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。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

SSH 認証の X.509v3 証明書 の前提条件

- SSH 認証機能の X.509v3 証明書では、**ip ssh server authenticate user** コマンドに代わり **ip ssh server algorithm authentication** コマンドが導入されています。**ip ssh server authenticate user** コマンドを使用すると、次の非推奨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 CLI ineffective.
```

- **default ip ssh server authenticate user** コマンドを使用して、**ip ssh server authenticate user** コマンドが動作しないようにします。こうすると、IOS セキュア シェル（SSH）サーバが **ip ssh server algorithm authentication** コマンドを使用するようになります。

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、IOS セキュア シェル（SSH）サーバ側だけに適用されます。
- IOS SSH サーバでは、x509v3-ssh-rsa アルゴリズム ベースの証明書、および IOS SSH サーバ側でのサーバとユーザの認証のみがサポートされます。

SSH 認証の X.509v3 証明書について

デジタル証明書

認証の有効性は、署名の公開キーと署名者の ID との間の連携強度によって異なります。X.509v3 形式（RFC5280）のデジタル証明書を使用して、ID を管理できるようにします。信頼されたルート認証局とその中間認証局による一連の署名で、特定の署名の公開キーと特定のデジタル ID とがバインドされます。

Public Key Infrastructure（PKI）トラストポイントは、デジタル証明書の管理を支援します。証明書とトラストポイントとが関連付けられることで、証明書を追跡できるようになります。トラストポイントには、認証局（CA）、さまざまな ID パラメータ、デジタル証明書に関する情報が含まれています。さまざまな証明書と関連付けるために、トラストポイントは複数作成できます。

X.509v3 を使用したサーバとユーザの認証

サーバ認証では、IOS セキュア シェル（SSH）サーバは確認のため自身の証明書を 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）で設定されているトラストポイントに関連付けられます。

ユーザ認証では、SSH クライアントは確認のため当該ユーザの証明書を IOS 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）で設定されている Public Key Infrastructure（PKI）トラストポイントを使用して、着信するユーザ証明書を検証します。

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

SSH 認証の X.509v3 証明書の設定方法

サーバ認証用のデジタル証明書を使用する IOS SSH サーバの設定

手順の概要

1. **enable**
2. **configureterminal**
3. **ip ssh server algorithm hostkey** {**x509v3-ssh-rsa** [**ssh-rsa**] | **ssh-rsa** [**x509v3-ssh-rsa**]}
4. **ip ssh server certificate profile**
5. **server**
6. **trustpoint sign***PKI-trustpoint-name*
7. **ocsp-response include**
8. **end**

手順の詳細

	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 モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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。設定されたアルゴリズムのみ、Secure Shell（SSH）クライアントとネゴシエートされます。 （注） IOS SSH サーバでは、少なくとも 1 つの設定済みホスト キー アルゴリズムが必要です。 • ssh-rsa：公開キーによる認証 • x509v3-ssh-rsa：証明書ベースの認証

	コマンドまたはアクション	目的
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認可書プロファイルを設定し、SSH 証明書プロファイルの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て、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`	サーバ証明書プロファイルに公開キー インフラストラクチャ（PKI）のトラストポイントをアタッチします。SSH サーバは、サーバ認証用にこの PKI トラストポイントに関連付けられた証明書を使用します。
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）応答またはサーバ証明書と共に OCSP Stapling を送信します。 （注） デフォルトでは、このコマンドの「no」形式で設定され、OCSP 応答はサーバ証明書と共に送信されません。
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 モードを開始します。

ユーザ認証用のユーザのデジタル証明書を検証する IOS SSH サーバの設定

手順の概要

1. **enable**
2. **configureterminal**
3. **ip ssh server algorithm authentication** {**publickey** | **keyboard** | **password**}
4. **ip ssh server algorithm publickey** {**x509v3-ssh-rsa** [**ssh-rsa**] | **ssh-rsa** [**x509v3-ssh-rsa**]}
5. **ip ssh server certificate profile**
6. **user**
7. **trustpoint verify***PKI-trustpoint-name*
8. **ocsp-response required**
9. **end**

手順の詳細

	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 モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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。設定されたアルゴリズムのみ、Secure Shell（SSH）クライアントとネゴシエートされます。 （注） IOS SSH サーバでは、少なくとも 1 つ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** コマンドを置き換えます。

	コマンドまたはアクション	目的
ステップ 4	**ip ssh server algorithm publickey** {**x509v3-ssh-rsa** [**ssh-rsa**] | **ssh-rsa** [**x509v3-ssh-rsa**]} 例： `Device(config)# ip ssh server algorithm publickey x509v3-ssh-rsa`	公開キー アルゴリズムの順序を定義します。設定されたアルゴリズムのみ、ユーザ認証のために SSH クライアントで受け入れられます。 （注） IOS SSH クライアントには、少なくとも 1 つの設定済みの公開キー アルゴリズムが必要です。 • ssh-rsa：公開キーによる認証 • x509v3-ssh-rsa：証明書ベースの認証
ステップ 5	**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の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	**user** 例： `Device(ssh-server-cert-profile)# user`	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。
ステップ 7	**trustpoint verify***PKI-trustpoint-name* 例： `Device(ssh-server-cert-profile-user)# trustpoint verify trust2`	受信するユーザ証明書を確認するために使用される公開キーインフラストラクチャ（PKI）のトラストポイントを設定します。 （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。
ステップ 8	**ocsp-response required** 例： `Device(ssh-server-cert-profile-user)# ocsp-response required`	（任意）受信するユーザ証明書と共に Online Certificate Status Protocol（OCSP）の応答の存在は必須です。 （注） デフォルトでは、このコマンドの「no」形式で設定され、ユーザ証明書は OCSP 応答なしで受け入れられます。
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設定モードを終了し、特権 EXEC モードを開始します。

サーバの設定と、デジタル証明書を使用したユーザ認証の確認

手順の概要

1. **enable**
2. **show ip ssh**

手順の詳細

ステップ 1 **enable**

特権 EXEC モードをイネーブルにします。

- パスワードを入力します（要求された場合）。

例：

```
Device> enable
```

ステップ 2 **show ip ssh**

現在設定されている認証方法を表示します。証明書ベースの認証を使用していることを確認するために、x509v3 ssh rsaアルゴリズムがホスト キー アルゴリズムに設定されているようにします。

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
```

SSH 認証の X.509v3 証明書の設定例

例：サーバ認証用のデジタル証明書を使用する IOS SSH サーバの設定

```
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)# exit
```

例：ユーザ認証のためのユーザのデジタル証明書を検証する IOS SSH サーバの設定

```
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 認証の X.509v3 証明書に関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
セキュリティ コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』 • 『Cisco IOS Security Command Reference: Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference: Commands S to Z』
SSH 認証	『*Secure Shell Configuration Guide*』の「Secure Shell-Configuring User Authentication Methods」の章
公開キー インフラストラクチャ（PKI）のトラストポイント	『*Public Key Infrastructure Configuration Guide*』の「Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment」の章

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

SSH 認証の X.509v3 証明書 の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、に進みます。Cisco.com のアカウントは必要ありません。

表 *1*：*SSH* 認証の *X.509v3* 証明書 の機能情報

機能名	リリース	機能情報
SSH 認証の X.509v3 証明書	Cisco IOS XE リリース 3.14S	SSH 認証の X.509v3 証明書 機能はサーバで 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。 次のコマンドが導入または変更されました。 **ip ssh server algorithm hostkey**、**ip ssh server algorithm authentication**、および **ip ssh server certificate profile**