

# PKI の設定

この章の内容は、次のとおりです。

- PKIの概要, 1 ページ
- PKIのライセンス要件, 6 ページ
- PKIの注意事項と制約事項, 6 ページ
- PKIのデフォルト設定, 7 ページ
- CA の設定とデジタル証明書, 7 ページ
- PKIの設定の確認, 23 ページ
- PKIの設定例, 24 ページ

# **PKI**の概要

ここでは、PKIについて説明します。

## CAとデジタル証明書

証明機関(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、各デバイスやユーザはキーペアを持ち、こ れには秘密キーと公開キーが含まれています。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。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。署名は、送信者の秘密キー を使用してデータを暗号化したときに作成されます。受信側は、送信側の公開キーを使用してメッ セージを復号化することで、シグニチャを検証します。このプロセスは、受信者が送信者の公開 キーのコピーを持っていて、これが本当に送信者のものであり、送信者を騙る他人のものではないことを高い確実性を持って知っていることを基盤としています。

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、名前、 シリアル番号、企業、部署またはIPアドレスなど、ユーザまたはデバイスを特定する情報を含ん でいます。また、エンティティの公開キーのコピーも含んでいます。証明書に署名する CA は、 受信者が明示的に信頼する第三者機関であり、アイデンティティの正当性を立証し、デジタル証 明書を作成します。

CAのシグニチャを検証するには、受信者は、CAの公開キーを認識している必要があります。一般的にはこのプロセスはアウトオブバンドか、インストール時に行われる操作によって処理されます。たとえば、通常のWebブラウザでは、デフォルトで、複数のCAの公開キーが設定されています。

## 信頼モデル、トラストポイント、アイデンティティCA

PKIの信頼モデルは、設定変更が可能な複数の信頼できる CA によって階層化されています。信頼できる CA のリストを使用して各参加デバイスを設定して、セキュリティ プロトコルの交換の際に入手したピアの証明書がローカルに信頼できる CA のいずれかで発行されていた場合には、これを認証できるようにすることができます。Cisco NX-OS ソフトウェアでは、信頼できる CA の自己署名ルート証明書(または下位 CA の証明書チェーン)をローカルに保存しています。信頼できる CA のルート証明書(または下位 CA の場合には全体のチェーン)を安全に入手するプロセスを、CA 認証と呼びます。

信頼できるCAについて設定された情報をトラストポイントと呼び、CA自体もトラストポイント CAと呼びます。この情報は、CA証明書(下位CAの場合は証明書チェーン)と証明書取消確認 情報で構成されています。

Cisco NX-OS デバイスは、トラストポイントに登録して、アイデンティティ証明書を入手し、キーペアと関連付けることができます。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 のキーペアとアイデンティティ証明書

アイデンティティ証明書を入手するには、1つまたは複数のRSAキーペアを作成し、各RSAキーペアとCiscoNX-OSデバイスが登録しようとしているトラストポイントCAを関連付けます。Cisco NX-OSデバイスは、CAごとにアイデンティティを1つだけ必要とします。これはCAごとに1 つのキーペアと1つのアイデンティティ証明書で構成されています。

Cisco NX-OS ソフトウェアでは、設定変更が可能なキーのサイズ(またはモジュラス)で RSA キーペアを作成できます。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、デバイスの完全修飾ドメイン名(FQDN)です。

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係を要約したものを次に 示します。

トラストポイントとは、Cisco NX-OS デバイスが、あらゆるアプリケーション(SSH など)のピア証明書用に信頼する特定のCAです。

- Cisco NX-OS デバイスは多数のトラストポイントを持つことができ、デバイス上のすべての アプリケーションがあらゆるトラストポイントCAで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。
- Cisco NX-OS デバイスは、トラストポイントに対応する CA に登録して、アイデンティティ 証明書を入手します。デバイスは複数のトラストポイントに登録できます。これは、各トラ ストポイントから異なるアイデンティティ証明書を入手できることを意味します。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、証明書の拡張機能として証明書に保存されます。
- トラストポイントに登録するときには、証明を受ける 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作成されていて、トラストポイントに関連付けられている必要があります。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との間のアソシエーション(関連付け)は、証明書、キーペア、またはトラストポイントが削除されて明示的になくなるまで有効です。
- •アイデンティティ証明書のサブジェクト名は、Cisco NX-OS デバイスの完全修飾ドメイン名です。
- デバイス上には1つまたは複数のRSAキーペアを作成でき、それぞれを1つまたは複数のトラストポイントに関連付けることができます。しかし、1つのトラストポイントに関連付けられるキーペアは1だけです。これは1つのCAからは1つのアイデンティティ証明書しか入手できないことを意味します。
- Cisco NX-OS デバイスが複数のアイデンティティ証明書を(それぞれ別の CA から)入手す る場合は、アプリケーションがピアとのセキュリティプロトコルの交換で使用する証明書 は、アプリケーション固有のものになります。
- 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。
- ある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入手したり、ある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。ある CA はあるアイデンティティ(または名前)を1回だけ証明し、同じ名前で複数の証明書を発行することはありません。ある CA から複数のアイデンティティ証明書を入手する必要があり、またその CA が同じ名前で複数の証明書の発行を許可している場合は、同じ CA 用の別のトラストポイントを定義して、別のキーペアを関連付け、証明を受ける必要があります。

## 複数の信頼できる CA のサポート

Cisco NX-OS デバイスは、複数のトラストポイントを設定して、それぞれを別の CA に関連付け ることにより、複数の CA を信頼できるようになります。信頼できる CA が複数あると、ピアに 証明書を発行した特定の CA にデバイスを登録する必要がなくなります。代わりに、ピアが信頼 する複数の信頼できる CA をデバイスに設定できます。すると、Cisco NX-OS デバイスは設定さ れている信頼できる CA を使用して、ピアから受信した証明書で、ピアデバイスの ID で定義され ている CA から発行されたものではないものを検証できるようになります。

## PKIの登録のサポート

登録とは、SSH などのアプリケーションに使用するデバイス用のアイデンティティ証明書を入手 するプロセスです。これは、証明書を要求するデバイスと、認証局の間で生じます。

Cisco NX-OS デバイスでは、PKI 登録プロセスを実行する際に、次の手順を取ります。

- ・デバイスでRSAの秘密キーと公開キーのペアを作成します。
- ・標準の形式で証明書要求を作成し、CAに送ります。

(注)

要求が CA で受信されたとき、CA サーバでは CA アドミニストレータが登録要求を手動で承認しなくてはならない場合があります。

- •発行された証明書を CA から受け取ります。これは CA の秘密キーで署名されています。
- ・デバイスの不揮発性のストレージ領域(ブートフラッシュ)に証明書を書き込みます。

## カットアンドペーストによる手動での登録

Cisco NX-OS ソフトウェアでは、手動でのカットアンドペーストによる証明書の取得と登録をサ ポートしています。カットアンドペーストによる登録とは、証明書要求をカットアンドペースト して、デバイスと CA 間で認証を行うことを意味します。

手動による登録プロセスでカットアンドペーストを使用するには、次の手順を実行する必要があ ります。

- 証明書登録要求を作成します。これはCisco NX-OS デバイスで base64 でエンコードされたテキスト形式として表示されます。
- エンコードされた証明書要求のテキストをEメールまたはWebフォームにカットアンドペーストし、CAに送ります。
- 発行された証明書(base64 でエンコードされたテキスト形式)をCAからEメールまたは Webブラウザによるダウンロードで受け取ります。
- ・証明書のインポート機能を使用して、発行された証明書をデバイスにカットアンドペースト します。

# 複数の RSA キー ペアとアイデンティティ CA のサポート

複数のアイデンティティ CA を使用すると、デバイスが複数のトラストポイントに登録できるようになり、その結果、別々の CA から複数のアイデンティティ証明書が発行されます。この機能によって、Cisco NX-OS デバイスは複数のピアを持つ SSH およびアプリケーションに、これらの ピアに対応する CA から発行された証明書を使用して参加できるようになります。 また複数の RSA キーペアの機能を使用すると、登録している各 CA ごとの別々のキーペアをデバイスで持てるようになります。これは、他の CA で指定されているキーの長さなどの要件と競合することなく、各 CA のポリシー要件に適合させることができます。デバイスでは複数の RSA キーペアを作成して、各キーペアを別々のトラストポイントに関連付けることができます。したがって、トラストポイントに登録するときには、関連付けられたキーペアを証明書要求の作成に使用します。

## ピア証明書の検証

PKIでは、Cisco NX-OS デバイスでのピア証明書の検証機能をサポートしています。Cisco NX-OS ソフトウェアでは、SSH などのアプリケーションのためのセキュリティ交換の際にピアから受け 取った証明書を検証します。アプリケーションはピア証明書の正当性を検証します。Cisco NX-OS ソフトウェアでは、ピア証明書の検証の際に次の手順を実行します。

- ・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。

取消確認については、Cisco NX-OS ソフトウェアでは証明書失効リスト(CRL)をサポートしています。トラストポイント CA ではこの方法を使用して、ピア証明書が取り消されていないことを確認できます。

## 証明書の取消確認

Cisco NX-OS ソフトウェアでは、CA 証明書の取消のステータスを確認できます。アプリケーションでは、指定した順序に従って取消確認メカニズムを使用できます。選択肢には、CRL、none、これらの方式の組み合わせがあります。

### CRLのサポート

CAでは証明書失効リスト(CRL)を管理して、有効期限前に取り消された証明書についての情報 を提供します。CAではCRLをリポジトリで公開して、発行したすべての証明書の中にダウンロー ド用の公開 URL 情報を記載しています。ピア証明書を検証するクライアントは、発行した CAか ら最新の CRL を入手して、これを使用して証明書が取り消されていないかどうかを確認できま 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 NX-OS ソフトウェアでは、先にダウンロードしたトラストポイントについての CRL を手動 で設定して、これをデバイスのブートフラッシュ(cert-store)にキャッシュすることができます。 ピア証明書の検証の際、Cisco NX-OS ソフトウェアは、CRL がすでにローカルにキャッシュされ ていて、取消確認でこの CRL を使用するよう設定されている場合にだけ、発行した CA からの CRL をチェックします。それ以外の場合、Cisco NX-OS ソフトウェアでは CRL チェックを実行せ ず、他の取消確認方式が設定されている場合を除き、証明書は取り消されていないと見なします。

## 証明書と対応するキーペアのインポートとエクスポート

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。このファイルは、後で同じデバイス(システムクラッシュ の後など)や交換したデバイスににインポートすることができます。PKCS#12ファイル内の情報 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)で構成され ています。

# PKI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。

製品	ライセンス要件
Cisco NX-OS	PKI機能にはライセンスは必要ありません。ラ イセンスパッケージに含まれていない機能はす べて Cisco NX-OS システムイメージにバンドル されており、追加費用は一切発生しません。 Cisco NX-OS ライセンス方式の詳細については、 『Cisco NX-OS Licensing Guide』を参照してくだ さい。

# PKIの注意事項と制約事項

PKIに関する注意事項と制約事項は次のとおりです。

- ・Cisco NX-OS デバイスに設定できるキーペアの最大数は16です。
- Cisco NX-OS デバイスで宣言できるトラストポイントの最大数は16です。
- ・Cisco NX-OS デバイスに設定できるアイデンティティ証明書の最大数は 16 です。
- ・CA証明書チェーン内の証明書の最大数は10です。
- ・ある CA に対して認証できるトラストポイントの最大数は 10 です。
- ・設定のロールバックでは PKI の設定はサポートしていません。
- Cisco NX-OS ソフトウェアでは、OSCP をサポートしていません。



Cisco IOS の CLI に慣れている場合、この機能に対応する Cisco NX-OS コマンドは通常使用する Cisco IOS コマンドと異なる場合があるので注意してください。

# PKI のデフォルト設定

次の表に、PKI パラメータのデフォルト設定を示します。

表1: PKI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	デバイスの 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	イネーブル
取消確認方式	CRL

# CAの設定とデジタル証明書

ここでは、Cisco NX-OS デバイス上で CA とデジタル証明書が相互に連携して動作するようにするために、実行が必要な作業について説明します。

## ホスト名とIPドメイン名の設定

デバイスのホスト名または IP ドメイン名をまだ設定していない場合は、設定する必要がありま す。これは、Cisco NX-OS ソフトウェアでは、アイデンティティ証明書のサブジェクトとして完 全修飾ドメイン名(FQDN)を使用するためです。また、Cisco NX-OS ソフトウェアでは、キーの 作成の際にラベルが指定されていないと、デバイスの FQDN をデフォルトのキーラベルとして使 用します。たとえば、DeviceA.example.com という名前の証明書は、DeviceA というデバイスのホ スト名と example.com というデバイスの IP ドメイン名に基づいています。

注意 証明書を作成した後にホスト名またはIPドメイン名を変更すると、証明書が無効になります。

	コマンドまたはアクション	目的
ステップ1	<b>configure terminal</b> 例: switch# configure terminal switch(config)#	グローバル コンフィギュレーションモー ドを開始します。
ステップ <b>2</b>	hostnamehostname 例: switch(config)# hostname DeviceA	デバイスのホスト名を設定します。
ステップ3	ip domain-namename [use-vrfvrf-name] 例: DeviceA(config)# ip domain-name example.com	デバイスの IP ドメイン名を設定します。 VRF 名が指定されていないと、このコマ ンドではデフォルトの VRF を使用しま す。
ステップ4	exit 例: switch(config)# exit switch#	設定モードを終了します。
ステップ5	show hosts 例: switch# show hosts	(任意) ⅠP ドメイン名を表示します。
ステップ 6	<pre>copy running-config startup-config の : switch# copy running-config startup-config</pre>	<ul> <li>(任意)</li> <li>実行コンフィギュレーションを、スター</li> <li>トアップコンフィギュレーションにコピー</li> <li>します。</li> </ul>

#### 手順

# RSA キーペアの生成

RSA キー ペアは、アプリケーション向けのセキュリティ プロトコルの交換時に、セキュリティ ペイロードの署名、暗号化、および復号化のために作成します。デバイスのための証明書を取得 する前に、RSA キー ペアを作成する必要があります。

Γ

	コマンドまたはアクション	目的
ステップ1	<b>configure terminal</b> 例: switch# configure terminal switch(config)#	グローバルコンフィギュレーションモードを開始し ます。
ステップ <b>2</b>	crypto key generate rsa         [label/abel-string] [exportable]         [modulussize]         例:         switch(config)# crypto key         generate rsa exportable	<ul> <li>RSA キーペアを生成します。デバイスに設定できる キーペアの最大数は16です。</li> <li>ラベル文字列には、大文字と小文字を区別して、最 大64文字の英数字で値を指定します。デフォルトの ラベル文字列は、ピリオド文字(.) で区切ったホス ト名と FQDN です。</li> <li>有効なモジュラスの値は512、768、1024、1536、お よび2048です。デフォルトのモジュラスのサイズは 512です。</li> <li>(注) 適切なキーのモジュラスを決定する際に は、Cisco NX-OS デバイスと CA(登録を 計画している対象)のセキュリティポリ シーを考慮する必要があります。</li> <li>デフォルトでは、キーペアはエクスポートできません。エクスポート可能なキーペアだけ、PKCS#12形 式でエクスポートできます。</li> <li>注意 キーペアのエクスポートの可否は変更でき ません。</li> </ul>
ステップ3	exit 例: switch(config)# exit switch#	設定モードを終了します。
ステップ4	<pre>show crypto key mypubkey rsa 例: switch# show crypto key mypubkey rsa</pre>	(任意) 作成したキーを表示します。
ステップ5	copy running-config startup-config         例:         switch# copy running-config startup-config	(任意) 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ます。

# トラストポイント CA のアソシエーションの作成

Cisco NX-OS デバイスとトラストポイント CA を関連付ける必要があります。

### はじめる前に

RSA キーペアを作成します。

	コマンドまたはアクション	目的
ステップ1	<pre>configure terminal 例: switch# configure terminal switch(config)#</pre>	グローバル コンフィギュレーションモードを開 始します。
ステップ <b>2</b>	<pre>crypto ca trustpointname 例: switch(config)# crypto ca trustpoint admin-ca switch(config-trustpoint)#</pre>	<ul> <li>デバイスが信頼するトラストポイント CA を宣言し、トラストポイントコンフィギュレーションモードを開始します。</li> <li>(注) デバイスに設定できるトラストポイントの最大数は 16 です。</li> </ul>
ステップ3	enrollment terminal 例: switch(config-trustpoint)# enrollment terminal	<ul> <li>手動でのカットアンドペーストによる証明書の</li> <li>登録をイネーブルにします。デフォルトではイ</li> <li>ネーブルになっています。</li> <li>(注) Cisco NX-OS ソフトウェアでは、手動</li> <li>でのカットアンドペースト方式による</li> <li>証明書の登録だけをサポートしています。</li> </ul>
ステップ4	rsakeypairlabel 例: switch(config-trustpoint)# rsakeypair SwitchA	<ul> <li>RSA キーペアのラベルを指定して、このトラストポイントを登録用に関連付けます。</li> <li>(注) CA ごとに1つの RSA キーペアだけを指定できます。</li> </ul>
ステップ5	exit 例: switch(config-trustpoint)# exit switch(config)#	トラストポイントコンフィギュレーションモー ドを終了します。
 ステップ6	<pre>show crypto ca trustpoints 例: switch(config)# show crypto ca trustpoints</pre>	(任意) トラストポイントの情報を表示します。

	コマンドまたはアクション	目的
ステップ <b>1</b>	copy running-config startup-config	(任意)
		実行コンフィギュレーションを、スタートアッ
	例: switch(config)# copy running-config startup-config	プ コンフィギュレーションにコピーします。

#### CA の認証

CA が Cisco NX-OS デバイスに対して認証されると、CA を信頼するプロセスの設定が完了しま す。まず、PEM 形式の CA の自己署名証明書を入手し、Cisco NX-OS デバイスを CA に対して認 証する必要があります。この証明書には、CA の公開キーが含まれています。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。



認証する CA が他の CA の下位 CA である場合、認証する CA は自己署名 CA ではありません。 その上位の CA がさらに別の CA の下位である場合もあります。最終的には自己署名 CA に到 達します。このタイプの CA 証明書を、認証する CA の CA 証明書チェーンと呼びます。この 場合は、CA 認証の際に、証明書チェーン内のすべての 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。CA 証明書チェーン内の証明書の最大数は 10 です。

#### はじめる前に

CA とのアソシエーションを作成します。

CA 証明書または CA 証明書チェーンを入手します。

	コマンドまたはアクション	目的
ス テッ プ1	<b>configure terminal</b> 例: switch# configure terminal switch(config)#	グローバル コンフィ ギュレーション モー ドを開始します。
ス テッ プ2	<pre>crypto ca authenticatename 例: switch(config)# crypto ca authenticate admin-ca input (cut &amp; paste) CA certificate (chain) in PEM format; end the input with a line containing only END OF INPUT :BEGIN CERTIFICATE MIIC4jCCAoygAwIBAgIQBWDSiay0GZRPSRIljK0ZejANBgkqhkiG9w0BAQUFADCB kDEgMB4GCSqGSIb3DQEJARYRYW1hbmRrZUBjaXNjby5jb20xCzAJBgNVBAYTAkl0</pre>	CAの証明書をカット アンドペーストする ようプロンプトが表 示されます。CAを宣 言したときに使用し た名前と同じ名前を 使用します。

٦

	コマンドまたはアクション	目的
	<pre>MRIwEAYDVQQIEwlLYXJuYXRha2ExEjAQBgNVBAcTCUJhbmdhbG9yZTEOMAwGA1UE ChMFQ21z728xEzARBgNVBAsTCn51dHN0b3JhZ2UxEjAQBgNVBAMTCUFWXJuYSBD QTAeFw0wNTA1MDMyMjQ2MzdFW0WL2AINDMyMjUUMTdamlGQMSAwHgYXKOZIhucN AQkBFhFhbWFuZGtlQGNpc2NvLmNvbTELMAkGA1UEBhMCSU4xEjAQBgNVBAgTCUth cm5hdGFrYTESMBAGA1UEBxMJQmFuZ2Fsb3JlMQ4wDAYDVQQKEwVDAXNjbzETMBEG AlUECXMKhnV0.3FvcmFnZTESMBAGA1UEBxMJQXBhcm5h1ENBMFwwDQYXKOZIhucN AQEBBQADSwAwSAJBAMW/7b3+DXJPANBsIHHz1uNccNM87ypyzwuoSNZXOMpeRXXI OzyBAgiXT2ASFuUOwQ1iDM&amp;rO/41jf8RxvYKvysCAWEAAaOBvzCEVDALEgNYHQ8E BAMCAcYwDvYDKOTAQH/BAUWAWEB/zAdBgNVHQ4EFgQUJyjKoMbrCNMRU2OyRhQ GgsWbHEwawYDVROfBGQwYjAuoCygKoYoaHR0CDouL3NzZS0wOC9DZXJORW5yb2xs L0FwYXJuYSUJMENBLmNybDAwoC6gLIYqZm1sZTovL1xcc3NL1FA4KEN1cnRFbnJv b6xcQXBhcm5hJTIwQOEuY3JsMBAGCSsGAQQBgjcVAQQDAgEAMA0GCSqGSIB3DQEB BQUAA0EAHv6UQ+8nE399Tww+KaGr0gONIJaqNgLh0AFcTOrEyuyt/WYGPzksF9Ea NBG7E0oN66zex0EOEfGlVs6mXp1//w== END CERTIFICATE END OF INPUT Fingerprint(s): MD5 Fingerprint=65:84:9A:27:D5:71:03:33:9C:12:23:92:38:6F:78:12 Do you accept this certificate? [yes/no]: yes</pre>	ある CA に対して認 証でです。 (注) 下位 CA の 認です。 (注) 下位 CA の 認です。 (注) 下位 CA の 認定の NX-OS ソ フトウェ自 名 CA に 到 この の た の に い の の ま の た い た の た の た の た の た の た の た の た の た の た の た の た の た の の し の の し の の の し の の の の い い の の の の し の の の の い い の の の い い の の い い の の い い の の の の の い い の の い い の の い い の の い い の つ た い の の い い の っ い て の た の こ の の い い の っ い い の っ い の た の こ の の の た い の の た の こ の の い い か い い の た の た の こ の の し に の う い の た の た の た の た の た の た の に の の の た い の い の い む い の し に の た の い の い い い い か い い の い い た の い の い い い の い い の い い の い の い の い の い の い の い の い の い し い い の い い の い い の い の い の い の い の い の い の っ い い つ い い の っ い っ い っ い い っ い っ い っ い っ い の っ い っ い っ い っ い っ い の っ い の っ い の っ い の っ い つ い っ い つ い っ い の っ い っ い っ い っ い つ つ つ い つ つ い つ つ つ つ い つ つ い つ つ い つ つ い つ つ い つ つ つ つ い つ つ つ つ い つ つ い つ つ つ い つ つ つ い い つ い つ い つ い つ い つ つ つ い つ い つ い つ い つ い つ い い つ い つ い つ つ つ い つ つ つ い こ い つ つ つ つ つ つ い つ つ つ つ つ つ つ こ つ つ つ つ つ つ つ つ つ つ つ つ つ
ス テッ プ <b>3</b>	exit 例:	設定モードを終了し ます。
	<pre>switch(config)# exit switch#</pre>	
ス テッ プ 4	show crypto ca trustpoints 例: switch# show crypto ca trustpoints	<ul><li>(任意)</li><li>トラストポイントCA</li><li>の情報を表示します。</li></ul>
ス テッ プ5	copy running-config startup-config 例: switch# copy running-config startup-config	(任意) 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 にコピーします。

ſ

## 証明書取消確認方法の設定

クライアント(SSH ユーザなど)とのセキュリティ交換の際に、Cisco NX-OS デバイスは、クラ イアントから送られたピア証明書の検証を実行します。検証プロセスには、証明書の取消状況の 確認が含まれます。

CAからダウンロードした CRL を確認するよう、デバイスに設定できます。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。しかし、証明書がダ ウンロードとダウンロードの中間で取り消され、デバイス側ではその取り消しに気付かない場合 も考えられます。

### はじめる前に

CA を認証します。

CRL チェックを使用する場合は、CRL が設定済みであることを確認します。

	コマンドまたはアクション	目的
ステップ1	<b>configure terminal</b> 例: switch# configure terminal switch(config)#	グローバルコンフィギュレーションモード を開始します。
ステップ2	crypto ca trustpointname 例: switch(config)# crypto ca trustpoint admin-ca switch(config-trustpoint)#	トラストポイント CA を指定し、トラスト ポイントコンフィギュレーションモードを 開始します。
ステップ3	revocation-check {crl [none]   none} 例: switch(config-trustpoint)# revocation-check none	<ul> <li>証明書取消確認方法を設定します。デフォルト方式は crl です。</li> <li>Cisco NX-OS ソフトウェアでは、指定した順序に従って証明書取消方式を使用します。</li> </ul>
ステップ4	exit 例: switch(config-trustpoint)# exit switch(config)#	トラストポイントコンフィギュレーション モードを終了します。
ステップ5	<pre>show crypto ca trustpoints 例: switch(config)# show crypto ca trustpoints</pre>	(任意) トラストポイントCAの情報を表示します。

	コマンドまたはアクション	目的
ステップ6	copy running-config startup-config	(任意)
		実行コンフィギュレーションを、スタート
	例: switch(config)# copy running-config startup-config	アップコンフィギュレーションにコピーし ます。

# 証明書要求の作成

使用する各デバイスのRSAキーペア用に、対応するトラストポイントCAからアイデンティティ 証明書を入手するために、要求を作成する必要があります。その後、表示された要求をCA宛の EメールまたはWebサイトのフォームにカットアンドペーストします。

### はじめる前に

CAとのアソシエーションを作成します。

CA 証明書または CA 証明書チェーンを入手します。

	コマンドまたはアクション	目的
ステッ プ1	<b>configure terminal</b> 例: switch# configure terminal switch(config)#	グローバルコンフィ ギュレーションモー ドを開始します。
ステッ プ <b>2</b>	<b>crypto ca enroll</b> <i>name</i> 例: switch(config)# crypto ca enroll admin-ca Create the certificate request	認証した CA に対す る証明書要求を作成 します。

	コマンドまたはアクション	目的
	Create a challenge password. You will need to verbally provide this password to the CA Administrator in order to revoke your certificate. For security reasons your password will not be saved in the configuration. Please make a note of it. Password:nbv123 The subject name in the certificate will be: DeviceA.cisco.com Include the switch serial number in the subject name? [yes/no]: no Include an IP address in the subject name [yes/no]: yes ip address:172.22.31.162 The certificate request will be displayed BEGIN CERTIFICATE REQUEST MIIBqzCCARQCAQAWHDEAMBGGAIUEAXMRVMVNYXMtMS5jaXNjby5jb20wgZ&wDQYJ KoZIhvcNAQEBBQADgYOAMIGJAoGBAL8Y1UAJ2NC7jUJ1DVaSMqNIgJ2kt8r141KY 0JC6ManNy4qxk8VeMXZSiLJ4JgTzKWdxbLbKTTysnjuCXGvjb+wj0hEhv/y51T9y P2NJJ8ornqShrvFZgC7ysN/PyMwKcgzhbVpj+rargZvHtGJ3IXTq4WoVkScZxV8S VqyH0vEvAgMBAAGgTzAVBgkqhkiG9w0BCQcxCBMGbmJ2MTIzMDYGCsqGSIb3DQEJ DjEpMCcwJQYDVRORAQH/BBswGYIRVmVnYXMtMS5jaXNjby5jb21HEKwHH6IwDQYJ KoZIhvcNAQEEBQADgYEAkT60KER6Q08nj0sDXZVHSfJZh6K6JtDz3Gkd99G1FWgt PftrNcWUE/pw6HayfQ12T3ecgNwe12d15133YBF2bktExiI6U188nT0jg1XMjja8 8a23bNDpNsM8rklwA6hWkrVL8NUZEFJxqbjfngPNTZacJCUS6ZqKCMetbKytUx0= END CERTIFICATE REQUEST	(注) チジワ記おだこフ設緒さん書消が合こワ入必りまで、スペークでは、この一定にれ。をすあにの一力要まがす。この人必りまでの。このでは、たちの、たちがす。
ステッ プ3	exit 例: switch(config-trustpoint)# exit switch(config)#	トラストポイントコ ンフィギュレーショ ンモードを終了しま す。
ステッ プ4	<pre>show crypto ca certificates 例: switch(config)# show crypto ca certificates</pre>	(任意) CA 証明書を表示し ます。
ステッ プ5	copy running-config startup-config 例: switch(config)# copy running-config startup-config	(任意) 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 にコピーします。

# アイデンティティ証明書のインストール

アイデンティティ証明書は、CAからEメールまたはWebブラウザ経由でbase64でエンコードされたテキスト形式で受信できます。CAから入手したアイデンティティ証明書を、エンコードされたテキストをカットアンドペーストしてインストールする必要があります。

## はじめる前に

CA とのアソシエーションを作成します。

CA 証明書または CA 証明書チェーンを入手します。

	コマンドまたはアクション	目的
ステッ プ1 ステッ	configure terminal 例: switch# configure terminal switch(config)# crypto ca importnamecertificate	グローバル コン フィギュレーション モードを開始しま す。 admin-ca という名前
プ2	<pre>ØJ: switch(config) # crypto ca import admin-ca certificate input (cut &amp; paste) certificate in PEM format: BEGIN CERTIFICATE MIIEADCCA6qgAwIBAgIKCjOO0QAAAAAADANBgkqhkiG9w0BAQUFADCBkDEgMB4G CSqGSIb3DQEJARYRYW1hbmRrZUBjaXNjby5jb20xCzAJBqNVBAYTAk1OMRIwEAYD VQQIEwlLYXJUYXRha2ExEjAQBgNVBACTCUJhbmdhbG9yZTEOMAwGA1UEChMFQ21z Y28xEZARBgNVBASTCm5ldHN0b3Jh22UxEjAQBgNVBAMTCUFWYXJUYSBDQTAeFw0w NTExMTIwMzAyNDBaFw0wNjExMTIwMzEyNDBAMBwxGjAYBgNVBAMTEVZ122FzLTEu Y21zY28uY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC/GNVACdjQu41C dQ1WkjKjSICdpLfK5eJSmNCQujGpzcuKsZPFXjF2UoiyeCYE8y1ncWyx5E08rJ47 glxr42/sI9IRIb/8udU/cj9jSfKK56koa7xWYAu8rDfz8jMCnIM4W1aY/q2q4Gb x7RifdV06uFqFZEgs17/Elash9LxLwIDAQABc4ICEzCCAg&amp;JQYDVRORAQH/BBsw GYIRVmVNYXMtMS5jaXNjby5jb22HBKwWH6IwHQYDVR00BBYEFKCLi+2sspWEfgrR bhWmlVy09jngMIHMBgNVHSMEgcQwgcGAFCco8kaDG6wjTEVNjsKYUBoLFmxxoYGW pIGTMIGQMSAwHgYJKoZIhvcNAQkBFhFhbWFuZGt1QGNpc2NvLmNvbTELMAkGA1UE BhMCSU4xEjAQBgNVBAgTCUthcm5hdGFYTESMBAGA1UEBxMJQWFuZ2Fsb3J1MQ4w DAYDVQQKEwvDaXNjbzETMBEGA1UECxMKbmV0c3RvcmFnZTESMBAGA1UEAxMJQXBh cm5hIENBghAFYNKJrLQZIE9JEiWMrR16MGsGA1UdHwRkMGIwLqAsoCqGKGh0dHA6 Ly9zc2UtMDgvQ2VydEVucm9sbC9BcGFybmE1MjBDQS5jcmwwMKAuoCyGKmZpbGU6 Ly9cXHNzZS0wOFxDZXJORW5yb2xsXEFwYXJuYSUyMENBLmNybDCBigYIKwYBBQUH AQEEfjB8MDSGCCSGAQUFBZAChi9odHRW0i8vc3N1LTA4L0N1cnRFbnJvbGwvc3N1 LTA4X0FwYXJuYSUyMENBLmNydDA9BggFBGEFBQcwAoYxZmlsZTovL1xcc3NLLTA4 XEN1cnRFbnJvbGxcc3N1LTA4X0FwYXJuYSUyMENBLmNydDANBgkqhkiG9w0BAQUF AANBADbGBGsbe7GNLh9xe0TWBNbm24U69ZSUDDCoCUZUUTgrpnTqVpPyejtsyflw E36cIZu4WsExREqxbTk8ycx7V5o= END CERTIFICATE</pre>	のCAに対するアイ デンティティ証明書 をカットアンドペー ストするよう、プロ ンプトが表示されま す。 デバイスに設定でき るアイデンティティ 証明書の最大数は 16です。
ステッ プ <b>3</b>	exit 例: switch(config)# exit switch#	設定モードを終了し ます。

	コマンドまたはアクション	目的
ステッ プ4	show crypto ca certificates 例: switch# show crypto ca certificates	(任意) CA 証明書を表示し ます。
ステッ プ 5	copy running-config startup-config 例: switch# copy running-config startup-config	(任意) 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

トラストポイントの設定が、Cisco NX-OS デバイスのリブート後も維持されていることを確認で きます。

トラストポイントの設定は、通常の Cisco NX-OS デバイスの設定であり、スタートアップコン フィギュレーションに確実にコピーした場合にだけ、システムのリブート後も維持されます。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後は実行コンフィギュレーションを保存して、削除が永続的に 反映されるようにしてください。

トラストポイントに関連付けられた証明書と CRL は、そのトラストポイントがすでにスタート アップ コンフィギュレーションに保存されていれば、インポートした時点で(つまりスタート アップ コンフィギュレーションにコピーしなくても)維持されるようになります。

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、これを外部のサーバ に保存することを推奨します。

(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。

# PKCS 12 形式でのアイデンティティ情報のエクスポート

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。デバイスのシステムクラッシュからの復元の際や、スーパーバイザモジュールの交換 の際には、証明書や RSA キー ペアをインポートすることができます。

(注) エクスポートの URL を指定するときに使用できるのは、bootflash:*filename* という形式だけです。

#### はじめる前に

CA を認証します。

アイデンティティ証明書をインストールします。

	コマンドまたはアクション	目的
ステップ1	configure terminal 例: switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開 始します。
_ ステップ <b>2</b>	crypto ca exportname pkcs12         bootflash:filenamepassword         例:         switch(config)# crypto ca         export admin-ca pkcs12         bootflash:adminid.p12 nbv123	アイデンティティ証明書と、トラストポイント CAの対応するキーペアとCA証明書をエクス ポートします。パスワードには、大文字と小文字 を区別して、最大128文字の英数字で値を指定し ます。
	exit 例: switch(config)# exit switch#	設定モードを終了します。
ステップ4	copy booflash:filenamescheme://server/ [url/]filename 例: switch# copy bootflash:adminid.p12 tftp:adminid.p12	PKCS#12形式のファイルをリモートサーバにコ ピーします。 scheme引数として、tftp:、ftp:、scp:、またはsftp: を指定できます。server引数は、リモートサーバ のアドレスまたは名前であり、url 引数はリモー トサーバにあるソースファイルへのパスです。 server、url、およびfilenameの各引数は、大文字 小文字を区別して入力します。

コマンドまたはアクション

目的

# PKCS 12 形式でのアイデンティティ情報のインポート

デバイスのシステムクラッシュからの復元の際や、スーパーバイザモジュールの交換の際には、 証明書や RSA キー ペアをインポートすることができます。

(注)

ſ

インポートのURLを指定するときに使用できるのは、bootflash:filenameという形式だけです。

## はじめる前に

CA 認証によってトラストポイントに関連付けられている RSA キー ペアがないこと、およびトラ ストポイントに関連付けられている CA がないことを確認して、トラストポイントが空であるよ うにします。

	コマンドまたはアクション	目的
ステップ1	<b>copy</b> scheme://server/[url/]filename <b>bootflash</b> :filename	PKCS#12 形式のファイルをリモー ト サーバからコピーします。
	例: switch# copy tftp:adminid.p12 bootflash:adminid.p12	<i>scheme</i> 引数として、 <b>tftp:</b> 、 <b>ftp:</b> 、 <b>scp:</b> 、または <b>sftp:</b> を指定できます。 <i>server</i> 引数は、リモートサーバのア ドレスまたは名前であり、 <i>url</i> 引数 はリモートサーバにあるソース ファイルへのパスです。 <i>server、url</i> 、および <i>filename</i> の各引 数は、大文字小文字を区別して入力 します。
ステップ2	<b>configure terminal</b> 例: switch# configure terminal switch(config)#	グローバル コンフィギュレーショ ン モードを開始します。
ステップ3	<pre>crypto ca importnamepksc12 bootflash:filename 例: switch(config)# crypto ca import admin-ca pkcs12 bootflash:adminid.p12 nbv123</pre>	アイデンティティ証明書と、トラス トポイント CA の対応するキー ペ アと CA 証明書をインポートしま す。

	コマンドまたはアクション	目的
ステップ4	exit	設定モードを終了します。
	例: switch(config)# exit switch#	
ステップ5	show crypto ca certificates 例: switch# show crypto ca certificates	(任意) CA 証明書を表示します。
ステップ6	copy running-config startup-config 例: switch# copy running-config startup-config	<ul> <li>(任意)</li> <li>実行コンフィギュレーションを、ス</li> <li>タートアップコンフィギュレーションにコピーします。</li> </ul>

# CRL の設定

トラストポイントからダウンロードした CRL を手動で設定することができます。Cisco NX-OS ソフトウェアでは、CRL をデバイスのブートフラッシュ(cert-store)にキャッシュします。ピア証明書の検証の際、Cisco NX-OS ソフトウェアが発行した CA からの CRL をチェックするのは、CRL をデバイスにダウンロードしていて、この CRL を使用する証明書取消確認を設定している場合だけです。

## はじめる前に

証明書取消確認がイネーブルになっていることを確認します。

コマンドまたはアクション	目的
ステッ プ1 グ1: 例: switch# copy tftp:adminca.crl bootflash:adminca.crl	リモート サーバから CRL をダウ ンロードします。 scheme 引数として、tftp:、ftp:、 scp:、または sftp: を指定できま す。server 引数は、リモート サー バのアドレスまたは名前であり、 url 引数はリモート サーバにある ソース ファイルへのパスです。 server、url、および filename の各 引数は、大文字小文字を区別して 入力します。

	コマンドまたはアクション	目的
ステッ プ <b>2</b>	configure terminal	グローバルコンフィギュレーショ ン モードを開始します。
	例: switch# configure terminal switch(config)#	
ステッ プ <b>3</b>	crypto ca crl requestnamebootflash:filename 例: switch(config)# crypto ca crl request admin-ca bootflash:adminca.crl	ファイルで指定されているCRLを 設定するか、現在のCRLと置き換 えます。
ステッ プ4	exit 例: switch(config)# exit switch#	設定モードを終了します。
ステッ プ5	show crypto ca crl <i>name</i> 例: switch# show crypto ca crl admin-ca	(任意) CA の CRL 情報を表示します。
ステッ プ6	copy running-config startup-config 例: switch# copy running-config startup-config	(任意) 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 ションにコピーします。

# CAの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 書を削除した後で、RSA キーペアとトラストポイントの関連付けを解除できます。証明書の削除 は、期限切れになった証明書や取り消された証明書、破損した(あるいは破損したと思われる) キーペア、現在は信頼されていないCA を削除するために必要です。

### 手順

I

	コマンドまたはアクション	目的
ステップ1	configure terminal	グローバルコンフィギュレーションモードを開 始します。
	例: switch# configure terminal switch(config)#	

	コマンドまたはアクション	目的
ステップ2	<pre>crypto ca trustpointname</pre>	トラストポイント CA を指定し、トラストポイ ントコンフィギュレーションモードを開始しま す。
	delete ca-certificate 例: switch(config-trustpoint)# delete ca-certificate	CA証明書または証明書チェーンを削除します。
ステップ4	delete certificate [force] 例: switch(config-trustpoint)# delete certificate	アイデンティティ証明書を削除します。 削除しようとしているアイデンティティ証明書 が証明書チェーン内の最後の証明書である場合 や、デバイス内の唯一のアイデンティティ証明 書である場合は、forceオプションを使用する必 要があります。この要件は、証明書チェーン内 の最後の証明書や唯一のアイデンティティ証明 書を誤って削除してしまい、アプリケーション (SSH など)で使用する証明書がなくなってし まうことを防ぐために設けられています。
ステップ5	exit 例: switch(config-trustpoint)# exit switch(config)#	トラストポイントコンフィギュレーションモー ドを終了します。
ステップ6	<pre>show crypto ca certificates [name]</pre>	(任意) CA の証明書情報を表示します。
 ステップ <b>1</b>	<pre>copy running-config startup-config  例: switch(config)# copy running-config startup-config</pre>	<ul> <li>(任意)</li> <li>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ます。</li> </ul>

# Cisco NX-OS デバイスからの RSA キーペアの削除

RSA キー ペアが何らかの理由で破損し、現在は使用されてないと見られるときには、その RSA キー ペアを Cisco NX-OS デバイスから削除することができます。



デバイスから RSA キーペアを削除した後、CA アドミニストレータに、その CA にあるこの デバイスの証明書を取り消すよう依頼します。その証明書を最初に要求したときに作成した チャレンジパスワードを入力する必要があります。

#### 手順

	コマンドまたはアクション	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
	例: switch# configure terminal switch(config)#	
ステップ2	crypto key zeroize rsalabel	RSA キーペアを削除します。
	<b>例:</b> switch(config)# crypto key zeroize rsa MyKey	
ステップ3	exit	設定モードを終了します。
	<b>例:</b> switch(config)# exit switch#	
ステップ4	show crypto key mypubkey rsa	(任意)
	<b>例:</b> switch# show crypto key mypubkey rsa	RSA キー ペアの設定を表示します。
ステップ5	copy running-config startup-config	(任意)
	<b>例:</b> switch# copy running-config startup-config	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 にコピーします。

# **PKI**の設定の確認

I

PKI 設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show crypto key mypubkey rsa	Cisco NX-OS デバイスで作成さ れた RSA 公開キーの情報を表 示します。

コマンド	目的
show crypto ca certificates	CA とアイデンティティ証明書 についての情報を表示します。
show crypto ca crl	CAのCRLについての情報を表 示します。
show crypto ca trustpoints	CA トラストポイントについて の情報を表示します。

# **PKI**の設定例

ここでは、Microsoft Windows Certificate サーバを使用して Cisco NX-OS デバイスで証明書と CRL を設定する作業の例について説明します。

# (注)

デジタル証明書の作成には、どのようなタイプのサーバでも使用できます。Microsoft Windows Certificate サーバに限られることはありません。

# Cisco NX-OS デバイスでの証明書の設定

Cisco NX-OS デバイスで証明書を設定するには、次の手順に従ってください。

### 手順

ステップ1	デバイスの FQDN を設定します。 switch# configure terminal Enter configuration commands, one per line. End with CNTL/Z. switch(config)# hostname Device-1 Device-1(config)#
ステップ <b>2</b>	デバイスの DNS ドメイン名を設定します。 Device-1(config)# <b>ip domain-name cisco.com</b>

ステップ3 トラストポイントを作成します。 Device-1(config)# crypto ca trustpoint myCA Device-1(config-trustpoint)# exit Device-1(config)# show crypto ca trustpoints trustpoint: myCA; key: revokation methods: crl ステップ4 このデバイス用の RSA キー ペアを作成します。 Device-1(config)# crypto key generate rsa label myKey exportable modulus 1024 Device-1(config)# show crypto key mypubkey rsa key label: myKey key size: 1024 exportable: yes

ステップ5 RSA キー ペアとトラストポイントを関連付けます。 Device-1(config)# crypto ca trustpoint myCA Device-1(config-trustpoint)# rsakeypair myKey Device-1(config-trustpoint)# exit Device-1(config)# show crypto ca trustpoints trustpoint: myCA; key: myKey revokation methods: crl

**ステップ6** Microsoft Certificate Service の Web インターフェイスから CA をダウンロードします。

**ステップ1** トラストポイントに登録する CA を認証します。

Device-1(config)# crypto ca authenticate myCA input (cut & paste) CA certificate (chain) in PEM format; end the input with a line containing only END OF INPUT : -----BEGIN CERTIFICATE-----

MIIC4jCCAoygAwIBAgIOBWDSiay0GZRPSRI1jK0ZejANBgkghkiG9w0BAQUFADCB kDEgMB4GCSqGSIb3DQEJARYRYW1hbmRrZUBjaXNjby5jb20xCzAJBgNVBAYTAk10 MRIwEAYDVQQIEw1LYXJuYXRha2ExEjAQBgNVBAcTCUJhbmdhbG9yZTEOMAwGA1UE ChMFQ21zY28xEzARBqNVBAsTCm51dHN0b3JhZ2UxEjAQBqNVBAMTCUFwYXJuYSBD QTAeFw0wNTA1MDMyMjQ2MzdaFw0wNzA1MDMyMjU1MTdaMIGQMSAwHqYJKoZIhvcN AQkBFhFhbWFuZGtlQGNpc2NvLmNvbTELMAkGA1UEBhMCSU4xEjAQBqNVBAqTCUth  ${\tt cm5hdGFrYTESMBAGA1UEBxMJQmFuZ2Fsb3J1MQ4wDAYDVQQKEwVDaXNjbzETMBEG}$ A1UECxMKbmV0c3RvcmFnZTESMBAGA1UEAxMJQXBhcm5hIENBMFwwDQYJKoZIhvcN AQEBBQADSwAwSAJBAMW/7b3+DXJPANBsIHHzluNccNM87ypyzwuoSNZXOMpeRXXI OzyBAgiXT2ASFuUOwQ1iDM8r0/41jf8RxvYKvysCAwEAAaOBvzCBvDALBgNVHQ8E BAMCAcYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUJyjyRoMbrCNMRU20yRhQ GgsWbHEwawYDVR0fBGQwYjAuoCygKoYoaHR0cDovL3NzZS0wOC9DZXJ0RW5yb2xs L0FwYXJuYSUyMENBLmNybDAwoC6gLIYqZmlsZTovL1xcc3N1LTA4XEN1cnRFbnJv bGxcQXBhcm5hJTIwQ0EuY3JsMBAGCSsGAQQBqjcVAQQDAqEAMA0GCSqGSIb3DQEB BQUAA0EAHv6UQ+8nE399Tww+KaGr0g0NIJaqNgLh0AFcT0rEyuyt/WYGPzksF9Ea NBG7E0oN66zex0EOEfG1Vs6mXp1//w==

----END CERTIFICATE-----

#### END OF INPUT

Fingerprint(s): MD5 Fingerprint=65:84:9A:27:D5:71:03:33:9C:12:23:92:38:6F:78:12
Do you accept this certificate? [yes/no]:y

```
Device-1(config)# show crypto ca certificates
Trustpoint: myCA
CA certificate 0:
subject= /emailAddress=admin@yourcompany.com/C=IN/ST=Karnataka/
L=Bangalore/0=Yourcompany/OU=netstorage/CN=Aparna CA
issuer= /emailAddress=admin@yourcompany.com/C=IN/ST=Karnataka/
L=Bangalore/0=Yourcompany/OU=netstorage/CN=Aparna CA
serial=0560D289ACB419944F4912258CAD197A
notBefore=May 3 22:46:37 2005 GMT
notAfter=May 3 22:55:17 2007 GMT
MD5 Fingerprint=65:84:9A:27:D5:71:03:33:9C:12:23:92:38:6F:78:12
```

purposes: sslserver sslclient ike

```
ステップ8
             トラストポイントに登録するために使用する証明書要求を作成します。
            Device-1(config) # crypto ca enroll myCA
             Create the certificate request ..
             Create a challenge password. You will need to verbally provide this
              password to the CA Administrator in order to revoke your certificate.
              For security reasons your password will not be saved in the configuration.
              Please make a note of it.
              Password: nbv123
             The subject name in the certificate will be: Device-1.cisco.com
             Include the switch serial number in the subject name? [yes/no]: no
             Include an IP address in the subject name [yes/no]: yes
             ip address: 10.10.1.1
             The certificate request will be displayed...
             ----BEGIN CERTIFICATE REQUEST----
            MIIBqzCCARQCAQAwHDEaMBgGA1UEAxMRVmVnYXMtMS5jaXNjby5jb20wgZ8wDQYJ
            KoZIhvcNAQEBBQADqY0AMIGJAoGBAL8Y1UAJ2NC7jUJ1DVaSMqNIqJ2kt8rl4lKY
            0JC6ManNy4qxk8VeMXZSiLJ4JgTzKWdxbLDkTTysnjuCXGvjb+wj0hEhv/y51T9y
            P2NJJ8ornqShrvFZgC7ysN/PyMwKcgzhbVpj+rargZvHtGJ91XTq4WoVkSCzXv8S
            VqyH0vEvAgMBAAGgTzAVBgkqhkiG9w0BCQcxCBMGbmJ2MTIzMDYGCSqGSIb3DQEJ
            DjEpMCcwJQYDVR0RAQH/BBswGYIRVmVnYXMtMS5jaXNjby5jb22HBKwWH6IwDQYJ
            KoZIhvcNAQEEBQADgYEAkT60KER6Qo8nj0sDXZVHSfJZh6K6JtDz3Gkd99GlFWgt
            PftrNcWUE/pw6HayfQl2T3ecgNwel2d15133YBF2bktExiI6Ul88nTOjglXMjja8
            8a23bNDpNsM8rklwA6hWkrVL8NUZEFJxqbjfngPNTZacJCUS6ZqKCMetbKytUx0=
             ----END CERTIFICATE REQUEST----
```

#### **ステップ9** Microsoft Certificate Service の Web インターフェイスからアイデンティティ証明書を要求します。

ステップ10 アイデンティティ証明書をインポートします。

Device-1(config)# crypto ca import myCA certificate
input (cut & paste) certificate in PEM format:
-----BEGIN CERTIFICATE-----

```
MIIEADCCA6qqAwIBAqIKCjOOoQAAAAAAdDANBqkqhkiG9w0BAQUFADCBkDEqMB4G
CSqGSIb3DQEJARYRYW1hbmRrZUBjaXNjby5jb20xCzAJBqNVBAYTAk1OMRIwEAYD
VQQIEwlLYXJuYXRha2ExEjAQBqNVBAcTCUJhbmdhbG9yZTEOMAwGA1UEChMFQ21z
{\tt Y28xEzARBgNVBAsTCm51dHN0b3JhZ2UxEjAQBgNVBAMTCUFwYXJuYSBDQTAeFw0w}
NTExMTIwMzAyNDBaFw0wNjExMTIwMzEyNDBaMBwxGjAYBgNVBAMTEVZ1Z2FzLTEu
Y21zY28uY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC/GNVACdjQu41C
dQ1WkjKjSICdpLfK5eJSmNCQujGpzcuKsZPFXjF2UoiyeCYE8ylncWyw5E08rJ47
glxr42/sI9IRIb/8udU/cj9jSSfKK56koa7xWYAu8rDfz8jMCnIM4W1aY/q2q4Gb
x7RifdV06uFqFZEgs17/Elash9LxLwIDAQABo4ICEzCCAg8wJQYDVR0RAQH/BBsw
GYIRVmVnYXMtMS5jaXNjby5jb22HBKwWH6IwHQYDVR00BBYEFKCLi+2sspWEfgrR
bhWmlVyo9jngMIHMBgNVHSMEgcQwgcGAFCco8kaDG6wjTEVNjskYUBoLFmxxoYGW
pIGTMIGOMSAwHqYJKoZIhvcNAQkBFhFhbWFuZGtlQGNpc2NvLmNvbTELMAkGA1UE
BhMCSU4x \texttt{EjAQBgNVBAgTCUthcm5hdGFrYTESMBAGA1UEBxMJQmFuZ2Fsb3J1MQ4w}
DAYDVQQKEwVDaXNjbzETMBEGA1UECxMKbmV0c3RvcmFnZTESMBAGA1UEAxMJQXBh
cm5h1ENBghAFYNKJrLQZ1E9JEiWMrR16MGsGA1UdHwRkMGIwLqAsoCqGKGh0dHA6
Ly9zc2UtMDqvQ2VydEVucm9sbC9BcGFybmE1MjBDQS5jcmwwMKAuoCyGKmZpbGU6
Ly9cXHNzZS0wOFxDZXJ0RW5yb2xsXEFwYXJuYSUyMENBLmNybDCBigYIKwYBBQUH
AQEEfjB8MDsGCCsGAQUFBzAChi9odHRwOi8vc3NlLTA4L0NlcnRFbnJvbGwvc3Nl
\verb"LTA4X0FwYXJuYSUyMENBLmNydDA9BggrBgEFBQcwAoYxZmlsZTovL1xcc3NlLTA4"
XEN1cnRFbnJvbGxcc3N1LTA4X0FwYXJuYSUyMENBLmNydDANBgkqhkiG9w0BAQUF
AANBADbGBGsbe7GNLh9xeOTWBNbm24U69ZSuDDcOcUZUUTgrpnTqVpPyejtsyf1w
```

E36cIZu4WsExREqxbTk8ycx7V5o= ----END CERTIFICATE-----Device-1(config)# exit Device-1#

ステップ11 証明書の設定を確認します。

**ステップ12** 証明書の設定をスタートアップ コンフィギュレーションに保存します。

# 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。

## 手順

**ステップ1** Microsoft Certificate Services の Web インターフェイスから、[Retrieve the CA certificate or certificate revocation task] をクリックし、[Next] をクリックします。

#### Microsoft Certificate Services -- Aparna CA

#### Welcome

You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-ma depending upon the type of certificate you request.

#### Select a task:

- Retrieve the CA certificate or certificate revocation list
- C Request a certificate
- C Check on a pending certificate

**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] を クリックし、[Download CA certificate] をクリックします。

<i>Microsoft</i> Certificate Services Aparna CA
Retrieve The CA Certificate Or Certificate Revocation List
It is not necessary to manually install the CA certification path if you request and install a certificate from this cer CA certification path will be installed for you automatically.
Choose file to download: CA Certificate: Current [Aparna CA] O DER encoded or • Base 64 encoded
Download CA certificate Download CA certification path Download latest certificate revocation list

**ステップ3** [File Download] ダイアログボックスにある [Open] をクリックします。

Microsoft Certificate Services Aparna CA Retrieve The CA Certificate Or Certificate Revo Install this CA certification path to allow your compute	cation List ter to trust certificates issued from this certification authority.
It is not necessary to manually install the CA CA certification path will be installed for you Choose file to download: CA Certificate: ODER encoded or OBas Download CA certificate Download CA certificate Download latest certificate re	Impose       Impose         Some files can harm your computer. If the file information below looks suspicious, or you do not fully trust the source, do not open or save this file.       Impose         File name:       certnew.cer         File type:       Security Certificate         From:       10.76.45.108         Impose       This type of file could harm your computer if it contains malicious code.         Would you like to open the file or save it to your computer?       Impose         Impose       Cancel       More Info
	Always ask before opening this type of file

**ステップ4** [Certificate] ダイアログボックスにある [Copy to File] をクリックし、[OK] をクリックします。

Install this CA sortification path to allow	ertificate	<u>1</u>	?X
It is not necessary to manually install th CA certification path will be installed fc	General Details Certification Show: <a>[<ai< a="">]</ai<></a>	Path Value	from this ce
Choose file to download: CA Certificate: CDER encoded or Download CA certifica Download CA certifica Download latest certific	Version Serial number Signature algorithm Issuer Valid from Valid to Subject Public key	V3 0560 D289 ACB4 1994 4F49 1 sha1R5A Aparna CA, netstorage, Cisco 04 Mei 2005 4:16:37 04 Mei 2007 4:25:17 Aparna CA, netstorage, Cisco R5A (512 Bits)	

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

It is not necessary to manually install th CA certification path will be installed for       Show: <all>       If om this certification         Choose file to download:       CA Certificate:       Current (Aparma CA)       If ield       Export File Format         CA Certificate:       Current (Aparma CA)       Serial numbe       Signature alc       Export File Format         Construction       DER encoded or       Signature alc       Select the format you want to use:       Select the format you want to use:         Download CA certification       Download latest certification       Descended binary X.509 (.CER)       Bage-64 encoded X.509 (.CER)         Download latest certification       Indude all certificates in the certification path if possible       Erronal Information Exchange - PKCS #12 (.PFX)         Indude all certificates in the certification path if possible       Erronal Information Exchange - PKCS #12 (.PFX)</all>	Install this CA certification path to allow General Deta	ills Certification Path	tion authority.
Choose file to download: CA Certificate: Current [Apama CA] O DER encoded or Download CA certificat Download CA certificat Download Iatest certific Download latest certific Download Iatest certific Certificate Export Wizard Certificate Export Wizard Certificate Export Wizard Certificates can be exported in a variety of file formats. Select the format you want to use: Derended binary X.509 (.CER) Derended X.509 (.CER) Certificates in the certification path if possible Certificates in the cer	It is not necessary to manually install th show: All:	>	from this certific
Image: Super Valid from Valid to       Select the format you want to use:         Image: Valid to       Subject         Image: Valid to       Subject <td< td=""><td>Choose file to download:</td><td>Certificate Export Wizard Export File Format Certificates can be exported in a varied</td><td>y of file formats.</td></td<>	Choose file to download:	Certificate Export Wizard Export File Format Certificates can be exported in a varied	y of file formats.
Eersonal Information Exchange - PRCS #12 (.PFX)      Include all certificates in the certification path if possible      Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above	© DER encoded or ( ☐ Valid fror ☐ Valid to ☐ Valid to ☐ Subject ☐ Download CA certifica ☐ Download latest certific	A Select the format you want to use: © DER encoded binary X.509 (.CER) © Base-64 encoded X.509 (.CER) © Gryptographic Message Syntax © Include all certificates in the	R) Standard - PKCS #7 Certificates (.P7B : certification path if possible
Delete the private key if the export is successful		<ul> <li>Personal unformation exchange</li> <li>Include all certificates in the</li> <li>Enable strong protection (rk</li> <li>Delete the private key if the</li> </ul>	- PRCD #12 (,PPA) : certification path if possible :equires IE 5.0, NT 4.0 SP4 or above) : export is successful

- **ステップ6** [Certificate Export Wizard] ダイアログボックスにある [File name:] テキストボックスに保存するファ 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で、[Finish] をクリックします。
- **ステップ8** Microsoft Windows の type コマンドを入力して、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#12 証明書署名要求(CSR)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には、次の手順に従ってください。

### 手順

```
ステップ1 Microsoft Certificate Services の Web インターフェイスから、[Request a certificate] をクリックし、
[Next] をクリックします。
```

Microsoft Certificate Services -- Aparna CA

#### Welcome

You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-ma depending upon the type of certificate you request.

#### Select a task:

- O Retrieve the CA certificate or certificate revocation list
- Request a certificate
- C Check on a pending certificate

ステップ2 [Advanced request] をクリックし、[Next] 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] をクリックし、[Next] をクリックします。

### Microsoft Certificate Services -- Aparna CA

#### Advanced Certificate Requests

You can request a certificate for yourself, another user, or a computer using one of the following methods. Note that t certification authority (CA) will determine the certificates that you can obtain.

- O Submit a certificate request to this CA using a form.
- Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 enco
- Request a certificate for a smart card on behalf of another user using the Smart Card Enrollment Station.
   You must have an enrollment agent certificate to submit a request for another user.

ステップ4 [Saved Request] テキストボックスに、base64の PKCS#10 証明書要求をペーストし、[Next] をク リックします。証明書要求が Cisco NX-OS デバイスのコンソールからコピーされます。

Γ

Saved Request:         VqyH0vEvAgMBAAGgTzAVBgkqhkiG9w0BCQcxCBMG         DjEpMCcwJQYDVRORAQH/BBswGYIRVmVnYXMtMS5j         KoZIhvcNAQEEBQADgYEAkT60KER6Qo8nj0sDXZVH         PftrNcWUE/pw6HayfQ12T3ecgNwe12d15133YBF2:         8a23bNDpNsM8rk1wA6hWkrVL8NUZEFJxqbjfngPN         END_CENTIFICATE_PF0VUST	
VqyH0vEvAgMBAAGgTzAVBgkqhkiG9w0BCQcxCBMG         DjEpMCcwJQYDVRORAQH/BBswGYIRVmVnYXMtMS5j         Base64 Encoded         KoZIhvcNAQEEBQADgYEAkT60KER608nj0sDXZVH         PftrNcWUE/pw6HayfQl2T3ecgNwel2d151333VBF2:         (PKCS #10 or #7):         Bas23bNDpNsM8rklwA6hWkrVL8NUZEFJxqbjfngPN	
Browse for a file to insert.	
Additional Attributes:	
Attributes:	

**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。

#### Microsoft Certificate Services -- Aparna CA

#### **Certificate Pending**

Your certificate request has been received. However, you must wait for an administrator to issue the certificate you r

Please return to this web site in a day or two to retrieve your certificate.

Note: You must return with this web browser within 10 days to retrieve your certificate

ステップ6 CAアドミニストレータが証明書要求を承認するのを確認します。

Certification Authority					
Action Yiew 🗍 🗢 🔿 🗈 [	• • •	B .			
Tree	Request ID	Binary Request	Request Disposition Message	Request Submission Date	Requester Nam
Certification Authority (Local)  Aparna CA  Revoked Certificates  Pending Requests  Failed Requests	116	BEGIN NE	Taken Under Submission	All Tasks Refresh Help	SSE-08\IUSR_S
ontains operations that can be perform	ed on the object	£5			

**ステップ7** Microsoft Certificate Services の Web インターフェイスから、[Check on a pending certificate] をクリックし、[Next] をクリックします。

#### Microsoft Certificate Services -- Aparna CA

#### Welcome

You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-ma depending upon the type of certificate you request.

#### Select a task:

- O Retrieve the CA certificate or certificate revocation list
- C Request a certificate
- Check on a pending certificate

**ステップ8** チェックする証明書要求を選択して、[Next] をクリックします。

Dioaco co	loct the cortificat		ant to chock:		
Flease se	Poqueet Certificat	e request you w a (12 Nanombor 20			
Gave	Prequest Certificat	e (12 Nopeniber 20	103 20.30.22)		

**ステップ9** [Base 64 encoded] をクリックして、[Download CA certificate] 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。

Download CA certificate       Some files can harm your computer. If the file information below looks suspicious, or you do not fully trust the source, do not open or save this file.         File name:       certure.cer         File type:       Security Certificate         From:       10.76.45.108
File name: certnew.cer File type: Security Certificate From: 10.76.45.108
File type: Security Certificate From: 10.76.45.108
From: 10.76.45.108
介 This type of file could harm your computer if it contains
malicious code.
Would you like to open the file or save it to your computer?
<u>D</u> pen Save Cancel More Info
↓ Juans ask befare opening this time of file

ステップ11 [Certificate] ボックスで、[Details] タブをクリックし、[Copy to File...] 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)] をクリックし、[Next] をク

## リックします。

Field       Value         Version       V3         Signature algorithm       sha1RSA         Signature algorithm       sha1RSA         Issuer       Aparna CA, netstorage, Cisco         Valid from       12 Nopember 2005 8:32:40         Valid to       12 Nopember 2005 8:42:40         Valid to       12 Nopember 2005 8:42:40         Valid to       12 Nopember 2005 8:42:40         Public key       RSA (1024 Bits)         Certificate Export Wizard         Edit Properties       Copy to File         OK       Edit Properties         OK       Egit Properties         OK       Egit Properties         OK       Egit Properties in the certificates in the certification path if possil         Endit Properties       OK		<b>_</b>	
Writion       V3         Serial number       DA33 8EA1 0000 0000 0074         Signature algorithm       sha1RSA         Issuer       Aparna CA, netstorage, Cisco         Valid from       12 Nopember 2005 8:32:40         Valid to       12 Nopember 2005 8:42:40         Valid to       12 Nopember 2005 8:42:40         Public key       RSA (1024 Bits)         Certificate Export Wizard         Edit Properties       Certificate Export Wizard         Edit Properties       Copy to File         OK       Bage-64 encoded X.509 (.CER)         Gryptographic Message Syntax Standard - PKCS #7 Cert       Include all certificates in the certification path if possil         Certain ender all certificates in the certification path if possil       Ended event is successful	Field	Value	
Signature algorithm       0A33 BEA1 0000 0000 0074         Signature algorithm       sha1RSA         Issuer       Aparna CA, netstorage, Cisco         Valid from       12 Nopember 2006 8:42:40         Valid to       12 Nopember 2006 8:42:40         Subject       Vegas-1.cisco.com         Public key       RSA (1024 Bits)         Edit Properties       Certificate Export Wizard         Edit Properties       Copy to File         OK       Certificates can be exported in a variety of file formats.         Select the format you want to use:       DER encoded binary X.509 (.CER)         © BER encoded X.509 (.CER)       Gryptographic Message Syntax Standard - PKCS #7 Cert         Include all certificates in the certification path if possil       Personal Information Exchange - PKCS #12 (.PFX)         Include all certificates in the certification path if possil       Enable strong protection (requires IE.50, NT 4.0 SP4	Version	V3	
Signature algorithm       Sharks A         Issuer       Aparna CA, netstorage, Cisco         Valid from       12 Nopember 2005 8:32:40         Valid to       12 Nopember 2006 8:42:40         Public key       RSA (1024 Bits)         Certificate Export Wizard         Export File Format         Certificates can be exported in a variety of file formats.         Select the format you want to use:         © BER encoded binary X.509 (.CER)         © Gryptographic Message Syntax Standard - PKCS #7 Cert         © Include all certificates in the certification path if possil         © Bersonal Information Exchange - PKCS #12 (.PFX)         Include all certificates in the certification path if possil         Enable strong protection (requires IE 50, NT 4) 0 SP4         Delete the private gey if the export is successful	Serial number	0A33 8EA1 0000 0000 0074	
Waid from       12 Nopember 2005 8:32:40         Waid to       12 Nopember 2006 8:42:40         Subject       Vegas-1.cisco.com         Public key       RSA (1024 Bits)         Edit Properties       Copy to File         OK       Edit Properties         OK       Gryptographic Message Syntax Standard - PKCS #7 Cert         Include all certificates in the certification path if possil         Endit entrication path if possil	Signature algorithm	Marca Cil petstorade Cisco	
Walid to       12 Nopember 2006 8:42:40         Subject       Vegas-1.cisco.com         Public key       RSA (1024 Bits)         Image: Construction of the second distribution of the	Valid from	12 Nopember 2005 8:32:40	
Subject       Vegas-1.cisco.com         Public key       RSA (1024 Bits)         Edit Properties       Certificate Export Wizard         Edit Properties       Copy to File         OK       DER encoded binary X.509 (.CER)         © gryptographic Message Syntax Standard - PKCS #7 Cert         Include all certificates in the certification path if possil         © Personal Information Exchange - PKCS #12 (.PFX)         Include all certificates in the certification path if possil         Enable strong protection (requires IE 5.0, NT 4.0 SP4         Delete the private key if the export is successful	Valid to	12 Nopember 2006 8:42:40	
Public key       RSA (1024 Bits)         Certificate Export Wizard         Export File Format         Certificates can be exported in a variety of file formats.         Edit Properties         Copy to File         OK         OK         Personal Information Exchange - PKCS #12 (.PFX)         Include all certificates in the certification path if possil         Personal Information Exchange - PKCS #12 (.PFX)         Include all certificates in the certification path if possil         Penable strong protection (requires IE 5.0, NT 4.0 SP4         Delete the private key if the export is successful	E Subject	Vegas-1.cisco.com	
Certificate Export Wizard         Export File Format         Certificates can be exported in a variety of file formats.         Certificates can be exported in a variety of file formats.         Select the format you want to use:         © DER encoded binary X.509 (.CER)         © Bage-64 encoded X.509 (.CER)         © Cryptographic Message Syntax Standard - PKCS #7 Cert         © Include all certificates in the certification path if possil         © Personal Information Exchange - PKCS #12 (.PFX)         © Include all certificates in the certification path if possil         © Enable strong protection (requires IE 5.0, NT 4.0 SP4         © Delete the private key if the export is successful	🖻 Public key	RSA (1024 Bits)	
Export File Format         Certificates can be exported in a variety of file formats.         Select the format you want to use:         DER encoded binary X.509 (.CER)         Bage-64 encoded X.509 (.CER)         Cryptographic Message Syntax Standard - PKCS #7 Cert         Include all certificates in the certification path if possil         Personal Information Exchange - PKC5 #12 (.PFX)         Include all certificates in the certification path if possil         Enable strong protection (requires IE 5.0, NT 4.0 SP4         Delete the private key if the export is successful	[		Certificate Export Wizard
Select the format you want to use:     Edit Properties     OK     Select the format you want to use:     DER encoded binary X.509 (.CER)     Bage-64 encoded X.509 (.CER)     Cryptographic Message Syntax Standard - PKCS #7 Cert     Include all certificates in the certification path if possil     Personal Information Exchange - PKCS #12 (.PFX)     Include all certificates in the certification path if possil     Enable strong protection (requires IE 5.0, NT 4.0 SP4)   Delete the private key if the export is successful			<b>Export File Format</b> Certificates can be exported in a variety of file formats.
Edit Properties       Copy to File         OK       Bage-64 encoded X.509 (.CER)         OK       Cryptographic Message Syntax Standard - PKCS #7 Cert         Include all certificates in the certification path if possil         Personal Information Exchange - PKCS #12 (.PFX)         Include all certificates in the certification path if possil         Enable strong protection (requires IE 5.0, NT 4.0 SP4         Delete the private key if the export is successful			Select the format you want to use:
Edit Properties       Copy to File         OK       © Gryptographic Message Syntax Standard - PKCS #7 Cert         Include all certificates in the certification path if possil       © Bersonal Information Exchange - PKCS #12 (.PFX)         Include all certificates in the certification path if possil       © Bersonal Information Exchange - PKCS #12 (.PFX)         Enable strong protection (requires IE 5.0, NT 4.0 SP4       © Delete the private key if the export is successful			DER encoded binary X.509 (.CER)
OK         OK         Include all certificates in the certification path if possil         Personal Information Exchange - PKCS #12 (.PFX)         Include all certificates in the certification path if possil         Enable all certificates in the certification path if possil         Enable strong protection (requires IE 5.0, NT 4.0 SP4         Delete the private key if the export is successful		Edit Properties	· Base-64 encoded X.509 (.CER)
OK       Include all certificates in the certification path if possil         C       Personal Information Exchange - PKCS #12 (.PFX)         Include all certificates in the certification path if possil         Include all certificates in the certification path if possil         Include all certificates in the certification path if possil         Include all certificates in the certification path if possil         Include all certificates in the certification path if possil         Include all certificates in the certification path if possil         Include all certificates in the certification path if possil         Include all certificates in the certification path if possil         Include all certificates in the certification path if possil         Include all certificates in the certification path if possil         Include all certificates in the certification path if possil         Include all certificates in the certification path if possil         Include all certificates in the certification path if possil         Include all certificates in the certification path if possil         Include all certificates in the certification path if possil         Include all certificates in the certification path if possil         Include all certificates in the certification path if possil         Include all certificates in the certification path if possil         Include all certificates in the certificates in the certificates in the certificates in the c			C Cryptographic Message Syntax Standard - PKCS #7 Certi
<ul> <li>Personal Information Exchange - PKCS #12 (.PFX)</li> <li>Include all certificates in the certification path if possi</li> <li>Enable strong protection (requires IE 5.0, NT 4.0 SP4</li> <li>Delete the private key if the export is successful</li> </ul>			
<ul> <li>Include all certificates in the certification path if possi</li> <li>Enable strong protection (requires IE 5.0, NT 4.0 SP4</li> <li>Delete the private key if the export is successful</li> </ul>		0	Include all certificates in the certification path if possib
Enable strong protection (requires IE 5.0, NT 4.0 SP4 Delete the private key if the export is successful			<ul> <li>Include all certificates in the certification path if possib</li> <li>Personal Information Exchange - PKC5 #12 (.PFX)</li> </ul>
Delete the private <u>key</u> if the export is successful		0	Include all certificates in the certification path if possib     Personal Information Exchange - PKCS #12 (.PFX)     Include all certificates in the certification path if possib
		0	Include all certificates in the certification path if possit     Personal Information Exchange - PKC5 #12 (.PFX)     Include all certificates in the certification path if possit     Enable strong protection (requires IE 5.0, NT 4.0 SP4
			Include all certificates in the certification path if possil     Personal Information Exchange - PKC5 #12 (.PFX)     Include all certificates in the certification path if possil     Enable strong protection (requires IE 5.0, NT 4.0 SP4     Delete the private key if the export is successful

**ステップ12** [Certificate Export Wizard] ダイアログボックスにある [File name:] テキストボックスに保存するファ 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。

٦

5how: <all></all>	<u> </u>		
Field	Value		
Version	V3		
Serial number	0A33 8EA1 0000 0000 0074		
Signature algorithm	shaires CA, petcherage, Cisso		
Valid from	12 Nopember 2005 8:32:40		
Valid to	12 Nopember 2006 8:42:40		
Subject	Vegas-1.cisco.com		
E Public key	RSA (1024 Bits)		
		Completing the Certif Wizard	ficate
	Edit Properties	Completing the Certif           Wizard           You have successfully completed the wizard.           You have specified the following sett           File Name	ficate   e Certificat tings:
	Edit Properties	Completing the Certif         Wizard         You have successfully completed the         wizard.         You have specified the following sett         File Name         Export Keys         Include all certificates in the certific         File Format	ficate   e Certificat tings: cation path
	Edit Properties;,;	Completing the Certif Wizard You have successfully completed the wizard. You have specified the following sets File Name Export Keys Include all certificates in the certific File Format	ficate   e Certificat tings: cation path

**ステップ14** Microsoft Windows の type コマンドを入力して、アイデンティティ証明書を Base-64 でエンコード された形式で表示します。

C:\WINNT\system32\cmd.exe	
D:\testcerts>type mylD.cer BEGIN CERTIFICATE II IEADCCA6qgAwIBAgIKCj00oQAAAAAAADDANBgkqhkiG9wØBAQUFADCBkDEgMB4G SqGSIb3DQEJARYRYW1hbmRrZUBjaXNjby5jb20xCzaJBgNUBAYTAk10MRIwEAYD QQIEwILYXJuYXRha2ExEjAQBgNUBAcTCUJhbmdhbG9yZTEOMAwGA1UEChMFQ21z 28xEzARBgNUBASTCn51dHNØb3JhZ2UxEjAQBgNUBAMTCUFwYXJuYSBQTAeFwØw ITEXMTIwZAyNDBaFWØwNjExMTIwMzEyNDBaMBwxGjAYBgNUBAMTEUZ1Z2FzLTEu 21zY28uY29tHIGFMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC/CNUACdjQu41C Q1WkjKjSICdpIfK5eJSmNCQujGpzcuKsZPFXjF2UoiyeCY8ylncWyw5E08rJ47 7lxr42/sI9IRIb/8udU/cj9jSSfKK56koa7xWYAu8rDfz8jMCnIM4WiaY/q2q4Gb 7RifdU06uFqFZEgs17/Elash9LxLwIDAQAB04ICE2CAg8wJQVDURØRAQH/BBsw WIRUmUnYXMtMS5jaXNjby5jb22HBKwWH6IwHQYDURØ0BBYEFKCLi+2sspWefgrR bNm1Uy09jngMIHMBgNUHSMEgcQwgcGAFCc08kaDG6wjTEUNjsKVUB0LFmxxoYGW DIGTMIGQMSAwHgYJKoZIhucNAQkBFhFhbWFuZGt1QGNpc2NvLmNubTELMAkGA1UE BMCSU4xEjAQBgNUBAgTCUthcm5hdGFrYTESMBAGA1UEBxMJQmFuZ2Fsb3J1MQ4w DAYDUQQKEwUDAXNjbzETMBEGA1UECxMKbmU063RucmFnZTESMBAGA1UEAxMJQXBh r5hIENBghAFYNKJrLqZ1E9JEiWMrR16MGsGAFUSBJmWKAu0CyGKmZpbGU6 Jy9c2UtMDgvQ2UydEUucm9sbC9BcGFybmELMjBDQS5jcmwWKAu0CyGKmZpbGU6 Jy9c2HNzZSØwOFxDZXJØRW5yb2xSEFwYXJuYSUyMENBLmNybDCBigYIKwYBBQUH HQEEfjB8MDsGCCsGAQUFBZAChi9odHRw0iBvc3N1LTA4L6N1cnRFbnJubGxca3N1LTA4 KENLcnRFbnJubGxcc3N1LTA4X0FwYXJuYSUyMENBLmNyDDANBgkqhkiG9w0BAQUF AANBADbGBGsbe7GNLH9xeOTWBNbm24U69ZSuDDcOcUZUUTgrpnTqUpPyejtsyf1w 236cIZu4WsExREqxDTK8ycx7U50= END CERTIFICATE	

# 証明書の取り消し

I

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。

### 手順

- **ステップ1** [Certification Authority] ツリーから、[Issued Certificates] フォルダをクリックします。リストから、 取り消す証明書を右クリックします。
- **ステップ2** [All Tasks] > [Revoke Certificate] の順に選択します。

Tree	Request ID	Requester Name	Binary Certificate	Serial Number	Certificate Effecti
Certification Authority (Local)	- 289	SSE-08\IUSR_SS	BEGIN CERTI	786263d000000000059	9/20/2005 4:27 A
Aparna CA	90	SSE-08\IUSR_SS	BEGIN CERTI	7862643d0000000005a	9/20/2005 4:27 A
Revoked Certificates	91	SSE-08\IUSR_SS	BEGIN CERTI	786264d90000000005b	9/20/2005 4:27 A
	92	SSE-08\IUSR_SS	BEGIN CERTI	7c3278180000000005c	9/20/2005 10:14
	93	SSE-08\IUSR_SS	BEGIN CERTI	7c3278270000000005d	9/20/2005 10:14
Eailed Requests	94	SSE-08\IUSR_SS	BEGIN CERTI	7c3278370000000005e	9/20/2005 10:14
	95	SSE-08\IUSR_SS	BEGIN CERTI	7c3278470000000005f	9/20/2005 10:14
	98	SSE-08\IUSR_SS	BEGIN CERTI	7ca48c2200000000062	9/21/2005 12:18
	99	SSE-08\IUSR_SS	BEGIN CERTI	021a9d1a00000000063	9/22/2005 1:45 A
	100	SSE-08\IUSR_SS	BEGIN CERTI	1c1013cf00000000064	9/27/2005 2:44 A
	101	SSE-08\IUSR_SS	BEGIN CERTI	1c10d19100000000065	9/27/2005 2:45 A
	102	SSE-08\IUSR_SS	BEGIN CERTI	2b4eb36700000000066	9/30/2005 1:46 A
	103	SSE-08\IUSR_SS	BEGIN CERTI	458b6b4300000000067	10/5/2005 4:03 A
	104	SSE-08\IUSR_SS	BEGIN CERTI	4eb5b32700000000068	10/6/2005 10:46
	105	SSE-08\IUSR_SS	BEGIN CERTI	4f60084100000000069	10/7/2005 1:52 A
	106	SSE-08\IUSR_SS	BEGIN CERTI	4fdf95640000000006a	10/7/2005 4:11 A
	107	SSE-08\IUSR_SS	BEGIN CERTI	5f3e8c960000000006b	10/10/2005 3:49
	108	SSE-08\IUSR_SS	BEGIN CERTI	5f413d200000000006c	10/10/2005 3:52
	109	SSE-08\IUSR_SS	BEGIN CERTI	17b22de80000000006d	10/18/2005 12:20
	110	SSE-08\IUSR_SS	BEGIN CERTI	17b306760000000006e	10/18/2005 12:21
	111	SSE-08\IUSR_SS	BEGIN CERTI	11ea38060000000006f	10/19/2005 11:58
	112	SSE-08\IUSR_SS	BEGIN CERTI	170bea8b000000000070	10/20/2005 11:53
	113	SSE-08\IUSR_SS	BEGIN CERTI	4aafff2e000000000071	10/31/2005 12:32
	114	SSE-08\IUSR_SS	BEGIN CERTI	78cc6e6c00000000072	11/8/2005 11:26
	115	SSE-08\IUSR_SS	BEGIN CERTI	78e3416100000000073	11/8/2005 11:51
	116	SSE-08\ILISP_SS	BEGIN CERTI	0a338ea100000000074	11/12/2005 8:32

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

Tree	Deguart TD	Demuscher Merry	Dinawa Caubificata	Control Municher	Carbificate FF
	Request ID		Binary Certificate	Serial Number	
Certification Authority (Local)	89	SSE-U8\IUSR_SS	BEGIN CERTI	7862630000000000059	9/20/2005 4:
🗄 [ 🕜 Aparna CA	90	SSE-08(IUSR_SS	BEGIN CERTI	/862643d0000000005a	9/20/2005 4:
	91	SSE-08\IUSR_SS	BEGIN CERTI	786264d90000000005b	9/20/2005 4:
Issued Certificates	92	SSE-08\IUSR_SS	BEGIN CERTI	7c3278180000000005c	9/20/2005 10
Pending Requests	93	SSE-08\IUSR_SS	BEGIN CERTI	7c3278270000000005d	9/20/2005 10
Failed Requests	94	SSE-08\IUSR_SS	BEGIN CERTI	7c3278370000000005e	9/20/2005 10
	95	SSE-08\IUSR_SS	BEGIN CERTI	7c3278470000000005f	9/20/2005 10
	98	Cortificate Devocatio	DECULCEDI	2 1 1 0000062	9/21/2005 12
	99	certificate Revocatio		p0000063	9/22/2005 1:
	100	Are you sure you want	to revoke the selected	certificate(s)? 0000064	9/27/2005 2:
	101			0000065	9/27/2005 2:
	102	You may specify a reas	on for this revocation.	0000066	9/30/2005 1:
	103	Reason code:		0000067	10/5/2005 4:
	104	Unspecified	-	p0000068	10/6/2005 10
	105	1		0000069	10/7/2005 1:
	106		Yes	No 000006a	10/7/2005 4:
	107			000006Ь	10/10/2005 3
	108	SSE-08\IUSR_SS	BEGIN CERTI	5F413d200000000006c	10/10/2005 3
	109	SSE-08\IUSR_SS	BEGIN CERTI	17b22de80000000006d	10/18/2005 1
	110	SSE-08\IUSR_SS	BEGIN CERTI	17b306760000000006e	10/18/2005 1
	111	SSE-08\IUSR_SS	BEGIN CERTI	11ea38060000000006f	10/19/2005 1
	112	SSE-08\IUSR_SS	BEGIN CERTI	170bea8b00000000070	10/20/2005 1
	113	SSE-08\IUSR_SS	BEGIN CERTI	4aafff2e00000000071	10/31/2005 1
	114	SSE-08\IUSR_SS	BEGIN CERTI	78cc6e6c00000000072	11/8/2005 11
	115	SSE-08\IUSR_SS	BEGIN CERTI	78e3416100000000073	11/8/2005 11
	116	SSE-08\IUSR_SS	BEGIN CERTI	0a338ea1000000000074	11/12/2005 8
		_			

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。

	Descurst TD	Demuschen Ner-	Dia any Caubificate	Constant and the second second	Carbificada Effectiva
~~			Binary Certificate		
Certification Authority (Local)	15	SSE-U8\IUSR_SS	BEGIN CERTI	5dae53cdUUUUUUUUUUU	6/30/2005 3:27 AM
Aparna CA	16	SSE-U8\IUSR_SS	BEGIN CERTI	5db14Ud3UUUUUUUUUUU	6/30/2005 3:30 AM
Revoked Certificates	17	SSE-U8\IUSR_SS	BEGIN CERTI	5e2d/c1b00000000011	6/30/2005 5:46 AM
Issued Certificates	18	SSE-08\IUSR_SS	BEGIN CERTI	16db4f8f00000000012	7/8/2005 3:21 AM
Pending Requests	19	SSE-08\IUSR_SS	BEGIN CERTI	261c392400000000013	7/14/2005 5:00 AM
	20	SSE-08\IUSR_SS	BEGIN CERTI	262b520200000000014	7/14/2005 5:16 AM
	21	SSE-08\IUSR_SS	BEGIN CERTI	2634c7f200000000015	7/14/2005 5:27 AM
	22	SSE-08\IUSR_SS	BEGIN CERTI	2635b00000000000016	7/14/2005 5:28 AM
	23	SSE-08\IUSR_SS	BEGIN CERTI	2648504000000000017	7/14/2005 5:48 AM
	24	SSE-08\IUSR_SS	BEGIN CERTI	2a27635700000000018	7/14/2005 11:51 PM
	25	SSE-08\IUSR_SS	BEGIN CERTI	3f88cbf700000000019	7/19/2005 3:29 AM
	26	SSE-08\IUSR_SS	BEGIN CERTI	6e4b5f5f0000000001a	7/28/2005 3:58 AM
	27	SSE-08\IUSR_SS	BEGIN CERTI	725b89d80000000001b	7/28/2005 10:54 PM
	28	SSE-08\IUSR_SS	BEGIN CERTI	735a88780000000001c	7/29/2005 3:33 AM
	29	SSE-08\IUSR_SS	BEGIN CERTI	148511c70000000001d	8/3/2005 11:30 PM
	30	SSE-08\IUSR_SS	BEGIN CERTI	14a7170100000000001e	8/4/2005 12:07 AM
	31	SSE-08\IUSR_SS	BEGIN CERTI	14fc45b50000000001f	8/4/2005 1:40 AM
	32	SSE-08\IUSR_SS	BEGIN CERTI	486ce80b00000000020	8/17/2005 3:58 AM
	33	SSE-08\IUSR_SS	BEGIN CERTI	4ca4a3aa000000000021	8/17/2005 11:37 PM
	47	SSE-08\IUSR_SS	BEGIN CERTI	1aa55c8e0000000002f	9/1/2005 11:36 PM
	63	SSE-08\IUSR_SS	BEGIN CERTI	3f0845dd0000000003f	9/9/2005 1:11 AM
	66	SSE-08\IUSR_SS	BEGIN CERTI	3f619b7e00000000042	9/9/2005 2:48 AM
	82	SSE-08\IUSR SS	BEGIN CERTI	6313c46300000000052	9/16/2005 1:09 AM
	96	SSE-08\IUSR SS	BEGIN CERTI	7c3861e3000000000060	9/20/2005 10:20 PM
	97	SSE-08\IUSR SS	BEGIN CERTI	7c6ee351000000000061	9/20/2005 11:20 PM
	116	SSE-08\IUSR_SS	BEGIN CERTI	0a338ea1000000000074	11/12/2005 8:32 AM
		10 17			

# CRLの作成と公開

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。

## 手順

ステップ1 [Certification Authority]の画面から、[Action]>[All Tasks]>[Publish]の順に選択します。

	Certification Au	thority					
[	Action View	(= =) 🔁	📧 💣 🕼 🗄	3   😫			
T	All Tasks 🛛 🕨	Publish	Request ID	Requester Name	Binary Certificate	Serial Number	Certificate Effect
2	Refresh	ty (Local)	- 🔯 15	SSE-08\IUSR_SS	BEGIN CERTI	5dae53cd000000000000	6/30/2005 3:27 A
ř.	Export List	-7 ()	16	SSE-08\IUSR_SS	BEGIN CERTI	5db140d3000000000010	6/30/2005 3:30 A
		rtificates	17	SSE-08\IUSR_SS	BEGIN CERTI	5e2d7c1b00000000011	6/30/2005 5:46 A
	Properties	ficates	18	SSE-08\IUSR_SS	BEGIN CERTI	16db4f8f000000000012	7/8/2005 3:21 AM
	Help	quests	19	SSE-08\IUSR_SS	BEGIN CERTI	261c3924000000000013	7/14/2005 5:00 A
Ľ.	Falled Red	quests	20	SSE-08\IUSR_SS	BEGIN CERTI	262b520200000000014	7/14/2005 5:16 A
			21	SSE-08\IUSR_SS	BEGIN CERTI	2634c7f200000000015	7/14/2005 5:27 A
			22	SSE-08\IUSR_SS	BEGIN CERTI	2635b00000000000016	7/14/2005 5:28 A
			23	SSE-08\IUSR_SS	BEGIN CERTI	26485040000000000017	7/14/2005 5:48 A
			24	SSE-08\IUSR_SS	BEGIN CERTI	2a27635700000000018	7/14/2005 11:51
			25	SSE-08\IUSR_SS	BEGIN CERTI	3f88cbf7000000000019	7/19/2005 3:29 A
			26	SSE-08\IUSR_SS	BEGIN CERTI	6e4b5f5f00000000001a	7/28/2005 3:58 A
			27	SSE-08\IUSR_SS	BEGIN CERTI	725b89d80000000001b	7/28/2005 10:54
			28	SSE-08\IUSR_SS	BEGIN CERTI	735a887800000000001c	7/29/2005 3:33 A
			29	SSE-08\IUSR_SS	BEGIN CERTI	148511c700000000001d	8/3/2005 11:30 P
			30	SSE-08\IUSR_SS	BEGIN CERTI	14a7170100000000001e	8/4/2005 12:07 A
			31	SSE-08\IUSR_SS	BEGIN CERTI	14fc45b500000000001f	8/4/2005 1:40 AM
			32	SSE-08\IUSR_SS	BEGIN CERTI	486ce80b00000000020	8/17/2005 3:58 A
			33	SSE-08\IUSR_SS	BEGIN CERTI	4ca4a3aa000000000021	8/17/2005 11:37
			47	SSE-08\IUSR_SS	BEGIN CERTI	1aa55c8e00000000002f	9/1/2005 11:36 P
			63	SSE-08\IUSR_SS	BEGIN CERTI	3f0845dd00000000003f	9/9/2005 1:11 AM
			66	SSE-08\IUSR_SS	BEGIN CERTI	3f619b7e000000000042	9/9/2005 2:48 AM
			82	SSE-08\IUSR_SS	BEGIN CERTI	6313c463000000000052	9/16/2005 1:09 A
			96	SSE-08\IUSR_SS	BEGIN CERTI	7c3861e3000000000000	9/20/2005 10:20
			97	SSE-08\IUSR_SS	BEGIN CERTI	7c6ee351000000000061	9/20/2005 11:20
			116	SSE-08\IUSR_SS	BEGIN CERTI	0a338ea100000000074	11/12/2005 8:32
			•				
Cor	ntains operations th	nat can be perfor	med on the object				
1000		and a second		540.		N	

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

Certification Authority					
] Action ⊻iew ] 🗢 → 🗈 💽	1 🗗 🗗 🗟	\$   <b>B</b>			
Tree	Request ID	Requester Name	Binary Certificate	Serial Number	Certificate Effective D
Certification Authority (Local)	15	SSE-08\IUSR_SS	BEGIN CERTI	5dae53cd00000000000f	6/30/2005 3:27 AM
	16	SSE-08\IUSR_SS	BEGIN CERTI	5db140d3000000000010	6/30/2005 3:30 AM
Revoked Certificates	17	SSE-08\IUSR_SS	BEGIN CERTI	5e2d7c1b00000000011	6/30/2005 5:46 AM
Issued Certificates	18	SSE-08\IUSR_SS	BEGIN CERTI	16db4f8f000000000012	7/8/2005 3:21 AM
Pending Requests	19	SSE-08\IUSR_SS	BEGIN CERTI	261c392400000000013	7/14/2005 5:00 AM
Failed Requests	20	SSE-08\IUSR_SS	BEGIN CERTI	262b520200000000014	7/14/2005 5:16 AM
	21	SSE-08\IUSR_SS	BEGIN CERTI	2634c7f200000000015	7/14/2005 5:27 AM
	22	SSE-08\IUSR_SS	BEGIN CERTI	2635b00000000000016	7/14/2005 5:28 AM
	23	SSE-08\IUSR_SS	BEGIN CERTI	2648504000000000017	7/14/2005 5:48 AM
The	e last published	CRL is still valid and ca	n be used by clients. A	re you sure you want to publish	a new CRL? 2005 3:58 AM 2005 10:54 PM 2005 3:33 AM 005 11:30 PM 005 12:07 AM
	31	SSE-08\IUSR_SS	BEGIN CERTI	14fc45b500000000001f	8/4/2005 1:40 AM
1	32	SSE-08\IUSR_SS	BEGIN CERTI	486ce80b00000000020	8/17/2005 3:58 AM
	33	SSE-08\IUSR_SS	BEGIN CERTI	4ca4a3aa000000000021	8/17/2005 11:37 PM
	47	SSE-08\IUSR_SS	BEGIN CERTI	1aa55c8e00000000002f	9/1/2005 11:36 PM
	63	SSE-08\IUSR_SS	BEGIN CERTI	3f0845dd0000000003f	9/9/2005 1:11 AM
	<b>100</b> 66	SSE-08\IUSR_SS	BEGIN CERTI	3f619b7e00000000042	9/9/2005 2:48 AM
	82	SSE-08\IUSR_SS	BEGIN CERTI	6313c46300000000052	9/16/2005 1:09 AM
	<b>100</b> 96	SSE-08\IUSR_SS	BEGIN CERTI	7c3861e3000000000060	9/20/2005 10:20 PM
	<b>100</b> 97	SSE-08\IUSR_SS	BEGIN CERTI	7c6ee35100000000061	9/20/2005 11:20 PM
	116	SSE-08\IUSR_SS	BEGIN CERTI	0a338ea100000000074	11/12/2005 8:32 AM
	•				

# 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。

## 手順

**ステップ1** Microsoft Certificate Services の Web インターフェイスから、[Retrieve the CA certificate or certificate revocation list] をクリックし、[Next] をクリックします。

Γ

Microsoft Certificate Services Aparna CA	Home
/elcome	
ou use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you ill be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-ma epending upon the type of certificate you request.	acquire a certificate, you al messages, and more
elect a task:	
Retrieve the CA certificate or certificate revocation list	
○ Request a certificate	
Check on a pending certificate	
	Next >

ステップ2	[Download latest certificate revocation list	]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で、保存するファイル名を入力して、[Save] をクリックします。





Microsoft Windows の type コマンドを入力して、CRL を表示します。

C:\WINNT\system32\cmd.exe	
D. 1. 4 4	A
D:\testCerts/type aparnach.cri RFGIN \SCA9 (RI	
MILIGBTCCBa8CA0EwDQYJKoZIhucNAQEFRQAwgZAxIDaeBgkghkiG9w0BCQEWEWEt	
YW5ka2VAY21zY28uY29tMQswCQYDVQQGEwJJT,jESMBAGA1UÊCBMJS2FybmF0YWth	
MRIwEAYDUQQHEw1CYW5nYWxvcmUxDjAMBgNVBÃoTBUNpc2NvMRMwEQYĎUQQLEwpu	
ZXRzdG9yYWd1MRIwEAYDVQQDEw1BcGFybmEgQ0EXDTA1MTExMjA0MzYwNFoXDTA1	
MTExOTE2NTYwNFowggSxMBsCCmEbCaEAAAAAAAIXDTA1MDgxNjIxNTIxOUowGwIX	
TN5GTgAAAAAAAxcNMDUwODE2MjE1MjI5WjAbAqpM/CtCAAAAAAAEFw0wNTA4MTYy	
MIUYNDFAMBSCCmxpnsIAAAAAAAAUXDIAIMDgxNjIxNIIIMIowGwIKbM993AAAAAAAA	
BICNMDUWNJH4MDHXMJHØWJHDH9DWZE//HHHHHHHHHHHHHHHIMØWNIH4MIY9MIUZMIVAMBSC	
CKZDERYHHHHHHHGADIHITDGXNJIXMITXNVOWKVIKUGGCHHHHHHHHGKCNTDUWNJI3 M MMB-001Liommo Cotlibrodre Econciccin I	
пјпелене и упримене и предостава и предостава и предостава и предостава и предостава и предостава и предостава Мјак и ради и ради и предостава и	
ſſĹŬŴŊŊŔĸŊġŇŎŔĸŎĊŴĸĊĸĬĔŴĬŖĔĸŢġĊŎŔŎŎŔŎŔĿŔĸĬŔĬŔĬĿĹŴŎŴŔĬŔŎſŊŶĊŎĿŔŎſŊŔĸŎĬŔŴŴ ĊĸŶŊĨĬŔŎĨĬĔŎŇĬĔŎŇŶĸĊĸĬĔŴĬŖĔĊĔĸġĊŎŎŎŎŎŔĿŇŇŊĬĿĸŎŇĔĊŇĬŔŎĬĬŴŎŔŎĸŎĬŔŎĬĬ	
DhcNMDILwNzEAMDAzMzII2WiAbAqndr IWNAAAAAPEwAwNTA4MTYuMTIIzMTWAMBsC	
C12xQNMAAAAAAABAXDTA1MDgxNiTxNTMxNUguKQTKXi18GuAAAAAAEBcNMDUUNza2	
M.iExM.iEwW.iAMMAoGA1UdFQQDCgEFMBsCChbbT48AAAAAABIXDTA1MDgxN.iIxNTMx	
NŬowGwIKJŇw5JAAAAAAAExcNMĎUwODE2MjE1MzE1WjAbAgomK1ICAAĂAAĂAUFwØw	
NTA3MTQwMDMzMTBaMBsCCiYØx/IAAAAAABUXDTA1MDcxNDAwMzIØNVowGwIKJjWw	
AAAAAAAAFhcNMDUwNzEOMDAzMTUxWjAbAgomSFBAAAAAAAAXFw0wNTA3MTQwMDNy	
MjVaMBsCCionY1cAAAAAABgXDTA1MDgxNjIxNTMxNVowGwIKP4jL9wAAAAAAGRcN	
MDUwODE2MjE1MzE1WjAbAgpuS19fAAAAAAAaFw0wNTA4MTYyMTUzMTVaMBsCCnJb	
idgAAAAAABsXDIA1MDg×NjI×NTM×NVowGwIKc1qIeAAAAAAHBcNMDUwODE2MjE1	
mzE1WjAbAgoUhKHHAAAAAAAdFwØwNIA4MIYYMIUZMIVaMBsCChSnFwEAAAAAABB4X	
DIHIMDGXNJIXNIMXNOOUGUIKFPXFTYHHHHHHHXCOMDUWDE3MIGZMDYGWJHDHGPI	
DOGLAHAHAHAHGENUWANA MATA COODINA DAADAGU AGU AGU AGU AGU AGU AGU AGU AGU AGU	
N2HUNTOSMURAQVCJ9HHHHHHLXCNNDUWHHINICWN2H2WJHJH9U/GEAUHHHHHHHH RuðuNTOSMURAJNI AM2JS-19Hm34000000EFYNTOIMDUwDNI/NDADAEuuGuIV	
$1 \times 0 \times 1 \times 1 \times 0 \times 1 \times 1 \times 0 \times 0$	
NZILUNTZAMBSCCDXU41EAAAAAAAGEXDTA1MDkuMDE4NTIZMEDuGuIkCiOODOAAAAAA	
dBcNMDIIxMTFvMDQzNDQvWrA1MDMvHvYDURA1BBqvFaAllJvjvBaMhrCNMBII2OvRhQ	
GasWbHEwEAYJKwYBBAGCNXUBBAMCAQAwDQYJKoZIhucNAQEFBQADQQALu91DCrhi	
HoCUBm9NgwzY.j.jJE.jgeU168CuaacFF3rkM8YyZYpu1c32R/VvU6aSxgrAC/SbsEa	
nxpJt5xYJNdy	
END X509 CRL	
D:\testcerts>	-1

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。

手順

### ステップ1 CRL ファイルを Cisco NX-OS デバイスのブートフラッシュにコピーします。 Device-1# copy tftp:apranaCA.crl bootflash:aparnaCA.crl ステップ2 CRL を設定します。 Device-1# configure terminal Device-1 (config) # crypto ca crl request myCA bootflash:aparnaCA.crl Device-1(config)# ステップ3 CRLの内容を表示します。 Device-1(config) # show crypto ca crl myCA Trustpoint: myCA CRL: Certificate Revocation List (CRL): Version 2 (0x1) Signature Algorithm: shalWithRSAEncryption Issuer: /emailAddress=admin@yourcompany.com/C=IN/ST=Karnatak Yourcompany/OU=netstorage/CN=Aparna CA Last Update: Nov 12 04:36:04 2005 GMT Next Update: Nov 19 16:56:04 2005 GMT CRL extensions: X509v3 Authority Key Identifier: keyid:27:28:F2:46:83:1B:AC:23:4C:45:4D:8E:C9:18:50:1 1.3.6.1.4.1.311.21.1: . . . Revoked Certificates: Serial Number: 611B09A10000000002 Revocation Date: Aug 16 21:52:19 2005 GMT Serial Number: 4CDE464E00000000003 Revocation Date: Aug 16 21:52:29 2005 GMT Serial Number: 4CFC2B4200000000004 Revocation Date: Aug 16 21:52:41 2005 GMT Serial Number: 6C699EC200000000005 Revocation Date: Aug 16 21:52:52 2005 GMT Serial Number: 6CCF7DDC0000000000 Revocation Date: Jun 8 00:12:04 2005 GMT Serial Number: 70CC4FFF00000000007 Revocation Date: Aug 16 21:53:15 2005 GMT Serial Number: 4D9B11160000000008 Revocation Date: Aug 16 21:53:15 2005 GMT Serial Number: 52A8023000000000009 Revocation Date: Jun 27 23:47:06 2005 GMT CRL entry extensions: X509v3 CRL Reason Code: CA Compromise Serial Number: 5349AD46000000000A Revocation Date: Jun 27 23:47:22 2005 GMT CRL entry extensions: X509v3 CRL Reason Code:

```
CA Compromise
Serial Number: 53BD173C000000000B
       Revocation Date: Jul 4 18:04:01 2005 GMT
       CRL entry extensions:
           X509v3 CRL Reason Code:
           Certificate Hold
Serial Number: 591E7ACE0000000000
       Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 5D3FD52E000000000D
       Revocation Date: Jun 29 22:07:25 2005 GMT
       CRL entry extensions:
           X509v3 CRL Reason Code:
           Key Compromise
Serial Number: 5DAB77130000000000
       Revocation Date: Jul 14 00:33:56 2005 GMT
    Serial Number: 5DAE53CD000000000F
       Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 5DB140D300000000000
       Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 5E2D7C1B00000000011
       Revocation Date: Jul 6 21:12:10 2005 GMT
       CRL entry extensions:
           X509v3 CRL Reason Code:
           Cessation Of Operation
Serial Number: 16DB4F8F00000000012
       Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 261C39240000000013
       Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 262B52020000000014
       Revocation Date: Jul 14 00:33:10 2005 GMT
    Serial Number: 2634C7F20000000015
       Revocation Date: Jul 14 00:32:45 2005 GMT
    Serial Number: 2635B00000000000016
       Revocation Date: Jul 14 00:31:51 2005 GMT
    Serial Number: 2648504000000000017
       Revocation Date: Jul 14 00:32:25 2005 GMT
    Serial Number: 2A2763570000000018
Revocation Date: Aug 16 21:53:15 2005 GMT
   Serial Number: 3F88CBF700000000019
       Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 6E4B5F5F0000000001A
       Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 725B89D8000000001B
       Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 735A88780000000001C
       Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 148511C7000000001D
       Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 14A717010000000001E
       Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 14FC45B5000000001F
       Revocation Date: Aug 17 18:30:42 2005 GMT
    Serial Number: 486CE80B00000000020
       Revocation Date: Aug 17 18:30:43 2005 GMT
    Serial Number: 4CA4A3AA00000000021
```

Revocation Date: Aug 17 18:30:43 2005 GMT Serial Number: 1AA55C8E000000002F Revocation Date: Sep 5 17:07:06 2005 GMT Serial Number: 3F0845DD000000003F Revocation Date: Sep 8 20:24:32 2005 GMT Serial Number: 3F619B7E00000000042 Revocation Date: Sep 8 21:40:48 2005 GMT Serial Number: 6313C4630000000052 Revocation Date: Sep 19 17:37:18 2005 GMT Serial Number: 7C3861E300000000000 Revocation Date: Sep 20 17:52:56 2005 GMT Serial Number: 7C6EE35100000000061 Revocation Date: Sep 20 18:52:30 2005 GMT Serial Number: 0A338EA100000000074 <-- Revoked identity certificate Revocation Date: Nov 12 04:34:42 2005 GMT Signature Algorithm: shalWithRSAEncryption Ob:cb:dd:43:0a:b8:62:1e:80:95:06:6f:4d:ab:0c:d8:8e:32: 44:8e:a7:94:97:af:02:b9:a6:9c:14:fd:eb:90:cf:18:c9:96: 29:bb:57:37:d9:1f:d5:bd:4e:9a:4b:18:2b:00:2f:d2:6e:c1: 1a:9f:1a:49:b7:9c:58:24:d7:72

 (注) 取り消されたデバイスのアイデンティティ証明書(シリアル番号は 0A338EA10000000074)が最後に表示されています。