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。

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 リリース 17.10 以降、次のキー交換および MAC アルゴリズムがデフォルトのリストから削除されました。

  キー交換アルゴリズム：

  - diffie-hellman-group14-sha1

  MAC アルゴリズム：

  - hmac-sha1
  - hmac-sha2-256
  - hmac-sha2-512

（注） **ip ssh server algorithm kex** コマンドを使用するとキー交換アルゴリズムを設定でき、**ip ssh server algorithm mac** コマンドを使用すると MAC アルゴリズムを設定できます。

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

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と、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]、Galois/Counter Mode [GCM]）、メッセージ認証コード（MAC）アルゴリズム、ホストキーアルゴリズム、キー交換（KEX）DH グループアルゴリズム、および公開キーアルゴリズムをサポートします。

表 *1:* サポートされるデフォルトおよびデフォルト以外の *IOS SSH* サーバーアルゴリズム

サポートされるアルゴリズム	デフォルト	非デフォルト
暗号化	**1.** chacha20-poly1305@openssh.com **2.** aes128-gcm@openssh.com **3.** aes256-gcm@openssh.com **4.** aes128-gcm **5.** aes256-gcm **6.** aes128-ctr **7.** aes192-ctr **8.** aes256-ctr	• aes128-cbc • aes192-cbc • aes256-cbc • 3des-cbc

サポートされるアルゴリズム	デフォルト	非デフォルト
HMAC	1. hmac-sha2-256-etm@openssh.com 2. hmac-sha2-512-etm@openssh.com	• hmac-sha1 • hmac-sha2-256 • hmac-sha2-512
ホストキー	1. rsa-sha2-512 2. rsa-sha2-256 3. ssh-rsa	• x509v3-ssh-rsa
KEX DH グループ	1. curve25519-sha256 2. curve25519-sha256@libssh.org 3. ecdh-sha2-nistp256 4. ecdh-sha2-nistp384 5. ecdh-sha2-nistp521 6. diffie-hellman-group14-sha256 7. diffie-hellman-group16-sha512	• diffie-hellman-group14-sha1
公開キー	1. ssh-rsa 2. ecdsa-sha2-nistp256 3. ecdsa-sha2-nistp384 4. ecdsa-sha2-nistp521 5. ssh-ed25519 6. x509v3-ecdsa-sha2-nistp256 7. x509v3-ecdsa-sha2-nistp384 8. x509v3-ecdsa-sha2-nistp521 9. rsa-sha2-256 10. rsa-sha2-512 11. x509v3-rsa2048-sha256	• x509v3-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]、Galois/Counter Mode (GCM)）、MAC アルゴリズム、および KEX DH グループアルゴリズムをサポートします。

表 *2:* サポートされるデフォルトおよびデフォルト以外の *IOS SSH* サーバーアルゴリズム

サポートされるアルゴリズム	デフォルト	非デフォルト
暗号化	**1.** chacha20-poly1305@openssh.com **2.** aes128-gcm@openssh.com **3.** aes256-gcm@openssh.com **4.** aes128-gcm **5.** aes256-gcm **6.** aes128-ctr **7.** aes192-ctr **8.** aes256-ctr	• aes128-cbc • aes192-cbc • aes256-cbc • 3des-cbc
HMAC	**1.** hmac-sha2-256-etm@openssh.com **2.** hmac-sha2-512-etm@openssh.com	• hmac-sha1 • hmac-sha2-256 • hmac-sha2-512
KEX DH グループ	**1.** curve25519-sha256 **2.** curve25519-sha256@libssh.org **3.** ecdh-sha2-nistp256 **4.** ecdh-sha2-nistp384 **5.** ecdh-sha2-nistp521 **6.** diffie-hellman-group14-sha256 **7.** diffie-hellman-group16-sha512	• diffie-hellman-group14-sha1

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

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

手順の概要

1. **enable**
2. **configure terminal**
3. **ip ssh** {**server** | **client**} **algorithm encryption** {**aes128-ctr** | **aes192-ctr** | **aes256-ctr** | **aes128-cbc** | **3des-cbc** | **aes192-cbc** | **aes256-cbc**}
4. **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）。
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**	**client**} **algorithm encryption** {**aes128-ctr**	**aes192-ctr**	**aes256-ctr**	**aes128-cbc**	**3des-cbc**	**aes192-cbc**	**aes256-cbc**}
								例：
								`Device(config)# ip ssh server algorithm encryption aes128-ctr aes192-ctr aes256-ctr aes128-cbc 3des-cbc aes192-cbc aes256-cbc`
								`Device(config)# ip ssh client algorithm encryption aes128-ctr aes192-ctr aes256-ctr aes128-cbc 3des-cbc aes192-cbc aes256-cbc`
									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。
									（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。
									（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 **no** 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 **no** 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
		（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。 `Device(config)# ip ssh server algorithm encryption aes128-ctr aes192-ctr aes256-ctr aes128-cbc 3des-cbc aes192-cbc aes256-cbc`
ステップ 4	**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

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 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	**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	**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** | **client**} **algorithm mac** {**hmac-sha2** | **hmac-sha2-96**} 例：	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。

	コマンドまたはアクション	目的

	`Device(config)# ip ssh server algorithm mac hmac-sha2 hmac-sha2-96`
	
	`Device(config)# ip ssh client algorithm mac hmac-sha2 hmac-sha2-96`
		（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。
		
		（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 **no** 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 **no** 形式を異なるアルゴリズム名で複数回使用します。
		
		（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。
		
		`Device(config)# ip ssh server algorithm mac hmac-sha2 hmac-sha2-96`

ステップ 4	**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

設定で最後の MAC 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 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

手順の概要

1. **enable**
2. **configure terminal**
3. **ip ssh server algorithm hostkey** {**x509v3-ssh-rsa** | **ssh-rsa**}
4. **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）。
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**} 例： `Device(config)# ip ssh server algorithm hostkey x509v3-ssh-rsa ssh-rsa`	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。 • x509v3-ssh-rsa：X.509v3 証明書ベース認証 • ssh-rsa：公開キーベース認証 （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 **no** 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 **no** 形式を異なるアルゴリズム名で複数回使用します。 （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。 `Device(config)# ip ssh server algorithm hostkey x509v3-ssh-rsa ssh-rsa`
ステップ 4	**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

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**

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, 3des-cbc, aes192-cbc, aes256-cbc
```

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-sha1 hmac-sha1-96
```

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 SSH アルゴリズムの設定例

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 3des-cbc aes192-cbc aes256-cbc
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 3des-cbc aes192-cbc aes256-cbc
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-sha1 hmac-sha1-96
Device(config)# end
```

例：Cisco IOS SSH サーバー用のキー交換 DH グループの設定

```
Device> enable
Device# configure terminal
Device(config)# ip ssh server algorithm kex diffie-hellman-group-exchange-sha1
```

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

```
Device> enable
Device# configure terminal
Device(config)# ip ssh server algorithm kex diffie-hellman-group14-sha1
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 ssh-rsa
Device(config)# end
```

コモンクライテリア認定用のSSHアルゴリズムの追加情報

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』[英語] • 『Cisco IOS Security Command Reference: Commands D to L』[英語] • 『Cisco IOS Security Command Reference: Commands M to R』[英語] • 『Cisco IOS Security Command Reference: Commands S to Z』[英語]
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：ユーザー認証方式の設定」の章
サーバーおよびユーザー認証での X.509v3 デジタル証明書	『セキュア シェル コンフィギュレーション ガイド』の「SSH 認証の X.509v3 証明書」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

コモンクライテリア認定用のSSH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 *3:* コモン クライテリア認定用の *SSH* アルゴリズムの機能情報

機能名	リリース	機能情報
コモン クライテリア認定用の SSH アルゴリズム	Cisco IOS XE Everest 16.5.1a	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。 この機能により、次のコマンドが導入されました：**ip ssh** {**server** | **client**} **algorithm encryption**、**ip ssh** {**server** | **client**} **algorithm mac**。
コモン クライテリア認定用の SSH アルゴリズム	Cisco IOS XE Cupertino 17.8.1	次のアルゴリズムに対する Cisco IOS SSH サーバーおよびクライアントのサポートが導入されました。 • chacha20-poly1305@openssh.com • ssh-ed25519 • curve25519-sha256@libssh.org
コモン クライテリア認定用の SSH アルゴリズム	Cisco IOS XE Cupertino 17.9.1	次のアルゴリズムに対する Cisco IOS SSH サーバーおよびクライアントのサポートが導入されました。 • aes128-gcm@openssh.com • aes256-gcm@openssh.com

弱い暗号の廃止	Cisco IOS XE リリース 17.10	次の変更が導入されました。
		• セキュアシェルバージョン 1.99 は、サポートされません。
		• 次の弱いキー交換および MAC アルゴリズムは、アルゴリズムのデフォルトリストから削除されます。
		  • diffie-hellman-group14-sha1
		  • hmac-sha1
		  • hmac-sha2-256
		  • hmac-sha2-512

機能名	リリース	機能情報
コモン クライテリア認定用の SSH アルゴリズム	Cisco IOS XE リリース 17.11.1a	次のアルゴリズムに対する Cisco IOS SSH サーバーおよびクライアントのサポートが導入されました。 • curve25519-sha256 • diffie-hellman-group14-sha256 • diffie-hellman-group16-sha512 • x509v3-rsa2048-sha256

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。