【安全性評価・実装評価】
判定結果(概要)

【安全性評価・実装評価】の目的

- 【安全性評価・実装評価】の目的
  現リスト掲載暗号、新規応募暗号、事務局選出暗号について、
  推奨候補暗号として十分な安全性・実装性能を有するか判断する。

- 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

公開鍵暗号の判定結果

○は第一次選定（評価A・B）の対象、
×は第一次選定（評価A・B）の対象としないことを示す

技術分類	暗号技術名	分類	方式委判定	実装委判定	判定
署名	DSA	現	○	○	○
	ECDSA	現	○	○	○
	RSASSA-PKCS-v1_5	現	○	○	○
	RSA-PSS	現	○	○	○
守秘	RSA-OAEP	現	○	○	○
	RSAES-PKCS-v1_5	現	×	○	×
鍵共有	DH	現	○	○	○
	ECDH	現	○	○	○
	PSEC-KEM	現	○	○	○

共通鍵暗号の判定結果

○は第一次選定（評価A・B）の対象、
×は第一次選定（評価A・B）の対象としないことを示す

技術分類	暗号技術名	分類	方式委判定	実装委判定	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	×	○	×

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、
×は第一次選定（評価A・B）の対象としないことを示す

技術分類	暗号技術名	分類	方式委	実装委	判定
ハッシュ関数	RIPEMD-160	現	×	○	×
	SHA-1	現	×	○	×
	SHA-256	現	○	○	○
	SHA-384	現	○	○	○
	SHA-512	現	○	○	○
メッセージ認証コード	CBC-MAC	事	×	○	×
	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	○	○	○