潜行するサイバー攻撃（第5回）

「史上最悪」の情報漏えい事件が残した教訓

2018.03.20

年々被害が深刻化するサイバー攻撃。2017年に米国の信用情報会社で発生した事件では1億人を超える顧客情報が流出、経営トップ辞任という事態に発展した。この事件は、サイバー攻撃の脅威に対する私たちの心構えを、あらためて考える契機になっている。

2017年9月、米国の大手信用情報会社エクイファックスから「サイバー攻撃により1億4000万件以上の個人情報が流出した可能性がある」との発表が行われた。流出が疑われたのは顧客の氏名・住所をはじめ、クレジットカード番号、社会保障番号、さらには運転免許証番号など極めて多岐にわたる。その規模と深刻さから「史上最悪レベル」と呼ばれるものとなった。

事件の引き金になったのは、同年3月に見つかった「Apache Struts2」の脆弱性だった。このソフトはWebアプリケーションを開発するためのフレームワーク（仕組み）だ。無償かつ自由に利用可能なことから広く使われる。半面、以前からたびたびセキュリティの脆弱性が指摘されていた

問題となった脆弱性（CVE-2017-5638）は、リモートで任意のコードが実行される恐れがあるというもの。3月7日に公開された後、わが国でもIPA（情報処理推進機構）が3月9日に注意喚起を行った。しかし、この脆弱性を悪用したサイバー攻撃は、数日間で一気に広がり、世界各国から不正アクセスの被害が報告される事態となる。日本でも東京都の都税支払いサイトやJETRO（日本貿易振興機構）、日本郵便のサイトなどが攻撃を受けた。

ところが、エクイファックスは脆弱性対策に必要なパッチ（修正プログラム）処理をすぐに行わなかった。7月末になってようやく対策に乗り出す。しかし、その時点ですでに膨大な個人情報が流出していた。同社の前CEOは、遅れの原因について「人為的、技術的ミスが重なった」と説明したものの、貴重な信用情報を扱う企業としてはあまりにずさんな対応だとして批判を浴びた。

被害の実態はさらに深刻？

エクイファックスの事件が明らかになって間もない2017年10月、今度は米国のインターネット関連企業ヤフーが、約30億件の個人情報が流出していたと発表した。そして翌11月には、同じく米国の配車サービス企業Uberから顧客、ドライバーの個人情報約5700件が流出したとの調査結果が公表された。

この2つの事件では被害の深刻さに加え、大きな問題が提起された。それは、被害の実態判明が遅いことだ。ヤフーの場合、サイバー攻撃が発生したのは2013年で、当時は10億件の個人情報流出を発表していた。しかし、その後同社が買収、統合を行う中で新たな事実が次々と明らかになる。4年後に、ユーザーのほぼすべてに当たる30億件の流出が判明した。

Uberの事件では2016年に情報流出が発生した後、その事実を1年以上にわたり当局に報告せず、隠していたことが問題視されている。さらに同社は攻撃者に対し、事件隠ぺいとデータ削除を条件に、10万ドル（約1120万円）を支払ったのも発覚した。企業としての姿勢、責任が問われる事態となった。

その他にも、サイバー攻撃による情報流出事件は後を絶たない。最近は報道を見ても「またか」と感じさえする。しかし、報じられる事件のほとんどは、攻撃を受けた側が当局や関連機関に報告した事例だ。流出数が少ない場合や、発覚によるイメージ低下を恐れて報告しない例を含めると、実際の被害はもっと大きいはずだ。

立場を超えた連携進む

情報窃取と並んでサイバー攻撃の大きな問題となっている「業務妨害」についても、重大な被害の報告が目立つ。中でも2017年春に急激な感染拡大を引き起こしたランサムウエア「WannaCry」が多くの企業、組織に被害をもたらしたのは記憶に新しい。

ランサムウエアはその名の通り、データ復元の「身代金」を奪うのが最大の目的だが、WannaCry拡散は、別の脅威をも生み出した。それは、ATMや医療機器、監視カメラなどパソコン以外の機器にも感染が広がり、停止や誤動作が頻発したことである。世界的にIoT（モノのインターネット）が推進される中でこのような攻撃が行われた場合、製造、サービス、公共インフラなどさまざまな業務が停止に追い込まれ、かつてないダメージを受ける可能性がある。

現在の状況を踏まえ、総務省のサイバーセキュリティタスクフォースは2017年10月、来るべきIoT、AI時代のセキュリティに関する課題をまとめた「IoTセキュリティ総合対策」を発表した。具体的な施策として、

1. 脆弱性対策に係る体制の整備
2. 研究開発の推進
3. 民間企業等におけるセキュリティ対策の促進
4. 人材育成の強化
5. 国際連携の推進

の5項目を挙げている。ただし、これらの課題は行政の主導だけで解決するものではない。大切なのは現場となる企業、組織に所属する人たちの意識であり、それぞれが立場や業種の枠を超えて緊密に連携することが重要だ。

ターゲットにされにくい組織へ

一方、攻撃者の側から見ると、いかにして「ガードの甘い」、そして「対応の遅い」標的を見つけるかが成否を分けるカギになる。エクイファックスの事件では、同社セキュリティ部門だけの判断でパッチ適用を見送り、最悪の結果につながった。同様に米ヤフーは経営形態の変化、Uberは社内管理体制の不備などが、攻撃者にとって格好のターゲットになる要素となった。ガードが固く、対応の素早い組織は標的になりにくい。

少し前まで、各企業、組織はセキュリティ強化のために予算を投じ、人材を確保してそれぞれに努力を積み重ねてきた。しかしサイバー攻撃の脅威は、もはや単独では対抗し切れないレベルに達しつつある。これからのセキュリティ対策は「連携」をキーワードに、社会全体で脅威に立ち向かう必要があるのだ。