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。

CiscoIP 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 電話 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、CiscoIPtelephony 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ときに適用されます。

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と権限を定義するリスト。方式リストを参照してください。
認証（Authentication）	通信エンティティの id を確認するプロセス。
承認	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。
証明局（CA）	証明書を発行する信頼できるエンティティ: 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	ダイジェスト認証では、SIP ユーザエージェントに対して id を認証するよう要求します。

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、シスコの認証局が署名する 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 ファイルに署名するため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	共有パスワードの MD5 ハッシュが SIP ユーザエージェントの id を確立するために使用される、デバイス認証の形式。
[ダイジェストユーザ（Digest User）]	SIP または SIP トランクを実行している電話が送信する認証要求に含まれるユーザ名。
デジタル署名（Digital Signature）	メッセージをハッシュしてから、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用して別のハッシュを生成し、2つのハッシュを比較して、メッセージが一致し、コンテンツがそのままであることを確認します。
DSP	デジタル シグナリング プロセッサ。
DSP ファーム	H.323 またはシスコの CP ゲートウェイで Dsp によって提供される IP テレフォニー会議用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。これにより、情報の機密性が確保され、目的の受信者だけがデータを読み取ることができるようになります。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、ファイルの改ざんが発生しないように、電話機でシグニチャを検証します。
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。
hash	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保証する IETF 定義のプロトコル。暗号化を使用することにより、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が確保されます。
イメージ認証	電話機にロードする前に、バイナリイメージの整合性とソースを検証するプロセス。
整合性	エンティティ間でデータの改ざんが発生しなかったことを保証するプロセス。
IPSec	エンドツーエンドのセキュリティのためにセキュアな h.323、.H、および RAS シグナリングチャネルを提供するトランスポート。
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。電話機または JTAPI/TAPI/CTI アプリケーションにインストールされている。
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。メディア暗号化では、IETFRFC3711 で定義されているように、Secure Real Time Protocol (SRTP) を使用します。
メッセージ/データの改ざん	攻撃者が転送中にメッセージを変更しようとした場合に発生するイベント。これには、コールの終了が含まれます。
方式リスト	承認プロセス中に SIP トランクで受信できるメッセージの特定のカテゴリを制限するツール。トランク側のアプリケーションまたはデバイスに対して許可される SIP 非 Invite 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。
Nonce	ダイジェスト認証要求ごとにサーバが生成する一意のランダムな番号。MD5 ハッシュを生成するために使用されます。
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または暗号化されていないコール。
非セキュアなデバイス	UDP または TCP シグナリングおよび非セキュアメディアを使用するデバイス。

用語	定義
PKI	公開キーインフラストラクチャ。公開キーの暗号化に必要な一連の要素 (セキュアな公開キーの配布、証明書、および認証局を含む) で構成されます。
公開/秘密キー	暗号化で使用されるキー。公開キーを利用できますが、秘密鍵は、それぞれの所有者に流通する非対称暗号化は、両方のキーを使用します。
リプレイ アタック	攻撃者が、電話またはプロキシサーバを識別する情報をキャプチャし、実際のデバイスであると偽装して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を偽装します。
RTP	リアルタイム トランスポート 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 コール	すべてのデバイスが認証され、シグナリングが暗号化され、メディア (音声ストリーム) が暗号化されるコール。
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。
Transport Layer Security（TLS）	インターネット上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。機能的には SSL と同等です。

用語	定義
信頼リスト（Trust List）	デジタル署名のない証明書リスト。
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 証明書をインポートするための ITU-T 暗号化規格。証明書の形式が含まれています。

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、クラスタ内のすべてのサーバで異なる場合があります。
- 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。

関連トピック

CAPF システム インタラクションと要件

機能リスト

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、音声ドメインへのアクセスを制御および防止するためのシグナリング認証と暗号化のための TLS と IPSec が含まれています。SRTP は、音声会話やその他のメディアのプライバシーと機密性を保護するために、メディア認証と暗号化を追加します。

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
トランスポート/接続/整合性	セキュアな TLS ポート	IPSec 関連付け

セキュリティ機能	回線側	トランク側
デバイス認証	Unified Communications Manager や CAPF による TLS 証明書交換	IPSec 証明書の交換または事前共有キー
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)、またはその両方]
メディア暗号化	SRTP	SRTP
承認	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* コールセキュリティ機能

セキュリティ機能	回線側	トランク側
トランスポート/接続/整合性	セキュアな 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 証明書の交換または事前共有キー
ダイジェスト認証	各 SIP デバイスは、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 電話 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
承認	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機には、コールのセキュリティレベルが表示されます。

- 電話機には、認証済みのシグナリングセキュリティレベルのコールのシールドアイコンが表示されます。シールドは、Cisco IP デバイス間のセキュアな接続を識別します。これは、デバイスに認証済みまたは暗号化済みのシグナリングがあることを意味します。
- 電話機には、暗号化されたメディアを含むコールのロックアイコンが表示されます。これは、デバイスが暗号化された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） 一部の電話機モデルでは、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、クラスタ間、およびマルチホップコールで変更できます。SCCP 回線、SIP 回線、および h.323 シグナリングは、参加しているエンドポイントに対するコールセキュリティステータスの変更に関する通知をサポートします。セキュリティアイコンに関連付けられている制限については、セキュリティアイコンと暗号化に関連するトピックを参照してください。

コールの音声およびビデオ部分は、コールのセキュリティステータスに基づいています。音声とビデオの両方の部分がセキュアである場合にのみ、コールの安全を考慮してください。次の表では、セキュリティアイコンが表示されるかどうか、および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ルール

コール内のメディアタイプとデバイスタイプ	シールドアイコンとロックアイコンの両方を表示する電話機	ロックアイコンのみを表示する電話機
セキュアな音声のみ	ロック	ロック
セキュアでないビデオでのセキュアな音声	シールド	なし
セキュアなビデオによるセキュアな音声	ロック	ロック
非セキュア音声のみを使用する認証済みデバイス	シールド	なし
非セキュアな音声およびビデオを備えた認証済みデバイス	シールド	なし

コール内のメディアタイプとデバイスタイプ	シールドアイコンとロックアイコンの両方を表示する電話機	ロックアイコンのみを表示する電話機
非セキュア音声のみを使用する非認証デバイス	なし	なし
非セキュアな音声およびビデオを備えた未認証デバイス	なし	なし

（注） 「コールセキュリティステータスを指定した場合の BFCP アプリケーション暗号化ステータスのオーバーライド」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場合に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。

会議および割り込みコールの場合、[セキュリティ (security)] アイコンに会議のセキュリティステータスが表示されます。

関連トピック

セキュアな会議アイコン

連携動作と制限事項

ここでは、インタラクションと制限事項について説明します。

セキュア会議機能に関連付けられているインタラクションと制限については、「関連項目」を参照してください。

関連トピック

連携動作, on page 10
[Restrictions（機能制限）], on page 11
セキュアな会議リソースの設定

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シスコ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

認可されたユーザに送信されるプレゼンス要求を制限するために、プレゼンスグループを設定します。SIP を実行している電話機およびトランクに対して、プレゼンスグループの許可を追加できます。

プレゼンスグループの設定の詳細については、Cisco Unified Communications Manager 機能設定ガイドを参照してください。

SIP トランク上のプレゼンス要求を許可および受け入れるように Unified Communications Manager を設定します。必要に応じて、リモートデバイスまたはアプリケーションからの着信プレゼンス要求を受け入れ、認証するように Unified Communications Manager を設定します。

SIP Trunk

SIP で開始される転送機能や他の高度な転送関連機能を使用するには、SIP トランク セキュリティ プロファイルを設定して、着信要求、Out-of-dialog 要求、REFER 要求を受け入れます。たとえば、Web 転送やクリックツーダイヤルがあります。

イベントをレポートしたり（MWI サポート）、（音声メッセージングサーバからの）コールごとの MTP 割り当てを減らしたりするには、非要請通知 SIP 要求を受け入れるように SIP トランク セキュリティ プロファイルを設定します。

REFERS および INVITES のヘッダーを置き換える SIP 要求を受け入れるように 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 は SIP トランクの外部コールを外部デバイスまたはパーティに転送できるようになりました。

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、ユーザがログインおよびログアウトする際に、異なるエンドユーザが別のログイン情報を保有しているため、SIP ダイジェストログイン情報が変更されます。

コンピュータ テレフォニー インテグレーション（CTI）

Cisco Unified Communications Manager Assistant は、CAPF プロファイルを（Cisco Unified Communications Manager Assistant ノードごとに 1 つ）設定している場合に CTI へのセキュアな接続をサポートします（トランスポート層セキュリティ接続）。

CTI TLS サポートでは、CTI/JTAPI/TAPI アプリケーションの複数のインスタンスが実行されている場合に、すべてのアプリケーションインスタンスに固有の InstanceID（IID）を設定する必要があります。IID 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します。

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になっている場合、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と同じ場合、Cisco Unity TSP は CTI Manager ポートを介して Unified Communications Manager に接続します。

[Restrictions（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約事項について説明します。

関連トピック

認証および暗号化, on page 12

認証および暗号化

認証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。

- デバイス認証なしでシグナリングまたはメディア暗号化を実装することはできません。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、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。

  ファイアウォールでUDP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 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介して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。

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 電話 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 電話 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 電話 は、暗号化されたコールに割り込むことができます。[セキュリティ (security)] アイコンは、会議のセキュリティステータスを示します。

関連トピック

セキュアな会議アイコン

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 電話 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 電話 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 電話 （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。

- トランスコーダが関係するコール
- メディアターミネーションポイントを含むコール

（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。

電話機のサポートと暗号化

SCCP を実行している次の Cisco Unified IP 電話 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 電話 は暗号化をサポートします。6901、6911、6921、6941、6945、6961、7811、7821、7841、7861、7832、7906G、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 電話 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。これらの電話機は、認証済みまたは非セキュアの参加者としてのみ、セキュアな会議および割り込みコールに参加できます。

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 電話 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。

電話機のサポートと暗号化されたセットアップファイル

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。一部の電話機は暗号化された設定ファイルをサポートしていますが、ファイルシグニチャを検証しません。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。

関連トピック

電話機モデルのサポート

セキュリティアイコンと暗号化

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。

- コールの転送や保留などのタスクを実行すると、暗号化ロックアイコンが電話機に表示されないことがあります。MOH など、これらのタスクに関連付けられているメディアストリームが暗号化されていない場合、ステータスは [暗号化 (encrypted)] から [非セキュア (not)] 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 を含むコールの場合、セキュリティアイコンには、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が表示されます。
- TLS 転送タイプを使用している場合、SIP トランクは暗号化された、または認証されていないセキュリティステータスを報告します。SRTP がネゴシエートされると、セキュリティステータスが暗号化されます。それ以外の場合は、認証されません。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。

会議やc割り込みなどのイベント中にパーティが認証されると、SIPトランクはトランク経由で認証済みステータスを報告します。(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に、sip トランクは sip 回線で現在使用されているように、sipトランクを介してセキュリティアイコンステータスを送信するために既存のコール情報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。
- 一部の電話機モデルでは、シールドアイコンではなく、ロックアイコンのみが表示されます。

関連トピック

セキュアな会議アイコン

クラスタおよびデバイスの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 電話 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。

電話機は、クラスタセキュリティモードが混合である場合にのみ、SRST対応ゲートウェイへのセキュアな接続を試行します。電話機の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ていて、SRST が許可されているかどうかを確認します。[トランクの設定 (Trunk Configuration)] ウィンドウでチェックボックスがオンになっており、有効な SRST 証明書が電話機の設定ファイルに存在します。

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）。各コールレッグは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、各コールレッグのダイジェスト認証は他のコールレッグから独立したままになります。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暗号化が実装されている場合、サードパーティスニッフィングツールは機能しません。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

Unified Communications Manager のセキュリティを設定する際には、次のベストプラクティスをお勧めします。

- 大規模なネットワークに導入する前に、安全なラボ環境でセキュリティのインストールと設定を必ず行ってください。
- 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 IPSec を使用します。

警告 IPSec の使用に失敗した場合は、セッション暗号キーがクリアテキストで送信されます。

- 電話料金の詐欺行為の防止するため、電話会議の機能拡張を設定します。詳細については、Cisco Unified Communications Manager システム設定ガイドを参照してください。

  コールの外部転送を制限するため、設定タスクを実行します。詳細については、Cisco Unified Communications Manager 機能設定ガイドを参照してください。

関連トピック

割り込みセットアップによるメディア暗号化, on page 18
デバイス、サーバ、クラスタ、およびサービスのリセット, on page 17

デバイスのリセット、サーバとクラスタのリブート、およびサービスの再起動

ここでは、デバイスをリセットする必要がある場合、サーバ/クラスタを再起動する場合、またはシスコユニファイドサービスを再起動する必要がある場合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で別のセキュリティプロファイルを適用した後、単一のデバイスをリセットします。
- 電話機のセキュリティ強化タスクを実行する場合は、デバイスをリセットします。

- クラスタセキュリティモードを混合モードから非セキュアモード (またはその逆) に変更した後で、デバイスをリセットします。
- Cisco CTL クライアントを設定した後、または CTL ファイルを更新した後に、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、デバイスをリセットします。
- TLS 接続のポートを更新した後、Cisco CTL Provider サービスを再起動します。
- クラスタセキュリティモードを混合モードから非セキュアモード (またはその逆) に変更した後、Cisco CallManager サービスを再起動します。
- 関連付けられた CAPF サービスパラメータを更新した後、Cisco Certificate Authority Proxy Function サービスを再起動します。
- Cisco CTL クライアントを設定した後、または CTL ファイルを更新した後に、シスコユニファイドサービスのすべての Cisco CallManager および cisco TFTP サービスを再起動します。クラスタ内でこれらのサービスを実行しているすべてのサーバで、次の作業を実行します。
- CTL プロバイダーサービスを開始または停止した後、すべての Cisco CallManager および Cisco TFTP サービスを再起動します。
- セキュア SRST 参照を設定した後、依存デバイスをリセットします。
- スマートカードサービスを開始および自動に設定した場合は、Cisco CTL クライアントをインストールした PC を再起動します。
- 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ているセキュリティ関連のサービスパラメータを設定した後、Cisco IP Manager Assistant サービス、Cisco Web Dialer 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。

電話機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するトピックを参照してください。

関連トピック

電話機へのセキュリティ プロファイルの適用

デバイス、サーバ、クラスタ、およびサービスのリセット

このセクションでは、Cisco Unified Serviceability で、デバイス、サーバ、クラスタ、およびサービスをリセットするシナリオについて説明します。

クラスタ内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。

手順

Step 1 Unified Communications Managerから、**[システム（System）]** > **[CiscoUnifiedCM]** を選択します。

Step 2 [検索（Find）] をクリックします。

設定されている Unified Communications Manager サーバの リストが表示されます。

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

Step 4 [リセット（Reset）] をクリックします。

Step 5 クラスタ内のサーバごとにステップ 2 とステップ 4 を実行します。

関連トピック

デバイスのリセット、サーバとクラスタのリブート、およびサービスの再起動, on page 16

割り込みセットアップによるメディア暗号化

暗号化用に Cisco Unified IP 電話 7962 および 7942 の割り込みを設定し、 Cisco Unified Communications Manager Administration で次のタスクを実行します。

- CTL クライアントで [クラスタセキュリティモード（Cluster Security Mode）] パラメータを更新します。
- [サービスパラメータ（Service Parameter）] ウィンドウで、[有効な組み込みブリッジ（Builtin Bridge Enable）] サービスパラメータを更新します。

タスクが完了すると、次のメッセージが表示されます。

注目 Cisco Unified IP 電話 モデル 7962 および 7942 の暗号化を設定する場合、暗号化されたデバイスは、暗号化されたコールに参加しているときに割り込みリクエストを受け入れ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。

Cisco Unified IP 電話7962 および 7942 （暗号化されたセキュリティ プロファイルで設定済み）では、[電話の設定（Phone Configuration）] ウィンドウにメッセージが表示 されません。[組み込みブリッジ（Built In Bridge）] 設定に **[デフォルト（Default）]** を選択するか、または [Default] と同等のデフォルト設定を選択します。いずれの選択にも同じ制限が適用されます。

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

関連トピック

割り込みと暗号化, on page 12

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

認証サポートを取得するには、次のいずれかのオプションを使用できます。

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

トランスポートセキュリティは、データのコーディング、パッキング、および送信を処理します。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、 CiscoIOS 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。

SRTP をサポートするデバイスで次のレベルのセキュリティを確保するために、セキュア RTP (SRTP) を TLS および IPSec トランスポートサービスに追加できます。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、CiscoUnifiedIPPhones 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、リプレイ攻撃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、IP 電話 と同じようにセキュアで信頼性の高いデータ転送モードを確立し、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を表示し、自己署名証明書を再生成し、 Cisco Unified Communications オペレーティングシステムの GUI で信頼証明書を削除することができます。

管理者は、コマンドラインインターフェイス (CLI) で自己署名証明書を再生成して表示することもできます。

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、共通名と同じ有効期間があるものの、シリアル番号と署名アルゴリズムが異なっていることを確認してください。

たとえば、`27:20:41: 0c: 5b:08:69:80:42:62: 4f:13: bd:16:06: 6a`のシリアル番号と SHA1 アルゴリズムが Cisco Unified Communications Manager tomcat 信頼に存在するルート CA です。`7b:35:33:71: 0b: 7c:08: b2:47: b3: aa: f9: 5c: 0d: ca: e4`シリアル番号と SHA256 アルゴリズムを使用して証明書をアップロードしようとすると、証明書の管理は次のように行われます。

1. 着信証明書の有効性が確認されます。
2. 同じ共通名の証明書が、tomcat trust フォルダで検索されます。
3. Tomcat trust フォルダに存在する証明書のシリアル番号と、アップロードする着信証明書がチェックされます。シリアル番号が異なる場合は、両方の証明書の有効期限の開始日が確認されます。着信証明書の有効開始タイムスタンプが既存の証明書の有効開始タイムスタンプよりも後の場合、既存の証明書は tomcat trust フォルダ内の新しい着信証明書に置き換わります。それ以外の場合、新しい着信証明書はアップロードされません。

SHA1 アルゴリズムと SHA256 アルゴリズムの両方に同じサブジェクト名または共通名があります。これは、それらが同じエンティティに属していることを意味します。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。シグニチャアルゴリズムに関係なく、特定の信頼フォルダでは、どのエンティティにも属する1つの証明書のみがサポートされます。

関連トピック

電話機の証明書タイプ, on page 21
サーバ証明書のタイプ, on page 23
外部 CA からの証明書のサポート, on page 24

電話機の証明書タイプ

電話機証明書は、電話機を認証するための一意の識別子です。これは、IP 攻撃に対するセキュリティにとって重要です。

電話機の証明書は次のとおりです。

表 5:

電話機の証明書	説明
製造元でインストールされる証明書（MIC）	MIC は Cisco Manufacturing CA によって署名され、署名された証明書はサポートされている Cisco Unified IP 電話 に自動的にインストールされます。 MICは、ローカルで有効な証明書（LSC）のインストールまたは暗号化された設定ファイルのダウンロードに対して、シスコ認証局プロキシ機能（CAPF）で認証します。管理者は証明書を変更、削除、または無効にできないため、有効期限が切れた後は使用できません。
ローカルで有効な証明書（LSC）	Cisco Unified IP 電話 は、セキュアモードで動作するために LSC を必要とし、認証と暗号化に使用されます。これらは CAPF、オンラインまたはオフライン CA により署名され、MIC よりも優先されます。 CAPF に関連付けられている必要なタスクを実行すると、サポートされている電話機にこの証明書がインストールされます。認証または暗号化を使用するようにデバイス セキュリティ モードを設定した後に、LSC により、Unified Communications Manager と電話機間の接続のセキュリティが確保されます。

ヒント MIC は LSC のインストール時にのみ使用することを推奨します。シスコでは、Unified Communications Manager との TLS 接続の認証用に LSC をサポートしています。電話の設定で TLS 認証などの目的でMICを使用した場合、MICルート証明書は容易に侵害されるため、当社は何ら責任を負いません

Unified Communications Manager への TLS 接続に LSC を使用するには、Cisco Unified IP 電話 6900、7900、8900、および9900シリーズをアップグレードします。今後の互換性の問題を回避するために、Unified Communications Manager 信頼ストアから MIC ルート証明書を削除します。

（注） Unified Communications Manager への TLS 接続に MIC を使用する一部の電話機モデルは、登録できない場合があります。

管理者は Unified Communications Manager 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。Unified Communications Manager 信頼ストアの更新と証明書の管理については、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。

（注） CallManger 信頼ストアから Cisco Manufacturing 証明書を削除すると、電話機の製造元でインストールされた証明書（MIC）を検証できないため、セキュアオンボーディング機能は動作しません。

関連トピック

認証と暗号化のセットアップ, on page 42

サーバ証明書のタイプ

サーバ証明書は、基本的にサーバを識別するための証明書です。サーバ証明書は、コンテンツを暗号化および復号化する論拠の役目を果たします。

Unified Communications Manager サーバ内の自己署名証明書（所有）証明書タイプは次のとおりです。

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

表 *6*: 証明書タイプと説明

証明書タイプ	説明
Cisco Unity サーバまたは Cisco Unity Connection 証明書	Cisco Unity と 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 デバイス証明書に署名します。Cisco unityの場合、 Cisco Unity TELEPHONY Integration Manager (UTIM) はこの証明書を管理します。Cisco Unity Connection の場合は、Cisco Unity Connection の管理機能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証明書を使用して、Unified Communications Manager との TLS 接続を確立します。
SIP プロキシサーバ証明書	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 Unified Communications Manager 証明書が含まれている場合、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。

（注） 証明書名は、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ます。すべてのデバイス (またはポート) は、ルート証明書をルートとする証明書を発行します。

次の追加の信頼ストアが存在します。

- tomcat および web アプリケーションの共通信頼ストア
- IPSec-trust
- CAPF-trust
- Userlicensing: 信頼
- TVS-trust
- Phone-SAST-trust
- Phone-CTL-trust

Cisco Unity Connection の CA 信頼証明書の詳細については、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。これらの信頼証明書は、電子メール、予定表情報、連絡先を取得するための Exchange または Meeting Place Express へのセキュアな接続を確保します。

外部 CA からの証明書のサポート

Unified Communications Manager は、PKCS#10 Certificate Signing Request（CSR; 証明書署名要求）メカニズムを使用して、サードパーティの認証局（CA）との統合をサポートします。このメカニズムには、Unified Communications Manager の GUI でアクセスできます。

現在、サードパーティ CA を使用しているお客様は、CSR メカニズムを使用して次の証明書を発行する必要があります。

- Unified Communications Manager
- CAPF
- IPSec
- Tomcat
- 信頼検証サービス（TVS）

（注） マルチサーバ（SAN）の CA 署名付き証明書は、証明書が発行元にアップロードされた場合にのみクラスタ内のノードに適用されます。新しいマルチサーバ証明書を生成します。新しいノードを追加したり、再作成するたびにクラスタにアップロードします。

システムを混合モードで実行すると、一部のエンドポイントでは、キーサイズが4096以上の CA 証明書を受け入れることができない場合があります。混合モードで CA 証明書を使用するには、次のいずれかのオプションを選択します。

- 証明書のキーサイズが 4096 未満の証明書を使用します。
- 自己署名証明書を使用します。

（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。

（注） 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 クライアントを実行した後、該当するサービスを再起動して更新します。

例：

- Unified Communications Manager 証明書を更新する際 に、TFTP サービスと Unified Communications Manager サービスを再起動します。
- CAPF 証明書を更新するときに CAPF を再起動します。

Unified Communications Manager 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（CSRs）の生成方法については、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。

関連トピック

Cisco CTL クライアントの設定
デフォルトのセキュリティ設定

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。

関連トピック

認証, on page 30
デバイス認証, on page 26
ダイジェスト認証, on page 28
ファイル認証, on page 27
イメージ認証, on page 26
シグナリング認証, on page 27

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『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。

関連トピック

Certificate Authority Proxy Function
Cisco CTL クライアントの設定

電話機モデルのサポート

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。

関連トピック

Cisco CTL クライアントの設定
電話機モデルのサポート

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。

関連トピック

Cisco CTL クライアントの設定

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。

関連トピック

SIP 電話のダイジェスト認証の設定
暗号化された電話設定ファイルの設定
SIP トランクのダイジェスト認証の設定

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。

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。

関連トピック

設定ファイルの暗号化, on page 38
メディア暗号化, on page 32
シグナリング暗号化, on page 32

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。

関連トピック

セキュアな会議リソースの設定

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。

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 AES128 で、...
- TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384: 暗号ストリングは AES256 です。 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 *7:* 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。

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-Series Servers Integrated Management Controller GUI Configuration Guide』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。

関連トピック

暗号化された TFTP 設定ファイルの概要
電話機モデルのサポート

暗号化された iX チャネル

Unified Communications Managerは、暗号化されたiXチャネルをサポートします。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

Unified Communications Manager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、Unified Communications Manager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、Unified Communications Manager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 電話 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

Unified Communications Managerは、エンドポイントが完全にセキュアなモードで展開されていない場合に、会議のエンドポイントからのメディアパス内のセキュアなアクティブコントロールメッセージのネゴシエーションを有効にします。たとえば、エンドポイントがオフネットで、モバイルおよびリモートアクセスモードで Unifird CM に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。

- システムは輸出規制要件に準拠しています。
- 会議ブリッジへの SIP トランクはセキュアです。

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への**ベストエフォート暗号化 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への**強制 IX 暗号化**

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。

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。

手順

Step 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。サービスは、アップグレード後に自動的にアクティブになります。

Step 2 ローカルで有効な証明書をインストール、アップグレード、トラブルシューティング、または削除するには、シスコのユニファイドサービスで 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タスクを実行することで、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。

Step 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。

Step 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。

Step 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。

Step 6 CiscoCTL 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。

Step 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には、次のタスクを実行します。

a) デバイス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のみがサポートされているデバイスの暗号化を設定する場合は、[電話の設定 (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 を実行している一部の電話機の場合)。

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

c) SIP を実行している電話にダイジェスト認証を使用する予定の場合は、[ダイジェスト認証を有効にする (Enable Digest Authentication)] チェックボックスをオンにします。

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

e) コンフィギュレーション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。

Step 8 電話機に電話セキュリティプロファイルを適用します。

次の手順はオプションです。

Step 9 （任意） ローカルで有効な証明書がサポートされている Cisco Unified IP 電話 にインストールされていることを確認します。

Step 10 （任意） SIP を実行している電話のダイジェスト認証を設定します。

Step 11 （任意） 電話機のセキュリティ強化タスクを実行します。

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。

Step 12 （任意） セキュリティ用の会議ブリッジ リソースを設定します。

Step 13 （任意） セキュリティのために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。

Step 14 （任意） 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。

Step 15 （任意） 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。

Step 16 （任意） 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予定の場合は、プロファイルの [ダイジェスト認証の有効化 (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は、許可されている SIP 要求の [authorization] 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にアプリケーションレベルの認証を実行する場合は、[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。

Step 17 （任意） 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。

Step 18 （任意） トランクのダイジェスト認証を設定します。

Step 19 （任意） SIP トランクセキュリティプロファイルの [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 [Authorization] チェックボックスをオンにして、許可された SIP 要求を設定します。

Step 20 （任意） すべての電話をリセットします。

Step 21 （任意） すべてのサーバをリブートします。

関連トピック

Certificate Authority Proxy Function サービスの有効化
Cisco CTL Provider サービスの有効化
電話機へのセキュリティ プロファイルの適用
SIP トランクセキュリティプロファイルの適用
認証, on page 30
Cisco CTL クライアントのインストール
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, on page 18
SIP 電話のダイジェスト認証の設定
SIP トランクのダイジェスト認証の設定
暗号化された TFTP 設定ファイルのヒント
暗号化された電話設定ファイルの設定

ゲートウェイおよびトランクの暗号化の設定
電話の認証文字列の入力
ネットワーク インフラストラクチャ内の IPSec 設定
電話のセキュリティ強化
電話セキュリティプロファイルの設定の前提条件
デバイス、サーバ、クラスタ、およびサービスのリセット, on page 17
セキュアな会議リソースの設定
セキュアな Survivable Remote Site Telephony（SRST）リファレンス
CAPF のセットアップ
Cisco CTL クライアントの設定
Cisco CTL クライアントのアップグレードと Cisco CTL ファイルの移行
ダイジェスト認証のエンタープライズパラメータの設定
電話セキュリティ プロファイルの設定
セキュア ポートの設定
SIP トランク セキュリティ プロファイルの設定
システム要件, on page 7
ボイス メッセージング ポートのセキュリティ設定

暗号管理

暗号の管理はオプションの機能で、すべてのTLSおよびSSH接続で許可されるセキュリティ暗号のセットを制御できます。暗号管理を使用すると、弱い暗号を無効にして最小レベルのセキュリティを有効にすることができます。

[**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（Cipher Management）]** 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。

- [All TLS（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、Unified Communications Manager および IM and Presence Service 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、Unified Communications Manager および IM and Presence Service 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。

（注） **[HTTPS TLS]** および **[すべての TLS（All 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（All 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 暗号（SSH Ciphers）]：このフィールドに割り当てられる暗号は、Unified Communications Manager および IM and Presence Service の SSH 接続に適用されます。

- [SSH キー交換（SSH Key Exchange）]：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、Unified Communications Manager および IM and Presence Service 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。

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

このセクションでは、推奨される暗号を一覧にします。構成済みの暗号に、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。推奨される暗号を設定した後で変更を有効にするには、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-sha2-512,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-group16-sha512, diffie-hellman-group14-sha256
```

非 FIPS 用の SSH KEX

```
ecdh-sha2-nistp521, ecdh-sha2-nistp384, ecdh-sha2-nistp256,
diffie-hellman-group14-sha1, diffie-hellman-group16-sha512, diffie-hellman-group14-sha256
```

暗号ストリングの設定

- [すべての TLS（All TLS）]、[SIP TLS]、および [HTTPS TLS] フィールドに必ず暗号ストリングを OpenSSL 暗号ストリング形式で入力してください。
- また、**[SSH 暗号（SSH Ciphers）]**、**[SSH MAC]**のアルゴリズム、および**[SSH キー交換（SSH Key Exchange）]** フィールドには、OpenSSH 形式で暗号またはアルゴリズムも入力してください。
- 推奨される暗号 （47 ページ）を確認してください。

異なるセキュアなインターフェイスで暗号ストリングを設定するには、「暗号の制限事項」セクションを参照してください。

手順

Step 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。
[暗号の管理（Cipher Management）] ページが表示されます。

Step 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。

Step 3 次のフィールドに暗号ストリングを設定しない場合に発生する状況を以下に示します。

- **[すべての TLS（All TLS）] または [HTTPS TLS]** フィールド：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（Enterprise parameters）]**（HTTPS 暗号）ページから設定を実行します。
- [すべての TLS（All TLS）] または [SIP TLS] フィールド：SIP インターフェイスポート（5061）は、暗号化モードの [エンタープライズパラメータ]（TLS 暗号）ページと認証モードの NULL-SHA 暗号から設定を取得します。

（注） **[HTTPS TLS]** または **[SIP TLS]** フィールドに暗号ストリングを設定しない場合、システムはデフォルトで **[ALL TLS（すべての TLS）]** フィールドから設定を取得します。

OpenSSL 暗号ストリングの形式の詳細については、https://www.openssl.org/docs/man1.0.2/apps/ciphers.htmlを参照してください。

Step 4 **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 暗号の OpenSSH 暗号ストリング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暗号（SSH Ciphers）]フィールドに暗号ストリング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
```

Step 5 **[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（SSH Key Exchange）]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
```

Step 6 **[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
```

Step 7 **[保存（Save）]** をクリックします。

（注） **[暗号拡張文字列（Cipher Expansion String）]**および**[アルゴリズム拡張文字列（Algorithm Expansion String）]**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、以下のエラーメッセージが表示されます。

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、以下のエラーメッセージが表示されます。

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（Cipher Expansion String）]** または **[アルゴリズム拡張文字列（Algorithm Expansion String）]**フィールドから暗号またはアルゴリズムを選択します。

対応するフィールドに暗号を設定した場合は、それぞれのサービスをリブートまたは再起動する必要があります。

表 *8*: 設定された暗号と対応するアクション

設定された暗号フィールド	操作
All TLS	暗号ストリングを有効にするために、クラスタ内のすべてのノードをリブートします。
HTTPS TLS	暗号ストリングを有効にするため、すべてのノードで Cisco Tomcat サービスを再起動します。
SIP TLS	暗号ストリングを有効にするために、すべてのノードで Unified Communications Manager を再起動します。
SSH 暗号	暗号ストリングを有効にするために、クラスタ内のすべてのノードをリブートします。

設定された暗号フィールド	操作
SSH キー交換 または SSH MAC	アルゴリズム文字列を有効にするために、クラスタ内のすべてのノードをリブートします。

（注） 暗号は、**[暗号の管理（Cipher Management）]**ページの **[暗号ストリング（Cipher String）]** フィールドに入力して有効にできます。これらの暗号を入力しない場合は、アプリケーションでサポートされているデフォルトの暗号すべてが有効になります。ただし、**[暗号の管理（Cipher Management）]** ページの **[暗号ストリング（Cipher String）]** フィールドに暗号ストリングを入力しない場合は、特定の弱い暗号を無効にすることもできます。

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、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、Unified Communications Manager などのアプリケーションでは、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ではないため、このような暗号をサポートしていない場合があります。個々のアプリケーションインターフェイスでサポートされている暗号のリストの詳細については、「アプリケーションの暗号のサポート （52 ページ）」セクションを参照してください。

GUI での検証

[暗号管理（Cipher Management）] 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 ではなく、AES128_SHA が設定されている場合（ハイフンの代わりに下線を使用）、OpenSSL はこれを無効な暗号スイートとして識別します。

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（TLS Context Configuration）] ページ経由のIM and Presence の Unified Communications Manager 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（Device Security Profile）] が [認証済み（Authenticated）] 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

[暗号管理（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。

[エンタープライズパラメータ（Enterprise Parameter）]「**[TLS の暗号（TLS Ciphers）]**」 が、「*[*サポートされているすべての暗号（*ALL Supported Ciphers*）*]*」 を使用して設定されていて、**[暗号管理（Cipher Management）]** ページが、**[すべての TLS（All TLS）]** インターフェイスの「*AES256-GCM-SHA384:AES256-SHA256*」暗号によって設定されている場合、すべてのアプリケーション SIP インターフェイスは 「*AAES256-GCM-SHA384:AES256-SHA256*」 暗号のみをサポートし、**[エンタプライズパラメータ（Enterprise Parameter）]** の値は無視されます。

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 *9 : 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 ***10 : Unified Communications Manager IM & Presence*** 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	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

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 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 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 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 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

表 ***11 : 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 • 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： aes256-ctr aes256-cbc aes128-ctr aes128-cbc aes256-ctr blowfish-cbc • MAC アルゴリズム： hmac-md5 hmac-sha2-256 hmac-sha1 hmac-sha1-96 hmac-md5-96 • KEX アルゴリズム： ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group14-sha1 diffie-hellman-group-exchange-sha256 diffie-hellman-group-exchange-sha1 diffie-hellman-group1-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
エンドユーザ（Linux OS）	SHA-512 – Hashing (salted)
DRS バックアップ/ RTMT SFTP	AES-128 – Encryption
アプリケーションユーザ	AES-256 – Encryption

暗号の制限

[暗号管理（Cipher Management）] ページでは、OpenSSL または OpenSSH がサポートする暗号を設定できます。ただし、暗号の一部は、偶発的なデータが偶発的に公開されることを回避するために、Cisco のセキュリティ標準に基づいて内部的に無効になっています。

[**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 CiscoIP 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* 一括管理ガイド
- 『*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* 電話 の管理ガイド