Cisco IP Phone のセキュリティ

- セキュリティ機能 （1 ページ）
- このドキュメントでサポートされる電話機 （6 ページ）
- シスコ製品のセキュリティ （6 ページ）

セキュリティ機能

セキュリティ機能によって、コールがセキュアで認証済みであることが保証されます。

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

ドメインを入力すると、Cisco IP Phone は指定されたサーバからの SIP メッセージにのみ応答します。

始める前に

電話管理の Web ページにアクセスします。電話機の Web ページ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 [システム設定（System Configuration）] セクションで、[制限付きアクセスドメイン（Restricted Access Domains）] に、電話機が応答する各 SIP サーバ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
```

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。

インターネット接続タイプの設定

接続は次のいずれかに設定できます。

- Dynamic Host Configuration Protocol（DHCP）：電話機はネットワークの DHCP サーバから IP アドレスを受け取ることができます。Cisco IP Phone は通常、DHCP サーバが IP アドレスをデバイスに割り当てたネットワークで動作します。IPアドレスは限られたリソースであるため、DHCP サーバは定期的に IP アドレスに対するデバイス リースを更新します。電話機が何らかの理由で IP アドレスを失った場合、またはネットワーク上の他のデバイスに同じ IP アドレスが割り当てられた場合、SIP プロキシと電話機間の通信は切断されるか品質が低下します。予想される SIP 応答が、対応する SIP コマンドが送信された後プログラム可能な時間内に受信されない場合、[更新時のDHCPタイムアウト（DHCP Timeout on Renewal）] パラメータでデバイスはその IP アドレスの更新を要求します。DHCP サーバが元々電話機に割り当てられている IP アドレスを返す場合は、DHCP 割り当てが正しく機能していると見なされます。それ以外の場合、電話機はリセットして問題を解決しようとします。
- 静的 IP：電話機の静的 IP アドレス。

始める前に

電話管理の Web ページにアクセスします。電話機の Web ページ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 [IPv4設定（IPv4 Settings）] セクションで、[接続タイプ（Connection Type）] ドロップダウン リスト ボックスを使用して接続タイプを選択します。

- Dynamic Host Configuration Protocol（DHCP）
- スタティック IP（Static IP）

ステップ 3 [IPv6設定（IPv6 Settings）] セクションで、[接続タイプ（Connection Type）] ドロップダウン リスト ボックスを使用して接続タイプを選択します。

- Dynamic Host Configuration Protocol（DHCP）
- スタティック IP（Static IP）

ステップ 4 [静的IP（Static IP）] を選択した場合、[静的IP設定（Static IP Settings）] セクションで以下を設定します。

- [静的IP（Static IP）]：電話機の静的 IP アドレス
- [ネットマスク（NetMask）]：電話機のネットマスク
- [ゲートウェイ（Gateway）]：ゲートウェイの IP アドレス

ステップ 5 [すべての変更の送信（Submit All Changes）] をクリックします。

DHCP オプションのサポート

次の表に、Cisco IP Phone でサポートされている DHCP オプションを示します。

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
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

電話機は、1 つのセッションで SIP INVITE（初期）メッセージをチャレンジすることができます。チャレンジは、サービス プロバイダー ネットワーク上の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。これが実施されると、デバイスに対する悪意のある攻撃を防御することにより、VoIP ネットワークのセキュリティが大幅に向上します。

始める前に

電話管理の Web ページにアクセスします。電話機の Web ページ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。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、[INVITEの認証（Auth INVITE）] ドロップダウン リスト ボックスから [はい（Yes）] を選択します。

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。

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 メッセージを暗号化します。SIP over TLS は、メディアではなく、シグナリング メッセージのみを暗号化します。

TLS には次の 2 つの層があります。

- TLS レコード 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 シェーク プロトコル：サーバとクライアントを認証し、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。

Cisco IP Phone 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。

SIP Over TLS シグナリング暗号化の設定

始める前に

電話管理の Web ページにアクセスします。電話機の Web ページ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。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）] ドロップダウンリスト ボックスから [TLS] を選択します。

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。

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。

始める前に

電話管理の Web ページにアクセスします。電話機の Web ページ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、**ldaps://<ldaps_server>[:port]** と入力します。

定義：

- **ldaps://** = **ldaps://** から始まる、IP アドレスまたはドメイン名を入力する前のサーバ文字列

- **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。

このドキュメントでサポートされる電話機

このドキュメントでは、次の電話機をサポートしています。

- Cisco IP Phone 7800 シリーズ マルチプラットフォーム フォン：
  - Cisco IP Phone 7811 マルチプラットフォーム フォン
  - Cisco IP Phone 7821 マルチプラットフォーム フォン
  - Cisco IP Phone 7841 マルチプラットフォーム フォン
  - Cisco IP Phone 7851 マルチプラットフォーム フォン

このドキュメントでは、電話機または Cisco IP Phone という用語は上記の電話機を指します。

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。シスコ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。