歯止めなく蔓延る脅威

サイバー攻撃

2020年を視野にその本質と対策を探る

(33)

サイバー攻撃は社会にさまざまな副作用を与えている。例えば社会を秩序立たせるために存在する法律への影響も決して小さくない。文字通りウイルスのように社会を蝕んでいるのだ。（北島圭）

「サイバー空間が企業セキュリティの重大な脅威になっていることを肌身で感じている」。こう話すのは弁護士法人エルティ総合法律事務所所長の藤谷護人弁護士だ。

第1にスマートフォンの問題に頭を悩ませているという。企業にとって従来のセキュリティ対策が通用しない構造的な問題が3点ある。ただそのことに企業が気付いていない。

一つ目は従来の企業からの情報漏えいは企業の管理するサーバ内にある情報資産の漏えいであり、そのサーバに対するリスク分析とリスクコントロールを行うことによってセキュリティを確保してきた。しかしスマートフォンによる情報漏えいは社員が自ら所有しプロバイダ契約しているので企業の直接的な管理権限が及ばず従来のリスクコントロールの要とされてきたアクセスコントロールなども適用の術がない。

また、従来のリスクコントロールは2本柱からなっている。一つは予防策であり、もう一つは抑制策だ。予防策というのは客観的にコントロールして防壁をつくること。防壁に穴があると、ここから脅威が飛び込んできて組織内の情報資産が侵害されるため、この穴を縮められれば、脅威が飛び込んでくる確率は減る。だから予防策は客観的な脆弱性を客観的な方法で狭める対策となる。

それに対して抑制策は、内部関係者に心理的な抑圧をかける対策だ。前述した通り、情報漏えいの7割以上が内部要因なので、内部関係者に「情報を漏えいするとクビになるぞ」といった抑圧をかけることでリスクを減らすわけだ。

「2本柱の内、客観的な予防策がまず講じられるべき。主観的な抑制策は予防策の車の両輪的に補完する位置づけだ。なぜなら主観的抑制策だけでは、客観的かつ継続的なリスク管理策の効果は期待できない。その半面で、アクセス権限を与えられている社員に対しては、心理的抑制策が最後の砦となるからだ」と藤谷弁護士は語る。

ところが、スマートフォンには、客観的防止策がそもそも適用できない。社員個人の所有物を個人がどう使おうと、企業は客観的な方法は何一つ持たないからだ。

予防策が利かないとなると、抑制策を最大限に発揮するしかない。つまり雇用契約を補完し、法律的にはその一部と評価されている「就業規則」をスマートフォンによる企業セキュリティの構造的変化に対応させるしかない。

具体的には「ソーシャルメディアポリシー」を就業規則のさらなる補完と位置付けて、もしソーシャルメディアポリシーに違反した場合は、就業規則違反で「懲戒」の対象になるということを全社員に周知する必要がある。しかし、ほとんどの企業はソーシャルメディアポリシーをつくっても、就業規則・雇用契約との関係などに思いが及んでいない。

さらに、スマートフォンによるセキュリティリスクは情報漏えいだけではない。不適切発言によって、企業が社会的信用を低下させる事案も同じくらいの割合で発生しており、「個人のデバイスなので、情報管理部門が管轄するものではない」という第1の問題のほかに、「情報漏えいばかりではなく個人の行動の問題なのだから、総務部門か人事部門か、しかし、どちらも電子機器のことはわからないといって、企業の中で所管部門を決められないという意味でのセキュリティ問題も引き起こしている」と藤谷弁護士は話す。

責任はどこにあるのか

「サイバー攻撃に対して、法律的な抑止力が有効に機能していない、こんな状況を一日でも放置することは、法治国家としての体をなしていない」と危機感を藤谷弁護士は口にする。

民事的には、サイバー攻撃を受けて企業に損害が発生すれば民法第709条に基づく損害賠償請求権が発生するが、攻撃者がどこのだれかを特定できなければ、裁判を起こすことすらできない。絵に描いた餅の損害賠償請求権など攻撃者にとって何も怖くはない。刑事的には、情報窃盗罪が定められていないことが問題だ。有体物の財産的価値よりも情報の財産的価値が格段に大きい企業にとって、社会における財産的秩序を支えてくれるはずの刑法による刑罰が「情報窃盗」に及ばないというのは、いかがなものか。刑罰は、人権に対する大きな脅威であり、罪刑法定主義は極めて大切なことだが、刑法が国民生活の安全を守れないという事態は、克服されなければならない。情報窃盗罪の代わりに、不正アクセス禁止法による刑罰が定められているが、標的型サイバー攻撃に対して、この法律による刑事捜査が有効に機能し、犯人が逮捕され、刑罰を受けたという話はほとんど聞かない。

この意味からも「サイバーセキュリティ基本法」が13年10月に成立したことは評価できる。この法律の第17条で「国は、サイバーセキュリティに関する犯罪の取締り及びその被害の拡大の防止のために必要な措置を講ずるものとする」と規定された。2020年の東京オリンピックまで、あと5年しかない。法律の機能である社会に対する事前の抑止力を発揮させてサイバー攻撃に対する耐性を備えた安全な国にしていくには、決して十分な時間とは言えない。

藤谷弁護士は「サイバー攻撃との関係では、インターネットの基本的仕組みをリアル社会における法的規制がシームレスに及ぶように、バーチャルトレサビリティを確保したものに改めるなど、抜本的な検討・推進が不可欠なのではないか」と提言する。

サイバー攻撃の副作用が飛散

法の効力が失われていく…