SSH 認証の X.509v3 証明書

SSH 認証の X.509v3 証明書

セキュアシェル（SSH）認証用の 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。

SSH 認証用のデジタル証明書の前提条件

SSH 認証用のデジタル証明書機能では、**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 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 認証用の X.509v3 証明書には、次の制限事項が適用されます。

- SSH 認証の X.509v3 証明書機能の実装は、IOS セキュア シェル（SSH）サーバ側にのみ適用できます。

- IOS SSH サーバは、IOS SSH サーバ側の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 証明書は、次の条件で失敗します。

- ルート認証機関がデバイスのトラストポイントとして設定されている場合。
- クライアントが、クライアント証明書、サブ CA 証明書、自己署名ルート認証局を含む自己署名ルート認証局につながる証明書チェーンを渡す場合。
- サブ CA 証明書がデバイスのトラストポイントとして設定されているが、ユーザ証明書のトラストポイントとして含まれていない場合。

SSH 認証用の X.509v3 証明書に関する情報

次の項では、デジタル証明書、サーバおよびユーザ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、IOS セキュア シェル（SSH）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 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、IOS SSH サーバ端末でサーバおよびユーザに対して有効になっています。

SSH 認証用の X.509v3 証明書の設定方法

次の項では、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 IOS SSH サーバの設定

次の項では、IOS SSH サーバがサーバ認証用にデジタル証明書を使用するための設定について説明します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `デバイス> 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	**configure terminal** 例： `デバイス# 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： `デバイス(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。 • 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： `デバイス(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：	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

	コマンドまたはアクション	目的
	デバイス(ssh-server-cert-profile)# **server**	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： デバイス (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： デバイス (ssh-server-cert-profile-server)# **ocsp-response include**	（任意）Online Certificate Status Protocol（OCSP）の応答または OCSP ステープ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は送信されません。
ステップ 8	**end** 例： デバイス (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確認するためのIOSSSHサーバの設定

次の項では、IOS SSH サーバがユーザ認証用にユーザのデジタル証明書を確認するための設定について説明します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： デバイス> **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	**configure terminal** 例：	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。

	コマンドまたはアクション	目的
	デバイス# **configure terminal**	
ステップ 3	**ip ssh server algorithm authentication** {**publickey** | **keyboard** | **password**} 例： デバイス(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） • IOS 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。 • 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。 • **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。
ステップ 4	**ip ssh server algorithm publickey** {**x509v3-ssh-rsa** [**ssh-rsa**] | **ssh-rsa** [**x509v3-ssh-rsa**]} 例： デバイス(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。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。 （注） IOS 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。 • 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	**ip ssh server certificate profile** 例： デバイス(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。

	コマンドまたはアクション	目的
ステップ 6	**user** 例： `デバイス(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： `デバイス (ssh-server-cert-profile-user)#trustpoint verify trust2`	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。 （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： `デバイス(ssh-server-cert-profile-user)# ocsp-response required`	（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。 （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。
ステップ 9	**end** 例： `デバイス (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 モードを開始します。

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

次の項では、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について説明します。

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	**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

次の項では、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 IOS 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 IOS 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)# exit
```

例：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IOSSSH 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 IOS 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 認証の X.509v3 証明書に関するその他の参考資料

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	『セキュア シェル コンフィギュレーション ガイド』の「セキュア シェル：ユーザ認証方式の設定」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、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。

表 *1 : SSH* 認証用の *X.509v3* 証明書の機能情報

機能情報	リリース	変更内容
SSH 認証の X.509v3 証明書	Cisco IOS XE Denali 16.1.x	SSH 認証用の 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。