



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](#)
- [証明書と証明書信頼リストの管理](#)
- [IPSEC の管理](#)

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] > [インターネット オプション] を選択します。
 - ステップ 3** [詳細設定] タブをクリックします。
 - ステップ 4** [詳細設定] タブの [セキュリティ] をスクロール ダウンします。
 - 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

次の各項では、[証明書の管理] 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 (P.6-2)
- 証明書または CTL のダウンロード (P.6-2)
- 証明書の削除と再作成 (P.6-3)
- 証明書または証明書信頼リストのアップロード (P.6-4)
- サードパーティの CA 証明書の使用法 (P.6-6)



(注)

[セキュリティ] 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 システムの管理ページ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] > [証明書の管理] を選択します。

[証明書の一覧] ウィンドウが表示されます。

ステップ 2 [検索] 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。

[証明書の設定] 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] ウィンドウに戻るには、[関連リンク] リストの [検索 / リストに戻る] を選択し、[移動] をクリックします。

証明書または CTL のダウンロード

証明書または CTL 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] > [証明書の管理] を選択します。

[証明書の一覧] ウィンドウが表示されます。

ステップ 2 [検索] 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。

[証明書の設定] ウィンドウが表示されます。

ステップ 4 [ダウンロード] 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 \(P.6-3\)](#)
- [証明書の再作成 \(P.6-3\)](#)

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。

手順

ステップ 1 [セキュリティ] > [証明書の管理] を選択します。

[証明書の一覧] ウィンドウが表示されます。

ステップ 2 [検索] 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。

[証明書の設定] ウィンドウが表示されます。

ステップ 4 [削除] 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] > [証明書の管理] を選択します。
- [証明書の一覧] ウィンドウが表示されます。
- ステップ 2** [新規作成] をクリックします。
- [証明書の作成] 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] リストから、証明書の名前を選択します。
- ステップ 4** [新規作成] をクリックします。
-

証明書または証明書信頼リストのアップロード



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。



(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 \(P.6-4\)](#)
- [証明書信頼リストのアップロード \(P.6-5\)](#)
- [ディレクトリの信頼証明書のアップロード \(P.6-5\)](#)

証明書のアップロード

手順

-
- ステップ 1** [セキュリティ] > [証明書の管理] を選択します。
- [証明書の一覧] 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] をクリックします。
- [証明書のアップロード] 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] 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]** 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]** テキストボックスに、ファイルのパスを入力します。
 - **[参照]** ボタンをクリックしてファイルを選択し、**[開く]** 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]** ボタンをクリックします。
-

証明書信頼リストのアップロード

手順

- ステップ1** **[セキュリティ]** > **[証明書の管理]** を選択します。
- [証明書の一覧]** ウィンドウが表示されます。
- ステップ2** **[CTL 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表示されます。
- ステップ3** **[証明書の名前]** 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]** 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]** テキストボックスに、ファイルのパスを入力します。
 - **[参照]** ボタンをクリックしてファイルを選択し、**[開く]** 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]** 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]** > **[証明書の管理]** を選択します。
- [証明書の一覧]** ウィンドウが表示されます。

ステップ 2 [CTL 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表示されます。

ステップ 3 [証明書の名前] 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 [ファイルのアップロード] 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] 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** を入力します。

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) 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やマニュアルを示します。

	作業	参照先
ステップ 1	サーバに CSR を作成する。	P.6-7 の「証明書署名要求の作成」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。	P.6-7 の「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 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、P.6-8 の「サードパーティの CA 証明書の取得」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、P.6-8 の「サードパーティの CA 証明書の取得」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。	P.6-4 の「証明書のアップロード」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。	P.6-4 の「証明書のアップロード」を参照してください。
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 セキュリティ ガイド』を参照してください。

	作業	参照先
ステップ 8	新しい証明書に影響す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。 サービスの再起動の詳細については、『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。

証明書署名要求の作成

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] > [証明書の管理] を選択します。
- [証明書の一覧] ウィンドウが表示されます。
- ステップ 2** [CSR の作成] をクリックします。
- [証明書署名要求の作成] 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] リストから、証明書の名前を選択します。
- ステップ 4** [CSR の作成] 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] > [証明書の管理] を選択します。
- [証明書の一覧] 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] をクリックします。
- [証明書署名要求のダウンロード] 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] 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] 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。
-

サードパーティの 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 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 DER 符号化フォーマットの証明書を受け入れます。

シスコは、Microsoft、Keon、および Verisign CA から取得されたサードパーティの証明書を検証します。それ以外の CA の証明書でも機能する場合がありますが、検証は行われません。


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通知が送信されることはありません。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] > [証明書モニタ] を選択します。
- [証明書モニタ] ウィンドウが表示されます。
- ステップ 2** 必要な設定情報を入力します。証明書モニタの有効期限のフィールドの説明については、表 6-1 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、[保存] をクリックします。

表 6-1 証明書モニタのフィールド説明

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)	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(E-mail IDs)	通知を送信するメール アドレスを入力します。
	 <p>(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。</p>

IPSEC の管理

次の各項では、IPSec 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 \(P.6-9\)](#)
- [既存の IPSec ポリシーの管理 \(P.6-11\)](#)



(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 ポリシーと割り当てを設定するには、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] > [IPSEC 設定] を選択します。
- [IPSEC ポリシーの一覧] 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 ポリシーの設定] 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] 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 6-2](#) 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 6-2 IPSEC のポリシーと割り当ての設定のフィールドと説明

フィールド	説明
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。
アソシエーション名 (Association Name)	各 IPSec 割り当てに付けられている割り当て名を指定します。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。

表 6-2 IPSEC のポリシーと割り当ての設定のフィールドと説明 (続き)

フィールド	説明
共有キー (Preshared Key)	[認証方式 (Authentication Method)] フィールドで [共有キー] を選択した場合は、共有キーを指定します。
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)	着信先の IP アドレスまたは FQDN を指定します。
接続先ポート (Destination Port)	着信先のポート番号を指定します。
ソース アドレス (Source Address)	ソース側の IP アドレスまたは FQDN を指定します。
ソース ポート (Source Port)	ソース側のポート番号を指定します。
モード (Mode)	トンネルまたは転送モードを指定します。
リモート ポート (Remote Port)	着信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。 <ul style="list-style-type: none"> • TCP • UDP • 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。 <ul style="list-style-type: none"> • 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。 <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 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
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。選択肢は 2、1、5、14、16、17、および 18 です。
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。選択肢は 2、1、5、14、16、17、および 18 です。
ポリシーの有効化 (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、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、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] > [IPSEC 設定] を選択します。



(注)

[セキュリティ] 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 システムの管理ページに再ログインする必要があります。

[IPSEC ポリシーの一覧] 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] ウィンドウが表示されます。
- b. ポリシーを有効化または無効化するには、[ポリシーの有効化] 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] 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] 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] をクリックします。

