証明書の管理

この章の内容は、次のとおりです。

サーバ証明書の管理

証明書署名要求（CSR）を生成して新しい証明書を取得し、新しい証明書をCisco IMCにアップロードして現在のサーバ証明書と交換することができます。サーバ証明書は、Verisignのようなパブリック認証局（CA）、または独自に使用している認証局のいずれかによって署名されます。生成される証明書キーの長さは 2048 ビットです。

（注） この章に記載されている以下のタスクを実行する前に、Cisco IMCの時刻が現在の時刻に設定されていることを確認します。

手順

ステップ 1 Cisco IMCから CSR を生成します。

ステップ 2 証明書の発行と署名を行う認証局にCSRファイルを送信します。組織で独自の自己署名証明書を生成している場合は、CSR ファイルを使用して自己署名証明書を生成できます。

ステップ 3 新しい証明書をCisco IMCにアップロードします。

（注） アップロードされた証明書は、Cisco IMCによって生成された CSR から作成されている必要があります。この方法で作成されていない証明書はアップロードしないでください。

証明書署名要求の生成

（注） [コモン ネーム（Common Name）]および [組織単位（Organization Unit）] フィールドでは、特殊文字（アンパサンド（**&**）など）を使用しないでください。

はじめる前に

- 証明書を設定するには、admin 権限を持つユーザとしてログインする必要があります。
- Cisco IMCの時刻が現在の時刻に設定されていることを確認してください。

手順

ステップ 1 [ナビゲーション（Navigation）]ペインの [管理者（Admin）] タブをクリックします。

ステップ 2 [管理者（Admin）] タブの [証明書管理（Certificate Management）] をクリックします。

ステップ 3 [アクション（Actions）]領域で、[新しい証明書署名要求の生成（Generate New Certificate Signing Request）] リンクをクリックします。
[新しい証明書署名要求の生成（Generate New Certificate Signing Request）]ダイアログボックスが表示されます。

ステップ 4 [新しい証明書署名要求の生成（Generate New Certificate Signing Request）]ダイアログボックスで、次のプロパティを更新します。

[名前（Name）]	説明
[コモン ネーム（Common Name）]フィールド	Cisco IMCの完全修飾名。 デフォルトでは、サーバの CN は CXXX-YYYYYY 形式で表示されます（XXX はサーバのモデル番号で YYYYYY はシリアル番号です）。 最新バージョンにアップグレードするときに、CN はそのまま保持されます。
[組織名（Organization Name）]フィールド	証明書を要求している組織。
[組織単位（Organization Unit）]フィールド	組織ユニット。
[地域（Locality）]フィールド	証明書を要求している会社の本社が存在する市または町。
[都道府県（State Name）]フィールド	証明書を要求している会社の本社が存在する都道府県。
[国コード（Country Code）]ドロップダウン リスト	会社が存在する国。
[メール（Email）]フィールド	会社の電子メールの連絡先。
[自己署名証明書（Self Signed Certificate）]チェックボックス	自己署名証明書を生成します。 **警告** 証明書の生成が成功した後、Cisco IMC Web GUI が再起動します。管理コントローラとの通信が一時的に切断され、再ログインが必要な場合があります。 （注） イネーブルにすると、自動的に CSR が生成され、署名およびアップロードが行われます。

（注） 自己署名証明書が有効な場合は、ステップ 5 および 6 を無視します。

ステップ 5 [CSR の作成（Generate CSR）]をクリックします。
[csr.txt を開いています（Opening csr.txt）]ダイアログボックスが表示されます。

ステップ 6 CSR ファイル csr.txt を管理するには、次のいずれかの手順を実行します。

a) [開く（Open With）]をクリックして csr.txt を表示します。

b) [ファイルの保存（Save File）]をクリックしてから [OK] をクリックし、ローカル マシンに csr.txt を保存します。

次の作業

- 証明書の発行と署名を行う認証局にCSRファイルを送信します。組織で独自の自己署名証明書を生成している場合は、CSR ファイルを使用して自己署名証明書を生成できます。
- 証明書のタイプが[サーバ（Server）] であることを確認します。

信頼できない CA 署名付き証明書の作成

パブリック認証局（CA）を使用してサーバ証明書の生成と署名を行う代わりに、独自の CA を運用して独自の証明書に署名することができます。このセクションでは、Linux で実行されている OpenSSL 証明書サーバを使用して CA を作成するコマンドおよびサーバ証明書を生成するコマンドについて説明します。OpenSSL の詳細については、http://www.openssl.orgを参照してください。

（注） これらのコマンドは、Cisco IMCではなく、OpenSSL パッケージを使用している Linux サーバで入力します。

はじめる前に

- 組織内のサーバで、証明書サーバのソフトウェア パッケージを取得してインストールします。
- Cisco IMCの時刻が現在の時刻に設定されていることを確認してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**openssl genrsa -out***CA_keyfilenamekeysize* 例： `# openssl genrsa -out ca.key 2048`	このコマンドは、CA で使用される RSA 秘密キーを生成します。 （注） ユーザ入力なしで CA がキーにアクセスできるように、このコマンドに -des3 オプションは使用しないでください。 指定されたファイル名には、指定されたサイズの RSA キーが含まれています。

	コマンドまたはアクション	目的
ステップ 2	**openssl req -new -x509 -days***numdays***-key***CA_keyfilename***-out***CA_certfilename* 例： `# openssl req -new -x509 -days 365 -key ca.key -out ca.crt`	このコマンドは、指定されたキーを使用して、CA の自己署名証明書を新規に作成します。証明書は指定された期間有効になります。このコマンドは、ユーザに証明書の追加情報を求めるプロンプトを表示します。 証明書サーバは、アクティブな CA です。
ステップ 3	**echo "nsCertType = server" > openssl.conf** 例： `# echo "nsCertType = server" > openssl.conf`	このコマンドは、証明書がサーバ限定の証明書であることを指定する行を OpenSSL 設定ファイルに追加します。この指定により、認証されたクライアントがサーバになりすます man-in-the-middle 攻撃を防御できます。 OpenSSL 設定ファイル openssl.conf には、"nsCertType = server" という文が含まれています。

ステップ 4	**openssl x509 -req -days***numdays***-in***CSR_filename***-CA***CA_certfilename***-set_serial 04 -CAkey***CA_keyfilename***-out***server_certfilename***-extfile openssl.conf**
	
	例：
	`# openssl x509 -req -days 365 -in csr.txt -CA ca.crt -set_serial 04`
	`-CAkey ca.key -out myserver05.crt -extfile openssl.conf`
		このコマンドは、CA が CSR ファイルを使用してサーバ証明書を生成するように指示します。
		
		サーバ証明書は、出力ファイルに含まれています。

ステップ 5	**openssl x509 -noout -text -purpose -in <cert file>** 例： `openssl x509 -noout -text -purpose -in <cert file>`	生成された証明書のタイプが [サーバ（Server）]であることを確認します。 （注） フィールド **Server SSL** および **Netscape SSL** サーバの値が yes でない場合は、タイプが [サーバ（Server）] の証明書を生成するように openssl.conf が設定され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 6	生成された証明書に正しい使用期限が設定されていない場合は、Cisco IMCの時刻が現在の時刻に設定されていることを確認し、手順 1 ～ 5 を繰り返して証明書を再生成します。	（任意） 正しい使用期限が設定された証明書が作成されます。

この例は、CA の作成方法、および新規に作成された CA が署名するサーバ証明書の生成方法を示します。これらのコマンドは、OpenSSL を実行している Linux サーバで入力します。

```
# /usr/bin/openssl genrsa -out ca.key 2048
Generating RSA private key, 2048 bit long modulus
.............++++++
.....++++++
e is 65537 (0x10001)
# /usr/bin/openssl req -new -x509 -days 365 -key ca.key -out ca.crt
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a
DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:US
State or Province Name (full name) [Berkshire]:California
Locality Name (eg, city) [Newbury]:San Jose
Organization Name (eg, company) [My Company Ltd]:Example Incorporated
Organizational Unit Name (eg, section) []:Unit A
Common Name (eg, your name or your server's hostname) []:example.com
Email Address []:admin@example.com
# echo "nsCertType = server" > openssl.conf
# /usr/bin/openssl x509 -req -days 365 -in csr.txt -CA ca.crt -set_serial 01 -CAkey ca.key -out server.crt
-extfile openssl.conf
Signature ok
subject=/C=US/ST=California/L=San Jose/O=Example Inc./OU=Unit
A/CN=example.com/emailAddress=john@example.com
Getting CA Private Key
#
```

次の作業

新しい証明書をCisco IMCにアップロードします。

Windows を使用した自己署名証明書の作成

はじめる前に

- 証明書を設定するには、admin 権限を持つユーザとしてログインする必要があります。

- Cisco IMCの時刻が現在の時刻に設定されていることを確認してください。

手順

ステップ 1 IIS マネージャを開いて管理するレベルに移動します。

ステップ 2 [Features]領域で、[サーバー証明書] をダブルクリックします。

ステップ 3 [操作]ペインで、[Create Self-Signed Certificate] をクリックします。

ステップ 4 [Create Self-Signed Certificate]ウィンドウで、[Specify a friendly name for the certificate] フィールドに証明書の名前を入力します。

ステップ 5 [OK]をクリックします。

ステップ 6 （任意） 生成された証明書に正しい使用期限が設定されていない場合は、Cisco IMCの時刻が現在の時刻に設定されていることを確認し、手順 1 ～ 5 を繰り返して証明書を再生成します。
正しい使用期限が設定された証明書が作成されます。

サーバ証明書のアップロード

はじめる前に

- 証明書をアップロードするには、admin 権限を持つユーザとしてログインする必要があります。
- アップロードする証明書ファイルは、ローカルにアクセスできるファイルシステムに配置されている必要があります。
- 生成された証明書のタイプが [サーバ（Server）] であることを確認します。

（注） 最初にCisco IMCの [証明書の管理（Certificate Management）] メニューを使用して CSR を生成してから、その CSR を使用してアップロードする証明書を取得する必要があります。この方法で取得されていない証明書はアップロードしないでください。

手順

ステップ 1 [ナビゲーション（Navigation）]ペインの [管理者（Admin）] タブをクリックします。

ステップ 2 [管理者（Admin）] タブの [証明書管理（Certificate Management）] をクリックします。

ステップ 3 [アクション（Actions）]領域で、[サーバ証明書のアップロード（Upload Server Certificate）] をクリックします。

[証明書のアップロード（Upload Certificate）] ダイアログボックスが表示されます。

ステップ 4 [証明書のアップロード（Upload Certificate）]ダイアログボックスで、次のプロパティを更新します。

[名前（Name）]	説明
[ファイル（File）]フィールド	アップロードする証明書ファイル。
[参照（Browse）]ボタン	目的の証明書ファイルに移動するためのダイアログボックスが開きます。
[証明書のアップロード（Upload Certificate）]ボタン	証明書をアップロードできます。

ステップ 5 [証明書のアップロード（Upload Certificate）] をクリックします。

サーバ証明書の内容の貼り付け

ローカル ファイル システムからサーバ証明書をアップロードする代わりに、テキスト フィールドに証明書の内容を貼り付けることで新しいサーバ証明書をアップロードすることもできます。

はじめる前に

- 証明書をアップロードするには、admin 権限を持つユーザとしてログインする必要があります。
- アップロードする証明書ファイルは、ローカルにアクセスできるファイル システムに配置されている必要があります。
- 生成された証明書のタイプが [サーバ（Server）] であることを確認します。
- アップロードする証明書が署名されていることを確認します。

手順

ステップ 1 [ナビゲーション（Navigation）]ペインの [管理者（Admin）] タブをクリックします。

ステップ 2 [管理者（Admin）] タブの [証明書管理（Certificate Management）] をクリックします。

ステップ 3 [アクション（Actions）]領域で [サーバ証明書の貼り付け（Paste Server Certificate）] をクリックします。

[サーバ証明書の貼り付け（Paste Server Certificate）]ダイアログボックスが表示されます。

ステップ 4 [サーバ証明書の貼り付け（Paste Server Certificate）]ダイアログ ボックスで、[証明書（Certificate）] テキスト フィールドにサーバ証明書の内容を貼り付け、[保存（Save）] をクリックします。
これにより、サーバに証明書がアップロードされます。

新しい証明書のトラブルシューティング

場合によっては、新しい証明書がシステムに表示されないことがあります。その場合、次のトラブルシューティング手順を実行し、Cisco IMC をリブートする必要があります。

はじめる前に

- 証明書をアップロードするには、admin 権限を持つユーザとしてログインする必要があります。
- 新しい証明書をアップロード済みである必要があります。

手順

ステップ 1 Cisco IMC サーバで新しいセキュア シェル セッションを開始します。

ステップ 2 **scope certificate** および **show detail** コマンドをそれぞれ実行し、アップロードした証明書が表示されることを確認します。

ステップ 3 セキュア シェルのコマンドライン インターフェイスを終了します。

ステップ 4 Cisco IMC Web インターフェイスにログインします。

ステップ 5 [ナビゲーション（Navigation）]ペインの [管理者（Admin）] タブをクリックします。

ステップ 6 [管理者（Admin）] タブの[ユーティリティ（Utilities）] をクリックします。

ステップ 7 [ユーティリティ（Utilities）]ペインの [アクション（Actions）] 領域で、[Cisco IMC の再起動（Reboot Cisco IMC）] をクリックします。

ステップ 8 [OK]をクリックします。

ステップ 9 Web ブラウザの履歴をクリアします。

ステップ 10 Cisco IMC からログアウトしてから再度ログインし、新しい証明書が使用されていることを確認します。