



SSH 認証の X.509v3 証明書

- [SSH 認証の X.509v3 証明書 \(1 ページ\)](#)

SSH 認証の X.509v3 証明書

SSH 認証の X.509v3 証明書機能は、サーバ内で X.509v3 デジタル証明書を使用し、セキュアシェル (SSH) サーバ側でユーザ認証を使用します。

このモジュールでは、デジタル証明書用のサーバおよびユーザ証明書プロファイルを設定する方法について説明します。

SSH 認証の X.509v3 証明書の前提条件

- SSH 認証の X.509v3 証明書機能では、**ip ssh server authenticate user** コマンドの代わりに **ip ssh server algorithm authentication** コマンドが導入されます。 **ip ssh server authenticate user** コマンドを使用すると、次の警告メッセージが表示されます。

```
Warning: SSH command accepted but this CLI will be deprecated soon.  
Please move to new CLI "ip ssh server algorithm authentication".  
Please configure "default ip ssh server authenticate user" to make the CLI ineffective.
```

- **default ip ssh server authenticate user** コマンドを使用して、**ip ssh server authenticate user** コマンドを無効にします。その後、IOS セキュアシェル (SSH) サーバは **ip ssh server algorithm authentication** コマンドを使用して起動します。

SSH 認証の X.509v3 証明書の制約事項

- SSH 認証の X.509v3 証明書機能の実装は、Cisco IOS XE セキュアシェル (SSH) サーバ側にも適用できます。
- SSH サーバは、サーバおよびユーザ認証について、x509v3-ssh-rsa アルゴリズムベースの証明書のみをサポートします。

SSH 認証用の X.509v3 証明書に関する情報

次に、デジタル証明書、およびサーバとユーザの認証について説明します。

デジタル証明書

認証の有効性は、公開署名キーとその署名者のアイデンティティとの関連の強さに依存します。X.509v3 形式 (RFC5280) のデジタル証明書は、アイデンティティの管理を実行するために使用されます。信頼できるルート証明機関とその中間証明機関による署名の連鎖によって、指定の公開署名キーと指定のデジタルアイデンティティがバインドされます。

公開キーインフラストラクチャ (PKI) のトラストポイントは、デジタル証明書の管理に役立ちます。証明書とトラストポイントを関連付けることによって、証明書を追跡できます。トラストポイントには、認証局 (CA)、さまざまなアイデンティティパラメータ、およびデジタル証明書に関する情報が含まれています。複数のトラストポイントを作成して、異なる証明書に関連付けることができます。

X.509v3 を使用したサーバおよびユーザ認証

サーバ認証の場合、Cisco IOS XE セキュアシェル (SSH) サーバが確認のためにそれ自体の証明書を SSH クライアントに送信します。このサーバ証明書は、サーバ証明書プロファイル (ssh-server-cert-profile-server コンフィギュレーションモード) で設定されたトラストポイントに関連付けられます。

ユーザ認証の場合、SSH クライアントが確認のためにユーザの証明書を SSH サーバに送信します。SSH サーバは、サーバ証明書プロファイル (ssh-server-cert-profile-user コンフィギュレーションモード) で設定された公開キーインフラストラクチャ (PKI) トラストポイントを使用して、受信したユーザ証明書を確認します。

デフォルトでは、証明書ベースの認証が SSH サーバ端末でサーバおよびユーザに対して有効になります。

SSH 認証用の X.509v3 証明書の設定方法

ここでは、SSH 認証用の X.509v3 証明書の設定方法について説明します。

サーバ認証にデジタル証明書を使用するための SSH サーバの設定

サーバ認証にデジタル証明書を使用するように SSH サーバを設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します (要求された場合)。

	コマンドまたはアクション	目的
ステップ 2	configure terminal 例 : Device# 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。
ステップ 3	ip ssh server algorithm hostkey {x509v3-ssh-rsa [ssh-rsa] ssh-rsa [x509v3-ssh-rsa]} 例 : Device (config)# ip ssh server algorithm hostkey x509v3-ssh-rsa	ホスト キー アルゴリズムの順序を定義します。セキュア シェル (SSH) クライアントとネゴシエートされるのは、設定済みのアルゴリズムのみです。 (注) IOS SSH サーバには、1 つ以上の設定済みホストキー アルゴリズムが必要です。 <ul style="list-style-type: none"> • ssh-rsa : 公開キーベース認証 • x509v3-ssh-rsa : 証明書ベース認証
ステップ 4	ip ssh server certificate profile 例 : Device (config)# ip ssh server certificate profile	サーバ証明書プロファイルおよびユーザ証明書プロファイルを設定し、SSH 証明書プロファイ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 5	server 例 : Device (ssh-server-cert-profile)# server	サーバ証明書プロファイルを設定し、SSH サーバ証明書プロファイルのユーザ コンフィギュレーション モードを開始します。
ステップ 6	trustpoint sign PKI-trustpoint-name 例 : Device (ssh-server-cert-profile-server)# trustpoint sign trust1	公開キー インフラストラクチャ (PKI) トラストポイントをサーバ証明書プロファイルにアタッチします。SSH サーバは、この PKI トラストポイントに関連付けられた証明書をサーバ認証に使用します。
ステップ 7	ocsp-response include 例 : Device (ssh-server-cert-profile-server)# ocsp-response include	(任意) Online Certificate Status Protocol (OCSP) の応答または OCSP ステータスリングをサーバ証明書と一緒に送信します。 (注) デフォルトではこのコマンドの no 形式が設定されており、OCSP 応答はサーバ証明書と一緒に送信されません。

	コマンドまたはアクション	目的
ステップ 8	end 例： Device (ssh-server-cert-profile-server) # end	SSH サーバ証明書プロファイルのサーバコンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。

ユーザ認証用のデジタル証明書を確認するための SSH サーバの設定

ユーザ認証にデジタル証明書を使用するように SSH サーバを設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none">パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# 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。
ステップ 3	ip ssh server algorithm authentication {publickey keyboard password} 例： Device (config) # ip ssh server algorithm authentication publickey	ユーザ認証アルゴリズムの順序を定義します。セキュア シェル (SSH) クライアントとネゴシエートされるのは、設定済みのアルゴリズムのみです。 (注) SSH サーバには、1 つ以上の設定済みユーザ認証アルゴリズムが必要です。 (注) ユーザ認証に証明書方式を使用するには、 publickey キーワードを設定する必要があります。 (注) ip ssh server algorithm authentication コマンドは ip ssh server authenticate user コマンドの代わりに使用します。

	コマンドまたはアクション	目的
ステップ 4	<p>ip ssh server algorithm publickey {x509v3-ssh-rsa [ssh-rsa] ssh-rsa [x509v3-ssh-rsa]}</p> <p>例 :</p> <pre>Device (config)# ip ssh server algorithm publickey x509v3-ssh-rsa</pre>	<p>公開キー アルゴリズムの順序を定義します。SSH クライアントによってユーザ認証に許可されるのは、設定済みのアルゴリズムのみです。</p> <p>(注) SSH クライアントには、1つ以上の設定済み公開キーアルゴリズムが必要です。</p> <ul style="list-style-type: none"> • ssh-rsa : 公開キーベース認証 • x509v3-ssh-rsa : 証明書ベース認証
ステップ 5	<p>ip ssh server certificate profile</p> <p>例 :</p> <pre>Device (config)# ip ssh server certificate profile</pre>	<p>サーバ証明書プロファイルおよびユーザ証明書プロファイルを設定し、SSH 証明書プロファイルコンフィギュレーションモードを開始します。</p>
ステップ 6	<p>user</p> <p>例 :</p> <pre>Device (ssh-server-cert-profile)# user</pre>	<p>ユーザ証明書プロファイルを設定し、SSH サーバ証明書プロファイルのユーザコンフィギュレーションモードを開始します。</p>
ステップ 7	<p>trustpoint verify PKI-trustpoint-name</p> <p>例 :</p> <pre>Device (ssh-server-cert-profile-user)# trustpoint verify trust2</pre>	<p>受信したユーザ証明書の確認に使用される公開キー インフラストラクチャ (PKI) トラストポイントを設定します。</p> <p>(注) 同じコマンドを複数回実行することで、複数のトラストポイントを設定します。最大 10 のトラストポイントを設定できます。</p>
ステップ 8	<p>ocsp-response required</p> <p>例 :</p> <pre>Device (ssh-server-cert-profile-user)# ocsp-response required</pre>	<p>(任意) 受信したユーザ証明書による Online Certificate Status Protocol (OCSP) の応答の有無を要求します。</p> <p>(注) デフォルトではこのコマンドの no 形式が設定されており、ユーザ証明書は OCSP 応答なしで受け入れられます。</p>

	コマンドまたはアクション	目的
ステップ 9	end 例： Device(ssh-server-cert-profile-user)# end	SSH サーバ証明書プロファイルのユーザコンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。

デジタル証明書を使用したサーバおよびユーザ認証の設定の確認

デジタル証明書を使用したサーバおよびユーザ認証の設定を確認するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	show ip ssh 例： Device# show ip ssh SSH Enabled - version 1.99 Authentication methods:publickey,keyboard-interactive,password Authentication Publickey Algorithms:x509v3-ssh-rsa,ssh-rsa Hostkey Algorithms:x509v3-ssh-rsa,ssh-rsa Authentication timeout: 120 secs; Authentication retries: 3 Minimum expected Diffie Hellman key size : 1024 bits	現在設定されている認証方式を表示します。証明書ベース認証の使用を確認するには、x509v3-ssh-rsa アルゴリズムが設定済みのホストキーアルゴリズムであることを確認します。

SSH 認証用の X.509v3 証明書の設定例

ここでは、デジタル証明書を使用したユーザおよびサーバ認証の例を示します。

例：サーバ認証にデジタル証明書を使用するための SSH サーバの設定

この例では、サーバ認証用のデジタル証明書を使用するための SSH サーバの設定方法を示します。

```
Device> enable
Device# configure terminal
```

```
Device(config)# ip ssh server algorithm hostkey x509v3-ssh-rsa
Device(config)# ip ssh server certificate profile
Device(ssh-server-cert-profile)# server
Device(ssh-server-cert-profile-server)# trustpoint sign trust1
Device(ssh-server-cert-profile-server)# end
```

例：ユーザ認証用のデジタル証明書を確認するための SSH サーバの設定

この例では、ユーザ認証用のユーザのデジタル証明書を確認するための SSH サーバの設定方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# ip ssh server algorithm authentication publickey
Device(config)# ip ssh server algorithm publickey x509v3-ssh-rsa
Device(config)# ip ssh server certificate profile
Device(ssh-server-cert-profile)# user
Device(ssh-server-cert-profile-user)# trustpoint verify trust2
Device(ssh-server-cert-profile-user)# end
```

SSH 認証用の X.509v3 証明書の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Fuji 16.9.2	SSH 認証の X.509v3 証明書	SSH 認証の X.509v3 証明書機能は、サーバ内で X.509v3 デジタル証明書を使用し、SSH サーバ側でユーザ認証を使用します。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> からアクセスします。

