2015.8.24 電経新聞「Point of View」

インターネット接続禁止令

藤谷 護人

「インターネット接続するパソコンの組織内LANからの切り離し」。内部的情報通信網と外部的情報通信網の分離という考え方だが、これは「組織の標的型サイバー攻撃に対する抜本的主要的予防的対策」であり、インターネットセキュリティ対策として、画期的な進展というべきである。

サイバー攻撃対策の観点からパソコンやスマートフォンを通信・非通信に使い分けるという提案がなされるようになっている。

今年6月1日に、露見した日本年金機構の事故の際に、駆けつけたセキュリティ事業者が真っ先に行ったのは、不正通信をしている部署のパソコンの「インターネット接続を遮断」することであった。

また、同年6月12日に、長野県上田市役所の庁内ネットワークに接続されている端末にマルウェアが感染したことが発覚し、市からは、二次被害を防止するために、「インターネットとの接続を遮断」せざるを得なかったとの発表があった。

これらの事件を受けて、総務省が同月24日に開催した、地方公共団体セキュリティ対策緊急会議において、内閣官房サイバーセキュリティ補佐官・東京電機大学教授の佐々木良一氏は、いまだ個人的見解であり、総務省としての正式見解ではないが、と前置きしつつも「(早期対応案として)インターネットに接続する必要のあるパソコンの庁内LANからの分離の準備が必要である」との趣旨述べた。

このことは、インターネットセキュリティ対策として、画期的な進展というべきである。

佐々木氏の見解は、「分離の準備」と控えめではあるが、明らかに、従来は、標的型攻撃によるメール添付が起因したウィルス感染発覚時の、事後的緊急的一時的な措置としか位置付けられていなかった「インターネット接続するパソコンの組織内LANからの切り離し対策」を、「組織の標的型サイバー攻撃に対する抜本的主要的予防的対策として実施すべきである、との提案」であると解釈できるからである。

この提案に接したときに、私の脳裏に浮かんだのは、1987年秋に海外研修の機会にロンドンのブリティッシュ・テレコム・インターナショナル(British Telecom International co.)の渉外部長にパソコン通信の活用について単独インタビュー訪問したときの彼の部屋の光景である。

彼のデスクの背後に2台のパソコンが設置されており、私の質問に対して、彼は「1台は、会社内基幹システムの端末であり、もう1台は、パソコン通信用のパソコンである」と答えてくれた。

1995年のインターネットの商用開放以来、わずか20年間のアフター・インターネット時代における技術的進歩により、同一の組織内LANに業務用のクラサバも外部とのインターネット通信をするパソコンも混在結合することが、利便性から、当たり前の光景になっていた。

しかし、いままさに標的型サイバー攻撃というアフター・インターネット時代の重大なセキュリティ脅威に直面した組織は、情報管理のコントロール策としてビフォ・インターネット時代に戻って、内部的情報通信網と外部的情報通信網の分離(内部的情報と外部的情報の分離的管理)という考え方・対策へと面舵を切らなければならない事態に直面したというべきである。

ふじたに・もりひと 弁護士法人エルティ総合法律事務所所長弁護士。ITーADRセンター所長。日本の弁護士の中で唯一の公認システム監査人、JISA正会員。