暗号技術検討会

２００５年度報告書

暗号技術検討会

２００６年３月

目次

【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」（平成 15 年 2 月）

１．はじめに

最近の国民生活・社会経済活動における IT 化の浸透はめざましいものがある。ネットショッピング、ネットバンキング、e-トレード既に我々の生活に定着した感がある。非接触型 IC カードが内蔵され、電子マネー、公共交通機関のプリペイドカード等の機能を持つ携帯電話も一般的になりつつある。

他方、IT 化による利便性の増大とともに、新種ウィルスやサイバー攻撃、フィッシング詐欺など、これまでになかった新次元のリスクに直面しており、IT に対する脅威が増加するとともに、その姿も多様化している。また最近では、ファイル交換ソフト「ウィニー」を通じて、企業官公庁の機密情報が流出する事件が続出している。このような環境の中、いかに IT の安全性・信頼性を確保するかという問題は、我々の社会が直面している喫緊の課題と言える。

政府としても、安全性及び信頼性の高い電子政府を実現するために、情報セキュリティの確保が不可欠であり、情報セキュリティ技術の基盤をなす暗号技術が重要であるとの認識を深めている。この認識は、2001 年 3 月に IT 戦略本部において決定された「e-Japan 重点計画」においても示され、さらに、同年 10 月に情報セキュリティ対策推進会議において「総務省及び経済産業省は、両省で実施している研究会の成果等も踏まえ、2002 年度中に「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を作成し、これを踏まえ、各省庁における暗号の利用方針について合意を目指す」ことが決定された。

これに先立ち、2000 年度、経済産業省（旧通商産業省）からの委託を受けて、独立行政法人情報処理推進機構（IPA、旧情報処理振興事業協会）は電子政府で利用可能な暗号技術を安全性および実装性など技術的な面から評価することを目的とした暗号技術評価委員会を設置するとともに同委員会の事務局を務めた。2001 年度からは独立行政法人情報通信研究機構（NICT、旧通信・放送機構）が同委員会の共同事務局として参加した。また、2001 年度には、暗号技術評価委員会に加えて、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が、暗号技術の利用に関し政策的な観点から検討を行うことを目的として、暗号技術検討会（以下、「本検討会」）を設置した。

本検討会は、電子政府で利用される暗号技術、国際標準化に関する暗号技術及び電子署名法等に基づいて利用される暗号技術の評価・調査研究、並びにその他暗号技術の利用等に関連する技術課題を検討対象としており、2002 年度には、それまでの検討及び評価を踏まえ、電子政府推奨暗号リスト案を作成した。これを受けて、総務省及び経済産業省は 2003 年 2 月に「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として公表した。2005 年度は、昨年度に引き続き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、暗号モジュール評価基準及び試験基準の作成のための調査・検討、

電子政府推奨暗号リストに関する調査・検討を行った。これらの結果をまとめた本報告書は、総務省及び経済産業省に対して報告するとともに、電子政府を構築する各府省関係者、及び一般の暗号ユーザの方々にも広く読んで頂くことを想定している。

なお、2005 年度の CRYPTREC 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、情報処理推進機構（IPA）及び情報通信研究機構（NICT）によってまとめられている「CRYPTREC Report 2005」を御参照頂きたい。

2005 年 5 月に IT 戦略本部の下に設置された「情報セキュリティ政策会議」により、「政府機関の情報セキュリティ対策のための統一基準」が同年 12 月に策定された。この統一基準においては、遵守事項として、電子政府推奨暗号リストの中からのアルゴリズムの選択について記述されており、電子政府推奨暗号リストの重要性がさらに高まってきている。また、2006 年 2 月に策定された「第１次情報セキュリティ基本計画」においても、電子政府で使われている推奨暗号の安全性を継続的に監視・調査することが求められている。

こうした中、本検討会は、今後も引き続き、国民が安心して利用できる電子政府を構築し、運用していくために、暗号技術を監視し、評価するとともに、暗号モジュールに関する評価基準及び試験基準を作成する等の活動を実施していく必要がある。このためには、CRYPTREC に関係する諸団体が一致団結して前進することが必要であり、今後とも関係者の方々の御協力を頂きながら、暗号技術検討会をはじめとする CRYPTREC 活動を積極的に推進していきたい。

末筆であるが、本検討会にご協力いただいた構成員の方々及びオブザーバとしてご参加頂いた方々をはじめ、関係者の皆様に心から謝意を表する次第である。

2006 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：今井秀樹東京大学教授）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：今井秀樹東京大学教授）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、防衛庁、法務省、外務省、財務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 として署名・認証技術調査 WG（主査：松本勉横浜国立大学教授)、ハッシュ関数・暗号利用モード調査 WG（主査：古原和邦東京大学助手）及び擬似乱数生成系調査 WG（主査：金子敏信東京理科大学教授）を設置し、検討を行った。

暗号技術監視委員会は NICT 及び IPA の委員会として開催し、総務省、経済産業省、警察庁、防衛庁、外務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、警察庁、防衛庁等がオブザーバとして参加した。

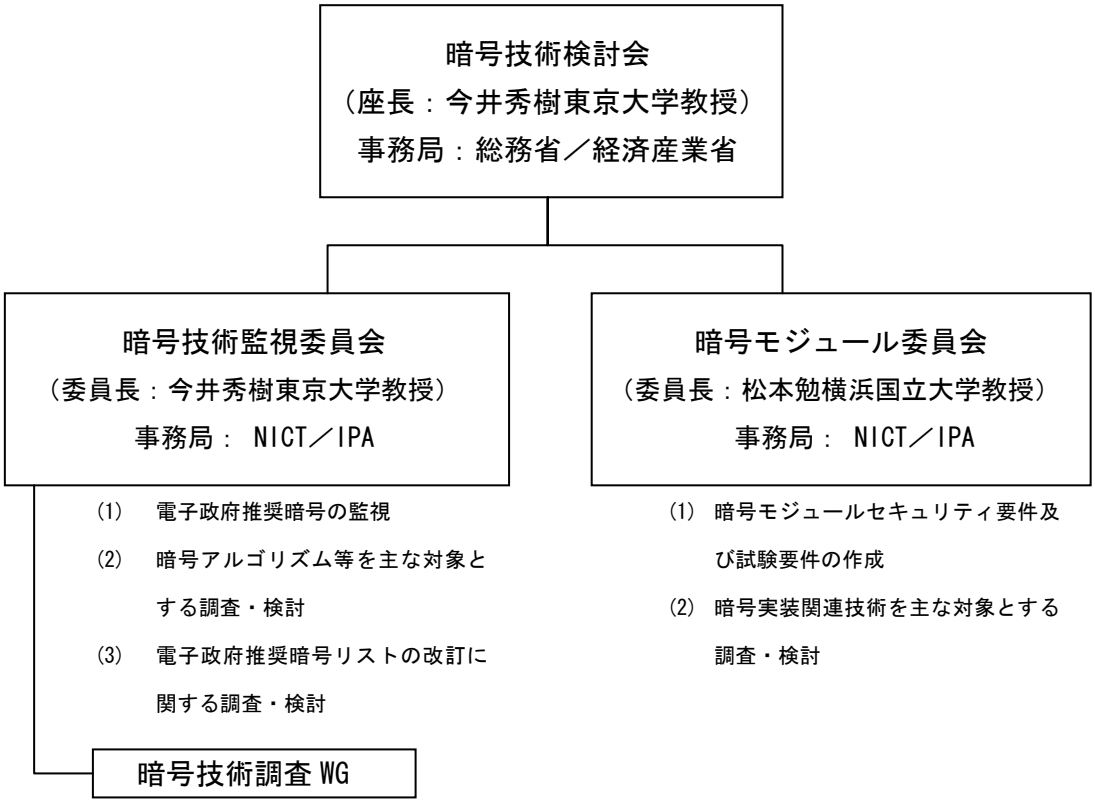


図 1　2005 年度の CRYPTREC の体制図

２．３．暗号技術検討会メンバー

（構成員）※肩書は 2006 年 3 月末現在。敬称略。

座 長	今井　秀樹	東京大学生産技術研究所教授
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 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務理事・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 情報セキュリティ技術部部長
	松本　勉	横浜国立大学大学院環境情報研究院教授
	松本　泰	次世代電子商取引推進協議会 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）※肩書は原則として参加当時のもの。敬称略。

小林　正彦	内閣官房情報セキュリティセンター内閣参事官
青山　研一	警察庁情報通信局情報技術解析課長
佐竹　基	防衛庁長官官房情報通信課長
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
牧　慎太郎	総務省自治行政局自治政策課情報政策企画官
土手　敏之	法務省民事局商事課専門官
杵渕　正己	外務省大臣官房情報通信課長
飯野　正弘	財務省大臣官房文書課情報管理室長
瀬戸　和吉	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
松島　裕一	独立行政法人情報通信研究機構情報通信部門長
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 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

2005 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】2005 年 10 月 12 日（水）
（主な議題）・暗号技術検討会の運営方針
・暗号技術検討会 2005 年度活動計画
・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

【第 2 回】2006 年 3 月 30 日（木）
（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 2005 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 17 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）ハッシュ関数の安全性評価について

平成 16 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。

平成 17 年度はハッシュ関数の安全性評価に表 2 に示す進展が見られた。その安全性評価成果を踏まえて、第 2 回暗号技術監視委員会（平成 18 年 3 月 8 日）において、ハッシュ関数の安全性に関する情報発信の内容及び方法についても、表 12 に示す電子政府推奨暗号リストの注釈変更（案）及び表 1 に示すコメント（案）の両案について検討されたが、最終案については、関連情報が整った段階で決定することとなった。

表 1　SHA-1 の安全性に関するコメント（案）

SHA-1 の安全性に関する見解（案）

平成 18 年 xx 月 xx 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等により 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、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/

以下に、ハッシュ関数の安全性評価の検討内容および見解を示す。

(a) SHA-1 の安全性評価について

SHA-1 に対する攻撃については、Wangの 2^{69}回のSHA-1 実行回数の計算量による攻撃アルゴリズムの概略がCRYPTO 2005 に先駆けてEurocrypt 2005 のランプセッションとECRYPT on Hash Functionにおいて発表された。これ以外にもBiham, JouxなどもSHA-1 の攻撃結果を発表している。CRYPTO 2005 では、Wangの攻撃アルゴリズムが正式に発表されたが、同時にランプセッションで計算量が 2^{63}まで削減できるという発表があった。

平成 17 年 10 月 31 日-11 月 1 日に開催された NIST（National Institute of Standards and Technology：(米国)国立標準技術研究所）の第 1 回ハッシュワークショップでは SHA-1、SHA-256 に関する技術面での現状把握があった。そこで、SHA-1 については平成 22 年に FIPS（Federal Information Processing Standards：(米国)連邦情報処理規格）から外すことが公表され、当面の間は SHA-256 は安全であるという認識が確認された。次世代ハッシュ関数(SHA-256 の後継)については、その選定方法から議論がされているが、公募/選定の実施を含めて結論に至っていない。NIST は第 2 回ハッシュワークショップを平成 18 年 8 月 24、25 日に予定している。

このことから、平成 17 年度は、ハッシュ関数・暗号利用モード調査ワーキンググループにおいて、電子政府推奨ハッシュ関数の安全性について分析・評価を実施した。表 2 に評価結果を示す。

表 2　平成 17 年度のハッシュ関数評価結果

ハッシュ関数	安全性評価
SHA-1	衝突発見困難性に対して、2^{69}回以下のSHA-1 の実行回数で攻撃できる手法が発見された。ただし、公開された攻撃アルゴリズムには一部不明な点があり、第三者によって実装して検証されたわけではない。しかし、この攻撃アルゴリズムの不明な点は近い将来に明らかになり第三者による実装が可能になると予想されるので、本攻撃アルゴリズムは極めて大きな脅威になると考えられる。 第二原像計算困難性に対しては、2^{60}バイトのメッセージに対して 2^{106}のSHA-1 の実行回数で攻撃される手法が公開されたが、平成 18 年 2 月の時点で脅威とは言えない。
RIPEMD-160	RIPEMD-160 は異なる二つのブロック暗号 L、R で構成され、そのうちブロック暗号 L については SHA-1 と同程度の差分パスの存在が予想できることが報告されている。これはデータ撹拌においてメッセージ置換とステップ依存のビットシフトの採用など SHA-1 と類似した関数を採用しているためであり、具体的なパスの発見など安全性に関する報告はないが、今後の研究の進展を考え研究動向について非常に注意する必要がある。
SHA-256/-384/-	実用的な安全性を脅かす攻撃方法が報告されていないた

512	め、これらのハッシュ関数は暗号の応用分野で使うのに十分安全であると考えられる。
Whirlpool	Whirlpool 全体では差分の拡散が十分であり、近年の攻撃手法を適用しても衝突発見は困難である。

(b) 情報発信について

署名・認証技術調査ワーキンググループでは、表 2 に示す評価結果を受けて、ハッシュ関数の安全性に関する技術的な情報を正式コメントとして公表する方法を検討し、表 12、表 13 に示す提案を行い、暗号技術監視委員会に報告した。

なお、NISTは平成 18 年 3 月 15 日にWebサイトにSHA-1 の利用について、表 3 に示す声明を発表した。(http://csrc.nist.gov/CryptoToolkit/tkhash.html)

表 3 NIST のハッシュ関数に関する声明文

March 15, 2006:
The SHA-2 family of hash functions (i.e., SHA-224, SHA-256, SHA-384 and SHA-512) may be used by Federal agencies for all applications using secure hash algorithms.
Federal agencies should stop using SHA-1 for digital signatures, digital time stamping and other applications that require collision resistance as soon as practical, and must use the SHA-2 family of hash functions for these applications after 2010.
After 2010, Federal agencies may use SHA-1 only for the following applications:
hash-based message authentication codes (HMACs); Okey derivation functions (KDFs);and random number generators (RNGs).
Regardless of use, NIST encourages application and protocol designers to use the SHA-2 family of hash functions for all new applications and protocols.

March 15, 2006:
安全なハッシュアルゴリズムを使う全てのアプリケーションに対して SHA-2 ファミリー (SHA-224, SHA-256, SHA-384, 及び SHA-512) のハッシュ関数を連邦政府機関が利用することは許される。連邦政府機関は、電子署名、タイムスタンプおよびハッシュ関数の衝突発見困難性を安全性の基礎とするその他の用途においては、実施上できるだけ早期に SHA-1 を使うことを止めるべきであり、2010 年以降はそれらのアプリケーションに対して SHA-2 ファミリーのハッシュ関数を使わなければならない。
2010 年以降は、連邦政府機関は次のアプリケーションに対してだけ SHA-1 を使うことが許される。
・ハッシュベースメッセージ認証コード (HMACs)
・鍵導出関数 (KDFs)
・擬似乱数生成系 (RNGs)

利用目的に係わらず、NIST はアプリケーションやプロトコルの設計者に全ての新しいアプリケーションとプロトコルに対して SHA-2 ファミリーのハッシュ関数を使うよう勧める。

(c) MD5 に対する見解について

MD5 に対する攻撃については実時間で衝突の発見が可能な状況にあり、それを使った X.509 電子証明書における不正やポストスクリプトなどのページ記述言語における問題など、実システムやアプリケーションのリスクが明らかになってきている。これらの情報収集分析の結果、MD5 に関する対応を暗号技術監視委員会で議論し平成 17 年 8 月 5 日に表 4 に示す「MD5 等に対する見解」として了承された。これは、平成 17 年 8 月 29 日に暗号技術検討会事務局より各府省に通知された。

表 4　MD5 等に関する見解

MD5 等に関する見解

平成１７年８月５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。

ハッシュ関数の MD5 並びに共通鍵暗号の DES(鍵長 56 ビット)、RC4 及び RC2（鍵長 128 ビット未満）は、暗号技術評価報告書（2002 年度版）＊に記述されている評価基準を満たしていない。このため、電子政府推奨暗号リストに掲載されていないこれら暗号の使用は薦められない。

なお、MD5 については、最近の研究動向によれば、MD5 に対する攻撃アルゴリズムが発表され、現実的な時間内に衝突が発見できる状況になった。さらに、MD5 を発行者署名に利用した場合に、公開鍵情報だけ（例えば RSA 暗号におけるモジュラス）が異なる 2 つの X.509 電子証明書を作成する不正行為が報告されており、衝突発見が現実的な問題に発展することを示唆している。このような不正行為以外にも現実的な問題に発展する危険性が指摘されていることから、認証局の自己署名証明書のフィンガープリントにおける MD5 の使用は薦められない。

＊参照：暗号技術評価報告書（２００２年度）
http://www.ipa.go.jp/security/enc/CRYPTREC/fy15/cryptrec20

（２）電子署名に関する技術的意見について

現在の電子署名法に基づく特定認証業務に係る電子署名の基準に記されている公開鍵暗号技術ではハッシュ関数として SHA-1 のみが規定されているため、SHA-1 以外のハッシュ関数を利用した電子署名が電子署名法では認められていない。

http://www.soumu.go.jp/joho_tsusin/top/ninshou-law/1-6.pdf
http://www.moj.go.jp/MINJI/minji32-3.html
http://www.meti.go.jp/policy/netsecurity/digitsign_sisin.pdf

そこで、SHA-256、SHA-384、SHA-512、RIPEMD-160 を利用した署名技術の是非について検討し、SHA-256、SHA-384、SHA-512 の 3 つのハッシュ関数を新たに追加すべきとの合意を得た。その内容は表 5 に示す新たな改定案を記載した「電子署名法の指針の改訂に係わる意見の提出」として、暗号技術監視委員会承認（平成 17 年 7 月 15 日)、暗号技術検討会承認（平成 17 年 10 月 12 日）を経て政府に提言した。

表 5　電子認証業務認定指針第三条及び第十条の改訂案

（１）告示第三条（特定認証業務に係る電子署名の基準）

一　RSA 方式（オブジェクト識別子　1.2.840.113549.1.1.5　又は 1.2.840.113549.1.1.11　又は　1.2.840.113549.1.1.12　又は 1.2.840.113549.1.1.13）であって、モジュラスとなる合成数が 1024 ビット以上のもの
二　RSA-PSS 方式（オブジェクト識別子 1.2.840.113549.1.1.10）であって、ハッシュ関数として SHA 方式（オブジェクト識別子 1.3.14.3.2.26 又は 2.16.840.1.101.3.4.2.1　又は　2.16.840.1.101.3.4.2.2　又は 2.16.840.1.101.3.4.2.3）を使用し、モジュラスとなる合成数が 1024 ビット以上のもの
三　ECDSA 方式（オブジェクト識別子 1.2.840.10045.4.1）であって、楕円曲線の定義体及び位数が 160 ビット以上のもの
四　DSA 方式（オブジェクト識別子 1.2.840.10040.4.3）であって、モジュラスとなる素数が 1024 ビットのもの

（２）告示第十条第二号（認定認証業務と他の業務との誤認を防止するための措置）

二　発行者署名検証符号に係る電子証明書の値を SHA-1（オブジェクト識別子 1.3.14.3.2.26 ）又は SHA-256（オブジェクト識別子 2.16.840.1.101.3.4.2.1）又は SHA-384（オブジェクト識別子 2.16.840.1.101.3.4.2.2）又は SHA-512（オブジェクト識別子 2.16.840.1.101.3.4.2.3）で変換した値によって認定認証業務を特定すること。

（３）NIST FIPS46-3 の廃止に伴う T-DES の扱いについて

NIST は平成 17 年 5 月 19 日付けで T-DES を規定した FIPS46-3 を廃止した。これを受けて、それが記載されている電子政府推奨暗号リストの注釈の取扱いについて検討し、「3-key Triple DES に係わる電子政府推奨暗号リストの注釈の一部修正について」を暗号技術監視委員会承認（平成 17 年 9 月 1 日)、暗号技術検討会承認（平成 17 年 10 月 12 日）を経て、行政情報システム関係課長連絡会議の配下の共通システム専門部会（平成 17 年 11 月 17 日）で各府省に周知するとともに、CRYPTERC の Web サイトに表 6 に示す内容で公開した。

表 6　電子政府推奨暗号リストの注釈の一部修正

3-Key Triple DES に係わる電子政府推奨暗号リストの注釈の一部修正について

平成 17 年 11 月 30 日
暗号技術監視委員会

NIST は2005年5月19日付けで、連邦政府が取り扱う情報の秘匿には Data Encryption Standard (DES) では十分な安全性をもたなくなったとして、Data Encryption Standard (DES) の規定を含んでいる NIST FIPS 46-3 を廃止した[1]。FIPS 46-3 の廃止に伴い, NIST SP 800-67を新たに発行して[2]、Triple Data Encryption Algorithm (TDEA) の規定を FIPS 46-3 からこれに移した。また、NIST は、FIPS 46-3 が再確認された1999年10月25日以来 Single DES (= DES) から Triple DES (= TDEA) (及び AES)への移行を推奨してきている。

一方、電子政府推奨暗号リスト（平成15年2月20日）では、3-key Triple DES[3]に対して次のように定めている。

（注3）新たな電子政府用システムを構築する場合は、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) FIPS 46-3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

今回のNISTの対応は、電子政府推奨暗号リストの考え方とは基本的に矛盾していないことから、暗号技術監視委員会（平成17年6月20日）および暗号技術検討会（平成17年10月12日）の意見にもとづき、リストそのものの変更は行わず、注釈の注4)において、

（修正前）1) FIPS 46-3として規定されていること

（修正後）1) SP800-67として規定されていること

の修正のみとして、下表を電子政府推奨暗号リストの末尾に添付する。

電子政府推奨暗号リストに関する修正情報				
修正日付	修正箇所	修正前	修正後	修正理由
平成 17 年 10 月 12 日	注釈の注 4)の 1)	FIPS 46-3 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

[1] http://csrc.nist.gov/publications/fips/05-9945-DES-Withdrawl.pdf
[2] http://csrc.nist.gov/publications/nistpubs/800-67/SP800-67.pdf
[3] Triple Data Encryption Algorithm (TDEA) の規定には最初の 2 つの鍵を独立に取り、3 つ目の鍵を 1 つ目の鍵と等しく取るオプションも含まれているが、CRYPTREC においては 3 つの鍵すべてを独立に取るオプションのみを 3-key Triple DES と呼んでいる。

（４）擬似乱数検定に関するミニマムセットの作成について

擬似乱数検定のためのミニマムセットとして、NIST の SP800-22 の 16 種類の検定法の中から表 7 に示す 14 種類をミニマムセットとして採択し、暗号モジュール委員会事務局に送付した。

表 7　乱数検定のミニマムセット

項番	検定の名称
1	頻度検定
2	ブロック単位の頻度検定
3	連検定
4	ブロック単位の最長連検定
5	2 値行列ランク検定
6	重なりの無いテンプレート適合検定
7	重なりのあるテンプレート適合検定
8	Maurer の「ユニバーサル統計量」
9	線形複雑度検定
10	系列頻度検定
11	累積和検定
12	ランダム回遊検定
13	変形ランダム回遊検定
14	近似エントロピー検定

３．１．３．暗号技術監視委員会開催状況

平成 17 年度、暗号技術監視委員会は、表 8 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 9 の通り計 12 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 8　暗号技術監視委員会の開催

回	年月日	議題
第 1 回	平成 17 年 6 月 20 日	活動方針確認、暗号技術監視状況報告
第 2 回	平成 18 年 3 月 8 日	暗号技術監視状況報告、CRYPTREC report 2005 審議

表 9　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 17 年 4 月 25 日	第 1 回署名・認証技術調査 WG
第 2 回	平成 17 年 6 月 8 日	第 2 回署名・認証技術調査 WG
第 3 回	平成 17 年 7 月 6 日	第 3 回署名・認証技術調査 WG
第 4 回	平成 17 年 7 月 28 日	第 1 回ハッシュ関数・暗号利用モード調査 WG
第 5 回	平成 17 年 8 月 11 日	第 1 回擬似乱数生成系調査 WG
第 6 回	平成 17 年 9 月 13 日	第 2 回ハッシュ関数・暗号利用モード調査 WG
第 7 回	平成 17 年 9 月 22 日	第 2 回擬似乱数生成系調査 WG
第 8 回	平成 17 年 11 月 25 日	第 3 回ハッシュ関数・暗号利用モード調査 WG
第 9 回	平成 17 年 12 月 27 日	第 4 回署名・認証技術調査 WG
第 10 回	平成 18 年 2 月 2 日	第 4 回ハッシュ関数・暗号利用モード調査 WG
第 11 回	平成 18 年 2 月 24 日	第 5 回ハッシュ関数・暗号利用モード調査 WG
第 12 回	平成 18 年 2 月 24 日	第 5 回署名・認証技術調査 WG

３．１．４．国際学会等における発表の動向

（１） 国際会議への参加状況

平成 17 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。

情報収集の結果、ハッシュ関数に関する安全性の評価の進展を除いては、電子政府推奨暗号の安全性に影響を与える発表等は見られなかった。

監視要員等を派遣した国際会議は、表 10 に示すとおりである。

表 10　国際会議への参加状況

学会名・会議名		開催国・都市	期間
ISO/IEC	ISO/IEC JTC 1/SC 27/WG 2	Vienna, Austria	2005/4/11 ～ 2005/4/19
EUROCRYPT 2005	Eurocrypt	Aarhus, Denmark	2005/5/23 ～ 2005/5/26
ECRYPT	STVL Workshop	Aarhus, Denmark	2005/5/26 ～ 2005/5/27
ECRYPT	ECRYPT on Hash Function	Krakow, Poland	2005/6/21 ～ 2005/6/22
SAC 2005	Selected Area in Cryptography	Kingston, CANADA	2005/8/11 ～ 2005/8/12
CRYPTO 2005	CRYPTO	Santa Barbara USA	2005/8/14 ～ 2005/8/18
HashWorkshop	NIST Hash Workshop	Washington, USA	2005/10/31～ 2005/11/1
ISO/IEC	ISO/IEC JTC 1/SC 27/WG 2	Kuala Lumpur, Malaysia	2005/11/7 ～ 2005/11/11

Asiacrypt	Asiacrypt	Chennai, India	2005/12/4～2005/12/8
Indocrypt	Indocrypt	Bangalole, India	2005/12/10～2005/12/12
CANS	The 4th International Conference on Cryptology and Network Security	Xian, China	2005/12/14～2005/12/16
CT-RSA	RSA Conference 2006, Cryptographers' Track	SanJose, USA	2006/2/13～2006/2/16

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

MD4 に関しては、2^{-2} から 2^{-6}確率の間の(トータルで 2^{8} operationsを超えない)計算量でMD4 の衝突を発見したという発表がなされた[Cryptanalysis of the Hash Functions MD4 and RIPEMD, Xiaoyun Wang, Xuejia Lai, Dengguo Feng, Hui Chen, Xiuyuan Yu, EUROCRYOPT2005]。

また、MD4 に対する第二原像攻撃 (Second-preimage Attack) として、ターゲットとなるメッセージを修正 (modify) してその修正したメッセージの第二原像 (Second-preimage) を求めるという不完全な形での攻撃が発表された [The Second-Preimage Attack on MD4,Hongbo Yu and Gaoli Wang and Guoyan Zhang and Xiaoyun Wang, CANS2005]

MD5 についても衝突攻撃が発表された。この衝突攻撃は、IBM P690 で MD5 の衝突を発見するのに必要な時間が、(M0, M0')の発見に約 1 時間(最速で 15 分)、(M1, M1')の発見に 15 秒から 5 分というものである [How to break MD5 and Other Hash Functions, Xiaoyun Wang, Hongbo Yu, EUROCRYPT2005]

SHA-0 については、4 ブロックSHA-0 の衝突攻撃により、80,000 CPU hoursで計算でき、具体的に衝突を示された [Collisions of SHA-0 and Reduced SHA-1, Eli Biham, Rafi Chen, Antoione Joux, Patrick Carribault, Christophe Lemuet, William Jalby, EUROCRYPT2005]。その後 この計算量は 2^{39}に改良された [Efficient Collision Search Attacks on SHA-0, Xiaoyun Wang, Hongbo Yu, and Yiqun Lisa Yin, CRYPTO2005]。

SHA-1 については、フルラウンドSHA-1 のディスターバンスベクトルを利用し、24 ステップから 80 ステップまでの近似衝突 (near collision) 差分パスで確率 2^{-68}のものを発見し、その後 1-23 ステップについてディスターバンスベクトルに対応する不可能な差分パスを可能な差分パスに変換する攻撃が発表された。衝突を発見するために必要な計算量は 2^{69}と見積もられている[Finding Collisions in the Full SHA-1, Xiaoyun Wang, Yiqun Lisa Yin, and Hongbo Yu, CRYPTO2005]。

その後、この計算量は 2^{63}にまで改良された[New Collision Search for SHA-1, Xiaoyun Wang, Andrew Yao and Frances Yao, CRYPTO2005]。

(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、無線システムBluetooth（ブルートゥース）に用いられているE0 というストリーム暗号の解読について鍵の最初の 24 ビットを $2^{23.8}$フレームかつ 2^{38}の計算量で推定が可能であるという発表があった[The Conditional Correlation Attack: A Practical Attack on Bluetooth Encryption, Yi Lu, Willi Meier, and Serge Vaudenay, CRYPTO2005]。

また、RC4 を用いた WEP という無線システムのセキュリティ規格に対して、鍵回復攻撃（key recovery attack）が提案され、入力する IV の生成の仕方(master key との関係)により攻撃しやすい場合があり、鍵の長さが伸びたとしてもそれを探索するのにかかる計算量は線形にしか増えず、実用的な攻撃だという発表がなされた。ただし、この攻撃が適用できる場合には制限があり、IV が攻撃に適した生成方法により作られた場合に限られる [A Practical Attack on the Fixed RC4 in the WEP Mode, Itsik Mantin, ASIACRYPT2005]。

他は、目新しいものは発表されていない。

(c)ブロック暗号の解読技術

電子政府推奨暗号の Camellia の解読に関する論文発表があったが、極めて少ない段数での評価であり、Camellia の安全性に直接影響するものではなかった。〔New Observation of Camellia, Duo Lei, Li Chao and Feng Keqin, SAC2005〕

2003 年に AES に対して XSL と呼ばれる代数的攻撃(Algebraic attack) が適用できるのではないかと言う発表があったが、それに対する否定的な結果として、XSL において中間値の消去を考えた場合に、効率的な攻撃が困難であることを示された。[An Analysis of the XSL Algorithm, Carlos Cid, and Gaetan Leurent, ASIACRYPT2005]。

3GPP の標準アルゴリズムとなっている KASUMI に対して、関連鍵矩形攻撃（related key rectangle attack）を適用することにより解読可能であるとする発表があったが、攻撃手法の前提に強い仮定があるため、実質的な利用については本攻撃の影響はほとんど無いと思われる。[A Related-Key Rectangle Attack on the Full KASUMI, Eli Biham, Orr Dunkelman, Nathan Keller, ASIACRYPT2005]

(d) 公開鍵暗号の解読技術

RSA暗号アルゴリズムに対して、Wiener攻撃(秘密鍵dのサイズが$N^{0.25}$以下の場合に多項式時間でdを求めるアルゴリズムが存在する)と 98 年にBoneh-Durfee-Frankelにより提案されたサイドチャネル攻撃の手法とを組み合わせた攻撃の論文が発表された。[Partial Key Exposure Attacks on RSA up to Full Size Exponents, Matthias Ernst, Ellen Jochemsz, Alexander May, Benne de Weger, EUROCRYPT 2005]

また、RSA暗号アルゴリズムに関する解析結果を示した論文が発表された。$ed \equiv 1(\mathrm{mod}\ lcm(p-1, q-1))$ なるd が小さい場合に想定される攻撃として、Continue fraction attack, lattice-based attack, factoring attack 等の様々な攻撃について解析し、現実的な範囲でのパラメータ評価を行った結果が示された。[Another Look at

Small RSA Exponents, M. Jason Hinek, CT-RSA 2006]

他、現在の電子政府推奨暗号リスト公開鍵暗号の安全性を急激に減少させる程の新しい解読技術は発表されていない。

また、最近の発表論文の傾向としては、従来一般的に安全性の証明モデルとして用いられていたランダムオラクルモデルとは異なる新しい安全性の証明モデルに関する研究をはじめとし、ランダムオラクルモデルに基づかない安全性証明による方式の提案・既にランダムオラクルモデルで安全性証明が示されている方式についてランダムオラクルの仮定を取り除いた場合の安全性解析等、”ハッシュ関数の出力≠ランダムオラクルの出力”の流れにのる発表が目立ちはじめている。

その他、アルゴリズムが仮定としている問題の解析等の研究も進展している。

国内では、ID ベース暗号やそれを利用したプロトコル・安全性モデル・困難性を仮定している問題の解析・実装技術及び実装解析・運用なども加味した上位アプリケーションなど研究のターゲットが多岐に渡っている。

３．２．暗号技術調査ワーキンググループ

３．２．１．概要

平成 17 年度は、SHA-1 の危殆化が顕在化してきたため、新規に署名・認証技術調査ワーキンググループを組織した。また、平成 16 年度の暗号利用モード調査ワーキンググループは、ハッシュ関数の暗号学的な安全性評価を活動に追加し、ハッシュ関数・暗号利用モード調査ワーキンググループと名称変更した。擬似乱数生成系調査ワーキンググループは昨年度の活動を継続した。各ワーキンググループ（WG）が活動した主要活動項目は、表 11 の通りである。

表 11　平成 17 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
署名・認証技術調査 WG	松本勉	①電子署名に関する技術的意見の提出 ②ハッシュ関数の安全性評価に関する情報発信方法の検討
ハッシュ関数・暗号利用モード調査 WG	古原和邦	①Wang 等の SHA-1 への攻撃の拡張性に関する検討 ②SHA-256、SHA-384、SHA-512 等の安全性の検討 ③暗号利用モード及びメッセージ認証の評価／標準化動向に関する調査
擬似乱数生成系調査 WG	金子敏信	擬似乱数生成系検定のためのミニマムセットの確定

３．２．２．署名・認証技術調査ワーキンググループ

（１）調査背景

ハッシュ関数に関する最近の研究結果が、電子政府及びシステム等におけるハッシュ関数の利用に及ぼす影響について調査する。特に、電子署名において、SHA-256、SHA-384、SHA-512 を利用できるように、これらのハッシュ関数の利用について調査する。主な検討項目は以下である。

１）電子署名法に基づく特定認証業務に係る電子署名の基準に記されている署名技術に関するハッシュ関数の利用についての調査と技術的意見の提出

２）MD5 の利用についての問題点の提出

３）ハッシュ関数の安全性評価に関する情報発信の方法についての検討

（２）活動内容

(a)　電子署名に関する技術的意見の提出

電子署名法に基づく特定認証業務に係る電子署名の基準に記されている公開鍵暗号技術で利用されているハッシュ関数として SHA-1 のみが規定されているため、SHA-1 以外のハッシュ関数を利用した電子署名が電子署名法では認められていない。そこで、SHA-256、SHA-384、SHA-512、RIPEMD-160 を利用した署名技術について検討し、電子署名に関する技術的意見を提言することが必要となっている。

SHA-256、SHA-384、SHA-512、RIPEMD-160 を利用した電子署名についての考え方を整理した上で、電子署名の指針の改訂に係わる意見を、「電子署名法の指針の改訂に係わる意見の提出」としてまとめた。

主な検討項目は以下であった。

１）電子署名の安全性が依存するアルゴリズム問題のパラメータサイズについてはこのまま維持する（規則第二条の第一,二,三号、告示第三条）。

２）電子政府推奨暗号リスト（平成 15 年 2 月 20 日）の注釈（注 6）において明記されているように、256 ビット以上のハッシュ関数を推奨しているので、RIPEMD-160 と SHA-224 の 2 つは追加しない。

３）RSASSA-PKCS1-v1_5 方式及びRSASSA-PSS方式[1]に関しては、ハッシュ関数SHA-256、SHA-384、SHA-512 の 3 つを追加する。

４）ECDSA 方式に関しては、平成 17 年 2 月 18 日時点でドラフト版である署名アルゴリズムの仕様書（SEC 1 v1.5 Working draft や Draft ANSI X9.62-2005）が正式版

[1] IETF RFC4055 において、SHA-1 以外のSHAの利用に係わるRSASSA-PSSに関する識別子が明確になった（平成 17 年 6 月 21 日）。

になり次第、ハッシュ関数 SHA-256、SHA-384、SHA-512 の 3 つの追加の検討をするが、セキュリティパラメータとの整合性を確認する必要はある。

５）DSA 方式に関しては変更なし。

６）告示第十条第二号（認定認証業務と他の業務との誤認を防止するための措置）に関しては、ハッシュ関数 SHA-256、SHA-384、SHA-512 の 3 つを追加する。

平成 17 年 7 月 15 日付けで暗号技術監視委員会にて承認され、平成 17 年 10 月 12 日暗号技術検討会へ提出されている。

（b）MD5 の利用についての問題点の提出

MD5 の衝突を発見することが容易な状況、及び、MD5の危殆化がシステムに及ぼす影響について、これまでに明らかにされてきている問題点をまとめた。

調査によって、不正行為以外にも現実的な問題に発展する危険性が示されていることから、暗号技術監視委員会の了承のもと、「MD5等に対する見解」を平成17年8月29日に暗号技術検討会事務局より各府省に通知した。

MD5については、以下のような問題点が知られている。

１）X.509 電子証明書における衝突

２）ポストスクリプトなどのページ記述言語における不正

（c）ハッシュ関数の安全性評価とその情報発信の方法についての検討

平成 17 年度、ハッシュ関数・暗号利用モード調査ワーキンググループでは、表 2 のようにハッシュ関数に関する安全性評価を実施した。

署名・認証技術調査ワーキンググループではこの評価結果を受けて、ハッシュ関数の安全性に関する技術的な情報を正式コメントとして公表する方法として、電子政府推奨暗号リスト（平成 15 年 2 月 20 日）において、SHA-1 及び RIPEMD-160 に付属している注釈を表 12 のように修正すべきであると判断した。

主な理由は以下の通り。

１）電子政府推奨暗号リスト及びその注釈が、CRYPTREC と外部との間の統一したインターフェイスとしての正式な文書であるから、注釈の修正をすることが適当である。

２）既存の注釈においても、256 ビット以上が望ましいとあり、問題意識は既に表明されているものの、ハッシュ関数の危殆化が進んでいるという事実を新たに、外部に公表する必要性がある。

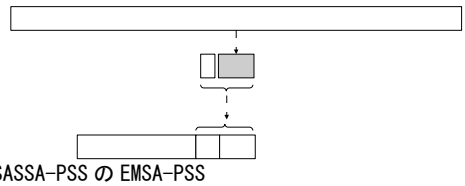
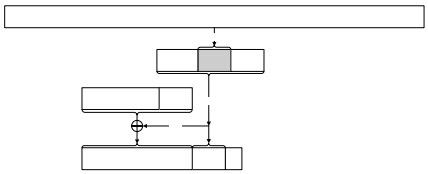
表 12　注釈修正についての素案

電子政府推奨暗号リスト（総務省・経済省、平成 15 年 2 月 20 日）の抜粋	
ハッシュ関数	RIPEMD-160(注 6)
	SHA-1(注 6)
	SHA-256
	SHA-384
	SHA-512
現在	（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。
素案※	（注 6）新たに電子政府用システムを構築または更改する場合、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。特に、ハッシュ関数の衝突発見困難性[2]を安全性の基礎とする用途においては、256 ビット以上のハッシュ関数を選択するべきである。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。

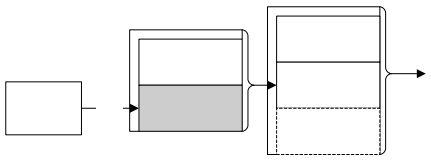
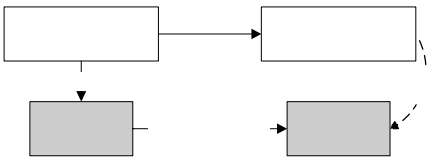
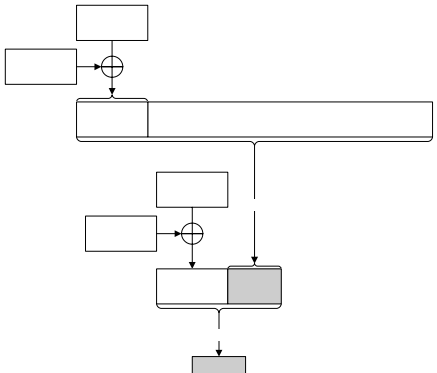
※ 表中の下線部が修正部分に相当する。

また、どのようなシステムであるとハッシュ関数の衝突発見からの影響を受けるのかについて、表 13 に示すようにハッシュ関数の利用形態別で分類した。

表 13　ハッシュ関数の利用に係わる類型化

分類	ハッシュ関数の安全性（擬似ランダム性を除く）	SHA-1 の利用に関する評価（2005 年度）	具体例
電子署名における入力メッセージのハッシュ値： 以下は、その例示である(署名生成における最初の段階)。 ・RSASSA-PKCS1-v1_5 の EMSA-PKCS1-v1_5  ・RSASSA-PSS の EMSA-PSS 	衝突発見困難性	衝突発見困難性については、2^{69} 回以下の SHA-1 の実行回数で攻撃できる手法が発見されている。	X.509 電子証明書(tbsCertificate 部分が入力メッセージにあたる)、 その他、X.509 形式を用いない電子署名全般

[2] 衝突発見困難性とは、ハッシュ値が一致するような異なる 2 つのメッセージを見つけることが計算量的に困難であることをいう(ハッシュ値は事前に与えられていない)。第二原像計算困難性とは、ある既知のメッセージとそのハッシュ値が与えられた時、ハッシュ値が与えられた値と一致するような別のメッセージを見つけることが計算量的に困難であることをいう。原像計算困難性とは、ある未知のメッセージのハッシュ値が与えられた時、ハッシュ値が与えられた値と一致するようなメッセージを見つけることが計算量的に困難であることをいう。

データやファイルのフィンガープリント (システム側にはハッシュ関数(のアルゴリズム識別子)とハッシュ値のみが明らかにされ、ユーザー側にのみハッシュ値の元となるメッセージが保持されている場合): 以下は、その例示である。 ・タイムスタンプ要求における要求側のメッセージフォーマット 	衝突発見困難性	衝突発見困難性については、2^{69}回以下のSHA-1の実行回数で攻撃できる手法が発見されている。	タイムスタンプサービスにおけるタイムスタンプ要求(メッセージのハッシュ値が MessageImprint フィールドに格納される)
データやファイルのフィンガープリント (ハッシュ値の元となるメッセージ及びハッシュ値の両方が明らかにされている場合): 以下は、その例示である。 ・通信における受信ファイルの検証 	第二原像計算困難性	第二原像計算困難性については、2^{60}バイトのメッセージに対して 2^{106}のSHA-1の実行回数で攻撃できる手法が公開されたが、2006 年 2 月の時点で脅威とは言えない。	データやファイルの暗号学的チェックサム
HMAC(IETF における RFC 2104 等で定められているもの): 	衝突発見困難性	初期値または入力の一部を秘密かつランダムとした場合の擬似ランダム性、衝突発見困難性が保証されていれば、SHA-1 を使った HMAC は安全である。	データやファイルの暗号学的チェックサム、暗号プロトコル(SSL3.0/TLS1.0, IPsec 等)の暗号学的チェックサム
暗号プロトコルや暗号アルゴリズムにおける補助関数など(鍵導出関数、マスク生成関数、擬似乱数生成系)	原像計算困難性、衝突発見困難性	特に問題は見つかっていない。	電子署名におけるエンコーディングメソッドの補助関数、公開鍵暗号や秘密鍵暗号、MAC のための鍵や初期値、salt 等の生成時の補助関数

タイムスタンプの要求側

TimeStampRe

version

HashAlgorithm

MessageImpr

任意の

M

.....

３．２．３．ハッシュ関数・暗号利用モード調査ワーキンググループ

（１） 調査背景

平成 16 年度、暗号利用モード調査ワーキンググループでは、米国を中心とする暗号利用モード標準の見直しの流れのもと、ブロック暗号を用いた暗号利用モードの調査研

究に注力した。平成 17 年度は、暗号利用モード標準化の動きが一段落したこと、ハッシュ関数の衝突解析に進展があり、現在利用されているハッシュ関数に対して脅威が生じる可能性が出てきたことから、電子政府推奨暗号の監視という観点より、ハッシュ関数の安全性に関する調査を行うこととした。平成 17 年度の目的は、電子政府推奨暗号リストに掲載されているハッシュ関数について最近提案されている攻撃方法の適用可能性を調査し安全性評価の再検討を行うと共に、主に米国で標準化が進んでいる暗号利用モードやメッセージ認証について調査を行い暗号技術監視委員会に報告することである。ハッシュ関数の安全性の検討に関しては署名・認証技術調査ワーキンググループと連携して評価項目や視点について吟味する。

ハッシュ関数の構成法としては、ブロック暗号に基づくもの(ISO/IEC 10118-2)、専用ハッシュ関数と呼ばれるもの(ISO/IEC 10118-3, FIPS180-2)、剰余演算を用いるもの(ISO/IEC 10118-4)などがあるが、電子政府推奨暗号にも含まれ、解析方法の進展が著しい、専用ハッシュ関数に注力して調査を行う必要がある。

（２）活動内容

(a) SHA-1 の安全性評価

【調査概要】

近年提案された SHA-1 の衝突攻撃(以下、Wang の攻撃手法と呼ぶ)について調査を行い、SHA-1 の安全性について検討した。

[W1] Xiaoyun Wang, Yiqun Lisa Yin and Hongbo Yu, "Finding Collisions in the Full SHA-1", Advances in Cryptology - CRYPTO2005, Lecture Notes in Computer Science Vol.3621, pp.17--36, Springer-Verlag, 2005

[W2] XiaoyunWang, Andrew C Yao and Frances Yao ," Cryptanalysis on SHA-1" http://www.csrc.nist.gov/pki/HashWorkshop/2005/Oct31_Presentations/Wang_SHA1-New-Result.pdf

Wang の攻撃手法の概要は、表 14 の通りである。

表 14 Wang の攻撃手法の概要

Wang の攻撃手法の位置づけ	暗号用ハッシュ関数が持つ衝突発見困難性と原像計算困難性および第二原像計算困難性のうち衝突発見困難性を誕生日攻撃よりも効率良く無効にしている。
攻撃条件	512 ビット入力に対して、1024 ビット (2 ブロック) を利用する
攻撃によって実現される脅威	ハッシュ値が同じになる 1024 ビットのメッセージ対を作成できる
攻撃コスト	誕生日攻撃が約 2^{80} 回のSHA-1 の実行を必要としているのに対して、 2^{69}回程度のSHA-1 の実行で攻撃が実行可能である。[W2]には 2^{63}回の実行回数による手法が述べられている。

SHA-1 の安全性の検討には、以下の技術的な検討と考察が必要である。

［検討 1］ Wang らの結果の追試(正しいのか、真偽判定に不明点はないか)

［検討 2］ 最終的な攻撃の実現可能性(改良の余地、攻撃計算量、実装容易性)

さらに Wang の攻撃手法には下記の技術的不明点がある。

a. 局所衝突の探索法とディスターバンスベクトルの最適性

b. 内部変数差分の決定法

c. 計算量見積もりの妥当性

そこで、これらを検討するために外部に評価依頼を行った。

以下、本年度の検討結果をまとめる。

（ｉ）技術的不明点 a. 局所衝突の探索法とディスターバンスベクトルの最適性

この課題について、局所衝突の見直しと組み合わせ探索及びその最適性について検討し、この最適性を裏付ける評価結果を得た。審議の結果、本質的な差分パスとそれから計算される充足確率の最適性は極めて高く、この観点からの劇的な攻撃の改良は困難と考えられると結論した。

（ii）技術的不明点 b. 内部変数差分の決定法

[W1]及び[W2]では内部変数差分の導出結果が例示され、その決定手法の一部が示されていない。しかしながら導出結果があれば、その後に続く処理の検証には障害にならず、また必要な計算量見積もりには影響を与えないことが確認された。従って、1 メッセージブロック目と 2 メッセージブロック目における 1 ラウンド目内部変数に対する差分の決定手法が明らかになっていないが、攻撃に必要な計算量の見積もりやアルゴリズムの検証において障害にならない、と結論した。

（iii）技術的不明点 c. 計算量見積もりの妥当性

技術的不明点b.が明らかでないものの計算量見積もりに影響を与えず、さらに必要な計算量は 2^{69}回のSHA-1 実行であることが確認された。従って、Wangの攻撃手法[W1]に必要な計算量見積もりは 2^{69}回のSHA-1 実行で妥当であると判断した。

上記の議論を踏まえて攻撃の実現性について検討した。Wang の攻撃手法[W1]は、計算量見積もりが確認できる程度に明らかになっているが、平成 18 年 2 月の時点では第三者が実装可能な状況にはない。しかし、攻撃アルゴリズムの大筋については確認できており、不明な部分も近い将来明らかになると予想する。

また、衝突探索に必要な攻撃アルゴリズムは、

・高い並列処理度

・極めて小さい必要メモリ量

という二つの特徴から、計算量単体評価の実現性と、攻撃全体の実現性のギャップは極めて小さいと考え、Wangらが発表したSHA-1 の計算量が 2^{63}の攻撃手法[W2]は、近い将来

に第三者による実装が可能になり、極めて大きな脅威となると考えられると結論した。

【SHA-1 の安全性評価のまとめ】

衝突発見困難性に対して、2^{69}回以下のSHA-1 の実行回数で攻撃できる手法が発見された。ただし、公開された攻撃アルゴリズムには一部不明な点があり、第三者によって実装して検証されたわけではない。しかし、アルゴリズムの不明な点は近い将来に明らかになり第三者による実装が可能になると予想されるので、本攻撃アルゴリズムは極めて大きな脅威になると考えられる。

第二原像計算困難性に対しては、2^{60}バイトのメッセージに対して 2^{106}のSHA-1 の実行回数で攻撃できる手法が公開されたが、平成 18 年 2 月の時点では脅威と言えない。

(b) SHA-256/-384/-512 の安全性評価

電子政府推奨ハッシュ関数である、SHA-256、SHA-384、SHA-512 に関する安全性を検討するために、外部に評価依頼を行った。

評価の結果、現時点ではSHA-1 の攻撃手法がそのまま適用できるわけではなく、SHA-2 の安全性を脅かすものではないとの結論が確認された。また、平成 15 年から平成 18 年 1 月末までに発表されたSHA-256、SHA-384、SHA-512 の安全性に関する論文を調査した結果、局所衝突に関しては、9 ステップで確率 2^{-66}で成立する局所衝突の発見が報告されているが、SHA-256 については 3 回以上の組み合わせが必要であり、誕生日攻撃を下回る計算量での攻撃には至っていないことが報告された。さらに、都合の良いメッセージ変更法が存在すると仮定した場合の安全性評価やメッセージ拡張関数の効果の解析について報告されているが、SHA-256、SHA-384、SHA-512 の安全性を脅かすレベルには達していないと結論された。

以上より、SHA-256、SHA-384、SHA-512 の安全性については、「実用的な安全性を脅かす攻撃方法が報告されていないため、これらのハッシュ関数は暗号の応用分野で使うのに十分安全であると考えられる」と結論した。

(c) RIPEMD-160 の安全性評価及び Whirlpool の調査

RIPEMD-160及びWhirlpoolの安全性を検討するために外部に評価依頼を行った。

評価の結果、RIPEMD-160はSHA-1と構造が異なるものの、メッセージ置換やステップ依存のビットシフトなど安全性について本質的な部分であるデータ撹拌の構造についてはSHA-1と同様であり、RIPEMD-160はSHA-1と同程度の衝突探索のための有効性を持つ差分パスを持つと予想されることが確認された。ただし、このような差分パスの探索は非

常に困難であり、現時点では有効な結果は得られていないことも示された。

しかしながら、研究の進展によってはSHA-1と同じ程度に危殆化する可能性があることから、「RIPEMD-160は異なる二つのブロック暗号L、Rで構成され、そのうちブロック暗号LについてはSHA-1と同程度の差分パスの存在が予想できることが報告されている。これはデータ撹拌においてメッセージ置換とステップ依存のビットシフトの採用などSHA-1と類似した関数を採用しているためであり、具体的なパスの発見など安全性に関する報告はないが、今後の研究の進展を考え研究動向について非常に注意する必要がある」と結論した。

WhirlpoolはRijmenとBarettoによって平成12年にNESSIEに提案され、その後、内部関数の仕様変更を経て平成17年にISO10118-3としてISO/IECの標準ハッシュ関数の一つに選ばれている。これまで安全性について述べられた文献はいくつかあるが、部分的な評価であり全体に関する安全性について言及されたものはない。

そこで、ビット単位の差分パス探索を行い差分特性確率の評価を行った結果、「Whirlpool全体では差分の拡散が十分であり、近年の攻撃手法を適用しても衝突発見は困難である」と結論した。

（d）暗号利用モード及びメッセージ認証の技術動向調査

暗号利用モード及びメッセージ認証の技術動向について平成 15 年度に引き続き調査を行った。新たなメッセージ認証方式として OMAC を追記し、NIST が OMAC1 を平成 17 年 5 月に SP800-38B として推奨方式に採用している情報を含めた。なお、NIST は OMAC1 を CMAC という名称で呼んでいる。

さらに HMAC の技術的詳細を追記し、その安全性について議論を行った。その結果、SHA-1 についてその初期値または入力の一部を秘密かつランダムとした場合の擬似ランダム性、衝突発見困難性が保証されていれば、SHA-1 を使った HMAC は安全である。Wang の攻撃手法は衝突攻撃であるが、上記の性質を脅かす結果は報告されておらず、HMAC の安全性に影響を与えないことを確認した。

３．２．４．擬似乱数生成系調査ワーキンググループ

（１）調査背景

電子政府推奨暗号リストにおける擬似乱数生成系では、SHA-1 を使った擬似乱数生成系が例示されている。しかし、用途によっては、例示された擬似乱数生成系以外でも、暗号学的に安全性が確認できれば、用途によっては利用できる場合もある。そこで電子政府で使用される擬似乱数生成系が、少なくとも高い乱数性を持つことを検証するためのツールが必要と考えられている。擬似乱数の検定法には様々な観点からの検定法が存

在しており、それらを複数集めて検定ツールとしてまとめられたものもいくつか存在する。代表的なものとしては、NIST Special Publication (SP) 800-22、DIEHARD、”The Art of Computer programming 準数値算法” D.Knuth 著に記載されたものなどが知られている。しかし、これらの検定ツールを比較検討すると、

１）検定ツールごと採用されている検定法が異なり、検定法の選択基準が明確になっていない

２）同じ検定手法でも検定ツール毎に閾値等の設定値が異なる場合がある

など問題点が存在する。特に、NIST SP800-22 に関しては、検定仕様のみならず対応する検定プログラムが公開されている。しかし、公開されている検定プログラムには、いくつかの検定法に不具合があることを指摘した学術論文がある。DIEHARD については、検定プログラムについては公開されているものの判断基準が示されていないので参考資料としての位置づけとした。

他方、暗号モジュール委員会で検討中の暗号モジュール評価においても擬似乱数検定が必要になるという背景があり、CRYPTREC としての擬似乱数検定ミニマムセットの策定を目標に、擬似乱数生成系の調査および検定法の調査を行っている。

（２）活動内容

乱数の検定法は一般的な乱数を対象としているが、CRYPTREC が対象としているのは暗号利用用途の擬似乱数生成系であり、このような観点から CRYPTREC が推奨する擬似乱数検定法をまとめた擬似乱数検定ツール(以下 CRYPTREC 擬似乱数検定ミニマムセット)を作成することを最終的な目標とした。

この CRYPTREC 擬似乱数検定ミニマムセットの導出にあたり各擬似乱数検定法の理論的根拠を確認し、どのような観点からの検定が CRYPTREC の方針に適切かを整理した。また、閾値等のパラメータを適切な値に修正した。

その結果、擬似乱数検定のためのミニマムセットとしては、NIST SP800-22 で取り上げられた 16 種類の検定法の中から表 15 に示す 14 種類の検定項目をミニマムセットとして採択した。

(a) 検定に対する可否判断基準

採択した 14 種類の検定項目に対して、NIST の SP 800-22 の検定法をベースに可否判断基準をリストアップし、検定に対する可否判断基準案を作成した。

表 15　検定に対する可否判断基準

検定項目名	可否判断基準	検定に用いるデータ-量
1.　頻度検定	p-value ≧ 0.01	1,000,000bit×1,000 本（総量 10^9bit）
2.　ブロック単位の頻度検定	p-value ≧ 0.01	
3.　連検定	p-value ≧ 0.01	

4. ブロック単位の最長連検定	p-value ≧ 0.01	
5. 2 値行列ランク検定	p-value ≧ 0.01	
6. 重なりの無いテンプレート適合検定	p-value ≧ 0.01	
7. 重なりのあるテンプレート適合検定	p-value ≧ 0.01	
8. Maurer の「ユニバーサル統計量」	p-value ≧ 0.01	
9. 線形複雑度検定	p-value ≧ 0.01	
10. 系列頻度検定	p-value ≧ 0.01	
11. 累積和検定	p-value ≧ 0.01	
12. ランダム回遊検定	p-value ≧ 0.01	
13. 変形ランダム回遊検定	p-value ≧ 0.01	
14. 近似エントロピー検定　(b)参照	p-value ≧ 0.01	

(b) 検定に用いる閾値等の修正

近似エントロピー検定においては、昨年度の調査結果からパラメータをせばめることによって利用できると考えられる。伏見らによる先行研究[伏見正則, ”乱数”, UP 応用数学選書, 東京大学出版会, 1989 年]では、$m < \log_2(n-6)$ で良いとあるが、昨年度実験した結果を考えると、具体的には、$m < \log_2(n-7)$ とパラメータの範囲を狭めることにより、正確な値をとりえると考えられる。以上のことから、近似エントロピー検定については範囲を狭めて（各ボックスに 100 個以上）ミニマムセットに含めることとした。

（c）ミニマムセット仕様書および擬似乱数検定ツールの作成

上記の結果に基づき、事務局で、NIST SP 800-22 “A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications”を参考に、「CRYPTREC 擬似乱数検定ミニマムセット仕様書」を作成した。

（３）まとめ

擬似乱数生成系調査ワーキンググループとしては、ワーキンググループ設置時点の目標である CRYPTREC 擬似乱数検定ミニマムセットの策定を完了した。一方、ISO/IEC JTC1 SC27 WG2 では、電子政府推奨暗号リスト中に例示された擬似乱数生成系以外の擬似乱数系を評価する際に利用する。ミニマムセットによる評価で不合格となる擬似乱数生成系は、採用しないように勧告する。

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

2003 年 2 月に、電子政府推奨暗号リストが発表され、どの暗号アルゴリズムが安全であるかの判断が公開された。しかし、実際に暗号を組み込んだ製品の安全性は、利用されている暗号アルゴリズムだけでなく、暗号アルゴリズムを実装した暗号モジュールにおける実装方法にも依存する。

CRYPTREC では 2003 年度から、次の 2 つを活動の柱として、暗号技術検討会の下に暗号モジュール委員会を設置した。

（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

４．１．２．暗号モジュール委員会の開催状況

2005 年度の暗号モジュール委員会は、計 5 回開催された。各回会合の概要は表１のとおりである。

表 16　2005 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 17 年 6 月 2 日 15:00～17:00	委員長互選 ISO/IEC JTC1 SC27/WG3 のウィーン会合報告 平成 17 年度暗号モジュール委員会活動計画（案）について 評価用標準プラットフォームによる実験データの収集について 運用ガイダンス第 0.1 版のレビュー
第 2 回	平成 17 年 10 月 14 日 15:00～17:00	NIST Physical Security Testing Workshop 報告 FDIS 19790 第 7 章日本語訳について
第 3 回	平成 17 年 12 月 16 日 13:00～15:00	FDIS 19790 の投票について 運用ガイダンス 2005-11-07 版について 暗号モジュール試験基準 2005-12-05 版について
第 4 回	平成 18 年 1 月 27 日 14:00～16:00	運用ガイダンス日本語訳について 暗号モジュール試験基準 2005-12-22 版について 「評価」及び「試験」の用語の使用方法について
第 5 回	平成 18 年 2 月 23 日	「暗号モジュールセキュリティ要件」2006-02-14 版に

	10：30～12：30	ついて CRYPTREC REPORT 2005「暗号モジュール委員会報告」(案)について

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

４．２．１．国際動向の概要

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[3] 140-2（米国NIST[4]）

（２）ISO[5]/IEC[6] 19790

４．２．１．１．FIPS 140-2

FIPS 140-2 は、米国/カナダが共同運用しているCMVP[7]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)[8]と運用ガイダンス(IG)[9]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は運用に関する説明を記述している。

NIST/CSE[10]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。

FIPS 140-2/-3 に関する詳細は、「４．２．２．FIPS 140-2 に関する動向」を参照のこと。

[3] Federal Information Processing Standard
[4] National Institute of Standards & Technology
[5] International Organization for Standardization
[6] International Electrotechnical Commission
[7] Cryptographic Module Validation Program
[8] Derived Test Requirements
[9] Implementation Guidance
[10] Communication Security Establishment

４．２．１．２．ISO/IEC 19790

ISO/IEC 19790 はFIPS 140-2 を元に作られた国際標準である。ISO/IEC JTC 1[11] 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[12]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Kuala Lumpur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。次回の 2006 年 5 月のMadrid会合で審議すべくWD[13]向け文書の準備中である。

ISO/IEC 19790 に関する詳細は、「４．２．３．ISO/IEC 19790 に関する動向」を参照のこと。

４．２．２．FIPS 140-2 及び関連文書に関する動向

４．２．２．１．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 が発行する米国政府標準規格である。

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 2006 年 1 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

[11] Joint Technical Committee 1
[12] Final Draft International Standard
[13] Working Draft

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 も FIP 140-2 と同様に適宜改訂されており、2004 年 3 月の改訂ドラフト版が 2006 年 1 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(すなわち、設定されたセキュリティレベルで、設定された分野のセキュリティ要求事項を暗号モジュールが満足するために適用しなければならない宣言)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、試験者が実施しなければならない試験手順を記述している。

（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、2005 年 12 月の改訂版が 2006 年 1 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)から構成されている。

“SECTION 1 から SECTION 14”は、FIPS 140-2 の 4.1 節から 4.11 節(SECTION 1 から SECTION 11 に対応)、APPENDIX A(SECTION 12 に対応)、APPENDIX B(SECTION 13 に対応)、APPENDIX C(SECTION 14 に対応)にそれぞれ対応しており、FIPS 140-2 で規定されるセキュリティ要求事項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。

“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。

４．２．２．２．FIPS 140-2の改訂に関する動向

2005 年 9 月 26 日～9 月 29 日に、米国ハワイのホノルルで「Physical Security Testing Workshop presented by the CMVP and IPA/INSTAC」が開催された。参加者は、59名で、内訳は次の通りであった。

米国(33)、カナダ(6)、英国(5)、フランス(2)、オランダ(1)、オーストラリア(1)、日本(9)、ドイツ(2)

この会議は、NIST/CSE と IPA 及び INSTAC が共催し CMVP 関係者向けに開いたサイドチャネル攻撃を含む物理セキュリティ試験ワークショップであり、物理セキュリティ関連技術のアップデートが目的であった。9 月 26 日、27 日の 2 日間にわたり、物理セキュリティに関する 19 本の発表があり、9 月 28 日、29 日は、主にパネルディスカッションが行われた。発表内容については、NIST の Web サイトに掲載されている。

http://csrc.nist.gov/cryptval/physec/physecdoc.html

＜CMVP について＞

この会議において、北米で行われている暗号モジュール試験及び認証制度である CMVP について、次のような説明及び今後の予定が発表された。

- FISMA(Federal Information Security Management Act)の猶予期間が終了したことにより、政府機関は、暗号モジュールを使用する際には、強制的に FIPS 140-2 で認証された暗号モジュールを使用しなければならなくなった。
- FIPS 140-2 は ISO/IEC 19790 の基となっている。
- FIPS 140-3 の改訂作業開始。
- 2005 年は 140 件の認証を行う予定。
- FIPS 186-3: Digital Signature Standard (DSS)が、近日中に発行される予定。
- CAVS(暗号アルゴリズム認証システム)で、SP 800-56：Key Establishment 及び TLS 1.0/IEEE 802.11i のプロトコル認証もサポートする予定。
- 2005 年 9 月現在 10 の試験機関が存在するが、2005 年中に 2 カ所増える予定。
- DES (FIPS 46-3)の失効により、2 年間をかけて、レガシーシステムでも AES/TDES に移行させる予定であり、予算処置がはかられることとなっている。

＜FIPS 140-3 について＞

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

- 2 つのセキュリティレベルの増設を行い、6 つのセキュリティレベルとなる。現行のセキュリティレベル 3 以上が再編される。【この会議後の情報によると、セキュリティレベル１から５の５段階に分けられることになったようである。】
- FIPS 140-2 の骨格に変更は無いが、全セクションに大幅な変更を加える。FIPS

140-1 から FIPS 140-2 への変更よりも、大きな変更となる。

・電力解析に関する要件が明示される。

・Software Security Section が設けられ Sub-Chip という新しい考え方を導入する。

・CC との関係を明確にする（Detached from CC［CC から分離］）。

・パワーアップ自己テストを含む、自己テストの章は、Pre-operational Test へ移行する。

・FIPS 140-3 での表現は ISO/IEC 19790 を継承する予定で、CSP・PSP の概念を取り入れる。これは、ISO/IEC 19790 2nd Edition を意識している（US として、CC 言語での再記述の意思が無いことを意味している）。また、FCC 要求事項を、FIPS 140-3 から取り下げる予定である。

・鍵のライフサイクル管理、暗号モジュールのライフサイクル管理も取り入れる。

＜FIPS 140-3 の物理セキュリティについて＞

この会議において、FIPS 140-2 の後継標準規格である FIPS 140-3 の物理セキュリティについて、次のようなアナウンスがあった。

・物理セキュリティに関する要求は、Non-Invasive/Invasive(非侵襲的/侵襲的)に分割して記述される。

・物理形態は、次の 4 つ。

- Sub-Chip
- Single-Chip
- Multi-Chip Embedded
- Multi-Chip Standalone

・VHDL の Source-code レベルでの試験が義務づけられる。

・セキュリティメカニズムについても詳細に文書化することが求められる。例えば、Removable covers and door に換気孔（Ventilating hole）等の開口部がある場合には、各ディバイスが observation から保護されている必要がある。

・場合によっては、セキュリティレベル 7 を設定し、CC で行なわれている様な Penetration Testing/Vulnerability Analysis の実施も考えられている。

＜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発表された。

・2005 年　9 月　　Draft #0 を試験機関に対して配布。

・2005 年 11 月　　Draft #1 を開示。3 ヶ月間のコメント募集期間を設ける。

・2006 年　2 月　　Draft #1 に対するコメント募集の〆切。

・2006 年　3 月　　DoC（米国商務省）による承認作業を開始予定。

・2006 年　9 月　　DoC（米国商務省）による承認。

・2006 年　3 月　　FIPS 140-3 発効予定。
・2007 年　9 月　　FIPS 140-2 廃止予定。

しかしながら、2006 年 2 月現在、Draft#0 を試験機関に対して配布すること以外の作業は大幅に遅れており、次のようにシフトされることが予想されている。

・2006 年　5 月　　Draft #1 を開示。3 ヶ月間のコメント募集期間を設ける。
・2006 年　8 月　　Draft #1 に対するコメント募集の〆切。
・2006 年　9 月　　DoC（米国商務省）による承認作業を開始予定。
・2006 年 12 月　　DoC（米国商務省）による承認。
・2007 年　6 月　　FIPS 140-3 発効予定。
・2007 年 12 月　　FIPS 140-2 廃止予定。

４．２．３．ISO/IEC 19790 に関する動向

ISO/IEC JTC 1 は、ISOとIECが共同で運営するIT技術標準規格化のための組織で、SC 27 委員会で情報セキュリティを、その下のWG 3 で情報セキュリティの評価基準を担当している。ISO/IEC JTC 1/SC 27/WG 3 は、2002 年 10 月から暗号モジュールに対するセキュリティ要件の国際標準規格化（規格番号 19790)を審議してきた。2005 年の国際会合は、4 月(オーストリア、ウィーン)と 10 月(マレーシア、クアラルンプール)の 2 回開催された。この間に暗号モジュール試験基準の国際標準化フェーズは、FCDからFDISへと進捗し、2005 年 12 月にはIS化するための投票が実施され、2006 年 3 月 1 日にIS[14]化が完了した。

ISO/IEC 19790 は、FIPS 140-2 をベースとした基準であるが、CC(Common Criteria)への連接性を意識しているため、詳細な評価項目は異なる部分が存在する。また、FIPS 140-3 については、成立見込み時期が ISO/IEC 19790 よりも遅いことから、ISO/IEC 19790 の内容を反映する可能性がある。

2005 年 4 月の会合では、暗号モジュールセキュリティ要件の国際標準規格化に付随した実際の試験に必要となる、暗号モジュール試験手順の標準化に関する study period の終結が宣言され、10 月の会合で、標準規格化作業が 2006 年 5 月の会合から開始されることが決まった。

４．２．４．国際標準規格への対応

今年度、暗号モジュール委員会では、４．１．２．１．節で述べたような暗号モジュール試験の標準規格化に関する国際動向に対応すべく、その準備として、以下の（１)、（２）の作業を行った。

（１）暗号モジュールセキュリティ要件の作成

[14] International Standard

2005 年 10 月会合で確認された国際標準規格（ISO/IEC FDIS 19790）に基づき、翻訳版を作成した。詳しくは、４．３．１．節に述べる。

（２）FDIS 19790 に対応した暗号モジュール試験要件の検討

2005 年 10 月会合で確認された国際標準規格（FDIS 19790）に対応する暗号モジュール試験要件の検討を行った。詳しくは、４．３．２．節に述べる。

４．３．暗号モジュールセキュリティ要件及び関連文書の策定

４．３．１．暗号モジュールセキュリティ要件の作成

昨年度の暗号モジュール委員会では、“FIPS PUB 140-2, SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES, CHANGE NOTICE(12-03-2002)”を翻訳したものを暗号モジュール評価基準第 0.1 版として発行した。

ISO/IEC JTC 1/SC 27/WG 3 では、FIPS PUB 140-2 を基に暗号モジュールのセキュリティ要件に関する規格 ISO/IEC 19790 を 2006 年 3 月 1 日付けで発行した。今年度の暗号モジュール委員会では、スケジュールの都合上、IS 発行を待つことが出来なかったため、投票文案として最終版となる ISO/IEC FDIS 19790 を翻訳し、「暗号モジュールセキュリティ要件」を策定した。なお、FDIS から IS に移行する過程では、基本的にエディトリアルな修正しか行われないため、IS 版の内容はほぼ反映されている。

「暗号モジュールセキュリティ要件」については、出版権、翻訳権等の関係上、当面非公開とする。

４．３．２．暗号モジュール試験要件の作成

昨年度の暗号モジュール委員会では、“Derived Test Requirements for FIPS PUB 140-2, Security Requirement for Cryptographic Modules (March 24, 2004 Draft)”を翻訳したものを暗号モジュール試験基準第 0.1 版として発行した。

今年度の暗号モジュール委員会では、暗号モジュール試験基準第 0.1 版を基に、FIPS 140-2 と ISO/IEC FDIS 19790 の差分を比較・検討して新たに試験要件の追加及び変更を行い、「暗号モジュール試験要件」を策定した。

「暗号モジュール試験要件」については、出版権、翻訳権等の関係上、当面非公開とする。

４．３．３．運用ガイダンスの検討

（１）運用ガイダンスの作成

まず、事務局にて米国 NIST が発行した“Implementation Guidance”の 2005 年 9 月改訂版の翻訳案を作成し、翻訳案に対して委員会内での審議を行い、英

文解釈の統一化を図った。

次に、“Implementation Guidance”が 2005 年 12 月に改訂されたため、その差分について、事務局にて翻訳案を作成し、同様に委員会内での審議を行い、英文解釈の統一化を図った。

そして、委員会内での英文解釈を統一化した“Implementation Guidance”の 2005 年 12 月改訂版の翻訳を「運用ガイダンス」としてまとめた。

（２）運用ガイダンスの構成

「運用ガイダンス」は、“Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program, Initial Release: March 28, 2003; Last Update: December 01, 2005”を翻訳したものであり、構成は、４．１．１節（３）で述べた“Implementation Guidance”と同様である。

本文は全 17 節から構成されており、「概要」、「全般的な問題」、「第１章　暗号モジュールの仕様」、「第２章　暗号モジュールのポート及びインタフェース」、「第３章　役割、サービス、及び認証」、「第４章　有限状態モデル」、「第５章　物理的セキュリティ」、「第６章　動作環境」、「第７章　暗号鍵管理」、「第８章　電磁妨害/電磁両立性(EMI/EMC)」、「第９章　自己テスト」、「第１０章　設計保証」、「第１１章　その他の攻撃への対処」、「第１２章　Appendix A: 文書要求事項のまとめ」、「第１３章　Appendix B: 推奨ソフトウエア開発手順」、「第 14 章　Appendix C: 暗号モジュールのセキュリティポリシ」、「取消された運用ガイダンス」が記述されている。

各節の冒頭には、NIST 及び CSE からの解答内容に関し、適用されるセキュリティレベル、有効期間、最終改訂日、DTR の関連するアサーションの番号(AS 番号)、DTR の関連する試験者に課せられる要求事項の番号(TE 番号)、DTR の関連するベンダに課せられる要求事項の番号(VE 番号)が記述されている。その後に、背景(節によっては記述されない)、NIST 及び CSE への質問内容、NIST 及び CSE からの解答、NIST 及び CSE からの追加コメントが順に記述されている。

「運用ガイダンス」については、下記 URL の「CRYPTREC Report 2005 の公開」から参照できる。

http://www.cryptrec.jp/report.html
http://www.ipa.go.jp/security/enc/CRYPTREC/index.html
http://cryptrec.nict.go.jp/cryptrec_info_publicity.html

４．４．非破壊攻撃及び破壊攻撃に対する調査・研究

４．４．１．SCIS 2006 での発表

2006 年 1 月に開催された SCIS 2006 では、サイドチャネル攻撃関係の講演は、3 セッションで全 12 件の発表があった。

そのうち、INSTAC-8 仕様に準拠したボードを用いたサイドチャネル攻撃の実験報告は、以下の 4 件であった。

（１）INSTAC-8 を用いた電力解析

（ａ）1C3-1　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［宮崎,辻村,松本（横浜国立大学)］

（ｂ）1C3-2　ストリーム暗号に対する DPA［久門,角尾（日本電気株式会社）,後藤,池永（早稲田大学)］

（ｃ）1C3-4　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［山口,山田（三菱電機株式会社)］

（ｄ）2C1-2　Sbox 特性を利用した DPA 評価手法の有効性検証［三宅,野崎,清水,新保 淳（(株）東芝)］

（２）電磁界を用いたサイドチャネル攻撃

電磁界を用いたサイドチャネル攻撃に関しては、講演者が独自に開発した FPGA 基板を用いた実験の報告がなされた。

（ａ）1C3-5　FPGA 上での電磁波/電界情報に基づくサイドチャネル解析の試行［佐伯,鈴木,佐藤（三菱電機株式会社)］

（３）その他の講演

（ア）安全性評価

電力解析を用いた実装方式の安全性評価に関しては、下記の 3 件の報告があった。

（ａ）1C3-3　2 線式回路による DPA 対策方式の安全性評価　［鈴木,佐伯（三菱電機株式会社)］

（ｂ）2C2-1　A power disturbance circuit for A5/1 resistant to power analysis attack　［戴,久門,劉,後藤,池永（早稲田大学）,角尾（ＮＥＣ)］

（ｃ）2C1-3　鍵付きハッシュ関数に対するサイドチャネル攻撃　［桶屋（(株）日立製作所)］

（イ）楕円曲線暗号に対する電力解析

楕円曲線暗号に対する電力解析に関する報告としては、以下の 2 件があった。

（ａ）2C1-1　Side Channel Attack on Improved XTR Single Exponentiation and a New Countermeasure　[D.G. Han,高木（函館みらい大)T.H. Kim (Korea University),H.W. Kim, K.I.Chung(ETRI)]

（ｂ）2C1-4　ランダム化射影座標を用いた楕円曲線暗号実装に対する電力解析　[酒井（三菱電機株式会社)]

（ウ）キャッシュ攻撃関係

2C2-2　サイドチャネル防御機構付き分割キャッシュアーキテクチャに関する一考察　[太田,川幡,角尾（日本電気株式会社）,辻原（株式会社ワイ・デー・ケー）,久保,洲崎（北陸日本電気ソフトウェア株式会社)]

（エ）TEMPEST 関係

2C2-3　PC から放出する電磁気的雑音と含有するモニタ表示画像の再現 [関口,田中,瀬戸,山村（情報通信研究機構)]

４．４．２．CHES 2005 での発表

2005 年 8 月に英エジンバラで開催された CHES 2006 では、サイドチャネル攻撃関係は、3 セッション 8 件の講演がなされた。

その内、電磁界（EM）攻撃に関して、1 セッション 3 件の講演があったことは注目される。

また、ハードウェアベースのサイドチャネル攻撃とその対策技術として、3 セッション 7 件の講演があった。

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、2006 年度以降以下の活動を実施していくこととする。

５．１．今後の CRYPTREC の活動目的及び活動内容

５．１．１．活動目的

CRYPTREC は、暗号技術及び暗号関連技術の評価等を通じて、電子政府等の安全性及び信頼性の確保に貢献することを目的として活動する。

５．１．２．活動内容

CRYPTRECは、2006年度以降も引き続き以下の活動を行う。なお、今後、新たに必要と考えられる事案が生じた場合には、その都度、暗号技術検討会において具体的な活動内容を検討していくものとする。

（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に関する調査・検討

暗号アルゴリズムに関する国際標準との関係も含め、電子政府推奨暗号リストの今後のあり方に係る論点について、技術的見地から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．今後の CRYPTREC 体制

CRYPTREC は、2006 年度以降も引き続き、「暗号技術検討会」、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」により構成されるものとする。

暗号技術検討会、暗号技術監視委員会、暗号モジュール委員会、暗号技術調査 WG の位置づけ、構成及び機能は以下のとおり。

５．２．１．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、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。

５．２．２．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な助言を行う。

５．２．３．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る。暗号モジュール委員会は、米国における暗号モジュールセキュリティ要件の次期バージョンであるFIPS 140-3及び、ISO/IECによる暗号モジュール試験要件（ISO/IEC 24759）の策定に対して貢献する。

また、電子政府推奨暗号の安全性及び信頼性確保のための、主として暗号実装関連技術等を対象とする調査・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[15]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（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）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。

---

15 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

（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。

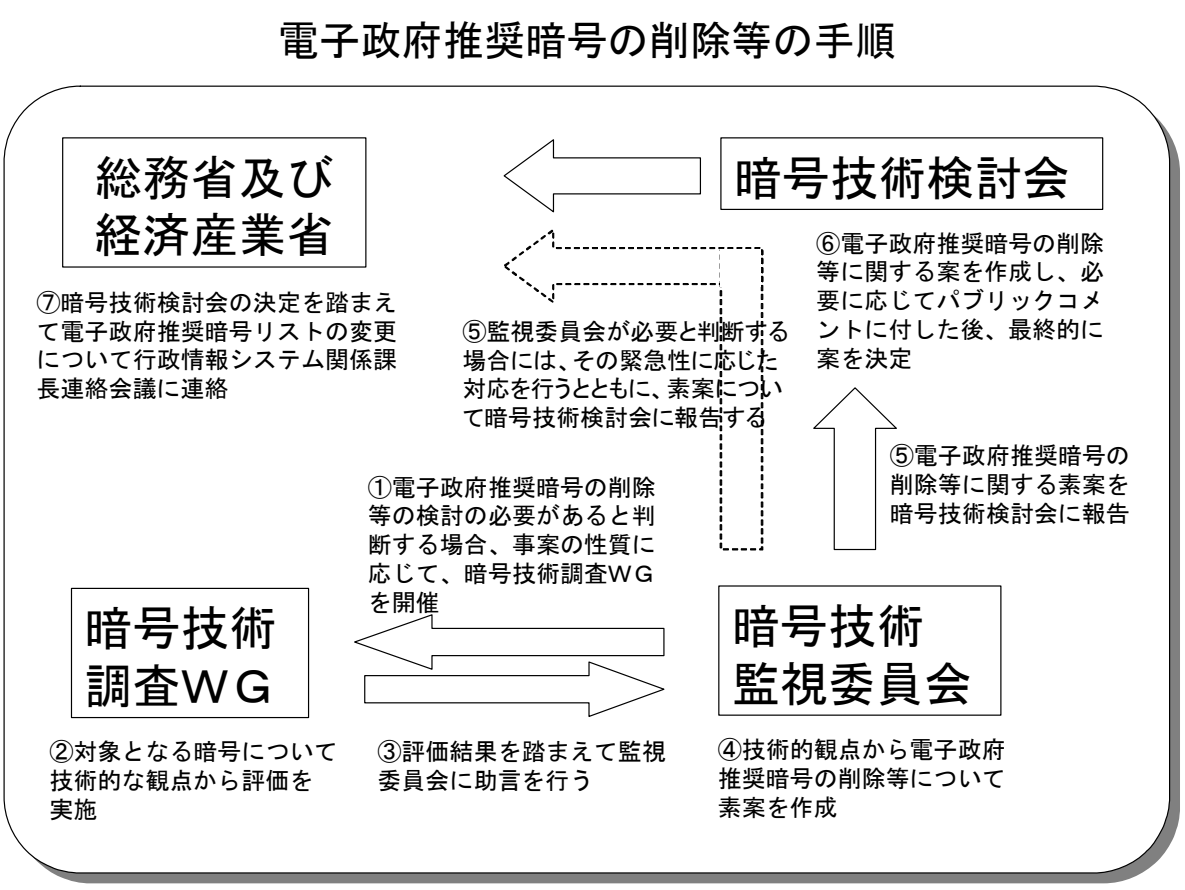


図２　電子政府推奨暗号削除等の手順

５．４．電子政府推奨暗号リストの改訂

５．４．１．基本的認識

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。そこで、危殆化した暗号の削除や新しい暗号の選定等により、電子政府推奨暗号リストを一定期間毎に改訂することが望ましい。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。

５．４．２．基本的考え方

リストの改訂作業の具体的な実施内容については、電子政府の導入状況及び電子政府推奨暗号の監視状況を考慮しつつ、然るべきタイミングで検討を行うこととする。なお、リスト改訂作業の実施方法としては、現在のところ、以下のような検討事項が想定されるところである。

（想定される検討事項）

（イ）公募の要否

（ロ）リスト項目（技術分類等）の見直し

（ハ）項目別の掲載暗号数

（ニ）評価基準、評価方法

また、改訂作業の具体的な開始時期については、検討会において検討の上決定するが、改訂作業の完了及び新リストの決定は、遅くともリスト策定から10年を経た2013年までに行うこととする。なお、仮に公募を実施するとした場合は、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、遅くとも2008年3月頃には公募のアナウンスを行うことが望ましい。

５．５．暗号モジュールに関する検討

電子政府の安全性及び信頼性を確保するためには、暗号技術レベルの安全性だけでなく暗号技術の実装の安全性を確保する必要があり、この観点から暗号モジュールのセキュリティ要件と試験要件を作成してきた。しかし、元とした米国の政府調達基準である FIPS 140-2 については、改訂作業を開始し、また、ISO/IEC においては、暗号モジュール試験要件を新規に策定する作業が開始されている。

このような状況を踏まえて、暗号モジュール委員会は、米国における暗号モジュールセ

キュリティ要件の次期バージョンである FIPS 140-3 及び、ISO/IEC による暗号モジュール試験要件（ISO/IEC 24759）の策定に対して貢献する。

なお、暗号モジュール委員会は、暗号技術監視委員会と連絡をとりつつ、電子政府推奨暗号の安全性及び信頼性確保のための暗号実装関連技術を主な対象とする調査・検討を併せて行うこととする。

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