弁護士が語る！経営者が知っておきたい法律の話(第108回)

法律面から見たサプライチェーンのセキュリティ(後編)

2023.09.26

前編では、サプライチェーンにおける情報セキュリティの問題と、それに伴い発生する法的リスクについて説明しました。後編では、インシデント発生の予防とインシデント発生時の対応について、主なポイントを説明します。

予防対策として必須の3つのポイント

まずは、インシデント発生の予防についてです。ポイントは、①セキュリティ対策の強化、②社内規定の整備(セキュリティを含む)、③従業員への研修の3つです。

①セキュリティ対策の強化
予防のためには、セキュリティ対策の強化が必須です。具体的な対策の内容については、本サイトに掲載している情報セキュリティに関する他の記事が参考になるでしょう。

セキュリティ対策の強化には費用が発生します。経済産業省と公正取引委員会は2022年10月に公表した「サプライチェーン全体のサイバーセキュリティ向上のための取引先とのパートナーシップの構築に向けて」で、発注側企業が取引先へのサイバーセキュリティ対策の実施を要請するに当たり、優越的地位の乱用として問題となるおそれがある行為として、①取引の対価の一方的決定、②セキュリティ対策費の負担の要請、③購入・利用強制に関する考え方を示しています。

②社内規定の整備(セキュリティを含む)
法的観点からは、情報管理規則の内容を見直して実施を徹底する他、インシデント対応体制を整備する必要があります。さらに、事業継続計画(BCP:Business Continuity Plan)を作成し、インシデント発生時に直ちに対応できるようにすることが重要です。最低限インシデント発生時の対応をする責任者を決定しておき、「インシデント発生時の対応」についてシミュレーションしておくとよいでしょう。

サプライチェーンにおけるインシデントの発生を予防する観点からは、対策に漏れが生じないように、サプライチェーンに関する基本契約書、業務委託契約書等で、情報セキュリティに関するそれぞれの責任範囲を明確化しておくことも重要です。

③従業員への研修
インシデントの発生を予防するには、従業員の情報リテラシーやモラルを向上させる必要があります。セキュリティ体制を強化したり、情報セキュリティに関する社内規定を整備したりしても、周知徹底されなければ効果が十分に発揮されません。このため、従業員に対して情報セキュリティに関する研修を実施し、意識の向上を図る必要があります。

次に、インシデント発生時の対応について解説します。まずは、インシデント発生直後の対応に関するイメージを持ってもらうため、小島プレス工業が2022年3月1日にプレスリリースとして公表した「ウィルス感染被害によるシステム停止事案発生のお知らせ」のうち、発生直後における対応の部分を引用します。

【2月26日(土)】
21時頃 弊社ファイルサーバにて障害の発生を検知
23時頃 障害発生したサーバの再起動後にウィルス感染と脅迫メッセージの存在を確認

【2月27日(日)】

未明 外部専門家協力のもと、さらなる攻撃予防のため取引先様及び外部とのネットワーク遮断

終日 全サーバを停止後、生産活動にかかるサーバのシステム稼働可否を確認し、一部復旧

【2月28日(月)】

日中 ネットワーク遮断前に授受したデータをもとに生産活動を計画通り継続

夕刻 翌日分の生産活動に必要な取引先様とのデータ授受の代替手段を検討したが、対応が困難と判断し、関係取引先様へ連絡

法律により報告が義務付けられているケースも… 続きを読む