企業情報セキュリティの実態と今後のセキュリティ統制、AI活用の展望

セキュリティ課題が多様化する中、NRIセキュアテクノロジーズは「企業における情報セキュリティ実態調査」を実施した。ランサムウェア被害下でもVPNは利用が続く、メールなりすまし対策のDMARCは導入が進むも活用に課題が残る、生成AIの活用認識が米豪と異なるなど、実態が明らかになった。

多発するインシデント、進む制度対応、新たに浮上する技術活用―セキュリティを巡る課題は多様化している。本稿では、NRIセキュアテクノロジーズが2024年に実施した、「企業における情報セキュリティ実態調査[1]」の内容から、注目度の高い三領域として、VPN、DMARC、生成AIの三つを取り上げ、実態と課題を読み解く。

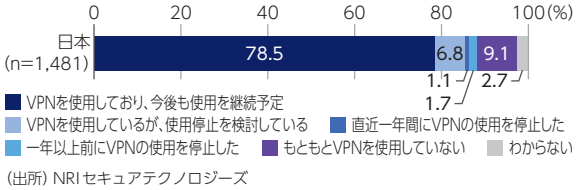
依然として根強いVPN活用ニーズ

2024年春、委託業務を担う企業がランサムウェア攻撃を受け、複数の委託元に関わる情報が漏洩する重大なインシデントが発生した。攻撃者はVPNを経由してネットワークに侵入し、業務関連情報を窃取した。

頻発するランサムウェア事案を受け、一部企業ではVPNの使用そのものを見直す動きも見られるが、調査によれば、回答企業の78.5%が「VPNを今後も使用予定」と回答しており、継続利用が一般的な選択肢となっている[2](図表1)。

VPNが今後も主要なリモートアクセス手段として広く利用されるのであれば、VPNという仕組み自体を問題視せずに、VPNを含んだアクセス経路の統制をどう高度化するかが課題となる。VPNの安全な運用には、脆弱性管理、アクセス制御、パッチ適用、ログ監視など、複合的で継続的な運用が不可欠であり、一般的なセキュリティ対策ではもはや実効性を担保できない。より高度な安全な設計と運用体制を構築する必要がある。

図表1　VPNの使用状況



(出所) NRIセキュアテクノロジーズ

DMARCのレポート分析に課題

DMARC[3]とは、メールの送信者が正規のドメインであることを確認し、不正なりすましをブロックする認証技術である。調査時点での日本企業におけるDMARC実施率は29.8%であった。実施率が約9割である米豪と比べれば依然として低いが、2023年の13.0%からは大幅に伸長しており、今後も普及が進むと見られる。

導入理由としては、Gmailの送信者ガイドラインへの対応と、なりすましメールへの対策の二つが主に挙げられている。現時点では、認証失敗時にもメールを通常通り配信する「None」ポリシーを設定している企業が大半だが、なりすまし対策の実効性を高めるためにも、今後は「Quarantine[4]」や「Reject[5]」といったより強いポリシーへの移行を検討する企業が多いと見込まれる。

日本企業の多くが共通して抱えている課題は、「DMARCレポートの分析ができていない」という点である(図表2)。DMARCを導入したことで可視化された情報は得られるものの、その内容が煩雑であり、十分な分析・活用にまで至っていない企業が多いというのが実情だ。

QuarantineやRejectでの運用が進んでいる米豪では「対象ドメインの洗い出しができていない」といった課題が表面化している。

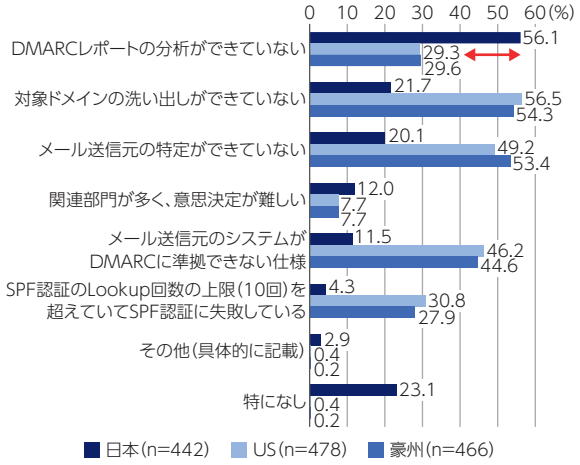
こうした課題は、今後日本でも直面し得るものである。もちろん日本企業における喫緊の課題は、可視化されたレポートの内容を分析し、実運用に活かす体制の整備である。その上で、将来のスムーズな高度化にそな

野村総合研究所　金融イノベーション研究部　©2025 Nomura Research Institute, Ltd. All rights reserved.

NOTE

1) 回答数2,491社（日本：1,481社、アメリカ（US）：507社、オーストラリア（豪州）：503社）。https://www.nri-secure.co.jp/download/insight2024-report
2) 一方で、「VPNを使用しているが、使用停止を検討している」と回答した企業は6.8%だった。
3) Domain-based Message Authentication, Reporting and Conformanceの略。メールに表示された送信元（ヘッダーFrom）ドメインから正規に送信されたメールであるかどうかを認証する、送信ドメイン認証技術。https://www.nri-secure.co.jp/glossary/dmarc
4) Quarantineは、DMARCで認証に失敗したメールを迷惑メールフォルダなどに隔離するよう受信側に指示するポリシー。
5) Rejectは、DMARCで認証に失敗したメールを受信側で拒否するよう指示する、最も厳格なポリシー。

図表2　DMARC実施の課題



（注1）DMARCを実施していると回答した企業のみを対象
（注2）複数選択可
（出所）NRIセキュアテクノロジーズ

えて、今後は送信元や対象ドメインの特定と棚卸、準拠が困難なシステムへの対応などの準備も必要になる。DMARCの導入はゴールではなくスタートである。運用と改善の積み重ねによって、その真価が発揮されていくものと認識すべきだろう。

日本と米豪で中身が異なる生成AI活用

限られたリソースの中で高度なセキュリティを維持することが求められる今、生成AIはその一端を担う手段となり得るかもしれない。「AIを活用して効率化したいセキュリティ対策」に対する回答では日本と米豪で明確な違いが見られた（図表3）。

日本企業の回答でまず目につくのは、「特になし」が3位に入っている点である。この結果は生成AIの活用可能性に関して、明確な活用イメージを持てていない企業が一定数存在することを示唆している。また、「攻撃の検知」、「脆弱性の検知」が上位に挙がっている点からは、生成AIを従来のセキュリティ製品の延長として捉えている傾向がうかがえる。これらの背景には、生成AI活用の具体的な事例共有がまだ十分とは言えず、各社が導入の糸口を見出しにくい状況があると考えられる。

一方、米豪企業では、「セキュリティルールの作成」や「セキュリティ対策の立案」といった、これまで自動化が進みにくかった思考的・計画的な領域に生成AIを活用しようとする意識が見られる。煩雑さや属人性ゆえに継続的な実施が難しかった業務が、生成AIの補完によって“定期的に見直すことができる業務”へと変われば、統制の硬直性は緩和され、状況に応じた柔軟なセキュリティガバナンス構築が可能になると予想される。

図表3　AIを活用して効率化したいセキュリティ対策

	日本（n=1,481）	US（n=507）	豪州（n=503）
1位	34.0% 脆弱性の検知	49.1% セキュリティルールの作成	50.9% セキュリティ対策状況の把握
2位	32.3% 攻撃の検知	43.8% セキュリティ対策状況の把握	41.9% セキュリティ対策の立案
3位	25.7% 特になし	37.5% セキュリティ対策の立案	40.6% セキュリティルールの作成
4位	24.9% セキュリティ動向に関する情報収集	33.3% 脆弱性の検知	36.4%
5位	21.8% セキュリティルールの作成	30.8% セキュリティ動向に関する情報収集	31.0% 攻撃の検知

（注1）最大3つの複数選択可
（注2）他選択肢：インシデント対応／セキュリティ訓練／その他（具体的に記載）
（出所）NRIセキュアテクノロジーズ

Writer's Profile

中土井 洋平太 Yoheita Nakadoi
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