Google Workspace

セキュリティの転換点

漸進的な修正では対応できなくなっている理由

2024 年 10 月

ごあいさつ

働き方や働く場所の変化によってビジネス環境が変化し続ける中、世界中の組織が急速に増大するセキュリティの脅威に直面しています。最近の Mandiant M-Trends レポートによると、昨年だけでも大規模な政府機関や民間企業に対する国家主導のスパイ活動や金銭目的のランサムウェア攻撃が増加したほか、通信からエンターテイメントまであらゆる業界でデータ侵害が相次いで発生しています。

組織が新たな脅威の状況への対処方法をより深く理解できるよう、Google はこのほど Hypothesis Group と提携して、グローバルなセキュリティに関する委託調査を実施しました。この調査では中規模からエンタープライズ規模の組織における 2,000 人以上の意思決定者を対象として、セキュリティへのアプローチ、現在起こっている変化、将来的の計画について話を聞きました。

この調査でわかったのは、未来の働き方はすでに広がっており、それに伴ってセキュリティ リスクの新たな時代が到来しているということです。しかし、多くの組織はこの変化に適応することなく、従来型の戦略とツールに注力しています。その結果、高額な支出を伴うセキュリティ インシデントが増加しており、事業運営の混乱、顧客データの侵害、信用の低下が引き起こされています。セキュリティに関して、現状維持ではもはや十分ではありません。今こそアプローチを根本的に変え、改善する必要があります。

企業に必要なのはより優れた保護を提供するセキュリティ プロダクトであり、使用するプロダクトの数を増やすことではありません。Google は、セキュリティ インシデントやセキュリティ侵害を当たり前ではなく、例外的な事象であるべきと考えています。また、安全性を重視して設計されたソリューションによって、組織が攻撃を未然に防ぐ能力にこれまで以上に自信を持てるよう支援したいとも考えています。

この調査が、お客様の組織とそのセキュリティ ニーズに関する継続的な対話の第一歩となり、業務の安全性向上に向けた取り組みにおいて、Google Workspace が戦略的パートナーとしてどのような役割を果たせるかを知っていただくきっかけになれば幸いです。

Andy

Andy Wen
Google Workspace Security
プロダクト管理シニア ディレクター

目次

はじめに

仕事を取り巻く環境は変化し続けています。ハイブリッドな勤務形態が何百万人もの働く人々にとって標準となり、AI がさらに進化する中、セキュリティ上の脅威は、変化に乗じて巧妙化と拡大を続けています。組織は、このような増大する新たなリスクへの認識を高めてはいますが、その多くは職場環境を本当に保護するために必要な大胆な選択を行うことを躊躇しています。

このホワイト ペーパーでは、今日のビジネス環境を緊迫させている主な要因について詳しく説明します。自社の戦略に自信を持つリーダーがいる一方で、深刻なセキュリティ インシデントが発生し続けていることは、認識と現実の間にギャップがあることを示しています。組織は、同じような対策を積み重ねるのではなく、変化の必要性を受け入れることで、このギャップを解消し、セキュリティの問題に適切に対応できるようになります。

Google Workspace は、現状と、組織のセキュリティ ポスチャーを強化するためにできることをより深く理解するために、インサイト、設計、戦略のエージェンシーである Hypothesis Group と提携して多角的な調査を実施しました。このイニシアチブの内容は以下のとおりです。

- 2024 年 7 月 22 日から 8 月 8 日にかけて実施された、米国、英国、インド、ブラジルの中規模組織（従業員数 300～999 人）とエンタープライズ組織（従業員数 1,000 人以上）の 2,000 人を超える IT、ビジネス、セキュリティ担当の意思決定者を対象とする定量的調査
- 2024 年 8 月 22 日から 26 日にかけて実施された、米国の意思決定者 6 人を対象とする定性的インタビュー
- セキュリティの現在の動向と将来に関する、以下の業界専門家との会話:

John McCumber 氏
元 NIST 共同議長、元 Gartner ディレクター、
現セキュリティ コラムニスト

Joshua Scarpino 博士
TrustEngine 情報セキュリティ担当 VP
Assessed Intelligence CEO

Rachel Tobac 氏
SocialProof Security CEO、
Women in Security and Privacy 理事会議長、CISA
Technical Advisory Council ボランティア

主な調査結果

セキュリティは危機的状況にあります。現在のアプローチは持続不可能でコストがかかることが判明した今、組織は進化する脅威に先手を打って対応するため、変化を早急に受け入れる必要に迫られています。

脅威の状況が急速に拡大する中で、セキュリティに対する新たなアプローチが求められていますが、変革に向けた投資を行っている企業はほとんどありません。

1. **現状維持では破綻します。**
   組織はセキュリティ ポスチャーに対する自信を表明していますが、リスクのある行動が数多く見られており、セキュリティ リーダーは懸念を強めています。

2. **組織はセキュリティ強化の必要性を認識しているものの、同じような対策を積み重ねるだけでは不十分です。**
   セキュリティを強化するために、リーダーたちは付加的な変更（ツールの追加、投資の拡大、保険料の増額）を行っています。しかし、セキュリティインシデントは依然として頻繁に発生し、多大なコストを発生させています。

3. **将来に向けた変化が必要です。**
   リーダーたちは、セキュリティ アプローチを合理化し、AI を活用して組織を守りたいという明確な願望を示しています。根本的な非効率性に対処したリーダーは、その場しのぎの解決策に留めたリーダーよりも大きな成果を挙げています。

セキュリティの問題に対処するための組織的なアプローチは、組織の規模や地域によって異なりますが、変化の必要性はすべての組織が認識しています。

4. **中規模組織（従業員数 300〜999 人）のセグメントは、変革の機が熟しています。**
   リーダーたちは旧式のテクノロジーと組織の複雑さに悩まされており、将来に向けて大きな不安を抱いています。しかし、その多くはセキュリティ アプローチを積極的に見直しており、方向転換に前向きです。

5. **世界的に見ると、各地域に独自の課題があり、セキュリティの問題に対応するにはそれぞれが独自のアプローチを策定する必要があります。**
   職場環境が今後も変化し続けることは世界中のリーダーたちが認識していますが、国によっては有効性や持続可能性が実証されたセキュリティ戦略がないため、広範な再評価が必要になります。

1

現状維持では破綻する

組織はセキュリティと働き方への自信を表明していますが、実際の行動には多くの穴があり、セキュリティ部門の意思決定者は夜も眠れない状況が続いています。

自信はあっても、働き方の変化によってセキュリティが低下

多くの組織は、少なくとも理論上はセキュリティに問題なく対処できていると考えています。IT、ビジネス、セキュリティを担当する意思決定者の **96%** が、データ、アプリケーション、デバイス、生成 AI などの新しいテクノロジーに関するセキュリティ管理能力に対して強い自信を表明しています。しかし、この自信を揺るがしかねない働き方の大きな変化が進んでいます。そうした変化には、ハイブリッドな勤務形態の増加や、生成 AI を始めとするさまざまな新しいツールの導入などがあります。

74%

が働き方が劇的に変化したと回答

「私たちは過渡期に生きています。利用できるツールの数は膨大です。しかし、方針と、これらすべての新しいツールを扱うための計画が定まっていないように感じられるため、大きな不安があります。」

- 製薬会社研究ディレクター

リスクの大きいツールと行動のまん延

多くの意思決定者から、組織をリスクにさらす数多くの慣行が報告されています。

- IT ポリシーに従っているのは **56%** のみ
- 組織内で使用されるツールの **19%** は未承認（組織で検証、承認されていない）
- 半数近く（**44%**）は、未承認のツールが「完全に安全」だと信じている
- 3 分の 2（**63%**）は、未承認の生成 AI ツールが毎週のように使用されていると回答
- 半数（**48%**）の意思決定者は、未承認の生成 AI ツールを信頼している

組織の発言と行動のギャップは、現在のセキュリティ ポスチャーに内在するリスクを浮き彫りにしています。さらに、シャドー IT サービスの使用は一般的になっていますがセキュリティ保護が難しく、インシデントだけでなくコンプライアンス違反のリスクも高まります。

> **「組織は、新しいテクノロジーがもたらす新たなリスクを必ずしも理解していないため、絶えず最新のリスクへの対応を迫られるセキュリティ リーダーの仕事は大変です。」**
>
> — **Joshua Scarpino 博士**
> Assessed.Intelligence CEO

セキュリティ リーダーの間で高まる不安

セキュリティ意思決定者（SDM）は、これらのリスクに気づいていないわけではありません。

63%

が、自社のテクノロジー環境のセキュリティは以前と比べて低下していると回答

4 分の 1 のツールがリスクが高いと考えられている

「[環境のセキュリティが低下しているという見解] は、管理が追いつかず、知識も足りていないという感覚に起因していると思います。使用されているすべてのツールとその使用場所、利用方法、さまざまな悪用方法を特定、理解することは、私たち全員にとっての課題です。」

— **John McCumber 氏**

元 NIST 共同議長、元 Gartner ディレクター、現セキュリティ コラムニスト

このようなリスクの高い行動が不安を生み出し、SDM の **93%** がセキュリティ インシデントの発生を懸念しています。この不安の原因は明白です。SDM にとって、最も大きな懸念は脆弱性と生成 AI 攻撃やデータ侵害などの外部攻撃ですが、意図的か、不注意によるものかを問わず、ユーザーの不適切な行動も不安材料となっています。

> **「意思決定者たちは心配で夜も眠れないと言っています。技術的ツールは完璧ではなく、人間による監視が必要な場面が多いため、意思決定者たちは大きなストレスを感じています。」**

— **Rachel Tobac 氏**
SocialProof Security CEO

93%
の SDM がセキュリティ インシデントの発生を懸念している

最も懸念されている攻撃と侵害

生成 AI 攻撃	**31%**
データ侵害	**30%**
サイバー恐喝	**26%**

エンドユーザーに関する主な懸念事項

不正アクセス	**24%**
従業員の過失	**20%**
認証情報の漏洩	**17%**

2

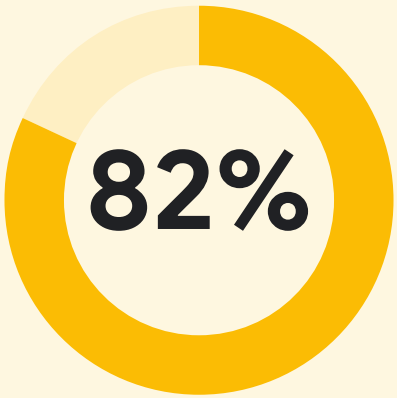
組織はセキュリティ強化の必要性を認識しているものの、同じような対策を積み重ねるだけでは不十分

セキュリティ対策強化の必要性は、かつてないほど緊急性を増しています。SDM は、現在の戦略が不十分であることを痛感しており、広範な改善の必要性を認識しています。しかし、広く採用されているアプローチは不十分で、逆効果になることも多いことが判明しています。

セキュリティ強化の明らかな必要性

82% の SDM が、セキュリティ対策を改善する必要があると回答しています。
半数以上が、現代の職場環境の複雑さにより、組織がセキュリティを維持しにくくなっていると回答しています。
59% が、時代遅れのテクノロジーに依存しているため、将来のセキュリティ ニーズに対する備えが不十分になっていることを認めています。

> 「長年にわたって数多くのセキュリティ ソリューションを導入してきましたが、一部は非常に古くなっており、交換か、少なくとも再評価が必要です。」
>
> — メディア、エンターテイメント業界 IT 担当 VP



のセキュリティ意思決定者が、組織のセキュリティ対策を改善する必要があると回答

漸進的な変化では不十分

半数の SDM が、過去 2 年間にサイバーセキュリティ戦略を大きく変化させたと述べていますが、それらの多くは革新的なものではなく、漸進的な変化にすぎません。実際、多くの組織はただ同じような対策の数を増やしているだけに見えます。

過去 2 年間における セキュリティ上の 主な変更

サイバーセキュリティ保険料の増額	37%
サイバーセキュリティ予算の増額	35%
ライセンスのアップグレード	34%
新しいサイバーセキュリティ プロバイダの追加	31%

これらの調整はある程度は有益かもしれませんが、戦略の根本的な変化というよりも、既存対策の増強と呼ぶべきものです。

> 「人々は同じような対策を次々と重ねて、費用だけが嵩み続けています。「多額の資金を投入したが、実際には問題の解決になっていない」と嘆く同僚や顧客の声を耳にします。非常に高価なプラットフォームにお金を投じても、パスワード マネージャーがないチームもあります。それでは、お金をかけて防弾窓にしたのに、ドアが完全に開いているようなものです。」

— **Rachel Tobac 氏**
SocialProof Security CEO

62%
新しい機能が必要な場合に既存ツールを交換せず、拡張すると回答した SDM の割合

10
エンタープライズ組織で使用されるセキュリティ ツールの平均数

61%
2 年前と比べて使用するセキュリティ ツールの数が増加した組織の割合

27%
重複しているセキュリティ ツールの割合

ツールの増やしすぎ問題と戦略の一貫性を高める必要性

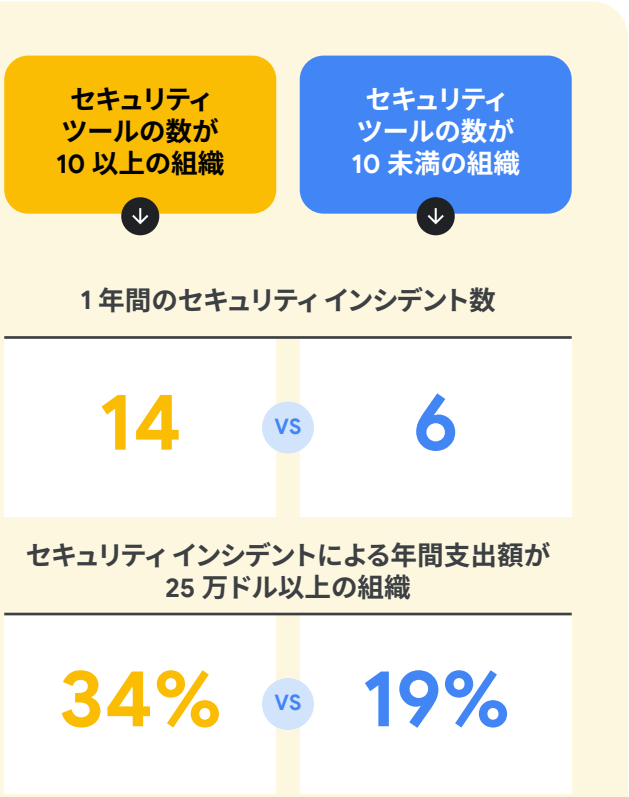
3 分の 2 以上の組織で、環境のセキュリティ保護にかける時間と費用を増やしても、依然として高額な支出を伴うインシデントが多数発生しています。

ツールの数を増やせばよいというわけではありません。10 を超えるセキュリティ ツールを使用している組織では、セキュリティ インシデントの発生頻度とコストの両方が高くなっています。

81%
インシデントが 1 年に 1 回以上発生する組織の割合

8 **1 年間に報告されたインシデントの平均数**

488 万米ドル
データ侵害 1 件のコスト総額の世界平均（2024 年）[1]



「セキュリティの要素ごとに異なるベンダーを使用していると、管理が非常に難しくなり、費用対効果も低下します。ですから、統合が必要です。現在のベンダー数を維持することは現実的ではありません。」

— メディア、エンターテイメント業界 IT 担当 VP

1.IBM - Cost of a Data Breach Report 2024

3

将来に向けた変化が不可欠

今回の調査で、SDM はセキュリティに対するアプローチの変更に前向きであり、新しい戦略やテクノロジーの導入に積極的な SDM が優位に立っていることが明らかになりました。

変化を切望

現在の情勢を受け、セキュリティ戦略に対する組織の考え方が変化しつつあります。

78%

がサイバーセキュリティの現状を受け、セキュリティに対する組織のアプローチの見直しを進めている

73%

がコストに関係なく、新しいセキュリティ アプローチの採用に積極的である

意思決定者は合理化されたセキュリティ ソリューションへの関心を強めており、**65%** が統合セキュリティ システムへの興味を示しています。また、さまざまなデータソースを単一のインターフェース内に統合するプラットフォームが、プロセスの合理化、オペレーションの強化、複数のツールを管理する負担の解消、時間の節約など、目に見えるメリットをもたらすことに同意しています。

生成 AI も注目を集めており、セキュリティ意思決定者の **59%** が、進化する脅威に対抗するための重要なツールであると考えています。

> 「AI がセキュリティにもたらす最大のメリットは、イベントへの対応、現行ツールの利用、ツールのオーケストレーションによる対応、報告、クリーンアップが可能になることです。」
>
> — **John McCumber 氏**
>
> 元 NIST 共同議長、元 Gartner ディレクター、現セキュリティ コラムニスト

59%

の SDM が生成 AI をデータセキュリティの重要ツールであると考えている

生成 AI を導入する主な理由

データ プライバシーの強化	**43%**
脅威インテリジェンスの強化	**37%**
セキュリティ運用の改善	**36%**
脅威の予防	**33%**

変化に投資するメリット

新しいアプローチに対する関心が高まっているにもかかわらず、古いツールの交換を積極的に進めている SDM は **38%** のみで、**62%** は現在の設定を拡張するに留まっています。

古いツールを交換した SDM の優位性（拡張に留めた SDM との比較）

1 年間の[セキュリティ インシデント報告数が 20% 少ない]

2 年前と比べ、使用するセキュリティ ツールの数が[同じか、減少した]と回答した割合が高い
（44% VS. 36%）

以前よりも環境のセキュリティ保護に[費やす時間が減少した]と回答した割合が高い
（33% VS. 28%）

> 「チームは、同じ保護機能の購入を繰り返す前に、購入したツールを監査して、すでに導入されている機能を把握する必要があります。利用可能な機能と、カバーする必要があるセキュリティ領域を把握することで、組織はツールをより深く理解でき、最終的にはセキュリティ インシデントや問題の減少につながります。」

— **Rachel Tobac 氏**
SocialProof Security CEO

4

中規模組織では変革の機が熟している

中規模組織（従業員数 300〜999 人）は、セキュリティの潜在能力を十分に発揮できておらず、そのことを把握しています。現代の職場環境の複雑さに苦慮するこれらの企業の懸念は、エンタープライズ組織（従業員数 1,000 人以上）よりもはるかに深刻です。

中規模組織の意思決定者は、現在のテクノロジー環境に対する不安の高まりも表明しています。こうした不安は、職場における生成 AI の急速な導入によってさらに増大しています。

73%

が、生成 AI の利用拡大によって組織内でのセキュリティ インシデントが増加したと回答

（エンタープライズ組織では 58%）

抱えている課題

	エンタープライズとの差
71% が、旧式のテクノロジーによって将来への備えが不十分になっていると回答	+23 ポイント
63% が、仕事の複雑さがセキュリティを低下させていると回答	+11 ポイント
73% が、生成 AI の利用がセキュリティ インシデントの増加につながったと回答	+15 ポイント

心情的負担

	エンタープライズとの差
63% が、起こりうるセキュリティ インシデントに大きな不安を感じている	+13 ポイント
63% が、自社のテクノロジー環境のセキュリティは以前と比べて低下していると回答	+12 ポイント
36% が、セキュリティ チームがセキュリティ上の脅威に圧倒されていると回答	+16 ポイント

新しいアプローチを受け入れる姿勢

82% の中規模組織の意思決定者が、セキュリティに対する組織のアプローチを積極的に見直していると回答しています。中規模組織の意思決定者は、クラウドネイティブ ソリューションのメリットに対する信頼を強めており、**81%** が、クラウドネイティブ アプリは従来のデスクトップ アプリケーションよりも安全であると述べています。クラウド テクノロジーに対するこのような信頼は、中規模組織が変化の必要性を認識しているだけでなく、より革新的なソリューションを導入する準備ができていることを示しています。

82%

の中規模組織の意思決定者が、セキュリティに対するアプローチを積極的に見直している

> **「中規模組織の独自性は、市場拡大に向けて迅速に準備し、スケーリングを進めていることです。ここで基盤を固めなければ、大きく後れを取り、現在抱えている懸念が現実のものとなるでしょう。」**

— **Joshua Scarpino 博士**
Assessed.Intelligence CEO

5

セキュリティの問題への対処は世界の各地域でアプローチが異なる

世界中の意思決定者が、過去 1 年間で働き方が大きく変化したことを認識していますが、このような変化に対処するアプローチは、特にセキュリティ面において、国によって大きく異なります。

すべての地域の意思決定者が、職場環境が 1 年前から変化したと回答しており、あらゆる市場でセキュリティに対するアプローチの見直しが進んでいます。

「12 か月前と比べて、働き方が大きく / ある程度変化した」

インド	85%
ブラジル	74%
英国	73%
米国	62%

「組織がセキュリティに対するアプローチを見直している」

インド	83%
ブラジル	76%
英国	82%
米国	71%

インド

複雑さに圧倒されながらも、変化に貪欲

インドのセキュリティ環境は、その複雑さとツールの増加スピードが際立っています。そんな中でも、インドの組織はセキュリティの向上と新たな選択肢の模索に非常に積極的で、変化に対する強い欲求があります。インドは明らかな転換点を迎えており、意思決定者たちはより合理的、効果的なセキュリティ戦略の必要性を認識しています。

セキュリティの概要	世界平均との差
35: 使用するツール（プロダクト、サービス、アプリなど）の平均数	+11
19: 使用するセキュリティ ツールの平均数	+9
67%: 仕事の複雑さがセキュリティを低下させていると回答した割合	+10 ポイント

変化への欲求	
82%: 組織のセキュリティ改善が必要だと考えていると回答した割合	+8 ポイント
81%: コストに関係なく、新しいセキュリティ アプローチの採用に積極的であると回答した割合	+8 ポイント

ブラジル

懸念が強まる中でも、具体的な脅威にはそれほど注目していない

ブラジルの意思決定者は、セキュリティインシデントとその結果に関する懸念を強めています。しかし、セキュリティ上の問題の具体的な原因についてはあまり関心がなく、結果に対する不安はあるものの、インシデントの原因となる脆弱性は気にかけていません。ブラジルの組織は変化への欲求を表明しており、生成 AI の導入には 71% もの組織が関心を示しています（世界平均は 62%）。

セキュリティに対する不安	世界平均との差
41%: セキュリティ インシデントに関する心配が絶えないと回答した割合	+19 ポイント
42%: インシデントによる信頼の喪失を懸念していると回答した割合	+8 ポイント
37%: インシデントによる顧客の喪失を懸念していると回答した割合	+7 ポイント
39%: インシデントによるブランド ダメージを懸念していると回答した割合	+5 ポイント

具体的な問題に対する関心の低さ	
40% : 旧式のテクノロジーによって将来の備えが不十分になっていると回答した割合	-19 ポイント
48%: 生成 AI の利用がインシデントの増加につながったと回答した割合	-17 ポイント
44%: 仕事の複雑さがセキュリティを低下させていると回答した割合	-13 ポイント

英国

新しいテクノロジーに関する不安はあるものの、行動は鈍い

英国の意思決定者は、特にレガシー システムと生成 AI の脅威に関連して、新しいテクノロジーがセキュリティに及ぼす影響に深い懸念を抱いています。しかし、英国ではこれらのリスクを軽減するためのポリシーの導入が遅れており、意思決定者は極度の疲労を訴えています。こうした課題にもかかわらず、英国の組織は新しいセキュリティ アプローチの導入にあまり積極的ではなく、むしろセキュリティ侵害は避けられないと考える傾向にあります。

テクノロジーに関する不安	世界平均との差
75%: 旧式のテクノロジーによって将来の備えが不十分になっていると回答した割合	+16 ポイント
77%: 生成 AI の利用がインシデントの増加につながったと回答した割合	+12 ポイント

課題はあるものの、変化には消極的	
43%: セキュリティ チームがセキュリティの脅威に圧倒されている / 極度の疲労を感じていると回答した割合	+15 ポイント
44%: セキュリティ侵害を避けられないと回答した割合	+14 ポイント
27%: 生成 AI 固有のセキュリティ ポリシーを導入していると回答した割合	-14 ポイント
60%: コストに関係なく、新しいセキュリティ アプローチの採用に積極的であると回答した割合	-13 ポイント

米国

過剰な自信によって潜在的なリスクを見落とす可能性

米国の意思決定者は、セキュリティ ポスチャーに強い自信を持っており、特に生成 AI に関しては侵害を懸念している割合が低くなっています。この楽観的な姿勢自体に問題はありませんが、データ侵害で生じるコストは米国が世界で最も高いため、急速に拡大する脅威の状況を米国の組織が過小評価しているのではないかという疑問が生じています。新たなリスクに明確に焦点を当てなければ、過剰な自信により、将来の攻撃に対する組織の脆弱性が放置されてしまう可能性があります。

セキュリティの状況に関する自信	世界平均との差
10%: セキュリティ インシデントに関する心配が絶えないと回答した割合	-12 ポイント
55%: 生成 AI の利用がインシデントの増加につながったと回答した割合	-10 ポイント
52%: 自社のテクノロジー環境のセキュリティは以前と比べて低下していると回答した割合	-4 ポイント

データ侵害で生じるコストが最も高い	
936 万米ドル 2024 年にデータ侵害で生じたコストの平均額[1]	+ 500 万ドル

1.IBM - Cost of a Data Breach Report 2024

重要なポイント

「セキュリティ リスクを組織全体に理解させることが重要です。経営幹部がセキュリティの価値提案を理解していないことがよくあります。セキュリティ専門家は何がリスクで、何が解決策なのかをシンプルに説明できる必要があります。」

Joshua Scarpino 博士
Assessed.Intelligence CEO

❶ セキュリティ部門のリーダーとビジネス リーダーの連携が必要

セキュリティ戦略を成功させるには、セキュリティ意思決定者とシニア エグゼクティブ リーダーがオープンなコミュニケーションによって連携し、効果的なリスク管理プロセスを確立する必要があります。SDM が関係者からの賛同を得てより深い協力関係を築くことが、セキュリティが生産的に機能するか、組織内での対立を招くかの分かれ目になる可能性があります。

❷ 改革をするのに侵害の発生を待つべきではない

データ侵害などの危機は、必要なセキュリティ対策への承認をセキュリティ意思決定者が得るための大きなきっかけとなり得ます。しかし、ランサムウェアなどのサイバー攻撃は、ほぼすべての企業のオペレーションを一夜にして物理的に停止させる可能性があるため、必要な変更を今すぐ積極的に行うことの重要性が高まっています。ほとんどの企業にとって、侵害は発生するかどうかではなく、いつ発生するかの問題となっています。

❸ 攻撃の起点に注目する

Mandiant の最新の M-Trends レポートによると、2023 年に成功した侵入の 72% は、個人情報の侵害（フィッシングや認証情報の盗難など）またはソフトウェアの脆弱性の利用が発端になっていました。つまり、これらの領域を改善できさえすれば、組織に大きなメリットがもたらされる可能性があります。たとえば、フィッシング耐性のある 2 要素認証を提供する Google Workspace のようなプロダクトを使用することで、スパム、フィッシング、マルウェアの 99.9% 以上がユーザーに届かないように自動的にブロックされます。また、パッチ適用や更新が必要なデスクトップ クライアント アプリやオンプレミス ソリューションがなくなります。

「人々は『大きくて高額なプログラムやツールを購入しなければならない。数十万ドルのコストをかけなければ効果は出ない』と考えてしまいがちです。実際には、最も大きな変化は、会社の組織的なポリシーや文化に関連して生まれることがあります。」

Rachel Tobac 氏
SocialProof Security CEO

「AI はセキュリティ ツールに組み込まれ、インシデントや脅威への対応能力を強化します。AI の機能が非常に大きな影響力を持つことになるでしょう。AI には、まだ実現されていない可能性がまだまだ残されていると思います。」

John McCumber 氏
元 NIST 共同議長、元 Gartner ディレクター、現セキュリティ コラムニスト

4 変化は小さなステップで実現可能

従来のソフトウェア エコシステム全体をモダナイズするのは困難に思えるかもしれませんが、段階的なアプローチを採用することで、エンドユーザーへの影響を最小限に抑えながら、セキュリティを大幅に向上させることができます。たとえば、Chrome Enterprise を導入することで、フィッシングとマルウェアへの対策が組み込まれた安全なブラウジング エクスペリエンス、VPN を使用しないゼロトラスト アクセス、すでに広く愛用されているウェブブラウザを使用したデータ保護管理をユーザーに提供できます。

5 生成 AI はリスクにも防壁にもなり得る

データ損失のリスクを軽減するには、Gemini のような安全で、業界標準に準拠した生成 AI ツールを使用することが重要です。生成 AI は、新たな脅威から組織を保護するためにも活用できます。たとえば、Gmail の AI 防御機能では、スパムやフィッシング攻撃に対する防御を強化するために、すでに大規模言語モデル（LLM）が使用されています。実際に、LLM によって、Gmail でブロックされるスパムが 20% 増加し、1 日に評価できるユーザーから報告されたスパムの数が 1,000 倍に増加しました。このように、AI のおかげで、何十億もの Gmail ユーザーの生活の質が大幅に向上しています。

調査の目的

01
セキュリティの現状を理解する（独自の優先事項、考え方、懸念事項、課題）

02
特に生成 AI の台頭に関連して、セキュリティとテクノロジーが組織に与える影響を評価する

03
セキュリティの未来、新たなトレンド、組織の未来への投資について考察する

調査方法

定量的調査

2024 年 7 月 22 日から 8 月 8 日にかけて実施された、米国、英国、ブラジル、インドの 2,025 人の回答者を対象とする 20 分のオンライン調査。

以下の基準を満たす回答者を対象としました。

- 従業員数 300 人以上のさまざまな規模の組織で勤務
  - 組織レベルまたはチームレベルのテクノロジー プロダクトや生産性向上プロダクトを管理するビジネスまたは IT 部門の意思決定者、もしくは
  - 組織のセキュリティ プロダクトを管理するセキュリティ意思決定者
- 規制産業と非規制産業を含む幅広い業種

地域	(n=)
米国	501
英国	523
ブラジル	501
インド	500
組織の規模	
中規模（従業員数 300〜999 人）	834
エンタープライズ（従業員数 1,000 人以上）	1,191
役職	
IT 部門の意思決定者	673
ビジネスの意思決定者	762
セキュリティ意思決定者	590
合計	2,025

詳細インタビュー

2024 年 8 月 22 日から 26 日にかけて米国で 6 回実施された、1 時間の詳細なインタビュー。従業員数 300 人以上の組織の最高経営幹部またはそれに準ずる地位に就く人物（ITDM、BDM、SDM を含む）を対象としました。

専門家インタビュー

プロジェクトの重要なマイルストーンでは、知見、専門知識、ソート パートナーシップを提供する 3 人のセキュリティ専門家に話を聞きました（John McCumber 博士、Joshua Scarpino 氏、Rachel Tobac 氏）。

調査とデザイン: hypothesis