードである、コントロールユーザープレーン分離（CUPS）ベースのアーキテクチャに向けて進化しています。ユーザープレーンとコントロールプレーンが統合することで、EPCネットワーク内の他の要素に対してもノードの機能が提供されます。ただし、ネットワークの観点から見ると、ユーザープレーンとコントロールプレーンを分離しておくことには多くの利点があります。たとえば、コントロールプレーンとユーザープレーンでそれぞれ異なる拡張をサポートできること、ユーザープレーンでセッションあたりにより多くのキャパシティをサポートできることなどが挙げられます。

この章では、P-GW、S-GW、およびSAEGW製品のコントロールプレーン実装に関連する詳細、コールフロー、および設定について概要を説明します。

- 製品の説明 （1 ページ）
- サポートされる機能 （2 ページ）
- 機能の仕組み （23 ページ）

製品の説明

既存の非CUPS SAEGWサービスは、Sxa、Sxb、およびSxab（SxaとSxaの組み合わせ）インターフェイスにコントロールプレーン機能を提供するために再利用されます。違いは次のとおりです。

1. P-GWとS-GWのそれぞれのEGTPCサービスは、GTP-Uサービスに関連付けられません。
2. ユーザープレーンへのインターフェイスであるSxサービスは、SAEGWサービスに関連付けられます。
3. GTP-Uサービスは、GTP-Uパケットを受信するためのSAEGWサービスに関連付けられます（ルータアドバタイズメント/ルータ要請またはコントロールプレーンで必要なデータバッファリング用）。

Sx インターフェイス

CUPS アーキテクチャの一部として、Sx インターフェイスはコントロールプレーンとユーザープレーン間の通信に使用されます。

コントロールプレーンでは、SAE-GW サービスはユーザープレーンとの通信のために Sx サービスに関連付けられます。また、単一の Sx サービスは、Sxa、Sxb、Sxab などのすべてのインターフェイスを処理できます。これはそれぞれ Pure-S、Pure-P、Collapsed PDN に必要です。

ライセンス情報

Cisco UPC CUPS は、Cisco Smart Licensing をサポートします。これは、クラウドベースのライセンスモデルでシスコのソフトウェアアセットの購入、デプロイメント、管理を簡単にします。詳細については、Smart Licensing コレクションページを参照してください。

サポートされる機能

3GPP ULI 拡張レポートのサポート

この機能拡張は、3GPP 標準に従って P-GW および GGSN の ULI 関連のギャップをカバーします。

S4SGSN は、S-GW を介して P-GW に ULI を報告します。P-GW は、以前に受信した ULI を使用して ULI の変更を決定します。P-GW が変更を検出し、変更要求が PCRF からイベントトリガーとして送信された場合、P-GW は PCRF に ULI を報告します。

SGSN は GGSN に ULI を報告します。GGSN は、以前に受信した ULI を使用して ULI の変更を決定します。GGSN が変更を検出し、変更要求が PCRF からイベントトリガーとして送信された場合、GGSN は PCRF に ULI を報告します。この機能は、GGSN で ULI フィールドの一部として受信した RAI の変更の検出もサポートします。

3GPP ULI レポートのサポート強化の詳細については、StarOS P-GW アドミニストレーションガイド [英語] の「3GPP ULI Reporting Support Enhanced」の項を参照してください。

AAA サーバーグループ

AAA サーバーグループ機能は、コンテキストまたはシステム内で Diameter/RADIUS サーバーグループを作成および管理するために使用されます。AAA サーバーグループにより、AAA 機能のサブスクライバ/APN/レルム単位で、サーバーグループ（リスト）を管理しやすくなります。

APN 設定のサポート



（注） リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	Release
初版	21.24 より前

CLI コマンド **radius-group**、**cc-home behaviour 0x10 profile 2**、**mediation-device** が APN 設定をサポートすることが、CUPS アーキテクチャで認定および検証済みです。

radius-group

この機能検証に基づき、CUPS アーキテクチャは、RADIUS 認証およびアカウンティングサーバーが設定された各グループで 800 の RADIUS サーバーグループをサポートします。

cc-home { behavior *bits* | profile *index* }

SGSN からの課金特性（CC）が受け付けられない場合に GGSN が使用する Home サブスクライバの課金特性を設定します。CLI で設定された値は、CUPS SAEGW サービスによって優先され、GTPP CDR レコードに適切に入力されます。

注：

- **behavior** *bits*：Home サブスクライバの課金特性の動作ビットを指定します。ビットは、001H ～ FFFH（2 進数では 0001 ～ 1111 1111 1111）までの任意の一意のビットに設定できます。最下位ビットは B1 に相当し、最上位ビットは B12 に相当します。
- **profile** *index*：Home サブスクライバの課金特性のプロファイル指数を指定します。指数は、0 ～ 15 までの任意の整数値に設定できます。デフォルト：8
- 詳細については、『*CLI*（コマンド ライン インターフェイス）リファレンス *A-B*』[英語] の「*APN Configuration Mode Commands* 」の章にある **cc-home** コマンドを参照してください。

mediation-device [context-name *context_name*] [delay-GTP-response] [no-early-PDUs] [no interims] +

このコマンドおよび関連するすべてのサブセクション CLI が CUPS でサポートされます。この CLI を使用すると、CUPS SAEGW サービスで**仲介デバイス**と、特定の APN に使用できるすべての関連設定を使用できます。

注：

- **context-name** *context_name*：この APN の仲介 VPN コンテキストを、大文字と小文字を区別する 1 ～ 79 文字の英数字で設定します。指定しない場合、仲介コンテキストはサブス

クライバの接続先コンテキストと同じになります。デフォルト：サブスクライバの接続先コンテキスト。

- **delay-GTP-response**：有効にすると、仲介デバイスからアカウンティング開始応答を受信するまで CPC 応答を遅延させます。デフォルトで、ディセーブルになっています。
- **no-early-pdus**：仲介デバイスから GGSN アカウンティング開始要求に対する応答を受信するまで、システムが MS からの PDU を遅延させるように設定します。PDU はキューに追加され、破棄されません。デフォルトで、ディセーブルになっています。
- **no-interim**：仲介サーバーへの中間の送信を無効にします。デフォルトで、ディセーブルになっています。
- 詳細については、『*CLI*（コマンド ライン インターフェイス）リファレンス *A-B*』[英語]の「*APN Configuration Mode Commands* 」の章にある **mediation-device** コマンドを参照してください。

egtpinmgr の非同期コア転送のサポート

egtpinmgr の再起動中の停止時間を最適化するため、egtpinmgr の非同期コア転送のサポートが CUPS に追加されました。

これまでは、egtpinmgr が再起動すると、まずコアダンプファイルの作成および転送を完了させ、それからリカバリプロセスを開始していました。しかし、コアファイルの転送にはかなりの時間がかかります。egtpinmgr の再起動時の停止時間は、egtpinmgr のリカバリ時間とコアファイル転送時間とを合算した時間でした。

非同期コア転送が CUPS でサポートされるようになったことで、リカバリプロセスに egtpinmgr が含まれるようになります。今後は、egtpinmgr プロセスがクラッシュすると、カーネルによるコアダンプファイルの転送とリソースの解放を待たずにリカバリが開始されます。その結果、egtpinmgr の再起動時の停止時間は、egtpinmgr のリカバリ時間のみに等しくなります。

この機能拡張により、egtpinmgr の再起動時の停止時間が短縮されます。停止時間は、egtpinmgr の回復に必要な時間のみとなり、コアファイルの作成と転送にかかる時間による影響を受けなくなります。

（注） egtpinmgr の非同期コア転送サポートは、非 CUPS アーキテクチャでサポートされている既存の機能です。このリリースでは、この機能が CUPS アーキテクチャで認定されました。

ビットレートマッピングのサポート

P-GW は、PCRF から受信したビット レート値を bps から kbps に変換します。この変換により、小数値が最も近い整数（floor）値に切り捨てられ、情報が失われる可能性があります。3GPP では、bps から kbps に変換すると小数値になる場合は、最も近い整数値（ceil）値に切り上げてアクセス側に送信することが推奨されています。

（注） bps から kbps への切り捨て（floor）値が PFCP インターフェイスで送信されるように設計が変更されました。

標準準拠

ビットレートマッピング機能は、3GPP TS 29.274 リリース 12 に準拠しています。

ビットレートマッピング機能の設定

P-GW の APN-AMBR、GBR、および MBR で、bps から kbps ビットレートの切り上げ（ceil）値を設定するには、次の手順を実行します。

```
configure
  context context_name
    pgw-service service_name
      [ no ] egtp bitrates-rounded-down-kbps
      end
```

P-GW の APN-AMBR、GBR、および MBR で、bps から kbps ビットレートの切り捨て（floor）値を設定するには、次の手順を実行します。

```
configure
  context context_name
    pgw-service service_name
      egtp bitrates-rounded-down-kbps
      end
```

CUPS の新しい動作

デフォルトでは、APN-AMBR、MBR、および GBR のビットレートの切り上げ値（kbps 単位）が Sx および GTP インターフェイスで送信されます。切り捨て動作を有効にするには、CLI を設定する必要があります。

コールログサマリー

コールログサマリー（CLS）は、セッション作成または削除、ベアラー作成、更新、または削除などのサブスクライバ アクティビティが外部サーバーに報告されるメカニズムです。

CUPS CP ノードで CLS が有効になっている場合、イベントレコードが生成されます。これらのレコードは、CSV ファイル形式でシャーシのハードディスクに保存できます。ファイルは、*.gz* 圧縮形式でも保存することが可能です。これらのファイルは、ネットワークの維持とトラブルシューティングを目的としたネットワークオペレータによるさらなる分析のために、後で外部サーバーに SFTP で送信されます。

CUPS モードでは、この機能はコントロールプレーンノードで有効にできます。このノードでは、SAEGW コールタイプに応じて SGW、PGW レコードが生成されます。

（注） コールログサマリー（CLS）の詳細については、StarOS の『SAEGW アドミニストレーションガイド』を参照してください。

HDD に対する課金データレコード

課金データレコード（CDR）は、課金対象イベントに関する情報のフォーマットされたコレクションです。生成された GTPP アカウンティング CDR は、保管のために外部ノードに送信されます。CDR は、外部ノードでサポートされている形式でファイルに書き込まれ、ハードディスク（HDD）に保存されます。FTP または SFTP プロトコルを使用して、CDR ファイルを HDD にプッシュしたり、HDD からプルしたりできます。

（注） バックアップなどの展開の使用例では、*/hd-raid/records/* の下に StarOS によって作成されたシステムディレクトリを使用しないことを強く推奨します。そのようなディレクトリを使用すると、製品の正常な機能に影響を与える可能性があります。

CDR は、非 CUPS アーキテクチャでサポートされていて、CUPS アーキテクチャで認定されている既存の機能です。詳細については、GTPP インターフェイス管理およびリファレンスガイド [英語] の「HDD Storage」の章を参照してください。

GTP-C パス障害の機能拡張とデバッグツールの改善

CUPS アーキテクチャでは、GTP-C パス障害機能を最適化し、GTP-C パス障害の問題に対するシステムのデバッグ機能を向上させるための機能拡張が追加されました。これらの機能拡張は、オペレータとエンジニアがシステムのさまざまな側面をデバッグし、ネットワーク内の GTP-C パス障害の根本原因を特定するのに役立ちます。また、S5、S8、S2b、および S2a インターフェイスを介したパス障害検出に影響を及ぼします。

これらの機能強化は、次の機能の一部です。

- 誤ったメッセージや偽のメッセージが原因で低い値のリスタートカウンタを受信した場合、パス障害を検出しないようにノードを設定でき、コールの損失を防げます。エコー要求/応答メッセージや制御メッセージ要求/応答メッセージによるパス障害を無効にするオプションも使用できるため、パス障害の誤検出が発生した場合にコールの損失を防げます。
- ネットワーク内の問題の根本原因をより迅速に診断できるように、GTP-C パス障害の統計情報の精度が向上しました。
- ピアごとに最後の 5 つのパス障害に関するパス障害履歴を、ネットワーク内のパス障害のデバッグに使用できます。

- シームレスなパス障害処理が実装されているため、冗長性イベント中のコールの損失が回避されます。



（注） GTP-Cパス障害の機能拡張と改善されたデバッグツールは、非CUPSアーキテクチャでサポートされている既存の機能です。このリリースでは、この機能はCUPSアーキテクチャで認定されています。詳細については、P-GW アドミニストレーション ガイド [英語] の「GTP-C Path Failure Enhancements and Enhanced Debugging Tools」の項を参照してください。

GTPP Suppress-CDR No Zero Volume

この機能により、バイト数カウントがゼロの CDR を抑制できるため、OCG ノードが CDR のフラッディングで過負荷になることはありません。CDR は次のように分類できます。

- Final-cdrs：これらの CDR は、コンテキストの最後に生成されます。
- Internal-trigger-cdrs：これらの CDR は、音量制限、時間制限、料金変更、または CLI コマンドを使用してユーザーが生成したインテリムなどの内部トリガーによって生成されます。
- External-trigger-cdrs：これらの CDR は、QoS 変更、RAT 変更などの外部トリガーによって生成されます。final-cdrs や internal-trigger-cdrs と見なされないすべてのトリガーは、external-trigger-cdrs と見なされます。

カスタマーは抑制する CDR を選択できます。

次に示す CLI コマンドは、CUPS でサポートされているさまざまな CDR トリガーで CDR を抑制するのに役立ちます。

- **[default | no] gtpp suppress-cdrs zero-volume { external-trigger-cdr | final-cdr | internal-trigger-cdr }**

合法的傍受

シスコによる合法的傍受機能は、CUPS でサポートされています。合法的傍受は、ライセンス対応の標準ベースの機能であり、法執行機関が疑わしい個人の潜在的な違法行為を監視するのを支援するメカニズムを、電気通信サービスプロバイダーに提供します。

合法的傍受機能の詳細とマニュアルの入手方法については、シスコのアカウント担当者にお問い合わせください。

ロケーションベースの DNS および PCSCF IP アドレスの選択

ロケーションベースの DNS および P-CSCF の選択により、ロケーション情報に従って DNS サーバーアドレスと P-CSCF IP アドレスを管理するオプションが使用可能となります。

P-GW は、トラッキングエリア識別子（TAI）によって DNS サーバーアドレスと P-CSCF IP アドレス情報を収集します。これは、TAC ベースの仮想 APN（VAPN）の選択によって実現されます。

セッション作成で UE が PCO 要求を送信すると、P-GW は受信したロケーション情報をもとに仮想 APN（VAPN）を選択します。PCO IE を含む選択済みの VAPN（DNS サーバーアドレスと P-CSCF IP アドレスが設定されている）がセッション作成応答で送信されます。

以下に、ロケーションベースの DNS および PCSCF IP アドレスの選択を有効にするための CLI コマンドを示します。

コマンド	説明
Tracking-area-code-range from <*start value*> **to** <*end value*>	トラッキングエリアコードの範囲（0 ～ 65536）を指定します。終了値は常に開始値より大きくなります。
P-cscf priority <*priority*> **ip/ipv6** <*IPv4/Ipv6 address*>	APN の P-CSCF アドレスの優先順位を指定します。Address_priority は 1 ～ 3 までの整数です。最も優先順位が高いのが「1」です。IPv4_address は、IPv4 ドット付き 10 進表記です。IPv6_address は、IPv6 コロン区切り 16 進表記です。
Show apn name <*APN Name*>	APN の PCSCF IP アドレスを表示します。
dns primary <*IPv4 address*> **Dns secondary** <*IPv4 address*> **ipv6 dns primary** <*IPv6 address*> **ipv6 dns secondary** <*IPv6 address*>	Primary：APN のプライマリ DNS サーバーを設定します。 Secondary：APN のセカンダリ DNS サーバーを設定します。設定できるセカンダリ DNS サーバーは 1 つのみです。 Address：IPv4 ドット付き 10 進表記で表記された DNS サーバーの IP アドレスです。デフォルト：primary = 0.0.0.0、secondary = 0.0.0.0 dns_address：削除する DNS サーバーの IP アドレスです。IPv4 ドット付き 10 進表記で表記します。
Show apn name <*APN Name*>	APN の DNS IP アドレスを表示します。

MPRA サポート

P-GW は、PCRF を使用する Gx インターフェイスを介した Feature-List-ID 2 の Multiple-Presence Reporting Area 機能のネゴシエーションをサポートします。CNO-ULI 機能は、P-GW や PCRF が Multiple-PRA をサポートしておらず、P-GW と PCRF の両方が CNO-ULI をサポートしている場合にのみ機能します。

IP-CAN セッションのライフタイム中に Multiple-PRA 機能をサポートするために、P-GW は、Presence-Reporting-Area-Information AVP を含む PRA-Install AVP の PCRF からのレポートエリア要求内にある UE プレゼンスの変更を処理します。各 AVP には、Presence-Reporting-Area-Identifier AVP 内の Presence Reporting Area 識別子が含まれています。

Presence Reporting Area（PRA）と Multiple-PRA の詳細については、StarOS P-GW のアドミニストレーション ガイド [英語] の「Presence Reporting Area」の章を参照してください。

5G エリアから 4G エリアへの移行時にデフォルトルールベースにフォールバックする

機能名	リリース情報	説明
PRA を使用して 5G から 4G への移行時にデフォルトルールベースにフォールバックする	2025.02.0	この機能により、通話が 5G から 4G エリアに移動した際に、デフォルトルールベースにフォールバックするセッションが有効になります。 これにより、通話が 5G から 4G に移動した際に、PCRF がインストールされたルールベースのみを削除した場合でも、APN で構成されたデフォルトルールで通話を継続できます。 **導入されたコマンド**： **active-charging fallback-to-apn-rulebase**：この CLI は、APN で構成され、セッションをデフォルトのルールベースにフォールバックさせます。 **デフォルト設定**：無効-有効にするには構成が必要です。

通話が最初に 4G に接続されると、APN で構成されたデフォルトルールが、4G ルールベースになります。セッションが、4G から 5G に移動すると、PCRF は、$G ルールベースを上書きし、5G ルールベースをインストールします。

ただし、セッションが 5G から 4G に再度移動すると、デフォルトの動作として、PCRF は、5G ルールベースを削除し、4G ルールベースをインストールしません。その結果、セッションが切断されます。

この問題を解決するために、この機能により、ネットワークオペレータは APN で構成されたデフォルトのルールベースにフォールバックようにセッションを構成できます。これにより、セッションが 5G から4Gに戻った後に PCRF がインストールされたルールベースのみを削除した場合でも、セッションを続行できます。

（注） この機能は、呼び出しから新しいルールベースをインストールすることなくルールベースが削除される、他のすべてのハンドオフシナリオに適用されます。

5G エリアから 4G エリアへの移行時にデフォルトルールベースへのフォールバックを有効にする

次の手順を実行して、5G から 4G への移行時にデフォルトルールベースへのフォールバックを有効にします。

手順

ステップ 1 グローバル コンフィギュレーション モードに入った後に、コマンド **context** *context_name* を使用して、コンテキストプロファイルのインスタンスを作成します。

例：

```
[local]qvpc-si# configure
[local]qvpc-si(config)# context ingress
[ingress]qvpc-si(config-ctx)#
```

ステップ 2 コマンド **apn** *apn_name* を使用して、APN 構成モードに入ります。

例：

```
[ingress]qvpc-si(config-ctx)# apn intershat
[ingress]qvpc-si(config-apn)#
```

ステップ 3 コマンド **active-charging fallback-to-apn-rulebase** を使用して、APN で構成されたデフォルトのルールベースへのフォールバックを有効にします。

例：

```
[ingress]qvpc-si(config-apn)# [no] active-charging fallback-to-apn-rulebase
```

（注）
- デフォルトでは、この CLI は無効になっています。
- このCLI構成は、新しい着信通話のみに適用されます。既存の通話は、進行中の通話には影響しません。

[no] を使用して CLI が構成され、PCRF がルールベースを削除したら、セッションは、APN で構成されたデフォルトのルールベースにはフォールバックされません。これにより、通話が終了します。

ステップ 4 コマンド **show apn name intershat** を使用して、APN でフォールバック機能が有効になっているかを確認します。

例：

```
[local]qvpc-si# show apn name intershat
access point name (APN):  intershat
authentication context:  ingress
pdp type:  ipv4 and ipv6
emergency: no
delay tolerant pdn: no
PCO Options:
    custom1      Mode: disabled
    custom2      Mode: disabled        PCO Value: n/a
    custom3      Mode: disabled        PCO Value: n/a
    custom4      Mode: disabled        PCO Value: n/a
    custom5      Mode: disabled        PCO Value: n/a
    custom6      Mode: disabled        PCO Value: n/a
    custom7      Mode: disabled        PCO Value: n/a
    custom8      Mode: disabled        PCO Value: n/a
```

```
    custom9      Mode: disabled        PCO Value: n/a
    custom10     Mode: disabled        PCO Value: n/a
    Link MTU: 1500
    Non-IP Link MTU: 1358
    Roamer Link MTU: 1500
    ePDG Selection FQDN: N/A
ehrpd access: N/A
.
.
.
.
Fallback To APN Rule Base : Disabled
```

No udp-checksum のサポート

この機能は、ダウンリンク サブスクライバ パケットの外部 GTPU ヘッダーで **udp-checksum** が無効になっている、GTPU サービスの CUPS の **no udp-checksum** CLI コマンドをサポートします。ダウンリンクパケットがインターネットから到着すると、GTPUヘッダーがパケットの先頭に追加され、アクセス側に送信されます。このパケットの外部 UDP レイヤの「チェックサム」値はゼロなので、最適化が可能になり、パフォーマンススループットが向上します。

この機能を有効にするには、次の設定を使用します。

```
configure
   context context_name
      gtpu-service gtpu_service_name
      [ no ] udp-checksum
      end
```

show コマンドと出力

ここでは、この機能をサポートするために使用可能なshowCLIコマンドについて説明します。

次のコマンドを使用して、**GTPU UDP チェックサム**が有効か無効かを確認します。

- **show gtpu-service all**：すべての GTPU サービスを表示します。
- **show gtpu-service name** *service_name*：特定の GTPU サービス名の情報を表示します。

egtpinmgr リカバリの最適化

以前は、egtpinmgr タスクが再起動すると、回復にかなりの時間がかかったため、egtpinmgr の回復中に SAEGW が新しいコールを受け入れられず、障害時間が長くなっていました。

ソフトウェアが拡張され、egtpinmgr リカバリの内部アルゴリズムと必要なデータ構造を最適化することで、egtpinmgrタスクが再起動した場合のリカバリ障害期間が最適化されています。さらに、リカバリ時間は、IMSI のセッション数ではなく、一意の IMSI の数によってのみ決まるようになりました。

（注） egtpinmgr リカバリの最適化は、非 CUPS アーキテクチャでサポートされている既存の機能です。このリリースでは、この機能が CUPS アーキテクチャで認定されました。

QUIC IETF の導入

現在のフレームワークでは、プラグイン到達時に、フロー内のすべてのパケットに対してディープパケットインスペクション（DPI）が実行されます。DPI は、パケットを分析し、確定的なパターンを抽出することによって実行されます。DPI は順番に実行され、アプリケーションの検出とそのサブタイプの分類を行います。プラグインは、DPI 後のフローを除外します。フローは検出後にオフロードされます。QUIC IETF の一部として、初回の QUIC ハンドシェイクパケット（Client Hello/Server Hello）はネットワーク上で暗号化されます。したがって、アプリケーションの検出に使用できる確定的なパターンはありません。p2p プラグインによる、検出用 SNI（Server Name Indication）の復号と取得が新たにサポートされるようになりました。

QUIC IETF の設定

QUIC IETF 復号を有効または無効にするには、次の設定を使用します。

```
configure
  active-charging service acs_service_name
    p2p-detection debug-param protocol-param p2p_quic_ietf_decrypt 1
    end
```

（注） デフォルトでは、CLI は無効になっており、TLS 復号によるパフォーマンスへの影響は最小限です。

クォータホールド時間のサポート

Quota-Hold-Time（QHT）は非アクティブ期間であり、この期間が経過すると、ゲートウェイ（Diameter クライアント）は使用状況を含む課金バケットを返し、クリーンな状態となります。

QHT 値は、OCS によって Multiple-Services-Credit-Control（MSCC）のカテゴリごとに提供されます。また、ゲートウェイには QHT のデフォルト値を設定するオプションがあります。このオプションでは、OCS から QHT AVP が提供されていない MSCC のデフォルト QHT 値を有効にします。

QHT タイマーは、MSCC バケットごとに実行されます。実行時にパケットなしで QHT タイマーが切れると、3GPP 仕様に従って [Reporting-Reason: QHT] として使用状況が報告されます。

OCS から CP で受信した QHT 値は、CUPS 仕様 3GPP TS 29.244 で定義されている「Quota Holding Time」IE で送信されます。また、Quota-Holding-Time IE を UP にプロビジョニングす

るとともに、Quota-Holding-Time SET に対応するビットを含む Reporting-Trigger が送信されるため、QHT が終了するとレポートが実行されます。

QHT Reporting-Trigger が有効になっている Quota-Holding-Time IE を受信した UP は、非アクティブ期間をモニターするために URR ごとのタイマーを開始します。非アクティブ期間が QHT 時間を超えると、Quota-Holding-Time のトリガーによって UP からの使用状況レポートが開始されます。

CP は、UP から QHT イベントを受信すると、MSCC バケットの使用状況を更新した後、OCS への QHT レポートをトリガーします。

クォータホールド時間の設定

CUPS でクォータホールド時間を有効にするには、次の設定を使用します。

```
configure
  require active-charging
  active-charging service service_name
    credit-control group group_name
      quota-hold-time timer_value
      end
```

注：

- **quota-hold-time**：課金バケットが使用状況を報告し、クリーンな状態になるまでの非アクティブ期間を設定します。

制限事項

QHT（inactivity-timer）は、通常、flow-idle timer よりも大きな値となります。flow-idle timer が QHT よりも大きいと、QHT が経過した後もフローが存在し、[NoQuota Pending-Traffic-Treatment] 設定に従って VPP によって処理される可能性があります。

S-GW ページングの機能拡張

S-GW ページングには、次のシナリオが含まれます。

シナリオ 1：S-GW が MME/S4-SGSN ノードにダウンリンクデータ通知（DDN）メッセージを送信します。MME/S4-SGSN は、DDN Ack メッセージで S-GW に応答します。MME/S4-SGSN からの DDN Ack メッセージを待つ間に、S-GW が優先順位の高いダウンリンクデータを受信した場合、S-GW は MME/S4-SGSN に DDN を再送信しません。

シナリオ 2：DDN が MME/S4-SGSN に送信され、TAU/RAU MBR が別の MME/S4-SGSN から受信された場合、S-GW は DDN を送信しません。

シナリオ 3：DDN が MME/S4-SGSN に送信され、[Cause] が 110 の DDN Ack を受信します。原因が 110 の DDN Ack は DDN 障害として扱われ、標準の DDN 障害アクション手順が開始されます。

これらのシナリオに対処するため、CUPS アーキテクチャの DDN 機能に次の 2 つの拡張機能が追加されました。

- S-GW での高優先順位 DDN
- MBR-DDN コリジョン処理

これらの拡張機能は、次をサポートします。

- S-GW および SAEGW での高優先順位 DDN。これにより、MME/S4-SGSN によるページングの優先順位付けが可能になります。
- ページング KPI および VoLTE サービスの拡張。
- DDN が失われないようにするための DDN メッセージとモビリティ手順。
- MBR ガードタイマー。一時的な HO を含む DDN Ack を受信すると開始されます。CLI コマンド **ddn temp-ho-rejection mbr-guard-timer** が導入され、原因が 110（一時的なハンドオーバーが進行中）の DDN Ack を受信した後、ガードタイマーによって MBR を待機できるようになりました。
- 制御ノードの変更によってトリガーされた DDN による TAU/RAU。

さらに、3GPP 標準規格に準拠するため、ダウンリンクデータ通知メッセージおよびモビリティ手順のサポートも強化されます。これにより、DDN メッセージと DDN をトリガーするダウンリンクデータが失われることがなくなります。そのため、SIP Invite データが原因で DDN が開始されるシナリオにおいて、ページング KPI と VoLTE の成功率が向上します。

（注） DDN 遅延および DDN スロットリングをサポートするダウンリンクデータ通知（DDN）メッセージについては、このガイドの「*DDN* 遅延および *DDN* スロットリングを使用した *SAEGW* アイドルバッファリング」の章を参照してください。

S-GW ページング拡張機能の動作、設定、モニタリング、および障害対応の詳細については、StarOS の『*S-GW* アドミニストレーション ガイド』[英語] の「*S-GW Paging Enhancements*」の章を参照してください。

コントロールプレーンでのセッションリカバリと ICSR

セッションリカバリ（SR）機能は、システム内のハードウェアまたはソフトウェアに障害が発生した場合に、サブスクライバセッション情報のシームレスなフェールオーバーと再構築を行い、完全に接続されたユーザーセッションが切断されるのを防ぎます。

シャーシ間セッションリカバリ（ICSR）機能は、サブスクライバのサービスを中断することなく継続的なコール処理を可能にする、最高レベルの可用性を実現します。ICSR により、オペレータは冗長性を確保するためにゲートウェイを設定することができます。ゲートウェイで障害が発生した場合、ICSR はその障害を迂回してセッションを透過的にルーティングできるため、ユーザーエクスペリエンスが維持されます。ICSR では、セッション情報と状態も維持されます。

既存の非 CUPS フレームワークは、CUPS コントロールプレーンの SR と ICSR をサポートするように拡張されます。コントロールプレーンでは、SR/ICSR のときに完全なセッション/PDN 状態が回復されます。

SR と ICSR の詳細については、『VPC-SI システム アドミニストレーション ガイド』の「Session Recovery」機能と「Interchassis Session Recovery」機能の章を参照してください。



重要 このリリースでは、コントロールプレーン（CP）で ICSR スイッチオーバーが実行された場合、**show sx peers** CLI コマンドは新しいアクティブシャーシで関連付けられたピアを表示しません。ただし、機能への影響はありません。

アクティブ CP とスタンバイ CP での SRP over IPsec

IPSec は、IP ネットワーク全体でセキュアなプライベート通信を提供するために相互にデータをやり取りする一連のプロトコルです。これらのプロトコルにより、システムはピアセキュリティ ゲートウェイとセキュアなトンネルを確立して維持できます。IPSec は、IP データグラムに機密性、データの完全性、アクセス制御、およびデータソース認証を提供します。

CUPS アーキテクチャでは IPSec プロトコルを活用して、アクティブ CP とスタンバイ CP 間のシャーシ間セッションリカバリ（ICSR）接続を介して送信されるパケットを暗号化します。この暗号化を実現するために、Service Redundancy Protocol（SRP）ピア間のすべてのトラフィックを照合するアクセスリストが定義され、このリストがクリプトマップに関連付けられます。このクリプトマップは、CP に存在する IPSec ピア間のセキュリティ アソシエーションを確立するために使用されます。

IPSec、その機能、および該当する CLI 設定の詳細については、StarOS の『IPSec Reference』を参照してください。

設定例

1. **IKEv1**：トンネルモード

   次にトンネルモードの IKEv1 の設定例を示します。

```
ACL:
   ip access-list acl_name
      permit ip host ipv4_address host ipv4_address
Transform Set:
crypto ipsec transform-set transform_name esp hmac sha1-96 cipher
aes-cbc-128
      mode tunnel
Policy:
ikev1 policy priority
      encryption aes-cbc-256
      group 5
      lifetime time
Crypto-Map:
crypto map map_name ipsec-ikev1
      match address acl_name
```

```
      set peer ipv4_address
      set ikev1 preshared-key ikev1_key
      set pfs group2
      set security-association lifetime seconds seconds
      set transform-set transform_name
Interface Association:
    interface interface_name
       ip address ipv4address_range
       crypto-map map_name
    interface interface_name loopback
       ip address address_range
!
ip route ipv4address_range interface_name
```

2. **IKEv1**：トランスポートモード

   次にトランスポートモードの IKEv1 の設定例を示します。

```
ACL:
   ip access-list acl_name
      permit ip host ipv4_address host ipv4_address
Transform Set:
crypto ipsec transform-set transform_name esp hmac sha1-96 cipher
aes-cbc-128
      mode transport
Policy:
ikev1 policy priority
      encryption aes-cbc-256
      group 5
      lifetime time
Crypto-Map:
crypto map map_name ipsec-ikev1
      match address acl_name
      set peer ipv4_address
      set ikev1 preshared-key ikev1_key
      set pfs group2
      set security-association lifetime seconds seconds
      set transform-set transform_name
Interface Association:
    interface interface_name
       ip address ipv4address_range
!
    interface interface_name loopback
       ip address address_range
       crypto-map map_name
!
ip route ipv4address_range interface_name
```

（注） IKEv1：認証ヘッダー（AH）プロトコルを使用したトランスポートモードはサポートされません。トンネルモードのみがサポートされます。ESP では認証と暗号化の両方が実行されるため、Encapsulating Security Payload（ESP）が推奨されます。

3. **IKEv2**：**IPv4**

次に IPv4 アドレスの IKEv1 の設定例を示します。

```
ACL:
   ip access-list acl_name
     permit ip host ipv4_address host ipv4_address
Transform Set:
ipsec transform-set transform_name
!
ikev2-ikesa transform-set transform_name
Crypto-Map:
crypto map map_name ikev2-ipv4
     match address name
     authentication local pre-shared-key key key_name
     authentication remote pre-shared-key key key_name
     ikev2-ikesa max-retransmission mt_value
     ikev2-ikesa retransmission-timeout rt_seconds
     ikev2-ikesa transform-set list name
     payload payload match ipv4
       ipsec transform-set list name
     peer ipv4_address
     ikev2-ikesa policy error-notification
Interface Association:
    interface interface_name
     ip address ipv4address_range
     crypto-map map_name
!
    interface interface_name loopback
     ip address ipv4address_range
!
 ip route ipv4address_range interface_name
```

4. **IKEv2**：**IPv6**

次に IPv6 アドレスの IKEv1 の設定例を示します。

```
ACL:
   ip access-list acl_name
     permit ip host ipv6_address host ipv6_address
Transform Set:
ipsec transform-set transform_name
!
ikev2-ikesa transform-set transform_name
Crypto-Map:
crypto map map_name ikev2-ipv6
     match address name
     authentication local pre-shared-key key key_name
     authentication remote pre-shared-key key key_name
     ikev2-ikesa transform-set list name
     payload payload match ipv6
       ipsec transform-set list name
!
     peer ipv6_address
Interface Association:
    interface interface_name
```

```
      ipv6 address ipv6_address
      crypto-map map_name
!
    interface interface_name loopback
      ipv6 address ipv6_address
!
 ipv6 route ipv6address_range interface_name
```

注：

- MTU は、ループバック インターフェイスの上限に設定する必要があります。次に例を示します。

```
configure
   context SRP
      ip path-mtu-max 1300
```

- IKEv1：認証ヘッダー（AH）プロトコルを使用したトランスポートモードはサポートされません。トンネルモードのみがサポートされます。ESP では認証と暗号化の両方が実行されるため、Encapsulating Security Payload（ESP）が推奨されます。
- 既存の IKEv1/IKEv2 ACL トンネルの自動削除：IKEv1 ポリシー内の重要な（認証、暗号化、ハッシュ、DH グループ）パラメータの変更により、そのコンテキスト内で確立されたすべてのトンネルが削除されます。

  詳細については、StarOS の『IPSec Reference』の「Auto-delete Existing IKEv1/IKEv2 ACL Tunnels」セクションを参照してください。

SRVCC PS から CS へのハンドオーバー指示および QoS クラスインデックス IMS メディア設定のサポート

この機能は、音声ベアラーの削除時に PCC ルールが非アクティブ化された原因を PCRF に通知します。この通知は、PCRF が適切に追加のアクションを実行するのに役立ちます。

この機能により、SRVCC のコンプライアンスが保証されます。この機能は、音声ベアラーの解放後の PS から CS へのハンドオーバー通知もサポートします。

LTE の SRVCC サービスを使用すると、IMS アンカー音声コールサービスにアクセスする単一の無線ユーザー機器（UE）で、LTE ネットワークから回線交換ドメインに切り替えることができます。1 つのアクセスネットワークだけで送受信に対応している間に、UE はネットワークを切り替えます。SRVCC サービスにより、UE が複数の無線アクセス技術（RAT）機能を備える必要がなくなります。

PS セッションをターゲットにハンドオーバーした後、送信元 MME は音声ベアラー（VB）を削除します。MME は、音声ベアラーを非アクティブ化することで VB を削除します。MME は、S-GW/P-GW に対する VB を禁止し、ベアラー削除コマンドメッセージ（TS 29.274 v9.5.0）で Bearer Flags IE に VB フラグを設定します。

IP-CAN ベアラーの終了は、PS から CS へのハンドオーバーが原因で発生します。PCEF は、PS_TO_CS_HANDOVER（TS 29.212 v10.2.0 および TS 23.203 v10.3.0）の値に設定された

Rule-Failure-Code AVP を含めることによって、この IP-CAN ベアラーに関連する PCC ルールを報告します。

課金ルールインストール内の新しい AVP PS-to-CS-Session-Continuity（3GPP リリース 11 で追加）のサポートは、PS から CS への連続性のベアラーサポートを示します。

QCI IMS メディア設定のサポート

セッションリカバリおよびICSR スイッチオーバー時の優先処理対象の IMS メディアベアラーをマークするには、QoS Class Index（QCI）の値を指定します。

モード

Exec > Global Configuration > Context Configuration > APN Configuration

configure > context <*context_name* > **apn** <*apn_name*>

上記のコマンドシーケンスを入力すると、次のプロンプトが表示されます。

[context_name]host_name(config-apn)#

構文

qci *value_bytes* **ims-media**

no qci *value_bytes* **ims-media**

（注）

- *no*：この IMS QCI 機能を無効にします。
- *ims_media*：セッションリカバリおよび ICSR スイッチオーバー時の優先処理対象の IMS メディアとして分類されたベアラーにマークを付けます。
- *value_bytes*：QCI 値を 1 ～ 254 の整数で指定します。

使用上のガイドライン

このコマンドを使用すると、セッションリカバリおよび ICSR スイッチオーバー時に優先的に処理する IMS メディアとして分類されたベアラーをマークするための QCI 値を指定できます。

この機能の導入には、次の前提条件が適用されます。

- 専用の APN を VoLTE トラフィック用に予約する必要があります。
- この APN に接続されたコールは、VoLTE に設定された QCI に一致する専用ベアラーがない限り、アクティブ VoLTE として分類されません。
- 優先処理は、アクティブな VoLTE であるコールにのみ適用されます。
- この APN に接続されたGGSNコールは、VoLTE に設定された QCIに一致するネットワーク開始ベアラーがない限り、アクティブ VoLTE として分類されません。
- VoLTE マーキングは、Gn-Gp ハンドオフで保持されます。

CLI コマンドを使用してこの機能を有効にすると、次のアクションが実行されます。

- ベアラーの作成時
  - 新しいベアラー QCI が APN 設定と照合されます。
  - QCI が APN 設定と一致する場合、ベアラーは優先処理の対象としてマークが付けられます。
  - Flow_entries はこの情報で変更されます（これが最初の VoLTE ベアラーの場合）。
  - Egtpu_session は、rx_setup 要求中に VoLTE タグで更新されます。
  - 通知メッセージは、VoLTE のタグ付けについて ECS に通知します。
- ベアラーの削除時
  - これが最後の VoLTE ベアラーである場合、Flow_entry は VoLTE 情報を使用して更新されます。
  - ECS には、指示メッセージを介して削除が通知されます。

次のコマンドは、QCI が 9 の IMS ベアラーの優先処理を有効にします。

qci 9 ims-media

ip hide-service-address CLI コマンドのサポート

ip hide-service-address CLI コマンドは CUPS でサポートされます。

この CLI を有効にすると、この APN を使用する GGSN の IP アドレスがモバイルステーション（MS）から到達不能になります。このコマンドは、APN ごとに設定します。

この機能を有効または無効にするには、次の設定を使用します。

```
configure
  context context_name
    apn apn_name
      [ default | no ] ip hide-service-address
      end
```

- **default**：モバイルステーションがこの APN を使用して GGSN IP アドレスに到達することを許可しません。
- **no**：モバイルステーションがこの APN を使用して GGSN IP アドレスに到達することを許可します。
- このコマンドを使用して、サブスクライバがトレースルートを使って、公的領域内にあり、サービスに設定されているネットワークアドレスを検出しないようにします。

regardless-of-other-triggers CLI コマンドのサポート

この機能は、CUPS の CLI で **regardless-of-other-triggers** オプションをサポートします。**regardless-of-other-triggers** オプションは、合間に発生する他の eG-CDR または P-GW-CDR トリガーに関係なく、一定の時間間隔での eG-CDR または P-GW-CDR の生成を有効にします。したがって、このオプションを有効にすると、他の CDR トリガーが発生しても、Time Limit CDR は秒単位の [interval] ごとに動的にトリガーされます。つまり、[Time Threshold] は、前回のしきい値時間とこの間隔の合計をもとに計算されます。このオプションは、セッションリカバリと ICSR をサポートします。

この機能を有効にするには、次の設定を使用します。

```
configure
  active-charging service service_name
    rulebase rulebase_name
      egcdr threshold interval interval regardless-of-other-triggers
      end
```

新しいコールを受信すると、次の手順が実行されます。

- 有効にすると、**regardless-of-other-triggers** の間に他の使用状況レポートがトリガーされてもタイマーはリセットされず、設定された間隔ごとに時間しきい値に対応するセッション使用状況レポートが生成されます。

show コマンドと出力

ここでは、この機能をサポートするために使用可能な show CLI コマンドについて説明します。

- **show active-charging rulebase name** *name*
- **show active-charging rulebase all**

これらの CLI コマンドの出力には、この機能をサポートする次のフィールドが含まれます。

- Interval Threshold：<seconds> (secs) Regardless of Other Triggers

デフォルトベアラーの TFT 抑制

機能説明

デフォルトベアラーの TFT 抑制は、UPC CUPS アーキテクチャでサポートされています。この機能をサポートするために、次の CLI コマンドが追加されました。

- **policy-control update-default-bearer**
- **no tft-notify-ue-def-bearer**

上記の CLI コマンドを使用して、QoS および ARP を使用せずに、またはデフォルトのベアラーと同じ QoS および ARP を使用して PCRF から受信したすべての定義済みルールをデフォルトのベアラーにバインドします。

重要　この CLI は、シャーシ設定のすべてのルールベースに適用されます。その間またはその後にルールベースが変更された場合、この CLI は現在の新しいルールベースにも引き続き適用されます。

TFT 抑制の設定

デフォルトベアラーの事前定義ルールの TFT 抑制の設定

デフォルトベアラーの TFT 抑制を設定するには、次のコマンドを使用します。

```
configure
  require active-charging
  require active-charging service_name
    [ default | no ] policy-control update-default-bearer
    end
```

注意　**no policy-control update-default-bearer** CLI コマンドを実行する際、charging-action に TFT 情報が追加されていないと、システムクラッシュが発生する可能性が高くなります。

デフォルトベアラーの TFT 抑制の設定

デフォルトベアラーの TFT 抑制を設定するには、次のコマンドを使用します。

```
configure
  require active-charging
  require active-charging service_name
    rulebase rulebase_name
      [ default | no ] tft-notify-ue-def-bearer
    end
```

（注）

- **default**：このコマンドにデフォルト設定を設定します。

  デフォルトベアラーの QoS を持つルールのみデフォルトベアラーへのバインドを無効にし、他のルールを無視しないように指定します。ルールはそれぞれの QoS に応じて、適切なベアラーにアタッチされます。また、UE（アクセス側）への TFT 更新は抑制されません。

- **no**：デフォルトベアラーの QoS を持つルールのデフォルトベアラーへのバインドを有効にし、他のルールを無視するよう指定します。

  QoS が指定されていない場合、ルールはデフォルトベアラーにアタッチされます。また、デフォルトベアラーでは、UE（アクセス側）への TFT 更新が抑制されます。このため、作成される default-bearer は常に 1 つのみです。

ゼロバイト EDR 抑制

CLI 制御機能であるゼロバイト イベント データ レコード（EDR）抑制は、フローのデータがない場合の EDR の作成を有効または無効にします。通常、ゼロバイト EDR は、フローに対して 2 つの連続する EDR が生成される場合に可能です。CLI コマンドは、フローの 2 番目の EDR を抑制します。

ゼロバイト EDR の抑制を有効または無効にするには、次の設定を使用します。

```
configure
  active-charging service service_name
    rulebase rulebase_name
      [ default | no ] edr suppress-zero-byte-records
      end
```

注：

- **default**：デフォルト設定でこのコマンドを設定します。

  デフォルト：[Disabled]。**no edr suppress-zero-byte-records** と同じ。

- **no**：ゼロバイト EDR の抑制を無効にします。

- **edr suppress-zero-byte-records**：ゼロバイト EDR を抑制します。

- **show user-plane-service statistics rulebase name** *rulebase_name* CLI コマンドの出力の「Total zero-byte EDRs suppress」フィールドを使用して、ゼロバイト EDR が抑制されているか確認できます。

機能の仕組み

アーキテクチャ

ユーザープレーンの選択

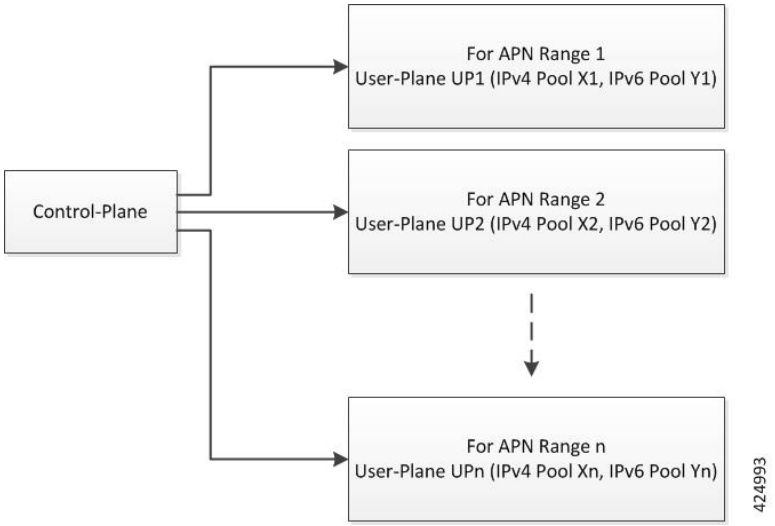
このセクションでは、コントロールプレーンが Sx インターフェイスを介して通信するために特定のユーザープレーンをどのように選択するのかを説明します。現在のメカニズムでは、ユーザー プレーン プロファイルを選択するためのキーとして、その PDN に関連付けられた APN 情報を使用します。

Pure-P/Collapsed PDN

次のフローでは、特定のユーザープレーングループを選択するためのキーとして APN がどのように使用されるのかを説明します。

```
    APN → Associated IP Pool → Associated User Plane Profile ID →
User Plane Profile
```

すべての APN は、関連付けられた IPv4 プールと IPv6 プールの両方で設定されます。また、APN 設定で設定されたすべての IP プールは、同じユーザープレーングループに関連付けられます。このグループには、ユーザープレーンの IP アドレスとユーザープレーンの機能に関連する情報が含まれています。コントロールプレーンがすべての APN の同じユーザープレーンと通信する必要がある場合、APN 設定の IPv4 および IPv6 プール設定は必要ありません。



注：

- コントロールプレーンは、複数のユーザープレーンと通信するように設定できます。
- ユーザープレーンと APN 間には 1-n マッピングがあります。
- 同じユーザープレーンを介して複数の APN に到達できますが、APN ごとに関連付けられるユーザープレーンは 1 つだけです。

Pure-S PDN

次のフローでは、特定のユーザープレーングループを選択するためのキーとして APN がどのように使用されるのかを説明します。APN プロファイルは、関連付けられたユーザープレーングループを使用して設定する必要があります。このグループには、ユーザープレーンの IP アドレスとユーザープレーンの機能に関連する情報が含まれています。

APN Profile → Associated User Plane Profile ID → User Plane Group

コール フロー

次に、CUPS アーキテクチャのコントロールプレーンフローの概要を示します。

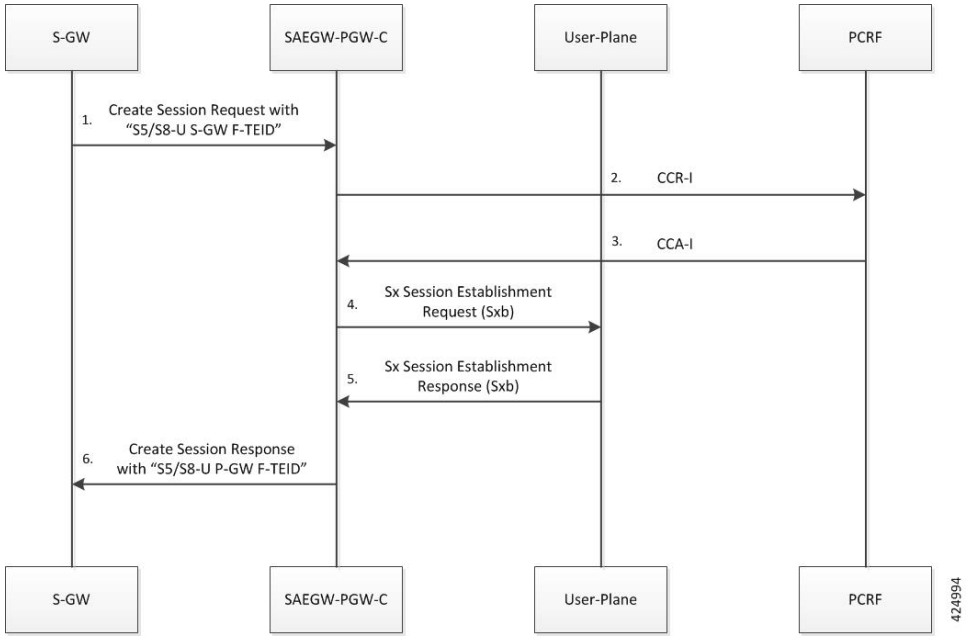
- セッション作成要求を受信すると、S-GW は最初に Sx 通信（Sx セッション確立要求/応答）を行ってから、P-GW にセッション作成要求を送信します。
- セッション作成要求を受信すると、P-GW は次の処理を順番に実行します。
  - Gx 通信（IP-CAN セッション確立手順）

- Sx 通信（Sx セッション確立要求/応答）
- S-GW へのセッション作成応答

- P-GW からセッション作成応答を受信すると、S-GW は最初に Sx 通信（Sx セッション変更要求/応答）を行ってから、MME にセッション作成応答を送信します。

初期接続手順（Pure-P）

次のコールフローは、Pure-P PDN の初期接続手順の概要を示しています。



1. CUPS SAEGW Pure-P コールの場合、SAEGW-PGW-C で次の処理が実行されます。
   - Gx インタラクション後、Gx 通信（CCR-I および CCA-I）を実行します。
   - IP プール（IP プールに関連付けられた APN）を使用して設定された **user-plane-profile** に基づいてユーザープレーンを選択します。
   - GTP-U セッションを確立します（IPv6/IPv4v6 PDN の場合、RA/RS に必要）。
   - 選択したユーザープレーンとの Sxab のインタラクションを実行します。
2. Sx 確立要求には、次の情報が含まれます。
   - アップリンクおよびダウンリンクデータパスの Create PDR/FAR/URR 情報：ダイナミック/事前定義済み/静的ルールの場合。
   - RA/RS の Create PDR/FAR：IPv6/IPv4v6 PDN タイプに必要。



重要

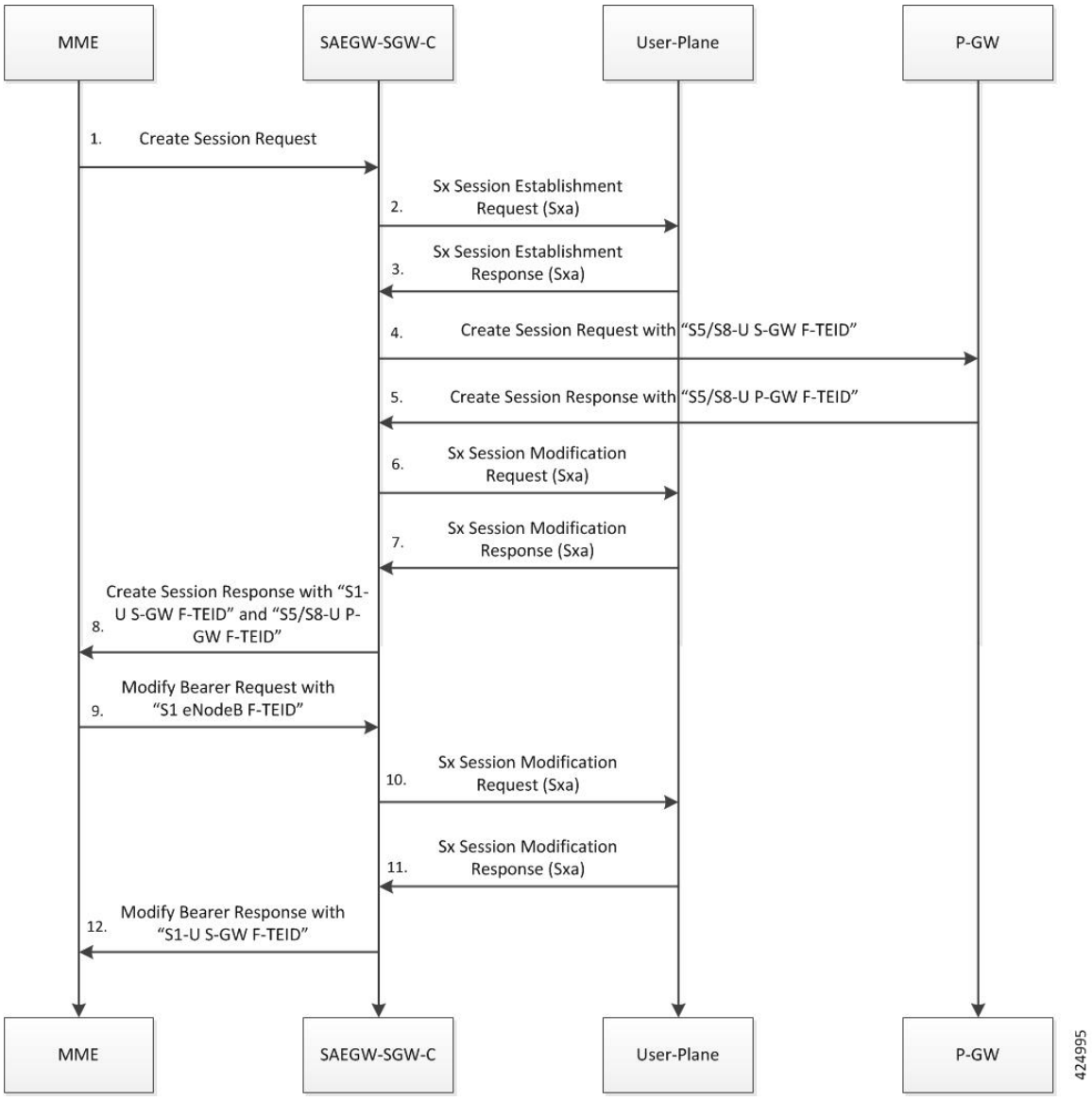
- Create Uplink PDR は、「S5/S8-U S-GW F-TEID」の IP アドレス情報に基づく「Outer Header Removal」で送信されます。
- Create Downlink FAR は、「Outer Header Creation」を「S5/S8-U S-GW F-TEID」にして送信されます。

- さらに、コントロールプレーンは、P-GW 入力 PDR「S5/S8-U P-GW F-TEID」に F-TEID を割り当てるようユーザープレーンに要求します。

3. ユーザープレーンは、Sx セッション確立応答の一部として次の情報を提供します。
   - 作成された PDR：P-GW 入力 PDR「S5/S8-U P-GW F-TEID」
4. Sx セッション確立応答を受信すると、SAEGW-PGW-C は「S5/S8-U P-GW F-TEID」を含むセッション作成応答を S-GW に送信します。

初期接続手順（Pure-S）

次のコールフローは、Pure-S PDN の初期接続手順の概要を示しています。



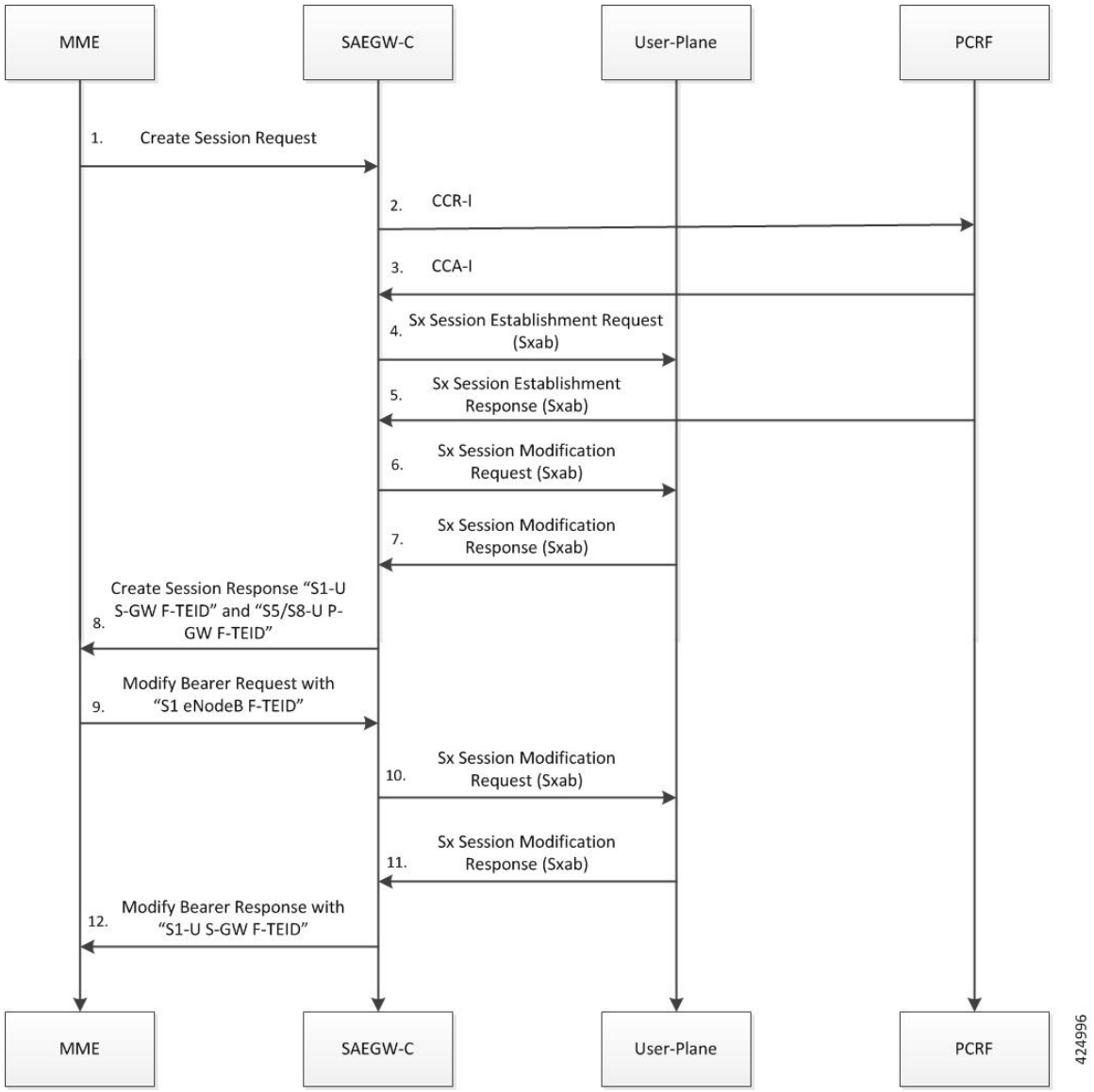
1. CUPS SAEGW Pure-S コールの場合、SAEGW-SGW-C で次の処理が実行されます。
   - APN プロファイルに基づいてユーザープレーンを選択します。
   - 選択したユーザープレーンとの Sxa インタラクションを実行します。
   - GTP-U インタラクションなし（非 CUPS 動作には必要であることに注意してください）。
2. Sx セッション確立要求には、次の情報が含まれます。
   - S-GW アップリンクおよびダウンリンクデータパスの Create PDR/FAR。
   - さらに、次の目的で F-TEID を割り当てるように、コントロールプレーンがユーザープレーンに要求します。

- S-GW 入力 PDR「S1-U S-GW F-TEID」
- S-GW 出力 PDR「S5/S8-U S-GW F-TEID」

3. ユーザープレーンは、Sx セッション確立応答の一部として次の情報を提供します。
   - 作成された PDR：S-GW 入力 PDR「S1-U S-GW F-TEID」
   - 作成された PDR：S-GW 出力 PDR「S5/S8-U S-GW F-TEID」
4. Sx セッション確立応答を受信すると、SAEGW-SGW-C は「S5/S8-U S-GW F-TEID」を含むセッション作成要求を P-GW に送信します。
5. セッション作成応答を受信すると、SAEGW-SGW-C で次の処理が実行されます。
   - Sx セッション変更要求のトリガー：
     - 「Outer Header Creation」を「S5/S8-U P-GW F-TEID」にしてアップリンク FAR を更新します。
     - 「S5/S8-U P-GW F-TEID」の IP アドレス情報に基づく「Outer Header Removal」でダウンリンク PDR を更新します。
6. Sx セッション変更応答を受信すると、SAEGW-SGW-C は「S1-U S-GW F-TEID」と「S5/S8-U P-GW F-TEID」を使用してセッション作成応答を MME に送信します。
7. ベアラー変更要求（MBR）を受信すると、SAEGW-SGW-C で次の処理が実行されます。
   - MBR は S-GW ノードによって消費されます。P-GW ノードへの GTP シグナリングはありません。
   - Sx セッション変更要求のトリガー：
     - 「Outer Header Creation」を「S1 eNodeB F-TEID」としてダウンリンク FAR を更新します。
     - 「S1 eNodeB F-TEID」の IP アドレス情報に基づいて、「Outer Header Removal」を使用してアップリンク PDR を更新します。
8. Sx セッション変更応答を受信すると、SAEGW-SGW-C は「S1-U S-GW F-TEID」を使用して MBR を送信します。

初期接続手順（Collapsed PDN）

次のコールフローは、Collapsed PDN の初期接続手順の概要を示しています。



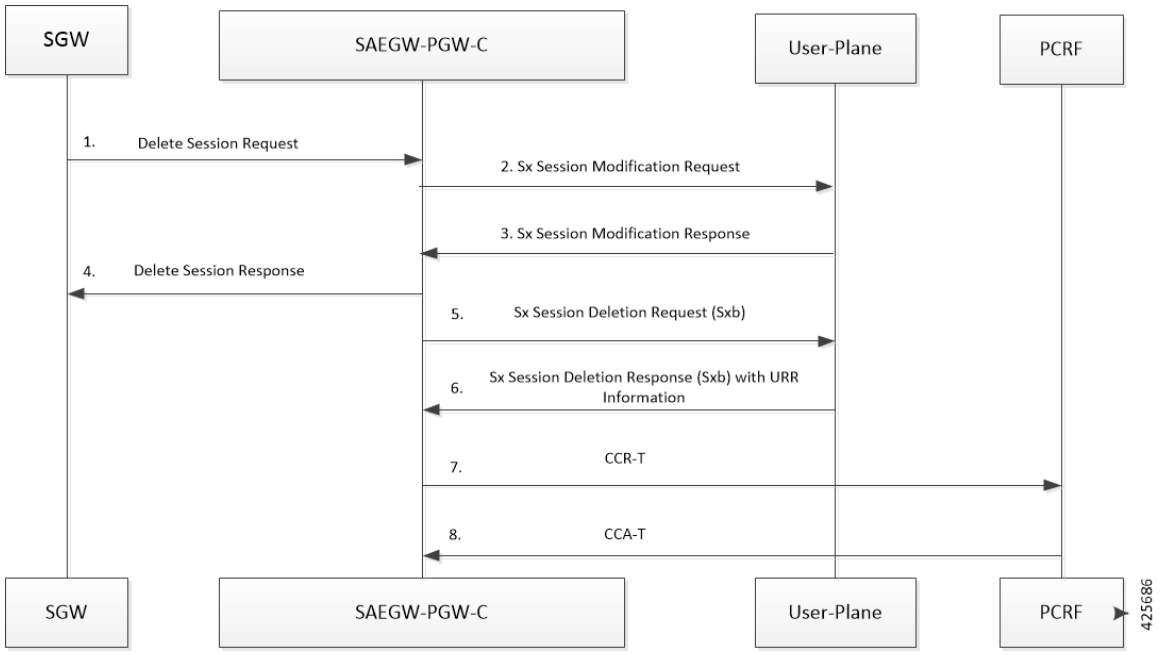
1. CUPS SAEGW Collapsed コールの場合、SAEGW-C で次の処理が実行されます。
   - Gx インタラクション後、Gx 通信（CCR-I および CCA-I）を実行します。
   - IP プール（IP プールに関連付けられた APN）を使用して設定された **user-plane-profile** に基づいてユーザープレーンを選択します。
   - GTP-U セッションを確立します（IPv6/IPv4v6 PDN の場合、RA/RS に必要）。
   - 選択したユーザープレーンと Sxab のインタラクションを実行します。
2. Sx 確立要求には、次の情報が含まれます。
   - S-GW アップリンクおよびダウンリンクデータパス（Sxa タイプ PDR）の Create PDR/FAR 情報。

- アップリンクおよびダウンリンクデータパス（Sxb タイプ PDR）の Create PDR/FAR/URR 情報。ダイナミック/事前定義/静的ルールの場合。
- RA/RS（Sxb タイプ PDR）の Create PDR/FAR：IPv6/IPv4v6 PDN タイプに必要。
- さらに、次の目的で F-TEID を割り当てるように、コントロールプレーンがユーザープレーンに要求します。
  - S-GW 入力「S1-U S-GW F-TEID」
  - S-GW 出力「S5/S8-U S-GW F-TEID」
  - P-GW 入力 PDR「S5/S8-U P-GW F-TEID」

3. ユーザープレーンは、Sx セッション確立応答の一部として次の情報を提供します。
   - 作成された PDR：S-GW 入力 PDR「S1-U S-GW F-TEID」
   - 作成された PDR：S-GW 出力 PDR「S5/S8-U S-GW F-TEID」
   - 作成された PDR：P-GW 入力 PDR「S5/S8-U P-GW F-TEID」
4. 正常な Sx セッション確立応答を受信すると、コントロールプレーンは次の情報を使用して Sx 変更要求をトリガーします。
   - 「S5/S8-U S-GW F-TEID」の IP アドレス情報に基づいて「Outer Header Removal」を使用して P-GW（Sxb）の「アップリンク PDR」を更新
   - 「Outer Header Creation」を「S5/S8-U S-GW F-TEID」として P-GW（Sxb）の「ダウンリンク FAR」を更新
   - 「Outer Header Creation」を「S5/S8-U P-GW F-TEID」として S-GW（Sxa）の「アップリンク FAR」を更新
   - 「S5/S8-U P-GW F-TEID」の IP アドレス情報に基づいて「Outer Header Removal」を使用して S-GW（Sxa）の「ダウンリンク PDR」を更新
5. Sx セッション変更応答を受信すると、SAEGW-C は「S1-U S-GW F-TEID」および「S5/S8-U P-GW F-TEID」を使用してセッション作成応答を MME に送信します。
6. ベアラー変更要求（MBR）を受信すると、SAEGW-C で次の処理が実行されます。
   - Sx セッション変更要求のトリガー：
     - 「Outer Header Creation」を「S1 eNodeB F-TEID」としてダウンリンク FAR を更新します。
     - 「S1 eNodeB F-TEID」の IP アドレス情報に基づいて、「Outer Header Removal」を使用してアップリンク PDR を更新します。
7. Sx セッション変更応答を受信すると、SAEGW-SGW-C は「S1-U S-GW F-TEID」を使用して MBR を送信します。

接続解除手順（Pure-P）：UE 開始

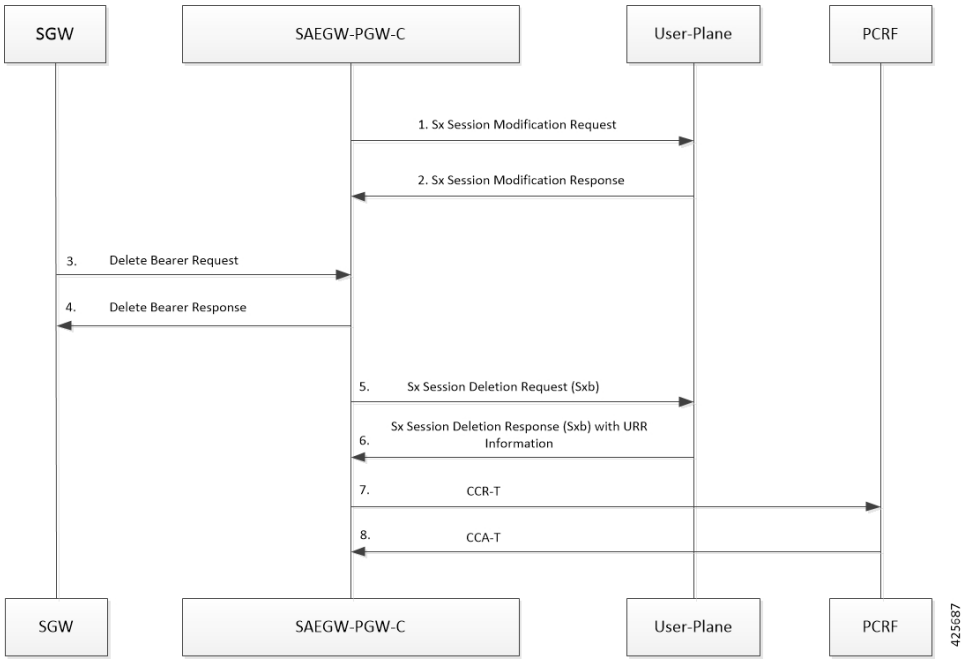
次のコールフローは、UE 開始 Pure-P PDN の接続解除手順の概要を示しています。



1. セッション削除要求を受信すると、SAE-GW-C が Sxab インタラクションを実行し、アップリンクとダウンリンク両方のデータパスに対する Apply Action を「DROP」にして FAR を更新します。
2. Sx セッション変更応答を受信すると、SAE-GW-C が MME にセッション削除応答を送信します。
3. CUPS SAEGW Pure-P コールの場合、SAEGW-PGW-C で次の処理が実行されます。
   - GTP-U セッションを削除します（IPv6/IPv4v6 PDN の場合は RA/RS に必要）。
   - 選択したユーザープレーンとの Sxab インタラクションを実行する。
4. Sx セッション削除応答を受信すると、SAEGW-PGW-C で次の処理が実行されます。
   - Gx 通信（CCR-T および CCA-T）を実行します。
   - 受信した URR 情報に基づいて CDR（Gz）を生成します。

接続解除手順（Pure-P）：ネットワーク開始

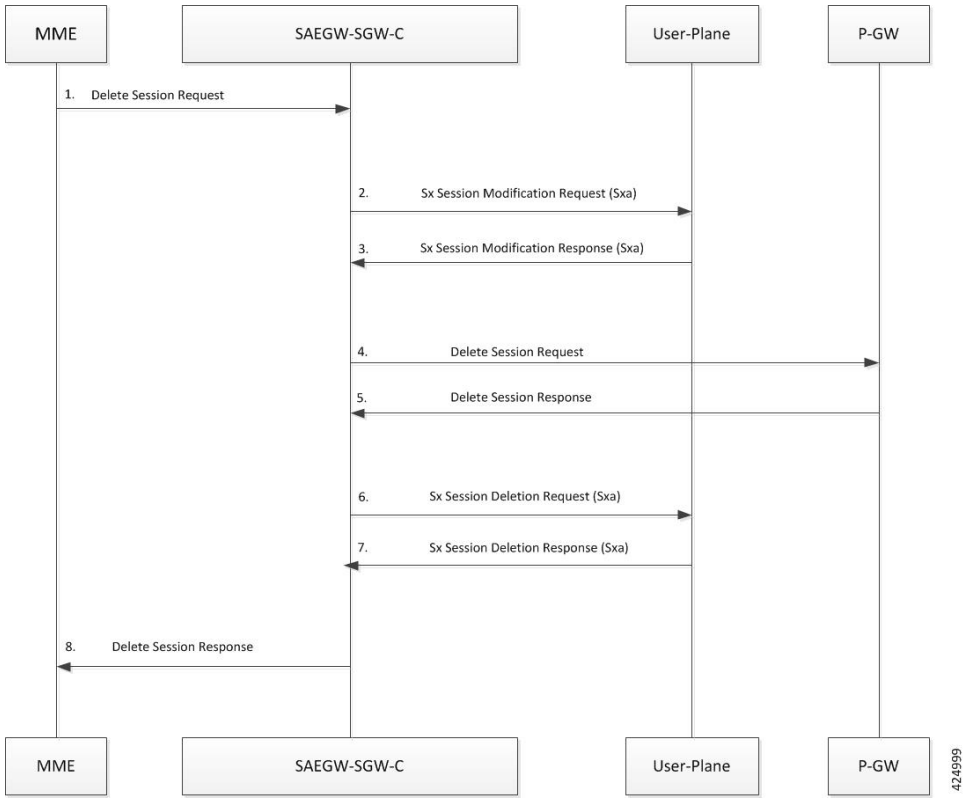
次のコールフローは、ネットワーク開始 Pure-P PDN の接続解除手順の概要を示しています。



1. ベアラー削除要求（RAR により開始されたもの、または **clear sub all** CLI によるもの）を受信すると、SAEGW-PGW-C は Sxab インタラクションを実行し、アップリンクとダウンリンク両方のデータパスに対する Apply Action を「DROP」にして FAR を更新します。
2. Sx セッション変更応答を受信すると、SAEGW-PGW-C が SGW にベアラー削除要求を送信します。
3. CUPS SAEGW Pure-P コールの場合、SAEGW-PGW-C で次の処理が実行されます。
   - GTP-U セッションを削除します（IPv6/IPv4v6 PDN の場合は RA/RS に必要）。
   - 選択したユーザープレーンとの Sxab インタラクションを実行する。
4. Sx セッション削除応答を受信すると、SAEGW-PGW-C で次の処理が実行されます。
   - Gx 通信（CCR-T および CCA-T）を実行します。
   - 受信した URR 情報に基づいて CDR（Gz）を生成します。

接続解除手順（Pure-S）：UE 開始

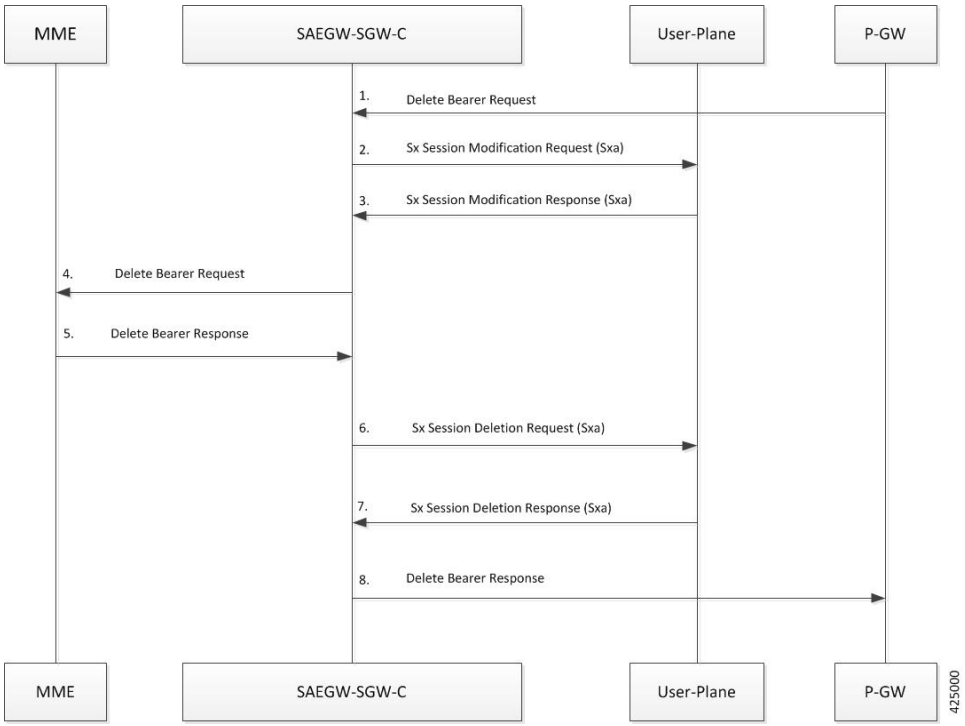
次のコールフローは、UE 開始 Pure-S PDN の接続解除手順の概要を示しています。



1. セッション削除要求を受信すると、SAEGW-SGW-C が Sxa インタラクションを実行し、アップリンクとダウンリンク両方のデータパスに対する Apply Action を「DROP」にして「FAR を更新」します。
2. Sx セッション変更応答を受信すると、SAEGW-SGW-C が P-GW にセッション削除要求を送信します。
3. セッション削除応答を受信すると、SAEGW-SGW-C が Sxa インタラクションを実行して Sx セッションを削除します。
4. Sx セッション削除応答を受信すると、SAEGW-SGW-C が MME にセッション削除応答を送信します。

接続解除手順（Pure-S）：ネットワーク開始

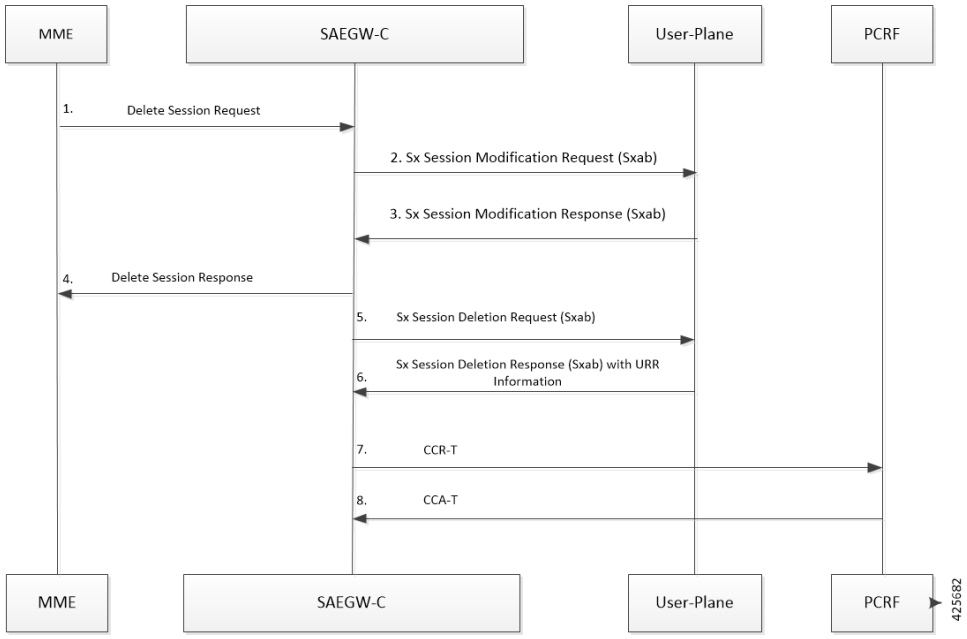
次のコールフローは、ネットワーク開始 Pure-S PDN の接続解除手順の概要を示しています。



1. ベアラー削除要求を受信すると、SAEGW-SGW-C が Sxa インタラクションを実行し、アップリンクとダウンリンク両方のデータパスに対する Apply Action を「DROP」にして「FAR を更新」します。
2. Sx セッション変更応答を受信すると、SAEGW-SGW-C が MME にベアラー削除要求を送信します。
3. MME からセッション削除応答を受信すると、SAEGW-SGW-C が Sxa インタラクションを実行して Sx セッションを削除します。
4. Sx セッション削除応答を受信すると、SAEGW-SGW-C が P-GW にベアラー削除応答を送信します。

切断手順（Collapsed）：UE 開始

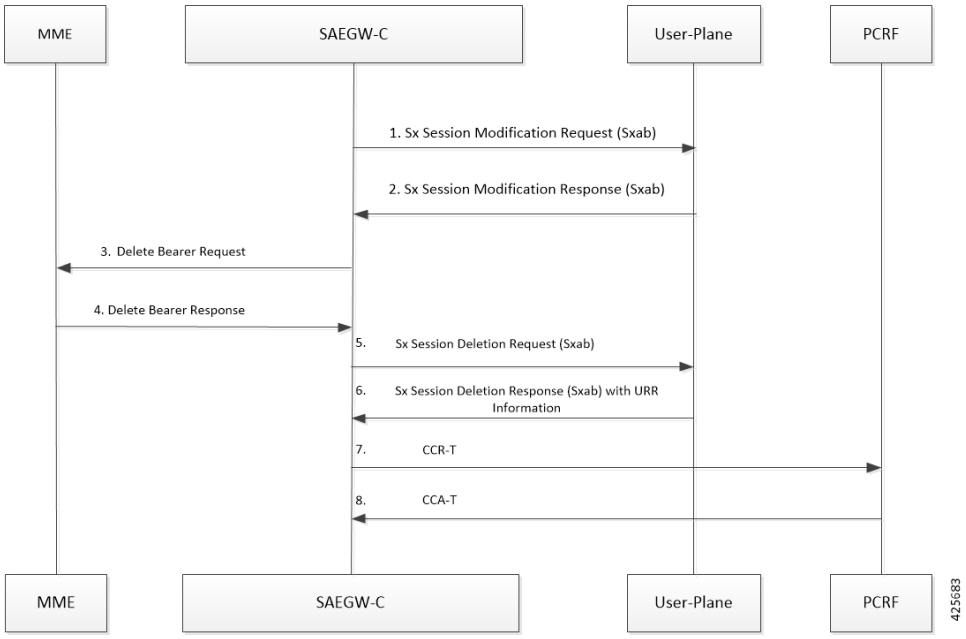
次のコールフローは、UE が開始した Collapsed PDN の切断手順の概要を示しています。



1. セッション削除要求を受信すると、SAEGW-C はSxabインタラクションを実行し、アップリンクとダウンリンクの両方のデータパスに対する Apply Action を「DROP」として FAR を更新します。
2. Sx セッション変更応答を受信すると、SAEGW-C は MME にセッション削除応答を送信します。
3. CUPS SAEGW Collapsed コールの場合、SAEGW-C で次の処理が実行されます。
   - GTP-U セッションを削除します（IPv6/IPv4v6 PDN の場合は RA/RS に必要）。
   - 選択したユーザープレーンとの Sxab インタラクションを実行します。
4. Sx セッション削除応答を受信すると、SAEGW-C で次の処理が実行されます。
   - Gx 通信（CCR-T および CCA-T）を実行します。
   - 受信した URR 情報に基づいて CDR（Gz）を生成します。

接続解除手順（Collapsed）：ネットワーク開始

次のコールフローは、ネットワークが開始した Collapsed PDN の接続解除手順の概要を示しています。

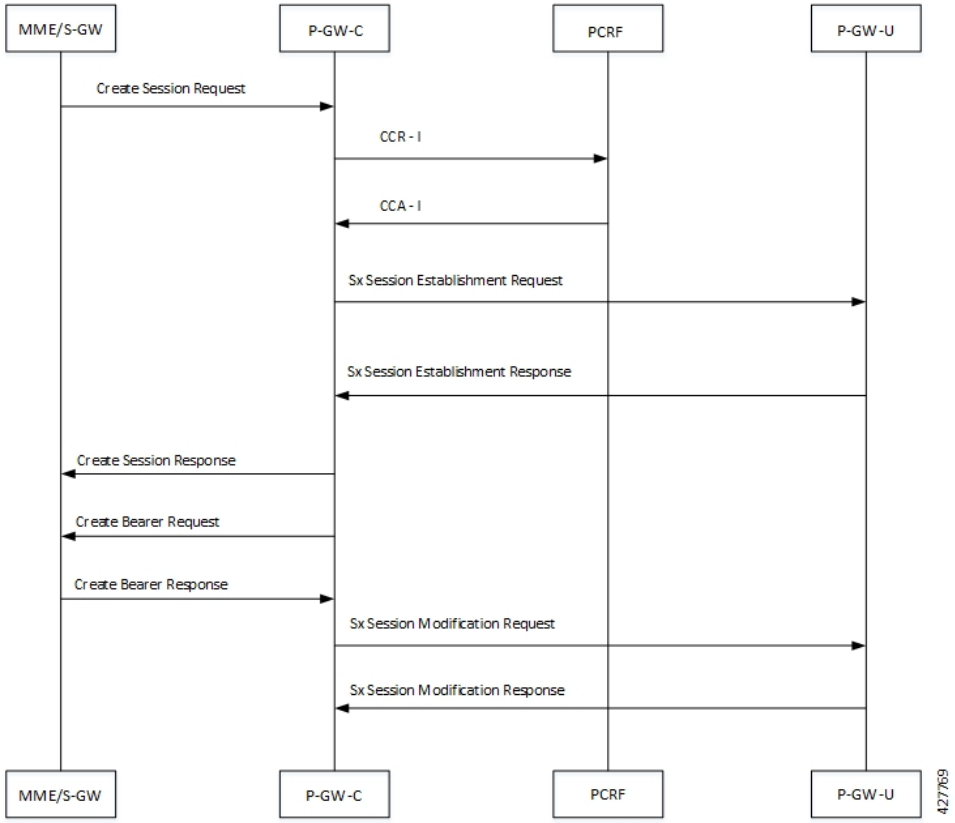


1. ベアラー削除要求（RAR により開始されたもの、または **clear sub all** CLI によるもの）を受信すると、SAEGW-C は Sxab インタラクションを実行し、アップリンクとダウンリンクの両方のデータパスに対する適用アクションを「DROP」にして FAR を更新します。
2. Sx セッション変更応答を受信すると、SAEGW-C は MME にベアラー削除要求を送信します。
3. CUPS SAEGW Collapsed コールの場合、SAEGW-C で次の処理が実行されます。
   - GTP-U セッションを削除します（IPv6/IPv4v6 PDN の場合は RA/RS に必要）。
   - 選択したユーザープレーンとの Sxab インタラクションを実行します。
4. Sx セッション削除応答を受信すると、SAEGW-C で次の処理が実行されます。
   - Gx 通信（CCR-T および CCA-T）を実行します。
   - 受信した URR 情報に基づいて CDR（Gz）を生成します。

専用ベアラーの作成、変更（更新）、削除

専用ベアラーの作成、更新、削除を行えるのは、P-GW と SAEGW のみです。

CCA-I でのベアラーの作成（Pure-P）

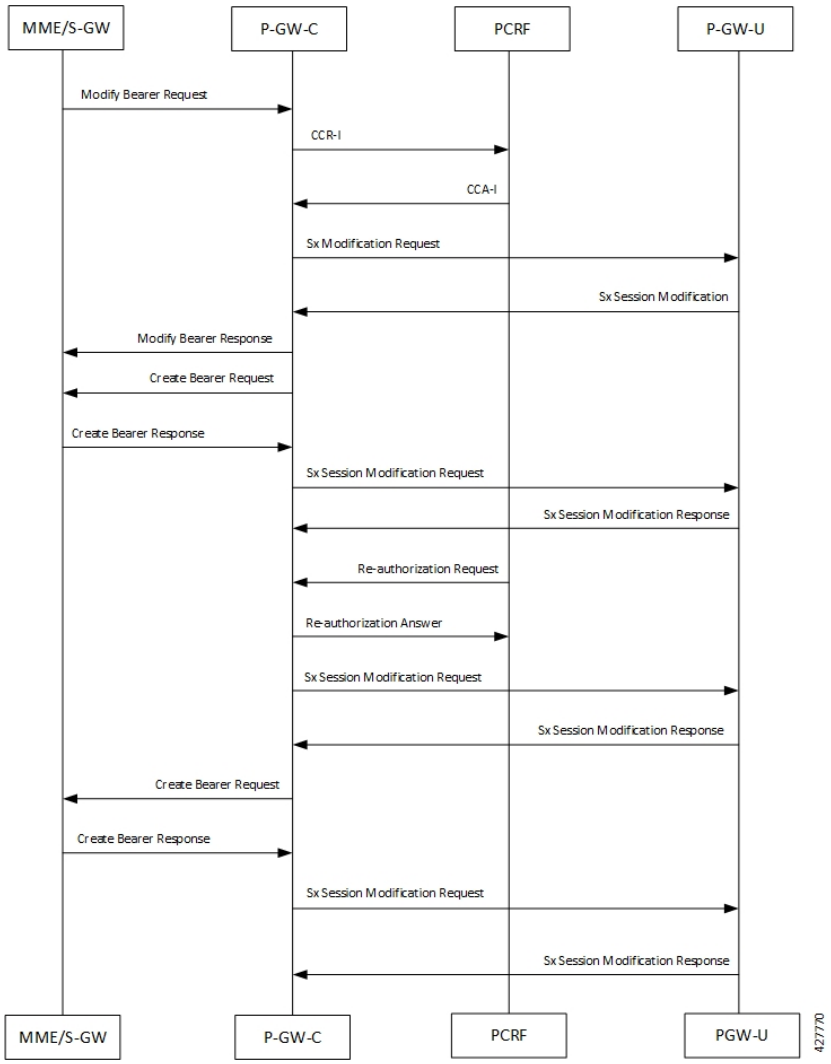


1. UE が最初の PDN を介して接続手順を開始します。S-GW が、他の必須パラメータとともに IMSI、APN、EBI、APN AMBR UL/DL を含むセッション作成要求を PGW-C に転送して PDN 接続を確立します。
2. PGW-C が Credit-Control-Request（初期）を PCRF に送信します。
3. PCRF が、APN AMBR UL/DL を使用して PGW-C に Credit-Control-Answer（初期）で応答し、デフォルトの QoS とは異なる QCI ARP でダイナミック/事前定義済みルールをインストールします。
4. PCRF から Credit-Control-Answer（初期）を受信すると、PGW-C が PGW-U への Sx セッション確立要求を開始し、ID x を選択してデフォルトベアラーの PDR を作成するとともに、ID y を選択して専用ベアラーの PDR を作成します。
5. P-GW-U が、作成された PDR と PGW-U のローカル FTEID のリストを使用して、Sx セッション確立応答で PGW-C に応答します。
6. P-GW-C が、最初の PDN 接続セットアップのために S-GW にセッション作成応答を送信します。
7. P-GW が、ベアラーコンテキストに P-GW の Data FTEID が入力されたベアラー作成要求を S-GW に送信します。

8. S-GW が、リモートデータ FTEID を使用してベアラー作成応答を送信します。これを受信すると、UP 機能への Sx 変更要求が開始され、リモート F-TEID を使用してすべてのダウンリンク FAR に対して Update FAR が送信されます。
9. P-GW-U が P-GW-C に Sx セッション変更応答で応答します。

MBR/MCmd/CCA-U および RAR によるベアラーの作成

次のコールフローは、MBR/MCmd/CCA-U および RAR によるベアラーの作成の概要を示しています。

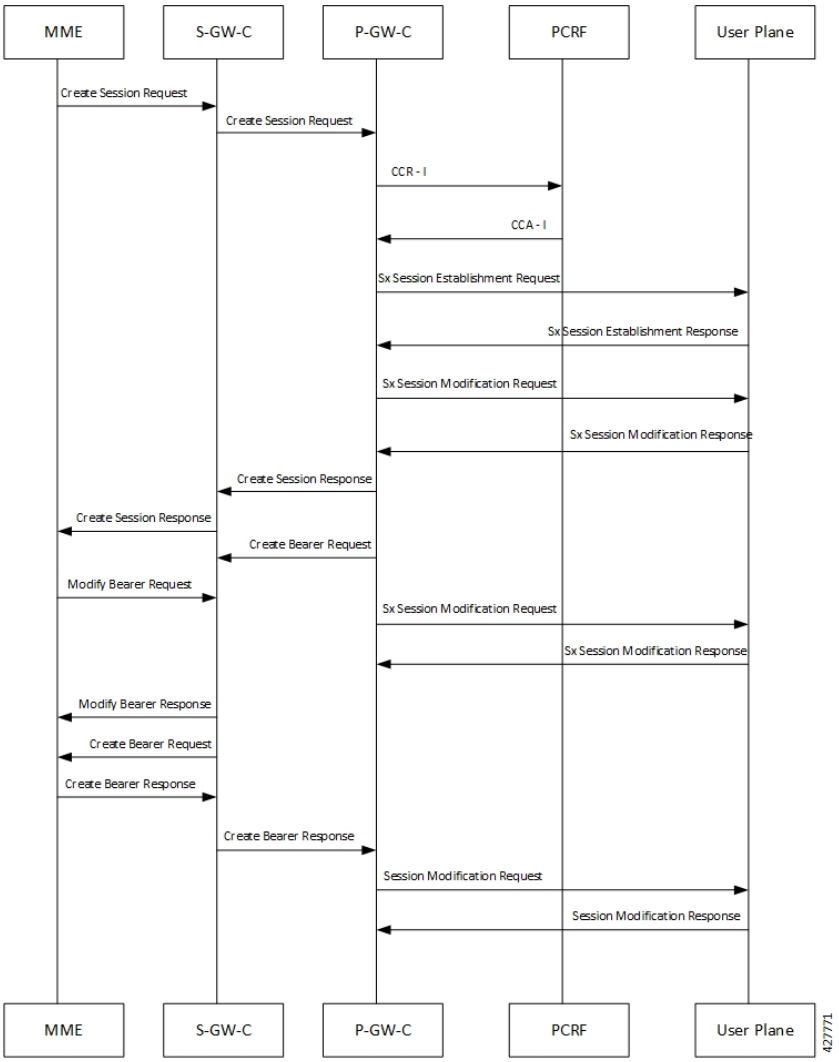


1. PCRF から Credit-Control-Answer（更新）または再承認要求を受信すると、P-GW-C が P-GW-U への Sx セッション変更要求を開始し、ID x を選択してデフォルトベアラーの PDR を作成するとともに、ID y を選択して専用ベアラーの PDR を作成します。
2. P-GW-U が、作成された PDR と P-GW-U のローカル FTEID のリストを使用して、Sx セッション変更応答で P-GW-C に応答します。

3. P-GW が、ベアラーコンテキストに P-GW の Data FTEID が入力されたベアラー作成要求を S-GW に送信します。
4. S-GW が、リモートデータ FTEID を使用してベアラー作成応答を送信します。これを受信すると、UP 機能への Sx 変更要求が開始され、リモート F-TEID を使用してすべてのダウンリンク FAR に対して Update FAR が送信されます。
5. P-GW-U が P-GW-C に Sx 変更応答で応答します。

Collapsed コールの専用ベアラーの作成

次のコールフローは、Collapsed コールのベアラー作成の概要を示しています。

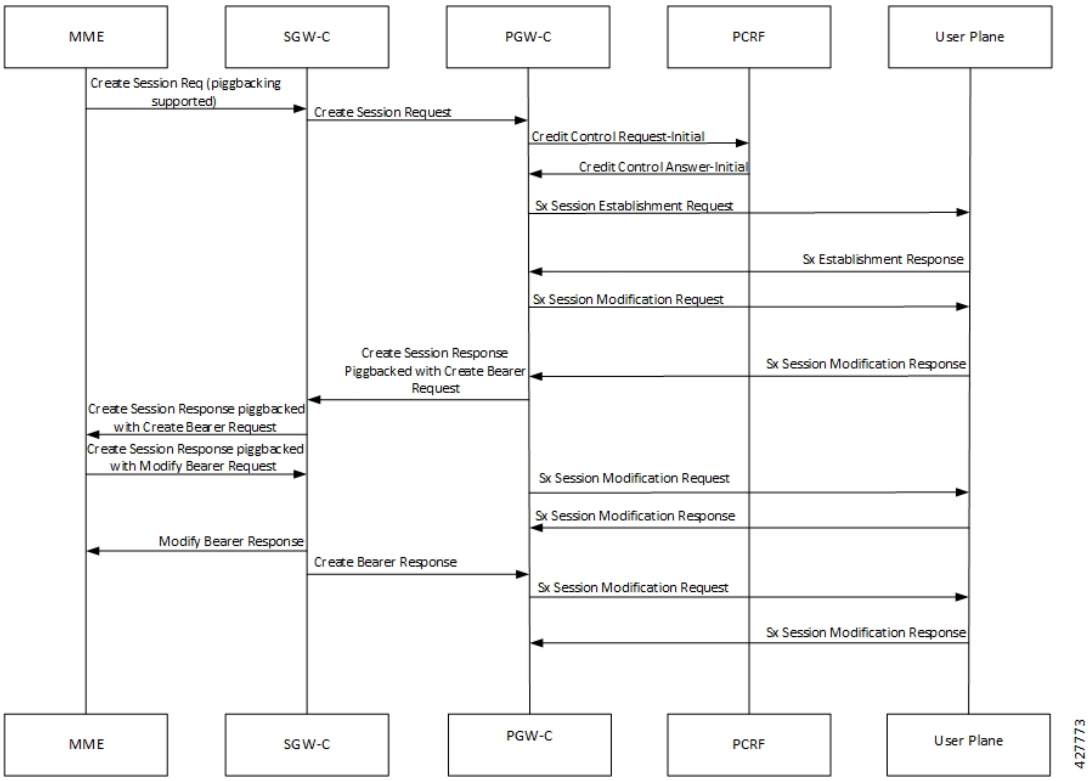


1. UE が最初の PDN を介して接続手順を開始します。SGW-C が、他の必須パラメータとともに IMSI、APN、EBI、APNAMBR UL/DL を含むセッション作成要求を PGW-C に転送して PDN 接続を確立します。

2. PGW-C が Credit-Control-Request（初期）を PCRF に送信します。
3. PCRF が、APN AMBR UL/DL を使用して PGW-C に Credit-Control-Answer（初期）で応答し、デフォルトの QoS とは異なる QCI ARP でダイナミック/事前定義済みルールをインストールします。
4. PCRF から Credit-Control-Answer（初期）を受信すると、PGW-C が SAEGW-U への Sx セッション確立要求を開始し、ID x を選択してデフォルトベアラーの PDR を作成するとともに、ID y を選択して専用ベアラーの PDR を作成します。
5. SAEGW-U が、作成された PDR と PGW-U のローカル FTEID のリストを使用して、Sx セッション確立応答で PGW-C に応答します。
6. SAEGW-U が、作成された PDR と PGW-U のローカル FTEID のリストを使用して、Sx セッション確立応答で PGW-C に応答します。
7. PGW-C が、最初の PDN 接続セットアップのために SGW-C にセッション作成応答を送信します。
8. PGW-C が、ベアラーコンテキストに PGW の Data FTEID が入力されたベアラー作成要求を SGW-C に送信します。
9. SGW-C が、Sx トランザクションが開始される eNodeB TEID を含むベアラー変更要求を受信します。
10. SGW-C が、リモートデータ FTEID を含むベアラー作成応答を受信します。これを受信すると、UP 機能への Sx 変更要求が開始され、リモート F-TEID を使用してすべてのダウンリンク FAR に対して Update FAR が送信されます。
11. SAEGW-U が P-GW-C に Sx セッション変更応答で応答します。

Collapsed コールに対して有効になっているピギーバックを使用したベアラーの作成

次のコールフローは、Collapsed コールに対して有効になっているピギーバックを使用したベアラー作成の概要を示しています。

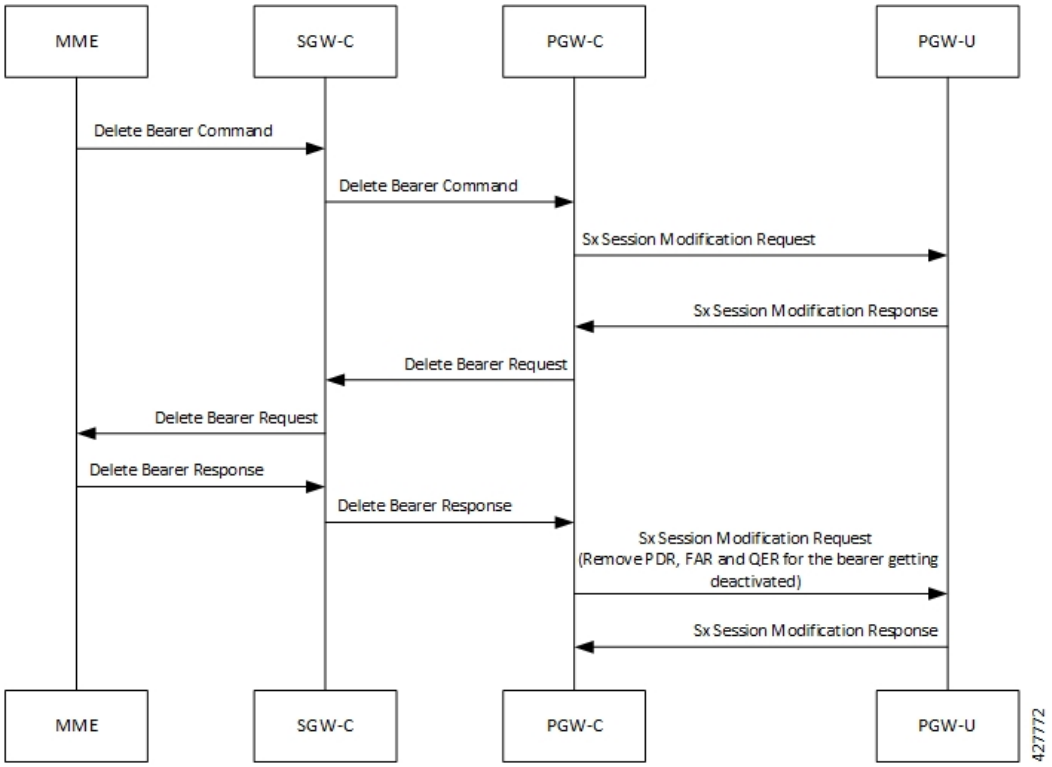


1. UE が最初の PDN を介して接続手順を開始します。SGW-C が、他の必須パラメータとともに IMSI、APN、EBI、APNAMBR UL/DL を含むセッション作成要求を PGW-C に転送して PDN 接続を確立します。
2. PGW-C が Credit-Control-Request（初期）を PCRF に送信します。
3. PCRF が、APN AMBR UL/DL を使用して PGW-C に Credit-Control-Answer（初期）で応答し、デフォルトの QoS とは異なる QCI ARP でダイナミック/事前定義済みルールをインストールします。
4. PCRF から Credit-Control-Answer（初期）を受信すると、PGW-C が SAEGW-U への Sx セッション確立要求を開始し、ID x を選択してデフォルトベアラーの PDR を作成するとともに、ID y を選択して専用ベアラーの PDR を作成します。
5. SAEGW-U が、作成された PDR と PGW-U のローカル FTEID のリストを使用して、Sx セッション確立応答で PGW-C に応答します。
6. Sx 変更要求がトリガーされ、デフォルトベアラーと専用ベアラー両方の PDR と FAR が更新されます。
7. PGW-C が、最初の PDN 接続セットアップのために SGW-C にセッション作成応答を送信します。
8. PGW-C が、ベアラーコンテキストに PGW の Data FTEID が入力されたベアラー作成要求を SGW-C に送信します。これは、PDN が完全に接続されるまで SGW-C でバッファリングされます。

9. SGW-C が、Sx トランザクションが開始される eNodeB TEID を含むベアラー変更要求を受信します。
10. SGW-C が、リモートデータ FTEID を含むベアラー作成応答を受信します。これを受信すると、UP 機能への Sx 変更要求が開始され、リモート F-TEID を使用してすべてのダウンリンク FAR に対して Update FAR が送信されます。
11. SAEGW-U が P-GW-C に Sx セッション確立応答で応答します。

Pure P コールのベアラー削除コマンドのコールフロー

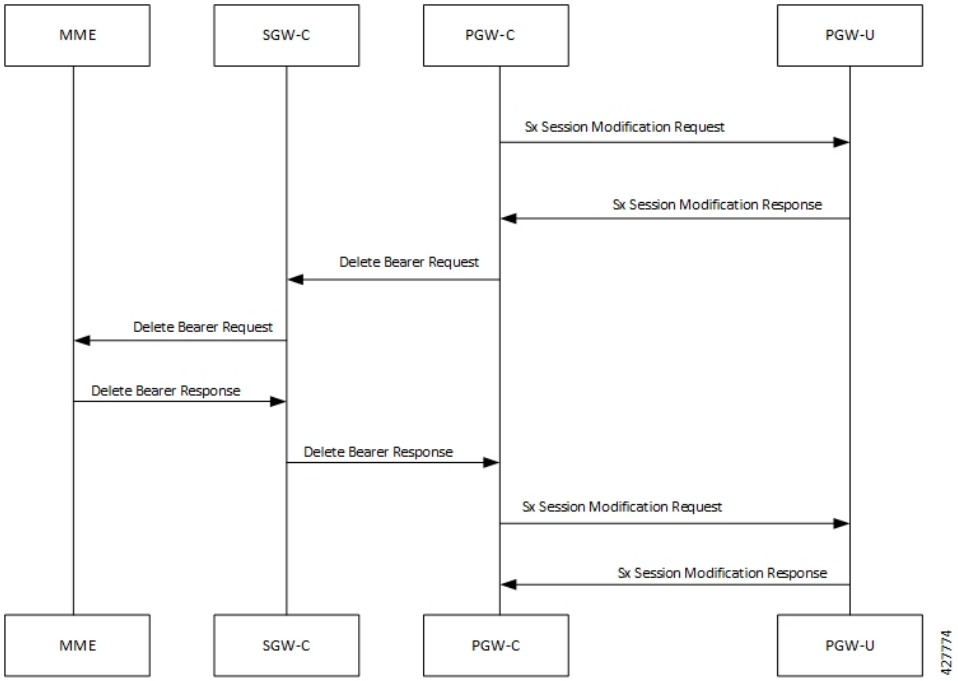
次のコールフローは、Pure P コールのコマンドコールフローの概要を示しています。



1. UE が最初の PDN を介して接続解除手順を開始します。SGW-C が、一連の専用ベアラーを削除するために、ベアラー削除コマンドを PGW-C に転送します。
2. PGW-C が、Apply Action を DROP にして専用ベアラーの All Update FAR で Sx 変更要求を送信します。
3. PGW-U が PGW-C に Sx セッション変更応答で応答します。
4. PGW-C がアクセス側にベアラー削除要求を送信し、ベアラー削除応答を受信すると、専用ベアラーの PDR と FAR を削除するために Sx 変更要求がトリガーされます。

Pure P コールのサブスクライバ EBI のクリア

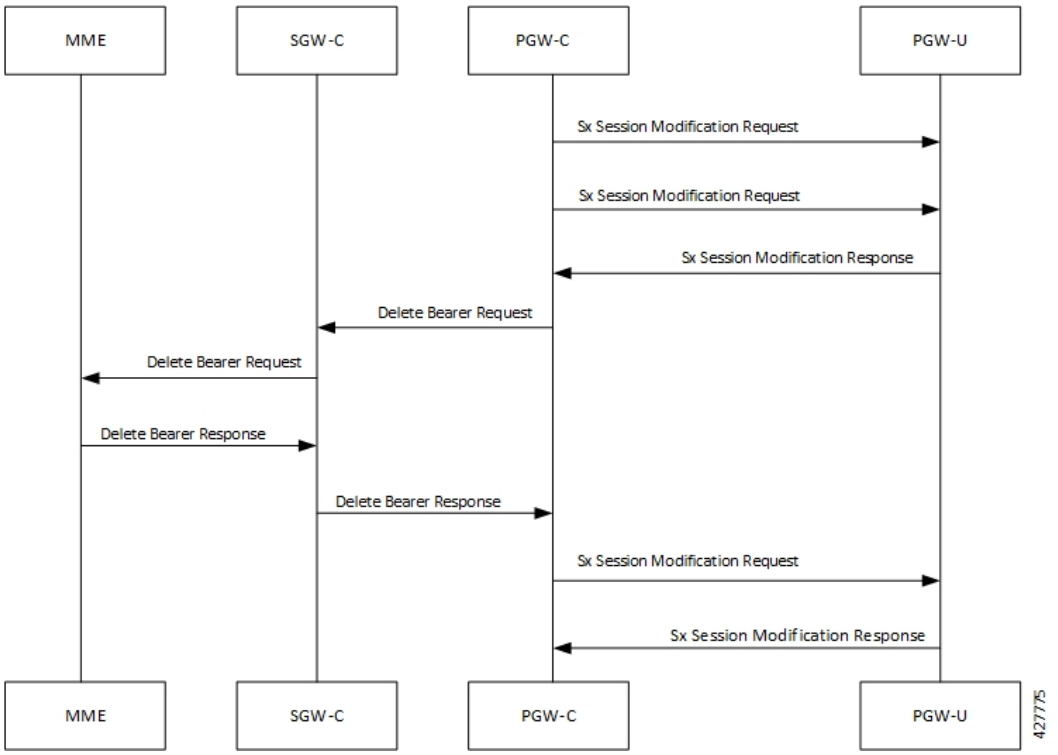
次のコールフローは、Pure P コールのサブスクライバ EBI クリアの概要を示しています



1. PGW-C が最初の PDN を介して接続解除手順を開始します。
2. PGW-C が、Apply Action を DROP にして専用ベアラーの All Update FAR で Sx 変更要求を送信します。
3. PGW-U が PGW-C に Sx セッション変更応答で応答します。
4. PGW-C がアクセス側にベアラー削除要求を送信し、ベアラー削除応答を受信すると、専用ベアラーの PDR と FAR を削除するために Sx 変更要求がトリガーされます。

Pure P コールの PCRF 開始削除

次のコールフローは、Pure P コールの PCRF 開始削除の概要を示しています。



1. PCRF が Rule-removal を実行し、これによって専用ベアラーが削除されます。
2. PGW-C が、Apply Action を DROP にして専用ベアラーの All Update FAR で Sx 変更要求を開始します。
3. PGW-U が PGW-C に Sx セッション変更応答で応答します。
4. PGW-C がアクセス側にベアラー削除要求を送信し、ベアラー削除応答を受信すると、専用ベアラーの PDR と FAR を削除するために Sx 変更要求がトリガーされます。

制限事項

専用ベアラーの作成と削除および変更（更新）には、次の制限があります。

- Pure S コールの専用ベアラーの作成はサポートされません。
- コリジョンシナリオでは、削除がすでに進行中のベアラーに対してイベント/操作が要求されると、セッションのクリーンアップがトリガーされます。たとえば、DELETE_BEARER_COMMAND（EBI＝6）の実行中に CCA-U/RAR（EBI＝6）が受信されます。

S-GW の専用ベアラーの追加、削除、および更新のサポート

機能説明

CUPS アーキテクチャでは、Pure-S コール向けの専用ベアラーの追加、削除、および更新がサポートされています。

この機能をサポートするため、次の機能が追加されています。

- SAEGW-CP は、Pure-S コール専用ベアラーのベアラー作成要求をサポートします。
- SAEGW-CP は、単一のベアラー作成要求で複数のベアラーコンテキストに対応できます。
- SAEGW-CP は、異なる PDN に対する複数のベアラー作成要求を並行してサポートします。これらの PDN は、Pure-S PDN または Collapsed と Pure-S の組み合わせです。
- SAEGW-UP は、ベアラーごとに Pure-S コールの VPP でアップリンク方向とダウンリンク方向のベアラーストリームを作成します。各方向ごとのストリーム数は、GTP-U サービスの IP アドレスによって異なります。
- SAEGW-CP は、専用ベアラーを使用したアクセスベアラー解放（RAB）要求をサポートしているため、すべてのベアラーに対応するすべての FAR が変更されます。
- SAEGW-CP は、専用ベアラーを使用したベアラー変更要求（アイドルモード、接続モード）をサポートします。
- SAEGW-CP は、MME からのベアラー作成応答の障害処理をサポートします。
- SAEGW-CP および SAEGW-UP は、VPP を使用したデフォルトおよび専用ベアラーの DSCP マーキングをサポートします。
- SAEGW-CP および SAEGW-UP は、専用ベアラーのベアラー削除要求をサポートします。SAEGW-UP は、それらのベアラーに属するベアラーストリームと TEP エントリを削除します。
- SAEGW-CP は、コールがアイドル状態の場合に Pure-S 専用ベアラーの作成をサポートします。
- SAEGW-CP は、Pure-S 専用ベアラーの S-GW 再配置（X2 ベースと S1 ベースの両方）をサポートします。
- SAEGW-CP は、Pure-S 専用ベアラーの更新シナリオをサポートします。
- SAEGW-CP は、セッション作成応答とともに Pure-S コール専用ベアラーのベアラー作成要求のピギーバックをサポートします。
- SAEGW-CP は、ベアラー変更要求とともに Pure-S コール専用ベアラーのベアラー作成応答のピギーバックをサポートします。
- P-GW が CCA-I の一部としてベアラー作成を受信し、P-GW がピギーバック要求を送信しない場合、SAEGW-CP は Pure-S 専用ベアラ—の作成をサポートします。この結果、セッション作成応答の後にベアラー作成要求が続きます。

- SAEGW-CP は、Pure-S 専用ベアラーを使用したセッションリカバリと ICSR をサポートします。
- SAEGW-CP は、ベアラー作成要求とベアラー削除要求（デフォルトのベアラー）のコリジョンをサポートします。
- SAEGW-CP は、ベアラー作成要求とセッション削除要求のコリジョンをサポートします。
- SAEGW-CP は、ベアラー作成応答とベアラー削除要求（デフォルトのベアラー）のコリジョンをサポートします。
- SAEGW-CP は、ベアラー作成応答とセッション削除要求のコリジョンをサポートします。
- SAEGW-CP は、Pure-S のデフォルトおよび専用ベアラーを使用した終了マーカーをサポートします。
- SAEGW-UP は、Pure-S のデフォルトおよび専用ベアラーを使用したセッションリカバリをサポートします。
- SAEGW-UP は、アイドル状態からアクティブ状態に遷移中の IPv4 から IPv6 へ、または IPv6 から IPv4 への IP トランスポートの動作、および S1U インターフェイスでのハンドオーバー手順をサポートします。接続時に S1U で選択されたトランスポートがサポートされます。たとえば、IPv4 eNodeB から IPv6 eNodeB への eNode ハンドオーバーが該当します。
- SAEGW-CP は、原因が Partially Accepted および Context Not Found の CBRsp をサポートします。
- SAEGW-CP は Pure-S コールのダウンリンク方向のデータ通知をサポートしているため、UE が Pure-S コールでアイドル状態に遷移すると、FAR アクションはバッファに設定されます。
- SAEGW-CP は、原因が PARTIALLY_ACCEPTED でコンテキストが見つからない場合のベアラー更新応答をサポートします。
- SAEGW-CP は、ユーザープレーンノードを含む他のピアノードからのエラー処理と障害処理をサポートします。

S-GW の再配置を伴う LTE ハンドオフのコールフロー

SAEGW 展開では、サブスクライバがアクティブモードかアイドルモードの場合、S-GW は「S-GW 再配置ハンドオフ作成セッション」要求を処理します。SAEGW 展開では、P-GW は「S-GW 再配置ハンドオフベアラー変更」要求を処理します。

アイドルモードの TAU の場合、OI が 1 に設定されていると、eNodeB FTEID は MME から送信される「セッション作成要求」で送信されません。

S-GW の変更を伴うトラッキングエリア更新手順の場合、コールフローは S-GW の変更を伴う X2 ベースのハンドオーバーと同じです。

X2 ベースのハンドオフを使用するアクティブサブスクライバの場合、OI が 1 に設定されていると、eNodeB FTEID は MME から送信される「セッション作成要求」に含まれています。

S1 ベースのハンドオーバーの場合、OI が 0 に設定されていると、MME からの「セッション作成要求」に eNodeB FTEID は含まれません。「セッション作成要求」の後に eNodeB FTEID を含む MME からの「ベアラー変更要求」が続きます。

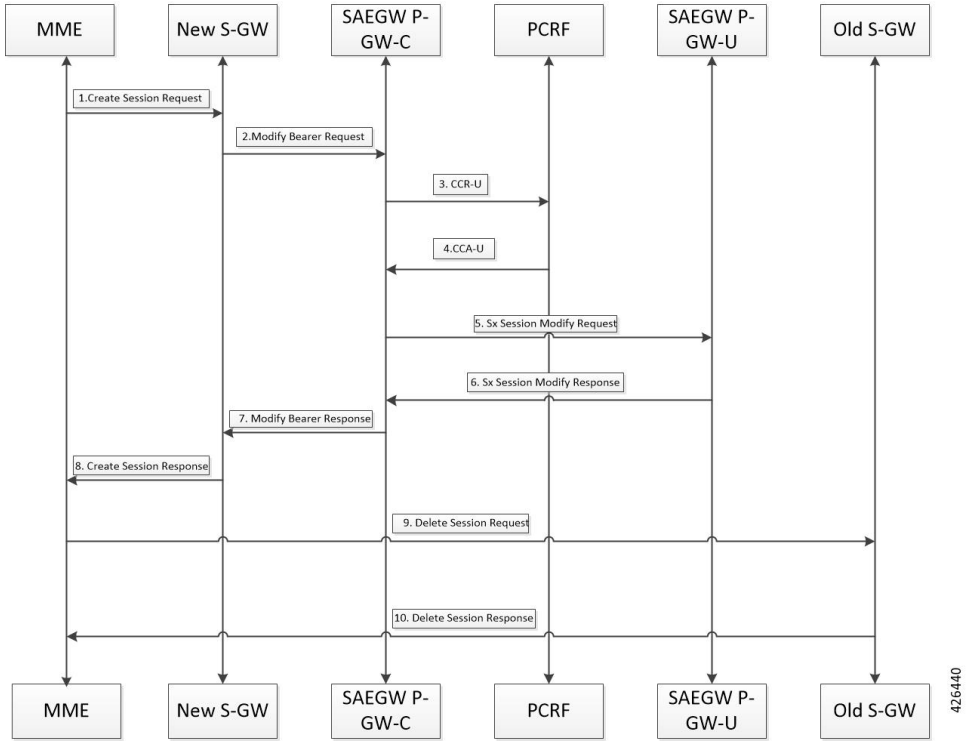
次のセクションでは、eNodeB FTEID がアクティブサブスクライバの「セッション作成要求」に含まれている、X2 および S1 ベースのハンドオーバーの S-GW 再配置コールフローを示します。

X2 ベースのハンドオーバーの S-GW 再配置コールフロー

このセクションでは、OI が 1 に設定されている場合における X2 ベースのハンドオーバーの S-GW 再配置コールフローについて説明します。

S-GW 再配置手順（*Pure-P*）

次のコールフローは、S-GW 再配置 Pure-P PDN の初期接続手順の概要を示しています。

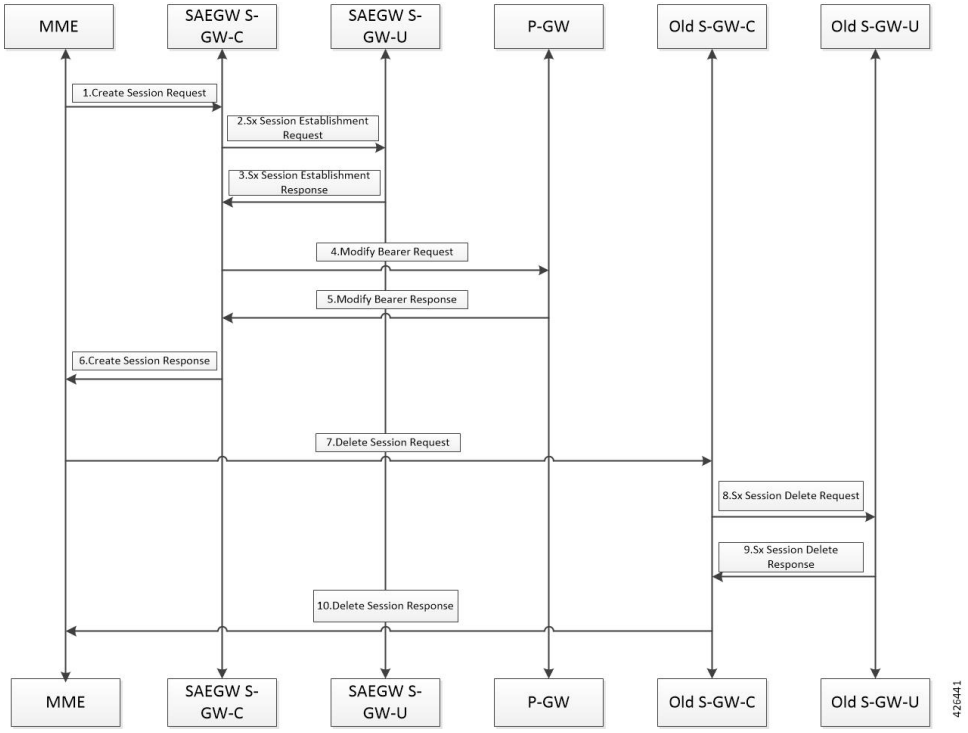


1. S-GW ハンドオーバーのときに、MME から新しい S-GW に「セッション作成要求」が送信されます。
2. 新しい S-GW から、S-GW S5/S8-U Data FTEID を使用して SAEGW-P-GW-C に「ベアラー変更要求」が送信されます。
3. SAEGW-PGW-C が Gx 通信（CCR-U）を実行します。
4. SAEGW-PGW-C が Gx 通信（CCA-U）を実行します。

5. Gx インタラクションの後、SAEGW-P-GW-C が SAEGW-PGW-U への「Sx 変更要求」をトリガーします。「Sx 変更要求」には次が含まれます。
   - S5/S8-U S-GW DATA FTEID の IP アドレス情報に基づいて設定された「Outer Header Removal」で「PDR（アップリンク UDR）を更新」します。
   - S5/S8-U S-GW DATA FTEID を使用して設定された「Outer Header Creation」で「FAR（ダウンリンク FAR）を更新」します。
6. SAEGW-P-GW-U が「Sx 変更応答」を送信します。
7. 「Sx 変更応答」を受信すると、SAEGW-P-GW-C が「ベアラー変更応答」を新しい S-GW に送信します。
8. その後、新しい S-GW が MME に「セッション作成応答」を送り返します。
9. MME が古い S-GW に「セッション削除要求」を送信します。
10. 古い S-GW が MME に「セッション削除応答」で応答します。

S-GW 再配置手順（*Pure-S*）

次のコールフローは、S-GW 再配置 Pure-S PDN の手順の概要を示しています。

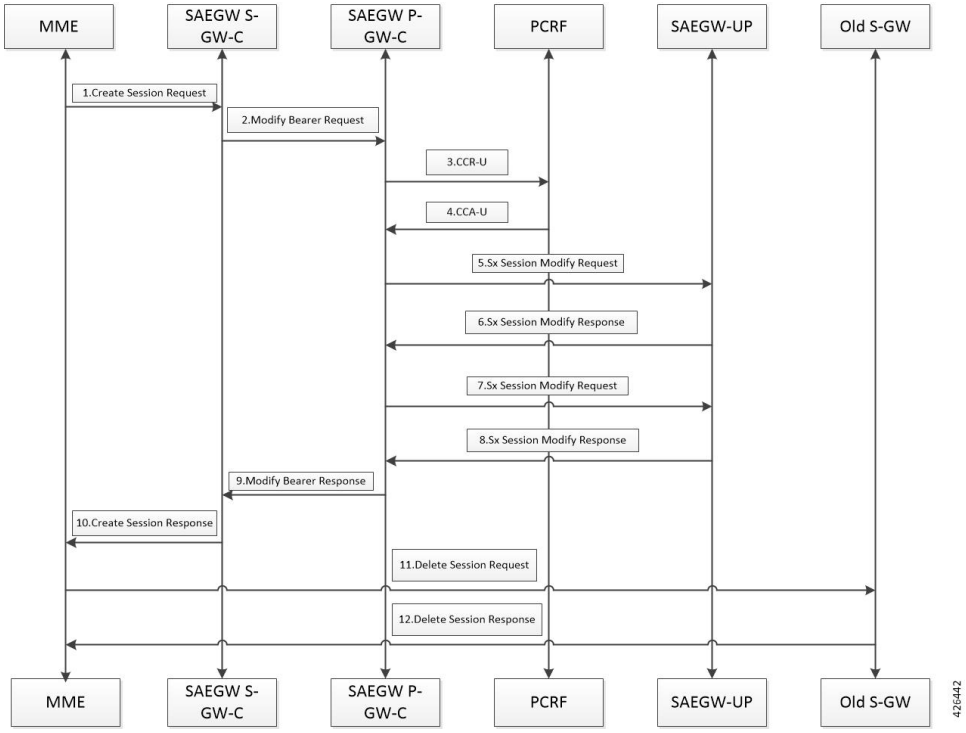


1. S-GW ハンドオーバーのときに、MME が enodeB FTEID、P-GW S5/S8-U DATA FTEID、P-GW S5/S8-C Ctrl FTEID を使用して「セッション作成要求」を新しい S-GW-C に送信します。

2. 新しい S-GW-C が新しい S-GW-U に「Sx 確立要求」を送信します。「Sx 確立要求」には次が含まれます。
   - eNodeB FTEID に基づいて設定された「Outer Header Removal」で「S-GW 入力 PDR を作成」します。
   - P-GW S5/S8-U Data FTEID に基づいて設定された「Outer Header Removal」で「S-GW 出力 PDR を作成」します。
   - P-GW S5/S8-U Data FTEID に設定された「Outer Header Creation」で「S-GW 入力 FAR を作成」します。
   - eNodeB FTEID に設定された「Outer Header Creation」で「S-GW 出力 FAR を作成」します。
   - X2 の eNodeB FTEID に設定された「Outer Header Creation」で「S-GW 出力 FAR を作成」します。TAU の場合、S-GW 出力 FAR に Outer Header Creation は含まれず、Apply Action は DROP に設定されます。
3. S-GW S1-U および S5/S8-U DATA FTEID とともに、S-GW-C で「Sx 確立応答」が受信されます。
4. S-GW-U から「Sx 確立応答」を受信すると、S-GW S5/S8-U DATA FTEID を使用して「ベアラー変更要求」が P-GW に送信されます。
5. P-GW が「ベアラー変更応答」で応答します。
6. 新しい S-GW-C が、S-GW ctrl S11C FTEID と S-GW S1-U DATA FTEID を使用して「セッション作成応答」を MME に送信します。
7. 「セッション作成応答」を受信すると、MME が古い S-GW-C に「セッション削除応答」を送信します。
8. 古い S-GW-C が古い S-GW-U に「Sx セッション削除要求」を送信します。
9. 古い S-GW-U が古い S-GW-C に「Sx セッション削除応答」で応答します。
10. 古い S-GW-C が MME に「セッション削除応答」で応答します。

Collapsed コールへの *S-GW* 再配置 *Pure-P* コール

次のコールフローは、Collapsed コールへの S-GW 再配置 Pure-P コールに関する手順の概要を示しています。



1. S-GW ハンドオーバーのときに、MME がそのサブスクライバの SAEGW アンカー P-GW コールの一部である新しい SAEGW-SGW-C に「セッション作成要求」を送信します。
2. SAEGW-S-GW-C で次の処理が実行されます。
   - S-GW-C は、Collapsed コールであることを検出すると Sx 通信を実行しません。
   - S-GW-C が、ゼロの S-GW S5/S8-U Data FTEID で P-GW-C への「ベアラー変更要求」をトリガーします。
3. SAEGW-P-GW-C が PCRF CCR-U を使用して Gx 通信を実行します。
4. SAEGW-P-GW-C が PCRF CCA-U を使用して Gx 通信を実行します。
5. Gx インタラクションが完了すると、SAEGW-P-GW-C が SAEGW-P-GW-U への「Sx 変更要求」をトリガーします。Sx 変更要求には次が含まれます。
   - S-GW 入力の「Create PDR」と「Create FAR」（Apply Action は DROP）。
   - S-GW 出力の「Create PDR」と「Create FAR」（Apply Action は DROP）。

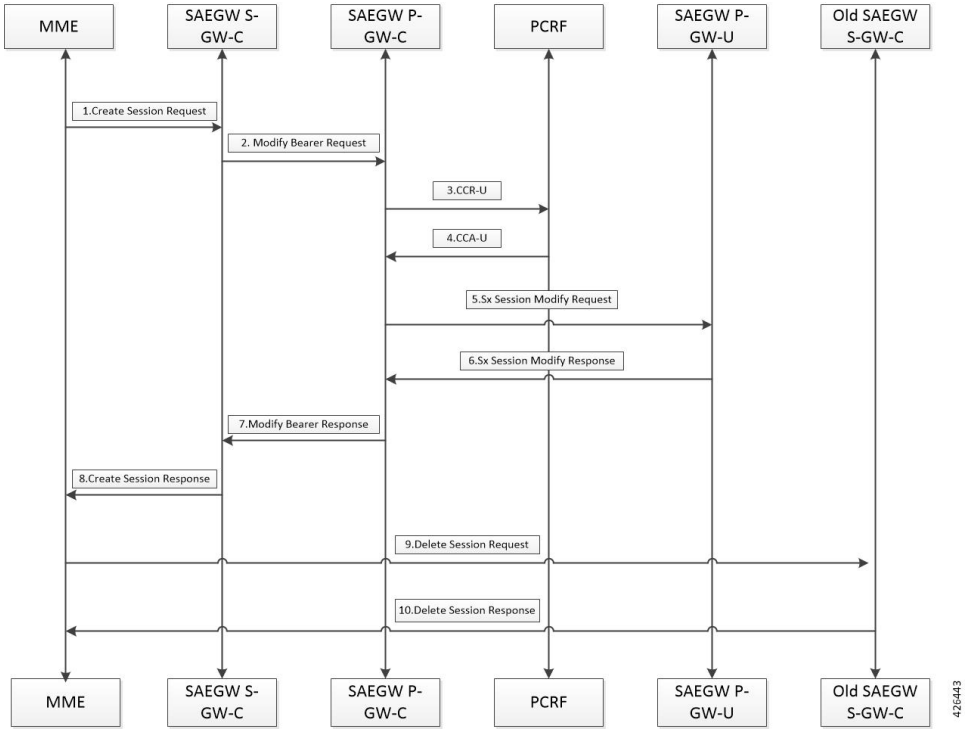
   コントロールプレーンが、アップリンクパスとダウンリンクパスの両方に次の S-GW DATA FTEIDS を割り当てるようにユーザープレーンに要求します。
   - S-GW S1-U DATA FTEID
   - S-GW S5/S8-U DATA FTEID

インターフェイスタイプが Sxb から Sxab に変更されます。つまり、Pure P コールから Collapsed コールになります。

6. SAEGW-P-GW-U が、Sxab インターフェイスを介して SAEGW-P-GW-C に「Sx 変更応答」で応答します。
7. SAEGW-P-GW-C が、SAEGW-P-GW-U への 2 番目の「Sx 変更要求」をトリガーします。「Sx 変更要求」には次が含まれます。
   - eNodeB S1-U DATA FTEID に基づいて設定された「Outer Header Removal」で S-GW 入力 PDR を更新します。
   - P-GW S5/S8-U DATA FTEID に基づいて設定された「Outer Header Removal」で S-GW 出力 PDR を更新します。
   - P-GW S5/S8-U DATA FTEID に設定された「Outer Header Creation」と Apply Action FORWARD で S-GW 入力 FAR を更新します。
   - eNodeB S1-U DATA FTEID に設定された「Outer Header Creation」と Apply Action FORWARD で S-GW 出力 FAR を更新します。TAU の場合、S-GW Egress FAR に「Outer Header Creation」は含まれず、Apply Action は DROP に設定されます。
   - S-GW S5/S8-U DATA FTEID に設定された「Outer Header Creation」と Apply Action FORWARD で P-GW 出力 FAR を更新します。
8. SAEGW-P-GW-U が SAEGW-P-GW-C に「Sx 変更応答」を送信します。
9. 「Sx 変更応答」を受信すると、SAEGW-PGW-C が「ベアラー変更応答」を SAEGW-S-GW-C に送信します。
10. SAEGW-S-GW-C が、S-GW ctrl S11c FTEID と S-GW S1-U DATA FTEID を使用して「セッション作成応答」を送信します。
11. MME が古い S-GW に「セッション削除要求」を送信します。
12. 古い S-GW が MME に「セッション削除応答」で応答します。

Pure-P コールへの *S-GW* 再配置 *Collapsed* コール

次のコールフローは、Pure-P コールへの S-GW 再配置 Collapsed コールに関する手順の概要を示しています。



1. S-GW ハンドオーバーのときに、MME が新しい S-GW に「セッション作成要求」を送信します。
2. 新しい S-GW が、S-GW S5/S8-U DATA FTEID を使用して SAEGW-P-GW-C に「ベアラー変更要求」を送信します。
3. SAEGW-P-GW-C が Gx 通信 CCR-U を実行します。
4. SAEGW-P-GW-C が Gx 通信 CCA-U を実行します。
5. Gx インタラクションの後、SAEGW-P-GW-C が SAEGW-P-GW-U に「Sx 変更要求」を送信します。
   - インターフェイスタイプが Sxab から Sxb に変更されます。つまり、Collapsed コールから Pure P コールになります。
   - 「S-GW 入力 PDR」および出力 PDR（Sxa タイプの PDR）を削除します。
   - アップリンクデータパスとダウンリンクデータパスに設定された「S-GW 入力 FAR」および出力 FAR を削除します。
   - S-GW S5/S8-U DATA FTEID に基づいて設定された「Outer Header Removal」で「P-GW 入力 PDR」を更新します。
   - S-GW S5/S8-U DATA FTEID に設定された「Outer Header Creation」で「P-GW 出力 FAR」を更新します。

（注） SAEGW/PGW-Cは、MMEからセッション削除要求（DSR）が送信されるまで、送信元SGW-UのSxaトンネルを保持します。このトンネル保持により、パスが切り替わるまでアップリンクデータがSGW-Uを介して流れるようになります。DSRでのSxaトンネル削除を有効または無効にするには、SAEGWサービス コンフィギュレーション モードで **sxa-tunnel-del-at-dsr-on-sgw-change** コマンドを使用します。詳細については、「Sxa トンネル削除の設定」セクションを参照してください。

6. SAEGW-P-GW-U が「Sx セッション変更応答」で応答します。
7. SAEGW-P-GW-C が新しい S-GW に「ベアラー変更応答」で応答します。
8. 新しい S-GW が MME に「セッション作成応答」で応答します。
9. 「セッション作成応答」を受信すると、MME が「セッション削除要求」を SAEGW-S-GW-C（旧 S-GW）に送信します。SAEGW-S-GW-C（旧 S-GW）は Sx 通信を実行しません。
10. SAEGW-S-GW-C（旧 S-GW）が MME に「セッション削除応答」で応答します。

Sxa トンネル削除の設定

Sxa トンネル削除を有効または無効にするには、次のコマンドを使用します。

```
configure
  context context_name
    saegw-service service_name
      [ no ] sxa-tunnel-del-at-dsr-on-sgw-change
      end
```

注：

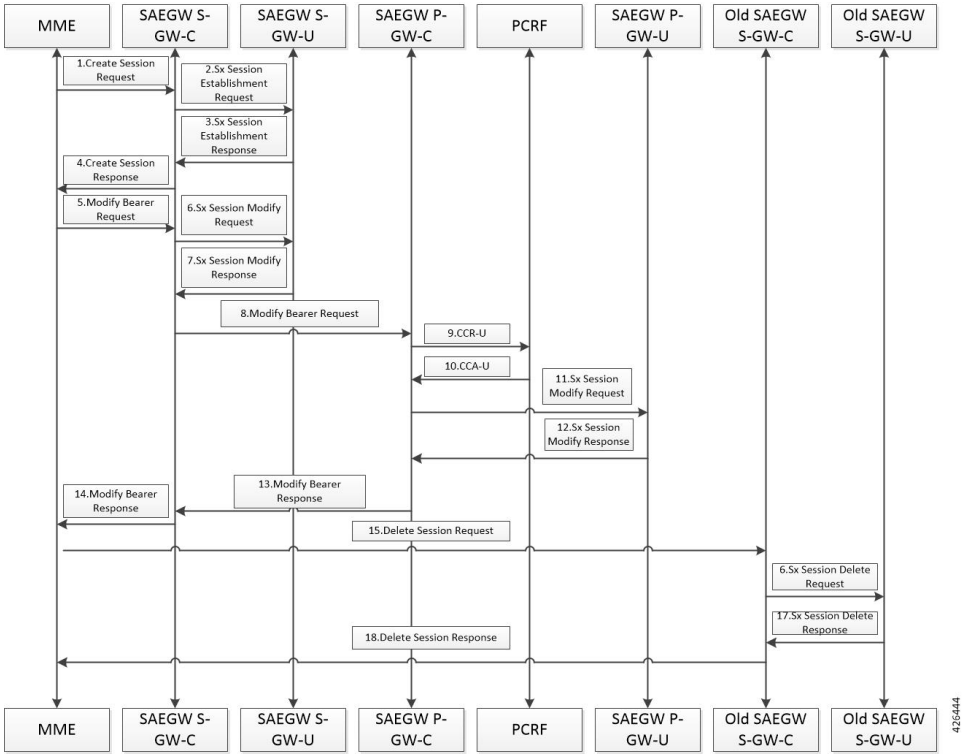
- **sxa-tunnel-del-at-dsr-on-sgw-change** ：SGW 再配置を伴う X2/S1 ベースのハンドオーバー中に DSR での Sxa トンネル削除を有効にします。
- **no sxa-tunnel-del-at-dsr-on-sgw-change** ：X2/S1 ベースのハンドオーバー中に DSR での Sxa トンネル削除を無効にします。
- デフォルトでは、この設定は無効になっています。
- この設定は、現在のセッションと新しいセッションのすべてに適用されます。

S1 ベースのハンドオーバーの S-GW 再配置コールフロー

このセクションでは、OI が 1 に設定されている場合における S1 ベースのハンドオーバーの S-GW 再配置コールフローについて説明します。

Pure-P および *Pure-S* コールフロー

次のコールフローは、OI が 0 に設定された S-GW 再配置 Pure-P および Pure-S PDN の手順の概要を示しています。



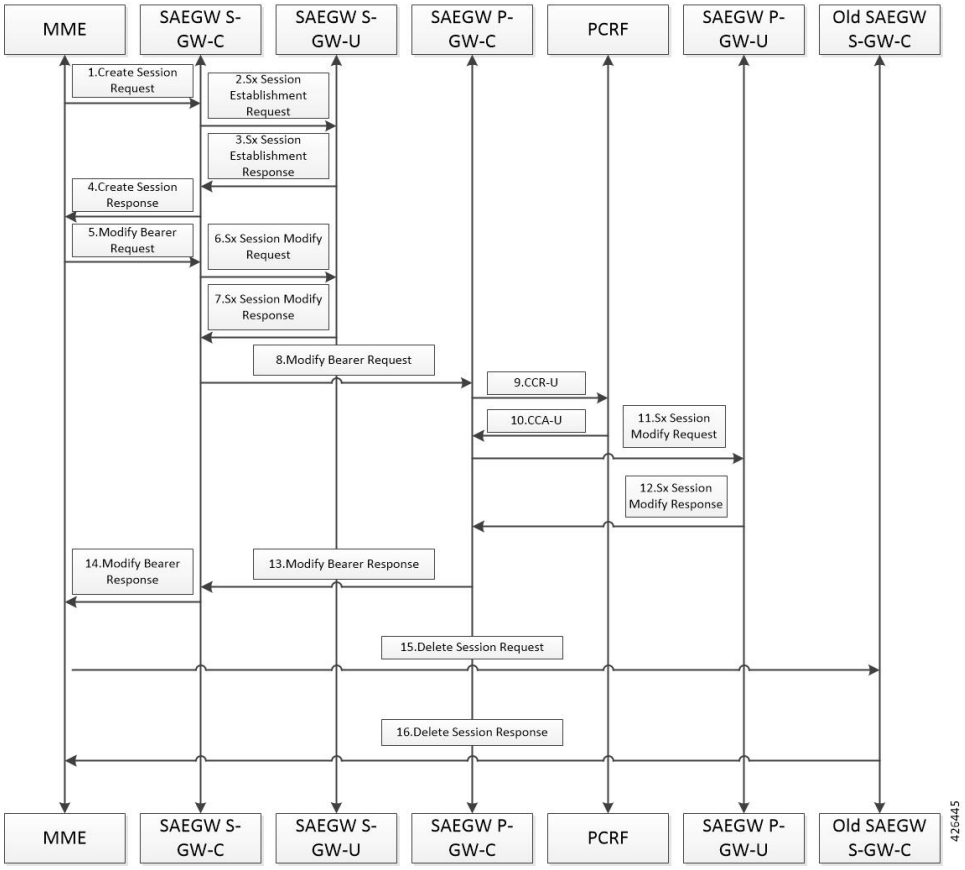
1. S-GW の変更を伴う S1 ベースのハンドオーバーのときに、MME が P-GW S5/S8-U DATA FTEID と P-GW S5/S8-C Ctrl FTEID を使用して「セッション作成要求」を新しい S-GW-C に送信します。
2. 新しい S-GW-C が新しい S-GW-U に「Sx 確立要求」を送信します。「Sx 確立要求」には次が含まれます。
   - 「S-GW 入力 PDR を作成」します。
   - P-GW S5/S8-U Data FTEID に基づいて設定された「Outer Header Removal」で「S-GW 出力 PDR を作成」します。
   - P-GW S5/S8-U Data FTEID に設定された「Outer Header Creation」で「S-GW 入力 FAR を作成」します。
   - Apply Action が DROP に設定された「Create S-GW Egress FAR」。
3. ユーザープレーンで割り当てられた S-GW S1-U および S5/S8-U DATA FTEID とともに、S-GW-C で「Sx 確立応答」が受信されます。
4. S-GW-U から「Sx 確立応答」を受信すると、S-GW-C が MME に「セッション作成応答」を送信します。
5. S-GW-C から「セッション作成応答」を受信すると、MME が eNodeB FTEID を使用して「ベアラー変更要求」を S-GW-C に送信します。
6. S-GW-C が S-GW-U に「Sx 変更要求」を送信します。

- eNodeB FTEID に基づいて設定された「Outer Header Removal」で「S-GW 入力 PDR」を更新します。
- eNodeB FTEID に基づいて設定された「Outer Header Creation」で「S-GW 出力 FAR」を更新します。

7. S-GW-U が S-GW-C に「Sx 変更応答」を送信します。
8. S-GW-C が、S-GW S5/S8-U DATA FTEID を使用して「ベアラー変更要求」を P-GW-C に送信します。
9. S-GW-C から「ベアラー変更要求」を受信すると、P-GW-C が PCRF CCR-U との Gx 通信を実行します。
10. S-GW-C から「ベアラー変更要求」を受信すると、P-GW-C が PCRF CCA-U との Gx 通信を実行します。
11. Gx インタラクションの後、P-GW-C が「Sx 変更要求」を P-GW-U に送信します。「Sx 変更要求」には次が含まれます。
    - S-GW S5/S8U DATA FTEID に基づく「Outer Header Removal」で P-GW 入力 PDR を更新します。
    - S-GW S5/S8U DATA FTEID に基づく「Outer Header Creation」で P-GW 出力 FAR を更新します。
12. P-GW-U が P-GW-C に「Sx 変更応答」を送り返します。
13. P-GW-C が S-GW-C に「ベアラー変更応答」を送信します。
14. P-GW が「ベアラー変更応答」で応答すると、SGW-C が S-GW ctrl S11C FTEID と S-GW S1-U DATA FTEID を使用して「ベアラー変更応答」を MME に送信します。
15. 「ベアラー変更応答」を受信すると、MME が古い S-GW-C に「セッション削除要求」を送信します。
16. 古い S-GW-C が古い S-GW-U に「Sx セッション削除要求」を送信します。
17. 古い S-GW-U が古い S-GW-C に「Sx セッション削除応答」で応答します。
18. 古い S-GW-C が MME に「セッション削除応答」で応答します。

Pure-P コールへの *S-GW* 再配置 *Collapsed* コール

次のコールフローは、Pure-P コールへの S-GW 再配置 Collapsed コールに関する手順の概要を示しています。



1. S-GW の変更を伴う S1 ベースのハンドオーバーのときに、MME が P-GW S5/S8-U DATA FTEID と P-GW S5/S8-C Ctrl FTEID を使用して「セッション作成要求」を新しい S-GW-C に送信します。
2. 新しい S-GW-C が新しい S-GW-U に「Sx 確立要求」を送信します。「Sx 確立要求」には次が含まれます。
   - 「S-GW 入力 PDR を作成」します。
   - P-GW S5/S8-U Data FTEID に基づいて設定された「Outer Header Removal」で「S-GW 出力 PDR を作成」します。
   - P-GW S5/S8-U Data FTEID に設定された「Outer Header Creation」で「S-GW 入力 FAR を作成」します。
   - Apply Action DROP で「S-GW 出力 FAR を作成」します。
3. UP で割り当てられた S-GW S1-U および S5/S8-U DATA FTEID とともに、S-GW-C で「Sx 確立応答」が受信されます。
4. S-GW-U から「Sx 確立応答」を受信すると、S-GW-C が MME に「セッション作成応答」を送信します。

5. S-GW-C から「セッション作成応答」を受信すると、MME が eNodeB FTEID を使用して「ベアラー変更要求」を S-GW-C に送信します。
6. S-GW-C が「Sx 変更要求」を S-GW-U に送信します。「Sx 変更要求」には次が含まれます。
   - eNodeB FTEID に基づく「Outer Header Removal」で「S-GW 入力 PDR を更新」します。
   - eNodeB FTEID に基づく「Outer Header Creation」で「S-GW 出力 FAR を更新」します。
7. S-GW-U が S-GW-C に「Sx 変更応答」を送信します。
8. S-GW-C が、S-GW S5/S8-U DATA FTEID を使用して「ベアラー変更要求」を P-GW-C に送信します。
9. S-GW-C から「ベアラー変更要求」を受信すると、P-GW-C が PCRF CCR-U との Gx 通信を実行します。
10. S-GW-C から「ベアラー変更要求」を受信すると、P-GW-C が PCRF CCA-U との Gx 通信を実行します。
11. Gx インタラクションの後、P-GW-C が「Sx 変更要求」を P-GW-U に送信します。「Sx 変更要求」には次が含まれます。
    - インターフェイスタイプが Sxab から Sxb に変更されます。つまり、Collapsed コールから Pure P コールになります。
    - 「S-GW 入力」および「出力 PDR を削除」します。
    - 「S-GW 入力」および「出力 FAR を削除」します。
    - S-GW S5/S8U DATA FTEID に基づく「Outer Header Removal」で「P-GW 入力 PDR を更新」します。
    - S-GW S5/S8U DATA FTEID に基づく「Outer Header Creation」で「P-GW 出力 FAR を更新」します。



（注） SAEGW/PGW-Cは、MMEからセッション削除要求（DSR）が送信されるまで、送信元SGW-UのSxaトンネルを保持します。このトンネル保持により、パスが切り替わるまでアップリンクデータがSGW-U を介して流れるようになります。DSR でのSxaトンネル削除を有効または無効にするには、SAEGW サービス コンフィギュレーション モードで **sxa-tunnel-del-at-dsr-on-sgw-change** コマンドを使用します。詳細については、「Sxa トンネル削除の設定」セクションを参照してください。

12. P-GW-U が P-GW-C に「Sx 変更応答」を送り返します。
13. P-GW-C が S-GW-C に「ベアラー変更応答」を送信します。

14. P-GW が「ベアラー変更応答」で応答すると、S-GW-C が S-GW ctrl S11C FTEID と S-GW S1-U DATA FTEIDを使用して「ベアラー変更応答」を MME に送信します。
15. 「ベアラー変更応答」を受信すると、MME が古い S-GW-C に「セッション削除要求」を送信します。古い S-GW-C は Sx 通信を実行しません。
16. 古い S-GW-C が MME に「セッション削除応答」で応答します。

Sxa トンネル削除の設定

Sxa トンネル削除を有効または無効にするには、次のコマンドを使用します。

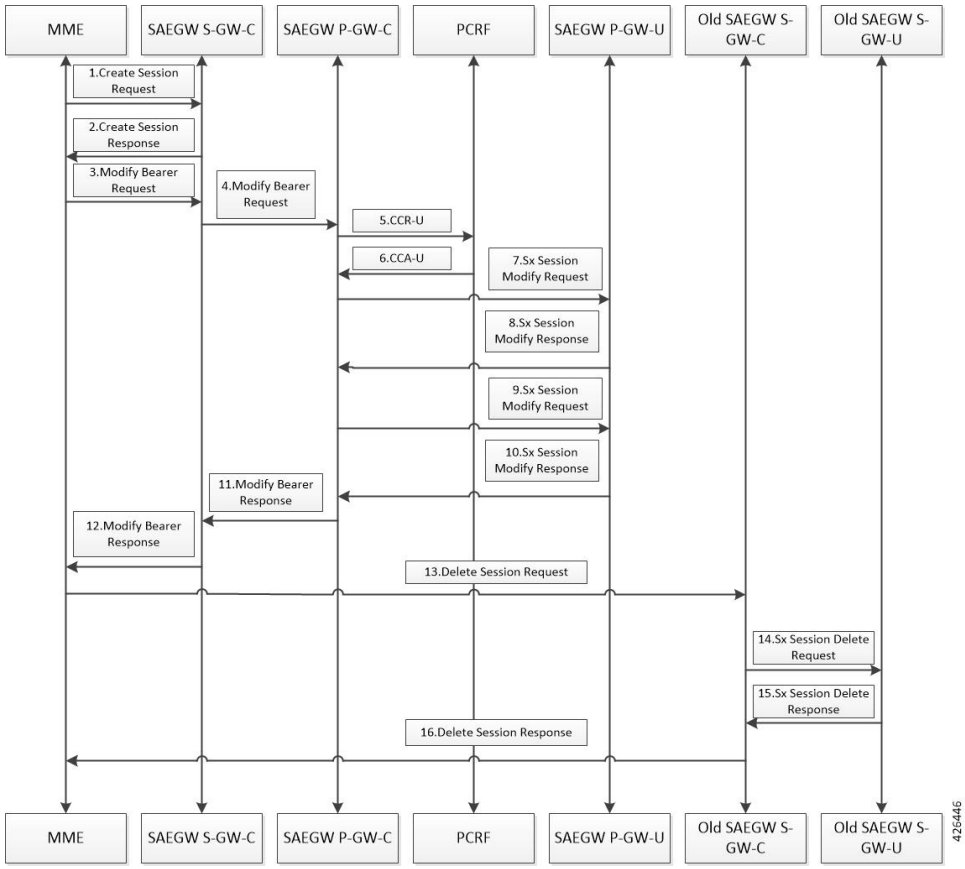
```
configure
  context context_name
    saegw-service service_name
      [ no ] sxa-tunnel-del-at-dsr-on-sgw-change
      end
```

注：

- **sxa-tunnel-del-at-dsr-on-sgw-change** ：SGW 再配置を伴う X2/S1 ベースのハンドオーバー中に DSR での Sxa トンネル削除を有効にします。
- **no sxa-tunnel-del-at-dsr-on-sgw-change** ：X2/S1 ベースのハンドオーバー中に DSR での Sxa トンネル削除を無効にします。
- デフォルトでは、この設定は無効になっています。
- この設定は、現在のセッションと新しいセッションのすべてに適用されます。

Collapsed コールへの *S-GW* 再配置 *Pure-P* コール

次のコールフローは、Collapsed コールへの S-GW 再配置 Pure-P コールに関する手順の概要を示しています。



1. S-GW ハンドオーバーのときに、MME がそのサブスクライバの SAEGW アンカー P-GW コールの一部である新しい SAEGW-S-GW-C に「セッション作成要求」を送信します。SGW-C は、Collapsed コールであることを検出すると Sx 通信を実行しません。
2. SGW-C が MME に「セッション作成応答」を送り返します。
3. 「セッション作成応答」を受信すると、MME が eNodeB FTEID を使用して「ベアラー変更要求」を S-GW-C に送信します。
4. S-GW-C が、ゼロの S-GW S5/S8-U Data FTEID で P-GW-C への「ベアラー変更要求」をトリガーします。Collapsed コールの「ベアラー変更要求」でゼロの S5/S8-U SGW DATA FTEID を許可します。
5. PCRF CCR-U との Gx 通信を実行します。
6. PCRF CCA-U との Gx 通信を実行します。
7. Gx インタラクションが完了すると、SAEGW-P-GW-C が SAEGW-P-GW-U への「Sx 変更要求」をトリガーします。 Sx 変更要求には次が含まれます。
   - （Apply Action DROP で）S-GW 入力の「PDR と FAR を作成」します。
   - （Apply Action DROP で）S-GW 出力の「PDR と FAR を作成」します。

コントロールプレーンが、アップリンクパスとダウンリンクパスの両方に次の S-GW DATA FTEIDS を割り当てるようにユーザープレーンに要求します。

- S-GW S1-U DATA FTEID
- S-GW S5/S8-U DATA FTEID

インターフェイスタイプが Sxb から Sxab に変更されます。つまり、Pure P コールから Collapsed コールになります。

8. SAEGW-P-GW-U が、Sxab インターフェイスを介して SAEGW-PGW-C に「Sx 変更応答」で応答します。
9. SAEGW-P-GW-C が、SAEGW-P-GW-U への 2 番目の「Sx 変更要求」をトリガーします。「Sx 変更要求」には次が含まれます。
   - eNodeB S1-U DATA FTEID に基づいて設定された「Outer Header Removal」で「S-GW 入力 PDR を更新」します。
   - P-GW S5/S8-U DATA FTEID に基づいて設定された「Outer Header Removal」で「S-GW 出力 PDR」を更新します。
   - P-GW S5/S8-U DATA FTEID に設定された「Outer Header Creation」と Apply Action FORWARD で「S-GW 入力 FAR を更新」します。
   - eNodeB S1-U DATA FTEID に設定された「Outer Header Creation」と Apply Action FORWARD で「S-GW 出力 FAR を更新」します。
   - S-GW S5/S8-U DATA FTEID に基づく「Outer Header Removal」で「P-GW 入力 PDR を更新」します。
   - S-GW S5/S8-U DATA FTEID に設定された「Outer Header Creation」と Apply Action FORWARD で「P-GW 出力 FAR を更新」します。
   - S-GW S5/S8-UDATA FTEID に基づいて設定された「Outer Header Removal」で「P-GW 入力 PDR」を更新します。
10. SAEGW-P-GW-U が SAEGW-P-GW-C に「Sx 変更応答」を送信します。
11. 「Sx 変更応答」を受信すると、SAEGW-PGW-C が「ベアラー変更応答」を SAEGW-SGW-C に送信します。
12. SAEGW-S-GW-C が、S-GW ctrl S11c FTEID と S-GW S1-U DATA FTEID を使用して「ベアラー変更応答」を送信します。
13. 「ベアラー変更応答」を受信すると、MME が古い SGW-C に「セッション削除要求」を送信します。
14. 古い SGW-C が古い SGW-U に「Sx セッション削除要求」を送信します。
15. 古い SGW-U が古い SGW-C に「Sx セッション削除応答」で応答します。
16. 古い SGW-C が MME に「セッション削除応答」で応答します。

PDN 更新手順

このセクションでは、CUPS アーキテクチャでサポートされている次の PDN 更新手順について説明します。

- UE 開始手順
  - ベアラー変更コマンド
  - Modify Bearer 要求
- ネットワーク開始手順
  - RAR
  - CCA-U（UE 開始手順または任意の内部トリガーの一部としてトリガーされる）

上記のシナリオは、SAEGW Pure-P と SAEGW Collapsed 両方のコールタイプでサポートされます。

次のような発生する可能性があるすべてのネットワーク障害のシナリオもサポートされます。

- Sx 障害（Sx 変更応答）
- GTP 障害（ベアラー更新応答）
- Gx 障害
- ベアラー作成応答障害

障害処理とコールドロップのシナリオ

次の表に、発生する可能性があるさまざまな Sx/GTP 障害シナリオと、その結果として生じる P-GW の動作を示します。また、コントロールプレーンとユーザープレーン間の不一致を回避するために P-GW がコール終了を開始する条件も示します。

Sx 変更障害のシナリオ	P-GW の動作
Sx 変更要求が伝送されている - URR をクエリ **注**：Sx 変更では、URR クエリとともに追加の IE が伝送される場合とされない場合があります（復元シナリオを除く）。 - ダイナミックルール追加（PDR/FAR/URR/QER を作成） - ルール追加を事前定義（PDR/URR を作成） - ルール更新（PDR/FAR/URR/QER を更新） - ダイナミックルール削除（PDR/QER を削除） - ダイナミックルール削除を事前定義（PDR を削除） - APN-AMBR QER 変更 - DSCP 変更（QoS 変更）	コールドロップ： あり **切断理由**：sxfail-opr-get-usagereport
a）Sx 変更要求が伝送されている - URR をクエリ b）Sx 変更応答が受信されている 原因：障害 + 使用状況情報	使用状況情報は処理されません。

Sx 変更障害のシナリオ	P-GW の動作
a）Sx 変更要求が伝送されている 1）ダイナミックルール追加（PDR/FAR/URR/QER を作成） 2）ルール追加を事前定義（PDR/URR を作成） 3）ルール更新（PDR/FAR/URR/QER を更新） 4）ダイナミックルール削除（PDR/QER を削除） 5）ダイナミックルール削除を事前定義（PDR を削除） 6）APN-AMBR QER 変更 7）DSCP 変更（QoS 変更） 8）URR をクエリ b）Sx 変更応答が受信されている 原因：障害	コントロールプレーンが別の「Sx 変更要求」を送信 1）アクションなし（CP と UP は同期） 2）アクションなし（CP と UP は同期） 3）CP と UP が同期されるようにルールを削除（「PDR/FAR/URR/QER」を削除） 4）コールドロップ（条件付き） a）PDR/URR を削除：コールドロップ b）QER/FAR を削除：コール保持、エラーログ 5）コールドロップ（条件付き） a）PDR を削除：コールドロップ b）QER を削除：コール保持、エラーログ 6）APN-AMBR QER 変更：アクションなし（CP と UP は同期） 7）DSCP 変更（QoS 変更）：アクションなし（CP と UP は同期） 8）コールドロップ **注**：現時点では、CP はルール削除イベントの一部として「Remove URR と Remove FAR」を送信しません。 **接続解除理由（優先順位順）**： sxfail-opr-get-usagereport sxfail-opr-create-rulebase-pdr sxfail-opr-remove-pdr

Sx 変更障害のシナリオ	P-GW の動作
a）Sx 変更要求が伝送されている 1）ダイナミックルール追加（PDR/FAR/URR/QER を作成） 2）ルール追加を事前定義（PDR/URR を作成） 3）ルール更新（PDR/FAR/URR/QER を更新） 4）ダイナミックルール削除（PDR/QER を削除） 5）ダイナミックルール削除を事前定義（PDR を削除） 6）APN-AMBR QER 変更 7）DSCP 変更（QoS 変更） 8）URR をクエリ b）「原因：成功」で Sx 変更応答が受信された後に次が続く c）ベアラー更新要求 d）ベアラー更新応答（原因 = 失敗）	コントロールプレーンは、別の「Sx 変更要求」を送信して古い状態に戻ります。 1）CP と UP が同期されるようにルールを削除（「PDR/FAR/URR/QER」を削除） 2）CP と UP が同期されるようにルールを削除（「PDR/QER」を削除） 3）CP と UP が同期されるようにルールを削除（「PDR/FAR/URR/QER」を削除） 4）アクションなし（CP と UP は同期） 5）アクションなし（CP と UP は同期） 6）CP と UP が同期されるように保持されている（古い）APN-AMBR を送信 7）CP と UP が同期されるように保持されている（古い QoS）DSCP を送信 8）アクションなし **注**：現時点では、CP はルール削除イベントの一部として「Remove URR と Remove FAR」を送信しません。
a）Sx 変更要求がベアラー更新応答の一部として開始された場合（障害）：CP と UP の同期を維持するため 1）PDR/FAR/URR/QER を削除 2）PDR/QER（ルールの事前定義）を削除 3）保持されている（古い）APN-AMBR QER 4）保持されている（古い）DSCP 5）URR をクエリ b）「原因：失敗」で Sx 変更応答が受信される	1）コールドロップ a）PDR/**URR** を削除：コールドロップ b）QER/**FAR** を削除：コール保持、エラーログ 2）コールドロップ（条件付き） a）PDR を削除：コールドロップ b）QER を削除：コール保持、エラーログ 3）コールドロップ 4）コールドロップ 5）URR クエリ：コールドロップ **接続解除の理由**：sxfail-opr-revert-info
Sx 変更要求が送信され、次の理由で失敗した場合： - Sx 変更応答（コンテキストが見つからない） - Sx 変更応答なし（Sx 再送信タイムアウト）	コールドロップ： あり **接続解除の理由**：sx-cntxt-not-found sx-no-response

シナリオ	コールドロップ
コンテキストが見つからない（GTP/Sx）	はい
再送信タイムアウト（GTP/Sx）	はい
GTP の原因：一時的な障害 Temp Failure CLI が設定されていない	なし：Sx Mod（古い APN-AMBR/デフォルト QoS 値に戻る、またはルールを削除）
GTP の原因：一時的な障害（再試行回数が上限に達した） Temp Failure CLI が設定されている	なし：Sx Mod（古い APN-AMBR/デフォルト QoS 値に戻る、またはルールを削除）
MBC -> UBReq -> UBRsp（使用可能なリソースなし）	コールドロップ動作は、非 cups とインラインである必要がある
MBR/RAR -> UBReq -> UBRsp（使用可能なリソースなし）	なし：Sx Mod（古い APN-AMBR/デフォルト QoS 値に戻る、またはルールを削除）
その他の原因（GTP/Sx）	なし：Sx Mod（古い APN-AMBR/デフォルト QoS 値に戻る、またはルールを削除）

PDN 更新手順：eNodeB F-TEIDu

機能説明

CUPS アーキテクチャの一部として、S-GW または SAE-GW の eNodeB を解放するための eNodeB F-TEIDu 更新またはアクセスベアラー解放（RAB）要求に対して Sx 変更要求を開始する手順が導入されています。

機能の仕組み

PDN の更新手順には、eNodeB F-TEIDu 更新/リリースに関する次のイベントが含まれます。

- eNodeB F-TEIDu 更新の場合

  1. SGW-C は、MME から eNodeB F-TEIDu 更新のベアラー変更要求を受信すると、SGW-U への Sx セッション変更要求を開始します。
  2. eNodeB F-TEIDu 更新の Sx 変更要求には、Apply Action が「Forward」の Update FAR と、Update Forwarding Parameters IE の一部である Outer Header Creation の更新された eNodeB IPv4/IPv6 アドレスが含まれています。

- eNodeB F-TEIDu リリースの場合

  1. SGW-Cは、MME から RAB 要求を受信すると、SGW-U への Sx 変更要求を開始します。

2. RAB は UE レベルのメッセージです。UE に複数の PDN 接続がある場合、Sx 変更要求は各 PDN 接続に個別に送信されます。
3. SGW-C は、宛先インターフェイスを ACCESS として、Update FAR を使用して Sx セッションの SGW-U への Sx セッション変更要求を開始します。Update FAR には、FAR ID と Apply Action「Drop」が含まれます。宛先インターフェイスが CORE の FAR は更新されません。

標準準拠

PDN 更新手順は、次の標準規格に準拠しています。

- 3GPP TS 23.401：「General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access」。
- 3GPP TS 29.274：「3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3」。
- 3GPP TS 29.244：「Interface between the Control Plane and the User Plane of EPC」。
- 3GPP TS 23.214：「Architecture enhancements for control and user plane separation of EPC nodes; Stage 2」。
- 3GPP TS 23.714：「Study on control and user plane separation of EPC nodes」。

Gx 更新手順

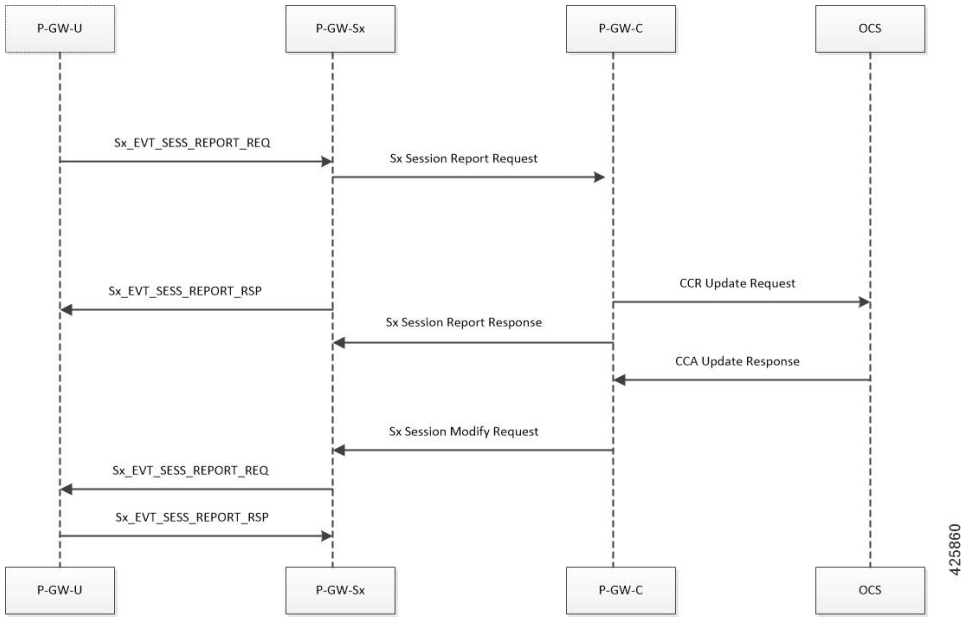
次に、Gx 更新手順の動作を示します。

- FAR 属性が同じ場合、共通の FAR が PDR に使用されます。
- フローステータス/評価グループ（のみ）の更新の場合、Update QER/URR が送信されます。つまり、このような場合は Update PDR は送信されません。
- ルールをインストールすると Create PDR と Create QER（SDF レベル）がトリガーされ、Create FAR と Create URR が含まれる場合もあれば、含まれない場合もあります（ルールでは他のルールの FAR と URR を再利用できます）。
- フローステータス/評価グループのルールを変更すると Update QER/Update URR がトリガーされ、Update PDR が含まれる場合もあれば、含まれない場合もあります（つまり、TFT/QoS の変更はありません）。
- TFT/QoS のルールを変更すると Update PDR がトリガーされ、Update QER/Update URR が含まれる場合もあれば、含まれない場合もあります（QER/URR の変更はありません）。
- ルール削除は、Sx 変更の一部としての Update QER、Update URR、Update FAR、または Update PDR が失敗した場合にトリガーされます。
- （ルールベースの）Remove PDR と Create PDR が失敗するとコールドロップが開始されます。

- PCRF から受信した APN-AMBR 変更によって Update QER がトリガーされます。
- 新しい QoS に対応する DSCP マーキングに変更がある場合、PCRF から受信した default-eps-bearer-qos の変更によって Update FAR がトリガーされます。

Gy インターフェイスを使用した P-GW セッションレポート

ここでは、Gyインターフェイスを使用したP-GWセッションのレポートについて説明します。



セッションセットアップ中の URR の作成

- コントロールプレーン機能は、Sx セッション確立要求で URR のリストと、対応する PDR での参照先を送信します。
- CCR/CCA-I メッセージ交換は、Sx セッション確立要求が CP によって生成され、ダイナミックルールとプリエンプティブ MSCC のクォータが OCS から受信されるまでに行われます。

セッション変更中/セッション中の URR の作成

- セッション中に PCRF からルール変更/インストールが行われると、PDR と URR をプロビジョニングするために Sx セッション変更要求が使用されます。セッション中に URR を作成するときにクォータ情報が OCS に存在しない場合は、「Start-of-Packet」トリガーが測定方法（時間とボリューム）とともに設定されます。
- 最初のパケットが到着すると、パケット検出のために「Start-of-Packet」トリガーがコントロールプレーンに送信され、コントロールプレーンは OCS サーバーとのクォータネゴシエーションを開始します。

セッション切断時の URR の処理

- P-GW ユーザープレーンは、Sx セッション削除応答の一部として URR 情報を送信します。
- P-GW コントロールプレーンは、これらの URR を対応する MSCC バケットにマッピングし、既存のフレームワークを使用して Gy/Ro インターフェイスで Credit-Control-Message を送信します。

セッション削除応答

- P-GW ユーザープレーンは、Sx 削除応答の一部として URR 情報を送信します。
- PGW コントロールプレーンは、これらの URR を対応する MSCC バケットにマッピングし、既存のフレームワークを使用して Gy/Ro インターフェイスで Credit-Control-Message を送信します。

Sx セッションレポート要求処理

P-GW ユーザープレーンは、ボリューム、時間クォータ、しきい値、有効時間、クォータホールド時間などのトリガーの使用状況レポートを送信します。P-GW コントロールプレーンは、対応する課金バケット（MSCC）に URR をマッピングし、各 MSCC の Credit-Control-Request Update を開始します。

Gy の URR レポート処理

URR レポートでは、P-GW ユーザープレーンによって送信されるトリガーに応じて、Credit-Control-Request-Update が生成されます。

- ユーザープレーンがトリガーの URR を報告すると、最初にコントロールプレーンの MSCC バケットにマッピングされます。値は MSCC データ構造で更新されます。
- 現在のレポートで URR バケットが処理されると、コントロールプレーンは更新中の MSCC バケットを分析し、すべての MSCC バケットを含む Credit-Control-Request-Update 要求を開始します。



重要 このリリースでは、単一の MSCC-per-update 機能はサポートされていません。

Gy の障害処理サポート

障害処理設定は、OCS サーバーとの通信中に障害が発生した場合に実行するアクションを指定するためのものです。指定可能な障害処理設定は、Continue、Terminate、Retry、Terminate です。Terminate と Retry-Terminate は、コントロールプレーンでのみ行われます。Continue の場合、次のアクションが実行されます。

- CCFH Continue アクションが適用されると、すべての Gy URR の関連付けが解除されて PDR から削除されるため、オンライン課金のレポート/課金は行われません。

- 「removeURR」IEは、ユーザープレーンへのすべてのGyURRに対してプロビジョニングされ、ユーザープレーンはURR へのすべての参照をクリアして内部で削除を行います。
- mscc 結果コード4010、4012、5003、5012、5031 を除く、MSCC レベルのエラー結果コードの処理がサポートされています。

セッション切断が原因の *Gy* での障害処理の仕組み

process_summary

このプロセスでは、特にオンライン課金システム（OCS）との通信障害が発生した場合に、ポリシーおよび課金適用機能（PCEF）が更新要求を処理する方法について説明します。

このプロセスに関与する主要なコンポーネントは次のとおりです。

- PCEF（ポリシーおよび課金適用機能）：OCS（CCR-I/U/T）とのクレジット制御セッションを開始し、セッションの状態とクォータ消費を管理します。
- OCS（オンライン課金システム）：クレジット制御要求を受信して処理し、課金情報を管理し、応答します。
- セカンダリサーバー：プライマリサーバーの通信が失敗した場合に、PCEFが使用するバックアップ OCS サーバー。
- SU メカニズム（サービス到達可能性メカニズム）：プライマリ OCS とセカンダリ OCS の両方との通信に失敗した場合に、PCEF でのクォータ割り当てメカニズムがトリガーされ、設定されている場合、暫定クォータ割り当てでセッションの続行を許可します。プライマリ OCS とセカンダリ OCS の両方との通信に失敗した場合にトリガーされる PCEF でのクォータ割り当てメカニズム。このメカニズムは、設定されている場合、暫定クォータ割り当てでセッションの続行を許可します。

process_workflow

このプロセスには次の段階が含まれます。

1. PCEF は、クレジット制御要求（CCR-I/CCR-U）を OCS に送信します。
2. PCEF は、プライマリ OCS との通信の問題を検出します。

問題	結果
トランスポート障害が検出された場合	PCEFは、セカンダリサーバーですぐに再試行します。

問題	結果
タイムアウトが検出された場合	Tx が期限切れになります。 （注） サービス到達不能（SU）は、セカンダリ OCS サーバーでもサーバー障害が検出された後、つまり Tx タイマーの期限切れ後にのみトリガーされます。Tx の期限切れ前に応答を受信した場合、PCEF は SU をアクティブ化しません。

3. PCEF は SU をアクティブ化し、セカンダリ OCS サーバーとの通信も失敗した場合にのみ暫定クォータを割り当てます。

問題	結果
中間ボリュームや時間、またはその両方が設定されている場合	暫定クォータが、セッションに割り当てられます。

4. PCEF は、サーバー再試行値が 0 より大きい場合、暫定クォータが枯渇した後（時間またはボリュームクォータ）、最後に試行された OCS サーバーへの CCR 要求（CCR-I/CCR-U）を再試行します。PCEF は、SU メカニズムをトリガーしたサーバーに別の CCR-I または CCR-U を送信します。この試行も失敗した場合、PCEF は、消費された未報告のクォータ全体を含む CCR-U を別のサーバーに送信します（CCR-U ベースの再試行のみ。CCR-I ベースの再試行の場合、消費されたクォータは含まれません）。

5. PCEF はこの障害メカニズムを繰り返し、構成された SU アクション（続行/終了）に応じて、セッションを切断するか、セッションを続行します。

   PCEF は、正常な応答を受信するか、再試行制限に達するまで、通信を試行し続けます。

問題	結果
トランスポート障害または Tx タイムアウトが再検出された場合	ステップ 2 ～ 4 を繰り返します。
サーバーの再試行回数が上限に達した場合	SU で構成されたアクションが終了している場合、セッションは切断されます。 （注） セッションは維持されますが、SU で構成されたアクションが続行の場合、OCS サーバーへの再試行は行われません。
OCS から正常な応答を受信した場合	PCEF は SU 状態を終了し、すべての中間使用状況を OCS に報告します。

6. CCR-U メッセージの最大再試行回数の超過によってセッションが切断されると、PCRF は、SU 状態で使用された消費された全部クォータとともに Credit Control Request Terminate

（CCR-T）をOCSに送信します。CCR-I失敗最大回数の超過によってセッションが切断された場合、OCS とのセッションが確立されていないため、CCR-T は送信されません。

7. OCSは、結果コード2002で最終レポートに応答し、セッションが終了するため、PCEFによってそれ以上の CCR はトリガーされません。

result

このプロセスにより、通信障害が発生した場合でも更新リクエストを堅牢に処理し、システムがセッション状態を管理し、障害発生中に中間クォータを割り当て、通信の再確立を試行し、サーバーへの到達不能が継続してセッションを切断する必要が生じた場合でも、消費したクォータを正確に報告できるようにします。

再承認要求の処理

RAR 要求が OCS サーバーから送信されると、コントロールプレーンは必要な課金バケットの「QueryURR」をユーザープレーンに送信します。ユーザープレーンがURRレポートをコントロールプレーンに送り返すと、コントロールプレーンは FORCED_REAUTHORIZATION トリガーの CCR-Update を送信します。

クォータ有効時間の処理

MSCCバケットのクォータ有効時間が受信されると、同じ情報がユーザープレーンに送信されます。直接使用できる特定のIEがないため、QVT値がTime-QuotaIEに入力され、URRがユーザープレーンに送信されます。QVT またはタイムクォータの小さい方の値が、Time-Quota IE で設定されます。また、Time-Quotaでユーザープレーンからの使用状況レポートがトリガーされると、解釈が行われて、Validity-Timeout の CCR-Update が生成されます。

ブラックリストに登録されたコンテンツの再承認

カテゴリ Multiple-Services-Credit-Control（MSCC）は、MSCC レベルで4012/4010結果コードを受信するとブラックリストに登録されます。これは、このカテゴリを通過するパケットがこれ以上なく、ドロップすることを意味します。CUPS では、FAR は DROP アクションで作成されて URR にリンクされ、0 クォータとともに QuotaFAR の一部として UP に送信されるため、UP は DROP アクションの適用を開始します。

非 CUPS アーキテクチャでは、タイマー（タイマーはローカルで設定された quota-retry-timer か ocs から提供される gating-expire-timer）の期限が切れた後の次のパケットで、これらのブラックリストに登録されたコンテンツを再認可する規定があります。このタイマーが期限切れになると、次のパケットの到着時にOCSへのクォータ割り当て要求がトリガーされます。CUPS モードでこれを行うには、CP でタイマーを実行します（非 CUPS アーキテクチャの場合は新しいタイマーを使用し、タイムスタンプを比較して行います）。

タイマー（QRT タイマーの GET のいずれか）の期限が切れると、FAR は URR から削除され、URR は Start-of-Traffic トリガーで変更されます。次のパケット到着時に Start-of-Traffic に関する URR レポートが CPU に提供されます。この情報は、CP で OCS にクォータを要求して新しいクォータ割り当てを取得するために使用できます。

この機能のバリエーションは、CLI **diameter reauth-blacklisted-content** の設定です。つまり、OCS はブラックリストに登録されたカテゴリの再有効化を要求するために RAR を送信できます。

Gy のサーバー到達不能サポート

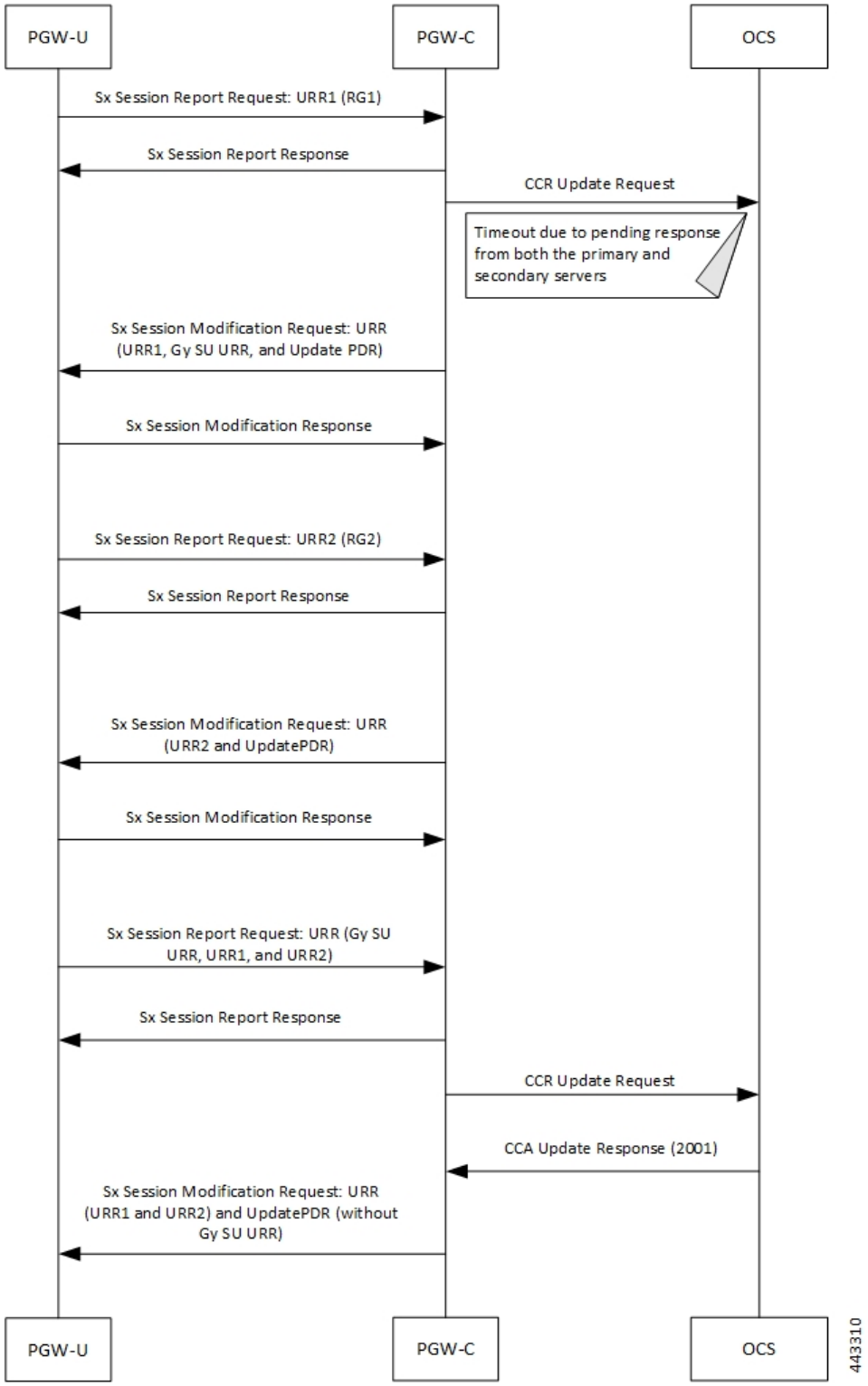
オンライン課金システム（OCS）で発生した問題、またはポリシー/課金適用機能（PCEF）と OCS 間の接続で発生した問題を解決するため、コントロールプレーン（CP）で Gy インターフェイスに対する Server-Unreachable（SU）メカニズムが設定されます。SU 設定により、障害発生後でもセッションを継続できるようになります。そのためのオプションとして、セッションがオフラインに変換されるまたは終了されるまでの暫定クォータ（ボリュームや時間）とサーバー再試行回数を設定できます。

新しい使用状況レポートルール（URR）バケットが作成されます。このバケットには、Gy セッションが SU 状態になったときの SU クォータが含まれます。新しい URR の ID は、SU URR が割り当てられると動的に生成されます。

CUPS ユーザープレーン（UP）ノードでは、既存の Vector Packet Processor（VPP）ストリームが新しい LC レコードによって変更されます。このレコードには、更新された SU URR バケットと既存の課金バケットが含まれます。

VPP ストリームが SU 状態の場合、GyURR と SU URR の 2 つのクォータ行を使用できます。GyURR が [linked-usage-reporting] トリガーが設定された状態で SU 状態になった場合、SU URR のクォータ行は VPP ストリームにリンクされます。

次の図は、CUPS での SU コールフローを示しています。


PGW-U
PGW-C
OCS
Sx Session Report Request: URR1 (RG1)
Sx Session Report Response
CCR Update Request
Timeout due to pending response from both the primary and secondary servers
Sx Session Modification Request: URR (URR1, Gy SU URR, and Update PDR)
Sx Session Modification Response
Sx Session Report Request: URR2 (RG2)
Sx Session Report Response
Sx Session Modification Request: URR (URR2 and UpdatePDR)
Sx Session Modification Response
Sx Session Report Request: URR (Gy SU URR, URR1, and URR2)
Sx Session Report Response
CCR Update Request
CCA Update Response (2001)
Sx Session Modification Request: URR (URR1 and URR2) and UpdatePDR (without Gy SU URR)
PGW-U
PGW-C
OCS
443310

ステップ	説明
1	PGW-U は、[Time and Volume] または [Quota and Threshold] などの内部トリガーにより、URR1（RG-1）を含む Sx セッションレポート要求メッセージを PGW-C に送信します。
2	PGW-C は要求を確認し、Sx セッションレポート応答メッセージを PGW-U に送信します。
3	PGW-C は、プライマリ OCS とセカンダリ OCS の両方に CCR 更新（CCR-U）要求メッセージを送信します。
4	プライマリ OCS とセカンダリ OCS の両方で CCR-U 要求メッセージが失敗すると、Gy セッションは SU 状態になります。Gy セッションの SU URR が作成され、関連する PDR にリンクされます。PGW-C は、UpdatePDR を含む Sx セッション変更要求メッセージを PGW-U に送信します。UpdatePDR の PDR URR リストには Gy SU URR が含まれます。
5	PGW-U は、両方の Gy バケット（URR1 と Gy SU URR1）の使用状況の更新を開始し、Sx セッション変更応答メッセージを PGW-C に送信します。
6	Gy URR バケットがクォータを使い切ると、PGW-U は URR2（RG-2）を含む別の Sx セッションレポート要求メッセージを PGW-C に送信します。
7	PGW-C は要求を確認し、Sx セッションレポート応答メッセージを PGW-U に送信します。
8	PGW-C は、UpdatePDR および Update RR2 を含む Sx セッション変更要求メッセージを PGW-U に送信します。UpdatePDR には、URR2 と Gy SU URR の両方を含む変更済み URR リストが含まれます。
9	PGW-U は Sx セッション変更応答メッセージを PGW-C に送信します。
10	Gy SU URR クォータを使い切ると、PGW-U は、URR1（RG-1）および URR2（RG-2）を含む Sx セッションレポート要求メッセージを PGW-C に送信します。
11	PGW-C は要求を確認し、Sx セッションレポート応答を送信します。
12	PGW-C は、SU の再試行後に CCR 更新（CCR-U）要求メッセージを OCS に送信します。
13	OCS は、[Result-Code] が 2001 の CCA 更新応答メッセージを送信します。
14	PGW-C は、URR1（RG-1）、URR2（RG-2）、および UpdatePDR（Gy SU URR なし）を含む Sx 変更要求メッセージを PGW-U に送信します。

CUPS における新しい動作

CUPS の新たな SU メカニズムは次のとおりです。

- 非 CUPS アーキテクチャでは、単一のノード（P-GW）によって Gy セッション状態とデータトラフィックが処理されるため、メッセージングによる遅延なく SU URR が作成されます。一方、CUPS モードでは、CP は追加のノードとなります。このノードは、セッション

状態に関する情報を保持し、ユーザープレーン（UP）からのURR要求を処理します。Gyセッションを SU URR に関連付けることができるのは、CP だけです。UP と CP 間のこのメッセージングにより遅延が発生し、データパケットは [Pending-Traffic-Treatment] 設定に従って処理され、通信が完了します。

- 非 CUPS アーキテクチャでは、SU 状態タイマーは、Time-Quota タイマーとは異なる方法で処理されます。SU クォータを使い切ると、OCS への再試行が発生し、新たに [next-interim-time-quota] が開始されます。一方、CUPS モードでは、SU 時間クォータを使用する場合、クォータの枯渇が CP に報告され、セッションが再びサーバー到達不能状態になると、前回の使用状況レポートからの経過時間が使用状況に計上されます。
- CUPS で **servers-unreachable after-timer-expiry** *timeout_period* CLI コマンドを使用することは推奨されません。代わりに、**servers-unreachable after-interim-time** *timeout_period* **server-retries** *retry_count* を使用して同様の動作を実現しますが、再試行回数は 1 回です（*retry_count* を「1」に設定）。

制限に達した後処理

制限到達後の後処理は、CUPS と非CUPSの両方のアーキテクチャでサポートされている3GPP非準拠の独自の動作です。この機能により、課金バケットのクォータを使い切った場合に、実装済みのリダイレクトまたは制限操作が可能になります。ただし、OCSサーバーは[FUI-Redirect]または[FUI-Restrict]を付与できません。この機能を使用する場合、オペレータは、使用可能なすべてのルール一致基準を組み合わせて（たとえば、IMSI ベースの一致基準を有効にするなど）、サブスクライバ/トラフィックごとに異なる処理を選択的に適用できます。この機能を有効にするには、次の CLI コマンドを使用します。

```
configure
  active-charging service service_name
    rulebase rulebase_name
      post-processing policy always
      end
```

また、**rule-application post-processing** CLI コマンドは、[ACS Ruledef Configuration] モードで limit-reached に設定する必要があります。

PTT no-quota Limited Pass

この機能により、サブスクライバは OCS からの応答を待機している間にネットワークを使用できます。Limited-Pass 設定では、サブスクライバが OCS からのクォータ応答を待機している間に消費できるボリュームを指定できます。使用量はそれぞれの課金バケットでカウントされ、次のクォータ割り当てに対して調整されます。

この機能を有効にするには、次の CLI コマンドを使用します。

```
configure
  active-charging service service_name
    credit-control
      pending-traffic-treatment noquota limited-pass volume volume
      end
```

Limited Pass Volume は、**noquota** のケース（クォータを初めて要求する評価グループ（RG））にのみ使用され、**quota-exhausted** には使用されません。Limited Pass Volume は、後続のクレジット要求には使用されません。

Limited Pass Volume が使い果たされるまで、トラフィックの通過が許可されます。使用量はそれぞれの課金バケットでカウントされ、付与された「クォータ」に対して調整されます。「クォータ」割り当てが実際の使用量よりも少ない場合、使用状況レポートを使用した OCS への即時レポートが発生し、より多くのクォータ割り当てが要求されます。後続の着信パケットは、「quota-exhausted」PTT 設定に従って処理されます。

OCS がクォータの拒否で応答する前に Limited Pass Volume が使い果たされていない場合、トラフィックはOCS応答後にブロックされます。ゲートウェイは、OCSが応答するまで、CCR-U（FINAL）（CUPS 以外の場合）または CCR-T（CUPS の場合）の Limited Pass Volume の使用状況を報告します。

OCS が応答する前に Limited Pass Volume が使い果たされた場合、OCS からクォータが付与されるまで、セッションの後続の着信パケットはドロップされます。

noquota のデフォルトの pending-traffic-treatment は Drop です。**default pending-traffic-treatment noquota** コマンドは、設定されたすべての Limited Pass Volume サイズを削除します。

PTT Quota-Exhausted Limited Pass

CUPS アーキテクチャの Pending-Traffic-Treatment（PTT）Quota-Exhausted Limited-Pass は、バッファリングオプションの代わりに使用できます。高速ネットワークでは、バッファリングオプションには現実的な制限があります。バッファリングでは、ゲートウェイで多数のパケットをバッファリングする必要があるため、メモリが不足し、帯域幅の速度に影響を及ぼすリスクが発生します。PTT Quota-Exhausted Limited Pass では、クォータ枯渇シナリオで設定された制限に達するまで、トラフィックを通過させます。

PTT は、Limited-Pass ボリュームを使いきるまでトラフィックを許可します。PTT は、付与された「クォータ」を基準に、それぞれの課金バケットの使用状況を計算し、調整します。「クォータ」割り当てが実際の使用量よりも少ない場合は、使用状況レポートを通じてすぐに OCS に報告し、追加のクォータ割り当てを要求します。

OCSによるクォータの拒否応答までにLimited-Passボリュームが枯渇しなければ、OCS応答後にトラフィックがブロックされます。ゲートウェイは、CCR-U（FINAL）で使用状況をレポートします。

OCSからの応答前にLimited-Passボリュームが枯渇した場合、OCSからクォータが付与されるまで、セッションの以降の着信パケットがドロップされます。

クォータが枯渇した場合の pending-traffic-treatment のデフォルト動作は [Drop] です。デフォルトの pending-traffic-treatment quota-exhausted CLI コマンドにより、設定済みの Limited-Pass ボリュームのサイズは削除されます。

この機能を有効にするには、次の CLI コマンドを使用します。

```
configure
  active-charging service service_name
    credit-control
      pending-traffic-treatment quota-exhausted limited-pass volume
```

volume
end

（注） 上記の CLI コマンドは、CUPS アーキテクチャにのみ適用されます。

注：

- **limited-pass**：OCS に到達できない場合に、サブスクライバへの制限付きアクセスを有効にします。
- **volume** *volume*：OCS に到達できない場合に、サブスクライバへの制限付きボリュームアクセスを有効にします。*volume* は、デフォルトのクォータサイズ（バイト単位）を指定します。クォータサイズは 1 ～ 4294967295 までの整数で指定する必要があります。

サポートされる機能と制限事項

ボリュームクォータ メカニズムを使用した基本的なコールフローは、Gy インターフェイスでの P-GW セッションレポートに関する次の制限付きでサポートされます。

- CCR/CCA-I、CCR/CCA-U および CCR/CCA-T、RAR/RAA メッセージのみがサポートされます。
- セッションセットアップ時およびセッション中のどちらでも、[Dynamic Rules with Online Enabled] がサポートされます。
- セッションセットアップ時およびセッション中のどちらでも、[Predefined Rules]（ダイナミックのみ）がサポートされます。「プリエンプティブな要求」の設定に制限はありません。
- オンライン課金を使用する静的ルールがサポートされます。
- Ignore-service-id がサポートされます。
- ボリュームクォータ/ボリュームしきい値メカニズムがサポートされます。
- イベントトリガー（クエリ URR が発生するもの）、および OCS への使用状況情報の送信がサポートされます。

重要 RAT 変更機能は、このリリースでは検証されていません。

- OCS が新しいクォータを付与する Sx セッション変更手順を通じた「updateURR」手順がサポートされます。
- ベアラーレベルの Gy とサブスクライバレベルの Gy がサポートされます。
- Pending-Traffic-Treatment（PTT）の [Drop] / [Pass] は、次の制限付きでサポートされます。
  - 現在サポートされているシナリオは、クォータなしとクォータ枯渇です。

- トリガー/再承認シナリオはサポートされていません。
- PTT アクション（[Forward] / [Drop]）は、クォータ取得で取得できるクォータが枯渇した後に考慮されます。

- 次のような障害シナリオが認定されています。
  - 障害処理の終了、続行と再試行、および終了：CC グループ/FHT を使用
  - エラー結果コードの処理（MSCC レベルとコマンドレベルの両方）がサポートされます。

- 実測時間クォータメカニズムがサポートされます。
- その他の時間クォータメカニズム（離散期間および連続期間）はサポートされません。
- Final-Unit-Indication Terminate メカニズムがサポートされます。
- [FUI-Restrict] はサポートされません。
- セッション中のルールのインストール/削除/変更はサポートされます。
- RAR メカニズムがサポートされます。
- Server-Unreachable（SU）メカニズムがサポートされたことにより、非CUPS P-GW と比較して動作が若干変更されました。
  - URR が UP でクォータを必要とする場合、使用状況レポートが CP に生成され、CP がリンクされた SU_URR で応答するまで、この URR に一致するパケットは [Pending-Traffic-Treatment] 設定で処理されます。
  - SU 時間クォータを使用する場合、クォータの枯渇が CP に報告され、セッションが再びサーバー到達不能状態になると、前回の使用状況レポートからの経過時間が使用状況に計上されます。

- Pending-Traffic-Treatment バッファメカニズムはサポートされません。
- [send-ccri on traffic-start] がサポートされます。
- [Quota-Hold-Time] がサポートされます。
- Quota-Consumption-Time メカニズムはサポートされません。
- [Quota-Validity-Time] がサポートされます。
- Gy でイベントが発生した場合の、Gy からの Gz レコードのトリガーがサポートされます。Gy-Gz 同期はサポートされません。
- Gy でイベントが発生した場合の、Gy からの Rf レコードのトリガーはサポートされません。
- [rated-group] 値では、「content-id」以外の値の設定がサポートされます。
  - RG「0」はサポートされません。

- Out-of-Credit、Reallocation-of-Credit イベントの PCRF へのトリガーは認定されていません。

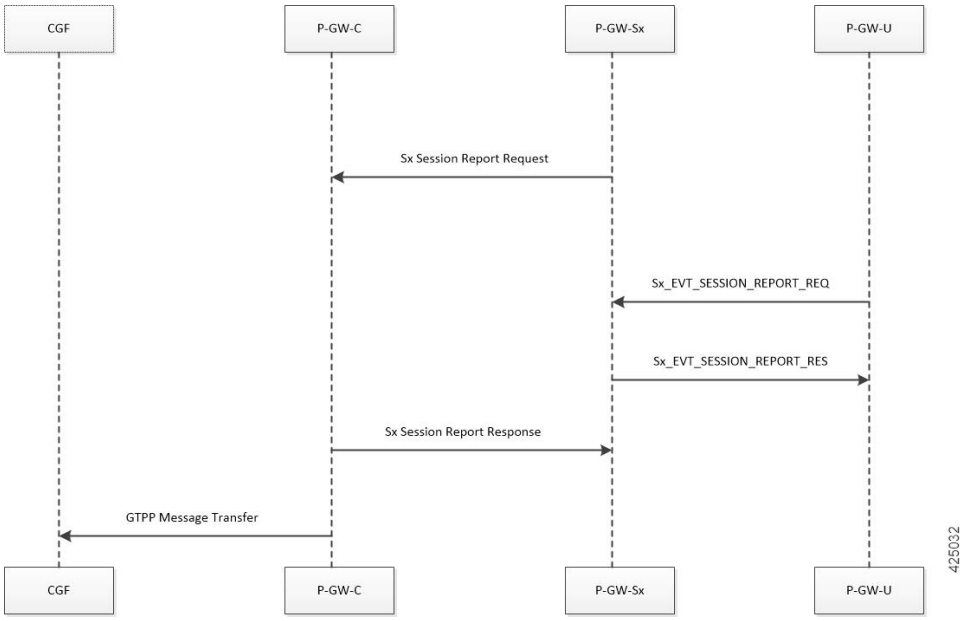


重要 PCRF に対するイベントトリガーの [Out-of-Credit] は、1 回限りの付与クォータ（合計ボリュームと付与ボリュームが同じ値）という制限付きで検証されます。

- CCR-I に関する OCS からの遅延応答がサポートされます。
- [Service-Specific-Units] はサポートされません。
- [Tariff-Time] の変更は、3GPP 仕様に従ってサポートされます。
- [Quota-Retry Timer] がサポートされます。
- **diameter mscc-final-unit-action terminate session** CLI コマンドは、[Credit Control Configuration] モードでサポートされます。
- [FUI-Redirect] は、次の制限付きでサポートされます。
  - HTTP のリダイレクトはサポートされません。
  - フィルタ ID/フィルタルールを使用した FUI リダイレクトはサポートされません。
  - WSP プロトコルはサポートされません。
  - 3GPP 仕様に従って、リダイレクトされたトラフィックは、[FUI-Redirect] のルールにヒットした場合にもリダイレクトされます。リダイレクトされたトラフィックの通過を許可するプロビジョニングはありません。
    - 3GPP 仕様に従って、CUPS アーキテクチャは **no diameter fui-redirected-flow allow** CLI コマンドの動作に準拠しています。
  - **redirect-require-user-agent** CLI コマンドはサポートされません。ユーザーエージェントが存在しない場合でも、リダイレクトは引き続き機能します。
  - 元の URL の追加はサポートされません。
  - **diameter redirect-validity-timer immediate** CLI コマンドがサポートされます。ただし、**diameter redirect-validity-timer traffic-start** CLI コマンドはサポートされません。
  - リダイレクトを脱するトークンベースのメカニズムはサポートされません。CUPS でリダイレクトを終了するには、OCS が Redirect Validity-Time または RAR を送信します。
  - FUI リダイレクトは、非 CUPS アーキテクチャでの動作と同様に、URL に対してのみサポートされます。
- PCRF/OCS からの rulebase の変更がサポートされます。

Gz インターフェイスを使用した P-GW セッションレポート

この項では、Gzインターフェイスを使用したP-GWセッションレポートについて説明します。



接続解除要求における URR 処理

- URR 情報は、Sx セッション削除応答の一部として PGW ユーザープレーンによって送信されます。
- P-GW コントロールプレーンは、これらの URR を対応する課金バケットにマッピングし、既存のフレームワークを使用して、Gz、Gy などの各インターフェイスで課金レコードを送信します。

Sx セッションレポート要求処理

P-GW ユーザープレーンは、ボリュームまたは時間しきい値のようなトリガーに関する使用状況レポートを送信します。P-GW コントロールプレーンは、対応する課金バケットに URR をマッピングします。

Gz の URR レポート処理

URR レポートにより、P-GW ユーザープレーンによって送信されたトリガーに応じて LOSDV バケットが作成され、P-GW CDR が生成されます。

- ベアラーレベルの URR を受信すると、対応するサブセッション/ベアラーの P-GW CDR が生成され、既存の LOSDV コンテナと現在のレポート要求の一部として作成される LOSDV コンテナが報告されます。ベアラーレベルの URR を受信すると、ユーザープレーンがすべての SDF レベルの URR も送信したと想定されます。

- SDF レベルの URR を受信すると、それらの URR は LOSDV コンテナとして保存されます。この場合、 fbc_bucket は URR から必要なカウントまたはタイムスタンプを使用して作成されます。

標準準拠

CUPS のコントロールプレーンは、次の標準規格に準拠しています。

- 3GPP 仕様 23.214 リリース 14.0：Universal Mobile Telecommunications System (UMTS); LTE; Architecture enhancements for control and user plane separation of EPC nodes。
- 3GPP 仕様 29.244 リリース 14.0：LTE; Interface between the Control Plane and the User Plane of EPC Nodes。
- 3GPP 仕様 23.401 リリース 14.0：3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。