セキュリティ

- セキュリティ （1 ページ）

セキュリティ

Internet Explorer のセキュリティオプションを設定する

サーバーから証明書をダウンロードするには、Internet Explorer のセキュリティ設定が次のように構成されていることを確認してください。

手順

ステップ 1 Internet Explorer を起動します。

ステップ 2 **[ツール]** > **[インターネット オプション]** に移動します。

ステップ 3 [Advanced]タブをクリックします。

ステップ 4 [詳細設定（Advanced）] タブの [セキュリティ（Security）] セクションまでスクロールします。

ステップ 5 必要に応じて、[**暗号化されたページをディスクに保存しない**] チェックボックスをオフにします。

ステップ 6 **OK**をクリックします。

証明書と証明書信頼リストの管理

次のトピックでは、証明書管理メニューから実行できる機能について説明します。

（注） [セキュリティ（Security）] メニュー項目にアクセスするには、管理者パスワードを使用して Cisco Unified Communications オペレーティング システムのアドミニストレーション に再度ログインする必要があります。

証明書を表示する

既存の証明書を表示するには、次の手順に従います。

手順

ステップ 1 **[セキュリティ]** > **[証明書管理]** に移動します。

証明書リスト ウィンドウが表示されます。

ステップ 2 検索コントロールを使用して証明書リストをフィルタリングできます。

ステップ 3 証明書または信頼ストアの詳細を表示するには、[共通名（Common Name）] の下にあるその証明書のファイル名をクリックします。

「証明書の詳細」ウィンドウには、証明書に関する情報が表示されます。 ファイルの整合性をチェックするために、証明書の SHA-512 チェックサム値も表示されます。

ステップ 4 証明書リスト ウィンドウに戻るには、証明書の詳細ウィンドウで [閉じる] をクリックします。

証明書をダウンロードする

Cisco Unified Communications オペレーティング システムから PC に証明書をダウンロードするには、次の手順に従います。

手順

ステップ 1 **[セキュリティ]** > **[証明書管理]** に移動します。

証明書リスト ウィンドウが表示されます。

ステップ 2 検索コントロールを使用して証明書リストをフィルタリングできます。

ステップ 3 共通名の下の証明書のファイル名をクリックします。

証明書の詳細ウィンドウが表示されます。

ステップ 4 [PEM ファイルのダウンロード（Download .PEM File）] または [.DER ファイルのダウンロード（Download .DER File）] をクリックします。

ステップ 5 [ファイルのダウンロード] ダイアログボックスで、 **[保存]** をクリックします。

証明書の削除と再生成

これらのセクションでは、証明書の削除と再生成について説明します。

証明書の削除

信頼できる証明書を削除するには、次の手順に従います。

注意 証明書を削除すると、システムの動作に影響する場合があります。 証明書リストから選択した証明書の既存の CSR はシステムから削除されるため、新しい CSR を生成する必要があります。 詳細については、 「証明書署名要求の生成」 を参照してください。

手順

ステップ 1 **[セキュリティ]** > **[証明書管理]** に移動します。

証明書リスト ウィンドウが表示されます。

ステップ 2 検索コントロールを使用して証明書リストをフィルタリングできます。

ステップ 3 共通名の下の証明書のファイル名をクリックします。

証明書の詳細ウィンドウが表示されます。

ステップ 4 [削除（Delete）]をクリックします。

証明書の再生成

証明書を再生成するには、次の手順に従います。

注意 証明書を再生成すると、システムの動作に影響する場合があります。

手順

ステップ 1 **[セキュリティ]** > **[証明書管理]** に移動します。

証明書リスト ウィンドウが表示されます。

ステップ 2 **「自己署名を生成」** > **または** > **「CSR を生成」**をクリックします。

[証明書の生成] ダイアログ ボックスが開きます。

ステップ 3 [証明書の名前（Certificate Name）] リストから、証明書の名前を選択します。 表示される証明書名の説明については、 表 6-1 を参照してください。

ステップ 4 [Generate]をクリックします。

（注）

Cisco Unified Communications オペレーティング システムで証明書を再生成した後、最新のバックアップに再生成された証明書が含まれるようにバックアップを実行する必要があります。 バックアップの実行方法については、『*Cisco Unity Connection* 用インストール・アップグレード・保守ガイド』を参照してください。

表 *1*: 証明書の名前と説明

Name	説明
tomcat	この自己署名ルート証明書は、Unity Connection サーバーのインストール中に生成され、証明書の種類は RSA キー ベースです。
ipsec	この自己署名ルート証明書は、MGCP および H.323 ゲートウェイとの IPSec 接続のインストール中に生成されます。
tomcat-ECDSA	この自己署名ルート証明書は、Unity Connection サーバーのインストール中に生成され、証明書の種類は EC キー ベースです。 （注） CallManager は証明書の命名規則でのみ使用されますが、生成される証明書は Unity Connection Server に固有です。

サードパーティの CA 証明書の使用

単一サーバー証明書と複数サーバー証明書の概要

名前が示すように、単一サーバー証明書には、その FQDN のみの信頼を識別する単一の FQDN が含まれます。 単一の FQDN またはドメインが、サブジェクト代替名（SAN）拡張に含まれます。 クラスター内に複数のサーバーがある場合、システムでは各サーバーに 1 つずつ、同数の X.509 証明書を生成する必要があります。

システムは、マルチサーバー証明書を使用して、複数のサーバー、ドメイン、またはサブドメインの信頼を識別します。 マルチサーバー証明書の SAN 拡張には、複数の FQDN またはドメインが含まれます。

（注） テレフォニー統合の場合、マルチサーバー SAN 証明書は SIP 統合でのみサポートされます。ただし、SCCP 統合では、単一サーバー証明書のみがサポートされます。

次の表は、単一サーバー証明書と複数サーバー証明書の基本的な違いを示しています。

表 *2:* 証明書の構成比較

単一サーバー証明書	マルチサーバー証明書
CN フィールドおよび/または SAN 拡張のいずれかに単一の FQDN またはドメインが含まれます。	SAN 拡張に存在する複数の FQDN またはドメインが含まれます。
システムは、クラスター内の各サーバーに 1 つの証明書を使用します。	1 つの証明書で複数のサーバーを識別します。
管理者は、証明書の有効期限切れ、秘密鍵の侵害などの状況において、各サーバー上で証明書と秘密鍵を再生成します。	この証明書は、すべてのサーバーに共通する 1 つの公開キーと秘密キーのペアのみをカバーするため、証明書とともにクラスター内のすべてのサーバーに同じ秘密キーを安全に転送する必要があります。いずれかのサーバーで秘密鍵が侵害された場合、すべてのサーバーに対して証明書と秘密鍵を再生成する必要があります。
大規模なクラスタでは、管理者がクラスタ内のサーバーごとに証明書署名要求（CSR）の生成、署名のための CA への CSR の送信、署名済み証明書のアップロードなどの手順を実行する必要があるため、単一サーバー証明書の生成は管理者にとって負担となる場合があります。	マルチサーバー証明書の管理では、管理者は特定のサーバーで一度だけ手順を実行すればよく、関連する秘密キーおよび署名済み証明書はシステムによってクラスタ内のすべてのサーバーに配布されるため、管理者の負担は軽減されます。

Cisco Unified Communications オペレーティング システムは、サードパーティの認証局 (CA) が PKCS # 10 証明書署名要求 (CSR) を使用して発行する証明書をサポートします。

次の表は、このプロセスの概要と追加ドキュメントへの参照を示しています。

	タスク	詳細情報
ステップ 1	Cisco Unified Communications オペレーティング システムのアドミニストレーション ウィンドウにログインします。	Cisco Unified Communications オペレーティング システムのアドミニストレーション では、システム管理者が、マルチサーバー オプションをサポートする個別の証明書の目的で CSR を生成するときに、配布タイプを選択できます。システムは、必要な SAN エントリを CSR に自動的に入力し、デフォルトの SAN エントリを画面に表示します。 マルチサーバー CSR を生成すると、システムはその CSR をクラスター内の必要なすべてのサーバーに自動的に配布します。 同様に、マルチサーバー CA 署名証明書をアップロードすると、システムはその証明書をクラスター内の必要なすべてのサーバーに自動的に配布します。
ステップ 2	サーバー上で CSR を生成します。	「証明書署名要求の生成」を参照してください 。
ステップ 3	CSR を PC にダウンロードします。	「証明書署名要求のダウンロード」を参照してください。
ステップ 4	CSR を使用して、CA からアプリケーション証明書を取得します。	CA からアプリケーション証明書を取得する方法については、こちらをご覧ください。「サードパーティ CA 証明書」で詳細な注意事項をご確認ください。
ステップ 5	CA ルート証明書を取得します。	CA からルート証明書を取得する方法については、こちらをご覧ください。 「サードパーティの CA 証明書」 で詳細な注意事項をご確認ください。
ステップ 6	CA ルート証明書をサーバーにアップロードします。	「信頼証明書のアップロード」 を参照してください。

	タスク	詳細情報
ステップ 7	アプリケーション証明書をサーバーにアップロードします。	「アプリケーション証明書のアップロード」 を参照してください。
ステップ 8	新しい証明書の影響を受けるサービスを再起動します。	すべての証明書の種類について、対応するサービスを再起動します。 • Tomcat 証明書または tomcat-ECDSA 証明書を更新する場合は、Cisco tomcat サービス、Connection IMAP Server、Cisco Dirsync サービス、Connection Jetty サービス、SMTP サービス、および Connection Conversation Manager サービスを再起動する必要があります。 サービスの再起動については、『Cisco Unified Communications Manager Serviceability アドミニストレーション ガイド』を参照してください。

証明書署名要求の生成

証明書署名要求を再生成するには、次の手順に従います。

手順

ステップ 1 **[セキュリティ（Security）]** > **[証明書管理（Certificate Management）]** を選択します。

証明書リスト ウィンドウが表示されます。

ステップ 2 検索コントロールを使用して証明書リストをフィルタリングします。

ステップ 3 **[CSR の作成（Generate CSR）]** をクリックすると、[証明書署名要求の作成（Generate Certificate Signing Request）] ダイアログボックスが開きます。

ステップ 4 [証明書の目的] ドロップダウン リスト ボックスから、必要な証明書の目的を選択します。

ステップ 5 [配布] ドロップダウン リスト ボックスから、必要な配布リスト項目を選択します。

（注）
マルチサーバー (SAN) オプションは、証明書の目的ドロップダウン リスト ボックスから tomcat または tomcat-ECDSA を選択した場合にのみ使用できます。 **CSR の生成** をクリックします。

デフォルトでは、システムは CN フィールドにサーバーの FQDN (またはホスト名) を入力します。 必要に応じて値を変更できます。 自己署名証明書の場合、CN は構成できません。

ステップ 6 マルチサーバー (SAN) の場合、サブジェクト代替名フィールドに追加のドメインを追加できます。

ステップ 7 「キーの長さ」ドロップダウン リスト ボックスから、証明書の目的に応じて値を選択します。

- 証明書の目的が tomcat または ipsec の場合は、1024、2048、3072、または 4096 を選択します。
- 証明書の目的が tomcat-ECDSA の場合は、256、384、または 521 を選択します。

ステップ 8 「ハッシュ アルゴリズム」ドロップダウン リスト ボックスから、証明書の目的に応じて選択します。

- 証明書の目的が tomcat または ipsec の場合は、SHA1 または SHA256 を選択します。
- 証明書の目的が tomcat-ECDSA の場合は、SHA384 または SHA512 を選択します。

ステップ 9 新しい CSR を生成するには、[生成] をクリックします。

（注）
特定の証明書タイプに対して生成された新しい CSR は、そのタイプの既存の CSR を上書きします。 CSR はクラスター内の必要なすべてのサーバーに自動的に配布されます。

証明書署名要求のダウンロード

証明書署名要求をダウンロードするには、次の手順に従います。

手順

ステップ 1 **[セキュリティ（Security）]** > **[証明書管理（Certificate Management）]** を選択します。

証明書リスト ウィンドウが表示されます。

ステップ 2 リストから、タイプが「CSR のみ」であるエントリの共通名と、共通名に一致する配布値をクリックします。

（注）
マルチサーバー SAN 証明書の場合は、タイプが「CSR のみ」で配布値が「マルチサーバー (SAN)」のエントリの共通名をクリックします。

CSR 詳細ウィンドウが表示されます。

ステップ 3 [CSR のダウンロード（Download CSR）]をクリックします。

ステップ 4 CSR のダウンロードが完了したら、[閉じる] をクリックします。

クラスター内のパブリッシャーとサブスクライバーの両方でマルチサーバー SAN 証明書を構成した後、Tomcat サービスを再起動する必要があります。 以下の手順を参照してください。

手順

ステップ 1 SSH アプリケーションを使用して Unity Connection サーバーにログインします。

ステップ 2 次の CLI コマンドを実行して Tomcat サービスを再起動します。
utils service restart Cisco Tomcat

サードパーティの CA 証明書

サードパーティの CA が発行したアプリケーション証明書を使用するには、CA から 署名済みのアプリケーション証明書と CA ルート証明書の両方を取得するか、アプリケーション証明書と CA 証明書の両方を含む PKCS#7 証明書チェーン（DER 形式）を取得する必要があります。これらの証明書の取得方法については、CA から情報を入手してください。手順は CA によって異なります。

Cisco Unified オペレーティング システムのアドミニストレーション は、PEM エンコード形式で CSR を生成します。 システムは、DER および PEM エンコード形式の証明書と、PEM 形式の PKCS#7 証明書チェーンを受け入れます。 すべての証明書タイプについて、各ノードで CA ルート証明書とアプリケーション証明書を取得してアップロードする必要があります。

Cisco Unified オペレーティング システムのアドミニストレーション の CSR には、CA にアプリケーション証明書を要求する際に含める必要がある拡張機能が含まれています。CA が ExtensionRequest メカニズムをサポートしていない場合は、次に示すように X.509 拡張機能を有効にする必要があります。

```
X509v3 Extended Key Usage:
TLS Web Server Authentication, TLS Web Client Authentication
X509v3 Key Usage:
Digital Signature, Key Encipherment, Data Encipherment
```

（注） 証明書の証明書署名要求(CSR)を生成し、SHA256 署名を使用してサードパーティの CA によって署名することができます。 その後、この署名済み証明書を Cisco Unified オペレーティング システムのアドミニストレーション にアップロードできます。これにより、Tomcat などの証明書で SHA256 がサポートされるようになります。

信頼証明書をアップロード

信頼証明書をアップロードするには、次の手順に従います。

手順

ステップ 1 **[セキュリティ（Security）]** > **[証明書管理（Certificate Management）]** に移動します。

証明書リスト ウィンドウが表示されます。

ステップ 2 **[証明書/証明書チェーンのアップロード]** をクリックします。

[証明書信頼リストのアップロード（Upload Certificate Trust List）] ダイアログボックスが開きます。

ステップ 3 **証明書の目的** ドロップダウン リストから証明書名を選択します。

ステップ 4 **説明** テキスト ボックスに CA ルート証明書の名前を入力します。

ステップ 5 アップロードするファイルを選択し、**[参照]** ボタンをクリックしてファイルに移動し、**[開く]** をクリックします。

ステップ 6 ファイルをサーバーにアップロードするには、**[アップロード]** ボタンをクリックします。

（注）
信頼証明書の場合、システムは証明書をクラスターの他のノードに自動的に配布します。

アプリケーション証明書のアップロード

Cisco Unified Communications オペレーティングシステムは、サードパーティの CA が発行する証明書をサポートしています。 PKCS#10 証明書署名要求 (CSR)。

手順

ステップ 1 サーバー上で CSR を生成します。

ステップ 2 CSR を PC にダウンロードします。

ステップ 3 CSR を使用して、CA または PKCS#7 形式の証明書チェーンからアプリケーション証明書を取得します。この証明書チェーンには、CA 証明書とともにアプリケーション証明書が含まれている場合があります。

ステップ 4 CA 証明書または証明書チェーンを取得します。

Tomcat アプリケーション証明書をアップロードするには、証明書の目的リストから **tomcat** を選択します。

Ipsec アプリケーション証明書をアップロードするには、証明書の目的リストから **ipsec** を選択します。

tomcat-ECDSA アプリケーション証明書をアップロードするには、証明書の目的リストから **tomcat-ECDSA** を選択します。

ステップ 5 **証明書の目的** ドロップダウン リストから証明書を選択します。

ステップ 6 アップロードするファイルを選択し、**[参照]** ボタンをクリックしてファイルに移動し、**[開く]** をクリックします。

ステップ 7 ファイルをサーバーにアップロードするには、**[アップロード]** ボタンをクリックします。

（注）
システムは、アプリケーション証明書を他のクラスタ ノードに自動的に配布しません。 複数のノードに同じ証明書が必要な場合は、各ノードに証明書を個別にアップロードする必要があります。 ただし、SAN証明書の場合、システムは証明書を他のクラスタ ノードに自動的に配布します。

証明書の有効期限を監視する

証明書の有効期限が近づくと、システムから自動的に電子メールが送信されます。 Certificate Expiration Monitor を表示および設定するには、次の手順に従います。

手順

ステップ 1 現在の Certificate Expiration Monitor 設定を表示するには、**[セキュリティ（Security）]** > **[証明書モニタ（Certificate Monitor）]** に移動します。

証明書モニタ ウィンドウが表示されます。

ステップ 2 必要な構成情報を入力します。 証明書モニタの有効期限フィールドの説明については、 表 6-3 を参照してください。

ステップ 3 変更を保存するには、 **[保存] をクリックします。**

表 *3*：証明書モニタフィールドの説明

フィールド	説明
通知開始時期	証明書の有効期限が切れる何日前に通知を受け取るかを入力します。
通知の頻度	通知の頻度を時間または日数で入力します。
メール通知の有効化	電子メール通知を有効にするには、チェックボックスをオンにします。
電子メール ID	通知を送信する電子メールアドレスを入力します。 （注） システムから通知を送信するには、SMTPホストを設定する必要があります。

証明書の失効

証明書の失効ステータスを取得するには、Online Certificate Status Protocol（OCSP）を使用します。

OCSP を構成するには、次の手順に従います。

手順

ステップ 1 **[セキュリティ（Security）]** > **[証明書管理（Certificate Management）]** に移動します。

証明書リスト ウィンドウが表示されます。

ステップ 2 [オンライン証明書ステータスプロトコルの設定] 領域で [OCSPの有効化] チェックボックスをオンにします。

ステップ 3 証明書が OCSP URI で構成されており、OCSP レスポンダーへの接続に使用される場合は、「証明書の OCSP URI を使用する」を選択します。

ステップ 4 OCSP レスポンダーへの接続に外部 URI または構成済み URI を使用する場合は、「構成された OCSP URI を使用する」を選択します。 [OCSP の設定済み URI（OCSP Configured URI）] フィールドに、証明書失効ステータスが確認されている、OCSP レスポンダの URI を入力します。

ステップ 5 失効チェックを実行するには、「失効チェックを有効にする」チェックボックスをオンにします。

（注）
失効および有効期限チェックのエンタープライズ パラメータが有効に設定されている場合、証明書失効サービスは LDAP および IPSec 接続に対してアクティブになります。

ステップ 6 証明書の失効ステータスを確認する周期を設定するには、[チェック間隔（Check Every）] の値を入力します。

- 失効ステータスを時間単位または日単位でチェックする場合に、[時間（Hours）] または [日（Days）] をクリックします。

ステップ 7 [保存（Save）] をクリックします。

警告
OCSP を有効にする前に、OCSP レスポンダ証明書を tomcat-trust にアップロードする必要があります。

（注）
証明書失効ステータスのチェックは、証明書または証明書チェーンのアップロード中にのみ実行され、証明書が失効している場合は適切なアラームが発生します。

証明書の失効を確実に反映させるために、Cisco Certificate Expiry Monitor サービスを再起動する必要があります。 [Cisco Unified Serviceability] > [ツール] > [コントロール センター - ネットワーク サービス] に移動し、Cisco Certificate Expiry Monitor サービスを再起動します。

IPSEC 証明書の生成

スタンドアロンまたはクラスターで ipsec 証明書を生成または再生成するには、次の手順に従います。

手順

ステップ 1 **[セキュリティ]** > **[証明書管理]** に移動します。

証明書リスト ウィンドウが表示されます。

ステップ 2 **[自己署名を生成]** > または > **[CSR を生成]** をクリックします。

[証明書の生成] ダイアログ ボックスが開きます。

ステップ 3 **証明書の目的** ドロップダウン リストから ipsec を選択します。

ステップ 4 [Generate]をクリックします。

証明書を生成すると、ipsec と ipsec trust がスタンドアロン サーバーまたはパブリッシャー サーバーの証明書で更新されます。

ステップ 5 サブスクライバサーバーの場合は、手順 1 から手順 4 に従って ipsec 証明書を生成します。 生成後、サブスクライバサーバーから ipsec 証明書をダウンロードします。

ステップ 6 サブスクライバサーバーで **[セキュリティ（Security）]** > **[証明書管理（Certificate Management）]** に移動します。

ステップ 7 **[証明書/証明書チェーンのアップロード]** をクリックします。

[証明書信頼リストのアップロード] ダイアログ ボックスが開きます。

ステップ 8 **[証明書目的（Certificate Purpose）]** ドロップダウンメニューで、[ipsec-trust] を選択します。

ステップ 9 証明書を参照して、 **[アップロード]** をクリックします。

ステップ 10 IPsec 証明書をサブスクライバサーバーにアップロードした後、以下のサービスを、まずパブリッシャサーバーで再起動し、その後サブスクライバサーバーで再起動します。

- Cisco DRF Master
- Cisco DRF Local

IPSEC 管理

次のトピックでは、IPSec メニューで実行できる機能について説明します。

（注） インストール中に、クラスター内のノード間で IPSec が自動的に設定されることはありません。

新しい IPSec ポリシーを設定する

新しい IPSec ポリシーと関連付けを設定するには、次の手順に従います。

（注） システムのアップグレード中に IPSec ポリシーを変更または作成しないでください。システムのアップグレード中に IPSec ポリシーに加えた変更は失われます。

注意 IPSec は、特に暗号化によってシステムのパフォーマンスに影響します。

手順

ステップ 1 **[セキュリティ（Security）]** > **[IPSEC の設定（IPSEC Configuration）]** に移動します。

IPSEC ポリシー リスト ウィンドウが表示されます。

ステップ 2 [新規追加] をクリックします。

IPSEC ポリシー構成ウィンドウが表示されます。

ステップ 3 IPSEC ポリシー構成ウィンドウに適切な情報を入力します。 このウィンドウのフィールドの説明については、 表 6-4 を参照してください。

ステップ 4 新しい IPSec ポリシーを設定するには、 **[保存]** をクリックします。

表 *4 : IPSEC* ポリシーとアソシエーションフィールドの説明

フィールド	説明
ポリシー グループ名（Policy Group Name）	IPSec ポリシー グループの名前を指定します。 名前には文字、数字、ハイフンのみを含めることができます。
ポリシー名（Policy Name）	IPSec ポリシーの名前を指定します。名前には文字、数字、ハイフンのみを含めることができます。
認証方式（Authentication Method）	認証方法を指定します。

フィールド	説明
事前共有キー（Preshared Key）	認証名フィールドで事前共有キーを選択した場合は、事前共有キーを指定します。 （注） 事前共有 IPSec キーには、英数字とハイフンのみを含めることができ、空白やその他の文字を含めることはできません。 Windows ベースのバージョンの Cisco Unified Communications Manager から移行する場合は、現在のバージョンの Cisco Unified Communications Manager と互換性を持たせるために、事前共有 IPSec キーの名前を変更する必要がある場合があります。
ピア タイプ（Peer Type）	ピアのタイプが同じか異なるかを指定します。
証明書の共通名	ピアタイプとして [異なる（Different）] を選択した場合は、新しい証明書の共通名を入力します。
接続先アドレス（Destination Address）	接続先の IP アドレスまたは FQDN を指定します。
宛先ポート（Destination Port）	接続先のポート番号を指定します。
ソース アドレス（Source Address）	ソースの IP アドレスまたは FQDN を指定します。
送信元ポート（Source Port）	ソースのポート番号を指定します。
モード（Mode）	トランスポートモードを指定します。
リモート ポート（Remote Port）	接続先で使用されるポート番号を指定します。
プロトコル	次のプロトコルまたは Any を指定します。 • [TCP] • UDP • 任意（Any）
暗号化アルゴリズム（Encryption Algorithm）	ドロップダウンリストから暗号化アルゴリズムを選択します。 選択肢は次のとおりです。 • DES • 3DES

フィールド	説明
ハッシュ アルゴリズム（Hash Algorithm）	ハッシュアルゴリズムを指定します • SHA1 - フェーズ 1 の IKE ネゴシエーションで使用されるハッシュアルゴリズム • MD5 - フェーズ 1 の IKE ネゴシエーションで使用されるハッシュアルゴリズム
ESP アルゴリズム（ESP Algorithm）	ドロップダウン リストから ESP アルゴリズムを選択します。 選択肢は次のとおりです。 • NULL_ENC • DES • 3DES • BLOWFISH • RIJNDAEL
フェーズ 1 のライフタイム（Phase One Life Time）	フェーズ 1 (IKE ネゴシエーション) の有効期間を秒単位で指定します。
フェーズ 1 の DH（Phase One DH）	ドロップダウン リストから、フェーズ 1 の DH 値を選択します。 選択肢は 2、1、5 です。
フェーズ 2 のライフタイム（Phase Two Life Time）	フェーズ 2 (IKE ネゴシエーション) の有効期間を秒単位で指定します。
フェーズ 2 の DH（Phase Two DH）	ドロップダウン リストから、フェーズ 2 の DH 値を選択します。 選択肢は 2、1、5 です。
ポリシーの有効化（Enable Policy）	チェックボックスをオンにして、ポリシーを有効にします。

既存の IPSec ポリシーの管理

既存の IPSec ポリシーを表示、有効化、無効化、または削除するには、次の手順に従います。

（注） システムのアップグレード中に IPSec ポリシーに変更を加えた場合、その変更は失われるため、アップグレード中に IPSec ポリシーを変更または作成しないでください。

注意 IPSec は、特に暗号化によってシステムのパフォーマンスに影響します。

⚠

注意 既存の IPSec ポリシーに変更を加えると、通常のシステム操作に影響する可能性があります。

手順

ステップ 1 **[セキュリティ （Security）]** > **[IPSEC の設定（IPSEC Configuration）]** に移動します。

（注）
[セキュリティ] メニュー項目にアクセスするには、管理者パスワードを使用して Cisco Unified Communications オペレーティング システムのアドミニストレーション に再度ログインする必要があります。

IPSEC ポリシー リスト ウィンドウが表示されます。

ステップ 2 ポリシーを表示、有効、または無効にするには、次の手順を実行します。

a) ポリシー名をクリックします。

IPSEC ポリシー構成ウィンドウが表示されます。

b) ポリシーを有効または無効にするには、**[ポリシーの有効化（Enable Policy）]** チェックボックスを使用します。

c) **[保存]** をクリックします。

ステップ 3 1 つまたは複数のポリシーを削除するには、次の手順を実行します。

a) 削除するポリシーの横にあるチェックボックスをオンにします。

[すべてを選択（Select All）]をクリックするとすべてのポリシーを選択でき、[すべてをクリア（Clear All）]を選択するとすべてのチェックボックスをクリアできます。

b) **[選択項目の削除(Delete Selected)]** をクリックします。

一括証明書管理

Extension Mobility Cross Cluster (EMCC) 機能をサポートするために、システムでは、クラスタ管理者によって設定された共通の SFTP サーバーとの間で一括インポートおよびエクスポート操作を実行できます。 一括証明書管理の使用方法の詳細については、『*Cisco Unified Communications Manager* セキュリティ機能』を参照してください。

一括証明書管理の場合は、次の手順に従います。

手順

ステップ 1 **[セキュリティ（Security）]** > **[一括証明書管理（Bulk Certificate Management）]** に移動します。 [一括証明書管理（Bulk Certificate Management）] ウィンドウが表示されます。

ステップ 2 [一括証明書管理（Bulk Certificate Management）] ウィンドウに適切な情報を入力します。 このウィンドウのフィールドの説明については、「一括証明書管理フィールドの説明」を参照してください。

ステップ 3 入力した値を保存するには、 **「保存」をクリックします。**

ステップ 4 証明書をエクスポートするには、**[エクスポート]** をクリックします。 一括証明書エクスポートポップアップ ウィンドウが表示されます。

ステップ 5 ドロップダウン メニューから、エクスポートする証明書の種類を選択します。

- Tomcat
- [TFTP]
- すべて（All）

ステップ 6 [エクスポート（Export）]をクリックします。

システムは、選択した証明書をエクスポートし、中央の SFTP サーバーに保存します。

表 *5:* 一括証明書管理フィールドの説明

フィールド	説明
IP アドレス（IP Address）	証明書をエクスポートする共通サーバーの IP アドレスを入力します。
Port	ポート番号を入力します。 デフォルト: 22
ユーザー ID（User ID）	サーバーにログインするために使用するユーザー ID を入力します。
[パスワード（Password）]	適切なパスワードを入力してください。
ディレクトリ	証明書を保存するサーバー上のディレクトリを入力します。 例: /users/cisco。

セッション管理

プラットフォーム管理者は、Cisco Unity Connection の次の Web インターフェイスについて、ユーザーまたは管理者のアクティブな Web セッションを終了できます。

- Cisco Unity Connection アドミニストレーション
- Cisco Unity Connection Serviceability
- Cisco Personal Communications Assistant
- Cisco Unity Connection Web 受信ボックス
- Cisco Unity Connection SRSV

ユーザーまたは管理者のアクティブな Web セッションを終了するには、次の手順に従います。

手順

ステップ 1 **[セキュリティ（Security）]** > **[セッション管理（Session Management）]** に移動します。 セッション管理ウィンドウが表示されます。

ステップ 2 [セッション管理（Session Management）ウィンドウで、**[ユーザーID（User ID）]** フィールドにアクティブなログインユーザーのエイリアスを入力します。

ステップ 3 ユーザーのアクティブな Web セッションを終了するには、 **[セッションを終了]** を選択します。

（注）
クラスターの場合は、クラスターの各ノードの Web セッションを終了する必要があります。

（注） セッション終了はプラットフォーム ユーザーには適用されません。 アクティブな Web セッションを終了するには、プラットフォームユーザーはセッションからログアウトするか、セッションがタイムアウトするまで待つ必要があります。

暗号管理

Cisco Unity Connection は**暗号管理**に対応しています。これにより、管理者はすべての TLS および SSH 接続で使用される暗号のセットを制御することができます。 Cisco Unity Connection のさまざまなセキュア インターフェイスに推奨される暗号を設定できます。

TLS インターフェイス

以下に記載されている TLS インターフェイスに対して、暗号を設定できます。

インターフェイス	説明
すべてのTLS	Cisco Unity Connection でサポートされているすべての TLS インターフェイスの暗号を設定できます。 例：SIP、SCCP、HTTPS、Jetty、SMTP、LDAP、IMAP インターフェイス。
HTTPS TLS	Cisco Unity Connection のすべての Cisco Tomcat インターフェイスの暗号を設定できます。
SIP TLS	Cisco Unity Connection の SIP インターフェイスの暗号を設定できます。 例：Unity Connection で安全な SIP 通話をサポートするテレフォニー ユーザー インターフェイス。 （注） SIP インターフェイスの暗号設定は、Cisco Unity Connection の無制限バージョンではサポートされていません。

SSH インターフェイス

以下に記載されている SSH インターフェイスに対して、暗号スイートおよびアルゴリズムを設定できます。

インターフェイス	説明
SSH 暗号	Cisco Unity Connection の SSH インターフェイスの暗号を設定できます。
SSH キー交換	Cisco Unity Connection の SSH インターフェイスの SSH キー交換アルゴリズムを設定できます。
SSH MAC	Cisco Unity Connection の SSH インターフェイスに対して SSH MAC アルゴリズムを設定できます。

推奨される暗号に関する詳細については、https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html にある『*Cisco Unified Communications Manager* 用セキュリティ ガイド』の「Cipher Management」の章を参照してください。

暗号文字列の設定

TLS および SSH インターフェイスの暗号文字列を設定するには、次の手順を実行します。

手順

ステップ 1 **[セキュリティ]** > **[暗号管理] に移動します。** [暗号管理] ページが表示されます。

ステップ 2 [暗号管理] ページで、 **[暗号文字列]** フィールドに、 **すべての TLS**、 **HTTPS TLS** 、 **SIP TLS** インターフェイスの暗号文字列を入力します。

（注）
HTTPS TLS または **SIP TLS** インターフェイスのいずれかに設定された暗号文字列は、[すべての TLS] フィールドで設定された暗号文字列を上書きします。

（注）
「暗号管理」 ページで設定された暗号は、 **「一般設定の編集」** ページの暗号設定を上書きします。 したがって、TLS および HTTPS インターフェイスの暗号を設定するには、 **暗号管理** ページを使用することをお勧めします。

ステップ 3 SSH 暗号の **暗号文字列** フィールドに暗号文字列を入力します。

ステップ 4 SSH キー交換のキー アルゴリズムを設定するには、 **[アルゴリズム文字列]** フィールドにアルゴリズム文字列を入力します。

ステップ 5 SSH MAC の MAC アルゴリズムを設定するには、 **[アルゴリズム文字列]** フィールドにアルゴリズム文字列を入力します。

ステップ 6 **保存**を選択します。

ページを保存した後、次の操作を実行する必要があります。

- クラスタ内の両方のノードを再起動して、 **すべての TLS**、 **SSH 暗号**、 **SSH キー交換** 、および **SSH MAC** インターフェイスの暗号を正常に構成します。
- **HTTPS TLS** インターフェイス上の暗号を正常に設定するには、Cisco Tomcat サービスを再起動します。
- **SIP TLS** インターフェイス上の暗号を正常に設定するには、Connection Conversation Manager サービスを再起動します。

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

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

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