デフォルトのセキュリティ

デフォルトのセキュリティの概要

デフォルトのセキュリティ機能は、追加の設定要件なしでサポートされる Cisco Unified IP Phone の基本的なレベルのセキュリティを提供します。

この機能は、サポートされる IP 電話機に対して次のデフォルトのセキュリティを提供します。

- TFTP のデフォルト認証
- オプションの暗号化
- 証明書の検証

デフォルトのセキュリティは、次のコンポーネントを使用して非セキュアな環境で基本的なセキュリティを提供します。

- アイデンティティ信頼リスト（ITL）：このファイルは、クラスタのインストール時に TFTP サービスがアクティブ化された後、信頼の確立のために Cisco Unified IP Phone により使用されます。
- 信頼検証サービス：このサービスは、すべての Unified Communications Manager ノードで実行され、Cisco Unified IP Phone の証明書を認証します。TVS 証明書と他のいくつかのキー証明書が ITL ファイルにバンドルされます。

初期信頼リスト

初期信頼リスト（ITL）ファイルは、エンドポイントが Unified Communications Manager を信頼できるよう、最初のセキュリティに使用されます。ITL は明示的に有効にするセキュリティ機能を必要としません。ITL ファイルは、TFTP サービスがアクティブになり、クラスタがイン

ストールされると自動的に作成されます。Unified Communications Manager の TFTP サーバの秘密キーは、ITL ファイルの署名に使用されます。

Unified Communications Manager クラスタまたはサーバが非セキュアモードの場合、ITL ファイルはサポートされている Cisco Unified IP Phone ごとにダウンロードされます。CLI コマンド **admin:show itl** を使用して、ITL ファイルの内容を表示できます。

Cisco Unified IP Phone は、次のタスクを実行するために ITL ファイルが必要です。

- CAPF とセキュアに通信する。設定ファイル暗号化をサポートするための前提条件です。
- 設定ファイルの署名を認証する。
- TVS を使用する EM サービス、ディレクトリ、MIDlet などのアプリケーション サーバを認証します。

Cisco IP 電話 に CTL ファイルがまだ存在していない場合、最初の ITL ファイルが自動的に信頼されます。テレビは、署名者に対応する証明書を返すことができる必要があります。

Cisco IP 電話 に既存の CTL ファイルがある場合、ITL ファイルの署名の認証にその CTL ファイルが使用されます。

（注） SHA-1 または MD5 アルゴリズム値は、初期信頼リスト（ITL）ファイルの値に変更があった場合にのみ変更されます。ITL ファイルのチェックサム値を使用すると、Cisco IP 電話 と Unified Communications Manager クラスタの間にある ITL ファイルの差異を特定できます。ITL ファイルのチェックサム値は、ITL ファイルを変更した場合にのみ変更されます。

最初の信頼リスト (ITL) ファイルは、CTL ファイルと同じ形式になっています。ただし、これはより小さく、スリムのバージョンです。

ITL ファイルには次の属性が適用されます。

- TFTP サービスがアクティブ化され、クラスタをインストールすると、システムによって ITL ファイルが自動的に作成されます。内容が変更された場合、ITL ファイルは自動的に更新されます。
- ITL ファイルは eToken を必要としません。このファイルはソフト eToken（TFTP サーバの CallManager 証明書に関連付けられている秘密キー）を使用します。
- リセット中、再起動中、または CTL ファイルのダウンロード後に、Cisco Unified IP Phone は ITL ファイルをダウンロードします。

ITL ファイルには次の証明書が含まれています。

- ITLRecovery 証明書：この証明書は ITL ファイルに署名します。
- TFTP サーバの CallManager 証明書：この証明書を使用すると、ITL ファイル署名と電話機設定ファイル署名を認証できます。
- クラスタ上で使用可能なすべての TVS 証明書：これらの証明書を使用すると、電話機は TVS と安全に通信し、証明書認証を要求できます。

- CAPF 証明書: これらの証明書は、コンフィギュレーションファイルの暗号化をサポートします。CAPF 証明書は必ずしも ITL ファイル内に存在する必要はありません（TVS で認証可能）が、CAPF 証明書によって CAPF への接続が簡易化されます。

ITL ファイルには証明書ごとに 1 つのレコードが含まれます。各レコードの内容は次のとおりです。

- 証明書
- Cisco IP 電話 によるルックアップを容易にするための、事前に抽出された証明書フィールド。
- 証明書の権限（TFTP、CUCM、TFTP+CCM、CAPF、TV、SAST）

TFTP サーバの CallManager 証明書は、2 つの異なる権限を持つ次の 2 つの ITL レコード内に存在します。

- TFTP 権限 または TFTP および CCM 権限：設定ファイルの署名を認証する。
- SAST 権限：ITL ファイルの署名を認証する。

ITLRecovery 証明書の証明書管理の変更

- ITLRecovery の有効期間が 5 年間から 20 年間に延長され、より長い期間にわたって同じ ITLRecovery 証明書が使用されるようになりました。

（注） ITLRecovery 証明書のデフォルトの有効期間は5年です。ただし、ITLRecovery 証明書の有効期間を5、10、15、または20年に設定することもできます。Unified Communications Manager のアップグレード時に、新しいリリースに ITLRecovery 証明書がコピーされます。

- ITLRecovery 証明書を再生成する前に、CLI と GUI の両方に警告メッセージが表示されます。この警告メッセージは、トークンレス CTL を使用しており、CallManager 証明書を再生成する場合に、CTL ファイルに更新された CallManager 証明書があり、その証明書がエンドポイントに更新されていることを確認するために表示されます。

ITLRecovery 証明書

ITLRecovery Certificate 機能では、新しい **ITL ファイルステータス**ドロップダウンリストが導入され、管理者は古いITLを持つ電話機を識別して、それらの電話機に必要なアクションを実行できるようになりました。

一部の電話機は、ITL ファイルが更新されたときに最新の ITL ファイルを取得せず、古いものを保持します（CM 証明書の更新など）。システムは、不一致の ITL ファイルがある電話機の集中型レポートをユーザインターフェイスに表示します。

次に、さまざまなITLRecoveryシナリオを示します。

TFTP Service Activaton：

- TFTPサービスがアクティブになると、生成されたITLファイルのハッシュがサーバのホスト名とともにDBに保存されます。ITLがTFTPコードで更新されるたびに更新されます。
- TFTPホスト名がすでにテーブルに存在する場合は、生成されたITLハッシュが保存されている値と比較されます。
  - ITLハッシュが同じでない場合、新しいITLハッシュがDBで更新されます。
  - ITLハッシュが同じ場合、TFTPログに「Tftp Itl hash not changed」と表示されます。

デバイス登録とITLFileのダウンロード

- 電話機がUnified Communications Managerに登録されると、サーバに存在するITLFileの詳細（サーバのホスト名、ハッシュ、タイムスタンプ）がDBに存在しません。
- 電話機がUnified Communications Managerに登録されると、電話機に適用されたITLファイルの詳細を含むSIPアラームが送信されます。これは、DBに保存されているITLファイルのハッシュと比較されます。
  - ITLハッシュが同じ場合、デバイスハッシュ情報は新しいタイムスタンプで更新されます。
  - ITLハッシュが同じでない場合、報告されたITLハッシュとタイムスタンプがデバイスに対して更新されます。
- 電話機の登録が解除されると、そのデバイスの信頼ハッシュ情報が削除されます。

連携動作と制限事項

Unified Communications Managerクラスタに39を超える証明書がある場合、Cisco IP電話上のITLファイルサイズが64キロバイトを超えます。ITLファイルサイズが増加すると、電話でのITLの正常なロードに影響し、Unified Communications Managerでの電話登録が失敗することになります。

信頼検証サービス

ネットワーク内に多数の電話機があり、Cisco Unified IP Phoneのメモリも限られています。したがって、Unified Communications ManagerはTVSを介してリモート信頼ストアとして動作するため、各電話機に証明書信頼ストアを配置する必要はありません。Cisco Unified IP PhoneはCTLファイルまたはITLファイルを使用して署名または証明書を検証できないため、検証のためにTVSサーバに問い合わせることもできます。したがって、中央信頼ストアを持つことは、信頼ストアをすべてのCisco Unified IP Phoneに持つよりも管理が簡単です。

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。

TV には、次の機能があります。

- 拡張性：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は、システムに自動的に反映されます。
- デフォルトのセキュリティ：非メディアおよびシグナリングセキュリティ機能はデフォルトのインストールに含まれており、ユーザの介入は必要ではありません。

（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場合は、CTL ファイルを作成してから、クラスタを混合モードに設定する必要がありますCTL ファイルを作成し、クラスタを混合モードに設定するには、CLI コマンド **utils ctl set-cluster mixed-mode** を使用します。

TVS を説明する基本的な概念を次に示します。

- TVS は、Unified Communications Manager サーバ 上で実行され、Cisco IP 電話に代わって証明書を認証します。
- Cisco Unified IP Phone は、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、TVS を信頼する必要があるだけです。
- ITL ファイルはユーザの介入なしで自動的に生成されます。ITL ファイルは、Cisco Unified IP Phone によりダウンロードされ、信頼はそこからフローします。

認証、整合性、および許可

整合性と認証は、次の脅威から保護します。

- TFTP ファイルの操作 (整合性)
- 電話とUnified Communications Managerとの間で行われる呼処理シグナリングの変更（認証）
- 頭字語で定義している中間者攻撃（認証）
- 電話およびサーバの ID 盗難（認証）
- リプレイ アタック（ダイジェスト認証）

認可は、認証されたユーザ、サービス、またはアプリケーションが実行できることを指定します。1つのセッションで複数の認証方式と許可方式を実装できます。

イメージ認証

このプロセスでは、電話機にロードする前に、ファームウェアロードのバイナリイメージの改ざんを防止します。イメージが改ざんされると、電話の認証プロセスが失敗し、イメージは拒否されます。イメージ認証は、Unified Communications Managerインストール時に自動的にイン

ストールされた署名付きバイナリ ファイルを使用して実行されます。同様に、webからダウンロードしたファームウェアアップデートにも、署名付きバイナリイメージが提供されます。

デバイス認証

このプロセスは、通信デバイスのアイデンティティを検証し、エンティティが正当なものであることを確認します。

デバイス認証は、Unified Communications Manager サーバと、サポート対象の Cisco Unified IP 電話 、SIP トランク、または JTAPI/TAPI/CTI アプリケーション（サポートされている場合）との間で発生します。これらのエンティティ間での認証済み接続は、それぞれのエンティティが相手側エンティティの証明書を受け入れた場合にのみ発生します。相互認証では、相互証明書交換のこのプロセスについて説明します。

デバイス認証は、CiscoCTL ファイルの作成（Unified Communications Manager サーバノードとアプリケーションの認証時）、およびCertificate Authority Proxy Function（電話とJTAPI/TAPI/CTIアプリケーションの認証時）に依存します。

ヒント SIP トランク経由で接続される SIP ユーザは、CallManager 信頼ストアに SIP ユーザ エージェント証明書が含まれ、SIP ユーザ エージェントの信頼ストアに Cisco Unified Communications Manager 証明書が含まれる場合に、Cisco Unified Communications Manager で認証されます。CallManager 信頼ストアの更新の詳細については、この Unified Communications Manager リリースに対応した『*Cisco Unified Communications Manager* アドミニストレーション ガイド』を参照してください。

ファイル認証

このプロセスは、電話機がダウンロードするデジタル署名されたファイルを検証します。たとえば、設定、リングリスト、ロケール、および CTL ファイルなどです。ファイルが作成後に改ざんされていないことを確認するため、電話によって署名が検証されます。サポートされるデバイスの一覧については、「電話モデルのサポート」を参照してください。

クラスタを混合モードに設定すると、TFTP サーバは、呼出音リスト、ローカライズされた ca.cnf、およびリングリスト wav ファイル (sgn 形式) などの静的ファイルに署名します。Tftp サーバは、ファイルに対してデータの変更が発生したことを確認するたびに、< デバイス名 > のファイルに署名します。

キャッシュが無効になっている場合、TFTP サーバは署名されたファイルをディスクに書き込みます。保存されたファイルが変更されたことを TFTP サーバが確認すると、TFTP サーバはファイルを再署名します。ディスク上の新しいファイルは、削除された保存済みファイルを上書きします。電話が新しいファイルをダウンロードできるようになる前に、関連するデバイスを管理者が [Unified Communications Manager] で再起動する必要があります。

電話機は、TFTP サーバからファイルを受信すると、ファイルの署名を検証することによってファイルの整合性を検証します。電話機で認証済み接続を確立するには、次の基準が満たされていることを確認します。

- 証明書が電話内に存在していること。
- CTL ファイルが電話に存在し、そのファイルに Unified Communications Manager エントリと証明書が存在していること。
- 認証または暗号化のためにデバイスを設定しました。

シグナリング認証

シグナリング整合性とも呼ばれるこのプロセスは、TLSプロトコルを使用して、伝送中にシグナリング パケットが改ざんされていないことを検証します。

シグナリング認証は証明書信頼リスト（CTL）ファイルの作成に依存します。

ダイジェスト認証

SIP トランクと電話のこのプロセスによって、Unified Communications Manager が Unified Communications Manager に接続されるデバイスのアイデンティティに対するチャレンジを実行できます。チャレンジが実施されると、デバイスはユーザ名とパスワードに類似したダイジェスト クレデンシャルを検証用に Unified Communications Manager に提出します。提出されたクレデンシャルが、データベース内でそのデバイスに対して設定されているクレデンシャルと一致した場合、ダイジェスト認証は成功となり、Unified Communications Manager によって SIP 要求が処理されます。

（注） クラスタセキュリティモードはダイジェスト認証には影響しないことに注意してください。

（注） デバイスのダイジェスト認証を有効にすると、デバイスには一意のダイジェストユーザ ID とパスワードを登録する必要があります。

電話ユーザやアプリケーション ユーザには、Unified Communications Manager データベースで SIP ダイジェスト クレデンシャルを設定します。

- アプリケーションの場合は、[アプリケーションユーザの設定 (Application User Configuration)] ウィンドウでダイジェストクレデンシャルを指定します。
- SIP を実行している電話の場合は、[エンドユーザ (End User)] ウィンドウでダイジェスト認証クレデンシャルを指定します。ユーザを設定した後にクレデンシャルを電話に関連付けるには、[電話の設定 (Phone Configuration)] ウィンドウでダイジェストユーザ (エンドユーザ) を選択します。電話をリセットした後、ログイン情報は TFTP サーバから電話機に提供される電話設定ファイル内に存在します。TFTP ダウンロードでダイジェストクレデンシャルがクリアテキストで送信されないようにするには、暗号化された電話設定ファイルの設定に関連するトピックを参照してください。

- SIP トランクで受信した課題については、SIP レルムを設定します。これにより、レルムのユーザ名 (デバイスまたはアプリケーションユーザ) とダイジェストクレデンシャルが指定されます。

外部電話やSIP実行中のトランクに対するダイジェスト認証を有効化してダイジェストクレデンシャルを設定する場合、Unified Communications Managerによってユーザ名、パスワード、レルムのハッシュを含むクレデンシャルのチェックサムが計算されます。システムでは、MD5ハッシュの計算に、乱数であるナンス値が使用されます。値はUnified Communications Managerによって暗号化され、ユーザ名とチェックサムがデータベースに保存されます。

チャレンジを開始するために、Unified Communications Manager では SIP 401（Unauthorized）メッセージが使用されます。このメッセージのヘッダーにはナンスとレルムが含まれています。電話またはトランクの SIP デバイスセキュリティプロファイルで、nonce の有効期間を設定します。Nonce の有効期間は、nonce 値が有効なままになる分数を指定します。この時間が経過すると、その外部デバイスは Unified Communications Manager によって拒否され、新しい番号が生成されます。

（注） Unified Communications Manager は SIP トランク経由で着信した、回線側の電話やデバイスから発信された SIP コールに対してはユーザ エージェント サーバ（UAS）として動作し、SIP トランクに由来する SIP コールに対してはユーザ エージェント クライアント（UAC）として動作し、回線から回線へ、またはトランクからトランクへの接続に対してはバック ツーバック ユーザエージェント（B2BUA）として動作します。ほとんどの環境において、Unified Communications Manager は主に SCCP と SIP エンドポイントを接続する B2BUA として動作します。(SIP ユーザエージェントは、SIP メッセージを発信するデバイスまたはアプリケーションを表します)。

ヒント ダイジェスト認証では、整合性や機密性は提供されません。デバイスの整合性と機密性を確保するには、デバイスが TLS をサポートしている場合は、デバイスの TLS プロトコルを設定します。デバイスが暗号化をサポートしている場合は、デバイスセキュリティモードを暗号化として設定します。デバイスが暗号化された電話設定ファイルをサポートしている場合は、ファイルの暗号化を設定します。

電話のダイジェスト認証

電話のダイジェスト認証を有効化すると、キープアライブ メッセージを除き、SIP を実行中の電話に対するすべての要求に対して Unified Communications Manager はチャレンジを実施します。Unified Communications Manager は回線側電話からのチャレンジに応答しません。

応答を受信すると、Unified Communications Manager はデータベースに保存されたユーザ名のチェックサムを、応答ヘッダー内のクレデンシャルに対して検証します。

SIP を実行中の電話は Unified Communications Manager レルムに存在します。このレルムはインストール時に [Unified Communications Manager Administration] で定義されます。SIP レルムは、サービスパラメータ [SIP Station Realm] を使用して電話にチャレンジするように設定します。

各ダイジェストユーザは、レルムごとに1セットのダイジェストクレデンシャルを持つことができます。

ヒント エンドユーザのダイジェスト認証を有効にしても、ダイジェストクレデンシャルを設定しない場合、電話機は登録に失敗します。クラスタモードが非セキュアであり、かつダイジェスト認証が有効化されダイジェスト クレデンシャルが設定されている場合、ダイジェスト クレデンシャルが電話に送信され、Unified Communications Manager は依然としてチャレンジを開始します。

トランクのダイジェスト認証

トランクのダイジェスト認証を有効化すると、Unified Communications Manager は、SIP トランクを介して接続された SIP デバイスとアプリケーションからの SIP トランク要求に対してチャレンジを実施します。システムでは、チャレンジ メッセージ内で [Cluster ID] エンタープライズ パラメータが使用されます。SIP トランクを介して接続する SIP ユーザ エージェントは、[Unified Communications Manager] でデバイスまたはアプリケーションに設定された一意のダイジェスト クレデンシャルを使用して応答します。

Unified Communications Manager が SIP トランク要求を開始した場合、SIP トランクを介して接続された SIP ユーザ エージェントは Unified Communications Manager のアイデンティティにチャレンジを行えます。これらの着信チャレンジに対しては、要求されたクレデンシャルをユーザに提供するように SIP レルムを設定します。Unified Communications Manager が SIP 401（Unauthorized）または SIP 407（Proxy Authentication Required）メッセージを受信した場合、Unified Communications Manager はトランクを介して接続するレルムの暗号化パスワードおよびチャレンジメッセージに指定されているユーザ名の暗号化されたパスワードをルックアップします。Unified Communications Manager によってパスワードが復号され、ダイジェストが計算され、応答メッセージ内に表現されます。

ヒント レルムは、SIP トランクを介して接続するドメイン (xyz.com など) を表します。これは、要求の送信元を識別するのに役に立ちます。

SIP レルムを設定するには、SIP トランクのダイジェスト認証に関連するトピックを参照してください。Unified Communications Manager にチャレンジを行うことができる SIP トランク ユーザ エージェントごとに、Unified Communications Manager で SIP レルム、ユーザ名、パスワードを設定する必要があります。各ユーザエージェントは、レルムごとに1セットのダイジェストクレデンシャルを持つことができます。

認証

Unified Communications Manager では、許可プロセスを使用して、SIP が実行されている電話、SIP トランク、および SIP トランクの SIP アプリケーション要求からのメッセージについて、特定のカテゴリを制限します。

- SIP INVITE メッセージと in-dialog メッセージ、および SIP が実行されている電話の場合、Unified Communications Manager では、コーリング サーチ スペースおよびパーティションによって許可を与えます。
- 電話機からの SIP SUBSCRIBE 要求の場合、Unified Communications Manager では、プレゼンス グループへのユーザ アクセスに許可を与えます。
- SIP トランクの場合、Unified Communications Manager では、プレゼンス サブスクリプションおよび特定の非 INVITE SIP メッセージ（Out-of-Dialog REFER、Unsolicited NOTIFY、Replaces ヘッダー付き SIP 要求など）の許可を与えます。許可された SIP 要求をウィンドウで確認する場合は、[SIP トランクセキュリティプロファイルの設定 (SIP Trunk Security Profile Configuration)] ウィンドウで承認を指定します。

SIP トランクアプリケーションの許可を有効にするには、[SIP Trunk Security Profile] ウィンドウで [Enable Application Level Authorization] チェックボックスと [Digest Authentication] チェックボックスをオンにします。次に、[Application User Configuration] ウィンドウで [allowed SIP request] チェックボックスをオンにします。

SIP トランク認証とアプリケーションレベル認証の両方をイネーブルにすると、最初に sip トランクに対して認証が行われ、次に SIP アプリケーションユーザに対して許可が行われます。トランクの場合、Unified Communications Manager では、トランクのアクセス コントロール リスト（ACL）情報をダウンロードしてキャッシュします。ACL 情報は、着信 SIP 要求に適用されます。ACL で SIP 要求が許可されていない場合、コールは403禁止メッセージで失敗します。

ACL で SIP 要求が許可されている場合、Unified Communications Manager では、[SIP Trunk Security Profile] でダイジェスト認証が有効になっているかどうかを確認します。ダイジェスト認証が無効でアプリケーションレベルの認証も無効の場合、Unified Communications Manager では要求を処理します。ダイジェスト認証が有効な場合、Unified Communications Manager では、着信要求に認証ヘッダーが存在することを確認してから、ダイジェスト認証を使用して発信元アプリケーションを識別します。ヘッダーが存在しない場合、Unified Communications Manager では 401 メッセージでデバイスに対するチャレンジを行います。

アプリケーションレベルの ACL を適用する前に、Unified Communications Manager では、ダイジェスト認証で SIP トランク ユーザ エージェントを認証します。したがって、アプリケーションレベルの認証を実行するには、その前に、SIP トランクセキュリティプロファイルでダイジェスト認証を有効にする必要があります。

NMAP スキャン操作

Windows または Linux プラットフォームでネットワークマッパー (NMAP) スキャンプログラムを実行して、脆弱性スキャンを実行できます。NMAP は、ネットワーク調査またはセキュリティ監査のための無料のオープンソースユーティリティを表します。

（注） NMAP DP スキャンが完了するまでに最大18時間かかる場合があります。

構文

nmap -n -vv -sU -p <*port_range*> <*ccm_ip_address*>

定義：

-n：DNS 解決なし。検出されたアクティブ IP アドレスに対して逆引き DNS 解決を行わないよう NMAP に指示します。NMAP 組み込みパラレル スタブ リゾルバを使用しても DNS の処理は遅くなる可能性があるため、このオプションを使用するとスキャン時間を削減できます。

-v: 冗長性レベルを上げます。これにより、進行中のスキャンに関する詳細情報がNMAPによって出力されます。開いているポートが検出されると、システムは開いているポートを表示します。NMAPがスキャンに数分以上かかると推定した場合は、完了時間の推定値を提供します。このオプションは、冗長性をさらに高めるために2回以上使用してください。

-sU：UDP ポート スキャンを指定します。

-p: スキャンするポートを指定し、デフォルトを上書きします。個々のポート番号は、ハイフンで区切られた範囲であることに注意してください (たとえば、1-1023)。

ccm_ip_address：Cisco Unified Communications Manager の IP アドレス。

自動登録

システムは混合モードと非セキュアモードの両方で自動登録をサポートします。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」がサポートされていないCisco IP 電話には、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。

Cisco Unified Communications Manager と ITL ファイルを使用したクラスタ間での IP フォンの移行

Unified Communications Manager 8.0(1) 以降では、新しいデフォルトのセキュリティ機能と初期信頼リスト（ITL）ファイルが導入されました。この新機能を使用する場合は、異なるユニファイドCMクラスタ間で電話を移動する際には注意が必要です。また、移行のための適切な手順に従っていることを確認してください。

注意 正しい手順に従わないと、数千台の電話のITLファイルを手動で削除しなければならない状況が発生する可能性があります。

新しい ITL ファイルをサポートする Cisco IP 電話 では、Unified CM TFTP サーバからこの特別なファイルをダウンロードする必要があります。ITL ファイルが電話にインストールされると、設定ファイルおよびITLファイルの以降の更新では、以下のいずれかによる署名が必要となります。

- 電話機に現在インストールされている TFTP サーバ証明書
- クラスタのいずれかで TV サービスを検証できる TFTP 証明書。ITL ファイルにリストされているクラスタ内の TV サービスの証明書を確認できます。

この新しいセキュリティ機能により、電話を別のクラスタに移動する場合に、次の3つの問題が発生する可能性があります。

1. 新しいクラスタのITLファイルが現在のITLファイルの署名者によって署名されていないため、電話が新しいITLファイルや設定ファイルを受け入れることができない問題。
2. 電話の既存のITLにリストされているTVSサーバは、電話が新しいクラスタに移動すると接続できなくなる可能性があるという問題。
3. TVS サーバが証明書の検証のためにアクセス可能でも、古いクラスタ サーバには新しいサーバ証明書がない可能性があるという問題。

この3つの問題のうち1つ以上が発生した場合、考えられる解決策の1つは、クラスタ間を移動中のすべての電話からITLファイルを手作業で削除することです。ただし、この解決方法は電話の数が増えるにつれて大変な労力を必要とするため、望ましい解決策ではありません。

最も推奨されるオプションは、Cisco Unified CM エンタープライズ パラメータ [Prepare Cluster for Rollback to pre-8.0] を使用することです。このパラメータを [True] に設定すると、電話は空の TVS および TFTP 証明書セクションを含む特殊な ITL ファイルをダウンロードします。

電話に空の ITL ファイルがあると、（8.x 以前の Unified CM クラスタへの移行の場合）電話は署名のない設定ファイルをすべて受け入れます。また、（異なる Unified CM 8.x クラスタへの移行の場合）新しい ITL ファイルをすべて受け入れます。

空の ITL ファイルは、電話の **[Settings]** > **[Security]** > **[Trust List]** > **[ITL]** をチェックすることで確認できます。古いTVSやTFTPサーバが指定されていた場所には、空のエントリが表示されます。

新しい空の ITL ファイルをダウンロードできるまで、電話には古い Unified CM サーバにアクセスできる必要があります。

古いクラスタをオンラインのままにする予定の場合は、[Prepare cluster For Rollback to pre-8.0] エンタープライズパラメータを無効にして、デフォルトでセキュリティを復元します。

暗号化

ヒント　暗号化機能は、Unified Communications Managerをサーバにインストールするときに自動的にインストールされます。

ここでは、Unified Communications Manager のサポートする暗号化のタイプについて説明します。

セキュア エンド ユーザ ログイン クレデンシャル

Unified Communications Manager リリース 12.5(1) 以降、すべてのエンド ユーザ ログイン クレデンシャルは、強化されたセキュリティを提供するためにSHA2を使用してハッシュされてい

ます。Unified Communications Manager リリース 12.5(1) 以前は、エンド ユーザの ログイン クレデンシャルは、SHA1 のみを使用してハッシュされていました。Unified Communications Manager リリース 12.5(1) には 「 古いクレデンシャルのアルゴリズムを持つユーザの Unified CM 」 レポートも含まれます。このレポートは、Cisco Unified Reporting のページで入手できます。このレポートを使用すると、管理者は、パスワードまたは PIN が SHA1 でハッシュされているすべてのエンド ユーザをリストできます。

SHA1 でハッシュされているエンドユーザのすべてのパスワードまたは PIN は、最初にログインが成功したときに自動的に SHA2 に移行されます。SHA1 でハッシュされている（古い）クレデンシャルを持つエンド ユーザは、次のいずれかの方法を使用して、自身の PIN またはパスワードを更新できます。

- 電話機のエクス テンション モビリティまたはディレクトリのアクセスにログインして、PIN を更新します。
- Cisco Jabber、Cisco Unified Communications セルフケアポータル、または Cisco Unified CM Administration にログインして、パスワードを更新します。

レポートの生成方法の詳細については、*Cisco Unified CM Administration* のオンライン ヘルプを参照してください。

シグナリング暗号化

シグナリング暗号化により、デバイスと Unified Communications Manager サーバ間で送信されるすべての SIP と SCCP シグナリング メッセージが暗号化されるようにできます。

シグナリング暗号化によって、相手に関連する情報、相手が入力した DTMF 番号、コール ステータス、メディア暗号キーなどの情報が、意図しないアクセスや不正なアクセスから保護されます。

クラスタを混合モードに設定している場合、Unified Communications Manager によるネットワーク アドレス変換（NAT）はサポートされません。NAT はシグナリング暗号化では動作しません。

ファイアウォールで UDP ALG を有効にして、メディアストリームのファイアウォールトラバーサルを許可することができます。UDP ALG を有効にすると、ファイアウォールの信頼できる側のメディアソースが、ファイアウォールを介してメディアパケットを送信することにより、ファイアウォールを通過する双方向メディアフローを開くことができます。

ヒント ハードウェア DSP リソースはこのタイプの接続を開始できないため、ファイアウォールの外側に存在する必要があります。

シグナリング暗号化は、NAT トラバーサルをサポートしていません。NAT を使用する代わりに、LAN 拡張 Vpn の使用を検討してください。

メディア暗号化

セキュアリアルタイムプロトコル (SRTP) を使用するメディア暗号化により、目的の受信者だけがサポートされているデバイス間でメディアストリームを解釈できるようになります。メディア暗号化には、デバイスのメディアのマスターキーペアの作成、デバイスへのキー配布、キーが転送される間のキー配布の保護などが含まれます。Unified Communications Manager では、SIP トランクに加えて、主に IOS ゲートウェイと、ゲートキーパー制御および非ゲートキーパー制御トランクの Unified Communications Manager H.323 トランク向けに SRTP がサポートされています。

（注） Cisco Unified Communications Manager では、デバイスおよびプロトコルの違いに応じて異なる方法でメディア暗号化キーが処理されます。SCCP を実行しているすべての電話は、Unified Communications Manager からメディア暗号化キーを取得します。この場合、TLS 暗号化シグナリング チャネルによって電話へのメディア暗号化キーのダウンロードが保護されます。SIP を実行している電話は、それ自体のメディア暗号化キーを生成して保存します。Unified Communications Manager システムによって導出されたメディア暗号化キーは、暗号化されたシグナリング パス経由で、H.323 用の IPSec で保護されたリンク、および SCCP と SIP 向けの MGCP または暗号化 TLS リンクを介してゲートウェイに安全に送信されます。

デバイスは、SRTP を使用できる場合、ネゴシエーション時にステートを示す必要があります。デバイスがキャッシュされた以前のネゴシエーション SDP を同じコール内の異なるデバイスと使用する場合、CUCM は SRTP をサポートしません。

デバイスが SRTP をサポートしている場合、システムは SRTP 接続を使用します。少なくとも 1つのデバイスが SRTP をサポートしていない場合、システムは RTP 接続を使用します。SRTP から RTP へのフォールバックは、セキュアなデバイスからセキュアではないデバイスへの転送、トランスコーディング、保留音などの場合に発生する可能性があります。

セキュリティ対応デバイスのほとんどにおいて、認証とシグナリング暗号化は、メディアを暗号化するための最小要件です。つまり、デバイスがシグナリング暗号化と認証をサポートしていない場合、メディア暗号化は行われません。CiscoIOS ゲートウェイとトランクは、認証なしでメディア暗号化をサポートします。CiscoIOS ゲートウェイおよびトランクの場合は、SRTP 機能 (メディア暗号化) を有効にするときに IPSec を設定する必要があります。

警告 ゲートウェイとトランクの SRTP またはシグナリング暗号化を設定する前に、Cisco では、Cisco IOS の転送 CP ゲートウェイ、h.323 ゲートウェイ、および h.323/トランクを使用して ipsec を設定することを強く推奨します。セキュリティ関連情報がクリアテキストで送信されないようにするために、IPSec 設定に依存します。Unified Communications Manager は、IPSec 接続が正しく設定されていることを確認しません。IPSec を正しく設定しないと、セキュリティ関連の情報が公開される可能性があります。

SIP トランクは TLS に依存して、セキュリティ関連の情報がクリアテキストで送信されないようにします。

次の例では、SCCP コールと転送 CP コールのメディア暗号化を示します。

1. デバイス A とデバイス B は、メディアの暗号化と認証をサポートしており、Unified Communications Manager に登録されています。
2. デバイス A がデバイス B に対してコールを発信すると、Unified Communications Manager はキーマネージャ機能に対しメディアセッションマスター値のセットを2つ要求します。
3. 両方のデバイスが2つのセットを受信します。1セットはメディアストリーム用、デバイス A はデバイス B、メディアストリームの場合はデバイス B (デバイス A) です。
4. デバイス A はマスター値の最初のセットを使用して、メディアストリーム (デバイス A) を暗号化および認証するキーを導出します。
5. マスター値の2番目のセットを使用して、デバイス A はメディアストリーム (デバイス B) を認証および復号化するキーを導出します。
6. デバイス B は、逆の動作シーケンスでこれらのセットを使用します。
7. デバイスがキーを受信すると、デバイスは必要なキー導出を実行し、SRTP パケット処理が行われます。

（注） SIP を実行している電話と H.323 トランクまたはゲートウェイは、独自の暗号パラメータを生成し、Unified Communications Manager に送信します。

電話会議でのメディア暗号化については、会議リソースの保護に関連するトピックを参照してください。

SecureHashAlgorithm（SHA-2）のSCCPゲートウェイおよびハードウェア会議ブリッジ

Skinny Client Control Protocol （SCCP）では、Unified Communications Manager で Transport Layer Security（TLS）および Secured Real-Time Transport Protocol（SRTP）を使用するシグナリング完全性およびメディアの暗号化によって、Foreign Exchange Station（FXS）アナログエンドポイントが拡張されます。

Unified Communications Manager では、SCCP ゲートウェイ（アナログエンドポイント）およびハードウェア会議ブリッジ（TLS および SRTP）での SHA-2 アルゴリズムのサポートが強化されました。

前提条件

SCCP アナログ エンドポイントおよびハードウェア会議ブリッジの SHA-2 サポートは、次のバージョンおよびゲートウェイ バージョンで機能します。Unified Communications Manager

- Unified CM バージョン 14 SU1 以降。

- ゲートウェイ IOS バージョン：IOS XE 17.6.1 であり、セキュアなシグナリングのために TLS V1.2 をサポートするように設定する必要があります。

Note

- アナログエンドポイントの場合、音声ゲートウェイで STCAPP を有効にし、FXS ポートが音声ゲートウェイで使用可能になっていることを確認して、Unified Communications Manager でセキュアな FXS ポートを登録します。
- ハードウェア会議ブリッジの場合、トランスコーディングセッション、MTP セッション、および会議の組み合わせを同時にサポートするため、会議用の安全な DSPFARM プロファイルが必要です。

オーバーライド機能

Unified Communications Manager は、リソースの可用性に応じて、これらの要求を許可または拒否する、ゲートウェイからの会議またはトランスコーディングサービスを要求します。

Cisco Unified OS の管理のユーザーインターフェイスの **[暗号管理（Cipher Management）]** ページで暗号を設定していない場合は、**Enterprise Parameters** > **TLS Ciphers** のデフォルト設定が認識され、ネゴシエートされます。SCCP Cisco IP Phone との下位互換性を避けるために、SCCP FXS はデフォルトで SHA-1 TLS 暗号になっています。

Cisco Unified CM 管理の >**[システム（Systems）]**> **[企業パラメータ（Enterprise Parameter）]**> **[TLS 暗号（TLS Ciphers）]** フィールドでデフォルトオプションの **[すべてのサポートされている暗号（All Supported Ciphers）]** を選択した場合、次の暗号が TLS 接続のために Unified CM によって認識され、ネゴシエートされます。AEAD_AES_256_GCM、AEAD_AES_128_GCM、AES_CM_128_HMAC_SHA1_32、SHA1_80、F8_128_HMAC_SHA1_32、F8_SHA1_80。ただし、**[Cisco Unified OS の管理（Cisco Unified OS Administration）]** > **[セキュリティ（Security）]** > **[暗号管理（Cipher Management）]** が**すべての TLS** インターフェイスで「AES256-GCM-SHA384:AES256-SHA256」に設定されている場合、すべての SIP インターフェイスは「AES256-GCM-SHA384:AES256-SHA256」暗号のみをサポートし、企業パラメータ値を無視します。詳細については、「暗号文字列の構成」および「暗号の制限」セクションを参照してください。

次に例を示します。

1. **[Cisco Unified OS の管理（Cisco Unified OS Administration）]** > では **[暗号管理（Cipher Management）]** が **[デフォルト（Default）]** に設定されており、SHA-1 TLS がネゴシエートされます。
2. **Cisco Unified OS の管理** > では、**[暗号管理（Cipher Management）]** が **[すべて（ALL）]** に設定されており、SHA-2 TLS がネゴシエートされます。

セキュアコールのアルゴリズム

Unified Communications Managerは、セキュアコールで追加アルゴリズムのネゴシエーションを許可するように拡張されています。この機能強化の一環として、SCCP バージョンは Unified Communications Manager でバージョン 23 に引き上げられました。

新しい Open Receive Channel（ORC）および Start Media Transmission（SMT）バージョン 23 構造は、新しい SHA-2 暗号スイートのキーおよびソルトサイズをサポートするために MAX_KEY_SIZE = 32 で実装されます。

Note SHA-2 は、SCCP 電話、H323、および MGCP ではサポートされていません。

SCCP 経由で登録されたアナログエンドポイントのメディアを保護するには、次の手順を実行します。

- Unfied CM に登録されている 2 つの安全な SCCP アナログエンドポイント間のコールは、SHA-2 暗号のいずれか（AEAD_AES_256_GCM または AEAD_AES_128_GCM）とネゴシエートする必要があります。
- セキュアな SCCP アナログエンドポイントと、Unfied CM に登録されている SHA-2 サポートを持つ SIP エンドポイント間のコールは、SHA-2 暗号のいずれか（AEAD_AES_256_GCM または AEAD_AES_128_GCM）とネゴシエートします。

会議がハードウェア会議ブリッジでホストされているときにメディアを保護するには:

- SHA-2 をサポートする SCCP アナログ エンドポイントまたは SIP エンドポイントが SCCP ハードウェア会議ブリッジに接続されている場合、SHA-2 暗号は AEAD_AES_256_GCM または AEAD_AES_128_GCM をネゴシエートします。
- セキュアな電話会議中に、セキュアな SCCP 会議のエンドポイントにメディア確立アルゴリズムが混在している場合、会議ブリッジはその特定のコールレッグで対応するアルゴリズムをネゴシエートします。

TLS および SIP SRTP に対する AES 256 暗号化のサポート

Cisco Collaboration ソリューションは、Transport Layer Security（TLS）および Secure Real-time Transport Protocol（SRTP）を使用し、シグナリングとメディア暗号化を行います。現在、128 ビット暗号キーを使用した Advanced Encryption Standard (AES) は、暗号化暗号として使用されています。AES では、認証方式として Hash-based Message Authentication Code Secure Hash Algorithm-1（HMAC-SHA-1）も使用されます。これらのアルゴリズムは、必要な変化するセキュリティとパフォーマンスのニーズに合わせて効果的に拡張することはできません。セキュリティとパフォーマンスの要件の増大に対応するため、Next-Generation Encryption（NGE）での、暗号化、認証、デジタル署名、およびキー交換用のアルゴリズムとプロトコルが開発されています。また、TLS および NGE をサポートするセッション開始プロトコル (SIP) SRTP の AES 128 の代わりに、AES 256 暗号化サポートが提供されます。

AES 256 Encryption Support for TLS and SIP SRTP が、シグナリング暗号化とメディア暗号化での AES 256 暗号化のサポートに重点を置くために拡張されています。この機能は、Unified Communications Manager 上で実行されているアプリケーションが、SHA-2（Secure Hash Algorithm）標準規格および Federal Information Processing Standards（FIPS）に準拠する、AES-256 ベースの暗号を使用して TLS 1.2 接続を開始してサポートするために役立ちます。

この機能には、次の要件があります。

- SIP トランクと SIP 回線が開始する接続。
- Unified Communications Manager が SIP 回線と SIP トランクを通じた SRTP コール用にサポートする暗号化であること。

（注） このリリースでは、TLS 1.2 は SIP などの一部のインターフェイスでサポートされていますが、すべてのインターフェイスでサポートされているわけではありません。TLS 1.0 および1.1 は、コラボレーション展開で有効にしたままにしておくことをお勧めします。

TLS での AES 256 および SHA 2 のサポート

Transport Layer Security（TLS）プロトコルでは、2 つのアプリケーション間の通信の認証、データの整合性、および機密性が提供されます。TLS 1.2 はセキュア ソケット レイヤ（SSL）プロトコル バージョン 3.0 をベースにしていますが、これら 2 つのプロトコルに相互の互換性はありません。TLS はクライアント/サーバ モードで動作し、一方がサーバとして機能し、もう一方がクライアントとして機能します。SSL は、伝送制御プロトコル (TCP) レイヤとアプリケーションの間のプロトコル層として配置され、クライアントとサーバ間のセキュアな接続を形成し、ネットワークを介して安全に通信できるようにします。TLS を動作させるには、信頼性の高いトランスポート層プロトコルとして TCP が必要です。

Unified Communications Manager における、TLS 1.2 での AES 256 および SHA-2（Secure Hash Algorithm-2）のサポートは、SIP トランクおよび SIP 回線によって開始される接続を処理するための機能強化です。AES 256 および SHA-2 に準拠する、サポートされる暗号方式は次のとおりです。

- TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256: 暗号ストリングは ECDH-RSA-AES128-GCM-SHA256 です。
- TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384: 暗号ストリングは ECDH-RSA-AES256-GCM-SHA384 です。

定義：

- TLS は、Transport Layer Security です
- ECDH は楕円曲線 Diffie-hellman (アルゴリズム) です。
- RSA is Rivest Shamir Adleman (アルゴリズム)
- AES は、Advanced Encryption Standards です

• GCM は、Galois/Counter Mode です

新しくサポートされた暗号方式に加えて、Unified Communications Manager では、TLS_RSA_WITH_AES_128_CBC_SHA が引き続きサポートされています。この暗号方式の暗号ストリングは AES128-SHA です。

（注）
- Unified Communications Manager の証明書は、RSA に基づいています。
- Unified Communications Manager では、シスコの各エンドポイント（各電話）で、上記の TLS 1.2 用の新しい暗号方式はサポートされません。
- Unified Communications Manager において TLS 1.2 での AES 256 および SHA-2（Secure Hash Algorithm-2）のサポート機能強化を使用すると、Certificate Authority Proxy Function（CAPF）のデフォルトのキー サイズが 2048 ビットに増えます。

SRTP SIP コールシグナリングでの AES 256 のサポート

Secure Real time Transport Protocol (SRTP) は、リアルタイムトランスポートプロトコル (RTP) の音声およびビデオメディアと、それに対応するリアルタイムトランスポート制御プロトコル (RTCP) ストリームの両方に機密性とデータの整合性を提供する方法を定義します。SRTP は、暗号化およびメッセージ認証ヘッダーを使用してこの方式を実装します。SRTP では、暗号化は rtp パケットのペイロードにのみ適用され、RTP ヘッダーには適用されません。ただし、メッセージ認証は RTP のヘッダーと RTP のペイロードの両方に適用されます。また、メッセージ認証がヘッダー内の RTP のシーケンス番号に適用されるため、SRTP ではリプレイ アタックに対する保護も間接的に提供されます。SRTP は、暗号化方法として 128 ビットの暗号キーによる Advanced Encryption Standard（AES）を使用します。また、認証方式として、Hash-based Message Authentication Code Secure Hash Algorithm-1（HMAC-SHA-1）も使用します。

Unified Communications Manager では、SIP 回線と SIP トランクを通じた SRTP コール用の暗号方式がサポートされます。これらの暗号暗号方式は AEAD_AES_256_GCM と AEAD_AES_128_GCM であり、AEAD は関連データを使用して認証され、GCM は Galois/Counter モードです。これらの暗号方式は GCM に基づいています。これらの暗号方式が Session Description Protocol (SDP) に存在する場合、AES 128 および SHA-1 ベースの暗号方式よりも高いプライオリティで処理されます。シスコの各エンドポイント（電話）では、Unified Communications Manager に SRTP のために追加した、これらの新しい暗号方式はサポートされません。

新たにサポートされる暗号方式に加えて、Unified Communications Manager では次の暗号方式が引き続きサポートされます。

- AES_CM_128_HMAC_SHA1_80
- AES_CM_128_HMAC_SHA1_32
- F8_128_HMAC_SHA1_80

AES 256 暗号化は、次のコールでサポートされています。

- Sip 回線から SIP 回線へのコールシグナリング
- Sip 回線から SIP トランクへのシグナリング
- Sip トランクから SIP トランクへのシグナリング

Cisco Unified Communications Manager の要件

- SIP トランクおよび SIP 回線接続での TLS バージョン1.2 のサポートを使用できます。
- 暗号サポート: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (暗号ストリング ECDHE-AES256 SHA384) および TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (暗号ストリング ECDHE-AES128): TLS 1.2 接続が確立されたときに使用可能になります。これらの暗号方式は GCM に基づいており、SHA-2 カテゴリに準拠しています。
- Unified Communications Manager は TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 暗号方式と TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 暗号方式を使用して TLS 1.2 を開始します。ピアが TLS 1.2 をサポートしていない場合、Unified Communications Manager は既存の AES128-SHA 暗号方式を使用した TLS 1.0 にフォールバックします。
- SIP 回線および SIP トランクを介した SRTP コールは、GCM ベースの AEAD_AES_256_GCM と AEAD_AES_128_GCM の暗号方式をサポートします。

連携動作と制限事項

- Unified Communications Manager の要件は、SIP 回線と SIP トランク、および基本的な SIP 間コールのみに適用されます。
- 非 SIP プロトコルに基づくデバイスタイプは、サポートされている暗号を使用した TLS バージョンの既存の動作を引き続きサポートします。Skinny Call Control Protocol (SCCP) は、以前にサポートされていた暗号方式を使用した TLS 1.2 もサポートしています。
- Sip から非 SIP へのコールでは、引き続き AES 128 および SHA-1 ベースの暗号方式が使用されます。

AES 80 ビット認証サポート

Unified Communications Manager は、128 ビット暗号化キーと 80 ビット認証タグを保留音（MOH）、自動音声応答（IVR）、アナンシエータの暗号化アルゴリズムとして使用する Advanced Encryption Standard（AES）をサポートしています。デフォルトでは、80ビット認証タグをサポートする電話機は、AES_CM_128_HMAC_SHA1_80 crypto 暗号方式を使用して MOH、IVR、および警報を再生します。

電話機が IP Voice Media Streaming (IPVMS) に安全に接続すると、AES_CM_128_HMAC_SHA1_80 crypto cipher に優先順位が付与されます。電話機が80ビット認証をサポートしていない場合、AES_CM_128_HMAC_SHA1_32 暗号に戻ります。電話が 80 ビットまたは 32 ビットの認証タグのいずれかをサポートしていない場合は、Real-time Transport Protocol（RTP）でネゴシエーションを行います。

（注） SCCP 電話は 32 ビット認証タグしかサポートしていません。そのため、電話と IPVMS とのネゴシエーションは、AES_CM_128_HMAC_SHA1_32 暗号でのみ行われます。

電話 A が AES_CM_128_HMAC_SHA1_80 暗号化アルゴリズムをサポートし、電話 B が AES_CM_128_HMAC_SHA1_32 暗号化アルゴリズムをサポートしている場合、ユーザ A（電話 A）がユーザ B（電話 B）にダイヤルしユーザ B が保留にすると、ユーザ A は MOH に接続されます。電話 A は 80 ビット認証タグしかサポートしないため、電話 A と MOH のネゴシエーションは AES_CM_128_HMAC_SHA1_80 暗号を介して行われます。

ユーザ B（電話 B）がユーザ A（電話 A）にダイヤルし、ユーザ A が保留にする場合、電話 B は 32 ビット認証タグしかサポートしていないので、電話 B と MOH のネゴシエーションは AES_CM_128_HMAC_SHA1_32 暗号により行われます。

電話が 80 ビット認証タグをサポートする場合、電話と IVR またはアナンシエータとのネゴシエーションは AES_CM_128_HMAC_SHA1_80 で行われます。

次の表は、電話がサポートする暗号化アルゴリズムとネゴシエーション暗号を示しています。

表 *1*：電話機能とネゴシエートされた暗号方式の比較

電話がサポートする暗号化アルゴリズム	ネゴシエートされた暗号
AES_CM_128_HMAC_SHA1_32 と AES_CM_128_HMAC_SHA1_80	AES_CM_128_HMAC_SHA1_80
AES_CM_128_HMAC_SHA1_32	AES_CM_128_HMAC_SHA1_32
AES_CM_128_HMAC_SHA1_80	AES_CM_128_HMAC_SHA1_80
AES_CM_128_HMAC_SHA1_32 と AES_CM_128_HMAC_SHA1_80 以外	RTP に戻ります。

メディアストリーミングデバイスとの SRTP 暗号の不一致

セキュアコールが保留、IVR、またはアナンシエータアナウンスなどの機能を呼び出しているときに、リモートの発信者が打診転送を実行すると、新しいコールレッグは MOH、IVR、またはアナンシエータとは異なる暗号機能をサポートする場合があります。これにより、暗号の不一致が発生し、エンドポイントの SRTP フォールバックオプションに応じて、コールは非セキュア モードにドロップされるか、完全にドロップされます。**Unified Communications Manager** > **の [システム（System）]** > **[サービス パラメータ（Service Parameters）]** > **[サービスパラメータ設定（Service Parameter Configuration）]**ウィンドウで **[暗号化されていないコールをブロック（Block Unencrypted Calls）]** サービスパラメータが **[True]** に設定されている場合でも、セキュアコールはドロップされます。

Unified Communications Manager プラットフォームの新しい拡張機能により、Cisco IP Voice Media Streaming（IPVMS）デバイス（MOH、IVR、またはアナンシエータ）以降のコール機能を交換

するときに、すべての暗号方式がサポートされます。SRTP フォールバック構成はアクティブコールに影響を与えず、セキュリティも損なわれません。

Note メディア デバイスは、SHA1_32 および SHA1_80 ビットの暗号化方式のみをサポートします。

自己暗号化ドライブ

Unified Communications Manager は、自己暗号化ドライブ（SED）をサポートしています。これは、フル ディスク暗号化（FDE）とも呼ばれます。FDE は、ハードドライブで使用可能なすべてのデータを暗号化するために使用される暗号化方式です。このデータには、ファイル、オペレーティングシステム、およびソフトウェアプログラムが含まれます。ディスク上の使用可能なハードウェアは、すべての受信データを暗号化し、すべての送信データの暗号化を解除します。

ドライブがロックされると、暗号化キーが内部で作成され保存されます。このドライブに保存されているすべてのデータは、そのキーを使用して暗号化され、暗号化された形式で保存されます。FDE は、キー ID とセキュリティ キーで構成されます。

詳細については、『Cisco UCS C シリーズサーバー Integrated Management Controller GUI コンフィギュレーション ガイド』を参照してください。

設定ファイルの暗号化

Unified Communications Manager は、ダイジェスト クレデンシャルや管理者パスワードといった機密データを、TFTP サーバからの設定ファイル ダウンロードの形で電話にプッシュします。

Unified Communications Manager において、データベース内では可逆暗号化を使用してこれらのクレデンシャルが保護されています。ダウンロードプロセス中のデータを保護するため、このオプションをサポートするすべての Cisco IP 電話 において、暗号化された設定ファイルを設定することを推奨します。このオプションを有効にすると、デバイスコンフィギュレーションファイルだけがダウンロード用に暗号化されます。

（注） 状況によっては、暗号化されていない電話機に機密データをダウンロードすることを選択することもできます。たとえば、電話機のトラブルシューティングなどです。

Unified Communications Manager は、暗号化キーを符号化してデータベースに保存します。TFTP サーバでは、対称暗号化キーを使用して設定ファイルの暗号化と復号が行われます。

- 電話に PKI 機能がある場合、Unified Communications Manager では電話の公開キーを使用して電話の設定ファイルを暗号化できます。
- 電話に PKI 機能がない場合、Unified Communications Manager と電話に一意の対称キーを設定する必要があります。

暗号化設定ファイルの設定は、[Unified Communications Manager Administration] の [Phone Security Profile] ウィンドウで有効化し、その後 [Phone Configuration] ウィンドウで電話に適用します。

デフォルトのセキュリティ管理タスク

デフォルトのセキュリティ管理タスクを以下に示します。

手順

	コマンドまたはアクション	目的
ステップ 1	Cisco Unified IP 電話 の ITL ファイルの更新	TFTP 構成ファイルを検証します。
ステップ 2	ITL ファイルステータスの取得	電話機の ITL ファイルステータスを取得します。
ステップ 3	Cisco Unified IP 電話 サポートリストの取得	Cisco Unified Reporting ページを使用して Cisco Unified IP Phone のサポートリストを取得します。
ステップ 4	8.0 より前のリリースへのクラスタのロールバック	ロールバック用のクラスタを準備します。
ステップ 5	ITL ファイルの一括リセットの実行 （27 ページ）	ITL ファイルの一括リセットの実行
ステップ 6	CTL ローカルキーのリセット	CLI コマンドを使用して Cisco Trust List（CTL）ファイルのリセットを実行する
ステップ 7	ITLRecovery 証明書の有効期間の表示	ITLRecovery 証明書の有効期間を表示します。
ステップ 8	認証と暗号化のセットアップ	新規インストールの認証と暗号化を実装します。

Cisco Unified IP 電話 の ITL ファイルの更新

電話機にインストールされている ITL ファイルでデフォルトのセキュリティを使用している Unified Communication Manager との集中型 TFTP では、TFTP 設定ファイルは検証されません。

リモートクラスタからの電話機が集中型 TFTP 展開に追加される前に、次の手順を実行します。

ステップ 1 中央 TFTP サーバで、Enterprise パラメータ**Prepare cluster for PRE CM-8.0 rollback**を有効にします。

ステップ 2 TVS および TFTP を再起動します。

ステップ 3 すべての電話機をリセットして、ITL 署名検証を無効にする新しい ITL ファイルがダウンロードされていることを確認します。

ステップ 4 HTTPS ではなく HTTP を使用するように、エンタープライズパラメータセキュア https Url を設定します。

（注） Unified Communications Manager のリリース 10.5 以降では、**[クラスタの 8.0 以前へのロールバック準備（Prepare Cluster for Rollback to pre-8.0）]** エンタープライズ パラメータを有効にした後、電話が自動的にリセットされます。中央 TFTP サーバの Unified Communications Manager バージョンとこのパラメータを有効にする方法については、『Cisco Unified Communications Manager セキュリティ ガイド』の「8.0 より前のリリースへのクラスタのロールバック」セクションを参照してください。

ITL ファイルステータスの取得

電話機の ITL ファイルステータスを取得するには、次の手順を使用します。

ステップ 1 Cisco Unified Communications Manager Administrationから、**[デバイス（Device）]** > **[電話（Phone）]** を選択します。

ステップ 2 **[電話機を探す（Find Phone where）]** ドロップダウンリストで **[ITL ファイルステータス（ITL File Status）]** を選択し、条件を選択します。

フィールド	説明
Match	サーバーと電話機の ITL ハッシュが同じ
MisMatch	サーバーの ITL ハッシュが電話の ITL ハッシュではない、または電話またはサーバーの ITL ハッシュが不明です。
Not Installed	電話機が新しい CUCM サーバーへの登録に失敗し、以前のサーバーにバウンスする

ステップ 3 [検索（Find）] をクリックします。

Cisco Unified IP 電話 サポートリストの取得

Cisco Unified Reporting ツールを使用して、デフォルトでセキュリティをサポートするシスコエンドポイントのリストを生成します。

ステップ 1 [Cisco Unified Reporting] から [システムレポート（System Reports）] をクリックします。

ステップ 2 [システムレポート（System Reports）] リストで、[Unified CM 電話機能一覧（Unified CM Phone Feature List）] をクリックします。

ステップ 3 **[製品（Product）]** ドロップダウンリストから、**[デフォルトのセキュリティ（Security By Default）]** を選択します。

ステップ 4 [送信（Submit）] をクリックします。
特定の電話でサポートされている機能のリストを含むレポートが生成されます。

8.0 より前のリリースへのクラスタのロールバック

クラスタを Unified Communications Manager の旧リリース（リリース 8.0 よりも前）にロールバックする場合は、その前に [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たロールバックの準備が必要です。

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

ステップ 1 Unified Communications Manager で、**[システム（System）]** > **[エンタープライズパラメータ設定（Enterprise Parameters Configuration）]** を選択します。

[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 Unified Communications Manager のバージョン 8.0 以前へロールバックする準備を行う場合のみ、このパラメータを有効にします。このパラメータが有効になっている間、HTTPS を使う電話サービス（たとえば、エクステンション モビリティなど）は機能しません。ただし、このパラメータが有効になっていても、基本的な電話の発信および受信は引き続き可能です。

ステップ 2 Cisco IP 電話が自動的に再起動され、Unified Communications Manager に登録されるまで、10 分間待ちます。

ステップ 3 クラスタ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 Manager* アドミニストレーション ガイド』を参照してください。

ステップ 4 クラスタが以前のバージョンへの切り替えを完了するまで待ちます。

ステップ 5 次のリリースのいずれかを混合モードで実行している場合、CTL クライアントの実行が必要です。

- Unified Communications Manager リリース 7.1(2)
  - 7.1 (2) のすべての通常リリース
  - 007.001 (002.32016.001) より前の712のすべての ES リリース
- Unified Communications Manager リリース 7.1（3）
  - 007.001 (003.21900.003) より前の713のすべての通常リリース = 7.1 (3a) su1a
  - 007.001 (003.21005.001) より前の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、「CTL クライアントの設定」の章を参照してください。

ステップ 6 「Prepare Cluster for Rollback to pre-8.0」 エンタープライズ パラメータが [True] に設定されている場合、社内ディレクトリが機能するために以下の変更が必要です。

[Device] > [Device Settings] > [Phone Services] > [Corporate Directory] で、サービス URL を「Application:Cisco/CorporateDirectory」から「http://<ipaddr>:8080/ccmcip/xmldirectoryinput.jsp」へと変更します。

ステップ 7 「[Prepare Cluster for Rollback to pre-8.0]」 エンタープライズ パラメータが [True] に設定されている場合、パーソナル ディレクトリが機能するために以下の変更が必要です。

[Device] > [Device Settings] > [Phone Services] > [Personal Directory] で、サービス URL を「Application:Cisco/PersonalDirectory」から「http://<ipaddr>>:8080/ccmpd/pdCheckLogin.do?name=undefined」へと変更します。

復帰後のリリース8.6 以降へのスイッチバック

クラスタをリリース7.xに戻した後にリリース8.6またはそれ以降のパーティションに切り替える場合は、次の手順に従います。

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再度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 Manager* アドミニストレーション ガイド』を参照してください。

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た場合は、CTL クライアントを実行する必要があります。

Unified Communications Manager リリース 7.1(2)

- 7.1 (2) のすべての通常リリース
- 007.001 (002.32016.001) より前の712のすべての ES リリース
- Unified Communications Manager リリース 7.1(3)
  - 007.001 (003.21900.003) より前の713のすべての通常リリース = 7.1 (3a) su1a
  - 007.001 (003.21005.001) より前の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、「CTL クライアントの設定」の章を参照してください。

ステップ 3 [Unified Communications Manager Administration]で 、**[System]** > **[Enterprise Parameters Configuration]** を選択します。

[Enterprise Parameters Configuration] ウィンドウが表示されます。

[Prepare Cluster for Rollback to pre-8.6] 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 4 Cisco Unified IP 電話 が自動的に再起動され、Unified Communications Manager に登録されるまで、10 分間待ちます。

ITL ファイルの一括リセットの実行

この手順は必ず Unified Communications Manager パブリッシャで実行してください。

電話機が ITL ファイル 署名者を信頼できなくなり、かつ TFTP サービスによってローカルに提供された ITL ファイルを認証できないか、TVS を使用して認証できない場合は、ITL ファイルの一括リセットが実行されます。

一括リセットを実行するには、CLI コマンド **utils itl reset** を使用します。このコマンドは新しい ITL リカバリファイルを生成し、電話機と CUCM の TFTP サービス間の信頼を再確立します。

ヒント　Unified Communications Manager をインストールする場合は、CLI コマンド **file get tftp** *ITLRecovery.p12* を使用して ITL リカバリペアをエクスポートしてから、DR を介してバックアップを実行します。（キーのエクスポート先となる）SFTP サーバとパスワードの入力を求めるプロンプトも表示されます。

ステップ 1　次のいずれかの手順を実行します。

- **utils itl reset localkey** を実行します。
- **utils itl reset remotekey** を実行します。

（注）　**utils itl reset localkey** の場合、ローカルキーはパブリッシャにあります。このコマンドを発行しているとき、ITL 回復キーをリセットしている間、ITL ファイルは CallManager キーによって一時的に署名されます。

ステップ 2　**show itl** を実行してリセットが正常に行われたことを確認します。

ステップ 3　Cisco Unified CM Administration から、**[システム（System）] > [エンタープライズパラメータ（Enterprise Parameters）]** を選択します。

ステップ 4　[Reset] をクリックします。

デバイスが再起動されます。これで、CallManager キーで署名された ITL ファイルをダウンロードし、設定ファイルを受け入れる準備が整いました。

ステップ 5　TFTP サービスを再起動し、すべてのデバイスを再起動します。

（注）　TFTP サービスを再起動すると、ITL ファイルが ITLRecovery キーによって署名され、ステップ 1 の変更がロールバックされます。

デバイスは、ITLRecovery キーで署名された ITL ファイルをダウンロードし、再度ユニファイドコミュニケーションマネージャに登録します。

CTL ローカルキーのリセット

Unified Communications Manager クラスタ上のデバイスがロックされ、信頼されたステータスが失われる場合は、CLI コマンド **ctl reset localkey** を使用して Cisco Trust List（CTL）ファイルのリセットを実行します。このコマンドにより、新しい CTL ファイルが生成されます。

ステップ 1 **utils ctl reset localkey** の実行

（注） **utils ctl reset localkey** では、ローカルキーはパブリッシャ側にあります。このコマンドを発行すると、CTL ファイルは ITLRecovery キーによって一時的に署名されます。

ステップ 2 リセットが正常に行われたことを確認するには **show ctl** を実行します。

ステップ 3 Cisco Unified CM Administration から、**[システム（System）]** > **[エンタープライズパラメータ（Enterprise Parameters）]** を選択します。
[エンタープライズパラメータの設定（Enterprise Parameters Configuration）] ページが表示されます。

ステップ 4 [Reset] をクリックします。

デバイスが再起動されます。これで、CallManager キーで署名された CTL ファイルをダウンロードし、設定ファイルを受け入れる準備が整いました。

ステップ 5 **utils ctl update CTLFile** を実行して、ステップ 1 の変更をロールバックする必要なサービスを再起動します。

デバイスが再起動されます。これで、ITLRecovery キーで署名された CTL ファイルをダウンロードし、設定ファイルを受け入れる準備が整いました。

デバイスは、必要なキーを使用して署名された CTL ファイルをダウンロードし、Unified Communications Manager に再度正しく登録します。

ITLRecovery 証明書の有効期間の表示

ITLRecovery 証明書は電話機での有効期間が長いです。[証明書ファイルデータ（Certificate File Data）] ペインに移動し、有効期間または他の ITLRecovery 証明書の詳細を表示できます。

ステップ 1 Cisco Unified OS の管理から、**[セキュリティ（Security）]** > **[証明書の管理（Certificate Management）]** を選択します。

ステップ 2 証明書を検索し、設定の詳細を表示するには、必要な検索パラメータを入力します。
条件に一致する証明書のリストが [証明書リスト（Certificate List）] ページに表示されます。

ステップ 3 [ITLRecovery] リンクをクリックして、有効期間を確認します。

ITLRecovery 証明書の詳細が [証明書ファイルデータ（Certificate File Data）] ペインに表示 されます。

有効期間は現在の年から 20 年です。

認証と暗号化のセットアップ

重要 **utils ctl** CLI コマンドセットを使用して、暗号化を設定することができます。このオプションの詳細については、『*Command Line Interface Guide for Cisco Unified Communications Solutions*』を参照してください。

次の手順では、認証と暗号化を実装するために実行する必要があるすべてのタスクについて説明します。指定されたセキュリティ機能に対して実行する必要があるタスクを含む章の参考資料については、「関連項目」を参照してください。

- 新規インストールの認証と暗号化を実装するには、次の表を参照してください。
- ノードをセキュアクラスタに追加するには、ノードの追加方法および新しいノード用のセキュリティの設定方法を説明している『*Installing Cisco Unified Communications Manager*』を参照してください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。