CISOにとってのアイデンティティの戦略的価値

ネットワーク境界が消失しつつある中で、アイデンティティがサイバーセキュリティのコントロールプレーンとなり、セキュリティ運用は大きく変化しています。本資料では、このような変化に関してEnterprise Strategy GroupがOktaと提携して実施した調査*の概要をご紹介します。この調査では、アイデンティティセキュリティがCISOにとっていかに重要な焦点となっているかについて、5つの重要な知見が得られました。

1. CISOは守りから攻めに転じている
2. CISOの責任が、戦略的なビジネスの推進へとシフトしている
3. CISOはアイデンティティが組織にとって最大の脆弱性であると認識している
4. CISOはアイデンティティセキュリティに簡単な解決策はないと考えている
5. テクノロジーの肥大化によって、アイデンティティセキュリティの問題が悪化している

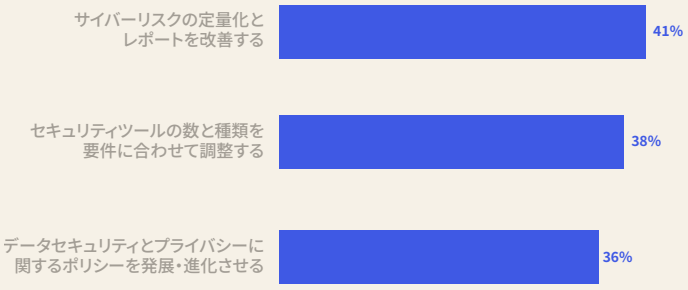
okta

重要な知見その1：

CISOは守りから攻めに転じている

従来の境界ベースのエンタープライズセキュリティ戦略は、どうしても守りに偏りがちでしたが、そのような姿勢ではもはや現代の業務に対応しきれなくなっています。ESGの調査によると、CISOの「取り組むべき課題」の上位項目はすべて、リスクの定量化や報告、制御の合理化、データプライバシーなど、先取的な戦略に集中していることがわかりました。

CISOが取り組むべき最も重要な課題



重要な知見その2：

CISOの責任が、戦略的なビジネスの推進へとシフトしている

ESGの調査によると、CISOが自身の責任を捉える視点は、より戦略的なものへと変化しつつあり、ビジネスにとって重要な成果の実現へとシフトが進んでいます。

CISOの最も重要な責任領域

データセキュリティとプライバシーに関するポリシーを発展・進化させる（ゼロトラストなど）

CISOは成功の測定基準の見直しを進めており、インシデント発生率や応答時間にとどまらず、ダウンタイムの頻度や期間がセキュリティイベントにどのように関連しているかなど、セキュリティがビジネスに与える影響を重視するようになっています。

ビジネスの成長や目標をセキュリティでどのように実現できるかを定量化・実証する

以前はコンプライアンス指標に重点をおいていたCISOの仕事も、今ではビジネスの生産性やその他の「人的指標」についてより戦略的に捉えるようになっています。

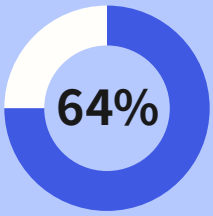
従業員と顧客全体で、堅牢でシームレスな認証を確保する

アイデンティティガバナンスの優先順位が急上昇しており、今回調査対象となったCISOも、認証情報管理やアクセスレビューなどの責務を、従業員や顧客のスムーズなアクセスをサポートするという観点から捉えるようになっています。

重要な知見その3：

CISOはアイデンティティが組織にとって最大の脆弱性であると認識している

事後対応型から事前対応型の戦略に移行しているとはいえ、調査対象のCISOの約3人に2人が、サイバー攻撃を防ぐのは難しいと回答しています。特に注目すべきは、CISOはアイデンティティセキュリティを最大の脆弱性として認識しており、自社の全体的なセキュリティ態勢を弱体化させるさまざまなアイデンティティの課題を報告している点です。これは意外なことではありません。広く報じられている調査によれば、アイデンティティは現在、データ侵害の主要な経路となっています。



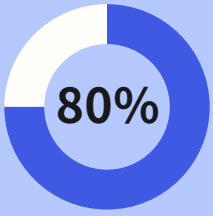
サイバーセキュリティ攻撃を阻止するのは**困難**だと回答したCISOの割合

3人中2人

セキュリティインシデントの大部分がアイデンティティに起因すると回答したCISOの割合

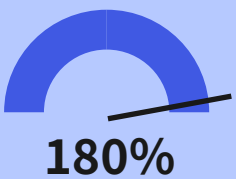
調査対象のCISOが挙げた、サイバー防御の妨げとなるアイデンティティの主な課題

1. 不正なアカウントの作成とサインインの試行を大規模に検出して防ぐことができない
2. アイデンティティガバナンスの実践に一貫性がない
3. より強力な認証方式に対応しておらず、パスワードに依存しすぎている
4. アイデンティティの運用が手作業中心で断片化している
5. MFAが不十分である



アイデンティティの侵害から始まるデータ侵害の割合

Verizon 2024年版データ侵害レポート



アイデンティティ関連攻撃の前年比増加率

Verizon 2024年版データ侵害レポート

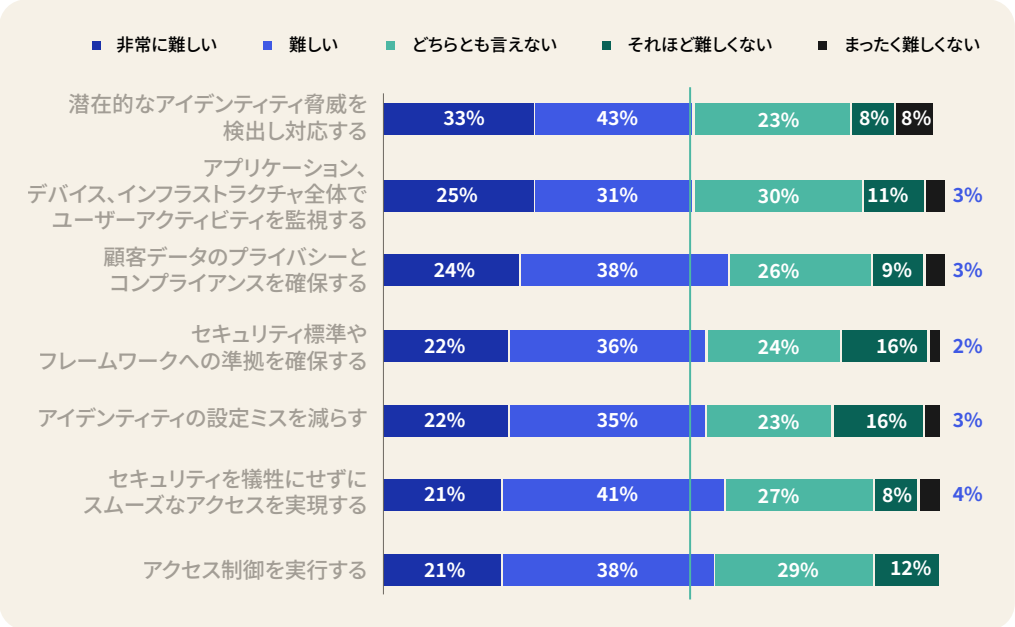
okta

重要な知見その4：

CISOはアイデンティティセキュリティに簡単な解決策はないと考えている

大半のデータ侵害にアイデンティティが関与していることを踏まえると、調査対象となったCISOの大多数（76%）がアイデンティティセキュリティの強化を最優先事項として考えているのも驚くにはあたりません。では、なぜいまだに「解決」されていないのでしょうか。

理由は、問題が1つではなく、さまざまな方面でアイデンティティセキュリティの戦いが繰り広げられているからです。大多数のCISOが、アイデンティティセキュリティの**あらゆる要素**が困難であると述べています。



重要な知見その5：

テクノロジーの肥大化によって、アイデンティティセキュリティの問題が悪化している

CISOの直面する「ビジネス推進」と「ビジネス保護」の両課題は1つの継続的なテーマに収束します。それは、テクノロジーの肥大化がすべてを悪化させていることです。テクノロジーの分散的な導入とSaaSの無秩序な増加という課題が多くの企業に蔓延していますが、その影響は今や現在セキュリティスタックにまで及んでいます。本調査では、ほとんどの組織が50社以上の異なるサイバーセキュリティベンダーと連携していることがわかりました。セキュリティチームは、複数のソリューション間でプロセスやデータフローを手作業で調整することに多くの時間を費やしており、CISOはうまくそれらを統合させて冗長性を排除しようと懸命になっています。

本調査で以下のことも明らかになりました。

アイデンティティセキュリティの最大リスク

1. セキュリティツール全体に点在する可視性のギャップ
2. アカウントの設定ミスや過剰な権限付与

スムーズなアクセスを実現する上での最大の障壁

1. ソリューション全体での監査証跡の管理
2. 複数のアイデンティティソリューションの運用の複雑さ

一般的な組織は60社の異なるサイバーセキュリティベンダーを利用している

Okta：アイデンティティファーストのセキュリティ戦略を支える

ESGの調査によって明確に実証されたのは、アイデンティティがもはや単なるIT機能ではなく、現代のエンタープライズセキュリティの基盤であるということです。Oktaのアイデンティティプラットフォームは、包括的なセキュリティと俊敏性を提供するために構築されており、予防的なアイデンティティファーストのアプローチで組織を牽引したいと考えるCISOを支援します。Oktaは、CISOが守りから攻めへとシフトできるようリスクの低減、複雑性の軽減、そして進化する脅威環境への自信ある対応を実現する、堅固なアイデンティティセキュリティ基盤を提供しています。

※ 本調査は、Enterprise Strategy GroupがOktaと共同で2025年1月から2025年2月頃に実施したものであり、北米、EMEA、APJ地域の150名以上のCISOにインタビューを行いました。

プラットフォームについて、さらに詳しい情報をご用意しています。

現在抱えておられる課題についてお聞かせください。
Oktaがどのように支援できるかをご案内いたします。

詳細を見る