Gx インターフェイスのサポート

この章では、サブスクライバのポリシーと課金制御をサポートする Gx インターフェイスの設定について説明します。

IMS サービスは、アクセスサポートとは無関係に、音声、ビデオ、およびデータの転送に関するアプリケーションサポートを提供します。ローミング IMS サブスクライバには、他の機能とは別に、必要十分で中断のない一貫性のあるシームレスなユーザーエクスペリエンスがアプリケーションセッション中に必要になります。また、使用されている特定の IMS アプリケーションによって消費されるリソースの料金のみがサブスクライバに請求されることも重要です。

この章に記載する手順を実行する前に、本アドミニストレーション ガイドの説明に従って、お使いのサービスモデルに最適な設定例を選択し、そのモデルに必要な要素を設定することを推奨します。

この章の内容は、次のとおりです。

Rel. 7 Gx インターフェイス

Rel. 7 Gx インターフェイスのサポートは、次の製品向けの Cisco ASR シャーシで利用できます。

- GGSN
- IPSG

ここでは、次の内容について説明します。

はじめに

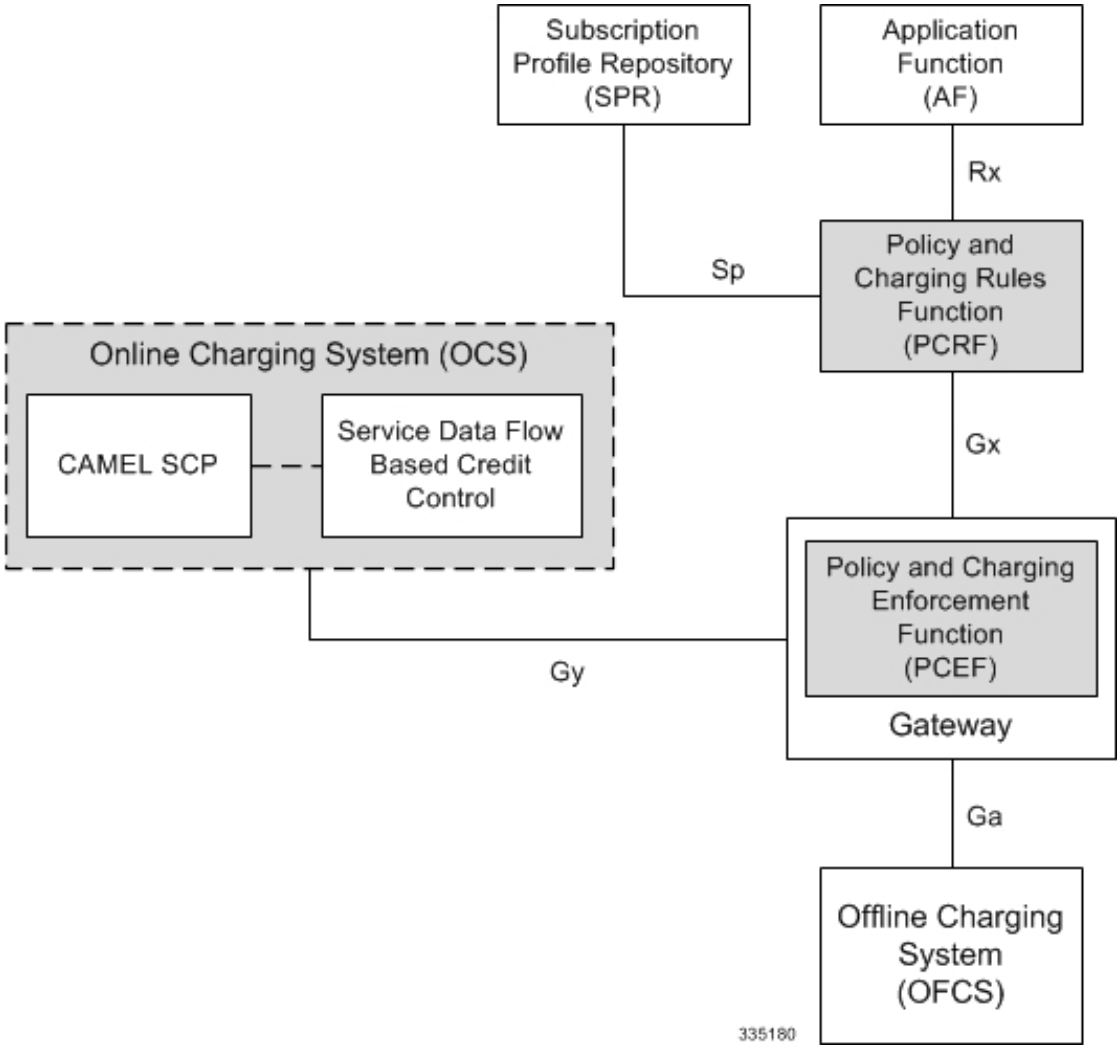
GPRS/UMTS ネットワークでの IMS 展開の場合、システムはポリシーベースのアドミッションコントロールのサポートおよびフローベース課金にリリース 7 Gx インターフェイスを使用します。Rel. 7 Gx インターフェイスは、ゲート設定、帯域幅制限などのポリシー制御適用機能をサポートし、フローベース課金もサポートします。これは、動的にプロビジョニングされたポリシー制御および課金（PCC）ルールによって実現されます。これらの PCC ルールは、サービスデータフロー（SDF）を識別し、課金を実行するために使用されます。ルールに関連付けられているその他のパラメータは、ポリシー制御を適用するために使用されます。

通信事業者は PCC アーキテクチャを利用することで、サービスベースの QoS ポリシーとフローベース課金制御を実行できます。PCC アーキテクチャでは、これは主にポリシーおよび課金適用機能（PCEF）/Cisco Systems GGSN とポリシーおよび課金ルール機能（PCRF）によって実現されます。

GPRS/UMTS ネットワークでは、クライアント機能は GGSNに付属しているため、IMS 承認のシナリオではゲートウェイとも呼ばれます。次の図では、ゲートウェイは Cisco Systems GGSN であり、PCEF 機能は Enhanced Charging Service（ECS）によって提供されます。Rel 7. Gx インターフェイスは、Diameter 接続として導入されます。Gx メッセージには、ほとんどの場合、ダイナミックルールのインストール/変更/削除と、事前定義されたルールのアクティブ化/非アクティブ化が含まれます。

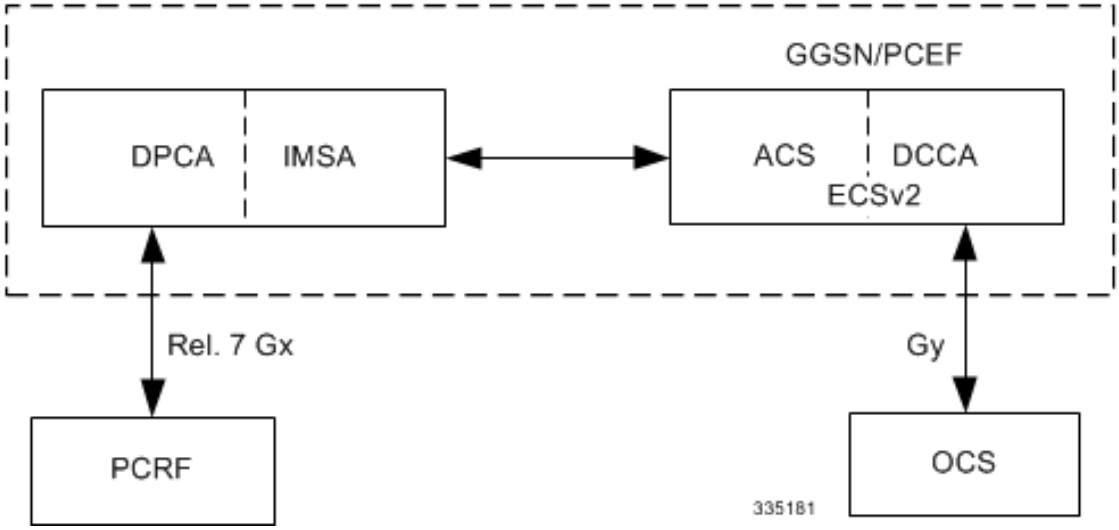
Rel. 7 Gx 参照ポイントは、ゲートウェイと PCRF の間にあります。この参照ポイントは、PCRF からゲートウェイへの PCC ルールのプロビジョニングと削除、およびゲートウェイから PCRF へのトラフィック プレーン イベントの送信に使用されます。Gx 参照ポイントは、アプリケーションに関連する AVP を適用することで、課金制御とポリシー制御のいずれかまたは両方に使用できます。次の図は、ポリシーおよび課金アーキテクチャに含まれるさまざまな要素間の参照ポイントを示します。

図 *1* : *PCC* 論理アーキテクチャ



ゲートウェイ内では、IMSA モジュールと DPCA モジュールが（SessMgr で）Gx プロトコル関連の機能を処理し、ポリシーの適用と課金は ECS で行われます。Gy プロトコル関連の機能は、DCCA モジュール内（ECS）で処理されます。次の図は、ゲートウェイ内のコンポーネント間の連携動作を示しています。

図 *2 : Cisco PCEF* 内の *PCC* アーキテクチャ



サポート対象のネットワークとプラットフォーム

この機能は、コアネットワークサービスの GGSN サービスを実行しているすべてのシャーシでサポートされています。

ライセンス要件

Rel. 7 Gx インターフェイスのサポートは、ライセンス供与されたシスコの機能です。別の機能ライセンスが必要になる場合があります。特定のライセンス要件の詳細については、シスコのアカウント担当者にお問い合わせください。ライセンスのインストールと確認の詳細については、『システム管理ガイド』の「ソフトウェア管理操作」の「ライセンスキーの管理」の項を参照してください。

サポートされる標準

Rel 7. Gx インターフェイスのサポートは、次の標準と RFC に基づいています。

- 3GPP TS 23.203 V7.6.0（2008-03）：3rd Generation Partnership Project、Technical Specification Group Services and System Aspects、Policy and charging control architecture（Release 7）
- 3GPP TS 29.212 V7.8.0（2009-03）：3rd Generation Partnership Project、Technical Specification Group Core Network and Terminals、Policy and Charging Control over Gx reference point（Release 7）
- 3GPP TS 29.213 V7.4.0（2008-03）：3rd Generation Partnership Project、Technical Specification Group Core Network and Terminals、Policy and Charging Control signalling flows and QoS parameter mapping（Release 7）
- RFC 3588、Diameter Base Protocol。2003 年 9 月
- RFC 4006、Diameter Credit-Control Application。2005 年 8 月

用語および定義

このセクションでは、Rel. 7 Gx に関連した機能と用語について説明します。

ポリシー制御

PCRF が IP-CAN ベアラーの制御方法を PCEF に指示するプロセス。

ポリシー制御は、次の機能で構成されます。

- **バインド**：バインドとは、サービスデータフロー（SDF）と、そのSDFを転送するIP CANベアラー（GPRS の場合は PDP コンテキスト）との間の関連付けの生成です。

  PCC ルールの QoS 要求と SDF テンプレートがベアラーバインドの入力になります。選択されたベアラーには、PCC ルールで示されているものと同じ QoS クラスが割り当てられます。

  IP-CANのタイプとベアラー制御モードに応じて、ベアラーバインドはPCRF、またはPCRFと PCEF の両方によって実行できます。

  - UE 専用 IP-CAN ベアラー確立モードの場合、PCRF がベアラーバインドを実行します。PCRFがベアラーバインドを実行する場合、ベアラーIDによってベアラー（PDPコンテキスト）が示されます。ベアラー ID で、PDP セッション内のベアラーが一意に識別されます。
  - UE/NW IP-CAN ベアラー確立モードの場合、PCRF はユーザー制御サービスの PCC ルールのバインドを実行し、PCEFはネットワーク制御サービスのPCCルールのバインドを実行します。

  PCEF ルールのバインドは、RAR や CCA-U などの PCRF メッセージで、「bearer-ID」なしで EPS IP-CAN ベアラーに対して BCM モードが UE のみに設定されている場合に成功します。

  3G から 4G へのハンドオーバーのシナリオでは、ルールバインドとルール削除はUE専用モードで正常に行われます。この変更/インストール/削除によるフィルタ（および関連情報）の変更は、UE専用モードでの更新としてUEに通知されず、UEに送信できません。これらのルールは課金のみに関して考慮されます。フィルタ（および関連情報）をUEに通知できるように、同じルールが 4G で再度変更されることが期待されます（ハンドオーバーが行われた場合）。

  GnGp HO シナリオ中にコリジョンが発生すると、CCR-U が生成され、ルール障害を報告するために PCRF に送信されます。

  この追加の Gx メッセージ（CCR-U）がトリガーされると、RAT_TYPE トリガーが有効になっている場合、複数のCCR-Uを設定する必要が生じます。設定しない場合、HO中にコリジョンが発生するたびにサブスクライバコールがドロップされます。

- **ゲート制御**：ゲート制御とは、SDFに属するパケットが目的のエンドポイントに向かってパススルーすることをブロックまたは許可することです。ゲートはPCCルール内で記述され、ゲート制御はSDFごとに適用されます。ゲートを開閉するコマンドを実行すると、対応するIPパケットの経路が有効または無効になります。ゲートが閉じられている場合、

関連する IP フローのすべてのパケットがドロップされます。ゲートが開いている場合、関連する IP フローのパケットの転送が許可されます。

- **イベントレポート**：イベントレポートは、ユーザープレーンでの新しい動作をトリガーするアプリケーションイベントの通知とこうしたイベントへの応答、およびゲートウェイ（PCEF）のリソースに関連したイベントのレポートです。
  - イベントトリガーを使用して、どの IP-CAN セッション変更や特定のイベントが発生すると、PCEF が PCC ルールを再要求するかを確認できます。PCEF から PCRF へのイベントトリガーレポートは、特定のイベントに応じて IP CAN セッションまたはベアラーに適用できますが、イベントトリガーのプロビジョニングはセッションレベルで行われます。

    イベントトリガーが不明なRARは動作を発生させずに無視され、DIAMETER_SUCCESS で応答されます。
  - イベントレポート機能（ERF）は、PCC ルールのプロビジョニング中に PCRF からイベントトリガーを受信し、イベントトリガー検出を実行します。受信したイベントトリガーに一致するイベントが発生すると、ERF は発生したイベントを PCRF に報告します。提示されたイベントトリガーが特定のパラメータ値に関連付けられている場合、ERF はそれらの値を PCRF への応答に含めます。イベントレポート機能を備えているのは PCEF です。

    SUCCESSFUL_RESOURCE_ALLOCATION (22) イベントトリガーは、次の条件で送信されます。
    - ルールが正常にインストールされた場合（およびイベントトリガーが PCRF によって導入され、resource-allocation-notification が有効になった場合）。
    - 部分的に失敗した場合、つまり、2 つ以上のルールがインストールされ、少なくとも 1 つのルールが正常にインストールされた場合。（およびイベントトリガーが PCRF によって導入され、resource-allocation-notification が有効になった場合）。

    完全に失敗した場合、つまり、ルールが 1 つもインストールされていない場合、イベントトリガー SUCCESSFUL_RESOURCE_ALLOCATION (22) は送信されません。

重要 このリリースでは、イベントトリガー「IP-CAN_CHANGE」および「MAX_NR_BEARERS_REACHED」はサポートされていません。

- **QoS 制御**：QoS 制御とは、SDF または IP-CAN ベアラーまたは QoS クラス識別子（QCI）に許可される最大 QoS の承認と適用のことです。複数の SDF の集約（GPRS の場合は PDP コンテキスト）の場合、個々の SDF の承認済み QoS 情報の組み合わせが、この集約の承認済み QoS として提供されます。
  - SDF ごとの QoS 制御により、PCC アーキテクチャは、特定の SDF ごとに適用される承認済み QoS を PCEF に提供できます。

- IP-CAN ベアラーの承認済み QoS の適用により、UE 開始 IP-CAN ベアラーの確立または変更の一環として、ゲートウェイ（PCEF）によって要求されたベアラー QoS のダウングレードまたはアップグレードが発生する可能性があります。また、オペレータのポリシーとネットワーク機能によっては、承認済み QoS の適用により、ネットワーク開始 IP-CAN ベアラーの確立または変更が発生する場合もあります。PCRF が IP-CAN ベアラーと PCC ルールの両方に承認済み QoS を提供する場合、個々の PCC ルールの承認済み QoS の適用が最初に実行されます。
- QoS 承認情報は、PCRF によって動的にプロビジョニングされる場合と、PCEF で事前定義された PCC ルールである場合があります。PCRF が PCC ルールを動的に提供する場合は、IP-CAN ベアラーに承認済み QoS 情報（統合された QoS）を提供できます。PCEF 内の事前定義された PCC ルールの場合、承認された QoS 情報は PCC ルールがアクティブになると有効になります。PCEF では、承認済み QoS 情報のさまざまなセット（PCRF から受信した情報と、事前定義された PCC ルールに対応する情報）が組み合わされます。PCRF は、事前定義された PCC ルールの承認済み QoS 情報を認識し、それらのルールをアクティブ化する際に、この情報を考慮します。これにより、PCRF によってアクティブ化される一連の PCC ルールの組み合わせによる承認済み QoS が、それらの PCC ルールが動的に提供されるか、事前定義されているか、またはその両方であるかに関係なく、サブスクリプションポリシーとオペレータポリシーによって指定された制限内に収まることが保証されます。

重要 このリリースでは、QoS リソース予約はサポートされていません。

サポートされる機能：

- 承認済み QoS のプロビジョニングとポリシー適用：PCRF は PCEF に承認済み QoS を提供する場合があります。承認済み QoS は、適用されるリソースの適切な値を提供します。
- IP CAN ベアラーごとの「承認済み QoS」のプロビジョニング：ベアラーバインドが PCRF によって実行される場合、IP-CAN ベアラーごとの承認済み QoS が使用されます。
- IP CAN ベアラーごとの「承認済み QoS」のポリシー適用：ポリシーベースの承認の適用を担当するのは PCEF です。結果として、要求された QoS が IP CAN ベアラーごとの「承認済み QoS」と一致することが保証されます。
- SDF ごとの承認済み QoS のポリシープロビジョニング：SDF ごとの承認済み QoS のプロビジョニングは、PCC ルールのプロビジョニング手順の一部です。
  - SDF ごとの承認済み QoS のポリシー適用：承認済み QoS が PCC ルールに対して定義されている場合、PCEF は、その PCC ルールに対応する SDF のデータレートを、PCC ルールに対して承認済みの最大帯域幅を超えないように制限します（制限を超えるパケットを破棄します）。
  - PCC ルールを非アクティブ化または削除すると、PCEF は、その PCC ルール用に予約されていたリソースを解放します。PCRF が IP-CAN ベアラーと PCC ルールの両方に

承認済み QoS を提供する場合、個々の PCC ルールの承認済み QoS の適用が最初に実行されます。

重要 このリリースでは、混合モード（BCM＝UE_NW）での承認済み QoS の範囲の調整はサポートされていません。

- • QCI ごとの承認済み QoS のプロビジョニング：PCEF がベアラーバインドを実行する場合、PCRF は非 GBR ベアラー QCI 値について QCI ごとの承認済み QoS をプロビジョニングできます。PCRF がベアラーバインドを実行する場合、PCRF は QCI ごとの承認済み QoS をプロビジョニングしません。PCRF は、GBR ベアラー QCI 値の QCI ごとの承認済み QoS をプロビジョニングしません。

重要 1 ー 9 の標準ベース QCI 値のみがサポートされます。QCI 値 1 ～ 9 は、3GPP Specification TS 23.203「Policy and charging control architecture」で定義されています。

- QCI ごとの承認済み QoS のポリシー適用：PCEF は、非 GBR ベアラー QCI 値の QCI ごとの承認済み QoS を受け取ることができます。

- その他の機能：
  - ベアラー制御モード選択：PCEF は、Gx 参照ポイントを介して、IP-CAN セッション確立時または（SGSN 変更の結果としての）IP-CAN セッション変更時に、ベアラー制御モード（BCM）選択の要求を通知する場合があります。この選択は「PCC ルール要求」の手順を使用して実行されます。

    Bearer-Control-Mode AVP が PCRF から受信されない場合、IP-CAN セッションは終了されません。UE/SGSN/GGSN 間でネゴシエートされた値は、BCM と見なされます。サービスタイプごとに、次の値が考慮されます。

    - GGSN：UE/SGSN/GGSN 間でネゴシエートされた値が考慮されます。

      次のシナリオでは、BCM として UE_ONLY が選択されています。

      シナリオ 1：

      - UE -> UE_ONLY
      - SGSN -> UE_ONLY
      - GGSN -> UE_ONLY
      - PCRF -> NO BCM

      シナリオ 2：

      - UE -> UE_ONLY

- SGSN -> UE_ONLY
- GGSN -> Mixed
- PCRF -> NO BCM

- GTP-PGW：UE_NW が BCM として考慮されます。
- IPSG：UE_ONLY が BCM として考慮されます。
- HSGW/SGW/PDIF/FA/PDSN/HA/MIPV6HA：NONE が BCM として考慮されます。

- PCC ルールのエラー処理：1 つ以上の PCC ルールのインストールまたはアクティブ化に失敗した場合、PCEF は、影響を受ける PCC ルールの CCR または RAA コマンドのいずれかに 1 つ以上の Charging-Rule-Report AVP を含めます。PCEF は、各 Charging-Rule-Report AVP 内に、1 つ以上の Charging-Rule-Name AVP または Charging-Rule-Base-Name AVP を追加することによってエラーの発生した PCC ルールを示し、Rule-Failure-Code AVP を追加することによってエラーの理由コードを示し、また PCC-Rule-Status AVP を追加します。

  1 つまたは複数の新しい PCC ルール（以前は正しくインストールされていなかったルール）のインストールまたはアクティブ化に失敗した場合、PCEF はプッシュモードとプルモードの両方で PCC-Rule-Status を INACTIVE に設定します。

  PCC ルールが正常にインストールまたはアクティブ化されたものの、PCEF によって適用できなくなった場合、PCEF は PCRF に新しい CCR コマンドを送信し、Charging-Rule-Report AVP を追加します。PCEF は、Charging-Rule-Report AVP 内に Rule-Failure-Code AVP を追加し、PCC-Rule-Status を INACTIVE に設定します。

  GnGp HO シナリオ中にコリジョンが発生すると、CCR-U が生成され、ルール障害を報告するために PCRF に送信されます。

  この追加の Gx メッセージ（CCR-U）がトリガーされると、RAT_TYPE トリガーが有効になっている場合、複数の CCR-U を設定する必要が生じます。設定しない場合、HO 中にコリジョンが発生するたびにサブスクライバコールがドロップされます。

- 時刻の手順：PCEF は、PCRF の指示に従って PCC ルール要求を実行します。再検証時間が PCRF によって設定されている場合、PCEF は、PCRF とのやり取りをトリガーし、確立された IP CAN セッションに関する PCC ルールを PCRF に要求します。PCEF が REVALIDATION_TIMEOUT イベントをトリガーすると、PCEF はタイマーを停止します。

重要 Rule-Activation-Time/Rule-Deactivation-Time/Revalidation-Time AVP は、その値が現在時刻または現在の IPSG 時刻より後の時刻に対応する場合にのみ正常に解析されます。それ以外の場合、AVP およびメッセージ全体が拒否されます。

CCA/RAR で Rule-Deactivation-Time AVP が省略されている場合、この AVP の以前の値は無効になります。新しい動作は、Gx の 3GPP 仕様、バージョン 12.1.0 に準拠しています。

PCRF が Rule-Deactivation-Time AVP なしで RAR/CCA-U で同じ事前定義済みルールを再度有効にすると、このルールの deactivation-time は削除されます。

以前の動作に切り替える場合、PCRF は PCRF メッセージ（RAR、CCA-U）で、predef-rule 名と一緒に Rule-Deactivation-Time AVP と同じ値を再送信する必要があります。

重要 この動作変更は、事前に定義したルールにのみ適用されます。

Gx でのファイアウォールポリシーのサポート：Diameter AVP「SN-Firewall-Policy」が Diameter ダイナミックディクショナリに追加され、Gx インターフェイスでファイアウォールポリシーをサポートできるようになりました。この AVP は CCA-I メッセージにエンコードされ、APN 設定を介して PDP コンテキストに静的に割り当てられた、またはRADIUS の Access-Accept を介して動的に割り当てられた fw-and-nat ポリシーを適用/上書きできます。この AVP は、任意の CCA-U または RAR メッセージ内で解析することも可能です。これにより、現在 PDP コンテキストに割り当てられている fw-and-nat ポリシーを変更できます。

課金制御

課金制御は、SDF に属するパケットを課金キーに関連付け、必要に応じてオンライン課金やオフライン課金を適用するプロセスです。フローベースの課金は、SDF のリアルタイム分析に基づいて、ベアラー使用量の差別化された課金を処理します。課金制御を可能にするために、PCC ルールの情報によって SDF が識別され、課金制御のパラメータが指定されます。PCC ルール情報は、サブスクリプションデータに依存する場合があります。

オンライン課金の場合、PCEF イベント時にオンライン課金アクションを適用できます（たとえば、QoS 変更時の再承認など）。

PCC ルールでは課金システムとの連携が不要であること、つまりこの SDF のアカウンティングもクレジット制御も実行せず、その後にオフライン課金情報が生成されないことを PCEF に示すことができます。

サポートされる機能：

- IP-CAN セッションの課金関連情報のプロビジョニング
- 課金アドレスのプロビジョニング：プライマリまたはセカンダリイベント課金機能名（オンライン課金サーバー（OCS）アドレスまたはピア名）

重要 このリリースでは、Gx を介したプライマリまたはセカンダリ課金収集機能名（オフライン課金サーバー（OFCS）アドレス）のプロビジョニングはサポートされていません。

- デフォルトの課金方法のプロビジョニング：このリリースでは、デフォルトの課金方法は CCR-I メッセージで送信されます。この場合、新しい AVP オンラインおよびオフラインが、設定に基づいて CCR-I メッセージで送信されます。コマンドレベルで受信した Online

または Offline AVP は、PCC ルールレベルで設定されていない場合、ダイナミックルールにのみ適用されます。

課金の相関

SDF レベルとアプリケーションレベル（IMS など）間の課金の相関、およびアプリケーションレベルでのオンライン課金サポートを目的として、該当する課金識別子と IP-CAN タイプ識別子が PCRF から AF に渡されます（これらの識別子が使用できる場合）。

IMS ベアラー課金の場合、IP マルチメディア コア ネットワーク（IM CN）サブシステムおよびパケット交換（PS）ドメインエンティティは、相関のある課金データを生成する必要があります。

これを実現するために、ゲートウェイは PDP コンテキストに関連付けられた GGSN 課金識別子（GCID）をそのアドレスとともに PCRF に提供します。次に PCRF は、P-CSCF によって提供される IMS 課金識別子（ICID）をゲートウェイに送信します。ゲートウェイは、課金データと課金システム間の相関を行えるように、GCID と ICID（PCRF から受信した場合）を含む課金レコードを生成します。

PCRF は、IMS セッションで IP フローを一意に識別するフロー識別子も提供します。

ポリシーおよび課金制御（PCC）ルール

PCC ルールにより、SDF の検出が可能になり、ポリシー制御や課金制御のパラメータが提供されます。PCC ルールの目的は次のとおりです。

- SDF に属するパケットを検出します。
  - PCC ルールの SDF フィルタに基づいてダウンリンク IP CAN ベアラーを選択します。
  - PCC ルール内の SDF フィルタを使用して、アップリンク IP フローが正しい IP CAN ベアラーで転送されるように強制します。
- SDF が提供するサービスを特定します。
- SDF に適用可能な課金パラメータを指定します。
- SDF のポリシー制御を提供します。

PCEF は PCC ルールの優先順位に従って、PCC ルールの SDF フィルタと照らし合わせて受信パケットを評価し、受信パケットごとに PCC ルールを選択します。パケットが SDF フィルタに一致すると、そのパケットの照合プロセスが完了し、そのフィルタの PCC ルールが適用されます。

PCC ルールには次の 2 種類があります。

- ダイナミック PCC ルール：Gx インターフェイスを介して PCEF に動的にプロビジョニングされるルール。この PCC ルールは事前に定義することも、PCRF で動的に生成することもできます。ダイナミック PCC ルールは任意のタイミングでインストール、変更、および削除できます。

- 定義済みPCCルール：通信事業者によってPCEFで事前設定されたルール。定義済みPCCルールは、PCRF が任意のタイミングでアクティブ化または非アクティブ化できます。PCEF 内の定義済み PCC ルールをグループ化すると、PCRF は Gx 参照ポイント上で一連の PCC ルールを動的にアクティブ化できます。

重要 3番目のルールであるスタティックPCCルールは、通信事業者によってシャーシに事前設定できます。スタティック PCC ルールは、PCRF で明示的に認識されておらず、PCRF の制御下にありません。スタティック PCC ルールは、Gx で制御されない汎用ベアラーにバインドされます。

PCC ルールの構成は次のとおりです。

- ルール名：PCEF と PCRF 間の通信で PCC ルールを参照するために使用されます。
- サービス識別子：SDFが関連するサービスやサービスコンポーネントを識別するために使用されます。
- サービス データ フロー フィルタ：サービスフローフィルタは、ルールを適用するトラフィックの選択に使用されます。
- 優先順位：SDF フィルタが重複しているさまざまな PCC ルールでは、ルールの優先順位によって、どのルールが適用されるかが決まります。ダイナミック PCC ルールと定義済み PCC ルールの優先順位が同じ場合は、ダイナミック PCC ルールが優先されます。
- ゲートステータス：SDF フィルタによって検出された SDF がアップリンク方向またはダウンリンク方向で通過するか（ゲートが開いている）、または破棄されるか（ゲートが閉じている）かを示します。
- QoS パラメータ：QoS 情報には、QoS クラス識別子（SDF の認定された QoS クラス）、割り当ておよび保持優先順位（ARP）、およびアップリンクとダウンリンクの認定ビットレートが含まれます。

重要 ECS は、ベアラーのバインドに ARP バイト全体を（QCI とともに）使用します。ダイナミックルールでは機能ビットと脆弱性ビットがオプションであるため、これらのフラグがないダイナミックルールを受信した場合、機能ビットが 1（無効）に設定され、脆弱性ビットが 0（有効）に設定されていると見なされます。事前定義済みルールでは、これらの 2 つのフラグはサポートされていないため、現時点では、すべての事前定義済みルールの機能ビットが 1（無効）に設定され、脆弱性ビットが 0（有効）に設定されていると見なされます。

- 課金キー（料金設定グループ）

- その他の課金パラメータ：課金パラメータは、オンライン課金インターフェイスとオフライン課金インターフェイスが使用されるかどうか、オフライン課金で計測される内容、どのレベルで PCEF がルールに関連する使用状況を報告するかなどを定義します。

重要 このリリースでは、ダイナミック PCC ルールの計測方式とレポートレベルの設定はサポートされていません。

アプリケーション機能（AF）が Rx インターフェイスを介してこの情報を提供した場合、PCC ルールにはアプリケーションとベアラーレイヤー間の課金相関を有効にするための AF レコード情報も含まれます。IMS の場合は、IMS 課金識別子（ICID）とフロー識別子が含まれます。

重要 ASR 5500 は、Gx メッセージのダイナミック課金ルールごとのフロー説明を含む 8 つのフロー情報のみをサポートします。

セッションマネージャがクラッシュした場合にベアラーごとに回復できる 24 の PCC ルールがあります。また、最大 24 の PCC ルールを ICSR 後に回復できます。

保留状態の PCC ルールの変更が受信されると、変更されたパラメータは P-GW でバッファに保存されます。保留中の要求に対する応答をアクセスネットワークから受信した後、P-GW はバッファされたパラメータの変更を処理し、必要に応じてネットワークに対する別の更新要求を生成します。

Gx 参照ポイントを介した PCC 手順

PCC ルールの要求

PCEF は、Gx 参照ポイントを使用して、次の場合に PCC ルールを要求します。

- IP-CAN セッションの確立時
- IP-CAN セッションの変更時

PCC ルールは、イベントトリガーを求めずに、PCC ルールのインストール/アクティブ化または適用の失敗の結果として要求することもできます。

PCC ルールのプロビジョニング

PCRF は、Rel. 8 Gx 参照ポイントを介して、PCEF で適用される PCC ルールを示します。これは、次のいずれかの手順で行われます。

- プル（PCEF により要請されたプロビジョニング）：PCEF による PCC ルールの要求に応じて、PCRF は CC-Answer で PCC ルールをプロビジョニングします。
- プッシュ（要請のないプロビジョニング）：PCRF は、PCEF からの要求を取得せずに PCC ルールのプロビジョニングを決定することがあります。たとえば、Rx 参照ポイントを介して PCRF に提供された情報への応答、または PCRF 内の内部トリガーへの応答。PCEF

からの要請なしにPCCルールをプロビジョニングするために、PCRFはこれらのPCCルールを RA 要求メッセージに含めます。この RA 要求によってトリガーされる CCR および CCA メッセージはありません。

PCEF からの要求ごとに、または要請のないプロビジョニング時に、PCRF は 0 個以上の PCC ルールをプロビジョニングします。PCRFは、次のいずれかの方法で単一のPCCルールに対する操作を実行できます。

- PCEFで事前定義されたPCCルールをアクティブ化または非アクティブ化する場合、PCRFは、Charging-Rule-Name AVP 内でこの PCC ルールへの参照をプロビジョニングし、Charging-Rule-Install AVP または Charging-Rule-Name AVP のいずれかを選択して必要なアクションを提示します。
- PCRF によりプロビジョニングされた PCC ルールをインストールまたは変更する場合、PCRF は、Charging-Rule-Install AVP 内で対応する Charging-Rule-Definition AVP をプロビジョニングします。
- 以前に PCRF によってプロビジョニングされた PCC ルールを削除する場合、PCRF は、このルールの名前を Charging-Rule-Remove AVP 内の Charging-Rule-Name AVP の値にしてプロビジョニングします。

重要 課金ルール名の最大長は 63 バイトです。課金ルール名の長さが 63 バイトを超える場合、Rule-Failure-Code が RESOURCES_LIMITATION の課金ルールレポートが送信されます。この課金ルールレポートは、ルール名の長さが 128 文字未満の場合にのみ送信されます。課金ルール名の長さが 128 文字以上の場合、課金ルールレポートは送信されません。

セッションの接続中、P-GW は、同じ CCR-U にルールの失敗とクレジットの不足を組み合わせて PCRF に送信します。

アップリンク IP パケットの PCC ルールの選択

PCC が有効になっている場合、PCEF は、PCC ルールの優先順位に従い、IP CAN ベアラーの PCRF が提供するアクティブな PCC ルールまたは事前定義済みのアクティブな PCC ルールのアップリンク SDF フィルタを使用してパケットを評価することで、IP CAN ベアラー内の受信アップリンク IP パケットそれぞれに適用する PCC ルールを選択します。

重要 PCRF が提供する PCC ルールと事前定義された PCC ルールが同じ優先順位を持つ場合、PCRF が提供する PCC ルールのアップリンク SDF フィルタが最初に適用されます。

重要 IMSA および ECS では、同じ優先順位の値を持つ 2 つ（以上）のダイナミックルールを PCRF にインストールできます。

パケットが SDF フィルタに一致すると、そのパケットの照合プロセスが完了し、そのフィルタの PCC ルールが適用されます。対応する IP CAN ベアラーのいずれの PCC ルールにも一致しないアップリンク IP パケットは廃棄されます。

ダウンリンク IP パケットの PCC ルールおよび IP CAN ベアラーの選択

PCC が有効になっている場合、PCEF は、PCC ルールの優先順位に従い、IP CAN セッションにおけるすべての IP CAN ベアラーの、PCRF が提供するアクティブな PCC ルールまたは事前定義済みのアクティブな PCC ルールのダウンリンク SDF フィルタを使用してパケットを評価することで、IP CAN セッション内の受信ダウンリンク IP パケットそれぞれに適用する PCC ルールを選択します。

重要 PCRF が提供する PCC ルールと事前定義された PCC ルールが同じ優先順位を持つ場合、PCRF が提供する PCC ルールのダウンリンク SDF フィルタが最初に適用されます。

パケットが SDF フィルタに一致すると、そのパケットの照合プロセスが完了し、そのフィルタの PCC ルールが適用されます。ダウンリンク IP パケットは、選択した PCC ルールがマッピングされている IP CAN ベアラー内で転送されます。IP CAN セッションのいずれの PCC ルールにも一致しないダウンリンク IP パケットは廃棄されます。

次の手順もサポートされています。

- IP-CAN ベアラー終了の表示の意味
- IP-CANセッション終了の表示：IP-CANセッションが終了している場合（たとえば、GPRSでIP-CANセッション内の最後のPDPコンテキストが終了している場合）、PCEFはPCRFに接続します。
- IP-CAN ベアラー終了の要求：IP CAN セッション内の最後の IP CAN ベアラーの終了が要求された場合、PCRF および PCEF は「IP-CAN セッション終了の要求」手順を適用します。
- IP-CAN セッション終了の要求：内部トリガーまたは SPR からのトリガーにより PCRF が IP CAN セッションの終了を決定した場合、PCRF は PCEF に通知します。PCEF は PCRF に確認応答し、その IP-CAN セッションで以前にインストールまたはアクティブ化されたすべての PCC ルールを即座に削除または非アクティブ化します。

PCEF は IP CAN セッションを終了するために、IP CAN 固有の手順を適用します。GPRS の場合、GGSNは、IP-CANセッション全体の終了が要求されたことを示すティアダウンインジケータを設定した PDP 非アクティブ化要求を送信します。さらに、PCEF は「IP CAN セッション終了の表示」の手順を適用します。

サブスクライバがダウンすると、PCRF から取得されたボリュームまたはルール情報は破棄されます。

Gx を介したボリュームレポート

ここでは、3GPP Rel. 9 の Gx を介したボリュームレポート機能について説明します。これは、Rel. 7 の Gx インターフェイスをサポートするすべての製品でサポートされます。

ライセンス要件

Gx を介したボリュームレポートは、シスコのライセンス供与された機能です。別の機能ライセンスが必要になる場合があります。特定のライセンス要件の詳細については、シスコのアカウント担当者にお問い合わせください。ライセンスのインストールと確認の詳細については、『システム管理ガイド』の「ソフトウェア管理操作」の「ライセンスキーの管理」の項を参照してください。

重要 Gx を介した課金機能または Gx を介したボリュームレポート機能に個別のライセンスは必要ありません。この機能は、「ポリシーインターフェイス」ライセンスの一部として有効にすることができます。

サポートされる標準

Gx を介したボリュームレポート機能は、次の標準規格に基づいています。

3GPP TS 29.212 V9.5.0 (2010-06)：3rd Generation Partnership Project、Technical Specification Group Core Network and Terminals、Policy and Charging Control over Gx reference point (Release 9)

機能の概要

Gx を介したボリュームレポート機能により、PCRF はサブスクライバのデータ使用量に基づいてリアルタイムの決定ができます。

重要 Volume Reporting over Gx は、ボリュームクォータにのみ適用されます。

PCEF は、最初からではなく、使用状況監視の最後のレポート以降の累積使用量のみを報告します。

使用量しきい値がゼロ（無限しきい値）に設定されている場合、PCEF によってそれ以上のしきい値イベントは生成されませんが、使用状況の監視は続行され、セッションの終了時に報告されます。

ベアラーの終了時の使用状況レポートと、アップリンク/ダウンリンクレベルのレポートがサポートされています。

次の手順を通じて、Gx を介したボリュームレポートの仕組みについて説明します。

1. PCEF は、PCRF からメッセージを受信した後、使用状況モニタリング関連の AVP を解析し、その情報を IMSA に送信します。
2. IMSA はこの情報で ECS を更新します。

3. PCRF からの使用状況モニタリング情報で ECS が更新されると、PCEF（ECS）はデータ使用状況の追跡を開始します。
4. セッションレベルのモニタリングの場合、ECS がデータ使用状況を保持します。
5. PCC ルールモニタリングの場合、モニタリングキーを一意の識別子として使用状況がモニタリングされます。各ノードがモニタリングキーごとの使用状況情報を保持します。データトラフィックが通過すると、使用量しきい値に照らして使用状況がチェックされ、「使用状況レポート」セクションに説明されているようにして報告されます。
6. PCEF は、しきい値に達した後、PCRF によって新しいしきい値が提供されるまで、データ使用状況を追跡し続けます。使用状況が報告された IP-CAN セッション変更の確認応答で、PCRF から新しい使用量しきい値が提供されない場合、その IP CAN セッションを対象とした PCEF での使用状況モニタリングは続行されません。

使用状況モニタリング

- セッションレベルでの使用状況モニタリング：PCRF は、Granted-Service-Unit AVP に使用量しきい値レベルを設定し、Usage-Monitoring-Level AVP を SESSION_LEVEL(0) に設定して、Usage-Monitoring-Information AVP を送信することで、Gx に関するセッションレベルのボリュームレポートにサブスクライブします。AVP が DPCA によって解析された後、IMSA は情報を ECS に対して更新します。ECS が更新されると、使用状況モニタリングが開始され、データトラフィックが発生するたびに使用量しきい値がチェックされます。セッションレベルでのモニタリングキーがサポートされています。

  PCRF からの 1 つのメッセージでのセッション使用状況の有効化と無効化がサポートされています。この操作は、モニタリングキーがセッションレベルで関連付けられている場合にのみ可能です。

  入力/出力オクテットのしきい値レベルに基づく使用状況のモニタリングがサポートされています。有効になっているしきい値レベルに基づいて使用状況が報告されます。複数のレベルが有効になっている場合は、いずれか 1 つのレベルで侵害が発生しても、有効になっているすべてのレベルについて使用状況が報告されます。モニタリングは、PCRF からの使用状況レポートの応答で欠落しているしきい値レベルで停止されます（PCRF が以前に有効にされた複数のレベルでモニタリングを継続する場合、完全なセットを再度提供することが期待されます）。

  合計しきい値レベルと GSU AVP の UL/DL しきい値レベルの両方が提供された場合はエラーとして扱われ、合計しきい値レベルのみが受け入れられます。

  次の要求がモニタリングキーの使用状況を報告した CCR-U への応答で受信された場合、同じモニタリングキーの追加の CCR-U が生成されます。

  - モニタリングキーを使用したルールレベルでの即時レポート要求
  - モニタリングキーを使用した、または使用しないセッションレベルでの即時レポート要求
  - ルールレベルでの明示的な無効化要求
  - セッションレベルでの明示的な無効化要求

上記のすべての要求がモニタリングキーの使用状況を報告した CCR-U への応答で受信された場合、同じモニタリングキーの追加の CCR-U は生成されません。また、すべてのアクティブなモニタリングキーの使用状況を報告した CCR-U への応答で、ルールレベルのモニタリングキーのない即時レポート要求を受信した場合、追加の CCR-U は生成されません。

- フローレベルの使用状況モニタリング：PCRF は、Granted-Service-Unit AVP に設定された使用量しきい値レベルと PCC_RULE_LEVEL(1) に設定された Usage-Monitoring-Level AVP とともに Usage-Monitoring-Information AVP を送信することで、Gx を介してフローレベルのボリュームレポートに登録します。フローレベルのモニタリングの場合、モニタリングキーは必須です。PCRF がルールとモニタリングキーを関連付ける際や、フローレベルで使用状況モニタリングを有効化または無効化する際に、モニタリングキーを使用して制御できるためです。AVP が DPCA によって解析された後、IMSA は情報を ECS に対して更新します。ECS が更新されると、使用状況モニタリングが開始され、データトラフィックが発生するたびに使用量しきい値がチェックされます。

  使用状況モニタリングは、スタティックルール、定義済みルール、およびダイナミックルール定義に対応しています。

  - スタティックルールの使用状況モニタリング：スタティックルールの場合、モニタリングキーに関連付けられた最後のルール削除に関する使用状況はレポートの対象外になります。この場合、PCRF から使用状況モニタリング情報のみを受信します。
  - 定義済みルールの使用状況モニタリング：事前定義されたルールに対して使用状況モニタリングを有効にする必要がある場合、PCRF は、モニタリングキーと使用量しきい値を含むルールおよび使用状況モニタリング情報を送信します。モニタリングキーは、その事前定義済みルールの PCEF で事前設定されているものと同じである必要があります。同じモニタリングキーに複数のルールを関連付けることができます。そのため、特定のモニタリングキーを有効にすると、同じモニタリングキーを持つ複数のルールのデータが追跡されることになります。AVP が DPCA によって解析された後、IMSA は情報を ECS に対して更新します。ECS が更新されると、使用状況モニタリングが開始され、データトラフィックが発生するたびに使用量しきい値がチェックされます。
  - ダイナミックルールの使用状況モニタリング：ダイナミックルール定義に対して使用状況モニタリングを有効にする必要がある場合、PCRF は課金ルールの定義や使用状況モニタリング情報（モニタリングキー、使用量しきい値など）とともにモニタリングキーを提供します。これにより、そのモニタリングキーに関連付けられているすべてのルールに対して使用状況モニタリングが実行されます。AVP が DPCA によって解析された後、IMSA は情報を ECS に対して更新します。ECS が更新されると、使用状況モニタリングが開始され、データトラフィックが発生するたびに使用量しきい値がチェックされます。ダイナミックルール定義のモニタリングキーは、PCRF によって動的に割り当てられます。これが、使用状況モニタリングのケースにおいて定義済みルールとの唯一の違いです。

複数のモニタリングキーで同時にしきい値違反が発生した場合、最初に 1 つのモニタリングキーの使用状況のみが報告されます。PCRF から正常な応答を受信すると、残りのモニタリン

グキーの使用状況が PCRF に報告されます。Tx 期限切れ/TCP リンクエラーが発生すると、報告されていない使用状況が ECS に保存されます。セッションでその後 PCRF と正常なやり取りがあった場合、報告されていない UMI が PCRF に送信されます。

使用状況レポート

サブスクライバレベルやフローレベルでの使用状況は、次の条件で PCRF に報告されます。

- 使用量しきい値に達した：PCEF はサブスクライバデータの使用量を記録し、PCRF によって指定される使用量しきい値に達しているかどうかを確認します。これは、セッションレベルとルールレベルの両方のレポートで行われます。

  セッションレベルのレポートでは、実際の使用量が、使用量しきい値と比較されます。

  ルールレベルのレポートでは、データトラフィックにヒットするルールを使用して、モニタリングキーが関連付けられているかどうかが確認され、モニタリングキーに基づいてデータ使用量が確認されます。条件が満たされると、使用状況の情報を IMSA に報告し、モニタリングを続行します。IMSA は、「USAGE_REPORT」トリガーが PCRF によって有効になっている場合に、CCR-U をトリガーします。この CCR で、Usage-Monitoring-Information AVP と、サブスクライバのデータ使用量を設定した「Used-Service-Unit」が送信されます。

  使用量しきい値に達したときに、PCRF が使用状況モニタリング情報に PCEF からの CCR による新しい使用量しきい値を提供しない場合、使用状況モニタリングは PCEF で停止し、使用状況は報告されません。

  Gx を介した非標準ボリュームレポートの実装では、しきい値に違反すると使用状況モニタリングが停止します。それ以外の場合はモニタリングが続行されます。CCA が受信されるまで、以降の使用状況は報告されません。

- 使用状況モニタリングが無効：レポートの使用状況、その他の外部トリガー、または PCRF 内部トリガーに関連しない PCEF からの CCR の結果として PCRF により使用状況モニタリングが無効にされた場合には、PCRF が Usage-Monitoring-Support AVP を USAGE_MONITORING_DISABLED に設定して使用状況モニタリングを明示的に無効にすると、PCEF はモニタリングを停止し、（モニタリングが有効だったときの）使用状況情報を PCRF に報告します。使用量しきい値に達したときに、PCRF が PCEF からの CCR による新しい使用量しきい値を提供しない場合、使用状況モニタリングは PCEF で停止し、これ以降の使用状況は報告されません。

- IP CAN セッションの終了：IP CAN セッションが終了すると、サブスクライバの累積使用状況情報が PCEF からの CCR-T で PCRF に報告されます。PCC 使用量レベル情報が PCRF によって有効になっている場合、PCC 使用量も報告されます。

  PCRF は RAR メッセージを使用し、その中に Session-Release-Cause AVP を含めて、IP CAN セッション終了を開始します。ただし、PCRF が CCA メッセージで IP CAN セッションを終了する場合もあります。不要な追加メッセージを回避するために、PCRF は、CCA-U メッセージ自体で、サブスクライバを終了するように P-GW に通知できます。そのため、すべての Gx ディクショナリの CCA メッセージに Session Release Cause が追加されました。

- PCC ルールの削除：PCRF が使用量モニタリングキーに関連付けられている最後の PCC ルールを非アクティブ化すると、PCEF はそのモニタリングキーのデータ使用量を含む CCR を送信します。使用量モニタリングキーに関連付けられている最後の PCC ルールが非アクティブであると PCEF が報告する場合に、CCR コマンドに Charging-Rule-Report AVP が含まれていたなら、PCEF は同じ CCR コマンドでそのモニタリングキーの累積使用量を報告します。あるいは、Charging-Rule-Report AVP が RAA コマンドに含まれている場合、PCEF は新規に CCR コマンドを送信して、使用状況モニタリングキーの累積使用量を報告します。PCRF によって設定された、ルールの非アクティブ化時間を使用した最後のルールの非アクティブ化に関する使用状況レポートがサポートされています。

  PCRF からのメッセージを受信すると、削除対象のルールがマーク付けされ、アクセス側の手順が完了した後にルールが削除されます。

- PCRF 要求使用状況レポート：最後のレポートの送信以降の累積使用量（即時レポートの場合も同様）。即時レポート後に使用量はリセットされ、使用状況モニタリングが続行されます。後続の使用状況レポートには現在のレポート以降の使用量が含まれるようになります。

- ベアラー終了時の使用状況レポートを追加できます。ベアラーが何らかの理由で削除されると、そのベアラーに関連付けられているルールも削除されます。そのため、使用状況は、ベアラー終了が原因で削除された最後のルールが関連ルールであるモニタリングキーで報告されます。

- 再検証のタイムアウト：非標準の実装では、使用状況モニタリングとレポートが有効になっていて、再検証タイムアウトが発生した場合、PCEF は CCR を送信して PCC ルールを要求し、最後のレポート以降（または、使用状況がまだ報告されていない場合には、使用状況レポートが有効になった時点以降）の有効なすべてのモニタリングキーのすべての累積使用量を、IP-CAN セッションレベル（有効な場合）およびサービスデータフローレベル（有効な場合）の累積使用量を使用して報告します。これがデフォルトの動作です。

  標準実装の場合、これは CLI 設定によって有効にする必要があります。

重要 再検証タイムアウト時の使用状況レポート機能は、Gx を介したボリュームレポートの非標準実装ではデフォルトで使用できます。この機能は標準実装で設定可能です。

使用状況が報告されると、使用量カウンタはゼロにリセットされます。PCEF は、しきい値に達した後、PCRF によって新しいしきい値が提供されるまで、データ使用状況の追跡を 0 から継続します。使用状況が報告された IP-CAN セッション変更の確認応答で、PCRF から新しい使用量しきい値が提供されない場合、その IP CAN セッションを対象とした PCEF での使用状況モニタリングは続行されず、CCR-CCA 間の累積使用量は破棄されます。

サーバーの再試行でトリガーされた CCR-U は、サーバーによって付与されたクォータを考慮して、USU を報告します。新たに作成された MSCC の場合、USU を報告するために暫定クォータ設定が取得されます。

Gx を介したボリュームレポート機能を設定する方法については、Gx を介したボリュームレポートの設定 （29 ページ） を参照してください。

Gx を介したボリュームレポート（VoRoGx）のための ICSR サポート

ボリュームのしきい値とボリュームの使用状況はスタンバイシャーシに同期され、スイッチオーバー後の既存セッションの Gx を介したボリュームレポートをサポートします。

このサポートがないと、たとえば適切な使用を強制するためにボリュームレポートを使用した場合に、サブスクライバが想定以上に高い速度を使用する可能性はありません。通信事業者はこれをすでに収益の損失と見なしている可能性があります。また、EUのローミング規制によって設定された制限に達すると、通知を受け取り、ブロック/リダイレクトされるローミングサブスクライバに深刻な影響を及ぼします。セッションがブロックされずにこの時点でセッションが継続する場合、通信事業者は上限を超えたデータに課金することができず、実質的な収益の大幅な損失が発生します（ローミングパートナーはSGSNで使用されるデータに課金する場合があります）。

Rel. 7 Gx の動作

ここでは、GPRS/UMTS ネットワークでの Rel. 7 Gx インターフェイスのサポートにより、サブスクライバのダイナミックポリシーと課金制御がどのように動作するかについて説明します。

次の図と表は、UE により開始される、システムと IMS コンポーネント間の IMSA プロセスについて説明しています。

この例では、Diameter ポリシー制御アプリケーション（DPCA）が PCRF への Gx インターフェイスです。PCRF との IMSA 間のインターフェイスは Gx インターフェイスで、セッションマネージャ（SessMgr）とオンライン課金サービス（OCS）間のインターフェイスは Gy インターフェイスです。IMSA サービスと DPCA はシステムの SessMgr の一部であることに注意してください。分かりやすくするために、図では分離されています。

重要 DPCA と IMSA は、ポリシーサーバーインターフェイスアプリケーション内の 1 つのモジュールとして動作します。

図 *3 : Rel. 7 Gx IMS* 承認コールのフロー

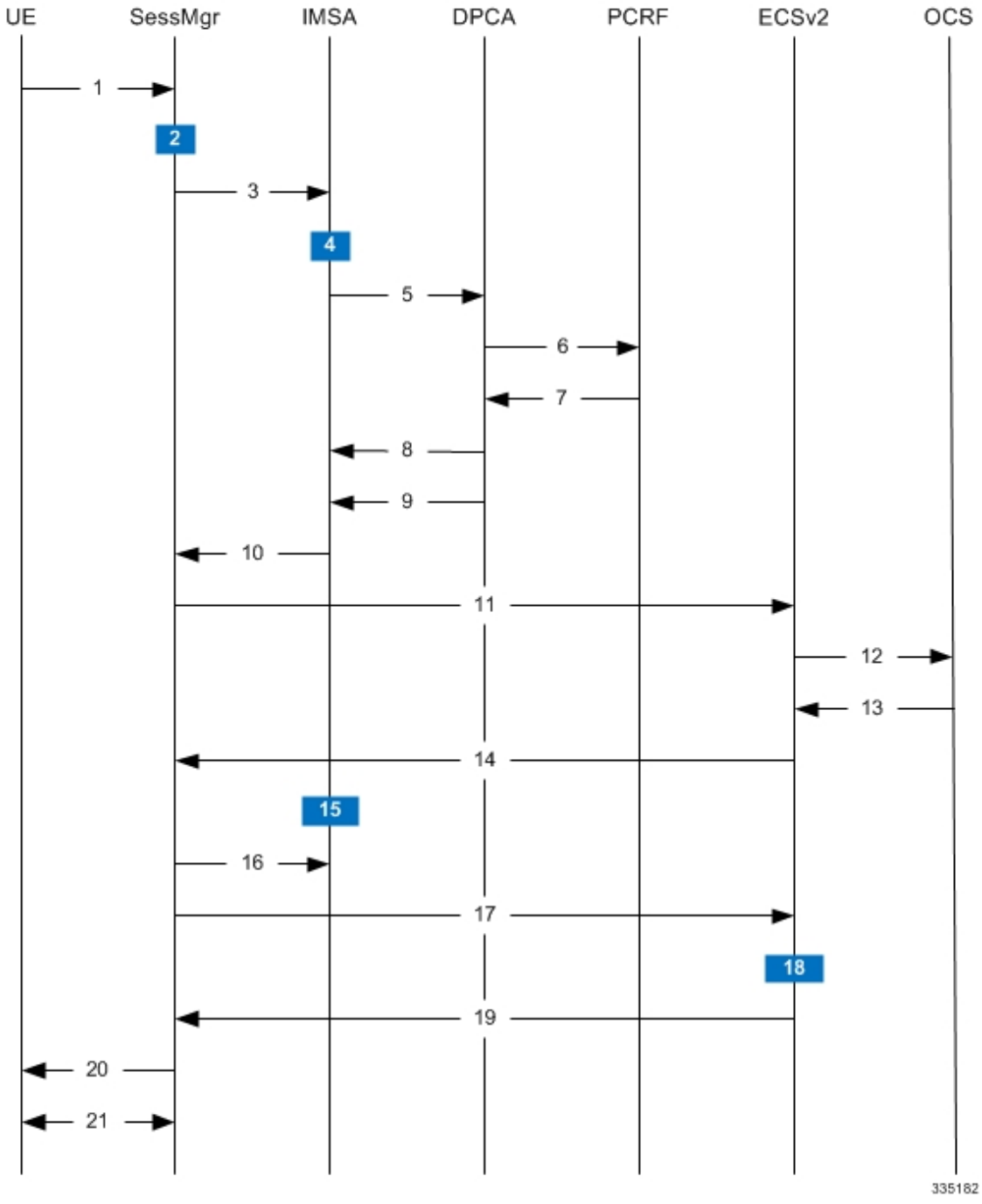


表 *1 : Rel. 7 Gx IMS* 承認コールのフローの説明

ステップ	説明
1	UE（IMS サブスクライバ）が、プライマリ PDP コンテキストのアクティブ化と作成を要求します。
2	SessMgr が UE に IP アドレスを割り当てます。
3	APN に対して IMSA が有効になっている場合、SessMgr は IMS 承認を要求します。
4	IMSA が、IP CAN セッションとベアラーにリソースを割り当て、ユーザーの選択キー（たとえば msisdn）に基づいて接続する PCRF を選択します。
5	IMSA が、DPCA モジュールに対して PCRF に承認要求を発行するよう要求します。
6	DPCA は、選択された PCRF に CCR 初期メッセージを送信します。このメッセージには、PRIMARY に設定された Context-Type AVP、および UE に割り当てられた IP アドレスが含まれます。このメッセージには、GENERAL に設定された Bearer-Usage AVP が含まれている場合があります。Bearer-Operation は Establishment に設定されています。PCRF がベアラーバインディングを行う場合、ベアラー ID が含まれます。
7	汎用 PDP コンテキスト用の事前設定済みルールセットが PCRF で提供されている場合、PCRF は CCA の事前設定済み課金ルールを送信することがあります。PCRF は、ダイナミックルールと承認された QoS パラメータも含める場合があります。
8	DPCA は、課金ルールの定義、課金ルールのインストール、PCRF から受信した QoS 情報、イベントトリガーなどを、PCRF から受信したルールに対応するベアラー ID とともに IMSA に渡します。IMSA が情報を保存します。ベアラー ID が存在せず、PCRF がベアラーバインディングを行う場合、ルールはスキップされます。一方、ベアラー ID が存在せず、PCEF がベアラーバインディングを行う場合、ルールが ECS に渡され、ベアラーバインディングが実行されます。
9	DPCA は、IMSA によって登録されたコールバック関数を呼び出します。
10	IMSA は、ベアラーが承認した QoS 情報を保存し、SessMgr に通知します。その他の PCRF によって提供される、PDP セッション全体に共通の情報（イベントトリガー、プライマリおよびセカンダリ OCS アドレスなど）は IMSA 内に保存されます。IMSA は、情報を処理した後、ポリシー承認が完了したことを SessMgr に通知します。
11	IMSA/DPCA でルールの検証が失敗した場合、Charging-Rule-Report AVP を含む PCRF に失敗が通知されます。それ以外の場合、IMSA が ECS セッションの作成を開始します。APN 名、プライマリおよびセカンダリ OCS サーバーアドレスなどが、SessMgr から ECS に送信されます。
12	ECS は、CC-Request-Type を INITIAL_REQUEST に設定した CCR(I) を OCS に送信してクレジット承認を実行し、クレジット制御セッションを開きます。この要求には、アクティブなルールベース ID（APN と AAA からのデフォルトのルールベース ID）と、GPRS 固有の属性（APN、UMTS QoS など）が含まれます。

ステップ	説明
13	OCS が CCA 初期メッセージを返します。これにより、静的に設定されたルールベースがアクティブ化されることがあります。また、プリエンプティブクォータが含まれていることがあります。
14	ECS が、応答メッセージで SessMgr に応答します。
15	SessMgr が、ダイナミックルールの IMSA を要求します。
16	IMSA がダイナミックルールを SessMgr に送信します。 RAR メッセージは、セッションが確立される前に許可されることに注意してください。 また、ダイナミックルール情報のリカバリとセッションマネージャの監査が進行中の場合は、RAR メッセージが拒否され、結果コード 3002 の RAA が送信されることに注意してください。
17	SessMgr が、ダイナミックルール情報を ECS に送信します。ゲートフローステータス情報およびフローごとの QoS（課金ルール）情報もメッセージで送信されます。
18	ECS は、受け取った事前定義済みルールをアクティブ化し、受け取ったダイナミックルールをインストールします。また、ゲートフローステータスと QoS パラメータが、ダイナミック課金ルールに従い ECS によって更新されます。Gx ルールベースは、ECS の group-of-ruledefs として扱われます。応答メッセージには、ECS でのルールプロビジョニングのステータスを伝達する課金ルールレポートが含まれます。ECS は、ベアラー ID のないルールに対して PCEF ベアラーバインディングを実行します。
19	ルールのプロビジョニングが部分的に失敗した場合、コンテキストセットアップが受け入れられ、失敗したルールの PCC ルールステータスを含む Charging-Rule-Report とともに、新しい CCR-U が PCRF に送信されます。ルールのプロビジョニングが完全に失敗すると、コンテキストセットアップが拒否されます。
20	PDP コンテキスト承認の応答に応じて、SessMgr は応答を UE に送信し、コールをアクティブにするか、拒否します。Charging-Rule-Report にいずれかのルールの部分的な失敗が含まれている場合、PCRF に通知され、コールがアクティブ化されます。Charging-Rule-Report に完全な失敗が含まれている場合、コールは拒否されます。
21	ステップ 18 での PCC ルールの PCEF ベアラーバインドに基づいて、UE を使用した 1 つ以上のネットワーク開始 PDP コンテキスト手順（Network Requested Update PDP Context（NRUPC）/Network Requested Secondary PDP Context Activation（NRSPCA））が行われます。

Rel. 7 Gx インターフェイス

Rel. 7 Gx インターフェイス機能を設定するには、コンテキストレベルで IMS 承認サービスを設定してから、IMS 承認サービスを使用するように APN を設定する必要があります。

Rel. 7 Gx インターフェイスの機能を設定するには、次の手順を実行します。

手順

ステップ 1 「コンテキストレベルでの IMS 承認サービスの設定 （25 ページ）」の説明に従って、GPRS/UMTS ネットワークの IMS サブスクライバの IMS 承認サービスをコンテキストレベルで設定します。

ステップ 2 「設定の確認 （27 ページ）」の説明に従って、設定内容を確認します。

ステップ 3 「APN への IMS 承認サービスの適用 （28 ページ）」の説明に従って、IMS サブスクライバの IMS 承認サービスを使用するように同じコンテキスト内の APN を設定します。

ステップ 4 「サブスクライバ設定の確認 （29 ページ）」の説明に従って、設定内容を確認します。

ステップ 5 オプション：「Gx を介したボリュームレポートの設定 （29 ページ）」の説明に従って、Gx を介したボリュームレポート機能を設定します。

ステップ 6 EXEC モードコマンド **save configuration** を使用して、フラッシュメモリ、外部メモリデバイス、もしくはネットワーク上の場所に設定を保存します。構成ファイルを検証して保存する方法の詳細については、『*System Administration Guide*』および『*Command Line Interface Reference*』を参照してください。

重要
この項の設定例で使用されているコマンドは、最もよく使用されているコマンドまたはその可能性の高いコマンド、および/またはキーワードオプションが提示される範囲で、基本機能を提供します。多くの場合は、他のオプションのコマンドやキーワードオプションを使用できます。すべてのコマンドの詳細については、『*Command Line Interface Reference*』を参照してください。

コンテキストレベルでの IMS 承認サービスの設定

次の例を使用して、GPRS や UMTS ネットワークの IMS サブスクライバの IMS 承認サービスをコンテキストレベルで設定します。

```
configure
     context <context_name>
          ims-auth-service <imsa_service_name>
               p-cscf discovery table { 1 | 2 } algorithm {
ip-address-modulus | msisdn-modulus | round-robin }
               p-cscf table { 1 | 2 } row-precedence <precedence_value> {
 address <ip_address> | ipv6-address <ipv6_address> } [ secondary { address
 <ip_address> | ipv6-address <ipv6_address> } ]
               policy-control
                    diameter origin endpoint <endpoint_name>
                    diameter dictionary <dictionary>
                    diameter request-timeout <timeout_duration>
                   diameter host-select table { { { 1 | 2 } algorithm
 { ip-address-modulus | msisdn-modulus | round-robin } } | prefix-table
 { 1 | 2 } }
                  diameter host-select row-precedence <precedence_value>
 table { { { 1 | 2 } host <host_name> [ realm <realm_id> ] [ secondary host
 <host_name> [ realm <realm_id> ] ] } | { prefix-table { 1 | 2 }
msisdn-prefix-from <msisdn_prefix_from> msisdn-prefix-to <msisdn_prefix_to>
```

```
host <host_name> [ realm <realm_id> ] [ secondary host <sec_host_name> [ realm
 <sec_realm_id> ] algorithm { active-standby | round-robin } ] } } [
-noconfirm ]
                    diameter host-select reselect subscriber-limit
<subscriber_limit> time-interval <duration>
                    failure-handling cc-request-type { any-request |
initial-request | terminate-request | update-request } {
diameter-result-code { any-error | <result_code> [ to <end_result_code> ] }
} { continue | retry-and-terminate | terminate }
                    end
```

注：

- <*context_name*> は、IMS 承認サービスを有効にするコンテキストの名前です。
- <*imsa_service_name*> は、Rel. 7 Gx インターフェイス承認用に設定する IMS 承認サービスの名前です。
- 最大 30 個の IMS 承認サービスプロファイルをシステムに設定できます。
- セカンダリ P-CSCF IP アドレスは、P-CSCF テーブルで設定できます。**p-cscf table** のコマンドの詳細については、『*Command Line Interface Reference*』を参照してください。

  p-cscf table 設定コマンドの構文は次のようになります。

  ```
  p-cscf table { 1 | 2 } row-precedence precedence_value { ipv4-address
  ipv4_address [ ipv6-address ipv6_address ] | ipv6-address ipv6_address [
  ipv4-address ipv4_address ] } [ secondary { ipv4-address ipv4_address [
   ipv6-address ipv6_address ] | ipv6-address ipv6_address [ ipv4-address
   ipv4_address ] } [ weight value ]
  ```

- Rel. 7 Gx インターフェイスのサポートを有効にするには、関連する Diameter ディクショナリを設定する必要があります。使用する具体的な Diameter ディクショナリの詳細については、シスコのアカウント担当者にお問い合わせください。
- MSISDN プレフィックス範囲ベースの PCRF 選択メカニズムを設定する場合

  Gx インターフェイスが一定範囲のサブスクライバの特定の PCRF に接続できるようにするには、**msisdn-prefix-from** <*msisdn_prefix_from*> と **msisdn-prefix-to** <*msisdn_prefix_to*> に、それぞれ開始 MSISDN と終了 MSISDN を設定します。

  Gx インターフェイスが特定のサブスクライバの特定の PCRF に接続できるようにするには、**msisdn-prefix-from** <*msisdn_prefix_from*> と **msisdn-prefix-to** <*msisdn_prefix_to*> の両方に同じ MSISDN を設定します。

  MSISDN プレフィックス範囲テーブルには、最大 128 行まで追加できます。

  MSISDN の範囲は、各行間で重ならないようにする必要があります。
- PCRF 選択のためのラウンドロビンアルゴリズムは、多数の PCRF を選択する場合にのみ効果的であり、細かいレベルでの効果は薄いです。
- オプション：サブスクライバの Quality of Service（QoS）更新タイムアウトを設定するには、IMS 承認サービス コンフィギュレーション モードで次のコマンドを入力します。

- オプション：シグナリング制限を設定するには、IMS 承認サービス コンフィギュレーション モードで次のコマンドを入力します。

  signaling-flag { deny | permit }

  signaling-flow permit server-address <*ip_address*> **[server-port {** <*port_number*> **| range** <*start_number*> **to** <*end_number*> **}] [description** <*string*> **]**

- オプション：汎用 PDP コンテキストでどのポリシーゲートにも一致しないパケットに対するアクションを設定するには、IMS 承認サービス コンフィギュレーション モードで次のコマンドを入力します。

  traffic-policy general-pdp-context no-matching-gates direction { downlink | uplink } { forward | discard }

- GGSN および PCEF で設定される PCRF ホスト宛先を設定するには、**diameter host-select** CLI コマンドを使用します。

- Gx が失敗したときに事前に定義されたルールを使用するように GGSN および PCEF を設定するには、**failure-handling cc-request-type** CLI を **continue** に設定します。使用可能または使用中のポリシーは引き続き使用され、PCRF とのそれ以上の連携はありません。

- デフォルトの課金方法のプロビジョニングには、次の設定を使用します。この場合、AVP のオンラインとオフラインは、設定に基づいてCCR-I メッセージで送信されます。コマンドレベルで受信した Online または Offline AVP は、PCC ルールレベルで設定されていない場合、ダイナミックルールにのみ適用されます。

  - オンラインの有効化を送信するには、次の設定を使用します。

    configure

    active-charging service <*ecs_service_name*>

    charging-action <*charging_action_name*>

    cca charging credit

    exit

  - オフラインの有効化を送信するには、次の設定を使用します。

    configure

    active-charging service <*ecs_service_name*>

    rulebase <*rulebase_name*>

    billing-records rf

    exit

設定の確認

IMS 承認サービスの設定を確認するには、次の手順を実行します。

手順

ステップ 1 次のコマンドを入力して、IMS 承認サービスを有効にしたコンテキストに変更します。

```
context <context_name>
```

ステップ 2 次のコマンドを入力して、サブスクライバの IMS 承認サービスの設定を確認します。

```
show ims-authorization service name <imsa_service_name>
```

APN への IMS 承認サービスの適用

コンテキストレベルで IMS 承認サービスを設定したら、IMS サブスクライバに IMS 承認サービスを使用するように APN を設定する必要があります。

次の例を使用して、Rel. 7 Gx インターフェイス （24 ページ） で説明されているように設定されたコンテキスト内で、以前に設定された APN に IMS 承認サービス機能を適用します。

```
configure
   context <context_name>
      apn <apn_name>
         ims-auth-service <imsa_service_name>
         active-charging rulebase <rulebase_name>
         end
```

注：

- <*context_name*> は、IMS 承認サービスが設定されたコンテキストの名前です。
- <*imsa_service_name*> は、コンテキストで IMS 認証用に設定された IMS 承認サービスの名前です。
- Rel. 7 Gx の場合、ECS ルールベースは APN で設定する必要があります。
- ECS では、PCEF バインディングシナリオの場合に Gx を介してルールベースを変更できます。古いルールベースがなくなると、そのルールベースからインストールされていたすべてのルールが削除されます。これにより、ルールなしで残されたいくつかのベアラー（PDP コンテキスト）が終了する可能性があります。ルールベースを変更する Gx メッセージがあり、このメッセージにより事前定義済みの一部のルールもアクティブ化される場合、ルールベースの変更が最初に行われ、新しいルールベースのルールがアクティブ化されます。また、ルールベースはコール全体に適用されます。1 つのコール内のすべての PDP コンテキスト（ベアラー）で、同じ ECS ルールベースが使用されます。
- ECS で構成された事前定義済みルールの場合、ダイナミックまたは事前定義済みルールの MBR と GBR は、PCEF バインディングに使用される前にチェックされます。すべてのルール（ダイナミックおよび事前定義済み）には、MBR が関連付けられている必要があります。GBR QCI を含むすべてのルールには、GBR も設定されている必要があります。そのため、事前定義済みルールでは、QCI が GBR QCI または非 GBR QCI のいずれであるかに

応じて、適切なピークデータレート、認定データレートを設定する必要があります。詳細については、ACS課金アクション コンフィギュレーション モードで**flow limit-for-bandwidth** CLI コマンドを参照してください。

- PCRF からの Gx ルールベース（Charging-Rule-Base-Name AVP）を ECS の group-of-ruledefs として解釈するには、アクティブ課金サービス コンフィギュレーション モードで次のコマンドを設定します。

  policy-control charging-rule-base-name active-charging-group-of-ruledefs

サブスクライバ設定の確認

次のコマンドを入力して、サブスクライバの IMS 承認サーバーの設定を確認します。

show subscribers ims-auth-service <*imsa_service_name*>

<*imsa_service_name*> は、IMS 認証用に設定された IMS 承認サービスの名前です。

Gx を介したボリュームレポートの設定

ここでは、Gxを介したボリュームレポートを有効にするのに必要な設定について説明します。

Gx を介したボリュームレポートを有効にするには、次の設定コマンドを使用します。

```
configure
     active-charging service <ecs_service_name>
          rulebase <rulebase_name>
             action priority <priority> dynamic-only ruledef <ruledef_name>
 charging-action <charging_action_name> monitoring-key <monitoring_key>
                exit
          exit
     context <context_name>
          ims-auth-service <imsa_service_name>
               policy-control
                    event-update send-usage-report [ reset-usage ]
                    end
```

注：

- PCEF が受け入れる最大モニタリングキー値は 4294967295 です。PCEF がより大きい値を送信すると、値は符号なし整数値に変換されます。
- **event-update** CLI を使用すると、イベントの更新時にボリューム使用状況レポートを有効にできます。オプションキーワード **reset-usage** を使用すると、差分レポートをサポートできます。このレポートでは、使用状況が報告され、PCEF でリセットされます。このオプションが設定されていない場合、イベント更新の一部として使用状況の情報を送信しますが、PCEF でリセットすることはしません。

統計情報の収集

ここでは、Rel. 7 Gx の統計と設定情報を収集する方法について説明します。

次の表では、最初の列に、収集する統計が示されており、2 つ目の列に、実行するアクションが示されています。

表 *2 : Rel. 7 Gx* 統計と情報の収集

統計/情報	実行するアクション
IMS 承認サービスのポリシー制御に固有の情報と統計。	**show ims-authorization policy-control statistics**
IMS 承認サービスに使用される、承認サーバーに固有の情報と統計。	**show ims-authorization servers ims-auth-service**
すべての IMS 承認サービスの情報。	**show ims-authorization service all**
IMS 承認サービスの統計。	**show ims-authorization service statistics**
IMS 承認サービスでアクティブなセッションの情報、設定、統計。	**show ims-authorization sessions all**
IMS 承認サービスでアクティブなセッションの完全な情報、設定、統計。	**show ims-authorization sessions full**
IMS 承認サービスでアクティブなセッションの要約情報。	**show ims-authorization sessions summary**
アクティブな課金サービスセッションの完全な統計。	**show active-charging sessions full**
サービスに設定されているすべてのルール定義に関する情報。	**show active-charging ruledef all**
システムに設定されているすべてのルールベースに関する情報。	**show active-charging rulebase all**
システムに設定されているすべての ruledef グループに関する情報。	**show active-charging group-of-ruledefs all**

Rel. 8 Gx インターフェイス

Rel. 8 Gx インターフェイスのサポートは、Cisco ASR シャーシで使用できます。

ここでは、次の内容について説明します。

• HA/PDSN Rel. 8 Gx インターフェイスのサポート （31 ページ）
• P-GW Rel. 8 Gx インターフェイスのサポート （49 ページ）

HA/PDSN Rel. 8 Gx インターフェイスのサポート

ここでは、CDMA ネットワークのサブスクライバに対してポリシーおよび課金制御をサポートするための、HA および PDSN 用 Rel. 8 Gx インターフェイスの設定について説明します

IMS サービスは、アクセスサポートとは無関係に、音声、ビデオ、およびデータの転送に関するアプリケーションサポートを提供します。CDMA ネットワーク内のローミング IMS サブスクライバには、他の機能とは別に、必要十分で中断のない一貫性のあるシームレスなユーザーエクスペリエンスがアプリケーションセッション中に必要になります。また、使用されている特定の IMS アプリケーションによって消費されるリソースの料金のみがサブスクライバに請求されることも重要です。

ここに記載する手順を実行する前に、本アドミニストレーション ガイドの説明に従って、お使いのサービスモデルに最適な設定例を選択し、そのモデルに必要な要素を設定することを推奨します。

ここでは、次の内容について説明します。

はじめに

CDMA ネットワークでの IMS 展開の場合、システムは、ポリシーベースのアドミッションコントロールのサポートおよびフローベース課金（FBC）に Rel. 8 Gx インターフェイスを使用します。Rel. 8 Gx インターフェイスは、ゲート設定、帯域幅制限などのポリシー制御適用機能をサポートし、FBC もサポートします。これは、動的にプロビジョニングされたポリシー制御および課金（PCC）ルールによって実現されます。これらの PCC ルールは、サービスデータフロー（SDF）を識別し、課金を実行するために使用されます。ルールに関連付けられているその他のパラメータは、ポリシー制御を適用するために使用されます。

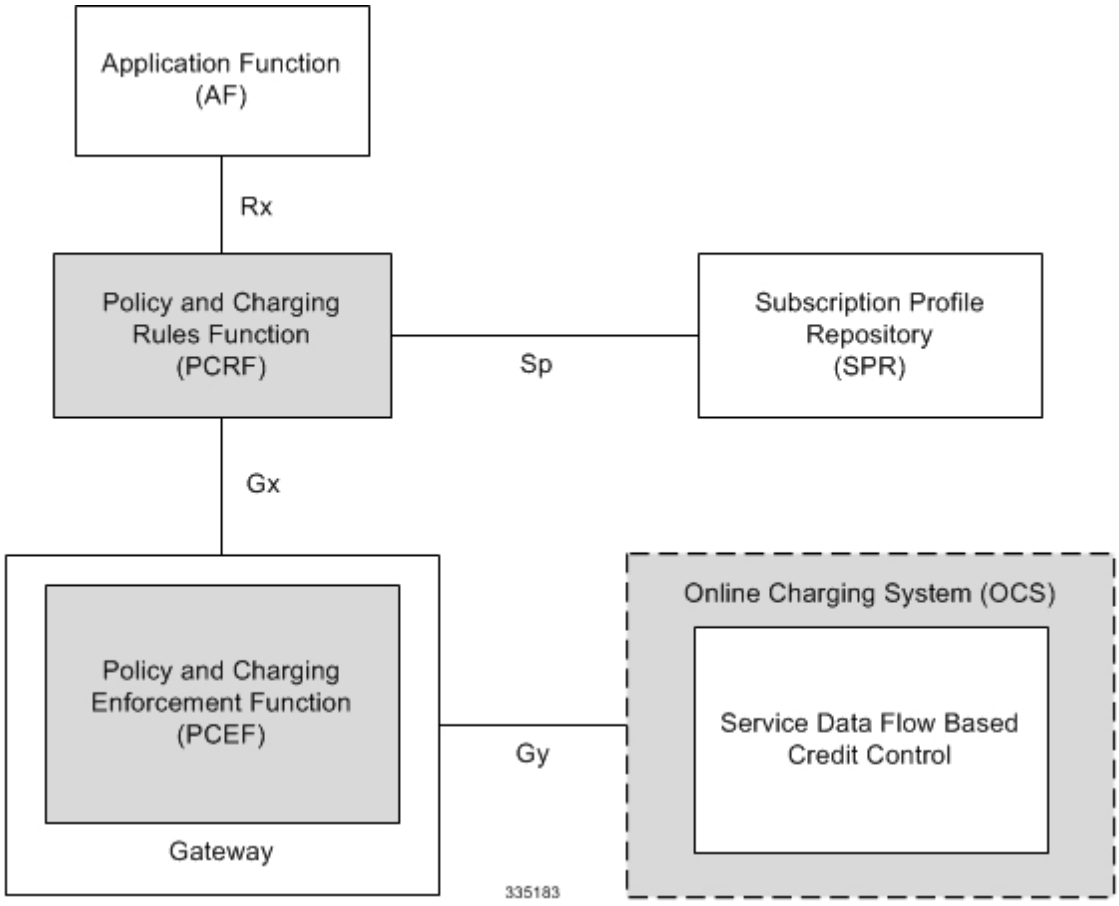
PCC アーキテクチャにより、オペレータは、サービスベースの QoS ポリシーと FBC 制御を実行できます。PCC アーキテクチャでは、これは主にポリシーおよび課金適用機能（PCEF）/HA/PDSN とポリシーおよび課金ルール機能（PCRF）によって実現されます。クライアント機能は HA/PDSN に付属しているため、IMS 承認（IMSA）シナリオではゲートウェイとも呼ばれます。PCEF 機能は、Enhanced Charging Service（ECS）により提供されます。Gx インターフェイスは、Diameter 接続として導入されます。Gx メッセージには、ほとんどの場合、ダイナミックルールのインストール/変更/削除と、事前定義されたルールのアクティブ化/非アクティブ化が含まれます。

Gx 参照ポイントは、ゲートウェイ/PCEF と PCRF の間にあります。この参照ポイントは、PCRF からゲートウェイ/PCEF への PCC ルールのプロビジョニングと削除、およびゲートウェイ/PCEF から PCRF へのトラフィック プレーン イベントの送信に使用されます。Gx 参照ポイントは、

アプリケーションに関連する AVP を適用することで、課金制御とポリシー制御のいずれかまたは両方に使用できます。

次の図は、ポリシーおよび課金アーキテクチャに含まれる要素間の参照ポイントを示します。

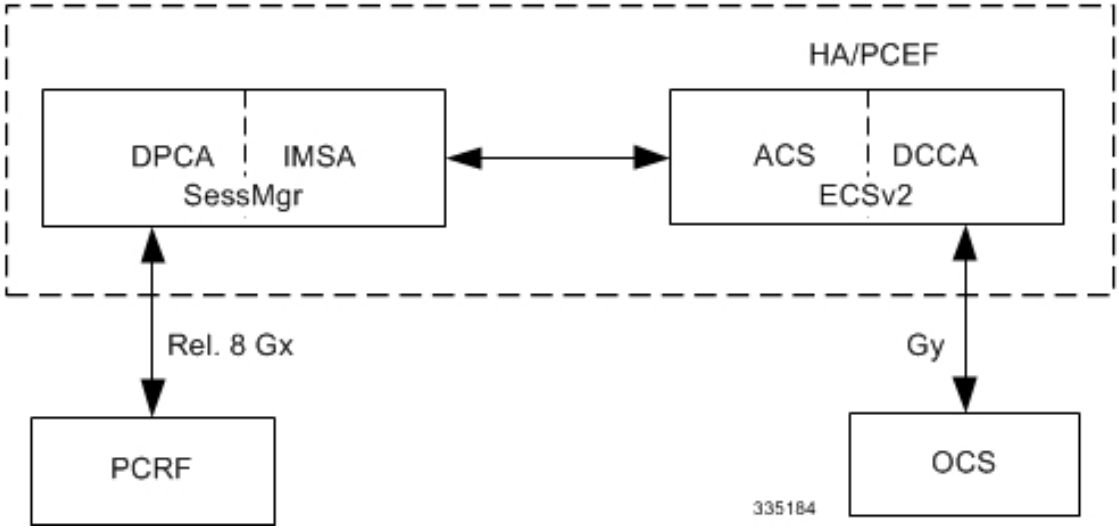
図 *4 : HA/PDSN Rel. 8 Gx PCC* 論理アーキテクチャ



ゲートウェイ内では、IMSA モジュールと DPCA モジュールが（SessMgr で）Gx プロトコル関連の機能を処理し、ポリシーの適用と課金は ECS で行われます。Gy プロトコル関連の機能は、DCCA モジュール内（ECS）で処理されます。

次の図は、ゲートウェイ内のコンポーネント間の連携動作を示しています。

図 *5 : HA/PDSN Rel. 8 Gx PCC* アーキテクチャ（*PCEF* 内）



ライセンス要件

HA/PDSN Rel. 8 Gx インターフェイスのサポートは、ライセンス供与されたシスコの機能です。別の機能ライセンスが必要になる場合があります。特定のライセンス要件の詳細については、シスコのアカウント担当者にお問い合わせください。ライセンスのインストールと確認の詳細については、『システム管理ガイド』の「ソフトウェア管理操作」の「ライセンスキーの管理」の項を参照してください。

サポートされる標準

HA/PDSN Rel 8. Gx インターフェイスのサポートは、次の標準と RFC に基づいています。

- 3GPP TS 23.203 V8.3.0 (2008-09) 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Policy and charging control architecture (Release 8)
- 3GPP TS 29.212 V8.6.0 (2009-12) 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control over Gx reference point (Release 8)
- 3GPP TS 29.213 V8.1.1 (2008-10) 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control signalling flows and QoS parameter mapping; (Release 8)
- RFC 3588、Diameter Base Protocol。2003 年 9 月
- RFC 4006、Diameter Credit-Control Application。2005 年 8 月

用語および定義

このセクションでは、HA/PDSN Rel. 8 Gx に関連した機能と用語について説明します。

ポリシー制御

PCRF が IP-CAN セッションの制御方法を PCEF に指示するプロセスです。

ポリシー制御は、次の機能で構成されます。

- バインディング
- ゲート制御
- イベントレポート
- QoS 制御
- その他の機能

バインディング

HA/PDSN Rel. 8 Gx の実装では、MIP セッション内にベアラーがないため、IP-CAN ベアラーの概念が適用されません。承認済みの IP-CAN セッションのみが適用されます。

ゲート制御

ゲート制御とは、SDF に属するパケットが目的のエンドポイントに向かってパススルーすることをブロックまたは許可することです。ゲートは PCC ルール内で記述され、ゲート制御は SDF ごとに適用されます。ゲートを開閉するコマンドを実行すると、対応する IP パケットの経路が有効または無効になります。ゲートが閉じられている場合、関連する IP フローのすべてのパケットがドロップされます。ゲートが開いている場合、関連する IP フローのパケットの転送が許可されます。

イベントレポート

重要 PCEF が要求していない場合の PCRF から PCEF へのイベントトリガーの無条件レポートはサポートされていません。

重要 HA/PDSN Rel. 8 Gx の実装では、AN_GW_CHANGE (21) イベントトリガーのみサポートされます。

イベントレポートは、ユーザープレーンでの新しい動作をトリガーするアプリケーションイベントの通知とこうしたイベントへの応答、およびゲートウェイ（PCEF）のリソースに関連したイベントのレポートです。イベントトリガーを使用して、どの IP-CAN セッション変更や特定のイベントが発生すると、PCEF が PCC ルールを再要求するかを確認できます。PCEF から PCRF へのイベントトリガーレポート、およびイベントトリガーのプロビジョニングは、IP-CAN セッションレベルで行われます。

PCEF にあるイベントレポート機能（ERF）は、PCC ルールのプロビジョニング中に PCRF からイベントトリガーを受信し、イベントトリガー検出を実行します。受信したイベントトリガーに一致するイベントが発生すると、ERF は発生したイベントを PCRF に報告します。提示されたイベントトリガーが特定のパラメータ値に関連付けられている場合、ERF はそれらの値を PCRF への応答に含めます。

QoS 制御

重要 HA/PDSN Rel. 8 Gx の実装では、承認済みの IP-CAN セッションのみがサポートされます。IP-CAN ベアラーごとの承認済み QoS のプロビジョニング、QCI ごとの承認済み QoS のポリシー適用、および混合モードでの承認済み QoS の範囲の調整は、適用されません。

QoS 制御とは、SDF に許可される最大 QoS の承認と適用のことです。複数の SDF の集約の場合、個々の SDF の承認済み QoS 情報の組み合わせが、この集約の承認済み QoS として提供されます。SDF ごとの QoS 制御により、PCC アーキテクチャは、特定の SDF ごとに適用される承認済み QoS を PCEF に提供できます。

QoS 承認情報は、PCRF によって動的にプロビジョニングされる場合と、PCEF で事前定義された PCC ルールである場合があります。PCEF 内の事前定義された PCC ルールの場合、承認された QoS 情報は PCC ルールがアクティブになると有効になります。PCEF では、承認済み QoS 情報のさまざまなセット（PCRF から受信した情報と、事前定義された PCC ルールに対応する情報）が組み合わされます。PCRF は、事前定義された PCC ルールの承認済み QoS 情報を認識し、それらのルールをアクティブ化する際に、この情報を考慮します。これにより、PCRF によってアクティブ化される一連の PCC ルールの組み合わせによる承認済み QoS が、それらの PCC ルールが動的に提供されるか、事前定義されているか、またはその両方であるかに関係なく、サブスクリプションポリシーとオペレータポリシーによって指定された制限内に収まることが保証されます。

サポートする機能は次のとおりです。

- 承認済み QoS のプロビジョニングとポリシー適用：PCRF は PCEF に承認済み QoS を提供する場合があります。承認済み QoS は、適用されるリソースの適切な値を提供します。
- SDF ごとの承認済み QoS のポリシープロビジョニング：SDF ごとの承認済み QoS のプロビジョニングは、PCC ルールのプロビジョニング手順の一部です。
- SDF ごとの承認済み QoS のポリシー適用：承認済み QoS が PCC ルールに対して定義されている場合、PCEF は、その PCC ルールに対応する SDF のデータレートを、PCC ルールに対して承認済みの最大帯域幅を超えないように制限します（制限を超えるパケットを破棄します）。
- PCC ルールを非アクティブ化または削除すると、PCEF は、その PCC ルール用に予約されていたリソースを解放します。

その他の機能

ここでは、他のいくつかの機能について説明します。

PCC ルールエラーの処理

1 つ以上の PCC ルールのインストールまたはアクティブ化が失敗した場合、PCEF は、影響を受ける PCC ルールの CCR または RAA コマンドのいずれかに 1 つまたは複数の Charging-Rule-Report AVP を含めることで、PCRF にエラーを通知します。PCEF は、各 Charging-Rule-Report AVP 内に、1 つ以上の Charging-Rule-Name AVP または

Charging-Rule-Base-Name AVP を追加することによってエラーの発生した PCC ルールを示し、Rule-Failure-Code AVP を追加することによってエラーの理由コードを示し、また PCC-Rule-Status AVP を追加します。

1つまたは複数の新しいPCCルール（以前は正しくインストールされていなかったルール）のインストールまたはアクティブ化が失敗した場合、PCEF はプッシュモードとプルモードの両方で PCC-Rule-Status を INACTIVE に設定します。

PCC ルールが正常にインストールまたはアクティブ化されたが、PCEF によって適用できなくなった場合、PCEF は PCRF に新しい CCR コマンドを送信し、Charging-Rule-Report AVP を追加します。PCEF は、Charging-Rule-Report AVP 内に Rule-Failure-Code AVP を追加し、PCC-Rule-Status を INACTIVE に設定します。

GnGp HO シナリオ中にコリジョンが発生すると、CCR-U が生成され、ルールエラーを報告するために PCRF に送信されます。

この追加の Gx メッセージ（CCR-U）がトリガーされると、RAT_TYPE トリガーが有効になっている場合、複数の CCR-U を設定する必要が生じます。 設定しない場合、HO 中にコリジョンが発生するたびにサブスクライバコールがドロップされます。

HA/PDSN の Gx 実装では、以下のルール障害コードがサポートされています。

- RATING_GROUP_ERROR（2）
- SERVICE_IDENTIFIER_ERROR（3）
- GW/PCEF_MALFUNCTION（4）
- RESOURCES_LIMITATION（5）

RAR 手順において1つ以上のPCCルールのインストールまたはアクティブ化が失敗した場合、Experimental-Result-Code AVP が DIAMETER_PCC_RULE_EVENT（5142）に設定された RAA コマンドが送信されます。

時刻プロシージャ

PCEF は、PCRF の指示に従って PCC ルール要求を実行します。再検証時間が PCRF によって設定されると、PCEF は PCRF との通信をトリガーし、確立された IP-CAN セッションに関する PCC ルールを PCRF に要求します。PCEF が REVALIDATION_TIMEOUT イベントをトリガーすると、PCEF はタイマーを停止します。

PCC ルールがインストールされている場合、非アクティブ状態です。Rule-Activation-Time / Rule-Deactivation-Time が指定されている場合、PCEF はその時間が経過した後にルールをアクティブまたは非アクティブに設定します。

CCA/RAR で Rule-Deactivation-Time AVP が省略されている場合、この AVP の以前の値は無効になります。新しい動作は、Gx の 3GPP 仕様、バージョン 12.1.0 に準拠しています。

PCRF が Rule-Deactivation-Time AVP なしで RAR/CCA-U で同じ事前定義済みルールを再度有効にすると、このルールの deactivation-time は削除されます。

以前の動作に切り替える場合、PCRF は PCRF メッセージ（RAR、CCA-U）で、predef-rule 名と一緒に Rule-Deactivation-Time AVP と同じ値を再送信する必要があります。

（注） この動作変更は、事前に定義したルールにのみ適用されます。

Gx 上のファイアウォールポリシーのサポート

Diameter AVP「SN-Firewall-Policy」が Diameter ダイナミックディクショナリに追加され、Gx インターフェイスでファイアウォールポリシーをサポートできるようになりました。この AVP は CCA-I メッセージにエンコードされ、APN 設定を介して PDP コンテキストに静的に割り当てられた、またはRADIUS の Access-Accept を介して動的に割り当てられた fw-and-nat ポリシーを適用/上書きできます。この AVP は、任意の CCA-U または RAR メッセージ内で解析することも可能です。これにより、現在 PDP コンテキストに割り当てられている fw-and-nat ポリシーを変更できます。

課金制御

重要 HA/PDSN Rel. 8 Gx の実装において、オフライン課金はサポートされていません。

課金制御は、SDF に属するパケットを課金キーに関連付け、必要に応じてオンライン課金を適用するプロセスです。FBC は、SDF のリアルタイム分析に基づいて、ベアラー使用量の差別化された課金を処理します。課金制御を可能にするために、PCC ルールの情報によって SDF が識別され、課金制御のパラメータが指定されます。PCC ルール情報は、サブスクリプションデータに依存する場合があります。

オンライン課金は Gy インターフェイスを介してサポートされます。オンライン課金の場合、PCEF イベント時にオンライン課金アクションを適用できます（たとえば、QoS 変更時の再承認など）。

PCC ルールでは課金システムとの連携が不要であること、つまりこの SDF のアカウンティングもクレジット制御も実行せず、その後オンライン課金もオフライン課金も実行されないことを PCEF に示すことができます。

サポートされる機能：

- IP-CAN セッションの課金関連情報のプロビジョニング
- 課金アドレスのプロビジョニング：プライマリまたはセカンダリイベント課金機能名（オンライン課金サーバー（OCS）アドレス）

重要 HA/PDSN Rel. 8 Gx の実装において、Gx を介したプライマリまたはセカンダリ課金収集機能名（オフライン課金サーバー（OFCS）アドレス）のプロビジョニングはサポートされていません。

- デフォルトの課金方法のプロビジョニング：このリリースでは、デフォルトの課金方法は CCR-I メッセージで送信されます。この場合、新しい AVP オンラインおよびオフラインが、設定に基づいて CCR-I メッセージで送信されます。コマンドレベルで受信した Online

または Offline AVP は、PCC ルールレベルで設定されていない場合、ダイナミックルールにのみ適用されます。

課金の相関

HA/PDSN Rel. 8 Gx の実装では、課金の相関はサポートされていません。PCRF は、IMS セッションで IP フローを一意に識別するフロー識別子を提供します。

ポリシーおよび課金制御（PCC）ルール

PCC ルールにより、SDF の検出が可能になり、ポリシー制御や課金制御のパラメータが提供されます。PCC ルールの目的は次のとおりです。

- PCC ルールの SDF フィルタ（パケットルールに一致）に基づいて、アップリンク IP フローとダウンリンク IP フローの両方のケースで、SDF に属するパケットを検出します。

  パケットと一致する PCC ルールがない場合、パケットはドロップされます。

- SDF が提供するサービスを特定します。
- SDF に適用可能な課金パラメータを指定します。
- SDF のポリシー制御を提供します。

PCEF は PCC ルールの優先順位に従って、PCC ルールの SDF フィルタと照らし合わせて受信パケットを評価し、受信パケットごとに PCC ルールを選択します。パケットが SDF フィルタに一致すると、そのパケットの照合プロセスが完了し、そのフィルタの PCC ルールが適用されます。

PCC ルールには次の 2 種類があります。

- ダイナミック PCC ルール：Gx インターフェイスを介して PCEF に動的にプロビジョニングされるルール。この PCC ルールは事前に定義することも、PCRF で動的に生成することもできます。ダイナミック PCC ルールは任意のタイミングでアクティブ化、変更、および非アクティブ化できます。
- 定義済み PCC ルール：通信事業者によって PCEF で事前設定されたルール。定義済み PCC ルールは、PCRF が任意のタイミングでアクティブ化または非アクティブ化できます。PCEF 内の定義済み PCC ルールをグループ化すると、PCRF は Gx 参照ポイント上で一連の PCC ルールを動的にアクティブ化できます。

重要 3 番目のルールであるスタティック PCC ルールは、通信事業者によってシャーシに事前設定できます。スタティック PCC ルールは、PCRF で明示的に認識されておらず、PCRF の制御下にありません。スタティック PCC ルールは、Gx で制御されない汎用ベアラーにバインドされます。

PCC ルールの構成は次のとおりです。

- ルール名：PCEF と PCRF 間の通信で PCC ルールを参照するために使用されます。

- サービス識別子：SDF が関連するサービスやサービスコンポーネントを識別するために使用されます。
- サービス データ フロー フィルタ：サービスフローフィルタは、ルールを適用するトラフィックの選択に使用されます。
- 優先順位：SDF フィルタが重複しているさまざまな PCC ルールでは、ルールの優先順位によって、どのルールが適用されるかが決まります。ダイナミック PCC ルールと定義済み PCC ルールの優先順位が同じ場合は、ダイナミック PCC ルールが優先されます。
- ゲートステータス：SDF フィルタによって検出された SDF がアップリンク方向またはダウンリンク方向で通過するか（ゲートが開いている）、または破棄されるか（ゲートが閉じている）かを示します。
- QoS パラメータ：QoS 情報には、QoS クラス識別子（SDF の認定された QoS クラス）と、アップリンクおよびダウンリンクの認定ビットレートが含まれます。
- 課金キー（料金設定グループ）
- その他の課金パラメータ：課金パラメータは、オンライン課金インターフェイスを使用するかどうか、どのレベルで PCEF がルールに関連する使用状況を報告するかなどを定義します。

重要 ダイナミック PCC ルールの計測方式とレポートレベルの設定はサポートされていません。

アプリケーション機能（AF）が Rx インターフェイスを介してこの情報を提供した場合、PCC ルールにはアプリケーションとベアラーレイヤー間の課金相関を有効にするための AF レコード情報も含まれます。IMS の場合は、IMS 課金識別子（ICID）とフロー識別子が含まれます。

重要 ASR 5500 は、Gx メッセージのダイナミック課金ルールごとのフロー説明を含む 8 つのフロー情報のみをサポートします。

セッションマネージャがクラッシュした場合、最大 24 の PCC ルールを ICSR 後に回復できます。

回復可能な PCC ルールの制限が増加しても、ルールが失われることはないため、エンドユーザーに適用される課金は影響を受けません。

保留状態の PCC ルールの変更が受信されると、変更されたパラメータは P-GW でバッファに保存されます。保留中の要求に対する応答をアクセスネットワークから受信した後、P-GW はバッファされたパラメータの変更を処理し、必要に応じてネットワークに対する別の更新要求を生成します。

Gx 参照ポイントを介した PCC 手順

PCC ルールの要求

PCEF は、Gx 参照ポイントを使用して、次の場合に PCC ルールを要求します。

- IP-CAN セッションの確立時
- IP-CAN セッションの変更時

PCC ルールは、イベントトリガーを求めずに、PCC ルールのインストール/アクティブ化または適用の失敗の結果として要求することもできます。

PCC ルールのプロビジョニング

PCRF は、Rel. 8 Gx 参照ポイントを介して、PCEF で適用される PCC ルールを示します。これは、次のいずれかの手順で行われます。

- プル（PCEF により要請されたプロビジョニング）：PCEF による PCC ルールの要求に応じて、PCRF は CC-Answer で PCC ルールをプロビジョニングします。
- プッシュ（要請のないプロビジョニング）：PCRF は、PCEF からの要求を取得せずに PCC ルールのプロビジョニングを決定することがあります。たとえば、Rx 参照ポイントを介して PCRF に提供された情報への応答、または PCRF 内の内部トリガーへの応答。PCEF からの要請なしに PCC ルールをプロビジョニングするために、PCRF はこれらの PCC ルールを RA 要求メッセージに含めます。この RA 要求によってトリガーされる CCR および CCA メッセージはありません。

PCEF からの要求ごとに、または要請のないプロビジョニング時に、PCRF は 0 個以上の PCC ルールをプロビジョニングします。PCRF は、次のいずれかの方法で単一の PCC ルールに対する操作を実行できます。

- PCEF で事前定義された PCC ルールをアクティブ化または非アクティブ化する場合、PCRF は、Charging-Rule-Name AVP 内でこの PCC ルールへの参照をプロビジョニングし、Charging-Rule-Install AVP または Charging-Rule-Name AVP のいずれかを選択して必要なアクションを提示します。
- PCRF によりプロビジョニングされた PCC ルールをインストールまたは変更する場合、PCRF は、Charging-Rule-Install AVP 内で対応する Charging-Rule-Definition AVP をプロビジョニングします。
- 以前に PCRF によってプロビジョニングされた PCC ルールを削除する場合、PCRF は、このルールの名前を Charging-Rule-Remove AVP 内の Charging-Rule-Name AVP の値にしてプロビジョニングします。

重要 課金ルール名の最大長は 63 バイトです。課金ルール名の長さが 63 バイトを超える場合、Rule-Failure-Code が RESOURCES_LIMITATION の課金ルールレポートが送信されます。この課金ルールレポートは、ルール名の長さが 128 文字未満の場合にのみ送信されます。課金ルール名の長さが 128 文字以上の場合、課金ルールレポートは送信されません。

セッションの接続中、P-GW は、同じ CCR-U にルールの失敗とクレジットの不足を組み合わせて PCRF に送信します。

アップリンク IP パケットの PCC ルールの選択

PCC が有効になっている場合、PCEF は、PCC ルールの優先順位に従い、IP CAN セッションの PCRF が提供するアクティブな PCC ルールまたは事前定義済みのアクティブな PCC ルールのアップリンク SDF フィルタを使用してパケットを評価することで、IP CAN セッション内の受信アップリンク IP パケットそれぞれに適用する PCC ルールを選択します。

重要 PCRF が提供する PCC ルールと事前定義された PCC ルールが同じ優先順位を持つ場合、PCRF が提供する PCC ルールのアップリンク SDF フィルタが最初に適用されます。

パケットが SDF フィルタに一致すると、そのパケットの照合プロセスが完了し、そのフィルタの PCC ルールが適用されます。対応する IP CAN セッションのいずれの PCC ルールにも一致しないアップリンク IP パケットは廃棄されます。

ダウンリンク IP パケットの PCC ルールの選択

PCC が有効になっている場合、PCEF は、PCC ルールの優先順位に従い、IP-CAN セッションの PCRF が提供するアクティブな PCC ルールまたは事前定義済みのアクティブな PCC ルールのダウンリンク SDF フィルタを使用してパケットを評価することで、IP-CAN セッション内の受信ダウンリンク IP パケットそれぞれに適用する PCC ルールを選択します。

重要 PCRF が提供する PCC ルールと事前定義された PCC ルールが同じ優先順位を持つ場合、PCRF が提供する PCC ルールのダウンリンク SDF フィルタが最初に適用されます。

パケットが SDF フィルタに一致すると、そのパケットの照合プロセスが完了し、そのフィルタの PCC ルールが適用されます。IP-CAN セッションのいずれの PCC ルールにも一致しないダウンリンク IP パケットは廃棄されます。

次の手順もサポートされています。

- IP-CAN セッション終了の表示：IP-CAN セッションが終了している場合、PCEF は PCRF に接続します。
- IP-CAN セッション終了の要求：内部トリガーまたは SPR からのトリガーにより PCRF が IP-CAN セッションの終了を決定した場合、PCRF は PCEF に通知します。PCEF は PCRF

に確認応答し、その IP-CAN セッションで以前にインストールまたはアクティブ化されたすべての PCC ルールを即座に削除または非アクティブ化します。

PCEF は IP-CAN セッションを終了するために、IP-CAN 固有の手順を適用します。HA または PDSN は、IP-CAN セッション全体の終了が要求されたことを示すティアダウンインジケータを設定した MIP 失効要求を送信します。さらに、PCEF は「IP-CAN セッション終了の表示」の手順を適用します。

- セッション確立中に Supported-Features AVP を使用して、送信元ホストがサポートする必須機能とオプション機能について宛先ホストに通知します。

機能の仕組み

このセクションでは、HA/PDSN Rel. 8 Gx インターフェイスサポートの仕組みについて説明します。

次の図と表は、UE により開始される、システムと IMS コンポーネント間の IMS 承認プロセスについて説明しています。

この例では、Diameter ポリシー制御アプリケーション（DPCA）が PCRF への Gx インターフェイスです。PCRF との IMSA 間のインターフェイスは Gx インターフェイスで、セッションマネージャ（SessMgr）とオンライン課金サービス（OCS）間のインターフェイスは Gy インターフェイスです。IMSA サービスと DPCA はシステムの SessMgr の一部であることに注意してください。分かりやすくするために、図では分離されています。

重要 DPCA と IMSA は、ポリシーサーバーインターフェイスアプリケーション内の 1 つのモジュールとして動作します。

図 *6 : HA/PDSN Rel. 8 Gx IMS* 承認コールのフロー

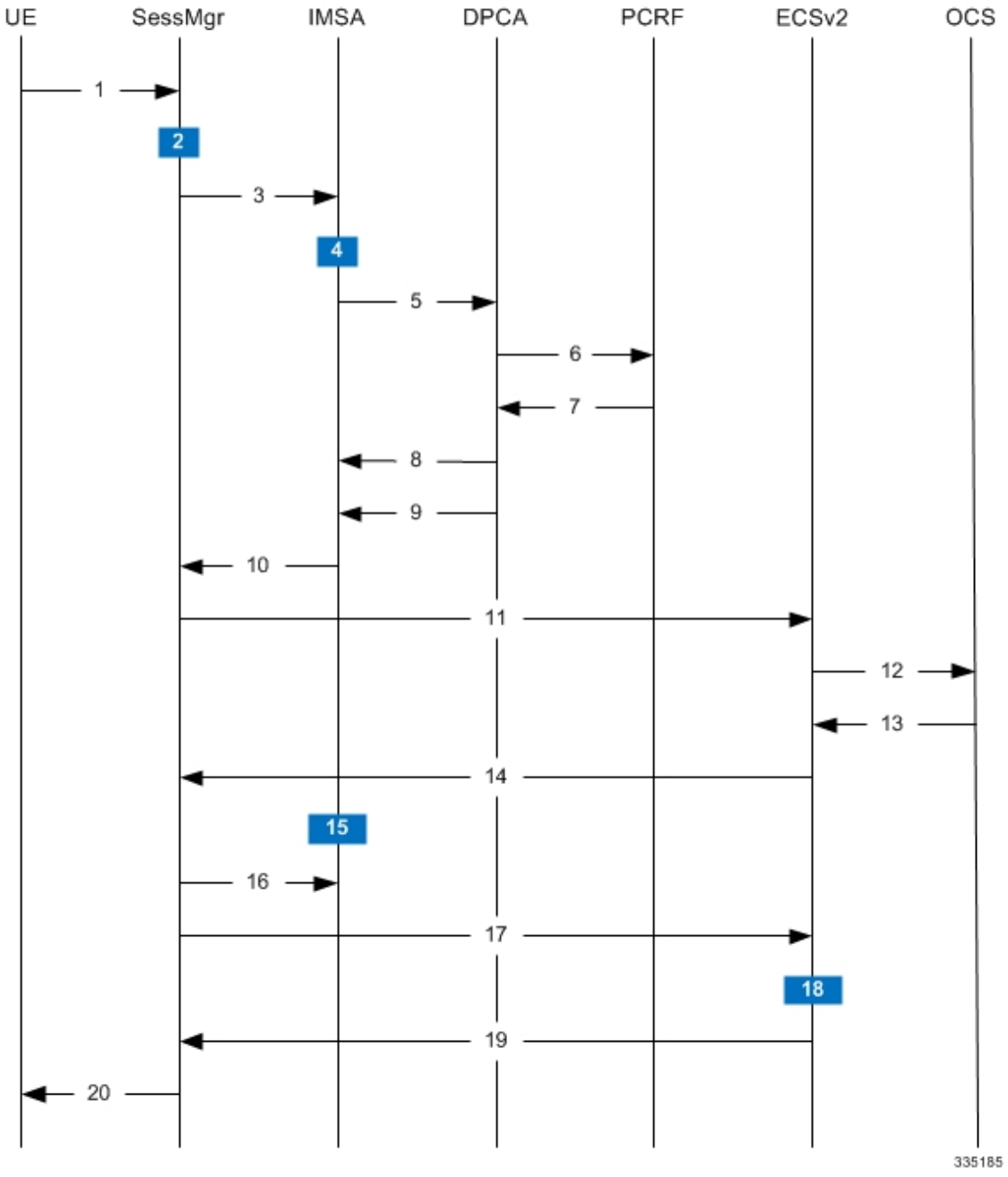


表 *3 : HA/PDSN Rel. 8 Gx IMS* 承認コールのフローの説明

ステップ	説明
1	UE（IMS サブスクライバ）が MIP 登録要求を要求します。
2	SessMgr が UE に IP アドレスを割り当てます。

ステップ	説明
3	サブスクライバに対して IMSA が有効になっている場合、SessMgr は IMS 承認を要求します。 IMSA サービスは、サブスクライバテンプレートで設定できます。または AAA から受け取ることもできます。
4	IMSA が、IP-CAN セッションにリソースを割り当て、ユーザーの選択キー（たとえば round-robin）に基づいて接続する PCRF を選択します。
5	IMSA が、DPCA モジュールに対して PCRF に承認要求を発行するよう要求します。
6	DPCA は、選択された PCRF に CCR 初期メッセージを送信します。
7	PCRF は、事前設定された課金ルールを CCA で送信できます。PCRF は、ダイナミックルールと承認された QoS パラメータも含める場合があります。
8	DPCA は、課金ルールの定義、課金ルールのインストール、PCRF から受信した QoS 情報、イベントトリガーなどを渡します。この情報は IMSA によって保存されます。
9	DPCA は、IMSA によって登録されたコールバック関数を呼び出します。
10	IP-CAN セッション全体に共通の PCRF 提供情報（イベントトリガー、プライマリ/セカンダリ OCS アドレスなど）は IMSA 内に保存されます。IMSA は、情報を処理した後、ポリシー承認が完了したことを SessMgr に通知します。
11	IMSA/DPCA でルールの検証が失敗した場合、Charging-Rule-Report AVP を含む PCRF に失敗が通知されます。それ以外の場合、IMSA が ECS セッションの作成を開始します。プライマリ/セカンダリ OCS サーバーアドレスなどが、SessMgr から ECS に送信されます。
12	ECS は、CC-Request-Type を INITIAL_REQUEST に設定した CCR(I) を OCS に送信してクレジット承認を実行し、クレジット制御セッションを開きます。この要求には、アクティブな Rulebase-Id（AAA からのデフォルトのルールベース ID）が含まれています。
13	OCS が CCA 初期メッセージを返します。これにより、静的に設定されたルールベースがアクティブ化されることがあります。また、プリエンプティブクォータが含まれていることがあります。
14	ECS が、応答メッセージで SessMgr に応答します。
15	SessMgr が、ダイナミックルールの IMSA を要求します。
16	IMSA がダイナミックルールを SessMgr に送信します。 RAR メッセージは、セッションが確立される前に許可されます。 また、ダイナミックルール情報のリカバリとセッションマネージャの監査が進行中の場合は、RAR メッセージが拒否され、結果コード 3002 の RAA が送信されることに注意してください。

ステップ	説明
17	SessMgr が、ダイナミックルール情報を ECS に送信します。ゲートフローステータス情報およびフローごとの QoS（課金ルール）情報もメッセージで送信されます。
18	ECS は、受け取った事前定義済みルールをアクティブ化し、受け取ったダイナミックルールをインストールします。また、ゲートフローステータスと QoS パラメータが、ダイナミック課金ルールに従い ECS によって更新されます。Gx ルールベースは、ECS の group-of-ruledefs として扱われます。応答メッセージには、ECS でのルールプロビジョニングのステータスを伝達する課金ルールレポートが含まれます。
19	ルールのプロビジョニングが部分的に失敗した場合、コンテキストセットアップが受け入れられ、失敗したルールの PCC ルールステータスを含む Charging-Rule-Report とともに、新しい CCR-U が PCRF に送信されます。ルールのプロビジョニングが完全に失敗すると、コンテキストセットアップが拒否されます。
20	MIP セッション承認の応答に応じて、SessMgr は応答を UE に送信し、コールをアクティブにするか、拒否します。Charging-Rule-Report にいずれかのルールの部分的な失敗が含まれている場合、PCRF に通知され、コールがアクティブ化されます。Charging-Rule-Report に完全な失敗が含まれている場合、コールは拒否されます。

HA/PDSN Rel. 8 Gx インターフェイスのサポート

HA/PDSN Rel. 8 Gx インターフェイスの機能を設定するには、次の手順を実行します。

1. コンテキストレベルでの IMS 承認サービスの設定 （46 ページ）の説明に従って、コンテキストレベルで IMS サブスクライバの IMSA サービスを設定します。
2. 同じコンテキスト内で、サブスクライバテンプレートへの IMS 承認サービスの適用 （47 ページ）の説明に従って、IMSA サービスを使用するためのサブスクライバテンプレートを設定します。
3. Exec モードコマンド **save configuration** を使用して、フラッシュメモリ、外部メモリデバイス、および/またはネットワークの場所に設定を保存します。構成ファイルを検証して保存する方法の詳細については、『*System Administration Guide*』および『*Command Line Interface Reference*』を参照してください。

重要 この項の設定例で使用されているコマンドは、最もよく使用されているコマンドまたはその可能性の高いコマンド、および/またはキーワードオプションが提示される範囲で、基本機能を提供します。多くの場合は、他のオプションのコマンドやキーワードオプションを使用できます。すべてのコマンドの詳細については、『*Command Line Interface Reference*』を参照してください。

コンテキストレベルでの IMS 承認サービスの設定

コンテキストレベルで IMS サブスクライバの IMSA サービスを設定するには、次の例に示すコマンドを使用します。

```
configure
     context <context_name>
          ims-auth-service <imsa_service_name>
               policy-control
                    diameter origin endpoint <endpoint_name>
                    diameter dictionary <dictionary>
                    diameter request-timeout <timeout_duration>
                    diameter host-select table { 1 | 2 } algorithm
round-robin
                   diameter host-select row-precedence <precedence_value>
 table { 1 | 2 } host <primary_host_name> [ realm <primary_realm_id> ] [
secondary host <secondary_host_name> [ realm <secondary_realm_id> ] ] [
-noconfirm ]
                    failure-handling cc-request-type { any-request |
initial-request | terminate-request | update-request } {
diameter-result-code { any-error | <result_code> [ to <end_result_code> ] }
} { continue | retry-and-terminate | terminate }
                    exit
               exit
          diameter endpoint <endpoint_name> [ -noconfirm ]
               origin realm <realm_name>
               use-proxy
               origin host <host_name> address <ip_address>
               no watchdog-timeout
               response-timeout <timeout_duration>
               connection timeout <timeout_duration>
               connection retry-timeout <timeout_duration>
              peer <primary_peer_name> [ realm <primary_realm_name> ] address
 <ip_address> [ port <port_number> ]
             peer <secondary_peer_name> [ realm <secondary_realm_name> ] address
 <ip_address> [ port <port_number> ]
               end
```

注：

- <*context_name*> は、IMSA サービスを有効にするコンテキストの名前です。
- <*imsa_service_name*> は、リリース8 Gx インターフェイス認証用に設定する IMSA サービスの名前です。
- 最大 30 個の IMS 承認サービスプロファイルをシステムに設定できます。
- Rel. 8 Gx インターフェイスのサポートを有効にするには、関連する Diameter ディクショナリを設定する必要があります。使用する具体的な Diameter ディクショナリの詳細については、シスコのアカウント担当者にお問い合わせください。
- PCRF 選択のためのラウンドロビンアルゴリズムは、多数の PCRF を選択する場合にのみ効果的であり、細かいレベルでの効果は薄いです。

- PCEF で設定される PCRF ホスト宛先を設定するには、**diameter host-select** CLI コマンドを使用します。
- Gx が失敗したときに事前に定義されたルールを使用するように PCEF を設定するには、**failure-handling cc-request-type** CLI を **continue** に設定します。使用可能または使用中のポリシーは引き続き使用され、PCRF とのそれ以上の連携はありません。

IMSA サービス設定の確認

IMSA サービスの設定を確認するには、次のコマンドを実行します。

1. IMSA サービスを有効にしたコンテキストに変更するには、次のコマンドを入力します。

   context <*context_name*>

2. 次のコマンドを入力して、IMSA サービスの設定を確認します。

   show ims-authorization service name <*imsa_service_name*>

サブスクライバテンプレートへの IMS 承認サービスの適用

コンテキストレベルで IMSA サービスを設定した後、同じコンテキスト内で、IMS サブスクライバに対して IMSA サービスを使用するようにサブスクライバテンプレートを設定する必要があります。

次の例を使用して、「コンテキストレベルでの IMS 承認サービスの設定 （46 ページ）」で説明されているように設定されたコンテキスト内のサブスクライバテンプレートに IMSA サービス機能を適用します。

```
configure
   context <context_name>
      subscriber default
         encrypted password <encrypted_password>
         ims-auth-service <imsa_service_name>
         ip access-group <access_group_name> in
         ip access-group <access_group_name> out
         ip context-name <context_name>
         mobile-ip home-agent <ip_address>
         active-charging rulebase <rulebase_name>
         end
```

注：

- <*context_name*> は、IMSA サービスが設定されたコンテキストの名前である必要があります。
- <*imsa_service_name*> は、コンテキストで IMS 認証用に設定された IMSA サービスの名前である必要があります。
- サブスクライバテンプレートで ECS ルールベースを設定する必要があります。

- PCRF からの Gx ルールベース（Charging-Rule-Base-Name AVP）を ECS の group-of-ruledefs として解釈するには、アクティブ課金サービス コンフィギュレーション モードで次のコマンドを設定します。

  policy-control charging-rule-base-name active-charging-group-of- ruledefs

サブスクライバ設定の確認

Exec CLI コンフィギュレーション モードで次のコマンドを入力して、サブスクライバの IMSA サービスの設定を確認します。

show subscribers ims-auth-service <*imsa_service_name*>

注：

- <*imsa_service_name*> は、IMS 認証用に設定された IMSA サービスの名前にする必要があります。

統計情報の収集

ここでは、Rel. 8 Gx の統計と設定情報を収集する方法について説明します。

次の表では、最初の列に、収集する統計が示されており、2 つ目の列に、実行するアクションが示されています。

表 *4 : HA/PDSN* リリース *8 Gx* の統計と情報の収集

統計/情報	実行するアクション
IMS 承認サービスのポリシー制御に固有の情報と統計。	**show ims-authorization policy-control statistics**
IMS 承認サービスに使用される、承認サーバーに固有の情報と統計。	**show ims-authorization servers ims-auth-service**
すべての IMS 承認サービスの情報。	**show ims-authorization service all**
IMS 承認サービスの統計。	**show ims-authorization service statistics**
IMS 承認サービスでアクティブなセッションの情報、設定、統計。	**show ims-authorization sessions all**
IMS 承認サービスでアクティブなセッションの完全な情報、設定、統計。	**show ims-authorization sessions full**
IMS 承認サービスでアクティブなセッションの要約情報。	**show ims-authorization sessions summary**
アクティブな課金サービスセッションの完全な統計。	**show active-charging sessions full**

統計/情報	実行するアクション
サービスに設定されているすべてのルール定義に関する情報。	**show active-charging ruledef all**
システムに設定されているすべてのルールベースに関する情報。	**show active-charging rulebase all**
システムに設定されているすべての ruledef グループに関する情報。	**show active-charging group-of-ruledefs all**

P-GW Rel. 8 Gx インターフェイスのサポート

はじめに

Gx 参照ポイントは、パケットデータネットワーク（PDN）ゲートウェイ（P-GW）上のポリシーおよび課金ルール機能（PCRF）とポリシーおよび課金適用機能（PCEF）の間にあります。Gx 参照ポイントは、PCRF から PCEF への PCC ルールのプロビジョニングと削除、および PCEF から PCRF へのトラフィック プレーン イベントの送信に使用されます。Gx 参照ポイントは、アプリケーションに関連する AVP を適用することで、課金制御とポリシー制御のいずれかまたは両方に使用できます。

PCEF は、ポリシーの適用とフローベースの課金機能を包含する機能要素です。この機能エンティティは P-GW にあります。これには、以下の主要な機能があります。

- ゲートウェイでのユーザー プレーン トラフィックの処理とその QoS の制御。
- サービスデータフローの検出とカウント、およびオンラインとオフラインの課金操作。
- ポリシー制御されているサービスデータフローの場合、PCEF は、対応するゲートウェイが開いている場合にのみ、サービスデータフローがゲートウェイを通過するのを許可します。
- 課金制御されているサービスデータフローの場合、PCEF は、対応するアクティブな PCC ルールがあり、オンライン課金で OCS がその課金キーで該当するクレジットを承認した場合にのみ、サービスデータフローがゲートウェイを通過するのを許可します。
- PCRF から要求された場合、PCEF は関連するサービスデータフローのステータスが変わったときに PCRF に報告します。
- SDF が BBERF でトンネリングされている場合、PCEF は、IP-CAN セッションの確立時のサービスデータフローのモビリティ プロトコル トンネリング ヘッダーについて PCRF に通知します。

用語および定義

このセクションでは、Rel. 8 Gx に関連した機能と用語について説明します。

Gx を介したボリュームレポート

ここでは、3GPP Rel. 9 の Gx を介したボリュームレポート機能について説明します。

ライセンス要件

Gx を介したボリュームレポートは、シスコのライセンス供与された機能です。別の機能ライセンスが必要になる場合があります。特定のライセンス要件の詳細については、シスコのアカウント担当者にお問い合わせください。ライセンスのインストールと確認の詳細については、『システム管理ガイド』の「ソフトウェア管理操作」の「ライセンスキーの管理」の項を参照してください。

重要 Gxを介した課金機能またはGxを介したボリュームレポート機能に個別のライセンスは必要ありません。この機能は、「ポリシーインターフェイス」ライセンスの一部として有効にすることができます。

サポートされる標準

Gx を介したボリュームレポート機能は、次の標準規格に基づいています。

3GPP TS 29.212 V9.5.0 (2010-06)：3rd Generation Partnership Project、Technical Specification Group Core Network and Terminals、Policy and Charging Control over Gx reference point (Release 9)

機能の概要

Gxを介したボリュームレポート機能により、PCRFはサブスクライバのデータ使用量に基づいてリアルタイムの決定ができます。

重要 Volume Reporting over Gx は、ボリュームクォータにのみ適用されます。

ボリュームレポートは、合計データ使用量レポートとアップリンク/ダウンリンクレベルのレポートの両方をサポートします。

PCEF は、最初からではなく、使用状況監視の最後のレポート以降の累積使用量のみを報告します。

使用量しきい値がゼロ（無限しきい値）に設定されている場合、PCEF によってそれ以上のしきい値イベントは生成されませんが、使用状況の監視は続行され、セッションの終了時に報告されます。

ベアラーの終了時の使用状況レポートがサポートされています。

次の手順を通じて、Gx を介したボリュームレポートの仕組みについて説明します。

1. PCEF は、PCRF からメッセージを受信した後、使用状況モニタリング関連の AVP を解析し、その情報を IMSA に送信します。
2. IMSA はこの情報で ECS を更新します。

3. PCRF からの使用状況モニタリング情報で ECS が更新されると、PCEF（ECS）はデータ使用状況の追跡を開始します。
4. セッションレベルのモニタリングの場合、ECS がデータ使用状況を保持します。
5. PCC ルールモニタリングの場合、モニタリングキーを一意の識別子として使用状況がモニタリングされます。各ノードがモニタリングキーごとの使用状況情報を保持します。データトラフィックが通過すると、使用量しきい値に照らして使用状況がチェックされ、「使用状況レポート」セクションに説明されているようにして報告されます。
6. PCEF は、しきい値に達した後、PCRF によって新しいしきい値が提供されるまで、データ使用状況を追跡し続けます。使用状況が報告された IP-CAN セッション変更の確認応答で、PCRF から新しい使用量しきい値が提供されない場合、その IP CAN セッションを対象とした PCEF での使用状況モニタリングは続行されません。

使用状況モニタリング

- セッションレベルでの使用状況モニタリング：PCRF は、Granted-Service-Unit AVP に使用量しきい値レベルを設定し、Usage-Monitoring-Level AVP を SESSION_LEVEL(0) に設定して、Usage-Monitoring-Information AVP を送信することで、Gx に関するセッションレベルのボリュームレポートにサブスクライブします。AVP が DPCA によって解析された後、IMSA は情報を ECS に対して更新します。ECS が更新されると、使用状況モニタリングが開始され、データトラフィックが発生するたびに使用量しきい値がチェックされます。PCRF は、セッションレベルでモニタリングキーをサポートしています。

  PCRF では、単一のメッセージでセッションの使用状況を有効または無効にすることができます。この操作は、モニタリングキーがセッションレベルで関連付けられている場合にのみ可能です。

  PCRF では、入力/出力オクテットのしきい値レベルに基づき使用状況をモニタリングできます。有効になっているしきい値レベルに基づいて使用状況が報告されます。複数のレベルが有効になっている場合は、いずれか1つのレベルで侵害が発生しても、有効になっているすべてのレベルについて使用状況が報告されます。モニタリングは、PCRF からの使用状況レポートの応答で欠落しているしきい値レベルで停止されます（PCRF が以前に有効にされた複数のレベルでモニタリングを継続する場合、完全なセットを再度提供することが期待されます）。

  合計しきい値レベルと GSU AVP の UL/DL しきい値レベルの両方が提供された場合はエラーとして扱われ、合計しきい値レベルのみが受け入れられます。

  次の要求がモニタリングキーの使用状況を報告した CCR-U への応答で受信された場合、同じモニタリングキーの追加の CCR-U が生成されます。

  - モニタリングキーを使用したルールレベルでの即時レポート要求
  - モニタリングキーを使用した、または使用しないセッションレベルでの即時レポート要求
  - ルールレベルでの明示的な無効化要求
  - セッションレベルでの明示的な無効化要求

上記のすべての要求がモニタリングキーの使用状況を報告した CCR-U への応答で受信された場合、同じモニタリングキーの追加の CCR-U は生成されません。また、すべてのアクティブなモニタリングキーの使用状況を報告した CCR-U への応答で、ルールレベルのモニタリングキーのない即時レポート要求を受信した場合、追加の CCR-U は生成されません。

- フローレベルの使用状況モニタリング：PCRF は、Granted-Service-Unit AVP に設定された使用量しきい値レベルと PCC_RULE_LEVEL(1) に設定された Usage-Monitoring-Level AVP とともに Usage-Monitoring-Information AVP を送信することで、Gx を介してフローレベルのボリュームレポートに登録します。フローレベルのモニタリングの場合、モニタリングキーは必須です。PCRF がルールとモニタリングキーを関連付ける際や、フローレベルで使用状況モニタリングを有効化または無効化する際に、モニタリングキーを使用して制御できるためです。AVP が DPCA によって解析された後、IMSA は情報を ECS に対して更新します。ECS が更新されると、使用状況モニタリングが開始され、データトラフィックが発生するたびに使用量しきい値がチェックされます。

  使用状況モニタリングは、スタティックルール、定義済みルール、およびダイナミックルール定義に対応しています。

  - スタティックルールの使用状況モニタリング：スタティックルールの場合、モニタリングキーに関連付けられた最後のルール削除に関する使用状況はレポートの対象外になります。この場合、PCRF から使用状況モニタリング情報のみを受信します。
  - 定義済みルールの使用状況モニタリング：事前定義されたルールに対して使用状況モニタリングを有効にする必要がある場合、PCRF は、モニタリングキーと使用量しきい値を含むルールおよび使用状況モニタリング情報を送信します。モニタリングキーは、その事前定義済みルールの PCEF で事前設定されているものと同じである必要があります。同じモニタリングキーに複数のルールを関連付けることができます。そのため、特定のモニタリングキーを有効にすると、同じモニタリングキーを持つ複数のルールのデータが追跡されることになります。AVP が DPCA によって解析された後、IMSA は情報を ECS に対して更新します。ECS が更新されると、使用状況モニタリングが開始され、データトラフィックが発生するたびに使用量しきい値がチェックされます。
  - ダイナミックルールの使用状況モニタリング：ダイナミックルール定義に対して使用状況モニタリングを有効にする必要がある場合、PCRF は課金ルールの定義や使用状況モニタリング情報（モニタリングキー、使用量しきい値など）とともにモニタリングキーを提供します。これにより、そのモニタリングキーに関連付けられているすべてのルールに対して使用状況モニタリングが実行されます。AVP が DPCA によって解析された後、IMSA は情報を ECS に対して更新します。ECS が更新されると、使用状況モニタリングが開始され、データトラフィックが発生するたびに使用量しきい値がチェックされます。ダイナミックルール定義のモニタリングキーは、PCRF によって動的に割り当てられます。これが、使用状況モニタリングのケースにおいて定義済みルールとの唯一の違いです。

モニタリングキーの 1 つの使用状況だけが最初に報告されます。PCRF から正常な応答を受信すると、残りのモニタリングキーの使用状況が PCRF に報告されます。Tx 期限切れ/TCP リン

クエラーが発生すると、報告されていない使用状況が ECS に保存されます。セッションでその後 PCRF と正常なやり取りがあった場合、報告されていない UMI が PCRF に送信されます。

使用状況レポート

サブスクライバレベルやフローレベルでの使用状況は、次の条件で PCRF に報告されます。

- 使用量しきい値に達した：PCEF はサブスクライバデータの使用量を記録し、PCRF によって指定される使用量しきい値に達しているかどうかを確認します。これは、セッションレベルとルールレベルの両方のレポートで行われます。

  セッションレベルのレポートでは、実際の使用量が、使用量しきい値と比較されます。

  ルールレベルのレポートでは、データトラフィックにヒットするルールを使用して、モニタリングキーが関連付けられているかどうかが確認され、モニタリングキーに基づいてデータ使用量が確認されます。条件が満たされると、使用状況の情報を IMSA に報告し、モニタリングを続行します。IMSA は、「USAGE_REPORT」トリガーが PCRF によって有効になっている場合に、CCR-U をトリガーします。この CCR で、Usage-Monitoring-Information AVP と、サブスクライバのデータ使用量を設定した「Used-Service-Unit」が送信されます。

  使用量しきい値に達したときに、PCRF が使用状況モニタリング情報に PCEF からの CCR による新しい使用量しきい値を提供しない場合、使用状況モニタリングは PCEF で停止し、使用状況は報告されません。

  Gx を介した非標準ボリュームレポートの実装では、しきい値に違反すると使用状況モニタリングが停止します。それ以外の場合はモニタリングが続行されます。CCA が受信されるまで、以降の使用状況は報告されません。

- 使用状況モニタリングが無効：レポートの使用状況、その他の外部トリガー、または PCRF 内部トリガーに関連しない PCEF からの CCR の結果として PCRF により使用状況モニタリングが無効にされた場合には、PCRF が Usage-Monitoring-Support AVP を USAGE_MONITORING_DISABLED に設定して使用状況モニタリングを明示的に無効にすると、PCEF はモニタリングを停止し、（モニタリングが有効だったときの）使用状況情報を PCRF に報告します。使用量しきい値に達したときに、PCRF が PCEF からの CCR による新しい使用量しきい値を提供しない場合、使用状況モニタリングは PCEF で停止し、これ以降の使用状況は報告されません。

- IP CAN セッションの終了：IP CAN セッションが終了すると、サブスクライバの累積使用状況情報が PCEF からの CCR-T で PCRF に報告されます。PCC 使用量レベル情報が PCRF によって有効になっている場合、PCC 使用量も報告されます。

  PCRF は RAR メッセージを使用し、その中に Session-Release-Cause AVP を含めて、IP CAN セッション終了を開始します。ただし、PCRF が CCA メッセージで IP CAN セッションを終了する場合もあります。不要な追加メッセージを回避するために、PCRF は、CCA-U メッセージ自体で、サブスクライバを終了するように P-GW に通知できます。そのため、すべての Gx ディクショナリの CCA メッセージに Session Release Cause が追加されました。

- PCC ルールの削除：PCRF が使用量モニタリングキーに関連付けられている最後の PCC ルールを非アクティブ化すると、PCEF はそのモニタリングキーのデータ使用量を含む CCR を送信します。使用量モニタリングキーに関連付けられている最後の PCC ルールが非アクティブであると PCEF が報告する場合に、CCR コマンドに Charging-Rule-Report AVP が含まれていたなら、PCEF は同じ CCR コマンドでそのモニタリングキーの累積使用量を報告します。あるいは、Charging-Rule-Report AVP が RAA コマンドに含まれている場合、PCEF は新規に CCR コマンドを送信して、使用状況モニタリングキーの累積使用量を報告します。PCRF によって設定された、ルールの非アクティブ化時間を使用した最後のルールの非アクティブ化に関する使用状況レポートがサポートされています。

  PCRF からのメッセージを受信すると、削除対象のルールがマーク付けされ、アクセス側の手順が完了した後にルールが削除されます。

- PCRF 要求使用状況レポート：最後のレポートの送信以降の累積使用量（即時レポートの場合も同様）。即時レポート後に使用量はリセットされ、使用状況モニタリングが続行されます。後続の使用状況レポートには現在のレポート以降の使用量が含まれるようになります。

- ベアラーの終了に関する使用状況レポートを追加できます。ベアラーが何らかの理由で削除されると、そのベアラーに関連付けられているルールも削除されます。そのため、使用状況は、ベアラー終了が原因で削除された最後のルールが関連ルールであるモニタリングキーで報告されます。

- 再検証のタイムアウト：非標準の実装では、使用状況モニタリングとレポートが有効になっていて、再検証タイムアウトが発生した場合、PCEF は CCR を送信して PCC ルールを要求し、最後のレポート以降（または、使用状況がまだ報告されていない場合には、使用状況レポートが有効になった時点以降）の有効なすべてのモニタリングキーのすべての累積使用量を、IP-CAN セッションレベル（有効な場合）およびサービスデータフローレベル（有効な場合）の累積使用量を使用して報告します。これがデフォルトの動作です。

  標準実装の場合、これは CLI 設定によって有効にする必要があります。

重要 再検証タイムアウト時の使用状況レポート機能は、Gx を介したボリュームレポートの非標準実装ではデフォルトで使用できます。この機能は標準実装で設定可能です。

使用状況が報告されると、使用量カウンタはゼロにリセットされます。PCEF は、しきい値に達した後、PCRF によって新しいしきい値が提供されるまで、データ使用状況の追跡を 0 から継続します。使用状況が報告された IP-CAN セッション変更の確認応答で、PCRF から新しい使用量しきい値が提供されない場合、その IP CAN セッションを対象とした PCEF での使用状況モニタリングは続行されず、CCR-CCA 間の累積使用量は破棄されます。

サーバーの再試行でトリガーされた CCR-U は、サーバーによって付与されたクォータを考慮して、USU を報告します。新たに作成された MSCC の場合、USU を報告するために暫定クォータ設定が取得されます。

Gx を介したボリュームレポート機能を設定する方法については、「Gx を介したボリュームレポートの設定 （29 ページ）」を参照してください。

Gx を介したボリュームレポート（*VoRoGx*）のための *ICSR* サポート

ボリュームのしきい値とボリュームの使用状況はスタンバイシャーシに同期され、ICSR スイッチオーバー後の既存のセッションの Gx を介したボリュームレポートをサポートします。

このサポートがないと、たとえば適切な使用を強制するためにボリュームレポートを使用した場合に、サブスクライバが想定以上に高い速度を使用する可能性はありません。通信事業者はこれをすでに収益の損失と見なしている可能性があります。また、EUのローミング規制によって設定された制限に達すると、通知を受け取り、ブロック/リダイレクトされるローミングサブスクライバに深刻な影響を及ぼします。セッションがブロックされずにこの時点でセッションが継続する場合、通信事業者は上限を超えたデータに課金することができず、実質的な収益の大幅な損失が発生します（ローミングパートナーはSGSNで使用されるデータに課金する場合があります）。

Rel. 9 Gx インターフェイス

Rel. 9 Gx インターフェイスのサポートは、Cisco ASR シャーシで使用できます。

P-GW Rel. 9 Gx インターフェイスのサポート

はじめに

Gx 参照ポイントは、パケットデータネットワーク（PDN）ゲートウェイ（P-GW）上のポリシーおよび課金ルール機能（PCRF）とポリシーおよび課金適用機能（PCEF）の間にあります。Gx 参照ポイントは、PCRF から PCEF への PCC ルールのプロビジョニングと削除、および PCEF から PCRF へのトラフィック プレーン イベントの送信に使用されます。Gx 参照ポイントは、アプリケーションに関連する AVP を適用することで、課金制御とポリシー制御のいずれかまたは両方に使用できます。

PCEF は、ポリシーの適用とフローベースの課金機能を包含する機能要素です。この機能エンティティは P-GW にあります。これには、以下の主要な機能があります。

- ゲートウェイでのユーザー プレーン トラフィックの処理とその QoS の制御。
- サービスデータフローの検出とカウント、およびオンラインとオフラインの課金操作。
- ポリシー制御されているサービスデータフローの場合、PCEF は、対応するゲートウェイが開いている場合にのみ、サービスデータフローがゲートウェイを通過するのを許可します。
- 課金制御されているサービスデータフローの場合、PCEF は、対応するアクティブな PCC ルールがあり、オンライン課金で OCS がその課金キーで該当するクレジットを承認した場合にのみ、サービスデータフローがゲートウェイを通過するのを許可します。
- PCRFから要求された場合、PCEFは関連するサービスデータフローのステータスが変わったときに PCRF に報告します。

- SDF が BBERF でトンネリングされている場合、PCEF は、IP-CAN セッションの確立時のサービスデータフローのモビリティ プロトコル トンネリング ヘッダーについて PCRF に通知します。

重要 ASR 5500 は、Gx メッセージのダイナミック課金ルールごとのフロー説明を含む 8 つのフロー情報のみをサポートします。

用語および定義

このセクションでは、Rel. 9 Gx に関連する機能と用語について説明します。.

Gx を介したボリュームレポート

ここでは、3GPP Rel. 9 の Gx を介したボリュームレポート機能について説明します。

ライセンス要件

Gx を介したボリュームレポートは、シスコのライセンス供与された機能です。別の機能ライセンスが必要になる場合があります。特定のライセンス要件の詳細については、シスコのアカウント担当者にお問い合わせください。ライセンスのインストールと確認の詳細については、『システム管理ガイド』の「ソフトウェア管理操作」の「ライセンスキーの管理」の項を参照してください。

重要 Gx を介した課金機能または Gx を介したボリュームレポート機能に個別のライセンスは必要ありません。この機能は、「ポリシーインターフェイス」ライセンスの一部として有効にすることができます。

サポートされる標準

Gx を介したボリュームレポート機能は、次の標準規格に基づいています。

3GPP TS 29.212 V9.5.0 (2011-01)：3rd Generation Partnership Project、Technical Specification Group Core Network and Terminals、Policy and Charging Control over Gx reference point (Release 9)

機能の概要

Volume Reporting over Gx 機能により、PCRF はサブスクライバのデータ使用量に基づいてリアルタイムの決定ができます。

重要 Volume Reporting over Gx は、ボリュームクォータにのみ適用されます。

Gx を介したボリュームレポートは、合計データ使用量レポートとアップリンク/ダウンリンクレベルのレポートの両方をサポートします。

PCEF は、最初からではなく、使用状況監視の最後のレポート以降の累積使用量のみを報告します。

使用量しきい値がゼロ（無限しきい値）に設定されている場合、PCEF によってそれ以上のしきい値イベントは生成されませんが、使用状況の監視は続行され、セッションの終了時に報告されます。

ベアラーの終了時の使用状況レポートがサポートされています。

次の手順を通じて、Gx を介したボリュームレポートの仕組みについて説明します。

1. PCEF は、PCRF からメッセージを受信した後、使用状況モニタリング関連の AVP を解析し、その情報を IMSA に送信します。
2. IMSA はこの情報で ECS を更新します。
3. PCRF からの使用状況モニタリング情報で ECS が更新されると、PCEF（ECS）はデータ使用状況の追跡を開始します。
4. セッションレベルのモニタリングの場合、ECS がデータ使用状況を保持します。
5. PCC ルールモニタリングの場合、モニタリングキーを一意の識別子として使用状況がモニタリングされます。各ノードがモニタリングキーごとの使用状況情報を保持します。データトラフィックが通過すると、使用量しきい値に照らして使用状況がチェックされ、「使用状況レポート」セクションに説明されているようにして報告されます。
6. PCEF は、しきい値に達した後、PCRF によって新しいしきい値が提供されるまで、データ使用状況を追跡し続けます。使用状況が報告された IP-CAN セッション変更の確認応答で、PCRF から新しい使用量しきい値が提供されない場合、その IP CAN セッションを対象とした PCEF での使用状況モニタリングは続行されません。

使用状況モニタリング

- セッションレベルでの使用状況モニタリング：PCRF は、Granted-Service-Unit AVP に使用量しきい値レベルを設定し、Usage-Monitoring-Level AVP をSESSION_LEVEL(0) に設定して、Usage-Monitoring-Information AVP を送信することで、Gx に関するセッションレベルのボリュームレポートにサブスクライブします。AVP が DPCA によって解析された後、IMSA は情報を ECS に対して更新します。ECS が更新されると、使用状況モニタリングが開始され、データトラフィックが発生するたびに使用量しきい値がチェックされます。PCRF は、セッションレベルでモニタリングキーをサポートしています。

  PCRF では、単一のメッセージでセッションの使用状況を有効または無効にすることができます。この操作は、モニタリングキーがセッションレベルで関連付けられている場合にのみ可能です。

PCRF では、入力/出力オクテットのしきい値レベルに基づき使用状況をモニタリングできます。有効になっているしきい値レベルに基づいて使用状況が報告されます。複数のレベルが有効になっている場合は、いずれか1つのレベルで侵害が発生しても、有効になっているすべてのレベルについて使用状況が報告されます。モニタリングは、PCRF からの使用状況レポートの応答で欠落しているしきい値レベルで停止されます（PCRF が以前に有効にされた複数のレベルでモニタリングを継続する場合、完全なセットを再度提供することが期待されます）。

合計しきい値レベルと GSU AVP の UL/DL しきい値レベルの両方が提供された場合はエラーとして扱われ、合計しきい値レベルのみが受け入れられます。

次の要求がモニタリングキーの使用状況を報告した CCR-U への応答で受信された場合、同じモニタリングキーの追加の CCR-U が生成されます。

- モニタリングキーを使用したルールレベルでの即時レポート要求
- モニタリングキーを使用した、または使用しないセッションレベルでの即時レポート要求
- ルールレベルでの明示的な無効化要求
- セッションレベルでの明示的な無効化要求

上記のすべての要求がモニタリングキーの使用状況を報告した CCR-U への応答で受信された場合、同じモニタリングキーの追加の CCR-U は生成されません。また、すべてのアクティブなモニタリングキーの使用状況を報告した CCR-U への応答で、ルールレベルのモニタリングキーのない即時レポート要求を受信した場合、追加の CCR-U は生成されません。

- フローレベルの使用状況モニタリング：PCRF は、Granted-Service-Unit AVP に設定された使用量しきい値レベルと PCC_RULE_LEVEL(1) に設定された Usage-Monitoring-Level AVP とともに Usage-Monitoring-Information AVP を送信することで、Gx を介してフローレベルのボリュームレポートに登録します。フローレベルのモニタリングの場合、モニタリングキーは必須です。PCRF がルールとモニタリングキーを関連付ける際や、フローレベルで使用状況モニタリングを有効化または無効化する際に、モニタリングキーを使用して制御できるためです。AVP が DPCA によって解析された後、IMSA は情報を ECS に対して更新します。ECS が更新されると、使用状況モニタリングが開始され、データトラフィックが発生するたびに使用量しきい値がチェックされます。

  使用状況モニタリングは、スタティックルール、定義済みルール、およびダイナミックルール定義に対応しています。

  - スタティックルールの使用状況モニタリング：スタティックルールの場合、モニタリングキーに関連付けられた最後のルール削除に関する使用状況はレポートの対象外になります。この場合、PCRF から使用状況モニタリング情報のみを受信します。
  - 定義済みルールの使用状況モニタリング：事前定義されたルールに対して使用状況モニタリングを有効にする必要がある場合、PCRF は、モニタリングキーと使用量しきい値を含むルールおよび使用状況モニタリング情報を送信します。モニタリングキーは、その事前定義済みルールの PCEF で事前設定されているものと同じである必要があります。同じモニタリングキーに複数のルールを関連付けることができます。そのため、特定のモニタリングキーを有効にすると、同じモニタリングキーを持つ複数の

ルールのデータが追跡されることになります。AVP が DPCA によって解析された後、IMSA は情報を ECS に対して更新します。ECS が更新されると、使用状況モニタリングが開始され、データトラフィックが発生するたびに使用量しきい値がチェックされます。

- ダイナミックルールの使用状況モニタリング：ダイナミックルール定義に対して使用状況モニタリングを有効にする必要がある場合、PCRF は課金ルールの定義や使用状況モニタリング情報（モニタリングキー、使用量しきい値など）とともにモニタリングキーを提供します。これにより、そのモニタリングキーに関連付けられているすべてのルールに対して使用状況モニタリングが実行されます。AVP が DPCA によって解析された後、IMSA は情報を ECS に対して更新します。ECS が更新されると、使用状況モニタリングが開始され、データトラフィックが発生するたびに使用量しきい値がチェックされます。ダイナミックルール定義のモニタリングキーは、PCRF によって動的に割り当てられます。これが、使用状況モニタリングのケースにおいて定義済みルールとの唯一の違いです。

モニタリングキーの 1 つの使用状況だけが最初に報告されます。PCRF から正常な応答を受信すると、残りのモニタリングキーの使用状況が PCRF に報告されます。Tx 期限切れ/TCP リンクエラーが発生すると、報告されていない使用状況が ECS に保存されます。セッションでその後 PCRF と正常なやり取りがあった場合、報告されていない UMI が PCRF に送信されます。

使用状況レポート

サブスクライバレベルやフローレベルでの使用状況は、次の条件で PCRF に報告されます。

- 使用量しきい値に達した：PCEF はサブスクライバデータの使用量を記録し、PCRF によって指定される使用量しきい値に達しているかどうかを確認します。これは、セッションレベルとルールレベルの両方のレポートで行われます。

  セッションレベルのレポートでは、実際の使用量が、使用量しきい値と比較されます。

  ルールレベルのレポートでは、データトラフィックにヒットするルールを使用して、モニタリングキーが関連付けられているかどうかが確認され、モニタリングキーに基づいてデータ使用量が確認されます。条件が満たされると、使用状況の情報を IMSA に報告し、モニタリングを続行します。IMSA は、「USAGE_REPORT」トリガーが PCRF によって有効になっている場合に、CCR-U をトリガーします。この CCR で、Usage-Monitoring-Information AVP と、サブスクライバのデータ使用量を設定した「Used-Service-Unit」が送信されます。

  使用量しきい値に達したときに、PCRF が使用状況モニタリング情報に PCEF からの CCR による新しい使用量しきい値を提供しない場合、使用状況モニタリングは PCEF で停止し、使用状況は報告されません。

  Gx を介した非標準ボリュームレポートの実装では、しきい値に違反すると使用状況モニタリングが停止します。それ以外の場合はモニタリングが続行されます。CCA が受信されるまで、以降の使用状況は報告されません。

- 使用状況モニタリングが無効：レポートの使用状況、その他の外部トリガー、または PCRF 内部トリガーに関連しない PCEF からの CCR の結果として PCRF により使用状況モニタ

リングが無効にされた場合には、PCRF が Usage-Monitoring-Support AVP を USAGE_MONITORING_DISABLED に設定して使用状況モニタリングを明示的に無効にすると、PCEF はモニタリングを停止し、（モニタリングが有効だったときの）使用状況情報を PCRF に報告します。使用量しきい値に達したときに、PCRF が PCEF からの CCR による新しい使用量しきい値を提供しない場合、使用状況モニタリングは PCEF で停止し、これ以降の使用状況は報告されません。

- IP CAN セッションの終了：IP CAN セッションが終了すると、サブスクライバの累積使用状況情報が PCEF からの CCR-T で PCRF に報告されます。PCC 使用量レベル情報が PCRF によって有効になっている場合、PCC 使用量も報告されます。

  PCRF は RAR メッセージを使用し、その中に Session-Release-Cause AVP を含めて、IP CAN セッション終了を開始します。ただし、PCRF が CCA メッセージで IP CAN セッションを終了する場合もあります。不要な追加メッセージを回避するために、PCRF は、CCA-U メッセージ自体で、サブスクライバを終了するように P-GW に通知できます。そのため、すべての Gx ディクショナリの CCA メッセージに Session Release Cause が追加されました。

- PCC ルールの削除：PCRF が使用量モニタリングキーに関連付けられている最後の PCC ルールを非アクティブ化すると、PCEF はそのモニタリングキーのデータ使用量を含む CCR を送信します。使用量モニタリングキーに関連付けられている最後の PCC ルールが非アクティブであると PCEF が報告する場合に、CCR コマンドに Charging-Rule-Report AVP が含まれていたなら、PCEF は同じ CCR コマンドでそのモニタリングキーの累積使用量を報告します。あるいは、Charging-Rule-Report AVP が RAA コマンドに含まれている場合、PCEF は新規に CCR コマンドを送信して、使用状況モニタリングキーの累積使用量を報告します。PCRF によって設定された、ルールの非アクティブ化時間を使用した最後のルールの非アクティブ化に関する使用状況レポートがサポートされています。

  PCRF からのメッセージを受信すると、削除対象のルールがマーク付けされ、アクセス側の手順が完了した後にルールが削除されます。

- PCRF 要求使用状況レポート：最後のレポートの送信以降の累積使用量（即時レポートの場合も同様）。即時レポート後に使用量はリセットされ、使用状況モニタリングが続行されます。後続の使用状況レポートには現在のレポート以降の使用量が含まれるようになります。

- ベアラーの終了に関する使用状況レポートを追加できます。ベアラーが何らかの理由で削除されると、そのベアラーに関連付けられているルールも削除されます。そのため、使用状況は、ベアラー終了が原因で削除された最後のルールが関連ルールであるモニタリングキーで報告されます。

- 再検証のタイムアウト：非標準の実装では、使用状況モニタリングとレポートが有効になっていて、再検証タイムアウトが発生した場合、PCEF は CCR を送信して PCC ルールを要求し、最後のレポート以降（または、使用状況がまだ報告されていない場合には、使用状況レポートが有効になった時点以降）の有効なすべてのモニタリングキーのすべての累積使用量を、IP-CAN セッションレベル（有効な場合）およびサービスデータフローレベル（有効な場合）の累積使用量を使用して報告します。これがデフォルトの動作です。

  標準実装の場合、これは CLI 設定によって有効にする必要があります。

重要 再検証タイムアウト時の使用状況レポート機能は、Gx を介したボリュームレポートの非標準実装ではデフォルトで使用できます。この機能は標準実装で設定可能です。

使用状況が報告されると、使用量カウンタはゼロにリセットされます。PCEF は、しきい値に達した後、PCRF によって新しいしきい値が提供されるまで、データ使用状況の追跡を 0 から継続します。使用状況が報告された IP-CAN セッション変更の確認応答で、PCRF から新しい使用量しきい値が提供されない場合、その IP CAN セッションを対象とした PCEF での使用状況モニタリングは続行されず、CCR-CCA 間の累積使用量は破棄されます。

サーバーの再試行でトリガーされた CCR-U は、サーバーによって付与されたクォータを考慮して、USU を報告します。新たに作成された MSCC の場合、USU を報告するために暫定クォータ設定が取得されます。

Gx を介したボリュームレポート機能を設定する方法については、「Gx を介したボリュームレポートの設定 （29 ページ）」を参照してください。

Gx を介したボリュームレポート（*VoRoGx*）のための *ICSR* サポート

ボリュームのしきい値とボリュームの使用状況はスタンバイシャーシに同期され、ICSR スイッチオーバー後の既存のセッションの Gx を介したボリュームレポートをサポートします。

このサポートがないと、たとえば適切な使用を強制するためにボリュームレポートを使用した場合に、サブスクライバが想定以上に高い速度を使用する可能性はありません。通信事業者はこれをすでに収益の損失と見なしている可能性があります。また、EU のローミング規制によって設定された制限に達すると、通知を受け取り、ブロック/リダイレクトされるローミングサブスクライバに深刻な影響を及ぼします。セッションがブロックされずにこの時点でセッションが継続する場合、通信事業者は上限を超えたデータに課金することができず、実質的な収益の大幅な損失が発生します（ローミングパートナーは SGSN で使用されるデータに課金する場合があります）。

IPFilterRule の 3GPP Rel. 9 コンプライアンス

このセクションでは、IPFilterRule 機能の 3GPP Rel. 9 コンプライアンスの概要と実装について説明します。

このセクションでは、この機能に関する次のトピックについて説明します。

機能説明

現在 PCEF は、Flow-Description AVP、TFT-Filter、および Packet-Filter-Content AVP の IPFilterRule に関して、3GPP Rel. 8 に準拠しています。ネットワークによって開始された専用ベアラーの作成または変更中、PCRF が Rel. 9 形式の Flow-Description AVP を使用して CCA-U または RAR

を送信するときに、PCEF が送信元および宛先 IP アドレスを誤って解釈し、UE に誤った TFT を送信していました。

PCRF が 3GPP Rel. 9 にアップグレードされても、PCEF は、UE によって開始されたセカンダリベアラーの作成または変更中、Flow-Description、TFT-Filter、および Packet-Filter-Content AVP を Rel. 8 形式で CCR-U に送信し続けます。

Flow-Description AVP、TFT-Filter、および Packet-Filter-Content AVP を PCEF 3GPP Rel. 9 に準拠させるため、次の変更が導入されます。

- Flow-Description AVP の IPFilterRule の送信元および宛先 IP アドレスの解釈は、3GPP Rel. 9 に準拠するように変更されます。つまり、ネットワークによって開始されたベアラー作成または変更中に UPLINK の Rel. 9 フロー説明が受信され、送信元 IP アドレスがリモートとして解釈され、宛先がローカル IP アドレスとして解釈されます。
- トラフィックフローの方向は、新しい Diameter AVP「Flow-Direction」から解釈されます。この新しい AVP で、フィルタが適用される 1 つまたは複数の方向、ダウンリンクのみ、アップリンクのみ、またはダウンリンクとアップリンクの両方（双方向）が示されます。
- IMSA モジュールは、TFT-Packet-Filter-Information および Packet-Filter-Information AVP を Rel. 9 形式でエンコードするように変更されました（ネゴシエートされたサポート対象機能が Rel. 9 以上の場合）。
- CCR-U の PCEF によって送信される Flow-Description、TFT-Filter、および Packet-Filter-Content AVP に対する Rel. 9 の変更を有効にするための設定サポートが提供されています。**diameter 3gpp-r9-flow-direction** CLI コマンドは、Rel. 9 の変更を有効にするために使用されます。この CLI コマンドが設定およびネゴシエートされた場合、サポートされる機能は、Rel. 9 以上（ゲートウェイと PCRF の両方が Rel. 9 以降に準拠）で、P-GW は Flow-Description、TFT-Filter、および Packet-Filter-Content AVP を Rel. 9 形式で送信します。

後方互換性は維持されています。つまり、Rel. 8（入出力を許可）および Rel. 9（フロー方向を含む出力を許可）形式が PCEF で受け入れられます。

3GPP Rel. 8 標準規格に従って、Flow-Description、TFT-Filter、および Packet-Filter-Content AVP の IPFilterRule が、UPLINK 方向の「入力許可」、DOWNLINK 方向の「出力許可」として送信されます。3GPP Rel. 9 以降、Flow-Information AVP 内の Flow-Description AVP には「出力許可」のみが含まれ、トラフィックフローの方向は Flow-Direction AVP で示されます。3GPP Rel. 9 形式では、UPLINK と DOWNLINK の両方が常に「出力許可」として送信されるため、「入力許可」の使用は廃止されます。

重要 この機能は、CCA-I でネゴシエートされたサポート対象の機能が Rel. 9 以上の場合にのみ、**diameter update-dictionary-avps { 3gpp-r9 | 3gpp-r10 }** CLI コマンドを使用して、3GPP Rel. 9 準拠の PCEF および PCRF のみに適用されます。

他の機能との関係

この機能は、**diameter update-dictionary-avps** CLI コマンドが 3gpp-r9 または 3gpp-r10 として設定されている場合にのみ機能します。つまり、PCEF は、**diameter 3gpp-r9-flow-direction** CLI コマンドが有効で、サポートされている機能が Rel. 9 以上である場合にのみ、3GPP Rel. 9 形式で Flow-Description、TFT-Filter、および Packet-Filter-Content AVP を送信します。この機能をアクティブ化する **diameter 3gpp-r9-flow-direction** CLI コマンドは、PCRF が Rel. 9 にアップグレードされた後にしか使用できません。9.

Rel. 9 準拠 AVP の設定

以下では、Flow-Description、TFT-Filter、および Packet-Filter-Content AVP の Rel. 9 の変更を有効にする設定コマンドについて説明します。

3GPP 準拠のための AVP のエンコーディング

次の設定コマンドを使用して、Rel. 9 形式の Flow-Description、TFT-Filter、および Packet-Filter-Content AVP から PCEF を制御します。

```
configure
   context context_name
      ims-auth-service service_name
         policy-control
            diameter 3gpp-r9-flow-direction
end
```

- **3gpp-r9-flow-direction**：3GPP Rel. 9 仕様に基づいて、Flow-Description、TFT-Filter、および Packet-Filter-Content AVP をエンコードします。デフォルトでは、この機能は無効になっています。
- この CLI 設定は、PCEF によって CCR-U で送信された TFT-Filter、Packet-Filter-Content、および Flow-Description AVP にのみ適用されます。
- この CLI コマンドは、PCRF が次にアップグレードされた後にしか使用できません：Rel. 9.
- この CLI コマンドは **diameter update-dictionary-avps { 3gpp-r9 | 3gpp-r10 }** と連携して動作します。**diameter 3gpp-r9-flow-direction** が設定され、サポート対象機能が 3gpp-r9 以上にネゴシエートされた場合、PCEF は、Flow-Description、TFT-Filter、および Packet-Filter-Content AVP を 3GPP Rel. 9 形式で送信します。

AVP コンプライアンスの設定の確認

次のコマンドを使用して、この機能の設定ステータスを確認します。

```
show ims-authorization service name service_name
```

service_name は、IMS 認証用に設定された IMS 承認サービスの名前にする必要があります。

「3GPP R9 Flow Direction Compliance」フィールドを使用して、この機能を有効にするか無効にするかを決定できます。

```
[local]st40# show ims-authorization service name gngp-gx
  Context: gngp
  IMS Authorization Service name: gngp-gx
  Service State: Enabled
  Service Mode: Single Interface Policy and Charging
...
  Diameter Policy Control:
   Endpoint: gx
   Origin-Realm: xyz.com
   Dictionary: r8-gx-standard
   Supported Features:
      3gpp-r9
...
   Host Selection: Table: 1 Algorithm: Round-Robin
   Host Reselection Subscriber Limit: Not Enabled
   Host Reselection Interval: Not Enabled
   Sgsn Change Reporting: Not Enabled
    3GPP R9 Flow Direction Compliance: Enabled
  Host Selection Table[1]: 1 Row(s)
   Precedence: 1
...
```

IPFilterRule の 3GPP Rel. 9 コンプライアンスのモニタリングと障害対応

この項では、この機能のサポートにおける show コマンドまたはその出力について説明します。

この機能に関連した障害については、次の操作を実行する必要があります。

- **show ims-authorization service name** <*service_name*> CLI コマンドを使用して、この機能が有効であるかどうかを確認します。有効になっていない場合は、**diameter 3gpp-r9-flow-direction** CLI コマンドを設定して、この機能が動作するかどうかを確認します。
- **monitor protocol** コマンドを実行し、CCA-I でネゴシエーションされたサポート機能が Rel. 9 以上であるかどうか確認します。そうでない場合、この機能は動作しません。**diameter update-dictionary-avps { 3gpp-r9 | 3gpp-r10 }** CLI コマンドを使用して、サポートされる機能を設定します。
- それでも問題が解決しない場合は、次の情報を入手して、シスコのアカウント担当者に詳細な分析を依頼してください。
  - オプション 24（GTPC）と 75-3（App Specific Diameter - DIAMETER Gx/Ty/Gxx）がオンになっているモニタープロトコルログ
  - acsmgr を有効にしたログ
  - **show active-charging sessions full all** および show ims-authorization sessions CLI コマンドの出力

show ims-authorization service name

Rel. 9 フロー方向変更が有効または無効になっているかどうかを示すために、この show コマンドの出力に新しいフィールド「3GPP R9 Flow Direction Compliance」が追加されました。

Rel. 10 Gx インターフェイス

Rel. 10 Gx インターフェイスのサポートは Cisco ASR シャーシで使用できます。

ここでは、次の内容について説明します。

• P-GW Rel. 10 Gx インターフェイスのサポート （65 ページ）

P-GW Rel. 10 Gx インターフェイスのサポート

はじめに

Gx 参照ポイントは、パケットデータネットワーク（PDN）ゲートウェイ（P-GW）上のポリシーおよび課金ルール機能（PCRF）とポリシーおよび課金適用機能（PCEF）の間にあります。Gx 参照ポイントは、PCRF から PCEF への PCC ルールのプロビジョニングと削除、および PCEF から PCRF へのトラフィック プレーン イベントの送信に使用されます。Gx 参照ポイントは、アプリケーションに関連する AVP を適用することで、課金制御とポリシー制御のいずれかまたは両方に使用できます。

PCEF は、ポリシーの適用とフローベースの課金機能を包含する機能要素です。この機能エンティティは P-GW にあります。これには、以下の主要な機能があります。

- ゲートウェイでのユーザー プレーン トラフィックの処理とその QoS の制御。
- サービスデータフローの検出とカウント、およびオンラインとオフラインの課金操作。
- ポリシー制御されているサービスデータフローの場合、PCEF は、対応するゲートウェイが開いている場合にのみ、サービスデータフローがゲートウェイを通過するのを許可します。
- 課金制御されているサービスデータフローの場合、PCEF は、対応するアクティブな PCC ルールがあり、オンライン課金で OCS がその課金キーで該当するクレジットを承認した場合にのみ、サービスデータフローがゲートウェイを通過するのを許可します。
- PCRF から要求された場合、PCEF は関連するサービスデータフローのステータスが変わったときに PCRF に報告します。
- SDF が BBERF でトンネリングされている場合、PCEF は、IP-CAN セッションの確立時のサービスデータフローのモビリティ プロトコル トンネリング ヘッダーについて PCRF に通知します。

重要 ASR 5500 は、Gx メッセージのダイナミック課金ルールごとのフロー説明を含む 8 つのフロー情報のみをサポートします。

用語および定義

このセクションでは、Rel. 10 Gx に関連する機能と用語について説明します。.

Gx を介したボリュームレポート

ここでは、3GPP Rel. 10 の Gx を介したボリュームレポートについて説明します。

ライセンス要件

Gx を介したボリュームレポートは、シスコのライセンス供与された機能です。別の機能ライセンスが必要になる場合があります。特定のライセンス要件の詳細については、シスコのアカウント担当者にお問い合わせください。ライセンスのインストールと確認の詳細については、『システム管理ガイド』の「ソフトウェア管理操作」の「ライセンスキーの管理」の項を参照してください。

重要 Gxを介した課金機能またはGxを介したボリュームレポート機能に個別のライセンスは必要ありません。この機能は、「ポリシーインターフェイス」ライセンスの一部として有効にすることができます。

サポートされる標準

Gx を介したボリュームレポート機能は、次の標準規格に基づいています。

3GPP TS 29.212 V10.5.0（2012-01）：3rd Generation Partnership Project、Technical Specification Group Core Network and Terminals、Policy and Charging Control over Gx reference point (Release 10)

機能の概要

Gxを介したボリュームレポート機能により、PCRFはサブスクライバのデータ使用量に基づいてリアルタイムの決定ができます。

重要 Volume Reporting over Gx は、ボリュームクォータにのみ適用されます。

PCEF は、最初からではなく、使用状況監視の最後のレポート以降の累積使用量のみを報告します。

使用量しきい値がゼロ（無限しきい値）に設定されている場合、PCEF によってそれ以上のしきい値イベントは生成されませんが、使用状況の監視は続行され、セッションの終了時に報告されます。

ベアラーの終了時の使用状況レポートがサポートされています。

次の手順を通じて、Gx を介したボリュームレポートの仕組みについて説明します。

1. PCEF は、PCRF からメッセージを受信した後、使用状況モニタリング関連の AVP を解析し、その情報を IMSA に送信します。

2. IMSA はこの情報で ECS を更新します。
3. PCRF からの使用状況モニタリング情報で ECS が更新されると、PCEF（ECS）はデータ使用状況の追跡を開始します。
4. セッションレベルのモニタリングの場合、ECS がデータ使用状況を保持します。
5. PCC ルールモニタリングの場合、モニタリングキーを一意の識別子として使用状況がモニタリングされます。各ノードがモニタリングキーごとの使用状況情報を保持します。データトラフィックが通過すると、使用量しきい値に照らして使用状況がチェックされ、「使用状況レポート」セクションに説明されているようにして報告されます。
6. PCEF は、しきい値に達した後、PCRF によって新しいしきい値が提供されるまで、データ使用状況を追跡し続けます。使用状況が報告された IP-CAN セッション変更の確認応答で、PCRF から新しい使用量しきい値が提供されない場合、その IP CAN セッションを対象とした PCEF での使用状況モニタリングは続行されません。

使用状況モニタリング

- セッションレベルでの使用状況モニタリング：PCRF は、Granted-Service-Unit AVP に使用量しきい値レベルを設定し、Usage-Monitoring-Level AVP を SESSION_LEVEL(0) に設定して、Usage-Monitoring-Information AVP を送信することで、Gx に関するセッションレベルのボリュームレポートにサブスクライブします。AVP が DPCA によって解析された後、IMSA は情報を ECS に対して更新します。ECS が更新されると、使用状況モニタリングが開始され、データトラフィックが発生するたびに使用量しきい値がチェックされます。PCRF は、セッションレベルでモニタリングキーをサポートしています。

  PCRF では、単一のメッセージでセッションの使用状況を有効または無効にすることができます。この操作は、モニタリングキーがセッションレベルで関連付けられている場合にのみ可能です。

  PCRF では、入力/出力オクテットのしきい値レベルに基づき使用状況をモニタリングできます。有効になっているしきい値レベルに基づいて使用状況が報告されます。複数のレベルが有効になっている場合は、いずれか1つのレベルで侵害が発生しても、有効になっているすべてのレベルについて使用状況が報告されます。モニタリングは、PCRF からの使用状況レポートの応答で欠落しているしきい値レベルで停止されます（PCRF が以前に有効にされた複数のレベルでモニタリングを継続する場合、完全なセットを再度提供することが期待されます）。

  合計しきい値レベルと GSU AVP の UL/DL しきい値レベルの両方が提供された場合はエラーとして扱われ、合計しきい値レベルのみが受け入れられます。

  次の要求がモニタリングキーの使用状況を報告した CCR-U への応答で受信された場合、同じモニタリングキーの追加の CCR-U が生成されます。

  - モニタリングキーを使用したルールレベルでの即時レポート要求
  - モニタリングキーを使用した、または使用しないセッションレベルでの即時レポート要求
  - ルールレベルでの明示的な無効化要求
  - セッションレベルでの明示的な無効化要求

上記のすべての要求が同じモニタリングキーの使用状況を報告した CCR-U への応答で受信された場合、モニタリングキーの追加の CCR-U は生成されません。また、すべてのアクティブなモニタリングキーの使用状況を報告した CCR-U への応答で、ルールレベルのモニタリングキーのない即時レポート要求を受信した場合、追加の CCR-U は生成されません。

- フローレベルの使用状況モニタリング：PCRF は、Granted-Service-Unit AVP に設定された使用量しきい値レベルと PCC_RULE_LEVEL(1) に設定された Usage-Monitoring-Level AVP とともに Usage-Monitoring-Information AVP を送信することで、Gx を介してフローレベルのボリュームレポートに登録します。フローレベルのモニタリングの場合、モニタリングキーは必須です。PCRF がルールとモニタリングキーを関連付ける際や、フローレベルで使用状況モニタリングを有効化または無効化する際に、モニタリングキーを使用して制御できるためです。AVP が DPCA によって解析された後、IMSA は情報を ECS に対して更新します。ECS が更新されると、使用状況モニタリングが開始され、データトラフィックが発生するたびに使用量しきい値がチェックされます。

  使用状況モニタリングは、スタティックルール、定義済みルール、およびダイナミックルール定義に対応しています。

  - スタティックルールの使用状況モニタリング：スタティックルールの場合、モニタリングキーに関連付けられた最後のルール削除に関する使用状況はレポートの対象外になります。この場合、PCRF から使用状況モニタリング情報のみを受信します。
  - 定義済みルールの使用状況モニタリング：事前定義されたルールに対して使用状況モニタリングを有効にする必要がある場合、PCRF は、モニタリングキーと使用量しきい値を含むルールおよび使用状況モニタリング情報を送信します。モニタリングキーは、その事前定義済みルールの PCEF で事前設定されているものと同じである必要があります。同じモニタリングキーに複数のルールを関連付けることができます。そのため、特定のモニタリングキーを有効にすると、同じモニタリングキーを持つ複数のルールのデータが追跡されることになります。AVP が DPCA によって解析された後、IMSA は情報を ECS に対して更新します。ECS が更新されると、使用状況モニタリングが開始され、データトラフィックが発生するたびに使用量しきい値がチェックされます。
  - ダイナミックルールの使用状況モニタリング：ダイナミックルール定義に対して使用状況モニタリングを有効にする必要がある場合、PCRF は課金ルールの定義や使用状況モニタリング情報（モニタリングキー、使用量しきい値など）とともにモニタリングキーを提供します。これにより、そのモニタリングキーに関連付けられているすべてのルールに対して使用状況モニタリングが実行されます。AVP が DPCA によって解析された後、IMSA は情報を ECS に対して更新します。ECS が更新されると、使用状況モニタリングが開始され、データトラフィックが発生するたびに使用量しきい値がチェックされます。ダイナミックルール定義のモニタリングキーは、PCRF によって動的に割り当てられます。これが、使用状況モニタリングのケースにおいて定義済みルールとの唯一の違いです。

複数のモニタリングキーで同時にしきい値違反が発生した場合、最初に 1 つのモニタリングキーの使用状況のみが報告されます。PCRF から正常な応答を受信すると、残りのモニタリン

グキーの使用状況が PCRF に報告されます。Tx 期限切れ/TCP リンクエラーが発生すると、報告されていない使用状況が ECS に保存されます。セッションでその後 PCRF と正常なやり取りがあった場合、報告されていない UMI が PCRF に送信されます。

使用状況レポート

サブスクライバレベルやフローレベルでの使用状況は、次の条件で PCRF に報告されます。

- 使用量しきい値に達した：PCEF はサブスクライバデータの使用量を記録し、PCRF によって指定される使用量しきい値に達しているかどうかを確認します。これは、セッションレベルとルールレベルの両方のレポートで行われます。

  セッションレベルのレポートでは、実際の使用量が、使用量しきい値と比較されます。

  ルールレベルのレポートでは、データトラフィックにヒットするルールを使用して、モニタリングキーが関連付けられているかどうかが確認され、モニタリングキーに基づいてデータ使用量が確認されます。条件が満たされると、使用状況の情報を IMSA に報告し、モニタリングを続行します。IMSA は、「USAGE_REPORT」トリガーが PCRF によって有効になっている場合に、CCR-U をトリガーします。この CCR で、Usage-Monitoring-Information AVP と、サブスクライバのデータ使用量を設定した「Used-Service-Unit」が送信されます。

  使用量しきい値に達したときに、PCRF が使用状況モニタリング情報に PCEF からの CCR による新しい使用量しきい値を提供しない場合、使用状況モニタリングは PCEF で停止し、使用状況は報告されません。

  Gx を介した非標準ボリュームレポートの実装では、しきい値に違反すると使用状況モニタリングが停止します。それ以外の場合はモニタリングが続行されます。CCA が受信されるまで、以降の使用状況は報告されません。

- 使用状況モニタリングが無効：レポートの使用状況、その他の外部トリガー、または PCRF 内部トリガーに関連しない PCEF からの CCR の結果として PCRF により使用状況モニタリングが無効にされた場合には、PCRF が Usage-Monitoring-Support AVP を USAGE_MONITORING_DISABLED に設定して使用状況モニタリングを明示的に無効にすると、PCEF はモニタリングを停止し、（モニタリングが有効だったときの）使用状況情報を PCRF に報告します。使用量しきい値に達したときに、PCRF が PCEF からの CCR による新しい使用量しきい値を提供しない場合、使用状況モニタリングは PCEF で停止し、これ以降の使用状況は報告されません。

- IP CAN セッションの終了：IP CAN セッションが終了すると、サブスクライバの累積使用状況情報が PCEF からの CCR-T で PCRF に報告されます。PCC 使用量レベル情報が PCRF によって有効になっている場合、PCC 使用量も報告されます。

  PCRF は RAR メッセージを使用し、その中に Session-Release-Cause AVP を含めて、IP CAN セッション終了を開始します。ただし、PCRF が CCA メッセージで IP CAN セッションを終了する場合もあります。不要な追加メッセージを回避するために、PCRF は、CCA-U メッセージ自体で、サブスクライバを終了するように P-GW に通知できます。そのため、すべての Gx ディクショナリの CCA メッセージに Session Release Cause が追加されました。

- PCC ルールの削除：PCRF が使用量モニタリングキーに関連付けられている最後の PCC ルールを非アクティブ化すると、PCEF はそのモニタリングキーのデータ使用量を含む CCR を送信します。使用量モニタリングキーに関連付けられている最後の PCC ルールが非アクティブであると PCEF が報告する場合に、CCR コマンドに Charging-Rule-Report AVP が含まれていたなら、PCEF は同じ CCR コマンドでそのモニタリングキーの累積使用量を報告します。あるいは、Charging-Rule-Report AVP が RAA コマンドに含まれている場合、PCEF は新規に CCR コマンドを送信して、使用状況モニタリングキーの累積使用量を報告します。PCRF によって設定された、ルールの非アクティブ化時間を使用した最後のルールの非アクティブ化に関する使用状況レポートがサポートされています。

  PCRF からのメッセージを受信すると、削除対象のルールがマーク付けされ、アクセス側の手順が完了した後にルールが削除されます。

- PCRF 要求使用状況レポート：最後のレポートの送信以降の累積使用量（即時レポートの場合も同様）。即時レポート後に使用量はリセットされ、使用状況モニタリングが続行されます。後続の使用状況レポートには現在のレポート以降の使用量が含まれるようになります。

- ベアラーの終了に関する使用状況レポートを追加できます。ベアラーが何らかの理由で削除されると、そのベアラーに関連付けられているルールも削除されます。そのため、使用状況は、ベアラー終了が原因で削除された最後のルールが関連ルールであるモニタリングキーで報告されます。

- 再検証のタイムアウト：非標準の実装では、使用状況モニタリングとレポートが有効になっていて、再検証タイムアウトが発生した場合、PCEF は CCR を送信して PCC ルールを要求し、最後のレポート以降（または、使用状況がまだ報告されていない場合には、使用状況レポートが有効になった時点以降）の有効なすべてのモニタリングキーのすべての累積使用量を、IP-CAN セッションレベル（有効な場合）およびサービスデータフローレベル（有効な場合）の累積使用量を使用して報告します。これがデフォルトの動作です。

  標準実装の場合、これは CLI 設定によって有効にする必要があります。

重要 再検証タイムアウト時の使用状況レポート機能は、Gx を介したボリュームレポートの非標準実装ではデフォルトで使用できます。この機能は標準実装で設定可能です。

使用状況が報告されると、使用量カウンタはゼロにリセットされます。PCEF は、しきい値に達した後、PCRF によって新しいしきい値が提供されるまで、データ使用状況の追跡を 0 から継続します。使用状況が報告された IP-CAN セッション変更の確認応答で、PCRF から新しい使用量しきい値が提供されない場合、その IP CAN セッションを対象とした PCEF での使用状況モニタリングは続行されず、CCR-CCA 間の累積使用量は破棄されます。

サーバーの再試行でトリガーされた CCR-U は、サーバーによって付与されたクォータを考慮して、USU を報告します。新たに作成された MSCC の場合、USU を報告するために暫定クォータ設定が取得されます。

Gx を介したボリュームレポート機能を設定する方法については、「Gx を介したボリュームレポートの設定 （29 ページ）」を参照してください。

Gx を介したボリュームレポート（*VoRoGx*）のための *ICSR* サポート

ボリュームのしきい値とボリュームの使用状況はスタンバイシャーシに同期され、スイッチオーバー後の既存セッションの Gx を介したボリュームレポートをサポートします。

このサポートがないと、たとえば適切な使用を強制するためにボリュームレポートを使用した場合に、サブスクライバが想定以上に高い速度を使用する可能性はありません。通信事業者はこれをすでに収益の損失と見なしている可能性があります。また、EUのローミング規制によって設定された制限に達すると、通知を受け取り、ブロック/リダイレクトされるローミングサブスクライバに深刻な影響を及ぼします。セッションがブロックされずにこの時点でセッションが継続する場合、通信事業者は上限を超えたデータに課金することができず、実質的な収益の大幅な損失が発生します（ローミングパートナーはSGSNで使用されるデータに課金する場合があります）。

Gx インターフェイスでの Supported-Features AVP の使用

Supported-Features AVP はセッションの確立中に使用され、送信元ホストがサポートする必須機能とオプション機能について宛先ホストに通知します。クライアントは、Diameterセッションの最初の要求で、セッションの正常な処理に必要な一連の機能を指定します。クライアントによってサポートされており、必要な機能セットの一部としてアドバタイズされていない機能がある場合、クライアントは、セッションを正常に処理するためのオプションであるこのオプション機能のセットを同じ要求で提供します。サーバーは、Diameterセッション内の最初の応答で、クライアントと共通する機能のセットと、同じ Diameter セッション内でサーバーがサポートする機能のセットを示します。以降のコマンドメッセージは、セッション確立中に、Supported-Features AVP に示されているサポート対象機能のリスト、および Supported-Features AVP に示されていない機能に常に準拠します。サポート対象としてアドバタイズされていない機能は、そのDiameterセッションのコマンドメッセージの作成に使用されません。特に明記されていない限り、Gx 参照ポイントでの Supported-Features AVP の使用は、サポートされている機能の動的な検出および関連するエラー処理の要件に準拠します。

Gx 参照ポイントの基本的役割は 3GPP Rel. 7 標準であり、機能はその役割の拡張です。元のホストが基本的な役割を超える機能をサポートしていない場合、Supported-Features AVP が Gx コマンドに存在しない場合があります。3GPP TS 29.229 に定義されているように、機能の新しい AVP を追加してアプリケーションを拡張する場合、新しい AVP は M ビットがクリアされ、AVP はコマンド ABNF で必須として定義されません。

Supported-Features AVP はある種グループ化されており、Vendor-Id、Feature-List-ID、および Feature-List の各 AVP が含まれています。Gx 参照ポイントでは、3GPP によって定義された機能を識別するために Supported-Features AVP を使用するため、Vendor-Id AVP には 3GPP のベンダーID（10415）が含まれます。Gx参照ポイントに複数の機能リストが定義されている場合、Feature-List-ID AVP はそれらのリストを互いに区別します。

機能ビット	機能	M/O	説明
0	Rel8	M	この機能は、3GPP Rel-8 の基本的な Gx の役割のサポートを示します。これには、基本の 3GPP Rel-7 Gx 標準でサポートされる AVP および対応するプロシージャが含まれますが、個別の機能ビットで表される機能は除外されます。

機能ビット	機能	M/O	説明
1	Rel9	M	この機能は、3GPP Rel-9 の基本的な Gx の役割のサポートを示します。これには、Rel8 機能ビットでサポートされる AVP および対応するプロシージャが含まれますが、個別の機能ビットで表される機能は除外されます。
3	Rel10	M	この機能は、3GPP Rel-10 の基本的な Gx の役割のサポートを示します。これには、Rel8 および Rel9 機能ビットでサポートされる AVP および対応するプロシージャが含まれますが、個別の機能ビットで表される機能は除外されます。
4	SponsoredConnectivity	O	この機能は、スポンサーデータ接続機能に対するサポートを示しています。PCEF がこの機能をサポートしている場合、PCRF はサブスクライバへのスポンサーデータ接続を承認できます。

PCEF が Diameter ディクショナリをリリース 8、9、または 10 として設定すると、PCRF は Supported-Features AVP を送信して、PCEF は PCRF がサポートする機能を認識できるようにします。PCEF が、要求された機能よりも少ない、または要求された機能よりも多いサポート対象の機能を受信した場合、サポート対象機能は、少ない方の機能にマッピングされます。

カスタムディクショナリ「dpca-custom24」が構成されている場合は、Vendor-Id AVP を含む Supported-Features AVP がすべての CCR メッセージで送信されます。

Rule-Failure-Code AVP

Rule-Failure-Code AVP は、QoS/PCC ルールのインストール、アクティブ化、適用を正常に実行できない理由を示します。Rule-Failure-Code AVP のタイプは列挙されます。PCC ルールが報告されている理由を特定するために、この情報が PCEF から Charging-Rule-Report AVP 内の PCRF に送られます。

2 つの新しいルール障害コード INCORRECT_FLOW_INFORMATION (12) と NO_BEARER_BOUND (15) が追加されています。既存のルール障害コード 9 の名前が MISSING_FLOW_INFORMATION に変更されます。3GPP リリース 10 の場合、ルール障害コード 9 は GW/PCEF_MALFUNCTION にマッピングされます。

スポンサーデータ接続

スポンサーはスポンサーデータ接続機能により通信事業者と取引関係を結びます。スポンサーはユーザーが関連するアプリケーション サービス プロバイダー（ASP）のサービスにアクセスできるようにするために、ユーザーのデータ接続料を通信事業者に支払います。または、ユーザーが基本使用料とは別に、トランザクションを使用した接続に対して料金を支払います。これは、ユーザーが通信事業者とサブスクリプション契約を締結していることが前提です。

スポンサーデータ接続機能は、 3GPP TS 29.212 仕様のリリース 10 で導入されました。スポンサードデータ接続機能がサポートされている場合、PCC ルールのスポンサー ID によって、エ

ンドユーザーへのサービス提供に必要な接続料金を通信事業者に支払うサードパーティ組織（スポンサー）が識別されます。

この機能の目的は、特定のフローセットのデータ使用量を個別に識別し、スポンサーに請求することです。これに対応するために、新しいレポートレベル「SPONSORED_CONNECTIVITY_LEVEL」がスポンサー接続レベルでのレポート用に追加され、ルールレベルで 2 つの新しい AVP「Sponsor-Identity」と「Application-Service-Provider-Identity」が導入されました。

スポンサーやアプリケーションサービスプロバイダーに関する情報やしきい値（オプション）がアプリケーション機能（AF）によって提供されると、1 つ以上の PCC ルールに関連付けられたサービスデータフローに対してスポンサーデータ接続が実行されます。

PCC ルールに基づくスポンサーデータ接続のプロビジョニングは、PCC ルールのプロビジョニング手順に従って実行されます。スポンサー ID は、PCC ルールの Charging-Rule-Definition AVP 内にある Sponsor-Identity AVP を使用して設定されます。アプリケーション サービス プロバイダーの ID は、PCC ルールの Charging-Rule-Definition AVP 内にある Application-Service-Provider-Identity AVP を使用して設定されます。Reporting-Level AVP の値が SPONSORED_CONNECTIVITY_LEVEL に設定されている場合は、Sponsor-Identity AVP および Application-Service-Provider-Identity AVP が含まれています。

AF からフローベースの使用量しきい値を受信すると、PCRF はスポンサー ID を使用してモニタリングキーを生成します。PCRF は使用量のモニタリング制御を要求することもあります。この場合、フローベースの使用量のみがスポンサーデータ接続に適用されます。PCEF は要求に応じて PCRF に使用量を報告する場合もあります。

新しい CLI コマンド「**diameter encode-supported-features**」がポリシー制御設定モードに追加され、サポートされる機能をスポンサー ID で送信できるようになりました。コマンドの詳細については、『*Command Line Interface Reference*』[英語] を参照してください。

スポンサー接続機能は、P-GW と PCRF の両方が 3GPP リリース10 に対応している場合にのみサポートされます。P-GW は、CCR-I でサポートされている機能の一部としてリリースを PCRF にアドバタイズします。P-GW がリリース 10 とスポンサー接続機能をサポートしているが、PCRF が（CCA-I でサポートされている機能の一部として）スポンサー接続機能をサポートしていない場合、この機能はオフになります。

スポンサー接続機能は、「dpca-custom8」Gx ディクショナリと連携します。セッションが PCRF からのスポンサー接続に対して有効になっており、オフライン課金が aaa-custom4 ディクショナリを使用して有効になっている場合、スポンサー接続の AVP が ACR 中間パケットと ACR 停止パケットで CDF サーバーに報告されます。Sponsor-Identity AVP と Application-Service-Provider-Identity AVP は、ACR パケット内でグループ化された Service-Data-Container AVP で送信されます。

この機能は、ダイナミックルールと Gx ディクショナリ（dpca-custom 15 および dpca-custom8）をサポートしています。

使用量のレポート

Gx を介したボリュームレポートの場合、PCRF はスポンサー ID に基づいて一意のモニタリングキーを生成します。異なるモニタリングキーを持つフローは個別に扱われるため、スポンサー ID を持つフローは個別に課金されます。

サポートされる Gx 機能

Gx でのポジティブ想定

プライマリとセカンダリ両方の PCRF サーバーが過負荷になっているシナリオでは、PCRF は P-GW と HSGW にエラーを返します。P-GW と HSGW の現在の動作は、プライマリとセカンダリの両方が失敗またはタイムアウトを返した場合にセッションを終了することです。

この機能は、ゲートウェイにローカルポリシーを適用してサブスクライバセッションが継続されるようにすることで、上述の動作を拡張するために開発されました。P-GW/HSGW は、エラーを処理し、イベントタイプに基づいて特定のルールを適用するため、ポジティブ想定機能を導入する必要があります。

重要 Gx ポジティブ想定を使用するには、有効なライセンスキーがインストールされている必要があります。ライセンスの入手方法の詳細については、シスコのアカウント担当者にお問い合わせください。

障害処理の動作が強化され、PCRF が使用できない場合に、サブスクライバサービスが確実に維持されるようになりました。また GW は、Diameter ビジー状態（3004）を受信したときに、設定可能な時間の間、PCRF との Diameter メッセージ（CCR および RAR）の送受信を停止することによって、PCRF へのトラフィックを削減することが必要です。

PCRF で次のいずれかの障害が発生した場合、GW は、障害処理を適用してサブスクライバを終了させるか、それ以上ポリシーを適用せずにブラウジングを許可するかを選択します。

- TCP リンク障害
- アプリケーションタイマー（Tx）の期限切れ
- 結果コードベースの障害

PCRF は、すべての接続レベルの障害、結果コード/実験結果コードの障害が発生した場合、ローカルポリシーにフォールバックできます。ローカルポリシーは、設定された時間の間、サブスクライバを許可する選択を下す場合があります。この間、コールのサブスクライバ/内部イベントはローカルポリシーから処理されます。タイマーの期限が切れた後、サブスクライバセッションを終了するか、PCRF を再試行できます。PCRF の再試行は、**timer-expiry event** が **reconnect-to-server** として設定されている場合にのみ行われることに注意してください。

フォールバックのサポートが障害処理テンプレートに追加されました。また、ローカルポリシーサービスは IMS 承認サービスに関連付けられている必要があります。

ローカルポリシーが適用されると、PCRF が有効になっているすべてのイベントトリガーが無効になります。サブスクライバセッションでローカルポリシーが使用されている場合、GW は、CCR-T の送信をスキップし、ローカルでセッションをクリーンアップします。

アクティブな Gx セッションで作成されたセッションの場合、GW は CCR-T をプライマリ PCRF に送信し、障害が発生すると、CCR-T をセカンダリ PCRF に送信します。CCR-T がプライマリとセカンダリの両方から失敗を返した場合、またはタイムアウトした場合、GW はセッションをローカルでクリーンアップします。

ローカルポリシーへのフォールバックは、次のシナリオで行われます。

- Tx タイマーの期限切れ
- Diabase エラー
- 結果コードエラー（持続的/一時的）
- 実験結果コード
- 応答タイムアウト

次のポイントは、PCRF への再接続が試行されるシナリオにのみ適用されます。

- サブスクライバが CCR-I 障害が原因でローカルポリシーにフォールバックした場合、タイマーの期限切れ後に CCR-I が PCRF に送信されます。成功した CCA-I コールは PCRF で続行されます。成功しなかった場合、コールはローカルポリシーで続行され、再試行カウントが増分されます。
- サブスクライバが CCR-U 障害のためにローカルポリシーにフォールバックした場合、IMS 承認アプリケーションは、イベントの変更が発生するまで、または PCRF から RAR を受信するまで待機します。
- タイマーの期限切れ後にイベントが変更された場合、CCR-U が PCRF に送信されます。CCA-U メッセージが成功すると、コールは PCRF で続行されます。成功しなかった場合は、ローカルポリシーでコールが実行され、再試行カウントが増分されます。
- タイマーの期限切れ後に RAR を受信した場合、コールは PCRF で続行されます。PCRF への接続の再試行期限が切れると、コールは切断されます。

CCR-I エラーに関するデフォルトポリシー

P-GW のローカル設定では、次のパラメータがサポートされています。設定パラメータは、APN ごとおよび RAT タイプごとに設定できます。

デフォルトベアラー課金ルールの次のフィールドは、APN ごとおよび RAT タイプごとに設定できます。

- ルール名
- 料金設定グループ
- Service ID
- オンライン課金
- オフライン課金
- QCI

- ARP
  - 優先度
  - QCI
  - QVI
- 最大要求帯域幅
  - UL
  - DL

フローの説明とフローステータスは設定できませんが、デフォルト値は Any to Any に設定され、フローステータスは Enabled に設定されます。

次のコマンドレベルのフィールドは、APN ごとおよび RAT タイプごとに設定できます。

- AMBR
  - UL
  - DL
- QCI
- ARP
  - 優先度
  - QCI
  - QVI

Gx バックオフ機能

このシナリオは、プライマリ PCRF クラスタが使用できないものの、新しい CCR-I メッセージを処理できるセカンダリ PCRF が使用可能な場合に適用されます。

シャーシが 3004 結果コードを受信すると、ピアのバックオフタイマーが開始され、タイマーが実行されている間、そのピアにメッセージは送信されません。

タイマーは、値がエンドポイント設定で設定されている場合にのみ開始されます。

P-GW/GGSN は、CCR が失敗した場合、サブスクライバに PCRF に再接続する優れた機会を提供します。この機能をサポートするために、設定可能な有効性タイマーとピアバックオフタイマーが、ローカルポリシーサービスおよびDiameterエンドポイント設定コマンドに導入されています。また、ローカルポリシータイマーの実行中に受信した RAR は、「DIAMETER_UNABLE_TO_DELIVER」が原因で拒否されます。

CLI コマンド **diameter encodeevent-avps local-fallback** がポリシー制御コンフィギュレーションモードで設定されている場合、再接続中にルールレポートが PCRF に送信されます。

ローカルポリシーでのボリュームレポートのサポート

この機能により、CCR-U障害シナリオでの、イベントベースではなく時間ベースの PCRF への再接続がサポートされます。

ローカルポリシーのボリュームレポートに関して、次の動作が見られました。

- CCR-U 障害の発生時、CCR-U は、サブスクライバイベントの受信時にのみ PCRF にトリガーされていました。
- CCR-U障害が発生し、コールがGxなしで続行された場合、しきい値が無限に設定されているため、報告されていないボリュームは失われました。次のCCR-UがPCRFにトリガーされると、累積ボリュームが PCRF に送信されました。
- 有効性タイマーの実行中に、RARは、原因コードdiameter_unable_to_comply（3002）で拒否されました。

タイマーベースの実装後、この機能により、既存の動作に次の変更が導入されます。

- send-usage-reportが設定されている場合、使用状況レポートを含むCCR-Uが、ローカルポリシータイマーの有効期限が切れた直後に送信されます。
- 報告されていない使用状況は、ECS に返されません。そのため、最後に CCR-U を試行してからの使用状況が PCRF に送信されます。
- タイマーが実行されている場合でも、RAR は受け入れられ、RAR で受信されたルールがインストールされます。

サブスクライバイベントを待つ代わりに、セッションをPCRFにすぐに接続し、更新された使用状況レポートを送信することができます。

セッションリカバリとセッション同期のサポート

現在、通常のシナリオで Gx のポジティブ想定機能が適用されていない場合、PCRF ノードとASR 5500 ゲートウェイノードは同期しています。ただし、PCRFがローカルで削除されたり、Gx セッション情報が損失しているシナリオが考えられます。また、メッセージの損失が原因で、ゲートウェイノードと PCRF のセッション状態が同期していない可能性もあります。

ネットワークがこのような状態になるのはまれですが、セッションの損失時にPCRFがGxセッションを復元し、またPCRFとゲートウェイ間でルールとセッション情報を同期させるのが、望ましい動作です。この機能を使用すると、PCRFとゲートウェイがセッション情報を同期し、失われた Gx セッションを復元できます。セッションリカバリ機能とセッション同期機能を有効にするための設定がサポートされるようになりました。

ゲートウェイ（GW）ノードとPCRFはセッション情報を交換する機能をサポートしています。GW は完全なサブスクライバセッション情報を提供して PCRF がセッション状態を確立できるようにします。これにより、上記のシナリオの発生を回避し、GW と PCRF が常に同期されるようになります。キーワード **session-recovery** および **session-sync** は、Gx 同期をサポートするために、ポリシー制御コンフィギュレーション モードで **diameter encode-supported-features** CLI コマンドと一緒に使用されます。

Gx のポジティブ想定機能の設定

Gx のポジティブ想定機能を設定するには、次の手順を実行します。

手順

ステップ 1 グローバル コンフィギュレーション レベルでのローカルポリシーサービスの設定 （78 ページ）の説明に従って、グローバル コンフィギュレーション レベルでサブスクライバのローカルポリシーサービスを設定します。

ステップ 2 グローバル コンフィギュレーション レベルでの障害処理テンプレートの設定 （79 ページ）の説明に従って、グローバル コンフィギュレーション レベルでローカルポリシーサービスを使用して、障害処理テンプレートを設定します。

ステップ 3 ローカルポリシーサービスと障害処理テンプレートの関連付け （79 ページ）の説明に従って、IMS 承認サービス内でローカルポリシーサービスと障害処理テンプレートを関連付けます。

ステップ 4 ローカルポリシーサービス設定の確認 （80 ページ）の説明に従って、設定内容を確認します。

ステップ 5 EXEC モードコマンド **save configuration** を使用して、フラッシュメモリ、外部メモリデバイス、もしくはネットワーク上の場所に設定を保存します。構成ファイルを検証して保存する方法の詳細については、『*System Administration Guide*』および『*Command Line Interface Reference*』を参照してください。

重要
この項の設定例で使用されているコマンドは、最もよく使用されているコマンドまたはその可能性の高いコマンド、および/またはキーワードオプションが提示される範囲で、基本機能を提供します。多くの場合は、他のオプションのコマンドやキーワードオプションを使用できます。すべてのコマンドの詳細については、『*Command Line Interface Reference*』を参照してください。

グローバル コンフィギュレーション レベルでのローカルポリシーサービスの設定

サブスクライバ向けのローカルポリシーサービスをグローバル コンフィギュレーション レベルで設定するには、次の例を使用します。

```
configure
    local-policy-service  LOCAL_PCC
         ruledef 2G_RULE
              condition priority 1 apn match .*
              exit
         ruledef all-plmn
              condition priority 1 serving-plmn match .*
              exit
         actiondef 2G_UPDATE
             action priority 1 activate-ambr uplink 18000 downlink 18000

              action priority 2 reject-requested-qos
              exit
         actiondef action1
              action priority 2 allow-requested-qos
              exit
         actiondef allow
              action priority 1 allow-session
```

```
            exit
        actiondef delete
            action priority 1 terminate-session
            exit
        actiondef lp_fall
            action priority 1 reconnect-to-server
            exit
        actiondef time
            action priority 1 start-timer timer duration 10
        exit
        eventbase default
            rule priority 1 event fallback ruledef 2G_RULE actiondef
time continue
            rule priority 2 event new-call ruledef 2G_RULE actiondef
action1
            rule priority 3 event location-change ruledef 2G_RULE
actiondef action1
          rule priority 5 event timer-expiry ruledef 2G_RULE actiondef
 lp_fall
            rule priority 6 event request-qos default-qos-change
ruledef 2G_RULE actiondef allow
            end
```

注：

- 一部のイベントが発生すると、イベントは、イベントベースのデフォルトの優先順位に基づいて最初に照合されます。一致したルールについて、対応する ruledef が満たされている場合、特定のアクションが実行されます。

グローバル コンフィギュレーション レベルでの障害処理テンプレートの設定

次の例を使用して、グローバル コンフィギュレーション レベルで障害処理テンプレートを設定します。

```
configure
   failure-handling-template <template_name>
      msg-type any failure-type any action continue local-fallback
      end
```

注：

- TCP リンク障害、アプリケーションタイマー（Tx）期限切れ、または結果コードベース障害が発生すると、関連する failure-handling が考慮され、failure-handling アクションが local-fallback として設定されている場合、コールは local-fallback モードにフォールバックします。

ローカルポリシーサービスと障害処理テンプレートの関連付け

ローカルポリシーサービスと障害処理テンプレートを関連付けるには、次の例を使用します。

```
configure
   context <context_name>
      ims-auth-service <service_name>
         associate local-policy-service <lp_service_name>
```

```
associate failure-handling <failure-handling-template-name>
end
```

ローカルポリシーサービス設定の確認

ローカルポリシーサービスの設定を確認するには、次のコマンドを使用します。

```
show local-policy statistics service service_name
```

Gx を介した時間レポート

ここでは、このリリースの GGSN でサポートされている Gx を介した時間レポートの機能について説明します。

ライセンス要件

Gx を介した時間レポート機能に個別のライセンスは必要ありません。この機能は、「ポリシーインターフェイス」ライセンスの一部として有効にすることができます。

特定のライセンス要件の詳細については、シスコのアカウント担当者にお問い合わせください。ライセンスのインストールと確認の詳細については、『システム管理ガイド』の「ソフトウェア管理操作」の「ライセンスキーの管理」の項を参照してください。

機能の概要

この非標準の Gx を介した時間使用状況レポート機能は、Gx を介したボリューム使用状況レポートに似ています。PCRF は、CCA または RAR で、セッション全体または特定のモニタリングキーの時間使用量しきい値を提供します。指定されたしきい値を超えると、使用状況レポートが CCR で PCRF に送信されます。この時間しきい値は、データトラフィックとは無関係です。使用量しきい値違反とは別に、使用状況レポートが PCRF に送信される他のシナリオがあります。

重要 Gx を介した時間レポートは、時間クォータにのみ適用されます。

PCEF は、最初からではなく、時間モニタリングの最後のレポート以降の累積時間使用状況のみを報告します。

時間使用量しきい値がゼロ（無限しきい値）に設定されている場合、PCEF によってそれ以上のしきい値イベントは生成されませんが、使用状況の監視は続行され、セッションの終了時に報告されます。

ベアラーの終了時の時間使用状況レポートがサポートされています。ベアラーが何らかの理由で削除されると、そのベアラーに関連付けられているルールも削除されます。そのため、使用状況は、ベアラー終了が原因で削除された最後のルールが関連ルールであるモニタリングキーで報告されます。

次の手順を通じて、Gx を介した時間レポートの仕組みについて説明します。

1. PCEF は、PCRF からメッセージを受信した後、時間モニタリング関連の AVP を解析し、その情報を IMSA に送信します。
2. IMSA はこの情報で ECS を更新します。
3. PCRF からの時間モニタリング情報で ECS が更新されると、PCEF（ECS）は時間使用状況の追跡を開始します。
4. セッションレベルのモニタリングの場合、ECS が時間使用状況を保持します。
5. PCC ルールモニタリングの場合、モニタリングキーを一意の識別子として使用状況がモニタリングされます。各ノードがモニタリングキーごとの時間使用状況情報を保持します。
6. PCEF は、しきい値に達した後、PCRF によって新しいしきい値が提供されるまで、時間使用状況を追跡し続けます。使用状況が報告された IP-CAN セッション変更の確認応答で、PCRF から新しい使用量しきい値が提供されない場合、その IP CAN セッションを対象とした PCEF での時間モニタリングは続行されません。

制限事項

このセクションでは、このリリースの Gx を介した時間レポートの制限事項を示します。

- Gx を介したボリュームレポートのように、整数のモニタリングキーのみがサポートされます。
- 時間とデータボリューム両方のモニタリングに同じモニタリングキーが使用されている場合、モニタリングキーを無効にすると、時間とデータ使用状況の両方のモニタリングが無効になります。
- 同じモニタリングキーが時間とデータ使用状況両方のモニタリングに使用されている場合、即時レポート要求が受信されると、そのモニタリングキーの時間とボリューム両方のレポートが送信されます。

使用状況モニタリング

次の 2 つのレベルの時間使用状況レポートがサポートされています。

- セッションレベルでの使用量のモニタリング
- フローレベルでの使用量のモニタリング

セッションレベルでの使用量のモニタリング

PCRF は、Granted-Service-Unit AVP に設定された使用量しきい値レベルおよび SESSION_LEVEL（0）に設定された Usage-Monitoring-Level AVP と共に Usage-Monitoring-Information AVP を送信することで、Gx を介してセッションレベル時間レポートにサブスクライブします。

フローレベルでの使用量のモニタリング

PCRF は、Granted-Service-Unit AVP に設定された使用量しきい値レベルおよび PCC_RULE_LEVEL(1) に設定された Usage-Monitoring-Level AVP とともに Usage-Monitoring-Information AVP を送信することで、Gx を介してフローレベル時間レポートをサブスクライブします。フローレベルのモニタリングの場合、モニタリングキーは必須で

す。PCRF がルールとモニタリングキーを関連付ける際や、フローレベルで使用状況モニタリングを有効化または無効化する際に、モニタリングキーを使用して制御できるためです。使用状況モニタリングは、定義済みルールとダイナミックルール定義の両方に対応しています。

事前定義されたスタティックルールの使用状況モニタリング

事前定義されたルールに対して使用状況モニタリングを有効にする必要がある場合、PCRFは、モニタリングキーと使用量しきい値を含むルールおよび使用状況モニタリング情報を送信します。モニタリングキーは、その事前定義済みルールの PCEF で事前設定されているものと同じである必要があります。同じモニタリングキーに複数のルールを関連付けることができます。そのため、特定のモニタリングキーを有効にすると、同じモニタリングキーを持つ複数のルールの時間が追跡されることになります。同様に、スタティックルールの使用状況モニタリング情報も PCRF から送信されます。

ダイナミックルール定義の使用状況モニタリング

ダイナミックルール定義に対して使用状況モニタリングを有効にする必要がある場合、PCRFは課金ルールの定義や使用状況モニタリング情報（モニタリングキー、使用量しきい値など）とともにモニタリングキーを提供します。これにより、そのモニタリングキーに関連付けられているすべてのルールに対して使用状況モニタリングが実行されます。

使用状況レポート

サブスクライバレベルやフローレベルでの時間の使用状況は、次の条件でPCRFに報告されます。

- 使用量しきい値に達した：PCEF はサブスクライバの使用量を記録し、PCRF によって指定される使用量しきい値に達しているかどうかを確認します。条件が満たされると、使用状況の情報をIMSAに報告し、モニタリングを続行します。IMSAは、「USAGE_REPORT」トリガーがPCRFによって有効になっている場合に、CCR-Uをトリガーします。設定された「Used-Service-Unit」の「CC-Time」とともに、Usage-Monitoring-Information AVP がこの CCR で送信され、サブスクライバの時間使用量を追跡します。
- 使用状況モニタリングが無効：レポートの使用状況、その他の外部トリガー、またはPCRF内部トリガーに関連しない PCEF からの CCR の結果として PCRF により使用状況モニタリングが無効にされた場合には、PCRF が Usage-Monitoring-Support AVP を USAGE_MONITORING_DISABLEDに設定して使用状況モニタリングを明示的に無効にすると、PCEF はモニタリングを停止し、（モニタリングが有効だったときの）使用状況情報を PCRF に報告します。
- IP CAN セッションの終了：IP CAN セッションが終了すると、サブスクライバの累積使用状況情報が PCEF からの CCR-T で PCRF に報告されます。

  PCRF はRAR メッセージを使用し、その中に Session-Release-Cause AVP を含めて、IP CAN セッション終了を開始します。ただし、PCRF が CCA メッセージで IP CAN セッションを終了する場合もあります。不要な追加メッセージを回避するために、PCRF は、CCA-U メッセージ自体で、サブスクライバを終了するようにP-GWに通知できます。そのため、すべての Gx ディクショナリの CCA メッセージに Session Release Cause が追加されました。

- PCC ルールの削除：PCRF が使用量モニタリングキーに関連付けられている最後の PCC ルールを非アクティブ化すると、PCEF はそのモニタリングキーの使用時間を含む CCR を送信します。使用量モニタリングキーに関連付けられている最後の PCC ルールが非アクティブであると PCEF が報告する場合に、CCR コマンドに Charging-Rule-Report AVP が含まれていたなら、PCEF は同じ CCR コマンドでそのモニタリングキーの累積使用量を報告します。あるいは、Charging-Rule-Report AVP が RAA コマンドに含まれている場合、PCEF は新規に CCR コマンドを送信して、使用状況モニタリングキーの累積使用量を報告します。
- PCRF が要求した使用状況レポート：PCRF が Usage-Monitoring-Report を USAGE_MONITORING_REPORT_REQUIRED に設定して Usage-Monitoring-Information を提供すると、PCEF は時間使用状況情報を送信します。モニタリングキーが PCRF によって提供される場合、そのモニタリングキーの時間使用状況は、使用量しきい値に関係なく PCRF に通知されます。モニタリングキーが PCRF によって提供されない場合、有効なすべてのモニタリングキーの時間使用状況が PCRF に通知されます。
- イベントベースのレポート：イベントベースのレポートは、CLI コマンド **event-update send-usage-report events** を使用して有効化できます。SGSN 変更、QoS 変更、再検証タイムアウトなどのイベントがこの CLI で設定されると、そのイベントが発生するたびに時間使用状況レポートが生成されます。

使用状況が報告されると、使用量カウンタはゼロにリセットされます。PCEF は、しきい値に達した後、PCRF によって新しいしきい値が提供されるまで、時間使用状況の追跡を 0 から継続します。使用状況が報告された IP-CAN セッション変更の確認応答で、PCRF から新しい使用量しきい値が提供されない場合、その IP CAN セッションを対象とした PCEF での時間使用状況モニタリングは続行されません。

Gx を介した時間レポート機能を設定する方法については、「Gx を介した時間レポートの設定（83 ページ）」を参照してください。

Gx を介した時間レポートの設定

ここでは、Gx を介した時間レポートを有効にするのに必要な設定について説明します。

Gx を介した時間レポートを有効にするには、次の設定を使用します。

```
configure
     active-charging service <ecs_service_name>
          rulebase <rulebase_name>
             action priority <priority> dynamic-only ruledef <ruledef_name>
 charging-action <charging_action_name> monitoring-key <monitoring_key>
                exit
          exit
     context <context_name>
          ims-auth-service <imsa_service_name>
               policy-control
                    event-update send-usage-report [ reset-usage ]
                    end
```

注：

- Gx を介した時間レポートを有効にするための設定は、Gx を介したボリュームレポートの設定と同じです。PCRF から時間しきい値を受信すると時間モニタリングが実行され、ボリュームしきい値を受信するとボリュームモニタリングが実行されます。
- PCEF が受け入れる最大モニタリングキー値は 4294967295 です。PCEF がより大きい値を送信すると、値は符号なし整数値に変換されます。
- **event-update** CLI を使用すると、イベントの更新時に時間使用状況レポートを送信できます。オプションキーワード **reset-usage** を使用すると、差分レポートをサポートできます。このレポートでは、使用状況が報告され、PCEF でリセットされます。このオプションが設定されていない場合、イベント更新の一部として時間使用状況の情報を送信しますが、PCEF でリセットすることはしません。

PCRF への複数のアクティブおよびスタンバイ Gx インターフェイスのサポート

以前の Gx の実装では、Diameter ポリシー制御アプリケーションに、IMS 認証サービスの一部としてホストを強制的に設定するか、ホストテンプレートを関連付けて、サブスクライバセッションごとに通信するホストを選択するという制限がありました。ピアの選択は diabase で実行でき、アプリケーションはホストを選択する必要がないため、この機能は、アプリケーションに課されていた制限を取り除き、diabase がラウンドロビン方式でピアを選択できるようにするために開発されました。さらに、この機能により、アプリケーションによって選択されたホストがアクティブでない場合でも、diabase でのピアの選択が処理されます。デフォルトの動作では、アプリケーションでのサーバー検出が失敗した場合にコールがドロップされるため、この動作の変更は、CLI コマンドの「**endpoint-peer-select**」によって制御されます。

コールが確立されると、IMSA モジュールは、接続されるプライマリピアとセカンダリピアを選択するために、IMSA サービスに関連付けられたホスト選択テーブル/プレフィックステーブル/ホストテンプレートをチェックします。ホストテーブル/プレフィックステーブル/ホストテンプレートが設定されていない場合、プレフィックステーブル内のどの行も一致しない場合、または IMSA によって選択されたホストが非アクティブである場合、CLI 設定に基づいて diabase モジュールに制御が渡され、ラウンドロビン方式でピアが選択されるか、CLI 設定に基づいてコールが終了します。

CCR メッセージが diabase エラー/Tx 期限切れ/応答タイムアウトになった場合、IMSA は、障害が発生したピアを除外することで diabase に代替ルートを選択させ、ルックアップが成功した場合はそのピアに切り替えます。

CCR/CCA メッセージが、diabase によって選択された直接接続ホストと交換され、新しいホストから RAR メッセージが受信されると、IMSA は、ホスト設定チェックをスキップし、新しいホストとのさらなる通信を許可します。コールの確立中に直接接続ホストがアプリケーションによって選択された場合、IMSA は、アプリケーションごとに新しいホストがセカンダリサーバーかどうかをチェックします。CCR/CCA メッセージが、diabase によって選択された DRA を介して間接的に接続されたホストと交換され、別の DRA を介して同じホストから RAR メッセージが受信されると、IMSA は、ホスト設定チェックをスキップし、新しい DRA を介した同じホストとのさらなる通信を許可します。コールの確立中に DRA がアプリケーションによって選択された場合、IMSA は、アプリケーションごとに新しい DRA がセカンダリサーバーか

どうかをチェックします。別の DRA を介して異なるホストから RAR メッセージを受信した場合でも、IMSA は、ホスト設定チェックをスキップし、新しい DRA を介した新しいホストとのさらなる通信を許可します。

障害シナリオにおける diabase での Diameter ピア選択の設定

次の設定により、IMSA で障害が発生した場合に diabase が Diameter ピアを選択できるようになります。

```
configure
   context context_name
      ims-auth-service service_name
         policy-control
            endpoint-peer-select [ on-host-select-failure |
on-inactive-host ]
            { default | no } endpoint-peer-select
            end
```

注：

- このコマンドは、IMS 承認アプリケーションによってホストを選択できなかった場合、または IMS 承認アプリケーションによって選択されたホストが非アクティブの場合に、データベースでサーバー選択を実行するために使用されます。たとえば、ホストテーブルが IMSA サービスで設定されていない場合、ホストテーブルは設定されているがアクティブ化されていない場合、プレフィックステーブルのどの行もサブスクライバと一致しない場合、ホストテンプレートが IMSA サービスに関連付けられていない場合、ホストテンプレートがホストを選択できなかった場合などです。
- **on-host-select-failure**：IMS 承認アプリケーションがホストを選択できなかった場合に diabase でサーバー選択を実行するように指定します。
- **on-inactive-host**：アプリケーションによって選択されたホストが非アクティブである場合に、diabase でサーバー選択を実行するように指定します。
- この CLI コマンドは、IMS 承認アプリケーションでサーバー選択が失敗した場合にコールを終了する以前の動作との下位互換性を維持するために、ポリシー制御設定モードで追加されます。

Gx インターフェイスにおける複数 CCR-U のサポート

ASR 5500 は、IMS 承認サービス コンフィギュレーション モードで設定可能な CLI コマンド「**max-outstanding-ccr-u**」を使用して、セッションごとに同時に複数の CCR-U メッセージをサポートします。よって、この CLI では、セッションあたりの CCR-U メッセージの最大数として、最大 12 の値を設定できます。

CLI ベースの実装では、要求メッセージがトリガーされたときにそのまま送信し、受信時に応答を処理できます。応答メッセージが順不同で受信された場合、ゲートウェイは順序の変更を行います。

PCRF に対する複数の未処理メッセージをサポートするには、次の項目がサポートされている必要があります。

- IMSA が複数の CCR-U メッセージを送信できる：これは、IMS 承認サービス コンフィギュレーション モードで **max-outstanding-ccr-u** コマンドを使用することで実現できます。
- 順序付けのための応答メッセージのキューイング：DPCA は、受信順序に関係なく、受信メッセージを解析する必要があります。IMSA は、応答をセッションマネージャに転送するか、ローカルでキューに入れるかを判定します。
- ピアスイッチ：複数の CCR-U がトリガーされると、IMSA は送信される各要求に対して Tx タイマーを開始します。Tx の最初の期限切れ時に、IMSA/DPCA はピアの切り替えを行います。つまり、IMSA は他のすべての要求の Tx タイマーを停止し、セカンダリピアに切り替えるか（可能な場合）、適切な障害処理アクションを実行します。
- 障害処理：Tx 期限切れによるピアスイッチ障害が発生した場合、DPCA は、ims-auth-service にある設定に基づいて障害処理アクションを実行します。
- バックプレッシャの処理：プライマリ PCRF に対して複数の CCR-U がトリガーされた場合、Tx タイムアウトによりすべてのメッセージがセカンダリ PCRF に切り替えられます。セカンダリサーバーがすでにバックプレッシャ状態にある場合、IMSA は最初のメッセージをバックプレッシャキューに入れ、メッセージが処理されると、次の保留中の要求が BP キューに入れられます。
- ボリュームレポート：使用状況レポートの複数の CCR-U が（別々のモニタリングキーに対して）トリガーされ、障害処理が「**continue send-ccrt-on-call-termination**」として設定されている場合、最初の Tx タイムアウトまたは応答タイムアウト時に、すべての CCR-U の使用状況レポートが ECS に送信されます。サブスクライバがダウンすると、未報告のすべての使用状況が CCR-T メッセージで送信されます。「**event-update send-usage-report**」CLI が存在する場合、複数の CCR-U の同じモニタリングキーの使用状況がレポートされる可能性があります。

max-outstanding-ccr-u CLI コマンドは複数 CCR-U の設定をサポートしますが、一度に送信されるアクセス側更新用の未処理の CCR-U は 1 つだけであり、内部更新用には複数の CCR-U が送信されます。

CCR-U がトリガーされる可能性があるアクセス側更新は次のとおりです。

- ベアラーリソースコマンド
- ベアラー要求の変更（S-GW の変更、RAT の変更、ULI の変更）
- ベアラー変更コマンド

CCR-U がトリガーされる内部更新は次のとおりです。

- S-GW の復元
- ベアラーのダウン（GGSN、BCM UE_Only）
- ULI/タイムゾーンの通知
- デフォルト EPS ベアラー QoS の障害
- APN AMBR の障害
- Charging-Rule-Report
- クレジットの不足/クレジットの再割り当て
- 使用状況レポート
- テザリングフロー検出
- アクセスネットワーク課金識別子

バックツーバック CCR-U をサポートするためのゲートウェイノードの設定

次の設定コマンドを使用すると、ゲートウェイによるPCRFへの複数のバックツーバックCCR-Uの送信が有効または無効になります。

```
configure
   context  context_name
      ims-auth-service   service_name
         policy-control
            [ default ] max-outstanding-ccr-u value
            end
```

注：

- *value* は、1 から 12 までの整数値にする必要があります。デフォルト値は 1 です。

Gx インターフェイスにおける RAN/NAS 原因 IE のサポート

3GPP TS 29.212 のリリース 12 仕様に準拠するために、新規サポート機能として「Netloc-RAN-NAS-Cause」が導入されました。この機能は、アクセスネットワークからPCRFにRANやNASの詳細なリリース原因コード情報を送信するために使用されます。利用するには、NetLoc 機能もサポートされている必要があります。

重要 この機能は、NetLoc機能のライセンスがインストールされている場合にのみ有効にできます。

NetLoc-RAN-NAS-Causeをサポートする機能が有効になっている場合には、Charging-Rule-Report AVP と、ベアラーおよびセッション削除イベントの CCR-T にそれぞれ、新しい Diameter AVP「RAN-NAS-Release-Cause」が含まれます。このAVPは、サブスクライバまたはベアラーの終了の原因コードを示します。

サポートされる機能「Netloc-RAN-NAS-Cause」の設定

次の設定では、サポートされている機能「Netloc-RAN-NAS-Cause」が有効になります。

```
configure
    context  context_name
         ims-auth-service  service_name
              policy-control
                   diameter encode-supported-features
netloc-ran-nas-cause
                   end
```

注：

- **netloc-ran-nas-cause**：Netloc-RAN-NAS-Cause 機能を有効にします。この機能はサポートされますが、デフォルトでは無効になっています。
- サポートされている機能である [netloc-ran-nas-code] と [netloc] を有効にすると、netloc-ran-nas-cause コードが PCRF に送信されます。

このサポートされている機能を無効にするには、次のコマンドを使用します。

```
[ default | no ] diameter encode-supported-features
```

Gx インターフェイスを介した ADC ルールのサポート

このリリースでは、P-GW は、3GPP 標準規格のリリース 11 仕様で定義されているように、Gx を介してアプリケーションの検出と制御（ADC）機能を使用します。

Gx を介した ADC 拡張は、特定のプロトコルまたはプロトコルのグループの開始と停止に関して PCRF に通知する機能を提供し、PCRF がこの情報を認識して、ユーザーがアプリケーションの使用を開始して、それが終了するまでの間、ユーザーの QoS を変更できるようにします。

ADC 情報のプロビジョニングは ADC ルールを介して行われ、PCRF によって開始されるアクションは PCC ルールを介して行われます。

ADC ルールは、アプリケーションフローの指定、検出、およびレポートをサポートするための動的な事前定義されたいくつかの PCC ルールを拡張したものです。これらのルールは、CCA-I/CCA-U/RAR イベントを介して PCRF によってインストール（変更/削除）されます。ADC ルールは、動的な PCC ルールまたは事前定義された PCC ルールのいずれかにすることができ、動的ルールおよび事前定義ルールの既存の属性が適用されます。

動的な PCC ルールには、トラフィックフローフィルタまたはアプリケーション ID のいずれかが含まれます。アプリケーション ID が存在する場合、ルールは ADC ルールとして扱われます。アプリケーション ID は、Boxer の設定で事前に定義されている ruledef の名前です。この ruledef には、P2P プロトコルによってサポートされているアプリケーションを定義するアプリケーションフィルタが含まれています。

PCEF は、PCRF インターフェイスから受信した ADC ルールを処理およびインストールし、指定されたアプリケーションを検出し、アプリケーショントラフィックの検出を PCRF に報告します。次に、PCRF はアプリケーショントラフィックのレポートを制御します。

PCEF は、PCRF によって有効になっている指定のアプリケーションをモニターし、アプリケーション ID を含む開始/停止イベントを生成します。このようなアプリケーション検出は、ADC PCC ルールがバインドされるベアラーとは無関係に実行されます。たとえば、ADC ルールが専用ベアラーにインストールされている一方で ADC トラフィックがデフォルトのベアラーで受信された場合でも、アプリケーション検出ユニットは PCRF に開始イベントを報告します。

重要 ADC ルールのサポートは、ライセンスで制御される機能です。特定のライセンス要件の詳細については、シスコのアカウント担当者にお問い合わせください。

この機能をサポートするため、次の Diameter AVP が Charging-Rule-Definition AVP に新たに追加されました。この AVP は、PCEF が PCRF から受信します。

- TDF アプリケーション識別子：PCEF 内のアプリケーションの検出と制御 PCC ルールが適用されるアプリケーション検出フィルタを参照します。TDF アプリケーション識別子 AVP は、PCRF へのレポート内のアプリケーションも参照します。

- Redirect-Information：検出されたアプリケーショントラフィックを別の制御対象アドレスにリダイレクトする必要があるかどうかを示します。
- Mute-Notification：この AVP は、PCEF からの特定の ADC/PCC ルールについて、検出されたアプリケーションの開始/停止の PCRF への通知をミュートするために使用されます。
- Application Detection Information：Mute-Notification AVP が課金ルールレポートに含まれておらず、APPLICATION_START/APPLICATION_STOP イベントトリガーが有効になっている場合、PCEF は TDF アプリケーション識別子に対応する PCRF に Application-Detection-Information を送信します。

さらに、2 つの新しいイベントトリガー「APPLICATION_START」および「APPLICATION_STOP」が、レポート目的で生成されます。

制限事項

ADC over Gx 機能の制限事項は以下のとおりです。

- ADC は ruledef のグループをサポートしていません。
- 重複するアプリケーション ID の登録はサポートされません。
- P2P フローの再アドレス付け/リダイレクションはサポートされません。
- リダイレクションは、GET/Response のトランザクションでのみ発生します。
- ポートベース、IP プロトコルベース、および URL ベースのアプリケーションはサポートされていません。
- ダイナミック ADC ルールの事前設定オプション（precedence、redirect-server-ip）はサポートされていません。
- 同じサブスクライバのアプリケーションの同時インスタンスは区別されません。
- アプリケーションフローでは、フローリカバリがサポートされていません。

Gx を介した ADC ルールの設定

次の設定により、Gx インターフェイスを介した ADC ルールが有効になります。

```
configure
   context  context_name
      ims-auth-service   service_name
         policy-control
            diameter encode-supported-features adc-rules
            end
```

注：

- キーワード「**adc-rules**」は、機能固有のライセンスが設定されている場合にのみ使用できます。
- ADC の場合、サポートされている機能の第 6 ビットが設定されます。

Gx を介した ADC ルールのサポートを無効にするには、次のコマンドを使用します。

```
[ default | no ] diameter encode-supported-features
```

TDF アプリケーション識別子での GoR 名のサポート

ASR 5500 では、TDF アプリケーション識別子として GoR 名を使用してインストールするダイナミックルールがサポートされています。ADC ルールが PCRF からダイナミックルールとしてインストールされている場合、TDF アプリケーション識別子には、P-GW で事前設定された GoR 名を含めることができます。

ADC 機能が有効になっている場合、PCRF は、P-GW 設定で事前定義された GoR の名前として、TDF アプリケーション識別子を送信できます。

- Charging-Rule-Definition AVP を使用したダイナミック課金ルールが PCRF からアクティブ化されると、PCRF は、ECS で TDF アプリケーション識別子として設定された GoR 名を指定できます。
- Charging-Rule-Definition AVP を含むダイナミック課金ルールがアクティブ化されると、PCRF は、RAR を使用して、Charging-Rule-Definition を介してルールを削除または変更できます。ルールの有効化または変更の際に、PCRF は、ルールの課金ルール属性を追加、変更、または削除できます。

PCRF からの TDF アプリケーション識別子の設定の変更を以下に示します。

- 非 ADC ダイナミックルールは、関連する ruledef または GoR 名とともに TDF アプリケーション識別子 AVP を送信することで、ADC ダイナミックルールに変更できます。

  ADC ダイナミックルールを非 ADC ダイナミックルールに変更することはできません。

- PCRF からの受信後に、次の AVP が変更され、適用されます。
  - 優先順位（Precedence）
  - Rating-Group/Service-Identifier/Sponsor-Identity（レポートレベルに応じて必須）
  - Metering-Method
  - Online/Offline
  - QoS-Information
  - Monitoring-Key
  - Redirect-Information
- ダイナミックルートは、TDF アプリケーション識別子 GoR の一部であるルールの全プロトコルに対して更新されます。
- ダイナミックルールの優先順位または TDF アプリケーション識別子の値が変更されると、新しいルール照合として APP-START および APP-STOP イベント通知が送信されます。ルール変更の前に APP-START 通知が送信されている場合、対応する APP-STOP 通知は送信されません。
- 関連付けられた GoR のランタイム削除はすぐに有効になり、APP-START がすでに送信されている場合、APP-STOP 通知は送信されません。サービスレベルでの GoR の追加では、

ダイナミック ADC ルールと事前定義された ADC ルールの両方で新しい追加を有効にするために、ルールを再インストールする必要があります。

ADC ミュートのカスタマイズ

以前は、3GPP ADC over Gx はアプリケーションのミュートステータスの変更をサポートしていませんでした。アプリケーションがミュートされると、ミュートを解除できませんでした。リリース 21.1 から、この機能にカスタム MUTE およびカスタム UNMUTE の機能が導入されました。ASR 5500 PCEF では、アプリケーション検出情報 CCRU のレポートを制御するためのカスタマイズをサポートするようになりました。このために、カスタム MUTE とカスタム UNMUTE という 2 つの可能な値を持つ AVP が導入されました。

- Gx メッセージには、標準ベースの MUTE とカスタム MUTE の両方が含まれている場合があります。
- 標準ベースの MUTE は、カスタムの MUTE および UNMUTE よりも優先されます。
- ダイナミック ADC ルールは、カスタム MUTE を使用してインストールおよび変更できます。
- Custom-Mute-Notification AVP は、CCA-I および RAR の PCRF によって送信できます。
- ダイナミック ADC ルールは、カスタム UNMUTE を使用して変更できます。
- 特定のダイナミック ADC ルールのカスタム MUTE では、PCEF はフローごとに APPLICATION_START/APPLICATION_STOP 応答を送信するのではなく、アプリケーション トラフィック全体に対して 1 つの APPLICATION_START/APPLICATION_STOP 応答を送信します。
- 特定のダイナミック ADC ルールのカスタム MUTE では、カスタム MUTE の前に APPLICATION_START が送信されていない場合、ダイナミックルールにヒットする次のフローパケットで 1 つの APPLICATION_START が送信されます。
- 特定のダイナミックルールのカスタム MUTE では、APPLICATION_START 応答がフローの 5 タプル情報とともに送信されます。
- 特定のダイナミックルールのカスタム MUTE では、APPLICATION_START 応答が TDF-Application-Instance-Identifier = 0 で送信されます。
- 特定のダイナミックルールのカスタム MUTE では、特定のダイナミックルールに関連付けられた最後のフローが終了すると、1 つの APPLICATION_STOP が送信されます。このような APPLICATION_STOP には、最後のフローの 5 タプル情報は含まれず、TDF-Application-Instance-Identifier = 0 で送信されます。
- 特定のダイナミックルールのカスタム UNMUTE では、APPLICATION START 応答が特定のダイナミックルールと照合された後、その後のすべてのフローに送信されます。
- カスタム UNMUTE の動作に変更はありません。これは、UNMUTING 以前はカスタム MUTED でも標準 MUTED でもありませんでした。APPLICATION_START および APPLICATION_STOP は、以前と同様に、フローごとに引き続き送信されます。
- カスタム UNMUTE では、PCEF は、終了するすべてのフローに対して APPLICATION_STOP を送信し、次に進みます。
- 特定のダイナミックルールは、カスタム MUTE または UNMUTE ステータスを含む SR と ICSR の両方で回復されます。特定のダイナミックルールの APPLICATION_START ステー

タスがチェックポイント化され、回復されます。これにより、リカバリ後に余分な APPLICATION_START が PCRF に送信されなくなります。

ADC カスタムミュート/ミュート解除機能の強化

機能情報

要約データ

[ステータス（Status）]	変更された機能
導入されたリリース	21.1
変更されたリリース	21.2
対象製品	SAEGW
該当プラットフォーム	ASR 5500
デフォルト設定	無効
関連する CDETS ID	CSCvd00699
このリリースでの関連する変更点	N/A
関連資料	Command Line Interface Reference SAEGW Administration Guide

マニュアルの変更履歴

重要 リリース 21.2 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	リリース	リリース日
このリリースで変更。	21.2	2017 年 4 月 27 日

変更された機能

「ADC ミュートのカスタマイズ」機能により、アプリケーション検出情報 CCRU のレポートを制御するカスタム MUTE/UNMUTE 機能が導入されました。PCRF はカスタム MUTE PCRF AVP を使用して、ADC アプリケーション通知を無効または有効にするタイミングを P-GW に通知するようになりました。

この機能は「ADC ミュートのカスタマイズ」機能をさらに強化し、カスタムミュートとミュート解除イベント間のフローアクティビティを報告します。P-GW はカスタムミュートイベント間のフローアクティビティを学習し、ADC ルールでカスタムミュート解除イベントが発生し

た後に PCRF に報告します。これにより、標準の ADC のミュートおよびミュート解除ケースで、ADC アプリケーションの開始および停止メカニズムが最小限となります。

新しい CLI コマンドが設定に応じてルールベースで実装されるようになりました。ルールごとに 1 回のみ、ADC アプリケーションの開始と停止が報告されます。これは、PCRF へのメッセージングフローを削減するのに役立ちます。

制限事項

この機能には次の制限があります。

- P-GW では、ADC ルールごとに最大 12 の学習済みフローが保存されます。上限の 12 に達すると、P-GW は最も古いフローの学習データを削除し、最新のフローについて学習します。P-GW がカスタムミュート解除イベントを受信すると、学習した通知内容を PCRF に伝えます。フローのアプリケーション開始通知が送信された場合、P-GW はアプリケーション停止通知を送信します。
- カスタムミュート解除のイベントが回復されない場合、アプリケーション開始通知を PCRF に送信するためにフロー情報が保存されます。
- LTE から Wi-Fi へのハンドオーバーでは、ADC ダイナミックルールごとのカスタムミュートまたはカスタムミュート解除で PCRF から受信した値が新しい RAT に適用されます。ハンドオーバーコンテキストで値が受信されない場合、存在するすべての ADC ダイナミックルールについて、RAT 変更前の以前の値が保持されます。
- CLI コマンド **adc notify** が有効になっている場合は、単一の ADC アプリケーションの開始と停止の通知が PCRF に送られます。同じ ADC ダイナミックルールに一致する複数のフローがある場合、1 つのアプリケーション開始通知と停止通知のみが PCRF に送信されます。
- この機能はダイナミックルールにのみ実装されます。

機能の仕組み

P-GW がパケットを受信し、ADC ルールイベントが PCRF から発生したときのイベントシーケンスは次のとおりです。

1. パケットが ECS ルールマッチングエンジンに到達します。
2. ルールマッチングエンジンは、ADC ダイナミックルールが一致するかどうかを確認します。また、PCRF やルールベースレベルの CLI を介してカスタムミュートが適用されているかどうかも確認します。単一のアプリケーション開始通知が以前に送信されていない場合は、送信されます。
3. 同じ ADC ルールに一致するすべての後続フローについて、アプリケーション開始通知が保存されます。これらの通知は、カスタムミュート解除イベントの受信後に CCRU で送信されます。

重要なポイントは次のとおりです。

- PCRF から受信した値の優先順位が最も高くなります。したがって、標準ミュートはカスタムミュートやカスタムミュート解除よりも優先されます。CLI *adc notify one* の優先順位が最も低くなります。
- CLI **adc notify one** がルールベースで設定されている場合、その逆の **no adc notify** が影響することはありません。CLI の影響を回避するには、次のタスクのいずれかを実行します。
  - CLI **adc notify once** が設定されていないルールベースに切り替えます。
  - その特定のダイナミックルールの「カスタムミュート解除」を送信します。

ADC 通知の設定

新しい CLI コマンド **adc notify**が、アクティブ課金サービスモードに追加されました。

この CLI が設定されると、ルールごとの ADC フローの一致に対して単一のアプリケーション開始通知またはアプリケーション停止通知が PCRF に送信されます。この CLI が設定され、PCRF がカスタムミュート通知を送信した場合、PCRF 通知は、通知をレポートするための標準的な動作よりも優先されます。

このキーワードのデフォルト値は false です。この CLI が設定されていない場合、ADC 通知の送信時にアクションは実行されません。

この機能を有効または無効にするには、以下のコマンドを入力します。

```
configure
  active-charging service <service_name>
    rulebase <rulebase_name>
      [no] adc notify [once]
      end
```

1 つの通知を設定するには、次のコマンドを使用します。

```
adc notify once
```

注：

- **no:** ADC 通知を無効にします。ADC 通知はデフォルトの動作に従って送信されます。
- **adc:** ADC 通知を設定します。
- **notify:** アプリケーション通知を設定します。このキーワードが設定されていない場合、ADC 通知はデフォルトの動作に従って送信されます。
- **once:** アプリケーション通知を 1 回だけ設定します。PCRF が優先されます。

TAI および ECGI 変更レポートのサポート

このセクションでは、TAI および ECGI 変更レポート機能の概要と導入について説明します。

このセクションでは、この機能に関する次のトピックについて説明します。

- 機能説明 （95 ページ）

機能説明

Gx を介した UE のユーザーロケーションレポートをアクティブ化する場合、PCRF は「USER_LOCATION_CHANGE（13）」イベントトリガーを使用して RAR と CCA を送信します。このイベントトリガーを受信すると、P-GW は通常、変更レポートアクション（CRA）情報要素（IE）を「レポート開始」とともに MME に送信し、MME 内の UE のロケーション変更レポートを有効にします。

現在のアーキテクチャでは、「USER_LOCATION_CHANGE（13）」トリガーを使用して、ユーザーロケーション情報（ULI）、トラッキング領域 ID（TAI）、および E-UTRAN セルグローバル ID（ECGI）の変更が報告されます。show configuration コマンドで新しいイベントトリガーを表示するために、CLI が変更されました。

重要 TAI レポートを機能させるには、値 33 を使用するように、ポリシー制御コンフィギュレーション モードで **diameter map usage-report** CLI コマンドを設定する必要があります。

PCRF は、TAI と ECGI の変更を報告するための CRA イベントをサブスクライブします。P-GW は、PCRF によってサブスクライブされた場合にのみ CCR-U でイベントトリガーを送信します。PCRF が ECGI の変更や TAI の変更のイベントトリガーをインストールすると、ECGI と TAI の変更（インストールされているトリガーに基づく）が報告されます。

TAI および ECGI 変更レポート機能は、3GPP TS 29.212 v9.7.0 に準拠しています。この機能は Gx インターフェイスでサポートされているため、ECGI や TAI の変更時に UE が追跡され、PCRF に報告できます。ユーザーロケーション情報に関するレポート機能の詳細については、展開している製品のアドミニストレーション ガイドを参照してください。

CRA 値は、PCRF から受信したイベントトリガーによって異なります。

Change Reporting Support Indication（CRSI）と ULI も、ベアラーリソースコマンドでサポートされています。

P-GW は、対応するベアラー削除応答を受信すると、ベアラー削除コマンドで MME からの受信した ULI を PCRF に送信します。ULI がベアラー削除コマンドとベアラー削除応答の両方に含まれている場合、ベアラー削除応答の ULI が PCRF に送信されます。ベアラー削除応答に ULI がない場合、ベアラー削除コマンドで受信した ULI が PCRF に送信されます。

他の機能との関係

この機能は、Event-Trigger AVP の USAGE_REPORT 値に依存しています。この機能は、USAGE_REPORT の値が 33 に設定されている場合にのみ機能します。これは、ポリシー制御コンフィギュレーション モードで **diameter map usage-report** CLI コマンドを使用して実現できます。

機能の仕組み

P-GW は、P-GW によって検出されたイベントトリガーに基づいて、イベントトリガー値を CCR-U で送信します。P-GW は、次の表に従って、イベントトリガーと ULI タイプを CCR-U で PCRF に送信します。

PCRF からのイベントトリガー	**CRA** 値	**P-GW** で検出されたイベント	**PCRF** への通知内容
ULI_CHANGE	6	TAI_CHANGE または ECGI_CHANGE	イベントトリガー：ULI_CHANGE ULI タイプ：TAI + ECGI
TAI_CHANGE	3	TAI_CHANGE	イベントトリガー：TAI_CHANGE ULI タイプ：TAI
ECGI_CHANGE	4	ECGI_CHANGE	イベントトリガー：ECGI_CHANGE ULI タイプ：ECGI
ULI_CHANGE + TAI_CHANGE	6	TAI_CHANGE	イベントトリガー：ULI_CHANGE+ TAI_CHANGE ULI タイプ：TAI+ECGI
ULI_CHANGE + ECGI_CHANGE	6	ECGI_CHANGE	イベントトリガー：ULI_CHANGE + ECGI_CHANGE ULI タイプ：TAI+ECGI
ULI_CHANGE + TAI_CHANGE + ECGI_CHANGE	6	TAI/ECGI が変更された	イベントトリガー：ULI_CHANGE + TAI/ECGI CHANGE ULI タイプ：TAI+ECGI
TAI_CHANGE + ECGI_CHANGE	6	TAI/ECGI が変更された	イベントトリガー：TAI_CHANGE/ECGI_CHANGE ULI タイプ：TAI+ECGI

PCRF からのイベントトリガー	CRA 値	P-GW で検出されたイベント	PCRF への通知内容
特に上記に記載されていない組み合わせについては、	6		イベントトリガー：ULI_CHANGE ULI タイプ：TAI+ECGI

制限事項

TAI および ECGI 変更レポート機能は、**diameter map usage-report** CLI コマンドが 33 に設定されている場合にのみサポートされます。

TAI および ECGI 変更レポート機能のモニタリングと障害対応

ここでは、TAI および ECGI 変更レポート機能のサポートにおける show コマンドとその出力について説明します。

show ims-authorization sessions full all

この機能をサポートするこの show コマンドの出力に、以下のフィールドが追加されました。

- TAI-Change：サブスクライバセッションの TAI が変更された場合に、このイベントトリガーを表示します。
- ECGI-Change：サブスクライバセッションの ECGI が変更された場合に、このイベントトリガーを表示します。

show ims-authorization service statistics all

この機能をサポートするこの show コマンドの出力に、以下の統計が追加されました。

- TAI 変更：P-GW が PCRF に TAI_CHANGE（26）イベントトリガーを報告した合計回数を表示します。
- ECGI 変更：P-GW が PCRF に ECGI_CHANGE（27）イベントトリガーを報告した合計回数を表示します。

ロケーションベースのローカルポリシールール適用

このセクションでは、ロケーションベースのローカルポリシー（LP）ルール適用機能の概要と実装について説明します。

このセクションでは、この機能に関する次のトピックについて説明します。

- 機能説明 （98 ページ）
- 機能の仕組み （98 ページ）

- ロケーションベースのローカルポリシールール適用機能の設定 （100 ページ）
- ロケーションベースのローカルポリシールール適用機能のモニタリングと障害対応 （102 ページ）

機能説明

この機能は、サブスクライバが企業APNに接続したときに、さまざまなE-UTRANセルグローバル識別子（ECGI）に対して事前定義されたさまざまなルールをアクティブにするために導入されました。サブスクライバは、企業エリア外にいる場合は、企業 APN との接続を明示的にダウンし、インターネット APN とのセッションを再確立する必要があります。企業 APN は PCRF を使用せず、ローカルポリシーのみを使用することを前提としています。この場合、APN に一致するすべてのコールがローカルポリシーに転送されます。

重要 この機能を動作させるには、ローカルポリシーを有効にするライセンスを設定する必要があります。ライセンス要件の詳細については、最寄りのシスコのアカウント担当者にお問い合わせください。

ECGIに対して事前定義されたさまざまなルールをアクティブ化するために、ローカルポリシーの設定は以下をサポートするように拡張されています。

- 一連の ECGI の設定と検証
- 変更レポートアクション（CRA）イベントによる ECGI_CHANGE イベントトリガーのインストール
- ECGI_CHANGE イベントの検出

この機能は、ローカルポリシー ruledef 条件との ECGI 一致に基づいて適用される次のアクションをサポートしています。

- ECGI が特定のグループに属した場合の ECGI_CHANGE イベント通知のリダイレクトルールを有効にする
- 他の ECGI に対するワイルドカードルールを有効にする

他の機能との関係

この機能は、TAI および ECGI 変更レポート機能に依存しています。これにより、セッションマネージャ モジュールから IMSA/ローカルポリシーモジュールへの ECGI 変更をレポートするためのフレームワークが提供されます。

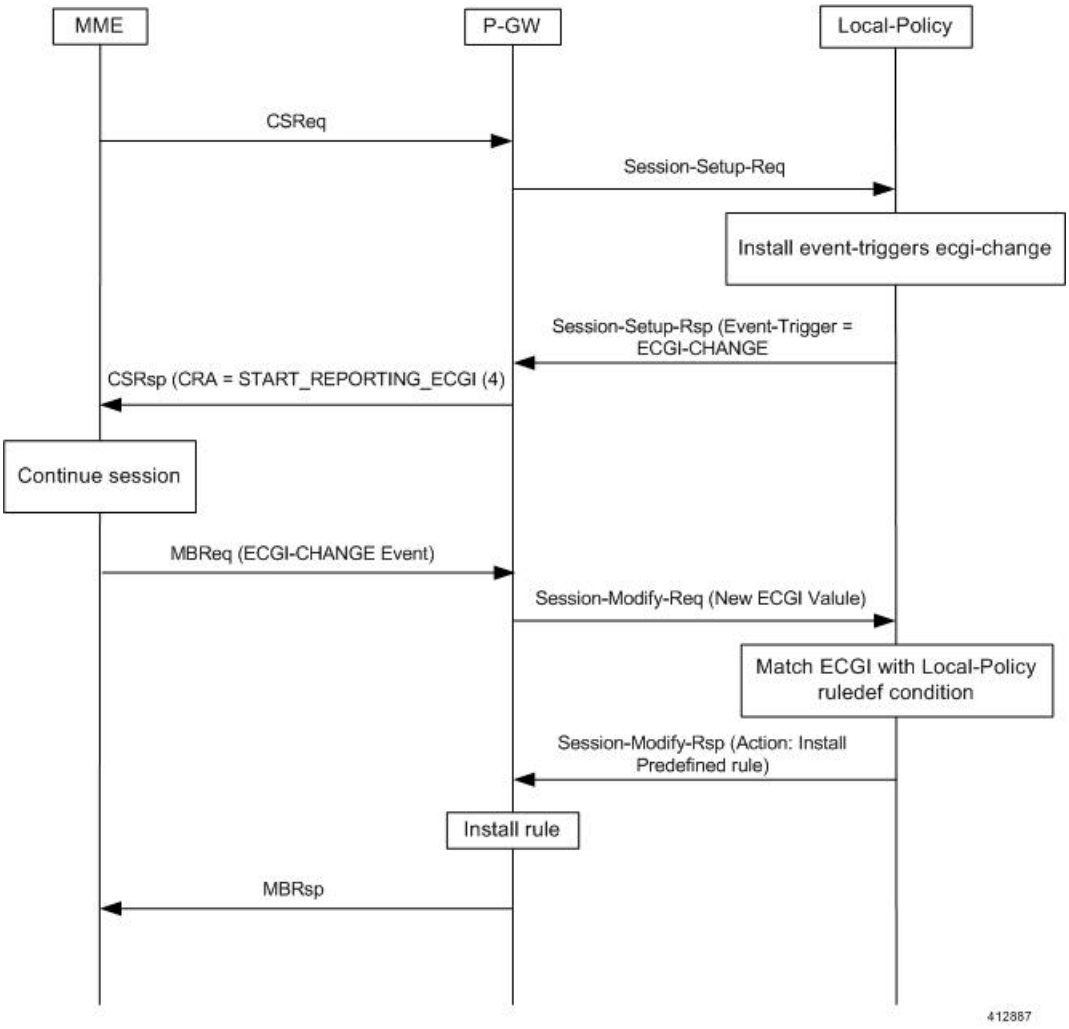
機能の仕組み

この項では、ECGI-CHANGE イベントトリガーに基づいて、ローカルポリシールールの選択と適用がどのように行われるかについて説明します。

Flows

次の図は、ECGI-CHANGE イベントがローカルポリシー、MME、および P-GW でどのように処理されるかを示しています。

図 *7 : ECGI* 変更イベントの処理



新しいコールが確立されると、ECGI 変更イベントトリガーがローカルポリシーから送信されます。P-GW は、セッション作成応答（CSRsp）で CRA 値 4 を送信して ECGI レポートを MME に要求します。MME は、変更通知要求/ベアラー変更要求（MBReq）を介して ECGI の変更を P-GW に通知します。P-GW でのローカルポリシー設定により ECGI 変更イベントが処理され、新しい ECGI が属する ECGI グループに基づいて適切なアクションが実行されます。1 つのアクションとして、ECGI が特定のグループに属する場合に特定のリダイレクトルールをアクティブ化することが考えられます。別のアクションとして、その他のすべての ECGI に対してワイルドカードルールを有効にすることが考えられます。

制限事項

ここでは、この機能の既知の制限について説明します。

- ECGI 変更の検出とトリガリングは、この機能の前提条件です。
- この機能は、特定の APN 内のすべての要求と応答が PCRF に接続せずにローカルポリシーに直接送信されるローカルポリシーのみ（lp のみ）モードでサポートされます。つまり、この機能は、ローカルポリシーフォールバックモードや、PCRF とローカルポリシーの両方が共存するデュアルモードでは機能しません。

ロケーションベースのローカルポリシールール適用機能の設定

このセクションでは、ECGI-Change イベント通知に基づいてルールの適用を有効にするための、local-policy 内パラメータの設定について説明します。

ECGI 変更トリガーの設定

次の設定を使用して、local-policy から ECGI-Change トリガーをインストールします。

```
configure
   local-policy-service service_name
      actiondef actiondef_name
         action priority priority event-triggers ecgi-change
         exit
      eventbase default
        rule priority priority event new-call ruledef ruledef_name actiondef
 actiondef_name [ continue ]
         end
```

注：

- **priority** *priority*：指定されたアクションの優先順位を指定します。*priority* は一意で、1 ～ 2048 の整数である必要があります。
- **ecgi-change**：このキーワードは、ECGI-CHANGE イベントトリガーをインストールするように指定します。有効にすると、ECGI-CHANGE イベントトリガーが local-policy から送信されます。
- 通信事業者が CRA 値を送信して MME で ECGI-Change 通知を有効にする場合は、この CLI コマンドを local-policy で設定します。

ECGI 変更イベントのルールの適用

次の設定を使用して、ECGI の変更の検出を有効にし、MME によって報告された ECGI-CHANGE イベントに対して特定のアクションを実行します。

```
configure
   local-policy-service service_name
      eventbase eventbase_name
         rule priority priority event ecgi-change ruledef ruledef_name
```

```
actiondef actiondef_name [ continue ]
         end
```

注：

- **priority** *priority*：指定されたルールの優先順位を指定します。*priority* は一意で、1 ～ 2048 の整数である必要があります。
- **ruledef** *ruledef_name*：ルールを特定の ruledef に関連付けます。*ruledef_name* は、このローカル QoS ポリシーサービス内にある既存の ruledef にする必要があります。
- **actiondef** *actiondef_name*：ルールを特定の actiondef に関連付けます。*actiondef_name* は、1 ～ 63 文字の英数字の文字列で表される、このローカル QoS ポリシーサービス内にある既存の actiondef である必要があります。
- **ecgi-change**：ECGI-CHANGE を検出する新しいイベントを有効にし、actiondef 設定で定義されているようにして ECGI-CHANGE イベントに特定のアクションを適用します。
- **continue**：後続のルールも照合されます。指定しない場合、ルールの評価は最初の一致の時点で終了します。

ECGI 値に基づくローカルポリシールールの適用

MME による ECGI-Change イベント通知で受信した ECGI 値に基づいてルールを適用するには、次の設定を使用します。

```
configure
   local-policy-service service_name
      ruledef ruledef_name
         condition priority priority ecgi mcc mcc_num mnc mnc_num eci { eq
| ge | gt | le | lt | match | ne | nomatch } regex | string_value | int_value
 | set }
         end
```

注：

- **priority** *priority*：指定された条件の優先順位を指定します。*priority* は一意で、1 ～ 2048 の整数である必要があります。
- **ecgi mcc** *mcc_num* **mnc** *mnc_num* **eci**：MCC、MNC、および ECI の値を使用して ECGI を設定します。
  - **mcc** *mcc_num* ：MCC は 001 ～ 999 の 3 桁の数字です。これは、サイズ 3 の文字列です。
  - **mnc** *mnc_num* ：MNC は 01 ～ 999 の 2 または 3 桁の数字です。これは、サイズ 2 ～ 3 の文字列です。
  - **eci**：ECI は 0x1 ～ 0xffffffff の 16 進数です。これは、サイズ 1 ～ 7 の文字列です。
- この CLI コマンドは、MME による ECGI-Change イベント通知で受信した特定の ECGI 値に基づいて通信事業者が特定のアクションを実行する場合に、local-policy で設定されます。

ロケーションベースの LP ルール適用設定の確認

次のコマンドを使用して、この機能の設定を確認します。

show configuration context

重要　この機能は、特定の APN 内のすべての要求と応答が PCRF に接続せずにローカルポリシーに直接送信されるローカルポリシーのみのモードでサポートされます。

この機能の設定例を次に示します。

```
configure
   context source
      apn corporate-apn
         ims-auth-service LocalPolicy_1
      exit
   exit
end

configure
   local-policy-service LocalPolicy_1
      ruledef any-imsi
         condition priority 1 imsi match *
      exit
      ruledef ecgi-group
         condition priority 1 ecgi mcc 123 mnc 456 eci eq ffff
      exit
      actiondef ecgi-trigger
         action priority 1 event-triggers ecgi-change
      exit
      actiondef ecgi-redirect-rule
         action priority 1 activate-rule namerule-1
      exit
      eventbase default
         rule priority 1 event new-call ruledef any-imsi actiondef
ecgi-trigger
         rule priority 2 event ecgi-change ruledef ecgi-group actiondef
ecgi-redirect-rule
        rule priority 3 event location-change ruledef ecgi-group actiondef
 ecgi-redirect-rule
      exit
   exit
end
```

ロケーションベースのローカルポリシールール適用機能のモニタリングと障害対応

この項では、ロケーションベースのローカルポリシールール適用機能のサポートに使用できる show コマンドとその出力について説明します。

この機能で問題が発生した場合、トラブルシューティングを行うには次の CLI コマンドを使用します。

show configuration context

logging filter active facility local-policy level debug

show local-policy statistics

show active-charging sessions full

show local-policy statistics summary

ECGI-CHANGE イベントトリガーのインストールをサポートするために、この show コマンドの出力に次の統計が追加されています。

- イベント統計：
  - ECGI Change：ローカルポリシーが受信した ECGI-CHANGE イベントトリガーの数を表示します。
- 変数一致統計
  - ECGI：ECGI が一致して、このイベントに基づいて特定のアクションが適用された回数を表示します。

GTP ベースの S2a/S2b の Gx サポート

GTP ベースの S2a/S2 インターフェイスの Gx サポートは、P-GW での Wi-Fi 統合のためにすべての顧客に拡張されました。この実装は、29.212 の標準 Rel. 8 Non-3GPP 仕様部分に準拠しており、加えて Rel. 10/Rel. 11 の C3-101419 C3-110338 C3-110225 C3-120852 C3-130321 C3-131222 CR に準拠しています。

この機能拡張の一部として、次の変更が導入されました。

- TWAN ID の AVP サポートが提供されました
- TWAN-ID が r8-gx-standard ディクショナリに追加されました

Gx ベースの仮想 APN の選択

このセクションでは、Gx ベースの仮想 APN 選択機能の概要と実装について説明します。

このセクションでは、この機能に関する次のトピックについて説明します。

- 機能説明 （104 ページ）
- Gx ベース仮想 APN 選択機能 （105 ページ）
- Gx ベース仮想 APN 選択のモニタリングと障害対応 （105 ページ）

機能説明

概要

現在の実装では、RADIUS またはローカル設定による仮想 APN（VAPN）の選択がサポートされています。ASR 5500 では、仮想 APN の選択に PCRF と Gx インターフェイスを使用してシグナリングの削減を実現しています。

機能ビットを 4 に設定する、新規のサポート機能「**virtual-apn**」が IMSA 設定に追加されました。この設定により、特定の IMS 承認サービスに対して Gx ベースの仮想 APN 選択機能が有効になります。この設定が P-GW や GGSN で有効になっている場合、P-GW または GGSN は、CCR-I の Supported-Features AVP を介してこの機能を PCRF にアドバタイズします。 VAPN が選択されている場合、PCRF は Experimental-Result-Code AVP が 5999（DIAMETER_GX_APN_CHANGE）に設定された CCR-I メッセージを拒否し、CCA-I の Called-Station-Id AVP メッセージを介して新しい APN を送信します。その後、既存のコールが切断され、新しい仮想 APN で再確立されます。Experimental Result Code 5999 にはシスコのベンダー ID が設定されていることに注意してください。

重要 この機能を有効にすると、（この機能を使用するコールの数に応じて）CPU に影響が出る可能性があります。

ライセンス要件

この機能を使用するには、有効なライセンスをインストールしてこの機能を設定する必要があります。特定のライセンス要件の詳細については、シスコのアカウント担当者にお問い合わせください。ライセンスのインストールと確認の詳細については、『システム管理ガイド』の「ソフトウェア管理操作」の「ライセンスキーの管理」の項を参照してください。

制限事項

この機能には次の制限があります。

- 新しい仮想 APN とのコールを確立するには、仮想 APN がサポートする機能のネゴシエーション、 実験結果コード（5999）、Called-Station-Id AVP を受信する必要があります。いずれかの条件が満たされていない場合、コールは終了します。
- また、CCA-I メッセージで受信した場合、障害処理は 5999 結果コードでは考慮されません。
- 実験結果コード 5999 が CCA-U で受信されると、障害処理アクションが実行されます。
- Called-Station-Id AVP を CCA-U または CCA-T で受信した場合、AVP は無視されます。
- ローカルポリシーによって開始された最初のメッセージで仮想 APN を受信すると、コールは終了します。
- PCRF が同じ仮想 APN を繰り返し送信すると、コールは終了します。

Gx ベース仮想 APN 選択機能

次のセクションでは、Gx ベース仮想 APN 選択を有効にするための設定コマンドについて説明します。

```
configure
    context  context_name
         ims-auth-service  service_name
              policy-control
                   diameter encode-supported-features virtual-apn
                   end
```

注：

- **virtual-apn**：このキーワードで、Gx ベース仮想 APN 選択機能の設定が有効になります。デフォルトでは、この機能は無効になっています。
- このキーワードはライセンスによって異なります。詳細については、シスコのアカウント担当者にお問い合わせください。

Gx ベース仮想 APN 設定の確認

Gx ベース仮想 APN 選択機能が Supported-Features AVP の一部として設定されているかどうかを表示するには、Exec モードで次のコマンドを使用します。

```
show ims-authorization sessions full all
```

この show コマンドの出力にある「Negotiated Supported Features」フィールドに、設定ステータスが表示されます。このサポートされている機能は、機能ライセンスが設定されている場合にのみ表示されます。

Gx ベース仮想 APN 選択のモニタリングと障害対応

この項では、この機能のサポートにおける show コマンドまたはその出力について説明します。

show ims-authorization policy-control statistics

新しい仮想 APN が選択された場合に PCRF が Diameter Experimental Result Code（5999）を送信する回数を追跡するために、この show コマンドの出力に次のフィールドが追加されました。

- **Gx APN Change**

この統計の詳細については、『*Statistics and Counters Reference*』を参照してください。

統計のデバッグ

Gx ベースの仮想 APN コールをデバッグするには、次のコマンドを使用します。

```
show session subsystem facility sessmgr debug-info
```

このコマンドは、Gx ベースの VAPN 機能に関連する詳細な統計を表示します。たとえば、受信した Gx VAPN の数、Gx VAPN を有効にした後の AAAMGR/SGX/DHCP メッセージの数、および Gx VAPN コールのセットアップ時間などを表示します。

Gx ベース仮想 APN 選択機能のバルク統計

IMSA スキーマ

次の新しいバルク統計変数が IMSA スキーマに追加され、新しい仮想 APN が選択された場合に PCRF が Diameter Experimental Result Code（5999）を送信する回数が追跡されるようになりました。

- dpca-expres-gx-apn-change

この変数の詳細については、『*Statistics and Counters Reference*』を参照してください。

システムスキーマ

PCRF から受信した仮想 APN の検証失敗が原因で P-GW、GGSN、または SAEGW セッションが切断された回数を追跡するために、次の新しい切断理由がシステムスキーマに追加されました。

- gx-vapn-selection-failed（618）

この変数の詳細については、『*Statistics and Counters Reference*』を参照してください。

異なるピアからの RAR の適切な処理

StarOS Gx アーキテクチャでは、ホストの選択が IMSA サービスで設定されている場合、すべての Diameter セッションがプライマリおよびセカンダリピアに関連付けられます。

PCRF と PCEF が複数の DRA を介して接続されているようなネットワークでは、PCRF がラウンドロビン方式で DRA を選択し、セッションの RAR がプライマリまたはセカンダリのいずれでもないピアから送信されることがあります。このようなシナリオを処理するために、プライマリでもセカンダリでもないピアから受信した RAR に応答する機能が追加されました。この場合、RAR への応答は、RAR の送信元であるピアを介して行われます。ただし、以降のセッションのシグナリングは以前に通信していたピアを介して行われます。セカンダリピアを介して RAR が受信されると、ホストスイッチが発生し、動作は変更されません。3 番目のピアからの RAR を処理できるようにするために、そのピアを Diameter エンドポイント設定で設定する必要があります。さらに言えば、この問題は、ホスト選択が IMSA サービスに設定されている場合にのみ発生します。ホスト選択がエンドポイントレベルで行われる場合、この問題は発生しません。

3 つの DRA があり、次の例に示すように設定されているとします。

```
configure
   context test
      diameter endpoint Gx
         ...
         peer DRA1 realm realmName address 192.168.23.3
         peer DRA2 realm realmName address 192.168.23.3 port 3869
         peer DRA3 realm realmName address 192.168.23.3 port 3870
         exit
      ims-auth-service imsa-Gx
```

```
        policy-control
           diameter host-select row-precedence 1 table 1 host DRA1
secondary host DRA2
end
```

この機能がない場合、DRA3 から RAR を受信すると、拒否されます。この機能を有効にすると、DRA3 からの RAR は DRA3 のみを介して応答されます。この場合、ピアの切り替えは発生せず、以前にピアの切り替えが発生していれば、後続のメッセージは DRA1 または DRA2 を介して送信されます。

制限事項

ここでは、この機能の制限について説明します。

- 異なる送信元ホストから受信された RAR は拒否されます。
- Diameter エンドポイントに設定されていない DRA から受信した RAR は拒否されます。

NetLoc の機能強化

この機能により、既存の NetLoc 機能に、3GPP 標準 R13 バージョンへの準拠が追加されます。

機能説明

重要 これはライセンスで制御される機能です。有効にするには、NetLoc 機能ライセンスキーが必要です。ライセンスの入手方法の詳細については、シスコのアカウント担当者にお問い合わせください。

この機能により、既存の NetLoc 機能に、3GPP 標準 R13 バージョンへの準拠が追加されます。この NetLoc 機能を使用して、IMS ネットワークは、WLAN アクセスネットワークから UE の位置情報を取得できます。これにより、位置関連の機能と、位置情報に基づく課金が強化されます。

この機能により、次の動作が変更されます。

- NetLoc 機能がシャーシで有効になっており、アクセスネットワーク情報（ANI-45）イベントトリガーがインストールされている場合、次の動作が変更されています。

表 *5 : PCRF* に対する *Gx* インターフェイスの動作の変更

PCRF Gx インターフェイスの相互作用	アクセス側の相互作用	リリース **21.1** より前の **ULI** および **MS TZ** の動作（標準 **Gx-R8/Custom15**（**AT&T**））	**ULI** および **MS TZ** の動作の変更（標準 **Gx-R8/Custom15**（**AT&T**））
課金ルールインストール要求で「0 - ULI」を含む RAI AVP を受信します。	**新しい ULI パラメータのみ**を含むベアラー作成応答を受信します。	**新しい ULI パラメータのみ**を含むベアラー作成応答を受信します。	動作の変更はありません。
課金ルールインストール要求で「0 - ULI」を含む RAI AVP を受信します。	**ULI パラメータを含まない**ベアラー作成応答を受信します。	古い ULI パラメータが、CCR-U メッセージで PCRF に送信されます。	3GPP-SGSN-MCC-MNC AVP に含まれる PLMN-id が PCRF に送信されます。
課金ルール変更要求で「0 - ULI」を含む RAI AVP を受信します。	**新しい ULI パラメータのみ**を含むベアラー更新応答を受信します。	新しい ULI パラメータが、CCR-U メッセージで PCRF に送信されます。	動作の変更はありません。
課金ルール変更要求で「0 - ULI」を含む RAI AVP を受信します。	**ULI パラメータを含まない**ベアラー更新応答を受信します。	古い ULI パラメータが、CCR-U メッセージで PCRF に送信されます。	3GPP-SGSN-MCC-MNC AVP に含まれる PLMN-id が PCRF に送信されます。
課金ルール変更要求で「0 - ULI」を含む RAI AVP を受信します。	**新しい ULI パラメータのみ**を含み、MS TZ パラメータを含まないベアラー削除応答を受信します。	新しい ULI パラメータと古い MS TZ パラメータが、CCR-U メッセージで PCRF に送信されます。	新しい ULI のみが、CCR-U メッセージで PCRF に送信されます。
課金ルール変更要求で「0 - ULI」を含む RAI AVP を受信します。	**ULI パラメータを含まず**、MS TZ パラメータも含まないベアラー削除応答を受信します。	古い ULI パラメータと古い MS TZ パラメータが、CCR-U メッセージで PCRF に送信されます。	3GPP-SGSN-MCC-MNC AVP に含まれる PLMN-id が PCRF に送信されます。
課金ルールインストール要求で「1 -MSTZ」を含む RAI AVP を受信します。	**新しい MS TZ パラメータのみ**を含むベアラー作成応答を受信します。	新しい MS TZ パラメータが、CCR-U メッセージで PCRF に送信されます。	動作の変更はありません。

PCRF Gx インターフェイスの相互作用	アクセス側の相互作用	リリース 21.1 より前の ULI および MS TZ の動作（標準 Gx-R8/Custom15（AT&T））	ULI および MS TZ の動作の変更（標準 Gx-R8/Custom15（AT&T））
課金ルールインストール要求で「1 -MSTZ」を含む RAI AVP を受信します。	**MS TZ パラメータを含まない**ベアラー作成応答を受信します。	古い MS TZ パラメータが、CCR-U メッセージで PCRF に送信されます。	動作の変更はありません。
課金ルール変更要求で「1-MSTZ」を含む RAI AVP を受信します。	**新しい MS TZ パラメータのみ**を含むベアラー更新応答を受信します。	新しい MS TZ パラメータが、CCR-U メッセージで PCRF に送信されます。	動作の変更はありません。
課金ルール変更要求で「1-MSTZ」を含む RAI AVP を受信します。	**MS TZ パラメータを含まない**ベアラー更新応答を受信します。	古い MS TZ パラメータが、CCR-U メッセージで PCRF に送信されます。	動作の変更はありません。
課金ルール変更要求で「1-MSTZ」を含む RAI AVP を受信します。	**新しい MS TZ パラメータのみ**を含むベアラー削除応答を受信します。	古い ULI パラメータと新しい MS TZ パラメータが、CCR-U メッセージで PCRF に送信されます。	新しい MS TZ のみが、CCR-U メッセージで PCRF に送信されます。
課金ルール変更要求で「1-MSTZ」を含む RAI AVP を受信します。	**MS TZ パラメータを含まない**ベアラー削除応答を受信します。	新しい ULI パラメータと古い MS TZ パラメータが、CCR-U メッセージで PCRF に送信されます。	古い MS TZ のみが PCRF に送信されます。
何も受信しません。	新しい ULI パラメータと新しい MS TZ パラメータを含むセッション削除要求を受信します。	新しい ULI パラメータと新しい MS TZ パラメータが、CCR-T メッセージで PCRF に送信されます。	動作の変更はありません。
何も受信しません。	新しい ULI パラメータを含み、MS TZ パラメータを含まないセッション削除要求を受信します。	新しい ULI パラメータと古い MS TZ パラメータが、CCR-T メッセージで PCRF に送信されます。	動作の変更はありません。

PCRF Gx インターフェイスの相互作用	アクセス側の相互作用	リリース 21.1 より前の ULI および MS TZ の動作（標準 Gx-R8/Custom15（AT&T））	ULI および MS TZ の動作の変更（標準 Gx-R8/Custom15（AT&T））
何も受信しません。	新しい ULI パラメータを含まず、MS TZ パラメータも含まないセッション削除要求を受信します。	古い ULI パラメータと古い MS TZ パラメータが、CCR-T メッセージで PCRF に送信されます。	動作の変更はありません。

重要 ULI と ULI タイムスタンプはペアになっていると見なされます。ULI タイムスタンプが転送される場合は、その ULI とともに転送および受信されます。ULI が受信され、ULI タイムスタンプが受信されない場合、その P-GW は、古いタイムスタンプを転送しません。

- Gx インターフェイスでは NETLOC-ACCESS-NOT-SUPPORTED に AVP を含めることができます。AVP をこのように含めることは、次の条件に基づきます。
  - RAT タイプが、E-UTRAN、UTRAN、WCDMA、GPRS、GERAN、W-LAN 以外である。
  - IP CAN タイプが、3GPP EPS、GPRS、非 3GPP EPS 以外である。
  - Required-Access-Info AVP を含む再承認要求が受信される。
  - シャーシで NetLoc 機能が有効になっている。
  - イベントトリガー ACCESS_NETWORK_INFO_REPORT (45) がインストールされている。

リリース 21.1 より前の動作（標準 Gx-R8/Custom15（AT&T））	新しい動作（標準 Gx-R8/Custom15（AT&T））
以前は、IP-CAN タイプまたは RAT タイプが NETLOC をサポートしていない場合、P-GW（PCEF）は、PCRF から受信した RAI を無視していました。	R8-Gx 標準および Custom15 Gx ディクショナリの再承認応答メッセージに新しい AVP である NetLoc-Access-Support が追加されました。

- 表 *6 : LastUserLocationInformation AVP* および *LastMSTimeZone AVP* に関する動作の変更

P-GW CDR の動作	21.1 リリース以降の、Custom 35/Custom 24/Custom 48 ディクショナリでの動作	Custom52 ディクショナリ（標準準拠の新しいディクショナリ）/Custom 35 ディクショナリ（顧客固有）

ベアラー削除コマンド/ベアラー削除要求/セッション削除要求で ULI を受信します。	ULI は P-GW CDR 生成の一部ではありませんでした。	ULI は、P-GW CDR 生成で **LastUserLocationInformation** AVP として記録されます（AVP は CLI コマンドを使用して制御されません）。
ベアラー削除コマンド/ベアラー削除要求/セッション削除要求で MS TZ を受信します。	MS TZ は P-GW CDR 生成の一部ではありませんでした。	MS TZ は、P-GW CDR 生成で **LastMSTimeZone** AVP として記録されます。 CDR は、通常リリースとしてリリースされます。この場合、MS TZ は完全なトリガーとして検出されず、MS TZ の変更を原因として追加の CDR がリリースされません。 AVP は CLI コマンドを使用して制御されません。

S-GW CDR の動作	**21.1 リリース以降の、Custom 35/Custom 24 ディクショナリでの動作**	**Custom24 ディクショナリ（標準ディクショナリ）/Custom 35 ディクショナリ（AT&T）**
ベアラー削除コマンド/ベアラー削除要求/セッション削除要求で ULI を受信します。	ULI は CDR 生成の一部ではありませんでした。	ULI は、S-GW CDR 生成で **LastUserLocationInformation** AVP として記録されます属性は CLI コマンドを使用して制御されます。
ベアラー削除コマンド/ベアラー削除要求/セッション削除要求で MS TZ を受信します。	MS TZ は CDR 生成の一部ではありませんでした。	MS TZ は、S-GW CDR 生成で **LastMSTimeZone** AVP として記録されます。属性は CLI コマンドを使用して制御されます。 CDR は、通常リリースとしてリリースされます。この場合、MS TZ は完全なトリガーとして検出されず、MS TZ の変更を原因として追加の CDR がリリースされません。

制限事項

1. この機能拡張は、S-GW、P-GW、および SAEGW にのみ適用されます。GGSN と SGSN では、NetLoc 機能の動作に変更はありません。

2. **Last-MS-Timezone** 属性と **Last ULI** 属性は、S-GW CDR 生成専用に custom24 および custom35 ディクショナリに追加されています。
3. CLI コマンド **gtpp attribute** に追加されたキーワード **last-ms-timezone** と **last-uli** は S-GW CDR の生成にのみ適用されます。
4. ディクショナリ custom35（お客様固有のディクショナリ）および custom52（3GPP R13 標準規格を遵守）に追加された **Last-MS-Timezone** 属性と **Last ULI** 属性は、P-GW CDR の生成にのみ適用されます。これらの属性は CLI で制御されません。

コマンドの変更

gtpp-attribute

この CLI コマンドは、オプション属性の指定を、GPRS/PDN/UMTS アクセスゲートウェイが生成するコール詳細レコード（CDR）に表示できるようにします。また、属性フィールド値をエンコードすることによって、情報が CDR にどのように表示されるかを定義します。CDR 生成中に属性を制御するために、キーワード **last-ms-timezone** と **last-uri** がこの CLI コマンドに追加されました。

重要 キーワードの追加は、S-GW CDR にのみ適用されます。P-GW CDR には適用されません。

```
configure
  context <context_name>
     gtpp group group_name
       gtpp attribute { last-ms-timezone | last-uli | .. }
       [no | default ] gtpp attribute { last-ms-timezone | last-uli
| .. }
  end
```

注：

- **no:** CDR から設定された GTPP 属性を削除します。
- **default:** 生成された CDR のデフォルトの GTPP 属性を設定します。また、生成された CDR の属性値のデフォルトの表示も設定します。
- **last-ms-timezone:** CDR フィールドに「Last MS-Timezone」を設定します。デフォルトのオプションが使用されている場合、このオプションは無効になります。
- **last-uli:** CDR フィールドに「Last ULI」を設定します。デフォルトのオプションが使用されている場合、このオプションは無効になります。

パフォーマンス指標の変更

show configuration

このコマンドは、以下の出力を表示するように変更されました。

- Last-MS-Timezone の有無

- 最後のユーザーロケーション情報の有無

show gtpp group name *group_name*

このコマンドは、以下の出力を表示するように変更されました。

```
    Last-MS-Timezone present: yes
    Last-User Location Information present:
yes
```

RAN-NAS 原因コードの機能強化

この章では、RAN-NAS 原因コードの機能強化について説明します。

機能説明

重要 これはライセンスで制御される機能です。NPLI の既存のライセンスを有効にする必要があります。ライセンスの入手方法の詳細については、シスコのアカウント担当者にお問い合わせください。

この機能により、Gx インターフェイス、P-GW、および S-GW CDR での「ベアラー作成失敗応答」、「ベアラー更新失敗応答」、および「ベアラー削除応答」に対する 3GPP RAN/NAS 原因コード IE のサポートが導入されています。これにより、通信事業者はアクセスネットワークから詳細な RAN/NAS リリース原因コード情報を取得できます。RAN/NAS 原因は、次のいずれかのメッセージでアクセス側から取得できます。

- ベアラー作成失敗応答
- ベアラー更新失敗応答
- セッション削除要求
- ベアラー削除応答
- ベアラー削除コマンド

顧客固有のディクショナリ Gx- dpca-custom15 および Gz-Custom35 の標準 IE に加え、S4、S11、S5、および S8 インターフェイス上の 3GPP リリース 12 RAN/NAS 原因 IE のこのサポートが、「セッション削除要求」および「ベアラー削除」コマンドのために存在し、プライベート拡張を介して提供されています。

ただし、「ERAB creation Failure」、「ERAB modification Failure」、および「ERAB release indication」メッセージで受信した RAN/NAS 原因は、S-GW と P-GW で処理されませんでした。したがって、P-GW によって PCRF に転送されず、P-GW および S-GW の CDR にも入力されませんでした。この機能強化により、S-GW（S4、S11 インターフェイス）および P-GW（S5、S8 インターフェイス）で、「ベアラー作成応答」、「ベアラー更新応答」、および「ベアラー削除応答」の RAN/NAS 原因コードを処理するためのサポートが追加されました。また、

RAN/NAS 原因コードは、P-GW によって PCRF に転送され、P-GW と S-GW の CDR に入力されます。

「ベアラー作成応答」、「ベアラー更新応答」、および「ベアラー削除応答」について、プライベート拡張に 3GPP リリース 12 RAN/NAS 原因 IE のサポートを追加する必要はありません。「セッション削除要求」と「ベアラー削除コマンド」内の 3GPP リリース 12 原因コード IE のプライベート拡張サポートは、引き続きサポートされます。

この機能強化により、dpca-custom15 ディクショナリの Gx インターフェイスと custom35 ディクショナリの Gz インターフェイスで、次の RAN/NAS 原因 IE の動作の変更が導入されます。

表 *7: RAN/NAS* 原因の *Gx* インターフェイス要件

Message	GTP 原因	RAN-NAS 原因情報を伝送する Gx メッセージ
ベアラー作成応答	Accepted	29.274 の表 7.2.4-2 に従い、RAN/NAS の原因は予期されません。そのため、受信しても無視され、PCRF に転送されません。
	Temporarily rejected due to HO in progress.	この GTP 原因による RAN/NAS 原因は、29.274 の表 C.4 に従って適用されません。そのため、受信しても無視され、PCRF に転送されません。
	Other GTP Causes	CCR-U
ベアラー更新応答	Accepted	29.274 の表 7.2.16-2 に従い、RAN/NAS 原因は予期されていません。そのため、受信しても無視され、PCRF に転送されません。
	No Resources	CCR-U
	Available	**重要** UE によって開始された（MBC）ベアラーの変更が GTP 原因「NO RESOURCES AVAILABLE」で失敗した場合、P-GW は PDN セッション全体を削除します。この場合、RAN-NAS 原因情報は CCR-T メッセージの一部として転送されます。
	Context Not Found	ベアラー更新応答をメッセージレベルの原因「CONTEXT NOT FOUND」とともに受信した場合、これは PDN の削除につながり、RAN-NAS 原因情報は CCR-T メッセージの一部として転送されます。
	Temporarily rejected due to HO in progress.	この GTP 原因による RAN/NAS 原因は、29.274 の表 C.4 に従って適用されません。そのため、この原因は受信しても無視され、PCRF に転送されません。
	Other GTP Causes	CCR-U

Message	GTP 原因	RAN-NAS 原因情報を伝送する Gx メッセージ
ベアラー削除応答	Temporarily rejected due to HO in progress	この GTP 原因による RAN/NAS 原因は、29.274 の表 C.4 に従って適用されません。そのため、この原因は受信しても無視され、PCRF に転送されません。 **重要** S-GW の既存の設計に従い、「ベアラー削除応答」を GTP 原因「Temporarily rejected due to handover/ TAU/ RAU procedure in progress」で受信した場合、GTP 原因が「Request Accepted」に変更され、P-GW に転送されます。この場合、RAN/NAS の原因を「ベアラー削除応答」で受信すると、S-GW はそれを P-GW に転送します。P-GW では、「ベアラー削除応答」を GTP 原因「Request Accepted」で受信しているため、RAN/NAS 原因が PCRF に転送され、P-GW の CDR に入力されます。この動作は、SAEGW および S-GW + P-GW の組み合わせのコールで見られます。
	Accepted / Other GTP CCR-UCauses	**重要** ネットワークで RAR/CCA-U を介して開始されたベアラー削除応答で RAN/NAS 原因を受信した場合、P-GW は、RAN/NAS 原因をレポートするために CCR-U を PCRF に送信しません。 このサポートは、29.212 リリース 13.5 の「RAN/NAS 機能の強化」により導入されました。

表 *8 : RAN/NAS* 原因の *Gz* インターフェイス要件

Message	S-GW CDR	P-GW CDR
セッション削除要求	対応	対応
ベアラー削除コマンド	対応	対応 注：RAN/NAS 原因をベアラー削除応答で受信した場合、これによりベアラー削除コマンドで受信した RAN/NAS 原因が上書きされます。
ベアラー作成失敗応答	非対応	非対応
ベアラー更新失敗応答	非対応	非対応
ベアラー削除応答	非対応	はい

制限事項

この機能には次の制限があります。

- S2a および S2b インターフェイスを介した RAN/NAS 原因のサポートは未サポートです。
- RAN/NAS 原因情報のサポートは、標準 Gx および Gz ディクショナリに追加されていません。
- P-GW は、GTP インターフェイスから受信した最初の 2 つの RAN/NAS 原因 IE（最大 1 つの RAN と最大 1 つの NAS）情報を処理します。たとえば、アクセスネットワークが不正な動作をし、2 つの NAS と 1 つの RAN の RAN/NAS 原因リストを送信した場合、最初の 2 つの原因のみが考慮され、検証されます。この場合、2 つの NAS 原因があり、許可される NAS は 1 つだけであるため、最初の NAS 原因だけが Gx インターフェイスと CDR で入力されます。
- 仕様 32.251 の表 5.2.3.4.1.1 および 表 5.2.3.4.2.1 に従い、失敗したベアラー作成応答と失敗したベアラー更新応答に対して S-GW CDR および P-GW CDR を生成するトリガーはありません。したがって、「ベアラー作成失敗」応答および「ベアラー更新失敗」応答で受信した RAN/NAS 原因は、Gz インターフェイスに送信されません。
- 「ベアラー削除」シナリオでは、「ベアラー削除」要求を受信した直後に S-GW CDR が生成されます。したがって、「ベアラー削除」応答で受信した RAN/NAS 原因は S-GW CDR に入力されません。
- ネットワークで RAR/CCA-U を介して開始された「ベアラー削除」応答で RAN/NAS 原因を受信した場合、P-GW は、RAN/NAS 原因をレポートするために CCR-U を PCRF に送信しません。このサポートは、仕様 29.212 リリース 13.5 の「RAN/NAS 機能の強化」により導入されました。
- RAN-NAS-Cause 機能がサポートされている場合、RAN/NAS 原因のみが PCRF に転送されます。ANI 情報は、NetLoc 機能が有効になっている場合にのみ転送されます。以下の表は、さまざまなシナリオを示しています。

シナリオ	RAN/NAS 原因の動作	ANI の動作
IP-CAN ベアラーの終了	RAN-NAS-Cause 機能がサポートされている場合（Netloc-ran-nas-cause CLI が設定されており、Supported-Features = RAN-NAS-CAUSE が Gx CCR-I/CCA-I でアサートされた場合）、PCEF はベアラー終了により受信した RAN 原因および/または NAS 原因を、Charging-Rule-Report AVP に含まれている RAN-NAS-Release-Cause AVP に含めます。	1 つ以上の失敗した課金ルールインストール要求が CCA-U/RAR で受信されたときに Required-Access-Info がアサートされた場合（Netloc CLI が設定され、Supported-Features = Netloc が Gx CCR-I/CCA-I でアサートされた場合）、ベアラーの終了中に受信した ANI 情報が CCR-U に入力されます。

シナリオ	RAN/NAS 原因の動作	ANI の動作
IP-CAN セッションの終了	RAN-NAS-Cause 機能がサポートされている場合（Netloc-ran-nas-cause CLI が設定されており、Supported-Features = RAN-NAS-CAUSE が Gx CCR-I/CCA-I でアサートされた場合）、PCEF はセッション終了により受信した RAN 原因および/または NAS 原因を、RAN-NAS-Release-Cause AVP にコマンドレベルで含めます。	1 つ以上の失敗した課金ルールインストール要求が CCA-U/RAR で受信されたときに Required-Access-Info がアサートされた場合（Netloc CLI が設定され、Supported-Features = Netloc が Gx CCR-I/CCA-I でアサートされた場合）、セッションの終了中に受信した ANI 情報が CCR-T に入力されます。
PCC ルールエラーの処理	RAN-NAS-Cause 機能がサポートされている場合（Netloc-ran-nas-cause CLI が設定されており、Supported-Features = RAN-NAS-CAUSE が Gx CCR-I/CCA-I でアサートされた場合）、PCEF はルールのインストール/アクティブ化/変更の失敗により受信した RAN 原因および/または NAS 原因を、Charging-Rule-Report AVP に含まれている RAN-NAS-Release-Cause AVP に含めます。	1 つ以上の失敗した課金ルールインストール要求が CCA-U/RAR で受信されたときに Required-Access-Info がアサートされた場合（Netloc CLI が設定され、Supported-Features = Netloc が Gx CCR-I/CCA-I でアサートされた場合）、ルールのインストール/アクティブ化/変更の失敗により受信した ANI 情報が CCR-U に入力されます。

コマンドの変更

diameter encode-supported-features netloc netloc-ran-nas-cause

この機能拡張では、この CLI コマンドの動作が変更されています。

以前の動作：RAN/NAS 原因機能を有効にするには、NetLoc 機能を有効にする必要がありました。この場合、CLI コマンド **diameter encode-supported-features netloc netloc-ran-nas-cause** で **netloc** キーワードを設定することが必須でした。

新しい動作：NetLoc 機能を設定しなくても、RAN/NAS 機能を有効にできるようになりました。これは、CLI コマンド **diameter encode-supported-features netloc netloc-ran-nas-cause** で **netloc** キーワードを設定する必要がないことを意味します。

```
configure > context context_name > ims-auth-service service_name > policy-control
 diameter encode-supported-features netloc netloc-ran-nas-cause
```

Diamproxy セッション ID 不一致の場合のセッションの切断

このセクションでは、Diamproxy グループ化情報とセッション ID の不一致の影響を受けるサブスクライバセッションをクリアする方法について説明します。

このセクションでは、この機能に関する次のトピックについて説明します。

機能説明

高速バックツーバック ICSR スイッチオーバーまたは広範囲にわたる複数のプロセス障害の間、Diameter プロキシセッションマネージャのマッピング情報は ICSR ペア間で保持されません。この Diameter プロキシセッション ID の不一致の結果、原因コード 5002（DIAMETER_UNKNOWN_SESSION_ID）で RAR が拒否されます。この動作は、VoLTE コールのセットアップ手順に影響します。そのため、Diameter プロキシセッションマネージャ マッピングの不一致が原因で影響を受けるサブスクライバセッションをクリアするためにこの機能が導入されました。動作を制御するために新しい CLI 設定が用意され、Diamproxy セッション ID の不一致を報告する新しいバルク統計カウンタがサポートされています。

バルク統計カウンタは、結果コードが 5002 の RAR メッセージが受信され、セッション ID Diampproxy マッピングの不一致が検出されて、セッションがクリアされた場合にのみ増分されます。CCR-T が PCRF に送信されるのを抑制し、原因コードとしての「Reactivation Requested」を使用してベアラー削除要求が S-GW に送信されます。そのため、サブスクライバは後続の VoLTE コールに影響を与えることなくすぐに再アタッチします。手動での介入は必要にならず、エラー 1 つのみが発生することになります。

重要 この機能拡張は IMS PDN にのみ適用されるため、この状況が発生した場合、手動での介入の必要がないエラーは 1 つに限定されます。これは Gx RAR にのみ適用されます。

Diamproxy セッション ID が一致しないセッションを削除するようシステムを設定する

続くセクションでは、Diamproxy グループ化情報とセッション ID の不一致が原因で影響を受けるサブスクライバセッションをシステムでクリアできるようにするための設定コマンドについて説明します。

一致しないサブスクライバセッションのクリア

セッション ID と Diamproxy の不一致が識別されたときに、シグナリングトリガーに基づいてサブスクライバセッションを切断するようにシステムを設定するには、次の設定コマンドを使用します。

```
configure
   context context_name
      ims-auth-service service_name
         policy-control
             diameter clear-session sessid-mismatch
end
```

- **sessid-mismatch**：セッション ID が一致しないセッションをクリアします。この CLI 設定はオプションです。
- デフォルトの設定は、**no diameter clear-session** です。デフォルトでは、セッションはクリアされません。

一致しないセッションを削除する設定の確認

次のコマンドを使用して、この機能の設定ステータスを確認します。

show ims-authorization service name *service_name*

service_name は、IMS 認証用に設定された IMS 承認サービスの名前にする必要があります。

このコマンドを実行すると、指定された IMS 承認サービス内で有効になっているすべての設定が表示されます。「セッション ID が一致しないセッションのクリア」フィールドを使用して、この機能を有効にするか無効にするかを決定できます。

```
[local]st40# show ims-authorization service name service1
  Context: test
  IMS Authorization Service name: service1
  Service State: Enabled
  Service Mode: Single Interface Policy and Charging
...
  Diameter Policy Control:
   Endpoint: gx
   Origin-Realm: xyz.com
   Dictionary: standard
   Supported Features:
      3gpp-r9
...
   Host Selection: Table: 1 Algorithm: Round-Robin
   Host Reselection Subscriber Limit: Not Enabled
   Host Reselection Interval: Not Enabled
   Sgsn Change Reporting: Not Enabled
     Session-Id Mismatch Clear Session: Enabled
   3GPP R9 Flow Direction Compliance: Not Enabled
  Host Selection Table[1]: 1 Row(s)
   Precedence: 1
...
```

不一致セッション削除機能のモニタリングと障害対応

この項では、この機能のサポートにおける show コマンドまたはその出力について説明します。

この機能に関連した障害については、次の操作を実行する必要があります。

- **show ims-authorization service name** <*service_name*> CLI コマンドを使用して、この機能が有効であるかどうかを確認します。有効になっていない場合は、**diameter clear-session sessid-mismatch** CLI コマンドを設定して、この機能が動作するかどうかを確認します。

- **show ims-authorization policy-control statistics debug-info** および **show diameter statistics proxy debug-info** CLI コマンドの出力を収集し、デバッグ統計を分析します。
- 影響を受けるセッションの削除中に報告されたシステムログを確認します。詳細な分析が必要な場合は、シスコのアカウント担当者にご連絡ください。

show ims-authorization service name

指定した IMS 承認サービス内でこの機能が有効になっているか無効になっているかを示すために、この show コマンドの出力に新しいフィールド「Session-Id Mismatch Clear Session」が追加されました。

IMSA スキーマ

次のバルク統計変数がこのスキーマに追加され、Diamproxy-Session ID の不一致が報告されるようになりました。

- dpca-rar-dp-mismatch：このカウンタは、セッション ID Diamproxy マッピングの不一致が原因で RAR の受信中にクリアされたセッションの合計数を表示します。

ミッションクリティカル QCI のネゴシエーションのサポート

このセクションでは、ミッションクリティカル QCI ネゴシエーション機能の概要と導入について説明します。

この項では、次のトピックについて取り上げます。

- 機能説明 （120 ページ）
- ミッションクリティカル QCI のネゴシエーションにおける DPCA の設定 （121 ページ）
- ミッションクリティカル QCI のモニタリングと障害対応 （122 ページ）

機能説明

ミッションクリティカル（MC）プッシュツートーク（PTT）サービスをサポートするために、一連の標準化された新しい QoS クラス識別子（QCI）（65、66、69、70）が導入されました。これらは、3GPP TS 23.203 v13.6.0 および 3GPP TS 23.401 v13.5.0 仕様で定義されている 65 ～ 66（GBR）および 69 ～ 70（非 GBR）のネットワーク開始型 QCI です。これらの QCI は、プレミアム モバイル ブロードバンド（PMB）/公安ソリューションに使用されます。

重要 MC-PTT QCI 機能を使用するには、ワイヤレス プライオリティ サービス（WPS）ライセンスを設定する必要があります。詳細については、シスコのアカウント担当者にお問い合わせください。

以前の動作：ゲートウェイは、標準 QCI（1 ～ 9）と通信事業者定義 QCI（128 ～ 254）のみを受け入れていました。PCRF が 10 ～ 127 の値を持つ QCI を送信する場合、ゲートウェイは要求を拒否します。MC QCI サポートは PCRF とネゴシエートされませんでした。

新しい動作：PCRF は、デフォルトベアラーの作成について新しい標準化された QCI の値である 69 と 70 を受け入れ、専用ベアラーの作成について 65、66、69、および 70 を受け入れます。

この機能を動作させるために、新しい設定可能な属性である **mission-critical-qcis**が、**diameter encode-supported-features** CLI コマンドに導入されました。この CLI オプションを有効にすると、ゲートウェイは、MC-QCI をサポートされる機能として設定することを許可し、その後、Supported-Features AVP を介して MC-PTT QCI 機能を PCRF とネゴシエートします。

WPS ライセンスが有効になっておらず、Diameter が MC-PTT QCI 機能（サポートされている機能のビットの一部）をネゴシエートするように設定されていない場合、ゲートウェイは、MC-PTT QCI を使用したセッション作成要求を拒否します。

この機能および関連する設定の詳細については、『*Release Change Reference*』ガイドの「*P-GW Enhancements for 21.0*」を参照してください。

ミッションクリティカル QCI のネゴシエーションにおける DPCA の設定

以下では、MC-PTT QCI 機能のサポートを有効にするための設定コマンドについて説明します。

ミッションクリティカル QCI 機能の有効化

MC-PTT QCI 機能を有効にするには、次の設定コマンドを使用します。

```
configure
   context context_name
      ims-auth-service service_name
         policy-control
            diameter encode-supported-features mission-critical-qcis
            end
```

注：

- **mission-critical-qcis**：このキーワードにより MC-PTT QCI 機能が有効になります。デフォルトでは、この機能は有効になりません。
- このキーワードは、WPS ライセンスが設定されている場合にのみ有効にできます。詳細については、シスコのアカウント担当者にお問い合わせください。
- この機能のネゴシエーションを無効にするには、既存の **no diameter encode-supported-features** コマンドを設定する必要があります。このコマンドを実行すると、サポートされている設定済み機能のいずれも PCRF とネゴシエーションされません。

ミッションクリティカル QCI 機能の設定の確認

show ims-authorization sessions full all コマンドにより、この機能の設定ステータスを示す表示が生成されます。

次の表示例は、ネゴシエートされたサポート対象機能の中で *mission-critical-qcis* なものを示す出力の一部のみを示しています。

```
show ims-authorization sessions full all

 CallId: 00004e29            Service Name:  ims-ggsn-auth
   IMSI: 123456789012341
   ....

 Negotiated Supported Features:
   3gpp-r8
   mission-critical-qcis
 Bound PCRF Server: 209.165.200.233
 Primary PCRF Server: 209.165.200.233
 Secondary PCRF Server: NA
 ....
```

ミッションクリティカル QCI のモニタリングと障害対応

以下では、ミッションクリティカルQCI機能をモニターするために使用できるコマンドについて説明します。

ミッションクリティカル QCI の show コマンドと出力

show ims-authorization sessions full all

上記のshowコマンドを実行すると、次のような統計が表示され、ミッションクリティカルQCI機能が有効かどうかが示されます。

```
show ims-authorization sessions full all

 CallId: 00004e29            Service Name:  ims-ggsn-auth
   IMSI: 123456789012341
   ....

 Negotiated Supported Features:
   3gpp-r8
   mission-critical-qcis
   ....
```

WLAN 向けの HSS および PCRF ベース P-CSCF 復元のサポート

ここでは、WLAN および EPC ネットワーク向けの HSS ベースおよび PCRF ベース P-CSCF 復元機能の概要と実装について説明します。

この項では、次のトピックについて取り上げます。

- 機能説明 （123 ページ）
- HSS/PCRF ベースの P-CSCF 復元の設定 （124 ページ）
- HSS および PCRF ベースの P-CSCF 復元のモニタリングと障害対応 （126 ページ）

機能説明

P-CSCF の復元手順が標準化され、P-CSCF 障害後のコール終了により UE と通信できなくなる時間が最小限に抑えられました。3GPP 標準規格リリース 13 に準拠して、この機能は、次の P-CSCF 復元メカニズムを含むように開発されています。

- 信頼できるまたは信頼できない WLAN アクセス（S2a/S2b）のための HSS ベース P-CSCF 復元
- LTE（S5/S8）および信頼できるまたは信頼できない WLAN アクセス（S2a/S2b）のための PCRF ベース P-CSCF 復元

重要 HSS ベースの P-CSCF 復元は、StarOS リリース 21.0 より前の LTE（S5 または S8）向けの P-GW でサポートされていました。

この機能は、基本と拡張の両方の P-CSCF 復元手順をサポートします。

重要 P-CSCF 復元は、ライセンスで制御される機能です。この機能を設定する前に、有効な機能ライセンスをインストールする必要があります。詳細については、シスコのアカウント担当者にお問い合わせください。

- **WLAN での HSS ベースの P-CSCF 復元**：

  P-CSCF 復元メカニズムがサポートされている場合、ゲートウェイは、S6b インターフェイスを介して送信される承認認証要求（AAR）メッセージ内の Feature-List AVP を介して AAA サーバーに復元サポートを示します。Feature-List AVP は、Supported-Features grouped AVP の一部です。Feature-List AVP のビット 0 は、WLAN での P-CSCF 復元サポートを示すために使用されます。

  P-CSCF 復元中に、3GPP AAA サーバーは、PGW が WLAN で HSS ベースの P-CSCF 復元をサポートしていることを確認した後、Re-authorization Request（RAR）コマンドで S6b を介して P-GW に P-CSCF 復元指示を送信します。 新しい Diameter AVP 「**RAR-Flags**」は、ビット 1 が設定された RAR メッセージ内にエンコードされ、AAA サーバーが WLAN で HSS ベースの P-CSCF 復元手順の実行を要求していることをゲートウェイに示します。

  AAA グループ設定の既存の CLI コマンド **diameter authentication** が拡張され、AAR メッセージ内の Supported-Features AVP の一部として P-CSCF 復元機能をエンコードするようになりました。

重要 Supported-Features は、RAT タイプ WLAN のすべての AAR メッセージで送信されます。すべての AAR で機能のネゴシエーションが必要です。再認証 AAR は、機能の再ネゴシエーションも行います。

- **PCRF ベースの P-CSCF 復元**：

  P-CSCF 復元メカニズムをサポートする PCEF は、Supported-Features AVP を介して CCR-I メッセージで復元サポートを示します。Supported-Feature-List AVP の 24 番目のビットは、このメカニズムがサポートされているかどうかを示します。

  ポリシー制御設定の既存の CLI コマンド **diameter encode-supported-features** が拡張され、PCRF による P-CSCF 復元機能サポートのネゴシエーションを許可するようになりました。P-CSCF 復元が要求されたことを PCEF に示すために、新しい Diameter AVP 「**PCSCF-Restoration-Indication**」が導入されました。これを行うには、AVP 値を 0 に設定します。

  Supported-Features AVP は、すべてのアクセスタイプ（eHRPD、P-GW、GGSN）の CCR-I でネゴシエートされます。ただし、復元トリガーを受信した場合、このトリガーは eHRPD および GGSN では無視されます。

制限事項

- 3GPP 標準仕様に従って、S6b 再承認要求が WLAN の P-CSCF 復元に使用される場合、拡張 P-CSCF 復元のために、ゲートウェイは、必須の AVP のみを含む承認要求を送信できます。ただし、現在の実装では、拡張 P-CSCF 復元に使用される再承認は、通常の再承認の一般的な承認要求です。これには、再承認 AAR のすべての AVP が含まれます。

この機能および関連する設定の詳細については、『*Release Change Reference*』ガイドの「*P-GW Enhancements for 21.0*」および「*SAEGW Enhancements for 21.0*」の項を参照してください。

HSS/PCRF ベースの P-CSCF 復元の設定

次の項では、HSS ベースおよび PCRF ベースの P-CSCF 復元機能のサポートを有効にするための設定コマンドについて説明します。

S6b AAA インターフェイスでの P-CSCF 復元通知の有効化

S6b インターフェイスを介して AAA サーバーに送信される AAR メッセージ内の Supported-Features AVP をエンコードするには、次の設定コマンドを使用します。

```
configure
   context context_name
      aaa group group_name
         diameter authentication encode-supported-features
pcscf-restoration-indication
         end
```

注：

- **encode-supported-features**：Supported-Features AVP をエンコードします。
- **pcscf-restoration-indication**：P-CSCF 復元の通知機能を有効にします。
- **default encode-supported-features**：AAR メッセージで Supported-Features AVP を送信しないデフォルト設定を指定します。

- **no encode-supported-features**：Supported-Features AVP を送信しないように、CLI コマンドを無効にします。
- **pcscf-restoration-indication** キーワードはライセンスによって異なります。詳細については、シスコのアカウント担当者にお問い合わせください。

Gx インターフェイスでの P-CSCF 復元通知の有効化

Gx インターフェイスで P-CSCF 復元通知機能を有効にするには、次の設定を使用します。

```
configure
   context context_name
      ims-auth-service service_name
         policy-control
            diameter encode-supported-features pcscf-restoration-ind
            end
```

注：

- **pcscf-restoration-ind**：P-CSCF 復元の通知機能を有効にします。このキーワードはライセンスによって異なります。詳細については、シスコのアカウント担当者にお問い合わせください。デフォルトでは、この機能は無効になっています。
- **default encode-supported-features**：デフォルト設定では、サポートされている機能が削除/リセットされます。
- **no encode-supported-features**：以前に設定されたサポート対象機能を削除します。

HSS/PCRF ベースの P-CSCF 復元の確認

show ims-authorization sessions full all

このコマンドにより、この機能のネゴシエーションステータスを示す表示が生成されます。

次の表示例は、ネゴシエートされたサポート対象機能の中で **pcscf-restoration-ind** を示す出力の一部のみを示しています。

```
show ims-authorization sessions full all

CallId: 00004e22            Service Name:  imsa-Gx
  IMSI: 123456789012341
  ....
Negotiated Supported Features:
  3gpp-r8
  pcscf-restoration-ind
....
```

show aaa group all

この機能が AAA グループで設定されている場合、この show コマンドは、サポート対象機能の一部として **pccf-restoration-ind** を表示します。

```
show aaa group all
 Group name:    default
 Context:   local
```

```
 Diameter config:
  Authentication:
....
Supported-Features:   pcscf-restoration-ind
....
```

HSS および PCRF ベースの P-CSCF 復元のモニタリングと障害対応

この項では、この機能のサポートにおける show コマンドまたはその出力について説明します。

次の操作を実行して、この機能に関連する障害をトラブルシュートできます。

- **show ims-authorization sessions full all** および **show aaa group all** CLI コマンドを使用して、機能が有効になっているかどうかを確認します。有効になっていない場合は、ポリシー制御と AAA グループ設定の両方で必要な CLI コマンドを設定し、動作するかどうかを確認します。
- **monitor protocol** コマンドを実行し、P-CSCF 復元機能のサポートが CCR-I および AAR メッセージでネゴシエートされているかどうかを確認します。ネゴシエートされていない場合は、この機能のそれぞれの CLI コマンドを有効にします。
- それでも問題が解決しない場合は、次の情報を入手して、シスコのアカウント担当者に詳細な分析を依頼してください。
  - オプション 74（EGTPC）および 75（App Specific Diameter -Gx/S6b）をオンにした状態でのプロトコルのモニターのログ
  - sessmgr、imsa、および diameter-auth が有効な状態でのログ
  - **show session disconnect reason** CLI コマンドの出力とサービスレベルの関連統計

show コマンドと出力

show ims-authorization sessions full all

この show コマンド出力の **Negotiated Supported Features** フィールドには、P-CSCF 復元機能が PCRF とネゴシエートされているかどうかが表示されます。

このサポートされている機能は、機能ライセンスが設定されている場合にのみ表示されます。

show aaa group all

この show コマンド出力の **Supported Features** フィールドには、P-CSCF 復元機能が Supported-Features AVP の一部として設定されているかどうかが表示されます。

このサポートされている機能は、機能ライセンスが設定されている場合にのみ表示されます。

show license information コマンドを実行します。

P-CSCF 復元機能を有効にするライセンスが設定されている場合、**show license information** コマンドにより、関連するライセンス情報が表示されます。

ログのモニタリング

ここでは、HSS および PCRF ベースの P-CSCF 復元機能に関連して生成されるログのモニター方法について説明します。

S6b Diameter プロトコルログ

Supported-Features フィールドは、AAR および AAA セクションで使用できます。生成されるログの出力は次のように表示されます。

```
<<<<OUTBOUND  15:37:23:561 Eventid:92870(5)
....
 [V] [M] Supported-Features:
   [M] Vendor-Id: 10415
   [V] Feature-List-ID: 1
   [V] Feature-List: 1
....
INBOUND>>>>>  15:37:23:562 Eventid:92871(5)
....
 [V] [M] Supported-Features:
   [M] Vendor-Id: 10415
   [V] Feature-List-ID: 1
   [V] Feature-List: 1
....
```

RAR-Flags フィールドは、RAR セクションで使用できます。生成されるログの出力は次のように表示されます。

```
INBOUND>>>>>  15:37:43:562 Eventid:92871(5)
....
[M] Re-Auth-Request-Type: AUTHORIZE_ONLY (0)
[V] RAR-Flags: 2
....
```

Gx Diameter プロトコルログ

Supported-Features で、CCR-I/CCA-I セクションの P-CSCF 復元の **Feature-List** が使用できます。生成される出力は次のように表示されます。

```
<<<<OUTBOUND  13:52:06:117 Eventid:92820(5)
....
 [V] [M] Supported-Features:
   [M] Vendor-Id: 10415
   [V] Feature-List-ID: 1
    [V] Feature-List: 16777217
....
INBOUND>>>>>  13:52:06:118 Eventid:92821(5)
....
 [V] [M] Supported-Features:
   [M] Vendor-Id: 10415
   [V] Feature-List-ID: 1
    [V] Feature-List: 16777216
....
```

PCSCF-Restoration-Indication AVP は RAR で使用できます。生成される出力は次のように表示されます。

```
INBOUND>>>>>  13:52:26:119 Eventid:92821(5)
....
[M] Re-Auth-Request-Type: AUTHORIZE_ONLY (0)
```

```
[V] PCSCF-Restoration-Indication: 0
....
```

ダイナミックルールのループ防止

機能情報

要約データ

[ステータス（Status）]	新しい機能
導入されたリリース	21.2
変更されたリリース	該当なし
対象製品	P-GW
該当プラットフォーム	ASR 5500
デフォルト設定	無効
関連する CDETS ID	CSCvc97345、CSCvd02249
このリリースでの関連する変更点	N/A
関連資料	P-GW Administration Guide Command Line Interface Reference

マニュアルの変更履歴

重要 リリース 21.2 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	リリース	リリース日
このリリースの新機能。	21.2	2017 年 4 月 27 日

機能説明

PCC（動的または事前定義）ルールのインストールに失敗すると、PCEF は、失敗したルールを報告するために、PCRF に対する CCR-U を開始します。PCRF が同じルール定義で応答すると、ルール障害 CCR-U が再度開始されます。この動作により、ルール障害のループが発生します。

この機能により、ゲートウェイは、ルールインストールの失敗を PCRF に 1 回だけ、正常にインストールされるまで報告することにより、ループを防止できます。

機能の仕組み

この機能は、CLI コマンドを使用して設定できます。サブスクライバの障害が報告されると、CLI コマンドを使用して、同じルールの障害は、正常にインストールされるまでそのサブスクライバに対して抑制されます。ルール名は、障害が報告されたサブスクライバ用に保持されます。ただし、ルールの障害の状態がエラーに修正された場合（たとえば、ルール定義が設定に追加され、ルールが正常にインストールされた場合）、ゲートウェイは、機能不全のルールのリストからルール名を削除します。そのため、特定のルールの障害が再発すると、PCRF に報告されます。

機能不全のルール名はチェックポイントの対象とならないため、セッションリカバリや ICSR などのリカバリイベントが発生した場合、これらのルールの障害は再度報告されます。

ダイナミックルールのループ防止の設定

ここでは、機能を有効にするのに必要な設定手順について説明します。

ループ防止の制御のための **ACS** ポリシーの有効化

ACS コンフィギュレーション モードで次のコマンドを使用して、PCRF と PCEF 間のルール障害ループを防止する機能を有効または無効にします。

```
configure
  active-charging service<service_name>
      policy-control report-rule-failure-once
      end
```

注：

- 設定すると、同じルールの失敗に対して CCR-U が 1 回だけ送信されます。
- デフォルトでは、この機能は無効です。
- 以前に設定済みの場合は、**no policy-control report-rule-failure-once** を使用して機能を無効にします。

モニタリングおよびトラブルシューティング

以下では、機能をモニターするために使用できるコマンドを説明します。

コマンドと出力の表示

ここでは、ダイナミックルールのループ防止機能のための show コマンドとそれらの出力について説明します。

show active-charging service all

上記のコマンドの出力が強化され、機能のステータス（有効または無効）が表示されるようになりました。次に例を示します。

```
show active-charging service all
```

```
.
.
.
Report Rule Failure Once: Enabled
```

show active-charging subscribers full all

上記のコマンドの出力が拡張され、報告されなかったルール失敗の合計数を示す新しいパラメータが表示されるようになりました。次に例を示します。

```
Callid:                          4e21        ACSMgr Card/Cpu:            15/0
Active Charging Service name:                                            acs
Active charging service scheme:
ACSMgr Instance:                  1          Number of Sub sessions:     1
Data Sessions Active:             0          Dynamic Routes created:     0
Uplink Bytes:                     0          Downlink Bytes:             0
Uplink Packets:                   0          Downlink Packets:           0
Accel Packets:                    0
FastPath Packets:                 0
Total NRSPCA Requests:            0          NRSPCA Req. Succeeded:      0
NRSPCA Req. Failed:               0
Total NRUPC Requests:             0          NRUPC Req. Succeeded:       0
NRUPC Req. Failed:                0
Pending NRSPCA Requests:          0          Pending NRUPC Requests:     0
Total Bound Dynamic Rules:        0          Total Bound Predef. Rules:  0
Data Sessions moved:              0
Bearers Terminated for no rules:                                         0
Failed Rulebase Install (unknown bearer-id):                             0
Failed Rule Install (unknown bearer-id):                                 0
Total number of rule failures not reported:                              1
```

show active-charging subsystem all

上記のコマンドの出力が拡張され、報告されなかったルール失敗の合計数を示す新しいパラメータが表示されるようになりました。次に例を示します。

```
Total ACS Managers:            2
Session Creation Succ:         1      Session Creation Fail:      0
.
.
.
Total Number of Unsolicited Downlink packets received : 0
Total Number of ICMP-HU packets sent :                   0

RADIUS Prepaid Statistics:
Total prepaid sess:            0      Current prepaid sess:       0
Total prepaid auth req:        0      Total prepaid auth success: 0
Total prepaid auth fail:       0      Total prepaid errors:       0
Total number of rule failures not reported :           4

Content Filtering URL Cache Statistics:
Total cached entries:          0
Total hits:                    0      Total misses:               0
.
.
.
```

RADIUS および Diameter Rf の中間アカウンティング インターバル タイマーの分離

機能情報

要約データ

[ステータス（Status）]	新しい機能
導入されたリリース	21.2
変更されたリリース	該当なし
対象製品	eHRPD、GGSN、P-GW
該当プラットフォーム	ASR 5500
デフォルト設定	無効
関連する CDETS ID	CSCvc97616
このリリースでの関連する変更点	N/A
関連資料	AAA Interface Administration and Reference Command Line Interface Reference

マニュアルの変更履歴

重要 リリース 21.2 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	リリース	リリース日
このリリースの新機能。	21.2	2017 年 4 月 27 日

機能説明

リリース 21.2 よりも前の Cisco StarOS プラットフォームには、アカウンティング中間レコードを RADIUS サーバーと Diameter Rf サーバーに送信する単一の設定パラメータがありました。そのため、使用可能な CLI オプションを使用して、さまざまな間隔でアカウンティング中間レコードを RADIUS サーバーと Diameter Rf サーバーに送信することができませんでした。この機能により、Diameter Rf および RADIUS アカウンティング アプリケーションにさまざまな中間間隔を設定するための CLI 制御メカニズムが提供されます。RADIUS サーバーおよび Diameter Rf サーバーに個別に設定可能な CLI および中間間隔タイマーの値を設定すると、使いやすさが向上します。

機能の仕組み

現在、Diameterアカウンティングは、RADIUSアカウンティングの暫定間隔に設定された値を使用します。CLI コマンドで設定可能なこの機能では、 Rf インターフェイスの Diameter アカウンティングの暫定間隔を個別に設定するためのオプションが提供されます。Diameter interim CLI が「**no**」オプションまたは特定のタイマー値を使用して設定されるまでは、RADIUS 暫定間隔値が互換性の尺度として Diameter 暫定間隔に使用されます。Diameter 設定が有効になると、RADIUS設定を変更しても Diameter設定に影響を与えることはなく、その逆も同様です。さまざまなシナリオで使用される Diameter の暫定間隔値を以下の表に示します。

RADIUS 設定	Diameter 設定	Diameter の暫定的な動作
設定なし または 暫定間隔：X または 暫定無効	暫定間隔：Y	暫定間隔：Y 注：X は Y と同じ場合と違う場合があります
設定なし または 暫定間隔：X または 暫定無効	「No」オプションを使用した暫定の無効化	暫定無効
設定なし または 暫定間隔：X または 暫定無効	設定なし	RADIUS 設定へのフォールバック

- リカバリ/ICSR の動作：PDN の作成時に使用された暫定的な間隔の設定は、PDN のライフタイム全体に適用されます。リカバリ/ICSRは、Diameterの暫定間隔に関する既存の PDN の動作に影響を与えません。
- ICSR アップグレード/ダウングレードの動作：
  - 既存のセッションは、古いシャーシに存在する RADIUS 設定に基づいて回復されます。
  - 新しいセッションの動作は、新たにアクティブになったシャーシで利用可能な設定に従います。

制限事項

この機能には次の既知の制限事項があります。

1. Diameter 中間インターバル CLI が設定されていない場合、P-GW は以前の動作を維持するため、Diameter アカウンティングでは RADIUS アカウンティングで設定されたものと同じ中間インターバル値が使用されます。
2. Diameter アカウンティングの設定が完了すると、以前の動作に戻すことはできません。

Diameter 中間アカウンティング インターバルの設定

RADIUS 中間アカウンティングインターバルとは別に Diameter 中間アカウンティングインターバルを設定するには、AAA サーバー グループ コンフィギュレーション モードで次のコマンドを使用します。

```
configure
    context context_name
      aaa group group_name
         diameter accounting interim interval interval_in_seconds
         end
```

注：

- *interval_in_seconds*：中間インターバルを指定します。50 ～ 40000000 の範囲にする必要があります。
- 以前に設定されている場合は、**no diameter accounting interim interval** を使用して Rf インターフェイスの中間アカウンティングメッセージを無効にします。
- デフォルトの Diameter 中間インターバル値はありません。
- Diameter 中間インターバル CLI が設定されていない場合、P-GW は以前の動作を維持するため、Diameter アカウンティングでは AAA サーバーグループの構成ブロックで使用可能な RADIUS 中間インターバルの設定が使用されます。

モニタリングおよびトラブルシューティング

以下では、機能をモニターするために使用できるコマンドについて説明します。

コマンドと出力の表示

この項では、この機能のサポートにおける show コマンドおよびコマンドの出力について説明します。

show aaa group { name <group_name> | all }

上記のコマンドの出力が変更されて、今後の Diameter Rf アカウンティングセッションに使用される暫定間隔の現在の設定を示す次の新しいフィールドが表示されます。

- Interim-timeout: <50-40000000> または <None>

次に、Diameter の暫定間隔が設定されていない場合の出力例を示します。

```
show aaa group name default
Group name:                    default
Context:                       pgw

Diameter config:
  Accounting:
    Request-timeout:           20
    Interim-timeout:           None
```

次に、Diameter の暫定間隔の値を 900 に設定した場合の出力例を示します。

```
show aaa group name default
Group name:                    default
Context:                       pgw

Diameter config:
  Accounting:
    Request-timeout:           20
    Interim-timeout:           900
```

show configuration [verbose]

上記のコマンドの出力が変更され、中間メッセージの間隔を秒単位で示す次の新しいフィールドが表示されるようになりました。

- diameter accounting interim interval <*value_in_seconds*>

次に、Diameter の中間間隔値を 60 に設定した場合の出力例を示します。

```
show configuration context isp verbose
config
    context isp
        aaa group default
            diameter accounting interim interval 60
```

Gy の OCS 障害レポートの強化

機能情報

要約データ

[ステータス（Status）]	変更された機能
導入されたリリース	21.1
変更されたリリース	21.2
対象製品	P-GW、SAEGW
該当プラットフォーム	ASR 5500
デフォルト設定	有効

関連する CDETS ID	CSCvc93904
このリリースでの関連する変更点	N/A
関連資料	AAA Interface Administration and Reference P-GW Administration Guide SAEGW Administration Guide

マニュアルの変更履歴

重要　リリース 21.2 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	リリース	リリース日
このリリースの新機能。	21.2	2017 年 4 月 27 日

機能説明

Cisco-Event-Trigger-Type AVP が CCA-I、CCA-U、または値が CREDIT_CONTROL_FAILURE（5）の RAR メッセージの PCRF によってインストールされる場合、シスコイベントグループ化 AVP が P-GW によって、OCS 障害コードの正確な値を含む CCR-U メッセージで PCRF に送信されます。このトリガーは、Gy で障害が発生した場合にのみ送信され、設定（クレジット制御障害の処理）に基づいて「続行」アクションが実行され、Gy セッションがオフライン状態に移行します。

この機能強化により、範囲ではなく正確な障害コードが PCRF に報告されます。たとえば、シスコ イベント トリガー タイプが CREDIT_CONTROL_FAILURE（5）で、CCA-U の OCS 障害コードが 3002 の場合、PCRF に送信される CCR-U では、シスコ CC 障害タイプ（グループ化された AVP シスコイベントの一部）が値 3002 で送信されます。

S5/S8 および S2b インターフェイスの RAN/NAS 原因コードに追加されたサポート

機能情報

要約データ

[ステータス（Status）]	変更された機能
導入されたリリース	21.1
変更されたリリース	21.2

対象製品	P-GW、S-GW、SAEGW
該当プラットフォーム	ASR 5500
デフォルト設定	無効
関連する CDETS ID	CSCuy93748/CSCvc97356
このリリースでの関連する変更点	N/A
関連資料	*P-GW Administration Guide* *S-GW Administration Guide* *SAEGW Administration Guide* *Command Line Interface Reference*

マニュアルの変更履歴

重要 リリース 21.2 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	リリース	リリース日
このリリースの新機能。	21.2	2017 年 4 月 27 日

変更された機能

重要 これはライセンスで制御される機能です。この機能用に別のライセンスがあります。NPLI の既存のライセンスを有効にする必要があります。または、シスコのアカウント担当者に、カスタムライセンスの取得方法をお問い合わせください。

IMS ドメインと VoWiFi の展開で課金を調整する場合、通信事業者は P-CSCF で入手可能な RAN または NAS（または両方）のリリース原因コード情報にアクセスする必要がある場合があります。P-GW は、アクセスネットワークから受信した ANI 情報とともに詳細な RAN/NAS 原因情報を提供し、さらに次のイベントに基づいて PCRF に提供します。

- ベアラーの非アクティブ化（ベアラー作成応答/ベアラー削除コマンド）
- セッションの非アクティブ化（セッション削除要求）
- ベアラーの作成/変更の失敗（原因が FAILURE の ベアラー作成/更新応答）

IMS ネットワークはアクセスネットワークから詳細な RAN または NAS（またはその両方）のリリース原因コード情報を取得できます。この情報は、コールパフォーマンス分析、ユーザー

QoE 分析、および適切な課金調整に使用されます。この機能は、S5、S8、Gx、および S2b インターフェイスでサポートされています。

この機能には、ベアラー作成応答、ベアラー更新応答、ベアラー削除応答、ベアラー削除コマンド、およびセッション削除要求での RAN/NAS 原因 IE のサポートが含まれています。次の表は、RAN/NAS 原因 IE でサポートされているプロトコルタイプを示しています。

表 *9 : RAN/NAS IE* のプロトコルタイプ

Interface	RAN/NAS IE でサポートされているプロトコルタイプ
S5/S8	S1AP Cause（1）/EMM Cause（2）/ESM Cause（3）
S2b	Diameter Cause（4）/IKEv2 Cause （5）

（注） 表にリストされているサポート対象プロトコルタイプの値以外の受信されたプロトコルタイプ値は、無視され、PCRF に転送されません。

RAN/NAS 原因の GTP インターフェイス要件

S5/S8 インターフェイスの場合、RAN/NAS 原因は、dpca-custom8 ディクショナリの次のメッセージでサポートされます。

- ベアラー作成失敗応答
- ベアラー更新失敗応答
- セッション削除要求
- ベアラー削除応答
- ベアラー削除コマンド

S2bインターフェイスでは、カスタムdpca-custom8ディクショナリの次のメッセージでRAN/NASの原因がサポートされています。

- ベアラー作成失敗応答
- ベアラー更新失敗応答
- セッション削除要求

RAN/NAS 原因の Gx インターフェイス要件

RAN/NAS 原因がカスタム dpca-custom8 ディクショナリに追加され、RAN/NAS の原因が確実に表示されるようになりました。RAN/NAS 原因を処理するための Gx インターフェイスの動作は次のとおりです。

表 *10 : RAN/NAS* 原因の *Gx* インターフェイス要件

Message	GTP 原因	RAN-NAS 原因情報を伝送する Gx メッセージ
ベアラー作成応答	Accepted	29.274 の表 7.2.4-2 に従い、RAN/NAS の原因は予期されません。したがって、受信しても無視され、PCRF に転送されません。
	Temporarily rejected due to HO in progress.	この GTP 原因による RAN/NAS 原因は、29.274 の表 C.4 に従って適用されません。したがって、受信しても無視され、PCRF に転送されません。
	Other GTP Causes	CCR-U
ベアラー更新応答	Accepted	29.274 の表 7.2.16-2 に従い、RAN/NAS 原因は予期されていません。したがって、受信しても無視され、PCRF に転送されません。
	No Resources Available	CCR-U （注） UE によって開始された（MBC）ベアラーの変更が GTP 原因「NO RESOURCES AVAILABLE」で失敗した場合、P-GW は PDN セッション全体を削除します。この場合、RAN-NAS 原因情報は CCR-T メッセージの一部として転送されます。
	Context Not Found	CCR-U （注） ベアラー更新応答をメッセージレベルの原因「CONTEXT NOT FOUND」とともに受信した場合、これは PDN の削除につながり、RAN-NAS 原因情報は CCR-T メッセージの一部として転送されます。
	Temporarily rejected due to HO in progress.	この GTP 原因による RAN/NAS 原因は、29.274 の表 C.4 に従って適用されません。したがって、受信しても無視され、PCRF に転送されません。
	Other GTP Causes	CCR-U

Message	GTP 原因	RAN-NAS 原因情報を伝送する Gx メッセージ
ベアラー削除応答	Temporarily rejected due to HO in progress	この GTP 原因による RAN/NAS 原因は、29.274 の表 C.4 に従って適用されません。したがって、受信しても無視され、PCRF に転送されません。 （注） • ベアラー削除コマンドの一部としてトリガーされるベアラー作成応答内で RAN/NAS 原因が受信され、原因が「Request Accepted」の場合、P-GW は（ベアラー作成応答で受信した）RAN/NAS 原因をPCRF に転送します。 • ベアラー削除コマンドで RAN/NAS 原因を受信し、ベアラー削除応答が「HO in progress」である場合、ベアラー削除コマンドで受信した RAN/NAS 原因は PCRF に転送されます。 • ベアラー削除コマンドで RAN/NAS 原因を受信し、ベアラー削除応答が「Accepted」または「Other Cause」である場合、新しい RAN/NAS 原因が PCRF に転送されます。
	Accepted / Other GTP CCR-UCauses	CCR-U （注） RAR/CCA-U を介して開始されたベアラー削除応答で RAN/NAS 原因を受信した場合、P-GW は、RAN/NAS 原因をレポートするために CCR-U を PCRF に送信しません。 このサポートは、29.212 リリース 13.5 の「RAN/NAS 機能の強化」により導入されました。
セッション削除要求	Accepted	CCR-T

PCRF に対する ANI の動作

3GPP 29.212 v13.4.0 のセクション 4.5.6、4.5.7、4.5.12 には、RAN-NAS-Cause 機能がサポートされている場合、PCEF は 3GPP-User-Location-Info AVP（利用可能な場合）、TWAN-Identifier（利用可能な場合で Trusted-WLAN 機能がサポートされている場合）、User-Location-Info-Time AVP（利用可能な場合）、および 3GPP-MS-TimeZone AVP（利用可能な場合）で、使用可能なアクセスネットワーク情報を提供する必要があると記載されています。

USER-LOCATION-INFO-TIME AVP が dpca-custom8 ディクショナリに追加され、ANI の一部として PCRF（使用可能な場合）に送信されます。また、RAN/NAS に対して新しい PROTOCOL-TYPE（1 ～ 5）がサポートされています。この AVP は、CCR-U と CCR-T（該当する場合）で確認できます。また、新しい PROTOCOL-TYPE（S1AP Cause、EMM Cause、ESM

Cause、IKEv2, DIAMETER）が Gx インターフェイスに表示されます（同じものが S5/S8/S2b インターフェイスを介して受信されている場合）。

S5/S8 インターフェイスの ANI の動作

P-GW は、RAN/NAS 原因とともに、dpca-custom8 ディクショナリの次の情報（存在する場合）も PCRF に送信します。

表 *11 : Gx* インターフェイスでの *GTP IE* から *ANI AVP* へのマッピング

GTP IE	Gx AVP
UE Time Zone	3GPP-MS-TimeZone
ULI Timestamp	User-Location-Info-Time
ユーザーロケーション情報	3GPP-User-Location-Info

RAN/NAS 機能が有効になっている場合、設定されたイベントトリガーに関係なく、ANI 情報が PCRF に送信されます。

S2b インターフェイスの ANI の動作

dpca-custom8 ディクショナリの場合、ANI 情報は PCRF に送信されません。また、dpca-custom8 ディクショナリの場合、TWAN-Identifier は ANI の一部としてはサポートされていません。

制限事項

この機能には次の制限があります。

- RAN/NAS 原因情報のサポートは、dpca-custom8 ディクショナリについてのみ追加されます。
- PGW は、GTP インターフェイスから受信した最初の 2 つの RAN/NAS 原因 IE（最大 1 つの RAN と最大 1 つの NAS）情報を処理します。たとえば、アクセスネットワークが不正な動作をし、2 つの NAS と 1 つの RAN の RAN/NAS 原因リストを送信した場合、最初の 2 つの原因のみが考慮され、検証されます。この場合、2 つの NAS 原因があり、最初の NAS 原因だけが Gx インターフェイスで入力されます。
- RAN/NAS 情報は Gx インターフェイスでのみ入力され、他のインターフェイスは影響を受けません。

コマンドの変更

diameter encode-supported-features netloc-ran-nas-cause

既存の CLI コマンドである **diameter encode-supported-features netloc-ran-nas-cause** を使用して、S5/S8 および S2b インターフェイスの各々で RAN/NAS 原因を有効にします。

この機能はデフォルトで無効に設定されています。

この機能を有効にするには、以下のコマンドを入力します。

```
configure
   context ISP1
      ims-auth-service IMSGx
        policy-control
        diameter encode-supported-features netloc-ran-nas-cause
        end
```

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。