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

企業やその経営者が損害賠償義務を負う主なリスクに関し、①企業と取引先、②企業と情報漏えいの被害者、③企業と経営者という観点から説明します。

例えば、自社がマルウエア（不正かつ有害な動作を行う目的で作成されたソフトウエア）に感染し、取引先企業の機密情報やサービス利用者の個人情報が漏えいするとともに、取引先もランサムウエアなどのマルウエアに感染するといった事案が想定されます。

まず、「①企業と取引先」についてです。サプライチェーンの観点からは、自社がマルウエアに感染し取引先にも侵入された場合、取引先での対応費用も損害賠償請求される可能性があります。取引先との間では秘密保持契約（NDA）が締結され、取引基本契約に秘密保持条項が定められていることが通常であり、自社のセキュリティ対策が不十分であったため取引先企業の機密情報が漏えいした場合には、これらの義務違反として損害賠償請求をされる可能性があります。

損害賠償額は個別具体的な事案により異なりますが、対応費用に関し、調査・復旧だけで数千万円以上にもなる場合が多く、これに営業損失なども追加されると莫大（ばくだい）な金額を請求されることも考えられます。例えば、新製品の開発情報が漏えいし、その結果として開発が中止されたような場合には賠償額が高額化する可能性が高いでしょう。なお、取引先との間では継続的な取引関係がある場合が多いので、裁判手続にはならず訴訟外の和解による解決が通常と考えられます。

次に「②企業と情報漏えいの被害者」についてです。マルウエアに感染した企業は自社が被害者という側面もある一方、情報漏えいしてしまった個人との関係では、情報の安全管理に過失があったとして、加害者になる場合も多いでしょう。このため、企業は当該個人に対して損害賠償として慰謝料等を支払う必要があります。

最後に「③企業と経営者」に関してです。自社のセキュリティ対策が不十分である場合、経営者を含む役員等は、善管注意義務（民法644条）に違反したとして、自社や取引先から責任を追及される可能性があります（会社法423条1項、429条）。なお、経済産業省とIPAが2023年3月に公表した「サイバーセキュリティ経営ガイドラインVer.3.0」では、サイバー攻撃から企業を守る観点で経営者が認識する必要のある「3原則」として、以下の事項が示されています。

1. 経営者のリーダーシップが重要

2. サプライチェーン全体にわたる対策への目配り

3. 社内外関係者との積極的なコミュニケーション

こうしたポイントを認識して、自社の情報セキュリティ対策について日頃から意識し、行動していないと、セキュリティインシデントが発生した場合、経営者自身も責任を追及されるリスクが増大します。中小企業でもサプライチェーンの一翼を担う以上、早急に対策を講じる必要があります。