

COHESITY

アイデンティティ ティレイヤーは

サイバー攻撃の最前線



セキュリティおよびITリーダーがアイデンティティインフラを復旧できることを**証明**しておくべき理由

はじめに

エンタープライズアイデンティティは、本来、業務をシンプルにするためのものでした。組織がデジタルアクセスの一元管理を始めたのは1960年代後半から1970年代初頭で、誰がアクセスでき、何にアクセスできるのかを1か所で決定できるようになりました。その後、LDAPやActive Directoryなどのプラットフォームによって、この考え方はネットワーク全体の信頼できる唯一の情報源へと発展しました。このアプローチは非常にうまく機能しました。

そこがまさに問題なのです。

この信頼できる唯一の情報源が、今や最も容易な侵入口になっています。攻撃者はもはや侵入しようとはしません。盗んだ認証情報と正当なアクセス権を使ってログインし、そのまま最も重要なシステムへと入り込みます。何も検知されません。アラームも鳴りません。攻撃者は従業員が毎朝使うのと同じ入口を使っています。そのため、これは多くのセキュリティプログラムが対処するよう設定していたものとは根本的に異なる問題です。

長年にわたり、組織は侵入者を締め出すための壁、つまり境界を中心に防御を構築してきました。壁は今でも存在しますが、攻撃者はもはや壁を乗り越えようとはしていません。**アイデンティティインフラを侵害するほうが容易で、気付かれにくく、成功率も高いため、アイデンティティはネットワーク境界に代わって攻撃の中心となっています。**多くのセキュリティスタックは、もともとこの領域で戦うようには設計されていません。

数字を見れば明らかです。2024年には、攻撃の79%がマルウェアを使用しないものでした。検出すべきウイルスはなく、ソーシャルエンジニアリング、盗まれた認証情報、信頼されたリモートツールが検知をすり抜けていました。2025年にはこの数字が82%に上昇し、攻撃者は有効な認証情報、信頼されたアイデンティティフロー、承認済みのSaaS統合を積極的に悪用して、検知されることなくドメイン間を移動しています (CrowdStrike Global Threat Report)。この傾向が示す方向は明らかです。

今や、本格的なセキュリティプログラムは、この受け入れがたい現実から出発しなければなりません。あらゆるアクセスを制御するために構築したシステムが、いつの間にかあらゆる場所への最も容易な侵入口になっています。だからといって、パニックになる必要はありません。何よりもまずアイデンティティを保護し、確実に復旧できることを証明しておく必要があります。

エンタープライズアイデンティティが攻撃される理由

攻撃者にとって、アイデンティティは企業内で最も価値が高く、最も少ない労力で狙える標的です。たった1つの認証情報を侵害するだけで、その先にあるすべてのものにアクセスが可能になるからです。アイデンティティは、単なる攻撃経路の1つではありません。現代の攻撃者が積極的に狙っている攻撃経路そのものです。

ただし、ここに問題があります: 現在のセキュリティスタックのほとんどは、この攻撃を阻止するようには設計されていません。EDR、ファイアウォール、ネットワークセグメンテーションはいずれも、侵入者を検知するためのものであり、有効な認証情報でログインした人物を疑うようには設計されていません。防御システムから見れば、攻撃者は正規の従業員とまったく同じに見えます。

しかも、この盲点はますます広がっています。多くのActive Directory環境は、数十年にわたって使用されています。長年にわたる応急的な修正、忘れられたアカウント、気付かれない設定ミスが、誰の目にも触れないところで積み重なっています。その積み重なりは、単なる技術的負債ではありません。鍵のかかっていない窓のようなもので、ここが攻撃者が真っ先に探す箇所です。

ハイブリッドアイデンティティは、この問題をさらに悪化させます。現在、多くの組織はオンプレミスのActive Directoryと、Entra IDやOktaなどのクラウドアイデンティティプロバイダーを併用しており、これらを接続するたびに攻撃対象領域が拡大します。さらに悪いことに、Entra IDやOktaの脆弱性は、しばしばActive Directoryに直接起因します。というのも、Active Directoryは通常、他のすべてのシステムが信頼する唯一の情報源だからです。基盤が破られれば、構造全体が揺らぎます。

ACTIVE DIRECTORYはエンタープライズアイデンティティの中核です

Active Directoryは25年以上にもわたってエンタープライズアイデンティティを支えており、現在も世界中の組織の90%で使用されています。ほとんどのクラウドアイデンティティプロバイダーはActive Directoryと連携または同期されているため、新しいプラットフォームを導入しても、Active Directoryは依然としてそれらすべてを支える基盤であり続けます。

実際:

- 人が操作する侵入攻撃の78%以上で、攻撃者はドメインコントローラーを侵害しています。
- そのうち35%では、ドメインコントローラーを起点としてランサムウェアが環境全体に拡散しています。

攻撃を受けた際、復旧の成否を左右するのは、多くの場合Active Directoryです。これが何を意味するか考えてみてください: 自社のバックアップソリューションにログインできなければ、何一つ復旧を開始できません。攻撃者はこの点を十分に理解しているため、バックアップシステムとActive Directoryを同時に攻撃するケースが増えています。両方を停止させられれば、もはや「最悪の一日」では済みません。人質を取られたような状況です。

そして、時間は容赦なく過ぎていきます。Active Directory構造全体の復旧には数日、場合によっては数週間かかることがあり、ダウンタイムが1時間延びるごとに、組織には最大73万ドルの損失が生じる可能性があります。[*\(Forrester, The Total Economic Impact™ of Quest Recovery Manager for Active Directory Disaster Recovery Edition\)*](#)。

従来のバックアップツールだけでは、この状況には対処できません。個々のドメインコントローラーやファイルをコピーすることはできても、Active Directoryの構造全体を再構築するために必要な、厳密な順序に従った一連の手順をオーケストレーションすることはできません。各構成要素をバックアップすることと、それらを元どおりに組み直せることは同じではありません。

サポートするデータ

32%

2025年上半期、アイデンティティベースの攻撃が増加。97%がパスワードスプレーまたはブルートフォース攻撃

(Microsoft Digital Defense Report 2025)

22%

の侵害で盗まれた認証情報が関与。特に基本的なWebアプリケーションへの攻撃では88%に盗まれた認証情報が関与

(Verizon 2025 Data Breach Investigations Report)

35%

のクラウドインシデントは有効なアカウントの悪用が原因

(CrowdStrike 2025 Global Threat Report)

アイデンティティは、現在そして将来にわたり、MVCと信頼の基盤となります

Minimum Viable Company (MVC) とは、存続し、必要不可欠な業務を維持するために必要な、組織の最小限かつ最も効率化された状態を指します。組織がサイバーインシデントに見舞われたとき、復旧できない原因は、バックアップの障害ではありません。すべてを一度に復旧しようとしたり、誤った順序で復旧しようとしたりすることが、失敗の原因となるケースが多くあります。

多くの組織が見落としているレイヤーの中心にあるのは、信頼と制御であり、アイデンティティはその両方が交わる中心に位置しています。企業全体へのアクセスを可能にするマスターキーなのです。信頼できるアイデンティティを確立できなければ、その他を安全にリストアすることもできません。

アイデンティティ/アクセス管理 (IAM) には、3つのコア機能があります:

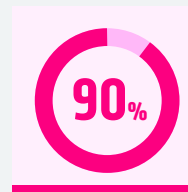
- **アイデンティティライフサイクル管理:** オンボーディング、ロールの更新、プロビジョニング解除を自動化し、従業員の入社、異動、退職に応じてアクセス権を常に適切な状態に維持します。
- **認証:** 通常は多要素認証 (MFA) とシングルサインオン (SSO) を使用して、ユーザーが本人であることを確認します。
- **認可:** 認証された各ユーザーに業務上必要なアクセス権のみを付与し、それ以外へのアクセスを制限します。

この3つの機能を組み合わせることで、Active Directory、Entra ID、Oktaは単なる裏方のインフラではなく、ビジネスを支える運用上の基盤となります。これらは、すべての従業員、すべてのアプリケーション、すべてのトランザクションを認証します。ここから、シンプルながら受け入れがたい1つの事実が浮かび上がります。アイデンティティインフラが停止すれば、ビジネスもそれとともに停止します。

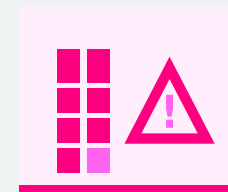
そして、この運用上の基盤は今後、さらに大きなリスクにさらされようとしています。組織がAIやエージェント型ワークフローの導入を急ぐ中、こうしたエージェントが安全に動作するにはアイデンティティインフラが欠かせません。この変化はすでにデータにも表れており、93%の組織が、パスワードのリセットやVPNアクセスなど機密性の高いセキュリティタスクにAIエージェントを使用しているか、使用を予定しています (Semperis, May 2026)。

ここで注目すべきなのは、こうしたエージェントが、タスクの実行や機密データへのアクセスを指示した従業員のアイデンティティを利用することが多いという点です。その一つひとつが、新たな鍵のセットになります。アイデンティティのセキュリティ確保、保護、復旧の重要性は、かつてないほど高まっています。

サポートするデータ



Active DirectoryとEntra IDは、世界の**企業**の**90%**以上で使用されています (Semperis)。



Active Directoryは**サイバー攻撃の10件中9件**に関与。設計に問題があるからではなく、広く普及していることが理由 ([Cohesity CERT](#))。

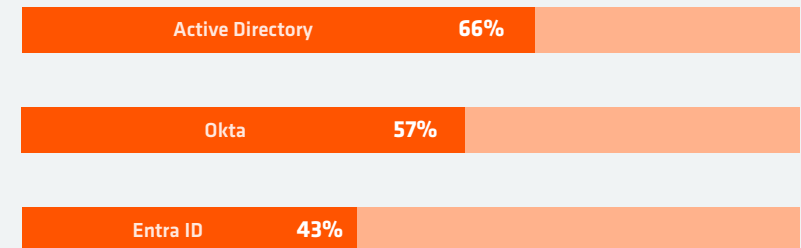
アイデンティティ、事業継続、サイバーレジリエンスの交点

従来の事業継続計画では、アイデンティティを電気のように扱っています。つまり、スイッチを入れれば利用できることが前提のインフラです。まさに、この前提が組織に壊滅的な被害をもたらします。アイデンティティを、もはや当然の前提とすることはできません。アイデンティティには、独自の復旧計画が必要です。

サイバーレジリエンスは、この前提を根本から覆します。アイデンティティを最初に攻撃されるもの、そして周囲のすべてが侵害された場合でも、(独立して、テスト済みで、隔離され、信頼できる状態で) 最初に復旧できなければならないものとして捉えます。「機能するはず」と「機能することを実証済み」の差が、攻撃後に組織が数日、場合によっては数週間を失う原因になります。ファイル自体は問題なくリストアできても、それを利用するユーザーを1人としてログインさせることができないためです。

セキュリティ、IT、経営の各リーダーが認識すべき点は明確です: 事業継続とサイバーレジリエンスを実現するには、プロアクティブなアイデンティティセキュリティとアイデンティティ復旧を、それぞれ独立した取り組みとして計画し、テストし、必要なリソースを確保する必要があります。ほかのすべてを復旧する過程で、これらも自動的に復旧されるとは決して考えないでください。

サポートするデータ



災害復旧計画にActive Directoryを含めている組織は66%、Entra IDは43%、Oktaは57%にとどまり、多くの事業継続計画でアイデンティティレイヤー自体が死角になっています (Semperis, Nov 2025)。



90%の組織がアイデンティティの脆弱性をスキャンしている一方、修復手順を整備しているのは51%、アイデンティティ復旧を自動化しているのはわずか57%です (Semperis, Nov 2025)。

対策を講じないことの代償

待つことの代償について考えてみます。待つことも一つの決断であり、しかも選択肢の中で最も高くつく決断からです。その代償は、金銭面だけでなく、業務面や評判の面にも及びます。

そのコストは1つではありません。コストは3つあり、それぞれが積み重なっていきます。

- 侵害によるコスト: インシデント対応、規制当局による罰金、法的リスク
- ダウンタイムによるコスト: 生産性の低下、売上機会の損失、アイデンティティレイヤーが無防備な間に繰り返される攻撃
- 信頼に関するコスト: サイバー保険料の上昇、経営幹部の責任、取引上のリスク

そして、待っている間もコストは増え続けます。アイデンティティの攻撃対象領域は、企業内でも特に狙われやすく、従来の防御策ではその変化に追いつくことができません。そのため、対策を先延ばしにするほどコストは増えていきます。対策しないまま四半期が過ぎるたびに、そのコストは増えていきます。先延ばしすることと、慎重さは同じではありません。それは、自ら抱えたわけでもない負債が、放っておくほど膨らんでいくようなものです。

サポートするデータ



3年間で、成功したアイデンティティ攻撃に**120万ドル**、ハイブリッドアイデンティティの手動監視に**10万9千ドル**、Active Directoryの手動復旧に伴う生産性低下とダウンタイムに**390万ドル**のコストを負う可能性があります。

(Forrester Total Economic Impact調査)。



データ侵害による世界平均コストは**444万ドル**ですが、認証情報を利用した侵害では約**467万ドル**に上り、特定から封じ込めまでに約292日を要します。これは、あらゆる攻撃ベクトルの中で最も長い期間です (IBM Cost of a Data Breach 2025)。



ランサムウェアをめぐる経済状況は変化しているものの、負担がなくなったわけではありません: 身代金支払い額の中央値は**11万5,000ドル**に低下し、被害組織の**64%**が支払いを拒否しました。その結果、身代金そのものではなく復旧に伴う運用コストを負担する組織が増え、アイデンティティを迅速に復旧する必要性がさらに高まっています (Verizon DBIR 2025)。



主要サイバー保険会社**8社すべて**が、保険引受時にアイデンティティ固有のセキュリティとレジリエンスを確認・検証しており、アイデンティティ強化を十分に実施していることを示せば、保険料の低下と補償範囲の拡大に直接つながります (Cohesity, “[Identity resilience is critical for cyber insurance](#)”)。

これらは、互いに無関係なデータではありません。これらは、侵害によるコストとダウンタイムによるコストの内訳です。さらに、保険会社が保険料をアイデンティティ態勢に直接結び付けるようになる中で、信頼に関するコストも加わってきます。アイデンティティへの対策を先延ばしにするほど、どのコストも増えていきます。いずれにしても、このコストを支払うことになります。問題は、今自分たちの判断で少額を負担するか、それとも後になって攻撃者に決められた条件で全額を支払うかです。

結論

現在、アイデンティティの侵害がほぼすべての重大なデータ侵害で確認されており、そのパターンは変わりません。攻撃者はただ侵入しようとはしません。有効な認証情報と信頼されたアイデンティティフローを使ってログインし、そうした攻撃を検知するようには設計されていない環境を、気付かれることなく移動します。そして、データを盗み、システムを掌握し、ランサムウェアをデプロイします。

しかし、これは避けられない事態ではありません。

数時間で復旧できる組織と、アイデンティティサービスへの信頼を取り戻すのに数週間かかる組織を分けるのは、運でも、費やした金額でもありません。違いを生むのは1つの判断です。必要になる前に、攻撃ライフサイクル全体を通じたアイデンティティレジリエンスを独立した取り組みとして構築していたかどうかです。

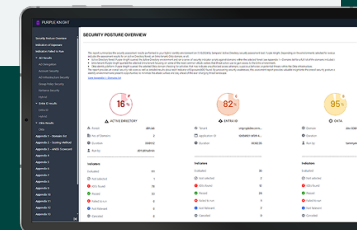
だからこそ、アイデンティティレジリエンスを選択肢ではなく、エンタープライズセキュリティの中核的な要件として扱う必要があります。アイデンティティは、企業への入口であり、基盤であり、同時に復旧のボトルネックでもあります。ポイントツールを寄せ集めるだけでは、十分な対策にはなりません。アイデンティティがいざというときにも使えると単純に想定している事業継続計画も、同じように不十分です。実際の攻撃にも耐えられるのは、必要になる前にテストし、有効性を実証しておいた戦略だけです。

幸い、今なら先手を打つことができます。サイバーレジリエンスを強化して、最も重要なアイデンティティシステムを保護しましょう。

そのために、Cohesityが支援します。

詳細はこちら: Cohesityによるアイデンティティレジリエンスの構築と強化について

無料のアイデンティティセキュリティ評価を受けて、 Active Directory、Entra ID、Okta全体の脆弱性やギャップを特定する





© 2026 Cohesity, Inc. All rights reserved. Cohesity、Cohesityのロゴ、SnapTree、SpanFS、DataPlatform、DataProtect、Helios、およびその他のCohesityのマークは、米国および/または海外におけるCohesity, Inc.の商標または登録商標です。その他の会社名および製品名は、関連する各企業の商標である可能性があります。本資料は、(a) Cohesityと弊社の事業および製品に関する情報を提供することを目的としています。(b) 本資料が作成された時点では、真実かつ正確であると考えられていますが、予告なく変更されることがあります。(c) 本資料は、「現状有姿」で提供されます。Cohesityは、いかなる種類の明示的または黙示的な条件、表明、保証も放棄します。