最新セキュリティマネジメント（第30回）

サプライチェーンの一員としてのセキュリティ対策

2023.11.20

独立行政法人情報処理推進機構（以下：IPA）は2023年10月31日に「サイバーセキュリティ経営ガイドライン Ver 3.0実践のためのプラクティス集 第4版」を発行した。これは、2023年3月に経済産業省とともに発行した「サイバーセキュリティ経営ガイドラインVer3.0」の「重要10項目」の実践に必要な事例を掲載したものだ。改めて、サプライチェーンの一員としての中小企業のサイバーセキュリティ対策のあり方を考えてみたい。

サプライチェーン全体でのセキュリティが課題に

経済産業省とIPAが発行している「サイバーセキュリティ経営ガイドライン」は、サイバーセキュリティという重要な経営課題に企業経営者がどう向き合うべきかをまとめたものだ。2023年3月に6年ぶりに改訂され、Ver3.0が発行された。

ガイドラインは「経営者が認識すべき3原則」「サイバーセキュリティ経営の重要10項目」を中心に構成され、管理体制やリスクの特定と対策の実装、インシデント発生に備えた体制、サプライチェーンセキュリティ対策の推進、ステークホルダーを含めた関係者とのコミュニケーションの推進など、広範囲にわたる取り組みが具体的に解説されている。

「サイバーセキュリティ経営ガイドライン Ver 3.0実践のためのプラクティス集」は、この取り組みを実践するために参考とすべき事例をまとめたものだ。中でも多くの中小企業に関係があるのは、サプライチェーンを構成する一員としてどのようなセキュリティ対策が求められるのかという点である。

経営者が認識すべき原則の1つにサプライチェーン全体への目配りを上げており、重要10項目でも「指示9：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状況把握及び対策」を取り上げている。「サイバーセキュリティ経営ガイドライン Ver 3.0実践のためのプラクティス集」では、指示9について6ページにわたって解説されている。

サプライチェーンを守るため自社でするべき対策

第4版で特に注目したいのが、サプライチェーン全体でサイバーセキュリティ対策を講じるため、実践のファーストステップとして「サプライチェーンで連携する各社が『自社ですべきこと』を実施する体制の構築」という新しいプラクティス（9-2）が追加された点だ。この事例から、求められるセキュリティ対策が見えてくる。

プラクティス（9-2）では、上場している従業員数8000人規模の輸送機器メーカーの例を挙げている。このメーカーは大企業から零細企業まで100社以上の委託先との取引があり、規模別に数社に状況をヒアリングしたところ、中小規模の企業を中心に「どう対策をして良いのか分からない」という意見が多く聞かれたという。そこで、各社が何をすべきかの検討を開始した。

まず、今後も取引が見込まれる委託先にセキュリティ担当者を設置できるかを照会し、できないと回答した企業には、企業規模に応じて実施すべき対策を連絡した。さらに、サプライチェーンに参加する全ての企業を対象に、セミナーを実施した

りセキュリティ対策の問い合わせ窓口を設けたり、対策状況のアンケート調査を毎年実施することなどを決めたという。

各社が実施すべき対策としては、一定規模の企業にはエンドポイントでの検知と対応のソリューションであるEDR（Endpoint Detection and Response）の自社運用か、外部のEDR付きのサポートサービスの契約を求めている。上記以外の規模の企業には、委託業務用の機器はインターネットに接続しないよう求め、接続する必要がある場合には上記クラスの区分と同様の対策を求めている。

この事例には、同社が実施しているアンケート調査項目の抜粋も掲載されている。一定規模の企業に対しては、セキュリティ対応方針の規定、情報管理に関するルールの整備、セキュリティ教育の実施などについての回答を求めている。これらはサプライチェーンの一員として中小企業に求められる最低限のセキュリティ対策といえるのだろう。

また、外部のEDRありのサポートサービスとして、IPAが推進している「サイバーセキュリティお助け隊サービス」を紹介している。これは、中小企業・小規模事業者向けのサービスで、IT導入補助金の支援も受けられる。サプライチェーンの一翼を担う以上、企業規模に関係なく企業の責任としてこうしたサイバーセキュリティ対策を求められると覚悟して、人員や費用などをあらかじめ想定しておくことをお勧めする。