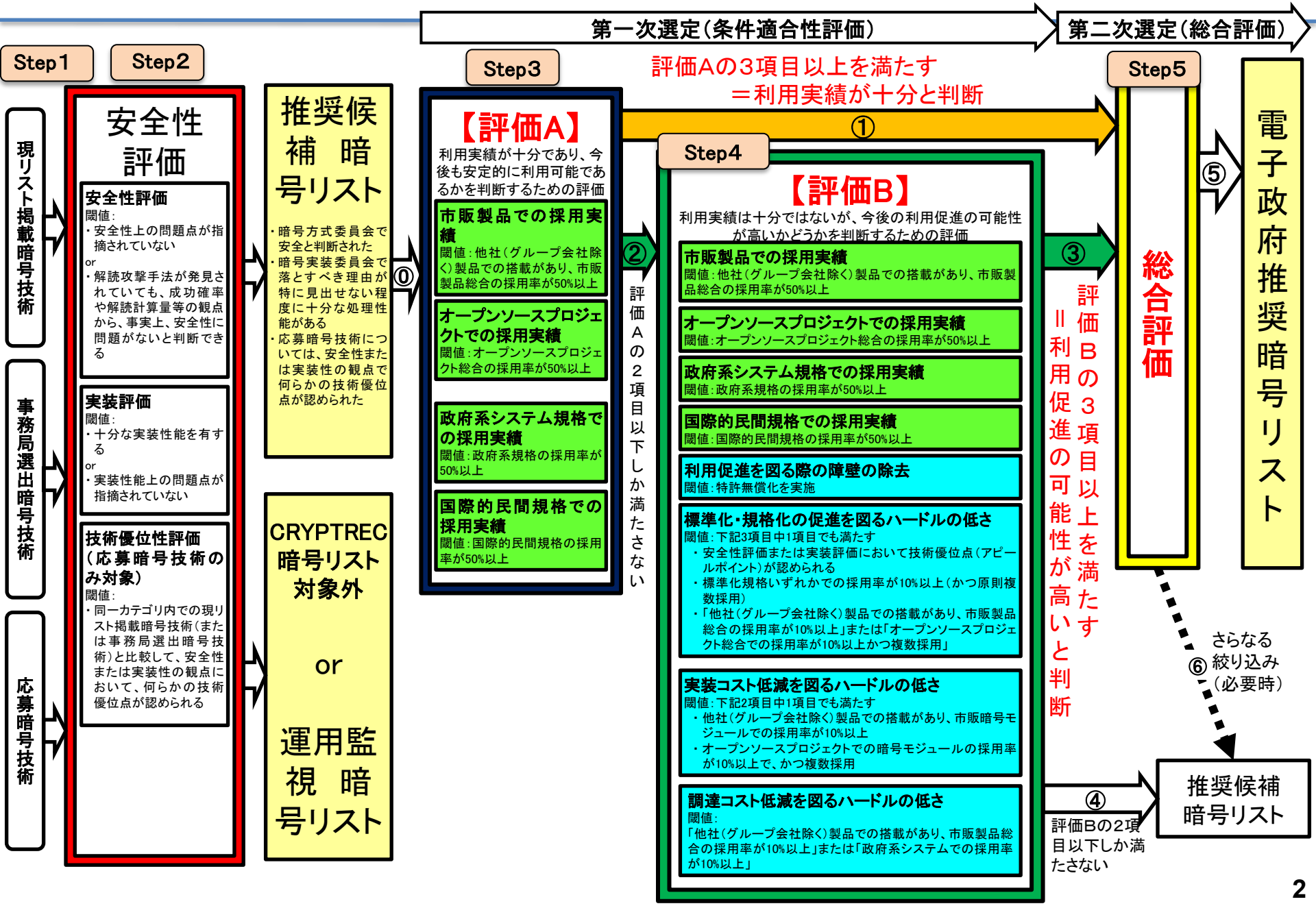
暗号技術の選定基準

選定基準一覧表（安全性評価・実装評価・条件適合性評価）



暗号選定遷移図

技術分類		電子政府推奨暗号リスト(平成15年2月20日版)
公開鍵暗号	署名	DSA ECDSA RSA-PSS RSASSA-PKCS1-v1_5
	守秘	RSA-OAEP RSAES-PKCS1-v1_5
	鍵共有	DH ECDH PSEC-KEM
共通鍵暗号	64ビットブロック暗号	CIPHERUNICORN-E Hierocrypt-L1 MISTY1 3-key Triple DES
	128ビットブロック暗号	AES Camellia CIPHERUNICORN-A Hierocrypt-3 SC2000
	ストリーム暗号	MUGI MULTI-S01 128-bit RC4
ハッシュ関数		RIPEMD-160 SHA-1 SHA-256 SHA-384 SHA-512
暗号利用モード		
MAC		
エンティティ認証		

技術分類		新規評価対象暗号	
		新規応募暗号	事務局選出暗号
公開鍵暗号	署名		
	守秘		
	鍵共有		
共通鍵暗号	64ビットブロック暗号		
	128ビットブロック暗号	CLEFIA	該当なし
	ストリーム暗号	Enocoro-128v2 KCipher-2	該当なし
ハッシュ関数			
暗号利用モード		該当なし	CBC CFB CTR OFB CCM GCM
MAC		PC-MAC-AES	CBC-MAC CMAC HMAC
エンティティ認証		該当なし	ISO/IEC9798-2 ISO/IEC9798-3 ISO/IEC9798-4

安全性評価／実装評価

【評価A】

利用実績が十分であり、今後も安定的に利用可能であるかを判断するための評価

【評価B】

利用実績は十分ではないが、今後の利用促進の可能性が高いかどうかを判断するための評価

技術分類		運用監視暗号リスト	CRYPTREC暗号リスト外
公開鍵暗号	署名	該当なし	該当なし
	守秘	RSAES-PKCS1-v1_5	該当なし
	鍵共有	該当なし	該当なし
共通鍵暗号	64ビットブロック暗号	該当なし	該当なし
	128ビットブロック暗号	該当なし	HyRAL※
	ストリーム暗号	128-bit RC4	該当なし
ハッシュ関数		RIPEMD-160 SHA-1	該当なし
暗号利用モード		該当なし	該当なし
MAC		CBC-MAC	該当なし
エンティティ認証		該当なし	該当なし

※ 新規応募暗号HyRAL(128ビットブロック暗号)については、2010年度の第一次評価の結果、第一次評価までで終了とし、CRYPTREC暗号リストに掲載しないこととなった。

技術分類		電子政府推奨暗号リスト(候補)	
		評価A通過(①)	評価B通過(②③)
公開鍵暗号	署名	DSA RSASSA-PKCS1-v1_5	ECDSA RSA-PSS
	守秘	該当なし	RSA-OAEP
	鍵共有	DH	ECDH
共通鍵暗号	64ビットブロック暗号	3-key Triple DES	該当なし
	128ビットブロック暗号	AES	Camellia
	ストリーム暗号	該当なし	KCipher-2
ハッシュ関数		該当なし	SHA-256 SHA-384 SHA-512
暗号利用モード		CBC	CFB CTR OFB CCM GCM
MAC		HMAC	CMAC
エンティティ認証		該当なし	ISO/IEC9798-2 ISO/IEC9798-3

技術分類		推奨候補暗号リスト
公開鍵暗号	署名	該当なし
	守秘	該当なし
	鍵共有	PSEC-KEM
共通鍵暗号	64ビットブロック暗号	CIPHERUNICORN-E Hierocrypt-L1 MISTY1
	128ビットブロック暗号	CIPHERUNICORN-A CLEFIA Hierocrypt-3 SC2000
	ストリーム暗号	Enocoro-128v2 MUGI MULTI-S01
ハッシュ関数		該当なし
暗号利用モード		該当なし
MAC		PC-MAC-AES
エンティティ認証		ISO/IEC9798-4

総合評価

電子政府推奨暗号リスト

①

②

③

④

⑤

⑥

さらなる絞り込み（必要時）