
KEEPER®

# アイデンティティ、AI、ゼロトラスト

## Infosecurity Europe、Black Hat USA、it-saからのサイバーセキュリティの視点

2025年グローバルセキュリティイベント調査

# 調査概要

Keeper Securityは2025年、ロンドンの「Infosecurity Europe」、ラスベガスの「Black Hat USA」、ニュルンベルクの「it-sa」という世界を代表する3つのセキュリティイベントで、370人を超えるサイバーセキュリティ専門家を対象に調査を実施しました。地理的条件や法規制、企業規模に違いはあるものの、調査結果から見えてきたのは共通した現実です。「アイデンティティが新たな境界線になっている」ということです。

欧州から北米にかけて、アイデンティティはサイバーセキュリティの最前線となっています。企業がハイブリッド環境やマルチクラウド、AIを活用した業務へと拡張する中で、デジタルアイデンティティの数は急増しています。人間のユーザーだけでなく、デバイスやサービスアカウントも1つひとつが侵入口となり得ます。特に、管理されていない認証情報の存在はリスクを高め、非人間IDの数の増加がその脅威を加速させています。

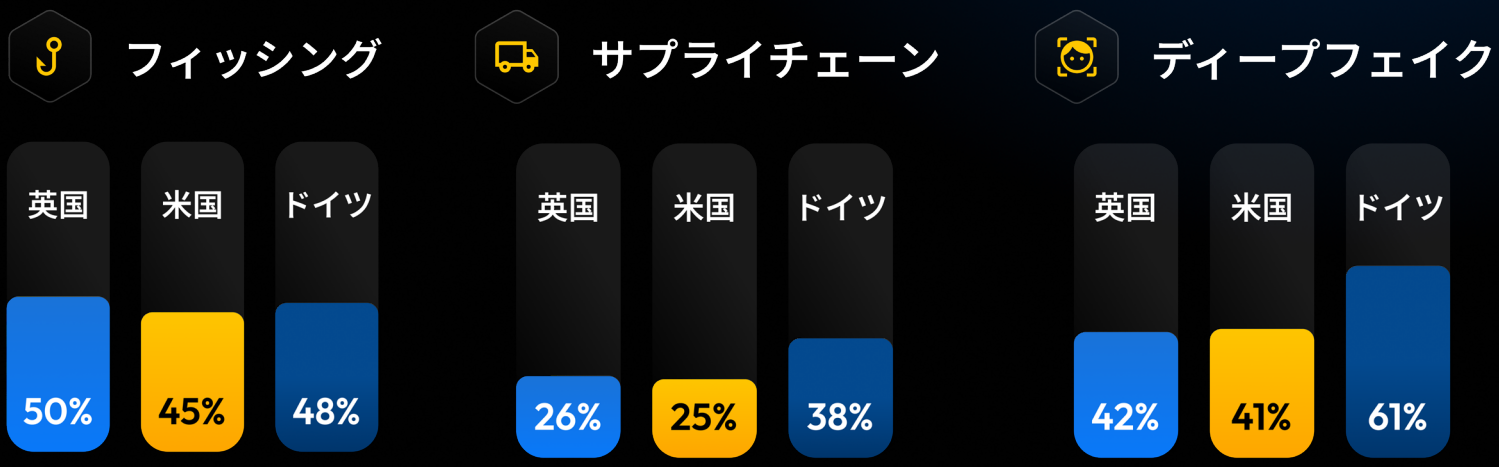
AIは、攻撃者と防御側の双方にとって戦いの構図を変えつつあります。攻撃者はフィッシングやディープフェイク、ランサムウェア、権限昇格を自動化し、防御側はAIを活用して本人確認や行動分析を強化し、不審な動きを検知しています。この進化のスピードは加速しており、組織は迅速な適応が求められています。

セキュリティリーダーたちは、進むべき道を理解しています。特権アクセス管理を強化し、認証基盤を近代化し、ゼロトラストを「戦略」から「実践」へ移すことです。しかし現実には、システムの複雑さや優先順位の競合、経営層の足並みの乱れなどにより、取り組みが停滞しています。この「認識と実行のギャップ」を攻撃者は巧みに突いています。

アイデンティティを中心とした防御の考え方は広く浸透していますが、実装の成熟度には地域差があります。このギャップをどう埋めるかが、現代の脅威に耐えうる組織を左右する分かれ道となります。

## 地域別の主なアイデンティティ関連脅威




# アイデンティティは主要な攻撃経路に

アイデンティティを悪用した脅威は、他のあらゆるサイバーリスクを上回り、すべての地域で最も一般的なセキュリティインシデントの原因となっています。フィッシング、認証情報の窃取、ディープフェイク、権限の不正利用は、今後12か月の間に大規模な侵害を引き起こす可能性が最も高い要因として、ランサムウェアを上回る位置づけとなりました。

Infosecurity Europeでは、回答者の50%が最も重大なアイデンティティ関連の脅威としてフィッシングを挙げ、42%がディープフェイク、26%がサプライチェーン攻撃を挙げました。米国でも結果はほぼ同様で、45%が主な懸念としてフィッシングを、41%がディープフェイクを、25%がサプライチェーン攻撃を指摘しています。ドイツではAIを活用した偽装への懸念がさらに高く、61%がディープフェイクを最大の脅威とし、48%がフィッシング、38%がサプライチェーン攻撃を挙げました。

これらの結果は、サイバーセキュリティにおいて「アイデンティティが共通の脆弱点になっている」という認識が広がっていることを示しています。攻撃者はネットワークではなくユーザーを狙い、認証やアクセス制御の弱点を突いて侵入しています。多要素認証 (MFA) の適用が一貫していないこと、アイデンティティ管理ツールの分断、特権認証情報の可視性不足といった課題が、依然として攻撃の余地を生んでいます。

このデータは、セキュリティのモダナイゼーションが急務であることを浮き彫りにしています。旧来型の認証と不完全なアイデンティティ・ガバナンスが、企業を長年にわたり同様の脅威にさらし続けています。ネットワーク境界がアイデンティティへと置き換わる現在、効果的な防御には、統合的な制御、集中管理された可視性、そしてリアルタイム監視と異常検知を備えた強固な認証が不可欠です。

# AIは「両刃の剣」

AIは、防御の在り方を大きく変える可能性を持つ一方で、急速に拡大する新たな脅威にもなっています。3つの地域すべてで、AIを活用した攻撃への対応に自信を持つ組織は少数にとどまりました。英国では12%、米国では16%の回答者が「自社はAIによる高度な脅威に十分対応できる」と答えました。ドイツでは28%が「準備ができている」と回答したものの、およそ3分の1は「ある程度の自信しかない」としています。

こうした懸念がある一方で、防御面におけるAIの可能性には強い期待が寄せられています。すべての地域で回答者は、今後3〜5年の間にアイデンティティおよびアクセスセキュリティを最も大きく変革する技術として「AIを活用した本人確認と認証」を挙げました。英国では53%、米国では57%、ドイツでは60%がこの技術を最も影響力のある革新と評価しています。一方で、パスワードレス認証、自動化されたアイデンティティ管理、量子耐性暗号化といったその他の新技術は、それに比べて低い評価にとどまりました。

AIは、攻撃と防御の双方の手法を同時に塗り替えています。攻撃者はAIを活用して、より巧妙なフィッシング攻撃やディープフェイク、認証情報の不正利用を仕掛ける一方、防御側はAIを導入して異常検知や本人確認、悪意のある行動の予測をリアルタイムで行っています。アイデンティティ管理やアクセス制御の枠組みにAIを効果的に組み込んだ組織は、防御力と可視性を高めることができます。逆に導入をためらう組織は、自動化とスピードが支配する脅威環境の中で取り残されるリスクを抱えることになります。

## AIを活用した脅威への対応に対する自信


十分に自信がある
英国

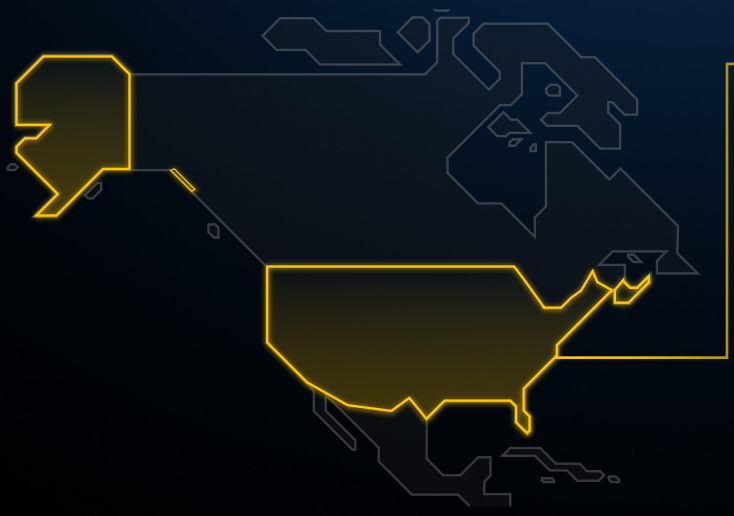

十分に自信がある
米国


十分に自信がある
ドイツ



# 今後3〜5年でアイデンティティセキュリティを変革すると予想される技術



## 米国

**57%** AIを活用した本人確認と認証

**26%** 自動化されたアイデンティティ管理

**38%** パスワードレス認証

**28%** 量子耐性暗号化

## 英国

**53%** AIを活用した本人確認と認証

**30%** 自動化されたアイデンティティ管理

**39%** パスワードレス認証

**24%** 量子耐性暗号化

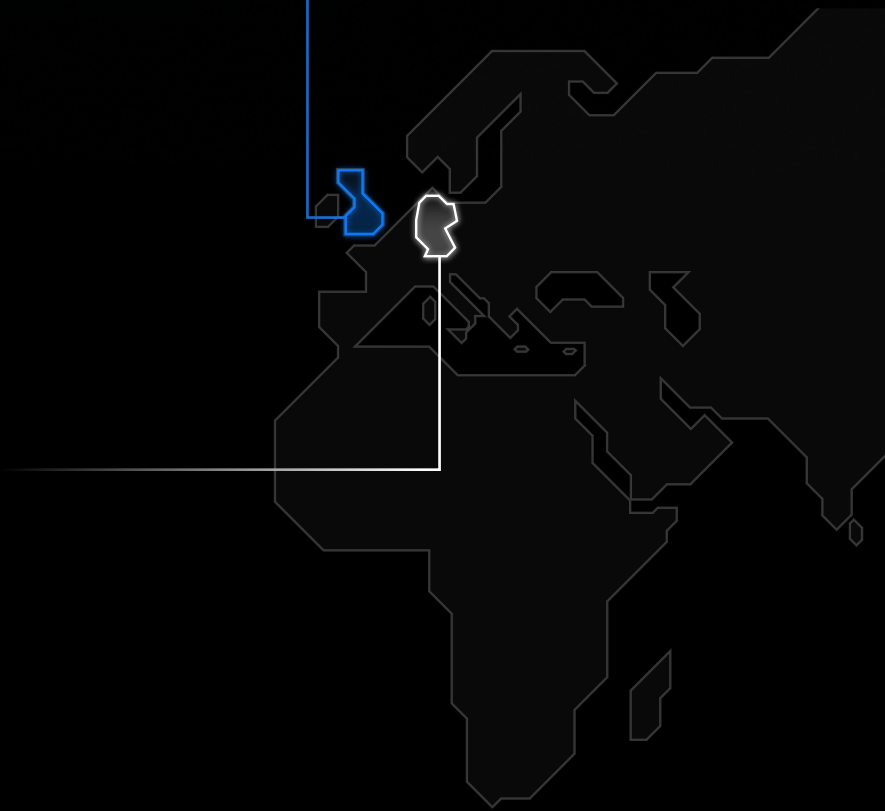
## ドイツ

**60%** AIを活用した本人確認と認証

**30%** 自動化されたアイデンティティ管理

**28%** パスワードレス認証

**18%** 量子耐性暗号化



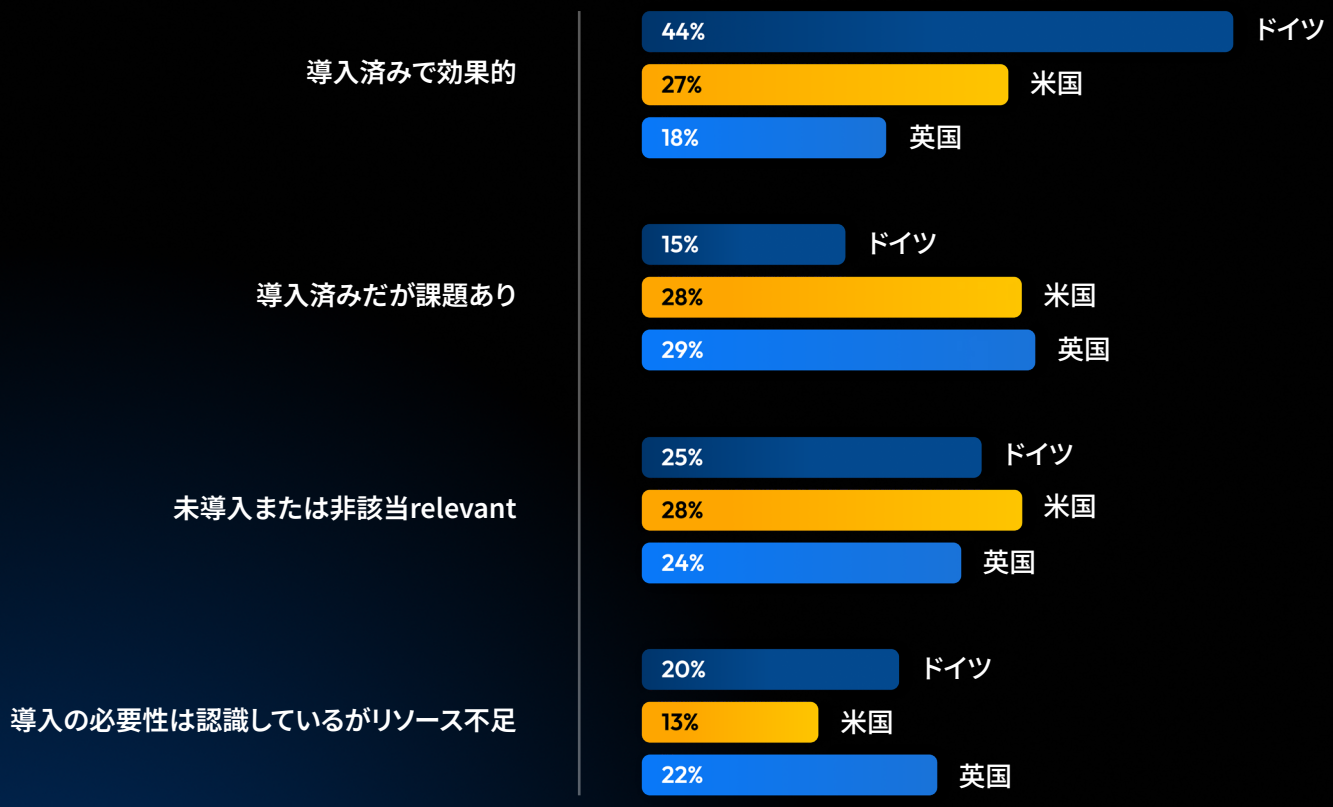
# ゼロトラストの理想と現実

ゼロトラストは現代のサイバーセキュリティにおいて欠かせない考え方となっていますが、導入の進展は依然として遅れています。Infosecurity Europeでは、ゼロトラストモデルを効果的に完全導入していると回答した割合はわずか18%にとどまりました。Black Hat USAではやや高く27%、ドイツのit-saでは44%が「効果的に導入している」と回答しており、英国の2倍以上という結果になりました。

**ドイツの組織の3分の1以上が、ゼロトラスト実現における最大の障壁として、経営陣の支援不足を挙げています**

進展を妨げる要因は、各地域で共通しています。英国では、31%が「予算や人員の制約」を最大の障壁に挙げ、次いで29%が「経営層の理解不足」を指摘しました。米国では、30%が「導入の複雑さ」を最大の課題とし、27%が「レガシーシステムとの統合の難しさ」を挙げています。ドイツでは、34%が「経営層の支援不足」を最大の課題とし、32%が「予算の制約が続いている」と回答しました。

すべての地域で、ゼロトラストは戦略上不可欠な方針として広く受け入れられていますが、実践面での成熟度にはばらつきがあります。多くの組織が、コストやシステムの複雑さ、社内の足並みの調整に苦慮しながら、最新のフレームワークをレガシーシステムと統合しようとしています。その結果、ゼロトラストは依然として「理想として掲げられている段階」にとどまり、十分に実現されているとは言えません。



# 特権アクセス管理の運用における不徹底

3つの市場全体で、10社中4社が一貫した多要素認証の適用または包括的な特権アクセス管理の導入を欠いています。このデータは明確な事実を裏付けています。組織はPAMの重要性を認識していながらも、依然として十分な投資と優先順位付けが行われていません。継続的な監視と自動化がなければ、「最小権限アクセス」は依然として目標にとどまり、確実な管理体制にはなり得ません。

## 英国

**43%**
特権アカウントに多要素認証が未適用

**37%**
PAMソリューション未導入

**34%**
不要になった特権が削除されない

## 米国

**40%**
特権アカウントに多要素認証が未適用

**33%**
PAMソリューション未導入

**34%**
不要になった特権が削除されない

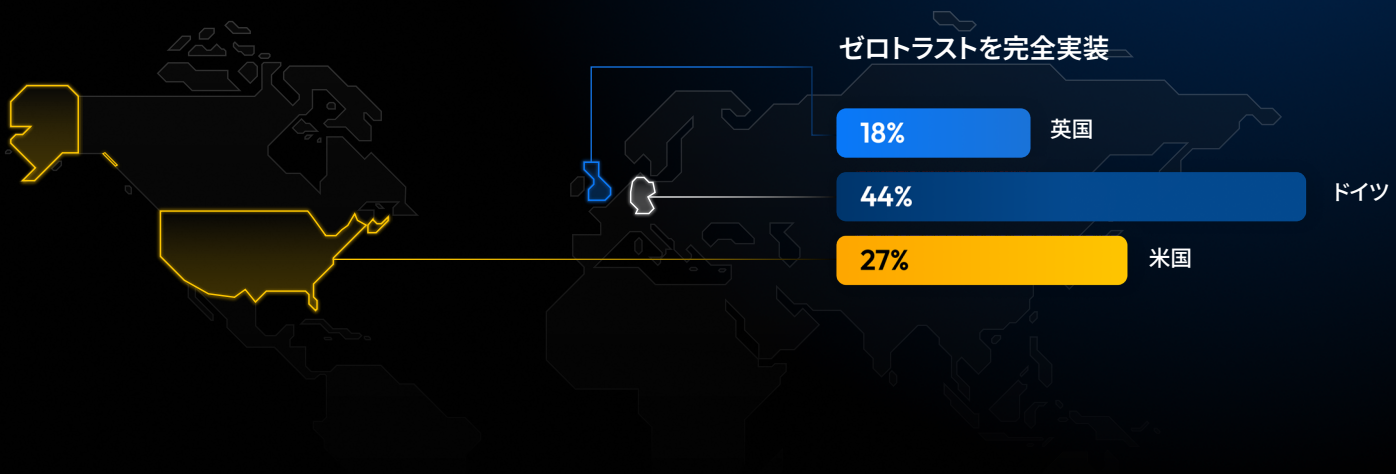
## ドイツ

**49%**
PAMソリューション未導入

**41%**
監視や監査の欠如

**33%**
第三者の審査が不十分




# 地域別の考察

## 英国: Infosecurity Europe

Infosecurity Europeの回答者は、アイデンティティ関連のリスクに対する認識は高いものの、十分な対応体制は整っていません。ゼロトラストを効果的に実施していると回答したのはわずか18%、AIによる脅威への対応に自信があると答えたのは12%にとどまりました。50%が主な懸念としてフィッシングを挙げる一方で、半数以上は「メディアがAI脅威の深刻さを誇張している」と感じています。この認識と準備のギャップから、英国の多くの組織は高い意識を持ちながらも、戦略を実際の行動に結びつけられていないことがうかがえます。

## 米国: Black Hat USA

Black Hat USAのサイバーセキュリティ専門家は、ゼロトラスト導入に一定の進展が見られるものの、依然として同様の課題に直面していると報告しました。回答者の27%が「ゼロトラストを完全に導入している」と答えた一方で、40%が「特権アカウントに多要素認証を一貫して適用していない」と認めています。主なアイデンティティ関連の脅威は引き続きフィッシング (45%) とディープフェイク (41%) であり、AIを活用した脅威への理解が進んでいるにもかかわらず、多くの米国組織はハイブリッド環境全体で防御を実運用に落とし込むことに苦労しています。

## ドイツ: it-sa

it-saの回答者は、ゼロトラストの成熟度に対する自信が高く、防御面でのAI活用にもより前向きな姿勢を示しました。44%が「ゼロトラストを効果的に実施している」と答え、60%が「今後3〜5年で最も大きな変革をもたらすセキュリティ技術はAIを活用した本人確認である」と考えています。一方で、34%が「経営層の支援不足」を最大の課題に挙げ、32%が「予算の制約が続いている」と回答しました。さらに、約半数 (49%) の組織が専用のPAMソリューションを導入していません。ドイツでは、アイデンティティ重視の戦略的方向性は明確である一方、運用面での実行力にはばらつきが見られます。

> **「アイデンティティはサイバーセキュリティの中核的な制御点となりました。ゼロトラストとPAMの導入を先導する組織は、アクセスを守るだけでなく、AI時代における安全で拡張性のある成長の基盤を築いています。」**
>
> **ダレン・グッチョーネ**
> **Keeper Security CEO兼共同創業者**

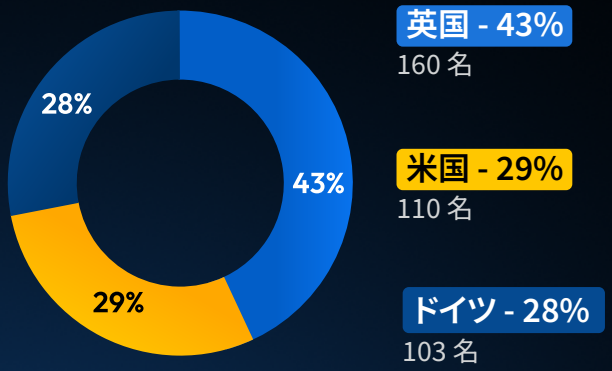
# Keeper Securityの見解

現代のサイバーセキュリティは、アイデンティティ管理、特権アクセス管理、そしてインテリジェントな自動化という3つの要素の融合によって成り立っています。これらの要素が、絶えず変化する脅威環境の中で、組織がユーザー・データ・インフラをどのように守るかという在り方を再定義しています。

ゼロトラストと特権アクセス管理は、もはや選択肢ではありません。これらは、現代の企業において事業の継続性、統制、拡張性を支える基盤となる枠組みです。方針を掲げるだけでなく実際の運用へと移行することで、組織は防御力を強化するだけでなく、サイバーセキュリティの新たな国際的標準を築くことができます。

ロンドン、ラスベガス、ニュルンベルクで得られた知見が示す結論は明確です。「アイデンティティこそが新たな境界線である」ということです。真のレジリエンス (強靭性) は、統制の取れた実行、継続的な評価、そして防御のあらゆる層におけるAIの責任ある活用によって支えられます。アイデンティティを保護し、最小権限を徹底し、インテリジェントな自動化を積極的に取り入れる組織は、今日の脅威に耐えるだけでなく、サイバーセキュリティの未来そのものを形づくる存在となるでしょう。

## 調査方法




Keeper Securityは、ロンドンのInfosecurity Europe、ラスベガスのBlack Hat USA、ニュルンベルクのit-saにおいて匿名で実施した対面アンケートを通じて、サイバーセキュリティおよびIT分野の専門家373名から回答を得ました。