CRYPTREC Report 2012

平成 25 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 2012 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。

2009 年度からは「電子政府推奨暗号リスト」の改定に対応するため、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、電子政府推奨暗号リスト改定のための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完了した。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をベースとした国際規格で規定されたサイドチャネル攻撃に対する安全性に関する適合試験に関するドラフト 3rd WD ISO/IEC 17825 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した。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定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。

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。

2012 年度以前の CRYPTREC Report は、下記 URL で参照できる。

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

本報告書ならびに上記 Web サイトから入手した CRYPTREC 活動に関する情報の利用に起因して生じた不利益や問題について、本委員会及び事務局は一切責任をもっていない。

本報告書に対するご意見、お問い合わせは、CRYPTREC 事務局までご連絡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。

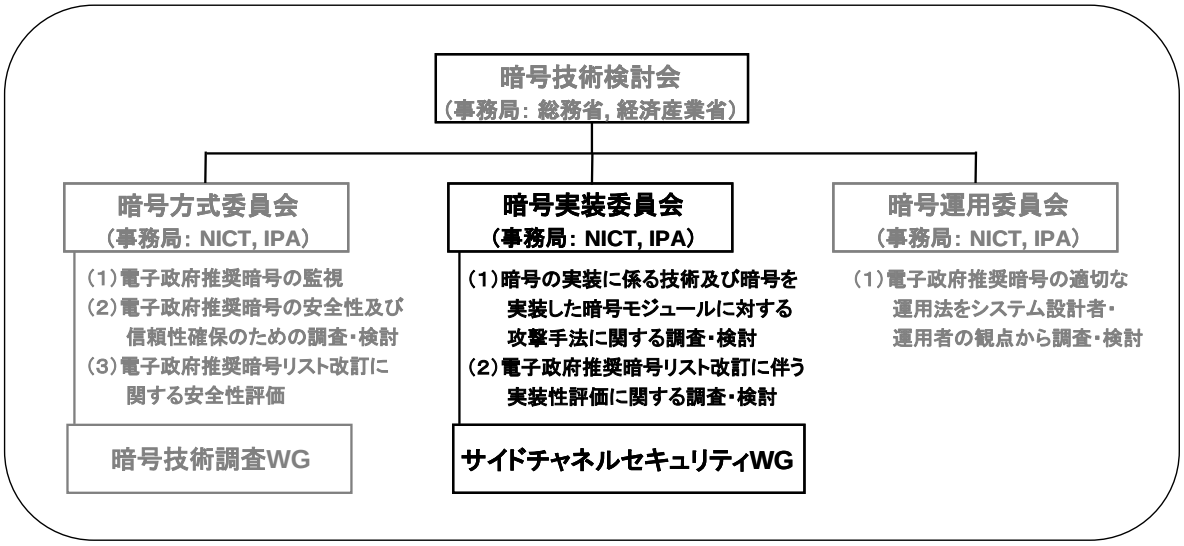


図１　2012 年度の CRYPTREC の体制

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

委員名簿

暗号実装委員会 （2013 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（2012 年 8 月まで）
委員	川村　信一	独立行政法人産業技術総合研究所　招聘研究員
委員	崎山　一男	国立大学法人電気通信大学　准教授
委員	佐藤　恒夫	三菱電機株式会社　グループマネージャー
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	山岸　篤弘	一般財団法人日本情報経済社会推進協会 主席研究員（2012 年 9 月から）
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
岡野	孝子	警察大学校　警察情報通信研究センター
村田	莉衣奈	総務省　行政管理局
上原	哲太郎	総務省　情報流通行政局　(2012 年 8 月から)
飯田	恭弘	総務省　情報流通行政局
鮫島	清豪	総務省　情報流通行政局　(2012 年 8 月まで)
樋口	有二	総務省　情報流通行政局　(2012 年 7 月まで)
吉田	丈夫	総務省　情報流通行政局　(2012 年 8 月から)
橋本	直樹	総務省　情報流通行政局　(2012 年 10 月から)
新谷	祐司	外務省　大臣官房
山中	豊	経済産業省　産業技術環境局

岩永　敏明　　経済産業省　産業技術環境局（2012 年 7 月から）
上村　昌博　　経済産業省　商務情報政策局
森川　淳　　経済産業省　商務情報政策局　（2012 年 11 月まで）
中谷　順一　　経済産業省　商務情報政策局　（2012 年 10 月から）
守山　速飛　　経済産業省　商務情報政策局
坂下　圭一　　防衛省　運用企画局
小森　旭　　防衛省　運用企画局
谷口　晋一　　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
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
高橋　幸雄　（2012 年 9 月まで）
平　　和昌　（2012 年 10 月から）
沼田　文彦
盛合　志帆
松尾　真一郎
野島　良
大久保　美也子
蓑輪　正　　（2013 年 1 月まで）
江村　恵太　（2012 年 8 月から）
黒川　貴司
金森　祥子
多賀　文吾
側高　幸治

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 年度までに改定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、改定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 の改定版である 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定に向け、「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 の改定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定草案が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を改定することが決まり、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定に向け、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の改定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定することで、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 に改定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第 2 次草案は 2009 年 12 月に公開された。さらに第 3 次草案が 2012 年 8 月 30 日に公開され、2012 年 10 月 1 日のコメント締め切り後、現在、2013 年 8 月に予定される商務省へ最終稿を提出すべく準備中である。

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。また、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、第 2 次草案では FIPS 140-2 と同様に 4 段階に戻った。

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

[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）

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。

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 の改定に対応し、FIPS 140-2 の後継標準となる FIPS 140-3 をベースに改定するべく早期改定を開始した。その後、FIPS 140-3 の改定草案作成が大幅に遅れたため、FIPS 140-3 と ISO/IEC 19790 の改定を並行して行うことが決まった。これに従い、ISO/IEC 19790 改定版(2nd ed.)の 1st WD は FIPS 140-3 の改定草案に若干遅れた 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

[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。

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)

[29] Field Programmable Gate Array

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、「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定

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に改定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 に改定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 に改定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定版の作成

NIST 発行の“Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program”は逐次改定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、

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

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

1.3.2 暗号実装委員会に移行後の活動

2009 年度の活動概要

(1) 電子政府推奨暗号リスト改定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定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 の改定草案に対応する国際規格 ISO/IEC 19790 の早期改定ドラフトに対して、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定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項目を決定した。

(2) 電子政府推奨暗号リスト改定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 の改定草案に対応する国際規格 ISO/IEC 19790 及び ISO/IEC 24759 の早期改定草案を 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。

2011 年度の活動概要

(1) 電子政府推奨暗号リスト改定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に関する詳細を検討・決定した。

(2) 電子政府推奨暗号リスト改定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、評価手法を再検討し、詳細を決定した。

(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 の改定草案に対応する国際規格 ISO/IEC 19790 及び ISO/IEC 24759 の早期改定草案を 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。

第 2 章　2012 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定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評価の実施

2.1.1　暗号リスト選定のフレームワーク

従来の電子政府推奨暗号リストは今回の改定後には、電子政府推奨暗号リスト、推奨候補暗号リスト、運用監視暗号リストの３つからなる構成される CRYPTREC 暗号リストに移行する。CRYPTREC 暗号リストに掲載する暗号を選定するために暗号運用委員会で作成し、暗号技術検討会で承認されたフレームワークを図 2.1 に示す。この図の中で暗号実装委員会が関与するのは【安全性評価／実装評価】、【評価Ｂ】、【総合評価】である。最後の【総合評価】は【評価Ａ】または【評価Ｂ】を追加した暗号の個数が許容の範囲を超えたときに、さらなる絞り込みを行うためのもので、今回は実施されなかった。以下では【安全性評価／実装評価】と【評価Ｂ】の各々について説明する。

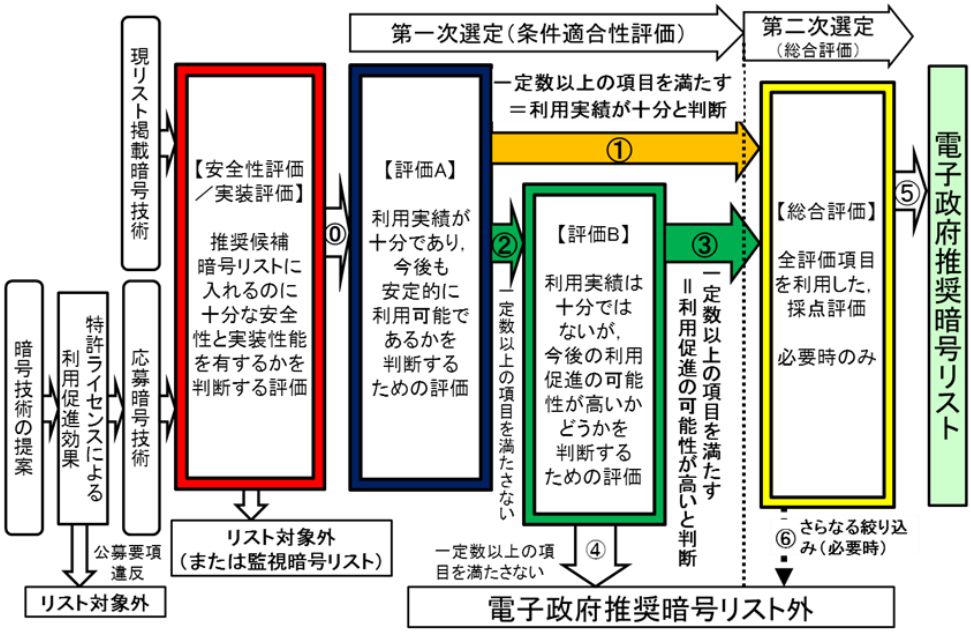


図 2.1　暗号選定のフレームワーク

2.1.2　【安全性評価／実装評価】における実装性能評価

【安全性評価／実装評価】では、評価対象暗号が推奨候補暗号リストに掲載されるのに相応しい安全性と実装性能の両方を備えているか判定する。安全性については暗号方式委員会が、実装性能については暗号実装委員会が判定を実施した。

(1) 実装性能評価の判定方針

暗号実装委員会では、評価対象の暗号を、既存の電子政府推奨暗号リスト掲載

暗号、今回の事務局選出暗号、新規応募暗号の 3 種類に分け、次のように扱うこととした。

(A) 従来の電子政府推奨暗号リスト掲載暗号

前回の暗号選定時に十分な実装性能を有していることを確認しているので、今回も十分な実装性能が有ると判定した。

(B) 事務局選出暗号

ISO/IEC や NIST など国際的な標準規格に採用されており、実装性能に関して特に問題は報告されていないので、十分な実装性能が有ると判定した。

(C) 新規応募暗号

今回の公募要項において、従来の電子政府推奨暗号リスト掲載の暗号に対して、安全性または実装性能における優位性があることが要求されている。暗号実装委員会では、独自に用意した実装環境での測定を行った。その結果、第 2 次評価に進んだ全ての新規応募暗号について、従来の電子政府推奨暗号リス装性能が有ると判定した。判定の内容について以下に述べる。

(2) 新規応募暗号の判定概要

(A) 判定基準

ソフトウェア実装及びハードウェア実装に関する評価指標の少なくとも一つにおいて、測定値が比較対象全てに対して優れていれば、優位性ありと判定した。比較対象は、既存の技術分類である 128 ビットブロック暗号及びストリーム暗号については同一分類に属する従来の電子政府推奨暗号全部、新規の技術分類であるメッセージ認証コードについては事務局選出暗号の代表である CMAC を比較対象とし、ブロック暗号には AES を使用した。

表 2.1　実装評価対象の暗号

技術分類	評価対象暗号	比較対象暗号	
	新規応募暗号	従来の推奨暗号	事務局選出暗号
128ビットブロック暗号	CLEFIA	AES Camellia CIPHERUNICORN-A Hierocrypt-3 SC2000	
ストリーム暗号	Enocoro-128v2	MUGI	
	KCipher-2	MULTI-S01*	
メッセージ認証コード	PC-MAC-AES		CMAC (AES)

* ハードウェア実装のみ測定

(B) 実装評価内容

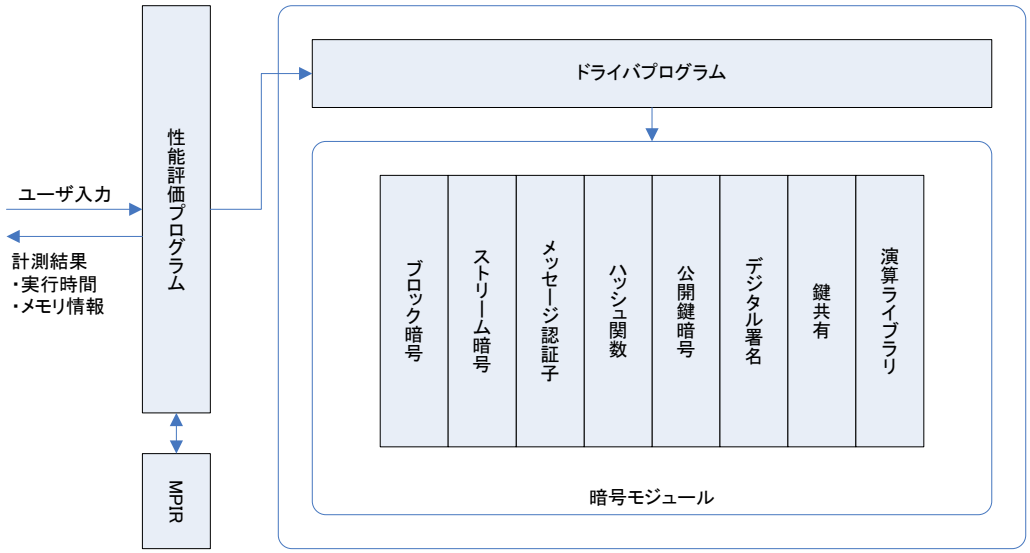
ソフトウェア実装については、Windows PC 上での実装性能を対象に、初期化時間、処理速度、使用メモリ量を測定した。

ハードウェア実装については、FPGA 上の実装性能を対象に、処理時間・速度、回路規模を測定した。

(C) 複数の実装を提出した新規応募暗号の扱い

既存の技術分類である 128 ビットブロック暗号及びストリーム暗号については、同一分類に属する従来の電子政府推奨暗号を比較対象とした。メッセージ認証コードは新規の技術分類であるので、事務局選出暗号の代表である CMAC を比較対象とし、ブロック暗号には AES を使用した。

(3) ソフトウェア実装評価



・ 図 2.2　ソフトウェア実装評価の概略

(A) ソフトウェア実装の測定方法

ソフトウェア実装の性能測定には、経済産業省の事業[32]として開発した評価ツールを使用した。図 2.2 に概略を示す。従来の電子政府推奨暗号と事務局選出の暗号に対する実装（暗号モジュール）は暗号ライブラリとして開発物の一部として提供されたものを使用した。新規応募暗号については、応募者に評価用実装開発のための情報をまとめた要項（付録 1）と開発環境を提供し、それを元に開発された評価用実装を使用した。

[32] 2009 年度経済産業省委託研究「クラウド環境　における暗号技術評価」の一環として開発

(B) ソフトウェア実装結果の注意点

次の理由から，測定データは評価対象が比較対象と同等以上の性能を有するかの判定のみに使用されるべきである。各暗号（特に比較対象の暗号）の最高性能を示すものではないことに注意されたい。

① 実装方法・開発環境の差異

新規応募暗号は応募者、現リスト掲載暗号は評価ツール開発者が実装と、実装者が異なる。

② 最適化における制約

MMX など CPU 固有の命令やインラインアセンブラを禁止している。

③ 他プロセスの影響

他のプロセスの影響を抑えきれず、飛びぬけて大きなクロック数が観測されている。不要プロセスの消去、スタンドアローン動作などの対策は実施した。

④ 評価ツール自体のオーバーヘッド

評価ツール自体がリソースを消費しており、メモリ使用量の絶対値参考にならない。

(C) 暗号ごとの特記事項

①AES（外部委託実装）

既存の実装結果と比べ、AES の暗号化速度が相対的に非常に遅い。原因は通常の高速化手法が利用されていないためと考えられる。

②AES（OpenSSL 版）

OpenSSL のソースコードを評価ツールのインターフェイスに合わせて、関数名と変数名を置換した。測定したところ、平文サイズが 16 バイトでの復号速度が暗号化速度と比較して約 1/3 と非常に遅かった。これは、評価ツールでは初期化の際に、暗号化用と復号用の鍵拡大を一括して行う仕様になっていることが、原因の可能性がある。

(4)ハードウェア実装評価

(A) ハードウェア実装の測定方法

ハードウェア実装性能の測定では、プラットフォームを FPGA とし、暗号実装に適し、かつ、入手が容易である SASEBO-GII(Xilinx Virtex-5/LX50 搭載）を利用した。測定用環境は産業技術総合研究所に委託して開発した。従来の電子政府推奨暗号と事務局が選出した暗号については、実装と性能測定をパステルネットワークス(株)に委託した。新規応募暗号については、応募者に、評価用実装開発のための情報をまとめた要項（付録 2）と実装サンプルを提供し、評価用実装と合成ツール Xilinx 社 ISE のサマリレポート等のデータ、サイドチャネル攻撃に関するデータの提出を要求し､提出データによって測定を行った。

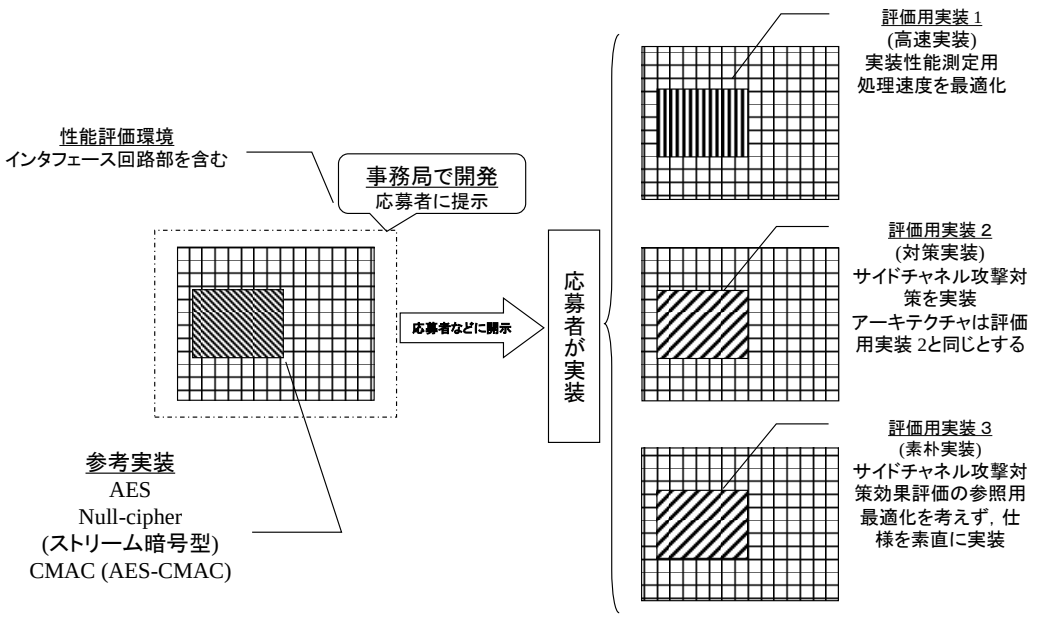


図 2.3　ハードウェア実装評価のイメージ

(B) ハードウェア実装結果の注意点

次の理由から、測定データは評価対象が比較対象と同等以上の性能を有するかの判定のみに使用されるべきである。各暗号（特に比較対象の暗号）の最高性能を示すものではないことに注意されたい。

① 実装方法・開発環境の差異

新規応募暗号は応募者、現リスト掲載暗号は評価ツール開発者が実装と、実装者が異なる。

② 一種類の実装デバイス（Xilinx Virtex-5 LX50）

異なるデバイスへの実装では性能の優劣が逆転する可能性がある。

(C) 暗号ごとの特記事項

① 新規応募暗号

当初、インターフェイス回路(I/F)を含んだ回路を対象としたが、より精度の高い情報を提供するため、本資料では外部委託実装と合わせて I/F を含まない実装での計測値を採用した。

②PC-MAC-AES（応募者実装）

AES の暗号コアは CMAC の AES コアとは異なる。

③ 外部委託実装全般

Virtex-5 を実装した SASEBO-GII ボードでの 24MHz 動作を前提に、シンプルなデータパスによる設計を行っている。このため、測定値が各暗号アルゴリズムの絶対的な実装性能を示すものではない。実装環境の制約に応じた最適化により、性能が大きく異なる可能性に留意する必要がある。

④ Hierocrypt-3（外部委託実装）

著しく低い性能となっているが、この理由は Virtex-5（Xc5lxff324-3）の制約によるところが大きい。今回は、仕様に忠実に従った結果、線形変換の構成要素のリソースが非常に大きくなり、32 ビット入出力処理を 4 組利用する 128 ビット処理が実現できなかった。そこで 1 組を 4 回繰り返すなどの対応を行ったところ、大幅なスループットの低下を招いた。

より大きなデバイスをターゲットにデータパスの最適化を行えば、性能の大幅な向上が可能である。また、今回の実装では独立にしているコンポーネントの共有化や実装ノウハウの利用によって、回路規模の大幅な縮小と大幅な性能向上も可能であると考えられる。

(5) 判定結果

下記項目において優位性を確認したため、現リスト暗号と同等以上の特長を有すると判定した。

表 2.2　新規応募暗号の電子政府推奨暗号(従来)に対する優位点

暗号名	ソフトウェア実装	ハードウェア実装
CLEFIA	初期化時間（16バイト, 1536バイト）, 暗号化速度（16バイト）, 復号速度（16バイト, 1536バイト）	回路効率, 規模（LUT-FF pair, LUT）
Enocoro-128v2	初期化時間（全平文長）, 暗号化速度（16バイト）, 復号速度（16バイト）, メモリ使用量（全平文長）	回路効率, 回路規模（LUT-FF pair, LUT, FF）
KCipher-2	初期化時間（全平文長）, 暗号化速度（全平文長）, 復号速度（全平文長）, メモリ使用量（全平文長）	暗号化速度, 回路効率, 回路規模（LUT-FF pair, LUT, FF）
PC-MAC-AES	MAC生成速度（全平文長）, MAC検証速度（1536バイト, 1048576バイト）, メモリ使用量（全平文長）	暗号化速度, 回路規模（LUT-FF pair）, 回路効率

実装性能評価で測定した全項目のデータは、付録 3 にレーダーチャートにまとめて示した。

2.1.3　【評価Ｂ】における実装性能評価

(1) 実装性能の判定方法

【評価Ｂ】では、【評価Ａ】で利用実績が現在は不十分と判定された暗号技術について、将来的に十分なレベルに達する見込みがあるかを判定する。【評価Ｂ】の判定項目の一つに「標準化・規格化の促進を図るハードルの低さ」があり、その下の判定項目の一つ（OR 条件）である「市場が認める程度の技術的アドバンテージ」のうち、実装評価性能に関する優位性の有無を暗号実装委員会で判定した。

判定においては、前回及び今回の公募に対して応募された暗号（以下、「応募暗号」という。）と、事務局が技術的な分類の中で、標準的なものとして候補に選出した暗号（以下、「標準的暗号」という。）に分けて、異なる基準で判定した。

(2) 応募暗号に関する判定

応募者に同一カテゴリの標準的な暗号技術に対する優位点とそれを示す資料を提出を要請し、その妥当性を委員会で判定した。提出がない場合は、優位性なしとした。以下に、公開鍵暗号、ブロック暗号、ストリーム暗号とメッセージ認証コードの順に判定結果とその理由を表に示す。

表 2.3　公開鍵暗号・署名の判定結果

暗号名	回答	比較対象	優位点	判定結果
ECDSA	有	RSA署名	鍵生成時間, 署名生成速度	有
RSASSA-PKCS-v1_5	無			無
RSA-PSS	無			無

表 2.4　公開鍵暗号・守秘の判定結果

暗号名	回答	比較対象	優位点	判定結果
RSA-OAEP	無			無
~~RSAES-PKCS1-v1_5~~ *	無			無

* RSAES-PKCS1-v1_5 は、暗号方式委員会で推奨候補暗号外と判定された。

表 2.5　公開鍵暗号・鍵共有の判定結果

暗号名	回答	比較対象	優位点	判定結果
ECDH	有	DH	鍵生成時間, 鍵共有処理	有
PSEC-KEM	有	DH	鍵交換速度	有

表 2.6　64 ビットブロック暗号の判定結果

暗号名	回答	比較対象	優位点	判定結果
CIPHERUNICORN-E	有	TDES	小型実装の実装サイズ	有
Hierocrypt-L1	有	MISTY1, TDES	暗号化(復号)速度	有
MISTY1	無			無

表 2.7　128 ビットブロック暗号の判定結果

暗号名	回答	比較対象	優位点	判定結果
CLEFIA	有	Camellia	回路効率，小型実装	有
Camellia	有	AES	初期化時間(鍵設定，IV設定)，速度，実装サイズ，クリティカルパス遅延，消費電力，回路効率等	有
CIPHERUNICORN-A	有	AES	特になし	無
Hierocrypt-3	有	AES, Camellia	速度(暗号化，復号)	有
SC2000	有	AES	速度，実装環境への対応性，キャッシュメモリの有効活用	有

表 2.8　ストリーム暗号の判定結果

暗号名	回答	比較対象	優位点	判定結果
Enocoro-128v2	有	ブロック暗号、128 ビットストリーム暗号	速度(乱数生成，暗号化)，回路規模	有
KCipher-2	有	MUGI	速度，初期化時間，内部状態サイズ	有
MUGI	有	AES, ストリーム暗号	回路規模，暗号化速度(ハードウェア実装)	有
MULTI-S01	有	AES-GCM, AES-CCM	(応募者は速度で優位性があると主張したが，確認できず)	無

表 2.9　メッセージ認証コードの判定結果

暗号名	回答	比較対象	優位点	判定結果
PC-MAC-AES	有	AESを使用した MAC一般	速度	有

(3) 標準的暗号の判定

標準的なものであることを根拠に一括で判定する方針となった。審議の結果、標準的な暗号として比較の基準となるものであるので、それ自体は優位性なしと判定することになった。

2.1.4　サイドチャネル攻撃への対策可能性検証

暗号実装委員会では、応募暗号の選考に直接利用しないものの、暗号利用者への情報提供を目的として、一部の応募暗号がサイドチャネル攻撃に対する対策が可能であるか確認した。確認対象の技術分類は共通鍵暗号であり、４件の応募暗号のうち、PC-MAC-AES(メッセージ認証コード)を除く、CLEFIA(128 ビットブロック暗号)、Enocoro-128v2(ストリーム暗号)、KCipher-2(ストリーム暗号)の 3 件である。

(1) サイドチャネル攻撃対策の有効性確認のための実装

対象とする実装環境は、SASEBO-GII 上の FPGA(Virtex-5)とした。攻撃方法は電力解析、攻撃箇所は特定の一段、攻撃方法における選択関数等の詳細情報の選択は応募者に任せることとした。応募者には有効性確認用に、図 2.3 の評価用実装 2 (対策実装)と評価用実装 3 (素朴実装)の 2 種類の提出を要求した。素朴実装は、仕様書から自然に導かれる素直な構成であり、サイドチャネル攻撃対策は行わないものである。対策実装は、素朴実装と同じアーキテクチャであり、サイドチャネル攻撃対策を施したものである。各々の実装性能を、付録 4 (2)に示す。

(2) サイドチャネル攻撃対策の有効性確認方法

鍵は 1 種類に固定し、ブロック暗号の平文、ストリーム暗号の初期ベクターは 1 波形ごとに毎回ランダムに与える。前項の素朴実装に対しては 1 万波形、対策版に対しては 10 万波形を測定し、応募者が提示した選択関数を利用した相関電力解析攻撃(CPA)を実施した。測定に用いた環境を付録 4 (1)の表 A4.1 と表 A4.2 に示す。

(3) サイドチャネル攻撃対策の有効性確認結果

3 種類の暗号とも、素朴実装では 2,000～4,000 波形で正解鍵が優勢になるのに対し、対策実装では 10 万波形でも正解鍵がその他の中に埋もれたままとなっており、対策の効果が確認できた。攻撃結果を付録 4 (3)の図 A4.4～9 に示したが、太線は正解鍵を、細い線はその他の鍵を表す。

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。昨年度までは、FIPS 140-3 とその試験要件に各々対応する ISO/IEC 19790 と ISO/IEC 24759 の早期改定ドラフトに対し、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てきた。

今年度は、ISO/IEC 19790 及び ISO/IEC 24759 の早期改定が一段落しつつあることから、これらを補うために作成が開始された ISO/IEC 17825（非侵襲攻撃に対する安全性に関する適合試験）を検討対象とし、3rd WD に対する日本コメントの原案を作成した。

2.3　2012 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[33]攻撃、SPA[34]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）[35]と ASIC[36]を搭載した SASEBO-R（LSI 版）[37]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 及びにが開発・製品化された。平成 23 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[38]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

---

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

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

[35] 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。

[36] ASIC：Application Specific Integrated Circuit

[37] 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。

[38] 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。

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本年度も引き続き行った。

また、国際標準規格に関しては、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 及び試験要件に関する国際規格 ISO/IEC 24759 の早期改定文書が固まりつつありリ、修正すべき箇所が減少した。一方、これらに記載された非侵襲攻撃に対する安全性に関する適合試験を規定すべく ISO/IEC 17825 の作成が開始されたので、これを検討対象とし、3rd 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。

2012 年度には、FIPS 140-3 に対応する ISO/IEC 19790 の早期改定が終了して 8 月 9 日付で発行され、FIPS 140-3 の試験要件(DTR)に対応する ISO/IEC 24759 の早期改定の草案も DIS に進んで改定作業は収束しつつある。これらの規格では、安全性レベルが 3 と 4 の暗号モジュール対しては、非侵襲攻撃に対する安全性が要求されている。しかしながら、具体的な試験項目の記載はなかったので、これを補うものとして、非侵襲攻撃に対する安全性に関する適合試験を規定すべく ISO/IEC 17825 の作成が開始された。そこで当規格ををを検討対象とすることを決定し、3rd WD に対する日本コメントの原案を作成した。（付録 5）

コメント原案は ISO/IEC JTC1 SC27/WG3 国内小委員会に提案され、そのまま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 2012 年度の発表論文を収集し、発表順にまとめた。

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 （2013 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　招聘研究員
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	盛合　志帆	独立行政法人情報通信研究機構　研究室長
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
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

松尾　真一郎
野島　良
箕輪　正
大久保　美也子
多賀　文吾
黒川　貴司
金森　祥子

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、2012 年度の発表についてまとめた。（表 2.10）

表 2.10　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	Diffie-Hellman 方式に対するメッセージ選択型電力解析	電子情報通信学会論文誌 Vol.J95-A, No.5, pp.436-445	2012.05.01	伊藤 孝一, 落合 隆夫, 鳥居 直哉（富士通研究所）
2	点のスカラ倍算に対するメッセージ選択型電力解析	電子情報通信学会論文誌 Vol.J95-A, No.5, pp.446-455	2012.05.01	伊藤 孝一, 山本 大, 古川 和快, 伊豆 哲也, 武仲 正彦, 鳥居 直哉（富士通研究所）
3	拡張 2 進 GCD 法を用いた逆元演算の実装に対するサイドチャネル攻撃	電子情報通信学会論文誌 Vol.J95-A, No.5, pp.456-463	2012.05.01	高橋 芳夫, 松本 勉（横浜国大）
4	Evaluation of Information Leakage from Cryptographic Hardware via Common-Mode Current	IEICE Transactions on Electronics, Vol.E95-C, No.6, pp.1089--1097	2012.06.01	Yuichi Hayashi, Naofumi Homma, Takaaki Mizuki, Takeshi Sugawara, Yoshiki Kayano, Takafumi Aoki, Shigeki Minegishi, Akashi Satoh, Hideaki Sone, Hiroshi Inoue
5	Feasibility of Fault Analysis Based on Intentional Electromagnetic Interference	EMC[39] 2012	2012.08.09	Junko Takahashi, Yu-ichi Hayashi, Naofumi Homma, Hitoshi Fuji, Takafumi Aoki
6	A Fault Model for Conducted Intentional ElectroMagnetic Interferences	EMC 2012, pp.788--793	2012.08.09	Laurent Sauvage, Sylvain Guilley, Jean-Luc Danger, Naofumi Homma, Yu-ichi Hayashi
7	Efficient mapping of EM radiation associated with information leakage for cryptographic devices	EMC 2012, pp.794--799	2012.08.09	Haruki Shimada, Yu-ichi Hayashi, Naofumi Homma, Takaaki Mizuki, Takafumi Aoki, Hideaki Sone, Laurent Sauvage, Jean-Luc Danger
8	An efficient method for estimating the area of information propagation through electromagnetic radiation	EMC 2012, pp.800--805	2012.08.09	Yu-ichi Hayashi, Naofumi Homma, Taishi Ikematsu, Takaaki Mizuki, Takafumi Aoki, Hideaki Sone, Jean-Luc Danger
9	An Efficient Countermeasure against Fault Sensitivity	FDTC[40] 2012, pp.95--102	2012.09.09	Sho Endo, Yang Li, Naofumi Homma, Kazuo Sakiyama, Kazuo Ohta, Takafumi Aoki
10	パイロットランプはサイドチャネルとして使える	ISEC[41]2012-54, pp.51-58	2012.09.21	齋藤 翔平, 松本 勉
11	サイドチャネルセキュリティを厳しく評価する効率のよい方法	ISEC2012-56, pp.67-74	2012.09.21	岸川 剛, 齋藤翔平, 土屋 遊, 遠山 毅, 松本 勉（横浜国大）
12	電磁波照射を用いたフォールト攻	ISEC2012-57, pp.1-8	2012.11.21	土屋 遊, 岸川 剛, 齋藤 翔平,

[39] EMC : International Symposium on Electromagnetic Compatibility（IEEE EMC Society）

[40] FDTC : Workshop on Fault Diagnosis and Tolerance in Cryptography

[41] ISEC : 情報セキュリティ研究会（電子情報通信学会）

	撃によるICカードからのAES鍵の抽出			遠山 毅, 佐々木 明彦, 佐藤 証, 松本 勉
13	Transient IEMI Threats for Cryptographic Devices	IEEE Trans. Electromagnetic Compatibility, Vol.55, No.1, pp.140--148	2013.02	Yuichi Hayashi, Naofumi Homma, Takaaki Mizuki, Takafumi Aoki, Hideaki Sone
14	Exploring the Relations Between Fault Sensitivity and Power Consumption	COSADE[42] 2013	2013.03.08	Yang Li, Sho Endo, Nicolas Debande, Naofumi Homma, Takafumi Aoki, Thanh-Ha Le, Jean-Luc Danger, Kazuo Ohta, Kazuo Sakiyama
15	Chosen-IV Correlation Power Analysis on KCipher-2 and a Countermeasure	COSADE 2013	2013.03.08	Takafumi Hibiki, Naofumi Homma, Takafumi Aoki, Yuto Nakano, Kazuhide Fukushima, Shinsaku Kiyomoto, Yutaka Miyake
16	イベントモデルシミュレーションによるサイドチャネル情報取得の効率化	SCIS[43]2013, 1E1-1	2013.01.22	浅井 稔也, 吉川 雅弥
17	スタンダードセルからの微小な EM リーク	SCIS2013, 1E1-3	2013.01.22	菅原 健, 鈴木 大輔, 佐伯 稔, 汐崎 充, 藤野 毅
18	耐タンパ性向上のための乗算マスクと Dual-Rail RSL メモリ方式を用いた AES 暗号回路の設計	SCIS2013, 1E1-4	2013.01.22	鵜飼 慎太郎, HOANG Anh-Tuan, 汐崎 充, 浅川 俊介, 橋本 祐樹, 藤野 毅
19	故障感度隠蔽のための効率的な対策とその評価	SCIS2013, 1E1-5	2012.01.22	遠藤 翔, 李 陽, 本間 尚文, 崎山 一男, 藤本 大介, 永田 真, 太田 和夫, 青木 孝文
20	サポートベクターマシンを用いる電力解析の攻撃能力に関する考察	SCIS2013, 1E2-2	2013.01.22	杉浦 広基, 駒野 雄一, 野崎 華恵
21	容量充電モデルを用いたシミュレーションによる相関電力解析の考察	SCIS2013, 1E2-3	2013.01.22	田中 大智, 藤本 大介, 永田 真
22	サイドチャネル攻撃に関する情報理論的解析	SCIS2013, 1E2-5	2013.01.22	水野 弘章, 岩井 啓輔, 田中 秀磨, 黒川 恭一
23	AES 暗号回路の設計・評価を効率的に行うサイドチャネル攻撃耐性検証法の一考察	SCIS2013, 3E2-4	2013.01.22	伊藤 弘樹, 汐崎 充, 藤野 毅
24	ソフトウェア実装暗号におけるシンボル置換を利用した電力解析対策手法	SCIS2013, 3E2-5	2013.01.24	前川 晃, 山下 哲孝, 岡村 利彦, 峯松 一彦, 洲崎 智保, 角尾 幸保
25	SRAM アクセスのサイドチャネル情報	SCIS2013, 3E3-1	2013.01.24	佐伯 稔, 鈴木 大輔, 菅原 健, 汐崎 充, 藤野 毅
26	Mechanism Analysis for Non-Uniform Mapping of Faulty S-box - Case Study of AES-COMP -	SCIS2013, 3E3-2	2013.01.24	松原 有沙, 李 陽, 太田 和夫, 崎山 一男
27	C-EMA と CEMA の攻撃性能の比較	SCIS2013, 3E3-3	2013.01.24	中曽根 俊貴, 李 陽, 佐々木 悠, 岩本 貢, 太田 和夫, 崎山 一男
28	自動的かつ高精度なキャッシュ攻撃評価法による攻撃に必要な平文数の解析	SCIS2013, 3E3-4	2013.01.24	高橋 順子, 福永 利徳
29	共通鍵暗号の S-box に対する線形結合ビットを用いたハミング重み CPA	SCIS2013, 3E4-1	2013.01.24	岸本 耕平, 古原 和邦, 河村 大輔, 岩下 明暁, 水野 善之
30	電力・電磁波解析攻撃におけるオンチップ・キャパシタの影響評価	SCIS2013, 3E4-2	2013.01.24	中井 綱人, 汐崎 充, 藤野 毅
31	選択入力文法の電磁波利用サイドチャネル解析への適用	SCIS2013, 3E4-3	2013.01.24	岸川 剛, 松本 勉

[42] COSADE：International Workshop on Constructive Side-Channel Analysis and Secure Design

[43] 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）

32	漏えい情報を用いて注入タイミングを制御可能な遠方からの故障注入手法	SCIS2013, 3E4-4	2013.01.24	林 優一, 本間 尚文, 水木 敬明, 青木 孝文, 曽根 秀昭
33	電磁波照射を用いたフォールト攻撃による IC カードからの AES 鍵の抽出（2）	第 75 回情報処理学会全国大会, 2Z-9, 3-533--3-534	2013.01.24	遠山 毅, 土屋 遊, 大野 仁, 岸川 剛, 齋藤 翔平, 佐々木 明彦, 佐藤 証, 松本 勉
34	LED 暗号ハードウェアに対する相関電力解析とその対策	ISEC2012-93, pp.87-94	2013.03.06	ヴィッレ ウリマウル, 遠藤 翔, 本間 尚文, 青木 孝文
35	LED パイロットランプを通じたサイドチャネル攻撃における高速光検出器の効果	ISEC2012-91, pp.71-78	2013-03-07	齋藤 翔平, 松本 勉
36	ソフトウェア実装 AES の選択入力文法によるサイドチャネルセキュリティ評価	ISEC2012-111, pp.195-20	2013-03-07	齋藤 翔平, 岸川 剛, 松本 勉
37	非加工接触型 IC カードのレーザー照射によるフォールト攻撃	電子情報通信学会論文誌 Vol.J95-A, No.5, pp.436-445	2013-03-08	大野 仁, 土屋 遊, 遠山 毅, 岸川 剛, 齋藤 翔平, 佐々木 明彦, 佐藤 証, 松本 勉

2.4 今後の課題

電子政府推奨暗号リストの改定に伴い、CRYPTREC は 2013 年度から図 2.4 の体制を移行する。暗号実装委員会が担当した課題の多くは、暗号技術評価委員会に引き継がれる。暗号技術評価委員会で引き継がれるべき課題を次に列挙する。

図 2.4　2013 年度の CRYPTREC 体制

2.4.1 実装安全性に関する継続的な動向調査

(1) 暗号実装における安全性を維持するため、サイドチャネル攻撃・故障利用攻撃に関する動向調査を継続する。

(2) 前項の動向調査の結果をどのように活用するか検討する。

2.4.2 実装性能の評価方式の検討

(1) 既存暗号と新規応募暗号のフェアな評価方法を検討する。ここでは、一般的な実装の定義や、実装間での最適化の差異の最小化を追求する。

(2) 評価プラットフォームの適切な選定と多様化を検討する。今回は、ソフトウェア実装は Windows PC、ハードウェア実装は Xilinx 社製 FPGA (Virtex 5)を実装環境としたが、今後はスマートフォンやタブレット等での利用を想定した実装環境を検討する必要がある。

第 3 章　開催状況

3.1　暗号実装委員会の開催状況

2012 年度の暗号実装委員会は、計 4 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　2012 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	2012 年　7 月 5 日 13:00～15:00	暗号実装委員会活動計画の審議・承認 次期リスト作成に向けた実装性能評価方針の検討 （【安全性評価／実装評価】,【評価Ｂ】,【総合評価】）
第 2 回	2012 年 9 月 4 日 14:00～16:00	【安全性評価／実装評価】の判定決定 【評価Ｂ】の状況報告（新規応募暗号者に対する質問実施状況）と評価方針決定
第 3 回	2012 年　10 月 9 日 10:30～12:30	【評価Ｂ】と【総合評価】の判定決定 実装性能評価結果の情報公開方法に関する検討
第 4 回	2013 年　3 月 14 日 10:00～12:00	実装評価データの一部更新 サイドチャネル攻撃対策の有効性確認 今後の課題検討

3.2　サイドチャネルセキュリティ WG の開催状況

2012 年度のサイドチャネルセキュリティ WG は、計 2 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　2012 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	2012 年 7 月 5 日 15:30～17:30	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	2013 年 3 月 14 日 13:00～15:00	ISO/IEC 国際標準対応

付録

付録１　応募暗号ソフトウェア実装評価実施要項

新規応募暗号の実装評価の際、応募者に提示した「応募暗号ソフトウェア実装評価実施要項」を次ページ以降に示す。

応募暗号ソフトウェア実装性能評価要項

2009 年度の公募に応募された暗号のソフトウェア実装性能を CRYPTREC 事務局で用意した性能評価ツールを用いてどのように評価するかについてまとめる。

１．ソフトウェア実装評価の目的について

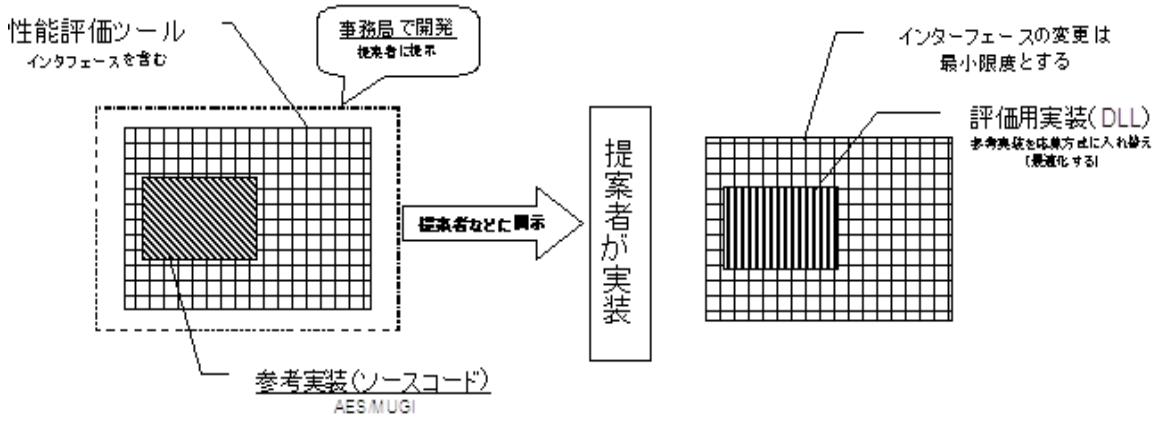
今回のソフトウェア実装評価は、Intrinsic 命令など特殊な専用命令を使用せず、通常の実装テクニックを利用して作成した C++のソースコードで、どの程度の処理速度が出るかを調べ、暗号利用者への参考情報とすることを主目的とする。既存の電子政府推奨暗号との性能比較は行うが、大まかに速いか遅いかを見るに留め、僅かな差で優劣を付けるものではない。

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・インターフェイスを含む雛形

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



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

2012 年 2 月 評価報告のまとめ

４．実装環境等

4.1 プラットフォーム／OS／使用言語

(1) 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

(2) OS は Windows 7 の 32 ビット版のみとする

(3) Visual Studio を開発環境とし、Visual C++ 2010 (10.0) SP1 を使用

(4) インライン・アセンブラの使用は禁止

(5) SSE/SSE2 等の Intrinsic 命令の使用は禁止

５．実装環境等

5.1 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。

5.2 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。

5.3 評価項目

(1) カテゴリ共通

(a) 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

(b) 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）

(c) 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）

(2) ブロック暗号

(a) 暗号化と復号の処理時間(クロック数の平均値等)

(b) 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

※ 変更前は、16 bytes, 64 bytes, 1,536 bytes, 4,096 bytes, 1,048,576 bytes(=1MB)の 6 種類

(3) ストリーム暗号

(a) 暗号化と復号の処理時間(クロック数の平均値等)

(b) 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

※　変更前は、8 bytes, 64 bytes, 576 bytes, 1,536 bytes, 4,096 bytes, 1,048,576 bytes(=1MB) の 6 種類

(4) メッセージ認証コード

(a) 認証コードの生成時間、検証時間(クロック数の平均値等)

(b) 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

※　変更前は、8 bytes, 64 bytes, 576 bytes, 1,536 bytes, 4,096 bytes, 1,048,576 bytes(=1MB) の 6 種類

6．事務局が提供する実装情報

(1) 暗号ライブラリ作成用ファイル一式

(a) プロジェクト・ファイル、ヘッダーファイル、ソースコード

(b) 暗号プリミティブのソースコードは次を含む
AES(ECB)、MUGI、AES-CMAC

(c) 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）

(2) 実装評価環境用ファイル一式

7．応募者の提出物

(1) 評価用実装（高速実装）

(a) DLL での提出を想定し、ソースコードは要求しない

(b) 測定箇所は関数呼び出しで設定

(c) 高速版を評価する

(2) インターフェイスの変更に関する記述（変更がなければ不要）

(3) 自己評価書

(a) 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

(4) 誓約書

(a) 本評価要項の記載通りに実装したことを誓約

以上

付録 2　応募暗号ハードウェア実装評価実施要項

新規応募暗号の実装評価の際、応募者に提示した「応募暗号ハードウェア実装評価実施要項」を次ページ以降に示す。

CRYPTREC 事務局

応募暗号ハードウェア実装性能評価要項

2009 年度の公募に応募された暗号のハードウェア実装性能評価における暗号モジュール開発についてまとめる。

1. ハードウェア実装評価の目的について

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。

(1) 処理速度の測定

(2) 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。

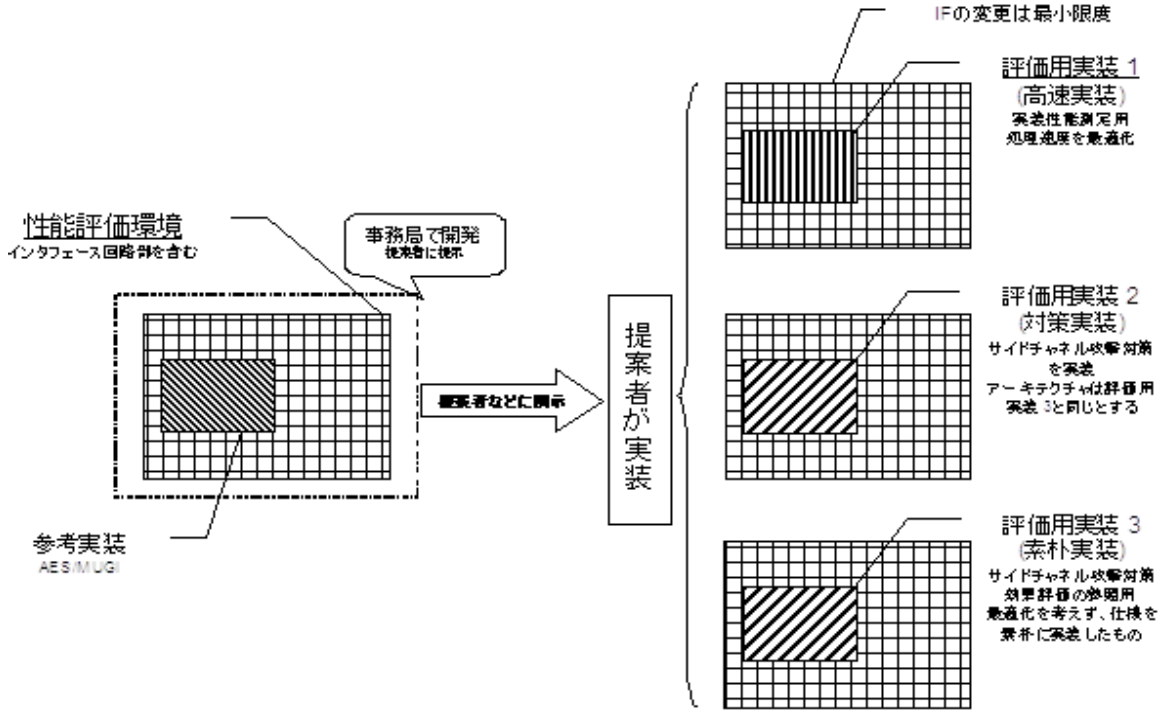
評価対象のカテゴリは、(1)については、ブロック暗号、ストリーム暗号、メッセージ認証コード、(2)についてはブロック暗号とストリーム暗号とする。

2. 用語の定義

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

性能評価環境　：事務局から提示する参考実装とインターフェイ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。

・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
2012 年 2 月 評価報告のまとめ

4. 評価の実装環境等

4.1 プラットフォーム

・Xilinx Virtex-5 LX50(SASEBO-GII 搭載の FPGA)

4.2 開発環境等

・ISE WebPACK Version 12.4

4.3 評価で参考とする仕様書、説明書等

別途配布した CD-ROM とメールで送付した資料を参照すること。

○「SASEBO(H23PRO-1309)」(CD-ROM)

電子政府推奨暗号回路 2011

－ 電子政府推奨暗号回路および制御ソフトウエア仕様書.doc

－ FPGA1_mugi/

○「電子政府推奨暗号回路および制御ソフトウエア」(11 月 7 日にメール送付)

CD-ROM の資料に、MUGI 用の制御用 C# ソースコードを加えたもの

5. 実装性能評価項目等 (評価用実装１)

5.1 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。

ブロック暗号は ECB モードのみとする。

・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。

他の鍵長については、自己評価結果として提出可とする。

5.2 最適化

・高速実装を評価対象とする。

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。

5.3 評価項目

(1) 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)

(2) 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)

(3) 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)

(4) 鍵スケジュールの設定に掛かる時間(ブロック暗号)

(5) 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)

6.1 鍵長

・ブロック暗号・ストリーム暗号とも 128 ビット鍵を評価対象とする。
他の鍵長については、自己評価結果として提出可とする。
暗号化のみで復号は対象としない。
ブロック暗号は ECB モードのみとする。
メッセージ認証コードは評価対象としない。

6.2 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
(a) 攻撃方法と選択関数は応募者が選定する。
(b) 攻撃箇所は特定の１段とする。
(a) (c) 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。

6.3 対策の有効性確認
(a) 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
・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
(b) 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。

7. 事務局が提供する実装情報
(1) ブロック暗号：参考実装（AES-ECB）
(2) ストリーム暗号：参考実装（Null cipher）
(3) 応募者向けハードウェア実装開発の手引き（本資料）

8. 応募者の提出物
(1) ３種類の評価用実装（評価用実装~~１~~２～３）
(a) 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
(b) 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
(2) ISE の合成で出力されるレポートのサマリ情報
(a) “トップモジュール名.par”を必須とし、その他は任意とする。
(3) シミュレーション波形
(4) タイミングチャート

(5) 電力解析で使用する選択関数（形式は、入力と仮想の電力）

(6) インターフェイスの書換えに関する記述（書換えがない場合は不要）

(7) 実装方針の説明（アーキテクチャを記述)

・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

・全体構造(ブロック図)、roll/unroll の区別、実装上の特徴

(8) 誓約書

(a)本要項の記載通りに実装したことを誓約

(9)自己評価書（提出は義務としない）

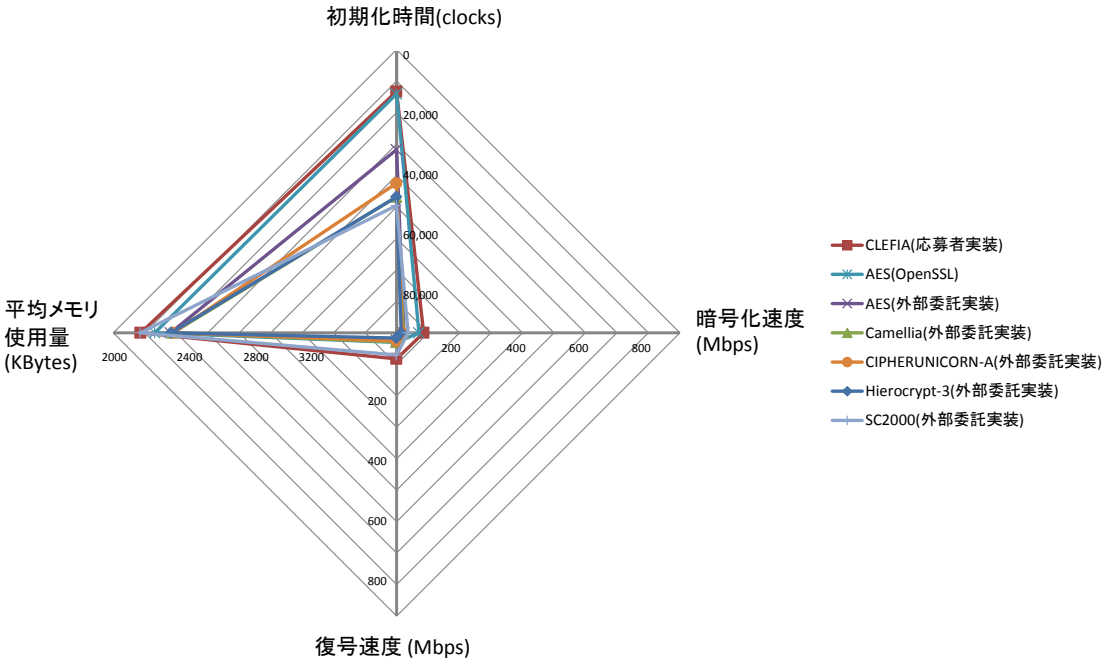
以上

付録 3　レーダーチャートによる測定結果の表示

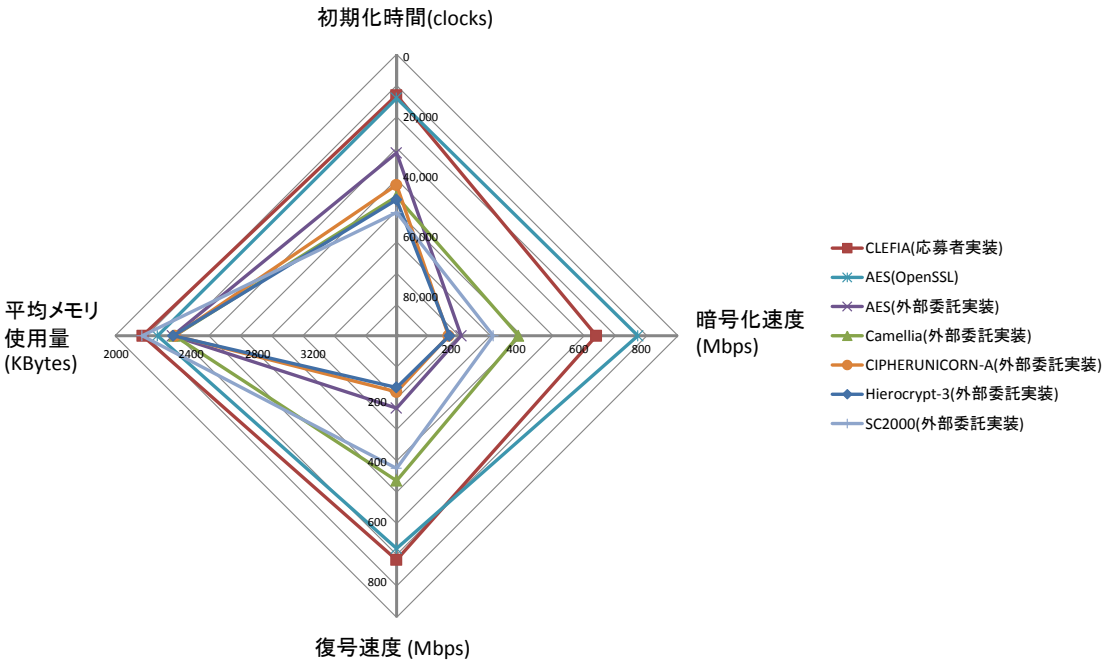
【安全性評価・実装評価】における実装性能評価で測定した全項目のデータを参考情報としてレーダーチャートで次ページ以降に示す。

（1） ブロック暗号

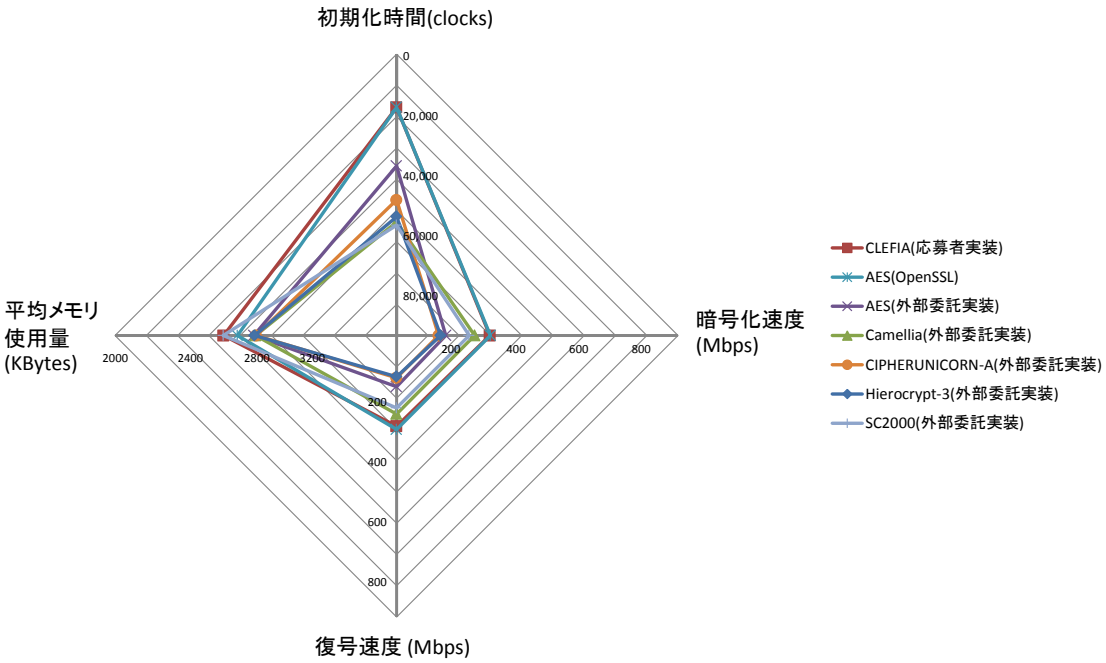
（A） ブロック暗号（S/W,平文 16 バイト）



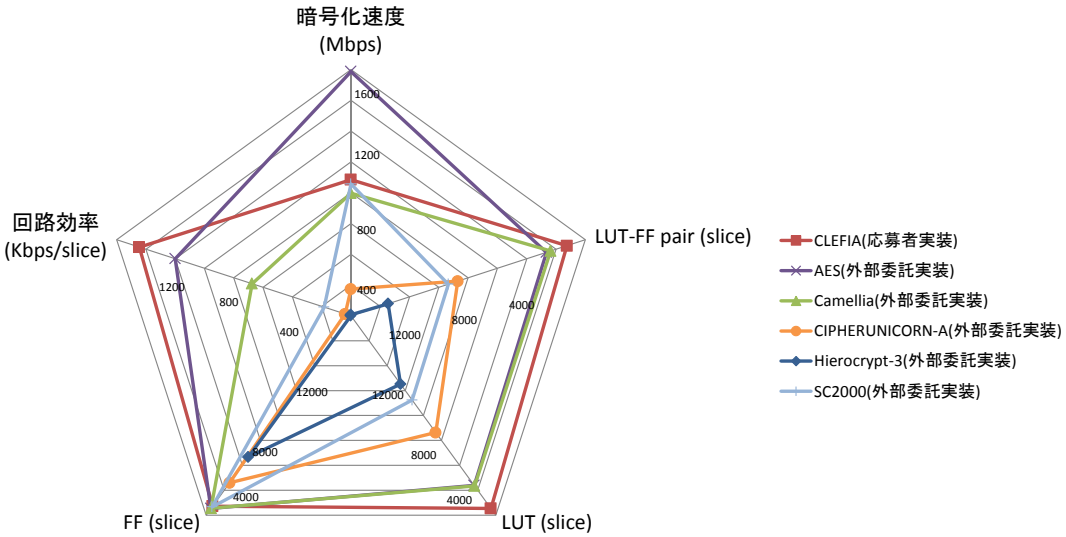
（B） ブロック暗号（S/W,平文 1536 バイト）



(C) ブロック暗号（S/W,平文 1048576 バイト）

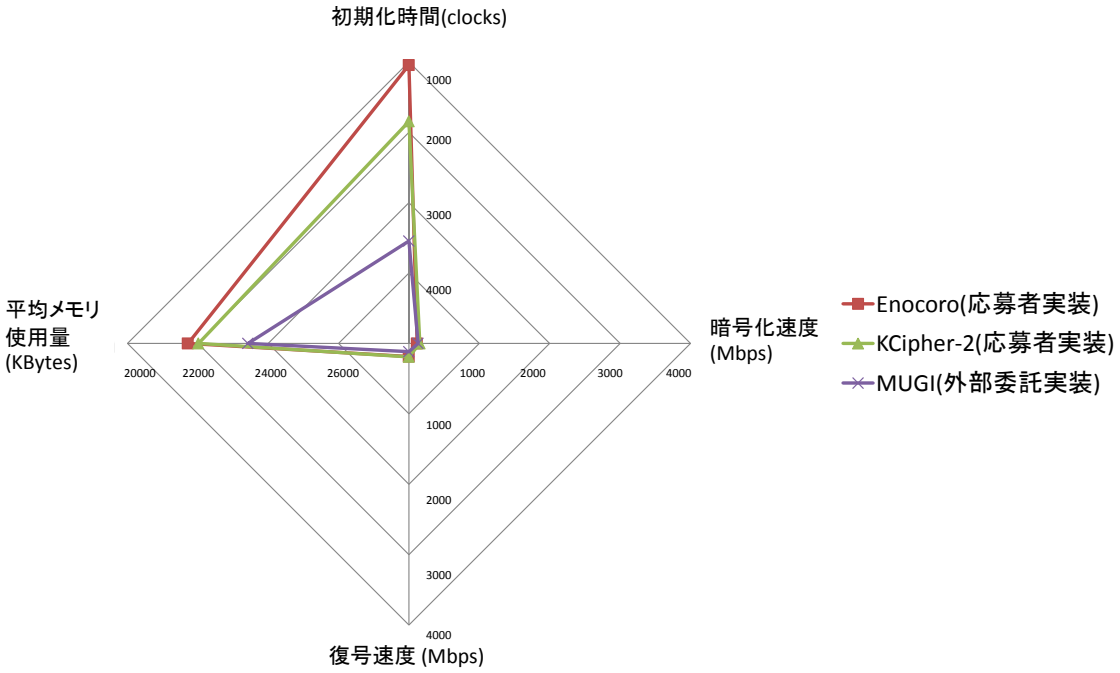


(D) ブロック暗号（H/W）

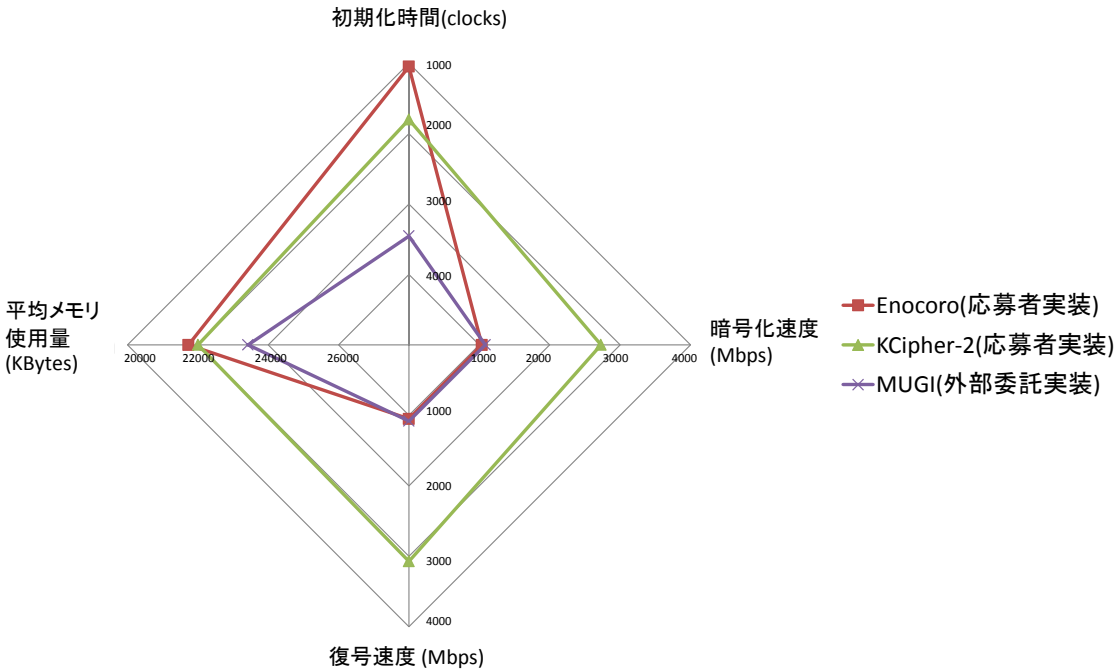


（2）ストリーム暗号

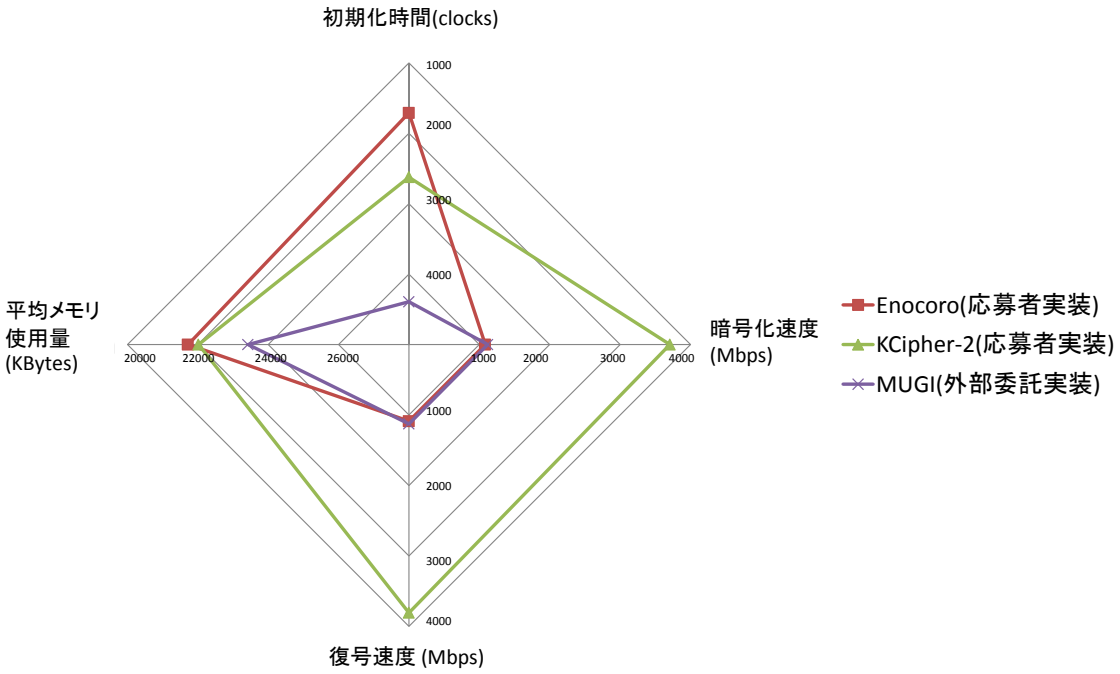
（A） ストリーム暗号（S/W,平文 8 バイト）



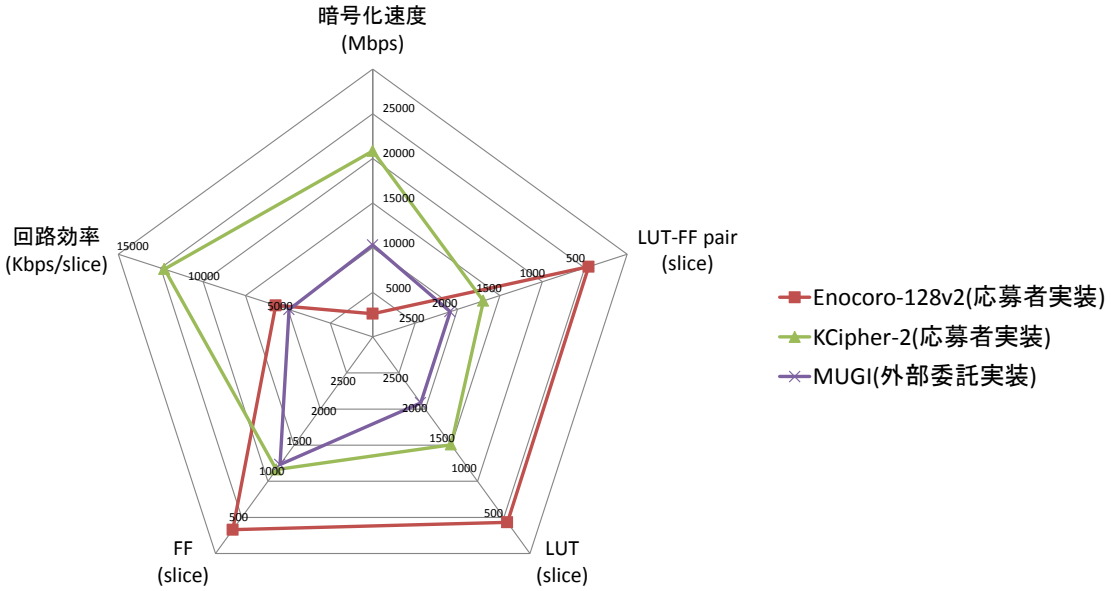
（B） ストリーム暗号（S/W,平文 1536 バイト）



（C） ストリーム暗号（S/W,平文 1048576 バイト）

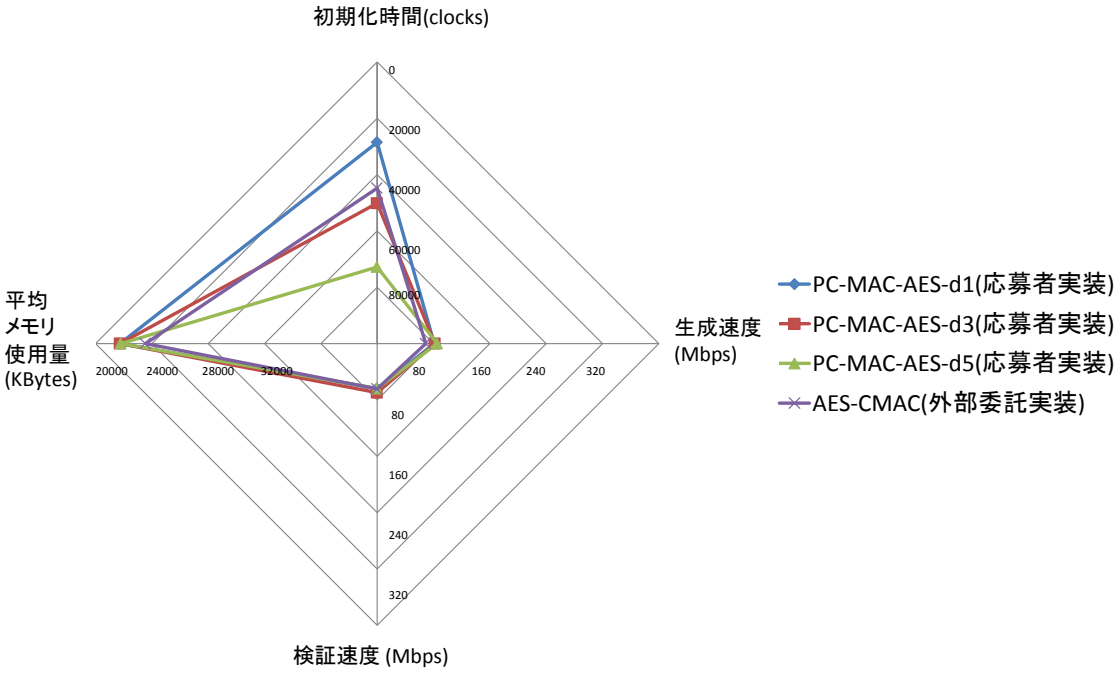


（D） ストリーム暗号（H/W）

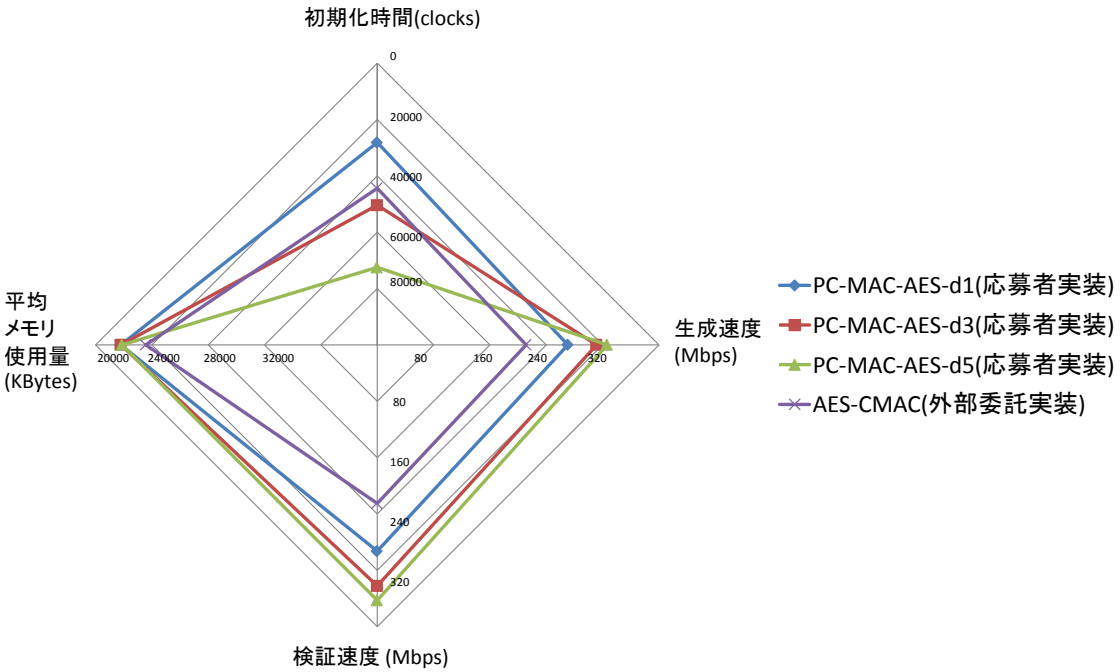


（３） メッセージ認証コード

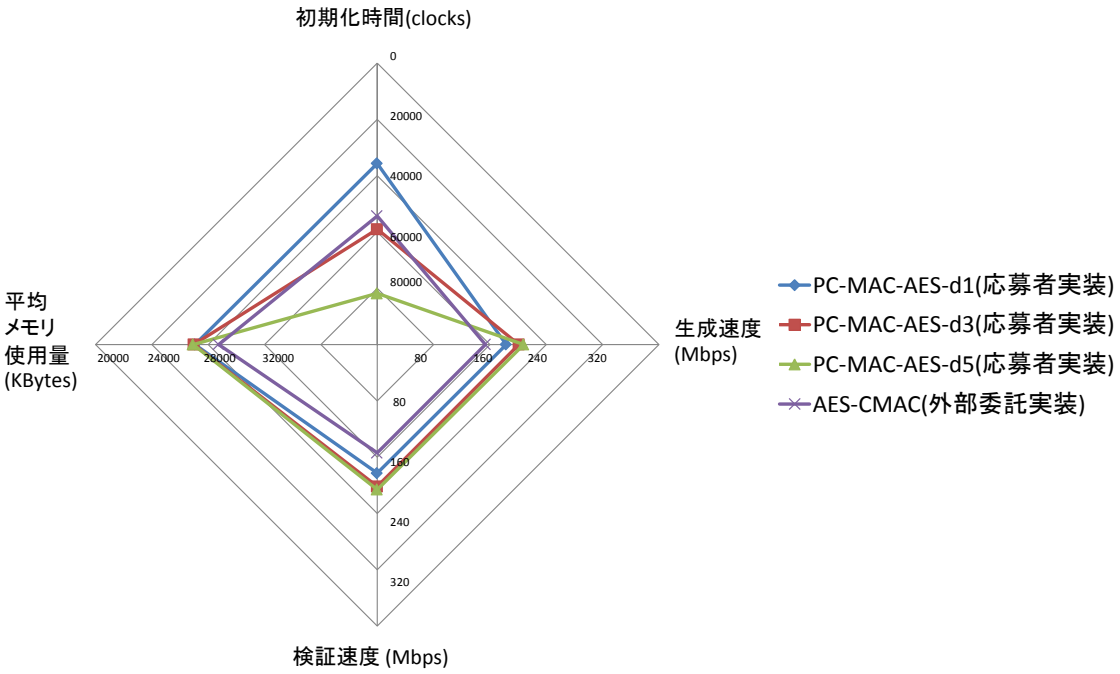
（A） メッセージ認証コード（S/W,平文 16 バイト）



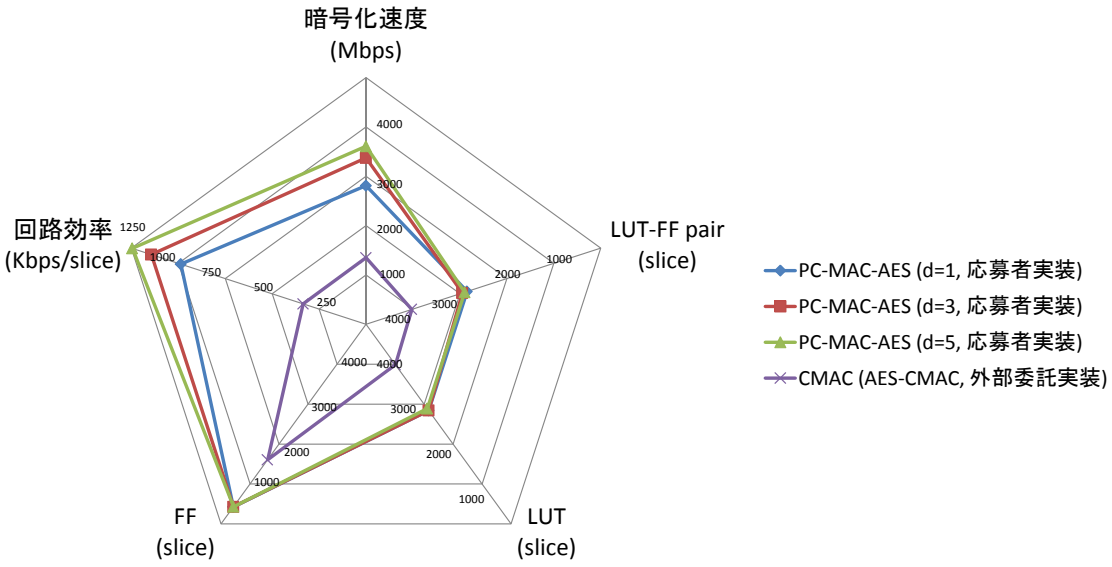
（B） メッセージ認証コード（S/W,平文 1536 バイト）



（C） メッセージ認証コード（S/W,平文 1048576 バイト）



（D） メッセージ認証コード（H/W）



付録 4　サイドチャネル攻撃対策の有効性確認に関するデータ

サイドチャネル攻撃対策の有効性確認に関するデータを以下に示す。

（1） FPGA 実装の測定環境

表 A4.1　CLEFIA と KCipher-2 のサイドチャネル測定環境

ISE バージョン	12.4
FPGA ボード	SASEBO-GII LX50
オシロスコープ	Tektronix TDS2024B
サンプリング周波数	2 GHz
波形数	10,000 (素朴実装)
	100,000 (対策実装)
動作周波数	2 MHz

表 A4.2　Enocoro-128v2 のサイドチャネル測定環境

ISE バージョン	12.4
FPGA ボード	SASEBO-GII LX50
オシロスコープ	Agilent infiniium MSO 9104A
サンプリング周波数	1 GHz
波形数	10,000 (素朴実装)
	100,000 (対策実装)
動作周波数	2 MHz

2 種類のオシロスコープが使用されているのは、片方(Agilent)が故障したためである。

（２） FPGA 実装での性能

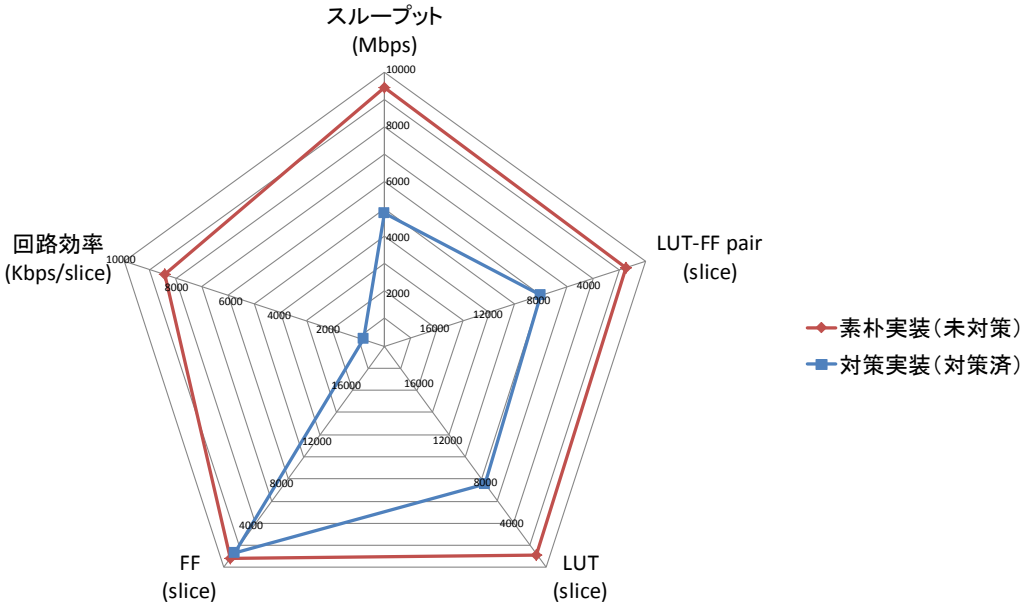


図 A4.1　CLEFIA の FPGA 実装評価結果

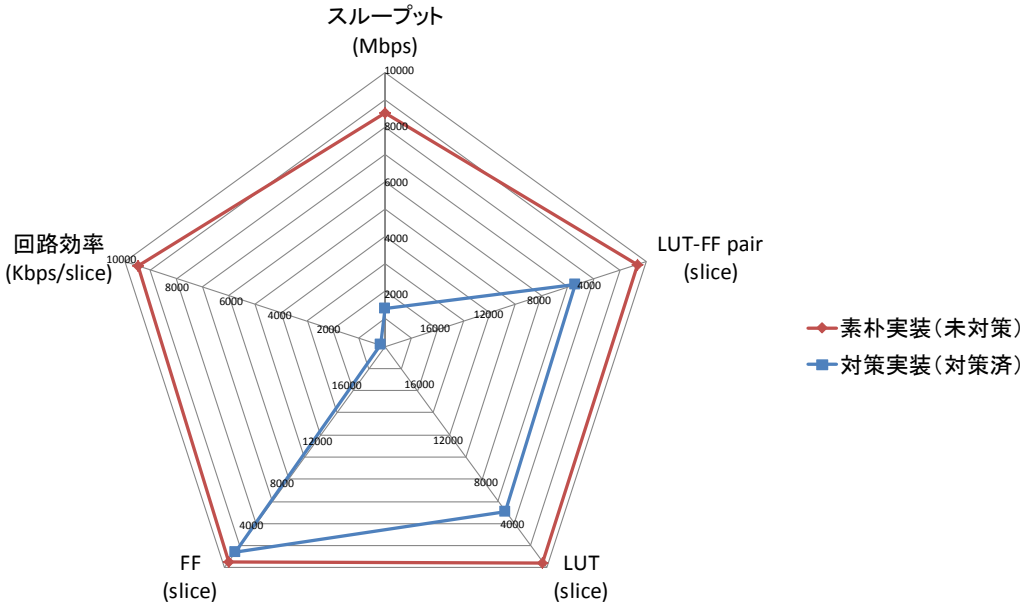


図 A4.2　　Enocoro-128v2 の FPGA 実装評価結果

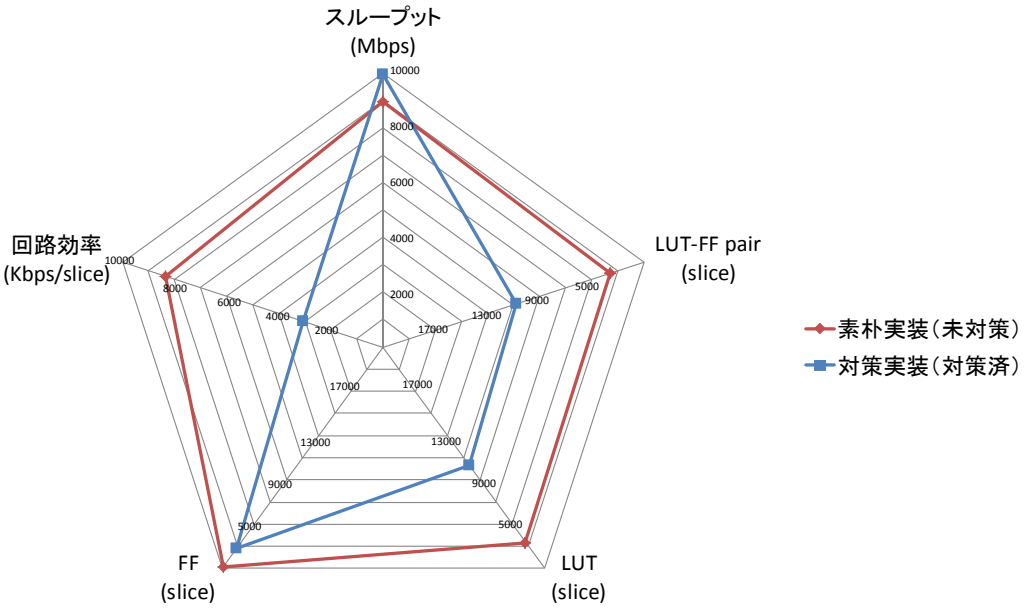


図 A4.3　KCipher-2 の FPGA 実装評価結果

（3） サイドチャネル攻撃対策の有効性確認結果

攻撃結果を図 A4.4～A4.9 に示す。図で正解鍵を太線で、その他を細い線で示した。3 種類の暗号とも、素朴実装では 2,000～4,000 波形で正解鍵が優勢になるのに対し、対策実装では 10 万波形でも正解鍵がその他の中に埋もれたままとなっており、対策の効果が確認できる。

(A) CLEFIA に対する攻撃

CLEFIA の対策実装では攻撃対策として、二線式プリチャージ・ロジックおよび乱数を用いたマスキングが使用されている。二線式プリチャージ・ロジックはサイドチャネル攻撃対策として代表的なものであるが、実装コストも高い。そのため、素朴実装と対策実装の回路規模の差が大きくなっている。

応募者が提示した選択関数は推定するビット数が大きく、鍵の全探索が困難だった。そこで、正解鍵を含む 8 種類の鍵を候補とした。攻撃結果を図 A4.4, A4.5 に示したが、素朴実装では 2,000 波形付近で正解鍵が優勢になるのに対し、対策実装では 10 万波形に至るまで正解鍵はその他鍵に埋もれており、対策の有効性が確認された。

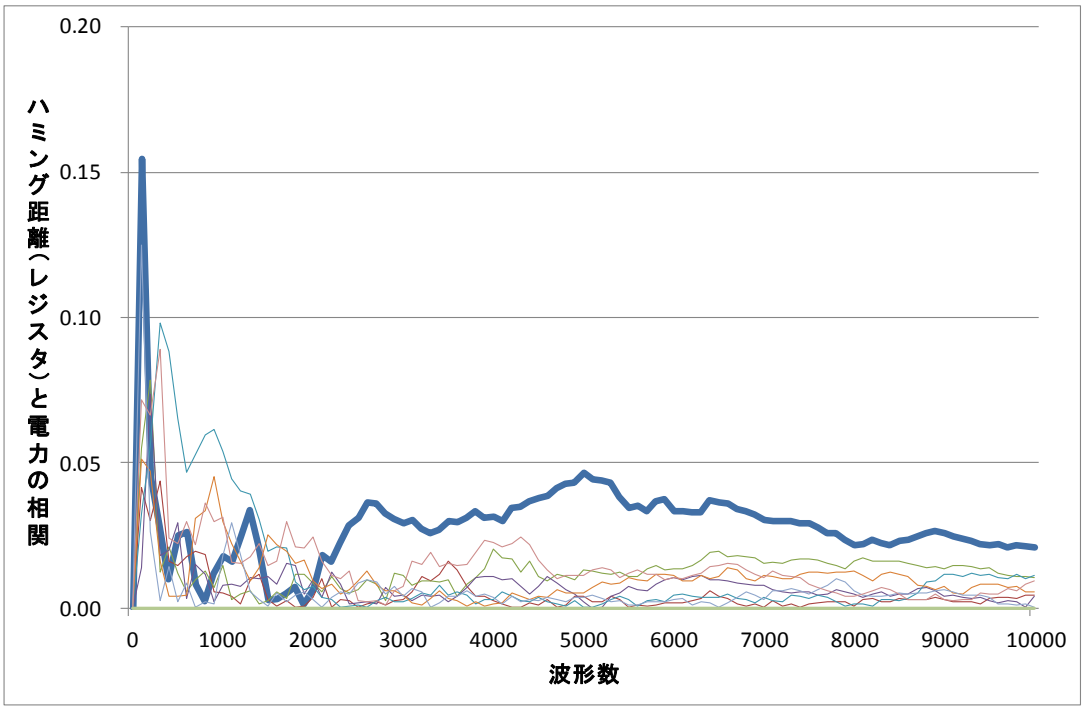


図 A4.4　CLEFIA の素朴実装に対する攻撃結果

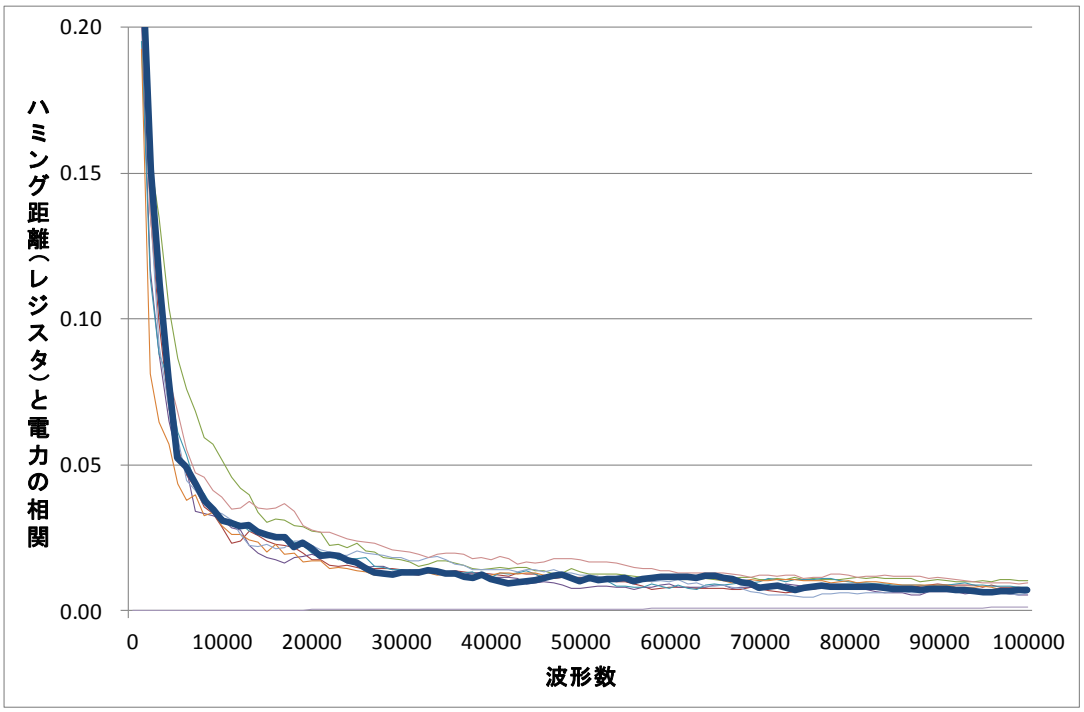


図 A4.5　CLEFIA の対策実装に対する攻撃結果

(B) Enocoro-128v2 に対する攻撃

Enocoro-128v2 の対策実装では攻撃対策として、2 個の乱数マスクを使用した Threshold Implementation (TI)が使用されている。TI は一般に DPA 対策として優れているが、実装コストも高い。そのため、素朴実装と対策実装の回路規模の差が大きくなっている。

応募者が提示した選択関数はレジスタの 8 ビットを対象とするもので、鍵の全探索が可能であり、正解鍵を含む 256 種類の鍵を候補とした。攻撃結果を図 A4.6, A4.7 に示したが、素朴実装では 4,000 波形付近で正解鍵が優勢になるのに対し、対策実装では 10 万波形に至るまで正解鍵はその他鍵に埋もれており、対策の有効性が確認された。

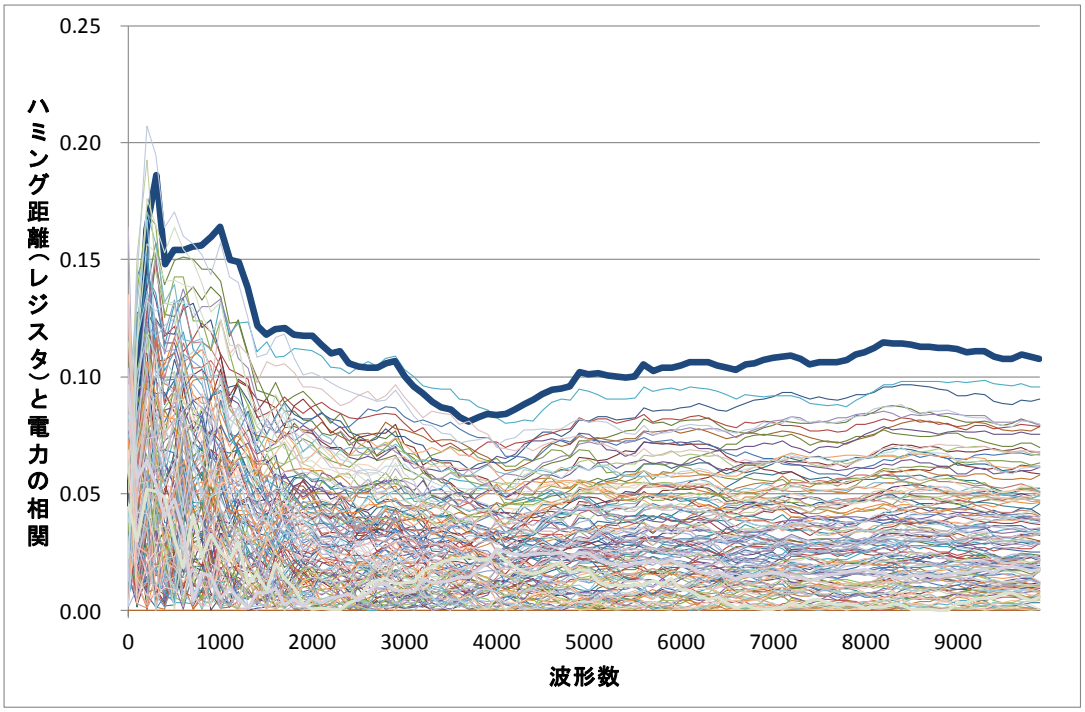


図 A4.6　Enocoro-128v2 の素朴実装に対する攻撃結果

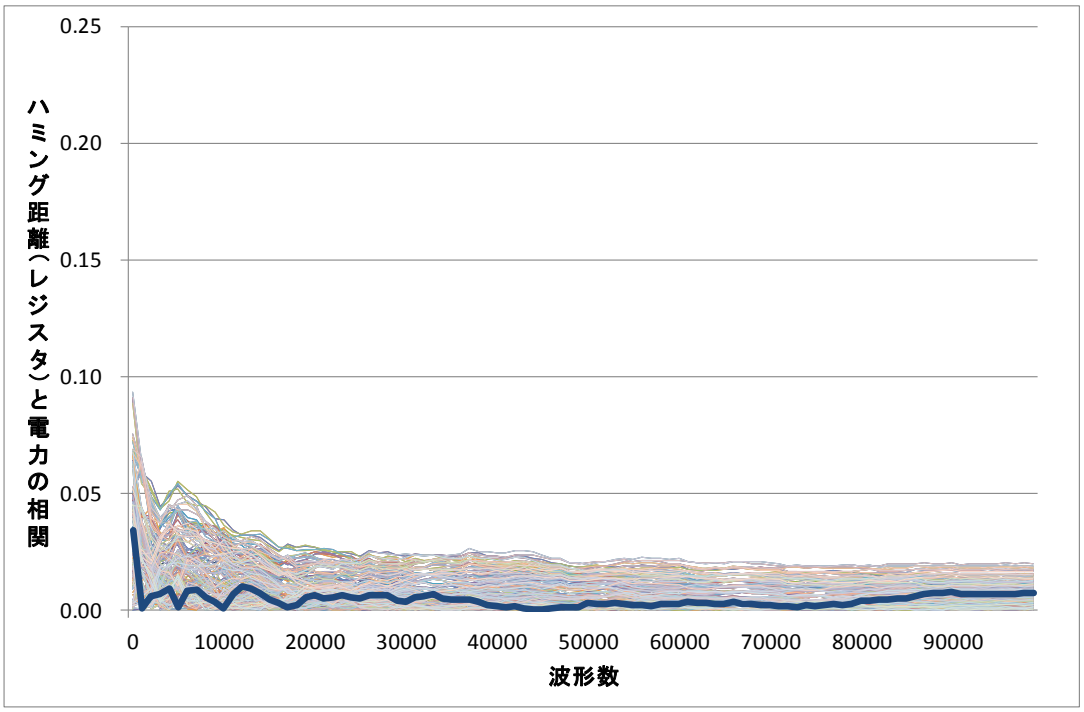


図 A4.7　Enocoro-128v2 の対策実装に対する攻撃結果

(C) KCipher-2 に対する攻撃

KCipher-2 の対策実装では攻撃対策として、乱数マスクが使用されている。

応募者が提示した選択関数のうち、シフトレジスタの 8 ビットを対象とし、正解鍵を含む 256 種類の鍵を候補とした。攻撃結果を図 A4.8, A4.9 に示したが、素朴実装では 2,000 波形付近で正解鍵が優勢になるのに対し、対策実装では 10 万波形に至るまで正解鍵はその他鍵に埋もれており、対策の有効性が確認された。

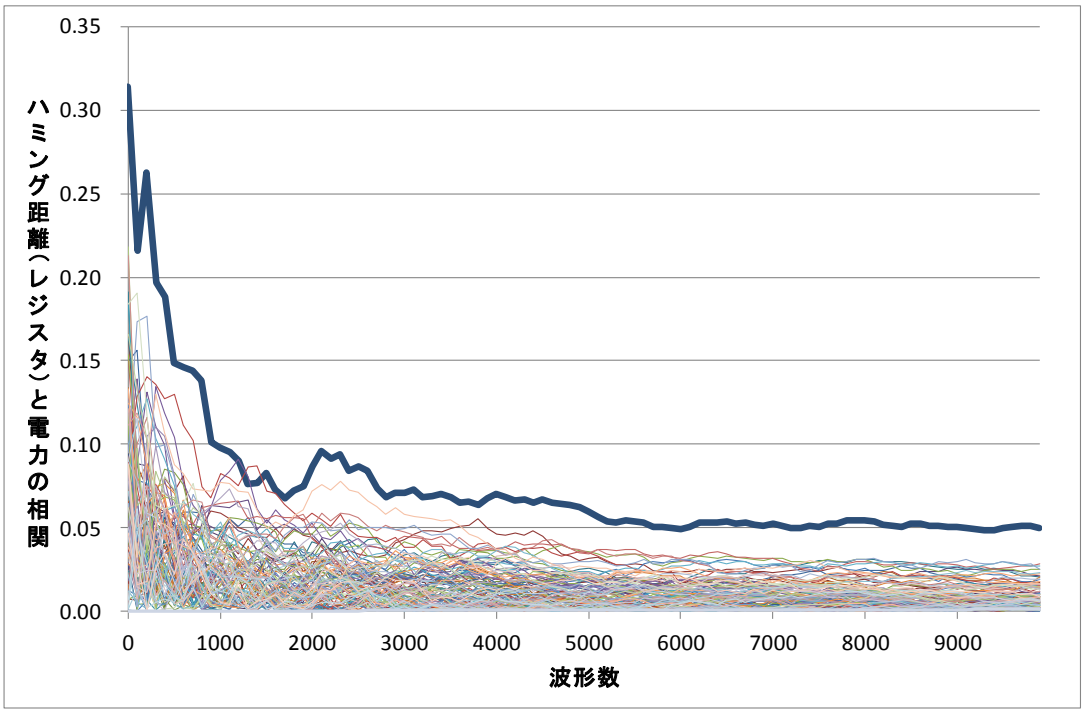


図 A4.8　KCipher-2 の素朴実装に対する攻撃結果

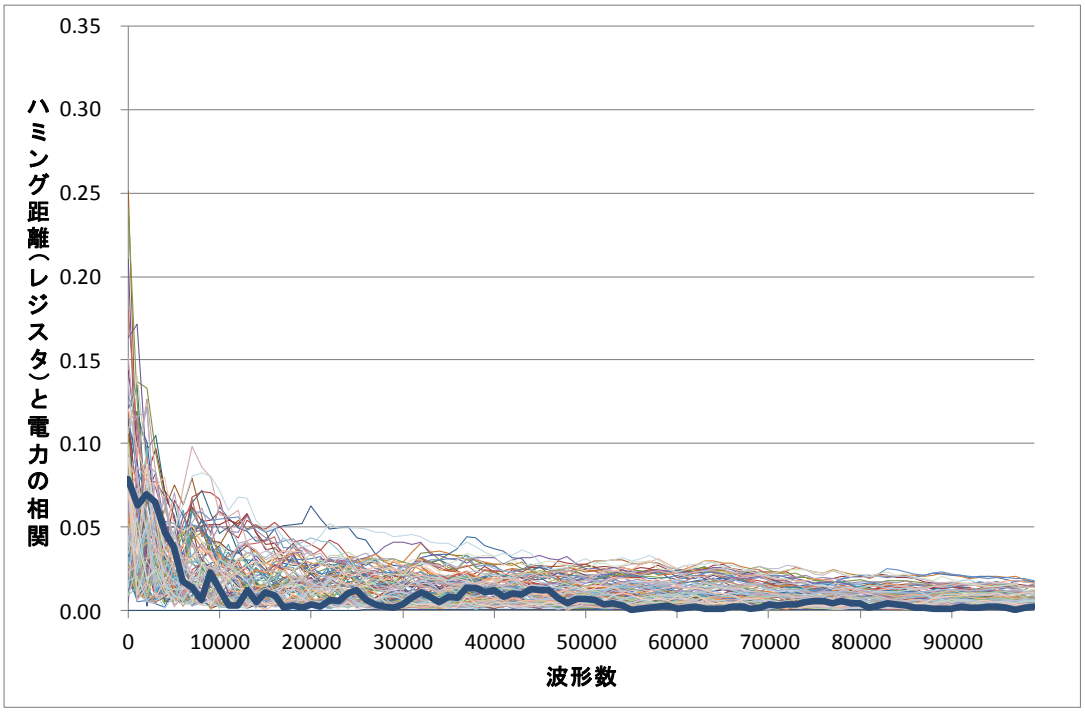


図 A4.9　KCipher-2 の対策実装に対する攻撃結果

付録5　ISO/IEC 3rd WD 17825に対するコメント

CRYPTREC comments on ISO/IEC 3rd WD 17825

Date: 2013-03-29	Document: **SC 27 N11783**

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**
JP1			ge	Not taken into account experimental environments such as sampling rate, measuring points and so on. They have a big impact on the results of the attack (evaluation).	Experimental environments should be discussed.	
JP2	6	Fig.5	te	Variation of EMA attack methods is not sufficient. Fundamentally, any PA attack method has its correspondence in EMA.	Add the following into Figure 5: C-EMA, MI-EMA, LR-EMA, 20ML-EMA, 20D-EMA	
JP3	6		ge	The following sentences should be included. (The place of inclusion is not limited to Clause 6.) 1) The number of Attack methods will increase in the future. 2) Testing laboratories can add appropriate and/or specific attack methods which are not included in this standard.		
JP4	6		ge	The introduced taxonomy seems to be not applied in the rest of this document.	Review and redraft the text.	
JP5	6	Fig 5	ed	The numbering of the figure is incorrect	Change the figure title to "Figure 6.1".	
JP6	6	Fig 5	ed	The figure is not in the form of line drawings and is not consistent with 6.6.5.2 of ISO/IEC Directives, Part 2.	Please change the figure to line drawings.	

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.

CRYPTREC comments on ISO/IEC 3rd WD 17825

Date: 2013-03-29	Document: **SC 27 N11783**

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**
JP7	6	NOTE 3, step 7	ed	“back to step 3“ is incorrect.	“back to step 4”	
JP8	6	NOTE3 NOTE4 NOTE5 NOTE6 NOTE7	ed	Symbols in these notes are hard to identify.	Please redraft the texts so that readers can easy to identify and easy to understand the contents.	
JP9	7	P6, L16	ed	A large space between “International” and “Standard”	Delete the space	
JP10	7	Table 7.1	ge	RNG and RBG	Two types of “true” and “pseudo” RNG (RBG) should be separately considered.	
JP11	8		te	Not taken into account capability of attackers (evaluators)	The capability should be discussed.	
JP12	8.3	Figure 8.3	te	The tolerance level is not provided.	Please define tolerance level.	
JP13	8.3		ed	The definition of CSP class is missing.	Please define CSP class in Clause 3.	
JP12	8.4	Paragraph 2	ed	Table 8.2 is missing.	Correct the table reference.	

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.

CRYPTREC comments on ISO/IEC 3rd WD 17825

Date: 2013-03-29	Document: **SC 27 N11783**

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**
JP14	8.4 8.5		ge	DPA seems to be supposed in the whole description, although there appears DPA (DEMA) in the caption of two figures. (For example, the title of Clause 8.5.1.1 is "SPA and TA", but SEMA should be included)	It should be noted that the descriptions on PA are also applicable to EMA.	
JP15	8.4, 8.5		te	(1) (1) In Clause 8.4, there are descriptions on DPA/DEMA, but no descriptions on SPA/SEMA and TA which are included for Symmetric-Key in Table 7.1. (2) (2) There are descriptions on Signature and Key agreement in Clause 8.5 "Leakage Analysis for Asymmetric Key Ciphers". But Key agreement is classified in other categories in Table 7.1. (3) (3) There are no reference to Security functions marked as A in Table 7.1.For example, it is not clear howe to test SPA on RNG in the flow of Figure 8.3.(The same traces are not always derived for randam number sequences.)	The descriptions of Clauses 8.4 and 8.5 should revised such that all test methods marked "A" in Table 7.1 are covered. And the clause titles should be changed such that they correspond to their contents.	
JP16	8.4 & 9.2.3		te	It is not clear whether the device passes or fails the test, when a significance level is calculated for each of 128 bits	Rewrite such that judgement criteria become clear.	

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.

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 AES by DPA, and only one bit does not satisfy the 0.95 criterion.		
JP17	8.5	Paragraph 3	ge	There is the following description: "they also depend on the performance, complexity, compactness and targeted security level, and therefore result from a necessary tradeoff" This kind of description can be a guide to vendor or manufacture, but is deviating from the main purpose of this International Standard, "Testing methods for the mitigation of non-invasive attack classes against cryptographic modules".	Move any sentences that would be regarded as guides for vendor or manufacture to NOTE or Annex.	
JP18	8.5, 8.5.1, 8.5.3		ed	Hanging paragraphs can be found. Please see 5.2.4 of ISO/IEC Directives, Part 2.	Redraft the text so that there is no hanging paragraph.	
JP19	8.5.1.1		ed	The table should be attached with a caption including the	Add the caption, such as "Table 8.2 :	

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.

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**
				number and title.	Leakage models for RSA".	
JP20 櫻井	8.5.3	Paragraph 2	ed	levels 5 and 6 are not defined in Clause 1, Scope.	Remove levels 5 and 6.	
JP21	9.2.1 9.3.1		te	The maximum measurement time should not be given.	Remove these clauses (9.2.1 and 9.3.1).	
JP22	9.2.2 9.2.3 9.2.4 9.3.2 9.3.3 9.3.4		te	1) The maximum measurement waveform number should not be limited. The measurement of 1,000,000 to 10,000,000 waveforms is usual in research papers. The cryptographic module which can be attacked by 10,000 waveforms is out of consideration. 2) It is not reasonable to set the security level by the measurement waveform number. With practical measurement/analysis environment, measurement of 100,000 to 1,000,000 waveforms is not difficult to achieve.	1) The waveform number is set to be 1,000,000 waveforms or more for DPA/DEMA to symmetric ciphers, and 10,000 waveforms or more for other attacks. 2) The leaked information amount should be considered in testing (the number of broken Sboxes, e.g.).	
JP23	9.2.2		te	It is not clear about why 11 waveforms are used.	The rationale for 11 waveforms should be provided.	
JP24	9.2.2 9.2.4		te	"Pre-determined" values are used, but it is not clear about what kind of pre-determined values are used, and their	Please list the pre-determined values if any, with their effectiveness.	

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.

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**
	9.3.2 9.3.4			effectiveness.		
JP25	9.3.2		te	It is not clear about why 21 waveforms are used.	The rationale for 21 waveforms should be provided.	
JP26	9.3.3		ed	DPA variant attack is not specified in Figure 8.4.	Change Figure 8.4 to Clause 8.4.	
JP27	Bibliography		ge	Current bibliography is not sufficient.	Various documents should be added to bibliography.	

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　2013 年 4 月 30 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
（技術本部　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