電話のセキュリティ強化

この章では、電話のセキュリティの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 （1 ページ）
- Web アクセスの無効化 （1 ページ）
- PC 音声 VLAN へのアクセスの無効化 （2 ページ）
- 設定へのアクセスの無効化 （2 ページ）
- PC ポートの無効化 （2 ページ）
- 電話のセキュリティ強化の設定 （3 ページ）
- 電話のセキュリティの強化に関する詳細情報の入手先 （3 ページ）

Gratuitous ARP の無効化

Cisco Unified IP Phone は、デフォルトでは Gratuitous 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 デバイスのスプーフィングを行えます。たとえば、デフォルトルータであると主張するパケットを攻撃者が送信する可能性があります。必要な場合、[Phone Configuration] ウィンドウで Gratuitous ARP を無効化できます。

（注） この機能を無効にしても、電話がデフォルト ルータを特定できなくなることはありません。

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 サービスが無効であるかどうかを確認するため、電話は、サービスの無効/有効を示す設定ファイル内のパラメータを解析します。Web サービスが無効な場合、電話は HTTP ポート 80 をモニタリング用に開かず、電話内部 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 Phone 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 Phone 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 Phone 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。
- Cisco Unified IP Phone 7970G は、PC ポートで送受信される、VLAN で 802.1Q のタグが含まれるすべてのパケットをドロップします。

設定へのアクセスの無効化

デフォルトでは、Cisco IP Phone 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 [Volume] ボタンに関連した設定を保存できません。たとえば、ユーザは音量の設定を保存できません。

この設定を無効にすると、電話の既存の [Contrast]、[Ring Type]、[Network Configuration]、[Model Information]、[Status]、および [Volume] の現在の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 ポートの無効化

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 Phone で PC ポートを有効にします。必要な場合、[Phone Configuration] ウィンドウで [PC Port] 設定を無効にできます。PC ポートの無効化は、ロビーや会議室の電話の場合に役立ちます。

（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を強化するには、PC ポート、設定へのアクセス、Gratuitous ARP、PC 音声 VLAN へのアクセス、電話機の Web アクセスなどの機能を無効にします。

このような電話機の機能を無効にするには、次の手順を実行します。

手順

ステップ 1 Unified Communications Manager Administrationで、**[デバイス（Device）]** > **[電話機（Phone）]** を選択します。

ステップ 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。

ステップ 3 デバイス名をクリックします。
[電話の設定（Phone Configuration）] ウィンドウが表示されます。

ステップ 4 次の製品固有のパラメータを見つけます。

a) PC Port
b) Settings Access
c) Gratuitous ARP
d) PC Voice VLAN Access
e) Web Access

ヒント これらの設定に関する情報を確認するには、**[電話の設定（Phone Configuration）]** ウィンドウで各種パラメータの横に表示されているヘルプアイコンをクリックします。

ステップ 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。スピーカーフォン、またはスピーカー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。

ステップ 6 **[保存（Save）]** をクリックします。

ステップ 7 [リセット（Reset）] をクリックします。

電話のセキュリティの強化に関する詳細情報の入手先

電話のセキュリティの強化に関する詳細情報の入手先