スポットライト：日本

日本のCISOとそのチームを取り巻く環境は、ますます複雑になり刻々と変化しています。今回の調査結果から、日本のサイバーセキュリティに携わるリーダーたちが、サイバー攻撃に対する防御（61%）、ハイブリッド型勤務社員の保護（52%）、Zero Trustアーキテクチャの導入（47%）の3つを主な課題と捉えていることが明らかになりました。

日本のサイバーセキュリティに携わるリーダーが直面する主な課題

61%
サイバー攻撃に対する防御

52%
ハイブリッド型勤務社員の保護

47%
Zero Trustの導入

耐障害性が高く目的に適ったサイバーセキュリティ体制を整備する上で乗り越えなければならない数々の課題があります。回答者は、サイバーセキュリティのアーキテクチャに関する重要課題として、57%が自社ITサプライチェーンに対する監視の限界、55%がアプリケーション保護におけるVPNとIPアドレスへの過剰依存、52%がパブリッククラウドに保存された自社のアプリケーションやデータの脆弱性を挙げました。これらの結果は、サイバーセキュリティが、従来のサイロ型の問題から、真に組織全体の規律へと変化していることを踏まえると、ビジネスにとって潜在的な頭痛の種になることも見えてきました。

今回の調査結果から、日本の回答者の81%が過去12か月間に何らかのサイバーセキュリティインシデントを経験しており、その内訳を見ると、中規模の企業で数値が高くなっていることがわかりました。日本で最も多くのサイバーセキュリティインシデントを経験した業界はメディア・電気通信、ビジネス・プロフェッショナルサービス、金融サービスでした。日本の回答者の40%が10回未満、60%が10回以上のサイバーセキュリティインシデントを過去12か月間に経験しています。

さらに、この調査結果から判明した日本で最も一般的なサイバーセキュリティインシデントは、マルウェア（53%）、ビジネスメール詐欺（48%）、ランサムウェア・スパイウェア（43%）。また、攻撃者の主な目的は、ランサムウェアの埋め込み（73%）、スパイウェアの埋め込み（69%）、データ流出（66%）と報告されています。

サイバーセキュリティインシデントの主な原因：

53%
マルウェア

48%
ビジネスメール詐欺

43%
ランサムウェア/スパイウェア

日本でのサイバーセキュリティインシデントが頻発しているにも関わらず、インシデントを回避するために「十分な対策を講じている」と回答したのは46%に留まりました。

日本の回答者が抱えるサイバーセキュリティアーキテクチャの最大の課題は、リーダーシップチームのトレーニング（19%）が最も多く、その後、ネットワークの動向分析（17%）、侵入防止システム（16%）、次世代型ファイアウォール（16%）と続きました。日本でSASEの実装は82%で、アジア太平洋地域全体の平均である80%と比較しても導入が進んでいることがわかりました。現時点で導入が遅れているのは、多要素認証、クラウドアクセスセキュリティブローカー（CASB）、暗号化で、回答者の17%が、まだいずれも導入していないと述べました。

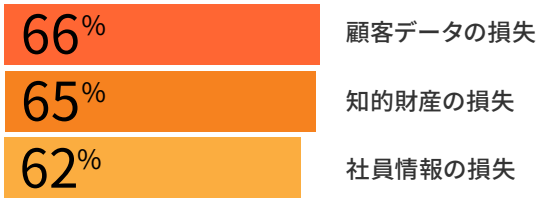
サイバーセキュリティ対策の準備状況で日本の回答者がより大きな課題と指摘したのは、資金不足（65%）よりも人材不足（72%）でした。こうした課題を抱えながらも、ほぼ9割の回答者が、サイバーセキュリティインシデントを検出してから24時間以内に解決できたと回答しています。

対策を支えるには長期的な投資が必要になります。日本の回答者の半数以上（53%）が、組織のIT予算全体のうち16%～25%がサイバーセキュリティに振り分けられていると回答しました。IT予算の21%以上をサイバーセキュリティに投資する可能性が高いと回答した業界の上位は、メディア・電気通信（54%）、エネルギー、公共料金（40%）、建設・不動産（38%）でした。

日本の回答者のおよそ3分の2（64%）が、6～15のサイバーセキュリティソリューションを導入済みであると回答しました。また、サイバーセキュリティアーキテクチャの一部としてソリューションを増やす計画があり、ソリューションを増強する予定と答えた回答者は76%に上りました。

サイバーセキュリティインシデントに伴う損失は、無視できるものではありません。日本の回答者のおよそ4分の3（71%）が、過去12か月間のサイバーセキュリティインシデントによる影響が100万ドル（約1億4,000万円）を超えたと回答しています。また、200万ドル（約2億8,000万円）以上の影響を受けた回答者も54%に上りました。サイバーセキュリティインシデントの影響が及んだのは、金銭面だけではありません。金銭面での影響以外で最大の損失として、顧客データの損失（66%）、企業秘密の損失（65%）、社員情報の損失（62%）が報告されました。

金銭面の影響以外での最大の影響



サイバーセキュリティインシデントの結果はそれだけに留まりませんでした。日本では、「ハイブリッド型勤務を減らした、または制限した」と回答したのは約48%、「ハイブリッド型勤務の拡大を保留した」は42%、「社員をレイオフせざるを得なかった」は37%でした。サイバーセキュリティインシデントを経験した回答者の89%が、インシデントを開示しました。

推奨事項

1. 適切な対策を講じることが第一。企業は統合型ソリューションに戦略的に投資して、ますます複雑になる脅威状況にZero Trustなどのアプローチで対応する必要があります。

2. 導入するソリューションの数は、少ないほど効果的。SASEを導入しセキュリティアーキテクチャを合理化することが、業界全体の人材不足の影響を軽減し、サイバーセキュリティを成功へと導くことになります。

3. 取締役会をはじめとする社内のセキュリティ文化の強化に時間を費やす。セキュリティ対策を進めるには、まず理解を深め、意識を高めることが先決です。

4. 強力なセキュリティ文化を確立する。会社にこうした文化が根付けば、CISOはインシデントの発生を待つことなく体制強化のビジネスケースを作成でき、甚大な財務損失のリスクを積極的に軽減できます。

5. サイバーセキュリティのサイロ化は徹底的に排除する。経営幹部はサイバーセキュリティをミッションクリティカルと考え、企業は自社スタッフ、サプライヤー、クライアントがベストプラクティスを順守するように総合的なアプローチをとる必要があります。

Cloudflareは、企業がサイバーセキュリティ対策の実装でどの段階にあるか、セキュリティチームの準備がどのレベルにあるかに関係なく、現代のサイバーセキュリティの課題に対応できるようお手伝いします。Cloudflareのプラットフォームは、企業の規模、実装段階、対策の準備レベルを問わず、サイバーセキュリティを簡素化し、人材不足を補い、いかなるタイプのサイバー脅威に対しても堅牢な防御ができるよう企業を支えます。

Cloudflareのソリューションの詳細、また、営業担当による説明、またはPOCをご希望の方は、次をご覧ください。
https://www.cloudflare.com

Cloudflareでは、現行セキュリティ体制の評価や行動計画の策定についてご相談を承ります。人、アプリケーション、デバイス、ネットワーク、データのサイバーセキュリティ強化に、どうCloudflareを活用できるか、お気軽にお問い合わせください。

こちらより「未来を守る：アジア太平洋地域サイバーセキュリティ調査」*のAPJCレポートをダウンロードいただけます。

*「未来を守る：アジア太平洋地域サイバーセキュリティ調査」は、アジア太平洋地域のセキュリティ市場で実施された調査結果をまとめたレポートです。本調査は14市場、4,000名を超えるサイバーセキュリティ関連の意思決定者とリーダーを対象に実施されました。