



# コモンクライテリア認定用の SSH アルゴリズム

- [コモンクライテリア認証のための SSH アルゴリズムの制限 \(1 ページ\)](#)
- [コモンクライテリア認定用の SSH アルゴリズムに関する情報 \(1 ページ\)](#)
- [コモンクライテリア認定用の SSH アルゴリズムの設定方法 \(3 ページ\)](#)
- [コモンクライテリア認定用の SSH アルゴリズムの設定例 \(8 ページ\)](#)
- [コモンクライテリア認定用の SSH アルゴリズムの確認 \(9 ページ\)](#)
- [コモンクライテリア認定用のセキュアシェルアルゴリズムの機能情報 \(10 ページ\)](#)

## コモンクライテリア認証のための SSH アルゴリズムの制限

Cisco IOS XE Amsterdam 17.1.1 以降、SHA1 はサポートされません。

## コモンクライテリア認定用の SSH アルゴリズムに関する情報

ここでは、コモンクライテリア認定のセキュアシェル (SSH) アルゴリズム、Cisco IOS SSH サーバーアルゴリズム、および Cisco IOS SSH クライアントアルゴリズムについて説明します。

## コモンクライテリア認定用の SSH アルゴリズム

セキュアシェル (SSH) 設定によって、Cisco IOS SSH サーバーおよびクライアントは、許可リストから設定されたアルゴリズムのネゴシエーションのみを許可することができます。リモートパーティが許可リストに含まれていないアルゴリズムのみを使用してネゴシエートしようとする、要求は拒否され、セッションは確立されません。

## Cisco IOS SSH サーバー アルゴリズム

Cisco IOS セキュア シェル (SSH) サーバーは、次の順序で暗号化アルゴリズム (Advanced Encryption Standard カウンタ モード [AES-CTR]、AES 暗号ブロック連鎖 [AES-CBC]、Triple Data Encryption Standard [3DES]) をサポートします。

サポートされるデフォルトの暗号化の順序 :

1. aes128-gcm
2. aes256-gcm
3. aes128-ctr
4. aes192-ctr
5. aes256-ctr

サポートされるデフォルト以外の暗号化の順序 :

1. aes128-cbc
2. aes192-cbc
3. aes256-cbc
4. 3des

Cisco IOS SSH クライアントは、次の順序でメッセージ認証コード (MAC) アルゴリズムをサポートします。

サポートされるデフォルトの HMAC の順序 :

1. hmac-sha2-256
2. hmac-sha2-512

Cisco IOS SSH クライアントがサポートするホストキーアルゴリズムは 1 つのみで、CLI 設定は必要ありません。

サポートされるデフォルトのホストキーの順序 :

1. x509v3-ssh-rsa
2. ssh-rsa

## Cisco IOS SSH クライアント アルゴリズム

Cisco IOS セキュア シェル (SSH) クライアントは、次の順序で暗号化アルゴリズム (Advanced Encryption Standard カウンタ モード [AES-CTR]、AES 暗号ブロック連鎖 [AES-CBC]、Triple Data Encryption Standard [3DES]) をサポートします。

サポートされるデフォルトの暗号化の順序 :

1. aes128-gcm

2. aes256-gcm
3. aes128-ctr
4. aes192-ctr
5. aes256-ctr

サポートされるデフォルト以外の暗号化の順序：

1. aes128-cbc
2. aes192-cbc
3. aes256-cbc
4. 3des

Cisco IOS SSH クライアントは、次の順序でメッセージ認証コード（MAC）アルゴリズムをサポートします。

サポートされるデフォルトの HMAC の順序：

1. hmac-sha2-256
2. hmac-sha2-512

Cisco IOS SSH クライアントがサポートするホストキーアルゴリズムは1つのみで、CLI 設定は必要ありません。

サポートされるデフォルトのホストキーの順序：

1. x509v3-ssh-rsa
2. ssh-rsa

## コモンクライテリア認定用の SSH アルゴリズムの設定方法

ここでは、設定とトラブルシューティング方法に関する情報を提供します。

- Cisco IOS SSH サーバーおよびクライアントの暗号キーアルゴリズム
- Cisco IOS SSH サーバーおよびクライアントの MAC アルゴリズム
- Cisco IOS SSH サーバーのホストキーアルゴリズム

# Cisco IOS SSH サーバーおよびクライアントの暗号キー アルゴリズムの設定

手順

	コマンドまたはアクション	目的
ステップ 1	<p><b>enable</b></p> <p>例 :</p> <pre>Device&gt; enable</pre>	<p>特権 EXEC モードを有効にします。</p> <p>パスワードを入力します (要求された場合)。</p>
ステップ 2	<p><b>configure terminal</b></p> <p>例 :</p> <pre>Device# configure terminal</pre>	<p>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。</p>
ステップ 3	<p><b>ip ssh {server   client} algorithm encryption {aes128-gcm   aes256-gcm   aes128-ctr   aes192-ctr   aes256-ctr   aes128cbc   aes192-cbc   3des}</b></p> <p>例 :</p> <pre>Device(config)# ip ssh server algorithm encryption aes128-gcm aes256-gcm aes128-ctr aes192-ctr aes256-ctr aes128-cbc aes192-cbc aes256-cbc 3des</pre> <pre>Device(config)# ip ssh client algorithm encryption aes128-gcm aes256-gcm aes128-ctr aes192-ctr aes256-ctr aes128-cbc aes192-cbc aes256-cbc 3des</pre>	<p>SSH サーバーおよびクライアントでの暗号化アルゴリズムの順序を定義します。この順序は、アルゴリズムのネゴシエーション時に指定されます。</p> <p>(注) Cisco IOS SSH サーバーおよびクライアントには、1つ以上の設定済み暗号化アルゴリズムが必要です。</p> <p>(注) 以前設定したアルゴリズムのリストから1つのアルゴリズムを無効にするには、このコマンドの <b>no</b> 形式を使用します。複数のアルゴリズムを無効にするには、このコマンドの <b>no</b> 形式を異なるアルゴリズム名で複数回使用します。</p>

	コマンドまたはアクション	目的
		<p>(注) デフォルト設定では、次に示すようにこのコマンドのデフォルト形式を使用します。</p> <pre>Device(config)# ip ssh server algorithm encryption aes128-gcm aes256-gcm aes128-ctr aes192-ctr aes256-ctr aes128-cbc aes192-cbc aes256-cbc 3des</pre>
ステップ 4	<p><b>end</b></p> <p>例 :</p> <pre>Device(config)# end</pre>	<p>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。</p>

## トラブルシューティングのヒント

設定で最後の暗号化アルゴリズムを無効にしようとする、次のメッセージが表示されてコマンドが拒否されます。

```
% SSH command rejected: All encryption algorithms cannot be disabled
```

## Cisco IOS SSH サーバーおよびクライアントの MAC アルゴリズムの設定

### 手順

	コマンドまたはアクション	目的
ステップ 1	<p><b>enable</b></p> <p>例 :</p> <pre>Device&gt; enable</pre>	<p>特権 EXEC モードを有効にします。</p> <ul style="list-style-type: none"> <li>パスワードを入力します (要求された場合)。</li> </ul>
ステップ 2	<p><b>configure terminal</b></p> <p>例 :</p> <pre>Device# configure terminal</pre>	<p>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。</p>
ステップ 3	<p><b>ip ssh {server   client} algorithm mac {hmac-sha2-256-etm   hmac-sha2-512-etm   hmac-sha2-256   hmac-sha2-512 }</b></p>	<p>SSH サーバーおよびクライアントでの MAC (メッセージ認証コード) アルゴ</p>

	コマンドまたはアクション	目的
	<p>例 :</p> <pre>Device(config)# ip ssh server algorithm mac hmac-sha2-256-etm hmac-sha2-512-etm hmac-sha2-256 hmac-sha2-512</pre> <pre>Device(config)# ip ssh client algorithm mac hmac-sha2-256-etm hmac-sha2-512-etm hmac-sha2-256 hmac-sha2-512</pre>	<p>リズムの順序を定義します。この順序は、アルゴリズムのネゴシエーション時に指定されます。</p> <p>(注) Cisco IOS SSH サーバーおよびクライアントには、1つ以上の設定済みハッシュメッセージ認証コード (HMAC) アルゴリズムが必要です。</p> <p>(注) 以前設定したアルゴリズムのリストから1つのアルゴリズムを無効にするには、このコマンドの <b>no</b> 形式を使用します。複数のアルゴリズムを無効にするには、このコマンドの <b>no</b> 形式を異なるアルゴリズム名で複数回使用します。</p> <p>(注) デフォルト設定では、次に示すようにこのコマンドのデフォルト形式を使用します。</p> <pre>Device(config)# ip ssh server algorithm mac hmac-sha2-256-etm hmac-sha2-512-etm hmac-sha2-256 hmac-sha2-512</pre>
<p>ステップ 4</p>	<p><b>end</b></p> <p>例 :</p> <pre>Device(config)# end</pre>	<p>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。</p>

## トラブルシューティングのヒント

設定で最後の MAC アルゴリズムを無効にしようとするすると、次のメッセージが表示されてコマンドが拒否されます。

```
% SSH command rejected: All mac algorithms cannot be disabled
```

## Cisco IOS SSH サーバーのホストキー アルゴリズムの設定

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例 : Device> <b>enable</b>	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	<b>configure terminal</b> 例 : Device# <b>configure terminal</b>	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	<b>ip ssh server algorithm hostkey {x509v3-ssh-rsa  rsa-sha2-512 rsa-sha2-256ssh-rsa}</b> 例 : Device (config)# <b>ip ssh server algorithm hostkey x509v3-ssh-rsa rsa-sha2-512 rsa-sha2-256 ssh-rsa</b>	ホストキー アルゴリズムの順序を定義します。Cisco IOS 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) Cisco IOS SSH サーバーには、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"> <li>• x509v3-ssh-rsa : X.509v3 証明書ベース認証</li> <li>• ssh-rsa : 公開キーベース認証</li> </ul> (注) 以前設定したアルゴリズムのリストから 1つのアルゴリズムを無効にするには、このコマンドの <b>no</b> 形式を使用します。複数のアルゴリズムを無効にするには、このコマンドの <b>no</b> 形式を異なるアルゴリズム名で複数回使用します。

	コマンドまたはアクション	目的
		<p>(注) デフォルト設定では、次に示すようにこのコマンドのデフォルト形式を使用します。</p> <pre>Device(config)# ip ssh server algorithm hostkey x509v3-ssh-rsa rsa-sha2-512 rsa-sha2-256 ssh-rsa</pre>
ステップ 4	<p><b>end</b></p> <p>例 :</p> <pre>Device(config)# end</pre>	<p>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。</p>

## トラブルシューティングのヒント

設定で最後のホストキー アルゴリズムを無効にしようとすると、次のメッセージが表示されてコマンドが拒否されます。

```
% SSH command rejected: All hostkey algorithms cannot be disabled
```

## コモンクライテリア認定用の SSH アルゴリズムの設定例

ここでは、コモン認定用の SSH アルゴリズムの設定例を示します。

### 例 : Cisco IOS SSH サーバーの暗号キー アルゴリズムの設定

```
Device> enable
Device# configure terminal
Device(config)# ip ssh server algorithm encryption aes128-ctr aes192-ctr aes256-ctr
aes128-cbc aes192-cbc aes256-cbc 3des
Device(config)# end
```

### 例 : Cisco IOS SSH クライアントの暗号キー アルゴリズムの設定

```
Device> enable
Device# configure terminal
Device(config)# ip ssh client algorithm encryption aes128-ctr aes192-ctr aes256-ctr
aes128-cbc aes192-cbc aes256-cbc 3des
```



```
Device(config)# end
```

## 例 : Cisco IOS SSH サーバーの MAC アルゴリズムの設定

```
Device> enable
Device# configure terminal
Device(config)# ip ssh server algorithm mac hmac-sha2-256-etm hmac-sha2-512-etm
hmac-sha2-256 hmac-sha2-512
Device(config)# end
```

## 例 : Cisco IOS SSH サーバーのホストキー アルゴリズムの設定

```
Device> enable
Device# configure terminal
Device(config)# ip ssh server algorithm hostkey x509v3-ssh-rsa rsa-sha2-512 rsa-sha2-256
ssh-rsaa
Device(config)# end
```

# コモンクライテリア認定用の SSH アルゴリズムの確認

### 手順

---

#### 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

設定済みのセキュアシェル (SSH) 暗号化、ホストキー、およびメッセージ認証コード (MAC) アルゴリズムを表示します。

例 :

次の **show ip ssh** コマンドの出力例は、デフォルトの順序で設定された暗号化アルゴリズムを示しています。

```
Device# show ip ssh
```

```
Encryption Algorithms: aes128-ctr aes192-ctr aes256-ctr aes128-cbc aes192-cbc aes256-cbc
3des
```

次の **show ip ssh** コマンドの出力例は、デフォルトの順序で設定された MAC アルゴリズムを示しています。

```
Device# show ip ssh
```

```
MAC Algorithms: hmac-sha2-256, hmac-sha2-512
```

次の **show ip ssh** コマンドの出力例は、デフォルトの順序で設定されたホストキー アルゴリズムを示しています。

```
Device# show ip ssh
```

```
Hostkey Algorithms: x509v3-ssh-rsa, ssh-rsa
```

## コモンクライテリア認定用のセキュアシェルアルゴリズムの機能情報

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 Everest 16.5.1a	コモンクライテリア認定用のセキュアシェルアルゴリズム	コモンクライテリア認定用の SSH アルゴリズム機能によって、コモンクライテリア認定を取得したアルゴリズムのリストおよび順序が提供されます。このモジュールでは、認定されたアルゴリズムのリストに基づいて SSH 接続を制限できるように、セキュアシェル (SSH) サーバーおよびクライアントの暗号化、メッセージ認証コード (MAC)、およびホストキーアルゴリズムの設定方法について説明します。

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> [英語] からアクセスします。

## 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。