CRYPTREC Report 2011

平成 24 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 2011 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効果確認作業を進めた。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実装攻撃技術および対策技術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。

2012 年 3 月

暗号実装委員会　委員長　本間　尚文

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。

2011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。

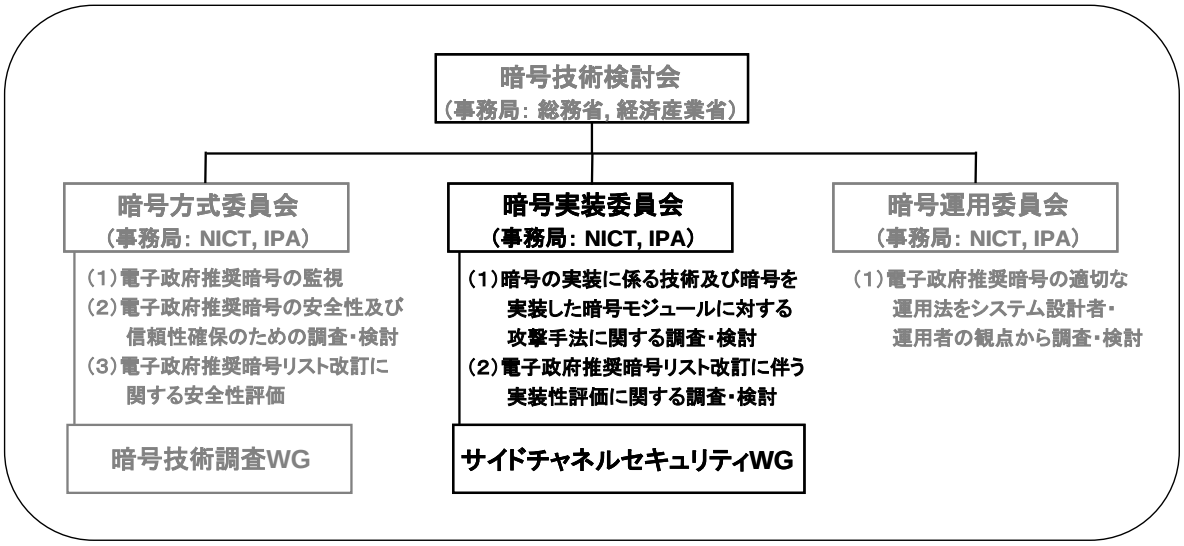


図１　2011 年度の CRYPTREC の体制

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

委員名簿

暗号実装委員会 （2012 年 3 月現在）

委員長	本間　尚文	国立大学法人東北大学　准教授
委員	植村　泰佳	電子商取引安全技術研究組合　専務理事
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	一般財団法人日本情報経済社会推進協会 センター長
委員	川村　信一	独立行政法人産業技術総合研究所　副所長 （2011 年 10 月より）
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　順子	日本電信電話株式会社　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	松崎　なつめ	パナソニック株式会社　チームリーダ
委員	松本　勉	国立大学法人横浜国立大学　教授
委員	渡辺　大	株式会社日立製作所　　主任研究員

オブザーバ

中山　慎一	内閣官房　情報セキュリティセンター（2011 年 7 月より）
岡野　孝子	警察大学校　警察情報通信研究センター
松宮　志麻	総務省　行政管理局
水野　伸太郎	総務省　情報流通行政局（2011 年 10 月まで）
佐々木　信行	総務省　情報流通行政局（2011 年 9 月まで）
谷岡　大祐	総務省　情報流通行政局（2011 年 7 月まで）
飯田　恭弘	総務省　情報流通行政局（2011 年 10 月より）
鮫島　清豪	総務省　情報流通行政局（2011 年 9 月より）
樋口　有二	総務省　情報流通行政局（2011 年 7 月より）
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
江口　純一	経済産業省　商務情報政策局

池西　淳　　経済産業省　商務情報政策局（2011 年 5 月まで）
守山　速飛　　経済産業省　商務情報政策局（2011 年 5 月より）
森川　淳　　経済産業省　商務情報政策局
坂下　圭一　　防衛省　運用企画局
佐藤　史生　　防衛省　技術研究本部
滝澤　修　　独立行政法人　情報通信研究機構

事務局

独立行政法人　情報処理推進機構
笹岡　賢二郎
近澤　武
山岸　篤弘
小暮　淳
神田　雅透
大熊　建司
恵本　健亮
鈴木　幸子

独立行政法人　情報通信研究機構
高橋　幸雄
近藤　玲子（2011 年 7 月まで）
沼田　文彦（2011 年 9 月より）
田中　秀磨（2011 年 12 月まで）
松尾　真一郎
野島　良
大久保　美也子
箕輪　正
黒川　貴司
金森　祥子
多賀　文吾

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会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討を行うことを目的として設立された。

---

[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）

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

[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

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。

2010 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決定

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能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。

(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決定

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 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 及び ISO/IEC 24759 の早期改訂草案を 8 月と 2 月の 2 回に渡って作成し、ISO/IEC SC27/WG3 国内小委員会に提出した。

1.3.2　2011 年度の活動概要

2011 年度暗号実装委員会の成果

2011 年度は、電子政府推奨暗号リスト改訂に向けた実装評価と暗号モジュールに関する国際標準策定への協力を実施した。

(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、ソフトウェア実装及びハードウェア実装の性能評価の実施

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ソフトウェア実装及びハードウェア実装での性能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。

第 2 章　2011 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、実装評価の実施

2.1.1　実装性能評価の概要

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。今年度は昨年度に決定した方針を基に、「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」を実施した。

ソフトウェア実装においては、性能評価項目として、処理速度を中心に初期化時間や使用するメモリ量を測定した。

ハードウェア実装においては、性能評価項目として、クリティカルパス遅延やスループット、実装サイズなどを測定するとともに、サイドチャネル攻撃への対策可能性を検証するため、対策版と未対策版の各々に対する攻撃の有効性と対策コストの評価を行った。

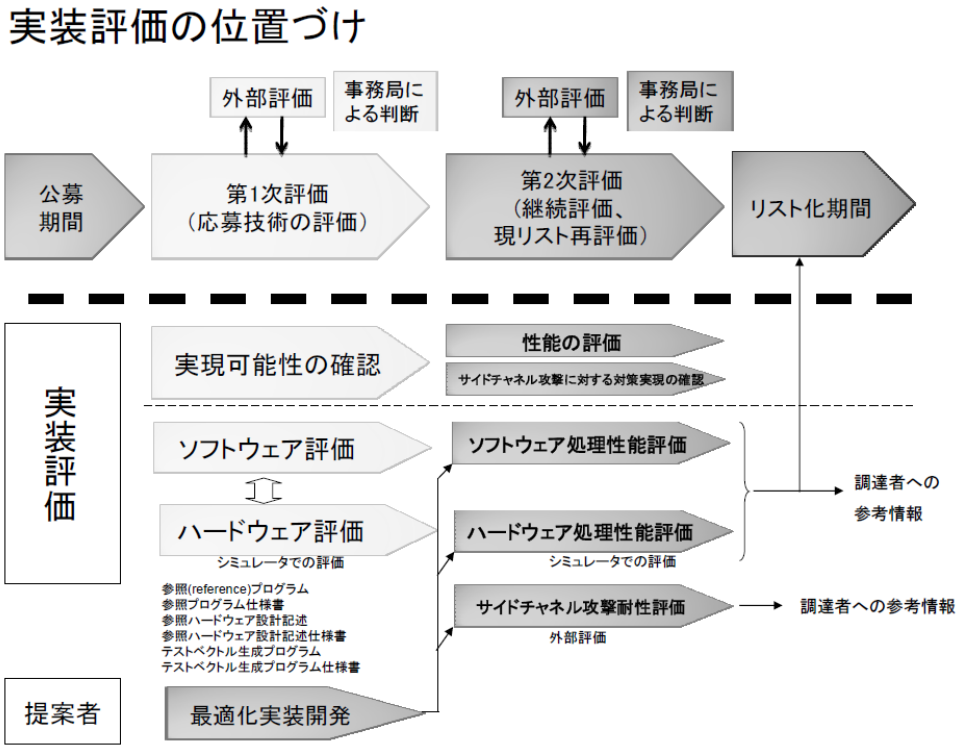


図 2.1　実装性能評価の位置づけ

2.1.2　ソフトウェア実装評価の実施要項の決定

今回のソフトウェア実装評価において、新規暗号の応募者向けに、評価内容と評価用実装の作成法をまとめた実装性能評価要項を作成し、実施状況に応じて内容を改訂しつつ、評価を実施した。以下に内容について記す。

(1) ソフトウェア実装評価の目的

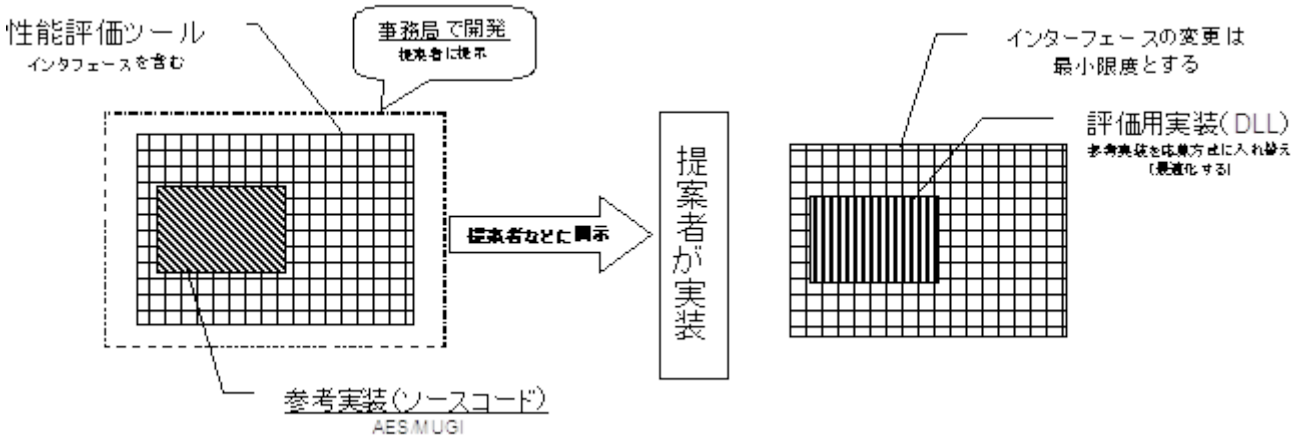
今回のソフトウェア実装評価は、Intrinsic 命令など特殊な専用命令を使用せず、通常の実装テクニックを利用して作成した C++のソースコードで、どの程度の処理速度が出るかを調べ、暗号利用者への参考情報とすることを主目的とする。既存の電子政府推奨暗号との性能比較は行うが、大まかに速いか遅いかを見るに留め、僅かな差で優劣を付けるものではない。

(2) 用語と評価のイメージ

参考実装：応募暗号方式を実装する際に参考とする暗号プリミティブのソースコード

性能評価ツール：事務局から提示する、参考実装と実装評価機能・インターフェースを含む雛形

評価用実装 :サンプル実装の参考実装の部分を応募暗号用に書き換えた評価用の実装



・ 図 2.2　ソフトウェア実装評価のイメージ

・

(3) 評価スケジュール

2011 年 6 月 10 日 応募者に評価ツールの提供と修正後のスケジュール通知

2011 年 8 月 15 日 応募者に評価の PC 環境(CPU 等)を通知

2011 年 10 月下～11 月上旬　事務局の評価環境によるトライアル実施。日程は応募者と調整予定。

2011 年 11 月 18 日 応募者による実装提出
2011 年 12 月評価実施

(4) 実装環境等（プラットフォーム／OS／使用言語）

(A) Intel x86 CPU 搭載の PC 環境
CPU: インテル Core i5-480M (2.66 MHz)
メモリ: DDR3 SDRAM, 4GB
(B) OS は Windows 7 の 32 ビット版のみとする
(C) Visual Studio を開発環境とし、Visual C++ 2010 (10.0) SP1 を使用
(D) インライン・アセンブラの使用は禁止
(E) SSE/SSE2 等の Intrinsic 命令の使用は禁止

(5) 実装条件等

(A) 鍵長
ブロック暗号・ストリーム暗号・動作モードとも 128 ビット鍵を評価対象とする。他の鍵長もサポートして良いが、メインの性能評価ではなく、参考情報としての扱いとなる。
(B) 最適化
高速実装を性能評価対象とする。
使用メモリ量は測定するが、他方式と比較し極端に大きな値でない限り問題としない。
(C) 評価項目
(ア) カテゴリ共通
① 状態の初期化に掛かる時間(クロック数の平均値等)。例えばストリーム暗号の場合、鍵と IV 設定の両方に要する時間
② プログラムサイズ（DLL ファイル） （通常の利用において支障のない範囲であることを確認）
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）
(イ) ブロック暗号
① 暗号化と復号の処理時間(クロック数の平均値等)
② 平文長は、16 bytes, 64 bytes, 576 bytes, 1,536 bytes, 4,096 bytes, 16,384 bytes, 1,048,576 bytes(=1MB) の 7 種類
(ウ) ストリーム暗号
① 暗号化と復号の処理時間(クロック数の平均値等)
② 平文長は、8 bytes, 64 bytes, 576 bytes, 1,536 bytes, 4,096 bytes, 16,384 bytes, 1,048,576 bytes(=1MB) の 7 種類
(エ) (4) メッセージ認証コード

① 認証コードの生成時間、検証時間(クロック数の平均値等)
② 平文長は、8 bytes, 64 bytes, 576 bytes, 1,536 bytes, 4,096 bytes, 16,384 bytes, 1,048,576 bytes(=1MB) の 7 種類

(6) 事務局が提供する実装情報

(A) 暗号ライブラリ作成用ファイル一式
(ア) プロジェクト・ファイル、ヘッダーファイル、ソースコード
暗号プリミティブのソースコードは次を含む
(イ) AES(ECB)、MUGI、AES-CMAC
(ウ) 作成のための文書（外部仕様書、関数説明書、取扱説明書、内部設計書）
(B) 実装評価環境用ファイル一式

(7) 応募者の提出物

(A) 評価用実装（高速実装）
(ア) DLL での提出を想定し、ソースコードは要求しない
(イ) 測定箇所は関数呼び出しで設定
(ウ) 高速版を評価する
(B) インターフェースの変更に関する記述（変更がなければ不要）
(C) 自己評価書
(ア) 応募時以降の評価結果。応募者以外の実装も記載可。提出は義務としない
(D) 誓約書
(ア) 本評価要項の記載通りに実装したことを誓約

2.1.3 ハードウェア実装評価の実施要項の決定

今回のハードウェア実装評価において、新規暗号の応募者向けに、評価内容と評価用実装の作成法をまとめた実装性能評価要項を作成し、実施状況に応じて内容を改訂しつつ、評価を実施した。以下に内容について記す。

(1) ハードウェア実装評価の目的

今回のハードウェア実装評価は、FPGA 実装において次の２点を評価することを目的とする。

(A) 処理速度の測定
(B) サイドチャネル攻撃への対策可能性の確認

速度評価については既存の電子政府推奨暗号との性能比較は行うが、

大まかに速いか遅いかを見るに留め、僅かな差で優劣を付けるものではない。サイドチャネル攻撃対策可能性については、攻撃耐性が改善し、かつ、対策のオーバーヘッドが大き過ぎないことを確認する。評価結果は、暗号利用者への参考情報とするべく公開する。

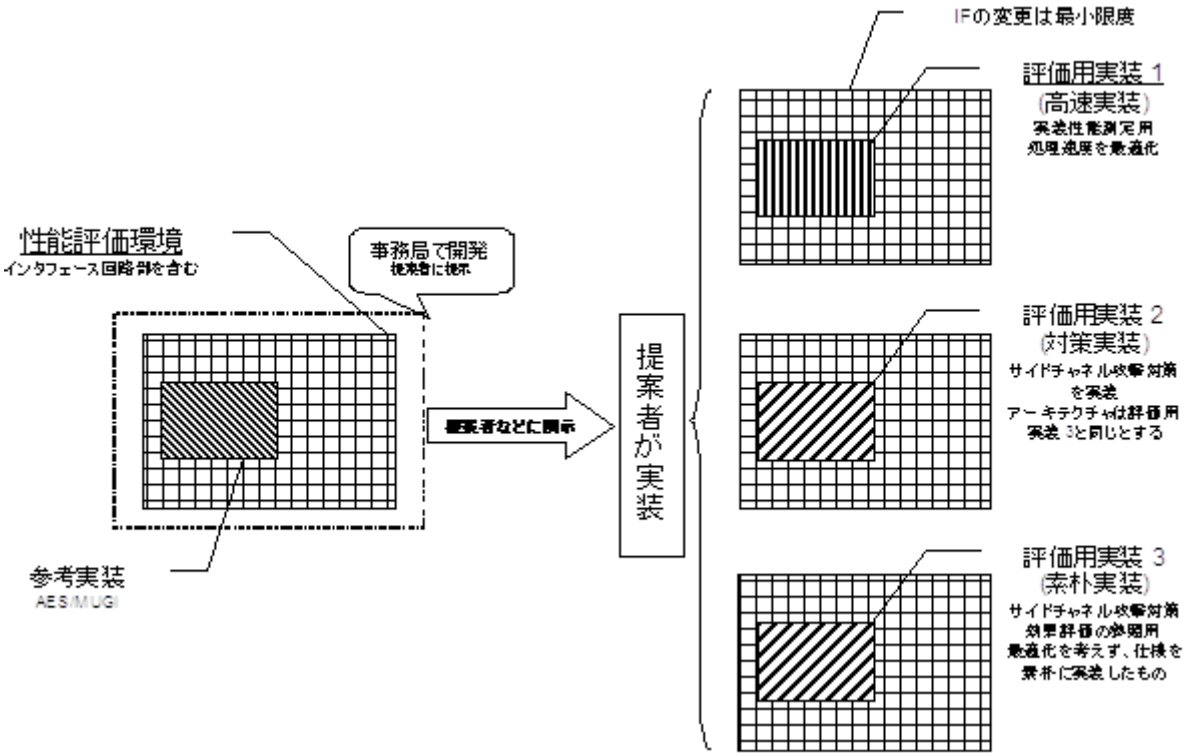
評価対象のカテゴリは、(A)については、ブロック暗号、ストリーム暗号、メッセージ認証コード、(B)についてはブロック暗号とストリーム暗号とする。

(2) 用語と評価のイメージ

参考実装：応募暗号方式を実装する際に参考とする暗号プリミティブの実装

性能評価ツール：事務局から提示する参考実装とインターフェース回路などの性能評価用の周辺回路からなる雛形

評価用実装 ：サンプル実装の参考実装の部分を応募暗号用に書き換えた評価用の実装で、次の３種類で構成される



※ストリーム暗号用の参考実装は、MUGI と同じインターフェイスを持ち、常に 0 を出力する Null cipher のソースコードを提供する。

・ 図 2.3　ソフトウェア実装評価のイメージ

・評価用実装 1 （高速実装）：
処理速度について最適化した実装
・評価用実装 2 （対策実装）：
サイドチャネル攻撃対策を施した実装で、アーキテクチャは評価用実装3と基本的に同じであるもの
・評価用実装 3 （素朴実装）：
サイドチャネル攻撃対策の効果を評価するための基準とする実装で次の2つを満たす。
・アルゴリズム仕様書から自然に導かれる素直な構成を取る
・サイドチャネル攻撃対策は行わない
・評価用実装1と共通でも良い。その場合、そのことを明記すること。

(3) 評価スケジュール

2011 年 8 月 15 日 応募者にハードウェア実装性能評価要項の提供と修正後スケジュール通知
2011 年 12 月 15 日 応募者による実装提出
2011 年 12 月 15 日～2012 年 1 月 31 日評価実施

(4) 実装環境等

(A) プラットフォーム環境
・Xilinx Virtex-5 LX50(SASEBO-GII 搭載の FPGA)
(B) 開発環境等
・ISE WebPACK Version 12.4
(C) 評価で参考とする仕様書、説明書等
・CD-ROM と Web ページで配布

(5) 実装性能評価項目等 （評価用実装１）

(A) 鍵長
(ア) 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。
(イ) ブロック暗号は ECB モードのみとする。
(ウ) メッセージ認証コードについては、応募者の推奨値を評価対象とする。
(エ) 他の鍵長については、自己評価結果として提出可とする。
(B) 最適化
(ア) 高速実装を評価対象とする。
(イ) 小型実装等については、自己評価結果として提出可とする。
(C) 評価項目

(ア)処理速度(クリティカルパス遅延とクロック数)　(ブロック暗号・ストリーム暗号・メッセージ認証コード共通)

(イ)内部レジスタサイズ(ブロック暗号・ストリーム暗号・メッセージ認証コード共通)

(ウ)プログラムサイズ(スライス数)　(ブロック暗号・ストリーム暗号・メッセージ認証コード共通)

(エ)鍵スケジュールの設定に掛かる時間(ブロック暗号)

(オ)状態の初期化に掛かる時間。初期設定が複数のプロセスに分かれる場合も区別せず、一体とする(ストリーム暗号、メッセージ認証コード)。

・ISE WebPACK で合成して得られるレポートのデータを適宜記載すること

(6) サイドチャネル攻撃対策の有効性確認　(評価用実装２・３を利用)

(A) 鍵長

(ア)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。

(イ)ブロック暗号は ECB モードのみとする。

(ウ)メッセージ認証コードは評価対象としない。

(B) 想定するサイドチャネル攻撃

・攻撃方法は電力解析とする。

(ア)攻撃方法と選択関数は応募者が選定する。

(イ)攻撃箇所は特定の１段とする。

(ウ)選択関数は、素朴実装に対する電力解析で最も少ない波形数で部分鍵を正しく特定できたものとする。

(C) 対策の有効性確認

(ア)対策の有効性に注目し、Xilinx Virtex-5 LX50 で実装可能であることを確認する。

① 対策に使用する乱数生成器は SHA-1 や AES 等を使って設計し、実装の中に組み込むこと。生成される乱数の品質は問わない

(イ)評価用実装３と評価用実装２について、各々10 万波形の測定を行う。測定波形に対し、応募者が提示した選択関数を使って、鍵が正しく推定できるか否か、推定できる場合は正しく推定できる最小の波形数を調べ、両者を比較することによって、対策の有効性を判定する。

(ウ)プログラムサイズ(スライス数)　(ブロック暗号・ストリーム暗号・メッセージ認証コード共通)

(エ) 鍵スケジュールの設定に掛かる時間（ブロック暗号）

(7) 事務局が提供する実装情報

(A) ブロック暗号：参考実装（AES-ECB）
(B) ストリーム暗号：参考実装（Null cipher）
(C) 応募者向けハードウェア実装開発の手引き

(8) 応募者の提出物

(A) ３種類の評価用実装（評価用実装~~1~~2～３）
(ア) 評価用実装２・３については、適切なトリガー(例: 暗号化開始時)を出し、測定点がトリガーからどれだけ後に設定したかの情報提出する。
(イ) ビットファイルの提出を必須とし、ソースコードの提出は求めない。
(B) ISE の合成で出力されるレポートのサマリ情報
(ア) “トップモジュール名.par”を必須とし、その他は任意とする。
(C) シミュレーション波形
(D) タイミングチャート
(E) 電力解析で使用する選択関数（形式は、入力と仮想の電力）
(F) インターフェースの書換えに関する記述（書換えがない場合は不要）
(G) 実装方針の説明（アーキテクチャを記述)
(ア) アーキテクチャ記述は最低限、次のマクロ情報を含むものとする。
(イ) 全体構造(ブロック図)、roll/unroll の区別、実装上の特徴。
(H) 誓約書
(I) 自己評価書（提出は義務としない）

2.1.4 ソフトウェア実装評価の実施状況

ソフトウェア実装の評価対象を図に示す。実装性能の測定は、2009 年度に経済産業省による委託研究「クラウド環境における暗号技術評価」の中で開発された評価ツールを利用する。この委託研究において、図に示した現リスト掲載暗号及びメッセージ認証コードの CMAC (AES-CMAC)の評価用実装が開発されており、これを今回の評価対象とした。新規応募暗号については、各提案企業に評価要項を提示し、2011 年 11 月中旬に実装の提出を受けた。

今回の評価ツールでは、暗号化等の処理時間を、関数呼び出しから終了のコールが届くまでのクロック数として計測するため、暗号処理以外のプロセスの影響を受ける。当初、160 回計測して上下 10%を切り捨てた後、平均値

を取ったが、測定セットごとの平均値の変動が大きかった。そこで、128 回計測した最小値を採用することにしたところ、変動が小さくなった。そこで、128 回の測定を 3 回繰り返し、最小値の平均値を採用することに決定した。測定は 2012 年 2 月までに終了し、第 3 回委員会で検討した。

今回の測定の結果について、暗号実装委員会では評価対象となった全暗号技術について、通常の PC 環境で実用上十分な性能を有すると判断している。しかしながら、実装開発者が一律でなく、今回の測定結果が本来の性能を反映していない可能性がある。このような事情を考慮し、公開方法は慎重に検討する必要があるため、2012 度の継続課題とし、本報告書には記載しないことになった。

2.1.5 ハードウェア実装評価の実施状況

ハードウェア実装の評価対象を図に示す。SASEBO-GII を使った実装性能の評価環境は、産業技術総合研究所・情報セキュリティ研究センターが開発したものを使用した。新規応募暗号については、各提案企業に評価要項を提示し、2012 年 1 月中旬までに実装(ビットファイル)と ISE デザインツールのレポート(抜粋)の提出を受けた。

性能評価測定は、ISE デザインツールのレポートに記載された値を利用し、SASEBO-GII の実機で動作確認を行った。サイドチャネル攻撃への対策可能性については、年度内に終了せず現在実施中である。

2.1.6 暗号運用委員会からの問い合わせ対応

暗号運用委員会では、2011 年度第 2 回委員会において、電子政府推奨暗号リストに採用する暗号技術を選定するための評価項目を仮決定した。その中に当委員会の「ソフトウェア実装性能評価」及び「ハードウェア実装性能評価」も含まれており、当委員会は(A)評価内容、(B)評価の精度、採用評価結果を選定基準として利用することに対する見解を回答するように求められた。(A)については第 3 回暗号運用委員会に向け、評価内容を回答した。(B)と(C)については、第 4 回暗号運用委員会に向けて回答した。

(B)に対しては、2008 年度に公開した「公募要項」を示し、今回の実装評価の目的が、調達者が調達するプラットフォームに要求される仕様（要求条件）を参考情報として提供することであり、暗号選択の選定基準として利用するための精度は持たない旨を回答した。

(C)に対しては、次の 4 つの理由に、単純に評価データだけで性能の優劣を判断することに対して反対する旨を回答した。

(1)評価したプラットフォームが限られている。

(2)評価した項目が限定されている。

(3)既存の電子政府推奨暗号リスト掲載暗号と新規応募暗号の実装者の違い。

(4)今回の結果は暗号の本来の実装性能を反映していない。

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 2011 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

2.3.1 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。

2.3.2 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

[32] DPA：Differential Power Analysis（差分電力解析）
[33] SPA：Simple Power Analysis（単純電力解析）

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 1st CD、及び試験要件に関する国際規格 ISO/IEC 24759 の早期改訂文書 1st WD と 2nd WD に対する日本コメントの原案を作成した。

(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

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。

2011 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/IEC19790 の早期改訂の草案 1st CD(2011 年 9 月発表)に対するコメント案を作成した。また、FIPS 140-3 の試験要件(DTR)に対応する ISO/IEC 24759 の早期改訂の草案 1st WD(2011 年 6 月発表)と 2nd WD(2012 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 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、2011 年度の発表をまとめた。

---

[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。

2.3.3　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 （2012 年 3 月現在）

主査	本間　尚文	国立大学法人東北大学　准教授
委員	川村　信一	独立行政法人産業技術総合研究所　副所長 （2011 年 10 月より）
委員	黒川　恭一	防衛大学校　教授
委員	佐伯　稔	三菱電機株式会社　主席研究員
委員	崎山　一男	国立大学法人電気通信大学　准教授
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　研究室長 （2011 年 12 月まで）
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	松本　勉	国立大学法人横浜国立大学　教授
委員	三宅　秀享	株式会社東芝　研究主務
委員	山越　公洋	日本電信電話株式会社　研究主任
委員	渡辺　大	株式会社日立製作所　主任研究員

事務局

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

独立行政法人　情報通信研究機構
- 松尾　真一郎
- 野島　良

箕輪　正
大久保　美也子
黒川　貴司
金森　祥子
多賀　文吾

2.3.4　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、2011 年度の発表についてまとめた。（表 2.4）

表 2.4　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	多倍長乗算のオペランドに着目した RSA 暗号ハードウェアのサイドチャネル解析	ISEC[38] 2011-8	2011.05.13	岸川剛, 松本勉
2	Revisit Fault Sensitivity Analysis on WDDL-AES	HOST[39] 2011	2011.06.06	Li Yang, Kazuo Ohta, and Kazuo Sakiyama
3	意図的な電磁妨害による暗号モジュールへの故障注入に関する検討	EMC[40], 2011-17, pp.53-57	2011.06.24	林優一, 菅原健, 本間尚文, 水木敬明, 青木孝文, 曽根秀昭
4	Non-Invasive EMI-Based Fault Injection Attack against Cryptographic Modules	ISEMC 2011, pp.763-767	2011.08.18	Yu-ichi Hayashi, Naofumi Homma, Takeshi Sugawara, Takaaki Mizuki, Takafumi Aoki, and Hideaki Sone
5	Identification of Information Leakage Points on a Cryptographic Device with an RSA Processor	ISEMC 2011, pp.773-778	2011.08.18	Olivier Meynard, Sylvain Guilley, Jean-Luc Danger, Yu-ichi Hayashi, and Naofumi Homma
6	Identification of Information Leakage Points on a Cryptographic Device with an RSA Processor	ISEMC 2011, pp.773-778	2011.08.18	Olivier Meynard, Sylvain Guilley, Jean-Luc Danger, Yu-ichi Hayashi, and Naofumi Homma
7	パイロットランプはサイドチャネルとして使えるか？	ISEC 2011-28	2011.09.09	松本勉, 齋藤翔平
8	On the Power of Fault Sensitivity Analysis and Collision Side-Channel Attack in a Combined Setting	CHES[41] 2011	2011.09.30	Amir Moradi, Oliver Mischke, Christof Paar, Yang Li, Kazuo Ohta, Kazuo Sakiyama
9	Uniqueness Enhancement of PUF Responses Based on the Locations of Random Outputting RS Latches	CHES 2011	2011.10.01	Dai Yamamoto, Kazuo Sakiyama, Mitsugu Iwamoto, Kazuo Ohta, Takao Ochiai, Masahiko Takenaka, Kouichi Itoh

[38] ISEC：情報セキュリティ研究会（電子情報通信学会）
[39] HOST：International Symposium on Hardware-Oriented Security and Trust（IEEE）
[40] EMC：International Symposium on Electromagnetic Compatibility（電子情報通信学会）
[41] CHES：Workshop on Cryptographic Hardware and Embeded Systems（IACR）

10	First Experimental Results of Correlation-Enhanced EMA Collision Attack	CHES 2011, Poster Session	2011.09.29	Toshiki Nakasone, Daisuke Nakatsu, Yang Li, Kazuo Ohta, Kazuo Sakiyama
11	High-performance Architecture for Concurrent Error Detection for AES Processors	IEICE Trans. Fundamentals, Vol. E94-A, No.10, pp.1971-1980, 2011	2011.10	Takeshi Sugawara, Naofumi Homma, Takafumi Aoki, and Akashi Satoh
12	Intentional Electromagnetic Interference for Fault Analysis on AES Block Cipher IC	EMCCOMPO 2011[42] 2011	2011.11.08	Yu-ichi Hayashi, Shigeto Gomisawa, Yang Li, Naofumi Homma, Kazuo Sakiyama, Takafumi Aoki, and Kazuo Ohta
13	クロック間衝突を用いた楕円曲線暗号実装に対する故障感度解析	ISEC[43] 2011-49	2011.11.15	阪本光，李陽，太田和夫，崎山一男
14	AAn On-chip Glitchy-clock Generator for Testing Fault Injection Attacks	Journal of Cryptographic Engineering, Vol.1, No.4, pp.265-270	2011.12	Sho Endo, Naofumi Homma, Takeshi Sugawara, Takafumi Aoki and Akashi
15	Uniquness Enhancement of PUF Responces Based on the Locations of Random Outputting RS Latches	ISEC 2011-68	2011.12.14	山本大，崎山一男，岩本貢，太田和夫，落合隆夫，武仲正彦，伊藤孝一
16	マスク対策 AES に対する誤り暗号文を用いた故障感度解析～CHES2011 での発表のレビュー～	ISEC 2011-66	2011.12.14	李陽，太田和夫，崎山一男
17	Differential Fault Analysis on Stream Cipher MUGI	IEICE Trans. Fundamentals, Vol.E95-A, No.1, 2012	2012.01	Junko Takahashi, Toshinori Fukunaga, and Kazuo Sakiyama
18	容量充電モデルを用いた高速なサイドチャネル攻撃評価手法	SCIS[44] 2012, 1C2-6	2012.01.30	藤本大介，永田真，片下敏宏，佐々木明彦，堀洋平，佐藤証
19	対策済み AES に対するサイドチャネル攻撃手法の有効性評価	SCIS2012, 2C1-5	2012.01.31	早崎拓馬，伊左次優太，猪狩幸大，堀洋平，今井秀樹
20	Threshold Implementation を利用したストリーム暗号 Enocoro-128 v2 の相関電力解析対策	SCIS2012, 2C2-1	2012.01.31	三上修吾，吉田博隆，渡辺大，崎山一男
21	Access-Driven Cache Attack の自動的な攻撃評価手法の提案	SCIS2012, 2C2-2	2012.01.31	高橋順子，阪本光，福永利徳，冨士仁，崎山一男
22	テンプレートを利用した時系列電力解析	SCIS2012, 2C2-5	2012.01.31	中津大介，李陽，太田和夫，崎山一男
23	IR ドロップを利用した故障感度解析と高温環境下における影響	SCIS2012, 2C3-3	2012.01.31	小池彩歌，李陽，中津大介，太田和夫，崎山一男
24	Combined Side-Channel Analysis の性能向上のための CPA と MIA の合成に関する研究	SCIS2012, 2C3-5	2012.01.31	伊左次優太，堀洋平，今井秀樹
25	クロック間衝突を利用した電磁波解析	SCIS2012, 3C1-1	2012.02.01	中曽根俊貴，中津大介，李陽，太田和夫，崎山一男
26	KCipher-2 に対する相関電力解析とその対策	SCIS2012, 3C1-2E	2012.02.01	響崇史，齋藤和也，本間尚文，青木孝文，仲野有登，福島和英，清本晋作，三宅優
27	Sensitive-Data Dependency of Faulty Behavior and Its Application	SCIS2012, 3C1-3E	2012.02.01	李陽，太田和夫，崎山一男
28	暗号機器上のサイドチャネル情報取得性分布図作成の効率化の検討	SCIS2012, 3C2-1	2012.02.01	林優一，水木敬明，本間尚文，曽根秀昭，青木孝文
29	Feistel 型暗号に対するサイドチ	SCIS2012, 3C2-2	2012.02.01	清水秀夫，遠藤つかさ，駒野雄

[42] EMCCOMPO：International Workshop on Electromagnetic Compatibility of Integrated Circuits（IEEE）

[43] ISEC：情報セキュリティ研究会（電子情報通信学会）

[44] 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）

	ャネル攻撃に関する考察			一
30	電力測定機能改良の暗号 LSI 用ボード SASEBO-RII とその評価	SCIS2012, 3C2-5	2012.02.01	片下敏宏, 堀洋平, 佐藤証
31	Fault Sensitivity Analysis のための回路シミュレーション	SCIS2012, 3C3-1	2012.02.01	菅原健, 鈴木大輔
32	オープンソース CPU のサイドチャネル評価	SCIS2012, 3C3-2	2012.02.01	佐伯稔, 鈴木大輔, 菅原健
33	ハミング距離モデルに基づく電力解析攻撃に対するパイプライン処理を用いた耐タンパー手法	SCIS2012, 3C3-4	2012.02.01	山下哲孝, 前川晃, 庄司陽彦, 中村考一, 飯田伴則, 木村隆幸, 角尾幸保
34	Information-Theoretic Approach to Optimal Differential Fault Analysis,	IEEE Trans. Inf. Forensic Secur., Vol.7, No.1, pp.109-120	2012.02	Kazuo Sakiyama, Yang Li, Mitsugu Iwamoto, and Kazuo Ohta
35	New Fault-Based Side-Channel Attack using Fault Sensitivity	IEEE Trans. Inf. Forensic Secur.,Vol.7, No.1, pp.88-97	2012.02	Yang Li, Kazuo Ohta, and Kazuo Sakiyama, “New Fault-Based Side-Channel
36	A proper security analysis method for CMOS cryptographic circuits	IEICE Electronics Express, Vol.9, No.6, pp.458-463	2012.03.25	Yoshio Takahashi, Tsutomu Matsumoto

2.4 今後の課題

2.4.1 電子政府推奨暗号リスト改訂のための、実装性能評価

(1)「実装性能評価」の測定結果をまとめる。

(2)「サイドチャネル攻撃に対する対策実現の確認」のために、実機による測定を行い、結果をまとめる。

2.4.2 サイドチャネル攻撃に関する調査と実験方法の検討

(1) サイドチャネル攻撃に関する研究動向を調査・分析する。

(2) 暗号モジュールに対するサイドチャネル攻撃耐性を評価するための実験方法を検討する。

2.4.3 暗号モジュールのセキュリティ要件の検討

(1) 暗号モジュールのセキュリティ要件に関する標準化動向を調査する。

(2) ISO/IEC 19790 及び 24759 早期改訂案に対するコメントを作成する。

第 3 章　開催状況

3.1　暗号実装委員会の開催状況

2011 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　2011 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	2011 年　9 月 12 日 14:00～16:00	委員長互選 暗号実装委員会活動計画の審議・承認 実装性能評価の進行状況報告
第 2 回	2011 年 12 月 19 日 13:30～15:30	実装性能評価の進行状況報告 ソフトウェア実装性能評価結果の検討 暗号運用委員会からの検討要請対応
第 3 回	2012 年　2 月 13 日 13:30～15:30	実装性能評価の進行状況報告 暗号運用委員会からの検討要請対応 実装評価報告書の作成方針検討

3.2　サイドチャネルセキュリティ WG の開催状況

2011 年度のサイドチャネルセキュリティ WG は、計 3 回開催された。各回会合の概要は表 3.2 のとおりである。

表 3.2　2011 年度サイドチャネルセキュリティ WG の開催状況

回	開催日時	主な議題
第 1 回	2011 年 12 月 19 日 16:00～17:30	サイドチャネルセキュリティ WG 年間活動計画 ISO/IEC 国際標準対応
第 2 回	2012 年　2 月 13 日 16:00～17:00	ISO/IEC 国際標準対応 国際会議等の参加報告

付録

付録１　早期改訂 ISO/IEC 1st CD 19790 に対するコメント

CRYPTREC comments on ISO/IEC 1st CD 19790 (revision)

Date: 2011-08-25	Document: **SC 27 N9581**

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 [	7.7.1	P36, L8	ed	is required at Security Level 4.	are required at Security Level 4.	
JP 2	7					
JP 3						

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.

付録 2　早期改訂 ISO/IEC 1st WD 24759 に対するコメント

CRYPTREC comments on ISO/IEC 1st WD 24759 (revision)

Date: 2011-08-25	Document: **SC 27 N9581**

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"	

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.

付録 3　早期改訂 ISO/IEC 2nd WD 24759 に対するコメント

CRYPTREC comments on ISO/IEC 2nd WD 24759 (revision)

Date: 2011-08-25	Document: **SC 27 N9581**

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	TE02.15.02	Paragraph 6	ed	“if they are do not provide security” grammatical error.	“if they do not provide security ”	
JP 2	TE02.18.02	Paragraph 6	ed	“if they are do not provide security” grammatical error..	“if they do not provide security ”	
JP 3	TE02.21.01	Line 2	ed	“description of the of the non-approved” grammatical error.	“description of the non-approved”	
JP 4	TE02.26.02	Line2	ed	“can only be access” grammatical error.	“can only be accessed”	
JP 5	AS02.32	Line1	ge	“shall not enter a degraded operation” seems to be contrary.	“shall not leave a degraded operation”	
JP 6	TE03.04.01	Line2	ed	“VE03.03.01”	“VE03.04.01”	

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.

発行日　2012 年 5 月 25 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