セキュリティ

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

ノードから証明書をダウンロードするには、次の手順に従って Internet Explorer のセキュリティ設定を構成します。

ステップ 1 Internet Explorer を起動します。

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

ステップ 3 **[詳細設定（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（Do not save encrypted pages to disk）]** 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を管理する

ここでは、[証明書管理（Certificate Management）] 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管理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、次の手順を実行します。

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

[証明書一覧（Certificate List）] ウィンドウが表示されます。

ステップ 2 証明書の一覧をフィルタするには、[検索（Find）] コントロールを使用できます。

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

[証明書の詳細（Certificate Details）] ウィンドウに、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（Certificate List）] ウィンドウに戻るには、[証明書の詳細（Certificate Details）] ウィンドウで [閉じる（Close）] 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。

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

[証明書一覧（Certificate List）] ウィンドウが表示されます。

ステップ 2 証明書の一覧をフィルタするには、[検索（Find）] コントロールを使用できます。

ステップ 3 [共通名（Common Name）] の下にある証明書のファイル名をクリックします。

[証明書詳細（Certificate Details）] 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（File Download）] ダイアログボックスで、**[保存（Save）]** をクリックします。

証明書を削除、再作成する

ここでは、証明書の削除と再生成について説明します。

証明書を削除する

信頼できる証明書を削除するには、次の手順を実行します。

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（Certificate）] 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、証明書署名要求を生成するを参照してください。

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

[証明書一覧（Certificate List）] ウィンドウが表示されます。

ステップ 2 証明書の一覧をフィルタするには、[検索（Find）] コントロールを使用できます。

ステップ 3 [共通名（Common Name）] の下にある証明書のファイル名をクリックします。

[証明書詳細（Certificate Details）] 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。

証明書を再生成する

証明書を再生成するには、次の手順を実行します。

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。

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

[証明書一覧（Certificate List）] ウィンドウが表示されます。

ステップ 2 **[Generate Self-signed（自己署名付きの生成）]** > または > **[CSRの生成（Generate CSR）]** をクリックします。

[証明書の生成（Generate Certificate）] ダイアログボックスが表示されます。

ステップ 3 [証明書名（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 1 : 証明書の名前と説明を参照してください。

ステップ 4 **[生成（Generate）]** をクリックします。

（注） Cisco Unified Communications Operating System で証明書を再作成したら、システムのバックアップを実行して、最新のバックアップに再作成した証明書が含まれるようにします。バックアップの実行については、『*Cisco Unity Connection* インストール、アップグレード、およびメンテナンスガイド』を参照してください。

表 *1:* 証明書の名前と説明

名前	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時に生成され、証明書タイプは RSA キーベースです。
ipsec	この自己署名ルート証明書は、MGCP ゲートウェイおよび 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時に生成され、証明書タイプは 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 サーバーに固有です。

サードパーティの CA 証明書を使用する

シングルサーバーおよびマルチ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の信頼のみを識別する単一のFQDNが含まれています。単一のFQDNまたはドメインがサブジェクト代替名（SAN）拡張に存在します。クラスタ内に複数のサーバーがある場合、システムはサーバーごとに1つずつ、同じ数の 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ています。

（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。

次の表に、単一サーバー証明書とマルチサーバー証明書の基本的な違いを示します。

表 *2:* 証明書の設定の比較

単一サーバー証明書	マルチサーバー証明書
CNフィールドまたはSAN拡張、あるいはその両方に単一のFQDNまたはドメインが含まれています。	SAN 拡張に存在する複数の FQDN またはドメインが含まれています。

単一サーバー証明書	マルチサーバー証明書
システムは、クラスタ内のサーバーごとに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、証明書の期限切れ、秘密キーの侵害などの状況で、個々のサーバーで証明書と秘密キーを再生成します。	この証明書は、すべてのサーバーに共通の公開キーと秘密キーのペアを1つだけカバーしているため、同じ秘密キーを証明書とともにクラスタ内のすべてのサーバーに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キーが侵害された場合は、すべてのサーバーに対して証明書と秘密キーを再生成する必要があります。
管理者は、クラスタ内の各サーバーについて、証明書署名要求（CSR）の生成、署名のためのCSRのCAへの送信、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、単一のサーバー証明書の生成は、大規模クラスタの管理者にとってオーバーヘッドになる可能性があります。	管理者は、特定のサーバーで手順を1回だけ実行し、システムがクラスタ内のすべてのサーバーに関連付けられた秘密キーと署名付き証明書を配布するため、マルチサーバー証明書を管理する際のオーバーヘッドが少なくなります。

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）で発行する証明書をサポートします。

次の表に、このプロセスの概要と、その他のドキュメントへの参照を示します。

	タスク	関連情報
ステップ 1	Cisco Unified Communications Operating System Administration にログインします。	Cisco Unified Communications オペレーティング システムの管理では、システム管理者は、マルチサーバーオプションをサポートする個々の証明書の目的で CSR を生成するときに、配布タイプを選択できます。CSR に必要な SAN エントリが自動的に入力され、デフォルトの SAN エントリが画面に表示されます。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 署名付き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。	証明書署名要求を生成する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。	証明書署名要求をダウンロードする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 からのアプリケーション証明書の取得に関する情報を取得します。その他の注意事項については、 サードパーティの CA 証明書 を参照してください。
ステップ 5	CA ルート証明書を取得します。	CA からのルート証明書の取得に関する情報を取得します。その他の注意事項については、 サードパーティの CA 証明書 を参照してください。
ステップ 6	サーバーに CA ルート証明書をアップロードします。	信頼できる証明書をアップロードするを参照してください。

	タスク	関連情報
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をアップロードする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。	すべての証明書タイプについて、対応するサービスを再起動します。 • Tomcat 証明書を更新する場合は、Cisco tomcat サービス、Connection IMAP サーバー、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。 • Tomcat-ECDSA 証明書を更新する場合は、Connection Conversation Manager サービスも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。

証明書署名要求を生成する

証明書署名要求を生成するには、次の手順に従います。

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

[証明書一覧（Certificate List）] ウィンドウが表示されます。

ステップ 2 証明書の一覧をフィルタするには、検索コントロールを使用します。

ステップ 3 **[CSRの生成（Generate CSR）]** をクリックすると、[証明書署名要求の生成（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（Certificate Purpose）] のドロップダウン 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 [配信（Distribution）] ドロップダウン リスト ボックスから、必要な配信リスト項目を選択します。

（注） [マルチサーバー（SAN）（Multi-server (SAN)）] オプションは、[証明書の目的（Certificate Purpose）] 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（Generate CSR）]** 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 は設定できません。

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（Subject Alternate Names）] フィールドにドメインを追加できます。

ステップ 7 [キー長（Key Length）] 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。

- tomcat または ipsec が証明書の目的である場合は、1024、2048、3072、または 4096 を選択します。
- tomcat-ECDSA が証明書の目的である場合は、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（Hash Algorithm）] 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を選択します。

- tomcat または ipsec が証明書の目的である場合は、SHA1 または SHA256 を選択します。
- tomcat-ECDSA が証明書の目的である場合は、SHA384 SHA512 を選択します。

ステップ 9 [Generate（生成）] をクリックして新しい CSR を生成します。

（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。

証明書署名要求をダウンロードする

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。

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

[証明書一覧（Certificate List）] 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」のエントリの共通名をクリックし、共通名に一致する分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、分布値が「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（CSR Details）] 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（Close）] をクリックします。

クラスタ内のパブリッシャとサブスクライバの両方でマルチサーバー SAN 証明書を設定した後、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。

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

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 CA が発行するアプリケーション証明書を使用するには、CA から署名付き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に関する情報は、CA から入手してください。プロセスは CA によって異なります。

Cisco Unified Operating System Administration は、PEM エンコーディング形式で 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、アップロードする必要があります。

Cisco Unified Operating System Administration CSR には、CA からのアプリケーション証明書のリクエストに含める必要のある拡張子が含まれています。CA が拡張要求メカニズムをサポートしていない場合は、次の手順に従って X.509 拡張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） 使用する証明書に対して証明書署名要求（CSR）を生成し、SHA256 署名を使用してサードパーティ CA に署名させることもできます。そして、この署名された証明書を Cisco Unified Operating System Administration にアップロードし直すことで、Tomcat やその他の証明書が SHA256 をサポートできるようになります。

信頼できる証明書をアップロードする

信頼証明書をアップロードするには、以下の手順に従います。

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

[証明書一覧（Certificate List）] 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（Upload Certificate/Certificate chain）]** をクリックします。

[証明書のアップロード（Upload Certificate）] ダイアログボックスが開きます。

ステップ 3 **[証明書の用途（Certificate Purpose）]** ドロップダウンリストで、証明書名を選択します。

ステップ 4 **[説明（Description）]** 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（Browse）]** ボタンをクリックしてファイルに移動します。次に、**[開く（Open）]** 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（Upload）]** 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をアップロードする

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

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。これには、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入手します。

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（Certificate Purpose）] 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（Certificate Purpose）] 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（Certificate Purpose）] リストから **[tomcat-ECDSA]** を選択します。

ステップ 5 **[証明書の用途（Certificate Purpose）]** ドロップダウンリストで、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（Browse）]** ボタンをクリックしてファイルに移動します。次に、**[開く（Open）]** 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（Upload）]** 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。複数のノードで同じ証明書を使用する必要がある場合は、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。

証明書の失効日をモニターする

証明書の有効期限が近づくと、システムが自動的に電子メールを送信することができます。証明書の有効期限モニターを表示および設定するには、次の手順を実行します。

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

[証明書モニター（Certificate Monitor）] ウィンドウが表示されます。

ステップ 2 必要な設定情報を入力します。[証明書モニターの有効期限（Certificate Monitor Expiration）] フィールドの説明については、 表 3 : 証明書有効期限モニターフィールド（表）証明書モニターのフィールド説明 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（Save）]** をクリックします。

表 *3* : 証明書モニターのフィールド説明

フィールド	説明
通知開始時刻（Notification Start Time）	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（Notification Frequency）	通知の頻度を時間または日単位で入力します。
電子メール通知の有効化（Enable E-mail Notification）	電子メール通知を有効にするには、このチェックボックスをオンにします。
電子メール ID（Email IDs）	通知を送信する電子メールアドレスを入力します。 （注） システムが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

オンライン証明書ステータスプロトコル（OCSP）を使用して、証明書の失効ステータスを取得できます。

OCSP を設定するには、次の手順を実行します。

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

[証明書一覧（Certificate List）] 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設定（Online Certificate Status Protocol Configuration）] 領域の [OCSP の有効化（Enable OCSP）] チェックボックスをオンにします。

ステップ 3 OCSP レスポンダに接続するために使用される OCSP URI を使用して証明書が設定されている場合は、[証明書の OCSP URI を使用（Use OCSP URI from Certificate）] を選択します。

ステップ 4 外部または設定済みの URI が OCSP レスポンダに接続するために使用される場合は、[設定済みの OCSP URI を使用（Use configured OCSP URI）] 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を確認する 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場合、[失効チェックの有効化（Enable Revocation Check）] チェック ボックスをオンにします。

（注） 証明書失効サービスは、失効および有効期限チェック 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に、LDAP 接続と IPSec 接続に使用できます。

ステップ 6 証明書失効ステータス チェックの頻度を設定する場合に、[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、tomcat-trust に OCSP レスポンダ証明書をアップロードする必要があります。

（注） 証明書の失効ステータスの確認は、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、証明書が失効した場合、適切なアラームが発生します。

証明書を確実に失効させるには、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（Tool）] > [コントロールセンター - ネットワークサービス（Control Center - Network Services）] に移動し、Cisco Certificate Expiry Monitor サービスを再起動します。

IPSEC 証明書を再作成する

スタンドアロンまたはクラスタで ipsec 証明書を生成または再生成するには、次の手順を実行します。

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

[証明書一覧（Certificate List）] ウィンドウが表示されます。

ステップ 2 **[Generate Self-signed（自己署名付きの生成）]** > または > **[CSRの生成（Generate CSR）]** をクリックします。

[証明書の生成（Generate Certificate）] ダイアログボックスが表示されます。

ステップ 3 **[証明書の目的（Certificate Purpose）]** ドロップダウンリストから [ipsec] を選択する。

ステップ 4 **[生成（Generate）]** をクリックします。

証明書の生成後、ipsec および ipsec trust は、スタンドアロンサーバーまたはパブリッシャ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、ステップ 1 ～ 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）]** の順に選択します。

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

[証明書のアップロード（Upload Certificate）] ダイアログボックスが開きます。

ステップ 8 **[証明書の目的（Certificate Purpose）]** ドロップダウンリストから [ipsec-trust] を選択する。

ステップ 9 証明書を参照し、**[アップロード（Upload）]** 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、最初にパブリッシャサーバーで、次にサブスクライバサーバーで以下のサービスを再起動します。

- Cisco DRF Master
- Cisco DRF Local

IPSEC 管理

ここでは、IPSec メニューで実行できる機能について説明します。

（注） IPSec は、インストール中にクラスタ内のノード間で自動的に設定されません。

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、次の手順を実行します。

（注） 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、特に暗号化において、システムのパフォーマンスに影響を与えます。

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

[IPSEC ポリシーリスト（IPSEC Policy List）] ウィンドウが表示されます。

ステップ 2 **[新規追加（Add New）]** をクリックします。

[IPSEC ポリシー設定（IPSEC Policy Configuration）] ウィンドウが表示されます。

ステップ 3 [IPSEC ポリシー設定（IPSEC Policy Configuration）] ウィンドウで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 4 : IPSecポリシーフィールド（表）IPSEC ポリシーとアソシエーションのフィールド説明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（Save）]** をクリックします。

表 *4 : IPSEC* ポリシーとアソシエーションのフィールド説明

フィールド	説明
ポリシーグループ名（Policy Group Name）	IPSec グループポリシーの名前を指定します。名前に指定できるのは、文字、数字、ハイフンのみです。
ポリシー名（Policy Name）	IPSec ポリシーの名前を指定します。名前に指定できるのは、文字、数字、ハイフンのみです。
認証方式（Authentication Method）	認証方式を指定します。
事前共有キー（Preshared Key）	[認証名（Authentication Name）] フィールドで [事前共有キー（Preshared Key）] 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使用できます。スペースやその他の文字は使用できません。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 と互換性があるように、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）	ピアが同じタイプであるか、異なるタイプであるかを指定します。
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。
接続先ポート（Destination Port）	接続先のポート番号を指定します。
接続元アドレス（Source Address）	接続元の IP アドレスまたは FQDN を指定します。
接続元ポート（Source Port）	接続元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）	接続先で使用するポート番号を指定します。

フィールド	説明
プロトコル（Protocol）	特定のプロトコル、または以下のいずれかを指定します。 • TCP • UDP • 任意
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。次のオプションがあります。 • DES • 3DES
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 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 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。次のオプションがあります。 • NULL_ENC • DES • 3DES • BLOWFISH • RIJNDAEL
フェーズ 1 ライフタイム（Phase One Life Time）	フェーズ 1 の IKE ネゴシエーションのライフタイムを秒単位で指定します。
フェーズ 1 DH（Phase One DH）	ドロップダウンリストから、[フェーズ 1 DH（Phase One DH）] 値を選択します。選択肢は、2、1、および 5 です。
フェーズ 2 ライフタイム（Phase Two Life Time）	フェーズ 2 の IKE ネゴシエーションのライフタイムを秒単位で指定します。
フェーズ 2 DH（Phase Two DH）	ドロップダウンリストから、[フェーズ 2 DH（Phase Two DH）] 値を選択します。選択肢は、2、1、および 5 です。

フィールド	説明
ポリシーの有効化（Enable Policy）	WPA ポリシーを有効にするには、このチェックボックスをオンにします。

既存の IPSec ポリシーを管理する

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、次の手順を実行します。

（注） システムのアップグレード中に IPSec ポリシーに加えられた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、特に暗号化において、システムのパフォーマンスに影響を与えます。

注意 既存の IPSec ポリシーに変更を加えると、通常のシステム動作に影響を与える可能性があります。

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

（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管理に再度ログインする必要があります。

[IPSEC ポリシーリスト（IPSEC Policy List）] ウィンドウが表示されます。

ステップ 2 ポリシーを表示、有効化、または無効化にするには、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 ポリシー設定（IPSEC Policy Configuration）] 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オンまたはオフにします。

c) **[保存（Save）]** 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) 削除したいポリシーの横の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。

証明書の一括管理

Extension Mobility Cross Cluster（EMCC）機能をサポートするために、システムでは、クラスタ管理者が設定した共通の 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。証明書の一括管理の使用方法の詳細については、『*Cisco Unified Communications Manager* セキュリティガイド』を参照してください。

証明書の一括管理の場合は、次の手順を実行します。

ステップ 1 **[セキュリティ（Security）]** > **[証明書の一括管理（Bulk Certificate Management）]** を選択します。[証明書の一括管理（Bulk Certificate Management）] ウィンドウが表示されます。

ステップ 2 [証明書の一括管理（Bulk Certificate Management）] ウィンドウで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 5 : 証明書の一括管理のフィールド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（Save）]** 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（Export）]** をクリックします。[証明書の一括エクスポート（Bulk Certificate Export）] 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タイプを選択します。

- Tomcat
- TFTP
- すべて

ステップ 6 **[エクスポート（Export）]** をクリックします。

選択した証明書がエクスポートされ、中央の SFTP サーバーに保存されます。

表 *5* : 証明書の一括管理のフィールド説明

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。
ポート（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）	サーバーへのログイン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ます。
ディレクトリ（Directory）	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 Administration
- Cisco Unity Connection Serviceability
- Cisco Personal Communications Assistant
- Cisco Unity Connection Web Inbox
- 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、次の手順を実行します。

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（Session Management）] 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、アクティブなログインユーザーのエイリアスを **[ユーザー ID（User ID）]** フィールドに入力します。

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、**[セッションの終了（Terminate Session）]** を選択します。

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

（注） セッションの終了は、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をログアウトするか、セッションがタイムアウトするまで待機する必要があります。

暗号管理

Cisco Unity Connection は、管理者がすべての TLS および SSH 接続に使用される暗号のセットを制御できる**暗号管理**をサポートしています。Cisco Unity Connection のさまざまなセキュアインターフェイスの推奨暗号を設定できます。

TLS インターフェイス

以下で説明する TLS インターフェイスの暗号を設定できます。

インターフェイス	説明
All TLS	サポートされている Cisco Unity Connection のすべての 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、および 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 でセキュアな SIP コール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

次に示す SSH インターフェイスの暗号と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 インターフェイスの SSH MAC アルゴリズムを設定できます。

推奨される暗号についての詳細は、https://www.cisco.com/c/ja_jp/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html にある『*Cisco Unified Communications Manager* セキュリティガイド』の「暗号管理」の項を参照してください。

暗号ストリングを設定する

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

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

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

（注） **HTTPS TLS** または **SIP TLS** インターフェイス用に設定された暗号文字列は、[すべての TLS（ALL 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（Cipher Management）]** ページで設定された暗号は、**[一般設定の編集（Edit General Configuration）]** 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（Cipher Management）]** 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（SSH Ciphers）] の **[暗号文字列（Cipher String）]** フィールドに暗号文字列を入力します。

ステップ 4 **[暗号文字列（Algorithm String）]** フィールドにアルゴリズム文字列を入力し、SSH キー交換のキーアルゴリズムを設定します。

ステップ 5 **[暗号文字列（Algorithm String）]** フィールドにアルゴリズム文字列を入力し、SSH MAC の MAC アルゴリズムを設定します。

ステップ 6 **[保存（Save）]** を選択します。

ページを保存したら、次の手順を実行する必要があります。

- **すべての TLS**、 **SSH 暗号**、 **SSH キー交換** 、および **SSH MAC** インターフェイスで暗号を正常に設定するには、クラスタ内の両方のノードを再起動します。
- **HTTPS TLS** インターフェイスで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** インターフェイスで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。