エグゼクティブサマリー

セキュリティ優先度調査 2023 年

セキュリティリーダーによる サイバーレジリエンスを巡る戦いは続く

FOUNDRY
an IDG, Inc. company

サイバーセキュリティの敵対者と防御側の戦いでは、少なくとも現時点では敵対者の方が多くのグローバル組織に対して優位に立っています。新たなフィッシング詐欺、マルウェア攻撃、サイバーセキュリティの脅威が容赦なく繰り返されることで、先んじて制することは困難です。さらに悪いことに、敵対勢力は自動化、Cybercrime as a Service（サービスとしてのサイバー犯罪）モデル、なりすまし、適応型の脅威を通じて、高度な攻撃を加速し、その範囲を拡大しています。

実際、セキュリティ優先度調査 2023 年において調査対象になったセキュリティリーダーの 88% が、自分の組織はサイバーリスクに対処できていないと考えています。それは確かにまずい状況のようですが、明るい面としては、この数字が 2022 年の 90% からは減少していることです。その理由は、セキュリティリーダーがリスクの深刻さについて組織全体または一部を苦労しながら説得しているからです（28%）。一部の組織は、人材と技術に十分な予算やリソースを投入していなかったり（26%）、必要なスキルのある人材を確保して維持することができない（26%）状況にあります。

しかし、このような課題にも解決策はあります。予算は増加しているか安定しており、セキュリティチームは AI セキュリティツールをテストして、スピードと俊敏性を向上させることで、スキル不足を補おうとしています。さらに、サイバー保険の契約を充実させ、インシデント対応を強化し、機密データを保護し、企業の回復力を高めるための新技術に投資しています。

セキュリティ優先度調査 2023 年では、世界各国の IT セキュリティエグゼクティブ、管理職、プロフェッショナル 790 人を対象に、現在および今後 1 年間に組織が重点的に取り組む

88%

のセキュリティリーダーは、サイバーリスクへの対処が不十分だと感じている。

悪意のないユーザーエラー（即ちフィッシング被害）は、組織におけるデータセキュリティインシデントの原因の第 1 位。

セキュリティプロジェクトをより深く理解するために調査を実施しました。また、この調査では IT とセキュリティチームが最も時間と戦略的思考を必要とする問題についても明らかにしています。この調査では、組織のデータまたはシステムが侵害されたことを示すイベントを「セキュリティインシデント」と定義しています。これには、ランサムウェア攻撃、データ侵害、第三者またはサプライチェーンへの侵入など、さまざまなセキュリティ侵害が含まれます。

セキュリティインシデントの原因と結果

あらゆるセキュリティ技術が利用可能であっても、セキュリティインシデントの責任はほとんどのケースで人間にあることを肝に銘じる必要があります。セキュリティインシデントの原因として最も多く挙げられたのは悪意のないユーザーエラーで、今年は 31% でした。その数は年々少しずつ減少しており、2021 年は 44%、昨年は 33% でした。これは、セキュリティ意識のトレーニングが増加したことや、ゼロトラストなどのセキュリティモデルが好影響を及ぼしている可能性があります。セキュリティインシデントの他の主な原因には、パッチ未適用ソフトウェアの脆弱性（27%）、第三者のセキュリティ脆弱性（25%）、およびオン / オフプレミスのサービスやシステムの設定ミスなどが挙げられています。

セキュリティの最優先事項

セキュリティリーダーは、セキュリティインシデントに対応するための適切な準備（41%）を筆頭に、来年の優先事項を数多く挙げています。機密・機微データの保護を強化させたいと考えています（36%）。企業の回復力も最大の関心事であり、34% の組織が IT とデータセキュリティのアップグレードを計画しており、33% がクラウドのデータとシステムのセキュリティを向上させたいと考えています。また、フィッシング攻撃やその他の人為的ミスを悪用した攻撃に引っかかる従業員は減少している一方で、32% の組織は依然として、エンドユーザーに対するセキュリティ意識向上トレーニングを強化・改善する計画を立てています。

今年のセキュリティ優先事項トップ 5:

1. セキュリティインシデントに対応するための適切な準備
2. 機密・機微データの保護強化
3. IT とデータのセキュリティをアップグレードして、会社の回復力を強化
4. クラウドのデータとシステムのセキュリティを向上
5. トレーニングを通じたエンドユーザーのセキュリティ意識の向上

セキュリティリーダーが
優先度を上げざるを得ない課題：

1. ガバナンスとコンプライアンス規制への対応
2. 予算の制約 /ROI の実証
3. 従業員の意識と教育の問題

しかし、こうした優先事項はしばしば逆風にさらされます。セキュリティリーダーは常に時間をやりくりする必要に迫られており、最近では、ガバナンスとコンプライアンス規制への対応に時間が取られています（26%）。セキュリティリーダーの半数近く（46%）は、SEC の新しい規則が自社のサイバーセキュリティ対策に影響を与えていると答えています。この規則では、サイバーセキュリティインシデントが投資家にとって重要であると判断されてから 4 日以内に情報を開示することを義務付けています。大企業の 1/3 以上（38%）が重要性を判断するためのプロセスがあると答えており、中小企業では 22% でした。全体の 30% はまだプロセスを開発中で、29% はプロセスがないと答えています。

98%

のセキュリティ予算が、今後 12 か月間で増加または横ばいで推移する。

セキュリティへの支出を決定する要素

- デジタルトランスフォーメーションの取り組み（51%）
- コンプライアンスと規制上の義務（45%）
- 業界のベストプラクティス（43%）

調査回答者によると、セキュリティの優先順位が低い原因として、予算の制約（24%）、従業員の意識やトレーニングの問題（23%）、IT 監査（22%）などを挙げています。

セキュリティの投資計画

全体的なセキュリティ予算は、調査対象のほぼすべての組織（98%）で今後 1 年間に増加するか、横ばいになる見込みです。全体的な支出を決定する要素には、デジタルトランスフォーメーションへの取り組み（51%）、コンプライアンス規制上の義務（45%）、業界のベストプラクティス（43%）など、ビジネスダイナミクスの変化に伴うリスクの変化によるものが挙げられています。具体的には、IT とセキュリティ部門のリーダーは、認証、データ分析、クラウドデータ保護、クラウドベースのサイバーセキュリティサービス、サイバーリスク保険（それぞれ 32%）などの分野を改善することに、集中的に支出しています。

技術：導入済みのものと次に導入されるもの

各組織は、過去 12 か月間に、廃止した数よりも多くのセキュリティツール、技術、サービス

> **69%**
> のセキュリティ意思決定者は、どのセキュリティツールやソリューションが自社に最適なのかを理解することがより困難になっていることに同意している。

を追加しています。3/4（75%）の組織が過去 1 年間に 3 つ以上の新しいセキュリティツールを追加したのに対し、同時期に 3 つ以上のツールを廃止した組織は 56% でした。

現在「使用されている」セキュリティ機能を尋ねると、認証(79%)、エンドポイント保護(76%)、アクセス制御（75%）、データのバックアップとリカバリーサービス（74%）、セキュリティ教育 / 啓発研修（74%）などが挙がりました。

組織は、セキュリティ予算の一部をこれら既存技術の改善に費やしています。たとえば、20% の組織が認証ツールをアップグレードまたは改良しており、アクセス制御（20%）も同様です。

検討中の最新セキュリティツール

69% のセキュリティリーダーは、自社にとってどのセキュリティツールやソリューションが最適なのかを把握することはより困難になっており、最適なセキュリティ技術を見定めるために数十種類の候補を調査しています。

前述したように、セキュリティリーダーは認証機能の改善を目指しており、そのためか、積極的に調査されている技術の筆頭がゼロトラストで 32% を占め、さらに 49% はすでにゼロトラストを使用しています。これらの数字は 2022 年から変化しておらず、調査段階の組織がまだ選択肢を検討していることを示していると思われます。

調査中の最新セキュリティツール上位 5 つは、セキュアアクセスサービスエッジ（SASE）、偽装技術、拡張検知と対応（XDR）、生体認証でした。

67% の組織は、セキュリティ技術に AI を活用している。

72% がすでに恩恵を受けており、未知の脅威の迅速な特定がメリットの第 1 位。

AI の台頭

進化し続ける脅威に対抗し、人員不足を補うために、自社のセキュリティ技術に人工知能を活用している企業は約 67% に達しています。この数字は大企業(79%) で高く、中小企業(55%) では低くなっています。AI は、脅威検知(44%)、マルウェア検知（36%）、アラートとトリアージの自動化(32%)、リアルタイムリスク予測(26%) に活用されています。セキュリティ責任者の

> **34%**
> のセキュリティの ITDM は、
> 必要なレベルの補償を得るためには、
> 複数のサイバーリスク保険に加入する
> 必要があると述べている。

3/4 近く（72%）が、自組織は AI を活用したセキュリティ技術の恩恵を受けていると答えています。これにより、未知の脅威をより迅速に特定し、対応時間を短縮し、時間のかかるタスクを排除し、従業員の作業負荷を軽減することができます。また、AI は従来型ソリューションよりも高速に大量のデータを選別することができます。

サイバー保険の加入

前述したように、今年の最大の支出の 1 つはサイバー保険への加入です。すでに半数以上の企業がサイバー保険に加入していますが、保険金を請求しなければならなかった企業はわずか 18% でした。さらに 22% が積極的に保険契約を調査しています。一部の組織は、これらの契約を必要悪と考えており、回答者の約半数がサイバーリスク保険はリスクを軽減する戦略の重要部分であると主張し（52%）、約半数がサイバー保険は高価すぎるとも述べています（53%）。また、契約の更新がより難しくなっている（44%）とも述べています。保険会社の要件を満たすのが難しすぎて、労力に見合わないと感じている人もいました（40%）。他には、必要なレベルの補償を得るためには、複数のサイバーリスク保険に加入する必要がある（34%）との意見もありました。

人と組織

組織のトップにおけるサイバーセキュリティリーダーは 1 年前と変わっておらず、65% の企業が CISO、CSO、またはセキュリティのトップエグゼクティブを擁しています。その数字は、大企業では昨年よりわずかに多く（83%）、中小企業では昨年よりわずかに少なく（47%）なっています。

> **85% のセキュリティリーダーは、取締役会と定期的または頻繁に協議している。**

国内外でセキュリティへの関心が高まるにつれ、取締役会はセキュリティ問題に対してより積極的な役割を果たすようになっています。セキュリティリーダーの大多数（85%）は、取締役会と定期的または頻繁に協議していると答えています。半数近く（48%）は、月に 1 回以上取締役会と協議しています。このコミュニケーションが以前より頻繁になった理由の 1 つは、セキュリティリーダーの 25% が取締役会の直属になっており、1 年前の 20% から増加したことにあります。

57%

は、セキュリティオペレーションセンターを設置する際の最大の課題として、スキルと知識の不足を挙げている。

さらに、より多くのセキュリティリーダーが、すべてのセキュリティ技術を統合・調整し、組織の脅威検知、対応、予防能力を向上させるために、オペレーションを一元化しています。約91%の組織は、社内または外部にセキュリティオペレーションセンター（SOC）を設置しているか、追加する計画があります。しかし、これらの組織のほとんど（90%）は、オペレーションセンターの人員とスキルの不足が続いており、SOCの予算も不足しています（35%）。

IT リーダーの半数以上は、人材不足を補うために、現在のスタッフのスキルアップと新しい役割への移行を進めています（56%）。一方で、一部のセキュリティ機能を委託したり（42%）、AI によりセキュリティ対策を自動化しています（38%）。

結論

セキュリティリーダーの実に 88% は、自組織がサイバーリスクへの対処ができていないと考えています。特に直面しているリスクの重大性を組織に説得することが重要です。

こうした状況を改善するために、より多くのセキュリティエグゼクティブが取締役会と定期的に協議しており、約半数の回答者が、取締役会はサイバーセキュリティ関連の問題について経験を積んでいると答えています。

IT リーダーは、新しいソリューションに投資し、現行のセキュリティスタックへの支出を増やすことで、セキュリティリスクに対処しています。

セキュリティリーダーの 98% は、今後 12 か月間で自社のセキュリティ予算は増加または横ばいで推移すると予想しています。サイバー保険や人工知能をセキュリティ技術に追加することで、防御の強化、データ保護、セキュリティ意識の向上に取り組むと答えています。

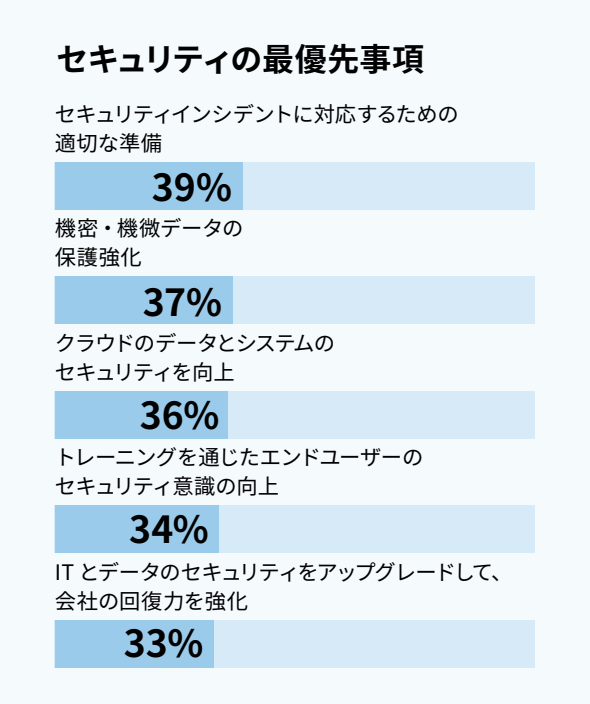
本調査について

セキュリティ優先度調査 2023 年は、790 人のセキュリティプロフェッショナルを対象にして実施した Foundry のオンラインアンケートのデータを分析しています。回答者全員が IT および / または企業の IT および物理的なセキュリティに関する意思決定に関与しており、77% が IT またはセキュリティのエグゼクティブなどの役職者です。回答者は、主に北米（49%）の企業を代表しており、一部アジア太平洋地域（33%）とヨーロッパ（18%）の企業が含まれています。これらの企業は、製造、テクノロジー、金融サービス、サービス、医療、サービス産業など、さまざまな業界にわたっています。平均企業規模 従業員数 11,110 人。

グローバルでの主な相違点

多くの質問において、セキュリティリーダーの回答は調査対象の 3 つの地域すべてで類似の結果を示しています。しかし、中にはいくつかの際立った重要な相違点がありました。

北米



セキュリティの戦略的取り組みより優先度を上げざるを得ない課題

- ガバナンスとコンプライアンス規制への対応 **(28%)**
- 予算の制約 /ROI の実証 **(27%)**
- 従業員の意識と教育の問題 **(25%)**

北米のセキュリティリーダーは何に支出を増やしているか？

98% は、今後 1 年間で予算は増加または横ばいで推移すると予想している。
以下の項目に支出を増やしている：

- サイバーリスク保険 **(35%)**
- データ分析 **(31%)**
- クラウドデータ保護 **(30%)**
- エンドポイント保護 **(30%)**

北米のセキュリティ意思決定者は、セキュリティスタックに追加するツールを調査している

以下の技術に着目している：

- SASE（セキュアアクセスサービスエッジ）**(34%)**
- SOAR（セキュリティオーケストレーションの自動化と対応）**(34%)**
- XDR（拡張検知と対応）**(33%)**
- ゼロトラスト技術 **(32%)**

AI がセキュリティに与える影響

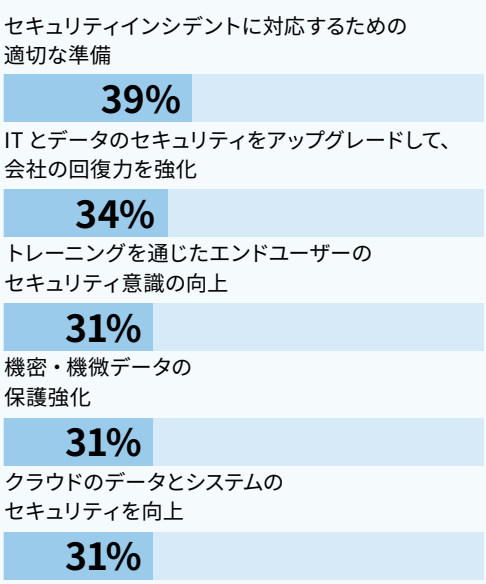
63%
の北米におけるセキュリティ ITDM は、セキュリティ技術に AI を活用している。

67% がすでに以下のメリットを享受している：

- 未知の脅威の迅速な特定 **(33%)**
- 検知と対応時間の短縮 **(30%)**
- AI は従来型ソリューションよりも高速に大量のデータを選別 **(30%)**

EMEA

セキュリティの最優先事項



セキュリティの戦略的取り組みより優先度を上げざるを得ない課題

- ガバナンスとコンプライアンス規制への対応 **(30%)**
- 組織外で発生するサイバー脅威のリスクへの備えや対処 **(26%)**
- 従業員の意識と教育の問題 **(23%)**

EMEA のセキュリティリーダーは何に支出を増やしているか？

96% **は、今後 1 年間で予算は増加または横ばいで推移すると予想している。**以下の項目に支出を増やしている：

- 認証 **(41%)**
- クラウドデータ保護 **(39%)**
- アプリケーション開発セキュリティ **(39%)**
- クラウドベースのサイバーセキュリティサービス **(38%)**

EMEA のセキュリティ意思決定者は、セキュリティスタックに追加するツールを調査している

以下の技術に着目している：

- ゼロトラスト技術 **(28%)**
- CASB（クラウドアクセスセキュリティブローカー）**(27%)**
- SASE（セキュアアクセスサービスエッジ）**(26%)**
- 偽装技術 **(26%)**

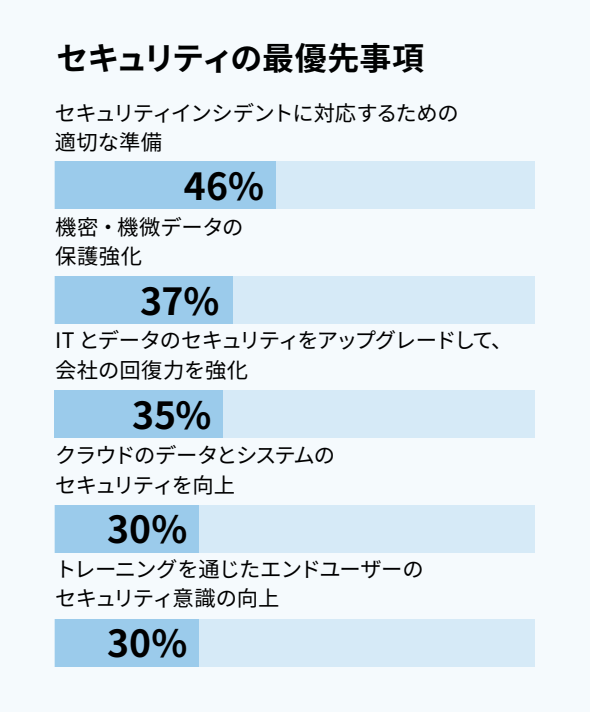
AI がセキュリティに与える影響

73%
の EMEA におけるセキュリティ ITDM は、セキュリティ技術に AI を活用している。

83% がすでに以下のメリットを享受している：

- 未知の脅威の迅速な特定 **(44%)**
- 検知と対応時間の短縮 **(40%)**
- 従業員のワークロードの削減 **(30%)**

アジア太平洋地域



セキュリティの戦略的取り組みより優先度を上げざるを得ない課題

- IT 管理者 **(24%)**
- 予期せぬビジネスリスク **(23%)**
- ガバナンスとコンプライアンス規制への対応 **(21%)**
- 予算の制約 /ROI の実証 **(21%)**

アジア太平洋地域のセキュリティリーダーは何に支出を増やしているか?

98% は、今後 1 年間で予算は増加または横ばいで推移すると予想している。以下の項目に支出を増やしている:

- クラウドベースのサイバーセキュリティサービス **(34%)**
- サイバー復旧サービスを含むデータのバックアップとリカバリー **(34%)**
- 認証 **(33%)**
- アプリケーション開発セキュリティ **(33%)**
- データ分析 **(32%)**
- クラウドインフラストラクチャ管理技術 **(32%)**

アジア太平洋地域のセキュリティ意思決定者は、セキュリティスタックに追加するツールを調査している

以下の技術に着目している:

- ゼロトラスト技術 **(34%)**
- XDR (拡張検知と対応)**(32%)**
- 偽装技術 **(30%)**

AI がセキュリティに与える影響

68%

のアジア太平洋地域における
セキュリティITDM は、セキュリティ技術に
AI を活用している。

75% がすでに以下のメリットを享受している:

- 未知の脅威の迅速な特定 **(39%)**
- 検知と対応時間の短縮 **(30%)**
- 時間のかかる作業の削減 **(28%)**
- 従業員のワークロードの削減 **(28%)**

市場動向の考察

市場動向に関するリサーチは、マーケターが既存顧客と潜在顧客についての理解を深め、質の高いつながりを構築するために**極めて有益**な手段です。Foundryは、テクノロジーバイヤーとベンダーの懸け橋を築く方法の一つとして、こうしたリサーチを重視しています。弊社は世界中の極めて重要なテクノロジーバイヤーやインフルエンサーと直接的な関係があるため、あらゆる顧客マーケティングにおいて貴重な情報をまとめ、価値あるリサーチ成果を生み出すことができます。弊社はこうしたリサーチを通じてアナリティクス、クラウド、IoT、セキュリティなどの特定のテクノロジーに関するお客様の考え方や課題を探り、IT購買プロセスにおける役割の変化を調べることにより、機会を見出すために必要な情報をテクノロジーマーケターに提供しています。

どのようなリサーチの実施が可能か、については、FoundryCo.com/tools-for-marketersでご確認いただけます。こちらに掲載されている調査のいずれかについて、詳細な結果の提示をお求めの場合は、Foundryの営業責任者にお尋ねいただくか、もしくはFoundryCo.com/contact-usからお問い合わせください。

購買プロセス

Foundryは毎年、エンタープライズのIT購買プロセスを詳しく調査し、誰が関与しているのか、誰が意思決定に影響を与えているのか、購買担当者は購買プロセス全体を通じてどのようなソースからテクノロジーに関する最新情報を得ているのか、購買担当者は提携しているベンダーとどのように関わることを望んでいるのか、を調査の上、報告しています。詳しくは、FoundryCo.com/customerjourneyをご覧ください。

購買プロセスに関するリサーチ内容

- テクノロジーに関する意思決定者の役割と影響力
- カスタマーエンゲージメント

テクノロジーに関する知見

Foundryは毎年、お客様が重視しているテクノロジーについて調査し、ビジネス上の課題、原動力、エンタープライズ内での利用状況を把握しています。このような調査は、顧客が何を重視しているか、市場がどこに向かっているかをITマーケターが理解できるようにするために考案されています。

役割と優先事項に関するリサーチ内容

- CIOを対象としたテクノロジーに関する調査：テクノロジーの優先事項
- CIOの現状

特定のテクノロジーに関するリサーチ内容

- データおよびアナリティクス
- クラウドコンピューティング
- デジタルビジネス
- セキュリティの優先事項

Foundryの最新情報

ニュースレター：メディアやマーケティングのトレンド、Foundry独自の調査結果、製品やイベントの情報をニュースレターで配信しています。ご登録はFoundryCo.com/newsletterで受け付けております。

Twitter：@FoundryIDG

LinkedIn：https://www.linkedin.com/company/foundryidg/

Website（グローバルサイト）：FoundryCo.com

Website（日本サイト）：FoundryCo.com/japan

Foundry（ファウンドリー）のご案内

弊社Foundryのビジョンは、テクノロジーを正しく活用することで世界をより良い場所にすることです。なぜなら、テクノロジーが適切に使われることは、世の中の善のために良い力となると信じているからです。

Foundry (an IDG, Inc. company) は、信頼されるVoiceとして、知識やエンゲージメント、そしてテクノロジーやセキュリティに関する意思決定をする人たちのコミュニティとの関係を深める、品質の高いコンテンツを提供しています。こうしたコンテンツを配信する弊社メディアブランドであるCIO®, Computerworld®, CSO®, InfoWorld®, Macworld®, NetworkWorld®, PCWorld®そしてTech Hiveは、最も影響力のあるテックバイヤーを対象に、進化するテクノロジー業界の最新情報を提供しています。

こうした信頼されたブランドと、弊社のグローバル規模のデータインテリジェンスプラットフォームを使い、市場の動向から購買意欲を特定、活性化することでお客様の成功をサポート致します。また、マーケティングサービスとしては、ビデオ、モバイル、ソーシャル、デジタルなど、様々なメディアでマーケティングに特化したコンテンツも作成しています。

詳細はFoundryCo.comにてご確認下さい。