暗号技術検討会

２０１０年度報告書

２０１１年３月

目次

１．はじめに

情報通信技術を安心・安全に利用できる環境を構築していくにあたり、暗号技術は必要不可欠なものとなっている。しかし同時に、解読技術等の進展に注意を払い、適切なものを使用するよう努めねばならない。例えば、2008 年末に、SSL サーバ証明書に使用されているハッシュ関数アルゴリズム MD5 の脆弱性をついて、偽の中間 CA 証明書を発行できるとの発表が行われるなど、暗号アルゴリズムの危殆化により、実社会で被害が出る可能性のある事例も出始めている。このことは、社会の重要な基盤である暗号アルゴリズムの危殆化について、引き続き監視を行っていくことが重要であることを示している。

政府においても、情報セキュリティ政策会議(議長：内閣官房長官)において、「政府機関において使用されている暗号アルゴリズム SHA-1 及び RSA1024 に係る移行指針（2008 年 4 月)」及び「国民を守る情報セキュリティ戦略（2010 年 5 月)」が決定され、政府機関に対しては暗号アルゴリズムの着実な移行の実施とともに、「電子政府推奨暗号リスト」の安全性の継続的な監視・調査の実施及び安全性の急激な低下に備えた対応計画の策定などが求められるなど、大きな動きが見られた。CRYPTREC としても、政府機関のこれらの動きに対して適切に支援を行うべく、調査・検討を進める必要がある。

昨年度は、「電子政府推奨暗号リスト」の改訂に向け、CRYPTREC の体制見直しを行い、暗号技術検討会の下に、暗号方式委員会、暗号実装委員会及び暗号運用委員会を設置し、必要な調査・検討等を開始し、リスト改訂のための暗号技術公募を実施した。今年度は、応募された暗号技術についての安全性評価を実施するとともに、次年度以降に予定している実装性や利用実績の評価方法の検討を実施するなどのリスト改訂に向けて着実に作業を進めるとともに、政府機関において使用されている SHA-1 及び RSA1024 の安全性が急激に低下した場合の CRYPTREC として対応方針の検討を進めたところである。

委員会別の活動状況を見てみると、暗号方式委員会では、昨年度応募された応募暗号技術について、安全性に関する１次評価を実施した。また、暗号技術の監視・調査等の活動、リストガイドの作成等を行った。暗号実装委員会では、電子政府推奨暗号リスト改訂に向けてハードウェア及びソフトウェア実装性評価の要件を決定するとともに、国際標準化機関 ISO/IEC による暗号モジュールのセキュリティ要件及び試験要件の規格改訂に貢献した。暗号運用委員会では、次期電子政府推奨暗号リストの位置付けを明確化するためにシナリオを整理し、それぞれの影響に関するの調査・分析を行い、結果をとりまとめた。

2010 年度の活動のうち、詳細な技術的事項については、暗号方式委員会、暗号実装委員会及び暗号運用委員会における議論を踏まえて、独立行政法人情報通信研究機構及び独立行政法人情報処理推進機構が取りまとめた「CRYPTREC Report 2010」を参照いただきたい。

末筆であるが、本検討会及び関係委員会に御協力いただいた構成員、オブザーバの方々をはじめ、関係者の皆様に心から謝意を表する次第である。

2011 年 3 月

暗号技術検討会

座長　今井　秀樹

２．暗号技術検討会開催の背景及び開催状況

２．１．暗号技術検討会開催の背景

高度情報通信ネットワークの安全性及び信頼性の確保は、我が国が目指す世界最先端のIT国家構築の基盤となるものであり、国民一人一人が安心してネットワークを利用するための前提となるものである。ITが産業・社会活動から国民生活、行政活動に必要不可欠な基盤として発展する一方で、情報セキュリティに関する問題等が、国民生活・社会経済活動に対して多大な影響を与える存在となっていることから、情報セキュリティ対策については、IT戦略本部に、情報セキュリティ政策に関する基本戦略の策定、情報セキュリティ政策の事前・事後評価の実施等の機能を有する「情報セキュリティ政策会議」を設置し、官民における統一的・横断的な、情報セキュリティ対策の推進を図ることとしている。

暗号技術は情報セキュリティの基盤技術であり、その安全性を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することが重要である。電子政府のセキュリティ確保のためには、安全性に優れた暗号技術を利用することが不可欠である。

このため、総務省及び経済産業省は、客観的な評価により安全性及び実装性に優れると判断される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の構築に貢献することを目指し、2001年度から本検討会を開催した。両省は、本検討会での検討及び評価の結果を踏まえ2003年2月20日に「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）を公表し（別添１参照）、2003年2月28日には、行政情報システム関係課長連絡会議において、各府省が情報システムの構築にあたり暗号を利用する場合には、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「各府省の情報システム調達における暗号の利用方針」が了承された。また、「政府機関の情報セキュリティ対策のための統一基準(第4版)（平成21年度修正）(2010年5月11日：情報セキュリティ政策会議)」においては、府省庁における暗号化及び電子署名のアルゴリズムについて、「電子政府推奨暗号リストに記載されたものが使用可能な場合には、それを使用すること」が定められているところである

総務省及び経済産業省は、国民が安心して電子政府を利用できるように、電子政府の安全性及び信頼性を確保するための活動を引き続き実施していくこととした。

２．２．CRYPTRECの体制

CRYPTRECとはCryptography Research and Evaluation Committeesの略であり、総務省及び経済産業省が共同で開催する暗号技術検討会（座長：今井秀樹中央大学教授）と、独立行政法人情報通信研究機構（NICT）及び独立行政法人情報処理推進機構（IPA）が共同で開催する委員会から構成される暗号技術評価プロジェクトをいう。2008年度までは、暗号技術検討会の下に、暗号技術監視委員会（委員長：今井秀樹中央大学教授）及び暗号モジュール委員会（委員長：松本勉横浜国立大学教授）を設置し、暗号技術検討会では、

「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・検討」として「暗号アルゴリズム等を主な対象とする調査・検討」及び「暗号実装関連技術を主な対象とする調査・検討」を行ってきており、これらの検討事項に関する技術的な検討等を「暗号技術監視委員会」及び「暗号モジュール委員会」において行っていたところである。

詳細については、「３章　電子政府推奨暗号リストの改訂」で後述するが、現在の電子政府推奨暗号リストの策定から 7 年余りが経過し、暗号技術に対する解析・攻撃技術の高度化や、新たな暗号技術の開発が進展している状況にあることから、CRYPTREC では、電子政府推奨暗号リストの改訂に向けた検討を行っているところであり、新しい電子政府推奨暗号リストに掲載される暗号については、政府等による調達等を容易にすることを目的として、「安全性」及び「実装性」の観点に加え、「製品化、利用実績等」の観点も取り入れることとしている。また、リスト掲載暗号の危殆化リスクが高まった際には、すぐにリストから削除するのではなく、「運用監視暗号リスト」に掲載し、暗号解読のリスクと電子政府システムにおける移行コスト等を勘案して、定期的に掲載継続の可否を判断する予定である。

新しい電子政府推奨暗号リストを策定・運用していくに当たり、「暗号技術の運用を主な対象とする調査・検討」等を行う必要があることから、それに合わせて 2009 年度に CRYPTREC の体制の見直しを行った。

具体的には、暗号技術検討会（座長：今井秀樹中央大学教授）の下に、暗号方式委員会（委員長：今井秀樹中央大学教授）、暗号実装委員会（委員長：松本勉横浜国立大学教授）及び暗号運用委員会（委員長：佐々木良一東京電機通信大学教授）を設置し、検討等を行った。(CRYPTREC の体制図は図 2.1 参照)

２．２．１．暗号技術検討会

暗号技術検討会（以下、「検討会」）は、電子政府推奨暗号の監視、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・検討、電子政府推奨暗号リスト改訂に関する調査・検討、暗号モジュールに関する国際標準化への協力等について、総合的な観点から検討を行った。

検討会は総務省政策統括官及び経済産業省商務情報政策局長の研究会として開催した。

２．２．２．暗号方式委員会

暗号方式委員会は、検討会の下に設置され、電子政府推奨暗号の監視、電子政府推奨暗号に関する暗号アルゴリズムを主な対象とする調査・検討、電子政府推奨暗号リスト改訂に関する調査・検討を行った。また、具体的な調査・検討に際して暗号方式委員会を支援することを目的に、同委員会の下に暗号技術調査 WG を設置し、検討を行った。

暗号方式委員会は NICT 及び IPA の委員会として開催した。

２．２．３．暗号実装委員会

暗号実装委員会は、検討会の下に設置され、ISO/IEC 等の国際標準の動向を注視しつつ、電子政府推奨暗号リスト掲載暗号技術に対するハードウェア及びソフトウェア実装性評価の実装環境や実装性能のほか、暗号実装技術、サイドチャネル攻撃等の暗号モジュールに対する攻撃手法等について調査・研究を行った。

暗号実装委員会は NICT 及び IPA の委員会として開催した。

２．２．４．暗号運用委員会

暗号運用委員会は、検討会の下に設置され、暗号技術に対する製品化・利用実績の評価方法に関する調査・研究を行った。

暗号運用委員会は NICT 及び IPA の委員会として開催した。

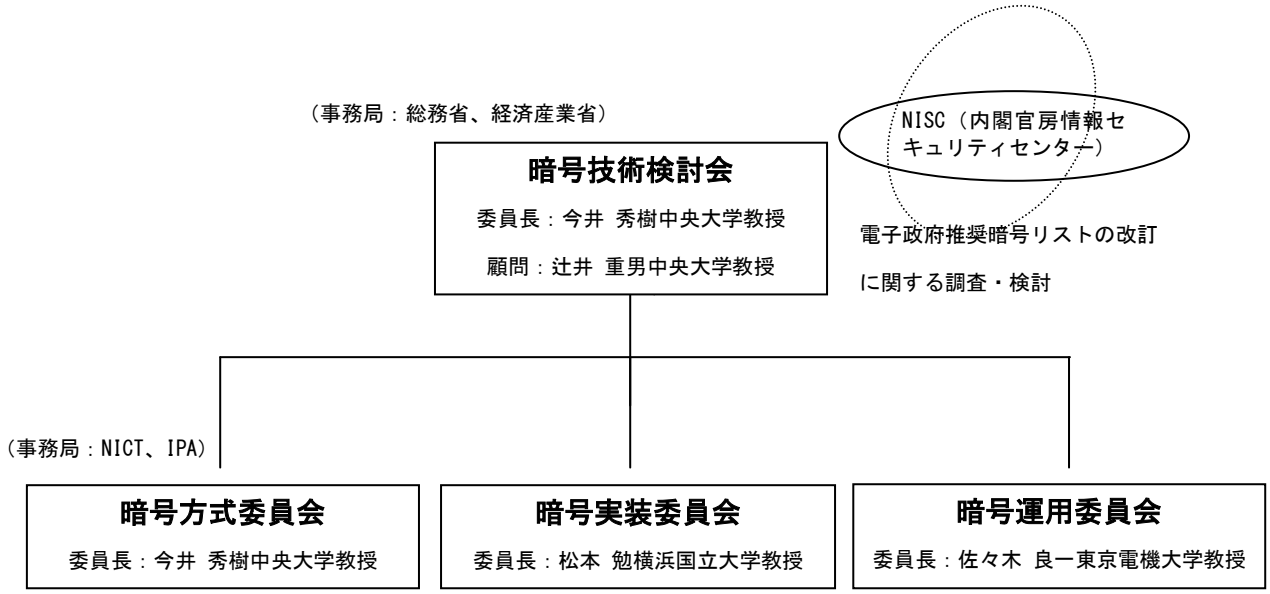


図 2.1　2010 年度 CRYPTREC の体制図

２．３．暗号技術検討会開催状況

2010 年度、検討会は 2 回開催予定であったが、2011 年 3 月 11 日に発生した東北地方太平洋沖地震の影響により、第２回開催が中止となったため、予定していた主な議題についてメール審議を行った。

各回会合の開催日及び主な議題は以下のとおり。

【第 1 回】2010 年 12 月 17 日（金）

（主な議題）・CRYPTREC の 運営方針

・電子政府推奨暗号リスト掲載暗号危殆化時の対応について

・電子政府推奨暗号リストの改訂に向けた活動について

（暗号方式委員会活動報告）

（暗号実装委員会活動報告）

（暗号運用委員会活動報告）

【第 2 回】2011 年 3 月 14 日（月）（震災により中止）

【メール審議】2011 年 3 月 18 日（金）～25 日（金）

（主な議題）・電子政府推奨暗号リスト掲載暗号危殆化時の対応について

・暗号技術検討会 2010 年度報告書（案）について

（電子政府推奨暗号リストの改訂に向けた進捗状況）

（暗号方式委員会活動報告）

（暗号実装委員会活動報告）

（暗号運用委員会活動報告）

３．電子政府推奨暗号リストの改訂

３．１．改訂の背景

CRYPTREC は、客観的な評価により安全性及び実装性に優れると判断される暗号技術をリストアップすることを目的に、2000 年度に暗号技術の公募・評価活動を開始し、2002 年度末に電子政府推奨暗号リスト（以下、「現リスト」）を発表した。

その後、各府省に対してその利用を推奨することにより、電子政府の高度な安全性と信頼性を確保することを目指して、2003 年度から監視活動及び安全性評価を継続して行ってきた。これにより、現リストの信頼性は高められ、また、それらの活動に基づいた暗号の危殆化への対応・提言は電子政府において広く認知されてきた。

現リストには、策定時点において、今後 10 年間は安心して利用できるという観点で選定された暗号が掲載されている。しかし、策定から 5 年余りが経過し、暗号技術に対する解析・攻撃技術の高度化や、新たな暗号技術の開発が進展している状況にある。

また、今日では CRYPTREC への要望が、暗号技術に対する安全性評価とその周知のみならず、安心・安全な情報通信システムを構築する上で、暗号技術の危殆化及び移行対策等を含めた、適切な暗号技術の選択を支援するものへと変化しつつある。

さらに、暗号技術の評価の面において、政府調達等における入手し易さや導入コスト、相互運用性と普及度合いの観点も取り入れる必要性が指摘されているところである。

これらの状況を踏まえ、2012 年度、現リストを改訂することが必要である。

３．２．現リストの改訂の目的

今回の改訂においては、第一に、電子政府において暗号技術を利用する際に安全な暗号技術を選択するための指針を与えること、第二に、暗号を利用した技術をシステムのセキュリティ要件に合わせて正しく組み込むための指針を与えることを目的とする。次期リストは、内閣官房情報セキュリティセンター（NISC）の調整により、情報セキュリティ政策会議で決定された「政府機関の情報セキュリティ対策のための統一基準」等から参照されることを想定している。

このため、今回の改訂にあたっては、新たに暗号技術の公募を行うとともに、現リストに掲載されている暗号技術の見直しを行い、現リストの全体の構成を改めることとする。

３．３．次期電子政府推奨暗号リストに関する考え方

次期電子政府推奨暗号リスト（以下「次期リスト」という。）については、現リストの改訂に関する骨子を策定（平成２０年１１月）し、これを踏まえた暗号技術公募要項を策定（平成２１年５月）してきており、その考え方の整理については、主に暗号運用委員会において検討を行っているところである。

今年度のその検討結果については、後述の「暗号運用委員会活動報告」のとおりであ

り、次期リストを取り巻く国内外の事情を踏まえた多角的な観点を視野に入れた検討を行う必要があるため、今後も継続してその考え方の具現化に向けた継続検討を行っていく必要があるところである。

３．４．電子政府推奨暗号リスト改訂のための暗号技術の公募（2009 年度）

３．４．１．公募の概要

CRYPTREC は評価対象暗号技術を公募し、暗号技術評価を実施する。特に、安全性及び実装性で、現リストに記載されている暗号アルゴリズムよりも優位な点を持ち、国際学会で注目されている新技術が提案されている暗号技術カテゴリであること、及び、現リストに掲載されている暗号技術と同カテゴリに属する暗号技術については、それらの暗号技術よりも、安全性もしくは実装性において優れた暗号技術であることを指針としている。

暗号技術評価の実施にあたっては、暗号技術評価に実績のある国内及び国外の専門家に委託した評価や学会及び論文誌等で発表された評価を踏まえ、各暗号技術の安全性及び実装性等の特徴を整理する。その結果は、事務局が開催するシンポジウムや報告書等を通じて、一般に公表することを予定している。

2009 年度から 2010 年度にかけては、主に応募された暗号技術の評価を実施する。また、2011 年度には、応募された暗号技術の評価を継続するほか、現リストに掲載されている暗号技術の再評価も行う。

暗号方式委員会、暗号実装委員会及び暗号運用委員会が、評価結果に基づき、「CRYPTREC 暗号リスト（仮称）」（以下、「次期リスト」という。）への暗号技術の記載について判定し、暗号技術検討会に報告する。報告された暗号技術の次期リストへの記載については、暗号技術検討会での検討を経た後、最終的に総務省及び経済産業省において決定される。決定については、2012 年度実施を予定している。

３．４．２．公募の対象

2009 年度公募対象の暗号技術の種別は、以下のとおり（表 3.1）である。ただし、主な留意事項としては、

- 応募される暗号技術は、2010 年 9 月末までに、査読付きの国際会議、又は、査読付きの国際論文誌で発表されているか、あるいは、採録が決定されているもの。
- 評価する際に知的財産の利用が無償で行えるもの。
- 公募する暗号技術、又はそれを実装した製品が、電子政府等の利用に際し、次期リスト策定後 3 年以内までに調達可能なもの。

等を挙げていた。

表 3.1 2009 年度公募対象の暗号技術の種別

暗号技術の種別	仕様の概要
ブロック暗号	平文及び暗号文ブロックサイズが 128 ビットであり、鍵長が 128 ビット、192 ビット又は 256 ビットであるブロック暗号で、現リストに掲載されている暗号技術と同等以上の特長（安全性又は実装性）を持つもの。
暗号利用モード	秘匿に関する 128 ビットブロック暗号及び 64 ビットブロック暗号を対象にした利用モード。
メッセージ認証コード	鍵長が 128 ビットである 128 ビットブロック暗号及び

	64 ビットブロック暗号を利用したメッセージ認証コード。
ストリーム暗号	鍵長が 128 ビット以上であり、平文をビット単位もしくはバイト単位で暗号化するストリーム暗号。
エンティティ認証	電子政府推奨暗号リストに掲載された共通鍵暗号、公開鍵暗号、ハッシュ関数、メッセージ認証コードの組み合わせによって実現されるエンティティ認証、あるいは、安全性を計算量的な困難さに帰着できるエンティティ認証を公募します。エンティティ認証を構成する要素技術は、現リストに掲載されている暗号技術を用いることを原則とします。要素技術として、現リストに掲載されていない共通鍵暗号、メッセージ認証コードを用いる場合は、これらの要素技術を同時に応募する必要があります。また、上記以外の要素技術を用いたエンティティ認証技術の応募も可能。

３．４．３．公募期間

2009 年 10 月 1 日～2010 年 2 月 4 日 17 時

３．４．４．応募暗号技術

2009 年度において、下記のとおり（表 3.2)、6 件の暗号技術について応募があった。

表 3.2　2009 年度応募暗号技術一覧

暗号種別	暗号技術名	応募者
128 ビットブロック暗号	CLEFIA	ソニー株式会社
	HyRAL	株式会社ローレルインテリジェントシステムズ
ストリーム暗号	Enocoro-128v2	株式会社日立製作所
	KCipher-2	KDDI 株式会社
メッセージ認証コード	PC-MAC-AES	日本電気株式会社
エンティティ認証	無限ワンタイムパスワード認証方式（Infinite One-Time Password)	日本ユニシス株式会社

※暗号利用モードについては応募なし。

３．４．５．事務局選出暗号技術

CRYPTREC におけるリストガイド策定時の検討結果などを参考に、国際標準化等の実績がある以下の暗号技術について、CRYPTREC 事務局より選出した（表 3.3)。

表 3.3　2009 年度事務局選出暗号技術一覧

暗号種別	暗号技術名	評価仕様
メッセージ認証コード	CBC-MAC	ISO/IEC 9797-1
	CMAC	NIST SP 800-38B
	HMAC	NIST FIPS 198-1

暗号利用モード	CBC モード	NIST SP 800-38A
	CFB モード	NIST SP 800-38A
	OFB モード	NIST SP 800-38A
	CTR モード	NIST SP 800-38A
	GCM モード	NIST SP 800-38C
	CCM モード	NIST SP 800-38C
エンティティ認証	共通鍵暗号利用による認証プロトコル	ISO/IEC 9798-2、対称暗号化アルゴリズムを使用する機構
	電子署名利用による認証プロトコル	ISO/IEC 9798-3、デジタル署名技術を使用する機構
	検査関数（MAC）による認証プロトコル	ISO/IEC 9798-4、暗号検査機能を使用する機構

※128 ビットブロック暗号及びストリーム暗号については選出なし。

３．５．応募暗号の評価スケジュール

2012 年度の電子政府推奨暗号リストの改訂に向けた応募暗号の評価スケジュールをまとめると以下の通り（図 3.4）。

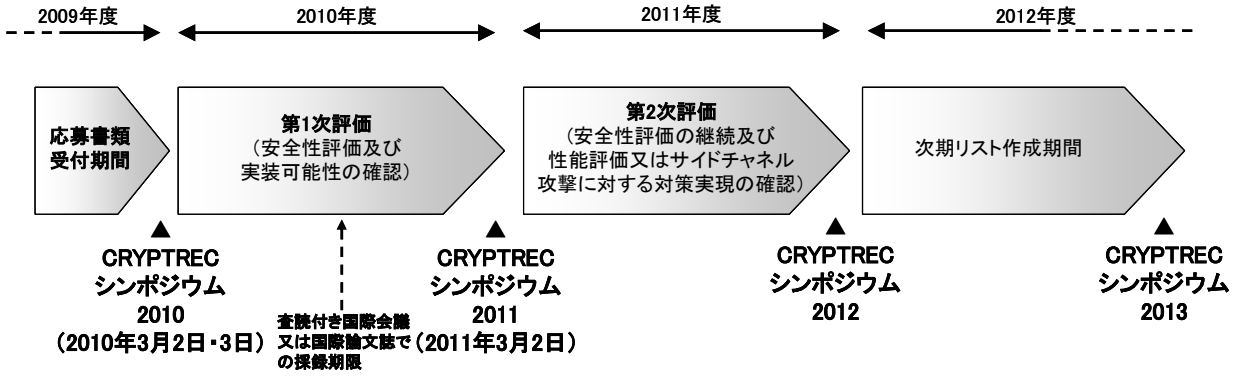


図 3.4 評価スケジュール

CRYPTREC シンポジウム 2010 開催：	2010 年 3 月 2 日・3 日
第 1 次評価実施：	2010 年 4 月～2011 年 3 月
CRYPTREC ジンポジウム 2011 開催：	2011 年 3 月 2 日
第 2 次評価実施：	2011 年 4 月～2012 年 3 月
CRYPTREC シンポジウム 2012：	2012 年 3 月頃
CRYPTREC シンポジウム 2013：	2013 年 3 月頃

2010 年度にかけては、主に応募された暗号技術の評価を実施する。また、2011 年度には、応募された暗号技術の評価を継続するほか、現リストに登録されている暗号技術の再評価も行う。

暗号方式委員会及び暗号実装委員会が、評価結果に基づき、「CRYPTREC 暗号リスト（仮称）」（以下、「次期リスト」という。）への暗号技術の記載について判定し、暗号技術検討会に答申する。答申された暗号技術の次期リストへの記載については、暗号技術検討会で

の検討を経た後、最終的に総務省及び経済産業省において決定される。決定については、2012 年度実施を予定している。

３．６．応募暗号の評価項目

安全性評価項目と実装性評価項目の 2 つに大別される。

（１）安全性評価項目

既知の一般的な攻撃法に対する耐性を評価する。また、その暗号に特化した攻撃法や、ヒューリスティックな安全性の根拠も評価の対象とすることがある。

（２）実装性評価項目

提出資料に基づいて、実現可能性の確認を行います。性能の評価に関して、ソフトウェア実装では、標準的なプラットフォーム上での性能（処理速度、メモリ使用量等）を評価する。また、ハードウェア実装（エンティティ認証を除く）では、使用するプロセス（FPGA[1]、ASIC[2]等）別に性能（処理速度、使用セル数又はゲート数等）を評価する。また、一部の暗号技術に対しては、サイドチャネル攻撃に対する対策実現の確認も行う。

なお、2009 年度公表した公募要項では、実装性評価の実施に際して、明確でない部分があったため、2010 年度暗号実装委員会において詳細を検討した。その結果は、CRYPTREC 統一 Web サイト（http://www.cryptrec.go.jp/）などを通じてアナウンスする予定である。

[1] FPGA：Field Programmable Gate Array
[2] ASIC：Application Specific Integrated Circuit

３．７．第１次評価の進捗状況

３．７．１．応募暗号技術の評価状況

2010 年度における応募暗号技術及び事務局選定暗号技術に関する第 1 次評価の進捗状況は以下の通りである。

表 3.5　応募暗号技術の第 1 次評価結果

暗号種別	暗号技術名	提案者	評価継続の要否
128 ビットブロック暗号	CLEFIA	ソニー株式会社	引き続き第 2 次評価を行う。
	HyRAL	株式会社ローレルインテリジェントシステムズ	128 ビット鍵長から 255 ビット鍵長においては、現在のところ問題点は見つかっていないが、256 ビット鍵長の場合、極小的な数であるが等価鍵の発見及び現実的な計算量での導出法が示された。よって、現リストに掲載されている暗号技術と同等以上の安全性を持たないと判断し、第 1 次評価までで評価終了とし、次期リストには掲載しない。
ストリーム暗号	Enocoro-128v2	株式会社日立製作所	引き続き第 2 次評価を行う。
	KCipher-2	KDDI 株式会社	引き続き第 2 次評価を行う。
メッセージ認証コード	PC-MAC-AES	日本電気株式会社	引き続き第 2 次評価を行う。

※ 暗号利用モードについては応募なし。

※ エンティティ認証に応募された無限ワンタイムパスワード認証方式については、2010 年 9 月末までに、査読付きの国際会議又は査読付きの国際論文誌で発表されなかったことにより、応募資格を喪失した。

３．７．２．事務局選出暗号技術の評価状況

表 3.6　応募暗号技術の第 1 次評価結果

暗号種別	暗号技術名	評価仕様	評価継続の要否
メッセージ認証コード	CBC-MAC	ISO/IEC 9797-1	今後、注意すべき利用方法や利用方法に関する注釈等について検討した上で、次期リストに掲載する。
	CMAC	NIST SP 800-38B	
	HMAC	NIST FIPS 198-1	
暗号利用モード	CBC モード	NIST SP 800-38A	
	CFB モード	NIST SP 800-38A	
	OFB モード	NIST SP 800-38A	
	CTR モード	NIST SP 800-38A	
	GCM モード	NIST SP 800-38C	
	CCM モード	NIST SP 800-38C	
エンティティ認証	共通鍵暗号利用による認証プロトコル	ISO/IEC 9798-2、対称暗号化アルゴリズムを使用する機構	一部のタイプに脆弱性を発見したので、それらについては利用しないよう注釈を付けた上で、次期リ

	電子署名利用による認証プロトコル	ISO/IEC 9798-3、デジタル署名技術を使用する機構	ストに掲載する。ただし、脆弱性の発見されたタイプに関しては、修正方法が存在するので、ISO/IECに対して修正を求め、修正が完了し次第、注釈に関して再検討を行う。
	検査関数（MAC）による認証プロトコル	ISO/IEC 9798-4、暗号検査機能を使用する機構	

※128ビットブロック暗号及びストリーム暗号については選出なし。

３．８．CRYPTREC シンポジウム 2011 の開催

2010 年度は、電子政府推奨暗号リストの改訂のための暗号技術公募（2009 年度）に応募された暗号技術に関する安全性評価を実施した。本シンポジウムにおいて、最新の評価結果を公表し、それらについて検討した。

３．８．１．プログラムの概要

日時：2011 年 3 月 2 日（水）10：00～16：00

場所：コクヨホール

主催：独立行政法人情報通信研究機構、独立行政法人情報処理推進機構

共催：総務省、経済産業省

参加人数：約 200 名

表 3.7　プログラム

3 月 2 日(水)	
時間	内容
10:00	開会挨拶
10:05	応募暗号技術の安全性評価について 1 ・ 128 ビットブロック暗号 -CLEFIA -HyRAL ・ メッセージ認証コード -PC-MAC-AES ・ エンティティ認証 -無限ワンタイムパスワード
11:50	昼休み
13:00	応募暗号技術の安全性評価について 2 ・ ストリーム暗号 -Enocoro-128v2 -KCipher-2
14:00	事務局選出暗号の安全性評価について
13:45	実装評価の方法について
15:40	安全性評価に関するまとめ
15:55	閉会挨拶

３．８．２．本シンポジウムで寄せられた意見・コメント等

シンポジウムでは、応募者等から応募暗号の安全性評価及び実装性評価に対する意見・コメントが寄せられた。以下にそれらの概要を記す。

（１） 応募暗号技術の安全性評価について

① CLEFIA

- □ 「弱鍵組」という表現は適切ではない。
  - ➢ 「弱鍵組」のような特性が関連鍵攻撃のような安全性評価につながるかどうか、現時点でははっきりしていない。

② HyRAL

- □ Double Key Modeにおいて排他的論理和を止めれば、鍵スケジュールの安全性は保たれる。
  - ➢ 本公募ではアルゴリズムの修正は認められない。

③ PC-MAC-AES

- □ 安全性証明における 2^{56} がタイトであるかどうかについては未解決である。
- □ 安全性証明よりもむしろ最終的にどの程度安全なのかどうかについて議論すべきである。
  - ➢ 一般的にブロック暗号利用モードにおいて 2^{64} はジェネリックなバウンドと考えられるので、それと比較するのも 1 つの考えである。攻撃手法の妥当性については学会の動向を見ていくのが良いのではないか。

④ Enocoro-128v2

- □ たくさんの鍵の中でどれか 1 個を解読できたら攻撃成功とみなすという攻撃シナリオは攻撃者にとってメリットが非常に小さいと思うが、これを有効とみなすと安全性は 64 ビットレベルに落ちてしまうので、現状で特に問題とは認識されていないのかどうか。
- □ 今後評価を進めていくと現行リスト掲載暗号、たとえば MUGI 等との優位性が問題となるが、アピールする点を確認したい。
  - ➢ MUGI は汎用性の高いストリーム暗号である。Enocoro は非常に小さく作れることを主眼にした、ハードウェアをメインのプラットフォームと考えている。小型実装の観点では、回路規模が小さくて速いのが特徴である。

⑤ KCipher-2

- □ 現行リスト掲載暗号との比較について、アピールする点はないか確認したい。
  - ➢ ソフトウェア実装に優れているという点がある。

（２） 事務局選出暗号

- ISO/IEC 9798-2 と ISO/IEC 9798-4 については現在定期見直しの時期にあることから、今回の評価結果を ISO に提出して、修正すべき点を提案したい。次期リストに付ける注釈について、今後、CRYPTREC において検討していくことが必要になるものと考えられる。
  - 一般ベンダやユーザの立場からは、リストを参照する上で、専門家が書いた前提条件などの注釈よりも、使って良いのか悪いのかの観点の方が重要である。
- エンティティ認証に対する中間者攻撃については、フォーマルメソッドを使った今回の評価において実施されている。

（３） 安全性評価のまとめ

- 関連鍵攻撃やキャッシュ攻撃を評価項目として、現時点で実現性に疑問があるから対象外とするか、長い間安全に使っていくことを念頭に入れ、より安全性の高いものを選出するために対象とすべきかどちらの方が良いか。攻撃の実現性の観点をどの程度考慮に入れて評価に反映させるか。
  - 可能な限り、より安全性の高い暗号を推奨していくのが良いと思う。
  - 正しく使用しても物理的な環境によってシナリオが成立してしまうものと、基本的に正しく使用していない場合に成立してしまうものとでは攻撃の性質が異なるので、別々に考えるべきである。
  - 関連鍵攻撃に関しては、シンプルな関連鍵を使うものから、暗号アルゴリズム事態をオラクルに使うようなものまでいろいろなレベルがあり、それぞれ実現可能性が異なるので、個々に判断すべきである。
  - 関連鍵攻撃やキャッシュ攻撃に対して攻撃が有効とされた AES に関して落とすのは現実的ではない。普及していて取り扱いを変えるという議論とより安全性の高い暗号を選択していくという議論は別にすべきである。普及状況に配慮して攻撃が有効という事実を隠すべきではなく、こういう問題点があるという注釈をつけて、広く情報提供するのが良い。
  - 次期リスト構成は 3 つのブロックに別れていて、利用実績や製品化実績も考慮に入れるので、少々の欠点が見つかっても非常に普及しているような暗号については何らかの配慮が入る場合がある。
- 暗号利用モードの ECB モードに関して、現場では使っている可能性があるので、次期リストの注釈を書くときに配慮をして欲しい。

（４） 実装評価の方法について

- キャッシュ攻撃を外しているのは、評価リソースが限られているので、電力解析に

注力しているからである。AES-NI[3]を使った評価については今後の検討課題である。

- 現行リスト掲載暗号に対してサイドチャネル攻撃対策の有効性確認を行わない理由はなぜか。公平な比較ができるものに関しては、同一環境で同じ実装者が行う方が適切だと思うが、今回の応募暗号については応募者が実装することになったのはどうしてか。
  - サイドチャネル攻撃については対策できることの確認を行うレベルであり、現行リスト掲載暗号と応募暗号との比較は行わないためである。現行リスト掲載暗号は提案されてから時間が経過しており、最適化手法のノウハウも蓄積されている段階にあるが、新規に提案された暗号は最適化の知見が評価側にはあまりないものと考えられる。提案がいかに良いのかということをアピールする形で、応募者の方から現行リスト掲載暗号の性能面で上回る結果を出して欲しい。
- 情報を出したくない応募者はデータを出さなくても良いという選択肢が欲しい。
  - 提出して頂いた性能が本当に出せるのかどうかを検証するのが目的である。推奨する側の CRYPTREC の立場からすれば、きちんと確認し自信をもって推奨できるものを取り揃えたいので、評価を行いたい。
- 今後、電子政府においてもスマートフォン環境における利用が増えると思うので、ARM や Java のような環境における評価が必要である。
- NIST の SHA-3 の選考が行われた後は、ハッシュ関数に関する現行リストの更新が行われると思うが、スケジュールはどうなっているのか。
  - SHA-3 の選考後に検討を開始するものと思う。他のカテゴリについても、重要性の高いものから随時リストの更新を検討していくことになっている。
- ハードウェア実装評価において、ブロック RAM を使っても良いか。
  - 情報提供を主眼としているので、例えばブロック RAM を利用した場合には、どれだけ使ったということを明記して頂きたい。
- サイドチャネル攻撃に関する研究があまり活発でなかった頃に、開発時にサイドチャネル攻撃に対する考慮がされていないとするならば、現行リスト掲載暗号の方が潜在的なリスクが高いと考えられる。新規提案に対して情報提供をして欲しいというからには、現行リスト掲載暗号に対しても情報提供をお願いするか、将来的に CRYPTREC として評価を進めるかどうかの考え方を明確にして欲しい。
  - 現行リスト掲載暗号についても、耐性がどの程度で、対策実装を行った場合、どの程度コストがかかり、どの程度処理性能が低下するのか検証すべきである。
  - 最終的に電子政府推奨暗号を決める段階になって、現行リスト掲載暗号を含めて、改めてサイドチャネル攻撃評価を総合的に考えて欲しい。
- ハードウェア実装評価に関する提出物については、公開等は予定されているのか。
  - ノウハウの塊を公開することは考えていない。ブラックボックスで評価できるように情報提供して頂ければと考えている。

---

[3] Advanced Encryption Standard New Instructions

４.電子政府推奨暗号リスト掲載暗号危殆化時の対応について

４．１．検討の背景・目的

暗号技術検討会では、電子政府推奨暗号リストに掲載する暗号アルゴリズムについて、安全性の監視や評価を継続的に実施し、暗号技術に対する解析・攻撃技術の高度化などの当該リスト策定時からの環境変化に対応するため、これまでに「MD5」、「3key T-DES」、「SHA-1」などに関する安全性情報を提供してきているところである。

特に「SHA-1」及び「RSA1024」に関しては、そのような環境変化により国内外でその安全性の低下に係る懸念や、新たなアルゴリズムへの世代交代の必要性が唱えられており、SSL サーバ証明書、電子署名、電子証明書、タイムスタンプなど、その利用率の高さから、本検討会からの情報などをもとに、政府や各業界などで暗号移行が進んでいる（※１，２）との認識である。

こうした世代交代の時期前後においては、社会的・経済的リスクに直結する急激な安全性低下も懸念される。特に電子政府においては、急激な安全性の低下に備え、あらかじめ緊急避難的な対応（コンティンジェンシープラン）の策定が各省庁に求められているところ（※３）であり、電子政府における緊急事案発生時の当該プランの発動に際し政府における緊急事案発生の判断を行うための情報源の一つとして、本検討会の技術情報も期待されているところでもある。

本検討会においては、２００２年度において、電子政府推奨暗号の監視の具体的な手法や、危殆化した暗号アルゴリズムの当該リストからの削除スキーム等について検討された（※４）が、緊急時の対応については議論されていないとの認識である。

こうした電子政府における動向や、本検討会からの情報提供の電子政府における重要度をかんがみると、本検討会としては、緊急時における迅速で正確な対応を実現するため、事前に各委員会の役割や情報伝達の流れなどについて検討しておくことが必要であると考えられる。

４．２．検討事項・検討の進め方

本検討会は、電子政府推奨暗号リストに掲載する暗号アルゴリズムの急激な安全性の低下時における暗号技術検討会及び各委員会の役割と連携方策について以下のとおり検討を進めることとした。

（１）検討事項

ア．急激な安全性低下事案発生時における各委員会の役割、及びそれを踏まえた全体の情報伝達の流れ

イ．各委員会で取るべきアクション、検討が必要な項目、及び外部への情報提供のタイミング

ウ．各委員会で判断を行うための想定検討期間

（２）検討の進め方（経緯）

・　第１回暗号技術検討会において事務局から検討の背景及び趣旨並びに次に掲げる検討事項案等を提案。

ア．緊急時業務の検討事項案
(1) 緊急対応を開始する契機（アラームトリガー）
　緊急対応を開始する契機となる事象
　（緊急対応を開始する緊急度の目安を含む。）
(2) 緊急対応時に執る行動（アクション）
　アラームトリガーを受けての行動
(3) 緊急対応時に検討するべき事項（役割）
　アクションにおける所要の作業内容
(4) 想定検討期間
　役割の遂行に要する期間の目安
(5) 委員会としてのアウトプット
　委員会外部へ伝達すべき事項
　（委員会外部との連携に要する事項を含む。）
(6) 検討課題
　(1)から(5)までを実現するために整理を要する事項

イ．情報伝達フロー
　関係者間の相関に係る概念

・　第２回暗号技術検討会までの期間に、各委員会において、通常業務に比し緊急業務として特に作業や整理を要する事項を調査。

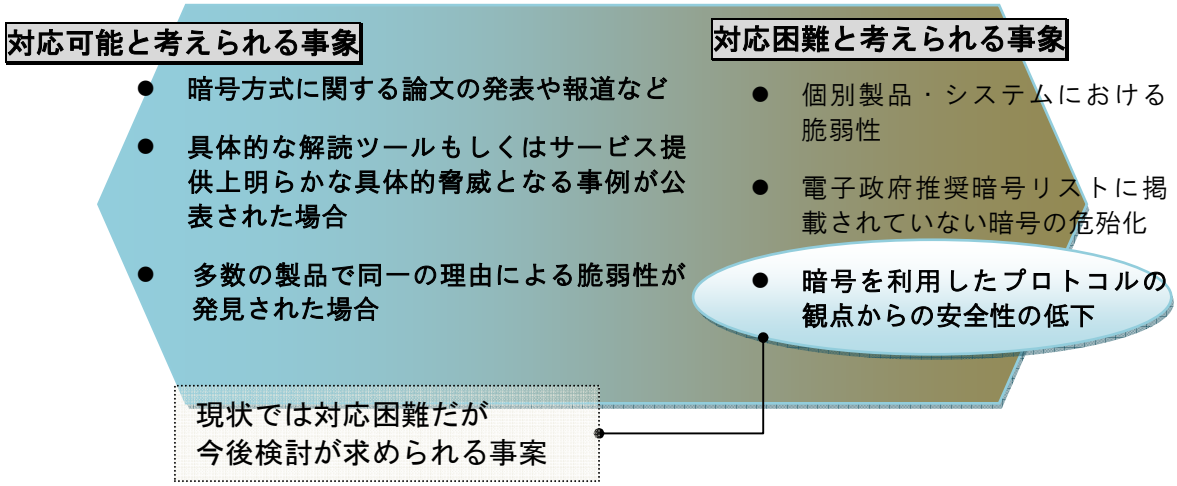
・　加えて、他の委員会との連携の在り方や、情報伝達フローを策定。

（３）検討結果

第１回暗号技術検討会から示された検討事項案「緊急時業務の検討事項案」に対し、各委員会で検討が行なわれ、暗号技術検討会及び各委員会における暗号危殆時対応案として取りまとめた。また、同じく示された検討事項案「情報伝達フロー案」に対する暗号技術検討会及び各委員会の相関案について取りまとめた。これらの検討結果は第２回暗号技術検討会（メール審議）に提出された。

本検討結果は、特に検討事項案「緊急時業務の検討事項案『(6) 検討課題（実現するために整理を要する事項)』」が多々考えられることを前提に、現在の暗号技術検討会の体制で対応可能な暗号危殆化事案としてとりまとめたものであることに留意されたい。

参考：危殆化事案の対応可能性



※１　電子政府情報システムは、「政府機関の情報システムにおいて使用されている暗号アルゴリズム SHA-1 及び RSA1024 に係る移行指針」（平成２０年４月２２日情報セキュリティ政策会議決定）に従い、各省庁で暗号移行計画を実行中。

※２　電子署名及び認証業務に関する法律（平成１２年法律第１０２号）に基づき認定を受けた民間認証局は、２０１３年度中に新アルゴリズムへ移行することを計画中。

※３　情報セキュリティ２０１０（平成２２年７月２２日　情報セキュリティ政策会議決定）

※４　暗号技術検討会２００２年度報告書を参照。

５．暗号方式委員会活動報告

５．１．活動の概要

暗号方式委員会は、電子政府推奨暗号リストに掲載された暗号に対する攻撃の予兆や被害に関する情報収集・分析を実施、電子政府推奨暗号リストの改定に向けた暗号技術の評価、および将来電子政府での利用が見込まれる暗号技術の調査を行うために、2008 年度まで開催していた暗号技術監視委員会を引き継ぐ形で、2009 年度から組織された。

暗号方式委員会では、電子政府推奨暗号の監視、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・検討及び電子政府推奨暗号リスト改訂に関する安全性評価を行う。

以下に、2010 年度の暗号方式委員会の活動内容について報告する。

５．１．１．今年度の活動指針

今年度は、2013 年から運用開始予定である新リスト体系の構築に向けて 2009 年度に実施した暗号技術公募に従い、新たに提案された応募暗号技術、および国際標準等から事務局で選出した暗号技術について、安全性評価を実施した。また、現在の電子政府推奨暗号リストに掲載されている暗号技術の安全性に関する監視活動を行った。この監視活動は、SHA-3 等の海外動向との整合性に関する検討も含む。この他、リストガイドの拡充も行った。

監視活動は、情報収集、情報分析、審議及び決定の 3 つのフェーズからなる。暗号技術検討会における電子政府推奨暗号の監視に関する基本的考え方は以下の通りである。

（１）実運用環境において安全性に問題が認められた電子政府推奨暗号は原則としてリストから削除する。
（２）電子政府推奨暗号の仕様変更は認めない。
（３）電子政府推奨暗号の仕様変更に到らないパラメータの修正等の簡易な修正を行うことにより当該暗号の安全性が維持される場合には、修正情報を周知して当該暗号をリストに残す。

以上の指針に基づき、暗号方式委員会は、研究集会、国際会議、研究論文誌、インターネット上の情報等を収集し、電子政府推奨暗号の安全性に関する情報を分析した。また、暗号技術調査ワーキンググループ（リストガイド）は暗号方式委員会の指示のもとに監視活動として必要な調査・検討活動を担当した。

また、第１回暗号技術検討会での検討を踏まえ、電子政府推奨暗号リストに掲載された暗号アルゴリズムの安全性が急激に低下した場合の対応方針についても検討を

行った。

５．１．２．暗号方式委員会開催状況

2010 年度、暗号方式委員会は、表5.1 の通り 2 回開催された。委員会の開催日及び主な議題は以下の通りである。

表 5.1　暗号方式委員会の開催

回	年月日	議題
第 1 回	2010 年 7 月 20 日	暗号方式委員会活動方針の検討、暗号技術調査ワーキンググループ活動方針の検討、応募暗号評価方法の検討、監視状況報告
第 2 回	2011 年 2 月 10 日	応募暗号評価結果（案）に係る検討、WG 活動報告、監視情報報告、急激な安全性の低下時における暗号方式委員会の役割の検討

５．２．委員会の調査・検討結果

５．２．１．応募暗号技術及び事務局選出暗号に関する第１次評価

2009 年度に応募された暗号技術と国際標準化等の実績がある暗号技術から事務局が選出した暗号技術に関して、安全性評価を実施した。その概要については、「３．７．第 1 次評価の進捗状況」に記載した通りである。詳細については、CRYPTREC Report 2010 を参照のこと。

５．２．２．監視状況

電子政府推奨暗号の安全性評価について 2010 年度中に収集した全ての情報は「情報収集」、「情報分析」フェーズに留まり、「審議及び決定」には至らず、電子政府推奨暗号の安全性に懸念を持たせるような事態は生じていないと判断した。以降、収集、分析した主たる情報について報告する。

（１）共通鍵暗号の安全性評価について

AES に対する攻撃の研究が盛んな状況は変わらないが、今年度、目立った動きとしては、関連鍵攻撃における解析の自動化と単一鍵攻撃研究の再活性化がある。AES-128 と AES-192 の関連鍵攻撃について、次のような従来より効率の良い結果が得られた。

・AES-128: 7 段(10 段中)を選択平文 2^{97} 個、計算量 2^{97} で攻撃可能
・AES-192: 12 段(12 段中)を選択平文 2^{116} 個、計算量 2^{169} で攻撃可能

一方、AES の単一鍵攻撃について、次のような従来より効率の良い結果が得られた。

・AES-192: 8 段(12 段中)を必要平文数 2^{113}、必要メモリ量 2^{129}、必要計算量 2^{172}
・AES-256: 8 段(14 段中)を必要平文数 2^{113}、必要メモリ量 2^{129}、必要計算量 2^{196}

（２）公開鍵暗号の安全性評価について

昨年度の暗号技術検討会報告書でも報告済みであるが、素因数分解問題に関して、The RSA Factoring Challenge[4] の RSA-768（768 ビット RSA 合成数）一般数体ふるい法で素因数分解されたことが Crypto 2010 で発表された。その後、この記録が更新されたという報告はない。

（３）ハッシュ関数の安全性評価について

Asiacrypt 2010 において、中間一致攻撃の改良によるハッシュ関数 Tiger、MD4、縮約版 SHA-2 への原像攻撃が発表された。SHA-2 への攻撃は IACR の ePrint 2010/016 によると、42 段 SHA-256 の場合 $2^{251.7}$ の計算量で、また 42 段 SHA-512 の場合 $2^{494.6}$ の計算量で、原像を求めることができるとされている。

また、NIST は 2010 年 12 月 9 日付けで SHA-3 コンペティションの最終 5 候補を発表した（表 5.2 参照）。今回の選考では安全性評価に重点が置かれた模様で、第 2 ラウンドの 14 候補に唯一残りハードウェア性能に優れていた日本提案の Luffa は残念ながら落選した。NIST は今後、2012 年春に最後の SHA-3 Candidate Conference を開催、2012 年の終盤に SHA-3 を決定するとしている。

表5.2 第3ラウンド(最終ラウンド)に進んだSHA-3候補一覧

名称	筆頭投稿者	開発国
BLAKE	Jean-Philippe Aumasson	スイス
Grøstl	Lars R. Knudsen	デンマーク、オーストリア
JH	Hongjun Wu	シンガポール
Keccak	The Keccak Team	ベルギー
Skein	Bruce Schneier	米国、ドイツ

第 2 ラウンド候補のハッシュ関数の評価結果は、NIST が「Status Report on the Second Round of the SHA-3 Cryptographic Hash Algorithm Competition」[5]として公表している。

（４）暗号技術標準化動向

暗号標準化動向としては、暗号アルゴリズムの掲載数に関する議論がある。現在、「暗号アルゴリズム」(18033)は、第 1 部:総論、第 2 部:非対称暗号、第 3 部:ブロック暗号、第 4 部:ストリーム暗号の 4 部で構成されている。「暗号アルゴリズム」(18033)に対する最近の改訂で第 2 部と第 3 部に新規のアルゴリズムが追加され、掲

[4] RSA 社（米国）の素因数分解問題に関するコンテスト。既に終了している。[5]
http://csrc.nist.gov/groups/ST/hash/sha-3/Round2/documents/Round2_Report_NISTIR_7764.pdf
[5] http://csrc.nist.gov/groups/ST/hash/sha-3/Round2/documents/Round2_Report_NISTIR_7764.pdf

載数が各々、8 方式と 5 方式となる予定であり、増加傾向にある。2010 年 10 月のベルリン会議において、欧州の暗号研究プロジェクト ECRYPT-II のリエゾンでもある Preneel 教授（ベルギー、KUL）が、第 3 部（ストリーム暗号）に ECRYPT-II のストリーム暗号に関するコンペティションで落選した方式が標準に採用される等という問題が生じ、採用基準を厳しくして掲載数を絞るように提案した。この提案をうけ、SC 27/WG 2 の上位組織である SC 27 では、WG 2 内で研究期間(Study Period)を開始することとし、アンケートと寄書募集の実施が決まった。この検討結果は、CRYPTREC の活動に影響を与える可能性があり、今後とも注意深く SC 27/WG 2 の動向調査し、慎重な対応する必要がある。

５．２．３．国際学会等における発表の動向

（１）国際会議等への参加状況

2010年度は、国内外の学術会議に参加し、暗号解読技術に関する情報収集を実施した。参加した国際会議は、表5. 3に示す通りである。

表 5.3　国際会議への参加状況

学会名・会議名		開催国・都市	期間
PKC 2010	International Conference on Practice and Theory in Public Key Cryptography	フランス パリ	2010 年 5 月 26 日～ 5 月 28 日
LCD	Lattice Crypto Day	フランス パリ	2010 年 5 月 29 日
Eurocrypt 2010	International Conference on the Theory and Applications of Cryptographic Techniques	フランス ニース／モナコ	2010 年 5 月 30 日～ 6 月 3 日
SAC 2010	Selected Areas in Cryptography	カナダ・ ウォータールー	2010 年 8 月 12 日～ 8 月 13 日
Crypto 2010	International Cryptology Conference	米国・ サンタバーバラ	2010 年 8 月 15 日～ 8 月 19 日
CHES 2010	Workshop on Cryptographic Hardware and Embedded Systems	米国・ サンタバーバラ	2010 年 8 月 18 日～ 8 月 20 日
FDTC 2010	Fault Diagnosis and Tolerance in Cryptography	米国・ サンタバーバラ	2010 年 8 月 21 日
2nd SHA-3 Conference	Second SHA-3 Candidate Conference	米国・ サンタバーバラ	2010 年 8 月 23 日～ 8 月 24 日
IWSEC 2010	International Workshop on Security	日本・神戸市	2010 年 11 月 22 日～ 11 月 24 日
Asiacrypt 2010	International Conference on the Theory and Application of Cryptology and Information Security	シンガポール・ シンガポール	2010 年 12 月 5 日～ 12 月 9 日
Pairing 2010	International Conference on Pairing-Based Cryptography	日本・加賀市	2010 年 12 月 13 日～ 12 月 15 日

５．３．暗号技術調査ワーキンググループ（リストガイド）の活動

５．３．１．暗号技術調査ワーキンググループ（リストガイド）の活動目的と経緯

CRYPTREC の暗号監視報告並びに国内外の暗号鍵管理等に関連する標準文書を基に、暗号技術の専門家並びに暗号実装・運用等に関わる専門家の知見を集約し、統一基準 1.5.2.4(1)(b)項に示される暗号鍵におけるフェーズごとの管理手順について、情報提供ならびに推奨事項を取り纏めて、リストガイドを作成した。2010 年度は電子政府システムにおける一般的なガイドについて作成を行うべく、米国における鍵管理の標準である NIST SP 800-57 をベースに、電子政府推奨暗号リストに掲載される公開鍵及び共通鍵暗号について、暗号鍵管理における暗号鍵の生成、有効期限の設定、廃棄、更新、鍵が露呈した場合の各フェーズを検討範囲とした。

SSL、PKI 等を実装するソフトウェア等の設定については、次年度以降の検討課題とする。

暗号技術調査ワーキンググループ（以下、「リストガイド WG」という）の 2010 年度の主要活動項目は、表 5.4 のとおりである。

表 5.4　2010 年度の主要活動項目

ワーキンググループ名	主査	主要活動項目
リストガイド WG	手塚 悟	暗号技術の専門家並びに暗号実装・運用等に関わる専門家の知見を集約し、統一基準 1.5.2.4(1)(b)項に示される暗号鍵におけるフェーズごとの管理手順について、情報提供ならびに推奨事項を取り纏めてリストガイドの作成

５．３．２．リストガイド WG の開催状況

本年度は、暗号技術調査ワーキンググループ（リストガイド）は、表 5.5 の通り計 3 回開催された。

表 5.5　暗号技術調査ワーキンググループ(リストガイド)の開催

回	年月日	議題
第 1 回	2010 年 9 月 27 日	リストガイド策定方法の検討
第 2 回	2010 年 12 月 2 日	リストガイド執筆内容の論点整理と議論、ヒアリング先の検討
第 3 回	2011 年 2 月 4 日	リストガイド（案）レビュー結果に対する修正検討、残課題に関する検討

第 1 回 WG（2010 年 9 月 27 日）では、今年度作成するリストガイド（鍵管理）の執筆内容、作業内容について議論を行った。作業方針としては、事務局で文書作成を行い、作業過程で生じた論点について WG で討議を行うとともに、委員各位にレビューを実施していただき、その結果を反映していくこととなった。また、実務経験者へのヒアリング等を行い、内容の充実をはかることとなった。本年度作成するリストガイド（鍵管理）の記述範囲については、個別システムを念頭に作業ならびにレビューを実施することとなったが、具体的な個別システムについては言及しないこととなった。加えて、個別の暗号プリミティブに関する情報については、監視報告の結果を流用するにとどめ、具体的なパラメータ等の扱いは時間的制約から別途検討することとなった。

第 2 回 WG（2010 年 12 月 2 日）では、作業過程で抽出された論点について議論を行うとともに、レビューの実施要領について合意した。議論を行った論点と議論の概要を以下に示す。

■ 論点 1　鍵の種類に関する取り扱い範囲

- 鍵共有、権限付与に関する鍵は除外する
- 擬似乱数生成器については、リストガイド（擬似乱数生成器）への参照を行う
- SP 800-131 に示される鍵長および有効期限については、米国連邦政府機関内での推奨であることを鑑み、CRYPTREC としての取扱いを検討する必要がある
- 証明書の種類に応じ様々な有効期限があるが、今年度は電子署名法に準拠し「最長 5 年」とし、個別事例については今後の課題とする
- 日本の電子政府の実態に即した鍵の分類に関する議論を行う必要があるが、時間的制約から今後の検討課題とする
- 昨今の社会情勢を鑑み、権限付与に関する鍵の取扱いについても検討が必要である
- IPsec をはじめとする暗号プロトコルにおける暗号鍵の取扱いについて、リストガイド（鍵共有）およびリストガイド（暗号プロトコルにおける暗号鍵管理）の作成が必要である

■ 論点 2　鍵の有効期限の設定指針

- 将来的な鍵の伸長について将来的な鍵長の扱いについて言及を行うべきである
- 有効期限切れ後の対応について、共通鍵の場合については検討が必要である

■ 論点 3　危殆化時の手順

- 鍵の漏洩時の対策に限定する
- 共通鍵暗号において具体的な対策を提供できない場合の取扱いについて検討が必要である
- 章のタイトルを内容に合わせて修正すべきである

■ 論点 4　SP 800-57 で参照されるドキュメントの取扱い

- FIPS 140-2 に言及される部分については「ISO 19790 に準拠」に修正すること

■ 論点 5　その他（用語等）

- レビューにて対応する

第 2 回 WG 終了後、12 月 22 日から 1 月 11 日までの期間で、リストガイド（鍵管理）素案に関する委員レビューを実施した。

第 3 回 WG（2011 年 2 月 4 日）では、委員レビューの結果を集約し、18 の検討項目について議論を行った。主な検討項目とその概要を以下に示す。

■ 暗号技術の用途と異なる用途での鍵の利用

- 同一の鍵を別用途で利用してよいか、電子政府の現状を踏まえてその可否を検討することが必要である

■ 署名生成鍵等の有効期限について

- 今年度のリストガイド（鍵管理）では、長期署名等は取り扱い範囲外としたが、今後検討を行う必要がある
- 署名生成鍵の有効期間と証明書の有効期間を分けて、今後検討を行う必要がある。署名生成鍵と署名検証鍵の有効期間と証明書の有効期間の関係など、法制度等も含めて検討する必要がある

■ 鍵の廃棄手順について

- コピーなどが行われている場合には、トレースや消去したことを確認する必要があるが、技術的な保証と枠組みとしての保証が必要である
- 今年度は、可能な範囲でまとめて、次年度以降の課題とする

５．３．３．リストガイド WG の成果概要

ワーキンググループの活動結果、SO800-57 をベースに、2010 年度版のリストガイドをとりまとめた。その目次(暫定版)を以下に示す。

目次

詳細については、2010 年度版リストガイドを参照のこと。

５．４．今後の予定

暗号方式委員会では、2011 年度においても継続的に電子政府推奨暗号に対する監視活動を実施する、また、2010 年度に第 1 次評価を実施した応募暗号技術のうち、継続評価と決まった暗号技術について現在の電子政府推奨暗号リストに掲載されている暗号技術に対する優位性を中心に、第 2 次評価を実施する。さらに、急激な安全性の低下が発生した場合の暗号方式委員会の役割、および活動についての議論を行う。

また、2010 年度に鍵管理について実施した暗号技術調査ワーキンググループ活動については、典型的な暗号技術における鍵管理手法などについて、継続してリストガイドの作成を実施する。

６．暗号実装委員会活動報告

６．１．活動の概要

暗号実装委員会は、電子政府推奨暗号リストに掲載された暗号を正しく安全に実装するための要件を検討するとともに、サイドチャネル攻撃を初めとする暗号実装関連の技術動向を調査するために、2008 年度まで開催していた暗号モジュール委員会を引き継ぐ形で、2009 年度から組織された。

今年度、暗号実装委員会では、暗号の実装に係る技術及び暗号を実装した暗号モジュールに対する攻撃手法に関する調査・検討と、電子政府推奨暗号リスト改訂に伴う実装性評価に関する調査・検討を行った。また、推奨暗号の安全性が急激に低下したときの CRYPTREC の対応における暗号実装委員会の役割について検討した。

以下に、2010 年度の暗号実装委員会の活動内容について報告する。

６．１．１．今年度の活動指針

今年度は、電子政府推奨暗号リスト改訂の一環として暗号技術の実装性能評価方法を検討するとともに、暗号モジュールに対する攻撃手法の動向を調査するため、また、電子政府システム安全性確保のため、次の項目を実施した。

(1) 実装性評価に関する検討
- 応募暗号技術及び現行の電子政府推奨暗号リスト掲載暗号技術に対するハードウェア実装及びソフトウェア実装の評価項目、評価手法、評価結果の判断基準を作成した。

(2) サイドチャネル攻撃耐性の評価に関する検討
- 応募暗号技術及び現行の電子政府推奨暗号リスト掲載暗号技術のサイドチャネル攻撃耐性に関する確認項目、確認手法を決定した。
- この活動の一環として、暗号モジュールに対するセキュリティ要件及び試験要件の国際標準化に協力した。

(3) サイドチャネル攻撃等の実験データに関する調査・検討
- サイドチャネル解析用プラットフォームである SASEBO ボード等を用いた比較実験を行い、暗号モジュールの安全性・信頼性を評価するための基礎データを収集した。
- 暗号実装技術及び暗号モジュールへのサイドチャネル攻撃等に関する攻撃技術の研究開発動向の調査を行った。

(4) 暗号の安全性が急激に低下したときの暗号実装委員会の役割の検討
- 電子政府システムで利用されている暗号の急激な安全性低下に対する CRYPTREC としての対応における暗号実装委員会の役割を検討した。

また、第１回暗号技術検討会での検討を踏まえ、電子政府推奨暗号リストに掲載された暗号アルゴリズムの安全性が急激に低下した場合の対応方針についても検討を行った。

６．１．２．暗号実装委員会開催状況

2010 年度、暗号実装委員会は、表 6.1 の通り 3 回開催された。開催日及び主な議題は以下の通りである。

表 6.1　暗号実装委員会の開催

回	年月日	議題
第 1 回	2010 年 7 月 23 日	活動計画の具体化のための審議・承認 応募暗号の実装評価についての検討
第 2 回	2010 年 9 月 28 日	応募暗号のソフトウェア実装評価の概要決定 現推奨暗号提案者に対するアンケートの内容検討
第 3 回	2011 年 3 月 4 日	暗号の急激に安全性低下した時の暗号実装委員会の役割検討 応募暗号の実装評価についての検討

６．２．委員会の調査・検討結果

６．２．１．実装性評価に関する検討

応募暗号技術及び現行の電子政府推奨暗号リスト掲載暗号技術に対するソフトウェア及びハードウェア実装性評価の実装環境並びに必要とされる実装性能の基準を検討した。ソフトウェア実装に関しては、評価環境を PC に絞り、実装評価項目の概要を決定し、評価ツールを開発した。ハードウェア実装に関しては SASEBO-GⅡを評価環境として利用することを決定し、実装性能評価の方法を検討した。

６．２．２．サイドチャネル攻撃耐性の評価に関する検討

応募暗号技術及び現行の電子政府推奨暗号リスト掲載暗号技術のサイドチャネル攻撃に対する対策の有効性評価について検討した。評価対象はハードウェア実装のみとし、同じアーキテクチャで対策有り・無しの２種類の攻撃耐性を比較して有効性を評価する方針とした。

６．２．３．サイドチャネル攻撃等の実験データに関する調査・検討

暗号モジュール関連の国際標準化への協力の観点から、暗号モジュールのセキュリティ要求事項 ISO/IEC 19790 およびその試験要件である ISO/IEC 24759 の改訂に対してサイドチャネル攻撃耐性の試験方法・判定基準の提案を目指している。

この活動は 2008 年度まで暗号モジュール委員会の下に置かれた電力解析実験ワーキンググループで行っていたが、電力解析に限定せず、電磁波解析や故障利用解析を含んだ検討を実施するため、2009 年度から「サイドチャネルセキュリティワーキンググループ」と改称し、活動を継承している。今年度は、ISO/IEC 19790 早期改訂にお

けるドラフトに対する日本コメントの原案を作成した。

６．３．サイドチャネルセキュリティワーキンググループの活動

６．３．１．サイドチャネルセキュリティワーキンググループの活動目的と経緯

2008 年度まで、電力解析実験ワーキンググループにおいて、INSTAC-8/-32 準拠ボードや SASEBO シリーズを対象に電力解析実験に関する実験データや学会動向に関する情報収集を行ってきた。しかし、サイドチャネル攻撃は電力解析に限定されるものでなく、電磁波解析や故障利用攻撃も含まれ、活動がワーキンググループ名と一致しなくなったため、2009 年度から CRYPTREC 全体の体制変更に合わせ、電力解析ワーキンググループを継承するものとして、サイドチャネルセキュリティワーキンググループが暗号実装委員会の下に置かれている。本年度は、次の２つを柱として活動した。

（１）ISO/IEC 19790 の早期改訂案の検討

（２）サイドチャネル攻撃検証に関する情報収集

６．３．２．サイドチャネルセキュリティワーキンググループの成果概要

本年度、サイドチャネルセキュリティワーキンググループの活動としては、ISO/IEC 19790 早期改訂のドラフトに対するコメント案作成を２回、メール審議を実施している。

ISO/IEC 19790 第 2 版の 2nd WD 及び 3rd WD に対するコメントを作成し、ISO/IEC JTC1 SC27 に対して SC27/WG3 国内小委員会経由で提出した。

また、サイドチャネル攻撃に関する情報収集も継続して行い、主として SASEBO シリーズの評価用標準ボードを利用した実験データの収集と解析をこれから実施する予定である。

６．４．今後の予定

2010 年度に決定した応募暗号の実装性評価の内容に従い、応募者に 4 種類の実装、性能評価用ソフトウェア、性能評価用ハードウェア実装、サイドチャネル攻撃対策済ハードウェア実装、サイドチャネル攻撃未対策ハードウェア実装の作成を依頼し、提出された実装を用いて実装性を評価する。また、現推奨暗号リスト掲載暗号に関しても、サイドチャネル攻撃対策評価を除く評価を行うが、実装開発は事務局で行う。なお、現推奨暗号の開発者には自分で評価用実装開発の意思があるかを問い合わせる予定である。上記の実装開発・評価の実施は一部外部に委託する予定である。

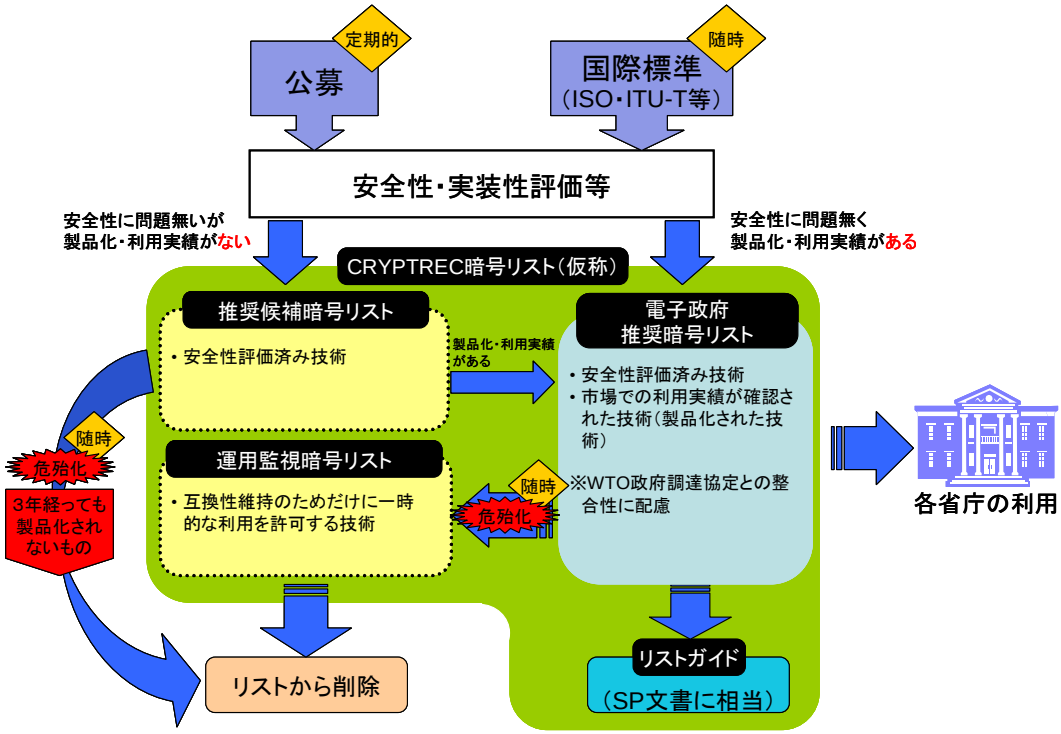
サイドチャネルセキュリティ WG では、引き続き ISO/IEC 19790 の早期改訂ドラフトに対するコメント案作成、サイドチャネル攻撃の研究動向調査を行う。

暗号の急激な安全性低下時の対応に関しては、検討を継続し、暗号実装委員会がアクションの起点となる可能性を探る。

７．暗号運用委員会活動報告

７．１．活動の概要

CRYPTREC では、2012 年度末の電子政府推奨暗号リストの改訂に向けた検討を行っているところであり、新しい電子政府推奨暗号リスト（以下「次期リスト」という。）に掲載される暗号については、政府等による調達等を容易にすることを目的として、「安全性」及び「実装性」の観点に加え、「製品化、利用実績等」の観点も取り入れることとしている。次期リストは、電子政府推奨暗号リスト、推奨候補暗号リスト、運用監視暗号リストから構成され、CRYPTREC 暗号リスト(仮称)として公開する予定である。



暗号運用委員会では、市場における製品化・利用実績等に関する評価の考え方を決める上で、電子政府推奨暗号リストと推奨候補暗号リストとに与える役割を明確にする必要があると考え、今年度は主に電子政府推奨暗号リストの考え方の明確化について検討を行う。具体的には、「電子政府推奨暗号リストの考え方」として 4 つのシナリオを置き、「シナリオの立場を採用したと想定」した時にその実施に伴って予想される「メリット（効果）・デメリット（課題）」、並びに課題解決への方向性を各シナリオについてまとめることを主たる目標に審議を行う。

合わせて、現在の「電子政府推奨暗号リスト」の課題点を抽出し、次期リストをどのような考え方のもとで作成することがよいのかについての情報を得ることを目的として、国内外の主要ベンダを中心に外部アンケートを実施する。本アンケート調査結果から明らか

となった点については「電子政府推奨暗号リストの考え方」に対するシナリオでの特徴的なメリット・デメリットの抽出や評価点を検討するうえでの基礎情報として取り扱う。

以上の結果は、電子政府推奨暗号リストを含む CRYPTREC 暗号リスト（仮称）全体の方向性を今後政府部内で議論する際の客観的資料として用いることを想定している。

また、次期リスト中の運用監視暗号リストに掲載される暗号技術の取り扱いに関連し、本年度は、第 1 回暗号技術検討会からの審議結果に基づき、急激な安全性低下に伴う暗号運用委員会としての対応方針について審議を行う。

以下に、2010 年度の暗号運用委員会の活動内容について報告する。

７．１．１．今年度の活動指針

2009 年度第 2 回暗号技術検討会において、2010 年度の暗号運用委員会での活動項目が以下の通り承認された。

(1) 暗号技術の製品化、利用実績等の評価手法の検討

電子政府暗号推奨リストに登録された暗号技術の利用者、市場における利用実績、国際標準化等に関する 2009 年度の議論を踏まえ、暗号技術の製品化・利用実績の評価手法に関する調査・検討を行い、評価項目の具体化、判断基準の検討等を行う。

また、WTO 政府調達協定との整合性に配慮する観点から、国際標準化された暗号技術、国際的な標準化団体における標準の取り扱い等について調査・検討を行う。

(2) 運用監視暗号リストに登録された暗号技術に関する検討

暗号技術の製品化、利用実績等の評価等を踏まえ、危殆化対策について調査・検討を行う。情報システムの移行における課題を整理しつつ、運用監視暗号リストに登録される暗号技術の取り扱い等について調査・検討を行う。

本年度の暗号運用委員会では、上記事項の具体的検討を行うにあたり、

① 2010 年度以降の活動計画の承認
② 電子政府推奨暗号リストの考え方の明確化に向けた検討
③ 暗号アルゴリズムの利用実態を明らかにするための外部アンケート調査
④ 急激な安全性低下に伴う暗号運用委員会としての対応方針

について審議を行った。

特に、電子政府推奨暗号リストを含む CRYPTREC 暗号リスト（仮称）全体の方向性を今後政府部内で議論する際の客観的資料として用いることを想定して、②及び③について集中的な審議を行うことにより、電子政府推奨暗号の考え方の違いによってどのようなメリット・デメリット・問題点が生じるのかを取りまとめた。

また、第１回暗号技術検討会での検討を踏まえ、電子政府推奨暗号リストに掲載された暗号アルゴリズムの安全性が急激に低下した場合の対応方針についても検討を行った。

７．１．２．暗号運用委員会開催状況

2010 年度の暗号運用委員会は、計 4 回開催された。各回会合の概要は表 7.1 のとおりである。また、第 2 回委員会から第 4 回委員会までの期間を利用し、外部アンケート調査を実施した。

表 7.1.暗号運用委員会の開催

回	開催日時	主な議題
第 1 回	2010 年 9 月 14 日	● 暗号運用委員会活動方針について ● 電子政府推奨暗号リストの考え方の明確化に向けた論点整理について ● 運用監視暗号リスト等に掲載される暗号技術の取り扱い方法について
第 2 回	2010 年 11 月 4 日	● 外部アンケート調査について ● 電子政府推奨暗号リストの考え方の明確化に向けたシナリオ再整理について ● シナリオ議論の論点整理について
	2010 年 12 月 ～2011 年 2 月	外部アンケート調査
第 3 回	2011 年 1 月 20 日	● シナリオ議論における論点項目のとりまとめについて ● 急激な安全性の低下時における運用委員会の役割について
第 4 回	2011 年 2 月 24 日	● アンケート調査結果について ● シナリオ議論における比較評価表のとりまとめについて ● 急激な安全性の低下時における運用委員会の役割について（第 2 回）

７．２．委員会の調査・検討結果

７．２．１．暗号技術の製品化、利用実績等の評価手法の検討

2009 年度第 2 回暗号技術検討会で承認された活動計画に基づき、第 1 回運用委員会にて暗号運用委員会の今後 3 年間の活動内容及びスケジュールが次のように再整理された。本年度の暗号運用委員会の具体的な活動内容については下記 7.2.2～7.2.5 にまとめる。

- **2010 年度活動内容：電子政府推奨暗号の考え方の明確化**

  以下の項目について議論を行い、その結果を取り纏めて電子政府推奨暗号リストの考え方（案）として暗号技術検討会に報告し、審議を求める。

  - 電子政府推奨暗号リストに何を求めるのか
  - その際のメリット（効果）・デメリット（課題）は何か

- デメリット（課題）に対してどのように対応すべきか

- **2011 年度活動内容：製品化、利用実績等の評価手法の検討**

  電子政府推奨暗号リストの考え方を具体的に反映するための製品化、利用実績、国際標準化等の評価手法について、2009 年度の議論を踏まえて検討を行う。

- **2012 年度活動内容：製品化、利用実績等の評価**

  2011 年度の検討結果を踏まえて、実際の製品化、利用実績、国際標準化等の調査・評価を行い、次期電子政府推奨暗号リスト改訂に反映させる。

７．２．２．電子政府推奨暗号の考え方の明確化に向けた評価軸について

「電子政府推奨暗号の考え方（結論）」として 4 つのシナリオ（下記 7.2.3）を置き、各々のシナリオに沿って議論を行う。なお、本委員会では、「どのシナリオを採用すべきか」の議論を必要に応じて今後暗号技術検討会等で行っていく際の情報として、「シナリオの立場を採用したと想定」した時にその実施に伴って予想される「メリット（効果）・デメリット（課題）」の抽出、並びに課題解決への方向性を各シナリオについてまとめることを主たる目的とした。

メリット・デメリットを検討する際にあたり、論点項目としては以下のものを取り扱うこととした。

A) 「安全性」に関する検討項目

(A-1) 電子政府推奨暗号アルゴリズムの安全性評価の充実度や監視活動の効率化に与える影響度の違い

(A-2) 電子政府推奨暗号アルゴリズムの安全性評価・監視活動の実施能力に与える影響度の違い

(A-3) 電子政府推奨暗号アルゴリズムの危殆化に伴う影響度の違い

(A-4) 電子政府推奨暗号アルゴリズムの危殆化対策（バックアップ）を日本政府の独自判断に基づいて実施することの実現可能性の違い

(A-5) その他、安全性に関する項目

B) 「調達容易性」に関する検討項目

(B-1) 電子政府推奨暗号リストと政府調達・製品製造段階での利用暗号アルゴリズム選択に関する相関度の違い

(B-2) 電子政府推奨暗号アルゴリズムの危殆化対策済み（バックアップ搭載）製品の調達コストに与える影響度の違い

(B-3) 電子政府推奨暗号アルゴリズムが政府調達におけるベンダロックイン（応募会社※もしくは関連会社からしか事実上調達できない）の原因となる可能性の違い

(B-4) 電子政府推奨暗号アルゴリズムを選定する際の現在の利用実績の重要度の違い

(B-5) その他、電子政府推奨暗号アルゴリズムの搭載製品・システム調達等における調達容易性に関する項目

C) 「標準化・規格化等への影響」に関する論点項目

(C-1) ISO/IEC や ITU の国際標準化策定に与える影響度の違い

(C-2) ISO/IEC や ITU 以外の様々な規格化(例えば IETF や IEEE など)等の活動に与える影響度の違い

(C-3) 応募会社※による標準化・規格化等への活動に対するモチベーションの違い

(C-4) その他、電子政府推奨暗号アルゴリズムの標準化・規格化等の活動全体に与える影響に関する項目

D) 「提案暗号（国産暗号）の利用促進」に関する論点項目

(D-1) （応募会社※以外の企業・団体等が）電子政府推奨暗号リストに選定された提案暗号（国産暗号）をサポートすることに対するモチベーションの違い

(D-2) 電子政府推奨暗号リストに選定された提案暗号（国産暗号）の知的所有権（特許ライセンス）を全世界特許無償化（worldwide royalty-free）することによる当該暗号アルゴリズムの利用促進効果の違い

(D-3) 応募会社※による提案暗号（国産暗号）の利用促進活動に対するモチベーションの違い

(D-4) 電子政府推奨暗号リストに選定された提案暗号（国産暗号）の利用促進活動を政策的に支援した場合のコストパフォーマンスの違い

(D-5) その他、電子政府推奨暗号リストに選定された提案暗号（国産暗号）の利用促進効果に関する項目

E) 「セキュリティ研究体制への影響」に関する評価項目

(E-1) 企業が新しい暗号アルゴリズムを開発することの位置づけ／モチベーションの違い

(E-2) 日本全体としての暗号研究体制に与える影響度の違い

(E-3) セキュリティ分野の競争力強化に向けた日本全体としてのセキュリティ研究体制の見直し機運につながる影響度の違い

(E-4) その他、セキュリティ研究体制の維持向上への影響に関する項目

F) 「CRYPTREC 活動成果」に関する評価項目

(F-1) 電子政府推奨暗号リストと推奨候補暗号リストとに分割することによる効果の違い

(F-2) 推奨候補暗号リストの位置づけの違い

(F-3) CRYPTREC 活動による成果利用全般に対するコストパフォーマンスの違い
(F-4) その他、CRYPTREC 活動成果に関する項目

※ 応募会社とは、CRYPTREC の前回公募(2001 年)または今回公募（2009 年）に暗号アルゴリズムを提案した企業のことを指す。

７．２．３.「電子政府推奨暗号リストの考え方」に対するシナリオ

「電子政府推奨暗号の考え方（結論)」の 4 つのシナリオは、それぞれの設定意図を参考として、以下のとおりに設定した。

【シナリオ 1（実際に利用されている暗号だけを電子政府推奨暗号に選定)】
CRYPTREC は今まで技術的側面で評価を実施してきたので、電子政府推奨暗号リストの掲載個数を限定するために、**「現状の調達容易性（利用実績)」を主たる判断材料**とし、有力な標準化規格で必須実装に指定されているなどの**「純技術的なその他要件」を考慮**して電子政府推奨暗号リストと推奨候補リストとの区分を行う。

【本シナリオの意図】

暗号方式委員会にて「安全である」と判断されない限りは、「電子政府推奨暗号リスト」はもとより「推奨候補暗号リスト」にさえ掲載されることはない。したがって、両リストの差異は「市場における利用実績が十分か否か」の観点しかない。

一方、2000 年の暗号輸出規制緩和以降は、事実上米国政府標準暗号だけが様々な国際標準化・規格化や製品化の対象として扱われ、そのほかの暗号は様々な国際標準化・規格化もしくは製品化から排除される流れが強まるなど、暗号をめぐる国際環境はこの 10 年で大きく変貌している。このことは、2009 年度に経済産業省が実施した暗号製品採用実績調査結果とも合致している。

以上の点を考慮すれば、「市場における利用実績（調達容易性）が十分か否か」の判断は、**2009 年度（もしくは 2011 年度に再実施する）暗号製品採用実績調査結果をベースに考えれば事実上十分**であるといえる。

【シナリオ 2（国際標準化・製品化促進の手段として電子政府推奨暗号リストを活用)】
「現状での調達容易性（利用実績)」だけで判断した場合には米国政府標準暗号のみが電子政府推奨暗号リストに掲載される可能性が高いうえ、米国政府標準暗号以外の暗号は国際標準化・製品化からも排除される流れが強まっている。
本シナリオでは、上記の点を考慮し、**「安全性」、「現状の調達容易性（利用実績)」ならびに「将来的な調達容易性（利用実績)」の見通しを踏まえ**つつ、電子政府推奨暗号リストの掲載個数を限定したうえで、提案暗号（国産暗号）の普及展開をどのように進めるべきかといった**「非技術的なその他要件」を最大限加味**して、電子政府推奨暗号リストと推奨候補リストとの区分を行う。

【本シナリオの意図】

2000 年の暗号輸出規制緩和以降は、事実上米国政府標準暗号だけが様々な国際標準化・規格化や製品化の対象として扱われ、そのほかの暗号は国際標準化・規格化もしくは製品化から排除される流れが強まるなど、暗号をめぐる国際環境はこの 10 年で大きく変貌している。

結果として、多数の提案暗号が現在の電子政府推奨暗号リストに掲載されているにもかかわらず、応募会社以外からのサポートがほとんど受けられないがゆえに、提案暗号の国際標準化・規格化、及び製品化が進んでいないのが実状である。加えて、米国政府標準暗号は「その他評価が必要な暗号」としてすでに取り扱われており、仮に提案暗号が 1 個も電子政府推奨暗号リストに掲載されなかったとしても政府調達手段として困ることはない。

このような現状を鑑みると、電子政府推奨暗号リストにおける提案暗号をどのように取り扱うべきかについて検討しなおす必要がある。そのひとつの考え方として、日本（政府）が利用する（少数個の）対象暗号を明確にすることにより、**当該暗号の様々な国際標準化・規格化、並びに製品化が国内外で促進され、製品調達が容易になることを期待する手段として電子政府推奨暗号リストを活用**することが考えられる。

【シナリオ 3（一定期間経過後の利用実績不振による電子政府推奨暗号からの降格）】
「現状での調達容易性（利用実績）」だけで判断した場合には米国政府標準暗号のみが電子政府推奨暗号リストに掲載される可能性が高いため、2012 年度末に CRYPTREC 暗号リスト（仮称）が改訂されるのに合わせて、提案暗号の普及展開を強力に実施するモチベーションを応募会社に持たせる必要がある。一方、一定期間経過後の普及展開が思わしくない提案暗号には電子政府推奨暗号リストから降格してもらうルールを導入することにより、将来的に電子政府推奨暗号リストの掲載個数を削減する余地を残す。
本シナリオでは、上記の点を考慮し、一定期間経過後の普及状況を厳格に判定する**「将来的な調達容易性（利用実績）」を重要視**して、電子政府推奨暗号リストと推奨候補リストとの区分を行う。

【本シナリオの意図】

当初から「電子政府推奨暗号リスト」と「推奨候補暗号リスト」に区分されてしまうと、「推奨候補暗号リスト」に入れられた（電子政府推奨暗号リストに掲載されなかった）提案暗号は一段格下の暗号と市場から受け取られる可能性があり、普及展開活動を行う上でマイナスの影響を及ぼす恐れがある。

一方で、ひとたび電子政府推奨暗号リストに掲載された後は利用実績や普及展開が思わしくなくても継続して掲載され続けることになれば、提案暗号の普及展開を強力に実施しない可能性がある。

以上の点を考慮すれば、一定期間経過後の普及状況を厳格に判定するルールを定め、**利用実績や普及展開が思わしくない提案暗号を電子政府推奨暗号リストから降格**させ

ることにより、将来的に電子政府推奨暗号リストの掲載個数を削減する余地を残しつつ、削減に伴う国内におけるセキュリティ研究開発体制への影響軽減に一定の配慮を行うやり方が考えられる。

【シナリオ 4（政府調達の選択肢としての提示。現状とほぼ同様）】
「調達容易性」を判断することは難しいうえ、電子政府推奨暗号リストの掲載個数を削減することによる効果も定かではない。
本シナリオでは、電子政府推奨暗号リストと推奨候補リストとの区分は**「安全性」を主たる判断基準**として行うことにより、現状とほぼ同様の構成とする。

【本シナリオの意図】

提案暗号は電子政府推奨暗号になっても市場でほとんど利用してもらえない現実があり、提案暗号の普及展開への取り組みに対して現在の電子政府推奨暗号リストが役に立っていないことは明らかである。

一方で、電子政府推奨暗号リストに入らなければ政府調達に向けた選択肢として認めてもらえず、応募会社さえも提案暗号の普及展開への取り組みをしなくなり、結果として国内におけるセキュリティ研究体制に対して大きなマイナスの影響を与える恐れがある。加えて、電子政府推奨暗号リストの掲載個数を削減したからといって、電子政府推奨暗号リストに掲載された提案暗号が市場で使われるようになる保証はない。

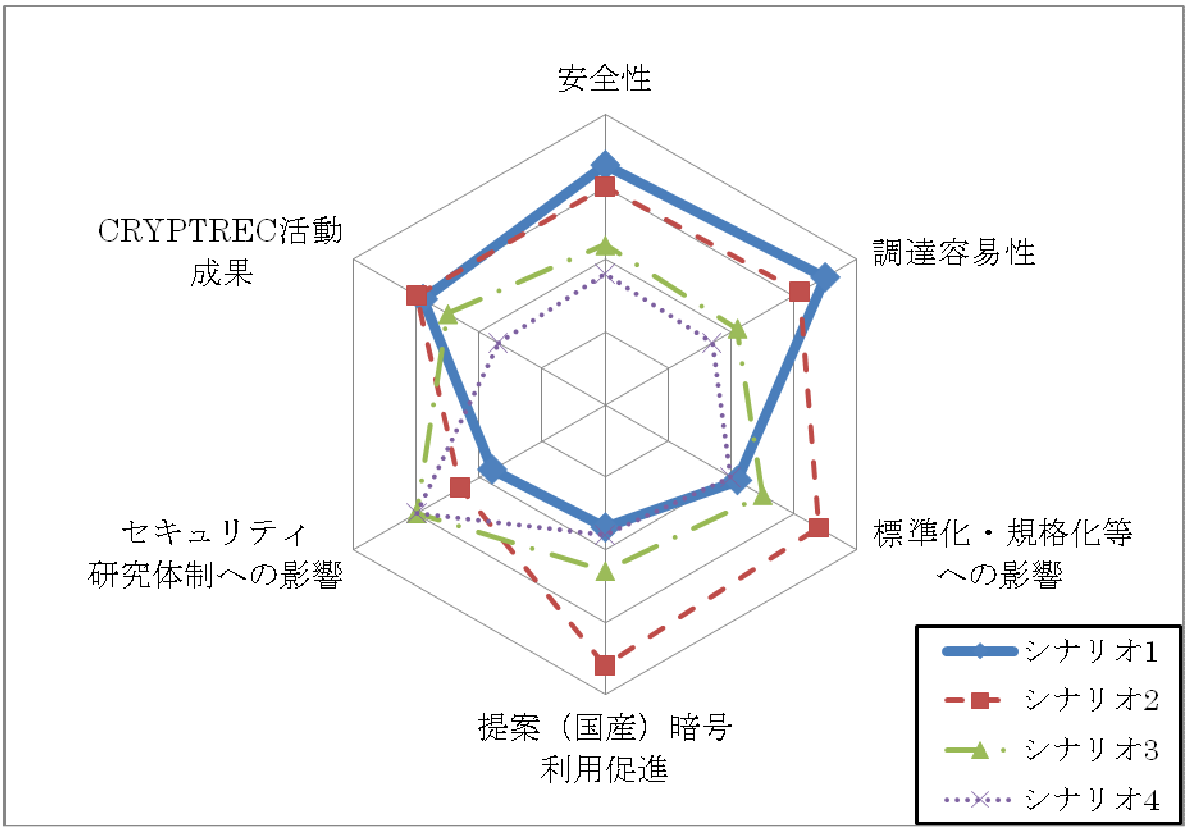
以上の点を考慮すれば、現状とほぼ同様の構成とすることによって、**政府調達に向けた選択肢の提示だけに役割をとどめ**、提案暗号の国際標準化・製品化促進の手段としては考えない。

７．２．４.「電子政府推奨暗号リストの考え方」に対する比較評価

電子政府推奨暗号の考え方（結論）として 4 つのシナリオを先に置いたうえで、それぞれのシナリオを実施したと想定した時に生じると考えられるメリット（効果）やデメリット（課題）の抽出を行った検討結果をもとに、最終的にメリット度合いとしてレーダーチャート表現にまとめたものである。

以下の 4 段階を基準として、シナリオごとに各評価軸のメリット度合いを「評価点」として表現した。一番外側が「4」で内側へ行くごとに「3」「2」「1」となる。

＜評価点＞
4：メリットのほうがかなり多い
3：どちらかといえばメリットのほうが多い
2：どちらかといえばデメリットのほうが多い
1：デメリットのほうがかなり多い



6.2.3 記載のシナリオにおいて、全体的にみると、シナリオ 2、シナリオ 1、シナリオ 3、シナリオ 4 の順にメリットが大きいと判断された。

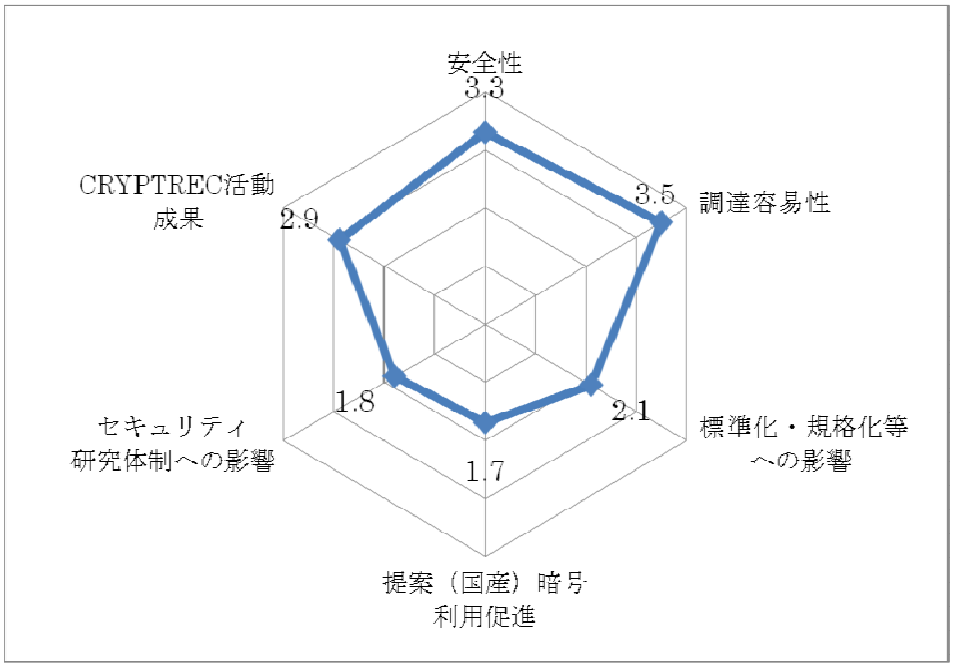
他方、「セキュリティ研究体制への影響」の評価軸における評価点とそれ以外の評価軸における評価点との出方が反対になっていることが象徴的である。これは、日本における暗号研究体制と現実の暗号利用実態との間で大きな乖離が生じている可能性があることを意味する。その結果、どのシナリオを取るにせよ、以下のような大きな問題が生じることが予想される。

なお、**上記の評価点は、それぞれのシナリオにおける以下の問題点が解消される、もしくは解消するための施策とセットで実施することが前提**となっていることに注意されたい。すなわち、以下の問題点が解消される施策がセットで行われない場合には、必ずしも上記の評価点が得られるとは限らない。

シナリオ No	問題点	問題点の解消法(案)
1	① 民間企業が新たな暗号アルゴリズムを開発する必要性が低下し、民間企業で暗号研究者を抱えられなくなる ⇒ CRYPTREC における暗号評価・監視に民間企業の暗号研究者が大きな役割を果たしているため、民間企業の暗号研究者の減少は暗号評価・監視が出来なくなることを意味する	暗号研究者の公的機関における雇用が必要(公的機関での暗号評価・監視の可能性)
2	① 民間企業が新たな暗号アルゴリズムを開発する必要性が低下し、民間企業で暗号研究者を抱えられなくなる ⇒ 応募企業間で優劣がつく可能性があり、シナリオ No1 よりも顕在化する時期が早い可能性あり ② 提案暗号の絞り込みが大変 ⇒ 従来の CRYPTREC のやり方から見ると大きな軌道修正になる ③ 絞り込んだとして本当に使われるのか疑問 ⇒ 絞り込むことによるメリットを生かせないとやる意味がない	① 暗号研究者の公的機関における雇用が必要(公的機関での暗号評価・監視の可能性) ② 広く使われるように提案暗号を振興することが目的であることを明確化 ②-1 パテントフリー等の実施 ②-2 推奨暗号リストから外れた組織への対応 ②-3 ISO 等からとのリエゾン関係構築 ③ プロトコル等へ活動範囲を展開(注力先の変更)
3	① 結局、現状と変わらない可能性が高い ⇒ いずれシナリオ No1 かシナリオ No4 になるのではないか？ ⇒ (応募企業以外も広く利用するような)提案暗号の振興が目的にないのであれば CRYPTREC を継続する産業政策的意義は少ない ② 現状のまま継続しても、提案暗号の利用機会が少ない現状から見て、いずれ民間企業で暗号研究者を抱えられなくなるのではないか ⇒ 気がついたときには暗号評価、監視をするための体制がない事態も想定される	(意見なし)
4	① 現状と変わらないと思われる ⇒ (応募企業以外も広く利用するような)提案暗号の振興が目的にないのであれば CRYPTREC を継続する産業政策的意義が説明できない ② 現状のまま継続しても、提案暗号の利用機会が少ない現状から見て、いずれ民間企業で暗号研究者を抱えられなくなるのではないか ⇒ 気がついたときには暗号評価、監視をするための体制がない事態も想定される	(意見なし)

以下では、各シナリオについての個別の評価結果を述べる。主な特徴点は、評価点を決める上で大きな要因となったメリット・デメリットを挙げたものである。なお、詳細なメリット・デメリット・留意点の取りまとめ状況については CRYPTREC Report 2010 を参照されたい。

【シナリオ１（実際に利用されている暗号だけを電子政府推奨暗号に選定）】



＜安全性＞

- 全世界の安全性評価研究成果結果を享受することができるため、安全性評価結果に対する蓄積・信頼性が厚い。また、監視活動が効率化できることで、監視コストが最も軽減できる
- 電子政府推奨暗号アルゴリズムは実際に広く使われる暗号なので、実装上のミスが少なく保守も容易になるため、むしろ安全性は高い
- 特定の電子政府推奨暗号アルゴリズムが広く利用されている可能性が高く、当該推奨暗号アルゴリズムが危殆化した場合の影響は広範囲に渡り、緊急対応すべき影響範囲は極めて大きい
- 電子政府推奨暗号アルゴリズムに対する危殆化に関する影響、対策に関する情報が国内外から得られ、的確で迅速な対応が可能となる

＜調達容易性＞

- 電子政府推奨暗号リストと製品調達上の利用可能暗号アルゴリズムとの親和性は極めて高い
- 提案暗号をバックアップに利用することは難しいが、米国の対応方針に沿って形成された市場からバックアップ製品を調達することができると考えられる
- あらゆるベンダの製品について電子政府推奨暗号アルゴリズムの多くに対応したモジュールが開発されるので、暗号アルゴリズムとしてのベンダごとの差異が少なくなり、ベンダロックインの要因になる恐れはない
- 日本独自の判断で、現時点で主流の暗号アルゴリズムから将来的に別のものに誘導しようとしても、実施は極めて困難

＜標準化・規格化等への影響＞

- 電子政府推奨暗号アルゴリズムは国際標準化・規格化済みと考えられ、ほとんど影響を与えることはない
- 提案暗号を国際標準化・規格化に提案する際、電子政府推奨暗号リストに含まれず推奨候補暗号リストに掲載されることになるので、普及度の低いものとして不利な解釈を受ける可能性がある
- 提案会社の国際標準化・規格化活動への支援材料にはならない可能性が高いため、応募会社のモチベーションを上げることは難しい

＜提案暗号（国産暗号）の利用促進＞

- 全世界特許無償化しても、提案暗号が電子政府推奨暗号リストに入らなければサポートするメリットが見出せず、採用拡大は期待できないため、（米国政府標準暗号によって）寡占されたままになる
- 提案暗号が電子政府推奨暗号アルゴリズムに選ばれる可能性は高くなく、支援対象が政策的に支援したい対象とマッチするとは限らない

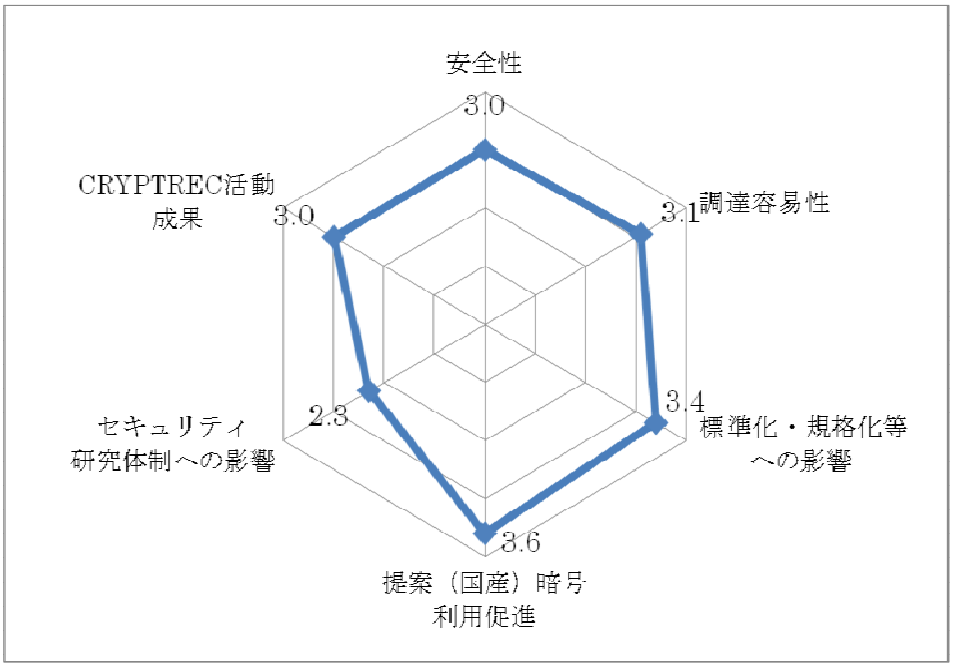
＜セキュリティ研究体制への影響＞

- 新しい暗号アルゴリズムを開発しても市場で受け入れられる可能性は低い。電子政府推奨暗号リスト入りするのは困難であり、推奨候補暗号リストでは普及が見込めないのでモチベーションが低下する
- 現在主流の暗号アルゴリズムの寿命が十分あると見込まれる間は独自暗号開発不要論が強まる可能性があり、特に企業における暗号研究体制の縮小が余儀なくされる恐れがある
- 欧米のように、現在の暗号アルゴリズム主体の研究体制からセキュリティ応用研究や特定用途向けセキュリティ研究主体の研究体制へのリソースシフトを促す効果が期待できる

＜CRYPTREC 活動成果＞

- 電子政府推奨暗号リストと推奨候補暗号リストで差異化が図られるので、リストの役割が明確化され、参照しやすくなる
- 電子政府推奨暗号リストに活動を注力でき、コストパフォーマンスが良い
- 提案暗号が推奨候補暗号リストから電子政府推奨暗号リストへ昇格できる可能性はほとんどない
- 結果的に米国政府の動きを追随する形になり、日本独自の施策がほとんど含まれていないため、事実上、CRYPTREC の活動の必要性低下が懸念される

【シナリオ 2（様々な標準化・製品化促進の手段として電子政府推奨暗号リストを活用）】



＜安全性＞

- 電子政府推奨暗号アルゴリズムの個数を限定するため、当該推奨暗号アルゴリズムに対する注目度が国内外で高まることが期待でき、安全性評価や監視活動を効率的に実施することができる。監視コストも軽減される
- 電子政府推奨暗号アルゴリズムは実際に広く使われる暗号なので、実装上のミスが少なく保守も容易になるため、むしろ安全性は高い
- 特定の電子政府推奨暗号アルゴリズムが広く利用されている可能性が高く、当該推奨暗号アルゴリズムが危殆化した場合の影響は広範囲に渡り、緊急対応すべき影響範囲は極めて大きい
- 電子政府推奨暗号アルゴリズムの個数を限定するため事前に相互接続等の必要な準備を整えておくことが可能であるので、危殆化時のバックアップとして迅速に供することができ、危殆化の影響を低減できると期待される

＜調達容易性＞

- 限定された電子政府推奨暗号アルゴリズムとしての提案暗号の位置づけが明確になり、利用の期待が高まる、あるいは調達基準として明確になれば、当該提案暗号の製品化が促進され、調達コストに与える影響が最低限に抑えられる
- 電子政府推奨暗号アルゴリズムの個数を限定するので当該推奨暗号アルゴリズムを搭載した製品が存在していると期待することができ、バックアップとして調達することが容易であると考えられる
- 電子政府推奨暗号アルゴリズムとしての提案暗号の位置づけが明確になれば、多くの企業の製品に当該提案暗号が搭載されることが期待できるので、ベンダロックインの要因になる恐れは少ない

- ある程度の製品数が整うまでの期間、危殆化対策済み（バックアップ搭載）製品を調達しようとすると、調達先が限定、もしくはコスト高につながる恐れがある
- 提案暗号の普及展開を重視すると利用実績だけでは判断できず、他の指標が必要。調達における基準の平等性の担保が確保できない可能性がある

＜標準化・規格化等への影響＞
- 電子政府推奨暗号リストが提案暗号の国際標準化・規格化促進手段として活用されれば国内外での注目が集まり、国際標準化（ISO/IEC や ITU）・規格（例えば IETF や IEEE）策定が促進される可能性がある
- 公的なお墨付きとして安全性評価の裏付けや電子政府への採用実績を紹介できる
- 電子政府推奨暗号アルゴリズムに選ばれた応募会社にとっては国際標準化や様々な規格化への支援材料になることが期待できるため、国際標準化や規格化活動へのモチベーションが上がる
- 電子政府推奨暗号アルゴリズムに選ばれなかった応募会社にとっては国際標準化や様々な規格化活動へのモチベーション向上につながらない

＜提案暗号（国産暗号）の利用促進＞
- 提案暗号が電子政府推奨暗号リストに含まれ製品化促進手段として活用されることで、促進策の内容がそのまま提案暗号をサポートすることに対するモチベーションにつながり、当該提案暗号の利用促進が期待できる
- 電子政府推奨暗号アルゴリズムの個数が限定されるため、政策的な支援の意図が明確になる上一つあたりの利用促進のためにかけられるコストが大きくなるので、当該提案暗号に対して効果的な支援が可能
- 電子政府推奨暗号リストに選ばれた提案暗号について特許無償化と国際標準化・規格化の促進により、他社（提案会社や他のシステム開発会社等）からの製品化・サポートも受けやすくなるため、当該提案暗号の利用が促進される可能性がある
- ベンダロックインを回避するためには全世界特許無償化をしていない提案暗号を利用促進活動の対象とすることはできない

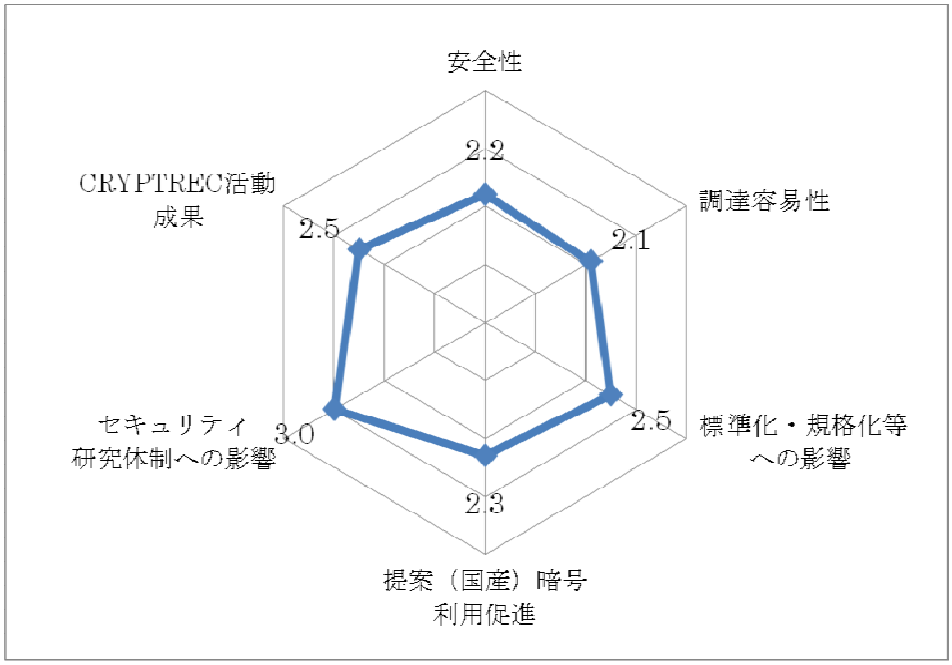
＜セキュリティ研究体制への影響＞
- 電子政府推奨暗号アルゴリズムの個数を限定するため、新しい暗号アルゴリズムを開発しても電子政府推奨暗号リスト入りするのは困難であり、推奨候補暗号リストでは普及が見込めないのでモチベーションが低下する
- 電子政府推奨暗号アルゴリズムの個数を限定するため、独自暗号開発不要論が強まる可能性があり、企業としての暗号研究体制の縮小の可能性がある
- 国産暗号として有望な暗号アルゴリズムが開発された場合には、応募会社の枠を超え官学民からのバックアップが期待される
- 欧米のように、現在の暗号アルゴリズム主体の研究体制からセキュリティ応用研究

や特定用途向けセキュリティ研究主体の研究体制へのリソースシフトを促す効果が期待できる

＜CRYPTREC 活動成果＞

- 電子政府推奨暗号リスト選定には提案暗号の普及展開の要素が必要であり、その判断・運用を行う組織として、CRYPTREC 活動の必要性を主張できる
- 電子政府推奨暗号リストに活動を注力でき、コストパフォーマンスが良い
- 電子政府推奨暗号リストと推奨候補暗号リストで差異化が図られるので、推奨する提案暗号を明確にするという意味から極めて明確
- 提案暗号の普及展開をどのように進めるべきかといった「その他」の要素が明確にならない限り、リストの位置づけは不明確
- 電子政府推奨リストに選ばれた提案暗号のプロモーションのためのコストが発生する

【シナリオ 3（一定期間経過後の利用実績不振による電子政府推奨暗号からの降格）】



＜安全性＞

- 代替暗号アルゴリズムの選択肢がある程度選択肢として用意されており、危殆化対策としてある程度の実現可能性はある
- 学会等での注目度の低い暗号アルゴリズムでは安全性評価の蓄積が少なく、普及度判定時に安全性の再評価が必要となる可能性がある。また暗号アルゴリズムごとに評価を行う暗号研究者が固定化されやすく、全体の安全性評価の充実度につながらない
- 電子政府推奨暗号アルゴリズムの数は多いが、実際に利用される暗号は限定される

ため、結果として実装・保守における安全性はシナリオ 1, 2 と同程度になると考えられる

- 電子政府推奨暗号アルゴリズムの数で考えればシナリオ 1, 2 よりもいずれかの電子政府推奨暗号アルゴリズムが危殆化する可能性は高い。広く利用されていない電子政府推奨暗号アルゴリズムが危殆化した場合、経済的な影響は限定的となる可能性があるが、「CRYPTREC がお墨付きを与えていた暗号（電子政府推奨暗号）が危殆化した」という点で CRYPTREC の信用が低下する可能性がある

＜調達容易性＞

- 意図してバックアップのアルゴリズムを用意する場合、選択肢が豊富
- サポートすべき電子政府推奨暗号アルゴリズムが明らかではなく、製品化を行う際の指針とはならないため、応募会社以外の暗号アルゴリズムの利用はすでにシェアを握った一部に限られる。そのほかの暗号アルゴリズムの製品化は進まず、調達先は依然限定され調達コストは高くなる
- 特定製品にしか搭載されていない電子政府推奨暗号アルゴリズムが採用されると将来にわたってベンダロックインが発生する恐れがある
- 採用した電子政府推奨暗号アルゴリズムが利用実績不足を理由に推奨候補暗号リストへ降格する恐れがある

＜標準化・規格化等への影響＞

- 電子政府推奨暗号アルゴリズムに選ばれた応募会社にとっては国際標準化への支援材料になると期待できるため、これらの国際標準化活動へのモチベーションはある
- 公的なお墨付きとして安全性評価の裏付けや電子政府への採用実績を紹介できる
- 複数の提案暗号が電子政府推奨リストに残る場合には、日本としてどの暗号アルゴリズムを必要としているのがはっきりしない、また普及状況により電子政府推奨暗号リストから外される可能性もあるため、日本からの国際標準化・規格化への提案が軽視もしくは無視される可能性が高い
- 提案会社は自らが興味を持つ国際標準化・規格化しか推進しない可能性がある
- 国際標準化や規格化（入り・選定中）を理由に、電子政府での利用実態がないにもかかわらず推奨リストに残り続けることがないか

＜提案暗号（国産暗号）の利用促進＞

- 純粋な自由競争であり、利用実績に応じて降格の可能性があるため、応募会社の利用促進活動に対するモチベーションを向上させる可能性がある
- 他社実績をつませないため、少なくとも自社の提案暗号が推奨候補暗号リストに降格しない限り、他社暗号アルゴリズムを利用しないモチベーションとなる。応募会社による囲い込み意識が働く
- 全世界特許無償は様々な国際標準化・規格化への採用活動をしていない応募会社の

ビジネスモデルと壊す恐れが高い

- 全世界特許無償化しても、様々な国際標準化・規格化に採用されていない提案暗号は（応募会社以外にとって）事実上サポートする対象になりえない
- 推奨候補暗号リストへの降格の恐れがある提案暗号の場合、応募会社以外の企業・団体がサポートする対象にはなりにくい
- 電子政府推奨暗号アルゴリズムの個数が多くなるほど、一つあたりの利用促進のためにかけられるコストが小さくなるため、効果的な支援は困難

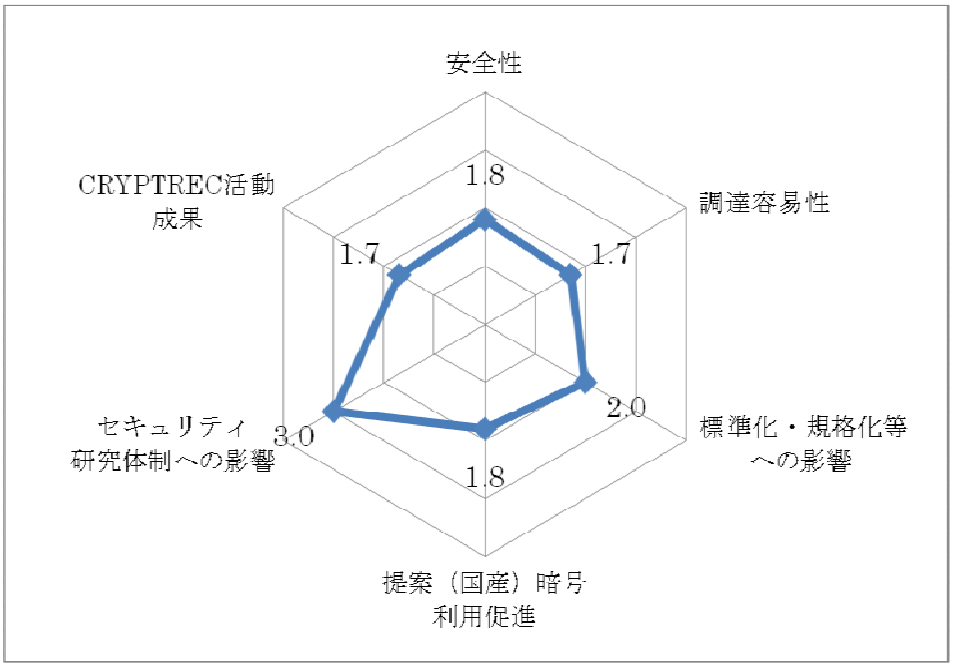
＜セキュリティ研究体制への影響＞

- 電子政府推奨暗号リストが新しい暗号アルゴリズムを開発した場合の一つの到達点としてのモチベーションにつながり、新しい暗号アルゴリズムの開発が継続できる可能性が高まる
- 安全性評価対象が多いため新しい安全性評価技術や検証の豊富な研究素材となり、暗号研究の強化につながる
- 普及度（だけ）が技術評価の指標としてクローズアップされる可能性があり、推奨候補暗号リストへ降格した提案暗号の応募会社では研究体制維持を難しくする可能性がある
- 応募会社内だけで自社開発暗号アルゴリズムを利用することが事実上の前提であるならば、経営判断の影響を受けやすい構造にある

＜CRYPTREC 活動成果＞

- 推奨候補暗号リストへの降格においてはその判断・運用を行う組織が必要であり、推奨候補暗号リストへの降格を行った後の電子政府推奨暗号リストを活かせるのであれば CRYPTREC 活動の必要性を主張できる
- 利用実績による降格は明確な基準が困難であり、電子政府推奨暗号リストと推奨候補暗号リストとの差異、位置づけは不明確
- 単に市場での普及に任せていても、現在の米国暗号有利の状況が変わるわけではなく、分割の意味ある効果は期待できない
- 危殆化以外の理由（利用実績等）による降格は暗号開発ベンダ、および市場に受け入れられない可能性がある
- 推奨候補暗号リストへの「降格の基準」に応じて、シナリオ 3 は、シナリオ 1, 2, 4 のいずれにもなりうる。シナリオ 3 を選択する場合には、推奨候補暗号リストへの降格後に電子政府推奨暗号リストがどうなるかをイメージできる程度に基準について議論しておくことが望ましい

【シナリオ 4（政府調達の選択肢としての提示。現状とほぼ同様）】



＜安全性＞

- 電子政府推奨暗号リストに代替暗号アルゴリズムが選択肢として用意されている
- 暗号アルゴリズムごとの安全性評価の度合に差が生じ、統一的な運用基準が適用できない。また暗号アルゴリズムごとに評価を行う暗号研究者が固定化されやすく、全体の安全性評価の充実度につながらない
- 電子政府推奨暗号アルゴリズムの個数が多いため、特定の暗号アルゴリズムに特化した安全性評価や監視活動を定常的に実施することは困難であり、全体的な評価効率も悪く監視コストがかさむ
- 電子政府推奨暗号アルゴリズムの数は多いが、実際に利用される暗号は限定されるため、結果として実装・保守における安全性はシナリオ 1，2 と同程度になると考えられる
- 電子政府推奨暗号アルゴリズムの数で考えればシナリオ 1，2 よりもいずれかの電子政府推奨暗号アルゴリズムが危殆化する可能性は高い。広く利用されていない電子政府推奨暗号アルゴリズムが危殆化した場合、経済的な影響は限定的となる可能性があるが、「CRYPTREC がお墨付きを与えていた暗号（電子政府推奨暗号）が危殆化した」という点で CRYPTREC の信用が低下する可能性がある

＜調達容易性＞

- 意図してバックアップのアルゴリズムを用意する場合、選択肢が豊富
- 製品調達が極めて容易なものからそうでないものまで同格に扱われ、実際の暗号アルゴリズム選択との相関性は薄い
- 応募会社以外の暗号アルゴリズムの利用はすでにシェアを握った一部に限られ、利用度が低い電子政府推奨暗号アルゴリズムが様々な企業で製品化される可能性は低

く、調達先は限定され調達コストは高くなる
- 特定製品にしか搭載されていない電子政府推奨暗号アルゴリズムが採用されると将来にわたってベンダロックインが発生する恐れがある

＜標準化・規格化等への影響＞
- 電子政府推奨暗号アルゴリズムに選ばれた応募会社にとっては国際標準化への支援材料になると期待できるため、これらの国際標準化活動へのモチベーションはある
- 公的なお墨付きとして安全性評価の裏付けや電子政府への採用実績を紹介できる
- 多数の暗号アルゴリズムの標準化提案は本来の標準化の意義に沿わない。日本としてどの暗号アルゴリズムを必要としているのかはっきりしないため、日本からの国際標準化・規格化への提案は拒絶または無視、軽視される可能性が高い
- 応募会社は自らが興味を持つ標準化・規格化しか推進しない可能性がある

＜提案暗号（国産暗号）の利用促進＞
- 純粋な自由競争であり、応募会社が自社のビジネス範囲内に囲い込んで利用することに対してはモチベーションがあると考えられる
- 自社の提案暗号が電子政府推奨暗号アルゴリズムとなっている状況で、他社の提案暗号をサポートするという状況は想定し難い
- 全世界特許無償化しても、様々な国際標準化・規格化に採用されていない提案暗号は（応募会社以外にとって）事実上サポートする対象になりえない
- 全世界特許無償は様々な国際標準化・規格化への採用活動をしていない応募会社のビジネスモデルと壊す恐れが高い
- 電子政府推奨暗号アルゴリズムの個数が多いため、一つあたりの利用促進のためにかけられるコストが小さく、平等公平に効果的な支援は困難

＜セキュリティ研究体制への影響＞
- 電子政府推奨暗号リストが新しい暗号アルゴリズムを開発した場合の一つの到達点としてのモチベーションにつながり、新しい暗号アルゴリズムの開発が継続できる可能性が高まる
- 安全性評価対象が多いため新しい安全性評価技術や検証の豊富な研究素材となり、暗号研究の強化につながる
- 応募会社内だけで自社開発暗号アルゴリズムを利用することが事実上前提であるため、経営判断の影響を受けやすい構造にある
- 欧米とは違い、暗号アルゴリズム主体の研究体制からセキュリティ応用研究主体の研究や特定用途向けセキュリティ研究主体の研究体制へのリソースシフトを妨げる恐れがある

＜CRYPTREC 活動成果＞

- 電子政府推奨暗号リストと推奨候補暗号リストとの差異、位置づけの違いは極めて不明確
- 推奨候補暗号リストに含まれる暗号アルゴリズムはほとんどないと考えられ、別リストである利点がない
- 電子政府推奨暗号アルゴリズムとなっていても調達が難しい暗号が存在する可能性があり、その場合、電子政府推奨暗号リストの価値が低下し、CRYPTREC の成果も分かりにくくなる

７．２．５．外部アンケート調査

現在の電子政府推奨暗号リストは技術的観点のみから作成されたものである。しかし、実際の電子政府情報システムの構築及び調達可能製品の製造の現場においては、必ずしも技術的観点だけで暗号アルゴリズムの選択が行われているわけではない。

そこで、現在の「電子政府推奨暗号リスト」の課題点を抽出し、「CRYPTREC 暗号リスト（仮称）」をどのような考え方のもとで作成することがよいのかについての情報を得ることを目的として実施したものである。アンケートの主たる調査項目は以下のとおり。

- 暗号搭載製品の開発や製造、情報システムの構築等における暗号利用（とりわけ暗号選択のプロセス）に関する実態を把握すること
- 現在の「電子政府推奨暗号リスト」の活用実態を把握すること
- 「CRYPTREC 暗号リスト（仮称）」や CRYPTREC に期待すること
- 暗号搭載製品の開発や製造、情報システムの構築等における提案暗号（国産暗号）に対する認識を広く把握すること

本調査では、運用委員会が選定した以下の 17 カテゴリの各々シェアトップ級ベンダとシステムインテグレータ、並びに政府機関を調査対象先として選定した。その中には応募企業関連の事業部門（応募ベンダと呼ぶ）も含む。また、応募企業の暗号開発部門（応募者）に対しては開発部門としての現状認識を質問した。

＜カテゴリ＞

- 官公庁向けシステムインテグレータ
- オペレーションシステム
- ブラウザ
- アプリケーションソフトウェア（ブラウザを除く）
- 暗号ライブラリ（暗号アルゴリズムを集めたソフトウェア）
- ルータ
- セキュリティアプライアンス製品
- サーバ／ストレージ
- HSM／PKI システム／認証局システム

- IC カード
- 半導体チップ
- デジタル複合機
- 輸入販売代理による輸入製品
- 固定網／NGN 通信事業者
- 携帯電話通信事業者
- サービスプロバイダ
- タイムスタンプビジネス

最終的に、ベンダ全 39 社（67 プロダクト）、システムインテグレータ全 8 社（11 システム）、政府機関全 4 府省（6 システム）から回答を得ることができた。協力いただいた企業は以下のとおりである（順不同、公表不可を除く）。

● ベンダ

凸版印刷株式会社
オーセンテック株式会社
キヤノン株式会社
KDDI 株式会社
大日本印刷株式会社
三菱電機インフォメーションシステムズ株式会社
日本電気株式会社
株式会社 PFU
ルネサスエレクトロニクス株式会社
EMC ジャパン株式会社
一般社団法人 Mozilla Japan
インフィニオンテクノロジーズジャパン株式会社
株式会社リコー
株式会社東芝
富士ゼロックス株式会社
富士通株式会社
ソニー株式会社
アマノビジネスソリューションズ株式会社
株式会社 ACCESS
ヤマハ株式会社
マイクロソフト株式会社
セコムトラストシステムズ株式会社
日本ベリサイン株式会社
株式会社バッファロー
タレスジャパン株式会社
シスコシステムズ合同会社
インテル株式会社
他、全 39 社・67 プロダクト

● システムインテグレータ

三菱電機株式会社
東芝ソリューション株式会社
新日鉄ソリューションズ株式会社
三菱電機インフォメーションシステムズ株式会社
株式会社日立製作所
他、全 8 社・11 システム

本調査結果から明らかとなった点は以下のとおりである。詳細については CRYPTREC Report 2010 を参照されたい。なお、これらの結果は「電子政府推奨暗号リストの考え方」に対するシナリオでの特徴的なメリット・デメリットの抽出や評価点を検討するうえでの基礎情報として取り扱った。

「ベンダ」からみる全体的な傾向

- （米国政府標準暗号以外の）暗号をサポートするかどうかは「お客様がいるか」「市場としての広がりがあるか」「様々な標準になっていて国際的知名度があるか」「特許無償で利用可能であるか」が大きなポイント
- 暗号アルゴリズム実装では「30%超のベンダ」が他社製品や OSS を利用
- 50%以上のベンダはサポートする暗号アルゴリズムの数が「必要最少限」もしくは「少ないほどよい」と考えている
- 80%以上のベンダが（CRYPTREC 以外の）標準規格等を製品開発の中で利用。相互接続性の観点から ISO/IEC だけでなく、ITU, IETF, IEEE なども多く参照
- 現在の国産暗号の製品化率は約 20～30%。今後国産暗号をサポートするかどうかは条件次第が約 40～50%で一番多い
- （日本以外の）各国政府等からの要求に対応して当該国の政府標準暗号を別途追加したケースが 10～20%はある
- 50%以上は 3 部構成の次期リストに対して好意的。特に「監視リスト」の受けが良い

「応募ベンダ」と「非応募ベンダ」との認識 の違い

- 「応募ベンダ」と「非応募ベンダ」とでは、一部の設問や回答に違いがみられるものの、全体的な傾向としては両者に大きな差があるわけではない
- 「応募ベンダ」と「非応募ベンダ」とで回答に違いがあったものの一つに国産暗号の採用理由がある。非応募ベンダでは「お客様要望」「様々な標準に採用され国際的知名度が高い」「特許無償で利用可」などが採用理由として多いのに対し、応募ベンダでは「他社との差異化提案」「自社開発暗号である」「処理性能が良い」などが多い

「ベンダ（システムインテグレータ）」と「政府機関」との認識の違い

- 推奨暗号の数を絞るか絞るべきではないかに対する考えが大きく異なる。
  ベンダの多数意見は「使う暗号は決まっている」「絞るほどむしろ安全性が高まる」「コストが抑えられる」「相互接続に問題ない」など“数を絞る”べきとするのに対し、政府機関の多数意見は「選択自由度が高まる」「絞ると影響が大きい」「絞るほど攻撃されやすい」など“数を絞らない”とする

「応募者」の主な現状認識

- 80%以上が「自社事業部や子会社での利用を約束」したうえでの開発目的に掲げる一方、現在の自社事業部や子会社での利用進捗率は 40～50%程度。ちなみに応募ベンダからの回答では国産暗号製品化実績率は約 30%
- 70%以上が「社会基盤としての利用」「米国政府標準暗号だけに頼るべきでない」と開発目的に掲げる一方、社会基盤のために必要な標準化を実際に進めているは

半数にとどまる。しかもその対象は提案中を含めても ISO/IEC だけが約 40%、そのほかの IETF などメジャーな標準化・規格化は 10%にも届かない

- 標準化を進める目的が「お墨付きを得るため」であり、「相互接続確保のため」は半数にとどまる

７．２．６．運用監視暗号リストに登録された暗号技術に関する検討

本年度は、第 1 回暗号技術検討会からの審議結果に基づき、急激な安全性低下に伴う暗号運用委員会としての対応方針について審議を行った。

当初予定していた運用監視暗号リスト等に掲載される暗号技術の取り扱い方法については、電子政府推奨暗号リストを含む CRYPTREC 暗号リスト（仮称）全体の方向性の議論と密接に関連することから、次年度以降、CRYPTREC 暗号リスト（仮称）全体の方向性が固まってから検討を開始することとした。

７．３．今後の予定

政府部内等での議論を踏まえ決定された電子政府推奨暗号リストの考え方に基づき、暗号運用委員会としては、その電子政府推奨暗号リストの考え方を具体的に反映するための製品化、利用実績、国際標準化等の評価手法について、2010 年度の議論を踏まえて検討を行う。

また、情報システムの移行における課題を整理しつつ、運用監視暗号リストに登録される暗号技術の取り扱い等について調査・検討を行う。

８．今後の CRYPTREC 活動について

CRYPTREC は、電子政府の安全性及び信頼性を確保し国民が安心して電子政府を利用できる環境を整備するため、「国民を守る情報セキュリティ戦略」等を踏まえつつ、2011 年度以降以下の活動を継続していく。

（１）電子政府推奨暗号リストの改訂に向けた取り組み

① 暗号技術の安全性評価

2013年の電子政府推奨暗号リストの改訂に向けて、応募暗号技術、現行の電子政府推奨暗号に対する安全性の評価を行う。

② 暗号技術の実装性評価

今年度検討したハードウェア及びソフトウェア実装性評価の評価項目、評価手法、評価基準を用いて、安全性評価を完了した応募暗号技術及び現行の電子政府推奨暗号に対する評価を実施する。また、サイドチャネル攻撃耐性に関する確認を実施する。

③ CRYPTREC暗号リスト(仮称)の各リストにおける取り扱い方法の検討

電子政府推奨暗号リストの考え方を具体的に反映するための製品化、利用実績、国際標準化等の評価手法・判断基準、及び運用監視暗号リストに登録される暗号技術の取り扱い方法等について調査・検討を行う。

（２）電子政府推奨暗号の監視活動

電子政府推奨暗号に選定された各暗号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。

（３）暗号技術の危殆化対策に関する調査・検討

情報システムの移行における課題を整理しつつ、暗号技術の危殆化対策について調査・検討を行う。

（４）暗号実装技術等に関する調査・検討

暗号実装技術及び暗号モジュールへのサイドチャネル攻撃等に関する攻撃技術の動向等の調査を行う。

（５）暗号技術に関する国際的な標準規格化活動への貢献

暗号モジュールのセキュリティ要件及び試験要件等に関する国際的な標準規格化活動に対して貢献する。

別添１

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
		SHA-512
	擬似乱数生成系(注 7)	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。

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

別添２

CRYPTREC 構成員・オブザーバ名簿

１．暗号技術検討会

暗号技術検討会の構成員、オブザーバは、以下の通り。（敬称略）

座 長	今井　秀樹	中央大学理工学部電気電子情報通信工学科教授
顧 問	辻井　重男	中央大学研究開発機構教授
	太田　和夫	電気通信大学電気通信学部情報通信工学科教授
	岡本　栄司	筑波大学大学院システム情報工学研究科教授
	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（社団法人電気通信事業者協会代表兼務）
	加藤　義文	社団法人テレコムサービス協会技術・サービス委員会委員長
	金子　敏信	東京理科大学理工学部電気電子情報工学科教授
	国分　明男	財団法人ニューメディア開発協会顧問・首席研究員
	櫻井　幸一	九州大学大学院システム情報科学研究院情報工学部門教授
	佐々木　良一	東京電機大学未来科学部情報メディア学科教授
	寶木　和夫	社団法人電子情報技術産業協会情報セキュリティ委員会委員
	武市　博明	一般社団法人情報通信ネットワーク産業協会常務理事
	苗村　憲司	情報セキュリティ大学院大学教授
	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長
	松本　勉	横浜国立大学大学院環境情報研究院教授
	松本　泰	セコム株式会社ＩＳ研究所基礎技術ディビジョン主席研究員
	米山　正夫	日本銀行金融研究所情報技術研究センター企画役

（オブザーバ）

木本　裕司	内閣官房情報セキュリティセンター内閣参事官
髙橋　浩二	警察庁情報通信局情報管理課長
澤田　稔一	総務省行政管理局行政情報システム企画課情報システム企画官
山崎　重孝	自治行政局住民制度課長
高地　圭輔	総務省自治行政局地域政策課地域情報政策室長
江原　健志	法務省民事局商事課長
中前　隆博	外務省大臣官房情報通信課長
寺岡　光博	財務省大臣官房文書課情報管理室長
田中　正幸	文部科学省大臣官房政策課情報化推進室長
松原　徳和	厚生労働省大臣官房統計情報部企画課情報企画室長
山本　雅亮	経済産業省産業技術環境局基準認証ユニット 情報電子標準化推進室長
坂下　圭一	防衛省運用企画局情報通信・研究課情報保証室長

高橋　幸雄	独立行政法人情報通信研究機構 情報通信セキュリティ研究センター長
渡辺　創	独立行政法人産業技術総合研究所情報セキュリティ研究センター 副研究センター長
矢島　秀浩	独立行政法人情報処理推進機構セキュリティセンター長
亀田　繁	財団法人日本情報処理開発協会電子署名・認証センター長
鈴田　信	財団法人金融情報システムセンター監査安全部長

２．暗号方式委員会

暗号方式委員会の委員、オブザーバは、以下の通り。（敬称略、五十音順）

委員長	今井　秀樹	中央大学　理工学部　電気電子通信工学科　教授
顧問	辻井　重男	中央大学　研究開発機構　教授
委員	太田　和夫	国立大学法人電気通信大学大学院　情報理工学研究科　教授
	金子　敏信	東京理科大学 理工学部電気電子情報工学科　教授
	佐々木　良一	東京電機大学 未来科学部情報メディア学科　教授
	高木　剛	国立大学法人九州大学大学院　数理学研究院　教授
	田中　秀磨	独立行政法人情報通信研究機構 情報通信セキュリティ研究センター セキュリティ基盤グループ グループリーダー
	松本　勉	国立大学法人横浜国立大学　大学院　環境情報研究院　教授
	山村　明弘	国立大学法人秋田大学大学院　工学資源学研究科　教授
	渡辺　創	独立行政法人産業技術総合研究所　情報セキュリティ研究センター 副研究センター長

（オブザーバ）

中嶋　良彰	内閣官房　情報セキュリティセンター　内閣参事官補佐
山口　利恵	内閣官房　情報セキュリティセンター　主査
根本　農史	内閣官房　情報セキュリティセンター　主査
末澤　洋	警察庁　情報通信局　情報管理課　課長補佐（2010 年 7 月まで）
初川　泰介	警察庁　情報通信局　情報管理課　課長補佐（2010 年 7 月から）
松本　和人	総務省　行政管理局　行政情報システム企画課　課長補佐（2010 年 7 月まで）
松宮　志麻	総務省　行政管理局　行政情報システム企画課　課長補佐（2010 年 7 月から）
浦舟　利幸	総務省　自治行政局　地域情報政策室　課長補佐
山﨑　敏明	総務省　自治行政局　住民制度課　理事官
大西　公一郎	総務省　自治行政局　住民制度課　課長補佐（2011 年 2 月まで）
浦上　哲朗	総務省　自治行政局　住民制度課　課長補佐(2011 年 2 月から)
佐久間　明彦	外務省　大臣官房　情報通信課　外務技官
山中　豊	経済産業省　産業技術環境局　情報電子標準化推進室　課長補佐
坂下　圭一	防衛省　運用企画局　情報通信・研究課　情報保証室長
石川　正興	防衛省　技術研究部　電子装備研究所　ネットワーク技術研究部 情報セキュリティ研究室長
滝澤　修	独立行政法人情報通信研究機構情報通信セキュリティ研究センター 防災・減災基盤技術グループ　グループリーダ

花岡　悟一郎　　独立行政法人産業技術総合研究所　情報セキュリティ研究センター
主任研究員

３．暗号実装委員会

暗号実装委員会の委員、オブザーバは、以下の通り。（敬称略、五十音順）

委員長	松本　勉	国立大学法人横浜国立大学大学院環境情報研究院　教授
委員	植村　泰佳	電子商取引安全技術研究組合　専務理事
	大須賀　勝美	ＮＴＴエレクトロニクス株式会社 セイフティ・ネットワーク事業部開発部　主事
	亀田　繁	財団法人日本情報処理開発協会電子署名・認証センター センター長
	佐藤　恒夫	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 開発第一チーム　チームリーダ
	佐藤　証	独立行政法人産業技術総合研究所情報セキュリティ研究センター ハードウェアセキュリティ研究チーム　研究チーム長
	﨑山　一男	国立大学法人電気通信大学大学院情報理工学研究科総合情報学専攻 准教授
	清水　秀夫	株式会社東芝研究開発センター コンピュータアーキテクチャ・セキュリティ ラボラトリー 主任研究員
	高橋　芳夫	株式会社ＮＴＴデータ技術開発本部ＳＩアーキテクチャ開発センタ シニアエキスパート
	角尾　幸保	日本電気株式会社情報・メディアプロセッシング研究所 暗号・符号テクノロジーグループ　主席研究員
	鳥居　直哉	株式会社富士通研究所ソフトウェア＆ソリューション研究所 セキュアコンピューティング研究部　部長
	福永　利徳	日本電信電話株式会社ＮＴＴ情報流通プラットフォーム研究所 情報セキュリティプロジェクト　主任研究員
	本間　尚文	国立大学法人東北大学大学院情報科学研究科情報基礎科学専攻 准教授
	松崎　なつめ	パナソニック株式会社デジタル･ネットワーク開発センター ネットワーク技術開発グループネットワーク第四チーム チームリーダ
	渡辺　大	株式会社日立製作所システム開発研究所第七部　研究員

（オブザーバ）

根本　農史	内閣官房　情報セキュリティセンター　主査
赤澤　康之	警察庁　情報通信局　情報管理課　係長
岡野　孝子	警察大学校　警察情報通信研究センター　基礎研究室　助教授

松宮　志麻	総務省　行政管理局　行政情報システム企画課　課長補佐
荒木　美敬	外務省　大臣官房　情報通信課
山中　豊	経済産業省　産業技術環境局　情報電子標準化推進室　課長補佐
千葉　修治	防衛省　陸上幕僚監部　情報通信・研究課　情報通信室　２等陸佐
石川　正興	防衛省　技術研究部　電子装備研究所　ネットワーク技術研究部 情報セキュリティ研究室長
坂下　圭一	防衛省　運用企画局　情報通信・研究課　情報保証室長
滝澤　修	独立行政法人情報通信研究機構情報通信セキュリティ研究センター セキュリティ基盤グループ/防災・減災基盤技術グループ グループリーダー
青木　林	財団法人日本規格協会　情報技術標準化研究センター　事務局
川村　信一	独立行政法人産業技術総合研究所　情報セキュリティ研究センター 副研究センター長

４．暗号運用委員会

暗号運用委員会の委員、オブザーバは、以下の通り。（敬称略、五十音順）

委員長	佐々木　良一	東京電機大学 未来科学部情報メディア学科 教授
委員	大岩　寛	独立行政法人産業技術総合研究所　情報セキュリティ研究センター ソフトウェアセキュリティ研究チーム 研究員
	菊池　浩明	東海大学 情報通信学部通信ネットワーク工学科 教授
	小松　文子	独立行政法人情報処理推進機構 セキュリティセンター 情報セキュリティ分析ラボラトリー ラボラトリー長
	鈴木　雅貴	日本銀行 金融研究所情報技術研究センター
	手塚　悟	東京工科大学 コンピュータサイエンス学部 教授
	松尾　真一郎	独立行政法人情報通信研究機構情報通信セキュリティ研究センター セキュリティ基盤グループ　主任研究員
	北村　伸弘	日本電気株式会社 第一システムソフトウェア事業部　マネージャー
	佐野　文彦	東芝ソリューション株式会社　IT 技術研究所　研究開発部 情報セキュリティラボラトリー 研究主務
	下江　達二	富士通株式会社 ソフトウェアＢＧミドルウェア事業本部 システム・マネジメント・ミドルウェア事業部　第三開発部 部長
	羽根　慎吾	株式会社日立製作所 システム開発研究所 第七部 702 研究ユニット 主任研究員
	前田　司	EMC ジャパン株式会社　RSA 事業本部 テクニカルサポート技術部　部長
	宮崎　一哉	三菱電機株式会社　情報技術総合研究所 情報システム構築技術部　チームリーダ

（オブザーバ）

中嶋　良彰	内閣官房　情報セキュリティセンター　内閣参事官補佐
山口　利恵	内閣官房　情報セキュリティセンター　主査
根本　農史	内閣官房　情報セキュリティセンター　主査
松宮　志麻	総務省　行政管理局　行政情報システム企画課　課長補佐
山中　豊	経済産業省　産業技術環境局　情報電子標準化推進室　課長補佐
日高　隆	経済産業省　大臣官房　情報システム厚生課 セキュリティ担当課長補佐
石川　正興	防衛省　技術研究部　電子装備研究所　ネットワーク技術研究部 情報セキュリティ研究室長