ISG RADIUS インターフェイス

この章では、使用可能なプリミティブやその使用方法など、Intelligent Services Gateway（ISG）RADIUS インターフェイスの概要について説明します。

概要

ISG は、要求が ISG から送信され、照会されたサーバが応答するプル モデルで通常使用される標準の RADIUS インターフェイスを提供します。また、ISG は、通常プッシュ モデルで使用される RFC 5176 で規定された RADIUS Change of Authorization（CoA）拡張機能をサポートし、外部の認証、許可、アカウンティング（AAA）またはポリシー サーバからのサービスのダイナミック再設定ができるようにします。

明確に定義された一連のプリミティブが、ISG によって外部サーバと通信するために使用されます。プリミティブはサービス アクセス ポイント（SAP）間のインタラクションの抽象的な表現であり、サービス ゲートウェイとサービス プロバイダー（SP）のバック エンド システム間で渡される情報のタイプを示します。さまざまな SAP 間のインタラクションの順序の例については、「使用例のシナリオ」を参照してください。

RADIUS インターフェイスは、ISG ではデフォルトでイネーブルです。ただし、次の属性については、一部の基本的な設定が必要になります。

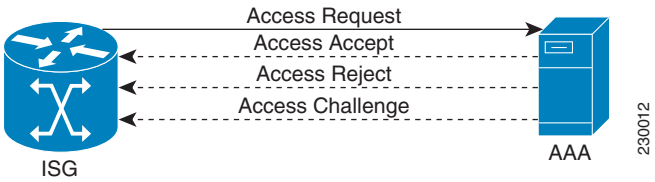
- セキュリティとパスワード：『*Intelligent Services Gateway Configuration Guide*, Cisco IOS Release 15.1S』の「Enabling ISG to Interact with External Policy Servers」の章を参照してください。
- アカウンティング：『*Intelligent Services Gateway Configuration Guide*, Cisco IOS Release 15.1S』の「Configuring ISG Accounting」の章を参照してください。
- プリペイド：『*Intelligent Services Gateway Configuration Guide*, Cisco IOS Release 15.1S』の「Configuring ISG Support for Prepaid Billing」の章を参照してください。

セッション認証または許可

セッション認証要求は、一般にサービス プロバイダーの AAA サーバに対するユーザ認証または許可のために生成されます。要求にはユーザ名やパスワードなどのセッションまたはユーザ クレデンシャルが含まれ、応答にはセッションに適用されるユーザ プロファイルのリスト機能とサービスを含む許可データが含まれます。

図 1 に、ISG デバイスからのセッション認証または許可要求（Access-Request）と予期される 3 つの可能な応答を示します。可能な応答のうち 1 つのみが返送されます。

図 1　　セッション認証プリミティブ



ここでは、使用可能な設定プリミティブについて説明します。次の項目で構成されます。

- 「セッション認証または許可」（P.1-2）
- 「セッション認証または許可の成功」（P.1-3）
- 「セッション認証または許可の失敗」（P.1-4）
- 「セッション認証チャレンジ」（P.1-4）

セッション認証または許可

RADIUS Access-Request メッセージは、セッション認証または許可に使用され、検証するクレデンシャルがメッセージで送信されることを意味します。この要求は、新しい PPP セッションが作成され、認証が必要な場合に自動的に送信されます。IP セッションの場合、この要求は、セッションが作成された後、セッション ポリシー内で ISG に「authenticate」アクション コマンドが設定されると送信されます。いずれの場合も、ユーザ名とパスワードは、エンド ユーザによって提供されます。セッション認証の例については、「使用例 1」を参照してください。

IP セッションの場合、Transparent Auto Logon（TAL）をセッション許可に使用できます。アクセス要求は、IP アドレスや MAC アドレスなどのいくつかの既知の識別子に基づいてセッション アイデンティティを検証する必要があり、明示的な認証が必要ではない場合に生成されます。この要求は、セッション ポリシー内で ISG に「authorize」アクション コマンドが設定されるとトリガーされます。この場合、ユーザ名属性はネットワーク ID（MAC、IP 回線 ID など）の伝送に使用され、パスワードはポリシー内で ISG によって指定されます。これにより、加入者が手動でユーザ名とパスワードを入力する必要がなくなります。セッション許可の例については、「使用例 2」を参照してください。

EAP タイプの認証では、アクセス要求は AP やワイヤレス コントローラなどのダウン ストリーム デバイスから発信され、ISG によってプロキシされる場合があります。

表 1 に、セッションの Access-Request 属性に一般的に関連付けられる標準 RADIUS 属性を示します。シスコはベンダー固有属性（VSA）を 2 タイプ使用します。属性と値のペア（AVPair）として定義されているものと、AVPair として定義されていないものです。表には、付録 A で定義されている Cisco Vendor-Specific AVPair 属性も含まれています。

表 1　Access-Request 属性

属性/VSA	タイプ	値
UserName	1	*<username>* または *<TAL Identifier>*
Password　または	2	*<user password>* または *<Password configured in TAL policy>*
CHAP-Password	3	*<chap challenge/response>*
NAS-IP-Address　または	4	*<ip-address>*
NAS-Identifier	32	*<identifier>* たとえば、ホスト名
NAS-Port	5	*<port>*
Service-Type	6	*<type>* 共通のパスワードを使用する場合は Outbound。 ユーザ パスワードを使用する場合は Framed。
Framed-Protocol	7	*<protocol>*
Framed-IP-Address	8	*<ip-address>*
Framed-IP-Netmask	9	*<netmask>*
Calling-Station-ID	31	*<Ethernet Address>*
Acct-Session-ID	44	*<unique ID>*
Event-Timestamp	55	*<time>*
CHAP-Challenge	60	*<challenge>*
NAS-Port-Type	61	*<Ethernet>*
NAS-Port-ID	87	*<value>*

表 2 に、Extensible Authentication Protocol（EAP）を採用するときの認証に含まれる追加属性を示します。

表 2　Access-Request 属性（EAP 配置用に追加）

属性/VSA	タイプ	値
EAP-Message	79	*<message>*
Message-Authenticator	80	*<signature>*

セッション認証または許可の成功

クレデンシャルの検証に成功すると、セッションに適用される許可情報を返す結果を提供するために、Access-Accept 応答が使用されます。この応答には、該当するサービス ID、サービス アクティブ化、機能、および属性を含むユーザ プロファイルが含まれています。セッション認証の Access-Accept の例については「使用例 1」を、セッション許可については「使用例 2」を参照してください。

Access-Accept

表 3 に、一般にセッション認証の Access-Accept に関連付けられる一部の標準 RADIUS 属性を示します。さらに、応答には、付録 A で定義されている Cisco Vendor-Specific 属性も含まれています。

表 3　セッション認証の Access-Accept 属性

属性/VSA	タイプ	値
Service Type	6	*<service type>*
Reply-Message	18	*<Message>*
Class	25	*<Class>*
Session Timeout	27	*<Absolute Timeout>*
Idle Timeout	28	*<Idle Timeout>*

セッション認証または許可の失敗

セッションのクレデンシャルを確認できない場合、Access-Reject 応答は失敗を意味し、失敗の理由を示す場合があります。

Access-Reject

表 4 に、セッション認証の Access-Reject 属性を示します。

表 4　Access-Accept の属性

属性/VSA	タイプ	値
Reply-Message	18	*<message>*

セッション認証チャレンジ

EAP 認証が有効な場合、バック エンド サーバは、チャレンジで応答できます。チャレンジ応答はマルチステージ EAP プロトコルに使用されます。ここで、EAP-Transport Layer Security（TLS）と同様の最初の暗号交換の後、簡単なトンネリングされた EAP プロトコルが完了まで実行されます。

Access-Challenge

表 5 に、セッションの Access-Challenge 属性を示します。

表 5　Access-Challenge の属性

属性/VSA	タイプ	値
Reply-Message	18	*<challenge prompt>*
EAP-Message	79	*<message>*
Message-Authenticator	80	*<signature>*

サービス認証およびサービス プロファイルのダウンロード

サービス プロファイルのダウンロードは、ISG で外部サーバからサービス定義を取得するために使用されます。このプロセスは、新規サービスがアクティブ化され、そのサービスが ISG にまだキャッシュされていない場合に発生します。例については、「使用例 1」を参照してください。

2 タイプのサービス認証シナリオがあります。サービス認証は、指定されたサーバでサービス プロファイルがダウンロードされ、（サービス プロファイル内で）追加認証が必要であることが確認されると実行される可能性があります。自動ログオン サービスでは、ユーザ名とパスワードがユーザ プロファイル内で指定され、サービスにログインするために使用されます。このシナリオが発生する過程およびタイミングの例については、「使用例 3」を参照してください。

2 つ目のタイプのサービス認証は、ユーザがポータルで新しいサービスを選択し、このサービスにアクセスするためにユーザ名とパスワードを入力する必要がある場合に起こる可能性があります。この場合、ユーザ名とパスワードは、このマニュアルで後述する「CoA Request:Service Activate」内で伝達されます。

図 2 に、ISG デバイスからのサービス認証またはサービス プロファイルのダウンロード（Access-Request）、および予期される 2 つの可能な応答を示します。可能な応答のうち 1 つのみが返送されます。

図 2　サービス認証またはサービス プロファイルのダウンロード

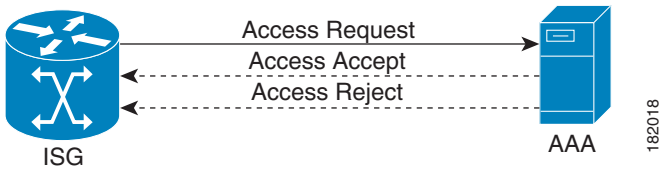


表 6 に、サービス認証とサービス プロファイルのダウンロードの Access-Request 属性、および付録 A で定義されている Cisco Vendor-Specific AVPair 属性を示します。

表 6　サービス認証またはサービス プロファイルのダウンロードの Access-Request 属性

属性/VSA	タイプ	値
UserName	1	サービス プロファイルのダウンロードの場合は *<service name>*、サービス認証の場合は *<username>*
Password	2	サービス プロファイルのダウンロードの場合は *<ISG configured>*、サービス認証の場合は *<user password>*
NAS-IP-Address	4	*<ip-address>*
NAS-Port	5	*<value>*
Service-Type	6	サービス プロファイルのダウンロードの場合は *<Outbound>*、サービス認証の場合は *<Framed>*
Calling-Station-ID	31	*<MAC address* or other >
NAS-Identifier	32	*<identifier>*
Acct-Session-ID	44	*<session-ID>*
Event-Timestamp	55	*<value>*

表 6　サービス認証またはサービス プロファイルのダウンロードの Access-Request 属性

属性/VSA	タイプ	値
NAS-Port-Type	61	<*Ethernet* or *ATM*>
NAS-Port-ID	87	<*value*>

サービス プロファイルのダウンロード成功

サービス プロファイルが取得できる場合は、サーバが Access Accept で応答します。サービス プロファイルには、トラフィック クラス、ポリシング レート、アカウンティング情報（Cisco Vendor-Specific AVPair 属性のいずれかと service-information タイプの Cisco Vendor-Specific Non-AVPair 属性のいずれか）などのサービス属性が含まれます。付録 A を参照してください。

サービス認証の成功

ユーザ サービスのクレデンシャルが確認されると、システム プロンプトは成功を示し、該当する追加属性が含まれる場合があります。

サービス認証またはサービス プロファイルのダウンロードの失敗

設定の認証要求が確認できない場合、システムは認証失敗メッセージで応答します。失敗の原因は、属性 18 を使用して符号化できます。

認可変更要求

認可変更（CoA）要求は、RFC 5176 に説明されているようにプッシュ モデルでサービス、セッション クエリー、機能プッシュ、アカウント ログオンおよびセッション終了のダイナミックなアクティブ化および非アクティブ化を可能にするために使用されます。このモデルは、1 つの要求と 2 つの可能な応答コードで構成されています。

- 認可変更要求（CoA 要求）
- CoA ACK（CoA-ACK）
- CoA NAK（CoA-NAK）

要求は CoA クライアント（通常は RADIUS またはポリシー サーバ）から発信されて、リスナーとして動作する ISG に送信されます。この項は、次の内容で構成されています。

- CoA 要求応答コード
- CoA ACK 応答コード
- CoA NAK 応答コード

RFC 5176 規定

RFC 5176 では、Cisco IOS ソフトウェアでサポートされているインターフェイスである ACK および NAK のパケット コードを使用して要求が直接応答されるメッセージの標準セットを含む、2 つの許可方法について説明しています。

- Diameter との互換性については、RFC 5176 は Authorize-Only service-type 属性値による CoA のプル メカニズムの使用を推奨しています。ただし、このメカニズムは Cisco IOS ソフトウェアによってサポートされていません。
- セキュリティのために、RFC 5176 では、Cisco IOS ソフトウェアでサポートされる IPsec の使用に言及しています。Event-Timestamp 属性による、IPsec を使用しないリプレイ防止はサポートされません。
- RFC 5176 で規定されている Disconnect Request メッセージは、パケット オブ ディスコネクト（POD）とも呼ばれ、PPP セッションの終了についてのみ ISG でサポートされます。リモート端末から ISG セッションを終了するには、この項で後述する CoA Request: Account Logoff プリミティブを使用します。
- RFC 5176 は State 属性の使用について説明しています。この属性はサポートされません。
- RFC 5176 は Proxy-State 属性の使用について説明しています。この属性はサポートされません。

（注）　CoA メッセージ内で暗号化された User Password 属性を送信する場合は、特別な配慮が必要です。詳細については、「Account Logon」（P.1-11）を参照してください。

前提条件

CoA インターフェイスを使用する場合は、セッションまたはサービス ターゲットがすでにデバイスに存在していると想定する必要があります。CoA は、セッションの機能（トラフィック ポリシー）の変更またはセッションに新しい機能を適用するために使用できます。アップデートは、アクティブ サービスではなくサブジェクトの親セッションだけに影響します。たとえば、アクティブ サービスまたはオンボックス サービス定義は変更できませんが、既存のサービスを非アクティブ化したり、新しいサービスをアクティブ化することはできます。

CoA 要求応答コード

ここでは、CoA 要求機能で使用されるプリミティブと属性について説明します。CoA 要求応答コードは、「機能プッシュ」として使用され、機能を親セッションに追加したり変更します。CoA 要求応答コードを使用して、ISG にコマンドを伝達することもできます。サポートされているコマンドを表 7 に示します。

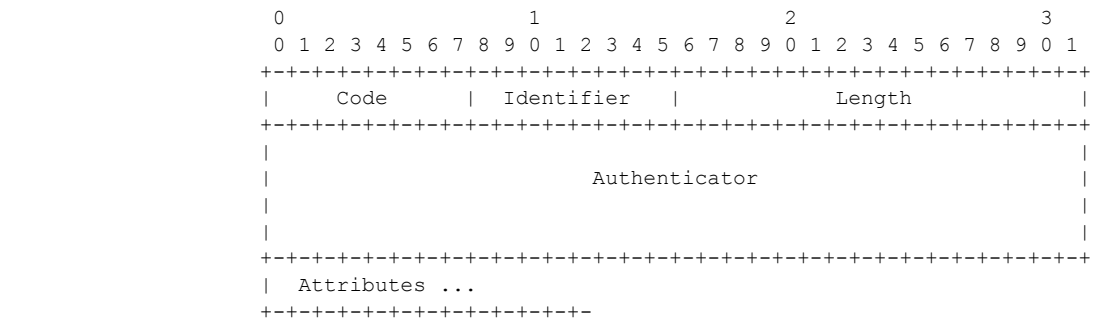
セッションを対象にするには、次のいずれかのセッション ID を使用できます。

- クライアントの IP アドレス（非 AVPair Account-Info 属性「S」として符号化）
- セッションの PBHK ID（非 AVPair Account-Info 属性「S」として符号化）
- RADIUS 属性 44 を使用するセッションの Account-Session-Id（CSCek31466 が必要）

サービスを対象とするには、次のサービス ID を使用する必要があります。

- Service-Name（非 AVPair Service-Info 属性「N」として符号化）

RFC 5176 で定義されている CoA 要求コードのパケットの形式は、コード、ID、長さ、オーセンティケータ、および Type Length Value（TLV; タイプ、長さ、値）形式の属性から構成されます。



属性フィールドは、Cisco VSA を送信するために使用します。「機能プッシュ」については、CoA コマンド コードが使用されていないため、VSA だけ CoA 要求に含まれます。

CoA コマンドについては、コマンド コードを伝送するために、サブ属性 252 が使用されます。コマンド コードはバイナリまたは ASCII で符号化できます。

表 7 は、ISG でサポートされる CoA コマンドの一覧です。

表 7　　ISG でサポートされる CoA コマンド

コマンド[1]	コード	値	バイナリ コマンド コード例	ASCII コマンド コード例
Account Logon[2]	1	*<username>*	vsa cisco 252 command-code = 01	vsa cisco generic 1 string "subscriber:command=account-logon"
Account Logoff	2	*<username>*	vsa cisco 252 command-code = 02	vsa cisco generic 1 string "subscriber:command=account-logoff" [3]
Session Query	4			[3]
（サービス情報の場合）		' '（スペース）	vsa cisco 252 command-code = 04 20	vsa cisco generic 1 string "subscriber:command=account-status-query"
（完全な ID の場合）		'&'（アンパサンド）	vsa cisco 252 command-code = 04 26	vsa cisco generic 1 string "subscriber:command=profile-status-query"
（両方の場合）		' &'（スペースとアンパサンド）	vsa cisco 252 command-code = 04 20 26	vsa cisco generic 1 string "subscriber:command=account-profile-status-query"
Session Query for Service Status	4	*<service name>*[4]	vsa cisco 252 command-code = 04 <service name>	vsa cisco generic 1 string "subscriber:command=service-status-query"
Service Activate	11	*<service name>*[4]	vsa cisco 252 command-code = 0B <service name>	vsa cisco generic 1 string "subscriber:command=activate-service"
Service Deactivate	12	*<service name>*[4]	vsa cisco 252 command-code = 0C <service name>	vsa cisco generic 1 string "subscriber:command=deactivate-service"

1. すべての CoA コマンドには、ISG と CoA クライアント間のセッション ID を含める必要があります。これは通常、クライアントの IP アドレス、または PBHK が使用されている場合はポート番号が続く ISG IP アドレスです。セッション ID は、個別の VSA として送信されます（例：vsa cisco 250 account-info = S10.10.10.11:85）。

2. ユーザ パスワードに必要な形式の詳細については、「Account Logon」（P.1-11）を参照してください。
3. ASCII 形式で送信される Account Logoff および Session Query では、ユーザ名属性は属性の値が空白の場合でも含める必要があります。
4. 16 進数のコマンド コードの形式を使用すると、サービス名はコマンド コードの直後に付けられますが、ASCII コマンド コード形式を使用すると、サービス名は個別の属性として送信されます。

```
vsa cisco generic 1 string "subscriber:service-name=service_name"
```

CoA ACK 応答コード

許可ステートの変更に成功した場合は、肯定確認応答（ACK）が送信されます。CoA ACK 内で返される属性は CoA 要求によって異なり、個々の CoA コマンドで検討されます。

CoA NAK 応答コード

否定確認応答（NAK）は許可ステートの変更に失敗したことを示し、エラーの理由を示す属性を含めることができます。複数のトラフィック ポリシーをプッシュすると、NAK は失敗した CoA を特定できません。現在、成功した CoA を確認できる唯一の方法は show コマンドの使用です。表 8 に CoA NAK の属性を示します。

表 8　　CoA-NAK の属性

属性/VSA	タイプ	値
UserName	1	*<username>*
ErrorCause <error cause>		*<error cause>*
Reply-Message 18 <message>	18	*<message>*

機能プッシュ

「機能プッシュ」は、親セッションのみを変更するために使用されますが、サービスの機能またはトラフィック ポリシーを変更するために使用することはできません。

「機能プッシュ」を使用すると、機能インスタンスを上書きし、まだ設定していない新機能を追加できます。ただし、新しく追加したトラフィック ポリシーは削除できません。したがって、サービス コンテナを使用する必要があります。サービスを非アクティブ化すると、トラフィック ポリシーの削除が可能になります。不完全なポリシー定義により、NAK メッセージが発生することがあります（アプリケーションは、その後セッションを終了できます）。

「機能プッシュ」にコマンド コードはありません。「機能プッシュ」には、追加または変更する機能に関連するセッション ID および Cisco VSA が含まれます。「機能プッシュ」の使用例については、「使用例 1」を参照してください。

CoA 要求を使用する ISG コマンド

次の項では、ISG セッションを使用するための特定の機能を提供する CoA 要求コマンドについて説明します。

- Service Activate

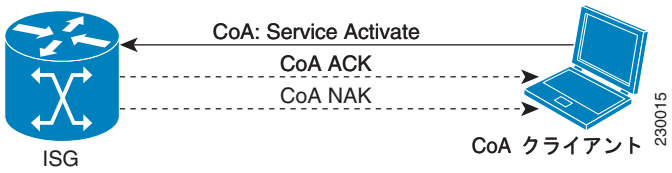
- Service Deactivate
- 複数のサービスのアクティブ化または非アクティブ化
- Account Logon
- Account Logoff
- Session Query
- Session Query for Service Status

Service Activate

Service Activate インターフェイスを使用して、指定したセッションのサービスをアクティブ化できます。パラメータには、セッション ID 属性およびアクティブ化するサービスの名前が含まれます。認証が必要なサービスの場合、これらの要求にサービスのユーザ名と許可パスワードも含めることができます。

図 3 に、CoA クライアントからの Service Activate 要求および ISG からの 2 つの可能な応答（1 つのみ返送されます）を示します。

図 3　CoA-Request、Service Activate



ISG がデバイスにまだキャッシュされていないサービスをアクティブ化するための要求を受信すると、ISG はサービスに適切なプロファイルをダウンロードします（「サービス プロファイルのダウンロード」を参照）。

サービスにさらに認証が必要な場合、ISG は、指定した RADIUS サーバに対してユーザを認証しようとします（「サービス認証」を参照）。

RADIUS サーバは、CoA 要求からのユーザ名とパスワードを使用してサービス プロファイルで指定されます（サービス プロファイル内の method-list 属性、subscriber:policy-directive = authenticate aaa-method-list service-list で参照されます）を認証します。

サービス エッジ デバイスは、サービスのアクティブ化に成功または成功したかどうかについて通知を送信します。サービスのアクティブ化が正常であり、サービスが認証を要求した場合、この応答には、そのサービスのサブスクライバごとの動作をさらに記述する追加属性も含めることができます。

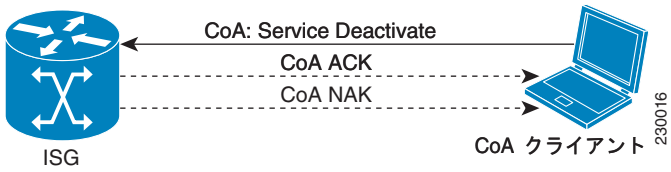
サービスのアクティブ化に成功しなかった場合、（障害モードを識別する）エラー コードも返されます。（RADIUS の場合、このエラー コードは、エラー メッセージ コード VSA - コマンド コードとして送信されます）。Service Activate の使用例については、「使用例 2」を参照してください。

Service Deactivate

Service Deactivate インターフェイスを使用して、セッションのサービスを非アクティブ化できます。サービス エッジ デバイスは、このメッセージの受信を確認する応答と非アクティブ化プロセスの結果を送信します。

表 5 に、CoA クライアントからの Service Deactivate 要求および ISG からの 2 つの可能な応答（1 つのみ返送されます）を示します。

図 4　CoA-Request、Service Deactivate



Service Deactivate メッセージの使用例については、「使用例 2」を参照してください。

複数のサービスのアクティブ化または非アクティブ化

Service Activate および Service Deactivate インターフェイスを使用して、単一の CoA-Request メッセージで複数のサービスをアクティブ化および非アクティブ化できます。CoA-Request メッセージには、複数の Service Activate および Service Deactivate 要求が含まれる場合があります。

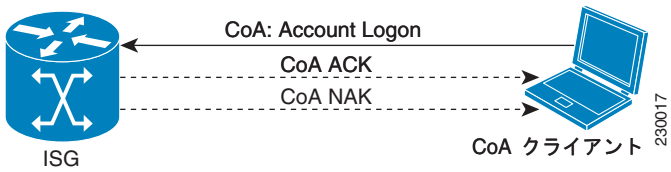
（注）　テキスト ベース コマンドは、単一 CoA メッセージでの複数の Service Activate および Service Deactivate ではサポートされません。単一 CoA メッセージでの複数の Service Activate および Service Deactivate ではバイナリ コマンドのみがサポートされます。

Account Logon

Account Logon 要求は、多くの場合、ISG の account-logon イベントをトリガーするためにポータルから送信されます。（account-logon イベントは、新しいセッションを認証する信号として ISG で一般的に使用されます）。Account Logon 要求には、ポータルで収集されたユーザ クレデンシャルが含まれます。Account Logon の使用例については、「使用例 1」を参照してください。

図 5 に、CoA クライアントから送信される Account Logon 要求、および ISG からの 2 つの可能な応答（そのうちの 1 つだけ返送されます）を示します。

図 5　CoA-Request: Account Logon

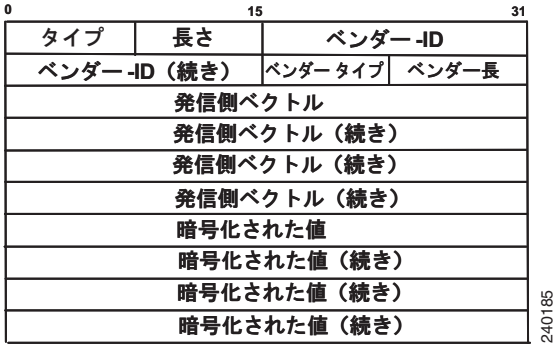


（RFC 5176 で規定されている）CoA メッセージでは、RADIUS アクセス メッセージの形式ではなく、RADIUS アカウンティング メッセージのメッセージ オーセンティケータ形式が使用されます。CoA Request Authenticator は、パケット全体の長さとデータのハッシュとして計算され、暗号化されたパスワードが必要です。一方、User-Password 属性は、プレーン テキスト パスワード、共有秘密、および Request Authenticator のハッシュとして計算され、Request Authenticator が必要です。標準 RADIUS 属性 2 を使用して CoA メッセージの暗号化パスワード属性を伝送すると、循環依存関係が確立されるため、伝送は不可能になります。

User-Password では、図 6 で示されている Cisco VSA 249 の形式を使用する必要があります。Cisco VSA 249 には、発信側ベクトルと暗号化パスワードがあります。発信側ベクトルは各属性に対して一意に生成される 16 オクテットの疑似乱数です。暗号化された値のフィールドは長さが前に付けられ、ゼロが 16 オクテットの偶数倍にパディングされたデータが含まれている 16 以上のオクテットです。

（注）　データ長を暗号化する US-ASCII および文字列からバイトへの符号化を使用しないでください。文字セット ISO8859-1 を使用する符号化を使用する必要があります。

図 6　　Cisco VSA 249 の形式



パスワードの例

次に、有効なアカウント ログオンを作成する例を示します。

ステップ 1　Data-Length および Password サブフィールドを連結して文字列フィールドのプレーン テキスト バージョンを構築します。

- 必要に応じて、長さ（オクテット単位）が 16 の偶数倍になるまで、文字列にゼロをパディングします。パスワードの長さを難読化するために、パディングにゼロ オクテット（0x00）を使用することを推奨します。
- 長さをパスワードの前に付け（ASCII ではなく raw）、16 の偶数倍ではなく 16 バイトの倍数になるまでパディングします。この例では、プレーン テキスト文字列は P で、パスワードは web です。

  P = 0x03 + web（16 進バイト：03 77 65 62 00 00 00 00 00 00 00 00 00 00 00 00）

ステップ 2　それぞれ最大 16 オクテットのブロックにクリア テキスト文字列 P を分割します（たとえば、p1、p2）。パディングを使用しない場合、最後のブロックに 16 未満のオクテットを含めることができます。

次の例では、共有秘密が S で、疑似乱数の 128 ビットの発信側ベクトルが I です。

S = cisco

I = IIIIIIIIIIIIIIII（16 進バイト：49 49 49 49 49 49 49 49 49 49 49 49 49 49 49 49）

暗号テキスト ブロックは、c(1)、c(2) のようになります。中間値は b1、b2 のようになります。

b1 = MD5 (cisco + IIIIIIIIIIIIIIII) = b4 04 ba b5 24 cb 6d f6 60 5e 21 ae e9 37 9d 26

b1 = MD5 (S + I)　　c(1) = p1 XOR b1

b2 = MD5 (S + c(1))　　c(2) = p2 XOR b2

bi = MD5 (S + c(i-1))　　c(i) = pi XOR bi

ステップ 3　暗号化された値には、c(1)+c(2)+...+c(i) が含まれます。+ は連結を表します。

c(1) = p1 XOR b1

p1　　03 77 65 62 00 00 00 00 00 00 00 00 00 00 00 00

XOR

b1　　b4 04 ba b5 24 cb 6d f6 60 5e 21 ae e9 37 9d 26

----

c(1) =　　b7 73 df d7 24 cb 6d f6 60 5e 21 ae e9 37 9d 26

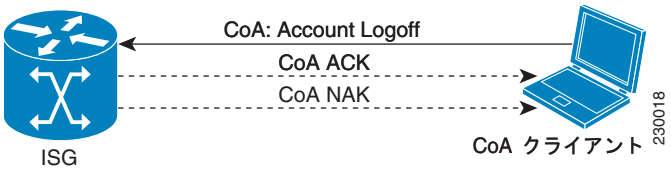
VSA 249 value = 49 49 49 49 49 49 49 49 49 49 49 49 49 49 49 49 b7 73 df d7 24 cb 6d f6 60 5e 21 ae e9 37 9d 26

Account Logoff

Account Logoff は、リモート サーバからサービス ゲートウェイのセッションを削除するのに使用します。これは、ユーザがポータルからの接続を解除したり、たとえば、プリペイドを ISG の外部に実装する場合に、管理上の理由で行うことができます。Account Logoff の使用例については、「使用例 1」を参照してください。

図 7 に、CoA クライアントからの Account Logoff 要求および ISG からの 2 つの可能な応答（1 つのみ返送されます）を示します。

図 7　CoA-Request、Account Logoff



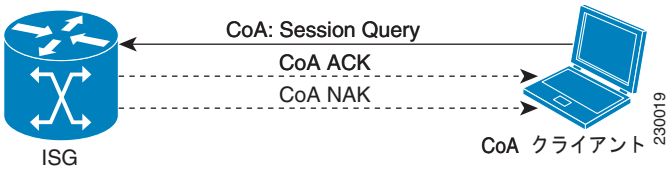
Session Query

セッション情報を要求するには、Session Query CoA コマンドを使用します。Session Query を符号化するには 3 種類の方法があります。

- コマンド コードの後に「 」（スペース）を付加すると、ISG に特定のセッションのサービス情報を返すように指示します。
- コマンド コードの後に「&」（アンパサンド）を付加すると、ISG にセッションの「完全な ID」と呼ばれるセッション情報を返すように指示します。
- 「 &」（スペースに続けてアンパサンド）を付加すると、2 つが結合されます。ISG は、完全な ID およびサービス情報の両方を返すように指示されます。

図 8 に、CoA クライアントからの CoA-Request、Session Query を示します。

図 8　CoA-Request、Session Query



Query VSA が 1 つのスペース文字で符号化される場合、Session Query へのシステム応答では、各アクティブ ユーザ サービスに関する詳細を返します。現在の返されたパラメータには、アクティブ サービスの期間、およびサービス ネットワークとの間を移動するデータのパケットとバイト数が含まれます。サービスがトンネル ベースではない場合、使用中の VRF が返される可能性があります。VRF の不在は、プライマリ サービスのステータスが返されるときにトンネル ベースのサービスが使用中であることを示します。

各アクティブ サービスのステータスは、Service Name VSA 内に埋め込まれて返され、形式は表 9 に示されているとおりです。

表 9　Service Name VSA 形式

属性/VSA	タイプ	値
Service Name VSA	9, 250 Account-Info	N;1;<*service name*>;<elapsed time (secs)>; <*username*>;<*downstream pkts*>; <*upstream pkts*>;<*downstream* i>; <*upstream bytes*>;<*VRF ID*>

Query VSA がアンパサンド文字で符号化される場合、セッション プロファイルおよびセッションの完全な ID に関連する情報がクライアントに返されます。完全な ID のフィールドがセッションを識別するために使用されます。完全な ID のフィールドには、有効なフィールド（IP address、MAC address、PBHK-id、VPI/VCI、circuit-id、remote-id、MSISDN、subinterface など）が含まれます。

RADIUS の完全な ID フィールドでは、ユーザ名と IP アドレスにそれぞれ標準属性（1 と 8）を使用します。追加の ID フィールドは、Account-Info VSA サブ属性として送信されます。これらのサブ属性は、「$」の後に ID タイプを表す他の文字（たとえば、MA は MAC アドレスを示し、SI はサブインターフェイスを示し、VP は VPI/VCI を示します）が続く完全な ID 値を持ちます。RADIUS の完全な ID フィールド属性を表 10 に示します。

表 10　RADIUS の完全な ID フィールド属性

属性/VSA	タイプ	値
Complete ID VSA（MAC）	9, 250 Account-Info	$MA<*MAC address*>
Complete ID VSA（サブ インターフェイス）	9, 250 Account-Info	$SI<*sub interface*>
Complete ID VSA（VPI/VCI）	9, 250 Account-Info	$VP<*VPI*/*VCI*>

Query VSA がスペースとアンパサンド文字の両方で符号化される場合、上記のすべての情報が返されます。Query VSA の使用例については、「使用例 1」を参照してください。

成功 RADIUS 応答は CoA-ACK として送信され、セッションが認証された場合は値「1」が付加された Query VSA 属性を、他のセッション（まだ認証されていないセッション、許可されたセッションなど）の場合は値「0」が付加された Query VSA 属性を返します。通常、ユーザ プロファイルにある追加属性が付けられます。

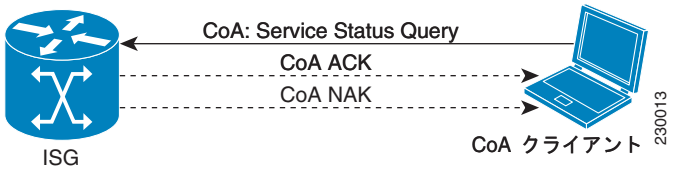
セッション ID が有効なセッションを参照していない場合、ISG はエラー メッセージを返します。RADIUS では、この障害は CoA-NAK で返され、返された Query VSA には「0」の値が付加されます。

Session Query for Service Status

Session Query for Service Status インターフェイスを使用して、特定のセッションにおけるサービスの現在の状態を判別できます。返される情報には、サービスのアクティブな期間が含まれます。

図 9 に、CoA クライアントからのサービス ステータスの要求を示します。

図 9　CoA-Request、Service Status Query



CoA-Request、Service Status Query

ISG デバイスは、CoA ACK または CoA NAK で CoA-Request; Session Query for Service Status に応答します。

セッションおよびサービスがアクティブである場合、ISG デバイスは、CoA-ACK メッセージ内で値が「1」の Query VSA を返し、サービス ステータスがサービス名の後に付けられます（Service Name VSA 内）。「1」はサービスがアクティブであることを示し、その後にサービスが起動している時間が続きます。

この属性の形式を表 11 に示します。

表 11　CoA-Request、Service Status Query の形式

属性/VSA	タイプ	値
Query VSA	9, 250 Command-Code	4"1"
Subscriber IP VSA	9, 250 Account-Info	S<IP[:port]>
Service Name VSA	9, 250 Account-Info	N"1"<*servicename*>;<*elapsed time* (*secs*)>;username

CoA Service Status Query の使用例については、「使用例 1」を参照してください。

セッションがアクティブでサービスがアクティブでない場合、ISG は CoA-ACK メッセージ内で値が「1」の Query VSA を返し、サービスがサービス名の後に付けられます（Service Name VSA 内）。「0」は、表 12 に示すように、サービスが非アクティブであることを示します。

表 12　ISG がセッションを認識、サービスが非アクティブ

属性/VSA	タイプ	値
Query VSA	9, 252 Command-Code	4"1"
Subscriber IP VSA	9, 250 Account-Info	S<IP[:port]>
Service Name VSA	9, 250 Account-Info	N"0"<*servicename*>

要求が成功せず、ISG がセッションを認識しない場合、ISG は表 13 に示されているように、CoA-NAK メッセージで値「0」が付加された Query VSA 属性を返します。

表 13　CoA-Request、Service Status Query が失敗

属性/VSA	タイプ	値
Query VSA	9, 250 Command-Code	4"0"
Subscriber IP VSA	9, 250 Account-Info	S<IP[:port]>

アカウンティング

セッションおよびサービスのアクティブ化状態は、セッションの開始時と停止時に送信されるアカウンティング要求属性、または中間アカウンティングによって報告されます。標準の **aaa accounting update** {*newinfo* | *periodic number*} コマンド設定を使用するか、IETF 標準属性 Acct-Interim-Interval、または Cisco AVPair acct-interval を使用して、これらの要求の頻度を制御できます。

前提条件

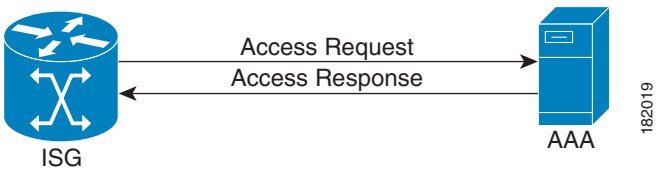
これらのインターフェイスでは、セッションまたはサービスが稼働し、認証がすでに行われ、ポリシーがアカウンティングに使用する method-list を制御することを前提にしています。

この項は、次の内容で構成されています。

- セッション アカウンティング
- サービス アカウンティング

図 10 に、AAA サーバに対するアカウンティング要求を示します。

図 10　アカウンティング要求/応答



セッション アカウンティング

セッション アカウンティングは、セッションの状態に関する情報を報告するために使用されます。

3 種類の Acct-Status-Type がセッション情報を収集するために使用されます。

- セッション アカウンティング Start
- セッション アカウンティング Stop
- セッション アカウンティング Interim
- セッション アカウンティング応答

アカウンティング要求が成功した場合、AAA サーバは指定アカウンティング要求の肯定確認応答で応答します（「セッション アカウンティング応答」を参照）。

セッション アカウンティング Start

Start 要求はセッションが開始され、データ トラフィックの準備ができていることを示します。セッション アカウンティング Start の使用方法については、「使用例 1」を参照してください。表 14 に、Acct-Status-Start 属性を示します。

表 14　Acct-Status-Start 属性

属性/VSA	タイプ	値
UserName	1	*<username>*
NAS-IP-Address	4	*<nasip>*
NAS-Port	5	*<port>*
Service-Type	6	Framed
Framed-Protocol	7	PPP
Framed-IP-Address	8	*<ip-address>*
Cisco VSA for session-id	9,250	S*<IP_addr>*:*<portbundle>*
NAS-Identifier	32	*<value>*
Acct-Status-Type	40	Start
Acct-Delay-Time	41	*<value>*
Acct-Session-Id	44	*<session-Id>*
NAS-Port-Type	61	*<type>*
NAS-Port-ID	87	*<id>*

セッション アカウンティング Stop

Stop 要求は、セッションが終了し、追加データ トラフィックが許可されないことを示します。アカウンティング Stop の使用方法については、「使用例 1」を参照してください。

表 15 に、Acct-Status-Stop 属性を示します。

表 15　Acct-Status-Stop 属性

属性/VSA	タイプ	値
UserName	1	<*username*>
NAS-IP-Address	4	<*nasip*>
NAS-Port	5	<*port*>
Service-Type	6	Framed
Framed-Protocol	7	PPP
Framed-IP-Address	8	<*ip-address*>
Cisco-AVPair	9, 1	disc-cause-ext=<*value*>
Cisco VSA for session-id	9,250	S<*IP_addr*>:<*portbundle*>
Control-Info	9, 253	I<*value*>
Control-Info	9, 253	O<*value*>
NAS-Identifier	32	<*value*>
Acct-Status-Type	40	Stop
Acct-Delay-Time	41	<*value*>
Acct-Input-Octets	42	<*value*>
Acct-Output-Octets	43	<*value*>
Acct-Session-Id	44	<*session-Id*>
Acct-Session-time	46	<*value*> (secs)
Acct-Input-Packets	47	<*value*>
Acct-Output-Packets	48	<*value*>
Acct-Terminate-Cause	49	<*value*>
NAS-Port-Type	61	<*type*>
NAS-Port-ID	87	<*id*>

セッション アカウンティング Interim

Interim 要求は、セッション開始以降の累積カウンタ、および IP アドレスの変更などの新しい情報を送信するために使用されます。

セッション アカウンティング応答

セッション アカウンティング要求が成功した場合、AAA サーバは指定アカウンティング要求の肯定確認応答で ISG デバイスに応答します。

サービス アカウンティング

サービス アカウンティングは、サービスの状態に関する情報を報告するために使用されます。

3 種類の Acct-Status-Type がサービス情報を収集するために使用されます。

- サービス アカウンティング Start
- サービス アカウンティング Stop

- サービス アカウンティング Interim
- サービス アカウンティング応答
- プリペイド アカウンティング
- プリペイド アカウンティング応答
- クラス ベースのアカウンティング

アカウンティング要求が成功した場合、AAA サーバは指定アカウンティング要求の肯定確認応答で応答します（「サービス アカウンティング応答」を参照）。

サービス アカウンティング Start

Start 要求は、サービスが設定されており、データ トラフィックを渡す準備ができていることを示します。サービス アカウンティング Start の使用方法については、「使用例 1」を参照してください。

表 16 に、Acct-Status-Start 属性を示します。

表 16　Acct-Status-Start の属性

属性/VSA	タイプ	値
username	1	*<username>*
NAS-IP-Address	4	*<nasip>*
NAS-Port	5	*<port>*
Service-Type	6	Framed
Framed-Protocol	7	PPP
Framed-IP-Address	8	*<ip-address>*
Cisco VSA for session-id	9,250	S*<IP_addr>*:*<portbundle>*
Service-Info	9, 251	N*<service-name>*
Parent-Session-ID	26, 9, 1	parent-session-id=*<id>*
Acct-Status-Type	40	Start
Acct-Delay-Time	41	*<value>*
Acct-Session-Id	44	*<session-Id>*
NAS-Port-Type	61	*<type>*
NAS-Port-ID	87	*<id>*

サービス アカウンティング Stop

Stop 要求は、サービスが終了し、追加データ トラフィックが許可されないことを示します。サービス アカウンティング Start の使用方法については、「使用例 1」を参照してください。

表 17 に、Acct-Status-Stop 属性を示します。

表 17　Acct-Status-Stop の属性

属性/VSA	タイプ	値
Username	1	*<username>*
NAS-IP-Address	4	*<nasip>*
NAS-Port	5	*<port>*

表 17　Acct-Status-Stop の属性

属性/VSA	タイプ	値
Service-Type	6	Framed
Framed-Protocol	7	PPP
Framed-IP-Address	8	<*ip-address*>
Service-Info	9, 251	N<*service-name*>
Cisco-AVPair	9, 1	disc-cause-ext=<*value*>
Cisco VSA for session-id	9,250	S<*IP_addr*>:<*portbundle*>
Control-Info	9, 253	I<*value*>
Control-Info	9, 253	O<*value*>
Parent-Session-ID	26, 9, 1	parent-session-id=<*id*>
NAS-Identifier	32	<*value*>
Acct-Status-Type	40	Start
Acct-Delay-Time	41	<*value*>
Acct-Input-Octets	42	<*value*>
Acct-Output-Octets	43	<*value*>
Acct-Session-Id	44	<*session-Id*>
Acct-Session-time	46	<*value*> (secs)
Acct-Input-Packets	47	<*value*>
Acct-Output-Packets	48	<*value*>
Acct-Terminate-Cause	49	<*value*>
NAS-Port-Type	61	<*type*>
NAS-Port-ID	87	<*id*>

サービス アカウンティング Interim

Interim 要求は、セッション開始以降の累積カウンタ、およびサービスに関連する新しい情報を送信するために使用されます。

サービス アカウンティング応答

サービス アカウンティング要求が成功した場合、AAA サーバは指定アカウンティング要求の肯定確認応答で ISG デバイスに応答します。

プリペイド アカウンティング

プリペイド アカウンティング メッセージは、クォータの使用状況を示します。表 18 に、プリペイド アカウンティング要求の属性を示します。

表 18　プリペイド アカウンティング要求の属性

属性/VSA	タイプ	値
UserName	1	<*username*>

プリペイド アカウンティング応答

プリペイド アカウンティング応答は、要求の受信を示す AAA サーバからの確認応答です。表 19 に、プリペイド アカウンティング応答の属性を示します。

表 19　プリペイド アカウンティング応答の属性

属性/VSA	タイプ	値
None		

クラス ベースのアカウンティング

クラス ベースのアカウンティング メッセージには、モジュラ QoS CLI（MQC）クラスマップに一致するトラフィックに関連する情報が含まれます。

クォータ再認可

サービスの支払いが事前に行われる場合に、提供されるサービスがクレジット制限内であることを確認するために、クォータ再認可機能が使用されます。

2 種類のクォータ再認可があります。

- 基本クォータ再認可：料金の境界を越えるさまざまな料金レートを考慮する情報が含まれます。レートは時刻に従って設定されます。
- 料金切り替えによるクォータ：料金の境界は存在しません。

サービス クレジットはユーザに割り当て可能なフラグメントまたはクォータで割り当てられます。

2 種類のクレジット クォータがあります。

- SSG Control Info 属性（QT）で指定される、秒単位の時間ベースのクォータ。
- SSG Control Info 属性（QV）で指定される、バイト単位のボリューム ベースのクォータ。

クォータ割り当てが期限切れになるか、または使用料が設定済みのしきい値を超えると、再認可イベントが生成されます。

前提条件

このインターフェイスを使用する場合は、セッションまたはサービス ターゲットがすでにデバイスに存在していると想定する必要があります。再認可イベントはプリペイド機能の設定によって制御できます。また、プリペイド機能がセッションの特定のサービス インスタンスに許可されるように、初期認可が実行されていることを前提とします。

基本クォータ再認可

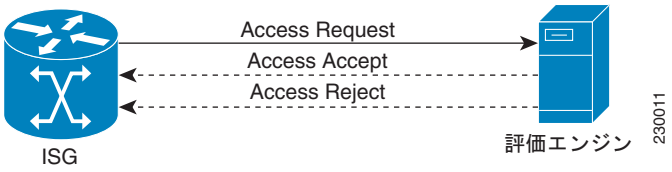
基本的なプリペイド サービスでは、3 種類の認可要求を使用できます。

- クォータ期限切れ
- アイドル タイマー期限切れ
- アイドル状態時の時間クォータ期限切れ

属性の Control-Info QT と Control-Info QV が再認可要求に含まれている場合、クォータ値にはサービスの開始以降の累積合計が含まれます。

いずれの場合も、再認可要求は、図 11 に示すように、Access-Request の後に Access-Accept または Access-Reject が続くという形をとります。

図 11　クォータ再認可の Access-Request



クォータ期限切れ

クォータが使い切られているか、まもなく使い切られる場合、再認可メッセージがサーバ（評価エンジン）に送信されます。表 20 に、クォータ期限切れプリミティブの Access-Request 属性を示します。

表 20　クォータ期限切れの Access-Request 属性

属性/VSA	タイプ	値
VolumeQuota	9, 253 Control-Info	*QV<value>*
TimeQuota	9, 253 Control-Info	*QT<value>*

アイドル タイマー期限切れ

アイドル タイマーの期限が切れると、再認可メッセージが開始され、アイドル サービスに対してクォータを再要求し、それをアクティブ サービスに与えることができます。表 21 に、アイドル タイマー期限切れプリミティブの Access-Request 属性を示します。

表 21　アイドル タイマー期限切れの Access-Request 属性

属性/VSA	タイプ	値
VolumeQuota	9, 253 Control-Info	*QV<value>*
TimeQuota	9, 253 Control-Info	*QT<value>*
PrepaidReauthReason	9, 253 Control-Info	*QR1*

アイドル状態時の時間クォータ期限切れ

ここでは、サービスがアイドル状態のときに時間クォータの期限が切れるとシステムがどのように応答するかを説明します。サービスがアイドル状態のときに時間クォータの期限が切れると、次の属性が使用されます。表 22 に、時間クォータ期限切れプリミティブの Access-Request 属性を示します。

表 22　時間クォータ期限切れの Access-Request 属性

属性/VSA	タイプ	値
VolumeQuota	9, 253 Control-Info	*QV<value>*
TimeQuota	9, 253 Control-Info	*QT<value>*
PrepaidReauthReason	9, 253 Control-Info	*QR0*

基本クォータ再認可の成功

評価エンジンが新しいクォータを割り当てることができる場合、Access-Accept がサーバ評価エンジンから返されます。表 23 に、時間クォータ期限切れプリミティブの Access-Accept 属性を示します。

表 23　時間クォータ期限切れの Access-Request 属性

属性/VSA	タイプ	値
VolumeQuota	9, 253 Control-Info	*QV<value>*
TimeQuota	9, 253 Control-Info	*QT<value>*
Idle-Timeout	28	*<idle-timeout>*

基本クォータ再認可の失敗

評価エンジンが新しいクォータを割り当てることができない場合、Access-Reject 障害メッセージがサーバ評価エンジンから送信されます。

料金切り替えによるクォータ

ここでは、料金切り替えによるクォータ プリミティブについて説明します。内容は次のとおりです。

- 概要
- PT クォータ期限切れ
- PT アイドル タイマー期限切れ
- アイドル状態時の時間クォータ期限切れ
- 料金後再認可の成功
- 料金後再認可の失敗

概要

基本的なクォータ要求は、料金切り替えエポックとともに、切り替え前または切り替え後の再認可要求に基づくプリミティブの二次元マトリクスを形成します。

6 つのプリミティブがあります。

- 切り替え前の再認可要求
  - クォータ期限切れ
  - アイドル タイマー期限切れ
  - アイドル状態時の時間クォータ期限切れ

  切り替え前の再許可プリミティブは、機能的には基本クォータ プリミティブと同じですが、個別プリミティブとは見なされません。
- 切り替え後の再認可要求
  - クォータ期限切れ
  - アイドル タイマー期限切れ
  - アイドル状態時の時間クォータ期限切れ

  切り替え後の再認可プリミティブは、料金エポック後に受信されたクォータの使用状況情報が含まれている可能性があるため、基本クォータ プリミティブと異なります。

PT クォータ期限切れ

クォータが料金切り替えエポック後に期限切れになると、切り替え前の再認可要求に対して Access-Request が送信されます。表 24 に、PT クォータ期限切れプリミティブの Access-Request 属性を示します。

表 24　PT クォータ期限切れの Access-Request 属性

属性/VSA	タイプ	値
VolumeQuota	9, 253 Control-Info	*QV<value>*
TimeQuota	9, 253 Control-Info	*QT<value>*
QuotaPostSwitch	9, 253 Control-Info	*QB<bytes used since switch>*

PT アイドル タイマー期限切れ

料金後（PT）エポックでアイドル タイマーの期限が切れると、再認可メッセージが開始され、アイドル サービスに対してクォータを再要求し、それをアクティブ サービスに与えることができます。表 25 に、PT アイドル タイマー期限切れプリミティブの Access-Request 属性を示します。

表 25　PT アイドル タイマー期限切れの Access-Request 属性

属性/VSA	タイプ	値
VolumeQuota	9, 253 Control-Info	*QV<value>*
TimeQuota	9, 253 Control-Info	*QT<value>*
QuotaPostSwitch	9, 253 Control-Info	*QB<bytes used since switch>*
PrepaidReauthReason	9, 253 Control-Info	*QR1*

アイドル状態時の時間クォータ期限切れ

ここでは、サービスがアイドル状態のときに PT 時間クォータの期限が切れるとシステムがどのように応答するかを説明します。

表 26 に、PT 時間クォータ期限切れプリミティブの Access-Request 属性を示します。

表 26　PT 時間クォータ期限切れの Access-Request 属性

属性/VSA	タイプ	値
VolumeQuota	9, 253 Control-Info	*QV<value>*
TimeQuota	9, 253 Control-Info	*QT<value>*
PrepaidReauthReason	9, 253 Control-Info	*QR0*

料金後再認可の成功

評価エンジンが新しいクォータを割り当てることができる場合、評価エンジンは PT 再認可の Access-Accept メッセージで応答します。

表 27 に、PT 再認可成功メッセージの Access-Accept 属性を示します。

表 27　TPT 再認可成功の Access-Accept 属性

属性/VSA	タイプ	値
VolumeQuota	9, 253 Control-Info	*QX<seconds>;<bytes>;<bytes>*
TimeQuota	9, 253 Control-Info	*QT<value>*
Idle-Timeout	28	*<idle-timeout>*

料金後再認可の失敗

評価エンジンが新しいクォータを割り当てることができない場合、評価エンジンは PT 再認可失敗の Access-Reject メッセージで応答します。

ISG CoA 機能のモニタリングおよびトラブルシューティング

ルータ上で ISG CoA 機能をモニタリングおよびトラブルシューティングするには、次の Cisco IOS コマンドを使用できます。

- **debug radius**
- **debug aaa coa**
- **debug aaa pod**
- **debug aaa subsys**

- **show aaa attributes protocol radius**