

Cisco Web セキュリティアプライアンス向け AsyncOS 12.x の暗号リスト

初版：2018 年 5 月 14 日

最終更新：2021 年 5 月 5 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)

TLS 1.0	TLS 1.1	TLS 1.2
ECDHE-RSA-AES256-SHA - YES	ECDHE-RSA-AES256-SHA - YES	ECDHE-RSA-AES256-GCM-SHA384 - YES
DHE-RSA-AES256-SHA - YES	DHE-RSA-AES256-SHA - YES	ECDHE-RSA-AES256-SHA384 - YES
DHE-RSA-CAMELLIA256-SHA - YES	DHE-RSA-CAMELLIA256-SHA - YES	ECDHE-RSA-AES256-SHA - YES
AES256-SHA - YES	AES256-SHA - YES	DHE-RSA-AES256-GCM-SHA384 - YES
CAMELLIA256-SHA - YES	CAMELLIA256-SHA - YES	DHE-RSA-AES256-SHA256 - YES
ECDHE-RSA-DES-CBC3-SHA - YES	ECDHE-RSA-DES-CBC3-SHA - YES	DHE-RSA-AES256-SHA - YES
EDH-RSA-DES-CBC3-SHA - YES	EDH-RSA-DES-CBC3-SHA - YES	DHE-RSA-CAMELLIA256-SHA - YES
DES-CBC3-SHA - YES	DES-CBC3-SHA - YES	AES256-GCM-SHA384 - YES
ECDHE-RSA-AES128-SHA - YES	ECDHE-RSA-AES128-SHA - YES	AES256-SHA256 - YES
DHE-RSA-AES128-SHA - YES	DHE-RSA-AES128-SHA - YES	AES256-SHA - YES
DHE-RSA-SEED-SHA - YES	DHE-RSA-SEED-SHA - YES	CAMELLIA256-SHA - YES
DHE-RSA-CAMELLIA128-SHA - YES	DHE-RSA-CAMELLIA128-SHA - YES	ECDHE-RSA-DES-CBC3-SHA - YES
AES128-SHA - YES	AES128-SHA - YES	EDH-RSA-DES-CBC3-SHA - YES

ポート 443 (SSL ポート)

TLS 1.0	TLS 1.1	TLS 1.2
SEED-SHA - YES	SEED-SHA - YES	DES-CBC3-SHA - YES
CAMELLIA128-SHA - YES	CAMELLIA128-SHA - YES	ECDHE-RSA-AES128-GCM-SHA256 - YES
		ECDHE-RSA-AES128-SHA256 - YES
		ECDHE-RSA-AES128-SHA - YES
		DHE-RSA-AES128-GCM-SHA256 - YES
		DHE-RSA-AES128-SHA256 - YES
		DHE-RSA-AES128-SHA - YES
		DHE-RSA-SEED-SHA - YES
		DHE-RSA-CAMELLIA128-SHA - YES
		AES128-GCM-SHA256 - YES
		AES128-SHA256 - YES
		AES128-SHA - YES
		SEED-SHA - YES
		CAMELLIA128-SHA - YES

ポート 443 (SSL ポート)

TLS 1.0	TLS 1.1	TLS 1.2	TLS 1.3
DHE-RSA-AES256-SHA - YES	DHE-RSA-AES256-SHA - YES	DHE-RSA-AES256-GCM-SHA384 - YES	TLS_AES_128_GCM_SHA256 - YES
DHE-RSA-CAMELLIA256-SHA - YES	DHE-RSA-CAMELLIA256-SHA - YES	DHE-RSA-AES256-SHA256 - YES	TLS_CHACHA20_POLY1305_SHA256 - YES
ADH-AES256-SHA - YES	ADH-AES256-SHA - YES	DHE-RSA-AES256-SHA - YES	TLS_AES_256_GCM_SHA384 - YES
ADH-CAMELLIA256-SHA - YES	ADH-CAMELLIA256-SHA - YES	DHE-RSA-CAMELLIA256-SHA - YES	
AES256-SHA - YES	AES256-SHA - YES	ADH-AES256-GCM-SHA384 - YES	
CAMELLIA256-SHA - YES	CAMELLIA256-SHA - YES	ADH-AES256-SHA256 - YES	
EDH-RSA-DES-CBC3-SHA - YES	EDH-RSA-DES-CBC3-SHA - YES	ADH-AES256-SHA - YES	
ADH-DES-CBC3-SHA - YES	ADH-DES-CBC3-SHA - YES	ADH-CAMELLIA256-SHA - YES	
DES-CBC3-SHA - YES	DES-CBC3-SHA - YES	AES256-GCM-SHA384 - YES	
DHE-RSA-AES128-SHA - YES	DHE-RSA-AES128-SHA - YES	AES256-SHA256 - YES	

TLS 1.0	TLS 1.1	TLS 1.2	TLS 1.3
DHE-RSA-SEED-SHA - YES	DHE-RSA-SEED-SHA - YES	AES256-SHA - YES	
DHE-RSA-CAMELLIA128-SHA - YES	DHE-RSA-CAMELLIA128-SHA - YES	CAMELLIA256-SHA - YES	
ADH-AES128-SHA - YES	ADH-AES128-SHA - YES	EDH-RSA-DES-CBC3-SHA - YES	
ADH-SEED-SHA - YES	ADH-SEED-SHA - YES	ADH-DES-CBC3-SHA - YES	
ADH-CAMELLIA128-SHA - YES	ADH-CAMELLIA128-SHA - YES	DES-CBC3-SHA - YES	
AES128-SHA - YES	AES128-SHA - YES	DHE-RSA-AES128-GCM-SHA256 - YES	
SEED-SHA - YES	SEED-SHA - YES	DHE-RSA-AES128-SHA256 - YES	
CAMELLIA128-SHA - YES	CAMELLIA128-SHA - YES	DHE-RSA-AES128-SHA - YES	
ECDHE-ECDSA-AES128-SHA - YES	ECDHE-ECDSA-AES128-SHA - YES	DHE-RSA-SEED-SHA - YES	
ECDHE-RSA-AES128-SHA - YES	ECDHE-RSA-AES128-SHA - YES	DHE-RSA-CAMELLIA128-SHA - YES	
		ADH-AES128-GCM-SHA256 - YES	
		ADH-AES128-SHA256 - YES	
		ADH-AES128-SHA - YES	
		ADH-SEED-SHA - YES	
		ADH-CAMELLIA128-SHA - YES	
		AES128-GCM-SHA256 - YES	
		AES128-SHA256 - YES	
		AES128-SHA - YES	
		SEED-SHA - YES	
		CAMELLIA128-SHA - YES	
		ECDHE-ECDSA-AES256-GCM-SHA384 - YES	
		ECDHE-ECDSA-CHACHA20-POLY1305 - YES	
		ECDHE-ECDSA-AES128-GCM-SHA256 - YES	
		ECDHE-ECDSA-AES256-SHA384 - YES	
		ECDHE-ECDSA-AES128-SHA256 - YES	

TLS 1.0	TLS 1.1	TLS 1.2	TLS 1.3
		ECDHE-RSA-AES256-GCM-SHA384 - YES	
		ECDHE-RSA-CHACHA20-POLY1305 - YES	
		ECDHE-RSA-AES128-GCM-SHA256 - YES	
		ECDHE-RSA-AES256-SHA384 - YES	
		ECDHE-RSA-AES128-SHA256 - YES	
		ECDHE-RSA-AES128-SHA - YES	
		ECDHE-ECDSA-AES128-CCM - YES	
		ECDHE-ECDSA-AES256-CCM - YES	
デフォルト モード : DHE-RSA-AES128-SHA - YES AES128-SHA - YES	デフォルト モード : DHE-RSA-AES128-SHA - YES AES128-SHA - YES	デフォルト モード : AES256-GCM-SHA384 - YES AES256-SHA256 - YES DHE-RSA-AES128-SHA - YES AES128-GCM-SHA256 - YES AES128-SHA256 - YES AES128-SHA - YES	デフォルト モード : TLS_AES_256_GCM_SHA384 - YES
(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。			(注) AsyncOS 12.0.1 以降のバージョンは TLS 1.3 をサポートします。

ポート 22 (SSH ポート)

ssh2-enum-algos :

1. `kex_algorithms` (7) :

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

4. `mac_algorithms` (4) :

- `hmac-sha1`
- `hmac-ripemd160`
- `hmac-ripemd160@openssh.com`
- `umac-64@openssh.com`

2. `encryption_algorithms`

(8) :

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

`compression_algorithms`

(2) :

- なし
- `zlib@openssh.com`

3.

`server_host_key_algorithms`

(4) :

- `ssh-dss`
- `ssh-rsa`
- `rsa-sha2-512`
- `rsa-sha2-256`

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
RC4-MD5	RC4-MD5
RC4-SHA	RC4-SHA

【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/）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、ネットワークトポロジ図、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.