



セキュリティ

この章では証明書の管理と IPSec の管理について説明し、次の作業を実行する手順を説明します。

- 「[Internet Explorer のセキュリティ オプションの設定](#)」
- 「[証明書と Certificate Trust List の管理](#)」
- 「[IPSEC 管理](#)」
- 「[Bulk Certificate Management](#)」

Internet Explorer のセキュリティ オプションの設定

サーバ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設定されていることを確認します。

手順

- ステップ 1** Internet Explorer を起動します。
 - ステップ 2** [Tools] > [Internet Options] を選択します。
 - ステップ 3** [Advanced] タブをクリックします。
 - ステップ 4** [Advanced] タブの [Security] セクションまでスクロール ダウンします。
 - ステップ 5** 必要に応じて、[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 Certificate Trust List の管理

次の各項では、[Certificate Management] メニューから実行できる機能を説明します。

- 「[証明書の表示](#)」
- 「[証明書のダウンロード](#)」
- 「[証明書の削除と再作成](#)」
- 「[証明書または Certificate Trust List のアップロード](#)」
- 「[サードパーティ製の CA 証明書の使用法](#)」



(注)

[Security] メニューの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ログインする必要があります。

証明書の表示

既存の証明書を表示するには、次の手順を実行します。

手順

- ステップ 1 [Security] > [Certificate Management] を選択します。
[Certificate List] ウィンドウが表示されます。
- ステップ 2 [Find] コントロールを使用すると、証明書の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、そのファイル名をクリックします。
[Certificate Configuration] ウィンドウに該当の証明書の情報が表示されます。
- ステップ 4 [Certificate List] ウィンドウに戻るには、[Related Links] リストの [Back To Find/List] を選択し、[Go] をクリックします。

証明書のダウンロード

証明書を Cisco Unified Communications オペレーティング システム から PC にダウンロードするには、次の手順を実行します。

手順

- ステップ 1 [Security] > [Certificate Management] を選択します。
[Certificate List] ウィンドウが表示されます。
- ステップ 2 [Find] コントロールを使用すると、証明書のリストをフィルタリングできます。
- ステップ 3 証明書のファイル名をクリックします。
[Certificate Configuration] ウィンドウが表示されます。
- ステップ 4 [Download] をクリックします。
- ステップ 5 [File Download] ダイアログボックスで、[Save] をクリックします。

証明書の削除と再作成

次の各項では、証明書の削除と再作成について説明します。

- [「証明書の削除」](#)
- [「証明書の再作成」](#)

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。[Certificate List] で選択する証明書については、システムから既存の CSR がすべて削除されます。新しい CSR を生成する必要があります。詳細については、「証明書署名要求の作成」(P.6-7) の手順を参照してください。

手順

- ステップ 1 [Security] > [Certificate Management] を選択します。
[Certificate List] ウィンドウが表示されます。
- ステップ 2 [Find] コントロールを使用すると、証明書の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 CTL のファイル名をクリックします。
[Certificate Configuration] ウィンドウが表示されます。
- ステップ 4 [Delete] をクリックします。

証明書の再作成

証明書を再作成するには、次の手順を実行します。



(注)

証明書の再作成に関する詳細については、『Cisco Unified Communications Manager Security Guide』の「Security by Default」の第3章を参照してください。



注意

証明書を再作成すると、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 [Security] > [Certificate Management] を選択します。
[Certificate List] ウィンドウが表示されます。
- ステップ 2 [Generate New] をクリックします。
[Generate Certificate] ダイアログボックスが表示されます。
- ステップ 3 [Certificate Name] リストから、証明書の名前を選択します。表示される証明書の名前の説明については、表 6-1 を参照してください。
- ステップ 4 [Generate New] をクリックします。



(注)

Cisco Unified Communications オペレーティング システム で証明書を再作成したら、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。バックアップに再作成した証明書が含まれず、何らかの理由で回復タスクを実行する必要がでた場合は、システム上の電話をそれぞれ手動でロック解除して、Cisco Unified Communications Manager に登録できるようにします。バックアップの実行に関する詳細については、『*Disaster Recovery System Administration Guide*』を参照してください。

表 6-1 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、HTTPS サーバのインストール中に生成されます。
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。
CallManager	この自己署名ルート証明書は、Cisco Unified Communications Manager のインストール中に自動的にインストールされます。この証明書はサーバの名前と Global Unique Identifier (GUID; グローバル一意識別子) を含んでおり、サーバの ID となります。
CAPF	このルート証明書は、Cisco CTL クライアントの設定を完了すると、現在のサーバまたはクラスタ内のすべてのサーバにコピーされます。
TVS	自己署名ルート証明書です。

証明書または Certificate Trust List のアップロード



注意

新しい証明書ファイルまたは Certificate Trust List (CTL) ファイルをアップロードすると、システムの動作に影響する場合があります。新しい証明書または証明信頼リストをアップロードした後は、[Cisco Unified Serviceability] > [Tools] > [Service Activation] を選択して、Cisco CallManager サービスを再起動する必要があります。詳細については、『*Cisco Unified Serviceability Administration Guide*』を参照してください。



(注)

システムが信頼証明書を他のクラスタ ノードに自動的に配信することはありません。複数のノードで同じ証明書が必要な場合は、証明書を各ノードに個々にアップロードする必要があります。

次の各項では、CA ルート証明書、アプリケーション証明書、または CTL ファイルをサーバにアップロードする方法について説明します。

- 「証明書のアップロード」
- 「Certificate Trust List のアップロード」
- 「ディレクトリの信頼証明書のアップロード」

証明書のアップロード

手順

-
- ステップ 1** [Security] > [Certificate Management] を選択します。
[Certificate List] ウィンドウが表示されます。
- ステップ 2** [Upload Certificate] をクリックします。
[Upload Certificate] ダイアログボックスが表示されます。
- ステップ 3** [Certificate Name] リストから、証明書の名前を選択します。
- ステップ 4** サードパーティの CA で発行されたアプリケーション証明書をアップロードする場合は、CA ルート証明書の名前を [Root Certificate] テキストボックスに入力します。CA ルート証明書をアップロードする場合は、このテキストボックスを空白のままにします。
- ステップ 5** 次のいずれかの手順で、アップロードするファイルを選択します。
- [Upload File] テキストボックスに、ファイルのパスを入力します。
 - [Browse] ボタンをクリックしてファイルを選択し、[Open] をクリックします。
- ステップ 6** ファイルをサーバにアップロードするには、[Upload File] ボタンをクリックします。
-

Certificate Trust List のアップロード

手順

-
- ステップ 1** [Security] > [Certificate Management] を選択します。
[Certificate List] ウィンドウが表示されます。
- ステップ 2** [Upload Certificate] をクリックします。
[Upload Certificate Trust List] ダイアログボックスが表示されます。
- ステップ 3** [Certificate Name] リストから、証明書の名前を選択します。
- ステップ 4** サードパーティの CA で発行されたアプリケーション証明書をアップロードする場合は、CA ルート証明書の名前を [Root Certificate] テキストボックスに入力します。CA ルート証明書をアップロードする場合は、このテキストボックスを空白のままにします。
- ステップ 5** 次のいずれかの手順で、アップロードするファイルを選択します。
- [Upload File] テキストボックスに、ファイルのパスを入力します。
 - [Browse] ボタンをクリックしてファイルを選択し、[Open] をクリックします。
- ステップ 6** ファイルをサーバにアップロードするには、[Upload File] ボタンをクリックします。
-

ディレクトリの信頼証明書のアップロード

手順

-
- ステップ 1** [Security] > [Certificate Management] を選択します。

- [Certificate List] ウィンドウが表示されます。
- ステップ 2** [Upload Certificate] をクリックします。
[Upload Certificate Trust List] ダイアログボックスが表示されます。
- ステップ 3** [Certificate Name] リストから、[directory-trust] を選択します。
- ステップ 4** アップロードするファイルを [Upload File] フィールドに入力します。
- ステップ 5** ファイルをアップロードするには、[Upload File] ボタンをクリックします。
- ステップ 6** Cisco Unified Serviceability にログインします。
- ステップ 7** [Tools] > [Control Center - Feature Services] を選択します。
- ステップ 8** Cisco Dirsync サービスを再起動します。
- ステップ 9** Cisco Unified Communications オペレーティング システム の CLI に管理者としてログインします。
- ステップ 10** Tomcat サービスを再起動するには、コマンド `utils service restart Cisco Tomcat` と入力します。
- ステップ 11** サービスの再起動後、SSL のディレクトリ契約を追加することができます。

サードパーティ製の CA 証明書の使用法

Cisco Unified Communications オペレーティング システム は、サードパーティ製の Certificate Authority (CA; 認証局) が PKCS # 10 Certificate Signing Request (CSR; 証明書署名要求) によって発行した証明書をサポートしています。次の表に、このプロセスの概要および参考となる文書を示します。

	作業	参考となる文書
ステップ 1	サーバに CSR を作成する。	「証明書署名要求の作成」(P.6-7) を参照してください。
ステップ 2	CSR を PC にダウンロードする。	「証明書署名要求のダウンロード」(P.6-7) を参照してください。
ステップ 3	CSR を使用して、CA からアプリケーション証明書を取得する。	アプリケーション証明書の取得に関する情報は、CA から入手してください。その他の注意事項については、「サードパーティ製の CA 証明書の取得」(P.6-8) を参照してください。
ステップ 4	CA ルート証明書を取得する。	ルート証明書の取得に関する情報は、CA から入手してください。その他の注意事項については、「サードパーティ製の CA 証明書の取得」(P.6-8) を参照してください。
ステップ 5	CA ルート証明書をサーバにアップロードする。	「証明書のアップロード」(P.6-5) を参照してください。
ステップ 6	アプリケーション証明書をサーバにアップロードする。	「証明書のアップロード」(P.6-5) を参照してください。

	作業	参考となる文書
ステップ7	CAPF または Cisco Unified Communications Manager の証明書を更新した場合は、新しい CTL ファイルを作成する。	『Cisco Unified Communications Manager Security Guide』を参照してください。
ステップ8	新しい証明書に影響されるサービスを再起動する。	すべての証明書タイプで、対応するサービスを再起動します（たとえば、Tomcat の証明書を更新した場合は Tomcat サービスを再起動します）。さらに、CAPF または Cisco Unified Communications Manager の証明書を更新した場合は、TFTP サービスも再起動します。 (注) Tomcat の証明書を更新した場合は、Cisco Unity Connection サービスアビリティで接続 IMAP サーバ サービスも再起動してください。 サービスの再起動の詳細については、『Cisco Unified Communications Manager Serviceability Administration Guide』を参照してください。

証明書署名要求の作成

Certificate Signing Request (CSR; 証明書署名要求) を作成するには、次の手順を実行します。

手順

- ステップ 1** [Security] > [Certificate Management] を選択します。
[Certificate List] ウィンドウが表示されます。
- ステップ 2** [Generate CSR] をクリックします。
[Generate Certificate Signing Request] ダイアログボックスが表示されます。
- ステップ 3** [Certificate Name] リストから、証明書の名前を選択します。



(注) Cisco Unified オペレーティング システムの現行リリースでは、[Certificate Name] リストの [Directory] オプションは使用できなくなりました。ただし、DirSync サービスをセキュア モードで実行する場合に必要なディレクトリの信頼証明書は、以前のリリースからアップロードできます。

- ステップ 4** [Generate CSR] をクリックします。

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、次の手順を実行します。

手順

- ステップ 1** [Security] > [Certificate Management] を選択します。
[Certificate List] ウィンドウが表示されます。

- ステップ 2** [Download CSR] をクリックします。
[Download Certificate Signing Request] ダイアログボックスが表示されます。
- ステップ 3** [Certificate Name] リストから、証明書の名前を選択します。
- ステップ 4** [Download CSR] をクリックします。
- ステップ 5** [File Download] ダイアログボックスで、[Save] をクリックします。

サードパーティ製の CA 証明書の取得

サードパーティの CA が発行するアプリケーション証明書を使用するには、署名付きのアプリケーション証明書と CA ルート証明書の両方を CA から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。入手の手順は、CA によって異なります。

CAPF および Cisco Unified Communications Manager の CSR には、CA へのアプリケーション証明書要求に含める必要のある拡張情報が含まれています。CA が拡張要求メカニズムをサポートしていない場合は、CSR 作成プロセスの最後のページに表示される X.509 拡張を有効にする必要があります。

Cisco Unified Communications オペレーティング システムでは、証明書は DER および PEM 符号化フォーマットで、CSR は PEM 符号化フォーマットで作成されます。また、DER および PEM 符号化フォーマットの証明書を受け入れます。

CAPF 以外の証明書の場合、それぞれのノードについて CA ルート証明書およびアプリケーション証明書を取得およびアップロードしてください。

CAPF の場合、1 つ目のノードについてのみ CA ルート証明書およびアプリケーション証明書を取得およびアップロードしてください。

CAPF および Cisco Unified Communications Manager の CSR には、CA へのアプリケーション証明書要求に含める必要のある拡張情報が含まれています。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 拡張をイネーブルにする必要があります。

- CAPF CSR では、次の拡張情報が使用されます。

```
X509v3 extensions:
X509v3 Key Usage:
Digital Signature, Certificate Sign
X509v3 Extended Key Usage:
TLS Web Server Authentication, IPSec End System
```

- Cisco Unified Communications Manager、Tomcat、および IPSec の CSR では、次の拡張情報を使用します。

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

アプリケーション証明書を署名した CA の CA ルート証明書をアップロードします。下位 CA がアプリケーション証明書を署名した場合、ルート CA ではなく、下位 CA の CA ルート証明書をアップロードします。

CA ルート証明書およびアプリケーション証明書をアップロードするには、同じ [Upload Certificate] ダイアログ ボックスを使用します。CA ルート証明書をアップロードする場合、*certificate type-trust* 形式の証明書を選択します。アプリケーション証明書をアップロードする場合、証明書タイプのみが含まれる証明書の名前を選択します。たとえば、Tomcat CA ルート証明書をアップロードする場合、[tomcat-trust] を選択し、Tomcat アプリケーション証明書をアップロードする場合、[tomcat] を選択します。

CAPF CA ルート証明書をアップロードすると、CallManager の信頼ストアにコピーされるため、CA ルート証明書を個別に CallManager にアップロードする必要はありません。

証明書の有効期限日の監視

証明書の有効期限日が近づいたときに、システムから自動的に E メールを送信できます。証明書有効期限モニタの表示と設定をするには、次の手順を実行します。

手順

- ステップ 1** 現在の証明書有効期限モニタの設定を表示するには、[Security] > [Certificate Monitor] を選択します。[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。[Certificate Monitor Expiration] フィールドの説明については、表 6-2 を参照してください。
- ステップ 3** 変更内容を保存するには、[Save] をクリックします。

表 6-2 [Certificate Monitor Expiration] フィールドの説明

フィールド	説明
Notification Start Time	証明書が無効になる何日前に通知を送信してもらうかを入力します。
Notification Frequency	通知の頻度を時間または日単位で入力します。
Enable E-mail Notification	E 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。
Email IDs	通知の送信先 E 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。

IPSEC 管理

次の各項では、[IPSec] のメニューで実行できる機能を説明します。

- 「新しい IPSec ポリシーの設定」
- 「既存の IPSec ポリシーの管理」



(注) IPSec は、インストール時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 ポリシーの設定

新しい IPSec ポリシーとアソシエーションを設定するには、次の手順を実行します。



(注)

システムのアップグレード中、IPSec ポリシーに何らかの変更を行ってもその変更は無効になります。アップグレード中は IPSec ポリシーを作成したり変更したりしないでください。



注意

IPSec はシステムのパフォーマンスに影響します (特に暗号化した場合)。

手順

- ステップ 1** [Security] > [IPSEC Configuration] を選択します。
[IPSEC Policy List] ウィンドウが表示されます。
- ステップ 2** [Add New] をクリックします。
[IPSEC Policy Configuration] ウィンドウが表示されます。
- ステップ 3** [IPSEC Policy Configuration] ウィンドウに適切な情報を入力します。このウィンドウの各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 4** 新しい IPSec ポリシーを設定するには、[Save] をクリックします。

表 6-3 [IPSEC Policy and Association] フィールドと説明

フィールド	説明
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、ハイフンのみを使用できます。
Policy Name	IPSec ポリシーの名前を指定します。名前には、文字、数字、ハイフンのみを使用できます。
Authentication Method	認証方式を指定します。
Preshared Key	[Authentication Method] フィールドで [Pre-shared 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、英字およびハイフンのみ使用できます。空白文字またはその他の文字は使用できません。Windows ベース バージョンの Cisco Unified Communications Manager から移行する場合、現行バージョンの 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ります。
Peer Type	ピアのタイプが同じか異なるかを指定します。
Certificate Name	[Peer Type] で [Different] を選択した場合、新しい証明書の名前を入力します。
Destination Address	宛先の IP アドレスまたは FQDN を指定します。
Destination Port	宛先のポート番号を指定します。
Source Address	ソースの IP アドレスまたは FQDN を指定します。
Source Port	ソースのポート番号を指定します。
Mode	転送モードを指定します。
Remote Port	宛先で使用されるポート番号を指定します。

表 6-3 [IPSEC Policy and Association] フィールドと説明 (続き)

フィールド	説明
Protocol	次のプロトコルまたは [Any] を指定します。 <ul style="list-style-type: none"> • TCP • UDP • Any
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。 <ul style="list-style-type: none"> • DES • 3DES
Hash Algorithm	ハッシュ アルゴリズムを指定します。 <ul style="list-style-type: none"> • 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 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。 <ul style="list-style-type: none"> • NULL_ENC • DES • 3DES • BLOWFISH • RIJNDAEL
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。
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。2、1 および 5 から選択できます。
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。
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。2、1 および 5 から選択できます。
Enable Policy	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 ポリシーの管理

既存の IPsec ポリシーを表示、イネーブル/ディセーブル、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、IPsec ポリシーに何らかの変更を行ってもその変更は無効になります。アップグレード中は IPsec ポリシーを作成したり変更したりしないでください。



注意

IPSec はシステムのパフォーマンスに影響します（特に暗号化した場合）。



注意

既存の IPSec ポリシーを変更すると、システムの正常な動作に影響する場合があります。

手順

ステップ 1 [Security] > [IPSEC Configuration] を選択します。



(注) [Security] メニューの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ログインする必要があります。

[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、イネーブル、またはディセーブルにするには、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 Policy Configuration] ウィンドウが表示されます。
- b. ポリシーをイネーブルまたはディセーブルにするには、[Enable Policy] チェックボックスを使用します。
- c. [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。
[Select All] をクリックするとすべてのポリシーを選択でき、[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. [Delete Selected] をクリックします。

Bulk Certificate Management

Extension Mobility Cross Cluster (EMCC) 機能をサポートするため、クラスタ管理者によって構成された共通 SFTP サーバ間で一括インポートおよびエクスポートを実行できます。



(注)

Cisco Unified IP Phone 8961、9951、または 9971 のファームウェア リリースが 9.0(2) で、クラスタが混合モードで実行されている場合、EMCC 機能が動作するためには、クラスタすべての CTL が共通した一連のセキュリティ トークンで署名される必要があります。すべてのクラスタで共通のトークンが 1 つ以上必要です。

証明書のエクスポート

[Bulk Certificate Management] を使用して証明書をエクスポートするには、次の手順を実行します。

手順

-
- ステップ 1** [Security] > [Bulk Certificate Management] を選択します。
[Bulk Certificate Management] ウィンドウが表示されます。
- ステップ 2** [Bulk Certificate Management] ウィンドウに適切な情報を入力します。このウィンドウの各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 3** 入力した値を保存するには、[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、[Export] をクリックします。
[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
 - All
- ステップ 6** [Export] をクリックします。
システムによって選択した証明書が中央 SFTP サーバにエクスポートおよび保存されます。
-

証明書のインポート

[Bulk Certificate Management] ウィンドウを使用して、他のクラスタからエクスポートした証明書をインポートすることもできます。ただし、[Import] ボタンが表示されるには、次の操作を完了する必要があります。

- クラスタ 2 つ以上から SFTP サーバに証明書をエクスポートします。
- エクスポートした証明書を統合します。

表 6-4 [Bulk Certificate Management] フィールドの説明

フィールド	説明
IP Address	証明書のエクスポート先となる共通サーバの 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
User ID	サーバのログインに使用するユーザ ID を入力します。
Password	適切なパスワードを入力します。
Directory	証明書の保存先となるサーバのディレクトリを入力します。 例： /users/cisco

