CSIRTを進化させる次の一手

本当に必要なセキュリティ施策の導き方
リスクスコアの算出フレームワーク活用術

PwCコンサルティング合同会社　ディレクター　辻　大輔
PwCコンサルティング合同会社　マネージャー　渕　遼亮

1. はじめに

限りある予算・人的リソースを踏まえて、次の一手として何をすべきか――。CSIRTの現場の多くでは、優先すべき施策について意見が割れているのが実情です。

セキュリティ対策が不十分という認識を持つ企業や組織は、各種法令やガイドラインを頼りに基本的なセキュリティ機能の整備を行っていることでしょう。一方、各種法令やガイドラインで求められる基本的なセキュリティ機能を具備した企業には、次の一手を導く万能な教科書はないため、自社のビジネスや組織、保有資産や施策導入状況などに鑑み、講じるべき施策を自ら選択する必要があります。この選択の際に重要なことは、サイバー攻撃への対処、セキュリティガバナンスの強化、あるいはセキュリティ業務負荷の解消といった性質の異なる課題であっても、その課題が持つ「リスク」を見極め、優先順位を設定することです。リスクを見極める「目」がなければ、費用対効果の小さい施策を講じてしまう、あるいは、施策の必要性を経営層に訴求できず導入が進まないなどといった課題に直面することでしょう。

今回は、上記の解決策として「リスクスコアの算出フレームワーク」の構築・活用を紹介すると共に、次に実施すべき施策を導く方法について記載します。

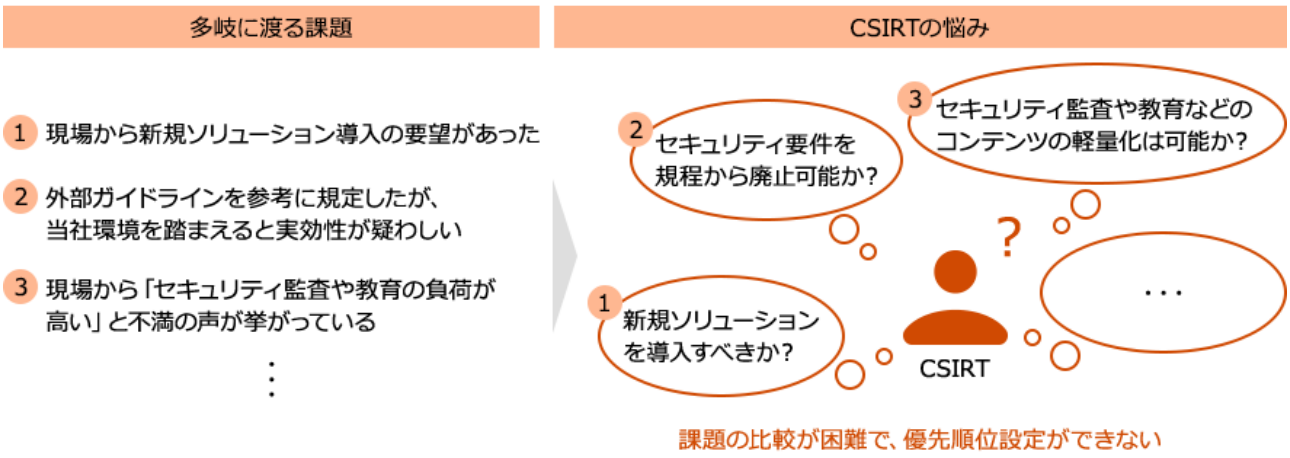
2. CSIRTが抱える課題

ビジネスのデジタル化が進むに連れ、セキュリティは企業にとって重要な経営課題となりました。CSIRTの活動は自ずとビジネスとの結びつきが強くなり、マネジメント層、あるいはビジネスの現場から多種多様な要望や依頼が届くようになりました。一方、CSIRTの活動には、未だ企業の生産性に対する効果が見えづらいことを理由に、十分な予算や人的リソースが配分されずに、多様な要望や課題は山積したままになっているケースが少なくありません。

限りある予算やリソースを何に投じるかは、CSIRT、ひいては企業にとって重要な意思決定です。しかし、CSIRTが抱える課題や要望は多岐にわたるため、同じ軸で重要性を評価することが困難です。そのため、自社にとって本当にやるべきことなのかを議論して優先順位を決定するというプロセスが不十分なまま、「説明が容易な新規ソリューション」、「他社採用の施策」、「難易度が低い保守的な施策」など、必要性を疑う施策が実行計画に含まれることもあります（図表1）。

小さなリスクの対応にリソースを投じて大きなリスクが見過ごされることはあってはなりません。こうした事態を避ける上で、自社の環境や既存の対策を踏まえて、リスクや効果を適切に評価するための仕組みであるリスクスコアの算出フレームワークを整備し、自社がやるべき施策の意思決定に活用することが有効です。

図表1.CSIRTが取り扱う課題



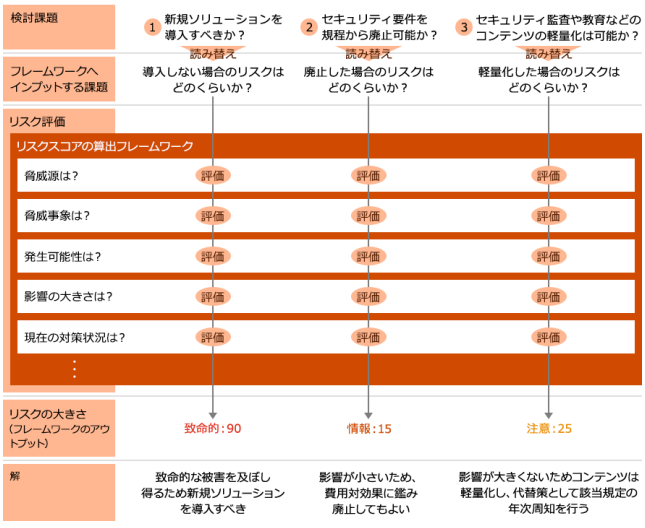
3.「リスクスコアの算出フレームワーク」とは

リスクスコアの算出フレームワークの1つに、米国標準技術研究所（NIST）が発行する”National Institute of Standards and Technology Special Publication 800-30 rev1, Guide for Conducting Risk Assessments, September 2012”（邦題『リスクアセスメントの実施の手引き』。以下、NIST SP800-30）があります。

NIST SP800-30におけるリスクアセスメントの実施プロセスは「脅威源を特定する→脅威事象を特定する→脆弱性と素因的条件を特定する→（脅威事象が発生する）可能性を特定する→影響の大きさを特定する→リスクを判断する」から構成されます。

「脅威源」「脅威事象」と聞くと、いわゆるサイバー攻撃や脆弱性情報で多く用いられる用語であることから、CSIRTが抱えるさまざまな課題を同一のフレームワークで評価することは困難に思えるかもしれません。しかし、サイバー攻撃と性質の異なるガバナンスや人材育成の問題であっても、その課題が残存すればどのような脅威事象が発生するのかをひも解くことで、そのリスクを導き出すことが可能です。リスクスコアの算出フレームワークは、多様な課題を一律の指標でリスクの大きさとして算定するツールであり、次の一手として何をすべきかを、リスクの大きさから客観的に判断できる効果を持ちます。

図表2：リスクスコアの算出フレームワークの活用



4. リスクスコアの算出フレームワークの活用

リスクスコアの算出フレームワークの活用によって、前述のような講じるべき施策の優先度の決定だけでなく、CSIRTに寄せられる検討課題にも、解を見出すことが可能になるでしょう。以下に例を記し、本コラムを締めくくりたいと思います（図表2）。

（1）新規ソリューションを導入すべきか？

リスクスコアの算出フレームワークを用いることで、新規ソリューションがもたらす効果、つまりソリューション自体がリスクをどの程度低減させるか、その大きさを評価することが可能になります。新規ソリューション導入の際に毎回リスク評価を行い、導入費用に鑑みながらデータとして蓄積することで、自社としての費用対効果の指標を構築することができ、施策の導入の是非を検討することができるようになります。

（2）セキュリティ要件を規程から廃止可能か？

セキュリティ規程の中には、外部のガイドラインや他社事例が引用元となり、自社に鑑みるとその効果が疑わしい要件が存在している場合があります。リスクスコアの算出フレームワークで、該当する要件を廃止した場合のリスクの大きさを算出できるため、要件の持つ効果が薄いことを客観的に証明できれば、スムーズに廃止へと導くことができます。

また、規定に要件を追加する場合も同様です。例えば、外部のガイドラインが求めるセキュリティ要件が、既に自社では技術的安全管理措置によってリスク低減済みであるなど、要件を追加しない場合のリスクを明らかにすることで、自社の規程に採用すべきかを判断することができます。

（3）セキュリティ監査や教育などのコンテンツの軽量化は可能か？

監査項目や教育コンテンツなどは年を追うごとに肥大化する傾向があり、対象者の業務負担を軽減するために、その分量の削減に迫られるケースがあります。リスクスコアの算出フレームワークを用いることで、各コンテンツの効果を横並びに評価することができ、効果の高いコンテンツに絞り込むことで、一定の水準を保ちつつ、対象者の業務負担を軽減することが可能になります。

お問い合わせ

PwCコンサルティング合同会社
〒100-6921　東京都千代田区丸の内2-6-1 丸の内パークビルディング
Tel：03-6250-1200（代表）　Mail：jp_cyber_inquiry@pwc.com