CHAPTER 3

デフォルトのセキュリティ

ここでは、次の内容について説明します。

概要

デフォルトのセキュリティは、次の自動セキュリティ機能を Cisco Unified IP Phone に提供します。

- 電話機設定ファイルの署名
- 電話機設定ファイルの暗号化に対するサポート
- Tomcat および他の Web サービス（MIDlet）での https

Cisco Unified Communications Manager リリース 8.0 では、CTL クライアントを実行せずに、これらのセキュリティ機能をデフォルトで使用できます。

（注） セキュアなシグナリングおよびメディアについては、引き続き CTL クライアントを実行して、ハードウェア eToken を使用することが必要です。

信頼検証サービス

Trust Verification Service（TVS; 信頼検証サービス）は、デフォルトのセキュリティの主要コンポーネントです。TVS を使用すると、HTTPS を確立しているときに、Cisco Unified IP Phone で EM サービス、ディレクトリ、および MIDlet などのアプリケーション サーバを認証できます。

TVS で提供される機能は次のとおりです。

- スケーラビリティ : Cisco Unified IP Phone のリソースは、信頼する証明書の数に影響されません。
- 柔軟性 : 信頼証明書の追加または削除が、システム内で自動的に反映されます。
- デフォルトのセキュリティ：メディアおよびシグナリングのセキュリティ以外の機能はデフォルトのインストールに含まれており、ユーザ操作は必要ありません。

（注）　セキュアなシグナリングおよびメディアを有効にするには、CTL クライアントが必要です。

TVS の概要

信頼検証サービスの基本概念は次のとおりです。

- TVS は Cisco Unified Communications Manager サーバで稼動して、Cisco Unified IP Phone の代わりに証明書を認証します。
- 信頼できる証明書をすべてダウンロードするのではなく、Cisco Unified IP Phone では TVS を信頼するだけで済みます。
- TVS 証明書およびいくつかのキー証明書が、Identity Trust List（ITL; ID 信頼リスト）という新しいファイルにまとめられます。
- ITL ファイルは、ユーザ操作なしで自動的に生成されます。
- ITL ファイルは、Cisco Unified IP Phone によってダウンロードされ、ここから信頼情報が取得されます。

初期信頼リスト

次のタスクを実行するには、Cisco Unified IP Phone に Initial Trust List（ITL; 初期信頼リスト）が必要です。

- 設定ファイルの署名の認証
- CAPF との安全な通話（設定ファイルの暗号化をサポートするための前提条件）
- TVS に対する信頼（特に https 証明書の認証）

Cisco Unified IP Phone に既存の CTL ファイルがない場合、最初の ITL ファイルが（CTL ファイルの場合と同様に）自動的に信頼されます。後続の ITL ファイルが同じ TFTP 秘密鍵で署名されているか、または TVS で署名者に応じた証明書を返すことができる必要があります。

Cisco Unified IP Phone に既存の CTL ファイルがある場合は、その CTL ファイルを使用して ITL ファイルの署名を認証します。

ITL ファイル

ITL ファイルには、初期信頼リストが格納されます。ITL ファイルは CTL ファイルと同じ形式で、基本的には CTL ファイルの小型版または縮小版です。ITL ファイルに適用される属性は、次のとおりです。

- CTL ファイルとは異なり、ITL ファイルはクラスタのインストール時にシステムによって自動的に作成され、内容の変更が必要になった場合には、自動的に更新されます。
- ITL ファイルに eToken は不要です。このファイルはソフト eToken（TFTP 秘密鍵）を使用します。
- ITL ファイルは、ブート時またはリセット時に CTL ファイル（ある場合）がダウンロードされた後すぐに、Cisco Unified IP Phone によってダウンロードされます。

ITL ファイルの内容

ITL ファイルには、次の証明書が含まれます。

- TFTP サーバの証明書。この証明書を使用すると、ITL ファイルの署名および電話機設定ファイルの署名を認証できます。
- クラスタ内のすべての TVS 証明書。この証明書を使用すると、電話機は TVS と安全に通信して証明書認証を要求できます。
- CAPF 証明書。この証明書を使用すると、設定ファイルの暗号化をサポートできます。ITL ファイルに必須というわけではありませんが（TVS で認証できる）、CAPF 証明書によって CAPF への接続が簡易化されます。

CTL ファイルと同様に、ITL ファイルには証明書ごとに 1 つのレコードが格納されます。各レコードの内容は次のとおりです。

- 証明書
- Cisco Unified IP Phone による簡易検索のために事前抽出された証明書フィールド
- 証明書権限（TFTP、CUCM、TFTP+CCM、CAPF、TVS、SAST）

TFTP 証明書は、次の 2 つの異なる権限を持つ 2 つの ITL レコードに含まれています。

- TFTP または TFTP+CCM 権限：設定ファイルの署名を認証します。
- SAST 権限：ITL ファイルの署名を認証します。

ITL ファイルと CTL ファイルの相互作用

Cisco Unified IP Phone では、クラスタのセキュリティ モード（非セキュアまたは混合モード）を確認するのに依然として CTL ファイルを使用します。CTL ファイルは、Cisco Unified Communications Manager のレコードに Cisco Unified Communications Manager の証明書を格納することで、クラスタ セキュリティ モードを追跡します。

ITL ファイルにも、クラスタ セキュリティ モードを示す情報が格納されます。

自動登録

クラスタが非セキュア モードの場合、システムによって自動登録がサポートされます。また、デフォルトの設定ファイルに対する署名も行われます。デフォルトのセキュリティをサポートしていない Cisco Unified IP Phone には、署名されていないデフォルトの設定ファイルが提供されます。

（注）　混合モードでは、自動登録はサポートされません。

サポートされている Cisco Unified IP Phone

Cisco Unified Reporting を使用すると、デフォルトのセキュリティをサポートしている Cisco Unified IP Phone のリストを取得できます。Cisco Unified Reporting を使用するには、次の手順に従います。

手順

ステップ 1　Cisco Unified Reporting のメイン ウィンドウから、[System Reports] をクリックします。

ステップ 2　[System Reports] リストから、[Unified CM Phone Feature List] をクリックします。

ステップ 3　[Feature] プルダウン メニューから、適切な機能を選択します。

ステップ 4　[Submit] をクリックします。

Cisco Unified Reporting の使用方法の詳細については、『*Cisco Unified Reporting Administration Guide*』を参照してください。

証明書の再生成

Cisco Unified Communications Manager の証明書の 1 つを再生成する場合には、この項の手順を実行する必要があります。

CAPF 証明書の再生成

CAPF 証明書を再生成するには、次の手順を実行します。

	手順	追加情報
ステップ 1	CAPF 証明書を再生成します。	『*Cisco Unified Communications Operating System Administration Guide*』の第 6 章「Security」を参照してください。
ステップ 2	CAPF サービスを再起動します。	「Certificate Authority Proxy Function サービスのアクティブ化」を参照してください。
ステップ 3	現在 TFTP サービスが稼動しているサーバで、このサービスを再起動します。	「TFTP サーバでの Cisco TFTP サービスの再起動」（P.3-6）を参照してください。
ステップ 4	Cisco Unified IP Phone をリセットします。	「すべての Cisco Unified IP Phone のリセット」（P.3-10）を参照してください。

TVS 証明書の再生成

TVS 証明書を再生成するには、次の手順を実行します。

（注）　クラスタ内のすべての TVS 証明書を再生成する場合、これらの手順は、すべての証明書を再生成した後に実行できます。

（注）　TVS および TFTP の両方の証明書を再生成する場合は、常にこれらの手順を実行してから TFTP 証明書を再生成します。この手順に従わないと、すべての Cisco Unified IP Phone から手動で ITL ファイルを削除することが必要になる場合があります。

	手順	追加情報
ステップ 1	TVS 証明書を再生成します。	『*Cisco Unified Communications Operating System Administration Guide*』の第 6 章「Security」を参照してください。
ステップ 2	現在 TFTP サービスが稼動しているサーバで、このサービスを再起動します。	詳細については、「TFTP サーバでの Cisco TFTP サービスの再起動」（P.3-6）を参照してください。
ステップ 3	Cisco Unified IP Phone をリセットします。	詳細については、「すべての Cisco Unified IP Phone のリセット」（P.3-10）を参照してください。

TFTP 証明書の再生成

TFTP 証明書を再生成するには、次の手順に従います。

（注） クラスタ内のすべての TFTP 証明書を再生成する場合、これらの手順は、すべての証明書を再生成した後に実行できます。

（注） TFTP および TVS の両方の証明書を再生成する場合は、常にこれらの手順を実行してから TVS 証明書を再生成します。この手順に従わないと、すべての Cisco Unified IP Phone から手動で ITL ファイルを削除することが必要になる場合があります。

	手順	追加情報
ステップ 1	TFTP 証明書を再生成します。	『*Cisco Unified Communications Operating System Administration Guide*』の第 6 章「Security」を参照してください。
ステップ 2	クラスタが混合モードの場合は、CTL クライアントを実行します。	第 4 章「Cisco CTL クライアントの設定」を参照してください。
ステップ 3	現在 Cisco TFTP サービスが稼動しているサーバで、このサービスを再起動します。	詳細については、「TFTP サーバでの Cisco TFTP サービスの再起動」（P.3-6）を参照してください。
ステップ 4	クラスタが混合モードの場合、次のサービスが起動されているときにはこれらのサービスを再起動します。 • Cisco CallManager • Cisco CTL Provider • Cisco CTL Manager	『*Cisco Unified Serviceability Administration Guide*』の第 11 章「Configuring Services」を参照してください。
ステップ 5	Cisco Unified IP Phone をリセットします。	詳細については、「すべての Cisco Unified IP Phone のリセット」（P.3-10）を参照してください。
ステップ 6	クラスタが EMCC 構成の一部の場合は、一括証明書プロビジョニングの手順を繰り返します。	『*Cisco Unified Communications Operating System Administration Guide*』の第 6 章「Security」を参照してください。

TFTP 証明書再生成後のシステムのバックアップ

ITL ファイルの信頼アンカーは、TFTP 秘密鍵というソフトウェア エンティティです。サーバがクラッシュすると鍵が失われ、電話機は新しい ITL ファイルを検証できなくなります。

Cisco Unified Communications Manager リリース 8.0 では、TFTP 証明書と秘密鍵の両方がディザスタ リカバリ システムによってバックアップされます。秘密鍵を保護するために、バックアップ パッケージは暗号化されます。サーバがクラッシュすると、以前の証明書および鍵が復元されます。

TFTP 証明書が再生成された場合は、常に新しいシステム バックアップを作成する必要があります。バックアップの手順については、『*Disaster Recovery System Administration Guide*』を参照してください。

Cisco Unified Communications Manager リリース 7.x からリリース 8.0 へのアップグレード

クラスタをリリース 7.x からリリース 8.0 にアップグレードするには、次の手順に従います。

手順

ステップ 1　通常のクラスタ アップグレード手順に従います。詳細については、『*Cisco Unified Communications Operating System Administration Guide*』の第 7 章「Software Upgrades」を参照してください。

ヒント　クラスタ内のすべてのノードを Cisco Unified Communications Manager リリース 8.0 にアップグレードした後、ここに示す手順に従って Cisco Unified IP Phone をシステムに登録する必要があります。

ステップ 2　次のいずれかのリリースを混合モードで使用している場合、CTL クライアントを実行する必要があります。

Cisco Unified Communications Manager リリース 7.1(2)

- 7.1(2) のすべての正規リリース
- 007.001(002.32016.001) よりも前の 712 のすべての ES リリース

Cisco Unified Communications Manager リリース 7.1(3)

- 007.001(003.21900.003) = 7.1(3a)su1a よりも前の 713 のすべての正規リリース
- 007.001(003.21005.001) よりも前の 713 のすべての ES リリース

（注）　CTL クライアントの実行方法の詳細については、第 4 章「Cisco CTL クライアントの設定」を参照してください。

TFTP サーバでの Cisco TFTP サービスの再起動

ステップ 3　Cisco Unified サービスアビリティで、[Tools] > [Control Center - Feature Services] の順に選択します。

[Control Center - Feature Services] ウィンドウが表示されます。

ステップ 4　Cisco Tftp サービスが稼動している各ノードで、このサービスを再起動します。

ステップ 5　TFTP がファイルを再作成するまで、5 分間待ちます。

すべての Cisco Unified IP Phone のリセット

（注）　電話機の設定を確実に最新の状態にするには、クラスタ内のすべての Cisco Unified IP Phone をリセットする必要があります。

ステップ 6　Cisco Unified Communications Manager の管理ページで、[システム (System)] > [エンタープライズパラメータ (Enterprise Parameters)] の順に選択します。

[エンタープライズパラメータ設定 (Enterprise Parameters Configuration)] ウィンドウが表示されます。

ステップ 7　[リセット (Reset)] をクリックします。

ステップ 8　Cisco Unified IP Phone が Cisco Unified Communications Manager に登録されるまで、10 分間待ちます。

クラスタのバックアップ

注意　クラスタを回復できるようにするには、Disaster Recovery System（DRS; ディザスタ リカバリ システム）を使用してクラスタをバックアップしておく必要があります。

ステップ 9　DRS を使用してクラスタをバックアップする方法については、『*Disaster Recovery System Administration Guide*』を参照してください。

8.0 よりも前のリリースへのクラスタのロールバック

クラスタを 8.0 よりも前の Cisco Unified Communications Manager のリリースにロールバックする前に、Prepare Cluster for Rollback to pre-8.0 エンタープライズ パラメータを使用して、クラスタをロールバックするための準備を行う必要があります。

注意　クラスタをロールバックするための準備を行わずに 8.0 よりも前の Cisco Unified Communications Manager のリリースにダウングレードすると、デフォルトのセキュリティを使用している Cisco Unified IP Phone は、Cisco Unified Communications Manager への登録時に CTL、ITL、および署名付き設定ファイルを要求するループに入ります。この状態の Cisco Unified IP Phone は設定ファイルの変更を認識できないため、システム内の個々の Cisco Unified IP Phone で、手動で ITL ファイルを削除することが必要になる場合があります。

クラスタをロールバックするための準備を行うには、クラスタ内の各サーバで次の手順に従います。

手順

ステップ 1　Cisco Unified Communications Manager の管理ページで、[システム (System)] > [エンタープライズパラメータ (Enterprise Parameters)] の順に選択します。

[エンタープライズパラメータ設定 (Enterprise Parameters Configuration)] ウィンドウが表示されます。

Prepare Cluster for Rollback to pre-8.0 エンタープライズ パラメータを [True] に設定します。

（注）　クラスタを 8.0 よりも前の Cisco Unified Communications Manager のリリースにロールバックする準備を行っている場合に限り、このパラメータを有効にします。https を使用する電話機サービス（エクステンション モビリティなど）は、このパラメータが有効になっている間は動作しません。ただし、このパラメータが有効になっていても、基本的な電話コールの発信および受信は引き続き実行できます。

すべてのノードでの Cisco 信頼検証サービスの再起動

（注）　この手順で示されている順番に従って、サービスを再起動する必要があります。

ステップ 2　Cisco Unified サービスアビリティで、[Tools] > [Control Center - Network Services] の順に選択します。

[Control Center - Network Services] ウィンドウが表示されます。

ステップ 3　Cisco 信頼検証サービスを再起動するには、ウィンドウの下部にある [Restart] ボタンをクリックします。

ステップ 4　クラスタ内のすべてのノードで Cisco 信頼検証サービスを再起動します。

TFTP サーバでの Cisco TFTP サービスの再起動

ステップ 5　Cisco Unified サービスアビリティで、[Tools] > [Control Center - Feature Services] の順に選択します。

[Control Center - Feature Services] ウィンドウが表示されます。

ステップ 6　Cisco Tftp サービスが稼動している各ノードで、このサービスを再起動します。

ステップ 7　TFTP がファイルを再作成するまで、5 分間待ちます。

すべての Cisco Unified IP Phone のリセット

（注）　電話機の設定を確実に最新の状態にするには、クラスタ内のすべての Cisco Unified IP Phone をリセットする必要があります。

ステップ 8　Cisco Unified Communications Manager の管理ページで、[システム (System)] > [エンタープライズパラメータ (Enterprise Parameters)] の順に選択します。

[エンタープライズパラメータ設定 (Enterprise Parameters Configuration)] ウィンドウが表示されます。

ステップ 9　[リセット (Reset)] をクリックします。

ステップ 10　Cisco Unified IP Phone が Cisco Unified Communications Manager に登録されるまで、10 分間待ちます。

以前のリリースへのクラスタの復元

ステップ 11　クラスタ内の各サーバを以前のリリースに戻します。クラスタを以前のバージョンに戻す方法の詳細については、『*Cisco Unified Communications Operating System Administration Guide*』の第 7 章「Software Upgrades」を参照してください。

ステップ 12　クラスタが以前のバージョンに切り替わるまで待ちます。

ステップ 13　次のいずれかのリリースを混合モードで使用している場合、CTL クライアントを実行する必要があります。

Cisco Unified Communications Manager リリース 7.1(2)

- 7.1(2) のすべての正規リリース
- 007.001(002.32016.001) よりも前の 712 のすべての ES リリース

Cisco Unified Communications Manager リリース 7.1(3)

- 007.001(003.21900.003) = 7.1(3a)su1a よりも前の 713 のすべての正規リリース
- 007.001(003.21005.001) よりも前の 713 のすべての ES リリース

（注） CTL クライアントの実行方法の詳細については、第 4 章「Cisco CTL クライアントの設定」を参照してください。

TFTP サーバでの Cisco TFTP サービスの再起動

ステップ 14　Cisco Unified サービスアビリティで、[Tools] > [Control Center - Feature Services] の順に選択します。

[Control Center - Feature Services] ウィンドウが表示されます。

ステップ 15　Cisco Tftp サービスが稼動している各ノードで、このサービスを再起動します。

ステップ 16　TFTP がファイルを再作成するまで、5 分間待ちます。

すべての Cisco Unified IP Phone のリセット

ステップ 17　Cisco Unified Communications Manager の管理ページで、[システム (System)] > [エンタープライズパラメータ (Enterprise Parameters)] の順に選択します。

[エンタープライズパラメータ設定 (Enterprise Parameters Configuration)] ウィンドウが表示されます。

ステップ 18　[リセット (Reset)] をクリックします。

ステップ 19　Cisco Unified IP Phone が Cisco Unified Communications Manager に登録されるまで、10 分間待ちます。

リリース 8.0 への切り替え

クラスタをリリース 7.x に戻した後でリリース 8.0 パーティションに切り替える場合は、この項の手順に従います。

手順

ステップ 1　クラスタを非アクティブのパーティションに切り替えるための手順に従います。詳細については、『*Cisco Unified Communications Operating System Administration Guide*』を参照してください。

ステップ 2　Cisco Unified Communications Manager の管理ページで、[システム (System)] > [エンタープライズパラメータ (Enterprise Parameters)] の順に選択します。

[エンタープライズパラメータ設定 (Enterprise Parameters Configuration)] ウィンドウが表示されます。

Prepare Cluster for Rollback to pre-8.0 エンタープライズ パラメータを [False] に設定します。

ステップ 3　次のいずれかのリリースを混合モードで使用していた場合、CTL クライアントを実行する必要があります。

Cisco Unified Communications Manager リリース 7.1(2)

- 7.1(2) のすべての正規リリース
- 007.001(002.32016.001) よりも前の 712 のすべての ES リリース

Cisco Unified Communications Manager リリース 7.1(3)

- 007.001(003.21900.003) = 7.1(3a)su1a よりも前の 713 のすべての正規リリース
- 007.001(003.21005.001) よりも前の 713 のすべての ES リリース

（注）　CTL クライアントの実行方法の詳細については、第 4 章「Cisco CTL クライアントの設定」を参照してください。

すべてのノードでの Cisco 信頼検証サービスの再起動

（注）　この手順で示されている順番に従って、サービスを再起動する必要があります。

ステップ 4　Cisco Unified サービスアビリティで、[Tools] > [Control Center - Network Services] の順に選択します。

[Control Center - Network Services] ウィンドウが表示されます。

ステップ 5　Cisco 信頼検証サービスを再起動するには、ウィンドウの下部にある [Restart] ボタンをクリックします。

ステップ 6　クラスタ内のすべてのノードで Cisco 信頼検証サービスを再起動します。

TFTP サーバでの Cisco TFTP サービスの再起動

ステップ 7　Cisco Unified サービスアビリティで、[Tools] > [Control Center - Feature Services] の順に選択します。

[Control Center - Feature Services] ウィンドウが表示されます。

ステップ 8　Cisco Tftp サービスが稼動している各ノードで、このサービスを再起動します。

ステップ 9　TFTP がファイルを再作成するまで、5 分間待ちます。

すべての Cisco Unified IP Phone のリセット

（注）　電話機の設定を確実に最新の状態にするには、クラスタ内のすべての Cisco Unified IP Phone をリセットする必要があります。

ステップ 10　Cisco Unified Communications Manager の管理ページで、[システム (System)] > [エンタープライズパラメータ (Enterprise Parameters)] の順に選択します。

[エンタープライズパラメータ設定 (Enterprise Parameters Configuration)] ウィンドウが表示されます。

ステップ 11　[リセット (Reset)] をクリックします。

ステップ 12　Cisco Unified IP Phone が Cisco Unified Communications Manager に登録されるまで、10 分間待ちます。