



# アナログエンドポイントに対する暗号化の設定

この章では、アナログエンドポイントの設定への暗号化について説明します。この機能を使用すると、アナログ電話のセキュアな SCCP 接続を Cisco VG2xx ゲートウェイに作成できます。ゲートウェイは SCCP シグナリング通信に Unified Communications Manager で Transport Layer Security (TLS) を使用し、音声通信には SRTP を使用します。証明書の管理などの既存の Unified Communications Manager TLS 機能が、セキュアな SCCP 通信に使用されます。

- [アナログ電話セキュリティプロファイル \(1 ページ\)](#)
- [セキュアなアナログ電話の証明書管理 \(1 ページ\)](#)

## アナログ電話セキュリティプロファイル

アナログ電話への暗号化された接続を確立するには、デバイスセキュリティモードのパラメータを [認証済み (Authenticated)] または [暗号化 (encrypted)] に設定したアナログ電話の電話セキュリティプロファイルを作成する必要があります。電話セキュリティプロファイルを作成するには、[Unified Communications Manager Administration] で、[System] > [Security Profile] > [Phone Security Profile] に移動します。

Cisco VG2xx ゲートウェイに接続されているアナログ電話を設定する場合は、[Device Security Profile] パラメータで、作成したセキュアなアナログプロファイルを選択します。[Device Security Profile] パラメータを設定するには、[Unified Communications Manager Administration] で [Device] > [Phone] に移動し、設定を行う電話の [Protocol Specific Information] セクションまでスクロールします。

関連トピック

[電話セキュリティプロファイルの設定](#)

## セキュアなアナログ電話の証明書管理

セキュアなアナログ電話を機能させるために、Cisco VG2xx によって使用されているのと同じ CA 署名付き証明書を Cisco Unified Communications Manager にインポートする必要があります。証明

書のインポートの詳細については、『*Administration Guide for Cisco Unified Communications Manager*』の第6章「**Security**」を参照してください。