ハイブリッドActive Directory サイバーレジリエンスの現状

Questの顧客430社とActive Directory（AD）ユーザを対象とし、今日のADセキュリティに関する組織の課題を知る目的で行った最近の調査に基づくレポート

Quest

現在の企業は、Active Directoryのセキュリティにどのように対応し、何に最も苦労しているでしょうか?

この疑問に答えるために、2023年9月にThe Experts Conference（TEC）を通じて「ハイブリッドActive Directoryのサイバーレジリエンスの現状」についての調査を実施したところ、ITプロフェッショナルとITエグゼクティブから430件以上の回答が寄せられました。

主な調査結果は驚くべきものでした。

ITプロフェッショナルのほとんどは、どこに焦点を当て、どのようにすれば組織をより安全に保護できるかを知っています。ただし、そのためのリソースとサポートを常に確保できるわけではありません。

トップ3の調査結果:

1. ITチームが最も苦労しているのは、不適切な設定を含むセキュリティリスクを特定し、制限することだと言います。
2. ITチームは、組織の最も重要なIT資産を保護するためには、Tier 0の資産（制御プレーン）の優先順位を設定するセキュリティモデルが効果的であることを知っています。しかし、このモデルはほとんど活用されていません。
3. IT組織は、ADセキュリティのニーズをすべてサポートできるほど十分な人員を確保しておらず、予算の縮小だけが理由ではありません。

主な調査結果1: ITプロフェッショナルが最も苦労しているのはリスクの露出の評価である

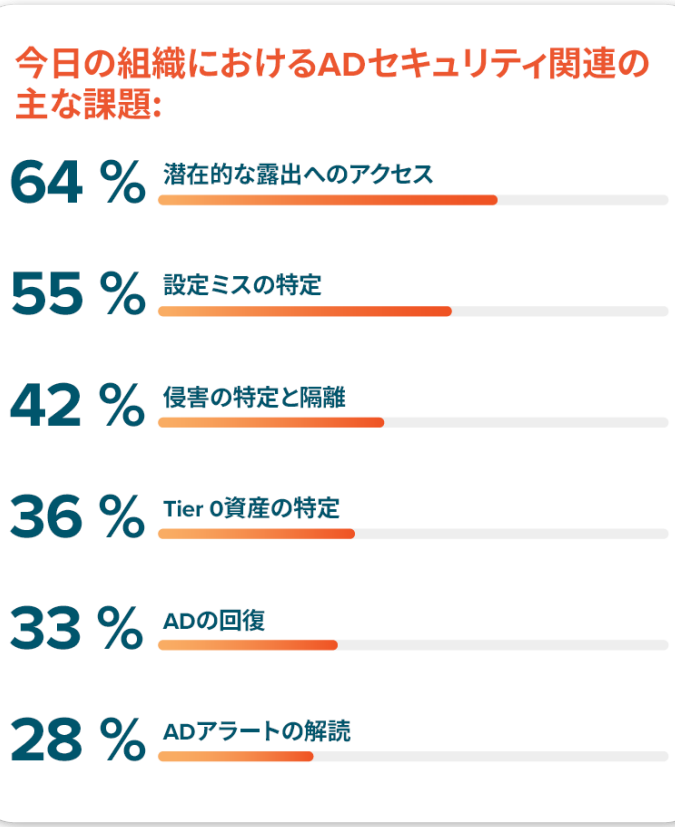
ここまでのところ、ITプロフェッショナルが最も苦労しているのは、設定ミスやその他のリスクを特定することです。このような弱点は、外部からの攻撃や組織内部の脅威のきっかけとなるため、Active Directoryのセキュリティにとって極めて重要です。

お客様の職務において、夜も眠れないほど気になるADのセキュリティ関連の懸念事項とは何ですか?

> **プラットフォームのセキュリティ体制とサイバーセキュリティの弱点、脅威の検出と攻撃経路のパターン、サイバー・セキュリティ・インシデントの可能性、プラットフォームを利用するアプリケーションとインフラストラクチャの追跡能力、Entra ID（Azure AD）プラットフォームとのハイブリッド統合、ADプラットフォームのリカバリとリカバリ後のプロセスです。**
>
> *大手プロフェッショナルサービス会社、IDサービス – ETS – テクノロジーおよび技術革新、インフラストラクチャエンジニア*

uevi.co/7780VLXB

今日の組織におけるADセキュリティ関連の主な課題:



uevi.co/6201DFAN

主な調査結果1: ITプロフェッショナルにとってのその他の最重要課題は、脅威の検知とADリカバリである

IT担当者は、セキュリティ侵害を検出したり、アラートを理解したりするのが難しいとも述べています。これらの作業は、脅威を迅速にシャットダウンし、その影響を抑えるために不可欠です。

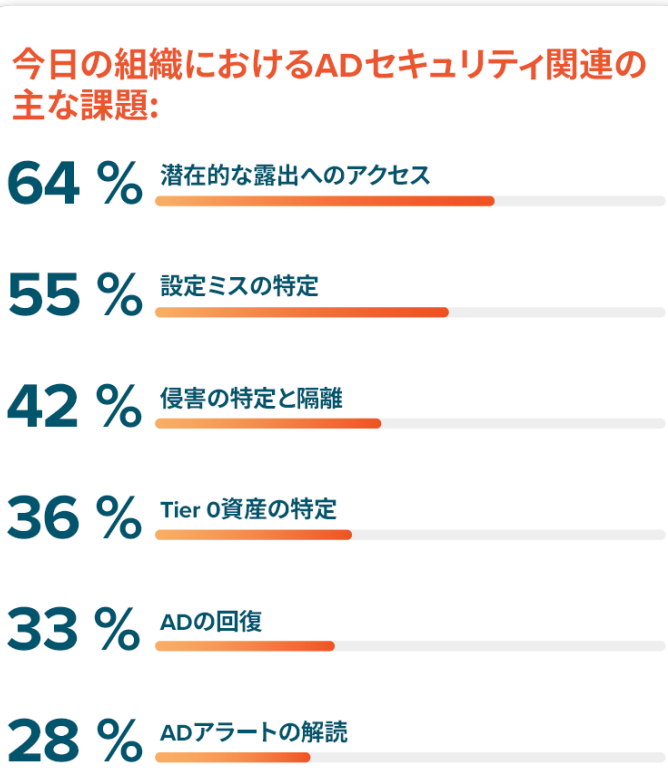
さらにITプロフェッショナルは、災害後にActive Directoryを復元するのに苦労しています。これは、サイバーレジリエンスにとって不可欠のタスクです。実際に、適切なツールがなければADをリカバリするには数日間から数週間かかり、その間はビジネスは完全に停止します。

お客様の職務において、夜も眠れないほど気になるADのセキュリティ関連の懸念事項とは何ですか?

> **外部からの不正侵入を迅速に特定し、検知後の復旧性を確保することです。**
>
> *大手プロフェッショナルサービス会社*

uevi.co/4949XYWI

今日の組織におけるADセキュリティ関連の主な課題:



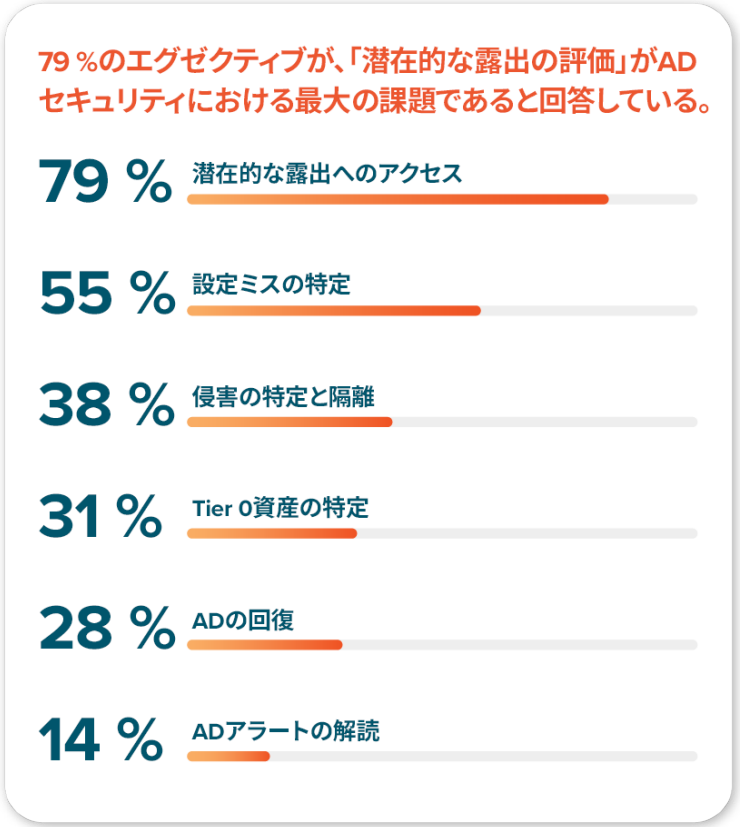
uevi.co/6201DFAN

主な調査結果1: ITエグゼクティブは同じ問題を挙げているが、リスクについてはより懸念している

ITプロフェッショナルとITエグゼクティブはそれぞれ重視する分野が異なるため、優先順位は必ずしも一致していません。しかし、ADのセキュリティ問題に関しては両グループの意見は一致しており、主要な問題の順序は完全に同じです。

顕著な違いは反応の強さです。ITプロフェッショナルの64 %に対し、ITエグゼクティブの10人に8人近くが、露出の評価が重要な課題であると回答しています。

しかし、これは驚くことではありません。ADリスクへの対処を怠れば、企業ブランドへの深刻かつ永続的なダメージにつながりかねないことをITエグゼクティブは強く認識しているからです。誰も、壊滅的なサイバー攻撃の被害者として次のニュースに名前が載ることは望んでいません。



uevi.co/1457CVQW

主な調査結果1: ITチームがADのセキュリティリスクをそれほど心配する理由とは?

実務担当者から経営陣まで、ITチーム全体がADのセキュリティ露出をこれほど懸念するのはなぜでしょうか。

答えは簡単です。Active Directoryは20年以上前から存在しており、その間にADの導入は規模も複雑さも爆発的に増大しています。そのため、ADで露出インジケータ（IoE）を見つけ、優先順位をつけ、攻撃対象領域を限定するために修正すべき方法を理解するのは容易ではありません。

一方、敵は何十年もかけてこのプラットフォームの弱点を発見し、悪用に磨きをかけてきました。

「サイバーレジリエンスの現状」の調査で、組織の規模や業種に関わらず、ITプロフェッショナルとITエグゼクティブの両方が挙げた懸案事項のトップが露出の評価であったことは、まったく不思議なことではありません。

お客様の職務において、夜も眠れないほど気になるADのセキュリティ関連の懸念事項とは何ですか?

> **ADは20年以上前からあるもので、攻撃者によく理解されており、適切に保護するのは非常に難しいのです。**
>
> *大手メディア企業、ID&コラボレーション担当副社長*

uevi.co/6668BKWD

主な調査結果1: お客様の同僚が心配するADの懸念事項とは?

お客様の職務において、夜も眠れないほど気になるADのセキュリティ関連の懸念事項とは何ですか?

> **適切に管理されていない変更や不適切なアクセスです。基本的にはヒューマンエラーの問題と言えます。**
>
> *中堅多角的金融サービス会社、*
> *シニア・テクノロジー・オフィサー*
>
> uevi.co/6712HKTU

> **特権アカウントの数とエスカレーションの両方、また信頼によるアクセス過多です。**
>
> *大手プロフェッショナルサービス会社、主任エンジニア*
>
> uevi.co/5976HYGO

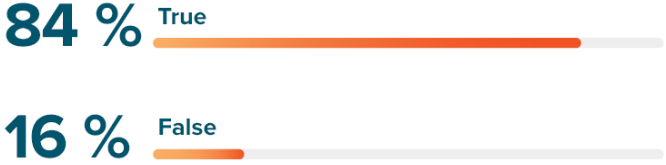
> **社内の脅威、不満を持つ従業員、マルウェアを拡散させるエンドユーザです。**
>
> *大手航空防衛会社、*
> *サイバー防御管理者*
>
> uevi.co/6008BWMF

主な調査結果2: ITプロフェッショナルはTier 0を優先することの重要性をよく理解している

Microsoftは10年来、Tier 0を中心としたADセキュリティモデルを導入するよう組織に働きかけてきました。Tier 0は、ドメイン管理者のような特権アカウントやドメインコントローラ（DC）のような重要なサーバを含む、組織の最も重要なすべてのIT資産で構成されています。

このメッセージははっきりと理解されており、調査回答者の84 %が、サイバーセキュリティとサイバーレジリエンスを確保するためのTier 0の重要性を理解していると答えています。

84 %が、最も重要なIT資産に優先順位を付け、セキュリティを確保する上でのADのTier 0構造（制御プレーン）の重要性を理解している。

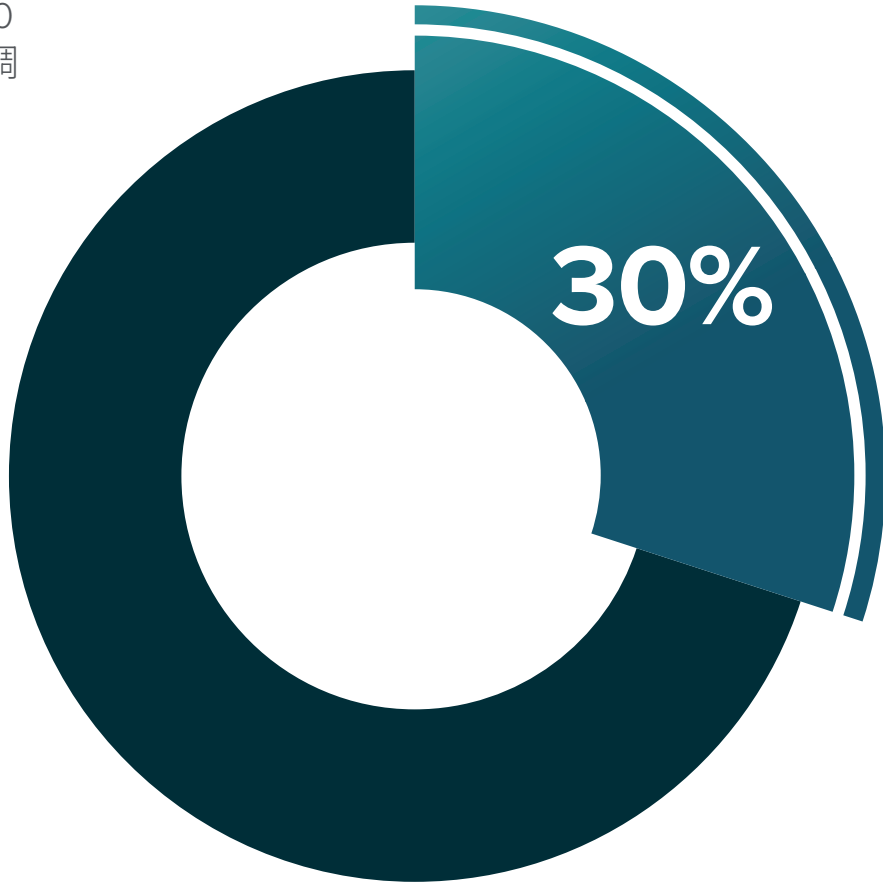


uevi.co/3915HSMV

主な調査結果2: …しかし、Tier 0のセキュリティモデルを使用しているのはわずか30 %に過ぎない

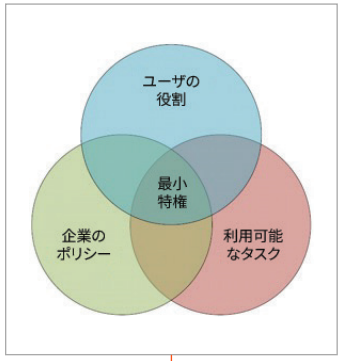
驚くべきことに、AD環境を安全に保つためにTier 0構造を積極的に利用していると答えているのは、調査回答者**10人のうちのわずか3人**です。

uevi.co/9945VLXB



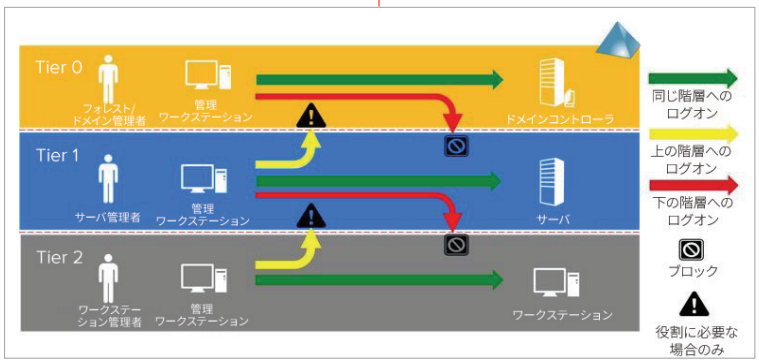
主な調査結果2: 安全なディレクトリ管理の進化

1999年: 最小特権

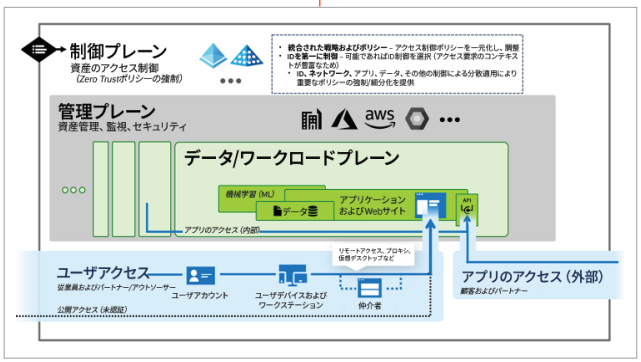


2014年: ESAE/レッドフォレスト

現在



2012年: 最小特権



2020年: エンタープライズ・アクセス・モデル

主な調査結果2: ここ数年でディレクトリのセキュリティはどのように変化したのか?

最初のADセキュリティモデルは最小特権の原則に根ざしたもので、各アカウントに必要なアクセス権だけを与え、それ以上でもそれ以下でもないというものでした。もちろん、この原則がITセキュリティの基礎となることに変わりはありませんが、実際には、すべてのIT資産に必要な保護のレベルは同じではありません。すべてを同じように一定期間固定しようとすると、AD環境の規模と複雑さが増すにつれて拡張性が損なわれます。

保護要件に基づいてIT資産を階層に分類する新しいモデルの一環として、Tier 0が2012年に導入されました。間もなくMicrosoftはこのアプローチをESEA（レッドフォレスト）モデルへと改良し、Tier 0が何を構成し、どのように保護すべきかをより明確にしました。

その後IT環境は、特にクラウドテクノロジーの急速な導入によりさらに劇的に変化し始めました。その結果生じるセキュリティ要件に対処するため、Microsoftは2020年にエンタープライズ・アクセス・モデルを導入しました。これは、今日のほとんどの顧客に対してMicrosoftが推奨するADセキュリティモデルです。

2012年以降Tier 0は、Microsoftが推奨するセキュリティモデルの必須の要素となっています。

主な調査結果3: ADセキュリティのすべてのニーズをサポートできる人員をIT組織が確保していない

では、100万ドルの質問に答えましょう。

なぜ組織は、脆弱性の評価、アクティブな脅威の発見、そのTier 0資産の優先順位付けなどのADセキュリティの重要なタスクで苦労しているのでしょうか。

その主な理由は、ADセキュリティに対応できる十分な人員が配置されているIT組織が半数だけであることです。

IT予算の逼迫がこの人員不足の一因であることは明らかですが、その全容ははるかに微妙なものです。

50 %が人員不足

現在のIT組織の半数が、現在の人員ではADセキュリティのニーズに対応できない。

uevi.co/3729DZGY

主な調査結果3: 要因A - ITプロフェッショナルが大きな負担を感じている

調査対象となったITプロフェッショナルの半数以上が、1日の中ですべてをこなすのに十分な時間を確保することが最優先事項だと答えています。

既に時間に追われている場合には、優先順位を見直したり、プロセスを手直ししたりすることができなくなります。その結果、単純な最小特権モデルから前進し、最新のエンタープライズ・アクセス・モデルの一環としてのTier 0を理解し、保護するようになる機会はほとんどありません。

53 %

が、必要なADセキュリティ関連の管理タスクを1日の中ですべて完了する時間を確保することが最優先事項であると述べている。

uevi.co/2446KRCF

主な調査結果3: 要因B - Active Directoryの専門知識が失われつつある

IT担当者に関する問題のもう1つの重要な側面は、Active Directoryの深い専門知識を持つITプロフェッショナルの不足が深刻化していることです。これには、以下の2つの相補的な傾向があります。

- ADセキュリティのトレーニングを受けた人材や、特定の制度的知識を持つ人材の多くが転職や退職を始めている。
- しかし、新入社員がかつてのようにADセキュリティの要件や慣行についてのトレーニングを受けていないため、後任となる人材がいないことが多い。実際にMicrosoftは重要なADトレーニングコースや認定資格をいくつか廃止しており、今後さらに多くのコースが廃止される予定になっている。

主な調査結果3: 要因C – ADセキュリティの責任者が不明確であることが多い

ID脅威の検出と対応（ITDR）に関してADチームとSecOpsチームの間で連携が取れていると回答した組織は、10社のうちの4社に過ぎません。その結果、誰が何の責任を負っているのか明確でないことが頻繁にあります。

さらに回答者の17 %が、ITDRの決定がITのリーダーシップに委ねられていると答えています。そのような組織では、現場のITプロフェッショナルが最新のADセキュリティモデルを導入するなどの取り組みを推進する可能性はさらに低くなります。

わずか41 %

の組織が、ADチームとSecOpsチームの間でADのID脅威の検出と対応（ITDR）について合意済み。

uevi.co/2271lWKF

17 %

の組織がITDRの決定をITリーダーシップ/CISOに委ねている。

uevi.co/9320CFKX

その他の注目すべき調査情報

さらに、次の2つの調査結果も注目に値します。

- NISTサイバーセキュリティフレームワーク（CSF）は、重要なADのIDインフラストラクチャを含むITエコシステムのセキュリティを強化するための貴重で柔軟なフレームワークを提供するものですが、CSFを完全に導入している組織は10社のうち6社未満です。
- 現在、多くの組織がサプライチェーンのリスク管理に非常に注意を払っています。これは、SolarWindsに侵入し、Microsoft、Intel、Ciscoなどのハイテク大手から、米国の国土安全保障省、国務省、財務省に至るまで、何千もの顧客に波及したサイバー攻撃のような壊滅的な被害を受けたためと思われます。

わずか58 %

の組織がNISTサイバーセキュリティフレームワークを完全に導入。

uevi.co/1945OEXU

約2/3がサプライチェーンのセキュリティを評価

64 %の組織が、サプライチェーンに含まれるベンダーに関連するセキュリティ慣行と潜在的リスクを評価している。

uevi.co/1897KEWM

推奨事項

Questの調査で報告されたADセキュリティの課題にお客様の組織も直面している場合、その課題に対処するための信頼できる戦略は以下の通りです。

Tier 0の資産を把握することで、最新のセキュリティモデルの導入に備える。

Tier 0資産に対する情報が不十分であることは、最新のエンタープライズ・アクセス・モデルの導入を妨げる理由にはなりません。サードパーティのソリューションを使用すると、すべての特権アカウント、グループ・ポリシー・オブジェクト、ドメインコントローラ、およびAzure AD Connectをホストするサーバなどの重要なサーバを含む、最も貴重なIT資産の包括的なインベントリを取得できます。

Tier 0を危険にさらす脆弱性を発見し、緩和する。

最近ADセキュリティ評価を実施していないのであれば、実施を予定してください。お客様の環境のどこが最も脆弱なのかを理解することが非常に重要です。これには、攻撃者がお客様の環境に足がかりを得るための設定ミスやその他の問題だけでなく、攻撃者が一旦侵入した後に特権をエスカレートさせ、横方向に移動してTier 0の資産に到達するために悪用する可能性のある弱点も含まれます。意図しない結果を避けるため、本番稼働を開始する前に、すべての修正を徹底的にテストしてください。

専門家と提携し、効果的なツールを選択することで、IT担当者の悩みを軽減する。

サイバー犯罪者は巧妙で容赦がないため、セキュリティインシデントは避けることができません。準備ができているかどうかを運任せにしてはいけません。信頼されるパートナーと協力し、NIST CSFに詳述されているすべての機能をカバーする包括的なADセキュリティソリューションに投資することで、脆弱性の緩和から脅威の検出と対応、ディザスタリカバリに至るまで、限られたITチームがADセキュリティタスクの全領域を処理できるようになります。

詳しくは、https://www.quest.com/jp-ja/solutions/cybersecurity-risk-management-solutions/をご覧ください。