CYBERARK®
THE IDENTITY SECURITY COMPANY®

Report

アイデンティティセキュリティの展望 ~ 2025年版 ~

セキュリティリーダーによるリスクと準備に関する見解

A Security Matters Research Report by CyberArk

目次

総論

総論

2025年版のアイデンティティセキュリティ展望へようこそ！この調査は、世界20カ国2,600人のセキュリティ意思決定者からの惜しみない洞察なしには実現できませんでした。ご協力いただいた皆様に心より感謝申し上げます。

このレポートでは、現代のITエコシステム全体にわたるアイデンティティに影響を与えるサイバー攻撃の傾向を具体的に分析し、セキュリティ専門家がどのように備えるべきかについての洞察を共有しています。

リピーターの読者の皆様は、AIがセキュリティ対策において攻撃者と防御者の双方を強力に支援していることをよくご存知でしょう。しかし、今年さらに興味深いのは、AI導入競争の激化により、マシンアイデンティティの急増によって意図せずして攻撃対象領域が拡大している点です。AIの第三の次元へようこそ。攻撃者はAIを利用して新たな脅威を生み出し、防御者はAIを利用して脅威から身を守ります。そして、企業は企業全体にエージェントAIを組み込むことで、新たなアイデンティティ中心のリスクに直面することになります。

一方で、現代において最も執拗かつ高度なサイバー攻撃が横行しており、10社中9社がアイデンティティ中心の侵害を報告しています。半数以上（51%）がフィッシング攻撃やビッシング攻撃の被害に複数回遭っています。同時に、AIの導入が認可の有無を問わずサイバーセキュリティリスクを増大させているとの回答も寄せられています。従業員の72%が業務でAIツールを日常的に使用しているという報告が組織から寄せられていますが、68%の組織では依然としてこれらのテクノロジーに対するアイデンティティセキュリティ対策が不十分です。現在、マシンアイデンティティは人間のアイデンティティを80倍以上上回っています。これを「前例のない」と呼ぶ人もいるかもしれませんが、私たちは「先駆者」という言葉を好んで使います。

もはや
マシンアイデンティティの数は
人のアイデンティティの
80 倍以上ともなっています

地政学的な見通しもそれほど明るくはありません。昨年、選挙サイバー干渉脅威調査報告書は、国家支援型の攻撃者が米国とその同盟国に対する妨害活動においてAIの利用を強化するだろうと警告しました。国家はこれらの攻撃を支援するだけでなく、サイバー犯罪組織と連携してサイバースパイ活動や偽情報の拡散を強化しています。彼らは企業、重要インフラ、さらには金融業界にまで攻撃を仕掛けており、最近ではByBitから15億ドル相当の仮想通貨が盗まれた事件もその例です。12月には、米国が中国政府のハッカーが財務省へのリモートアクセスを取得したことを確認しました。これは「大規模なサイバーセキュリティインシデント」と表現されています。

Executive Overview

AIは世界中の人々の想像力を掻き立てています。しかし、哲学者ポール・ヴィリリオがかつて言ったように、「船を発明すれば、難破船も発明する」のです。保護できるAIは、攻撃にも使えます。脆弱性を検知し、それを悪用するのです。

AI導入競争の中で、組織は意図せずして、管理もセキュリティ保護もされていないマシンIDを急増させています。過負荷のチームは、それらを管理するための可視性を持っていません。AIエージェントの特権アクセスは、既存のセキュリティモデルでは対応できない、全く新しい脅威ベクトルを表しています。この「過剰達成」のアイデンティティ脅威の状況において、レジリエンスを維持するためには、誰かが舵を取るのを待つことはできません。私たちは、アイデンティティリスク戦略を自ら主導し、適応、対応、そして回復できるようにアプローチを近代化する必要があります。

もしあなたがすでにシートベルトを締めているなら、今度は噛み付いてみましょう。なんいう時代を私たちは生きているのでしょう。

今年のレポートの内容は次のとおりです。

1. AIがアイデンティティ中心の脅威の三重奏となる可能性
2. 機械アイデンティティの衝撃的な急増、安全でない特権アクセスを持つ人間のアイデンティティの範囲、そして企業に突きつけられる特有の課題
3. アイデンティティサイロの出現と、それがビジネスのレジリエンスをいかに損なうか

機密性の高いデータを侵害や漏洩から保護することは、信頼と運用のレジリエンス（回復力）を維持するために不可欠です。いつものように、データを詳しく分析し、何が進化しているかを明らかにし、組織が正しいサイバーセキュリティの歴史を築くために今すぐ実行できるステップを共有します。

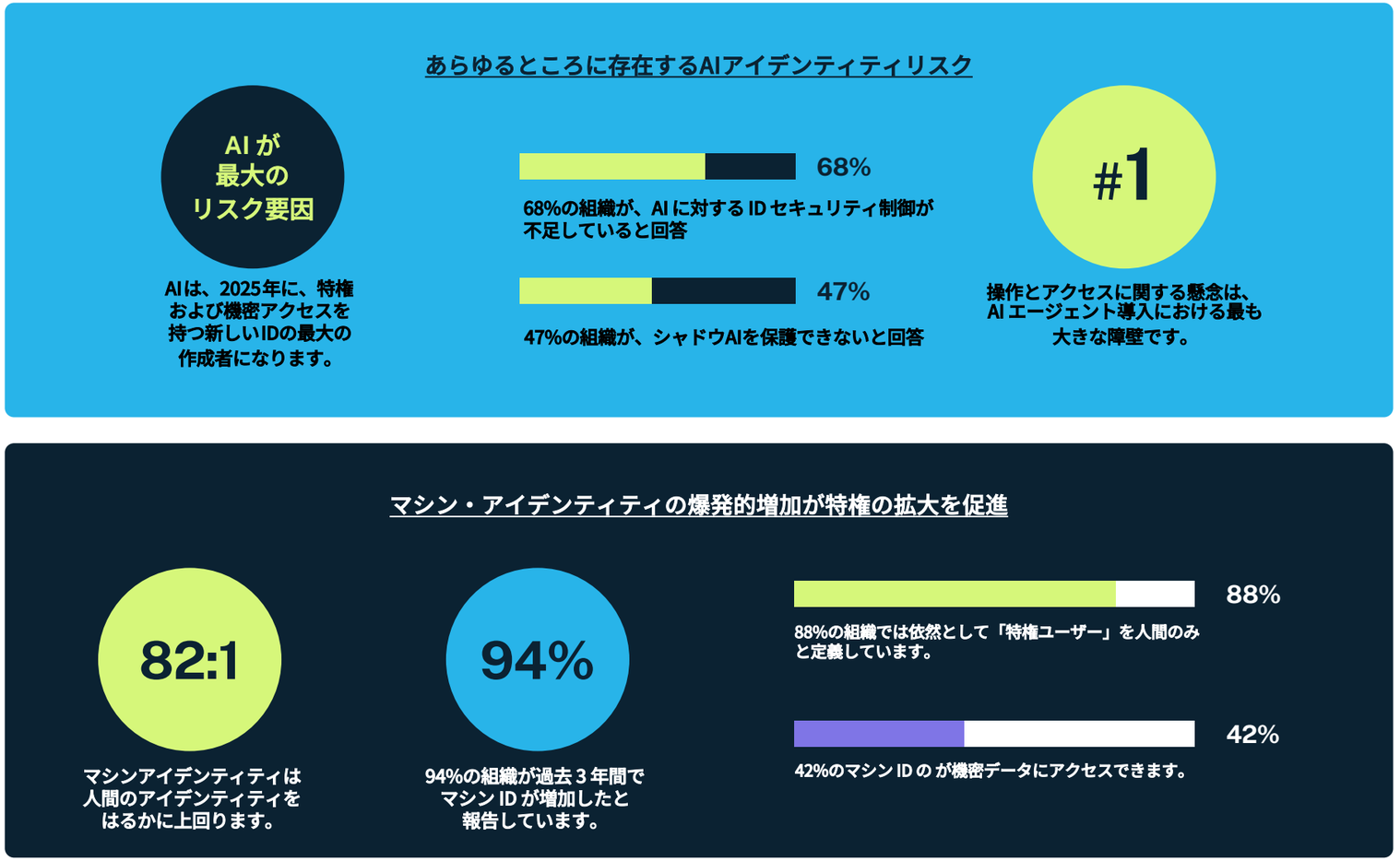
Clarence Hinton
Chief Strategy Officer, CyberArk

Clarence Hinton
Chief Strategy Officer

AIは世界中の人々の想像力を捉えています。しかし、哲学者ポール・ヴィリリオがかつて言ったように、「船を発明するということは、難破船も発明するということ」なのです。

Executive Overview

概要



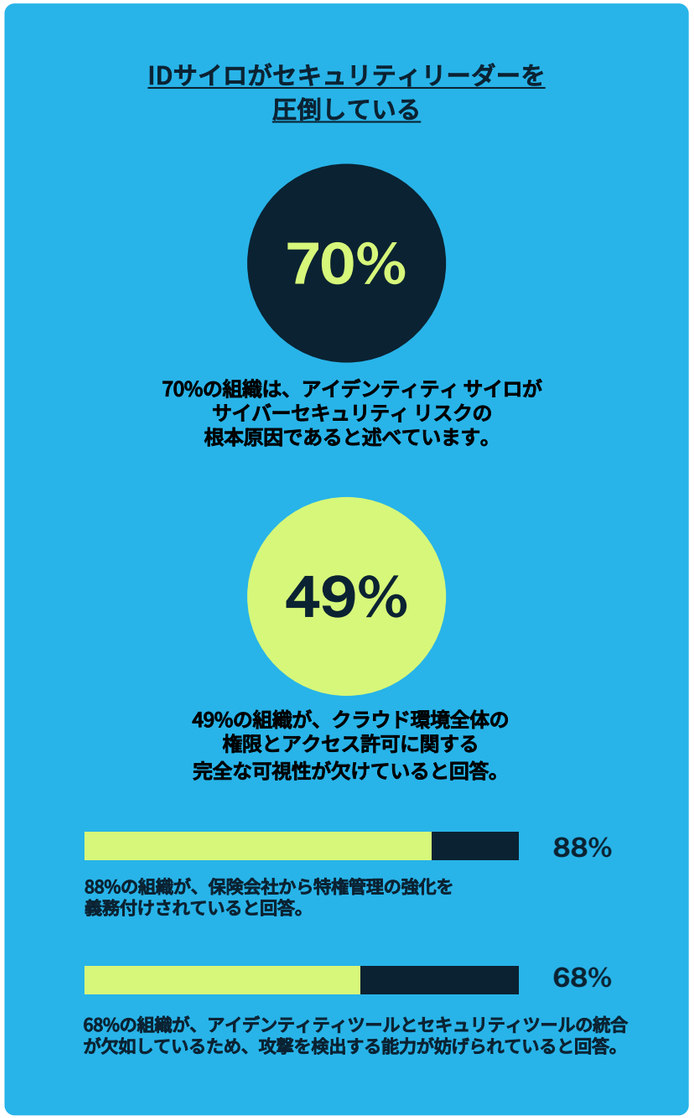


図 1. AI、マシン ID、サイロが ID リスクに与える影響を強調する主な傾向 (n=2,600)

AIの三要素:

攻撃者、防御者、アイデンティティリスク

CYBERARK®

AIの三要素：攻撃者、防御者、そしてアイデンティティリスク

2025年には、AIが人間を手作業や反復的なプロセスから解放していない場所を見つけるのは難しいでしょう。AIは現在、私たちの電力網を制御し、農作物を監視し、交通を誘導し、サイバーセキュリティを強化しています。当社の調査によると、回答者の94%（図2）がAIとLLMプロセスを活用して、全体的なアイデンティティセキュリティ戦略を強化しています。図3は、回答者の61%が今後12ヶ月以内に人間とマシンの両方のアイデンティティを保護するためにAIの活用を検討していることを示しています。残念ながら、攻撃者はAIを活用して攻撃をより迅速かつ巧妙にし、阻止を困難にすることで、既に優位に立っています。

さらに、当社のレポートでは、2025年にはAIとLLMが、特権アクセスと機密アクセスを持つ最も多くの新しいアイデンティティの作成を促進すると予想されていることがわかっています。これは、組織が導入するAIシステム、そしてそれらのシステムが作成する新しいアイデンティティを保護しなければならないことを意味します。本質的に、私たちはAIをシステムに侵入する武器として、そしてシステムを保護する防御者として管理する必要があるのです。そして今、AI自体もシステムとしてセキュリティを確保する必要があります。

今年のレポートでは、AIのこれら3つの側面がセキュリティチームにどのようなプレッシャーを与えているかを詳しく見ていきます。

使いにくく、エラーだらけのスパム、そして私たちが恋しいもの

過去12ヶ月間、フィッシングは依然として個人情報漏洩の主な原因となっています。変化したのは、AIを活用したこれらの攻撃の規模、巧妙さ、そして成功率です。

攻撃者は、高度にパーソナライズされ、コンテキストを認識し、正規の送信者とほぼ区別がつかないような、AIが生成したフィッシングメールを送信できます。AIは公開データを分析し、トーンやフォーマットを模倣し、メッセージをリアルタイムで調整できるため、セキュリティに精通したユーザーでさえも容易に騙すことができます。さらに、AIはメール、チャット、音声チャネルを介したアウトリーチを自動化・調整できるため、ソーシャルエンジニアリングキャンペーンはかつてないほど説得力のあるものになっています。

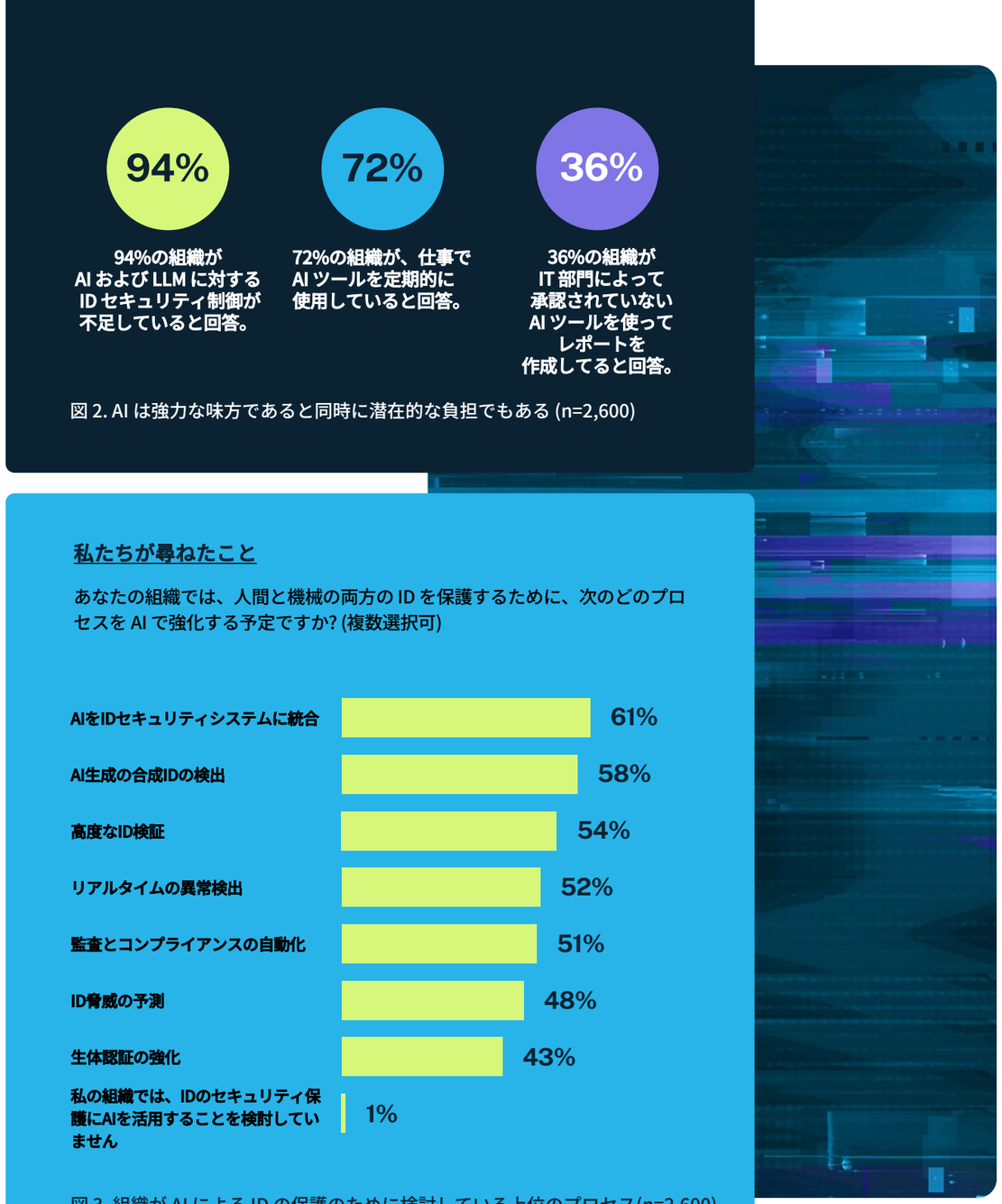


図 2. AI は強力な味方であると同時に潜在的な負担でもある (n=2,600)

図 3. 組織が AI による ID の保護のために検討している上位のプロセス(n=2,600)

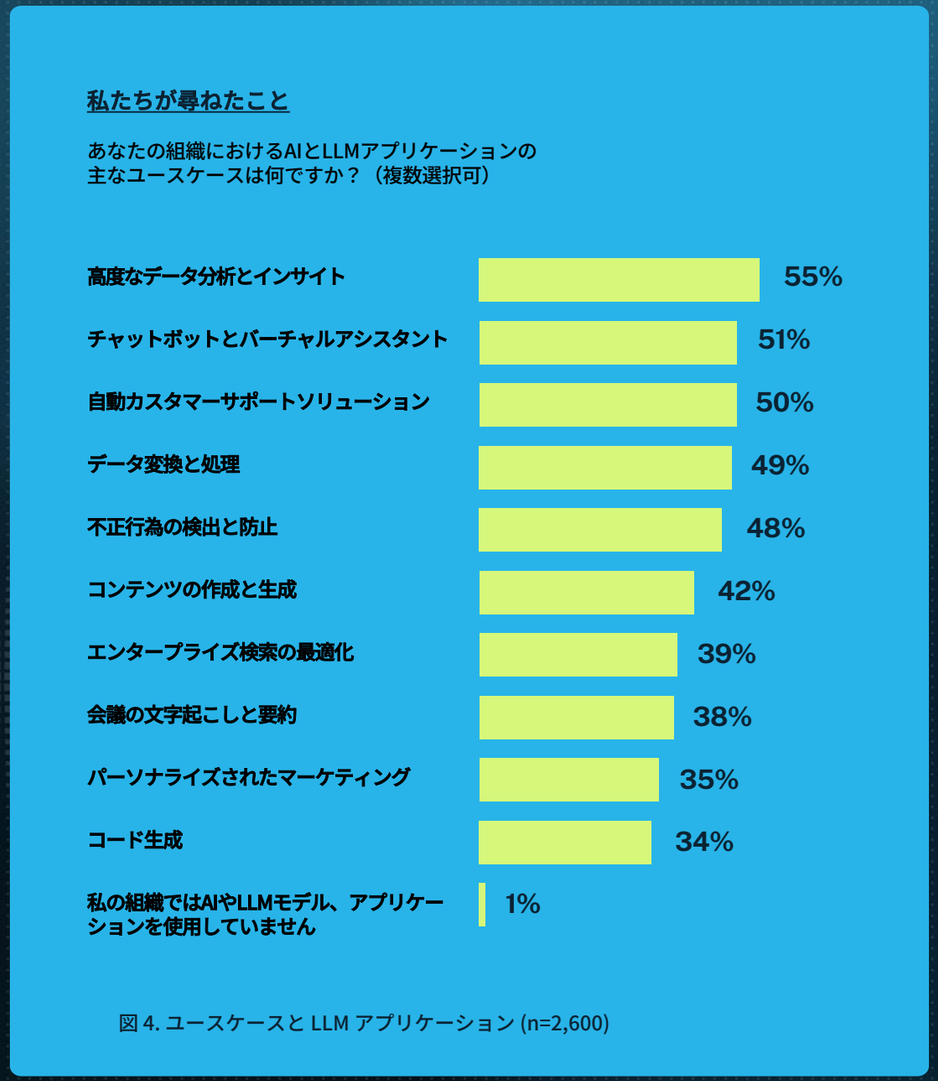


図 4. ユースケースと LLM アプリケーション (n=2,600)

AIの三要素：攻撃者、防御者、そしてアイデンティティリスク

AIが生成したフィッシングは、認証情報の収集、権限の昇格、脆弱なアプリケーションの悪用、特権アクセスの侵害、認証情報ベースの攻撃を迅速に実行しようとする攻撃者にとって、非常に効果的な侵入口となります。10社中9社が、この種の侵害を　　経験したと報告しています。回答者の4分の3以上が、組織内でフィッシング攻撃（AIを活用したディープフェイク詐欺を含む）の被害に遭ったと報告しており、そのうち半数以上が複数回の被害に遭っています。

一例として、2月には、ジョルジオ・アルマーニ氏を含む著名なイタリアの実業家を狙った詐欺事件が発生しました。AIを用いて、イタリア国防大臣グイド・クロゼット氏の声を模倣したのです。詐欺師たちは、誘拐されたジャーナリストの救出を装って資金援助を要求し、少なくとも1人の被害者が香港の銀行口座に100万ユーロを送金しました。

アイデンティティセキュリティの新たな鍵

セキュリティチームにとって、AIは対応時間を数時間から数秒へと短縮できます。煩雑な人間の介入を必要としないため、過去の攻撃パターンを絶えず分析し、次の攻撃を予測し、脆弱性を優先順位付けし、脅威を自動的に遮断することができます。セキュリティオペレーションセンター（SOC）は、AIを活用して膨大なID関連の脅威データをリアルタイムでふるいにかけることができます。これは、人間のアナリストに代わるものではなく、アナリストの能力を補完するものです。

AIはまた、時間のかかる反復的なタスクを処理し、有用な洞察を引き出すため、セキュリティチームはより大きな脅威に集中し、よりスマートで戦略的な意思決定を行うことができます。セキュリティオーケストレーション、自動化、および対応（SOAR）システムと組み合わせることで、人間とAIの連携により、インシデント対応をより効率的かつ適応的に行うことができます。図4では、55%の組織が高度な分析と異常検知にAIを使用していると回答しています。回答者は、2025年にID関連の脅威を軽減する上で最も効果的なツールの一つとしてAIを挙げています。

AI は時間のかかる反復的なタスクを処理し、有用な洞察を明らかにするため、セキュリティ チームはより大きな脅威に集中し、よりスマートで戦略的な意思決定を行うことができます。

新しい相棒/スーパーヴィランに会いましょう

しかし、AI主導のサイバーセキュリティが最前線の防御戦略となるにつれ、AIシステム（マシンIDを含む）のセキュリティ確保は、同様に重要になります。AIは膨大な量のデータに依存するため、侵害、悪用、不正アクセスのリスクが高まります。図5は、AIモデルの使用によって機密データへのアクセスが可能になり、サイバーリスクが生じることを認識している組織が82%あることを示しています。

AIモデルは、悪意のある者の手に渡ると、データベースクエリの実行、外部API呼び出しの実行、さらにはネットワークに接続されたマシンへのアクセスにまで操作される可能性があります。調査によると、攻撃者は様々なモデルにおいてほぼ100%の成功率で「ジェイルブレイク」（LLMを操作してユーザーの個人情報（名前、ID、メールアドレス、支払い情報など）を秘密裏に抽出・送信する）を行う新たな方法を発見しています。

AIモデルのジェイルブレイクは単なる理論的な演習ではありません。組織がAIの影響を十分に理解しないままAIの導入を急ぐ中で、セキュリティ上の懸念が高まっています。ちなみに、サイバーアークの新しいFuzzyAIツールが話題になっているのは、まさにこのためです。テストしたすべてのモデルをジェイルブレイクすることに成功しています。オープンソースプロジェクトとしてGitHubで公開されているこのツールは、組織や研究者が攻撃者に悪用される前にAIのセキュリティギャップを体系的に特定し、修正するのに役立ちます。

シャドーAI：誰も承認していないけど、みんな使っている

企業はAIツールのホスティングに複数のアプローチを採用しており、OpenAI、Google、Amazon Bedrock、Meta AIなどの世界有数のLLM AIモデルを採用することが多く、公開されているトレーニングデータセットと独自の企業データを組み合わせてAIをトレーニングし、問題解決を支援しています。64%の回答者が、組織のAIツールはすべてIT部門によって承認・管理されていると回答していますが、知識ギャップも存在します。ほぼ半数（47%）が、組織では使用されている「シャドーAI」ツールのすべてを保護・管理できていないと回答しています（図5）。

82%

82%の組織が、AI モデルの使用により機密情報へのアクセスリスクが生じると回答。

68%

68%の組織が、AI および LLM に対する ID セキュリティ制御が実施されていないと回答。

47%

47%の組織が、組織内でのシャドーAIの利用を安全に保護できないと報告しています。

図 5. AI の導入がセキュリティ管理を上回っています (n=2,600)

AIの三要素：攻撃者、防御者、そしてアイデンティティリスク

多くの企業では、AIの活用がIT部門やセキュリティ部門の管轄範囲外になっています。シャドーAI、つまり従業員や部門が正式な承認を得ずにAIアプリケーション、モデル、またはAI搭載機能を使用するケースが増加しています。当社のレポートによると、回答者の36%がIT部門による完全な承認や管理を受けていないAIツールを使用していることが、シャドーAIのリスクにつながっていると報告しています。

シャドーITとは異なり、シャドーAIの検出はさらに困難です。AI機能は承認されたソフトウェアに目に見えない形で組み込まれていることが多いため、組織はどのAIツールが企業データを処理しているのかを把握できない可能性があります。これは大きな問題です。例えば、従業員が誤ってAIサービスに独自のデータや個人データを送信した場合、そのデータは社外で保存または記録される可能性があります。また、財務チームがAIプロンプトにAPIキーや機密レコードを入力させることで、知らず知らずのうちに公開してしまう可能性があり、AIプロバイダーによってログに記録されてしまう可能性があります。

AIの入力、意思決定、トレーニングデータを保護するための適切な管理体制がなければ、攻撃者はインジェクション攻撃、モデルポイズニング、あるいはAIの挙動にバイアスをかけるための様々な攻撃を用いて、これらのプロセスのいずれかを破壊してしまう可能性があります。

このリスクをさらに悪化させているのは、AIモデルが展開される環境の多様性です（図6）。AIの導入が拡大し、監視が薄れていくにつれて、組織はセキュリティを確保できる範囲を超えてイノベーションを進める可能性があります。オンプレミスであれクラウドであれ、企業はAIのトレーニング、展開、運用化をどのようにセキュリティで保護するかを決定する必要があります。ポリシーと監視がなければ、シャドーAIはセキュリティと規制上の負担を増大させ、企業をコンプライアンス違反、データ漏洩、その他様々な問題にさらすことになります。

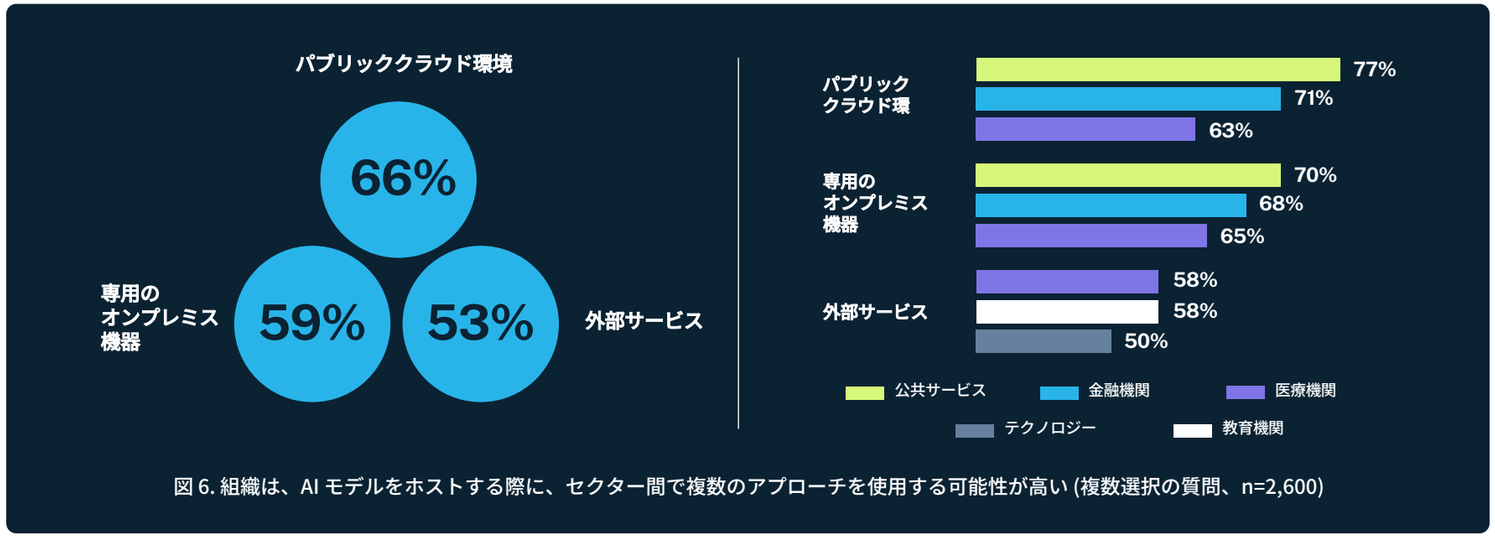
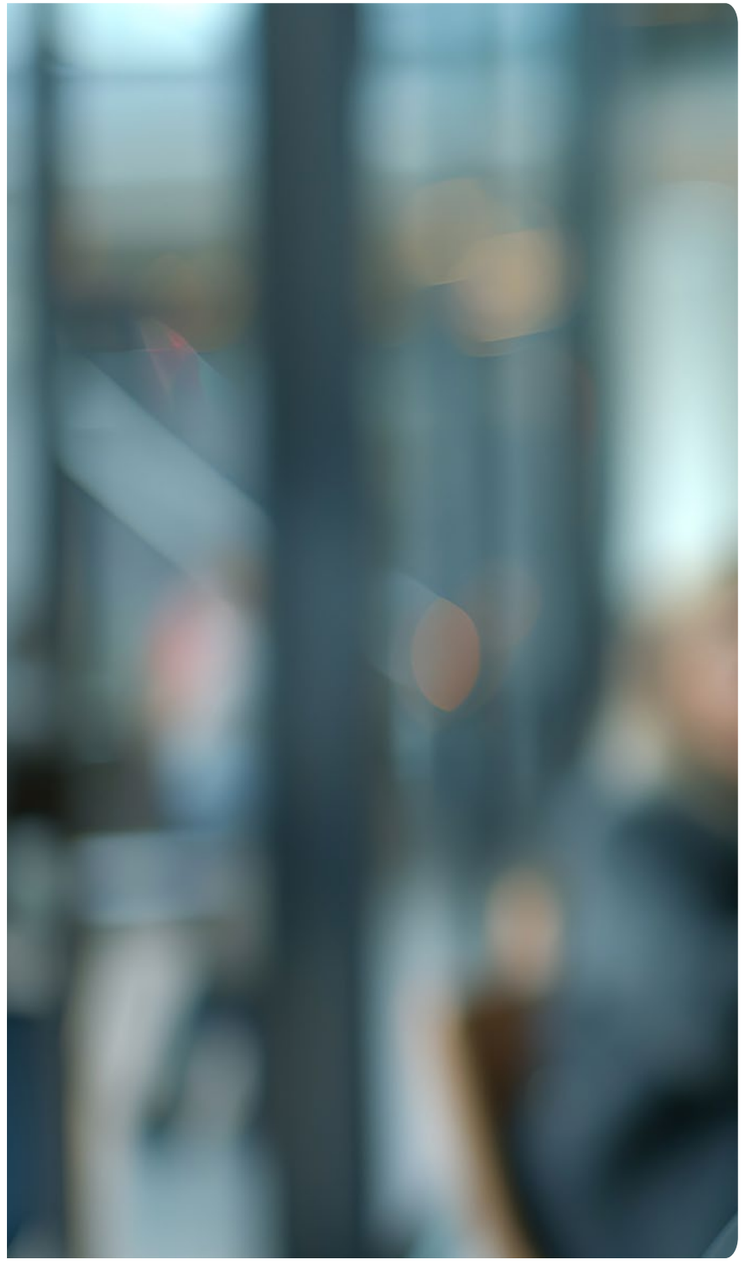


図 6. 組織は、AI モデルをホストする際に、セクター間で複数のアプローチを使用する可能性が高い (複数選択の質問、n=2,600)



未来からの衝撃：AIエージェントの出現

AIのセキュリティ確保が課題として不十分な場合、AIエージェントは、新たな耐久レースを提供することになかもしれません。AIエージェントは、人間のような自律性を備えた動的なマシンIDとして、全く新しいレベルの複雑さをもたらします。単なる情報処理コンテンツツールではなく、AIエージェントは定義された目標に基づいて認識、推論、行動するマシンIDです。では、数千、あるいは数百万ものこれらのエンティティを保護することを想像してみてください。システム（および他のエージェント）との適切な認証を確保し、機密データへの特権アクセスを規制し、多様なシステムや地域にまたがって権限が残存する不正エージェントを回避するための厳格なライフサイクル管理を維持する必要があります。大規模かつ適切に管理・監視されなければ、多くの問題が発生する可能性があります。

AIエージェントの攻撃対象領域は、次の3つの重要な層にまたがっています。

1. インフラストラクチャ層：エージェントが存在するシステムの認証情報
2. アクセス層：エージェントに関連付けられた権限または資格
3. モデル層：AI自体。これは、騙されたり乗っ取られたりする可能性があります

最初の2つは、マシンIDのセキュリティ確保におけるよくある課題を反映していますが、3つ目は、AIの非決定論的な動作と推論能力に関連する特有のリスクをもたらします。これは、まさに不正行為につながります。ガードレールがなければ、モデル層のAIエージェントは、人間よりもはるかに速く、悪意のあるコマンドの実行、データ漏洩、権限の昇格、または不正アクセスの許可を行うように操作される可能性があります。従来のIAMシステムは、数千（または数百万）のこれらのインテリジェントエンティティに必要な認証、認可、および監視プロトコルを処理できる体制が整っていません。

専門家は、まだ広く導入されていませんが、2028年までにAIエージェントが日常業務の意思決定の少なくとも15%を行うようになると予測しています。そのメリットは否定できませんが、準備がなければ、組織は多額のセキュリティ負債を抱えるリスクがあります（図7）。ここでは、場当たり的な修正は通用しません。組織には堅牢なバックエンドインフラストラクチャが必要です。ベストプラクティスには以下が含まれます。

- AI IDが不正アクセスに悪用されることを防ぐ特権アクセス制御
- AI駆動型マシンIDの活動を継続的に可視化するガバナンス
- AIの活用を責任ある導入と規制遵守に整合させる行動規範。当社では、企業全体にわたってコンテキスト認識型、相互運用性、そして安全なAIエージェントワークフローを保証する初期のAI設計標準であるモデルコンテキストプロトコル（MCP）をサポートしています。

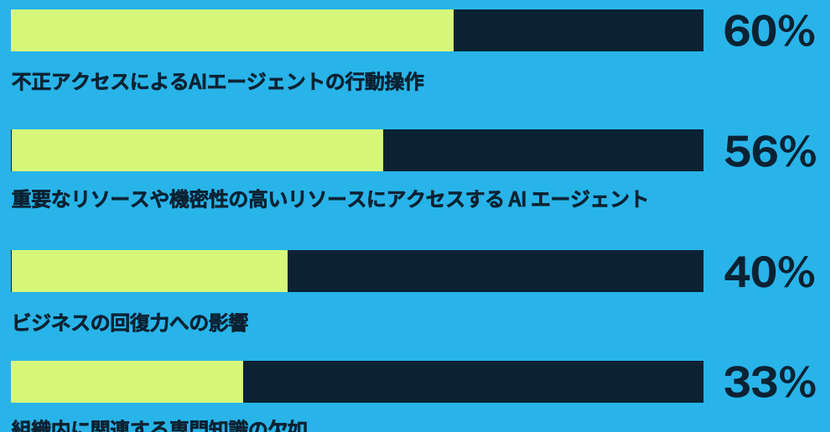


図 7. AI エージェントに関して組織が直面する主な課題
(複数選択可、n=2,600)

AIの三要素：攻撃者、防御者、そしてアイデンティティリスク

CyberArk Insight

AIは今やビジネスに不可欠な要素となっています。今後の展望としては、AIを活用したソリューションやサービスの開発、導入、そして活用方法に関する積極的な対策が不可欠です。

私たちは３段階のアプローチをお勧めします。

- **セキュアな開発：**AIシステムを支援するコードやモデルを作成する開発者は、トレーニングデータがクリーンで代表的であることを保証する強力なセキュリティプラクティスに従う必要があります。
- **セキュアな導入：**AIシステムをテスト段階から運用環境に移行し、ユーザーや他のシステムとやり取りする際には、運用環境は厳格なIDセキュリティ対策を遵守し、改ざん、不正アクセス、操作から保護する必要があります。
- **セキュアな利用：**攻撃者がユーザーアクセスを悪用できないようにするためには、AIをIDセキュリティモデルに統合する必要があります。これは、後付けではなく、包括的な戦略の一部として行う必要があります。

安全なアイデンティティ＝安全なAIエージェント

人間のように振る舞うマシンには、人間とマシンの両方のセキュリティ管理が必要です。各エージェントは、人間のユーザーと同様に、一意に識別、認証、管理される必要がありますが、同時に、マシン規模の運用に必要な厳格さも求められます。こうした二重の保護体制がなければ、初期のRPA導入で見られたような、なりすまし、過剰な権限付与、そしてガバナンスの欠如によって悪用される可能性が高まった、アイデンティティの混乱を繰り返すリスクがあります。

マシンアイデンティティ：スプロールの覚醒

CYBERARK®

マシンアイデンティティ：スプロールの覚醒

人間の目（または監査ログ）には見えませんが、マシンIDはデジタルインフラを静かに稼働させています。マシンIDがなければ、デバイス、クラウド、サーバー、アプリケーション、コンテナ、そしてソフトウェアプロセスは、鍵がテープで留められた錠前と同じくらい安全でしょう。しかし、毎日、新しいクラウドワークロード、AI/MLサービス、自動化プロセス、そして相互接続されたシステムがオンラインになり、認証のために新しいマシンIDが必要になります。マシンIDの増加量、種類、そして速度が減速の兆しを見せないのは当然のことです。組織の94%が過去3年間でマシンIDの増加を報告しています。企業は、驚異的なマシンIDの急増の中で事業を展開しています。人間のID1つに対してマシンIDは80以上あり、このデータは2022年に初めて報告されて以来、ほぼ倍増しています（図8）。この比率は、金融セクターでは96:1、英国では100:1にも達し、人間のセキュリティチームにとっては恐ろしい課題となっています。

調査回答者の半数以上（54%）は、AIとLLMツールの導入が、特権アクセスや機密アクセスを持つマシンIDの作成を今後も促進すると予測しています。マシンIDは特権リソースへの直接的なチャネルを持つことが多いため、攻撃対象領域は拡大するどころか、爆発的に増加しています。

皆さん、ビジョンボードを取り出してみてください。組織は「特権ユーザー」に対する理解を深めていません。「特権ユーザー」を人間のみと定義する組織は依然として88%で、2024年には61%に増加しています。図8では、マシンIDの42%、ボットとマシンアカウントの68%が機密データにアクセスできることがわかりました（人間ユーザーの場合は37%）。マシンIDを「特権ユーザー」と見なしているのはわずか12%（図9）。このギャップを埋めるには、人間中心の「ユーザー」の定義を超えて、マシンにとっての「特権」を再定義する必要があります。人間以外のアイデンティティに対する特権アクセスは、見た目は異なるかもしれませんが、同様に可視化、管理、そしてガバナンスが不可欠です。

一般的に、マシンIDセキュリティ（MIS）は、ボットやサービスアカウントからスクリプト、クラウドワークロード、AIエージェントに至るまで、人間以外の重要なアイデンティティすべてを保護します。これらのエンティティが自律性とアクセスを獲得するにつれて、MISはもはや単なるIT衛生上の問題ではなく、エンタープライズセキュリティの中核を成す柱となります。

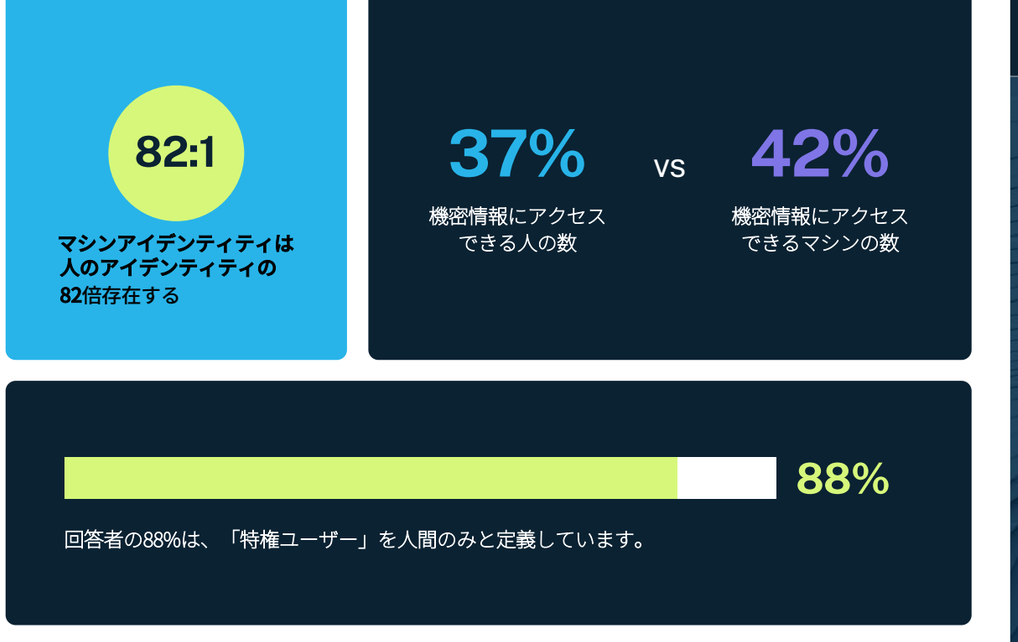


図 8. マシンID は量とアクセス リスクの点で人間を上回っています (n=2,600)

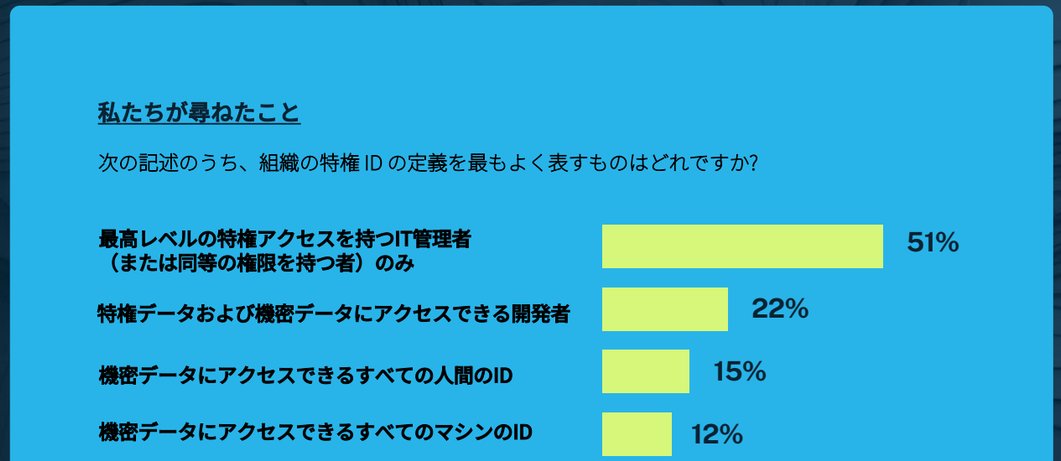


図 9. 組織全体の特権 ID の定義 (n=2,600)

私たちが尋ねたこと

今後 12 か月間に組織内で ID 数が増加する主な要因は何ですか? (複数選択可)

図 10. AI を超えたアイデンティティの増殖予測 (n=2,600)

嵐の中の（安全でない）港

サイバー犯罪者は好き嫌いをしません。どんなアイデンティティでも標的となります。そして、環境内で最も静かなユーザーであるマシンIDは、しばしば最も脆弱です。マシンIDに過剰な権限や永続的な権限が付与されている場合、攻撃者はそのマシンアカウントのIDを乗っ取るための経路を見つけることができます。攻撃者は、自身のデバイスやアプリを企業のIDシステムに登録し、検知されることなくアクセスを維持することができます。コードリポジトリ、ログ、構成ファイルからAPIキー、証明書、シークレットを抽出することも可能です。放棄されたサービスアカウントを乗っ取ることも可能です。攻撃者には非常に多くの選択肢があります。

これらの調査結果と一致して、マシンIDは、IT環境全体で最も管理されていない未知のIDという点で、今年最も認識されているIDリスクとして浮上しました。回答者の33%は、「特権」を人間のIDにのみ適用し、マシンIDには適用しないことでリスクを管理できていないと認めています。

冒頭で述べたように、セキュリティチームは規制当局からの矛盾したシグナルに対処しています。米国では、近年の変化から、AI監視へのより非干渉的なアプローチへの移行が示唆されており、規制緩和がイノベーションを促進するのか、それとも影響範囲を拡大するだけなのかという疑問が生じています。一部の連邦ガイドラインでは依然としてマシンIDが重要なゲートキーパーとして認識されていますが、現在、その動きの多くは米国外にあります。

例えばアジア太平洋地域では、オーストラリアのサイバーセキュリティ法2024が、同国初の広範に適用可能なサイバーセキュリティに特化した法律となりました。この法律は、政府がID管理を強化し、AIシステムのセキュリティ確保とガバナンスの方法を成文化しようとしているという、近年のトレンドを反映しています。一方、欧州連合（EU）はAI法の制定を推進しており、EUで事業を展開する企業は、厳格な新基準を満たすためにAIモデルを綿密に監視し、文書化しなければならないため、これに違反すれば多額の罰金が科せられます。

IDの急増はAIだけの問題ではありません。現代のインフラ全体にわたる、より広範かつ体系的な変化であり、慎重な計画が必要です。回答者の 59% は、今後 12 か月間で、マシン ID (クラウドワークロードからアプリの認証情報、自動化されたサービスまで) が ID の成長を牽引する主な要因となり、AI や LLM さえも上回ると予測しています (図 10)。

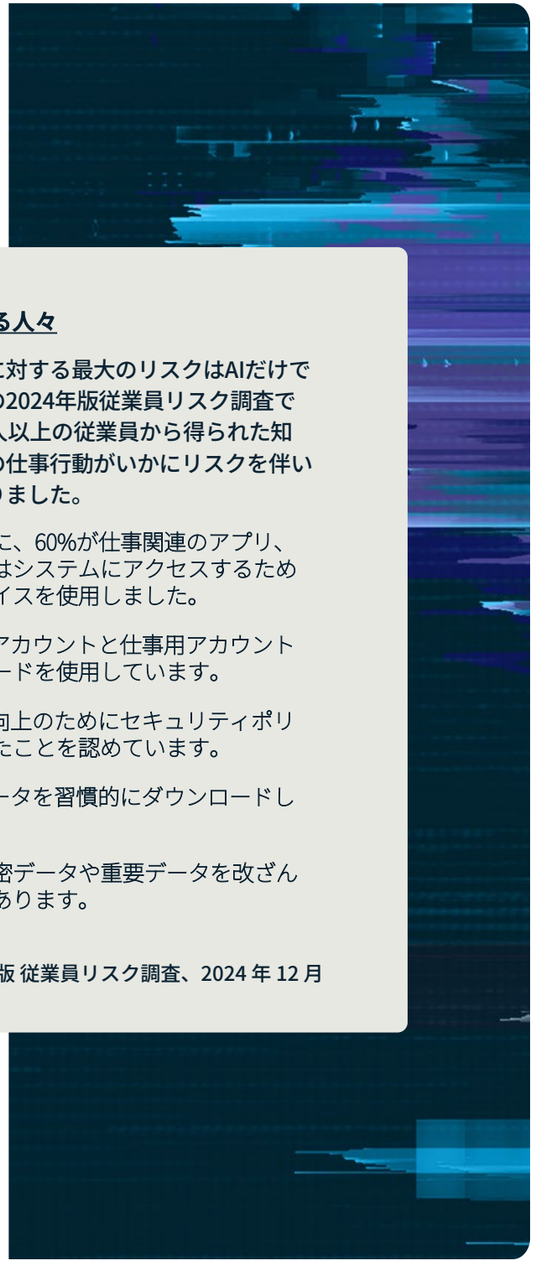
無知はリスク：アイデンティティの拡散における人間的側面

古き良き時代を懐かしんでいますか？ご安心ください。人間のアイデンティティは依然としてお馴染みの悩みの種であり、その悩みは拡散というよりもむしろ権限に関するものです。3大クラウドプラットフォームだけでも、4万を超える権限が存在します。従業員は、企業全体で数十ものSaaSアプリケーション、複数のクラウドプラットフォーム、AIツールにアクセスする必要があり、どこからでもログインしています。管理されていないエンドポイントは、セキュリティ上の大きな盲点となり、効果的な監視と保護が困難です。可視性がほとんど、あるいは全くないため、ITチームやセキュリティチームは潜在的なリスクに気付かないだけでなく、それらを適用することもできません。

CyberArk Insight

組織は、ソリューションの一元化と、従業員、IT、開発者、マシンなど、あらゆるアイデンティティがライフサイクルのあらゆる段階、つまり作成から利用に至るまでのあらゆる段階でセキュリティリスクをもたらすことを認識したアイデンティティセキュリティ戦略の導入に注力する必要があります。残念ながら、万能薬はなく、セキュリティ対策は山積みです。検討すべき点をいくつかご紹介します。

- ユーザーと管理者のセッションを監視、分析、監査し、脅威を検出できる制御機能により、すべてのIDを保護します。特権アクセス管理（PAM）と最小権限制御は、すべてのIDが役割に必要なアクセス権のみを持つようにするために不可欠です。
- 特権ユーザーの定義を見直し、すべてのマシン、サービスアカウント、ワークロードを含めるようにしてください。
- 管理対象を明確に把握してください。セキュリティチームは、クラウドサービスプロバイダーの組み込み（ネイティブ）シークレットストアでシークレットを検出する必要があります。
- すべてのアプリケーションとワークロードの種類にわたって、最初のリクエストからインストールまで、証明書のライフサイクルを自動化します。これにより、エラーが削減され、貴重なセキュリティチームのリソースの浪費を回避できます。
- セキュアブラウジングソリューションを導入することで、管理されていないエンドポイントのリスクを軽減します。
- ジャストインタイムまたは動的なシークレットローテーション、強力な認証および認可メカニズム、ロールベースアクセス制御（RBAC）などのさまざまなアプローチを活用します。



特権アクセスを支える人々

組織のセキュリティに対する最大のリスクはAIだけではありません。当社の2024年版従業員リスク調査では、世界中の14,000人以上の従業員から得られた知見が集められ、人間の仕事行動がいかにリスクを伴い得るかが明らかになりました。

- 過去12ヶ月間に、60%が仕事関連のアプリ、メール、またはシステムにアクセスするために個人用デバイスを使用しました。
- 36%が個人用アカウントと仕事用アカウントで同じパスワードを使用しています。
- 65%が生産性向上のためにセキュリティポリシーを回避したことを認めています。
- 40%が顧客データを習慣的にダウンロードしています。
- 3人に1人が機密データや重要データを改ざんする可能性があります。

CyberArk 2024年版 従業員リスク調査、2024 年 12 月

サイロを打破し、実を取る

サイロを打破し、実を取る

ほとんどの企業にとって、アイデンティティセキュリティは最初から壮大な戦略の一部だったわけではありません。組織がテクノロジースタックを構築する中で、少しずつ積み上げられてきたのです。通常の業務プロセス（合併、レガシーシステムなど）の中で、複数のグループがそれぞれ独立したシステムと異なるテクノロジーを使い分け、似たような目標の微妙に異なるバージョンを達成することになりました。つまり、サイロ化とは、農家にとっては良いことかもしれませんが、ビジネスのレジリエンスにとっては致命的なものです。当社の調査では、回答者の70%がサイロを組織リスクの根本原因と認識しています。ハイブリッドインフラストラクチャや、一部の監視されていないAIアプリの使用（図11）を考慮すると、サイロ化は戦略というより、信頼の喪失のように感じられるでしょう。

特権アクセス：管理を強化し、謎を解き明かす

この断片化は、権限とアクセス権限の追跡に重大な影響を及ぼします。組織の94%がすべてのクラウドセッションを自動的に保護・監視するツールを使用している一方で、68%はID管理ツールとセキュリティツールの統合不足が攻撃検知の妨げになっていると回答しています（政府機関では84%に上ります）。一方、攻撃者はこれらの障害に全く対処しておらず、機敏に行動し、環境間をシームレスに移動することができます。

サイロ化はコンプライアンスを困難にし、保険料の上昇にもつながります。前回のサイバー保険更新以降、回答者の88%が保険会社がより厳格な権限管理を求めていると回答し、89%がサイバー保険会社が最小権限の原則のより厳格な遵守を求めていると回答しています。

私たちが尋ねたこと

次のどれが組織内でアイデンティティ サイロを生み出しましたか? (複数選択可)

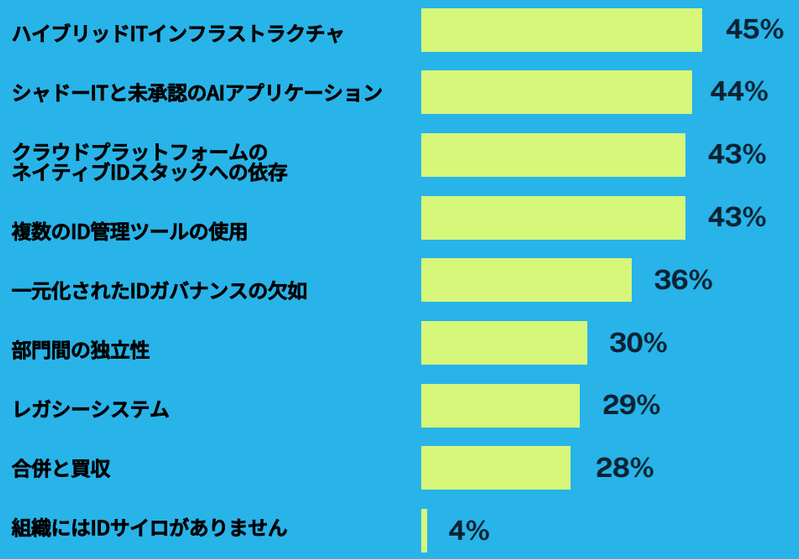


図 11. 組織におけるアイデンティティ サイロの原因 (n=2,600)

88% の回答者は、サイバー保険プロバイダーから権限制御の実装に関して厳しい要件に直面していると回答しています。

見えないものを守ることはできない

調査回答者のほぼ半数（49%）は、組織がクラウド環境全体の権限とアクセス権限を完全に把握できていないと回答しています（図12）。

アイデンティティ管理が確立されている場合でも、その適用は不均一です。クラウドインフラストラクチャとワークロードをカバーしていると回答した企業は40%未満です。DevOps環境（35%）、AIおよびLLM（32%）、サービスアカウント（23%）では、これらの領域が最も急速にリスクが増大しているにもかかわらず、管理率はさらに低下しています（図13）。

IGAは、全体を一つにまとめます。

IGAとPAMは、セキュリティインフラストラクチャの鉄人（アイアンマン）とジャービス（ジャービス）のようなものです。それぞれ独立して機能を発揮し、組み合わせることで完全なものとなります。

アイデンティティガバナンスと管理は、企業全体の可視性を高めるために不可欠です。IGAは、アイデンティティおよびアクセス管理（IAM）および特権アクセス管理システムと連携して、オンプレミス、クラウド、ハイブリッド環境全体のアイデンティティ管理を一元化・自動化します。リアルタイムのリスク評価に基づき、一貫したアイデンティティポリシー、アクセス制御、そして最小限の権限によるアクセスを確保します。これは、ゼロトラストの導入と、大規模なマシンアイデンティティの管理とセキュリティ確保の両方にとって不可欠です。

IGAの自動化は、監視を強化し、人的遅延を排除するとともに、組織がさまざまな政府および業界の規制に準拠するのに役立ちます。これにより、従業員の疲弊を防ぐことができます。

私たちが尋ねたこと

次の点について、どの程度同意または反対しますか?
私の組織では、クラウド環境全体の権限とアクセス許可を完全に把握できていません.

49%
が同意と回答

図 12. 回答者のクラウド環境全体の可視性レベル (n=2,600)

私たちが尋ねたこと

あなたの組織では、以下のどの環境とデバイスに対して ID セキュリティ制御を実施していますか? (複数選択可)

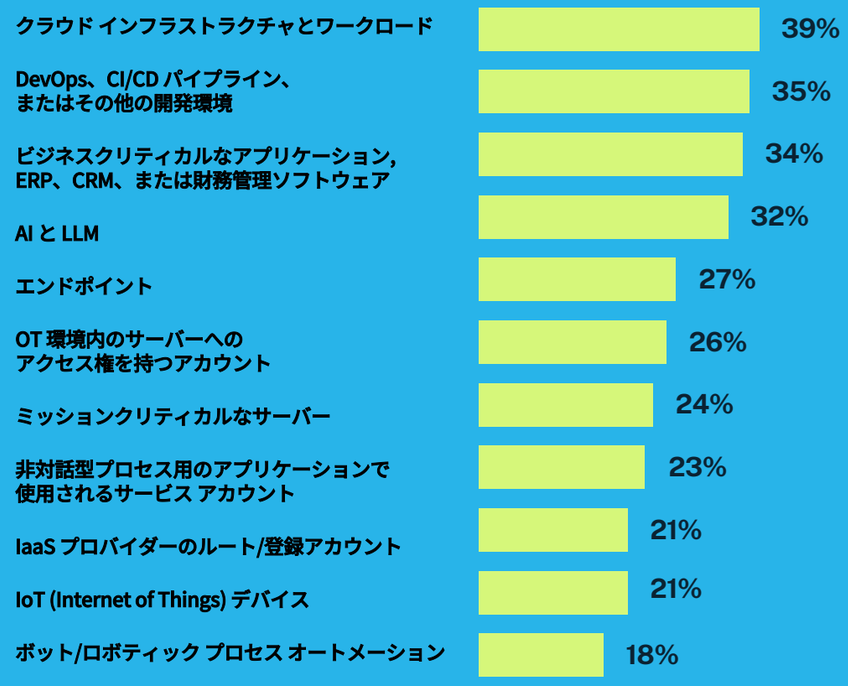


図 13. さまざまな環境における ID セキュリティ制御 (n=2,600)

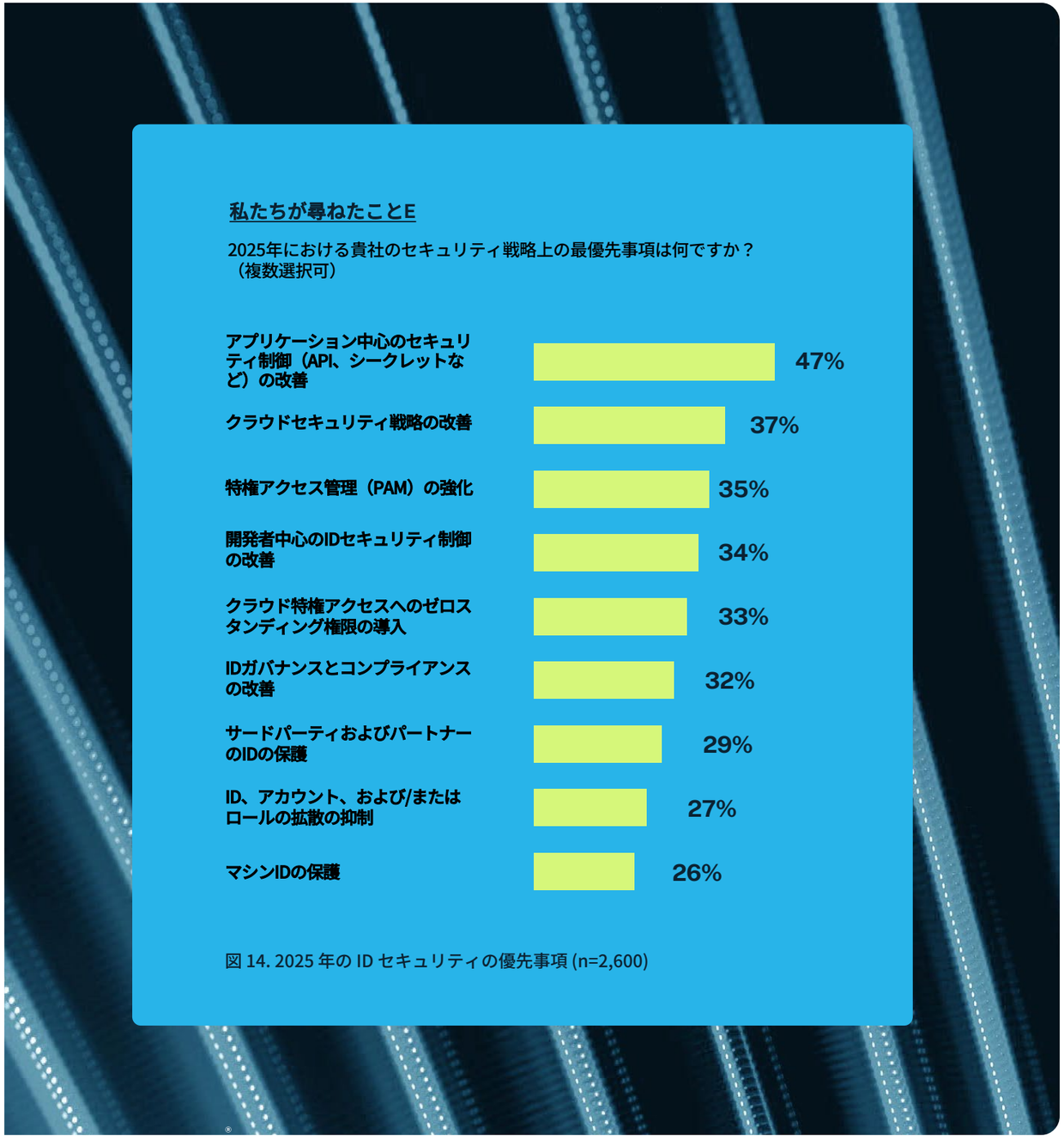


図 14. 2025 年の ID セキュリティの優先事項 (n=2,600)

サイロを破壊し、実を取る

2025年の戦略的アイデンティティセキュリティ投資項目

大多数の組織（87%）が、過去12か月間に、サプライチェーン攻撃や特権アクセスの侵害、IDおよび認証情報の盗難など、IDを中心とする侵害を少なくとも2件経験したと回答しています。しかし、セキュリティ専門家の75%は、組織において強力なサイバーセキュリティよりもビジネス効率を優先していると考えています。

朗報としては、組織がこれらの課題を認識しており、今後1年間で重要な優先事項に優先順位を付けていることが挙げられます。

図14に示すように、組織のほぼ半数（47%）が、独自の環境を保護するために、より優れたアプリケーションベースのセキュリティ制御を求めており、35%はより強力な特権アクセス管理（PAM）制御が最善の策であると認識しています。また、ますます複雑化するエコシステム全体にわたる監視の一貫性の欠如を考慮し、32%がIDガバナンスとコンプライアンス（IGA）への投資を計画しています。

セキュリティ専門家の 75% は、組織内で強力なサイバーセキュリティよりもビジネス効率が優先されると考えています。

サイロを破壊し、実を取る

CyberArk Insight

断片化されたレガシー ソリューションに対処することが、組織全体の姿勢を強化し、最終的には回復力のある企業を構築するための最善の方法です。

- 攻撃者の視点で考えましょう。最新の脅威を常に把握し、管理のギャップを常に把握しましょう。
- 「保護のための構築」の考え方を取り入れ、すべてのアイデンティティ、リソース、アカウントは、作成された瞬間から自動化と適切なレベルのインテリジェントな権限制御によって保護されます。
- IAMとアイデンティティセキュリティプロセスを合理化・自動化します。手動プロセスは、セキュリティの遅延やギャップを引き起こし、攻撃者に悪用される可能性があります。
- アイデンティティセキュリティツールを統合・一元化することで、運用効率を向上させ、セキュリティのタイムリー性を高め、分断されたアイデンティティプロセスを簡素化します。
- 複雑なマルチクラウドのユースケースに対応するために構築された、より高速で適応性の高いIGAソリューションでモダナイズします。

回答者の 70% は、サイロが組織リスクの根本原因であると考えています。

まとめ

まとめ

今日のサイバーセキュリティの脅威とAIに関する話題は、あまりにも蔓延し、しばしば背景の雑音に紛れ込んでいますが、私たちはこのけたたましい警鐘を鳴らす音を無視することはできません。

ランサムウェアは国家の資金調達手段となり、サイバー犯罪は最も収益性が高く、拡張性の高いビジネスモデルとなっています。

攻撃者はAIを戦術に組み込み、攻撃の拡張性と効率性を高めています。一方、組織はAIをワークフローに組み込み、新たなセキュリティ上の盲点を生み出しています。近い将来、AIエージェントは人間のような意思決定を行い、機械のように拡張できるようになるでしょう。

マシンIDの膨大な量、多様性、そして速度は、組織に既にその管理方法とセキュリティ保護方法の見直しを迫っています。一方、セキュリティチームは、対応すべきツール、アラート、そして不足するリソースに頭を悩ませています。

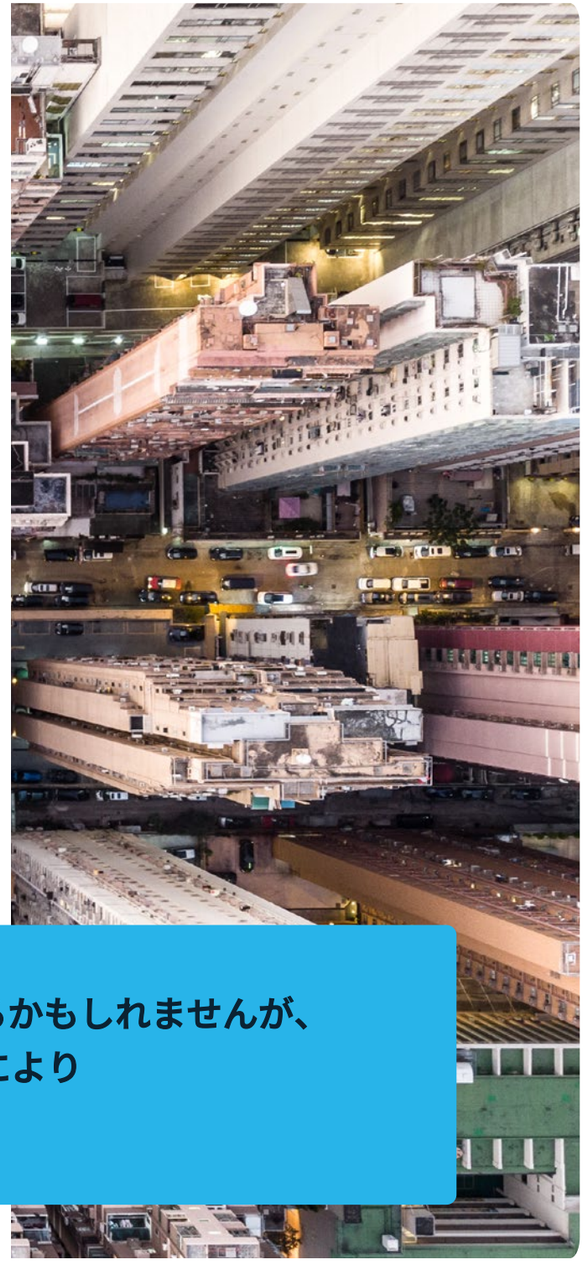
これらすべての中核を成すのは、IDです。どのような方法であれ、すべての攻撃者の目的はIDを侵害することです。この一点に絞ることで、今年そしてそれ以降の脅威への対応方法が簡素化され、再構築されるはずです。

2025年には、私たちが直面する集合的なリスクは、しばしば存在そのものを脅かすものとなるでしょう。しかし、私たちには、この状況に対応するための強力なリソースがあります。AIはルールを書き換えるかもしれませんが、アイデンティティセキュリティはリスクを抑制します。組織は、人間とマシンを問わず、あらゆるアイデンティティを保護し、現実世界のアイデンティティ脅威に対応する、一貫性のあるエンドツーエンドのエクスペリエンスを提供する必要があります。適切な準備があれば、次に何が起こっても、それを凌駕し、先手を打って、先を行き、そして耐え抜く防御を構築できます。

ビジネスのレジリエンス（回復力）を構築するには、組織はアイデンティティセキュリティを基盤とした、実践的でリスクベースのアプローチが必要です。そのためには、

- 大規模なAIエージェントの認証とセキュリティ保護を実現すること
- 機密データへのアクセスを管理・制限すること
- AI IDライフサイクルを制御し、不正アクセスを防止すること
- 経験豊富で信頼できるパートナーと連携し、セキュリティツールを統合すること

AI エージェントがより多くの責任を担い、特権アクセスの境界が拡大するにつれて、この戦略により、業務を中断することなく、サイバーセキュリティ インシデントを効果的に予測し、耐え、回復できるようになります。



AI によりルールが書き換えられるかもしれませんが、アイデンティティ セキュリティにより リスクを制御できます。

付録

付録

集計方法とデモグラフィック

本レポートは、2025年1月から2月にかけて、民間および公共部門の組織全体で調査されました。この調査は、B2Bテクノロジーリサーチパートナーの Vanson Bourne社が、ブラジル、カナダ、メキシコ、米国、フランス、ドイツ、イタリア、オランダ、南アフリカ、スペイン、英国、UAE、オーストラリア、インド、香港、イスラエル、日本、サウジアラビア、シンガポール、台湾に拠点を置く2,600人のサイバーセキュリティ意思決定者を対象に実施しました。

回答者の所在地域

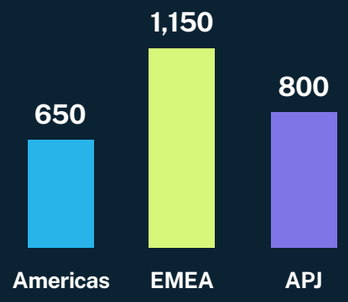


図15. 回答者の地域別内訳（n=2,600）

回答者の業種

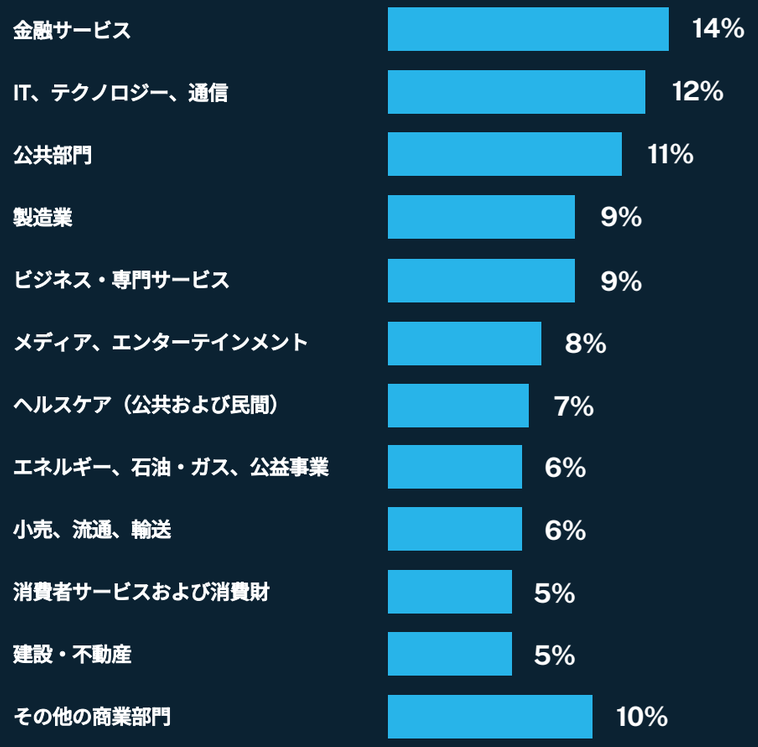


図16. 回答者の業種別内訳（n=2,600）

回答者が所属する企業の売上規模

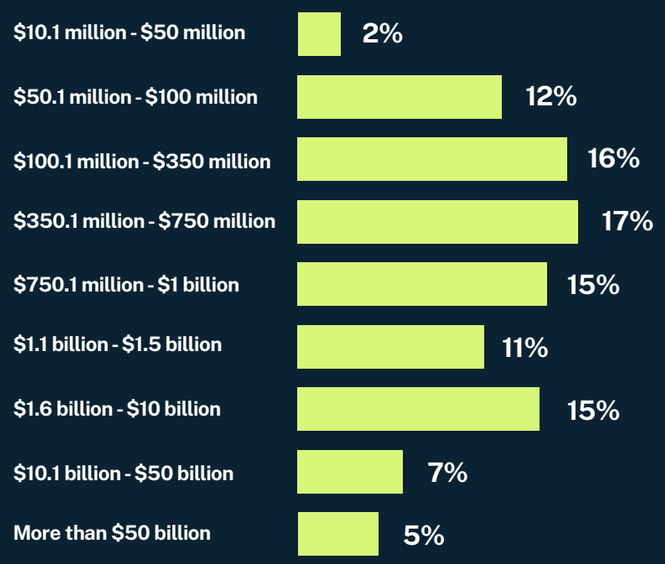


図17. 回答者が所属する企業が報告した2024年の売上規模（n=2,600）

回答者が所属する部門

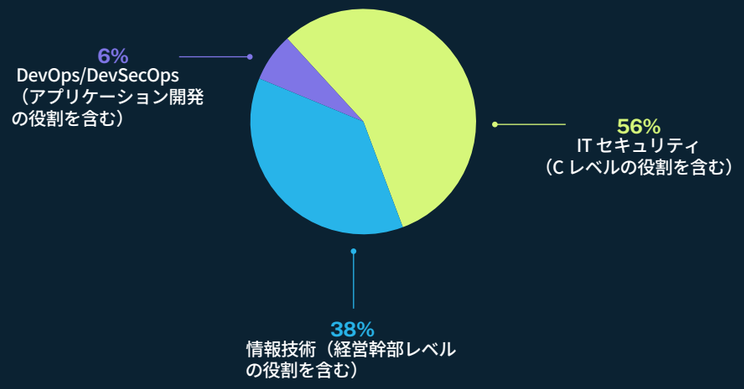


図18. 回答者の部門別内訳（n=2,600）

回答者の役職

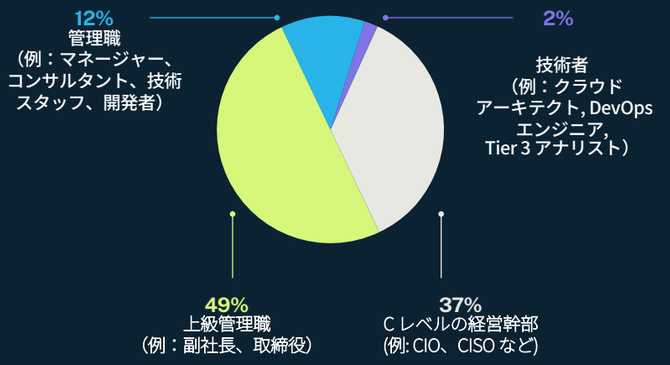


図19. 回答者の職名別内訳（n=2,600）

アイデンティティセキュリティの責任者

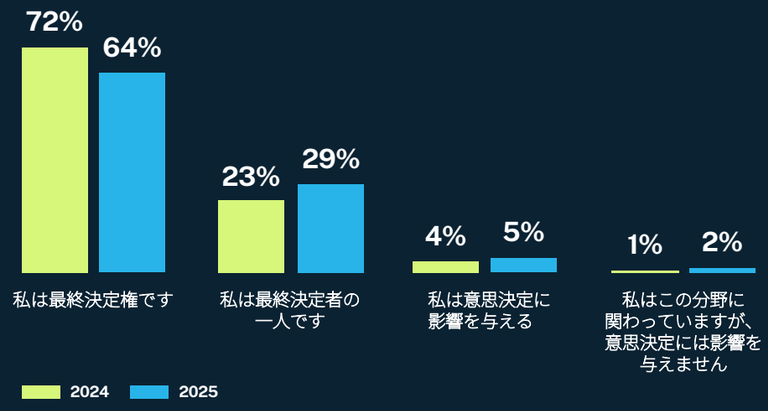


図 20. アイデンティティ セキュリティ責任別の回答者の内訳 (n=2,600)

SECURITYMATTERS

CYBERARK® Research

AIへの世界的な投資は莫大です。アイデンティティセキュリティのリスクはさらに深刻です。アイデンティティセキュリティの取り組みを導くベストプラクティスをご紹介します。

詳しく知る

About CyberArk

CyberArk (NASDAQ: CYBR) is the global leader in identity security, trusted by organizations around the world to secure human and machine identities in the modern enterprise. CyberArk's AI-powered Identity Security Platform applies intelligent privilege controls to every identity with continuous threat prevention, detection and response across the identity lifecycle. With CyberArk, organizations can reduce operational and security risks by enabling zero trust and least privilege with complete visibility, empowering all users and identities, including workforce, IT, developers and machines, to securely access any resource, located anywhere, from everywhere. Learn more at www.cyberark.com.

CYBERARK®