# 事業会社のサイバーセキュリティ体制と課題

情報セキュリティ大学院大学 博士前期課程 2 年　坂井武

## はじめに

昨今、ランサムウェア攻撃によるシステム障害やWebサービスからの個人情報漏洩、一般の顧客を対象としたフィッシング詐欺、さらには「能動的サイバー防御」の必要性など、サイバーセキュリティに関する報道が頻繁に行われている。これらの報道では、発生した事象や被害については詳しく述べられているが、組織が日頃からどのように対策しているかについてはあまり触れられていない。本稿では、事業会社におけるサイバーセキュリティ確保のための体制、その具体的な業務内容、そして課題と展望について述べる。

## サイバーセキュリティ担当組織の設置状況と業務内容[1]

NRIセキュアテクノロジーズ社の調査結果によると、企業規模別のサイバーセキュリティ専門組織を有する割合は、従業員数10,000人以上で約76％、1,000人から10,000人で約40％、1,000人未満で約22％となっている。この調査結果では、その専門組織の人員数については言及されていないが、大企業でも100人を超える専任の人員を有する場合もあれば、他業務と兼務する数名の人員で対応している場合もあるなど、業種や業態によって規模は様々である。また、内閣サイバーセキュリティセンター（NISC）は、その専門組織の典型的な機能として「経営層」「戦略マネジメント層」「実務者・技術者層」の3層で整理している。さらに、経済産業省および情報処理推進機構（IPA）は、それぞれの役割を以下のように定義している。

・経営層
取締役会や執行役員会議において、セキュリティ意識の啓発、対策方針の指示、予算・実施事項の承認などの意思決定を担う。

・戦略マネジメント層
経営企画部門、管理部門、セキュリティ統括部門、内部監査部門が該当する。サイバーセキュリティに関連する代表的な業務としては、リスクアセスメント、ポリシーやガイドラインの制定、サイバー攻撃による被害が発生した際のコントロールや広報・法務対応、内部監査などを担う。

・実務者・技術者層
情報システム部などのデジタル関係部門や事業部門が該当する。システムの開発・設計段階で実施する代表的な業務としては、脆弱性診断というセキュリティ観点で行うテストがある。これは、開発したシステムに脆弱性（システム停止や内容の改ざん、機密情報の漏洩に至るような不具合）があるかどうかを技術的にチェックするものである。機密情報漏洩へと至る脆弱性（SQLインジェクション脆弱性[2]など）は、このプロセスで見つかることが多い。

システムの運用・保守段階では、サイバー攻撃の発生状況を監視する業務がある。具体的には、システムに導入したセキュリティ対策製品が発するアラートを精査し、それがサイバー攻撃に起因するものかどうか、システムが影響を受けたかどうかを24時間365日体制で分析する業務である。また、この段階で欠かせないのは、近年は1年間で3万件程度の数が判明するソフトウェアの脆弱性への対応である。危険度にもよるが、それらは攻撃者に悪用される可能性がある。ランサムウェア攻撃で特に用いられるのがVPN機器[3]で判明する脆弱性で、メーカーから提供される修正パッチを可能な限り早く適用するなどの対策を行う必要がある。これらに加え、万が一セキュリティインシデントが発生した際の技術的な調査も、この段階で行う重要な業務の一つである。

## 課題と展望

これまで述べてきたように、サイバーセキュリティに関する業務は多岐にわたり、それぞれが独立した専門領域を形成している。そして、サイバーセキュリティ専門組織を有する企業の割合やその規模は様々だが、それらの業務を担当できる人員が慢性的に不足している点では共通している。この背景として、サイバーセキュリティ人材には高度な専門知識が要求されるため、その市場価値と需要が高いことが挙げられる。

この問題の短期的な解決策として、実務者・技術者が担う脆弱性診断やサイバー攻撃の監視といった業務をセキュリティ専門会社に委託することが考えられる。しかし、外部委託には相応のコストがかかる。即戦力の経験者を中途採用する方法もあるが、スキルを有する人材の獲得は熾烈な競争となっており、他社よりも高い年収など、好条件を提示しなければ採用は困難である。また、高い年収を理由として中途入社した人材は、他社からさらに高い年収を提示されるとあっさり転職してしまう可能性もある。

そのため、長期的な解決策としては、自社への愛着と誇りを持つ人員をセキュリティ人材として育成することが重要である。加えて、その人材についても他社への転職を防ぐため、キャリアパスの明示や成長機会の提供により従業員満足度を高め、他社に見劣りしない待遇を提供することが不可欠である。

＜参考文献＞
NRIセキュアテクノロジーズ株式会社「NRI Secure Insight 2022～企業における情報セキュリティ実態調査～」2023年2月1日。
内閣サイバーセキュリティセンター「サイバーセキュリティ人材の育成に関する施策間連携ワーキンググループ報告書」2018年5月31日。
経済産業省・独立行政法人情報処理推進機構（IPA）「サイバーセキュリティ体制構築・人材確保の手引き　第2.0版」2022年6月。

1　本稿末尾に記載の参考文献を参照。
2　SQLインジェクション脆弱性とは、データベースへの不正アクセスが可能な脆弱性である。
3　VPN機器とは、主に企業内に設置する、仮想的な専用線を実現するための機器である。近年はテレワークのために用いられることが多い。