CRYPTREC Report 2003

暗号モジュール委員会報告書

平成 16 年 3 月

独立行政法人　情報処理推進機構

通信・放送機構

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 2003 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。各府省は、情報システムの構築に当たって暗号を利用する場合には、調達仕様書における入札要件化等の方法により、可能な限り電子政府推奨暗号の利用を推進する旨が合意されており、電子政府システムの安全性確保に向けた具体的な取り組みの一つとなっている。

しかし、暗号製品については、暗号アルゴリズムそのものではなく、その実装方法に問題があることが多いため、暗号化 LSI チップ等の暗号製品(暗号モジュール)の安全性を評価することも必要である。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評価・認証制度(CMVP[1])を運用している。また、ISO/IEC JCT1/SC27 においては、暗号モジュールに関するセキュリティ要求事項の国際標準化に向けた審議が開始されている。

このような背景から、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・放送機構が共同で運営する暗号モジュール委員会が新たに設置されることとなった。暗号モジュール委員会では、本年度の活動として、先行する米国とカナダの基準をベースにわが国に適した暗号モジュールの評価基準と試験基準の検討を行うとともに、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、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

[1] Cryptographic Module Validation Program

本報告書の利用にあたって

本報告書の想定読者は、一般的な情報セキュリティの基礎知識を有している方である。例えば、電子署名やGPKI[2]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についている方などを想定している。ただし、暗号モジュールの試験基準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を記述した。また、本報告書とは別に、暗号モジュール評価基準第 0 版、暗号モジュール試験基準第 0 版、及び暗号モジュールへの攻撃に対する調査をまとめた。これらについては、下記URLの「CRYPTREC Report 2003の公開」で参照できる。

http://www.ipa.go.jp/security/enc/CRYPTREC/index.html
http://www.shiba.tao.go.jp/kenkyu/CRYPTREC/index.html

暗号モジュール評価基準第0版及び暗号モジュール試験基準第0版は、米国NIST[3]が発行している下記の 2 つの標準をそれぞれ翻訳したものであり、暗号モジュール試験基準第 0 版は、翻訳に加え、さらに英文の解釈や基準内容の理解に必要と思われる解説やコメント等を加えたものであることに注意されたい。

来年度、これら第 0 版をもとに、わが国において暗号モジュールの評価基準及び試験基準を運用する上での問題点及び改善点について調査検討を進め、第 1 版として完成させる予定である。

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

・Derived Test Requirements for FIPS PUB 140-2, Security Requirement for Cryptographic Modules (February 12, 2003 Draft)

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】　cryptrec@ipa.go.jp 又は cryptrec@shiba.tao.go.jp

---

[2] Government Public Key Infrastructure
[3] National Institute of Standards and Technology

暗号モジュール委員会　委員名簿

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	上野　天徳	財団法人日本品質保証機構　主任
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	佐伯　正夫	三菱電機インフォメーションシステムズ株式会社 副センター長
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	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 主管研究員
委員	細川　正広	日本電気株式会社 マネージャー
委員	横田　薫	松下電器産業株式会社 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

鳥居　秀行	警察庁　情報通信局（2003 年 7 月まで）
山田　浩一	警察庁　情報通信局
中山　毅彦	警察庁　情報通信局
知識　親美	警察大学校　情報通信研究センター
富田　哲	防衛庁　長官官房
一條　靖彦	防衛庁　陸上幕僚監部
石川　正興	防衛庁　技術研究本部
山本　寛繁	総務省　行政管理局
藤本 昌彦	総務省 情報通信政策局（2003 年 7 月まで）
佐藤 憲一郎	総務省 情報通信政策局（2003 年 7 月まで）
福岡 晃	総務省 情報通信政策局（2003 年 7 月まで）
野崎 雅稔	総務省 情報通信政策局
榎本 淳一	総務省 情報通信政策局

黒田 崇	総務省 情報通信政策局
石川　雅一	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
北浦　康弘	経済産業省　商務情報政策局
滝澤　修	独立行政法人通信総合研究所
才所　敏明	財団法人日本規格協会（2003 年 10 月まで）
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

内藤理（2003 年 5 月まで）、早貸淳子、河内浩明、網島和博、大塚玲、小柳津育郎、黒川貴司、杉田誠、田中公明、矢田健一（2003 年 8 月まで）、山岸篤弘

通信・放送機構

喜安拓（2003 年 7 月まで）、大久保明、横山隆裕（2003 年 7 月まで）、鳥居秀行、天野滋、高橋靖典、田中秀磨、半澤則之、藤田真史、山村明弘

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上で相手と直接対面することなしに受発注や決済等の重要な情報をやり取りする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の電子化を実現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。そのため、暗号技術を電子政府等で利用するためには、暗号技術を客観的に評価することが極めて重要となる。

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。この委員会は、産学の最高水準の暗号専門家により構成され、わが国における本格的な暗号技術評価プロジェクトがスタートすることになった。2001 年度からは委員会の共同事務局として通信・放送機構（TAO）が参加することとなった。

また、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して政策的な観点から検討が開始された。暗号技術評価委員会と暗号技術検討会には、関係する省庁もオブザーバとして参加する等、政府横断的な活動となっており、これらを総称して、CRYPTREC（Cryptography Research & Evaluation Committees）と呼ぶことになった。

2000 年度から 2002 年度までの 3 年間に及ぶ CRYPTREC 活動によって、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に客観的な評価が実施された結果、合計 29 方式の暗号技術が安全性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。

1.2 暗号モジュール委員会の新設

電子政府推奨暗号リストが公表されたが、今後これらの暗号方式の安全性を継続的に確認する必要があり、また、暗号アルゴリズムレベルの安全性だけでなく、暗号 LSI チップ等の暗号アルゴリズムが実装された製品（暗号モジュール）の安全性を確保する必要がある。

このような状況を踏まえて、2003 年度の CRYPTREC 体制を次のように再編し、暗号技術に関する調査検討及び評価に関する活動を継続して実施することとなった（図 1.1 参照）。

(1) 暗号技術検討会は、暗号技術の評価・利用等に関して政策的な観点から検討を行うものとして、存続する。

(2) 暗号技術評価委員会を発展的に改組し、電子政府推奨暗号の安全性の監視等を行う暗号技術監視委員会に再編する。

(3) 暗号モジュールの評価基準及び試験基準の作成や暗号実装関連技術等の調査・検討を行う暗号モジュール委員会を新たに設置する。

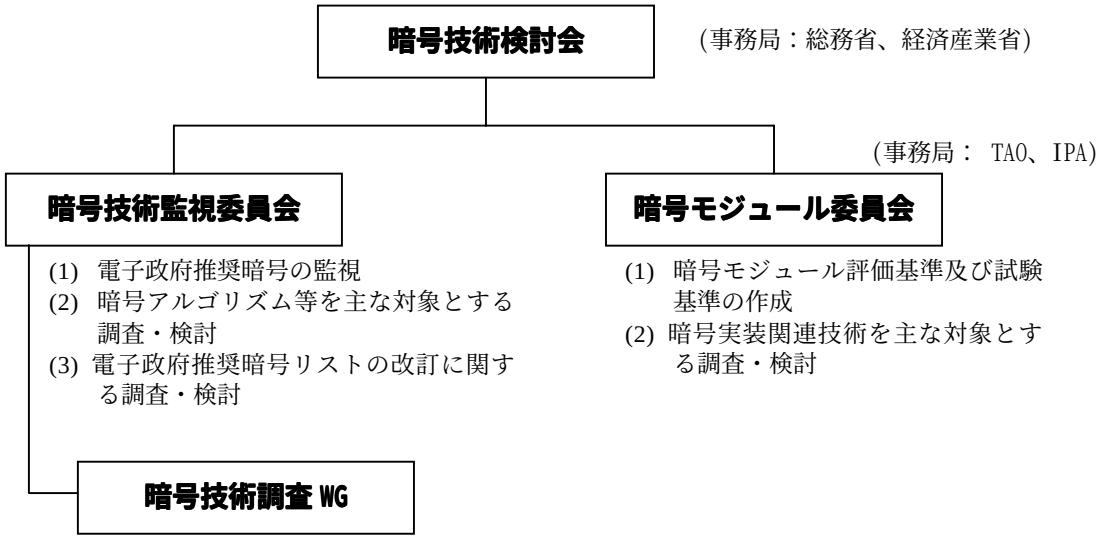

図 1.1 CRYPTREC 体制図

1.3 暗号モジュール評価に関する国際動向

米国 NIST は、カナダ CSE と共同で、CMVP(Cryptographic Module Validation Program)という暗号技術を実装レベルで評価・認証する制度を運用している。また、2002 年 10 月にワルシャワで開催された ISO/IEC JTC1 の会合で、米国とカナダが自国の政府調達基準である FIPS PUB 140-2[4](以下、FIPS 140-2 と記す)をベースに、暗号モジュールに対するセキュリティ要求事項の国際標準化を NWI[5]として提案した。英、仏、独等の欧州諸国もこの動きに同調しており、ISO/IEC JTC1/SC27 WG3 における審議の結果、第 1 フェーズとして、FIPS 140-2 をなるべくそのまま生かす形で標準化する方向で検討が進められることになった。

欧州各国においても、独自の基準によって暗号モジュールに対する評価・認証が行われているようであるが、その内容は公開されていない。世界的に見ても、現在のところ、暗号モジュールの評価に関して参照可能なものは、FIPS 140-2 及びその試験基準である DTR(Derived Test Requirements for FIPS PUB 140-2)だけであり、本委員会の活動の一つとして、上記 2 つの資料をベースに、わが国において適用可能な基準を検討することとなった。

1.4 暗号モジュールに対する攻撃に関する研究動向

暗号モジュールの設計者は、多くの場合、信頼できる計算環境の中に秘密情報が保存され、それらの情報が外部からはアクセスできないことを想定している。しかし、実際には、マイクロチップは秘密情報を用いて演算を行う際、設計者の予想しなかった情報 (side-channel information) を外部に漏らしてしまうことがある。このような情報を利用して、秘密情報の解析を行う方法がサイドチャネル攻撃である。

具体的には、実行時の漏洩情報、すなわち、暗号処理装置外部から計測可能な情報（例えば、計算時間や電力消費量など）と、秘密鍵等の秘密情報との間の相関関係を利用して、秘密情報を推定しようとする攻撃手法であり、特に IC カードに対しては、大きな脅威となり得ることが報告されている。

本委員会では、このような攻撃を非破壊攻撃と呼び、LSI チップなどを破壊して中の秘密情報を盗み出すというような攻撃を破壊攻撃と呼ぶことにした。後述のように、本委員会では非破壊攻撃を主な対象として調査検討を進めることとした。

現在、わが国における非破壊攻撃に関する研究は、世界レベルで見ると遅れている。ま

---

[4] Federal Information Processing Standards Publication 140-2

[5] New Work Item

た現時点では、FIPS 140-2 には攻撃に対する具体的な項目は規定されていないが、FIPS 140-2（又は、ISO/IEC 標準）の数年後の内容改訂時には、非破壊攻撃に関する対策項目が追加される可能性が大きい。

欧米の標準を単に利用するだけでなく、わが国が主体的に技術研究を行って、その成果を国際標準化に反映し、世界に貢献することが求められている。そのためには、非破壊攻撃に関する研究を今から進め、数年後に他国と同等に意見が交わせるよう、わが国のポテンシャルを上げておくことが必要である。

1.5 暗号モジュール委員会の活動目的

以上のような状況を踏まえ、2002 年度の暗号技術検討会の報告書において、暗号モジュール委員会の活動目的が次のように設定された。

(a) 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得ることをも視野に入れながら、2005 年 3 月を目処に暗号モジュール評価基準及び試験基準を作成する。

(b)暗号技術監視委員会と連携をとりつつ、電子政府推奨暗号の安全性及び信頼性確保のための暗号実装関連技術を主な対象とする調査・検討を併せて行う。

上記を踏まえ、今年度の活動目的として、次の項目を設定した。

(1)FIPS 140-2 及び DTR の内容を調査・検討し、わが国の基準として適用可能な暗号モジュールの評価基準及び試験基準第 0 版を作成する。

(2)暗号実装関連技術について、最新の研究動向を調査し、各種攻撃手法やその対策の検討、評価基準への取り入れ方策等に関して、今後の調査・研究方針を決定する。

第 2 章　委員会開催状況

2003 年度、暗号モジュール委員会は、計 9 回開催された。各回会合の概要は以下のとおりである。

回	開催日時	主な議題
第 1 回	平成 15 年 6 月 16 日 10:00～12:00	暗号モジュール委員会の活動方針 ISO/IEC JTC1/SC27 WG2 ケベック会合報告
第 2 回	平成 15 年 7 月 25 日 14:00～17:00	暗号モジュール委員会の活動方針 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 ・研究方針検討のための文献調査依頼 暗号モジュール評価基準及び試験基準の検討 ・暗号モジュール仕様 ・暗号モジュールのポートとインタフェース
第 3 回	平成 15 年 8 月 29 日 14:00～18:00	ISO/IEC JTC1/SC27 1st Working Draft についてのコメント 暗号モジュール評価基準及び試験基準の検討 ・役割・サービス・及び認証 ・有限状態モデル
第 4 回	平成 15 年 9 月 17 日 15:00～18:00	暗号モジュールに実装された暗号アルゴリズムの検証方法について
第 5 回	平成 15 年 10 月 10 日 14:00～20:00	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 ・研究方針案 暗号モジュール評価基準及び試験基準の検討 ・物理セキュリティ
第 6 回	平成 15 年 11 月 20 日 14:00～16:50	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 ・研究方針案 暗号モジュール評価基準及び試験基準の検討 ・動作環境 ・暗号鍵管理
第 7 回	平成 15 年 12 月 19 日 13:00～17:00	評価用標準プラットフォームでの研究に関する検討 ・評価用標準プラットフォーム要求仕様案、研究方法について 暗号モジュール評価基準及び試験基準の検討 ・電磁妨害/電磁両立性 ・自己テスト

第 8 回	平成 16 年 1 月 16 日 14:00～17:00	評価用標準プラットフォームでの研究に関する検討 ・評価用標準プラットフォーム要求仕様案、研究方法について 暗号モジュール評価基準及び試験基準の検討 ・設計保証 ・その他の攻撃の対処
第 9 回	平成 16 年 2 月 13 日 15:00～17:30	暗号モジュール評価基準及び試験基準の検討(第 0 版案) 2003 年度報告書の検討

第 3 章　活動内容と成果概要

3.1　暗号モジュール評価基準及び試験基準の策定

3.1.1　FIPS 140-2 の概要

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求事項を規定した、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、その後、CHANGE NOTICE が発行されており、本委員会では、2002 年 12 月に発行された版を基準策定のための検討資料とした。

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。

3.1.2　DTR の概要

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 FIPS 140 と同様、適宜改訂される。本委員会では、2003 年 2 月に発行されたドラフト版を基準策定のための検討資料とした。

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。

3.1.3 評価基準及び試験基準第0版の作成

暗号モジュールの評価基準及び試験基準の作成に関しては、FIPS 140-2及びDTRの翻訳作業から着手した。FIPS 140-2 に記載されている全ての要求事項は、DTR ではアサーションとして同じ内容が記載されており、作業重複を避けるため、DTRの翻訳作業を中心に進めた。また、1.3節で述べたように、ISO/IEC JTC1/SC27 WG3において、現在、FIPS 140-2をベースにした暗号モジュール評価基準の国際標準化に関する審議が行われており、そうした動向に柔軟に対応できるようにするため、翻訳作業においては、なるべく原文に近い形で訳文を作成することにした。

次に、作成した訳文をもとに、英文解釈の統一を図るとともに、基準内容に関する不明点及び問題点の抽出・整理を行い、表 3.1 に示す問題点整理表にまとめた。なお、制度面に関するものについては、本委員会だけでは解決できないことから、問題点抽出のみにとどめ、主に技術的内容についての議論を行った。また、委員会内で解決できなかった技術的内容については、NISTへ質問状を送付し、回答を求める等の作業を実施した。

以上の作業より作成したFIPS 140-2及びDTRの翻訳版は、暗号モジュールの評価基準及び試験基準の第0版と位置付け、今後、これら第0版をもとに、抽出・整理した問題点の解決や運用上の問題点の洗い出し等について調査検討を進め、わが国の基準として適用可能な暗号モジュールの評価基準及び試験基準の第1版を作成する予定である。

また、暗号モジュール委員会では、経済産業省からの依頼を受け、平成15年6月にISO/IEC JTC1/SC27 WG3から提示された暗号モジュール評価基準に関する国際規格の一次案について、その内容を精査し、暗号モジュール委員会としてのコメント提出を行った。

表 3.1　暗号モジュールの評価基準及び試験基準における問題点整理表

No.	対象	指摘箇所	問題点
1	評価基準	1.2 節 第 4 段落	電子政府向け暗号モジュールの要求事項において、CC(Common Criteria)への適合を含めてよいのかの検討が必要である。
2	試験基準	TE01.08.05	試験者は、何をもって十分詳細と判断するのかを NIST に確認する必要がある。 TE01.08.02 や TE01.08.03 にて挙げられている箇条書き項目が含まれていれば十分詳細とするのか、それとも、その箇条書き項目の内容が十分詳細であるかどうかを判断する必要があるのか？
3	評価基準 試験基準	4.1 節 第 11 段落 AS01.14	「高級言語（High-level specification languages）を用いて設計されていなければならない」とあるが、「高級仕様言語を用いた設計」がどのようなことを指すのかを NIST に確認する必要がある。
4	試験基準	TE02.01.04	実際どのように検証すればよいのかを NIST に確認する必要がある。
5	試験基準	VE02.11.01	主要カテゴリが何を指しているかを NIST に確認する必要がある。
6	試験基準	VE03.20.01	"authentication"は、"authorization"の誤りではないかを NIST に確認する必要がある。ただし、TE03.20.02 の内容から、誤りでない可能性もある。
7	試験基準	VE03.22.01	"authentication data to the module"は、直前の AS03.22 の"authentication data within the cryptographic module"と同じ意味かどうかを NIST に確認する必要がある。
8	試験基準	TE04.05.02	"the finite state diagrams"は"the state transition diagrams"と同じ意味かどうかを NIST に確認する必要がある。
9	評価基準 試験基準	4.5 節 第 1 段落 AS05.01	(1)"When installed"は、" to deter unauthorized use or modification of the module (including substitution of the entire module)"にかかるのか、又は、文章全体にかかるのかを NIST に確認する必要がある。 (2)"When installed"は、「インストールの作業中」か、又は、「インストールされている状態」の意味のどちらであるかを NIST に確認する必要がある。
10	試験基準	TE05.09.02	"operational keys"の定義を NIST に確認する必要がある。
11	評価基準 試験基準	4.5.3 節 第 4 段落 AS05.34	"production-grade"の定義を NIST に確認する必要がある。
12	試験基準	VE05.37.03	機械的錠が掛けられている場合において、錠についての文書の必要性を NIST に確認する必要がある。

13	評価基準 試験基準	4.5.3 節 第 22 段落 AS05.41	"strong enclosure"の定義を NIST に確認する必要がある。
14	試験基準	TE05.47.01	"The vendor literature"は、"documentation"の間違いかどうか確認する必要がある。間違いでなければ、"The vendor literature"の定義を NIST に確認する必要がある。
15	試験基準	TE05.53.04	本試験は、「囲いが除去可能なカバー若しくはドアを有する場合」に必要な試験かどうかを NIST に確認する必要がある。
16	試験基準	TE06.08.02	(1)「改ざん」の定義を NIST に確認する必要がある。(意味を持たない変更も改ざんと扱うのかどうか？) (2)「完全性が維持される場合には」とは、「事実として完全性が維持されている」のか、又は「事実として完全性は崩れているが維持されているように見える」のか、どちらの意味なのかを NIST に確認する必要がある。
17	試験基準	TE07.01.02	本試験内容は、1 項、2 項の条件の両方があって初めて成立する内容であり、かつ、1 項の"access"には、"modify"も含まれるが、"modify"に関しては、2 項で述べているので、1 項では暗号化された鍵にアクセスできてもよいという解釈でよいかを NIST に確認する必要がある。
18	評価基準 試験基準	4.8 節全体 8 章全体	本節/本章に記載されている FCC(強制法規)に相当する規格は日本にはないため、電子政府向け暗号モジュールの要求事項として、本節/本章をどのように扱うかについて検討が必要である。
19	試験基準	VE09.31.01, VE09.33.01	DTR における AS と VE の TE において、AS の段階で明示的に文書化の要求と実装上の要求をしている場合と、AS では機能面の要求だけで、VE や TE で文書化と実装面に分離している場合と１つの VE や TE の中で文書化と実装の一致を要求している場合があり、首尾一貫していないため、第１版作成に向け、記載されている内容が何を要求しているのか(例えば、文書化のみを要求/実装の一致を要求/文書化 + 実装の一致を要求等をコメント欄に記載する)を明確化するかどうかを含め、再度整理が必要である。
20	評価基準 試験基準	4.9.2 節 第 14 段落 AS09.43	本試験は、次のｎbit を生成して比較するのか、又はシフト詰めして比較するのか、又はどちらでもよいのかを NIST に確認する必要がある。 例：1 bit 単位で乱数生成する場合、 ・初期化後：2n bit 生成して、n bit で分けて、比較する。 ・その後： <A> 1 bit 生成して、2n bit を 1 bit シフト詰めして比較する？ <B> n bit 生成して、2n bit を n bit シフト詰めして比較する？

21	試験基準	TE10.15.01	注に記載されている"NCSC-TG-10"に相当する規格は日本にはないため、電子政府向け暗号モジュールの要求事項として、本注をどのように扱うかについて検討が必要である。
22	評価基準 試験基準	APPENDIX A 第1段落 AS12.01	"the validation facility"は「試験機関」の誤りではないかを NIST に確認する必要がある。

3.1.4 評価基準及び試験基準第 0 版の構成

暗号モジュール評価基準第 0 版は ”FIPS PUB 140-2, SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES, CHENGE NOTICE (12-03-2002) ”を翻訳したものであり、構成は FIPS 140-2 と同様の構成である。

本文は、第 1 章には概要、第 2 章には用語及び略語集、第 3 章には機能的セキュリティ目標、第 4 章にはセキュリティ要求事項を記述している。さらに、第 4 章は全 11 節から構成され、各節でそれぞれの分野のセキュリティ要求事項を規定している。第 4.1 節には暗号モジュール仕様、第 4.2 節には暗号モジュールのポート及びインタフェース、第 4.3 節には役割・サービス・認証、第 4.4 節には有限状態モデル、第 4.5 節には物理セキュリティ、第 4.6 節には動作環境、第 4.7 節には暗号鍵管理、第 4.8 節には電磁妨害/電磁両立性、第 4.9 節には自己テスト、第 4.10 節には設計保証、第 4.11 節にはその他の攻撃の対処を記述している。

また、附属書として、APPENDIX A には文書要求事項のまとめ、APPENDIX B には推奨ソフトウエア開発手順、APPENDIX C には暗号モジュールのセキュリティポリシ、APPENDIX D には参考文献、APPENDIX E には使用可能なインターネットの URL を記述している。

暗号モジュール試験基準第 0 版は、 ”Derived Test Requirements for FIPS PUB 140-2, Security Requirement for Cryptographic Modules (February 12, 2003 Draft) ”を翻訳し、さらに英文の解釈や基準内容の理解に必要と思われる箇所には、欄を設け、解説やコメント等を加えたものであり、構成は、DTR と同様である。

本文は、第 1 章には暗号モジュール仕様、第 2 章には暗号モジュールのポート及びインタフェース、第 3 章には役割・サービス・認証、第 4 章には有限状態モデル、第 5 章には物理セキュリティ、第 6 章には動作環境、第 7 章には暗号鍵管理、第 8 章には電磁妨害/電磁両立性、第 9 章には自己テスト、第 10 章には設計保証、第 11 章にはその他の攻撃の対処を記述している。

また、附属書として、APPENDIX A には文書要求事項のまとめ、APPENDIX B には推奨ソフトウエア開発手順、APPENDIX C には暗号モジュールのセキュリティポリシを記述している。

試験基準では、評価基準に対応するセキュリティ要求事項をアサーションと呼び、AS で始まるシーケンス番号で識別している。また、そのアサーションに対応したベンダに課せられる要求事項は VE で始まるシーケンス番号で識別し、そのアサーションに対応した試験者に課せられる要求事項は TE で始まるシーケンス番号で識別している。各章では、アサーションごとに、AS、VE、TE の順に各要求事項を記述している。

暗号モジュール評価基準第 0 版及び暗号モジュール試験基準第 0 版については、下記 URL の「CRYPTREC Report 2003 の公開」で参照できる。

http://www.ipa.go.jp/security/enc/CRYPTREC/index.html
http://www.shiba.tao.go.jp/kenkyu/CRYPTREC/index.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　暗号モジュールへの攻撃法

暗号モジュールに埋め込まれている暗号鍵や復号鍵等の秘密情報を暴露したり推定したりする攻撃には、以下の例に示すように大きく 2 種類に分けられる。

(a)暗号モジュールを動作させた時の実行時間や消費電力量等、外部から観測することにより得られる情報のみを用いて、秘密情報を取り出すような攻撃

(b)暗号モジュールを包んでいるパッケージ等をレーザや薬品などで破壊し、暗号モジュール内部の回路を露出させ、秘密情報を取り出すような攻撃

暗号モジュール委員会では、上記(a)のような攻撃を「非破壊攻撃」、(b)のような攻撃を「破壊攻撃」と定義した。各攻撃には、更にいくつかの攻撃法があり、その分類を図 3.1 に示す。

非破壊攻撃は、破壊攻撃を受けた場合と異なり、攻撃を受けた跡（タンパー証跡）が残りにくく、また攻撃コストも破壊攻撃に比べ安価に攻撃が行える傾向にある。

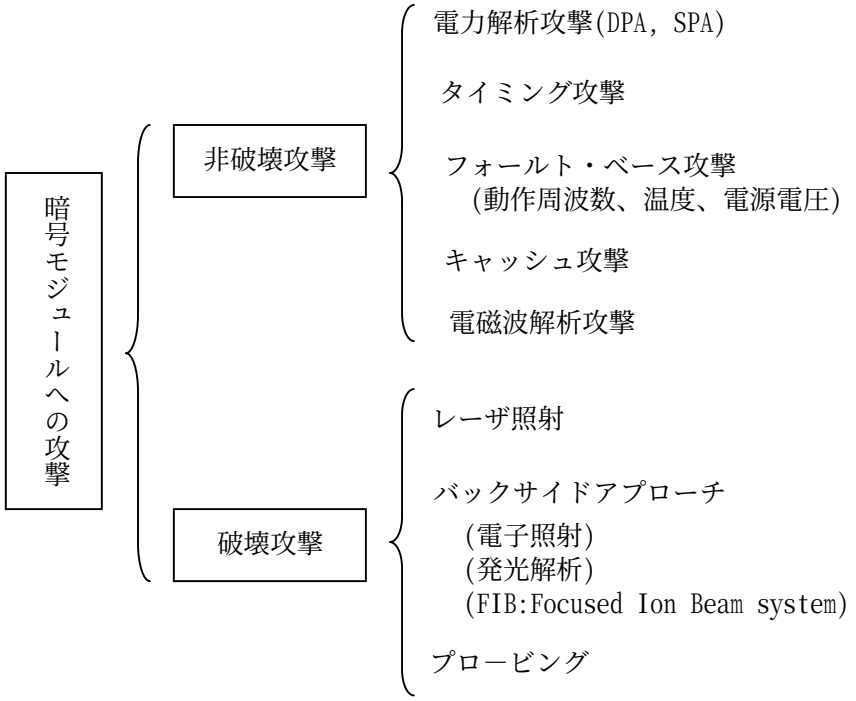

図 3.1　攻撃手法の分類

3.2.2 具体的な調査・研究テーマについての検討

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・研究において、その具体的な調査・研究テーマを検討するにあたり、日本規格協会情報技術標準化研究センター(INSTAC)[6]耐タンパー性に関する標準化調査研究委員会と共同で文献調査を行った。
調査する文献については、最近の約 5 年間で主要な学会等（CRYPTO, CHES 等）で発表されている暗号モジュールの非破壊攻撃及び破壊攻撃に関する主な論文を抽出し、その内容を調査した。文献調査結果のまとめを表 3.2 に示す。表中の No.欄の番号は、調査した文献の整理番号である。

表 3.2　暗号モジュールへの非破壊攻撃及び破壊攻撃に対する文献調査まとめ

対策の記載有無	攻撃内容		件数	割合	No
有り	破壊攻撃		5	5%	1, 2, 4, 12, 74
	非破壊攻撃	電力解析攻撃	36	38%	22, 23, 26, 27, 28, 29, 31, 32, 34, 39, 41, 42, 43, 44, 46, 47, 50, 51, 52, 53, 54, 57, 58, 59, 60, 61, 62, 64, 65, 68, 72, 73, 75, 90, 93, 94
		電力解析攻撃＋α	8	8%	13, 37, 45, 48, 55, 56, 89, 95
		タイミング攻撃	6	6%	16, 17, 18, 19, 91, 92
		フォールト・ベース	4	4%	5, 6, 11, 49
		キャッシュ攻撃	2	2%	81, 86
		電磁波解析	2	2%	69, 71
		その他	6	6%	10, 14, 36, 67, 88, 97
無し	---		27	28%	3, 7, 8, 9, 20, 21, 24, 25, 30, 33, 35, 38, 40, 63, 66, 70, 76, 77, 78, 79, 80, 82, 83, 84, 85, 87, 96
合計			96	100%	

※詳細は下記 URL の「CRYPTREC Report 2003 の公開」で参照できる。
http://www.ipa.go.jp/security/enc/CRYPTREC/index.html
http://www.shiba.tao.go.jp/kenkyu/CRYPTREC/index.html

[6] http://www.jsa.or.jp/domestic/instac/base.htm

この調査結果を見ると、攻撃への対策が記述されている非破壊攻撃の電力解析攻撃に関する文献が多い。これは、この攻撃が現在注目されており、各研究機関で多くの対策が検討され、研究が進んでいると考えられる。

非破壊攻撃に関しては、以下のような理由からも、第一に調査・研究を進める必要があると考える。

1) 非破壊攻撃は、安価な攻撃コストで多大な攻撃効果が得られる可能性が高い。
2) 非破壊攻撃は、タンパー証跡が残らないものが多く、対策を運用でカバーできない場合がある。
3) 欧州の CC[7]評価機関、米国の CMVP 試験機関や NIST、カナダの CSE へのヒアリングにおいても、サイドチャネル攻撃対策は必須という意見が得られている。

上記結果から、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・研究の具体的なテーマを非破壊攻撃の電力解析攻撃に関する調査・研究とした。

3.2.3 電力解析攻撃に対する評価用標準プラットフォームの検討

(1) 電力解析攻撃に関する研究方針

この電力解析攻撃に関する研究の位置付けは、電力解析攻撃への対策に関する評価基準及び試験基準策定のための予備的な研究である。このため理論だけでなく、攻撃及び対策の効果に対する追試実験等を行い、実データに基づいた研究を行うことを研究方針とした。

本研究方針を進める具体的方法としては、基準策定のための必要なデータを多くの研究機関から効率的に収集できるように、評価用標準プラットフォームを構築し、このプラットフォーム上での評価手法の確立を目指すこととした。

(2) 評価用標準プラットフォーム構築に関する検討

電力解析攻撃に関して実データに基づく研究を進める場合、現状以下のような問題点が考えられる。

- 各社の研究機関で ASIC[8]又は ASSP[9]による評価研究がなされていることが予想されるが、その評価結果は機密情報となることが多いため、評価結果の公表が難しく、研究発展の障壁になっている。
- 電力解析攻撃対策の効果検証については、自他間の比較評価が効果的だが、

---

7 Common Criteria
8 Application Specific Integrated Circuit
9 Application Specific Standard Product

ASIC 等による評価の場合、他社製チップは設計内容等が不明（機密情報）であり、比較評価が難しい。

- 現在、電力解析攻撃に関する論文は、シミュレーション結果の報告が多く、実証データは少ない。

上記問題点を踏まえ、評価用標準プラットフォームを構築する手段としては、以下の理由により、FPGA[10]で構築することとした。

- FPGA は、ASIC や ASSP よりもはるかに安価で容易に製造できるため、共通的な実験環境を広範囲にしかも容易に整えることができる。
- 評価用標準プラットフォームを FPGA で構築することにより、同一の実験環境が各機関で容易に準備できるため、色々な技術や効果の比較が容易にでき、電力解析攻撃の研究に関する技術力向上に貢献できる。
- 評価用標準プラットフォームでの評価結果は、一般的なデータとなり、公表し易く、研究促進に貢献できる。

ただし、FPGA で構築した評価用標準プラットフォームで研究を進めるにあたり、以下のような懸念点も残る。

- FPGA による評価結果と ASIC 等による評価結果が一致しない(相関性がない)ことが考えられる。
- FPGA による評価は、電力解析攻撃対策の中でも、実装のためのアルゴリズム対策の検討には効果的と思われるが、ゲートレベルでのハードウェア対策の検討には効果的でない。

しかし、本研究分野において、わが国が主体的に技術研究を行い、基準策定を進めていくためには、早い時期から必要な基礎データを数多く収集する必要がある。従って、委員会では、いくつかの懸念点はあるものの、早期に着手可能であり、評価対象を柔軟かつ広範囲に設定できる FPGA による電力解析攻撃の評価を行うこととした。

(3) 評価用標準プラットフォームの要求仕様

FPGA による評価用標準プラットフォーム作成において、今年度はその要求仕様を検討した。

まず、評価用標準プラットフォーム作成の方針は以下とした。

- ハードウェア暗号機能ブロック（共通鍵暗号アクセラレータ、法剰余演算アクセラレータ）の電力解析攻撃の耐性評価が行えること。
- タイミング攻撃の評価も行えること。
- 対策効果の確認が容易に行えること。

評価用標準プラットフォームのイメージ図を図 3.2 に示す。イメージ図に記載され

[10] Field Programmable Gate Array

ている FPGA 部、インタフェース部、電源部についての要求仕様を以下にまとめる。

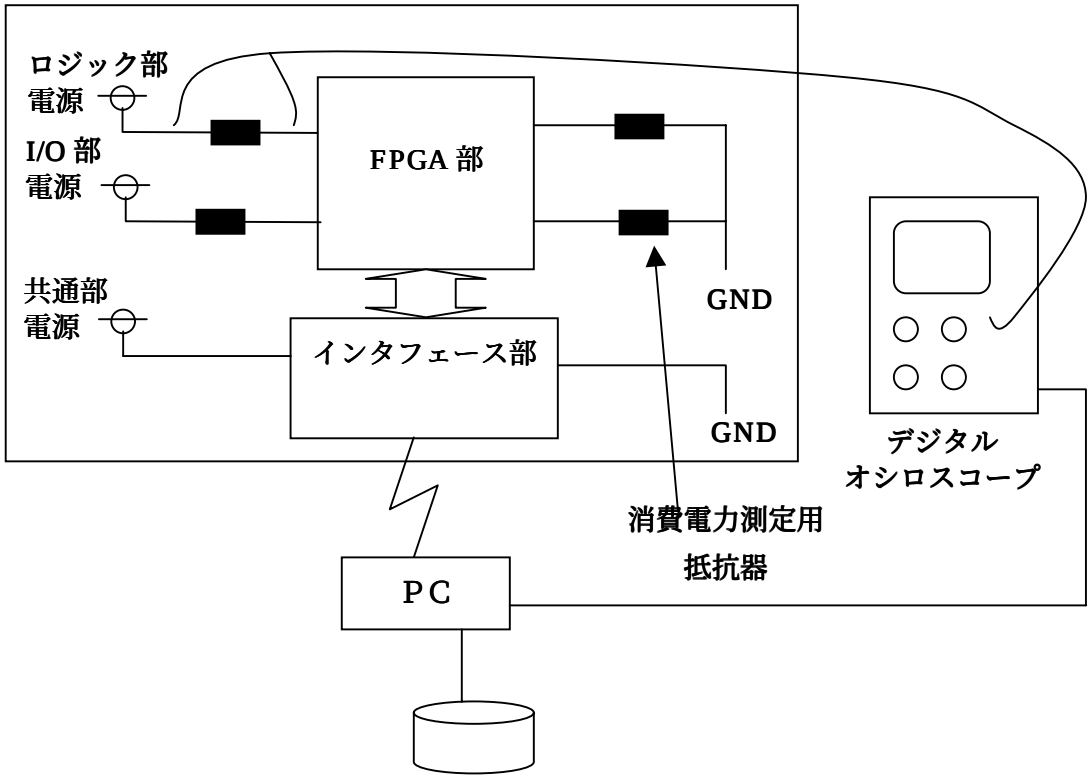

図 3.2　評価用標準プラットフォームのイメージ図

(a)FPGA 部

[必須仕様]

- 子基板上に実装し、子基板の差替えで複数の FPGA に対応できること。
- FPGA の I/O 部及びロジック部の電源は別々にすること。
- 暗号機能部を FPGA に実装ができること。
- 暗号機能部で処理するデータは PC から入力できること。
- 動作クロックの変更（水晶発振器の差し替え、外部クロック入力端子経由等）が可能なこと。
- 暗号機能部で処理するデータは PC に出力できること。

[オプション仕様]

- HDL 記述の MPU（SH-2、M32R、Z80 等）が搭載できること。
- 動作クロックへの干渉（クロック入力端子経由）が可能なこと。

・ 汎用 MPU (32bitMPU、16bitMPU、8bitMPU) と FPGA、RAM (32KB 以上) 、ROM を備えた子基板にも対応できること。

(b)インタフェース部

[必須仕様]

・ PC とのインタフェースとして、RS-232C インタフェースを有すること。
・ シリアルパラレル変換回路を有すること。
・ FPGA 部とのインタフェース仕様を変更できること。
・ 測定の開始点を指示するトリガ出力 (端子) を設けること。

[オプション仕様]

・ パラレルシリアル変換回路を有すること。

(c)電源部

[必須仕様]

・ 評価用標準プラットフォームの基板上に実装すること。
・ 電源、FPGA 部、周辺ロジック (インタフェース部、FPGA コンフィグレーション回路等) はそれぞれ分離すること。
・ 消費電力測定用抵抗器は基板表層で挿入でき、かつ、電力供給側又は GND 側のいずれかの挿入の選択が可能なこと。
・ 上記挿入する抵抗器は 10Ωを標準とする (容易に変更可能なこと) 。
・ デジタルオシロスコープのプローブ接続用端子を基板上に設けること (電圧プローブ又は電流プローブに対応可能なこと)。

[オプション仕様]

・ 電源へ干渉 (供給電圧の変更、瞬断、電源電圧の瞬間的な変更等) が可能なこと。
・ 電源ノイズは、無負荷状態 (FPGA を実装していない状態) で 50mVp-p 以下に抑えること。

※類似の FPGA に関する参考資料

1) S. Berna Örs, E. Oswald, and B. Preneel, ”Power-Analysis Attacks on an FPGA — First Experimental Results”, CHES2003, LNCS 2779, pp.35-50, Springer, 2003(September)
2) 山口、橋本、大熊、”高集積 FPGA 上に実装した共通鍵暗号への電力差分解析”、SCIS2004、2A4-5、2004-01

3.2.4 今後の活動方針

今後の活動としては、評価用標準プラットフォームを作成し、これを用いた評価手法の確立を目指す。評価手法確立後は、評価用標準プラットフォームの利用推進を検討し、暗号モジュール評価基準及び試験基準策定のための評価データの蓄積を行っていく。また、3.2.3(2)項で示したように、FPGAによる評価結果とASIC等による評価結果が一致しない(相関性がない)ことが考えられる。この点を明らかにする目的で、ASIC等による評価の検討も行っていく。