04

セキュリティ

企業のセキュリティ投資意向と脅威認識

NRIセキュアテクノロジーズが実施した企業のセキュリティ予算と脅威認識についての調査によると、セキュリティ投資は防御・検知が中心ながら、追加投資ではレジリエンス・ガバナンスへの意欲が高く、警戒する脅威はランサム攻撃であった。ヒトの判断や運用の隙を突く攻撃への警戒も根強い。

NRIセキュアテクノロジーズは、日本企業を対象にサイバーセキュリティに関する実態調査を実施し、「NRI Secure Insight 2025[1)]」を公表した。この実態調査は2002年から始まり、今年で23回目となる。本稿では、その中から比較的動きの大きかったセキュリティ予算の意向と企業の脅威認識という2つのトピックを取り上げる。

【セキュリティ予算】追加投資の伸びが大きいのはレジリエンスとガバナンス

企業のセキュリティ予算の意向を把握するため、NIST CSF 2.0[2)](米国国立標準技術研究所が策定したサイバーセキュリティフレームワーク）をベースに調査し、分析した。NIST CSF 2.0は、サイバーセキュリティの取り組みを「統治」「特定」「防御」「検知」「対応」「復旧」の6機能[3)]で整理している。2024年の改訂で新しく「統治（ガバナンス）」が加わり、技術対策だけでなく、経営レベルの意思決定や責任分担まで含めている。

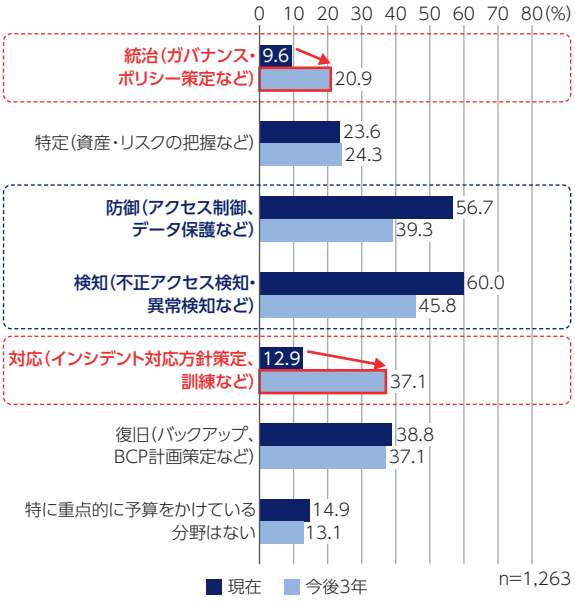
本調査では、6機能のうち「現在、相対的に予算を多くかけている分野」と、「今後3年間で予算を増やしたい分野」をそれぞれ尋ねた。

その結果、前者の「現在、相対的に予算を多くかけている分野」との回答が多かったのは「検知」（60.0%）と「防御」（56.7%）であった（図表1）。現在の予算配分は、入口対策や不正アクセスの検知といった技術的な備えに厚みがあることが分かる。これは、従来の企業のセキュリティ対策が、社内外の境界で入口を守る発想（境界防御）中心であったことや、「検知」「防御」領域のセキュリティ製品（EDR、ファイアウォール等）が豊富であることが背景にあると推察される。

一方、「今後3年間で予算を増やしたい分野」として回答が多かったのは、「検知」（45.8%）、「防御」（39.3%）、「対応」（37.1%）で、「検知」と「防御」は水準は下がるものの依然上位にある。ただし、現在の配分と今後の増額意向を比較すると、「対応」と「統治」が大きく伸びている。「対応」はレジリエンス（回復力）を構成する機能の一つであり、インシデント発生時の初動、封じ込め、演習、外部専門家との連携など、侵入されることを想定して被害を最小限に抑える備えを指す。

他方、「統治（ガバナンス）」は、どのリスクを優先し、誰が判断し、どこまで責任を持つかを平時から明確にしておく取り組みである。前者は有事の実効性、後者は平時の意思決定と説明責任を支える。企業は、防御・検知を土台として維持しつつ、追加投資では対応力と統治の整

図表1　セキュリティ予算の現在と今後



（注）最大3つの複数選択可
（出所）NRIセキュアテクノロジーズ「NRI Secure Insight 2025」

NOTE

1) 日本企業の回答数1,236社。
https://www.nri-secure.co.jp/download/insight2025-report
2) https://www.nist.gov/cyberframework
3) 各機能の概要は以下。
統治：組織のサイバーセキュリティリスク管理戦略、意思決定への期待、およびポリシーを設定し、伝達し、監視する
特定：組織の現在のサイバーセキュリティリスクを理解する
防御：組織のサイバーセキュリティリスクを管理するための保護策を使用する
検知：サイバーセキュリティ攻撃や侵害の可能性を発見し、分析する
対応：検出されたサイバーセキュリティインシデントに関する対応を行う
復旧：サイバーセキュリティインシデントに影響を受けた資産や業務を復旧する
4) 2024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/10threats/10threats2025.html

備に厚みを増そうとしているスタンスが読みとれる。

【企業の脅威認識】ヒトに起因する内部脅威を警戒

IPAが毎年公表する「情報セキュリティ10大脅威[4]」は、日本企業のセキュリティ担当者が脅威動向を把握するための重要な参照情報となっている。今回の調査では、このIPAの10大脅威（2025年版）に掲載されている項目を使い、企業が実際にどの脅威を警戒しているかを直接尋ねた。

調査の結果、「ランサム攻撃による被害」が企業の警戒度でも1位（80.8%）であった。2位以下の項目と25ポイント以上の差がついており、事業停止の恐れがあるランサムウェア攻撃に対する警戒感の高さが際立っている。

上位5項目の中には、「内部不正による情報漏えい等」（2位、54.8%）、「ビジネスメール詐欺」（4位、46.2%）、「不注意による情報漏えい等」（5位、42.4%）も入っている。これらに共通するのは、人の判断や日常業務の運用の隙を突いて被害が成立しやすい点である。内部不正や不注意による情報漏えいは内部者の悪意やミスに起因するが、ビジネスメール詐欺もまた、送金や承認といった業務プロセスと人の判断を狙う攻撃である。このような人的要因のリスクは技術的な防御策だけでは抑えにくく、従業員教育、権限管理の徹底、業務プロセスの見直しを含めた組織的な備えが求められる。

また、「サプライチェーンや委託先を狙った攻撃」は企業全体では7位（33.0%）とIPAの順位に比して低くとどまった。ただし従業員規模による違いが大きく、従業員1万人以上の企業（57社）の中では4位（57.9%）、千人～1万人未満の企業（335社）の中で4位（42.1%）、千人未満の企業（871社）で8位（27.9%）と、規模が大きいほど警戒感が高いという傾向がある。大企業が警戒するこのリスクも、規模の小さい取引先には十分に意識されていない可能性があり、リスク管理が脆弱な取引先がサプライチェーン全体の弱点になりうる。個社の問題として閉じず、サプライチェーン全体でリスクを捉える視点が求められよう。

図表2　企業の警戒項目（IPA10大脅威2025）

IPA脅威の順位	本調査の順位(注)	脅威名	割合
1位	1位	ランサム攻撃による被害	80.8%
4位	2位 (+2)	内部不正による情報漏えい等	54.8%
3位	3位	システムの脆弱性を突いた攻撃	53.3%
9位	4位 (+5)	ビジネスメール詐欺	46.2%
10位	5位 (+5)	不注意による情報漏えい等	42.4%
5位	6位 (−1)	機密情報等を狙った標的型攻撃	39.7%
2位	7位 (−5)	サプライチェーンや委託先を狙った攻撃	33.0%
6位	8位 (−2)	リモートワーク等の環境や仕組みを狙った攻撃	30.9%
8位	9位 (−1)	分散型サービス妨害攻撃（DDoS攻撃）	10.6%
7位	10位 (−3)	地政学的リスクに起因するサイバー攻撃	7.2%

(注) IPA10大脅威の項目ごとに企業の警戒度合いを調査。括弧内の数字は、"IPA脅威の順位"との差分を示す。最大5つの複数選択可。他の選択肢として「その他／特になし」
(出所) 独立行政法人情報処理推進機構（IPA）「情報セキュリティ 10大脅威 2025（組織編）」及びNRIセキュアテクノロジーズ「NRI Secure Insight 2025」

Writer's Profile

野口 智矢 Tomoya Noguchi
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