暗号技術検討会

２０１１年度報告書

２０１２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、2011 年 8 月に、政府の情報システムにも広く使用されている技術であり、電子政府推奨暗号リストにも掲載している Advanced Encryption Standard(AES)に対する新たな攻撃手法が国際会議にて報告されるなど、解読に新たな展開が見られた。このことは、ただちに現実的な脅威につながることはないものの、暗号技術の危殆化は予測が難しいものであるため、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、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、実装性や利用実績の評価方法の検討を実施するなど、リスト改訂に向けて着実に作業を進めた。また、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。今年度は、来年度の電子政府推奨暗号リスト改訂に向け、継続して暗号技術の安全性評価を行うと共に、実装性能評価を実施し、また、利用実績の評価等の選定基準の検討を行った。

委員会別の活動状況を見てみると、暗号方式委員会では、応募された応募暗号技術について、安全性に関する２次評価及び現リストに掲載された暗号技術の再評価を実施した。また、暗号技術の監視・調査等の活動、リストガイドの作成、計算機能力進化の予測の更新等を行った。暗号実装委員会では、応募暗号技術について、ハードウェア及びソフトウェア実装性評価を実施及びサイドチャネルのセキュリティ対策の検討等を行った。暗号運用委員会では、昨年度整理した次期電子政府推奨暗号リストのシナリオに従い、電子政府推奨暗号の選定基準の検討を行った。

2011 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 2011」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。

2012 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管理基準（2011 年 4 月 21 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。

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、現在 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 年度より、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、検討等を行っている。(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。

（座長：今井秀樹中央大学教授）

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。

（委員長：今井秀樹中央大学教授）

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。

（委員長：本間尚文東北大学准教授）

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、電子政府推奨暗号の選定スキームの検討、取りまとめ及び、電子政府推奨暗号の利用促進体制の検討を行った。

暗号運用委員会は NICT 及び IPA の委員会として開催した。

（委員長：松本勉横浜国立大学教授）

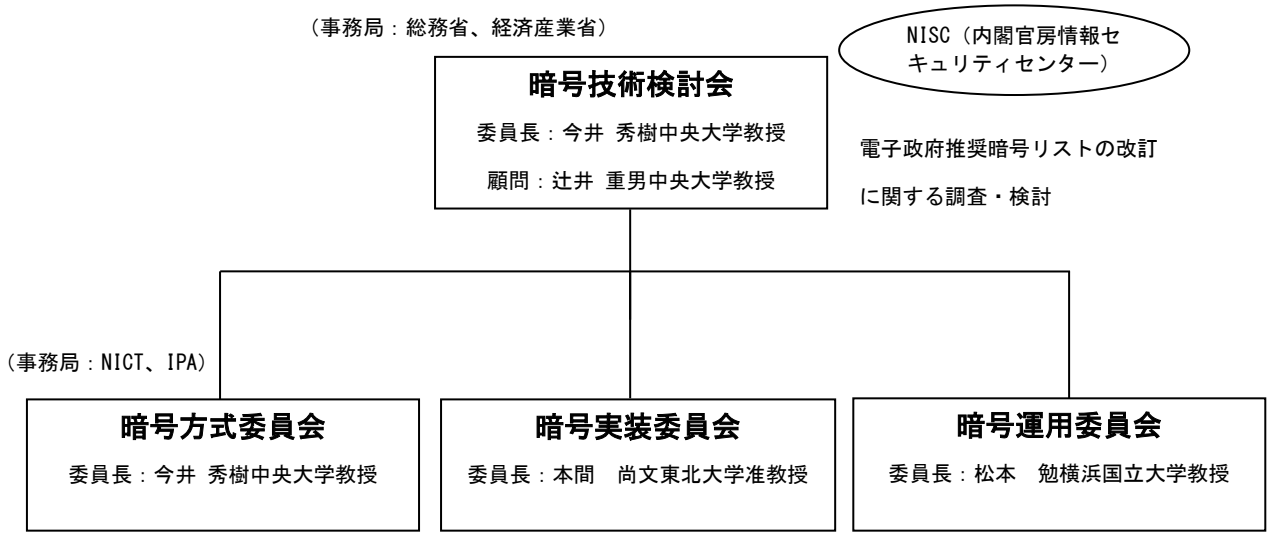


図 2.1　2011 年度 CRYPTREC の体制図

２．３．暗号技術検討会開催状況

2011 年度、検討会は計 2 回開催された。各回会合の開催日及び主な議題は以下のとおり。

【第 1 回】2011 年 6 月 30 日（木）

（主な議題）　・次期電子政府推奨暗号リストの考え方について
・2010 年度の活動報告及び 2011 年度活動計画（案）について

【第 2 回】2012 年 3 月 8 日（木）

（主な議題）　・次期電子政府推奨暗号リストの選定スキーム（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について
・2011 年度の活動報告及び 2012 年度活動計画（案）について

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、次期リスト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、または、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、また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 ビットまたは 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（安全性または実装性）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　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とおり。

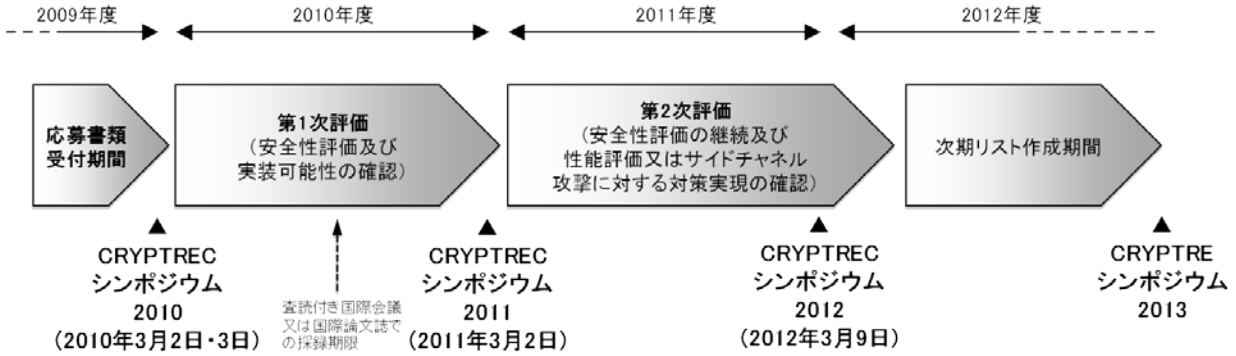


図 3.4 評価スケジュール

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～
CRYPTREC シンポジウム 2012：　2012 年 3 月 9 日
CRYPTREC シンポジウム 2013：　2013 年 3 月頃

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う。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、使用セル数またはゲート数等）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、暗号実装委員会において詳細を検討し、その結果を応募者にアナウンスした。

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

３．７．第１次評価の進捗状況

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とおりである。

３．７．１．応募暗号技術の評価状況

表 3.5　応募暗号技術の第 1 次評価結果(2010 年度実施)

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また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(2010 年度実施)

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、次期リストに掲載する。ただし、脆弱性
	電子署名利用に	ISO/IEC 9798-3、デジ	

	よる認証プロトコル	タル署名技術を使用する機構	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．第 2 次評価及び現リストに記載された暗号技術の再評価の進捗状況

2011 年度における応募暗号技術に関する第 2 次評価及び現在、電子政府推奨暗号リストに掲載された暗号技術の安全性に関する再評価の進捗状況は以下のとおりである。

３．８．１．安全性評価状況

(1) 128 ビットブロック暗号の鍵拡大関数の安全性

関連鍵攻撃 [3]に対する安全性評価を目的として鍵拡大関数の差分特性確率 [4]の上界を評価した。差分特性確率は、秘密鍵を操作したときに拡大鍵を制御できる確率の上界を示しており、関連鍵攻撃についての安全性の指標になると考えられる。本評価において排他的論理和、定数加乗算に関しては全て攻撃者に都合の良い差分伝播が確率 1 で生じるとし、攻撃者有利に評価をしている。

表 3.7　鍵拡大関数の差分特性確率の上界

鍵長 / アルゴリズム	差分特性確率の上界		
	128 ビット	192 ビット	256 ビット
AES	2^{-24}	2^{-6}	2^{-6}
Camellia	2^{-30}	2^{-18}	2^{-18}
CIPHERUNICORN-A	2^{-259}	2^{-175}	2^{-133}
Hierocrypt-3	2^{-36}	2^{-36}	2^{-36}
SC2000	2^{-48}	2^{-24}	2^{-24}

この結果から、AES と比較した場合、Camellia、CIPHERUNICORN-A、Hierocrypt-3 及び SC2000 は関連鍵攻撃に対して、より耐性があると見積もられる。関連鍵攻撃は、192/256 ビット鍵の AES に対して解読可能であることが示されているが、特殊な攻撃条件のため現実的な脅威には至っていないと考えられる。関連鍵攻撃に対して安全であることの必要性については今後検討が必要である。

等価鍵存在 [5]に関しては、AES、Camellia、CIPHERUNICORN-A及びHierocrypt-3 については鍵拡大関数が全単射であることから等価鍵が存在しない。SC2000 については、拡大鍵計算の途中で生成される中間鍵には衝突がないことが確認されているが、拡大鍵については未確認である。

---

[3] 関連鍵攻撃とは、攻撃者が秘密鍵を操作できるという仮定の下での攻撃である。

[4] 鍵拡大関数にはデータ撹拌部における拡大鍵挿入に相当するものがないため、単に active s-box について最大差分確率の積を取ることにより上界を算出している。

[5] 等価鍵とは、任意の平文の暗号化において同じ暗号文を出力する秘密鍵の組をいう。

(2) 128 ビットブロック暗号の 192/256 ビット鍵の場合の安全性評価

192/256 ビット鍵の場合の計算量的安全性を関連鍵攻撃まで想定して概算で見積もるため、差分/線形特性確率の上界を評価した。本評価においてはデータ撹拌部のみを考え、データ撹拌部全ラウンドの丸め差分／線形パスを探索することによりその特性確率の上界を評価している。ただし、排他的論理和やビットシフトなどの線形演算に関しては確率 1 で、算術加乗算や s-box などの非線形演算に関しては最大差分確率で、それぞれ攻撃者に都合の良い差分伝播が生じるとし、攻撃者有利の評価を行った。

(a) 差分攻撃

表 3.8　データ撹拌部の差分特性確率の上界

アルゴリズム＼鍵長	差分特性確率の上界		
	128 ビット	192 ビット	256 ビット
AES	2^{-336}	2^{-456}	2^{-486}
Camellia	2^{-216}	2^{-288}	192 ビット鍵と同じ
CIPHERUNICORN-A	2^{-190}[1][6]	128 ビット鍵と同じ	128 ビット鍵と同じ
Hierocrypt-3	2^{-450}	2^{-480}	2^{-600}
SC2000	(2^{-187}[2] [7])	(2^{-215}[2])	192 ビット鍵と同じ

表 3.9　攻撃計算量が鍵全数探索を上回るラウンド数／暗号化ラウンド数

アルゴリズム＼鍵長	攻撃計算量が鍵全数探索を上回るラウンド数／暗号化ラウンド数		
	128 ビット	192 ビット	256 ビット
AES	4/10	7/12	8/14
Camellia	12/18	17/24	22/24
CIPHERUNICORN-A	12/16[1]	-	-
Hierocrypt-3	2/6	4/7	4/8
SC2000	(13/19[2])	(21/22[2])	-

-は 1 を超えた場合である。

ア　AES、Camellia 及び Hierocrypt-3

全てのアルゴリズムについて修正を行うことなしに評価を行った。Camellia のデータ撹拌部は 192 及び 256 ビット鍵において同じ構造であるため差分特性確率は等しい値となる。

---

[6] [1]　角尾幸保、久保博靖、茂真紀、洲崎智保、宮内宏, “CIPHERUNICORN-Aの差分解読／線形解読に対する安全性について（II）”、SCIS 2003, 5D-1, 2003.

[7] [2]　H.Yanami, T.Shimoyama, and O.Dunkelman, Differential and Linear Cryptanalysis of a Reduced-Round SC2000, FSE 2002, LNCS 2365: 34-48

イ　CIPHERUNICORN-A

データ撹拌部はすべての鍵長において同じ構造であるため、差分特性確率は鍵長に依らず一定である。ラウンド関数の構造が複雑であり拡大鍵入力の独立性を考慮した差分特性確率の見積もりが難しいことから、参考文献[1]の結果を事務局の評価とした。この結果から示される差分特性確率の上界は、全鍵長において、2^{-190} である。

ウ　SC2000

丸め差分評価では 2^{128} 以上の計算量的安全性を確認できなかったため、参考文献[2]の結果を全ラウンドに適用した。表中の()内の値は、[2]の繰り返しパスを全ラウンドにそのまま適用した値である。128 ビット鍵では 2^{-187}、192/256 ビット鍵では 2^{-215} の差分パスが存在する。

(b) 線形攻撃

表 3.10　データ撹拌部の線形特性確率の上界

アルゴリズム＼鍵長	線形特性確率の上界		
	128 ビット	192 ビット	256 ビット
AES	2^{-330}	2^{-450}	2^{-480}
Camellia	2^{-204}	2^{-276}	192 ビット鍵と同じ
CIPHERUNICORN-A	2^{-171}	128 ビット鍵と同じ	128 ビット鍵と同じ
Hierocrypt-3	2^{-450}	2^{-480}	2^{-600}
SC2000	($2^{-162.98}$[2])	($2^{-201.81}$[2])	192 ビット鍵と同じ

表 3.11　攻撃計算量が鍵全数探索を上回るラウンド数／暗号化ラウンド数

アルゴリズム＼鍵長	攻撃計算量が鍵全数探索を上回るラウンド数／暗号化ラウンド数		
	128 ビット	192 ビット	256 ビット
AES	4/10*	7/12	8/14
Camellia	12/18*	17/24*	23/24*
CIPHERUNICORN-A	12/16	-	-
Hierocrypt-3	2/6	4/7	4/8
SC2000	(16/19[2])	(22/22[2])	-

-は１を超えた場合である。

ア　AES、Camellia 及び Hierocrypt-3

Camellia の評価は、FL 関数無しで行った。AES、Hierocrypt-3 に対しては、アルゴリズムを修正することなしに評価を行った。

イ　CIPHERUNICORN-A

データ撹拌部はすべての鍵長において同じ構造であるため、線形特性確率は鍵長に依らず一定である。ラウンド関数の構造が複雑であり、簡易な構造に変形したmF

関数を用いて評価した。参考文献[1][3]と異なり、定数乗算及び、A3 関数に関し、bit単位の接続可能性に極力配慮した再評価を行った。しかし、拡大鍵入力の独立性を考慮した評価結果は[1][3][8]と、同じである。この結果から示される線形特性確率の上界は、全鍵長において、2^{-171} である。

ウ　SC2000

S-box として、4,5,6 ビット幅の物 3 種類が混在する事及びビットスライス構造を持つ為、トランケート評価では、大幅に緩い上界しか得られない。表中の()内の値は、参考文献[2]の繰り返しパスを全ラウンドに適用した値である。

192/256 ビット鍵の場合の安全性に関する取扱いについては今後検討が必要である。

(3) MULTI-S01 の MAC 機能について

MULTI-S01 はストリーム暗号として現リストに掲載されているが、 提案者は MAC 機能も謳っている。次期リストの暗号種別において新たに MAC を追加したので、MAC 機能に関する評価が必要である。

[8] [3]　金子敏信, “共通鍵ブロック暗号CIPHERUNICORN-Aの安全性に関する詳細調査報告書”, http://www.cryptrec.go.jp/estimation/rep_ID0027.pdf, 2001

３．８．２．実装性評価状況

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実装性能及びハードウェア実装性能の評価を実施した。評価対象の暗号技術と評価用実装の開発者を表 3.12 に示す。

表 3.12　評価対象の暗号技術と評価用実装の開発者

評価対象 アルゴリズム	実装評価		実装者
	ソフトウェア評価	ハードウェア評価	
CLEFIA	○	○	応募者
Enocoro-128v2	○	○	応募者
KCipher-2	○	○	応募者
PC-MAC-AES	○	○	応募者
AES	○	○	外部委託先
Camellia	○	○	外部委託先
CIPHERUNICORN-A	○	○	外部委託先
Hierocrypt-3	○	○	外部委託先
SC2000	○	○	外部委託先
MUGI	○	○	外部委託先
MULTI-S01	－	○	外部委託先
AES-CMAC	○	○	外部委託先

(1) ソフトウェア実装の性能評価

評価環境には、2009 年度に経済産業省による研究開発事業「クラウド環境における暗号技術評価」として開発された性能評価ツールを利用し、通常の PC 環境における処理速度、実装サイズ等を測定する方針に沿って実装評価を実施した。

現リスト掲載暗号の評価用実装は、性能評価ツールに添付の暗号ライブラリとして用意されているものを利用した。新規応募暗号については、実装開発に必要な情報をまとめた「応募暗号ソフトウェア実装性能評価要項」を応募者に配布し、評価用暗号モジュールの提出を依頼した。11 月内に全応募者から暗号モジュールが提出され、現リスト掲載暗号と合わせて、初期化、暗号化(MAC 生成)、復号(MAC 検証)に掛かったクロック数、使用したメモリ量を測定し、ソフトウェア実装性能評価はほぼ終了した。評価の結果、いずれの暗号技術も十分な実装性能を有していることを確認した。

測定結果のまとめ方と公開方法については、さらに検討する必要があるため、2012 年度もソフトウェア実装評価活動は継続する。

(2) ハードウェア実装性能の評価

実装プラットフォームに、サイドチャネル攻撃用標準評価ボード SASEBO-GII(産業技術総合研究所と東北大学が開発)を、評価環境には CRYPTREC の依頼により産業技術総合研究所が開発したものを利用して、高速実装における処理性能の評価とサイドチャネル攻撃に対する対策可能性の確認を実施した。

現リスト掲載暗号については、サイドチャネル攻撃対策可能性の確認は実施せず、

高速実装の開発及び性能評価を、一般競争入札で選考した業者に委託した。実装情報とその評価結果は 2 月末に納入され、現在その内容を確認中である。

新規応募暗号については、応募者に実装開発に必要な情報をまとめた「応募暗号ハードウェア実装性能評価要項」配布し、次の３種類の実装を提出するように依頼した。

評価用実装 1 （高速実装）
評価用実装 2 （対策実装）
評価用実装 3 （素朴実装）

これらの実装は 1 月内に提出され、高速実装については、動作周波数、暗号化・復号のサイクル数、実装サイズなどの測定がほぼ終了した。いずれの新規応募暗号技術も十分な実装性能を有していることを確認した。サイドチャネル攻撃対策可能性については、有効性を確認するための測定を準備中である。

３．９．CRYPTREC シンポジウム 2012 の開催

2011 年度は、電子政府推奨暗号リストの改訂のために応募暗号技術の第 2 次評価及び現リストに掲載された暗号技術の再評価を実施し、次期リスト選定基準の検討を行った。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。

３．９．１．プログラムの概要

日時：2012 年 3 月 9 日（金）10：00～15：45

場所：秋葉原 UDX

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：205 名

表 3.13　プログラム

3 月 9 日(金)		
時間	内容	
10:00	開会挨拶	
10:10	暗号方式委員会報告	応募暗号技術や現リストに掲載されている暗号技術に対する安全性評価の進行状況についての説明
10:40	暗号実装委員会報告	応募暗号技術と現リストに掲載されている暗号技術に対する実装性能評価の進行状況についての説明
11:40	昼休み	
12:40	暗号運用委員会報告	次期電子政府推奨暗号選定にあたっての考え方、並びに選定基準の検討状況についての説明
13:55	休憩	
14:10	ネットワークセキュリティについて 篠田陽一教授（北陸先端科学技術大学院大学）	
14:55	情報セキュリティ人材育成について 今井秀樹教授（中央大学）	
15:40	閉会挨拶	

４．電子政府推奨暗号選定のための選考基準案

４．１．電子政府推奨暗号選定の観点

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。

2010 年度暗号運用委員会で取りまとめた活動報告をもとに、2011 年度第 1 回暗号技術検討会にて次期リストの考え方についての審議を行った結果、次期リストに求める役割としては、以下の目標を実現する方向で今後の検討を進めるよう、意見集約が行われた。

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	「安全性」、「現状の調達容易性（利用実績）」、「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。	米国政府標準暗号以外の暗号は国際標準化や規格化、製品化からも排除される流れが強まっている点を考慮。 提案暗号に対する国としてのバックアップの明確化。

上記の方針を踏まえ、電子政府推奨暗号選定のための選考基準案の検討を行うにあたっては、「安全性」、「現状の調達容易性（利用実績）」並びに「将来的な調達容易性（利用実績）」の見通しを考慮し、以下の 2 つの観点で次期リストに掲載する暗号技術を選定することとした。

【観点(i)】

すでに現状の調達容易性（利用実績）が十分に高く、かつ将来的な安全性にも十分な余裕度があって、今後も安定して利用できる見込みがある暗号技術を選定する。

【観点(ii)】

現状の調達容易性（利用実績）は十分に高いとは言えないものの、以下の条件すべてを満たす暗号技術を選定する。

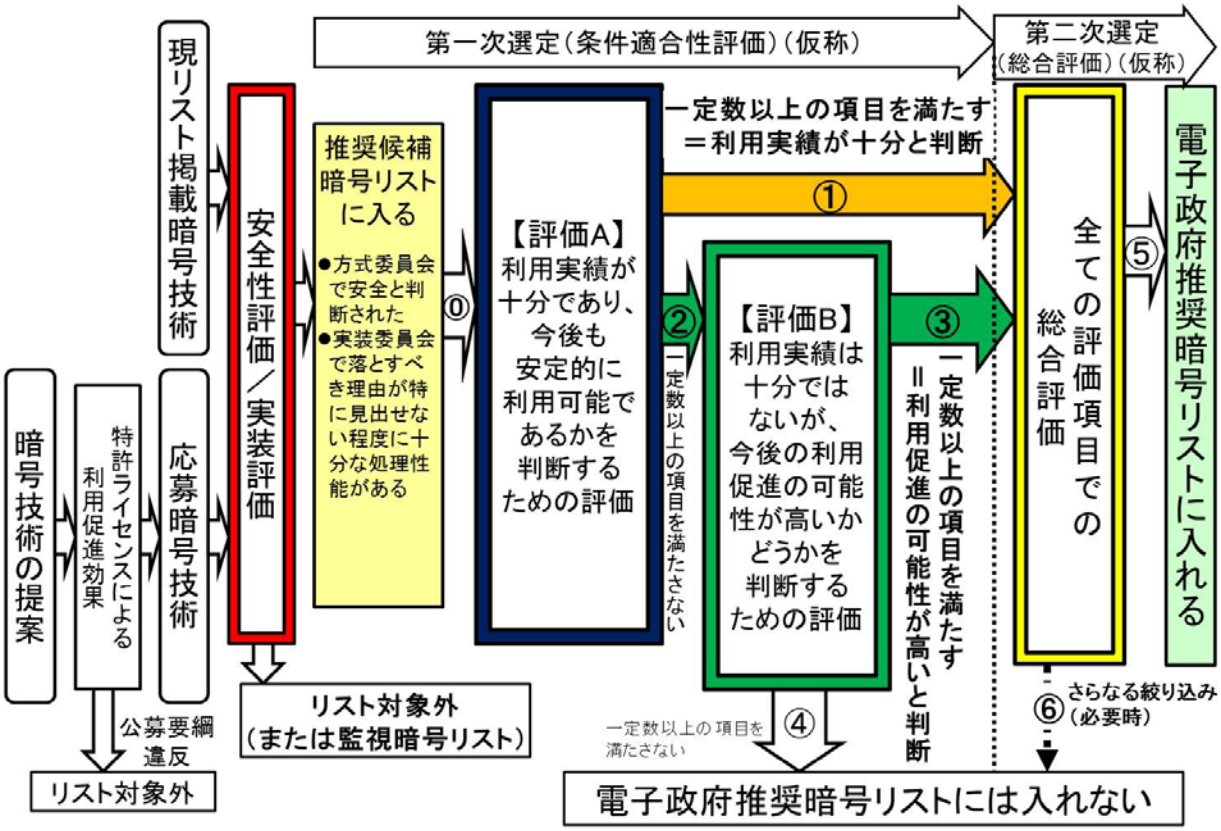
- 上記観点(i)で選定される暗号技術のなかで最も高い安全性を有するものと同等かそれ以上の安全性を有すると評価される。
- 今後の普及展開支援によって、国際標準化・製品化促進が図られると期待できる根拠がある。
- 今後の普及展開支援によって、将来的な調達容易性（利用実績）が十分に高くなると期待できる根拠がある。

４．２．電子政府推奨暗号選定のための選考基準案の考え方

４．１の観点(i)及び観点(ii)の考え方に沿い、次期リストに含める暗号技術を以下の考え方により選定する（図 4.1)。なお、本選考基準案の考え方については、2011 年度暗号運用委員会で審議された結果をもとに、第 2 回暗号技術検討会で承認したものである。暗号運用委員会での審議過程については、７．暗号運用委員会活動報告を参照されたい。

- 観点(i)により選定される可能性がある暗号技術は、評価 A において「現在の利用実績が十分である」と判断されたものである（選定ルート①を通るもの)。
- 観点(ii)により選定される可能性がある暗号技術は、評価 B により「現在の利用実績は十分とは言えないが、今後の利用促進の可能性が高い」と判断されたものである（選定ルート②③を通るもの)。

図 4.1　選定ルールのフレームワーク



評価 A で用いる「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」を行うために、表 4.2 に示す 4 つの評価項目を用いる。各々の評価項目について設定された選考基準を満たしているかを判断し、4 つの評価項目のうち一定数以上の項目が基準を満たしていれば「現在の利用実績が十分である」と判断する。

現時点では、各評価項目での選考基準の“具体的な基準値”は審議中であるので、選考

基準を決めるにあたっての“基本的な考え方”を示しておく。なお、選考基準の基本的な考え方としては、第一次選定（条件適合性評価）（仮称）段階（評価 A 及び評価 B）において出来る限り次期リストに掲載される暗号技術の個数を絞り込むこととし、そのための明示的な基準を“選考基準”として設定する。その意図は以下のとおりである。

- 次期推奨暗号リストへの不選定の理由が明確に説明できるようにする。
- 調査方法や調査対象の選定の仕方によって、評価結果における精度上の問題がある程度含まれることは織り込んでおく。
- 評価結果における精度上の問題がある程度含まれていても、次期推奨暗号リストへの選定・不選定が極力変わらないような選考基準とする。
- 総合評価は、「選定ルート①で第一次選定を通過した暗号技術」と「選定ルート②③で第一次選定を通過した暗号技術」との間で、現状の利用実績の評価差をある程度緩和することが本来の趣旨であり、絞り込み評価として利用することは極力避ける。
- 本来の選定意図とは異なる暗号技術が第一次選定を通過するような緩い選考基準は極力避ける。

表 4.2　評価 A での評価項目及び選考基準の基本的な考え方

評価項目	選考基準の基本的な考え方
市販製品での採用実績 （販売会社数・種類・種別）	一定数以上の採用実績があることに加え、提案会社・グループ会社以外での採用実績もある。
オープンソースプロジェクトでの採用実績	一定数以上のプロジェクトでの採用実績がある。 ※正式版（リリース版）に採用済みのものだけを取り上げる。
政府系システム規格での採用実績	一定数以上の政府系システム規格での採用実績がある。 ※規格化への採用が合意された段階のものまで含める（最終承認待ち）。
国際的な民間メジャー規格での採用実績	一定数以上の国際的な民間メジャー規格での採用実績がある。 ※規格化への採用が合意された段階のものまで含める（最終承認待ち）。

同様に、評価 B で用いる「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」を行うために、評価 A で用いた評価項目 4 つに加え、表 4.3 に示す 4 つの評価項目を追加する。つまり、評価 B においては、8 つの評価項目のうち一定数以上の項目が基準を満たしていれば「今後の利用促進の可能性が高い」と判断する。

表 4.3　評価 B での評価項目及び選考基準の基本的な考え方

<table>
<tr><td colspan="4">評価 A（「市販製品での採用実績　（販売会社数・種類・種別）」「オープンソースプロジェクトでの採用実績」「政府系システム規格での採用実績」「国際的な民間メジャー規格での採用実績」）に加えて</td></tr>
<tr><td colspan="3">評価項目</td><td>選考基準の基本的な考え方</td></tr>
<tr><td colspan="3">利用促進を図る際の障壁の除去</td><td>非差別的に特許無償許諾を実施。
（許諾契約締結が条件であってもよい）</td></tr>
<tr><td rowspan="3">標準化・規格化の促進を図るハードルの低さ</td><td rowspan="3">ＯＲ条件</td><td>技術的アピールポイント</td><td>市場が認める程度の技術的アドバンテージがある。</td></tr>
<tr><td>標準化等のアピールポイント</td><td>他の一定数以上の標準化・規格化に採用されていれる。</td></tr>
<tr><td>採用実績のアピールポイント</td><td>一定数以上の利用実績や製品・オープンソースプロジェクトでの採用実績がある。</td></tr>
<tr><td rowspan="2">実装コスト低減を図るハードルの低さ</td><td rowspan="2">ＯＲ条件</td><td>採用実績のアピールポイント</td><td>一定数以上の OS や暗号モジュールでの採用実績がある。</td></tr>
<tr><td>オープンソースのアピールポイント</td><td>一定数以上の暗号モジュールとして使えるオープンソースプロジェクトでの採用実績がある。</td></tr>
<tr><td>調達コスト低減を図るハードルの低さ</td><td colspan="2">採用実績のアピールポイント</td><td>一定数以上の利用実績や製品・オープンソースプロジェクトでの採用実績がある。</td></tr>
</table>

第二次選定（総合評価）においては、表 4.4 に示す各評価項目に決められた加点基準をもとに総合評価を行うことする。その際、「選定ルート①で第一次選定を通過した暗号技術」と「選定ルート②③で第一次選定を通過した暗号技術」との間で現状の利用実績の評価差をある程度緩和するために、「利用促進が図られると期待される根拠」に該当する 4 つの評価項目については「選定ルート②③で第一次選定を通過した暗号技術」に対してのみ加点対象とする。

表 4.4　総合評価の基本的な考え方

評価項目		選定ルート①で通過	選定ルート②③で通過
技術的側面	安全性についての仕様上のアドバンテージ	○	○
	論文数の多寡によるアドバンテージ	○	○
	ソフトウェア実装性能評価	○	○
	ハードウェア実装性能評価	○	○
現状での利用実績	政府系システムでの採用実績	○	○
	市販製品での採用実績	○	○
	オープンソースプロジェクトでの採用実績	○	○
	特許ライセンスによる利用促進効果	○	○
	オープンソース公開による利用促進効果	○	○
	政府系システム規格での採用実績	○	○
	国際標準規格での採用実績	○	○
	国際的な民間メジャー規格での採用実績	○	○
	民間の特定団体規格での採用実績	○	○
利用促進が図られると期待される根拠	利用促進を図る際の障壁の除去	－	○
	標準化・規格化の促進を図るハードルの低さ	－	○
	実装コスト低減を図るハードルの低さ	－	○
	調達コスト低減を図るハードルの低さ	－	○

凡例：　○：加点対象　　－：加点対象としない

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、及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、2011 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、主に、現リストに記載されている暗号技術に関する安全性評価を実施した。また、暗号技術の安全性に関する監視活動を行った。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とおりである。

(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。

５．１．２．暗号方式委員会開催状況

2011 年度、暗号方式委員会は、表 5.1 のとおり 2 回開催された。委員会の開催日及び主な議題は以下のとおりである。

表 5.1　暗号方式委員会の開催

回	年月日	議題
第 1 回	2011 年 8 月 5 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、暗号技術評価方法の検討、監視状況報告。
第 2 回	2012 年 2 月 24 日	暗号技術評価結果（案）に係る検討、WG 活動報告、監視情報報告。

５．２．委員会の調査・検討結果

５．２．１．現リストに掲載された暗号技術に関する評価

128 ビットブロック暗号に関して、鍵拡大関数の安全性や 192 ビット／256 ビット鍵長の場合の安全性に関する評価を実施した。その概要については、「３．８．１．安全性評価状況」に記載したとおりである。詳細については、CRYPTREC Report 2011 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 2011 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。

（共通鍵暗号の安全性評価について）

AES に対する最初の単一鍵攻撃が Crypto 2011 のランプセッションで公表され、正式な国際発表論文としては Asiacrypt 2011 で発表された。本攻撃では、以前よりハッシュ関数に適用されていた Meet-in-the-Middle 攻撃を改良してブロック暗号に適用した Biclique Attack が利用されている。基本的には鍵回復における総当たり攻撃において、その効率性を高めたものであり、論文では AES-128 に対して $2^{126.1}$、AES-192 に対して $2^{189.7}$、AES-256 に対して $2^{254.4}$ の計算量で鍵回復ができるとしているが、計算量の減少は約 2 ビット分と非常に少ない。この手法をより発展させて効率的な攻撃に結びつけることは難しく、AES の安全自体への影響はほとんどないと考えられる。Biclique Attack は他のブロック暗号にも適用可能ということであり、今後の動向には注意する必要がある。

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

2011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5.2に示すとおりである。

表 5.2　国際会議への参加状況

学会名・会議名		開催国・都市	期間
SAC 2011	Selected Areas in Cryptography	カナダ・トロント	2011 年 8 月 11 日～8 月 12 日
Crypto 2011	International Cryptology Conference	米国・サンタバーバラ	2011 年 8 月 14 日～8 月 18 日
NIAT 2011	Non-Invasive Attack Testing Workshop	日本・奈良	2011 年 9 月 26 日～9 月 27 日
FDTC 2011	Fault Diagnosis and Tolerance in Cryptography	日本・奈良	2011 年 9 月 28 日
CHES 2011	Workshop on Cryptographic Hardware and Embedded Systems	日本・奈良	2011 年 9 月 29 日～10 月 1 日
Asiacrypt 2011	International Conference on the Theory and Application of Cryptology and Information Security	韓国・ソウル	2011 年 12 月 5 日～12 月 8 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 の暗号監視報告等各種報告書、並びに国内外の暗号プロトコル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、鍵共有技術、及び一般的な暗号プロトコルにおける暗号技術の利用方法について、情報提供並びに推奨事項を取り纏めて、リストガイドを作成した。2011 年度は電子政府推奨暗号における鍵共有として、DH(ANSI X9.42-2003、NIST SP 800-56A)、ECDH(SEC1, NIST SP 800-56A)、PSEC-KEM のガイド、及び一般的な暗号プロトコルとして、SSL3.0、TLS 1.0/1.1/1.2、IPsec、DNSSEC のリストガイドを作成した。

暗号技術調査ワーキンググループ（リストガイド）（以下、「リストガイド WG」という）の 2011 年度の主要活動項目は、表 5.3 のとおりである。

表 5.3　2011 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 東京工科大学教授	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、鍵共有技術、及び一般的な暗号プロトコルにおける暗号技術の利用方法について、情報提供並びに推奨事項を取り纏めて、リストガイドを作成。

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 5.4 のとおり計 2 回開催された。

表 5.4　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	2011 年 11 月 14 日	リストガイドの構成、執筆内容、作業方針の検討
第 2 回	2012 年 1 月 24 日	● 各検討項目に関する検討を元にした議論と執筆内容の確定 ● 今年度作業から判明した課題についての整理

第 1 回リストガイド WG（2011 年 11 月 14 日）では、今年度作成するリストガイドの構成、執筆内容、作業方針について議論を行った。今年度作成するリストガイドは、電子政府推奨暗号の鍵共有（DH、ECDH、PSEC-KEM)、SSL/TLS、IPsec、DNSSEC の 4 つに分けて構成することとした。それぞれの項目に係る執筆内容については、表 5.5 のとおり。

表 5.5　2011 年度リストガイド執筆内容・検討項目

リストガイド	執筆内容・検討項目
電子政府推奨暗号：鍵共有	・ DH,ECDH のスキーム・アルゴリズムの整理・記載 ・ PSEC-KEM のスキームの追記及びアルゴリズムの記載 ・ FFC/ECC セキュリティパラメータの推奨 ・ FFC/ECC ドメインパラメータの整理 ・ KDF に関する整理
SSL/TLS	・ SSL/TLS の実行環境の整理 ・ 推奨暗号スイート一覧作成 ・ PSK、SRP の取扱い ・ DES/3DES/RC4 に関する取扱い
IPsec	・ 推奨暗号スイートの一覧作成 ・ HMAC-SHA1-96 の取扱い
DNSSEC	・ DNSSEC ソフトウェアの整理 ・ 推奨暗号スイートの一覧作成 ・ ZSK、KSK に係る鍵長の推奨

推奨暗号スイート一覧の作成においては CRYPTREC として推奨している暗号技術以外の暗号スイートを除いた一覧を作成することを大方針とし、具体的には以下の場合を除いた暗号スイート一覧を作成することとした。

- 電子政府推奨暗号として指定された暗号プリミティブを用いているが、鍵長等について安全性上問題がある場合
- 電子政府推奨暗号として指定された技術カテゴリであるが、指定されていない暗号プリミティブを用いている場合
- 電子政府推奨暗号として指定されていない技術カテゴリであり、かつ、安全性に問題がある場合

作業方針として、検討項目について事務局で検討を進めるとともに、執筆内容に沿って各リストガイドの素案の作成を行い、適時委員のレビュー及び検討・作業を行いながら作業を進めることとなった。

この他、JCMVP 櫻井様より鍵共有に係る暗号モジュール試験方法及び動向について講演いただくとともに、DNSSEC の仕組み及び動向について民田委員より講演をいただいた。

第 2 回リストガイド WG（2012 年 01 月 24 日）では、各検討項目に関する検討結果を示し、議論を行い執筆内容の確定を行った。また、併せて、今年度作業から判明した課題について整理・議論を行った（4 節参照）。具体的な議論の内容と結果について以下に示す。

□ FFC/ECC　セキュリティパラメータについて

- 新規システムでの導入も含め、暗号強度 128 ビット相当以上への切り替えを推奨する。
  - ✧ FFC：|p|=2048、|q|=224
  - ✧ ECC：f=224 以上
- 暗号強度 80 ビット相当については当面（2～3 年）程度の利用を認める。

- ✧ FFC：|p|=1024、|q|=160
- ✧ ECC：f=160-223

□ FFC/ECC　ドメインパラメータについて

- ➢ FFC のドメインパラメータについては、SP 800-56A、FIPS 180-3 に記載される L=|p|,N=|q|の組を記載する。
- ➢ ECC については、NIST が指定する曲線(FIPS 180-3)及び SEC2 で指定される曲線を明示し、情報提供を行う。

□ SSL/TLS　実行環境について

- ➢ クライアントサイドの実行環境について、OS とブラウザのペアを整理し、SSL/TLS の各バージョンの利用可能性を調査した。
- ➢ 結果、TLS 1.1/1.2 を利用できるのは Microsoft 社の Windows 7 + SP 1 環境における Internet Explorer 9 のみであることが判明した。
- ➢ OpenSSL 等での TLS 1.1/1.2 対応が進み始めた状況を踏まえ、今後円滑に TLS 1.1/1.2 が利用できるように環境を整備することを付言することとした。

□ IPsec　HMAC-SHA-1-96 の取扱いについて

- ➢ HMAC-SHA-1-96 については 96 ビット程度の安全性を有していることを確認した。
- ➢ 一方で、IPsec においては HMAC-SHA-1-96 をはずして推奨暗号スイート一覧を作成することは、実用上困難であることから、安全性については 96 ビット相当であることを付言することとした。

□ DNSSEC 推奨鍵長

- ➢ 比較的長期間(13 ヶ月程度)利用する KSK については 2048 ビット相当以上を推奨することとした。
- ➢ 比較的短期間(1 ヶ月程度)利用する ZSK については、実用上の問題も加味し、1024 ビット相当以上を推奨することとした。

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、2011 年度版のリストガイドとして、以下の 4 つの文書をとりまとめた。

- ● 2011 年度版リストガイド（電子政府推奨暗号：鍵共有）
- ● 2011 年度版リストガイド（SSL/TLS）
- ● 2011 年度版リストガイド（IPsec）
- ● 2011 年度版リストガイド（DNSSEC）

詳細については、2011 年度版リストガイドを参照のこと。

これまでの作業過程において抽出された課題を以下に示す。

■ 電子政府推奨暗号：鍵共有

① 楕円曲線に係る検討

・ NIST Curve, SEC2 等、各種標準のコンフォーマンスの確認
・ CRYPTREC として推奨する楕円曲線パラメータの策定

② KDF に係る検討
・ CRYPTREC として推奨する KDF Set の策定

③ 素数判定に係る検討
・ 素数判定アルゴリズムの利用方法の整理

■ SSL/TLS

④ RC4_128、3DES_EDE に関する取扱い

⑤ RFC 等の策定状況に基づく、推奨暗号スイートの定期的なメンテナンス

⑥ サーバサイド TLS の対応状況及び設定方法についての整理・推奨

⑦ PSK に係る鍵管理、SRP の安全性に関する確認

■ IPsec

⑧ RFC 等の策定状況に基づく、推奨暗号スイートの定期的なメンテナンス

■ DNSSEC

⑨ ZSK、KSK に係る鍵管理・鍵更新に関するリストガイドの作成

上記課題については、今後の CRYPTREC の活動において適切な委員会やワーキンググループで検討を行う。

５．４．暗号技術調査ワーキンググループ（計算機能力評価）の活動

５．４．１．暗号技術調査ワーキンググループ（計算機能力評価）の活動目的と経緯

RSA-1024 を安全に使える期間の根拠となっている計算機能力進化の予測図（暗号技術検討会 2006 年度報告書、12 ページ、図 2）は様々な場所において有効に活用されているが、作成が 2006 年度であり、更新が必要となっている。また、一定期間毎に更新されることも求められている。これらの状況を鑑みて、2006 年度に作成されたグラフの見直しと更新作業及び公開の方法について検討を行った。

暗号技術調査ワーキンググループ（計算機能力評価）（以下、「計算機能力評価 WG」という）の 2011 年度の主要活動項目は、表 5.6 のとおりである。

表 5.6　2011 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
計算機能力評価 WG	高木剛 九州大学 教授	・2006 年度から現在までに新規のスーパーコンピュータが開発されており、それらをプロットする。 ・予測図によれば、RSA-1024 は世界最速のスーパーコンピュータを占有して計算すると、1 年間で解読される状況に到達したと読める。この解釈で問題がないか、または必要に応じて補足すべき資料を作成すべきかを検討する。 ・予測図の更新に関して、年度単位もしくは新しいスーパーコンピュータの誕生を目途にするなど、更新する機会について検討する。さらに公開の方法についても検討する。

５．４．２．計算機能力評価 WG の開催状況

本年度は、計算機能力評価ワーキンググループは、表 5.7 のとおり計 2 回開催された。

表 5.7　暗号技術調査ワーキンググループ(計算機能力評価)の開催

回	年月日	議題
第 1 回	2011 年 10 月 6 日	活動計画や作業内容についての審議と了承
第 2 回	2011 年 12 月 21 日	報告内容についての審議と了承

５．４．３．計算機能力評価 WG の成果概要

(1) 予測図の見直し

CRYPTRECでは、CRYPTREC Report 2006[9]において「1 年間でふるい処理を完了するのに要求される処理能力の予測」に関する図を公表した。そこでは、計算機性能の将来予測に関して、スーパーコンピュータのベンチマーク結果の 1 位から 500 位を 1993 年から

[9] http://www.cryptrec.go.jp/report/c06_wat_final.pdf

半年毎に集計している WebサイトTOP500.Org[10]に掲載されているデータを利用している。現在までに 2007 年 6 月から 2011 年 11 月までのベンチマーク結果が追加されているので、以前公表した図についても下記のとおり更新した。また、一般数体ふるい法が利用された過去の素因数分解記録についてもプロットした。

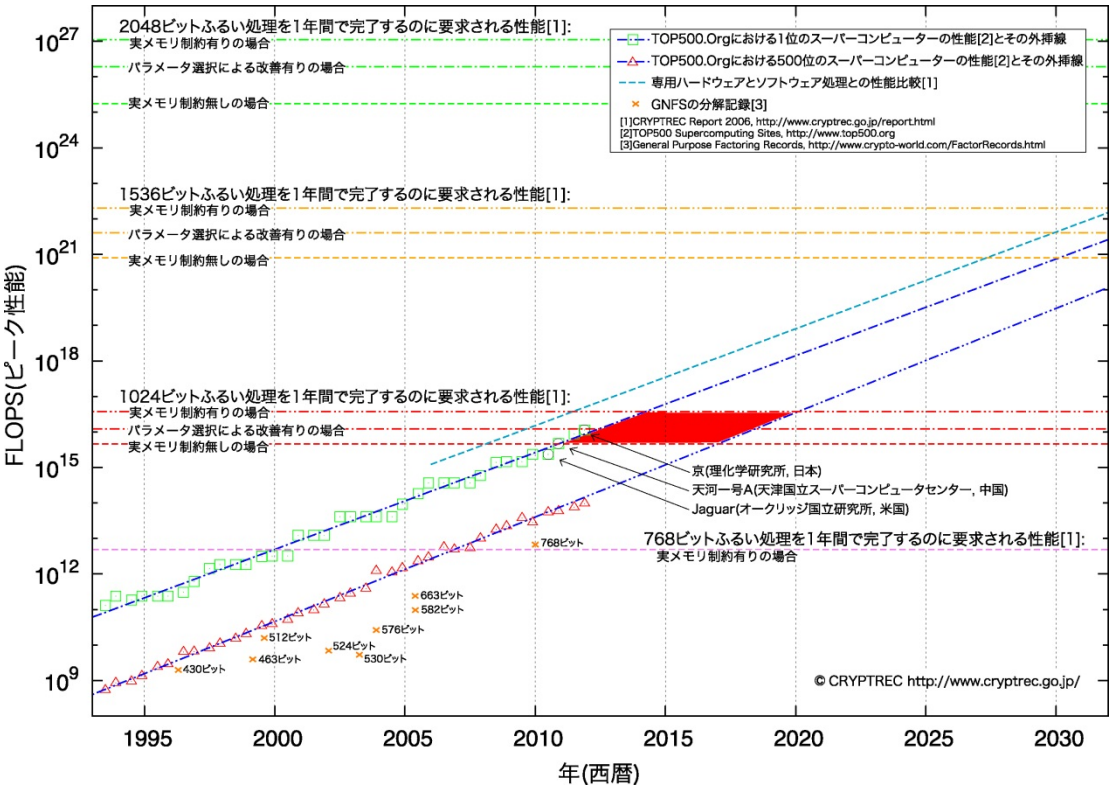


図 5.8　1 年間でふるい処理を完了するのに要求される処理能力の予測(2011 年 12 月更新)

(2) 2011 年現在における状況の解説

(a) ふるい処理の前段階の多項式選択ステップの改善により完了時期が若干前倒しされる可能性はあるものの、過去の予測を大きく変えるものではないため、ふるい処理に要する計算量の推定に関する情報の更新は行わなかった。つまり、図 5.8 の水平方向に描かれているすべての点線（ふるい処理を 1 年間で完了するのに要求される性能）の位置は以前と変わらない。

(b) 2011 年 11 月現在におけるtop 1 のスーパーコンピュータの性能は、1024 ビットふるい処理を 1 年間で完了するのに要する性能における、「実メモリ制約無しの場合」を超え、「パラメータ選択による改善有りの場合」の水準まで近づいてきている。計算機能力の進展が現状のとおり達成され続けている限りは、菱形領域内に入った計算機で当該処理を各々の制約条件[11]のもと 1 年間で完了できるとの予測は現在も妥当で

[10] http://www.top500.org/
[11] 制約条件とは、実メモリ制約有り／パラメータ選択改善有り／実メモリ制約無し、のいずれかを指す。

あると考えられる。つまり、RSA1024 の安全性評価は以前と変わらず、過去における、

CRYPTREC Report 2006 の 18 ページの上から 2 行目：

法パラメータのサイズが 1024 ビットの IFP(n=pq 型素因数分解問題)を 1 年間の計算によって完了させるためには、10^{15}FLOPS から 10^{17}FLOPS の処理能力を持つ計算機が要求され、高性能のスーパーコンピュータが過去の成長率を続けて成長した場合に、そのレベルに到達する時期は、図 2.2 に示すように 2010 年～2020 年の間と推定することができた。

電子署名及び認証業務に関する法律の施行状況に係る検討会報告書(平成 20 年 3 月）[12]の 18 ページの下から 6 行目：

二 RSA1024bit については、概ね 2015 年以降に、危殆化のおそれが高まってくることが示されている(図 2-4)こと。

という報告ついても特に変更を要するものではない。従って、2008 年 4 月に情報セキュリティ政策会議において決定されている「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」[13]は、その記載のとおり対応していくことが望ましいと考えられる。

(c) 公表されているデータ [14]に基づいて、過去のRSA分解記録をプロットした。なお、RSA768 の記録は、CRYPTREC Report 2006 に公表したデータにおけるRSA768 に関する推定値（実メモリ制約有りの場合）とほぼ同じである。

(d) 暗号の安全性の尺度としてコストが用いられることが多いが、電気代、場所のコストや並列処理に必要となる通信時間が考慮してされているとは限らないことなど、コスト換算に関して様々な前提条件があることに注意が必要である。費用対効果の観点から考えると、RSA-1024 解読のための最も現実的な選択肢は汎用計算機であり、文献 [15][16]に基づく概算によれば、おおよそ 10 億ドル(以上)のコストが必要となる。独立行政法人理化学研究所と富士通株式会社が共同開発したスーパーコンピュータ「京」の総事業費が約 1120 億円であることを考慮に入れると、この概算はスーパーコンピュータを購入する経費に匹敵しており、「1 年間でふるい処理を完了するのに要求される処理能力の予測」に関する図とほぼ整合性が取れていることがわかる。

[12] http://www.soumu.go.jp/menu_news/s-news/2008/080530_4.html
[13] http://www.nisc.go.jp/active/general/res_niscrypt.html
[14] http://www.crypto-world.com/FactorRecords.html
[15] http://eprint.iacr.org/2009/389
[16] http://eprint.iacr.org/2011/254

(3) 更新作業のあり方について

予測図に関して、最新のデータが欲しいという要望があるため、公開方法について検討し、下記のとおりの結論を得た。

(a) 公開場所

CRYPTREC の Web サイト及び CRYPTREC Report に掲載する。

※CRYPTREC Report については、その年度の最新データのみ掲載する。

(b) 公開する内容

「(1) 予測図の見直しにおける図 5.8」と「(2) 2011 年現在における状況の解説(a)～(c)」

(c) 更新頻度

ア　TOP500.Org における更新頻度に合わせて、スーパーコンピュータのプロットに関しては原則年 2 回更新を行う。RSA 分解記録が出た場合は、その都度更新する。

イ　暗号方式委員会にてメール審議を行い、承認の後に公開／更新を行う。

(d) 予測図の取り扱い予測図は多目的に引用されてきていることから、予測図のみの引用は可能とし、公開の際は、予測図と安全性評価に関する文言とは切り離し可能とする。引用の際は、CRYPTREC 事務局(info@cryptrec.go.jp)への連絡を希望する。

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はじめとする暗号実装関連の技術動向を調査するために、2008 年度まで組織され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、電子政府推奨暗号リスト改訂に伴う実装性能評価を実施するとともに、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と防御に関する調査・検討を行った。

以下に、2011 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とその対策の動向を調査した。特に次の項目を実施した。

(1) リスト改訂のための実装性能評価

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実装及びハードウェア実装の性能評価に関する詳細を決定し評価を実施した。

(2) リスト改訂のためのサイドチャネル攻撃対策可能性の評価

応募暗号技術のハードウェア実装において、サイドチャネル攻撃対策が可能であることを検証するための評価項目を決定し、評価を開始した。

(3) リスト改訂のためのサイドチャネル攻撃耐性の評価に関する検討

・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とその対策技術の研究開発動向を調査・検討した。この調査・検討において、サイドチャネル解析用プラットフォームである SASEBO ボードを用いた研究に重点をおいた。

・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活動に協力した。

６．１．２．暗号実装委員会開催状況

2011 年度、暗号実装委員会は、表 6.1 のとおり 3 回開催された。開催日及び主な議題は以下のとおりである。

表 6.1　暗号実装委員会の開催

回	年月日	議題
第 1 回	2011 年　9 月 12 日	委員長互選 活動計画の審議・承認 実装性能評価の進行状況報告
第 2 回	2011 年 12 月 19 日	実装性能評価の進行状況報告 ソフトウェア実装性能評価結果の検討 暗号運用委員会からの検討要請対応
第 3 回	2012 年　2 月 13 日	実装性能評価の進行状況報告 暗号運用委員会からの検討要請対応 実装評価報告書の作成方針検討

６．２．委員会の活動状況

６．２．１．実装性能評価

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実装性能及びハードウェア実装性能の評価を実施した。応募暗号技術に関しては、ソフトウェアとハードウェアの両方について、評価対象の実装を開発するための要項を作成して応募者に提示した。新規応募暗号は全て期限内に実装物が提出され、ソフトウェア実装について性能評価がほぼ終了した。ハードウェア実装については、性能評価はほぼ終了し、サイドチャネル攻撃対策可能性は評価中である。

６．２．２．暗号運用委員会からの検討要請対応

暗号運用委員会では、安全性・実装性能ともに十分な候補暗号から、電子政府推奨暗号リストに掲載する暗号を絞り込むための選択基準を検討している。その検討を行う上で，暗号運用委員会から、暗号実装委員会に次の三項目（(A)実装性能評価の内容 (B)実装性能評価の精度 (C)実装性能評価の結果を暗号選択に利用することについての見解）について質問があった。

暗号実装委員会では、(A)については、具体的な評価環境・評価項目を回答した。(B)と(C)については、通常の実装環境で問題なく利用できるか否かは判定できるものの、詳細な性能比較に適したものにはなっていないため、評価結果を暗号選択で利用することについては望ましくないと回答した。

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

暗号実装委員会の下に設置されたサイドチャネルセキュリティワーキンググループ（WG）において、SASEBO ボードを評価環境とするものを中心に、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とその対策技術の研究開発動向を調査・検討した。

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、2009 年度からは「サイドチャネルセキュリティワーキンググループ」（後述）として活動を継承している。

今年度は、暗号モジュールのセキュリティ要求事項 ISO/IEC 19790 及びその試験要件で

ある ISO/IEC 24759 に反映させるべく、改訂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、近年電磁波解析や故障利用攻撃の研究も活発になされており、活動とワーキンググループ名との間にずれが生じた。そこで、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（以下、「サイドチャネルセキュリティ WG」という）が暗号実装委員会の下に設置された。本年度は、次の２つを柱として活動した。

(1) ISO/IEC 19790 及び ISO/IEC 24759 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 WG の開催状況

2011 年度、サイドチャネルセキュリティ WG は、表 6.2 のとおり 2 回開催された。開催日及び主な議題は以下のとおりである。

表 6.2　サイドチャネルセキュリティ WG の開催

回	年月日	議題
第 1 回	2011 年 12 月 19 日	活動計画の審議・承認 国際標準化対応についての方針検討
第 2 回	2012 年　2 月 13 日	ISO/IEC DIS 19790 及び ISO/IEC 2nd WD 24759 に対する日本コメント案作成 国際会議等の参加報告

６．３．３．サイドチャネルセキュリティ WG の成果概要

本年度は、ISO/IEC 19790 第 2 版の 1st CD と DIS、及び、ISO/IEC 24759 第 2 版の 1st WD と 2nd 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。なお、コメント案作成時期に合わせて WG を開催することが困難であったため、打ち合わせ等の作業はメーリングリストを通じて行った。

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

2011 年度は応募暗号の実装評価の内容に従い、応募者に４種類の実装、性能評価用ソフトウェア実装、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、提出された実装に対して性能評価を実施した。現在、ハードウェア実装とハードウェア実装の性能評価はほぼ完了した。

2012 年度は、サイドチャネル攻撃対策可能性の評価を完了するとともに、実装評価結果を報告書にまとめる。

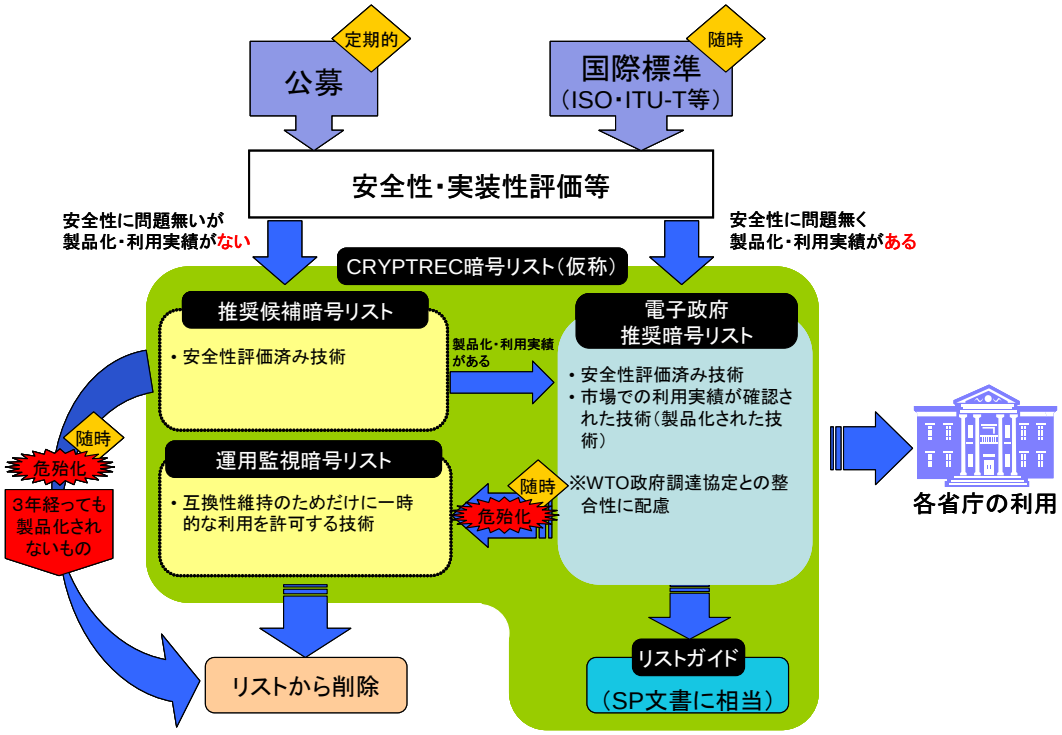
サイドチャネルセキュリティ WG では、引き続き ISO/IEC 19790 及び ISO/IEC 24759 の早期改訂ドラフトに対するコメント案作成、サイドチャネル攻撃の研究動向調査を行う。

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。

図 7.1　新しい電子政府推奨暗号リストの構成



【電子政府推奨暗号リスト】

CRYPTREC により安全性が確認され、かつ市場において利用実績が十分である暗号技術リスト。電子政府構築（政府調達）の際には当該技術の利用を推奨する（現リストと同等の位置づけ）。ここに登録される技術は国際標準化機関等により、標準化されていることが望まれる。

【推奨候補暗号リスト】

CRYPTREC により安全性が確認されているが、市場において利用実績が十分でない普及段階にある暗号技術が登録されているリスト。今後、利用が期待される新規技術等はここに分類される。電子政府構築（政府調達）の際には当該技術も利用することができる。

【運用監視暗号リスト】

電子政府推奨暗号リストに登録されていたが、実際に解読されるリスクが高まるなど、推奨すべき状態ではなくなったもののうち、互換性維持のために継続利用を容認するもののリスト。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。CRYPTREC として互換性維持以外の目的では利用を推奨しない。

暗号運用委員会では、2011 年度第 1 回暗号技術検討会で審議・意見集約された「電子政府推奨暗号リストの考え方」に基づき、次期リストの実運用における方向性を具体化するための必要な検討を行う。具体的には、2012 年度に電子政府推奨暗号を選定するために用いる選考基準案の検討、及び、電子政府推奨暗号リストに掲載される暗号アルゴリズムについて、費用対効果の観点を考慮しつつ、当該暗号アルゴリズムの利用が促進されるような取り組み方法についての検討を主に実施する。

以下に、2011 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

2011 年度第 1 回暗号技術検討会において承認された 2011 年度暗号運用委員会活動計画に基づき、本年度の暗号運用委員会の審議を行った。

特に、(1)の電子政府推奨暗号選定のための選考基準については、実際の電子政府推奨暗号の選定作業が本格化する前に明らかにしておく必要があるため、本年度の最重要項目として検討を行い、選考基準案の考え方を取りまとめた。

(1) 電子政府推奨暗号選定のための選考基準案の検討

次期 CRYPTREC 暗号リスト（仮称）の方向性を踏まえ、2012 年度に電子政府推奨暗号を選定するために用いる選考基準案を検討する。

(2) 電子政府推奨暗号の利用促進体制の検討

電子政府推奨暗号リストに掲載される暗号アルゴリズムについて、費用対効果の観点を考慮しつつ、当該暗号アルゴリズムの利用が促進されるような取り組み方法について検討する。

(3) 運用監視暗号リストへの遷移要件に関する基準の検討

電子政府推奨暗号リストに掲載されている暗号アルゴリズムの安全性が暗号学会等で低下したことが判明した場合の対応について、必要に応じて検討する。

(4) その他

暗号運用委員会としての、コンティンジェンシープランに対する寄与の可能性について、必要に応じて、継続して検討する。

また、2012 年度に向けて、推奨候補暗号リストの活用方法、次期 CRYPTREC 暗号リスト（仮称）策定に伴う暗号学界への影響と対策、等に関する予備検討を開始する。

７．１．２．暗号運用委員会開催状況

2011 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 7.2 のとおりである。

表 7.2　2011 年度暗号運用委員会概要

回	開催日時	主な議題
第 1 回	2011 年 9 月 21 日	● 暗号運用委員会活動計画について ● 次期電子政府推奨暗号の選考基準案の検討について（第 1 回）
第 2 回	2011 年 11 月 18 日	● 次期電子政府推奨暗号の利用促進取り組みへの検討について ● 次期電子政府推奨暗号の選考基準案の検討について（第 2 回）
第 3 回	2012 年 1 月 27 日	● 次期電子政府推奨暗号の選考基準案の検討について（第 3 回）
第 4 回	2012 年 2 月 24 日	● 次期電子政府推奨暗号の選考基準案の検討について（第 4 回）

７．２．委員会の調査・検討結果

７．２．１　次期推奨暗号リストに掲載する暗号技術選定の考え方

2010 年度の暗号運用委員会で取りまとめた活動報告をもとに、2011 年度第 1 回暗号技術検討会にて審議を行った結果、次期電子政府推奨暗号リスト（以下、次期推奨暗号リスト）に求める役割としては、以下の目標を実現する方向で今後の検討を進めるよう、意見集約が行われた。

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	「安全性」、「現状の調達容易性（利用実績）」、「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。	米国政府標準暗号以外の暗号は国際標準化や規格化、製品化からも排除される流れが強まっている点を考慮。 提案暗号に対する国としてのバックアップの明確化。

2011 年度暗号運用委員会では、上記方針の趣旨について、「安全性」、「現状の調達容易性（利用実績）」並びに「将来的な調達容易性（利用実績）」の見通しを考慮した、以下の 2 つの観点で次期推奨暗号リストに掲載する暗号技術を選定することと解釈した。その解釈を前提として、電子政府推奨暗号選定のための選考基準案の検討を進めた。

【観点(i)】

すでに現状の調達容易性（利用実績）が十分に高く、かつ将来的な安全性にも十分な余裕度があって、今後も安定して利用できる見込みがある暗号技術を選定する.

【観点(ii)】

現状の調達容易性（利用実績）は十分に高いとは言えないものの、以下の条件すべてを満たす暗号技術を選定する。

- 上記観点(i)で選定される暗号技術のなかで最も高い安全性を有するものと同等かそれ以上の安全性を有すると評価される。
- 今後の普及展開支援によって、国際標準化・製品化促進が図られると期待できる根拠がある。
- 今後の普及展開支援によって、将来的な調達容易性（利用実績）が十分に高くなると期待できる根拠がある。

７．２．２　次期推奨暗号リストに掲載する暗号技術選定のための評価項目

7.2.1 で記した観点(i)及び観点(ii)の考え方に則った暗号技術を次期推奨暗号リストに選定するために、どのような意図をもった評価項目を含めるべきかについての検討を行った。その際、2009 年度に経済産業省が実施した「暗号モジュールの市場動向等に関する調査研究」における「暗号アルゴリズムの市場性」の調査結果、並びに 2010 年度に暗号運用委員会が実施した「暗号アルゴリズムの利用実態に関する外部アンケート調査」の調査結果等も参考にした。

検討の結果、以下の評価観点を踏まえ、最終的に 17 個の評価項目を選定した。具体的な評価項目並びに評価意図は表 7.2 にまとめたとおりである。

- 「技術的側面」での評価観点
  技術的に優れているかどうかを評価する。
  - 安全性
  - 処理性能
- 「現状の調達容易性（利用実績)」での評価観点
  主に観点(i)の意味での利用実績を満たしているかどうかを評価する。
  - 市販製品やオープンソースプロジェクトでの利用状況
  - 政府系システムでの利用状況
  - 各種標準化・規格化での採用状況
- 「利用促進が図られると期待される根拠」での評価観点
  主に観点(ii)の意味での利用促進が図られると今後期待される根拠を満たしているかどうかを評価する。
  - 各種標準化・規格化が促進されるか
  - 調達コストや実装コストの低減につながるか

表 7.3　評価項目及び評価意図のまとめ

評価項目		評価意図
技術的側面	安全性についての仕様上の特長に関するアドバンテージ	安全性評価の安全性アドバンテージを認めるかを判断する。
	論文数の多寡によるアドバンテージ	安全性評価の信頼性アドバンテージを認めるかを判断する。
	ソフトウェア実装性能評価	ソフトウェアでの実装性能の優位性を判断する。
	ハードウェア実装性能評価	ハードウェアでの実装性能の優位性を判断する。
現状での利用実績	政府系システムでの採用実績	政府系システムでの利用状況により必要性を判断する。
	市販製品での採用実績（販売会社数・種類・種別）	市販製品での利用状況により必要性を判断する。
	オープンソースプロジェクトでの採用実績	利用容易性・利用促進性、及び仲間作りの進捗度合いを判断する。
	特許ライセンスによる利用促進効果	特許ライセンスによるベンダロックインの懸念度合い及び利用容易性・利用促進性を判断する。
	オープンソース公開による利用促進効果	利用容易性や利用促進性を判断する。
	政府系システム規格での採用実績	政府系システムでの必要性を判断する。
	国際標準規格での採用実績	国際的な認知度・成熟度の進捗度合いを判断する。
	国際的な民間メジャー規格での採用実績	利用可能性及び国際的な認知度・成熟度・仲間作りの進捗度合いを判断する。
	民間の特定団体規格での採用実績	民間での必要性を判断する。
利用促進が図られると期待される根拠	利用促進を図る際の障壁の除去	既存アルゴリズムと比較して、利用促進を図る際の障壁を除去できるかを判断する。
	標準化・規格化の促進を図るハードルの低さ	標準化・規格化済みアルゴリズムに対する、標準化・規格化を促進するうえでのアピールポイントの有効度を評価する。
	実装コスト低減を図るハードルの低さ	新たな暗号を追加で実装する際の実装コストを低減するうえでのアピールポイントの有効度を判断する。
	調達コスト低減を図るハードルの低さ	新たな暗号が追加された製品やシステムを調達する際の調達コストを低減するうえでのアピールポイントの有効度を判断する。

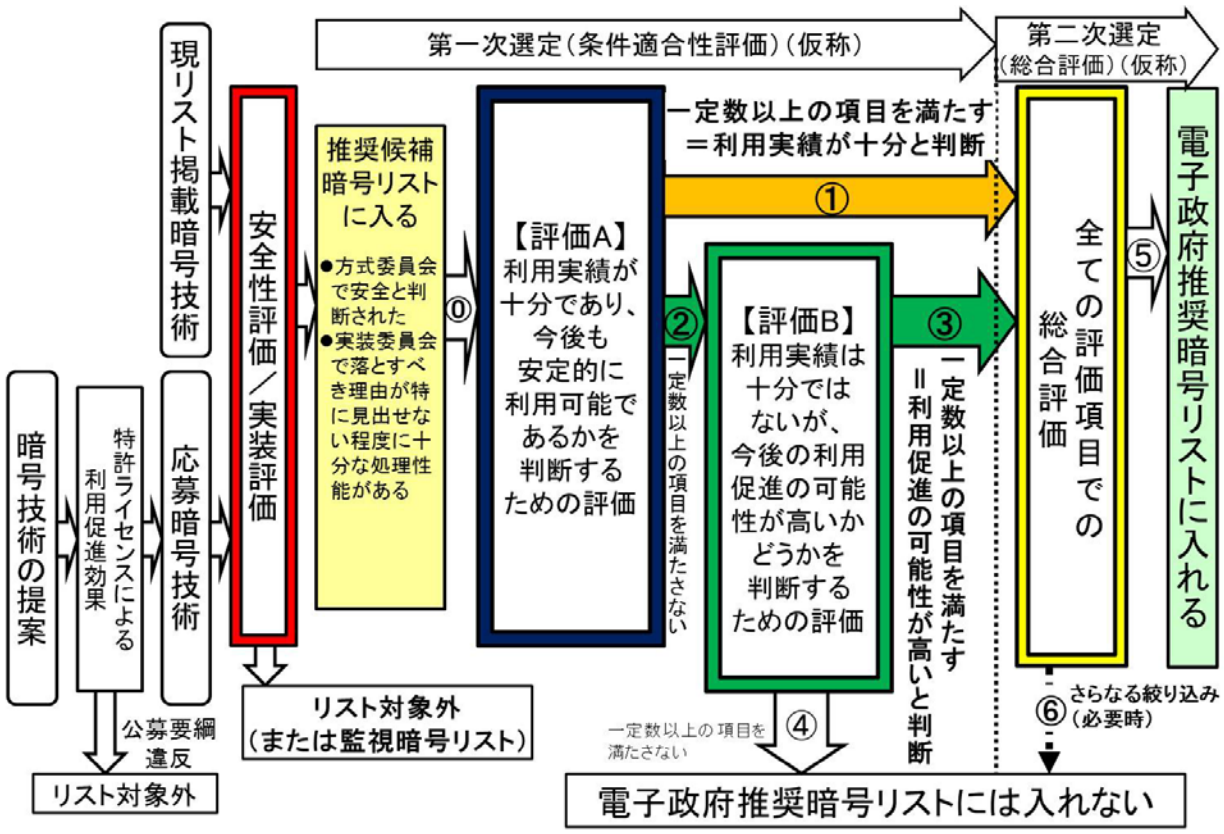
７．２．３　次期推奨暗号リストに掲載する暗号技術の選定ルールの考え方

7.2.2 で選定した全 17 個の評価項目における評価結果をもとに、次期推奨暗号リストに掲載する暗号技術を選定することになる。そこで、7.2.1 で示した観点(i)及び観点(ii)の考え方に沿い、次期推奨暗号リストに掲載する暗号技術を以下の考え方により選定するフレームワーク（案）を検討した（図 7.4)。

その際、次期推奨暗号リストが頻繁に更新されるような選定ルールであると政府調達の場面で混乱が生じる懸念があるため、ある程度の期間は固定して安定的に利用できることを想定する必要がある。また、2012 年度の改訂では次期推奨暗号リストに掲載されなかった暗号技術や今後新規に開発される暗号技術が、次々回以降の改訂において電子政府推奨暗号リストを目指す場合にどのような普及活動を行っておくべきかの指針を与えることにも留意した。

- 観点(i)により選定される可能性がある暗号技術は、評価 A において「現在の利用実績が十分である」と判断されたものである（選定ルート①を通るもの)。
- 観点(ii)により選定される可能性がある暗号技術は、評価 B により「現在の利用実績は十分とは言えないが、今後の利用促進の可能性が高い」と判断されたものである（選定ルート②③を通るもの)。

図 7.4　選定ルールのフレームワーク（案）



このフレームワーク（案）では、評価 A にて、「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」を行うための評価項目について各々設定された選考基準を満たしているかを判断し、一定数以上の評価項目が基準を満たしていれば「現在の利用実績が十分である」と判断する。評価 B でも、「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」を行うための評価項目について同様の考え方を行い、評価 B における評価項目のうち一定数以上の項目が基準を満たしていれば「今後の利用促進の可能性が高い」と判断する。詳細については、7.2.4 を参照されたい。

なお、各評価項目に設定する選考基準を決めるにあたっての基本的な考え方としては、第一次選定（条件適合性評価）（仮称）段階（評価 A 及び評価 B）において出来る限り次期推奨暗号リストに掲載される暗号技術の個数を絞り込むこととし、そのための明示的な基準を“選考基準”として設定する。その意図は以下のとおりである。

- 次期推奨暗号リストへの不選定の理由が明確に説明できるようにする。
- 調査方法や調査対象の選定の仕方によって、評価結果における精度上の問題がある程度含まれることは織り込んでおく。
- 評価結果における精度上の問題がある程度含まれていても、次期推奨暗号リストへの選定・不選定が極力変わらないような選考基準とする。
- 総合評価は、「選定ルート①で第一次選定を通過した暗号技術」と「選定ルート②③で第一次選定を通過した暗号技術」との間で、現状の利用実績の評価差をある程度緩和することが本来の趣旨であり、絞り込み評価として利用することは極力避ける。
- 本来の選定意図とは異なる暗号技術が第一次選定を通過するような緩い選考基準は極力避ける。

第二次選定（総合評価）においては、各評価項目に決められた加点基準をもとに総合評価を行うことする。その際、「選定ルート①で第一次選定を通過した暗号技術」と「選定ルート②③で第一次選定を通過した暗号技術」との間で現状の利用実績の評価差をある程度緩和するために、「利用促進が図られると期待される根拠」に該当する 4 つの評価項目については「選定ルート②③で第一次選定を通過した暗号技術」に対してのみ加点対象とする。詳細については、７．２．５を参照されたい。

７．２．４　第一次選定（条件適合性評価）（仮称）における選考基準案の考え方（案）

【評価 A について】

評価 A で用いる「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」を行うための評価項目の対象としては、表 7.3 における「現状での利用実績」における 9 項目が該当する。これらについて、評価 A での選考基準に採用するか否か、採用するとすればどのような選考基準案とすべきかについて検討を行った。

検討の結果、9 項目中 4 項目について評価 A での選考基準として採用することとし、合わせて選考基準の基本的な考え方を取りまとめた（表 7.5）。これにより、表 7.5 に示す 4 つの評価項目について設定された選考基準を満たしているかを判断し、一定数以上の評価項目が基準を満たしていれば「現在の利用実績が十分である」と判断する。

なお、基本的な考え方における意図は以下のとおりである。

- 十分な利用実績があると判断する以上は「一定数以上の採用実績」は必要である。
- コスト低減の観点からは、提案会社・グループ会社以外の企業を含めた、複数企業から調達できるようにすべきである。
- オープンソースプロジェクトで採用された暗号技術が実際の製品やシステムに組み込まれて使われるのは「正式版（リリース版）」である。
- 規格化については、最終承認待ちまで来ればいずれ規格化されるが、それ以前の状態では規格化されないまま終わる可能性がある。

表 7.5　評価 A での評価項目及び選考基準の基本的な考え方（案）

評価項目	選考基準の基本的な考え方
市販製品での採用実績 （販売会社数・種類・種別）	一定数以上の採用実績があることに加え、提案会社・グループ会社以外での採用実績もある。
オープンソースプロジェクトでの採用実績	一定数以上のプロジェクトでの採用実績がある。 ※正式版（リリース版）に採用済みのものだけを取り上げる。
政府系システム規格での採用実績	一定数以上の政府系システム規格での採用実績がある。 ※規格化への採用が合意された段階のものまで含める（最終承認待ち）。
国際的な民間メジャー規格での採用実績	一定数以上の国際的な民間メジャー規格での採用実績がある。 ※規格化への採用が合意された段階のものまで含める（最終承認待ち）。

また、評価 A での選考基準に採用しなかった 5 項目については、採用しなかった理由を表 7.6 に記す。

表 7.6　評価 A での選考基準に採用しなかった理由

評価項目	採用しなかった理由
政府系システムでの採用実績	「政府系システム規格」での採用実績により評価を行えばよい。
特許ライセンスによる利用促進効果	公募要綱との関係から、特許ライセンス条件について厳しい条件を課すことは適当ではない。
オープンソース公開による利用促進効果	製品またはプロジェクトとしてのサポートがなく、利用促進効果が明確ではない。
国際標準規格での採用実績	国際標準規格に採用されただけでは実質的な利用促進効果が大きくない（現時点では影響力がある支配的な規格とはいえない）。
民間の特定団体規格での採用実績	得られる情報の精度に幅があり、適切な評価が困難である。

【評価 B について】

評価 B で用いる「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」を行うために、評価 A で用いた評価項目 4 つに加え、表 7.5 に示す「利用促進が図られると期待される根拠」の 4 つの評価項目を追加する。つまり、評価 B においては、8 つの評価項目のうち一定数以上の項目が基準を満たしていれば「今後の利用促進の可能性が高い」と判断する。

評価 B における選考基準の基本的考え方は表 7.7 に示すとおりであり、基本的な考え方における意図は以下のとおりである。

- 利用促進として様々な後押しを図るのであれば特許ライセンス条件による制約は極力除去すべきである。
- 技術的アピールポイントを認める項目が一つもないと採用実績があるものしか選考基準を満たすことができず、新規に開発した暗号技術ほど不利な状況に置かれるので、何らかの対策が必要である。
- 利用実績が全くなく、普及に向けた活動や条件が整っていないものは今後も利用促進の可能性が高くないと考えられるため、そのことを判断するための基準として「一定数の採用実績」は必要。ただし、評価 A での「一定数」の基準よりも低めの基準とすることで、評価 A と評価 B での採用実績等の差を考慮する。

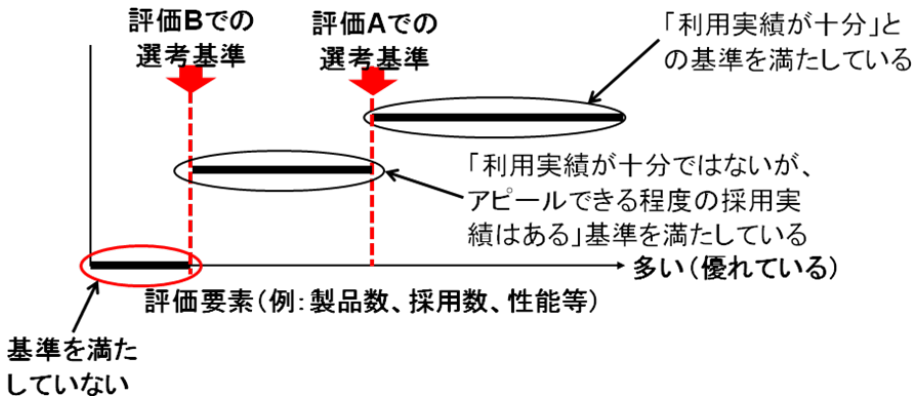


表 7.7 評価 B での評価項目及び選考基準の基本的な考え方（案）

<table>
<tr><td colspan="4">評価 A（「市販製品での採用実績　（販売会社数・種類・種別）」「オープンソースプロジェクトでの採用実績」「政府系システム規格での採用実績」「国際的な民間メジャー規格での採用実績」）に加えて</td></tr>
<tr><td colspan="3">評価項目</td><td>選考基準の基本的な考え方</td></tr>
<tr><td colspan="3">利用促進を図る際の障壁の除去</td><td>非差別的条件での特許無償許諾を実施。
（許諾契約締結が条件であってもよい）</td></tr>
<tr><td rowspan="3">標準化・規格化の促進を図るハードルの低さ</td><td rowspan="3">ＯＲ条件</td><td>技術的アピールポイント</td><td>市場が認める程度の技術的アドバンテージがある。</td></tr>
<tr><td>標準化等のアピールポイント</td><td>他の一定数以上の標準化・規格化に採用されている。</td></tr>
<tr><td>採用実績のアピールポイント</td><td>一定数以上の利用実績や製品・オープンソースプロジェクトでの採用実績がある。</td></tr>
<tr><td rowspan="2">実装コスト低減を図るハードルの低さ</td><td rowspan="2">ＯＲ条件</td><td>採用実績のアピールポイント</td><td>一定数以上の OS や暗号モジュールでの採用実績がある。</td></tr>
<tr><td>オープンソースのアピールポイント</td><td>一定数以上の暗号モジュールとして使えるオープンソースプロジェクトでの採用実績がある。</td></tr>
<tr><td>調達コスト低減を図るハードルの低さ</td><td colspan="2">採用実績のアピールポイント</td><td>一定数以上の利用実績や製品・オープンソースプロジェクトでの採用実績がある。</td></tr>
</table>

７．２．５　第二次選定（総合評価）（仮称）における基本的な考え方（案）

第二次選定（総合評価）においては、表 7.3 に示す各評価項目に決められた加点基準をもとに総合評価を行うことする。その際、「選定ルート①で第一次選定を通過した暗号技術」と「選定ルート②③で第一次選定を通過した暗号技術」との間で現状の利用実績の評価差をある程度緩和するために、「利用促進が図られると期待される根拠」に該当する 4 つの評価項目については「選定ルート②③で第一次選定を通過した暗号技術」に対してのみ加点対象とする。

総合評価の加点基準の基本的な考え方は、評価項目ごとに評価要素（例：製品数、採用数、性能等）の優劣によって 1 段階から数段階の配点を割り当て、最終的にはそれらの配点の合計点により総合評価を行うことを想定している。その際、製品やシステム、規格等の重要性等による重みづけを考慮する。表 7.8 に総合評価の基本的な考え方をまとめる。

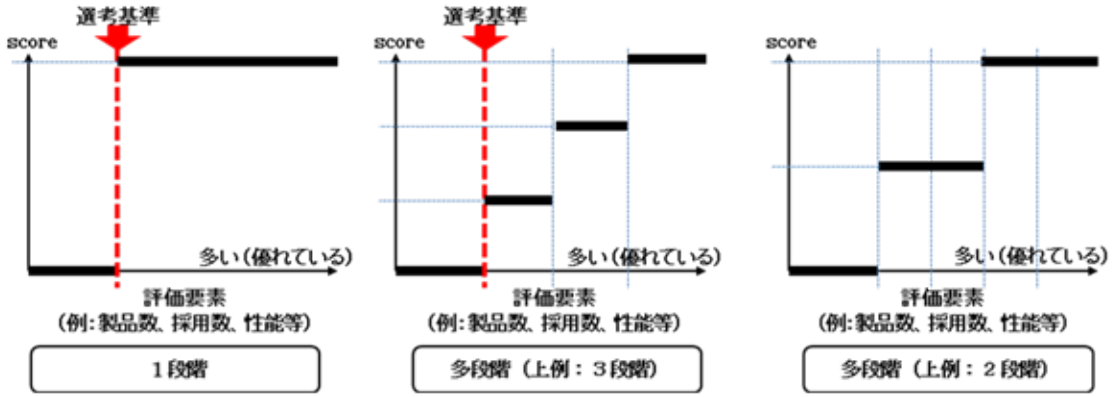


表 7.8　総合評価の基本的な考え方（案）

評価項目		加点基準	重みづけ	ルート①で通過	ルート②③で通過
技術的側面	安全性についての仕様上のアドバンテージ	暗号方式委員会に見解を求める。		○	○
	論文数の多寡によるアドバンテージ	暗号方式委員会に見解を求める。		○	○
	ソフトウェア実装性能評価	暗号実装委員会に見解を求める。		○	○
	ハードウェア実装性能評価	暗号実装委員会に見解を求める。		○	○
現状での利用実績	政府系システムでの採用実績	採用実績による２～３段階の点数をつける。	システムの違いによる重みづけを考慮する。	○	○
	市販製品での採用実績	採用実績による２～３段階の点数をつける。	製品の重要度やシェアによる重みづけを考慮する。	○	○
	オープンソースプロジェクトでの採用実績	採用実績による２～３段階の点数をつける。	プロジェクトの重要度や信頼度による重みづけを考慮する。	○	○
	特許ライセンスによる利用促進効果	ライセンス条件による２段階の点数をつける。 ● 許諾契約なしの特許無償または特許なし ● 許諾契約ありの特許無償		○	○
	オープンソース公開による利用促進効果	１段階 ● 一定の性能を持ったオープンソースをオープンソースプロジェクトに提案しているものだけを対象		○	○
	政府系システム規格での採用実績	採用実績による２～３段階の点数をつける。	規格の違いによる重みづけを考慮する。	○	○
	国際標準規格での採用実績	１段階 ● 対象となる規格が少ないと考えられるため		○	○

	国際的な民間メジャー規格での採用実績	採用実績による２～３段階の点数をつける。	規格の違いによる重みづけを考慮する。	○	○
	民間の特定団体規格での採用実績	採用実績による２～３段階の点数をつける。	規格の違いによる重みづけを考慮する。	○	○
利用促進が図られると期待される根拠	利用促進を図る際の障壁の除去	ライセンス条件による２段階の点数をつける。 ● 許諾契約なしの特許無償または特許なし ● 許諾契約ありの特許無償		－	○
	標準化・規格化の促進を図るハードルの低さ	アピールポイントによる２～５段階の点数をつける。		－	○
	実装コスト低減を図るハードルの低さ	アピールポイントによる２～５段階の点数をつける。		－	○
	調達コスト低減を図るハードルの低さ	アピールポイントによる２～５段階の点数をつける。		－	○

凡例：　○：加点対象　　－：加点対象としない

７．２．６　利用実績調査の基本的考え方

2012 年度には、評価 A 及び評価 B での利用実績評価の基礎データとなる利用実績調査を実施する予定としている。利用実績調査の基本的考え方は、2009 年度に経済産業省が実施した利用実績調査とほぼ同様の手法を踏襲するものとする。具体的には以下のとおり。

（手法）

以下の情報源から利用している暗号技術を調査し、現状での利用実績とみなす。

- 応募暗号及び現リスト掲載暗号の応募者からの情報提供
- 暗号技術を搭載している市販製品の販売会社へのアンケート
  - 例１：2009 年度の利用実績調査の際にアンケート票を送付した企業
  - 例２：市場調査報告書等において売上高調査に協力している企業
- 政府機関へのアンケート
- インターネット上で公開されている情報
  - 例１：オープンソースプロジェクト
  - 例２：国際的な民間メジャー規格

（想定調査対象数）

2012 年 6 月 30 日時点までで、発売または公開中で入手可能、もしくは新製品としての発売がアナウンスされているもの。

- 市販製品： 2009 年度の利用実績調査時をやや上回る調査数
- 政府機関： 10～20 程度
- （政府機関を除く）規格等：
  - ✧ 国際標準規格（ISO/IEC, ITU, ICAO）
  - ✧ 国際的な民間メジャー規格（IETF, IEEE, EMVCo, OMA（携帯電話））
- 民間の特定団体規格（CAS, DRM, ETC, DNLA, …）：当該規格を管理するコンソーシアム（10～20 程度）
- オープンソースプロジェクト（OpenSSL, Mozilla, Linux, FreeBSD, OpenJava, Android, …）：信頼度の高いプロジェクトから 20 程度

（注意）

非公開製品・非公開システム・非公開規格での採用実績などについて、用意できるどのような手段を用いても確認できないものは実績として考慮しない。

７．２．７　特許ライセンスの取り扱い

上記で示したように、特許ライセンス条件の取り扱いについて、応募時点での公募要綱に書かれた条件とは少なからず異なる状況が発生している。そのため、本報告書及び CRYPTREC シンポジウム 2012 等で特許ライセンスの取り扱いについて説明した後、必要があれば応募者が特許ライセンスの宣誓を変更できるようにすべきである。

そこで、暗号運用委員会としては、2012 年 9 月 30 日時点の特許ライセンス宣誓により評価を実施することとし、2012 年 9 月 30 日までは特許ライセンス宣誓の変更を認めることが妥当と判断した。

７．２．８　電子政府推奨暗号の利用促進体制の検討

次期電子政府推奨暗号リストに掲載する国産暗号を絞り込んだとしても本当に使われるようになるのかという課題がある。

そのため、本年度の暗号運用委員会では、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する目的を達成するために、次期電子政府推奨暗号、とりわけ国産暗号の利用促進が図られるような取り組みを検討するにあたって考慮すべき観点と論点の洗い出しを行った。次年度、論点の検討を進めていくこととした。

(1) 将来的な目標として、現在の米国政府標準暗号と同じように、標準化や製品化での主導権を日本が取れるようにしていくためのロードマップを描くべきである。

論点：主導権をとるといった場合、いつ頃（達成時期）までにどのような状態を達成すべきゴールとして目指すべきかについて明らかにする必要がある。

(2) 実際問題として、暗号のバンドル先である IT 製品が米国主導で作られている以上、市場原理で国産暗号が普及していくのを期待することは難しい。

論点：調達コストに大きく跳ね返らないレベルで、十分な制約をかけて国産暗号を使わせる土壌を少しずつ作っていく方策について検討する必要がある。

論点：米国政府標準暗号といえども米国内の主要ベンダの支持が得られず全く普及しなかったものもあることを考慮すれば、日本で決定したことに対して主要ベンダの支持が得られるようにするための方策について検討する必要がある。

(3) 日本の技術力は高いが、標準化・規格化への提案の仕方に統一性が見られないので、技術力とは関係ない部分で存在感を示せていない。

論点：標準化を手掛けると専門的に人を長期間張り付ける必要があり、企業負担が大きいなか、今後の標準化・規格化への活動主体として誰が何を担うべきかについて検討する必要がある。

７．２．９　その他の検討事項

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や遷移要件に関する基準については、次期推奨暗号リストの選定後になって初めて利用されることから、次年度以降、次期推奨暗号リストの選定基準が完全に決定してから検討を開始することとした。

７．３．今後の予定

本年度の暗号運用委員会で検討した次期推奨暗号リストに掲載する暗号技術の選定ルール（案）についてさらに精緻化し、具体的な選考基準値案を 2012 年度上期に確定するとともに、利用実績調査を実施し、2012 年度末の次期推奨暗号リストの策定につなげていく。

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の調査・検討を 2012 年度下期に行う。さらに、引き続き、国産暗号の利用促進が図られるような取組や、次期 CRYPTREC 暗号リスト（仮称）策定に伴う暗号学界への影響と対策等について検討する。

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、2012 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組

(a) 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、応募暗号技術及び現リストに掲載された暗号技術に関する安全性の評価を行う。

(b) 暗号技術の実装性評価

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。

(c) 電子政府推奨暗号の選定基準の検討

次期推奨暗号リストに掲載する暗号技術の選定ルールに基づき、未確定となっている評価基準案の精緻化及び具体的な選定基準値を決定する。

(d) 利用実績の調査

新規応募暗号及び現リスト掲載暗号に対して、次期推奨暗号リストに掲載する暗号技術を選定する際の評価項目である現状の利用実績についての調査を実施する。

(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。

(4) 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。

(5) 電子政府推奨暗号の利用促進体制の検討

電子政府推奨暗号リストに掲載される暗号アルゴリズムについて、費用対効果の観点を考慮しつつ、当該暗号アルゴリズムの利用が促進されるような取り組み方法について検討する。

(6) 運用監視暗号リストへの遷移要件に関する基準の検討

電子政府推奨暗号リストに掲載されている暗号アルゴリズムの安全性が暗号学会等で低下したことが判明した場合の暗号運用委員会としての対応について検討する。

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。

別添２

2011 年度　暗号技術検討会　構成員・オブザーバ名簿（平成 24 年 3 月 8 日現在）

（構成員）

◎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
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 岡本特別研究室　室長（社団法人電気通信事業者協会代表兼務）
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	一般財団法人ニューメディア開発協会　顧問・首席研究員
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	一般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
近澤　　武	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 グループリーダー（ISO/IEC JTC 1/SC 27/WG 2 Convenor（国際主査））
○辻井　重男	中央大学　研究開発機構　教授
中山　靖司	日本銀行　金融研究所情報技術研究センター　企画役
本間　尚文	東北大学大学院　情報科学研究科　准教授
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
松尾　真一郎	独立行政法人情報通信研究機構　ネットワークセキュリティ研究所 セキュリティアーキテクチャ研究室　室長 （ISO/IEC JTC1 SC27/WG2 （国内小委員会主査））
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研究所基盤技術ディビジョン 認証基盤グループグループリーダ
持麾　裕之	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

◎：座長、○：顧問

（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
岡本　克己	警察庁情報通信局情報管理課長
栗原　利男	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
濱島　秀夫	総務省自治行政局地域政策課地域情報政策室長
高原　　剛	総務省自治行政局住民制度課長
河合　芳光	法務省民事局商事課長
三澤　　康	外務省大臣官房情報通信課長
橋本　真吾	財務省大臣官房文書課業務企画室長
田中　正幸	文部科学省大臣官房政策課情報化推進室長
川上　一郎	厚生労働省大臣官房統計情報部企画課情報企画室長
藤原　達也	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ネットワークセキュリティ研究所長
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
笹岡　賢二郎	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	一般財団法人日本情報経済社会推進協会電子署名・認証センター長
鈴田　　信	公益財団法人金融情報システムセンター監査安全部長