Unified Communications Manager Express 電話ハッカーの侵入阻止

内容

概要

このドキュメントでは、Cisco Communications Manager Express（CME）システムを保護し、通話料金の不正の脅威を軽減するために使用できる設定について説明します。CME は、ユニファイド コミュニケーションの実装を望む組織のための、スマートかつ簡単で安全なソリューションを実現するシスコのルータベース コール制御ソリューションです。このドキュメントで説明しているセキュリティ対策を実行して、セキュリティ制御のレベルを向上し、通話料金不正の可能性を減らすことを強く推奨します。

このドキュメントの目的は、シスコ音声ゲートウェイと CME で使用できるさまざまなセキュリティ ツールについての知識や情報を提供することです。これらのツールを CME システムで実装

して、内部および外部の利用者による不正通話の脅威を軽減することができます。

このドキュメントでは、さまざまな通話料金セキュリティおよび機能制限ツールで CME システムを設定する方法を説明します。また、特定の導入で特定のセキュリティ ツールが使用される理由の概要も示します。

Cisco の ISR プラットフォームの全体的な固有の柔軟性により、さまざまなタイプの導入で CME を導入できます。したがって、CME のロックダウンのために、このドキュメントで説明する機能の組み合わせを使用することが必要となる場合があります。このドキュメントは、CME へのセキュリティ ツールの適用方法のガイドラインとして使用できますが、内部および外部の利用者による通話料金不正や不正使用が発生しないことを保証するものではありません。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Unified Communications Manager Express

使用するコンポーネント

このドキュメントの情報は、Cisco Unified Communications Manager Express 4.3 および CME 7.0 に基づいています。

注：Cisco Unified CME 7.0には、Cisco Unified Communicationsのバージョンに合わせて7.0に番号が変更されたCisco Unified CME 4.3と同じ機能が含まれています。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

概要

このドキュメントでは、通話料金不正の脅威を軽減するために CME システムで使用できる最も一般的なセキュリティ ツールについて説明します。このドキュメントが参照する CME セキュリティ ツールには、通話料金制限ツールと機能制限ツールがあります。

通話料金制限ツール

- ダイヤルイン
- 時間外の通話料金制限
- 制限クラス

- H.323/SIP トランクのアクセスを制限するアクセス リスト

機能制限ツール

- 転送パターン
- 転送パターンのブロック
- 最大転送時間
- 最大コール転送時間
- ローカル コールの転送禁止
- auto-reg-ephone 禁止

Cisco Unity Express 制限ツール

- Cisco Unity Express PSTN アクセスの保護
- メッセージ通知制限

コール ロギング

- 呼詳細レコード（CDR）をキャプチャするコール ロギング

内部および外部の脅威

このドキュメントでは、内部および外部の利用者からの脅威について説明します。内部利用者には、CME システムにある IP Phone ユーザが含まれます。外部利用者には、ホスト CME を使用して、不正なコール発信や受信側の CME システムへの課金を試みる可能性がある外部システムのユーザが含まれます。

通話料金制限ツール

ダイヤルイン

概要

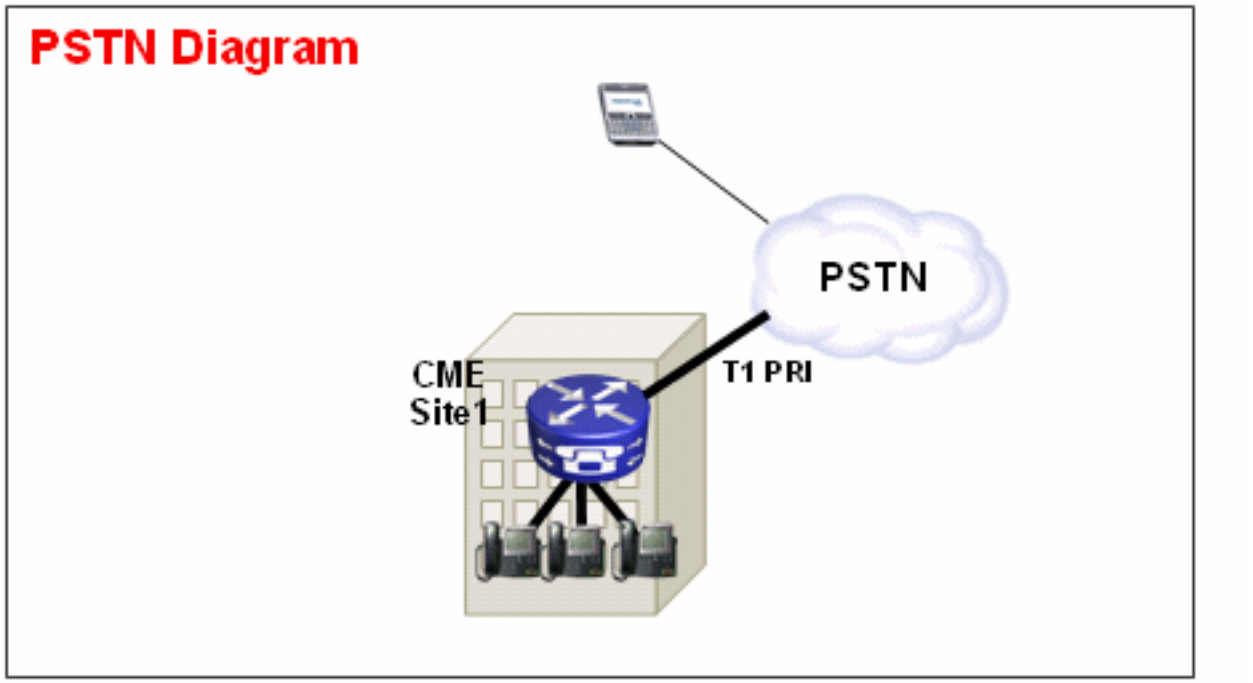
シスコ音声ゲートウェイではダイヤルイン（DID）が使用され、PBX または CO スイッチから番号を受信した後にゲートウェイが着信コールを処理できます。DID が有効な場合、シスコ ゲートウェイは発信者に対してセカンダリ ダイヤル トーンを再生せず、追加の番号が発信者から収集されるまで待機しません。ゲートウェイはコールを直接、着信番号識別サービス（DNIS）に一致する宛先に転送します。 これを 1 段階ダイヤリングと呼びます。

注：これは外部の脅威**です**。

問題の説明

シスコ ゲートウェイと CME のどちらでもダイヤルインが設定されていない場合は、CO または PBX からシスコ ゲートウェイにコールが着信するたびに、発信者に対してセカンダリ ダイヤル トーンが再生されます。これは、2 ステージ ダイヤリングと呼びます。PSTN 発信者に対してセカンダリ ダイヤル トーンが再生された後は、発信者は番号を入力して、内線番号を呼び出すこと

ができます。また、PSTN アクセス コードを知っている場合は、長距離や国際電話の番号をダイヤルできます。このため、PSTN 発信者が CME システムを使用して、長距離通話または国際通話を発信し、その料金が企業に請求されるという問題が発生します。



例 1

サイト 1 で CME は、T1 PRI トランクを介して PSTN に接続されています。PSTN のプロバイダーは、CME サイト 1 の **40855512.**.CMEサイト1のDID範囲。したがって、4085551200 ~ 4085551299宛てのPSTNコールはすべてCMEへの着信にルーティングされます。システムで**ダイヤルインを設定していない場合は、着信 PSTN 発信者にセカンダリ ダイヤル トーンが再生され、この発信者は、手動で内線番号をダイヤルする必要があります。**より大きな問題は、発信者が不正使用者であり、システムの PSTN アクセス コード (一般的には 9) を知っている場合は、**9 をダイヤルした後、目的のあらゆる宛先の番号をダイヤルできることです。**

解決策 1

この脅威を軽減するには、**ダイヤルイン**を設定する必要があります。これにより、シスコ ゲートウェイによって、着信 DNIS に一致する宛先への着信コールが直接転送されます。

サンプル コンフィギュレーション

```
dial-peer voice 1 pots
port 1/0:23
incoming called-number .
direct-inward-dial
```

DID が正常に機能するように、**direct-inward-dial コマンドが設定されている正しい POTS ダイヤル ピアと着信コールが必ず照合されるようにします。**この例では、T1 PRIがポート1/0:23に接続されています。正しい着信ダイヤルピアを照合するには、DID POTSダイヤルピアの下で **incoming called-number** dial peerコマンドを発行します。

例 2

サイト 1 で CME は、T1 PRI トランクを介して PSTN に接続されています。PSTNプロバイダー

は**40855512..**と**40855513..**CMEサイト1のDID範囲。したがって、4085551200 ~ 4085551299および4085551300 ~ 4085551399宛てのPSTNコールはすべて、CMEへの着信にルーティングされます。

誤った設定：

このセクションの設定例のように着信ダイヤル ピアを設定した場合は、通話料金不正の可能性が残ります。この着信ダイヤルピアの問題は、**40852512..**への着信コールのみに一致し**て、DIDサービス**を適用することです。PSTNコールが**40852513..**に着信する場合、着信potsダイヤルピアが一致しなく、DIDサービスは適用されません。DID を含む着信ダイヤル ピアが一致しない場合は、デフォルトのダイヤル ピア 0 が使用されます。デフォルトでは DID は、ダイヤルピア 0 上では無効になっています。

サンプル コンフィギュレーション

```
dial-peer voice 1 pots
incoming called-number 40855512..
direct-inward-dial
```

正しい設定

着信ダイヤル ピアで DID サービスを設定する適切な方法を、次の例に示します。

サンプル コンフィギュレーション

```
dial-peer voice 1 pots
port 1/0:23
incoming called-number .
direct-inward-dial
```

デジタル T1/E1 音声ポートの DID の詳細については、「POTS ダイヤル ピア用の DID 設定」を参照してください。

注：DIDの使用は、音声ポートでPrivate-Line Automatic Ringdown(PLAR)が使用されている場合や、着信ダイヤルピアでAuto-Attendant(AA)などのサービススクリプトが使用されている場合は必要ありません。

設定例：PLAR

```
voice-port 1/0
connection-plar 1001
```

設定例：サービス スクリプト

```
dial-peer voice 1 pots
service AA
port 1/0:23
```

時間外の通話料金制限

概要

時間外通話料金の制限は、CME 4.3/7.0 で使用できる新しいセキュリティ ツールです。これにより、時間と日付に基づいて通話料金制限のポリシーを設定できます。特定の時間帯または常に、

事前に定義された番号にユーザがコールを発信できないようにポリシーを設定できます。7 x 24 の時間外コール ブロッキングのポリシーを設定している場合は、一連の番号も制限されます。内部ユーザは、これらの番号を入力して call-forward all（すべてのコールの転送）を設定できます。

注：これは内部の脅威**です。**

例 1

次の例では、発信コールがブロックされる番号のパターンを定義しています。パターン 1 および 2 では、「1」および「011」で始まる外部番号へのコールが、月曜から金曜の午前 7 時以前と午後 7 時以後、土曜の午前 7 時以前と午後 1 以後、および日曜（1 日中）にブロックされます。パターン 3 では、900 番へのコールが週 7 日、1 日 24 時間にわたってブロックされます。

サンプル コンフィギュレーション

```
telephony-service
after-hours block pattern 1 91
after-hours block pattern 2 9011
after-hours block pattern 3 91900 7-24
after-hours day mon 19:00 07:00
after-hours day tue 19:00 07:00
after-hours day wed 19:00 07:00
after-hours day thu 19:00 07:00
after-hours day fri 19:00 07:00
after-hours day sat 13:00 07:00
after-hours day sun 12:00 12:00
```

通話料金制限の詳細については、「コール ブロッキングの設定」を参照してください。

制限クラス

概要

細かく制御できる通話料金制限が必要な場合は、制限クラス（COR）を使用します。「制限クラス：例」を参照してください。

H.323/SIP トランクの通話料金不正の制限

概要

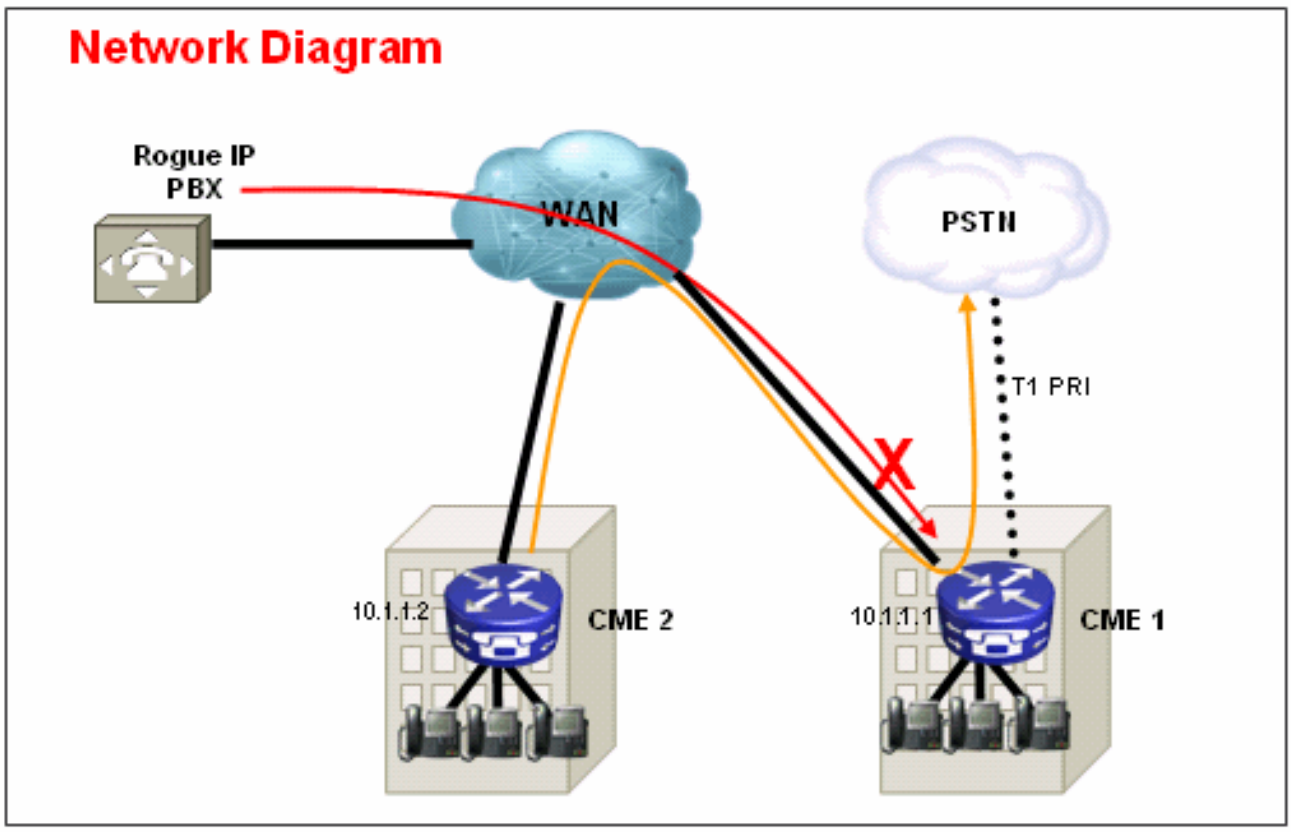
CME システムが WAN で SIP または H.323 トランクを介して他の CME デバイスに接続されている場合は、CME への SIP/H.323 トランク アクセスを制限して、不正使用者がシステムを使用してコールを PSTN に不正に中継することを防止できます。

注：これは外部の脅威**です。**

例 1

この例では、CME 1 に PSTN 接続があります。CME 2 は、H.323 トランクを介して WAN で CME 1 に接続されています。CME 1を保護するには、アクセスリストを設定してWANインターフェイスに着信し、CME 2からのIPトラフィックのみを許可します。これにより、不正なIP

PBXがCME 1経由でPSTNにVoIPコールを送信できなくなります。



解決方法

CME 1 の WAN のインターフェイスが、未知の不正デバイスからのトラフィックを受け入れないようにしてください。暗黙の「deny all」（すべてを拒否）が、アクセス リストの末尾にあることに注意してください。着信 IP トラフィックの発信元として、さらにデバイスを許可する場合は、そのデバイスの IP アドレスを必ずアクセス リストに追加してください。

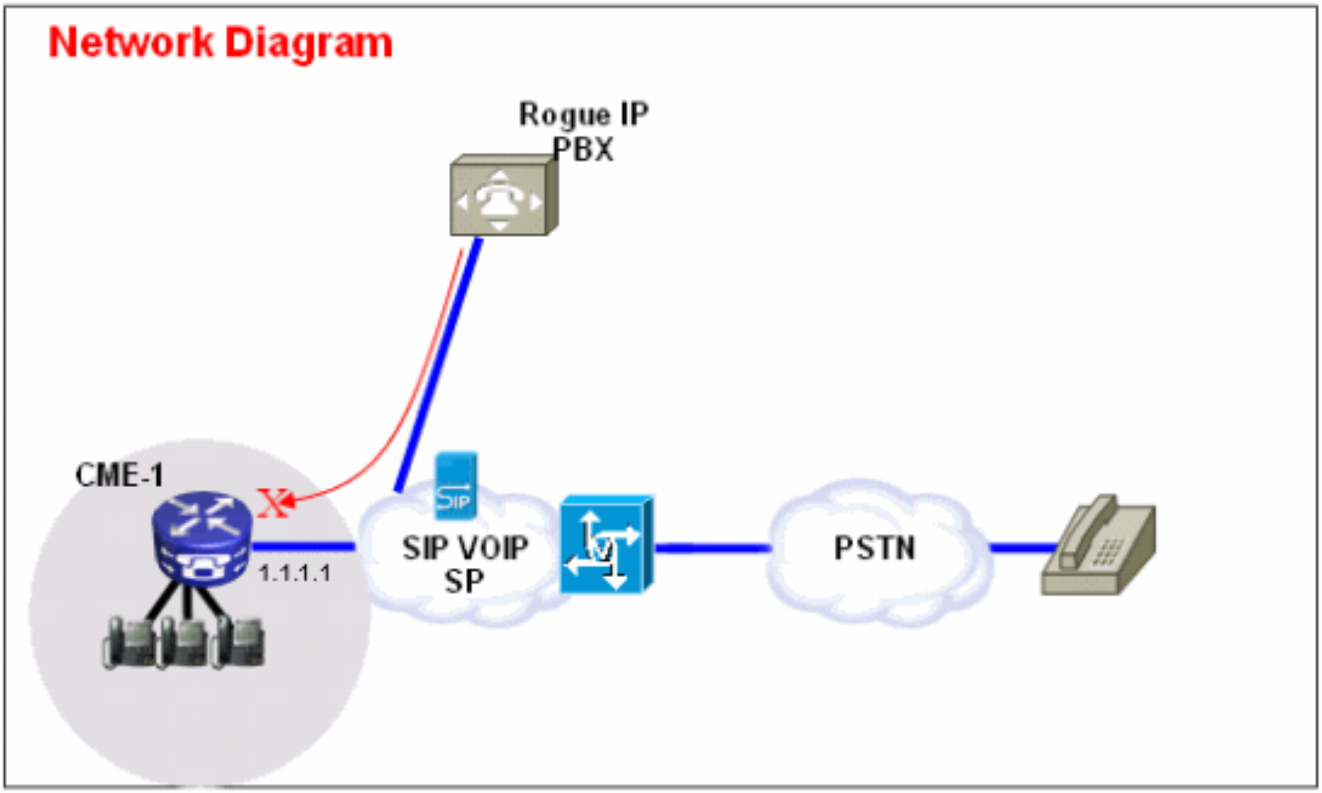
設定例：CME 1

```
interface serial 0/0
  ip access-group 100 in
!
access-list 100 permit ip 10.1.1.2 255.255.255.255 any
```

例 2

この例では、「Cisco CallManager Express（CME）SIP トランキングの設定例」にある例の設定で、CME 1 が PSTN 接続の SIP プロバイダーに接続されています。

CME 1 はパブリック インターネット上にあるため、不正なユーザがパブリック IP アドレスをスキャンして、H.323（TCP 1720）または SIP（UDP または TCP 5060）シグナリング用のよく知られているポートを見つけ、SIP または H.323 メッセージを送信することで SIP トランクから PSTN にコールをルーティングした場合は、*通話料金不正が発生する可能性があります*。この場合の最も一般的な不正は、不正ユーザが SIP または H.323 トランクを介して複数の国際通話を発信し、これらの不正通話の料金を CME 1 の所有者に支払わせることです。このような料金は数千ドルに上る場合もあります。



解決方法

この脅威を軽減するために、複数のソリューションを使用できます。CME 1 への VoIP シグナリング（SIP または H.323）の中に WAN リンクを使用しないものがある場合は、CME 1 のファイアウォール テクニック（アクセス リストまたは ACL）で、できる限りブロックする必要があります。

1. CME 1 の Cisco IOS® ファイアウォールで WAN インターフェイスを保護してください。これは、既知の SIP または H.323 トラフィックだけに、WAN インターフェイスで受信することを許可することを意味します。他のすべての SIP または H.323 トラフィックはブロックされます。このためには、SIP VoIP SP が SIP トランクでのシグナリングに使用する IP アドレスを把握している必要があります。このソリューションでは、ネットワークで使用されるすべての IP アドレスまたは DNS 名を SP が提供することが前提です。また、DNS 名を使用している場合は、設定が、その名前を解決できる DNS サーバが到達可能であることを必要とします。また、SPが終端のアドレスを変更する場合は、CME 1で設定を更新する必要があります。これらの行は、すでにWANインターフェイスに存在するACLエントリに加えて追加する必要があります。設定例：CME 1
```
interface serial 0/0
  ip access-group 100 in
!
access-list 100 permit udp host 1.1.1.254 eq 5060 any
!--- 1.1.1.254 is SP SIP proxy access-list 100 permit udp host 1.1.1.254 any eq 5060
access-list 100 permit udp any any range 16384 32767
```
2. 必ず、SIP トランクで受信するコールがヘアピニングで戻され**ないようにしてください。**これは、特定の既知の PSTN 番号範囲へのコールの SIP - SIP ヘアピニングのみが CME 1 の設定で許可され、他のすべてのコールはブロックされることを意味します。CME 1の内線または自動応答またはボイスメールにマッピングされたSIPトランクに着信するPSTN番号に対して、特定の着信ダイヤルピアを設定する必要があります。CME 1 PSTN番号範囲に含まれない番号への他のすべてのコールはブロックされます。これは、CME 1 のボイスメールへのコール転送（Cisco Unity Express）、および IP Phone から PSTN 番号へのすべてのコ

ールの転送には影響しません。最初のコールは、CME 1 の内線宛てのままであるためです。設定例：CME 1

```
dial-peer voice 1000 voip
  description ** Incoming call to 4085551000 from SIP trunk **
  voice-class codec 1
  voice-class sip dtmf-relay force rtp-nte
  session protocol sipv2
  incoming called-number 4085551000
  dtmf-relay rtp-nte
  no vad
!
dial-peer voice 1001 voip
  permission term
!--- Prevent hairpinning calls back over SIP Trunk. description ** Incoming call from SIP
trunk ** voice-class codec 1 voice-class sip dtmf-relay force rtp-nte session protocol
sipv2 incoming called-number .T
!--- Applies to all other inbound calls. dtmf-relay rtp-nte no vad
```

3. 特定のダイヤル文字列をブロックするには、変換ルールを使用してください。ほとんどの通話料金不正は、国際通話に関連しています。そのため、特定のダイヤル文字列に一致する特定の着信ダイヤル ピアを作成すると、それらへのコールをブロックできます。ほとんどのCMEは、ダイヤルアウトに9などの特定のアクセスコードを使用し、米国の国際ダイヤルコードは011です。したがって、米国でブロックする最も一般的なダイヤル文字列は9011で、その後はSIPトランクに着信します。設定例：CME 1

```
voice translation-rule 1000
 rule 1 reject /^9011/
 rule 2 reject /^91900…….$/
 rule 3 reject /^91976…….$/
!
voice translation-profile BLOCK
translate called 1000
!
dial-peer voice 1000 voip
description ** Incoming call from SIP trunk **
incoming called-number 9011T
call-block translation-profile incoming BLOCK
```

機能制限ツール

転送パターン

概要

ローカル SCCP IP 電話の番号以外のすべての番号への転送は、デフォルトで自動的にブロックされます。設定時に、ローカル以外の番号に転送できるように変更できます。**transfer-pattern コマンドは、Cisco SCCP IP 電話からのテレフォニー コールの、Cisco IP Phone 以外の電話（別の CME システムの外部 PSTN コールまたは電話など）への転送を許可するために使用されます。transfer-pattern を使用して、内線番号宛てのコールだけ、または特定のエリア コードの PSTN 番号宛てだけにコールを制限することができます。**次の例は、transfer-pattern コマンドを使用して、さまざまな番号にコールを制限する方法を示します。

注：これは内部の脅威**です。**

例 1

408 エリア コードへのコール転送だけをユーザに許可します。この例では、9T の宛先パターンを持つダイヤルピアで CME が設定されていることが前提です。

サンプル コンフィギュレーション

```
telephony-service
transfer-pattern 91408
```

転送パターンのブロック

概要

Cisco Unified CME 4.0 以降のバージョンでは、個々の電話機が、グローバルで転送が有効になっている番号にコールを転送できないようにすることができます。**transfer-pattern blocked コマンドは transfer-pattern コマンドより優先され、POTS または VoIP ダイヤル ピアが到達する必要があるすべての宛先へのコール転送を無効にします。**これには、PSTN 番号、他の音声ゲートウェイ、および Cisco Unity Express が含まれます。これにより、Cisco Unified CME システムの外部にコールが転送された場合に、個々の電話で通話料金が発生することがなくなります。コール転送のブロックは、個々の電話機に対して設定することも、一連の電話機に適用されるテンプレートの一部として設定することもできます。

注：これは内部の脅威**です。**

例 1

この設定例では、ephone 1 が、転送パターン（グローバルに定義された）を使用したコール転送を許可されていないのに対し、ephone 2 は、テレフォニー サービスの下で定義された転送パターンを使用してコールを転送できます。

サンプル コンフィギュレーション

```
ephone-template 1
transfer-pattern blocked
!
ephone 1
ephone-template 1
!
ephone 2
!
```

最大転送時間

概要

transfer max-length コマンドで、コールの転送時にユーザがダイヤルできる最大桁数を指定します。transfer-pattern max-length は transfer-pattern コマンドより優先され、転送先として許可されている最大桁数を指定します。引数は、コールの転送先の番号で許可されている桁数を指定します。範囲：3 ～ 16。デフォルト：16.

注：これは内部の脅威**です。**

例 1

この設定では、この ephone テンプレートを備えており、最大 4 桁の宛先に転送されるように適用されている電話のみが許可されます。

サンプル コンフィギュレーション

```
ephone-template 1
transfer max-length 4
```

最大コール転送時間

概要

IP Phone の CfwdALL ソフト キーで入力できる桁数を制限するには、ephone-dn または ephone-dn-template コンフィギュレーション モードで **call-forward max-length コマンドを使用します。** 入力できる桁数の制限を削除するには、このコマンドの **no 形式を使用します。**

注：これは内部の脅威**です。**

例 1

この例では、ディレクトリ内線 101 が、長さが 1 ~ 4 桁の任意の内線番号にコール転送を実行できます。4 桁を超える長さの宛先へのコール転送は失敗します。

サンプル コンフィギュレーション

```
ephone-dn  1  dual-line
number 101
call-forward max-length 4
```

または

```
ephone-dn-template  1
call-forward max-length 4
```

ローカル コールの転送禁止

概要

no forward local-calls コマンドを ephone-dn コンフィギュレーション モードで使用すると、forward local-calls が適用されていない特定の ephone-dn への内部コールは、ephone-dn がビジーであるか、応答しない場合に転送されません。内部発信者がこの ephone-dn に発信し、ephone-dn がビジーである場合は、発信者にビジー信号が再生されます。内部発信者がこの ephone-dn に発信し、ephone-dn が応答しない場合は、発信者にリングバック信号が再生されます。内部コールは、コール転送が ephone dn に対して有効になっていても転送されません。

注：これは内部の脅威**です。**

例 1

この例では、内線番号 2222 が内線番号 3675 をコールし、リングバックまたはビジー信号が再生されます。外部発信者が内線番号 3675 に到達したが、応答がない場合は、コールが内線番号

4000 に転送されます。

サンプル コンフィギュレーション

```
ephone-dn  25
number 3675
no forward local-calls
call-forward noan 4000 timeout 30
```

CME システムでの自動登録の無効化

概要

auto-reg-ephone が SCCP CME システムのテレフォニー サービスの下で有効になっている場合は、システムに接続されている新しい IP Phone が自動登録されます。また、自動的に内線番号を割り当てるように auto assign が設定されている場合、新しい IP Phone はただちに発信することができます。

注：これは内部の脅威**です。**

例 1

この設定では、ephone を手動で追加して CME システムに登録し、それを使用して IP テレフォニー コールを発信する必要があるように、新しい CME システムが設定されます。

解決方法

テレフォニー サービスの下で **no auto-reg-ephone を無効にして、CME システムに接続されている新しい IP Phone が CME システムに自動登録されないようにすることができます。**

サンプル コンフィギュレーション

```
telephony-service
no auto-reg-ephone
```

例 2

SCCP CME を使用し、Cisco SIP 電話機をシステムに登録する予定である場合は、SIP エンドポイントがユーザ名とパスワードで認証する必要があるようにシステムを設定してください。そのためには、次のように設定します。

```
voice register global
 mode cme
 source-address 192.168.10.1 port 5060
 authenticate register
```

SIP CME の総合的な設定ガイドについては、「SIP：Cisco Unified CME のセットアップ」を参照してください。

Cisco Unity Express 制限ツール

Cisco Unity Express のセキュリティ：AA PSTN アクセス

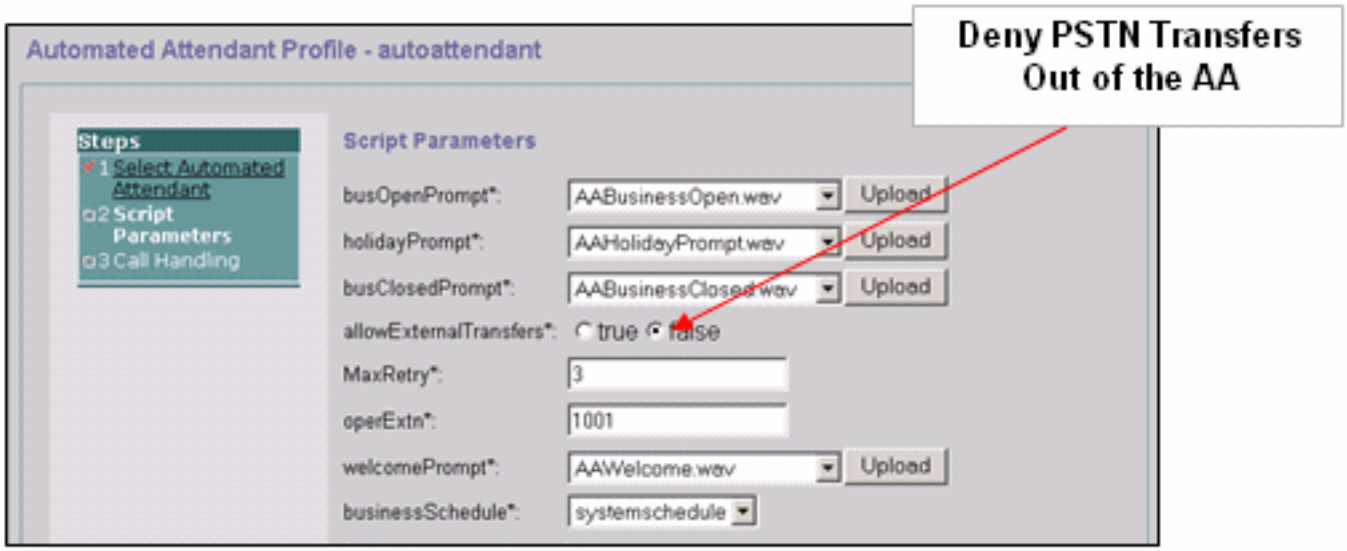
概要

着信コールが Cisco Unity Express の自動アテンダント（AA）に転送されるようにシステムを設定すると、Cisco Unity Express の AA から PSTN への外部転送を無効にすることが必要になる場合があります。こうすると、外部ユーザは、Cisco Unity Express の AA に到達した後に外線番号に発信できなくなります。

注：これは外部の脅威**です。**

注： 解決方法

注：Cisco Unity Express GUIで**allowExternalTransfers**オプションを無効にします。



注：AAからのPSTNアクセスが必要な場合は、スクリプトで有効と見なされる番号または番号の範囲を制限します。

Cisco Unity Express 規制テーブル

概要

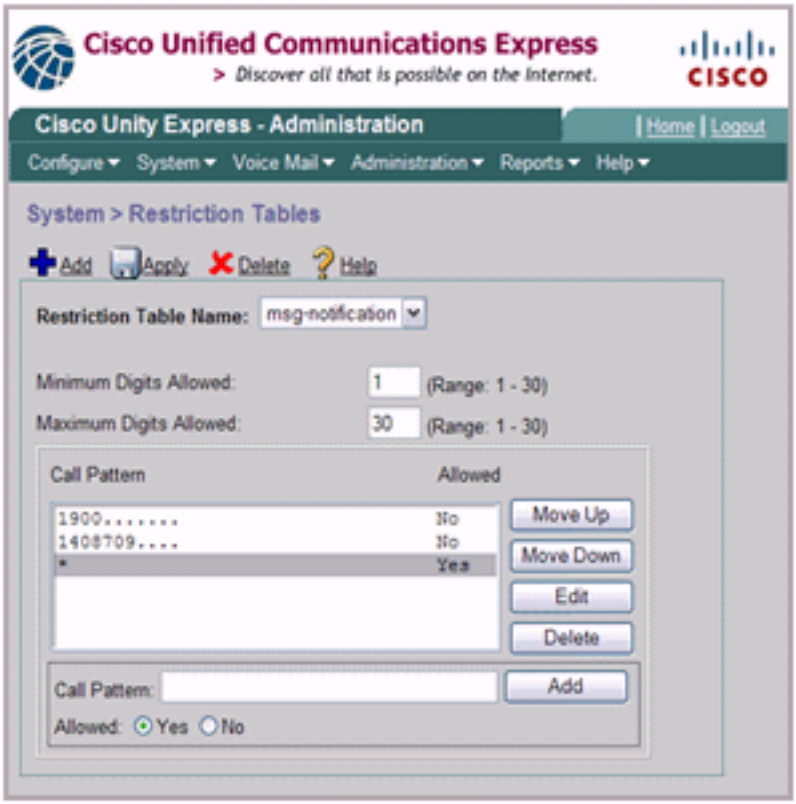
Cisco Unity Express 規制テーブルを使用すると、Cisco Unity Express からの発信時に到達可能な宛先を制限できます。Cisco Unity Express 規制テーブルは、コールを発信する Cisco Unity Express システムでの通話料金不正や悪意のある使用を防ぐために使用できます。Cisco Unity Express 規制テーブルを使用する場合は、ワイルド カード照合のためのコール パターンを指定できます。Cisco Unity Express 規制テーブルを使用するアプリケーションは次のとおりです。

- ファクス
- Cisco Unity Express Live Reply
- Message Notification
- Non-Subscriber Message Delivery

注：これは内部の脅威**です。**

解決方法

発信の外部コールで Cisco Unity Express が到達可能な宛先パターンを制限するために、Cisco Unity Express GUI で、[System] > [Restrictions Tables] **の [Call Pattern] を設定します。**



コール ロギング

拡張 CDR

CME システムを設定して、拡張 CDR をキャプチャし、ルータ フラッシュまたは外部 FTP サーバに CDR のログを記録することができます。これらのレコードを使用してコールを再トレースし、内部または外部利用者による不正使用が発生しているかどうかを確認することができます。

Cisco IOS Release 12.4(15) XY の CME 4.3/7.0 で導入されたファイル アカウンティング機能により、カンマ区切り値（.csv）形式のアカウンティング レコードをキャプチャし、内部フラッシュまたは外部 FTP サーバのファイルにレコードを保存することができます。これで、ゲートウェイのアカウンティング サポートが拡張されます。また、アカウンティング情報のロギングの AAA および syslog メカニズムも含まれます。

アカウンティング処理では、シスコ音声ゲートウェイで作成された各コール レッグのアカウンティング データが収集されます。この情報は、課金レコードの生成などの後処理アクティビティおよびネットワーク解析に使用できます。シスコ音声ゲートウェイは、シスコが定義した属性を含む呼詳細レコード（CDR）の形式でアカウンティング データをキャプチャします。ゲートウェイは、RADIUS サーバや syslog サーバに CDR を送信でき、新しいファイル方式を使用して .csv 形式でフラッシュまたは FTP サーバに送信できます。

拡張 CDR 機能の詳細については、「CDR の例」を参照してください。

関連情報

- Cisco Unified Communications Manager Express のセキュリティのベスト プラクティス
- Cisco Communications Manager Express アドミニストレータ ガイド
- Cisco Communications Manager Express アドミニストレータ ガイド - コール ブロッキング
- IOS プラットフォームでのダイヤル ピア照合について
- 音声変換プロファイルを使用した番号変換
- CME ソリューション レファレンス ネットワーク設計ガイド
- テクニカル サポートとドキュメント – Cisco Systems