セキュリティ

この章では証明書管理と IP セキュリティ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。

- 証明書と証明書信頼リストの管理
- 証明書の表示
- 証明書または CTL のダウンロード
- 証明書の削除と再作成
- 証明書または証明書信頼リストのアップロード
- 証明書署名要求のダウンロード
- 証明書の有効期限日の監視
- IP セキュリティ管理
- 既存の IPSec ポリシーの表示または変更
- 新しい IPSec ポリシーの設定

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

証明書の管理メニュー オプションを使用すると、次の機能を実行できます。

- 証明書の表示
- 証明書と証明書信頼リスト（CTL）のアップロード
- 証明書と CTL のダウンロード
- 証明書の削除
- 証明書の再作成
- 証明書署名要求（CSR）のダウンロード
- 証明書の有効期限の監視

（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び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］>［証明書の表示］**を選択します。

Select Certificates or Trust Store ウィンドウが表示されます。

ステップ 2　表示する証明書のタイプのチェックボックス、［自分の証明書 (Own Certificates)］または［信頼証明書 (Trust Certificates)］のいずれかをオンにします。

Display Certificates or Trust Units ウィンドウが表示されます。

ステップ 3　表示する証明書のタイプのチェックボックスをオンにします。

Display Certificates or Trust Store ウィンドウが表示されます。

ステップ 4　表示する証明書の信頼ストアのチェックボックスをオンにします。

Details of a Certificate ウィンドウが表示されます。

ステップ 5　証明書の詳細を表示したら、他のメニュー オプションを選択して Details of Certificate ウィンドウを閉じます。

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］>［証明書 /CTL のダウンロード］を選択します。

［証明書 /CTL/CSR のダウンロードの選択 (Select Certificate/CTL/CSR Download)］ウィンドウが表示されます。

ステップ 2　該当するダウンロード タイプ、［自分の証明書のダウンロード (Download Own Cert)］、［信頼証明書のダウンロード (Download Trust Cert)］、または［CTL ファイルのダウンロード (Download CTL File)］のいずれかのチェックボックスをオンにします。［次へ］をクリックします。

Download Certificates or Trust Units ウィンドウが表示されます。

ステップ 3　ダウンロードする既存の証明書タイプのチェックボックスをオンにし、［次へ］をクリックします。

Display Certificates or Trust Store ウィンドウが表示されます。

ステップ 4　ダウンロードする既存の証明書のチェックボックスをオンにし、［次へ］をクリックします。

［証明書 /CTL/CSR のダウンロード (Certificate/CTL/CSR Download)］ウィンドウが表示されます。

ステップ 5　**continue** リンクをクリックします。

選択した証明書を示すディレクトリが表示されます。

ステップ 6　証明書または CTL を PC に保存するには、証明書または CTL の名前を右クリックし、［対象をファイルに保存］をクリックします。

ステップ 7　証明書または CTL を保存する場所を入力します。

ステップ 8　［保存］をクリックします。

証明書の削除と再作成

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。

手順

ステップ 1　［セキュリティ］>［証明書の管理］>［証明書の削除 / 再作成］を選択します。

ステップ 2　［信頼証明書の削除 (Delete Trust Cert)］チェックボックスをオンにし、［次へ］をクリックします。

Display Certificates or Trust Units For Delete/Regenerate ウィンドウが表示されます。

ステップ 3　削除する既存の証明書タイプのチェックボックスをオンにし、［次へ］をクリックします。

Delete Certificates or Trust Store ウィンドウが表示されます。

ステップ 4　削除する証明書の［既存の証明書名 (Existing certificate name(s))］チェックボックスをオンにし、［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］>［証明書の削除 / 再作成］を選択します。

Select Certificates or Trust Store for Deletion ウィンドウが表示されます。

ステップ 2　［自己署名証明書の再作成 (Regenerate Self-Signed Cert)］チェックボックスをオンにし、［次へ］をクリックします。

ステップ 3　再作成する証明書の該当する［既存の証明書タイプ (Existing Certificates Types)］チェックボックスをオンにし、［次へ］をクリックします。

ステップ 4　該当する［既存の証明書］チェックボックスをオンにし、［再作成］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。

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］>［証明書 /CTL のアップロード］を選択します。

［証明書 /CTL のアップロードの選択 (Select Certificate/CTL Upload)］ウィンドウが表示されます。

ステップ 2　次のオプション ボタンのいずれかを選択し、［次へ］をクリックします。

- 自分の証明書のアップロード（Upload Own Cert）：サードパーティの CA によって発行されたアプリケーション証明書をアップロードします。
- 信頼証明書のアップロード（Upload Trust Cert）：CA ルート証明書または信頼アプリケーション証明書をアップロードします。
- CTL ファイルのアップロード（Upload CTL File）：CTL ファイルをアップロードします。

Certificate type for the upload including CTL ウィンドウが表示されます。

ステップ 3　Certificate type for the upload including CTL ウィンドウで、次の手順を実行します。

a. 証明書または CTL のタイプを［既存の証明書タイプ (Existing certificate types)］リストから選択します。

b. 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［ルート証明書名（Root Cert Name、拡張子は不要）］テキストボックスに入力します。CA ルート証明書または CTL 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。

c. ［次へ］をクリックします。

［証明書 /CTL のアップロード］ウィンドウが表示されます。

ステップ 4　［証明書 /CTL のアップロード］ウィンドウで、次の手順を実行します。

a. 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。

- ［アップロードするファイル名］テキストボックスで、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。

b. ファイルをサーバにアップロードするには、［アップロード］ボタンをクリックします。

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］>［CSR のダウンロード / 作成］を選択します。

Select Certificate type for CSR ウィンドウが表示されます。

ステップ 2　ダウンロードする CSR の［既存の証明書タイプ (Existing Certificate Types)］チェックボックスをオンにします。

ステップ 3　**Download CSR if any** チェックボックスをオンにします。

［証明書 /CTL/CSR のダウンロード (Certificate/CTL/CSR Download)］ウィンドウが表示されます。

ステップ 4　**continue** をクリックします。

ディレクトリに選択した証明書が表示されます。

ステップ 5　CSR を PC に保存するには、証明書または CTL の名前を右クリックし、［対象をファイルに保存］をクリックします。

ステップ 6　証明書または CTL の保存先を入力します。

ステップ 7　［保存］をクリックします。

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.6-6 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.6-7 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.6-7 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.6-5 の「証明書または証明書信頼リストのアップロード」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.6-5 の「証明書または証明書信頼リストのアップロード」を参照してください。

	作業	参照先
ステップ 7	CAPF または Cisco Unified Presence Server の証明書を更新した場合、新しい CTL ファイルを作成する。	『*Cisco Unified CallManager セキュリティ ガイド*』を参照してください。
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 Presence Server 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 Presence Server サービスアビリティ 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**］>［**CSR のダウンロード / 作成**］を選択します。

Select Certificate type for CSR ウィンドウが表示されます。

ステップ 2　作成する証明書のタイプを［**既存の証明書タイプ (Existing Certificate Types)**］で選択します。

ステップ 3　**Generate a new CSR** オプション ボタンを選択します。

ステップ 4　［**次へ**］をクリックします。

Cert/IPSEC Operation (CSR/Config/Assoc Create) Done ウィンドウが表示され、CSR の作成に成功したことが示されます。

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 Presence Server 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ウィンドウに表示される 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行うには、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］>［証明書の管理］>［証明書有効期限モニタ］>［設定の表示］**を選択します。

Show Cert Expiry Monitoring Config ウィンドウが表示されます。このウィンドウには、現在の設定情報が表示されます。

ステップ 2　証明書有効期限モニタを設定するには、**［セキュリティ］>［証明書の管理］>［証明書有効期限モニタ］>［設定の変更］**を選択します。

Change Cert Expiry Monitoring Config ウィンドウが表示されます。

ステップ 3　必要な設定情報を入力します。［証明書有効期限モニタ］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 4　変更内容を保存するには、**［送信］**をクリックします。

表 6-1　証明書有効期限モニタのフィールド説明

フィールド	説明
通知 / アラート開始時刻 (Notification/Alert 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。
通知の最初の頻度 : 毎 (Initial Frequency of Notification: Every)	通知の頻度を時間または日単位で入力します。
有効 / 無効を指定するには右のオプションをクリックしてください	メール通知を有効にするには、**ENABLE** をクリックします。
通知用に入力したメール ID(Email IDs entered for Notification):	通知を送信するメール 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。

IP セキュリティ管理

［IPSec］メニュー オプションを使用すると、次の機能を実行できます。

- 既存の IPSec ポリシーの表示または変更
- 新しい IPSec ポリシーの設定

（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ることはありません。

既存の IPSec ポリシーの表示または変更

既存の IPSec ポリシーを表示または変更するには、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 の管理］>［IPSEC の表示 / 変更］**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びログインする必要があります。

Display IPSEC Policy ウィンドウが表示されます。

ステップ 2　該当するポリシーをチェックし、**［次へ］**をクリックします。

ステップ 3　次の操作のいずれかを実行します。

- IPSec ポリシーを表示するには、**［詳細を表示］**リンクをクリックします。
- IPSec ポリシーを削除するには、**［削除］**をクリックします。
- IPSec ポリシーをアクティブにするには、**［有効］**をクリックします。
- IPSec ポリシーを無効にするには、**［無効］**をクリックします。

注意 既存の IPSec ポリシーに何らかの変更を行うと、システムの正常な動作に影響する場合があります。

ステップ 4　［詳細を表示］リンクをクリックすると、詳細ウィンドウが表示されます。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。

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 の管理］**>**［新規 IPSec の設定］**を選択します。

［選択の設定 (Setup Select)］ウィンドウが表示されます。

ステップ 2　**［証明書］**または**［事前共有キー］**チェックボックスをオンにします。

- ［証明書］をオンにする場合は、**［同じタイプ (Same Type)］**または**［異なるタイプ (Different Type)］**ノードをオンにします。
- ［事前共有キー］をオンにする場合は、キーの名前を入力します。

ステップ 3　**［次へ］**をクリックします。

［IPSEC のポリシーと割り当ての設定 (Setup IPSEC Policy and Association)］ウィンドウが表示されます。

ステップ 4　［IPSEC のポリシーと割り当ての設定 (Setup IPSEC Policy and Association)］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 5　新しい IPSec ポリシーを設定するには、**［送信］**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。
着信先アドレス タイプ (Dest. Address Type)	着信先アドレス タイプを指定します。 • IP：着信先のピリオドで区切られた IP アドレス • FQDN：着信先の完全修飾ドメイン名
ソース アドレス タイプ (Source Address Type)	ソース アドレス タイプを指定します。 • IP：ソースのピリオドで区切られた IP アドレス • FQDN：ソースの完全修飾ドメイン名
トンネル / 転送 (Tunnel/Transport)	トンネルまたは転送を指定します。
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 • Any
着信先ポート (Dest. Port)	着信先で使用されるポート番号を指定します。
フェーズ 1 のライフタイム（Phase 1 Life Time in seconds、秒）	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。
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
フェーズ 2 のライフタイム（Phase 2 Life Time in seconds、秒）	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。
AH アルゴリズム (AH Algorithm)	このフィールドは機能しないため、代わりに［ESP アルゴリズム (ESP Algorithm)］フィールドを使用して認証アルゴリズムを選択します。
割り当て名 (Assoc. 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。
着信先アドレス (Dest. Address)	着信先の IP アドレスまたは FQDN 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。
リモート ポート (Remote Port)	着信先のポート番号を指定します。
ソース ポート (Source Port)	ソース側のポート番号を指定します。
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
フェーズ 1 の DH 値 (Phase 1 DH value)	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。

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
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 2 の DH 値 (Phase 2 DH value)	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。