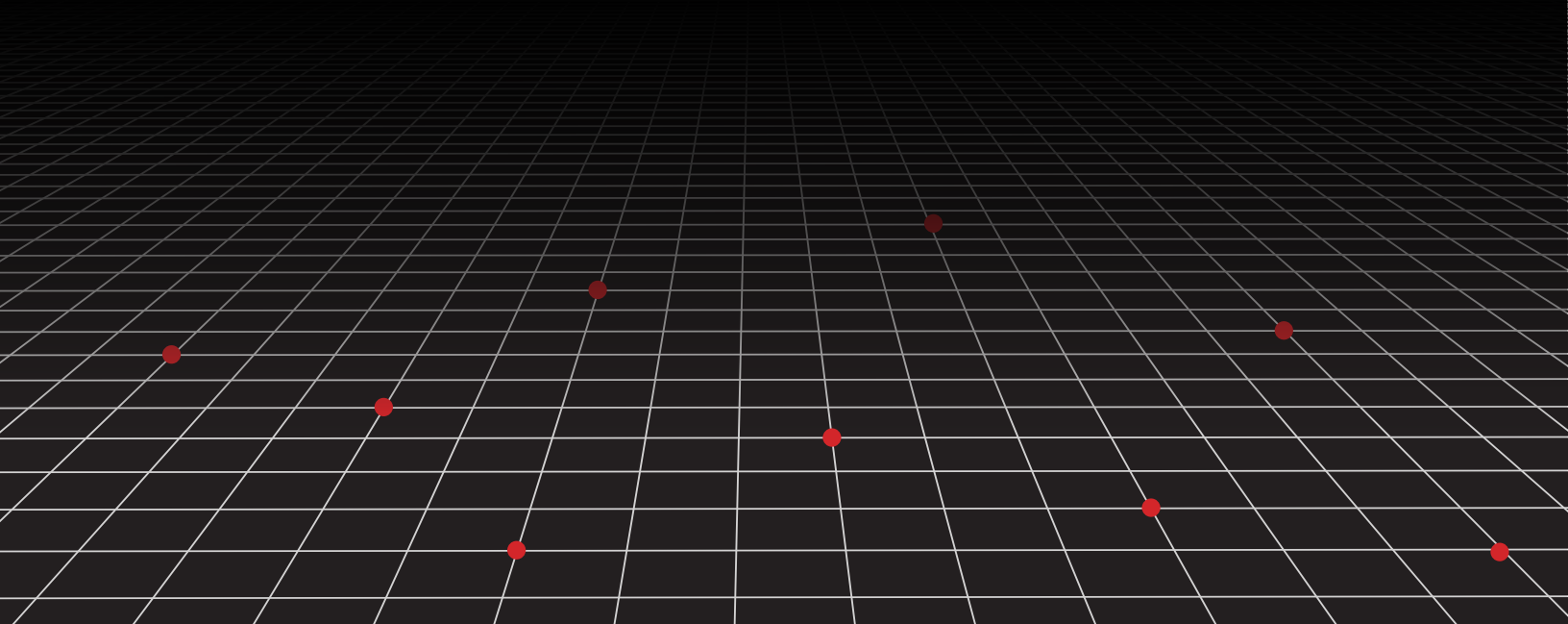
fastly

Fastly セキュリティリサーチレポート

岐路に立つサイバーセキュリティ

脅威とデジタル破壊が激化する時代に、
日本がサイバーセキュリティを強化するには



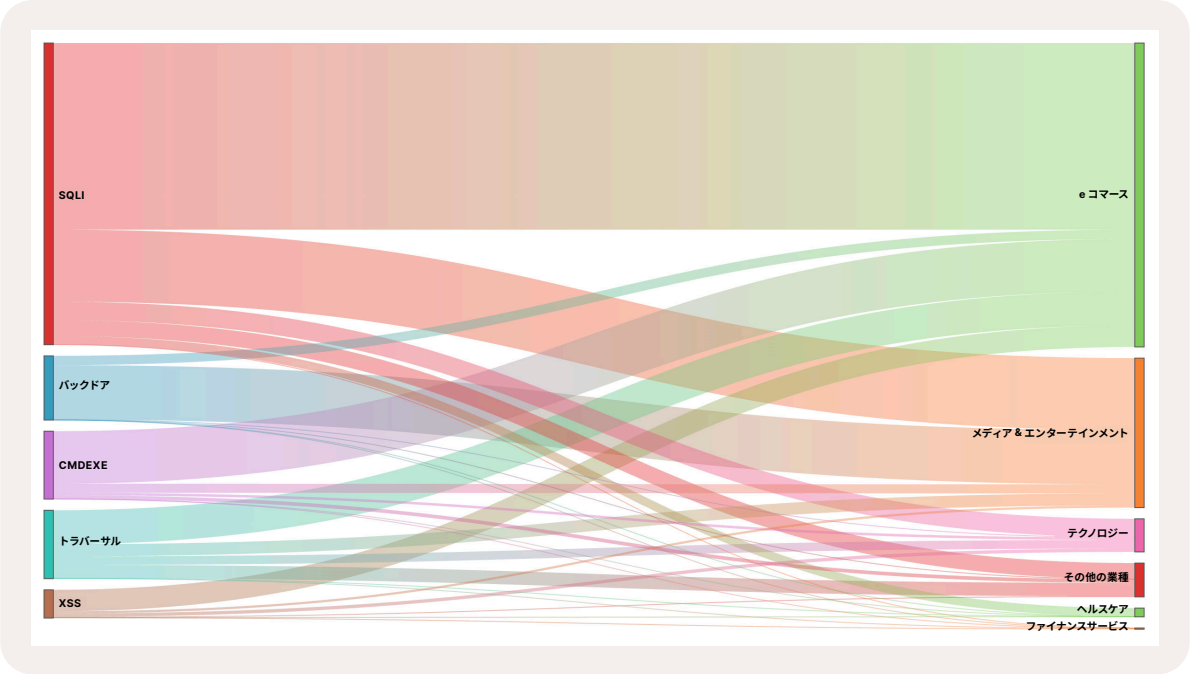
エグゼクティブサマリー

過去 12 か月を振り返ると、サイバーセキュリティの重要性は増し続けています。さらに CrowdStrike のアップデートで設定ミスが発生した際、何百万台もの Windows PC がオフラインになり、世界中がこの史上最大規模のサイバー障害の影響を受けました。

国際的なサイバー事件が見出しを飾ることが多い一方で、日本国内ではそれと同じくらい注視すべき脅威が着実に増加しています。2024 年 12 月、国内最大の金融機関である三菱 UFJ 銀行は、生体認証や企業プラットフォームなどのオンラインバンキングサービスを混乱させる大規模な DDoS 攻撃を受けました。この事件は、国家インフラとデジタルの信頼に対するリスクの高まりを明確にしています。

これらの出来事により、サイバーセキュリティは運用上の懸念事項から取締役会レベルの必須事項に昇格し、規制当局による監視が強化され、各セクターのリーダーが進化する脅威の状況に対応するため、より積極的でリソースを十分に備えたセキュリティ戦略に投資するようになりました。

このような状況を背景にサイバーセキュリティとデジタルレジリエンスを強化する必要性がこれまで以上に高まっていますが、過去 12 か月を詳しく見てみると、セキュリティプログラムは不安な状態にあることがわかります。現在、サイバーセキュリティの取り組みは以前よりもさらに激しい逆風に直面しています。このような逆風の大部分が、予算の精査や組織内でのサイバーセキュリティに対する責任の所在に関する混乱など、非技術的なものです。



Fastly が観測した日本最大の攻撃と、過去 *365* 日間に最も標的にされた業種 *(2024年5月 - 2025年5月)*

以前のグローバルセキュリティレポートでも述べたように、オンラインセキュリティは岐路に立たされています。そこで、企業による重要なサイバーセキュリティ問題への対処方法や業界の方向性についてより詳しいインサイトを得るため、Fastly は 2024 年後半にビジネス / 消費者市場調査会社 Sapio と共同でサイバーセキュリティに関して影響力を持つ世界中の 1,800 人の IT 意思決定者を対象に調査を実施しました。このレポートでは、日本に焦点を当て、企業が直面しているサイバーセキュリティの課題と、その克服に向けた今後の取り組みに関する詳細なインサイトが得られます。以下は主な調査結果です。

- **セキュリティへの取り組みは極めて不安定な状況にあります。**IT 意思決定者の 82% が今後 12 か月にサイバーセキュリティへの投資が増加すると予想する一方、この支出の結果は厳しく精査されることになります。セキュリティチームは、有効な防御戦略を実現するための予算を継続的に確保するため、経営陣を説得するのに苦労しています。経営陣には、デジタルトランスフォーメーションや IT の近代化など、他にも取り組むべき優先事項が多く、セキュリティへの取り組みが業務の足かせになっていると感じているのです。
- **組織はサイバーセキュリティ業務の拡大をめぐる課題に直面しています。**経営陣に対して自らの役割を正当化しようと苦慮する一方で、サイバーセキュリティの非効率性を示す懸念すべき兆候が見られます。回答者の 3 分の 1 以上がサイバーセキュリティ向けのリソースをどのように割り当てるべきか明確に把握していないと感じており、これが「過剰に投資している」という感覚につながっています。
- **企業が必要とする人材が市場で不足しています。**また、より多くのキャパシティが必要とされ、複雑さが増す中、サイバーセキュリティの取り組みを拡大する力が不足している兆候も見られます。従来、企業は高まるサイバーセキュリティのニーズに対応するため、より多くの人材に投資してきましたが、今年はアクセス可能な人材プールに対する大きな不満が見られます。そのため、進化するサイバーセキュリティのニーズに対処するには、スキル管理のプラクティスを見直す必要があります。
- **テクノロジーの複雑さがサイバーセキュリティの取り組みを妨げています。**企業がセキュリティ対策のスケーラビリティを求める中で、サイバー脅威に対抗するために組織が使用するテクノロジーもまた課題となっています。企業は依然として、インシデント対応などのサイバーセキュリティ業務を困難にする複雑で重複したツールセットに悩まされています。2024 年に発生した CrowdStrike の障害により、セキュリティ製品・サービスが注目を浴び、セキュリティ責任者は使用しているサイバーセキュリティツールのリスクとメリットに疑問を持ち始めています。

サイバーセキュリティへの支出が不足している可能性

適切な投資がなければ何も起こりません。サイバーセキュリティについても同じことが言えます。攻撃が増加してより巧妙になるにつれ、防御者はアセットを保護するために資金を投入する必要があります。調査では望ましい意図が示されたものの、現実にはいくつかの問題が浮き彫りになりました。

2023 年当時、調査対象の 4 分の 3 がサイバーセキュリティへの投資を増やすことを計画していました。しかし 1 年が経過した現在、企業の半数がサイバーセキュリティの主要分野への投資が不十分であると感じており、そのために攻撃に対して脆弱になっていると懸念しています。世界的に見ると、このような不安は米国企業の間で最も強く (61%)、これは米国企業が最も多くの攻撃を経験していたことを考えると当然と言えます。

一般的に企業は適切なサイバーセキュリティ分野に投資していると感じており、世界では 71% が投資とサイバーセキュリティ戦略が一致していると報告しています (日本では 59%)。それにもかかわらず、なぜ多くの企業がセキュリティへの投資が不十分であると感じているのでしょうか？

投資を正当化する難しさ

このようなギャップの原因は、簡単に解決できる、サイバーセキュリティに対する認識の欠如だけではありません。むしろサイバーセキュリティは他の優先事項の障害とみなされており、回答者の上司の 45% が、サイバーセキュリティのためにイノベーションがスローダウンすることを懸念しています。IT の近代化はデジタルトランスフォーメーションの取り組みにおいて重要な要素であり、回答者の 43% がサイバーセキュリティへの投資がこの取り組みを妨げていると感じています。

サイバーセキュリティの担当者は、これらの優先事項に直面している経営陣に対してコストを正当化する必要がありますが、44% がそれに成功していません。回答者の 72% がサイバーセキュリティへの投資は収益と成長の目標達成に貢献していると感じている一方で、サイバーセキュリティへの支出による ROI を数値化できたという自信がある回答者は 62% と中程度にとどまりました。問題の一部はリソースをどこに使うべきかを理解することにあります。回答者の 36% が、リソースの配分に関する明確な計画がないまま過度に投資を行ったと答えています。

おそらく投資を減らすべきでない組織が投資を削減している現状

望ましい傾向として、昨年よりも多くの組織 (87%) がサイバーセキュリティへの投資を増やすことを計画しています。しかし、2023 年に 76% の企業がサイバーセキュリティへの投資増加を予定していたにもかかわらず、今年の調査で回答者の半数が依然として投資が足りないと感じていることから、意図が現実を反映していない可能性があります。

意外ではないかもしれませんが、サイバーセキュリティへの投資を削減する予定があるのはわずか 4% であり、これは必ずしもセキュリティ機能の縮小を意味するとは限りません。競争が激化する中で、コスト削減を図る企業は、より安価なソリューションに移行したり、コスト効率を高めるために契約を統合したり、オープンソースのオプションを検討したりしている可能性があります。できるだけ経費を減らして多くを成し遂げようとすることに問題はありませんが、コストを削減しているグループのパフォーマンスが比較的低いことは懸念をもたらします。このグループでは過去 12 か月に平均 68 件のセキュリティインシデントが発生しており、全体平均の 40 件を 70% 上回っています。

リスク分析は投資の重要な要素

企業は適切な効果をもたらす予防策と対応策に投資することで多くを達成できます。そのためには、リスク分析、すなわち特定の企業にとって最も影響の大きいサイバーリスクの理解とそれらの軽減策への投資の集中の両方に対する成熟したアプローチが必要です。

「リスク」は経営陣にとって理解しやすい言葉です。サイバーセキュリティ担当者は、サイバーセキュリティによってイノベーションとビジネス変革を安全に進められる理由を多忙な経営陣たちに証明できる、重要なリスク軽減の指標を示すことによって、彼らが理解できる言葉で説得できます。また、プロダクションチームと連携し、可能な限り自動化を取り入れながら開発サイクルの早い段階でセキュリティ対策を導入することで、これらの対策の効果を高め、ワークフローへの支障を抑えられます。

復旧時間

政治情勢の観点から見ると、2025 年は波乱の幕開けとなりました。議論のトーンは妥協を許さず、対立の構図がすぐに作られてしまいます。このことは自分の勤める企業が世間の非難の的になりうることを思い知らせるものであり、CISO が夜も眠れなくなるには十分な要因かもしれません。「万事順調」な状態から「攻撃を受けている」状態に変わるまではほんの一瞬です。

オンライン攻撃の件数が減少している兆候はまったく見られません。攻撃の数、被害の大きさ、それらへの対応・復旧・再発防止に要する時間、いずれを取っても状況は深刻です。オンライン攻撃は、企業の最も痛いところ、つまり評判と収益を狙って損害を与える常套手段として使われ続けています。

日本の参加者に、オンライン攻撃から完全に復旧するまでに通常どれくらいの時間がかかるかを尋ねたところ、平均で 7.12 か月との回答が得られました。これは、世界全体の平均である 7.34 か月よりわずかに短い期間です。ただし、驚くことに世界の回答者の 30%は 1 ～ 3 か月以内に復旧を完了できたと回答している一方で、13%は復旧に 1 年以上を要する攻撃を経験したと回答しています。

なぜこれほどまでに差があるのでしょうか？その答えの 1 つは、サイバーセキュリティへの投資が減少すると、復旧時間が長くなることは間違いありません。今後 12 か月間の支出を減らす予定の企業と、復旧に 8 か月以上かかると見込んでいる企業の間には、直接的な相関関係が見られました。認識と現実のギャップは拡大しており、セキュリティ投資を削減しようとしている企業は、インシデントからの復旧に平均 11 か月を要しており、これは予想よりも約 3 分の 1 長いのです。対照的に、セキュリティ投資を維持・増加させている組織では、はるかに迅速な復旧を果たしています。

予防措置が回復戦術のトップに

日本において、最も一般的な予防策として挙げられたのは、より強力なセキュリティの導入 (39%) と従業員への追加トレーニングの実施 (36%) でした。これは「学んだ教訓」や将来的な攻撃の防止に重点が置かれていることを反映しています。世界全体ではそれぞれ 43% と 41% であり、日本の数字はやや低めです。最も優先度の高い回答に特段の驚きはないものの、トレーニングがここまで高く評価されていることに驚く人もいるかもしれません。この理由は 2 つ考えられます。1 つは、働く場所の柔軟性を認める文化に対応するために、企業がセキュリティ手順を調整している最中であることです。もう 1 つは、ソーシャルエンジニアリングが攻撃の足掛かりとしてますます使われており、リモートワークの拡大に伴い従業員の警戒心を高めるトレーニングの重要性が増していることです。

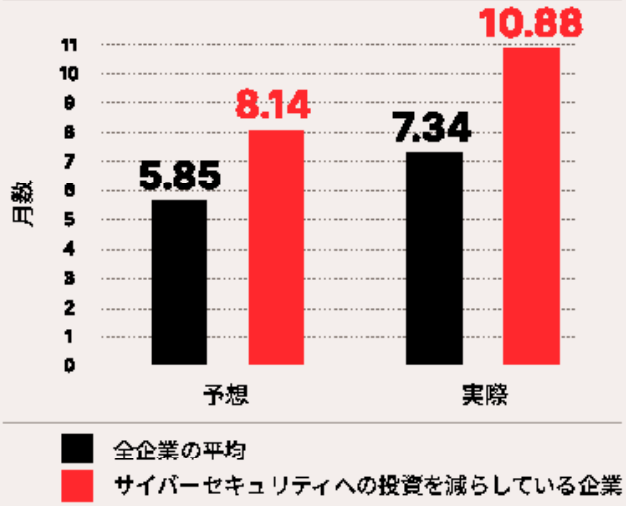
日本では、バックアップからの復元 (38%ー世界と同じ) やステークホルダーとのコミュニケーション (34%ーこれも世界と同じ) など、インシデント復旧を支援する具体的なアクションを優先する企業が増えています。フォレンジック分析は、悪意のある内部者や外部攻撃者に対する法的措置の追求や規制レポート作成に不可欠ですが、最も引用されることが少なく、わずか 25%に過ぎません。これも世界的なレスポンスと同様です。明るい面として、日本の回答者の 29% がインシデント対応プレイブックおよびサポートツールに追加の予算を割り当てており、これは世界全体の 32% からわずかに減少しています。

調査によれば、日本の多くの企業は復旧のために社内リソースを活用しており、54% が自社の IT チームを頼りにしていると回答しました。一方、外部のサイバーセキュリティ企業に支援を依頼し

ているのは 45% でした。コストを相殺するためにサイバー保険を利用している企業は 3 割未満にとどまっており、2024 年のデータ侵害による平均コストは過去最高の 488 万ドルに達していることから、この数字は今後も減少すると予想されています。

最後に、日本は EDR ベンダーに関して、世界の他の国々に比べて忠誠心が低いことが分かります。回答者の 28%は、最近のセキュリティイベントを考慮して、ベンダーの変更を検討していると述べました。それでも、多くの人は既存のツールを使い続け、より有効に活用したり最適化したりする方法を探しています。これら二つの国の回答者の 46% が、これが好ましいアプローチであると答えました。

図1
サイバーセキュリティインシデントからの回復時間



自信と現実：組織はインフラストラクチャセキュリティを過大評価しているか？

セキュリティインシデントは長らく IT 専門家にとって日常の一部であり、ほぼすべての企業がその経験を有しています。日本および全世界の回答者のうち、セキュリティインシデントを一度も経験していないと答えたのはわずか 14%でした。過去 1 年間で、調査対象の組織は平均して 40 件のインシデントを経験しています。最も影響を受けたのは米国企業で、週に 1 件、12 か月間で 64 件のインシデントを経験しており、規模の大きな企業は攻撃対象領域が広いことやブランドの知名度が高いこともあり、より多くの危険にさらされています。

ここで強調しておきたいのは、インシデントが必ずしもオンライン攻撃を意味するわけではないということです。実際、調査対象の日本企業の 30%が「設定ミス」によるインシデントを経験したと回答し、29%が「ソフトウェアのバグ」が原因だったとしています。しかし、パッチ適用や IT の変更は遅れがちで、19%の企業がこれによりセキュリティギャップが生じていると述べています。DevSecOps を取り入れることで、バグを未然に防ぎ、脆弱性の修正を加速することが可能です。

もう 1 つの重要な問題は、手動プロセスと自動プロセスの間にある緊張関係です。手作業は 26%のインシデントの原因となっており、18%の回答者が、セキュリティをテクノロジーソリューションに組み込むのではなく、社員の手作業によってセキュリティポリシーを適用していることが問題を引き起こしていると報告しています。

金銭的な損害をもたらすサイバーインシデント

原因が誰であれ、何であれ、サイバーインシデントは重大な収益の損失をもたらします。回答者の 26%が「収益に影響が出た」と答えました。全世界で見ると、経済的損失があった場合、企業は平均して収益の 2.98%を失っています。日本企業では 2.84%の収益が失われています。金銭的には測りにくいものの、ダウンタイムも大きな影響の 1 つであり、次いでデータ損失も重要な結果として挙げられます。

さらに、オンラインセキュリティインシデントは重大な法的・規制上のリスクも伴います。日本の回答者のうち 19%が「コンプライアンス違反があった」と回答し、23%が「顧客アカウントの侵害があった」としており、これはプライバシー法違反につながる可能性があります。

評判の毀損も深刻な懸念事項で、日本の組織の 22%に影響を及ぼしています。さらに、19%が「顧客の信頼の低下」、24%が「顧客満足度の低下」を報告しており、これらは顧客の維持に直結する問題です。インシデント後に顧客離れが増加したと答えた組織は 8%にのぼります。

次なる脅威に立ち向かう

サイバー脅威に対する懸念は依然として高いままです。特に自動化された攻撃者の増加は深刻で、49%の回答者が「夜も眠れない」としています。現在のセキュリティ技術スタックで対応できるか不安視する声も多く、26%が「防御に自動化が不足している」と答え、17%は「変更管理の遅さが足を引っ張っている」としています。実際、「サイバーセキュリティの自動化」は今後 12 か月間のセキュリティ優先事項の第 2 位に挙げられ、回答者の 21%が重要だと回答しました。この不安はイノベーションにも影を落としています。デジタル変革は成長を約束しますが、44%が「ソフトウェアやインフラを拡張すれば攻撃リスクが高まる」と心配しており、40%は「最新かつ複雑なアーキテクチャを保護する経験が十分ではない」と感じています。さらに広い視野で見ると、59%が「高度な脅威への対応ができていない」と感じ、57%は「社内のサイバーセキュリティ技術が十分でない」と答えています。

DDoS 対策の詳細

分散型サービス妨害 (DDoS) 攻撃は発生から四半世紀が経過しているにもかかわらず、依然として止むことなく脅威をもたらしています。23% の企業が今後 12 か月の脅威として DDoS 攻撃を挙げています。

2024 年に DDoS 攻撃を受けた企業の 62% でダウンタイムによる被害が問題となり、半数以上 (52%) が大幅な収益損失を報告し、70% が運用コストの高騰に苦しんでいます。

矛盾しているのは、投資の優先順位として DDoS 対策は 9 位 (25%) に過ぎないにもかかわらず、今後 12 か月の脅威として DDoS 攻撃を挙げた回答者の 45% は対策が十分にできていないと感じている点です。DDoS 攻撃を緩和するさまざまな方法があります。最も一般的なのは、クラウドベースの DDoS 対策の導入 (71%) で、56% は ISP に支援を求めています。また、54% がオンプレミスの緩和策をソリューションとして導入しています。クラウドとオンプレミスで使用できる Web アプリケーションファイアウォール（WAF）は人気が高く、66% を占めています。

サイバーセキュリティ投資はリスクの増大に追いついているか？

効果的なサイバーセキュリティは、適切な投資なしには実現しません。脅威が増加し、攻撃者が高度化する中、組織はオンラインの資産やインフラを守るために、有意義なリソースを継続的に投入する必要があります。しかし、強い意志とは裏腹に、私たちが目にするデータは重大な欠陥を明らかにしています。

2023 年には、全世界の回答者の 75%が「セキュリティ投資を増やす予定」と答えていました。しかし 1 年後、半数が「重要分野への投資が不十分だった」と答えています。投資が不十分だと感じている企業では、脅威にさらされているという懸念が生まれています。この感情は特に米国で顕著で、61%の組織が「ギャップがある」と認識しており、これは同地域でのインシデント発生率の高さと相関しています。日本の合計は 53%とやや低めです。

興味深いことに、世界全体で 79% が現在の投資が戦略目標と一致していると述べています（日本では驚異的な 84%）。では、なぜ多くの人々がオンラインセキュリティへの投資が不十分だと感じているのでしょうか？

投資を正当化する難しさ

予算が厳しいことだけが、セキュリティ投資を難しくしているわけではありません。回答から見えてきたのは、「サイバーセキュリティは他の優先事項にとって障害だと見なされている」という現実です。驚くべきことに、回答者の 35%の経営幹部が「サイバーセキュリティの取り組みがイノベーションの足かせになっている」と心配しています。IT の近代化はデジタルトランスフォーメーションの取り組みにおいて重要な要素であり、回答者の 27% がサイバーセキュリティへの投資がこの取り組みを妨げていると感じています。

サイバーセキュリティの担当者は、経営陣に対してコストを正当化する必要がありますが、42% がそれに成功していません。回答者の 71% がサイバーセキュリティへの投資は収益と成長の目標達成に貢献していると感じている一方で、サイバーセキュリティへの支出による ROI を数値化できたという自信がある回答者は 63% と比較的高い数値です。問題の一部は資金をどこに使うべきかを理解することにあります。全世界では、36% がリソースの配分に関する明確な計画がないまま過度に投資を行ったと答え、日本ではその割合が 29%でした。

セキュリティ予算の削減はリスクを招く

明るい面として、驚くべきことに、回答者の 82% が今年サイバーセキュリティへの投資を増やす予定です。しかし、今回の企業の半数がまだ投資不足だと述べていることを考慮すると、意図だけでは現実に反映されないかもしれません。

さらに朗報としては、セキュリティ支出の削減を予定している企業はわずか 3%です。この数字だけを見れば高いように思えますが、必ずしも保護レベルを引き下げることを意味しません。これらの企業は、コストの安いソリューションへの移行、ベンダー契約の統合、オープンソースの活用などを検討している可能性があります。

支出の最適化は理にかなっています。しかし、データは「コスト削減派」が代償を払っていることを示しています。予算を削減予定とするグループは、過去 1 年で平均 68 件のセキュリティインシデントを経験しており、全体平均の 40 件に比べて 70%も多くなっています。これは、コスト削減の裏に潜む見えない代償に関する重要な問いを投げかけています。

リスク分析：スマートなサイバー投資の基盤

サイバーセキュリティ投資の効果を最大化するには、成熟したリスク分析アプローチから始めることが不可欠です。自社特有の環境において最も重大な脅威を特定することで、組織は予防および対応の取り組みに投資を集中させ、実質的な保護を実現できます。

「リスク」は経営陣にとって理解しやすい言葉です。サイバーセキュリティの責任者は、セキュリティがどのように安全なイノベーションやビジネス変革を支えているかを明確に示す、高レベルのリスク軽減指標を提示することで、両者の橋渡しができます。

また、エンジニアリング部門や製品チームとの連携も重要です。開発ライフサイクルの早い段階、特に自動化を通じてセキュリティを組み込むことで、防御がより効果的で、業務への影響も少なく、スケーラビリティにも優れたものになります。

サイバーセキュリティのスキルギャップ：それ自体が増大する脅威

サイバーセキュリティにおけるスキルの不足は、依然として大きな障壁となっており、日本も例外ではありません。実に 4 分の 1（25%）の組織が、現代のセキュリティ脅威に対処するための必要な専門知識が不足していると回答しています。さらに問題を悪化させているのが、49%の組織がサイバーセキュリティ人材への投資（採用・報酬の両面）が不十分であると認識している点です。その結果、今後 12 か月に向けた最優先事項として、22%の組織が人材育成と採用を挙げています。

サイバーセキュリティ人材の不足による影響は深刻です。組織はサイバー攻撃に対して脆弱になるだけでなく、インシデント発生時の対応時間が長くなり、コストも増大します。これらの課題は、既存のチームにさらなる負担をかけ、継続的な予防策の推進にも支障をきたしかねません。

このギャップの大きな要因は、企業が人材を探している場所と、資格のある専門家が実際に居住している場所との間に不一致があることかもしれません。調査対象となった組織の半数以上（57%）は、人材プールに必要な特定のスキルが不足していると報告していますが、同時に 8%はサイバーセキュリティ職の採用で大きな問題に直面していないと述べています。

業界の多くの人が証言するように、セキュリティ人材の育成はすぐには実現しません。新卒者や新入社員を効果的なチームメンバーにするには、かなりの時間と労力が必要です。これらの個人は、組織のツールやシステムに関する技術的な専門知識を習得するだけでなく、社内のワークフローや企業文化に関する微妙な理解も深める必要があります。

多くの国と同様に、日本もサイバーセキュリティの専門家不足に悩まされており、公共部門と民間部門の両方でレジリエンスに対する大きな障壁を生み出しています。教育システムでは、次世代のサイバーセキュリティ人材を育成するための道筋が限られているため、多くの組織がそのギャップを埋めるために民間部門に目を向けています。Fastly の日本担当カントリー・マネージャーである今野芳弘氏は次のように述べています。「私たちの顧客や見込み客は、リスクを管理するだけでなく、緊急に必要な社内の知識と能力を構築するために、テクノロジーパートナーとセキュリティコンサルタントに大きく依存しています。多くの場合、これらのリソースは長期的なレジリエンスへの重要な架け橋となっています」

こうした課題は、組織の成長に伴ってさらに顕在化します。より大規模で複雑な環境での業務は、特に経験の浅い人材にとって大きなプレッシャーとなります。13%の回答者が「大規模なテクノロジーインフラへの未経験」が、セキュリティチーム内での成功を妨げる大きな障壁であるとしています。

これらの問題に取り組むには、人材パイプラインの育成、スキルアッププログラムへの投資、採用戦略を実際の組織のニーズに合わせることに、意図的かつ持続的に注力する必要があります。

外部からの採用に代わる手段

現在直面している課題を踏まえ、企業はスキル開発の取り組みを社内の人材強化に向けるべきです。これにはいくつかの選択肢があります

スキルアップ：既存の従業員は、すでに自社の文化を理解しており、業務システムやプロセスについて基本的な知識を持っているため、新たな責任を担うための学習が可能です。

メンタリング：若手社員は、経験豊富なスタッフによる現場でのトレーニングを通じて貴重なスキルを習得し、有能なプロフェッショナルへと成長していきます。

部門横断的なコラボレーション：セキュリティチームが IT、コンプライアンス、サポート、製品開発チームなどとより良く連携できれば、社員はさまざまな部門におけるセキュリティの役割を理解するようになります。この枠組みの中で、人材の一時的な異動

(セコンドメント) を導入することも検討すべきです。最終的な目標は、セキュリティ部門以外のチームにもスキルや責任を広げることにあります。たとえば、製品開発チームとの間でセキュリティ知識を統合すれば、開発プロセスにおいて「セキュア・バイ・デザイン」の原則を適用できるようになります。

さまざまな部門を横断して働くスタッフを社内で登用することには、多くの利点があります。こうした実践は、すべての従業員がセキュリティの責任に関与する必要があることを示すものです。また、このような取り組みは、企業のデジタルトランスフォーメーション（DX）推進にも貢献します。セキュリティが組み込まれた企業文化は、デジタルトランスフォーメーションを支えつつ、デジタル化の進展によって脆弱性が増すと考えている 44% の企業が抱えるセキュリティ面の懸念にも対応します。

図2
現在の人材プールにおける問題点

シフトする説明責任のマッピング

サイバーインシデントが発生した場合、説明責任の所在は誰にあるのでしょうか？現在、規制当局はその責任を最高情報セキュリティ責任者(CISO)に直接問うようになっています。2023 年 10 月、米国証券取引委員会（SEC）は、SolarWinds 社だけでなく、同社の CISO であるティモシー・G・ブラウン氏に対して、詐欺および内部統制違反の罪で訴追しました。大半の罪状は後に棄却されましたが、規制当局は CISO の法的責任を明確に定義する新たな表現を用いるようになっています。

CISO の説明責任に関する意味の無い対応

回答者の 94%によると、ほとんどの組織は説明責任構造の変化を反映するためにポリシーの変更を実施しています。多くの組織は、真の実体を欠いた変更を実施しています。最も一般的に実施されている施策は、CISO に戦略的ディスカッションへの出席権を与えることであり、特に目立った進展とは言えません（32%）。

対策の中には自己弁護的なものやチェックボックスをチェックするだけのものもあります。「監督機関によるセキュリティ情報開示文書への監視を強化する予定」と答えた組織は 29% で、これは単に規則順守への取り組みを表明しているに過ぎません。同率の 29% の組織が、「規制当局の調査に備え、サイバーセキュリティ部門の社員に法的防御策を提供する予定」としています。調査対象グループの中で、日本の回答者のうち CISO にサイバーセキュリティ基準に関する法的義務があると答えたのはわずか 21% でした。

Fastly の CISO を務める Marshall Erwin は「これらのセキュリティ対策は悪くはありませんが自己防衛にすぎず、実際にセキュリティ体制を強化することはできません」と述べています。

責任の所在

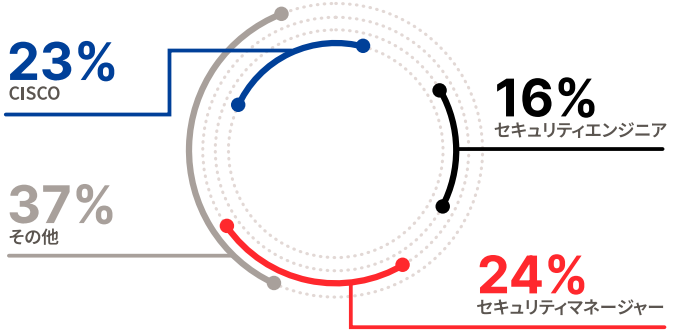
重大な問題の 1 つは、サイバーセキュリティインシデントに対する責任の分担が不明確であることです。複数の職位に属する従業員がそれぞれに部分的な責任を持っているため、組織全体として明確なセキュリティリーダーを欠いているのです。調査結果によると、責任の所在として最も多く挙げられたのはセキュリティエンジニア（24%）で、CISO は 2 位（23%）でした。セキュリティマネージャー（16%）がそれに続きます。

いくつかの肯定的な指標が存在します。サイバーセキュリティの責任を引き受けるチームが増えていることは、インシデントの責任が従来のセキュリティの役割、例えば SOC アナリスト（10%）、アプリケーション開発者（7%）、サイト信頼性エンジニア（7%）を超えていることを示しています。

ただし、これは理論上の話であり、実際には誰も責任を取っていないという状況につながります。サイバーセキュリティに関する役割と責任を明確に認識している回答者はわずか 43% に過ぎません。

約 3 分の 2（63%）の組織では、インシデント発生時の責任の所在が不明確であると回答しています。最終的には、誰かが責任を取る必要があるのです。

図3
サイバーセキュリティインシデントに対する責任の所在



狙われる社員

組織全体でセキュリティを共通の責任として理解し、従業員にポリシーを実行する権限を与えることが不可欠です。29% の回答者が「ソーシャルエンジニアリング攻撃」を来年最も懸念される脅威と考えており、これは特に重要な点です。ハイブリッドワークへの移行は新たなセキュリティ課題を生み出しており、65% の組織が「リモートワーカーが攻撃対象になるだろう」と予想しています。

70% の組織は「サイバーセキュリティに関するコンプライアンスを全社員に適切に説明している」と述べています。このアプローチは一定の成果を上げており、IT 部門以外の従業員のうち 57% が「自分の業務がサイバーセキュリティに影響を与える」と認識しており、54% の従業員が「セキュリティ規則を遵守している」と答えています。最大の課題は「サイバーセキュリティ教育の不足」であり、これは日本の組織の 56% が直面している問題です。

ルールを守るためには、十分なリソースの提供が必要です。57% の企業が「そのためのリソースを提供している」と答えています。また、報告手順が必ずしも明確ではありません。73% の回答者は「全従業員がアクセスできる明確な報告プロセスがある」と答えていますが、IT 以外の職種の従業員の 50% がセキュリティ脅威の識別と対応に自信がないとしています。

変化する環境に対応できる適切なツールの選択

サイバーセキュリティの脅威は進化を続けており、それに対応するための防御ツールの継続的なアップデートが求められます。

日本では、「関連する技術スキルの不足」が 53% で最大のセキュリティ懸念事項として挙げられています。次に高いのは 29% で「ソーシャルエンジニアリング」です。これにはビジネスメール詐欺やランサムウェアなどの攻撃における重要なステップであるフィッシングなど、一般的な脅威も含まれます。

多くのセキュリティ脅威が複雑に絡み合い、環境の理解と対応がさらに難しくなっています。例えば、アカウント乗っ取り（23% が懸念）は多くの場合フィッシングから始まり、データ流出（35%）はランサムウェアによる侵害の一般的な結果です。

前述のように、回答者の 21%によると、SolarWinds ハッキングおよび Kaseya ランサムウェア攻撃により、組織はサードパーティの侵害を重大なセキュリティ上の懸念として認識するようになりました。

保護対策への投資

多くの組織が脅威対策のために製品やサービスへの戦略的投資を行っています。現代的な認証システムに対して前向きな投資傾向を示しており、33% と 3 番目に重要な投資項目に位置付けられています。ID およびアクセス管理ツールは、多要素認証（MFA）と共に、ソーシャルエンジニアリングへの効果的な対抗策として注目されています。

また、API の脆弱性への懸念の高まりにより、API ゲートウェイセキュリティへの投資が 24% に達しています。Web アプリケーションファイアウォール（WAF）を購入した組織は 28% と、Web アプリケーションの脆弱性を懸念する 24% を上回っており、WAF が小規模な DDoS 攻撃を含む複数の攻撃に対する標準的な防御策として認識されていることを示しています。Web アプリケーションおよび API セキュリティソリューションには、組織ごとに年間平均 158 万ドルが投資されています。

DDoS 対策への投資が 18% で 11 位、ボット対策が 8% で最下位だったのは意外でした。ボットはクレデンシャルスタッフィングの主要手段となっており、これがアカウント乗っ取りの大きな要因になっています。

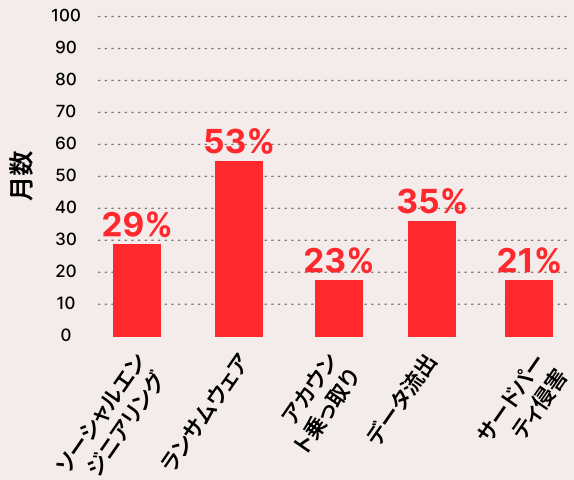
このほか、インシデント対応サービスにも投資が行われています。リスク移転としてのサイバー保険は、33% でモダン認証と並び最も高い投資項目となっています。23% の回答者がこのアプローチを採用しており、Managed Security Service 企業を通じてサイバー脅威への予防・対応を図っています。

セキュリティ業務のアウトソーシングを選んだ組織のうち、複数のサービスプロバイダーと連携することが多く、24% がこのアプローチを採用している一方、33% はセキュリティ対応を単一の外部サービスプロバイダーに一任しています。15% の組織はセキュリティ対応を社内チームに統合することを選択していますが、18% はセキュリティ対応を社内チームと外部パートナーで分担しています。

現行のセキュリティツールは統合が困難

ツールの重複使用は、多くの組織にとって問題を引き起こしています。調査によると、企業は平均で 7.85 個のネットワークおよびアプリケーションセキュリティソリューションを使用しており、日本では 6.5 個とやや少なめです。回答者の中で、ツールの冗長性率は 36% に達しています。

図4
ツールの整理統合を望む主な理由



セキュリティプレイブックの書き換え：最初から一元化され、組み込まれたアプローチを

今回の調査から得られる最大の示唆は、「企業は激化するサイバー脅威と限られたサイバーセキュリティ予算の狭間に立たされている」ということです。回答者の 64% は「サイバーセキュリティは不可欠」と認識している一方で、約半数が「投資不足により脆弱性を感じている」と答えました。す。多くの企業が今後の支出増加を計画しているものの、過去の傾向からは「意図＝実行」ではないことが示されています。主な障壁の一つは、経営層への費用対効果の説明です。経営層は、セキュリティ以外への資金配分の方が価値があると考えています。

断片化され重複したツールセットへの依存は問題をさらに悪化させています。このような継ぎはぎ状態のサイバーセキュリティスタックは費用がかかり、統合と維持が複雑なためです。これは、変化する脅威の状況を追いかけ、時間の経過と共に少しずつ進化するリアクティブなサイバーセキュリティ戦略の自然な結果でもあります。

「セキュア・バイ・デザイン」が求められる時代

組織はコストと複雑さが制御不能に陥るのを防ぎながら、急増するセキュリティリスクに効率的に対処するために革新する必要があります。それには、脅威を識別して軽減できる標準的なメカニズムをビジネス全体に適用することが求められます。

複雑さとコストの削減をもたらすツールセットの統合は、このようなメカニズムの重要な要素です。各リスクの影響と確率に基づいてツールの機能をリスクにマッピングする成熟したリスク管理が必要になりますが、これは業種や企業規模などの要因によって異なります。

もうひとつ必要なのは、セキュリティに関する一連の普遍的な原則と、顧客向けの製品やサービスから社内のワークフローに至るまで、あらゆる開発プロセスにこれらの原則を適用する意志です。設計段階からこれらを適用することで、セキュリティを徹底的に強化できます。

この「セキュリティ・バイ・デザイン」の概念をソフトウェアアーキテクチャに導入することを優先事項に挙げた回答者はわずか 11% にとどまり、脅威対策のランキングで 6 位でした。これは技術的な変革であると同時に文化的な変革でもあり、エンジニアにとって両方とも容易ではないことから、納得できる結果と言えました。

さらに別の問題も存在します。回答者の 37% が「サイバーセキュリティは時間と予算の無駄であり、他の領域にこれらを費やした方がよい」と感じていることです。このように感じている人は、サイバーセキュリティへの投資を減らす可能性がはるかに高い (53%) ことがわかりました。

「経営陣の間でサイバーセキュリティが見えづらいことがここで問題になっている」と Erwin は警告しています。「セキュリティプログラムが効果的な場合、多くのリスクが軽減され、侵害やインシデントの可能性が減ります。しかし経営陣はその価値を直接見ることがありません」(Erwin)。

このような姿勢を変えるのは容易ではありませんが、最初のステップとしてサイバーセキュリティへの投資と定量化可能なリスクベースの結果の間にある直接的な関係をマッピングすることから始めることをお勧めします。

Fastly について

Fastly の強力でプログラム可能なエッジクラウドプラットフォームは、世界のトップブランドが、エッジコンピューティング、配信、セキュリティ、オブザーバビリティの提供を通じて、高速で安全かつ魅力的なオンラインエクスペリエンスを提供できるよう支援し、サイトのパフォーマンスを向上させ、セキュリティを強化し、世界規模でのイノベーションを推進します。他のプロバイダーと比較して、Fastly の強力で高性能な最新のプラットフォームアーキテクチャにより、開発者は市場投入までの時間を短縮し、業界をリードする実証済みのコスト削減を実現しながら、安全な Web サイトやアプリを配信できます。Reddit、Neiman Marcus、Universal Music Group、SeatGeek など世界中の組織が、インターネットエクスペリエンスの向上に Fastly を信頼して活用しています。Fastly の詳細については https://www.fastly.com/jp をご覧ください。また、X @FastlyJapan でも最新情報をご覧いただけます。