



INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

IPA 暗号フォーラム 2006

独立行政法人 情報処理推進機構
セキュリティセンター 暗号グループ
山岸 篤弘

自己紹介

- 暗号グループのリーダー
- パネルディスカッションに臨む立場
 - しかるべき政府機関を引きずり出そう！
 - 失敗
 - 責任を取って壇上に・・・
 - こんなはずでは無かったのに・・・
 - 電子政府推奨暗号リストの利用促進
 - CRYPTRECの事務局
 - 監視
 - 暗号モジュールのセキュリティ要件/試験要件
 - 暗号モジュール試験及び認証

情報セキュリティ技術が支えるネットワーク社会

ネットワーク社会

脅威(不正アクセスなど)

政治

電子投票
電子役所
電子警察

電子

経済

電子商取引
電子決済
(電子マネー)

公証

文化

コンテンツ流通
著作権保護

法・制度・保険
運用・管理

社会制度

倫理

監視・監査
教育・啓発など

セキュリティシステム構築技術

情報セキュリティシステム技術

セキュアプロトコル技術

PKI構築技術

実装技術とその評価技術

アクセス制御技術

鍵回復技術

侵入検知技術

情報セキュリティ要素技術

個人認証技術

暗号技術

電子透かし技術

電子政府推奨暗号リスト

公開鍵 暗号	署名	DSA	共通鍵 暗号	64ビット ブロック 暗号(注 3)	CIPHERUNICORN-E
		ECDSA			Hierocrypt-L1
		RSASSA-PKCS-v1_5			MISTY1
		RSA-PSS			3-key Triple DES (注4)
	守秘	RSA-OAEP		128ビット ブロック 暗号	AES
		RSAES-PKCS-v1_5(注1)			Camellia
	鍵共有	DH			CIPHERUNICORN-A
		ECDH			Hierocrypt-3
		PSEC-KME(注2)			SC2000
	その他	ハッシュ 関数			RIPEMD-160(注6)
SHA-1(注6)			MUGI		
SHA-256/-384/-512			128-bit RC4 (注5)		

電子政府推奨暗号リスト

- (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、以下の条件を配慮し、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。

ハッシュ関数の認証数の推移

