CLOUDFLARE

セキュリティの新局面を乗り切る：日本のサイバーセキュリティ対策準備状況調査

過去12か月間、日本の脅威状況は依然不安定で回答者の30%がデータ侵害を経験したと回答[1]。

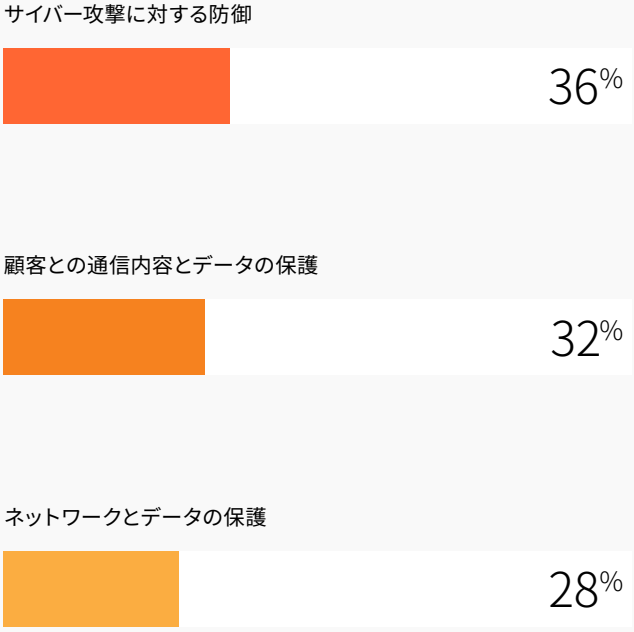
データ侵害を経験した回答者の79%が頻度が増したと回答し、11回以上と答えた回答者は41%に上りました。データ侵害が最も多かったのは大企業（36%）で、最もよく狙われた業界はメディア・電気通信（56%）、旅行・観光・ホスピタリティ（58%）、教育（43%）でした。

サイバーセキュリティは引き続きIT支出の重要分野であり、回答者の79%が自社IT予算の10%以上をサイバーセキュリティに費やしていると回答しました。サイバーセキュリティの最優先事項として挙げられたのは、サイバー攻撃に対する防御（36%）、顧客との通信内容とデータの保護（32%）、企業のネットワークとデータの保護（28%）です。

日本の特徴と周辺国との比較

	日本	アジア太平洋・日本・中国
過去12か月間にデータ侵害を経験した割合が低い	30%	41%
過去2年以内にランサムウェア攻撃を受けて身代金を支払った割合が低い	31%	70%
AIによるデータ侵害の巧妙化と深刻化を懸念する傾向が強い	90%	87%

サイバーセキュリティの最優先事項



統合はよく用いられる戦術のようで、人的資源が逼迫（54%）、サイバー攻撃からの復旧が長期化（43%）、既存のソリューションやソフトウェアとの統合が困難（42%）、反復的なタスクや重要でないサイバーセキュリティ機能に費やされる時間が過多（42%）など、多数のベンダーを利用することから生じる問題がこの戦術をとる理由になっています。

データ侵害を起こした攻撃ベクトルの上位3種はWeb攻撃（59%）、フィッシング（43%）、マルウェア（43%）で、最も頻繁に狙われた資産は顧客データ（70%）、ユーザーアクセス（70%）、個人を特定できる情報（58%）でした。また、回答者の90%が、AIによってデータ侵害の巧妙度や深刻度が高まることを懸念していることもわかりました。

厳しい脅威状況ではありますが、レジリエンスの向上を示す兆候が見られます。回答者の75%がデータ侵害を防ぐ準備はできていると感じ、64%が自社のサイバーセキュリティ体制は少なくとも「ある程度成熟」していると考えています。データ侵害を防止する「準備はある程度できている」という回答が多かったのは、IT・テクノロジー、メディア・電気通信、旅行・観光・ホスピタリティの分野の企業でした。

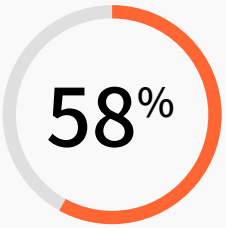
1. データ侵害は、攻撃者が企業のアプリケーション、データ、ネットワークに不正にアクセスするインシデントであり、インシデントはシステムの完全性を損なう可能性のある行為です。

ゼロトラストの導入が進んでおり、回答者の42%が「現在、ゼロトラストソリューションに投資している」と答えています。さらに41%が、今後12か月間にゼロトラストに投資することを計画中です。投資推進の主な理由は、脆弱なIoTデバイスがもたらすリスクを低減するため（58%）、ユーザー資格情報の窃盗やフィッシングの影響を多要素認証によって軽減するため（56%）、攻撃発生時に被害を狭い範囲に隔離するため（55%）でした。

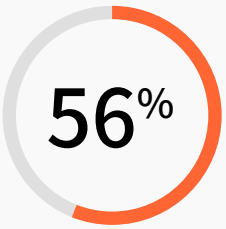
回答者が直面している他の課題としては、サイバーセキュリティ人材の不足（41%）、AIがもたらす新たな脅威（37%）などが挙がっています。回答者が自社のサイバーセキュリティソリューションを評価した際の主な基準は、サイバー攻撃の検出（47%）と対応（51%）にかかる時間でした。

ランサムウェアに関する懸念が膨らんでいる状況は変わりません。回答者の41%がランサムウェアに関する懸念を示し、Webアプリやサーバーにあるパッチ未適用の脆弱性を攻撃者が悪用（58%）するというのが最も一般的な侵入手口であることがわかりました。

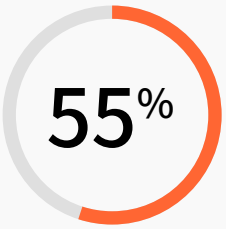
ゼロトラスト実現に向けた投資の主な推進要因



脆弱なIoTデバイスがもたらすリスクを低減



多要素認証によりユーザー資格情報の窃取やフィッシングの影響を軽減



攻撃発生時に被害を狭い範囲に隔離

規制対応やコンプライアンスに費やすリソース

回答者所属企業の42%が、規制およびコンプライアンス要件への対応にIT予算の5%以上を支出

日本では38%の回答者が、週の勤務時間の10%以上を業界の規制要件と認証の遵守に費やしていると報告

過去2年以内にランサムウェア攻撃を経験したと答えた回答者の所属企業は、31%が身代金を支払っていました。そのうち42%は、支払わないと公約していたにもかかわらずです。身代金支払いの主要因は顧客からの圧力（38%）でした。しかし、回答者は所属企業のセキュリティについて、従業員トレーニング（57%）、二要素認証（69%）、マルウェア対策ソフトウェア（69%）の導入といったランサムウェア脅威の軽減策をとっており、少なくとも「ある程度成熟している」と考えています。

今年の調査では、規制とコンプライアンスも重要なテーマとして浮上しました。回答者の所属企業の42%が、規制およびコンプライアンス要件への対応にIT予算の5%以上を費やしています。また、回答者の38%が、業界の規制要件や認証要件の充足に週の勤務時間の10%以上を費やしていると報告しています。それでも、こうした規制対応やコンプライアンスへの投資は企業に好影響をもたらしてきました。プライバシーやセキュリティのベースラインレベル上昇（52%）、企業の技術とデータの完全性向上（40%）、企業の評判やブランド評価の向上（38%）などです。

推奨事項

上記の調査結果を基に、今後1年間でCISOがとるべき行動として以下の6つの推奨事項を提案します。

ソリューションの合理化により複雑さを軽減

当社は昨年のレポートで、SASEによるセキュリティアーキテクチャの合理化を提案しました。これは今年も引き続き推奨していますが、その根拠は明白です。ソリューションやITベンダーを増やしたからと言って、リスクが軽減されるわけではないということが実証されているからです。企業は、より慎重なアプローチでデプロイするソリューションの数を最小限に抑え、ソリューション供給ITベンダーを統合することを検討する必要があります。

チェーンの最弱箇所を強化

グローバルで相互接続された今日の環境では、すべての企業がソフトウェアサプライチェーンに依存しています。アプリケーションはオープンソースコード、API、サードパーティ統合を前提に構築されており、それらがすべて攻撃対象領域の拡大要因になっています。このように攻撃対象領域が拡大しているため、新しいパートナーのオンボーディングは、ツール自体だけでなく、その開発エコシステム全体を信頼するという選択を意味します。境界型セキュリティモデルから誰も信用しないゼロトラストモデルへ移行し、攻撃者は既にネットワーク内にいると想定してユーザー、デバイス、ワークロードをIDとコンテキストに基づいて評価することにより、サプライチェーン侵害に関連するリスクを軽減することができます。セキュア・バイ・デザインの原則を貫くパートナーをお探しください。

ランサムウェア攻撃者のレバレッジを制限し、要求対応計画を策定

ランサムウェア攻撃が増加しており、CISOと取締役会は対応計画を整備しておく必要があります。今回の調査で、その計画に身代金の支払いを含めるべきでないことが裏付けられました。身代金を支払った企業は必ずといっていいほど、その対応を後悔しているからです。当社は、ゼロトラスト機能によって侵害発生時のラテラルムーブメントを最小限に抑える戦略を推奨します。さらに、堅牢な復旧プログラムによって、攻撃者の要求のレバレッジを低下させます。まずは、最も重要なシステムとデータについて定期的データバックアップ（有効性と完全性を確認後に）を行うことが安心の第一歩です。ギャップを特定し、業務復旧と影響軽減のための力を付けるには、定期的な災害復旧テストが極めて重要です。

AIによる攻撃増強に対する備え

攻撃者はAIを使ってくるでしょうから、CISOはAI防御戦略を整備する必要があります。サイバーセキュリティリーダーは対策のアウトソーシングを慎重に行う必要がありますが、人材モデル、ガバナンスフレームワーク、コンプライアンス要件を精査し、データの利用を監視することが重要です。誰もが今すぐとれる重要な行動は、サードパーティベンダーとのエンゲージメント条件を見直して、自社データがベンダーのAIモデルでどう使われるかを理解し、それが自社の要件に合っているかを確認することです。現在お使いのセキュリティツールはAI攻撃の増加にどう対処するでしょうか？Cloudflare製品の多くは、当社の巨大グローバルネットワークの脅威インテリジェンスを活用し、新たな脅威に先制的に対処しています。

投資をCAPEXからOPEXへシフト

多くの企業では予算が逼迫しており、サイバーセキュリティリーダーには財務管理の手腕が求められます。将来の状態に合うよう既存チームメンバーのスキルアップを行い、複雑さを軽減し、プロセスを合理化することを検討しましょう。役割分担を見直して有効性を最大化し、ラグタイムを短縮する機会を見出しましょう。一部機能をMSPへアウトソーシングし、投資をCAPEXからOPEXへシフトすることも検討に値します。

厳格な精査を覚悟

サイバーセキュリティに関しては社内外の監視が厳しくなり、担当リーダーは今まで以上の重圧を感じています。この監視は今後も続きます。CISOは、変化する規制（国内・国際）にすかさず対応し、取締役会メンバーのニーズにも応えられるよう、絶えず努力する必要があります。明確なスコープとスケジュールで監査に取り組むことで、顧客に付加価値を与えず、リスクも低減させないようなタスクを減らすことができます。

コネクティビティクラウドへ移行

Cloudflareは、企業の人材、アプリ、ネットワークを接続し保護するコネクティビティクラウドという新たなサービスカテゴリーを提供し、あらゆる環境のセキュリティを確保する上で重要な役割を果たします。企業は、アプリケーション、API、ネットワークセキュリティ、ゼロトラスト、グローバル脅威インテリジェンスなど、Cloudflareの幅広いセキュリティサービスポートフォリオを活用することにより、サイバー攻撃に備えてデジタルインフラを強化できます。オンラインデータと知的財産のセキュリティを確保して、ブランドインテグリティを守ることができるのです。

これらのセキュリティサービスは、Cloudflareのプログラム可能なグローバルクラウドネットワークサービスの統合プラットフォーム上に構築されています。このプラットフォームは、世界のインターネットトラフィックの大きな割合を接続・保護し、1日あたり平均1820億件の脅威を阻止しています。このグローバルクラウドネットワークは、ネットワークやインフラストラクチャの障害に備えて冗長性と回復力を提供することにより、ダウンタイムのリスクを最小限に抑え、高可用性を確保します。Cloudflareソリューションスイートの詳細情報、営業担当によるデモやPOCをご希望の方は、**cloudflare.com**をご覧ください。現行セキュリティ体制の評価と、従業員、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向けた行動計画の策定をCloudflareがお手伝いします。

こちらをスキャンしてレポート全文をご覧ください

***セキュリティの新局面を乗り切る：アジア太平洋地域サイバーセキュリティ対策準備状況調査**は、アジア太平洋、日本、中国のセキュリティ市場の調査結果をまとめたレポートです。本調査は14市場で、サイバーセキュリティ関連の意思決定者およびリーダー3,844名を対象に実施されました。