セキュリティの概要

Unified Communications Manager システムにセキュリティ対策を実装すると、電話や Unified Communications Manager サーバの個人情報/ID の盗用、データ改ざん、コール シグナリング/メディア ストリーム改ざんを防止できます。

Cisco IP テレフォニー ネットワークでは、認証済み通信ストリームを確立および維持し、ファイルを電話に転送する前にそのファイルにデジタル署名して、Cisco Unified IP Phone 間のメディア ストリームとコール シグナリングを暗号化します。

用語および略語

次の表の定義は、Cisco IP テレフォニー ネットワークの認証、暗号化およびその他のセキュリティ機能を設定する際に適用されます。

表 *1:* 用語

用語	定義
アクセス コントロール リスト（ACL）	システム機能およびリソースにアクセスするための権限およびアクセス許可を定義するリスト。方式リストを参照してください。
認証	通信エンティティのアイデンティティを確認するプロセス。
許可	認証されたユーザ、サービス、またはアプリケーションに、要求されたアクションを実行するために必要なアクセス許可があるかどうかを指定するプロセス。Unified Communications Manager では、許可されたユーザに特定のトランク側 SIP 要求を制限するセキュリティ プロセスです。
認証ヘッダー	チャレンジに対する SIP ユーザ エージェントの応答。
証明書	証明書保持者名、公開キー、および証明書を発行する認証局のデジタル署名を含むメッセージ。
認証局（CA）	証明書を発行する信頼されたエンティティ：シスコまたはサードパーティのエンティティ。
認証局プロキシ機能（CAPF）	サポートするデバイスが Unified Communications Manager Administration を使用して、ローカルで有効な証明書を要求できるプロセス。
証明書信頼リスト（CTL）	CLI コマンドセット **utils cli** または CTL クライアントで作成され、Cisco Site Administrator Security Token（セキュリティ トークン）によって署名されたファイル。電話が信頼するサーバの証明書のリストを含みます。
Challenge	ダイジェスト認証において、SIP ユーザ エージェントに対しそのアイデンティティの認証を求める要求。

用語	定義
Cisco Site Administrator Security Token（セキュリティ トークン、etoken）	秘密キーと、Cisco Certificate Authority が署名する X.509v3 証明書を含むポータブル ハードウェア セキュリティ モジュール。ファイル認証に使用され、CTL ファイルの署名に使用される場合があります。 ハードウェア セキュリティ トークンは CTL クライアントにのみ必要です。CLI コマンド セット **utils ctl** はハードウェア セキュリティ トークンを必要としません。
デバイス認証	デバイスのアイデンティティを検証してエンティティが正当なものであることを接続の確立前に確認するプロセス。
ダイジェスト認証	デバイス認証の 1 つで、SIP ユーザ エージェントのアイデンティティを設定するために（特に）共有パスワードの MD5 ハッシュを使用します。
Digest User	SIP を実行している電話または SIP トランクが送信する許可要求に含まれているユーザ名。
デジタル署名	メッセージをハッシュし、その後署名者の秘密キーを使用してメッセージを暗号化することによって生成される値。受信者は署名者の公開キーを使用してメッセージとハッシュを復号化し、同じハッシュ関数を使って別のハッシュを作成し、次に 2 つのハッシュを比較し、メッセージが一致しており内容が変更されていないことを確認します。
DSP	デジタル シグナリング プロセッサ。
DSP ファーム	H.323 または MGCP ゲートウェイの DSP で提供される IP テレフォニー会議のネットワーク リソース。
暗号化	データを暗号文に変換するプロセス。情報の機密性を保持し、対象とする受信者のみがデータを読み取ることができるようにします。暗号化アルゴリズムと暗号キーが必要です。

用語	定義
ファイル認証	電話がダウンロードするデジタル署名ファイルを検証するプロセス。ファイルの作成後にファイルの改ざんが発生していないことを確認するため、電話で署名が検証されます。
H.323	インターネットの標準規格の 1 つで、一連の共通コーデック、コール設定とネゴシエーション手順、および基本的なデータ転送方法を定義します。
ハッシュ	ハッシュ関数を使用してテキスト文字列から生成される、通常は16進数の数値。これにより、データに対して 1 つの小さなデジタル「「フィンガープリント」」が作成されます。
Hypertext Transfer Protocol Over Secure Sockets Layer（HTTPS）	（少なくとも）HTTPS サーバのアイデンティティを確認する IETF 定義のプロトコル。暗号化を使用して、Tomcat サーバとブラウザ クライアントの間で交換される情報の機密性を確保します。
イメージ認証	電話がバイナリ イメージをロードする前に、そのバイナリ イメージの整合性と送信元を電話が検証するプロセス。
完全性	データの改ざんがエンティティ間で実行されていないことを確認するプロセス。
IPSec	エンドツーエンド セキュリティ用にセキュアな H.225、H.245、RAS シグナリング チャネルを提供する転送方式。
ローカルで有効な証明書（LSC）	CAPF が発行するデジタル X.509v3 証明書。電話または JTAPI/TAPI/CTI アプリケーションにインストールされます。
製造元でインストールされる証明書（MIC）	Cisco 認証局が署名し、サポートされている電話に Cisco Manufacturing によってインストールされるデジタル X.509v3 証明書。LSC が電話にインストールされると、CAPF の認証メカニズムとして使用されます。
中間者攻撃	Unified Communications Manager と電話との間で流れる情報を攻撃者が監視して改変できるようにするプロセス。

用語	定義
マルチポイント コントロール ユニット（MCU）	複数の H.323 エンドポイントを接続し、複数のユーザが IP ベースのビデオ会議に参加できるようにする柔軟なシステム。
MD5	暗号化で使用されるハッシュ関数。
メディア暗号化	暗号化手順によってメディアの機密性を保護するプロセス。メディア暗号化は IETF RFC 3711 で定義された Secure Real-Time Protocol（SRTP）を使用します。
メッセージ/データの改ざん	攻撃者が送信中にメッセージを変更しようとするイベント。コールの途中終了も含まれます。
方式リスト	許可プロセス中に SIP トランクに着信する可能性のある特定のカテゴリのメッセージを制限するツール。ランク側アプリケーションやデバイスで可能な SIP nonINVITE 方式を定義します。メソッド ACL とも呼ばれます。
混合モード	セキュア/非セキュア プロファイルおよび RTP/SRTP メディアを持つデバイスが Unified Communications Manager に接続できるようにするために設定する Unified Communications Manager のセキュリティ モード。
ナンス	サーバが各ダイジェスト認証要求に対して生成する一意のランダムな数値。MD5 ハッシュの生成に使用されます。
非セキュア モード	非セキュア プロファイルおよび RTP メディアを持つデバイスが Unified Communications Manager に接続できるようにするために設定する Unified Communications Manager のセキュリティ モード。
非セキュア コール	少なくとも 1 つのデバイスが認証も暗号化もされていないコール。
非セキュアなデバイス	UDP または TCP シグナリングと非セキュア メディアを使用するデバイス。
PKI	保護された公開キー配布、証明書と認証局など、公開キーの暗号化に必要な一連の要素からなる公開キー インフラストラクチャ。

用語	定義
公開/秘密キー	暗号化に使用されるキー。公開キーは幅広く使用可能ですが、秘密キーはそれぞれの所有者により保持されます。非対称暗号化では両方のキーが使用されます。
リプレイ アタック	攻撃者が実際のデバイスになりすまして、電話またはプロキシサーバを特定する情報をキャプチャし情報を再生するイベント。たとえば、プロキシサーバの秘密キーのなりすましなど。
RTP	リアルタイム転送プロトコル
Simple Certificate Enrollment Protocol（SCEP）	X.509証明書を発行する認証局との通信に使用されるプロトコル。
セキュアなコール	すべてのデバイスが認証され、シグナリングとメディア（音声ストリーム）が暗号化されているコール。
シグナリング認証	伝送中にシグナリング パケットに改ざんがなかったことを検証する TLS プロセス。
シグナリング暗号化	デバイスと Unified Communications Manager サーバの間で送信されるすべてのシグナリング メッセージの機密を保護するために暗号化手法を使用するプロセス。
SIP レルム	Unified Communications Manager がチャレンジに応答するために使用する文字列（名前）。
SRTP	Secure Real-Time Transport Protocol。ネットワーク上の音声会話のセキュリティを確保し、リプレイ アタックからの保護を提供するプロトコル。
SSL	インターネットでの電子メールなどのデータ通信を保護する暗号化プロトコル。後継のTLSと同等の機能を持ちます。
トランスポート レイヤ セキュリティ（TLS）	インターネットでの電子メールなどのデータ通信を保護する暗号化プロトコルで、機能としては SSL と同等です。
信頼リスト	デジタル署名なしの証明書リスト。

用語	定義
信頼ストア	Unified Communications Manager などのアプリケーションが明示的に信頼する X.509 証明書のリポジトリ。
X.509	PKI 証明書インポート用の ITU-T 暗号化規格であり、証明書の形式が含まれます。

システム要件

認証または暗号化に関するシステム要件は次のとおりです。

- 管理者パスワードは、クラスタ内の各サーバで異なる必要があります。
- Cisco CTL クライアントで使用されたユーザ名とパスワード（Unified Communications Manager サーバへのログイン用）は [Unified Communications Manager Administration] のユーザ名およびパスワード（[Unified Communications Manager Administration] へのログインに使用するユーザ名とパスワード）と一致する必要があります。
- ボイス メール ポートのセキュリティを設定する前に、この Cisco Unified Communications Manager リリースをサポートするバージョンの Cisco Unity または Unity Connection システムをインストールしていることを確認します。

機能一覧

Unified Communications Manager システムは、コール セキュリティに対してトランスポート層からアプリケーション層にかけてのマルチレイヤ アプローチを採用しています。

Transport Layer Security には、シグナリングの認証と暗号化のための TLS および IPSec が含まれ、音声ドメインへのアクセスの制御と防止が実現されます。SRTP によってメディアの認証と暗号化が付加され、音声会話と他のメディアのプライバシーと機密性が保護されます。

次の表は、機能のサポート状況と設定状況に応じて SCCP コール セッション中に Unified Communications Manager に実装可能な認証と暗号化機能の概要を示します。

表 *2 : SCCP* コールのセキュリティ機能

セキュリティ機能	回線側	トランク側
転送/接続/整合性	セキュア TLS ポート	IPSec 関連付け
デバイス認証	Unified Communications Manager や CAPF による TLS 証明書交換	IPSec 証明書交換または事前共有キー

セキュリティ機能	回線側	トランク側
シグナリング認証/暗号化	TLS モード：認証済みまたは暗号化済み	IPSec（認証ヘッダー、暗号化（ESP）、または両方）
メディア暗号化	SRTP	SRTP
許可	プレゼンス要求	プレゼンス要求
（注）　デバイスでサポートされる機能はデバイス タイプによって異なります。		

次の表に、機能のサポート状況と設定状況に応じて SIP コール セッション中に Unified Communications Manager に実装可能な認証と暗号化機能の概要を示します。

表 *3: SIP* コールのセキュリティ機能

セキュリティ機能	回線側	トランク側
転送/接続/整合性	セキュア TLS ポート	セキュア TLS ポート
デバイス認証	Unified Communications Manager や CAPF による TLS 証明書交換	IPSec 証明書交換または事前共有キー
ダイジェスト認証	各 SIP デバイスが一意のダイジェストユーザ クレデンシャルを使用します。	SIP トランク ユーザ エージェントは一意のダイジェスト クレデンシャルを使用します。
シグナリング認証/暗号化	TLS モード：認証済みまたは暗号化済み（Cisco Unified IP Phone 7942/7962 を除く）。	TLS モード：認証済みまたは暗号化済みモード
メディア暗号化	SRTP	SRTP
許可	プレゼンス要求	プレゼンス要求 方式リスト
（注）　デバイスでサポートされる機能はデバイス タイプによって異なります。		

セキュリティ アイコン

Unified Communications Manager は、コールに参加する Unified Communications Manager サーバおよびデバイスのセキュリティ レベルに応じてコールのセキュリティ ステータスを提供します。

セキュリティ アイコンをサポートする電話には、コールのセキュリティ レベルが表示されます。

- 電話は、シグナリング セキュリティ レベルが「認証済み」のコールに対してはシールド アイコンを表示します。シールドは Cisco IP デバイス間のセキュアな接続を示します。これは、デバイスのシグナリングが認証済みまたは暗号化されていることを意味します。
- 電話は、暗号化されたメディアのコールに対してはロック アイコンを表示します。これは、デバイスが暗号化シグナリングと暗号化メディアを使用していることを意味します。

（注） 一部の電話モデルでは、ロック アイコンのみが表示されます。

コールのセキュリティ ステータスは、ポイントツーポイント、クラスタ間およびクラスタ内、マルチホップ コールで変わることがあります。SCCP 回線、SIP 回線、および H.323 シグナリングでは、参加エンドポイントへのコール セキュリティ ステータスの変更の通知がサポートされています。セキュリティ アイコンに関連する制約については、セキュリティ アイコンおよび暗号化に関するトピックを参照してください。

コールの音声とビデオ部分がコールのセキュリティ ステータスのベースとなります。コールは、音声とビデオ部分の両方がセキュアである場合に限り、安全とみなされます。次の表で、セキュリティアイコンが表示されるかどうかと、どのアイコンが表示されるかを決定するルールについて説明します。

表 *4:* セキュリティ アイコンの表示規則

コールのメディア タイプとデバイス タイプ	シールドおよびロック アイコンの両方を表示する電話	ロック アイコンのみを表示する電話
セキュアな音声のみ	ロック	ロック
セキュアな音声と非セキュアなビデオ	シールド	なし
セキュアな音声とセキュアなビデオ	ロック	ロック
非セキュアな音声のみの認証済みデバイス	シールド	なし
非セキュアな音声とビデオがある認証済みデバイス	シールド	なし
非セキュアな音声のみの非認証デバイス	なし	なし
非セキュアな音声とビデオがある非認証デバイス	なし	なし

（注） 「Override BFCP Application Encryption Status When Designating Call Security Status」サービス パラメータは、パラメータ値が [True] で音声がセキュアであると、ロック アイコンを表示します。この状態は、他のすべてのメディア チャネルのセキュリティ ステータスを無視します。デフォルト パラメータ値は [False] です。

電話会議と割り込みコールでは、セキュリティ アイコンは会議のセキュリティ ステータスを表示します。

連携動作と制限事項

ここでは、連携動作と制限事項について説明します。

セキュアな会議機能に関する連携動作と制限事項の詳細については、関連項目を参照してください。

連携動作

このセクションでは、Unified Communications Manager アプリケーションと Cisco のセキュリティ機能の連携動作について説明します。

プレゼンス

SIP を実行している電話やトランクにプレゼンス グループ認証を追加するには、プレゼンス グループを設定して、プレゼンス要求を認証済みユーザに限定します。

プレゼンス グループ設定の詳細については、『*Feature Configuration Guide for Cisco Unified Communications Manager*』を参照してください。

SIP トランクでプレゼンス要求を許可するには、SIP トランクでのプレゼンス要求を許可するよう Unified Communications Manager を設定します。また必要な場合には、リモートデバイスやアプリケーションからの着信プレゼンス要求の受け入れと認証を行うよう Unified Communications Manager を設定します。

SIP トランク

SIP で開始された転送機能、および SIP トランクでの Web 転送やクリック ツー ダイヤルといったその他転送関連の高度な機能を使用するには、着信 Out-of-Dialog REFER 要求を受け入れるよう SIP トランク セキュリティ プロファイルを設定します。

イベント レポートのサポート（MWI サポートなど）を提供する場合、および（ボイス メッセージ サーバなどからの）コールごとの MTP 割り当てを減少させる場合は、Unsolicited NOTIFY SIP 要求を受け入れるよう SIP トランク セキュリティ プロファイルを設定します。

Unified Communications Manager が、SIP トランクの外部コールを外部デバイスまたは外部パーティに転送できるようにするには（在席転送の場合など）、REFERS および INVITES の Replaces

ヘッダー付き SIP 要求を受け入れるよう、SIP トランク セキュリティ プロファイルを設定します。

エクステンション モビリティ

エクステンションモビリティの場合、ユーザのログインとログアウトの際にSIPダイジェストクレデンシャルが変化します。異なるユーザには異なるクレデンシャルが設定されるためです。

CTI

CAPF プロファイルを設定した場合（各 Unified Communications Manager Assistant ノードに 1 つ）、Unified Communications Manager Assistant は CTI へのセキュアな接続をサポートします（Transport Layer Security 接続）。

CTI/JTAPI/TAPI アプリケーションのインスタンスが複数実行されている場合、CTI TLS をサポートするには、CTI Manager と JTAPI/TSP/CTI アプリケーション間のシグナリングおよびメディア通信ストリームを保護するために、すべてのアプリケーションインスタンスに一意のインスタンス ID（IID）を設定する必要があります。

デバイス セキュリティ モードが認証済みまたは暗号化済みの場合、Cisco Unity-CM TSP は Unified Communications Manager TLS ポートを介して Unified Communications Manager に接続します。セキュリティ モードが非セキュアの場合、Cisco Unity TSP は CTI Manager ポートを介して Unified Communications Manager に接続します。

機能制限

ここでは、シスコのセキュリティ機能に適用される制限事項について説明します。

認証および暗号化

認証機能および暗号化機能をインストールして設定する前に、次の制限事項を考慮してください。

- シグナリング暗号化またはメディア暗号化は、デバイス認証なしでは実装できません。デバイス認証をインストールするには、Cisco CTL Provider サービスを有効にしてから、Cisco CTL クライアントをインストールして設定します。
- 混合モードを設定している場合、Unified Communications Manager ではネットワーク アドレス変換（NAT）がサポートされません。

  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ために、ファイアウォールで UDP を有効にできます。UDP を有効にすると、ファイアウォールの信頼できる側にあるメディア 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のメディア 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置く必要があります。

シグナリング暗号化では、NAT トラバーサルがサポートされません。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。

割り込みと暗号化

割り込みと暗号化には次の制約事項が適用されます。

- 帯域幅の要件のため、Cisco IP Phone 7942 と 7962 は、アクティブな暗号化されたコールでの暗号化されたデバイスからの割り込みをサポートしません。割り込みの試行は失敗します。発信側の電話では、割り込みが失敗したことを示すトーンが再生されます。
- リリース 8.2 以前のリリースを実行中の暗号化された Cisco IP Phone は、認証済み参加者または非セキュア参加者としてのみアクティブな通話に割り込みできます。
- 発信者がセキュアな SCCP コールに割り込む場合、システムはターゲットデバイスで内部トーン再生メカニズムを使用し、ステータスはセキュアのままになります。
- 発信者がセキュアな SIP コールに割り込む場合、システムは保留トーンを再生し、トーンの間 Unified Communications Manager がコールを非セキュアとして分類します。

（注）　リリース 8.3 以降を実行中の、非セキュアまたは認証済み Cisco IP Phone は、暗号化されたコールに割り込むことができます。会議のセキュリティ ステータスは、セキュリティ アイコンによって表示されます。

ワイドバンド コーデックと暗号化

以下の情報は、暗号化向けに設定され、ワイドバンド コーデック地域が割り当てられている Cisco Unified IP Phone 7962 および 7942 に適用されます。TLS/SRTP 向けに設定された Cisco Unified IP Phone 7962 および 7942 にのみ適用されます。

暗号化されたコールを確立するため、Unified Communications Manager はワイドバンド コーデックを無視して、電話のコーデック リストからサポートされる別のコーデックを選択します。コールに参加する他のデバイスが暗号化向けに設定されていない場合、Unified Communications Manager はワイドバンド コーデックを使用して、認証済または非セキュア コールを確立することがあります。

メディア リソースと暗号化

Unified Communications Manager は、メディア リソースが使用されないセキュアな Cisco Unified IP Phone（SCCP または SIP）、セキュアな CTI デバイス/ルート ポイント、セキュアな Cisco MGCP IOS ゲートウェイ、セキュアな SIP トランク、セキュアな H.323 ゲートウェイ、セキュ

アな会議ブリッジ、およびセキュアな H.323/H.245/H.225 トランクの間での認証済みコールと暗号化コールをサポートしています。次の状況では Unified Communications Manager はメディア暗号化を提供しません。

- トランスコーダに関連するコール
- メディア ターミネーション ポイントに関連するコール

（注） MTP 暗号化は、非パススルー MTP でのみサポートされていません。

電話のサポートと暗号化

SCCP を実行している次の Cisco Unified IP Phone は暗号化をサポートします。6901、6911、6921、6941、6945、6961、7906G、7911G、7925G、7925G-EX、7926G、7931G、7941G、7941G-GE、7942G、7945G、7961G、7961G-GE、7962G、7965G、7975G、8941、8945、および 9961。

SIP を実行している次の Cisco Unified IP Phone は暗号化をサポートします。6901、6911、6921、6941、6945、6961、7811、7821、7841、7861、7832、79 06G、7911G、7941G、7941G-GE、7942G、7961G、7961G-GE、7962G、7965G、7975G、8811、8821、8821-EX、8832、8841、8845、8851、8851NR、8865、8865NR、8941、8945、8961、9971、および 9971。

詳細は、暗号化とこのバージョンの Unified Communications Manager をサポートする『*System Configuration Guide for Cisco Unified Communications Manager*』を参照してください。

警告 セキュリティ機能を最大限に活用するため、Cisco IP Phone をファームウェアリリース 8.3 に更新することが推奨されます。リリース 8.3 はこの Unified Communications Manager リリースの暗号化機能をサポートします。以前のリリースを実行している暗号化済みの電話は、これらの機能を完全にサポートしてはいません。これらの電話は、認証済みまたは非セキュアな参加者として、セキュアな会議と割り込みコールにのみ参加することができます。

以前のリリースの Unified Communications Manager でファームウェアリリース 8.3 を実行している Cisco IP Phone は、会議または割り込みコールにおいて、会議のセキュリティ ステータスではなく、電話の接続のセキュリティ ステータスを表示します。また、会議リストなどのセキュアな会議機能をサポートしません。

電話のサポートと暗号化された設定ファイル

すべての電話が暗号化された設定ファイルをサポートするわけではありません。暗号化された設定ファイルをサポートするが、署名を検証しない電話もあります。暗号化された設定ファイルをサポートするすべての電話には、完全に暗号化された設定ファイルを受信するために Unified Communications Manager リリース 5.0 以降と互換性があるファームウェアが必要です。

セキュリティ アイコンおよび暗号化

セキュリティ アイコンおよび暗号化には次の制約事項が適用されます。

- コールの転送やコール保留時などのタスクを実行するときに、暗号化ロック アイコンが電話に表示されない場合があります。MOH など、これらのタスクに関連付けられたメディア ストリームが暗号化されていない場合、ステータスが暗号化から非セキュアに変わります。
- Unified Communications Manager は、H.323 トランクを通過中のコールに対してはシールド アイコンを表示しません。
- PSTN に関連するコールでは、セキュリティ アイコンはコールの IP ドメイン部分のみのセキュリティ ステータスを示します。
- TLS 転送タイプを使用する場合、SIP トランクが報告するセキュリティ ステータスは暗号化または非認証です。SRTP がネゴシエートされると、セキュリティ ステータスは暗号化になります。SRTP がネゴシエートされていない場合は、非認証のままになります。これにより、Unified Communications Manager のコール制御は、SIP トランクに関連するコールの全体的なセキュリティ レベルを特定できます。

  SIP トランクは、ミートミー会議または C 割り込みなどの発生時に参加者が認証されると、認証済みの状態をトランク経由で報告します。（SIP トランクは引き続き TLS/SRTP を使用します。）
- セキュアなモニタリングと録音のため、SIP トランクは SIP 回線によって現在使用されているように SIP トランクのセキュリティ アイコンの状態を送信するときに既存の Call Info ヘッダー メカニズムを使用します。これにより、SIP トランクのピアがコールの全体的なセキュリティ ステータスをモニタできるようになります。
- 一部の電話モデルでは、ロック アイコンしか表示されず、シールド アイコンが表示されません。

クラスタ セキュリティ モードとデバイス セキュリティ モード

（注） デバイス セキュリティ モードは、Cisco IP Phone または SIP トランクのセキュリティ機能を設定します。クラスタ セキュリティ モードは、スタンドアロン サーバまたはクラスタのセキュリティ機能を設定します。

クラスタ セキュリティ モードが非セキュアになると、デバイス セキュリティ モードは電話の設定ファイルで非セキュアになります。このような状況では、デバイス セキュリティ モードに認証済みまたは暗号化済みが指定されていた場合でも、電話と SRST 対応ゲートウェイまたは Unified Communications Manager との間に非セキュアな接続が作成されます。[SRST Allowed] チェックボックスなど、デバイス セキュリティ モード以外のセキュリティ関連の設定は無視されます。[Unified Communications Manager Administration] でセキュリティ設定が削除されることはありませんが、セキュリティは実現されません。

電話が SRST 対応ゲートウェイへのセキュアな接続を試行するのは、クラスタ セキュリティ モードが混合モードであり、電話設定ファイルのデバイス セキュリティ モードが認証済みまたは暗号化済みに設定され、[Trunk Configuration] ウィンドウで [SRST Allowed?] チェックボックスがオンであり、かつ電話設定ファイルに有効な SRST 証明書が存在する場合のみです。

ダイジェスト認証と暗号化

Unified Communications Manager では、SIP コールが 2 つ以上の独立したコール レッグとして定義されます。2 つの SIP デバイス間での標準の 2 者間通話の場合、2 つのコール レッグが存在します。1 つのレッグは発信元 SIP ユーザ エージェントと Unified Communications Manager の間（発信元コール レッグ）、もう 1 つのレッグは Unified Communications Manager と接続先 SIP ユーザ エージェントとの間です（終端コール レッグ）。各コール レッグが個別のダイアログを表します。ダイジェスト認証はポイントツーポイント プロセスであるため、各コール レッグでのダイジェスト認証は他のコール レッグから独立しています。SRTP 機能は、ユーザ エージェント間でネゴシエートされる機能に応じて、コール レッグごとに変更できます。

パケット キャプチャと暗号化

SRTP 暗号化を実装すると、サードパーティのスニフィング ツールが機能しません。適切な認証で承認された管理者は [Unified Communications Manager Administration] で設定を変更してパケット キャプチャを開始できます（パケット キャプチャをサポートしているデバイスの場合）。このリリースに対応した『*Troubleshooting Guide for Cisco Unified Communications Manager*』を参照し、Unified Communications Manager でのパケット キャプチャの設定に関する情報をご確認ください。

ベスト プラクティス

セキュリティの設定時には、次のベストプラクティスを強く推奨します。

- 必ず安全なラボ環境でインストール作業および設定作業を実行してから、広範囲のネットワークに展開します。
- リモート ロケーションにあるゲートウェイおよびその他のアプリケーション サーバに対して IPSec を使用します。

警告 IPSec を使用しない場合、セッション暗号キーがクリア テキストで転送されます。

- 電話料金の詐欺行為を防止するためには、『*System Configuration Guide for Cisco Unified Communications Manager*』で説明されている会議の機能拡張を設定します。同様に、コールの外部転送を制限する設定作業を実行します。この作業の実行方法については、『*Feature Configuration Guide for Cisco Unified Communications Manager*』を参照してください。

デバイスのリセット、サーバとクラスタのリブート、サービスの再起動

ここでは、Cisco Unified Serviceability でどのようなときにデバイスのリセット、サーバ/クラスタのリブート、サービスの再起動が必要になるかについて説明します。

次の注意事項を考慮してください。

- [Cisco Unified Communications Manager Administration] で単一のデバイスに別のセキュリティ プロファイルを適用した後は、そのデバイスをリセットします。
- 電話のセキュリティ強化作業を実施した場合、デバイスをリセットします。
- 混合モードから非セキュア モード（またはその逆）にクラスタのセキュリティ モードを変更した後は、デバイスをリセットします。
- Cisco CTL クライアントの設定後、または CTL ファイルの更新後は、すべてのデバイスを再起動します。
- CAPF エンタープライズ パラメータを更新した後は、デバイスをリセットします。
- TLS 接続ポートを更新した後は、Cisco CTL Provider サービスを再起動します。
- 混合モードから非セキュア モード（またはその逆）にクラスタのセキュリティ モードを変更した後は、Cisco CallManager サービスを再起動します。
- 関連する CAPF サービス パラメータを更新した後は、Cisco Certificate Authority Proxy Function サービスを再起動します。
- Cisco CTL クライアントの設定後、または CTL ファイルの更新後は、Cisco Unified Serviceability 内の Cisco CallManager サービスおよび Cisco TFTP サービスをすべて再起動します。クラスタ内でこれらのサービスを実行するすべてのサーバで、この作業を実行します。
- CTL Provider サービスを開始または停止した後は、Cisco CallManager サービスおよび Cisco TFTP サービスをすべて再起動します。
- セキュア SRST リファレンスの設定後は、従属デバイスをリセットします。
- Smart Card サービスを [Started] および [Automatic] に設定した場合、Cisco CTL クライアントをインストールした PC をリブートします。
- アプリケーションユーザ CAPF プロファイルに関連付けられたセキュリティ関連のサービス パラメータを設定した後は、Cisco IP Manager Assistant サービス、Cisco WebDialer Web サービスおよび Cisco Extended Functions サービスを再起動します。

Cisco CallManager サービスの再起動については、『*Cisco Unified Serviceability Administration Guide*』を参照してください。

電話の設定を更新した後に単一のデバイスをリセットするには、電話セキュリティ プロファイルの適用に関連したトピックを参照してください。

デバイスのリセット、サーバとクラスタのリブート、サービスのリセット

この項では、デバイスのリセット、Cisco Unified Serviceability でのサービスの再起動、またはサーバ/クラスタのリブートが必要となる場合について説明します。

クラスタのすべてのデバイスをリセットするには、次の手順を実行します。

始める前に

作業を進める前にデバイスのリセット、サーバとクラスタのリブートとサービスの再起動に関するガイドラインを参照してください。

手順

ステップ 1 [Unified Communications Manager Administration] で、**[System]** > **[Cisco Unified CM]** を選択します。

[Find/List] ウィンドウが表示されます。

ステップ 2 [Find] をクリックします。

設定されている Unified Communications Manager サーバの一覧が表示されます。

ステップ 3 デバイスをリセットする Unified Communications Manager を選択します。

ステップ 4 [Reset] をクリックします。

ステップ 5 クラスタ内の各サーバでステップ 2 （17 ページ）とステップ 4 （17 ページ）を実行します。

割り込みによるメディア暗号化の設定

暗号化が設定されている Cisco Unified IP Phone 7962 および 7942 に割り込みを設定しようとすると、次のメッセージが表示されます。

注目 Cisco Unified IP Phone のモデル 7962 および 7942 に暗号化を設定する場合、暗号化されたコールに参加している間、それらの暗号化されたデバイスは割り込みリクエストを受け付けることができません。コールが暗号化されていると、割り込みの試行は失敗します。

[Unified Communications Manager Administration] で以下の作業を行うと、メッセージが表示されます。

- CTL クライアントの [Cluster Security Mode] パラメータを更新する。
- [Service Parameter] ウィンドウの [Builtin Bridge Enable] パラメータを更新する。

暗号化されたセキュリティ プロファイルが Cisco Unified IP Phone 7962 および 7942 に設定され、[Built In Bridge] 設定で **[Default]**（または [Default] と同等の設定）を選択した場合には、このメッセージは [Phone Configuration] ウィンドウに表示されません。ただし同じ制限が適用されます。

ヒント　変更を有効にするには、従属する Cisco IP デバイスをリセットする必要があります。

詳細については、割り込みと暗号化に関連する項目を参照してください。

CTLクライアント、SSL、CAPF、およびセキュリティトークンのインストール

認証サポートを実現するために、次のいずれかのオプションを選択できます。

1. [Unified Communications Manager Administration] から Cisco CTL クライアントをインストールします。Cisco CTL クライアント オプションの場合、少なくとも 2 つのセキュリティ トークンを入手する必要があります。
2. CLI コマンドセット **utils ctl** を使用します。この場合、セキュリティ トークンは不要です。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。

Unified Communications Manager をインストールすると、メディアおよびシグナリングの暗号化機能が自動的にインストールされます。

Unified Communications Manager によって、Unified Communications Manager 仮想ディレクトリ用のセキュア ソケット レイヤ（SSL）が自動的にインストールされます。

Cisco Certificate Authority Proxy Function（CAPF）では、[Unified Communications Manager Administration] の一部として自動的にインストールされます。

TLS および IPSec

転送セキュリティはデータのコーディング、パッキング、および送信を扱います。Unified Communications Manager は次のセキュアなトランスポート プロトコルを提供しています。

- Transport Layer Security（TLS）はセキュア ポートと証明書交換を使用して、2 つのシステム間またはデバイス間でセキュアで信頼できるデータ転送を実現します。TLS は音声ドメインへのアクセスを防ぐために、Unified Communications Manager 制御システム、デバイス、およびプロセス間の接続を保護および制御します。Unified Communications Manager は TLS を使用して SCCP を実行する電話へのセキュアな SCCP コール、および SIP を実行する電話またはトランクへの SIP コールを保護します。

- IP Security（IPSec）は、Unified Communications Manager とゲートウェイ間のセキュアで信頼できるデータ転送を実現します。IPSec は、 Cisco IOS MGCP および H.323 ゲートウェイにシグナリング認証および暗号化を実装します。

セキュア RTP（SRTP）サポートするデバイスにおいて、TLS および IPSec 転送サービスに次のセキュリティ レベルの SRTP を追加できます。SRTP はメディア ストリーム（音声パケット）を認証および暗号化し、Cisco Unified IP Phone の TDM またはアナログ音声ゲートウェイ ポートから発信または終了した音声会話が、音声ドメインへのアクセスを得ている可能性のある盗聴者から保護します。SRTP は、リプレイ アタックに対する保護を追加します。

Cisco Unified Communications Manager 9.0 以降はデュアル モード スマートフォンの TLS/SRTP サポートを提供しています。TLS は携帯電話については IP Phone と同じセキュアで信頼できるデータ転送モードを設定し、SRTP は音声会話を暗号化します。

証明書

証明書は、クライアントとサーバのアイデンティティを保護します。ルート証明書がインストールされた後、証明書はルート信頼ストアに追加され、デバイスとアプリケーション ユーザとの間を含め、ユーザとホストの間の接続を保護します。

管理者はサーバ証明書のフィンガープリントの参照、自己署名証明書の再生性、および信頼証明書の削除を Cisco Unified Communications Operating System GUI で実行できます。

管理者は、自己署名証明書の再生成と参照を CLI（コマンド ライン インターフェイス）でも実行できます。

CallManager 信頼ストアの更新と証明書の管理の詳細については、この Unified Communications Manager リリースに対応した『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。

（注）

- Unified Communications Manager でサポートされている証明書の形式は PEM（.pem）および DER（.der）だけです。
- DER あるいは PEM の証明書のサポートされる最大サイズは 4096 ビットです。

（注） 2 つの証明書をアップロードする場合は、それらの共通名と有効期間は同じであるものの、シリアル番号と署名アルゴリズムは異なるものであることを確認してください。

たとえば、Cisco Unified Communications Manager tomcat-trust には、シリアル番号が 27:20:41:0c: 5b:08:69:80:42:62:4f:13:bd:16:06:6a、アルゴリズムが SHA1 のルート CA が存在します。シリアル番号が 7b:35:33:71:0b:7 c: 08:b2:47:b3:aa:f9:5 c: 0 d: ca:e4、アルゴリズムが SHA256 の証明書をアップロードしようとすると、証明書の管理処理は次のように実行されます。

1. 受信した証明書の妥当性が検証されます。
2. Tomcat 信頼フォルダから、共通名が同じである証明書が検索されます。
3. Tomcat 信頼フォルダの既存の証明書のシリアル番号と、アップロードしている受信証明書のシリアル番号がチェックされます。それらのシリアル番号が異なる場合は、両方の証明書の有効期限開始日を確認します。アップロードしている証明書の有効期限開始タイムスタンプが、既存の証明書の有効期限開始タイムスタンプよりも後である場合、Tomcat 信頼フォルダの中の既存の証明書が新しく受信した証明書で置き換えられます。そうでない場合、新しい証明書はアップロードされません。

SHA1 と SHA256 のアルゴリズムでは、件名または共通名が同じであれば、同じエンティティに属していることを意味しています。Unified Communications Manager のフレームワークでは、Unified Communications Manager サーバでそれらの 2 つのアルゴリズムを同時にサポートすることはしません。特定の信頼フォルダ内では、署名アルゴリズムが何であれ、いずれかのエンティティに属する 1 つの証明書のみがサポートされます。

電話の証明書タイプ

シスコは次の証明書タイプを電話で使用します。

- 製造元でインストールされる証明書（MIC）：Cisco Manufacturing はこの証明書をサポートされている電話に自動的にインストールします。製造元でインストールされる証明書は LSC インストールの Cisco Certificate Authority Proxy Function（CAPF）を認証します。製造元でインストールされる証明書を上書きしたり、削除することはできません。
- ローカルで有効な証明書（LSC）：このタイプの証明書は Cisco Certificate Authority Proxy Function（CAPF）に関連する必要な作業の実行後に、電話にインストールされます。デバイス セキュリティ モードを認証または暗号化に設定した後で、LSC は Unified Communications Manager と電話の間の接続を保護します。

ヒント　製造元でインストールされる証明書（MIC）をLSCのインストールでのみ使用することが推奨されます。シスコではCisco Unified Communications ManagerとのTLS接続の認証のためにLSCをサポートしています。MICルート証明書は侵害される可能性があるため、TLS認証またはその他の目的にMICを使用するように電話を設定するお客様は、ご自身の責任で行ってください。MICが侵害された場合シスコはその責任を負いません。

将来的な互換性の問題を回避するため、Unified Communications ManagerとのTLS接続にLSCを使用するためにCisco Unified IP Phone 6900シリーズ、7900シリーズ、8900シリーズ、9900シリーズをアップグレードし、MICルート証明書をCallManager信頼ストアから削除することが推奨されます。Unified Communications ManagerとのTLS接続にMICを使用する一部の電話モデルは登録できない場合があることに注意してください。

管理者はCallManager信頼ストアから次のMICルート証明書を削除する必要があります。

CAP-RTP-001

CAP-RTP-002

Cisco_Manufacturing_CA

Cisco_Root_CA_2048

Cisco_Manufacturing_CA_SHA2

Cisco_Root_CA_M2

ACT2_SUDI_CA

CAPF信頼ストアに残されたMICルート証明書は、証明書のアップグレードに使用されます。CallManager信頼ストアの更新および証明書の管理についての詳細は、このリリースに対応した『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。

（注）　CallManager信頼ストアから証明書を削除した場合、UCMは電話機のMICを信頼しないため、セキュア オンボーディング機能は動作しません。

サーバ証明書のタイプ

Unified Communications Managerサーバでは次の自己署名（所有）証明書タイプが使用されます。

- HTTPS証明書（Tomcat）:自己署名ルート証明書は、HTTPSサーバのUnified Communications Managerインストール時に生成されます。Cisco Unity Connectionは、SMTPおよびIMAPサービスにこの証明書を使用します。
- CallManager証明書：自己署名ルート証明書はUnified Communications Managerサーバに Unified Communications Managerを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。

- CAPF 証明書：Cisco CTL クライアント設定を完了すると、Unified Communications Manager のインストール時に生成されるこのルート証明書が、ご使用のサーバまたはクラスタ内のすべてのサーバにコピーされます。
- IPSec 証明書（ipsec_cert）：自己署名ルート証明書は、Unified Communications Manager のインストール時に、MGCP および H.323 ゲートウェイとの IPSec 接続用に生成されます。
- SRST 対応ゲートウェイの証明書：[Unified Communications Manager Administration] でのセキュアな SRST リファレンスの設定時に、Unified Communications Manager は SRST 対応ゲートウェイの証明書をゲートウェイから取得し Unified Communications Manager データベースに保存します。デバイスをリセットすると、証明書は電話の設定ファイルに追加されます。証明書はデータベースに格納されているため、証明書の管理ツールでこの証明書を管理することはできません。
- TVS 証明書：信頼検証サービス（TVS）をサポートする自己署名証明書です。
- Phone-SAST-trust 証明書：このカテゴリでは、システムが Cisco Unified IP Phone の VPN 証明書をインポートできます。これらの証明書は Midlet 信頼ストアに保存されます。
- 電話証明書信頼ストア（Phone-trust）：Unified Communications Manager はこの証明書タイプを使用して電話での HTTPS アクセスをサポートします。Cisco Unified Communications Operating System GUI を使用して証明書を Phone-trust ストアにアップロードできます。Cisco Unified IP Phone からの安全な Web アクセス（HTTPS）をサポートするため、Phone-CTL-trust にある証明書は CTL ファイルのメカニズムによって電話にダウンロードされます。電話の信頼証明書はサーバに残り、電話は TVS 経由でリクエスト可能です。

Unified Communications Manager は次のタイプの証明書を CallManager 信頼ストアにインポートします。

- Cisco Unity サーバまたは Cisco Unity Connection 証明書：Cisco Unity および Cisco Unity Connection はこの自己署名ルート証明書を使用して Cisco Unity SCCP および Cisco Unity Connection SCCP のデバイス証明書に署名します。Cisco Unity では、Cisco Unity Telephony Integration Manager（UTIM）がこの証明書を管理します。Cisco Unity Connection では、Cisco Unity Connection Administration がこの証明書を管理します。
- Cisco Unity および Cisco Unity Connection SCCP デバイス証明書：Cisco Unity および Cisco Unity Connection SCCP デバイスはこの署名付き証明書を使用して Unified Communications Manager との TLS 接続を確立します。
- 証明書の名前はボイス メール サーバ名に基づく証明書のサブジェクト名のハッシュを表しています。すべてのデバイス（またはポート）が、ルート証明書をルートとする証明書を発行します。
- SIP プロキシ サーバの証明書：CallManager 信頼ストアに SIP ユーザ エージェントの証明書が含まれ、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、SIP トランク経由で接続する SIP ユーザ エージェントは Unified Communications Manager に対して認証されます。

次の信頼ストアがあります。

- Tomcat および Web アプリケーション用の共通信頼ストア
- IPSec-trust
- CAPF-trust
- Userlicensing-trust
- TVS-trust
- Phone-SAST-trust
- Phone-CTL-trust

外部 CA からの証明書のサポート

Unified Communications Manager は PKCS#10 証明書署名要求（CSR）のメカニズムを利用してサードパーティ認証局（CA）との統合をサポートします。これは Cisco Unified Communications Operating System 証明書マネージャ GUI でアクセス可能です。現在サードパーティ CA を使用しているお客様は、Cisco CallManager、CAPF、IPSec、および Tomcat 証明書を発行するために CSR のメカニズムを使用する必要があります。

（注） マルチサーバ（SAN）CA 署名付き証明書を使用する際、マルチサーバ証明書は、パブリッシャにアップロードされる時点でクラスタに存在するノードのみに適用されます。したがって、ノードを再構築したり、クラスタに新しいノードを追加したりするたびに、新しいマルチサーバ証明書を生成して、クラスタにアップロードする必要があります。

システムを混合モードで実行すると、キー サイズが 4096 以上の CA 証明書を受け入れないエンドポイントもあります。CA 証明書を混合モードで使用するには、次のいずれかのオプションを選択してください。

- 証明書のキー サイズが 4096 未満の証明書の使用
- 自己署名証明書の使用

（注） このリリースの Unified Communications Manager は SCEP インターフェイスをサポートしません。

サードパーティの CA 署名付き証明書をプラットフォームにアップロードした後、CTL クライアントを実行して CTL ファイルを更新する必要があります。CTL クライアントの実行後、更新のために適切なサービスを再起動します。たとえば、Unified Communications Manager 証明書を更新するときは Cisco CallManager および Cisco TFTP サービスを再起動し、CAPF 証明書を更新するときは CAPF を再起動します。

（注） Cisco CallManager 証明書または CAPF 証明書をアップロードした後に、ITL ファイルを更新するために自動的に電話がリセットされる場合があります。

プラットフォームでの証明書署名要求（CSR）の生成については、この Unified Communications Manager リリースに対応した『Administration Guide for Cisco Unified Communications Manager』を参照してください。

認証、整合性、および許可

整合性および認証によって、次の脅威から保護されます。

- TFTP によるファイル操作（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）
- 表 1 : 用語 （2 ページ） 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）

許可では、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アクションを指定します。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

このプロセスは、電話へのロード前にバイナリ イメージ（ファームウェア ロード）が改ざんされることを防止します。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 アップデートでも、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 Phone、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。相互認証が、相互証明書交換のこのプロセスを表しています。

デバイス認証は、Cisco CTL 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『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。

ファイル認証

このプロセスは、設定ファイル、リング リスト ファイル、ロケール ファイル、および CTL ファイルなど、電話によってダウンロードされる、デジタル署名されたファイルを検証します。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、リング リスト ファイル、ローカライズ ファイル、default.cnf.xml、リング リスト WAV ファイルなどのスタティック ファイルは TFTP サーバによって、.sgn フォーマットで署名されます。TFTP サーバは、ファイルのデータに発生した変更を検証するたびに、<device name>.cnf.xml フォーマットでファイルに署名します。

キャッシュが無効の場合、TFTP サーバは署名付き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が TFTP サーバによって確認された場合、TFTP サーバによってファイルが再度署名されます。ディスクの新しいファイルによって保存済みファイルが上書きされ、保存済みファイルは削除されます。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。

電話では、ファイルが TFTP サーバから受信されると、署名の検証によってファイルの整合性が確認されます。電話で認証済み接続を確立するには、次の条件への適合を確認します。

- 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。
- デバイスに認証または暗号化が設定されていること。

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影響しないことに注意してください。

（注） あるデバイスのダイジェスト認証を有効にすると、登録する一意のダイジェスト ユーザ ID とパスワードが要求されます。

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。

- アプリケーションには、[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には、[End User] ウィンドウでダイジェスト認証用の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と関連付けるには、[Phone Configuration] ウィンドウで [Digest User]（エンドユーザ）を選択します。電話をリセットした後、クレデンシャルは TFTP サーバからその電話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チャレンジの場合、レルム ユーザ名（デバイスまたはアプリケーション ユーザ）およびダイジェスト クレデンシャルを指定する SIP レルムを設定します。

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。ナンス有効期間は、電話またはトランクの SIP デバイス セキュリティ プロファイルで設

定します。ナンス有効期間には、ナンス値が有効な時間を分単位で指定します。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 メッセージを発信した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、TLS をサポートするデバイスであれば、デバイスに TLS プロトコルを設定します。暗号化をサポートするデバイスであれば、デバイス セキュリティ モードを暗号化に設定します。暗号化された電話設定ファイルをサポートするデバイスであれば、ファイルに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。電話へのチャレンジについて SIP レルムを設定するには、サービス パラメータ [SIP Station Realm] を使用します。各ダイジェスト ユーザには、レルムごとに 1 セットのダイジェスト クレデンシャルを設定できます。

ヒント エンドユーザのダイジェスト認証を有効にするが、ダイジェストクレデンシャルを設定しない場合、電話の登録が失敗します。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、xyz.com のように SIP トランクを介して接続される領域を表し、要求の送信元を判別するのに役立ちます。

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の関連項目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 エージェントには、レルムごとに 1 セットのダイジェスト クレデンシャルを設定できます。

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。[SIP Trunk Security Profile Configuration] ウィンドウで、許可する SIP 要求をオンにする際に、許可を指定します。

SIP トランクの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 [Enable Digest Authentication] チェックボックスをオンにしてから、[Application User Configuration] ウィンドウで許可する SIP 要求のチェックボックスをオンにします。

SIP トランクの許可とアプリケーション レベルの許可（認証）の両方を有効化した場合、最初に SIP トランクの許可が実行され、次に SIP アプリケーション ユーザの許可が実行されます。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 Forbidden 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。このため、アプリケーションレベルの許可（認証）を実行するには、事前に [SIP Trunk Security Profile] でダイジェスト認証を有効にする必要があります。

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資格情報

Unified Communications Manager リリース 12.5(1) 以降、すべてのエンドユーザーログイン資格情報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 クレデンシャルの [SHA1] のみを使用してハッシュされました。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] 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パスワードまたは PIN はすべて、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）資格情報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。

レポートを生成する方法の詳細についてを参照してください、 *Cisco Unified CM Administration Online Help* 。

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、メディア ストリームによるファイアウォール トラバーサルを許可できます。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のメディア 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置く必要があります。

シグナリング暗号化では、NAT トラバーサルがサポートされません。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

Secure Real-Time Protocol（SRTP）を使用するメディア暗号化により、サポートされるデバイス間で対象の受信者だけがメディア 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。1 つ以上のデバイスが SRTP をサポートしていない場合は、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。Cisco IOS ゲートウェイおよびトランクでは、認証なしのメディア暗号化がサポートされています。SRTP 機能（メディア暗号化）を有効にする場合、Cisco IOS ゲートウェイおよびトランクに IPSec を設定する必要があります。

警告 Cisco IOS MGCP ゲートウェイ、H.323 ゲートウェイおよび H.323/H.245/H.225 トランクにおいて、セキュリティ関連情報が暗号化されずに送信されないようにすることは、IPSec 設定に依存しています。したがって、ゲートウェイおよびトランクに SRTP またはシグナリング暗号化を設定する前に、IPSec を設定することを強く推奨します。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、セキュリティ関連情報が公開される可能性があります。

SIP トランクでは、セキュリティ関連情報が暗号化されない状態で送信されることがないようにするために、TLS が使用されます。

次の例は、SCCP および MGCP 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 つのセットを受け取ります。 1 つはデバイス A からデバイス B へのメディア ストリーム用のセット、もう 1 つはデバイス B からデバイス A へのメディア ストリーム用のセットです。
4. デバイス A はマスター値の最初のセットを使用して、デバイス A からデバイス B へのメディア ストリームの暗号化と認証のためのキーを導出します。

5. デバイス A はマスター値の 2 番目のセットを使用して、デバイス B からデバイス A へのメディア ストリームの認証と復号のためのキーを導出します。
6. デバイス B はこれとは反対の操作手順でこれらのセットを使用します。
7. デバイスは、キーを受信した後に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項目を参照してください。

AES 256 Encryption Support for TLS and SIP SRTP

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、暗号化アルゴリズムとして、128 ビットの暗号キーを使用した Advanced Encryption Standard（AES）が使用されています。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、変化していく不可欠なセキュリティとパフォーマンスのニーズを満たすために有効に拡張できません。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、AES 128 の代わりに、AES 256 暗号化のサポートが、NGE をサポートする TLS and Session Initiation Protocol（SIP）SRTP に提供されています。

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 トランクおよび SIP 回線が開始する接続であること。
- 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。

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 Transmission Control Protocol（TCP）層とアプリケーション間のプロトコル層として位置付けられ、各クライアントとサーバ間にセキュアな接続を形成して、それらがネットワークを通じて安全に通信できるようにします。TLS が動作するためには、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。

値は次のとおりです。

- TLS は、Transport Layer Security です
- ECDH は、アルゴリズムの楕円曲線 Diffie-Hellman です
- RSA は、アルゴリズムの Rivest Shamir Adleman です
- 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）では、Real-time Transport Protocol（RTP）の音声メディアとビデオ メディアの両方と、それらに付随する Real-time Transport Control Protocol（RTCP）ストリームに対して機密性およびデータの整合性を提供する方法を定義します。SRTP では、暗号化とメッセージ認証ヘッダーを使用して、この方法を実装します。SRTP では、暗号化は RTP パケットのペイロードだけに適用され、RTP の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。これらの暗号方式は、AEAD_AES_256_GCM と AEAD_AES_128_GCM で、AEAD は Authenticated-Encryption with Associated-Data、GCM は Galois/Counter Mode 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）内に存在する場合、AES 128 ベースの暗号方式および SHA-1 ベースの暗号方式に比べてより高い優先順位で処理されます。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 トランクと SIP 回線接続について TLS バージョン 1.2 がサポートされました。
- 暗号のサポート：TLS 1.2 接続時に、TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384（暗号ストリング ECDHE-RSA-AES256-GCM-SHA384）および TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256（暗号ストリング ECDHE-RSA-AES128-GCM-SHA256）が利用可能です。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 回線と SIP トランクを介した SRTP コールでは、GCM ベースの AEAD_AES_256_GCM 暗号方式と AEAD_AES_128_GCM 暗号方式がサポートされます。

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では、これまでのサポートされていた暗号による TLS バージョン使用時の動作が引き続きサポートされます。Skinny Call Control Protocol（SCCP）では、これまでにサポートされていた暗号による TLS 1.2 もサポートされています。
- 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は、MOH、IVR、アナンシエータを AES_CM_128_HMAC_SHA1_80 暗号化アルゴリズムを用いて再生します。

電話が IP 音声メディア ストリーミング（IPVMS）に安全に接続する際、AES_CM_128_HMAC_SHA1_80 暗号化アルゴリズムが優先的に使用されます。電話が 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 *5:* 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

電話がサポートする暗号化アルゴリズム	ネゴシエーション暗号
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。

自己暗号化ドライブ

統一された CM 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、https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/sw/gui/config/guide/2-0/b_Cisco_UCS_C-series_GUI_Configuration_Guide_201/b_Cisco_UCS_C-series_GUI_Configuration_Guide_201_chapter_010011.html#concept_E8C37FA4A71F4C8F8E1B9B94305AD844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 Phone 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。このオプションが有効にされると、デバイス設定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、機密データの電話へのダウンロードにクリアテキストを選択することもできます。たとえば、電話のトラブルシュートや自動登録などの場合が考えられます。

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。

暗号化された iX チャネル

Unified Communications Manager は、暗号化された iX チャンネルをサポートしています。IX チャネルは、ビデオ会議でのSIPフォン間でアプリケーションメディアを多重化するための信頼性の高いチャネルを提供します。暗号化された iX チャネルは、DTLS を使用して導入にセキュリティを追加し、アプリケーションメディアがiXチャネルを介して送信されるようにし、メディアを傍受しようとする中級者が見ることができないようにします。

[パススルーモード] の IOS MTP および RSVP エージェントは、暗号化された iX チャネルもサポートしています。

設定

ユニファイドコミュニケーションマネージャーの暗号化されたiXチャネルを有効にするには、次のことを実行する必要があります。

- 任意の中間 SIP トランクによって使用される [SIP プロファイル設定（SIP Profile Configuration）] の [**iX アプリケーション メディアを許可（Allow iX Application Media**）] チェックボックスをオンにします。この設定では、iXチャネルのネゴシエーションがオンになります。
- セキュア着信**アイコン表示ポリシー**サービスパラメータを設定して、セキュアロックアイコンを有効にします。デフォルトでは、[**BFCP および iX トランスポート以外の全メディアを暗号化すべき（All media except BFCP and iX transports must be encrypted**）] に設定されています。

暗号化モード

暗号化された電話機の場合、2 種類のセッション記述プロトコル (SDP) を使用して、ユニファイドコミュニケーションマネージャーがサポートしている暗号化チャネルの暗号化をサポートしています。この暗号化タイプは、エンドポイントがサポートするものであり、ユニファイドコミュニケーションマネージャーの設定可能な項目ではありません。

- **ベストエフォート方式**の暗号化: SDP オファーは暗号化された ix チャネルを目的としていますが、SIP ピアがサポートしていない場合は、暗号化されていない ix チャネルにフォー

ルバックします。このアプローチは、ソリューションで暗号化が必須ではない場合に使用することができます。

たとえば、暗号化はクラウドで必須であり、単一の企業ではありません。

ベストエフォート iX 暗号化

M = アプリケーション 12345 **UDP/UDT/IX ***

A = セットアップ: actpass

A = 指紋: SHA-1 < キー >

- **強制暗号化**: SDP オファーは、暗号化された iX チャネルに対してのみ使用できます。このオファーは、SIP ピアが iX チャネルの暗号化をサポートしていない場合には拒否されます。このアプローチは、エンドポイント間で暗号化が必須になっている展開で使用できます。

  たとえば、2 つの SIP デバイス間の暗号化は必須です。

  強制 iX 暗号化

  m = アプリケーション 12345 **UDP/DTLS/UDT/IX ***

  A = セットアップ: actpass

  A = 指紋: SHA-1 < キー >

デフォルトでは、すべての Cisco IP Phone はベストエフォート iX 暗号化を提供するように設定されています。ただし、Ciscoテレプレゼンスエンドポイントの製品固有の設定**内で**暗号化**モード**をオンに設定するか、または cisco Meeting Server の設定を再設定することによって、これを強制的に暗号化にすることができます。

非暗号化メディア

エンドポイントが完全なセキュア モードで導入されていない可能性がある場合は、Unified Communication Manager を使用して、会議のエンドポイントからのメディア パスでセキュア アクティブコントロールメッセージをネゴシエートできます。たとえば、エンドポイントがオフネットで、MRA モードの CUCM で登録されている場合などです。

前提条件

この機能の使用を開始する前に、次のことを確認してください。

- システムが輸出規制要件を満たしている
- 会議ブリッジへの SIP トランクがセキュアである

Unified CM は、セキュアでないエンドポイントまたはソフトフォンに対してセキュアアクティブ コントロール メッセージの DTLS 情報をネゴシエートし、次の方法でメッセージを受信できます。

- オンプレミスの登録済みエンドポイントまたはソフトフォンに対しては**ベストエフォート方式の暗号化 iX**

- オフプレミスの登録済みエンドポイントまたはソフトフォンに対しては**強制 iX 暗号化**

NMAP スキャン操作

すべての Windows または Linux プラットフォームで脆弱性スキャンを実行するには、Network Mapper（NMAP）スキャン プログラムを実行できます。NMAP はネットワーク調査やセキュリティ監査を行う、無料のオープン ソースのユーティリティです。

（注） NMAP DP スキャンは、完了までに最大 18 時間かかります。

シンタックス

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

値は次のとおりです。

-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、NMAP が出力する進行中のスキャンに関する情報が増えます。開いているポートは検出次第表示され、NMAP がスキャンに数分以上かかると推定した場合には完了までにかかる時間が表示されます。冗長度をさらに上げるには、このオプションを 2 回以上使用します。

-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、デフォルトをオーバーライドします。個々のポート番号と、ハイフンを使用したポート番号の範囲を使用できることにご注意ください（例：1-1023）。

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

認証と暗号化のセットアップ

重要 この手順は CTL クライアントの暗号化オプションに適用されます。また、**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もできます。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。

次の手順は、認証および暗号化を実装するために必要なすべての手順を示します。指定されたセキュリティ機能のために行う必要がある作業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。

- 新規インストールで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。

手順

ステップ 1 [Cisco Unified Serviceability] で Cisco CTL Provider サービスをアクティブにします。

クラスタの各 Unified Communications Manager サーバの Cisco CTL Provider サービスを必ずアクティブにします。

ヒント Unified Communications Manager のアップグレード前にこのサービスをアクティブにした場合は、サービスを再度アクティブにする必要はありません。アップグレード後にサービスは自動的にアクティブになります。

ステップ 2 ローカルで有効な証明書のインストール、アップグレード、トラブルシュート、または削除を行うには、[Cisco Unified Serviceability] で Cisco Certificate Authority Proxy サービスをアクティブにします。

最初のノードでのみ Cisco Certificate Authority Proxy サービスをアクティブにします。

ワンポイントアドバイス Cisco CTL クライアントをインストールして設定する前に、この作業を実行すれば、CAPF を使用するために CTL ファイルを更新する必要がなくなります。

ステップ 3 デフォルトのポート設定を使用しない場合は、TLS 接続用のポートを設定します。

ヒント Unified Communications Manager のアップグレードの前にこれらの設定項目を設定した場合は、設定項目はアップグレード中に自動的に移行されます。

ステップ 4 暗号化に Cisco CTL クライアントを使用している場合は、Cisco CTL クライアント用に設定するサーバについて、少なくとも 2 つのセキュリティ トークンとパスワード、ホスト名または IP アドレス、およびポート番号を入手します。

（注） **utils ctl** CLI オプションの場合、ハードウェア セキュリティ トークンは不要です。

ステップ 5 Cisco CTL クライアントをインストールします。

ヒント 今回のリリースの Unified Communications Manager にアップグレードした後で Cisco CTL ファイルを更新するには、今回のリリースの [Unified Communications Manager Administration] で利用可能なプラグインをインストールする必要があります。

ステップ 6 Cisco CTL クライアントを設定します。

ヒント Unified Communications Manager のアップグレード前に Cisco CTL ファイルを作成した場合、Cisco CTL ファイルはアップグレード中に自動的に移行されます。今回のリリースの Unified Communications Manager にアップグレードした後で Cisco CTL ファイルを更新するには、Cisco CTL クライアントの最新バージョンをインストールして設定する必要があります。

ステップ 7 電話セキュリティ プロファイルを設定します。

プロファイルを設定するときは、次の作業を実行します。

a) デバイスのセキュリティ モードを設定します。

ヒント デバイス セキュリティ モードは、Unified Communications Manager のアップグレード時に自動的に移行されます。以前のリリースの認証だけをサポートしていたデバイスに暗号化を設定する場合は、[Phone Configuration] ウィンドウで暗号化のセキュリティ プロファイルを選択する必要があります。

b) CAPF 設定を行います（SCCP および SIP を実行する一部の電話の場合）。

追加の CAPF 設定が [Phone Configuration] ウィンドウに表示されます。

c) SIP を実行する電話でダイジェスト認証を使用する場合は、[Enable Digest Authentication] チェックボックスをオンにします。

d) 暗号化された設定ファイルを有効にするには（SCCP および SIP を実行する一部の電話の場合）、[Encrypted Config] チェックボックスをオンにします。

e) 設定ファイルのダウンロードでダイジェスト クレデンシャルを除外するには、[Exclude Digest Credential in Configuration File] チェックボックスをオンにします。

ステップ 8 電話に電話セキュリティ プロファイルを適用します。

ステップ 9 電話に証明書を発行するように CAPF を設定します。

ヒント 今回のリリースの Unified Communications Manager へのアップグレード前に証明書の操作を実行し、CAPF をサブスクライバ サーバで実行した場合、CAPF データをパブリッシャ データベース サーバにコピーしてから、クラスタを今回のリリースの Cisco Unified Communications Manager にアップグレードする必要があります。

注意 Unified Communications Manager サブスクライバ サーバの CAPF データは Unified Communications Manager データベースに移行されないため、データをデータベースにコピーしなければ、データは失われます。データが失われても、CAPF ユーティリティを使用して発行したローカルで有効な証明書は電話に残ります。しかし、この証明書はもう有効でないため、今回のリリースの CAPF ユーティリティは証明書を再発行する必要があります。

次の手順は、省略可能です。

ステップ 10 サポートされている Cisco Unified IP Phone にローカルで有効な証明書がインストールされたことを確認します。

ステップ 11 SIP を実行する電話のダイジェスト認証を設定します。

ステップ 12 電話のセキュリティ強化作業を実行します。

ヒント 電話のセキュリティ強化設定を Unified Communications Manager のアップグレード前に設定した場合、デバイス設定はアップグレード中に自動的に移行されます。

ステップ 13 セキュリティ用の会議ブリッジ リソースを設定します。

ステップ 14 セキュリティ用のボイスメール ポートを設定します。

詳細については、このリリースの Unified Communications Manager の該当する Cisco Unity または Cisco Unity Connection 統合ガイドを参照してください。

ステップ 15 SRST リファレンスのセキュリティを設定します。

ヒント 前のリリースの Unified Communications Manager でセキュア SRST リファレンスを設定した場合、その設定は Unified Communications Manager のアップグレード中に自動的に移行されます。

ステップ 16 IPSec を設定します。

詳細については、『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。

ステップ 17 SIP トランク セキュリティ プロファイルを設定します。

ダイジェスト認証を使用する場合は、プロファイルの [Enable Digest Authentication] チェックボックスをオンにします。

トランクレベルの認証の場合、許可する SIP 要求の認証チェックボックスをオンにします。

トランクレベルの認証の後、アプリケーションレベルの許可を発生させる場合は、[Enable Application Level Authorization] チェックボックスをオンにします。

ダイジェスト認証をオンにしない限り、アプリケーションレベルの認証はオンにできません。

ステップ 18 SIP トランク セキュリティ プロファイルをトランクに適用します。

ステップ 19 トランクのダイジェスト認証を設定します。

ステップ 20 SIP トランク セキュリティ プロファイルで [Enable Application Level Authorization] チェックボックスをオンにした場合は、[Application User Configuration] ウィンドウの認証チェックボックスをオンにして、許可する SIP 要求を設定します。

ステップ 21 すべての電話をリセットします。

ステップ 22 すべてのサーバをリブートします。

暗号管理

Cipher management を使用すると、管理者は、各 TLS および SSH 接続で許可される一連のセキュリティ暗号を制御することができます。暗号管理では、弱い暗号を無効にして最小レベルのセキュリティを保証します。

[**Cipher Management**] ページには、デフォルト値はありません。代わりに、暗号化管理機能は、許可されている暗号を設定している場合にのみ有効になります。暗号管理ページで設定している場合でも、特定の弱い暗号は許可されません。

次の TLS インターフェイスおよび SSH インターフェイスで暗号を設定することができます。

- **すべての**tls: このフィールドに割り当てられている暗号は、ユニファイドコミュニケーションマネージャーおよびIMとプレゼンスのTLSプロトコルをサポートするすべてのサーバおよびクライアント接続に適用されます。
- **HTTPS TLS**: このフィールドに割り当てられる暗号は、ユニファイドコミュニケーションマネージャーおよびIMおよびプレゼンスのTLSプロトコルをサポートするポート443および8443上のすべてのCisco Tomcat接続に適用されます。**Https tls**および**すべての TLS**フィールドに暗号**を割り当てる場合、https tls**上で設定されて**いる暗号**がすべてのtls暗号を上書きします。
- **SIP TLS**: このフィールドに割り当てられる暗号は、ユニファイドコミュニケーションマネージャー上のTLSプロトコルをサポートするsip tlsインターフェイスを介して送受信されるすべての暗号化接続に適用されます。SCCPまたはCTIデバイスには適用されません。

  認証モードのSIPインターフェイスは、ナル-SHA暗号のみをサポートしています。SIPインターフェイスまたはすべてのインターフェイスで暗号化を設定した場合は、認証モードはサポートされなくなります。

  SIP TLSおよび**ALL TLS**フィールドで暗号を割り当てる場合、SIP TLSで設定した暗号は、ALL TLSs暗号を上書きします。
- **SSH の暗号化**: このフィールドに割り当てられる暗号は、ユニファイドコミュニケーションマネージャーおよびIMおよびプレゼンスのSSH接続に適用されます。
- **SSH キー交換**: このフィールドで割り当てられるキー交換アルゴリズムは、ユニファイドコミュニケーションマネージャーおよびIMとプレゼンスのSSHインターフェイスに適用されます。

カーブのネゴシエーション

次に、曲線のネゴシエーションの点を示します。

- ECDSAの暗号は、ECDSA証明書のキーサイズに基づいて、さまざまなECカーブとネゴシエートされます。
- RSAの暗号化は、証明書のキーサイズに関係なく、すべてのECカーブとネゴシエートされます。
- ECDSA証明書のキーサイズは、TLSネゴシエーションを発生させるための曲線サイズと同じである必要があります。

例：

クライアントがP-384 ECのカーブを提供する場合、384キー証明書とECDSAの暗号がネゴシエートされます。

曲線のネゴシエーションは、RSA暗号とECDSA暗号の両方のクライアント設定に基づいています。

例：

証明書のサイズが384ビットであり、クライアントのオファーリングがP-521の場合、P-384 P-256 ECのネゴシエーションが発生すると、P-521の曲線でTLSネゴシエーションが発生します。クライアントによって提供されるカーブは最初のP-521であり、P-384曲線もリストから利用できます。証明書サイズが384ビットであり、クライアントオファーリングがP-521、P-256の場合、P-384曲線がクライアントによって提供されないため、TLSネゴシエーションは行われません。

EC カーブでサポートされている暗号を次に示します。

```
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
```

推奨される暗号

警告 構成済みの暗号に、以下に示す推奨暗号が含まれていることを確認してください。含まれていない場合は、セキュアインターフェイスを介した他の製品との相互運用性に問題が発生する可能性があります。変更を有効にするには、**[暗号管理（Cipher Management）]** ページの値を変更したときに、影響を受けるサービスを再起動するかサーバをリブートします。

警告 SSH MACインターフェイスでsha2-512を設定すると、DRSとCDRの機能が影響を受けます。

暗号aes128-gcm@openssh.comの設定、"ssh Cipherの" フィールド内のaes256-gcm@openssh.com、またはssh kex "のsha2-nistp256アルゴリズムのみを設定すると、DRSとCDRの機能が失われます。

シスコでは、TLSおよびSSHインターフェイスの構成用に次の暗号ストリングを推奨しています。

TLS

```
ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:
ECDHE-RSA-AES256-SHA:AES256-GCM-SHA384:AES256-SHA256:AES256-SHA:
ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-SHA256:
ECDHE-RSA-AES128-SHA:AES128-GCM-SHA256:AES128-SHA256:AES128-SHA
```

SSH 暗号

```
aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com
```

SSH MAC

```
hmac-sha2-256,hmac-sha1
```

FIPS 用の SSH KEX

```
ecdh-sha2-nistp521,ecdh-sha2-nistp384,ecdh-sha2-nistp256,diffie-hellman-group14-sha1,
diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1
```

非 FIPS 用の SSH KEX

```
ecdh-sha2-nistp521,ecdh-sha2-nistp384,ecdh-sha2-nistp256,diffie-hellman-group14-sha1,
diffie-hellman-group1-sha1,diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1
```

暗号ストリングの設定

異なるセキュリティで保護されたインターフェイスで暗号文字列を設定するには、次の手順を実行します。

始める前に

- すべての **tls**、**SIP tls**、および**HTTPS tls**フィールドに必ず暗号文字列を OpenSSL cipher string 形式で入力してください。

  Ssh の**暗号化**、ssh MAC 、および**ssh キー交換**フィールドで、OpenSSH 形式の暗号またはアルゴリズムを入力してください。

- 推奨される暗号 （44 ページ）を確認してください。

手順

ステップ 1 [Cisco Unified OS の管理（Cisco Unified OS Administration）] から、**[セキュリティ（Security）]** > **[暗号の管理（Cipher Management）]** を選択します。

ステップ 2 **ALL TLS**、**SIP TLS**、**HTTP TLS**フィールドで暗号ストリングを設定するには、暗号ストリングを OpenSSL 暗号ストリング フォーマットで **[暗号ストリング（Cipher String）]** フィールドに入力します。

OpenSSL の暗号ストリング フォーマットの詳細については、https://www.openssl.org/docs/man1.0.2/apps/ciphers.htmlを参照してください。

（注） **[HTTPS TLS]** または **[SIP TLS]** フィールドの暗号ストリングを設定しない場合、デフォルトによりシステムは **ALL TLS** インターフェイスの設定を使用します。

（注） **All TLS**または**HTTPS TLS**フィールドで暗号文字列を設定しない場合、HTTPS TLS インターフェイスポート (8443) は、エンタープライズパラメータ (HTTPS 暗号) からの設定を取得します。

（注） **All TLS**または**SIP TLS**フィールドで暗号文字列を設定しない場合、SIP インターフェイスポート (5061) は、エンタープライズパラメータ (HTTPS 暗号) からの設定を暗号化モードで取得します。さらに、NULL-SHA 暗号を認証モードで取得します。

ステップ 3 **SSH 暗号化**、フィールドで暗号ストリングを設定するには、暗号ストリングを OpenSSL 暗号ストリング フォーマットで **[暗号ストリング（Cipher String）]** フィールドに入力します。

SSH 暗号化の OpenSSH の暗号ストリング フォーマットの詳細については、https://www.ssh.com/manuals/server-admin/44/Ciphers_and_MACs.htmlを参照してください。

[**Ssh cipher (ssh cipher)**] フィールドで暗号文字列を設定しなかった場合、デフォルトでは、次の暗号がすべての ssh 接続に適用されます。

FIPS モードで、次の様になります。

```
aes128-ctr, aes192-ctr, aes256-ctr,
aes128-gcm@openssh.com, aes256-gcm@openssh.com
```

非 FIPS モードで、次のようになります。

```
aes128-ctr, aes192-ctr, aes256-ctr,
aes128-gcm@openssh.com, aes256-gcm@openssh.com
```

ステップ 4 **[SSHキー交換（SSH Key Exchange）]** のキー交換アルゴリズムを設定するには、**[アルゴリズム文字列（Algorithm String）]** フィールドにアルゴリズム文字列を OpenSSH 文字列形式で入力します。

SSH キー交換用の OpenSSH アルゴリズム文字列形式の詳細については、https://tools.ietf.org/id/draft-ietf-curdle-ssh-kex-sha2-09.htmlを参照してください。

Ssh キー交換フィールドでキー交換アルゴリズムを設定しなかった場合、デフォルトでは、次のキー交換アルゴリズムがすべての ssh 接続に適用されます。

FIPS モードで、次の様になります。

```
diffie-hellman-group1-sha1,diffie-hellman-group14-sha1,
diffie-hellman-group-exchange-sha1,diffie-hellman-group-exchange-sha256,
ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521
```

非 FIPS モードで、次のようになります。

```
diffie-hellman-group1-sha1, diffie-hellman-group14-sha1,
diffie-hellman-group-exchange-sha1,diffie-hellman-group-exchange-sha256,
ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521
```

ステップ 5 **[SSH MAC]** フィールドで MAC アルゴリズムを設定するには、**[アルゴリズム文字列（Algorithm String）]** フィールドにアルゴリズム文字列を OpenSSH 文字列形式で入力します。

SSH MAC の OpenSSH アルゴリズム文字列形式の詳細については、https://www.ssh.com/manuals/server-admin/44/Ciphers_and_MACs.html を参照してください。

[**SSH MAC**)] フィールドで MAC アルゴリズムを設定しなかった場合、次の MAC アルゴリズムがデフォルトですべての SSH 接続に適用されます。

FIPS モードで、次の様になります。

```
hmac-sha1
```

非 FIPS モードで、次のようになります。

```
hmac-sha1
```

ステップ 6 **[保存（Save）]** をクリックします。

（注） 暗号化展開文字列および**アルゴリズム拡張文字列**フィールドを編集することはできません。

システムは、**All TLS**、**STP TLS**、**HTTPS TLS**、および**SSH 暗号化** における暗号化を検証し、**[実際の暗号方式（Actual Ciphers）]** フィールドに自動的に暗号方式を入力します。

[暗号ストリング（Cipher String）] フィールドに無効な暗号が入力されると、**[暗号化拡張文字列（Cipher Expansion String）]** フィールドに自動的な入力は行われず、以下のエラーが表示されます。

無効な暗号ストリングが入力されました

システムは、**[SSHキー交換（SSH Key Exchange）]** および **[SSH MAC]** フィールドのアルゴリズムを検証し、**[アルゴリズム拡張文字列（Algorithm Expansion String）]** フィールドに自動的にアルゴリズム文字列を入力します。

[アルゴリズム文字列（Algorithm String）] フィールドに無効なアルゴリズムが入力されると、**[アルゴリズム拡張文字列（Algorithm Expansion String）]** フィールドに自動的な入力は行われず、以下のエラーが表示されます。

無効なアルゴリズム文字列が入力されました

（注） [実際の暗号方式（Actual Ciphers）] または [実際のアルゴリズム（Actual Algorithms）] フィールドに自動的に入力される暗号またはアルゴリズムは、有効な暗号またはアルゴリズムです。システムは、**暗号拡張**文字列または**アルゴリズム拡張文字列**フィールドからの暗号またはアルゴリズムを選択します。

次のタスク

構成を保存すると、次のことを実行します。

- [**すべての TLS (All TLS)**] フィールドでの暗号化を設定した場合は、クラスタ内のすべてのノードをリブートして、暗号文字列を有効にします。
- [**HTTPS TLS (HTTPS TLS)**] フィールドでのみの暗号化を設定した場合は、すべてのノード上の Cisco Tomcat サービスを再起動して、暗号文字列を有効にします。

- **SIP TLS**フィールドでのみの暗号化を設定した場合は、すべてのノードでCisco CallManagerサービスを再起動して、暗号文字列を有効にします。
- **SSHの暗号**フィールドに暗号を設定した場合は、クラスタ内のすべてのノードをリブートして、暗号文字列を有効にします。
- **SSH キー交換**または**SSH MAC**フィールドで暗号を設定した場合は、クラスタ内のすべてのノードをリブートして、アルゴリズム文字列を有効にします。

関連トピック

推奨される暗号 （44 ページ）
暗号の制限 （48 ページ）
暗号の制限 （57 ページ）

暗号の制限

[Cipher **Management** configuration] ページでは任意の数の暗号を設定できますが、各アプリケーションには、そのインターフェイスでサポートされている暗号のリストがあります。たとえば、すべて**の TLS**インターフェイスで ECDHE または DHE または ECDSA ベースの暗号が表示される場合がありますが、Cisco Call Manager などのアプリケーションでは、このような暗号をサポートしていない場合があります。EC カーブまたは dhe アルゴリズムはこのアプリケーションのインターフェイスに対して有効になっていません。個々のアプリケーションアプリケーションの暗号のサポート （49 ページ）インターフェイスでサポートされている暗号のリストについては、以下のセクションを参照してください。

GUI での検証

暗号管理ページの暗号は、OpenSSL のガイドラインに従って検証されます。たとえば、次のように設定されている暗号があるとします。失敗しました。!MD5、暗号文字列は "不良" は暗号化されていないことを認識していても、有効であると見なされます。OpenSSL は、これを有効な文字列と見なします。AES128_SHA が AES128-SHA ではなく、ハイフンではなくアンダースコアを使用して設定されている場合、OpenSSL はこれを無効な暗号 (suite) として識別します。

認証モード (NULL 暗号)

アプリケーションインターフェイスがNULLの暗号を使用している場合は、**暗号管理**ページの**ALL TLS**または**SIP TLS** フィールドに暗号リストを設定することによって、NULL 暗号のサポートを無効にすることができます。

NULL 暗号を使用するアプリケーションインターフェイスの例は次のとおりです。

- **すべての TLS インターフェイス**: tls コンテキストの設定**ページ経由の**IM およびプレゼンスの SIP プロキシ。
- **SIP TLSインターフェイス:** sip または sccp で、いずれ**かのデバイス セキュリティ プロファイル**が認証済みモードに設定されている場合に、sip または sccp が経由します。

NULL 暗号を使用する必要がある場合は、これら 2 つのインターフェイスのいずれについても暗号を設定しないでください。

オーバーライド機能

[**Cipher Management**] ページの設定により、各アプリケーションと、暗号が設定されているその他の場所のデフォルト設定が上書きされます。つまり、[**Cipher Management**] ページで暗号が設定されていない場合は、すべてのインターフェイスの元の機能が保持されます。

たとえば、**エンタープライズパラメータ**「**TLS の暗号**」が、サポートされ「ているすべて」の暗号**を使用**して設定され「ていて、*cipher Management* ページが暗号によって構成されている場合、*AES256-GCM-SHA384: AES256-SHA256*」すべて**の TLS**インターフェイスで、すべてのアプリケーション 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、**エンタプライズは無視されますパラメータ**値。

アプリケーションの暗号のサポート

次の表は、アプリケーションインターフェイスと、TLS および SSH インターフェイスでサポートされているすべての対応する暗号およびアルゴリズムを示しています。

表 *6 : TLS* 暗号のためのユニファイドコミュニケーションマネージャーの暗号サポート

アプリケーション/プロセス	プロトコル	ポート	サポート対象の暗号方式
Cisco CallManager	TCP/TLS	2443	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: ECDHE-RSA-AES256-SHA: AES256-GCM-SHA384: AES256-SHA256: AES256-SHA:CAMELLIA256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: AES128-GCM-SHA256: AES128-SHA256:AES128-SHA: CAMELLIA128-SHA
DRS	TCP/TLS	4040	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: ECDHE-RSA-AES256-SHA: DHE-RSA-CAMELLIA256-SHA: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA:CAMELLIA256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: DHE-RSA-CAMELLIA128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA:CAMELLIA128-SHA

アプリケーション/プロセス	プロトコル	ポート	サポート対象の暗号方式
Cisco Tomcat	TCP/TLS	8443 / 443	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: ECDHE-RSA-AES256-SHA: DHE-RSA-AES256-GCM-SHA384: DHE-RSA-AES256-SHA256: DHE-RSA-AES256-SHA: DHE-RSA-CAMELLIA256-SHA: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA:CAMELLIA256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: DHE-RSA-AES128-GCM-SHA256: DHE-RSA-AES128-SHA256: DHE-RSA-AES128-SHA: DHE-RSA-CAMELLIA128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA:CAMELLIA128-SHA: ECDHE-RSA-DES-CBC3-SHA: EDH-RSA-DES-CBC3-SHA: DES-CBC3-SHA ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-SHA384: ECDHE-ECDSA-AES256-SHA: ECDHE-ECDSA-AES128-GCM-SHA256: ECDHE-ECDSA-AES128-SHA256: ECDHE-ECDSA-AES128-SHA: ECDHE-ECDSA-DES-CBC3-SHA
Cisco CallManager	TCP/TLS	5061	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-GCM-SHA384 ECDHE-RSA-AES256-SHA384: ECDHE-ECDSA-AES256-SHA384: ECDHE-RSA-AES256-SHA ECDHE-ECDSA-AES256-SHA: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA:CAMELLIA256-SHA ECDHE-ECDSA-AES128-GCM-SHA256 ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256 ECDHE-ECDSA-AES128-SHA256: ECDHE-RSA-AES128-SHA ECDHE-ECDSA-AES128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA:CAMELLIA128-SHA: ECDHE-ECDSA-DES-CBC3-SHA
Cisco CTL Provider	TCP/TLS	2444	AES256-GCM-SHA384:AES256-SHA256: AES256-SHA:CAMELLIA256-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA:CAMELLIA128-SHA:
Cisco Certificate Authority Proxy Function	TCP/TLS	3804	AES256-GCM-SHA384:AES256-SHA256: AES256-SHA:CAMELLIA256-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA:CAMELLIA128-SHA:

アプリケーション/プロセス	プロトコル	ポート	サポート対象の暗号方式
CTIManager	TCP/TLS	2749	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: ECDHE-RSA-AES256-SHA: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA:CAMELLIA256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA:CAMELLIA128-SHA
シスコ信頼検証サービス	TCP/TLS	2445	AES256-GCM-SHA384:AES256-SHA256: AES256-SHA:CAMELLIA256-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA:CAMELLIA128-SHA
Cisco Intercluster Lookup Service	TCP/TLS	7501	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: ECDHE-RSA-AES256-SHA:AES256-GCM-SHA384: AES256-SHA256:AES256-SHA: CAMELLIA256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA:CAMELLIA128-SHA:
安全な設定ダウンロード (HAPROXY)	TCP/TLS	6971、6972	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: ECDHE-RSA-AES256-SHA: DHE-RSA-CAMELLIA256-SHA: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA:CAMELLIA256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: DHE-RSA-CAMELLIA128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA:CAMELLIA128-SHA: ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-SHA384: ECDHE-ECDSA-AES256-SHA: ECDHE-ECDSA-AES128-SHA256: ECDHE-ECDSA-AES128-SHA: ECDHE-ECDSA-DES-CBC3-SHA:

アプリケーション/プロセス	プロトコル	ポート	サポート対象の暗号方式
認証済み UDS 連絡先の検索	TCP/TLS	9443	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: ECDHE-RSA-AES256-SHA: DHE-RSA-CAMELLIA256-SHA: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA:CAMELLIA256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: DHE-RSA-CAMELLIA128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA:CAMELLIA128-SHA: ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-SHA384: ECDHE-ECDSA-AES256-SHA: ECDHE-ECDSA-AES128-SHA256: ECDHE-ECDSA-AES128-SHA: ECDHE-ECDSA-DES-CBC3-SHA:

表 *1: Cisco* ユニファイドコミュニケーションマネージャー *IM &* プレゼンス暗号サポートが *TLS* の暗号でサポートされています

アプリケーション/プロセス	プロトコル	ポート	サポート対象の暗号方式
Cisco SIP Proxy	TCP/TLS	8083	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: ECDHE-ECDSA-AES256-SHA384: ECDHE-RSA-AES256-SHA: ECDHE-ECDSA-AES256-SHA: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA:CAMELLIA256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-ECDSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-ECDSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: ECDHE-ECDSA-AES128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA:CAMELLIA128-SHA: ECDHE-RSA-DES-CBC3-SHA: ECDHE-ECDSA-DES-CBC3-SHA: DES-CBC3-SHA

アプリケーション/プロセス	プロトコル	ポート	サポート対象の暗号方式
Cisco SIP Proxy	TCP/TLS	5061	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: ECDHE-ECDSA-AES256-SHA384: ECDHE-RSA-AES256-SHA: ECDHE-ECDSA-AES256-SHA: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA:CAMELLIA256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-ECDSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-ECDSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: ECDHE-ECDSA-AES128-SHA: AES128-GCM-SHA256: AES128-SHA256: AES128-SHA:CAMELLIA128-SHA: ECDHE-RSA-DES-CBC3-SHA: ECDHE-ECDSA-DES-CBC3-SHA: DES-CBC3-SHA
Cisco XCP XMPP Federation Connection Manager	TCP/TLS	5269	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: ECDHE-ECDSA-AES256-SHA384: ECDHE-RSA-AES256-SHA: ECDHE-ECDSA-AES256-SHA: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA:CAMELLIA256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-ECDSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-ECDSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: ECDHE-ECDSA-AES128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA:CAMELLIA128-SHA: ECDHE-RSA-DES-CBC3-SHA: ECDHE-ECDSA-DES-CBC3-SHA: DES-CBC3-SHA

アプリケーション/プロセス	プロトコル	ポート	サポート対象の暗号方式
Cisco SIP Proxy	TCP/TLS	5062	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: ECDHE-ECDSA-AES256-SHA384: ECDHE-RSA-AES256-SHA: ECDHE-ECDSA-AES256-SHA: AES256-GCM-SHA384: AES256-SHA256:AES256-SHA: CAMELLIA256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-ECDSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-ECDSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: ECDHE-ECDSA-AES128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA:CAMELLIA128-SHA: ECDHE-RSA-DES-CBC3-SHA: ECDHE-ECDSA-DES-CBC3-SHA: DES-CBC3-SHA
Cisco XCP Client Connection Manager	TCP/TLS	5222	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: ECDHE-ECDSA-AES256-SHA384: ECDHE-RSA-AES256-SHA: ECDHE-ECDSA-AES256-SHA: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA:CAMELLIA256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-ECDSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-ECDSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: ECDHE-ECDSA-AES128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA:CAMELLIA128-SHA: ECDHE-RSA-DES-CBC3-SHA: ECDHE-ECDSA-DES-CBC3-SHA: DES-CBC3-SHA

アプリケーション/プロセス	プロトコル	ポート	サポート対象の暗号方式
Cisco Tomcat	TCP/TLS	8443、443	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: ECDHE-RSA-AES256-SHA: DHE-RSA-AES256-GCM-SHA384: DHE-RSA-AES256-SHA256: DHE-RSA-AES256-SHA: DHE-RSA-CAMELLIA256-SHA: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA:CAMELLIA256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: DHE-RSA-AES128-GCM-SHA256: DHE-RSA-AES128-SHA256: DHE-RSA-AES128-SHA: DHE-RSA-CAMELLIA128-SHA: AES128-GCM-SHA256: AES128-SHA256:AES128-SHA: CAMELLIA128-SHA: ECDHE-RSA-DES-CBC3-SHA: EDH-RSA-DES-CBC3-SHA: DES-CBC3-SHA ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-SHA384: ECDHE-ECDSA-AES256-SHA: ECDHE-ECDSA-AES128-GCM-SHA256: ECDHE-ECDSA-AES128-SHA256: ECDHE-ECDSA-AES128-SHA: ECDHE-ECDSA-DES-CBC3-SHA

表 *8 : SSH* 暗号の暗号サポート

サービス	暗号/アルゴリズム
SSH サーバ	• 暗号: aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com • MAC アルゴリズム： hmac-sha2-256 hmac-sha1 • KEX アルゴリズム： ecdh-sha2-nistp521 ecdh-sha2-nistp384 ecdh-sha2-nistp256 diffie-hellman-group14-sha1 diffie-hellman-group1-sha1 diffie-hellman-group-exchange-sha256 diffie-hellman-group-exchange-sha1

サービス	暗号/アルゴリズム
SSH クライアント	• 暗号： aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com • MAC アルゴリズム： hmac-sha2-256 hmac-sha1 • KEX アルゴリズム： ecdh-sha2-nistp521 ecdh-sha2-nistp384 ecdh-sha2-nistp256 diffie-hellman-group14-sha1 diffie-hellman-group1-sha1 diffie-hellman-group-exchange-sha256 diffie-hellman-group-exchange-sha1
DRS クライアント	• 暗号： aes128-ctr aes192-ctr aes256-ctr • MAC アルゴリズム： hmac-sha2-256 hmac-sha1 • KEX アルゴリズム： ecdh-sha2-nistp521 ecdh-sha2-nistp384 diffie-hellman-group14-sha1 diffie-hellman-group1-sha1 diffie-hellman-group-exchange-sha256 diffie-hellman-group-exchange-sha1

サービス	暗号/アルゴリズム
SFTP クライアント	• 暗号： aes128-ctr aes192-ctr aes256-ctr • MAC アルゴリズム： hmac-sha2-256 hmac-sha1 • KEX アルゴリズム： ecdh-sha2-nistp521 ecdh-sha2-nistp384 diffie-hellman-group14-sha1 diffie-hellman-group1-sha1 diffie-hellman-group-exchange-sha256 diffie-hellman-group-exchange-sha1

暗号の制限

[**Cipher Management**] ページでは、OpenSSL または OpenSSH でサポートされている暗号の設定を行うことができますが、重要なデータが偶発的に公開されることを回避するために、一部の暗号は Cisco のセキュリティ標準に基づいて内部的に無効化されています。

[**Cipher Management**] ページで暗号を設定すると、次の暗号が基本的に無効になります。

TLS を無効にした暗号

```
EDH-RSA-DES-CBC-SHA:EDH-DSS-DES-CBC-SHA:ADH-DES-CBC-SHA:
DES-CBC-SHA:KRB5-DES-CBC-SHA:KRB5-DES-CBC-MD5:EXP-EDH-RSA-DES-CBC-SHA:
EXP-EDH-DSS-DES-CBC-SHA:EXP-ADH-DES-CBC-SHA:EXP-DES-CBC-SHA:EXP-RC2-CBC-MD5:
EXP-KRB5-RC2-CBC-SHA:EXP-KRB5-DES-CBC-SHA:EXP-KRB5-RC2-CBC-MD5:EXP-KRB5-DES-CBC-MD5:
EXP-ADH-RC4-MD5:EXP-RC4-MD5:EXP-KRB5-RC4-SHA:EXP-KRB5-RC4-MD5:ADH-AES256-GCM-SHA384:
ADH-AES256-SHA256:ADH-AES256-SHA:ADH-CAMELLIA256-SHA:ADH-AES128-GCM-SHA256:ADH-AES128-SHA256:
ADH-AES128-SHA:ADH-SEED-SHA:ADH-CAMELLIA128-SHA:ADH-DES-CBC3-SHA:ADH-RC4-MD5:
AECDH-AES256-SHA:AECDH-AES128-SHA:AECDH-DES-CBC3-SHA:AECDH-RC4-SHA:AECDH-NULL-SHA:
DES-CBC3-MD5:IDEA-CBC-MD5:RC2-CBC-MD5:RC4-MD5:ECDHE-RSA-RC4-SHA:ECDHE-ECDSA-RC4-SHA:
ECDH-RSA-RC4-SHA:ECDH-ECDSA-RC4-SHA:RC4-SHA:RC4-MD5:PSK-RC4-SHA:KRB5-RC4-SHA:
KRB5-RC4-MD5:IDEA-CBC-SHA:KRB5-IDEA-CBC-SHA:KRB5-IDEA-CBC-MD5:DHE-RSA-SEED-SHA:
DHE-DSS-SEED-SHA:SEED-SHA:KRB5-DES-CBC3-MD5:NULL-MD5:PSK-AES256-CBC-SHA:
PSK-AES128-CBC-SHA:PSK-3DES-EDE-CBC-SHA:ECDHE-RSA-NULL-SHA:ECDHE-ECDSA-NULL-SHA:
ECDH-RSA-NULL-SHA:ECDH-ECDSA-NULL-SHA:NULL-SHA256:NULL-SHA
```

SSH 無効暗号

```
3des-cbc,aes128-cbc,aes192-cbc,aes256-cbc,rijndael-cbc@lysator.liu.se
```

SSH が無効になっている KEX アルゴリズム

```
curve25519-sha256@libssh.org,gss-gex-sha1-,gss-group1-sha1-,gss-group14-sha1-
```

SSH が無効になっている MAC アルゴリズム

```
hmac-sha1-etm@openssh.com,hmac-sha2-256-etm@openssh.com
```

詳細情報の入手先

関連するシスコのドキュメント

関連する Cisco IP Telephony アプリケーションと製品の詳細については、次のドキュメントを参照してください。

- 『*System Configuration Guide for Cisco Unified Communications Manager*』
- 『*Administration Guide for Cisco Unified Communications Manager*』
- 『*Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways*』
- 『*Cisco Unified Communications Manager Integration Guide for Cisco Unity*』
- 『*Cisco Unified Communications Manager Integration Guide for Cisco Unity Connection*』
- 『SRST 対応ゲートウェイに対応した *Cisco Unified Survivable Remote Site Telephony (SRST) Administration Guide*
- 『*Administration Guide for Cisco Unified Communications Manager*』
- 『*Cisco Unified Communications Manager Bulk Administration Guide*』
- 『*Cisco Unified Communications Manager*のトラブルシューティングガイド』
- 電話機モデルをサポートする *Cisco IP Phone* の管理ガイド