情報通信部会長報告

第３回情報通信部会は、１０月３日イヤタカにおいて３９名の出席を得て開催いたしました。今回は、「情報セキュリティ対策セミナー」と題し、（公財）日本電信電話ユーザ協会、秋田県警察本部、情報通信部会の３団体の共催で開催しました。内容は以下のとおりです。

■第一部「サイバー犯罪の現状について」

講師：秋田県警察本部 警務部警務課 サイバーセキュリティ対策係長 和田真哉氏

・サイバー攻撃への対策は大きく４つ

１．ＯＳやソフトウェアは最新の状態にする

２．ウィルス対策ソフトを導入する

３．パスワードを強化する

４．各種設定を見直す

⇒いずれも１０年前から変わっていないが重要である。

●技術的対策と人的対策は両輪であり、どんなにすぐれた技術や対策も従業員に浸透していなければ意味がない。

■第二部「企業における情報セキュリティのポイントと対策について」

講師：東日本電信電話㈱秋田支店 副支店長兼ビジネスイノベーション部長 堀靖幸氏

・2016 年の 1 年間で日本国内のネットワークへ向けられた不正アクセス数は 1281 億件（1 秒 4000 件）と過去最高となった。

・こうした現状を背景に、今年 5 月に改正個人情報保護法が施行され、中小企業も適用対象となった。

・主な被害としては、（対応に追われての）業務停止、高額な費用負担、信用失墜、情報消失などが挙げられる。

・代表的な情報セキュリティ被害

１．標的型攻撃による情報流出

⇒名前のイメージは特定企業への攻撃だが、実際は「ばらまき型（無差別攻撃）」。

２．ランサムウェアによる被害

⇒ランサム（Ransom = 身代金）。ファイルの暗号化や画面のロックを行い、復旧と引き換えに金銭を要求する。しかし、金銭を支払っても復旧されることはない。

３．内部不正による情報漏洩とそれに伴う業務停止

⇒組織内部の職員や元職員による情報の不正な持ち出しや、安易に持ち出した情報の不適切な管理による紛失、情報漏洩につながるケースがある。

●情報セキュリティは社員の意識が第一である。被害急増の背景には、誰もがパソコンを使う環境になったことも大きい。「知らずに」「うっかり」による被害も多い。社員の意識を醸成し、注意を怠らないことが大切。

●しかし、標的型攻撃やランサムウェアをはじめ、ネットワークへの攻撃は日々巧妙化しているため、いくら社員の意識を醸成してもミスは起こる。社員の判断以前に技術でカバーできるところは対応すべきで、可能な限り様々なセキュリティ対策ソフトやシステムを導入するなど多層防御も検討いただきたい。

以上が、情報通信部会からの報告です。