電話ハッカーの侵入阻止の設定

このモジュールでは、Cisco Unified Communications Manager Express（Cisco Unified CME）の電話ハッカーの侵入阻止機能について説明します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、「電話ハッカーの侵入阻止の機能情報」（P.526）を参照してください。

プラットフォームのサポートおよび Cisco IOS および Catalyst OS 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 には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

内容

電話ハッカーの侵入阻止設定の前提条件

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

電話ハッカーの侵入阻止について

Cisco Unified CME 8.1 では、電話ハッカーの侵入阻止機能が拡張され、無許可のユーザによる潜在的な電話の不正利用から Cisco Unified CME システムが保護されます。Cisco Unified CME における電話ハッカーの侵入阻止のための機能拡張は次のとおりです。

- IP アドレス信頼認証
- 着信 ISDN コールに対するダイヤル イン
- 一致するダイヤルピアのない ISDN コールの切断
- 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

IP アドレス信頼認証

IP アドレス信頼認証プロセスは、無許可のコールをブロックし、無許可のユーザによる潜在的な電話の不正利用から Cisco Unified CME システムを保護するために役立ちます。Cisco Unified CME では、デフォルトで **IP アドレス信頼認証**がイネーブルになっています。IP アドレス信頼認証がイネーブルになっている場合、Cisco Unified CME は着信 VoIP コールのリモート IP アドレスがシステム **IP アドレス信頼リスト**から正常に検証されたときのみ着信 VoIP（SIP/H.323）コールを受け入れます。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。詳細については、「着信 VoIP コール用の IP アドレス信頼認証の設定」（P.514）を参照してください。

Cisco Unified CME は着信 VOIP コールのリモート IP アドレスを検証するために **IP アドレス信頼リスト**を維持します。Cisco Unified CME は VoIP ダイヤルピアの IPv4 セッション ターゲットを保存して、信頼できる IP アドレスを **IP アドレス信頼リスト**に自動的に追加します。IPv4 セッション ターゲットは、動作中の VoIP ダイヤルピアのステータスが「アップ」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。信頼できる IP アドレスのリストに定義可能な IPv4 アドレスの数は最大 10050 個です。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 アドレスの手動による追加の詳細については、「着信 VoIP コール用の有効な IP アドレスの追加」（P.517）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 エラー メッセージは、voice iec syslog オプションがイネーブルの場合に 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
```

Cisco Unified CME に「ゲートウェイ」が定義され、「session-target ras」が設定された VoIP ダイヤルピアの動作ステータスがアップとなっている場合は、**IP アドレス信頼リスト**認証を一時停止する必要があります。その場合、着信 VOIP コール ルーティングはゲートキーパーによって制御されます。表 48 に、各種のトリガー条件における管理状態と動作状態を示します。

表 48　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	動作状態
ip address trusted authenticate がイネーブル。	ダウン	ダウン
「ゲートウェイ」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 ダイヤルピアの動作状態が「アップ」	アップ	ダウン
ip address trusted authenticate がイネーブルで、「ゲートウェイ」が定義されていないか、セッション ターゲットとして「ras」が設定された VoIP ダイヤルピアの動作状態が「アップ」でない	アップ	アップ

（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）をイネーブルにする前に SIP 認証をイネーブル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 CME 8.1 以降のバージョンでは、着信 ISDN コールに対する電話ハッカーの侵入阻止のために、**direct-inward-dial isdn** 機能がイネーブルにされています。選択した一般電話サービス（POTS）ダイヤルピアで **direct-inward-dial** オプションがディセーブルにされていても、着信 ISDN 一括ダイヤル コールの着信番号が、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コールのセットアップ用に選択されていない場合、着信 ISDN コールは原因コード「unassigned-number (1)」で切断されます。着信 ISDN コールに対するダイヤル インの詳細については、「着信 ISDN コールに対するダイヤル インの設定」（P.519）を参照してください。

一致するダイヤルピアのない ISDN コールの切断

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。Cisco Unified CME および音声ゲートウェイは、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 コール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には、**dial-peer no-match disconnect-cause** コマンドを使用して着信 ISDN コールを切断します。

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 CME および音声ゲートウェイは、FXO コールを原因コード「unassigned-number (1)」で切断します。Cisco Unified CME はデフォルトで FXO 音声ポートから **no secondary dialtone** コマンドを使用して、アナログまたはデジタル FXO ポートで 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 ポートでのセカンダリ ダイヤル トーンのブロッ

ク」（P.521）を参照してください。

電話ハッカーの侵入阻止の設定方法

ここでは、次の作業について説明します。

着信 VoIP コール用の IP アドレス信頼認証の設定

前提条件

- Cisco Unified CME 8.1 以降のバージョン。

制約事項

- IP アドレス信頼認証は、着信 SIP コールが SIP 電話機から発信された場合はスキップされます。
- 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 コールでは、IP アドレス信頼認証が「アップ」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。

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. 終了
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 モードをイネーブルにします。 • 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 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	**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 アドレス認証をイネーブルにします。 IP アドレス信頼リスト認証は、デフォルトでイネーブルになっています。「**no ip address trusted list authenticate**」コマンドを使用すると、IP アドレス信頼リスト認証がディセーブルになります。
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。

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、拒否された着信コールのコール ブロック原因を確認します。

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)

VoIP Dial-peer IPv4 Session Targets:
Peer Tag        Oper State      Session Target
--------        ----------      --------------
11              DOWN            ipv4:1.3.45.1
1               UP              ipv4:1.3.45.1

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 172.19.245.0 255.255.255.0''
```

着信 VoIP コール用の有効な IP アドレスの追加

前提条件

- Cisco Unified CME 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 list**
5. **ipv4** *ipv4 address network mask*
6. 終了
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 モードをイネーブルにします。 • 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 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	**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`
	`Router(cfg-iptrust-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(config)#voice service voip`
	`Router(conf-voi-serv)#ip taddress trusted list`
	`Router(cfg-iptrust-list)#ipv4 172.19.245.1`
	`Router(cfg-iptrust-list)#ipv4 172.19.243.1`
		ip address trusted list で最大 100 個の IPv4 アドレスを追加できます。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。
		• （任意）*network mask*：サブネット IP アドレスを定義できます。

	コマンドまたはアクション	目的
ステップ 6	**end** **例：** `Router(config-register-pool)# 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 shared-line`	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 アドレスとして設定された 4 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)

VoIP Dial-peer IPv4 Session Targets:
Peer Tag        Oper State      Session Target
--------        ----------      --------------
11              DOWN            ipv4:1.3.45.1
1               UP              ipv4:1.3.45.1

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
```

着信 ISDN コールに対するダイヤル インの設定

着信 ISDN コールに対してダイヤル インを設定するには、次の手順を実行します。

制約事項

- 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. 終了

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 モードをイネーブルにします。 • 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 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	**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）をイネーブルにします。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 ポートでのセカンダリ ダイヤル トーンのブロック

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 トーンをブロックするには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **voice-port**
4. **no secondary dialtone**
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 モードをイネーブルにします。 • 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 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	**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 トーンがディセーブルに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 コールが 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** がコール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** コマンドを使用して、IEC コードのテキスト説明を見つけます。

```
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 **Enable iec statistics** コマンドを使用して、IEC 統計情報を表示します。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# Enable iec statistics
Router(config)#voice statistics type iec
Router#show voice statistics iec since-reboot
Internal Error Code counters
----------------------------
Counters since reboot:
  SUBSYSTEM Application Framework Core [subsystem code 3]
      [errcode  31] Toll fraud call rejected                  2
```

ステップ 3 **enable IEC syslog** コマンドを使用して、IEC エラー付きでコールが解放されたときに記録された 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 コール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、ttp://www.cisco.com/en/US/docs/ios/voice/monitor/configuration/guide/vt_voip_err_cds_ps6350_TSD_Products_Configuration_Guide_Chapter.html 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
```

その他の関連資料

ここでは、Virtual Route Forwarding に関する関連資料について説明します。

関連資料

関連項目	参照先
Cisco Unified CME の設定	• *『Cisco Unified Communications Manager Express System Administrator Guide』* • *『Cisco Unified Communications Manager Express Command Reference』*
Cisco IOS の音声設定	• *『Cisco IOS Voice Configuration Library』* • *『Cisco IOS Voice Command Reference』*
Cisco Unified CME 用の電話機のマニュアル	• *『User Documentation for Cisco Unified IP Phones』*

標準

Standard	タイトル
この機能によってサポートされる新しい標準または変更された標準はありません。またこの機能による既存標準のサポートに変更はありません。	—

MIB

MIB	MIB リンク
新しい MIB または変更された MIB はサポートされていません。また、既存の MIB に対するサポートに変更はありません。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs/

RFC

RFC	タイトル
新しい RFC または変更された RFC はサポートされていません。また、既存の RFC に対するサポートに変更はありません。	—

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

電話ハッカーの侵入阻止の機能情報

表 49 に、この機能のリリース履歴を示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

プラットフォームのサポートおよびソフトウェア 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 を使用すると、Cisco IOS および Catalyst OS ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator にアクセスするには、http://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。

（注） 表 49 に、特定の Cisco IOS ソフトウェア リリース トレインの中で特定の機能のサポートが導入された Cisco IOS ソフトウェア リリースだけを示します。その機能は、特に断りがない限り、それ以降の一連の Cisco IOS ソフトウェア リリースでもサポートされます。

表 49　Virtual Route Forwarding の機能情報

機能名	Cisco Unified CME のバージョン	機能情報
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。