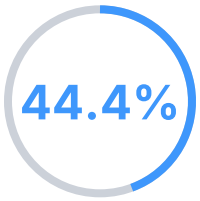
jamf

JAMF AIガバナンス調査：

IT・セキュリティ責任者687名が明かすAIガバナンスの最新事情

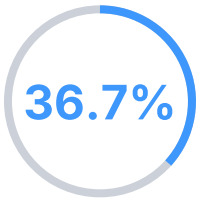
所見概要

Apple活用企業のIT・セキュリティ責任者687名を対象として、AI導入の規模、目標、セキュリティについて調査しました。結果は以下の通りです。



自動化

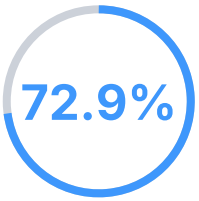
導入



ガバナンス

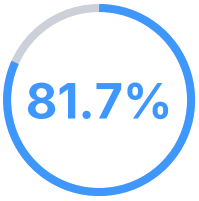
AI関連の優先事項トップ3は共通

調査では、**AI関連の最優先事項**としてIT業務の自動化（44.4%）、AI生産性支援ツールの導入（41.0%）、AIガバナンスの確立（36.7%）が挙げられました。



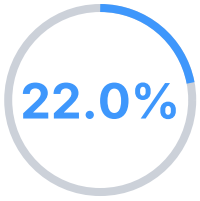
AI導入済みの企業の割合

対象企業の約4分の3が何らかの形でAIを導入していました。もはや導入するかどうかを議論する時期は過ぎ、ガバナンスが必須事項となっています。



AIリスクに直面している企業の割合

コストまたはセキュリティのインシデントを22.0%が経験し、59.7%は当面のリスクとみなしています。AIリスクは既に起きているか、必ず起きるものと予想されています。



コストまたはセキュリティのインシデントを経験した企業の割合

5分の1以上の企業がコストかセキュリティ、または両方のインシデントを経験しています。その影響は予算とセキュリティ部門へ同時に及んでいます。

インシデント発生率の増加量

AI関連のインシデントを経験した割合は、AIの試験段階の企業が19.4%であるのに対し業務に深く統合している企業では27.1%に上りました。リスク発生率は導入段階に反比例ではなく比例します。

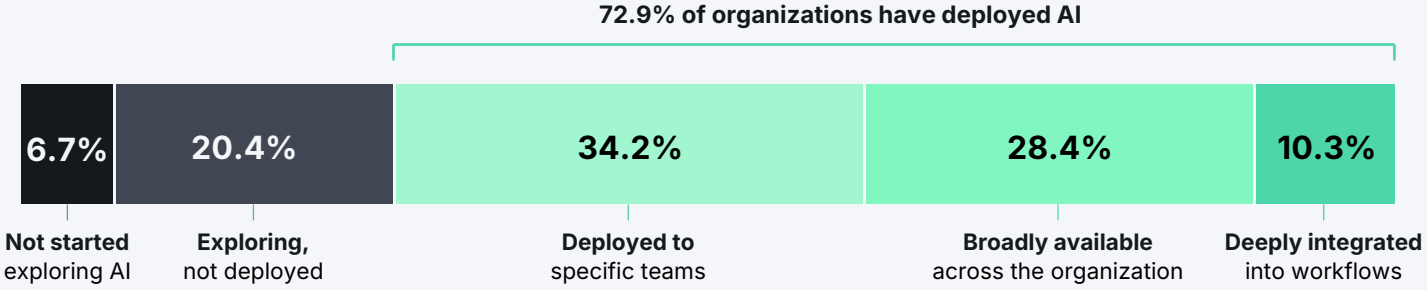
AIの活用を進めるほど、リスクが高まる。

多くの組織がAIの活用を推進していますが、それに合わせてリスクも増大します。シャドーAI、告知のないソフトウェア機能の組み込み、オンデバイスツールやエージェンティックツールの利用により、統治が難しく監査もしにくい盲点が生まれます。AI導入の深さとリスクの深さは比例します。今や、インシデントが起きるかどうかではなく、いつ起きるかが問題になっています。

チャート1

Appleユーザ企業のAI導入段階

ポイント：Apple製品を活用する企業の約4分の3が、チームレベルでの試験的利用から日常業務との緊密な統合まで、何らかの形でAIを導入しています。もはや、導入すべきかどうかを議論する時期ではありません。



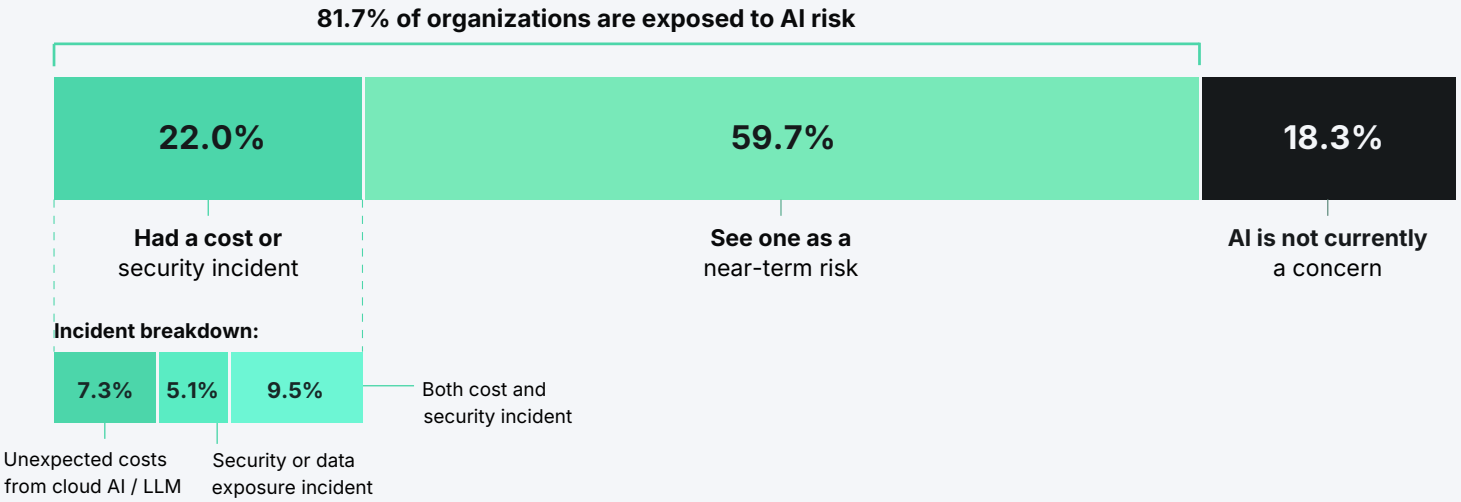
脚注：回答者 = IT・セキュリティ責任者687名。2026年第2四半期。

約4分の3の企業がAIを導入しているにもかかわらず、導入の規模を広げてもリスクは減少するどころか、むしろ悪化しています。回答者の22.0%がインシデントを経験しており、その内訳として7.3%がクラウドAI/LLMによる想定外のコスト、5.1%がセキュリティ事象またはデータ漏洩、9.5%が両インシデントに遭遇しています。まだインシデントを経験していない企業も、59.7%が将来的に発生すると予測しています。

チャート2

過去12ヶ月に発生したAI関連のインシデントおよび問題

ポイント：22.0%の企業がAI関連のインシデントを経験しており、59.7%はいずれ経験すると予測しています。調査時点でAIが問題になっていなかった回答者の割合は18.3%に過ぎません。



脚注：回答者 = 681名。パターンは両調査サンプルで独立して見られた。

しかし、データから直感に反する所見が判明しました。インシデントの発生率が一番高いのは、AI成熟度の最も高い企業だったのです。

チャート3

AIの活用レベルに見るインシデント発生の割合

ポイント: AI活用レベルが深い組織ほど、インシデントの発生率が高くなる傾向に。インシデントを経験した割合は、試験段階の企業では19.4%であるのに対し、成熟度が最も高い企業では27.1%に及んでいました。

脚注: 回答者 = IT・セキュリティ責任者683名。2026年第2四半期。

企業がAIの試験導入の段階を過ぎると、インシデント発生率が増加していました。インシデントを報告した企業の割合は、試験段階の企業（19.4%）に比べてAIを緊密に統合している企業（27.1%）の方が40%高くなっています。

⚠ AIの課題には共通の傾向が見られる

インシデント対策について自由回答形式で尋ねたところ、回答は4つの傾向に集中しました。

シャドーAI

生産性の向上、AIツールの流行、さらに会社全体でのAI活用の推進の結果、従業員は日常的にAIを利用するようになっています。多くの場合、IT部門に承認を求めることなく個人用アカウントを作成しており、機密データを入力するケースも見られます。そのため、IT部門はどのAIシステムが使用されているのか把握できず、AIプラットフォームの制御あるいは禁止も困難になっています。こうして可視性が失われた状態では、セキュリティおよびガバナンスは不可能ではないにしろ、容易なことではありません。

ベンダースプロール

今や新しいAIベースソフトウェアが次々に発表されていた時期は過ぎ、多くのアプリで既存製品にAIが組み込まれるようになっています。IT部門でAIツールの候補を審査して導入するには時間も手間もかかり、特にAIの発展に追従しようとするとさらにハードルが上がります。本調査では、どのAIプラットフォームが自社の従業員に最適かを判断し、認可したAIツールを社内で使用させるのが困難であるという声が寄せられました。導入の入口が増えた結果、AIの保護が難しくなっているのです。

エージェンティック/デベロッパーAI

セキュアな導入と可視化、AI機能、ユーザ教育などの重要な領域において、エージェンティックAIとデベロッパーAIに関連する課題が生じています。調査では、エージェンティックAIの導入管理について、ユーザ支援とデータ保護の両立が問題になっているという意見が見られました。また、コマンドラインツールやサードパーティ製パッケージ、IDE拡張機能、組み込みLLMなどの可視化も共通の問題となっていました。エージェンティックAIに適切な権限を付与している場合でも、コードベースに危険なコードや問題のあるコードを追加したり、必要なコードを削除したりすると、深刻なリスクが生じます。開発関連の問題は、開発者ではないユーザにも及びます。こうしたユーザは、適切な審査や品質検査を行うことなく独自のアプリを作成するからです。

想定外のコスト

IT部門は、コスト、自社の取り組み、セキュリティのバランス調整に追われています。クラウドAIやLLM APIで採用されている従量課金制は費用の予測が難しく、開発部門が新しいツールを次々に導入する結果、有料ライセンスの重複が進んでいます。実際に使用されているツールを可視化する手段がないため、IT部門はどのツールを整理すべきかの判断を手探りで進めるしかありません。

ガバナンスと生産性は表裏一体。

AI導入企業では、AIの活用が深く浸透するほどインシデント率が増加している。

回答者共通の課題は、可視性・導入・ベンダースプロール・コスト。

上記の所見をまとめると、1つの現実が浮かび上がります。**AIの導入が急すぎて、ガバナンスが追いついていない**のです。

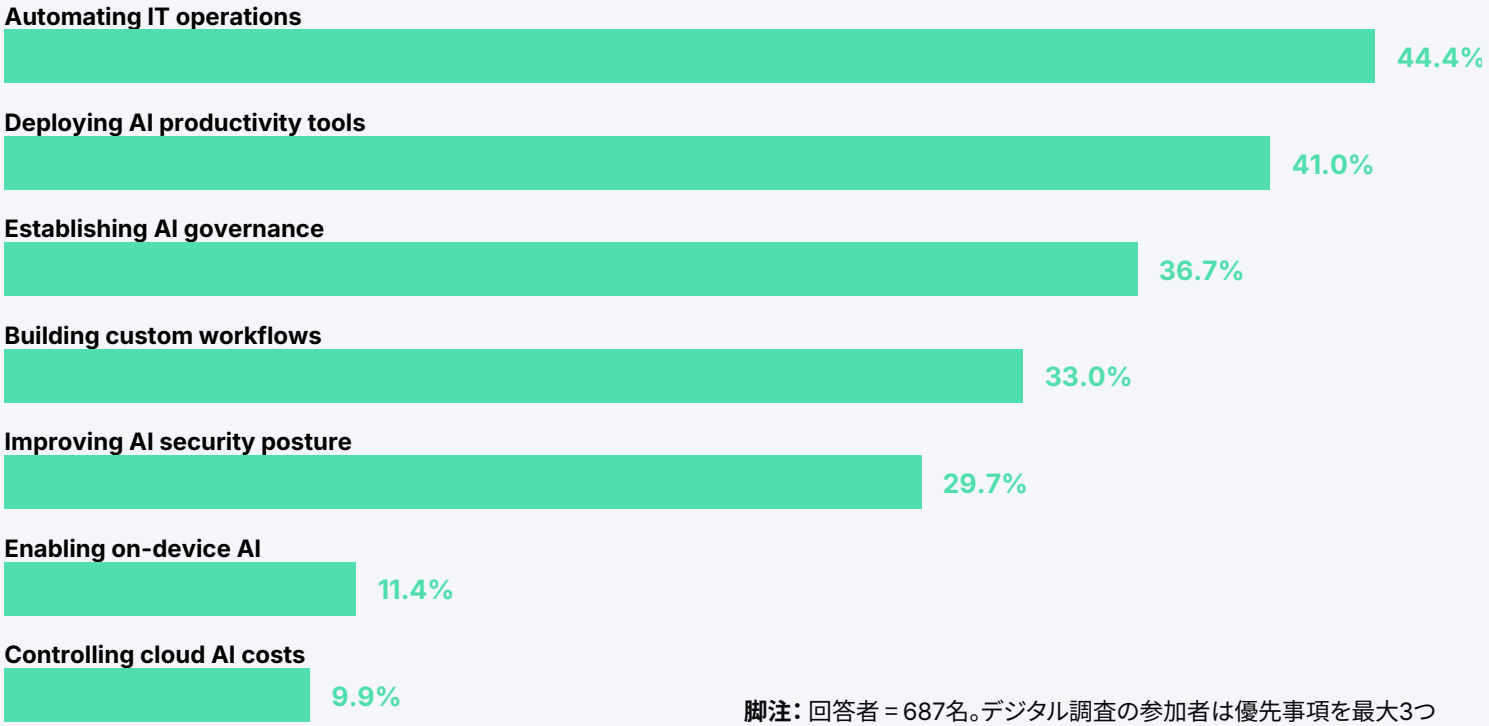
この事実を表しているのが、シャドーAI、社内データやシステムへのアクセス点の露出、余剰な（しかも高額な）プラットフォームの導入、IT部門が把握できず測定しにくいリスクの発生といった現状です。

そのため、IT部門には、AIによりあらゆる人の働き方が変わっている現実を踏まえて優先事項を見直すことが求められています。

チャート4

今後12ヶ月間での対応を予定しているAI関連の優先事項

ポイント：IT業務の自動化、生産性支援ツールの展開、ガバナンスの確立の優先度は回答者間でほぼ同じです。ガバナンスは支援の後ではなく、同時に進めるべきものです。



脚注：回答者＝687名。デジタル調査の参加者は優先事項を最大3つ選択し、対面調査の参加者は1つを選択。詳細は「調査手法」を参照。

ガバナンスと支援は真逆のプロセスと考える方もいるでしょう。導入するAIツールの数が増えるほど、ガバナンスは困難になります。IT部門は相反する優先事項のバランス調整を常に強いられており、AIも例外ではありません。問題はAIの導入速度であり、AI機能とリスクは新たな領域へと突入しているのです。

そのため、回答者は前述の優先事項を同時に進めています。急ぎすぎればインシデントの発生率が高まり、慎重すぎれば従業員が抜け道を見つけ、セキュリティが損なわれてしまいます。

実際の意見：業界で生じているAIの課題

本調査では178件の自由回答をまとめ、上記所見の背景を示す詳細な情報を得ました。
以下に、そのうち8件を示します*。

ユーザからアクセスを求められるようになり、導入を先送りしてきたセキュリティ部門に圧力が生じています。しかし、根本の問題は未解決のままです。**完全に管理しようとすれば生産性が損なわれ、管理を緩めれば重大なコンプライアンスのリスクが生じます。**

どのベンダーも、ユーザの要望にかかわらずAIを組み込んでいます。一括での無効化は時間稼ぎにはなりますが、いつか破綻します。さらなる懸念として、クラウドでデータがどのように処理されるのか、データの行き先をユーザが管理できるのかという点も問題です。

既知のAIサイトのブロックは難しくありません。しかし、CLIツール、IDE拡張機能、ブラウザ拡張機能、GitHubで提供されているパッケージは**大部分が不透明**であり、1つの経路を塞いでもユーザは別の経路を見つけます。

規制産業や一部管轄区では、あらゆるものの導入前に所定のコンプライアンスフレームワークを実装する必要があります。しかし、現時点で**これらのツールやフレームワークは要件を満たしていません。**

シャドーAIとブラックボックスのスクリプト実行がリスクのトップです。次いで、非技術者のユーザがバイブコーディングで独自アプリを作成した結果、中身をよく理解せず、データの露出に気づかず放置してしまうことが挙げられます。

AI利用者の希望とライセンスの購入意思にずれがあります。導入を早急に進めた部門ではエージェントの重複が生じた結果、**コストが増大しており、どのツールを維持する価値があるか決める明確なフレームワークもありません。**

開発環境や本番環境へのアクセスをAIエージェントに付与することには同意できません。エージェントが指示とはまったく異なる作業をして、データが消えたと報告するのではないかという不安があります。**適切に管理しながらエージェンティック機能を導入する方法はいまだに見つかっていません。**

ハルシネーションによる出力が事実として扱われると同時に、AIが日常業務に深く組み込まれていくことで、**リテラシーが間に合わずリスクが急速に増大しています。**

* 上記回答は、178件の自由回答に見られたパターンを基にJamfが作成したものです。各回答は実際の回答の詳細ではなく、繰り返し見られた話題を抜粋しています。

対応策：ガバナンスの4原則

1.

可視性を高める

多くの回答者が述べているように、可視化はなによりも重要です。見えないものを統治することはできません。しかし、当然ながら困難も伴います。インストール済みアプリの監査やトラフィック監視を頻繁に行うと、AIプラットフォームとのやり取りを特定しやすくなります。ユーザはローカルAIプラットフォームを利用するものであり、また承認済みの非AIアプリケーションでも機能セットにAIが追加されることがあるので、AI実行時検出の結果はより詳しく調査する必要があります。

2.

ガバナンスの対象はユーザではなくツール

多くのIT部門にとって、組織のAIポリシーはITを考慮することなく唐突に作成されるものです。さらにこうしたポリシーでは、できる限り速やかなAIの活用拡大が推奨されます。ユーザ向けガイダンスが提供されていたとしても、強制力はありません。その結果、シャドーAIが発生します。

そうではなく、組織のリスク許容度およびセキュリティガイドラインに基づいてガバナンスの方針を決定し、その内容をAIツールのデータ共有設定（アクセス可能なデータ、データの処理方法、AIが変更可能な対象）に反映すべきです。シャドーAIが起きるとユーザの透明性が損なわれますが、トラフィック、データ、API呼び出しは把握できます。見えるものだけを統治しましょう。

3.

ガバナンスを環境に組み込む

AIの導入を急ぎすぎた企業では、インシデント発生率が高まっていました。重要なのは順序です。ガバナンスはアプリ導入への対策としてではなく、同時に行う必要があります。口で言うほど簡単でないのは事実であり、未処理の仕事が溜まっている方もいるでしょう。しかし、どのツールが使用されているかを特定してユーザに提供し、アクセスポリシーを策定すれば、AIツールの利用を安全に拡大しやすくなります。

4.

既存システムへの「後付け」ではなく、Apple専用ツールを活用する

ネットワークベースのツールでは、トラフィックを通じ、どのクラウドAIサービスがいつ、どれくらい使用されているかを把握できます。この情報は役に立ちますが、対象はネットワーク上にとどまります。AI本体がクラウド上で実行されている場合でも、アクセスが行われるのはデバイス上です。どのツールがインストールされ、どのプロセスが発生し、どのファイルにアクセスされたかという情報は、DNSログでは確認できません。Appleネイティブのツールであれば、ツールやプロセス、ファイルアクセスを確認し、アクセス許可を管理して、このギャップを埋められます。

支援対象を統治し、統治対象を支援する

AI導入のスピードは、大半のガバナンスフレームワークの想定を超えています。しかし、現時点で生じている課題に、導入方法を縛られる必要はありません。ユーザの要望に応じてAIツールを提供するか、各ツールの利用方法を厳格化するかの二者択一にする必要もありません。

成功の鍵は、導入を急ぐことでも、管理を厳格化することでもないからです。成功する企業は、ガバナンスと支援を同じプロジェクトとして扱い、導入当初からAI環境を可視化し、アクセスを制御しています。Apple活用企業がこれを実現するには、管理対象の実行環境を把握するツールが必要です。クラウドのトラフィック、オンデバイスモデル、エージェントプロセスは発するシグナルがそれぞれ異なり、Apple専用の監視ツールでなければ大部分を補足できません。ガバナンスをどれだけ強固にできるかは、ツールの可視化性能にかかっています。

AIの導入を遅らせることはできませんが、統治することはできます。対応はそこから始めましょう。

調査手法

データ収集は2つのフェーズに分けて実施されました。第1フェーズは2026年3月から4月にかけて、Jamfカスタマーコミュニティに対して実施されました（回答者数：338名）。第2フェーズは、北米の6都市で開催されたイベント「Jamf Nation Live」の会場にて対面によるアンケート調査として実施されました（回答者数：349名）。これらを統合し、687名のIT・セキュリティ責任者から回答を得ました。すべての回答者は、Jamfを導入している組織でAppleデバイスの一括管理・保護を担当しています。

優先事項に関する質問では、質問時点から12ヶ月間におけるAI関連の優先事項を選択するよう依頼しました。選択可能な優先事項の数は、3月～4月の調査では最大3つ、Jamf Nation Liveにおける調査では1つとしました。本質問の結果における割合は、回答者全687名のうち、各優先事項を最優先事項として選択した回答者の割合に相当します。透明性確保のため、両調査における選択に関する規定をここに示します。

統計的検定により2つのフェーズで母集団に重複がなく、AI成熟度の平均はJamf Nation Liveの回答者の方が低いことを確認しました。傾向に関する所見は、どちらのサンプルでも独立的に維持されていました。回答者のデータは、回答がどの回答者または組織のものであるか判別できないよう、すべて匿名扱いで収集および分析されました。回答者に参加報酬は提供されていません。