経営課題としてのセキュリティー対策を統合的かつ継続的にご支援いたします

日本アイ・ビー・エム株式会社
CISO
執行役員
セキュリティー事業本部長
志済 聡子

経営課題として組織的な対応が進む海外企業

今日のセキュリティー・リスクは深刻です。特定の企業や組織を標的にした組織立ったサイバー犯罪が急増し、その多くは、機密情報の売買や操業妨害によって「経済的な利」を得ることを目的としています。攻撃は執拗となり、手口も年を追うごとに巧妙化・悪質化しています。自社の情報資産や顧客・取引先、ひいては事業を守るには、「セキュリティー対策はIT部門単独の責任」という姿勢ではなく経営課題と位置づけ、全社的な取り組みが必要だと言えるでしょう。

海外ではすでに多くの企業が、「CISO（Chief Information Security Officer：最高情報セキュリティー責任者）」を設け、組織・体制の強化を図っています。CISOは自社における情報セキュリティーの総責任者であり、全社的なセキュリティー対策を統率するばかりではなく、他の経営陣に対してセキュリティー対策の重要性や、それを怠ることの経営リスクを認識させる使命も帯びています。また、さまざまな企業のCISOが業界別に集結することで、コミュニティーを形成しています。一方、日本においては、CISOがまだ定着しておらず、CIO（最高情報責任者）が兼務したり、CIO管轄下のIT部門が権限を持たず、責任だけを担うケースが多く見受けられます。

また、リスク・マネジメントの観点からは、「万が一の事態への備え」を強化することも重要です。近年、モバイル・デバイスの普及、IoT（Internet of Things：モノのインターネット）の進展など、攻撃用のマルウェアを侵入させる対象機器・経路が増大しています。侵入を防ぐための対策も重要ですが、侵入された後の被害をいかに最小限に食い止めるかという「ダメージ・コントロール」の重要

性が増しています。それに伴い急務となっているのが、万が一の事態に備えるための体制、すなわち「セキュリティー・インシデントに迅速に対処できる体制」を整えることです。海外企業の間では、専門チーム「CSIRT（Computer Security Incident Response Team）」を組織することが浸透しつつあり、IBM社内でもグローバル・レベルで常にセキュリティー・リスクを監視し、いざというときに迅速に対処できるようCSIRTを設置しています。日本においても、特に官公庁や金融機関など、高度なセキュリティー対策が求められる企業・組織の間ではCSIRT作りが進められています。

サイバー攻撃が高度化・多様化する中で、経営課題としてセキュリティー戦略を描き遂行していくためには、CISOやCSIRTなど組織的な対応が急務になっていると言えるでしょう。

環境の変化に対応して、継続的な取り組みが必要

技術的な面からセキュリティーを考えるとき、サイバー攻撃の変化や自社のIT環境の変化に合わせて、継続的な強化を図っていく必要があります。また、近年の巧妙なサイバー攻撃に対抗していくためには、異なる役割を担う複数のセキュリティー製品を連携させ、脅威の迅速な検出・対処を可能にする全体設計を行うことが重要です。

さらに、セキュリティー対策は技術の導入だけでは完結せず、セキュリティー・ポリシーを適切に運用するための体制とプロセスを作り上げ、しっかりと運用していくことが不可欠です。前述したCSIRTも、インシデント対応プランを策定しチームを組織すれば終わる取り組みではなく、演習の繰り返しによってチームの対応力を強化すべきでしょう。また、ポリシー自体もIT環境およびビジネス形態の変化に応じて適宜更新していく必要があります。

統合的な解決策を提供するIBM

日本IBMは2015年10月より、セキュリティー事業を担う複数の組織体制を統合・刷新し、「セキュリティー事業本部」を設置しました。その狙いは、これまで別組織であったセキュリティー製品とセキュリティー・サービスの部門を一体化させることで、お客様の課題に応じて必要な製品・サービスを迅速に提供するとともに、セキュリティー対策の継続強化と適切な運用を包括的にご支援することです。

IBMでは、多様なセキュリティー・リスクに網羅的に対応できる製品群はもとより、実効性の高いコンサルティング・サービス、構築・実装支援サービス、運用・監視サービス、緊急時対応のサービスなどを提供しています。それらを、グローバルワイドに、標準化された形で高品質に展開できることが、お客様にとってのIBMの大きな価値でもあります。

例えば、運用・監視サービスの拠点「SOC（Security Operation Center）」は、日本を含む世界10カ所に広がり、お客様システムのネットワーク・セキュリティーの状況を24時間365日体制で監視しています。IBMは世界133カ国で、日におよそ150億件のセキュリティー・イベントを監視し、そのリアルタイムの攻撃インシデント情報をベースに最新の攻撃から未知の脅威までを分析、さらにその成果をいち早く製品の防御エンジンに反映させることで、高い品質の攻撃検知・防御のご支援を実現しています。これは、セキュリティーの製品とサービスを両方有するベンダーのみの大きな価値であり、セキュリティー課題に対する統合的な解決策を提供できるIBMの強みだと考えます。