COHESITY

# アイデンティティ レジリエンスソリューション の評価に関する エグゼクティブガイド

アクセスのロックダウン、貴重なデータの保護、破壊的なサイバー攻撃からの迅速な復旧のために知っておくべき情報をご紹介します。

# アイデンティティ・アクセス管理システムは、悪意のある攻撃者にとっては格好の標的となっています。

## これはなぜでしょうか?

サイバー攻撃の10件中9件は、アイデンティティ・アクセス管理 (IAM) システムを標的としています。これは、あらゆる組織のインフラストラクチャの中で最も攻撃を受けやすい部分です。

アイデンティティ管理システムは、これが侵害されると、組織内のほぼすべてのリソースへのアクセス権を攻撃者に与えることになるため、極めて価値の高い標的となります。そのため、アイデンティティレジリエンスは包括的なサイバーレジリエンス戦略の礎となっています。最低限の業務機能を迅速に復旧させるためには、多くの重要なシステムやビジネスプロセスがアイデンティティサービスに依存しているため、アイデンティティサービスは、信頼できる状態に戻すべき最優先のワークロードの一つに位置付けられる必要があります。

ほとんどの組織にとって、主要なIAMであり、他のIDプロバイダーの信頼できる情報源となっているのは、オンプレミスのMicrosoft Active Directory (AD) です。ADのサイバー復旧は、特に複数のフォレストを含む複雑な環境においては、専門的な知識を要する困難なプロセスであり、「単なるワークロードの一つ」ではありません。ADに加え、Entra IDやOktaなどを併用しているケースも少なくありません。

サイバー攻撃に対する防御を強化するにあたっては、すべての重要なアイデンティティサービスにわたる、エンドツーエンドのアイデンティティレジリエンス戦略を確実に策定する必要があります。

> *「サイバー攻撃から100%安全である組織などありません。だからこそ、侵害から復旧する力、すなわちレジリエンスへの投資が必要なのです。」*

アイデンティティレジリエンスにより、ビジネスにおいて以下を実現できます。

- **アイデンティティ脅威の検知と対処:** アイデンティティ脅威検知・対応 (ITDR) を通じて進行中のアイデンティティベースの攻撃を検知し、人の介入を待てないリスクの高い変更を自動的にロールバックします。
- **アイデンティティサービスのクリーンな復旧と信頼の回復:** 持続的な再感染につながる攻撃者やバックドアを復活させることなく、アイデンティティサービスを復旧させます。
- **ダウンタイムの削減:** アイデンティティはアクセスと認証の鍵となります。これが機能しなくなると、ビジネスは停止してしまいます。アイデンティティ攻撃から事業運営を安全かつシームレスに復旧できるようにすることで、ダウンタイムを削減します。

サイバー攻撃から100%安全である組織などありません。だからこそ、侵害から復旧する力、すなわちレジリエンスへの投資が必要なのです。組織は、アイデンティティベースの攻撃を継続的に検知して対処し、いかなる状況下でもAD、Entra ID、Oktaをリーンかつ迅速に復旧させる実証済みの復旧戦略を導入することで、アイデンティティレジリエンスを向上および拡大させる必要があります。本ガイドは、ソリューションの評価、適切な質問の提起、および今日の脅威からアイデンティティインフラを保護するための確かな投資を行う上で役立ちます。

# アイデンティティレジリエンスソリューションを選ぶ際のポイント

選択肢を評価する際、アイデンティティを単に、バックアップと必要に応じた復旧の対象となるワークロードの一つとして考えがちですが、これは危険なほど時代遅れの考え方です。サイバーレジリエンスをアイデンティティおよびアクセスシステムにまで拡大する最新のアプローチでは、攻撃ライフサイクルのあらゆる段階において、高度なプロアクティブセキュリティとクリーンな復旧を組み合わせています。真のエンタープライズ対応のアイデンティティレジリエンスソリューションと他のソリューションを区別するものは、以下の通りです。

**高度なITDR:** アイデンティティレジリエンスは、侵害が発生する前から始まります。ADのようなIAMシステムは、組織の鍵となる情報を管理しているため、攻撃者が最初に標的とするシステムとなることがよくあります。単にバックアップを取るだけでは不十分です。組織で導入するソリューションは、アイデンティティ脅威検知・対応機能を通じて、アイデンティティ環境のセキュリティ体制を継続的に監視できる必要があります。これにより、脆弱性を検知し、アイデンティティインフラのセキュリティを強化するとともに、対処を自動化することができます。人の介入を待てない悪意のある変更に対して、自動的にロールバックや対処を行うことで、攻撃が成功する可能性を低減できます。こうした継続的な脅威の検知と対処、そしてプロアクティブなセキュリティ強化を実施することで、攻撃者がアイデンティティシステムを悪用する前に、その動きを阻止することができます。

**攻撃に耐える保護機能:** 万が一侵害が発生した場合、クリーンなバックアップデータによってアイデンティティインフラを復旧できるよう徹底することが重要です。攻撃者は、バックアップが最後の防衛線であることを熟知しているため、積極的に二重恐喝の手口を用いたり、バックアップデータを暗号化・改ざん・削除しようとしたりします。その結果、被害者はほぼ無防備な状態に追い込まれ、法外な身代金の支払いを余儀なくされてしまいます。アイデンティティレジリエンスソリューションは、設計段階からイミュータビリティ (変更不可) を備えている必要があります。これにより、攻撃者がドメイン管理者の認証情報を取得したとしても、ADのバックアップが改ざんされることを防ぐことができます。WORMストレージ、クォーラムベースの承認、暗号化による検証は、回復力のあるバックアップにとって不可欠な機能です。攻撃者がネットワーク内に侵入した際に、保護レイヤーが機能しなければ、実質的に保護されているとは言えません。

**迅速かつマルウェア感染のない復旧:** アイデンティティが侵害されると、ダウンタイムはあらゆる業務部門に波及します。復旧のスピードも重要ですが、復旧の完全性も同様に重要です。信頼性を検証せずに単にアイデンティティをリストアするだけでは、マルウェアやバックドアが再び侵入するリスクがあり、感染の再発や恐ろしい悪循環に陥る可能性があります。効果的なソリューションでは、AD、Entra ID、Oktaの自動化・オーケストレーションされた迅速な復旧を組み合わせる必要があります。特にADについては、侵害された認証情報やマルウェアが再び持ち込まれないよう、復旧処理をOSから切り離す必要があります。これにより、信頼できる復旧を通じて持続的な感染を防止し、復旧プロセス中のダウンタイムを削減できます。

**細かい単位での復旧オプション:** すべてのアイデンティティ侵害インシデントがフルリストアを必要とするわけではありません。オブジェクトレベル、属性レベル、フォレストレベルの復旧オプションを提供する細かい単位での復旧により、時間を節約し、業務の混乱を軽減します。フォレストレベルおよび細かい単位での復旧ツールを備えることで、ヘルプデスクへの問い合わせから本格的なサイバーインシデントに至るまで、あらゆる状況に適したソリューションを確保できます。

**ハイブリッドアイデンティティ全体にわたる保護:** アイデンティティは、もはやオンプレミスのADだけに限定されません。Entra IDやOktaは、特にクラウドアプリへのアクセスにおいて、急速に企業のアイデンティティアーキテクチャの重要な要素となりつつあります。ハイブリッドアイデンティティ環境全体でシームレスに動作し、AD、Entra ID、Oktaのすべてを保護する、将来を見据えたレジリエンスソリューションが必要です。多くの組織では、Entra IDやOktaがADと同期されているため、Entra IDやOktaを確実かつ安全にリストアさせるには、まずADを保護および復旧する能力が必要になります。Entra IDとOktaはADとは別のアプリケーションであり、オンプレミスからクラウドへの一方向の同期が行われているため、オンプレミスの保護がなければ、ソリューションの半分しか機能していないことになります。アイデンティティレジリエンスソリューションには、Entra IDとOktaのセキュリティを確保し、クリーンに復旧できる保護および復旧機能も含まれている必要があり、クラウドアイデンティティの継続性を確保する必要があります。

**侵害後のフォレンジック調査による信頼性の検証と将来の攻撃の防止:** インサイトのない復旧は、インシデントの再発のリスクを高めます。最新のソリューションには、復旧がクリーンであるかどうかをチームが検証できるフォレンジック機能が組み込まれている必要があります。これは、インシデント後の調査に役立つだけでなく、予防措置を策定する上でも非常に重要です。企業が防御体制を強化し、コンプライアンスや規制報告要件を満たす上で役立ちます。復旧後のデューデリジェンスが欠けていると、二次攻撃を受けるリスクにさらされます。フォレンジック調査は、後回しにすべきものではありません。これはアイデンティティレジリエンスに不可欠な要素です。

**インターネット接続なしで復旧する機能:** 壊滅的な障害やサイバー攻撃が発生した場合、安定した、あるいは安全なインターネット接続が確保できるとは限りません。アイデンティティレジリエンスソリューションは、インターネットが利用できない状況でも重要なアイデンティティシステムを確実に復旧させ、あらゆる状況下でシステムをクリーンにリストアし、オンライン状態に戻せるものでなければなりません。

**年中無休のインシデント対応サポート:** アイデンティティは、特に復旧に関して言えば、独特かつ複雑なワークロードです。重要なアイデンティティインフラのサイバー復旧においては、ソリューションのベンダーが、アイデンティティの保護、セキュリティ確保、および復旧において実績ある専門知識を持ち、顧客に必要なガイダンスを提供できることを確認することが重要です。復旧の状況はそれぞれ異なるため、経験豊富な専門家による適切な対応サポートとフォレンジック調査が、組織が最も壊滅的なアイデンティティ攻撃やサービス停止から、自信を持って迅速に復旧するための鍵となります。

# ベンダーに確認すべき重要な質問

1. 攻撃者がActive Directory、Entra ID、Oktaのバックアップを改ざんまたは削除するのをどのように防ぎますか?
2. アイデンティティインフラストラクチャ全体を1日以内に完全に復旧できることを実証できますか?
3. 復旧したAD、Entra ID、Oktaにマルウェアやバックドアが含まれていないこと、または侵害された認証情報が再度持ち込まれていないことを、どう検証しますか?
4. インターネット接続なしで、同じ操作感とUIのままでアイデンティティを復旧できますか?
5. ハイブリッドアイデンティティ環境 (オンプレミスAD + Entra ID + Okta) に対応していますか?
6. 貴社のソリューションは、ADのフォレスト全体の復旧を自動的に実行し、Microsoft Recovery Runbookに準拠できますか?
7. 貴社のソリューションは、侵害が発生する前に悪意のある攻撃者を検知・排除するため、ID固有の脅威を特定していますか?

# 注意すべき警告サイン

- ! 復旧中にOSを切り離す機能がない。アイデンティティデータを含むOSを復旧すると、マルウェアやバックドアを復活させてしまう可能性があります。
- ! 復旧対象として物理/仮想ソースを指定する機能がない。厳密なパッチレベルを要求すると、ダウンタイムが長引く可能性があります。
- ! 年中無休のインシデント対応サポートのための、アイデンティティフォレンジックおよびインシデント対応の専門知識 (IFIR) がない。
- ! アイデンティティセキュリティ機能が存在しない。レジリエンスには、影響が生じる前のリスクの低減や、侵害を防ぐための脅威の軽減も含まれます。
- ! Microsoftのネイティブツールのみに依存しているソリューション。これらは手動操作で、処理が遅く、最も必要な時に信頼性に欠けます。
- ! バックアップが本番環境に保存されている。攻撃者がバックアップを消去できるため、復旧手段を失ってしまう可能性があります。
- ! 複数のドメインコントローラー (DC) を並行して復旧するためのオーケストレーションや自動化機能がない。これがないと、管理者はストレスの高い混乱した状況下で、時間のかかる手動操作を強いられることになります。
- ! ソリューションが安全で安定したインターネット接続に依存している。サイバー攻撃や復旧時にインターネット接続が確保されていることを前提にしたり、それに頼ったりすることはできません。
- ! 復旧のテスト機能がない。事前に検証ができないものは、信頼することができません。

# ベンダー評価チェックリスト

ベンダーとの打ち合わせ時にこのスコアカードを活用してください:

| 要件 | ベンダー1 | ベンダー2 | ベンダー3 | 注記 |
|---|---|---|---|---|
| 複数のDCを並行して復旧 (ADの場合) | | | | |
| 復旧対象としてあらゆる物理/仮想ソースを指定可能 | | | | |
| イミュータブルな (変更不可の)、隔離されたADバックアップ | | | | |
| オブジェクトからフォレストレベルまでの細かい単位での復旧 | | | | |
| 自動化されたフォレスト復旧ワークフロー | | | | |
| 攻撃経路を特定して遮断するためのプロアクティブなセキュリティ強化 | | | | |
| バックアップ内のマルウェア／データ破損の検知 | | | | |
| 改ざん防止機能を備えた複数ソースの変更追跡とロールバック | | | | |
| 攻撃対象となりやすいサービスアカウントのインベントリおよび監視 | | | | |
| ハイブリッドAD (オンプレミス + Entra ID) のサポート | | | | |
| インターネット接続なしで復旧する機能 | | | | |
| 侵害後のフォレンジック調査 | | | | |
| 拡張性 (マルチフォレスト/グローバル) | | | | |
| 年中無休の専門家によるインシデント対応サポート | | | | |

# 結論

ほぼすべての重大な情報漏洩事件の中心には、アイデンティティベースの侵害があります。そのため、重要なアイデンティティシステムにおけるサイバーレジリエンスの強化は、もはや任意の選択肢ではなく、企業セキュリティの基盤となっています。

実績のあるアイデンティティレジリエンスソリューションは、バックアップだけにとどまりません。アイデンティティの侵害に対する耐性を強化し、アイデンティティ攻撃や脅威を防御し、信頼性の高い超高速復旧を実現するとともに、マルウェア感染のない信頼できるリストアの実施に向けたバックドアの閉鎖を支援します。アイデンティティレジリエンスの詳細や、それが最も重要なアイデンティティサービスのセキュリティ確保にどのように役立つかについては、今すぐCohesityのアカウントチームにお問い合わせください。



COHESITY

cohesity.com
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054

4500064-004-JP 7-2026