

「SSL/TLS アプライアンス製品の暗号設定方法等の調査報告書」のアップデート

2018年10月
独立行政法人 情報処理推進機構

1. 概要

富士通株式会社より、IPCOMシリーズ(IPCOM EX2700 IN)の後継製品であるIPCOM EX2-3500に関する分冊が提供されたため、提供された情報を基に、本調査報告書の表 3-1 及び表 5.1-2 の IPCOM シリーズの情報を最新化する。

2. 『表 3-1 調査対象製品一覧』のアップデート情報

表 3-1 調査対象製品一覧 (本報告書 P.4)

項番	メーカー	機種名	ファームウェア バージョン	代理店	備考
1	Cisco	ASA 5512	9.5(2)5	シスコシステムズ	・ASA シリーズ
2	F5 ネットワークス	BIG-IP 3900	12.0.0	F5 ネットワークスジャパン	・BIG-IP シリーズ
3	A10 ネットワークス	3030S	-	A10 ネットワークス	・Thunder シリーズ ・ソフトウェアバージョン : 2.7.2-P7-SP3
4	日本ラドウェア	Alteon VA	-	日本ラドウェア	・Alteon シリーズ ・ソフトウェア製品(バージョン : 30.2.1.100)
5-1	富士通	IPCOM EX2700 IN	E20L32 NF0201 B01	富士通	発売終了製品
5-2	富士通	IPCOM EX2-3500	-	富士通	・IPCOM EX2 シリーズ ・ソフトウェアバージョン: V01L03
6	NEC	InterSecVM/LB V3.0 for VMWare	-	NEC	・InterSec シリーズ ・ソフトウェア製品(アップデートモジュール Rel 1.0)

7	Array Networks	APV2600	-	Array Networks	・ APV シリーズ ・ ソフトウェアバージョン: ArrayOS Rel.APV.8.6.0.14
8	日立製作所	Hitachi LoadBalancer EL130	-	日立製作所	・ A10 ネットワークス Thunder 1030S の OEM 製品 ・ ソフトウェアバージョン: 2.7.1-P6
9	バラクーダネットワークス	Barracuda Load Balancer ADC モデル 340	6.0.0.005	バラクーダネットワークス ジャパン	・ Load Balancer ADC シリーズ
10	バラクーダネットワークス	Barracuda WAF モデル 360	8.1.0.009	バラクーダネットワークス ジャパン	・ WAF シリーズ
11	Citrix	MPX8005c	NS11.0 Build 64.34.nc	マクニカネットワークス	・ NetScaler MPX シリーズ
12	セイコーソリューションズ	Netwiser SX-3850	7.3.20	セイコーソリューションズ	・ Netwiser シリーズ
13	Cisco	WSA S370	8.8.0-085	シスコシステムズ	・ WSA シリーズ
14	Imperva	SecureSphere X2010	11.0.0.30	マクニカネットワークス	・ SecureSphere シリーズ

3. 『表 5.1-2 「設定ガイドライン」の要求設定への対応』のアップデート情報

表 5.1-1 「設定ガイドライン」の要求設定への対応 (P.7 – P.8)

項番	調査対象製品	高セキュリティ	推奨セキュリティ	セキュリティ例外
1	Cisco ASA シリーズ	RSA 証明書及び ECDSA 証明書の両方を同時に設定時		
		設定 (準拠) できる	設定 (準拠) できる	設定できない
2	F5 ネットワークス BIG-IP シリーズ	RSA 証明書及び ECDSA 証明書の両方を同時に設定時		
		EC 系のみを設定すれば準拠できる	設定 (準拠) できる	設定 (準拠) できる
3	A10 ネットワークス Thunder シリーズ	RSA 証明書設定時 (※片方のみ設定可)		
		EC 系のみを設定すれば準拠できる	設定 (準拠) できる	設定 (準拠) できる
		ECDSA 証明書設定時 (※片方のみ設定可)		
		設定できない	設定 (準拠) できる	設定できない

4	日本ラドウェア Alteon シリーズ	RSA 証明書及び ECDSA 証明書の両方を同時に設定時		
		設定（準拠）できる	設定（準拠）できる	設定（準拠）できる
5-1	富士通 IPCOM EX2700 IN シリーズ	RSA 証明書設定時		
		設定できない	設定（準拠）できる	設定（準拠）できる
5-2	富士通 IPCOM EX2-3500 シリーズ	RSA 証明書設定時		
		設定（準拠）できる	設定（準拠）できる	設定（準拠）できる
6	NEC InterSec シリーズ	RSA 証明書設定時		
		設定できない	設定（準拠）できる	設定（準拠）できる
7	Array Networks APV シリーズ	RSA 証明書設定時（※片方のみ設定可）		
		設定（準拠）できる	設定（準拠）できる	設定（準拠）できる
		ECDSA 証明書設定時（※片方のみ設定可）		
		設定（準拠）できる	デフォルトで準拠できる	設定（準拠）できる
8	日立製作所 Hitachi Load Balancer EL130	RSA 証明書設定時		
		設定できない	設定（準拠）できる	設定（準拠）できる
9	バラクーダネットワークス Barracuda Load Balancer ADC シリーズ	RSA 証明書及び ECDSA 証明書の両方を同時に設定時		
		設定（準拠）できる	設定（準拠）できる	設定（準拠）できる
10	バラクーダネットワークス Barracuda WAF シリーズ	RSA 証明書及び ECDSA 証明書の両方を同時に設定時		
		設定（準拠）できる	設定（準拠）できる	設定（準拠）できる
11	Citrix NetScaler MPX シリーズ	RSA 証明書設定時		
		設定（準拠）できる	設定（準拠）できる	設定（準拠）できる
12	セイコーソリューションズ Netwiser シリーズ	RSA 証明書設定時		
		設定（準拠）できる	設定（準拠）できる	設定（準拠）できる

※調査対象製品の具体的な機種名等は表 3-1 調査対象製品一覧 参照。

※EC 系：楕円曲線暗号が含まれる暗号スイート。

以上