TrendAI™ Research

TrendAI™ 2026 サイバーリスクレポート

目次

2025年版サイバーリスクレポートの調査結果を土台として、TrendAI™ Research は、進化し続ける脅威情勢に組織が先手を打つために必要なデータを提供できるよう、世界中の企業環境にわたるリスクの動向を継続的に追跡しています。

このプロアクティブなアプローチを実現するため、本レポートでは TrendAI Vision One™ Cyber Risk Exposure Management（CREM）ソリューションのデータを活用しています。CREM は、アタックサーフェス全体のリスクを評価し、優先順位を付け、適切な対策を実施することで、組織のデジタル資産を保護します。

CREM の中核をなすのがサイバーリスクインデックス（CRI）です。CRI は、個々の資産スコアとリスク要因スコアを統合し、組織全体のセキュリティリスクを定量化する指標です。当社の調査では、CRI が平均を上回る組織は、平均を下回る組織よりも攻撃を受ける可能性が高いことが分かっています。CREM は、各資産の攻撃エクスポージャーとセキュリティ設定を資産の重要度と掛け合わせてこの指標を算出し、0〜100のスコアを次の3つのリスクレベルに区分します。

- 低リスク（0〜30）：比較的安全な状態とみなされ、通常は即時の対応を必要としません。
- 中リスク（31〜69）：複数のリスク要因への対処が必要であり、対策を実施すべき段階です。
- 高リスク（70〜100）：深刻なエクスポージャー（リスクにさらされている領域）に直面しており、迅速かつ強固なセキュリティ対策が不可欠です。

リスクベースのアプローチは、企業のセキュリティ体制を改善するうえで当社が最も重視する指針であり続けています。エクスポージャーがどこに集中しているか、攻撃者がそれをどのように悪用するか、防御側がどれだけ迅速に対応できるかを理解することで、組織は事後対応的な防御からプロアクティブなレジリエンス（回復力）へと移行できます。

1

本レポートのデータについて

本年のレポートでは、TrendAI Vision One™ の Attack Path Prediction（攻撃経路予測）機能のテレメトリから得られた新しいデータセットを導入し、年次分析の柱であるサイバーリスクインデックスのスコアとイベント検出を、将来予測の観点から補完しています。CRI が組織のリスク体制の現在の状態を測定するのに対し、Attack Path Prediction は、攻撃者がその環境内で現実にたどり得る経路をマッピングし、露出した侵入起点、アクティブなリスクイベント、脆弱な標的資産を、起点から終点までの一連の攻撃シーケンスとして結び付けます。予測された経路が悪用される前に可視化することで、このデータセットは分析の枠組みをエクスポージャーの測定から攻撃者視点のシミュレーションへと移し、攻撃者の動き方に基づいてどのリスクから対処すべきかを判断する具体的な根拠をセキュリティチームに提供します。

本レポートは、前回のサイバーリスクレポートを土台とした移行期のレポートであり、主として2025年のテレメトリに基づいています。特に断りのない限り、調査結果は同年のデータによるものです。通年データがまだ揃っていない領域では、入手可能な最新のデータセットのスナップショットを用いているセクションもあります。これらは完全な年間測定ではなく、傾向を示す知見を提供することを意図したものです。

2026年のテレメトリが蓄積されるのに伴い、2027年版レポートでは、ここで示したリスク、検出、脆弱性、攻撃経路に関する基礎的な分析の上に、AI関連のリスクおよび脅威のデータセットをさらに拡充していく予定です。

本レポートは、TrendAI Vision One™ プラットフォームを利用する組織のテレメトリと、TrendAI™ の脅威インテリジェンスに基づいています。本レポートの数値は、特定の業界・地域や脅威情勢全体を統計的に代表するサンプルではなく、当社の顧客基盤における観測結果を反映したものであり、傾向を示すシグナルとして提示しています。また、指標が変動あるいは乖離する理由に関する説明は、統計的に検証された因果関係ではなく、アナリストの知見に基づく判断を反映したものです。これらの知見は、リスクの認知と優先順位付けを支援することを目的としており、個々の組織のベンチマークや、コンプライアンス・法務・投資に関する意思決定への利用を意図したものではありません。情報は公開時点のものであり、現状のまま提供されます。

2

リスクデータ

2025年のサイバーリスクインデックス全体平均

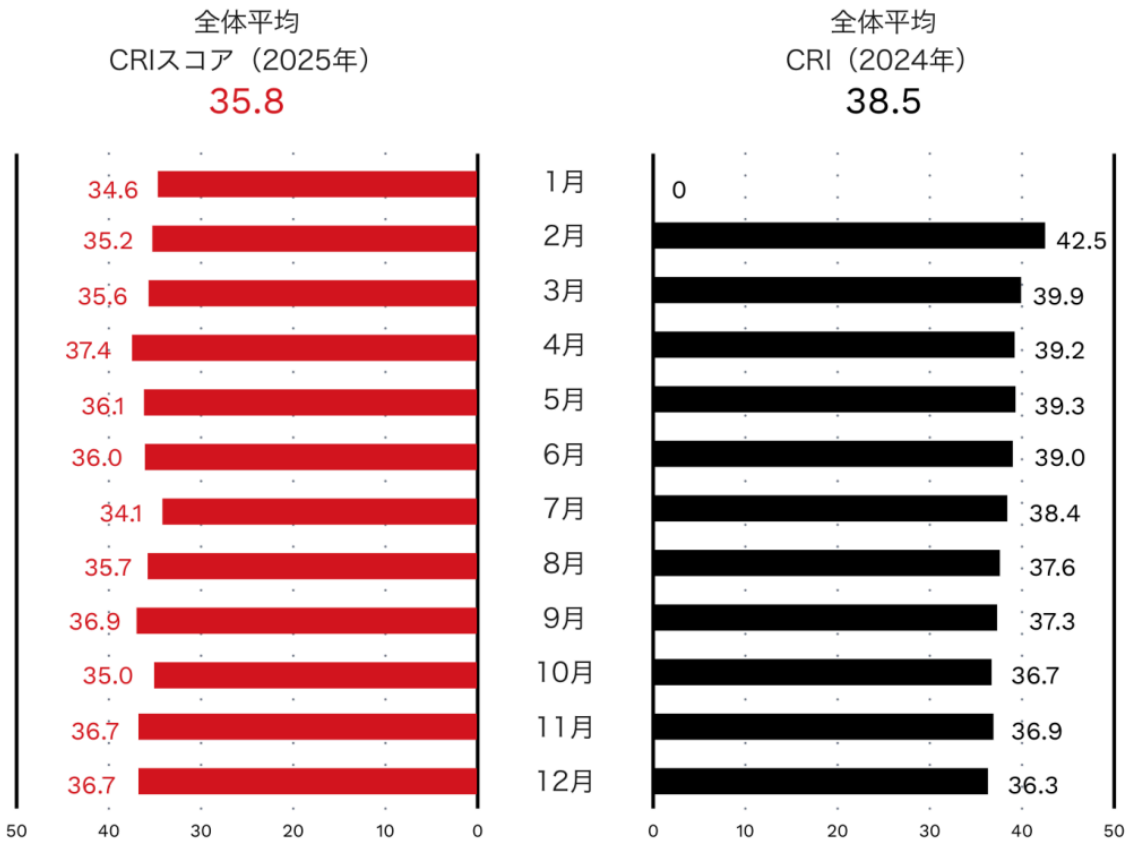


図1. 2024年と2025年のサイバーリスクインデックスの年間平均および月別内訳の比較。数値は小数第1位に丸めています。

（注：2024年1月のデータが存在しないのは、同月末にダッシュボードのアルゴリズムが、CRI の算出に影響する重み合算方式へ更新されたためです。）

2025年の年間平均 CRI は35.8となり、2024年の平均38.5（2024年2月～12月）から大きく改善しました。これは2024年を通じて見られた低下（改善）傾向の継続であり、企業がサイバーリスク管理の運用定着をさらに進めていることを示唆しています。ただし、35.8という値は依然として中リスク帯に位置している点に注意が必要です。

2025年の月次推移は、2024年の着実な低下と比べると変動が見られます。1月は34.6と比較的低い水準で始まり、4月に最高値の37.4まで急上昇した後、7月には最低値の34.1まで下がり、その後再び上昇して11月と12月はいずれも36.7で落ち着きました。

こうした上下動を繰り返すパターンは、42.5から36.3までほぼ一貫して前月比で改善した2024年とは対照的です。組織は基礎的な体制こそ改善したものの、継続的な改善の維持には苦戦している可能性があり、季節的なリソース制約や、プロアクティブではなく事後対応的なリスク管理サイクルを反映しているとも考えられます。

4月の急上昇は特に注目に値します。多くの組織で新しい会計年度・予算年度が始まる時期にあたり、新規プロジェクトやクラウド展開が、管理策の整備が追いつく前に新たなリスクを持ち込んでいる可能性があります。

テレメトリ対象のすべての組織が、規模や業種を問わず依然として中リスク帯に位置しています。前進は確かですが、取り組みはまだ道半ばです。

平均CRIが高い上位10業種

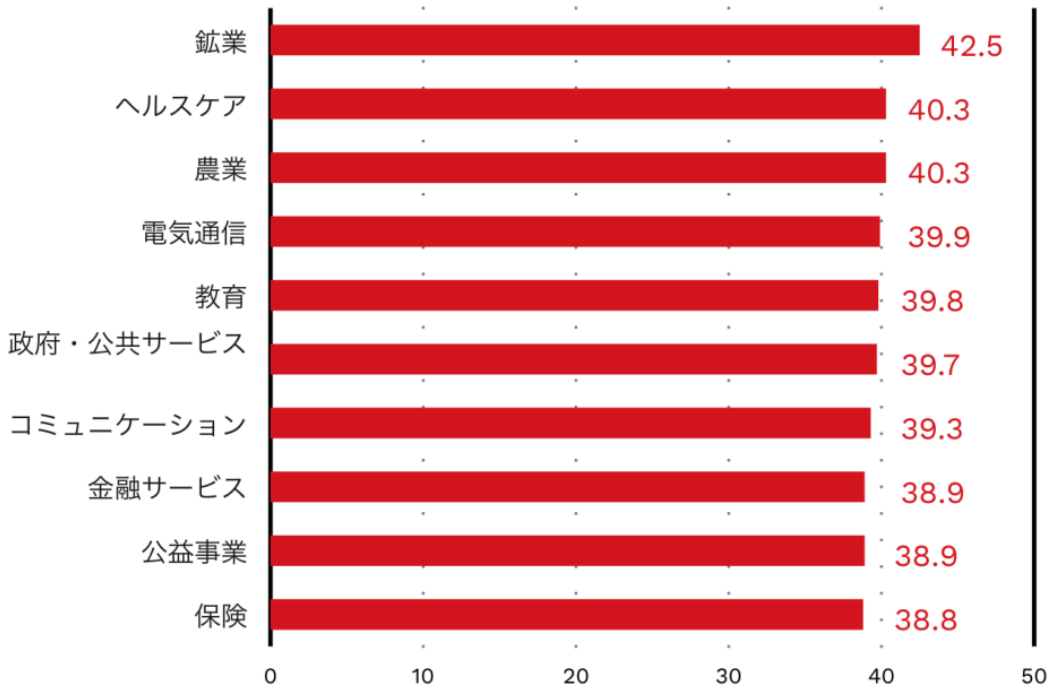


図2. 2025年（1月〜12月）の年間平均CRIが高い上位10業種。数値は小数第1位に丸めており、順位は丸める前の数値に基づきます。

2025年のテレメトリでは、2024年から業種ランキングの入れ替わりが見られます。本セクションでは、上位業種ごとの CRI と、そのスコアに寄与したと考えられる要因を見ていきます。

鉱業が2025年に初めてリスクランキングの首位に立ちました。昨年の上位10業種に入っていなかったこの業種が、現在では全業種の中で最も高い平均CRIを記録しています。

鉱業がリスクランキングの最上位に浮上した背景には、加速するデジタルトランスフォーメーションと、歴史的に整備が遅れてきたセキュリティ基盤の組み合わせがあるとみられます。鉱業の現場では、地理的に分散した拠点にコネクテッドセンサー、自律走行車両、遠隔監視システムの導入が進んでおり、アタックサーフェスが急速に拡大しています。

同時に、この業種のリスクイベントの筆頭がクラウドアプリへのアクセスではなくメール経由の脅威であることは、ユーザ教育やメールフィルタリングといった基本的なセキュリティ衛生が、OT（オペレーショナルテクノロジー）の導入ペースに追いついていない可能性を示しています。インターネット接続を想定せ

ずに設計されたレガシー OT システムが次々とネットワークに接続され、業務を止めずにパッチを適用することが難しい脆弱性を生み出しています。

ヘルスケアは2年連続でトップ3にとどまっています。複雑なデバイス群、遅いパッチ適用サイクル、解消されないアイデンティティ管理の不備がリスクを押し上げています。

ヘルスケア業界の CRI が高止まりしているのは、短期間では解決の難しい構造的な課題を反映しています。この業種は、医用画像機器から患者モニタリングシステムまで、きわめて多様でレガシーなデバイス群を管理しており、その多くは、規制当局の承認なしには、あるいは患者ケアの継続性を危険にさらすことなしには容易にパッチを適用できない古いソフトウェアで稼働しています。

2024年のパッチ適用平均時間（MTTP）のデータでは、ヘルスケアは41.5日と最もパッチ適用が遅い業界であり、この課題を裏付けています。設定不備イベントの最上位は Device Control 設定であり、数千台規模のコネクテッドエンドポイントを統制する難しさと整合しています。リスクイベントの最上位は Risky Cloud App Access（リスクの高いクラウドアプリへのアクセス）であり、クラウドベースのツールの導入が、それを保護するためのガバナンスの枠組みを上回るペースで進んでいる状況を反映しているとみられます。

農業のリスクプロファイルは、技術面の変革と切り離せません。業務効率を牽引している IoT（モノのインターネット）デバイスや自動化された機械類そのものが、セキュリティ管理策の整備が追いつかない速さでアタックサーフェスを拡大させています。

農業の CRI が高止まりしているのは、セキュリティ成熟度の向上を上回るペースで進む同業種のデジタルトランスフォーメーションを反映しています。精密農業技術、コネクテッド灌漑システム、自動収穫機、サプライチェーン管理プラットフォームの導入により、アタックサーフェスは短期間で劇的に拡大しました。設定不備イベントの最上位は Device Control 設定であり、この IoT の普及と整合しています。

リスクイベントには、メールとクラウドアプリに関する2つの Data Loss Prevention（情報漏洩対策）イベントが目立って現れており、業務やサプライチェーンに関わる機密データが十分な統制なしに送信されている可能性を示唆しています。このリスクは、サードパーティのベンダやサービスプロバイダへの依存度が高いという同業種の特性によってさらに増幅されます。これらの事業者が新たな脆弱性を持ち込む可能性もあるためです。

電気通信は2025年に初めて上位5業種に入りました。リスクの高いクラウドアプリへのアクセスと長期間未使用のアイデンティティアカウントが主要なリスク要因であり、これは企業全般に共通する課題ですが、重要インフラを担うこの業種では影響がより深刻になります。

電気通信の組織は、クラウドネイティブアーキテクチャへの移行、5Gネットワークの展開、ソフトウェア定義型インフラの拡大という大規模なインフラ変革の只中にあります。この転換は必然的に、セキュリティ管理策の確立が追いつかない速さで新たなリスク経路を持ち込みます。

設定不備イベントの最上位が Suspicious Connection Service 設定であることは、ネットワーク接続の管理を本業とする業種だけに特に注目されます。ネットワークに最も精通しているはずの組織でさえ、大規模環境で最適なセキュリティ設定を維持することに苦戦していることを示唆しています。大規模で複雑なユーザディレクトリと急速なインフラ変化が重なることで、長期間未使用のアカウントの管理は根強い課題であり続けています。

教育は全業種の中で最も大きな改善を記録し、2024年初頭の四半期ピーク値45.1から2025年には39.8まで低下しました。改善は確かなものですが、リスクイベントの上位を依然として長期間未使用のアカウントと脆弱な認証ポリシーが占めており、この業種のアイデンティティ管理の課題は未解決のままです。

教育の改善は、規制圧力の高まり、同業種で相次いだ著名な侵害事案による意識向上、そして2024年版レポートの調査結果を受けた集中的な修復の取り組みの成果とみられます。しかし、残されたリスクの要因は構造的なものである可能性が高いと考えられます。教育機関は、学生・教員・職員が定期的に入れ替わる、きわめて大規模で流動的なユーザ集団を管理しており、アカウントのライフサイクル管理は本質的に他の多くの業種より複雑になります。

特に公的機関では予算の制約により、自動化されたアイデンティティガバナンスツールへの投資が限られます。さらに、個人所有デバイスが学内ネットワークに接続されることが多いためエンドポイント管理は一層複雑になっており、設定不備一覧の最上位を Non-Optimized Security Agent Password Unlock 設定が占めていることの説明にもなり得ます。

政府・公共サービスの組織の CRI は2025年に39.7となり、昨年の40.3からわずかに改善しました。攻撃が成功した場合の影響が業務の中断にとどまらず、公共の安全や国家安全保障にまで及ぶことを踏まえると、この業種はより急なカーブで CRI を引き下げていく必要があります。

一方、コミュニケーション業界は2024年の平均41.6から2025年には39.3へと改善し、上位10業種の中でも前年比の改善幅が大きい業種の一つとなりました。ただし、リスクイベントの中心は依然としてメール経由の脅威と情報漏洩インシデントが占めています。

金融サービスの組織の CRI は2025年に38.9となり、2024年からの緩やかな改善が続いています。多要素認証（MFA）が無効化されたアカウントが主要リスクイベントに含まれており、最も規制が厳しくセキュリティ意識の高い業種であっても、基礎的なアイデンティティ衛生の不備と無縁ではないことを示しています。

公益事業は2025年に初めて上位10業種に入りました。IT と OT の融合が、従来のセキュリティの枠組みでは想定されていなかった新たなアタックサーフェスを生み出している業種です。

保険は CRI 38.8で上位10業種の最後に位置し、2024年の41.0から低下しました。MFA が無効化されたアカウントと Risky Cloud App Access が主要リスクイベントとして残り続けているほか、他に類を見ないほど多様化したマルチクラウド環境がガバナンスの複雑さをもたらし、修復の遅れにつながっている可能性があります。他業種で一般的な Amazon Web Services（AWS）と Microsoft Azure に加えて Google

Cloud Platform（GCP）を利用していることが、その複雑さに拍車をかけています。リスクのコストを把握することと、その削減を大規模に運用定着させることは、依然としてまったく別の課題です。

企業規模別の平均CRI

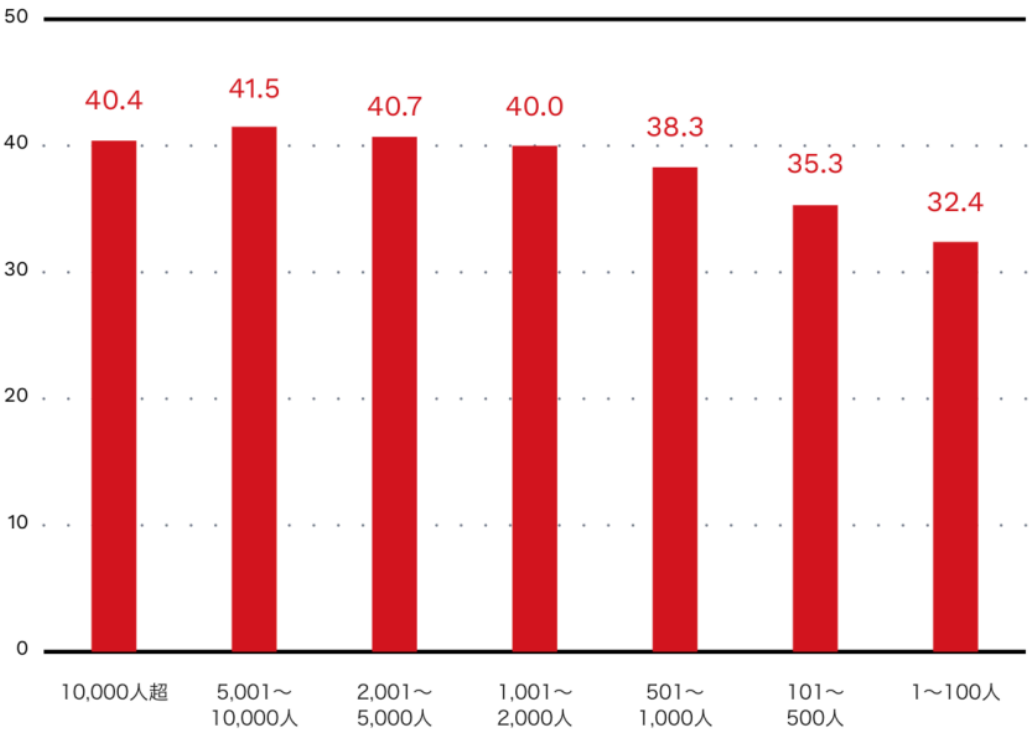


図3. 2025年（1月～12月）の従業員数別に見た組織規模ごとの年間平均リスクスコアの内訳。数値は小数第1位に丸めています。

小規模組織（従業員100人以下）は全体として最もリスクの低い層であり続けていますが、2025年に CRI が前年比で上昇した唯一の規模セグメントとなりました。この上昇は、より大きなサプライチェーンへの入口として中小企業への攻撃者の関心が高まっていることに加え、拡大する脅威情勢に対応するための専任セキュリティリソースが限られていることを反映しているとみられます。少人数の IT チームがセキュリティを兼務で管理していることが多いため、攻撃者の関心がわずかに高まるだけでもリスクは大きく増加し得ます。

従業員501～1,000人の組織は着実な改善を示しているとみられます。これは、エンタープライズ級の機能を手の届く範囲にもたらすマネージドセキュリティサービスやプラットフォーム型セキュリティツールの導入拡大を反映していると考えられます。ただし、このセグメントも38.3と中リスク帯に位置しています。

従業員1,001～2,000人の組織は2024年から2.3ポイント低下と、2025年の中でも大きな改善を記録しました。この規模の組織は通常、専任セキュリティチームの設置やエンタープライズセキュリティプラットフォームの体系的な導入が進む、成熟度の節目にあります。改善は、こうした投資が測定可能な成果を生み始めたことを反映しているとみられますが、拡大するユーザ基盤とハイブリッドインフラの管理の複雑さにより、リスクはより小規模な組織と比べて高い水準にとどまっています。

従業員2,001〜5,000人の組織は3.2ポイントの改善を示しました。この規模の組織には通常、セキュリティオペレーションセンター（SOC）や専任のリスク管理部門が設置されています。改善は、こうしたチームがより成熟した脆弱性管理・アイデンティティガバナンスのプログラムを運用に定着させつつあることを反映しているとみられます。残る40.7というリスクは、大規模で分散した従業員とマルチクラウド環境を管理することに内在する複雑さを映し出しています。

一方、従業員5,001〜10,000人のエンタープライズは2.5ポイントの堅調な改善を示したものの、2025年の規模別セグメントの中で最も高い CRI を記録しました。この規模の組織は、最大規模のエンタープライズに匹敵するネットワークの複雑さを抱えながら、従業員10,000人超の組織が持つセキュリティ運用の成熟度、ツールへの投資、人員の厚みをまだ備えていない場合があります。これは独特の脆弱性プロファイルを生んでおり、この層のセキュリティリーダーは特に注意を払う必要があります。

最大規模のエンタープライズは2024年から3.8ポイント低下と、全規模帯の中で最も大きな改善を記録しました。これは、専任 SOC、自動化された対応プレイブック、複雑な環境全体のリスク管理を一元化する TrendAI Vision One™ のようなプラットフォームへの大規模な投資といった、エンタープライズセキュリティプログラムのスケールメリットを反映しているとみられます。しかし、40.4という値が示すとおり、最大規模の組織は依然としてより小規模な組織に比べて高いリスクを抱えており、投資水準にかかわらず、エンタープライズ規模では複雑さこそが最大の課題であり続けることを物語っています。資産、ユーザ、サードパーティ連携の膨大な数を踏まえると、わずかな改善であっても、複雑な作業を簡素化するプラットフォームに支えられた、組織全体での持続的かつ協調的な取り組みが必要になります。

3

リスクイベントと検出

検出数の多いリスクイベント

	リスクイベント
1	Risky Cloud App Access
2	Stale Microsoft Entra ID Account
3	Virtual Analyzer - Email Risk
4	Microsoft Entra ID Account with Weak Sign-In Security Policy - MFA Disabled
5	ZTSA Rule Match - Private Access Control
6	Advanced Spam Protection - Policy Violation
7	On-Premises AD Account with Weak Sign-In Security Policy - Password Expiration Disabled
8	Stale On-Premises AD Account
9	Microsoft Entra ID Account with Weak Sign-In Security Policy - Password Expiration Disabled
10	Virtual Analyzer - Cloud App Risk

表1. 2025年（1月〜12月）に検出数の多かったリスクイベント上位10件

Risky Cloud App Access（リスクの高いクラウドアプリへのアクセス）が2024年に続き首位を維持しました。企業のクラウド移行の流れに減速の兆しはなく、従業員がどのクラウドアプリケーションにアクセスするかの統制に、組織は引き続き苦戦しています。

Stale Microsoft Entra ID Account（長期間未使用の Microsoft Entra ID アカウント）が2位を占めており、アイデンティティ衛生が依然として構造的な問題であることを示唆しています。長期間未使用のアカウントが2年連続で上位2位以内にとどまっていることは、修復の取り組みがアカウントの無秩序な増加に追いついていないことを物語っています。

5位に入った ZTSA（Zero Trust Secure Access）Rule Match - Private Access Control は新顔です。これは顧客基盤全体でゼロトラスト導入が拡大し、従来は捕捉されていなかったポリシー違反が可視化されるようになったことを反映しているとみられます。組織が従来の境界ベースのセキュリティモデルから、アイデンティティとポリシーに基づくアクセス制御へと移行するのに伴い、ユーザやデバイスによる社内アプリケーション・リソースへのアクセスを統制するためにゼロトラストの枠組みが展開されています。このイベントが上位5件に現れたことは、これらの枠組みが今や相当な規模で検出を生み出していることを意味します。

MFA が無効化されたアカウントとパスワード有効期限が無効化されたアカウントは引き続き懸念事項であり、脆弱な認証ポリシーが広く存在するという2024年の調査結果と整合しています。

Virtual Analyzer - Cloud App Risk は今回初めて一覧に入りました。クラウド導入の広がりに伴い、クラウドアプリケーションのサンドボックス解析による検出が増加していることを示唆しています。

業種別の内訳からは、主要な攻撃経路が業種ごとに分かれている様子がうかがえます。鉱業だけはクラウドアプリへのアクセスではなくメール経由の脅威（Virtual Analyzer - Email Risk）が筆頭であり、標的型のスピアフィッシングキャンペーンがこの業種の主要な経路になっている可能性を示唆しています。

ヘルスケア、農業、電気通信はいずれも Risky Cloud App Access が筆頭である一方、教育では Stale Microsoft Entra ID Account イベントが最上位を占めており、大規模で分散したユーザ集団を抱えるという、かねて指摘されてきたアイデンティティ管理の課題を裏付けています。

平均CRIが高い上位5業種で検出数の多いリスクイベント

	鉱業	ヘルスケア	農業	電気通信	教育
1	Virtual Analyzer - Email Risk	Risky Cloud App Access	Risky Cloud App Access	Risky Cloud App Access	Stale Microsoft Entra ID Account
2	Risky Cloud App Access	Stale Microsoft Entra ID Account	Data Loss Prevention - Email Violation	Stale Microsoft Entra ID Account	Microsoft Entra ID Account with Weak Sign-In Security Policy - MFA Disabled
3	Stale Microsoft Entra ID Account	Microsoft Entra ID Account with Weak Sign-In Security Policy - MFA Disabled	Microsoft Entra ID Account with Weak Sign-In Security Policy - MFA Disabled	Advanced Spam Protection - Policy Violation	Risky Cloud App Access
4	Malware Scanning - Email Threat	Virtual Analyzer - Email Risk	Advanced Spam Protection - Policy Violation	Data Loss Prevention - Email Violation	Microsoft Entra ID Account with Weak Sign-In Security Policy - Password Expiration Disabled
5	Virtual Analyzer - Cloud App Risk	On-Premises AD Account with Weak Sign-In Security Policy - Password Expiration Disabled	Data Loss Prevention - Cloud App Violation	Microsoft Entra ID Account with Weak Sign-In Security Policy - MFA Disabled	Microsoft Entra ID Account with Weak Sign-In Security Policy - Strong Password Disabled

図4. 2025年（1月〜12月）の年間平均CRIが高い上位5業種それぞれで検出数の多かったリスクイベント

鉱業は上位5業種の中で唯一、クラウドアプリへのアクセスよりもメール経由の脅威が上位に来ており、標的型フィッシングキャンペーンが初期侵入の主要な経路であることを示しています。OT のエクスポージャーが大きく、セキュリティ成熟度が限られるこの業種では、メール経由の侵害が成功した場合の影響はエンドポイントをはるかに超えて広がります。

ヘルスケアのリスクイベントプロファイルは、ハイブリッド環境という実態を映し出しています。上位にはクラウドアクセスのリスクが並び、下位半分にはオンプレミスの Active Directory（AD）アカウントの弱点が現れています。この分布は、アイデンティティリスクが2つの並行するインフラにまたがって管理されていることを示しており、ヘルスケアの組織はクラウドとオンプレミスのどちらか一方の管理策だけでは CRI に対処できないことを意味します。

農業は上位5業種の中で唯一、リスクイベントの上位を Data Loss Prevention（情報漏洩対策）違反が占めており、メールとクラウドアプリ双方の違反が Risky Cloud App Access と並んで現れています。このパターンは、サプライチェーンや業務に関わる機密データが、十分に統制されていない経路を通じて組織外へ

流出していることを示すシグナルです。MFA が無効化されたアカウントがこのリスクに拍車をかけており、データ移動を可能にしているアカウント自体が十分に保護されていない状態が放置されています。

電気通信は、受信メールのポリシー違反と送信側の情報漏洩対策の不備の両方が上位5件に同時に入っている唯一の業種です。このリスクプロファイルは組織自身にとどまらず、この業種に依存する顧客や重要インフラにまで及びます。膨大な量の機密性の高い顧客データを扱う業種にとって、受信側の脅威エクスポージャーと送信側のデータガバナンスの不備の組み合わせは、とりわけ重大です。

教育の主要リスクイベント5件のうち4件は、長期間未使用のアカウント、MFA の無効化、パスワード有効期限の無効化、強力なパスワードの無効化と、いずれもアカウントと認証情報のセキュリティに直結するものです。これは上位5業種の中で最もアイデンティティに集中したリスクプロファイルです。規模が大きく入れ替わりの激しいユーザ集団全体でアカウントのライフサイクル管理が体系化・自動化されるまでは、他にどのような管理策を講じても、教育の CRI の低減は険しい道のりであり続けるでしょう。

検出数の多い TrendAI Vision One™ の設定不備

	設定不備イベント
1	Web Reputation Settings in TrendAI Vision One™ Endpoint Security Not Optimized
2	Device Control Settings in TrendAI Vision One™ Endpoint Security Not Optimized
3	TrendAI Vision One™ Endpoint Security Agent Not Supported
4	Anti-Malware Scanning Settings in TrendAI Vision One™ Endpoint Security Not Optimized
5	Smart Feedback Settings in TrendAI Vision One™ Endpoint Security Not Optimized
6	Predictive Machine Learning Settings in TrendAI Vision One™ Endpoint Security Not Optimized
7	Endpoint Sensor Settings in TrendAI Vision One™ Endpoint Security Not Optimized
8	TrendAI™ Apex One Firewall Settings in TrendAI Vision One™ Endpoint Security Not Optimized
9	Application Control Settings in TrendAI Vision One™ Endpoint Security Not Optimized
10	Behavior Monitoring Settings in TrendAI Vision One™ Endpoint Security Not Optimized

表2. 2025年（1月〜12月）に検出数の多かった設定不備上位10件

設定不備のデータから得られる最も重要な示唆は、個々の項目ではなく、項目間の関係にあります。Web レピュテーション、不正プログラム対策、予測型機械学習、エンドポイントセンサー、ファイアウォール、アプリケーションコントロール、挙動監視は互いに独立した管理策ではなく、統合された多層防御アーキテクチャを構成しています。同一の顧客環境でこの7つが同時に最適化されないまま放置されると、その結果生じるセキュリティ体制の弱さは、7つの欠陥の単純な合計にはとどまりません。それぞれの弱点が他の弱点を増幅させるのです。

Web Reputation 設定は2年連続で設定不備一覧の最上位を占めており、顧客基盤全体で最も放置され続けている設定となっています。フィッシングと悪意ある Web コンテンツが依然として初期侵入の主要な経路

であることを踏まえると、この設定を最適化しないまま放置することは、防御の最前線に重大かつ本来不要なギャップを生み出します。2年にわたって最上位にとどまり続けていることは、修復ガイダンスだけでは不十分であり、測定可能な改善を実現するには、自動化された強制適用やより強固なデフォルト設定が必要である可能性を示唆しています。

Device Control 設定の最適化不足は、広範でありながら過小評価されがちな、データ持ち出しと不正プログラム持ち込みのリスクをもたらします。リモートワークやハイブリッドワークによって個人所有デバイスを企業インフラと併用することが当たり前になった時代において、適切に構成されたデバイス制御ポリシーの欠如は恒常的な死角を生みます。この設定不備が、コネクテッドな物理デバイスを大量に抱えるヘルスケアと農業でそれぞれ最上位に現れていることは、デバイスガバナンスが個別の設定漏れではなく業種全体の課題であることを裏付けています。

Anti-Malware Scanning 設定の最適化不足は、スキャン頻度の低下、重要なファイルタイプやディレクトリの除外、リアルタイム保護の無効化を意味し得ます。いずれも、悪意あるファイルを実行前に検出・ブロックする能力に重大なギャップを生みます。

Smart Feedback は、エンドポイントが匿名化された脅威インテリジェンスを TrendAI™ のグローバル脅威ネットワークに還元し、個々の顧客環境での検出成果をセキュリティエコシステム全体で共有できるようにする機能です。この設定が最適化されていない組織は、事実上この集合知の輪から離脱していることになり、自らの環境で利用できる脅威インテリジェンスの質と、コミュニティ全体の防御ネットワークへの貢献の両方を損なっています。

平均CRIが高い上位5業種で検出数の多い TrendAI Vision One™ の設定不備

	鉱業	ヘルスケア	農業	電気通信	教育
1	Endpoint Sensor Settings in TrendAI Vision One™ Endpoint Security Not Optimized	Device Control Settings in TrendAI Vision One™ Endpoint Security Not Optimized	Device Control Settings in TrendAI Vision One™ Endpoint Security Not Optimized	Suspicious Connection Service Settings in TrendAI Vision One™ Endpoint Security Not Optimized	Non-Optimized Security Agent Password Unlock Settings in TrendAI Vision One™ Endpoint Security
2	TrendAI Vision One™ Endpoint Security Agent Not Supported	TrendAI Vision One™ Endpoint Security Agent Not Supported	Application Control Settings in TrendAI Vision One™ Endpoint Security Not Optimized	Non-Optimized Security Agent Password Unlock Settings in TrendAI Vision One™ Endpoint Security	Smart Feedback Settings in TrendAI Vision One™ Endpoint Security Not Optimized
3	Suspicious Connection Service Settings in TrendAI Vision One™ Endpoint Security Not Optimized	Predictive Machine Learning Settings in TrendAI Vision One™ Endpoint Security Not Optimized	Non-Optimized Security Agent Password Unlock Settings in TrendAI Vision One™ Endpoint Security	Anti-Malware Scanning Settings in TrendAI Vision One™ Endpoint Security Not Optimized	Behavior Monitoring Settings in TrendAI Vision One™ Endpoint Security Not Optimized
4	Non-Optimized Security Agent Password Unlock Settings in TrendAI Vision One™ Endpoint Security	TrendAI™ Apex One Firewall Settings in TrendAI Vision One™ Endpoint Security Not Optimized	TrendAI Vision One™ Endpoint Security Agent Not Supported	TrendAI™ Apex One Firewall Settings in TrendAI Vision One™ Endpoint Security Not Optimized	Application Control Settings in TrendAI Vision One™ Endpoint Security Not Optimized
5	Application Control Settings in TrendAI Vision One™ Endpoint Security Not Optimized	Smart Feedback Settings in TrendAI Vision One™ Endpoint Security Not Optimized	Endpoint Sensor Settings in TrendAI Vision One™ Endpoint Security Not Optimized	Application Control Settings in TrendAI Vision One™ Endpoint Security Not Optimized	Device Control Settings in TrendAI Vision One™ Endpoint Security Not Optimized

図5. 2025年（1月〜12月）の年間平均CRIが高い上位5業種それぞれで検出数の多かった設定不備

鉱業の設定不備の筆頭は、Endpoint Sensor 設定の最適化不足です。センサーは可視性の基盤であることを踏まえると、これは看過できない結果であり、鉱業の組織が検出能力に大きな死角を抱えている恐れがあることを意味します。

ヘルスケアの設定不備の筆頭は Device Control 設定の最適化不足であり、ネットワークに接続された大量の医療機器の管理というこの業種の課題と整合しています。

農業でも Device Control 設定が最上位の設定不備であり、2024年版レポートでも指摘した、この業種で拡大する IoT と自動化された機械類の導入状況を反映しています。

電気通信だけは Suspicious Connection Service 設定が設定不備の筆頭です。異常な接続パターンが重要な脅威指標となるネットワーク集約型の環境を持つこの業種にとって、これは的を射た結果と言えます。

教育の設定不備の筆頭は Non-Optimized Security Agent Password Unlock 設定であり、この業種のアイデンティティ関連リスクイベントや、学生が管理することも多い大規模なデバイス群という実態と整合する結果です。

検出数の多い TrendAI Vision One™ のクラウド設定不備

	クラウド設定不備イベント
1	Application Control Settings in TrendAI Vision One™ Endpoint Security - Endpoint & Workload Security Not Optimized
2	Firewall Settings in TrendAI Vision One™ Endpoint Security - Endpoint & Workload Security Not Optimized
3	Log Inspection Settings in TrendAI Vision One™ Endpoint Security - Endpoint & Workload Security Not Optimized
4	Device Control Settings in TrendAI Vision One™ Endpoint Security - Endpoint & Workload Security Not Optimized
5	Anti-Malware Settings in TrendAI Vision One™ Endpoint Security - Endpoint & Workload Security Not Optimized
6	File Integrity Monitoring (FIM) Settings in TrendAI Vision One™ Endpoint Security - Endpoint & Workload Security Not Optimized
7	Web Reputation Settings in TrendAI Vision One™ Endpoint Security - Endpoint & Workload Security Not Optimized
8	Intrusion Prevention System (IPS) Settings in TrendAI Vision One™ Endpoint Security - Endpoint & Workload Security Not Optimized
9	Smart Feedback Settings in TrendAI Vision One™ Endpoint Security - Endpoint & Workload Security Not Optimized
10	Activity Monitoring Settings in TrendAI Vision One™ Endpoint Security - Endpoint & Workload Security Not Optimized

表3. 2025年（1月〜12月）に検出数の多かったクラウド設定不備上位10件

クラウドワークロード保護を導入している組織が、その保護を実効性あるものにするための設定を一貫して最適化できていません。顧客基盤全体で、「導入」と「運用定着」の間のギャップが大規模に存在し続けていることを示唆しています。

クラウド設定不備一覧の最上位は Application Control です。これは、クラウドワークロードやコンテナ環境内でどのアプリケーションやプロセスの実行を許可するかを統制する管理策です。クラウドワークロードは多くの場合インターネットに面し、高度に自動化され、急速に変化するため、クラウド環境における Application Control 設定の最適化不足はとりわけ重大です。アプリケーションガバナンスのポリシーが正確に定義され、積極的に維持されていなければ、不正または悪意あるプロセスが実行される機会が頻繁に生じます。

Firewall 設定は、ワークロードレベルでのネットワークトラフィックのフィルタリングを担い、個々のクラウドインスタンスやコンテナに対してどの送受信接続を許可するかを制御します。この文脈での設定の最適化不足は、過度に寛容な受信ルール、データ持ち出しを可能にする無制限の送信接続、セキュリティより可用性を優先するデフォルト設定などを意味し得ます。

Log Inspection は、システムログとアプリケーションログをリアルタイムに分析し、クラウドワークロード内のセキュリティ関連イベント、ポリシー違反、侵入の痕跡（IoC: Indicators of Compromise）を検出します。この設定不備の影響は、直接的な検出ギャップにとどまりません。コンプライアンスの枠組みはログの収集と分析を基礎的な統制として義務付けており、Log Inspection 設定が最適化されていない組織は、セキュリティリスクと並行して、認識されていないコンプライアンス上のエクスポージャーも抱えている可能性があります。

クラウド・ワークロード環境における Device Control は、仮想デバイスの接続やストレージ構成を含む、クラウドインスタンスと周辺機器・ストレージデバイスとの相互作用を統制します。エンドポイントの設定不備一覧で2位を占めるのに加えてクラウド設定不備でも4位に現れていることは、デバイスガバナンスが物理環境と仮想環境の両方にまたがる根深い課題であることを示唆しています。クラウドワークロードの文脈では、Device Control 設定の最適化不足により、クラウドインスタンスと外部ストレージ間の不正なデータ転送が可能になったり、誤設定されたボリューム接続を通じたデータ持ち出しの経路が生まれたり、不適切に統制された仮想デバイス接続を通じて悪意あるコンテンツが持ち込まれたりする恐れがあります。

クラウド環境で Anti-Malware 設定を最適化しないまま運用することは、ワークロードのライフサイクル全体を通じた一貫した不正プログラムスキャンなしにクラウドワークロードを稼働させていることを意味します。この課題はクラウド運用のスピードによってさらに深刻になります。ワークロードが自動化されたパイプラインで次々と立ち上がる環境では、手動での構成が必要な設定や、Policy as Code として強制されていない設定は、展開のペースに常に後れを取ることになります。

平均CRIが高い上位5業種で検出数の多いクラウド設定不備

	鉱業	ヘルスケア	農業	電気通信	教育
1	Application Control Settings in TrendAI Vision One™ Endpoint Security - Endpoint & Workload Security Not Optimized	Anti-Malware Settings in TrendAI Vision One™ Endpoint Security - Endpoint & Workload Security Not Optimized	File Integrity Monitoring (FIM) Settings in TrendAI Vision One™ Endpoint Security - Endpoint & Workload Security Not Optimized	Log Inspection Settings in TrendAI Vision One™ Endpoint Security - Endpoint & Workload Security Not Optimized	Predictive Machine Learning Settings in TrendAI Vision One™ Endpoint Security Not Optimized
2	Firewall Settings in TrendAI Vision One™ Endpoint Security - Endpoint & Workload Security Not Optimized	Application Control Settings in TrendAI Vision One™ Endpoint Security - Endpoint & Workload Security Not Optimized	Log Inspection Settings in TrendAI Vision One™ Endpoint Security - Endpoint & Workload Security Not Optimized	Application Control Settings in TrendAI Vision One™ Endpoint Security - Endpoint & Workload Security Not Optimized	Web Reputation Settings in TrendAI Vision One™ Endpoint Security - Endpoint & Workload Security Not Optimized
3	Log Inspection Settings in TrendAI Vision One™ Endpoint Security - Endpoint & Workload Security Not Optimized	Web Reputation Settings in TrendAI Vision One™ Endpoint Security - Endpoint & Workload Security Not Optimized	Firewall Settings in TrendAI Vision One™ Endpoint Security - Endpoint & Workload Security Not Optimized	Device Control Settings in TrendAI Vision One™ Endpoint Security - Endpoint & Workload Security Not Optimized	Anti-Malware Settings in TrendAI Vision One™ Endpoint Security - Endpoint & Workload Security Not Optimized
4	File Integrity Monitoring (FIM) Settings in TrendAI Vision One™ Endpoint Security - Endpoint & Workload Security Not Optimized	Smart Feedback Settings in TrendAI Vision One™ Endpoint Security - Endpoint & Workload Security Not Optimized	Intrusion Prevention System (IPS) Settings in TrendAI Vision One™ Endpoint Security - Endpoint & Workload Security Not Optimized	Smart Feedback Settings in TrendAI Vision One™ Endpoint Security - Endpoint & Workload Security Not Optimized	Intrusion Prevention System (IPS) Settings in TrendAI Vision One™ Endpoint Security - Endpoint & Workload Security Not Optimized
5	Agent Self-Protection Settings in TrendAI Vision One™ Endpoint Security - Endpoint & Workload Security Not Optimized	Device Control Settings in TrendAI Vision One™ Endpoint Security - Endpoint & Workload Security Not Optimized	Anti-Malware Settings in TrendAI Vision One™ Endpoint Security - Endpoint & Workload Security Not Optimized	File Integrity Monitoring (FIM) Settings in TrendAI Vision One™ Endpoint Security - Endpoint & Workload Security Not Optimized	Application Control Settings in TrendAI Vision One™ Endpoint Security - Endpoint & Workload Security Not Optimized

図6. 2025年（1月〜12月）の年間平均CRIが高い上位5業種それぞれで検出数の多かったクラウド設定不備

鉱業のクラウド設定不備の上位は Application Control 設定と Firewall 設定です。この2つの管理策のギャップが重なると、鉱業の環境では、ネットワークレベルのフィルタリングがほとんどないまま不正なアプリケーションが実行されている恐れがあり、リスクの高い組み合わせとなります。

ヘルスケアのクラウド設定不備の筆頭は Anti-Malware 設定で、Application Control 設定が続きます。多様でレガシーなデバイス群の保護というこの業種の課題と整合する結果です。

農業のクラウド設定不備の筆頭は File Integrity Monitoring（FIM）設定です。FIM は OT システムの改ざんを検出するための重要な管理策であり、IoT のエクスポージャーが大きいこの業種にとって重大な意味を持ちます。

電気通信のクラウド設定不備の最上位は Log Inspection 設定です。異常なトラフィックパターンの検出が最重要となる業種にとって、これは深刻なギャップです。

検出数の多い XDR モデル検出

	モデル名
1	Possible Disabling of Antivirus Software
2	Hacking Tool Detection - Blocked
3	Registry Run Key Creation Pointing to Files in Temp Location
4	Unknown Threat Detection and Mitigation via Predictive Machine Learning
5	Threat Intelligence Sweeping
6	[Heuristic Attribute] Backdoor File Detection
7	[Heuristic Attribute] Possible OS Credential Dumping
8	File Detections in Windows Directory - Blocked
9	Possible Account Compromise - Atypical Travel
10	Eicar Test File Detection

表4. 2025年（1月〜12月）に検出数の多かった XDR モデル検出上位10件

2025年の XDR モデル検出データは、攻撃者が何よりも防御回避と永続性の確立を優先する脅威情勢を示唆しています。

Possible Disabling of Antivirus Software（ウイルス対策ソフトウェア無効化の可能性）が最上位に浮上したことは、認証情報ダンプが首位だった2024年からの大きな変化です。この変化は、キルチェーンの早い段階で防御を無効化するほうが、回避を試みるよりも確実だと攻撃者が学習したことを示唆しています。

上位10件のモデル検出を総合すると、攻撃者が体系的かつ執拗であり、環境の奥深くへ進む前に足場を固めることへの注力を強めている姿が浮かび上がります。

4

脆弱性と対応データ

検出数の多い未修正 CVE 上位10件

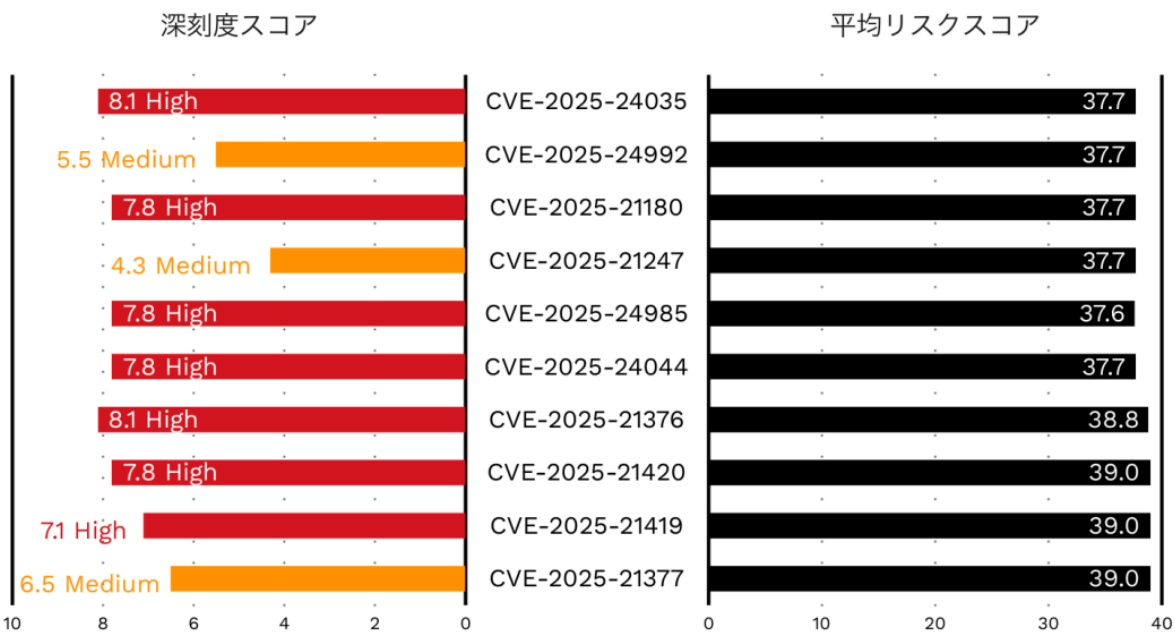


図7. 2025年（1月〜12月）に顧客環境で未修正のまま検出された脆弱性上位10件。米国国立標準技術研究所（NIST）による CVSS 深刻度スコアと、それぞれの平均リスクスコアを併記しています。数値は小数第1位に丸めており、順位は丸める前の数値に基づきます。

この一覧には高と中の深刻度スコアが混在していますが、後述の分析が示すとおり、深刻度スコアだけでは実際のリスクをうまく測れません。10件の CVE のうち3件は中程度の深刻度でありながら、検出数の多い未修正脆弱性の上位10件に入っています。これは、共通脆弱性評価システム（CVSS）のスコアのみでパッチの優先順位を決め、高深刻度に満たないものの優先度を一律に下げるという、企業で一般的な運用に疑問を投げかける結果です。

2つの脆弱性クラスは、組み合わさると危険な相乗効果を生みます。1つ目はリモートコード実行（RCE）で、CVE-2025-24035（Windows リモートデスクトップサービス）、CVE-2025-24985（Windows Fast FAT ファイルシステム）、CVE-2025-21376（Windows Lightweight Directory Access Protocol（LDAP））、CVE-2025-21180（Windows exFAT ファイルシステム）が該当し、攻撃者による任意のコードのリモート実行を可能にします。2つ目は権限昇格（EoP）で、CVE-2025-24044（Windows カーネルモードドライバ）、CVE-2025-21420 および CVE-2025-21419（Windows システムユーティリティ）が該当し、初期侵入の足がかりからシステムの完全掌握へと至る昇格経路を提供します。同一環境に未修正の RCE と EoP の脆弱性が併存することは考え得る限り最も危険な組み合わせであり、未対応の場合、企業はこれらの脆弱性へのパッチ適用を確実に行う必要があります。

一覧のうち CVE-2025-24992（5.5）、CVE-2025-21247（4.3）、CVE-2025-21377（6.5）の3件は中程度の深刻度スコアであり、これらが上位10件に入っていることは、本年の脆弱性データにおける最も重要な調査結果の一つです。

CVE-2025-24992 は Windows NTFS のバッファオーバーリードの脆弱性で、ローカルでの情報漏洩につながる可能性があり、この一覧にある RCE 脆弱性の悪用を容易にする恐れがあります。CVE-2025-21247 は Windows のゾーンベースのコンテンツセキュリティをバイパスし、信頼されていないコンテンツをオペレーティングシステムに信頼済みと誤認させます。CVE-2025-21377 は NTLM 認証ハッシュを漏洩させ、そのハッシュを使ってネットワーク上で当該ユーザとして認証される恐れがあります。

この3件の中深刻度の脆弱性は、いずれも単体では致命的ではありません。しかし、この一覧にある高深刻度の脆弱性や、XDR データに記録された攻撃者の手口と組み合わさると、きわめて危険なものになります。深刻度スコアだけに基づくパッチ優先順位付けの戦略では、こうした悪用を後押しする脆弱性が組織的に放置され、高深刻度のエクスプロイトの成功率と被害を高める条件がそのまま維持されてしまいます。リスクベースの脆弱性管理には、個々の脆弱性が単体でどれほど深刻に見えるかだけでなく、脆弱性同士がどのように相互作用するかを理解することが必要です。

本レポートでは、CVSS 深刻度スコアに加えて、各 CVE の平均リスクスコアを掲載しています。これは TrendAI Vision One™ プラットフォーム独自のリスクスコアリング手法で算出したもので、深刻度だけでなく、実際の悪用（ITW: in-the-wild）の活動状況や悪用可能性といった実世界のシグナルを加味しています。これらのスコアは顧客テレメトリ全体の平均値であり、活発な悪用状況を考慮すると、CVE のリスクが静的な深刻度評価からどれほど乖離し得るかを示すことを意図しています。実際のエクスポージャーは組織固有の環境、構成、補完的な管理策に依存するため、企業はこれらの数値を傾向として捉えるべきです。各 CVE が自社システムにもたらす正確なリスクの評価には TrendAI Vision One™ プラットフォームを活用し、それに応じてパッチを適用してください。

仮想パッチと悪用までの時間

115日

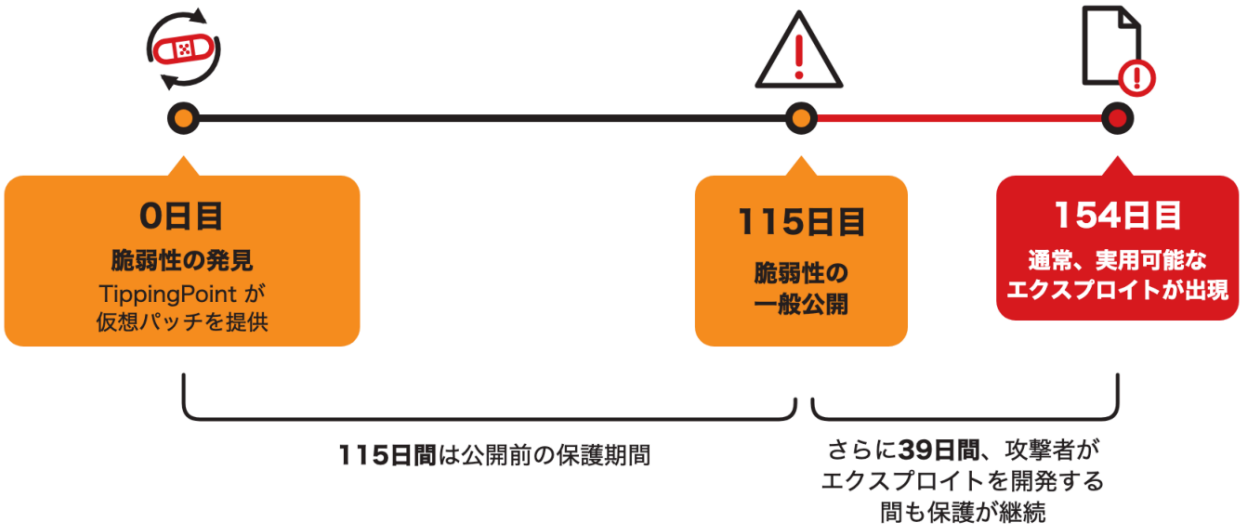
仮想パッチのリードタイム

脆弱性の発見からの平均
（TrendAI™ TippingPoint™、
2025年の脆弱性）

39日

悪用までの時間

一般公開からの平均
（脆弱性情勢全般）



注意すべきは、この2つの数値が同じゴールを目指す競争を測ったものではなく、それぞれ異なる起点から計測されているという点です。仮想パッチのリードタイムは、TrendAI™ TippingPoint™ が脆弱性を最初に特定した「発見」の時点から計測を始めます。これは多くの場合、その存在が誰にも知られていない段階です。一方、悪用までの時間（Time to Exploit）は、攻撃者が攻撃の組み立てに必要な情報をようやく手にする「一般公開」の時点から計測を始めます。

発見は必ず公開に先行するため、TippingPoint のお客さまは、攻撃者の時計が動き出すよりもはるか前から保護されています。仮想パッチが適用された状態で平均115日間の先行期間があり、公開から約39日後に攻撃者が実用可能なエクスプロイトを手にする頃には、TippingPoint のお客さまは最大154日間保護されてきたことになります。

これこそが仮想パッチの中核的な価値です。発見からベンダによる正式パッチの提供までのギャップを埋め、正式な修正のテストと展開が進む間も組織を継続的に保護します。エクスポージャーの空白期間はなく、防御の開始を公開まで待つ必要もありません。

ただしリスクは、仮想パッチを正式なパッチ適用への橋渡しとしてではなく、その代替として扱ってしまうことにあります。39日という武器化までの猶予は短く、仮想パッチを一時的な措置ではなく主要な管理策として頼っている組織は、ルールの展開が遅れた場合、実際に悪用が行われている期間に無防備な状態に置かれかねません。

このリスクは深刻度の低い脆弱性でさらに大きくなります。CVE-2025-24992、CVE-2025-21247、CVE-2025-21377 は、正式なパッチ適用の順番待ちでも仮想パッチルールの優先順位付けでも、後回しにされる可能性が高い脆弱性です。この一覧にある高深刻度エクスプロイトを後押しする役割が実証されているにもかかわらず、です。CVSS スコアのみに基づくパッチ適用への反論は、仮想パッチの優先順位付けにもそのまま当てはまります。

5

Attack Path Prediction データ

攻撃者が環境内をどのように移動するかを理解するには、脆弱性や設定不備の一覧だけでは足りません。個々のエクスポージャーを現実の侵害へと変える一連のシーケンス、すなわち初期侵入の足がかりから水平移動・内部活動を経て価値の高い標的へ至る連鎖のステップをモデル化することが必要です。

TrendAI Vision One™ の Attack Path Prediction（攻撃経路予測）機能は、まさにそれを実現します。本セクションで提示するデータセットは、顧客基盤全体のアクティブな攻撃経路を分析し、経路の生成を最も多く引き起こしているリスクイベント、侵入起点となることが最も多い資産タイプ、そして攻撃シーケンスが成立した際に攻撃者が最終的に到達することの多い標的を明らかにします。

予測される攻撃経路の数は組織の複雑さに比例して増えますが、経路の起点となりやすいイベントと終点となる資産は、組織がリスク管理の優先順位を決める際の指針になります。

Attack Path Prediction の調査結果は、執筆時点で入手可能な最新のテレメトリに基づいています。2025年通年の Attack Path Prediction データがまだ揃っていないため、本セクションは完全な年間測定ではなく、新たに現れつつある攻撃経路パターンの傾向を示すものとしてお読みください。

攻撃経路の生成に関与するリスクイベント上位5件

Attack Path Prediction のデータセットから得られる、運用面で最も実行に移しやすい調査結果の一つが、アクティブな攻撃経路の起点に構成要素として最も頻繁に現れるリスクイベントの特定です。これらは単に環境内で検出数が多いイベントではありません。攻撃者に悪用可能な出発点を与えることで、攻撃経路の形成を現に可能にしているイベントです。

この区別は重要です。検出には頻繁に現れるものの攻撃経路の先頭にはめったに現れないイベントは、修復の優先度が異なります。優先度が最も高いのは、攻撃者の一連の行動の起点となる条件として一貫して機能しているイベントです。

順位	リスクイベント要因	カテゴリ	攻撃経路総数
1	脆弱性	CVE	2,317,503
2	Potential Brute Force Attack – Password Spraying	検出	1,135,327
3	Potential Brute Force Attack – Password Guessing	検出	880,527
4	Behavior Monitoring Detection for Built-in Windows Tools	検出	539,106
5	Multiple command-and-control (C&C) Connections via Common Protocols	検出	452,085

表5. TrendAI Vision One™ がマッピングした攻撃経路数が最も多かったリスクイベント上位5件（2025年5月〜6月）

脆弱性は2,317,503件の攻撃経路で1位を占めており、これは下位2つのブルートフォース系認証情報イベントの合計を約15%上回る数です。本レポートで先に示した CVE の状況と併せて見ると、攻撃経路データは、それらの未修正の脆弱性が眠ったまま放置されているわけではないことを示唆しています。未修正の脆弱性は、顧客基盤全体で成立し得る攻撃経路の起点として、単独で最大の発生源となっています。

2位と3位のリスクイベントであるパスワードスプレーとパスワード推測は、いずれもブルートフォース型の認証情報攻撃であり、合わせて200万件超の攻撃経路の起点となっています。両手法が突くのは同じ構造的弱点です。すなわち、脆弱なパスワード、使い回されたパスワード、無期限のパスワードで保護され、多要素認証が強制されていないアカウントです。この結果は、CRI データに記録されたアイデンティティ関連リスクイベントと整合しています。そこでは、MFA が無効化されたアカウントとパスワード有効期限の無効化ポリシーが、リスクの高い業種全体で目立って現れていました。

パスワードスプレー（よく使われる少数のパスワードを多数のアカウントに対して試す手法）は、特定の環境に対してとりわけ有効です。パスワードポリシーに一貫性がない環境や、正規ユーザの業務を妨げないようロックアウトのしきい値が緩く設定されている環境で成功します。パスワード推測は、より多くの候補認証情報を使って特定の価値の高いアカウントを狙います。両者は、積極的に堅牢化されていないアイデンティティ基盤に対する、最も確実な初期侵入経路です。これらが一覧の上位近くに位置していることは、攻撃者が予測された攻撃経路の大半を、まさに CRI データが防御の最も弱い場所として示す地点から始めていることを示唆しています。

一方、4位と5位のリスクイベントは、脆弱性の悪用や認証情報を使った侵入が成功した後に何が起きるかを示唆しています。Behavior Monitoring Detection for Built-in Windows Tools は、Windows 標準のユーティリティが悪意ある目的に使われる行為を捕捉します。信頼されたシステムプロセスの範囲内で活動することで、攻撃者はシグネチャベースの検出から姿を隠し、環境内での潜伏時間を引き延ばします。

5位の Multiple command-and-control (C&C) Connections via Common Protocols は、アクティブな攻撃経路のかなりの割合に、確立済みの C&C チャネルが含まれていることを示しています。テレメトリ対象の環境の少なくない部分が初期侵入の段階を越え、攻撃者が実際に活動する状態にまで達しているということです。

構成リスクイベントと CRI の調査結果との関連

2025年に攻撃経路の生成を引き起こしている構成リスクイベントは、CRI データセットに記録されたリスクイベントや設定不備と無関係ではありません。むしろ、未解決のまま残されたそれらの状態がもたらした下流の帰結と見ることができます。

未修正の脆弱性が大差で首位を占めており、前のセクションで示した CVE の調査結果と整合しています。同じ Windows の RCE および EoP の脆弱性が、230万件超の攻撃経路を生み出す侵入条件となっているのです。CRI データは組織がこれらの脆弱性を十分な速さで解消できていないことを、攻撃経路データは攻撃者がその遅れを大規模に悪用し得ることを、それぞれ示唆しています。

2位と3位の認証情報攻撃イベントは、CRI データが2年連続で警告してきたアイデンティティガバナンスの不備の帰結です。長期間未使用のアカウントと MFA が無効化された認証情報は、パスワードスプレーとパスワード推測が必要とする条件そのものを作り出しています。

組織は、大規模かつ同時に活動する2つの異なる初期侵入経路に直面しています。1つは未修正のソフトウェア脆弱性を悪用する技術的な経路、もう1つは認証情報衛生の不備を悪用する人的な経路です。一方だけを塞いでも、アタックサーフェスの大半は露出したままです。Attack Path Prediction のデータを CVE の検出量や CRI のリスクイベントと併せて読むと、本レポートの他の箇所と同じ結論に行き着きます。これらのリスクに対処する能力は、組織が導入済みのツールにすでに備わっているということです。ギャップは運用定着にあり、攻撃経路の件数は、そのギャップの代償を具体的な数字で示しています。

侵入起点と標的となる資産タイプ

攻撃経路の起点となるリスクイベントに加えて、テレメトリからは、どの資産タイプが侵入起点となることが多く、どの資産タイプが成立した経路の最終標的として到達されることが多いかについて、一貫したパターンが見えてきます。攻撃シーケンスの両端を理解することで、組織は管理策の優先順位付けをより正確に行えるようになります。頻出する侵入起点を堅牢化すれば新たな経路が生まれる速度を抑えられ、頻出する標的資産を保護すれば経路が成立してしまった場合の影響を抑えられます。

侵入起点となる資産タイプ上位5件

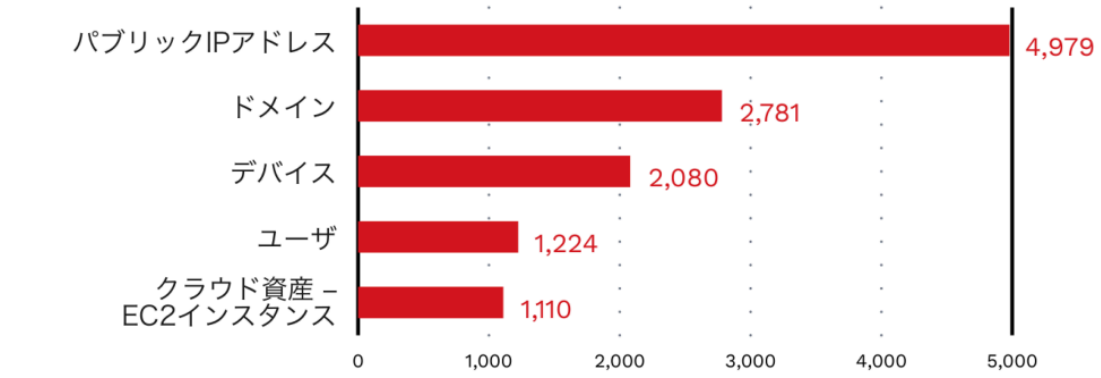


図8. TrendAI Vision One™ Attack Path Prediction がマッピングした、検出数の多い侵入起点資産タイプ上位5件（2025年12月～2026年5月）

パブリック IP アドレスは、顧客基盤全体で1日平均4,979件と、大差で最も多い侵入起点です。この結果は、インターネットに面したインフラに内在する境界エクスポージャーを反映しています。パブリック IP アドレスは外部の攻撃者が最初に遭遇する面であり、保護が不十分な場合、攻撃チェーンの出発点となります。

2位のドメイン資産は、パブリック IP アドレスと対をなして、攻撃経路の起点となる境界エクスポージャーの側面を形づくっています。パブリック IP アドレスがネットワークに直接さらされる面そのものだとす

れば、ドメイン資産、すなわちそれらの IP アドレスに紐付く DNS（ドメインネームシステム）ホスト名は、その表面の上に載る名前付きサービスを表します。Web エンドポイント、メールサーバ、VPN（仮想プライベートネットワーク）ゲートウェイ、管理インターフェースなどです。組織の境界に迫る攻撃者は、この両方に同時に遭遇します。ドメイン資産が侵入起点として多い（1日2,781件）ことは、名前付きサービスが、その名前解決先の IP アドレスと同じくらい直接的に狙われていることを示唆しています。クラウド設定不備のデータで示したファイアウォールやアプリケーションコントロールの設定の最適化不足は、まさにこれら露出したサービスがどのトラフィックを受け入れるかを決める管理策であるだけに、ここで特に重要になります。

一方、ユーザ資産が侵入起点となっていることは、構成リスクイベントのセクションで示したパスワードベースの攻撃によって可能になるアカウントの直接侵害が、攻撃者が最初の足がかりを得る主要な手段であることを示唆しています。

EC2（Elastic Compute Cloud）インスタンスが5位に現れたことは、クラウドネイティブなコンピュート資産が、もはや内部での中継地点にとどまらず、攻撃経路の重要かつ直接的な侵入起点となっていることを裏付けています。この結果は、クラウドワークロード上の Application Control 設定と Firewall 設定の最適化不足が、インターネットに面したクラウドインフラに直接のアタックサーフェスを生み出しているというクラウド設定不備のデータと整合しています。

標的となる資産タイプ上位5件

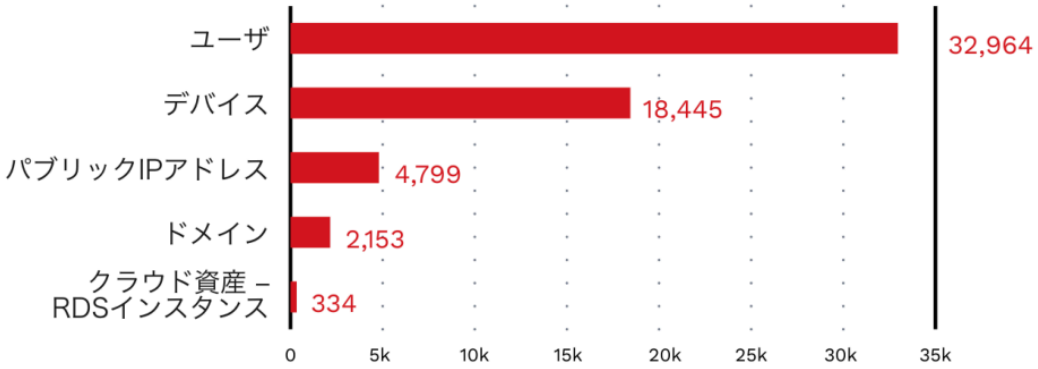


図9. TrendAI Vision One™ Attack Path Prediction がマッピングした、標的とされた資産タイプ上位5件（2025年12月〜2026年5月）

ユーザアカウントは、成立した攻撃経路の最終標的として圧倒的に多く、標的とされたユーザ資産は1日平均33,000件近くと、2位の資産タイプの2倍近くに達します。この結果は、本レポート全体で示してきたアイデンティティ衛生の不備をどう解釈すべきかに直結します。長期間未使用のアカウント、MFA が無効化された認証情報、脆弱なパスワードポリシーは、抽象的に CRI スコアを押し上げるだけのリスクイベントではありません。攻撃チェーンの到達先としてユーザアカウントが選ばれやすくなる、具体的な条件そのものです。成立した攻撃経路を通じて高権限のユーザアカウントに到達した攻撃者は、水平移動・内部活動、データ持ち出し、ランサムウェア展開に必要なアクセス権を手に入れます。

2位のデバイス資産は、エンドポイントの侵害が依然として主要な目標であることを示唆しており、ウイルス対策の無効化やハッキングツールの展開が攻撃者の主要な手口として現れた XDR モデル検出データと整合しています。

5位に RDS（Relational Database Service）インスタンスが入っていることは、クラウドネイティブなデータ層という新たな側面を示しています。リレーショナルデータベースサービスはあらゆるクラウド環境で最も機密性の高い資産の一つであり、それが攻撃経路の標的として現れていることは、攻撃者がコンピュートノードだけでなくデータストアへと進んでいることを示唆しています。

6

外部脅威データ

各リークサイトで報告された侵害成功件数の多いランサムウェアグループ

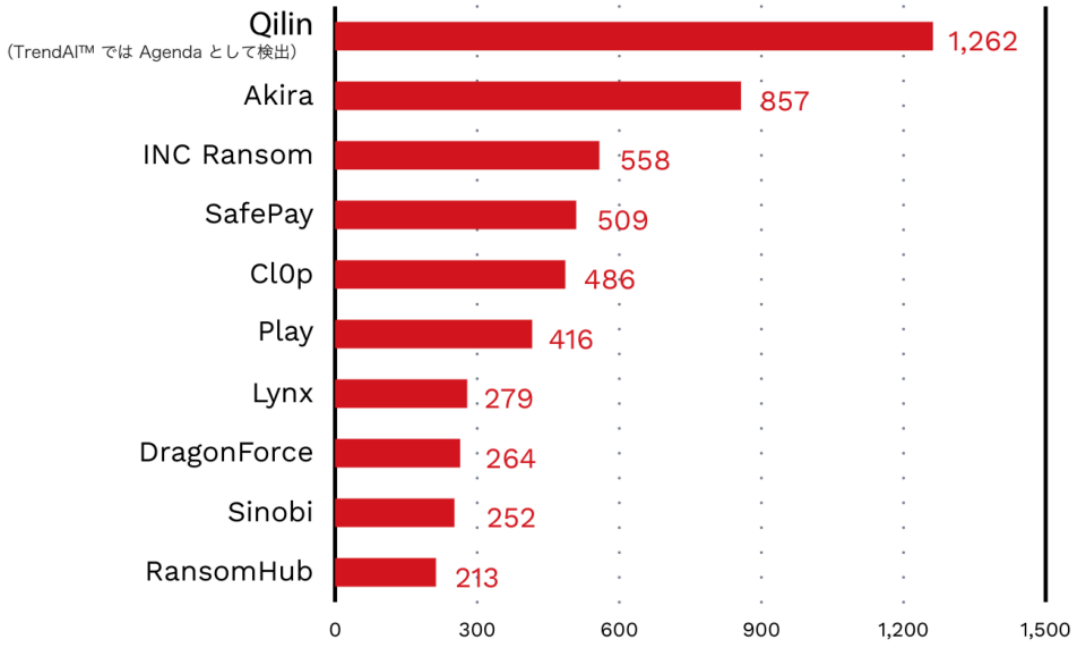


図10. TrendAI™ Research による2025年（1月〜12月）のリークサイトデータのモニタリングに基づく、公表された侵害成功件数が最も多いランサムウェアグループ上位10件

TrendAI™ Research によるサイバー犯罪アンダーグラウンドのモニタリングに基づく2025年のランサムウェア情勢は、昨年の調査結果から大きく様変わりしました。ここでの「侵害件数」は、身代金の支払いに応じなかった企業に対するランサムウェア攻撃の成功件数を指します。つまり、身代金を支払った企業が存在する可能性を踏まえると、実際の攻撃成功件数はこれより多いかもしれません。上位10グループを合計した確認済み侵害件数は2024年比で約236%増加し、被害組織の合計は1,518件から5,096件になりました。ランキングにはまったく新しい5つのグループが加わり、かつて支配的だった2つのグループが姿を消し、確認済み侵害を前年比1,200%超増やしたグループも現れました。2025年のランサムウェアエコシステムは、昨年のレポートに記録されたものよりも細分化が進み、活発さと危険性を増しています。

ランサムウェア Qilin（TrendAI™ では Agenda として検出）は、2024年の最下位（公表された侵害92件）から2025年には最も活発なランサムウェアグループへと躍進しました。本年の外部脅威データの中で最も際立った調査結果です。確認済みの企業侵害が1年で1,270%増加したことは、競合グループの摘発後にアフィリエイト（実行役）を積極的に勧誘するなどして、同グループが作戦規模を大幅に拡大したことを示唆しています。Agenda はランサムウェア・アズ・ア・サービス（RaaS）のプラットフォームとして運営されており、その成長は中核グループ自身の活動だけでなく、そのツール群をより広範な標的に展開するアフィリエイトネットワークの拡大を反映しています。この急速な台頭は、ピークではなく、2026年も激化が続くことを示す先行指標として捉えるべきです。

Akira は確認済み侵害を106件から857件へと708%増やし、2025年で2番目に活発なランサムウェアグループとなりました。Qilin と並ぶその台頭は、LockBit の摘発と RansomHub の衰退によって生じた空白が、単一の後継グループではなく、同時に拡大する複数のグループによって埋められたことを示唆しています。

INC Ransom は確認済み侵害558件で初めて上位10位に入り、一躍第一級のランサムウェアグループとなりました。同グループは、ヘルスケアや教育といった価値の高い業種を狙うこと、そしてデータの暗号化と窃取データの公開の脅しを組み合わせた二重恐喝の手口を用いることで知られています。

SafePay も新顔で、確認済み侵害509件の4位でデビューしました。2025年を迎える時点で SafePay について公に知られていたことは比較的少なく、ランキング上位への突然の登場は、業界にとって大きなインテリジェンスギャップとなっています。

Lynx も新規グループとして確認済み侵害279件で上位10位に入り、新規参入者が急速に一定の規模へ達するというランサムウェアエコシステムの構図を裏付けています。Lynx は複数の業種の組織を標的とし、暗号化と並んでデータ持ち出しに重点を置き、機密データ公開の脅しによって被害者への圧力を強めていることが観測されています。

DragonForce も確認済み侵害264件で上位10位に初登場しました。業種や地域を問わない、比較的無差別な標的選定が特徴です。当初はハクティビスト系に近いグループとして観測されていましたが、ランサムウェアの運営主体へと変貌しました。その侵害件数の多さは、攻撃者が活動範囲と収益化の手段を広げていくという、より大きな潮流を反映しています。

Sinobi は確認済み侵害252件でランキングに入りました。2025年の上位10グループの中でも、公開情報が最も少ないグループの一つです。事前にほとんど知られていなかったグループがこの規模で現れたことから、脅威インテリジェンスチームが優先的に追跡すべき対象と言えます。

Cl0p が確認済み侵害486件で5位に入ったことは、ランサムウェアエコシステムで最も歴史のあるグループの一つが復活したことを意味します。Cl0p はかねて、マネージドファイル転送製品やエンタープライズソフトウェアプラットフォームのゼロデイ脆弱性の大規模悪用と結び付けられてきました。組織を個別に狙うのではなく、広く導入されているエンタープライズツールを侵害することで、短期間に多数の被害を生み出す戦略です。

企業にとって、この示唆は重大です。既知のグループとその確立された TTPs（戦術・技術・手順）を軸に組み立てた防御戦略は、これほど急速に再編される情勢には必ず後れを取ります。最も有効な防御は、特定グループに関するインテリジェンスではなく、誰が悪用するかにかかわらず、それらのグループが突く根本的なエクスポージャーを減らすことです。

外部脅威の地域別・業種別モニタリング

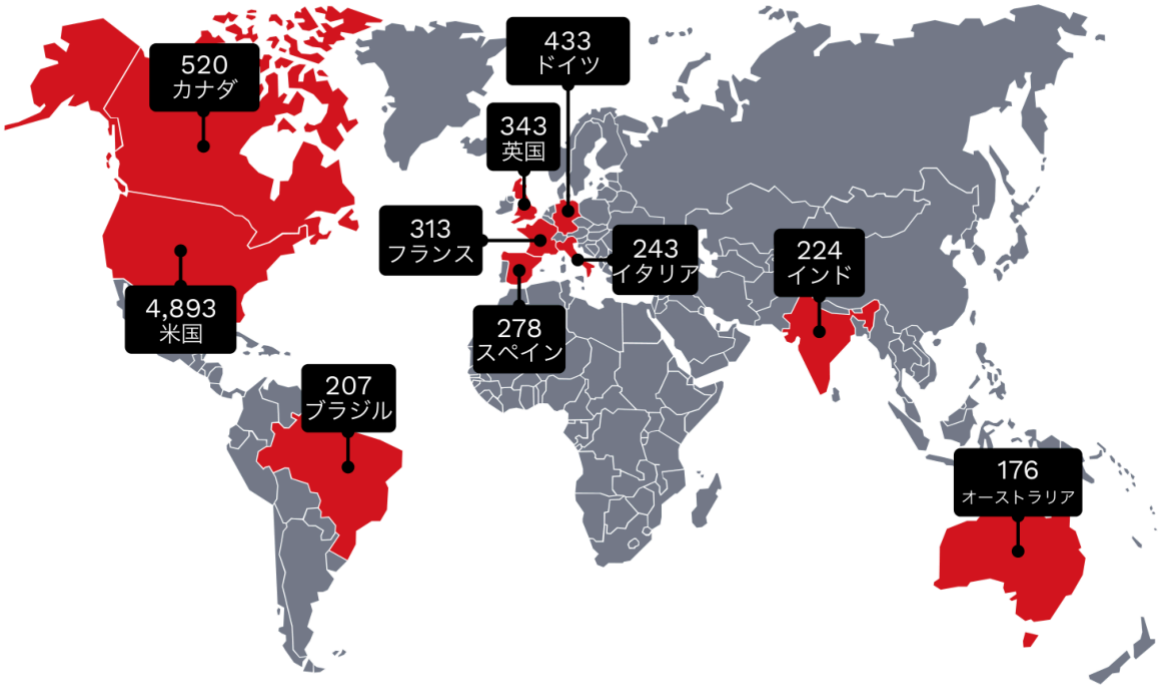


図11. TrendAI™ Research による2025年（1月～12月）のリークサイトデータのモニタリングに基づく、公表された侵害成功件数が最も多い上位10か国

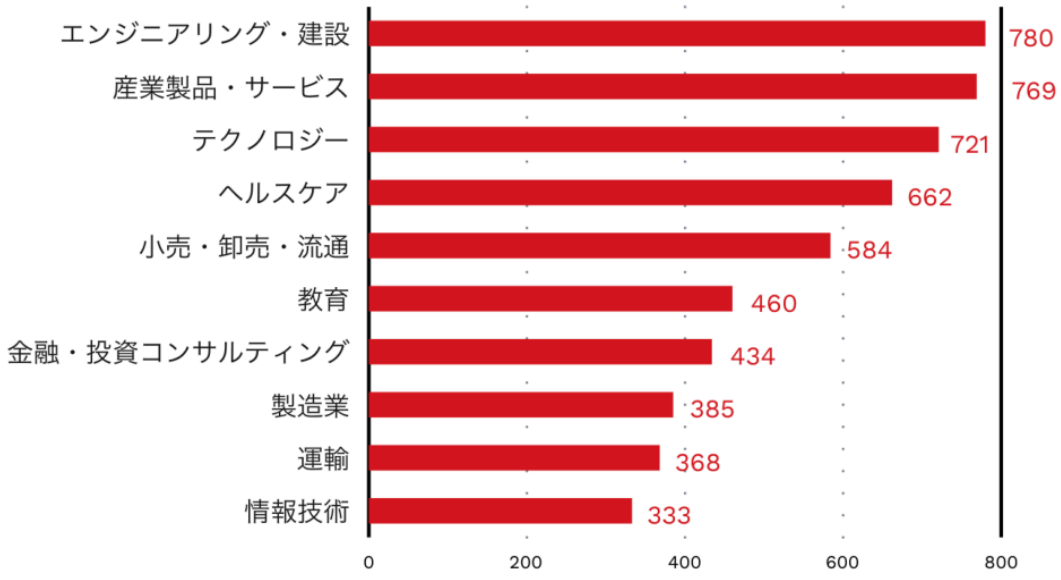


図12. TrendAI™ Research による2025年（1月～12月）のリークサイトデータのモニタリングに基づく、公表された侵害成功件数が最も多い上位10業種

7

結論と推奨事項

サイバーリスクインデックスの低下は、リスクベースのセキュリティ管理が企業顧客基盤全体で測定可能な成果を生んでいることを示唆しています。しかし、確認済みランサムウェア侵害の236%増、新たな第一級脅威グループ5つの出現、そしてアイデンティティガバナンス・エンドポイント設定・パッチ管理における基礎的な不備の残存は、別の方向を指し示しています。これらを総合すると、セキュリティ体制の改善が、必ずしもより安全な環境に結び付いていない可能性が浮かび上がります。

本レポートの調査結果は、一貫した、そして対処可能な要因の組み合わせを指し示しています。顧客環境では複数のセキュリティ設定が同時に最適化されないまま運用され続けており、リスクの高い業種では長期間未使用のアカウントや認証の弱いアカウントが放置され、高深刻度のエクスプロイトを直接後押しし得る中深刻度の脆弱性は、CVSS スコアのみでパッチを適用する組織によって優先度を下げられています。いずれの場合も、リスクに対処する能力は導入済みのツールの中にすでに存在します。ギャップは技術ではなく、運用定着にあるのです。

本年の Attack Path Prediction データは、そのギャップを具体的な形で示しました。攻撃経路の起点の上位を占めるのは脆弱性、パスワードスプレー、パスワード推測であり、未修正の CVE と、解消されないアイデンティティ衛生の不備を突いているとみられます。そして、リスクの高い業種で CRI の主要リスクイベントとして現れているのと同じユーザアカウントが、成立した攻撃チェーンの最終標的として最も多く到達されています。組織がすでに測定できているエクスポージャーこそが、攻撃者が起点から終点までの攻撃シーケンスを組み立てるために現に悪用しているものなのです。

運用定着のギャップを埋めるには、定期的なセキュリティ活動から継続的なリスク管理への移行が必要です。サイバーリスクインデックスをはじめとする TrendAI Vision One™ の機能群は、その移行の定量的な基盤となり、エクスポージャーの把握、修復の優先順位付け、経時的な進捗測定について、セキュリティ部門と経営層が共有できるデータ主導の土台を提供します。本年のデータで最も大きな改善を遂げた組織は、このモデルを場当たり的に採用したのではなく、体系的に運用へ定着させた組織でした。

TrendAI Vision One™ Cyber Risk Exposure Management（CREM）ソリューションは、設定不備、脆弱性、アイデンティティリスク、リスクの高いイベントを単一のビューで捉える、アタックサーフェスの継続的な可視化を提供します。その XDR 機能は、この可視性をメール、エンドポイント、クラウド、ネットワークにまたがる検出と対応につなげます。自動化されたプレイブックと AI 主導の修復は、エンタープライズ規模でリスクインテリジェンスに基づいて行動する際の運用負荷を軽減します。TrendAI Vision One™ が備える脅威インテリジェンスを最大限に活用できるかどうかが、脅威情勢に後追いで対応するセキュリティプログラムと、その先を行くプログラムとの分かれ目になります。

企業は、導入済みのセキュリティ設定を最適化し、アイデンティティガバナンスを大規模に徹底し、連鎖的なエクスプロイトのリスクを考慮した脆弱性の優先順位付けを取り入れる必要があります。あわせて、

リスク低減を継続的・測定可能かつ環境に即したものにできるセキュリティプラットフォームやソリューションが備える脅威インテリジェンスを、余すところなく活用すべきです。

TREND MICRO

〒160-0022
東京都新宿区新宿 4-1-6　JR 新宿ミライナタワー
https://www.trendmicro.com

トレンドマイクロはサイバーセキュリティのグローバルリーダとしてデジタル情報を安全に交換できる世界の実現に貢献します。私たちの革新的なソリューションはデータセンター、クラウド、ネットワーク、エンドポイントにおける多層的なセキュリティをお客様に提供します。

当社のリーダシップの根幹であるトレンドマイクロリサーチは、多くのエキスパートに支えられています。それは最新の脅威を発見し、重要なインサイトを公に共有し、サイバー犯罪の防止を支援することに情熱を注ぐ人材です。当社のグローバルチームは、日に数百万もの脅威を特定し、脆弱性の開示を先導し、標的型攻撃・AI・IoT・サイバー犯罪等における革新的な研究結果を公表しています。私たちは次に来る脅威を予測し、セキュリティ業界が進むべき方向を示しうる示唆に富んだ研究成果を提供するため、継続的に取り組んでまいります。

このような知見をもっとご覧になりたい方へ

research.trendmicro.com/securitynews

TrendAI™

TrendAI™ は、AI セキュリティのグローバルリーダーであり、Trend Micro のエンタープライズ事業部門として、AI の完全な可視化と統合されたセキュリティにより、組織に信頼をもたらし、イノベーションを促進し、リスクを排除します。

TrendAI™ は、185か国の大手企業や政府機関から信頼され、アイデンティティからインフラ、データに至るまで、組織全体を保護します。

AI Fearlessly.

詳細はこちら：**trendaisecurity.com**