最新セキュリティマネジメント（第11回）

サプライチェーン全体の対策及び状況把握

2022.04.19

経済産業省が策定した「セキュリティ経営ガイドライン」で、経営者が社内に対して指示すべきポイントとして示された「重要10項目」。今回は9番目の項目「ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握」について解説する。

サプライチェーン全体の対策が重要

経済産業省と独立行政法人情報処理推進機構（IPA）が共同で策定した「サイバーセキュリティ経営ガイドライン Ver2.0」では、企業のIT活用を推進する上で経営者が認識すべきサイバーセキュリティに関する原則や、経営者がリーダーシップをもって取り組むべき項目がまとめられている。

企業が行うサイバーセキュリティ対策は、当事者となる自分の組織だけに限られたものではない。商品・サービスの取引先をはじめ、ビジネスパートナーや業務委託先など、多くの関係者で構成されるさまざまな業務プロセスの集合体である「サプライチェーン」全体で取り組む必要がある。

例えば、サイバー攻撃では、対策が不十分な状態にある1つの企業を「踏み台」として、その取引先である企業へと攻撃を拡大し、重大な被害をもたらすケースが後を絶たない。また、関係する企業の被害状況を十分把握できないことが原因で対策が遅れた結果、サプライチェーン全体の運用が停止する事態を招くケースも発生している。このような場合、「委託先の対策が不十分で被害を防げなかった」といった説明は通用しない。外部から見た場合、このような主張は責任転嫁と捉えられ、全ての関係者が姿勢を問われることになる。

今回は監査の実施や対策状況の把握を含むサイバーセキュリティ対策のPDCAについて、系列企業、サプライチェーンのビジネスパートナーやシステム管理の運用委託先などを含めた運用を進める方法と、システム管理などの委託について、自分の組織で対応する部分と外部に委託する部分で適切な切り分けを行う方法について解説する。

契約時にセキュリティ対策を確認

言うまでもないことだが、サイバーセキュリティ対策には相応の「労力」と「コスト」が必要だ。サプライチェーン全体で考えた場合、企業によっては人員不足で対策が不十分になっていたり、思うように関連予算を割り当てられていなかったりするケースも出てくるだろう。

本ガイドラインでは、サイバーセキュリティ対策は自分の組織だけで完結するものではなく、サプライチェーン全体で取り組むべき課題であると指摘しているが、現代のサプライチェーンは非常に大規模なものとなっており、全ての関係先が十分な対策を取っているかを確認することは難しい。さらに、海外の拠点や取引先まで含めなければならない場合にはグローバルな対応が必要になり、さらに把握が困難になっているというのが現状だ。

そこで、本ガイドラインではサプライチェーンのセキュリティ対策を推進する第一歩として、「契約」の重要性を挙げている。これは、企業間でさまざまな取引を開始するに当たり、相手先が現時点でどのようなサイバーセキュリティ対策を実施しているか、不測の事態が発生した場合にどのような体制で解決を図るのかといった取り組みの内容を確認した上で、契約を行うべきというものだ。

言い換えれば、ビジネスを始める条件の1つとしてセキュリティ対策を挙げ、「条件を満たさない企業とは取引しない」という姿勢を示すべきだとしている。長年取引がある企業に関しても改めて現状を報告してもらったり、報告内容に不備がある場合は再度確認したりする必要もある。「これまで問題なかったから大丈夫だろう」という甘い姿勢、判断が大きなリスクとなり、深刻な事態を招くと認識すべきだ。

「遠慮・忖度」なき協力体制の構築… 続きを読む