Rubrik Zero Labs

アイデンティティの危機

アイデンティティを悪用した脅威に対するレジリエンスの理解と構築

目次

概要

Rubrik Zero LabsとWakefield Researchは先頃、アイデンティティを悪用した攻撃からの保護および復旧の対策状況を把握するため、世界各地の1,625名のITおよびセキュリティリーダーを対象に調査を実施しました。Rubrikはバックアップデータに埋め込まれた脅威を調査するために、毎日**220万件のスナップショット**をスキャンしていますが、本調査はこれに加えて行ったものです。

クラウドへの移行、リモートワークの導入、そして現在ではエージェント型AIが発展していく中、従来のネットワークの境界は消滅しつつあり、アイデンティティはもはや単なる制御層ではなくなっています。アイデンティティは主要な攻撃対象領域になっており、脅威アクターはこれを兵器化してIT環境にアクセスし、攻撃の過程で「寄生」しています。今日発生しているの侵害の圧倒的多数は、ネットワークの防御層を回避することよりも、信頼と有効な認証情報を悪用することが前提となっています。

ほぼすべての攻撃で、人間または非人間のアイデンティティの要素が、初回アクセス時、権限昇格時、あるいは水平移動の実行時のいずれの場合でも含まれているため、本調査の回答者の大多数（**90%**）が、アイデンティティを悪用した攻撃は自社組織にとって他に類を見ない最大の脅威であると回答しているのも当然です。

このレポートの目的は、重要な焦点領域と予想される対応タイムラインに注目し、組織がアイデンティティ攻撃に対抗できる能力を数値化することです。

最後に、以下を含むアイデンティティレジリエンスの必須要素を確認します。

人間と非人間のアイデンティティ両方を考慮に入れた、すべてのオンプレミスおよびクラウドのアイデンティティプロバイダー間でのリアルタイムの**可視性、対応、復旧**能力の連携

中核的なアイデンティティインフラストラクチャそのものを感染前の状態に迅速かつ確実に復旧する組織の能力に対する確信の構築

攻撃対象領域とアイデンティティ侵害の影響範囲を限定するための**ゼロトラストの原則**を通じたアイデンティティ強化とレジリエンス構築の導入

組織の全体的な**サイバーレジリエンスライフサイクル計画にアイデンティティレジリエンスを組み込む方法**

この包括的なアプローチによってのみ、組織はアイデンティティインフラストラクチャを強化し、起こり得るダウンタイムや収益の損失、評判の悪化を回避できます。

ここでまずは前回の調査から対前年比の傾向を確認します。

2024年と2025年の比較
調査傾向
(Wakefield)

90%

が過去1年間にサイバー攻撃を経験しています

2024年に少なくとも1回経験したと報告された割合と同じです

89%

のランサムウェア攻撃の被害者が、データを復旧するため、または攻撃を停止させるために身代金を支払いました

20%

が25回を超える攻撃を経験したと報告しており、2024年の18%から増加しています

100回以上の攻撃を経験した割合は11%で、2024年の8%からわずかに増加しています

復旧時間に対する確信度が低下

2025年では、サイバーインシデントから12時間以内に完全復旧できると考えている割合は28%にすぎず、2024年の43%から減少しています

77%

が前年よりも規模が大きいクラウド環境を管理していると報告しました

58%

が、今後1年間に直面するサイバー攻撃の半数以上がエージェントAIによるものになると考えています

58%

が、侵害後にサービス運用を完全に回復するには2日以上かかると考えています

アイデンティティの侵害：

脅威アクターの環境寄生型攻撃の足がかり

今日のサイバーインシデントのほとんどには、何らかの形でアイデンティティの侵害がかかわっています。
しかし、アイデンティティは、標的そのものではなくツールとして捉えるべきです。
現在、アイデンティティは脅威アクターの最終目的ではなく、本来の目的（監視、データ窃取、恐喝など）を達成するための手段となっていることがほとんどです。

現在、基本的なWebアプリケーション攻撃の

86%

が、盗んだ認証情報を利用しています

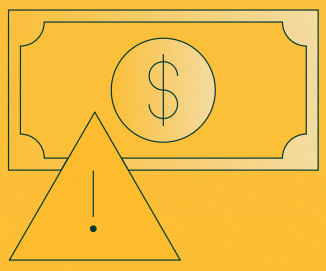
(Verizon)[1]

CrowdStrikeによる検知の

79%

が「マルウェアフリー」です。これは攻撃者が従来型のマルウェアを展開することなく、ログインしていたということです

(CrowdStrike 2025)[2]



侵害あたり

4.67

万ドル（USD）

攻撃者が侵害した認証情報を利用した場合の平均コスト

(IBM)[3]

アイデンティティ侵害は侵入経路となり、脅威アクターに次の行為を許してしまいます。

管理ツール、SaaSサービスなどの正規のプロセス、あるいはアイデンティティワークフロー自体を悪用することで、検知を回避する「環境への寄生」

以前に侵害した認証情報を使用した更なる攻撃の実行

組織の正規のガバナンスおよび可視性の外部に「シャドーアイデンティティプラットフォーム」（不正なテナントやアイデンティティインフラストラクチャ）を作成するなどにより、標的の環境内で持続性を維持

[1] https://www.verizon.com/business/resources/reports/dbir/
[2] https://www.crowdstrike.com/en-us/resources/reports/global-threat-report-executive-summary-2025/
[3] https://www.ibm.com/reports/data-breach

侵害の標的になっているのは人間のアイデンティティだけではありません。非人間アイデンティティ（NHI）も攻撃を受けています。これらは一般的に、自動化されたITプロセス、証明書、コンテナ、自動化ツール、サービスアカウント、AIエージェントを認証するために使用されるAPIトークンです。

NHIは現在、82対1の割合で人間ユーザーの数を上回っているとする指標もあります。[4]脅威アクターの攻撃対象領域が劇的に増加しており、エージェント型AIの導入がさらに進むにつれて、増える一方となります。

脅威アクターは目的に応じて、人間のアイデンティティとNHIを異なる理由で標的にします。それぞれのカテゴリを防御するために、どの目的でどのアイデンティティが狙われるのかを理解することが極めて重要です。

	人間のアイデンティティ （従業員アカウント、管理者ログイン情報など）	**非人間のアイデンティティ** （サービスアカウント、APIキー、トークンなど）
主要な目標	**初期アクセス**、偵察、既存のユーザーレベル権限の活用	ステルス、**永続化**、高度なシステムアクセス
主要なリスク	**ソーシャルエンジニアリング**に対する脆弱性	**設定ミス**に対する脆弱性、指数関数的に増殖する傾向
防御回避	**維持が困難：**人間のアカウントは通常、MFA、アクセスポリシー、不可能な移動などの行動分析によって保護されています	**維持が容易：**多くの場合、NHIはMFAが設定されておらず、監視制御が少ないため、自動化された活動は、正規のバックグラウンドノイズに簡単に紛れ込むことができます
権限	権限は通常、エンジニアや営業担当などの**特定のロール**に関連付けられています	多くの場合、権限はシステム**全体に及んでおり、過剰**です。例えば、システム内のすべてのデータベースを読み取れるサービスアカウントがあります
永続化	**無効化が容易：**人間のアカウントは、インシデント発生時に数分でロックアウトし、パスワードを変更し、セッションを終了させることができます	**無効化が困難：**NHIは長期間存続し、忘れられたり、重要な業務に必須であったりするため、変更が困難で混乱を招きます

[4] https://www.cyberark.com/resources/white-papers/2025-identity-security-landscape-executive-summary

脅威アクターのアイデンティティへの執着

人間のアイデンティティと非人間のアイデンティティのどちらも、最近注目を集めた
サイバーセキュリティインシデントの多くで中心的役割を担っていました。

Entra IDおよびn0Authを水平移動に使用

2025年6月、Microsoftのクラウドベースのアイデンティティおよびアクセス管理（IAM）サービスであるEntra IDに、依然として脆弱性が含まれていることが確認されました。この脆弱性は、脅威アクターが侵害されたSaaSアプリケーションを起点に、組織の中核的なMicrosoft 365リソースへと展開し、企業の機密データへのアクセスを許可することができてしまうというものです。[5]

1つのメール属性を、標的のアドレスと一致するように操作するだけで、ユーザーは脆弱なSaaSアプリケーションに属する「Microsoftを使用してログイン」機能を使用し、アクセス権を得ることができてしまいます。アプリケーションのアイデンティティアサーションロジックに対するこの攻撃は、迅速な水平移動と、SharePointやTeamsなどの中核的な企業向け生産性ツールへの自由なアクセスを可能にしてしまいます。

この欠陥は元々2023年に警告が出されていましたが、それでも数万のSaaSアプリに影響を与えたと考えられています。n0Authでは、テナント側での修復が必須であるため、中央で修正を一括で行うことはできません。この事例では、Microsoftの利用者が多かったことにより、このアプリケーションレベルのアイデンティティの欠陥の影響範囲が大幅に広がりました。攻撃者は、多くの場合権限昇格を目的として、2025年を通してEntra IDを狙い続けました。

ToolShell攻撃でオンプレミスのSharePointサーバーが標的に

2025年7月のToolShell攻撃で悪用されたような重大な脆弱性は、鍵認証などのアイデンティティの側面が、いかにして脅威アクターに操作されうるのかを示しています。この事例では、国家による支援が疑われている脅威アクターが、価値の高い標的に属するオンプレミスのSharePointサーバーを認証するために使用されているマシンの鍵を窃取することを優先しました。これはおそらく、侵害した環境内から長期にわたるスパイ活動を行うためです。[6]

ここに、スパイ行為などの目的で、継続的な攻撃を実行しようと目論む意欲的な脅威アクターにとってのNHIの重要性が表れています。鍵はトークンよりも持続性があるため、セキュリティチームがセキュリティインシデント後の迅速なローテーションや、ToolShell攻撃を可能にしている類のCVEの検知を優先することが重要になります。

Scattered Spiderが人間の心理をハッキング

Scattered Spiderグループは、頻繁にITスタッフやヘルプデスクのスタッフを装い、個人を騙して認証情報を開示させたり、多要素認証（MFA）を回避したりしています。こうした試みが成功した根本的要因は、人間の心理を悪用したことにあります。特に、問題をすばやく解決しなければならないというプレッシャーにさらされることの多いサポートチームの、対応力および固有の共感性をついています。伝えられるところによると、2023年8月、同グループは洗剤メーカー大手Cloroxのサードパーティのヘルプデスクを呼び出し、パスワードの設定を要求して3億8000万ドルの損害を生じさせました。[7]

Scattered Spiderの攻撃の成功は、ソフトウェアのゼロデイ脆弱性を検知することではなく、ソーシャルエンジニアリングにより初回アクセス権を獲得し、次にPowerShellやSaaSサービスなどのネイティブツールを悪用するという方法によるものです。これは、技術ソリューションだけでは保護が十分ではないことを意味します。代わりに、組織は継続的な適応型のセキュリティ意識向上トレーニングやアイデンティティインフラストラクチャのレジリエンス構築など、人間中心のセキュリティに投資する必要があります。

[5] https://www.infosecurity-magazine.com/news/microsoft-noauth-flaw-2025/
[6] https://www.recordedfuture.com/blog/toolshell-exploit-chain-thousands-sharepoint-servers-risk
[7] https://www.cybersecuritydive.com/news/clorox-380-million-suit-cognizant-cyberattack/753837/

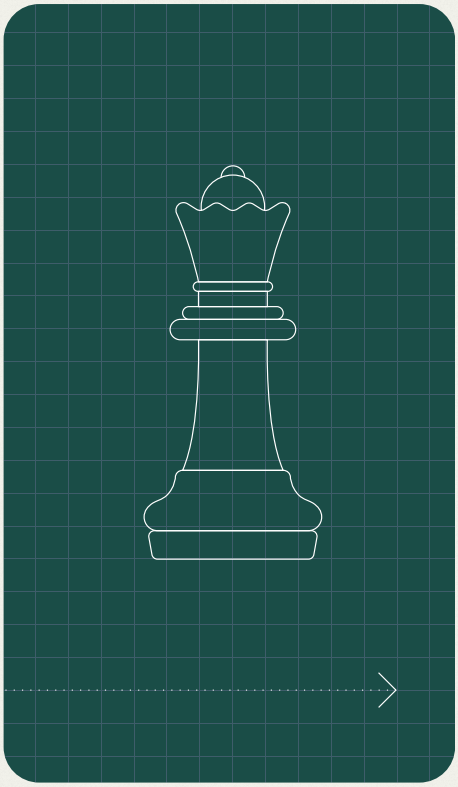
アイデンティティの悪用により もたらされた混乱

アイデンティティの侵害は、攻撃者に「王国への鍵」を与えてしまうようなものです。脅威アクターはその環境に居座り、正規のツールを悪用し、監視の実行やデータの窃取を行うことができてしまいます。

一度侵害に成功するだけでどれだけの損害を生じさせられるのかを評価すれば、
アイデンティティへの注目度が高まった理由がよくわかるでしょう。

影響のカテゴリ	結果	影響を受ける組織のアセット
データ侵害	PII、知的財産、財務データ、その他の貴重なデータの流出	顧客データ、従業員データ、企業秘密、競争優位性、財務記録
財務上の損失	直接的な詐欺被害、インシデント対応費用、法務費用、規制当局からの罰金	予算、収益、法的リソース
イメージの悪化	顧客の信頼喪失、ブランドの毀損、否定的な評判	ブランド価値、顧客およびパートナーとの関係、市場価値
運用の混乱	システムダウンタイム、サービス中断、アカウントロックアウト	収益、ITインフラストラクチャ投資、セキュリティ管理
永続化と権限昇格	バックドアの設置（サービスプリンシパル、フェデレーション改変）、シャドウアイデンティティプラットフォームの作成	ITインフラストラクチャ、アイデンティティおよびアクセス管理、セキュリティ管理
コンプライアンスと法的リスク	データプライバシー規制（GDPR、CCPA）違反、訴訟	法的リソース、コンプライアンス部門
サプライチェーンの侵害	連鎖的な攻撃につながるビジネスパートナーや他の第三者への侵害	パートナーエコシステム、サプライチェーンの完全性、評判

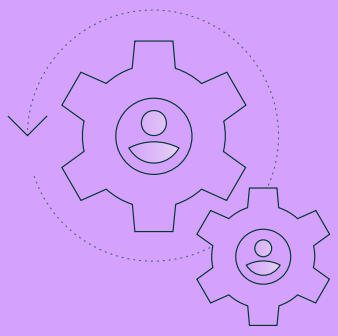
組織の反応



調査対象のITおよびセキュリティリーダーの

90%

は、アイデンティティを悪用したサイバー攻撃が、組織に対する一番の脅威であると回答しました。

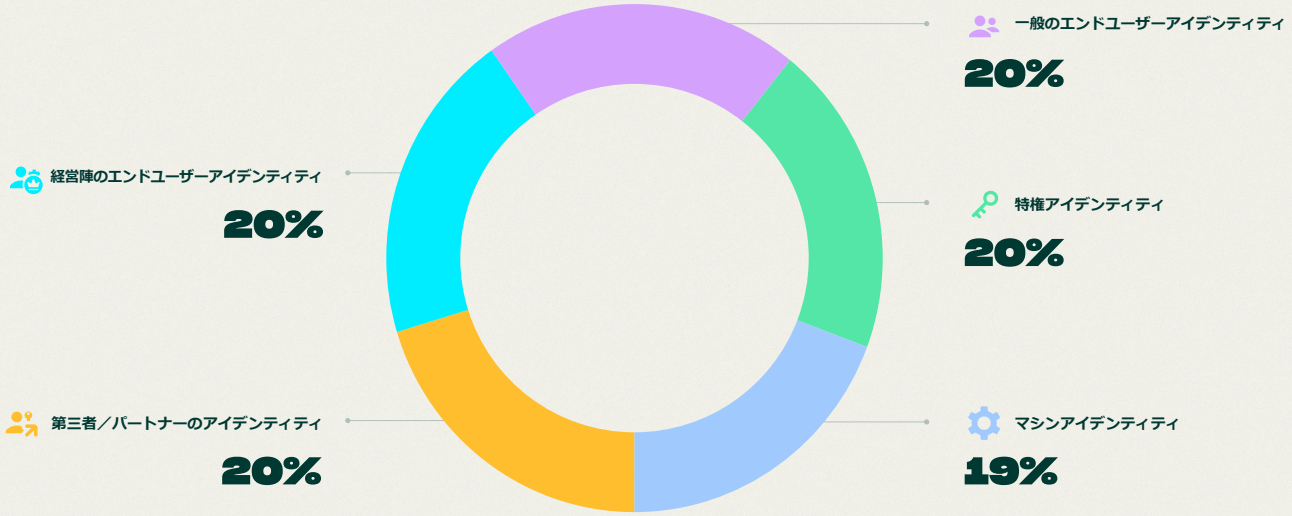


リーダーの

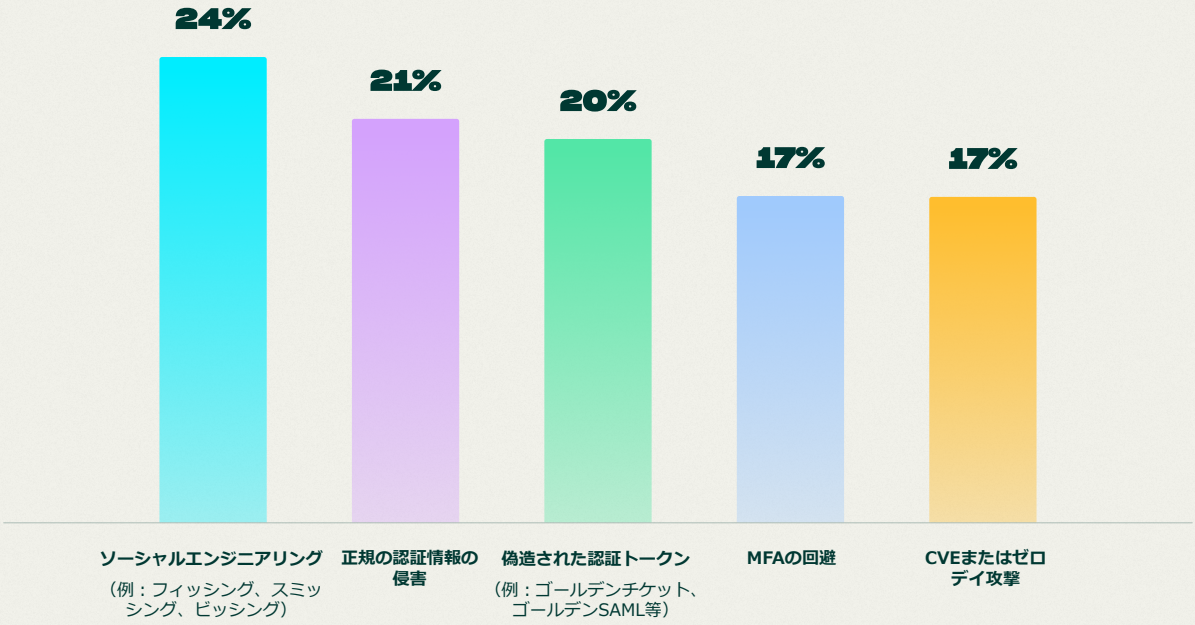
89%

は、今後12か月の間に、デジタルアイデンティティ管理、アイデンティティインフラストラクチャ、およびアイデンティティセキュリティの運用または改善のために専門家を雇用しようと計画しています。

侵害が最も懸念されるアイデンティティの種類



リーダーたちはかつて、特権アカウントのみを優先していましたが、現在ではすべての
アイデンティティが極めて重要であるという意見で明確に一致しています。これは、最初の権限が
何であるかにかかわらず、侵害されたアカウントはどれでも、攻撃者が水平移動
および権限昇格を行うための危険な足がかりになることが認識されているということです。



また、セキュリティの優先事項が変わってきたこともデータで示されています。
ソーシャルエンジニアリング（24%）がトップではあるものの、MFAの回避（17%）と
偽造された認証トークン（20%）が、現在ではゼロデイ脆弱性（17%）並みに
危険とみなされるようになりました。

これは重大な変化です。高度なアイデンティティ偽造による「ログイン」攻撃が、
従来の「侵入」型エクスプロイトよりもまん延している脅威であるという
新しい現実をリーダーたちが認識し始めたことを示しています。

Mandiantは、対応したクラウド侵害の件数が2024年に史上最多に上ったと報告しており[8]、その一番の理由として、アイデンティティソリューションのセキュリティ制御が十分ではないことを挙げています。アイデンティティが攻撃経路へと進化する中で、アイデンティティアクセス管理（IAM）ソリューションは最新の手法に追いつけずにいます。

これには、以下のような原因が考えられます。

アイデンティティは多面的である

特権アクセス管理（PAM）、ロールベースアクセス制御（RBAC）、そしてAPIセキュリティはすべてIAMの下位区分であり、おそらく単体のベンダーにより提供されているため、攻撃対象領域が広がってしまっています。

新しいタイプのアイデンティティが常に登場している

NHIの一種であるAIボットやエージェントは5年前には存在していませんでした。また、APIはこれまでになく利用されています。エージェントによりマシン間アイデンティティの数が爆発的に増大しますが、多くの場合、人間のアカウントに適用されるライフサイクル管理（プロビジョニング、ローテーション、プロビジョニングの解除など）のような成熟性には欠けています。

脅威アクターによるアイデンティティの悪用手段が進化している

エンドポイントと境界の防御効果が高まるにつれて、脅威アクターはますます「侵入ではなくログイン」による認証情報の窃取を優先するようになっています。

クラウドにより新たなリスクが生じている

クラウドネイティブIAMの複雑さと粒度により、人的ミスや設定ミスが生じやすくなっています。攻撃者は、こうした過剰な権限が付与されたロールや、誤って設定された公開権限などの設定ミスを積極的に探しています。

[8] https://services.google.com/fh/files/misc/m-trends-2025-en.pdf

したがって、以下の結果は当然のことと言えるでしょう。

87%

のITおよびセキュリティリーダーは現在、IAMプロバイダーを乗り換えることを計画しているか、すでにそのプロセスを開始しています。

そのうちの

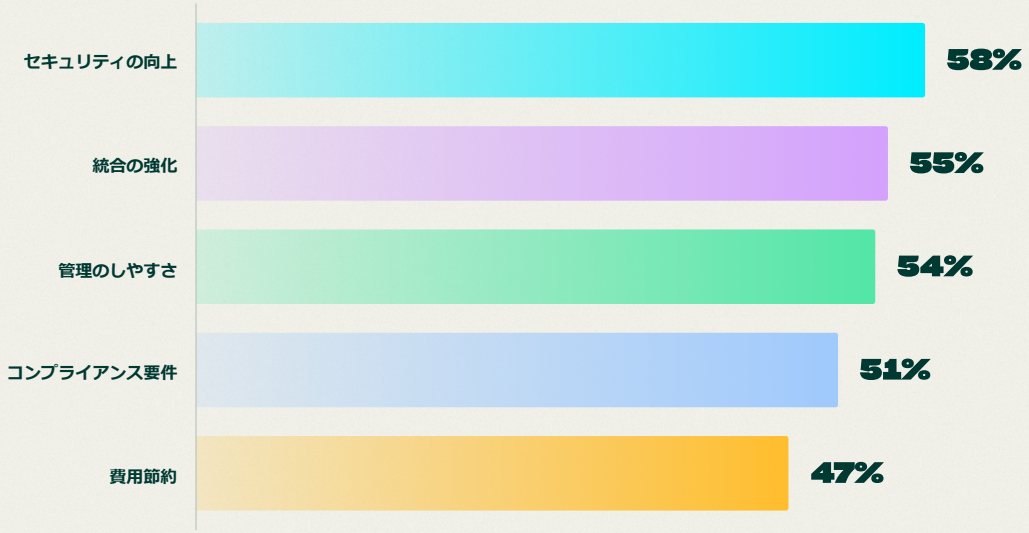
58%

が、セキュリティ上の理由によるものであり、多くの単一ソリューションではアイデンティティを悪用した脅威に対処するための機能セットが欠けていることを示唆しています。

60%

60%が過去3年以内にIAMプロバイダーを乗り換えたにもかかわらず、このような結果になっています。

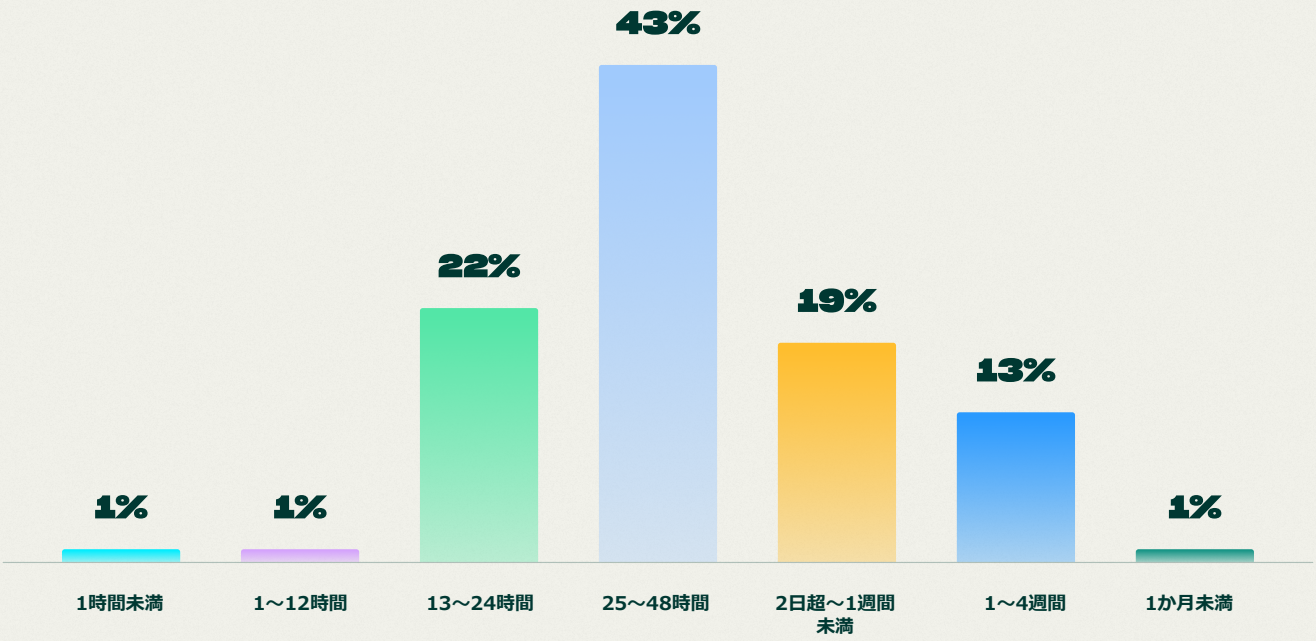
アイデンティティプロバイダーの乗り換えに至る主な理由



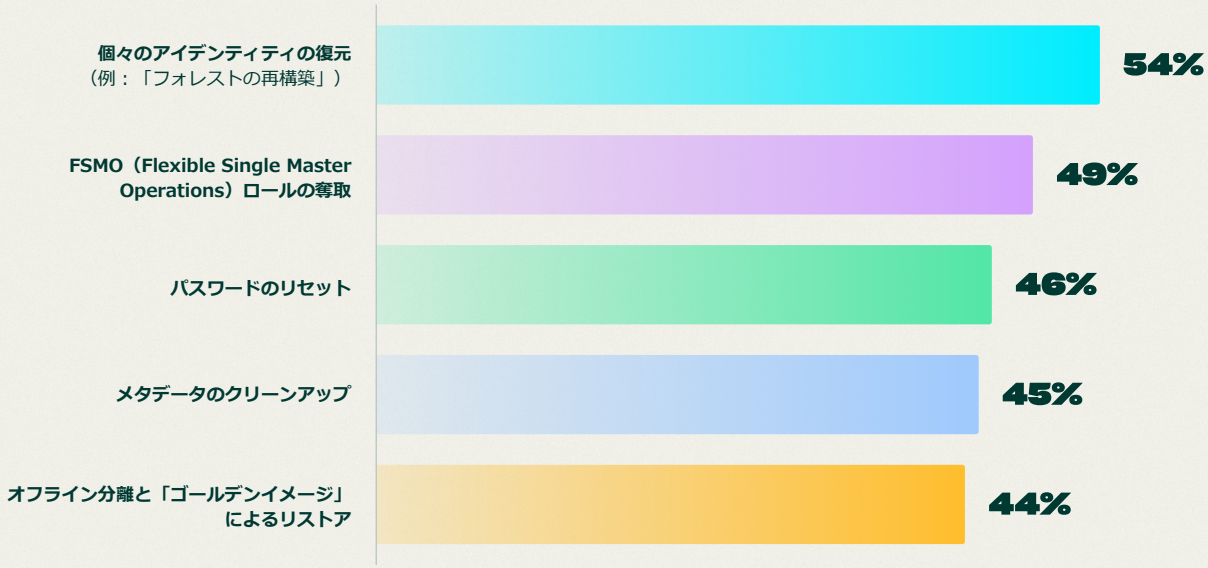
さらに懸念すべきことは、侵害後にアイデンティティインフラストラクチャを復旧するためにかかる時間です。ダウンタイムにより生じるコストが**1分あたり6,000ドル**[9]に達しうる場合、組織は手動の復旧プロセス（**54%**）に依存していれば、すぐに経費の増大に直面するでしょう。

[9] https://www.isaca.org/resources/news-and-trends/industry-news/2024/centralized-services-and-their-impact-on-business-continuity

アイデンティティインフラストラクチャの侵害を受けてから復旧するまでの所要時間



手作業の復旧手順が必要なプロセス



興味深いことに、**回答者の89%はAIエージェントをアイデンティティインフラストラクチャに部分的にまたは完全に組み入れています。**こうしたNHIの新しい形態も、大規模に、かつライフサイクル全体を通じて保護し、兵器化を防ぐ必要があります。すでに、回答者の半数以上（**58%**）が、来年に**直面するサイバー攻撃の半数以上がエージェント型AI主導のものになると推定しています。**

どの脅威アクターがどのアイデンティティを、どんな理由で標的としているのかを把握できていないことが、組織の対策と復旧時間を測定し、短縮する能力を妨げているもう1つの要因です。

復旧はなぜ長期化するのか

データ主導の答えはMTTR

多くの場合、組織はサイバーレジリエンスに向けて努力しますが、
それを数値化することに苦戦しています。
サイバー脅威の予測、対抗、復旧、そしてそれに適応する
能力はどのように測定できるのでしょうか。

目標復旧時間（RTO）および目標復旧ポイント（RPO）は従来からある指標ですが、
これらでは、全容がわかりません。インシデントのRTOは4時間だったとしても、
実際の復旧に32日間かかっている場合があるかもしれません。RPOは分単位で
測定されていたとしても、銀行などの業界では、数十万件のトランザクションにかかわる
データが失われてしまうこともあります。これらの例では、復旧オペレーションチームが
かなり非現実的な目標を設定していたことがわかりますが、その理由はわかりません。

さらに、多くの業界ではさまざまな指標に依拠しているため、業界をまたいでの復旧時間に
関する標準的な理解を妨げているおそれがあります。脅威が検知されたタイミングで時間の
計測を止める人もいれば、脅威が完全に消滅してはじめてそうする人もいます。このような
違いがあることで、組織のサイバーレジリエンスを真に理解することが難しくなっています。

Rubrik Zero Labsが**平均修復時間（MTTR）**を業界標準として提案しているのは
そのためです。フェーズを認識した、組織のサイバーインシデントからの
復旧能力を測定するデータ主導の指標です。

MTTR分解のための新しいフレームワーク

MTTRは単一の指標ではありません。個別のフェーズに分解できる、複数のステップを経るプロセスで、有意義な知見を獲得し、改善の余地のある分野を特定できます。この復旧モデルは、以下のように構成されています。

検知	これは、サイバー攻撃であろうと誤削除であろうと、あらゆるインシデントの出発点となります。
範囲の特定	この段階では、影響を受けたすべてのシステムとアセット、またそれらの依存関係を把握するための包括的な取り組みが行われます。どのアプリケーションとデータベースが互いに依存しているかを把握することが重要です。
クリーンな復旧ポイントの特定	通常、これは最も時間がかかり、最も重要な段階です。運用をリストアするための、マルウェアのない信頼できるバックアップを探すのにかかる時間です。従来は、専用の「クリーンルーム」ラボ環境のセットアップに数週間～数か月を要していました。クラウドベースのインフラストラクチャや自動化などの最新ツールにより、この時間は大幅に短縮されつつあります。
リストア	これは、実際にデータをリストアする作業です。これに数週間かかる場合、スループットの問題を示唆している可能性があります。つまり、高リスクの復旧時間を短縮するためにインフラに投資すべきという、データに基づく論拠となります。現在の組織が保有するデータ量を考えると、この段階は、クリーンな復旧ポイントの特定を抜いて、最も時間のかかる復旧ステップになる可能性があります。
検証	アプリケーションの健全性とデータアクセスを確保するには、どのくらい時間がかかりますか？必要な人間および非人間のアイデンティティが正しく機能し、通信しているかを確認するには、どのくらい時間がかかりますか？

各フェーズを個別に測定することで、組織は、文脈に紐づかない単一の数値を脱却し、ボトルネックを特定してデータ主導の意思決定を下すために必要な粒度の高い知見を得ることができます。

段階的な指標	計測開始	計測停止	説明
平均検知時間（MTTD）	攻撃の影響が生じた時刻またはアラートが発生した時刻	既知の復旧範囲の確認時	検知、異常分析、SIEMの相関により計測します
平均範囲特定時間（MTTS）	検知の確認	復旧オブジェクトリストのロック	グローバル検索、データ分類、SLAメタデータでこの段階を推進します。
平均クリーンスナップショット選択時間（MTTCS）	範囲のロック	クリーンで侵害されていないスナップショットの特定	不変性、脅威スキャン、スナップショット健全性スコアリングにより、この時間を短縮します
平均リストア時間（MTTR）	リストアトリガー	データがワークロードで利用可能になる	即時復旧、ライブマウント、およびクラウド災害復旧のオーケストレーション機能により促進します
平均検証時間（MTTV）	データアクセスの準備完了	アプリケーションの健全性が確認される	アプリケーション整合性、自動化プレイブック、リストア後のマルウェアスキャンによって実現します

総MTTR（運用） = MTTD + MTTScope + MTTCS + MTTRestore + MTTValidate

MTTRが重要である理由

今日の組織は、バックアップデータ内から得られる知見を見落としがちです。
MTTRは、この「重要資産」を、復旧を確実にするだけでなく、
レジリエンスを測定するためのツールに変換するのです。

突き詰めると、MTTRとは、以下の継続的な成熟度評価サイクルのフェーズの1つです。

1

レジリエンスの特定

リスク評価と同様の高性能な採点システムにより、最重要のアプリケーションおよび起こり得る攻撃シナリオをもとに、攻撃に対する現在の耐久力を把握します。

2

存続できる最小限の事業の確立

調査やアプリケーションの重要度別のリストを超えて、継続性を維持するのに必要な必須のアプリケーションとデータベース、およびその依存関係を、ミッションクリティカルを優先することにより完全に把握します。

3

復旧能力の検証

真の危機シミュレーション（現実的で対話型の訓練を模したソフトウェア主導のシナリオ）を通じて、将来の改善のための基準となる、平時での取り組みの測定可能な復旧時間の指標を生成します。

4

分析と改善

復旧対応の各フェーズで、ボトルネックが生じている場所および対処方法の特定を行います。たとえば、ミッションクリティカルな復旧データを20TBから2TBまで削減すれば、復旧時にスループットを大幅に減らすことができます。

重要なことに、MTTRデータを匿名化し集計することで、組織は業界や地域の同業他社に対する強力なベンチマークを作成することができます。これにより、セキュリティ、IT、復旧オペレーションの各チームは復旧速度や信頼性といった重要業績評価指標に対する共通の理解を得られるため、リーダーがサイバーレジリエンスのための資金を確保し、サイロ化の解消に貢献できるようになります。

アイデンティティレジリエンスの教育：

推奨事項と対応能力

アイデンティティを単なる保護対象の資産と捉えないでください。今日の企業において、アイデンティティは安全対策上のあらゆる意思決定に必要な重要な制御プレーンになると考えるべきです。

単なるエンドポイントとネットワーク中心の防衛策から、包括的なアイデンティティ統制、特権アクセスの管理、そして高度な認証ソリューションへと投資先をシフトする必要があります。今や、侵害を受けたアイデンティティは、組織の最重要資産に直接つながる、しかし見過ごされることの多い経路となります。アイデンティティが最も重要な制御ポイントになるのはこのためです。

アイデンティティを悪用する攻撃の件数を考慮すると、
組織は次のことを優先する必要があります。

アイデンティティの可視性と復旧

クラウドのAPIキーが侵害された場合、どのシステムを切断する必要があるでしょうか。OktaまたはActive Directoryの管理アカウントが乗っ取られた場合、すばやく問題の切り分けを行い、影響を受けたユーザーの再認証を実行できますか。この質問の答えを理解し対処策を講じるには、ハイブリッド型のアイデンティティ環境全体に対するリアルタイムの可視性と復旧機能が必要になります。

アイデンティティレジリエンスの構築

レジリエンスとは、迅速かつ確実に回復する能力のことです。Active Directoryまたはクラウドディレクトリのデータの安全なオフラインバックアップは、アイデンティティサービスが暗号化または消去された場合に、それらをすばやく再構築するために必要不可欠となります。復旧のステップをセキュリティと並行して計画することで、アイデンティティの侵害から生じるダウンタイムと金銭的損害を大幅に低減することができます。

ゼロトラストの原則に則った攻撃対象領域と影響範囲の制限

アイデンティティは、境界と考えてください。すべてのアクセス要求を、ネットワークの内外を問わず、常に認証、承認、暗号化する必要があります。実質的には、強力なMFA認証、条件付きアクセスポリシー、そして設計段階での最小権限アクセスを実施することになります。

ゼロトラストをアイデンティティのセキュリティに適用する

最小権限とロールベースのアクセス制御（RBAC）

すべてのユーザーとデバイスには、場所に関係なく、具体的なジョブの実行に必要な最小限のアクセス権のみを付与します。

ジャストインタイム（JIT）アクセス

昇格権限またはアクセス権の付与は、ユーザーが慎重に行うべきタスクの完了に必要な期間に限定して行います。その後、権限は自動的に取り消されるようにしておきます。

継続的な検証

強力なMFAに加え、ユーザーのアイデンティティ、デバイスの態勢、状況（場所や時間など）を常時監視・再評価して、セッション全体を通じてアクセス権の維持または取り消しを行います。

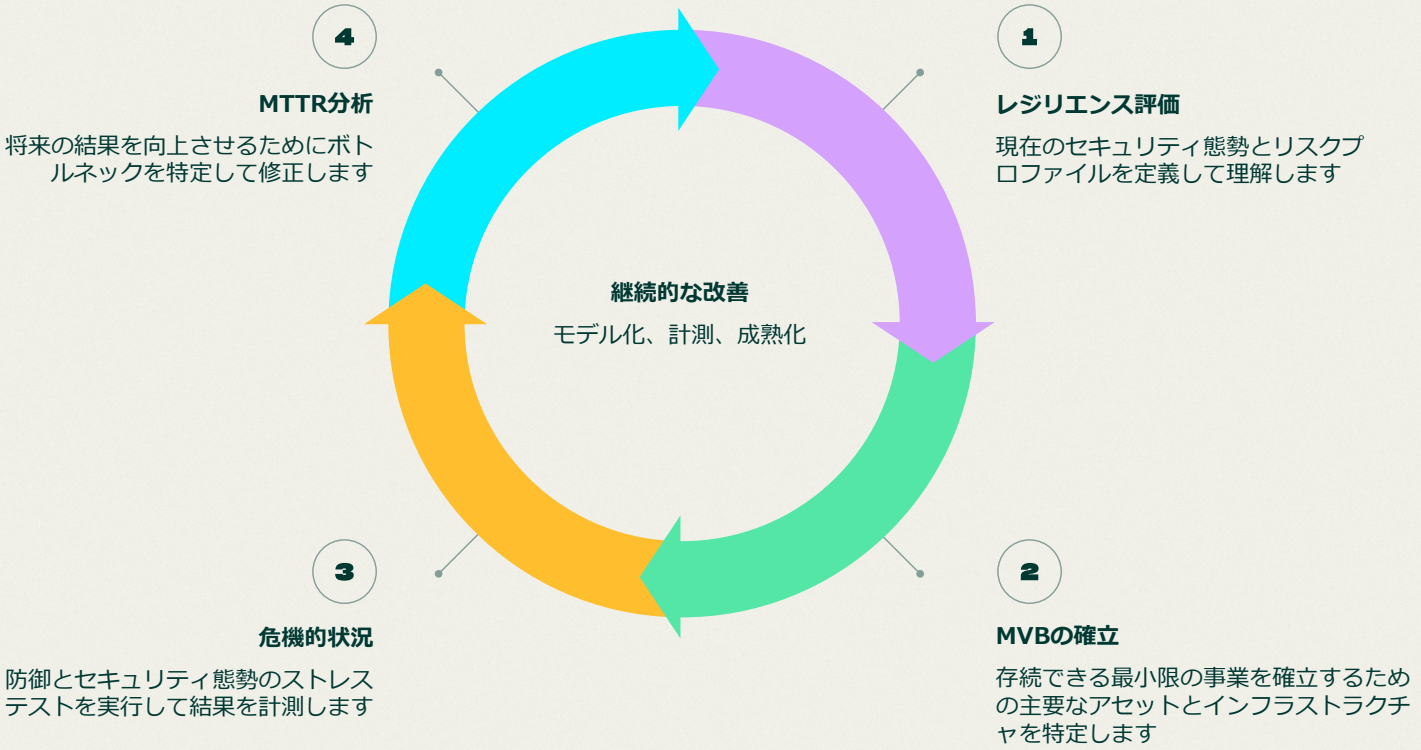
マイクロセグメンテーション

ネットワークを細分化することで、潜在的な侵害を封じ込め、許可されていないユーザーが侵害対象の貴重なリソースを求めて、セグメントの横断や水平移動を容易には行えないようにする必要があります。

サイバーレジリエンスのライフサイクル

真のサイバーレジリエンスは、**リスク管理、事業の継続**、および**インシデント対応**を1つの戦略に統合することにより、サイバーセキュリティ以上のものとなります。目的は、ただ攻撃を防ぐだけではなく、攻撃に耐え、影響を最小限に抑えて迅速に回復することです。

サイバーレジリエンスのライフサイクル



サイバー攻撃の予測、抵抗、復旧、および適応のためのNISTのガイダンス[10]に準拠しているRubrik Zero Labsのフレームワークは、レジリエンスを実務担当者にとって運用可能なものとし、上級管理者にベンチマークと改善指標を提供することを目指しています。

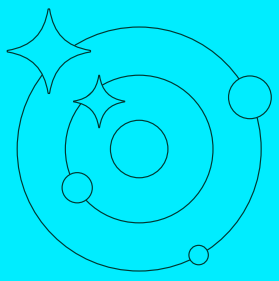
アイデンティティレジリエンス計画を、サイバーレジリエンス強化のためのより広範な取り組みに組み込むことで、組織は混乱を最小限に抑え、ビジネスクリティカルな資産を保護し、大切なステークホルダーからの信頼を得るための有意義な一歩を踏み出すことになります。

[10] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf

データおよび調査手法

Rubrik Zero Labsは、組織のデータセキュリティリスクの低減を目的とした、実用的で公正な知見の提供に取り組んでいます。

この目的を達成するため、Rubrikは次の3つを主な情報源としています。

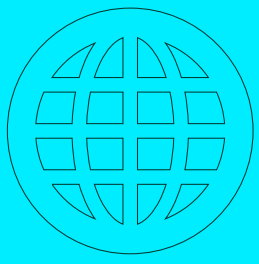


Rubrikテレメトリー

標準的な組織のデータ環境と関連するリスクについての分析情報を取得するため、Rubrikのテレメトリーを採用しました

独立した調査

Wakefield Researchを通じて得た1,600人以上のIT／セキュリティチームのリーダーによる視点を提供しています



組織に貢献

定評あるサイバーセキュリティ企業および機関による調査結果を提供しています