IPA Technical Watch

2011 年 5 月 11 日
独立行政法人情報処理推進機構

IPA テクニカルウォッチ：『暗号をめぐる最近の話題』に関するレポート
～　SSL/TLS や暗号世代交代に関連する話題から　～

IPA（独立行政法人情報処理推進機構、理事長：藤江 一正）は、最近 SSL/TLS [*1] プロトコル等、一般ユーザーにも少なからず影響を与えるような、暗号に関する事故・事象が複数連続して発生していることを受け、関係者および一般ユーザーに対して注意を促すため、「暗号をめぐる最近の話題」と題して取りまとめ、技術レポート（IPA テクニカルウォッチ第 2 回）として公開しました。

オンラインショッピング、インターネットバンキング、ネットトレード等のサービスでは、送信する情報を暗号化するため、および接続先の Web サーバが正当なものであるか確認するため、SSL/TLS プロトコルが利用されています。そして、そのようなサイトの「セキュリティ」の項目をみると、ほぼ例外なく「お客様の情報を守るために“SSL という暗号化技術”を採用」といった記載がされています。しかし、その SSL/TLS プロトコルに関する事故が最近複数発生しており、一般ユーザーが被害を受ける恐れがあったことが判明しました。

報道によれば個人情報が悪用されるなどの深刻な被害には至っていないようですが、IPA ではこれらの事故について深刻な事案と捉え、特に「Comodo 社による不正 SSL サーバ証明書 [*2] 発行」と「大手百貨店の Web サーバ設定ミス」について、公開されている情報から事故内容を分析し、事故からくみ取るべき教訓や対処法について取りまとめました。これには、認証局 [*3]、Web サイト構築者、Web サイト運営者はもとより、一般ユーザーに対しての注意喚起を含んでいます。

また、暗号世代交代（暗号アルゴリズムの 2010 年問題）についての話題も、節目であった 2010 年が過ぎ、米国で新たな動きが見られました。本レポートでは、「改訂された暗号アルゴリズム移行方針 SP800-131A」と「新たな米国政府標準ハッシュ関数策定（SHA-3 コンペや DRAFT FIPS 180-4）」に関する最新情報についても取りまとめました。

■ 本件に関するお問い合わせ先
IPA セキュリティセンター　神田／近澤
Tel: 03-5978-7550 Fax: 03-5978-7518 E-mail: isec-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] SSL/TLS：Secure Socket Layer/Transport Layer Security。 データの暗号化などを行い、インターネットを介して Web サイト（Web サーバ側）とブラウザ（クライアント側）間で安全な通信を行うための通信手順。
[*2] SSL サーバ証明書：SSL/TLS プロトコルで接続される Web サーバの身元や当該サーバが利用する公開鍵情報等が正当であることを保証するために認証局が発行する証明書。
[*3] 認証局：Web サーバの身元や当該サーバが利用する公開鍵情報等が正当であるかを審査し、SSL サーバ証明書を発行する業務を行う、信頼できる第三者機関。