P-CSCF のサポート

Proxy-Call Session Control Function（P-CSCF）は、IP Multimedia Subsystem（IMS）ユーザの最初のアクセス ポイントです。P-CSCF はユーザ機器のプロキシ サーバとして動作します。ユーザ機器で送受信される Session Initiation Protocol（SIP; セッション開始プロトコル）シグナリング トラフィックはすべて、P-CSCF を経由する必要があります。P-CSCF は、ユーザ機器からの要求を検証して転送し、応答を処理して、ユーザ機器に転送します。

SIP 処理プロシージャのコンテキストでは、P-CSCF はユーザ エージェントとしても動作します。セッション中に異常な状態が発生すると、P-CSCF はユーザ機器に代わり、一方的にセッションをリリースできます。ユーザ エージェント ロールは、ユーザのパブリック ID およびプライベート ID の送信など、登録中に必要な個別の SIP メッセージの生成にも使用できます。運用ネットワークでは、持続性、ユーザ数、推測トラフィック量、ネットワーク トポロジに基づいて、複数の P-CSCF が使用されることがあります。また、P-CSCF は、SIP サーバと呼ばれることもあります。

Cisco Unified Border Element（SP Edition）上に P-CSCF サポートを実装する場合、ユーザは SIP 隣接用の継承プロファイルを選択する必要があります。利用できる継承プロファイルは次の 3 種類です。

- 標準 Non-IMS プロファイル
- P-CSCF アクセス プロファイル
- P-CSCF コア プロファイル

これらの各プロファイルでは、複数の隣接に適用できる IMS 関連のコンフィギュレーション フィールド セットがグループ化されています。

有効なプロファイルを設定すると、プロファイルが設定されていない隣接に対して、このプロファイルが適用されます。SIP 隣接用のプロファイルがすでに選択されている場合には、エンティティのプロファイルに代わり、既存のプロファイルが使用されます。

Cisco IOS XE Release 2.5 以降の Cisco Unified Border Element（SP Edition）では、Authentication and Key Agreement（AKA）を使用した Hypertext Transfer Protocol（HTTP; ハイパーテキスト転送プロトコル）ダイジェスト認証を SIP コールでサポートします。
このタイプの認証は、モバイル IMS を展開するアクセス認証に使用され、一般に、電話機内部のモバイル加入者のカードに常駐しています。特殊な設定は不要です。唯一の要件は、ネットワークのアクセス側に UNI SIP プロファイルを設定する必要があることです。

Cisco Unified Border Element（SP Edition）は、以前は Integrated Session Border Controller と呼ばれており、このマニュアルでは通常 Session Border Controller（SBC; セッション ボーダー コントローラ）と呼びます。

本章で使用されているコマンドの詳細な説明については、次の場所にある『*Cisco Unified Border Element (SP Edition) Command Reference: Unified Model*』を参照してください。

http://www.cisco.com/en/US/docs/ios/sbc/command/reference/sbcu_book.html

すべての Cisco IOS コマンドの詳細については、http://tools.cisco.com/Support/CLILookup にある Command Lookup Tool を使用するか、Cisco IOS マスター コマンド リストを参照してください。

（注） Cisco IOS XR ソフトウェア リリース　以降、この機能がサポートされているのは統合モデルだけです。

P-CSCF サポートの機能履歴

リリース	変更内容
Cisco IOS XR ソフトウェア リリース	このサポートは、統合モデルのサポートとともに、Cisco IOS XR に追加されました。
Cisco IOS XE Release 2.5	Cisco ASR 1000 シリーズ ルータに AKA 機能を使用した HTTP ダイジェスト認証機能が追加されました。

内容

このモジュールの構成は次のとおりです。

P-CSCF サポートを実装する場合の制約事項

P-CSCF サポートの実装には、次の制約および制限が適用されます。

- Visited Network Identifier は、継承プロファイルの一部ではないため、隣接単位で個別に設定する必要があります。
- この機能では、IPsec または Network Attachment Subsystem（NASS）バンドル認証によるアクセス リンクの確保はサポートされません。
- この機能は、緊急コールをサポートしていません。

P-CSCF サポートに関する情報

ここでは、次の項目について説明します。

標準 Non-IMS プロファイル

このプロファイルは、既存の Cisco Unified Border Element（SP Edition）機能との互換性を提供し、IMS ネットワークで動作しない隣接に対して使用されます。このプロファイルを隣接に使用すると、Cisco Unified Border Element（SP Edition）のプロパティは次のようになります。

- SBC がシグナリング パスに存続できるように、Contact ヘッダーが書き換えられます。

- 未知のヘッダー、方式、およびオプションはデフォルトでパススルーが拒否されます。
- Cisco Unified Border Element（SP Edition）は、アウトバウンド信号に Path ヘッダーを付加しません。
- Cisco Unified Border Element（SP Edition）は、アウトバウンド信号に Record-Route ヘッダーを付加しません。
- Non-REGISTER 要求を送受信するために、この隣接のエンドポイントを登録する必要はありません。
- エンドポイントは、アウトバウンド信号に Route ヘッダーを付加する必要はありません。
- 隣接は、アウトバウンド信号用の P-Charging Vector ヘッダーを生成しません。

P-CSCF アクセス プロファイル

このプロファイルは、P-CSCF アクセス隣接機能の実行に必要なコンフィギュレーションを提供します。このプロファイルを隣接に使用すると、Cisco Unified Border Element（SP Edition）のプロパティは次のようになります。

- Contact ヘッダーは書き換えられません。
- Non-REGISTER 要求を送受信するには、この隣接のエンドポイントを登録する必要があります。
- エンドポイントは、レジストラからの Service-Route セットと一致する Route ヘッダーをアウトバウンド信号に付加する必要があります。
- SBC は、P-CSCF プロファイルを持つ隣接のアウトバウンド信号に Record-Route ヘッダーを付加します。
- SBC は、アウトバウンド信号に Path ヘッダーを付加しません。
- 隣接は、アウトバウンド信号用の P-Charging Vector ヘッダーを生成しません。
- SBC はデフォルトで、P-Asserted Identity、Security-Client、Security-Verify、P-Charging-Function Addresses、P-Charging-Vector、および P-Media-Authorization を除き、すべてのインバウンド非必須ヘッダーのパススルーを許可します。
- SBC はデフォルトで、P-Charging-Function-Addresses、P-Charging-Vector、および P-Media-Authorization を除き、すべてのアウトバウンド非必須ヘッダーを許可します。
- SBC は、すべてのインバウンド非必須方式のパススルーを許可します。
- SBC は、すべてのアウトバウンド非必須方式のパススルーを許可します。UE のレジストラとしての動作は許可されません。
- Supported、Require、または Proxy-Require ヘッダー内の Options タグは、両方向でパススルーが許可されます。

P-CSCF コア プロファイル

このプロファイルは、P-CSCF コア隣接機能の実行に必要なコンフィギュレーションを提供します。このプロファイルを隣接に使用すると、Cisco Unified Border Element（SP Edition）のプロパティは次のようになります。

- Contact ヘッダーは書き換えられません。
- SBC は、デフォルトで、P-Charging-Function-Addresses および P-Media-Authorization を除き、すべてのインバウンド未知ヘッダーを許可します。

- SBC は、P-CSCF プロファイルを持つ隣接のアウトバウンド信号に Record-Route ヘッダーを付加します。
- SBC は、P-CSCF からのアウトバウンド REGISTER 信号に Path ヘッダーを付加します。
- 隣接は、アウトバウンド信号用の P-Charging Vector ヘッダーを生成します。
- Non-REGISTER 要求を送受信するために、この隣接のエンドポイントを登録する必要はありません。
- SBC は、デフォルトで、P-Charging-Function-Addresses および P-Media-Authorization を除き、すべてのアウトバウンド非必須ヘッダーを許可します。
- SBC は、すべての未知方式のパススルーを許可します。
- Supported、Require、または Proxy-Require ヘッダー内の Options タグは、両方向でパススルーが許可されます。

メソッド プロファイル、ヘッダー プロファイル、およびオプションのプロファイルに対する P-CSCF 継承プロファイルの影響

P-CSCF 継承プロファイルを使用すると、選択した P-CSCF 継承プロファイルに基づいたコールに次のプロファイル セット（メソッド プロファイル、ヘッダー プロファイル、オプション プロファイル）が動的に割り当てられます。表 1 に、特定のメソッド プロファイル、ヘッダー プロファイル、およびオプション プロファイルに影響する P-CSCF 継承プロファイルを示します。

この影響は、header-profile、method-profile、またはオプションのプロファイルについての隣接の設定では確認できません。必要に応じて、ヘッダー、メソッド、およびオプションのプロファイルの明示的な設定によって上書きされます。

表 1　ヘッダー、メソッド、およびオプションのプロファイルに対する P-CSCF 継承プロファイルの影響

P-CSCF 継承プロファイル	メソッド プロファイル	ヘッダー プロファイル	オプション プロファイル
preset-p-cscf-access	preset-acc-in-mth タイプ：ブラックリスト アクション：どのメソッドも拒否しない preset-acc-out-mth タイプ：ブラックリスト アクション：REGISTER を拒否する	preset-acc-in-hdr タイプ：ブラックリスト アクション：セキュリティ クライアントを削除する Security-Verify を削除する P-Charging-Vector を削除する P-Asserted-Identity を削除する P-Visited-Network-ID を削除する P-Media-Authorization を削除する P-Charging-Function-Addresses を削除する preset-acc-out-hdr タイプ：ブラックリスト アクション： P-Charging-Vector を削除する P-Media-Authorization を削除する	preset-acc-in-opt preset-acc-out-opt タイプ：ブラックリスト アクション：オプションなし（すべてを渡す）
preset-p-cscf-core	preset-core-in-mth タイプ：ブラックリスト アクション：どのメソッドも削除しない preset-core-out-mth タイプ：ブラックリスト アクション：どのメソッドも拒否しない	preset-core-in-hdr preset-core-out-hdr タイプ：ブラックリスト アクション：ヘッダーを削除しない（すべてを渡す）	preset-core-in-opt preset-core-out-opt タイプ：ブラックリスト アクション：オプションなし（すべてを渡す）
preset-standard-non-ims	preset-std-in-mth preset-std-out-mth タイプ：ホワイトリスト アクション：INFO を渡す UPDATE を渡す	preset-std-in-hdr preset-std-out-hdr タイプ：ホワイトリスト アクション：Server を渡す Diversion を渡す Resource-Priority を渡す	preset-std-in-opt preset-std-out-opt タイプ：ホワイトリスト アクション：Replaces（のみ）を渡す

P-CSCF サポートの実装

ここでは、固有のプロファイルおよびプロファイルの継承の設定方法について説明します。

プロファイルの継承の設定

手順の概要

1. **configure terminal**
2. **sbc** *service-name*
3. **sbe**
4. **sip inherit profile preset-p-cscf-access**
5. **adjacency sip** *adjacency-name*
6. **inherit profile preset-p-cscf-access**
7. **visited network identifier** *network-name*
8. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードをイネーブルにします。
ステップ 2	**sbc** *service-name* **例：** `Router(config)# sbc mysbc`	SBC サービスのモードを開始します。 • *service-name* 引数を使用して、サービスの名前を定義します。
ステップ 3	**sbe** **例：** `Router(config-sbc)# sbe`	SBC サービス内で SBE エンティティのモードを開始します。
ステップ 4	**sip inherit profile preset-p-cscf-access** **例：** `Router(config-sbc-sbe)# sip inherit profile preset-p-cscf-access`	P-CSCF Access 継承プロファイルをグローバル プロファイルとして設定します。他の設定可能なパラメータのリストは、**sip inherit profile** コマンドを参照してください。
ステップ 5	**adjacency sip** *adjacency-name* **例：** `Router(config-sbc-sbe)# adjacency sip sipadj`	SBE SIP 隣接のモードを開始します。 • *adjacency-name* 引数を使用して、SIP 隣接名を定義します。

	コマンドまたはアクション	目的
ステップ 6	**inherit profile preset-p-cscf-access** **例：** `Router(config-sbc-sbe-adj-sip)# inherit profile preset-p-cscf-access`	SIP 隣接が、P-CSCF-Access プロファイルを使用するように設定します。
ステップ 7	**visited network identifier** *network-name* **例：** `Router(config-sbc-sbe-adj-sip)# visited network identifier mynetwork.com`	SIP 隣接に、指定の Visited Network Identifier を設定します。
ステップ 8	**exit** **例：** `Router(config-sbc-sbe-adj-sip)# exit`	SIP 隣接モードを終了して、SBE モードに戻ります。

AKA を使用した HTTP ダイジェスト認証に関する情報

ここでは、次の項目について説明します。

Cisco Unified Border Element（SP Edition）では、SIP コールに対し、Authentication and Key Agreement（AKA）を使用して Hypertext Transfer Protocol（HTTP; ハイパーテキスト転送プロトコル）ダイジェスト認証をサポートします。このタイプの認証は、モバイル IMS を展開するアクセス認証に使用され、一般に、電話機内部のモバイル加入者のカードに常駐することがあります。Cisco Unified Border Element（SP Edition）は、アクセス側（P-CSCF アクセス側プロファイルを持つ側）に User-to-Network Interconnections（UNI）SIP プロファイルが設定されている限り、特殊な設定を必要とせずに、AKA 機能を使用して HTTP ダイジェスト認証をサポートします。

AKA は、Universal Mobile Telecommunications System（UMTS）ネットワークにユーザ認証とセッション キー配布を行う機能です。AKA はチャレンジレスポンスをベースにしています。チャレンジに対するレスポンスは、電話機内の加入者のカード上で実行されるアプリケーションによって計算されます。

HTTP ダイジェスト認証は、IP-PBX で一般的な認証方式です。HTTP ダイジェスト認証の手順は、有効なデバイスだけがネットワークに確実に（SIP レベルで）登録できるようにするために使用されます。SBC は、一般的な登録コール フローである、認証チャレンジとそのレスポンスのパススルーをサポートしています。一般的なコール フローは、エンドポイントからの SIP REGISTER メッセージで構成され、これが SBC によって SIP レジストラにルーティングされます。レジストラは、401 Unauthorized レスポンスと「チャレンジ」で応答します。

このチャレンジにはランダムな番号が含まれており、エンドポイントはこれを使用してレスポンスを計算し、結果を別の REGISTER メッセージで送信します。最後に、レスポンスが有効な場合、レジストラは 200 OK メッセージで応答します。AKA を使用した HTTP ダイジェスト認証の場合、チャレンジに対するレスポンスは、電話機内のモバイル加入者のカード上で実行されるアプリケーションによって計算されます。SBC は、SIP 登録を許可する SIP プロファイルをイネーブルにする方法により、この一般的なコール フローをサポートします。

これ以外に、AKA を使用した HTTP ダイジェスト認証を行う場合、IPsec 接続を確立（実際には 2 つの IPsec 接続）するためのプロシージャに、シグナリング セキュリティを確保する性能面での不安があります。Cisco Unified Border Element（SP Edition）は IPsec をサポートしていますが、ポート セキュリティ関連の ID およびキー情報を SIP メッセージから抽出する機能は、Cisco IOS XE Release 2.5 ではサポートされていません。

AKA を使用した HTTP ダイジェスト認証

次のタスクでは、preset-access プロファイルと preset-core プロファイルを設定する必要がある関連する 2 つの隣接に、AKA を使用して HTTP ダイジェスト認証を設定します。

手順の概要

1. **configure terminal**
2. **sbc** *sbc-name*
3. **sbe**
4. **adjacency** {**sip** | **h323**} *adjacency-name*
5. **inherit profile {preset-access | preset-core | preset-ibcf-ext-untrusted | preset-ibcf-external | preset-ibcf-internal | preset-p-cscf-access | preset-p-cscf-core | preset-peering | preset-standard-non-ims}**
6. **exit**
7. **adjacency** {**sip** | **h323**} *adjacency-name*
8. **inherit profile {preset-access | preset-core | preset-ibcf-ext-untrusted | preset-ibcf-external | preset-ibcf-internal | preset-p-cscf-access | preset-p-cscf-core | preset-peering | preset-standard-non-ims}**
9. **exit**
10. **end**
11. **show sbc** *sbc-name* **sbe adjacencies** ***adjacency-name*** **detail**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードをイネーブルにします。
ステップ 2	**sbc** *sbc-name* **例：** `Router(config)# sbc mySbc`	SBC で SBC サービスを作成して、SBC コンフィギュレーション モードを開始します。
ステップ 3	**sbe** **例：** `Router(config-sbc)# sbe`	SBC の Signaling Border Element（SBE）機能のモードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**adjacency** {**sip** | **h323**} *adjacency-name* **例：** `Router(config-sbc-sbe)# adjacency sip sipEndpoint`	エンドポイントに接する SIP 隣接を設定し、隣接 SIP コンフィギュレーション モードを開始します。
ステップ 5	**inherit profile {preset-access | preset-core | preset-ibcf-ext-untrusted | preset-ibcf-external | preset-ibcf-internal | preset-p-cscf-access | preset-p-cscf-core | preset-peering | preset-standard-non-ims}** **例：** `Router(config-sbc-sbe-adj-sip)# inherit profile preset-p-cscf-access`	必須。エンドポイントに接する SIP 隣接に、プリセット P-CSCF アクセス プロファイルを設定します。 P-CSCF は Proxy-Call Session Control Function の略で、その機能の一部はユーザ認証と IMS 端末との IPsec セキュリティ アソシエーションの確立です。

ステップ 6	`exit`
	
	例：
	`Router(config-sbc-sbe-adj-sip)# exit`
		隣接 SIP コンフィギュレーション モードを終了し、SBE コンフィギュレーション モードを開始します。

ステップ 7	**adjacency** {**sip** | **h323**} *adjacency-name* **例：** `Router(config-sbc-sbe)# adjacency sip SoftSwitch`	レジストラ / ソフトスイッチに接する SIP 隣接を設定し、隣接 SIP コンフィギュレーション モードを開始します。
ステップ 8	**inherit profile {preset-access | preset-core | preset-ibcf-ext-untrusted | preset-ibcf-external | preset-ibcf-internal | preset-p-cscf-access | preset-p-cscf-core | preset-peering | preset-standard-non-ims}** **例：** `Router(config-sbc-sbe-adj-sip)# inherit profile preset-p-cscf-core`	必須。レジストラ / ソフトスイッチに接する SIP 隣接用の preset P-CSCF core プロファイルを設定します。 レジストラに接する隣接は、一般に preset-core プロファイルが設定されています。デフォルトは preset-core です。

ステップ 9	`exit`
	
	例：
	`Router(config-sbc-sbe-adj-sip)# exit`
		隣接 SIP コンフィギュレーション モードを終了し、SBE コンフィギュレーション モードを開始します。

ステップ 10	`end`
	
	例：
	`Router(config-sbc-sbe)# end`
		SBE コンフィギュレーション モードを終了して EXEC モードに戻ります。

ステップ 11	**show sbc** *sbc-name* **sbe adjacencies** ***adjacency-name*** **detail** **例：** `Router# show sbc sbe mySBC sbe adjacencies SoftSwitch detail`	指定の SIP 隣接についてのすべての詳しいフィールド出力を表示します。

AKA を使用した HTTP ダイジェスト認証の設定例

次に、AKA を使用する HTTP ダイジェスト認証を検証するための設定例を示します。

```
sbc asr
 sbe
   adjacency sip UE
    inherit profile preset-p-cscf-access
    visited network identifier open-ims.test
    local-id host pcscf.open-ims.test
    signaling-address ipv4 10.190.5.129
    signaling-port 4060
    remote-address ipv4 10.0.0.0 255.255.0.0
    signaling-peer 10.0.120.19
    dbe-location-id 100
    fast-register disable
    attach

   adjacency sip OpenIMSCore
    inherit profile preset-p-cscf-core
    visited network identifier open-ims.test
    local-id host pcscf.open-ims.test
    signaling-address ipv4 10.190.5.129
    signaling-port 4060
    remote-address ipv4 10.0.48.236 255.255.255.255
    signaling-peer 10.0.48.236
    dbe-location-id 100
    registration rewrite-register
    registration target address open-ims.test
    attach
```