CHAPTER 5

Unified オペレーティング システムでのセキュリティ証明書の管理

オペレーティング システムのセキュリティ オプションでは、次の 2 つの方法でセキュリティ証明書を管理できます。

- 証明書の管理（Certificate Management）：証明書、証明書信頼リスト（CTL）、および証明書署名要求（CSR）を管理します。証明書の表示、アップロード、ダウンロード、削除、および再作成を行うことができます。
- 証明書モニタ（Certificate Monitor）：サーバで証明書の有効期限を監視できます。

- 「証明書および証明書信頼リストの管理方法」（P.1）
- 「サード パーティの CA 証明書の使用方法」（P.6）

証明書および証明書信頼リストの管理方法

- 「証明書の表示」（P.1）
- 「証明書または証明書信頼リストのダウンロード」（P.2）
- 「証明書の削除」（P.3）
- 「証明書の再生成」（P.3）
- 「証明書または証明書信頼リストのアップロード」（P.4）
- 「ディレクトリの信頼証明書のアップロード」（P.5）

証明書の表示

はじめる前に

[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 オペレーティング システムの管理（Cisco Unified Operating System Administration）] に再サインインする必要があります。

手順

ステップ 1 [Cisco Unified オペレーティング システムの管理（Cisco Unified Operating System Administration）] にサインインします。

ステップ 2　[セキュリティ（Security）] > [証明書の管理（Certificate Management）] を選択します。

ステップ 3　次のいずれかの操作を実行します。

目的	アクション
証明書リストのフィルタリング	検索基準を入力し、次のように [検索（Find）] コントロールを使用します。 **a.** レコードをフィルタリングまたは検索するには、次のいずれかの操作を実行します。 – 最初のリスト ボックスから検索パラメータを選択します。 – 2 番目のリスト ボックスから検索パターンを選択します。 – 必要に応じて、適切な検索テキストを指定します。 **b.** [検索（Find）] を選択します。
証明書または信頼ストアの詳細を表示します。	証明書の .PEM または .DER ファイル名を選択します。
[証明書の一覧（Certificate List）] ウィンドウに戻ります。	**a.** [関連リンク（Related Links）] リストで [検索 / リストに戻る（Back to Find/List）] を選択します。 **b.** [移動（Go）] を選択します。

証明書または証明書信頼リストのダウンロード

はじめる前に

[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 オペレーティング システムの管理（Cisco Unified Operating System Administration）] に再サインインする必要があります。

手順

ステップ 1　[Cisco Unified オペレーティング システムの管理（Cisco Unified Operating System Administration）] にサインインします。

ステップ 2　[セキュリティ（Security）] > [証明書の管理（Certificate Management）] を選択します。

ステップ 3　必要に応じて、[検索（Find）] コントロールを使用して、証明書を次のようにフィルタリングします。

a. レコードをフィルタリングまたは検索するには、次のいずれかの操作を実行します。
- 最初のリスト ボックスから検索パラメータを選択します。
- 2 番目のリスト ボックスから検索パターンを選択します。
- 必要に応じて、適切な検索テキストを指定します。

b. [検索（Find）] を選択します。

ステップ 4　証明書または CTL のファイル名を選択します。

ステップ 5　[ダウンロード（Download）] を選択します。

証明書の削除

削除できる証明書は、信頼できる証明書だけです。システムで生成される自己署名証明書は削除できません。

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（Certificate List）] から選択する証明書に既存の CSR がある場合、システムから削除されるので、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.7）を参照してください。

はじめる前に

[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 オペレーティング システムの管理（Cisco Unified Operating System Administration）] に再サインインする必要があります。

手順

ステップ 1　[Cisco Unified オペレーティング システムの管理（Cisco Unified Operating System Administration）] にサインインします。

ステップ 2　[セキュリティ（Security）] > [証明書の管理（Certificate Management）] を選択します。

ステップ 3　必要に応じて、[検索（Find）] コントロールを使用して、証明書を次のようにフィルタリングします。

a.　レコードをフィルタリングまたは検索するには、次のいずれかの操作を実行します。
- 最初のリスト ボックスから検索パラメータを選択します。
- 2 番目のリスト ボックスから検索パターンを選択します。
- 必要に応じて、適切な検索テキストを指定します。

b.　[検索（Find）] を選択します。

ステップ 4　証明書または CTL のファイル名を選択します。

ステップ 5　[削除（Delete）] を選択します。

証明書の再生成

再生成できる証明書は、"cert" というタイプの証明書だけです。

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。

はじめる前に

[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 オペレーティング システムの管理（Cisco Unified Operating System Administration）] に再サインインする必要があります。

手順

ステップ 1　[Cisco Unified オペレーティング システムの管理（Cisco Unified Operating System Administration）] にサインインします。

ステップ 2　[セキュリティ（Security）] > [証明書の管理（Certificate Management）] を選択します。

ステップ 3　[新規作成（Generate New）] を選択します。

ステップ 4　[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 5-1　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、セキュア IPSec サーバ接続のインストール中に生成されます。
cup	この自己署名ルート証明書は、Cisco Unified Presence サーバのインストール中に生成されます。
cup-xmpp	この自己署名ルート証明書は、Cisco Unified Presence サーバのインストール中に生成されます。
cup-xmpp-s2s	この自己署名ルート証明書は、Cisco Unified Presence サーバのインストール中に生成されます。 **（注）** cup-xmpp-s2s の信頼証明書は、一般的な XMPP 信頼証明書とともに cup-xmpp-trust に保存されます。

ステップ 5　[新規作成（Generate New）] を選択します。

トラブルシューティングのヒント

Cisco Unified Presence クラスタで、Tomcat 証明書をアップロードまたは再生成した後で Tomcat Web サーバを再起動します。

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。

はじめる前に

- 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。
- [セキュリティ（Security）] メニューの項目にアクセスするには、[Cisco Unified オペレーティング システムの管理（Cisco Unified Operating System Administration）] からサインアウトし、管理者パスワードを使用して再サインインする必要があります。

手順

ステップ 1　[Cisco Unified オペレーティング システムの管理（Cisco Unified Operating System Administration）] にサインインします。

ステップ 2　[セキュリティ（Security）] > [証明書の管理（Certificate Management）] を選択します。

ステップ 3　[証明書のアップロード（Upload Certificate）] を選択します。

ステップ 4　[証明書の名前（Certificate Name）] リストから証明書または CTL の名前を選択します。

ステップ 5　次のいずれかの操作を実行します。

a. 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。

b. CA ルート証明書をアップロードする場合は、[ルート証明書（Root Certificate）] テキスト ボックスを空白のままにします。

ステップ 6　次のいずれかの操作を実行して、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へのパスを入力します。
- [参照（Browse）] を選択して、ファイルに移動します。
- [開く（Open）] を選択します。

ステップ 7　[ファイルのアップロード（Upload File）] を選択して、サーバにファイルをアップロードします。

トラブルシューティングのヒント

Cisco Unified Presence クラスタで、Tomcat 証明書をアップロードまたは再生成した後で Tomcat Web サーバを再起動します。

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　[Cisco Unified オペレーティング システムの管理（Cisco Unified Operating System Administration）] にサインインします。

ステップ 2　[セキュリティ（Security）] > [証明書の管理（Certificate Management）] を選択します。

ステップ 3　[証明書のアップロード（Upload Certificate）] を選択します。

ステップ 4　[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 5　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 6　[ファイルのアップロード（Upload File）] を選択します。

ステップ 7　Cisco Unified Serviceability にサインインします。

ステップ 8　[ツール（Tools）] > [コントロール センタ - Feature Services（Control Center - Feature Services）] を選択します。

ステップ 9　**Cisco Dirsync** サービスを再起動します。

ステップ 10　Cisco Unified オペレーティング システム の CLI に管理者としてサインインします。

ステップ 11　コマンド **utils service restart Cisco Tomcat** を入力して、Tomcat サービスを再起動します。

ステップ 12　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 証明書の使用方法

Cisco Unified オペレーティング システム は、サード パーティの Certificate Authority（CA; 認証局）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。

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 Presence の証明書署名要求（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 生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 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、DER および DER エンコーディング 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 の CA から取得したサード パーティの証明書を検証済みです。他の CA からの証明書は機能する可能性はありますが、検証されていません。

- 「サード パーティの証明書プロセスの管理」（P.6）
- 「証明書署名要求の生成」（P.7）
- 「証明書署名要求のダウンロード」（P.7）
- 「証明書の有効期限日の監視」（P.8）

サード パーティの証明書プロセスの管理

この手順では、サード パーティの証明書プロセスの概要を順序に従って説明します。

	作業	詳細情報
ステップ 1	サーバに CSR を作成する。	「証明書署名要求の生成」（P.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.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。
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。
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。	「証明書または証明書信頼リストのアップロード」（P.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する。	「証明書または証明書信頼リストのアップロード」（P.4）を参照してください。

	作業	詳細情報
ステップ 7	CAPF または Cisco Unified Presence 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。	「証明書または証明書信頼リストのアップロード」（P.4）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）。 サービスの再起動については、『*Cisco Unified Serviceability Administration Guide for Cisco Unified Presence*』を参照してください。

証明書署名要求の生成

はじめる前に

- [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 オペレーティング システムの管理（Cisco Unified Operating System Administration）] に再サインインする必要があります。
- 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。

手順

ステップ 1　[Cisco Unified オペレーティング システムの管理（Cisco Unified Operating System Administration）] にサインインします。

ステップ 2　[セキュリティ（Security）] > [証明書の管理（Certificate Management）] を選択します。

ステップ 3　[CSR の作成（Generate CSR）] を選択します。

ステップ 4　[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 5　[CSR の作成（Generate CSR）] を選択します。

関連項目

「ディレクトリの信頼証明書のアップロード」（P.5）

証明書署名要求のダウンロード

はじめる前に

[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 オペレーティング システムの管理（Cisco Unified Operating System Administration）] に再サインインする必要があります。

手順

ステップ 1　[Cisco Unified オペレーティング システムの管理（Cisco Unified Operating System Administration）] にサインインします。

ステップ 2　[セキュリティ（Security）] > [証明書の管理（Certificate Management）] を選択します。

ステップ 3　[CSR のダウンロード（Download CSR）] を選択します。

ステップ 4　[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 5　[CSR のダウンロード（Download CSR）] を選択します。

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電子メールを送信できます。

手順

ステップ 1　[Cisco Unified オペレーティング システムの管理（Cisco Unified Operating System Administration）] にサインインします。

ステップ 2　[セキュリティ（Security）] > [証明書モニタ（Certificate Monitor）] を選択して、現在の証明書有効期限モニタの設定を表示します。

ステップ 3　必要な設定情報を入力します。

表 5-2　[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）	電子メール通知を有効にする場合は、チェックボックスをオンにします。
メール ID（E-mail 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ようにするには、SMTP ホストを設定する必要があります。