

# Cisco Web セキュリティアプライアンス向け AsyncOS 11.8 の暗号リスト

初版：2021 年 10 月 1 日

## Cisco Web セキュリティアプライアンスについて

Cisco Web セキュリティアプライアンスはインターネットトラフィックを代行受信してモニターし、ポリシーを適用することによって、マルウェア、機密データの漏洩、生産性の低下などのインターネットベースの脅威から内部ネットワークを保護します。

## サポート対象の暗号方式

このセクションには、Cisco Web セキュリティアプライアンス向け AsyncOS のサポート対象の暗号（SSL と SSH）のリストが含まれています。

### ポート 8443（管理インターフェイス）

SSL V 3.0	TLS 1.0	TLS 1.1	TLS 1.2
ECDHE-RSA-AES256-SHA	ECDHE-RSA-AES256-SHA	ECDHE-RSA-AES256-SHA	ECDHE-RSA-AES256-GCM-SHA384
DHE-RSA-AES256-SHA	DHE-RSA-AES256-SHA	DHE-RSA-AES256-SHA	ECDHE-RSA-AES256-SHA384
DHE-RSA-CAMELLIA256-SHA	DHE-RSA-CAMELLIA256-SHA	DHE-RSA-CAMELLIA256-SHA	ECDHE-RSA-AES256-SHA
AES256-SHA	AES256-SHA	AES256-SHA	DHE-RSA-AES256-GCM-SHA384
CAMELLIA256-SHA	CAMELLIA256-SHA	CAMELLIA256-SHA	DHE-RSA-AES256-SHA256
ECDHE-RSA-AES128-SHA	ECDHE-RSA-AES128-SHA	ECDHE-RSA-AES128-SHA	DHE-RSA-AES256-SHA
DHE-RSA-AES128-SHA	DHE-RSA-AES128-SHA	DHE-RSA-AES128-SHA	DHE-RSA-CAMELLIA256-SHA
DHE-RSA-SEED-SHA	DHE-RSA-SEED-SHA	DHE-RSA-SEED-SHA	AES256-GCM-SHA384
DHE-RSA-CAMELLIA128-SHA	DHE-RSA-CAMELLIA128-SHA	DHE-RSA-CAMELLIA128-SHA	AES256-SHA256
AES128-SHA	AES128-SHA	AES128-SHA	AES256-SHA
SEED-SHA	SEED-SHA	SEED-SHA	CAMELLIA256-SHA
CAMELLIA128-SHA	CAMELLIA128-SHA	CAMELLIA128-SHA	ECDHE-RSA-AES128-GCM-SHA256
			ECDHE-RSA-AES128-SHA256
			ECDHE-RSA-AES128-SHA
			DHE-RSA-AES128-GCM-SHA256

SSL V 3.0	TLS 1.0	TLS 1.1	TLS 1.2
			DHE-RSA-AES128-SHA
			DHE-RSA-SEED-SHA
			DHE-RSA-CAMELLIA128-SHA
			AES128-GCM-SHA256
			AES128-SHA256
			AES128-SHA
			SEED-SHA
			CAMELLIA128-SHA

## ポート 443 (HTTPS プロキシサービス)

SSL V 3.0	TLS 1.0	TLS 1.1	TLS 1.2
DHE-RSA-AES256-SHA	DHE-RSA-AES256-SHA	DHE-RSA-AES256-SHA	DHE-RSA-AES256-GCM-SHA384
DHE-RSA-CAMELLIA256-SHA	DHE-RSA-CAMELLIA256-SHA	DHE-RSA-CAMELLIA256-SHA	DHE-RSA-AES256-SHA256
AES256-SHA	AES256-SHA	AES256-SHA	DHE-RSA-AES256-SHA
CAMELLIA256-SHA	CAMELLIA256-SHA	CAMELLIA256-SHA	DHE-RSA-AES128-GCM-SHA256
DHE-RSA-AES128-SHA	DHE-RSA-AES128-SHA	DHE-RSA-AES128-SHA	DHE-RSA-AES128-SHA
DHE-RSA-SEED-SHA	DHE-RSA-SEED-SHA	DHE-RSA-SEED-SHA	DHE-RSA-CAMELLIA256-SHA
DHE-RSA-CAMELLIA128-SHA	DHE-RSA-CAMELLIA128-SHA	DHE-RSA-CAMELLIA128-SHA	DHE-RSA-AES128-SHA256
AES128-SHA	AES128-SHA	AES128-SHA	SEED-SHA
SEED-SHA	SEED-SHA	SEED-SHA	CAMELLIA128-SHA
CAMELLIA128-SHA	CAMELLIA128-SHA	CAMELLIA128-SHA	CAMELLIA256-SHA
DHE-DSS-AES256-SHA	DHE-DSS-AES256-SHA	DHE-DSS-AES256-SHA	AES256-SHA
DHE-DSS-CAMELLIA256-SHA	DHE-DSS-CAMELLIA256-SHA	DHE-DSS-CAMELLIA256-SHA	AES128-SHA256
DHE-DSS-AES128-SHA	DHE-DSS-AES128-SHA	DHE-DSS-AES128-SHA	AES128-GCM-SHA256
DHE-DSS-SEED-SHA	DHE-DSS-SEED-SHA	DHE-DSS-SEED-SHA	AES256-SHA256
DHE-DSS-CAMELLIA128-SHA	DHE-DSS-CAMELLIA128-SHA	DHE-DSS-CAMELLIA128-SHA	AES256-GCM-SHA384
DES-CBC3-SHA	DES-CBC3-SHA	DES-CBC3-SHA	AES128-SHA
EDH-RSA-DES-CBC3-SHA	EDH-RSA-DES-CBC3-SHA	EDH-RSA-DES-CBC3-SHA	DHE-RSA-AES128-SHA
IDEA-CBC-SHA	IDEA-CBC-SHA	IDEA-CBC-SHA	DHE-RSA-SEED-SHA
ADH-AES128-SHA	ADH-AES128-SHA	ADH-AES128-SHA	DHE-RSA-CAMELLIA128-SHA
ADH-SEED-SHA	ADH-SEED-SHA	ADH-SEED-SHA	DES-CBC3-SHA

SSL V 3.0	TLS 1.0	TLS 1.1	TLS 1.2
ADH-CAMELLIA128-SHA	ADH-CAMELLIA128-SHA	ADH-CAMELLIA128-SHA	EDH-RSA-DES-CBC3-SHA
ADH-AES256-SHA	ADH-AES256-SHA	ADH-AES256-SHA	IDEA-CBC-SHA
ADH-CAMELLIA256-SHA	ADH-CAMELLIA256-SHA	ADH-CAMELLIA256-SHA	ADH-AES256-GCM-SHA384
ADH-DES-CBC3-SHA	ADH-DES-CBC3-SHA	ADH-DES-CBC3-SHA	ADH-AES256-SHA256
			ADH-AES256-SHA
			ADH-CAMELLIA256-SHA
			ADH-AES128-GCM-SHA256
			ADH-AES128-SHA256
			ADH-AES128-SHA
			ADH-SEED-SHA
			ADH-DES-CBC3-SHA
			ADH-CAMELLIA128-SHA
			DHE-DSS-AES256-GCM-SHA384
			DHE-DSS-AES256-SHA256
			DHE-DSS-AES256-SHA
			DHE-DSS-CAMELLIA256-SHA
			DHE-DSS-AES128-GCM-SHA256
			DHE-DSS-AES128-SHA256
			DHE-DSS-AES128-SHA
			DHE-DSS-SEED-SHA
			DHE-DSS-CAMELLIA128-SHA
デフォルト モード： AES128-SHA DHE-RSA-AES128-SHA	デフォルト モード： AES128-SHA DHE-RSA-AES128-SHA	デフォルト モード： AES128-SHA DHE-RSA-AES128-SHA	デフォルト モード： AES128-SHA256 AES128-GCM-SHA256 AES256-SHA256 AES256-GCM-SHA384 AES128-SHA DHE-RSA-AES128-SHA
(注) デフォルトモードは、Cisco Web セキュリティアプライアンスで設定された「SSL 暗号ストリング」でサポートされる暗号を表します。			
(注) AsyncOS 12.0.1 以降のバージョンでは、TLS 1.0、TLS 1.1、および TLS 1.2 の ECDHE 関連暗号がサポートされています。			

## ポート 22 (SSH ポート)

### OpenSSH\_7.3p1:

#### 1. key\_algorithm (7):

- diffie-hellman-group1-sha1
- diffie-hellman-group14-sha1
- diffie-hellman-group-exchange-sha1
- diffie-hellman-group-exchange-sha256
- ecdh-sha2-nistp256
- ecdh-sha2-nistp384
- ecdh-sha2-nistp521

#### 2. encryption\_algorithm (8): 3.mac\_algorithms (4):

- 3des-cbc
- aes128-cbc
- aes192-cbc
- aes256-cbc
- rijndael-cbc@lysator.liu.se
- aes128-ctr
- aes192-ctr
- aes256-ctr
- hmac-sha1
- hmac-ripemd160
- hmac-ripemd160@openssh.com
- umac-64@openssh.com

## サポート対象外の暗号方式

このセクションには、サポート対象外の暗号のリストが含まれています。

### ポート 8443 (管理インターフェイス)

SSL V 3.0	TLS 1.0
RC2-CBC-MD5	RC2-CBC-MD5
RC4-MD5	RC4-MD5
IDEA-CBC-MD5	IDEA-CBC-MD5
DES-CBC3-MD5	DES-CBC3-MD5

---

【注意】シスコ製品をご使用になる前に、安全上の注意（[www.cisco.com/jp/go/safety\\_warning/](http://www.cisco.com/jp/go/safety_warning/)）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

このマニュアルで使用しているIPアドレスと電話番号は、実際のアドレスと電話番号を示すものではありません。マニュアル内の例、コマンド表示出力、ネットワークボジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

© 2021 Cisco Systems, Inc. All rights reserved.