CHAPTER 6

認証局およびデジタル証明書の設定

この章では、次の事項について説明します。

認証局およびデジタル証明書の概要

公開キー インフラストラクチャ（PKI）サポートは、ネットワーク上での安全な通信を確保するために、Cisco MDS 9000 ファミリ スイッチに、デジタル証明書を取得および使用する手段を提供します。PKI サポートにより、IPsec/IKE および SSH の管理機能およびスケーラビリティが提供されます。

認証局（CA）は証明書要求を管理して、ホスト、ネットワーク デバイス、ユーザなどの参加エンティティに証明書を発行します。CA は参加エンティティに対して集中型のキー管理を行います。

デジタル署名は、公開キー暗号法に基づいて、デバイスや個々のユーザをデジタル的に認証します。RSA 暗号化システムなどの公開キー暗号法では、各デバイスまたはユーザに、秘密キーと公開キーの両方を含むキー ペアが設定されます。秘密キーは秘密裡に保管し、これを知っているのは所有するデバイスまたはユーザだけです。一方、公開キーは誰もが知っているものです。両方のキーは、相互に補完的に動作します。これらのキーの一方で暗号化されたものは、他方のキーで復号化できます。送信者の秘密キーによってデータが暗号化されると、シグニチャが形成されます。受信者は、送信者の公開キーを使用してメッセージを復号化し、シグニチャを確認します。このプロセスでは、受信者が送信者の公開キーのコピーを取得していて、そのキーが確実に送信者のものであり、送信者を装っている他者のものではないことを確信している必要があります。

ここで説明する内容は、次のとおりです。

CA およびデジタル証明書の目的

CA は、証明書の要求を管理して、ホスト、ネットワーク デバイス、またはユーザなどの加入エンティティに対して証明書を発行します。CA は参加エンティティに対して集中型のキー管理を行います。

デジタル署名は、公開キー暗号法に基づいて、デバイスや個々のユーザをデジタル的に認証します。RSA 暗号化システムなどの公開キー暗号法では、各デバイスまたはユーザに、秘密キーと公開キーの両方を含むキー ペアが設定されます。秘密キーは秘密裡に保管し、これを知っているのは所有するデバイスまたはユーザだけです。一方、公開キーは誰もが知っているものです。両方のキーは、相互に補完的に動作します。これらのキーの一方で暗号化されたものは、他方のキーで復号化できます。送信者の秘密キーによってデータが暗号化されると、シグニチャが形成されます。受信者は、送信者の公開キーを使用してメッセージを復号化し、シグニチャを確認します。このプロセスでは、受信者が送信者の公開キーのコピーを取得していて、そのキーが確実に送信者のものであり、送信者を装っている他者のものではないことを確信している必要があります。

デジタル証明書は、デジタル署名と送信者を結び付けるものです。デジタル証明書には、ユーザまたはデバイスを識別するための名前、シリアル番号、会社、部門、IP アドレスなどの情報が含まれます。また、エンティティの公開キーのコピーも含まれています。証明書そのものは、アイデンティティの確認およびデジタル証明書の作成について、受信者によって明示的に信頼されている第三者である CA により署名されています。

CA のシグニチャを確認するには、受信者が CA の公開キーを知っている必要があります。このプロセスは通常、アウトオブバンド、またはインストール時に実行される操作によって処理されます。たとえば、ほとんどの Web ブラウザには、デフォルトで複数の CA の公開キーが設定されています。IPSec の基本コンポーネントであるインターネット キー交換（IKE）は、デジタル シグニチャを使用して、セキュリティ アソシエーションを設定する前にピア デバイスをスケーラブルに認証できます。

信頼モデル、トラストポイント、アイデンティティ CA

PKI サポートで使用されるトラスト モデルは、設定可能な複数の信頼できる CA による階層構造です。各加入エンティティには、セキュリティ プロトコル エクスチェンジによって取得したピアの証明書を確認できるように、信頼できる CA のリストが設定されます。ただし、その証明書がローカルの信頼できる CA の 1 つから発行されていることが条件になります。これを実行するために、CA が自己署名したルート証明書（または下位 CA の証明書チェーン）がローカルに保管されます。信頼できる CA のルート証明書（または下位 CA の場合には完全な証明書チェーン）を安全に取得し、ローカルで保管するプロセスは、*CA 認証*と呼ばれ、CA を信頼するための必須ステップです。

ローカルに設定された信頼できる CA の情報を *トラスト ポイント*、CA そのものを *トラスト ポイント CA* と呼びます。この情報は、CA 証明書（または下位 CA の証明書チェーン）と、証明書失効チェック情報によって構成されます。

MDS スイッチも、（IPsec/IKE などの）アイデンティティ証明書を取得するために、トラスト ポイントに登録できます。このトラストポイントを *アイデンティティ CA* と呼びます。

RSA キー ペアおよびアイデンティティ証明書

1 つ以上の RSA キー ペアを生成し、各 RSA キー ペアに、アイデンティティ証明書を取得するために MDS スイッチを登録するトラスト ポイント CA を関連付けることができます。MDS スイッチは、各 CA について 1 つのアイデンティティ、つまり 1 つのキー ペアと 1 つのアイデンティティ証明書だけを必要とします。

Cisco MDS NX-OS では、RSA キー ペアの生成時に、キーのサイズ（または絶対値）を設定できます。デフォルトのキーのサイズは 512 です。また、RSA キー ペアのラベルも設定できます。デフォルトのキー ラベルは、スイッチの完全修飾ドメイン名（FQDN）です。

次に、トラスト ポイント、RSA キー ペア、およびアイデンティティ証明書の関連についての要約を示します。

- トラスト ポイントは、MDS スイッチが任意のアプリケーション（IKE または SSH など）に関して、ピアの証明書を確認するために信頼する特定の CA になります。
- MDS スイッチには多数のトラスト ポイントを設定でき、スイッチ上のすべてのアプリケーションは、いずれかのトラスト ポイント CA から発行されたピア証明書を信頼できます。
- トラストポイントは特定のアプリケーション用に限定されません。
- MDS スイッチは、アイデンティティ証明書を取得するためのトラスト ポイントに相当する CA に登録されます。スイッチを複数のトラスト ポイントに登録して、各トラスト ポイントから個別のアイデンティティ証明書を取得できます。アイデンティティ証明書は、発行する CA によって証明書に指定されている目的に応じてアプリケーションで使用します。証明書の目的は、証明書の拡張情報として証明書に保管されます。
- トラスト ポイントへの登録時に、認証される RSA キー ペアを指定する必要があります。このキー ペアは、登録要求を作成する前に生成して、トラスト ポイントに関連付ける必要があります。トラスト ポイント、キー ペア、およびアイデンティティ証明書間のアソシエーションは、証明書、キー ペア、またはトラスト ポイントを削除して明示的に廃棄されるまで有効です。
- アイデンティティ証明書のサブジェクト名は、MDS スイッチの FQDN です。
- スイッチに 1 つ以上の RSA キー ペアを生成して、各キー ペアを 1 つ以上のトラスト ポイントに関連付けることができます。ただし、トラスト ポイントに関連付けることができるキー ペアは 1 つだけです。つまり、各 CA から取得できるアイデンティティ証明書は 1 つだけです。
- 複数のアイデンティティ証明書を（それぞれ異なる CA から）取得した場合、アプリケーションがピアとのセキュリティ プロトコル エクスチェンジに使用する証明書は、アプリケーションによって異なります。
- 1 つのアプリケーションに 1 つまたは複数のトラストポイントを指定する必要はありません。証明書の目的がアプリケーションの要件を満たしていれば、どのアプリケーションもあらゆるトラストポイントで発行されたあらゆる証明書を使用できます。
- 1 つのトラスト ポイントから複数のアイデンティティ証明書を取得したり、1 つのトラスト ポイントに複数のキー ペアを関連付ける必要はありません。CA 証明書は、付与されたアイデンティティ（の名前）を一度だけ使用し、同じサブジェクト名で複数の証明書は発行しません。1 つの CA から複数のアイデンティティ証明書を取得する必要がある場合には、同じ CA に対して別のトラストポイントを定義し、別のキー ペアを関連付けて、認証を受けます。ただし、その CA が同じサブジェクト名で複数の証明書を発行できることが条件になります。

複数の信頼できる CA のサポート

MDS スイッチには、複数のトラスト ポイントを設定して、それぞれ異なる CA に関連付けることにより、複数の信頼できる CA を設定できます。複数の信頼できる CA を設定する場合、ピアに証明書を発行した特定の CA に対して、スイッチを登録する必要はありません。代わりに、ピアが信頼する複数の信頼できる CA をスイッチに設定します。スイッチは、ピアの証明書がスイッチのアイデンティティを定義した CA 以外の CA から発行されていても、設定された信頼できる CA を使用して、ピアの証明書を確認できます。

複数の信頼できる CA を設定することにより、IKE を使用して IPsec トンネルを確立する場合に、異なるドメイン（異なる CA）に登録した 2 台以上のスイッチ間で相互のアイデンティティを確認できます。

PKI 登録サポート

登録は、IPsec/IKE または SSH などのアプリケーションに使用する、スイッチのアイデンティティ証明書を取得するプロセスです。このプロセスは、証明書を要求するスイッチと CA 間で実行されます。

スイッチの PKI 登録プロセスでは、次の手順を実行します。

1. スイッチ上に RSA 秘密キーと公開キーのキー ペアを生成します。
2. 証明書要求を標準形式で生成し、CA に転送します。
3. CA が受信した登録要求を承認する場合、CA サーバ上で CA 管理者による手動操作が必要になることがあります。
4. CA から発行され、CA の秘密キーが署名された証明書を受信します。
5. 証明書を、スイッチ上の不揮発性ストレージ領域（ブートフラッシュ）に書き込みます。

カットアンドペーストによる手動登録

Cisco MDS NX-OS は、手動でのカットアンドペースト方式による証明書の検索および登録をサポートしています。カットアンドペーストによる登録では、文字通り、スイッチと CA 間で、証明書要求と生成された証明書をカットアンドペーストする必要があります。手順は、次のとおりです。

1. 登録証明書要求を作成します。この要求は、base64 符号化テキスト形式で表示されます。
2. 符号化された証明書要求テキストを、E メールまたは Web 形式にカットアンドペーストして、CA に送信します。
3. E メール メッセージまたは Web ブラウザでのダウンロードにより、CA から発行された証明書（base64 符号化テキスト形式）を受信します。
4. 証明書インポート機能を使用して、発行された証明書をスイッチにカットアンドペーストします。

（注） DCNM-SAN は、カットアンドペーストをサポートしていません。代わりに、登録要求（証明書署名要求）をファイルに保存して、CA に手動で送信できます。

複数の RSA キー ペアおよびアイデンティティ CA のサポート

複数のアイデンティティ CA をサポートすることにより、スイッチを複数のトラスト ポイントに登録できます。その結果、異なる CA から 1 つずつ、複数のアイデンティティ証明書を取得できます。これにより、各ピアで許容される適切な CA から発行された証明書を使用して、多数のピアとの IPSec および他のアプリケーションにスイッチを加入させることができます。

複数の RSA キー ペアのサポート機能により、スイッチ上で、登録した各 CA ごとに異なるキー ペアを保持できます。したがって、キーの長さなど、他の CA から指定された要件と対立することなく、各 CA のポリシー要件と一致させることができます。スイッチ上で複数の RSA キー ペアを生成し、各キー ペアを異なるトラスト ポイントに関連付けることができます。これにより、トラスト ポイントへの登録時に、関連付けたキー ペアを使用して証明書要求を作成できます。

ピア証明書の確認

MDS スイッチの PKI サポートを使用して、ピアの証明書を確認できます。スイッチは、IPsec/IKE および SSH など、アプリケーション固有のセキュリティ エクスチェンジの実行時に、ピアから提示された証明書を確認します。アプリケーションは、提示されたピア証明書の有効性を確認します。ピア証明書の確認プロセスでは、次の手順が実行されます。

- ピア証明書がローカルの信頼できる CA のいずれかから発行されていることを確認します。
- ピア証明書が現在時刻において有効であること（期限切れでない）ことを確認します。
- ピア証明書が、発行した CA によって取り消されていないことを確認します。

失効チェックでは、2 つの方式がサポートされています。証明書失効リスト（CRL）および Online Certificate Status Protocol（OCSP）です。トラスト ポイントは、いずれかまたは両方の方式を使用して、ピア証明書が失効されていないことを確認します。

CRL のダウンロード、キャッシュ、およびチェックのサポート

証明書失効リスト（CRL）は、期限前に失効された証明書の情報を提供するために CA によって保持され、レポジトリで公開されます。ダウンロード用の URL が公開され、すべての発行済み証明書にも指定されています。ピア証明書を確認するクライアントは、発行元 CA から最新の CRL を取得し、この情報を使用して、証明書が失効しているかどうかを判別する必要があります。クライアントは、自身の信頼できる CA のすべてまたは一部の CRL をローカルにキャッシュして、その CRL が期限切れになるまで必要に応じて使用することができます。

Cisco MDS NX-OS では、トラスト ポイント用の CRL を事前にダウンロードして、スイッチのブートフラッシュにキャッシュされるように手動で設定できます。IPSec または SSH によるピア証明書の確認では、CRL がローカルでキャッシュされ、失効チェックに CRL が使用されるように設定されている場合にかぎり、発行元 CA の CRL が参照されます。それ以外の場合、他の失効チェック方式が設定されていなければ、失効チェックは実行されず、証明書は失効していないと見なされます。このモードの CRL チェックは、CRL オプションと呼ばれています。

OCSP サポート

Online Certificate Status Protocol（OCSP）は、オンラインでの証明書失効チェックを容易にします。各トラスト ポイントに OCSP URL を指定できます。アプリケーションは、失効チェック方式を、指定された順序で選択します。CRL、OCSP、none、またはこれらの方式の組み合わせを指定できます。

証明書および関連キー ペアのインポート/エクスポートのサポート

CA 認証と登録のプロセスの一環として、下位 CA 証明書（または証明書チェーン）とアイデンティティ証明書を標準の PEM（base64）形式でインポートできます。

トラストポイントでのアイデンティティ情報全体を、パスワードで保護される PKCS#12 標準形式でファイルにエクスポートできます。この情報を、以降で同じスイッチ（システム クラッシュ後など）または交換したスイッチにインポートできます。PKCS#12 ファイルには、RSA キー ペア、アイデンティティ証明書、および CA 証明書（またはチェーン）の情報が含まれます。

最大限度

表 6-1 に、CA およびデジタル証明書のパラメータの最大限度を示します。

表 6-1　CA およびデジタル証明書の最大限度

機能	最大限度
スイッチ上で宣言するトラスト ポイント	16
スイッチ上で生成する RSA キー ペア	16
スイッチ上に設定するアイデンティティ証明書	16
CA 証明書チェーンに含まれる証明書	10
特定の CA に対して認証されるトラスト ポイント	10

デフォルト設定

表 6-2 に、CA およびデジタル証明書のパラメータのデフォルト設定を示します。

表 6-2　CA およびデジタル証明書のパラメータのデフォルト値

パラメータ	デフォルト
トラスト ポイント	なし
RSA キー ペア	なし
RSA キー ペアのラベル	Switch FQDN
RSA キー ペアのモジュール	512
RSA キー ペアのエクスポートの可否	Yes
トラスト ポイントの失効チェック方式	CRL

CA およびデジタル証明書の設定

ここでは、Cisco MDS スイッチ装置で CA およびデジタル証明書を相互運用するために必要な作業について説明します。この項の内容は、次のとおりです。

- 「ホスト名および IP ドメイン名の設定」（P.6-7）
- 「RSA キー ペアの生成」（P.6-7）

ホスト名および IP ドメイン名の設定

スイッチのホスト名および IP ドメイン名が未設定の場合には、これらを設定する必要があります。アイデンティティ証明書のサブジェクトとして、スイッチの FQDN が使用されるからです。また、キー ペアの生成時にキー ラベルを指定しない場合、デフォルトのキー ラベルとしてスイッチの FQDN が使用されます。たとえば、SwitchA.example.com という名前の証明書は、SwitchA というスイッチのホスト名と、example.com というスイッチの IP ドメイン名で構成されています。

注意　証明書の生成後にホスト名または IP ドメイン名を変更すると、証明書が無効になることがあります。

手順の詳細

ホスト名および IP ドメイン名の設定方法については、『*Cisco MDS 9000 NX-OS Fundamental Configuration Guide*』を参照してください。

RSA キー ペアの生成

RSA キー ペアは、IKE/IPsec および SSH などのアプリケーションによるセキュリティ プロトコル エクスチェンジの実行中に、署名およびセキュリティ ペイロードの暗号化/復号化に使用されます。RSA キー ペアは、スイッチの証明書を取得する前に必要になります。

手順の詳細

RSA サーバ キー ペアを生成する手順は、次のとおりです。

ステップ 1　[Information] ペインで、[Switches] > [Security] を展開し、[PKI] を選択します。

ステップ 2　[RSA Key-Pair] タブをクリックします。

ステップ 3　[Create Row] をクリックします。

ステップ 4　RSA キー ペアを作成するスイッチを選択します。

ステップ 5　RSA キー ペアに名前を指定します。

ステップ 6　サイズまたは絶対値を選択します。有効なモジュラスの値は 512、768、1024、1536、および 2048 です。

（注）　キーの絶対値を指定するときは、ローカル サイト（MDS スイッチ）および CA（登録先）のセキュリティ ポリシー（または要件）を考慮してください。

（注）　スイッチに設定できるキー ペアの最大数は、16 です。

ステップ 7　キーをエクスポート可能にする場合には、[Exportable] チェックボックスをオンにします。

注意　キー ペアのエクスポート設定は、キー ペアの生成後は変更できません。

（注）　RKCS#12 形式でエクスポートできるのは、エクスポート可能なキー ペアだけです。

ステップ 8　[Create] をクリックして、RSA キー ペアを作成します。

トラスト ポイント CA アソシエーションの作成

手順の詳細

トラスト ポイント CA アソシエーションを作成する手順は、次のとおりです。

ステップ 1　[Physical Attributes] ペインで、[Switches] > [Security] を展開し、[PKI] を選択します。

ステップ 2　[Information] ペインで [Trust Point] タブをクリックします。

ステップ 3　[Create Row] をクリックします。

ステップ 4　[Switch] ドロップダウン メニューから、トラスト ポイント CA を作成するスイッチを選択します。

ステップ 5　トラスト ポイント CA に名前を指定します。

ステップ 6　登録時に、このトラスト ポイントに関連付けるキー ペアの名前を選択します。「RSA キー ペアの生成」（P.6-7）で作成した名前です。各 CA に 1 つの RSA キー ペアだけを指定できます。

ステップ 7　[RevokeCheckMethod] ドロップダウン メニューから、使用する証明書失効チェック方式を選択します。CRL、OCSP、CRL OCSP、または OCSP CRL を使用して、証明書の失効をチェックできます。

CRL OCSP オプションでは、最初にローカルに保管されている CRL を使用して証明書の失効がチェックされます。見つからない場合、OCSP を使用して、ステップ 7 で指定した URL 上で証明書の失効がチェックされます。

ステップ 8　OCSP 証明書失効チェック方式を選択した場合には、OCSP の URL を入力します。

（注）　OCSP の URL は、失効チェック方式を設定する前に、設定しておく必要があります。

ステップ 9　[Create] をクリックして、トラスト ポイント CA を作成します。

ブートフラッシュへのファイルのコピー

手順の詳細

Device Manager を使用してブートフラッシュにファイルをコピーする手順は、次のとおりです。

ステップ 1　[Admin] > [Flash Files] を選択します。

ステップ 2　[Device] フィールドでブートフラッシュを選択します。

ステップ 3　[Copy] をクリックします。

ステップ 4　[Protocol] フィールドで、[tftp] を選択します。

ステップ 5　[Browse] ボタンをクリックして、ブートフラッシュにコピーする適切なファイルを検索します。

ステップ 6　[Apply] をクリックして、変更を適用します。

CA の認証

信頼できる CA の設定プロセスは、MDS スイッチに対して CA が認証された場合にかぎり、完了します。スイッチは、CA を認証する必要があります。CA を認証するには、CA の公開キーが含まれている CA の自己署名付きの証明書を PEM 形式で取得します。この CA の証明書は自己署名（CA が自身の証明書に署名したもの）であるため、CA の公開キーは、CA アドミニストレータに連絡し、CA 証明書のフィンガープリントを比較して手動で認証する必要があります。

（注）　認証される CA が自己署名した CA ではない場合（つまり、別の CA の下位 CA で、その別の CA もまた、最終的に自己署名した別の CA の下位 CA であるような場合）には、CA 認証の手順で、認証チェーンに含まれるすべての CA の CA 証明書の完全なリストを入力する必要があります。これは、認証される CA の *CA 認証チェーン*と呼ばれます。CA 証明書チェーン内の証明書の最大数は 10 です。

手順の詳細

CA を認証する手順は、次のとおりです。

ステップ 1　[Physical Attributes] ペインで、[Switches] > [Security] を展開し、[PKI] を選択します。

ステップ 2　[Information] ペインで [Trust Point Actions] タブをクリックします。

ステップ 3　[Command] フィールドのドロップダウン メニューをクリックして、適切なオプションを選択します。

使用可能なオプションは、[caauth]、[cadelete]、[certreq]、[certimport]、[certdelete]、[pkcs12import]、および [pkcs12export] です。CA を認証して、その CA の証明書または証明書チェーンをトラスト ポイントに設定するには、[caauth] オプションを選択します。

ステップ 4　URL フィールドの [...] ボタンをクリックして、[Bootflash Files] ダイアログボックスから適切なインポート証明書ファイルを選択します。bootflash:filename 形式で、CA 証明書またはチェーンが含まれているファイル名です。

（注）　特定の CA に対して最大 10 のトラスト ポイントを認証できます。

（注）　[Import Certificate] ダイアログボックスで必要なファイルが見つからない場合には、ファイルがブートフラッシュにコピーされているかどうかを確認します。「ブートフラッシュへのファイルのコピー」（P.9）を参照してください。

ステップ 5　[Apply Changes] をクリックして、変更を保存します。

認証が確認されるかどうかは、フィンガープリントの手動検証によって証明書が受け入れられるかどうかによります。

CA 認証の確認

「CA の認証」（P.6-9）のステップ 5 で説明したように、フィンガープリントの確認に基づいて CA 証明書を受け入れるには、CA 認証のあとに CA の確認が必要です。

手順の詳細

CA 認証を確認する手順は、次のとおりです。

ステップ 1　[Physical Attributes] ペインで、[Switches] > [Security] を展開し、[PKI] を選択します。

ステップ 2　[Information] ペインで [Trust Point Actions] タブをクリックします。

ステップ 3　トラスト ポイント行の [IssuerCert FingerPrint] カラムの表示から、確認する CA 証明書のフィンガープリントを書き留めます。CA 証明書のフィンガープリントと、CA から通知された（CA の Web サイトから取得した）フィンガープリントを比較します。

フィンガープリントが正確に一致していれば、[Command] ドロップダウン メニューの [certconfirm] コマンドを使用して、CA を受け入れます。一致していない場合は、[certnoconfirm] コマンドを使用して CA を拒否します。

ステップ 4　ステップ 3 で [certconfirm] を選択した場合は、[Command] をクリックして、ドロップダウン メニューから [certconfirm] 処理を選択します。[Apply Changes] をクリックします。

ステップ 3 で [certnoconfirm] を選択した場合は、[Command] をクリックして、ドロップダウン メニューから [certnoconfirm] 処理を選択します。[Apply Changes] をクリックします。

証明書の失効チェック方式の設定

クライアント（IKE ピアまたは SSH ユーザなど）とのセキュリティ エクスチェンジの実行中に、MDS スイッチはクライアントから送信されたピア証明書の確認を実行します。この確認プロセスには、証明書失効ステータスのチェックを含めることができます。

送信された証明書が失効しているかどうかを調べるには、複数の方式があります。スイッチが CA からダウンロードした CRL をチェックするように設定するか（「CRL の設定」（P.6-15）を参照）、ネットワークでサポートされている場合には OSCP を使用するか、またはその両方を使用できます。CRL のダウンロードとローカルでの確認では、ネットワーク上にトラフィックは発生しません。ただし、

CRL のダウンロード後に証明書が失効された場合、失効ステータスを認識できません。OSCP では、CA の最新の CRL をチェックできます。ただし、OSCP を使用するとネットワーク トラフィックが生成されるので、ネットワークの効率に影響することがあります。失効証明書をチェックする最も確実な方法は、ローカル CRL チェックと OSCP の両方を使用することです。

（注）　証明書の失効チェックを設定する前に、CA を認証する必要があります。

DCNM-SAN では、トラスト ポイント CA の作成時に証明書失効チェック方式を設定できます。「トラスト ポイント CA アソシエーションの作成」（P.6-8）を参照してください。

証明書要求の生成

スイッチの各 RSA キー ペアについて、関連付けたトラスト ポイント CA からアイデンティティ証明書を取得するには、要求を生成する必要があります。さらに、表示された要求を、CA 宛ての E メール メッセージまたは Web サイト フォームにカットアンドペーストします。

手順の詳細

CA から署名入り証明書要求を生成する手順は、次のとおりです。

ステップ 1　[Physical Attributes] ペインで、[Switches] > [Security] を展開し、[PKI] を選択します。

ステップ 2　[Information] ペインで [Trust Point Actions] タブをクリックします。

ステップ 3　[Command] ドロップダウン メニューから、[certreq] オプションを選択します。

このトラスト ポイント エントリに対応する CA のアイデンティティ証明書を取得するために必要な PKCS#10 証明書署名要求（CSR）が生成されます。エントリには、関連付けたキー ペアが必要です。CA 証明書または証明書チェーンが、**caauth** 処理によって設定されている必要があります。「CA の認証」（P.6-9）を参照してください。

ステップ 4　生成した証明書要求を保管する出力ファイル名を入力します。

PEM 形式で生成された CSR が保管されます。bootflash:filename 形式を使用します。この CSR を、アイデンティティ証明書を取得する CA に送信する必要があります。アイデンティティ証明書を取得したあと、証明書をこのトラスト ポイントにインストールします。「アイデンティティ証明書のインストール」（P.6-11）を参照してください。

ステップ 5　CSR に含める *チャレンジ* パスワードを入力します。

（注）　チャレンジ パスワードは、設定には保存されません。このパスワードは、証明書を失効する必要がある場合に要求されるので、パスワードを覚えておく必要があります。

ステップ 6　[Apply Changes] をクリックして、変更を保存します。

アイデンティティ証明書のインストール

CA からのアイデンティティ証明書は、base64 符号化テキスト形式で、E メールまたは Web ブラウザで受信します。CLI インポート機能使用して符号化テキストをカットアンドペーストすることにより、CA のアイデンティティ証明書をインストールする必要があります。

手順の詳細

CA から受信したアイデンティティ証明書をインストールする手順は、次のとおりです。

ステップ 1　[Physical Attributes] ペインで、[Switches] > [Security] を展開し、[PKI] を選択します。

ステップ 2　[Information] ペインで [Trust Point Actions] タブをクリックします。

ステップ 3　[Command] ドロップダウン メニューから [certimport] オプションを選択して、このトラスト ポイントにアイデンティティ証明書をインポートします。アイデンティティ証明書は、事前に生成した CSR により、対応する CA から取得します（「証明書要求の生成」（P.6-11）を参照）。

（注）　アイデンティティ証明書は、ブートフラッシュ内に PEM 形式のファイルで保存されている必要があります。

ステップ 4　URL フィールドに、ブートフラッシュにコピーされている証明書ファイルの名前を、bootflash:filename 形式で入力します。

ステップ 5　[Apply Changes] をクリックして変更を保存します。

正常に実行されると、アイデンティティ証明書の値、および証明書のファイル名などの関連オブジェクトが、アイデンティティ証明書内の対応する属性に応じて、適切な値に自動的に更新されます。

コンフィギュレーションの保存

変更したコンフィギュレーションは、終了時に情報が失われないように、保存しておく必要があります。

手順の詳細

コンフィギュレーションを保存する手順は、次のとおりです。

ステップ 1　[Physical Attributes] ペインで、[Switches] を展開し、[Copy Configuration] を選択します。

ステップ 2　RSA キー ペアおよび証明書を含む、スイッチのコンフィギュレーションを選択します。

ステップ 3　[Apply Changes] をクリックして、変更を保存します。

トラスト ポイントの設定がリブート後も維持されていることの確認

トラスト ポイント設定は、標準の Cisco NX-OS コンフィギュレーションであるため、スタートアップ コンフィギュレーションに明示的にコピーした場合にかぎり、システム リブート後も存続します。トラスト ポイント設定をスタートアップ コンフィギュレーションにコピーしておけば、トラスト ポイントに関連する証明書、キー ペア、および CRL が自動的に保持されます。逆に、トラスト ポイントがスタートアップ コンフィギュレーションにコピーされていないと、証明書、キー ペア、および関連 CRL は保持されません。リブート後に、対応するトラスト ポイント設定が必要になるからです。設定した証明書、キー ペア、および CRL を確実に保持するために、必ず、実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーしてください。また、証明書またはキー ペアを削除した場合も、削除を反映させるために、実行コンフィギュレーションを保存してください。

特定のトラスト ポイントがスタートアップ コンフィギュレーションに保存されていれば、トラスト ポイントに関連する証明書および CRL は、インポートした時点で（スタートアップ コンフィギュレーションに明示的にコピーしなくても）自動的に存続します。

また、パスワードで保護したアイデンティティ証明書のバックアップを作成して、外部サーバに保存しておくことを推奨します（「PKCS#12 形式でのアイデンティティ情報のエクスポートとインポート」（P.6-13）を参照）。

（注） コンフィギュレーションを外部サーバにコピーすると、証明書およびキー ペアも保存されます。

CA および証明書の設定のモニタリングとメンテナンス

このセクションの作業は、オプションです。ここで説明する内容は、次のとおりです。

- 「PKCS#12 形式でのアイデンティティ情報のエクスポートとインポート」（P.6-13）
- 「CRL の設定」（P.6-15）
- 「CA 設定からの証明書の削除」（P.6-15）
- 「スイッチからの RSA キー ペアの削除」（P.6-16）

PKCS#12 形式でのアイデンティティ情報のエクスポートとインポート

アイデンティティ証明書を、トラストポイントの RSA キー ペアや CA 証明書（または下位 CA の場合はチェーン全体）と一緒に PKCS#12 ファイルにバックアップ目的でエクスポートすることができます。以降で、スイッチをシステム クラッシュから回復する場合、またはスーパーバイザ モジュールを交換する場合に、証明書および RSA キー ペアをインポートできます。

（注） エクスポートおよびインポートの URL の指定では、**bootflash:***filename* 形式のローカル構文だけがサポートされます。

手順の詳細

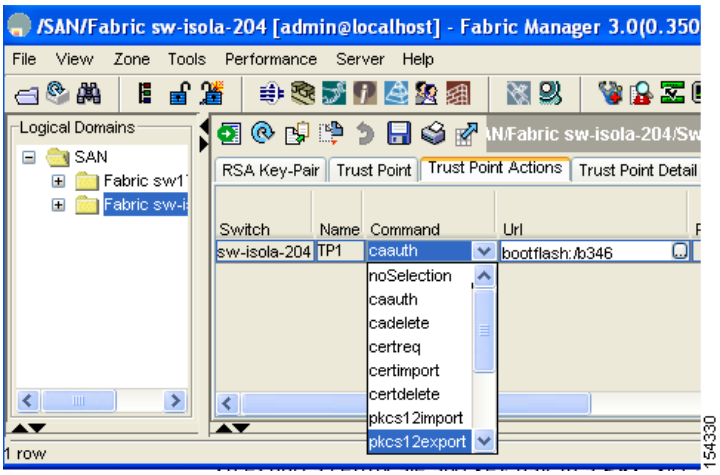
証明書およびキー ペアを RKCS#12 形式ファイルにエクスポートする手順は、次のとおりです。

ステップ 1　[Physical Attributes] ペインで、[Switches] > [Security] を展開し、[PKI] を選択します。

ステップ 2　[Information] ペインで [Trust Point Actions] タブをクリックします（図 6-1 を参照）。

ステップ 3　[Command] ドロップダウン メニューで [pkcs12export] オプションを選択し、選択したトラスト ポイントからキー ペア、アイデンティティ証明書、および CA 証明書または証明書チェーンを RKCS#12 形式でエクスポートします。

図 6-1　キー ペアをエクスポートする [pkcs12export] オプション



ステップ 4　エクスポートした PKCS#12 アイデンティティを保存する出力ファイル名を、bootflash:filename 形式で入力します。

ステップ 5　必要なパスワードを入力します。このパスワードは、PKCS#12 データの符号化用に設定されます。正常に完了すると、エクスポートしたデータがブートフラッシュ内の指定ファイルに格納されます。

ステップ 6　[Apply Changes] をクリックして、変更を保存します。

PKCS#12 形式ファイルとして保存された証明書およびキー ペアをインポートする手順は、次のとおりです。

ステップ 1　[Physical Attributes] ペインで、[Switches] > [Security] を展開し、[PKI] を選択します。

ステップ 2　[Information] ペインで [Trust Point Actions] タブをクリックします（図 6-1 を参照）。

ステップ 3　[Command] ドロップダウン メニューで [pkcs12import] オプションを選択し、RKCS#12 形式のキー ペア、アイデンティティ証明書、および CA 証明書または証明書チェーンを、選択したトラスト ポイントにインポートします。

ステップ 4　PKCS#12 アイデンティティを含む入力ファイル名を、bootflash:filename 形式で入力します。

ステップ 5　必要なパスワードを入力します。このパスワードは、PKCS#12 データの復号化用に設定されます。完了すると、インポートしたデータがブートフラッシュ内の指定ファイルに格納されます。

ステップ 6　[Apply Changes] をクリックして、変更を保存します。

完了すると、RSA キー ペア テーブルに、インポートしたキー ペアに対応するトラスト ポイントが作成されます。トラスト ポイントの証明書情報が更新されます。

（注）　PKCS#12 ファイルを正常にインポートするには、トラスト ポイントが空白である（RSA キー ペアが関連付けられていない、および CA 認証により CA が関連付けられていない）必要があります。

CRL の設定

手順の詳細

ファイルからトラスト ポイントに CRL を設定する手順は、次のとおりです。

ステップ 1　[Physical Attributes] ペインで、[Switches] > [Security] > [PKI] をクリックします。

ステップ 2　[Information] ペインで [Trust Point Actions] タブをクリックします。

ステップ 3　[Command] ドロップダウン メニューから [crlimport] オプションを選択して、選択したトラスト ポイントに CRL をインポートします。

ステップ 4　URL フィールドに、CRL の入力ファイル名を bootflash:filename 形式で入力します。

ステップ 5　[Apply Changes] をクリックして、変更を保存します。

CA 設定からの証明書の削除

トラスト ポイントに設定されているアイデンティティ証明書や CA 証明書を削除できます。最初にアイデンティティ証明書を削除し、その後で CA 証明書を削除します。アイデンティティ証明書を削除したあと、トラスト ポイントから RSA キー ペアの関連付けを解除できます。期限切れまたは失効した証明書、キー ペアが信用できない（または信用できない可能性がある）証明書、または信頼できなくなった CA を除去するには、証明書を削除する必要があります。

手順の詳細

DCNM-SAN を使用して、トラスト ポイントから CA 証明書（または下位 CA のチェーン全体）を削除する手順は、次のとおりです。

ステップ 1　[Physical Attributes] ペインで、[Switches] > [Security] > [PKI] をクリックします。

ステップ 2　[Information] ペインで [Trust Point Actions] タブをクリックします。

ステップ 3　[Command] ドロップダウン メニューから [cadelete] オプションを選択して、トラスト ポイントからアイデンティティ証明書を削除します。

（注）　削除するアイデンティティ証明書が、デバイスの最後または唯一のアイデンティティ証明書である場合には、**forcecertdelete** 処理を使用して削除する必要があります。これは、管理者が最後または唯一のアイデンティティ証明書を誤って削除し、アプリケーション（IKE および SSH など）で使用する証明書が存在しない状態になるのを防止するためです。

ステップ 4　[Apply Changes] をクリックして、変更を保存します。

アイデンティティ証明書を削除するには、[Trust Point Actions] タブをクリックし、[Command] ドロップダウン メニューから [certdelete] または [forcecertdelete] を選択します。

スイッチからの RSA キー ペアの削除

特定の状況では、スイッチの RSA キー ペアの削除が必要になることがあります。たとえば、何らかの原因で RSA キー ペアの信用性が失われ、もはや使用しない場合には、そのキー ペアを削除すべきです。

手順の詳細

スイッチから RSA キー ペアを削除する手順は、次のとおりです。

ステップ 1　[Physical Attributes] ペインで、[Switches] > [Security] を展開し、[PKI] を選択します。

ステップ 2　[Information] ペインで、[RSA Key-Pair] タブをクリックします。

ステップ 3　[Delete Row] をクリックします。

ステップ 4　[Confirmation] ダイアログボックスで、[Yes] または [No] をクリックします。

（注）　スイッチから RSA キー ペアを削除したあと、CA でそのスイッチの証明書を失効するように、CA 管理者に依頼してください。その証明書を要求した場合には、作成したチャレンジ パスワードを提供する必要があります。「証明書要求の生成」（P.6-11）を参照してください。

設定例

ここでは、Microsoft Windows Certificate サーバを使用して、Cisco MDS 9000 ファミリ スイッチ上に証明書および CRL を設定するための作業例を示します。

ここで説明する内容は、次のとおりです。

MDS スイッチでの証明書の設定

MDS スイッチで証明書を設定する手順は、次のとおりです。

ステップ 1　[Switches] を選択し、[LogicalName] フィールドでスイッチのホスト名を設定します。

ステップ 2　[Switches] > [Interfaces] > [Management] > [DNS] を選択し、[DefaultDomainName] フィールドを設定します。

ステップ 3　次の手順で、スイッチの RSA キー ペアを作成します。

a. [Switches] > [Security] > [PKI] を選択し、[RSA Key-Pair] タブを選択します。

b. [Create Row] をクリックし、名前とサイズのフィールドを設定します。

c. [Exportable] チェックボックスをクリックし、[Create] をクリックします。

ステップ 4　次の手順で、トラスト ポイントを作成し、RSA キー ペアを関連付けます。

a. [Switches] > [Security] > [PKI] を選択し、[Trustpoints] タブを選択します。

b. [Create Row] をクリックし、[TrustPointName] フィールドを設定します。

c. [KeyPairName] ドロップダウン メニューから RSA キー ペアを選択します。

d. [CARevoke] ドロップダウン メニューから、証明書失効方式を選択します。

e. [Create] をクリックします。

ステップ 5　[Switches] > [Copy Configuration] を選択し、[Apply Changes] をクリックして、実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーし、トラスト ポイントとキー ペアを保存します。

ステップ 6　トラスト ポイント CA として追加する CA から、CA 証明書をダウンロードします。

ステップ 7　次の手順で、トラスト ポイントに登録する CA を認証します。

a. Device Manager を使用して、[Admin] > [Flash Files] を選択し、[Copy] を選択して、CA 証明書をブートフラッシュに tftp でコピーします。

b. DCNM-SAN を使用して、[Switches] > [Security] > [PKI] を選択し、[TrustPoint Actions] タブを選択します。

c. [Command] ドロップダウン メニューから、[cauth] を選択します。

d. URL フィールドで [...] をクリックし、ブートフラッシュから CA 証明書を選択します。

e. [Apply Changes] をクリックして、トラスト ポイントに登録する CA を認証します。

f. [Information] ペインで [Trust Point Actions] タブをクリックします。

g. トラスト ポイント行の [IssuerCert FingerPrint] カラムの表示から、確認する CA 証明書のフィンガープリントを書き留めます。CA 証明書のフィンガープリントと、CA から通知された（CA の Web サイトから取得した）フィンガープリントを比較します。フィンガープリントが正確に一致していれば、トラスト ポイントの **certconfirm** 処理を実行して、CA を受け入れます。一致していない場合は、トラスト ポイントの **certnoconfirm** 処理を実行して、CA を拒否します。

h. ステップ g で [certconfirm] を選択した場合には、[Trust Point Actions] タブをクリックし、[Command] ドロップダウン メニューから [certconfirm] を選択して、[Apply Changes] をクリックします。

i. ステップ g で [certnoconfirm] を選択した場合には、[Trust Point Actions] タブをクリックし、[Command] ドロップダウン メニューから [certconfirm] を選択して、[Apply Changes] をクリックします。

ステップ 8　次の手順で、トラスト ポイントに登録させるための証明書要求を生成します。

a. [Information] ペインで [Trust Point Actions] タブをクリックします。

b. [Command] ドロップダウン メニューから、[certreq] を選択します。このトラスト ポイント エントリに対応する CA のアイデンティティ証明書を取得するために必要な PKCS#10 証明書署名要求（CSR）が生成されます。

c. 生成した証明書要求を保管する出力ファイル名を入力します。bootflash:filename 形式で指定する必要があります。このファイルに、生成した CSR が PEM 形式で保管されます。

d. CSR に含める *チャレンジ* パスワードを入力します。チャレンジ パスワードは、設定には保存されません。このパスワードは、証明書を失効する必要がある場合に要求されるので、パスワードを覚えておく必要があります。

e. [Apply Changes] をクリックして、変更を保存します。

ステップ 9　CA にアイデンティティ証明書を要求します。

（注） アイデンティティ証明書が発行される前に、CA から手動での確認が要求されることがあります。

ステップ 10　次の手順で、アイデンティティ証明書をインポートします。

a. Device Manager を使用して、[Admin] > [Flash Files] を選択し、[Copy] を選択して、CA 証明書をブートフラッシュに tftp でコピーします。

b. DCNM-SAN を使用して、[Switches] > [Security] > [PKI] を選択し、[TrustPoint Actions] タブをクリックします。

c. [Command] ドロップダウン メニューから [certimport] オプションを選択して、このトラスト ポイントにアイデンティティ証明書をインポートします。

（注） アイデンティティ証明書は、ブートフラッシュ内に PEM 形式のファイルで保存されている必要があります。

d. URL フィールドに、ブートフラッシュにコピーした証明書ファイルの名前を、bootflash:filename 形式で入力します。

e. [Apply Changes] をクリックして変更を保存します。

正常に実行されると、アイデンティティ証明書の値、および証明書のファイル名などの関連オブジェクトが、アイデンティティ証明書内の対応する属性に応じて、適切な値に自動的に更新されます。

CA 証明書のダウンロード

Microsoft Certificate Service の Web インターフェイスから CA 証明書をダウンロードする手順は、次のとおりです。

ステップ 1　Microsoft Certificate Services Web インターフェイスの [Retrieve the CA certificate or certificate revocation task] オプション ボタンを選択し、[Next] ボタンをクリックします。

ステップ 2　表示されたリストから、ダウンロードする CA 証明書ファイルを選択します。[Base 64 encoded] オプション ボタンをクリックし、[Download CA certificate] リンクをクリックします。

ステップ 3　[File Download] ダイアログボックスで、[Open] ボタンをクリックします。

ステップ 4　[Certificate] ダイアログボックスで [Copy to File] ボタンをクリックし、[OK] をクリックします。

ステップ 5　[Certificate Export Wizard] ダイアログボックスで [Base-64 encoded X.509 (CER)] を選択し、[Next] をクリックします。

ステップ 6　[Certificate Export Wizard] ダイアログボックスの [File name:] テキスト ボックスに宛先ファイル名を入力し、[Next] をクリックします。

ステップ 7　[Certificate Export Wizard] ダイアログボックスの [Finish] ボタンをクリックします。

ステップ 8　Microsoft Windows の **type** コマンドを使用して、Base-64（PEM）形式で保存されている CA 証明書を表示します。

アイデンティティ証明書の要求

PKCS#10 CRS を使用して Microsoft Certificate サーバにアイデンティティ証明書を要求する手順は、次のとおりです。

ステップ 1　Microsoft Certificate Services Web インターフェイス上の [Request a certificate] オプション ボタンを選択し、[Next] ボタンをクリックします。

ステップ 2　[Advanced Request] オプション ボタンを選択し、[Next] ボタンをクリックします。

ステップ 3　[Submit a certificate request using a base64 encoded PKCS#10 file or a renewal request using a base64 encoded PKCS#7 file] オプション ボタンを選択し、[Next] ボタンをクリックします。

ステップ 4　[Saved Request] テキスト ボックスに base64 PKCS#10 証明書要求をペーストし、[Next] をクリックします。

MDS スイッチのコンソールから、証明書要求がコピーされます（「証明書要求の生成」（P.6-11）および「MDS スイッチでの証明書の設定」（P.6-16）を参照）。

ステップ 5　CA アドミニストレータから証明書が発行されるまで、1 ～ 2 日間待ちます。

ステップ 6　CA 管理者により証明書要求が承認されます。

ステップ 7　Microsoft Certificate Services Web インターフェイス上の [Check on a pending certificate] オプション ボタンを選択し、[Next] ボタンをクリックします。

ステップ 8　確認する証明書要求を選択し、[Next] をクリックします。

ステップ 9　[Base 64 encoded] を選択し、[Download CA certificate] リンクをクリックします。

ステップ 10　[File Download] ダイアログボックスで、[Open] をクリックします。

ステップ 11　[Certificate] ダイアログボックスで [Details] タブをクリックし、[Copy to File] ボタンをクリックします。[Certificate Export Wizard] ダイアログボックスで [Base-64 encoded X.509 (.CER)] オプション ボタンを選択し、[Next] ボタンをクリックします。

ステップ 12　[Certificate Export Wizard] ダイアログボックスの [File name:] テキスト ボックスに宛先ファイル名を入力し、[Next] をクリックします。

ステップ 13　[Finish] をクリックします。

ステップ 14　Microsoft Windows の **type** コマンドを使用して、base-64 符号化形式のアイデンティティ証明書を表示します。

証明書の失効

Microsoft CA 管理者プログラムを使用して証明書を取り消す手順は、次のとおりです。

ステップ 1　Certification Authority ツリーで、**Issued Certificates** フォルダをクリックします。リストから、失効させる証明書を右クリックします。

ステップ 2　[All Tasks] > [Revoke Certificate] を選択します。

ステップ 3　[Reason code] ドロップダウン リストから失効の理由を選択し、[Yes] をクリックします。

ステップ 4　[Revoked Certificates] フォルダをクリックして、証明書の取り消しを表示および確認します。

CRL の生成および公開

Microsoft CA 管理者プログラムを使用して CRL を作成および公開する手順は、次のとおりです。

ステップ 1　[Certification Authority] 画面で、[Action] > [All Tasks] > [Publish] を選択します。

ステップ 2　[Certificate Revocation List] ダイアログボックスで [Yes] をクリックし、最新の CRL を公開します。

CRL のダウンロード

Microsoft 社の CA の Web サイトから CRL をダウンロードする手順は、次のとおりです。

ステップ 1　Microsoft Certificate Services Web インターフェイス上の [Request the CA certificate or certificate revocation list] オプション ボタンを選択し、[Next] ボタンをクリックします。

ステップ 2　[Download latest certificate revocation list] リンクをクリックします。

ステップ 3　[File Download] ダイアログボックスで、[Save] をクリックします。

ステップ 4　[Save As] ダイアログボックスに宛先ファイル名を入力し、[Save] をクリックします。

ステップ 5　Microsoft Windows の **type** コマンドを使用して、CRL を表示します。

CRL のインポート

CRL を CA に対応するトラストポイントにインポートする手順は、次のとおりです。

ステップ 1　[Physical Attributes] ペインで、[Switches] > [Security] > [PKI] をクリックします。

ステップ 2　[Information] ペインで [Trust Point Actions] タブをクリックします。

ステップ 3　[Command] ドロップダウン メニューから [crlimport] オプションを選択して、選択したトラスト ポイントに CRL をインポートします。

ステップ 4　URL フィールドに、CRL の入力ファイル名を bootflash:filename 形式で入力します。

ステップ 5　[Apply Changes] をクリックして、変更を保存します。

（注）　失効しているスイッチのアイデンティティ証明書（シリアル番号 0A338EA1000000000074）は、最後にリストされます