HCD-PP の SFR と JCMVP 暗号アルゴリズム確認の対応表

第 1.0 版

IT セキュリティ評価及び認証制度では、HCD-PP v1.0 に基づく暗号アルゴリズムの実装の適切性を評価するにあたり、暗号モジュール試験及び認証制度(JCMVP)の暗号アルゴリズム確認の結果を活用することを許容しています。

本資料は、JCMVP の暗号アルゴリズム確認を活用するため、HCD-PP v1.0 で使用されている暗号関係の SFR と、JCMVP の暗号アルゴリズム確認登録簿との対応を示すものです。

独立行政法人情報処理推進機構
セキュリティセンター
セキュリティ技術評価部

2019 年 2 月 21 日発行

目次

1. はじめに

本資料は、「Protection Profile for Hardcopy Devices, 1.0 dated September 10, 2015」（以下、“HCD-PP v1.0”という。）で使用されている暗号関係の SFR と、JCMVP の暗号アルゴリズム確認登録簿との対応を示したものです。

JCMVP の暗号アルゴリズム確認登録簿の確認リストは以下のとおりです。

1. 非対称鍵暗号（公開鍵暗号および鍵共有）
   - DSA 確認リスト　https://www.ipa.go.jp/security/jcmvp/algval/dsaval.html
   - ECDSA 確認リスト　https://www.ipa.go.jp/security/jcmvp/algval/ecdsaval.html
   - RSA 確認リスト　https://www.ipa.go.jp/security/jcmvp/algval/rsaval.html

   - DH 確認リスト　https://www.ipa.go.jp/security/jcmvp/algval/dhval.html
   - ECDH 確認リスト　https://www.ipa.go.jp/security/jcmvp/algval/ecdhval.html

2. 共通鍵暗号
   - AES 確認リスト　https://www.ipa.go.jp/security/jcmvp/algval/aesval.html

3. ハッシュ関数
   - SHS 確認リスト　https://www.ipa.go.jp/security/jcmvp/algval/shaval.html

4. メッセージ認証
   - HMAC 確認リスト　https://www.ipa.go.jp/security/jcmvp/algval/hmacval.html

5. 乱数生成
   - DRBG 確認リスト　https://www.ipa.go.jp/security/jcmvp/algval/drbgval.html

6. 鍵導出関数
   - KDF 確認リスト　https://www.ipa.go.jp/security/jcmvp/algval/kdfval.html
   - PBKDF 確認リスト　（2019 年 2 月現在で確認された実装は無い）

2. SFR と JCMVP の確認リストの対応表

本章では、HCD-PP v1.0 の SFR と、それに対応する JCMVP の確認リストの名称及び暗号アルゴリズム実装試験に使用するパラメタの対応を示します。

なお、表中で使用されている「任意」は、JCMVP の確認リストに記載されているパラメタの値がどれでも良いことを意味しています。 ただし、JCMVP の暗号アルゴリズム確認時には、確認条件として取り得る値が制限されます。

2.1 暗号鍵生成（非対称鍵用）

SFR	JCMVP 確認リスト名 及びパラメタ
FCS_CKM.1 - Key Generation	
NIST SP 800-56A, for finite field-based schemes, cryptographic key sizes equivalent to, or greater than, a symmetric key strength of 112 bits (key pair generation portions of FIPS 186-4)	DH 確認リスト **・DH group 24 (2048-bit MODP with 256-bit POS)の場合** 機能: KEY(gen) bit length of p: 2048 bit length of q: 256 生成方法: 任意 (Key Pair Generation Using Extra Random Bits, または, Key Pair Generation by Testing Candidates) **・DH Group 14 等の非 FIPS 186-4 の場合** 未対応

SFR		JCMVP 確認リスト名 及びパラメタ
	NIST SP 800-56B, for RSA-based schemes, cryptographic key sizes equivalent to, or greater than, a symmetric key strength of 112 bits (key pair generation portions of FIPS 186-4)	RSA 確認リスト 機能: KEY(gen) MOD: 2048, または, 3072 (bits) CRT: 任意（CRT あり, または, CRT なし） e: 任意（65537, または, random） ※FIPS 186-4 の「B.3.3 Generation of Random Primes that are Probably Prime」および「Probabilistic Primality Tests Table C.3」に対応。
	NIST SP 800-56A, for elliptic curve-based schemes, implementing NIST curves P-256, P-384, P-521 (as defined in FIPS 186-4)	ECDSA 確認リスト または ECDH 確認リスト 機能: PKG（KEY(gen)の表記の場合もあり） CURVES: P-256, または, P-384, または, P-521 生成方法: 任意 (Key Pair Generation Using Extra Random Bits, または, Key Pair Generation by Testing Candidates)

2.2 対称鍵暗号化/復号、鍵ラッピング

SFR	JCMVP 確認リスト名 及びパラメタ
FCS_COP.1 - AES Encryption / Decryption, Key Wrapping	
CBC (NIST SP 800-38A) cryptographic key sizes 128 bits, 256 bits	AES 確認リスト CBC 機能: 暗号化, 復号 鍵長: 128, または, 256 (bits)
CMAC (NIST SP800-38B) [1]	—
CCM (NIST SP 800-38C) cryptographic key sizes 128 bits, 256 bits	AES 確認リスト CCM 機能: Generation-Encryption, Decryption-Verification 鍵長: 128, または, 256 (bits) 他パラメタ: 任意
GCM (NIST SP 800-38D) cryptographic key sizes 128 bits, 256 bits	AES 確認リスト ・ストレージ暗号化の場合 GCM 機能: 暗号化, 復号 鍵長: 128, または, 256 (bits) 他パラメタ: 任意

[1] HCD-PP v1.0 では、暗号通信用の FCS_COP.1(a) (Symmetric encryption / decryption)の選択肢に NIST SP 800-38B (CMAC Mode) が記述されているが、依存関係にある IPsec や TLS の SFR の選択肢には記述はない。

SFR		JCMVP 確認リスト名 及びパラメタ
		・暗号通信の場合 GCM 機能: 暗号化, 復号 鍵長: 128, または, 256 (bits) IV 生成: 外部 IV: 96 (bits) Tag length: 128, または, 64, または, 96(bits) [2] AAD length: プロトコルに依存
	XTS (IEEE 1619) cryptographic key sizes 128 bits, 256 bits	AES 確認リスト XTS 機能: 暗号化, 復号 鍵長: XTS_128, または, XTS_256 他パラメタ: 任意
	KW (NIST SP 800-38F)	未対応
	KWP (NIST SP 800-38F)	未対応

[2] 64(bits)及び 96(bits)は、サポートしている場合

2.3 鍵配送

SFR	JCMVP 確認リスト名 及びパラメタ
FCS_COP.1 - Key Transport	
RSA KTS-OAEP (NIST SP 800-56B) cryptographic key size 2048, 3072	RSA 確認リスト ALG: RSA-OAEP 機能: 暗号化, 復号 MOD: 2048, 3072 (bits) e: 任意（65537, または, random） SHS: SHA-256, または, SHA-384, または, SHA-512 MGF: ANSI X9.44 (SHA-256), または, ANSI X9.44 (SHA-384), または, ANSI X9.44 (SHA-512) DRBG: Hash_DRBG, HMAC_DRBG, または CTR_DRBG（暗号化の場合）
RSA KTS-KEM-KWS (NIST SP 800-56B [3])	未対応

[3] KTS-KEM-KWS は NIST SP 800-56B Rev.2 から削除される可能性がある。

2.4 署名生成/検証

SFR	JCMVP 確認リスト名 及びパラメタ
FCS_COP.1 - Signature	
DSA (FIPS 186-4) key sizes (modulus) 2048 bits or greater	DSA 確認リスト ・**Trusted update** の場合 機能: SIG(ver) bit length of p: 2048 bit length of q: 224, または, 256 SHS: SHA-224, または, SHA-256 または 機能: SIG(ver) bit length of p: 3072 bit length of q: 256 SHS: SHA-256
rDSA (FIPS 186-4) key sizes (modulus) 2048 bits or greater	RSA 確認リスト ・**Trusted update** の場合 ALG: RSASSA-PKCS1_v1_5 機能: SIG(ver) MOD: 2048, または, 3072 (bits) e: 任意（65537, または, random） SHS: SHA-256, または, SHA-384, または, SHA-512 または

SFR		JCMVP 確認リスト名 及びパラメタ
		ALG: RSASSA-PSS 機能: SIG(ver) MOD: 2048, または, 3072 (bits) e: 任意（65537, または, random） SHS: SHA-256, または, SHA-384, または, SHA-512 MGF: ANSI X9.44 (SHA-256), または, ANSI X9.44 (SHA-384), または, ANSI X9.44 (SHA-512) ※アルゴリズム ANSI X9.31 は未対応 **・暗号通信（IKEv2, TLS）の場合** ALG: RSASSA-PKCS1_v1_5 機能: SIG(gen), SIG(ver) MOD: 2048, または, 3072 (bits) e: 任意（65537, または, random） SHS: SHA-1, または, SHA-256, または, SHA-384, または, SHA-512 **・暗号通信（IKEv1）の場合** 未対応（IKEv1 は非 FIPS 186-4）
	ECDSA (FIPS 186-4) key sizes 256 bits or greater, implementing NIST curves P-256, P-384, P-521 (as defined in FIPS 186-4)	ECDSA 確認リスト **・Trusted update の場合** 機能: SIG(ver) CURVES: P-256 SHS: SHA-1, または, SHA-256, または, SHA-384, または,

SFR	JCMVP 確認リスト名 及びパラメタ
	SHA-512 または 機能: SIG(ver) CURVES: P-384 SHS: SHA-1, または, SHA-256, または, SHA-384, または, SHA-512 または 機能: SIG(ver) CURVES: P-521 SHS: SHA-1, または, SHA-256, または, SHA-384, または, SHA-512 ・暗号通信（TLS）の場合 機能: SIG(gen), SIG(ver) ※CURVES と SHS の組合せは Trusted update の場合と同じ。 ・暗号通信（IKEv1, IKEv2）の場合 機能: SIG(gen), SIG(ver) CURVES: P-256 SHS: SHA-256 または 機能: SIG(gen), SIG(ver) CURVES: P-384 SHS: SHA-384

SFR		JCMVP 確認リスト名 及びパラメタ
		または 機能: SIG(gen), SIG(ver) CURVES: P-521 SHS: SHA-512

2.5 ハッシュアルゴリズム

SFR		JCMVP 確認リスト名 及びパラメタ
FCS_COP.1 - Hash Algorithm		
	SHA-1, SHA-256, SHA-384, SHA-512 (ISO/IEC 10118-3:2004)	SHS 確認リスト SHA-1, または, SHA-256, または, SHA-384, または, SHA-512 ※Byte-oriented Mode のみに対応

2.6 鍵付ハッシュメッセージ認証

SFR	JCMVP 確認リスト名 及びパラメタ
FCS_COP.1 - Keyed-Hash	
・ストレージ暗号化用 HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-512 (ISO/IEC 9797-2:2011, ISO/IEC 10118)	HMAC 確認リスト HMAC-SHA-1, または, HMAC-SHA-256, または, HMAC-SHA-512 Key Size Ranges Tested: KS < BS, KS = BS
・暗号通信用 HMAC-SHA-1, *HMAC-SHA-224* [4], HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512 (FIPS 198-1, FIPS 180-3)	HMAC 確認リスト HMAC-SHA-1, または, HMAC-SHA-256, または, HMAC-SHA-384, または, HMAC-SHA-512 Key Size Ranges Tested: KS < BS, KS > BS, KS = BS ※パラメタは、プロトコルと使用条件に依存。

[4] HCD-PP v1.0 では、暗号通信用の FCS_COP.1(g) (for keyed-hash message authentication)の選択肢に HMAC-SHA-224 が記述されているが、IPsec や TLS では HMAC-SHA-224 は使われていない。

2.7 暗号鍵導出

SFR	JCMVP 確認リスト 及びパラメタ
FCS_KDF_EXT.1 - Key Derivation	
NIST SP 800-108 (KDF in Counter Mode, KDF in Feedback Mode, KDF in Double-Pipeline Iteration Mode), using keyed-hash functions	KDF 確認リスト KDF in Counter Mode PRF: HMAC-SHA-1, または, HMAC-SHA-256, または, HMAC-SHA-512 Bit length of counter: 8, 16, 24, または 32 または KDF in Feedback Mode PRF: HMAC-SHA-1, または, HMAC-SHA-256, または, HMAC-SHA-512 Bit length of counter: 8, 16, 24, または 32 (但し、counter を PRF の入力に含める場合) without counter (但し、counter を PRF の入力に含めない場合) 他パラメタ: 任意 または KDF in Double Pipeline Iteration Mode PRF: HMAC-SHA-1, または, HMAC-SHA-256, または, HMAC-SHA-512 Bit length of counter: 8, 16, 24, または 32 (但し、counter を PRF の入力に含める場合) without counter (但し、counter を PRF の入力に含めない場合) ※「Counter Location」は SP 800-108 の仕様どおり（米国 CAVP の Before Fixed Data に該当）

SFR		JCMVP 確認リスト 及びパラメタ
	NIST SP 800-132 (Password-based Key Derivation Functions), using keyed-hash functions	PBKDF 確認リスト（名称未定） PBKDF PRF: HMAC-SHA-256, または, HMAC-SHA-512 Iteration count: 1,000 以上 100,000 以下 Password size ranges tested: 次の 1 つ以上がサポートされていること - 112 ≤ **len** (*P*) < *B* - **len**(*P*) = *B* - **len**(*P*) > *B* Salt size ranges tested: 次の 1 つ以上がサポートされていること - 128 ≤ **len**(*S*) < (*hLen* - 32) - **len**(*S*) = (*hLen* - 32) - **len**(*S*) > (*hLen* - 32) DRBG: Hash_DRBG, HMAC_DRBG, または CTR_DRBG

2.8 暗号パスワードの生成と条件付け

SFR	JCMVP 確認リスト名 及びパラメタ
FCS_PCC_EXT.1 - Password Construction and Conditioning	
NIST SP 800-132 (Password-based Key Derivation Functions), with HMAC-SHA-256, *HMAC-SHA-384* [5], HMAC-SHA-512, with 1000 or more iterations, and output key sizes 128, 256	PBKDF 確認リスト（名称未定） PBKDF PRF: HMAC-SHA-256, または, HMAC-SHA-512 Iteration count: 1,000 以上 100,000 以下 Password size ranges tested: 次の 1 つ以上がサポートされていること - 112 ≤ **len** (*P*) < *B* - **len**(*P*) = *B* - **len**(*P*) > *B* Salt size ranges tested: 次の 1 つ以上がサポートされていること - 128 ≤ **len**(*S*) < (*hLen* - 32) - **len**(*S*) = (*hLen* - 32) - **len**(*S*) > (*hLen* - 32) DRBG: Hash_DRBG, HMAC_DRBG, または CTR_DRBG

[5] HCD-PP v1.0 では、FCS_PCC_EXT.1 の選択肢に HMAC-SHA-384 が記述されているが、依存関係にあるストレージ暗号化用の FCS_COP.1(h) (for keyed-hash message authentication) の選択肢には記述はない。

2.9 乱数ビット生成

SFR	JCMVP 確認リスト名 及びパラメタ
FCS_RBG_EXT.1 - Random Bit Generation	
Hash_DRBG (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512) ISO/IEC 18031:2011, NIST SP 800-90A	DRBG 確認リスト Hash_DRBG Prediction Resistance Tested: 任意（Enabled, または, Disabled） SHS: SHA-1, または, SHA-224, または, SHA-256, または, SHA-384, または, SHA-512
HMAC_DRBG (HMAC-SHA-1, HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512) ISO/IEC 18031:2011, NIST SP 800-90A	DRBG 確認リスト HMAC_DRBG Prediction Resistance Tested: 任意（Enabled, または, Disabled） HMAC: HMAC-SHA-1, または, HMAC-SHA-224, または, HMAC-SHA-256, または, HMAC-SHA-384, または, HMAC-SHA-512
CTR_DRBG (AES) ISO/IEC 18031:2011, NIST SP 800-90A	DRBG 確認リスト CTR_DRBG with DF, CTR_DRBG without DF [6] Prediction Resistance Tested: 任意（Enabled, または, Disabled） AES: AES-128, または, AES-256

以上

[6] ISO/IEC 18031:2011 では CTR_DRBG without DF は規定されていない。