予習・復習 IT用語

このコーナーでは、最新のものから昔から耳にしているものまで、IT関連用語を新旧取り混ぜてご紹介します。

Q 暗号の2010年問題

A 携帯電話やインターネットを安全に使うために必要な暗号化方式の世代交代

私たちが普段なにげなく利用している携帯電話やネットショッピング。通話内容やカード番号をほかの人に盗み聞きされないようにするために暗号化技術が使われています。今回は、身近なところでも使われている暗号化方式の世代交代のお話です。

暗号化とは、第三者に盗聴や改ざんされないように、決まった規則（鍵と暗号化アルゴリズム）に従って元の情報（平文）を暗号文に変換することです。解読されにくさ（強度）は、鍵の長さと暗号化アルゴリズムの複雑さで決まります。

一方、暗号の解読に使われるコンピュータの処理速度は、15年間で10倍になるといわれています。それにあわせて、暗号化方式もより解読されにくいものに世代交代させる必要があります。

米国国立標準技術研究所（NIST）は、2010年末をつぎの世代交代時期としています（前回は2002年）。国内においては、内閣官房情報セキュリティセンター（NISC）が、政府機関の情報システムにおいて、2013年度までは従来の暗号化アルゴリズムを継続して使用し、2014年度から順次切り替えるとの方針を打ち出しています。

この世代交代をいかにスムーズに行うかが「暗号の2010年問題」です。

新しい暗号化方式を導入するためには、ハードウェアやソフトウェアを新方式に対応させなければなりません。一部の携帯電話は、新方式に対応しておらず、買い替えてもらう必要があります。また、ブラウザやウェブサイトを新方式に対応させる必要があります。

対応が必要なモノが、多くの人や社会インフラにゆきわたっています。新旧の方式を使い続けることにより得られる相互運用性と、新方式にスパッと切り替えることにより得られる安全性とを考慮しながら移行する必要があります。このことが暗号化方式の世代交代の困難さを増しています。

Q Linux（リナックス）

A フリーに利用できるUNIXライクなオペレーティングシステム

Linuxは、オープンソースソフトウェア（OSS）として開発が進められているUNIXライクなオペレーティングシステム（OS）です。OSSとしてソースコードが無償で公開され、誰でも自由に改変、再配布が行えます。本来はOSの核であるカーネルを指しますが、OS関連ソフトウェアと組み合わせたディストリビューションを指す場合もあります。

Linuxは、フィンランドの大学院生 Linus Torvalds（リーナス・トーバルズ）氏（当時）が独自に開発したOSです。名前のLinusとUNIXのxからLinuxと名づけられました。1991年9月にバージョン0.01のソースコードがインターネットに公開され、1994年3月に1.0.0が公開されました。2009年7月現在、2.6.30.3が公開されています。この間、OSSとして世界中のボランティアが改良に加わり、機能強化されてきました。主にUNIX互換のサーバ系OSとして利用されています。さらに、携帯電話や組込機器などのプラットフォームにも移植されています。携帯電話プラットフォームのAndroidは、OS部分はLinux 2.6カーネルをベースとしています。

Linuxカーネルだけではそれ単体でOSとして動作しませんが、ウィンドウシステム、管理用コマンド、開発ツール、アプリケーションなど、関連ソフトウェアをまとめてパッケージ化したものが各種組織から有償／無償で提供されています。これをディストリビューションと呼びます。始まりはインストールを簡便化するためのパッケージ化でしたが、今では関連ソフトウェアのバージョン管理やメンテナンス機能が強化されています。

Linuxの出現は、IT業界のオープンソース化に大きな影響を与え、有力ソフトウェアがオープンソースで開発される例が多くあります。さらに、システムインテグレーションやサービス面でOSSを利用するための新しいビジネスモデルが登場しています。