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):

- 3des-cbc
- aes128-cbc
- aes192-cbc
- aes256-cbc
- rijndael-cbc@lysator.liu.se
- aes128-ctr
- aes192-ctr
- aes256-ctr

3.mac_algorithms (4):

- 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