戦略的な情報セキュリティ対策のために
現在の対策状況を可視化・評価することの重要性

十川 基／中島由宏

昨今、企業へのサイバー攻撃件数が増え、手口も巧妙化している。企業の費用・時間の負担は年々増加し、情報セキュリティ担当者の負担も大きくなっている。一方で、予算や要員を十分に確保できない企業も多い。

年々高度化するサイバー攻撃に効率的に対応するためには、戦略的アプローチが有効となる。網羅的・具体的な国内外の各種基準・ガイドラインを組み合わせ現在のセキュリティ対策状況を評価・分析し、必要な施策に優先順位を付ける。そして経営層を巻き込んで中長期計画を策定し、計画の実行後は定期的に確認・見直しを実施する。具体例として、セキュリティ対策の明確な優先順位付けを実現した事例と、自社の状況を的確に把握し、認識の適切な共有を実現した事例を紹介し、その有効性を確認する。

最後に、経済産業省と独立行政法人情報処理推進機構（IPA）が策定した「サイバーセキュリティ経営ガイドライン」を紹介し、経営戦略の一部としてセキュリティ対策の内容や優先順位を判断する必要性について提言する。

セキュリティ対策の難しさ

情報漏洩などの事件が起きるたびに、IT部門が経営陣などから「自社でも同様の事件が起きないか」「セキュリティ対策は十分か」について説明を求められるケースは少なくない。ベンダーが提案するさまざまなセキュリティ対策の有効性に確信が持てず、ベンダーの言いなりになってはいないかと危惧している企業も多い。こうした状況から脱しようと、公開されているセキュリティガイドラインを参考に対策を立てようとする企業もあるが、海外を含め多くのガイドラインが存在するため、どれをベースにすればよいのかを判断するのは容易ではない。また、自社の事業規模や業務内容、業界の特性に合わせた対策にとどめたくても、最低限満たすべきセキュリティレベルを決めること自体が難しい。

こうしたことから、本来必要な対策が実施されないことによりセキュリティリスクが残存したり、逆に不必要な対策にまで投資したりするケースは少なくない。そこで提案したいのが、次節で説明する戦略的なセキュリティ対策の立案である。

戦略的なセキュリティ対策

戦略的なセキュリティ対策とは、自社の進むべき方向性とシナリオに基づいて適切な優先度を付けたセキュリティ対策のことである。以下、それをどのようにして立案すべきか、ステップごとに解説していく。基本的には、目指すべき目標を定め、現状を把握し、目標とのギャップを埋めるための対策を立案するという進め方である。

(1) 自社のセキュリティ基準の決定

まず、各種のガイドラインを参考に、自社のセキュリティ基準を定める。主要なガイドラインには次のものがある。

①ISO/IEC 27001/27002（国際標準化機構（ISO）と国際電気標準会議（IEC）策定）
②Cybersecurity Framework Version 1.0（米国の国立標準技術研究所（NIST）策定）
③Critical Security Control for Effective Cyber Defense Version 6.0（米国のインター

ネット・セキュリティ・センター（CIS）策定）

④金融機関等コンピュータシステムの安全対策基準（日本の金融情報システムセンター（FISC）策定）

その他、国内外のさまざまなガイドラインがあるが、内容の粒度や深度、範囲、具体的な対策事例が異なっているため、自社に最適な形で組み合わせて使うことが望ましい。

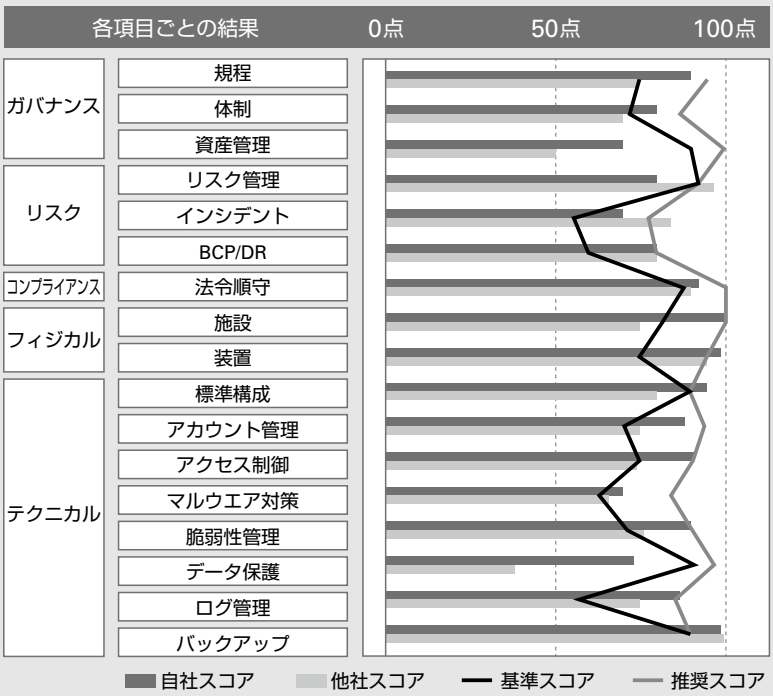
(2) 現状の調査

次に、どの情報資産やシステムが守るべき対象とされているか、どのような対策がなされているかを調査する。守るべき対象は、多層防御の観点から、社内外をつなぐネットワークや端末、組織の体制なども含めて考える必要がある。より精度の高い調査結果を得るためには、担当者へのヒアリングだけでなく、機器のログが正しく取得されているか、機器の設定が設計書やパラメーターシートの通りに正しく行われているかなどを確認することも必要である。

(3) 現在の対策の分析

調査結果に基づいて、現在の対策状況を分析・可視化する。以下のように複数の手法があり、それらを組み合わせて多角的に分析することで、自社の対策状況をより正確に把握できる。図1にNRIセキュアテクノロジーズ（以下、NRIセキュア）による自社と他社の比較分析（可視化）の例を示す。

図1　セキュリティ対策状況分析（可視化）の例



①定量分析

どこまで防御策が講じられているかを定量的に分析する。そのために、セキュリティが十分に確保された目指すべきレベルと、必要最低限のレベル（ベースライン）を定義した上で、各脅威に対する現在の対策状況を数値化する。これにより、自社の対策のどこに不足があるかを定量的に把握できる。

②リスクシナリオ別評価

昨今の事件・事故を踏まえ、標的型攻撃や情報持ち出しなどの想定シナリオに基づいて対策状況を評価する。これにより、シナリオ別に自社の対策のウイークポイントを被害に遭う前に把握することができ、各種のリスクに対する具体的な対策が明確になる。

③網羅性・合理性の評価

どのレイヤーでどのような対策

が行われているかを可視化し、対策の不備・不足とともに機能の重複についても評価を行う。機能を網羅的に確認してみると、実施しようとしていた対策の重複や効果の薄さに気付くことができ、自社に必要十分な対策が明確になる。

④他社比較

同業他社との比較を通じて自社のセキュリティ対策の過不足を把握することで、業界に合った適切なセキュリティ対策と、かけるべき適正なコストを把握できる。

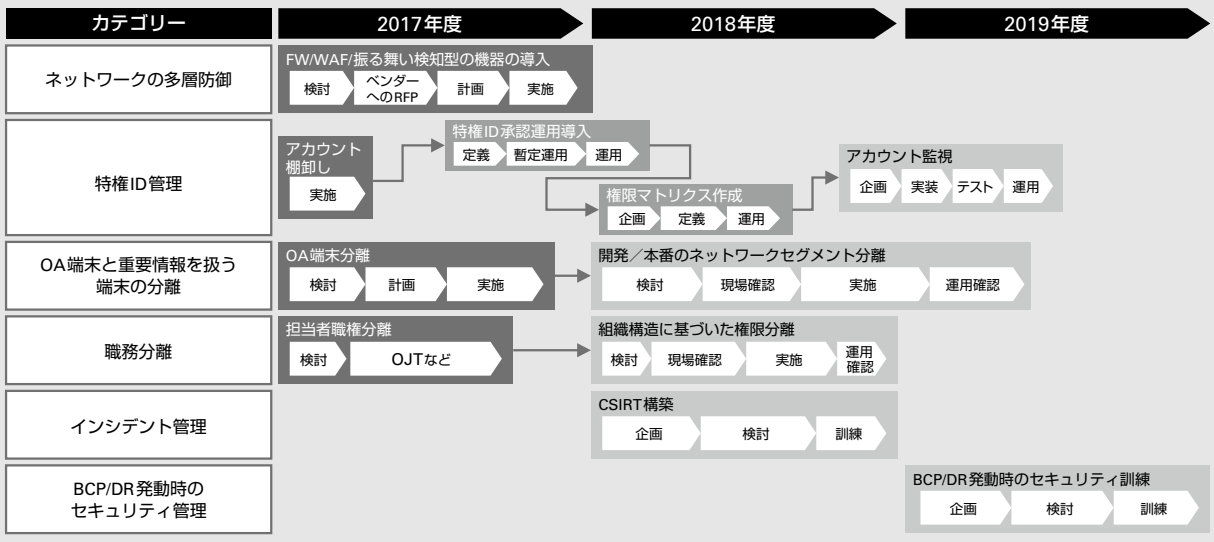
(4) 経営層を巻き込んだ中長期計画の策定

以上の分析に基づいて、必要な対策ごとに効果と実現性を踏まえた優先順位を設定し、中長期計画を策定する。図2は中長期計画の例である。中長期計画は、対策の実施に必要な期間、コスト、人員などを具体的に整理し、実現性のある計画に落とし込んだものである。最も重視すべきことは、経営層による形式的な承認ではなく、経営層を巻き込んだ合意形成である。なぜなら、入念に策定された中長期計画であったとしても、経営方針のようにトップダウンで実行されないと現場に浸透しない可能性があるからだ。そして少なくとも半年に1回は、計画の進捗について経営層を含めた確認会を実施し、必要に応じて計画の修正を行うべきである。

対策状況を可視化する効果

前述の手順により、自社に最適なセキュリティ対策を立案することが可能となる。しかしながら、業界横断的な知識やセキュリティの高度な専門知識が必要であり、そのような人材を社内で確保することは極めて難しい。そのため、NRIセキュアでは、国内外の主要なガイドラインを組み合わせ、企業のセキュリティ対策状況を網羅的・横断的に診断するサービス「NRI Secure Framework」(以下、「NSF」)を2016年3月から提供している。同サービスでは、独自調査で入手した国内外700社以上の

図2　中長期的なセキュリティ計画の例



セキュリティ対策状況のデータに基づいて、業種・規模が近い企業との比較も可能になっている。「NSF」は金融、製造、エネルギー、運輸、商社、流通など複数の業種で既に利用実績があり、次のような効果が得られている。

①対策優先度の明確化

流通業のA社では、Webアプリケーションの脆弱性を突かれ、機密情報が漏洩する事故が発生した。暫定的な対応の後、対策に不備がないかを「NSF」によって診断した。「NSF」では、Webアプリケーションだけでなく、社内外をつなぐネットワーク、社内ネットワーク上に配置された重要なサーバー、業務で使用するPC、それらを管理する組織や物理的なセキュリティ対策などを、多層防御の観点で多角的に診断する。そのため、外部からの攻撃への対策状況だけでなく、マルウエア感染後の情報探索や内部不正への対策状況も適切に評価することができる。

診断の結果、A社では外部脅威に対してはネットワーク層を中心に多角的な対策が行われているものの、ネットワーク層の防御壁を突破されるとその後の情報探索などを検知できないこと、アクセス統制に不備があり内部不正を誘発しやすい環境となっていることが分かった。付き合いがあるセキュリティベンダーは、事故を契機に外部脅威へのさまざまな追加対策を提案していたが、「NSF」の活用により、今のA社に必要な対策およびその優先度を見極められるようになり、結果として対策への投資判断の基準も明確化された。

②リスクおよび状況の認識共有

製造業のB社とC社は、経営統合の準備を進める過程で新会社における情報セキュリティ基盤のあり方を議論したが、両社のセキュリティ担当者の議論が全くかみ合わなかった。両社のセキュリティ基準にずれがあり、それぞれのセキュリティ対策状況を同じ物差しで評価できなかったためである。両社の依頼を受けたNRIセキュアは「NSF」を活用して、両社のセキュリティ対策状況の違いを分かりやすく数値で可視化した。また、定められていた目標スコアと評価結果を比較することで、両社の強みと弱みを一目で分かるようにした。両社からは、同じ物差しを使った本質的な議論が行え、あるべき姿を整理できたとの評価を得た。

期待される経営者のリーダーシップ

2015年12月、経済産業省は独立行政法人情報処理推進機構（IPA）と共に「サイバーセキュリティ経営ガイドライン」を策定した。そこでは、サイバー攻撃から企業を守るという観点で、経営者が認識すべき「3原則」と、CISO（最高情報セキュリティ責任者）など担当幹部に指示すべき「重要10項目」が示されている。同省はこのガイドラインの活用により、経営者のリーダーシップの下でサイバーセキュリティ対策が実現されることを期待している。企業戦略の一部として経営者が責任を持って対策の内容や優先順位を判断することが求められているといえよう。そのための第一歩が、客観的な判断基準を持って自社のセキュリティ対策状況を網羅的に可視化し評価することなのである。

『ITソリューションフロンティア』2016年10月号から転載

十川 基（そがわはじめ）
ストラテジーコンサルティング部主任セキュリティコンサルタント

中島由宏（なかじまよしひろ）
ストラテジーコンサルティング部副主任セキュリティコンサルタント