先端技術キーワード解説

知っておきたい最新の動き

[TLS（Transport Layer Security）]

インターネットでの通信の安全に関して、よく目にした用語が SSL（Secure Sockets Layer）です。ホームページを閲覧したときなど、よく、「本ページは SSL で暗号化されています。」などというメッセージを見ることがありました。その SSL が突然、2015 年、使用禁止となりました。一体、何があったのでしょうか。

インターネットなどの TCP/IP ネットワークは、そもそも、安全性が保証されていません。このため、常に、通信の盗聴やなりすまし、改ざんといった危険があります。これに対して、通信データを守る必要があります。

そこで、最初に現れたのが、これまでよく目にした SSL です。SSL はトランスポート層のプロトコルで、TCP の代替として利用できます。このため、HTTP （Hypertext Transfer Protocol）に限らず様々な上位層のプロトコルと組み合わせて使用することができます。なお、SSL を利用した HTTP は、HTTPS と言います。URL は、「https://」で始まります。（よく見かける URL です。）

SSL 自体は、1994 年、ネットエスケープ社により開発されました。その後、1995 年、脆弱性の確保、機能アップなどを行った SSL3.0 が、ネットエスケープ社のプロダクトに実装されたことをきっかけに、事実上の標準となりました。

ところが、2014 年 10 月、重大なことが発覚します。SSL3.0 に、極めて危険な「POODLE （Padding Oracle On Downgraded Legacy Encryption）」という脆弱性があることがわかりました。

これは、簡単に言うと、まず、暗号文を傍受します。次に、傍受した暗号文の一部を改変してサーバーに送信します。これに対して、Web サーバーはそれぞれに特有の反応をします。これらの多数の送信を繰り返しながら、この反応を分析すると暗号文の内容を推測できることがわかったのです。（ただし、今のところ、攻撃の事実は報告されておりません。）

これに驚いた IETF（Internet Engineering Task Force：インターネットの標準化を進めている団体）は、2015 年 6 月、SSL 3.0 の使用を禁止しました。

それでは、「POODLE」への対策はどうすればよいかが大きな問題となります。基本は、脆弱なバージョンの SSL3.0 を無効化することとされています。（意外なことでした。）

実は、SSL3.0 が事実上の標準となった後、1999 年から IETF が、改めて SSL3.0 をベースに、TLS（Transport Layer Security）として、標準化作業を始めました。このため、初期バージョンである TLS1.0 は SSL3.0 と仕組みは、ほぼ同じです。（このため、SSL/TLS という表現もあります。）

その後、TLS は、改良を重ね、TLS1.1. TLS1.2、TLS1.3 とバージョンアップがされました。このため、いつの間にか、SSL3.0 が取り残されたようになってしまったのです。

現在、TLS の最新バージョンであれば、脆弱性への対処が可能とされています。つまり、対策としては、脆弱なバージョンである SSL3.0 を無効化し、TLS の最新バージョンへのアップグレードを行うことです。（すでに、主要な Web プラウザである Chrome、Firefox、Internet Explorer（IE）の最新版では、SSL3.0

は初期設定で無効になっています。）

インターネットにおける安全な通信手段と言えば、SSL でした。それが、これからは、TLS に入れ替わります。ただ、その交代劇の裏側には、標準化を巡る複雑な事情がありました。

（注）
本解説は、執筆当時の状況に基づいて解説をしております。ご覧になる時には、状況が変わっている可能性がありますので、ご注意をお願いします。

技術・経営の戦略研究・トータルサポータ
ティー・エム研究所
工学博士
中小企業診断士
社会保険労務士（登録予定）
代表　芳賀　知
E-Mail：info_tm-lab@mbn.nifty.com　URL：http://tm-lab@a.la9.jp/