# 暗号技術検討会

# ２００８年度報告書

暗号技術検討会

２００９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、解読技術の進展に注意を払い、適切なものを使用するよう注意を払う必要もある。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 証明書を発行可能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。このため、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。

政府においても、2008 年 4 月の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」が決定されるなど、大きな動きが見られた。また、電子署名法で利用する暗号アルゴリズムについて、SHA-2 を追加する告示改正作業が行われているところである。CRYPTREC ではこれまで、SHA-1 や RSA1024 の安全性についての見解や報告を行ってきており、今回、これらの動きにその内容が反映されたことは、CRYPTREC の活動の成果と言える。

暗号アルゴリズム移行問題に加え、今年度は、「電子政府推奨暗号リスト」の改訂に向けても取組が行われている。電子政府推奨暗号リスト改訂については、「第 2 次情報セキュリティ基本計画（2009 年 2 月情報セキュリティ政策会議決定)」において、「電子政府の安全性及び信頼性を確保するため、電子政府で使われている推奨暗号について、その安全性を継続的に監視・調査するとともに、技術動向及び国際的な取組みを踏まえ、現行の「電子政府推奨暗号リスト」の 2013 年度改訂に向けて、関係機関において所要の作業を進める」こととされていることを踏まえ、リスト改訂のための暗号技術公募要項の策定、リスト改訂に関する広報イベント「CRYPTREC シンポジウム 2009～電子政府推奨暗号リスト改訂に向けて～」の開催など、リスト改訂に向けて着実に作業を進めてきているところである。

委員会別の活動状況を見てみると、暗号技術監視委員会では、電子政府推奨暗号に関する暗号技術の監視・調査等の活動、電子政府推奨暗号リストの利用指針及び電子政府システムの構築に必要な技術等を示すリストガイドの作成に加えて、ID ベース暗号の技術動向の調査を行った。また、暗号モジュール委員会では、北米の FIPS や国際標準機関である ISO/IEC に関する暗号モジュールのセキュリティ要件及び試験要件の調査や、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公募要件を作成した。

2008 年度の活動のうち、詳細な技術的事項については、暗号技術監視委員会及び暗号モジュール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ている「CRYPTREC Report 2008」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。

2009 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、構成員及び開催状況

### 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。高度情報通信ネットワーク社会形成基本法に基づく e-Japan 重点計画-2004（2004 年 6 月 15 日　IT 戦略本部決定）では、特に、電子政府や電子自治体、重要インフラ等の公共的分野のサービスについては、国民の社会経済活動に大きな影響を及ぼすことのないよう、情報セキュリティ対策の一層の充実を図ることを目標としており、政府は情報セキュリティに関する諸施策を実施している。また、平成 17 年 4 月に、情報セキュリティ対策の統一的・横断的な総合調整を強化することを目的とした「内閣官房情報セキュリティセンター」が設置され、同年 5 月には、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」が IT 戦略本部内に設置され、セキュリティ政策の強化が図られている。

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。

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）による暗号技術評価プロジェクトを指す（CRYPTREC の体制図は図 2.1 参照）。暗号技術検討会、暗号技術監視委員会及び暗号モジュール委員会は以下のように検討等を進めた。

### 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・検討及び暗号モジュールセキュリティ要件及び試験要件の作成等について、総合的な観点から検討を行った。

検討会は総務省大臣官房総括審議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、内閣官房、警察庁、法務省、外務省、財務省、防衛省等がオブザーバとして参加した。

### ２．２．２．暗号技術監視委員会

暗号技術監視委員会（以下、「監視委員会」）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。なお、監視委員会の日常業務を行う監視要員を NICT 及び IPA に配置した。また、具体的な調査・検討に際して監視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。

監視委員会は NICT 及び IPA の委員会として開催し、総務省、経済産業省のほか、警察庁、外務省、防衛省等がオブザーバとして参加した。

### ２．２．３．暗号モジュール委員会

暗号モジュール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、将来的に政府調達基準等として利用されることをも視野に入れながら、電子政府推奨暗号に準拠した暗号モジュール製品に対する暗号モジュールセキュリティ要件及び試験要件の策定に向けた検討、電子政府推奨暗号リスト改訂に必要なハードウェア及びソフトウェア実装性評価の公募要件の検討を行った。また、上記セキュリティ要件及び試験要件の検討に資するため、暗号モジュールへの非破壊攻撃及び破壊攻撃に対する調査・研究を行った。

暗号モジュール委員会は NICT 及び IPA の委員会として開催し、総務省、経済産業省のほか、警察庁、外務省、防衛省等がオブザーバとして参加した。

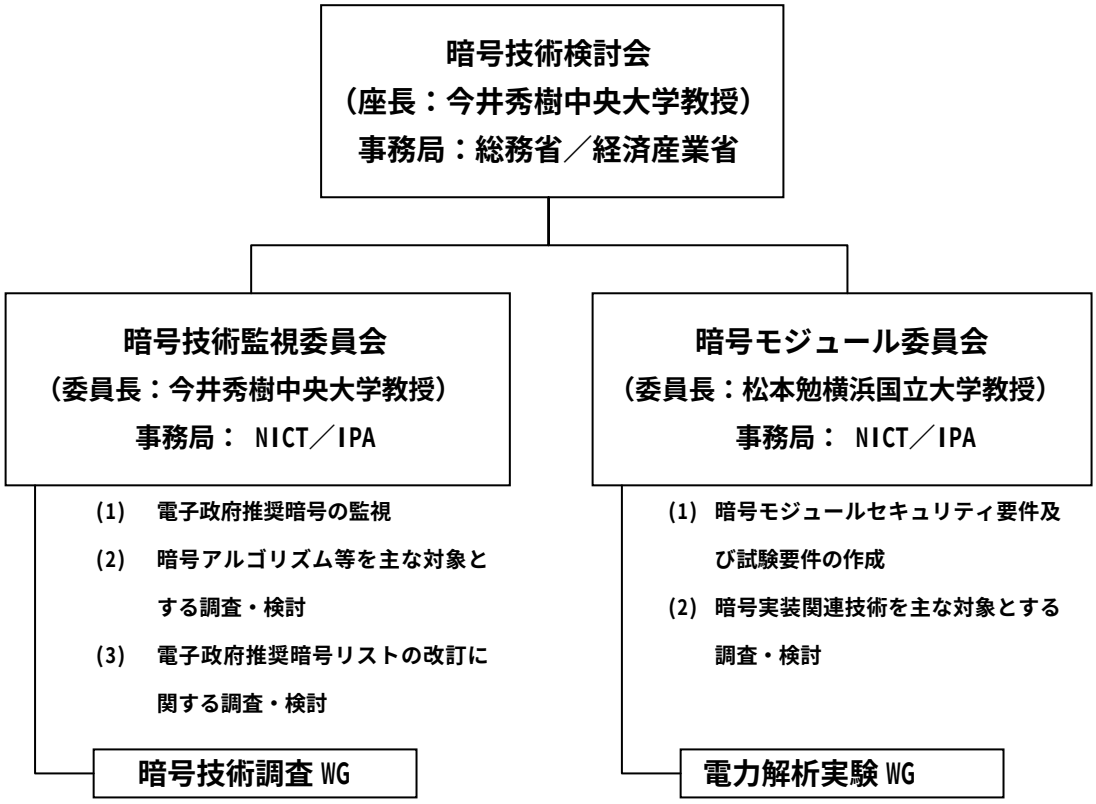


**図 2.1　2008 年度 CRYPTREC の体制図**

## ２．３．暗号技術検討会メンバー

（構成員）※肩書は 2009 年 3 月末現在（途中交代者は交代時）。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 | 情報セキュリティ大学院大学学長 |
| | 岩下　直行 | 日本銀行金融研究所情報技術研究センター長 |
| | 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<br>主席研究員（(社）電気通信事業者協会代表兼務） |
| | 加藤　義文 | （社）テレコムサービス協会技術委員会委員長 |
| | 金子　敏信 | 東京理科大学理工学部電気電子情報工学科教授 |
| | 国分　明男 | （財）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 |
| | 宝木　和夫 | （社）電子情報技術産業協会情報セキュリティ委員会委員 |
| | 武市　博明 | 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<br>（次世代電子商取引推進協議会<br>電子署名認証サブワーキンググループリーダ） |

（オブザーバ）

| | |
|---|---|
| 伊藤　毅志 | 内閣官房情報セキュリティセンター内閣参事官 |
| 高橋　浩二 | 警察庁情報通信局情報管理課長 |
| 中井川　禎彦 | 総務省行政管理局行政情報システム企画課管理官<br>（2008 年 11 月まで） |
| 橋本　敏 | 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<br>（2008 年 11 月から） |
| 塚田　桂祐 | 総務省自治行政局地域政策課参事官（2008 年 11 月まで） |
| 井上　知義 | 総務省自治行政局地域政策課地域情報政策室長（2008 年 11 月から） |
| 新井　孝雄 | 総務省情報流通行政局情報流通振興課情報セキュリティ対策室長<br>（2009 年 3 月から） |
| 相澤　哲 | 法務省民事局商事課長（2009 年 1 月まで） |
| 江原　健志 | 法務省民事局商事課長（2009 年 1 月から） |
| 菊田　豊 | 外務省大臣官房情報通信課長 |
| 児玉　清隆 | 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 |
| 山田　一彦 | 厚生労働省大臣官房統計情報部企画課情報企画室長補佐 |
| 和泉　章 | 経済産業省産業技術環境局基準認証政策課情報電気標準化推進室長（2008 年 11 月まで） |
| 井上　幹邦 | 経済産業省産業技術環境局基準認証政策課情報電気標準化推進室長（2008 年 11 月から） |
| 武田　仁己 | 防衛省運用企画局情報通信・研究課情報保証室長 |
| 篠田　陽一 | （独）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 |
| 大蒔　和仁 | （独）産業技術総合研究所研究コーディネータ（情報通信・エレクトロニクス担当）（2008 年 11 月まで） |
| 大塚　玲 | （独）産業技術総合研究所情報セキュリティ研究センター セキュリティ基盤技術研究チーム長（2008 年 11 月から） |
| 山田　安秀 | （独）情報処理推進機構セキュリティセンター長 |
| 亀田　繁 | （財）日本情報処理開発協会電子署名・認証センター長 |
| 岸本　博之 | （財）金融情報システムセンター監査安全部長 |

## ２．４．暗号技術検討会開催状況

2008 年度、検討会は計 3 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】2008 年 7 月 4 日（金）

（主な議題）・CRYPTREC の 運営方針及び活動計画
・暗号技術検討会活動計画
・暗号技術監視委員会活動報告計画
・暗号モジュール委員会活動計画

【第 2 回】2008 年 11 月 7 日（金）

（主な議題）・暗号モジュール委員会中間報告
・暗号技術監視委員会中間報告
・「電子政府推奨暗号リストの改訂のための暗号技術公募要項（2009 年度）（案）」について

【メール審議】2009 年 2 月 4 日(水)～10 日(火)

（議　　題）・「電子政府推奨暗号リストの改訂のための暗号技術公募要項（2009 年度）（案）」について

【第 3 回】2009 年 3 月 27 日（金）

（主な議題）・電子政府推奨暗号リストの改訂に向けた活動について
・暗号技術監視委員会活動報告
・暗号モジュール委員会活動報告
・暗号技術検討会 2008 年度報告書
・今後の CRYPTREC 活動

## 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．電子政府推奨暗号リストの改訂に関する骨子

以上の考え方のもと、CRYPTREC では「電子政府推奨暗号リストの改訂に関する骨子（案）」（以下、骨子案という。）を作成し、総務省及び経済産業省において、2008 年 8 月 6 日から 9 月 5 日にかけてパブリックコメント[1]を行った。その結果[2]、全部で個人・企業

[1] http://search.e-gov.go.jp/servlet/Public?CLASSNAME=Pcm1010&BID=145207347
[2] http://search.e-gov.go.jp/servlet/Public?ANKEN_TYPE=3&CLASSNAME=Pcm1090&KID=145207347

から合計 7 件の意見があった。以下に、骨子案の内容について報告する。

### ３．３．１．現リストの構成の見直し

現時点で CRYPTREC が公開している暗号リストは現行の電子政府推奨暗号リストのみであるが、今回の見直しに合わせて、下記の（１）～（３）の各リスト及び（４）リストガイドをまとめて「CRYPTREC 暗号リスト（仮称）」（以下、「次期リスト」）として公開する。

（１）電子政府推奨暗号リスト（仮称）
（２）推奨暗号候補リスト（仮称）
（３）互換性維持暗号リスト（仮称）
（４）リストガイド

CRYPTREC により安全性が確認された暗号技術は、（１）～（３）の 3 つのリストのいずれかに登録される。各リストへの登録は、WTO 政府調達協定との整合性に配慮しつつ、安全性や市場動向により決定される。登録の見直しは一定の間隔で行う。

現リストに掲載されている暗号技術については、安全性の再評価を行った上で 2013 年の次期リスト運用開始前に推奨暗号候補リスト（仮称）へ登録されていたものとして扱う。2013 年の次期リスト運用開始時には、新たに応募された技術と共に製品化の状況・技術の利用状況により電子政府推奨暗号リスト（仮称）へ登録するかの決定を行う。

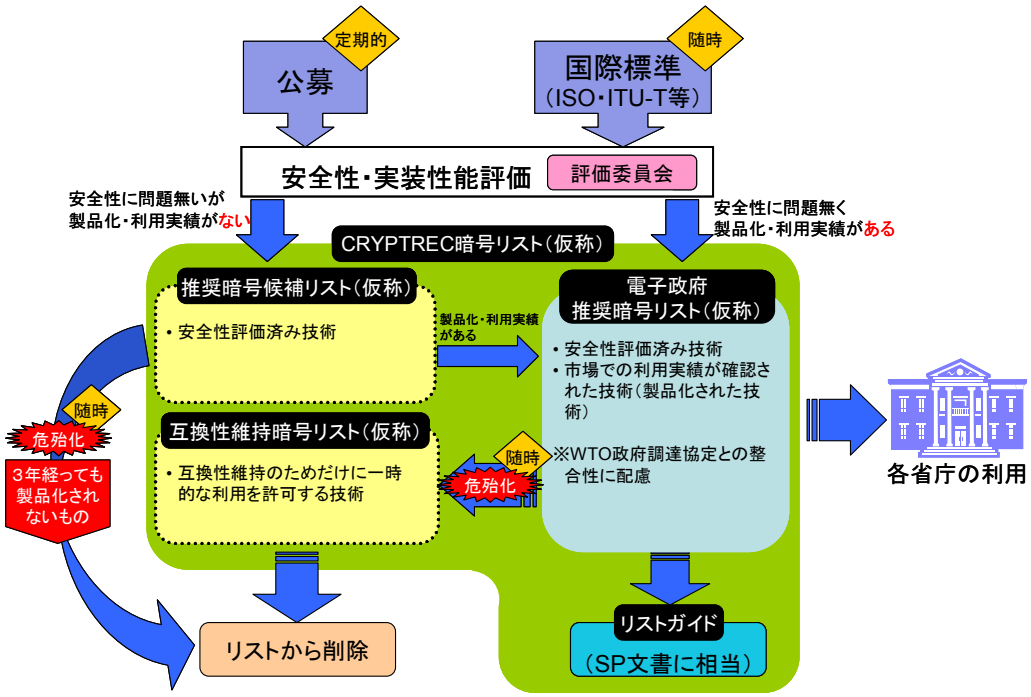


図 3.1 リスト改訂概念図

次期リストにおける各（部分）リストの役割は以下の通りである。

（１）電子政府推奨暗号リスト（仮称）

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技術リスト。電子政府構築（政府調達）の際には当該技術を推奨する（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しい。電子政府推奨暗号リスト（仮称）に登録されるカテゴリ別の暗号数はいたずらに多くならないことを基本とする。

（２）推奨暗号候補リスト（仮称）

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）の際には当該技術を調達しても良い。

一定期間ごとに普及の度合いの調査を行い、利用実績が十分であると認められれば電子政府推奨暗号リスト（仮称）に登録される。また、利用実績が十分であると認められなかった場合にはここから削除される。そして、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暗号技術は随時削除される。

（３）互換性維持暗号リスト（仮称）

電子政府推奨暗号リスト（仮称）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 として新規調達を推奨しない。

（４）リストガイド

電子政府で利用されている、あるいは利用する可能性のある技術について、その技術概要と、推奨する利用方法を記述する。また、次期リストに記載された技術の中で、安全性を維持するため正しいパラメータの設定が要求される技術における具体的なパラメータ設定方法の記述を行う。さらに、将来必要になると予想されるセキュリティ技術については、その開発状況や利用可能性について記載する。リストガイドは、システム運用者や設計者の利用や、システム利用者への啓発を目的とする。

### ３．３．２．暗号技術公募の基本方針

原則として、一定期間ごとにリストを見直し、必要があれば公募を行う。公募を行う際の基本方針は以下の通りである。

（１）公募対象のカテゴリは、下記の（1a）～（1c）のいずれかの条件を満たすものとする。

(1a) 現リストに含まれていないが、電子政府システムの構築において安全性及び実装性の高い技術仕様の推奨が必要とされている暗号技術カテゴリであること。

(1b) 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。

（1c）普及・標準化が見込まれる暗号技術カテゴリであること。

（２）応募可能な暗号技術は、下記の（2a）～（2e）のすべての条件を満たすものとする。

（2a）十分な安全性を有する暗号技術であること。ただし、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。

（2b）個別のシステムやアプリケーションの仕様に依存しない、汎用的な暗号技術であること。

（2c）当該技術を利用した製品が販売済みであるか又は、販売の予定があること。

（2d）安全性評価及び、実装性能評価に足る技術仕様が公表されていること。

（2e）暗号技術に関する基本特許については、製造、販売、使用に対して、無償（Royalty Free）又は、妥当かつ非差別的（Reasonable And Non-Discriminatory）な条件で、暗号技術の実施許諾権が与えられること。

### ３．３．３．2009 年度公募カテゴリ

2009 年度は、３．３．２．(1)（1a）に該当するものとして暗号利用モード、メッセージ認証コード及びエンティティ認証、３．３．２．(1)（1b）に該当するものとしてブロック暗号及びストリーム暗号を公募対象のカテゴリとする。

なお、現リストにおいて例示的に技術名の記載があるカテゴリである、擬似乱数生成系については、公開鍵暗号技術等で利用される要素技術であり、相互接続性に影響を与えないこと、安全性要件として満たすべき乱数検定法が示されていることから、リストガイドにて参照することが適当であると考えられる。よって、電子政府推奨暗号リスト（仮称）及び推奨暗号候補リスト（仮称）から外し、2009 年度公募カテゴリには入れないこととする。

以上のことから、次期リストの技術カテゴリは表 3.1 のとおり。

表 3.1 次期 CRYPTREC 暗号リスト（仮称）カテゴリ（現リストとの比較）

| 電子政府推奨暗号リスト（現リスト） | CRYPTREC 暗号リスト(仮称)（次期リスト） |
|---|---|
| 署名 | 署名 |
| 守秘 | 守秘 |
| 鍵共有 | 鍵共有 |
| 64 ビットブロック暗号 | ブロック暗号 |
| 128 ビットブロック暗号 | |
| ストリーム暗号 | ストリーム暗号 |
| | メッセージ認証コード |
| | 暗号利用モード |
| ハッシュ関数 | ハッシュ関数 |
| 疑似乱数生成系 | |
| | エンティティ認証 |

### ３．３．４．今後のスケジュール

2009 年度　第 3 四半期　公募書類受付開始（提出書類の審査を実施。）
2009 年度　第 4 四半期　公募〆切

2010 年度　第 1 次評価期間（主に、応募暗号技術の評価を実施。）
2011 年度　第 2 次評価期間（応募暗号技術の継続評価の他、現リストに登録されている暗号技術の再評価等も実施。）

2012 年度　第 1 四半期～第 3 四半期　次期リスト（案）の策定
2012 年度　第 4 四半期　次期リストの発表
2013 年度　第 1 四半期　次期リストの運用開始

## ３．４．電子政府推奨暗号リスト改訂のための暗号技術公募要項（2009 年度）

骨子案に対するパブリックコメントの結果を踏まえ、CRYPTREC では、「電子政府推奨暗号リスト改訂のための暗号技術公募要項（2009 年度）」（別添２参照）を策定した。以下に、電子政府推奨暗号リスト改訂のための暗号技術公募要項（2009 年度）の概要について報告する。

### ３．４．１．公募の概要

CRYPTREC は評価対象暗号技術を公募し、CRYPTREC 事務局の情報通信研究機構及び情報処理推進機構（以下、「事務局」という。）は、暗号技術評価を実施する。

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、事務局が開催するワークショップ（「３．４．７　ワークショップの開催」を参照のこと。）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、現リストに登録されている暗号技術の再評価も行う。

CRYPTREC 内に設置された「評価委員会（仮称）」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。

### ３．４．２．公募の対象

2009 年度公募の対象となる暗号技術の種別は、骨子案において公表した以下のとおり（表 3.2）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。

等を挙げている。

表 3.2 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．提出書類

今回の応募に際して必要な提出書類は以下のとおり。

（１）暗号技術応募書
（２）暗号技術仕様書
（３）自己評価書
（４）テストベクトル、テストベクトル生成ソースコード及びその仕様書、
（５）参照ソースコード及びその仕様書
（６）参照ハードウェア設計記述及びその仕様書
（７）誓約書
（８）公開の状況等に関する情報

（９）応募暗号説明会発表資料

（１０）自己チェックリスト

詳細については、「電子政府推奨暗号リスト改訂のための暗号技術公募要項（2009 年度）」（別添２）を参照のこと。

### ３．４．４．評価スケジュール（予定）

| | |
|---|---|
| 応募暗号説明会開催： | 2010 年 3 月頃 |
| 第 1 次評価実施： | 2010 年 4 月～2011 年 3 月 |
| 第 1 回ワークショップ開催： | 2011 年 2 月頃 |
| 第 2 次評価実施： | 2011 年 4 月～2012 年 3 月 |
| 第 2 回ワークショップ開催： | 2012 年 2 月頃 |
| 2012 年度シンポジウム： | 2013 年 2 月頃 |

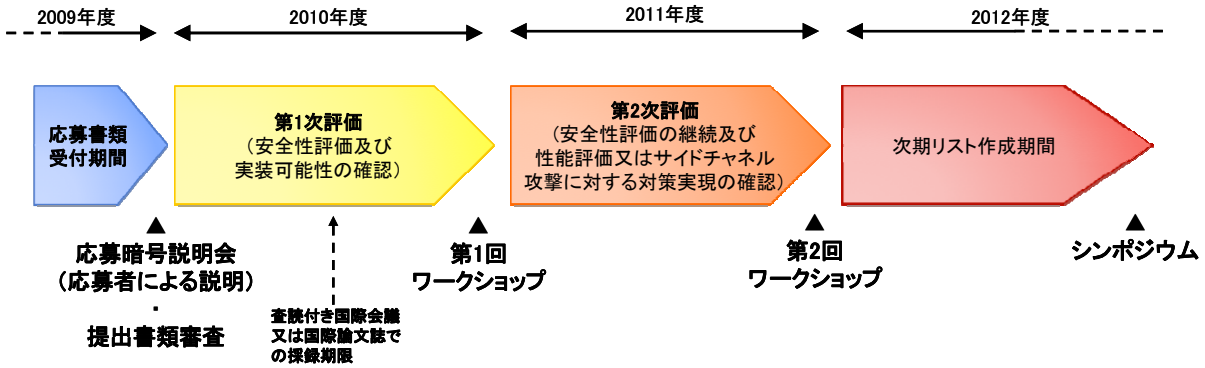


図 3.2 評価スケジュール（予定）

### ３．４．５．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[3]、ASIC[4]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

[3] FPGA：Field Programmable Gate Array
[4] ASIC：Application Specific Integrated Circuit

チャネル攻撃に対する対策実現の確認も行う。

なお、今回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るので、次年度以降に詳細を検討する必要がある。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。詳細については、「電子政府推奨暗号リスト改訂のための暗号技術公募要項（2009 年度）」（別添２）を参照のこと。

### ３．４．６．応募暗号説明会の開催

応募された暗号技術の評価を開始するにあたり、応募者自ら公の場で、応募暗号技術の技術仕様、安全性、実装性、公開状況、及びライセンス等について説明する機会を設ける予定である。正式日程などの詳細については、2009 年 10 月頃に 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。

### ３．４．７．ワークショップの開催

開催時点までの評価委員会（仮称）における最新の評価結果を公表し、それらを検討する場を設ける予定である。この機会を利用して、応募者が自らの意見を述べることもできる。

第 1 次評価実施期間（2010 年 4 月～2011 年 3 月）の後に開催予定の第 1 回ワークショップでは、応募暗号技術の安全性評価及び実現可能性の確認結果を公表する予定である。また、第 2 次評価実施期間（2011 年 4 月～2012 年 3 月）の後に開催予定の第 2 回ワークショップでは、第 1 次評価実施期間後に継続して実施された安全性評価、性能の評価及びサイドチャネル攻撃に対する対策実現の確認結果を公表する予定である。また、現リストに掲載されている暗号技術に関する再評価の結果も公表する予定である。詳細については、各年度の 10 月頃に正式日程を 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。

## ３．５．CRYPTREC シンポジウム 2009 について

2009 年度から 2012 年度にかけて実施する、電子政府推奨暗号リストの改訂の背景や目的及び、暗号技術公募とその評価等について広く一般に周知するために、シンポジウムを開催した。また、それに加えて、公募カテゴリを中心とした暗号技術の最新動向を一般に周知するため、また、今後の暗号研究の方向性についてより大局的な議論を行うために、パネルディスカッションを併設した。以下に、本シンポジウムの概要について報告する。

### ３．５．１．プログラムの概要

日時：2009 年 2 月 18 日（水）13：00～16：30

主催：NICT・IPA　共催：総務省・経済産業省

場所：虎ノ門パストラルホテル　本館 1 階　葵の間

参加人数：約 230 名

表 3.3　プログラム

| 時間 | | 目的 |
|---|---|---|
| 13:00 | 開会の挨拶 | 総務省/経済産業省 |
| 13:05 | 講演 1「電子政府推奨暗号リストについて」（今井委員長） | ・電子政府推奨暗号リストの重要性について<br>・電子政府推奨暗号リスト改訂の理由および目的について |
| 13:15 | 講演 2「リスト改訂スキームについて」（山村委員） | ・今後の電子政府推奨暗号リストの改訂スキームについての説明、特に、リスト間遷移条件を中心にスキームの詳細についての説明<br>・質疑応答によって得られた有意義な意見はスキームを最終決定する際の参考とする |
| 13:40 | 講演 3「暗号技術の公募について」CRYPTREC 事務局 | ・今回の暗号技術の公募について、公募要項を基に説明 |
| 14:00 | 休憩 | |
| 14:10 | パネル 1<br>「公募対象カテゴリを中心とした暗号技術の動向について」<br>モデレータ：高木剛(公立はこだて未来大学)<br>パネリスト：大塚玲(産業技術総合研究所)、下山武司(富士通研究所)、盛合志帆(ソニー)、吉田博隆(日立製作所) | ・公募を行うカテゴリの最新技術動向と、電子政府にとってどのようなアルゴリズムが求められるかを中心にパネルを行い、評価基準を決定する際の参考とする<br>・将来的にリストに掲載する可能性のある暗号について、パネルを行い、将来のリスト掲載の可能性について周知をしておく |
| 15:00 | 休憩 | |
| 15:15 | パネル 2<br>「日本の暗号研究と電子政府推奨暗号の今後について」<br>モデレータ：佐々木良一(東京電機大学)<br>パネリスト：岩下直行(日本銀行)、辻井重男(情報セキュリティ大学院大学)、苗村憲司(SC27/WG2 コンビーナ)、松本勉(横浜国立大学)、伊藤毅志（内閣官房情報セキュリティセンター） | ・現行の電子政府推奨暗号リストやその(2001 年当時の)選定方法について、問題点や反省点を明示する<br>・今後の電子政府推奨暗号リスト、CRYPTREC、および、日本の暗号研究の方向性についてより大局的な観点から議論を行う |
| 16:25 | 閉会の挨拶 | NICT/IPA |

### ３．５．２．本シンポジウムで寄せられた意見・コメント等

パネル 1 及びパネル 2 では、パネリスト等から、これから実施される電子政府推奨暗号リストの改訂や暗号技術公募に対する意見・コメントが寄せられた。ここではそれらの概要を記しておく。

（1） 暗号技術公募について

- 実装プラットフォームや実装方法に強く依存するサイドチャネル攻撃に対する耐性をどのように評価・比較していくのか。
- サイドチャネル攻撃に対する耐性という評価項目が挙がっているが、どこまで厳密に行うつもりなのか、応募する側にも評価する側にもコストがかかることが懸念させる。
- 暗号アルゴリズムの評価ならCall for attackというような手段もあるが、サイドチャネル攻撃の場合には、例えば、応募者が攻撃対象の実装をサンプルとして提供して、call for attackをする方法を思い付くが、この場合にはその経費をCRYPTRECが負担することになるのか？ CRYPTRECとして、サイドチャネル攻撃に対する評価方法をどのように考えているか、お聞きしたい。
- Call for attackの実施に必要な予算の確保は難しいので、今回のリスト改訂では、ある実装に対して安全性が示されることが必要という趣旨で評価を実施する予定である。コストをかけた特別な実装方法などではなく、通常で利用できる範囲でサイドチャネル攻撃に対する耐性を確認する予定である。
- 公募カテゴリにはモードとMACがあるが、対象としている分類を明確にすべきである。
- 客観的な安全性評価の行われたエンティティ認証に基づくシステムが構築されていくことを期待している。
- 将来CRYPTRECでハッシュ関数を公募する際には、汎用のハッシュ関数の他にも、特殊用途やハッシュ関数関連のモードについても検討するべきである。
- IDベース暗号を調達する際には、主に、数学的基盤、ペアリングアルゴリズム、プロトコル、運用の4つの点が定まっている必要があるが、CRYPTRECとして扱うべき領域について検討する必要がある。

（2） 電子政府推奨暗号リストの今後について

- 評価し尽くされ、長持ちする汎用の実用的な暗号アルゴリズムを厳選すべきである。競争力の点で少数であることが本質的であり、同じカテゴリなら高々2 個。また、専任の機関が自分のものとして責任をもって維持管理していくことが必要である。
- 政府等の大口ユーザーの意思の表明がはっきりしていないので、制度的な裏づけの下で利用していくべきである。
- 安全性に問題がある場合には国際標準技術を使わないことに問題はないだろうが、それ以外の場合は WTO 政府調達協定では問題になるだろう。WTO 協定の恩恵をうけているのは実は日本であり、ISO/IEC 規格との整合性の確保を

お願いしたい。

- 今後は、専門家側は評価にあたって実務上の影響を分析して考慮し、ユーザー側は評価結果を実務によりきちんと反映していくことが必要である。
- 政府機関では危殆化対策としてこれから数年程度かけてシステム移行を行っていく予定である。CRYPTREC には今後もリアルタイムでの情報提供をお願いしたい。
- 電子署名を認証に利用することは多いが、電子政府推奨暗号リストでは認証に利用できるかどうかははっきりしないところがある。
- 電子政府推奨暗号リストを参考にしているという結果も出てきているが、電子政府推奨暗号リストは民間での利用が低いことが問題である。
- 暗号危殆化における世代交代については幅を持たせて進めていくことが必要である。
- 企業において暗号研究者の数を減らす傾向が出てきている。セキュリティ技術に携わる人口を維持するための強化が必要である。CRYPTREC は人材育成という面でも重要な活動であるので、今度も維持していく体制作りが必要である。

## ４．暗号技術監視委員会活動報告

### ４．１．監視活動

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・分析が重要であることから、暗号技術監視委員会が 2003 年度に組織され、活動を行っている。以下に、2008 年度の暗号技術監視委員会の活動内容について報告する。

#### ４．１．１．活動の指針

暗号技術監視委員会は電子政府推奨暗号リスト掲載の暗号に関する研究動向を把握して、暗号技術の安全性について監視を行い、必要に応じて電子政府システムにおける暗号技術の情報収集と電子政府推奨暗号リストの改訂について暗号技術検討会に対して助言を行う。また、暗号理論全体の技術動向を把握して、最新技術との比較を行い、電子政府システムにおける暗号技術の陳腐化を避けるため、将来の電子政府推奨暗号リストの改訂を考慮して、電子政府推奨暗号に関する調査・検討を行う。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、監視要員は研究集会、国際会議、研究論文誌、インターネット上の情報等を監視し、電子政府推奨暗号の安全性に関して情報を分析し、それを暗号技術監視委員会に報告する。また、暗号技術調査ワーキンググループは暗号技術監視委員会の指示のもとに監視活動として必要な調査・検討活動を担当する。

#### ４．１．２．監視状況

（１）共通鍵暗号の安全性評価について

2008 年度の報告時点では、収集した全ての情報が、「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。

具体的な動きとしては、SAC 2008 において、FL 関数を除いた縮小版のブロック暗号 Camellia に対し、128 ビット鍵で 12 段（フルラウンド 18 段）まで、256 ビット鍵で 16 段（フルラウンド 24 段）までという不能差分攻撃が報告されている。また、ASIACRYPT 2008 において、縮小版のブロック暗号 MISTY1（フルラウンド 8

段）に対し、FL 関数付きで 6 段まで、FL 関数なしで 7 段までという不能差分攻撃が報告されている。なお、この解読手法は 2003 年度に学会発表がなされており、監視活動において既知のものである。さらに、MISTY1 に対しては、SCIS 2009 において、データ量 $2^{54.1}$ 及び計算量 $2^{120.8}$ で 7 段という高階差分攻撃が報告されている。また、CRYPTO 2008 において、ストリーム暗号 RC4 に対し、計算量 $2^{579}$（現実的な仮定のものでは計算量 $2^{241}$）という内部状態回復攻撃が示されている。

（２）ハッシュ関数の安全性評価について

2008 年度の報告時点では、収集した全ての情報が、「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。

具体的な動きとしては、CRYPTO 2008 において、縮小版の SHA-1（フルラウンド 80 段）に対し、44 段で計算量 $2^{157}$ という原像攻撃が報告されている。また、SAC 2008 において、縮小版の SHA-256（フルラウンド 64 段）に対し、23 段で計算量 $2^{44.9}$、24 段で計算量 $2^{53.0}$ の、縮小版の SHA-512（フルラウンド 80 段）に対し、23 段で計算量 $2^{18}$、24 段で計算量 $2^{28.5}$ の衝突発見攻撃が報告されている。さらに、FSE 2009 において、24 段に縮小した SHA-256 に対し、計算量 $2^{240}$ の原像攻撃と第 2 原像攻撃、24 段に縮小した SHA-512 に対し、計算量 $2^{480}$ の原像攻撃と第 2 原像攻撃が報告されている。

（３）公開鍵暗号方式の安全性評価について

2008 年度の報告時点では、収集した全ての情報が、「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。

具体的な動きとしては、ANTS-VIII において、Certicom 社の ECC Challenge[5]でまだ解かれていない楕円曲線 ECC2K-130 に関する離散対数問題の計算量について報告があり、2 万台の計算機を使用すれば 2 年で解けると見積もられている。また、ASIACRYPT 2008 において、素体上の離散対数問題に対する Pollard のρ法の高速化手法が提案され、1024 ビットのランダムな素体では従来よりも 10 倍程速くなると報告されている。

（４）その他の安全性評価について

リストには含まれていないが、Eurocrypt 2008 において、大手自動車メーカの多くで採用されているキーレスエントリー・システムで使われるブロック暗号 KeeLoq に対し、攻撃可能な条件が $2^{16}$ 個の既知平文と暗号化 $2^{44.5}$ 回分の計算量にまで削減され、初めて現実的な脅威となっている。また、ASIACRYPT 2008 において、欧州で実施されているプロジェクトである eSTREAM の最終選考まで残っていたスト

[5] http://www.certicom.com/index.php/the-certicom-ecc-challenge/

リーム暗号 F－FCSR-H に対する現実的な攻撃が報告され、その結果により最終選考から急遽、外されている。また、MD5 に対して Eurocrypt 2007 において発表されていた衝突発見攻撃の一種（Chosen-prefix Collision）[6]を電子証明書に関する署名の偽造に応用して、現実的な計算量で中間 CA 証明書の偽造に成功したことが 2008 年の暮れに報告されている[7]。そして、PKC 2007 で提案されていた多変数公開鍵暗号系である ℓIC を用いた署名方式 ℓIC⁻に対して、署名偽造や秘密鍵の解読が可能なことが報告されている。

### （５）暗号技術標準化動向

#### ① SHA-3 選考

National Institute of Standard and Technology (NIST)は 2009 年 2 月 25 日～2 月 28 日の日程で、次世代ハッシュ関数 SHA-3 の選考のための第 1 回会合(The First SHA-3 Candidate Conference)をルーベン・カトリック大学（ベルギー）にて開催した。参加者は約 220 名であった。

ハッシュ関数の説明を行うセッションでは、2008 年 10 月までに応募のあった 64 件のうち、書類審査を通過した 51 件で、この会議までに脆弱性が発見され、提案の取り下げがあった 10 件と今回の会議に参加したかったもの 5 件を除く、36 件のプレゼンテーションが行われた。

NIST による評価観点の説明と議論を行うセッションでは、今後のハッシュ関数の評価において、重要なポイントとなる部分について現時点での NIST の見解を紹介するとともに、参加者からの意見を聴取するセッションが 4 件行われた。各セッションのテーマは以下の通りであった。

(a) System Properties：SHA-3選定にあたって対象とすべきシステム要件

少なくとも電子署名、鍵導出関数、HMAC、擬似乱数生成をサポートすることが示された。処理性能と実装性のトレードオフの観点としては、ゲート数、ハードウェアのハッシュ性能への依存度、メモリサイズ、並列性等が挙げられた。議論を受けて、NISTは、最小限の要求事項と優先順位の低い評価軸を今後提示することを表明した。

(b) System Evaluation：安全性評価の方法

安全性評価のためのモデル設定について現状の案が紹介され、その後参加者から意見が聴取された。アルゴリズムの安全性を示す状態として、

- Completely breaks：　現実的な攻撃が存在する
- Wounds：　原像(preimage)が$2^n$より少ない計算量で計算できる等の、安全性要件を満たさない

---

[6] 最近の研究結果では計算量が $2^{41}$ と報告されている。SHA-1 に関する Chosen-prefix Collision の計算量について $2^{80}$ 弱という見積が出されているので、今後注意が必要である。詳しくは、http://eprint.iacr.org/2009/111/ または、http://www.win.tue.nl/hashclash/rogue-ca/を参照のこと。

[7] JVNVU#836068、MD5 アルゴリズムへの攻撃を利用した X.509 証明書の偽造、http://jvn.jp/cert/JVNVU836068/

- Undermines confidence： 近似衝突(near collision)、擬似衝突(pseudo collision)等、内部にいくつかの脆弱性が存在するが、第2原像(second preimage)や衝突(collision)等は発見されていない
- Little to no concern： 衝突(collision)、第2原像(second preimage)等が発見されており考慮の対象外

という4つの定義が提示された。

(c) System-Performance Tradeoff：安全性と性能のトレードオフ

幅広いアプリケーションに柔軟に対応するために、ブロック長やラウンド数等のパラメータを可変とすることが想定されている。第2ラウンドに向けて、パラメータの仕様の修正の他に、エディトリアルな変更、安全性評価の記述、評価例の追加等を行うことが認められた。さらに、第2ラウンドに選ばれた候補に対しては、変更の理由を示すことを条件にアルゴリズムの微修正を行うことも認められた。また、参照プラットフォームであるIntel IA-32及びAMD64上でSHA-256、SHA-512と同等の性能を実現するパラメータにおいて安全でない場合は、選考の優先順位が下がることが示された。一方で、第2ラウンドへの選考においては性能を特に重視する意図はないことが表明された。また、演算に必要なリソースの観点では、第1ラウンドではソフトウェア実装におけるリソースに注目するとともに、スマートカードのような制約された環境での実装性についても評価を行い、ハードウェア実装については、第1ラウンドでは概要的な評価を行い、第2ラウンドにおいてゲート数を含めた詳細な評価を行うことを表明した。その他、並列実装、アルゴリズム解析の容易性、複数の組み込みシステムへの適正等も評価項目として挙げられた。

(d) The Way Forward：今後の評価の進め方

SHA-3への要件がさまざまであることからパラメータの選択設計が重要であること、また、安全性の評価に加え、性能評価も考慮していることが表明された。今後、第1ラウンドでは特に安全性の評価を重視する形で評価を行い、2009年8月に開催されるCRYPTO 2009の前までに約15件の候補に絞ることが宣言された。この際、異なる設計思想のものをバランス良く残す方針が示された。さらに、研究者に対しては2009年の6月1日までに第1ラウンドの候補に対して、安全性評価結果やコメントを提示するように求めた。なお、次回の会議はCRYPTO 2010辺りに実施される予定である。

その他のセッションでは、提案されているハッシュ関数の分析や比較状況に関する発表や、最新の研究成果に関する発表があった。

② ECRYPT

欧州では ECRYPT（以下、「ECRYPT I」という。）[8]に引き続き、ECRYPT II[9]が 2008

[8] http://www.ecrypt.eu.org/ecrypt1/

年 8 月から開始されている。ECRYPT II は、

- Symmetric techniques virtual lab (SymLab) … 共通鍵暗号系に関するの研究
- Multi-party and asymmetric algorithms virtual lab virtual lab (MAYA) … 公開鍵暗号系に関する研究
- Secure and efficient implementations virtual lab (VAMPIRE) … 暗号技術の実装に関する研究

の 3 つの活動に分かれている。

なお、前回の ECRYPT I では、優れたストリーム暗号を選定するためのプロジェクト eSTREAM[10]を実施していたが、最終的に下記のように選定されている[11]。

表 4.1 eSTREAM 最終選考結果

| Profile 1 (Software-oriented) | Profile 2 (Hardware-oriented) |
|---|---|
| HC-128 | Grain v1 |
| Rabbit | MICKEY v2 |
| Salsa20/12 | Trivium |
| SOSEMANUK | |

### ４．１．３．暗号技術監視委員会開催状況

2008 年度、暗号技術監視委員会は、表 4.2 の通り 4 回開催された。暗号技術調査ワーキンググループは、表 4.3 の通り計 8 回開催された。各会合の開催日及び主な議題は以下の通りである。

表 4.2 暗号技術監視委員会の開催

| 回 | 年月日 | 議題 |
|---|---|---|
| 第 1 回 | 2008 年 7 月 28 日 | 活動方針、リスト改訂及び公募要項の検討、監視状況の報告 |
| 第 2 回 | 2008 年 10 月 28 日 | WG 活動の中間報告、公募要項の検討、監視状況の報告 |
| 第 3 回 | 2008 年 12 月 19 日 | WG 活動の中間報告、公募要項の検討、シンポジウム開催準備及び監視状況の報告 |
| 第 4 回 | 2009 年 3 月 4 日 | WG の報告書案の検討、シンポジウムの開催報告、CRYPTREC Report 2008 の検討 |

表 4.3 暗号技術調査ワーキンググループの開催

| 回 | 年月日 | 議題 |
|---|---|---|
| 第 1 回 | 2008 年 9 月 2 日 | 第 1 回リストガイド WG<br>（活動目的と内容の確認、作業の割り振り） |
| 第 2 回 | 2008 年 9 月 11 日 | 第 1 回 ID ベース暗号 WG<br>（活動目的と内容の確認、作業の割り振り） |
| 第 3 回 | 2008 年 11 月 20 日 | 第 2 回 ID ベース暗号 WG<br>（調査内容の中間報告とその検討） |

[9] http://www.ecrypt.eu.org/
[10] http://www.ecrypt.eu.org/stream/
[11] http://www.ecrypt.eu.org/stream/announcements.html

| | | |
|---|---|---|
| 第 4 回 | 2008 年 11 月 28 日 | 第 2 回リストガイド WG<br>（調査内容の中間報告とその検討） |
| 第 5 回 | 2008 年 12 月 18 日 | 第 3 回 ID ベース暗号 WG<br>（調査内容の報告とその検討） |
| 第 6 回 | 2009 年 1 月 9 日 | 第 3 回リストガイド WG<br>（調査内容の報告とその検討） |
| 第 7 回 | 2009 年 2 月 17 日 | 第 4 回 ID ベース暗号 WG<br>（報告書案の検討、標準化に向けた課題の検討） |
| 第 8 回 | 2009 年 3 月 3 日 | 第 4 回リストガイド WG<br>（報告書案の検討） |

### ４．１．４．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

2008 年度は、国内・国外の学会に参加し、暗号解読技術に関する情報収集を実施した。

監視要員等を派遣した国際会議等は、表 4.4 に示す通りである。

表 4.4　国際会議・国内会議への参加状況

| 学会名・会議名 | | 開催国・都市 | 期間 |
|---|---|---|---|
| PKC 2008 | 11th International Workshop on Practice and Theory in Public Key Cryptography | バルセロナ<br>(スペイン) | 3 月 9 日～<br>3 月 12 日 |
| TCC 2008 | Fifth Theory of Cryptography Conference | ニューヨーク<br>(米国) | 3 月 19 日～<br>3 月 21 日 |
| ANTS-Ⅷ | Eighth Algorithmic Number Theory Symposium | バンフ<br>(カナダ) | 5 月 18 日～<br>5 月 22 日 |
| FDTC 2008 | Workshop on Fault Diagnosis and Tolerance in Cryptography | ワシントン<br>（米国） | 8 月 10 日～<br>8 月 10 日 |
| CHES 2008 | Workshop on Cryptographic Hardware and Embedded Systems | ワシントン<br>（米国） | 8 月 10 日～<br>8 月 13 日 |
| SAC 2008 | Workshop on Selected Areas in Cryptography | サックヴィル<br>（カナダ） | 8 月 13 日～<br>8 月 15 日 |
| CRYPTO 2008 | International Cryptology Conference | サンタバーバラ<br>（米国） | 8 月 17 日～<br>8 月 21 日 |
| ECC 2008 | Workshop on Elliptic Curve Cryptography | ユトレヒト<br>（オランダ） | 9 月 22 日～<br>9 月 24 日 |
| PQCrypto 2008 | International Workshop on Post-Quantum Cryptography | シンシナティ<br>（米国） | 10 月 17 日～<br>10 月 19 日 |

| | | | |
|---|---|---|---|
| ASIACRYPT 2008 | International Conference on the Theory and Application of Cryptology & Information Security | メルボルン（オーストラリア） | 12 月 7 日～12 月 11 日 |
| SCIS 2009 | 2009 年暗号と情報セキュリティシンポジウム | 大津(日本) | 1 月 20 日～1 月 23 日 |
| FSE 2009 | Workshop on Fast Software Encryption | ルーベン（ベルギー） | 2 月 22 日～2 月 25 日 |
| SHA-3 Candidate Conference | SHA-3 Candidate Conference | ルーベン（ベルギー） | 2 月 25 日～2 月 28 日 |

以下に、国際学会等に発表された論文を中心に、暗号解読技術の最新動向について述べる。

（２）解読技術の動向

① ブロック暗号の解読技術

従来からの代数的攻撃の研究が着実に進んでいる。MISTY1 に対して高階差分攻撃を適用することで、8 段中 7 段まで攻撃可能になった[高階差分攻撃に関する 7 ラウンド MISTY1 の安全性、齊藤 照夫、茂 真紀、川幡 剛嗣、角尾 幸保、SCIS 2009]。

また、代数攻撃に差分解読法のような確率的法を組み合わせる方式が開発され、軽量暗号として注目される PRESENT に適用したところ、31 段中 17 段まで解読可能という評価が出ている[Algebraic Techniques in Differential Cryptanalysis、Martin Albrecht and Carlos Cid、FSE 2009]。

② ストリーム暗号の解読技術

暗号研究プロジェクト eSTREAM で採用された暗号 F-FCSR-H と Sosemanuk、国際標準(ISO/IEC 18033-4)に採用された SNOW 2.0 に対する解読が示された[Breaking the F-FCSR-H Stream Cipher in Real Time、Martin Hell and Thomas Johansson、ASIACRYPT 2008]。特に、F-FCSR-H に対する攻撃は現実的な時間で実際に鍵の復元が可能であることを実証したものである。この攻撃の発表を受け、eSTREAM の終了時にハードウェア向け暗号としてポートフォリオに掲載されていたのが、削除された。

Sosemanuk と SNOW 2.0 に対する攻撃は、全数探索よりも少ない計算量で高い確率で鍵が復元できると評価したものである[Cryptanalysis of Sosemanuk and SNOW 2.0 Using Linear Masks、Jung-Keun Lee、Dong Hoon Lee、Sangwoo Park、ASIACRYPT 2008]。

製品に対する現実的な攻撃も幾つか報告されている。第 3 世代携帯電話の規格 GSM で利用されているストリーム暗号である A5/1 への攻撃の実装報告が行われた。

解読可能であるとする理論解析結果は既知であった。Xilinx 社製 Spartan3-XC3S1000 FPGA 120 個を使った高性能低コストの暗号解読専用機 COPACOBANA 上に実装し、予備的な実装でフル実装した場合の性能を外挿したところ、最適化したデザインで全探索をすると 11.78 時間、鍵発見の平均時間は 5.89 時間という見積もりを得た[A Real-World Attack Breaking A5/1 within Hours、Timo Gendrullis、Martin Novotny、Andy Rupp、CHES2008]。

広く普及している、ストリーム暗号 RC4 を使った無線通信プロトコル WEP に対し、104 ビット鍵の場合でも、40,000 パケット程度の受動的観測だけで破れることが示された。従来は、プロトコルの初期ベクトル IV に弱いものが選ばれる等の条件があったが、今回はそのような制約なしで適用できる[Breaking WEP with Any 104-bit Keys —All WEP Keys Can Be Recovered Using IP Packets Only—、寺村 亮一、朝倉 康生、大東 俊博、桑門 秀典、森井 昌克、SCIS2009]。

③　ハッシュ関数の解読技術

衝突発見では、SHA-1 の攻撃段数が 80 段中 70 段のままで大きな進展が無かったものの、より大規模な方式に対する解析が進んだ。SHA-256 の衝突は、64 段中 24 段まで発見できた[Collisions and other Non-Random Properties for Step-Reduced SHA-256、Sebastiaan Indesteege、Florian Mendel、Bart Preneel and Christian Rechberger、SAC 2008]。また、国際標準(ISO/IEC 10118-3)に採用されている Whirlpool の衝突は、10 段中 4.5 段まで計算可能になった[The Rebound Attack: Cryptanalysis of Reduced Whirlpool and Grøstl、Florian Mendel、Christian Rechberger、Martin Schläffer and Søren S. Thomsen、FSE 2009]。

原像計算や第 2 原像計算では、中間データの一部について誕生日攻撃を適用する攻撃手法が開発され、攻撃が進展した。原像攻撃では、SHA-1 が 80 段中 44 段まで[Preimages for Reduced SHA-0 and SHA-1、Christophe De Canniere、Christian Rechberger、CRYPTO 2008]、SHA-256 が 64 段中 36 段まで[Preimage Attacks on MD, HAVAL, SHA, and Others、Yu Sasaki and Kazumaro Aoki、CRYPTO 2008 Rump]、SHA-512 が 64 段中 24 段まで[FSE 2009]可能となった。第 2 原像攻撃では、SHA-256 が 64 段中 24 段まで、SHA-512 が 64 段中 24 段まで可能となった[Preimage Attacks on Reduced Tiger and SHA-2、Takanori Isobe、Kyoji Shibutani、FSE 2009]。

④　公開鍵暗号の解読技術

素因数分解に関しては、数体篩法の内部で利用される楕円曲線法(ECM)などの高速化が進展している。モンゴメリ型楕円曲線の代わりに、効率的な演算規則を持つエドワーズ型楕円曲線を GMP-ECM に組み込み 7% の高速化に成功したことが報告された[Edwards Curves and the ECM Factorisation Method、Peter Birkner、ECC 2008]。

離散対数問題に関しては、素体上の離散対数問題に対する ρ 法を高速化する方法の提案が行われ、1024 bit のランダム素体の離散対数問題に対する ρ 法が従来より 10 倍以上高速化された[Speeding up the Pollard Rho Method on Prime Fields、Jung Hee Cheon、Jin Hong and Minkyu Kim、ASIACRYPT 2008]。

楕円曲線上の離散対数問題に関しては、Certicom 社の ECC challenge（楕円曲線に関する暗号解読コンテスト）でまだ解けていない ECC2K-130 の攻撃計算量について、2 万台のマシンを 2 年稼動させれば解読可能との見積もりが報告された[Implementing a Feasible Attack against ECC2K-130 Certicom Challenge、Ahmad Lavasani、Reza Mohammadi、ANTS-VIII poster]。また、ある条件を満たす拡大体上に定義された楕円曲線の定義体上有理点に関する離散対数問題を解く準指数時間アルゴリズムの報告が行われた。Weil Descent Attack の一種と見られる。しばしば利用される 2 の拡大体にはこの条件は適用できないとのこと。以前から指摘されている事ではあるが、こうした曲線を使用する場合は注意してパラメータを選ぶ必要がある。[An update on ECDLP over extension fields、Claus Diem、ECC 2008 rump]。

その他、PKC 2007 で提案されていた多変数公開鍵暗号系である ℓIC を用いた署名方式 ℓIC－に対して、署名偽造や秘密鍵の解読が可能なことが報告されている[Total Break of the ℓ-IC Signature Scheme、P.A. Fouque、G. Macariorat、L. Perret and J. Stern、PKC2008]

⑤　その他

多くの車のドアロックシステム、また欧米のほとんどのガレージ開閉システムに採用されている KeeLoq システムに対する現実的な攻撃が報告された。KeeLoq システムでは Manufacturer 鍵は一意で、それとシリアル番号とから、各コントローラーのデバイス鍵が作られる。システムのすべてのレシーバーには、Manufacturer 鍵が埋め込まれており、送られてくるシリアル番号とからデバイス鍵を認証する。電力解析により、実際の製品から、Manufacturer 鍵やデバイス鍵を取り出すことに成功し、鍵の複製や本物の鍵を無効にすることができた。ECC 2008 では公演中の実製品攻撃デモンストレーションに成功した[On the Power of Power Analysis in the Real World: A complete Break of the KEELOQ Code Hopping Scheme、Thomas Eisenbarth、Timo Kasper、Amir Moradi、Christof Paar、CRYPTO 2008] [On the Power of Power Analysis in the Real World、Timo Kasper、ECC 2008]。

CRYPTO 2008 の招待講演にて Adi Shamir からブロック暗号、ストリーム暗号、MAC など広範囲の暗号に適用することができる非常に強力な代数的攻撃手法である CUBE attack が紹介された[How to Solve it: New Techniques in Algebraic Cryptanalysis、Adi Shamir、CRYPTO 2008]。

## ４．２．暗号技術調査ワーキンググループ

### ４．２．１．概要

2008 年度は、近年活発に研究が行われ、かつ、IEEE や IETF で標準化が行われる等、将来において電子政府での利用が見込まれる可能性もあることから、新規に ID ベース暗号ワーキンググループを組織した。

リストガイド WG と ID ベース暗号 WG の 2008 年度の主要活動項目は、表 4.5 のとおりである。

表 4.5　2008 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 | 佐々木 良一 | ① CRYPTREC が今年度策定した電子政府推奨暗号リストの改訂に関する骨子に基づき、リストガイドで取り扱う対象技術の体系化やロードマップについて検討<br>② 対象仕様の明確化 |
| ID ベース暗号 WG | 高木 剛 | ① ID ベース暗号、ペアリング利用技術の安全性評価手法の調査<br>② ID ベース暗号、ペアリング関連技術の実用化に関する動向調査<br>③ ID ベース暗号、ペアリング関連技術の標準化に向けた検討 |

### ４．２．２．リストガイドワーキンググループ

（１）調査背景

2007 年度に策定したリストガイドにおいては、標準的なセキュリティ技術において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利用形態を分析し、それぞれの利用形態について、推奨される暗号アルゴリズム、および推奨されるセキュリティパラメータを示した。2007 年度のリストガイドでは、標準的な利用方法に関する網羅性は確保できたが、一方で電子政府における調達元と調達先にとって一意に参照できる形態が望ましいこと、また策定する利用方法や仕様は暗号モジュール評価に対して曖昧さを残さないことが求められること、暗号技術の実際の利用状況から次期リスト策定前に推奨となる実装を示す技術が存在すること、などの課題が存在した。

そこで、2008 年度のリストガイド WG においては、上記の課題に対応するために、以下の活動方針のもと、活動を行った。

- リストガイドを、電子政府における利用形態ごとの暗号技術仕様と位置づけて体系化し、識別子を付与することにより、調達の際に識別子によって一意に調達仕様が示すことができるようにする。

- 体系におけるリストガイドを 2013 年までに整備することを念頭に、優先順位の高い利用形態と技術から、推奨される利用方法や技術仕様をまとめる。
- 暗号モジュール評価における評価対象の仕様での曖昧さを解消するため、モジュール評価における評価者にとって曖昧でない利用方法を提示すること。
- 現在、広く使われているが電子政府推奨暗号リストにおいて標準化されていない技術について、2013 年より前にも推奨される使われ方を示す必要があるため、リストガイドの中で推奨を示す。

本 WG の 2008 年度の活動では上記の方針に沿って、

- 優先順位の高い「PKI 向け電子署名」
- 現在電子政府推奨暗号リストに存在しない、メッセージ認証子と暗号利用モードについて、仕様の策定を行った。

2008 年度のリストガイドは、暗号技術を利用したシステムの調達を行う調達元とシステムの構築を行う調達先が、暗号技術の実装に関する仕様の共通の参照先として使われると同時に、暗号モジュール評価においても参照されることを想定している。仕様策定にあたっては、2007 年度版リストガイドと同様、作成完了後 3 年間程度において有効な内容として執筆を行った。

（２）活動内容

2008 年度は、PKI 向け電子署名、メッセージ認証子、暗号利用モードについて、リストガイドの検討を行った。

まず、最初の検討として、各技術について電子政府における利用形態の調査を行った。その上で、ISO、IETF などの国際標準規格において、既に規格化されている内容について調査を行い、それらの標準の内容について、我が国の電子政府における利用に問題がない場合にはその内容に沿った執筆内容とし、不足点、問題点がある場合にはその不足点を補う検討を行い追加の記述を行った。

リストガイドの構成は、それぞれの技術が分冊的に参照されることを考慮し、共通的に以下の通りとすることとした。

（ア）本文書の位置づけ

文書の目的、Introduction など

（イ）定義

用語および記号などの定義

（ウ）技術概要

基本的なセキュリティ機能、利用のモデル、技術の構成要素、主要技術の仕様、比較

（エ）実装仕様

各技術の実装仕様

（オ）テストベクトル

実装評価などに用いるテストベクトル

その上で、リストガイドを記述する上で以下の議論を行った。

(a) PKI 向け電子署名

- 記述の対象を DSA、ECDSA、RSASSA-PKCS1-v1_5，RSASSA-PSS とした。
- DSA、ECDSA については、ドラフトであるが、NIST FIPS PUB 186-3 draft をベースに記載を行い、その他の標準については参考情報として記載した。
- 安全性については、NIST SP 800-57 を基本に進め、CRYPTREC の監視状況に基づく見解も含めることとした。

(b) メッセージ認証子

- 記述の対象を、HMAC、CBCMAC、CMAC とした。
- HMAC については、NIST FIPS PUB 198 をベースとし、CMAC については NIST SP 800-38B をベースとして記述した。
- CBC-MAC は、金融業界で利用されているため、互換性維持の観点から基本的にはリストガイドとして作成するが、強いて利用する必要がない場合には推奨しないことを明示した。
- HMAC における SHA-1 の利用等、アプリケーションごとに要求条件が異なる場合には、それに関連する事項を参考情報として可能な限り掲載した。
- 内部で利用されている暗号プリミティブについては、現在の電子政府推奨暗号リストに記載される暗号プリミティブをベースに進めた。
- 現在使われていないと考えられる暗号プリミティブについては、国際標準に関する参考情報として記載した。
- MAC の出力の truncated output は、NIST FIPS PUB 198 を引用し、参考情報として提示した。

(c) 暗号利用モード

- 記述の対象を、ECB、CBC、CFB、OFB、CTR の各モードとした。
- 技術的詳細に関しては、NIST SP 800-38A をベースに記載した。
- CBC モードを長く続ける場合には誤りが発生しやすくなる等、利用するパラメータについて、標準仕様に記載されていない場合でも、アドバイス可能な事項は極力記載した。
- 細かいパラメータの推奨方法については、明確なものについては記述した。
- パディングの誤った利用方法については、注意を記述した。
- 各モードの特徴について、安全性、処理速度、並列処理、自己同期性、エラー伝播、パディングの必要性、初期ベクトルなどについて比較を行うとともに、簡潔な根拠を追記することとした。

また、活動においては、ISO などの国際標準との整合性、金融分野などの業界標準の動向を参考にし、記述内容の精査も合わせて行った。

（3）まとめ

2008 年度の活動では、国際標準との整合性を考慮しながら、PKI 向け電子署名、メッセージ認証子、暗号利用モードに関する推奨される利用方法、実装仕様をまとめた。今後の活動としては、本年度の策定内容について、CRYPTREC における監視活動の結果に基づいて、適宜維持管理を行うとともに、次年度以降、仕様策定の優先順位に応じてリストガイドの残りの項目について整備を進めることが必要である。

### 4．2．3．ID ベース暗号ワーキンググループ

（1）調査背景

2001 年に利便性の高い公開鍵暗号としてペアリングという特別な数学的な性質を用いた「ID ベース暗号」が提案されて以来、ID ベース暗号、およびペアリングを利用した各種暗号技術の研究が活発に行われている。また、IEEE や IETF で標準化が行われるなど、実用化に近い段階に入っている。本技術分野は、近い将来電子政府での利用も見込まれ、その場合には、CRYPTREC における評価、および電子政府推奨暗号リストへの掲載を行うことも視野に入れる必要がある。

本ワーキンググループの活動目的は、将来 ID ベース暗号の CRYPTREC での評価の実施や、電子政府推奨暗号リストにおける公募の実施の可能性の検討に向けた現状調査を行い、将来の検討に資する知見を取りまとめることにある。

そのため、ID ベース暗号、およびペアリング技術を将来 CRYPTREC で評価、および公募するための事前調査として以下の観点での調査を行った。

- 技術の概要と想定されるアプリケーション
- 安全性評価手法と安全性評価の現状
- 実装アルゴリズムと実装の現状
- 国際会議における研究発表の動向、および標準化動向
- 製品動向、および知的財産権の動向

（2）活動内容

本ワーキンググループでは、上記の 5 つの面について調査を行い、以下のような動向を取りまとめた。

(a) 技術の概要と想定されるアプリケーション

- ID ベース暗号技術の概要、および有用性について調査を行った。ID ベース暗号の有用な点として、PKI における認証局が不要となる点、新規ユーザへの対応が容易である点、未登録者への暗号データの送信が可能である点を挙げた。
- ID ベース暗号の課題としては、ID の信頼性の確保、鍵生成センタの信頼性の

確保、鍵更新、ユーザ鍵の無効化といった運用面の課題を挙げた。

- ID ベース暗号を構成する基本的な構造を挙げた上で、既存の方式の分類を行った。
- ID ベース暗号から、放送暗号、属性暗号など多くのアプリケーションが発展していることを示した。
- 公開鍵インフラとして利用した場合のメリットとデメリットを深く考察し、特に公開鍵証明書が不要になるメリットがある一方、上記に挙げた鍵更新と無効化を考えた場合 PKI に対するメリットが少ないことも判明している。また、ID ベース署名自体には、PKI ベースの署名に対するメリットは認められない。一方で、基礎となるペアリングによって多くのアプリケーションが派生しており、その点における暗号学的メリットがあることを挙げている。

(b) 安全性評価手法と安全性評価の現状

- ID ベース暗号における安全性は、既存の公開鍵暗号と同様に数学的に困難な問題への帰着によって行われることを示し、その上で ID ベース暗号の安全性レベルの定義と、数学的な仮定と、その強さの評価方法をまとめた。
- ペアリングを用いた暗号技術においては、新たな数学的仮定が数多く提案されている。まず、ベースとなる楕円曲線上における数学的に困難な問題について調査を行うとともに、ペアリング逆関数問題の困難性、および安全性証明に利用される問題に関する調査を行った。

(c) 実装アルゴリズムと実装の現状

ここでは、特にペアリングに焦点を当て、ペアリングを実現する著名なアルゴリズムとして、Tate ペアリング、ηT ペアリング、Ate ペアリングについて、その実装アルゴリズムを示すとともに、PC、FPGA、スマートカード、組み込み用 CPU における楕円曲線、実行環境に応じた処理の実行時間をまとめた。

(d) 国際会議における研究発表の動向、および標準化動向

- ID ベース暗号、およびペアリング技術に関する国際会議における発表の動向の調査を行った。対象としては、IACR 主催の会議、IACR ePrint アーカイブ、その他の国際会議である。
- 発表論文は、基礎的な技術（主にペアリング計算の高速化やアルゴリズムの改良）と、応用技術、アプリケーションの提案の 2 種類に大別される。
- 国際標準化の動向を調査した。現状では、IETF、ISO/IEC、IEEE において標準化活動が認められるため、これらの内容を調査した。

(e) 製品動向、および知的財産権動向

- ID ベース暗号、およびペアリング技術を実装した製品について、製品のリスト、製品の概略、入手方法の調査を行った。16 の製品についての調査結果が

まとまった。

- 「世界で少なくとも 600 万人が利用している」という報告もなされている。
- 知的財産権の調査として、日米の特許に関する状況の違いに触れながら、日本、および米国で出願されている特許の出願番号、出願日、出願人、出願の状態、特許の概要などについて調査結果をまとめた。

（3）まとめ

2008 年度の活動では、（1）の 5 項目について調査を行い、報告書としてまとめた。電子政府での利用を考慮に入れて、安全性、実装性の面という理論的な成熟度に加えて、アプリケーション、および製品動向という成熟度の現状も把握した。また、それらの調査結果をもとに、CRYPTREC での今後の検討課題を洗い出し、次年度以降の検討に資することとした。

次年度以降の検討項目として指摘した項目は以下の通りである。

- ID ベース暗号に関連する評価対象とする領域。ID ベース暗号を調達する際には、主に、数学的基盤、ペアリングアルゴリズム、プロトコル、運用の 4 つの点が定まっている必要があるが、CRYPTREC として扱うべき領域について検討する必要がある。
- ID ベース暗号を調達する際の課題。特に ID ベース暗号の利用に当たっては、鍵生成センタの運用などに条件があるほか、鍵更新、無効化、ID の信頼性など解決すべき課題があるため、これらの課題についての更なる検討が必要である。

# ５．暗号モジュール委員会活動報告

## ５．１．暗号モジュール委員会の概要

### ５．１．１．暗号モジュール委員会の活動目的と経緯

電子政府の安全性及び信頼性を確保するためには、暗号アルゴリズムの安全性はいうまでもなく暗号技術を実装した暗号モジュール製品（暗号製品）の安全性確保が非常に重要である。この観点から暗号モジュール委員会は、暗号モジュールのセキュリティ要件と試験要件(DTR[12])につき検討し、自己完結的な文書として一応の完成をみた。その後、上記セキュリティ要件作成の参考とした米国の FIPS[13] 140-2 をベースとする国際標準規格が ISO[14]/IEC[15] 19790 として成立し、その JIS[16](JIS X 19790)化もなされた。また、2006 年には ISO/IEC 19790 に対応する暗号モジュール試験要件の検討も開始され、2008 年 3 月に ISO/IEC 24759 として国際標準となっている。

一方、FIPS 140-2 は 2005 年より NIST[17]を中心として改訂の検討が開始され、2007 年に FIPS 140-3 の 1st Draft が公表された。

このため、本委員会は、国際規格においては JTC1/SC27 の国内審議団体を通じて、また、次世代の国際規格に影響を与える可能性のある FIPS については NIST 等との連絡により、規格の充実について技術内容面から積極的に寄与してきた。また、並行して、暗号モジュールへの脅威となっている電力解析攻撃や電磁波解析攻撃等のサイドチャネル攻撃と、それらの防御に関する実装評価技術の実験及び情報収集活動を行ってきた。2008 年度も、サイドチャネル攻撃について、電力解析実験ワーキンググループによる実験を通じて継続してこれらの活動を行い、暗号製品の安全性の確保と規格の標準化に貢献することを目的とする。

### ５．１．２．暗号モジュール委員会の開催状況

2008 年度の暗号モジュール委員会は、計 4 回開催された。各回会合の概要は表 5.1 のとおりである。

表 5.1　2008 年度暗号モジュール委員会の開催状況

| 回 | 開催日時 | 主な議題 |
|---|---|---|
| 第 1 回 | 2008 年 8 月 1 日<br>10:00～11:30 | 暗号モジュール委員会活動計画<br>電力解析実験ワーキンググループ活動計画<br>電子政府推奨暗号リスト改訂と関連した活動について |

[12] DTR：Derived Test Requirements
[13] FIPS：Federal Information Processing Standard
[14] ISO：International Organization for Standardization
[15] IEC：International Electrotechnical Commission
[16] JIS：Japanese Industrial Standards
[17] NIST：National Institute of Standards & Technology

| | | |
|---|---|---|
| 第 2 回 | 2008 年 10 月 31 日<br>14:00～16:00 | 電子政府推奨暗号リスト改訂と関連した活動について<br>電力解析実験ワーキンググループ中間報告<br>規格・標準化動向等についての報告 |
| 第 3 回 | 2008 年 12 月 15 日<br>10:00～12:00 | 電子政府推奨暗号リスト改訂と関連した活動について<br>CRYPTREC シンポジウム 2009「リスト改訂に向けて」の告知 |
| 第 4 回 | 2009 年 2 月 20 日<br>18:00～20:00 | 2008 年度電力解析実験ワーキンググループの活動報告<br>2008 年度暗号モジュール委員会の活動報告（案）について |

## ５．２．活動内容と成果概要

暗号モジュール委員会は、今年度は下記の活動を行った。

（１）電子政府推奨暗号リスト改訂のための、ハードウェア及びソフトウェア実装性評価の公募要件作成

「電子政府推奨暗号リスト改訂のための暗号技術公募要項（2009 年度）」について暗号技術検討会の依頼を受け、暗号モジュールの実装に関する第一次評価と第二次評価の評価項目について検討を行った。

（２）サイドチャネル攻撃のセキュリティ要件と NIST FIPS 140-3 DTR 等への標準化への協力

NIST による暗号モジュールセキュリティ要件 FIPS 140-3 の改訂作業が大幅に遅れ、2009 年 1 月末現在 FIPS 140-3 草案に対する改訂版は公開されていない。また、FIPS 140-3 に対応する DTR も公開されていない。

さらに、FIPS 140-3 に基づき早期改訂が予定されている ISO/IEC 19790 検討に関しては WD[18]が提出されていない。そのため、これらの標準化に関する検討は、来年度以降に先送りすることとなった。

（３）暗号モジュールへの攻撃の監視と分析

監視要員による国内外で開催された会議等への出席により、最新情報を収集し、監視委員会にて報告を行い、情報を共有した。

（４）電力解析実験ワーキンググループよる実験

サイドチャネル解析用プラットフォームの仕様である INSTAC[19]-8/-32[20]仕様に準拠したボードや SASEBO[21]ボード等を用いた比較実験を依頼した結果、電力解析実験ワーキンググループから以下の項目に関する報告が提出された。

① サイドチャネル攻撃に関する比較実験

② 採取データの形式の統一化

---

[18] WD：Working Draft

[19] INSTAC：情報技術標準化研究センター（Information Technology Research and Standardization Center）

[20] INSTAC-8/-32：サイドチャネル攻撃耐性評価用標準プラットフォーム仕様（-8 は 8bit 版，-32 は 32bit 版）

[21] SASEBO: サイドチャネル攻撃実験用標準評価ボード（Side-channel Attack Standard Evaluation BOard）で 2 種類の Xilinx Virtex-II Pro FPGA である xc2vp7 と xc2vp30 を搭載。

SASEBO ボードに関しては，平成 19 年度経済産業省委託事業「暗号モジュールの実装攻撃の評価に関する調査研究」の中で産業技術総合研究所と東北大学が新たに開発を行った，Xilinx 社製 FPGA を実装した SASEBO-G，ALTERA 社製 FPGA を実装した SASEBO-B,そしてカスタム暗号 LSI を実装した SASEBO-R の 3 種類が，電力解析実験ワーキンググループの委員が所属する研究機関に対して提供された。これにより，アーキテクチャの異なるハードウェア上でのサイドチャネル攻撃実験が行える環境が整った．そこで，本ワーキンググループにおいても産総研の了承のもと，各委員がこれらの SASEBO ボードを活用した比較実験を行うこととした。

③ 実験データの標準評価方法の検討
④ 電力解析攻撃実験のための評価ボードを利用した研究の調査
⑤ 今後の検討項目

## ５．３．電力解析実験ワーキンググループの活動

### ５．３．１．電力解析実験ワーキンググループの活動目的と経緯

暗号モジュールへのサイドチャネル攻撃は、特に IC カードのようなワンチップモジュールにとっては大きな脅威となる。サイドチャネル攻撃の中でも、暗号モジュールの消費電力を計測することで、鍵情報を推定する電力解析攻撃（DPA[22]攻撃、SPA[23]攻撃、タイミング攻撃等）は、簡便な攻撃環境・リソースで実現することが可能となるため、今後対策の実施が必須となると考えられる。

しかし、サイドチャネル攻撃に対するセキュリティ要件や試験要件は未だ具体的に決められていない。

そこで、実験データを収集・分析し、サイドチャネル攻撃に対するセキュリティ要件、試験要件の検討に資することを目的とする。

### ５．３．２． 電力解析実験ワーキンググループの開催状況

2008 年度の電力解析実験ワーキンググループは、計 4 回開催された。各回会合の概要は表 5.2 のとおりである。

表 5.2　2008 年度電力解析実験ワーキンググループの開催状況

| 回 | 開催日時 | 主な議題 |
|---|---|---|
| 第 1 回 | 2008 年 9 月 3 日<br>14:00～16:00 | 電力解析実験ワーキンググループ活動計画<br>データの交換用標準フォーマットについて |
| 第 2 回 | 2008 年 10 月 3 日<br>15:00～17:00 | データの交換用標準フォーマットについて<br>実験の進め方について<br>FPGA[24]と ASIC[25]の比較実験結果の検討 |
| 第 3 回 | 2008 年 11 月 26 日<br>15:00～17:00 | 実験データの標準評価方法について<br>実験環境等についての検討 |
| 第 4 回 | 2009 年 2 月 4 日<br>14:30～16:30 | 2008 年度電力解析実験ワーキンググループの活動のまとめ<br>暗号モジュール委員会への報告書の作成<br>2009 年度の活動計画(案)について |

### ５．３．３．電力解析実験ワーキンググループの成果概要

本ワーキンググループでは 2006 年度の開始当時から、実験用標準評価ボード等に搭載された暗号モジュールについて、電力解析攻撃に関する実験方法と、標準的な試験方

[22] DPA：Differential Power Analysis（差分電力解析）
[23] SPA：Simple Power Analysis（単純電力解析）
[24] FPGA：Field Programmable Gate Array
[25] ASIC：Application Specific Integrated Circuit

法と、安全性の基準の検討を行ってきた。産業技術総合研究所と東北大学が開発した実験用評価ボード SASEBO（Xilinx 版）の利用に加え、2008 年度は、新たに FPGA を搭載した SASEBO-G（Xilinx 版）[26]と ASIC を搭載した SASEBO-R（LSI[27]版）[28]等が開発されたため、これらを利用し、FPGA と ASIC の暗号モジュールにおける実験結果の違いを調べることを主要課題として活動を行い、比較実験結果とそれに関連する実験データの統一化、標準評価方法の検討を今年度の成果とした。

（1）サイドチャネル攻撃に関する比較実験

委員が行った実験成果についてワーキンググループで検討を行った。

3 種類のサイドチャネル攻撃実験用標準評価ボード SASEBO（Xilinx 版)、SASEBO-G（Xilinx 版)、SASEBO-R（LSI 版）搭載の各 AES 暗号モジュールについて、電力相関解析(CPA[29])の比較実験を行った結果、Xilinx の FPGA と ASIC ではどちらも類似した結果となり、採取する波形データの数が多ければ攻撃は成功することが確認された。

それらは、それぞれＳボックスの作り方による実装の違いによって測定結果に違いが存在することが確認できた。

また、動作クロック周波数が低い場合と時間当たりの波形データのサンプル数が多い場合の方が、そうでない場合より攻撃成功確率が高いことが確認され、オシロスコープの性能による、クロック周波数、サンプル間隔の条件によって攻撃の成功確率が異なることが判明した。

（2）採取データの形式の統一化

実験で採取した波形のデータを委員等の間で共有し、相互での評価が可能となる様にデータファイルの互換性についての検討を行い、波形データ交換標準フォーマット(WXF[30])として波形データの形式の統一化を行った。

この標準フォーマットには付属情報が記述出来る様になっており、波形データの利用者は、その波形データの特性がどのようなものか参考情報として利用可能となっている。

（3）標準評価方法の検討

電力解析の評価において最も有効な方法として、ピアソンの積率相関係数を用いた CPA について検討し、この方法を電力解析実験ワーキンググループでの標準評価方法の一つとして定めた。

---

[26] SASEBO-G：SASEBO-G は SASEBO の改良版で Xilinx 社の Virtex-II Pro FPGA である xc2vp7 と xc2vp30 を搭載したサイドチャネル攻撃実験用標準評価ボード

[27] LSI：Large Scale Integration

[28] SASEBO-R：TSMC 社の 130nm CMOS ライブラリによって製造された，専用暗号 LSI を搭載した ASIC 版のサイドチャネル攻撃実験用標準評価ボード

[29] CPA：Correlation Power Analysis

[30] WXF：Waveform data eXchange Format

また CPA の評価結果の表示方法として、縦軸を相関係数の平均とし横軸を波形数としたグラフを標準の表示方法に決めた。

結果のグラフにおいては無相関のグラフと有意なハミング重み／ハミング距離のグラフに分離できた点を正解鍵が求まる波形数の位置とし、これを判定基準として決めた。この点については、電力解析攻撃の未対策版の暗号モジュールでの相関は分離可能であるが、対策版ではその点を求めるには膨大な波形数が必要と推定した。

（4）電力解析攻撃実験のための評価ボードを利用した研究の調査

産業技術総合研究所 情報セキュリティ研究センター（RCIS[31]）と東北大学大学院 情報科学研究科が開発したサイドチャネル攻撃実験用標準評価ボード（SASEBO）等を使用した、電力解析実験ワーキンググループの委員による、2008年度の発表についてまとめた（表 5.3)。

（5）今後の検討項目

・暗号モジュールへの最適な電力解析の実験方法の検討

今年度の実験用標準評価ボードの比較実験結果から、暗号モジュールの動作クロック周波数を低く設定することと、波形のサンプリング間隔を短くすることで、攻撃の成功確率が向上することが確認されている。これらを基に評価のための測定環境や測定ポイント等の条件について検討し、実験結果の改善を行い、電力解析攻撃が成功するための測定コストと測定時間条件を意識して、最適な試験方法を検討することが今後の課題である。

[31] RCIS：Research Center for Information Security

## 表 5.3　評価ボードを使用した発表論文リスト

| | タイトル | 学会名・会議名 | 発表年月日 | 著者 | 使用ボード種類 |
|---|---|---|---|---|---|
| 1 | SASEBO ボードに搭載された AES 回路へのサイドチャネル攻撃とその検証 | ISEC[32] | 2008.5.16 | 南崎 大作，岩井 啓輔，黒川 恭一（防衛大学校） | SASEBO |
| 2 | サイドチャネル攻撃評価用自動測定ソフトウェアの開発 | ISEC | 2008.5.16 | 岩井 啓輔，南崎 大作，黒川 恭一（防衛大学校） | SASEBO |
| 3 | Collision-Based Power Analysis of Modular Exponentiation Using Chosen-Message Pairs | CHES2008[33] | 2008.8.11 | 本間 尚文，宮本 篤志，青木 孝文（東北大学），佐藤 証（産業技術総合研究所），Adi Shamir(ワイツマン研究所) | SASEBO |
| 4 | High-Performance Concurrent Error Detection Scheme for AES Hardware | CHES2008 | 2008.8.11 | 佐藤 証（産業技術総合研究所），本間 尚文，菅原 健，青木 孝文（東北大学） | SASEBO |
| 5 | 鍵候補の篩い分けによる CPA の高速化と鍵推定精度の向上 | CSS2008 D5-1[34] | 2008.10.9 | 片下 敏宏，佐藤 証(産業技術総合研究所),菅原 健，本間 尚文，青木 孝文(東北大学) | SASEBO |
| 6 | 電源ライン上の漏洩情報を用いたサイドチャネル攻撃 | CSS2008 D5-2 | 2008.10.9 | 林 優一，菅原 健，本間 尚文，水木 敬明，青木 孝文，曽根 秀昭(東北大学),佐藤 証(産業技術総合研究所) | SASEBO |
| 7 | 標準評価基板上の ASIC への差分電力解析実験 | CSS2008 D5-3 | 2008.10.9 | 菅原 健，本間 尚文，青木 孝文(東北大学),佐藤 証(産業技術総合研究所) | SASEBO-R |
| 8 | 暗号モジュールへの信号ラインからのサイドチャネル攻撃（２）- 詳細実験結果 | CSS2008 D5-4 | 2008.10.9 | 渡部 良太，高橋 芳夫，松本 勉(横浜国立大学) | SASEBO |
| 9 | SASEBO における FPGA に対する電力解析/電磁波解析実験 | ISEC | 2008.11.13 | 庄司 陽彦(株式会社ワイ･デー･ケー/情報セキュリティ大)，野澤 晃，木村 隆幸（株式会社ワイ・デー・ケー），洲崎 智保，山下 哲孝，角尾 幸保（日本電気株式会社） | SASEBO |
| 10 | FPGA & ASIC Implementation of Differential Power Analysis Attack on AES | INSCRYPT[35] | 2008.12.15 | Guoyu QIAN，Yibo FAN(早稲田大学)，角尾 幸保(日本電気株式会社) ，池永 剛,後藤 敏(早稲田大学) | SASEBO-G<br>SASEBO-R |
| 11 | CPA 攻撃用実験環境の構築 | ISEC | 2008.12.17 | 南崎 大作，岩井 啓輔，黒川 恭一（防衛大学校） | SASEBO |
| 12 | テーブルネットワーク型AES実装の新手法の提案(2) | SCIS[36] | 2009.1.20 | 山口 晃由，佐藤 恒夫（三菱電機株式会社） | INSTAC-8 |
| 13 | 自己完結型テンプレート攻撃 | SCIS | 2009.1.20 | 鈴木 大輔（三菱電機株式会社/横浜国立大学），佐伯 稔（三菱電機株式会社），松本 勉（横浜国立大学） | SASEBO-R |
| 14 | ブロック暗号の回路アーキテクチャに対するサイドチャネル耐性評価(1) | SCIS | 2009.1.20 | 鈴木 大輔（三菱電機株式会社/横浜国立大学），佐伯 稔，清水 孝一（三菱電機株式会社） | SASEBO-R |
| 15 | ブロック暗号の回路アーキテクチャに対するサイドチャネル耐性評価(2) | SCIS | 2009.1.20 | 佐伯 稔（三菱電機株式会社），鈴木 大輔（三菱電機株式会社/横浜国立大学），清水 孝一（三菱電機株式会社） | SASEBO-R |
| 16 | RSL 技術を用いた耐 DPA 暗号 LSI の設計手法 －プロトタイプ LSI に対する DPA 評価結果－ | SCIS | 2009.1.20 | 佐伯 稔（三菱電機株式会社），鈴木 大輔（三菱電機株式会社/横浜国立大学） | SASEBO-R |
| 17 | サイドチャネル攻撃評価用 ISO/IEC 標準暗号プロセッサの開発 | SCIS | 2009.1.21 | 本間 尚文，宮本 篤志，菅原 健，青木 孝文（東北大学），佐藤 証（産業技術総合研究所） | SASEBO-R |
| 18 | べき乗剰余演算に対する比較電力解析の応用 | SCIS | 2009.1.21 | 宮本 篤志，本間 尚文，青木 孝文（東北大学），佐藤 証（産業技術総合研究所） | SASEBO |

[32] ISEC：情報セキュリティ研究会（電子情報通信学会）
[33] CHES：Workshop on Cryptographic Hardware and Embedded Systems（International Association for Cryptologic Research (IACR)）
[34] CSS：Computer Security Symposium（情報処理学会）
[35] INSCRYPT：International Confernces on Information Security and Cryptology (Chinese Association for Cryptologic Research and The State Key Laboratory of Information Security (SKLOIS) of China)
[36] SCIS：暗号と情報セキュリティシンポジウム（電子情報通信学会）

| | | | | | |
|---|---|---|---|---|---|
| 19 | 電磁波を利用した故障利用攻撃の実験手法に関する一考察 | SCIS | 2009.1.21 | 田中 秀磨（情報通信研究機構） | SASEBO |
| 20 | 高周波クロックによる RSL 技術を用いた AES へのフォールト攻撃実験 | SCIS | 2009.1.21 | 八木 達哉，崎山 一男，太田 和夫（電気通信大学） | SASEBO-R |
| 21 | フォールト混入時における RSL 技術による暗号回路モデルを用いた安全性解析 | SCIS | 2009.1.21 | 泉 雅巳，太田 和夫，崎山 一男（電気通信大学） | SASEBO-R |
| 22 | 電力解析と電荷の充放電に関する考察 | SCIS | 2009.1.22 | 品川 宗介，市川 哲也（三菱電機エンジニアリング株式会社），佐藤 恒夫（三菱電機株式会社） | SASEBO-R |
| 23 | SASEBO における FPGA に対する電力解析／電磁波解析実験 | SCIS | 2009.1.22 | 庄司 陽彦（株式会社ワイ・デー・ケー／情報セキュリティ大学院大学），野澤 晃，木村 隆幸（株式会社ワイ・デー・ケー），洲崎 智保，山下 哲孝，角尾 幸保（日本電気株式会社） | INSTAC-32<br>SASEBO |
| 24 | 信号処理を利用した SASEBO における差分電力解析 | SCIS | 2009.1.22 | 山下 哲孝，洲崎 智保（日本電気株式会社），庄司 陽彦，野澤 晃，木村 隆幸（株式会社ワイ・デー・ケー），角尾 幸保（日本電気株式会社） | SASEBO |
| 25 | 波形選別による差分電力解析の改善について | SCIS | 2009.1.22 | 野澤 晃，庄司 陽彦，木村 隆幸（株式会社ワイ・デー・ケー），洲崎 智保，山下 哲孝，角尾 幸保（日本電気株式会社） | SASEBO |
| 26 | 最近傍から計測した磁界を用いた差分電磁波解析 | SCIS | 2009.1.22 | 菅原 健，鳥塚 英樹，本間 尚文（東北大学），佐藤 証（産業技術総合研究所），青木 孝文，山口 正洋（東北大学） | SASEBO-R |
| 27 | サイドチャネル解析研究に役立つ波形データ交換用標準フォーマット WXF の提案 | SCIS | 2009.1.22 | 松本 勉（横浜国立大学），高橋 芳夫（横浜国立大学／NTT データ） | SASEBO-R |
| 28 | CPA に対するデカップリングキャパシタの影響の予備検証 | SCIS | 2009.1.22 | 片下 敏宏，佐藤 証（産業技術総合研究所），菅原 健，本間 尚文，青木 孝文（東北大学） | SASEBO-R |

## ６．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、「第２次情報セキュリティ基本計画」等を踏まえつつ、2009 年度以降以下の活動を実施していく。

### （１）電子政府推奨暗号の監視

電子政府推奨暗号に選定された各暗号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（別添３参照）。

### （２）電子政府推奨暗号の安全性及び信頼性確保のための調査・検討

#### ①　暗号アルゴリズム等を主な対象とする調査・検討

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

#### ②　暗号実装関連技術を主な対象とする調査・検討

実装攻撃等の暗号実装関連技術を主な対象とする調査及び検討を行う。

### （３）電子政府推奨暗号リストの改訂に関する調査・検討

2009年度後半に電子政府推奨暗号リストの改訂に向けた暗号技術の公募を行う。また、リスト改訂に必要な調査及び検討を行う。

### （４）暗号モジュールに関する国際標準規格化への貢献

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

### （５）体制の見直しに関する検討

電子政府推奨暗号リストの改訂に向け、2009 年度後半に暗号の公募開始を予定していることから、これらに適切に対応していくため、必要に応じて体制の見直しに関する検討を行う。

**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<br>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

# 電子政府推奨暗号リスト改訂のための暗号技術公募要項（2009 年度）

CRYPTREC 事務局

2009 年 3 月 27 日

# 目次



**＜添付資料＞**

別紙 1 暗号技術応募書（提出資料 1）
別紙 2 誓約書（提出資料 6）
別紙 3 公開の状況等に関する情報（提出資料 7）
別紙 4 自己チェックリスト（提出資料 9）

## 1. 公募の概要

総務省及び経済産業省が開催している暗号技術検討会（座長：今井秀樹中央大学教授）では、電子政府利用等に資する暗号技術の評価等を行っており、2003年2月に発表した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（以下、「電子政府推奨暗号リスト」又は「現リスト」という。）の改訂を行うことを目的として、「電子政府推奨暗号リストの改訂に関する骨子(案)」（以下、「骨子案」という。）を作成し、2008年8月6日から2008年9月5日までの間、当該骨子案について意見募集[1]を行いました。

意見募集の結果[2]を踏まえ、CRYPTRECでは、「電子政府推奨暗号リスト改訂のための暗号技術公募要項（2009年度）」を策定しましたので、公表いたします。

（1）これを受けて、CRYPTREC は評価対象暗号技術を公募し、CRYPTREC 事務局の情報通信研究機構及び情報処理推進機構（以下、「事務局」という。）は、暗号技術評価を実施します。
（2）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します。その結果は、事務局が開催するワークショップ（「9．ワークショップ」を参照のこと。）や報告書等を通じて、一般に公表することを予定しています。応募者にとって不利益と解される情報を含むこともあり得ます。
（3）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します。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います。
（4）CRYPTREC 内に設置された「評価委員会（仮称）」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します。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ます。決定については、2012 年度実施を予定しています。なお、仮称付きの語句に関しては、「5．公募の目的」又は骨子案をご覧下さい。

## 2. 公募の対象

### 2.1. 暗号技術の種別

（1）共通鍵暗号技術

共通鍵暗号技術に関しては、以下の暗号技術の種別に属する方式を公募します。

a) 128bit ブロック暗号 （鍵長 128bit/192bit/256bit）
b) ストリーム暗号 （鍵長 128bit 以上）

[1] http://search.e-gov.go.jp/servlet/Public?CLASSNAME=Pcm1010&BID=145207347
[2] http://search.e-gov.go.jp/servlet/Public?ANKEN_TYPE=3&CLASSNAME=Pcm1090&KID=145207347

（2）メッセージ認証コード
鍵長が 128bit である 128bit ブロック暗号及び 64bit ブロック暗号を利用したメッセージ認証コードを公募します。

（3）暗号利用モード
秘匿に関する 128bit ブロック暗号及び 64bit ブロック暗号を対象とした利用モードを公募します。

（4）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です。

## 2.2. 応募暗号に関する留意事項

（1） ブロック暗号及びストリーム暗号については、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）を持つ技術に限ります。
（2） 同一の技術的根拠を有する方式に関しては、最善な方式を選択して、1 つの暗号技術の種別のみに応募して下さい。
（3） 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に限ります。
（4） 国内及び国外において評価が可能であり、かつ、第三者が全ての機能を実装可能となる情報を開示してあるものに限ります。評価を依頼する際に必須なものです。したがって、応募書類受付締切までに公知であることを明確にして下さい。なお、万一応募書類締切時点までに公知にできない理由がある場合には、2009 年 9 月末までに事務局へ相談して下さい。
（5） 評価する際に知的財産の利用が無償で行えるものに限ります。
（6） 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であることを条件とします。

## 3. 応募方法

（1）提出期限
2009 年 10 月 1 日から 2010 年 2 月 4 日 17 時（必着）までに情報通信研究機構・情報通信セキュリティ研究センター内 CRYPTREC 事務局宛てに郵送又は宅配便にて提出

して下さい。また、書類提出は、郵送又は宅配便でのみ受付け、応募者持参による受付は行いません。なお、送料は発信元払いでお願いします。

（2）提出物

提出書類（文書及び電子媒体）（「6．提出書類」を参照のこと。）を 1 つの封筒に入れ、「暗号技術応募」と表に朱記の上、提出して下さい。1 応募暗号技術につき 1 封筒での提出として下さい。

電子媒体については、全ての電子データを CD-R（ISO 9660 Level 1 又は Joliet 形式）にまとめて入れ、暗号技術名と応募者名を記入して下さい。なお、提出物については返却致しませんのでご了承下さい。

（3）応募に関する問い合わせ及び提出先

情報通信研究機構　情報通信セキュリティ研究センター内　CRYPTREC 事務局宛
〒184-8795　東京都小金井市貫井北町四丁目 2 番 1 号
e-mail：　info@cryptrec.go.jp
FAX：　042-327-5609
問い合わせの受付は e-mail 又は FAX のみとします（電話での問い合わせは、ご遠慮下さい）。

## 4．　応募に際しての留意事項

（1）応募に際しては、提出書類（「6．提出書類」を参照のこと。）に漏れが無いことを確認の上、応募者側で自己チェックリストを記入し、提出書類に添えて提出して下さい。
（2）別紙 2（p.22 参照）の誓約書を提出して下さい。
（3）本公募の実施に際し、事務局と応募者との間での金銭の授受は行いません。暗号技術の開発、書類の作成、自己評価その他の応募に際して応募者側で発生する費用、及び追加資料等の作成及び提出、実装性評価時の立会い等に際して応募者側で発生する費用は、応募者が負担して下さい。評価の委託その他の事務局側で発生する費用は事務局が負担します。
（4）評価者（外部評価者を含む）については、審査の公平性の観点から、応募者に対して開示しません。
（5）応募担当者は、適時連絡が取れ、日本語が話せる方として下さい。特に、応募書類受付締切から応募暗号説明会までの期間は、常時連絡が取れるようにお願いします。また、応募担当者の連絡先等に変更が生じる場合は、速やかに事務局へ暗号技術応募書（電子データ含む）の更新版を送付願います。
（6）提出資料の不備、暗号技術に関連する知的財産の実施・利用やライセンス上に問題がある等、評価の実施が困難であると事務局が判断した場合には、応募資格を喪失する場合がありますのでご了承下さい。

## 5. 公募の目的

### 5.1. 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」という。）を発表しました。

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ました。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ました。

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ます。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ります。

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ります。

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やすさや導入コスト、相互運用性、普及度合い等の観点も取り入れる必要性が指摘されているところです。

これらの状況を踏まえ、2013 年度以降の電子政府における暗号技術の利用に当たり、信頼性のある暗号技術のリストとして、現リストの改訂を行います。この結果は、電子政府において暗号技術を利用する際の参考として様々な形で利用されることが期待されます。

### 5.2. 新しい CRYPTREC 暗号リストの構成と本公募の位置づけ

先に述べた背景に従い、2013 年度から、推奨する暗号のリストのみから構成される現リストから、新たな推奨暗号の体系に移行する予定です。

今回の見直しに合わせて、下記の（1）～（3）の各リスト及び(4)リストガイドをまとめて「CRYPTREC 暗号リスト（仮称）」（以下、「次期リスト」という。）として公開します。

(1) 電子政府推奨暗号リスト（仮称）
(2) 推奨暗号候補リスト（仮称）
(3) 互換性維持暗号リスト（仮称）
(4) リストガイド

CRYPTREC により安全性が確認された暗号技術は、（1）～（3）の 3 つのリストのいずれかに登録されます。各リストへの登録は、WTO 政府調達協定との整合性に配慮し

つつ、安全性や市場動向により決定されます。登録の見直しは一定の間隔で行います。
　現リストに掲載されている暗号技術については、安全性の再評価を行った上で次期リスト運用開始前に推奨暗号候補リスト（仮称）へ登録されていたものとして扱います。次期リスト運用開始時には、新たに応募された技術と共に製品化の状況・技術の利用状況等により電子政府推奨暗号リスト（仮称）へ登録するか否かの決定を行います。

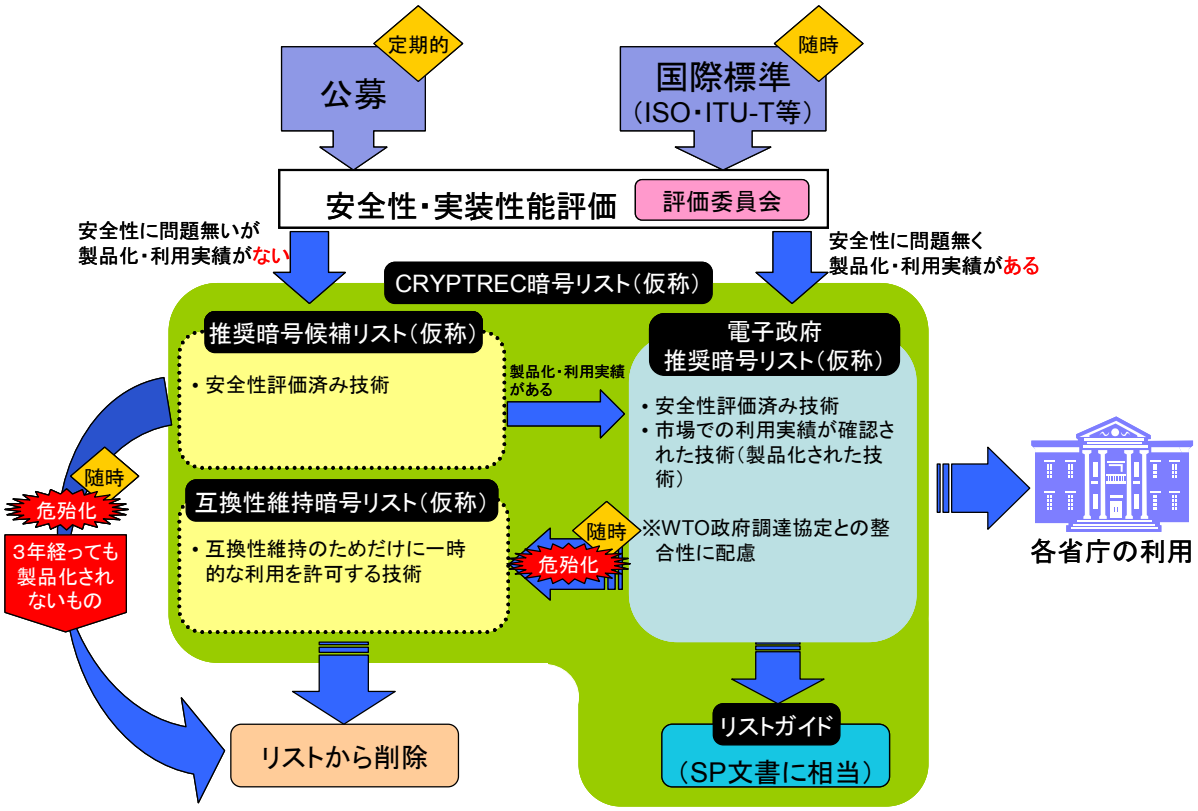


図 1．リスト改訂概念（案）

次期リストにおけるそれぞれのリストの役割は以下のとおりです。

(1) 電子政府推奨暗号リスト（仮称）

　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します（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ます。

(2) 推奨暗号候補リスト（仮称）

　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ます。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ます。

本リストに登録された技術は、一定期間ごとに普及の度合いの調査を行い、利用実績が十分であると認められれば電子政府推奨暗号リスト（仮称）に登録されます。また、利用実績が十分であると認められなかった場合にはここから削除されます。危殆化が生じた暗号技術については、随時ここから削除されます。

(3) 互換性維持暗号リスト（仮称）

電子政府推奨暗号リスト（仮称）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します。CRYPTREC として互換性維持以外の目的では利用を推奨しません。

(4) リストガイド

電子政府で利用されている、あるいは利用する可能性のある暗号技術について、その技術概要と、推奨する利用方法を記述します。また、次期リストに記載された技術の中で、安全性を維持するため正しいパラメータの設定が要求される技術における具体的なパラメータ設定方法の記述を行います。さらに、将来必要になると予想されるセキュリティ技術については、その開発状況や利用可能性について記載します。リストガイドは、システム運用者及び設計者の利用や、システム利用者への啓発を目的とします。

今回の暗号技術の公募は、現リストにおいて早期にリストの改訂が必要である技術カテゴリを対象として、推奨暗号候補リスト（仮称）、あるいは電子政府推奨暗号リスト（仮称）へ登録するための、安全性及び実装性の評価を行うことを目的に行います。

## 6. 提出書類

今回の応募に際して必要な提出書類は以下のとおりです。なお、提出された情報については、CRYPTREC 統一 Web サイト（http://www.cryptrec.go.jp/）にて公開する予定です。

| 項番 | 提出書類 | 1.記述言語<br>2.提出形式 | 作成要領の書式 | 電子データのファイル名 | 参照ページ |
|---|---|---|---|---|---|
| 6.1 | 暗号技術応募書 | 1.和文及び英文<br>2.文書及び電子データ | 別紙 1 | 和文:09appl_j.pdf<br>英文:09appl_e.pdf | 9 |
| 6.2 | 暗号技術仕様書 | 1.和文及び英文<br>2.文書及び電子データ | なし | 和文:09spec_j.pdf<br>英文:09spec_e.pdf | 9 |
| 6.3 | 自己評価書 | 1.和文及び英文<br>2.文書及び電子データ | なし | 和文:09eval_j.pdf<br>英文:09eval_e.pdf | 10 |
| 6.4 | テストベクトル | 2.電子データのみ | なし | 半角英数で、任意 | 11 |
| 6.5 | 参照ソースコード | 1.英文<br>2.電子データのみ | なし | 半角英数で、任意 | 12 |
| | 参照ソースコード仕様書 | 1.和文及び英文<br>2.文書及び電子データ | なし | 和文:09sref_j.pdf<br>英文:09sref_e.pdf | |
| | 参照ハードウェア設計記述 | 1.英文<br>2.電子データのみ | なし | 半角英数で、任意 | |
| | 参照ハードウェア設計記述仕様書 | 1.和文及び英文<br>2.文書及び電子データ | なし | 和文:09href_j.pdf<br>英文:09href_e.pdf | |
| | テストベクトル生成ソースコード | 1.英文<br>2.電子データのみ | なし | 半角英数で、任意 | |
| | テストベクトル生成ソースコード仕様書 | 1.和文及び英文<br>2.文書及び電子データ | なし | 和文:09tvec_j.pdf<br>英文:09tvec_e.pdf | |
| 6.6 | 誓約書 | 1.和文<br>2.文書の原本 | 別紙 2 | なし | 13 |
| 6.7 | 公開の状況等に関する情報 | 1.和文<br>2.文書及び電子データ | 別紙 3 | 和文:09publ_j.pdf | 13 |
| 6.8 | 応募暗号説明会発表資料 | 1.和文及び英文<br>2.文書及び電子データ | なし | 和文:09brfg_j.pdf<br>英文:09brfg_e.pdf | 14 |
| 6.9 | 自己チェックリスト | 1.和文<br>2.文書の写し | 別紙 4 | なし | 14 |

表 1．提出書類一覧

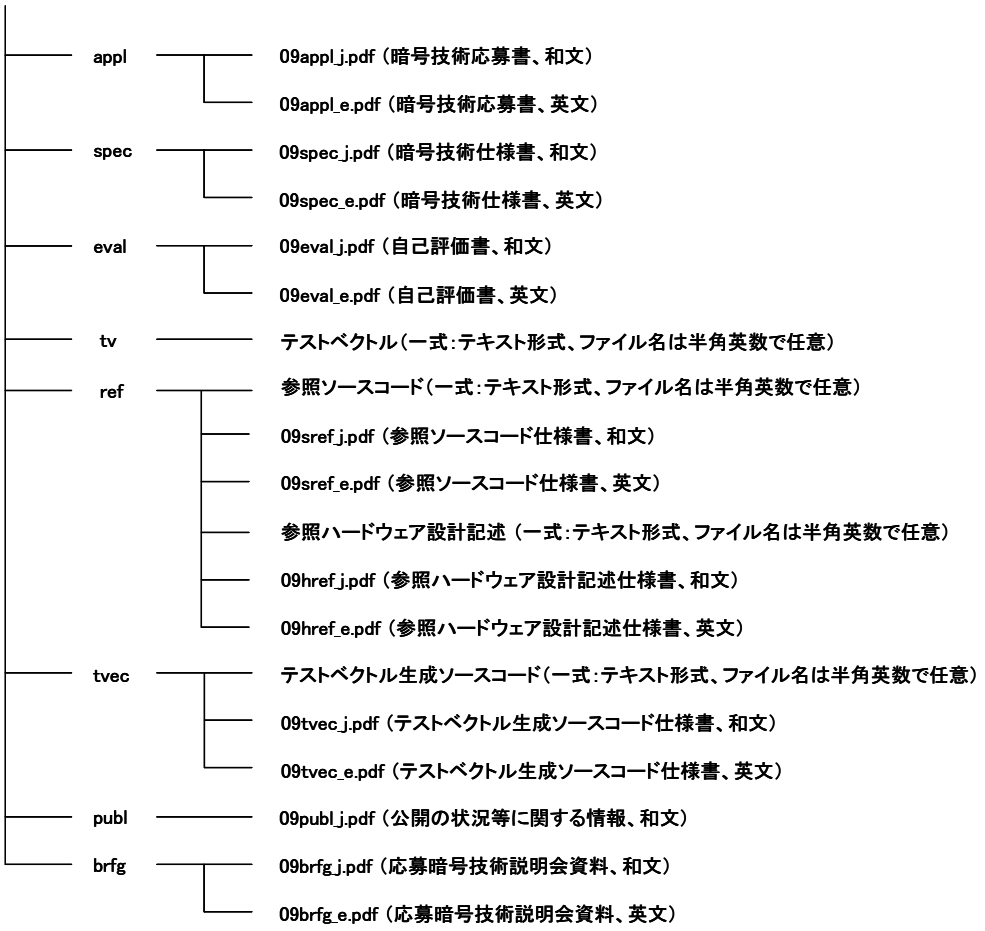


**図 2．提出書類（電子データ）の構成図**

**ⅰ）提出書類となる各種電子ファイルは、上に示すようなファイル名（半角英数）をつけて下さい。**

**ⅱ）電子ファイルは、それぞれ上に示すようなディレクトリを作成し、対応するディレクトリ直下に保存して下さい。（ディレクトリ名は半角英数）**

**注）**

**○文書については、全て日本工業規格 A4 判として下さい。**

**○6.1～6.3、6.5 及び 6.8 は、和文・英文両方の提出が必要です。和文を正文とし、両者の内容に齟齬があった場合は和文を優先しますが、可能な限り同一の内容として下さい。評価の実施に関して支障が出る場合には応募資格を喪失することもあり得ます。**

**○6.1～6.3、6.5、6.7 及び 6.8 のファイル形式については、以下のものとし、表 2 に示したファイル名を使用して下さい。**

**・Adobe PDF 形式**

**日本語版：Adobe Acrobat 日本語フォントで読めるもの**

**英語版：Adobe Acrobat で読めるもの**

**○6.4 及び 6.5 のプログラムの電子データについては、テキスト形式として下さい。**

**○評価においては国外における評価も想定していますので、提出書類のうち 6.1～6.3、6.5 及び 6.8 の電子媒体については、全ての電子データを CD-R(ISO 9660 Level 1 又**

は Joliet 形式)にまとめて入れ、暗号技術名と応募者名を記入して下さい。

それぞれの提出書類について、以下に説明します。

### 6.1. 暗号技術応募書（別紙 1 の書式）

ⅰ）応募日
・応募書提出日を記入して下さい。

ⅱ）暗号技術名
・正式名称を読み方も含めて記述して下さい。また、正式名称が長い場合は、略称名を 5 文字程度のアルファベット表記で記述して下さい。

ⅲ）応募暗号技術公開ホームページ URL
・国内外の暗号技術者が、評価を行う際に必要となるデータを参照できるホームページ URL を記入して下さい（和文及び英文）。

ⅳ）応募暗号種別
・該当する項目を 1 つだけ選択して下さい。

ⅴ）応募責任者
・今回の応募に関する一切の責任を負う方とします。
・本応募に関する責任者の企業・団体名、所属・役職及び氏名を記入して下さい。

ⅵ）応募担当者
・今回の応募に関し、事務局との問い合わせ・連絡窓口となる方とします。
・本応募担当者は、日本語が話せる方として下さい。
・応募担当者の氏名、企業・団体名、所属・役職、所在地、電話番号（代表、直通を明記)、FAX 番号及び e-mail アドレスを記入して下さい。

ⅶ）開発者
・開発者の氏名及び企業・団体名を記入して下さい。

ⅷ)応募暗号調達窓口
・次期リスト策定後 3 年以内までに調達可能であることが応募条件であることから、応募暗号技術を調達する場合の窓口（連絡先）を記述して下さい。
・応募時点で正式な調達窓口が設置されていない場合においても、調達に関する問い合わせに答えられる仮窓口を記述して下さい。

ⅳ)応募暗号説明会
・応募暗号説明会における発表予定者名、参加人数を記述して下さい。

### 6.2. 暗号技術仕様書

ア　設計方針、設計基準
ⅰ)応募暗号技術についての設計方針及び設計基準を記述して下さい。
ⅱ)共通鍵暗号の場合は、現リストに記載された暗号技術と同等以上の特長（安全性又は実装性等）についても記述して下さい。

イ　暗号アルゴリズム（実装に必要な全情報）
第三者が評価・実装するために十分な仕様が完全に記述されていることが必

要です。記述が十分でない場合、応募資格を喪失することがあります。具体的には以下に従って下さい。

ⅰ）暗号アルゴリズムの完全な仕様を記述して下さい。アルゴリズムの実装に必要なすべての情報（数式、テーブル、アルゴリズム、図及びパラメータ）を記述して下さい。

ⅱ）暗号鍵等のパラメータの設定に条件がある場合には、パラメータの設定基準、推奨値も記述して下さい。

ⅲ）共通鍵暗号で複数の鍵長をサポートする場合には、互換性の有無に関しても明記して下さい。

ⅳ）応募技術の入出力は、ビット列レベルで記述して下さい。

ⅴ）入力が Z/nZ（Z は有理整数環）の元等、実装する上で実現法が一意に定まらない場合は、ビット列への変換法の推奨方式も同時に提示して下さい。

ⅵ）endian の種類を記述して下さい。

ⅶ）高速実装やコンパクト実装に関する方法等があれば記述して下さい。

ⅷ）実装方法についての説明

本応募暗号技術を実装するために必要な実装手順等の情報を記述して下さい。

情報が不十分であるために実装ができない場合には、応募資格を喪失することがあります。

また、評価に必要な情報の追加提出を求めることがあります。

ウ　バージョン情報

今回の応募以外に、同一若しくは類似した名称で他に発表又は応募した暗号技術、同一仕様で名称が異なった暗号技術等があれば列挙して下さい。

また、それぞれの相違点を明記して下さい。また、バージョン更新時に推奨パラメータが変更された場合には、変更した理由を明記して下さい。

バージョンの更新について、設計思想、安全性及び実装性の違いを明確に記述して下さい。また、バージョン更新をした理由についても明記して下さい。

異なるバージョン間における互換性の有無を完全に記述して下さい。バージョンが異なる場合に想定されるユーザー側のメリット及びデメリットについても記述して下さい。

エ　利用実績・推奨用途等

応募暗号技術に係る利用実績や推奨用途について記述して下さい。

### 6.3. 自己評価書

応募される暗号技術に対する応募者自身による自己評価情報を記述して下さい。自己評価が十分でないと判断される場合には、応募資格を喪失することがあります。

また、ウ・エ・オ・カの項目については詳細に記述して下さい。

ア　設計思想

他の著名な暗号技術との差別化、優位性等も含め記述して下さい（既存の技術と比べて優位性がある部分、提案技術が電子政府で使用するものとして妥当であると考えられる部分等）。

イ　ベースとして用いる理論（数学的仮定）・技術

応募される暗号に、ベースとして用いられている理論（数学的仮定）や技術について記述して下さい。

ウ　安全性に対する評価

応募される暗号の安全性に関する根拠及び通常想定される汎用的な攻撃法に対する対抗策を具体的に示して下さい。

想定する攻撃法に関しては、「7．評価項目」を参考にして下さい。なお、評価項目に例示されている攻撃法が適用できない場合には、評価は必要ありませんが、その攻撃法が適用できないと判断した理由を明示して下さい。但し、全く自己評価がなされていない場合は、応募資格を喪失する場合があります。

応募暗号に固有の特殊な攻撃法が想定される場合には、その攻撃法に対し施した対抗策についても具体的に提出して下さい。

提案方式に対する既知の攻撃論文の有無や学会(ASIACRYPT、CRYPTO、EUROCRYPT、FSE、ISEC、PKC、SCIS 等)等で攻撃や問題点が指摘されている場合には、その攻撃論文を引用し、これに対する技術的コメントを記述して下さい。

証明可能安全性を主張する場合にはそのレベルを記述し、その論証を行うか、学会等で発表されているならその論文等について記述して下さい。

エ　ソフトウェアの実装性評価

速度評価、リソース使用量（コード量・ワークエリア）、記述言語、評価プラットホーム等を記述して下さい。また、実際に速度計測を行った場合には、計測法を詳細に記述して下さい。

※ブロック暗号に関しては、鍵スケジュール部単独の速度評価結果も記述して下さい。

オ　ハードウェアの実装性評価

使用したプロセス（Field Programmable Gate-Array、Gate-Array 等）、速度評価、設計環境、リソース使用量（Field Programmable Gate-Array の場合は使用セル量、Gate-Array 等の場合はゲート数）等を記述して下さい。

※ エンティティ認証は対象外です。

カ　サイドチャネル攻撃に対する評価

本項目は、自己評価書の提出に当たっては必須ではありませんが、サイドチャネル攻撃に対する耐性を主張する場合には、攻撃法、施した対抗策及び動作環境等についてできるだけ詳しく記述して下さい。学会等で発表されているならその論文等について記述して下さい。

キ　第三者評価実績

既に第三者評価を受けた実績がある場合には、評価者名及び評価結果を記述して下さい。開示可能であれば、報告書のコピーもあわせて（できるだけ電子データで）添付して下さい。

## 6.4. テストベクトル

実装性確認のために十分な量のテストベクトルを記述して下さい。十分な量のテストベクトルが提出されないときには応募資格を喪失することがあります。テストベクトルは暗号処理途中の中間結果と、暗号全体をブラックボックスと見な

したときの入出力対の 2 種類を提出して下さい。どちらのファイルもテキスト形式で生成し、キャラクタセットとしては ASCII のみを使って下さい。改行コードは MS-DOS 形式(CR+LF)とします。

暗号処理途中の中間結果については、応募暗号技術を第三者が実装する上でデバッグの役に立つ情報について、少なくとも入出力 1 対に対応するデータをなるべく詳しく記述して下さい。例えば、共通鍵暗号については繰り返し処理ごとの入出力等を記述して下さい。

暗号全体をブラックボックスと見たときの入出力対については、以下に示す応募する暗号技術ごとの方針に従って下さい。どの暗号技術についても、テストベクトルには endian の間違い等ビット列表記が反転した場合等を検出できるデータを含む等、テストベクトルとして相応しい入出力を選んで下さい。

乱数を用いる場合は、再度検証可能なように、擬似乱数生成系を用い、種(Seed)を明示して下さい。

ア　共通鍵暗号技術

ⅰ)ストリーム暗号

10 例以上の鍵に対し、8192bit 以上の処理例

ⅱ)ブロック暗号

10 例以上の鍵に対し、128 ブロック以上の処理例

イ　メッセージ認証コード

3 例以上の鍵に対し、3 例以上の処理例

ウ　暗号利用モード

3 例以上の鍵に対し、3 例以上の処理例

エ　エンティティ認証

共通鍵暗号を利用する場合には、3 例以上の鍵に対し、3 例以上の処理例。テストベクトルには、ランダムに生成されたデータを含んで下さい。

公開鍵暗号を利用する場合には、3 例以上の鍵に対し、3 例以上の処理例。テストベクトルには、ランダムに生成されたデータを含んで下さい。また、ベキ乗剰余等の数学的構造を含む場合は、境界条件となるデータを含んで下さい。

なお、再度検証可能なように、擬似乱数生成系を用い、種（Seed）を明示して下さい。

## 6.5. 参照ソースコード

ⅰ） 応募暗号技術の実装が実際に可能であることを確認するため、また応募暗号技術に関連する各種データの正当性の効率的な検証を可能とするために参照ソースコードとその仕様書を提出して下さい。

参照ソースコードは、ソフトウェアの実装性評価向けには ANSI C で、ハードウェアの実装性評価向けには Verilog-HDL で記述して下さい。なお、この目的を達成するため、参照ソースコードを見難くするような、処理中の機微データをゼロクリアする等の安全性を高めるような部分を記述する必要はありません。

ⅱ） 参照ソースコードでは、推奨パラメータを含む応募暗号技術の全ての機能を

実現して下さい。さらに、参照ソースコードの可読性を落とさない範囲で移植性の高いものとして下さい。例えば、ソフトウェア評価の場合には、endian 非依存とし、最低限 int、long、pointer の長さが 32bit の処理系で動くように作成して下さい。多倍長整数を利用する場合は GNU MP ライブラリなどの利用を推奨します。

iii) テストベクトル生成ソースコードとその仕様書も提出して下さい。テストベクトル生成プログラムは参照ソースコード中の関数を呼び出すものとします。

### 6.6. 誓約書（別紙 2 の書式）

本項目に関しては、別紙 2 の書式に従って記述して下さい。提出がない場合には、応募資格を喪失しますのでご留意下さい。

### 6.7. 公開の状況等に関する情報（別紙 3 の書式）

本項目に関しては、別紙 3 の書式に従い下記ア～ウの内容について記述して下さい。

ア　応募暗号技術の公開時期とその学会名

本公募では、仕様等が公開されている暗号技術を評価対象としていますので、仕様等の公開の状況を確認するために必要な情報（応募暗号技術が公開された時期、学会名、あるいは掲載文献名等）を提出して下さい。なお、応募時点で仕様等の公開がなされていない場合には、その時点での状況とともに、2010 年 9 月末までの公開スケジュールを提出し、応募暗号技術に関する論文発表や仕様書等の公開された際には、その状況を確認するために必要な情報を提出して下さい。

イ　輸出規制問題を解決していることの宣誓書とその証拠

応募された暗号技術の評価については、事務局より評価の一部を海外を含めた評価者に外部委託することを予定しており、提出された情報を我が国の非居住者である委託者に提供すること等も予想されます。このため、「6. 提出書類」の 6.1～6.5 及び 6.7 の情報のそれぞれについて、非居住者への提供等に際して輸出管理上許可が不要であると考える場合には、その根拠及び確認のための文書を提出して下さい（例えば、学会誌、雑誌、論文集等で既に公開されており不特定多数の方が自由に入手できる情報であるため許可不要と考える場合には、当該学会誌、雑誌、論文誌等の関連部分等を提出するとともに、公開形態についての説明を加えて下さい）。

ウ　知的財産権とライセンス

応募された暗号技術に関して取得あるいは出願中の特許、著作権、ライセンス方針等の知的財産に関する状況を応募書類の「自社特許とその扱い」の中で記述して下さい。

応募された暗号技術に関連し、他社が特許権、著作権等の知的財産を保有する場合、それらの権利関係についても、応募書類の「関連する他社の特許」の

中で可能な範囲で記述して下さい。

事務局及び評価者が評価の実施に際して必要となる知的財産の利用（特許法上の発明の実施、著作権法上の著作物（全ての応募書類）の複製・領布等、事務局が評価を委託する第三者による利用を含む）を無償で行えることを明記して下さい。知的財産上の制限により評価の実施が妨げられる場合は、応募資格を喪失することがあります。

また、政府機関で使用する場合のライセンス方針を記述して下さい（無償又は、妥当かつ非差別的な条件に限ります）。

なお、評価のために、事務局及び評価者が応募者と、秘密保持契約等の特別な契約を結ぶことはいたしません。

### 6.8. 応募暗号説明会資料

応募される暗号技術についての説明資料を作成し、Adobe PDF 形式にて提出して下さい。資料構成としては、以下を参考にし、説明内容は 15 分程度のもので作成して下さい。なお、白黒のハードコピーが配布資料となることにご留意下さい。

<資料構成>

１．表紙（応募暗号名、発表者名を記載）
２．技術仕様について
３．安全性に関する自己評価について
４．実装性に関する自己評価について
５．公開状況、ライセンス等について

### 6.9. 自己チェックリスト（別紙 4 の書式）

「自己チェックリスト」に従って内容を確認して下さい。このチェック結果を記入した「自己チェックリスト」の写しを、提出物と同じく封筒に入れて提出して下さい。

# 7.　評価項目

## 7.1.　評価スケジュール（予定）

| | |
|---|---|
| 応募暗号説明会開催： | 2010 年 3 月頃 |
| 第 1 次評価実施： | 2010 年 4 月～2011 年 3 月 |
| 第 1 回ワークショップ開催： | 2011 年 2 月頃 |
| 第 2 次評価実施： | 2011 年 4 月～2012 年 3 月 |
| 第 2 回ワークショップ開催： | 2012 年 2 月頃 |
| 2012 年度シンポジウム： | 2013 年 2 月頃 |

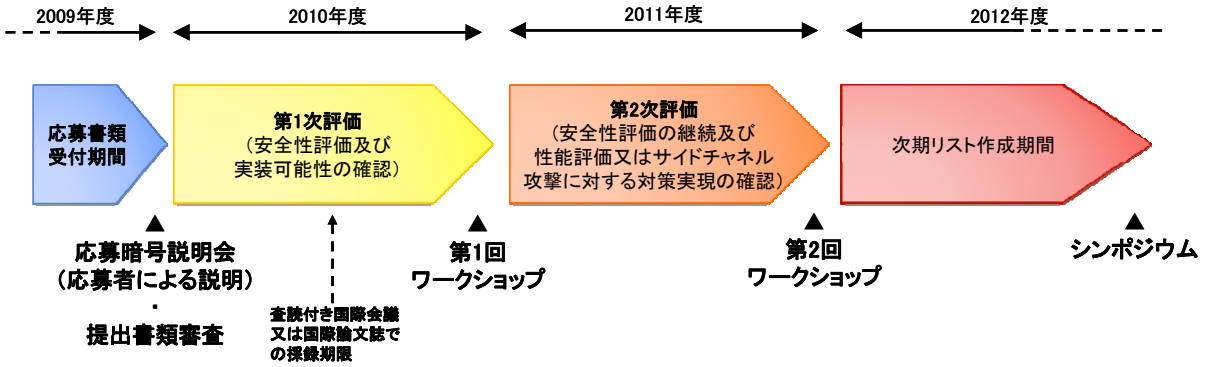


図 3．評価スケジュール（予定）

## 7.2.　共通鍵暗号技術

共通鍵暗号については、現リストに掲載されている暗号技術と比較して安全性又は実装性において優れた暗号技術を公募します。そのため、評価においても現リストに掲載された暗号に対する優位点の評価を行います。

（１）安全性評価項目

暗号は守秘目的以外にも利用されるので、いわゆる暗号文単独攻撃以外の既知平文攻撃、(適応的)選択平文・暗号文攻撃、関連鍵攻撃、選択IV攻撃等、攻撃者にとって非常に都合のよい環境での耐性も評価します。

ア　ブロック暗号に関する評価項目

差分攻撃法や線形攻撃法等の既知の一般的な攻撃法に対する耐性を評価します。また、応募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ります。その他、サイドチャネル攻撃等に対する耐性についても評価します。

イ　ストリーム暗号に関する評価項目

time/memory/data-tradeoffや分割統治攻撃、相関攻撃、またGroebner基底計算アルゴリズムを元にした代数攻撃等の既知の攻撃法に対する耐性を評価しま

す。また、応募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ります。その他、サイドチャネル攻撃等に対する耐性についても評価します。

（2）実装性評価項目

ア　共通条件

「7.6 実装性評価について」を参照して下さい。

イ　ソフトウェア実装による評価項目

ソフトウェア実装に関しては、次の項目について評価します。

ⅰ）標準的なプラットホーム上での処理速度、リソースの使用量（コード量、作業領域等）等を評価します。

ⅱ）鍵スケジュール個別の処理速度も評価します。

ウ　ハードウェア実装による評価項目

使用するプロセス（Field Programmable Gate-Array、Gate-Array 等）別に、処理速度評価及びリソースの使用状況（Field Programmable Gate-Array の場合には使用セル数、Gate-Array 等の場合には使用ゲート数等）を評価します。

## 7.3. メッセージ認証コード

（1）安全性評価項目

利用ブロック暗号をもとにした証明可能安全性、特に適応的選択文書攻撃や、検証オラクルを多数回呼び出したときの識別不能性について評価します。また、nonce や乱数要素の有無についても評価します。さらに利用ブロック暗号に対する仮定の強さ(ideal cipher modelや関連鍵攻撃耐性)についても評価します。さらに、利用ブロック暗号に特定の方式を適用した場合の安全性についても評価の対象とすることがあります。

（2）実装性評価項目

ア　共通条件

「7.6 実装性評価について」を参照して下さい。

イ　ソフトウェア実装による評価項目

ソフトウェア実装に関しては、次の項目について評価します。

ⅰ）標準的なプラットホーム上での処理速度、リソースの使用状況（コード量、作業領域等）等を評価します。

ⅱ）鍵スケジュール個別の処理速度も評価します。

ウ　ハードウェア実装による評価項目

使用するプロセス（Field Programmable Gate-Array、Gate-Array 等）別に、処理速度評価及びリソース使用量（Field Programmable Gate-Array の場合には使用セル数、Gate-Array 等の場合には使用ゲート数等）を評価します。

## 7.4. 暗号利用モード

（1）安全性評価項目

利用ブロック暗号をもとにした証明可能安全性、特に適応的選択平文・暗号文攻撃に対する識別不能性について評価します。また、nonceや乱数要素の有無についても評価します。さらに利用ブロック暗号に対する仮定の強さ(ideal cipher modelや関連鍵攻撃耐性)についても評価します。さらに、利用ブロック暗号に特定の方式を適用した場合の安全性についても評価の対象とすることがあります。

（2）実装性評価項目

ア　共通条件

「7.6 実装性評価について」を参照して下さい。

イ　ソフトウェア実装による評価項目

ソフトウェア実装に関しては、次の項目について評価します。

ⅰ）標準的なプラットホーム上での処理速度、リソースの使用状況（コード量、作業領域等）等を評価します。

ⅱ）鍵スケジュール個別の処理速度も評価します。

ウ　ハードウェア実装による評価項目

使用するプロセス（Field Programmable Gate-Array、Gate-Array 等）別に、処理速度評価及びリソース使用量（Field Programmable Gate-Array の場合には使用セル数、Gate-Array 等の場合には使用ゲート数等）を評価します。

## 7.5. エンティティ認証

（1）安全性評価項目

安全性の評価は、エンティティ認証としてのセキュリティに問題が生じないことを、形式的な手法を用いて行います。安全性を脅かす状態としては、なりすましの成功、セッションの取り換え等を想定します。

暗号プリミティブとして、電子政府推奨暗号リストに掲載されている、あるいは応募中の共通鍵暗号、公開鍵暗号、ハッシュ関数、メッセージ認証コードのみを利用している場合には、暗号プリミティブを理想的に安全なものとして安全性の評価を行います。その他の暗号プリミティブを用いる場合には、暗号プリミティブを理想化せずに安全性の検証を行います。

上記のいずれの場合も、提案者はプロトコルの安全性を示す情報を提出し、本公募における安全性評価では、これらの正当性を検証します。

（2）実装性評価項目

エンティティ認証プロトコルの実装性能評価として、ソフトウェアによる実装性評価を行います。標準的なプラットホーム上での処理速度、リソースの使用状況（コード量、作業領域等）等を評価します。通信時間は考慮しません。

ア　共通条件

「7.6 実装性評価について」を参照して下さい。

## 7.6. 実装性評価について

実装性評価について共通的な条件を記述します。実装性評価を行う目的は、

- 実現可能性の確認、
- 性能の評価
- サイドチャネル攻撃に対する対策実現の確認

の 3 つです。

（1）実現可能性の確認

- 提案された暗号アルゴリズムが、事務局が指定した動作環境において実装可能であり、かつ、動作可能であることを確認することが目的です。応募時に提出されたテストベクトルを処理できることを確認します。第 1 次評価期間内に実施します。
- 実現可能性の確認で用いた参照ソースコード及び参照ハードウェア設計記述は、性能の評価には利用しませんが、第三者が実装する場合の参考として公開する予定です。想定している動作環境は、以下のとおりです。
- 暗号利用モード及びメッセージ認証コードの実装性評価では、128bit ブロック暗号及び 64bit ブロック暗号を使用するものとします。ここで用いるブロック暗号は、事務局から提供します。

（i） ソフトウェアでの実現可能性の確認のための動作環境

- CPU: Intel x86 アーキテクチャ互換のプロセッサ
- Memory: 2GB 以上
- OS: Microsoft Windows のいずれかのエディション

（ii）ハードウェアでの実現可能性の確認のための動作環境

- FPGA： Xilinx FPGA XC5VLX30、もしくは、XC5VLX50

また、設計環境としては以下のとおりです。

（i） ソフトウェアでの実現可能性の確認のための設計環境

- 記述言語： ANSI-C 言語
- Compiler: Microsoft Visual Studio

（ii）ハードウェアでの実現可能性の確認のための動作環境

- 設計記述言語： Verilog-HDL
- 論理合成： Xilinx ISE Foundation
- 配置配線： Xilinx ISE Foundation
- 論理シミュレーション： Mentor Graphics ModelSim

### （2）性能の評価

- 性能の評価は、安全性評価及び実現可能性の確認を通過し、次期リストへの掲載が可能と判断された暗号技術に対して第 2 次評価期間内に実施します。
- 性能の評価を行う動作環境については、実現可能性の確認で使用する動作環境に準じるものを想定していますが、性能の評価を実施する上で必要となる情報は、安全性評価及び実現可能性の確認の段階（2010 年 10 月頃）で、公開する予定です。
- 性能の評価で使用する実装については、事務局からソースコードの提出を要求しませんが、事務局が指定する動作環境にて実行可能なロードモジュールを応募者側で実装して頂き、事務局立会いにて実地で測定を行うことを想定しています。詳細については、2010 年度末までに 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す。
- ソフトウェアの性能の評価に関しては、通常の PC 環境における性能を測定します。各暗号技術の種別毎の評価項目については、7.2 から 7.5 の該当する評価項目を参照して下さい。処理速度のほか、リソース使用量（静的メモリ量、動的メモリ量）の評価を想定しています。
- ハードウェアの性能の評価に関しては、FPGA 環境における性能をシミュレーションにより測定します。回路規模、クリティカルパス遅延及びスループットの測定を想定しています。

### （3）サイドチャネル攻撃に対する対策実現の確認

- サイドチャネル攻撃に対する対策を実装アルゴリズムで実現できることを確認することが目的です。ソフトウェア実装及びハードウェア実装の両方を対象とします。第 2 次評価期間内に実施します。
- 原則として、提出された自己評価書に記述された対策技術を確認の対象としますが、応募書類提出後に学会又は論文誌に採録された応募暗号に関する対策についても、脅威の重要度・実現性等を考慮して、評価委員会（仮称）が別途認めたものを確認の対象とすることがあります。
- サイドチャネル攻撃に対する対策実現の確認で使用する実装については、事務局からソースコードの提出を要求しませんが、事務局が指定する動作環境にて実行可能なロードモジュールを応募者側で実装して頂き、事務局立会いにて実地で測定を行うことも想定しています。詳細については、2010 年度末までに 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す。

## 8. 応募暗号説明会について

応募された暗号技術の評価を開始するにあたり、応募者自ら公の場で、応募暗号技術の技術仕様、安全性、実装性、公開状況、及びライセンス等について説明する機会を設けます。本説明会は一般公開とし、全応募者が説明することを原則とします。

説明時間を 15 分程度、質疑応答時間を 10 分程度取ることを予定していますが、応募者数が多い場合には短くなることがあります。

正式日程などの詳細については、2009 年 10 月頃に 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す。

## 9. ワークショップについて

ワークショップ（「7.1 評価スケジュール（予定）」を参照のこと。）は、開催時点までの評価委員会（仮称）における最新の評価結果を公表し、それらを検討する場を設けるために開催されます。この機会を利用して、応募者が自らの意見を述べることもできます。

第 1 次評価実施期間（2010 年 4 月～2011 年 3 月）の後に開催予定の第 1 回ワークショップでは、応募暗号技術の安全性評価及び実現可能性の確認結果を公表する予定です。

第 2 次評価実施期間（2011 年 4 月～2012 年 3 月）の後に開催予定の第 2 回ワークショップでは、第 1 次評価実施期間後に継続して実施された安全性評価、性能の評価及びサイドチャネル攻撃に対する対策実現の確認結果を公表する予定です。また、現リストに掲載されている暗号技術に関する再評価の結果も公表する予定です。

詳細については、各年度の 10 月頃に正式日程を 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す。

## 10. シンポジウムについて

シンポジウム（「7.1 評価スケジュール（予定）」を参照のこと。）は、それまでに実施されてきた電子政府推奨暗号リストの改訂、暗号技術公募と評価活動及び次期リスト策定に関して、広く一般に報告するために開催することを想定しています。詳細については、確定し次第、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す。

以　上

（別紙 1）

| 受付番号 | |
|---|---|

応募日　20　　年　　月　　日

CRYPTREC 事務局　御中

# 暗号技術応募書（提出資料 1）

| | | | |
|---|---|---|---|
| 暗号技術名： | | | 略称名： |
| 応募暗号技術公開ホームページURL： | | | |
| 応募暗号種別 | | | |
| １．共通暗号技術 | a)128bitブロック暗号　b)ストリーム暗号 | | |
| ２．メッセージ認証コード | | | |
| ３．暗号利用モード | | | |
| ４．エンティティ認証 | | | |
| 応募責任者 | | | |
| 企業・団体名： | | | |
| 責任者氏名： | 印 | 所属・役職： | |
| 応募担当者 | | | |
| 企業・団体名： | | | |
| 担当者氏名： | | 所属・役職： | |
| 所在地：〒 | | | |
| TEL：（代表） | | （直通） | |
| FAX: | | e-mail: | |
| 開発者 | | | |
| 開発者名： | | 企業・団体名： | |
| 応募暗号調達窓口 | | | |
| 担当者氏名： | | 所属・役職： | |
| 企業・団体名： | | 所在地：〒 | |
| TEL: | FAX: | e-mail: | |
| 応募暗号説明会 | | | |
| 発表者氏名： | | 参加人数： | |
| TEL: | FAX: | e-mail: | |

（別紙 2）

CRYPTREC 事務局宛

# 誓約書（提出資料 6）

このたび、「電子政府推奨暗号リスト改訂のための暗号技術公募」への応募にあたり、以下の事項について、ここに誓います。

記

1. 応募暗号技術○○○○○○○○に関するすべての技術は公知であり、提出書類を国外の評価者等に提供することは輸出管理上の許可が不要であること
2. 応募暗号技術○○○○○○○○の評価において、事務局との間において金銭等の授受を行わないこと
3. 応募暗号技術○○○○○○○○に係る評価を行う際に、当該暗号技術に関連する特許権、著作権等の知的財産の実施・利用について、CRYPTREC 検討会事務局（外部評価者を含む）に対して、無償で通常実施権や利用許諾等を与えること。
4. 応募暗号技術○○○○○○○○に関する特許権、著作権等の知的財産については、それを利用する製品等に対して、無償又は妥当かつ非差別的な条件で、通常実施権、利用許諾等を与えること
5. 応募暗号技術○○○○○○○○の評価において、不利益と解される情報を含むことがあっても異議を申し立てないこと
6. 応募暗号技術○○○○○○○○が、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い場合には、応募資格を喪失することに異議を申し立てないこと
7. 応募暗号技術○○○○○○○○を使用する製品は、｛既に製品化され調達可能になっている／CRYPTREC 暗号リスト（仮称）策定後 3 年以内に製品化がなされるよう鋭意努力する｝こと
8. 応募暗号技術○○○○○○○○の評価結果の如何に関わらず、CRYPTREC 暗号リスト（仮称）に掲載されなくても異議を申し立てないこと

20○○年○月○日

応募暗号責任者
会社名・部署名　○○○○○○○○
住　所　○○○○○○○○丁目○番○号
氏　名　○○○○○○　　印

以　上

（別紙 3）

各項目の記入スペースの配分は応募者の任意とします。1 ページに収める必要はありません。

# 公開の状況等に関する情報（提出資料 7）

| |
|---|
| 暗号技術名： |
| 応募責任者名：<br>印 |
| ⅰ)応募暗号技術を発表した国際会議又は国際論文誌に関する情報を列挙して下さい：<br>発表期日：<br>発表者：<br>会議名又は論文誌名： |
| ⅱ)輸出管理<br>輸出管理上の許可が不要であることを示す根拠に関する情報を列挙して下さい： |
| ⅲ) 知的財産とライセンス方針：<br>応募暗号技術に関連する知財権などに関する情報を明記して下さい。また、電子政府で使用する際のライセンス方針を明記して下さい： |
| ⅳ)調達可能性について<br>応募暗号技術が既に製品等で利用されている場合には、その製品名に関する情報を列挙して下さい： |
| その他関連事項等あれば記載して下さい。 |

（別紙 4）

## 自己チェックリスト （提出書類 9）

暗号技術名＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

本チェックリストは、あくまでも事務手続き上のチェックリストです。
下記内容が確認できたら、□部分を黒く(■)塗りつぶして使用します。

＜チェック項目＞

□ 1.応募暗号技術は、次期リスト策定後、3 年以内に製品化がなされ、調達可能ですか？
□ 2.応募暗号技術は、応募書類受付締切までに公知となっていますか？
□ 3.応募暗号技術は、査読付きの国際会議、国際論文誌に採録されていますか？
□ 4.一つの暗号技術の種別のみに応募していますか？
□ 5.応募暗号技術は、今回公募する暗号技術の種別に該当しますか？
□ 6.応募に必要な以下の提出物（文書・電子データ）が揃っていますか？
［暗号技術応募書、暗号技術仕様書、自己評価書、テストベクトル、参照ソースコード、誓約書、公開状況等に関する情報、応募暗号説明会資料、自己チェックリスト］
□ 7.以下の内容が網羅されていますか？

●暗号技術応募書（P．9)
□ 8.応募暗号技術公開ホームページ URL が記載されていますか？
□ 9.応募担当者は、適時連絡が取れ、日本語が話せる方ですか？
□10.応募担当者の電話番号（代表、直通を明記)、FAX 番号、e-mail アドレスをもれなく記入していますか？

●暗号技術仕様書（P．9)
□11.応募暗号が現リストに掲載されている暗号技術と同等以上の特長を持つ点について記述していますか？
□12.実装に必要な全情報を記載していますか？
□13.応募暗号技術は第三者が全ての機能を実装可能ですか？
□14.今回の応募以外に、同じような名称で他に発表又は応募した暗号技術があれば列挙していますか？

●自己評価書（P．10)
□15.十分な自己評価が記載されていますか？

●テストベクトル（P．11)
□16.公募要項に示された要求件数以上のテストベクトルが提出されていますか？

●参照ソースコード（P．12)
□17.実装動作確認済ですか？
□18.テストベクトル生成ソースコードは添付されていますか？

●誓約書(P．13)
□19．提出資料に誓約書は含まれていますか？

●公開の状況等に関する情報（P．13)
□20.応募暗号技術の公開時期とその学会名は記述されていますか？
□21.輸出規制問題を解決していることの証拠について記載及び資料添付されていますか？
□22.知財権とライセンスについて記載されていますか？
□23.ライセンス方針は、電子政府における利用において無償か、あるいは、妥当かつ非差別的な条件となっていますか？

●応募暗号説明会発表資料（P．14)
□24.提出資料に応募暗号説明会発表資料は含まれていますか？

別添３

# 電子政府推奨暗号の監視

## １．電子政府推奨暗号の監視の基本的な考え方

CRYPTRECは、電子政府推奨暗号の安全性及び信頼性を確保することを目的とし、継続的に暗号技術に関する情報を収集し、必要に応じて暗号の安全性を評価する電子政府推奨暗号の監視活動を行う。

監視は、以下のような考え方に基づいて実施することとする。

（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原則として認めない。

（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。

## ２．電子政府推奨暗号の監視の具体的内容

電子政府推奨暗号の監視は、調査研究、リストからの削除、修正情報の周知等からなる。それぞれの具体的内容は以下（１）～（４）のとおりとする。

（１）暗号技術調査・研究及びデータの蓄積

暗号技術に関する調査研究を実施し、国際標準化の動向等種々のデータを蓄積する。

（２）電子政府推奨暗号の削除

① 電子政府推奨暗号が実運用環境上において攻撃により破られる可能性が高いと判断される場合であって、かつ当該暗号の仕様を変更すること無く攻撃を回避することが不可能であると判断される場合には、当該暗号をリストから削除する。

② 電子政府推奨暗号が実運用環境上において攻撃により破られる可能性が高いと判断される場合であって、かつ当該暗号の仕様を変更すること無く、パラメータの修正等の簡易な修正を行うことによって攻撃を回避することが可能であると判断される場合であっても、その方法等を記述した修正情報が当該暗号の仕様書の管理者より提案されない場合には、当該暗号をリストから削除する。

（３）電子政府推奨暗号に関する修正情報の周知

① 電子政府推奨暗号が実運用環境上において攻撃により破られる可能性が高いと判断される場合であって、電子政府推奨暗号の仕様変更ではなくパラメータの修正等の簡易な修正を実施することにより当該攻撃を回避することができると判断される場合には、当該修正方法を修正情報として周知する。

② ①の場合において、修正情報は仕様書の管理者から提案させることとし、監視委員会は、提案された修正情報を加味して当該電子政府推奨暗号の安全性評価を実施する。仕様書の管理者より修正情報の提案がなされない場合には、当該暗号をリストから削除する。

③ 監視委員会は応募暗号[1]以外の電子政府推奨暗号が実運用環境上において攻撃により破られる可能性が高いとは判断していないにも関わらず、当該暗号に関する修正情報が仕様書の管理者により発行された場合であって（パラメータ修正等の簡易な修正に限る）、監視委員会が当該修正情報を加味した上で安全性評価を実施し、安全性が確保されていると判断する場合には当該修正情報を周知する。

④ 電子政府推奨暗号リストに掲載された応募暗号の仕様について、国際標準化機関による標準化の過程で修正等が行われ、当該暗号に関する修正情報が仕様書の管理者により提案された場合であって、監視委員会が当該修正情報を加味した上で安全性評価を実施し、安全性が確保されていると判断する場合には当該修正情報を周知する。

⑤ 電子政府推奨暗号の仕様書に瑕疵（誤字、脱字）あるいは実装上の解釈が不明瞭な箇所があり、当該暗号に関する修正情報が仕様書の管理者により提案された場合であって、監視委員会が当該暗号に関する修正情報を当該暗号の仕様変更に当たらないと判断する場合には当該修正情報を周知する。

⑥ 技術動向の変化に適切に対応するため、電子政府推奨暗号の安全性に影響を与えない範囲での暗号技術仕様書の参照先の変更が必要となった場合であって、監視委員会が暗号技術仕様書の参照先の変更が当該暗号の本質的な仕様変更に当たらないと判断する場合には当該仕様書の参照先情報を周知する。ただし、下位互換性を維持する必要がある場合には、新規の暗号技術仕様書の参照先の追加を行い、従来の暗号技術仕様書の参照先の削除は行わない。

（４）電子政府推奨暗号の追加

① 電子政府推奨暗号リストの改訂が行われるまでは、電子政府推奨暗号の追加は例外的な扱いとする。

② 電子政府推奨暗号リストに掲載されていない暗号が国際的に高い評価を得ている

---

[1] 応募暗号：電子政府推奨暗号のうち、以下のものを指す。
（公開鍵暗号）ECDSA，RSA-PSS，RSA-OAEP，ECDH，PSEC-KEM
（共通鍵暗号）CIPHERUNICORN-E，Hierocrypt-L1，MISTY1，Camellia，CIPHERUNICORN-A，
Hierocrypt-3，SC2000，MUGI，MULTI-S01

場合であって、検討会が当該暗号を新たに評価することが必要と判断し、かつ、評価の結果、検討会が当該暗号を電子政府推奨暗号リストへ掲載することが適切と判断する場合には、当該暗号を電子政府推奨暗号リストへ追加する。

③ 電子政府推奨暗号リストへの追加を検討する場合には、「10年間は安心して利用できる」という観点から評価を行う。

④ 電子政府調達者より、電子政府推奨暗号リストに無い新たな用途及び当該用途に適した暗号の追加に関する要望がよせられた場合であって、かつ、検討会としても当該用途の追加が適切と判断した上で、それに適した暗号の評価を実施し、その結果、適切な暗号を選定した場合には、当該用途及び当該暗号を電子政府推奨暗号リストへ追加することとする。

## ３．電子政府推奨暗号の監視の手順

電子政府推奨暗号の監視の手順は、（１）監視委員会における情報収集、（２）監視委員会における情報分析、（３）監視委員会及び検討会における審議及び決定の３段階からなる。具体的には以下のとおりとする。ただし、監視委員会が、電子政府推奨暗号リストの変更を直ちに行うべき事態が発生していると判断する場合は、以下に示す手順に関わらず、その緊急性に応じた対応を実施する。

### （１）監視委員会における情報収集

監視委員会は以下のように情報収集を行うこととする。

① 国内外の学会等への参加等を通じて暗号技術に関する情報（学術論文、発表原稿等）を収集する。

② 調査WGメンバー等との連絡体制を整備し、同メンバーから恒常的に情報提供を受ける。

③ 応募暗号については、原則として応募元から情報提供を受ける。

④ その他、一般からの情報提供も受ける。

### （２）監視委員会における情報分析

監視委員会は、（１）により収集された情報を分析し、電子政府推奨暗号の削除等を検討すべき事態が発生しているか否か判断する。その結果、監視委員会が電子政府推奨暗号の削除等を検討すべき事態が発生していると判断する場合には、事案の性質に応じて、調査WGを開催する。

### （３）監視委員会及び検討会における審議及び決定

① 調査WGは、技術的観点から、監視委員会に対して助言を行う。なお、調査WGは、応募元等より修正情報の提供を受け、同修正情報を加味した暗号の安全性評価も行う。

② 監視委員会は、調査WGの助言を踏まえて、電子政府推奨暗号の削除等を実施するか否かについて素案を作成し、検討会に報告する。

③ 検討会は、総合的な観点から当該素案を審議し電子政府推奨暗号の削除等に関する案を作成する。同案が電子政府推奨暗号リストに変更を加えるものである場合、総務省及び経済産業省はパブリックコメントに付し、その結果を検討会に報告する。検討会は、パブリックコメントの結果を踏まえて、電子政府推奨暗号の削除等に関する案を決定する。

④ 検討会の決定に基づいて電子政府推奨暗号リストの変更を行った場合、総務省及び経済産業省は、電子政府推奨暗号リストの変更について行政情報システム関係課長連絡会議等に連絡する。

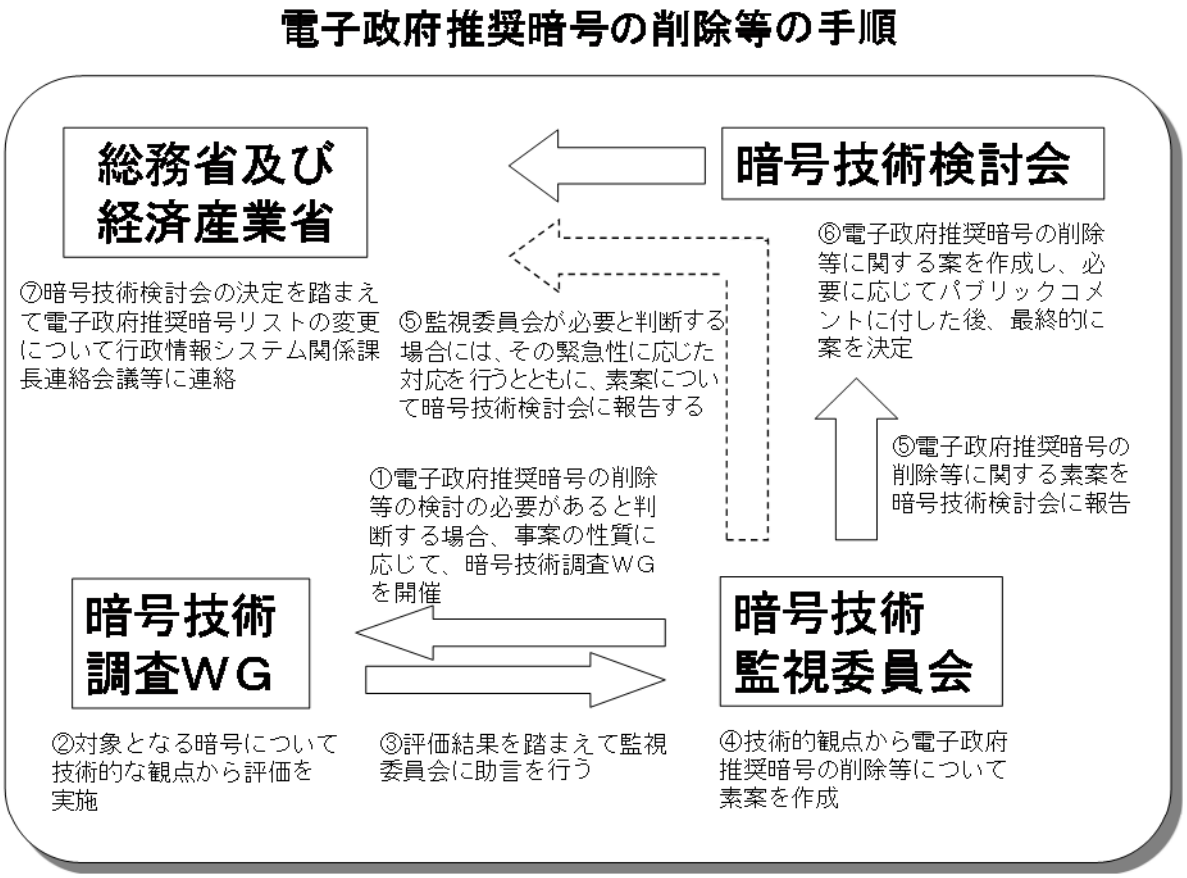


**図6.1　電子政府推奨暗号削除等の手順**