レポート

アイデンティティセキュリティの現状 2026 年版

17 か国の IT およびサイバーセキュリティリーダー 5,000 人から得られた洞察

SOPHOS

はじめに

アイデンティティはサイバーセキュリティの境界線であり、その境界は拡大し続けています。その背景には、AI システムがメール、ファイル、SaaS アプリケーション、そして人間および人間以外のアイデンティティを通じて、企業データへアクセスする機会が増えていることがあります。その結果、機密情報へのアクセスや持ち出しが以前より容易になり、さまざまなリスクが高まっています。

組織ではクラウド導入やリモートワークの推進に加え、マシン間接続に依存するアプリケーションやサービスの増加が進んでおり、人間と人間以外の両方のデジタルアイデンティティの数が爆発的に増加しています。すべてのユーザー認証情報、API キー、サービスアカウント、OAuth トークンが、攻撃者にとって侵入経路となる可能性があります。そのため、アイデンティティセキュリティは、現代のサイバー防御において最も重要かつ対処が難しい領域の 1 つとなっています。

攻撃者も、この変化を認識しています。窃取された認証情報、侵害されたサービスアカウント、従業員を狙ったソーシャルエンジニアリング攻撃は、現在、世界中の侵害事例において最も一般的な初期アクセス方法となっています。攻撃者は AI と自動化を活用し、より多くのシステムへ、より迅速に侵入しています。その結果として生じる被害は、データ窃取や恐喝から、業務を数日から数週間にわたり停止させる大規模なランサムウェア攻撃にまで及びます。

アイデンティティ関連脅威の実態と影響規模を把握するため、ソフォスは独立した機関に調査を委託し、17 か国の IT およびサイバーセキュリティ責任者 5,000 人を対象に、2025 年におけるアイデンティティ脅威の被害経験と影響について調査しました。本レポートでは、その調査結果をもとに、アイデンティティ攻撃の発生頻度、組織による検知と阻止能力、攻撃によって生じた影響、侵害成功の根本原因、財務的損失、そしてアイデンティティセキュリティ対策の現状について分析します。

調査結果からは、アイデンティティ脅威が広範囲に及び、深刻な影響をもたらすとともに、ランサムウェアと密接に結びついている実態が浮き彫りになりました。アイデンティティセキュリティへの投資を怠る組織は、業務運営、財務、企業の信頼性に重大なリスクを抱えることになります。

5,000 人

独立した調査会社が実施したグローバルな調査に参加した 17 か国の IT およびセキュリティのリーダーの数

主な調査結果の概要

- **過去 12 か月間に、71% の組織が少なくとも 1 件のアイデンティティ関連セキュリティ侵害を経験しており、**被害を受けた組織では平均 3 件の攻撃が発生していました。
- **侵害を受けた組織の 14% は、最も重大なアイデンティティ攻撃について、**被害が発生する前に検知して阻止することができませんでした。
- **アイデンティティ侵害の復旧にかかった平均費用は 164 万ドルで、**中央値は 75 万ドルでした。
- **アイデンティティ攻撃が成功した場合の主な被害は、**データ窃取 (49%) とランサムウェア (48%) でした。
- **ランサムウェア被害を受けた組織の 3 分の 2 (67%) は、そのランサムウェア攻撃が同時に最も重大なアイデンティティ攻撃でもあったと回答しており、**アイデンティティ侵害からランサムウェアへ至る明確な攻撃フローが存在することが示されました。
- **人間以外のアイデンティティ (NHI) の管理の不備は、**アイデンティティ侵害の 41% で指摘されており、人為的ミス (43%) に次いで 2 番目に多い要因となっています。
- **人間以外のアイデンティティの管理が不十分な組織は、金銭窃取の被害を受ける可能性が 22% 高く、**恐喝被害を受ける可能性も 24% 高いことが分かりました。さらに、復旧コストの総額は平均より約 15 万ドル高いと報告されています。
- **サービスアカウントや人間以外のアイデンティティを定期的にローテーションまたは監査している組織は 3 分の 1 (34%) にとどまり、**継続的に実施している組織はわずか 11% でした。攻撃者は、このようなセキュリティギャップを悪用しています。
- **不審なログイン試行を継続的に監視している組織はわずか 24% にとどまり、**半数以上は 3 か月に 1 回以下の頻度でしか確認していません。
- **アイデンティティ侵害の発生率が最も高かったのは、エネルギー / 石油・ガス / 公共事業 (80%) および中央 / 連邦政府機関 (78%) でした。**一方、最も低かったのは IT/テクノロジー / 通信 (63%) と医療機関 (63%) でした。
- **従業員数 100 ～ 250 人規模の組織は、**1,001 ～ 3,000 人規模の組織と比べて、アイデンティティ攻撃を検知できる割合が 72% 低いことが分かりました（19% 対 11%）。

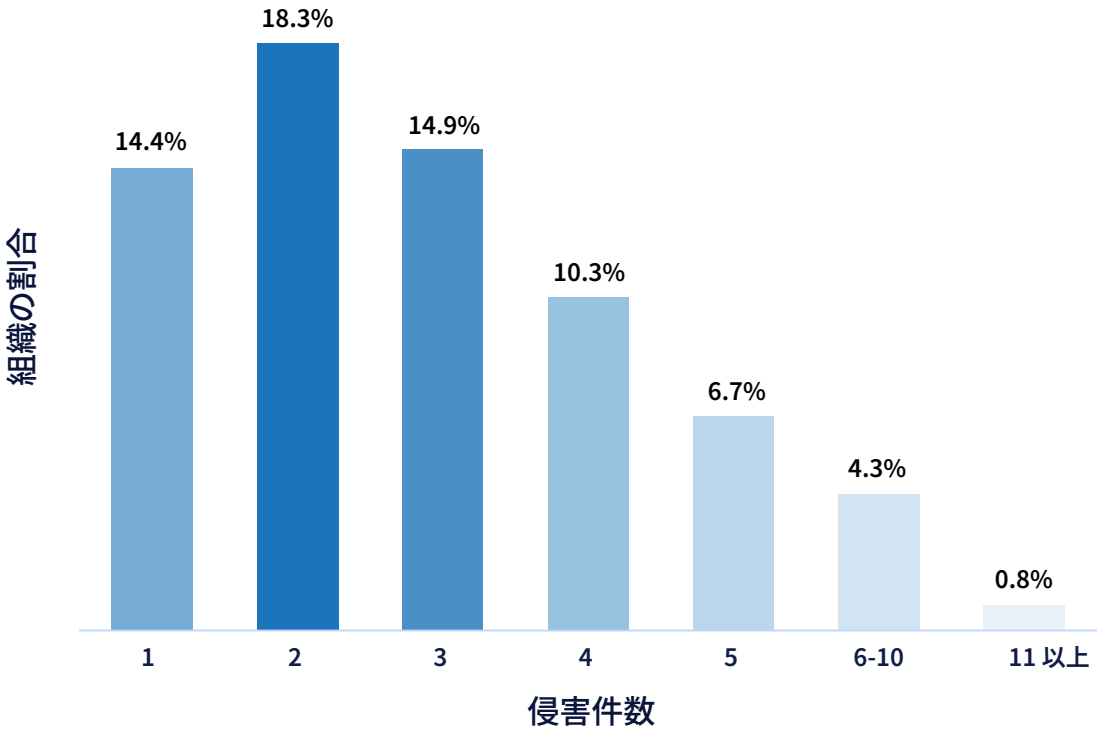
詳細な調査結果

アイデンティティ攻撃の発生頻度

今回の調査から、アイデンティティに関連する侵害は例外的な事例ではなく、常態化していることが明らかになりました。過去 12 か月間に、10 社中 7 社以上 (70.9%) が少なくとも 1 件のアイデンティティ関連セキュリティ侵害を経験していました。侵害を受けていないと明確に回答した組織はわずか 22.6% にとどまり、6.4% は、自社が把握していない形で侵害が発生していた可能性があると認めています。

侵害を受けた組織では、インシデント件数の平均は 3.1 件に達しており、アイデンティティ攻撃が一度で終わるケースはまれであることを示しています。回答者の 5% は、過去 1 年間に 6 件以上の侵害を経験したと報告しています。

アイデンティティ侵害の発生頻度分布



過去 12 か月間にアイデンティティに関連するセキュリティ侵害を経験しましたか？経験した場合、何件の侵害がありましたか？ 回答者数 =5,000

67%

2025 年に Sophos Incident Response および Sophos MDR が対応したインシデントのうちアイデンティティが攻撃に起因していた割合

Sophos X-Ops Insight

国別分析

侵害発生率には地域によって大きなばらつきが見られます。スイス (88.7%) が最も高い侵害率を報告しており、世界平均を 18 % 上回りました。これに続いてメキシコ (83.3%)、イタリア (80.0%) が高い水準となっています。最も影響が少なかったのはドイツ (62.6%)、コロンビア (62.7%)、日本 (64.7%) でしたが、いずれも 60% を超える高い水準となっています。

国	侵害率	vs. 世界平均 (70.9%)
スイス	88.7%	+17.8 pp
メキシコ	83.3%	+12.4 pp
イタリア	80.0%	+9.1 pp
オーストラリア	79.7%	+8.8 pp
インド	76.8%	+5.9 pp
南アフリカ	75.0%	+4.1 pp
ブラジル	74.0%	+3.1 pp
アラブ首長国連邦 (UAE)	73.3%	+2.4 pp
シンガポール	72.0%	+1.1 pp
スペイン	70.0%	-0.9 pp
チリ	66.7%	-4.2 pp
米国	66.1%	-4.8 pp
フランス	66.0%	-4.9 pp
英国	65.3%	-5.6 pp
日本	64.7%	-6.2 pp
コロンビア	62.7%	-8.2 pp
ドイツ	62.6%	-8.3 pp

過去 12 か月間にアイデンティティに関連するセキュリティ侵害を経験しましたか？経験した場合、何件の侵害がありましたか？ 回答者数 =5,000

業界別分析

業界別に見ると、エネルギー / 石油 / ガス / 公共事業 (80.3%) および中央 / 連邦政府機関 (78.4%) が、最も高い侵害発生率を報告しています。IT/ テクノロジー / 通信 (63.1%) と医療機関 (63.4%) が最も低い水準となっており、これらの業界ではセキュリティ投資の成熟度が相対的に高いことが影響している可能性があります。

業種	侵害率
エネルギー / 石油・ガス / 公共サービス	80.3%
中央 / 連邦政府	78.4%
建設 / 不動産	76.1%
製造 / 生産	73.6%
小売業	72.0%
初等中等教育機関 (K-12)	71.1%
金融サービス	71.0%
メディア / レジャー / エンターテイメント	70.9%
地方自治体 / 州政府	69.6%
流通 / 輸送	67.6%
高等専門教育機関	65.9%
ビジネス / プロフェッショナルサービス	64.5%
医療機関	63.4%
IT/ テクノロジー / 通信	63.1%

過去 12 か月間にアイデンティティに関連するセキュリティ侵害を経験しましたか？経験した場合、何件の侵害がありましたか？ 回答者数 =5,000

コンプライアンス状況の指標

コンプライアンス要件への対応を「非常に困難」と回答した組織では、侵害率が 82.4% に達し、「ある程度困難」または「まったく困難ではない」と回答した組織 (68.3%) よりも 14% 高い結果となりました。この結果は、コンプライアンス対応に苦慮しているほど、より広範なセキュリティ上の脆弱性を抱えていることを示す重要な指標となります。

アイデンティティセキュリティの基礎

組織が管理すべき 4 つのタイプのアイデンティティ

あらゆる組織が、さまざまなタイプのアイデンティティにアクセス権を付与しています。それぞれのアイデンティティに固有のリスクがあります。

カテゴリ 1 – 従業員のアイデンティティ

業務を行うためにシステムやデータへのアクセスが必要な組織内の関係者。

- 従業員
- 請負業者
- IT および情報セキュリティ管理者 (高いシステム権限を必要とする役割の担当者)
- 経営幹部 (攻撃者にとって特に価値の高い標的となり得る役割の担当者)

カテゴリ 2 – 外部のアイデンティティ

特定の役割や業務上のやり取りを遂行するために、一時的または継続的に組織外からアクセス権が付与される個人。

- パートナー
- サプライヤー
- カスタマーサービス

カテゴリ 3 – 人間以外のアイデンティティ (NHI)

人間の介在なしにタスクを実行するためにアクセス権が付与されたソフトウェア、システム、および自動化プロセス。

- サービスアカウント (例：定期バックアップなど)
- API キー (例：アプリ連携など)
- AI エージェント (例：自律的なタスクなど)
- IoT デバイス (例：センサーやカメラなど)

カテゴリ 4 – 特権アイデンティティ (最もリスクが高い)

機密システムやデータへの高度なアクセス権を持つ、特権が付与された人間または人間以外のアイデンティティ。

- スーパ管理者 (システム全体の完全な制御権限を持つユーザー)
- ルートアカウント (例：クラウド環境における管理者権限アクセス)
- 共有アカウント (例：チーム単位で共有されるログイン情報)
- 緊急アクセス (例：緊急時用の特権アクセス)

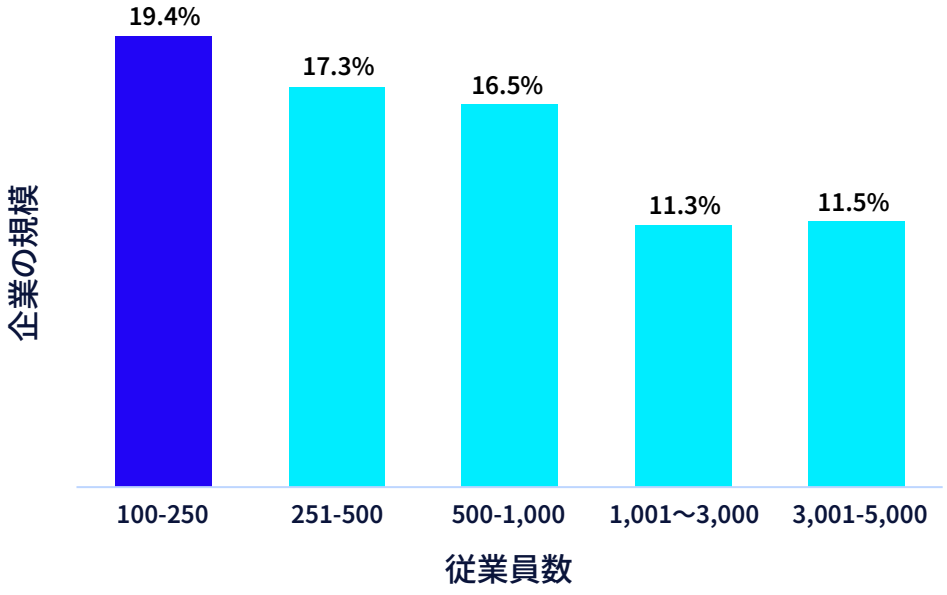
すべてのアイデンティティが侵入経路となり得ます。誰が、あるいは何がシステムにアクセスできるのかを管理し、そのアクセスが適切であり監視されていることを担保することは、組織がセキュリティを維持するうえで最も重要な取り組みの一つです。

アイデンティティ攻撃を検知および阻止する能力

2025 年にアイデンティティ関連の侵害を経験した 3,545 人の回答者のうちの 85.4% は、最も重大な攻撃を被害が発生する前に検知および阻止することができました。これは、多くの組織が一定の検知能力を備えていることを示す一方で、攻撃を阻止できなかった 14.4% は、発生頻度は低いものの影響の大きい重大なリスクを抱えており、後続の調査結果が示すように、その影響は深刻なものとなっています。

組織規模別の検知失敗率

小規模組織は、攻撃を検知できる可能性が大幅に低くなっています。調査対象の最小規模企業 (従業員 100 ～ 250 人) では、19.4% が攻撃を阻止できなかったのに対し、従業員 1,001 ～ 3,000 人規模の組織では 11.3% にとどまり、ほぼ 2 倍の差が見られました。この差は、中小規模の企業が直面しているリソースおよび対応能力の課題を浮き彫りにしています。



過去 12 か月間において経験した最も重大なアイデンティティ攻撃について、その攻撃による被害が発生する前に検知し、阻止することはできましたか？母数：アイデンティティ関連のセキュリティ侵害を経験した組織の数。回答者数 =3,545。

国別の検知失敗率

検知失敗率はブラジル (21.6%) とスイス (21.1%) で最も高く、一方で英国 (7.1%) とメキシコ (9.6%) が最も低い結果となりました。注目すべき点として、スイスは侵害率の高さに加えて検知失敗率も高く、特にリスクの高い市場であることが分かります。

国	検知失敗率
ブラジル	**21.6%**
スイス	21.1%
日本	19.6%
スペイン	18.1%
チリ	18.0%
シンガポール	17.6%
ドイツ	17.4%
フランス	14.6%
イタリア	14.6%
オーストラリア	13.8%
コロンビア	13.8%
米国	12.8%
アラブ首長国連邦 (UAE)	11.8%
インド	11.2%
南アフリカ	10.7%
メキシコ	9.8%
英国	7.1%

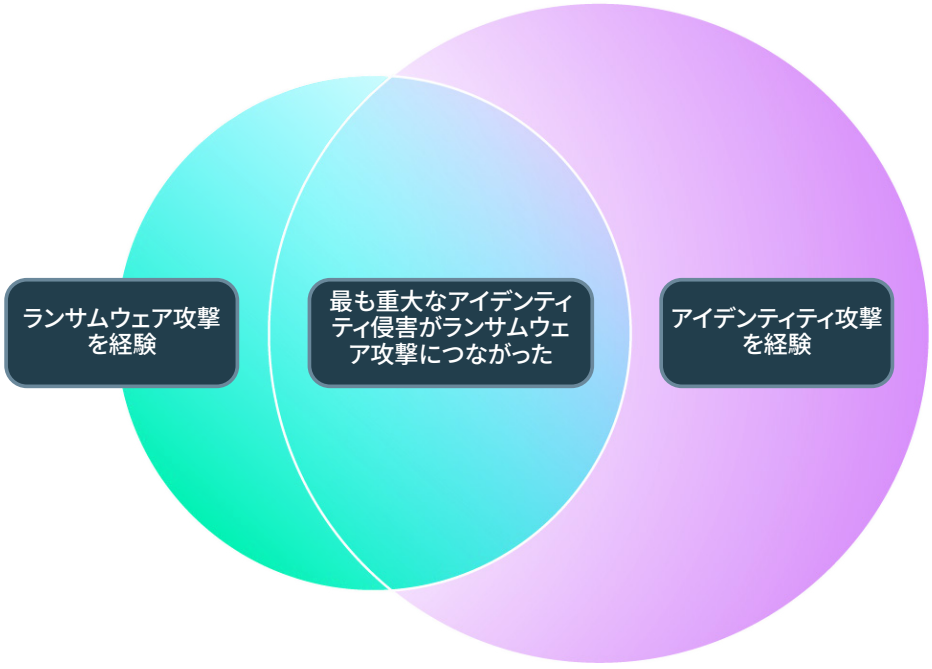
過去 12 か月間において経験した最も重大なアイデンティティ攻撃について、その攻撃による被害が発生する前に検知し、阻止することはできましたか？母数：アイデンティティ関連のセキュリティ侵害を経験した組織の数。回答者数 =3,545。

業界別の検知失敗率

メディア / レジャー / エンターテインメント業界 (22.4%) が最も高い検知失敗率を示し、次いで製造業 (18.4%)、金融サービス (17.9%) が続きました。医療業界が最も低い検知失敗率 (8.1%) を示しましたが、厳格な規制要件が課せられていることが脅威監視への投資を促している可能性があります。

アイデンティティとランサムウェアの関連性

本調査で最も注意すべき発見の一つは、アイデンティティ攻撃とランサムウェアの間に直接的な関連があることです。2025 年にランサムウェア被害を受けた組織のうち、3 分の 2 (66.5%) は、そのランサムウェアインシデントが自社における最も重大なアイデンティティ攻撃と同一のイベントであったと回答しています。すべての攻撃がデータ暗号化につながったわけではないものの、アイデンティティの侵害がランサムウェアを展開する主要な手段であることが示されています。



過去 1 年間にランサムウェア攻撃を受けましたか？という質問に「はい」と回答（回答者数 =5,000)。過去 12 か月間にアイデンティティに関連するセキュリティ侵害を経験しましたか？該当する場合、何件でしたか？ (回答者数 =5,000) [両方「はい」と回答した場合] ランサムウェアインシデントは、最も重大なアイデンティティ関連攻撃と同一のイベントでしたか？

組織規模別のランサムウェアとアイデンティティの関連性

アイデンティティとランサムウェアの関連性は、従業員 1,001 ～ 3,000 人規模の組織で最も高く (71.6%)、従業員 100 ～ 250 人規模の組織で最も低い結果となりました (62.4%)。このばらつきは、組織インフラの複雑性、可視性のレベル、あるいは攻撃経路と被害結果を関連付ける能力がセグメントごとに異なることを反映している可能性があります。

組織の規模	ランサムウェア＝アイデンティティ攻撃
従業員 100 ～ 250 人	62.4%
従業員 251 ～ 500 人	68.2%
従業員 501 ～ 1,000 人	62.5%
従業員 1,001 ～ 3,000 人	**71.6%**
従業員 3,001 ～ 5,000 人	64.6%

過去 1 年間にランサムウェア攻撃を受けましたか？という質問に「はい」と回答（回答者数 =5,000）。過去 12 か月間にアイデンティティに関連するセキュリティ侵害を経験しましたか？該当する場合、何件でしたか？ (回答者数 =5,000) [両方「はい」と回答した場合] ランサムウェアインシデントは、最も重大なアイデンティティ関連攻撃と同一のイベントでしたか？

業界別分析

高等教育機関 (76.8%) および流通 / 輸送 (75.0%) では、ランサムウェアとアイデンティティの関連性が最も強く見られた一方で、金融サービス (57.6%) および IT/ テクノロジー / 通信 (61.1%) では比較的低い結果となりましたが、いずれも過半数を大きく上回っています。

検知されなかったアイデンティティ侵害の影響

最も重大なアイデンティティ攻撃を阻止できなかった 510 の組織では、被害は深刻かつ多岐にわたり、1 件のインシデントあたり平均で 2 つの影響が報告されました。

結果	侵害された組織の割合
データ窃取 – 攻撃者による機密データの盗み出し	**48.8%**
ランサムウェア – ランサムウェア攻撃の実行を支援するために盗まれた認証情報が使用されたケース	48.4%
恐喝 – 攻撃者が脅迫により金銭を要求したケース	43.9%
破壊工作 — 攻撃者が認証情報を使用して組織に損害を与えたケース	30.0%
金銭窃取 — 支払いの不正送金	28.0%
金銭窃取 — アカウントから資金が盗まれたケース	25.5%
サマリー：金銭窃盗 (あらゆる形態)	**46.7%**

このアイデンティティ侵害が組織にどのような影響をもたらしましたか？母数：セキュリティ侵害を防ぐことができなかった組織。
回答者数 =510。

アイデンティティが侵害された組織のほぼ半数がデータ窃取 (48.8%) の被害を受けており、ほぼ同じ割合でランサムウェア被害 (48.4%) も発生していました。ほぼ半数 (46.7%) が、不正送金や資金窃取、またはその両方を含む直接的な金銭被害を経験しています。これらに加えて恐喝被害 (43.9%) も確認されており、アイデンティティ攻撃を検知できなければ、ほぼ例外なく重大な被害につながることを示しています。

組織が被害に遭った要因

攻撃が成功する要因を理解することは、予防のために不可欠です。今回の調査では、人的要因、プロセス上の問題、技術的な不備が複合的に作用し、組織がアイデンティティベースの攻撃被害に遭っている実態が明らかになりました。また、原因が単一であるケースはまれであり、回答者はインシデントに至った根本原因として平均で 2 つの項目を挙げています。

根本原因	侵害された組織の割合
人為的ミス — 従業員が騙されて認証情報を提供した	**42.7%**
人間以外のアイデンティティ管理の不備 (例：コード内に保存された API キー、静的な認証情報、過去にアプリケーションとシステムを接続していた孤立したサービスアカウントなど)	40.6%
不十分な従業員のアイデンティティ管理	38.6%
外部アプリケーションに付与されたアクセス権および権限に対する可視性の不足	35.7%
不十分なサプライヤーや請負業者のアイデンティティ管理	31.4%
外部アプリケーションに付与されたアクセス権および権限に対する制御の不足	30.8%
悪意のあるインサイダー — 従業員が意図的に攻撃を助長したケース	26.7%
概要：不十分な人間のアイデンティティ管理 (あらゆる形態)	**60.2%**
概要：外部アプリケーションに付与されたアクセス権および権限に関する問題 (あらゆる形態)	**56.1%**

アイデンティティ関連攻撃の被害に遭った原因は何でしたか？該当するものをすべて選択してください。母数：セキュリティ侵害を防ぐことができなかった組織。回答者数 =510。

人為的ミスは、アイデンティティ侵害につながる最大の要因であり、被害を受けた組織の 42.7% が原因として挙げています。次いで多かったのは、人間以外のアイデンティティ管理の不備（40.6%）でした。これには、コード内に保存された API キー、静的な認証情報、監査や監視が難しい孤立したサービスアカウントなどが含まれており、特に深刻な問題となっています。

従業員が意図的に攻撃を手助けした悪意あるインサイダーによる活動は、4 分の 1 を超える (26.7%) の攻撃で確認されており、強固な内部統制と継続的な監視の重要性を浮き彫りにしています。

全体として見ると、人間のアイデンティティ管理の不備 (60.2%) が、組織がアイデンティティベースの攻撃被害に遭う最大の要因でした。また、外部アプリケーションに付与されたアクセス権や権限に関する問題も、56.1% のインシデントに関連していました。

59.5%

2025 年のソフォスアクティブアドバーサリーレポートで分析された MDR 事例の 59.5% において、標的となったシステムで MFA (十年前から存在するテクノロジー) が有効ではありませんでした。

Sophos X-Ops Insight

組織規模別の分析

大規模組織は、小規模組織と比べて複数のアイデンティティリスク領域でより多くの課題を抱えています。これは監視および保護すべき環境が大規模で複雑であることを反映していると考えられます。

従業員 1,001 ～ 3,000 人規模の組織では、55.6% が人為的ミスを根本原因として挙げており、従業員 251 ～ 500 人規模の組織の 29.0% を大きく上回りました。同様に、従業員 3,001 ～ 5,000 人規模の組織では、68.6% が人間のアイデンティティ管理の不備によって攻撃被害を受けたと回答しており、従業員 100 ～ 250 人規模の組織 (58.5%) を上回りました。

人間以外のアイデンティティとは

人間以外のアイデンティティ (NHI) とは、人の介在なしにリソースへアクセスできるよう、ソフトウェア、システム、または自動化プロセスに付与されるデジタル認証情報です。NHI はパスワードの代わりに、以下のような認証情報を用いて自身を認証します。

- アプリケーションに接続する API キー
- バックアップを実行しているサービスアカウント
- SaaS との連携用の OAuth トークン
- データベースにアクセスする AI エージェント

NHI の認証情報も、人間のログイン情報と同様に盗まれ、不正利用される可能性があります。NHI には広範かつ高い権限が付与されているケースが非常に多いため、組織が NHI の権限を定期的に監査していない場合、その問題はさらに深刻になります。

NHI の数は人間の数を大幅に上回っており、組織によってはその比率が 100 対 1 を超えるケースもあります。近年、この比率の増加を大きく後押ししている要因の一つが、エージェント型 AI です。

96%

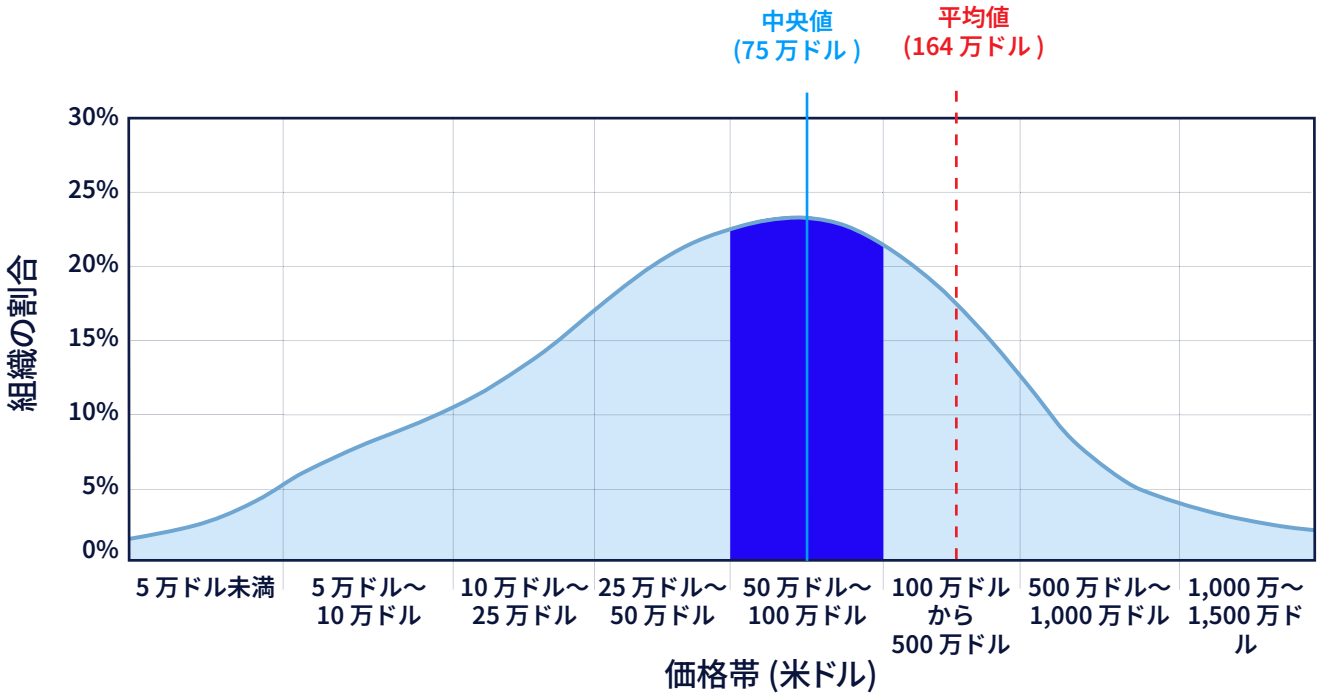
マルチテナントアプリケーションが存在していた Sophos ITDR の顧客環境の割合これらの環境と関係する NHI を監査したり、単に列挙したりすることさえ困難な場合があります。

Sophos X-Ops Insight

アイデンティティ侵害による財務的損失

アイデンティティ侵害に成功された組織は、多額の復旧コストを負担することになりました。世界全体で見ると、復旧費用の平均額は 1,637,363 ドル、中央値は 75 万ドルでした。侵害を受けた組織の 73% は 25 万ドル以上の費用が発生したと見積もっており、ほぼ 4 分の 1 (23.7%) は 50 万～ 100 万ドルの範囲でした。

費用の内訳



アイデンティティ侵害を修復するために要した総コストはどの程度でしたか？母数：セキュリティ侵害を防ぐことができなかった組織。回答者数 =510。

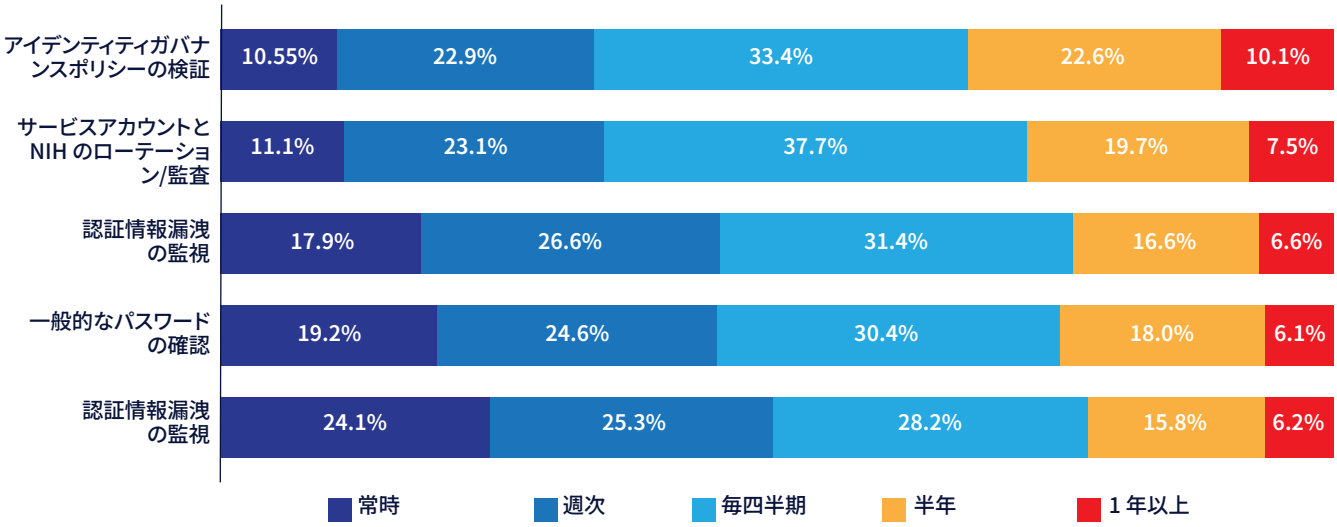
組織規模別の費用

組織の規模	平均コスト	中央値
従業員 100 ～ 250 人	1,125,562 ドル	375,000 ドル
従業員 251 ～ 500 人	1,978,043 ドル	750,000 ドル
従業員 501 ～ 1,000 人	1,009,205 ドル	375,000 ドル
従業員 1,001 ～ 3,000 人	1,907,594 ドル	750,000 ドル
従業員 3,001 ～ 5,000 人	2,452,929 ドル	750,000 ドル

アイデンティティ侵害を修復するために要した総コストはどの程度でしたか？母数：セキュリティ侵害を防ぐことができなかった組織。回答者数 =510。

アイデンティティセキュリティ対策の現状

本調査では、アイデンティティ管理における 5 つの主要な取り組みについて、組織がどの程度の頻度で実施しているかを調査しました。調査結果からは、ベストプラクティスと実態の間に大きな乖離が存在していることが明らかになりました。こうしたギャップが、アイデンティティ攻撃へのリスクを高めています。



以下のアイデンティティ管理活動をどのくらいの頻度で実施していますか？ 回答者数 =5,000

不審なログイン試行の監視は、リアルタイムで実施される取り組みとして最も一般的なもの (継続的に実施：24.1%) でした。しかし、それでも半数以上の組織 (50.6%) は、確認頻度が 3 か月に 1 回以下にとどまっています。侵害の要因として第 2 位となっていることを踏まえると重要な対策であるにもかかわらず、人間以外のアイデンティティのローテーションや監査を毎週以上の頻度で実施している組織は、わずか 34.3% にとどまっています。

アイデンティティガバナンスポリシーの見直しは、継続的に実施されている割合が最も低い取り組み (10.5%) でした。組織の 3 分の 1 (33.3%) は四半期に 1 回以下の頻度でしかポリシーを見直しておらず、22.6% は半年に 1 回のみ実施していると回答しています。アイデンティティ脅威が急速に進化している現状を踏まえると、年 1 回、半年に 1 回、あるいは四半期ごとの見直しでは、危険な空白期間が生じます。

エージェント型 AI：加速する NHI の問題

エージェント型 AI によって、NHI 管理の課題は大幅に深刻化しています。より多くのアイデンティティが、より速いペースで生成され、より広範なアクセス権を持つ一方で、人による監督は大幅に減少しているためです。NHI に関する主な課題には、以下が含まれます。

- **AI エージェントが NHI を自動的に増殖させる**
  すべての AI エージェントには、それぞれ専用のアイデンティティと認証情報が必要です。特に重要なのは、エージェントがサブタスクを実行するために新たなエージェントを自律的に生成できる点です。そのたびに新しい認証情報が作成されますが、人が関与または監督することはほとんどありません。
- **AI エージェントには、広範かつ継続的なアクセスが必要**
  AI エージェントは業務を遂行するために、カレンダー、データベース、CRM、ファイルストレージ、API など、多数のシステムにわたってアクセスする必要があります。人間のアカウントとは異なり、こうしたアクセス権は失効することがほとんどなく、監査も十分に行われていません。
- **AI エージェントは、従来の NHI よりも監視が困難**
  バックアップ用サービスアカウントは、毎晩同じ時間に同じタスクを実行するため、監視が容易です。一方、AI エージェントは自律的に判断を行い、24 時間 365 日稼働し、動作が予測できないため、異常が発生した際にそれを検知することが非常に困難になります。
- **サードパーティの AI エージェントには、未知のリスクがある**
  組織がサードパーティ AI エージェントの機能を利用する場合、そうしたエージェントが保持する認証情報やアクセス権限を事実上引き継ぐことになります。しかし、そのエージェントがどの程度安全に構築されているのか、また何にアクセス可能なのかについては、十分な可視性が得られないケースが少なくありません。
- **セキュリティルールは、AI エージェント向けに作られたものではない**
  多くのアイデンティティセキュリティフレームワークは、人間のユーザーと単純なマシンアカウントを前提として構築されています。しかし、自律的に認証情報を生成、委任、廃止できるエージェントは想定されておらず、その結果、ガバナンス上の大きなギャップが生じています。

エージェント型 AI は、NHI のセキュリティが CISO の最重要課題へと浮上した主要な要因の一つです。

不十分な人間以外のアイデンティティ管理がもたらす影響

前述のとおり、人間以外のアイデンティティ (NHI) 管理の不備は、成功した攻撃の 40.6% において根本原因となっていました。さらに詳しく見ると、侵害された NHI は、侵害発生時の金銭的被害を大幅に拡大させることが明らかになっています。

特に注目すべき点として、NHI 管理が不十分な組織では、平均と比較して、アカウントからの不正送金 による金銭的窃取が 27.9% と大幅に高く、恐喝（脅迫による金銭要求）も 24.4% 高い水準となっており、こうした攻撃に対して著しく脆弱であることが分かります。唯一の例外として、データ窃取とランサムウェアのカテゴリでは、NHI 管理が不十分な組織のほうが平均よりわずかに良好な結果となっていましたが、その差はごく小さいものにとどまっています。

結果	侵害されたすべての組織に占める割合	侵害された組織で人間以外のアイデンティティ管理が不十分であった割合	人間以外のアイデンティティ管理が不備だった場合との差異 (%)
データ窃取 – 攻撃者による機密データの盗み出し	48.8%	47.8%	-2.1%
ランサムウェア – ランサムウェア攻撃の実行を支援するために盗まれた認証情報が使用されたケース	48.4%	46.4%	-4.1%
恐喝 – 攻撃者が脅迫により金銭を要求したケース	43.9%	**54.6%**	**+24.4%**
破壊工作 — 攻撃者が認証情報を使用して組織に損害を与えたケース	30.0%	33.8%	+12.7%
金銭窃取 — 支払いの不正送金	28.0%	**35.8%**	**+27.9%**
金銭窃取 — アカウントから資金が盗まれたケース	25.5%	29.9%	+15.7
概要:金銭窃盗 (あらゆる形態)	**46.7%**	**57.0%**	**+22%**

このアイデンティティ侵害が組織にどのような影響をもたらしましたか？母数：セキュリティ侵害を防ぐことができなかった組織。回答者数 =510 (すべての侵害事例)、回答者数 =207 (NHI が関連していた侵害事例)

NHI の脆弱性がもたらす金銭的影響の増大を踏まえると、NHI 管理が不十分な組織では、アイデンティティ侵害からの復旧コストが全体的に顕著に高くなるのは当然の結果といえます。平均的な復旧費用と比較して、一般的なコストは約 15 万ドル高い水準となっています。

アイデンティティの侵害からの復旧にかかる平均費用

NHI の管理状態が不十分であることと、NHI 関連の侵害を経験する傾向との間には、明確な相関関係が見られます。全体では、組織の 3 分の 1 (34%) がサービスアカウントや NHI のローテーションや監査を継続的または毎週実施している一方で、NHI の侵害が原因で被害を受けた組織では、その割合は 4 分の 1 (24%) に低下しています。

まとめ

本調査の結果は、決して楽観視できない状況であることを示しています。過去 1 年間で、アイデンティティ関連の侵害は 10 組織中 7 組以上に影響を及ぼしており、被害を受けた企業あたりの平均発生件数は 3 件を超えています。これは理論上のリスクでも、特定の業界や地域に限定された問題でもありません。あらゆる規模、業界、地域の組織に影響を及ぼす、普遍的かつ広範に存在する脅威です。調査データは、アイデンティティ攻撃がランサムウェア、データ窃取、恐喝といった攻撃が組織に侵入する「入口」となっていることを示しています。ランサムウェア被害を受けた組織の 67% は、そのインシデントがアイデンティティ侵害に直接起因していることを特定しています。

アイデンティティ攻撃が成功した場合、その影響は深刻かつ多岐にわたります。侵害を受けた組織のほぼ半数がデータ窃取またはランサムウェア被害を経験しており、平均復旧コストは 164 万ドルに達することから、各インシデントは財務的に大きな影響を及ぼす重大な事象となっています。

根本原因は構造的な脆弱性を示しており、人為的ミス (42.7%)、人間以外のアイデンティティ管理の不備 (40.6%)、およびサードパーティアプリケーションの権限に対する可視性不足 (35.7%) はいずれも対処可能であるものの、継続的な投資と慎重な対応がなければ解決は困難です。小規模組織が大規模組織と比較して攻撃の検知に失敗する確率が約 2 倍に達しているという事実は、セキュリティコミュニティが対応すべき「サイバーセキュリティ格差」を浮き彫りにしています。

最も懸念すべき点は、アイデンティティセキュリティ対策の現状態です。不審なログイン活動を継続的に監視している組織は約 4 分の 1 にとどまり、人間以外のアイデンティティの認証情報を定期的にローテーションしている組織も 3 分の 1 未満にすぎません。これらは、まさに攻撃者が悪用できる重大な弱点となっています。

組織は、アイデンティティセキュリティを一度きりのプロジェクトではなく、継続的な運用として取り組む必要があります。この取り組みを継続する組織は、2025 年に顕在化した脅威、そして 2026 年以降も拡大し続ける脅威に対して、より強固な防御態勢を構築できるようになります。

ソフォスの提言

本調査が示すとおり、強固なアイデンティティセキュリティは、サイバーリスクを低減する効果的な戦略において不可欠です。アイデンティティ関連攻撃へのリスクを低減するために、組織は人間および人間以外のアイデンティティの両方に対して、多層防御の仕組みを構築する必要があります。継続的な改善プログラムの一環として、必要な対策から着手して、推奨される対策に順次取り組んでください。

必要な対策

人間のアイデンティティ

- すべてのユーザーアカウントに多要素認証 (MFA) を適用します。
- 特権操作と通常操作で、異なる認証情報を使用します。
- アカウントをロックアウトする仕組みとブルートフォース攻撃への対策を実装します。
- シングルサインオン (SSO) でアイデンティティ管理を一元化します。
- 最新のフィッシングや認証情報の窃取手法を反映したユーザー意識向上トレーニングを従業員に受講させます。

人間以外のアイデンティティ

- 人間以外のすべてのアイデンティティのインベントリを定期的に作成して分類します。
- 長期間有効なシークレットではなく、有効期限の短い認証情報を使用します。

人間と人間以外のアイデンティティ

- 最小権限アクセスを適用します。
- 認証情報を適切に保護して管理します。
- 利用されていないアイデンティティは速やかに無効化または削除します。
- 従業員によるリソースアクセスを監査して廃止する正式なオフボードプロセスを適用します。
- すべての認証アクティビティを記録および監視し、ログを少なくとも 30 日間保持します。

推奨される対策

人間のアイデンティティ

- 条件付きアクセスとリスクベースのポリシーを実装します。
- 主要な認証方法としてパスキーを導入します (ハードウェアまたはソフトウェア)。
- Security Assertion Markup Language (SAML) や、より新しい OpenID Connect (OIDC) など、広く普及しているアイデンティティプロトコルを使用して、アイデンティティをフェデレーションします。

人間以外のアイデンティティ

- 静的なシークレットではなくワークロードアイデンティティフェデレーションを使用します。
- NHI 向けのシークレット管理プラットフォームを大規模に採用します。
- サポートされているプラットフォーム (GitHub、GitLab) でシークレットのスキャンを有効にします。

人間と人間以外のアイデンティティ

- 特権アクセス管理 (PAM) ソリューションを導入します。
- ゼロトラストのセキュリティモデルを採用します。
- 定期的なアクセスレビューと権限の再認定を実施します。
- ITDR (Identity Threat Detection and Response) 機能を導入します。
- アイデンティティとロールごとにネットワークアクセスをセグメント化します。
- 本レポートで示したアイデンティティ関連インシデントに対応するために、アイデンティティインシデント対応プレイブックを 1 つ以上定義し、定期的にテストします。

詳細はこちら

「アイデンティティセキュリティのベストプラクティスガイド」を参照してください。

調査方法

本調査は、2026 年第 1 四半期にソフォスの委託を受けて Vanson Bourne が実施しました。17 か国の 5,000 人の IT およびサイバーセキュリティ意思決定者にインタビューが行われました。対象となった国は、米国、ブラジル、チリ、コロンビア、メキシコ、英国、フランス、ドイツ、イタリア、スペイン、スイス、オーストラリア、インド、日本、シンガポール、南アフリカ、およびアラブ首長国連邦です。回答者は、15 の業界にわたる従業員 100 ～ 5,000 人規模の組織から構成されています。

SOPHOS

アイデンティティセキュリティに関するニーズや、ソフォスの支援についてご相談は、ソフォスの Web サイトにアクセスいただくか、当社のアドバイザーまでお問い合わせください。

ソフォス株式会社営業部
Email: sales@sophos.co.jp

2026-05-08 JA (TA) CRE-5312