トピックス

経営課題としてのセキュリティ管理
―効率的かつ継続的に取り組むための3つの指針―

昨今、企業には、セキュリティを経営課題として捉えることが求められている。本稿では、人材不足や新たな脅威が発現し続ける状況において、効率的かつ継続的にセキュリティを管理することの難しさについて説き、デジタル技術を取り入れたリスク管理の要点について提言する。

NRIセキュアテクノロジーズ
コンサルティング事業本部
GRCプラットフォーム室
上級セキュリティコンサルタント
渡部（わたなべ）　惣（おさむ）
専門は情報セキュリティに関する調査・ビジネス企画・コンサルティング

NRIセキュアテクノロジーズ
コンサルティング事業本部
GRCプラットフォーム室
副主任セキュリティコンサルタント
森（もり）　茉莉香（まりか）
専門は情報セキュリティに関する調査・ビジネス企画・コンサルティング

セキュリティを経営課題として捉える

企業の経営者がリーダーシップを取ってサイバーセキュリティ対策を推進するための指針として、2015年12月に経済産業省が「サイバーセキュリティ経営ガイドライン」を策定してから数年がたつ。これまではセキュリティを“コスト”と捉える企業も多かったのではないだろうか。現在では、安定した事業活動や成長のために必須な“投資”として捉え、経営者がリーダーシップを発揮してセキュリティ対策を推進することが求められている。

では、具体的に何をすればよいのだろうか。

セキュリティリスクの管理においても、ポイントは他のリスクと同様である。まずリスクを「特定」し、リスクへの「対策を実施」する。そして継続的に「内容を見直す」という3つのポイントが重要となる。

(1) リスクの把握と計画の策定

自社にとって守るべき情報・資産を特定し、セキュリティ脅威の発生可能性と影響度からリスクを把握する。そのリスクへの対応計画を策定し、経営資源を適切に配分する。

(2) リスク対策の実施と進捗（しんちょく）の把握

計画に沿ったセキュリティ対策が実施されているか、その進捗を把握し、必要に応じて経営資源の追加投入などの判断を行う。

(3) 対策の継続的な見直し

対応方針の見直しや課題解決のための改善活動を推進する。

さらに、上記のリスク管理は自社だけでなく、外部の委託先や取引先、またグループ企業でも確実に実施し、サプライチェーン全体の管理状況を把握する必要がある。

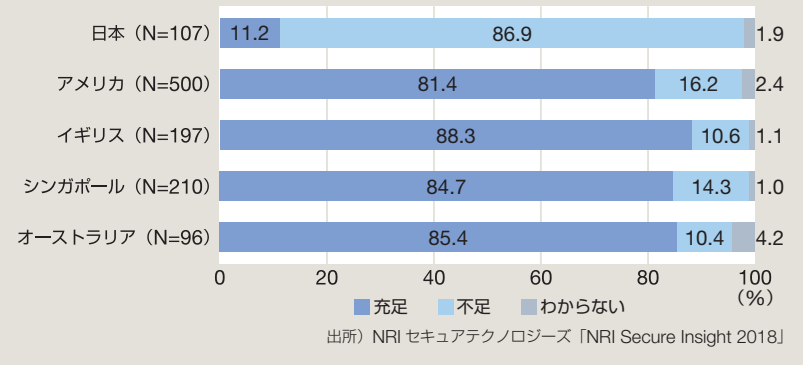
これらを完璧に実行できているといえる企業は、決して多くはない。日本のセキュリティ人材が圧倒的に不足しているという状況が、この原因の1つとして考えられる。

人材不足の状況下における セキュリティリスク管理の課題

NRIセキュアテクノロジーズ（以下、NRI

セキュア）が2018年に実施した、日本（107社）、アメリカ（500社）、イギリス（197社）、シンガポール（210社）、オーストラリア（96社）の計1,110社が回答した情報セキュリティに関するアンケート「NRI Secure Insight 2018」では、日本は他4カ国と比較して圧倒的にセキュリティ対策に従事する人材が不足していることが明確となる結果になった。（図1参照）

図1　セキュリティ対策に従事する人材の充足状況



出所）NRI セキュアテクノロジーズ「NRI Secure Insight 2018」

また、経済産業省が2016年に報告した「IT人材の最新動向と将来推計に関する調査結果」によると、日本全体でセキュリティの専門性を持った人材が、2020年までに約20万人不足するといわれており、セキュリティ人材が不足する状況は今後ますます深刻化することが予想される。

では、これらの人材不足は、どのような原因によって引き起こされているのか。大きく分けて以下の3つの背景があると考えられる。

・セキュリティ業務の属人化
・多様化・複雑化する脅威
・経営層と現場の間のコミュニケーションギャップ

この3つが、企業のセキュリティ人材不足の本質的な背景であり、セキュリティ経営を難しくしている原因である。さらにサプライチェーン全体のリスク管理状況の把握も求められるようになると、対応すべき対象が海外企業にまで拡大するケースもあり、セキュリティ経営の実現はより困難になる。

これらの状況を踏まえると、これからのセキュリティ経営に必要不可欠なものは、次の2点である。1つは現場の負荷を抑えながら効率的に業務を運営すること、そしてもう1つは、多様化・複雑化する脅威に対して、現場と経営層が共通の理解を持ち、投資の判断に必要な情報が適時的確に得られる「仕組み」を整備することである。

（1）セキュリティ業務の「標準化」

まずは、「セキュリティ業務の属人化」への対策について考えてみたい。

セキュリティ業務は、物理的なものからアプリケーションに至るまで、対象が非常に幅広く、ITの中でも特に難易度の高い業務の1つである。そのため多くの企業では、長年かけて担当者がセキュリティ業務をマスターしたため、担当者を変更しないというケースがよくある。その結果として、業務が「属人化」してしまうことがある。これが大きな問題につながる。

属人化により、社内のセキュリティリスクやそれらへの対策状況などが、特定の担当者しか知らないという事態になる。セキュリティ対策の客観性・妥当性が失われるだけでなく、いつまでたっても「特定の人物だけが忙しい」という状態に陥ってしまう。

このような状態から抜け出すためには、セキュリティ業務の「標準化」が必要である。

標準化の上で前提となるのは、自社が保有するセキュリティリスクの全体像を把握することである。それらを見極めた上で、各リスクのコントロールに必要な業務を決めていく。そして、それらの業務に対する手順を1つずつ定義し、文書化する。

リスク評価や対策内容の検討の際には、担当者の主観だけでなく、客観的な視点を取り入れる必要があることに留意したい。前述の「サイバーセキュリティ経営ガイドライン」など、公的機関や民間団体が公開している各種基準やガイドラインの利用を推奨する。これにより、従来は特定のセキュリティ担当者の視点でのみ行われていた業務に客観的な視点が加わり、業務の抜け・漏れを排除できる。

業務のプロセスや手順が定義されることで、担当者が不在の場合や繁忙時に、他の社員でも業務を代行できるようになる。また、業務の中で専門的なスキルが必要ないものが明確になれば、他部署の人材や協力会社に委託できるようになる。これにより担当者は、最も注力すべき、セキュリティの戦略や企画などのクリエイティブな分野にリソースを振り向けられるようになる。

(2) 多様化・複雑化する脅威には、最新技術と組織で対応する

次に、「多様化・複雑化する脅威」にはどう対処すればいいのか。

標的型攻撃はますます巧妙になり、ランサムウェア（感染したPCのデータを暗号化するなどして利用できないようにし、解除するために身代金の支払いを要求する不正プログラム）など新たなタイプのマルウェアも続々と生まれている。これらの脅威に、より効率的に対処するには、最新の技術を活用することに尽きる。

例えば、社内で端末がマルウェアに感染した場合。従来の運用では、まず担当者が不審な通信をネットワーク機器などから検知し、IPアドレスから端末を特定して、端末を社内LANから隔離するといった作業が必要だった。しかし、現在では、新たな概念の製品が登場している。「EDR（Endpoint Detection and Response）」と呼ばれる製品であり、これを使うと、不審な動作や振る舞いを端末側で検知し、すぐに担当者にアラートが送られる。担当者はリモートで端末を隔離し、端末内の詳細な調査を行うことができる。誤検知か疑わしい場合には、ひとまず隔離し、外部の専門業者に調査を依頼することも可能である。

つまり、今までは特定の担当者や社外のプロフェッショナルしかできなかった作業が、簡単に誰でも実施できるようになってきている。人材不足の状況を改善するには、これらの革新的な技術も、積極的に活用していくべきである。

(3) 経営―現場間に「共通のモノサシ」を作る

最後は、セキュリティに関する「経営層と現場の間のコミュニケーションギャップ」についてである。

企業のセキュリティの現場では、担当者が経営層へ報告する際に、専門的用語を多用したり、複雑な攻撃の手口を説明したりするため、経営層が内容を理解できない場合もある。結果、セキュリティ対策への投資の稟議（りんぎ）が承認されなかったり、必要な対策を講じる

ことに時間がかかったりして、業務の停滞につながることがある。

これを打開するには、まず現場の部門が、経営層に伝わるようなメッセージを訴求していかなければならない。そのためには、セキュリティリスクが顕在化した場合に事業にどのような影響を与えるのか、そして現状、どのような対策がなされているかなど、ポイントを押さえつつ、簡潔な表現で伝える必要がある。

一方で、経営層はそれらを理解して、セキュリティを経営課題と捉え、対策にコミットしていくことが重要となる。

サイバーセキュリティ経営ガイドラインの「経営者が認識すべき3原則」では、最初の1つに、「経営者は、サイバーセキュリティリスクを認識し、リーダーシップによって対策を進めることが必要」と規定されている。

現場部門は、自社の事業特性を考慮してセキュリティリスクを特定し、経営層にも伝わる表現でそれらを伝え、経営層はそれに対してコミットする。経営層と現場部門が相互に歩み寄っていくことが、セキュリティ経営の効率化につながる。

「Secure SketCH」による セキュリティ経営実現

セキュリティ経営実現のための1つの取り組みの例として、「Secure SketCH（セキュア スケッチ）」を紹介する。（図2参照）

Secure SketCHは、NRIセキュアが開発した無料のWebサービスである。このWebサービスは、セキュリティ対策状況の可視化を目的としている。ユーザーは78の設問に答えるだけで、自社のセキュリティ対策状況をスコア・ランクで把握できる。加えて、他社との比較結果を、偏差値として確認できる。セキュリティ対策状況を俯瞰（ふかん）的に把握できるので、経営層が見ても、全体像が一目で分かる。実際に、経営層とのコミュニケーションツールとしての活用事例も多い。

Secure SketCHはシミュレーション機能も有している。例えばある対策を実施した場合、どの程度スコアが変動するか、対策前に確認できる。これにより、最もスコアが高くなる対策から優先的に取り組むといったように、費用対効果の観点で対策の優先順位付けを判断する材料になる。

セキュリティ経営を効率的に実現していくために、ぜひSecure SketCHを活用いただければ幸いである。 ■

図2 「Secure SketCH」評価画面