Information-technology
Promotion
Agency, Japan

プレスリリース
2012 年 2 月 27 日
独立行政法人情報処理推進機構

IPA と米国 NIST、暗号モジュール試験及び認証制度の共同認証で合意

IPA（独立行政法人情報処理推進機構、理事長：藤江 一正）と米国 NIST（National Institute of Standards and Technology、国立標準技術研究所）は、それぞれの機関で実施している暗号モジュール試験及び認証制度について、両制度間で共同認証を行うことの基本的な合意に達しました。

暗号技術を利用した情報セキュリティ製品やシステムの安全性を確保するためには、暗号アルゴリズム（暗号化をするための手順）をハードウェア、ソフトウェア等で実現している暗号モジュール(*1)の安全性の確保が特に重要となります。

北米では、暗号モジュールに暗号アルゴリズムが正しく実装されていることを確認するとともに、暗号鍵、ID、パスワード等の重要情報の安全性が確保されていることを認証する制度として、CMVP（Cryptographic Module Validation Program）を米国NISTとカナダCSEC(*2)が認証機関として 1995 年 7 月から運営しています。また、日本においても、IPAが認証機関として同等の制度である「暗号モジュール試験及び認証制度」(JCMVP: Japan Cryptographic Module Validation Program)を、2007 年 4 月から運営しています。

このCMVPとJCMVPは独立した制度であり、認証対象の暗号アルゴリズムリストには差異がありますが、今回の合意によって、両者の共通部分については共同認証(*3)を適用することが可能になります。共同認証の流れについては、別紙を参照ください。

共同認証を適用することによって、日本国内の暗号モジュールのベンダーは、JCMVP に認証申請することで CMVP 認証も取得することが可能になります。米国では CMVP 認証取得が連邦政府調達の必須要件になっており、民間においても事実上の標準となっていることから、米国市場での競争力の向上が期待できます。

また、CMVP で認証された暗号モジュールが JCMVP の認証製品リストに載ることにより、日本国内の暗号モジュールのユーザーは、安心して使用できる暗号モジュールを調達しやすくなります。

IPA では、2012 年度上期中に、共同認証の運用を開始する予定です。

なお、本件については、3 月 12 日（月）に IPA で開催する「暗号モジュール試験及び認証制度の説明会」においても説明を行う予定です。

■本件に関するお問い合わせ先
IPA　技術本部　セキュリティセンター 情報セキュリティ認証室　近藤／櫻井
Tel: 03-5978-7545　Fax: 03-5978-7548　E-mail: jcmvp-info@ipa.go.jp
■報道関係からのお問い合わせ先
IPA　戦略企画部　広報グループ　横山／大海
Tel: 03-5978-7503　Fax: 03-5978-7510　E-mail: pr-inq@ipa.go.jp

(*1) 暗号モジュール: 暗号アルゴリズムをハードウェア、ソフトウェアで実現しているもの。暗号モジュールには IC カード、暗号化ルーター、暗号化ストレージ等があり、機密データの保護や電子署名等の機能を実現しています。

(*2) CSEC: Communications Security Establishment Canada. CMVP を NIST と共同で運営しているカナダの政府機関。

(*3) 共同認証とは、JCMVP あるいは CMVP のいずれか一方に認証申請を行い、暗号モジュール試験を受け、同一の試験報告書に基づいて、両制度の認証機関による共同レビューを受けた上で両制度から認証を受けることを意味します。共同レビューとは、両制度の認証機関が、暗号モジュール試験の試験報告書を共同でレビューすることを意味します。