eBook

アイデンティティをセキュリティの要に

人間、機械、AIの最新アイデンティティ戦略を推進するための3つの原則

okta

okta

「アイデンティティ」というと、何を思い浮かべますか？

多くの人は、最初にセキュリティを思い浮かべます。当然です。認証情報の盗難、フィッシング、セッションハイジャック、そして自律システムの急速な台頭が脅威情勢を占める今、アイデンティティは主要な攻撃対象となっています。攻撃者は、アイデンティティを利用して、機密性の高いシステムにアクセスし、特権をエスカレーションし、環境内を横方向に移動します。

今日、アイデンティティはもはや従業員と顧客だけを指すものではなくなりました。アイデンティティには、非人間アイデンティティ、サービスアカウント、ワークロード、API、そしてユーザーに代わって動作するAIエージェントが含まれます。組織がAI主導のシステムや自動化を大規模に導入するに伴い、ガバナンスとコントロールを必要とするアイデンティティの数は急速に増え続けています。

しかし、多くの組織は、まだその対応に追いついていません。依然として時代遅れの境界ベースのセキュリティモデルに固執し、アイデンティティを中心とした脅威に対して適切な保護を提供できないネットワークやデバイスの制御に依存しています。人間、非人間、AI駆動型アイデンティティ全体にわたって可視性が断片化しているため、セキュリティチームは、プロアクティブにポリシーを適用するのではなく、事後対応に追われています。

AIによってアイデンティティに関する課題が急増

組織が自律型AIエージェントや自動化されたワークフローを導入するにつれて、システムがますますユーザーに代わって動作するようになっています。これらのエージェントは、機械的なスピードで、データを取得し、タスクを実行し、複数のアプリケーションとやり取りします。これらのアクションを制御する統合されたアイデンティティレイヤーが存在しない場合、組織は、従来のセキュリティ制御を超えて動作する新しいタイプの未管理のアイデンティティが作られるリスクを抱えています。

最新のアイデンティティ戦略の定義

最新のアイデンティティ戦略は、テクノロジーエコシステム全体の一元化された制御レイヤーとしてアイデンティティを確立します。人間、非人間、AI主導のアクティビティに対して一元的な可視性を提供し、悪用される前に脆弱性を特定して、進化するリスクにリアルタイムで対応します。

また、組織が安全に拡張できるようになります。AIエージェント、サービス、アプリケーションの自律的な動作が増加するに伴い、アイデンティティはイノベーションを減速させることなく、最小権限とポリシーベースのアクセスを適用し続ける必要があります。

この資料では、AI時代において、アイデンティティが企業のセキュリティの基盤であるべき理由を解説し、以下の情報を提供します。

- アイデンティティに関連する脅威が進化・加速している現状
- 従来のアイデンティティ管理手法が組織の脆弱性を引き起こしている理由
- 最新のアイデンティティ戦略を定義するための3つの原則

エンタープライズセキュリティスタックの断片化

過去10年で、エンタープライズ技術スタックは大きく変貌しました。クラウドサービス、SaaSアプリケーション、API、リモートワークは、組織の構築および運用方法を一変させました。今日、AIエージェントと自動化システムが、その変化をさらに加速させています。アプリケーションは、ただ接続するだけではなくなりました。今では動作します。サービスはデータを保存するだけではなくなりました。タスクを実行します。AIシステムは、システム全体から情報を取得し、ワークフローをトリガーし、意思決定を行います。

このような環境において、単一のエンタープライズライセンス契約の下で技術的な統一を行うという考え方は、もはや現実的ではありません。組織は、競争力を維持し、迅速に行動するために、ベストオブブリードのソリューションのエコシステムを構築しています。その結果、強固で柔軟なインフラストラクチャを実現しています。しかし、複雑さも増しています。

最新の技術スタックは高度に分散化され、深く相互に関連しています。新しいアプリケーション、サービス、API、ワークロード、AIエージェントごとに、新たなアイデンティティが生まれます。これらのアイデンティティは、クラウド、オンプレミス環境、SaaSプラットフォーム、カスタムアプリ、インフラストラクチャ全体にわたって機能します。一元的に制御されない場合、アイデンティティは複雑に絡み合ったシステムや環境全体で断片化してしまいます。

テクノロジーのサイロ化がセキュリティの盲点を生む

断片化は、重大なセキュリティ上のリスクを生み出します。人間のアイデンティティ、サービスアカウント、マシンアイデンティティ、AIエージェントは多くの場合、別々のシステムに存在し、ポリシーに一貫性がなく、監視も不十分な状態です。これにより、攻撃対象領域が拡大し、気付かないうちに認証情報が盗まれたり、トークンが不正使用されたり、特権のエスカレーションが行われたりする可能性が高まります。

セキュリティチームは、このような状況において、一元的な可視性を確保しようと苦心しています。ログが分散していて、ポリシーに一貫性がありません。非人間アイデンティティは、制御できる速度よりも速いペースで増加しています。AIシステムがますます自律的に動作するようになるにつれて、組織は、新たな課題に直面しています。機械的なスピードで制御を強化するという課題です。

多くのAIエージェントと自動化サービスは、永続的な認証情報と複数のシステムへの広範なアクセス権を用いて動作しています。これらのアイデンティティが適切に検出・管理されていない場合、意図された目的が終了した後も、特権付きの許可を保持し続ける可能性があります。これにより、監視がほとんどない状態でシステム全体で動作する強力なアイデンティティのプールが拡大し、攻撃対象領域と侵害時の影響の両方が拡大します。

攻撃者はこうした変化を見逃しません。アイデンティティは、一元化されていない制御ポイントであることが多いため、主要な攻撃ベクトルになっています。Oktaも参加した「2024 Verizon Data Breach Report」によると、侵害の80%は、何らかの形でアイデンティティ漏洩が関与しています。侵害の認識と封じ込めにかかる平均日数は、依然として約290日です。

okta

今こそアイデンティティを変革すべき時

アイデンティティがセキュリティにおいて重要な役割を果たすことは、どの組織も理解しています。しかし従来、その役割は、認証とアクセスコントロールに限定されていました。また、アイデンティティは、人間および非人間アイデンティティ全体にわたって、エンタープライズ規模の可視性、ガバナンス、制御を実現する一元化された制御レイヤーという、同等に重要な役割も担っており、この意味でアイデンティティを活用している組織はごく少数に限られます。

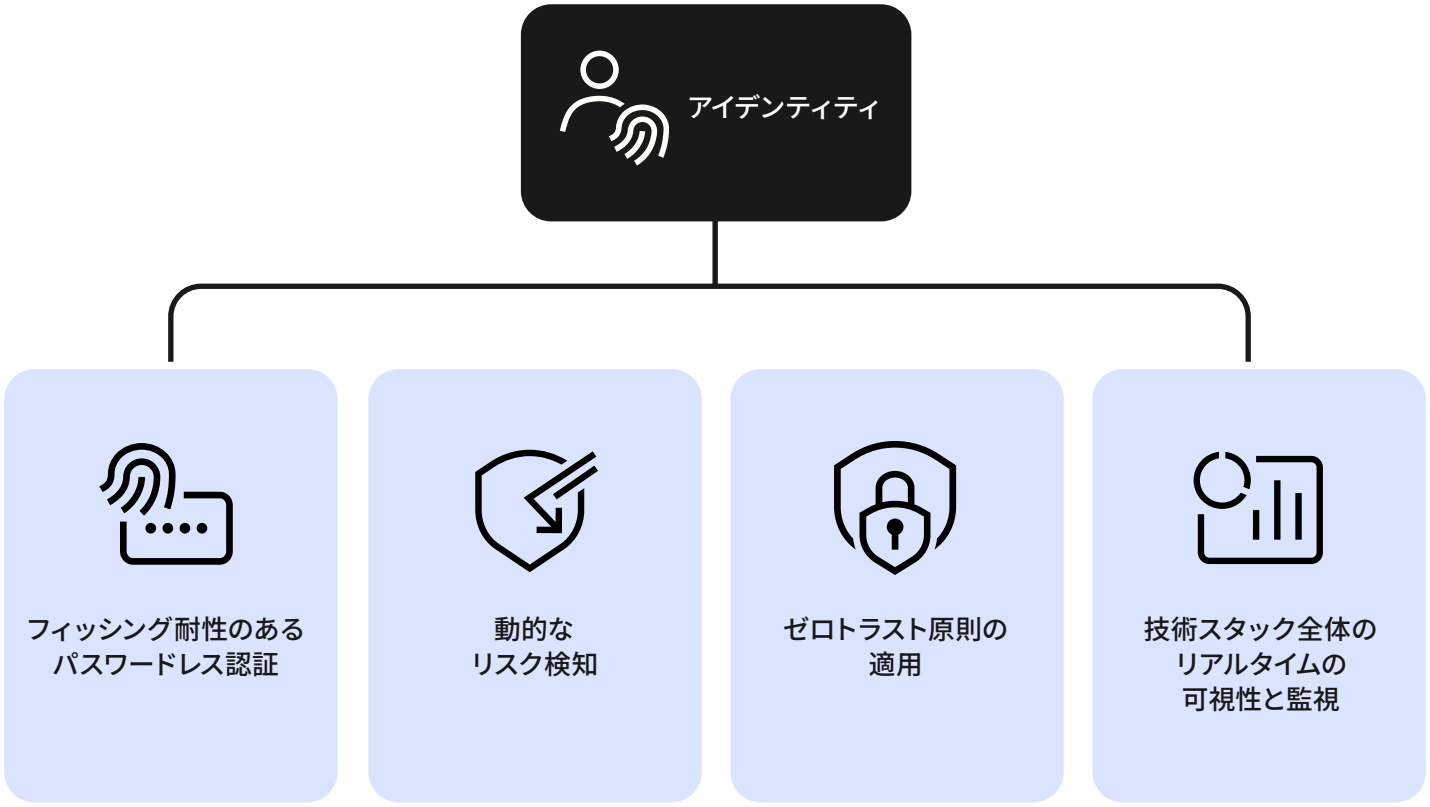
たとえば、多くの組織は、認証による安全なアクセスを実現にするために、アイデンティティに依存しています。しかし、アイデンティティがテクノロジーとセキュリティのエコシステム全体でより深く統合されると、セッションが確立された後でも、継続的なリスク評価、リアルタイムのポリシー適用、自動修復を強化できます。AIエージェントと自動化システムがユーザーの代わりに動作する環境において、アイデンティティは、誰がシステムにアクセスしているかだけでなく、次に何が許可されるかを検証しなければなりません。

アイデンティティを中心とするセキュリティエコシステム

この可能性を無視することは、データが既に示している事実を見落とすことになります。つまり、今やアイデンティティは、エンタープライズのサイバーセキュリティにおいて主要な戦場になっています。攻撃者は、アイデンティティを利用して、最初のアクセス権を得て、特権をエスカレーションし、環境内を移動します。また、アイデンティティは、組織が説明責任を確立し、最小権限を適用し、大規模に制御を維持する手段でもあります。

最新のアイデンティティ戦略は、セキュリティとテクノロジーのエコシステム全体をつなげるレイヤーとして機能し、可視性、ガバナンス、制御を統合します。ログイン時だけでなく、人間、サービス、AIエージェントが開始したかを問わず、あらゆるやり取りにおいて態勢を強化します。

この状況に対応するためには、アイデンティティとは何か、そしてアイデンティティの活用方法について、より広範かつ戦略的な視点を持つ必要があります。



脅威の詳細な分析

攻撃者は、時代遅れのアイデンティティ管理手法を狙っています。断片化したITおよびセキュリティ環境では、重要なリソース、アプリケーション、アイデンティティが分断されたシステムやインフラストラクチャに分散するため、人間および非人間アイデンティティに関連する攻撃が見過ごされ、対処されずに放置されるリスクが高まります。AIエージェントと自動化システムがより多くのデータにアクセスし、より多くのアクションを実行するようになるに伴い、脆弱なアイデンティティ管理がもたらす影響は、より深刻なものになります。

手作業のプロセス

許可設定の手順が煩雑で時間がかかることで、アクセスの判断で人的なミスが起きやすくなり、ポリシーの適用にもばらつきが生じます。

見落とし

ユーザー、サービス、ワークロード、AIエージェント全体のリアルタイムなセキュリティ態勢、アイデンティティの挙動、許可に対して可視性が限定されます。

対応の遅れ

検出と修復の遅延により、制御が介入する前に、攻撃者や不正な自動化プロセスが、アイデンティティに関連する脆弱性を悪用してしまいます。

この問題が無くなることはありません。むしろ急増しています。AI搭載アプリケーション、サービス、非人間アイデンティティ、AIエージェントは、アイデンティティ攻撃対象領域を拡大し、実行スピードを加速させます。アイデンティティ関連の攻撃は、もはや認証情報の窃取に留まりません。盗まれたセッションCookie、トークンのリプレイ、特権のエスカレーションなどの認証後の脅威は、分散化された環境を監視するセキュリティチームに新たな課題をもたらしています。

さらに資金力のある国家主体の攻撃者、内部脅威、管理されていない自律型システムを考慮すると、アイデンティティを中心とした脅威情勢は急速に進化しています。

91%

組織の91%は、すでにAIエージェントを使用しているが、そのうち管理戦略が整っている組織はわずか10%

（Okta）

80%

データ漏洩の80%以上が、アイデンティティを狙った攻撃に起因している

（Verizon）

180%

アイデンティティを狙った攻撃は、前年比180%のペースで増加している

（Verizon）

19億

2023年には、Fortune 1000企業から従業員のセッションCookie 19億件が窃取された

（Fortune）

okta

アイデンティティこそがセキュリティの根幹

脅威環境を見ると、アイデンティティを狙う脅威が増大し、リスクが拡大しています。組織がクラウドサービス、非人間アイデンティティ、AIエージェントの利用を拡大するにつれて、アイデンティティは主要な攻撃対象領域になると同時に、主要なコントロールポイントにもなります。

アイデンティティはただのリスク源ではありません。コントロールを確立する最大のチャンスでもあります。アイデンティティをセキュリティ戦略の中心に据えることで、組織は、事後対応型の防御から継続的な制御へと移行でき、リスクが実害に変わる前に、アクセスと自動化アクションを検証できます。

アイデンティティが、人間、サービス、AIエージェント全体で統合されると、侵害を防止し、セキュリティとテクノロジー投資の価値を最大化するための基盤となります。

最新のアイデンティティ戦略を推進するための3つの原則

ここまで、アイデンティティ優先のセキュリティの重要性について検討してきました。次に、より実践的な内容に踏み込み、組織のアイデンティティを現在の状態からAI主導の環境に適した状態へと導く方法を見ていきましょう。

最新のクラウドネイティブなアイデンティティプラットフォームは、断片化を減らし、制御を一元化するための手段を提供します。人間および非人間アイデンティティ、サービス、AIエージェント全体にわたる一元的でリアルタイムな可視化を提供するため、IT・セキュリティチームは盲点を排除し、リスクを特定し、対応速度を向上できるようになります。

これらの価値は、次の3つの基本原則に整理することができます。

全体的な可視性

ユーザー、非人間アイデンティティ、AIエージェント全体で、脆弱性が見過ごされたり、未対応のままにならないように確認します。

オーケストレーションの強化

システム、サービス、自動化されたワークフロー全体で、リアルタイムの修復とポリシーベースの制御を適用します。

広く深い統合

一貫したガバナンスと制御を可能にするために、セキュリティとテクノロジーエコシステム全体でアイデンティティをつなげます。

市場を評価する際、組織は、これら3つの側面すべてに対応するプラットフォームを求めるべきです。

第1の原則

全体的な可視性

アプリケーション、サービス、システムごとに個別にアクセス許可を管理すると、悪用されやすいセキュリティのギャップが生じ、ポリシーの適用も一貫性がなくなります。非人間アイデンティティとAIエージェントの増加に伴い、これらのギャップはユーザーアカウントだけでなく、API、ワークロード、自動化されたプロセスにも拡大します。

最新のアイデンティティプラットフォームは、アクセスのライフサイクル管理を一元化および簡素化すると同時に、環境全体のアイデンティティアクティビティを包括的かつリアルタイムで把握できるようにする必要があります。人間のアイデンティティ、サービスアカウント、ワークロード、AIエージェントに対する統合された可視性を提供し、チームが脆弱性を早期に検出して、ポリシーを一貫して大規模に適用できるようにする必要があります。

主な機能

アクセスガバナンスとライフサイクル管理

システム全体のプロビジョニングとプロビジョニング解除を一元化し、入社、異動、離職に伴うプロセスを自動化し、ユーザーおよび非人間アイデンティティのアクセスを継続的に認定するツール。

セキュリティ態勢と脅威に対する可視性

アイデンティティ構成を監視し、構成ミスを検出し、アプリケーション、インフラストラクチャ、AI主導のシステム全体にわたって、アイデンティティ関連のリスクに関するリアルタイムな洞察を提供する機能。

特権付きアクセスおよび機密性の高いアクセスの制御

管理者アカウント、サービスアカウント、昇格された権限で動作するAIエージェントを含み、影響の大きいアイデンティティを保護。

Continuous Risk Evaluation

人間または自動化システムが開始したかを問わず、不審なアクティビティを迅速に検出して、対応できるようにするリアルタイムの監視とシグナルの集約。

チェックリスト：貴社のアイデンティティプラットフォームは...

- ☐ ユーザー、非人間アイデンティティ、AIエージェント、カスタマーアカウント全体にわたって脅威を可視化できますか？
- ☐ 技術スタック全体からのサードパーティシグナルを取り込み、リスクに対する包括的かつリアルタイムの可視化を実現できますか？
- ☐ ゼロトラストの原則に基づいてアイデンティティ態勢を継続的に評価できますか？
- ☐ 一貫性のないMFAの適用や、アカウントの無秩序な増加、過剰な特権付きサービスアカウントなどの構成ミスを特定できますか？
- ☐ 従業員のロールが変更になったり、非人間アイデンティティが必要でなくなったりした場合に、プロビジョニングおよびプロビジョニング解除を自動で実行できますか？
- ☐ 特権ユーザー、サービス、AIエージェントに対して、きめ細かいアクセスコントロールを適用できますか？
- ☐ 非人間アイデンティティを検出し、それらの許可と動作を監視できますか？
- ☐ アイデンティティライフサイクル管理を一元化するために、人事システムやディレクトリと統合できますか？
- ☐ カスタマーアイデンティティを大規模に管理・保護できますか？

第2の原則

オーケストレーションの強化

断片化したセキュリティスタックは、膨大な量のリスクデータを生成します。そのデータを分析し、必要な対応を講じるための統合されたアイデンティティ主導の制御レイヤーがない場合、チームは複数のシステムにまたがるログの関連付けを強いられ、被害が発生した後の対応に追われます。その結果、対応が遅いセキュリティ態勢となり、自動化されたワークフロー、非人間アイデンティティ、機械的なスピードで動作するAIエージェントに追いつけなくなります。

最新のアイデンティティプラットフォームは、組織がリアルタイムで脅威を防止、検出、修復できるようにする必要があります。可視化だけでなく、リスクシグナルを自動化された制御アクションへと変換し、ユーザー、サービスアカウント、AIエージェントによって開始されたかどうかを問わず、不審な動作は、すぐに評価、制御されるようにする必要があります。

チェックリスト：貴社のアイデンティティプラットフォームは...

- ☐ 自動修復およびポリシー適用アクションの設定作業を簡素化できますか？
- ☐ リスクシグナル、コンテキストデータ、動的なポリシーに基づいて応答をカスタマイズできますか？
- ☐ ステップアップ認証、セッションの取り消し、ユニバーサルログアウトなどの保護アクションをトリガーしますか？
- ☐ 継続的な保護を強化するために、フィッシング耐性のある認証方法と統合できますか？
- ☐ アクティブなセッション中に、デバイス態勢とコンテキストのリスクを評価できますか？
- ☐ 悪意のあるIPアドレスや異常なアクティビティをリアルタイムでブロックできますか？
- ☐ セキュリティ制御を弱めることなく、安全なセルフサービスの要素回復を実現できますか？
- ☐ 自動化されたアクションやAI主導のアクションを含み、認証後もアイデンティティアクティビティを継続的に評価できますか？

第3の原則

広く深い統合

テクノロジーエコシステムの強さは、そのコンポーネント同士の結びつきの強さに左右されます。アプリケーション、インフラストラクチャ、セキュリティツール、API、AIシステム全体でシームレスに統合されていなければ、組織は、一貫したアイデンティティ制御を適用し、その投資の価値を最大限に引き出すことが困難になります。

最新のアイデンティティプラットフォームは、環境内のあらゆる要素を連携して、一貫したガバナンス、リスク監視、制御を可能にする必要があります。ベンダーニュートラルなアイデンティティプラットフォームは、開発者やITチームに不必要な統合作業の負担をかけることなく、SaaS、クラウド、カスタムアプリケーション、AI主導システム全体で、人間および非人間アイデンティティの統合を可能にします。

チェックリスト：貴社のアイデンティティプラットフォームは...

- ☐ CRM、生産性、コラボレーション、ERP、IT運用ツールなどの主要なエンタープライズSaaSアプリケーションと統合できますか？
- ☐ プロビジョニングやシングルサインオンだけでなく、認証前、認証時、認証後も制御を徹底するように、アイデンティティ保護を拡張できますか？
- ☐ 脅威検知、リスクスコアリング、自動修復を強化するために、スタック全体にセキュリティツールを統合できますか？
- ☐ API、サービス、AIエージェントを、一貫したアイデンティティガバナンスとポリシー適用でサポートできますか？
- ☐ システム全体で安全なワークフローをトリガーするために、ノーコードまたはローコードの自動化機能を提供しますか？
- ☐ 環境の進化に応じて、新しいアプリケーション、サービス、AI機能をサポートするために、拡張性を提供しますか？

統合セキュリティ戦略の成果

アイデンティティ優先の統合セキュリティは、単なる概念ではありません。現実の運用において、保護を強化し、業務を効率化し、より複雑な環境で組織が安全に拡張できるようにして、測定可能な成果をもたらします。

アイデンティティセキュリティと侵害からの保護

人間および非人間アイデンティティのすべてを保護することでセキュリティ態勢を強化し、侵害につながる前に、アイデンティティベースの脅威を検出、封じ込み、修復できるようにします。

運用効率とレジリエンス

断片化されたアイデンティティシステムを統合して、俊敏性を高め、運用コストを削減し、価値実現までの時間を短縮する統合コントロールレイヤーを構築することで、運用を簡素化して、複雑さを軽減します。

AIの可視化と制御

一元的な可視性、ポリシー適用、新たなAI主導のワークフロー全体にわたる安全なアクセスコントロールを提供することで、AIエージェントと自動化システムのガバナンスを確立します。

統合セキュリティ戦略の主な成果に関する詳細をご確認ください。

okta

アイデンティティ優先のセキュリティの実現に向けて

アイデンティティ優先のセキュリティが全面的に実現すると、アプリケーション、サービス、自動化システムを構築、接続、運用する際に、安全かつ管理しやすいオープンなエコシステムがサポートされます。アイデンティティのサイロ化はもう発生しません。

コストも時間もかかるカスタム統合も不要です。従業員、顧客、機械主導の環境全体において、セキュリティギャップや盲点もなくなります。アイデンティティを中心として統合された技術スタックは、あらゆるやり取りにおいて、一貫したガバナンスと制御を可能にします。

アイデンティティをセキュリティの要に

「アイデンティティはセキュリティである」は、強調してもし過ぎることはありません。脅威に先手を打ち、レジリエンスの高い長期的な保護を構築するために、セキュリティとITのリーダーは、環境全体にわたってアイデンティティを管理、制御、統合する方法を最新化する必要があります。

アイデンティティが、人間、非人間アイデンティティ、自動化システム全体で統合されると、組織は、リスクを削減し、運用管理を強化し、大規模で安全なイノベーションが可能になります。強固なアイデンティティ基盤は、ますます高度化する攻撃から保護すると同時に、今日の分散化したAI主導の環境に必要な俊敏性も提供します。

アイデンティティ戦略を前進させ、Oktaの専門家から的確な推奨を受けるには、こちらから詳細をご確認いただくか、または当社のチームにお問い合わせください。

Oktaについて
Okta, Inc.は、The World's Identity Company™です。AI、機械、人間のアイデンティティを保護することで、誰もが安心してあらゆるテクノロジーを利用できるようになります。当社のカスタマーソリューションとワークフォースソリューションは、ビジネスと開発者が、セキュリティ、効率性、イノベーションを推進できるようにし、同時にAIエージェント、ユーザー、従業員、パートナーを保護します。世界をリードするブランドが認証、認可、その他の機能でOktaを信頼する理由については、okta.comをご覧ください。

okta

Okta Inc.
100 First Street
San Francisco, CA 94105
info@okta.com
1-888-722-7871