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」（P.6-1）
- 「証明書と証明書信頼リストの管理」（P.6-1）
- 「IPSEC 管理」（P.6-9）

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 [ツール（Tools）] > [インターネット オプション（Internet Options）] を選択します。

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の管理

次の各項では、[証明書の管理（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）　[セキュリティ（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　[セキュリティ（Security）] > [証明書の管理（Certificate Management）] を選択します。

[証明書の一覧（Certificate List）] ウィンドウが表示されます。

ステップ 2　[検索（Find）] コントロールを使用して、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。

[証明書の設定（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　[証明書の一覧（Certificate List）] ウィンドウに戻るには、[関連リンク（Related Links）] リストの [検索 / リストに戻る（Back To Find/List）] を選択し、[移動（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　[セキュリティ（Security）] > [証明書の管理（Certificate Management）] を選択します。

[証明書の一覧（Certificate List）] ウィンドウが表示されます。

ステップ 2　[検索（Find）] コントロールを使用して、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。

[証明書の設定（Certificate Configuration）] ウィンドウが表示されます。

ステップ 4　[ダウンロード（Download）] 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
- 証明書の再生成

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。[証明書の一覧（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、「証明書署名要求の生成」（P.6-7）の手順を参照してください。

手順

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。

[証明書の一覧（Certificate List）] ウィンドウが表示されます。

ステップ 2　[検索（Find）] コントロールを使用して、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。

[証明書の設定（Certificate Configuration）] 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

証明書を再作成するには、次の手順を実行します。

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

[証明書の一覧（Certificate List）] ウィンドウが表示されます。

ステップ 2　[新規作成（Generate New）] をクリックします。

[証明書の作成（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　[新規作成（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作成されます。
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グローバル固有識別子（GUID）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。

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証明書信頼リスト（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書信頼リストをアップロードした後は、[Cisco Unified サービスアビリティ（Cisco Unified Serviceability）] > [ツール（Tools）] > [サービスの有効化（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）　信頼証明書は他のクラスタ ノードに自動的には配信されません。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別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　[セキュリティ（Security）] > [証明書の管理（Certificate Management）] を選択します。

[証明書の一覧（Certificate List）] ウィンドウが表示されます。

ステップ 2　[証明書のアップロード（Upload Certificate）] 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表示されます。

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。

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 [ルート証明書（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。

- [ファイルのアップロード（Upload File）] テキストボックスに、ファイルのパスを入力します。
- [参照（Browse）] ボタンをクリックしてファイルを選択し、[開く（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、[ファイルのアップロード（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　[セキュリティ（Security）] > [証明書の管理（Certificate Management）] を選択します。

[証明書の一覧（Certificate List）] ウィンドウが表示されます。

ステップ 2　[証明書のアップロード（Upload Certificate）] 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表示されます。

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。

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 [ルート証明書（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。

- [ファイルのアップロード（Upload File）] テキストボックスに、ファイルのパスを入力します。
- [参照（Browse）] ボタンをクリックしてファイルを選択し、[開く（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、[ファイルのアップロード（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　[セキュリティ（Security）] > [証明書の管理（Certificate Management）] を選択します。

[証明書の一覧（Certificate List）] ウィンドウが表示されます。

ステップ 2　[証明書のアップロード（Upload Certificate）] 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表示されます。

ステップ 3　[証明書の名前（Certificate Name）] リストから、[ディレクトリの信頼性（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 [ファイルのアップロード（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、[ファイルのアップロード（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（ツール）] > [コントロール センターの機能サービス（Control Center - Feature Services）] の順に選択します。

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 パーティの認証局（CA）が PKCS # 10 証明書署名要求（CSR）を使用し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。

	タスク	詳細情報
ステップ 1	サーバに CSR を作成します。	「証明書署名要求の生成」（P.6-7）を参照してください。
ステップ 2	CSR を PC にダウンロードします。	「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します。	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します。	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します。	「証明書のアップロード」（P.6-4）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します。	「証明書のアップロード」（P.6-4）を参照してください。

	タスク	詳細情報
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。

証明書署名要求の生成

証明書署名要求（CSR）を作成するには、次の手順を実行します。

手順

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

[証明書の一覧（Certificate List）] ウィンドウが表示されます。

ステップ 2　[CSR の作成（Generate CSR）] をクリックします。

[証明書署名要求の作成（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　[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。

（注） Cisco Unified オペレーティング システムの現行リリースでは、[証明書の名前（Certificate Name）] リストの [ディレクトリ（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となる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　[CSR の作成（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　[セキュリティ（Security）] > [証明書の管理（Certificate Management）] を選択します。

[証明書の一覧（Certificate List）] ウィンドウが表示されます。

ステップ 2　[CSR のダウンロード（Download CSR）] をクリックします。

[証明書署名要求のダウンロード（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　[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。

ステップ 4　[CSR のダウンロード（Download CSR）] 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。

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 エンコーディング フォーマットで、CSR は PEM エンコーディング フォーマットで生成されます。また、PEM および DER エンコード形式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してアップロードします。

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、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 [証明書のアップロード（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 の信頼性（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（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モニタ

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電子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、[セキュリティ（Security）] > [証明書モニタ（Certificate Monitor）] を選択します。

[証明書モニタ（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。[証明書の有効期限日の監視（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　変更を保存するには、[保存（Save）] をクリックします。

表 6-2　[証明書モニタ（Certificate Monitor）] フィールドの説明

フィールド	説明
通知開始時期（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。
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。
メール通知の有効化（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。
メール ID（Email IDs）	通知の送信先電子メール 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。

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　[セキュリティ（Security）] > [IPSEC 設定（IPSEC Configuration）] を選択します。

[IPSEC ポリシーの一覧（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 ポリシーの設定（IPSEC Policy Configuration）] ウィンドウが表示されます。

ステップ 3　[IPSEC ポリシーの設定（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、[保存（Save）] をクリックします。

表 6-3　[IPSEC ポリシーとアソシエーション（IPSEC Policy and Association）] フィールドと説明

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、ハイフンのみを使用できます。
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、ハイフンのみを使用できます。
認証方式（Authentication Method）	認証方式を指定します。
事前共有キー（Preshared Key）	[認証方式（Authentication Method）] フィールドで [事前共有キー（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。
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。
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。
接続元のアドレス（Source Address）	ソースの IP アドレスまたは FQDN を指定します。

表 6-3　[IPSEC ポリシーとアソシエーション（IPSEC Policy and Association）] フィールドと説明

フィールド	説明
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）	転送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（Protocol）	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
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。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 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 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。2、1 および 5 から選択できます。
フェーズ 2 のライフタイム（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 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。2、1 および 5 から選択できます。
ポリシーを有効（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 [セキュリティ（Security）] > [IPSEC 設定（IPSEC Configuration）] を選択します。

（注） [セキュリティ（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 ポリシーの一覧（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、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 ポリシーの設定（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、[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（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。

[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。