

平成 15 年 3 月 31 日  
総 務 省  
経 済 産 業 省

## 「暗号技術検討会 2002 年度報告書」の公表

総務省及び経済産業省は、暗号技術の普及による情報セキュリティ対策の推進を図るため、2001 年 5 月から「暗号技術検討会」(座長：今井秀樹東京大学教授)を開催し、「電子政府」における調達のための推奨すべき暗号のリスト(電子政府推奨暗号リスト)作成のための暗号技術の評価等を実施してまいりました。今般、「暗号技術検討会 2002 年度報告書」が取りまとめられましたので、公表いたします。

本検討会では、電子政府推奨暗号リスト作成のための暗号技術の評価等を実施してきましたが、このたび、2002 年度報告書が取りまとめられたものです。

なお、報告書の概要は別紙 1、検討会の構成員は別紙 2 のとおりです。

連絡先：経済産業省商務情報政策局  
情報セキュリティ政策室  
(担当：北浦課長補佐)  
電話：(直通) 03 - 3501 - 0397  
FAX： 03 - 3501 - 6639

## 「暗号技術検討会 2002 年度報告書」の概要

### 1 . 暗号技術検討会開催の背景

電子政府等の実現に向けて、高度情報通信ネットワークの安全性及び信頼性を確保するためには、情報セキュリティの基盤技術である暗号技術について、一定水準以上の安全性と信頼性を有するものを利用することが不可欠であり、また、その安全性と信頼性は、暗号技術の専門家により技術的、専門的な見地から客観的に評価されることが必要である。

そのため、総務省及び経済産業省は、共同で「暗号技術検討会」を開催し、暗号技術を公募の上、客観的に評価し、安全性及び実装性に優れた暗号技術をリスト化し、各府省に対してその利用を推奨することにより、高度な安全性と信頼性に支えられ、国民が安心して利用できる電子政府等の構築に貢献することを目指すこととした。

### 2 . CRYPTREC の体制

総務省及び経済産業省が開催する「暗号技術検討会」(座長：今井秀樹東京大学教授)並びに、通信・放送機構(TAO)及び情報処理振興事業協会(IPA)が開催する「暗号技術評価委員会」(委員長：今井秀樹東京大学教授)の両研究会による暗号評価プロジェクト「CRYPTREC (Cryptography Research and Evaluation Committees)」の体制(別添1参照)で、検討・評価を進めた。

### 3 . 電子政府推奨暗号リスト案の作成

2001 年度に引き続き暗号技術の評価を実施し、「電子政府」における調達のための推奨すべき暗号のリスト(電子政府推奨暗号リスト)案を作成した。

なお、リスト案については、平成 14 年 11 月 28 日から同年 12 月 25 日まで総務省及び経済産業省においてパブリックコメントを実施し、その結果寄せられた意見等も検討した上、平成 15 年 2 月 20 日に、両省から電子政府推奨暗号リスト(別添 2)として公表した。

おって、本リストについて、各府省は可能な限り電子政府推奨暗号リストに掲載された暗号の利用を推進する旨の利用方針が、平成 15 年 2 月 28 日に、各府省で合意された。

#### 4．暗号調達のためのガイドブックの作成

暗号技術検討会の下に「暗号調達ガイドブック作成WG」(リーダ：佐々木良一東京電機大学教授)を設置し、各府省の調達担当者が利用目的に合った暗号アルゴリズムを電子政府推奨暗号リストから適切に選択する際の参考となるよう、暗号アルゴリズムの選定手順や電子政府推奨暗号等を解説する手引書「暗号調達のためのガイドブック」を作成した。

#### 5．今後の CRYPTREC 活動

2003 年度以降、電子政府等の安全性及び信頼性の確保に貢献することを目的として、以下のような活動を行うこととした。

##### (1) 電子政府推奨暗号の監視

電子政府推奨暗号に選定された各暗号アルゴリズムの安全性等についての情報収集や評価を行い、必要に応じて修正情報の周知やリストからの削除等の電子政府推奨暗号リストの変更を行う。

##### (2) 電子政府推奨暗号の安全性及び信頼性確保のための調査及び検討

###### (イ) 暗号アルゴリズム等を主な対象とする調査及び検討

暗号アルゴリズムや素因数分解問題等の数論的問題の困難性を主な対象とする調査及び検討を行う。

###### (ロ) 暗号実装関連技術を主な対象とする調査及び検討

実装攻撃等の暗号実装関連技術を主な対象とする調査及び検討を行う。

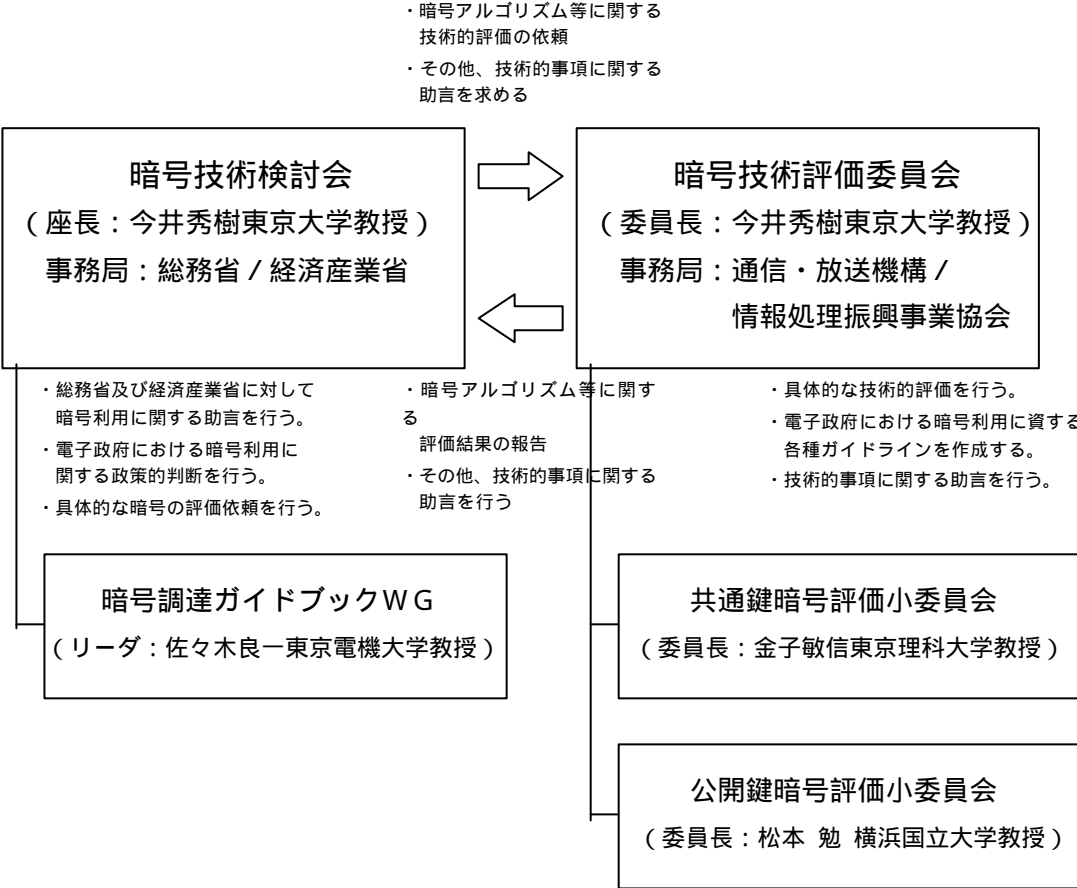
##### (3) 電子政府推奨暗号リストの改訂に関する調査及び検討

将来の電子政府推奨暗号リストの改訂(新たな電子政府推奨暗号リストの策定及び本件電子政府推奨暗号リストの廃棄)のために必要な調査及び検討を行う。

##### (4) 暗号モジュール評価基準の作成

暗号モジュール評価基準及び試験基準を作成する。

# CRYPTREC(Cryptography Research and Evaluation Committees)



## 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 <sup>(注1)</sup>
	鍵共有	DH
		ECDH
		PSEC-KEM <sup>(注2)</sup>
共通鍵暗号	64 ビットブロック暗号 <sup>(注3)</sup>	CIPHERUNICORN-E
		Hierocrypt-L1
		MISTY1
		3-key Triple DES <sup>(注4)</sup>
	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 <sup>(注5)</sup>
その他	ハッシュ関数	RIPEMD-160 <sup>(注6)</sup>
		SHA-1 <sup>(注6)</sup>
		SHA-256
		SHA-384
		SHA-512
	擬似乱数生成系 <sup>(注7)</sup>	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。

## 「暗号技術検討会」構成員

座長	今井 秀樹	東京大学生産技術研究所教授
顧問	辻井 重男	中央大学理工学部情報工学科教授
	岩下 直行	日本銀行金融研究所研究第2課企画役
	岡崎 宏	情報通信ネットワーク産業協会常務理事
	岡本 栄司	筑波大学電子・情報工学系教授
	岡本 龍明	日本電信電話株式会社情報流通プラットフォーム研究所主席研究員 ( (社)電気通信事業者協会代表兼務 )
	小田 雅一	(社)情報サービス産業協会セキュリティ委員会委員
	小柳津 育郎	NTTエレクトロニクス株式会社セキュリティシステム事業部技術部長
	加藤 義文	(社)テレコムサービス協会技術委員会委員長
	金子 敏信	東京理科大学理工学部電気工学科教授
	国分 明男	(財)ニューメディア開発協会常務理事開発本部長
	櫻井 幸一	九州大学大学院システム情報科学研究科教授
	佐々木 良一	東京電機大学工学部情報メディア学科教授
	宝木 和夫	(社)電子情報技術産業協会情報セキュリティ委員会委員
	苗村 憲司	慶応義塾大学環境情報学部教授
	松井 充	三菱電機株式会社情報技術総合研究所情報セキュリティ技術部 チームリーダー
	松本 勉	横浜国立大学大学院環境情報研究院教授

(敬称略)