暗号化音声インスペクションの TLS プロキシの設定

この章では、暗号化音声インスペクション機能の TLS プロキシ用に ASA を設定する方法を説明します。

この章の内容は、次のとおりです。

暗号化音声インスペクションの TLS プロキシに関する情報

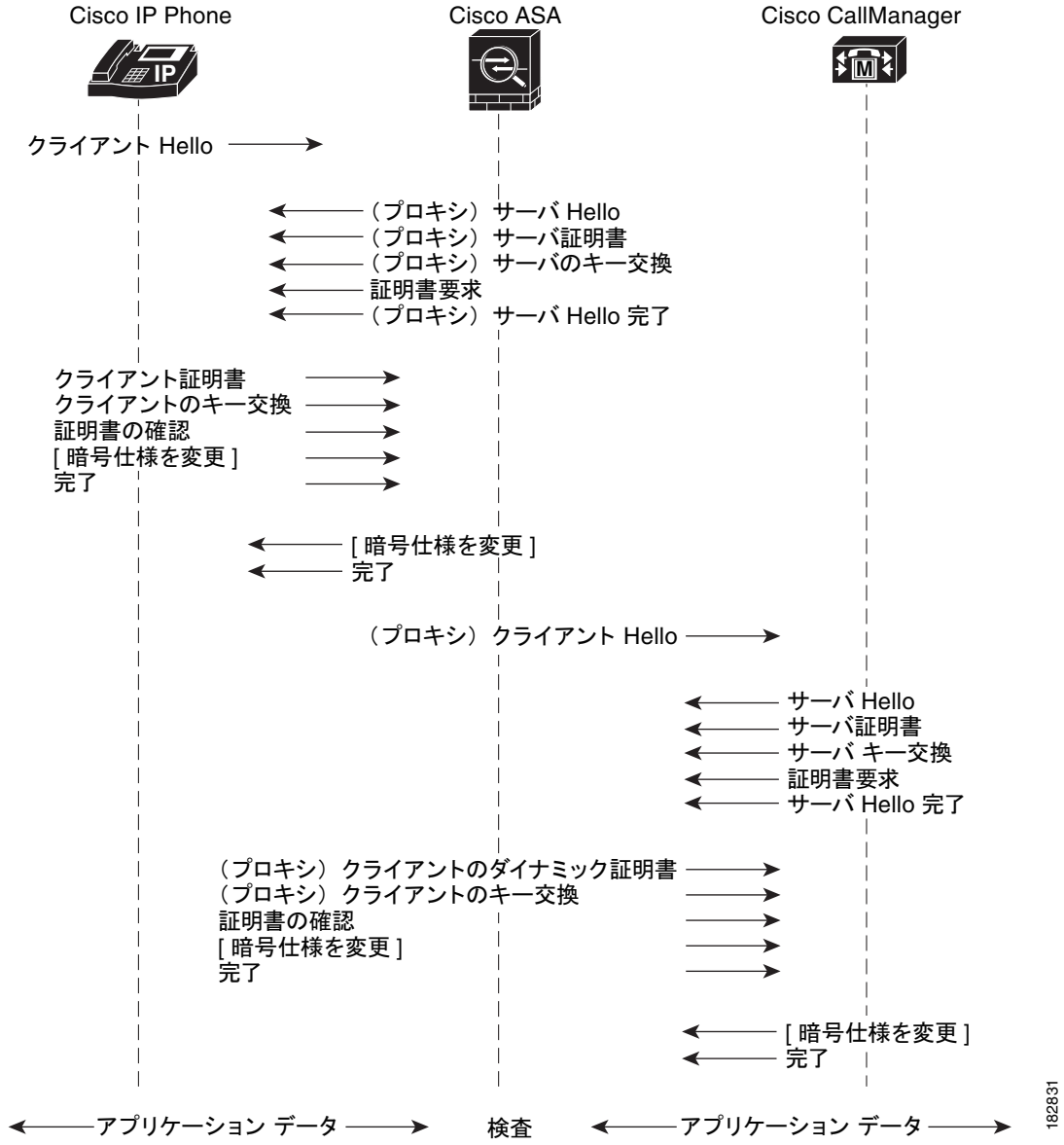
エンドツーエンド暗号化では、ネットワーク セキュリティ アプライアンスがメディアやシグナリング トラフィックに対して「受信停止」になることがよくあります。これにより、アクセス コントロールや脅威回避セキュリティの機能が低下する場合があります。このように可視性が失われると、ファイアウォール機能と暗号化された音声間の相互運用性が失われ、企業では両方の主要なセキュリティ要件に対応できない状態が続く可能性があります。

ASA は、シスコ暗号化エンドポイントから Cisco Unified Communications Manager（Cisco UCM）までの暗号化されたシグナリングを代行受信して復号化し、必要な脅威回避とアクセス コントロールを適用します。また、Cisco UCM サーバへのトラフィックを再暗号化して機密性を保証することもできます。

通常、ASA の TLS プロキシ機能は、構内の統合された通信ネットワークに展開されます。このソリューションは、エンドツーエンド暗号化とファイアウォールを利用して Unified Communications Manager サーバを保護する構成に最も適しています。

図 17-1 のセキュリティ アプライアンスは、Cisco IP Phone と Cisco UCM の対話で、クライアントとサーバの両方のプロキシとして機能します。

図 17-1　TLS プロキシ フロー



統合された通信の暗号化されたシグナリングの復号化と検査

暗号化音声インスペクションを使用すると、セキュリティ アプライアンスは、音声シグナリング トラフィックの復号化、検査、変更（必要に応じて NAT フィックスアップの実行など）、および再暗号化を行う一方で、Skinny および SIP プロトコルに対する既存の VoIP インスペクション機能はすべて維持します。音声シグナリングが復号化されると、プレーンテキストのシグナリング メッセージが既存のインスペクション エンジンに渡されます。

セキュリティ アプライアンスは、Cisco IP Phone と Cisco UCM の間の TLS プロキシとして機能します。プロキシは、電話と Cisco UCM の間の音声通話に対しては透過的です。Cisco IP Phone は、登録の前に Cisco UCM から Certificate Trust List（CTL; 証明書信頼リスト）をダウンロードします。CTL

には、TFTP サーバや Cisco UCM サーバなど、電話が信頼すべきデバイスの ID（証明書）が含まれています。サーバ プロキシをサポートするには、CTL ファイルに、セキュリティ アプライアンスが Cisco UCM 用に作成した証明書が含まれている必要があります。セキュリティ アプライアンスが Cisco IP Phone に代わってコールをプロキシするには、セキュリティ アプライアンス上にある、認証局によって発行され、Cisco UCM が確認可能な証明書（電話のローカル ダイナミック証明書）を提示する必要があります。

TLS プロキシは、Cisco Unified CallManager Release 5.1 以降でサポートされています。ユーザは Cisco UCM のセキュリティ機能について詳しく知っておく必要があります。Cisco UCM のセキュリティの背景と詳細な説明については、次の Cisco Unified CallManager のマニュアルを参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/5_0/sec_vir/ae/sec504/index.htm

TLS プロキシは、暗号化レイヤに適用されるので、アプリケーション レイヤ プロトコル インスペクションを設定する必要があります。ユーザは ASA のインスペクション機能、特に Skinny インスペクションと SIP インスペクションについて詳しく知っておく必要があります。

TLS プロキシでサポートされる Cisco UCM および IP Phone

Cisco Unified Communications Manager

次のリリースの Cisco Unified Communications Manager が TLS プロキシでサポートされています。

- Cisco Unified CallManager バージョン 4.*x*
- Cisco Unified CallManager バージョン 5.0
- Cisco Unified CallManager バージョン 5.1
- Cisco Unified Communications Manager 6.1
- Cisco Unified Communications Manager 7.0
- Cisco Unified Communications Manager 8.0

Cisco Unified IP Phone

Cisco Unified IP Phones 7900 シリーズの次の IP Phone が TLS プロキシでサポートされています。

- Cisco Unified IP Phone 7985
- Cisco Unified IP Phone 7975
- Cisco Unified IP Phone 7971
- Cisco Unified IP Phone 7970
- Cisco Unified IP Phone 7965
- Cisco Unified IP Phone 7962
- Cisco Unified IP Phone 7961
- Cisco Unified IP Phone 7961G-GE
- Cisco Unified IP Phone 7960
- Cisco Unified IP Phone 7945
- Cisco Unified IP Phone 7942
- Cisco Unified IP Phone 7941
- Cisco Unified IP Phone 7941G-GE

- Cisco Unified IP Phone 7940
- Cisco Unified Wireless IP Phone 7921
- Cisco Unified Wireless IP Phone 7925
- Cisco IP Communicator（CIPC）ソフトウェア電話

TLS プロキシのライセンス

ASA でサポートされる暗号化音声インスペクション機能の TLS プロキシには、Unified Communications Proxy ライセンスが必要です。

次の表に、Unified Communications Proxy ライセンスの詳細をプラットフォーム別に示します。

（注） この機能は、ペイロード暗号化機能のないモデルでは使用できません。

モデル	ライセンス要件[1]
ASA 5505	基本ライセンスと Security Plus ライセンス：2 セッション。 *オプション ライセンス：24 セッション。*
ASA 5510	基本ライセンスと Security Plus ライセンス：2 セッション。 *オプション ライセンス：24、50、または 100 セッション。*
ASA 5520	基本ライセンス：2 セッション。 *オプション ライセンス：24、50、100、250、500、750、または 1000 セッション。*
ASA 5540	基本ライセンス：2 セッション。 *オプション ライセンス：24、50、100、250、500、750、1000、または 2000 セッション。*
ASA 5550	基本ライセンス：2 セッション。 *オプション ライセンス：24、50、100、250、500、750、1000、2000、または 3000 セッション。*
ASA 5580	基本ライセンス：2 セッション。 *オプション ライセンス：24、50、100、250、500、750、1000、2000、3000、5000、または 10,000 セッション。*[2]
ASA 5512-X	基本ライセンス：2 セッション。 *オプション ライセンス：24、50、100、250、または 500 セッション。*
ASA 5515-X	基本ライセンス：2 セッション。 *オプション ライセンス：24、50、100、250、または 500 セッション。*
ASA 5525-X	基本ライセンス：2 セッション。 *オプション ライセンス：24、50、100、250、500、750、または 1000 セッション。*
ASA 5545-X	基本ライセンス：2 セッション。 *オプション ライセンス：24、50、100、250、500、750、1000、または 2000 セッション。*
ASA 5555-X	基本ライセンス：2 セッション。 *オプション ライセンス：24、50、100、250、500、750、1000、2000、または 3000 セッション。*

モデル	ライセンス要件[1]
ASA 5585-X（SSP-10）	基本ライセンス：2 セッション。 *オプション ライセンス：24、50、100、250、500、750、1000、2000、または 3000 セッション。*
ASA 5585-X（SSP-20、-40、または -60）	基本ライセンス：2 セッション。 *オプション ライセンス：24、50、100、250、500、750、1000、2000、3000、5000、または 10,000 セッション。*[2]
ASASM	基本ライセンス：2 セッション。 *オプション ライセンス：24、50、100、250、500、750、1000、2000、3000、5000、または 10,000 セッション。*[2]

1. 次のアプリケーションでは、接続時に TLS プロキシ セッションを使用します。これらのアプリケーションで使用される各 TLS プロキシ セッション（およびこれらのアプリケーションのみ）は UC ライセンスの制限に対してカウントされます。
   - 電話プロキシ
   - プレゼンス フェデレーション プロキシ
   - 暗号化音声インスペクション

   TLS プロキシ セッションを使用するその他のアプリケーション（ライセンスが不要な Mobility Advantage Proxy、個別の IME ライセンスが必要な IME など）では、UC 制限に対してカウントしません。

   UC アプリケーションによっては、1 つの接続に複数のセッションを使用する場合があります。たとえば、プライマリとバックアップの Cisco Unified Communications Manager を電話に設定した場合は、TLS プロキシ接続が 2 つあるため、UC Proxy セッションも 2 つ使用されます。

   [Configuration] > [Firewall] > [Unified Communications] > [TLS Proxy] ペインを使用して個別に TLS プロキシの制限を設定します。デフォルトの TLS プロキシ制限よりも高い UC ライセンスを適用する場合、ASA では、その UC 制限に一致するように TLS プロキシの制限が自動的に設定されます。UC ライセンスの制限よりも TLS プロキシ制限が優先されます。TLS プロキシ制限を UC ライセンスよりも少なく設定すると、UC ライセンスですべてのセッションを使用できません。

   注：「K8」で終わるライセンス製品番号（たとえばユーザ数が 250 未満のライセンス）では、TLS プロキシ セッション数は 1000 までに制限されます。「K9」で終わるライセンス製品番号（たとえばユーザ数が 250 以上のライセンス）では、TLS プロキシの制限はコンフィギュレーションに依存し、モデルの制限が最大数になります。K8 と K9 は、エクスポートについてそのライセンスが制限されるかどうかを示します。K8 は制限されず、K9 は制限されます。

   注：設定をクリアすると、TLS プロキシ制限がモデルのデフォルトに設定されます。このデフォルトが UC ライセンスの制限よりも低い場合、制限を再度引き上げるようにエラー メッセージが表示されます（ASDM の [TLS Proxy] ペインを使用します）。フェールオーバーを使用して、プライマリ ユニットで [File] > [Save Running Configuration to Standby Unit] を使用して設定の同期を強制する場合、**clear configure all** コマンドがセカンダリ ユニットに自動的に生成されるので、セカンダリ ユニットに警告メッセージが表示されることがあります。コンフィギュレーションの同期によりプライマリ装置の TLS プロキシ制限の設定が復元されるため、この警告は無視できます。

   接続には、SRTP 暗号化セッションを使用する場合もあります。
   - K8 ライセンスでは、SRTP セッション数は 250 までに制限されます。
   - K9 ライセンスに制限はありません。

   （注）メディアの暗号化/復号化を必要とするコールだけが、SRTP 制限に対してカウントされます。コールに対してパススルーが設定されている場合は、両方のレッグが SRTP であっても、SRTP 制限に対してカウントされません。
2. 10,000 セッション UC ライセンスの場合、組み合わせたセッション数は合計 10,000 までですが、電話プロキシ セッションの最大数は 5000 です。

表 17-1 に、TLS セッションのデフォルト数と最大数の詳細をプラットフォーム別に示します。

表 17-1　セキュリティ アプライアンス上での TLS セッションのデフォルト数と最大数

セキュリティ アプライアンス プラットフォーム	TLS セッションのデフォルト数	TLS セッションの最大数
ASA 5505	10	80
ASA 5510	100	200
ASA 5520	300	1200
ASA 5540	1000	4500
ASA 5550	2000	4500
ASA 5580	4000	13,000

ライセンスの詳細については、一般的な操作のコンフィギュレーション ガイドの Chapter 3, “Managing Feature Licenses for Cisco ASA Version 9.1,” を参照してください。

暗号化音声インスペクションの TLS プロキシの前提条件

TLS プロキシを設定する前に、次の前提条件を満たす必要があります。

- TLS プロキシを設定する前に、セキュリティ アプライアンスの時刻を設定する必要があります。手動で時刻を設定し、時刻を表示するには、**clock set** コマンドと **show clock** コマンドを使用します。セキュリティ アプライアンスでは Cisco Unified CallManager クラスタと同じ NTP サーバを使用することをお勧めします。セキュリティ アプライアンスと Cisco Unified CallManager サーバの間で時刻が同期していないと、証明書確認が失敗し、その結果、TLS ハンドシェイクが失敗する場合があります。
- Cisco Unified CallManager と相互運用するには、3DES-AES ライセンスが必要です。AES は、Cisco Unified CallManager と Cisco IP Phone で使用されるデフォルトの暗号です。
- Cisco UCM に保存されている次の証明書をインポートします。ASA で電話プロキシを使用するには、これらの証明書が必要です。
  - Cisco_Manufacturing_CA
  - CAP-RTP-001
  - CAP-RTP-002
  - CAPF 証明書（任意）

    LSC プロビジョニングが必要な場合や、IP 電話の LSC がイネーブルになっている場合は、Cisco UCM から CAPF 証明書をインポートする必要があります。Cisco UCM に CAPF 証明書が複数ある場合は、それらのすべてを ASA にインポートする必要があります。

  第 16 章「Cisco 電話プロキシの設定」を参照してください。たとえば、電話プロキシで IP 電話の証明書を検証するには、CA 製造業者証明書が必要です。

暗号化音声インスペクションの TLS プロキシの設定

この項では、次のトピックについて取り上げます。

- 「[TLS Proxy] ペインの設定」（P.17-8）
- 「TLS Proxy インスタンスの追加」（P.17-9）

CTL Provider

[CTL Provider] オプションは、Certificate Trust List（CTL）プロバイダー サービスを設定するために使用します。

[CTL Provider] ペインでは、Certificate Trust List プロバイダー サービスを定義および設定して、暗号化トラフィック インスペクションをイネーブルにできます。

フィールド

- [CTL Provider Name]：CTL プロバイダー名を一覧表示します。
- [Client Details]：クライアントの名前と IP アドレスを一覧表示します。
  - [Interface Name]：定義されているインターフェイス名を一覧表示します。
  - [IP Address]：定義されているインターフェイス IP アドレスを一覧表示します。
- [Certificate Name]：エクスポートする証明書を一覧表示します。
- [Add]：CTL プロバイダーを追加します。
- [Edit]：CTL プロバイダーを編集します。
- [Delete]：CTL プロバイダーを削除します。

Add/Edit CTL Provider

[Add/Edit CTL Provider] ダイアログボックスでは、CTL プロバイダーのパラメータを定義できます。

フィールド

- [CTL Provider Name]：CTL プロバイダー名を指定します。
- [Certificate to be Exported]：クライアントにエクスポートする証明書を指定します。
  - [Certificate Name]：クライアントにエクスポートする証明書の名前を指定します。
  - [Manage]：ID 証明書を管理します。
- [Client Details]：接続を許可するクライアントを指定します。
  - [Client to be Added]：クライアント リストに追加するクライアント インターフェイスと IP アドレスを指定します。

    [Interface]：クライアント インターフェイスを指定します。

    [IP Address]：クライアント IP アドレスを指定します。

    [Add]：クライアント リストに新しいクライアントを追加します。

    [Delete]：クライアント リストから選択したクライアントを削除します。

- [More Options]：TLS ハンドシェイク中に通知または照合する使用可能でアクティブなアルゴリズムを指定します。
  - [Parse the CTL file provided by the CTL Client and install trustpoints]：このオプションでインストールされたトラストポイントの名前には「_internal_CTL_」というプレフィックスがつきます。ディセーブルにした場合、各 CallManager サーバと CAPF 証明書を手動でインポートおよびインストールする必要があります。
  - [Port Number]：CTL プロバイダーがリッスンするポートを指定します。ポートは、クラスタの CallManager サーバがリッスンするポート（[CallManager administration] ページの [Enterprise Parameters] で設定されたもの）と同じである必要があります。デフォルト値は 2444 です。
  - [Authentication]：クライアントがプロバイダーの認証を受けるためのユーザ名とパスワードを指定します。

    [Username]：クライアントのユーザ名。

    [Password]：クライアントのパスワード。

    [Confirm Password]：クライアントのパスワード。

[TLS Proxy] ペインの設定

（注）　この機能は、適応型セキュリティ アプライアンスのバージョン 8.1.2 に対してはサポートされていません。

TLS Proxy を設定するには、[Configuration] > [Firewall] > [Unified Communications] > [TLS Proxy] ペインを使用します。

TLS Proxy を設定すれば、TLS Proxy を使用して、Cisco CallManager と対話する SSL 暗号化 VoIP シグナリング（Skinny および SIP）の検査をイネーブルにし、次の Cisco Unified Communications の機能に対して ASA をイネーブルにできます。

- Presence Federation の一部である、Cisco Unified Presence Server（CUPS）の TLS Proxy
- Mobile Advantage の一部である、Cisco Unified Mobility Advantage（CUMA）の TLS Proxy
- 電話プロキシ

フィールド

- [TLS Proxy Name]：TLS Proxy 名を一覧表示します。
- [Server Proxy Certificate]：トラストポイントを一覧表示します。自己署名または証明書サーバに登録済みのいずれかになります。
- [Local Dynamic Certificate Issuer]：クライアント ダイナミック証明書またはサーバ ダイナミック証明書を発行するローカル認証局を一覧表示します。
- [Client Proxy Certificate]：TLS クライアントのプロキシ証明書を一覧表示します。ASA では、プロキシと TLS クライアント間のハンドシェイク中における TLS クライアントの認証に、クライアント プロキシ証明書が使用されます。この証明書は、自己署名の場合と、認証局に登録済みの場合と、またはサードパーティによって発行される場合があります。
- [Add]：[Add TLS Proxy Instance Wizard] を起動して、TLS Proxy を追加します。TLS Proxy のインスタンスを作成する手順については、「TLS Proxy インスタンスの追加」（P.17-9）を参照してください。

- [Edit]：TLS Proxy を編集します。[Edit] パネル内の各フィールドは、TLS Proxy インスタンスを追加するときに表示されるフィールドとまったく同じです。「Edit TLS Proxy Instance – Server Configuration」（P.17-14）および「Edit TLS Proxy Instance – Client Configuration」（P.17-15）を参照してください。
- [Delete]：TLS Proxy を削除します。
- [Maximum Sessions]：サポートする TLS Proxy の最大セッション数を指定できます。
  - ASA がサポートする必要がある TLS Proxy の最大セッション数を指定します。
  - 最大セッション数の最小値は 1 です。最大値は、プラットフォームによって異なります。

    Cisco ASA 5505 適応型セキュリティ アプライアンスの場合は：10

    Cisco ASA 5510 セキュリティ アプライアンスの場合は：100

    Cisco ASA 5520 セキュリティ アプライアンスの場合は：300

    Cisco ASA 5540 セキュリティ アプライアンスの場合は：1000

    Cisco ASA 5550 適応型セキュリティ アプライアンスの場合は：2000

    Cisco ASA 5580 適応型セキュリティ アプライアンスの場合は：4000

（注） 最大セッション数は、すべての TLS Proxy セッションに対してグローバルに適用されます。

TLS Proxy インスタンスの追加

（注） この機能は、適応型セキュリティ アプライアンスのバージョン 8.1.2 に対してはサポートされていません。

[Add TLS Proxy Instance Wizard] を使用し、Cisco CallManager と対話する SSL 暗号化 VoIP シグナリング（Skinny および SIP）の検査をイネーブルにするため、また、ASA 上の Cisco Unified Communications 機能をサポートするために、TLS Proxy を追加します。

このウィザードは [Configuration] > [Firewall] > [Unified Communications] > [TLS Proxy] ペインから使用できます。

ステップ 1　[Configuration] > [Firewall] > [Unified Communications] > [TLS Proxy] ペインを開きます。

ステップ 2　新しい TLS Proxy インスタンスを追加するには、[Add] をクリックします。

[Add TLS Proxy Instance Wizard] が開きます。

ステップ 3　[TLS Proxy Name] フィールドで、TLS Proxy の名前を入力します。

ステップ 4　[Next] をクリックします。

[Add TLS Proxy Instance Wizard – Server Configuration] ダイアログボックスが開きます。ウィザードのこのステップで、Cisco Unified Call Manager（CUCM）サーバ、Cisco Unified Presence Server（CUPS）、または Cisco Unified Mobility Advantage（CUMA）サーバなどの、元の TLS サーバのサーバ プロキシ パラメータを設定します。「Add TLS Proxy Instance Wizard – Server Configuration」（P.17-10）を参照してください。

サーバ プロキシ パラメータを設定したら、ウィザードの案内に従ってクライアント プロキシ パラメータを設定し（「Add TLS Proxy Instance Wizard – Client Configuration」（P.17-11）を参照）、指示に従って、ASDM の外部で TLS Proxy を完全に機能させるための手順を完了させます（「Add TLS Proxy Instance Wizard – Other Steps」（P.17-13）を参照）。

Add TLS Proxy Instance Wizard – Server Configuration

（注）　この機能は、適応型セキュリティ アプライアンスのバージョン 8.1.2 に対してはサポートされていません。

[Add TLS Proxy Instance Wizard] を使用し、Cisco CallManager と対話する SSL 暗号化 VoIP シグナリング（Skinny および SIP）の検査をイネーブルにするため、また、ASA 上の Cisco Unified Communications 機能をサポートするために、TLS Proxy を追加します。

[Add TLS Proxy Instance Wizard] は、[Configuration] > [Firewall] > [Unified Communications] > [TLS Proxy] ペインから実行できます。

ステップ 1　[Add TLS Proxy Instance Wizard] の最初のステップを完了させます。「TLS Proxy インスタンスの追加」（P.17-9）を参照してください。

[Add TLS Proxy Instance Wizard – Server Configuration] ダイアログボックスが開きます。

ステップ 2　次のいずれかを実行して、サーバ プロキシ証明書を指定します。

- 新しい証明書を追加するには、[Manage] をクリックします。[Manage Identify Certificates] ダイアログボックスが開きます。

  Phone Proxy が混合モードの CUCM クラスタで動作している場合、[Manage Identify Certificates] ダイアログボックスの [Add] をクリックして CUCM 証明書をインポートする必要があります。一般的な操作のコンフィギュレーション ガイドの “Configuring Identity Certificates Authentication” section on page 38-55 を参照してください。

- 既存の証明書を選択するには、ドロップダウン リストから選択します。

  Phone Proxy の TLS Proxy を設定する場合、ファイル名が **_internal_PP_** から始まる証明書を選択します。Phone Proxy の CTL ファイルを作成すると、ASA では、TFTP ファイルに署名するために Phone Proxy が使用する内部トラストポイントが作成されます。トラストポイントには **_internal_PP_***ctl-instance_filename* という名前が付けられます。

サーバ プロキシ証明書は、TLS ハンドシェイク中に表示するトラストポイントを指定するために使用されます。トラストポイントは自己署名の場合と、ローカルでプロキシの証明書サービスに登録済みの場合があります。たとえば、Phone Proxy の場合、IP 電話とのハンドシェイク中に、Phone Proxy によってサーバ プロキシ証明書が使用されます。

ステップ 3　ASA の信頼ストアに TLS サーバ証明書をインストールして、ASA が、プロキシと TLS サーバ間の TLS ハンドシェイク中に、TLS サーバを認証できるようにするには、[Install TLS Server's Certificate] をクリックします。

[Manage CA Certificates] ダイアログボックスが開きます。一般的な操作のコンフィギュレーション ガイドの “Guidelines and Limitations” section on page 38-10 を参照してください。[Add] をクリックして、[Install Certificate] ダイアログボックスを開きます。一般的な操作のコンフィギュレーション ガイドの “Adding or Installing a CA Certificate” section on page 38-13 を参照してください。

Phone Proxy の TLS Proxy を設定する場合、[Install TLS Server's Certificate] をクリックして、Cisco Unified Call Manager（CUCM）証明書をインストールします。その結果、プロキシが、CUCM サーバの代わりに IP 電話を認証できるようになります。

ステップ 4　ASA に対して、TLS ハンドシェイク中に、証明書を表示し、TLS クライアントを認証することを要求するには、[Enable client authentication during TLS Proxy handshake] チェックボックスをオンにします。

Mobile Advantage（CUMC クライアントと CUMC サーバ）の TLS Proxy インスタンスを追加する場合、クライアントがクライアント証明書を送信できないときはチェックボックスをディセーブルにします。

ステップ 5　[Next] をクリックします。

[Add TLS Proxy Instance Wizard – Client Configuration] ダイアログボックスが開きます。ウィザードのこのステップでは、Mobile Advantage の CUMC クライアント、Presence Federation の CUP または MS LCS/OCS クライアント、または Phone Proxy の IP フォンなどの、元の TLS クライアントのクライアント プロキシ パラメータを設定します。「Add TLS Proxy Instance Wizard – Client Configuration」（P.17-11）を参照してください。

クライアント プロキシ パラメータを設定したら、ウィザードの指示に従って、ASDM の外部で TLS Proxy を完全に機能させるための手順を完了させます（「Add TLS Proxy Instance Wizard – Other Steps」（P.17-13）を参照）。

Add TLS Proxy Instance Wizard – Client Configuration

（注）　この機能は、適応型セキュリティ アプライアンスのバージョン 8.1.2 に対してはサポートされていません。

[Add TLS Proxy Instance Wizard] を使用し、Cisco CallManager と対話する SSL 暗号化 VoIP シグナリング（Skinny および SIP）の検査をイネーブルにするため、また、ASA 上の Cisco Unified Communications 機能をサポートするために、TLS Proxy を追加します。

このウィザードは [Configuration] > [Firewall] > [Unified Communications] > [TLS Proxy] ペインから使用できます。

ステップ 1　[Add TLS Proxy Instance Wizard] の最初の 2 つのステップを完了させます。「TLS Proxy インスタンスの追加」（P.17-9）および「Add TLS Proxy Instance Wizard – Client Configuration」（P.17-11）を参照してください。

[Add TLS Proxy Instance Wizard – Client Configuration] ダイアログボックスが開きます。

ステップ 2　TLS Proxy に対して使用するクライアント プロキシ証明書を指定するには、次を実行します。クライアント プロキシ証明書が 2 つのサーバ間で使用されている場合、このオプションを選択します。たとえば、Cisco Unified Presence Server（CUPS）を使用する Presence Federation の TLS Proxy を設定する場合、TLS クライアントと TLS サーバの両方が共にサーバとなります。

a.　[Specify the proxy certificate for the TLS Client...] チェックボックスをオンにします。

b.　証明書をドロップダウン リストから選択します。

または

新しいクライアント プロキシ証明書を作成するには、[Manage] をクリックします。[Manage Identify Certificates] ダイアログボックスが開きます。一般的な操作のコンフィギュレーション ガイドの “Configuring Identity Certificates Authentication” section on page 38-55 を参照してください。

（注）　CUCM クラスタの混合セキュリティ モードを使用している Phone Proxy の TLS Proxy を設定する場合、LDC Issuer を設定する必要があります。LDC Issuer は、クライアント ダイナミック証明書またはサーバ ダイナミック証明書を発行するローカル認証局を一覧表示します。

ステップ 3　TLS Proxy に対して使用する LDC Issuer を指定するには、次を実行します。[LDC Issuer] オプションを選択して設定すると、ASA が認証局となり、TLS クライアントに対して証明書を発行します。

a. [Specify the internal Certificate Authority to sign the local dynamic certificate for phones...] チェックボックスをオンにします。

b. [Certificates] オプション ボタンをオンにし、ドロップダウン リストから自己署名証明書を選択し、[Manage] をクリックして、新しい LDC Issuer を作成します。[Manage Identify Certificates] ダイアログボックスが開きます。一般的な操作のコンフィギュレーション ガイドの “Configuring Identity Certificates Authentication” section on page 38-55 を参照してください。

または

[Certificate Authority] オプション ボタンをオンにし、認証局（CA）を指定します。CA サーバを指定する場合、その CA サーバが、ASA で作成され、イネーブルになっている必要があります。CA サーバを作成およびイネーブルにするには、[Manage] をクリックします。[Edit CA Server Settings] ダイアログボックスが開きます。一般的な操作のコンフィギュレーション ガイドの “Authenticating Using the Local CA” section on page 38-63 を参照してください。

（注）　ローカル認証局の初期設定後にコンフィギュレーションを変更するには、ローカル認証局をディセーブルにします。

c. [Key-Pair Name] フィールドで、ドロップダウン リストからキー ペアを選択します。リストには、クライアント ダイナミック証明書が使用する、定義済みの RSA キー ペアが表示されます。生成時刻、使用方法、係数サイズ、キー データなど、キー ペアの詳細を表示するには、[Show] をクリックします。

または

新しいキー ペアを作成するには、[New] をクリックします。[Add Key Pair] ダイアログボックスが開きます。[Key Pair] フィールドの詳細については、一般的な操作のコンフィギュレーション ガイドの “Configuring Identity Certificates Authentication” section on page 38-55 を参照してください。

ステップ 4　[Security Algorithms] 領域で、TLS ハンドシェイク中に通知または照合する使用可能でアクティブなアルゴリズムを指定します。

- [Available Algorithms]：TLS ハンドシェイク中に通知または照合する使用可能なアルゴリズム（des-sha1、3des-sha1、aes128-sha1、aes256-sha1、null-sha1）を一覧表示します。

  [Add]：選択したアルゴリズムをアクティブ リストに追加します。

  [Remove]：選択したアルゴリズムをアクティブ リストから削除します。

- [Active Algorithms]：TLS ハンドシェイク中に通知または照合するアクティブなアルゴリズム（des-sha1、3des-sha1、aes128-sha1、aes256-sha1、null-sha1）を一覧表示します。クライアント プロキシ（サーバに対する TLS クライアントとして機能）の場合、2 つの TLS レッグ間の非対称暗号化方式のために、ユーザ定義のアルゴリズムで hello メッセージの元のアルゴリズムが置き換えられます。たとえば、Call Manager をオフロードするために、プロキシと Call Manager の間のレッグにはヌル暗号化が使用される場合があります。

[Move Up]：アルゴリズムをリストの上に移動します。

[Move Down]：アルゴリズムをリストの下に移動します。

ステップ 5　[Next] をクリックします。

[Add TLS Proxy Instance Wizard – Other Steps] ダイアログボックスが開きます。[Other Steps] ダイアログボックスの指示に従って、ASDM の外部で TLS Proxy を完全に機能させるための手順を完了させます（「Add TLS Proxy Instance Wizard – Other Steps」（P.17-13）を参照）。

Add TLS Proxy Instance Wizard – Other Steps

（注）　この機能は、適応型セキュリティ アプライアンスのバージョン 8.1.2 に対してはサポートされていません。

[Add TLS Proxy Instance Wizard] の最後のダイアログボックスでは、TLS Proxy を完全に機能させるために必要な追加の手順が示されます。特に、TLS Proxy のコンフィギュレーションを完成するためには、次のタスクを実行する必要があります。

- ローカル CA 証明書または LDC Issuer をエクスポートし、元の TLS サーバにインストールします。

  LDC Issuer をエクスポートするには、[Configuration] > [Firewall] > [Advanced] > [Certificate Management] > [Identity Certificates] > [Export] に移動します。一般的な操作のコンフィギュレーション ガイドの“Exporting an Identity Certificate” section on page 38-58 を参照してください。

- TLS Proxy の場合、TLS サーバと TLS クライアント間の Skinny および SIP インスペクションをイネーブルにします。「SIP インスペクション」（P.11-21）および「Skinny（SCCP）インスペクション」（P.11-33）を参照してください。（CUP を使用する）Presence Federation の TLS Proxy を設定する場合、SIP インスペクションだけをイネーブルにします。これは、この機能が SIP プロトコルだけをサポートしているからです。

- CUMA の TLS Proxy の場合、MMP インスペクションをイネーブルにします。

- ASA の内部認証局を使用して TLS クライアントの LDC Issuer に署名するには、次を実行します。

  – Cisco CTL クライアントを使用して、サーバ プロキシ証明書を CTL ファイルに追加し、CTL ファイルを ASA にインストールします。

    Cisco CTL クライアントの詳細については、『*Cisco Unified CallManager Security Guide*』の「Configuring the Cisco CTL Client」を参照してください。

    http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/security/5_0_4/secuauth.html

    CTL ファイルを ASA にインストールするには、[Configuration] > [Firewall] > [Unified Communications] > [CTL Provider] > [Add] に移動します。[Add CTL Provider] ダイアログボックスが開きます。このダイアログボックスを使用した CTL ファイルのインストールについては、「Add/Edit CTL Provider」（P.17-7）を参照してください。

  – CTL クライアントからの接続のための CTL プロバイダー インスタンスを作成します。「Add/Edit CTL Provider」（P.17-7）を参照してください。

Edit TLS Proxy Instance – Server Configuration

（注）　この機能は、適応型セキュリティ アプライアンスのバージョン 8.1.2 に対してはサポートされていません。

TLS Proxy によって、Cisco Call Manager と対話する SSL 暗号化 VoIP シグナリング（Skinny および SIP）の検査がイネーブルになり、ASA 上の Cisco Unified Communications 機能がサポートされます。

[Edit TLS Proxy – Server Configuration] タブを使用して、Cisco Unified Call Manager（CUCM）サーバ、Cisco Unified Presence Server（CUPS）、または Cisco Unified Mobility Advantage（CUMA）サーバなどの、元の TLS サーバのサーバ プロキシ パラメータを編集します。

ステップ 1　[Configuration] > [Firewall] > [Unified Communications] > [TLS Proxy] ペインを開きます。

ステップ 2　TLS Proxy インスタンスを編集するには、[Edit] をクリックします。

[Edit TLS Proxy Instance] ダイアログボックスが開きます。

ステップ 3　必要に応じて、[Server Configuration] タブをクリックします。

ステップ 4　次のいずれかを実行して、サーバ プロキシ証明書を指定します。

- 新しい証明書を追加するには、[Manage] をクリックします。[Manage Identify Certificates] ダイアログボックスが開きます。

  Phone Proxy が混合モードの CUCM クラスタで動作している場合、[Manage Identify Certificates] ダイアログボックスの [Add] をクリックして CUCM 証明書をインポートする必要があります。一般的な操作のコンフィギュレーション ガイドの “Configuring CA Certificate Authentication” section on page 38-12 を参照してください。

- 既存の証明書を選択するには、ドロップダウン リストから選択します。

  Phone Proxy の TLS Proxy を設定する場合、ファイル名が **_internal_PP_** から始まる証明書を選択します。Phone Proxy の CTL ファイルを作成すると、ASA では、TFTP ファイルに署名するために Phone Proxy が使用する内部トラストポイントが作成されます。トラストポイントには **_internal_PP_***ctl-instance_filename* という名前が付けられます。

サーバ プロキシ証明書は、TLS ハンドシェイク中に表示するトラストポイントを指定するために使用されます。トラストポイントは自己署名の場合と、ローカルでプロキシの証明書サービスに登録済みの場合があります。たとえば、Phone Proxy の場合、IP 電話とのハンドシェイク中に、Phone Proxy によってサーバ プロキシ証明書が使用されます。

ステップ 5　ASA の信頼ストアに TLS サーバ証明書をインストールして、ASA が、プロキシと TLS サーバ間の TLS ハンドシェイク中に、TLS サーバを認証できるようにするには、[Install TLS Server's Certificate] をクリックします。

[Manage CA Certificates] ダイアログボックスが開きます。一般的な操作のコンフィギュレーション ガイドの “Guidelines and Limitations” section on page 38-10 を参照してください。[Add] をクリックして、[Install Certificate] ダイアログボックスを開きます。一般的な操作のコンフィギュレーション ガイドの “Configuring CA Certificate Authentication” section on page 38-12 を参照してください。

Phone Proxy の TLS Proxy を設定する場合、[Install TLS Server's Certificate] をクリックして、Cisco Unified Call Manager（CUCM）証明書をインストールします。その結果、プロキシが、CUCM サーバの代わりに IP 電話を認証できるようになります。

ステップ 6　ASA に対して、TLS ハンドシェイク中に、証明書を表示し、TLS クライアントを認証することを要求するには、[Enable client authentication during TLS Proxy handshake] チェックボックスをオンにします。

Mobile Advantage（CUMC クライアントと CUMC サーバ）の TLS Proxy インスタンスを追加する場合、クライアントがクライアント証明書を送信できないときはチェックボックスをディセーブルにします。

ステップ 7　[Apply] をクリックして、変更内容を保存します。

Edit TLS Proxy Instance – Client Configuration

（注）　この機能は、適応型セキュリティ アプライアンスのバージョン 8.1.2 に対してはサポートされていません。

TLS Proxy によって、Cisco Call Manager と対話する SSL 暗号化 VoIP シグナリング（Skinny および SIP）の検査がイネーブルになり、ASA 上の Cisco Unified Communications 機能がサポートされます。

[Edit TLS Proxy] ダイアログボックス内の各フィールドは、TLS Proxy インスタンスを追加するときに表示されるフィールドとまったく同じです。[Edit TLS Proxy – Client Configuration] タブを使用して、IP phones、CUMA クライアント、Cisco Unified Presence Server（CUPS）、Microsoft OCS サーバなどの、元の TLS クライアントのクライアント プロキシ パラメータを編集します。

ステップ 1　[Configuration] > [Firewall] > [Unified Communications] > [TLS Proxy] ペインを開きます。

ステップ 2　TLS Proxy インスタンスを編集するには、[Edit] をクリックします。

[Edit TLS Proxy Instance] ダイアログボックスが開きます。

ステップ 3　必要に応じて、[Client Configuration] タブをクリックします。

ステップ 4　TLS Proxy に対して使用するクライアント プロキシ証明書を指定するには、次を実行します。クライアント プロキシ証明書が 2 つのサーバ間で使用されている場合、このオプションを選択します。たとえば、Cisco Unified Presence Server（CUPS）を使用する Presence Federation の TLS Proxy を設定する場合、TLS クライアントと TLS サーバの両方が共にサーバとなります。

a.　[Specify the proxy certificate for the TLS Client...] チェックボックスをオンにします。

b.　証明書をドロップダウン リストから選択します。

または

新しいクライアント プロキシ証明書を作成するには、[Manage] をクリックします。[Manage Identify Certificates] ダイアログボックスが開きます。一般的な操作のコンフィギュレーション ガイドの “Configuring Identity Certificates Authentication” section on page 38-55 を参照してください。

（注）　CUCM クラスタの混合セキュリティ モードを使用している Phone Proxy の TLS Proxy を設定する場合、LDC Issuer を設定する必要があります。LDC Issuer は、クライアント ダイナミック証明書またはサーバ ダイナミック証明書を発行するローカル認証局を一覧表示します。

ステップ 5　TLS Proxy に対して使用する LDC Issuer を指定するには、次を実行します。[LDC Issuer] オプションを選択して設定すると、ASA が認証局となり、TLS クライアントに対して証明書を発行します。

a.　[Specify the internal Certificate Authority to sign the local dynamic certificate for phones...] チェックボックスをオンにします。

b. [Certificates] オプション ボタンをオンにし、ドロップダウン リストから自己署名証明書を選択し、[Manage] をクリックして、新しい LDC Issuer を作成します。[Manage Identify Certificates] ダイアログボックスが開きます。一般的な操作のコンフィギュレーション ガイドの “Configuring Identity Certificates Authentication” section on page 38-55 を参照してください。

または

[Certificate Authority] オプション ボタンをオンにし、認証局（CA）を指定します。CA サーバを指定する場合、その CA サーバが、ASA で作成され、イネーブルになっている必要があります。CA サーバを作成およびイネーブルにするには、[Manage] をクリックします。[Edit CA Server Settings] ダイアログボックスが開きます。一般的な操作のコンフィギュレーション ガイドの “Authenticating Using the Local CA” section on page 38-63 を参照してください。

（注） ローカル認証局の初期設定後にコンフィギュレーションを変更するには、ローカル認証局をディセーブルにします。

c. [Key-Pair Name] フィールドで、ドロップダウン リストからキー ペアを選択します。リストには、クライアント ダイナミック証明書が使用する、定義済みの RSA キー ペアが表示されます。生成時刻、使用方法、係数サイズ、キー データなど、キー ペアの詳細を表示するには、[Show] をクリックします。

または

新しいキー ペアを作成するには、[New] をクリックします。[Add Key Pair] ダイアログボックスが開きます。[Key Pair] フィールドの詳細については、一般的な操作のコンフィギュレーション ガイドの “Configuring Identity Certificates Authentication” section on page 38-55 を参照してください。

ステップ 6　[Security Algorithms] 領域で、TLS ハンドシェイク中に通知または照合する使用可能でアクティブなアルゴリズムを指定します。

- [Available Algorithms]：TLS ハンドシェイク中に通知または照合する使用可能なアルゴリズム（des-sha1、3des-sha1、aes128-sha1、aes256-sha1、null-sha1）を一覧表示します。

  [Add]：選択したアルゴリズムをアクティブ リストに追加します。

  [Remove]：選択したアルゴリズムをアクティブ リストから削除します。

- [Active Algorithms]：TLS ハンドシェイク中に通知または照合するアクティブなアルゴリズム（des-sha1、3des-sha1、aes128-sha1、aes256-sha1、null-sha1）を一覧表示します。クライアント プロキシ（サーバに対する TLS クライアントとして機能）の場合、2 つの TLS レッグ間の非対称暗号化方式のために、ユーザ定義のアルゴリズムで hello メッセージの元のアルゴリズムが置き換えられます。たとえば、Call Manager をオフロードするために、プロキシと Call Manager の間のレッグにはヌル暗号化が使用される場合があります。

  [Move Up]：アルゴリズムをリストの上に移動します。

  [Move Down]：アルゴリズムをリストの下に移動します。

ステップ 7　[Apply] をクリックして、変更内容を保存します。

TLS プロキシ

この機能がサポートされるのは、ASA バージョン 8.0.x のうち 8.0.4 よりも前のものとバージョン 8.1 のみです。

（注）　この機能は、8.0.4 よりも前のバージョンの適応型セキュリティ アプライアンスおよびバージョン 8.1.2 に対しては、サポートされていません。

[TLS Proxy] オプションを使用して、Cisco CallManager と対話する SSL 暗号化 VoIP シグナリング（Skinny および SIP）の検査をイネーブルにします。

[TLS Proxy] ペインでは、Transaction Layer Security（TLS）Proxy を定義および設定して暗号化トラフィック インスペクションをイネーブルにできます。

フィールド

- [TLS Proxy Name]：TLS Proxy 名を一覧表示します。
- [Server]：トラストポイントを一覧表示します。自己署名または証明書サーバに登録済みのいずれかになります。
- [Local Dynamic Certificate Issuer]：クライアント ダイナミック証明書またはサーバ ダイナミック証明書を発行するローカル認証局を一覧表示します。
- [Local Dynamic Certificate Key Pair]：クライアント ダイナミック証明書またはサーバ ダイナミック証明書が使用する RSA キー ペアを一覧表示します。
- [Add]：TLS Proxy を追加します。
- [Edit]：TLS Proxy を編集します。
- [Delete]：TLS Proxy を削除します。
- [Maximum Sessions]：サポートする TLS Proxy の最大セッション数を指定できます。
  - ASA がサポートする必要がある TLS Proxy の最大セッション数を指定します。デフォルトでは、ASA がサポートするセッション数は 300 です。[Maximum number of sessions] オプションをイネーブルにします。
  - セッションの最大数：最小数は 1 です。最大値は、プラットフォームによって異なります。デフォルトは 300 です。

Add/Edit TLS Proxy

（注）　この機能は、8.0.4 よりも前のバージョンの適応型セキュリティ アプライアンスおよびバージョン 8.1.2 に対しては、サポートされていません。

[Add/Edit TLS Proxy] ダイアログボックスでは、TLS Proxy のパラメータを定義できます。

フィールド

- [TLS Proxy Name]：TLS Proxy 名を指定します。
- [Server Configuration]：プロキシ証明書名を指定します。
  - [Server]：TLS ハンドシェイク中に提示するトラストポイントを指定します。トラストポイントは自己署名の場合と、ローカルでプロキシの証明書サービスに登録済みの場合があります。
- [Client Configuration]：ローカル ダイナミック証明書の発行者とキー ペアを指定します。
  - [Local Dynamic Certificate Issuer]：クライアント ダイナミック証明書またはサーバ ダイナミック証明書を発行するローカル認証局を一覧表示します。

    [Certificate Authority Server]：認証局サーバを指定します。

[Certificate]：証明書を指定します。

[Manage]：ローカル認証局を設定します。初期設定の終了後にコンフィギュレーションを変更する場合は、ローカル認証局をディセーブルにします。

- [Local Dynamic Certificate Key Pair]：クライアント ダイナミック証明書が使用する RSA キー ペアを一覧表示します。

  [Key-Pair Name]：定義済みキー ペアを指定します。

  [Show]：生成時刻、使用方法、係数サイズ、キー データなど、キー ペアの詳細を表示します。

  [New]：新しいキー ペアを定義できます。

- [More Options]：TLS ハンドシェイク中に通知または照合する使用可能でアクティブなアルゴリズムを指定します。
  - [Available Algorithms]：TLS ハンドシェイク中に通知または照合する使用可能なアルゴリズム（des-sha1、3des-sha1、aes128-sha1、aes256-sha1、null-sha1）を一覧表示します。

    [Add]：選択したアルゴリズムをアクティブ リストに追加します。

    [Remove]：選択したアルゴリズムをアクティブ リストから削除します。
  - [Active Algorithms]：TLS ハンドシェイク中に通知または照合するアクティブなアルゴリズム（des-sha1、3des-sha1、aes128-sha1、aes256-sha1、null-sha1）を一覧表示します。クライアント プロキシ（サーバに対する TLS クライアントとして機能）の場合、2 つの TLS レッグ間の非対称暗号化方式のために、ユーザ定義のアルゴリズムで hello メッセージの元のアルゴリズムが置き換えられます。たとえば、CallManager をオフロードするために、プロキシと CallManager の間のレッグにはヌル暗号化が使用される場合があります。

    [Move Up]：アルゴリズムをリストの上に移動します。

    [Move Down]：アルゴリズムをリストの下に移動します。

暗号化音声インスペクションの TLS プロキシの機能履歴

表 17-2 に、この機能のリリース履歴を示します。

表 17-2　Cisco 電話プロキシの機能履歴

機能名	リリース	機能情報
TLS プロキシ	8.0(2)	TLS プロキシ機能が導入されました。