JCMVPに関するユーザ向けガイドライン試作

楊 鵬 * 松浦 幹太 *

概 要

暗号モジュール試験及び認証制度による認証は暗号モジュールの中に推奨されている暗号アルゴリズムが適切に実装され，鍵等の重要情報のセキュリティが確保されたことが保証できる．本論文では，暗号モジュール試験及び認証制度のユーザ向けガイドラインの必要性を説明し，ガイドライン試作の方針について報告する．

1 はじめに

現在，企業や個人にとって情報セキュリティは死活問題につながる大きなポイントになっている．情報セキュリティ対策としてITセキュリティ評価及び認証制度（JISEC）が広範に利用されているが，その場合暗号アルゴリズム実装評価を行う場合，ソースコードチェックにより行われることになる．これに対して，暗号アルゴリズムに関する高い専門知識と豊富な業務経験が要求される．そこで，JISECの補完制度として，暗号モジュール試験及び認証制度（JCMVP）は暗号アルゴリズムが適正に実装されていることを保証する制度[1]が登場している．

具体的に，暗号モジュールとは承認されたセキュリティ機能を実装した，暗号境界内のハードウェア，ソフトウェア又はファームウェアの集合である．JCMVPとは，暗号モジュールに実装されたセキュリティ機能が正しく実装されていることを確認する共に，鍵やID，パスワード等の重要情報のセキュリティを確保する第三者評価制度であり，2006年6月より試行運用がIPAにより開始された．更に，JCMVP認証の取得によって，認可されていない暗号モジュールの利用，内容の開示，変更を防止ができ，承認されて動作モードで動作する時，その暗号モジュールが適切に動作することが保証でき，またエラーを検出した場合，秘密情報の危殆化を防止することができる．

視野を広げると，米国とカナダにJCMVPと同等な制度が存在する．それはCryptographic Module Validation Program（CMVP）という．但し，CMVPでは暗号モジュールセキュリティ要求事項としてFIPS 140-2 [2]を採用されており，JCMVPでは要求事項としてFIPS 140-2をベースにして作成されたISO/IEC 19790の国際一致規格であるJIS X 19790を採用されている．特に，CMVPでは承認されたセキュリティ機能はFIPS 140-2のAnnex Aで規定されており，JCMVPでは承認された暗号アルゴリズムはCRYPTRECの作成した電子政府推奨暗号リストからJCMVP技術審議委員会の審議を経て決定されている．

2 ユーザ向けガイドラインの必要性

情報セキュリティ認証制度が数多に存在する．それぞれのオーディエンス群は異なり，各オーディエンスが果たす役割も違うのが言うまでもない．JISECの場合，ベンダー向けのガイドラインとユーザ向けのガイドラインが，両方ともIPAのホームページから入手できる．一方，JCMVPのベンダー向けのガイドラインはIPAのホームページに公開されているが，ユーザ向けのガイドラインは存在しない．（内閣官房情報セキュリティセンターが発表した統一基準の中に強化遵守事項が記載されているが，これはガイドラインに該当しないと筆者は考える．）こういう場面になった理由の一つとして，JISECの認証プロセスの中でユーザは協力を求められる反面，JCMVPの場合ユーザは認証取得済みの製品を購入・使用すること以外，認証プロセスに参加する必要がないからだと考えられる．

しかしながら，JCMVPを政府機関のみならず，民間企業や大学，NPOなどにも普及させるためには，ユーザ向けのガイドラインが必要であろう．

*東京大学生産技術研究所 〒153-8505 東京都目黒区駒場4-6-1 {pengyang,kanta}@iis.u-tokyo.ac.jp

JCMVP認証製品を導入することによって，ユーザが如何なる情報セキュリティ機能を確保できるか，こういうような安心感をユーザに与えるのは非常に重要である．実際に，CMVPなどの認証制度を推進する文書[3]が米国商務省所管の国家機関NISTにより公開されている．

3 試作方針

試作対象のJCMVPのユーザ向けガイドラインの中に，JCMVPの概要や認証製品の導入プロセスなどの基本情報をユーザに周知させること以外，JCMVPとCMVPの間の相互認証見込みも含める予定がある．

更に，JCMVPとJISECの相互補完性を紹介する．何故ならば，JCMVPはあくまでも暗号モジュールの安全性しか保証できず，システム全体のセキュリティ要望に沿うため，ユーザにとってJCMVPのみならの製品選定に穏当を欠き，JISECも含めた意思決定をとったほうが良策になる．

また，情報セキュリティ製品の認証制度を民間の企業や団体などに推進しようとするのであれば，制度の導入方法を説明する前に，制度の導入によるセキュリティ向上効果を明確にすることが先決だ．特に，現在情報システム投資にあたる予算が削減されつつある環境において，認証を受けた情報セキュリティ製品の導入は一見コストアップになってしまうようだが，実際，ユーザにとって投資戦略が想定通りに機能するのに決定的な役割を果たすとも言えるでよう．

例えば，カナダの国家暗号エージェンシCSEの統計結果によると，2009年にCMVP試験を受けた製品の中で，セキュリティ機能不備などの不具合率は54%にも及んだ．いわば，セキュリティ製品全体の中に，驚くべき高確率で暗号モジュールの不具合率が示唆される．もしこのような環境で製品を導入すれば，実装バッグによる実害に結びつく確率が高まり，その結果，ユーザがシステム脆弱性アセスメントをした上で定めた投資戦略の指向性が変更し，想定範囲外に変移してしまう可能性も十分考えられる．この論点は，2008年に松浦[4, 5]によって提案された情報セキュリティ投資の理論モデルに支持されている．松浦の理論では，情報セキュリティの生産性空間について分析を行い，情報セキュリティの生産性の定量的な変動により最適投資戦略の定性的な改変が可能であることを提唱している．

4 むすび

情報セキュリティの認証制度は多数存在するが，ユーザ向けのガイドラインが少ない．本稿では，暗号モジュール試験及び認証制度のユーザ向けガイドラインの必要性を述べ，ガイドラインを開発する方針について紹介した．本ガイドラインによって，ユーザが情報システム投資を厳選する際に，JCMVP準拠製品の取捨選択をするための意思決定への助言が得られる．特に，関連統計データと情報セキュリティ投資理論モデル両方に基づいて，ユーザに有益なアドバイスを与えることが期待されている．

本ガイドラインは2010年3月末までに公開を予定する．公開後，JCMVPを運営しているIPAに引用される予定がある．

謝辞

本研究は，NEDO産業技術研究助成事業（若手グラント「産業技術に関する社会科学分野」）の援助を受けた．

参考文献

[1] A. Yamagishi, K. Matsuura, and H. Imai. Cryptographic module validation program in japan. In *Engineering Management Conference '05*, pp. 485–489. IEEE, 2005.

[2] NIST. NIST FIPS PUB 140-2, 2001. Security Requirements for Cryptographic Modules.

[3] NIST. NIST special publication 800-36, 2003. Guide to Selecting Information Technology Security Products.

[4] K. Matsuura. Productivity space of information security in an extension of the Gordon-Loeb's investment model. In *2008 Workshop on the Economics of Information Security*, 2008.

[5] K. Matsuura. Productivity space of information security in an extension of the Gordon-Loeb's investment model. In *Managing Information Risk and the Economics of Security*, pp. 99–119. Springer, 2009.