セキュア シェル：ユーザー認証方式の設定

セキュア シェル：ユーザー認証方式の設定機能によって、セキュア シェル（SSH）サーバーで使用可能なユーザー認証方式を設定できます。

セキュア シェルの制約事項：ユーザー認証方式の設定

セキュア シェル（SSH）サーバーと SSH クライアントは、データ暗号化ソフトウェア（DES）（56 ビット）および 3DES（168 ビット）イメージでのみサポートされます。

セキュア シェルに関する情報：ユーザー認証方式の設定

セキュア シェル ユーザー認証の概要

セキュア シェル（SSH）を使用することによって、SSH クライアントはシスコデバイス（Cisco IOS SSH サーバー）に対してセキュアで暗号化された接続を確立できます。SSH クライアントは SSH プロトコルを使用して、デバイス認証と暗号化を実行します。

SSH サーバーは、3 種類のユーザー認証方式をサポートし、これらの認証方式を事前に定義された次の順序で SSH クライアントに送信します。

- 公開キー認証方式

- キーボード インタラクティブ認証方式
- パスワード認証方式

デフォルトでは、すべてのユーザー認証方式が有効になっています。無効な方式が SSH ユーザー認証プロトコルでネゴシエートされないように特定のユーザー認証を無効にするには、**no ip ssh server authenticate user** {**publickey** | **keyboard** | **pasword**} コマンドを使用します。この機能によって、SSHサーバーは、事前に定義された順序とは異なる順序で希望のユーザー認証方式を指定できます。**ip ssh server authenticate user** {**publickey** | **keyboard** | **pasword**} コマンドを使用すると、無効になっているユーザー認証方式を有効にできます。

RFC 4252（セキュア シェル（SSH）認証プロトコル）のとおり、公開キー認証方式は必須です。この機能によって、SSH サーバーで RFC の動作をオーバーライドして、公開キー認証を含む任意の SSH ユーザー認証方式を無効にすることができます。

たとえば、SSHサーバーでパスワード認証方式を希望する場合、SSHサーバーで公開キー認証方式とキーボードインタラクティブ認証方式を無効にすることができます。

セキュアシェルの設定方法：ユーザー認証方式の設定方法

SSH サーバーのユーザー認証の設定

このタスクを実行して、セキュア シェル（SSH）サーバーでのユーザー認証方式を設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **no ip ssh server authenticate user** {**publickey** | **keyboard** | **pasword**}
4. **ip ssh server authenticate user** {**publickey** | **keyboard** | **pasword**}
5. **default ip ssh server authenticate user**
6. **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	**no ip ssh server authenticate user** {**publickey** | **keyboard** | **pasword**}
	例：
	`Device(config)# no ip ssh server authenticate user publickey`
	`%SSH:Publickey disabled.Overriding RFC`
		セキュア シェル（SSH）サーバーでユーザー認証方式を無効にします。
		（注） **no ip ssh server authenticate user publickey** コマンドを使用して公開キー認証を無効にすると、警告メッセージが表示されます。このコマンドは、公開キー認証が必須であることが明記されている RFC 4252（セキュア シェル（SSH）認証プロトコル）の動作をオーバーライドします。

ステップ 4	**ip ssh server authenticate user** {**publickey** | **keyboard** | **pasword**} 例： `Device(config)# ip ssh server authenticate user publickey`	SSH サーバーで無効になっているユーザー認証方法を有効にします。
ステップ 5	**default ip ssh server authenticate user** 例： `Device(config)# default ip ssh server authenticate user`	すべてのユーザー認証方式が事前に定義された順序で有効になっているデフォルトの動作に戻ります。
ステップ 6	**end** 例： `Device(config)# end`	グローバル 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。

トラブルシューティングのヒント

- **no ip ssh server authenticate user publickey** コマンドを使用して公開キーベースの認証方式を無効にすると、公開キー認証が必須の RFC 4252（セキュア シェル（SSH）認証プロトコル）の動作がオーバーライドされ、次の警告メッセージが表示されます。

  `%SSH:Publickey disabled.Overriding RFC`

- 3 つすべての認証方式が無効になっている場合、次の警告メッセージが表示されます。

  `%SSH:No auth method configured.Incoming connection will be dropped`

- 3 つすべての認証方式が SSH サーバーで無効になっているときに SSH クライアントから SSH セッション要求を受信した場合、接続要求は SSH サーバーでドロップされ、次の形式でシステム ログ メッセージが表示されます。

```
%SSH-3-NO_USERAUTH: No auth method configured for SSH Server. Incoming connection
from <ip address> (tty = <ttynum>) dropped
```

SSH サーバーのユーザー認証の確認

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 モードを有効にします。

- 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

セキュア シェル（SSH）のバージョンおよび設定データを表示します。

例：

次の **show ip ssh** コマンドの出力例では、3 つすべてのユーザー認証方式が SSH サーバーで有効になっていることを確認します。

```
Device# show ip ssh

Authentication methods:publickey,keyboard-interactive,password
```

次の **show ip ssh** コマンドの出力例では、3 つすべてのユーザー認証方式が SSH サーバーで無効になっていることを確認します。

```
Device# show ip ssh

Authentication methods:NONE
```

セキュア シェルの設定例：ユーザー認証方式の設定

例：ユーザー認証方式の無効化

次の例では、公開キーベースの認証方式およびキーボードベースの認証方式を無効にし、パスワードベースの認証方式を使用して SSH クライアントが SSH サーバーに接続できるようにする方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# no ip ssh server authenticate user publickey
%SSH:Publickey disabled.Overriding RFC
Device(config)# no ip ssh server authenticate user keyboard
Device(config)# exit
```

例：ユーザー認証方式の有効化

次の例では、公開キーベースの認証方式およびキーボードベースの認証方式を有効にする方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# ip ssh server authenticate user publickey
Device(config)# ip ssh server authenticate user keyboard
Device(config)# exit
```

例：デフォルトのユーザー認証方式の設定

次の例では、3 つすべてのユーザー認証方式が事前に定義された順序で有効になっているデフォルトの動作に戻す方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# default ip ssh server authenticate user
Device(config)# exit
```

セキュア シェルの追加情報：ユーザー認証方式の設定

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 の設定	『セキュア シェル コンフィギュレーション ガイド』

標準および RFC

標準/RFC	タイトル
RFC 4252	『セキュア シェル（*SSH*）認証プロトコル』
RFC 4253	『セキュア シェル（*SSH*）トランスポート層プロトコル』

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/support

セキュア シェルの機能情報：ユーザー認証方式の設定

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:* セキュア シェルの機能情報：ユーザー認証方式の設定

機能名	リリース	機能情報
セキュア シェル：ユーザー認証方式の設定	Cisco IOS XE Release 3.10S	セキュア シェル：ユーザー認証方式の設定機能によって、セキュア シェル（SSH）サーバーで使用可能なユーザー認証方式を設定できます。 次のコマンドが導入されました：**ip ssh server authenticate user**。 この機能は、Cisco IOS XE Release3.10 で、Cisco ASR 1000 シリーズアグリゲーション サービス ルータに導入されました。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。