弁護士が語る！経営者が知っておきたい法律の話(第107回)

法律面から見たサプライチェーンのセキュリティ(前編)

2023.08.24

2022年3月、小島プレス工業のサーバーがランサムウエアに感染し、これにより同社と取引をしていたトヨタ自動車の国内全工場が稼働を停止しました。小島プレス工業が公表したシステム停止事案調査報告書(第1報)では、「子会社が独自に特定外部企業との専用通信に利用していたリモート接続機器に脆弱性があり、そのことがきっかけとなり不正アクセスを受けました。攻撃者はそのリモート接続機器から子会社内のネットワークに侵入し、さらに当社内ネットワークへ侵入して」との説明があり、小島プレス工業の子会社が最初の攻撃対象であったと明らかにされています。

また、2022年10月に同じくランサムウエアによる被害を受けた大阪急性期・総合医療センターの事案も、調査委員会が作成した報告書では、侵入経路は患者給食業務受託事業者の給食センターを経由したサプライチェーン攻撃であったとされています。

このように、サプライチェーン(商品の企画・開発から調達、製造、在庫管理、物流、販売までの一連のプロセスおよび個の商流に関わる組織群)における情報セキュリティが問題となっています。IPA(独立行政法人情報処理推進機構)が公表している情報セキュリティ10大脅威2023でも、「組織」向け脅威の2位が「サプライチェーンの弱点を悪用した攻撃」です。なお、1位は「ランサムウェアによる被害」でした。

サプライチェーンでは、業務の効率化のために受発注システムを共同で利用している場合が多く、セキュリティ対策が弱い企業が狙われ、そこから取引先である大企業に侵入するといった手段が一般化しています。

これまで中小企業では、自社の事業はBtoBが主であるため消費者の個人情報は保有していない、狙われるような機密情報はないといった認識から、情報が流出するリスクと比べセキュリティ対策費用は割高であると考え、積極的に対応しないといった姿勢も散見されていました。

一方で、近時はサイバーインシデントにより、取引先などサプライチェーン全体に損害を与えるリスクが現実化しています。大企業が取引先を選ぶ際には、セキュリティ対策が適切にされている企業であるかという観点も重要になってきており、セキュリティ対策が不十分な場合は、取引先から外される可能性も出てきています。

今回、サプライチェーンにおける情報セキュリティの問題に関し、前編では法的リスクについて、後編では法的リスクを踏まえたインシデント発生の予防や、発生時の対応について説明します。なお、本記事は法的な観点からのアプローチが主であり、技術的な観点などについては、「最新セキュリティマネジメント」といった本サイトの記事を参考にしてください。

経営者個人がダメージを負う可能性も… 続きを読む