電話ハッカーの侵入阻止

前提条件

以下は、Unified Cisco Mobility Express で電話料金詐欺防止を構成するための前提条件です。

トランク側で電話料金詐欺防止を構成する前提条件

- Cisco Unified CME 8.1 以降のバージョン。
- Cisco IOS Release 15.1(2)T。

回線側 SIP で電話料金詐欺防止を構成する前提条件

- Unified Cisco Mobility Express 12.6 以降のバージョン
- Cisco IOS XE Gibraltar リリース 16.11.1a 以降。

概要

Unified Cisco Mobility Express リリース 12.6 は、Unified Cisco Mobility Express の SIP 回線側にセキュリティを適用することにより、既存の [電話料金詐欺防止（Toll Fraud Prevention）] 機能を

強化します。この機能拡張により、Unified Cisco Mobility Express システムは、SIP 回線側からの不正ユーザーによる潜在的な通話料金詐欺の悪用から保護されます。

SIP 回線を介したセキュアな通話のための Unified Cisco Mobility Express の電話料金詐欺防止の主な機能の一部は次のとおりです。

- 処理される SIP 回線からのすべての REGISTER メッセージ。
- セカンダリ Cisco Mobility Express が有効になっている場合、SIP 回線からの REFER メッセージはプライマリ Cisco Mobility Express でのみ処理されます（参照先: urn:X-cisco-remotecc:token-registration）。
- エンドポイントから Unified Cisco Mobility Express にトリガーされるすべての SIP 回線メッセージが認証されます。
- エンドポイントの IP アドレスが IP アドレスの信頼できるリストに含まれていない場合、通話は Unified Cisco Mobility Express を介して発信されません。

Unified Cisco Mobility Express 12.6 以降での電話料金詐欺防止の詳細については、「Unified Cisco Mobility Express での SIP 回線側の電話料金詐欺防止 （2 ページ）」を参照してください。

（注） Unified Cisco Mobility Express 8.1 ～ 12.5 リリースでは、通話料金詐欺の防止は、SIP トランクを介した通話の保護のみに制限されていました。SIP トランクを介した電話料金詐欺防止の詳細については、「電話料金詐欺防止のための信頼できる IP アドレスリストの構成」を参照してください。

Unified Cisco Mobility Express での SIP 回線側の電話料金詐欺防止

Unified Cisco Mobility Express 12.6 は、Unified Cisco Mobility Express の SIP 回線側にセキュリティと電話料金詐欺防止を適用します。**ip address trusted authentication** 構成は、回線側で不正な通話をブロックします。したがって、[電話料金詐欺防止（Toll fraud Prevention）]機能は、Unified Cisco Mobility Express 12.6 以降を回線側の不正ユーザーから保護します。

Unified Cisco Mobility Express 12.6 での電話料金詐欺防止の構成の一部として、すべての回線側エンドポイントを Unified Cisco Mobility Express に登録する必要があります。以下は、Unified Cisco Mobility Express 12.6 の電話料金詐欺防止の構成です。

- CLI コマンド **ip address trusted authentication** は、Unified Cisco Mobility Express ではデフォルトで有効になっています。このコマンドにより、Unified Cisco Mobility Express システムでセキュリティが有効になります。
- 次のように、**iptrust-list** 構成モードで信頼できる電話機の IP アドレスまたはサブネットを入力することにより、Unified Cisco Mobility Express エンドポイントを信頼できるものとして手動構成できます。

```
Router (conf-voi-serv)#ip address trusted list
Router(cfg-iptrust-list)#ipv4 192.168.10.11
```

- 次のように、Unified Cisco Mobility Express エンドポイントの手動で追加された IP アドレスを確認できます。

```
Router(cfg-iptrust-list)#do show run | s voice service voip
voice service voip
ip address trusted list
ipv4 192.168.10.30
ipv4 192.168.10.31
ipv4 192.168.10.32
ipv4 192.168.10.33
media bulk-stats
```

- CLI コマンド **ip address trusted list** は、登録されているすべてのディレクトリ番号からの着信通話の IP アドレスを一覧表示します。**voice service voip** コマンドは、構成モードで構成されます。

- **show ip address trusted list** CLI コマンドは、信頼できる IP アドレスのリストを表示します。信頼できる IP アドレスは、次のリストで表示されます。
  - ダイヤルピア（トランク側にのみ適用可能)：ダイヤルピア 構成モードで設定されている電話機の IP アドレスの詳細を提供します。
  - 構成された IP アドレスの信頼できるリスト：手動で構成された信頼できる IP アドレスの詳細を提供します。
  - 動的 IP アドレスの信頼できるリスト：登録済み電話機の IP アドレスに関する詳細を提供します。このリストは、Unified Cisco Mobility Express 12.6 リリースで導入されました。
  - サーバーグループ：server-groups 構成モードで構成されている電話機の IP アドレスの詳細を提供します。

```
Router>enable
Router#show ip address trusted list
IP Address Trusted Authentication
Administration State: UP
Operation State: UP

IP Address Trusted Call Block Cause: call-reject (21)

VoIP Dial-peer IPv4 and IPv6 Session Targets:
Peer Tag Oper State Session Target
-------- ---------- --------------
4         UP        ipv4:10.65.125.155

Configured IP Address Trusted List:
ipv4 192.168.20.1
ipv4 192.168.20.2 255.255.0.0
ipv4 192.168.20.3 255.255.0.0
ipv4 192.168.20.4 255.255.255.0

Dynamic IP Address Trusted List:
IP Address                          Subnet Mask      Count   Reason
---------------------------------   ------------     -----   ----------------
ipv4:8.55.22.36                                      1       Phone Registered
ipv4:192.168.10.12                                   2       Phone Registered
ipv6:2001:420:54FF:13::312:0 119                     1       Phone Registered
ipv4:8.55.22.15                                      1       Phone Registered
```

- CLI コマンド **ip address trusted list** は、Unified Cisco Mobility Express 上のすべての信頼できる IP Phone の IP アドレスに関する情報を提供します。Unified Cisco Mobility Express の特定の IP Phone に固有の情報については、CLI コマンド **show ip address trusted check** を使用してください。

```
Router#show ip address trusted check 8.55.0.139
ip[8.55.0.139] authentication is FAILED!

Router#show ip address trusted check 8.55.0.136
ip[8.55.0.136] authenticate is PASSED by dynamic TrustList
```

- **sip** 構成モードの CLI コマンド **silent-discard untrusted** は、信頼できない送信元からの SIP 要求を破棄します。このコマンドは、Unified Cisco Mobility Express ではデフォルトで有効になっています。

アップグレードの考慮事項

Unified Cisco Mobility Express 12.6 バージョンにアップグレードする場合、通話料金の不正防止をサポートするために追加の設定を実行する必要はありません。Unified Cisco Mobility Express で手動で設定または自動登録されたすべてのエンドポイントは、Unified Cisco Mobility Express IP アドレス信頼リストに追加されます。CLI コマンド **show ip address trusted list** の出力で、信頼できる IP アドレスのリストを表示できます。

IP アドレス信頼認証

IP アドレス信頼認証プロセスは、無許可の呼び出しをブロックし、無許可のユーザーによる潜在的な電話の不正利用から Cisco Unified Cisco Mobility Express システムを保護するために役立ちます。Unified Cisco Mobility Express では、デフォルトで **IP address trusted authentication** が有効化されています。IP アドレス信頼認証が有効になっている場合、Unified Cisco Mobility Expressは、着信 VoIP 通話のリモート IP アドレスが正常にシステム **IP address trusted list** から検証された場合のみ、着信 VoIP（SIP/H.323）通話を許可します。IP アドレス信頼認証に失敗した場合、着信 VoIP コールはアプリケーションによってユーザ定義の原因コード付きで切断され、新しいアプリケーション内部エラー コード 31 メッセージ（TOLL_FRAUD_CALL_BLOCK）が記録されます。構成情報については、着信 VoIP 通話用の IP アドレス信頼認証の構成 （6 ページ）を参照してください。

Unified Cisco Mobility Express は、**IP address trusted list** を維持し、着信通話 VOIP 通話のリモート IP アドレスを検証します。Unified Cisco Mobility Express は、VoIP ダイヤルピアの IPv4 セッションターゲットを保存し、信頼できる IP アドレスを **IP address trusted list** に自動追加します。IPv4 セッションターゲットは、動作中の VoIP ダイヤルピアの状態が「UP」であるときのみ信頼できる IP アドレスとして識別されます。100 までの IPv4 アドレスを信頼できる IP アドレスリストで定義できます。信頼できる IP アドレスのリスト内で IP アドレスの重複は許可されません。着信 VOIP コールの信頼できる IP アドレスは手動で 100 個まで追加できます。信頼できる IP アドレスの手動追加については、「着信 VoIP 通話用の有効な IP アドレスの追加 （8 ページ）」を参照してください。

コール詳細レコード（CDR）履歴レコードは、IP アドレス信頼認証に失敗した結果、コールがブロックされたときに生成されます。新しい音声の内部エラー コード（IEC）が CDR 履歴レコードに保存されます。[音声iec syslog（voice iec syslog）] オプションが有効な場合、音声 IEC エラーメッセージは、 syslog に記録されます。次に、IEC 電話ハッカーの侵入コールを拒否したときの syslog 表示を示します。

```
*Aug 14 19:54:32.507: %VOICE_IEC-3-GW: Application Framework Core: Internal Error (Toll
 fraud call rejected): IEC=1.1.228.3.31.0 on callID 3 GUID=AE5066C5883E11DE8026A96657501A09
```

Unified Cisco Mobility Express が「gateway」と定義され、「session-target ras」が設定された VoIP ダイヤルピアの動作状態が、[アップ（UP）] の場合、**IP address trusted list** 認証を一時停止する必要があります。着信 VOIP コールルーティングがゲートキーパーによって制御されます。表 1 : IP アドレス信頼認証の管理状態と動作状態 （5 ページ） は、管理者状態と動作状態を異なるトリガー条件で表示します。

表 *1 : IP* アドレス信頼認証の管理状態と動作状態

トリガー条件	管理状態	操作ステータス
ip address trusted authenticate が有効になっている場合。	Down	Down
「gateway」が定義され、セッションターゲットとして「ras」が設定された VoIP ダイヤルピアが [アップ（UP）] 動作状態の場合	Up	Down
ip address trusted authenticate が有効で、「gateway」が定義されていないまたは、セッションターゲットとして「ras」が設定された VoIP ダイヤルピアが [アップ（UP）] 動作状態ではない場合	Up	Up

（注） 潜在的な電話ハッカーの侵入の脅威を防止するには、Out-Of-Dialog REFER（OOD-R）を有効にする前に SIP 認証を有効にすることを推奨します。

着信 ISDN コールに対するダイヤル イン

Cisco Unified Cisco Mobility Express 8.1 以降のバージョンでは、着信 ISDN 通話に対する電話料金詐欺防止用に **direct-inward-dial isdn** 機能が有効になっています。インバウンドの単純な旧式の電話サービス（POTS）ダイヤルピアで **direct-inward-dial** オプションが無効化されていても、着信 ISDN 一括ダイヤル通話の着信番号が、発信ダイヤルピアイベントの照合に使用されます。発信ダイヤルピアが発信通話のセットアップ用に選択されていない場合、着信 ISDN 通話は原因コード「unassigned-number (1)」で切断されます。構成情報については、着信 ISDN 通話用のダイヤルイン方式（DID）の構成 （10 ページ）を参照してください。

一致するダイヤルピアのない ISDN 通話の切断

Cisco Unified CME 8.1 以降のバージョンでは、一致する着信音声ダイヤルピアが選択されていない場合に、無許可の ISDN コールが切断されます。2 段階ダイヤルサービスを含むデフォルトの POTS ダイヤルピア動作を回避して着信 ISDN 通話を処理するように着信ダイヤルピアが選択されていない場合、Cisco Unified Cisco Mobility Express および音声ゲートウェイは、**dial-peer no-match disconnect-cause** コマンドを使用して、着信通話 ISDN 通話を切断します。

アナログおよびデジタル FXO ポートでの 2 段階ダイヤルサービスのブロック

Cisco Unified CME 8.1 以降のバージョンでは、アナログまたはデジタル FXO ポートがオフフックになり、Private Line Automatic Ringdown（PLAR）接続が音声ポートからセットアップされない場合に開始される、2 段階ダイヤルサービスがブロックされます。したがって、発信ダイヤルピアは着信アナログまたはデジタル FXO コール用に選択されず、ダイヤルされた番号は FXO コールから収集されません。Cisco Unified Cisco Mobility Express および音声ゲートウェイは、原因コード「unassigned-number (1)」で FXO 通話を切断します。Cisco Unified Cisco Mobility Express はデフォルトで、FXO 音声ポートからの **no secondary dialtone** を使用して、アナログまたはデジタル FXO ポートの 2 段階ダイヤルサービスをブロックします。アナログおよびデジタル FXO ポートでの 2 段階ダイヤル サービスのブロックの詳細については、アナログおよびデジタル FXO ポートでセカンダリダイヤルトーンをブロック （11 ページ）を参照してください。

電話料金詐欺防止の構成

着信 VoIP 通話用の IP アドレス信頼認証の構成

制約事項

- IP アドレス信頼認証は、着信コールが IPv6 コールの場合はスキップされます。
- 着信 VoIP 通話では、IP アドレス信頼認証が「UP」動作状態の場合に IP 信頼認証を呼び出す必要があります。

始める前に

- SIP 回線通話用の Unified Cisco Mobility Express 12.6 以降のバージョン。
- セキュアトランクコール用の Unified Cisco Mobility Express 8.1 以降のバージョン。

手順の概要

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **ip address trusted authenticate**
5. **ip-address trusted call-block cause code**
6. **end**
7. **show ip address trusted list**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル構成モードを開始します。
ステップ 3	**voice service voip** 例： `Router(config)# voice service voip`	voice service voip コンフィギュレーション モードを開始します。
ステップ 4	**ip address trusted authenticate** 例： `Router(conf-voi-serv)# ip address trusted authenticate`	電話ハッカーの侵入阻止サポートのため、着信H.323またはSIP トランク コールの IP アドレス認証を有効にします。 IPアドレス信頼リスト認証は、デフォルトで有効になっています。「**no ip address trusted list authenticate**」コマンドを使用すると、IPアドレスの信頼できるリスト認証を無効にできます。
ステップ 5	**ip-address trusted call-block cause code** 例： `Router(conf-voi-serv)#ip address trusted call-block cause call-reject`	着信コールがIPアドレス信頼認証に対して拒否された場合に原因コードを発行します。 （注） IPアドレス信頼認証に失敗した場合は、着信 VoIP コールを切断するために call-reject (21) 原因コードが発行されます。
ステップ 6	**end** 例： `Router()# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的

ステップ 7	**show ip address trusted list**
	例：
	`Router#show ip address trusted list`
	`IP Address Trusted Authentication`
	`Administration State: UP`
	`Operation State: UP`
	
	`IP Address Trusted Call Block Cause: call-reject (21)`
		着信 H.323 または SIP トランクコールの有効な IP アドレスのリスト、拒否された着信通話の通話ブロックの原因を確認します。

例

ルータ #**show ip address trusted list**

```
IP Address Trusted Authentication
Administration State: UP
Operation State: UP

IP Address Trusted Call Block Cause: call-reject (21)

VoIP Dial-peer IPv4 and IPv6 Session Targets:
Peer Tag     Oper State     Session Target
--------     ----------     --------------
4             UP             ipv4:10.65.125.155

Configured IP Address Trusted List:
ipv4 192.168.10.20
ipv4 192.168.10.21
ipv4 192.168.10.22

Dynamic IP Address Trusted List:
ipv4 8.55.0.134 [1]
ipv4 8.55.0.136 [2]
ipv4 8.55.0.213 [1]
```

着信 VoIP 通話用の有効な IP アドレスの追加

始める前に

- セキュアなトランク通話用の Unified Cisco Mobility Express 8.1 以降。

手順の概要

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **ip address trusted list**
5. **ipv4** {*<ipv4 address>* [*<network mask>*]}
6. **end**

7. **show ip address trusted list**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル構成モードを開始します。
ステップ 3	**voice service voip** 例： `Router(config)# voice service voip`	voice service voip コンフィギュレーション モードを開始します。
ステップ 4	**ip address trusted list** 例： `Router(conf-voi-serv)# ip address trusted list`	ip address trusted list モードを開始して、有効な IP アドレスを手動で追加できるようにします。
ステップ 5	**ipv4** {*<ipv4 address>* [*<network mask>*]} 例： `Router(cfg-iptrust-list)#ipv4 192.168.10.20`	**ip address trusted list** で最大 100 の IPv4 アドレスの追加を許可します。IP アドレス信頼リスト内で IP アドレスの重複は許可されません。 • （オプション）*network mask* ーサブネット IP アドレスを定義します。
ステップ 6	**end** 例： `Router(cfg-iptrust-list)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show ip address trusted list** 例： `Router# show ip address trusted list`	着信 H.323 または SIP トランク コール用の有効な IP アドレスのリストを表示します。

例

次の例は、信頼できる IP アドレスとして構成された 3 個の IP アドレスを示しています。

```
Router#show ip address trusted list
IP Address Trusted Authentication
```

```
 Administration State: UP
 Operation State:      UP

IP Address Trusted Call Block Cause: call-reject (21)

IP Address Trusted List:
ipv4 192.168.10.20
ipv4 192.168.10.21
ipv4 192.168.10.22
```

着信 ISDN 通話用のダイヤルイン方式（DID）の構成

始める前に

- direct-inward-dial isdn は、着信 ISDN オーバーラップ ダイヤル コール用としてサポートされません。

手順の概要

1. **enable**
2. **configure terminal**
3. **voice service pots**
4. *direct-inward-dial isdn*
5. **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	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル構成モードを開始します。

ステップ 3	**voice service pots**
	例：
	`Router(config)# voice service pots`
	`Router(conf-voi-serv)#`
		音声電話サービス カプセル化タイプ（POTS）で音声サービス コンフィギュレーション モードを開始します。

ステップ 4	*direct-inward-dial isdn* 例： `Router(conf-voi-serv)#direct-inward-dial isdn`	着信 ISDN 番号に対するダイヤル イン（DID）を有効にします。着信 ISDN（一括ダイヤル）コールは、番号が DID トランクから受信されたように処理されます。着信者番号は、発信ダイヤルピアの選択に使

	コマンドまたはアクション	目的
		用されます。ダイヤルトーンは発信者側に聞こえません。
ステップ 5	**exit** 例： `Router(conf-voi-serv)# exit`	voice service pots コンフィギュレーション モードを終了します。

例

```
!
voice service voip
 ip address trusted list
 ipv4 172.19.245.1
 ipv4 172.19.247.1
 ipv4 172.19.243.1
 ipv4 171.19.245.1
 ipv4 171.19.10.1
 allow-connections h323 to h323
 allow-connections h323 to sip
 allow-connections sip to h323
 allow-connections sip to sip
 supplementary-service media-renegotiate
 sip
 registrar server expires max 120 min 120
!
!
dial-peer voice 1 voip
 destination-pattern 5511...
 session protocol sipv2
 session target ipv4:1.3.45.1
 incoming called-number 5522...
 direct-inward-dial
 dtmf-relay sip-notify
 codec g711ulaw
!
dial-peer voice 100 pots
 destination-pattern 91...
 incoming called-number 2...
 forward-digits 4
!
```

アナログおよびデジタル FXO ポートでセカンダリダイヤルトーンをブロック

手順の概要

1. **enable**
2. **configure terminal**
3. **voice-port**
4. *no secondary dialtone*
5. **end**

6. **show run**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル構成モードを開始します。
ステップ 3	**voice-port** 例： `Router(config)#voice-p 2/0/0`	音声ポート コンフィギュレーション モードを開始します。 • アナログまたはデジタル FXO ポート番号を入力します。
ステップ 4	*no secondary dialtone* 例： `Router((config-voiceport)# no secondary dialtone`	アナログおよびデジタル FXO ポートでセカンダリダイヤルトーンをブロックします。
ステップ 5	**end** 例： `Router(conf-voiceport)# exit`	特権 EXEC モードに戻ります。
ステップ 6	**show run** 例： `Router# show run | sec voice-port 2/0/0`	特定の音声ポートでセカンダリダイヤルトーンが無効化されていることを確認します。

例

```
Router# conf t
Router(config)#voice-p 2/0/0
Router(config-voiceport)# no secondary dialtone
!
end

Router# show run | sec voice-port 2/0/0
Foreign Exchange Office 2/0/0 Slot is 2, Sub-unit is 0, Port is 0
 Type of VoicePort is FXO
 Operation State is DORMANT
 Administrative State is UP
 ...
 Secondary dialtone is disabled
```

電話ハッカーの侵入阻止のトラブルシューティングのヒント

着信 VOIP 通話が IP アドレス信頼認証によって拒否される場合は、特定の内部エラー コード（IEC）**1.1.228.3.31.0** が通話履歴レコードに保存されます。IEC サポートを使用すると、失敗したコールまたは拒否されたコールをモニタできます。拒否されたコールをモニタするには、次の手順を実行します。

ステップ 1 **show voice iec description** コマンドを使用すると、IEC コードのテキスト説明を検索できます。

例：

```
Router# show voice iec description 1.1.228.3.31.0
    IEC Version: 1
    Entity: 1 (Gateway)
    Category: 228 (User is denied access to this service)
    Subsystem: 3 (Application Framework Core)
    Error: 31 (Toll fraud call rejected)
    Diagnostic Code: 0
```

ステップ 2 **voice statistics type iec** コマンドを使用して、IEC 静的情報を表示します。次の例は、電話ハッカーの侵入コール拒否エラー コードのために、2 コールが拒否されたことを示しています。

例：

```
Router(config)#voice statistics type iec
Router(config)#end
Router#show voice statistics iec since-reboot
Router#show voice statistics iec since-restart

Internal Error Code counters
----------------------------
Counters since reboot:
  SUBSYSTEM Application Framework Core [subsystem code 3]
      [errcode  31] Toll fraud call rejected
```

ステップ 3 **enable IEC syslog** コマンドを使用して、IEC エラーがある通話が終了した際に記録された syslog メッセージを確認します。

例：

```
Router# Enable iec syslog
Router (config)#voice iec syslog

Feb 11 01:42:57.371: %VOICE_IEC-3-GW: Application Framework Core:
Internal Error (Toll fraud call rejected): IEC=1.1.228.3.31.0 on
callID 288 GUID=DB3F10AC619711DCA7618593A790099E
```

ステップ 4 **show call history voice last** コマンドを使用して、着信 VOIP 通話の送信元アドレスを確認します。

例：

```
Router# show call history voice last 1

GENERIC:
SetupTime=3306550 ms
Index=6
...
```

```
InternalErrorCode=1.1.228.3.31.0
...
RemoteMediaIPAddress=1.5.14.13
...
```

ステップ 5 IEC は Radius Accounting Stop レコードの VSA に保存されます。外部 RADIUS サーバを使用して、拒否されたコールをモニタできます。

例：

```
Feb 11 01:44:06.527: RADIUS:   Cisco AVpair       [1] 36
"internal-error-code=1.1.228.3.31.0"
```

ステップ 6 IEC の詳細を cCallHistoryIec MIB オブジェクトから取得します。IEC の詳細については、『Cisco IOS 音声トラブルシューティングおよびモニタリングガイド』を参照してください。

例：

```
getmany 1.5.14.10 cCallHistoryIec
cCallHistoryIec.6.1 = 1.1.228.3.31.0
>getmany 172.19.156.132 cCallHistory
cCallHistorySetupTime.6 = 815385
cCallHistoryPeerAddress.6 = 1300
cCallHistoryPeerSubAddress.6 =
cCallHistoryPeerId.6 = 8000
cCallHistoryPeerIfIndex.6 = 76
cCallHistoryLogicalIfIndex.6 = 0
cCallHistoryDisconnectCause.6 = 15
cCallHistoryDisconnectText.6 = call rejected (21)
cCallHistoryConnectTime.6 = 0
cCallHistoryDisconnectTime.6 = 815387
cCallHistoryCallOrigin.6 = answer(2)
cCallHistoryChargedUnits.6 = 0
cCallHistoryInfoType.6 = speech(2)
cCallHistoryTransmitPackets.6 = 0
cCallHistoryTransmitBytes.6 = 0
cCallHistoryReceivePackets.6 = 0
cCallHistoryReceiveBytes.6 = 0
cCallHistoryReleaseSrc.6 = internalCallControlApp(7)
cCallHistoryIec.6.1 = 1.1.228.3.31.0

>getone 172.19.156.132 cvVoIPCallHistoryRemMediaIPAddr.6
cvVoIPCallHistoryRemMediaIPAddr.6 = 1.5.14.13
```

電話ハッカーの侵入阻止の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *2:* 電話ハッカーの侵入阻止の機能情報

機能名	**Cisco Unified Cisco Mobility Express** のバージョン	機能情報
回線側 Unified Cisco Mobility Express での電話料金詐欺防止	12.6	Unified Cisco Mobility Express の 回線側エンドポイントに対して電話料金詐欺防止サポートが導入されました。
Cisco Unified CME の電話ハッカーの侵入阻止	8.1	電話ハッカーの侵入阻止機能のサポートが導入されました。

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。