暗号技術検討会

２００７年度報告書

暗号技術検討会

２００８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。

「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 2007」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。

2007 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を行った。暗号技術監視委員会では、これまでの電子政府推奨暗号に関する暗号技術の監視、調査等の活動に加え、電子政府推奨暗号リストの利用指針及び電子政府システムの構築に必要な技術等を示すリストガイドを作成した。また、暗号モジュール委員会では、北米の FIPS や国際標準機関である ISO/IEC に関する暗号モジュールのセキュリティ要件及び試験要件の調査や、同機関への提案等を実施した。

なお、2007 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 2007」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。

2008 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ワーキンググループを設置し、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、同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、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。

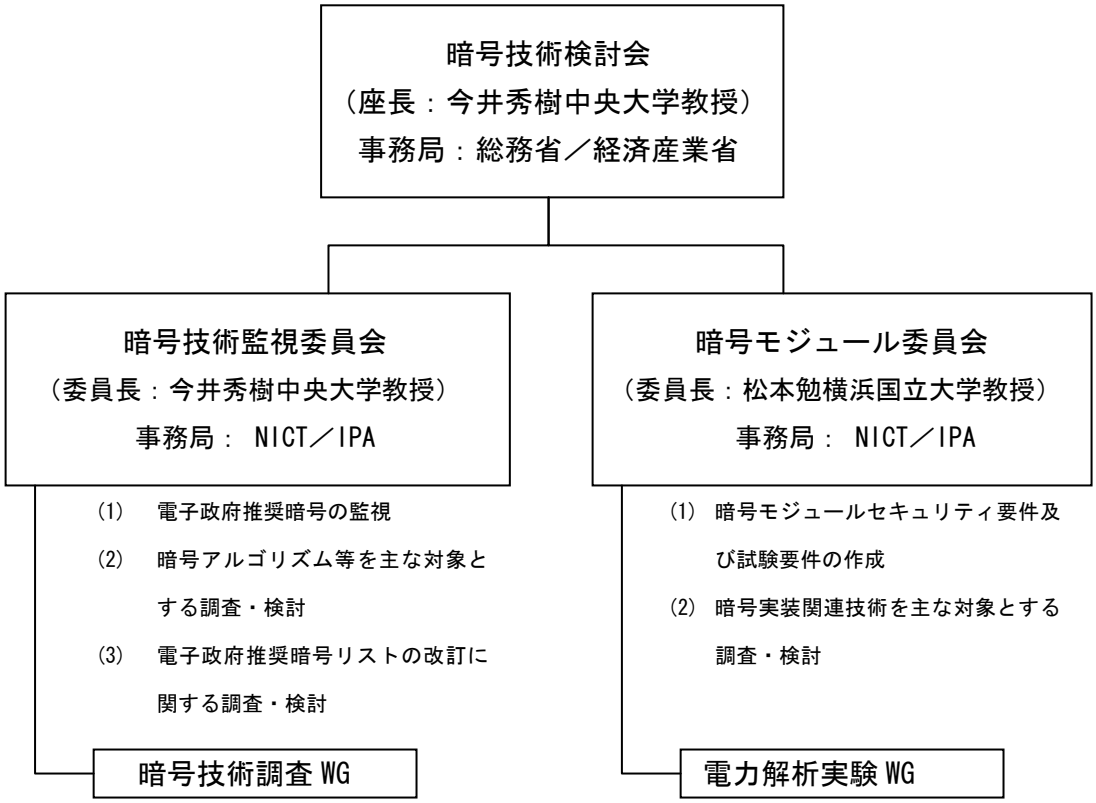

図 1　2007 年度 CRYPTREC の体制図

２．３．暗号技術検討会メンバー

（構成員）※肩書は 2008 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 主席研究員（（社）電気通信事業者協会代表兼務）
	加藤　義文	（社）テレコムサービス協会技術委員会委員長
	金子　敏信	東京理科大学理工学部電気電子情報工学科教授
	国分　明男	（財）ニューメディア開発協会顧問・首席研究員
	櫻井　幸一	九州大学大学院システム情報科学研究院教授
	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）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	セコム株式会社ＩＳ研究所基礎技術ディビジョン主席研究員

（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
塚田　桂祐	総務省大臣官房参事官
相澤　哲	法務省民事局商事課長
菊田　豊	外務省大臣官房情報通信課長
児玉　清隆	財務省大臣官房文書課情報管理室長
田中　正幸	文部科学省大臣官房政策課情報化推進室長
佐藤　勉	厚生労働省大臣官房統計情報部企画課情報企画室長補佐
和泉　章	経済産業省産業技術環境局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）情報通信研究機構情報通信セキュリティ研究センター長
大蒔　和仁	（独）産業技術総合研究所研究コーディネータ
山田　安秀	（独）情報処理推進機構セキュリティセンター長
亀田　繁	（財）日本情報処理開発協会電子署名・認証センター長
郡山　信	（財）金融情報システムセンター監査安全部長

２．４．暗号技術検討会開催状況

2007 年度、検討会は計 3 回開催された。各回会合の開催日及び主な議題は以下のとおり。

【第 1 回】2007 年 6 月 15 日（金）

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

【第 2 回】2007 年 11 月 20 日（火）

（主な議題）・暗号モジュール委員会中間報告
・暗号技術監視委員会中間報告
・暗号技術仕様の変更手順について
・電子政府推奨暗号リストの改訂に向けた検討に関する中間報告

【メール審議】2007 年 3 月 3 日(月)～5 日(水)

（議　　題）・電子署名及び認証業務に関する法律の施行状況に係る検討会からの照会（SHA-1 及び RSA1024bit の危殆化に係る見解）について

【第 3 回】2008 年 3 月 25 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 2007 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 19 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訂を考慮して、電子政府推奨暗号に関する調査・検討を行う。監視活動は、情報収集、情報分析、審議及び決定の 3 つのフェーズからなる。

暗号技術検討会における電子政府推奨暗号の監視に関する基本的考え方は以下の通りである。

（１） 実運用環境において安全性に問題が認められた電子政府推奨暗号は原則としてリストから削除する。

（２） 電子政府推奨暗号の仕様変更は認めない。

（３） 電子政府推奨暗号の仕様変更に到らないパラメータの修正等の簡易な修正を行うことにより当該暗号の安全性が維持される場合には、修正情報を周知して当該暗号をリストに残す。

以上の指針に基づき、監視要員は研究集会、国際会議、研究論文誌、インターネット上の情報等を監視し、電子政府推奨暗号の安全性に関して情報を分析し、それを暗号技術監視委員会に報告する。また、暗号技術調査ワーキンググループは暗号技術監視委員会の指示のもとに監視活動として必要な調査・検討活動を担当する。

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 19 年度の報告時点では、収集した全ての情報が、「情報収集」、「情報分析」フェーズに留まり、「審議及び決定」には至らず、電子政府推奨暗号の安全性に懸念を持たせるような事態は生じていないと判断した。

具体的な動きとしては、ECRYPT Hash Workshop 2007 において、C.Canniere(グラーツ工科大)らが 2 ブロックメッセージに対して、SHA-1 の 70 段縮小版の衝突発見を発表している。また、CRYPTO2007 において、A.Joux(DGA and Versailles University)らも、共通鍵暗号への攻撃手法の一つであるブーメラン攻撃を応用し SHA-1 の 70 段縮小版の衝突発見を発表している。

また、Eurocrypt2007 において、A.Lenstra らが、MD5 の衝突探索攻撃を応用して、X.509 の署名偽造に成功した事例を発表している。

さらに、メールなどの受信時の認証などとして用いられている、チャレンジレスポンス型で MD5 を利用した暗号プロトコル APOP に関しての解析結果が示された。理論的には 79 文字までは総当り攻撃よりも有効な解析が実行可能となることが示されている。

（２）公開鍵暗号方式の安全性評価について

平成 19 年度の報告時点では、収集した全ての情報が、「情報収集」、「情報分析」フェーズに留まり、「審議及び決定」には至らず、電子政府推奨暗号の安全性に懸念を持たせるような事態は生じていないと判断した。

具体的な動きとしては、Eurocrypt2007 において、K. Aoki(NTT)らが特殊数体篩法(SNFS)を利用した、1039 ビットの合成数 $2^{1039}-1$ の素因数分解例を発表している。なお、特殊数体篩法は大部分の合成数に対して適用できないので、1024 ビット鍵の RSA 暗号の安全性が低下したわけではない。

（３）暗号技術標準化動向

NIST による次世代ハッシュ関数 SHA-3 の公募が 2007 年 11 月 2 日付けで開始された。公募要領や安全性や実装性能で評価する方針が表明されている。

３．１．３．暗号技術監視委員会開催状況

平成 19 年度、暗号技術監視委員会は、表 1 の通り 3 回開催された。暗号技術調査ワーキンググループは、表 2 の通り計 8 回開催された。各会合の開催日及び主な議題は以下の通りである。

表 1　暗号技術監視委員会の開催

回	年月日	議題
第 1 回	平成 19 年 6 月 5 日	活動方針確認、暗号技術監視状況報告
第 2 回	平成 19 年 11 月 13 日	暗号技術調査 WG 中間報告、電子政府推奨暗号リスト改訂のための検討状況報告
第 3 回	平成 20 年 3 月 3 日	監視状況報告、CRYPTREC Report 2007 審議

表 2　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 19 年 5 月 16 日	第 1 回公開鍵暗号 WG（活動計画の審議）
第 2 回	平成 19 年 8 月 7 日	第 1 回リストガイド WG（活動内容の審議）
第 3 回	平成 19 年 10 月 17 日	第 2 回リストガイド WG（対象技術の審議）
第 4 回	平成 19 年 12 月 18 日	第 2 回公開鍵暗号 WG（活動計画修正の審議）
第 5 回	平成 20 年 1 月 16 日	第 3 回リストガイド WG（報告書 0 次案の審議）
第 6 回	平成 20 年 2 月 8 日	第 3 回公開鍵暗号 WG（仕様及び仕様参照先の審議）
第 7 回	平成 20 年 2 月 22 日	第 4 回公開鍵暗号 WG（報告書 0 次案の審議）
第 8 回	平成 20 年 2 月 25 日	第 4 回リストガイド WG（報告書 1 次案の審議）

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

監視要員等を派遣した国際会議は、表 3 に示すとおりである。

表 3　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
TCC 2007	The fourth Theory of Cryptography Conference	アムステルダム（オランダ）	2 月 21 日～2 月 26 日
FSE 2007	The 14th Fast Software Encryption	ルクセンブルグ（ルクセンブルグ）	3 月 26 日～3 月 28 日
PKC 2007	The 10th International Workshop on Practice and Theory in Public Key Cryptography	北京（中国）	4 月 16 日～4 月 20 日
Eurocrypt 2007	26th International Conference on the Theory and Application of Cryptographic Techniques	バルセロナ（スペイン）	5 月 21 日～5 月 24 日
ECRYPT Hash Workshop 2007	ECRYPT Hash Workshop 2007	バルセロナ（スペイン）	5 月 24･25 日
SAC 2007	The 14th Annual Workshop on Selected Areas in Cryptography	オタワ（カナダ）	8 月 16･17 日
CRYPTO 2007	The 28th International Cryptology Conference	サンタバーバラ（米国）	8 月 19 日～8 月 23 日
ECRYPT/SHARCS ’ 07	Special-purpose Hardware for Attacking Cryptographic Systems	ウィーン（オーストリア）	9 月 9 日～9 月 10 日
FDTC 2007	4th Workshop on Fault Diagnosis and Tolerance in Cryptography	ウィーン（オーストリア）	9 月 10 日
CHES 2007	9th Workshop on Cryptographic Hardware and Embedded Systems	ウィーン（オーストリア）	9 月 11 日～9 月 13 日
ECRYPT/TFC	Tools for Cryptanalysis	クラクフ（ポーランド）	9 月 24 日～9 月 25 日
IEEE/FOCS 2007	48th Annual IEEE Symposium on Foundations Of Computer Science	プロヴィデンス（米国）	10 月 20 日～10 月 23 日
ProvSec 2007	International Conference on Provable Security 2007	ウロンゴン（オーストラリ	11 月 1 日～11 月 2 日

Asiacrypt 2007	The 14th Annual International Conference on the Theory and Application of Cryptology & Information Security	クチン（マレーシア）	12月3日～12月6日
FSE	The 15th Fast Software Encryption	ローザンヌ（スイス）	2月11日～2月13日
ECRYPT/SASC 2008	The State of the Art of Stream Ciphers IV	ローザンヌ（スイス）	2月13日・14日

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

（２）解読技術の動向

① ハッシュ関数の解読技術

SHA-1 の衝突発見法の研究も段階的に進み、衝突発見可能段数はこれまでの 64 段から 70 段まで伸び、フルラウンド 80 段に近づいた。80 段に対する差分経路は分かっているので、グリッド計算機と分散 PC を合わせた衝突メッセージの発見プロジェクトも実施中である。[On the full cost collision search for SHA-1, C.De Canniere et al., ECRYPT Hash Workshop 2007;Dedicated Collision Search, C.Rechberger, SHARCS 2007] また、ブロック暗号用のブーメラン攻撃法を適用することで、70 段の衝突を発見している。この攻撃では差分経路は変えないものの、衝突発見の計算量を 1/30 に削減する方法も提案されている。[Hash Functions and the (Amplified) Boomerang Attack, A.Joux & T.Peyrin, CRYPTO 2007]

MD4 と MD5 に対しては衝突発見法の効率が非常に向上し、通常の PC でも短時間で実行可能となっている。第 2 原像計算も実行可能となり、それを利用した署名偽造も提案されている。[Full Key-Recovery Attacks on HMAC/NMAC-MD4 and NMAC-MD5, P.A.Fouque et al.,CRYPTO 2007] さらに、MD4 では原像計算困難性も否定されるに至った。[MD4 is Not One-Way, G.Leurent, FSE 2008]

② ストリーム暗号の解読技術

GSM で利用されている A5/2 に対する攻撃がいくつか提案されているが、実際に解こうとすると連立方程式の解法のコストの大きさが問題になる。そこで 0.18μロジックの専用 ASIC で Gauss-Jordan 法を実装したところ、事前計算無しで、約１秒で初期状態を復元することに成功した。[Hardware-Assisted Realtime Attack on A5/2 without Precomputations, A.Bogdanov et al., CHES 2007]

RC4 は広く利用されているストリーム暗号の一つで、鍵セットアップ(KSA)の後、擬似乱数生成(PRGA)を行うという２段階の動作を行う。従来から、KSA 後の状態に偏りがあることが知られ、それを利用した攻撃法が提案されてきたが、致命的ではないと考えられてきた。この発表では、鍵に関する情報に関わりなく、256 番目及び 257 番目の出力バイトで、状態の偏りが最も大きくなる時刻を明らかにした。この偏

りは、ランダムに選んだ 1 万個の暗号化鍵に対し、148 個で現れる。[New Form of Permutation Bias and Secret Key Leakage in Keystream Bytesof RC4, S.Maitra & G.Paul, FSE 2008]

③ ブロック暗号の解読技術

AES に対する SQUARE 攻撃の手法を応用して 5 段の識別子を作り、それを利用した中間一致攻撃が提案された。この攻撃によって、192 ビット鍵 AES で 7 段まで、256 ビット鍵 AES で 8 段まで解読可能であることが示された。[A Meet-in-the-Middle Attack on 8-Round AES, H.Demirci & A.A.Selcuk, FSE 2008]

SQUARE 攻撃を一般化した Integral 攻撃は AES のような SPN 型に対して有効であることが知られているが、S-box のサイズを単位とするのが基本となっている。しかし、ビット・パターンに着目したビット単位の積分攻撃も可能である。ビット単位の Integra 攻撃をブロック暗号に適用したところ、AES の設計者が設計した Noekeon で 5 段まで、AES 最終 5 候補の一つの Serpent で 5 段まで、CHES 2007 で小型実装用に提案された PRESENT で 7 段まで解読可能であることが分かった。[Bit-Pattern Based Integral Attack, M.R.Zaba et al., FSE 2008]

自動車のキーレス・エントリで実際に使われている 64 ビット・ブロック暗号 KeeLoq は、非線形 FSR を利用した設計で、既に攻撃法がいくつか発表されていたが、既知平文が 2^{32} 個も必要である点で現実的でなかった。スライド攻撃と代数攻撃を組み合わせることで、既知平文 2^{16} 個で解読できた。現実的な脅威につながる可能性が高まった。[Algebraic and Slide Attacks on KeeLoq, N.T.Courtois et al., FSE 2008]

非対称 Feistel 暗号に対する汎用の攻撃法として C.S.Jutla が CRYPTO 1998 で提案した一般化バースデイ攻撃があるが、Integral 攻撃の考え方を応用することでより効率の良い解読法が実現できた。[Generic Attacks on Unbalanced Feistel Schemes with Expanding Functions, J.Patarin, Asiacrypt 2007]

④ 公開鍵暗号の解読技術

SFLASH は、2003 年に NESSIE で選ばれた多変数２次連立方程式に基づくディジタル署名方式で、スマートカードのような低リソースの環境での利用に向いている。Eurocrypt 2007 で、SFLASHv2 のパラメータを変更すると攻撃できる公開鍵の差分を利用した攻撃法が発表され、更に CRYPTO2007 では更に極座標形式(polar form)を利用することで連立方程式の線形化を行い、SFLASHv2, SFLASHv3 共に破れることが示された。これらは A.Shamir 氏・J.Stern 氏およびその研究室からの示された一連の結果である。[Cryptanalysis of SFLASH with Slightly Modified Parameters, Vivien Dubois, Pierre-Alain Fouque and Jacques Stern, Eurocrypt 2007] [Practical Cryptanalysis of SFLASH, Vivien Dubois, Pierre-Alain Fouque, Adi Shamir and Jacques Stern, CRYPTO 2007]

数体篩法専用ハードウェアを作成し、ふるい部分の高速化を図ったハードウェア

を利用した解析にはTWIRL (a wafer-scale design) があるが、TWIRLに比べ2～3.5倍程度遅いが、メモリ量を削減していており TWIRL に比べ安価で構成可能な方法である。[Non-Wafer-Scale Sieving Hardware for the NFS: Another Attempt to Cope with 1024-bit, Willi Geiselmann and Rainer Steinwandt, Eurocrypt2007]

1039 ビットの合成数 $2^{1039}-1$ の素因数分解が特殊数体篩法(SNFS)を利用して実現された。既にこの合成数が 5080711 という素因数を持つことは分かっていたので、ここではこれで割った 1017 ビット数の素因数分解ができることを示した。また、本実験は遠隔地を結び分散処理を実施し得られた結果である。なお、特殊数体篩法は大部分の合成数に対して適用できないので、1024 ビット鍵の RSA 暗号の安全性が決定的に低下したというわけではない。[A Kilobit Special Number Field Sieve Factorization, Kazumaro Aoki, Jens Franke, Thorsten Kleinjung, Arjen K. Lenstra, and Dag Arne Osvik, Eurocrypt2007]

⑤ 暗号プロトコルの解読技術

メールなどの受信時の認証などとして用いられている、チャレンジレスポンス型で MD5 を利用したプロトコル APOP に関しての解析結果が示された。G.Leurent らはプロトコルの中で用いているパスワードについて 3 文字まで現実的な時間内で推定可能であることを示した。更に、佐々木らは Chosen Challenge attack の環境下では 31 文字のパスワードは容易に解読可能であること、また現実的な環境下では約 1 時間に 1 文字の解読に成功、31 時間で 31 文字のパスワードの解読が可能であることを示している。この攻撃手法を用いると理論的には 79 文字までは総当り攻撃よりも有効な解析が実行可能となることを示した。

[Message Freedom in MD4 and MD5 Collisions: Application to APOP, Gaetan Leurent, FSE 2007] [Extended APOP Password Recovery Attack, Yu Sasaki, Lei Wang, Kazuo Ohta and Noboru Kunihiro, FSE2007 Rump]

MD5 の衝突耐性の不備を利用して、X.509 に従った一対の署名が作れることを実例によって示した。2005 年の ACISP で Lenstra-Wagner らにより MD5 の脆弱性に起因する X.509 で異なる署名が作成できることは示されていたが、当初は(結果として)同じユーザ(ID)に対して異なる公開鍵を持つような署名の生成に留まっていた為、実質的な脅威はそれほど大きくなかったが、本結果では異なる ID に対する署名が生成できることから実質的な脅威につながる結果であるといえる。技術的には MD5 への攻撃がより強力になり意図する任意の 2 つの IHVs(Intermediate Hash Values)に対する衝突発見が可能になったためである。この署名対を作るのに要する計算量は MD5 の圧縮関数 2^{52} 回分であり、Eindhoven 技術大学のクラスター計算機と分散 PC(ボランティア 1200 名)を利用した HashClash プロジェクト(ピーク性能 400GFlops)で合計 6 カ月掛かった。MD5 の脆弱性を強く印象付ける結果である。[Chosen-prefix Collisions for MD5 and Colliding X.509 Certificates for Different Identities, Marc Stevens, Arjen Lenstra and Benne de Weger, Eurocrypt2007]

RFID のタグの認証に注目し、満たされるべき安全性の要求条件を提示し、8 つ安

全性レベルを定義し、それら定義間の帰着関係を示した(但し、タグ認証にのみ言及しており、リーダ認証は含まれていない)。ここ 2～3 年の間、RFID の認証関係の論文は数多く出ているが安全性に関してきちんと議論されているものはあまり多くない。本結果は、今後の RFID の認証方式を提案していく上でも一つの指標になると考えられる。[On Privacy Models for RFID, Serge Vaudenay, Asiacrypt2007]

⑥ その他

NIST の提唱している NIST SP 800-90 の楕円曲線を利用した random number generator に関する解析結果においては、楕円曲線上での DH 問題の困難性、2 つの新たな問題に対する困難性(x-アルゴリズム問題、truncated point problem) を満たすときは ECRNG(Elliptic curve random number generator)は安全であるとしている。truncated problem に関して、NIST が規定している範囲内でごく小さなビット数が truncate されている場合であっても、解けてしまうことがあることを示した。これは、ストリーム暗号に用いられているような場合その安全性を保障できない場合があることを意味する。一方、nonce としての使用や鍵生成などの場合には無害である。[A Security Analysis of the NIST SP 800-90 Elliptic Curve Random Number Generator, Daniel R.L. Brown and Kristian Gjøsteen, CRYPTO 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 19 年度は、現在広く利用されているセキュリティに関する標準技術について、安全に利用するための指針を示すため、新規にリストガイドワーキンググループを組織した。

リストガイド WG と公開鍵暗号 WG の平成 19 年度の主要活動項目は、表 4 の通りである。

表 4　平成 19 年度の主要活動項目

ワーキンググループ名	主査	主要活動項目
リストガイド WG	佐々木良一	① 技術対象となる標準技術についての調査・検討 ② 暗号アルゴリズムの選択についての検討 ③ セキュリティパラメータについての検討
公開鍵暗号 WG	太田和夫	① ST SP 800-56A に関する DH 及び ECDH の安全性についての調査・検討 ② SECG SEC1 及び ANS X9.62 に関する ECDSA の安全性についての調査・検討 ③ PSEC-KEM に関する安全性についての調査・検討

３．２．２．リストガイドワーキンググループ

（１）調査背景

電子政府システムにおいて、安全な暗号技術を利用することを目的に、総務省および経済産業省が共同で開催する暗号技術検討会のもと、電子政府推奨暗号リストが 2003 年 2 月 20 日に公表された。また、2003 年 2 月 28 日に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。

この電子政府推奨暗号リストは、安全性が確認された暗号アルゴリズムが列挙されている。一方、安全な電子政府システムを構築する際には、暗号アルゴリズムが組み合わされて使われているセキュリティの標準技術が調達の際の選択基準となる。そのため、構築する電子政府システムの安全性を確認するためには、暗号アルゴリズムの安全性とセキュリティの標準技術の関係を理解したうえで、推奨される標準技術を利用することが必要となる。

リストガイドワーキンググループでは、上記の課題を解決するために、電子政府推奨暗号リストガイド（以下「リストガイド」という。）を作成した。リストガイドは、電子政府で利用されている、あるいは利用する可能性のある暗号を利用したセキュリティ技術の安全性と暗号アルゴリズムの安全性の関係を示した上で、標準技術の中で選択することが望ましい暗号アルゴリズムとそのセキュリティパラメータを示したものである。

リストガイドの想定読者は、電子政府システムの調達者、およびシステム構築を行うベンダである。

システム調達者は、電子政府システムの調達を行う際に、その調達仕様の中にセキュリティに関する要件を盛り込む。調達に際し、システムベンダは提案書類の中に、暗号技術を用いたセキュリティ技術の利用を盛り込む。リストガイドは、システム調達者が提案されたセキュリティ技術が本当に安全であるかどうかを確認する際に参照する。

一方、システムベンダは、調達の際の安全性のガイドラインとして、本リストガイドの情報を参照して仕様の策定、および設計を行うことで、調達要件に沿った安全なシステム構築を容易に行うことができる。

（２）活動内容

リストガイドワーキンググループでは、電子政府で利用されている、あるいは利用する可能性のある暗号を利用したセキュリティ技術について、その技術概要と、推奨する利用方法を導出することを目的として、検討を行った。

【検討方針】

リストガイドにおいて、推奨される利用方法を選ぶ際の選択基準は以下の通りである。

・基本的な考え方として、使ってはいけない暗号技術を除外することを目標とする。
・標準規格の中に定められている暗号アルゴリズムの中に、電子政府推奨暗号リストに含まれる暗号アルゴリズムがある場合、当該アルゴリズムを推奨とする。
・標準規格の中で、特に暗号アルゴリズムが定められていない場合には、電子政府推奨暗号リストの暗号アルゴリズムを適用する。
・電子政府推奨暗号リストで注釈がついているアルゴリズムについては、標準規格の中で他に選択肢がない場合を除いては、リストガイド内では推奨しない。
・電子政府推奨暗号リストにない暗号技術（MAC など）については、標準で規定されている技術などで問題があるかどうかを確認する。
・セキュリティパラメータは、該当する利用方法に必要な保証期間を念頭に、過去の CRYPTREC レポートでの監視結果に基づいて選択する。
・公開鍵暗号の鍵長については、2048 ビット以上を基本とする。ただし、規格や実装上の制約により 2048 ビット以上の鍵長を利用することが困難であることが想定される場合には、必要な有効期間に応じて、注釈つきで短い鍵長について別途、記載をする。
・DSA については、2048 ビットの仕様が策定されつつあるが、ドラフト版であるため、参考として掲載している。仕様と評価が固まり次第、推奨とする。
・パディングの方式が複数定義されている暗号技術の場合、過去の CRYPTREC Report での安全性評価に従い、最も安全な方式について推奨とする。

【記述対象技術】

記述対象のセキュリティ技術は、

・認証技術
・PKI 関連技術
・通信路の暗号化技術
・蓄積データの暗号化技術
・改ざん検知、時刻認証技術
・鍵管理
・MAC、KDF

である。その中で、ISO、IEC、ITU、IETF、NIST などの標準化機関で定められた標準技術について記述を行っている。

【記述項目】

リストガイドには、電子政府システムで利用することが想定される、上記の標準的なセキュリティ技術について、

・技術の概要
・想定される脅威
・脅威に対する対策方針
・技術が備えるべき要件
・標準化動向
・技術の安全性と、暗号アルゴリズムの安全性の関係
・推奨される利用方法（暗号アルゴリズム、セキュリティパラメータ）

を記述している。

【推奨される利用方法】

① エンティティ認証

エンティティ認証においては、SSL、SSH のような相手認証の技術と、ワンタイムパスワード、認証付き鍵交換、公開鍵暗号や共通鍵暗号を用いる認証プロトコル、IC カードや TPM を利用した認証方式についての検討を行った。

SSL の証明書の認証においては、2048 ビット以上の電子署名アルゴリズム、鍵交換においても 2048 ビット以上の公開鍵技術（楕円の場合は 224 ビット以上）の利用、完全性の保証においては HMAC-SHA1、暗号通信においては AES、Camellia の 128 ビット以上を推奨とした。また、ハッシュ関数については SHA-1 が RFC で規定されているため、注釈つきで掲載している。SSH においても、SSL と同様の推奨アルゴリズムとした。

ワンタイムパスワードにおいては、ハッシュ関数を利用した技術を取り上げ、SHA-256/384/512 と CRYPTREC で例示した疑似乱数生成系を利用することを推奨した。

認証つき鍵交換については、共通鍵を用いる場合リスト掲載の 128 ビットブロック暗号と、CRYPTREC REPORT 2005 において安全性が確かめられた MAC を推奨とすることにした。公開鍵を用いる場合、2048 ビット以上の共通鍵技術（楕円の場合 192 ビット以上）、ハッシュ関数として SHA-256/384/512、MAC として CRYPTREC REPORT 2005 において安全性が確かめられた MAC を推奨とすることにした。

IC カードを利用した認証技術、共通鍵暗号、公開鍵暗号、MAC を利用した認証技術についても、同様の推奨とした。

② PKI

証明書の発行、CRL の発行、OCSP プロトコルについての検討を行った。

証明書の発行においては、SHA-256/384/512 と、2048 ビット以上の電子署名技術を推奨とした。また、CRL の発行、OCSP における電子署名も同様の推奨とした。

③ 通信路の暗号化

通信路における暗号化方式として、PIN の暗号化、SSL-VPN、IPsec-VPN、無線 LAN、鍵共有方式について検討を行った。

PIN の暗号化については、共通鍵暗号を用いる場合にはリストに掲載された 128 ビット以上のブロック暗号を、公開鍵アルゴリズムの場合には RSA-OAEO 2048 ビット以上を、MAC として CRYPTREC REPORT2005 において安全性が確かめられた MAC を推奨とすることにした。

SSL-VPN については、エンティティ認証における SSL と同様の推奨とした。IPsec-VPN については、IKE のための鍵共有においては 2048 ビット以上の鍵共有技術と 2048 ビット以上の電子署名技術、相手認証においては 2048 ビット以上の電子署名技術と 128 ビット以上の AES、Camellia、MAC として CRYPTREC REPORT2005 において安全性が確かめられた MAC を推奨とすることにした。

無線 LAN については、可能な限り WPA2 を利用すること、WEP を利用しないこととした。

鍵共有方式については、エンティティ認証における認証付き鍵交換と同様とした。

④ 蓄積データの暗号化

蓄積データの暗号化技術として、ファイル暗号化、DB の暗号化、OS による暗号化を対象に検討を行った。

ファイル暗号化では OpenPGP を対象として、乱数生成においてリストで例示されている疑似乱数生成系を、共通鍵暗号として AES128 ビット以上を、公開鍵暗号としては RFC4880 で規定されているため RSAES-PKCS-v1_5 2048 ビット以上を、ハッシュ関数として SHA-256/384/512 を、電子署名アルゴリズムにおいて RSASSA-PKCS-v1_5 あるいは DSA の 2048 ビット以上を掲載した。

DB による暗号化では Oracle における暗号化方式を例にとり、同様の暗号化方式を採用した場合にリストに掲載されている 128 ビット以上のブロック暗号を推奨とした。

OS による暗号化では、MS Windows 2000 以降に掲載されている EPS を例にとり、同様の暗号方式を採用した場合に、乱数生成としてリストで例示されている疑似乱数生成系を、共通鍵暗号としてリストに掲載されている 128 ビット以上のブロック暗号を、公開鍵暗号として RSA-OAEP 2048 ビット以上を、鍵共有として PSEC-KEM 224 ビット以上を、証明書向けハッシュ関数として SHA-256/384/512、電子署名アルゴリズムにおいて RSASSA-PKCS-v1_5、DSA の 2048 ビット以上、ECDSA 224 ビット以上を掲載した。

⑤ 改ざん検知・時刻保証

改ざん検知技術として、ハッシュ関数を用いた方法、MAC を用いた方法、電子署名を用いた方法、S/MIME、コード署名技術を、時刻保証技術として、電子署名を用いたタイムスタンプ方式について検討を行った。

ハッシュ関数を用いた改ざん検知では、SHA-256/384/512 を推奨とした。MAC を用いた方法では、CRYPTREC REPORT2005 において安全性が確かめられた MAC を推奨とした。電子署名を用いた方法では、RSASSA-PKCS-v1_5、DSA の 2048 ビット以上、ECDSA 224 ビット以上と SHA-256/384/512 ビットのハッシュ関数を掲載した。S/MIME においても、同様の推奨とした。コード署名技術においては、Microsoft 社の Authenticode、JAVA SDK のコード署名を対象に検討を行い、RSASSA-PKCS-v1_5、DSA の 2048 ビット以上、ECDSA 224 ビット以上と SHA-256/384/512 ビットのハッシュ関数を掲載した。

電子署名を用いたタイムスタンプ方式については、RSASSA-PKCS-v1_5、DSA の 2048 ビット以上、ECDSA 224 ビット以上と SHA-256/384/512 ビットのハッシュ関数を掲載した。

⑥ 鍵管理

暗号鍵管理に関する基本的な要件を示す。生成から破棄に至る暗号鍵のライフサイクルとその各段階における鍵管理上の機能と保護について、NIST SP800-57 Part1 および ISO 11568-1/2/4 を参考に記述した。また、利用場面における鍵管理を具体的に示すために、署名用途 PKI のプライベート鍵を例に、鍵ライフサイクル、鍵管理機能、保護対策の方針について検討を示した。

⑦ 暗号利用モード及び MAC（メッセージ認証コード）

現状の電子政府推奨暗号リストでは、暗号利用モード及び MAC に関する言及がないため、暗号利用モードに関しては、EBC、CBC、k-CFB、OFB、CTR の各モード、MAC に関しては、CBC-MAC、EMAC、XCBC、CMAC、HMAC の各 MAC について、その概要と安全性、性能などの評価を掲載した。

⑧ 鍵導出関数

現状の電子政府推奨暗号リストでは、暗号実装の評価に足る鍵導出関数に関する仕様の言及がないため、KDF 関数に関する概要、ハッシュ関数ベースの KDF、HAMC ベースの KDF 関数の概要と、安全性に関する評価を掲載した。評価結果としては、SHA-1/256/384/512 を利用する限り、NIST SP800-56A、ANS X9.42、SECG SEC1 で使用される KDF 関数の安全性が直ちに脅かされる状態でないことを掲載した。

３．２．３．公開鍵暗号ワーキンググループ

（１）調査背景

公開鍵暗号 WG の 2007 年度当初の活動目的は、NIST から提出されている Draft FIPS 186-3 に記載されている DSA について、1024 ビットより長い鍵サイズをサポートする変更部分を確認の上、その安全性について検討することであった。

その後、暗号モジュール試験及び認証制度（以下、「JCMVP」という。）の事務局から、

電子政府推奨暗号リスト記載の暗号技術と JCMVP において承認されたセキュリティ機能との間のいくつかの差異について JCMVP の要望を認めるよう検討依頼があったため、その調整が整うまで本 WG の開催を見合わせていた。

暗号技術検討会（2007 年 11 月 20 日開催、第 2 回）において、上述の要望等に対応して「電子政府推奨暗号の監視の具体的な内容」の一部修正が認められた。したがって、公開鍵暗号 WG では JCMVP の要請等に基づいて検討が必要となった暗号技術に関して、技術的な部分に限定して検討を実施した。

公開鍵暗号 WG が提出する結果に基づき、第 3 回暗号技術監視委員会及び第 3 回暗号技術検討会において、電子政府推奨暗号の仕様書の参照先の変更（追加を含む）及び仕様の変更が決定した。

（２）活動内容

公開鍵暗号ワーキンググループでは、暗号技術監視委員会及び暗号技術検討会において、検討対象の暗号技術における「仕様書の参照先の変更（追加を含む）または仕様書の変更」に関して、その妥当性を判断できる資料を作成するために、年度当初に計画された検討項目に優先して、次の各項目の安全性について調査・検討を行うこととした。

- （DH 及び ECDH に係る）鍵導出関数（KDF 関数、Key Derivation Function）
- （ECDSA 及び ECDH に係る）楕円曲線ドメインパラメータ（の生成・検証）
- （ISO/IEC 化に伴い生じた仕様変更に係る）PSEC-KEM

なお、NIST FIPS 186-2 (+ Change Notice 1)における DSA（鍵長が 1024 ビット）については、ANS X9.30:1-1997 と FIPS PUB 186-2 の仕様は基本的に同じであったが、FIPS PUB 186-2 は Change Notice 1 において鍵サイズ（1024 ビット未満は仕様外）と擬似乱数生成器に対して仕様変更があった。

擬似乱数生成系の問題点（DSAに関するBleichenbacherの指摘[1]）はCRYPTRECでは既に対応済みで、電子政府推奨暗号リストにおける例示において、指摘されていた問題点を有する擬似乱数生成器は除外されている[2]。このため、特に安全性には問題はないことが判明している。

よって、仕様書の参照先を変更する場合には、FIPS 186-2 (+ Change Notice 1)のみとするのは妥当であると考えられる。

① DH の安全性評価

現在の電子政府推奨暗号リストにおける DH の仕様参照先は ANS X9.42-2001 である。ANS X9.42 と NIST SP800-56A の間に存在する技術仕様上の主な差異は、

---

[1] r を160 ビットの乱数、q を160 ビットの素数としたときに, r mod q の分布が偏ることを利用したもの。

[2] CRYPTREC Report 2002 第 5 章 擬似乱数生成系の評価,
http://www2.nict.go.jp/y/y213/cryptrec_publicity/c02_report.pdf

（イ） 有限体ドメインパラメータについては、ANS X9.42 のものは、NIST SP800-56A に適合しない場合があるが、NIST SP800-56A のものは ANS X9.42 に適合する。

（ロ） KDF 関数について差異が存在する。どちらもハッシュ関数を使用する KDF 関数としては同じタイプに属するので、安全なハッシュ関数を使用すれば、安全性上問題はない。

（ハ） その他、DH のスキームの種類、公開鍵の検証、鍵配送手法、鍵確立プロセスについて、NIST SP800-56A の方がより強い制限を課している。

となっている。

よって、NIST SP800-56A について安全性上の問題はない。なお、ANS X9.42-2003 という改訂版が発行されており、スキーム自体には変更はないものの、素数生成に関連する補助関数の記述に微修正があるため、ANS X9.42-2001 は ANS X9.42-2003 に変更すべきである。

仕様の参照先を変更する場合には、KDF 関数に関する差異による相互接続性を考慮すれば、NIST SP 800-56A を参照先として追加することが妥当であると考えられる。

詳細は、CRYPTREC Report 2007 付録 3 を参照のこと。

② ECDSA の安全性評価

現在の電子政府推奨暗号リストにおける ECDSA の仕様参照先は SECG SEC 1 v1.0 である。SECG SEC 1 v1.0 と ANS X9.62-2005 の間に存在する技術仕様上の差異は、楕円曲線ドメインパラメータの選択方法にあり、以下が主なものです：

（イ） セキュリティレベル[3]の許容範囲：

ANS X9.62-2005はセキュリティレベルが80以上となっていて、SECG SEC 1 v1.0のようなセキュリティレベルが80未満のレベルは許容していない。

（ロ） 基礎体の標数が2の場合の、基礎体の基底を表す既約多項式の許容範囲：

SECG SEC 1 v1.0とANS X9.62-2005の間で、一方が許容するパラメータを他方が許容しない場合があるため、相互接続できない場合があり得る。

（ハ） コファクターの許容範囲：

ANS X9.62-2005はSECG SEC 1 v1.0よりも条件が緩和されているが、セキュリティレベルに依存して、ベースポイントの位数の下限が規定されているので、安全性が低下することはない。

[3] セキュリティレベルについては、ANS X9.62-2005 の 6.1 節及び SECG SEC 1 v1.0 の 3.1 節を参照のこと。

（ニ）　MOV条件

ANS X9.62-2005はSECG SEC 1 v1.0よりも条件が厳しくなっているので、安全性に問題はない。

（ホ）　擬似乱数生成器

SECG SEC 1 v1.0では、擬似乱数生成器について特に指定がない一方で、ANS X9.62-2005では、HMAC_DRBGというHMACベースの擬似乱数生成器が承認されたものとして利用できる。これは、JCMVPにおいて2007年度中に評価されており、安全性に問題はない。

したがって、（イ）～（ホ）の違いから、SECG SEC 1 Ver.1.0 と ANS X9.62-2005 のどちらを認証基準にするにしても、他方が認証されないことがあり得るので、仕様書の参照先を変更する場合には、ANS X9.62-2005 を追加するのが妥当であると考えられる。

詳細は、CRYPTREC Report 2007 付録 3 を参照のこと。

③ ECDH の安全性評価

現在の電子政府推奨暗号リストにおける ECDH の仕様参照先は SEC 1 Ver.1.0 である。SEC 1 Ver.1.0 と NIST SP800-56A の間に存在する技術仕様上の主な差異は、

（イ）　楕円曲線ドメインパラメータについて差異が存在する。安全性上の問題点はないものの、相互接続性に支障をきたす可能性がある。

（ロ）　KDF 関数について差異が存在する。どちらもハッシュ関数を使用する KDF 関数としては同じタイプに属するので、安全なハッシュ関数を使用すれば、安全性上問題はない。

（ハ）　security level、擬似乱数生成器、standard なプリミティブの使用について、NIST SP800-56A の方がより強い制限を課している。

また、NIST SP800-56A では key を次のように static key と ephemeral key とに区別している。

- ephemeral key : トランザクション毎に変えること(を通常とする)key
- static key : 鍵交換のエンティティや秘密鍵のオーナーの Identifier と結び付いた key であり、ephemeral key より長寿命な key

（ニ）　NIST SP800-56A に規定されている 5 種類のスキームのうち、ephemeral key のみを使う最も構造の単純なスキームが、SECG SEC 1-v1.0 のスキーム(それにより強い制限を課したもの)に相当する。NIST SP800-56A のその他 4 種類のスキームは、static key の使用を伴うスキームである。

したがって、NIST SP800-56Aのephemeral key のみを使うスキームC(2,0,ECC CDH)[4]はSECG SEC 1 v1.0 のスキームに相当し、安全性上の問題はないものの、NIST SP800-56Aのstatic keyを使う残りの 4 種類のECDHスキームについては、SECG SEC 1 v1.0 で規定されているスキームの範囲を超えており、仕様書の参照先の変更先として結論付けるにはさらなる検討が必要であると考えられる。

詳細は、CRYPTREC Report 2007 付録 3 を参照のこと。

④ PSEC-KEM の安全性評価

現在の電子政府推奨暗号リストにおける仕様参照先は、2002 年度までに提案者から応募された提出書類に基づくものである[5]。

過去のCRYPTREC ReportにおいてPSEC-KEMは、「KEM 技術に関する証明可能安全性がランダムオラクルモデルのもとで楕円曲線DH計算問題に帰着されるように示されている。したがって、KEM(Key Encapsulation Mechanism)-DEM(Data Encapsulation Mechanism)構成に利用することは安全である。」と評価されている。

ISO/IEC 18033-2の審議過程において、エディタ並びに各国からのコメント等を吸収する形で、提案された仕様に一部修正が加えられ、最終的に規格化されたものが電子政府推奨暗号リスト策定時のものと若干異なるものとなってしまった。そこで仕様書の変更の妥当性を判断できる資料を作成するために今年度評価が行われた。評価に当たっては、提案者に新たに資料の提出を求めた。

一部仕様変更により、証明可能安全性において証明の見直しが必要となるものの、ISO/IEC 18033-2:2006 の仕様そのままではなく、楕円曲線上の群に限定して議論することで、従来と同様の安全性を示すことができる。現仕様と比べて、安全性評価結果の帰着効率が 2 倍程度低下するが、安全性への影響は小さいといえる。

よって、ISO/IEC 18033-2:2006 における PSEC-KEM については楕円曲線上の群に限定することで安全性上の問題はないと考えられ、仕様の変更についても問題はない。

詳細は、CRYPTREC Report 2007 付録 3 を参照のこと。

（３）まとめ

以上の検討結果により、電子政府推奨暗号リストに記載された一部の暗号技術において、仕様の変更、仕様書の参照先の変更または追加として修正情報を周知すべき内容は、以下の表 5 の通りである。

---

[4] C については、NIST SP 800-56A の 6 節、Table 4 及び Table 5 (p.51)を参照のこと。

[5] PSEC-KEM 仕様書(2002 年 5 月 14 日)
http://cryptrec.nict.go.jp/cryptrec_03_spec_cypherlist_files/PDF/02_02jspec.pdf

表 5　2007 年度修正情報を周知すべき内容

暗号技術名	仕様参照先（修正前）	仕様参照先（修正後）[6]	事由
DSA	ANS X9.30:1-1997	NIST FIPS PUB 186-2 (+ Change Notice 1)	本報告書 5.3.2 節(3)の⑥、仕様の参照先の変更
DH	ANS X9.42-2001	ANS X9.42-2003 及び NIST SP 800-56A	本報告書 5.3.2 節(3)の⑥、仕様の参照先の追加
ECDH	SECG SEC 1 v1.0	SECG SEC 1 v1.0 及び NIST SP 800-56A の C(2,0,ECC CDH)が定めるスキーム	本報告書 5.3.2 節(3)の⑥、仕様の参照先の追加
ECDSA	SECG SEC 1 v1.0	SECG SEC 1 v1.0 及び ANS X9.62-2005	本報告書 5.3.2 節(3)の⑥、仕様の参照先の追加
PSEC-KEM	PSEC-KEM 仕様書 2002 年 5 月 14 日版 (公募時の応募書類)	PSEC-KEM 仕様書 2008 年 1 月 18 日版※	本報告書 5.3.2 節(3)の④、仕様の変更

[6] http://www.cryptrec.go.jp/method.html を参照のこと。

※　事務局注）第 3 回暗号技術検討会開催後、主に型変換関数に関する修正等が施された仕様書の再提出があった（2008 年 4 月 14 日）。当該修正等は安全性には影響がないものと判断されたことから（2008 年 4 月 30 日、暗号技術監視委員会）、最終的に、本修正版（2008 年 4 月 14 日版）が仕様参照先として適当であると承認された（2008 年 6 月 10 日、暗号技術検討会）。

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、(1)については北米の FIPS と国際標準 ISO/IEC に関する暗号モジュールのセキュリティ要件及び試験要件を調査し、標準化のためのコメントの検討を行っている。また、(2)の一環としては、INSTAC-8 仕様及び 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会の下に設けた。2007 年度には、産業技術総合研究所と東北大学が開発した新たな暗号モジュールへのサイドチャネル攻撃実験を目的として新たに開発したサイドチャネル攻撃実験用標準評価ボード(SASEBO)を電力解析実験ワーキンググループの委員に配布し、実験結果の収集を行った。またボード間の個体差による実験結果の差異の発生の有無についても確認を行った。

４．１．２．暗号モジュール委員会の開催状況

2007 年度の暗号モジュール委員会は、計 4 回開催された。各回会合の概要は表 6 のとおりである。

表 6　2007 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 19 年 6 月 6 日 10:00～12:00	暗号モジュール委員会規程について 委員長互選 ISO/IEC JTC1/SC27/WG3 のロシア会合報告 平成 19 年度暗号モジュール委員会活動計画（案）について ISO/IEC FDC 24759 の審議について CMVP 運用ガイダンス改定版の事務局による翻訳について
第 2 回	平成 19 年 7 月 25 日 14:00～16:00	ISO/IEC FDC 24759 の審議 NITS FIPS 140-3 のドラフトに関する審議

		運用ガイダンス改定の審議について 第１回電力解析実験ワーキンググループの開催報告
第３回	平成 19 年 9 月 28 日 10:00～18:00	NIST FIPS 140-3 ドラフトのコメント審議 （INSTAC:耐タンパー委員会と合同で開催）
第４回	平成 20 年 2 月 15 日 10:00～12:00	ISO/IEC 24759 FDIS の報告 CMVP 運用ガイダンス改定版の事務局による翻訳版の報告 2007 年度電力解析実験ワーキンググループの活動報告 CRYPTREC Report 2007(案)について 2008 年度の活動(案)について

４．２．活動内容と成果概要

４．２．１．　北米における暗号モジュールセキュリティ要件関連の調査

(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。

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 2008 年 3 月時点での最新版となっているが、Annex A は MOD の部分が 2007 年 12 月 18 日に GCM と GCD が追加され、Annex B は 2007 年 7 月 14 日に変更され、単一レベル OS に対する PP が追加となり、Annex C は 2007 年 10 月 18 日に SP800-90 の RNG の部分が追加となり、Annex D は IG（運用ガイダンス）の更新により 2008 年 1 月 16 日に更新されている。

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 FIPS 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 2008 年３月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[7]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[8]、試験者が実施しなければならない試験手順[9]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、2008 年 2 月 7 日の改訂版[10]が 2008 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) FIPS 140-2 の FIPS 140-3 への改訂

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 年目の見直しとして、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[11]、2005 年 9 月に物理セキュリ

---

[7] 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。
[8] Vender Evidence (VE と略す)
[9] Tester Evidence (TE と略す)
[10] 日本語版も 2008 年 1 月 24 日の改訂版が 2008 年 3 月時点での最新版となっている。
[11] CMVP 2004 Symposium: http://csrc.nist.gov/cryptval/cmvp2004/

ティ試験のワークショップ[12]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。1st Draft は 2006 年 11 月末にコメント募集用に公開される予定であったが、2007 年 9 月に公開となった。

①FIPS 140-3 の概要

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 章から構成される。EMI[13]に関する章は削除された。FSM[14]はデザインアシュアランス（設計保証）の章に入れた。
- ソフトウエアセキュリティとnon-invasive attack [15]（非破壊攻撃）の新たな章（分野）が増えた。
- ソフトウエ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、セキュリレベル 3 から 5 までのレベルで要求される。但し、要求内容は FIPS 140-2 レベルであり、DTR で更に詳細に記述される予定である。

②FIPS 140-3 への改訂スケジュールについて

現在、FIPS 140-3 への改訂スケジュールは次のように公開されている。

- 2007 年 3 月 31 日　Draft について、CMVP 内部(NIST＋CSE)でレビューが完了。
- 2007 年 7 月 13 日　1st Draft を開示。90 日間のコメント募集期間を設ける。
- 2007 年 10 月 12 日　1st Draft に対するコメント募集の〆切。
- 2008 年 3 月 18 日　FIPS 140-3 Software Security Workshop を開催。
- 2008 年 第 2 四半期　2nd Draft のためのパブリックコメントの募集を開始（変更の可能性有り）。
- 2008 年 第 4 四半期　米国商務省による承認（変更の可能性有り）。
- 2008 年 その後 6 ヶ月　DTR が発行される。FIPS 140-3 の試験の受け入れ開始。FIPS 140-2 も試験の受け入れは継続される。
- 2008 年 その後 6 ヶ月　FIPS 140-2 の試験の受け入れを終了。

---

[12] Physical Security Testing Workshop: http://csrc.nist.gov/cryptval/physec/physecdoc.html
[13] EMI: Electro Magnetic Interference 電磁妨害
[14] 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。
[15] 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。

４．２．２．ISO/IECにおける暗号モジュールセキュリティ要件関連の調査

(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)との関係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となる。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た。2007年5月のロシア会合においてFCDに進み、その後FCD投票が行われた。2008年3月現在ではFDISが公開されている。

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の整合性を保ちつつ反映させる必要がある。

４．２．３．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 24795が作成中であり、第2回暗号モジュール委員会にてFDISのドキュメントに対するコメントを作成し、8月27日開催のSC 27の国内委員会に委員経由で提出した。

コメントの内容としては、FDISのドキュメントということでエディトリアルな記述のミスや参照先の誤った記述に関する修正を指摘する部分が多かったが、6.8.1章のAS07.08のRandom bit generatorsにおいてRBG (Random bit generators) とその動作

モードについて、AS07.10、VB07.08.01、TE07.08.01、TE07.08.02 で「ISO/IEC 18031 準拠」するということになっており、正しく記述がされていないため、この部分は「承認されたものを使用する」に変更を依頼した。また、FDIS が 12 月に開示されたため、2 月の第 4 回暗号モジュール委員会では 3 月の ISO/IEC JTC 1/SC 27 国内委員会での FDIS 投票の検討のためのコメントを依頼した。

４．２．４．FIPS 140-3 の 1st Draft に対するコメント作成

当初、FIPS 140-3 の 1st Draft は 2006 年 11 月末にコメント募集用に公開される予定であったが、2007 年 7 月に公開となったため、暗号モジュール委員会と INSTAC 耐タンパー性標準化調査委員会 WG1 では 9 月 28 日に第 3 回暗号モジュール委員会を合同で開催し、1st Draft の検討を行い、コメント案の作成を行い 10 月 11 日に NIST に提出した。

コメントの要点は各セキュリティレベルにおける要求事項として 4.6 章および 4.7 章で示されている部分の要求事項がその通りで良いかどうかで、セキュリティレベルによる要件の変更を提案した。

・レベル 3 ではDPA[16]とSEMA[17]を追加。

・レベル 4 ではDPAとSEMA、DEMA[18]更にFIA[19]を追加。

・レベル 5 では FIA を追加。

またレベル 3 と 4 では主要な攻撃に耐性を持つこととし、レベル 5 では一通りの攻撃に対して更なる耐性を持つ必要があることとするよう依頼した。

４．３．電力解析実験ワーキンググループの活動

４．３．１．電力解析実験ワーキンググループの活動目的と経緯

暗号モジュール、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[20]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た。2006 年度には、今まで独

---

[16] DPA：(Differential Power Analysis) 差分電力解析。
[17] SEMA：(Simple Electro Magnetic Analysis) 単純電磁波解析。
[18] DEMA：(Differential Electro Magnetic Analysis) 差分電磁波解析。
[19] FIA：(Fault Induction Analysis) 故障利用解析。
[20] SPA：(Simple Power Analysis) 単純電力解析。

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会の下に設けた。

４．３．２．電力解析実験ワーキンググループの開催状況

2007 年度の電力解析実験ワーキンググループは、計 4 回開催された。各回会合の概要は表 7 のとおりである。

表 7　2007 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 19 年 6 月 27 日 14:00～16:00	電力解析実験ワーキンググループ活動計画(案) について 実験の目的と実験手順について 新たな標準評価ボードについて
第 2 回	平成 19 年 10 月 5 日 14:00～16:00	SASEBO ボードの配布と実験状況について 横浜国立大学による SASEBO ボードの個体差の確認実験結果の報告
第 3 回	平成 19 年 12 月 21 日 12:00～14:00	試験機関のための試験手順および試験機材の検討 SASEBO ボード等に関する実験の報告等
第 4 回	平成 20 年 2 月 6 日 14:00～16:00	2007 年度電力解析実験ワーキンググループの活動のまとめと報告書の作成について 電力解析攻撃実験のための評価ボードを用いたサイドチャネル攻撃の研究発表論文のまとめ 2008 年度の活動(案)について

４．３．３．電力解析実験ワーキンググループの成果概要

(1)　横浜国立大学によるサイドチャネル攻撃実験用標準評価ボードの検査

産業総合技術研究所 情報セキュリティ研究センター（RCIS）と東北大学大学院 情報科学研究科による、暗号モジュールへのサイドチャネル攻撃実験を目的として新たに開発したサイドチャネル攻撃実験用標準評価ボード（SASEBO）をワーキンググループ委員等に配布することを前提として、東北大学大学院 情報科学研究科にて作成された暗号アルゴリズムを搭載し作成したボード 80 セット全数について、横浜国立大学にて動作特性の差異に関する実験調査を行い、その結果の報告が行われた。

実験用標準評価ボードに個体差が有り、ある実験結果が他のボードでは再現されないという状況が起きるのではないかという疑問が有った。そのため横浜国立大学において、今回作成された産業技術総合研究所開発のボードのうち、第 1 次配布予定の 30 枚について調査を行った結果、測定した電力波形には差異があり、大きく 4 グループに分類されるが、FPGA の特性による差異はほとんど存在せず、FPGA の Vcc 及び GND に直列に挿入されているシャント用抵抗の交流特性の影響の方が大きい様であった。

ワーキンググループでは、ボードの個体差について FPGA の影響は無く、シャント用抵抗のロットの個体差が影響していると結論付けた。

(2)　サイドチャネル攻撃用標準評価ボードの配布

2007 年 9 月にサイドチャネル攻撃実験用標準評価ボード（SASEBO：Side-Channel Attack Standard Evaluation Board）とそれに用いる、暗号アルゴリズム（AES,Camellia,DES,Misty1）のソースコードを電力解析実験ワーキンググループの委

員に配布した。

SASEBO は経済産業省の委託事業「暗号モジュールの実装攻撃の評価に関する調査研究」の中で産業技術総合研究所と東北大学が開発した。

また、SASEBO で用いる暗号アルゴリズムのソースコードは東北大学と産業技術総合研究所情報セキュリティ研究センターにより共同開発されたものである。

このボードは、FPGA を搭載し、各種暗号アルゴリズム及びサイドチャネル攻撃へのカウンターメジャー機能を有する暗号アルゴリズムの搭載を可能とし、暗号ハードウェアの消費電力や放射電磁波の高精度な測定を可能とするものである。

(3) 電力解析攻撃研究会の開催

暗号を安全に使用するために、サイドチャネル攻撃を考慮せざるを得なくなってきている。また、米国標準技術研究所（NIST）で改訂作業中の暗号モジュールに対するセキュリティ要件第三版（FIPS 140-3）でも、サイドチャネル攻撃に対する要件を盛り込む方向で検討が進んでいる。サイドチャネル攻撃の中でも電力解析攻撃は、痕跡を残さずに暗号モジュール内の鍵情報を入手できる可能性が高いため、十分な対策を施す必要がある。そこで、CRYPTREC 暗号モジュール委員会と電力解析実験ワーキンググループでは、電力解析攻撃、タイミング攻撃を提案した米 Cryptography Research Inc.の Paul Kocher 氏を招いて、電力解析攻撃研究会を開催し、電力解析攻撃の現状を紹介するとともに、意見交換を実施した。

開催日時　2008 年 1 月 18 日（金）　10:00～12:00
開催場所　独立行政法人　情報処理推進機構　15 階委員会室１，２
講演者　Cryptography Research Inc. Paul Kocher 氏
講演題目　Part Ⅰ：Countermeasure Design & Validation Strategies for Power Analysis & related Attacks
Part Ⅱ：Complexity, Security, and the Future

(4) 電力解析攻撃実験のための評価ボードを利用した研究成果

電力解析実験ワーキンググループの委員による、INSTACにおける耐タンパー性標準化調査研究委員会の活動成果であるサイドチャネル攻撃耐性評価用標準プラットフォーム仕様INSTAC-8/-32 準拠プラットフォーム（INSTAC-8[21], INSTAC-32[22]）、産業技術総合研究所 情報セキュリティ研究センター（RCIS）と東北大学大学院 情報科学研究科による、暗号モジュールへのサイドチャネル攻撃実験を目的として新たに開発したサイドチャネル攻撃実験用標準評価ボード（SASEBO[23]）等を使用した 2007 年度の発表についてまとめた。

---

[21] INSTAC-8:サイドチャネル攻撃耐性評価用標準プラットフォーム仕様 INSTAC-8/32 準拠プラットフォーム（8bit 版）
[22] INSTAC-32：サイドチャネル攻撃耐性評価用標準プラットフォーム仕様 INSTAC-8/32 準拠プラットフォーム（32bit 版）
[23] SASEBO: サイドチャネル攻撃実験用標準評価ボード

表 8　評価ボードを使用した発表論文リスト

	タイトル	学会名・会議名	発表年月日	著者	使用ボード種類
1	DPA Using Phase-Based Waveform Matching against Random-Delay Countermeasure	ISCAS 2007[24]	2007/5/29	S. Nagashima, N. Homma, Y. Imai, T. Aoki, and A. Satoh	INSTAC-8
2	SPA Against an FPGA-Based RSA Implementation with a High-Radix Montgomery Multiplier	ISCAS 2007	2007/5/29	A. Miyamoto, N. Homma, T. Aoki, and A. Satoh	INSTAC-8
3	波形フィルタリングによる暗号モジュールへの高精度電力解析	DICOMO2007[25]	2007/7/6	長嶋聖、本間尚文、菅原健、青木孝文(東北大学 大学院情報科学研究科)、佐藤証（産業技術総合研究所）	INSTAC-8
4	特定入力パターンを用いた RSA 暗号ハードウェアの単純電力解析	DICOMO2007	2007/7/6	宮本篤志、本間尚文、青木孝文(東北大学 大学院情報科学研究科)、佐藤証（産業技術総合研究所）	INSTAC-8
5	サイドチャネル攻撃標準評価 FPGA ボードを用いた暗号ハードウェアに対する電力解析実験	DICOMO2007	2007/7/6	菅原健、本間尚文、青木孝文(東北大学 大学院情報科学研究科)、佐藤証（産業技術総合研究所）	INSTAC-32 SASEBO
6	ハードウェア実装された XOR 演算部に対する DPA 手法	FIT2007[26]	2007/9/7	辻洋平、岩井啓輔、黒川恭一（防衛大学校）	INSTAC-32
7	電力解析攻撃実験用ボードの個体差評価について	CSS2007[27]	2007/10/31	高橋 芳夫(横浜国立大学、(株)NTT データ)、 鳥越 慎、石和田 大気、渡部 良太、松本 勉(横浜国立大学)	SASEBO
8.	RSA暗号に対する平文選択型SPAの実験的評価	CSS2007	2007/11/2	宮本篤志、本間尚文、青木孝文（東北大学)、佐藤証（産業技術総合研究所）	SASEBO
9	AES のテーブルネットワーク型 FPGA 実装における耐電力解析テーブル設計法	ISEC[28]	2007/12/19	鳥越　慎、高橋芳夫、松本　勉（横国大）	SASEBO
10	ハードウェア実装された AES 暗号の XOR 演算部に対する DPA 検証	ISEC	2007/12/19	辻洋平、岩井啓輔、黒川恭一（防衛大学校）	SASEBO
11	RSA 暗号に対する平文選択型電力解析攻撃の検討	SCIS2008[29]	2008/1/22	本間尚文（東北大学)、宮本篤志（東北大学)，青木孝文（東北大学)、佐藤証（産業技術総合研究所）	SASEBO
12	INSTAC-32 準拠ボードにおける CPU に対する電力解析／電磁波解析比較	SCIS2008	2008/1/22	庄司 陽彦（株式会社 ワイ・デー・ケー)、野澤 晃（株式会社 ワイ・デー・ケー)、木村 隆幸（株式会社 ワイ・デー・ケー)、久門 亨（日本電気株式会社)、山下 哲孝（日本電気株式会社)、角尾 幸保（日本電気株式会社）	INSTAC-32
13	サイドチャネル攻撃標準評価ボードを用いた電力および電磁波解析実験	SCIS2008	2008/1/22	福永利徳（NTT 情報流通プラットフォーム研究所)、高橋順子（NTT 情報流通プラットフォーム研究所)、山越公洋（NTT マイクロシステムインテグレーション研究所)、瀬賀研二（長岡技術科学大学）	SASEBO
14	高分解能プローブの試作による電磁界解析実験	SCIS2008	2008/1/22	三宅 秀享（株式会社東芝 研究開発センター)、藤崎 浩一（株式会	SASEBO

[24] ISCAS： International Symposium on Circuits and Systems (The Institute of Electrical and Electronics Engineers, Inc.)
[25] DICOMO：マルチメディア，分散，協調とモバイルシンポジウム（情報処理学会）
[26] FIT:情報科学技術フォーラム（情報処理学会，電子情報通信学会）
[27] 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）
[28] ISEC：情報セキュリティ研究会（電子情報通信学会）
[29] 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）

				社東芝 研究開発センター)、清水 秀夫（株式会社東芝 研究開発センター)、新保 淳（株式会社東芝 研究開発センター）	
15	FPGA に対する電磁界解析実験	SCIS2008	2008/1/22	藤崎　浩一（東芝　研究開発センター)、三宅 秀享（東芝　研究開発センター)、清水秀夫（東芝　研究開発センター）	SASEBO INSTAC-32 S3E[30]
16	テーブルネットワーク型 AES 実装の新手法の提案	SCIS2008	2008/1/23	山口　晃由（三菱電機株式会社情報技術総合研究所)、品川　宗介（三菱電機エンジニアリング株式会社　鎌倉事業所)、佐藤　恒夫（三菱電機株式会社　情報技術総合研究所）	INSTAC-8
17	RSL 技術を用いた耐 DPA 暗号 LSI の設計手法- スタンダードセルによる RSL の実現と AES 回路への適用-	SCIS2008	2008/1/23	鈴木　大輔（三菱電機株式会社)、佐伯　稔（三菱電機株式会社)、佐藤　証（独立行政法人産業技術総合研究所）	SASEBO
18	RSL 技術を用いた耐 DPA 暗号 LSI の設計手法 - 設計段階における事前 DPA 評価-	SCIS2008	2008/1/23	佐伯　稔（三菱電機株式会社)、鈴木　大輔（三菱電機株式会社)、佐藤　証（独立行政法人産業技術総合研究所）	SASEBO
19	バンドパスフィルタを用いた高精度な差分サイドチャネル解析	ISEC	2008/2/29	久門　亨、山下哲孝、洲崎智保、角尾幸保（NEC)、庄司陽彦、野澤晃、木村隆幸（YDK）	INSTAC-32
20	暗号モジュールへの信号ラインからのサイドチャネル攻撃　～ FPGA 実装 AES における実験例 ～	ISEC	2008/2/29	渡部良太、鳥越　慎、高橋芳夫、松本　勉（横国大）	SASEBO
21	サイドチャネル攻撃標準評価ボード(SASEBO)を使った AES 暗号の実装評価実験	情報処理学会第 70 回全国大会	2008/3/15	南崎大作,岩井啓輔,黒川恭一（防衛大学校）	SASEBO

[30] S3E：Spartan 3E starter kit

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、2008 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、利用者側から見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

① 暗号アルゴリズム等を主な対象とする調査・検討

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

② 暗号実装関連技術を主な対象とする調査・検討

実装攻撃等の暗号実装関連技術を主な対象とする調査及び検討を行う。

（３）電子政府推奨暗号リストの改訂に関する調査・検討

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、2008 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「暗号技術調査ワーキンググループ」及び暗号モジュール委員会の下に設置される「電力解析実験ワーキンググループ」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の活動内容

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

① 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。

② 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。

③ 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。

2008 年度、監視委員会では、2007 年度に設置した調査 WG（リストガイド）の活動を継続し、未掲載な暗号技術に関して調査・検討し、リストガイドのアップデートを行うことを計画している。

また、電子政府推奨暗号リストの改訂に関しては、仮に公募を実施する場合には、リスト項目（カテゴリ）の見直し、評価基準、評価方法等を調査・検討した上で、新しい暗号の選定のための公募要領等の作成が求められるので、これに則した調査・検討を早急に開始することが必要である。

なお、リスト項目（カテゴリ）の見直しにおいて、リスト項目（カテゴリ）に位置付けられなかった、現在発展途上の新しい暗号技術についても、今後、実用性に加え、公平な評価基準や評価手法等の枠組みの整備がどの程度可能であるのか等の関連する調査研究を行うことが望ましい。

また、内閣官房情報セキュリティセンター（NISC）において作成された、「政府機関の情報システムにおいて使用されている暗号アルゴリズム SHA-1 及び RSA1024 に係る移行指針」（案）においても、政府統一的な移行指針が固まりつつあることに鑑み、電子政府推奨暗号についても、暗号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早急に進めることが期待される。

５．２．２．暗号モジュール委員会の活動内容

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・実験・検討等を行う。

（１）暗号モジュール委員会

暗号モジュールの国際規格等の標準規格を検討すると共に、電力解析実験ワーキンググループに調査および実験を依頼し、その検討結果に基づき、規格への反映を行い、電子政府推奨暗号の安全性および信頼性を確保する。

（２）電力解析実験ワーキンググループ

暗号モジュールの安全性および信頼性の主たる根拠となる、電力解析攻撃や電磁波解析攻撃を中心とするサイドチャネル攻撃の脅威とその対策等に関する暗号実装関連技術等の調査及び実験を行い、その活動結果を暗号モジュール委員会に提示する。

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な考え方

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

監視は、以下のような考え方に基づいて実施することとする。

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

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

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

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

（３）電子政府推奨暗号に関する修正情報の周知

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

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

③ 監視委員会は応募暗号[31]以外の電子政府推奨暗号が実運用環境上において攻撃により破られる可能性が高いとは判断していないにも関わらず、当該暗号に関する修正情報が仕様書の管理者により発行された場合であって（パラメータ修正等の簡易な修正に限る）、監視委員会が当該修正情報を加味した上で安全性評価を実施し、安全性が確保されていると判断する場合には当該修正情報を周知する。

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

---

[31] 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

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

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

（４）電子政府推奨暗号の追加

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

② 電子政府推奨暗号リストに掲載されていない暗号が国際的に高い評価を得ている場合であって、検討会が当該暗号を新たに評価することが必要と判断し、かつ、評価の結果、検討会が当該暗号を電子政府推奨暗号リストへ掲載することが適切と判断する場合には、当該暗号を電子政府推奨暗号リストへ追加する。

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

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

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。

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

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

③ 応募暗号については、原則として応募元から情報提供を受ける。

④ その他、一般からの情報提供も受ける。

（２）監視委員会における情報分析

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

（３）監視委員会及び検討会における審議及び決定

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

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

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

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

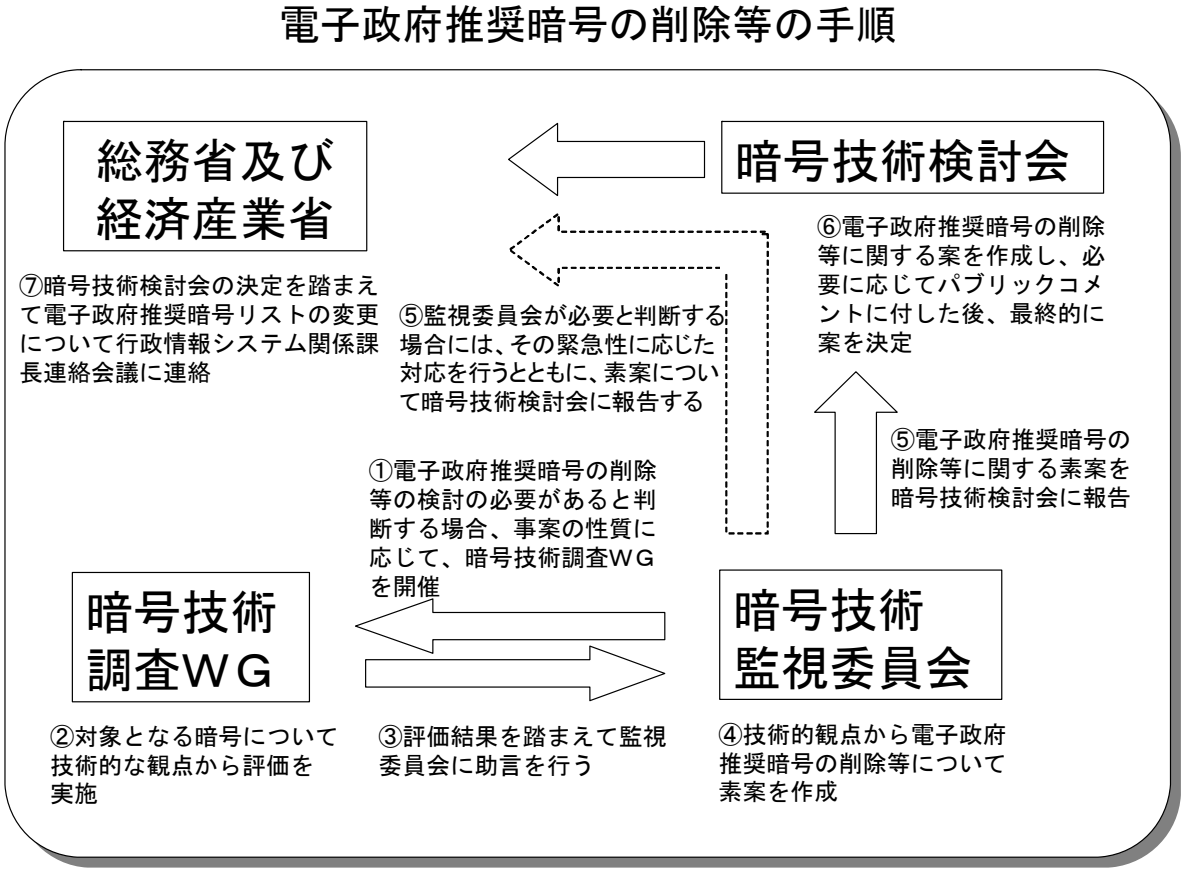

図2　電子政府推奨暗号削除等の手順

５．４　電子政府推奨暗号リストの見直し

５．４．１　見直しの目的

今回の電子政府推奨暗号リストの改訂においては、第一に、電子政府において暗号技術を利用する際に安全な暗号技術を選択する指針を与え、第二に、暗号を利用した技術を、システムのセキュリティ要件に合わせて正しく組み込むことを目的とする。さらに民間での利用を促進し、暗号技術の利用の啓発を進めるための方策を講じる。

このため、暗号リストの見直しにあたっては、全体の構成を見直すとともに、現在の電子政府推奨暗号リストに掲載されている暗号技術の見直し及びリストに新たに掲載する暗号技術の公募を行うこととする。

５．４．２　構成の見直し

現時点で CRYPTREC が公開している推奨暗号リストは「電子政府推奨暗号リスト」のみであるが、今回の見直しに合わせて、下記の各リスト及びリストガイドをまとめて「CRYPTREC 暗号リスト（仮称）」として公開する。これらの資料は、内閣官房情報セキュリティセンターの政府機関統一基準等において参照されることを想定している。

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

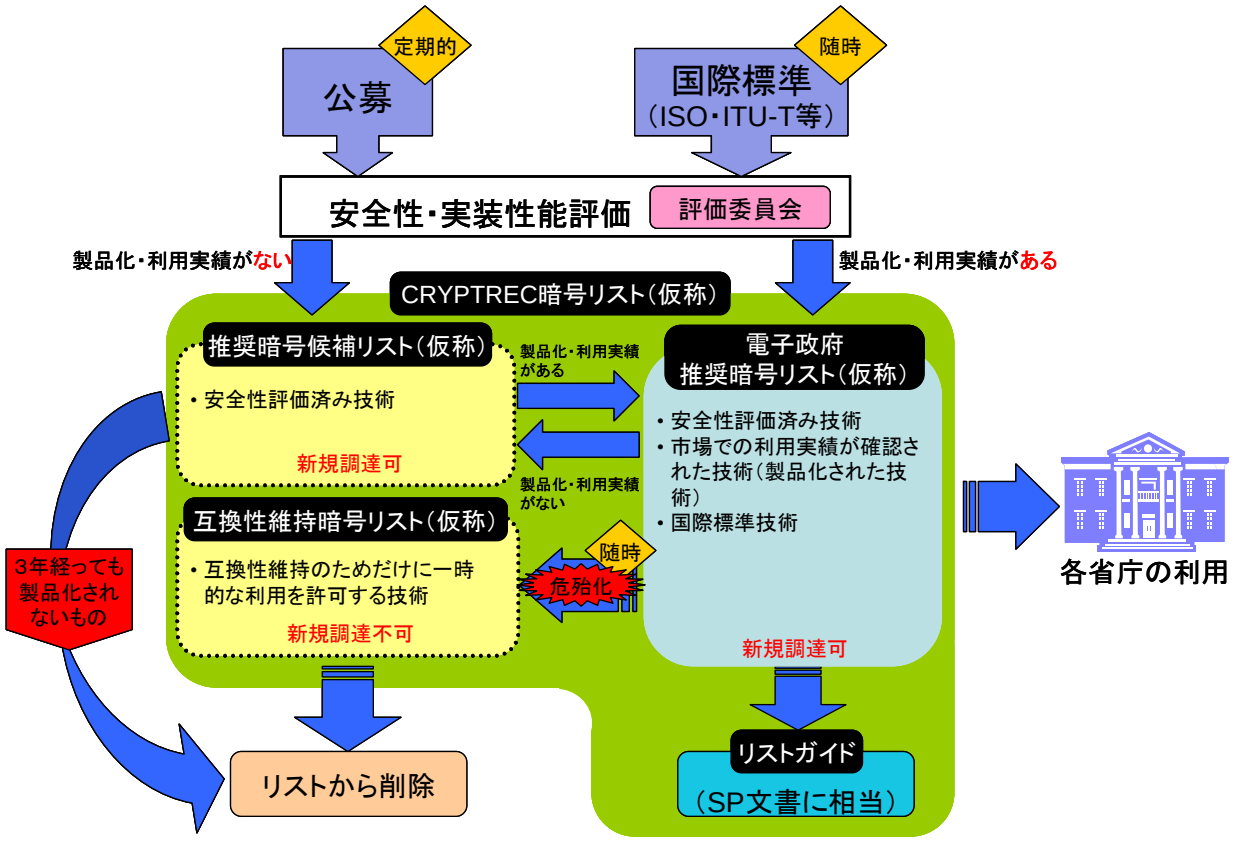

図 3 CRYPTREC 暗号リストの全体像

５．４．３ CRYPTREC 暗号リストの内容

（１）電子政府推奨暗号リスト

電子政府システムにおいて利用すべき暗号を示すものである。十分な安全性を持ち、実装性能が優れ、利用実績が十分にある暗号により構成される。

電子政府推奨暗号リストに掲載されるためには、推奨暗号候補リストに掲載されるための評価に加え、さらに利用実績が十分と判断される必要がある。また、WTO/TBT 協定を配慮し、国際標準であり、国際的な相互接続性を確保するために必要である暗号技術については安全性評価を行い、その性能を確認した上で電子政府推奨暗号リストに掲載する。

当リストに掲載される暗号については、その技術の利用において仕様がオブジェクト ID（またはアルゴリズム ID）単位で明確に特定されることを求める。また、ライセンスについて提案者以外が自由に利用できる状態であることを求める。加えて、電子政府推奨暗号リストに掲載された技術と、暗号モジュール試験及び認証制度（JCMVP 制度）との連携をスムーズに行うため、電子政府推奨暗号にはモジュール評価に足る実装仕様を

求める。

掲載技術の数の制限及び仕様の管理維持の具体的な方法にについて今後検討する必要がある。

（２）推奨暗号候補リスト

安全性及び実装性能に問題が無いことを評価して確認した暗号であるが、利用実績や製品化が十分に進んでいない暗号を示すものである。

推奨暗号候補リストに掲載される暗号技術の安全性評価の情報も外部に公開される。現電子政府推奨暗号リストに掲載されていたもので、十分に利用実績が進んでいない暗号は電子政府推奨暗号リストから外し、推奨暗号候補リストに掲載するが、利用実績が十分認められることとなれば電子政府推奨暗号リストに再び掲載されることもある。

（３）互換性維持暗号リスト

これまで推奨暗号リストに掲載されていた暗号であったが十分な安全性を確保していないと判断された場合には、「電子政府推奨暗号リスト」への掲載から外す。その際、当該暗号が利用できなくなることによって相互運用性（相互接続性）が担保出来なくなる可能性がある場合において、一時的に利用することがやむを得ない暗号を示すものである。

安全性については保証されないため、利用者が十分に注意して利用すべきものである。

（４）リストガイド

「電子政府推奨暗号リスト」に掲載された暗号の利用指針及び電子政府システムの構築には欠かせない技術を示す。たとえば、セキュリティパラメータの選択方法、応用システムにおける適切な暗号技術の選択、システム運用者や設計者の利用だけでなく、システム利用者への啓発などを含む。さらに、将来必要になるであろう、セキュリティ技術についてその開発状況や利用可能性について記載する。

５．４．４　暗号技術公募の基本方針

CRYPTREC 暗号リストの策定に当たっては、現電子政府推奨暗号リストに掲載されている暗号技術についての安全性の再評価（再確認）に加え、新たに技術の公募を２００９年度に行う。公募の基本方針は下記のとおり。

（１） 原則として、一定期間ごとに新しい暗号技術カテゴリの評価を実施する。

（２）公募に当たっては、応募可能な暗号技術の条件を下記のとおりとする。

① 十分な安全性を有する暗号技術であること。ただし、既にリストに掲載されている暗号技術と同カテゴリに属する暗号技術については、それらの暗号技術よりも安全性及び実装性において優れた暗号技術であること。

② 現状で広く利用されている暗号技術、あるいは、2013 年時点で広く利用される見込がある暗号技術であること。

③　個別のシステムやアプリケーションの仕様に依存しない、汎用的な暗号技術であること。

④　安全性に関する評価を行うことができる（評価方法、評価基準、および評価体制が整備されている）あるいは評価を行うことができるようになると見込まれる暗号技術であること

⑤　国際標準機関によってすでに標準化が行われている。あるいは、標準化が見込まれる暗号技術であること。

５．４．５　リスト改訂に向けた活動計画

公募に向けた準備として、

①　公募カテゴリ

②　安全性及び実装性能の評価手法

③　仕様書の管理手法

④　公募要領（応募書類）、規則

を策定するとともに、公募を広く一般に公知するためのイベント開催を行う。なお、公募要領については、2008 年度内にパブリックコメントを経て決定する。

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