

電子政府推奨暗号リスト

平成15年2月20日

総 務 省

経 済 産 業 省

技術分類		名称
公開鍵暗号	署名	DSA
		ECDSA
		RSASSA-PKCS1-v1_5
		RSA-PSS
	守秘	RSA-OAEP
		RSAES-PKCS1-v1_5 ^(注1)
	鍵共有	DH
		ECDH
		PSEC-KEM ^(注2)
共通鍵暗号	64ビットブロック暗号 ^(注3)	CIPHERUNICORN-E
		Hierocrypt-L1
		MISTY1
		3-key Triple DES ^(注4)
	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 ^(注5)
その他	ハッシュ関数	RIPEMD-160 ^(注6)
		SHA-1 ^(注6)
		SHA-256
		SHA-384
	擬似乱数生成系 ^(注7)	SHA-512
		PRNG based on SHA-1 in ANSI X9.42-2001 Annex C.1
		PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) Appendix 3.1
		PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) revised Appendix 3.1

注釈：(注1) SSL3.0/TLS1.0で使用実績があることから当面の使用を認める。

(注2) KEM (Key Encapsulation Mechanism) -DEM(Data Encapsulation Mechanism) 構成における利用を前提とする。

- (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使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。
- (注 4) 3-key Triple DES は、以下の条件を考慮し、当面の使用を認める。
- 1) FIPS46-3 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
- (注 5) 128-bit RC4 は、SSL3.0/TLS1.0 以上に限定して利用することを想定している。なお、リストに掲載されている別の暗号が利用できるのであれば、そちらを使用することが望ましい。
- (注 6) 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使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。
- (注 7) 擬似乱数生成系は、その利用特性上、インタオペラビリティを確保する必要性がないため、暗号学的に安全な擬似乱数生成アルゴリズムであれば、どれを利用しても基本的に問題が生じない。したがって、ここに掲載する擬似乱数生成アルゴリズムは「例示」である。

別添

電子政府推奨暗号リストに関する修正情報

修正日付	修正箇所	修正前	修正後	修正理由
平成17年10月12日	注釈の注4)の1)	FIPS46-3として規定されていること	SP800-67として規定されていること	仕様変更を伴わない、仕様書の指定先の変更