共通コンポーネント

Cisco Unified Border Element の次のコンポーネントは、このマニュアルの設定プロファイルの例すべてに共通です。

- セキュア メディア
- 隣接
- コール ポリシー
- CAC ポリシー
- SIP プロファイル

セキュア メディア

セキュア メディア セグメントでは、2 つのネットワーク間でシグナリングされていない暗号化データ ストリームをセキュアに転送します。

セキュア メディアはデフォルトでディセーブルです。セキュア メディアをイネーブルにするには、SBC の設定では、グローバル レベルで設定します。イネーブルにすると、すべてのコールに適用されます。

セキュア メディアをイネーブルにすると、Cisco Unified Border Element は、すべてのエンド ポイントが、実際のエンド ポイントの機能に関係なく、暗号化データ ストリームを処理できると想定します。

セキュア メディアは、次のタイプの任意のアドレスに適用可能です。

- インターフェイスの物理アドレス
- インターフェイスの論理アドレス
- サービス仮想インターフェイス（SVI）アドレス

次の例は、セキュア メディアをイネーブルにする例を示します。

```
sbc MY_SBC
    sbe
    secure-media
    …
    …
```

secure-media コマンドの実行後に設定された接続はすべて、セキュアな接続です。

隣接

Cisco Unified Border Element と、カスタマー、ネットワーク、ビジネス、またはサービス プロバイダー間の接続を隣接といいます。隣接の設定には、Cisco Unified Border Element と、カスタマー、ネットワーク、ビジネス、またはサービス プロバイダー間の接続に使用される、隣接のローカル IP アドレスとリモート IP アドレスが含まれています。

隣接には次の 2 種類があります。

- バックツーバック ユーザ エージェントとして機能する Session Initiation Protocol（SIP）隣接
- H.323 ゲートウェイとして機能する H.323

隣接はアカウントでグループ化できます。アカウントを使用すれば、カスタマーに基づいてコール ポリシーおよび CAC ポリシーを定義できます。

シグナリング アドレスを隣接ごとに設定し、各シグナリング アドレスをシグナリング ポートと組み合わせる必要があります。SBC は、シグナリングおよび制御パケットの受信に、IP アドレス/ポート番号のペアを使用します。

SIP 隣接では、シグナリング アドレスをリモート デバイスへの発信プロキシ アドレスとして指定します。

シグナリング アドレスは次のタイプのアドレスのいずれかです。

- ルータに設定されたループバック アドレス
- インターフェイスの物理アドレス
- サブインターフェイスの論理アドレス
- スタティック仮想アドレス（SVI）

次に、Business-to-Business Telepresence 設定プロファイルの例の隣接設定の例を示します。

```
adjacency sip CUCM1
    vrf CUCM1
    header-profile inbound PASS-HEADERS
    header-profile outbound PASS-HEADERS
    method-profile inbound method1
    method-profile outbound method1
    option-profile ua inbound option1
    option-profile ua outbound option1
    preferred-transport tcp
    security trusted-unencrypted
    signaling-address ipv4 23.61.1.1
        statistics method summary
    signaling-port 5160
    remote-address ipv4 175.181.0.10 255.255.255.255
    signaling-peer 175.181.0.10
    signaling-peer-port 5160
    account CUCM1
    attach

adjacency sip CUCM2
    vrf CUCM2
    header-profile inbound PASS-HEADERS
    header-profile outbound PASS-HEADERS
    method-profile inbound method1
    method-profile outbound method1
    option-profile ua inbound option1
    option-profile ua outbound option1
    preferred-transport tcp
    security trusted-unencrypted
    signaling-address ipv4 23.61.2.1
```

```
statistics method summary
signaling-port 5160
remote-address ipv4 175.182.0.12 255.255.255.255
signaling-peer 175.182.0.12
signaling-peer-port 5160
account CUCM2
attach
```

（注） VRF 作成の例については、「VRF の例」（P.103）を参照してください。

コール ポリシー

コール ポリシーは、SBC が新しいコール イベントに応答する方法を定義する一連のルールです。コール ポリシーには、番号分析およびルーティングが含まれます。

コール ポリシー セットには、隣接名、送信元番号、および宛先番号などのエントリが含まれている 1 つ以上のテーブルが含まれます。SBC は、この表のエントリで着信コールと発信コール パケットのフィールドを照合するために、次のテーブルを使用します。これらの一致に基づいて、SBC は次のタスクを実行できます。

- 別のテーブルへの移動
- 隣接の選択
- コールの完了

コール ポリシーの設定

次に、2 つの CUCM 隣接（CUCM1 および CUCM2）を接続するエントリ コマンドおよびテーブル エントリでコール ポリシーを設定する例を示します。

```
sbc MY_SBC
    sbe
    secure-media
        ….
        ….
        ….
    call-policy-set 1
        first-call-routing-table start-table
        rtg-src-adjacency-table start-table
        entry 1
            match-adjacency CUCM2
            dst-adjacency CUCM1
            action complete
        entry 2
            match-adjacency CUCM1
            dst-adjacency CUCM2
            action complete
        complete
    active-call-policy-set 1
```

番号分析

番号分析コール ポリシーが有効な電話番号の Cisco Unified Border Element テーブルの番号と着信と発信番号を比較します。

SBC では、コール ポリシー エントリ テーブルに設定されているエントリと着信番号を照合することで、分析に番号が付けられます。番号分析コール ポリシーは、新しいコール イベントだけに適用されます。着信番号がコール ポリシーのどのエントリとも一致しない場合、SBC はコールを拒否します。

番号分析コール ポリシーは次の機能を実行できます。

- 番号検証
- 番号カテゴリ化
- ディジット操作

番号分析は、次のタイプのコール ポリシー テーブルの有効な番号で着信番号と照合することで行われます。

- dst-number：このタイプのテーブルには、照合値が宛先の完全な番号を表すエントリが含まれます。このようなテーブルでは、着信ディジット ストリング全体がエントリの照合値に正確に一致する場合、エントリがイベントに一致します。
- dst-prefix：このタイプのテーブルには、照合値が宛先の番号のプレフィクスを表すエントリが含まれます。このようなテーブルでは、着信ディジット ストリングのサブセット（着信ディジット ストリングの先頭部分から抽出された連続するディジットからなるサブセット）が、エントリの照合値に正確に一致する場合、エントリがイベントに一致します。
- src-number：このタイプのテーブルには、照合値が送信元の完全な番号を表すエントリが含まれます。このようなテーブルでは、送信元ディジット ストリング全体がエントリの照合値に正確に一致する場合、エントリがイベントに一致します。
- src-prefix：このタイプのテーブルには、照合値が送信元の番号のプレフィクスを表すエントリが含まれます。このようなテーブルでは、送信元ディジット ストリングのサブセット（送信元ディジット ストリングの先頭部分から抽出された連続するディジットからなるサブセット）が存在し、エントリの照合値に正確に一致する場合、エントリがイベントに一致します。

（注） 番号分析中に、宛先番号のみを変更できます。送信元番号は変更できません。ルーティング時に送信元番号を変更できます。

コール ポリシー テーブル エントリの形式は、形式が限定された、着信ディジットのストリングを表す正規表現です。表 1 で、使用される形式の構文について説明します。

表 1　番号分析表現

表現	説明
X	0 ～ 9 の任意の数値。
( )	カッコ内のディジットはオプションです。たとえば、(0)XXXX は、0XXXX と XXXX を表します。
[ ]	角カッコ内のディジットのいずれかが使用されます。たとえば、[01]XXX は、0XXX と 1XXX を表します。値の範囲を角カッコ内で表すことができます。たとえば、[013-5]XXX は、0XXX、1XXX、3XXX、4XXX および 5XXX を表します。
*	電話の * キー。
#	電話の # キー。
-	ディジットの区切り文字
,	ディジットの区切り文字
a-f/A-F	16 進数

番号およびプレフィクスのマッチングの詳細については、『*Cisco Unified Border Element (SP Edition) Configuration Guide: Unified Model*』の第 12 章「Implementing Cisco Unified Border Element (SP Edition) Policies」を参照してください。

番号検証

番号検証コール ポリシーは、着信番号がコール ポリシー テーブルの有効な電話番号と一致しているかどうかを確認します。次に、番号検証を行うコール ポリシーの設定例を示します。

```
sbc MY_SBC
    sbe
        call-policy-set 2
            first-number-analysis-table VALIDATE-DEST-PREFIX
            na-dst-prefix-table VALIDATE-DEST-PREFIX
            entry 1
                match-prefix 8XX
                action accept
                exit
            entry 2
                match-prefix 911
                action accept
                exit
            entry 3
                match-prefix 1XX
                action accept
                exit
            entry 4
                match-prefix X
                action reject
                exit
            complete
        active-call-policy-set 2
```

番号カテゴリ化

番号カテゴリ化を使用すれば、処理中にコール イベントをユーザ定義のカテゴリに分類することができます。カテゴリに配置されるイベントは、CAC ポリシーの段階で参照できます。次に、番号カテゴリ化を行うコール ポリシーの設定例を示します。

```
sbc MY_SBC
    sbe
        call-policy-set 3
            first-number-analysis-table VALIDATE-DEST-PREFIX
            na-dst-prefix-table VALIDATE-DEST-PREFIX
            entry 1
                match-prefix 8X
                category Non-emergency
                action accept
                exit
            entry 2
                match-prefix 1XX
                category Non-Emergency
                action accept
                exit
            entry 3
                match-prefix 911
                category Emergency
                action accept
                exit
            entry 4
                match-prefix X
                action reject
                exit
        complete
    active-call-policy-set 3
```

ディジット操作

ディジット操作は、E.164 形式などの標準形式に通話番号を再フォーマットするプロセスです。次の例では、entry 1 の **edit-dst del-prefix 1** コマンドで着信番号から先行する 1 の桁を削除し、ストリング全体を削除します。

次に、ディジット操作を行うコール ポリシーの設定例を示します。

```
sbc MY_SBC
    sbe
        call-policy-set 4
            first-number-analysis-table VALIDATE-DEST-PREFIX
            na-dst-prefix-table VALIDATE-DEST-PREFIX
            entry 1
                match-prefix 8X
                category Non-emergency
                edit-dst del-prefix 1
                action accept
                exit
            entry 2
                match-prefix 1XX
                category Non-Emergency
                action accept
                exit
            entry 3
                match-prefix 911
                category Emergency
                action accept
                exit
            entry 4
                match-prefix X
                action reject
                exit
        complete
    active-call-policy-set 4
```

ルーティング

ルーティングは、コール ポリシー テーブルでも処理されます。ルーティングは、シグナリング要求の送信先のネクスト ホップおよび VoIP シグナリング エンティティを決定する処理です。

ルーティング コール ポリシーは、新しいコール イベントと加入者登録イベントに適用されます。

ルーティング コール ポリシーは、2 段階で適用されます。

1. ディジット操作
2. 宛先隣接（またはロード バランシングの隣接グループ）の選択

正規表現を使用して次のようなエンティティと照合するルーティング ルールを設定できます。

- ユーザ名
- ドメイン名（送信元または宛先 SIP URI の一部）

コール番号の桁はルーティング プロセス中に変更も置換もできます。

（注） 新しいコール イベントが既存の加入者登録と一致すると、新しいコールは既存の加入者登録の送信元 IP アドレスとポートに自動的にルーティングされます。これに対して設定済みポリシーは不要です。設定済みポリシーはこのようなコールのルーティングに影響しません。

（注） ルーティング コール ポリシーは、アップデート シグナリング メッセージのようなコール アップデート イベントに適用されません。コール アップデート イベントは、コールの宛先隣接に自動的にルーティングされます。

次の設定では、コールのプレフィクス番号に基づいてコールをルーティングするためのルーティング コール ポリシー テーブルを設定する例を示します。

```
sbc MY_SBC
    sbe
        call-policy-set 5
        first-call-routing-table ROUTE-ON-DEST-NUM
        rtg-dst-address-table ROUTE-ON-DEST-NUM
        entry 1
            match-address 212
            prefix
            edit add-prefix 1
            dst-adjacency CUCM1
            action complete
            exit
        entry 2
            match-address 215
            prefix
            dst-adjacency CUCM1
             action complete
            entry 3
            match-address 732
            prefix
            dst-adjacency CUCM2
            action complete
            exit
        entry 4
            match-address 908
            prefix
            dst-adjacency CUCM2
            edit replace 609
            action complete
            exit
        complete
    active-call-policy-set 5
```

CAC ポリシー

コール アドミッション制御（CAC）ポリシーは、特定のネットワークの CAC ポリシーで設定した制限に基づいて、コール イベントを許可または拒否するかどうかを決定します。

CAC ポリシーの主な用途は、次のとおりです。

- DoS 攻撃の防止
- サービス レベル契約（SLA）の実装

DoS 攻撃の防止

DoS 攻撃やマスメディアによる電話参加など、有害なおそれがあるレベルの負荷に対して、負荷の影響を受けやすいネットワーク要素を守るために CAC ポリシーを使用します。

SLA の実装

組織間の SLA のポリシングとネットワーク利用率のレベルを超えないようにするために CAC ポリシーを使用します。

CAC ポリシーは、どのタイプのコール イベントにも適用できます。イベントが CAC ポリシーにより認可されていない場合、Cisco Unified Border Element はコール イベントを拒否し、該当するエラー コードを返します。

（注） コール アドミッション イベントだけを CAC ポリシーで設定します。その他の番号分析やルーティングなどのコール イベントは、コール ポリシーで設定します。

次に、メディア ストリームの帯域幅フィールドを無視するように CAC ポリシーを設定する例を示します。帯域幅フィールドを無視すると、Cisco Unified Border Element は Secure Real-Time Transport Protocol（SRTP）から Real-Time Transport Protocol（RTP）にメディア ストリームをダウングレードできます。

```
sbc MY_SBC
    sbe
    secure-media
        ….
        ….
        ….
    cac-policy-set 1
        description Ignore the  bandwidth field in SDP
        first-cac-table BW
        first-cac-scope call
        cac-table BW
        table-type policy-set
        entry 1
            media bandwidth-field ignore
            action cac-complete
    active-cac-policy-set 1
```

SIP プロファイル

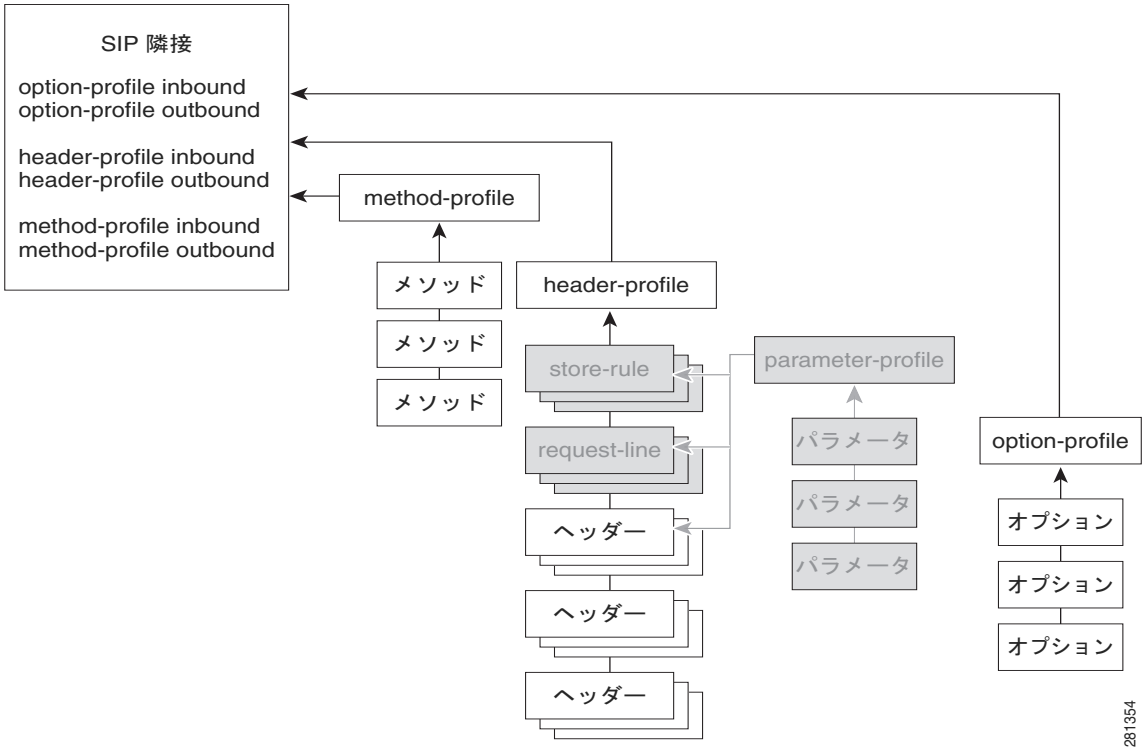
SIP プロファイルを使用して、リスト ヘッダーまたはメソッドを含むホワイトリストまたはブラックリスト、およびそれらに対して実行されるアクションを作成できます。ホワイトリストは要求を受け入れるために使用します。ブラックリストは要求を拒否するために使用します。

次のタイプの SIP プロファイルはホワイトリストまたはブラックリストに使用できます。

- ヘッダー プロファイル
- メソッド プロファイル
- パラメータ プロファイル
- オプション プロファイル

図 2 に、さまざまなプロファイルと、それらが SIP 隣接にどのように接続されるかを示します。ヘッダー プロファイルは、個々のメソッドと関連付けることもできますが、この例では、ヘッダー プロファイルを SIP 隣接に直接関連付けます。プロファイルは、入力 SIP 隣接および出力 SIP 隣接に関連付ける必要があります。

図 2　　隣接に接続するメソッド、ヘッダー、オプション プロファイル



（注） パラメータ プロファイルをヘッダーに直接関連付けられますが、パラメータ プロファイルは、このマニュアルの Telepresence の例では使用しません。したがって、パラメータは、図 2 ではグレー表示しています。

このマニュアルの Telepresence の例では、次の 2 つのホワイトリストを使用し、ブラックリストは使用しません。

- メソッド プロファイルのホワイトリスト
- ヘッダー プロファイルのホワイトリスト

リストのヘッダーまたはメソッドの各エントリは任意で次のいずれかのアクションを割り当てることができます。

- Pass
- Reject

ホワイトリストは Pass アクションだけを使用します。ブラックリストは Reject アクションだけを使用します。

ヘッダー プロファイルは、ホワイトリストまたはブラックリストを使用してパスまたは拒否する事前定義されたヘッダーのリストです。

メソッド プロファイルは、ホワイトリストまたはブラックリストを使用してパスまたは拒否する事前定義されたメソッドのリストです。

オプション プロファイルは、ホワイトリストまたはブラックリストにすることでパスまたは拒否できる定義済みのオプションのリストです。Telepresence の例では、必須の Telepresence オプションの TIMER および REPLACES は、メソッド プロファイルのホワイトリストでパスされます。

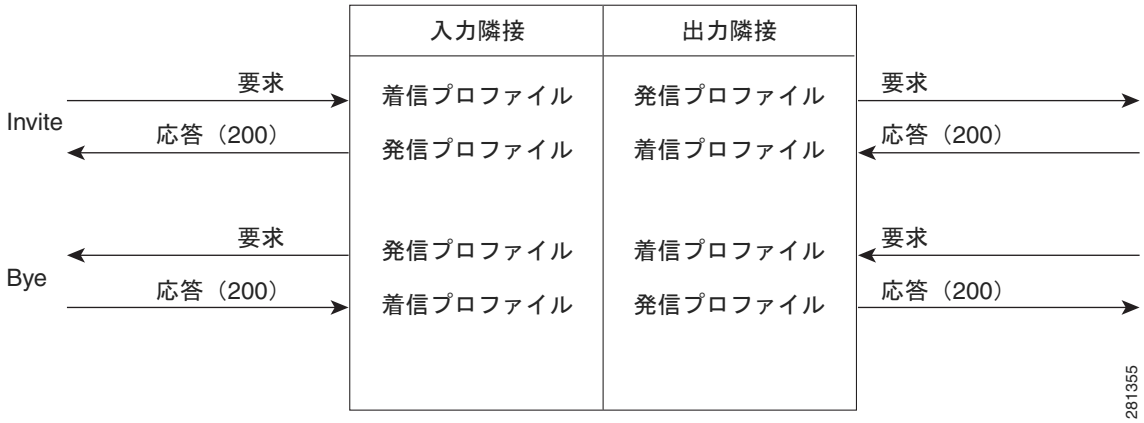
ホワイトリストは、**sip header-profile** コマンドを使用し、ヘッダーまたはメソッドをエントリとして追加し、各エントリに Pass アクションを割り当てて作成されます。

メソッド プロファイルのホワイトリストは全体の SIP メッセージに適用されます。メソッド プロファイルのアクションはデフォルト プロファイルの動作を上書きします。

ヘッダー プロファイルのホワイトリストは SIP メッセージの行にだけ適用されます。ヘッダー プロファイルは、ヘッダーの任意の部分と一致できますが、ヘッダー全体の置換しかできません。

プロファイルは、各隣接の着信側および発信側で適用する必要があります。図 3 で、コール中の隣接間のプロファイルのフローを示します。

図 3　　コール中のプロファイルのフロー



すべてのヘッダーは、入力隣接の Bye レスポンス（200）によって処理される前に、パス、削除または変更されます。すべてのメッセージは、回線に送信される前に出力隣接の Bye レスポンス（200）によって処理された後に、パス、削除または変更されます。

（注） 入力側に着信するメッセージで機能するヘッダーとメソッドのアクションの場合は、着信プロファイルからヘッダーおよびメソッドを入力側で最初にパスする必要があります。

次の例では、着信および発信プロファイルにホワイトリストを付加する例を示します。

```
adjacency sip CUCM1
    header-profile inbound PASS-HEADERS
    header-profile outbound PASS-HEADERS
    method-profile inbound method1
    method-profile outbound method1
    option-profile ua inbound option1
    option-profile ua outbound option1

adjacency sip CUCM2
    header-profile inbound PASS-HEADERS
    header-profile outbound PASS-HEADERS
    method-profile inbound method1
    method-profile outbound method1
    option-profile ua inbound option1
    option-profile ua outbound option1
```

プロファイルは、隣接に接続している場合は、削除できません。どの隣接がプロファイルを使用しているか確認するには、次の show コマンドを入力します。

- show sbc sbe sip method-profile
- show sbc sbe sip essential-methods

ヘッダー プロファイル

次のヘッダー プロファイルのホワイトリストでは、表示されているすべてのヘッダーをパスするように設定されます。

```
sbc MY_SBC
    sbe
    secure-media
        …
    sip header-profile PASS-HEADERS
        description “pass non-essential headers”
        header Allow entry 1
            action pass
        header Min-SE entry 1
            action pass
        header Reason entry 1
            action pass
        header SERVER entry 1
        action pass
        header DIVERSION entry 1
        action pass
        header Allow-Events entry 1
        action pass
        header Remote-Party-ID entry 1
        action pass
        header Session-Expires entry 1
        action pass
        header session-expiry entry 1
        action pass
        header RESOURCE-PRIORITY entry 1
        action pass
```

表 2 に、PASS-HEADERS ホワイトリストの 3 つのヘッダー エントリについて説明します。

表 2　PASS-HEADERS ホワイトリストの 3 つのエントリの説明

ヘッダー	説明
header SERVER entry	要求の処理にユーザ エージェント サーバ（UAS）が使用するソフトウェアに関する情報が含まれます。
header DIVERSION entry	コールを転送するユーザに基づいてフィーチャ ロジックの実装を許可します。
header RESOURCE-PRIORITY entry	緊急事態によって引き起こされるリソース不足の間、SIP でシグナリングされたリソースへのアクセスの優先順位付けを支援します。

メソッド プロファイル

次のメソッド プロファイルのホワイトリストでは、メソッドはアクションで設定され、プロファイルはオプションで設定されます。

```
sbc MY_SBC
    sbe
    secure-media

    sip method-profile method1
        description “pass default methods”
        pass-body
        method INFO
            action pass
        method OPTION
            action pass
        method UPDATE
            action pass
    sip option-profile option1
        description “pass default options plus TIMER”
        option TIMER
        option REPLACES
    …
```