KEEPER®

サイバー攻撃対策の未来

前例のない脅威に備えるITリーダー

March 2024

サイバー攻撃がかつてないほど巧妙化している一方で、ITリーダーは新たな脅威に対処する準備が不足していると感じている

Keeper SecurityがTrendCandy Research社と協力し、800人以上のITおよびセキュリティ担当者を対象として2024年に実施した世界規模の調査によると、サイバー攻撃は人工知能（AI）の脅威や高度化した新たな攻撃手法によってますます巧妙化していることが明らかになりました。調査回答者の92%は、サイバー攻撃の発生頻度が前年と比べて増加していると回答しており、現在、多くのITリーダーはこうした新たな脅威に対処しつつ、攻撃数の増加に対しても取り組みが必要となっています。2024年、セキュリティはますます複雑化しており、これまで以上にリスクが高まっています。

パスワードやパスキー、特権アクセス、シークレット、リモート接続の保護に向けてゼロトラスト、ゼロ知識のサイバーセキュリティソフトウェアを提供する大手プロバイダーのKeeper Securityは、2024年時点におけるサイバーセキュリティの現状を把握するため、独立系調査機関に依頼し、世界中のセキュリティリーダーからサイバーセキュリティの動向と今後の防衛策についての知見を得ました。

サイバー攻撃は増加の一途をたどり、より巧妙化している

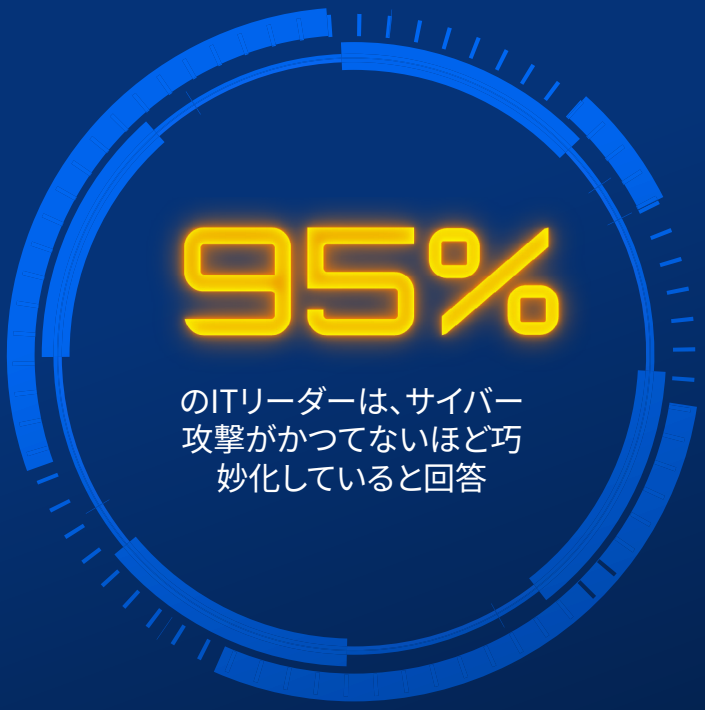
急速に高度化する脅威、新たな規制、パスキーなどの進歩、デスクトップから空間コンピューティングヘッドセットに至るまで各種デバイスの急速な普及に伴い、サイバーセキュリティはこれまで以上に重要性を増しています。今回の調査において、ITおよびセキュリティリーダーの大多数である92%が、サイバーセキュリティが最優先事項だと回答しています。また、回答者の92%は、サイバー攻撃が年々増加していると答えており、こうしたリーダーたちは常に対策に追われています。サイバー犯罪者は、これまでの安全対策を打ち破り脆弱な組織に最大の損害を与えるために、工夫を凝らして執拗に攻撃を仕掛けています。

サイバー攻撃の件数が増加するにつれて、その影響も大きくなっています。回答者の73%は、サイバー攻撃をきっかけとする金銭的損失を経験しています。財務上の直接的な影響は、サイバー攻撃を受けたことによる多大な影響のひとつですが、他の影響として、事業の中断、永続的な収益の損失、顧客やパートナーの減少、評判の低下などが挙げられます。

ITリーダーに、組織のどの部分がサイバー攻撃を受けるのかを挙げてもらいました。

KEEPER

ITリーダーの95%は、サイバーセキュリティインシデントの頻発と対処に必要なコストの増加に伴い、サイバー攻撃の巧妙化や新たなテクノロジーを駆使した脅威への備えが間に合わないと回答しています。



回答者によると、新たな種類の攻撃として最も深刻なものは以下のとおりです。

1. AIを駆使した攻撃
2. ディープフェイク
3. サプライチェーン攻撃
4. クラウドジャッキング
5. モノのインターネット（IoT）攻撃
6. 5Gネットワーク攻撃
7. ファイルレス攻撃

KEEPER

防御が難しいと感じているサイバー攻撃は以下のとおりです。

- 35% AIを駆使した攻撃
- 30% ディープフェイク
- 29% 5Gネットワーク攻撃
- 25% クラウドジャッキング
- 23% ファイルレス攻撃

AIを駆使した攻撃は最も深刻な脅威であると同時に、最も対処が難しい脅威だと考えられています。悪意のある攻撃者は、AIを武器にしてフィッシングやパスワード解読などの代表的な攻撃手法を素早く実行し、拡大化させています。これは、進化する脅威に対抗する上で、高度な防御メカニズムと基本的なベストプラクティスを組み合わせた、サイバーセキュリティに対する積極的なアプローチの必要性を浮き彫りにしています。

世界的に、ITリーダーがAIセキュリティ全般の強化に向けて検討している対策は以下のとおりです。

データの暗号化

従業員トレーニングと意識向上

高度な脅威検出システム

北米のITリーダーは、AI主導の脅威に対抗するため、高度な脅威検知システム（50%）とデータ暗号化（50%）ツールの使用を検討しています。

サイバー脅威がますます悪質化・巧妙化していく中で、ITリーダーは常に優位に立つため、セキュリティに対して多元的なアプローチを採用し戦術と戦略を適応させなければなりません。

攻撃の勢いは衰えを見せない

新たな脅威が迫り来る一方、ITリーダーは、以下に挙げる今日の代表的な攻撃にも対処しています。

61%	59%	49%	38%	37%
フィッシング	マルウェア	ランサムウェア	パスワード攻撃	サービス拒否（DoS）攻撃

北米では、調査回答者の49%がパスワード攻撃が最も一般的なサイバー攻撃であると回答しており、これは世界平均を11%上回っています。

盗まれたパスワードや認証情報、脆弱なパスワードや認証情報が、依然としてデータ侵害の主な原因となっています。調査回答者の52%は、自社のITチームがパスワードの頻繁な盗難への対応に追われていると回答しており、このことから、すべてのアカウントに強力でユニークなパスワードを作成し、それらを安全に保存する重要性があらためて示されました。漏洩した認証情報が悪意のある人物の手に渡るのを防ぐために、72%の企業がダークウェブを監視し、従業員の認証情報が盗まれていないかを調べています。ダークウェブ監視サービスを利用することで、組織はアカウント情報を常に把握し、認証情報が漏洩したことが判明した場合に直ちに措置を講じることができます。また、専用のパスワードマネージャーを導入することで、両方の問題に正面から取り組むことが可能になり、最高レベルの暗号化とダークウェブスキャンやアラートなどの機能を利用できるようになります。

KEEPER

ITリーダーから回答を得た増加傾向にあるサイバー攻撃

フィッシング
51%

マルウェア
49%

ランサムウェア
44%

パスワード攻撃
31%

サービス拒否（DoS）攻撃
28%

今日、実に67%もの企業がフィッシング攻撃への対策に苦戦しています。AIツールが爆発的に広まったことで、フィッシング詐欺の真実味が増し、サイバー犯罪者が詐欺を大規模に展開できるようになったため、この問題は深刻なものとなっています。さらに、回答者の84%は、AIが搭載されたツールの普及に伴い、フィッシングやスミッシングを検知しづらくなってきたと述べており、AIセキュリティに関してはAIを利用したフィッシングが最も懸念される事項（42%）であると回答しています。

攻撃の背後にいる人物とは？最も狙われているのは誰か？

今日、最も一般的なサイバー攻撃実行者のトップ3は以下のとおりです。

30%
独立系ハッカー

20%
ハクティビスト集団

11%
企業スパイ行為エージェント

攻撃の多くは、何千マイルも離れた独立系ハッカーやハクティビスト集団によるものですが、組織内という身近な場所で発生する可能性もあります。調査対象者の40%は、従業員が原因のサイバー攻撃を経験したことがあると回答しました。これは、意図的および非意図的な内部脅威の両方を阻止する技術を導入する重要性を強調するものです。特権アクセス管理（PAM）ソリューションは、IT管理者やセキュリティ担当者が特権認証情報を管理および保護し、最小特権の原則を適用する上で有用です。万が一、サイバー犯罪者が組織のネットワークへのアクセス権を入手した場合でも、PAMプラットフォームがラテラルムーブメントを防ぐことで被害を最小限に抑えることができます。

外部の脅威によって最大のリスクに直面するのは誰でしょうか？サイバー犯罪者は、金銭の取引や機密性の高い個人情報の不正入手を狙って特定の業界に近づいています 。

今日のITリーダーはサイバー攻撃の急増によって、既存の脅威と進化を続ける脅威の両方に対処するため、サイバーセキュリティ戦略への積極的な取り組みが必要不可欠です。

最も頻繁にハッキングされる業界のトップ3は以下のとおりです。

ホスピタリティ/旅行

攻撃は毎週発生しており、サイバー攻撃にはランサムウェアやマルウェアが最もよく使用される

製造業

攻撃は毎週発生しており、サイバー攻撃にはフィッシングやマルウェアが最もよく使用される

金融サービス

攻撃は毎月発生しており、サイバー攻撃にはフィッシングやマルウェアが最もよく使用される

結論

攻撃は変化しているが、サイバーセキュリティの根本的なベストプラクティスは変わらない

Keeperの調査は、大規模から中小規模まで多くの企業に大混乱をもたらしている、新たな攻撃手法を明らかにしました。AIを駆使した攻撃を筆頭に、サイバー犯罪者が利用する手口はますます巧妙化しています。技術が発展を遂げる中、進化し続ける脅威に対抗するには適応力が不可欠です。

脅威が絶え間なく進化する現状において、デジタル環境で組織を保護するという基本的なルールは依然として重要です。組織は、蔓延しているサイバー攻撃を防ぐために、パスワードマネージャーやPAMといったソリューションの導入を優先する必要があります。パスワードマネージャーは強力なパスワード慣行を徹底させることでリスクを軽減し、PAMはハイレベルなアクセスを制御および監視することで組織の重要な資産を保護します。そして、両方を組み合わせることで、たとえサイバー攻撃が発生した場合でも、防御力を強化し、起こりうる被害を最小限に抑えることができます。これらのソリューションを統合することで、不正アクセスの制限と全体的なサイバーセキュリティの回復力を強化し、**現在そして将来も**、長年にわたって使用できる多層的なセキュリティ対策が実現します。