# 暗号技術検討会

# ２００９年度報告書

２０１０年３月

目次

## １．はじめに

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

政府においても、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公表してきており、これらの動きにその内容が反映されたことは、CRYPTREC の活動のひとつの成果と言える。

今年度は、さらに「電子政府推奨暗号リスト」の改訂に向け、これまでの主な活動である「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」に加えて、「暗号技術の運用を主な対象とする調査・検討」を進めるために、CRYPTREC の体制見直しを行い、暗号技術検討会の下に、暗号方式委員会、暗号実装委員会及び暗号運用委員会を設置し、調査・検討等を開始した。また、リスト改訂のための暗号技術公募の実施、公募への応募暗号技術の説明を行う広報イベント「CRYPTREC シンポジウム 2010～応募暗号説明会～」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、暗号方式委員会では、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、暗号実装委員会では、米国連邦政府の情報処理標準である FIPS や国際標準化機関 ISO/IEC の標準におけ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を行うとともに、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。暗号運用委員会では、リスト改訂における新たな評価項目である「暗号技術に対する製品化・利用実績」について、評価方法に関する検討を開始した。

2009 年度の活動のうち、詳細な技術的事項については、暗号方式委員会及び暗号実装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 2009」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。

2010 年 3 月

暗号技術検討会
座長　今井　秀樹

## ２．暗号技術検討会開催の背景及び開催状況

### ２．１．暗号技術検討会開催の背景

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

暗号技術は情報セキュリティの基盤技術であり、その安全性を暗号技術の専門家により技術的、専門的な見地から客観的に評価することが重要である。電子政府のセキュリティ確保のためには、安全性に優れた暗号技術を利用することが不可欠である。

このため、総務省及び経済産業省は、客観的な評価により安全性及び実装性に優れると判断される暗号技術をリスト化し、各府省に対してその利用を推奨することにより、高度な安全性と信頼性に支えられ、国民が安心して利用できる電子政府の構築に貢献することを目指し、2001年度から本検討会を開催した。両省は、本検討会での検討及び評価の結果を踏まえ2003年2月20日に「電子政府」における調達のための推奨すべき暗号のリスト（電子政府推奨暗号リスト）を公表し（別添１参照）、2003年2月28日には、行政情報システム関係課長連絡会議において、各府省が情報システムの構築にあたり暗号を利用する場合には、可能な限り、電子政府推奨暗号リストに掲載された暗号の利用を推進する旨の「各府省の情報システム調達における暗号の利用方針」が了承された。また、「政府機関の情報セキュリティ対策のための統一基準(第4版)（2009年2月3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．新しい電子政府推奨暗号リストに対応したCRYPTRECの体制見直しについて

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

ろである。

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

これまで、暗号技術検討会では、「電子政府推奨暗号の安全性及び信頼性確保のための調査・検討」として「暗号アルゴリズム等を主な対象とする調査・検討」及び「暗号実装関連技術を主な対象とする調査・検討」を行ってきており、これらの検討事項に関する技術的な検討を「暗号技術監視委員会」及び「暗号モジュール委員会」において行っていたところであるが、今後は、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、それに合わせて体制の見直しを行った。

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

### ２．２．１．暗号技術検討会

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

検討会は総務省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た。

### ２．２．２．暗号方式委員会

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

暗号方式委員会は NICT 及び IPA の委員会として開催した。

### ２．２．３．暗号実装委員会

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

暗号実装委員会は NICT 及び IPA の委員会として開催した。

### ２．２．４．暗号運用委員会

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

暗号運用委員会は NICT 及び IPA の委員会として開催した。

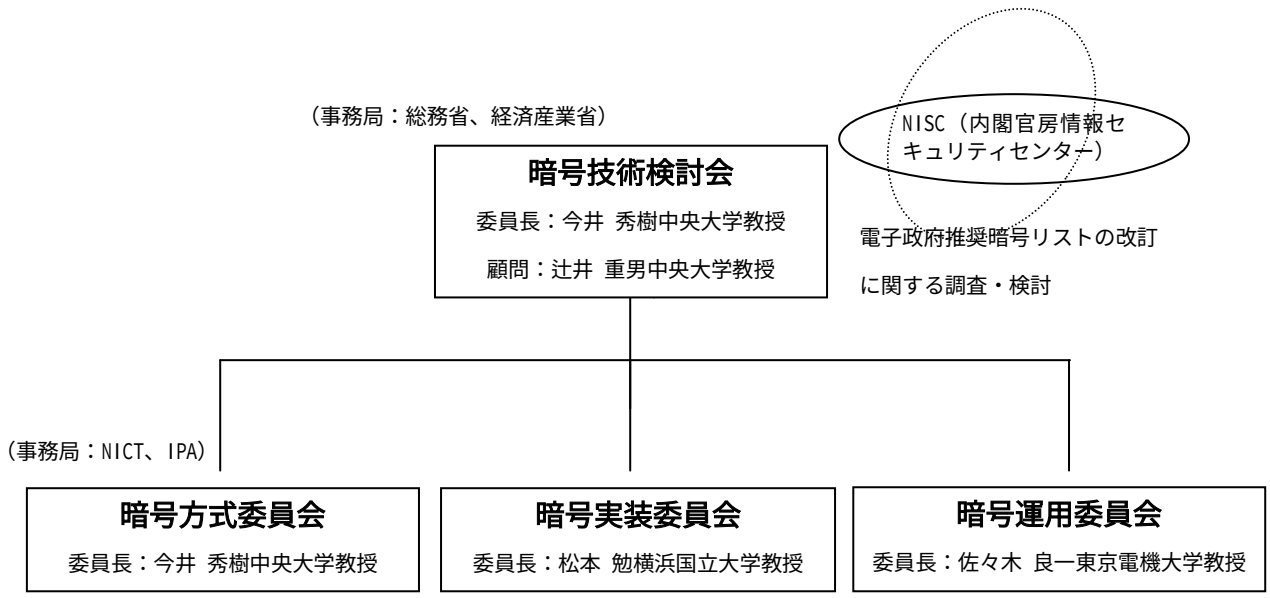



図 2.1　2009 年度 CRYPTREC の体制図

## ２．３．暗号技術検討会開催状況

2009 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】2009 年 7 月 10 日（金）

（主な議題）・CRYPTREC の 運営方針及び活動計画

・新しい電子政府推奨暗号リストに対応した体制見直しについて

・2009 年度暗号技術検討会活動計画

・2009 年度暗号方式委員会活動計画

・2009 年度暗号実装委員会活動計画

・2009 年度暗号運用委員会活動計画

【第 2 回】2010 年 3 月 16 日（火）

（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

・暗号技術検討会 2009 年度報告書

（暗号方式委員会活動報告）

（暗号実装委員会活動報告）

（暗号運用委員会活動報告）

・2010 年度暗号技術検討会活動計画

・2010 年度暗号方式委員会活動計画

・2010 年度暗号実装委員会活動計画

・2010 年度暗号運用委員会活動計画

## 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改訂のための暗号技術公募要項（2009 年度）

#### ３．３．１．公募の概要

CRYPTREC は評価対象暗号技術を公募し、暗号技術評価を実施する。特に、安全性及び実装性で、現リストに記載されている暗号アルゴリズムよりも優位な点を持ち、国際学会で注目されている新技術が提案されている暗号技術カテゴリであること、及び、現リ

ストに掲載されている暗号技術と同カテゴリに属する暗号技術については、それらの暗号技術よりも、安全性もしくは実装性において優れた暗号技術であることを指針としている。

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

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

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

### ３．３．２．公募の対象

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

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

等を挙げている。

表 3.1 2009 年度公募対象の暗号技術の種別

| 暗号技術の種別 | 仕様の概要 |
|---|---|
| ブロック暗号 | 平文及び暗号文ブロックサイズが 128 ビットであり、鍵長が 128 ビット、192 ビット又は 256 ビットであるブロック暗号で、現リストに掲載されている暗号技術と同等以上の特長（安全性又は実装性）を持つもの。 |
| 暗号利用モード | 秘匿に関する 128 ビットブロック暗号及び 64 ビットブロック暗号を対象にした利用モード。 |
| メッセージ認証コード | 鍵長が 128 ビットである 128 ビットブロック暗号及び 64 ビットブロック暗号を利用したメッセージ認証コード。 |
| ストリーム暗号 | 鍵長が 128 ビット以上であり、平文をビット単位もしくはバイト単位で暗号化するストリーム暗号。 |

| 暗号技術の種別 | 仕様の概要 |
|---|---|
| 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。 |

### ３．３．３．公募期間

2009 年 10 月 1 日～2010 年 2 月 4 日 17 時（必着）

### ３．３．４．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今後の応募暗号の評価スケジュールをまとめると以下の通り。

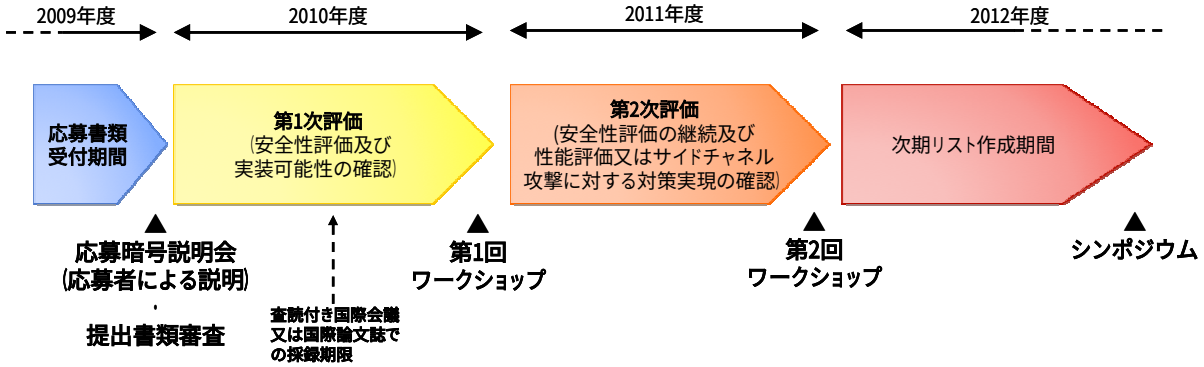



図 3.2 評価スケジュール

| | |
|---|---|
| 応募暗号説明会開催： | 2010 年 3 月 2 日、3 日 |
| 第 1 次評価実施： | 2010 年 4 月～2011 年 3 月 |
| 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 |

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

暗号方式委員会及び暗号実装委員会が、評価結果に基づき、「CRYPTREC 暗号リスト（仮

称)」(以下、「次期リスト」という。)への暗号技術の記載について判定し、暗号技術検討会に答申する。答申された暗号技術の次期リストへの記載については、暗号技術検討会での検討を経た後、最終的に総務省及び経済産業省において決定される。決定については、2012 年度実施を予定している。

### ３．３．５．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[1]、ASIC[2]等）別に性能（処理速度、使用セル数又はゲート数等）を評価する。また、一部の暗号技術に対しては、サイドチャネル攻撃に対する対策実現の確認も行う。

なお、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。

### ３．３．６．応募暗号技術

下記のとおり 6 件の暗号技術について応募があった。

① 128bit 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

② ストリーム暗号

・Enocoro　　株式会社日立製作所
・KCipher－2　　KDDI 株式会社

---

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

③ メッセージ認証コード

・PC-MAC-AES　　日本電気株式会社

④ 暗号利用モード

なし

⑤ 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

### ３．３．７．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 事務局より選出する。

① 128bit ブロック暗号

なし

② ストリーム暗号

なし

③ メッセージ認証コード（リストガイド策定時の検討により選定）

・CBC-MAC
・CMAC
・HMAC

④ 暗号利用モード（リストガイド策定時の検討等により選定）

・CBC モード
・CTR モード
・CFB モード
・OFB モード
・CCM モード
・GCM モード

⑤ エンティティ認証（標準策定状況により選定）

・ISO/IEC 9798-2 共通鍵暗号利用による認証プロトコル
・ISO/IEC 9798-3 電子署名利用による認証プロトコル
・ISO/IEC 9798-4 検査関数（MAC）による認証プロトコル

### ３．３．８．CRYPTREC シンポジウムの開催

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(CRYPTREC シンポジウム 2010)を設けた。

また、CRYPTREC での最新の評価結果を公表し、それらを検討する場（ワークショップ）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。

## ３．４．CRYPTREC シンポジウム 2010－応募暗号説明会－について

電子政府推奨暗号リストの改訂のための暗号技術公募（2009 年度）に応募された暗号技術についての現状の報告と、暗号研究の方向性や今後策定する CRYPTREC 暗号リスト（仮称）の在り方を議論するため、シンポジウムを開催することとした。

### ３．４．１．プログラムの概要

日時：3 月 2 日（火）、3 月 3 日（水）10：00～16：00
場所：コクヨホール
主催：独立行政法人情報通信研究機構、独立行政法人情報処理推進機構
共催：総務省、経済産業省
参加人数：230 名

表 3.3　プログラム

| 3 月 2 日(火)（講演者敬称略） | |
|---|---|
| 時間 | 内容（講演者） |
| 10:00 | 開会挨拶（経済産業省） |
| 10:10 | 講演<br>「2009 年度の CRYPTREC 活動の概要と今後について」<br>（暗号技術検討会座長　今井秀樹（中央大学教授）） |
| 10:40 | 「応募状況について 1」<br>（CRYPTREC 事務局） |
| 11:00 | 「応募暗号のプレゼンテーション 1」<br>ストリーム暗号<br>・Enocoro　株式会社日立製作所<br>・KCipher-2　KDDI 株式会社<br>メッセージ認証コード<br>・PC-MAC-AES　日本電気株式会社 |
| 12:30 | 昼休み |
| 13:45 | 「公募カテゴリーの事務局選出暗号および評価についての事務局見解 1」<br>（CRYPTREC 事務局） |
| 14:30 | 休　憩 |
| 14:45 | パネル 1<br>「暗号技術の実装について」<br>モデレータ<br>松本勉（横浜国立大学）<br>パネリスト<br>崎山一男（電気通信大学）<br>佐藤証（産業技術総合研究所）中嶋純子（三菱電機株式会社） |
| 16:00 | 挨拶（NICT） |

| 3 月 3 日(水)（講演者敬称略） | |
|---|---|
| 時間 | 内容（講演者） |
| 10:00 | 挨拶（IPA） |
| 10:10 | 講演<br>「暗号研究の普及と今後について」（暗号技術検討会顧問<br>辻井　重男（中央大学教授）） |
| 10:40 | 「応募状況について 2」<br>（CRYPTREC 事務局） |
| 11:00 | 「応募暗号のプレゼンテーション 2」<br>128bit ブロック暗号<br>・CLEFIA　ソニー株式会社<br>・HyRAL　株式会社ローレルインテリジェントシステムズ<br>エンティティ認証<br>・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 |
| 12:30 | 昼休み |
| 13:45 | 「公募カテゴリーの事務局選出暗号および評価についての事務局見解 2」<br>（CRYPTREC 事務局） |
| 14:30 | 休　憩 |
| 14:45 | パネル 2<br>「公開鍵暗号技術の最新動向について」<br>モデレータ<br>高木　剛（公立はこだて未来大学）<br>パネリスト<br>田中圭介（東京工業大学）<br>宮地充子（北陸先端科学技術大学院大学）<br>伊豆哲也（株式会社富士通研究所） |
| 16:00 | 閉会挨拶（総務省） |

### ３．４．２．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。以下にそれらの概要を記す。

（１） 暗号技術の実装について

- 実装性評価の実施方針
  - (ア) 評価プラットフォーム
    - ① ソフトウェア評価（PC環境／組み込み）について
      - ソフトウェア実装評価の対象については、PCやサーバだけでなく、組み込み環境も重要である、
      - ただし、同一環境での横並びの評価をするのが難しいため、評価環境に関する検討が必要である。
    - ② ハードウェア評価（FGPA／ASIC）について
      - ハードウェアの実装エリアの広さと処理速度のトレードオフを考慮すべきである、このトレードオフを定性的にグラフなどで表し、比較できることを評価基準に入れて欲しい。
  - (イ) 評価フローについて
    - ① 使用言語（C言語／アセンブラ、Verilog／Custom Cell）の規定も検討すべきである。
    - ② 多くのパラメータ(C言語のコンパイルオプション、実装条件等)も決める必要がある。
  - (ウ) 評価基準について
    - ① 実装効率（例：スループット、レイテンシー、回路規模、消費電力）
      - 実装効率のどの値を重視すれば良いのか選択が難しい。
      - 実装効率毎の評価情報も必要である。
- サイドチャネル攻撃の実施方針
  - (ア) 安全性評価
    - アルゴリズム評価と対物理攻撃耐性は分けて考えるべきである。

（２） 公開鍵暗号技術の最新動向について

- 共通鍵・RSA 暗号・楕円曲線暗号の間の等価安全性を評価し、暗号アルゴリズム・鍵長をいつまで安全に使用できるのかを評価して欲しい。
- 暗号アルゴリズム・暗号プロトコル・暗号実装の脆弱性情報をリアルタイムに提供して欲しい。

## ４．暗号方式委員会活動報告

### ４．１．活動の概要

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

暗号方式委員会では、電子政府推奨暗号の監視、電子政府推奨暗号の安全性及び信頼性確保のための調査・検討及び電子政府推奨暗号リスト改訂に関する安全性評価を行う。

以下に、2009 年度の暗号方式委員会の活動内容について報告する。

#### ４．１．１．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の本格的な体制作りを始めた。また、電子政府推奨暗号リストの改訂のための暗号技術公募に関する検討、現在の電子政府推奨暗号リストに掲載されている暗号技術の安全性に関する監視活動を行った。この監視活動は、暗号技術監視委員会から継続した活動であり、海外動向との整合性（SHA-3 等）に関する検討も含む。この他、リストガイドの拡充も行った。

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

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

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

### ４．１．２．暗号方式委員会開催状況

2009 年度、暗号方式委員会は、表 4.1 の通り 2 回開催された。暗号技術調査ワーキンググループ（リストガイド）は、表 4.2 の通り計 3 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。

(1) 暗号方式委員会

表 4.1　暗号方式委員会の開催

| 回 | 年月日 | 議題 |
|---|---|---|
| 第 1 回 | 2009 年 8 月 5 日 | 活動方針の検討、監視状況報告 |
| 第 2 回 | 2010 年 2 月 18 日 | WG 活動報告、監視情報報告、報告書案の検討 |

(2) 暗号技術調査ワーキンググループ（リストガイド）

表 4.2　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 | 2009 年 9 月 1 日 | WG 活動方針の検討、作業の割り振り |
| 第 2 回 | 2009 年 10 月 22 日 | 調査内容の中間報告とその検討 |
| 第 3 回 | 2010 年 2 月 4 日 | 報告書案の検討 |

## ４．２．委員会の調査・検討結果

### ４．２．１．監視状況

電子政府推奨暗号の安全性評価について 2009 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。以降、収集、分析した主たる情報について報告する。

（１）共通鍵暗号の安全性評価について

AES に対する関連鍵攻撃に関する解析方法が大きく進展している。現時点における最良の攻撃は、いずれも関連鍵のシナリオで AES-256 に対して事前計算テーブルサイズ（データ計算量）$2^{99.5}$、実行時間（時間計算量）$2^{99.5}$、必要メモリーサイズ（領域計算量）$2^{77}$、AES-192 に対して事前計算テーブルサイズ $2^{123}$、実行時間 $2^{176}$、必要メモリーサイズ $2^{152}$ と見積もられている。使用する鍵が独立な乱数とみなせる場合、これらの結果が現実的な脅威となることは無い。AES を理想暗号として使用するハッシュ関数、暗号利用モードあるいはメッセージ認証コードなどの理論的安全性については、

これらの結果の影響を受ける可能性がある。また、ブロック長 64 ビット、鍵長 128 ビットの MISTY1 に対して積分攻撃を適用した結果、FL 関数を全部入れた 6 段(フルスペックは 8 段)が $2^{32}$ 個の選択暗号文と暗号化 $2^{126.1}$ 回分の計算量で攻撃可能との見積が示された。また、ブロック長・鍵長ともに 128 ビットの Camellia に対しては不能差分攻撃が有効で、FL 関数なしの 12 段を選択平文 $2^{116.3}$ 個、計算複雑度 $2^{116.6}$ で攻撃可能との見積が示された。

（2）公開鍵暗号の安全性評価について

素因数分解問題に関して、The RSA Factoring Challenge[3] の RSA-768（768 ビット RSA 合成数）が一般数体ふるい法で素因数分解されたとの報告があった。数百台の PC を 2 年間程度使用したとのこと。この結果は CRYPTREC で 2006 年度に実施した安全性評価の見解と良く一致している。

離散対数問題に関しては、SCIS 2010 にて GF($3^{6\cdot 71}$)上の離散対数計算（676 ビット，位数の最大素因子 112 ビット）が関数体ふるい法で実現されたとの報告があった。100 コア弱の PC を 1 ヶ月間程度使用したとのこと。離散対数問題に関しても、素因数分解問題と同様に解析技術が向上していると考えられる。

楕円離散対数問題に関しては、112-bit の素体楕円離散対数計算が Pollard のρ法で実現されたとの報告があった。200 台の PlayStation 3 を半年間程度使用したとのこと。

（3）ハッシュ関数の安全性評価について

段数縮小版 SHA-1 の原像攻撃可能段数が 48 段まで向上した事が報告された。また、段数縮小版 SHA-256 と段数縮小版 SHA-512 に関して原像攻撃可能段数がそれぞれ 64 段中 43 段および 80 段中 46 段まで向上した事が報告された。近年の原像攻撃の発展は概ね中間一致攻撃の高度化による成果である。

（4）暗号技術標準化動向

SHA-3 選考において、米国 NIST は、2009 年 7 月 24 日に第 2 ラウンドに進むことができる SHA-3 候補のハッシュ関数アルゴリズムを 14 個選出した。それらは以下の通りである。

表4.3 第2ラウンドに進んだSHA-3候補一覧

| | | |
|---|---|---|
| BLAKE | Grostl | Shabal |
| BLUE MIDNIGHT WISH | Hamsi | SHAvite-3 |
| CubeHash | JH | SIMD |
| ECHO | Keccak | Skein |
| Fugue | Luffa | |

[3] RSA 社（米国）の素因数分解問題に関するコンテスト。既に終了している。

選出したハッシュ関数に関する概要については、NIST が「Status Report on the First Round of the SHA-3 Cryptographic Hash Algorithm Competition」[4]として公表している。また、次回の第 2 ラウンド SHA-3 候補会議は、2010 年 8 月 23・24 日に開催される予定である。

なお、NIST による SHA-3 評価・選定の結果を参考にして、国内における電子政府推奨暗号におけるハッシュ関数の推奨を行うことが考えられるため、CRYPTREC では NIST の評価プロセスに対して評価基準に関する提案を行うべく、電気通信大学、産業技術総合研究所、及び、NICT を主なメンバーとして、「ハードウエア評価に関する評価基準」及び「プロトコルの安全性を考慮した方式の安全性評価基準」について検討中であり、その結果を第 2 ラウンド SHA-3 候補会議にて発表する予定である。

### ４．２．２．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

2009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4.4に示す通りである。

表 4.4　国際会議への参加状況

| 学会名・会議名 | | 開催国・都市 | 期間 |
|---|---|---|---|
| TCC 2009 | Theory of Cryptography Conference | サンフランシスコ（米国） | 2009 年 3 月 15 日～3 月 17 日 |
| PKC 2009 | International Conference on Practice and Theory in Public Key Cryptography | アーバイン（米国） | 2009 年 3 月 18 日～3 月 20 日 |
| Eurocrypt 2009 | International Conference on the Theory and Applications of Cryptographic Techniques | ケルン（ドイツ） | 2009 年 4 月 26 日～4 月 30 日 |
| Pairing 2009 | International Conference on Pairing-based Cryptography | パロアルト（米国） | 2009 年 8 月 12 日～8 月 14 日 |
| SAC 2009 | Workshop on Selected Areas in Cryptography | カルガリー（カナダ） | 2009 年 8 月 13 日～8 月 14 日 |
| Crypto 2009 | International Cryptology Conference | サンタバーバラ（米国） | 2009 年 8 月 17 日～8 月 20 日 |

[4] http://csrc.nist.gov/groups/ST/hash/sha-3/Round1/documents/sha3_NISTIR7620.pdf

| 学会名・会議名 | | 開催国・都市 | 期間 |
|---|---|---|---|
| ECC 2009 | Workshop on Elliptic Curve Cryptography | カルガリー（カナダ） | 2009 年 8 月 24 日～8 月 26 日 |
| FDTC 2009 | Workshop on Fault Diagnosis and Tolerance In Cryptography | ローザンヌ（スイス） | 2009 年 9 月 6 日 |
| CHES 2009 | Workshop on Cryptographic Hardware and Embedded Systems | ローザンヌ（スイス） | 2009 年 9 月 6 日～9 月 9 日 |
| SHARCS 2009 | Special-purpose Hardware for Attacking Cryptographic Systems | ローザンヌ（スイス） | 2009 年 9 月 9 日～9 月 10 日 |
| Asiacrypt 2009 | International Conference on the Theory and Application of Cryptology and | 東京（日本） | 2009 年 12 月 6 日～12 月 10 日 |
| FSE 2010 | Fast Software Encryption workshop | 韓国（ソウル） | 2010 年 2 月 7 日～2 月 10 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

主に AES などを対象に関連鍵攻撃に関する発表が相次いで行われている。フルラウンドの AES-256 に対する関連鍵攻撃において、データおよび時間の複雑度 $2^{131}$、メモリ量 $2^{65}$ で $2^{35}$ 個の関連鍵のうちの 1 つを鍵回復できるとの見積に続いて、フルラウンドの AES-256 に対してデータおよび時間複雑度 $2^{99.5}$、メモリ量 $2^{77}$ で攻撃可能、フルラウンドの AES-192 に対してデータ複雑度 $2^{123}$、時間複雑度 $2^{176}$、メモリ量 $2^{152}$ で攻撃可能との見積が示された[Related-key Cryptanalysis of the Full AES-192 and AES-256、Biryukov and Khovratovich、 Asiacrypt 2009]。

また、ブロック長 64 ビット、鍵長 128 ビットの MISTY1 に対して積分攻撃を適用した結果、FL 関数を全部入れた 6 段(フルスペックは 8 段)が $2^{32}$ 個の選択暗号文と暗号化 $2^{126.1}$ 回分の計算量で攻撃可能との見積が示された[Improved integral attacks on MISTY1、Sun and Lei、SAC 2009]。

また、ブロック長・鍵長ともに 128 ビットの Camellia に対しては不能差分攻撃が有効で、FL 関数なしの 12 段を選択平文 $2^{116.3}$ 個、計算複雑度 $2^{116.6}$ で攻撃可能との見積が示された[New results on impossible differential cryptanalysis of

reduced-round Camellia-128、Mala、Shakiba、Dakhilalian and Bagherikaram、SAC 2009]。

② ストリーム暗号の解読技術

欧州のストリーム暗号研究プロジェクト eSTREAM において、ハードウェア向け方式として最終候補(Phase 3)に残った DECIMv2 と DECIM-128 は、Krawczyk のパラメータを使った収縮生成器(shrinking generator)が使用されており、不規則に破棄する(irregularly decimated)ストリーム暗号と呼ばれる。この収縮生成器を使った機構に対する従来よりもずっと良い相関が発見され、初期状態を復元する攻撃法に適用された結果、160 ビット縮小版 DECIMv2(192 ビット LFSR 使用)では、計算量が操作 $2^{76.3}$ 回分、メモリが $2^{71.3}$ ビット、データが $2^{35.1}$ ビット必要であると見積もられ、256 ビット縮小版 DECIM-128(288 ビットの LFSR を使用)では、計算量が操作 $2^{124}$ 回分、メモリが $2^{117}$ ビット、データが $2^{36.1}$ ビット必要であると見積もられた[New Cryptanalysis of Irregularly Decimated Stream Ciphers、Zhang、SAC 2009]。

③ ハッシュ関数の解読技術

中間一致攻撃をハッシュ関数の原像攻撃に利用する方法を、メッセージ・スケジュールが線形変換の場合にも使えるように拡張した結果、SHA-0 では圧縮関数計算 $2^{156.6}$ 回で 52 ステップまで、SHA-1 では圧縮関数計算 $2^{159.3}$ 回で 48 ステップまで原像攻撃可能であるとの報告があった[Meet-in-the-Middle Preimage Attacks Against Reduced SHA-0 and SHA-1、Aoki and Sasaki、Crypto 2009]。

SHA-2 ファミリーは NIST が SHA-1 の後継としたハッシュ関数であり、今まで衝突探索の研究は比較的進んでおり、SHA-256 に対しては 64 段中 24 段まで衝突発見攻撃が提案されている。一方、中間一致を利用した原像攻撃を SHA-2 ファミリーに適用した結果、SHA-224 では擬似衝突探索が 43 段で計算量は $2^{219.9}$、SHA-256 では衝突及び擬似衝突探索が 43 段で計算量はそれぞれ $2^{254.9}$ と $2^{251.9}$、SHA-384 では擬似衝突探索が 43 段で計算量はそれぞれ $2^{366}$、SHA-512 では衝突及び擬似衝突探索が 46 段で計算量はそれぞれ $2^{509}$ と $2^{511.5}$ と見積もられている[Preimages for Step-Reduced SHA-2、Aoki、Guo、Matusiewicz、Sasaki and Wang、Asiacrypt 2009]。

また、MD5 ハッシュ関数を利用した中間 CA の公開鍵証明書の偽造が可能であることが示されている[Short Chosen-Prefix Collisions for MD5 and the Creation of a Rogue CA Cert、Stevens、Sotirov、Appelbaum、Lenstra、Molnar、Osvik and de Weger、Crypto 2009]。

④ 公開鍵暗号の解読技術

素因数分解に関しては、The RSA factoring challenge の 768 ビット(10 進 232 桁)合成数 RSA-768 の素因数分解に成功した(これまでの世界記録は、663 ビット、10 進 200 桁)という報告があった。スイス連邦工科大学ローザンヌ校、日本電信電話株式会

社、ドイツ・ボン大学、フランス・国立情報学自動制御研究所、アメリカ・マイクロソフト研究所、オランダ・国立情報工学・数学研究所らの共同研究により、一般数体ふるい法を用いて約 2 年間で達成された[ePrint 2010/006]。

離散対数問題に関しては、関数体ふるい法により、GF(3)の 6×71 次拡大体(676 ビット)における離散対数計算に成功したことが示された(これまでの記録は GF(2)の 613 次拡大)。関係探索ステップでは 96 コアの計算機で約 18 日間、線型代数ステップでは 80 コアで約 0.5 日間、特定の元の離散対数計算ステップでは 48 コアで約 14 日間を費やした[GF($3^{6\cdot71}$)上の離散対数計算実験、林、篠原、王、松尾、白勢、高木、SCIS 2010]。

また、楕円曲線上の離散対数問題に関しては、スイス連邦工科大学ローザンヌ校およびアメリカ・マイクロソフト研究所により、112 ビット素体上楕円曲線離散対数問題の解読に成功した(これまでの世界記録は Certicom Challenge の 109 ビット)との報告があった。解読には、Pollard のρ法を 200 台の PlayStation 3 で実行することにより約半年間(連続使用であれば 3.5 ヶ月間と見積もられる)で行われている[Pollard Rho on the PlayStation 3、Bos、Kaihara and Montgomery、SHARCS 2009]。

Certicom ECC challenge のうち、ECC2K-130、ECC2-131、ECC2K-163、ECC2-163 関して、様々なプラットフォーム(FPGA/ハードウェア/ソフトウェア)上でのパラレルρ法による解読計算量に関する評価が発表された。それによると、ECC2K-130(130 ビット Koblitz 曲線)の解読には、$2^{60.8}$ のρ法 iteration 関数呼び出しが必要であるが、実現可能であるとのこと[The Certicom Challenges ECC2-X、Bailey、Baldwin、Batina、Bernstein、Birkner、Bos、van Damme、de Meulenaer、Fan、Guneysu、Gurkaynak、Kleinjung、Lange、Mentens、Paar、Regazzoni、Schwabe and Uhsadel、SHARCS 2009]。

さらに、楕円曲線暗号と RSA 暗号の安全性比較として、1024 bit の RSA は 136 ～ 142 bit の楕円曲線暗号と同等の強度しか持たないことが報告された[楕円曲線暗号と RSA 暗号の安全性比較、下山、伊豆、小暮、安田、SCIS 2010]。

⑤ その他

国際民間航空機関（ICAO）の次世代 IC 旅券などに採用されている ISO/IEC9796-2:2002（RSA 文書回復型署名）の Scheme 1 に関して、パディング[5]の問題により現実的計算量で存在的偽造が可能な事が報告された。必要な署名の数などから、この攻撃が直ちに現実的脅威となる訳ではないが、今後新たな規格を考える場合は証明可能安全な方法を採用すべきとしている[Practical Cryptanalysis of ISO/IEC 9796-2 and EMV Signatures、Coron、Naccache、Tibouchi and Weinmann、CRYPTO 2009]。

[5] 署名を生成する為のデータフォーマット

## ４．３．暗号技術調査ワーキンググループ（リストガイド）の活動

### ４．３．１．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

2008 年度に ID ベース暗号ワーキンググループにおいて、将来の CRYPTREC における評価を見据える形で、ID ベース暗号に関する全般的な調査を行った。その結果、基本的な技術についての知見を得ることができた。一方で、現実のシステムに適用したときの適切な利用方法については、より多くの検討が必要であるとの結論に至った。

そのため、本年度の活動として、電子政府システムにおける ID ベース暗号利用のモデルケースを設定し、このモデルケースに対応して安全性および実装性の観点から利用方法についての検討を行った。また、擬似乱数生成については、国際標準化機構と国際電気標準会議(ISO/IEC)および、NIST において標準化が行われている。一方で、CRYPTREC では、擬似乱数生成に関しては、電子政府推奨暗号リストにおける例示として取り扱われているのみとなっている。擬似乱数生成に関しては、一般的に互換性の必要性が低いため、モジュール評価においても役立てるよう、一意に特定できる仕様をリストガイドとして記載することとした。

暗号技術調査ワーキンググループ（以下、「リストガイド WG」という）の 2009 年度の主要活動項目は、表 4.5 のとおりである。

表 4.5　2009 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 | 高木　剛 | ① ID ベース暗号を電子政府におけるアプリケーションに適用した場合の推奨される利用方法と課題の調査<br>② 擬似乱数生成アルゴリズムに関するリストガイドの作成 |

### ４．３．２．リストガイド WG の開催状況

本年度は、3 回のリストガイド WG を開催した。

第 1 回リストガイド WG（2009 年 9 月 1 日）では、今年度の執筆内容、および執筆の担当についての議論を実施した。その結果、ID ベース暗号については、「(1)ID ベース暗号を現実のシステムに適用する場合の課題」、「(2)電子政府で想定されるアプリケーションでの推奨技術の検討」、「(3)ペアリングに依存しない ID ベース暗号の調査」の 3 点を執筆内容とすることが決められた。また、擬似乱数生成については、JCMVP、ISO、ANSI における標準化動向を調査し、本リストガイドにおける記述領域を検討することとなった。

第 2 回リストガイド WG（2009 年 10 月 22 日）では、各執筆内容の骨子の議論を行った。(1)の内容については、PKI などの既存のセキュリティ機構が保証するトラス

トの仕組みと ID ベース暗号が保証するトラストを比較し、ID ベース暗号に求められる課題についての議論を行った。(2)の内容については、NISC が提示している電子政府システムのモデル[6]について、どのモデルを検討対象とするかが議論され、Web サービスシステムと電子メールシステムが対象として選ばれた。また、(3)については調査対象の技術に関する現状調査の骨子が示された。疑似乱数生成については、安全性、および著作権などの面での検討の結果、JCMVP での認証対象の技術について執筆することとなった。

第 3 回リストガイド WG（2010 年 2 月 4 日）では、各委員担当の報告書案の説明を行ってもらい、修正点の洗い出しを実施した。特に、(1)の内容において記述する、ID ベース暗号のメリットが活かしやすいアプリケーション領域と、(2)での適用例の記述についての整合性のチェックを中心に実施した。また、擬似乱数生成については、執筆内容のレビューを実施した。疑似乱数生成アルゴリズム間の比較について、記述できる項目を検討し、必要に応じて追加することとなった。

### ４．３．３．リストガイド WG の成果概要

2009 年度版のリストガイドは、ID ベース暗号のパートと擬似乱数生成のパートに分かれる。以下、2009 年度版のリストガイドの目次と記述内容を示す。

1　ID ベース暗号

1.1　ID ベース暗号の実システムへの適用

- ID ベース暗号を実社会に適用する際の課題、PKI における信頼との対比
- ID ベース暗号の利用が適する領域に関する提言

1.2　アプリケーションモデルとアプリケーションへの適用の際の実装

- 電子メールに応用した場合の実装と推奨（メールの暗号化）
- Web を利用した情報提供と管理に利用した場合の課題（認証）

1.3　ペアリングを用いない ID ベース暗号

- 格子理論を用いた ID ベース暗号（Gentry-Peikert-Vaikuntanathan、Agrawal-Boyen、Cash-Hofheinz-Kiltz、Peikert）の方式の概要、メリット・デメリット
- 格子理論に基づく暗号の特徴
- 平方剰余判定問題に基づく ID ベース暗号（Cocks、Boneh-Gentry-Hamburg）の方式の概要、メリット・デメリット

---

[6] 「情報システムの構築等におけるセキュリティ要件及びセキュリティ機能の検討に関する解説書」 2007 年 11 月 内閣官房情報セキュリティセンター

2　擬似乱数生成

- 擬似乱数生成の概要とセキュリティ要件
- 実装仕様
  - 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
  - ANSI X9.31 Appendix A.2.4 Using 3-Key Triple DES
  - ANSI X9.31 Appendix A.2.4 Using AES
  - Hash_DRBG
  - HMAC_DRBG
  - CTR_DRBG
- 方式間の比較

詳細については、2009 年度版リストガイドを参照のこと。

# ５．暗号実装委員会活動報告

## ５．１．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が正しく安全に実装されるための要件を検討するとともに、サイドチャネル攻撃を初めとする暗号実装関連の技術動向を調査するために、2008 年度まで開催していた暗号モジュール委員会を引き継ぐ形で、2009 年度から組織された。

暗号実装委員会では、暗号の実装に係る技術及び暗号を実装した暗号モジュールに対する攻撃手法に関する調査・検討、電子政府推奨暗号リスト改訂に伴う実装性評価に関する調査・検討を行う。

以下に、2009 年度の暗号実装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、電子政府推奨暗号リスト改訂のための暗号技術公募におけるサイドチャネル攻撃耐性の評価に関する検討を行った。また、暗号実装技術の動向調査及び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の動向調査を実施した。これらの動向調査は、暗号モジュール委員会から継承した活動であり、暗号モジュール関連の国際標準化への協力を含み、実際の作業は暗号実装委員会の下に置かれるサイドチャネルセキュリティワーキンググループで実施された。

### ５．１．２．暗号実装委員会開催状況

2009 年度、暗号実装委員会は、表 5.1 の通り 3 回開催された。開催日及び主な議題は以下の通りである。

表 5.1　暗号実装委員会の開催

| 回 | 年月日 | 議題 |
|---|---|---|
| 第 1 回 | 2009 年 8 月 5 日 | 活動方針の検討 |
| 第 2 回 | 2009 年 10 月 2 日 | 実装性能・サイドチャネル攻撃耐性評価の検討 |
| 第 3 回 | 2010 年 2 月 22 日 | 実装性能・サイドチャネル攻撃耐性評価の検討 |

## ５．２．委員会の調査・検討結果

### ５．２．１．実装性能評価に関する検討

応募暗号技術及び現行の電子政府推奨暗号リスト掲載暗号技術に対するハードウェア及びソフトウェア実装性評価の実装環境及び必要とされる実装性能の基準を決定した。具体的には次の項目の基本線を決定した。

（1）ソフトウェア及びハードウェア実装性能評価ツールに関する仕様
（2）実装性能評価のための実装用インタフェース仕様
（3）ソフトウェア及びハードウェア実装性能評価の評価項目、評価手法、評価結果の判断基準

### ５．２．２．サイドチャネル攻撃耐性の評価に関する検討

応募暗号技術及び現行の電子政府推奨暗号リスト掲載暗号技術のサイドチャネル攻撃耐性に関する評価項目、評価手法の検討及びそのためのソフトウェア/ハードウェア実装要件の検討を行い、暗号方式委員会と連携して、基本方針を決定した。

### ５．２．３．サイドチャネル攻撃等の実験データに関する調査・検討

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

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

## ５．３．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

### ５．３．１．サイドチャネルセキュリティワーキンググループの活動目的と経緯

2008 年度まで、電力解析実験ワーキンググループにおいて、INSTAC-8/-32 準拠ボードや SASEBO シリーズを対象に電力解析実験に関する実験データや学会動向に関する情報収集を行ってきた。しかし、サイドチャネル攻撃は電力解析に限定されるものでなく、電磁波解析や故障利用攻撃も含まれ、活動がワーキンググループ名と一致しなくなった。

本年度は CRYPTREC 全体の体制変更に合わせ、電力解析ワーキンググループを継承するものとして、サイドチャネルセキュリティワーキンググループが暗号実装委員会の下に置かれた。本年度は、次の２つを柱として活動した。

（1）ISO/IEC 19790 の早期改訂案の検討
（2）サイドチャネル攻撃検証に関する情報収集

### ５．３．２．サイドチャネルセキュリティワーキンググループの開催状況

本年度は、サイドチャネルセキュリティワーキンググループは、表 5.2 の通り計 2 回開催された。

表 5.2　サイドチャネルセキュリティワーキンググループの開催

| 回 | 年月日 | 議題 |
|---|---|---|
| 第 1 回 | 2009 年 9 月 2 日 | WG 活動方針の検討、作業の割り振り |
| 第 2 回 | 2010 年 2 月 5 日 | 報告書案の検討 |

第 1 回 WG（2009 年 9 月 2 日）では、CRYPTREC の体制変更の説明と、今年度の活動方針について検討を行った。

第 2 回 WG（2010 年 2 月 5 日）では、2 月中旬に ISO/IEC 19790 第 2 版の 1st WD が公開されることが報告され、公開後、委員に担当箇所を割り当て、英文のコメントを作成することが同意された。また、作成されたコメント案は、松本主査が SC27/WG3 国内小委員会に提出し、SC27 国際事務局に提出する手順であることが紹介された。

### ５．３．３．サイドチャネルセキュリティワーキンググループの成果概要

本年度は、ISO/IEC 19790 第 2 版の 1st 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、1st WD の公開が第 2 回 WG の後であったため、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行った。

## ６．暗号運用委員会活動報告

### ６．１．活動の概要

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

これまで、暗号技術検討会では、「電子政府推奨暗号の安全性及び信頼性確保のための調査・検討」として「暗号アルゴリズム等を主な対象とする調査・検討」及び「暗号実装関連技術を主な対象とする調査・検討」を行ってきており、これらの検討事項に関する技術的な検討を「暗号技術監視委員会」及び「暗号モジュール委員会」において行っていたところである。

暗号運用委員会は、新しい電子政府推奨暗号リスト（以下「次期リスト」という。）を策定・運用していくにあたって必要となる「暗号技術の運用を主な対象とする調査・検討」を行うために、本年度から新たに設置された。具体的には、電子政府システム等で利用される電子政府推奨暗号の適切な運用について、システム設計者・運用者の観点から調査・検討を行う。特に、次期リスト策定における「暗号技術に対する製品化・利用実績等の評価」について評価方針や評価基準等の検討を行う。さらに、電子政府推奨暗号リストと国際標準技術等との整合性についても検討する。

また、次期リスト策定における「運用監視暗号リスト」に掲載された暗号技術の取り扱い方針について検討する。システム運用者の観点から、今後危殆化により移行が必要とされた場合、より円滑な作業を可能にするための調査・検討を行う。

以下に、2009 年度の暗号運用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

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の進展に伴い、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ため、暗号技術検討会において、現在の電子政府推奨暗号リストを改訂し、2013 年度から新たな推奨暗号の体系に移行することとなった。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（以下、「３リスト」という。）、リストガイドから構成され、CRYPTREC 暗号リスト(仮称)として公開することとなった。安全性が確認された暗号技術は、３リストのいずれかに登録されることになり、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するとともに、一定の間隔で見直すこととしている。

（参考）次期リストの役割

（1）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。

（2）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。

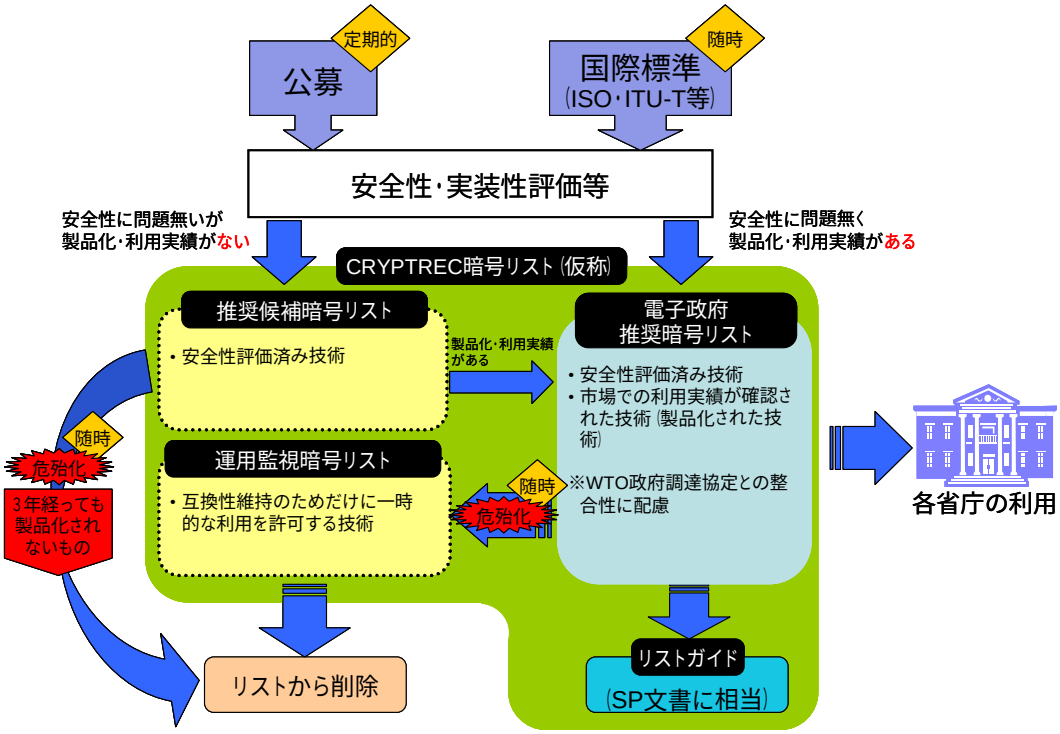
本リストに登録された技術は、一定期間ごとに普及の度合いの調査を行い、利用実績が十分であると認められれば電子政府推奨暗号リストに登録される。また、利用実績が十分であると認められなかった場合にはここから削除される。危殆化が生じた暗号技術については、随時ここから削除される。

（3）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。

（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、システム運用者及び設計者の利用や、システム利用者への啓発を目的とする。




今年度は、３リストの参照者の分析を行うとともに、電子政府推奨暗号リストと推奨候補暗号リストを区分するため、市場における利用実績及び国際標準に関する評価の考え方、危殆化した暗号技術として運用監視暗号リストに登録された暗号技術の扱い等について議論した。

### ６．１．２．暗号運用委員会開催状況

2009 年度の暗号運用委員会は、計 2 回開催された。各回会合の概要は表 6.1 のとおりである。

表 6.1　2009 年度暗号運用委員会の開催状況

| 回 | 開催日時 | 主な議題 |
|---|---|---|
| 第 1 回 | 2009 年 10 月 23 日 | 暗号運用委員会活動計画についての検討<br>電子政府推奨暗号リストに関する検討 |
| 第 2 回 | 2010 年 2 月 22 日 | 国際標準化及び市場での利用実績に関する検討<br>2009 年度暗号運用委員会の活動報告(案)についての検討 |

## ６．２．委員会の調査・検討結果

### ６．２．１　電子政府推奨暗号リストの参照者の分析

暗号技術の製品化、利用実績等の評価に当たって、電子政府推奨暗号リストに掲載された暗号技術の利用者について整理を行った。

まず、電子政府を構築するために情報システムを調達する政府が第一義的な利用者とな

る。各府省が情報システムの構築に当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こととしている他、「政府機関の情報セキュリティ対策の統一基準(第４版)」(2009 年 2 月情報セキュリティ政策会議)においては、暗号化及び電子署名のアルゴリズムについてリストに掲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としている。

特定の暗号技術についての電子政府における利用実績は、次期リストの運用に当たっては重要な指標となる。

次に、暗号技術の製品化状況の評価に当たっては、暗号技術、暗号ライブラリ、暗号モジュール等の開発を行う暗号ベンダが暗号技術をどのように市場に供給しているかということも重要な指標となり得る。

その他、暗号ベンダの提供する暗号ライブラリや暗号モジュール等を利用して、特定の目的の情報システムを構築し、政府等に納入するシステムインテグレータや政府が調達することとなるような暗号を組み込んだコンシューマ向けの製品や電子政府と関わる認証業務等を行う製品・サービス提供者が電子政府推奨暗号リストの参照者と考えられる。

製品化、利用実績等の評価に当たっては、以上の４者を対象とした調査等が必要と考えられ、今後具体的な調査手法について検討を行う必要がある。

### ６．２．２　市場における利用実績に関する考え方

IT 製品には、様々な暗号技術が用いられていることから、すべての暗号アルゴリズムの利用実績を網羅的に調査することは困難である。このため、利用実績に関する判断基準として、例えば、一つの製品でも搭載実績があれば利用実績があればよいと考える方法、搭載されている製品の重要性を加味して重要と判断されたアプリケーションへの搭載実績を利用実績とする方法など、以下の例が考えられる。

**①　搭載されている製品が一つでもあることを利用実績とする判断方法の例**

- 暗号アルゴリズム開発会社自身が販売する部品・製品への搭載事例があること
- 暗号アルゴリズム開発会社以外の会社等が販売する部品・製品への搭載事例があること
- JCMVP 等の関連制度の認証を受けている製品への搭載事例があること

**②　搭載されている製品の重要性を加味して利用実績を検討する方法の例**

- 主要なオープンソースソフトウェア(Linux など)への搭載事例があること
- 主要なアプリケーションでの搭載事例があること

暗号技術の利用実績については、どのような考え方が適切か、暗号アルゴリズムが搭載された製品の市場シェア・販売数量・販売額等について考慮すべきか、具体的にどのような調査方法が有効と考えられるか等の観点から、議論を行い、以下のような意見があげられ、さらに検討を続けることとなった。

- 利用実績が多い暗号の方が安全性評価の対象になり易いので、利用実績が少なく安全性評価の機会が少ない暗号よりも、利用実績が多く安全性評価の機会が多い暗号の方が安全性の面で良いと考えられる。
- 導入後のサポートへの期待という意味でも、製品化・普及の評価は意味があると考えられる。
- 業界で採用している暗号とこれから利用を推進していく暗号において同じ基準で評価するのは適切ではないのではないか。
- デファクト暗号についてのコンセンサスは概ね取れているものと考えられるが、明確な基準を設けるのは難しい。
- 暗号モジュールのセキュリティ機能に関する動作確認をしておくことは調達において重要であることから、JCMVP 認証製品への搭載の有無も暗号アルゴリズムの利用実績を評価するうえでの基準とすべきと考えられる。

### ６．２．３　国際標準についての考え方

政府等が情報システムを調達するに当たっては、WTO 政府調達協定と整合的に調達する必要がある。WTO 政府調達協定では、技術仕様について適当な場合には国際標準が存在するときは当該国際標準等に基づいて定めることとされていることから、次期リストに登録される暗号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。

国際標準の観点からの評価を実施するため、暗号技術がどのような条件を満たせば、国際標準と考えることが適当か検討を行った。

例えば、国際機関である国際標準化機構(ISO)、国際電気標準化会議(IEC)、国際電気通信連合(ITU)において、暗号技術がアルゴリズムとして標準化されている場合、アプリケーションやシステムの規格において暗号アルゴリズムが指定されている場合がある他、事実上の標準として採用されている暗号技術の標準を定めている業界団体や特定の国、組織等があり、国際機関と類似した標準化が行われており、具体的には以下のような例がある。

**①　国際標準化機関が定めた標準**

＜例＞

○国際標準化機構（ISO）、国際電気標準会議（IEC）[7]

ISO/IEC でアルゴリズムとして標準化されている例[8]

ISO/IEC 9796：（デジタル署名）

ISO/IEC 9797:（MAC）

ISO/IEC10118：（ハッシュ関数）

ISO/IEC11770：（鍵管理）

[7] ISO/IEC JTC 1：Joint Technical Committee 1

[8] ISO/IEC JTC1/SC27 が管理

ISO/IEC14888：(デジタル署名)
ISO/IEC18031：(擬似乱数生成)
ISO/IEC18033：(公開鍵暗号・ブロック暗号・ストリーム暗号)　等

ISO や ISO/IEC でアプリケーションやシステムの規格において暗号アルゴリズムが指定されている可能性がある例（”encryption”のキーワードで検索される例）[9]
ISO 9564：(金融サービスでの PIN 暗号化)
ISO15764：(高度交通システムのデータリンク)
ISO21000：(MPEG-21 著作権保護)
ISO26429：(デジタルシネマ)
ISO26430：(デジタルシネマ)
ISO/IEC29116:（メディアストリーミング）　等

○国際電気通信連合（ITU)
ITU でアルゴリズムとして標準化されている例
規格名を見る限り現時点では発見できなかった。

ITU でアプリケーションやシステムの規格において暗号アルゴリズムが指定されている可能性がある例（”encryption”のキーワードで検索される例）
ITU SECU：(サイバーセキュリティガイド)
ITU H.235：(音声暗号)
ITU Y.SecMechanisms:（NGN セキュリティ機構）
ITU-R M.1457：(国際間携帯通信インタフェース)　等

**② 業界団体（IETF,IEEE,W3C など）が定めた標準**
＜例＞
○IETF(Internet Engineering Task Force)[10]
RFC[11]でアルゴリズムとして標準化されている例（いずれも Informational として扱われる）
RFC2994, RFC3174, RSA3447, RFC3713　等

RFC でアプリケーションやプロトコルの規格において暗号アルゴリズムが指定されている可能性がある例（メインプロトコルの場合 Standard として扱われることが多い）
RFC4132, 5746：SSL/TLS 関連
RFC2451, 3602, 4306, 4312：IPsec 関連
RFC3565, 3657, 3853, 4056, 5083, 5652, 5750, 5751, 5754: S/MIME, CMS 関連
RFC3156: OpenPGP 関連
RFC3962, 4120: Kerberos 関連
RFC4344, 4419, 4432: SSH 関連　等

[9] ISO/IEC JTC1/SC27 以外が管理
[10] インターネット技術の標準化を推進する任意団体
[11] RFC:Request For Comments

○IEEE (The Institute of Electrical and Electronics Engineers)
IEEE でアルゴリズムとして標準化されている例
IEEE P1363：(公開鍵暗号) 等

IEEE でアプリケーションやプロトコルの規格において暗号アルゴリズムが指定されている可能性がある例
IEEE802.1AE：LAN 等での伝送関連
IEEE802.3AH：GE-PON 技術関連
IEEE802.11i：無線 LAN 技術関連 等

○W3C(World Wide Web Consortium)[12]
WWW でアルゴリズムとして標準化されている例
規格名を見る限り現時点では発見できなかった。

WWW でアプリケーションやプロトコルの規格において暗号アルゴリズムが指定されている可能性がある例
XML Encryption, XML Signature：XML 関連 等

**③ 特定の国が定めた標準（FIPS,ANSI,ETSI など）**
＜例＞
○FIPS (Federal Information Processing Standards)[13]
FIPS/SP でアルゴリズムとして標準化されている例
FIPS180-3, FIPS186-3, FIPS197, SP800-67 等

FIPS/SP でアプリケーションやプロトコルの規格において暗号アルゴリズムが指定されている可能性がある例
FIPS191：Guideline for The Analysis of Local Area Network Security,
FIPS201, SP800-78-1：Personal Identity Verification
SP800-52: Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations
SP800-77: Guide to IPsec VPN 等

○米国規格協会（ANSI : American National Standards Institute）[14]
ANSI でアルゴリズムとして標準化されている例
ANSI X9.30, ANSI X9.42, ANSI X9.63, ANSI X9.65, ANSI X9.82 等

ANSI でアプリケーションやプロトコルの規格において暗号アルゴリズムが指定されている可能性がある例
ANSI X9.24：(リテール金融サービス)
ANSI X9.96：(XML 暗号化)
ANSI X9.97：(金融向けセキュアデバイス) 等

[12] WWW で利用される技術の標準化をすすめる団体
[13] 米国標準技術研究所（NIST）が策定している規格
[14] 米国における工業的な分野の標準化組織

○欧州電気通信標準化機構（ETSI: European Telecommunications Standards Institute）[15]

ETSI でアルゴリズムとして標準化されている可能性がある例

TS 102 176　　等

ETSI でアプリケーションやプロトコルの規格において暗号アルゴリズムが指定されている可能性がある例

TS 187 003：(NGN セキュリティ)

TS 102 731：(高度交通システム)

TS 102 573：(電子署名基盤)　　等

**④ 特定の組織（RSA,EMV など）が定めた標準**

＜例＞

○PKCS(Public-Key Cryptography Standards)[16]

PKCS でアルゴリズムとして標準化されている例

PKCS#1, PKCS#3, PKCS#13　　等

PKCS でアプリケーションやプロトコルの規格において暗号アルゴリズムが指定されている可能性がある例

PKCS#7：(電子メール)

PKCS#11：(トークンインターフェース)　　等

○EMV（Europay-Mastercard-Visa）[17]

EMV でアプリケーションやプロトコルの規格において暗号アルゴリズムが指定されている例

EMV4.2：(クレジットカード用 IC 仕様)　　等

暗号技術の国際標準に関しては、暗号アルゴリズムの標準のみを対象とすべきか、アプリケーションやシステムの規格で採用されている標準を考慮する必要があるか、どのような標準（アルゴリズム又はアプリーション）が、実際の製品開発の参考にされているか、いずれの標準化機関により標準化されている標準を国際標準ととらえるか、標準化団体により標準の位置づけの違い、事実上の標準となっている場合の考え方等の観点から、議論を行い、以下のような意見があげられ、さらに検討を続けることとなった。

- 標準化団体によっては技術毎にステータスがあり、取り扱いが異なる場合があるのではないか。
- 標準化されていなくても社会インフラレベルまで普及した場合は、評価すべきではないか。
- 標準化団体の動向が運用に与える影響を調査すべきではないか。

[15] ヨーロッパにおける電気通信産業に関する標準化組織

[16] RSA セキュリティが定めた公開鍵暗号標準

[17] 3 大クレジットカード会社がクレジットカード共通仕様として標準化したもの

- 電子政府推奨暗号を選定する際の国際標準化の整理であれば、国際標準の暗号からどのような暗号を選ぶかというのではなく、それぞれの暗号がどのような条件を満たしていれば国際標準化されていると言えるのかという視点で検討するのが良いのではないか。
- 応募暗号と事務局提案暗号との間で対象となる標準化団体やステータスなどについての考え方が異なっても良いのではないか。

### ６．２．４　運用監視暗号リスト登録暗号の危殆化対策の検討

運用監視暗号リストに登録されることなった暗号の危殆化対策の検討については、当該リストへの登録、当該リストからの削除の評価基準等の具体化が必要なことから、暗号技術の製品化、利用実績等の評価も踏まえつつ、暗号技術の３リストへの登録見直しの期間や方法の具体化を図った上で、次期リストの運用監視暗号リストに登録する暗号の危殆化対策の検討を次年度に実施していくこととした。

### ６．２．５　先導的技術調査ワーキンググループ

危殆化対策など、優先すべき課題があるとの指摘を踏まえ、あらためて調査・検討の優先度が高いセキュリティ技術を整理した上で、ワーキンググループの設置の検討を行うこととした。

## ７．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、2010 年度以降以下の活動を実施していく。

（１）電子政府推奨暗号リストの改訂に向けた取り組み

①　電子政府推奨暗号公募への応募暗号の安全性評価

2013年の電子政府推奨暗号リストの改訂に向けて、応募暗号技術に対する安全性の第一次評価を行う。

②　暗号技術の実装性能評価等に関する検討

応募暗号技術及び現行の電子政府推奨暗号に対するハードウェア及びソフトウェア実装性評価の評価項目、評価手法、評価基準を作成する。また、サイドチャネル攻撃耐性に関する確認項目、確認手法を決定する。

③　暗号技術の製品化、利用実績等の評価手法の検討

暗号技術の製品化・利用実績の評価手法、国際標準化動向に関する調査・検討を行い、評価項目の具体化、判断基準の検討等を行う。

（２）電子政府推奨暗号の監視活動

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

（３）暗号技術の危殆化対策に関する調査・検討

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

（４）暗号実装技術等に関する調査・検討

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

（５）暗号モジュール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に関する国際的な標準規格化活動に対して貢献する。

別添１

# 電子政府推奨暗号リスト

平成１５年２月２０日
総　　務　　省
経　済　産　業　省

| 技術分類 | | 名称 |
|---|---|---|
| 公開鍵暗号 | 署名 | DSA |
| | | ECDSA |
| | | RSASSA-PKCS1-v1_5 |
| | | RSA-PSS |
| | 守秘 | RSA-OAEP |
| | | RSAES-PKCS1-v1_5(注 1) |
| | 鍵共有 | DH |
| | | ECDH |
| | | PSEC-KEM(注 2) |
| 共通鍵暗号 | 64 ビットブロック暗号(注 3) | CIPHERUNICORN-E |
| | | Hierocrypt-L1 |
| | | MISTY1 |
| | | 3-key Triple DES(注 4) |
| | 128 ビットブロック暗号 | AES |
| | | Camellia |
| | | CIPHERUNICORN-A |
| | | Hierocrypt-3 |
| | | SC2000 |
| | ストリーム暗号 | MUGI |
| | | MULTI-S01 |
| | | 128-bit RC4(注 5) |
| その他 | ハッシュ関数 | RIPEMD-160(注 6) |
| | | SHA-1(注 6) |
| | | SHA-256 |
| | | SHA-384 |
| | | SHA-512 |
| | 擬似乱数生成系(注 7) | PRNG based on SHA-1 in ANSI X9.42-2001 Annex C.1 |
| | | PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) Appendix 3.1 |
| | | PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) revised Appendix 3.1 |

注釈：(注 1)　SSL3.0/TLS1.0 で使用実績があることから当面の使用を認める。

(注 2)　KEM（Key Encapsulation Mechanism）-DEM(Data Encapsulation Mechanism)構成における利用を前提とする。

(注 3)　新たな電子政府用システムを構築する場合、より長いブロック長の暗号が使用できるのであれば、128 ビットブロック暗号を選択することが望ましい。

(注 4)　3-key Triple DES は、以下の条件を考慮し、当面の使用を認める。

1)　FIPS46-3 として規定されていること

2)　デファクトスタンダードとしての位置を保っていること

(注 5)　128-bit RC4 は、SSL3.0/TLS1.0 以上に限定して利用することを想定している。なお、リストに掲載されている別の暗号が利用できるのであれば、そちらを使用することが望ましい。

(注6)　新たな電子政府用システムを構築する場合、より長いハッシュ値のものが使用できるのであれば、256ビット以上のハッシュ関数を選択することが望ましい。ただし、公開鍵暗号での仕様上、利用すべきハッシュ関数が指定されている場合には、この限りではない。

(注7)　擬似乱数生成系は、その利用特性上、インタオペラビリティを確保する必要性がないため、暗号学的に安全な擬似乱数生成アルゴリズムであれば、どれを利用しても基本的に問題が生じない。したがって、ここに掲載する擬似乱数生成アルゴリズムは「例示」である。

## 電子政府推奨暗号リストに関する修正情報

| 修正日付 | 修正箇所 | 修正前 | 修正後 | 修正理由 |
|---|---|---|---|---|
| 平成 17 年<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 構成員・オブザーバ名簿

## １．暗号技術検討会

暗号技術検討会の構成員、オブザーバは、以下の通り。（敬称略）

| | | |
|---|---|---|
| 座 長 | 今井　秀樹 | 中央大学理工学部電気電子情報通信工学科教授 |
| 顧 問 | 辻井　重男 | 中央大学研究開発機構教授 |
| | 宇根　正志 | 日本銀行金融研究所情報技術研究センター企画役 |
| | 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（社団法人電気通信事業者協会代表兼務） |
| | 加藤　義文 | 社団法人テレコムサービス協会技術委員会委員長 |
| | 金子　敏信 | 東京理科大学理工学部電気電子情報工学科教授 |
| | 国分　明男 | 財団法人ニューメディア開発協会顧問・首席研究員 |
| | 櫻井　幸一 | 九州大学大学院システム情報科学研究院情報工学部門教授 |
| | 佐々木　良一 | 東京電機大学未来科学部情報メディア学科教授 |
| | 宝木　和夫 | 社団法人電子情報技術産業協会情報セキュリティ委員会委員 |
| | 武市　博明 | 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）

| | |
|---|---|
| 木本　裕司 | 内閣官房情報セキュリティセンター内閣参事官 |
| 髙橋　浩二 | 警察庁情報通信局情報管理課長 |
| 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 |
| 高地　圭輔 | 総務省自治行政局地域政策課地域情報政策室長 |
| 中野　正康 | 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 |
| 江原　健志 | 法務省民事局商事課長 |
| 中前　隆博 | 外務省大臣官房情報通信課長 |
| 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 |
| 小貫　卓也 | 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 |
| 井上　幹邦 | 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 |
| 篠田　陽一 | 独立行政法人情報通信研究機構情報通信セキュリティ研究センター長 |
| 大塚　玲 | 独立行政法人産業技術総合研究所セキュリティ基盤技術研究チーム長 |
| 矢島　秀浩 | 独立行政法人情報処理推進機構セキュリティセンター長 |
| 亀田　繁 | 財団法人日本情報処理開発協会電子署名・認証センター長 |
| 岸本　博之 | 財団法人金融情報システムセンター監査安全部長 |

## ２．暗号方式委員会

暗号方式委員会の委員、オブザーバは、以下の通り。（敬称略、五十音順）

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

（オブザーバ）

| | |
|---|---|
| 中嶋　良彰 | 内閣官房　情報セキュリティセンター　内閣参事官補佐 |
| 山口　利恵 | 内閣官房　情報セキュリティセンター　主査 |
| 根本　農史 | 内閣官房　情報セキュリティセンター　主査 |
| 末澤　洋 | 警察庁　情報通信局　情報管理課　課長補佐 |
| 松本　和人 | 総務省　行政管理局　行政情報システム企画課　課長補佐 |
| 館　圭輔 | 総務省　自治行政局　地域情報政策室　課長補佐 |
| 山﨑　敏明 | 総務省　自治行政局　市町村課　理事官 |
| 佐々木　信行 | 総務省　情報流通行政局　情報セキュリティ対策室　係長 |
| 荒木　美敬 | 外務省　大臣官房　情報通信課 |
| 山中　豊 | 経済産業省　産業技術環境局　情報電子標準化推進室　課長補佐 |
| 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 |
| 千葉　修治 | 防衛省　陸上幕僚監部　情報通信・研究課　情報通信室　２等陸佐 |
| 滝澤　修 | 独立行政法人情報通信研究機構情報通信セキュリティ研究センター 防災・減災基盤技術グループ　グループリーダ |
| 大塚　玲 | 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 セキュリティ基盤技術研究チーム長 |

## ３．暗号実装委員会

暗号実装委員会の委員、オブザーバは、以下の通り。（敬称略、五十音順）

| | | |
|---|---|---|
| 委員長 | 松本　勉 | 国立大学法人横浜国立大学大学院環境情報研究院　教授 |
| 委員 | 植村　泰佳 | 電子商取引安全技術研究組合　専務理事 |
| | 大須賀　勝美 | ＮＴＴエレクトロニクス株式会社<br>セイフティ・ネットワーク事業部開発部　主事 |
| | 亀田　繁 | 財団法人日本情報処理開発協会電子署名・認証センター<br>センター長 |
| | 佐藤　恒夫 | 三菱電機株式会社情報技術総合研究所情報セキュリティ技術部<br>開発第一チーム　チームリーダ |
| | 佐藤　証 | 独立行政法人産業技術総合研究所情報セキュリティ研究センター<br>ハードウェアセキュリティ研究チーム　研究チーム長 |
| | 﨑山　一男 | 国立大学法人電気通信大学電気通信学部情報通信工学科　准教授 |
| | 清水　秀夫 | 株式会社東芝研究開発センター<br>コンピュータアーキテクチャ・セキュリティ　ラボラトリー<br>研究主務 |
| | 高橋　芳夫 | 株式会社ＮＴＴデータ技術開発本部ＳＩアーキテクチャ開発センタ<br>シニアエキスパート |
| | 角尾　幸保 | 日本電気株式会社共通基盤ソフトウェア研究所<br>情報通信セキュリティＲＧ　主席研究員 |
| | 鳥居　直哉 | 株式会社富士通研究所ソフトウェア＆ソリューション研究所<br>セキュアコンピューティング研究部　部長 |
| | 福永　利徳 | 日本電信電話株式会社ＮＴＴ情報流通プラットフォーム研究所<br>情報セキュリティプロジェクト　研究主任 |
| | 本間　尚文 | 国立大学法人東北大学　大学院情報科学研究科　准教授 |
| | 松崎　なつめ | パナソニック株式会社デジタル･ネットワーク開発センター<br>ネットワーク技術開発グループネットワーク第四チーム<br>チームリーダ |
| | 渡辺　大 | 株式会社日立製作所システム開発研究所第七部　研究員 |

（オブザーバ）

| | |
|---|---|
| 赤澤　康之 | 警察庁　情報通信局　情報管理課　係長 |
| 伊東　信孝 | 警察大学校　警察情報通信研究センター　基礎研究室　助教授 |
| 松本　和人 | 総務省　行政管理局　行政情報システム企画課　課長補佐 |
| 荒木　美敬 | 外務省　大臣官房　情報通信課 |
| 山中　豊 | 経済産業省　産業技術環境局　情報電子標準化推進室　課長補佐 |

| | |
|---|---|
| 千葉　修治 | 防衛省　陸上幕僚監部　情報通信・研究課　情報通信室　２等陸佐 |
| 石川　正興 | 防衛省　技術研究本部　電子装備研究所　ネットワーク技術研究部<br>情報保障室長 |
| 坂下　圭一 | 防衛省　運用企画局　情報通信・研究課　情報保証室長 |
| 滝澤　修 | 独立行政法人情報通信研究機構情報通信セキュリティ研究センター<br>セキュリティ基盤グループ/防災・減災基盤技術グループ<br>グループリーダー |
| 青木　林 | 財団法人日本規格協会　情報技術標準化研究センター　事務局 |
| 川村　信一 | 独立行政法人産業技術総合研究所　情報セキュリティ研究センター<br>副研究センター長 |

## ４．暗号運用委員会

暗号運用委員会の委員、オブザーバは、以下の通り。（敬称略、五十音順）

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

（オブザーバ）

| | |
|---|---|
| 中嶋　良彰 | 内閣官房　情報セキュリティセンター　内閣参事官補佐 |
| 山口　利恵 | 内閣官房　情報セキュリティセンター　主査 |
| 根本　農史 | 内閣官房　情報セキュリティセンター　主査 |
| 松本　和人 | 総務省　行政管理局　行政情報システム企画課　課長補佐 |
| 佐々木　信行 | 総務省　情報流通行政局　情報セキュリティ対策室　係長 |
| 山中　豊 | 経済産業省　産業技術環境局　情報電子標準化推進室　課長補佐 |
| 日高　隆 | 経済産業省　大臣官房　情報システム厚生課 セキュリティ担当課長補佐 |

別添３

# 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 10 月 1 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 内に設置された暗号方式委員会、暗号実装委員会及び暗号運用委員会が、評価結果に基づき、「CRYPTREC 暗号リスト（仮称）」（以下、「次期リスト」という。）への暗号技術の記載について判定し、暗号技術検討会に答申します。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10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。

⑴ 電子政府推奨暗号リスト
⑵ 推奨候補暗号リスト
⑶ 運用監視暗号リスト
⑷ 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候補暗号リスト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。

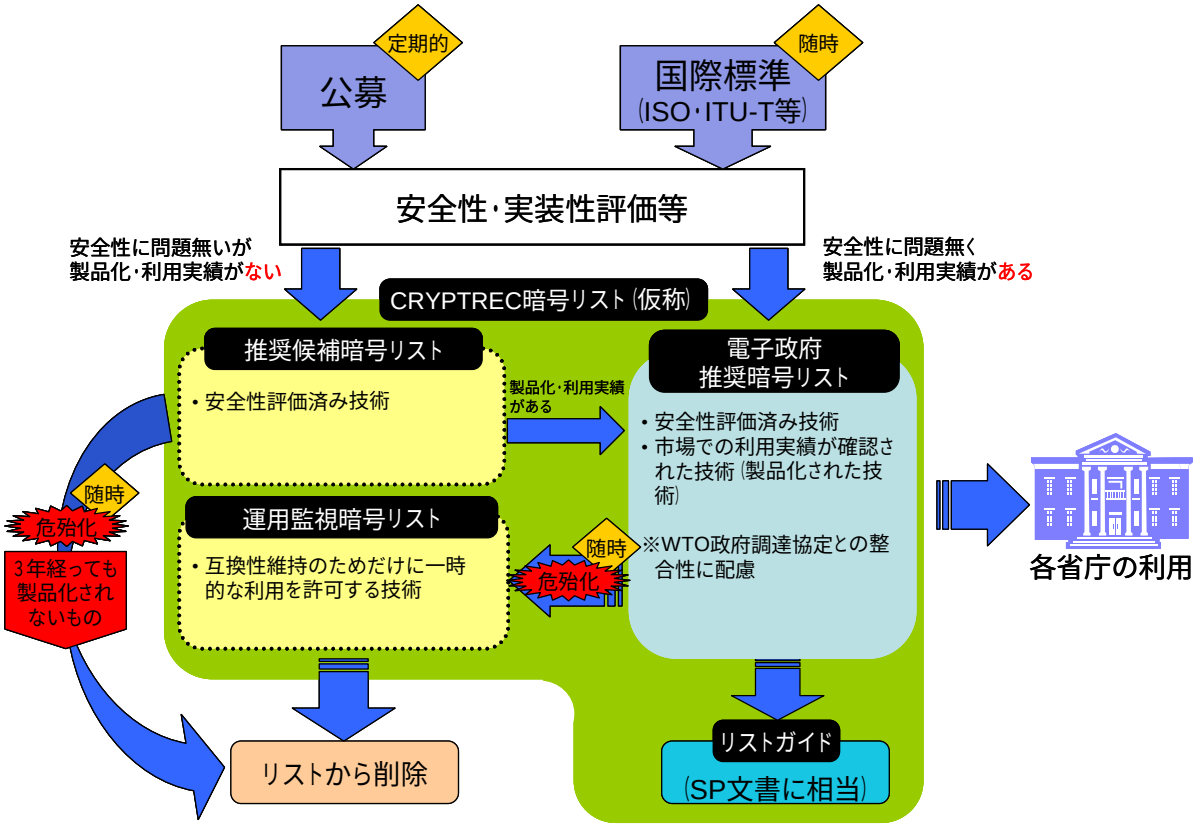



図 1．リスト改訂概念（案）

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

　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) 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、推奨候補暗号リスト、あるいは電子政府推奨暗号リストへ登録するための、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

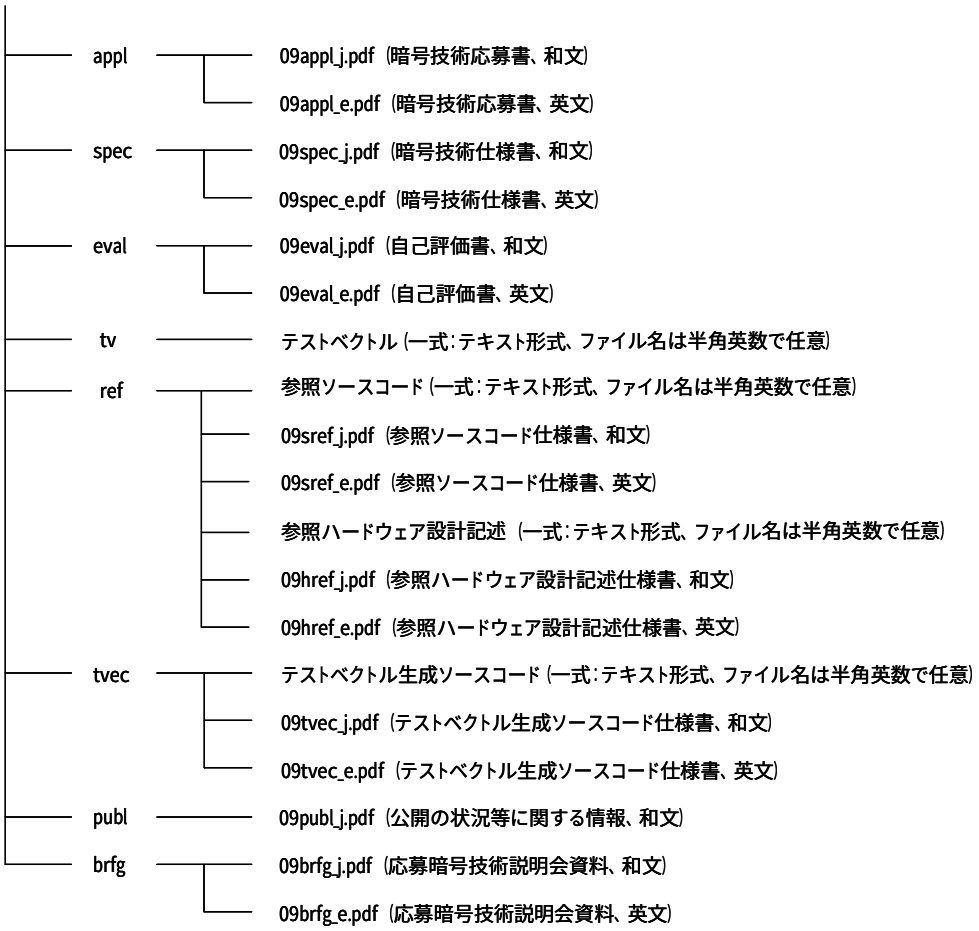



図 2．提出書類（電子データ）の構成図

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. 応募暗号説明会発表資料

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 2 日、3 月 3 日 |
| 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 |

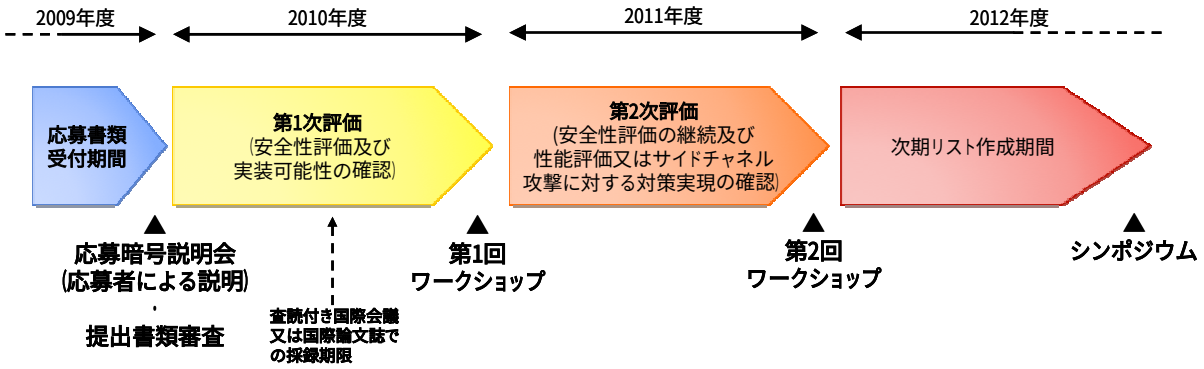



図 3．評価スケジュール（予定）

### 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、暗号実装委員会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。

プログラムなどの詳細については、確定次第、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。

また､応募者数の事前把握のため､応募を予定されている方は2009年11月30日(月)までに、CRYPTREC 事務局あてご連絡をお願いいたします。なお、この事前連絡は任意のものであり、書類等の提出を求めるものではありません。

## 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、開催時点までの暗号方式委員会及び暗号実装委員会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？