

個人情報をめぐる最近の動向について

平成 25 年 2 月 20 日、発明会館において、JISA 情報セキュリティ／個人情報保護セミナー「個人情報をめぐる最近の動向について」が開催された。出席者は 205 名。

(1) 「遠隔操作ウイルス等最新のサイバー攻撃への対応」

独立行政法人情報処理推進機構 セキュリティセンター 調査役 加賀谷伸一郎氏

今回の遠隔ウイルス事件では特に新しい技術が使われたということはなく、従来から利用されてきたツールや仕組みの組み合わせで犯行が行われた。遠隔操作のツールそのものはリモートデスクトップのひとつであり、20 年以上前から利用されている便利なツールであるが、本人の知らないところで仕組まれることに問題がある。情報セキュリティで最も基本的なことは、信頼出来ない場所で、出所不明のソフトウェアを利用しないという原則を守ること、これを現実世界に置き換えると、喉が渴いている時に偶然道ばたに落ちていたペットボトルを拾って飲むことと同じ位危険な行為と言える。

パソコン使用時に注意すべきことは、ウイルス対策ソフトの導入と適切な運用、脆弱性の解消の 2 点であり、ウイルス定義ファイルを最新にすること、OSをはじめとする全てのソフトを最新化することが被害を最小にすることに繋がる。

このほか、新聞等で報道されていないウイルスの挙動やインターネットバンキングで行われているコンピュータ犯罪の事例と対策、スマートフォン利用において注意すべき点などが、実際の事例を交えて分かりやすく解説された。

(2) 「個人情報保護のISO化の動向」

情報セキュリティ大学院大学 教授 原田洋之助氏

ISO では 2006 年から ISO9001、ISO14001、ISO/IEC27001 などの ISO マネジメント規格の整合性を確保するための議論が行われており、ISO 規格全体が共通化される方向にある。そのため、今後制定／改正される全ての ISO マネジメント規格は、原則として ISO MSS の共通構造、共通テキスト、用語、定義等に従う必要がある。規格間の相違は、個々の適用分野の運営管理において特別な相違が必要とされる部分についてのみ認められる。

2011 年秋にケニアのナイロビで行われた会合で、韓国から個人情報保護の ISO 化の提案(PIMS:Privacy/Personal Information Management Systems)があり、SC27 のWG1とWG5の共同の Study Period が開始された。

その後 2011 年にスウェーデンのストックホルム会合、2012 年秋にイタリアのローマ会合が行われ、PIMSの認証にはISO/IEC29100 を要求条件とする必要があり、現在のセクター別規格では不十分なことから、セクター別規格を 27001 と組み合わせる方法を拡張する必要があるとの結論が出た。現在PIMSはSPの段階にあり、正式なISO化にはまだ数年を要すると思われる。

また、プライバシーに関連する規格として ISO/IEC29100 (PII:Personally Identifiable Information)の概要も併せて紹介された。

(佐藤)

