安全性評価結果

目次

1. はじめに

- 【安全性評価・実装評価】の目的
  推奨候補暗号としての十分な安全性・実装性能の有無を判定する。

- 評価対象暗号の分類
  （現）現リスト掲載暗号
  （新）新規応募暗号
  （事）事務局選出暗号

- 判定結果

公開鍵暗号（守秘）　RSAES-PKCS1-v1_5,
ストリーム暗号　RC4,
ハッシュ関数　RIPEMD-160, SHA-1,
メッセージ認証コード CBC-MAC
について、安全性上の問題から次期リストの運用監視暗号とすると判定した。その他の評価対象暗号については、推奨候補暗号としての十分な安全性を有すると判定した。

以下、判定結果を示した後、判定理由および注釈について記す。

2. 公開鍵暗号の判定結果

○は第一次選定（評価A・B）の対象とすることを示す

技術分類	暗号技術名	分類	判定
署名	DSA	現	○
	ECDSA	現	○
	RSASSA-PKCS1-v1_5	現	○
	RSA-PSS	現	○
守秘	RSA-OAEP	現	○
	RSAES-PKCS1-v1_5*	現	**運用監視暗号**
鍵共有	DH	現	○
	ECDH	現	○
	PSEC-KEM*	現	○

*は次期リストにおいて注釈がつく暗号技術を示す

2. 共通鍵暗号の判定結果

○は第一次選定（評価A・B）の対象とすることを示す

技術分類	暗号技術名	分類	判定
64ビットブロック暗号*	CIPHERUNICORN-E	現	○
	Hierocrypt-L1	現	○
	MISTY1	現	○
	3-key Triple DES*	現	○
128ビットブロック暗号	AES	現	○
	Camellia	現	○
	CIPHERUNICORN-A	現	○
	CLEFIA	新	○
	Hierocrypt-3	現	○
	SC2000	現	○
ストリーム暗号	Enocoro-128v2	新	○
	KCipher-2	新	○
	MUGI	現	○
	MULTI-S01*	現	○
	128-bit RC4*	現	**運用監視暗号**

*は次期リストにおいて注釈がつく暗号技術を示す

2. その他暗号技術の判定結果

○は第一次選定（評価A・B）の対象とすることを示す

技術分類	暗号技術名	分類	判定
ハッシュ関数	RIPEMD-160*	現	**運用監視暗号**
	SHA-1*	現	**運用監視暗号**
	SHA-256	現	○
	SHA-384	現	○
	SHA-512	現	○
メッセージ認証コード	CBC-MAC	事	**運用監視暗号**
	CMAC	事	○
	HMAC	事	○
	PC—MAC-AES	新	○
暗号利用モード	CBC	事	○
	CFB	事	○
	OFB	事	○
	CTR	事	○
	CCM	事	○
	GCM*	事	○
エンティティ認証	ISO/IEC 9798-2	事	○
	ISO/IEC 9798-3	事	○
	ISO/IEC 9798-4	事	○

*は次期リストにおいて注釈がつく暗号技術を示す

3. 判定理由および次期リストにおける注釈：公開鍵暗号

技術分類	暗号技術名	判定	判定理由および次期リストにおける注釈
署名	DSA	○	安全性上の問題が報告されておらず、また注釈もついていないため、次期リストの推奨候補暗号とする。
	ECDSA	○	
	RSASSA-PKCS1-v1_5	○	
	RSA-PSS	○	
守秘	RSA-OAEP	○	
	RSAES-PKCS1-v1_5*	監視	現在、注釈「SSL3.0/TLS1.0 で利用実績があることから当面の利用を認める」が付与されている。Bleichenbacherの攻撃[B98]といった現実的な攻撃が起因となり付与された注釈であり、次期リストの運用監視暗号とする。新たな注釈は「SSL3.0/TLS1.0,1.1,1.2 で利用実績があることから当面の利用を認める」とする。
鍵共有	DH	○	安全性上の問題が報告されておらず、また注釈もついていないため、次期リストの推奨候補暗号とする。
	ECDH	○	
	PSEC-KEM*	○	現在、注釈「KEM(Key Encapsulating Mechanism)-DEM(Data Encapsulating Mechanism)構成における利用を前提とする」が付与されている。メッセージの秘匿化に利用する技術をDEM にすることを推奨しているものであり、鍵共有部である (PSEC-) KEMに、安全性に係わる問題は報告されていないため、次期リストの推奨候補暗号とする。注釈は、引き続き同じものを利用する。

*は次期リストにおいて注釈がつく暗号技術を示す

3. 判定理由および次期リストにおける注釈：ブロック暗号

技術分類	暗号技術名	判定	判定理由および次期リストにおける注釈
64ビットブロック暗号*	CIPHERUNICORN-E	○	安全性に係る問題は報告されていないため、次期リストの推奨候補暗号とする。注釈は、以前と同じものを利用する。 (注3)新たな電子政府用システムを構築する場合、より長いブロック長の暗号が利用できるのであれば、128ビットブロック暗号を選択することが望ましい。
	Hierocrypt-L1	○	
	MISTY1	○	
	3-key Triple DES*	○	安全性に係る問題は報告されていないため、次期リストの推奨候補暗号とする。注釈は、以前と同じものを利用する。 (注3)及び(注4) 3-keyTriple DESは、以下の条件を考慮し、当面の利用を認める。1)(NIST の)SP 800-67 として規定されていること。2)デファクトスタンダードとしての位置を保っていること。
128ビットブロック暗号	AES	○	AES-192/AES-256 は関連鍵攻撃に対する脆弱性を有するが[BK09]、単一鍵の通常の利用に関しては安全性に問題はない。また、鍵の全数探索の効率性を高めた Biclique 攻撃[BKR11]は多くのブロック暗号に適用可能であるが、AES に対する Biclique 攻撃は依然として計算量が大きいため、安全性に問題はない。
	Camellia	○	安全性に係る問題が報告されていないため、次期リストの推奨候補暗号とする。
	CIPHERUNICORN-A	○	
	CLEFIA	○	
	Hierocrypt-3	○	
	SC2000	○	

*は次期リストにおいて注釈がつく暗号技術を示す

3. 判定理由および次期リストにおける注釈：ストリーム暗号

技術分類	暗号技術名	判定	判定理由および次期リストにおける注釈
ストリーム暗号	Enocoro-128v2	○	安全性に係る問題は報告されていないため、次期リストの推奨候補暗号とする。
	KCipher-2	○	
	MUGI	○	
	MULTI-S01*	○	MULTI-S01 の認証部分の構造は GCM のそれと類似しており、FSE 2012 において報告された GCMの弱鍵発見手法[S12]が適用可能であるが、その割合は非常に小さいため、安全性に問題はない。他に安全性に係わる問題が報告されていないため、次期リストの推奨暗号暗号とする。なお、パディング方法に問題があるため、平文サイズが 64 ビットの倍数でなければ正常に復号できないため[FWT00] 、注釈は、「平文サイズは 64 ビットの倍数に限る。」とする。なお、ISO/IEC 18033-4 において同じ名称の暗号技術があるが、CRYPTREC に応募されたものとは異なる。
	128-bit RC4*	監視	同じ平文を各々別々の鍵で暗号化しブロードキャストするような場合において、安全性に係る問題が報告されている[I12]ため、次期リストの運用監視暗号とする。注釈は、引き続き同じものを利用する。 (注5)128-bitRC4は、SSL(TLS1.0以上)に限定して利用すること。

*は次期リストにおいて注釈がつく暗号技術を示す

3. 判定理由および次期リストにおける注釈：ハッシュ関数・MAC

技術分類	暗号技術名	判定	判定理由および次期リストにおける注釈
ハッシュ関数	RIPEMD-160*	監視	現在、注釈「新たな電子政府用システムを構築する場合、より長いハッシュ値のものが利用できるのであれば、256 ビット以上のハッシュ関数を選択することが望ましい。ただし、公開鍵暗号での仕様上、利用すべきハッシュ関数が指定されている場合には、この限りではない。」が付与されている。本暗号技術のハッシュ長は 160 ビットであり、安全性の観点から 256 ビット以上のハッシュ関数を選択することが望ましいため、次期リストの運用監視暗号とする。
	SHA-1*	監視	
	SHA-256	○	安全性上の問題が報告されておらず、また注釈もついていないため、次期リストの推奨候補暗号とする。
	SHA-384	○	
	SHA-512	○	
メッセージ認証コード	CBC-MAC*	監視	メッセージ長が固定の場合、MAC として安全であるが、メッセージ長が可変の場合、容易に MAC の偽造が出来る[MOV96] 。安全性に問題があるため、次期リストの運用監視暗号にする。注釈は、「安全性の観点から、メッセージ長を固定して利用すべきである。」とする。
	CMAC	○	安全性上の問題が報告されておらず、また注釈もついていないため、次期リストの推奨候補暗号とする。
	HMAC	○	
	PC―MAC-AES	○	安全性に係る問題は報告されていないため、次期リストの推奨候補暗号とする。

*は次期リストにおいて注釈がつく暗号技術を示す

3. 判定理由および次期リストにおける注釈：モード・エンティティ認証

技術分類	暗号技術名	判定	判定理由および次期リストにおける注釈
暗号利用モード	CBC	○	安全性上の問題が報告されておらず、また注釈もついていないため、次期リストの推奨候補暗号とする。
	CFB	○	
	OFB	○	
	CTR	○	
	CCM	○	
	GCM*	○	FSE 2012 において弱鍵の存在が報告されたが[S12] 、その割合は非常に小さいため、安全性に問題はない。CRYPTO 2012 において、安全性証明に問題が見つかったが、新たに証明が修正された[IOM12] 。他に安全性に係る問題は報告されていないため、次期リストの推奨候補暗号とする。注釈は、「初期化ベクトル長は 96 ビットを推奨する。」とする。
エンティティ認証	ISO/IEC 9798-2	○	本技術は第 1 次評価において一部のタイプに脆弱性が発見されたが、ISO/IEC にて規格修正され、安全性上の問題が取り除かれたため、次期リストの推奨候補暗号とする。注釈は付与しない。
	ISO/IEC 9798-3	○	
	ISO/IEC 9798-4	○	

*は次期リストにおいて注釈がつく暗号技術を示す

3. 参考文献

[B98] D. Bleichenbacher: Chosen Ciphertext Attacks Against Protocols Based on the RSA Encryption Standard PKCS #1, CRYPTO 1998, pp.1-12, 1998.

[BK09] A. Biryukov and D. Khovratovich, Related-key Cryptanalysis of the Full AES-192 and AES-256, Asiacrypt 2009, LNCS 5912, p.1-18.

[BKR11] A. Bogdanov, D. Khovratovich and C. Rechberger, Biclique Cryptanalysis of the Full AES, ASIACRYPT 2011, LNCS 7023, p.344-371.

[FWT00] 古屋, 渡辺, 宝木, MULTI-S01 のパディングと安全性についての考察、信学技法、ISEC2000-68.

[I12] 五十部, ストリーム暗号RC4の安全性評価, 2012年度外部評価, 2012.

[IOM12] T. Iwata, K. Ohashi and K. Minematsu, Breaking and Repairing GCM Security Proofs, CRYPTO 2012, LNCS 7417, p.31-49.

[MOV96] A.J. Menezes, P.C. van Oorschot, and S.A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996.

[S12] Saarinen, Cycling Attacks on GCM, GHASH and Other Polynomial MACs and Hashes, FSE 2012, LNCS 7549, p.216-225.