CRYPTREC Report 2005

平成 18 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 1
本報告書の利用にあたって 2
委員会構成 4
委員名簿 5
第１章　活動の背景と目的 7
1.1　CRYPTREC 活動の経緯 7
1.2　暗号モジュール委員会の活動目的 8
1.3　暗号モジュールセキュリティ要件に関する国際動向 8
1.3.1　FIPS 140-2 8
1.3.2　ISO/IEC 19790 9
1.4　暗号モジュール委員会の活動概況 9
第２章　委員会の開催状況 13
第３章　活動内容と成果概要 14
3.1　暗号モジュールセキュリティ要件等の策定 14
3.1.1　北米における暗号モジュールセキュリティ要件等の概要 14
3.1.2　国際標準規格への対応検討 15
3.1.2.1　国際標準規格の動向 15
3.1.2.2　国際標準規格への対応 18
3.1.3　暗号モジュールセキュリティ要件の作成 19
3.1.4　暗号モジュール試験要件の作成 19
3.1.5　運用ガイダンスの検討 21
3.2　非破壊攻撃及び破壊攻撃に対する調査・研究 23
3.2.1　SCIS 2006 での発表 23
3.2.2　CHES 2005 での発表 26
参考文献 28

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 2005 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 JTC1/SC27/WG3 においては、暗号モジュールセキュリティ要件の国際標準規格化がほぼ完了し、暗号モジュール試験要件の標準規格化作業も開始されようとしている。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 JTC1/SC27/WG3 において、ほぼ標準規格化が完了した 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。また、本報告書の別冊として、暗号モジュールセキュリティ要件、暗号モジュール試験要件、及び運用ガイダンスをまとめた。

運用ガイダンスについては、下記 URL の「CRYPTREC Report 2005 の公開」で参照できる。

http://www.cryptrec.jp/report.html
http://www.ipa.go.jp/security/enc/CRYPTREC/index.html
http://cryptrec.nict.go.jp/cryptrec_info_publicity.html

別冊の暗号モジュールセキュリティ要件は、下記(1)から導出された国際規格である下記(2)を翻訳したものである。

別冊の暗号モジュール試験要件は、昨年度作成した暗号モジュール試験基準第 0.1 版(下記(3)を翻訳したもの)に対し、下記(2)のセキュリティ要件へ対応するために見直しを行ったものである。

別冊の運用ガイダンスは、米国 NIST が発行する下記(4)の Implementation Guidance を翻訳したものである。

(1) FIPS PUB 140-2, SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES, CHANGE NOTICE (12-03-2002)

(2) ISO/IEC FDIS 19790 Information Technology Security Techniques - Security requirements for cryptographic modules (2005-10-31)

(3) Derived Test Requirements for FIPS PUB 140-2, Security Requirement for

Cryptographic Modules (March 24, 2004 Draft)

(4)Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program (Initial Release: March 28, 2003; Last Update: December 01, 2005)

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 等の国際標準規格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、暗号モジュールセキュリティ要件及び試験要件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。

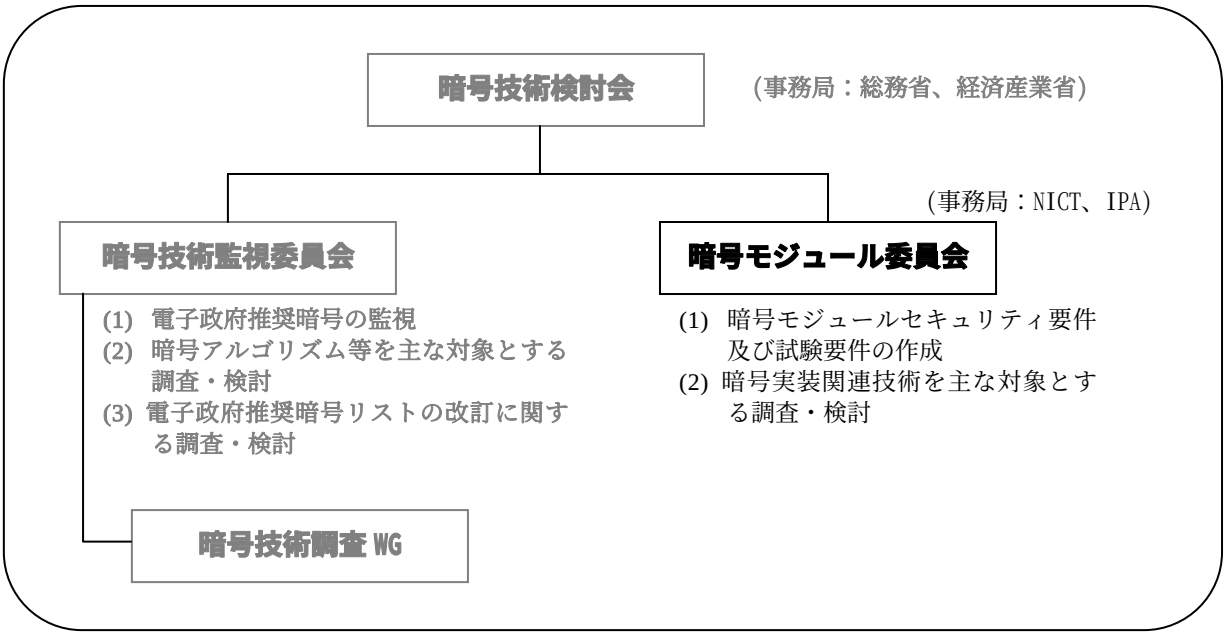

図１　2005 年度の CRYPTREC の体制

委員名簿

暗号モジュール委員会　(2006 年 1 月現在)

委員長	松本　勉	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
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	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	東芝ソリューション株式会社　SI 技術担当
委員	鳥居　直哉	株式会社富士通研究所　部長
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
委員	米倉　昭利	財団法人日本情報処理開発協会　センター長 (2005 年 9 月まで)

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
山城　瑞樹	防衛庁　長官官房
加納　信生	防衛庁　陸上幕僚監部
石川　正興	防衛庁　技術研究本部
武田　仁己	防衛庁　技術研究本部
山本　寛繁	総務省　行政管理局

野崎　雅稔　　総務省　情報通信政策局(2005 年 8 月まで)
榎本　淳一　　総務省　情報通信政策局(2005 年 8 月まで)
黒田　崇　　総務省　情報通信政策局(2005 年 7 月まで)
増子　喬紀　　総務省　情報通信政策局
網野　尚子　　総務省　情報通信政策局
石川　雅一　　外務省　大臣官房(2005 年 7 月まで)
山元　明裕　　外務省　大臣官房
勝亦　眞人　　経済産業省　産業技術環境局
小谷　光弘　　経済産業省　産業技術環境局
柳原　聡子　　経済産業省　商務情報政策局(2005 年 7 月まで)
松井　洋二　　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
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

事務局

独立行政法人 情報処理推進機構
三角育生、西原正人、上野天徳、大熊建司、大塚玲、小柳津育郎、杉田誠、
山岸篤弘、大久保美也子

独立行政法人 情報通信研究機構
山村明弘、田中秀磨、外川政夫、黒川貴司、吉野智明、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行政手続きを電子化する電子政府システムの構築が精力的に進められている。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)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 暗号モジュール委員会の活動目的

2003 年 2 月に、電子政府推奨暗号リストが発表され、どの暗号アルゴリズムが安全であるかの判断が公開された。しかし、実際に暗号を組み込んだ製品の安全性は、利用されている暗号アルゴリズムだけでなく、暗号アルゴリズムを組み込んだ暗号モジュールにおける実装方法にも依存する。

CRYPTREC では 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)暗号モジュールセキュリティ要件及び試験要件の策定

(2)暗号モジュールへの非破壊攻撃及び破壊攻撃に対する調査・研究

(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セキュリティ要件及び試験要件の策定作業を行う。(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。

1.3 暗号モジュールセキュリティ要件に関する国際動向

暗号モジュールに関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次の 2 つがある。

(1)FIPS[1] 140-2 (米国 NIST[2])

(2)ISO[3]/IEC[4] 19790

1.3.1 FIPS 140-2

FIPS 140-2 は、米国/カナダが共同運用している CMVP[5]制度で利用されている暗号モジュールセキュリティ要件に関する標準規格であり、米国 NIST によって発行されている。この標準規格の関連文書に試験要件(DTR)[6]と運用ガイダンス(IG)[7]の 2 種類があり、NIST は必要に応じて適宜改訂している。DTR は暗号モジュールを試験する際の基準であり、IG は運用に関する説明を記述している。

NIST/CSE[8]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

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

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的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。

1.3.2 ISO/IEC 19790

ISO/IEC 19790 は FIPS 140-2 を元に作られた国際標準規格である。ISO/IEC JTC1[9] SC27/WG3 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[10]投票で可決され、2006 年 3 月 1 日付けで発行された。

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。次回の 2006 年 5 月の Madrid 会合で審議すべく WD[11]向け文書の準備中である。

1.4 暗号モジュール委員会の活動概況

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 等の国際標準規格の動向を注視しつつ、北米の評価基準及び試験基準の翻訳作業を行い、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[12]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

審議中の国際標準規格(ISO/IEC 19790)が、ベースとなる FIPS 140-2 と内容的に大きく異なってくる可能性が出てきた。そこで、前年度の基準第 0 版の改訂に国際標準規格

9 Joint Technical Committee 1
10 Final Draft International Standard
11 Working Draft
12 Field Programmable Gate Array

への対応も追加して、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 と国際標準規格(1st CD 19790)との差分表を作成し、作成した差分表を翻訳する。

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 JTC1/SC27/WG3 への技術コメント作成協力

国際標準規格(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 年度に仕様策定を行った評価用標準プラットフォームを実装した評価用ボードを入手し、希望する委員に配布するとともに、よりハイエンドな評価用標準プラットフォームの策定を行った。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。

具体的な作業は、次の a)～c)。

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[13]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開発し、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ている。

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

---

[13] 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

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)暗号モジュール評価基準(暗号モジュールセキュリティ要件)及び試験基準(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 JTC1/SC27/WG3への技術コメント作成協力

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

b)運用ガイダンスの改訂

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

c) 暗号モジュールセキュリティ要件及び暗号モジュール試験要件の策定

2004年度作成した暗号モジュール評価基準第0.1版及び試験基準第0.1版を基に、FDIS 19790に対応するための検討を行い、暗号モジュールセキュリティ要件及び暗号モジュール試験要件を策定した。

(2)暗号モジュールへの非破壊攻撃及び破壊攻撃に対する調査・研究

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

2005 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 3 つが挙げられる。

(1) 暗号モジュールセキュリティ要件

ISO/IEC 19790 の投票文案である、ISO/IEC FDIS 19790 (2005-10-31)を日本語化した。尚、この ISO/IEC FDIS 19790 は、若干の編集上の修正を加えて、2006 年 3 月に国際規格化された。

(2) 暗号モジュール試験要件

FIPS 140-2 の DTR を日本語化した、昨年度の成果である「試験基準第 0.1 版」を基に ISO/IEC FDIS 19790 と FIPS 140-2 との差分を考慮し、暗号モジュール委員会独自の案を策定した。

(3) 運用ガイダンス

NIST 発行の“ Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program(Initial Release: March 28, 2003 Last Update: December 01, 2005) ”を日本語化した。

第 2 章　委員会の開催状況

2005 年度の暗号モジュール委員会は、計 5 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　2005 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 17 年 6 月 2 日 15:00～17:00	委員長互選 ISO/IEC JTC1 SC27/WG3 のウィーン会合報告 平成 17 年度暗号モジュール委員会活動計画（案）について 評価用標準プラットフォームによる実験データの収集について 運用ガイダンス第 0.1 版のレビュー
第 2 回	平成 17 年 10 月 14 日 15:00～17:00	NIST Physical Security Testing Workshop 報告 FDIS 19790 第 7 章日本語訳について
第 3 回	平成 17 年 12 月 16 日 13:00～15:00	FDIS 19790 の投票について 運用ガイダンス 2005-11-07 版について 暗号モジュール試験基準 2005-12-05 版について
第 4 回	平成 18 年 1 月 27 日 14:00～16:00	運用ガイダンス日本語訳について 暗号モジュール試験基準 2005-12-22 版について 「評価」及び「試験」の用語の使用方法について
第 5 回	平成 18 年 2 月 23 日 10：30～12：30	「暗号モジュールセキュリティ要件」2006-02-14 版について CRYPTREC REPORT 2005「暗号モジュール委員会報告」(案)について

第 3 章　活動内容と成果概要

3.1　暗号モジュールセキュリティ要件等の策定

3.1.1　北米における暗号モジュールセキュリティ要件等の概要

(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 が発行する米国政府標準である。

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 2006 年 1 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 も FIP 140-2 と同様に適宜改訂されており、2004 年 3 月の改訂ドラフト版が 2006 年 1 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(すなわち、設定されたセキュリティレベルで、設定された分野のセキュリティ要求事項を暗号モジュールが満足するために適用しなければならない宣言)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、試験者が実施しなければならない試験手順を記述している。

(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、2005 年 12 月の改訂版が 2006 年 1 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)から構成されている。

“SECTION 1 から SECTION 14”は、FIPS 140-2 の 4.1 節から 4.11 節(SECTION 1 から SECTION 11 に対応)、APPENDIX A(SECTION 12 に対応)、 APPENDIX B(SECTION 13 に対応)、APPENDIX C(SECTION 14 に対応)にそれぞれ対応しており、FIPS 140-2 で規定されるセキュリティ要求事項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。

“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。

3.1.2 国際標準規格への対応検討

3.1.2.1 国際標準規格の動向

FIPS 140-2 を元にした IS 化が、ISO/IEC JTC1/SC27/WG3 で検討されている。暗号モジュール評価に関する国際的な動向としては、(1)米国/カナダが共同運用している CMVP、(2)ISO/IEC JTC1/SC27/WG3 で審議中の暗号モジュールセキュリティ要件の国際標準規格化、の 2 つが重要である。

(1)CMVP 動向

2005 年 9 月 26 日～9 月 29 日に、米国ハワイのホノルルで「Physical Security Testing Workshop presented by the CMVP and IPA/INSTAC」が開催された。参加者は、59 名で、内訳は次の通りであった。

米国(33)、カナダ(6)、英国(5)、フランス(2)、オランダ(1)、オーストラリア(1)
日本(9)、ドイツ(2)

この会議は、NIST/CSE と IPA 及び INSTAC が共催し CMVP 関係者向けに開いたサイドチャネル攻撃を含む物理的セキュリティ試験ワークショップであり、物理的セキュリティ関連技術のアップデートが目的であった。9 月 26 日、27 日の 2 日間にわたり、物理的セ

キュリティに関する19本の発表があり、9月28日、29日は、主にパネルディスカッションが行われた。発表内容については、NISTのWebサイトに掲載されている。

http://csrc.nist.gov/cryptval/physec/physecdoc.html

＜CMVPについて＞

この会議において、北米で行われている暗号モジュール試験及び認証制度であるCMVPについて、次のような説明及び今後の予定が発表された。

- FISMA(Federal Information Security Management Act)の猶予期間が終了したことにより、政府機関は、暗号モジュールを使用する際には、強制的にFIPS 140-2で認証された暗号モジュールを使用しなければならなくなった。
- FIPS 140-2はISO/IEC 19790の基となっている。
- FIPS 140-3の改訂作業開始。
- 2005年は140件の認証を行う予定。
- FIPS 186-3:Digital Signature Standard (DSS)が、近日中に発行される予定。
- CAVS(暗号アルゴリズム認証システム)で、SP 800-56：Key Establishment及びTLS1.0/IEEE 802.11iのプロトコル認証もサポートする予定。
- 2005年9月現在10の試験機関が存在するが、2005年中に2カ所増える予定。
- DES（FIPS 46-3)の失効により、2年間をかけて、レガシーシステムでもAES/TDESに移行させる予定であり、予算処置がはかられることとなっている。

＜FIPS 140-3について＞

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。

- 2つのセキュリティレベルの増設を行い、6つのセキュリティレベルとなる。現行のセキュリティレベル3以上が再編される。【この会議後の情報によると、セキュリティレベル1から5の5段階に分けられることになったようである。】
- FIPS 140-2の骨格に変更は無いが、全セクションに大幅な変更を加える。FIPS 140-1からFIPS 140-2への変更よりも、大きな変更となる。
- 電力解析に関する基準が明示される。
- Software Security Sectionが設けられSub-Chipという新しい考え方を導入する。
- CCとの関係を明確にする（Detached from CC [CCから分離] ）。
- パワーアップ自己テストを含む、自己テストの章は、Pre-operational Testへ移行する。
- FIPS 140-3での表現はISO/IEC 19790を継承する予定で、CSP・PSPの概念を取り入れる。これは、IS/IEC 19790, 2nd Editionを意識している（USとして、CC言語での再記述の意思が無いことを意味している)。また、FCC要求事項を、FIPS 140-3から取り下げる予定である。

・ 鍵のライフサイクル管理、暗号モジュールのライフサイクル管理も取り入れる。

＜FIPS 140-3 の物理的セキュリティについて＞

この会議において、FIPS 140-2 の後継規格である FIPS 140-3 の物理的セキュリティについて、次のようなアナウンスがあった。

・ 物理的セキュリティに関する要求は、Non-Invasive/Invasive(非侵襲的/侵襲的)に分割して記述される。
・ 物理形態は、次の 4 つ。
  - Sub-Chip
  - Single-Chip
  - Multi-Chip Embedded
  - Multi-Chip Standalone
・ VHDL の Source-code レベルでの試験が義務づけられる。
・ セキュリティメカニズムについても詳細に文書化することが求められる。例えば、Removable covers and door に換気孔（Ventilating hole）等の開口部がある場合には、各ディバイスが observation から保護されている必要がある。
・ 場合によっては、セキュリティレベル 7 を設定し、CC で行なわれている様な Penetration Testing/Vulnerability Analysis の実施も考えられている。

＜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発表された。

・ 2005 年 9 月　　Draft#0 を試験機関に対して配布。
・ 2005 年 11 月　　Draft#1 を開示。3 ヶ月間のコメント募集期間を設ける。
・ 2006 年 2 月　　Draft#1 に対するコメント募集の〆切。
・ 2006 年 3 月　　DoC(米国商務省)による承認作業を開始予定。
・ 2006 年 9 月　　DoC(米国商務省)による承認。
・ 2006 年 3 月　　FIPS 140-3 発効予定。
・ 2007 年 9 月　　FIPS 140-2 廃止予定。

しかしながら、2006 年 2 月現在、Draft#0 を試験機関に対して配布すること以外の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。

・ 2006 年 5 月　　Draft#1 を開示。3 ヶ月間のコメント募集期間を設ける。
・ 2006 年 8 月　　Draft#1 に対するコメント募集の〆切。
・ 2006 年 9 月　　DoC(米国商務省)による承認作業を開始予定。
・ 2006 年 12 月　　DoC(米国商務省)による承認。
・ 2007 年 6 月　　FIPS 140-3 発効予定。
・ 2007 年 12 月　　FIPS 140-2 廃止予定。

(2)ISO/IEC JTC 1/SC 27/WG 3 動向

ISO/IEC JTC1 は、ISO と IEC が共同で運営する IT 技術標準化のための組織で、SC27 委員会で情報セキュリティを、その下の WG3 で情報セキュリティの試験基準を担当している。ISO/IEC JTC 1/SC 27/WG 3 は、2002 年 10 月から暗号モジュールセキュリティ要件の国際標準規格化 11(規格予定番号 19790)を審議している。2005 年の国際会合は、4 月(オーストリア、ウィーン)と 10 月(マレーシア、クアラルンプール)の 2 回開催された。この間に暗号モジュールセキュリティ要件の国際標準規格化フェーズは、FCD から FDIS へと進捗し、2005 年 12 月には IS 化するための投票が実施され、2006 年 3 月に IS 化された。

2004 年度活動と同様、2005 年 4 月及び 10 月の会合には、暗号モジュール委員会での修正コメントをベースに ISO/IEC JTC 1/SC 27/WG 3 国内委員会でのコメント審議を行い、日本 NB としての修正コメントを提出した。日本 NB としては、11 件のコメントを提出し、全て受理された。

暗号モジュールセキュリティ要件の国際標準規格（ISO/IEC 19790）は、FIPS 140-2 をベースとした標準であるが、CC(Common Criteria)への連接性を意識しているため、詳細なセキュリティ要件は異なる部分が存在する。

また、2005 年 4 月の会合では、暗号モジュールセキュリティ要件の国際標準規格化に付随した実際の試験に必要となる、暗号モジュール試験要件の標準化に関する study period の終結が宣言され、10 月の会合で、標準化作業が 2006 年 5 月の会合から開始されることが決まった。

3.1.2.2 国際標準規格への対応

今年度、暗号モジュール委員会では、3.1.2.1 節で述べたような暗号モジュール試験の標準化に関する国際動向に対応すべく、その準備として、以下の(1),(2)の作業を行った。

(1)暗号モジュールセキュリティ要件の作成

2005 年 10 月会合で確認された国際標準規格（ISO/IEC FDIS 19790）に基づき、翻訳版を作成した。この FDIS 19790 の翻訳版は、CRYPTREC Report 2005 の別冊として公開される。詳しくは、3.1.3 節に述べる。

(2)FDIS 19790 に対応した暗号モジュール試験要件の検討

2005 年 10 月会合で確認された国際標準規格（FDIS 19790）に対応する暗号モジュール試験要件の検討を行った。詳しくは、3.1.4 節に述べる。

3.1.3 暗号モジュールセキュリティ要件の作成

昨年度の暗号モジュール委員会では、“FIPS PUB 140-2, SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES, CHANGE NOTICE(12-03-2002)”を翻訳したものを暗号モジュール評価基準第0.1版として発行した。

ISO/IEC JTC1/SC27/WG3で、FIPS PUB 140-2をISO/IEC 19790としてIS化する議論がなされた。

そこで、今年度の暗号モジュール委員会では、IS 化するための投票文案であるISO/IEC FDIS 19790を翻訳し、「暗号モジュールセキュリティ要件」を策定した。

「暗号モジュールセキュリティ要件」については、出版権、翻訳権等の関係上、当面非公開とする。

3.1.4 暗号モジュール試験要件の作成

昨年度の暗号モジュール委員会では、“Derived Test Requirements for FIPS PUB 140-2, Security Requirement for Cryptographic Modules (March 24, 2004 Draft)”を翻訳したものを暗号モジュール試験基準第0.1版として発行した。

今年度の暗号モジュール委員会では、暗号モジュール試験基準第0.1版を基に、ISO/IEC FDIS 19790 を考慮して新たに試験要件の追加及び変更を行い、「暗号モジュール試験要件」を策定した。

「暗号モジュール試験要件」についても、出版権、翻訳権等の関係上、当面非公開とする。

また、「暗号モジュール試験要件」で使われる用語について、CC 用語との比較を行った。次の表2及び表3を参照いただきたい。

表 2： CC 及び「暗号モジュール試験要件」で使われる用語

用語	解説
実証する (Demonstrate)	この用語は、結論に導く分析を意味する。ただし、数学的な意味での形式的な分析ほどの厳格さは求めない。
記述する (Describe)	この用語は、エンティティのある種の特定の詳細が提供されることを要求する。
決定する (Determine)	この用語は、特定の結論に到達することを目的として、独立の分析が行われることを要求する。この用語の利用は「確認する」または「検証する」と異なる。なぜなら、これらの他の用語は、レビューする必要がある分析がすでに行われていることを暗示するが、「決定する」の用語の使用は、通常、これまでに分析が行われていないときの真に独立した分析を暗示するからである。
保証する (Ensure)	この用語は、それだけで使用される場合、アクションとその結果の間の強い因果関係を暗示する。
説明する (Explain)	この用語は、「記述する」及び「実証する」の両方とは異なる。これは、行われたアクションの道筋が必ずしも最適であったかどうかを実際に論証せずに、「何故」 (Why?) の質問に答えることを意図している。
特定する (Specify)	この用語は、「記述する」と同じ文脈で使用されるが、さらに厳格で正確であることを意図している。「定義する」(define)とほぼ同様である。
検証する (Verify)	この用語は、文脈において「確認する」と同様であるが、さらに厳格な意味合いを持つ。試験者のアクションの文脈でこの用語が使用されるときは、試験者に独立の労力を要求することを示す。

※これらの用語は、CC パート 3 の用語（7.4 節）に掲載されており、暗号モジュール試験要件でも使用されている。

表 3： 「暗号モジュール試験要件」で使用される用語

用語	解説
承認された (Approved)	この用語は、制度によって、暗号モジュールに適用可能であると判断され、公示された標準、動作モード、セキュリティ機能などであることを表す形容詞として用いられる。
認証する (Authenticate)	この用語は、オペレータがシステム又はアプリケーションを利用する権利があることを主張した場合に、その確認を行うことを意味する。 「認証する（Validate)」とは異なる意味を持つことに注意が必要である。
評価する (Evaluate)	この用語は、ISO/IEC 15408 の要求事項を満たしていることを「IT セキュリティ評価及び認証制度」のもとで確認することを意味する。 「暗号モジュール試験及び認証制度」において ISO/IEC 19790 の要求事項を満たしていることの確認には、「評価する」は使用せず、「試験する」を使用することに注意が必要である。
試験する (Test)	この用語は、以下のいずれかを意味する。 ① ISO/IEC 19790 の要求事項を満たしていることを「暗号モジュール試験及び認証制度」のもとで確認すること。 ② ①を確認するために用いる、暗号モジュールの性質と能力を個々の手法によって試すこと。
認証する (Validate)	この用語は、「暗号モジュール試験及び認証制度」のもとで、試験機関によって提出された試験結果を、認証機関が一定の方法で検証し、適正であると判断することを意味する。 「認証する（Authenticate)」とは異なる意味を持つことに注意が必要である。

※これらの用語は、暗号モジュール試験要件で使用されているが、CC パート 3 の用語には掲載されていない。

3.1.5 運用ガイダンスの検討

(1) 運用ガイダンスの作成

まず、事務局にて米国 NIST が発行した“Implementation Guidance”の 2005 年 9 月改訂版の翻訳案を作成し、翻訳案に対して委員会内での審議を行い、英文解釈の統一化を図った。

次に、“Implementation Guidance”が 2005 年 12 月に改訂されたため、その差分について、事務局にて翻訳案を作成し、同様に委員会内での審議を行い、英文解釈の統一化を図った。

そして、委員会内での英文解釈を統一化した“Implementation Guidance”の 2005 年 12 月改訂版の翻訳を「運用ガイダンス」としてまとめた。

(2) 運用ガイダンスの構成

「運用ガイダンス」は、“Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program, Initial Release: March 28, 2003; Last Update: December 01, 2005”を翻訳したものであり、構成は、3.1.1 節(3)で述べた“Implementation Guidance”と同様である。

本文は全 17 節から構成されており、「概要」、「全般的な問題」、「第 1 章　暗号モジュールの仕様」、「第 2 章　暗号モジュールのポート及びインタフェース」、「第 3 章　役割、サービス、及び認証」、「第 4 章　有限状態モデル」、「第 5 章　物理的セキュリティ」、「第 6 章　動作環境」、「第 7 章　暗号鍵管理」、「第 8 章　電磁妨害/電磁両立性(EMI/EMC)」、「第 9 章　自己テスト」、「第 10 章　設計保証」、「第 11 章　その他の攻撃への対処」、「第 12 章　Appendix A: 文書要求事項のまとめ」、「第 13 章　Appendix B: 推奨ソフトウェア開発手順」、「第 14 章　Appendix C: 暗号モジュールのセキュリティポリシ」、「取消された運用ガイダンス」が記述されている。

各節の冒頭には、NIST 及び CSE からの解答内容に関し、適用されるセキュリティレベル、有効期間、最終改訂日、DTR の関連するアサーションの番号(AS 番号)、DTR の関連する試験者に課せられる要求事項の番号(TE 番号)、DTR の関連するベンダに課せられる要求事項の番号(VE 番号)が記述されている。その後に、背景(節によっては記述されない)、NIST 及び CSE への質問内容、NIST 及び CSE からの解答、NIST 及び CSE からの追加コメントが順に記述されている。

「運用ガイダンス」については、下記 URL の「CRYPTREC Report 2005 の公開」から参照できる。

http://www.cryptrec.jp/report.html
http://www.ipa.go.jp/security/enc/CRYPTREC/index.html
http://cryptrec.nict.go.jp/cryptrec_info_publicity.html

3.2 非破壊攻撃及び破壊攻撃に対する調査・研究

3.2.1 SCIS 2006 での発表

SCIS(Symposium on Cryptography and Information Security)は、1984 年以来毎年開催され、暗号と情報セキュリティ技術に関する最新の研究成果を発表する場と情報交換の場を提供している。

2006 年 1 月に開催された SCIS 2006 では、サイドチャネル攻撃関係の講演は、3 セッションで全 12 件の発表があった。

そのうち、INSTAC-8 に準拠したボードを用いたサイドチャネル攻撃の実験報告は、以下の 4 件であった。

(1) INSTAC-8 に準拠したボードを用いた電力解析

(a) 1C3-1 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,辻村,松本（横浜国立大学)］

AES の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。本手法は、DPA の参照値となる値を計算で使用しないため、参照値に依存した消費電力変化がなくなるため、観測結果を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と主張している。500 回の計測データを統計処理した結果では、未対策版で現れたピーク（鍵情報の漏洩）は、見られなくなっている。

(b) 1C3-2 ストリーム暗号に対する DPA［久門,角尾（日本電気株式会社）,後藤,池永（早稲田大学)］

ストリーム暗号の Key Setup モードにおいて使用される秘密鍵 K と初期値 IV との XOR 演算を対象として、Multi-bit DPA を用いた解析結果が報告された。攻撃対象とした暗号アルゴリズムは、携帯電話システムである GSM（Global System for Mobile Communications）で採用されていた A5/1 である。INSTAC-8 に準拠したボード上に FW 実装している。Multi-bit DPA を用いることで、高い解析力と精度が実現でき、測定波形数 3000 波形において、正しい鍵の推定を行う事ができた。Multi-bit DPA を用いることで、測定時間の短縮という効果が得られるとしている。また、提案する攻撃手法は、多くのストリーム暗号に採用されている鍵セットアップ演算を対象とするため、様々なストリーム暗号に対して汎用的な解析であると主張している。

(c) 1C3-4 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,山田（三菱電機株式会社)］

暗号モジュールの鍵を推定するのではなく、電力解析の手法を用いて、暗号モジュールでの実行コードを解析する手法の提案である。INSTAC-8 に準拠したボードを用いた実

験では、実際の実行コードの解析にいたっていないが、実行コードの解析を行うことで、使用されている暗号アルゴリズムが未知の場合や非公開の暗号アルゴリズムが用いられている場合でも、実行コードの推定が可能となり、結果的に暗号アルゴリズムの同定が可能となることを示唆している。

現在、実行コードを解析するためには、IC を解体し、内蔵されている ROM を解析する必要があるが、電力解析、電磁波解析では、非侵襲で実行コードの解析が可能になる可能性があるため、今後の動向を注目する必要がある。また、この手法による実行コードの解析に対して、これまで提案されてきた難読化技法の有効性も確認する必要がある。

(d)2C1-2　Sbox 特性を利用した DPA 評価手法の有効性検証[三宅,野崎,清水,新保 淳((株) 東芝)]

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、Sbox 特性を利用した DPA 評価手法(all-key 判定法) を提案しその有効性を実験的に確認している。all-key 判定法では、全 bit の相関性を利用するため、少ない測定回数で、鍵の推定に成功する可能性があることを示した。

(2)　電磁界を用いたサイドチャネル攻撃

電磁界を用いたサイドチャネル攻撃に関しては、講演者が独自に開発した FPGA 基板を用いた実験の報告がなされた。

・1C3-5　FPGA 上での電磁波/電界情報に基くサイドチャネル解析の試行 [佐伯,鈴木,佐藤 (三菱電機株式会社)]

消費電力の変化に着目したサイドチャネル解析ではなく、暗号処理を行うことで発生する放射電磁界の変化を解析する、電磁波解析の報告。講演者らが提案している差分電力解析(DPA) 対策である RSL(Random Switching Logic) 及び他の既存の DPA 対策方式を比較評価している。

放射電磁界の変化は、消費電力の変化に対応したものであり、原理的に電力解析と同等の解析結果が得られると主張している。ただし、測定対象とした FPGA は金属パッケージであり、しかもプローブの空間分解能が大きいもで、FPGA の電源供給ラインでの消費電力を測定している可能性が高いことが指摘されていた。この指摘が正しいければ、本報告は、通常の電力解析を電磁界で観測したことになる。

(3)　その他の講演

(ア) 安全性評価

電力解析を用いた実装方式の安全性評価に関しては、次の 3 件の報告があった。

(a)1C3-3　2 線式回路による DPA 対策方式の安全性評価

鈴木, 佐伯 (三菱電機株式会社)

CHES 2005 で Mangard らによって提案された MDPL という 2 線式回路による DPA 対策

の安全性評価の報告。

(b)2C2-1　A power disturbance circuit for A5/1 resistant to power analysis attack

W.Dai,久門, 後藤,池永(早稲田大学),Z.Liu (Kitakyushu Foundation for the Advancement of Industry Science and Technology) ,角尾 (日本電気)

ディジタル携帯電話システムであるGSMで使用されていたA5/1に対する電力解析攻撃シミュレーションの報告。

（c）2C1-3　鍵付きハッシュ関数に対するサイドチャネル攻撃

桶屋（(株）日立製作所）

鍵付きハッシュ関数 HMAC に関する電力解析の報告。ブロック暗号を用いた HMAC の構成法の一つである PVG 構成法を用いると鍵が露呈する場合があるという報告。

（イ）楕円曲線暗号に対する電力解析

楕円曲線暗号に対する電力解析に関する報告としては、次の 2 件があった。

（a）2C1-1　Side Channel Attack on Improved XTR Single Exponentiation and a New Countermeasure

D.G. Han,高木　（函館みらい大)T.H. Kim (Korea University),H.W. Kim, K.I.Chung(ETRI)

楕円曲線暗号の効率的な実装方式である XTR-ISE に対する電力解析の報告とその対策が提案された。

（b）2C1-4　ランダム化射影座標を用いた楕円曲線暗号実装に対する電力解析

酒井（三菱電機株式会社）

電力解析対策として、ランダム化過程を利用した楕円曲線暗号の実装では使用曲線と計算アルゴリズムにより、計算途中でランダム化の影響を受けない中間データが発生することを、素体 Fp 上の NIST 推奨楕円曲線でも存在することを報告している。

（ウ）キャッシュ攻撃関係

キャッシュ攻撃に関する報告としては、次の 2 件があった。

(a) 2C2-2　サイドチャネル防御機構付き分割キャッシュアーキテクチャに関する一考察

［太田,川幡,角尾（日本電気株式会社）,辻原（株式会社ワイ・デー・ケー）,久保,洲崎（北陸日本電気ソフトウェア株式会社)］

サイドチャネル攻撃の一つであるキャッシュ攻撃に対する対策案提案。MPU アーキテクチャとキャッシュ割り当てを工夫している。

(b) 3E3-2 キャッシュ攻撃による SEED のラウンド鍵の導出

[池田,市川,金子（東京理科大）]

SEED にキャッシュ攻撃を適用し、ラウンド鍵全てを求める手法を提案している。

（エ）TEMPEST 関係

2C2-3　PC から放出する電磁気的雑音と含有するモニター表示画像の再現

［関口,田中,瀬戸,山村（情報通信研究機構）］

端末とそのモニターをつなぐ RGB ケーブルから漏洩する電磁波を利用し、モニター表示情報を解析できることが報告された。また、この漏洩電磁波を用いたモニター表示情報の解析手順を提案している。

3.2.2 CHES 2005 での発表

CHES(Workshop on Cryptographic Hardware and Embedded Systems)とは、組込みシステムにおける暗号のハードウェア実装及びセキュリティに焦点を当てたワークショップである。2005 年 8 月に英エジンバラで開催された CHES 2005 では、サイドチャネル攻撃関係は、3 セッション 8 件の講演がなされた。

その内、電磁界(EM)攻撃に関して、1 セッション 3 件の講演があったことは注目される。

また、ハードウェアベースのサイドチャネル攻撃とその対策技術として、3 セッション 7 件の講演があった。

CHES 2005 の予稿集入手が遅れているため、詳細な情報を入手できていない。そのため、関係する講演の題目だけを紹介する。

（1）Side Channel I

- Resistance of Randomized Projective Coordinates Against Power Analysis
- Templates as Master Keys
- A Stochastic Model for Differential Side Channel Cryptanalysis

（2）Side Channel II(EM)

- EM Analysis of Rijndael and ECC on a Wireless Java-based PDA
- Security Limits for Compromising Emanations
- Security Evaluation Against Electromagnetic Analysis at Design Time

（3）Side Channel III

- On Second-Order Differential Power Analysis
- Improved Higher-Order Side-Channel Attacks with FPGA Experiments

（4）Hardware Attacks and Countermeasures I

- Successfully Attacking Masked AES Hardware Implementations
- Masked Dual-Rail Pre-Charge Logic: DPA-Resistance without Routing Constraints

- Masking at Gate Level in the Presence of Glitches

（5）Hardware Attacks and Countermeasures II

- Data Remanence in Flash Memory Devices
- Prototype IC with WDDL and Differential Routing DPA Resistance Assessment

（6）Hardware Attacks and Countermeasures III

- DPA Leakage Models for CMOS Logic Circuits
- The "backend duplication" method

参考文献

[1] 宮崎 隆行, 辻村 達徳, 松本 勉, ”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”, 2006 年 暗号と情報セキュリティシンポジウム予稿集 1C3-1, 2006 年 1 月

[2] 久門 亨, 角尾 幸保, 後藤 敏, 池永 剛, ”ストリーム暗号に対する DPA”, 2006 年 暗号と情報セキュリティシンポジウム予稿集 1C3-2, 2006 年 1 月

[3] 鈴木 大輔, 佐伯 稔, ”2 線式回路による DPA 対策方式の安全性評価”, 2006 年 暗号と情報セキュリティシンポジウム予稿集 1C3-31, 2006 年 1 月

[4] 山口 晃由, 山田 敬喜, ”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”, 2006 年 暗号と情報セキュリティシンポジウム予稿集 1C3-4, 2006 年 1 月

[5] 佐伯 稔, 鈴木 大輔, 佐藤 恒夫, ”FPGA 上での電磁波/電界情報に基くサイドチャネル解析の試行”, 2006 年 暗号と情報セキュリティシンポジウム予稿集 1C3-5, 2006 年 1 月

[6] Dong-Guk Han, Tsuyoshi Takagi, Tae Hyun Kim, Ho Won Kim, Kyo Il Chung, ”Side Channel Attack on Improved XTR Single Exponentiation and a New Countermeasure2006 年 暗号と情報セキュリティシンポジウム予稿集 2C1-1, 2006 年 1 月 ”,

[7] 三宅 秀享, 野崎 華恵, 清水 秀夫, 新保 淳, ”Sbox 特性を利用した DPA 評価手法の有効性検証”, 2006 年 暗号と情報セキュリティシンポジウム予稿集 2C1-2, 2006 年 1 月

[8] 桶屋 勝幸, ”鍵付きハッシュ関数に対するサイドチャネル攻撃”, 2006 年 暗号と情報セキュリティシンポジウム予稿集 2C1-3, 2006 年 1 月

[9] 酒井 康行, ”ランダム化射影座標を用いた楕円曲線暗号実装に対する電力解析”, 2006 年 暗号と情報セキュリティシンポジウム予稿集 2C1-4, 2006 年 1 月

[10] Wei Dai, Tohru Hisakado, Zhenyu Liu, Satoshi Goto, Takeshi Ikenaga, Yukiyasu Tsunoo, ”A power disturbance circuit for A5/1 resistant to power analysis attack”, 2006 年 暗号と情報セキュリティシンポジウム予稿集 2C2-1, 2006 年 1 月

[11] 太田 良二, 辻原 悦子, 川幡 剛嗣, 久保 博靖, 洲崎 智保, 角尾 幸保, ”サイドチャネル防御機構付き分割キャッシュアーキテクチャに関する一考察”, 2006 年 暗号と情報セキュリティシンポジウム予稿集 2C2-21, 2006 年 1 月

[12] 関口 秀紀, 田中 秀磨, 瀬戸 信二, 山村 明弘, ”PC から放出する電磁気的雑音と含有するモニタ表示画像の再現”, 2006 年 暗号と情報セキュリティシンポジウム予稿集 2C2-3, 2006 年 1 月

[13] 小池 正修, ”2 並列剰余乗算を用いたベキ乗剰余算の高速化に関する考察”, 2006 年 暗号と情報セキュリティシンポジウム予稿集 2C3-1, 2006 年 1 月

[14] 小田 哲, 青木 和麻呂, 小林 鉄太郎, ”Pentium 4 における Camellia の高速実装”, 2006 年 暗号と情報セキュリティシンポジウム予稿集 2C3-2, 2006 年 1 月

[15] 福田 明香, 松井 充, ”64-bit プロセッサにおける共通鍵暗号のソフトウェア実装性能解析”, 2006 年 暗号と情報セキュリティシンポジウム予稿集 2C3-3, 2006 年 1 月

[16] 古川 和快, 武仲 正彦, 久門 耕一, 平井 聡, 山村 周史, 山本 昌生, "Itanium 2 プロセッサ上における RSA 暗号の高速実装", 2006 年 暗号と情報セキュリティシンポジウム予稿集 2C3-4, 2006 年 1 月

[17] 峯松 一彦, 角尾 幸保, "差分一様性を持つ置換を利用したメッセージ認証方式と AES による実装について", 2006 年 暗号と情報セキュリティシンポジウム予稿集 2C3-5, 2006 年 1 月

[18] 宮本 篤志, 本間 尚文, 青木 孝文, 佐藤 証, "積和演算器に基づくスケーラブル高基数モンゴメリ乗算器の設計と評価", 2006 年 暗号と情報セキュリティシンポジウム予稿集 2C4-1, 2006 年 1 月

[19] 大和田 徹, 平 重喜, 松本 貴士, 川村 嘉郁, "MUGI, AES, SHA-1/256 統合ハードウェアの実装"2006 年 暗号と情報セキュリティシンポジウム予稿集 2C4-2, 2006 年 1 月

[20] 松永 明, 松本 勉, "テーブルネットワーク型暗号ソフトウェアの一クラスの耐タンパー性評価" 2006 年 暗号と情報セキュリティシンポジウム予稿集 2C4-3, 2006 年 1 月

[21] 豊福 達也, 田端 利宏, 櫻井 幸一, "メソッド実行順序の擬似的入れ替えによる難読化手法の提案"2006 年 暗号と情報セキュリティシンポジウム予稿集 2C4-4, 2006 年 1 月

[22] Pei Chi Cheng, Chung Huang Yang, Kouichi Sakurai, "Design and Implementation of a Live-CA CD/DVD on an Open Source Environment"2006 年 暗号と情報セキュリティシンポジウム予稿集 2C4-5, 2006 年 1 月

[23] William Dupuy, Sebastien Kunz-Jacques, "Resistance of Randomized Projective Coordinates Against Power Analysis", Proceeding of Workshop on Cryptographic Hardware and Embedded Systems (CHES 2005), Springer-Verlag, LNCS 3659 pp.1-14, 2005

[24] Dakshi Agrawal, Josyula R Rao, Pankaj Rohatgi, Kai Schramm, "Templates as Master Keys", Proceeding of Workshop on Cryptographic Hardware and Embedded Systems (CHES 2005), Springer-Verlag, LNCS 3659 pp.15-29, 2005

[25] Werner Schindler, Kerstin Lemke,Christof Paar, "A Stochastic Model for Differential Side Channel Cryptanalysis", Proceeding of Workshop on Cryptographic Hardware and Embedded Systems (CHES 2005), Springer-Verlag, LNCS 3659 pp.30-46, 2005

[25] Stefan Mangard, Norbert Pramstaller, Elisabeth Oswald, "Successfully Attacking Masked AES Hardware Implementations", Proceeding of Workshop on Cryptographic Hardware and Embedded Systems (CHES 2005), Springer-Verlag, LNCS 3659 pp.157-171, 2005

[27] Thomas Popp, Stefan Mangard, "Masked Dual-Rail Pre-Charge Logic: DPA-Resistance without Routing Constraints", Proceeding of Workshop on Cryptographic Hardware and Embedded Systems (CHES 2005), Springer-Verlag, LNCS 3659 pp.156-171, 2005

[28] Wieland Fischer, Berndt M. Gammel, "Masking at Gate Level in the Presence of Glitches", Proceeding of Workshop on Cryptographic Hardware and Embedded Systems (CHES 2005), Springer-Verlag, LNCS 3659 pp.172-186, 2005

[29] C.Gebotys, S.Ho, C.Tiu, "EM Analysis of Rijndael and ECC on a Wireless Java-based PDA", Proceeding of Workshop on Cryptographic Hardware and Embedded Systems (CHES 2005),

Springer-Verlag, LNCS 3659 pp.250-264, 2005

[30] Markus G. Kuhn, ”Security Limits for Compromising Emanations”, Proceeding of Workshop on Cryptographic Hardware and Embedded Systems (CHES 2005), Springer-Verlag, LNCS 3659 pp.265-279, 2005

[31] Huiyun Li, Theodore Markettos, Simon Moore, ”Security Evaluation Against Electromagnetic Analysis at Design Time”, Proceeding of Workshop on Cryptographic Hardware and Embedded Systems (CHES 2005), Springer-Verlag, LNCS 3659 pp.280-292, 2005

[32] Marc Joye, Pascal Paillier, Berry Schoenmakers, ”On Second-Order Differential Power Analysis”, Proceeding of Workshop on Cryptographic Hardware and Embedded Systems (CHES 2005), Springer-Verlag, LNCS 3659 pp.293-308, 2005

[33] Eric Peeters, Francois-Xavier Standaert, Nicolas Donckers, Jean-Jacques Quisquater, ””, Proceeding of Workshop on Cryptographic Hardware and Embedded Systems (CHES 2005), Springer-Verlag, LNCS 3659 pp.309-323, 2005

[34] Sergei Skorobogatov, ”Data Remanence in Flash Memory Devices”, Proceeding of Workshop on Cryptographic Hardware and Embedded Systems (CHES 2005), Springer-Verlag, LNCS 3659 pp.339-353, 2005

[35] Kris Tiri, David Hwang, Alireza Hodjat, Bo-Cheng Lai, Shenglin Yang, Patrick Schaumont, Ingrid Verbauwhede, ”Prototype IC with WDDL and Differential Routing DPA Resistance Assessment”, Proceeding of Workshop on Cryptographic Hardware and Embedded Systems (CHES 2005), Springer-Verlag, LNCS 3659 pp.354-365, 2005

[36] Daisuke Suzuki, Minoru Saeki, Tetsuya Ichikawa, ”DPA Leakage Models for CMOS Logic Circuits”, Proceeding of Workshop on Cryptographic Hardware and Embedded Systems (CHES 2005), Springer-Verlag, LNCS 3659 pp.366-382, 2005

[37] Sylvain Guilley, Philippe Hoogvorst, Yves Mathieu, Renaud Pacalet, ”The "backend duplication" method”, Proceeding of Workshop on Cryptographic Hardware and Embedded Systems (CHES 2005), Springer-Verlag, LNCS 3659 pp.383-397, 2005

[38] 藤崎浩一, 清水秀夫, 新保 淳, ”32bitCPU を対象とした電力解析用評価環境の開発と実証実験”, 電子情報通信学会 技術研究報告 信学技報, vol. 105, no. 193, ISEC 2005-19, pp. 75-82, 2005 年 7 月.

[39] Katsuyuki Okeya, Tsuyoshi Takagi, Camille Vuillaume, ”Defeating Simple Power Analysis on Koblitz Curves”, 電子情報通信学会 技術研究報告 信学技報, vol. 105, no. 193, ISEC 2005-18, pp. 67-74, 2005 年 7 月

[40] 萩原雄一, Travis Spann, 武部達明, ”日本の CMVP の方向性 II”, 電子情報通信学会 技術研究報告 信学技報, vol. 105, no. 193, ISEC 2005-29, pp. 147-153, 2005 年 7 月.

[41] 豊福達也, 田端利宏, 櫻井幸一, ”乱数を用いた難読化手法の複雑な制御構造への適用に関する一考察”, 電子情報通信学会 技術研究報告 vol. 105, no. 193, ISEC 2005-38, 2005 年 7 月

[42] 野崎華恵, 安田心一, 藤崎浩一, 新保 淳, 藤田 忍,"DPA マスク対策における乱数の影響について", 電子情報通信学会 技術研究報告 信学技報, vol. 105, no. 290, ISEC 2005-77, pp. 7-13, 2005 年 9 月.

[43] 角石洋輔, 佐々木明彦, 阿部公輝, "DES への差分電力解析攻撃における参照位置とビット数について", 電子情報通信学会 技術研究報告 信学技報, vol. 105, no. 396, ISEC 2005-106, pp. 51-56, 2005 年 11 月.

[44] 高橋芳夫, 佐藤 証, 梅田伸明, "ブロック暗号の FPGA 実装に対するサイドチャネル攻撃", 電子情報通信学会 技術研究報告 信学技報, vol. 105, no. 484, ISEC 2005-111, pp. 5-10, 2005 年 12 月.

[45] 高木直史, "ハードウェアサポートによるガロア体上の演算の高速化", 電子情報通信学会 技術研究報告 信学技報, vol. 105, no. , ISEC 2005- , pp. - , 2006 年 3 月.

[46] 角尾幸保, 久門 亨, 辻原悦子, 松本 勉, 川村信一, 藤崎浩, "INSTAC-8 準拠評価ボードを使った実装攻撃実験の結果報告", 電子情報通信学会 技術研究報告 信学技報, vol. 105, no. , ISEC 2005- , pp. - , 2006 年 3 月.

[47] 山内裕史, 池田 誠, 浅田邦博, "微細素子のパラメータばらつきによる耐タンパーLSI の劣化と対策", 電子情報通信学会 技術研究報告 信学技報, vol. 105, no. , ISEC 2005- , pp. - , 2006 年 3 月.

[48] 北原 潤, 桶屋勝幸, "ハッシュ関数のハードウェア実装および耐タンパ性の一評価", 電子情報通信学会 技術研究報告 信学技報, vol. 105, no. , ISEC 2005- , pp. - , 2006 年 3 月.

[49] 今井裕一, 本間尚文, 長嶋 聖, 青木孝文, 佐藤 証, "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", 電子情報通信学会 技術研究報告 信学技報, vol. 105, no. , ISEC 2005- , pp. - , 2006 年 3 月.

[50] 池田尚隆, 山口 梢, 金子敏信, "平均値法を適用したキャッシュ攻撃における必要平文数の理論的考察", 電子情報通信学会 技術研究報告 信学技報, vol. 105, no. , ISEC 2005- , pp. - , 2006 年 3 月.

[51] 服部 太郎, 双紙 正和, 宮地 充子, "動的解析に対し耐タンパ性を持つ難読化手法の提案", 情報処理学会 CSEC 研究会, 2006 年 3 月