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

制限付きアクセス ドメインの設定

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** での**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**上の**レポートルール**
- **プロビジョニング**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 （3 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ー （2 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ー

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ー

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。 次のいずれかを実行します。 • 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。 `<DHCP_Option_To_Use ua="na">66,160,159,150,60,43,125</DHCP_Option_To_Use>` • 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。 **例**：66,160,159,150,60,43,125 デフォルト：66,160,159,150,60,43,125
[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。 次のいずれかを実行します。 • 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。 `<DHCPv6_Option_To_Use ua="na">17,160,159</DHCPv6_Option_To_Use>` • 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。 **例**: 17,160,159 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
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

ネットワーク標準規格	説明
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
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 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 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
DHCP オプション 125	ベンダー識別ベンダー固有の情報 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
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]** 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。

Transport Layer Security

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。「Transport Layer Security （5 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**セクションで、**SIPトランスポート**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>
```

例えば、 `ldaps://<ldaps_server>[:port]` と入力します。

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。

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] 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。

各デバイスがHTTPSセッション中に提供する固有のクライアント証明書では、その件名フィールドに識別情報が埋め込まれています。この情報は、HTTPS サーバを介して、安全なリクエストを処理するために起動されるCGIスクリプトで使用できます。特に、証明書の件名は、ユニットの製品名（OU 要素）、MAC アドレス（S 要素）、シリアル番号（L 要素）を示します。

次は、Cisco IP 電話 8841 マルチプラットフォーム フォンのクライアント証明書にある件名フィールドの例で、以下の要素を示しています。

```
OU=CP-8841-3PCC, L=88012BA01234, S=000e08abcdef
```

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。

- Log_Request_Msg
- Log_Success_Msg
- Log_Failure_Msg

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 DHCPv6 クライアントポート 546
SIP UDP	**回線有効化** が**はい（Yes）**に設定され、**SIP トランスポート** が **UDP** または **自動** に設定されている場合、**音声** > **内線<n>** > **SIP 設定** > **SIPポート（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 （13 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。
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。

デフォルトのオープン TCP ポート	説明
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。 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** フィールドを**有効**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。

ファイアウォールオプションのキーワード	説明
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。 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。 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。 NO_ICMP_PING,TCP:12000,UDP:8000:8010 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。 • 着信 ICMP/ICMPv6 **Echo** (Ping) リクエストをドロップします。 • 着信接続用の TCP ポート 12000 (IPv4 および IPv6) を開きます。 • 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。 （注） 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。 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。 • 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。 • 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 ポート範囲を開きます。<xxx to yyy>を含む。 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。例えば、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 ポート範囲を開きます。<xxx to yyy>を含む。 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。例えば、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/Cisco ヘッドセットアップグレード
- LDAPs
- 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/man1.0.2/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 （17 ページ）を参照してください。

システムは、無効な値を空白値と見なします。**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**

- 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、コンパイル時に決定される**デフォルト**の暗号リストを使用します。
- XMPP では、暗号リストt **HIGH:MEDIUM:AES:@STRENGTH**を使用します。

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。

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 1.0.2l 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 1.0.2 l)*

文字列	文字列	文字列
DEFAULT	aDSS、DSS	ADH
COMPLEMENTOFDEFAULT	aECDSA、ECDSA	DH
すべて	AES128、AES256、AES	kECDHE、EECDH
COMPLEMENTOFALL	CAMELLIA128, CAMELLIA256, CAMELLIA	ECDH
中規模	SEED	aRSA
eNULL、NULL	kDHr、Kdhr、kDH	aDH
aNULL	kDHE、kEDH	TLSv 1.2, TLSv1, SSLv3
kRSA、RSA	DHE、EDH	AESGCM
3DES	SHA1、SHA	SUITEB128、SUITEB128ONLY、SUITEB192
MD5	SHA256、SHA384	

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
- 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|いいえです。デフォルト設定は、いいえです

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 （19 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** > **内線(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 （19 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

次の表は、電話機のウェブインターフェイスの **音声** > **内線(n)** タブにある **SIP 設定**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ています。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。 次のいずれかを実行します。 • 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。 `<MediaSec_Request_1_ ua="na">Yes</MediaSec_Request_1_>` • 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。 有効値: はい（Yes） |いいえ（No） • **[**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。 • **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。 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。 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。 次のいずれかを実行します。 • 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。 `<MediaSec_Over_TLS_Only_1_ ua="na">No</MediaSec_Over_TLS_Only_1_>` • 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。 有効値: はい（Yes） |いいえ（No） • **[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。 • **[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。 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 電話は、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 電話はまた、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 電話には、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。

[802.1X認証の有効化（Enable 802.1X Authentication）]

電話機上で 802.1X 認証を有効にできます。802.1 X 認証が有効になっている場合、電話機は 802.1 X 認証を使用してネットワークアクセスを要求します。802.1 X 認証を無効にすると、電話機は CDP を使用して VLAN とネットワークアクセスを取得します。電話画面メニューにトランザクションステータスを表示することもできます。

手順

ステップ 1 802.1 X 認証を有効にするには、次のいずれかの操作を実行します。

- 電話機のウェブインターフェイスで、**音声**>システムを選択し、**802.1X 認証有効化**フィールドを**[はい（Yes）]**に設定します。その後、**すべての変更の送信**をクリックします。
- 設定ファイル(cfg.xml)で、次の形式で文字列を入力します。

```
<Enable_802.1X_Authentication ua="rw">Yes</Enable_802.1X_Authentication>
```

- 電話機上で、**アプリケーション** > **ネットワーク設定** > **イーサネット設定** > **802.1X 認証**の順に押します。次に、**選択**ボタンで**デバイス認証**フィールドを**オン**に切り替え、**送信**を押します。

ステップ 2 （オプション）**トランザクションステータス**を選択して、以下を表示します。

- **トランザクションステータス**：802.1X認証のトランザクション ステータスを表示します。状態は、以下のようになります
  - 認証中: 認証プロセスが進行中であることを示します。
  - 認証済み（*Authenticated*）：電話が認証されたことを示します。
  - 無効化802.1X 認証が電話機で無効になっています。
- **プロトコル**：802.1x 認証に使用される EAP 方式を表示します。このプロトコルは、EAP-FAST または EAP-TLS にすることができます。

ステップ 3 を押して、メニューを終了します。

シスコ製品のセキュリティ

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。