# 暗号技術検討会

# ２００６年度報告書

暗号技術検討会

２００７年３月

目次

## １．はじめに

「IT 新改革戦略」において、「いつでも、どこでも、誰でも IT の恩恵を実感できる社会の実現」が目標として掲げられる一方で、Winny(ウィニー)などを介して感染するウイルスや特定の相手を狙って仕掛ける「ターゲット型攻撃」などの新たな脅威も発生しており、IT を安心・安全に利用できる環境の構築は喫緊の課題となっている。

2006 年 2 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、我が国の情報セキュリティ問題全般に関する中長期計画(2006～2008 年度の３ケ年計画)として「第１次情報セキュリティ基本計画」が決定された。同計画においては、暗号技術に関して今後取り組むべき重点政策として、「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、暗号の適切な利用方策について検討を進める」こととされており、電子政府推奨暗号の監視等を任務とする本暗号技術検討会の役割は更に重要性を増している。

2006 年度の暗号技術検討会においては、暗号技術監視委員会及び暗号モジュール委員会の協力を得て、電子政府推奨暗号の監視、電子政府推奨暗号の安全性・信頼性確保のための調査、暗号モジュール評価に係るセキュリティ要件の作成等に加え、「SHA-1 の安全性に関する見解」を取りまとめた。なお、暗号モジュールについては、暗号モジュール委員会の成果を活用し、独立行政法人情報処理推進機構において、本年４月からの本格運用に向け、現在「暗号モジュール試験及び認証制度」が試行されている等、安全性確保に向けた取組みが進展しつつある。

「第１次情報セキュリティ基本計画」の年度計画である「セキュア・ジャパン 2006」では、「電子政府推奨暗号について、その危殆化が発生した際の取扱い手順及び実施体制の検討を進める」こととされているため、今後、SHA-1 に係る見解等、暗号技術検討会の発信する情報を踏まえ、内閣官房情報セキュリティセンターをはじめとする政府機関において、暗号の危殆化に備えた対応体制等が整備されることを期待するものである。

なお、2006 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 2006」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。

2007 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、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 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技術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。

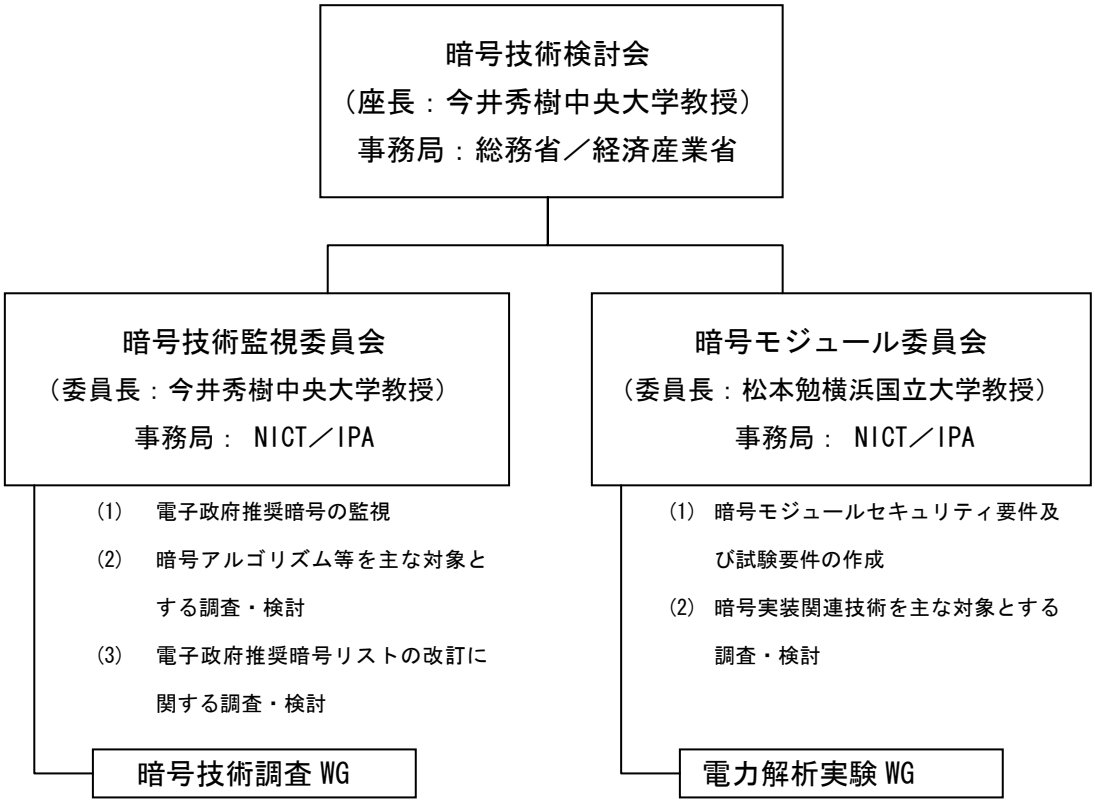



図 1　2006 年度の CRYPTREC の体制図

## ２．３．暗号技術検討会メンバー

（構成員）※肩書は 2007 年 3 月末現在。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 |
| | 岡崎　宏 | 情報通信ネットワーク産業協会常務理事 |
| | 岡本　栄司 | 筑波大学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常任理事・開発グループ長 |
| | 櫻井　幸一 | 九州大学大学院システム情報科学研究院教授 |
| | 佐々木　良一 | 東京電機大学工学部情報メディア学科教授 |
| | 宝木　和夫 | 社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 |
| | 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<br>情報セキュリティ技術部次長 |
| | 松本　勉 | 横浜国立大学大学院環境情報研究院教授 |
| | 松本　泰 | 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 |
| 内藤　伸悟 | 警察庁情報通信局情報技術解析課長 |
| 中井川　禎彦 | 総務省行政管理局行政情報システム企画課情報システム管理官 |
| 田中　敦仁 | 総務省自治行政局自治政策課情報政策企画官 |
| 相澤　哲 | 法務省民事局商事課長 |
| 杵渕　正己 | 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 |
| 和泉　章 | 経済産業省産業技術環境局標準課情報電気標準化推進室長 |
| 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 |
| 大蒔　和仁 | 独立行政法人産業技術総合研究所情報処理研究部門長（兼）<br>研究エディネータ（情報通信担当） |
| 三角　育生 | 独立行政法人情報処理推進機構セキュリティセンター所長 |

亀田　繁　　財団法人情報処理開発協会電子署名・認証センター長
郡山　信　　財団法人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

2006 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】2006 年 7 月 7 日（金）
（主な議題）・暗号技術検討会の運営方針
・暗号技術検討会 2006 年度活動計画
・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】2007 年 3 月 27 日（火）
（主な議題）・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
・今後の CRYPTREC 活動
・暗号技術検討会 2006 年度報告書

## ３．暗号技術監視委員会活動報告

### ３．１．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平成 15 年度に組織され、活動を行っている。以下に、平成 18 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。

#### ３．１．１．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正を考慮して、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。

#### ３．１．２．監視状況

（１）共通鍵暗号及びその他（ハッシュ関数や擬似乱数生成系）の安全性評価について

平成 18 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。また、平成 17 年度評価において進展

が見られた SHA-1（ハッシュ関数）については、「暗号技術検討会　２００５年度報告書」の３．１．２．節　監視状況、（１）ハッシュ関数の安全性評価について（ｐ．８）でまとめられた状況から変化はなかった。なお、本安全性評価の成果については、参照 1 のとおり「SHA-1 の安全性に関する見解」として、暗号技術監視委員会承認（平成 18 年 6 月 28 日）を経て、検討会事務局から内閣官房情報セキュリティセンターへ提出された。

（参照１）SHA-1 の安全性に関する見解

## SHA-1 の安全性に関する見解

平成 18 年６月 28 日
暗号技術監視委員会

電子政府における情報セキュリティ確保のために、各府省の情報システム構築において暗号を利用する場合には、「各府省の情報システム調達における暗号の利用方針」（平成 15 年 2 月 28 日 行政情報システム関係課長連絡会議了承）において、必要とされる安全性・信頼性などに応じ、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ものとされている。
また、情報セキュリティ政策会議から出された「政府機関の情報セキュリティ対策のための統一基準（2005 年 12 月版（全体版初版））」（平成 17 年 12 月 13 日）においても、新規（更新を含む。）に暗号化又は電子署名の付与のアルゴリズムを導入する場合には、電子政府推奨暗号リストの中から選択することが基本遵守事項として明記されている。

電子政府推奨暗号リストでは、ハッシュ関数の SHA-1 は注釈において、『（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。』と規定している。

SHA-1については、最近の研究動向によれば、Wangらにより$2^{69}$回以下のSHA-1の実行回数で同じハッシュ値を持つ2つのメッセージが発見できる衝突探索攻撃アルゴリズムが発表され、CRYPTRECで検証した結果、$2^{69}$回のSHA-1の実行回数で衝突発見できることの妥当性は検証された。また、近い将来に$2^{63}$回以下のSHA-1の実行回数で衝突発見できることも妥当性があるとの結論を得た。このことは、SHA-1を長期間にわたって利用する電子署名やタイムスタンプなどは、近い将来にSHA-1の衝突発見が現実的な問題に発展する可能性を示唆している。
このようなことから、電子署名やタイムスタンプのように長期間にわたって利用するシステムでは、新規（更新を含む）に暗号化又は電子署名の付与のアルゴリズムを導入する場合には、SHA-256 ビット以上のハッシュ関数の使用を薦める。

＊参照：CRYPTREC Report 2005「暗号技術監視委員会報告」
http://cryptrec.jp/

（参考）

各種文献等を踏まえ、以下の参考情報を提供する。ただし、CRYPTREC として、ここで引用した文献等の内容の正確性、信頼性、妥当性を保証するものではない。

ハッシュ関数のSHA-1 を利用している電子署名システムにおいて、仮に $2^{63}$回のSHA-1の実行回数で衝突が起こるということになれば、例えば、一般に用いられているCPUで構成される「PCクラスタ型」[i]のスーパーコンピュータのうち 2006 年 4 月現在で国内最高速のもの[ii]を使用して約 7 年間計算すると、同じハッシュ値を生成する異なる文書などが作成できる可能性がある。

具体的には、電子署名された原文と同一の電子署名を生成できる別の文書が作成（偽造）され得るということであり、電子署名された文書（原文）の真がんの判断ができなくなるおそれがある。

現時点では、電子署名された文書の有効性に疑問は生じていないが、SHA-1 の衝突に関する最近の研究結果は、今後、暗号研究の進歩やコンピュータ処理能力の向上[iii]などによって、文書の有効期間が本来よりも著しく短縮され、電子署名された文書であっても、否認、なりすまし又は改ざんといった脅威にさらされる危険性があることを示唆している。

衝突発見に要する時間の目安（推定）

| SHA-1 の実行回数 | 2006 年 4 月現在 |
|---|---|
| $2^{69}$回 | ・国内最高速のスパコンで約 462 年以下 |
| $2^{63}$回 | ・国内最高速のスパコンで約 7 年以下 |

処理時間については、計算アルゴリズムや計算機のアーキテクチャなどに依存して大きく変わり得るため、この年数はあくまで推定である。なお、今後の進歩によっては、スーパーコンピュータだけではなく、インターネットを利用して世界中の国々で分散処理を行う分散コンピューティングシステム[iv]によっても、本推定以上の衝突発見能力を実現できる可能性がある。

---

[i]クラスタとは、複数のコンピュータをネットワークを介して相互に接続して統合し、より高い性能を求めたコンピュータ・システムのこと。

[ii]東京工業大学 学術国際情報センター スーパーコンピューティング・グリッドシステム「TSUBAME (Tokyo-tech Supercomputer and UBiquitously Accessible Mass-storage Environment)」(http://www.gsic.titech.ac.jp/Japanese/Publication/pressrelease04032006.html.ja)

[iii]たとえば、ムーアの法則(http://www.intel.co.jp/jp/developer/technology/silicon/mooreslaw/index.htm)など。

[iv]たとえば、distributed.net(http://distributed.net/)など。

（２）公開鍵暗号方式の安全性評価について

電子政府推奨暗号リストに記載されている公開鍵暗号方式の安全性は、(a) IFP（n=pq 型素因数分解問題)、(b) DLP （有限体上の離散対数問題)、(c) ECDLP （楕円曲線上の離散対数問題）のいずれかの困難性に依存している。「暗号技術検討会　２００２年度報告書」の３．２．４．節　暗号技術評価結果の概要、（１）公開鍵暗号方式の総評について（ｐ．１２）では、それぞれ以下のような判断をしてきた。

（a）IFP （n=pq 型素因数分解問題）

安全性の観点から法パラメータ n=pq のサイズは 1024 ビット以上のものを利用することを強く推奨する。

（b）DLP （有限体上の離散対数問題）

安全性の観点からパラメータ p のサイズは 1024 ビット以上を選択することを強く推奨する。

（c）ECDLP （楕円曲線上の離散対数問題）

安全性の観点から群位数が 160 ビット以上の素因子をもつようなパラメータを選択することを強く推奨する。

一方、NIST（National Institute of Standards and Technology：(米国)国立標準技術研究所）は、Special Publication 800-57、Recommendation for Key Management - Part 1: General (Revised)[1] の 66 ページのTable 4 において、以下の表 1 に示されるような推奨値を与えており、2010 年以降、上記のような数論的問題の困難性に関するパラメータ選択では強い安全性を求められる利用に関しては安全性が十分でないことを示唆している。

表 1 Table 4: Recommended algorithms and minimum key sizes

| Algorithm security lifetimes | Symmetric key algorithms (Encryption & MAC) | FFC (e.g., DSA, D-H) | IFC (e.g.,RSA) | ECC (e.g.,ECDSA) |
|---|---|---|---|---|
| Through 2010 (min. of 80 bits strength) | 2TDEA<br>3TDEA<br>AES-128<br>AES-192<br>AES-256 | Min.:<br>L=1024;<br>N=160 | Min.:<br>L=1024 | Min.:<br>f=160 |
| Through 2030 (min. of 112 bits strength) | 3TDEA<br>AES-128<br>AES-192<br>AES-256 | Min.:<br>L=2048;<br>N=224 | Min.:<br>L=2048 | Min.:<br>f=224 |
| Beyond 2030 (min. of 128 bits strength) | AES-128<br>AES-192<br>AES-256 | Min.:<br>L=3072;<br>N=256 | Min.:<br>L=3072 | Min.:<br>f=256 |

[1] http://csrc.nist.gov/publications/nistpubs/ から入手可能。

また、欧州連合（European Union）が策定した研究と技術開発のための第6次(2002-2006)枠組み計画（Sixth Framework Programme）[2]において、科学・技術の研究・開発を支援するための情報社会技術プログラム（Information Societies Technology Programme）の一環として、ECRYPT - European Network of Excellence for Cryptology[3]という情報セキュリティ研究活動が実施されているが、そこから公表されている年次報告書（ECRYPT Yearly Report on Algorithms and Keysizes[4]）では、Chapter 7、Table 7.2において、以下の表2に示されるような各種暗号技術におけるパラメータサイズの比較が示されている。

表2　Table 7.2: Key-size Equivalence

| Security(bits) | RSA | DLOG | | EC |
|---|---|---|---|---|
| | | Field size | Subfield | |
| 48 | 480 | 480 | 96 | 96 |
| 56 | 640 | 640 | 112 | 112 |
| 64 | 816 | 816 | 128 | 128 |
| 80 | 1248 | 1248 | 160 | 160 |
| 112 | 2432 | 2432 | 224 | 224 |
| 128 | 3248 | 3248 | 256 | 256 |
| 160 | 5312 | 5312 | 320 | 320 |
| 192 | 7936 | 7936 | 384 | 384 |
| 256 | 15424 | 15424 | 512 | 512 |

そこで、平成 18 年度は、上記の数論的問題の困難性への攻撃に関する計算量について調査・検討を行い、セキュリティパラメータの選択及び利用期限に関する考察を行った。特に、IFP （n=pq 型素因数分解問題）に関しては、理論的な考察だけではなく、ソフトウェア実装及びハードウェア実装を実施し[5]、実験を基にして攻撃に必要な計算量の見積もりを行った。以下に、上記の数論的問題の困難性の安全性評価について見解を示す。詳細は、３．２．２節またはCRYPTREC Report 2006[6]を参照のこと。

（A）IFP （n=pq 型素因数分解問題）[7]

（イ）問題の困難性について

現在のところ最も有望である一般数体ふるい法を用いて計算量を評価した。今回は時間的な制約から、「ふるい処理」部分のみを実装することで、計算量を見積もることとした。以下の表 3 にソフトウェア評価の結果を示す。また、以下の表

[2] http://www.cordis.lu/fp6/
[3] http://www.ecrypt.eu.org/index.html
[4] http://www.ecrypt.eu.org/documents.htmlから入手可能。
[5] 実際には、それぞれ、暗号技術監視委員会から依頼された外部評価者、及び、情報通信研究機構（NICT）の委託研究先による実装である。
[6] http://www.cryptrec.jp/report.htmlから入手可能。
[7] 表１では、IFC欄に相当する。

4 にハードウェア評価の結果を示す。

表 3　ふるい処理の計算量の推測（単位は、AMD Athlon 64 2.2GHz x 年[8]との比）

| 法パラメータのサイズ（ビット） / ふるい処理のパラメータ選択 | 768 | 1024 | 1536 | 2048 |
|---|---|---|---|---|
| 実メモリに制約（2GB RAM）がある場合の見積もり | 1108 | $8.4 \times 10^{6}$ | $4.5 \times 10^{12}$ | $25 \times 10^{16}$ |
| ふるい処理に関するパラメータ選択をより改善した場合の見積もり | - | $2.8 \times 10^{6}$ | $0.92 \times 10^{12}$ | $4.4 \times 10^{16}$ |
| 実メモリにそれほど制約がない場合の見積もり | - | $1.05 \times 10^{6}$ | $0.18 \times 10^{12}$ | $0.4 \times 10^{16}$ |

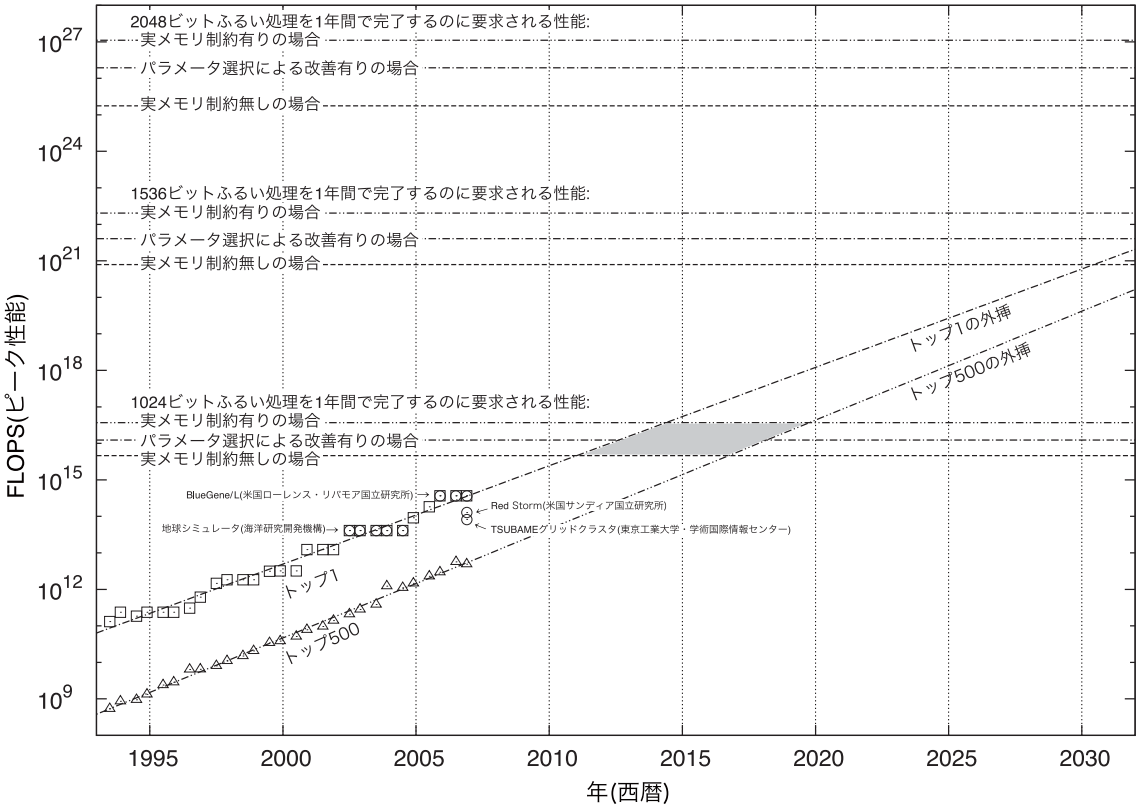
表 4　ハードウェア（HW）とソフトウェア（SW）の処理性能の比率

| 法パラメータのサイズ（ビット） | 1024 | 1536 | 2048 |
|---|---|---|---|
| 処理性能の比率（SW の処理時間／HW の処理時間） | 5.73 | 8.83 | 10.41 |

表 3 で示された計算量を換算して、素因数分解が所定の時間内に可能になるものと推測される時期について考察するため、Ｐ２２～２３に示す７つの前提の下、将来獲得するものと予測される計算処理能力の推移と、IFP （n=pq 型素因数分解問題）を１年間で完了する計算機の FLOPS（ピーク性能)値をグラフに表すと、図 2 のようになる。

図 2　1 年間でふるい処理を完了するのに要求される処理性能の予測[9]

[8] AMD社製CPUであるAthlon 64 2.2GHz を 1 年間動作し続けたときに得られる計算量を意味する。
[9] 参考（コスト）: 地球シミュレータ（海洋研究開発機構）約 400 億円、TSUBAME（東京工業大学)約 20 億円、BlueGene/L（米国ローレンス・リバモア国立研究所）約 1 億ドル、Red Storm（米国サンディア国立研究所）約 9000 万ドル




以上をまとめると、新たな攻撃法によって、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。しかしながら、計算機性能の向上による計算能力の増大が主な危殆化の要因とした場合[10]、攻撃者の獲得可能な解読計算能力が、HPC[11]の傾向を最も良く示すという意味で、スーパーコンピュータの世界第 1 位[12]と同等なレベルで向上していくと仮定すると、法パラメータn=pq のサイズが 1024 ビットのIFP （n=pq 型素因数分解問題）が 1 年間の計算によって攻撃可能になる時期については、2010 年～2020 年の間と推定することができた。

従って、NIST が示す推奨アルゴリズムと最小鍵長（表 1）における、法パラメータ n=pq のサイズが 1024 ビットの IFP （n=pq 型素因数分解問題）の利用期限の根拠の 1 つとして解読計算能力の増大が推定されるが、不明な部分も残るため、引き続き注意していくことが必要と考える。

（ロ）実装不備がもたらす脆弱性について

次に、国際学会等においては、RSA 署名（電子政府推奨暗号リストに記載されている RSASSA-PKCS1-v1_5 を含む）について、公開指数（public exponent） e が小さく、署名検証時のパディング長のチェックを無視した不適切な実装に対する攻撃

[10]今後の研究によって、一般数体ふるい法等のアルゴリズムの改良により処理時間が短縮することがあり得るが、今回の評価では無視している

[11] High Performance Computingの略。

[12] TOP500.OrgのWebサイト、http://www.top500.org/による。

方法が 2006 年 8 月に発表されている。従って、

- RSA署名の公開指数には、e=3 等の小さな値を利用しない
- ハッシュ値の後に無意味なデータが加えられていないかどうかの確認をする

等の偽造防止策が必要である（詳細は、３．１．４節を参照のこと）。

(B) DLP （有限体上の離散対数問題）[13]

新たな攻撃法によって、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。安全性の観点から、DLP （有限体上の離散対数問題）のパラメータ p は、IFP （n=pq 型素因数分解問題）の法パラメータ n=pq のサイズと同等にしておけば十分である。

(C) ECDLP （楕円曲線上の離散対数問題）[14]

新たな攻撃法や既存の攻撃法の改良によって、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。ECDLP （楕円曲線上の離散対数問題）のパラメータを群位数が 160 ビット以上の素因子をもつように選択すれば、少なくとも 2010 年までは安全である。

### （３）暗号技術標準化動向

NISTが 2006 年 8 月に開催した 2nd Hash Workshop[15]では、主に次世代ハッシュ関数（AHS[16]）の仕様、および公募プロセスに関連する議論が行われた。以下に概要を記載する。なお、他の組織における暗号技術標準化動向を含め、詳細は、CRYPTREC Report 2006 を参照のこと。

(a) 今後の公募スケジュールについて

AHSアルゴリズムの公募については、NISTより仮のタイムスケジュール[17]が以下の表 5 ように示されている。

[13] 表 1 では、FFC欄に相当する。
[14] 表 1 では、ECC欄に相当する。
[15] http://www.csrc.nist.gov/pki/HashWorkshop/index.htmlからたどれる。
[16] Advanced Hash Standardの略。
[17] 1Q（1 月-3 月）、2Q（4 月-6 月）、3Q（7 月-9 月）、4Q（10 月-12 月）

表 5　次期ハッシュ関数選定の仮スケジュール

| | |
|---|---|
| Year 1(2007) | |
| 1Q | ・ 最小限の要求仕様、公募における要件、評価基準の案の公開とパブリックコメントの募集 |
| 2Q | ・ コメントに対する対応の実施 |
| 3Q | ・ 最小限の要求仕様、公募における要件、評価基準の最終版の公開<br>・ 新ハッシュ関数の募集開始 |
| Year 2(2008) | |
| 3Q | ・ 新ハッシュ関数の公募締め切り |
| 4Q | ・ 応募アルゴリズムのレビューと、基本的な公募要件に沿った候補のアルゴリズムの選定。<br>・ 第 1 ラウンドの候補をアナウンスする 1st Hash Function Candidate Conference の開催し、応募者によるプレゼンテーションの実施<br>・ 第 1 ラウンドの候補アルゴリズムに対するパブリックコメントの募集 |
| Year 3(2009) | |
| 4Q | ・ パブリックコメントの締め切り<br>・ 2nd Hash Function Candidate Conference を開催し、応募アルゴリズムの評価結果についての議論、応募者によるアルゴリズムの修正の提示を行う |
| Year 4(2010) | |
| 1Q | ・ 応募アルゴリズムに対するパブリックコメントの結果を参考に、最終候補アルゴリズムの選定作業を実施し、選定のためのレポートを作成する |
| 2Q | ・ 最終候補アルゴリズムのアナウンスと選定レポートの公開<br>・ 最終候補アルゴリズムの応募者よる修正の実施<br>・ 最終ラウンドの開始 |
| Year 5(2011) | |
| 2Q | ・ 最終ラウンドのパブリックコメント終了 |
| 3Q | ・ Final Hash Function Candidate Conference の開催し、最終候補アルゴリズムの応募者によるコメントについてのディスカッションの実施 |
| 4Q | ・ パブリックコメントの結果を参考に、次期ハッシュ関数を決定<br>・ 最終選定結果のレポートを作成<br>・ 次期ハッシュ関数のアナウンス |
| Year 6(2012) | |
| 1Q | ・ 次期ハッシュ関数の仕様のドラフトを作成<br>・ ドラフトの公開とパブリックコメントの募集 |
| 2Q | ・ パブリックコメントの締め切りと、コメントに対する対応の実施 |
| 3Q | ・ 次期ハッシュ関数に対する商務長官の承認の実施 |

(b) 次世代ハッシュ関数公募の仕様

2007 年 1 月に、NISTはAHSアルゴリズムの公募について、Federal Register Vol.72[18]に掲載しており、現在パブリックコメントを募集している。パブリックコメントの締め切りは 2007 年 4 月 27 日である。

[18] http://www.csrc.nist.gov/pki/HashWorkshop/FederalRegister/Federal%20Register%20Notice%20for%20Requirements%20&%20Criteria%20-%20E7-927.pdf

### ３．１．３．暗号技術監視委員会開催状況

平成 18 年度、暗号技術監視委員会は、表 6 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は、表 7 の通り計 6 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 6　暗号技術監視委員会の開催

| 回 | 年月日 | 議題 |
|---|---|---|
| 第 1 回 | 平成 18 年 7 月 24 日 | 活動方針確認、暗号技術監視状況報告 |
| 第 2 回 | 平成 19 年 3 月 9 日 | 暗号技術監視状況報告、CRYPTREC report 2006 審議 |

表 7　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 | 平成 18 年 8 月 4 日 | 第 1 回公開鍵暗号 WG（活動方針の審議） |
| 第 2 回 | 平成 18 年 9 月 7 日 | 第 2 回公開鍵暗号 WG（活動内容の審議） |
| 第 3 回 | 平成 18 年 12 月 27 日 | 第 3 回公開鍵暗号 WG（中間報告の審議） |
| 第 4 回 | 平成 19 年 2 月 5 日 | 第 4 回公開鍵暗号 WG（最終報告の審議） |
| 第 5 回 | 平成 19 年 2 月 5 日 | 第 5 回公開鍵暗号 WG（同上） |
| 第 6 回 | 平成 19 年 3 月 7 日 | 第 6 回公開鍵暗号 WG（CRYPTREC report 2006 審議） |

### ３．１．４．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

平成 18 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。

今回調査した研究発表で、電子政府推奨暗号の安全性に大きく関わるものとして、ハッシュ関数SHA-1 に対する解析の進展がある。SHA-1 は近年、安全性への懸念が高まり、昨年度は衝突の発見が 58 段までだったのが 64 段まで伸びており[19]、今後の研究に注目する必要がある。

監視要員等を派遣した国際会議は、表 8 に示すとおりである[20]。

表 8　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 |
|---|---|---|---|
| FC | Financial Cryptography and Data Security '06 | Anguilla, British West Indies | 2006/2/27～2006/3/2 |
| TCC | Theory of Cryptography Conference 2006 | New York, USA | 2006/3/4～2006/3/7 |

[19] 実際に使われるSHA-1 は 80 段であり、衝突が発見されたのはその短縮版である。
[20] 昨年度報告書に記載しなかった分を含む。

| | | | |
|---|---|---|---|
| FSE | Fast Software Encryption 2006 | Graz, Austria | 2006/3/15～2006/3/17 |
| PKC | 9th International Conference on Theory and Practice of Public Key Cryptography | New York, USA | 2006/4/24～2006/4/26 |
| EUROCRYPT | EUROCRYPT 2006 | St. Petersburg, Russia | 2006/5/28～2006/6/1 |
| ACNS | 4th International Conference on Applied Cryptography and Network Security | Singapore, Singapore | 2006/6/6 ～2006/6/9 |
| ACISP | 11th Australasian Conference on Information Security and Privacy | Melbourne, Australia | 2006/7/3 ～2006/7/5 |
| SAC | 13th Annual Workshop on Selected Areas in Cryptography | Montreal, Canada | 2006/8/17 ～2006/8/18 |
| CRYPTO | CRYPTO 2006 | Santa Barbara, USA | 2006/8/20 ～2006/8/24 |
| NIST HW | NIST Second Hash Workshop | Santa Barbara, USA | 2006/8/24 ～2006/8/25 |
| VietCrypt | International Conference on Cryptology in Vietnam 2006 | Hanoi, Vietnam | 2006/9/25 ～2006/9/28 |
| Asiacrypt | Asiacrypt 2006 | Shanghai, China | 2006/12/4 ～2006/12/7 |
| SCIS(国内) | Symposium on Cryptography and Information Security 2007 | 長崎, 日本 | 2007/1/23 ～2007/1/26 |
| CT-RSA | RSA Conference Cryptographers Track | San Francisco, USA | 2007/2/5 ～2007/2/9 |
| TCC | The fourth Theory of Cryptography Conference | Amsterdam, Netherlands | 2007/2/22 ～2007/2/24 |

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

(a)　ハッシュ関数の解読技術

SHA-1 については従来の衝突発見段数の記録が 58 段から 64 段に更新（フルラウンドは 80 段）されたことが注目される。従来の衝突発見の記録が 1 ブロックのテキストに対し 80 段中 58 段の短縮版までだったのに対し、この結果では 2 ブロックのテキストで 64 段短縮版まで伸ばすのに成功している。この研究は、非線形キャラクタリスティックという新概念の導入により衝突発見効率を向上させた点に特徴がある。[Finding SHA-1 Characteristics, Christophe De Cannière and Christian Rechberger , Asiacrypt 2006]

現在 MAC (Message Authentication Code)として HMACS-SHA-1 が SHA-1 と組み合わされて標準的に用いられているが、近年の SHA-1 に対するアタックを利用した HMACS-SHA-1 などに対するアタックについて新しい報告があった。HMAC と NMAC は 1996 年にカリ

フォルニア大学サンディエゴ校の Bellare 氏により提案されていたメッセージ認証コードの方式で、特に HMAC は標準化され広く用いられている。今回の報告で、HMAC-MD4 や HMAC-MD5、HMAC-SHA-0 については現実的なアタックが可能であり、HMAC-SHA-1 については 34 段短縮版 SHA-1 を用いた HMAC についてはアタック可能であるというものであったが、フルラウンド SHA-1 を用いた HMAC-SHA-1 については現段階でアタック不能である。[Forgery and Partial Key Recovery Attacks on HMAC and NMAC Using Hash Collisions, Scott Contini and Yiqun Lisa Yin, Asiacrypt 2006]

SHA-224, 256 についてもアタックの試みがあった。しかしこの結果は SHA-224 の場合で 19 段短縮版、SHA-256 の場合で 18 段短縮版の衝突発見が可能（フルラウンドは 64 段）というもので、現段階でフルラウンドの安全性は脅かされていない。[Analysis of Step-Reduced SHA-256, F.Mendel, N.Pramstaller, C.Rechberger and V.Rijmen, FSE 2006]

(b) ストリーム暗号の解読技術

ストリーム暗号については、ストリーム暗号の国際規格 ISO/IEC 18033-4 に採用されている SNOW 2.0 に対するアタックが発表されたことが注目される。このアタックは $2^{179}$の長さの出力系列を得ることにより統計的な偏りが検出できるというものである。まだ必要とされる系列長が長く、現実的な脅威にはなっていない。[Improved Linear Distinguishers for SNOW 2.0, K.Nyberg, J.Wallén C.Rechberger and V.Rijmen, FSE 2006]

(c)ブロック暗号の解読技術

ブロック暗号については、中国科学院の研究者による 7 段または 8 段簡略版 192 ビット鍵 AES に対する関連鍵不能差分攻撃による解析が注目される。従来の解読記録は更新してはいないため電子政府推奨暗号の安全性には影響は無いものの、近年中国が急速に暗号解析の研究レベルを向上させてきており、今後の動向に注目する必要がある。[Improved Related-Key Impossible Differential Attacks on Reduced-Round AES-192, Wentao Zhang, Wenling Wu, Lei Zhang and Dengguo Feng, SAC06]

(d)公開鍵暗号の解読技術

RSA署名について、正しくない実装に対する効果的な攻撃方法が発表された。具体的には、PKCS #1 (RSA Cryptography Standard) 等に基づくRSA署名について公開鍵の指数 e が小さく、署名検証時のパディング長のチェックを省略した実装に対し、不正につける string を調節することにより、検証で受理されてしまう署名の偽造が比較的容易に実現できる可能性を指摘した。CRYPTRECとしては、既に2002年にその危険性を指摘していた。( CRYPTREC Report 2002 P112 参照) 本発表をトリガに各種関係機関はレポート・対応策などを提示した。[Forging some RSA signatures with pencil and paper, Daniel Bleichenbacher, CRYPTO 2006, Rump session]

RSA 暗号に関して、秘密鍵 d が小さい場合の効率的な解析手法の研究結果がいくつか従来結果として示されている。CRT(Chinese Remainder Theorem) 等を用いる方法や Lattice を利用した方法、従来方法の効率的な部分を併用した方法など結果が示されている。また、

dが小さい場合の攻撃手法に対する一般化への試みなども行なわれている。[New

Attacks on RSA with Small Secret CRT-Exponents, Daniel Bleichenbacher and Alex May, PKC 2006], [A Strategy for Finding Roots of Multivariate Polynomial with New Applications in Attacking RSA Variants, Ellen Jochemsz and Alexander May, Asiacrypt 2006]

また、離散対数問題の解法に関しても研究が活発化してきている。実質的な脅威をもたらすにはいたっていないが、その効率的な解析方法に関する研究は進んでおり、以後の動向に注意が必要である。[An Algorithm to Solve the Discrete Logarithm Problem with the Number Field Sieve, An Commeine and Igor Semaev, PKC 2006], [Cryptanalysis of an Efficient Proof of Knowledge of Discrete Logarithm, Sébastien Kunz-Jacques, Gwenaëlle Martinet, Guillaume Poupard and Jacques Stern, PKC 2006]

その他、近年活発化している動きとしては、IDベースを利用した各種効率のよいアルゴリズム・プロトコルやLatticeを用いた解析などが挙げられる。欧米では、電子投票に関する研究なども注目されているようであり、 CRYPTO 2006 の Invited Talk の一つにもなっていた。[Receipt-Free Universally-Verifiable Voting With Everlasting Privacy, Tal Moran and Moni Naor, CRYPTO 2006], [Defeating Malicious Servers in a Blind Signatures Based Voting System, Sebastien Canard, Matthieu Gaud and Jacques Traore, FC06], [Cryptographic Protocols for Electronic Voting, David Wagner, CRYPTO 2006 Invited talk]

安全性証明のモデルに関しては、従来よく用いられていたランダムオラクルモデルを離れる動きがあり、より現実に即したモデルの模索が活発化している。一例では、フォーマルメソッドの概念とを融合したモデルの検討[Automated Security Proofs with Sequences of Games, Bruno Blanchet and David Pointcheval, CRYPTO 2006]や複数のアルゴリズムが混在するようなプロトコルの安全性証明等に有効と考えられる ユニバーサルコンポーザブルモデル(Universal Composable Model)に関して、従来提案されているモデルからより使いやすいモデルや現実に即したモデルへのアプローチに関する研究も進んできている。また、近年取上げられ始めている危殆化等の概念等を加味したモデルの検討なども発表された。

[Generalized Environmental Security from Number Theoretic Assumptions, Tal Malkin, Ryan Moriart and Nikolai Yakovenko, TCC 2006] , [Universally Composable Security with Global Setup, Ran Canetti, Yevgeniy Dodis, Rafael Pass and Shabsi Walfish, TCC 2007], [Long-term Security and Universal Composability, Jörn Müller-Quade and Dominique Unruh, TCC 2007]

## ３．２．暗号技術調査ワーキンググループ

### ３．２．１．概要

平成 18 年度は、数論的問題（素因数分解問題や有限体及び楕円曲線上の離散対数問

題）の困難性について調査を行い、主に公開鍵暗号方式のセキュリティパラメータサイズの選択について検討を行うため、新規に公開鍵暗号ワーキンググループを組織した。ワーキンググループ（WG）が活動した主要活動項目は、表9の通りである。

表9　平成18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 |
|---|---|---|
| 公開鍵暗号WG | 太田和夫 | ①素因数分解問題の困難性の計算量についての調査・検討<br>②有限体及び楕円曲線上の離散対数問題の計算量についての調査・検討<br>③電子政府推奨暗号リストに記載されている公開鍵暗号技術に関する仕様書の改訂等(NIST や ANSI における見直しに伴うもの)について調査・検討 |

NIST の FIPS 186-3(ドラフト版)と FIPS 186-2 との差異については、今年度調査を行ったが、数論的問題の困難性の有する計算量について調査・検討に注力したため、電子政府推奨暗号リストに記載されている公開鍵暗号技術に関する仕様書の改訂等(NIST や ANSI における見直しに伴うもの)の詳細な調査・検討は、次年度に実施することとした。なお、詳細は、CRYPTREC Report 2006 を参照のこと。

### ３．２．２．公開鍵暗号ワーキンググループ

（１）調査背景

数論的問題の困難性に関する評価については、電子政府推奨暗号リストの作成に向けて、数論的問題の困難性に依存して暗号プリミティブの安全性を主張する暗号スキームを横断的に評価した際、2002 年度までにCRYPTREC Report 2002[21]にまとめられた。

その他に、電子政府推奨暗号リストの作成と並行してCRYPTRECが実施した素因数分解実験プロジェクトによって 2003 年度までに調査・研究された内容については、CRYPTREC Report 2003 にまとめられ、実験データから合成数のサイズが 1024 ビットの一般数体ふるい法に必要な計算量見積もりについて予測がなされている。また、同年度には、一般数体ふるい法を効率的に行うための計算機のアーキテクチャであるTWIRLの実現可能性についても調査を行ってきている[22]。

[21] http://www2.nict.go.jp/y/y213/cryptrec_publicity/c02_report.pdf、http://www.cryptrec.jp/report.html から入手可能。
[22] http://www2.nict.go.jp/y/y213/cryptrec_publicity/c03-wat040427.pdf、http://www.cryptrec.jp/report.htmlから入手可能。

以上の調査・研究を踏まえ、CRYPTRECでは、当面の間、1024 ビット以上のIFP（n=pq 型素因数分解問題）の安全性には問題がないものと判断してきた。しかし、電子政府推奨暗号リストの作成から既に約 4 年経ち、当時の評価が現在も有効かどうかを含めて再評価を行う必要性が高まってきている。EUにおいてはECRYPTが年次報告書（ECRYPT Yearly Report on Algorithms and Keysizes[23]）において表 2（ｐ．１１）を提供し、各暗号技術におけるパラメータの比較を示している。米国においてはNISTがSP 800-57, Recommendation on Key Management, Part 1 において表 1（ｐ．１０）を提供しており、2010 年まではIFP （n=pq 型素因数分解問題）において 1024 ビット以上の法サイズの使用を推奨しているが、それ以降は 2048 ビットを推奨している。

本ワーキンググループでは、電子政府関連システムに限らず、暗号技術を利用したシステムに関する業務に就いている方々に、安全なパラメータサイズを含めて公開鍵暗号技術の安全な利用方法について情報を提供する必要があると考えている。

（２）活動内容

(A) IFP （n=pq 型素因数分解問題）の安全性評価

【調査概要】

＜ソフトウェア評価＞

表 1 に示された NIST による「法サイズが 1024 ビットの IFP （n=pq 型素因数分解問題）が 2010 年まで有効(暗に、それ以降の有効性は保証していない)」との根拠を、ソフトウェア実装・実行して実績が上がっている技術を基にして、検証することを目的とした。

現在のところ最も有望である一般数体ふるい法を用いて、IFP （n=pq 型素因数分解問題）の計算量を評価した。今回は時間的な制約から、1536 ビットと 2048 ビットの「ふるい処理」のみをソフトウェア実装することで、計算量を見積もることとした。また、ほぼ同様な手順で評価された 768 ビットと 1024 ビットの結果についても補足をしている。ここで、一般数体ふるい法における計算時間の主要項である「ふるい処理」と「線形代数処理」は、漸近的な実行時間の評価において同等であり、これまでのところ、一般数体ふるい法により分解された合成数の世界記録において、ふるい処理の方が線形代数処理より多くの時間を要していることが知られていることから、この計算量見積もりには妥当性がある。

得られた評価結果は、表 3（ｐ．１２）に示されている。評価に利用した CPU は AMD Athlon 64 2.2GHz (2GB RAM)である。表 3（ｐ．１２）の各行において、下の行ほどふるい処理のパラメータ選択が最適化されているが、仮定の積み重ねであるため見積もりの精度が落ちてくることに注意する。詳細は、CRYPTREC Report 2006 を参照のこ

[23] http://www.ecrypt.eu.org/documents.htmlから入手可能。

と。

＜ハードウェア評価＞

素因数分解専用ハードウェアの処理性能を、動作可能なハードウェアとして設計・製造されたシステムを基に、その処理性能を計測し、ソフトウェアの性能と比較することで推測した。ハードウェア装置としては、情報通信研究機構(NICT)による委託研究[24]によって開発された素因数分解ハードウェア装置(ふるい処理装置)を利用して、実験を行った。

ふるいの結果として抽出される要素の個数、並びに、ふるい処理が終了するまでに実施するlog 加算の延べ回数は、ふるい処理を行なう際に入力するパラメータを固定すれば[25]、ふるい処理を実施する装置(専用ハードウェア、PC上のソフトウェア)にかかわらず一定である。このことを利用して、ハードウェア(HW)とソフトウェア(SW)における処理時間の比較を行った。

得られた評価結果は、表 4（ｐ．１２）に示されている。現在のところ、専用ハードウェア装置の実装に要するコストは不明であるが、仮に実装が可能となった場合には、攻撃可能となる時期が、ソフトウェア処理による場合よりもさらに早まる可能性がある[26]。詳細は、CRYPTREC Report 2006 を参照のこと。

＜計算量と計算能力についての考察＞

表 3（ｐ．１２）で示された計算量を換算して、素因数分解が所定の時間内に可能になるものと推測される時期について考察する。

第一に、IFP （n=pq 型素因数分解問題）の攻撃に必要な計算量に関しては、以下のような前提を設けた。

前提 1: ふるい処理の計算量見積もりについては、表 3 の値を採用する。

前提 2: 素因数分解のアルゴリズムに関しては、これから 30 年間はブレークスルーがなく、一般数体ふるい法よりも効率の良いアルゴリズムが発見されないものとする。また、アルゴリズム等の大きな改良もないものとする。つまり、計算機性能の向上による計算能力の増大が、安全性を脅かす主な要因とみなす。

前提 3: ふるい処理の計算が 1 年間で処理し終えることをもって、素因数分解が完了したものとみなす。漸近的な実行時間の評価において、ふるい処理と線形代数処理は同じオーダーであること、一般数体ふるい法により分解された合成数の世界記録において、これまでのところふるい処理の方が線形代数処理よ

---

[24] 情報通信研究機構（NICT）の委託研究「素因数分解の困難性に基づく暗号の技術的評価に関する研究開発」、http://www2.nict.go.jp/q/q265/s802/s1_seika.htm

[25] 実際には、処理時間を最適化するために、法サイズに依存して変えるのが一般的である。

[26] 独立行政法人理化学研究所が構築したピーク性能 1 ペタフロップス(PFLOPS)を実現する分子動力学シミュレーション専用コンピュータ・システムMDGRAPE-3 のような可能性が考えられる。http://www.riken.jp/r-world/info/release/press/2006/060619/index.html

り多くの時間を要していることから[27]、このように仮定した。

第二に、計算機性能の将来予測に関しては、さまざまなモデルを設定可能であるが[28]、本ワーキンググループでは、以下のような前提を設けた。

前提 4: 計算機性能の将来予測に関しては、スーパーコンピュータのベンチマーク結果[29]の 1 位から 500 位を 1993 年から半年毎に集計しているWebサイトTOP500.Orgに過去掲載された計算機におけるFLOPS(ピーク性能)の統計値を外挿することにより算出する。ここを取り上げたのは、このような情報を収集している場所が他にはなく、実際に構築されたスーパーコンピュータのうち、高性能なものの代表として相応しいと考えられるからである。

前提 5: 近年の汎用 CPU 及びスーパーコンピュータにおける整数演算性能と浮動小数点演算性能については、ほぼ同等であるとした。

最後に、計算量の換算に関しては、以下のような前提を設けた。

前提 6: 一般数体ふるい法の処理はもっぱら CPU の整数演算を用いるものなので、計算能力の比較には、整数演算性能を用いるのが適当であるが、前提 5 により、CPU における浮動小数点演算性能への換算を行った。

前提 7: 基準点として用いる CPU の FLOPS（ピーク性能)値は、(クロック周波数)x(浮動小数点演算ユニット数)によって見積もる。Athlon 64 2.2 GHz の場合は、4.4 GFLOPS である。

以上の前提の基、将来獲得するものと予測される計算処理能力の推移と、IFP（n=pq 型素因数分解問題）を１年間で完了する計算機の FLOPS（ピーク性能)値をグラフに表すと、図２（ｐ．１３）のようになる。

【IFP （n=pq 型素因数分解問題）の安全性評価のまとめ】

新たな攻撃法によって、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。しかしながら、計算機性能の向上による計算能力の増大が主な危殆化の要因とした場合[31]、攻撃者の獲得可能な解読計算能力が、HPCの傾向を最も良く示すという意

---

[27] DLP （有限体上の離散対数問題）の場合には、線形代数処理の方がふるい処理よりも時間がかかることがある。

[28] 独立行政法人 情報処理推進機構、電子政府行政情報化事業「将来の暗号技術に関する安全性要件調査」調査報告書、2004 年 2 月、第 4 章
http://www.ipa.go.jp/security/fy15/reports/crypt_requirement/documents/crypt_requirement.pdf

[29] 実際の順位付けには、浮動小数点演算性能を測るために、一般的な線形方程式系を解く速さを測定するLINPACKというベンチマークプログラムの結果が利用されている。LINPACK性能はピーク性能とは異なる。また、計算機のアーキテクチャによっては、ここには載らないようなスーパーコンピュータもある。

[30] http://www.top500.org/

[31] 今後の研究によって、一般数体ふるい法等のアルゴリズムの改良により処理時間が短縮することがあり得るが、今回の評価では無視している。

味で、スーパーコンピュータの世界第 1 位[32]と同等なレベルで向上していくと仮定すると、法パラメータn=pq のサイズが 1024 ビットのIFP （n=pq 型素因数分解問題）が 1 年間の計算によって攻撃可能になる時期については、2010 年～2020 年の間と推定することができた。

従って、NIST が示す推奨アルゴリズムと最小鍵長（表 1、ｐ． ８）における、法パラメータ n=pq のサイズが 1024 ビットの IFP （n=pq 型素因数分解問題）の利用期限の根拠の 1 つとして解読計算能力の増大が推定されるが、不明な部分も残るため、引き続き注意していくことが必要と考える。

（B）DLP （有限体上の離散対数問題）の安全性評価

【調査概要と DLP の安全性評価のまとめ】

現時点では、新たな攻撃法によって、安全性に懸念を持たせるような事態は生じていないことを確認した。

DLP （有限体上の離散対数問題）と IFP （n=pq 型の素因数分解問題）の漸近的な計算量のオーダーは同じである。現状では DLP （有限体上の離散対数問題）の解かれた記録は、IFP （n=pq 型素因数分解問題）での解かれた記録に比べ、10 進 50 桁程度ビットのサイズが小さい。これは DLP （有限体上の離散対数問題）に関する評価研究が素因数分解問題の研究ほど活発に行われていないためだと考えられる。

従って、DLP （有限体上の離散対数問題）ベースの安全な鍵サイズは、IFP （n=pq 型の素因数分解問題）ベースの安全な鍵サイズと同等である。詳細は、CRYPTREC Report 2006 を参照のこと。

（C）ECDLP （楕円曲線上の離散対数問題）の安全性評価

【調査概要と ECDLP の安全性評価のまとめ】

現時点では、新たな攻撃法や既存の攻撃法の改良によって、安全性に懸念を持たせるような事態は生じていないことを確認した。

楕円加算・倍算1回の処理速度と、共通鍵暗号の暗号化1回分の処理速度を比較すると、概算で同程度であることが経験的に知られている。一般的なECDLP （楕円曲線上の離散対数問題）に対する解法としては、Rho 法が最も有効であり、ECDLP （楕円曲線上の離散対数問題） の入力サイズを k とすると、その計算量は$O(2^{k/2})$となる[33]。このことから、ECDLP に基づく公開鍵暗号の安全な鍵サイズの評価には、共通鍵暗号の安全な鍵サイズの評価を用いた。

---

[32] TOP500.OrgのWebサイト、http://www.top500.org/による。

[33] $f(n)=O(g(n))$ とは、n に依存しない正の定数 c と整数 m が存在して、$n \geqq m$ である任意の n について $f(n) \leqq cg(n)$ が成立することを意味し、このとき、$f(n)$ は オーダー $g(n)$ であるという。

従って、ECDLP （楕円曲線上の離散対数問題）に基づく公開鍵暗号の安全な鍵サイズは、160ビット以上であれば、少なくとも2010年までは安全であると評価できる。詳細は、CRYPTREC Report 2006を参照のこと。

# ４．暗号モジュール委員会活動報告

## ４．１．暗号モジュール委員会の概要

### ４．１．１．暗号モジュール委員会の活動目的と経緯

暗号を組み込んだ製品の安全性を実現するには、安全性が確認された暗号の利用が不可欠であり、2003 年 2 月に発表された電子政府推奨暗号リストに記載された暗号から選択することによりこの条件は満たされる。しかし、暗号を組み込んだ製品の安全性を保つにはこれだけでは不十分であり、暗号アルゴリズムが適切に実装されていることを確認する必要がある。

適切な暗号実装を確認する仕組みとして、米国・カナダでは CMVP として試験及び認証の制度が実施されている。CRYPTREC では、このような制度の基となる暗号モジュールが満たすべきセキュリティ要件等の原案作成、及びその原案作成に必要となる実装攻撃に関する知見を得るための活動が必要と判断し、2003 年度から、暗号技術検討会の下に暗号モジュール委員会を設置し、活動項目を次のように定めた。

（１）暗号モジュールセキュリティ要件及び試験要件の策定

（２）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

暗号モジュール委員会では、（２）の一環として、INSTAC-8 及び INSTAC-32 仕様に準拠した標準プラットフォームを希望する委員に配布して、実験データの収集を実施してきた。2006 年度には、今まで独立であった個々の実験を組織化して加速するため、電力解析実験ワーキンググループを暗号モジュール委員委員会の下に設けた。

### ４．１．２．暗号モジュール委員会の開催状況

2006 年度の暗号モジュール委員会は、計 3 回開催された。各回会合の概要は表 10 のとおりである。

表 10　2006 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 | 平成 18 年 7 月 26 日<br>10:00～12:00 | 暗号モジュール委員会規程について<br>ISO/IEC JTC 1 SC 27/WG 3 のマドリッド会合報告<br>平成 18 年度暗号モジュール委員会活動計画（案）について<br>ISO/IEC 24759 1st WD のコメント案審議<br>電力解析実験 WG（仮称）設置について |
| 第 2 回 | 平成 18 年 12 月 15 日<br>13:30～15:30 | ISO/IEC JTC 1 SC 27/WG 3 の南アフリカ会合報告<br>ISO/IEC 24759 1st WD のコメント処理案審議について |

| | | |
|---|---|---|
| 第 3 回 | 平成 19 年 3 月 15 日<br>10:30～12:30 | ISO/IEC 24759 1st CD コメント案審議<br>CRYPTREC Report 2006(案)について<br>2007 年度のスケジュール(案)について |

2006 年度の電力解析実験ワーキンググループは、計 2 回開催された。各回会合の概要は表 11 のとおりである。

表 11　2006 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 | 平成 18 年 12 月 27 日<br>10:00～12:00 | 電力解析実験ワーキンググループ規程について<br>暗号モジュール委員会の運営方針<br>電力解析実験ワーキンググループ設立に至る背景と経緯<br>電力解析実験ワーキンググループ活動計画(案) |
| 第 2 回 | 平成 19 年 3 月 2 日<br>14:00～16:00 | 2006 年度まとめと報告書の作成について<br>2007 年度の活動について<br>電力解析関係発表論文 |

## ４．２．暗号モジュールセキュリティ要件の標準化に関する国際動向と対応

暗号モジュールに関するセキュリティ要件として国際的な影響力を持つものには次の２つがある。

（１）FIPS[34] 140-2（米国NIST[35]）

（２）ISO[36]/IEC[37] 19790

### ４．２．１．FIPS 140-2

FIPS 140-2 は、米国/カナダが共同運用しているCMVP[38]制度で利用されているセキュリティ要件に関する標準であり、米国NISTによって発行されている。この標準の関連文書に試験要件(DTR[39])と運用ガイダンス(IG[40])の 2 種類があり、NISTは必要に応じて適宜改訂している。DTRは暗号モジュールを試験する際の要件であり、IGは運用に関す

[34] Federal Information Processing Standard
[35] National Institute of Standards & Technology
[36] International Organization for Standardization
[37] International Electrotechnical Commission
[38] Cryptographic Module Validation Program
[39] Derived Test Requirements. 具体的な試験項目を規定。
[40] Implementation Guidance. 実際の運用のためのノウハウを記述。

る説明を記述している。

NIST/CSE[41]は5年ごとの定期見直しに従い、セキュリティ要件を次期バージョンFIPS 140-3 に改訂する作業を開始している。この準備及び周知のため、2004 年 9 月に“CMVP Symposium 2004”を開催した。2005 年 9 月には、FIPS 140-3 に盛り込むべき物理セキュリティ関連技術をテーマとした“NIST Physical Security Testing Workshop”が開催された。ここで、2007 年 3 月のFIPS 140-3 発効予定、2007 年 9 月のFIPS 140-2 の廃止予定というスケジュールが発表された。しかし、2006 年 12 月にNISTとIPAの間で開かれた定期会議ではFIPS 140-3 の最初のドラフト発表が 2007 年 1 月末と後退するなど、スケジュールは大幅に遅れている。

FIPS 140-2/-3 に関する詳細は、「４．３．１．FIPS 140-2 及び関連文書の概要」及び「４．３．２．FIPS 140-2 の改訂に関する動向」を参照のこと。

### ４．２．２．ISO/IEC 19790

ISO/IEC 19790 はFIPS 140-2 を元に作られた国際規格である。ISO/IEC JTC 1[42] SC 27/WG 3 のプロジェクトとして審議され、2005 年 12 月締め切りで行われたFDIS[43]投票で可決され、2006 年 3 月 1 日に発行された。

また、実際の運用に必要であるということで、FIPS 140-2 同様、ISO/IEC 19790 に対する試験要件の標準化が新規プロジェクトとして承認され、規格番号 24759 が割り当てられている。2005 年 11 月のクアラルンプールでプロジェクトの承認が報告され、エディタとしてRandy Easter(米国NIST)、コエディタとしてJean-Pierre Quemard(仏)とHans von Sommerfeldが任命された。現在、1st CD[44]の投票中であり、今後順調に進めば、2007 年 5 月のロシア会合でFCD投票に進むことが決まり、2008 年の前半にISO/IEC 24759 として発行される見込みである。

ISO/IEC 19790 に関する詳細は、「４．３．３．ISO/IEC 19790 に関する動向」を参照のこと。

## ４．３．活動内容と成果概要

### ４．３．１．FIPS 140-2 及び関連文書の概要

（１）FIPS 140-2 (SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES)

FIPS 140 は、コンピュータシステム及び電気通信システム内の暗号モジュールに対するセキュリティ要件を規定した、NIST が発行する米国連邦標準規格である。

---

[41] Communication Security Establishment
[42] Joint Technical Committee 1
[43] Final Draft International Standard
[44] Committee Draft

FIPS 140 は、政府及び産業界で構成されたワーキンググループによって開発された。1994 年 1 月に FIPS 140-1 が制定され、2001 年 5 月には FIPS 140-2 として改訂された。FIPS 140-2 は、ベンダ、試験機関、及びユーザ団体から寄せられたコメントに基づいた変更だけでなく、FIPS 140-1 が開発された以降に利用可能となった標準規格及び技術の変更も取り入れている。FIPS 140-2 は適宜改訂されており、2002 年 12 月の改訂版が 2007 年 3 月時点での最新版となっている。

FIPS 140-2 は、暗号モジュールのセキュアな設計及び実装のために、暗号モジュールが満たすべき 11 分野(暗号モジュールの仕様、暗号モジュールのポート及びインタフェース、役割・サービス・認証、有限状態モデル、物理的セキュリティ、動作環境、暗号鍵管理、電磁妨害/電磁両立性、自己テスト、設計保証、その他の攻撃への対処)のセキュリティ要求事項を規定しており、さらに、保護すべきデータの重要性と使用環境に応じて暗号モジュールを提供できるように、分野ごとに 4 段階のセキュリティレベル(セキュリティレベル 1～4)を規定している。

（２）DTR (Derived Test Requirements for FIPS PUB 140-2)

DTR は、暗号モジュールが FIPS 140-2 で規定されたセキュリティ要求事項を満たしているかどうかを試験する際に、試験者が実施しなければならない試験手順及びベンダが提供しなければならない情報を規定したものである。

DTR は FIP 140-2 と同様に適宜改訂されており、2004 年 3 月 24 日の改訂版が 2007 年 3 月時点での最新版となっている。

DTRは、全 11 章から構成されており、各章はFIPS 140-2 で規定された 11 分野に対応している。各章では、FIPS 140-2 に対応するセキュリティ要求事項をアサーション[45]として記述している。全てのアサーションはFIPS 140-2 から直接引用している。

各アサーションの次には、順に、ベンダが提供しなければならない情報[46]、試験者が実施しなければならない試験手順[47]を記述している。

（３）Implementation Guidance

Implementation Guidance は、CMVP、特に DTR に関する、ベンダや試験機関等からの問合せに対して、NIST 及び CSE が回答したコメントを CMVP に関するガイダンスとしてまとめたものである。

Implementation Guidance もFIPS 140-2 及びDTRと同様に適宜改訂されており、

[45] Assertion (ASと略す)。暗号モジュールが、設定された分野のセキュリティ要件を、設定されたセキュリティレベルで満足するために適用しなければならない宣言。
[46] Vender Evidence (VEと略す)
[47] Tester Evidence (TEと略す)

2007 年 3 月の改訂版[48]が 2007 年 3 月時点での最新版となっている。

Implementation Guidance は、全 17 節(OVERVIEW, GENERAL ISSUES, SECTION 1 から SECTION 14, EXPIRED IMPLEMENTAITON GUIDANCE)から構成される。

“SECTION 1 から SECTION 14”は、次図のように FIPS 140-2 の各節とそれぞれ対応しており、セキュリティ要件の分野ごとに整理され、記述されている。また、複数の分野に当てはまる内容については、最適な分野の SECTION に記述されている。

| Implementation Guidance | FIPS 140-2 |
|---|---|
| SECTION 1 ～ SECTION 11 | 4.1 ～ 4.11 |
| SECTION 12 | APPENDIX A |
| SECTION 13 | APPENDIX B |
| SECTION 14 | APPENDIX C |

“OVERVIEW”には“Implementation Guidance”の概要が記述されており、“GENERAL ISSUES”には、SECTION 1 から SECTION 14 の分野に特定されない全般的な問題が整理され、記述されている。また、取消された運用ガイダンスを記述するために、“EXPIRED IMPLEMENTAITON GUIDANCE”の節が用意されているが、現在、何も記述されていない。

### ４．３．２．FIPS 140-2 の改訂に関する動向

近年の暗号モジュールの実装や攻撃法に関する進歩は目覚しく、2001 年に発効した FIPS 140-2 は現状に合わなくなってきている。そこで、NISTは 5 年見直しとして、2006 年を目処とした後継のFIPS 140-3 への移行準備を進めてきた。その一環として、2004 年 9 月にメリーランド州でCMVP 2004 シンポジウム[49]、2005 年 9 月に物理セキュリティ試験のワークショップ[50]が開かれ、FIPS 140-3 に関する議論が行われるとともに、移行計画が発表されてきた。

2006 年 12 月 17 日～22 日には、米国ワシントンDC近郊のメリーランド州 ゲイザースバーグでNISTの情報セキュリティ関連部門CSD[51]とIPAセキュリティセンターの定期会議が開催され、テーマの一つとして暗号モジュール試験及び認証制度が取り上げられた。参加者は、28 名で、内訳は米国NIST(13)、米国商務省(1)、カナダCSE(1)、経済産業省(2)、産業技術総合研究所(2)、日本規格協会(2)、NRIセキュアテクノロジーズ(1)、IPA(6)であった。

---

[48] 日本語版は 2005 年 12 月版が 2007 年 3 月時点での最新版となっている。
[49] CMVP 2004 Symposium: http://csrc.nist.gov/cryptval/cmvp2004/
[50] Physical Security Testing Workshop: http://csrc.nist.gov/cryptval/physec/physecdoc.html
[51] Computer Security Division

この会議は NIST の CSD と IPA セキュリティセンターが定期的に開催するものであり、今回、暗号モジュール試験及び認証制度が５つの主要議題の１つとして選ばれ、12 月 18 日午後に実施された。

＜FIPS 140-3 の概要＞

この会議において、FIPS 140-2 の後継規格である FIPS 140-3 についての次のようなアナウンスがあった。

・セキュリレベルは 5 レベルとなる（FIPS 140-2 は 4 レベルであり、2004 年 9 月の CMVP 2004 では 6 レベルとすることが示唆されていた）。
・11 章からなる。EMI[52]に関する章は無くなった。FSM[53]はデザインアシュアランス（設計保証）の章に入れた。
・新しい章（分野）は 2 つ増えた。ひとつは、ソフトウェアセキュリティ、あとのひとつはnon-invasive attack[54]（非破壊攻撃）。
・ソフトウェアセキュリティの中にはハードウェア、ソフトウェア、ハイブリッドの 3 タイプのモジュールがある。ハイブリッドモジュールは IG1.9 に定義されている。
・非破壊攻撃は、FIPS 140-2 では、4 章 11 節の Mitigation of Other Attacks で記述していた。FIPS 140-3 では、独立させるとともに、セキュリティレベル 3 から 5 までのレベルで要求する。但し、要求内容は FIPS 140-2 レベルであり、DTR でもっと詳しく書く予定である。

＜FIPS 140-3 への改訂スケジュールについて＞

この会議において、FIPS 140-3 への改訂スケジュールが次のように説明された。

・2007 年 1 月中　Draft を CMVP 内部(NIST＋CSE)でレビュー。
・2007 年 1 月　　レビュー結果を反映した版を各試験機関でレビュー。
・2007 年 1 月末　1st Draft を開示。90 日間のコメント募集期間を設ける。
・2007 年 4 月末　1st Draft に対するコメント募集の〆切。
・2007 年 春　　CMVP Symposium 2007 を開催
・2007 年 夏　　2nd Draft を開示。短期のパブリックコメント募集。
・2007 年 秋　　米国商務省による承認。

しかしながら、2007 年 3 月現在、試験機関に対する Draft も配布されておらず、次のようにシフトされることが予想されている。

・2007 年 3 月中　レビュー結果を反映した版を各試験機関でレビュー。
・2007 年 3 月末　1st Draft を開示。90 日間のコメント募集期間を設ける。

---

[52] EMI: Electro Magnetic Interference電磁妨害

[53] FSM: 有限状態モデル（Finite State Model）。暗号モジュールの動作を、有限状態モデルとして記述する。

[54] 非破壊攻撃：暗号モジュールに対して、物理的な侵入（カバーへ穴を開ける等の物理的手段を伴う侵入）を伴わない解析技術。代表的なものとしては、電力解析攻撃、故障誘導攻撃などがある。

・2007 年 6 月末　1st Draft に対するコメント募集の〆切。
・2007 年 夏～秋　CMVP Symposium 2007 を開催
・2007 年 秋　　2nd Draft を開示。短期のパブリックコメント募集。
・2007 年 冬　　米国商務省による承認。

### ４．３．３．ISO/IEC 19790 に関する動向

（１）ISO/IEC JTC 1/SC 27/WG 3

ISO/IEC JTC 1 は、ISO と IEC が共同で運営する IT 技術標準化のための技術委員会で、その下の SC 27 委員会が情報セキュリティを担当している。その下の WG 3 で評価技術が情報セキュリティに関する評価基準などが扱われている。

（２）ISO/IEC 19790 (Security requirements for cryptographic modules)

ISO/IEC JTC 1/SC 27/WG 3 は、米国とカナダの提案に従い、2002 年 10 月から暗号モジュールセキュリティ要件の国際規格化を審議し、規格予定番号 19790 が割り当てられた。2005 年 10 月のマレーシア会合において FCD 案に対する編集作業が行われ、国際事務局による編集作業の後、2005 年 12 月には FDIS 投票が実施され、賛成多数で 2006 年 3 月 1 月に ISO/IEC 19790 として正式に発行された。

ISO/IEC 19790 は、FIPS 140-2 をベースとした基準であり、当初 CC(Common Criteria)への連接性を意識して記述様式を変更することが検討された。しかし、審議の進行に伴って CC に対する配慮は薄れ、その点に関する影響はほとんどなくなった。なお、暗号技術に関し、FIPS 140-2 では秘密鍵も公開鍵も CSP として区別しなかったのを秘密鍵は CSP、公開鍵は PSP と２種類に分解するなど、技術的な記述の精緻化が図られた。

（３）ISO/IEC 24759 (Test requirements for cryptographic modules)

2005 年 4 月のウィーン会合において、暗号モジュールセキュリティ要件の国際規格 ISO/IEC 19790 に付随して実際の試験に必要となる、暗号モジュール試験要件の規格化のプロジェクトが承認され、予定規格番号 24759 が割り当てられた。2006 年 5 月のスペイン会合で WD、2006 年 11 月の南アフリカ会合で 1st CD に関する審議が行われ、2007 年 5 月のロシア会合において FCD に進むか否かが審議される。

ISO/IEC 24759 の章立てや 4 つのセキュリティレベルは FIPS 140-2 の DTR と基本的に同じである。ただし、FIPS 140-2 から ISO/IEC 19790 が作成された際の修正を整合性を保ちつつ反映させる必要がある。

### ４．３．４．2006 年度の活動

（１）海外動向への対応

2006 年度、暗号モジュール委員会では、暗号モジュールセキュリティ要件に関する海外動向に対応すべく、次の（イ），（ロ）の作業を予定していた。

（イ）暗号モジュール試験要件の国際規格 ISO/IEC 24759 へのコメント提案

ISO/IEC JTC 1/SC 27 において、セキュリティ要件の国際規格 ISO/IEC 19790 に対応した試験要件の規格 ISO/IEC 24759 が作成中であり、1st CD のドキュメントに対する多数のコメント案を作成し、SC 27 の国内委員会に提出した。コメント案には、セキュリティ要件と具体的試験の不整合を正すものなど技術的に重要なものも含まれており、2007 年 5 月に開催される SC 27 ロシア会合での審議対象となる予定である。

（ロ）FIPS 140-3 の 1st Draft に対するコメント作成

当初、2006 年 11 月末にコメント募集用に公開されるはずだった FIPS 140-3 の 1st Draft に対する検討とコメント案作成を予定していた。しかし、2007 年 3 月 15 日現在、まだ発表されておらず、2007 年度に持ち越しとなった。

（２）セキュリティ要件等に関する文書の作成

暗号モジュール委員会では、2005 年度末に ISO/IEC 19790 を和訳した「暗号モジュールセキュリティ要件」、FIPS 140-2 の DTR の和訳に FIPS 140-2 と ISO/IEC 19790 の差分を反映した「暗号モジュール試験要件(2006-03-31 版)」、及び FIPS 140-2 の Implementation Guidance(2005 年 12 月版)を和訳した「暗号モジュール運用ガイダンス(2006-03-31 版)」の 3 つを作成した。なお、ISO/IEC 規格の著作権を考慮し、セキュリティ要件と試験要件は公開せず、運用ガイダンスのみ公開した。

FIPS 140-2 からISO/IEC 19790 を作成する際、曖昧だった概念が明確化されるなど、技術的な整備が行われた。具体例としては、FIPS 140-2 では公開鍵暗号の秘密鍵と公開鍵をCSP[55]として同じ扱いにしていたが、ISO/IEC 19790 では秘密鍵はCSP、公開鍵はPSP[56]と区別するという精緻化を行った。暗号モジュール試験要件の作成には、このような改良に伴う修正に多くの労力を要した。

なお、上記のセキュリティ要件は「JIS X 19790　セキュリティ技術-暗号モジュールのセキュリティ要求事項」、試験要件は「JIS X 5091 セキュリティ技術-暗号モジュールのセキュリティ試験要件」の素案として利用された。JIS X 19790 は国際規格 ISO/IEC 19790 の翻訳であり、オリジナルが存在したが、JIS X 5091 は対応する国際規格 ISO/IEC 24759 が作成中であったため、上記暗号モジュール試験要件が大きく貢献した。

[55] Crytical Security Parameter. 開示によって安全性に影響を受ける秘密データ。
[56] Public Security Parameter. 開示しても良いが、改ざんされると安全性に影響を受けるデータ。

## ４．３．５．電力解析実験ワーキンググループの設置

（１）設置の経緯と目的

暗号モジュール、特に IC カードのようなワンチップモジュールにとって、サイドチャネル攻撃、その中でも、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 攻撃、SPA 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、今後の暗号モジュールでは、対策を施すことが必須となると考えられる。しかし、FIPS 140-2 や ISO/IEC 19790 などのセキュリティ要件では、サイドチャネル攻撃に対する明確かつ具体的な規定が存在しなかった。

暗号モジュール委員会ではこのような現状を踏まえ、サイドチャネル攻撃に対するセキュリティ要件、試験要件に関する規定の作成を目的として、日本規格協会 情報技術標準化研究センター（INSTAC）で開発した INSTAC-8 仕様及び INSTAC-32 仕様に準拠した電力解析実験用評価ボードを配布し、実験結果の収集を行っている。この活動により、有益な実験結果が出始めている。

2006 年度は、実際に利用されている暗号 LSI に近い形態の評価用標準プラットフォームを作るべく、関連機関と協力して ASIC チップの開発を進めた。また、配布した電力解析実験評価用標準プラットフォーム等を利用した実験の方針を決め、実験データを収集・分析し、電力解析攻撃等のサイドチャネル攻撃に対するセキュリティ要件案、試験要件案を作成する目的で、暗号モジュール委員会の下に電力解析実験ワーキンググループを設置した。活動の具体的な項目は次の通り。

・評価用標準プラットフォームを用いた実験手法の情報共有
・評価用標準プラットフォームを用いた実験結果の検討
・経済産業省にて計画中の暗号処理 LSI による、実験の実施及びその実験結果の検討
・暗号処理 LSI と評価用標準プラットフォームでの実験結果比較検討
・検討結果を用いた、セキュリティ要件案の作成
・サイドチャネル攻撃対策技術の試験要件・判定基準の作成

（２）INSTAC-8/-32 仕様準拠ボードを利用した研究成果

これまでに発表された INSTAC-8/-32 仕様準拠ボードを利用した電力解析実験関係の論文を収集した結果、表 12 に示すように発表論文は 30 件に達し、電力解析実験に関する研究の活性化に大きく貢献したことが確認された。

# 表 12　INSTAC 仕様準拠ボード関連電力解析関係発表論文リスト

| | タ　イ　ト　ル | 学会名・会議名 | 発表年月日 | 著　　者 |
|---|---|---|---|---|
| 1 | 8bitCPUを対象とした電力解析用評価環境の開発と実証実験 | ISEC | 2004/07/21 | 藤崎浩一、友枝裕樹、三宅秀享、駒野雄一、新保　淳、<br>川村信一（㈱東芝） |
| 2 | A5/1 に対するサイドチャネル攻撃（2D2-2） | SCIS2005 | 2005/01/26 | 一色寿幸（日本電気㈱）、辻原悦子（㈱ワイ・デー・ケー）、<br>峯松一彦、角尾幸保（日本電気㈱） |
| 3 | SBOXの特性を利用したDPA評価手法(4E1-1) | SCIS2005 | 2005/01/28 | 三宅秀享、野崎華恵、清水秀夫、新保　淳（㈱東芝） |
| 4 | INSTAC-8を用いたサイドチャネル攻撃に関する一考察（3T-1） | 情報処理学会<br>第67回全国大会 | 2005/03/03 | 和田崇臣、甲斐切皇男、岩井啓輔、黒川恭一（防衛大学校） |
| 5 | CPUボード上のブロック暗号に対するサイドチャネル攻撃 | ISEC | 2005/03/17 | 高橋芳夫（㈱NTTデータ）、<br>福永利徳、大塚浩昭、神田雅透（㈱NTT） |
| 6 | 32bitCPUを対象とした電力解析用評価環境の開発と実証実験 | ISEC | 2005/07/21 | 藤崎浩一、清水秀夫、新保　淳（㈱東芝） |
| 7 | Experimental Results on INSTAC-8 Compliant Board | NIST & IPA<br>Physical Security<br>Testing Workshop | 2005/09/26 | 角尾幸保（JSA、日本電気㈱）、久門　亨（日本電気㈱）、<br>辻原悦子（(株)ワイ・デー・ケー）、松本　勉（JSA、横浜国立大学）、<br>川村信一、藤崎浩一（JSA、㈱東芝） |
| 8 | ストリーム暗号に対するDPA（1C3-2） | SCIS2006 | 2006/01/17 | 久門　亨、角尾幸保（日本電気㈱）、<br>後藤　敏、池永　剛（早稲田大学） |
| 9 | 共通鍵暗号におけるテーブルを用いた電力差分解析対策法について(1C3-1) | SCIS2006 | 2006/01/17 | 宮崎隆行、辻村達徳、松本　勉（横浜国立大学） |
| 10 | 汎用CPUにおけるサイドチャネル情報からの命令コードの解析(1C3-4) | SCIS2006 | 2006/01/17 | 山口晃由、山田敬喜（三菱電機㈱） |
| 11 | Sbox特性を利用したDPA評価手法の有効性検証（2C1-2） | SCIS2006 | 2006/01/18 | 三宅秀享、野崎華恵、清水秀夫、新保　淳（㈱東芝） |
| 12 | 位相限定相関法に基づく高精度波形解析とそのサイドチャネル攻撃への応用 | ISEC | 2006/03/16 | 今井裕一、本間尚文、長嶋　聖、青木孝文（東北大）、<br>佐藤　証（日本アイ・ビー・エム㈱） |
| 13 | INSTAC-8 準拠評価ボードを使った実装攻撃実験の結果報告 | ISEC | 2006/03/16 | 角尾幸保（JSA、日本電気㈱）、久門　亨（日本電気㈱）、<br>辻原悦子（(株)ワイ・デー・ケー）、松本　勉（JSA、横浜国立大学）、<br>川村信一、藤崎浩一（JSA、㈱東芝） |
| 14 | ブロック暗号のマスク対策付FPGA実装に対するビット遷移に着目したDPAの適用 | ISEC | 2006/05/19 | 高橋芳夫（㈱NTTデータ、横浜国立大学）、松本　勉（横浜国立大学）、<br>佐藤　証（日本アイ・ビー・エム㈱） |
| 15 | 漏洩電磁波による共通鍵暗号処理ハードウェアの動作解析(1F-11) | 電気関係学会<br>東北支部連合大会 | 2006/08/31 | 菅原　健、本間尚文、青木孝文（東北大学）、<br>佐藤　証（日本アイ・ビー・エム㈱） |
| 16 | DPA対策実験による電力解析評価用プラットフォームの検証（M-052） | 第5回情報科学技術<br>フォーラム　FIT2006 | 2006/09/07 | 辻　洋平、岩井啓輔、黒川恭一（防衛大学校） |
| 17 | High-resolution side-channel attack using phase-based waveform matching | CHES 2006 | 2006/10/12 | 本間尚文 、長嶋 聖、今井裕一、青木孝文（東北大学）、<br>佐藤　証（日本アイ・ビー・エム㈱） |
| 18 | 位相限定相関法による波形マッチングを用いた高精度差分電力解析法(1C-3) | CSS2006 | 2006/10/26 | 今井裕一、本間尚文、長嶋　聖、青木孝文（東北大学）、<br>佐藤　証（日本アイ・ビー・エム株式会社） |
| 19 | RSA暗号のFPGA実装に対するSPA耐性評価(4B-4) | CSS2006 | 2006/10/26 | 宮本篤志、本間尚文、青木孝文（東北大学）、<br>佐藤　証（日本アイ・ビー・エム㈱） |
| 20 | 位相限定相関法に基づく高精度波形マッチング -- 暗号ハードウェアの動作解析への応用 -- | 第21回信号処理シンポジウム | 2006/11/16 | 長嶋　聖、本間尚文、今井裕一、青木孝文（東北大学）、<br>佐藤　証（日本アイ・ビー・エム㈱） |
| 21 | テーブルネットワークを用いたFPGA実装AESとその電力差分解析耐性 | ISEC | 2006/11/17 | 辻村達徳（横浜国立大学）、高橋芳夫（横浜国立大学、㈱NTTデータ）、<br>松本　勉（横浜国立大学） |
| 22 | 位相限定相関法を用いた高精度差分電力解析とそのノイズ耐性評価（2E4-5） | SCIS2007 | 2007/01/24 | 本間尚文 、長嶋　聖、今井裕一、青木孝文（東北大学）、<br>佐藤　証（日本アイ・ビー・エム㈱） |
| 23 | INSTAC-32準拠ボードを使用した電力解析自動化の適用例（2E4-6） | SCIS2007 | 2007/01/24 | 庄司陽彦、野澤　晃、木村隆幸（㈱ワイ・デー・ケー）、<br>久門　亨（日本電気㈱）、深澤　宏（NECマイクロシステム㈱）、<br>角尾幸保（日本電気㈱） |
| 24 | RSA暗号を実装したINSTAC-32に対するサイドチャネル攻撃実験（3E3-3） | SCIS2007 | 2007/01/25 | 深澤　宏、東　邦彦（NECマイクロシステム㈱）、<br>後藤　敏、池永　剛（早稲田大学）、角尾幸保、久門　亨（日本電気㈱）、<br>庄司陽彦（(株)ワイ・デー・ケー） |
| 25 | eSTREAM 提案暗号へのDPA解析報告(3E4-5) | SCIS2007 | 2007/01/25 | 久門 亨、角尾幸保（日本電気㈱）、深澤　宏（NECマイクロシステム㈱）、<br>庄司陽彦（㈱ワイ・デー・ケー）、後藤　敏、池永　剛（早稲田大学） |
| 26 | 固定値入力を用いたRSA暗号ハードウェアに対するSPA（3E3-2） | SCIS2007 | 2007/01/25 | 本間尚文 、宮本篤志、青木孝文（東北大学）、<br>佐藤　証（日本アイ・ビー・エム㈱） |
| 27 | 信号遅延を考慮したDPA耐性評価　--- MRSLとDRSLの場合 ---（3E3-1） | SCIS2007 | 2007/01/25 | 佐伯　稔（三菱電機㈱） |
| 28 | テーブルネットワーク型CPUボード実装AESの電力差分解析耐性(3E4-4) | SCIS2007 | 2007/01/25 | 鳥越　慎、辻村達徳（横浜国立大学）、<br>高橋芳夫（横浜国立大学、㈱NTTデータ）、松本　勉（横浜国立大学） |
| 29 | アンロールパイプライン型FPGA実装AESの電力差分解析耐性(3E4-3) | SCIS2007 | 2007/01/25 | 辻村達徳（横浜国立大学）、高橋芳夫（横浜国立大学、㈱NTTデータ）、<br>松本　勉（横浜国立大学） |
| 30 | INSTAC-32準拠プラットフォームを用いたRSAに対する故障利用攻撃実験 | ISEC | 2007/03/15 | 藤崎浩一、清水秀夫（㈱東芝） |

ISEC：情報セキュリティ研究会（電子情報通信学会）

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）

CHES：Workshop on Cryptographic Hardware and Embedded Systems
（The International Association for Cryptologic Research ）

CSS：コンピュータセキュリティシンポジウム（情報処理学会）

## ５．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、2007 年度以降以下の活動を実施していくこととする。

### ５．１．暗号技術検討会の活動内容

暗号技術検討会（以下、「検討会」）は、電子政府推奨暗号リストに掲載された暗号技術の監視、関連する調査研究、及び、暗号技術の危殆化や暗号プロトコル等その他暗号技術の評価・利用等に関する事項について、利用者側からみたわかりやすさにも配慮しつつ総合的な観点から検討を行う。また、電子政府等のセキュリティの確保のため、政府のセキュリティ関係機関等との連携、調整を図る。

また、電子政府推奨暗号について、その危殆化が発生した際の問題等に係る政府内での検討に際して、技術的・専門的な助言等を行う。

（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。

（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

（イ）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。

（ロ）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

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

（４）暗号モジュール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。

## ５．２．委員会及びワーキンググループの構成及び活動内容

CRYPTREC は、2007 年度以降も引き続き、暗号技術検討会の下に設置される「暗号技術監視委員会」及び「暗号モジュール委員会」並びに暗号技術監視委員会の下に設置される「暗号技術調査 WG」及び暗号モジュール委員会の下に設置される「電力解析実験 WG」により構成されるものとする。

### ５．２．１．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る。監視委員会は、数名の有識者等により構成され、安全性及び信頼性確保の観点から、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・検討を適宜行うとともに電子政府推奨暗号リストの改訂に関する調査・検討を行う。

（１）暗号技術調査ワーキンググループ

（イ）暗号技術調査WG（以下、「調査WG」）は、電子政府推奨暗号リストの変更案等の作成、及び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として、監視委員会の下に設置される。

（ロ）調査WGは、監視委員会からの要請により事案の性質に応じて開催されることとし、監視委員会に対して電子政府推奨暗号リストの変更案の作成等に関する専門的助言を行う。

（ハ）その他、調査WGは、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具体的な調査・検討（電子政府における暗号利用状況調査等）を行い、監視委員会に対して専門的助言を行う。

2007 年度、監視委員会では、2006 年度に設置した調査 WG（公開鍵暗号）の活動を継続し、電子政府推奨暗号リストに記載されている公開鍵暗号方式に関するパラメータ等について調査・検討を行うことを計画している。

### ５．２．２．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る。暗号モジュール委員会は、電子政府推奨暗号の安全性及び信頼性を確保するため、暗号実装関連技術等を対象とする調査・検討を行う。具体的な活動として、暗号モジュール委員会及びその下に設置される電力解析実験ワーキンググループで以下の事項に係る調査・検討等を行う。

（１）暗号モジュール委員会

（イ）国際規格 ISO/IEC 19790/24759 及び米国 NIST FIPS 140 シリーズの作成・更新に対する意見・コメント提出。

（ロ）国際規格及び米国規格を基にした日本における暗号モジュールのセキュリティ要件の素案（日本語）の作成を行う。

（２）電力解析実験ワーキンググループ

コメント提案の根拠となる電力解析を中心とするサイドチャネル攻撃に関する暗号実装関連技術等の調査・検討を行う。

## ５．３．電子政府推奨暗号の監視

### ５．３．１．電子政府推奨暗号の監視の基本的考え方

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。

### ５．３．２．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

（イ）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。

（ロ）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

（イ）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。

（ロ）（イ）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。

（ハ）監視委員会は応募暗号[57]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）電子政府推奨暗号の追加

（イ）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。

（ロ）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

---

[57] 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

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。

（ハ）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。

（ニ）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。

### ５．３．３．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。

（イ）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。
（ロ）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。
（ハ）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。
（ニ）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

（イ）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。

（ロ）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。

（ハ）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。

（ニ）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。

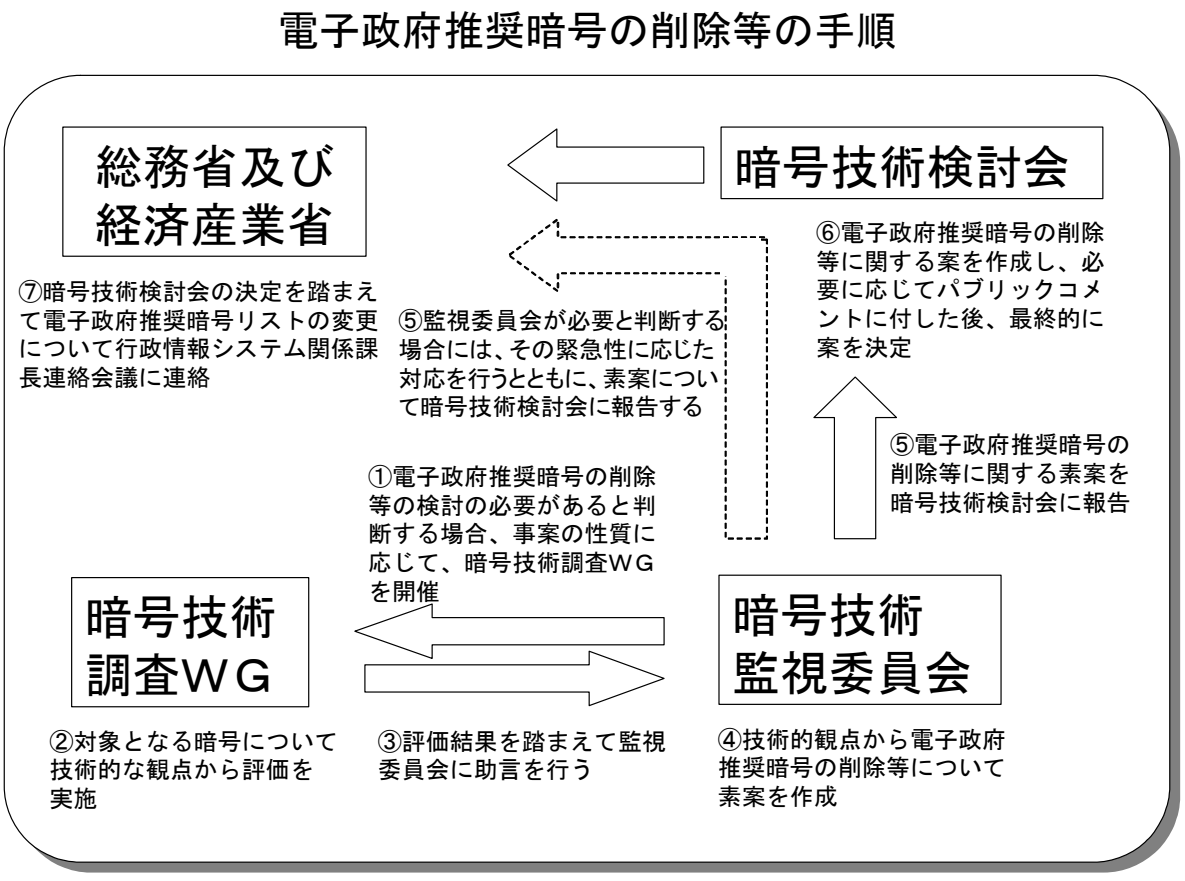



図4　電子政府推奨暗号削除等の手順

## ５．４．電子政府推奨暗号リストの改訂に関する検討

電子政府推奨暗号リストには、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から選定された暗号が掲載されている。しかし、暗号に対する解析や攻撃の技術や手法はますます高度化しており、電子政府推奨暗号は常に危殆化の危険にさらされている。一方、新たな暗号の開発も進んでおり、今後、安全性や実装性に優れた新しい暗号の出現が期待されるところである。

2007 年度は電子政府推奨暗号リスト策定から５年目を迎える一方、改訂を実施する際に、仮に公募を実施する場合は、公募のアナウンス（公募開始時期、公募期間、評価期間、新リスト発表時期等の公表）から新リストの策定まで、5 年程度の期間をかけることが望ましいと考えられることから、2007 年度において、電子政府推奨暗号リストの改訂作業の具体的な開始時期や実施方法等について検討する。その際、現行リストについても、リスト策定以降の技術の進展等を踏まえた部分修正の観点に配慮する。

なお、検討にあたっては、内閣官房情報セキュリティセンター（ＮＩＳＣ）、行政情報システム関係課長連絡会議等との連携を図ることとする。

# 参考資料「各府省の情報システム調達における暗号の利用方針」

# 各府省の情報システム調達における暗号の利用方針

平成15年2月28日
行政情報システム関係課長連絡会議了承

電子政府における情報セキュリティ確保のために、各府省の情報システムにおいて暗号を利用する場合には、一定水準以上の安全性及び信頼性を有する暗号の利用が不可欠であり、また、その安全性・信頼性は客観的な評価を得たものであることが必要である。

かかる観点から、「電子政府の情報セキュリティ確保のためのアクションプラン」（平成13年10月10日、情報セキュリティ対策推進会議）に基づき、総務省及び経済産業省において、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」：別添参照）を策定したところである。

これを踏まえ、各府省は、情報システムの構築に当たり暗号を利用する場合には、調達仕様書において上記暗号リストに掲載された暗号を利用することを入札要件とする等の方法により、必要とされる安全性・信頼性などに応じ、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ものとする。

なお、総務省及び経済産業省は、「電子政府推奨暗号リスト」に掲載された暗号の安全性及び信頼性について、今後の情報通信技術の進展を踏まえ必要に応じ評価を行うとともに、「電子政府推奨暗号リスト」の内容の変更を行う場合には本会議に報告することとする。

別　添

# 電子政府推奨暗号リスト

平成１５年２月２０日
総　　務　　省
経　済　産　業　省

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

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

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

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

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

1） FIPS46-3 として規定されていること

2） デファクトスタンダードとしての位置を保っていること

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

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

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

別添

# 電子政府推奨暗号リストに関する修正情報

| 修正日付 | 修正箇所 | 修正前 | 修正後 | 修正理由 |
|---|---|---|---|---|
| 平成１７年１０月１２日 | 注釈の注 4）の 1） | FIPS46-3 として規定されていること | SP800-67 として規定されていること | 仕様変更を伴わない、仕様書の指定先の変更 |