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

セキュリティ機能は、コールが安全で認証済みであることを保証します。

ドメインと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 メッセージにだけ応答します。

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 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** > **システム**を選択します。

ステップ 2 [制限付きアクセス ドメイン（Restricted Access Domains）] フィールドの [システム設定（System Configuration）] セクションで、電話機に応答させる各 SIP サーバの完全修飾ドメイン名（FQDN）を入力します。FQDN をカンマで区切ります。

例：

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

ステップ 3 [すべての変更を送信（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

接続タイプは次のいずれかに設定できます。

- Dynamic Host Configuration Protocol（DHCP）：電話機でネットワーク DHCP サーバから IP アドレスを受信できるようにします。Cisco IP Phone は、通常、DHCP サーバがデバイスにIPアドレスを割り当てるネットワーク上で動作します。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 アドレスを消失した場合や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は、SIPプロキシと電話機間の通信が切断されるか、品質が低下します。想定されている SIP 応答が対応する SIP コマンドの送信後のプログラム可能な時間内に受信されなかった場合は、必ず、[更新時の DHCP タイムアウト（DHCP Timeout on Renewal）] パラメータによりデバイスがその 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。そうでない場合は、電話機がリセットして問題を解決しようとします。
- スタティック IP（Static IP）：電話のスタティック 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 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** > **システム**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。

- ダイナミック ホスト コンフィギュレーション プロトコル（DHCP）
- 静的 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。

- ダイナミック ホスト コンフィギュレーション プロトコル（DHCP）
- 静的 IP

ステップ 4 スタティック IP を選択したら、[スタティック IP の設定（Static IP Settings）] セクションで次の設定を構成します。

- [スタティック IP（Static IP）]：電話機のスタティック 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 IP アドレス

ステップ 5 [すべての変更を送信（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	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	時間オフセット
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 TR.69 自動設定サーバ（ACS）の検出に使用できます。
DHCP オプション 56	NTP サーバ IPv6 を使用する NTP サーバの構成
DHCP オプション 60	ベンダー クラス識別子
DHCP オプション 66	TFTP サーバ名
DHCP オプション 125	ベンダー識別のためのベンダー固有の情報 TR.69 自動設定サーバ（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

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 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** > **内線(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 [すべての変更を送信（Submit All Changes）] をクリックします。

Transport Layer Security

トランスポート層セキュリティ（TLS）はインターネット上の通信を保護し、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 はシグナリング メッセージだけを暗号化し、メディアは暗号化しません。

TLS には 2 つの層があります。

- TLS レコード プロトコル：SIP または TCH などの信頼性の高いトランスポート プロトコルに階層化されます。この層は対称データ暗号化を使用して接続がプライベートであることを保証し、その接続の信頼性が高いことを保証します。
- TLS ハンドシェイク プロトコル：アプリケーション プロトコルがデータを送信または受信する前に、サーバとクライアントを認証し、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 トランスポートの標準として UDP を使用しますが、電話機は、より安全性の高い SIP over TLS もサポートしています。

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 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** > **内線(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 [すべての変更を送信（Submit All Changes）] をクリックします。

LDAP over TLS の設定

TLS 経由の LDAP を設定すると、サーバと特定の電話間においてセキュリティで保護されたデータの転送が可能です。

注目 Cisco では、認証方法をデフォルト値である **なし** に設定することを推奨します。サーバ フィールドの横にある認証フィールドで **None**、**Simple**、または **DIGEST-MD5** の値が使用されます。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 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** > **電話**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** 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。

値は次のとおりです。

- **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

- **ポート** = ポート番号。デフォルト値：636

ステップ 3 [すべての変更を送信（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サポートされる電話機は、次のとおりです。

- Cisco IP Phone 8800 シリーズ マルチプラットフォーム電話機：
  - Cisco IP Phone 8811 マルチプラットフォーム電話機
  - Cisco IP Phone 8841 マルチプラットフォーム電話機
  - Cisco IP Phone 8845 マルチプラットフォーム電話機
  - Cisco IP Phone 8851 マルチプラットフォーム電話機
  - Cisco IP Phone 8861 マルチプラットフォーム電話機
  - Cisco IP Phone 8865 マルチプラットフォーム電話機

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、配布および使用に際しては、米国および他国の法律が適用されます。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。米国および現地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。