CRYPTREC Report 2010

平成 23 年 3 月

独立行政法人 情報処理推進機構

独立行政法人 情報通信研究機構

「暗号実装委員会報告」

目次

はじめに

本報告書は、暗号技術検討会の下に設置された暗号実装委員会の 2010 年度活動報告である。

2000 年度から 3 年間に渡る暗号技術評価プロジェクト(CRYPTREC)の活動の成果として、2003 年 2 月に総務省と経済産業省から「電子政府推奨暗号リスト」が公表された。その後、CRYPTREC においては、暗号アルゴリズムそのものの安全性評価だけでなく、暗号化 LSI 等の暗号製品(暗号モジュール)の安全性を評価する必要性を認識し、暗号技術検討会の下に、独立行政法人 情報処理推進機構と通信・放送機構(現 独立行政法人 情報通信研究機構)が共同で運営する暗号モジュール委員会を設置し、暗号モジュールの安全性に関する要件の検討等を行ってきた。

昨年度は「電子政府推奨暗号リスト」の改訂に対応するため、暗号モジュール委員会は暗号実装委員会に移行し、暗号監視委員会を継承した暗号方式委員会とともに「電子政府推奨暗号リスト改訂のための暗号技術公募（2009 年度)」を行い、計 6 件の応募を受けた。また、暗号実装委員会の下にサイドチャネルセキュリティワーキンググループを置き、電力解析実験ワーキンググループの活動を発展的に引き継いだ。

本年度は、応募暗号に対する実装性能評価とサイドチャネル攻撃対策の実施可能性検証について詳細に検討を行った。サイドチャネルセキュリティワーキンググループでは米国 FIPS 140-3 をベースとしたドラフト 1st WD ISO/IEC 19790 を検討してコメント案を作成、国内 SC27/WG3 小委員会経由で国際事務局に提案するとともに、暗号モジュールに対するサイドチャネル攻撃などの攻撃法や対策の調査研究を実施し、将来のセキュリティ要件への適用の準備を進めた。

本委員会の活動が、わが国における電子政府推奨暗号リストの改訂作業と暗号実装関連技術の研究の進展に寄与できれば、幸いである。

末筆ではあるが、本活動に様々な形でご協力いただいた委員の皆様、事務局および関係者の皆様に謝意を表する次第である。

2011 年 3 月

暗号実装委員会　委員長　松本　勉

本報告書の利用にあたって

本報告書は、一般的な情報セキュリティの基礎知識を有している読者を想定している。例えば、電子署名や GPKI[1]を利用するシステムなど暗号関連の電子政府関連システムに関する業務の従事者などを想定している。ただし、暗号モジュールセキュリティ要件及び暗号モジュール試験要件、並びに運用ガイダンスを理解するためには、ある程度の暗号技術の実装経験があることが望ましい。

本報告書の第 1 章には暗号実装委員会の活動の背景と目的、第 2 章には暗号実装委員会の活動内容と成果概要、第 3 章には暗号実装委員会の委員会開催状況を記述した。

2009 年度以前の CRYPTREC Report は、下記 URL で参照できる。

http://www.cryptrec.go.jp/report.html

本報告書に対するご意見、お問合せ等は、CRYPTREC 事務局までご連絡していただけると幸いである。

【問合せ先】　info@cryptrec.go.jp

[1] GPKI：Government Public Key Infrastructure（政府認証基盤）

委員会構成

暗号実装委員会は、図 1 に示すように、総務省と経済産業省が共同で共催する暗号技術検討会の下に設置され、独立行政法人 情報処理推進機構（IPA）と独立行政法人 情報通信研究機構（NICT）が共同運営している。

暗号実装委員会では、ISO[2]/IEC[3]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、暗号モジュール評価基準及び試験基準の策定を行っている。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・検討も行っている。

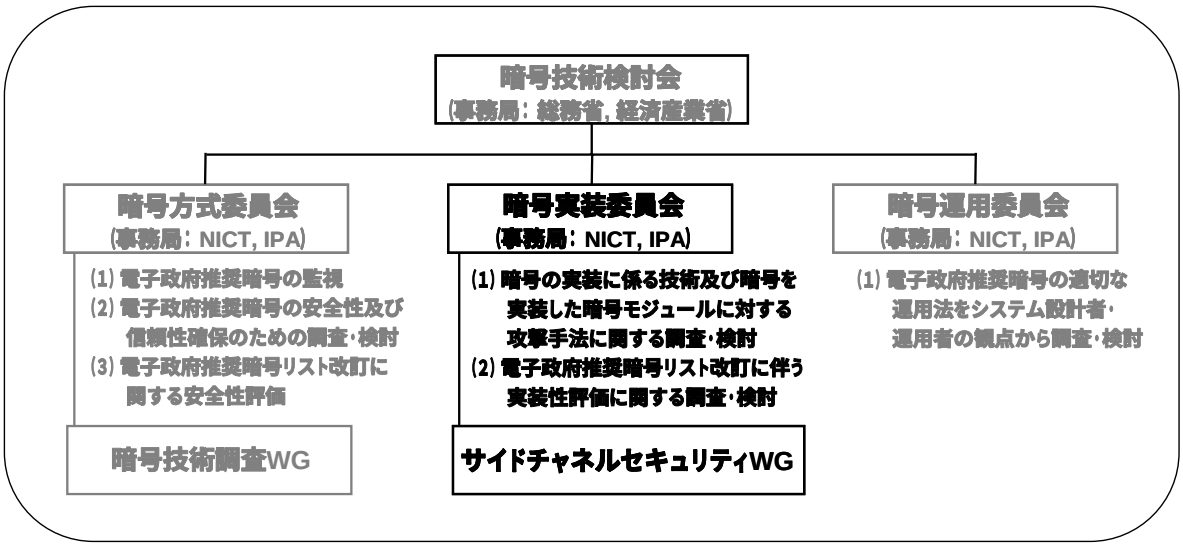


図 1　2010 年度の CRYPTREC の体制

[2] ISO：International Standard Organization
[3] IEC：International Electrotechnical Commission

委員名簿

暗号実装委員会　(2011 年 3 月現在)

委員長	松本　勉	国立大学法人横浜国立大学　教授
委員（委員長代理）	佐藤　証	独立行政法人産業技術総合研究所　研究チーム長
委員	植村　泰佳	電子商取引安全技術研究組合　専務理事
委員	大須賀　勝美	NTT エレクトロニクス株式会社　主事
委員	亀田　繁	財団法人日本情報処理開発協会　センター長
委員	崎山　一男	国立大学法人電気通信大学　准教授
委員	佐藤　恒夫	三菱電機株式会社　チームリーダ
委員	清水　秀夫	株式会社東芝　主任研究員
委員	高橋　芳夫	株式会社 NTT データ　シニアエキスパート
委員	角尾　幸保	日本電気株式会社　主席研究員
委員	鳥居　直哉	株式会社富士通研究所　部長
委員	福永　利徳	日本電信電話株式会社　主任研究員
委員	本間　尚文	国立大学法人東北大学　准教授
委員	松崎　なつめ	パナソニック株式会社　チームリーダ
委員	渡辺　大	株式会社日立製作所　研究員

オブザーバ

根本　農史	内閣官房　情報セキュリティセンター（2010 年 9 月から）
赤澤　康之	警察庁　情報通信局
岡野　孝子	警察大学校　警察情報通信研究センター（2010 年 4 月から）
松本　和人	総務省　行政管理局（2010 年 7 月まで）
松宮　志麻	総務省　行政管理局（2010 年 7 月から）
島田　淳一	総務省　情報通信国際戦略局（2010 年 7 月まで）
古賀　康之	総務省　情報通信国際戦略局（2010 年 7 月まで）
梶原　亮	総務省　情報通信国際戦略局（2010 年 7 月まで）
齊藤　修啓	総務省　情報通信国際戦略局（2010 年 7 月まで）
水野　伸太郎	総務省　情報流通行政局（2010 年 7 月から）
佐々木　信行	総務省　情報流通行政局（2010 年 7 月から）
谷岡　大祐	総務省　情報流通行政局（2010 年 7 月から）
荒木　美敬	外務省　大臣官房

山中　豊　　経済産業省　産業技術環境局
乃田　昌幸　　経済産業省　商務情報政策局（2010 年 4 月から）
下里　圭司　　経済産業省　商務情報政策局（2010 年 7 月まで）
森川　淳　　経済産業省　商務情報政策局（2010 年 7 月から）
島田　紀章　　経済産業省　商務情報政策局（2010 年 4 月から）
池西　淳　　経済産業省　商務情報政策局
千葉　修治　　防衛省　陸上幕僚監部
石川　正興　　防衛省　技術研究本部
坂下　圭一　　防衛省　運用企画局
滝澤　修　　独立行政法人　情報通信研究機構
川村　信一　　独立行政法人　産業技術総合研究所
青木　林　　財団法人　日本規格協会

事務局

独立行政法人　情報処理推進機構
矢島　秀浩
山岸　篤弘
近澤　武
小暮　淳
神田　雅透
大熊　建司
鈴木　幸子

独立行政法人　情報通信研究機構
篠田　陽一（2010 年 7 月まで）
高橋　幸雄（2010 年 7 月から）
田中　秀磨
松尾　真一郎
大久保美也子
黒川　貴司
金森　祥子

第１章　活動の背景と目的

1.1　CRYPTREC 活動の経緯

インターネットの普及と情報通信技術の飛躍的な発展により、社会・経済のネットワーク化が急速に進展している。中でも、電子商取引に代表されるように、オープンなネットワークを介して相手と直接対面することなく重要な情報をやり取りし、受発注や決済等を行うことが日常的になってきている。

また、政府の動きとしても、各種申請届出手続きや政府調達などの行政サービスを電子化する電子政府システムの構築が行われ、国民生活に浸透し始めている。また、高度情報通信ネットワーク社会推進戦略本部（ＩＴ戦略本部）の重点計画等で、電子政府システムにおける情報セキュリティの確保及びその基盤となる暗号技術の重要性が認識され、関連する施策が実行に移されている。

このような状況で、現在、様々な暗号技術が開発され、それを組み込んだ多くの製品が市場に提供されているが、全ての暗号技術の安全性が評価・確認されている訳ではない。特に、電子政府システムの安全性を保つには、暗号技術を客観的に評価することが極めて重要である。

以上のような背景から、通商産業省（現経済産業省）からの委託を受けて、情報処理振興事業協会（現 独立行政法人 情報処理推進機構(IPA)）は電子政府で利用可能な暗号技術を安全性及び実装性能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 2000 年 5 月に設置した。産学の最高水準の暗号専門家で構成されたこの委員会の設置により、わが国において本格的な暗号技術評価プロジェクトがスタートした。 翌年度には、委員会の共同事務局として通信・放送機構（現 独立行政法人 情報通信研究機構(NICT)）が参加した。

2001 年度には、経済産業省と総務省が共同で暗号技術検討会を設置し、暗号技術の利用に関する政策的な観点からの検討が開始された。暗号技術評価委員会と暗号技術検討会は、関係する省庁がオブザーバとして参加する等、政府横断的な活動であり、これらを総称して、CRYPTREC(CRYPTography Research and Evaluation Committees)と呼んでいる。

2000 年度から 2002 年度までの 3 年間に及ぶ CRYPTREC 活動で、電子政府システムで安心して利用できる暗号を選定するための客観的な評価が実施された。その結果、合計 29 方式の暗号技術が安全性及び実装性能に問題がないとされ、2003 年 2 月に総務省と経済産業省によって「電子政府推奨暗号リスト」が公開された。

2003 年度からは、電子政府の安全性及び信頼性を引き続き確保していくため、新しい体制に移行した。暗号技術検討会は存続とし、暗号技術検討会の下に「暗号技術監視委員会」及び「暗号モジュール委員会」を新設し、さらに、「暗号技術監視委員会」の下に「暗号技術調査 WG」を新設した。従来の暗号技術評価委員会は、

暗号技術監視委員会に発展的に再編され、電子政府推奨暗号リストに掲載された暗号の安全性を監視してきた。従来の公開鍵暗号評価小委員会及び共通鍵評価小委員会は暗号技術調査 WG に再編され、監視委員会で必要と判断した個別テーマに関する調査を実施している。また、暗号モジュール委員会では、暗号技術を実装した暗号モジュール製品（暗号製品）の安全性確保のために、暗号モジュール製品に対するセキュリティ要件とその試験方法の検討を行ってきた。

特に、暗号モジュール委員会では、2006 年度の 12 月からは、暗号モジュールへの実際の脅威となりつつあるサイドチャネル攻撃の一つである電力解析攻撃等について、実験を踏まえて脅威と対策を検討することにより、暗号モジュール製品の安全性を確保すると共に、FIPS[4]（Federal Information Processing Standard） PUB[5] 140-3 の試験要件作成に反映させることを目標として、「暗号モジュール委員会」の下に「電力解析実験 WG」を新設した。

この WG では、財団法人 日本規格協会 情報技術標準化センター（INSTAC[6]） 耐タンパー性標準化調査研究委員会による、サイドチャネル攻撃耐性評価標準プラットフォーム仕様 INSTAC-8/-32[7]準拠のプラットフォーム（INSTAC-8, INSTAC-32）や産業技術総合研究所情報セキュリティ研究センターが、経済産業省からの委託を受けて開発したサイドチャネル攻撃用標準評価ボード（SASEBO：Side-channel Attack Standard Evaluation BOard）を用いた実験を行うことにより、電力解析に対する技術的な蓄積を実施してきている。

電子政府推奨暗号リストは 2013 年度までに改訂することが決まっており、2008 年度に暗号技術監視委員会において、改訂及び新設する暗号技術カテゴリを決め公募要項の検討を行った。2009 年度には、暗号技術公募に備えるために CRYPTREC の体制を変更し、暗号技術監視委員会は暗号方式委員会に、暗号モジュール委員は暗号実装委員会に改称し、従来の活動内容を引き継ぐとともに、各々、応募暗号技術の安全性評価、及び、応募暗号技術の実装性能評価とサイドチャネル攻撃の対策可能性確認を活動目標に加えた。また、暗号モジュール委員会下の電力解析実験 WG はサイドチャネルセキュリティ WG に改称し、電力解析に限らず、電磁波解析やキャッシュタイミング攻撃などサイドチャネル攻撃一般に対象を広げることになった。

1.1.1 活動の総括

暗号モジュール委員会は、2003 年 3 月に策定された「電子政府推奨暗号リスト」に掲載された暗号技術を安全に使用するために、暗号機能を提供する暗号モジュールへの実装攻撃等の暗号実装関連技術を主な対象として調査及び検

[4] FIPS：Federal Information Processing Standard
[5] FIPS PUB:Federal Information Processing Standards Publication
[6] INSTAC：情報技術標準化研究センター (Information Technology Research and Standardization Center)
[7] INSTAC-8/-32：サイドチャネル攻撃耐性評価用標準プラットフォーム仕様（-8 は 8bit 版, -32 は 32bit 版）

討を行うことを目的として設立された。

2003 年、2004 年の両年度にわたり、米国 NIST[8]とカナダ CSE[9]が運用している CMVP[10]（暗号モジュール試験及び認証）制度の調査を行い、暗号モジュールに対するセキュリティ要件及び試験要件に対する研究を実施し、暗号モジュールに対するセキュリティ要件(案)及び試験要件（案）を作成した。

このセキュリティ要件等を検討する間、米国およびカナダが運用していた CMVP 制度における暗号モジュールに対するセキュリティ要件である FIPS（Federal Information Processing Standard）PUB 140-2 を国際標準規格とする審議が ISO[11]/IEC[12] JTC[13]1 SC[14]27/WG[15]3 で開始されたため、2004 年度からは、規格文書の草案に対するコメント作成等の活動や 2006 年度に検討が開始された FIPS 140-2 の改訂版である FISP 140-3 に対する検討作業を行ってきた。

2006 年 12 月には、FIPS 140-3 の試験要件作成に反映させることを目標として、「暗号モジュール委員会」の下に「電力解析実験 WG」を新設した。この WG では、暗号モジュールへの実際の脅威となりつつあるサイドチャネル攻撃の一つである電力解析攻撃等について、実験を踏まえて脅威と対策を検討することにより、暗号モジュール製品の安全性を確保することを目指している。

2009 年 7 月には、電子政府推奨暗号リストの改訂に向け、「暗号モジュール委員会」は「暗号実装委員会」に改称し、従来の活動を引き継ぐとともに、暗号技術の公募要項作成、及び、実装性能等の評価を活動目的に加えた。また、「電力解析実験ワーキンググループ」は「サイドチャネルセキュリティワーキンググループ」に改称し、調査対象を電力解析からサイドチャネル攻撃一般に拡張するとともに、FIPS 140-3 及びそれに対応する国際規格 ISO/IEC 19790 の改訂の草案に対するコメント作成作業を継承している。

1.1.2 暗号モジュール委員会／暗号実装委員会を取り巻く環境の変化

2003 年に暗号モジュール委員会が活動を開始した後、2004 年には、独立行政法人 情報通信研究機構が発足し、2005 年には、独立行政法人 産業技術総合研究所(AIST[16])の情報セキュリティ研究センター(RCIS[17])が発足し、暗号モジュールの安全性評価に対する研究体制の充実がはかられた。さらに、2006 年には、ISO/IEC JTC1 SC27 での暗号モジュールに対するセキュリティ要件の国

[8] NIST：National Institute of Standards & Technology（米国国立標準技術研究所）
[9] CSE：Communications Security Establishment
[10] CMVP：(Cryptographic Module Validation Program)
[11] ISO：International Standard Organization（国際標準化機構）
[12] IEC：International Electrotechnical Commission（国際電器標準会議）
[13] JTC：Joint Technical Committee（合同技術委員会）
[14] SC：SubCommittee（副委員会）
[15] WG：Working Group（ワーキンググループ）
[16] AIST：Advanced Industrial Sciens and Technology
[17] RCIS：Research Center for Information Security

際標準(ISO/IEC 19790)の成立を受け、独立行政法人 情報処理推進機構内に暗号モジュール試験及び認証の試験機関と認証機関を創設し、日本における暗号モジュールの試験及び認証制度(JCMVP)が創設された。

2006年度にFIPS 140-2の次期バージョンFIPS 140-3の作成検討が始まり、2007年7月に第1次草案が公開、これに対するコメントを反映した改訂草案が2009年12月に公開された。この草案に対するコメントを反映して、FIPS 140-3が制定される予定である。一方、ISO/IEC JTC1 SC27では、2008年5月にFIPS 140-3をベースとしてISO/IEC 19790を改訂することが決まり、2010年2月に1st WDが発表された。

このような環境の変化に合わせ、暗号モジュール委員会ではFIPS 140-3草案へのコメント作成を行うとともに、暗号モジュールの安全性の確保と試験要件作成への反映を目標に電力解析実験WGを組織し、サイドチャネル攻撃耐性評価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, INSTAC-32）やその後継機種であるサイドチャネル攻撃実験用標準評価ボード（SASEBO[18]）を用いて、電力解析に対する技術的な蓄積を実施してきた。

2009年度には、暗号モジュール委員会は電子政府推奨暗号リスト改訂に向け、暗号実装委員会に改称した。同時に、電力解析実験WGは調査対象を電力解析からサイドチャネル攻撃一般に拡張し、サイドチャネルセキュリティWGに改称し、FIPS 140-3とISO/IEC 19790の改訂草案に対するコメント作成作業を引き継いだ。

1.2 暗号モジュールの試験及び認証に関する国際標準化動向

安心できる実用的な情報セキュリティシステムの構築において、安全で実装性能の高い暗号アルゴリズムの選択は不可欠の条件である。しかし、それだけでは不十分であり、暗号アルゴリズムを適切な方法で実装することが不可欠である。暗号アルゴリズムをソフトウェア及びハードウェアとして実装したものを暗号モジュールとよび、暗号モジュールに対して、動作の信頼性や安全性を規定した規格をセキュリティ要件と呼ぶ。この暗号モジュールに対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、米国及びカナダで運用されているCMVP[19]制度で用いら

[18] SASEBO: サイドチャネル攻撃実験用標準評価ボード（Side-channel Attack Standard Evaluation BOard）で2種類のXilinx Virtex-II Pro FPGAであるxc2vp7とxc2vp30を搭載。
SASEBOボードに関しては、平成19年度経済産業省委託事業「暗号モジュールの実装攻撃の評価に関する調査研究」の中で産業技術総合研究所と東北大学が新たに開発を行った、Xilinx社製FPGAを実装したSASEBO-G、ALTERA社製FPGAを実装したSASEBO-B、そしてカスタム暗号LSIを実装したSASEBO-Rの3種類が、電力解析実験ワーキンググループの委員が所属する研究機関に対して提供され、これにより、アーキテクチャの異なるハードウェア上でのサイドチャネル攻撃実験が行える環境が整った。そこで、本ワーキンググループにおいても産総研の了承のもと、各委員がこれらのSASEBOボードを活用した比較実験を行うこととした。

[19] Cryptographic Module Validation Program

れている FIPS 140-2 と FIPS 140-2 をベースとして国際規格となった ISO[20]/IEC[21] 19790 が存在する。

1.2.1 FIPS 140-2/140-3

FIPS 140-2 は、米国 NIST/カナダ CSE[22]が共同運用している CMVP 制度で利用されているセキュリティ要件に関する規格であり、米国 NIST によって発行されている。この規格の関連文書としては、試験要件(DTR[23])と運用ガイダンス(IG[24])の 2 種類がある。DTR は暗号モジュールがセキュリティ要件を実際に満たすか確かめるための試験項目を定めたものである。また、IG には試験を実施する際の運用法を定めたもので、質問とそれに対する回答という形式で記述されている。NIST はこれら関連文書を必要に応じて適宜改訂することで、暗号モジュール試験及び認証制度を柔軟に運用している。

NIST/CSE 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 に改訂する作業を行っている。2007 年 7 月には、FIPS 140-3 の第 1 次草案が公開され、これに対するコメントを反映した改訂草案は予定よりも大幅に遅れたものの、2009 年 12 月に公開された。改訂草案に対するコメント受付は、2010 年 3 月 11 日に締め切られた。

FIPS 140-3 では、サイドチャネル攻撃へのセキュリティ要件が盛り込まれていることが特徴である。第 1 次草案ではセキュリティレベルを 5 段階に増やしていたが、改訂草案では FIPS 140-2 と同様、4 段階に戻っている。

1.2.2 ISO/IEC 19790 と ISO/IEC 24759

ISO/IEC 19790 は、FIPS 140-2 を基に作られた国際規格である。ISO/IEC JTC 1 SC 27/WG 3 のプロジェクトとして審議され、2006 年 3 月 1 日に発行された。

また、FIPS 140-2 に対応する試験要件(DTR)に対応した ISO/IEC 19790 に対する試験要件の標準化は、FIPS 140-2 に対応する試験要件(DTR)と運用ガイダンス(IG)をベースとして、2008 年 6 月に ISO/IEC 24759 として規格化された。

ISO/IEC 19790 は、2007 年 3 月に日本工業標準調査会(JISC[25])によって JIS[26]化され、JIS X 19790 として発行された。また、JIS X 19790 に対応する試験規格は、暗号モジュール委員会で検討してきた「暗号モジュール試験基準第 0.1 版」をベースとして、2007 年 3 月に、JIS X 5091 として発行された。しかし、ISO/IEC 24759(2008 年 6 月発行)をベースとした JIS X 24759 が JIS X 19790 に対する試験規格として 2009 年 10 月に発行されるに伴い、JIS X 5091 は廃止された。

---

[20] International Organization for Standardization
[21] International Electrotechnical Commission
[22] Communication Security Establishment
[23] Derived Test Requirements
[24] Implementation Guidance
[25] JISC：Japanese Industrial Standards Committee（日本工業標準調査会）
[26] JIS：Japanese Industrial Standards（日本工業規格）

2006 年 3 月に発行された ISO/IEC 19790 は、米国 NIST で進められている FIPS140-2 の改訂に対応し、FIPS 140-2 の後継標準となる FIPS 140-3 をベースに改訂するべく早期改訂を開始した。その後、FIPS 140-3 の改訂草案作成が大幅に遅れたため、FIPS 140-3 と ISO/IEC 19790 の改訂を並行して行うことが決まった。これに従い、ISO/IEC 19790 改訂版(2nd ed.)の 1st WD は FIPS 140-3 の改訂草案に若干遅れた 2010 年 2 月に発表され、同年 3 月 30 日にコメント受付が締め切られた。これらの草案は、両標準化団体の規約の違いを反映して編集上の差異は若干異なるものの、技術的内容は同じである。

1.3 暗号実装委員会の活動状況

1.3.1 暗号モジュール委員会時代の活動

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。

この目的のためには、実装が適切に行われていることを確認する仕組みが必要であり、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に対するセキュリティ要件等の素案作成、及びその素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、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)暗号モジュール評価基準[27]及び試験基準[28]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

(1)では、将来的に政府調達基準として利用されることを前提に暗号モジュール評価基準及び試験基準の策定作業を行う。(2)では、暗号モジュールの実装方法の安全性評価を行うための基礎となるデータを収集する。

2003 年度の活動概要

(1) 暗号モジュール評価基準及び試験基準の策定

国内基準策定を目指し、ISO/IEC 国際規格の動向を注視しつつ、北米の評価基準及び試験基準を翻訳し、暗号モジュール評価基準及び試験基準の第 0 版として発行した。

(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

暗号モジュールの実装方法に対する安全性評価法の一環として、非破壊攻

[27] 2005 年度の活動で、「評価基準」は「セキュリティ要件」に変更された。
[28] 2005 年度の活動で、「試験基準」は「試験要件」に変更された。

撃の１つである電力解析をテーマに選び、調査・研究の共通基盤を整えるため、FPGA[29]による評価用標準プラットフォームの要求仕様を策定した。

2004 年度の活動概要

(1) 暗号モジュール評価基準及び試験基準の策定

審議中の国際規格(ISO/IEC 19790)で、FIPS 140-2 の内容を変更する方針が出された。変更点を反映すべく、前年度の基準第 0 版に対し、次の a)～e)の作業を行った。

a)暗号モジュール評価基準の差分表の作成

FIPS 140-2 と国際規格(1st CD 19790)との差分表を作成し、翻訳する。

b)差分表に対応した暗号モジュール試験基準の検討表の作成

上記 a)で作成した暗号モジュール評価基準の差分表に対応した暗号モジュール試験基準の検討表の作成を行う。

c)ISO/IEC JTC 1/SC 27/WG 3 への技術コメント作成協力

国際標準(ISO/IEC 19790)案に対する日本コメント案作成の協力を行う。

d)運用ガイダンス第 0 版の作成

NIST 発行の“ Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program(Last Update: April 28, 2004) ”及び 4 月 28 日以降に改版に対し、逐次翻訳作業を実施する。

e)暗号モジュール評価基準及び試験基準第 0.1 版の作成

2003 年度作成した第 0 版に対して、NIST 発行の FIPS 140-2, DTR の CHANGE NOTICE を反映した修正を行い、第 0.1 版とする。

(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

2003 年度に策定した評価用標準プラットフォームの仕様に従った評価用ボードを調達し、希望する委員に配布するとともに、よりスペックの高い評価用標準プラットフォームの仕様を策定した。また、非破壊攻撃及び破壊攻撃に関する学会活動の調査を行った。具体的には、次の a)～c)の作業を行った。

a)評価用標準プラットフォーム仕様の評価用ボードの調達(8 ビット CPU)

INSTAC の耐タンパー性に関する標準化調査研究委員会が策定した「電力解析のための汎用 8 ビット CPU を用いた評価用標準プラットフォーム仕様」に従った評価用標準プラットフォームを実装し、希望する委員に無償配布した。無償配布の条件として、得られた成果の学会等での発表を義務付けた。

b)評価用標準プラットフォーム仕様の策定(32 ビット CPU)

INSTAC の耐タンパー性に関する標準化調査研究委員会と協調して、

[29] Field Programmable Gate Array

「評価用標準プラットフォーム仕様」を策定した。具体的には、INSTAC が策定した「電力解析のための汎用 32 ビット CPU を用いた評価用標準プラットフォーム仕様」と、2003 年度の暗号モジュール委員会で策定した「FPGA を用いた評価用標準プラットフォーム仕様」を融合して、「評価用標準プラットフォーム仕様」を策定した。

c)非破壊攻撃及び破壊攻撃に関する学会活動調査

次の学会に参加し、非破壊攻撃及び破壊攻撃に関する発表を聴講した。ISEC 研究会(7 月、徳島)、CHES 2004(8 月米国・ボストン)、ICD 研究会(9 月、東京)、CSS 2004(10 月、札幌市)、ASIACRYPT 2004(12 月、韓国・済州島)。また、IACR e-Print Archives を初めとする Web 上の発表論文も調査した。

2005 年度の活動概要

(1) 暗号モジュールセキュリティ要件及び暗号モジュール試験要件の策定

前年度に引き続き、FIPS 140-2 と ISO/IEC 19790 に関する動向調査を行いつつ、基準類の策定作業を進めた。基準類のバージョン番号は、2006 年度に発行される正式版を第 1 版とし、それ以前は日付でバージョンを区別する方針になった。

また、前年度では、「暗号モジュール評価基準」「暗号モジュール試験基準」というタイトルで、基準類の策定を行った。しかし、FIPS 140-2 では、「evaluation」と「testing(又は test)」を明確に区別して使用しており、「evaluation」は、Common Criteria 関連の部分でしか使用されていない。Common Criteria 関連では「評価」、FIPS 140-2 関連では「試験」ということで、用語の使用方法の統一を図った。これにより、基準類のタイトルを、次のように変更した。

FIPS PUB 140-2 Security requirements for cryptographic modules
→「暗号モジュールセキュリティ要件」

Derived Test Requirements [DTR] for FIPS PUB 140-2
→「暗号モジュール試験要件」

a)ISO/IEC JTC 1/SC 27/WG 3 への技術コメント作成協力

国際標準(FCD 19790, FDIS 19790)案に対する日本コメント案作成協力を行った。

b)運用ガイダンスの改訂

NIST 発行の“ Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program ”の改版に対し、逐次翻訳作業を実施した。

c)暗号モジュールセキュリティ要件及び暗号モジュール試験要件の策定

2004 年度作成した暗号モジュール評価基準第 0.1 版及び試験基準第 0.1

版を基に、FDIS 19790 に対応するための検討を行い、暗号モジュールセキュリティ要件及び暗号モジュール試験要件を策定した。

(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

2004 年度に仕様策定を行った評価用標準プラットフォーム(32 ビット CPU)を実装した評価用ボードの開発を発注し、希望する委員に配布した。昨年度と同様、無償配布の条件として、得られた成果の学会等での発表を義務付けた。

2006 年度の活動概要

(1) 暗号モジュール試験要件の国際規格作成への貢献

ISO/IEC JTC 1 SC 27 において、ISO/IEC 19790 に対応する試験要件 ISO/IEC 24759 が作成中である。暗号モジュール委員会では、24759 の草案 WD 及び 1st CD に対するコメント案を作成し、SC 27 国内委員会経由で国際事務局に提案した。

(2) 電力解析実験ワーキンググループの立ち上げ

米国では FIPS 140-2 が FIPS 140-3 に改訂される作業が進められており、その中でサイドチャネル攻撃に関する要件が追加される予定である。暗号モジュール委員会では、サイドチャネル攻撃の一種である電力解析に関する要件の策定に貢献するため、INSTAC-8/-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、実験データの収集を進めてきた。2006 年度は、今まで独立していた実験活動を組織化し、実験効率を高めるため、電力解析実験ワーキンググループを立ち上げた。

(3) 暗号モジュールセキュリティ要件・試験要件の JIS 化

当委員会で作成した「暗号モジュールセキュリティ要件」と「暗号モジュール試験要件 2006-03-31 版」が各々、次の JIS 規格の素案として利用された。

「JIS X 19790 セキュリティ技術-暗号モジュールのセキュリティ要求事項」

「JIS X 5091 セキュリティ技術-暗号モジュールのセキュリティ試験要件」

2007 年度の活動概要

(1) 暗号モジュール試験要件の国際規格作成への貢献

FIPS 140-2 を基にセキュリティ要件の国際規格 ISO/IEC 19790 が作成され、2006 年に発行されたが、現在、ISO/IEC JTC 1/SC 27 では、19790 に対応した試験要件 ISO/IEC 24759 作成のプロジェクトを進めている。暗号モジュール委員会では、7 月 25 日の第 2 回暗号モジュール委員会で 24759 の最終草案を審議し、SC 27 の国内委員会に対し、コメント案の作成に協力

した。

(2) FIPS 140-3 へのコメント提出

NIST は、FIPS 140-2 を FIPS 140-3 に改訂する準備を進めている。7 月 13 日に草案が発行され、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 日に合同で委員会を開催し、日本としてのコメントをまとめ、10 月 11 日に NIST へ提出した。

(3) 電力解析実験ワーキンググループの活動

米国では FIPS 140-2 を FIPS 140-3 に改訂する作業が進められており、その中でサイドチャネル攻撃に関する要件が追加される。暗号モジュール委員会では、サイドチャネル攻撃に関する要件の策定に貢献するため、INSTAC-8/-32 仕様に準拠した標準プラットフォームを委員に配布し、実験データの収集を進めてきた。9 月には更に産業技術総合研究所と東北大学による新たな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[30],Camellia,DES[31],Misty1）のソースコードが開発され、電力解析実験ワーキンググループの委員に配布し、暗号モジュールの安全性と標準化の検討ための実験活動とそのまとめを行った。

(4) FIPS 140-2 と 暗号モジュール試験及び認証制度のための運用ガイダンスの日本語の改訂版の作成

NIST 発行の“Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program”は逐次改訂版の発行が行われている。それに対応し暗号モジュール委員会では、日本語の翻訳版の作成作業を行っており、3 月の時点では 2008 年 1 月 24 日版を「FIPS PUB 140-2 と暗号モジュール試験及び認証制度のための運用ガイダンス」として作成した。

2008 年度の活動概要

(1) 電子政府推奨暗号リスト改訂のための公募要項における、ハードウェア実装及びソフトウェア実装の性能評価項目作成

電子政府推奨暗号リスト改訂のための「暗号技術公募要項（2009 年度）（案）」作成において暗号技術検討会の依頼を受け、応募暗号の実装性能に関する第一次評価と第二次評価の評価項目を作成した。

(2) 暗号モジュールに対するサイドチャネル攻撃の監視と分析

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

(3) 電力解析実験ワーキンググループよる実験

サイドチャネル解析用プラットフォームの仕様である INSTAC-8/-32 仕様

[30] AES：Advanced Encryption Standard（米国標準暗号）
[31] DES：Data Encryption Standard（旧米国標準暗号）

に準拠したボードや SASEBO ボード等を用いた比較実験を依頼した結果、電力解析実験ワーキンググループから以下の項目に関する報告が提出された。

１．サイドチャネル攻撃に関する比較実験
２．採取データの形式の統一化
３．実験データの標準評価方法の検討
４．電力解析攻撃実験のための評価ボードを利用した研究の調査
５．今後の検討項目

2009 年度の活動概要

(1) 電子政府推奨暗号リスト改訂のための公募評価における、ハードウェア実装及びソフトウェア実装の性能評価の検討

2009 年度の応募暗号の実装性能評価に関する第一次評価(動作確認)を行うとともに、第二次評価(詳細評価)内容を継続して検討した。

(2) 電子政府推奨暗号リスト改訂のための公募評価における、サイドチャネル攻撃対策の可能性評価の検討

2009 年度の応募暗号のサイドチャネル攻撃対策可能性の評価方法を継続して検討した。

(3) 暗号モジュールのセキュリティ要件 ISO/IEC 19790 等、標準化への協力

FIPS 140-3 の改訂草案に対応する国際規格 ISO/IEC 19790 の早期改訂ドラフトに対して、サイドチャネルセキュリティ WG と共同でコメントを作成した。

1.3.2　2010 年度の活動概要

2010 年度暗号実装委員会の成果

今年度の暗号実装委員会の主要成果としては、次の 4 つが挙げられる。

(1) 電子政府推奨暗号リスト改訂のための公募評価における、ハードウェア実装及びソフトウェア実装の性能評価の詳細検討

応募暗号技術及び現行の電子政府推奨暗号リスト掲載暗号技術に対するハードウェア及びソフトウェア実装性評価の実装環境及び必要とされる実装性能の基準となる次の各項を決定した。

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

(2) 電子政府推奨暗号リスト改訂のための公募評価における、サイドチャネ

ル攻撃耐性の評価の詳細検討

応募暗号技術及び現行の電子政府推奨暗号リスト掲載暗号技術のサイドチャネル攻撃耐性に関する評価項目、評価手法の検討し、評価対象はハードウェア実装に絞り、実装要件を決定した。

(3) 暗号モジュールのセキュリティ要件の国際標準規格策定への協力

昨年度に引き続き、FIPS 140-3 の改訂草案に対応する国際規格 ISO/IEC 19790 早期改訂の草案を 8 月と 2 月の 2 回に渡って作成し、松本委員長から ISO/IEC SC27/WG3 国内小委員会に提出された。

(4) 暗号アルゴリズム危殆化時の緊急対応の検討

暗号技術検討会がまとめた電子政府システムで利用されている暗号アルゴリズム急激な安全性の低下時の CRYPTREC 各組織の役割分担を受け、暗号実装委員会が取るべき役割について検討した。

第 2 章　2010 年度の活動内容と成果概要

2.1　電子政府推奨暗号リスト改訂のための公募評価における、ハードウェア実装及びソフトウェア実装評価の詳細検討

2.1.1　実装性評価の概要

電子政府推奨暗号リスト改訂のための公募評価における、実装性に関わる評価について 2008 年度の暗号モジュール委員会で検討した結果の概要を図 2.1 に示す。今年度は昨年度に引き続き、「ソフトウェア処理性能評価」、「ハードウェア処理性能評価」、「サイドチャネル攻撃耐性評価」について検討し、具体案としてまとめた。

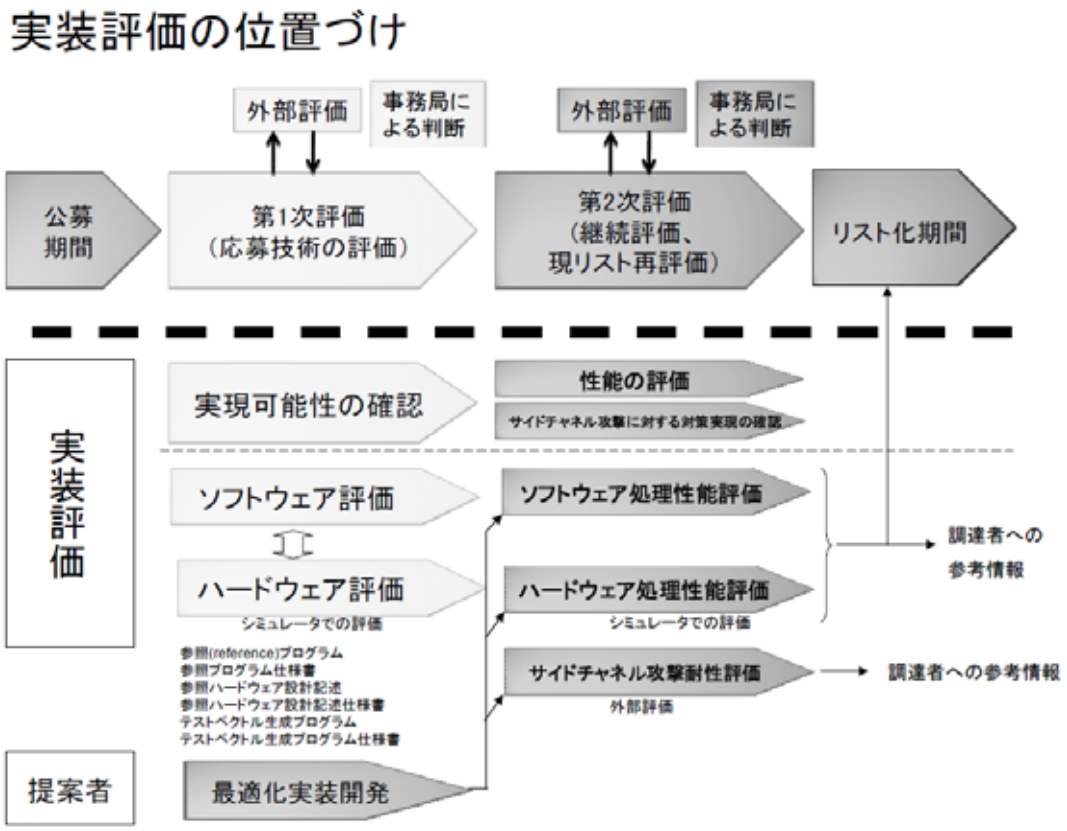


図 2.1　実装性評価の位置づけ

.

2.1.2　実装評価の詳細

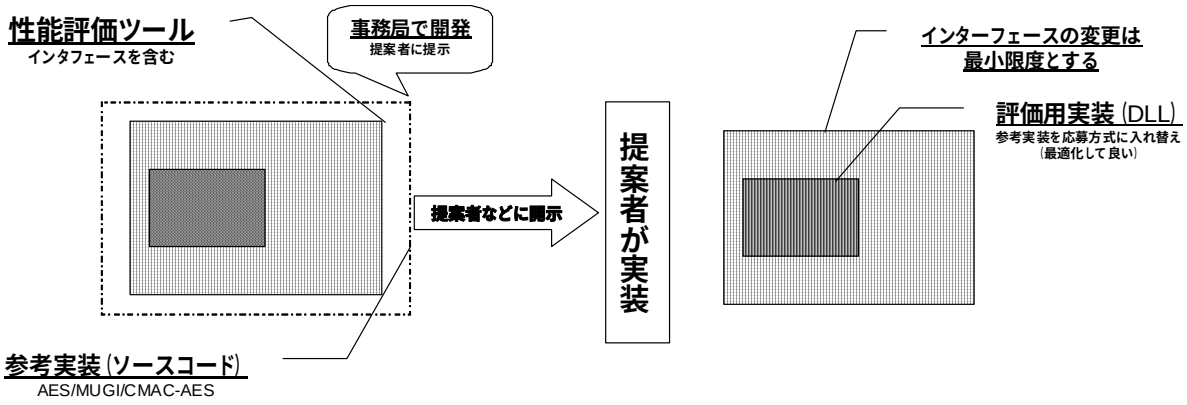
2010 年度は 2009 年度に引き続き、応募暗号の実装評価について検討し、

評価の具体案を作成した。実装評価は、処理速度等の実装性能評価とサイドチャネル攻撃に対する対策可能性について分かれる。実装性能評価はソフトウェア実装とハードウェア実装の両方で実施するが、サイドチャネル攻撃対策可能性の評価はハードウェア実装のみ実施する。以下では、これらの各々について検討結果を記述する。

(1) ソフトウェア実装の性能評価

ア　実装性評価の方法

- 図 2.2 に 2011 年度に実施するソフトウェア実装性能評価の実施手順に関するイメージを示す。
-



- 図 2.2　ソフトウェア実装性評価の手順

- 事務局は図 2.2 の左に示したサンプル実装を開発し、暗号技術応募者に提示する。
- サンプル実装は、暗号アルゴリズム・コアとしての現電子政府推奨暗号リストに記載されているブロック暗号 AES とストリーム暗号 MUGI、及び、事務局推薦のメッセージ認証コード CMAC-AES の参考実装と、インターフェース（回路）とで構成される。
- 応募者は参考実装の部分を応募暗号技術で書き換えた評価用実装を作成し、事務局に提出する。
  (1) 評価用実装は処理性能を評価するための評価用実装 1 個であり、インターフェースの部分は必要最小限の変更を許すものとする。

イ　実装性評価環境

Intel x86 CPU + MS-Windows 7（32 ビット版と 64 ビット版両方）

Visual Studio を開発環境とし、Visual C++ 2010 (10.0)を使用する

ウ　評価項目等

(i) ブロック暗号・ストリーム暗号とも鍵長は 128 ビットとする。

(0) 他の鍵長での性能は参考情報とする。

(ii) 高速実装を性能評価対象とする。

(1) 処理速度と使用リソース利用を評価基準とする。

(iii)評価項目

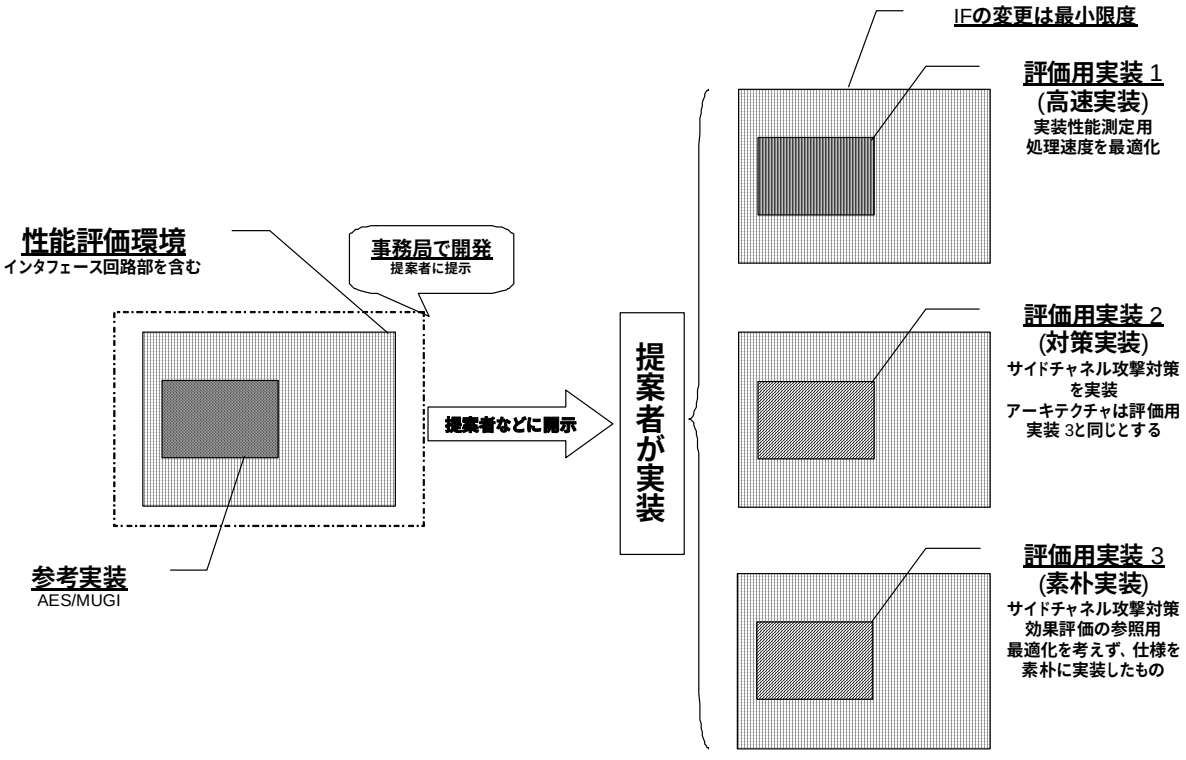
(1) 暗号化と復号の処理速度。short message と long message

(2) 初期設定に掛かる時間

(3) メモリ消費量　（通常の利用において支障のない範囲であることを確認）

(4) プログラムサイズ（DLL ファイルによる提出を想定）　（通常の利用において支障のない範囲であることを確認）

(2) ハードウェア実装の性能評価とサイドチャネル攻撃対策可能性評価



・ 図 2.3　ハードウェア実装性評価の手順

ア　実装性評価の方法

・ 図 2.3 に 2011 年度に実施するハードウェア実装性能評価とサイドチ

ャネル攻撃対策可能性評価の実施手順に関するイメージを示す。

- 事務局は図 2.3 の左に示したサンプル実装を開発し、暗号技術応募者に提示する。
- サンプル実装は、暗号アルゴリズム・コアとしての現電子政府推奨暗号リストに記載されているブロック暗号 AES とストリーム暗号 MUGI の参考実装と、インターフェース（回路）とで構成される。
- 応募者は参考実装の部分を応募暗号技術で書き換えた評価用実装を作成し、事務局に提出する。
- 評価用実装は処理性能を評価するための評価用実装 1(高速実装)、サイドチャネル攻撃対策を施した評価用実装 2(対策実装)、評価用実装 2 と同じアーキテクチャで対策を施していない評価用実装 3(素朴実装)の 3 種類を提出することとし、インターフェースの部分は必要最小限の変更を許すものとする。

イ　実装性評価環境

Xilinx Virtex-5 LX30/LX50(SASEBO-GⅡ搭載の FPGA) + ISE WebPACK

ISE WebPACK Version 11.5 を開発環境とする

ウ　処理性能評価基準

(i) ブロック暗号・ストリーム暗号とも鍵長は 128 ビットとする。
  (1) 他の鍵長での性能は参考情報とする。
(ii) 高速実装を性能評価対象とする。
  (1) 処理速度と使用リソース利用を評価基準とする。
(iii) スピード／処理性能、サイズの２つを基本とする。
  (1) 処理速度(スループット)は I/F に依存するので、critical path 遅延とサイクル数に置き換える。
  (2) 実装での I/F の書き換えは必要最小限に限定する。
  (3) 実装方針の説明にアーキテクチャを書くこととする。

エ　サイドチャネル攻撃に対する対策実現の確認

(i) 鍵長

ブロック暗号・ストリーム暗号とも 128 ビットを評価対象とする。

(ii) 評価対象の攻撃法は、単純電力解析(SPA)と差分電力解析(DPA)
  (1) DPA には多様なバリエーションがあるが、暗号モジュールセキュリティ要件（ISO/IEC 19790 :2006 / FIPS 140-2）が規定する広い定義を採用する

(2) 攻撃対象は、実装者が指定する特定の一段に限定する
(3) 攻撃対象と DPA の選択関数は応募者が選定し、選定理由の説明を付ける

(iii)対策の有効性確認
(1) 対策の有効性に注目し、実装コストは通常の利用に支障のない範囲であることを確認する
(2) 攻撃コストの上限（例: 10 万波形）を設定し、対策実装(評価用実装 2)と素朴実装(評価用実装 3)に対するサイドチャネル攻撃耐性を評価・比較し、対策の有効性を確認する

2.2 暗号モジュールセキュリティ要件の国際標準化への協力

暗号モジュールのセキュリティ要件に関しては、FIPS 140-3 の作成と対応する国際規格 ISO/IEC 19790 の内容が一致するように同期して文書を更新する方針が決まっている。昨年度は、2009 年 12 月に公開された FIPS 140-3 改訂草案に対応する ISO/IEC 19790 の早期改訂の草案 1st WD に対し、暗号実装委員会下のサイドチャネルセキュリティ WG でコメントを作成し、暗号実装委員会の確認を経て提出した。

今年度も、2nd WD(2010 年 7 月発表)と 3rd WD(2011 年 1 月発表)に対するコメント案を作成した。コメント案は松本委員長が委員を務める ISO/IEC JTC1 SC27/WG3 国内小委員会に提案され、日本コメント案として国際事務局に提出された。

2.3 暗号アルゴリズム危殆化時の緊急対応の検討

暗号技術検討会では、電子政府システムで利用されている暗号アルゴリズムの安全性が急激に低下した時の暗号技術検討会及び各委員会の役割を検討した結果をまとめた。暗号実装委員会ではこれを受け、委員会としての役割について検討し、基本的には暗号方式委員会からの要請を受けて実装に関する評価等を行うことを確認した。暗号実装委員会の判断でアラームを発するケースの可能性も検討したが明確な結論は出ず、検討を継続することが決まった。

2.4 2010 年度サイドチャネルセキュリティワーキンググループの活動

2.4.1 活動目的

暗号モジュールへのサイドチャネル攻撃は、特に IC カードのようなワンチップモジュールにとっては大きな脅威となる。サイドチャネル攻撃の中でも、暗号モジュールの消費電力を計測することで、鍵情報を推定する電力解析攻撃

（DPA[32]攻撃、SPA[33]攻撃、タイミング攻撃等）は、簡便な攻撃環境・リソースで実現することが可能となるため、今後対策の実施が必須となると考えられる。

しかし、サイドチャネル攻撃に対するセキュリティ要件や試験要件は現在作成途上にある。

そこで、サイドチャネルセキュリティワーキンググループでは、実験データを収集・分析し、サイドチャネル攻撃に対するセキュリティ要件、試験要件の検討に資することを目的としている。

2.4.2 今年度の成果概要

本ワーキンググループの前身である平成 18 年度に設置された電力解析実験ワーキンググループのときから、実験用標準評価ボード等に搭載された暗号モジュールについて、電力解析攻撃に関する実験方法と、標準的な試験方法と、安全性の基準の検討を行ってきた。産業技術総合研究所と東北大学が開発した実験用評価ボード SASEBO（Xilinx 版）の利用に加え、平成 20 年度は、新たに FPGA を搭載した SASEBO-G（Xilinx 版）[34]と ASIC[35]を搭載した SASEBO-R（LSI 版）[36]等が開発された。平成 21 年度には、SASEBO-G の FPGA を Virtex-5 LX30/50 バージョンアップし、ロジック容量の増加などの機能追加を行った SASEBO-GII が開発・製品化された。今年度は、IC カードのサイドチャネル攻撃評価試験用に IC カードソケットを装備した SASEBO-W[37]が開発され、これら SASEBO シリーズを中心とするサイドチャネル評価用標準プラットフォームを使ったサイドチャネル攻撃及び防御法に関する実験データの収集を行った。

また、暗号実装委員会からの依頼を受け、暗号モジュールのセキュリティ要件に関する国際規格 ISO/IEC 19790 の早期改訂文書 2nd WD 及び 3rd WD に対する日本コメントの作成に寄与した。

(1) 暗号モジュールセキュリティ要件の国際標準化への協力

---

[32] DPA：Differential Power Analysis（差分電力解析）

[33] SPA：Simple Power Analysis（単純電力解析）

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

[35] ASIC：Application Specific Integrated Circuit

[36] SASEBO-R：TSMC 社の 130nm CMOS ライブラリによって製造された、専用暗号 LSI を搭載した ASIC 版のサイドチャネル攻撃実験用標準評価ボード。ASIC には、6 種類の AES 暗号モジュール（①合成体（暗号化/復号実装），②合成体（暗号化のみ実装），③CASE 文記述（暗号化のみ実装），④AND-XOR1 段（暗号化のみ実装），⑤AND-XOR3 段（暗号化のみ実装），⑥①の FPGA 用ネットリストを使用）と DES，MISTY-1，Camellia，SEED，CAST128，RSA(1024bit)の暗号モジュールを実装している。

[37] SASEBO-W：暗号ハードウェアとして普及している IC カードのサイドチャネル攻撃評価試験用に IC カードソケットを装備し、制御用に Xilinx 社製 FPGA Spartan-6 LX150 を実装したサイドチャネル攻撃実験用標準評価ボード。

暗号モジュールのセキュリティ要件に関しては、FIPS 140-3 の作成と対応する国際規格 ISO/IEC 19790 の内容が一致するように同期して文書を更新する方針が決まっている。昨年度は、2009 年 12 月に公開された FIPS 140-3 改訂草案に対応する ISO/IEC 19790 の早期改訂の草案 1st WD に対してコメントを作成し、暗号実装委員会が内容を確認の後、国内委員会経由で国際事務局に提出された。

今年度も、2nd WD(2010 年 7 月発表)と 3rd WD(2011 年 1 月発表)に対するコメント案を作成した。コメント案は松本委員長が委員を務める ISO/IEC JTC1 SC27/WG3 国内小委員会に提案され、内容の修正なく日本コメント案として国際事務局に提出された。

(2) 電力解析攻撃実験のための評価ボードを利用した研究の調査

産業技術総合研究所 情報セキュリティ研究センター（RCIS）と東北大学大学院 情報科学研究科が開発したサイドチャネル攻撃実験用標準評価ボード（SASEBO）等を使用した、電力解析実験ワーキンググループの委員による、2010 年度の発表をまとめた。

2.4.3 委員構成

サイドチャネルセキュリティワーキンググループ (2010 年 3 月現在)

主査	松本　勉	国立大学法人横浜国立大学　教授
委員（主査代理）	佐藤　証	独立行政法人産業技術総合研究所　研究チーム長
委員	黒川　恭一	防衛大学校　教授
委員	崎山　一男	国立大学法人電気通信大学　准教授
委員	佐伯　稔	三菱電機株式会社　主席研究員
委員	高橋　芳夫	株式会社 NTT データ　シニアエキスパート
委員	田中　秀磨	独立行政法人情報通信研究機構　グループリーダー
委員	角尾　幸保	日本電気株式会社　主席研究員
委員	鳥居　直哉	株式会社富士通研究所　部長
委員	東　邦彦	ルネサスマイクロシステム株式会社 シニアデザインエンジニア
委員	藤崎　浩一	株式会社東芝　研究主務

委員	渡辺　大	株式会社日立製作所　研究員
委員	本間　尚文	国立大学法人東北大学　准教授
委員	山越　公洋	日本電信電話株式会社　研究主任

事務局

独立行政法人　情報処理推進機構
- 山岸　篤弘
- 近澤　武
- 神田　雅透
- 大熊　建司
- 鈴木　幸子

独立行政法人　情報通信研究機構
- 松尾　真一郎
- 黒川　貴司
- 金森　祥子

2.4.4 サイドチャネル攻撃実験のための評価ボードを利用した研究の調査

産業技術総合研究所 情報セキュリティ研究センター（RCIS）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開発したサイドチャネル攻撃実験用標準評価ボード（SASEBO）等を使用した、電力解析実験ワーキンググループの委員による、2010 年度の発表についてまとめた。（表 2.7）

表 2.7 発表論文リスト

	タイトル	学会名・会議名	発表年月日	著者
1	Comparative Power Analysis of Modular Exponentiation Algorithms	IEEE Transactions on Computers	2010.06.01	Naofumi Homma, Atsushi Miyamoto, Takafumi Aoki, Akashi Satoh, and Adi Shamir
2	暗号モジュールの電力差分解析耐性評価における電力モデル等の決定方法	情報処理学会論文誌	2010.06.01	高橋芳夫, 松本勉
3	Hardware Implementations of Hash Function Luffa	HOST[38] 2010	2010.06.14	Akashi Satoh, Ttoshihiro Katashita, Takeshi Sugawara, Takafumi Aoki, and Naofumi Homma
4	Secure Implementation of Cryptogpraphic Modules -Development of Standard Evaluation Environment for Side Channel Attacks-	Synthesiology[39]	2010.07.01	Akashi Satoh, Toshihiro Katashita, and Hirofumi Sakane
5	暗号 LSI の電源ノイズシミュレーションによるサイドチャネル解析	DICOMO[40] 2010	2010.07.09	片下 敏宏, 佐藤 証, 永田 真, 藤本 大介
6	Electromagnetic Information Leakage for Side-Channel Analysis of Cryptographic Modules	EMC[41]2010	2010.07.27	Naofumi Homma, Takafumi Aoki, Akashi Satoh
7	Development of an on-chip micro shielded-loop probe to evaluate performance of magnetic film to protect a cryptographic LSI from electromagnetic analysis	EMC2010	2010.07.27	Yu-ichi Hayashi, Takeshi Sugawara, Yoshiki Kayano, Naofumi Homma, Takaaki Mizuki, Akashi Satoh, Takafumi Aoki, Shigeki Minegishi, Hideaki Sone, Hiroshi Inoue
8	Information Leakage from Cryptographic Hardware via Common-Mode Current	EMC 2010	2010.07.27	Yu-ichi Hayashi, Takeshi Sugawara, Yoshiki Kayano, Naofumi Homma, Takaaki Mizuki, Akashi Satoh, Takafumi Aoki, Shigeki Minegishi, Hideaki Sone, Hiroshi Inoue
9	Multiple-Valued Costant-Power Adder and Its Application to Cryptographic Processor	電子情報通信学会英文論文誌 D	2010.08.01	Naofumi Homma, Yuichi Baba, Atsushi Miyamoto, and Takafumi Aoki
10	Profiling Attack using Multivariate Regression Analysis	ELEX[42]	2010.08.19	Takeshi Sugawara, Naofumi Homma, Takafumi Aoki, and Akashi Satoh
11	Fault Sensitive Analysis	CHES[43] 2010	2010.08.25	Li Yang, Kazuo Sakiyama, Shigeto Gomisawa, Toshinori Fukunaga, Junko Takahashi,

[38] HOST：International Symposium on Hardware-Oriented Security and Trust（IEEE）
[39] Synthesiology：シンセシオロジー（産業技術総合研究所）
[40] DICOMO：Multimedia, Distributed, Cooperative, and Mobile Symposium（情報処理学会）
[41] EMC：International Symposium on Electromagnetic Compatibility（電子情報通信学会）
[42] ELEX：IEICE Electronics Express（電子情報通信学会）
[43] CHES：Workshop on Cryptographic Hardware and Embeded Systems（IACR）

				and Kazuo Ohta
12	Combination of SW Countermeasure and CPU Modification on FPGA Against Power Analysis	WISA[44] 2010	2010.08.26	Daisuke Nakatsu, Li Yang, Kazuo Sakiyama, and Kazuo Ohta
13	楕円曲線暗号ハードウェアの電力解析による安全性評価	電気関係学会東北支部連合大会	2010.09.10	齋藤 和也, 菅原 健, 本間 尚文, 青木 孝文, 佐藤 証
14	暗号ハードウェアの局所情報と電磁波解析 (その２)	ISEC[45]	2010.09.07	森田 秀一, 松本 勉, 高橋 芳夫, 四方 順司
15	AES に実装されたレジスタに対する相互情報量解析の適用	FIT[46] 2010	2010.09.07	若林邦爾, 岩井啓輔, 黒川恭一
16	対数モデルを用いた相関電力解析	FIT 2010	2010.12.01	櫻井敦規, 黒川恭一, 岩井啓輔
17	近磁界測定によるサイドチャネル評価実験	SLDM[47]	2010.12.01	片下 敏宏, 堀 洋平, 佐藤 証
18	確率密度関数の推定法と MIA 成功率に関する一考察	SLDM	2010.12.01	堀 洋平, 吉田 隆弘, 片下 敏宏, 佐藤 証
19	Fault Analysis on Stream Cipher MUGI	ICISC[48] 2010	2010.12.03	Junko Takahashi, Toshinori Fukunaga, and Kazuo Sakiyama
20	対数モデルを用いた CPA に対するローパスフィルタの適用	ISEC	2010.12.15	櫻井敦規, 岩井啓輔, 黒川恭一
21	組合せを利用する分類法を用いた相互情報量解析	ISEC	2010.12.15	若林邦爾, 岩井啓輔, 黒川恭一
22	Power Analysis against a DPA-resistant S-box Implementation Based on the Fourier Transform	電子情報通信学会英文論文誌 A	2011.01.01	Yang Li, Kazuo Sakiyama, Shinichi Kawamura, and Kazuo Ohta
23	べき乗剰余演算に対する故障注入を用いた電力解析攻撃	SCIS[49]	2011.01.25	遠藤 翔, 本間 尚文, 菅原 健, 青木 孝文
24	暗号ハードウェアの局所情報と電磁波解析 (その 3)	SCIS	2011.01.26	森田 秀一, 松本 勉, 高橋芳夫, 四方順司
25	電磁波を用いた電源線からのフォールト攻撃	SCIS	2011.01.27	林 優一,菅原 健, 本間 尚文, 水木 敬明, 青木 孝文, 曽根 秀昭
26	ブロック暗号に対する Access-driven キャッシュ攻撃の一考察	SCIS	2011.01.26	高橋順子, 福永利徳
27	異なる電力解析攻撃対策を施したＡＥＳ暗号回路のセキュリティ比較	SCIS	2011.01.27	三村 英伸, 松本 勉
28	An on-chip glitchy-clock generator and its application to safe-error attack	COSADE[50] 2011	2011.02.25	Sho Endo, Takeshi Sugawara, Naofumi Homma, Takafumi Aoki, and Akashi Satoh
29	Enhancement of Simple Electro-Magnetic Attacks by Pre-characterization in Frequency Domain and Demodulation Techniques	DATE 2011[51]	2011.03.17	金 用大, 菅原 健, 本間 尚文, 青木 孝文(東北大学), 佐藤 証 (産業技術総合研究所情報セキュリティ研究センター)

[44] WISA：International Workshop on Information Security Applications
[45] ISEC：情報セキュリティ研究会（電子情報通信学会）
[46] FIT：情報科学技術フォーラム（情報処理学会）
[47] SLDM：システム LSI 設計技術研究発表会（情報処理学会）
[48] ICICS：International Conference on Information and Communications Security
[49] 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）
[50] COSADE：International Workshop on Constructive Side-Channel Analysis and Secure Design
[51] DATE：Design, Automation and Test in Europe（ACM）

2.5　今後の課題

2.5.1　電子政府推奨暗号リスト改訂のための、ハードウェア及びソフトウェア実装性評価

(1)「実装性能評価」の実施要項作成と実施

(2)「サイドチャネル攻撃に対する対策実現の確認」の実施要項作成と実施

2.5.2　サイドチャネル攻撃のセキュリティ要件の検討

(1) ISO/IEC 19790 及び 24759 早期改定案へのコメント作成

2.5.3　サイドチャネルセキュリティワーキンググループよる実験

(1) 暗号モジュールへの最適なサイドチャネル攻撃の実験方法の検討

第 3 章　開催状況

3.1　暗号実装委員会の開催状況

2010 年度の暗号実装委員会は、計 3 回開催された。各回会合の概要は表 3.1 のとおりである。

表 3.1　2010 年度暗号実装委員会の開催状況

回	開催日時	主な議題
第 1 回	平成 22 年 7 月 23 日 10:00～12:30	暗号実装委員会活動計画 サイドチャネルセキュリティワーキンググループ活動計画 応募暗号技術の実装評価に関する検討
第 2 回	平成 22 年 9 月 28 日 15:30～17:30	応募暗号技術の実装性能評価法に関する詳細検討 応募暗号技術のサイドチャネル攻撃対策可能性の確認法に関する詳細検討 ISO/IEC 19790 の 2nd WD コメント提出
第 3 回	平成 23 年 3 月 4 日 16:00～18:00	応募暗号技術の実装性能評価法に関する詳細検討 応募暗号技術のサイドチャネル攻撃対策可能性の確認法に関する詳細検討 暗号アルゴリズム危殆化時の緊急対応の検討

3.2　サイドチャネルセキュリティワーキンググループの活動状況

2010 年度のサイドチャネルセキュリティワーキンググループでは、平成 22 年 8 月と平成 23 年 2 月に、暗号モジュールのセキュリティ要件の国際標準規格 ISO/IEC 19790 の早期改訂ドラフト 2nd WD と 3rd WD をメール審議により作成した。

また、年度末にはサイドチャネル攻撃に関係する研究成果の報告を収集した。

付録

付録 1　早期改訂 ISO/IEC 2nd WD 19790 に対するコメント

CRYPTREC comments on ISO/IEC 2nd WD 19790

Date: 2010-08-25	Document: **SC 27 N8776**

1	2	(3)	4	5	(6)	(7)
NB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the NB**	**Proposed change by the NB**	**Resolution on each comment**
JP 1 [	7.1	Table 1	ed	Line “Self-Tests” ...and critical functions tests.	Please replace “functions tests” to “function test”	•
JP 2	7.4.1	Para 4	ed	...built in self-test (BIST) “BIST” is used only in this sentence.	Remove the abbreviation.	•
JP 3	7.4.2	Para 3	ed	(In the itemize environment) Item 2 and 4 use periods after the headings while the others use colons.	Unify the notations.	•
JP 4	7.4.2	Para 3	ed	(In the itemize environment) The headings of the items 3 to 5 use imperative while the others use nominal.	Unify the notations.	•
JP 5	7.4.3	Para 2, 2nd type, last line	ed	“previously authorised..” two periods	Please delete an extra period.	•
JP 6	7.4.3	Para 5, item 3	te	The 3rd bullet is written as follows. “For each attempt to use the approved authentication mechanism, **the probability** shall [04.45] meet the strength of the authentication objective. For multiple attempts to use the approved authentication mechanism during a one-minute period, the probability shall [04.46] meet the strength	Please define “**the probability**” clearly or describe the contents of the probability. (e.g. False Acceptance Rate)	•

3 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 3, 4 are compulsory.

1	2	(3)	4	5	(6)	(7)
NB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the NB**	**Proposed change by the NB**	**Resolution on each comment**
				of the authentication objective." The definition of "the probability" is not clear.		
JP 7	7.4.3	Para 5, item 4	ed	The 4th bullet: (e.g., password sise restrictions).	Please replace "sise" with "size".	•
JP 8	7.5	Para 1,	ed	The 1st bullet is written as follows. all software and firmware shall [05.03] be in a form that satisfies the requirements of this international standard without modification prior to installation (Clause 7.11.7); Clause 7.11.7 (End of Life) may be nothing to do with the above description. Clause 7.11.6 is appropriate.	Please replace "(Clause 7.11.7)" with "(Clause 7.11.6)".	•
JP 9	7.5	SECURITY LEVEL 2, Para1, 2nd bullet	te	"not easily human readable" is ambiguous.	Please express more clearly.	•
JP 10	7.6.1	Para 4, 2.A 3rd line	te	"in a programmable device (e.g., a programmable hardware module)" "a programmable device" is the same meaning as "a programmable hardware module". The	Please replace "a programmable device" with "a programmable hardware module" and delete (e.g).	•

3 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 3, 4 are compulsory.

1	2	(3)	4	5	(6)	(7)
NB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the NB**	**Proposed change by the NB**	**Resolution on each comment**
				description of e.g. is redundant.		
JP 11	7.6.1	Para 4, 3.A last part	ed	"e.[space]g."	"e.g."	•
JP 12	7.6.1	Last paragraph	te	"If the operational environment is *non-modifiable* or a *limited* operational environment, only the operating system requirements in Clause 7.6.1 shall [06.01] apply." There is no requirement in Clause 7.6.1 itself. Not "Clause 7.6.1" but "Clause 7.6.2" is appropriate.	Please replace "Clause 7.6.1" with "Clause 7.6.2".	•
JP 13	7.6.1	Last paragraph	te	"If the operational environment is a modifiable operational environment, the operating system requirements in Clauses 7.6.1 and 7.6.2 shall [06.02] apply." "Clause 7.6.1" and "Clause 7.6.2" are nothing to do with "a *modifiable* operational environment". The contents of "a *modifiable* operational environment" are described in Clause 7.6.3.	Please delete "Clause 7.6.1", and replace "Clause 7.6.2" with "Clause 7.6.3".	•
JP 14	7.7.1	four lines above Table	ed	There are two periods at the end of the sentence.	Please delete an extra period.	•

3 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 3, 4 are compulsory.

CRYPTREC comments on ISO/IEC 2nd WD 19790

Date: 2010-08-25	Document: **SC 27 N8776**

1	2	(3)	4	5	(6)	(7)
NB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the NB**	**Proposed change by the NB**	**Resolution on each comment**
		3				
JP 15	7.7.1	Table 3	te	It is difficult to see if protection against side-channel attacks is needed or not from the table.	The contents of Clause 7.8 and Annex F, which describes the requirements on side-channel attack protections, should be included in the table.	●
JP 16	7.7.1	Table 3, Security Level 2, General Requirements	ed	“holes are slits”	Please replace “holes are slits” with “holes and slits.”	●
JP 17	7.7.3.2	The last line	ed	The period comes off.	Please add a period.	●
JP 18	7.10.1	Para 6	te	There is a possibility that the user of a cryptographic module needs to know whether the module is in a self-test.	Add a sentence that “If the user of a cryptographic module needs the indicator for self-tests, the module may output a self-test indicator during the self-test.	●
JP 19	7.10.3.1	Para 2,	te	It is required that if a cryptographic module has two independent implementations of the same cryptographic	Add a bulleted requirement that “if a	●

3 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 3, 4 are compulsory.

CRYPTREC comments on ISO/IEC 2nd WD 19790

Date: 2010-08-25	Document: **SC 27 N8776**

1	2	(3)	4	5	(6)	(7)
NB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the NB**	**Proposed change by the NB**	**Resolution on each comment**
		bullet		algorithm, the outputs of the two implementations shall be continuously compared. But, a cryptographic module can have 3 or more independent implementations.	cryptographic module includes three or more independent implementations of the same cryptographic algorithm, then the module shall continuously compare the outputs of all the implementations, and, if at least one of the outputs of the implementations is not equal, the cryptographic algorithm test shall fail."	

3 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 3, 4 are compulsory.

付録 2　早期改訂 ISO/IEC 3rd WD 19790 に対するコメント

CRYPTREC comments on ISO/IEC 3rd ISO/IEC WD 19790

Date: 2011-02-16	Document: **SC 27 N9052**

1	2	(3)	4	5	(6)	(7)
NB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the NB**	**Proposed change by the NB**	**Resolution on each comment**
JP 1	7.2.3.2	Last paragraph, Line 3	te	"enter" seems to be incoherent	"leave a degraded mode operation"	
JP 2	7.3.2	Item 2, Line 1	te	Exception seems to include "control data output"	In parentheses add "and control data output via the control output interface"	
JP 3	7.4.2	5. of the list	ed	"Perform Zeroise"	"Perform zeroisation"	
JP 4	7.4.2.2	Paragraph 1, Line 2	ed	"…Approved security functions…" A capital is used not at line head.	…approved security functions…	
JP 5	7.4.2.2	The first item of the list	te	No description about inactivation.	Check if undesirable inactivation is a threat.	
JP 6	7.4.3	6th para	te	If the cryptographic module uses security functions to authenticate the operator, then those security functions **shall [04.45]** be approved security functions. Is the last word "security functions" equal to the former "those security functions"? The meaning of this passage is not well defined.	Please insert an article (a, the, some, or something) before the last "security functions".	
JP 7	7.6.1	Table 2	te	The information about "Operational Environment" is lacking. Although the 2nd paragraph of page 39 mentions the example (firmware and software).	Please indicate the examples of "Non-Modifiable", "Limited" and "Modifiable" in this table.	
JP 8	7.6.3	Line 14 in page 41	te	・ modifications, accesses, deletions, and additions of cryptographic data and SSPs; ・ attempts to provide invalid input for Crypto Officer functions; ・ addition or deletion of an operator to and from a Crypto Officer role (if those roles are managed the cryptographic module);	Please indicate the examples of these bullets. (e.g. What is the "a security-relevant Crypto Officer function" in 4th bullet?)	

CRYPTREC comments on ISO/IEC 3rd ISO/IEC WD 19790

Date: 2011-02-16	Document: **SC 27 N9052**

1	2	(3)	4	5	(6)	(7)
NB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the NB**	**Proposed change by the NB**	**Resolution on each comment**
				・ the use of a security-relevant Crypto Officer function; ・ requests to access authentication data associated with the cryptographic module; ・ the use of an authentication mechanism (e.g., login) associated with the cryptographic module; and ・ explicit requests to assume a Crypto Officer role. What are the examples of theses bullets except for 6th bullet (e.g., login)?		
JP 9	7.6.3	Last para	ed	"The audit record should be protected against unauthorized modification through the use of an approved security function." The font size of this passage is smaller than other sentences.	Please coordinate the font size of this passage with other sentences.	

発行日　2011 年 6 月 20 日第 1 版
発行者

- **〒113-6591**
  東京都文京区本駒込二丁目 28 番 8 号
  独立行政法人 情報処理推進機構
  （セキュリティセンター 暗号グループ）
  INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN
  2-28-8 HONKOMAGOME, BUNKYO-KU
  TOKYO, 113-6591 JAPAN

- 〒184-8795
  東京都小金井市貫井北四丁目 2 番 1 号
  独立行政法人 情報通信研究機構
  （ネットワークセキュリティ研究所 セキュリティ基盤研究室、
  セキュリティアーキテクチャ研究室）
  NATIONAL INSTITUTE OF
  INFORMATION AND COMMUNICATIONS TECHNOLOGY
  4-2-1 NUKUI-KITAMACHI,KOGANEI
  TOKYO,184-8795 JAPAN