CHAPTER 38

# 証明書の設定

この章では、デジタル証明書の設定方法について説明します。次の項目を取り上げます。



## デジタル証明書に関する情報

デジタル証明書は、認証に使用されるデジタル ID を保持しています。デジタル証明書には、名前、シリアル番号、会社、部門、または IP アドレスなど、ユーザまたはデバイスを識別する情報が含まれます。CA は、証明書に「署名」してその認証を確認することで、デバイスまたはユーザのアイデンティティを保証する、信頼できる機関です。CA は、公開キーまたは秘密キーの暗号化を使用してセキュリティを保証する PKI コンテキストで、デジタル証明書を発行します。

デジタル証明書を使用して認証を行う場合は、適応型セキュリティ アプライアンス に 1 つ以上の ID 証明書と、その発行元の CA 証明書が必要です。この設定では、複数のアイデンティティ、ルート、および証明書の階層が許可されます。次に、使用可能な各種デジタル証明書について説明します。

- *CA 証明書*は、他の証明書に署名するために使用されます。これは自己署名され、*ルート証明書*と呼ばれます。別の CA 証明書により発行される証明書は、*下位証明書*と呼ばれます。詳細については、「CA 証明書認証の設定」（P.38-2）を参照してください。
- *ID 証明書*は、特定のシステムまたはホストの証明書です。この証明書も CA により発行されます。詳細については、「ID 証明書の認証の設定」（P.38-9）を参照してください。
- *コード署名者証明書*は、コードに署名するためのデジタル署名を作成する際に使用される特殊な証明書であり、署名されたコードそのものが証明書の作成元を示しています。詳細については、「コード署名者証明書の設定」（P.38-14）を参照してください。

ローカル CA は、適応型セキュリティ アプライアンス の独立認証局機能を統合したもので、証明書の配布と、発行された証明書に対するセキュアな失効チェックを行います。Web サイトのログイン ページからユーザ登録を行う場合には、ローカル CA により実現されるセキュアで設定可能な内部認証局機能によって、証明書の認証を行うことができます。詳細については、「ローカル CA を使用した認証」（P.38-16）、「ユーザ証明書の管理」（P.38-23）、および「ユーザ データベースの管理」（P.38-20）を参照してください。

（注）　CA 証明書および ID 証明書は、サイトツーサイト VPN 接続およびリモート アクセス VPN 接続の両方に適用されます。このマニュアルに記載の手順は、ASDM GUI でリモート アクセス VPN を使用する場合の手順です。

# デジタル証明書のライセンス要件

次の表に、この機能のライセンス要件を示します。

| モデル | ライセンス要件 |
|---|---|
| すべてのモデル | 基本ライセンス |

# 注意事項と制約事項

この項では、この機能のガイドラインと制限事項について説明します。

### コンテキスト モードのガイドライン

シングル コンテキスト モードとマルチ コンテキスト モードでサポートされています。

### ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードとトランスペアレント ファイアウォール モードでサポートされています。

### フェールオーバーのガイドライン

ステートフル フェールオーバーではセッションの複製はサポートされません。

### IPv6 のガイドライン

IPv6 をサポートします。

# CA 証明書認証の設定

[CA Certificates] ペインには、使用可能な証明書、発行先および発行元の CA サーバによる識別、証明書の有効期限日、関連付けられているトラストポイント、および証明書の使用法と目的が表示されます。[CA Certificates] ペインでは、次のタスクを実行できます。

- 自己署名または下位 CA 証明書を認証します。
- CA 証明書を 適応型セキュリティ アプライアンス にインストールします。
- 新しい証明書コンフィギュレーションを作成します。

- 既存の証明書コンフィギュレーションを編集します。
- CA 証明書を手動で取得してインポートします。
- 適応型セキュリティ アプライアンス が SCEP を使用して CA に接続して、自動的に証明書を取得およびインストールするようにします。
- 選択した証明書の詳細と発行元情報を表示します。
- 既存の CA 証明書の CRL にアクセスします。
- 既存の CA 証明書のコンフィギュレーションを削除します。
- 新規作成または修正した CA 証明書コンフィギュレーションを保存します。
- 変更内容をすべて破棄して、証明書コンフィギュレーションを元の設定に戻します。

この項では、次のトピックについて取り上げます。



# CA 証明書の追加またはインストール

PEM 形式での証明書の手動による貼り付けや、SCEP を使用した自動登録により、既存のファイルから証明書コンフィギュレーションを新たに追加できます。SCEP は、ユーザの介入を最小限しか必要としない、セキュアなメッセージング プロトコルです。SCEP を使用すると、VPN Concentrator Manager のみを使用して証明書を登録およびインストールできます。

CA 証明書を追加またはインストールするには、次の手順を実行します。

**ステップ 1**　メイン ASDM アプリケーション ウィンドウで、[Configuration] > [Remote Access VPN] > [Certificate Management] > [CA Certificates] の順に選択します。

**ステップ 2**　[Add] をクリックします。

[Install Certificate] ダイアログボックスが表示されます。選択されたトラストポイント名が読み取り専用形式で表示されます。

**ステップ 3**　既存のファイルから証明書コンフィギュレーションを追加するには、[Install from a file] オプション ボタンをクリックします（これがデフォルトの設定です）。

**ステップ 4**　パスおよびファイル名を入力するか、または [Browse] をクリックしてファイルを検索します。次に、[Install Certificate] をクリックします。

**ステップ 5**　手動で登録するには、[Paste certificate in PEM format] オプション ボタンをクリックします。

**ステップ 6**　PEM 形式（base64 または 16 進数）の証明書をコピーして、指定の領域に貼り付け、[Install Certificate] をクリックします。

**ステップ 7**　自動で登録するには、[Use SCEP] オプション ボタンをクリックします。適応型セキュリティ アプライアンス が、SCEP を使用して CA に接続し、証明書を取得して、証明書をデバイスにインストールします。SCEP を使用するには、インターネットを介して、SCEP をサポートする CA に登録する必要があります。SCEP を使用した自動登録では、ユーザは次の情報を入力する必要があります。

- 自動インストールする証明書のパスとファイル名。
- 証明書のインストールの最大再試行分数。デフォルトは 1 分です。
- 証明書のインストールの再試行回数。デフォルトは 0 です。この場合は、再試行時間内であれば何度でも再試行できます。

**ステップ 8**　新規および既存の証明書のその他のコンフィギュレーション オプションを表示するには、[More Options] をクリックします。

[Configuration Options for CA Certificates] ペインが表示されます。

**ステップ 9**　以降の手順については、「失効に関する CA 証明書の設定」（P.38-5）を参照してください。

# CA 証明書コンフィギュレーションの編集または削除

既存の CA 証明書コンフィギュレーションを変更または削除するには、次の手順を実行します。

**ステップ 1**　既存の CA 証明書コンフィギュレーションを変更するには、コンフィギュレーションを選択し、[Edit] をクリックします。

[Edit Options for CA Certificates] ペインが表示されます。これらのいずれかの設定を変更するには、後述の項で手順を参照してください。

- 「失効に関する CA 証明書の設定」（P.38-5）
- 「CRL 取得ポリシーの設定」（P.38-5）
- 「CRL 取得方式の設定」（P.38-6）
- 「OCSP ルールの設定」（P.38-7）
- 「高度な CRL および OCSP の設定」（P.38-7）

**ステップ 2**　CA 証明書コンフィギュレーションを削除するには、コンフィギュレーションを選択し、[Delete] をクリックします。

**（注）**　証明書コンフィギュレーションを削除すると、復元できなくなります。削除した証明書を再作成するには、[Add] をクリックして、証明書コンフィギュレーションの情報をすべて再入力します。

# CA 証明書の詳細の表示

選択した CA 証明書に関する詳細情報を表示するには、[Show Details] をクリックして、次の 3 つの*表示専用タブ*が含まれる [Certificate Details] ダイアログボックスを表示します。

- [General] タブには、タイプ、シリアル番号、ステータス、用途、公開キー タイプ、CRL 分散ポイント、証明書の有効期間、および関連付けられているトラストポイントの値が表示されます。これらの値は、[Available] と [Pending] の両方のステータスに適用されます。
- [Issued to] タブには、サブジェクト DN または証明書所有者の X.500 フィールドとその値が表示されます。これらの値は、[Available] ステータスのみに適用されます。
- [Issued by] タブには、証明書を付与したエンティティの X.500 フィールドが表示されます。これらの値は、[Available] ステータスのみに適用されます。

# CRL の要求

現在のバージョンの CRL を更新するには、[Request CRL] をクリックします。CRL の更新により、証明書ユーザに現在のステータスが反映されます。要求が失敗した場合は、エラー メッセージが表示されます。CRL は、更新された後、期限が切れるまで自動的に再生成されますが、[Request CRL] をクリックすれば、CRL ファイルの更新と再生成がその場で実行されます。

# 失効に関する CA 証明書の設定

失効に関して CA 証明書を設定するには、次の手順を実行します。

**ステップ 1**　[Configuration Options for CA Certificates] ペインで、[Revocation Check] タブをクリックします。

**ステップ 2**　証明書の失効チェックをディセーブルにするには、[Do not check certificates for revocation] オプション ボタンをクリックします。

**ステップ 3**　1 つ以上の失効チェック方式（CRL または OCSP）を選択するには、[Check certificates for revocation] オプション ボタンをクリックします。

**ステップ 4**　[Revocation Methods] 領域の左側に、選択可能な方式が表示されます。[Add] をクリックして方式を右側に移動すると、その方式が使用可能になります。[Move Up] または [Move Down] をクリックして、方式の順序を変更します。

選択した方式は、追加した順序で実装されます。方式からエラーが返された場合は、その次の失効チェック方式がアクティブになります。

**ステップ 5**　証明書の検証中に失効チェックのエラーを無視するには、[Consider certificate valid if revocation checking returns errors] チェックボックスをオンにします。

**ステップ 6**　[OK] をクリックして、[Revocation Check] タブを閉じます。また、続行する場合は「CRL 取得ポリシーの設定」（P.38-5）を参照してください。

# CRL 取得ポリシーの設定

CRL 取得ポリシーを設定するには、次の手順を実行します。

**ステップ 1**　[Configuration Options for CA Certificates] ペインで、[CRL Retrieval Policy] タブをクリックします。

**ステップ 2**　[Use CRL Distribution Point from the certificate] チェックボックスをオンにして、チェック対象の証明書から CRL 分散ポイントに失効チェックを転送します。

**ステップ 3**　[Use Static URLs configured below] チェックボックスをオンにして、CRL の取得に使用する特定の URL を一覧表示します。選択した URL は、追加した順序で実装されます。指定した URL でエラーが発生した場合は、その次の URL が使用されます。

**ステップ 4**　[Static Configuration] 領域で、[Add] をクリックします。

[Add Static URL] ダイアログボックスが表示されます。

**ステップ 5**　[URL] フィールドに、CRL の分散に使用するスタティック URL を入力して、[OK] をクリックします。

入力した URL が [Static URLs] リストに表示されます。

**ステップ 6**　スタティック URL を変更するには、URL を選択し、[Edit] をクリックします。

**ステップ 7**　既存のスタティック URL を削除するには、URL を選択し、[Delete] をクリックします。

**ステップ 8**　スタティック URL の表示順序を変更するには、[Move Up] または [Move Down] をクリックします。

**ステップ 9**　[OK] をクリックして、このタブを閉じます。また、続行する場合は「CRL 取得方式の設定」（P.38-6）を参照してください。

# CRL 取得方式の設定

CRL 取得方式を設定するには、次の手順を実行します。

**ステップ 1**　[Configuration Options for CA Certificates] ペインで、[CRL Retrieval Methods] タブをクリックします。

**ステップ 2**　次の 3 つの取得方式のいずれかを選択します。

- CRL の取得で LDAP をイネーブルにするには、[Enable Lightweight Directory Access Protocol (LDAP)] チェックボックスをオンにします。LDAP を使用して CRL を取得する場合は、指定した LDAP サーバにパスワードを使用して接続することで、LDAP セッションが開始されます。デフォルトの場合、この接続には TCP ポート 389 が使用されます。次の必須パラメータを入力します。
  - 名前
  - パスワード
  - パスワードの確認
  - デフォルト サーバ（サーバ名）
  - デフォルト ポート（389）
- CRL の取得で HTTP をイネーブルにするには、[Enable HTTP] チェックボックスをオンにします。
- CRL の取得で SCEP をイネーブルにするには、[Enable Simple Certificate Enrollment Protocol (SCEP)] チェックボックスをオンにします。

**ステップ 3**　[OK] をクリックして、このタブを閉じます。また、続行する場合は「OCSP ルールの設定」（P.38-7）を参照してください。

# OCSP ルールの設定

適応型セキュリティ アプライアンスでは、プライオリティ順に OCSP ルールが検証され、最初に一致したルールが適用されます。CRL の代わりに X.509 デジタル証明書が使用されます。

（注）　OCSP ルールを追加する前に、必ず証明書マップを設定しておいてください。証明書マップが設定されていない場合、エラー メッセージが表示されます。証明書マップを設定するには、[Configuration] > [Network (Client) Access, Advanced] > [IPSec] > [Certificate to Connection Profile Maps] > [Rules] > [Add] を選択します。

X.509 デジタル証明書の失効ステータスを取得するための OCSP ルールを設定するには、次の手順を実行します。

**ステップ 1**　[Configuration Options for CA Certificates] ペインで、[OCSP Rules] タブをクリックします。

**ステップ 2**　この OCSP ルールと照合する証明書マップを選択します。証明書マップにより、ユーザ権限と、証明書の特定のフィールドとの照合が行われます。[Certificate] フィールドに、適応型セキュリティ アプライアンス において応答側の証明書の検証に使用される CA の名前が表示されます。[Index] フィールドに、ルールのプライオリティ番号が表示されます。[URL] フィールドに、この証明書の OCSP サーバの URL が表示されます。

**ステップ 3**　新しい OCSP ルールを追加するには、[Add] をクリックします。

[Add OCSP Rule] ダイアログボックスが表示されます。

**ステップ 4**　使用する証明書マップをドロップダウン リストから選択します。

**ステップ 5**　使用する証明書をドロップダウン リストから選択します。

**ステップ 6**　ルールのプライオリティ番号を入力します。

**ステップ 7**　この証明書の OCSP サーバの URL を入力します。

**ステップ 8**　完了したら、[OK] をクリックして、このダイアログボックスを閉じます。

新しく追加された OCSP ルールがリストに表示されます。

**ステップ 9**　既存の OCSP ルールを編集するには、ルールを選択し、[Edit] をクリックします。

**ステップ 10**　OCSP ルールを削除するには、ルールを選択し、[Delete] をクリックします。

**ステップ 11**　[OK] をクリックして、このタブを閉じます。また、続行する場合は「高度な CRL および OCSP の設定」（P.38-7）を参照してください。

# 高度な CRL および OCSP の設定

証明書は発行されると、一定期間有効です。CA は、安全上の問題や名前またはアソシエーションの変更などの理由で、期限が切れる前に証明書を無効にすることがあります。CA は、無効になった証明書の署名付きリストを定期的に発行します。失効チェックをイネーブルにすると、適応型セキュリティ アプライアンスでは、検証中の証明書が CA により無効になっていないかについてのチェックが行われます。適応型セキュリティ アプライアンスでは、失効ステータスに対して、CRL および OCSP という 2 つのチェック方法がサポートされています。

CRL および OCSP の追加設定を行うには、次の手順を実行します。

**ステップ 1**　[Configuration Options for CA Certificates] ペインで、[Advanced] タブをクリックします。

**ステップ 2**　[CRL Options] 領域で、キャッシュのリフレッシュを行う間隔を分数で入力します。デフォルトは 60 分です。範囲は 1 ～ 1440 分です。CA から同じ CRL を何度も受け取る必要のないように、適応型セキュリティ アプライアンス では、取得した CRL をローカルで保存できます。これを CRL キャッシングと呼びます。CRL キャッシュの容量はプラットフォームによって異なり、すべてのコンテキストについて累積されます。新たに取得した CRL をキャッシュすることで、保存制限を超える可能性がある場合は、適応型セキュリティ アプライアンスにより使用頻度が最も低い CRL が削除され、使用可能な空き容量が確保されます。

**ステップ 3**　[Enforce next CRL update] チェックボックスをオンにして、Next Update 値の有効期限が切れていない CRL に限り、有効な CRL として使用できるようにします。[Enforce next CRL update] チェックボックスをオフにすると、Next Update 値がない場合や、Next Update 値の有効期限が切れている場合でも有効な CRL として使用できます。

**ステップ 4**　[OCSP Options] 領域で、OCSP サーバの URL を入力します。適応型セキュリティ アプライアンス で使用される OCSP サーバは、次の順に選択されます。

1. 一致証明書上書きルールの OCSP URL に対応するサーバ
2. 選択された [OCSP Options] 属性に設定した OCSP URL に対応するサーバ
3. リモート ユーザ証明書の AIA フィールドで指定されたサーバ

**ステップ 5**　デフォルトでは、[Disable nonce extension] チェックボックスがオンになっています。この設定では、暗号化によって要求を応答にバインドし、リプレイ アタックを回避します。このプロセスでは、要求と応答との間でそれぞれのナンス拡張を照合し、両者が同一であることを確認することで、リプレイ アタックを防ぐことができます。ただし、事前に生成した応答には、各要求と一致するナンス拡張は含まれていません。そのため、使用している OCSP サーバから、事前に生成した応答を送信する場合は、[Disable nonce extension] チェックボックスをオフにしてください。

**ステップ 6**　[Validation Policy] 領域で、次のオプションのいずれかを選択します。

- この CA を使用して検証できるリモート セッションのタイプを制限するには、[SSL] オプション ボタンまたは [IPsec] オプション ボタンをクリックします。
- いずれのタイプのセッションも CA で検証できるようにするには、[SSL and IPSec] オプション ボタンをクリックします。

**ステップ 7**　[Other Options] 領域で、次のオプションのいずれかを選択します。

- 指定した CA の証明書を 適応型セキュリティ アプライアンス で受け入れるようにするには、[Accept certificates issued by this CA] チェックボックスをオンにします。
- 下位 CA の証明書を 適応型セキュリティ アプライアンス で受け入れるようにするには、[Accept certificates issued by the subordinate CAs of this CA] チェックボックスをオンにします。

**ステップ 8**　[OK] をクリックしてこのタブを閉じ、[Apply] をクリックしてコンフィギュレーションの変更を保存します。

### 次の作業

「ID 証明書の認証の設定」（P.38-9）を参照してください。

# ID 証明書の認証の設定

ID 証明書は、適応型セキュリティ アプライアンス 経由の VPN アクセスの認証に使用できます。[Identity Certificates Authentication] ペインでは、次のタスクを実行できます。

- 新しい ID 証明書を追加またはインポートする。
- ID 証明書の詳細を表示する。
- 既存の ID 証明書を削除する。
- 既存の ID 証明書をエクスポートする。
- 既存の ID 証明書をインストールする。
- Entrust に ID 証明書を登録する。

この項では、次のトピックについて取り上げます。



## ID 証明書の追加またはインポート

新しい ID 証明書コンフィギュレーションを追加またはインポートするには、次の手順を実行します。

**ステップ 1**　メイン ASDM アプリケーション ウィンドウで、[Configuration] > [Remote Access VPN] > [Certificate Management] > [Identity Certificates] の順に選択します。

**ステップ 2**　[Add] をクリックします。

選択されたトラストポイント名が上部に示された [Add Identity Certificate] ダイアログボックスが表示されます。

**ステップ 3**　既存のファイルから ID 証明書をインポートするには、[Import the identity certificate from a file] オプション ボタンをクリックします。

**ステップ 4**　PKCS12 ファイルの復号化に使用するパスフレーズを入力します。

**ステップ 5**　ファイルのパス名を入力するか、[Browse] をクリックして [Import ID Certificate File] ダイアログボックスを表示します。証明書ファイルを見つけて、[Import ID Certificate File] をクリックします。

**ステップ 6**　新しい ID 証明書を追加するには、[Add a new identity certificate] オプション ボタンをクリックします。

**ステップ 7**　[New] をクリックして、[Add Key Pair] ダイアログボックスを表示します。

**ステップ 8**　デフォルトのキー ペア名を使用する場合は、[Use default keypair name] オプション ボタンをクリックします。

**ステップ 9**　新しいキー ペア名を使用する場合は、[Enter a new key pair name] オプション ボタンをクリックし、新しい名前を入力します。適応型セキュリティ アプライアンスでは、複数のキー ペアをサポートします。

**ステップ 10**　ドロップダウン リストから係数サイズを選択します。

**ステップ 11**　[General purpose] オプション ボタン（デフォルト）または [Special] オプション ボタンをクリックして、キー ペアの用途を選択します。[Special] オプション ボタンを選択すると、適応型セキュリティ アプライアンス により署名用と暗号化用の 2 つのキー ペアが生成されます。この選択は、対応する識別用に 2 つの証明書が必要なことを示します。

**ステップ 12**　[Generate Now] をクリックして新しいキー ペアを作成し、[Show] をクリックして [Key Pair Details] ダイアログボックスを表示します。ここには、次の*表示専用*の情報が示されます。

- 公開キーが認証の対象となるキー ペアの名前。
- キー ペアの生成日時。
- RSA キー ペアの用途。
- キー ペアの係数サイズ（512、768、1024、および 2048 ビット）。デフォルト値は 1024 です。
- テキスト形式の特定のキー データを含むキー データ。

**ステップ 13**　完了したら [OK] をクリックして、[Key Pair Details] ダイアログボックスを閉じます。

**ステップ 14**　ID 証明書で DN を形成するための証明書サブジェクト DN を選択します。次に [Select] をクリックして、[Certificate Subject DN] ダイアログボックスを表示します。

**ステップ 15**　ドロップダウン リストから追加する DN 属性を 1 つ以上選択し、値を入力し、[Add] をクリックします。証明書サブジェクト DN の使用可能な X.500 属性は、次のとおりです。

- Common Name（CN）
- Department（OU）
- Company Name（O）
- Country（C）
- State/Province（ST）
- Location（L）
- E-mail Address（EA）

**ステップ 16**　完了したら [OK] をクリックして、[Certificate Subject DN] ダイアログボックスを閉じます。

**ステップ 17**　自己署名証明書を作成するには、[Generate self-signed certificate] チェックボックスをオンにします。

**ステップ 18**　ID 証明書がローカル CA として動作するようにするには、[Act as local certificate authority and issue dynamic certificates to TLS proxy] チェックボックスをオンにします。

**ステップ 19**　追加の ID 証明書設定を行うには、[Advanced] をクリックします。

[Certificate Parameters]、[Enrollment Mode]、および [SCEP Challenge Password] の 3 つのタブを持つ [Advanced Options] ダイアログボックスが表示されます。

**（注）**　登録モード設定と SCEP チャレンジ パスワードは自己署名証明書では使用できません。

**ステップ 20**　[Certificate Parameters] タブをクリックし、次の情報を入力します。

- DNS ツリー階層内のノードの位置を示す FQDN（完全修飾ドメイン名）。
- ID 証明書に関連付けられている電子メール アドレス。
- 4 分割ドット付き 10 進表記の、ネットワーク上の 適応型セキュリティ アプライアンス IP アドレスです。

- 適応型セキュリティ アプライアンス シリアル番号を証明書パラメータに追加するには、[Include serial number of the device] チェックボックスをオンにします。

**ステップ 21**　[Enrollment Mode] タブをクリックし、次の情報を入力します。

- [Request by manual enrollment] オプション ボタンまたは [Request from a CA] オプション ボタンをクリックして、登録方式を選択します。
- SCEP を介して自動的にインストールされる証明書の登録 URL。
- ID 証明書のインストールに許可される最大再試行分数。デフォルトは 1 分です。
- ID 証明書のインストールに許可される最大再試行回数。デフォルトは 0 です。この場合は、再試行時間内であれば何度でも再試行できます。

**ステップ 22**　[SCEP Challenge Password] タブをクリックし、次の情報を入力します。

- SCEP パスワード
- SCEP パスワードを確認のために再入力

**ステップ 23**　完了したら [OK] をクリックして、[Advanced Options] ダイアログボックスを閉じます。

**ステップ 24**　[Add Identity Certificate] ペインで、[Add Certificate] をクリックします。

[Identity Certificates] リストに新しい ID 証明書が表示されます。

**ステップ 25**　[Apply] をクリックし、新しい ID 証明書コンフィギュレーションを保存します。

# ID 証明書の詳細の表示

選択した ID 証明書に関する詳細情報を表示するには、[Show Details] をクリックして、次の 3 つの*表示専用タブ*が含まれる [Certificate Details] ダイアログボックスを表示します。

- [General] タブには、タイプ、シリアル番号、ステータス、用途、公開キー タイプ、CRL 分散ポイント、証明書の有効期間、および関連付けられているトラストポイントの値が表示されます。これらの値は、[Available] と [Pending] の両方のステータスに適用されます。
- [Issued to] タブには、サブジェクト DN または証明書所有者の X.500 フィールドとその値が表示されます。これらの値は、[Available] ステータスのみに適用されます。
- [Issued by] タブには、証明書を付与したエンティティの X.500 フィールドが表示されます。これらの値は、[Available] ステータスのみに適用されます。

# ID 証明書の削除

ID 証明書コンフィギュレーションを削除するには、コンフィギュレーションを選択し、[Delete] をクリックします。

**（注）**　証明書コンフィギュレーションを削除すると、復元できなくなります。削除した証明書を再作成するには、[Add] をクリックして、証明書コンフィギュレーションの情報をすべて再入力します。

# ID 証明書のエクスポート

証明書コンフィギュレーションおよび関連付けられているすべてのキーと証明書を、公開キーの暗号化標準である PKCS12 形式でエクスポートできます。これには、base64 エンコードまたは 16 進数形式を使用できます。完全なコンフィギュレーションには、チェーン全体（ルート CA 証明書、ID 証明書、キー ペア）は含まれますが、登録設定（サブジェクト名、FQDN など）は含まれません。通常、この機能は、同じグループ内の適応型セキュリティ アプライアンス間で証明書を複製するために行うフェールオーバーまたはロードバランシングの設定に使用されます。たとえば、リモート アクセス クライアントから中央処理装置への呼び出しが複数のユニットで処理されている場合、これらのユニット間では、証明書コンフィギュレーションが同一であることが必要となります。このような場合、管理者は、証明書コンフィギュレーションをエクスポートしたうえで、適応型セキュリティ アプライアンスのグループ全体にインポートできます。

ID 証明書をエクスポートするには、次の手順を実行します。

**ステップ 1**　[Export] をクリックし、[Export Certificate] ダイアログボックスを表示します。

**ステップ 2**　証明書コンフィギュレーションをエクスポートするときに使用する PKCS12 形式ファイルの名前を入力します。または、[Browse] をクリックして [Export ID Certificate File] ダイアログボックスを表示し、証明書コンフィギュレーションをエクスポートするファイルを探します。

**ステップ 3**　[PKCS12 Format] オプション ボタンまたは [PEM Format] オプション ボタンをクリックして、証明書の形式を選択します。

**ステップ 4**　PKCS12 ファイルをエクスポート用に暗号化するために使用するパスフレーズを入力します。

**ステップ 5**　暗号化パスフレーズを確認のために再入力します。

**ステップ 6**　[Export Certificate] をクリックして、証明書コンフィギュレーションをエクスポートします。

情報ダイアログボックスが表示され、証明書コンフィギュレーション ファイルが指定の場所に正常にエクスポートされたことが示されます。

# 証明書署名要求の生成

**（注）**　Entrust がサポートしているのは、モジュラスのサイズが 1024 のキー*だけ*です。それ以外のキーを使用している場合は、Entrust にお問い合わせください。

Entrust に送信する証明書署名要求を生成するには、次の手順を実行します。

**ステップ 1**　[Enroll ASA SSL VPN with Entrust] をクリックして、[Generate Certificate Signing Request] ダイアログボックスを表示します。

**ステップ 2**　[Key Pair] 領域で、次の手順を実行します。

**a.**　ドロップダウン リストから、設定されたキー ペアのいずれかを選択します。

**b.**　[Show] をクリックして [Key Details] ダイアログボックスを表示します。ここには、選択されたキー ペアの生成日時、用途（一般的または特殊な用途）、係数サイズ、およびキー データといった情報が示されます。

**c.**　完了したら [OK] をクリックして、[Key Details] ダイアログボックスを閉じます。

**d.** [New] をクリックして、[Add Key Pair] ダイアログボックスを表示します。以降の手順については、「ID 証明書の追加またはインポート」（P.38-9）の手順 8 に進みます。生成したキー ペアは 適応型セキュリティ アプライアンス に送信するか、ファイルに保存できます。

**ステップ 3**　[Certificate Subject DN] 領域で、次の情報を入力します。

**a.** 適応型セキュリティ アプライアンス の FQDN または IP アドレス。

**b.** 会社の名前。

**c.** 2 文字の国番号。

**ステップ 4**　[Optional Parameters] 領域で、次の手順を実行します。

**a.** [Select] をクリックして、[Additional DN Attributes] ダイアログボックスを表示します。

**b.** ドロップダウン リストから追加する属性を選択し、値を入力します。

**c.** [Add] をクリックして、各属性を [attribute] テーブルに追加します。

**d.** [Delete] をクリックして、[attribute] テーブルから属性を削除します。

**e.** 完了したら [OK] をクリックして、[Additional DN Attributes] ダイアログボックスを閉じます。

[Additional DN Attributes] フィールドに追加された属性が表示されます。

**ステップ 5**　CA から要求された場合は、完全修飾ドメイン名情報を追加で入力します。

**ステップ 6**　[Generate Request] をクリックして、証明書署名要求を生成します。生成した証明書署名要求については、Entrust に送信するか、ファイルに保存するか、または後で送信するかを選択できます。

CSR が示された [Enroll with Entrust] ダイアログボックスが表示されます。

**ステップ 7**　登録プロセスを完了するには、http://www.entrust.net/cisco/ にある [request a certificate from Entrust] リンクをクリックします。その際、示された CSR をコピーして貼り付け、それを Entrust Web フォームを使用して送信します。後で登録する場合は、生成された CSR をファイルに保存し、[Identity Certificates] ペインの [enroll with Entrust] リンクをクリックして登録プロセスを完了します。

**ステップ 8**　Entrust により、要求の認証が確認された後、証明書が発行されます。これには数日間かかる場合があります。次に、[Identity Certificate] ペインで保留中の要求を選択し、[Install] をクリックして、証明書をインストールする必要があります。[Close] をクリックして、[Enroll with Entrust] ダイアログボックスを閉じます。

# アイデンティティ証明書のインストール

[Identity Certificates] ペインの [Install] ボタンは、保留中の登録がない場合はグレー表示されます。適応型セキュリティ アプライアンス が CSR を受信した場合は必ず、[Identity Certificates] ペインに保留中の ID 証明書が表示されます。保留中の ID 証明書を選択すると、[Install] ボタンがアクティブになります。

保留中の要求を CA に転送すると、CA はそのファイルを登録して証明書を 適応型セキュリティ アプライアンス に返します。証明書を受信したら、[Install] をクリックし、該当する ID 証明書を選択して操作を完了します。

保留中の ID 証明書をインストールするには、次の手順を実行します。

**ステップ 1**　[Identity Certificates] ペインで、[Add] をクリックし、[Add Identity Certificate] ダイアログボックスを表示します。

**ステップ 2**　[Add Identity Certificate] ダイアログボックスで、[Add a new identity certificate] オプション ボタンをクリックします。

**ステップ 3**　（任意）キー ペアを変更するか、新しいキー ペアを作成します。キー ペアは必須です。

**ステップ 4**　[Certificate Subject DN] に情報を入力し、[Select] をクリックして、[Certificate Subject DN] ダイアログボックスを表示します。

**ステップ 5**　関係する CA で必要なサブジェクト DN 属性をすべて指定し、[OK] をクリックして [Certificate Subject DN] ダイアログボックスを閉じます。

**ステップ 6**　[Add Identity Certificate] ダイアログボックスで、[Advanced] をクリックして [Advanced Options] ダイアログボックスを表示します。

**ステップ 7**　以降の手順については、「ID 証明書の認証の設定」（P.38-9）の手順 17 ～ 23 を参照してください。

**ステップ 8**　[Add Identity Certificate] ダイアログボックスで、[Add Certificate] をクリックします。

[Identity Certificate Request] ダイアログボックスが表示されます。

**ステップ 9**　テキスト タイプの CSR ファイル名（c:\verisign-csr.txt など）を入力し、[OK] をクリックします。

**ステップ 10**　CSR テキスト ファイルを CA に送信します。送信する代わりに、CA の Web サイトにある CSR 登録ページにテキスト ファイルを貼り付けることもできます。

**ステップ 11**　CA から ID 証明書が返されたら、[Identity Certificates] ペインに移動し、保留中の証明書エントリを選択して、[Install] をクリックします。

[Install Identity Certificate] ダイアログボックスが表示されます。

**ステップ 12**　該当するオプション ボタンをクリックして、次のいずれかのオプションを選択します。

- Install from a file

  または、[Browse] をクリックし、ファイルを検索します。
- Paste the certificate data in base-64 format

  コピーした証明書データを指定された領域に貼り付けます。

**ステップ 13**　[Install Certificate] をクリックします。

**ステップ 14**　[Apply] をクリックし、新しくインストールした証明書とその 適応型セキュリティ アプライアンス コンフィギュレーションを保存します。

### 次の作業

「コード署名者証明書の設定」（P.38-14）を参照してください。

# コード署名者証明書の設定

コード署名により、デジタル署名が、実際の実行可能なコードに追加されます。このデジタル署名には、署名者を認証し、署名以降にそのコードが変更されていないことを保証するのに十分な情報が含まれています。

コード署名者証明書は、関連付けられている秘密キーがデジタル署名の作成に使用される特殊な証明書です。コードの署名に使用される証明書は CA から取得され、署名されたコードが証明書の発生元を示します。[Code Signer] ペインで、または [Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Advanced] > [Java Code Signer] を選択して、コード署名者証明書をインポートできます。

[Code Signer] ペインでは、次のタスクを実行できます。

- コード署名者証明書の詳細を表示する。

- 既存のコード署名者証明書を削除する。
- 既存のコード署名者証明書をインポートする。
- 既存のコード署名者証明書をエクスポートする。
- Entrust にコード署名者証明書を登録する。

この項では、次のトピックについて取り上げます。



# コード署名者証明書の詳細の表示

選択した ID 証明書に関する詳細情報を表示するには、[Show Details] をクリックして、次の 3 つの*表示専用タブ*が含まれる [Certificate Details] ダイアログボックスを表示します。

- [General] タブには、タイプ、シリアル番号、ステータス、用途、公開キー タイプ、CRL 分散ポイント、証明書の有効期間、および関連付けられているトラストポイントの値が表示されます。これらの値は、[Available] と [Pending] の両方のステータスに適用されます。
- [Issued to] タブには、サブジェクト DN または証明書所有者の X.500 フィールドとその値が表示されます。これらの値は、[Available] ステータスのみに適用されます。
- [Issued by] タブには、証明書を付与したエンティティの X.500 フィールドが表示されます。これらの値は、[Available] ステータスのみに適用されます。

# コード署名者証明書の削除

コード署名者証明書コンフィギュレーションを削除するには、コンフィギュレーションを選択し、[Delete] をクリックします。

**（注）** 証明書コンフィギュレーションを削除すると、復元できなくなります。削除した証明書を再作成するには、[Import] をクリックして、証明書コンフィギュレーションの情報をすべて再入力します。

# コード署名者証明書のインポート

コード署名者証明書をインポートするには、次の手順を実行します。

**ステップ 1**　[Code Signer] ペインで、[Import] をクリックし、[Import Certificate] ダイアログボックスを表示します。

**ステップ 2**　PKCS12 形式ファイルの復号化に使用するパスフレーズを入力します。

**ステップ 3**　インポートするファイルの名前を入力するか、[Browse] をクリックして [Import ID Certificate File] ダイアログボックスを表示し、ファイルを検索します。

**ステップ 4**　インポートするファイルを選択し、[Import ID Certificate File] をクリックします。

[Import Certificate] ダイアログボックスに、選択した証明書ファイルが表示されます。

**ステップ 5**　[Import Certificate] をクリックします。

[Code Signer] ペインにインポートされた証明書が表示されます。

**ステップ 6**　[Apply] をクリックし、新しくインポートしたコード署名者証明書コンフィギュレーションを保存します。

## コード署名者証明書のエクスポート

コード署名者証明書をエクスポートするには、次の手順を実行します。

**ステップ 1**　[Code Signer] ペインで、[Export] をクリックし、[Export Certificate] ダイアログボックスを表示します。

**ステップ 2**　証明書コンフィギュレーションをエクスポートするときに使用する PKCS12 形式ファイルの名前を入力します。

**ステップ 3**　公開キー暗号化標準（base64 エンコードまたは 16 進数形式を使用できます）を使用するには、[Certificate Format] 領域で [PKCS12 format] オプション ボタンをクリックします。使用しない場合は、[PEM format] オプション ボタンをクリックします。

**ステップ 4**　[Browse] をクリックして [Export ID Certificate File] ダイアログボックスを表示し、証明書コンフィギュレーションをエクスポートするファイルを探します。

**ステップ 5**　ファイルを選択し、[Export ID Certificate File] をクリックします。

[Export Certificate] ダイアログボックスに、選択した証明書ファイルが表示されます。

**ステップ 6**　エクスポート用の PKCS12 形式ファイルの復号化に使用するパスフレーズを入力します。

**ステップ 7**　復号化パスフレーズを確認のために再入力します。

**ステップ 8**　[Export Certificate] をクリックして、証明書コンフィギュレーションをエクスポートします。

### 次の作業

「ローカル CA を使用した認証」（P.38-16）を参照してください。

# ローカル CA を使用した認証

ブラウザベースおよびクライアントベースの SSL VPN 接続では、ローカル CA により実現される、適応型セキュリティ アプライアンス 上に存在するセキュアで設定可能な内部認証局によって、証明書の認証を行うことができます。

ユーザの登録は、指定された Web サイトにログインすることによって行われます。ローカル CA は、適応型セキュリティ アプライアンス の基本認証局の動作を統合したもので、証明書の配布と、発行された証明書に対するセキュアな失効チェックを行います。

ローカル CA を使用すると、次のタスクを実行できます。

- ローカル CA サーバを設定する。
- ローカル CA 証明書の失効 / 失効解除を行う。

- CRL を更新する。
- ローカル CA ユーザを追加、編集、および削除する。

この項では、次のトピックについて取り上げます。

- 「ローカル CA サーバの設定」（P.38-17）
- 「ローカル CA サーバの削除」（P.38-20）

# ローカル CA サーバの設定

適応型セキュリティ アプライアンス でローカル CA サーバを設定するには、次の手順を実行します。

**ステップ 1**　[CA Server] ペインで、ローカル CA サーバをアクティブにするには、[Enable] オプション ボタンをクリックします。デフォルトではディセーブルになっています。ローカル CA サーバをイネーブルにすると、適応型セキュリティ アプライアンスによりローカル CA サーバ証明書、キー ペア、および必要なデータベース ファイルが生成され、ローカル CA サーバ証明書とキー ペアが PKCS12 ファイルにアーカイブされます。

**（注）**　設定済みのローカル CA をイネーブルにする前に、オプションのすべての設定を慎重に見直してください。イネーブルにした後で、証明書の発行者名とキー サイズ サーバ値を変更することはできません。

自己署名した証明書のキーの使用拡張により、キー暗号化、キー シグニチャ、CRL 署名、および証明書署名がイネーブルになります。

**ステップ 2**　ローカル CA を初めてイネーブルにするときには、英数字のイネーブル パスフレーズを指定する必要があります。イネーブル パスフレーズは、7 文字以上の英数字である必要があります。このパスフレーズにより、ストレージにアーカイブされたローカル CA 証明書およびローカル CA 証明書のキー ペアが保護され、不正なシャットダウンや予期しないシャットダウンが発生しないようにローカル CA サーバが保護されます。ローカル CA 証明書またはキー ペアが失われ、その復元が必要となった場合、PKCS12 アーカイブのロックを解除するためには、このパスフレーズが必要です。

**（注）**　ローカル CA サーバをイネーブルにするには、イネーブル パスフレーズが必要です。イネーブル パスフレーズの記録は、必ず安全な場所に保管してください。

**ステップ 3**　適応型セキュリティ アプライアンス をリブートしてもコンフィギュレーションが失われないように、[Apply] をクリックして、ローカル CA 証明書とキー ペアを保存します。

**ステップ 4**　ローカル CA の初回設定後にローカル CA を変更または再設定する場合は、[Disable] オプション ボタンをクリックして、適応型セキュリティ アプライアンス上のローカル CA サーバをシャットダウンする必要があります。この状態では、コンフィギュレーションおよびすべての関連ファイルはストレージ内に保持され、登録はディセーブルになっています。

設定したローカル CA がイネーブルになると、次の 2 つの設定が*表示専用*になります。

- [Issuer Name] フィールド。発行元のサブジェクト名とドメイン名がリストで示されます。これは、ユーザ名とサブジェクト名のデフォルト DN 設定により構成され、cn=FQDN という形式で示されます。ローカル CA サーバは、証明書を付与するエンティティです。証明書のデフォルト名は、cn=hostname.domainname という形式で表示されます。

- [CA Server Key Size] 設定。これは、ローカル CA サーバに生成されるサーバ証明書を対象とします。キー サイズには、キーごとに 512、768、1024、または 2048 ビットのいずれかを指定できます。デフォルトは、1 つのキーあたり 1024 ビットです。

**ステップ 5**　ドロップダウン リストから、ローカル CA サーバが発行した各ユーザ証明書に対して生成されるキーペアのクライアント キー サイズを選択します。キー サイズには、キーごとに 512、768、1024、または 2048 ビットのいずれかを指定できます。デフォルトは、1 つのキーあたり 1024 ビットです。

**ステップ 6**　CA 証明書のライフタイム値を入力します。これは、CA サーバ証明書の有効期間を日数単位で指定するものです。デフォルトは、3650 日（10 年）です。

ローカル CA サーバでは、CA 証明書の期限が切れる 30 日前に後継の CA 証明書が自動的に生成されます。この証明書をエクスポートし、他のデバイスにインポートすることにより、ローカル CA が発行したユーザ証明書のローカル CA 証明書検証を、期限が切れた後に行うことができます。

期限切れが近付いていることをユーザに通知するために、次の syslog メッセージが [ASDM Syslog Messages] ペインに表示されます。

```
%ASA-1-717049: Local CA Server certificate is due to expire in days days and a replacement
certificate is available for export.
```

**（注）**　この自動ロールオーバーが通知されたら、管理者は、新しいローカル CA 証明書が有効期限の前に必要なすべてのデバイスにインポートされるようにする必要があります。

**ステップ 7**　クライアント証明書のライフタイム値を入力します。これは、CA サーバが発行したユーザ証明書の有効期間を日数単位で指定するものです。デフォルトは 365 日（1 年）です。

[SMTP Server & Email Settings] 領域で、次の設定を指定して、ローカル CA サーバに対する電子メール アクセスを設定します。

**a.**　SMTP メール サーバ名または IP アドレスを入力します。または、省略符号（[...]）をクリックして [Browse Server Name/IP Address] ダイアログボックスを表示し、ここからサーバ名または IP アドレスを選択します。完了したら [OK] をクリックして、[Browse Server Name/IP Address] ダイアログボックスを閉じます。

**b.**　ローカル CA ユーザに電子メール メッセージを送信する際に使用する From アドレスを adminname@host.com という形式で入力します。自動電子メール メッセージは、新規登録ユーザへのワンタイム パスワードの送信や、証明書の更新が必要なときの電子メール メッセージの発行に使用されます。

**c.**　ローカル CA サーバからユーザに送信されるすべてのメッセージで使用される件名を入力します。件名を指定しない場合のデフォルトは「Certificate Enrollment Invitation」です。

**ステップ 8**　その他のオプションを設定するには、[More Options] ドロップダウン矢印をクリックします。

**ステップ 9**　CRL 分散ポイント（適応型セキュリティ アプライアンス 上の CRL の場所）を入力します。デフォルトの場所は、http://hostname.domain/+CSCOCA+/asa_ca.crl です。

**ステップ 10**　特定のインターフェイスおよびポートで、CRL に HTTP ダウンロードできるようにするには、ドロップダウン リストから publish-CRL インターフェイスを選択します。次に、1 ～ 65535 の任意のポート番号を入力します。デフォルトのポート番号は TCP ポート 80 です。

**（注）**　CRL の名前は変更できません。LOCAL-CA-SERVER.crl という名前が常に使用されます。

たとえば、http://10.10.10.100/user8/my_crl_file という URL を入力します。この場合、指定された IP アドレスを持つインターフェイスのみが動作します。要求を受信すると、適応型セキュリティ アプライアンス によってパス /user8/my_crl_file と設定済み URL が照合されます。パスが一致すると、適応型セキュリティ アプライアンスから、保存されている CRL ファイルが返されます。

**ステップ 11**　CRL の有効期間である CRL ライフタイムを時間単位で入力します。CA 証明書のデフォルトは 6 時間です。

ローカル CA では、ユーザ証明書が失効するたびまたは失効解除されるたびに、更新された CRL が再発行されますが、失効状態に変更がない場合、CRL の再発行は、そのライフタイムの中で 1 回しか行われません。[CA Certificates] ペインで [Request CRL] をクリックすると、CRL を即時に更新して再生成できます。

**ステップ 12**　データベース ストレージの場所を入力して、ローカル CA コンフィギュレーションとデータ ファイル用のストレージ領域を指定します。適応型セキュリティ アプライアンスでは、ユーザ情報、発行済み証明書、および失効リストへのアクセスと実装にローカル CA データベースが使用されます。外部ファイルを指定する場合は、外部ファイルへのパス名を入力するか、[Browse] をクリックして [Database Storage Location] ダイアログボックスを表示します。

**ステップ 13**　表示されるフォルダのリストからストレージの場所を選択し、[OK] をクリックします。

**（注）**　フラッシュ メモリには、3500 人以下のユーザを持つデータベースを保存できます。ユーザの数がそれを超えるデータベースでは外部ストレージが必要になります。

**ステップ 14**　発行された証明書のユーザ名に追加されるデフォルト サブジェクト（DN 文字列）を入力します。次に示す DN 属性を指定できます。

- CN（一般名）
- SN（姓名の姓）
- O（組織名）
- L（地名）
- C（国）
- OU（組織ユニット）
- EA（電子メール アドレス）
- ST（州 / 都道府県）
- T（タイトル）

**ステップ 15**　登録されたユーザがユーザ証明書を登録および取得するための PKCS12 登録ファイルを取得できる期間を、時間単位で入力します。この登録期間は、ワンタイム パスワードの有効期間とは関係ありません。デフォルトは 24 時間です。

**（注）**　ローカル CA の証明書の登録は、クライアントレス SSL VPN 接続でのみサポートされます。このタイプの接続の場合、クライアントと 適応型セキュリティ アプライアンス の通信は、標準の HTML を使用して Web ブラウザ経由で行われます。

**ステップ 16**　登録ユーザに電子メールで送信されたワンタイム パスワードの有効期間を入力します。デフォルトは 72 時間です。

**ステップ 17**　期限の何日前になったら、ユーザに期限切れ通知の電子メールを送信するかを入力します。デフォルトは、14 日です。

**ステップ 18**　[Apply] をクリックし、新しいまたは変更された CA 証明書コンフィギュレーションを保存します。変更を破棄して元の設定に戻す場合は、[Reset] をクリックします。

# ローカル CA サーバの削除

適応型セキュリティ アプライアンス からローカル CA サーバを削除するには、次の手順を実行します。

**ステップ 1**　[CA Server] ペインで、[Delete Certificate Authority Server] をクリックします。

[Delete Certificate Authority] ダイアログボックスが表示されます。

**ステップ 2**　CA サーバを削除する場合は、[OK] をクリックします。CA サーバを保持する場合は、[Cancel] をクリックします。

**（注）**　削除したローカル CA サーバは、復元および復旧できません。削除した CA サーバ コンフィギュレーションを再作成する場合は、CA サーバ コンフィギュレーション情報をすべて再入力する必要があります。

### 次の作業

「ユーザ データベースの管理」（P.38-20）を参照してください。

# ユーザ データベースの管理

ローカル CA ユーザ データベースには、ユーザ識別情報とユーザ ステータス（登録済み、許可、失効など）が格納されています。[Manage User Database] ペインでは、次のタスクを実行できます。

- ローカル CA データベースにユーザを追加する。
- 既存のユーザ識別情報を変更する。
- ローカル CA データベースからユーザを削除する。
- ユーザを登録する。
- CRL を更新する。
- ユーザに OTP を電子メールで送信する。
- OTP を表示または再生成（置換）する。

この項では、次のトピックについて取り上げます。

## ローカル CA ユーザの追加

ローカル CA ユーザを追加するには、次の手順を実行します。

**ステップ 1**　新しいユーザをローカル CA データベースに追加するには、[Add] をクリックして、[Add User] ダイアログボックスを表示します。

**ステップ 2**　有効なユーザ名を入力します。

**ステップ 3**　既存の有効な電子メール アドレスを入力します。

**ステップ 4**　サブジェクト（DN 文字列）を入力します。または、[Select] をクリックして、[Certificate Subject DN] ダイアログボックスを表示します。

**ステップ 5**　ドロップダウン リストから追加する DN 属性を 1 つ以上選択し、値を入力し、[Add] をクリックします。証明書サブジェクト DN の使用可能な X.500 属性は、次のとおりです。

- Common Name（CN）
- Department（OU）
- Company Name（O）
- Country（C）
- State/Province（ST）
- Location（L）
- E-mail Address（EA）

**ステップ 6**　完了したら [OK] をクリックして、[Certificate Subject DN] ダイアログボックスを閉じます。

**ステップ 7**　[Allow enrollment] チェックボックスをオンにしてユーザを登録し、[Add User] をクリックします。

[Manage User Database] ペインに新しいユーザが表示されます。

## 最初の OTP の送信または OTP の置換

新規追加されたユーザに対して、一意の OTP とローカル CA 登録 URL が記載された登録許可の電子メール通知を自動的に送信するには、[Email OTP] をクリックします。

OTP が新規ユーザに送信されたことを示す [Information] ダイアログボックスが表示されます。

自動的に新しい OTP を再発行して、新しいパスワードが記載された電子メール通知を既存のユーザまたは新規ユーザに送信するには、[Replace OTP] をクリックします。

## ローカル CA ユーザの編集

データベース内の既存のローカル CA ユーザに関する情報を変更するには、次の手順を実行します。

**ステップ 1**　特定のユーザを選択し、[Edit] をクリックして [Edit User] ダイアログボックスを表示します。

**ステップ 2**　有効なユーザ名を入力します。

**ステップ 3**　既存の有効な電子メール アドレスを入力します。

**ステップ 4**　サブジェクト（DN 文字列）を入力します。または、[Select] をクリックして、[Certificate Subject DN] ダイアログボックスを表示します。

**ステップ 5**　ドロップダウン リストから変更する DN 属性を 1 つ以上選択し、値を入力し、[Add] または [Delete] をクリックします。証明書サブジェクト DN の使用可能な X.500 属性は、次のとおりです。

- Common Name（CN）
- Department（OU）
- Company Name（O）
- Country（C）
- State/Province（ST）
- Location（L）
- E-mail Address（EA）

**ステップ 6**　完了したら [OK] をクリックして、[Certificate Subject DN] ダイアログボックスを閉じます。

**ステップ 7**　[Allow enrollment] チェックボックスをオンにしてユーザを再登録し、[Edit User] をクリックします。

[Manage User Database] ペインに更新されたユーザ詳細が表示されます。

## ローカル CA ユーザの削除

ユーザをデータベースから削除し、そのユーザに発行されたすべての証明書をローカル CA データベースから削除するには、ユーザを選択し、[Delete] をクリックします。

**（注）**　削除されたユーザは復元できません。削除したユーザ レコードを再作成するには、[Add] をクリックして、そのユーザの情報をすべて再入力します。

## ユーザ登録の許可

選択したユーザを登録するには、[Allow Enrollment] をクリックします。

[Manage User Database] ペインに示されるユーザのステータスが [enrolled] に変わります。

**（注）**　ユーザがすでに登録されている場合は、エラー メッセージが表示されます。

## OTP の表示または再生成

選択したユーザの OTP を表示または再生成するには、次の手順を実行します。

**ステップ 1**　[View/Regenerate OTP] をクリックして、[View & Regenerate OTP] ダイアログボックスを表示します。

現在の OTP が表示されます。

**ステップ 2**　完了したら [OK] をクリックし、[View & Regenerate OTP] ダイアログボックスを閉じます。

**ステップ 3**　OTP を再生成するには、[Regenerate OTP] をクリックします。

新しく生成された OTP が表示されます。

**ステップ 4**　[OK] をクリックして、[View & Regenerate OTP] ダイアログボックスを閉じます。

**次の作業**

「ユーザ証明書の管理」（P.38-23）を参照してください。

# ユーザ証明書の管理

証明書のステータスを変更するには、次の手順を実行します。

**ステップ 1**　[Manage User Certificates] ペインで、ユーザ名または証明書のシリアル番号で特定の証明書を選択します。

**ステップ 2**　次のいずれかのオプションを選択します。

- ユーザ証明書のライフタイムが期限切れになった場合は、ユーザのアクセス権を削除するために、[Revoke] をクリックします。また、ローカル CA により、証明書データベース内にあるその証明書に失効のマークが付けられ、情報が自動的に更新されて、CRL が再発行されます。
- アクセス権を復元するには、ユーザの失効した証明書を選択して、[Unrevoke] をクリックします。また、ローカル CA により、証明書データベース内にあるその証明書に失効解除のマークが付けられ、証明書の情報が自動的に更新された後、更新された CRL が再発行されます。

**ステップ 3**　完了したら [Apply] をクリックして、変更を保存します。

**次の作業**

「CRL のモニタリング」（P.38-23）を参照してください。

# CRL のモニタリング

CRL をモニタするには、次の手順を実行します。

**ステップ 1**　ASDM メイン アプリケーション ウィンドウで、[Monitoring] > [Properties] > [CRL] の順に選択します。

**ステップ 2**　[CRL] 領域で、ドロップダウン リストから CA 証明書名を選択します。

**ステップ 3**　CRL の詳細を表示するには、[View CRL] をクリックします。次に例を示します。

```
CRL Issuer Name:
    cn=asa4.cisco.com
    LastUpdate: 09:58:34 UTC Nov 11 2009
    NextUpdate: 15:58:34 UTC Nov 11 2009
    Cached Until: 15:58:34 UTC Nov 11 2009
    Retrieved from CRL Distribution Point:
      ** CDP Not Published - Retrieved via SCEP
    Size (bytes): 224
    Associated Trustpoints: LOCAL-CA-SERVER
```

**ステップ 4**　完了したら [Clear CRL] をクリックして CRL の詳細を削除し、表示する別の CA 証明書を選択します。

# 証明書管理の機能履歴

表 38-1 に、各機能変更と、それが実装されたプラットフォーム リリースを示します。ASDM は、複数のプラットフォーム リリースとの下位互換性があるため、サポートが追加された特定の ASDM リリースは一覧には含まれていません。

**表 38-1　証明書管理の機能履歴**

| 機能名 | プラットフォーム リリース | 機能情報 |
|---|---|---|
| Certificate Management | 7.0(1) | デジタル証明書（CA 証明書、ID 証明書、およびコード署名者証明書など）は、認証用のデジタル ID を提供します。デジタル証明書には、名前、シリアル番号、会社、部門、または IP アドレスなど、ユーザまたはデバイスを識別する情報が含まれます。CA は、証明書に「署名」してその認証を確認することで、デバイスまたはユーザのアイデンティティを保証する、信頼できる機関です。CA は、公開キーまたは秘密キーの暗号化を使用してセキュリティを保証する PKI コンテキストで、デジタル証明書を発行します。<br>次のパスが、使用される VPN 接続の種類に基づいて導入されました。<br>• [Configuration] > [Remote Access VPN] > [Certificate Management]<br>• [Configuration] > [Site-to-Site VPN] > [Certificate Management]。 |