社団法人 情報処理学会 研究報告
IPSJ SIG Technical Reports

2005－ＣＳＥＣ－30 (21)
2005／7／21

日本のCMVPの方向性 II

萩原 雄一† Travis Spann‡ 武部 達明*

†株式会社シーフォーテクノロジー R&D事業本部 コンサルティング部
〒141-0021 東京都品川区上大崎 2-13-17 目黒東急ビル5階
‡ InfoGard Laboratories, Inc., FIPS 140-2 Evaluation Department
641 Higuera Street, Second Floor, San Luis Obispo, CA 93401
* 横河電機株式会社 開発基盤センター
〒180-8750 東京都武蔵野市中町 2-9-32 (M53-2)
E-mail: †y-hagiwara@c4t.jp, ‡tspann@infogard.com, *Tatsuaki.Takebe@jp.yokogawa.com

あらまし 電子政府推奨暗号リストが策定された日本では，現在，米国およびカナダにならって，暗号モジュール評価制度 (CMVP)が検討されている．米国のCMVP及び独立行政法人情報処理推進機構から提案のあった移行制度を検討しつつ日本にとって望ましい方向性を提案する．

キーワード FIPS 140-2, CMVP, 認証機関，認定機関，試験機関，ベンダ

The Direction of Japan's CMVP II

Yuichi Hagiwara† Travis Spann‡ and Tatsuaki Takebe*

† C4 Technology, Inc., Consulting Department, R&D Division
Meguro Tokyu Bldg., 5th Floor, 2-13-17 Kamiosaki Shinagawa-ku, Tokyo 141-0021
‡ InfoGard Laboratories, Inc., FIPS 140-2 Evaluation Department
641 Higuera Street, Second Floor, San Luis Obispo, CA 93401
* Yokogawa Electric Corporation, Development Infrastructure Deptartment
2-9-32 (M53-2) Naka-cho, Musashino-shi, Tokyo 180-8750
E-mail: †y-hagiwara@c4t.jp, ‡tspann@infogard.com, *Tatsuaki.Takebe@jp.yokogawa.com

Abstract As Japan now has her own e-government recommended cipher list, is seeking the possibilities to have her own Cryptographic Module Validation Program (CMVP). We investigate the original CMVP established by National Institute of Standards and Technology (NIST) and Communications Security Establishment (CSE) as well as transition plans proposed by the Information-Technology Promotion Association Japan (IPA), and suggest the most beneficial directions.

Keyword FIPS 140-2, CMVP, Validation Authority, Accreditation Body, Testing Laboratory, Vendor

1. 背景

1.1. 日本の状況

総務省及び経済産業省は，2003年2月20日に電子政府の安全性及び信頼性を確保するために使用が推奨される暗号のリストを発表した[1]．また独立行政法人情報処理推進機構（以下，IPAと略す）はそれらの暗号を実装した暗号モジュールの安全性評価基準を作成することを表明している[2]．

暗号モジュール委員会は，暗号モジュール評価基準および試験基準を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，近年中に暗号モジュール評価基準及び試験基準を作成することを表明した．2004年3月には，その皮切りとして，FIPS 140-2[1]及びその試験基準（Derived Test Requirements：DTR[2]）の翻訳物を評価基準および試験基準の0版として発表した[3]．また，2005年3月には評価基準及び試験基準の0.1版を公表し，新たに実装ガイダンス

[1] CRYPTRECの報告について，
http://www.ipa.go.jp/security/enc/CRYPTREC/fy15/cryptrec20030604_press.html
[2] 2003年度暗号モジュール委員会活動について，
http://www.ipa.go.jp/security/enc/CRYPTREC/fy15/cryptrec20030801_modplan.html
[3] CRYPTREC Report 2003の公開，
http://www.ipa.go.jp/security/enc/CRYPTREC/fy15/cryptrec20040310_report01.html

(Implementation Guidance[3]) の 0 版も発表した[4].

IPA は暗号モジュールの評価基準及び試験基準を活用した暗号モジュール評価制度を立ち上げることも提案しており,そのスキームについての提案も 2005 年の 1 月に行った[4].

1.2. 海外の状況

暗号モジュール評価制度 (Cryptographic Module Validation Program : CMVP) は既に米国及びカナダが共同で実施しており[5], その評価基準である FIPS 140-2 は国際セキュリティ規格 ISO/IEC 19790[6]の最初のドラフトとして提案された. FIPS 140-2 は米国の規格であるため, 審議の過程で米国特有の連邦通信委員会の要件等が削除され, 使用可能なアルゴリズムに関しては米国独自のものから他の ISO 規格へと変更されている. ISO/IEC 19790 は,近年中の制定が目標とされており, 様々な国の暗号モジュール評価制度の基準となることが予想される.

英国の CESG[7] (Communications Electronic Security Group : 通信電子セキュリティグループ) も 2003 年に FIPS 140-2 及び CMVP を承認した. CESG は英国政府機関内での FIPS 140-2 適合認証取得済みモジュールの使用を推奨している.

2. 米国の状況

FIPS 140-2 の前身である FIPS 140-1[5]の制定及び CMVP の運用以前には暗号モジュールに対するセキュリティ要件の規定及び試験は NSA (National Security Agency :《米》国家安全保障局) によって行われていた[8]. NIST (National Institution of Standards and Technology :《米》国立標準技術研究所) と CSE (Communications Security Establishment :《加》通信安全保障機構) により, 1995 年 CMVP の運用が開始された. CMVP の目的は民生品の暗号モジュールを政府機関が機密ではないが重要な情報を保護するために利用して問題ないことをテストし, 認証することである.

暗号モジュールを評価することによる利点は次のとおりである.

- 暗号モジュールの設計全体の品質を高め, 暗号アルゴリズムの実装がセキュリティを考慮した設計となっていることの保証を高める
- ベンダは, 試験機関が設計を分析する際に必ず発見する脆弱性を製品の市場投入前に修正できるので, 製品がより安全になる
- ほとんどの場合においてソースコードの構造が再構成され, よりモジュール化したものとなる. 結果として, ベンダは各モジュールを再利用することが可能になり, リソースの節減及びプログラム上のバグが減少する
- 暗号モジュールの設計を第三者機関が分析することにより, セキュリティ及び機能面に対し第三者評価を行うことが可能になる

2.1. CMVP の構成要素

CMVP を健全に運用するためには 5 つの必要条件がある. それぞれ暗号モジュール評価基準及び関連する規格, ベンダ, 試験機関, 認定機関, 認証機関である.

2.1.1. 暗号モジュール評価基準及び関連する規格

暗号モジュール評価基準は CMVP の最も基本となる構成要素である. CMVP の場合, 評価基準は FIPS 140-2 である. FIPS 140-2 では 11 の分野に渡り 1 (最低) から 4 (最高) までのセキュリティレベルごとに要件が規定されている. 暗号モジュールは各分野に対してベンダの望むセキュリティレベルで評価され, 全体的なレベルとして最も低いレベルをその合格レベルと主張できる.

FIPS 140-2 の規格に適合していることを判定するテスト要件は DTR に記されている. 他にも FIPS 140-2 はアルゴリズム及び鍵管理に関し, 他の規格を参照している.

CAVP[9] (Cryptographic Algorithm Validation Program : 暗号アルゴリズム評価制度) では NIST が認定された試験機関に対し, アルゴリズムテストを行うためのツールを配布している.

2.1.2. ベンダ

ベンダは FIPS 140-2 の基準に適合する暗号モジュールを開発し, 基準を満たすことをドキュメントで主張する業者である. FIPS 140-2 では暗号モジュールは暗号機能を含むソフトウェア, ファームウェア, ハードウェア, もしくはその組み合わせとなり, 暗号モジュールを開発するベンダも様々となる. ソフトウェア暗号モジュールの例としては E メールの暗号プログラム, 暗号ライブラリ, データ暗号ソフト, セキュア通信プログラムが挙げられる. ハードウェア暗号モジュールの例としては VPN, シングルチップスマートカード,

---

[4] CRYPTREC Report 2004 の公開, http://www.ipa.go.jp/security/enc/CRYPTREC/fy16/cryptrec20050421_report01.html

[5] CMVP, http://csrc.nist.gov/cryptval/

[6] ISO/IEC 19790 Information technology – Security techniques – Security requirements for cryptographic modules

[7] CESG, http://www.cesg.gov.uk/site/iacs/index.cfm?menuSelected=5&displayPage=5

[8] Additional Cryptographic Module Lists, http://csrc.nist.gov/cryptval/140-1/1401val0.htm

[9] CAVP, http://csrc.nist.gov/cryptval/cavp.htm

シングルチップ暗号プロセッサ，無線機，PCI 暗号ボードが挙げられる．

2.1.3. 試験機関

ベンダの製品が FIPS 140-2 に準拠しているかを評価するのは認定された試験機関のみ[10]である．試験機関は信頼を受けた第三者機関であり，評価を行う暗号モジュールのいかなる設計にも携わってはならない．試験機関は暗号モジュール，ソースコード，FIPS 140-2 で規定される仕様設計ドキュメント等をベンダから受け取り，DTR の規定に従って評価する．

2.1.4. 認定機関

CMVP に対する認定機関は NVLAP[11]（National Voluntary Laboratory Accreditation Program：米国公認機関による試験機関認定プログラム）である．NVLAP により，暗号モジュールを評価する試験機関が認定される．NVLAP は試験機関に対し ISO/IEC 17025[12], NIST Handbook 150[6]および NIST Handbook 150-17[7]への適合性を審査する．

認定機関は試験機関を毎年審査する．また，現地での監査及び審査を隔年で行う．

2.1.5. 認証機関

認証機関は試験機関が作成したテスト報告書及びベンダが作成した暗号モジュールのセキュリティポリシーを精査し，その製品が評価基準，FIPS 140-2 に適合しているかを判定する．暗号モジュールおよび評価結果に関して生ずる全ての質問は試験機関に向けられ，ベンダにフォローが生ずることもある．

認証プロセスが終了した際には CMVP は適合を認める NIST 及び CSE の代表者によって署名される証明書を発行する．

2.2. CMVP の問題点

現在米国及びカナダが共同で行っている CMVP には多少の問題点が存在する．

2.2.1. 長大な待ち時間

評価候補の暗号モジュール，評価を行う試験機関の増加は CMVP における人材の増加を遙かに上回った．結果として，一時は CMVP に対して認証を要求されるモジュールは評価を開始されるまで 6 ヶ月以上の時間を要し，認証製品としての市場投入のタイミングを図ることが難しかった．2005 年 6 月現在の待ち時間は 3 ヶ月となっており，CMVP の人材も増加傾向にあるため将来的には 6 週間以下になることが見込まれている．

2.2.2. 統一感のないセキュリティポリシー

セキュリティポリシーは暗号モジュールが安全であることを FIPS 140-2 の評価要件に従って表明するドキュメントであり，ベンダに公表が義務付けられた唯一の非機密ドキュメントである．購入者はセキュリティポリシーをその製品が必要なセキュリティ要件を満たしているかを判断する材料の 1 つとして利用する．また，ユーザはセキュリティポリシーをモジュールの安全な利用を確証するために利用する．このため，セキュリティポリシーは重要なドキュメントであるが，CMVP によって標準様式による記述が義務付けられておらず，多様な書式，様々な表記レベルが許可されている．そのため，ユーザが正しい判断を行うためには毎回セキュリティポリシーを熟読しなければならず，その労力は膨大である．ベンダがプロプライエタリな情報を隠蔽するため，時としてベンダの作成するセキュリティポリシーは曖昧になり，誤解されやすい表記になってしまうこともある．

2.2.3. 評価基準の解釈論

評価基準である FIPS 140-2 は大変抽象的に要件を説明しているが，それらはあらゆる形態の暗号モジュール及び技術に適用されなければならない．認証機関である CMVP は規格の解釈に対して公式な見解を表明する責任を持つ．一時期，規格の解釈は頻繁にケースバイケースベースで行われ，その解釈を要求した試験機関にのみ非公式に行われた．その結果，異なる試験機関に対し異なる解釈が説明される事態が生じた．これにより，異なる試験機関から異なる解釈を説明され混乱と矛盾を感じたベンダも多数あった．この事態に対し，CMVP より，限られた数の解釈及び公式な見解が実装ガイダンスを通して各試験機関に表明された．

近年では CMVP はベンダの機密情報を開示しない場合において，試験機関に対する公式な見解を各試験機関に同時に表明するポリシーを採用した．また，試験機関が CMVP に対して規格の解釈を要求する質問をしたとき，その試験機関は同時に他の試験機関全てに対してもコメントを要求することが推奨されている．他にも規格の解釈は試験機関同士の会議において随時行われている．この結果，試験機関の中で規格に対する理解が深まった．最終的にはベンダは全ての認定された試験機関から同じ見解を得られなければならない．

3. 日本における暗号モジュール評価制度

2005 年 1 月に IPA は暗号モジュール評価制度を提案しており，完全な段階及びそれまでの移行制度も提案した．完全な段階では米国のものをならっているが，移行制度に関しては独自のものである．本章では提案された 2 つの移行制度について検討する．

---

[10] CMT Laboratories, http://csrc.nist.gov/cryptval/1401labs.htm

[11] NVLAP, http://ts.nist.gov/ts/htdocs/210/214/214.htm

[12] ISO/IEC 17025, General Requirements for the Competence of Calibration and Testing Laboratories

3.1. 自主評価方式

自主評価方式とは，ベンダの品質管理部門が試験機関に代わりテストを行い，そのテスト報告書に対し認証機関が適合認証の判断を行う．

3.1.1. 自主評価方式の問題点

自主評価方式の問題点は4つあるとIPAは指摘している．

- ベンダ間で評価レベルに差が生じる
- 評価結果の中立性が確保できない
- 国際相互認証制度を導入した際に制度の再構築が必要である
- 中小ベンダ向けには独立の試験機関が必要

我々は新たに2つの問題点を提起する．

- ベンダが主張する自称準拠は信頼性に欠ける：
  IPAが指摘する様に評価レベルの差は起こるが，それより深刻なのは評価自体の信憑性である．米国のCMVPでも初期段階において試験機関を設立する際に，米国政府機関はFIPS 140-1にベンダが準拠していると主張する暗号モジュールを1996年の1月31日まで購入することが可能であったが[13]，現在は，その様なモジュールの購入を禁止した．更に，評価制度を運用してきた過去のデータの反省，すなわち評価で，25%以上のアルゴリズムに欠陥が発見され，50%近くのモジュールには欠陥が発見され，95%以上のモジュールにドキュメントの不備が発見された事実[8]を鑑みると，自称準拠を容認することは難しい．上述の50%は新規に認証を要求したモジュールの他に，既に認証を取得しているモジュールに対する変更を含んでおり，実際，提出された全てのモジュールに対して何らかの不適合が発見された．
- ユーザにとってのメリットが存在しない：
  認証制度で合格していないのにFIPS 140-2レベルX相当と宣伝を行っている製品が既に多数ある．新たに自主評価方式で仮に適合判定を下された製品であっても評価結果の中立性は確保できず，ユーザにとっての利益とはなりにくい．これは，IPAが指摘する通りである．さらに，ベンダ独自による要件の解釈は誤った統一感の無いものになると先述の米国のCMVPのデータから予測され，その自主評価結果を読み解いてユーザが正しい製品の比較を行うことはまず不可能である．

3.2. 認証機関併設方式

認証機関併設方式とは認証機関の一部として試験機関を併設して試験を行う方式である．自主評価方式で問題となる中立な評価が行えると共に，将来の試験機関での試験要員の教育を実施できるメリットがあるとされる．

3.2.1. 認証機関併設方式の問題点

認証機関併設方式の問題点は1つあるとIPAは指摘している．

- 競争原理が働かないため評価コストが高止まりとなる可能性がある．

我々は新たに2つの問題点を提起する．

- 認証機関と試験機関が同一のため，生じる問題：
  認証機関と試験機関が同一のため，評価の問題指摘が厳正に行える保証が十分でない．
- 試験機関が潜在的に持つ問題：
  認証機関の形態によっては他企業からの出向研究員を認める場合が考えられる．試験機関が認証機関の一部であるのならば，その研究員が他企業のソースコードを入手する可能性は否定できず，ベンダにとっては大きな懸念材料となる．

4. 理想的な暗号モジュール評価制度

2章及び3章にて問題点を提起したが，本章では理想的な暗号モジュール評価制度の要素を説明する．

4.1. 教育された人材

暗号モジュール評価制度において最も重要なのは人材の確保である．試験者は評価基準及び試験方法を熟知していなければならず，認証者は試験者の報告書を理解するに足りる知識を持たなければならない．さらに試験者は評価基準をベンダに的確に説明できなければならない．

4.2. 認定機関

CMVPには暗号モジュールの評価を行う試験機関に対する認定を行う独立した認定機関が必要である．認定機関はISO/IEC 17025等で定義されている品質機構に基づく監査を行えるのであれば認証機関と同一でも良い．

4.3. 独立した関係

ベンダ，試験機関，認定機関，認証機関はそれぞれ独立していなければならず，試験機関は製品の設計に携わってはならない．

試験機関は厳正な試験を行うためにベンダと利益を共有してはならない．また，認証機関は試験機関の報告書を精査し，試験機関に見落としがなかったか，正しく評価できているかを慎重に判断しなければならない．他にも，ベンダは暗号モジュールのコンサルティングを行う試験機関を利用する際には知的財産が流

[13] Additional Cryptographic Module Lists, http://csrc.nist.gov/cryptval/140-1/1401val0.htm

用されない可能性を否定できないため，細心の注意を払わなければならない．ベンダが他社，すなわち試験機関に全てのソースコードを渡したのに知的財産が流出しない可能性が無いとは言えないからである．

4.4. ツールの使用

米国のCMVPではアルゴリズムの試験を効率的に行うためにツールを使用している．このツールに依存することにより，アルゴリズムの実装を試験する場合にも試験者がソースを全て追いかける必要はなくなり，試験者の負担が大幅に減る．

4.5. 需要の確保

ベンダにとって暗号モジュールの認証を取得することが魅力的でなければ，ベンダにとっては負担でしかないため暗号モジュール評価制度は計画倒れとなってしまう．そのため，認証を受けた暗号モジュールに対する需要が無ければならない．米国では認証を取得することが政府調達の際の必須要件と法律で定まっているため，ベンダにとって大きな動機付けとなっている．必須要件とはならずとも認証を取得することによって明確な差別化を図ることが可能になるのならばベンダにとって大きな魅力となりうる．

5. 日本の暗号モジュール評価制度に対する提案

各章の内容を踏まえた上で，日本の暗号モジュール評価制度に対する提案をこの章で行う．

5.1. 米国のCMVPを踏まえての提案

2章で言及した米国のCMVPの問題を踏まえての改善策を提案する．

5.1.1. 待ち行列の解消

認証されるまでの待ち時間はベンダにとっては懸念材料である．開発に3ヶ月，試験に3ヶ月かかったとしても，認証機関にレビューされるまでに5ヶ月待っていては認証されるまでに合計で1年かかってしまい，その間に市場に投入される競合他社及び自社の新製品との差別化が難しくなる．

日本の暗号モジュール評価制度はテスト報告書を適時，審査し，時宜にかなった認証サービスを提供しなければならない．そのためには，政府機関による財政的及び戦略的支援が必要であり，ベンダに対する適切な費用請求も含まれる．

特に作業によっては，暗号モジュールに対して高度な専門的技術がそれほど要求されないものもあるので，その様な作業を通して人材を教育することが可能である．

5.1.2. テンプレートの提示

特に公開されるセキュリティポリシーに関してはテンプレートを作成し，提示することにより一定の精度を確保することが可能となる．ユーザ・認証機関ともに毎回ベンダ独自のセキュリティポリシーを熟読する必要はなくなり，負担が減ることが予想される．

5.1.3. 解釈問題に対する対応

米国のCMVPでは多くの解釈問題がケースバイケースで対処され，プロジェクトによりその解釈が異なることがある．ケースバイケースの判断を認証機関が行った際には，判断基準を含め公表し，今後各ベンダはその判断を基準にすることを認める．各ベンダは認証機関の判断基準及び根拠を理解することができるために，今後の実装について検討することが可能になり，試験機関はその実装が問題ないかを公表された内容に基づいて判断することが可能になる．更に，認証機関はケースバイケースの対応を迫られることが少なくなるために判定に要する時間が少なくなる．

ただし，ベンダの機密情報に触れる危険性があると試験機関及び認証機関が判断したもの，ベンダが公表したくないと表明したものについては除外する．

5.1.4. 既存の試験機関の受け入れ

既に米国のCMVPで認可され，活動している試験機関に対しても，米国に拠点を置きながら日本の暗号モジュール評価制度に参入することを受け入れることにより，彼らの経験を様々な問題を解決することに使うことが可能になる．また，初期段階からもベンダ，試験機関，認証機関の独立した関係を築くことが可能になる．

この受け入れ制度により，既存の試験機関の顧客は，日本のCMVPとの偏差分の評価および，セキュリティポリシーと試験報告書の翻訳作業という少ない負担のみで，日本でのCMVP認証を得ることができ，日本市場に参入できるので，日本の暗号モジュール評価制度で認証を取得することを魅力と受け止め，日本のCMVPに参加することが予想される．これは，制度を盛り上げる材料となる．

既存の試験機関に対しては3つの役割を割り当てる．

- 暗号モジュールを試験すること
- 試験機関に対しての教育
- 認証機関に対しての支援

5.1.4.1. 既存試験機関による暗号モジュールに対する試験

既存試験機関により暗号モジュールに対する試験が行われるのならば，米国のCMVPに参加しているベンダにとって，日本のCMVPに参加する敷居が低くなることを意味する．健全なCMVPを運用するためには，国内のベンダだけではなく，海外のベンダも参加することが必要である．

5.1.4.2. 試験機関に対する教育

試験機関が問題に当たった際に，解決策を提供することが可能なのは米国のCMVPで経験をつんだ既存の試験機関のみである．既存の試験機関からの教育，サポートを受け，日本の試験機関は円滑に暗号モジュールの試験が可能になる．

5.1.4.3. 認証機関に対する支援

認証機関は試験機関の報告書に基づき判断を行うが，報告書に関する十分な知識，及び実際にどの様な試験がどの様な基準で行われているかを知らなければならない．

また，試験機関が行っている試験内容に関して問題が無いかの判断を仰ぐことも可能になり，より厳正な判断を行うことが可能になる．試験機関の試験品質を確かなものにするために，試験機関の認定基準及び試験結果の認証に対し多大な労力が尽くされることであろう．認定機関は下記の項目を含む試験機関の試験品質，技術，独立性を確証する制度を運用しなければならない．

- 試験機関が適切な技術を所有していることを確証するためのプロセス
- 試験機関が独立性と信頼の両方を備える価値観とビジネスモデルを所有していることを確証するためのプロセス
- 認定機関が十分な技術，知識を持った機関のみを試験機関として認定する制度
- 認定機関が品質，技術，独立性を維持できない試験機関を排除する制度
- ベンダの知的財産を保護する制度

これらの要件を迅速に認証機関が満たすようになるため支援が必要となる．これを米国の認証機関に求めることも可能かもしれないが，3 つの理由により難しいと予想される．

- 政府機関の一員として，NIST は利益を得ることを禁止されているため，日本の認証機関に対しての教育で損益が生じないよう，しかし，同時に利益を計上するという禁止条項に抵触せぬよう，トレーニングの課金制度を決めることが極めて難しい
- 先述した通り，米国の認証機関の人員不足により，FIPS 140-2 認証プロセスは多くの時間を要するものとなってしまった．米国の認証機関は日本の認証機関を支援する前にこの問題に対応しなければならない

5.2. テストツールの開発

テストツールを開発することは 2 つの点から望ましいと考えられる．

- 迅速な試験の実施
- 一定レベルの保証

テストツールでは暗号モジュールのセキュリティレベル及び形態により適用される試験項目が自動で生成され，テスト漏れを防ぐことが可能になり，また適用される試験項目が明瞭となる．

5.2.1. 迅速な試験の実施

特にアルゴリズムの試験を迅速に行うためには試験機関がテストツールを使用することが望ましい．これにより，数学・コンピュータ言語に精通していない試験者もアルゴリズムの試験を行うことが可能になる．

また，アルゴリズムの試験を行うためのツールは可能であるのならばソースコードを公開することが望まれる．データの取り扱い方の問題で本来ならば準拠しているモジュールが不合格となってしまい，解決までにかなりの期間を要することが米国のCMVPでは少なくないからである．

5.2.2. 一定レベルの保証

試験機関が報告書を作成する際にもテストツールを使用することにより，各項目を漏らすことなく試験したことを確認することが可能になり，認証機関は試験漏れを疑う必要がなくなる．

さらに，各試験機関が試験項目を共有するため，評価に対して一貫性を保証することが可能になる．

5.3. 暗号モジュールテスト要件の再構築

ハードウェアに焦点を当てた要件をソフトウェアのみで構成されたモジュールに適用しようとする際には，様々な混乱が生じる．細心の注意を持ってソフトウェアのみで構成された暗号モジュールに対する評価基準の再構築を行わなければならない．他にも追加のガイダンスでソフトウェア暗号モジュールが適切で十分な場面（ネットワーク環境に接続されず，警備員と監視カメラによって守られている金庫室等での運用）やハードウェア暗号モジュールによってしか適切なセキュリティを確保できない場面（暗号モジュールが悪意のある攻撃者のいる環境に置かれ，攻撃者が装置に対して物理的な攻撃が可能な場面等）でのテスト要件の違いを明確にすべきである．

6. 結論

本稿では既に米国で運用されているCMVP及びIPAから提案のあった移行制度の検討を基に更なる向上のための提案を記した．暗号は普段気づかないものに対しても組み込まれており，使用を誤ると国民の生活が脅かされることにも繋がる．また，一度製品が「認証」された，もしくは「安全」であるとみなされると，ユーザの態度が変わり，結果として製品説明書で規定される適切な運用環境から外れた，正常動作を保証されない運用環境で使用されてしまうこともあるため，認

証の判断は慎重に行われなければならない．セキュリティポリシーから正しい使用法が読み取れ，誤使用が予防され，意識せずとも正しく暗号モジュールが使用されるよう，日本の評価制度の今後に期待したい．

今後，健全な暗号モジュール評価制度の普及，促進を目指す上で本稿が参考となれば幸いである．

文　献

[1] National Institute of Standards and Technology, Security Requirements for Cryptographic Modules. FIPS 140-2, 25 May, 2001

[2] National Institute of Standards and Technology, Derived Test Requirements for FIPS PUB 140-2, Security Requirements for Cryptographic Modules, 24 March, 2004

[3] National Institute of Standards and Technology, Communications Security Establishment, Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program, 21 January, 2005

[4] 山岸篤弘，網島和博，近藤潤一，大熊建司，西原正人，“わが国における暗号モジュール評価制度について”，SCIS 2005, 2B4-1, 2005 年 1 月 26 日

[5] National Institute of Standards and Technology, Security Requirements for Cryptographic Modules. FIPS 140-1, 11 January, 1994

[6] National Institute of Standards and Technology, NIST Handbook 150:2001, NVLAP Procedures and General Requirements, July, 2001

[7] National Institute of Standards and Technology, NIST Handbook 150-17 Information Technology Security Testing - Cryptographic Module Testing, June, 2000

[8] National Institute of Standards and Technology, Communications Security Establishment, Frequently Asked Questions for the Cryptographic Module Validation Program, 20 May, 2005