# Cisco IP 電話のセキュリティ


- ドメインおよびインターネットの設定 （1 ページ）
- SIP INVITE メッセージのチャレンジの設定 （5 ページ）
- RFC-8760 のサポート （6 ページ）
- INVITE の認証と再同期-再起動の認証の有効化 （6 ページ）
- ホテリング認証へのダイジェストアルゴリズム追加のサポート （7 ページ）
- TLS 最小値の制御 （7 ページ）
- Webex のメトリクスサービスを有効にする （9 ページ）
- サービスラッシュ時の PRT アップロード制御を有効にする （10 ページ）
- トランスポート レイヤ セキュリティ （11 ページ）
- HTTPS プロビジョニング （14 ページ）
- ファイアウォールを有効にする （17 ページ）
- 追加のオプションを使用してファイアウォールを設定する （19 ページ）
- 暗号リストを設定する （21 ページ）
- SIP over TLS のホスト名検証を有効化する （24 ページ）
- メディアプレーンセキュリティネゴシエーションの顧客開始モードを有効にする （25 ページ）
- 802.1X 認証 （28 ページ）
- プロキシサーバーをセットアップする （37 ページ）
- FIPS モードの有効化 （44 ページ）
- シスコ製品のセキュリティの概要 （45 ページ）


# ドメインおよびインターネットの設定

## 制限付きアクセス ドメインを構成する

指定されたサーバのみを使用して登録、プロビジョニング、ファームウェアアップグレード、およびレポートを送信するように、電話機を設定することができます。 指定されたサーバを使用しない登録、プロビジョニング、アップグレード、およびレポートは、電話機では実行でき

ません。使用するサーバを指定する場合は、以下のフィールドに入力するサーバがリストに含まれていることを確認してください。

- **プロビジョニング**タブ上の**プロファイルルール**、**プロファイルルール B**、**プロファイルルール C**、および**プロファイルルール D**
- **プロビジョニング**タブ上の**アップグレードルール**および **Cisco ヘッドセットアップグレードルール**
- **プロビジョニング**タブ上の**レポートルール**
- **プロビジョニング**タブ上の**カスタム CA ルール**
- **内線（n）**タブ上の**プロキシ**および**アウトバウンドプロキシ**

### 始める前に

電話機 ウェブインターフェイスへのアクセス.

### 手順

**ステップ 1** **[音声（Voice）]** > **[システム（System）]** を選択します。

**ステップ 2** **システム設定**セクションで、**制限付きアクセスドメイン**フィールドを見つけ、各サーバーの完全修飾ドメイン名（FQDN）を入力します。 FQDN はカンマで区切ります。

**例：**

```
voiceip.com, voiceip1.com
```

次の形式で文字列を入力することによって、設定ファイル(cfg.xml)でこのパラメータを設定することができます。

```
<Restricted_Access_Domains ua="na">voiceip.com, voiceip1.com</Restricted_Access_Domains>
```

**ステップ 3** [すべての変更の送信（Submit All Changes）]をクリックします。

# DHCP オプションを設定する

電話機が DHCP オプションを使用する順序を設定することができます。 DHCP オプションのヘルプについては、DHCP オプションのサポート （4 ページ）を参照してください。

### 始める前に

電話機 ウェブインターフェイスへのアクセス.

手順

**ステップ 1** **[音声（Voice）]** > **[プロビジョニング（Provisioning）]** を選択します。

**ステップ 2** **設定プロファイル** セクションで、DHCPオプション設定のパラメータ （3 ページ）表の説明に従って、**使用するDHCPオプション**と **使用するDHCPv6オプション** を設定します。

**ステップ 3** [すべての変更の送信（Submit All Changes）]をクリックします。

## DHCPオプション設定のパラメータ

次の表は、電話機のウェブインターフェイスの音声>プロビジョニングタブの下にある設定プロファイルセクションにおけるDHCPオプション設定のパラメータの機能と使用方法を定義しています。 また、パラメータを設定するために、XML (cfg.xml) コードを含む電話構成ファイルに追加される文字列のシンタックスも定義します。

**表 *1 : DHCP*オプション設定のパラメータ**

| パラメータ | 説明 |
|---|---|
| [使用するDHCPオプション（DHCP Option To Use）] | ファームウェアおよびプロファイルを取得するために使用される、コンマで区切られた DHCP オプション。<br>次のいずれかを実行します。<br>• XML (cfg.xml)を使用した電話機の設定ファイルでは、次の形式で文字列を入力します。<br>`<DHCP_Option_To_Use ua="na">66,160,159,150,60,43,125</DHCP_Option_To_Use>`<br>• 電話機のウェブページで、DHCP オプションをコンマで区切って入力します。<br>**例**：66,160,159,150,60,43,125<br>デフォルト：66,160,159,150,60,43,125 |

| パラメータ | 説明 |
| --- | --- |
| [使用するDHCPv6オプション（DHCPv6 Option To Use）] | ファームウェアおよびプロファイルを取得するために使用される、コンマで区切られた DHCPv6 オプション。<br>次のいずれかを実行します。<br>• XML (cfg.xml)を使用した電話機の設定ファイルでは、次の形式で文字列を入力します。<br>`<DHCPv6_Option_To_Use ua="na">17,160,159</DHCPv6_Option_To_Use>`<br>• 電話機のウェブページで、DHCP オプションをコンマで区切って入力します。<br>**例**：17,160,159<br>デフォルト：17,160,159 |

## DHCP オプションのサポート

次の表に、複数の電話機でサポートされている DHCP オプションを表示します。

| ネットワーク標準規格 | 説明 |
| --- | --- |
| DHCP オプション 1 | サブネット マスク（Subnet mask） |
| DHCP オプション 2 | タイム オフセット |
| DHCP オプション 3 | ルータ |
| DHCP オプション 6 | ドメイン ネーム サーバ |
| DHCP オプション 15 | ドメイン名（Domain Name） |
| DHCP オプション 41 | IP アドレスのリース期間 |
| DHCP オプション 42 | NTP サーバ |
| DHCP オプション 43 | ベンダー固有の情報<br>TR.69 自動コンフィギュレーション サーバ（ACS）の検出に使用できます。 |
| DHCP オプション 56 | NTP サーバ<br>IPv6 を使用した NTP サーバの構成 |
| DHCP オプション 60 | ベンダー クラス ID |
| DHCP オプション 66 | TFTP サーバ名 |

| ネットワーク標準規格 | 説明 |
|---|---|
| DHCP オプション 125 | ベンダー識別ベンダー固有の情報<br>TR.69 自動コンフィギュレーション サーバ（ACS）の検出に使用できます。 |
| DHCP オプション 150 | TFTP サーバ（TFTP server） |
| DHCP オプション 159 | プロビジョニング サーバ IP |
| DHCP オプション 160 | プロビジョニング URL |

# SIP INVITE メッセージのチャレンジの設定

セッションでSIP INVITE（初期化）メッセージにチャレンジするように電話を設定できます。チャレンジは、サービス プロバイダー ネットワーク上でデバイスとの相互作用が許可されるSIP サーバを制限します。 これにより、電話機に対する悪意のある攻撃を防ぐことができます。 有効に設定した場合、SIP プロキシからの初期の着信 INVITE リクエストに認証が必要になります。

XML（cfg.xml）コードを使用して電話機構成ファイルのパラメータを設定することもできます。

### 始める前に

電話機 ウェブインターフェイスへのアクセス.

### 手順

**ステップ 1** **[音声（Voice）]** > **[内線（n）（Ext(n)）]** を選択します。ここで、n は内線番号です。

**ステップ 2** **[SIP 設定 (SIP Settings)]**セクションで、**[認証 INVITE（Auth INVITE）]** リストから **[はい（Yes）]** を選択してこの機能を有効にするか、**[いいえ（No）]** を選択して無効にします。

次の形式で文字列を入力することによって、設定ファイル(cfg.xml) でこのパラメータを設定することができます。

```
<Auth_INVITE_1>Yes</Auth_INVITE_1_>
```

デフォルト：**いいえ(No)**

**ステップ 3** [すべての変更の送信（Submit All Changes）]をクリックします。

# RFC-8760 のサポート

RFC-3261 を置き換えて、RFC-8760 で指定される追加の認証ダイジェストアルゴリズムのサポートを追加できます。 RFC-8760 は、SHA256、SHA-512/256、MD5 などのダイジェストアルゴリズムを指定します。 RFC-8760 を使用すると、電話機は認証ヘッダーフィールドなしで SIP REGISTER または INVITE または SUBSCRIBE 要求を送信します。 SIP サーバーは、www-authenticate または proxy-authenticate ヘッダーフィールドを使用して 401/407 ステータスコードに応答します。 SIP サーバーは、複数の www-authenticate ヘッダーで応答します。 複数のヘッダーが送信される場合、それぞれが異なるアルゴリズムを持つ必要があり、最も優先されるアルゴリズムが先頭になります。 RFC-8760 のサポートは、RFC-3261 に比べて利点があります。次の表に、さまざまなシナリオを示します。

| 手順 | SIP 要求の方向 | RFC-3261 | RFC-8760 |
|---|---|---|---|
| ステップ 1 | 電話機から SIP サーバー | 電話機は、認証なしで SIP 要求を送信します。 | 電話機は、認証なしで SIP 要求を送信します。 |
| ステップ 2 | SIP サーバーから電話機 | SIP サーバーは、MD5 アルゴリズムで 1 つの www-authenticate を使用して 401 ステータスに応答します。 | SIP サーバーは、異なるアルゴリズム（SHA-256、SHA-512-256、MD5）で 1 つまたは複数の www-authenticate を使用して 401 ステータスに応答します。 |
| ステップ 3 | 電話機から SIP サーバー | 電話機が、要求の送信、および MD5 アルゴリズムでの認証ヘッダーの追加を再試行します。 | 電話機が、要求の送信、および最も上位のヘッダーフィールド（SHA-256）を使用した認証の追加を再試行します。 |
| ステップ 4 | SIP サーバーから電話機 | SIP サーバーが認証を検証します。 | SIP サーバーが認証を検証します。 |

# INVITE の認証と再同期-再起動の認証の有効化

RFC 8760 を使用して電話の認証を有効にできます。

### 始める前に

- 電話管理の Web ページにアクセスします。 電話機 ウェブインターフェイスへのアクセスを参照してください。
- **[SIP の設定（SIP Settings）]** セクションで **[INVITE の認証（Auth Invite）]** が **[はい（Yes）]** に設定されていること。

手順

**ステップ 1** **[音声（Voice）]** > **[内線（n）（Ext(n)）]** を選択します。ここで、n は内線番号です。

**ステップ 2** **[SIP 設定（SIP Settings）]** セクションで、**[RFC8760 サポート認証（Auth Support RFC8760）]** リストから **[はい（Yes）]** を選択します。

**[はい（Yes）]** を選択すると、電話認証は RFC 8760 をサポートします。**[いいえ（No）]** を選択すると無効になります。

次の形式で文字列を入力することによって、設定ファイル(cfg.xml) でこのパラメータを設定することができます。

```
<Auth_Support_RFC8760>Yes</Auth_Support_RFC8760/>
```

デフォルト: **[いいえ（No）]**

**ステップ 3** [すべての変更の送信（Submit All Changes）]をクリックします。

# ホテリング認証へのダイジェストアルゴリズム追加のサポート

ホテリング認証に RFC 8760 のサポートが追加されました。 この機能をサポートするために、SHA-256、SHA-512、および SHA-256 ダイジェストアルゴリズムが電話に追加されます。 これまでは、MD5 アルゴリズムのみがサポートされていました。

# TLS 最小値の制御

TLS パラメータを使用して、電話機の最小 TLS 値を制御できます。 設定すると、TLS クライアントと TLS サーバ間のネゴシエーションに最小 TLS バージョンが使用されます。

クライアントとサーバの TLS の最小バージョンをそれぞれ 1.0、1.1、1.2 などに設定できます。

### 始める前に

- 電話管理のウェブページにアクセスします。 電話機 ウェブインターフェイスへのアクセスを参照してください。

手順

**ステップ 1** **[音声（Voice）]** > **[システム（System）]**を選択します。

**ステップ 2** **[セキュリティ設定]**セクションで、**[TLS クライアントの最小バージョン]**リストから TLS バージョンを選択します。

- **TLS 1.0**: TLS クライアントは、TLS のバージョン 1.0 から 1.2 をサポートします。

  サーバの TLS バージョンが 1.0 未満の場合、接続を確立できません。

- **TLS 1.1**: TLS クライアントは TLS 1.1 および 1.2 をサポートします。

  サーバの TLS バージョンが 1.1 未満の場合、接続を確立できません。

- **TLS 1.2** (デフォルト): TLS クライアントは TLS 1.2 のみをサポートします。

  サーバの TLS バージョンが 1.2 未満の場合、接続を確立できません。

次の表に、TLS クライアント最小値の結果を簡単に示します。

| TLS クライアントの最小バージョン | サーバの TLS バージョン | 結果 |
|---|---|---|
| TLS 1.0 | TLS 1.0 | TLS 1.0 |
| | TLS 1.1 | TLS 1.1 |
| | TLS 1.2 | TLS 1.2 |
| TLS 1.1 | TLS 1.0 | プロトコルアラート |
| | TLS 1.1 | TLS 1.1 |
| | TLS 1.2 | TLS 1.2 |
| TLS 1.2 | TLS 1.0 | プロトコルアラート |
| | TLS 1.1 | プロトコルアラート |
| | TLS 1.2 | TLS 1.2 |

次の形式で文字列を入力することによって、設定ファイル(cfg.xml)でこのパラメータを設定することができます。

```
<TLS_Client_Min_Version ua="na">TLS 1.2</TLS_Client_Min_Version>
```

デフォルト値: **TLS 1.2**

（注）
この機能は、SIP over TLS、XMPP、E911 Geolocation、Wifi など、電話によって開始されるほとんどの TLS クライアントに適用されています。

**ステップ 3** **TLS サーバの最小バージョン** リストから TLS バージョンを選択します。 ユーザは、電話に接続するために TLS をサポートする HTTPS クライアントを使用する必要があります。

- **TLS 1.1**: TLS サーバは TLS 1.1 および 1.2 をサポートしています。

  クライアントの TLS バージョンが 1.1 未満の場合、接続を確立できません。

- **TLS 1.2** (デフォルト): TLS サーバは TLS 1.2 のみをサポートします。

  クライアントの TLS バージョンが 1.2 未満の場合、接続を確立できません。

次の表に、TLS サーバー最小値の結果を簡単に示します。

| TLS サーバの最小バージョン | クライアントの TLS バージョン | 結果 |
|---|---|---|
| TLS 1.1 | TLS 1.0 | プロトコルアラート |
| | TLS 1.1 | TLS 1.1 |
| | TLS 1.2 | TLS 1.2 |
| TLS 1.2 | TLS 1.0 | プロトコルアラート |
| | TLS 1.1 | プロトコルアラート |
| | TLS 1.2 | TLS 1.2 |

次の形式で文字列を入力することによって、設定ファイル(cfg.xml)でこのパラメータを設定することができます。

```
<TLS_Server_Min_Version ua="na">TLS 1.2</TLS_Server_Min_Version>
```

デフォルト値: **TLS 1.2**

**ステップ 4** [すべての変更の送信（Submit All Changes）]をクリックします。

# Webex のメトリクスサービスを有効にする

メトリクスを有効にすると、すべてのメトリクスサービスの電話制御が可能になります。

### 始める前に

- 電話管理の Web ページにアクセスします。 電話機 ウェブインターフェイスへのアクセスを参照してください。

### 手順

**ステップ 1** **[音声（Voice）]** > **[電話（Phone）]** を選択します

**ステップ 2** **[Webex]** セクションの **[メトリクス有効化（Metrics Enable）]** リストで、**[はい（Yes）]** を選択します。

**[はい（Yes）]** を選択すると、すべてのメトリクス メッセージの送信が電話によって制御されます。 **[いいえ（No）]** を選択すると、制御が無効になります。

次の形式で文字列を入力することによって、設定ファイル(cfg.xml)でこのパラメータを設定することができます。

```
<Webex_Metrics_Enable ua="na">Yes</Webex_Metrics_Enable>
```

デフォルト: **[いいえ（No）]**

**ステップ 3** [すべての変更の送信（Submit All Changes）]をクリックします。

# サービスラッシュ時の PRT アップロード制御を有効にする

電話がクラッシュした場合に、PRT パッケージをサーバに自動的にアップロードするかどうかを指定できます。

### 始める前に

- 電話管理の Web ページにアクセスします。 電話機 ウェブインターフェイスへのアクセスを参照してください。

### 手順

**ステップ 1** **[音声（Voice）]** > **[プロビジョニング（Provisioning）]** を選択します。

**ステップ 2** **[（Problem Report Tool）]** セクションで、**[クラッシュ時に PRT をアップロード（PRT Upload at Crash）]** から **[はい（Yes）]** を選択します。

**[はい（Yes）]** を選択すると、電話はクラッシュ処理の自動アップロードを制御します。 **[いいえ（No）]** を選択すると、制御が無効になります。

次の形式で文字列を入力することによって、設定ファイル(cfg.xml)でこのパラメータを設定することができます。

```
<PRT_Upload_at_Crash ua="na">Yes</PRT_Upload_at_Crash>
```

デフォルト: **[いいえ（No）]**

**ステップ 3** [すべての変更の送信（Submit All Changes）]をクリックします。

# トランスポート レイヤ セキュリティ

Transport Layer Security（TLS）は、インターネット上での通信を保護および認証するための標準プロトコルです。 SIP over TLS は、サービス プロバイダーの SIP プロキシとエンド ユーザ間の SIP メッセージシグナリングを暗号化します。

Cisco IP 電話は SIP トランスポート用の標準として UDP を使用しますが、セキュリティ強化のため SIP over TLS もサポートします。

次の表は、2 つの TLS レイヤーを示します。

**表 *2 : TLS* レイヤー**

| Protocol Name | 説明 |
|---|---|
| TLS 録音プロトコル | SIP や TCH などの信頼性の高いトランスポート プロトコルで階層化されたこの層は、接続が対称データ暗号化の使用を通してプライベートであることと、その接続が信頼できることを保証します。 |
| TLS ハンドシェイクプロトコル | サーバと顧客を認証し、アプリケーション プロトコルがデータを送受信する前に暗号化アルゴリズムと暗号キーをネゴシエートします。 |

## SIP Over TLS でシグナリングを暗号化する

SIP over TLS を使用してシグナリングメッセージを暗号化する場合は、追加されたセキュリティを設定できます。

### 始める前に

電話機 ウェブインターフェイスへのアクセス.「トランスポート レイヤ セキュリティ （11 ページ）」を参照。

### 手順

**ステップ 1** **[音声（Voice）] > [内線（n）（Ext(n)）]** を選択します。ここで、n は内線番号です。

**ステップ 2** **[SIP 設定（SIP Settings）]** セクションで、**[SIP トランスポート（SIP Transport）]** リストから **[TLS]** を選択します。

次の形式で文字列を入力することによって、設定ファイル(cfg.xml) でこのパラメータを設定することができます。

```
<SIP_Transport_1_ ua="na">TLS</SIP_Transport_1_>
```

.

使用可能なオプションは次のとおりです。

- UDP
- [TCP]
- TLS
- 自動

デフォルト：**UDP**

**ステップ 3** [すべての変更の送信（Submit All Changes）]をクリックします。

# LDAP over TLS の設定

LDAP over TLS（LDAPS）を設定して、サーバと特定の電話機間の安全なデータ転送を有効にできます。

**注目** シスコでは、認証方式をデフォルト値の **[なし（None）]** のままにしておくことを推奨しています。[サーバ（server）]フィールドの隣は、**[なし（None）]**、**[シンプル（Simple）]**、または **[Digest-MD5]** の値を使用する認証フィールドです。 認証には **[TLS]** の値はありません。 ソフトウェアはサーバ文字列の LDAPS プロトコルから認証方法を決定します。

XML（cfg.xml）コードを使用して電話機構成ファイルのパラメータを設定することもできます。

### 始める前に

電話管理の Web ページにアクセスします。 電話機 ウェブインターフェイスへのアクセスを参照してください。

### 手順

**ステップ 1** **[音声（Voice）]** > **[電話（Phone）]** を選択します。

**ステップ 2** [LDAP] セクションで、サーバ アドレスを [サーバ（Server）] フィールドに入力します。

次の形式で文字列を入力することによって、設定ファイル(cfg.xml) でこのパラメータを設定することができます。

```
<LDAP_Server ua="na">ldaps://10.45.76.79</LDAP_Server>
```

たとえば、`ldaps://<ldaps_server>[:port]` を入力します。

引数の説明

- **`ldaps://`**= サーバーアドレス文字列の開始。

- **Ldaps_server** = IP アドレスまたはドメイン名
- **port** = ポート番号 デフォルト：636

**ステップ 3** [すべての変更の送信（Submit All Changes）]をクリックします。

# StartTLS の設定

電話機と LDAP サーバ間の通信には、開始トランスポートレイヤセキュリティ (StartTLS) を有効にすることができます。セキュリティで保護された通信と安全でない通信の両方に同じネットワークポート (デフォルト 389) を使用します。 LDAP サーバが StartTLS をサポートしている場合、TLS は通信を暗号化します。それ以外の場合は、通信はプレーンテキストになります。

### 始める前に

- 電話管理の Web ページにアクセスします。 電話機 ウェブインターフェイスへのアクセス を参照してください。

### 手順

**ステップ 1** **[音声（Voice）] > [電話（Phone）]** を選択します。

**ステップ 2** [LDAP] セクションで、サーバ アドレスを [サーバ（Server）] フィールドに入力します。

たとえば、`ldap://<ldap_server>[:port]` を入力します。

ここで、

- **ldap://** = URLのスキーム、サーバーアドレス文字列の開始
- **Ldap_server** = IP アドレスまたはドメイン名
- **port** = ポート番号

次の形式で文字列を入力することによって、設定ファイル (cfg.xml) でこのパラメータを設定することができます。

```
<LDAP_Server ua="na">ldap://<ldap_server>[:port]</LDAP_Server>
```

**ステップ 3** **StartTLS 有効**フィールドを**はい**に設定します。

次の形式で文字列を入力することによって、設定ファイル (cfg.xml) でこのパラメータを設定することができます。

```
<LDAP_StartTLS_Enable ua="na">可</LDAP_StartTLS_Enable>
```

**ステップ 4** [すべての変更の送信（Submit All Changes）]をクリックします。

関連トピック

LDAPディレクトリのパラメータ

# HTTPS プロビジョニング

電話機は、リモートに導入されたユニットを管理する際のセキュリティを強化するために、プロビジョニング用に HTTPS をサポートします。 各電話機は、Sipura CA サーバ ルート証明書に加えて、固有の SLL クライアント証明書（および関連付けられた秘密キー）を保持します。ルート証明書を使って、電話機は認証されたプロビジョニング サーバを認識し、認証されていないサーバを拒否できます。 一方、クライアント証明書を使うと、プロビジョニング サーバはリクエストを発行した個々のデバイスを識別できます。

HTTPS を使用して導入を管理するサービス プロバイダーでは、HTTPS を使用した電話機の再同期先となるプロビジョニング サーバごとにサーバ証明書を生成する必要があります。 サーバ証明書はシスコ サーバの CA ルート キーで署名される必要があります。導入済みのすべてのユニットはすべての証明書を保持します。 署名されたサーバ証明書を取得するには、サービス プロバイダーが証明書署名要求をシスコに送信します。シスコはプロビジョニング サーバへのインストール用にサーバ証明書に署名して返送します。

プロビジョニング サーバ証明書には、共通名（CN）フィールドと、対象内でサーバを実行しているホストの FQDN を含める必要があります。 オプションで、ホストの FQDN に続く情報をスラッシュ（/）文字で区切って含めることができます。 次の例は、電話機で有効として受け入れられる CN エントリです。

```
CN=sprov.callme.com
CN=pv.telco.net/mailto:admin@telco.net
CN=prof.voice.com/info@voice.com
```

電話機では、サーバ証明書の検証に加えて、サーバ証明書で指定されたサーバ名の DNS ルックアップに対してサーバ IP アドレスをテストします。

## 署名付きサーバ証明書の取得

OpenSSL ユーティリティで、証明書署名要求を生成できます。 次の例は、1024 ビットの RSA 公開キーと秘密キーのペアおよび証明書署名要求を生成する **openssl** コマンドを示しています。

```
openssl req -new -out provserver.csr
```

このコマンドでは、**privkey.pem** と対応する証明書署名要求 **provserver.csr** にサーバの秘密キーが生成されます。 サービス プロバイダーは、**privkey.pem** 秘密キーを維持し、署名のために **provserver.csr** をシスコに提出します。 **provserver.csr** ファイルを受信すると、シスコは署名付きサーバ証明書 **provserver.crt** を生成します。

## 手順

**ステップ 1** https://software.cisco.com/software/cda/home に移動し、CCO クレデンシャルでログインします。

（注）
電話機を初めてネットワークに接続する場合、または初期設定へのリセット後にネットワークに接続する場合に、セットアップされている DHCP オプションがないと、電話機はゼロ タッチ プロビジョニングのためにデバイス アクティベーション サーバに接続します。 新しい電話機は、プロビジョニングに「webapps.cisco.com」 の代わりに 「activate.cisco.com」 を使用します。 11.2(1) より前のファームウェアを搭載している電話機は、引き続き 「webapps.cisco.com」 を使用します。 ファイアウォールで両方のドメイン名を許可することが推奨されます。

**ステップ 2** [証明書の管理（Certificate Management）]を選択します。

[CSRの署名（Sign CSR）]タブで、前の手順の CSR を署名用にアップロードします。

**ステップ 3** [製品の選択（Select Product）] ドロップダウン リスト ボックスから [SPA1xxファームウェア1.3.3以降（SPA1xx firmware 1.3.3 and newer）]、[SPA232Dファームウェア1.3.3以降（SPA232D firmware 1.3.3 and newer）]、[SPA5xxファームウェア7.5.6以降（SPA5xx firmware 7.5.6 and newer）]、[CP-78xx-3PCC]、および [CP-88xx-3PCC]を選択します。

**ステップ 4** [CSRファイル（CSR File）]フィールドで、[参照（Browse）]をクリックし、署名用に CSR を選択します。

**ステップ 5** 暗号方式を選択します。

- MD5
- SHA1
- SHA256

SHA256 暗号化を選択することが推奨されます。

**ステップ 6** [サインイン期間（Sign in Duration）] ドロップダウン リスト ボックスで、適切な期間（1 年など）を選択します。

**ステップ 7** [証明書の署名要求（Sign Certificate Request）]をクリックします。

**ステップ 8** 署名付き証明書を受信するには、次のいずれかのオプションを選択します。

- [受信者の電子メールアドレスを入力する（Enter Recipient's Email Address）] : 電子メールで証明書を受け取る場合は、このフィールドに電子メール アドレスを入力します。
- [ダウンロード（Download）] : 署名付き証明書をダウンロードする場合は、このオプションを選択します。

**ステップ 9** [送信（Submit）]をクリックします。

署名付きサーバ証明書は、前に指定した電子メールアドレスに送信されるか、ダウンロードされます。

# マルチプラットフォーム フォンの CA クライアント ルート証明書

シスコは、サービス プロバイダーにマルチプラットフォーム フォンのクライアント ルート証明書も提供しています。 このルート証明書により、各電話機で保持されるクライアント証明書が本物であることが証明されます。 マルチプラットフォーム フォンは、Verisign、Cybertrust などで提供される証明書のように、サードパーティの署名付き証明書もサポートします。

電話機が個別の証明書を保持するかどうかを判断するには、$CCERT プロビジョニング マクロ変数を使用します。 変数の値は、固有のクライアント証明書の有無に従って、Installed または Not Installed のいずれかに展開されます。 一般的な証明書の場合は、User-Agent フィールドの HTTP リクエスト ヘッダーからユニットのシリアル番号を取得できます。

HTTPS サーバを設定して、接続しているクライアントに SSL 証明書を要求することができます。 これを有効にすると、サーバは、シスコが提供するマルチプラットフォーム フォンのクライアント ルート証明書を使用してクライアント証明書を検証できます。 その後、サーバは、以降の処理のために証明書情報を CGI に提供できます。

証明書の保存場所はさまざまです。 たとえば、Apache をインストールした場合には、プロビジョニング サーバの署名付き証明書、関連付けられた秘密キー、マルチプラットフォーム フォン CA クライアントのルート証明書を保存するファイル パスは次のようになります。

```
# Server Certificate:
SSLCertificateFile /etc/httpd/conf/provserver.crt

# Server Private Key:
SSLCertificateKeyFile /etc/httpd/conf/provserver.key

# Certificate Authority (CA):
SSLCACertificateFile /etc/httpd/conf/spacroot.crt
```

個別の情報は、HTTPS サーバの資料を参照してください。

シスコのクライアント証明書ルート認証局が、独自の証明書にそれぞれ署名します。 関連するルート証明書が作成され、クライアント認証の目的でサービス プロバイダーがそれを利用できるようになります。

# 冗長プロビジョニング サーバ

プロビジョニング サーバは、IP アドレスまたは完全修飾ドメイン名（FQDN）で指定できます。 FQDN を使用すると、冗長なプロビジョニング サーバの導入が容易になります。 プロビジョニング サーバが FQDN によって識別される場合、電話機は DNS を介して FQDN を IP アドレスに解決しようとします。 プロビジョニングでは DNS A レコードのみサポートされます。 DNS SRV のアドレス解決はプロビジョニングには使用できません。 電話機は、サーバが応答するまで A レコードの処理を続行します。 A レコードの応答にサーバが関連付けられていない場合、電話機は syslog サーバにエラーを記録します。

# syslog サーバ

<Syslog Server> パラメータを使用して syslog サーバを電話機に設定している場合、再同期およびアップグレード操作のメッセージが syslog サーバーに送信されます。 メッセージはリモート ファイル リクエストの開始時（設定プロファイルまたはファームウェアのロード）、および操作の完了時（成功または失敗を示す）に生成できます。

ログに記録されたメッセージは次のパラメータで設定され、実際の syslog メッセージにマクロ展開されます。

# ファイアウォールを有効にする

オペレーティングシステムを強化することにより、電話のセキュリティを改善しました。この強化により、電話機は悪意のある着信トラフィックから保護するファイアウォールを備えています。ファイアウォールは、受信データと送信データのポートを追跡します。予期しないソースからの着信トラフィックが検出されると、アクセスがブロックされます。ファイアウォールはすべての発信トラフィックを許可します。

ファイアウォールは、通常、ブロックされているポートを動的にロック解除します。発信 TCP 接続または UDP フローは、リターントラフィックと継続トラフィックに対するポートのブロックを解除します。フローがアクティブな間、ポートはブロックされていない状態になります。このポートは、フローが停止またはエージングするときに、ブロックされた状態に戻ります。

従来の設定である IPv6 マルチキャスト Ping **音声** > **システム** > **ipv6 設定** > **ブロードキャストエコー**は、新しいファイアウォール設定に関係なく動作し続けます。

通常、ファイアウォール設定の変更によって電話機を再起動することはありません。通常、電話機のソフト再起動はファイアウォール動作に影響しません。

ファイアウォールは、デフォルトでは有効になっています。無効にしている場合は、電話機のウェブページから有効にすることができます。

### 始める前に

電話機 ウェブインターフェイスへのアクセス

### 手順

**ステップ 1** **音声** > **システム** > **セキュリティ設定**を選択します。

**ステップ 2** **ファイアウォール** ドロップダウンリストで、**[有効（Enabled）]** を選択します。

次の形式で文字列を入力することによって、設定ファイル (cfg .xml) でこのパラメータを設定することもできます。

```
<Firewall ua="na">Enabled</Firewall>
```

有効値は、無効|有効です。 デフォルト値は [有効（Enabled）] です。

**ステップ 3** [すべての変更の送信（Submit All Changes）]をクリックします。
これにより、デフォルトで開いている UDP ポートと TCP ポートでファイアウォールが有効になります。

**ステップ 4** ネットワークを以前の動作に戻したい場合は、**[無効（Disabled）]** を選択します。

次の表では、デフォルトのオープン UDP ポートを説明しています。

**表 *3*: ファイアウォールデフォルトのオープン *UDP* ポート**

| デフォルトのオープン UDP ポート | 説明 |
|---|---|
| DHCP/DHCPv6 | DHCP クライアントポート 68<br>DHCPv6 クライアントポート 546 |
| SIP UDP | **[回線の有効化（Line Enable）]** が **[はい（Yes）]** に設定され、**[SIP トランスポート（SIP Transport）]** が **[UDP]** または **[自動（Auto）]** に設定されている場合、**[音声（Voice）]** > **[内線（Ext）]<n>** > **[SIP 設定（SIP Settings）]** > **[SIP ポート（SIP Port）]**（例：5060）でポートを設定します。 |
| RTP/RTCP | **RTP ポートの最小値**から**RTPポートの最大値 + 1** までの UDP ポート範囲 |
| PFS（ピア ファームウェア共有） | **アップグレード有効化**と**ピアファームウェア共有**が **[はい（Yes）]** に設定されている場合、ポート 4051になります。 |
| TFTP クライアント | ポート 53240-53245 リモートサーバーが標準の TFTP ポート 69 以外のポートを使用している場合は、このポート範囲が必要です。サーバーが標準ポート 69 を使用している場合は、これをオフにすることができます。追加のオプションを使用してファイアウォールを設定する （19 ページ）を参照してください。 |
| TR-069 | **TR-069を有効にする** が **[はい（Yes）]** に設定されている場合、UDP/STUN ポート 7999 になります。 |

次の表では、デフォルトのオープン UDP ポートを説明しています。

**表 *4*: ファイアウォールデフォルト オープン *TCP* ポート**

| デフォルトのオープン TCP ポート | 説明 |
|---|---|
| [Webサーバ（Web server）] | **ウェブサーバを有効にする**が **[はい（Yes）]** されている場合、ウェブサーバーポート経由で設定されたポート（デフォルト 80）になります。 |

| デフォルトのオープン TCP ポート | 説明 |
|---|---|
| PFS（ピア ファームウェア共有） | **アップグレード有効化**と**ピアファームウェア共有**の両方が **[はい（Yes）]** に設定されている場合、ポート 4051 および 6970 になります。 |
| TR-069 | **TR-069を有効にする**が **[はい（Yes）]** に設定されている場合、TR-069接続リクエストURLのHTTP/SOAPポートになります。<br>ポートは、範囲 8000-9999 からランダムに選択されます。 |

# 追加のオプションを使用してファイアウォールを設定する

**ファイアウォールオプションオプション**フィールドで、追加オプションを設定することができます。 フィールドの各オプションのキーワードを入力し、キーワードをコンマ (,) で区切ります。 一部のキーワードには値があります。 コロン (:)で値を区切りますます。

### 始める前に

電話機 ウェブインターフェイスへのアクセス

### 手順

**ステップ 1** **音声** > **システム** > **セキュリティ設定**に移動します。

**ステップ 2** **[ファイアウォール（Firewall）]** フィールド **[有効（Enabled）]** に設定します

**ステップ 3** **ファイアウォールオプション** に、キーワードを入力します。 ポートの一覧は、IPv4 プロトコルと IPv6 プロトコルの両方に適用されます。

キーワードを入力する際、

- 各キーワードはカンマ (,)で区切ります。
- キーワード値は、コロン (:)で区切ります。

表 *5:* ファイアウォールのオプション設定

| ファイアウォールオプションのキーワード | 説明 |
|---|---|
| フィールドが空です。 | ファイアウォールは、デフォルトのオープンポートを使用して実行されます。 |
| NO_ICMP_PING | ファイアウォールは、ICMP/ICMPv6 **Echo**リクエスト(Ping)の着信をブロックします。<br>このオプションでは、電話機に対する一部のタイプのトレースルートリクエストを中断する場合があります。 Windows **tracert** はその一例です。<br>オプションの組み合わせを使用した**ファイアウォールオプション**エントリの例を次に示します。<br>NO_ICMP_PING,TCP:12000,UDP:8000:8010<br>ファイアウォールは、デフォルト設定と次の追加オプションで実行されます。<br>• 着信 ICMP/ICMPv6 **Echo** (Ping) リクエストをドロップします。<br>• 着信接続用の TCP ポート 12000 (IPv4 および IPv6) を開きます。<br>• 着信リクエストに対して UDP ポート範囲 8000-8010 (IPv4 および IPv6) を開きます。 |
| NO_ICMP_UNREACHABLE | 電話機は、UDP ポートに対して ICMP および ICMPv6 の宛先到着不可（Destination Unreachable） を送信しません。<br>（注）<br>この例外は、RTP ポート範囲内のポートで、常に宛先到着不可（Destination Unreachable） を送信することです。<br>このオプションでは、電話機に対する一部のタイプの **トレースルート** リクエストを中断する場合があります。 例えば、Linux **トレースルート**が中断する可能性があります。 |
| NO_CISCO_TFTP | • 電話機は、TFTP クライアントのポート範囲 (UDP 53240:53245) を開いていません。<br>• 非標準 (非 69) TFTP サーバポートに対するリクエストは失敗します。<br>• 標準 TFTP サーバポート 69 へのリクエスト。 |

| ファイアウォールオプションのキーワード | 説明 |
|---|---|
| 次のキーワードとオプションは、電話機が着信リクエストを処理するカスタムアプリケーションを実行するときに適用されます。 | |
| UDP:<xxx> | UDP ポート <xxx> を開きます。 |
| UDP:<xxx:yyy> | UDP ポート範囲 <xxx to yyy> を開きます。<br>最大 5 個の UDP ポートオプション (単一のポートとポート範囲) を保持できます。 たとえば、3 つの UDP:<xxx> および 2 つの UDP:<xxx:yyy> を保持することができます。 |
| TCP:<xxx> | TCP ポート <xxx> を開きます。 |
| TCP:<xxx:yyy> | TCP ポート範囲 <xxx to yyy> を開きます。<br>最大 5 個の TCP ポートオプション (単一のポートとポート範囲) を保持できます。 たとえば、4 つの TCP:<xxx> と 1 つの TCP:<xxx:yyy> を保持することができます。 |

次の形式で文字列を入力することによって、設定ファイル (cfg .xml) でこのパラメータを設定することもできます。

```
<Firewall_Config ua="na">NO_ICMP_PING</Firewall_Config>
```

**ステップ 4** [すべての変更の送信（Submit All Changes）]をクリックします。

# 暗号リストを設定する

電話機の TLS アプリケーションが使用する暗号スイートを指定することができます。 指定された暗号リストは、TLS プロトコルを使用するすべてのアプリケーションに適用されます。お使いの電話機の TLS アプリケーションには、次のものが含まれます。

- カスタマー CA プロビジョニング
- E911 地理位置情報
- ファームウェア/シスコ ヘッドセットアップグレード
- LDAPS
- LDAP (StartTLS)
- 画像ダウンロード

- ロゴダウンロード
- ディクショナリダウンロード
- プロビジョニング
- レポートアップロード
- PRTアップロード
- SIP オーバー TLS
- TR-069
- WebSocket API
- XML サービス
- XSI サービス

また、TR-069 パラメータ (`Device.X_CISCO_SecuritySettings.TLSCipherList`) または設定ファイル(cfg.xml)で暗号を指定することもできます。 設定ファイルに次のフォーマットで文字列を入力します。

```
<TLS_Cipher_List ua="na">RSA:!aNULL:!eNULL</TLS_Cipher_List>
```

### 始める前に

電話管理のウェブページにアクセスして、 電話機 ウェブインターフェイスへのアクセスを参照してください。

## 手順

**ステップ 1** **[音声（Voice）] > [システム（System）]** を選択します。

**ステップ 2** **セキュリティ設定**セクションで、**TLS 暗号化リスト**フィールドに暗号スイートまたは暗号スイートの組み合わせを入力します。

**例**：

```
RSA:!aNULL:!eNULL
```

RSA認証を使用してこれらの暗号スイートをサポートしますが、暗号化と認証を行わない暗号スイートを除きます

（注）
有効な暗号リストは、 https://www.openssl.org/docs/man1.1.1/man1/ciphers.htmlで定義されている形式に従う必要があります。 電話機は、OpenSSL ウェブページにリストされているすべての暗号文字列をサポートしていません。 サポートされる文字列については、サポートされている暗号文字列 （24 ページ）を参照してください。

**TLS暗号リスト**フィールドに空白または無効な値が含まれている場合、使用される暗号スイートはアプリケーションによって異なります。このフィールドに空白または無効な値が含まれている場合は、アプリケーションが使用する以下のスイートの一覧を参照してください。

- ウェブサーバ (HTTPS) アプリケーションは、次の暗号スイートを使用します。
  - **ECDHE-RSA-AES256-GCM-SHA384**
  - **ECDHE-RSA-AES128-GCM-SHA256**
  - **AES256-SHA**
  - **AES128-SHA**
  - **DES-CBC3-SHA**
- XMPP では、暗号リストt **HIGH:MEDIUM:AES:@STRENGTH**を使用します。
- SIP、TR-069、および curl ライブラリを使用するその他のアプリケーションは、**デフォルト**の暗号ストリングを使用します。**デフォルト**の暗号ストリングには、電話機がサポートする次の暗号スイートが含まれます。

```
DEFAULT Cipher Suites (28 suites):
        ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
        ECDHE_RSA_WITH_AES_256_GCM_SHA384
        DHE_RSA_WITH_AES_256_GCM_SHA384
        ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
        ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
        DHE_RSA_WITH_CHACHA20_POLY1305_SHA256
        ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
        ECDHE_RSA_WITH_AES_128_GCM_SHA256
        DHE_RSA_WITH_AES_128_GCM_SHA256
        ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
        ECDHE_RSA_WITH_AES_256_CBC_SHA384
        DHE_RSA_WITH_AES_256_CBC_SHA256
        ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
        ECDHE_RSA_WITH_AES_128_CBC_SHA256
        DHE_RSA_WITH_AES_128_CBC_SHA256
        ECDHE_ECDSA_WITH_AES_256_CBC_SHA
        ECDHE_RSA_WITH_AES_256_CBC_SHA
        DHE_RSA_WITH_AES_256_CBC_SHA
        ECDHE_ECDSA_WITH_AES_128_CBC_SHA
        ECDHE_RSA_WITH_AES_128_CBC_SHA
        DHE_RSA_WITH_AES_128_CBC_SHA
        RSA_WITH_AES_256_GCM_SHA384
        RSA_WITH_AES_128_GCM_SHA256
        RSA_WITH_AES_256_CBC_SHA256
        RSA_WITH_AES_128_CBC_SHA256
        RSA_WITH_AES_256_CBC_SHA
        RSA_WITH_AES_128_CBC_SHA
        EMPTY_RENEGOTIATION_INFO_SCSV
```

**ステップ3** [すべての変更の送信（Submit All Changes）]をクリックします。

# サポートされている暗号文字列

次に示すサポートされている暗号文字列は、OpenSSL 1.1.1d 標準に基づいています。

**表 *6 :* サポートされている暗号文字列 *(OpenSSL 1.1.1d)***

| 文字列 | 文字列 | 文字列 |
|---|---|---|
| DEFAULT | kECDHE、kEECDH | CAMELLIA128, CAMELLIA256, CAMELLIA |
| COMPLEMENTOFDEFAULT | ECDHE、EECDH | CHACHA20 |
| すべて | ECDH | SEED |
| COMPLEMENTOFALL | AECDH | MD5 |
| 高 | aRSA | SHA1、SHA |
| 中規模 | aDSS、DSS | SHA256、SHA384 |
| eNULL、NULL | aECDSA、ECDSA | SUITEB128、SUITEB128ONLY、SUITEB192 |
| aNULL | TLSv 1.2, TLSv1, SSLv3 | |
| kRSA、RSA | AES128、AES256、AES | |
| kDHE、kEDH、DH | AESGCM | |
| DHE、EDH | AESCCM、AESCCM8 | |
| ADH | ARIA128、ARIA256、ARIA | |

# SIP over TLS のホスト名検証を有効化する

TLS を使用している場合は、電話回線上の電話機のセキュリティを向上させることができます。 電話回線はホスト名を確認して、接続が安全であるかどうかを確認できます。

TLS接続を介して、電話機はサーバアイデンティティを確認するためにホスト名を検証できます。 電話機は、サブジェクトの別名 (SAN) と一般名 (CN) の両方をチェックできます。 有効な証明書のホスト名がサーバとの通信に使用されるホスト名と一致する場合、TLS接続が確立されます。 それ以外の場合、TLS 接続は失敗します。

電話機は、常に、以下のアプリケーションのホスト名を確認します。

- LDAPS
- LDAP (StartTLS)
- XMPP

- HTTPS 経由のイメージアップグレード
- HTTPS over HTTPS
- HTTPS 経由でのファイルのダウンロード
- TR-069

電話回線が TLS を介して SIP メッセージを転送する場合、**内線(n)**タブの **TLS名検証** フィールドを使用して回線を設定し、ホスト名の検証を有効にするか、あるいはバイパスするかを設定できます。

### 始める前に

- 電話管理の Web ページにアクセスします。 電話機 ウェブインターフェイスへのアクセスを参照してください。
- 内線 (n)]タブで、**SIP トランスポート**を**TLS に設定します**。

### 手順

**ステップ 1** **音声** > **内線 (n)**.に移動します。

**ステップ 2** **[プロキシと登録** セクションで、**TLS名検証** フィールドを **[はい（Yes）]** に設定してホスト名検証を有効にするか、**[いいえ（No）]** に 設定してホスト名検証をバイパスします。

次の形式で文字列を入力することによって、設定ファイル (cfg .xml) でこのパラメータを設定することもできます。

```
<TLS_Name_Validate_1_ ua="na">Yes</TLS_Name_Validate_1_>
```

有効値は、 はいまたはいいえです。デフォルト設定は、はいです

**ステップ 3** [すべての変更の送信（Submit All Changes）]をクリックします。

# メディアプレーンセキュリティネゴシエーションの顧客開始モードを有効にする

メディアセッションを保護するには、サーバーとのメディアプレーンセキュリティネゴシエーションを開始するように電話機を設定できます。 セキュリティメカニズムは、RFC 3329 に記載されている標準と、メディア用の内線ドラフトアセキュリティメカニズム名アに従っています (https://tools.ietf.org/html/draft-dawes-sipcore-mediasec-parameter-08#ref-2を参照)。 電話機とサーバ間でのネゴシエーションの転送では、UDP、TCP、およびTLS を介した SIP プロトコルを使用できます。 シグナリングトランスポートプロトコルが TLS の場合にのみ メディアプレーンセキュリティネゴシエーションが適用されるように制限することができます。

このパラメータは、設定ファイル(cfg.xml)のパラメータでも設定できます。 各パラメータを設定するには、メディア平面セキュリティネゴシエーションのパラメータ （26 ページ）の文字列のシンタックスを参照してください。

### 始める前に

電話管理の Web ページにアクセスします。 電話機 ウェブインターフェイスへのアクセスを参照してください。

### 手順

**ステップ 1** **[音声（Voice）]** > **内線（n）（Ext(n)）**を選択します。

**ステップ 2** **SIP の設定**セクションで、**MediaSec リクエスト**および**MediaSec Over TLS Only**フィールドをメディア平面セキュリティネゴシエーションのパラメータ （26 ページ）で定義されているように設定します

**ステップ 3** [すべての変更の送信（Submit All Changes）]をクリックします。

# メディア平面セキュリティネゴシエーションのパラメータ

次の表で、電話機のウェブインターフェイスの **[音声（Voice）]**> **[内線（n）（Ext (n)）]** タブにある **[SIP 設定（SIP Settings）]** セクションにおける、メディア平面セキュリティネゴシエーション用パラメータの機能と使用方法を定義します。 また、パラメータを設定するために、XML コードを含む電話設定ファイルに追加される文字列のシンタックスも定義します。

表 *7:* メディア平面セキュリティネゴシエーションのパラメータ

| パラメータ | 説明 |
| --- | --- |
| MediaSec リクエスト | 電話機がサーバとのメディア平面セキュリティネゴシエーションを開始するかどうかを指定します。<br>次のいずれかを実行します。<br>• XML (cfg.xml)を使用した電話機の設定ファイルでは、次の形式で文字列を入力します。<br>`<MediaSec_Request_1_ ua="na">Yes</MediaSec_Request_1_>`<br>• 電話機のウェブインターフェイスで、必要に応じてこのフィールドを **[はい（Yes）]** または **[いいえ（No）]** に設定します。<br>有効値: はい（Yes）| いいえ（No）<br>• **[**はい (Yes)]: クライアントが開始するモード。 電話機は、メディア平面セキュリティネゴシエーションを開始します。<br>• **いいえ（No）**—サーバ起動モード。サーバがメディア平面セキュリティネゴシエーションを開始します。電話機はネゴシエーションを開始しませんが、サーバからのネゴシエーション要求を処理して、安全な通話を確立できます。<br>デフォルト：[いいえ（No）] |

| パラメータ | 説明 |
| --- | --- |
| MediaSec Over TLS のみ | メディア平面セキュリティネゴシエーションが適用されるシグナリングトランスポートプロトコルを指定します。<br><br>このフィールドで **[はい（Yes）]** に設定する前に、シグナリングプロトコルが TLS であることを確認してください。<br><br>次のいずれかを実行します。<br><br>• XML (cfg.xml)を使用した電話機の設定ファイルでは、次の形式で文字列を入力します。<br><br>`<MediaSec_Over_TLS_Only_1_ ua="na">No</MediaSec_Over_TLS_Only_1_>`<br><br>• 電話機のウェブインターフェイスで、必要に応じてこのフィールドを **[はい（Yes）]** または **[いいえ（No）]** に設定します。<br><br>有効値: はい（Yes）| いいえ（No）<br><br>• **[はい（Yes）]**： 電話機は、シグナリングトランスポートプロトコルがTLSの場合にのみ、メディア平面セキュリティネゴシエーションを開始または処理します。<br><br>• **[いいえ （No）]**: 電話機は、シグナリングトランスポートプロトコルに関係なく、メディア平面セキュリティネゴシエーションを開始し、処理します。<br><br>デフォルト：[いいえ（No）] |

# 802.1X 認証

Cisco IP 電話は、Cisco Discovery Protocol(CDP)を使用してLANスイッチを識別し、VLAN 割当やインラインパワー要件などのパラメータを決定します。 CDP では、ローカルに接続されたワークステーションは識別されません。 Cisco IP Phones は、EAPOL パススルーメカニズムを提供します。 このメカニズムを使用すると、Cisco IP 電話に接続されたワークステーションは、LAN スイッチにある 802.1X オーセンティケータに EAPOL メッセージを渡すことができます。 パススルー メカニズムにより、IP フォンはネットワークにアクセスする前にデータ エンドポイントを認証する際 LAN スイッチとして動作しません。

Cisco IP Phones はまた、プロキシ EAPOL ログオフメカニズムも提供します。 ローカルに接続された PC が IP フォンから切断された場合でも、LAN スイッチと IP フォン間のリンクは維持されるので、LAN スイッチは物理リンクの障害を認識しません。 ネットワークの完全性が脅かされるのを避けるため、IP フォンはダウンストリーム PC の代わりに EAPOL ログオフ メッセージをスイッチに送ります。これは、LAN スイッチにダウンストリーム PC の認証エントリをクリアさせます。

802.1X 認証のサポートには、次のようなコンポーネントが必要です。

- Cisco IP 電話: 電話機は、ネットワークへのアクセス要求を開始します。 Cisco IP Phones には、802.1x サプリカントが含まれています。 このサプリカントを使用して、ネットワーク管理者は IP 電話と LAN スイッチ ポートの接続を制御できます。 電話機に含まれる 802.1X サプリカントの現在のリリースでは、ネットワーク認証に EAP-FAST オプションと EAP-TLS オプションが使用されています。
- Cisco Secure Access Control Server（ACS）（またはその他のサードパーティ製認証サーバ）：認証サーバと電話機の両方に、電話機を認証するための共有秘密が設定されている必要があります。
- 802.1Xをサポートする LAN スイッチ：このスイッチはオーセンティケーターとして機能し、電話と認証サーバー間でメッセージを送受信します。 この交換が完了した後、スイッチはネットワークへの電話機のアクセスを許可または拒否します。

802.1X を設定するには、次の手順を実行する必要があります。

- 電話機で 802.1X 認証をイネーブルにする前に、他のコンポーネントを設定します。
- PC ポートの設定：802.1X 標準では VLAN が考慮されないため、特定のスイッチ ポートに対してデバイスを 1 つだけ認証することを推奨します。 ただし、一部のスイッチはマルチドメイン認証をサポートしています。 スイッチの設定により、PC を電話機の PC ポートに接続できるかどうかが決定されます。
  - はい（Yes）：マルチドメイン認証をサポートするスイッチを使用している場合は、PCポートを有効にして、PCを接続することができます。 この場合、スイッチと接続先 PC 間の認証情報の交換をモニタするために、Cisco IP 電話はプロキシ EAPOL ログオフをサポートします。
  - いいえ（No）：スイッチが同じポート上の複数の 802.1X 準拠デバイスをサポートしていない場合は、802.1X 認証を有効にする際に PC ポートを無効にする必要があります。 このポートを無効にしないで PC を接続しようとすると、スイッチは電話機と PC の両方に対してネットワーク アクセスを拒否します。
- ボイス VLAN の設定：802.1X 標準では VLAN が考慮されないため、この設定をスイッチのサポートに基づいて行うようにしてください。
  - 有効：複数ドメインの認証をサポートするスイッチを使用している場合は、ボイス VLAN を引き続き使用できます。
  - 無効：スイッチで複数ドメインの認証がサポートされていない場合は、ボイス VLAN を無効にし、ポートをネイティブ VLAN に割り当てることを検討してください。

# カスタム デバイス証明書を手動でインストールする

電話管理ウェブページから証明書をアップロードすることで、電話にカスタムデバイス証明書 (CDC) を手動でインストールできます。

### 始める前に

電話のカスタム デバイス証明書をインストールするには、以下が必要です。

- OpenSSL 3.0 以降により生成された証明書ファイル（.p12 または .pfx）。 このファイルには証明書と秘密鍵が含まれています。 このファイルを PC に保存します。
- 証明書の抽出パスワードです。 パスワードは証明書ファイルの解読に使用されます。 パスワードの長さは 14 文字より大きくなければなりません。
- 電話機管理のウェブページにアクセスします。 電話機 ウェブインターフェイスへのアクセスを参照してください。

### 手順

**ステップ 1** **[証明書（Certificate）]** > **[カスタム（Custom）]** を選択します。

**ステップ 2** **証明書の追加** セクションで、 **参照...** をクリックします。

**ステップ 3** PC の証明書を参照します。

**ステップ 4** [抽出パスワード（Extract password）]フィールドに、証明書の抽出パスワードを入力します。

**ステップ 5** [アップロード（Upload）]をクリックします。

証明書ファイルとパスワードが正しい場合、「証明書が追加されました。」というメッセージが表示されます。そうでない場合、アップロードは失敗し、証明書をアップロードできないことを示すエラーメッセージが表示されます。

**ステップ 6** インストール済みの証明書を確認するには、**[既存の証明書（Existing Certificates）]** セクションで **[表示（View）]** をクリックします。

**ステップ 7** （任意） インストールされた証明書を電話から削除するには、**[既存の証明書（Existing Certificates）]** セクションで **[削除（Delete）]** をクリックします。

ボタンをクリックすると、削除操作が確認なしですぐに開始されます。

証明書が正常に削除されると、「証明書が削除されました。」というメッセージが表示されます。

# SCEP でカスタム デバイス証明書を自動的にインストールする

証明書ファイルを手動でアップロードしたくない場合、または証明書ファイルがない場合は、Simple Certificate Enrollment Protocol (SCEP) パラメーターをセットアップして、カスタムデバイス証明書 (CDC) を自動的にインストールできます。

SCEP パラメータが正しく設定されている場合、電話機は SCEP サーバーに要求を送信し、定義された指紋を使用して、CA 証明書がデバイスによって検証されます。

### 始める前に

電話のカスタム デバイス証明書をインストールするには、以下が必要です。

- SCEP サーバアドレス
- SCEP サーバのルート CA 証明書の SHA-1 または SHA-256 フィンガープリント
- 電話機管理のウェブページにアクセスします。 電話機 ウェブインターフェイスへのアクセスを参照してください。

### 手順

**ステップ 1** 電話管理のウェブページにアクセスします。

**ステップ 2** **[証明書（Certificate）] > [カスタム（Custom）]** を選択します。

**ステップ 3** [ **SCEP 設定 1** ] セクションで、次の表 SCEP 設定用の パラメータの説明に従ってパラメータを設定します。

**ステップ 4** [すべての変更の送信（Submit All Changes）]をクリックします。

## SCEP 構成のパラメータ

次の表では、電話機管理 Web インターフェイスの **[SCEP 設定 1（SCEP Configuration 1）]** セクションの **[証明書（Certificate）] > [カスタム（Custom）]** タブにある SCEP 設定パラメータの機能と使用方法を定義します。また、パラメータを設定するために電話設定ファイル(cfg.xml)に追加される文字列の構文も定義します。

**表 *8 : SCEP* 構成のパラメータ**

| パラメータ | 説明 |
|---|---|
| サーバ（Server） | SCEP サーバアドレス。 このパラメータは必須です。<br>次のいずれかを実行します。<br>• XML（cfg.xml）を使用した電話機の設定ファイルでは、次の形式で文字列を入力します。<br>`<CDC_Server_1_ ua="na">http://10.79.57.91</CDC_Server_1_>`<br>• 電話管理ウェブページで、SCEP サーバアドレスを入力します。<br>有効な値: URL または IP アドレス。 HTTPS スキームはサポートされていません。<br>デフォルト：空 |

| パラメータ | 説明 |
| --- | --- |
| ルート CA フィンガープリント | SCEP プロセス中の検証のためのルート CA の SHA256 または SHA1 指紋。 このパラメータは必須です。<br>次のいずれかを実行します。<br>• XML（cfg.xml）を使用した電話機の設定ファイルでは、次の形式で文字列を入力します。<br><CDC_Root_CA_Fingerprint_1_ ua="na">12040870625C5B755D73F5925285F8F5FF5D55AF</CDC_Root_CA_Fingerprint_1_><br>• 電話機の管理ウェブページで、有効な指紋を入力します。<br>デフォルト：空 |
| チャレンジパスワード | SCEP 経由の証明書登録中の電話機に対する Certificate Authority（CA）認証用のチャレンジパスワード。 このパラメータはオプションです。<br>実際の SCEP 環境により、チャレンジパスワードの動作は異なります。<br>• 電話機が CA と通信する Cisco RA から証明書を取得する場合、CA ではチャレンジパスワードはサポートされません。この場合、Cisco RA は CA にアクセスするための認証に電話機の MIC/SUDI を使用します。電話機は最初の登録と証明書の更新の両方に MIC/SUDI を使用します。<br>• 電話が CA と直接通信することで証明書を取得する場合、チャレンジ パスワードは CA でサポートされます。構成されている場合、最初の登録にのみ使用されます。 証明書の更新では、インストールされている証明書が代わりに使用されます。<br>次のいずれかを実行します。<br>• XML（cfg.xml）を使用した電話機の設定ファイルでは、次の形式で文字列を入力します。<br><CDC_Challenge_Password_1_ ua="na">B36A11A834EED055</CDC_Challenge_Password_1_><br>パスワードは構成ファイル内でマスクされています。<br>• 電話管理ウェブページで、チャレンジパスワードを入力します。<br>デフォルト：空 |

# DHCP オプション 43 経由の SCEP パラメータ設定

電話ウェブページでの手動設定による SCEP 証明書の登録に加えて、DHCP オプション 43 を使用して DHCP サーバからパラメータを入力することもできます。 DHCP オプション 43 は

SCEP パラメーターで事前設定されており、後で電話が DHCP サーバーからパラメーターを取得して、SCEP 証明書の登録を実行できます。

（注）
- DHCP オプション 43 による SCEP パラメータ設定は、工場出荷時設定にリセットされた電話機でのみ利用できます。
- 電話機は、オプション 43 とリモートプロビジョニング（例えば、オプション 66,160,159,150、またはクラウドプロビジョニング）の両方をサポートするネットワーク内に配置しないでください。 そうしないと、電話機はオプション 43 設定を取得できない場合があります。

DHCP オプション 43 の SCEP パラメーターを設定して SCEP 証明書を登録するには、次の手順を実行します。

1. SCEP 環境を準備します。

   SCEP 環境設定の詳細については、SCEP サーバのドキュメントを参照してください。

2. DHCP オプション 43 ( *8.4* ベンダー固有情報、*RFC 2132* で定義) をセットアップします。

   サブオプション (10-15) は メソッド用に予約されています。

| 電話機ウェブページのパラメータ | サブオプション | タイプ | 長さ (バイト) | 必須 |
|---|---|---|---|---|
| FIPS モード | 10 | boolean | 1 | いいえ |
| サーバ（Server） | 11 | 文字列 | **サーバ + チャレンジパスワード** の最大長は 208 バイト未満でなければなりません。 | 対応 |
| ルート CA フィンガープリント | 12 | バイナリ | 20 (SHA-1) または 32 (SHA-256) | 対応 |
| チャレンジ パスワード | 13 | 文字列 | **[サーバー（Server）]** + **[チャレンジパスワード（Challenge Password）]** の最大長は 208 バイト以下でなければなりません。 | いいえ |

| 電話機ウェブページのパラメータ | サブオプション | タイプ | 長さ (バイト) | 必須 |
|---|---|---|---|---|
| [802.1X認証の有効化（Enable 802.1X Authentication）] | 14 | boolean | 1 | いいえ |
| 証明書の選択 | 15 | 符号なし 8 ビット | 1 | いいえ |

DHCP オプション 43 を使用する場合、この方法の以下の特性に注意してください。

- サブオプション (10–15) はカスタムデバイス証明書 (CDC) 用に予約されています。
- DHCP オプション 43 の最大長は 255 バイトです。
- **FIPS モード** の値は、オンボーディングプロビジョニングの設定と一致している必要があります。そうしないと、電話はオンボーディング後に以前にインストールされた証明書の取得に失敗します。 具体的には、
  - FIPS モードが無効な環境で電話機が登録される場合、DHCP オプション 43 でパラメータ **[FIPS モード（FIPS Mode）]** を設定する必要はありません。デフォルトでは、FIPS モードが無効になっています。
  - FIPS モードが有効な環境に電話を登録する場合、DHCP オプション 43 で FIPS モードを有効にする必要があります。詳細は FIPS モードの有効化 （44 ページ）を参照してください。
- オプション 43 のパスワードはクリアテキストです。

  チャレンジパスワードが空の場合、電話は最初の登録と証明書の更新に MIC/SUDI を使用します。 チャレンジ パスワードが構成されている場合、それは最初の登録にのみ使用され、インストールされた証明書が証明書の更新に使用されます。
- **[802.1X 認証の有効化（Enable 802.1X Authentication）]** と **[証明書の選択（Certificate Select）]** は、有線ネットワークの電話機にのみ使用されます。
- DHCP オプション 60 (ベンダー クラス識別子) は、デバイス モデルを識別するために使用されます。

次の表では DHCP オプション 43（サブオプション 10 から 15）の例を示します。

| サブオプション 10 進数または 16 進数 | 値の長さ（バイト）10 進数または 16 進数 | 値 | 16 進数値 |
|---|---|---|---|
| 10/0a | 1/01 | 1 (0: 無効; 1: 有効) | 01 |
| 11/0b | 18/12 | http://10.79.57.91 | 687474703a2f2f31302e37392e35372e3931 |
| 12/0c | 20/14 | 1[illegible]AF | 1[illegible]AF |

| サブオプション 10 進数または 16 進数 | 値の長さ（バイト）10 進数または 16 進数 | 値 | 16 進数値 |
|---|---|---|---|
| 13/0d | 16/10 | D233CCF9B9952A15 | 443233334343463942393935324131335 |
| 14/0e | 1/01 | 1（0：いいえ、1：はい） | 01 |
| 15/0f | 1/01 | 1（0：製造元でインストール、1：カスタムインストール） | 01 |

パラメータ値の概要:

- FIPS モード = `Enabled`
- サーバ = `http://10.79.57.91`
- ルート CA フィンガープリント = `12040870625C5B755D73F5925285F8F5FF5D55AF`
- チャレンジ パスワード = `D233CCF9B9952A15`
- 802.1X 認証を有効にする = `Yes`
- 証明書の選択 = `Custom installed`

最終的な 16 進数値の構文は次のとおりです: `{<suboption><length><value>}...`

上記のパラメータ値によると、最終的な 16 進値は以下の通りです。

0a01010b12687474703a2f2f31302e37392e35372e39310c14120408706625C5B755D73F5925285F8F5FF5D55AF0d1044323333434346394239393532413135350e01010f0101

3. DHCP サーバで DHCP オプション 43 を構成します。

（注） この手順は、Cisco Network Register の DHCP オプション 43 構成の例を提供します。

1. DHCP オプション定義セットを追加します。

   ベンダーオプション文字列 は IP 電話のモデル名です。 たとえば、CP-8865-3PCC、CP-8832-3PCC などです。

2. DHCP オプション 43 とサブオプションを DHCP オプション定義セットに追加します。

   **例**：

3. オプション 43 を DHCP ポリシーに追加し、値を次のようにセットアップします。

   **例**：

   ```
   (10 1)(11 http://10.79.57.91)(12 12040870625C5B755D73F5925285F8F5FF5D55AF)(13
   D233CCF9B9952A15)(14 1)(15 1)
   ```

4. 設定を確認します。 Wireshark を使用して、電話とサービスの間のネットワーク トラフィックのトレースをキャプチャできます。

4. 電話機の工場出荷時設定へのリセットを実行します。

   電話がリセットされた後、パラメータ **サーバ**、 **ルート CA 指紋**、および **チャレンジパスワード** が自動的に入力されます。 電話機管理のウェブページにアクセスします。これらのパラメータは、**[SCEP 設定 1（SCEP Configuration 1）]** の **[証明書（Certificate）]** > **[カスタム（Custom）]** セクションに位置しています。

   インストール済みの証明書を確認するには、**[既存の証明書（Existing Certificates）]** セクションで **[表示（View）]** をクリックします。

   証明書のインストール状況を確認するには、**[証明書（Certificate）]** > **[カスタム証明書ステータス（Custom Cert Status）]** を選択します。 **ダウンロード状況 1** に最新の結果が表示されます。 証明書の登録中に問題が発生した場合、トラブルシューティングの目的で、ダウンロードの状況に問題の理由を表示できます。

（注） チャレンジパスワード認証が失敗した場合、ユーザーは電話スクリーン上でパスワードを入力するように指示されます。

5. オプション：インストールされた証明書を電話から削除するには、**[既存の証明書（Existing Certificates）]** セクションで **[削除（Delete）]** をクリックします。

（注） ボタンをクリックすると、削除操作が確認なしですぐに開始されます。

## SCEP による証明書の更新

デバイス証明書は、SCEP プロセスによって自動的に更新できます。

- 電話機は、証明書が 15 日後に期限切れになるかどうかを 4 時間ごとに確認します。 その場合、電話は証明書の更新プロセスを自動的に開始します。
- チャレンジパスワードが空の場合、電話は最初の登録と証明書の更新の両方に MIC/SUDI を使用します。 チャレンジ パスワードが設定されている場合、最初の登録にのみ使用され、既存/インストール済みの証明書が証明書の更新に使用されます。
- 電話は、新しい証明書を取得するまで、古いデバイス証明書を削除しません。
- デバイスの証明書または CA の有効期限が切れているために証明書の更新が失敗した場合、電話は最初の登録を自動的にトリガーします。 一方、チャレンジ パスワード認証が失敗すると、電話スクリーンにパスワード入力画面がポップアップ表示され、ユーザは電話でチャレンジ パスワードを入力するように求められます。

# プロキシサーバーをセットアップする

セキュリティを向上するためにプロキシサーバーを使用するように電話機を設定できます。プロキシサーバーは、電話機とインターネット間のファイアウォールとして動作します。設定が成功すると、電話機はプロキシサーバーを介してインターネットに接続し、電話機をサイバー攻撃から保護します。

自動設定スクリプトを使用するか、または手動でホストサーバー（ホスト名または IP アドレス）とプロキシサーバーのポートを設定することで、プロキシサーバーを設定できます。

設定すると、HTTP プロキシ機能は、HTTP プロトコルを使用するすべてのアプリケーションに適用されます。 アプリケーションには、次のものが含まれます。

- GDS（アクティベーション コードによるオンボーディング）
- EDOS デバイスの有効化
- Webex クラウドへのオンボーディング（EDOS および GDS 経由）
- 証明書認証
- プロビジョニング
- ファームウェア アップグレード
- 電話ステータスレポート

- PRTアップロード
- XSI サービス
- Webex サービス
- E911 地理位置情報

### 始める前に

電話管理の Web ページにアクセスします。 電話機 ウェブインターフェイスへのアクセスを参照してください。

## 手順

**ステップ 1** **[音声（Voice）]** > **[システム（System）]** を選択します。

**ステップ 2** **[HTTP プロキシ設定（HTTP Proxy Settings）]** セクションで、要件に応じてパラメータ **[プロキシモード（Proxy Mode）]** とその他のパラメータを設定します。 詳細については、次の手順で説明します。

**ステップ 3** 次のいずれか 1 つの処理を実行します。

- **[プロキシモード（Proxy Mode）]** は **[自動（Auto）]** です。
  - **[自動検出を使用（WPAD）（Use Auto Discovery (WPAD)）]** が **[はい（Yes）]** の場合は、それ以上のアクションは不要です。 電話機は、Web プロキシ自動検出（WPAD）プロトコルによってプロキシ自動設定（PAC）ファイルを自動的に取得します。
  - **[自動検出を使用（WPAD）（Use Auto Discovery (WPAD)）]** が **[いいえ（No）]** の場合は、**[PAC URL]** に有効な URL を入力します。
- **[プロキシモード（Proxy Mode）]** は **[手動（Manual）]** です。
  - **[プロキシサーバーに認証が必要（Proxy Server Requires Authentication）]** が **[いいえ（No）]** の場合は、**[プロキシホスト（Proxy Host）]** にプロキシサーバーを入力し、**[プロキシポート（Proxy Port）]** にプロキシポートを入力します。
  - **[プロキシサーバーに認証が必要（Proxy Server Requires Authentication）]** が **[はい（Yes）]** の場合は、**[プロキシホスト（Proxy Host）]** にプロキシサーバーを入力し、**[プロキシポート（Proxy Port）]** にプロキシポートを入力します。 **[ユーザー名（Username）]** にユーザー名を入力し、**[パスワード（Password）]** にパスワードを入力します。
- **[プロキシモード（Proxy Mode）]** が **[オフ（Off）]** の場合は、HTTP プロキシ機能は電話機で無効になります。

このパラメータは、電話機の設定ファイル(cfg.xml)のパラメータでも設定できます。 各パラメータを設定するには、HTTP プロキシ設定のパラメータ （39 ページ）の文字列のシンタックスを参照してください。

**ステップ 4** [すべての変更の送信（Submit All Changes）]をクリックします。

# HTTP プロキシ設定のパラメータ

次の表で、電話機のウェブインターフェイスの **[音声（Voice）]** > **[システム（System）]** タブにある**[HTTP プロキシ設定（HTTP Proxy Settings）]** セクションにおける、HTTP プロキシパラメータの機能と使用方法を定義します。 また、パラメータを設定するために、XML コードを含む電話設定ファイルに追加される文字列のシンタックスも定義します。

表 *9: HTTP* プロキシ設定のパラメータ

| パラメータ | 説明とデフォルト値 |
|---|---|
| プロキシモード | 電話機が使用する HTTP プロキシモードを指定するか、HTTP プロキシ機能を無効にします。<br>• 自動<br>電話機は自動的にプロキシ自動設定（PAC）ファイルを取得し、プロキシサーバーを選択します。 このモードでは、Web プロキシ自動検出（WPAD）プロトコルを使用して PAC ファイルを取得するか、または手動で PAC ファイルの有効な URL を入力するかどうかを決定できます。<br>パラメータの詳細については、「自動検出を使用（WPAD）」および「PAC URL」を参照してください。<br>• 手動<br>サーバー（ホスト名または IP アドレス）とプロキシサーバーのポートを手動で指定する必要があります。<br>パラメータの詳細については、「プロキシホスト」と「プロキシポート」を参照してください。<br>• オフ<br>電話機の HTTP プロキシ機能を無効にします。<br>次のいずれかを実行します。<br>• XML (cfg.xml)を使用した電話機の設定ファイルでは、次の形式で文字列を入力します。<br>`<Proxy_Mode ua="rw">Off</Proxy_Mode>`<br>• 電話機の Web インターフェイスで、プロキシモードを選択するか、この機能を無効にします。<br>有効値：Auto、Manual、および Off<br>デフォルト：Off |

| パラメータ | 説明とデフォルト値 |
|---|---|
| 自動ディスカバリ(WPAD)を使用 | 電話機が Web プロキシ自動検出（WPAD）プロトコルを使用して PAC ファイルを取得するかどうかを決定します。<br><br>WPAD プロトコルは、DHCP または DNS、あるいは両方のネットワークプロトコルを使用して、プロキシ自動設定（PAC）ファイルを自動的に特定します。 PAC ファイルは、特定の URL のプロキシサーバーを選択するために使用されます。 このファイルは、ローカルまたはネットワーク上でホストできます。<br><br>• パラメータの設定は、**[プロキシモード（Proxy Mode）]** が **[自動（Auto）]** に設定されている場合に有効になります。<br><br>• パラメータを **[いいえ（No）]** に設定した場合は、PAC URL を指定する必要があります。<br><br>パラメータの詳細については、PAC URL を参照してください。<br><br>次のいずれかを実行します。<br><br>• XML (cfg.xml)を使用した電話機の設定ファイルでは、次の形式で文字列を入力します。<br><br>`<Use_Auto_Discovery__WPAD_ ua="rw">Yes</Use_Auto_Discovery__WPAD_>`<br><br>• 電話機ウェブインターフェイスで、必要に応じて [はい（Yes）] または [いいえ（No）] を選択します<br><br>有効値: はい（Yes）といいえ（No）<br><br>デフォルト：はい（Yes） |
| PAC URL | PAC ファイルの URL。<br><br>たとえば、`http://proxy.department.branch.example.com` などです。<br><br>TFTP、HTTP、および HTTPS がサポートされています。<br><br>**[プロキシモード（Proxy Mode）]** を **[自動（Auto）]** に設定し、**[自動検出を使用（WPAD）（Use Auto Discovery (WPAD)）]** を **[いいえ（No）]** に設定した場合は、このパラメータを設定する必要があります。<br><br>次のいずれかを実行します。<br><br>• XML (cfg.xml)を使用した電話機の設定ファイルでは、次の形式で文字列を入力します。<br><br>`<PAC_URL ua="rw">http://proxy.department.branch.example.com/pac</PAC_URL>`<br><br>• 電話機の Web インターフェイスで、PAC ファイルを特定する有効な URL を入力します。<br><br>デフォルト：空 |

| パラメータ | 説明とデフォルト値 |
| --- | --- |
| プロキシホスト | アクセスする電話機のプロキシホストサーバーの IP アドレスまたはホスト名です。 次に例を示します。<br>`proxy.example.com`<br>スキーム（`http://` または `https://`）は不要です。<br>**[プロキシモード（Proxy Mode）]** を **[手動（Manual）]** に設定した場合は、このパラメータを設定する必要があります。<br>次のいずれかを実行します。<br>• XML (cfg.xml)を使用した電話機の設定ファイルでは、次の形式で文字列を入力します。<br>`<Proxy_Host ua="rw">proxy.example.com</Proxy_Host>`<br>• 電話のウェブインターフェイスで、プロキシサーバーの IP アドレスまたはホスト名を入力します。<br>デフォルト：空 |
| プロキシポート | プロキシホストサーバーのポート番号。<br>**[プロキシモード（Proxy Mode）]** を **[手動（Manual）]** に設定した場合は、このパラメータを設定する必要があります。<br>次のいずれかを実行します。<br>• XML (cfg.xml)を使用した電話機の設定ファイルでは、次の形式で文字列を入力します。<br>`<Proxy_Port ua="rw">3128</Proxy_Port>`<br>• 電話機の Web インターフェイスで、サーバーポートを入力します。<br>デフォルト：3128 |

| パラメータ | 説明とデフォルト値 |
| --- | --- |
| プロキシサーバーに認証が必要（Proxy Server Requires Authentication） | ユーザーが、プロキシサーバーに必要な認証資格情報（ユーザー名とパスワード）を入力する必要かどうかを決定します。 このパラメータは、プロキシサーバの実際の動作に応じて設定されます。<br>このパラメータを **[はい（Yes）]** に設定した場合は、**[ユーザー名（Username）]** と **[パスワード（Password）]** を設定する必要があります。<br>パラメータの詳細については、「ユーザー名」と「パスワード」を参照してください。<br>パラメータの設定は、**[プロキシモード（Proxy Mode）]** が **[手動（Manual）]** に設定されている場合に有効になります。<br>次のいずれかを実行します。<br>• XML (cfg.xml)を使用した電話機の設定ファイルでは、次の形式で文字列を入力します。<br>`<Proxy_Server_Requires_Authentication ua="rw">No</Proxy_Server_Requires_Authentication>`<br>• 電話機のウェブインターフェイスで、必要に応じてこのフィールドを [はい（Yes）] または [いいえ（No）] に設定します。<br>有効値: はい（Yes）といいえ（No）<br>デフォルト：[いいえ（No）] |
| ユーザ名 | プロキシサーバーの資格情報を持つユーザーのユーザー名。<br>**[プロキシモード（Proxy Mode）]** が **[手動（Manual）]** に設定され、**[プロキシサーバーに認証が必要（Proxy Server Requires Authentication）]** が **[はい（Yes）]** に設定されている場合は、パラメータを設定する必要があります。<br>次のいずれかを実行します。<br>• XML (cfg.xml)を使用した電話機の設定ファイルでは、次の形式で文字列を入力します。<br>`<Proxy_Username ua="rw">Example</Proxy_Username>`<br>• 電話機のウェブインターフェイスで、ユーザー名を入力します。<br>デフォルト：空 |

| パラメータ | 説明とデフォルト値 |
|---|---|
| [パスワード（Password）] | プロキシ認証用に指定されたユーザー名のパスワード。<br>**[プロキシモード（Proxy Mode）]** が **[手動（Manual）]** に設定され、**[プロキシサーバーに認証が必要（Proxy Server Requires Authentication）]** が **[はい（Yes）]** に設定されている場合は、パラメータを設定する必要があります。<br>次のいずれかを実行します。<br>• XML (cfg.xml)を使用した電話機の設定ファイルでは、次の形式で文字列を入力します。<br>`<Proxy_Password ua="rw">Example</Proxy_Password>`<br>• 電話機の Web インターフェイスで、ユーザーのプロキシ認証に有効なパスワードを入力します。<br>デフォルト：空 |

# FIPS モードの有効化

電話機を連邦情報処理標準規格（FIPS）に準拠させることができます。

FIPS は、非軍事政府内、およびそれらの機関と連携する政府請負業者やベンダーが使用するドキュメント処理、暗号化アルゴリズム、および他の情報技術標準を説明する一連の規格です。OpenSSL FOM（FIPS Object Module）は、慎重に定義されたソフトウェアコンポーネントであり、OpenSSL ライブラリとの互換性を目的として設計されています。そのため、OpenSSL ライブラリおよび API を使用する製品は、最小限の労力で FIPS 140-2 検証済み暗号化を使用するように変換できます。

FIPS モードには制限があります。

- TR069 は無効
- HTTP ダイジェスト認証は無効

### 始める前に

- 電話管理の Web ページにアクセスします。 電話機 ウェブインターフェイスへのアクセス を参照してください。

### 手順

**ステップ 1** **[音声（Voice）]** > **[システム（System）]** を選択します。

**ステップ 2** **[セキュリティ設定（Security Settings）]**セクションで、**[FIPS モード（FIPS Mode）]**パラメータから **[はい（Yes）]** または **[いいえ（No）]** を選択します。

FIPS モードを有効にしないと、電話機にセキュリティエラーメッセージが表示され、電話機を再起動する必要があります。

また、FIPS モードの有効化に失敗すると、電話機では、**[ステータスメッセージ（Status messages）]** 画面に FIPS 関連のエラーメッセージが表示されます。

**ステップ 3** [すべての変更の送信（Submit All Changes）]をクリックします。
FIPS を有効にすると、電話機で次の機能がシームレスに機能します。

| | | |
|---|---|---|
| イメージ認証（Image authentication） | PRT アップロード | ワンボタンで参加（OBTJ） |
| 安全なストレージ | ファームウェア アップグレード | SIP オーバー TLS |
| 設定ファイルの暗号化 | プロファイルの再同期 | SRTP |
| 802.1x | オンボードサービス | SIP ダイジェスト（RFC 8760） |
| HTTPS サーバー | Webex オンボーディング、Webex 通話記録、Webex ディレクトリ | HTTP プロキシ |

# シスコ製品のセキュリティの概要

本製品には暗号化機能が備わっており、輸入、輸出、配布および使用に適用される米国および他の国の法律の対象となります。 Cisco の暗号化製品を譲渡された第三者は、その暗号化技術の輸入、輸出、配布、および使用を許可されたわけではありません。 輸入業者、輸出業者、販売業者、およびユーザは、米国および他の国での法律を順守する責任があります。 本製品を使用するにあたっては、関係法令の順守に同意したものと見なされます。 米国および他の国の法律を順守できない場合は、本製品を至急送り返してください。

米国の輸出規制の詳細については、https://www.bis.doc.gov/policiesandregulations/ear/index.htm をご覧ください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。