今日の焦点

Winnyによる情報流出事件をめぐって

本年２月、海上自衛隊の「極秘」とされている暗号関係の書類や、戦闘訓練の計画表など多くの機密データがネット上に流出したことが発覚し、大騒ぎとなった。これらのデータは、他国の情報機関やテロ組織にとっては宝の山とも言えるトップシークレットの情報だといわれている。さらに３月には、陸上自衛隊の訓練計画や航空自衛隊の行動計画などのデータも流出していることが分かり、これでは防衛庁ではなく漏洩庁ではないかと揶揄される結果となった。しかし情報漏洩はそれだけでなく岡山県警や愛知県警の捜査資料、京都刑務所などの受刑者や被告の個人情報、TBSの出演者情報、ジャスダック証券取引所の資料などの情報流出が発覚し、相次いで報じられている。

こうした官公庁や大企業の情報漏洩のニュースは大々的に報じられるが、恐らく小規模の情報漏洩はその何倍にも達しているものと考えられる。政府も３月15日に情報流出対策としてWinnyを使わないよう通達をだしたほどである。

これら情報漏洩の原因ははっきりしており、不特定多数の個人間で直接情報のやり取りを行うP2P（Peer to Peer）型のファイル交換ソフトWinnyと、これを悪用するウイルスAntinnyによるものである。Winnyは、音楽や映像などのコンテンツを自由に共有できるため人気となり、使い方が雑誌などで紹介されてから利用者が急増しており、現在利用者は200万人以上と見られている。

一般的にWinny利用者がパソコン内の公開フォルダにデータをコピーしておけば、Winnyを利用しているユーザー誰もがそのファイルを入手できる。ところが、ウイルスAntinnyが入り込むと、パソコン内の公開したくないWordやExcel等のデータファイルも公開フォルダにコピーされてしまい、他のWinny利用者に流出してしまうことになる。このためAntinnyは、暴露ウイルスとも呼ばれている。このウイルスの感染を未然に防ぐにはウイルス対策ソフトを利用すればよいが、Antinnyウイルスには亜種が次々に発生しているため、検出できないことが多く、やはり完全な対策はWinnyを利用しないことに限られる。

この一連の事件で分かったことは、Winnyによる情報漏洩の問題はすでに一昨年から起きており、省庁によっては、Winnyの使用を禁じていたにもかかわらず、この種の指示が徹底されていないことと、意外に私物のパソコンが業務に使われており、業務用パソコンが十分に配備されていないケースが多いということである。今やパソコンは業務に必要不可欠な道具であり、私物パソコンでは仕事をしない、させないなど、公私の使い分けを明確にすべきである。

もうひとつこの事件で何とも皮肉な論理矛盾が起きていることが分かった。このWinnyの開発者は、Winnyを開発し、改良を繰り返していたことが著作権法違反ほう助に当たるとして逮捕され、現在公判中である。保釈中の被告が、３月９日の第20回公判で「（流出拡大を）防ぐ改良は容易にできる。しかし、『改良などの開発はしない』との誓約書を京都府警に提出しており、また罪に問われる可能性があるので、積極的に改良はできない」と述べている。Winnyの開発者を逮捕した結果、Winnyの欠陥が放置され続け、社会に多大な被害を与えているにもかかわらず、どうすることもできないという奇妙な現象が起きているのである。

最近は、このWinnyに限らず、ネット犯罪が急増している。警察庁が２月23日にまとめたサイバー犯罪の検挙状況によると、昨年１年間に全国の警察が検挙した件数は、前年（2,081件）より約千件増え3,161件に達し、統計をとり始めた2000年以降の最多記録を更新した。このうちネットワークを利用した犯罪では、詐欺が前年比の約2.6倍となる1,408件に上っている。今年１月には、スパイウエアを使ったネットバンキング預金詐取事件で、スパイウエアの作成者が初めて逮捕された。また、２月にはフィッシングの手口を使いネットオークションの商品をだましとったとして25歳の容疑者を逮捕したが、フィッシング詐欺事件の摘発も国内初である。

今年は昨年にもましてネット詐取やサイバー攻撃が多発する年になる恐れが高い。これらのネット犯罪に対しては、技術的対策だけでは限界がある。ネット利用者は、少しでもおかしいと感じたら、添付ファイルを開いたり、むやみにクリックしたりせずに、常に冷静に適切な状況判断をする姿勢が求められる。