CRYPTREC Report 2006

平成 19 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

「暗号モジュール委員会報告」

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モジュール委員会の 2006 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いる。

海外では既に米国とカナダが共同で、FIPS 140-2 という政府調達基準に基づいて暗号モジュールに関する試験・認証制度を運用している。また、ISO/IEC JTC 1/SC 27/WG 3 においては、暗号モジュールセキュリティ要件の国際規格 ISO/IEC 19790 が完成し、暗号モジュール試験要件の企画作成が進められている。これらの動向を考慮し、暗号モジュール委員会においては、わが国における暗号モジュールセキュリティ要件、試験要件の原案検討作業を、2003 年度より開始し、進めてきた。

本年度は、ISO/IEC JTC 1/SC 27/WG 3 において作成された国際規格 ISO/IEC 19790 に対応した暗号モジュールセキュリティ要件の翻訳版の作成と、それに対応する試験要件を行うとともに、サイドチャネル攻撃などの暗号モジュールに対する攻撃法や対策の調査研究を実施し、将来のセキュリティ要件への適用の準備を進めた。本活動を契機として、わが国における暗号実装関連技術の研究が進展することを期待したい。

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。

暗号モジュール委員会　委員長　松本　勉

本報告書の利用にあたって

本報告書は、一般的な情報セキュリティの基礎知識を有している読者を想定している。例えば､電子署名や GPKI 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 章には暗号モジュール委員会の活動の背景と目的、第 2 章には暗号モジュール委員会の委員会開催状況、第 3 章には暗号モジュール委員会の活動内容と成果概要を記述した。

2005 年度以前の CRYPTREC Report は、下記 URL で参照できる。

http://www.cryptrec.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.jp

委員会構成

暗号モジュール委員会は、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。

暗号モジュール委員会では、ISO/IEC 等の国際標準の動向を注視しつつ、将来的に政府調達基準等として利用されることをも視野に入れながら、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。

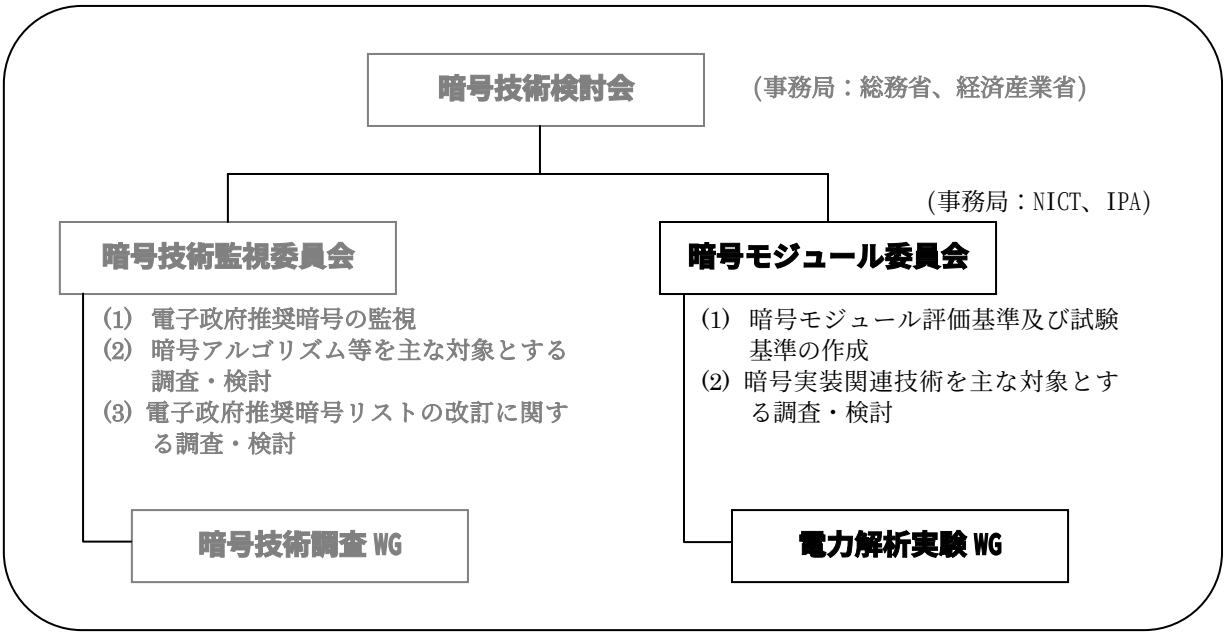

図１　2006 年度の CRYPTREC の体制

委員名簿

暗号モジュール委員会　(2007 年 3 月現在)

委員長	松本　勉	国立大学法人横浜国立大学 大学院　教授
委員	石田　修一	株式会社日立製作所　研究員 (2006 年 9 月まで)
委員	植村　泰佳	電子商取引安全技術研究組合　常務理事
委員	大須賀　勝美	NTT エレクトロニクス株式会社　技術主査
委員	太田　和夫	国立大学法人電気通信大学　教授
委員	大塚　浩昭	日本電信電話株式会社
委員	亀田　繁	財団法人日本情報処理開発協会　センター長
委員	佐伯　稔	三菱電機株式会社　主席研究員
委員	佐藤　証	日本アイ・ビー・エム株式会社　主任研究員
委員	高橋　芳夫	株式会社 NTT データ　シニアエキスパート
委員	角尾　幸保	日本電気株式会社　主席研究員
委員	栃窪　孝也	日本大学　専任講師
委員	鳥居　直哉	株式会社富士通研究所　部長
委員	古屋　聡一	株式会社日立製作所　研究員
委員	森岡　澄夫	日本電気株式会社　主任研究員
委員	横田　薫	松下電器産業株式会社　主任技師
委員	吉田　健一郎	財団法人日本品質保証機構　参与

オブザーバ

山田　浩一	警察庁　情報通信局(2005 年 7 月まで)
中山　毅彦	警察庁　情報通信局(2005 年 7 月まで)
金剛　章	警察庁　情報通信局
谷川　健	警察庁　情報通信局
平間　弘法	警察大学校　警察情報通信研究センター
山本　寛繁	総務省　行政管理局
藤田　和重	総務省　情報通信政策局
能登　治	総務省　情報通信政策局(2006 年 7 月まで)
増子　喬紀	総務省　情報通信政策局(2006 年 7 月まで)
川崎　光博	総務省　情報通信政策局

網野　尚子　　総務省　情報通信政策局
山元　明裕　　外務省　大臣官房
森田　信輝　　経済産業省　産業技術環境局
小野塚　直人　経済産業省　商務情報政策局
太田　保光　　経済産業省　商務情報政策局
神藤　守　　防衛省　陸上幕僚監部
石川　正興　　防衛省　技術研究本部
武田　仁己　　防衛省　運用企画局
滝澤　修　　独立行政法人 情報通信研究機構
川村　信一　　財団法人日本規格協会
瀬戸　洋一　　財団法人日本規格協会
山中　正幸　　財団法人日本規格協会

電力解析実験ワーキンググループ　(2007 年 3 月現在)

委員長	松本　勉	国立大学法人横浜国立大学 大学院　教授
委員	太田　和夫	電気通信大学　教授
委員	栃窪　孝也	日本大学　専任講師
委員	山村　明弘	独立行政法人情報通信研究機構　グループリーダ
委員	黒川　恭一	防衛大学校　助教授
委員	後藤　敏	早稲田大学　大学院　教授
委員	古屋　聡一	株式会社日立製作所　研究員
委員	井上　弘士	国立大学法人九州大学　大学院　助教授
委員	角尾　幸保	日本電気株式会社　主席研究員
委員	高橋　芳夫	株式会社 NTT データ　シニアエキスパート
委員	佐藤　証	日本アイ・ビー・エム株式会社　課長
委員	佐藤　恒夫	三菱電機株式会社　チームリーダー
委員	森岡　澄夫	日本電気株式会社　主任研究員
委員	山越　公洋	日本電信電話株式会社　研究主任
委員	深澤　宏	NEC マイクロシステム株式会社　主任
委員	鳥居　直哉	株式会社富士通研究所　部長
委員	藤崎　浩一	株式会社東芝　研究主務
委員	本間　尚文	国立大学法人東北大学　大学院　助手
委員	今福　健太郎	独立行政法人産業技術総合研究所　研究チーム長

事務局

独立行政法人 情報処理推進機構

三角育生、山岸篤弘、大塚玲、大熊建司、杉田誠、大久保美也子、
伊東徹（平成 18 年 9 月から）、鈴木幸子（平成 18 年 12 月から）

独立行政法人 情報通信研究機構

篠田陽一、山村明弘、黒川貴司、松尾真一郎、松尾俊彦、金森祥子

第１章　活動の背景と目的

1.1　CRYPTREC 活動の経緯

近年のインターネットの爆発的な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。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進められている。e-Japan 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。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する。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する。

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である、暗号モジュールに対して、動作の信頼性や安全性を評価する基準をセキュリティ要件と呼び、国際的な影響力を持つものには次の２つがある。

(1)FIPS[1] 140-2 (米国NIST[2]、カナダCSE[3])

(2)ISO[4]/IEC[5] 19790

1.2.1 FIPS 140-2/140-3

FIPS 140-2 は、米国/カナダが共同運用しているCMVP[6]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に試験要件(DTR[7])と運用ガイダンス(IG[8])の 2 種類があり、NISTは必要に応じて適宜改訂している。DTRは暗号モジュール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/CSE[9]は 5 年ごとの定期見直しに従い、セキュリティ要件を次期バージョンFIPS 140-3 に改訂する作業を開始している。この準備及び周知のため、2004 年 9 月に“CMVP Symposium 2004”を開催した。2005 年 9 月には、FIPS 140-3 に盛り込むべき物理セキュリティ関連技術をテーマとした“NIST Physical Security Testing Workshop”が開催された。ここで、2007 年 3 月のFIPS 140-3 発効予定、2007 年 9 月のFIPS 140-2 の廃止予定というスケジュールが発表された。しかし、予定は大幅に遅れる見込みであり、2007 年 3 月 15 日現在、ドラフトすら公開されていない状況である。

---

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

1.2.2 ISO/IEC 19790

ISO/IEC 19790 は、FIPS 140-2 を元に作られた国際規格である。ISO/IEC JTC 1[10] SC 27/WG 3 のプロジェクトとして審議され、2005 年 12 月締め切りで行われたFDIS[11]投票で可決され、国際事務局の修正後 2006 年 3 月 1 日に発行された。

また、実際の運用に必要であるということで、FIPS 140-2 同様、ISO/IEC 19790 に対する試験要件の標準化が新規プロジェクトとして承認され、規格番号 24759 が割り当てられている。2005 年 11 月のKuala Lumpurでプロジェクトの承認が報告され、エディタとして Randy Easter(米国NIST)、コエディタとしてJean-Pierre Quemard(仏)とHans von Sommerfeldが任命された。2007 年 3 月現在、1st CD[12]の投票中で、今後、順調に進めば、2007 年 5 月のロシア会合で 1st CD案のコメント処理を経てFCD投票に進み、2008 年には規格化される見込みである。

米国NISTはFIPS 140-2 の後継として準備中のFIPS 140-3 の国際規格化をSC 27 のロシア会合に新規検討事項(NP[13])として提案する予定である。NISTは、FIPS 140-2 のIS版であるISO/IEC 19790 とは別に、FIPS 140-3 のIS版を作りたい意向だと伝えられているが、JTC 1 としては例外的な扱いであり、今後の進行は予断を許さない。

1.3 暗号モジュール委員会の活動状況

1.3.1 過去の経緯

暗号を組み込んだ製品の安全性を実現するには、安全性が確認された暗号の利用が不可欠であり、2003 年 2 月に発表された電子政府推奨暗号リストに記載された暗号から選択することによりこの条件は満たされる。しかし、暗号を組み込んだ製品の安全性を保つにはこれだけでは不十分であり、暗号アルゴリズムが適切に実装されていることを確認する必要がある。

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[14]及び試験基準[15]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

---

[10] Joint Technical Committee 1
[11] Final Draft International Standard
[12] Committee Draft
[13] New Work Item Proposal
[14] 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。
[15] 2005 年度の活動で、「試験基準」は「試験要件」に変更された。

(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[16]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。

[16] Field Programmable Gate Array

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[17]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、「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 PUB 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

[17] Information Technology Research and Standardization Center, JSA／(財)日本規格協会 情報技術標準化研究センター

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ている。

1.3.2 2006 年度の活動概要

2006 年度暗号モジュール委員会の活動方針

(1)ISO/IEC 24759 への技術コメント作成協力

FIPS 140-2 を元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。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、24759 のドラフトを検討し、SC 27 の国内委員会に対し、コメント案の作成に協力する。

(2)FIPS 140-3 の動向調査

NIST は、2007 年に FIPS 140-2 を 140-3 に改訂する準備を進めている。今年度中にドラフトが発行される予定であり、日本としてコメントをまとめるべく、調査活動を行う。

(3)電力解析実験の取りまとめ

電力解析実験の知見を収集するため、評価用標準プラットフォームとして、2004 年度に 8 ビット CPU 版、2005 年度に 32 ビット CPU・FPGA 版を開発し、希望する委員に配布して実験を行っている。今年度は個々の実験を束ね、具体的なセキュリティ要件、試験要件の提案に結びつけるための活動を開始する。

2006 年度暗号モジュール委員会の成果

今年度の暗号モジュール委員会の成果としては、次の 2 つが挙げられる。

(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 のドラフト 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／INSTAC-32 仕様に準拠した標準プラットフォームを希望する委員に配布し、実験データの収集を進めてきた。今年度は、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、2006 年 3 月発行予定の次の 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」

第 2 章　活動内容と成果概要

2.1　暗号モジュールセキュリティ要件等の策定

2.1.1　北米における暗号モジュールセキュリティ要件関連の動向

(1)FIPS 140-2 (SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES)

FIPS 140 は、コンピュータシステム及び電気通信システム内の暗号モジュールに対するセキュリティ要件を規定した、NIST が発行する米国連邦標準規格である。

FIPS 140 は､政府及び産業界で構成されたワーキンググループによって開発された。1994 年 1 月に FIPS 140-1 が制定され､2001 年 5 月には FIPS 140-2 として改訂された。FIPS 140-2 は、ベンダ、試験機関、及びユーザ団体から寄せられたコメントに基づいた変更だけでなく、FIPS 140-1 が開発された以降に利用可能となった標準規格及び技術の変更も取り入れている。FIPS 140-2 は適宜改訂されており、2002 年 12 月の改訂版が 2007 年 3 月時点での最新版となっている。

FIPS 140-2 は、暗号モジュールのセキュアな設計及び実装のために、暗号モジュールが満たすべき 11 分野(暗号モジュールの仕様、暗号モジュールのポート及びインタフェース、役割・サービス・認証、有限状態モデル、物理的セキュリティ、動作環境、暗号鍵管理、電磁妨害/電磁両立性、自己テスト、設計保証、その他の攻撃への対処)のセキュリティ要求事項を規定しており、さらに、保護すべきデータの重要性と使用環境に応じて暗号モジュールを提供できるように、分野ごとに 4 段階のセキュリティレベル(セキュリティレベル 1～4)を規定している。

(2)DTR (Derived Test Requirements for FIPS PUB 140-2)

DTR は、暗号モジュールが FIPS 140-2 で規定されたセキュリティ要求事項を満たしているかどうかを試験する際に、試験者が実施しなければならない試験手順及びベンダが提供しなければならない情報を規定したものである。

DTR は FIP 140-2 と同様に適宜改訂されており、2004 年 3 月 24 日の改訂版が 2007 年 3 月時点での最新版となっている。

DTRは、全 11 章から構成されており、各章はFIPS 140-2 で規定された 11 分野に対応している。各章では、FIPS 140-2 に対応するセキュリティ要求事項をアサーション[18]として記述している。全てのアサーションはFIPS 140-2 から直接引用している。

各アサーションの次には、順に、ベンダが提供しなければならない情報[19]、試験者

[18] Assertion (ASと略す)。暗号モジュールが、設定された分野のセキュリティ要件を、設定されたセキュリティレベルで満足するために適用しなければならない宣言。
[19] Vender Evidence (VEと略す)

が実施しなければならない試験手順[20]を記述している。

(3) Implementation Guidance

Implementation Guidance は、CMVP、特に DTR に関する、ベンダや試験機関等からの問合せに対して、NIST 及び CSE が回答したコメントを CMVP に関するガイダンスとしてまとめたものである。

Implementation Guidance もFIPS 140-2 及びDTRと同様に適宜改訂されており、2007 年 3 月の改訂版[21]が 2007 年 3 月時点での最新版となっている。

Implementation Guidance は、全 17 節(OVERVIEW, GENERAL ISSUES, SECTION 1 から SECTION 14, EXPIRED IMPLEMENTAITON GUIDANCE)から構成される。

“SECTION 1 から SECTION 14”は、次図のように FIPS 140-2 の各節とそれぞれ対応しており、セキュリティ要件の分野ごとに整理され、記述されている。また、複数の分野に当てはまる内容については、最適な分野の SECTION に記述されている。

Implementation Guidance	FIPS 140-2
SECTION 1 ～ SECTION 11	4.1 ～ 4.11
SECTION 12	APPENDIX A
SECTION 13	APPENDIX B
SECTION 14	APPENDIX C

“OVERVIEW”には“Implementation Guidance”の概要が記述されており、“GENERAL ISSUES”には、SECTION 1 から SECTION 14 の分野に特定されない全般的な問題が整理され、記述されている。また、取消された運用ガイダンスを記述するために、“EXPIRED IMPLEMENTAITON GUIDANCE”の節が用意されているが、現在、何も記述されていない。

(4)FIPS 140-2 の FIPS 140-3 への改訂

近年の暗号モジュールの実装や攻撃法に関する進歩は目覚しく、2001 年に発効した FIPS 140-2 は現状に合わなくなってきている。そこで、NISTは 5 年見直しとして、2006 年を目処とした後継のFIPS 140-3 への移行準備を進めてきた。その一環として、2004 年 9 月にメリーランド州でCMVP 2004 シンポジウム[22]、2005 年 9 月に物理セキュリティ試験のワークショップ[23]が開かれ、FIPS 140-3 に関する議論が行われるとともに、移行計画が発表されてきた。

---

[20] Tester Evidence (TEと略す)
[21] 日本語版は 2005 年 12 月の改訂版が 2007 年 3 月時点での最新版となっている。
[22] CMVP 2004 Symposium: http://csrc.nist.gov/cryptval/cmvp2004/
[23] Physical Security Testing Workshop:
http://csrc.nist.gov/cryptval/physec/physecdoc.html

2006 年 12 月 17 日～22 日には、米国ワシントンDC近郊のメリーランド州 ゲイザースバーグでNISTの情報セキュリティ関連部門CSD[24]とIPAセキュリティセンターの定期会議が開催され、テーマの一つとして暗号モジュール試験及び認証制度が取り上げられた。参加者は、28 名で、内訳は次の通りであった。

米国 NIST(13)、米国商務省(1)、カナダ CSE(1)、経済産業省(2)、産業技術総合研究所(2)、日本規格協会(2)、NRI セキュアテクノロジーズ(1)、IPA(6)、

この会議は NIST の CSD と IPA セキュリティセンターが定期的に開催するものであり、今回、暗号モジュール試験及び認証制度が５つの主要議題の１つとして選ばれ、12 月 18 日午後に実施された。

＜FIPS 140-3 の概要＞

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

・セキュリレベルは 5 レベルとなる（FIPS 140-2 は 4 レベルであり、2004 年 9 月の CMVP 2004 では 6 レベルとすることが示唆されていた)。

・11 章からなる。EMI[25]に関する章は無くなった。FSM[26]はデザインアシュアランス（設計保証）の章に入れた。

・新しい章（分野）は 2 つ増えた。ひとつは、ソフトウエアセキュリティ、あとのひとつはnon-invasive attack [27]（非破壊攻撃)。

・ソフトウエアセキュリティの中にはハードウェア、ソフトウェア、ハイブリッドの 3 タイプのモジュールがある。ハイブリッドモジュールは IG1.9 に定義されている。

・非破壊攻撃は、FIPS 140-2 では、4 章 11 節の Mitigation of Other Attacks で記述していた。FIPS 140-3 では、独立させるとともに、セキュリレベル 3 から 5 までのレベルで要求する。但し、要求内容は FIPS 140-2 レベルであり、DTR でもっと詳しく書く予定である。

＜FIPS 140-3 への改訂スケジュールについて＞

この会議において、FIPS 140-3 への改訂スケジュールが次のように説明された。

・2007 年 1 月中　Draft を CMVP 内部(NIST＋CSE)でレビュー。

・2007 年 1 月　　レビュー結果を反映した版を各試験機関でレビュー。

---

[24] Computer Security Division

[25] EMI: Electro Magnetic Interference電磁妨害

[26] FSM: 有限状態モデル（Finite State Model)。暗号モジュールの動作を、有限状態モデルとして記述する。

[27] 非破壊攻撃：暗号モジュールに対して、物理的な侵入（カバーへ穴を開ける等の物理的手段を伴う侵入）を伴わない解析技術。代表的なものとしては、電力解析攻撃、故障誘導攻撃などがある。

・2007 年 1 月末　1st Draft を開示。90 日間のコメント募集期間を設ける。
・2007 年 4 月末　1st Draft に対するコメント募集の〆切。
・2007 年 春　　CMVP Symposium 2007 を開催
・2007 年 夏　　2nd Draft を開示。短期のパブリックコメント募集。
・2007 年 秋　　米国商務省による承認。

しかしながら、2007 年 3 月現在、試験機関に対する Draft も配布されておらず、作業は大幅に遅れており、次のようにシフトされることが予想されている。

・2007 年 3 月中　レビュー結果を反映した版を各試験機関でレビュー。
・2007 年 3 月末　1st Draft を開示。90 日間のコメント募集期間を設ける。
・2007 年 6 月末　1st Draft に対するコメント募集の〆切。
・2007 年 夏～秋　CMVP Symposium 2007 を開催
・2007 年 秋　　2nd Draft を開示。短期のパブリックコメント募集。
・2007 年 冬　　米国商務省による承認。

2.1.2　ISO/IEC における暗号モジュールセキュリティ要件関連の動向

(1)ISO/IEC JTC 1/SC 27/WG 3

ISO/IEC JTC 1 は、ISO と IEC が共同で運営する IT 技術標準化のための技術委員会で、その下の SC 27 委員会が情報セキュリティを担当している。その下の WG 3 で評価技術が情報セキュリティに関する評価基準などが扱われている。

(2)ISO/IEC 19790 (Security requirements for cryptographic modules)

ISO/IEC JTC 1/SC 27/WG 3 は、米国とカナダの提案に従い、2002 年 10 月から暗号モジュールセキュリティ要件の国際規格化を審議し、規格予定番号 19790 が割り当てられた。2005 年 10 月のマレーシア会合において FCD 案に対する編集作業が行われ、国際事務局による編集作業の後、2005 年 12 月には FDIS 投票が実施され、賛成多数で 2006 年 3 月 1 月に ISO/IEC 19790 として正式に発行された。

ISO/IEC 19790 は、FIPS 140-2 をベースとした基準であり、当初 CC(Common Criteria) への連接性を意識して記述様式を変更することが検討された。しかし、審議の進行に伴って CC に対する配慮は薄れ、その点に関する影響はほとんどなくなった。なお、暗号技術に関し、FIPS 140-2 では秘密鍵も公開鍵も CSP として区別しなかったのを秘密鍵は CSP、公開鍵は PSP と 2 種類に分解するなど、技術的な記述の精緻化が図られた。

(3)ISO/IEC 24759 (Test requirements for cryptographic modules)

2005 年 4 月のウィーン会合において、暗号モジュールセキュリティ要件の国際規格 ISO/IEC 19790 に付随して実際の試験に必要となる、暗号モジュール試験要件の規格化のプロジェクトが承認され、予定規格番号 24759 が割り当てられた。2006 年 5 月の

スペイン会合で WD、2006 年 11 月の南アフリカ会合で 1st CD に関する審議が行われ、2007 年 5 月のロシア会合において FCD に進むか否かが審議される。

ISO/IEC 24759 の章立てや 4 つのセキュリティレベルは FIPS 140-2 の DTR と基本的に同じである。ただし、FIPS 140-2 から ISO/IEC 19790 が作成された際の修正を整合性を保ちつつ反映させる必要がある。

2.1.3 2006 年度の暗号モジュール委員会の活動

2.1.3.1 海外動向への対応

今年度、暗号モジュール委員会では、暗号モジュールセキュリティ要件に関する海外動向に対応すべく、次の(1),(2)の作業を予定していた。

(1)暗号モジュール試験要件の国際規格 ISO/IEC 24759 へのコメント提案

ISO/IEC JTC 1/SC 27 において、セキュリティ要件の国際規格 ISO/IEC 19790 に対応した試験要件の規格 ISO/IEC 24795 が作成中であり、1st CD のドキュメントに対するコメント案を作成し、SC 27 の国内委員会に提出した。

(2)FIPS 140-3 の 1st Draft に対するコメント作成

当初、2006 年 11 月末にコメント募集用に公開されるはずだった FIPS 140-3 の 1st Draft に対する検討とコメント案作成を予定していた。しかし、2007 年 3 月 15 日現在、まだ発表されておらず、来年度に持ち越しになった。

2.1.3.2 セキュリティ要件等の作成

暗号モジュール委員会では、2005 年度末に ISO/IEC 19790 を和訳した「暗号モジュールセキュリティ要件」、FIPS 140-2 の DTR の和訳に FIPS 140-2 と ISO/IEC 19790 の差分を反映した「暗号モジュール試験要件(2006-03-31 版)、及び FIPS 140-2 の Implementation Guidance(2005 年 12 月版)を和訳した「暗号モジュール運用ガイダンス(2006-03-31 版)」の 3 つを作成した。ISO/IEC 規格の著作権を考慮し、セキュリティ要件と試験要件は公開せず、運用ガイダンスのみ公開した。今年度は文書作成の作業は休止している。

上記文書は、2007 年 3 月に発行される予定の暗号モジュール試験に関する JIS 規格の素案として利用された。具体的には、上記のセキュリティ要件は「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」、試験要件は「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」の素案となっている。

JIS X 19790 は、国際規格 ISO/IEC 19790 の和訳であり、一部用語の置き換えがあるものの、セキュリティ要件の翻訳がベースとなっている。また、JIS X 5091 は、国際規格 ISO/IEC 24759 の和訳となるべきところ、24759 が未完成のため、FIPS 140-2 の DTR の和訳に ISO/IEC 19790 の内容を反映させて作った試験要件がベースとなった。

「暗号モジュール運用ガイダンス」については、下記 URL にある「CRYPTREC Report

2005 運用ガイダンス 2006-03-01 版」として参照できる。

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

2.2 電力解析実験ワーキンググループの設置

2.2.1 設置の経緯と目的

暗号モジュール、特にICカードのようなワンチップモジュールにとって、サイドチャネル攻撃は、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攻撃、SPA攻撃）等は、簡便な攻撃環境・リソースで実現することが可能となるため、今後の暗号モジュールでは、対策を施すことが必須となると考えられる。

一方、2003年以来、暗号モジュール委員会では、米国の暗号モジュールに対するセキュリティ要件（FIPS 140-2）やFIPS 140-2をベースとした国際規格（ISO/IEC 19790）を元に、暗号モジュールに対するセキュリティ要件、試験要件の検討を進めてきた。しかし、FIPS 140-2やISO/IEC 19790では、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に関する明確かつ具体的な規定が存在しない。

暗号モジュール委員会ではこのような現状を踏まえ、サイドチャネル攻撃に対するセキュリティ要件、試験要件に関する規定の作成を目的として、日本規格協会 情報技術標準化研究センター（INSTAC）で開発したINSTAC-8仕様及びINSTAC-32仕様に準拠した電力解析実験用評価ボードを配布し、実験結果の収集を行っている。この活動により、有益な実験結果が出始めている。しかし、活動全体が組織化されていないため、今後、どのような成果が出て、いつ頃、セキュリティ要件、試験要件の規定にまとめられるかといった見通しが立っていない。

そこで、配布した電力解析実験評価用標準プラットフォーム等を利用した実験の方針を決め、実験データを収集・分析し、電力解析攻撃等のサイドチャネル攻撃に対するセキュリティ要件案・試験要件案を作成し国際標準化活動に対して貢献すべく、暗号モジュール委員会の下に電力解析実験ワーキンググループを設置した。

活動の具体的な項目は次の通り。

- 評価用標準プラットフォームを用いた実験手法の共通化
- 評価用標準プラットフォームを用いた実験結果の検討
- 経済産業省にて計画中の暗号処理LSIによる、実験の実施及びその実験結果の検討
- 暗号処理LSIと評価用標準プラットフォームでの実験結果比較検討
- 検討結果を用いた、セキュリティ要件案の作成
- サイドチャネル攻撃対策技術の試験要件・判定基準の作成

2.2.2 INSTAC-8/-32仕様準拠ボードを利用した研究成果

これまでに発表されたINSTAC-8/-32仕様準拠ボードを利用した電力解析実験関係の論文を収集し表１に示した。

表１　INSTAC 仕様準拠ボード関連電力解析関係発表論文リスト

	タ　イ　ト　ル	学会名・会議名	発表年月日	著　　者
1	8bitCPUを対象とした電力解析用評価環境の開発と実証実験	ISEC	2004/07/21	藤崎浩一、友枝裕樹、三宅秀享、駒野雄一、新保　淳、 川村信一（㈱東芝）
2	A5/1 に対するサイドチャネル攻撃（2D2-2）	SCIS2005	2005/01/26	一色寿幸（日本電気㈱）、辻原悦子（㈱ワイ・デー・ケー）、 峯松一彦、角尾幸保（日本電気㈱）
3	SBOXの特性を利用したDPA評価手法(4E1-1)	SCIS2005	2005/01/28	三宅秀享、野崎華恵、清水秀夫、新保　淳（㈱東芝）
4	INSTAC-8を用いたサイドチャネル攻撃に関する一考察（3T-1）	情報処理学会 第67回全国大会	2005/03/03	和田崇臣、甲斐切皇男、岩井啓輔、黒川恭一（防衛大学校）
5	CPUボード上のブロック暗号に対するサイドチャネル攻撃	ISEC	2005/03/17	高橋芳夫（㈱NTTデータ）、 福永利徳、大塚浩昭、神田雅透（㈱NTT）
6	32bitCPUを対象とした電力解析用評価環境の開発と実証実験	ISEC	2005/07/21	藤崎浩一、清水秀夫、新保　淳（㈱東芝）
7	Experimental Results on INSTAC-8 Compliant Board	NIST & IPA Physical Security Testing Workshop	2005/09/26	角尾幸保（JSA、日本電気㈱）、久門　亨（日本電気㈱）、 辻原悦子（(株)ワイ・デー・ケー）、松本　勉（JSA、横浜国立大学）、 川村信一、藤崎浩一（JSA、㈱東芝）
8	ストリーム暗号に対するDPA（1C3-2）	SCIS2006	2006/01/17	久門　亨、角尾幸保（日本電気㈱）、 後藤　敏、池永　剛（早稲田大学）
9	共通鍵暗号におけるテーブルを用いた電力差分解析対策法について(1C3-1)	SCIS2006	2006/01/17	宮崎隆行、辻村達徳、松本　勉（横浜国立大学）
10	汎用CPUにおけるサイドチャネル情報からの命令コードの解析(1C3-4)	SCIS2006	2006/01/17	山口晃由、山田敬喜（三菱電機㈱）
11	Sbox特性を利用したDPA評価手法の有効性検証(2C1-2)	SCIS2006	2006/01/18	三宅秀享、野崎華恵、清水秀夫、新保　淳（㈱東芝）
12	位相限定相関法に基づく高精度波形解析とそのサイドチャネル攻撃への応用	ISEC	2006/03/16	今井裕一、本間尚文、長嶋　聖、青木孝文（東北大）、 佐藤　証（日本アイ・ビー・エム㈱）
13	INSTAC-8 準拠評価ボードを使った実装攻撃実験の結果報告	ISEC	2006/03/16	角尾幸保（JSA、日本電気㈱）、久門　亨（日本電気㈱）、 辻原悦子（(株)ワイ・デー・ケー）、松本　勉（JSA、横浜国立大学）、 川村信一、藤崎浩一（JSA、㈱東芝）
14	ブロック暗号のマスク対策付FPGA実装に対するビット遷移に着目したDPAの適用	ISEC	2006/05/19	高橋芳夫（㈱NTTデータ、横浜国立大学）、松本　勉（横浜国立大学）、 佐藤　証（日本アイ・ビー・エム㈱）
15	漏洩電磁波による共通鍵暗号処理ハードウェアの動作解析(1F-11)	電気関係学会 東北支部連合大会	2006/08/31	菅原　健、本間尚文、青木孝文（東北大学）、 佐藤　証（日本アイ・ビー・エム㈱）
16	DPA対策実験による電力解析評価用プラットフォームの検証（M-052）	第5回情報科学技術フォーラム　FIT2006	2006/09/07	辻　洋平、岩井啓輔、黒川恭一（防衛大学校）
17	High-resolution side-channel attack using phase-based waveform matching	CHES 2006	2006/10/12	本間尚文 、長嶋 聖、今井裕一、青木孝文（東北大学）、 佐藤　証（日本アイ・ビー・エム㈱）
18	位相限定相関法による波形マッチングを用いた高精度差分電力解析法(1C-3)	CSS2006	2006/10/26	今井裕一、本間尚文、長嶋　聖、青木孝文（東北大学）、 佐藤　証（日本アイ・ビー・エム株式会社）
19	RSA暗号のFPGA実装に対するSPA耐性評価(4B-4)	CSS2006	2006/10/26	宮本篤志、本間尚文、青木孝文（東北大学）、 佐藤　証（日本アイ・ビー・エム㈱）
20	位相限定相関法に基づく高精度波形マッチング -- 暗号ハードウェアの動作解析への応用 --	第21回信号処理シンポジウム	2006/11/16	長嶋　聖、本間尚文、今井裕一、青木孝文（東北大学）、 佐藤　証（日本アイ・ビー・エム㈱）
21	テーブルネットワークを用いたFPGA実装AESとその電力差分解析耐性	ISEC	2006/11/17	辻村達徳（横浜国立大学）、高橋芳夫（横浜国立大学、㈱NTTデータ）、 松本　勉（横浜国立大学）
22	位相限定相関法を用いた高精度差分電力解析とそのノイズ耐性評価（2E4-5）	SCIS2007	2007/01/24	本間尚文 、長嶋　聖、今井裕一、青木孝文（東北大学）、 佐藤　証（日本アイ・ビー・エム㈱）
23	INSTAC-32準拠ボードを使用した電力解析自動化の適用例（2E4-6）	SCIS2007	2007/01/24	庄司陽彦、野澤　晃、木村隆幸（㈱ワイ・デー・ケー）、 久門　亨（日本電気㈱）、深澤　宏（NECマイクロシステム㈱）、 角尾幸保（日本電気㈱）
24	RSA暗号を実装したINSTAC-32に対するサイドチャネル攻撃実験（3E3-3）	SCIS2007	2007/01/25	深澤　宏、東　邦彦（NECマイクロシステム㈱）、 後藤　敏、池永　剛（早稲田大学）、角尾幸保、久門　亨（日本電気㈱）、 庄司陽彦（(株)ワイ・デー・ケー）
25	eSTREAM 提案暗号へのDPA解析報告(3E4-5)	SCIS2007	2007/01/25	久門 亨、角尾幸保（日本電気㈱）、深澤　宏（NECマイクロシステム㈱）、 庄司陽彦（㈱ワイ・デー・ケー）、後藤　敏、池永　剛（早稲田大学）
26	固定値入力を用いたRSA暗号ハードウェアに対するSPA（3E3-2）	SCIS2007	2007/01/25	本間尚文 、宮本篤志、青木孝文（東北大学）、 佐藤　証（日本アイ・ビー・エム㈱）
27	信号遅延を考慮したDPA耐性評価　--- MRSLとDRSLの場合 ---（3E3-1）	SCIS2007	2007/01/25	佐伯　稔（三菱電機㈱）
28	テーブルネットワーク型CPUボード実装AESの電力差分解析耐性(3E4-4)	SCIS2007	2007/01/25	鳥越　慎、辻村達徳（横浜国立大学）、 高橋芳夫（横浜国立大学、㈱NTTデータ）、松本　勉（横浜国立大学）
29	アンロールパイプライン型FPGA実装AESの電力差分解析耐性(3E4-3)	SCIS2007	2007/01/25	辻村達徳（横浜国立大学）、高橋芳夫（横浜国立大学、㈱NTTデータ）、 松本　勉（横浜国立大学）
30	INSTAC-32準拠プラットフォームを用いたRSAに対する故障利用攻撃実験	ISEC	2007/03/15	藤崎浩一、清水秀夫（㈱東芝）

ISEC：情報セキュリティ研究会（電子情報通信学会）
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）
CHES：Workshop on Cryptographic Hardware and Embedded Systems
（The International Association for Cryptologic Research ）
CSS：コンピュータセキュリティシンポジウム（情報処理学会）

(1) 8bitCPU を対象とした電力解析用評価環境の開発と実証実験 [藤崎浩一，友枝裕樹，三宅秀享，駒野雄一，新保　淳，川村信一（(株)東芝）] ISEC
暗号機能を搭載した機器に対して、暗号演算時の消費電力や演算時間などを用いて鍵情報を導出するサイドチャネル攻撃の研究が盛んに行われている。サイドチャンネル攻撃に対する標準的な実験評価環境がないために、提案されている攻撃手法および対策の有効性を統一的に評価することが難しいという問題があった。(財)日本企画協会情報技術標準化研究センター(INSTAC)耐タンパー性調査研究委員会では、平成 15 年度に 8bitCPU を対象としたサイドチャネル攻撃の標準的プラットフォームの仕様を策定し、インターネットを通じて公開している。この論文では、このプラットフォームの仕様を説明し、さらに本プラットフォームを用いて DES に対する差分電力攻撃(Differential Power Analysis)の実証実験を行った結果を報告している。

(2) A5/1 に対するサイドチャネル攻撃 [一色寿幸（日本電気株式会社），辻原悦子（(株)ワイ・デー・ケー），峯松一彦，角尾幸保（日本電気株式会社）] SCIS2005
欧州における携帯電話の規格 GSM（Global System for Mobile Communications）において、 A5/1 と呼ばれるストリーム暗号が使われていた。この論文では、clock-control に関する情報をサイドチャネルとして得られると仮定して、A5/1 の内部状態を推定する新たな解析法を提案している。提案解析法は、A5/1 の各時刻において 2 つの線形フィードバックシフトレジスタ(LFSR) が shift したか、あるいは 3 つの LFSR が shift したかが攻撃者の得られるサイドチャネル情報から分かるとき、平均 229:48 の探索によって内部状態を決定できる。

(3) SBOX の特性を利用した DPA 評価手法 [三宅秀享、野崎華恵、清水秀夫、新保　淳（㈱東芝）] SCIS2005
共通鍵暗号に対する DPA（Differential Power Analysis）において秘密鍵を特定する際に、参照値として S-BOX の特性を利用した場合には、一般的に真の鍵と外れ鍵を区別しにくいという特徴がある。この論文では、DES の S-BOX の特性を利用したＤＰＡ評価手法を示している。
この手法は、S-BOX 処理の特性上、外れ鍵においてもある相関値パターンを持つことを利用した解析方法であり、S-BOX 出力信号を用いた DPA での真の鍵の判定精度を向上させるものである。本手法を実機の測定データに適用し、効果が得られた結果についても示して

いる。

(4)　INSTAC-8 を用いたサイドチャネル攻撃に関する一考察 [和田崇臣, 甲斐切皇男, 岩井啓輔, 黒川恭一（防衛大学校）]　情報処理学会第 67 回全国大会
この研究では、INSTAC-8 を用いたサイドチャネル攻撃に関する検証として、サイドチャネル攻撃の中でも暗号デバイスの消費電力を用いて鍵を解読する電力差分解析(DPA)に着目し、簡易な暗号に対する DPA を行っている。
その結果、鍵と消費電力に強い相関関係があることが確認されている。

(5)　CPU ボード上のブロック暗号に対するサイドチャネル攻撃 [高橋芳夫(㈱NTT データ), 福永利徳, 大塚浩昭, 神田雅透（㈱NTT）]　ISEC
暗号装置に対するサイドチャネル攻撃について多くの研究がなされている。この攻撃には実装の詳細が未知でも可能な攻撃があるが、実装の詳細を把握した上で行えば、より強い攻撃となると考えられる。この論文では、ブロック暗号を CPU ボードに実装する場合の典型例について、実装を詳細に調査分析できるという条件の下で、効率的な実装情報の取得方法を検討し、CPU ボードで測定したデータを元に攻撃実験を行った結果を報告している。CPU ボードから事前取得した情報を用いると、2 個の測定データがあれば９０％の確率で、1 個の測定データでも６５％の確率で攻撃に成功している。

(6)　32bitCPU を対象とした電力解析用評価環境の開発と実証実験 [藤崎浩一, 清水秀夫, 新保　淳（㈱東芝）]　ISEC
現在、サイドチャネル攻撃に対する標準的な実験評価環境がないために、提案されている攻撃手法および対策の有効性を統一的に評価することが難しいという問題がある。そこで、(財)日本規格協会情報技術標準化研究センター(INSTAC)耐タンパー性調査研究委員会では、平成 16 年度に 32bit CPU を対象としたサイドチャネル攻撃の標準的プラットフォームの仕様を策定した。この論文では、このプラットフォームの仕様を説明し、仕様に準拠した基板を用いて DES に対する差分電力解析と RSA に対する単純電力解析の実証実験を行った結果を報告している。

(7)　Experimental Results on INSTAC-8 Compliant Board [角尾幸保（JSA/INSTAC/TSRC, 日本電気㈱), 久門　亨（日本電気㈱), 辻原悦子（ (株)ワイ・デー・ケー), 松本　勉（JSA/INSTAC/TSRC, 横浜国立大学), 川村信一, 藤崎浩一（JSA/INSTAC/TSRC, ㈱東芝）] Physical Security Testing Workshop
この論文では、INSTAC-8 準拠評価ボードを使ったサイドチャネル攻撃の実験結果を 3 件報告している。3 件の実験は、それぞれ差分電力解析（DPA)、電磁波解析（EMA)、単純電力解析（SPA）の例である。第 1 の実験は、DES 暗号に DPA を適用した例であり、INSTAC-8 準拠評価ボードが設計通りに動作するかを確認するために、評価ボードの製造者が実施し

ている。第 2 の実験は、鍵加算後 S-box（換字テーブル）を参照する処理 1 つをミニ暗号とみなし、EMA を適用した例であり、TECHNICAL REPORT OF IEICE で高橋らが報告している。第 3 の実験は、A5/1 暗号に SPA を適用した例である。
この論文は 2005 年 9 月に NIST と IPA によりハワイで共同開催された Physical Security Testing Workshop にて報告したものである。
Physical Security Testing Workshop
Web ページ： http://www.nist.gov/public_affairs/confpage/050926htm.htm
論文掲載： http://csrc.nist.gov/cryptval/physec/physecdoc.html

(8) ストリーム暗号に対する DPA [久門 亨、角尾幸保（日本電気㈱)、後藤 敏、池永剛（早稲田大学）] SCIS2006
この論文ではストリーム暗号に対する実装攻撃手法を提案している。攻撃手法は、2005 年 9 月に開催された Physical Security Testing Workshop において、ストリーム暗号 A5/1 に対して電力解析実験を実施した経験から電力解析を採用しているが、今回は、前回の SPA に対してより高い解析力と精度をもつ DPA を採用し、その中でも特に強力な Multi-bit DPA を適用している。
この提案手法の有効性を確認するため、INSTAC-8 準拠評価用標準プラットフォーム上で、32 ビットの XOR 演算に対して解析対象のビット幅を変えて検証を行った結果、ビット幅が 8 ビットまでは差分波形の差分値が増加し、それ以降は 8 ビット単位で同様の波形を繰り返す事を確認している。また、4 ビットの鍵に対する解析実験を行った結果、オシロスコープの解像度 500MSample/sec、測定波形数 3000 波形において、鍵の推定を行う事ができている。さらに、XOR 演算と Multi-bit DPA の採用によって、推定した鍵が完全に一致しなくてもその波形の形状と向きから、どの程度推定した鍵が一致しているかを判断し鍵を絞り込む事ができるため、測定回数の削減が可能となっている。

(9) 共通鍵暗号におけるテーブルを用いた電力差分解析対策法について [宮崎隆行,辻村達徳, 松本 勉（横浜国立大学）] SCIS2006
共通鍵暗号に対する電力差分解析 (Differential Power Analysis、 DPA) においては、暗号アルゴリズムの計算途中の値を参照値として、統計的な処理により秘密鍵を特定する。この論文では、計算の一部をテーブル (入出力の対応表) にすることによる DPA 対策を提案している。この手法は、DPA の参照値となる値を計算で使用しないことにより、参照値に依存した消費電力変化をなくし、統計的な処理を行った際に、消費電力の差分が発生しないようにする手法である。この手法を共通鍵ブロック暗号方式の一つである AES に適用したものを、INSTAC-8 準拠プラットフォーム上で実装し、測定によって得られた結果を示している。

(10) 汎用 CPU におけるサイドチャネル情報からの命令コードの解析 [山口晃由, 山田敬

喜（三菱電機㈱）]　SCIS2006
1998 年に Kocher が電力解析を提案して以来、多くのサイドチャネル解析法が提案されている。しかしながら、これまでの解析法は、暗号アルゴリズムや実装法が既知の場合にのみ適用可能であり、暗号アルゴリズムが未知の場合は適用できないことが多い。暗号装置の中には、実装されている暗号が非公開のものもあり、従来の方法ではこれらの装置の解析を行えない。この論文では、汎用 CPU をターゲットに、実装アルゴリズム非公開の暗号装置に対する解析スキームの検討を行っている。特に、INSTAC-8 準拠評価ボードを用いて、サイドチャネル情報から実行コードの推定を試みている。

(11)　Sbox 特性を利用した DPA 評価手法の有効性検証[三宅秀享，野崎華恵，清水秀夫，新保　淳（㈱東芝）]　SCIS2006
この論文では、全ての鍵候補の相関値に着目して真の鍵を判定する all-key 判定法の有効性について検討し、all-key 判定法の有効性はポートによる偏りがあることを示している。また、大別して 2 種の比較方法を用いて従来法（1-key 判定法）との比較を行い、DPA に用いる消費電力波形のサンプル数が十分でない場合でも従来法より効果的である可能性を示している。

(12)　位相限定相関法に基づく高精度波形解析とそのサイドチャネル攻撃への応用 [今井裕一，本間尚文，長嶋　聖，青木孝文（東北大），佐藤　証（日本アイ・ビー・エム㈱）] ISEC
この論文では、位相限定相関法を用いた高精度な波形位置あわせ手法とそのサイドチャネル攻撃への応用について述べている。一般に SPA や DPA のような電力解析攻撃では、ノイズ成分の低減や秘密情報の抽出のため電力波形データへの統計的な処理を必要とする。しかし、一連の電力波形データには、しばしば測定時の取り込み誤差による位置ずれが含まれる。提案する手法は、離散フーリエ変換した波形より得られる位相成分から、サンプリング分解能を越える精度で信号波形間の位置ずれ量を推定している。波形間の位置ずれを高精度に補正することで電力解析攻撃の効果を高めることができる。この論文では、Z80 プロセッサ上の DES のソフトウェア実装に対する DPA によりその可能性を示している。

(13)　INSTAC-8 準拠評価ボードを使った実装攻撃実験の結果報告 [角尾幸保（JSA，日本電気㈱），久門　亨（日本電気株），辻原悦子（ (株)ワイ・デー・ケー），松本　勉（JSA，横浜国立大学），川村信一，藤崎浩一（JSA，㈱東芝）]　ISEC
この論文では、INSTAC-8 準拠評価ボードを使ったサイドチャネル攻撃の実験結果を 3 件報告している。3 件の実験は、それぞれ差分電力解析（DPA）、電磁波解析（EMA）、単純電力解析（SPA）の例である。第 1 の実験は、DES 暗号に DPA を適用した例であり、INSTAC-8 準拠評価ボードが設計通りに動作するかを確認するために、評価ボードの製造者が実施している。第 2 の実験は、鍵加算後 S-box（換字テーブル）を参照する処理 1 つをミニ暗号

とみなし、EMA を適用した例であり、TECHNICAL REPORT OF IEICE で高橋らが報告している。第 3 の実験は、A5/1 暗号に SPA を適用した例であり、著者らが 2005 年 5 月に行った結果を報告している。本論文は 2005 年 9 月に開催された Physical Security Testing Workshop で報告したものの日本語版である。

(14)　ブロック暗号のマスク対策付 FPGA 実装に対するビット遷移に着目した DPA の適用 [高橋芳夫（㈱NTT データ，横浜国立大学)，松本　勉（横浜国立大学)，佐藤 証（日本アイ・ビー・エム㈱）]　ISEC
電力差分攻撃（DPA)の対策法の一つである Akker と Giraud によるマスク法（以下、AG マスク法）は、中間データを乱数でマスクすることで攻撃を不可に、あるいは攻撃に要するコストを増加できることが知られている。
この対策法は、従来の DPA は中間データのビットの値と電力波形の相関関係を利用する攻撃であるため、ビット値を乱数と XOR して隠蔽することで攻撃を阻止するものである。しかしながら、ビットの値ではなく、ビットの遷移に注目した DPA ならば未対策時と同じコストで AG マスク法を攻撃できる可能性がある．この論文では，AG マスク法に対するビット遷移に着目した DPA の適用可能性を FPGA に実装した DES を例として分析している。そして FPGA に対策付 DES を搭載して攻撃実験を行い、未対策時と同じコストで AG マスク法が攻撃できることを確認している。

(15)　漏洩電磁波による共通鍵暗号処理ハードウェアの動作解析 [菅原　健，本間尚文，青木孝文（東北大学)，佐藤　証（日本アイ・ビー・エム㈱）]　電気関係学会東北支部連合大会
インターネットや携帯電話を利用した電子商取引の発展に伴い、暗号技術はこれまで以上に身近なものとなった。AES (Advanced Encryption Standard)に代表される共通鍵暗号は、電子認証システムやスマートカードなどの通信秘匿性向上のため、現在広く利用されている。しかし、近年、暗号処理ハードウェアのサイドチャネル情報(消費電力、処理時間、電磁波など) を利用して秘密情報を奪うサイドチャネル攻撃の危険性が指摘されている。この論文では、漏洩電磁波を用いて共通鍵暗号処理ハードウェアの秘密情報を推定する電磁波解析について述べている。

(16)　DPA 対策実験による電力解析評価用プラットフォームの検証 [辻　洋平, 岩井啓輔, 黒川恭一（防衛大学校）]　第 5 回情報科学技術フォーラム FIT2006
サイドチャネルアタック用プラットフォームとして SCAPE と INSTAC-32 準拠ボードを用いて DPA を行った際に、期待する成果が得られるかを比較検証している。
どちらのプラットフォームでも、DPA に無対策の AND 回路に関してはその消費電力差を確認している。
また、Messerges の提案したマスク方法の不十分な点から、消費電力差においてパルスを

確認している。

(17) High-resolution side-channel attack using phase-based waveform matching [本間尚文 , 長嶋　聖, 今井 裕一, 青木孝文（東北大学), 佐藤　証（日本アイ・ビー・エム㈱）] CHES 2006
この論文では位相限定相関法に基づく高精度波形マッチング手法を提案し、そのサイドチャネル攻撃への応用を示している。単純電力解析(SPA)や差分電力解析(DPA)などの攻撃は、雑音の減少と、秘密情報の復元のために信号波形の統計分析(例えば、パワートレース)を使用する。 しかしながら、波形データは測定値にしばしば変位誤差を含んでいる。 波形の離散型フーリエ変換におけるフェーズコンポーネントの使用で、信号波形の間のサンプリング解像度より高精度での変位を見積もることが可能となる。この高精度マッチング法を使用することでサイドチャンネル攻撃の精度を高めることができる。この論文では、Z80プロセッサの上での DES のソフトウェア実装において実験的な DPA と差分電磁解析(DEMA)による従来のアプローチとの比較により、位相限定相関に基づく方法の利点を示している。

(18) 位相限定相関法による波形マッチングを用いた高精度差分電力解析法 [今井裕一, 本間尚文, 長嶋　聖, 青木孝文（東北大学), 佐藤　証（日本アイ・ビー・エム㈱）] CSS2006
暗号モジュールの差分電力解析(DPA) では、秘密鍵に応じて変化する微弱な電力を多数の波形サンプルの統計処理によって増幅するため、ある特定のポイントの波形を正確なタイミングで取得することが不可欠である。そこで DPA 対策の一つとして、暗号処理中にランダム遅延やダミーサイクルを挿入して波形をひずませる手法が用いられる。この論文では、そのような対策を施した DES のソフトウェア実装に、サンプリング分解能を越える高精度な波形マッチング手法を適用することで、対策を施していない場合と同様に DPA が可能であることを示している。

(19) RSA 暗号の FPGA 実装に対する SPA 耐性評価 [宮本篤志, 本間尚文, 青木孝文（東北大学), 佐藤　証（日本アイ・ビー・エム㈱）] CSS2006
RSA 暗号の単純電力解析（SPA）は、鍵のビットパターンに応じて繰り返される乗算と自乗算の波形の違いを見分けるものである。そのため、ハードウェア実装においては乗算器の構成が、その攻撃成功の可否に大きく影響すると考えられる。
そこでこの論文では、FPGA を用いて、ハードウェアマクロとして用意されている乗算器と独自に設計した乗算器の 2 種類に対して RSA 暗号を実装し、両者の SPA 耐性評価実験を行っている。

(20) 位相限定相関法に基づく高精度波形マッチング -- 暗号ハードウェアの動作解析への応用 – [長嶋聖, 本間尚文, 今井裕一, 青木孝文（東北大学), 佐藤　証（日本アイ・ビー・エム㈱）] 第 21 回信号処理シンポジウム

この論文では、位相限定相関法に基づく高精度波形マッチング手法を提案し、その暗号ハードウェアの動作解析への応用を示している。波形解析では通常、ノイズ成分の低減や特徴量抽出のため複数の波形を測定して統計的な処理を行う。このとき波形の取得は、単にハードウェアへ外部から供給するクロックに同期するだけでなく、解析対象の内部処理のタイミングに正確に合わせることが重要となる。しかし一般のハードウェアが、内部解析に都合のよいトリガ信号を出力している状況は考えにくい。そこで、波形取得後に内部処理のタイミングを推定して、波形間の位置合わせを行う高精度なマッチング手法を提案している。これは、離散フーリエ変換した波形より得られる位相成分を利用しており、サンプリング分解能を越える精度で信号波形間の位置ずれ量を推定することが可能である。提案手法を暗号ハードウェアの差分電力解析に適用した実験を通して、その有効性を検証している。

(21) テーブルネットワークを用いた FPGA 実装 AES とその電力差分解析耐性 [辻村達徳（横浜国立大学), 高橋芳夫（横浜国立大学, ㈱NTT データ), 松本　勉（横浜国立大学）] ISEC
共通鍵ブロック暗号に対する電力差分解析は、暗号アルゴリズムの計算途中の値を参照値として、統計的な処理により鍵を特定する。この論文では、鍵の導出を困難にするソフトウェア実装方式であるテーブルネットワーク型暗号実装を DPA 対策としてハードウェア実装に適用し、FPGA 実装 AES を用いて行った実験結果から、テーブルネットワーク型暗号実装の電力差分解析耐性を示している。

(22) 位相限定相関法を用いた高精度差分電力解析とそのノイズ耐性評価 [本間尚文 ,長嶋　聖, 今井裕一, 青木孝文 (東北大学), 佐藤　証 (日本アイ・ビー・エム㈱)] SCIS2007
暗号モジュールの差分電力解析(DPA) では、秘密鍵に応じて変化する微弱な電力を多数の波形サンプルの統計処理によって増幅するため、ある特定のポイントの波形を正確なタイミングで取得することが不可欠である。しかし、一連の電力波形データには、しばしば測定時の取り込み誤差や DPA 対策による位置ずれが含まれる。また一方で、取得時のノイズや電源電圧の変動により不規則な変形が含まれる。この論文では、位相限定相関法を用いた波形マッチング手法により、データの位置ずれや変形のある波形に対しても高精度な DPA が可能であることを示している。マイクロプロセッサ上の DES のソフトウェア実装に対する DPA によりその有効性を評価している。

(23) INSTAC-32 準拠ボードを使用した電力解析自動化の適用例 [庄司陽彦, 野澤　晃, 木村隆幸 ((株)ワイ・デー・ケー), 久門　亨 (日本電気㈱), 深澤　宏 (NEC マイクロシステム㈱), 角尾幸保 (日本電気㈱)] SCIS2007
この論文では、サイドチャネル攻撃の一つである「電力解析」について、消費電力の測定を効率化するために、計測器接続の標準インターフェイスである VISA を使用した自動解析

環境を検討している。検討した結果を INSTAC-32 準拠評価ボードに適用した例として示すことにより、第三者評価を効率的に実施できる環境を推進することを目的としている。

(24) RSA 暗号を実装した INSTAC-32 に対するサイドチャネル攻撃実験 [深澤 宏, 東 邦彦（NEC マイクロシステム㈱), 後藤 敏, 池永 剛（早稲田大学), 角尾幸保, 久門 亨（日本電気㈱), 庄司陽彦（ (株)ワイ・デー・ケー）] SCIS2007
この論文では、INSTAC-32 上で行った RSA 暗号に対するサイドチャネル攻撃の実験結果を報告している。INSTAC-32 は、汎用 CPU と FPGA を搭載した耐タンパー性評価実験用の標準プラットフォームである。過去に INSTAC-32 の CPU+FPGA を使った実験は報告されていないため、両者の協調動作を攻撃対象とする実験を行っている。この論文では、暗復号処理に用いるべき乗剰余演算器のみを FPGA に実装し、それを m-ary 法により CPU（ソフトウェア）からくり返し使用するように RSA 暗号を実装している。この実装に対してテンプレート攻撃を実施し、その消費電力波形の観測と秘密鍵の特定を行っている。その結果 2bit の m-ary 法の場合、4 通りの特徴的な消費電力波形（テンプレート）が観測でき、これらを使って秘密鍵を特定できることを確認している。この論文は、INSTAC-32 の CPU＋FPGA 構成で RSA 暗号の電力解析を行った最初の報告である。

(25) eSTREAM 提案暗号への DPA 解析報告 [久門 亨, 角尾幸保 (日本電気㈱), 深澤 宏（NEC マイクロシステム㈱), 庄司陽彦 ((株)ワイ・デー・ケー), 後藤 敏, 池永 剛 (早稲田大学）] SCIS2007
この論文では、eSTREAM プロジェクト提案暗号に対して実施した差分電力解析(DPA) の解析結果を報告している。現在、eSTREAM プロジェクトでは、次世代のストリーム暗号の策定を目的に、SW 実装では 13 種類、HW 実装では 21 種類のアルゴリズムに対する評価が実施されている。しかし、その評価はアルゴリズム解析や実装性が主であり、実装攻撃に対しては提案者自身の評価を除きほとんど行われていない。そこで著者らは、これらの暗号に対して、ストリーム暗号の初期処理に着目した DPA の適用検討を行っている。解析対象は、SW 実装向けに評価が実施されている DRAGON、LEX、Py、DICING としている。解析の結果、DRAGON、LEX、DICING では、初期処理において秘密鍵と初期値の排他的論理和による演算が存在するため秘密鍵を容易に導出可能であり、Py では、秘密鍵の導出は出来ないものの秘密情報の一部が導出可能であることがわかった。また、INSTAC-8 準拠評価ボード上への実装に対する解析実験では、400 個のサイドチャネル情報で DPA に成功している。

(26) 固定値入力を用いた RSA 暗号ハードウェアに対する SPA [本間尚文 , 宮本篤志, 青木孝文（東北大学), 佐藤 証（日本アイ・ビー・エム㈱）] SCIS2007
この論文では、べき乗剰余演算ハードウェアに N－1（N は法）という特定の入力を与え、自乗剰余算と乗剰余算の動作波形を 3 種類に固定して指数のビットパターンを導出する単純電力解析（SPA）を提案している。この手法は、その回路アーキテクチャやアルゴリズ

ムに関する知識を必要とせず、入力データをコントロールするだけであるため非常に強力である。また SPA 対策として挿入されるダミー乗算サイクルの判別も可能とする。2 種類のモンゴメリ乗算アルゴリズムと 2 種類の乗算器による 4 つの RSA 暗号ハードウェアを FPGA 上に実装し、ランダムパターンと N-1 の 2 つの入力に対してそれぞれの電力波形を観測し、提案手法の有効性を検証している。

(27) 信号遅延を考慮した DPA 耐性評価 --- MRSL と DRSL の場合 --- [佐伯 稔（三菱電機㈱）] SCIS2007
近年、論理回路の基本構成要素レベルの DPA 対策方式が研究されており、著者らも RSL と呼ぶ対策方式を提案している。RSL は単一論理ゲートでデータマスク付きの演算を行い、かつ、入力データとは独立に生成されるイネーブル信号を用いて過渡遷移を抑制する点が特徴である。2006 年には RSL の考え方を導入したいくつかの DPA 対策方式が提案された。その中の MRSL は、RSL をベースとしつつ、RSL とは異なる方法で過渡遷移を抑制するものである。また、DRSL は、2 線式回路による相補動作とデータマスクを組合わせた MDPL における遅延差に基づくリーク可能性を回避するために RSL を利用している。これらの対策方式は、入力データパターンに依存して出力遷移タイミングが変動し得る点が、RSL とは本質的に異なる。この論文では、この点に着目して MRSL と DRSL の DPA 耐性を評価している。また、FPGA を用いた実機による DPA 実験も行い、評価結果を検証している。その結果、どちらの対策方式においても入力信号に十分な遅延差が存在するとリークする可能性があることが確認されている。

(28) テーブルネットワーク型 CPU ボード実装 AES の電力差分解析耐性 [鳥越 慎, 辻村達徳（横浜国立大学), 高橋芳夫（横浜国立大学, ㈱NTT データ), 松本 勉（横浜国立大学）] SCIS2007
暗号実装時に対処が必要な脅威として、電力差分解析による攻撃が知られている。電力差分解析は、暗号処理時のデバイスの消費電力を測定し、統計処理を行うことで鍵を特定する攻撃法である。この論文では、鍵の導出を困難にするソフトウェア実装方式であるテーブルネットワーク型暗号実装を、電力差分解析への対策として適用する際のテーブル設計指針について検討しており、CPU ボード実装 AES を用いて行った実験結果から、テーブルネットワーク型暗号実装の電力差分解析耐性を示している。

(29) アンロールパイプライン型 FPGA 実装 AES の電力差分解析耐性 [辻村達徳(横浜国立大学), 高橋芳夫（横浜国立大学, ㈱NTT データ), 松本 勉（横浜国立大学）] SCIS2007
共通鍵ブロック暗号に対する電力差分解析は、暗号アルゴリズムの計算途中の値を参照値として、統計的な処理により鍵を特定する。この論文では、アンロールパイプライン型実装について、FPGA 実装 AES を用いて実験を行い、ループ型とアンロールパイプライン型の実装方式での電力差分解析耐性の比較や、テーブルネットワークを用いた DPA 対策をアン

ロールパイプライン型に適用したときの電力差分解析耐性を示している。

(30) INSTAC-32 準拠プラットフォームを用いた RSA に対する故障利用攻撃実験 [藤崎浩一, 清水秀夫（㈱東芝）] ISEC
実行時に暗号モジュールを誤動作させ、そのときの演算結果から秘密情報を求めるという故障利用攻撃がある．この故障利用攻撃手法の中で、攻撃を成功させるための条件の制約が少ない攻撃手法を A.Lenstra が提案した。この攻撃手法は、中国剰余定理を用いた RSA に対して有効であり、特定の演算時に誤動作を起こすことができれば秘密情報を求めることができるとしている。この攻撃手法の追試を、32bitCPU を搭載した標準的評価用プラットフォームを用いて行い、攻撃に成功することができた。

2.2.3 活動計画

電力解析実験ワーキンググループ(WG)の主要な活動目的は､電力解析攻撃等のサイドチャネル攻撃に対して暗号モジュールを防御する技術を確立すること、また暗号モジュール製品試験の為のセキュリティ要件・試験技術の開発にある。そこで、電力解析を中心とするサイドチャネル攻撃の攻撃方法及び対策方法に関する調査・検討を行い、セキュリティ要件・試験要件を開発するとともに、その国際標準化活動に対して貢献して行くものとする。具体的には INSTAC-8/-32 仕様準拠ボードを利用した実験の計画の策定・実行を行う。2006 年度開催の WG では、実験の実行のために解決すべき課題として次のものが指摘された。

１．実験結果の比較のため、共通化された実験環境や実験方法が必要である。
２．INSTAC-32 仕様準拠ボード間に消費電力等、ハードウェアのばらつきがある。
３．実験データは実験環境やノイズの影響が大きい。
４．企業からは実験に関するノウハウや生データの公開が容易でない。
５.実験結果からセキュリティ要件･試験要件を導き出す方法論がまだ明らかでない。

課題１～３に対応するために実験の環境や方法の共通化は不可欠であるが､課題４のように企業からの情報提供には制約がある。そこで、公的研究機関や大学等、詳細な情報提供に支障の少ない組織が主体となって、実験の共通化に必要な情報を公開していく方針になった。また、課題５の方法論は今後、当 WG で検討していく必要がある。このような状況を踏まえ、次のように 2007 年度の計画を設定した。

・2007 年度上期
実験環境・実験方法の共通化についての検討
１．実験方法の共通化
２．電源のノイズに対する対策
３．実験で得られたデータの解析方法の共通化
・2007 年度下期

上期に共通化した実験方法等の有効性を確認する。

・2007 年度通年

INSTAC-32 仕様準拠ボードの個体差の比較測定も並行して実施する。

第 3 章　開催状況

2006 年度の暗号モジュール委員会は、計 3 回開催された。各回会合の概要は表 1 のとおりである。

表 1　2006 年度暗号モジュール委員会の開催状況

回	開催日時	主な議題
第 1 回	平成 18 年 7 月 26 日 10:00～12:00	暗号モジュール委員会規程について ISO/IEC JTC 1 SC 27/WG 3 のマドリッド会合報告 平成 18 年度暗号モジュール委員会活動計画（案）について ISO/IEC 24759 1st WD のコメント案審議 電力解析実験 WG（仮称）設置について
第 2 回	平成 18 年 12 月 15 日 13:30～15:30	ISO/IEC JTC 1 SC 27/WG 3 の南アフリカ会合報告 ISO/IEC 24759 1st WDのコメント処理案審議について
第 3 回	平成 19 年 3 月 15 日 10:30～12:30	ISO/IEC 24759 1st CDコメント案審議 CRYPTREC Report 2006(案)について 2007 年度のスケジュール(案)について

2006 年度の電力解析実験ワーキンググループは、計 2 回開催された。各回会合の概要は表 2 のとおりである。

表 2　2006 年度電力解析実験ワーキンググループの開催状況

回	開催日時	主な議題
第 1 回	平成 18 年 12 月 27 日 10:00～12:00	電力解析実験ワーキンググループ規程について 暗号モジュール委員会の運営方針 電力解析実験ワーキンググループ設立に至る背景と経緯 電力解析実験ワーキンググループ活動計画(案)
第 2 回	平成 19 年 3 月 2 日 14:00～16:00	2006 年度まとめと報告書の作成について 来年度の活動について 電力解析関係発表論文