電話のセキュリティ強化

この章では、電話機のセキュリティ強化について説明します。電話のセキュリティを強化するタスクは、[Unified Communications Manager Administration] の **[Phone Configuration]** ウィンドウで行います。

Gratuitous ARP の無効化

デフォルトでは、 Cisco Unified IP 電話 s は ARP パケットを受け入れます。デバイスが使用する Gratuitous ARP パケットは、ネットワークにデバイスの存在を公表するために使用されます。ただし、攻撃者はこれらのパケットを使用して、有効なネットワークデバイスをスプーフィングすることができます。たとえば、攻撃者は、デフォルトルータであると主張するパケットを送信する可能性があります。これを選択した場合は、[**電話の設定 (Phone Configuration)**] ウィンドウで、無償 ARP を無効にすることができます。

（注） この機能を無効にしても、電話機がデフォルトルータを特定することはできません。

Web アクセスの無効化

電話の Web サーバ機能を無効にすると、統計および設定情報を提供する電話内部の Web ページへのアクセスがブロックされます。Cisco Quality Report Tool などの機能は、電話の Web ページに

アクセスしないと正しく動作しません。また、Web サーバを無効にすると、CiscoWorks など、Web アクセスに依存するサービスアビリティ アプリケーションにも影響します。

Web サービスが無効になっているかどうかを確認するために、電話機は設定ファイルのパラメータを解析して、サービスが無効になっているか、有効になっているかを示します。Web サービスが無効になっている場合、電話機はモニタリング目的で HTTP ポート80を開かず、電話機の内部 web ページへのアクセスをブロックします。

PC 音声 VLAN へのアクセスの無効化

デフォルトでは、Cisco IP 電話 はスイッチ ポート（上流に位置するスイッチに面したポート）で受信したすべてのパケットを PC ポートに転送します。[Phone Configuration] ウィンドウの [PC Voice VLAN Access] 設定を無効にすると、PC ポートから受信した音声 VLAN 機能を使用するパケットはドロップされます。さまざまな Cisco IP 電話 がそれぞれ異なる方法でこの機能を使用しています。

- Cisco Unified IP 電話 7942 と 7962 は、PC ポートで送受信される、音声 VLAN のタグが付いたパケットをドロップします。

アクセスの無効化の設定

デフォルトでは、Cisco IP 電話 の [Applications] ボタンを押すと、電話の設定情報を含むさまざまな情報にアクセスできます。[Phone Configuration] ウィンドウで [Setting Access] パラメータ設定を無効にすると、通常は電話の [Applications] ボタンを押すと表示されるすべてのオプション（[Contrast]、[Ring Type]、[Network Configuration]、[Model Information]、[Status] などの設定）へのアクセスが拒否されます。

Unified Communications Manager Administration 内の設定を無効にすると、以前の設定は電話に表示されません。この設定を無効にすると、電話ユーザは [音量 (Volume)] ボタンに関連付けられている設定を保存できません。たとえば、ユーザはボリュームを保存できません。

この設定を無効にすると、現在のコントラスト、呼出音タイプ、ネットワーク設定、モデル情報、ステータス、および電話機に存在するボリューム設定が自動的に保存されます。これらの電話機設定を変更するには、Unified Communications Manager Administration で [設定へのアクセス（Setting Access）] 設定を有効にします。

PC ポートのディセーブル化

デフォルトでは、Unified Communications Manager は PC ポートを備えているすべての Cisco IP 電話 で PC ポートを有効にします。これを選択した場合は、[電話の設定 (Phone Configuration)] ウィンドウで [PC ポート (PC Port)] 設定を無効にすることができます。PC ポートを無効にすると、ロビーまたは会議室の電話機で役立ちます。

（注） PCポートは一部の電話機で使用でき、ユーザは電話機にコンピュータを接続できます。この接続方法は、ユーザが 1 つの LAN ポートだけを必要とすることを意味します。

電話のセキュリティ強化の設定

電話のセキュリティ強化は、接続のセキュリティを強化するために電話機に適用できるオプションの設定で構成されています。次の 3 つの設定ウィンドウのいずれかを使用して設定を適用できます。

- 電話の設定 - [電話の設定（Phone Configuration）] ウィンドウを使用して、個々の電話に設定を適用します。
- 共通の電話プロファイル - [共通の電話プロファイル（Common Phone Profile）] ウィンドウを使用して、このプロファイルを使用するすべての電話機に設定を適用します。
- 企業電話 - [企業電話（Enterprise Phone）] ウィンドウを使用して、企業全体のすべての電話機に設定を適用します。

（注） これらの各ウィンドウに競合する設定が表示される場合、電話が正しい設定を判断するために使用する優先順位は次のとおりです。1) 電話の設定、2) 共通の電話プロファイル、3) 企業電話。

電話のセキュリティ強化を設定するには、次の手順を実行します。

手順

Step 1 Cisco Unified Communications Manager Administrationから、**[デバイス（Device）]** > **[電話（Phone）]** を選択します。

Step 2 電話機の検索条件を指定して **[検索（Find）]** をクリックし、すべての電話機を表示します。

Step 3 デバイス名をクリックします。

Step 4 次の製品固有のパラメータを見つけます。

a) [PC ポート（PC Port）]
b) [設定アクセス（Settings Access）]
c) [無償 ARP（Gratuitous ARP）]
d) [PC の音声 VLAN へのアクセス（PC Voice VLAN Access）]
e) [Web アクセス（Web Access）]

ヒント これらの設定の情報を確認するには、**[電話の設定 (Phone Configuration)]** ウィンドウのパラメータの横に表示される [ヘルプ (help)] アイコンをクリックします。

Step 5 無効にする各パラメータのドロップダウンリストから、[**無効 (Disabled)**] を選択します。スピーカフォンまたはスピーカフォンとヘッドセットを無効にするには、対応するチェックボックスをオンにします。

Step 6 [保存（Save）] をクリックします。

Step 7 [リセット（Reset）] をクリックします。

関連トピック

電話機のセキュリティ強化に関する詳細情報の入手先, on page 4

電話機のセキュリティ強化に関する詳細情報の入手先

関連トピック

Gratuitous ARP の無効化, on page 1
Web アクセスの無効化, on page 1
PC 音声 VLAN へのアクセスの無効化, on page 2
アクセスの無効化の設定, on page 2
PC ポートのディセーブル化, on page 2