サプライチェーンリスクと対策アプローチ ～企業における情報セキュリティ実態調査を踏まえて～

サプライチェーン構造の複雑化に伴い、セキュリティリスクが日々増加している。サプライチェーンのセキュリティ統制を効率的に、かつ効果的に実施するためには、現実的な統制範囲を定義し、対象先の重要度に応じた水準を策定したうえで、モニタリングの継続的な強化が求められる。

セキュリティ人材と予算の不足

NRIセキュアテクノロジーズ（以下、NRIセキュア）は2002年より毎年、企業における情報セキュリティ実態調査を実施し、今年2月に20回目となる調査レポート「NRI Secure Insight 2022[1)]」を公表した。

レポートによると、日本企業の約9割が自社にセキュリティ人材が「不足している」と回答している。特にセキュリティ戦略・企画を策定する役割が期待されるマネジメント層が不足しており、現場のセキュリティ担当者が日々の対策実行や運用業務だけでなく、本来マネジメント層が実施すべき戦略・企画の策定も兼務せざるを得ない状況となっていることが推察できる。

セキュリティ人材不足の課題は過去10年以上改善がみられておらず、長年続く人材の不足感を解消するには、「人材の拡充」と「業務の効率化」の両観点において、多面的な施策の実行と継続的な改善が求められる。

また、予算面については、「セキュリティ関連予算の割合がIT関連予算の10%未満」と回答した企業は、日本全体の約7割に対し、米国・豪州では全体の3割程度であった。日本が米国・豪州の企業と比べて、セキュリティ予算獲得に対する苦労・悩みがうかがえる。

セキュリティ予算獲得には、経営層とのコミュニケーションに「経営者の視点」を取り入れ、セキュリティを「自分事」として捉えられるための創意工夫が求められる。具体的には、①同業他社の事例や対策状況を引き合いに出す、②新しいセキュリティ対策が全社のDX推進や利益に貢献するかを伝える、③自社起因で発生したインシデントの影響がサプライチェーン全体に波及する可能性を伝えることなどが効果的である。

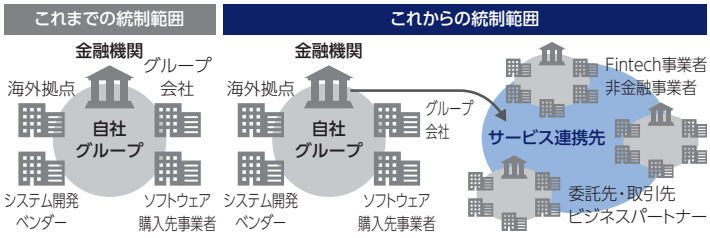
金融機関のサプライチェーン構造の複雑化に伴うリスクと課題

IPAが今年1月に公表した「情報セキュリティ10大脅威 2023［組織編］[2)]」において、「サプライチェーンの弱点を悪用した攻撃」は2位であった（前年度3位）。

これまで金融機関において、グループ会社や海外拠点、システム開発ベンダー等がセキュリティの統制対象であった。しかし、近年、Fintech事業者や非金融事業者（組み込み型決済・保険・貸付・投資・銀行などへの提供者）、その他多数の委託先・取引先企業を介してエンドユーザに多様な金融サービスを提供する機会が増え、サプライチェーン構造の複雑化に伴いセキュリティを統制しなければならない対象範囲が拡大している（図表1）。

サプライチェーンに関するセキュリティインシデントとしては、2023年1月に大手保険会社において、外部委託先が起因となった情報漏洩事故が発生した。サプライチェーンのセキュリティリスクを低減するためには、各企業のセキュリティ対策状況の把握と継続的な対策強化が必須である。

図表1　拡大するセキュリティの統制範囲

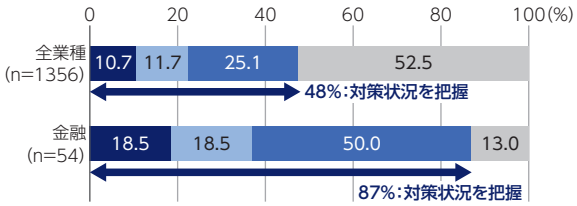


(出所) 野村総合研究所

NOTE

1) 回答数2,877社（日本：1,800社、アメリカ：547社、オーストラリア：530社）。
https://www.nri-secure.co.jp/download/insight2022-report
2) 2022年に発生した社会的に影響が大きかったと考えられる情報セキュリティの事案から、IPAが脅威候補を選出し、審議・投票を行い決定したもの。
（出所）「IPA 情報処理推進機構」
https://www.ipa.go.jp/security/vuln/10threats2023.html
3) 企業が、委託先や取引先の製品・サービスが規制・財務・オペレーションの面で負の影響を発生させないようにするためのリスク管理プロセス。
4) NRIセキュアでは、①～③の一連のアプローチを元にWeb上で複数の拠点のセキュリティ対策状況を管理できるVRMツールとしてSecure SketCH（セキュアスケッチ）を提供している。Secure SketCHは、Web上で75問の設問に回答するだけで、各種ガイドラインに沿ったセキュリティ評価を「得点」や「偏差値」で定量的に見える化し、効率的に対策を推進できるセキュリティSaaS。サプライチェーンのセキュリティ対策状況の把握と対策レベル向上にも寄与する。
https://www.nri-secure.co.jp/service/solution/secure-sketch
5) NRIセキュアのSecure SketCHによるセキュリティ評価結果を、京都銀行が統合報告書に掲載。
https://www.nri-secure.co.jp/news/2022/0907

図表2　国内の委託先やビジネスパートナーのセキュリティ対策状況の把握



■ セキュリティ対策状況が改善されていることを定期的に確認している
■ セキュリティ対策状況を把握し、自社の水準をみたすため改善を要求している
■ セキュリティ対策状況を把握している
■ セキュリティ対策状況を把握していない

（注）該当なしを除く
（出所）野村総合研究所

レポートによると「国内の委託先やビジネスパートナーのセキュリティ対策状況を把握している」と回答した日本企業は、約48%であった。さらに金融機関に限れば、約87%と高いことがわかった（図表2）。

しかし、金融機関の把握割合が高いからといって楽観はできない。それはセキュリティ対策状況の把握の方法に課題があるためである。各企業の対策状況を把握するための手段として、一般的にセキュリティチェックシートを用いたアンケート形式の評価を実施する場合が多い。サプライチェーンに対するセキュリティ対応の課題を調査したところ、「アンケートでセキュリティを確認しているが実効性の観点で不安がある」という回答が全体の回答よりも金融機関の場合は約28ポイントも突出して高いという結果が出ており、アンケート評価に実効性の不安を感じていることがわかる。

サプライチェーンリスクへの対策アプローチ

限られた人材と予算の中で、サプライチェーンを構成するすべての企業のセキュリティ対策状況を把握し、各社に対して同水準のセキュリティを要求することは、いずれも困難を要する。

まずは、①連携する情報やサービスの重要性（保有情報や事業依存度）などビジネス環境に即した評価軸を定義し、②定義した軸により各企業の重要度（高・中・低など）を分類し、③重要度に応じたセキュリティ水準を策定した上でアンケート評価を実装する、という一連のアプローチが必要である。また米国では大量の拠点のリスク管理を効率的かつ継続的に実現するために、VRM（Vendor Risk Management）[3]ツールの活用が進む。日本においても、Web上で複数の企業のセキュリティ対策状況を管理できるようなVRMツールへの注目が高まっている[4]。

また③の評価における実効性の不安を解消するためには、アンケートのバイアスを低減させるために、SRS（Security Rating Services）による客観的な視点の評価を組み合わせる方法もある。SRSはインターネット上の公開情報をもとに、公開サーバやネットワーク機器におけるセキュリティ上望ましくない設定を自動的に検出して、企業のセキュリティ対策状況を定量的に評価できるツールであり、近年日本国内の金融機関でも導入が進んでいる[5]。

サプライチェーンのセキュリティ統制を効率的に、かつ効果的に実施するためにVRMやSRSのようなツールの活用も今後の選択肢の一つとして考えたい。

Writer's Profile

藪内 俊平 Shumpei Yabuuchi
NRIセキュアテクノロジーズ
セキュリティコンサルタント
専門はセキュリティリスク評価
focus@nri.co.jp