AIエージェントなどの非人間アイデンティティを管理するには

アイデンティティ・ファーストの最新セキュリティ戦略で実現

非人間アイデンティティによって業務改善が進むが、リスクも高まる

多くの業界で、マシンやサービス、AIエージェント用に非人間アイデンティティ（NHI）の使用が急激に増えているのには、十分な理由があります。NHIによって、コラボレーションやイノベーション、生産性に対する企業の中核能力を強化できるからです。

しかしNHIは、AI活用時代に向けた企業の備えに役立つ一方で、攻撃者が悪用する可能性のある新たな攻撃ベクトルを作り出しています。AIエージェントは特に、人間のユーザーや従来のソフトウェアとは異なる動作をすることから、組織に新たなタイプの脆弱性をもたらします。非常に機密性の高いデータへのアクセスを必要とする場合が多いため、攻撃者にとっては一段と魅力的な標的となり、組織にとってはセキュリティ確保が困難な対象となります。

アイデンティティ・ファーストのセキュリティへの一元的なアプローチがなければ、NHIを活用する組織は、急速に拡大する攻撃対象領域を保護できずに、リスクを大幅に高めることになります。

一部の企業では

NHIの数が今や、人間のアイデンティティの**50倍**に達している

Forbes

46%の組織がこの1年でNHIのアカウントまたは認証情報の侵害を経験しており、さらに**26%**の組織は侵害を受けた可能性があると疑っている

TechTarget ESG

新たなリスクの時代

AWSなどのクラウドサービスやクラウド・プラットフォームの利用増加とともにNHIの利用も増加しており、生成AIツール、AIと自動化、デジタル・ワークフローでの利用が拡大しています。エンタープライズ・システムは、絶えず人間が監視しなくても安全かつ効率的に連携する必要があります。AIエージェントで使用されるサービスアカウントなどのNHIによってこれが可能になるのは、アプリケーションやサービスが相互に認証できるようになるからであり、結果として、自動化されたタスクやデータ交換、さらには、人間では不可能か、あるいは多大な時間を費やす必要があった複雑な業務プロセスを実現できます。

管理されていないNHIは非常に脆弱であるため、組織はこの新たなリスクを軽減するための戦略を検討しなければなりません。NHIが認証に使用するシークレットやキー、トークンが間違った人の手に渡ることがあれば、機密性の高いアプリケーションやデータに対して、攻撃者が深く、広範囲にアクセスできるようになってしまいます。

特に、非人間アイデンティティ（NHI）をチャットボットやデジタル・アシスタントのような生成AIツールで使用する場合、生成AIツールはユーザー・コンテキストを提供できないため、次のような脅威が新たに生じる可能性があります。

プロンプト・インジェクションとデータ・ポイズニング

攻撃者がプロンプトを操作したり、悪意のあるコンテンツを注入したりすると、生成AIツールがデータソースから不適切または不正確な情報を生成するようになる可能性があります。

シャドーアクセスとラテラル・ムーブメント

攻撃者が、生成AIツールを悪用して、接続されたシステム（Salesforce、Jira、社内Wikiなど、生成AIツールの問い合わせ先システム）から機密コンテンツにアクセスできるようになる可能性があります。

データの過剰なエクスポージャー

生成AIツールは、大量の機密データにアクセスする場合が少なくありません。基盤となるデータソースにユーザーのコンテキストが適切に伝わらない場合、ユーザーが役割に適切な範囲を超えて情報にアクセスしてしまう可能性があります。

51%の企業がAIエージェントを導入済み

PagerDuty

NHI関連の侵害を防止できる自信があると答えたセキュリティチームはわずか**15%**

Cloud Security Alliance

AIエージェント特有のリスク

NHIの潜在的なリスクとメリットが最も顕著に現れるのは、AIエージェントのケースです。AIエージェントは、人や組織に代わって自律的に行動することで、運用の効率化や、個人に合わせた自動的な顧客サービスを、これまで想像もできなかったレベルで実現します。

しかし、この能力は両刃の剣でもあります。AIエージェントは、改善を続けるためにデータやリソース、フィードバックを利用しますが、これらはすべて、認証、認可されたアクセスを利用します。これだけの広範なアクセスは、その背後にあるNHIを狙ってアイデンティティ・ベースの攻撃を仕掛けようとする攻撃者には格好の標的となります。

多くの組織では、非人間アイデンティティやマシン・アイデンティティは十分に監視されていないか、そもそも監視されていません。NHIが過剰な権限を付与されたまま、認証情報がローテーションされず、目的を終えた後でも長期間有効になっている場合が非常に多く、攻撃者に悪用されかねない重大な脆弱性が生み出されています。異なるシステムやアプリケーションにアイデンティティ機能が分散しているIT環境やセキュリティ環境では、こうした脆弱性が見過ごされ、気付いたときには手遅れという事態になりがちです。

アイデンティティは脆弱性。アイデンティティのセキュリティがその対応策。

要点：

NHIに関連した脆弱性を防御する最善の策は、まず、可視性と実施体制に不備を生み出している、ばらばらのアイデンティティ・システムを取り除くことから始まります。アイデンティティ・システムを単一のプラットフォームに統合することで、組織はNHIの制御を改善するとともに、管理効率を向上させることができます。最新のアイデンティティ・プラットフォームは、セキュリティに対するこのような統合アプローチの実現を支援します。

Amazon Bedrockで生成AIソリューションを開発する際には、迅速なデプロイメントとセキュアなアクセス・コントロールを両立させる必要があるため、これが特に重要になります。Oktaは、Bedrock環境でコントロールプレーンとして機能し、認可されたユーザーとAIエージェントだけが機密性の高いモデルやサービスにアクセスできるようにします。

Oktaでできること

Oktaのプラットフォームは、非人間アイデンティティやマシン・アイデンティティの管理に対して、堅牢かつ簡素化されたアプローチを可能にします。Oktaは、組織のアイデンティティ管理を1つのアイデンティティ・セキュリティ・ファブリックに統合することで、盲点をなくし、NHIがどこに存在し、何にアクセスできるかを包括的に把握できるようにします。

Identity Security Posture Management

- NHIの継続的な監視とリスク分析を提供
- 連携されていないローカルのサービスアカウントを自動検出し、リスクのあるNHIを特定
- マシン・アイデンティティのMFAギャップと認証情報の悪用を検出
- NHI関連のセキュリティ問題に対し、フレームワーク・コンプライアンス・マッピングとガイド付きの是正ワークフローを提供

Okta Privileged Access

- サービスアカウントのパスワードをセキュアに管理し、誰が何にどのくらいの期間アクセスできるかを定義したポリシーを適用
- シークレットを自動的にローテーションし、長期間有効な認証情報の露出を防止
- 誰または何がアカウントをチェックアウトしたかを監査、追跡

安全なアイデンティティ統合

SaaSアプリケーションとの高度なセキュリティ統合によって、長時間のNHIアクセスを防ぎ、エコシステム全体のNHIを保護します。

- **ライフサイクルとエンタイトルメント管理：**NHIのアイデンティティのプロビジョニングとプロビジョニング解除を自動化し、ジャストインタイム・アクセスを確保
- **統合シングルサインオン（SSO）とポリシー適用：**SSOとセキュリティ・ポリシーをサービスアカウントとマシン・アイデンティティに拡張
- **ワークフローの自動化とセッションの終了：**自動化オフボーディングとセッション失効を実施し、孤立したNHIの発生を防止

Okta + Amazon：セキュアな生成AI運用の鍵

Amazon Qは、AWSを使用して構築するすべてのユーザーに生成AIを活用した支援を提供することで、ソフトウェア開発者、ビジネス・インテリジェンス・アナリスト、コンタクトセンターの従業員などの中核チームの業務遂行方法を変革しています。

Amazon Qの効率性や生産性、CXの利点と、OktaのAI対応セキュリティツールのスイートを組み合わせることで、組織は強力な生成AIを新たなリスク源にさらすことなく、中核業務の枠組みに組み込むことができます。

生成AIのセキュアな導入

Oktaのエンタープライズ・レベルのアイデンティティ・セキュリティで、Amazon Qに保存されているデータを不正アクセスから保護しながら、自動化を活用したOktaのライフサイクル管理ツールでアイデンティティ管理を効率化できます。

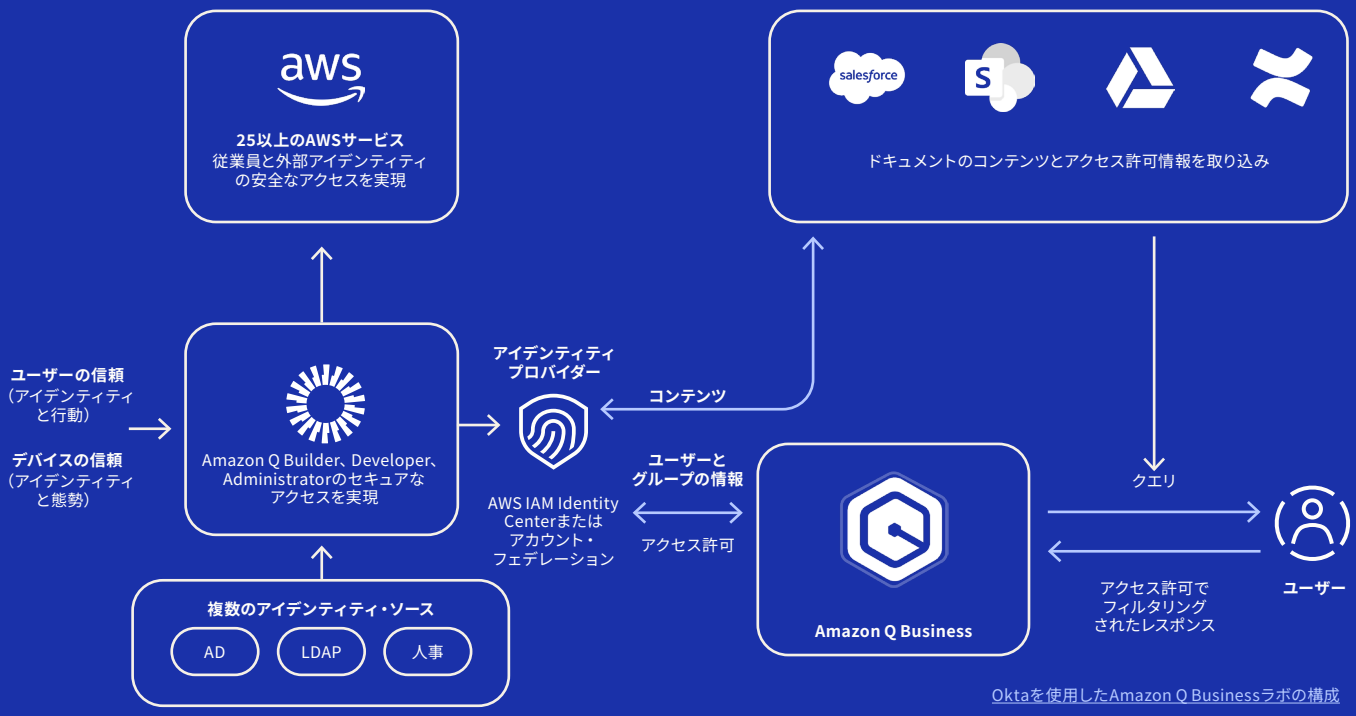
生産性の最大化

Amazon Qの支援を活用すれば、チームはより創造的かつ生産的になれます。会議の要約の作成、コンテンツの作成、作業の完了を、新たなリスクにデータをさらすことなく実行できます。

シームレスなアクセスを提供

特定のデータセットへのロールベースのアクセスによって、合理的でセキュアなアクセスを実現します。リクエストに応じて、または自動化ベースの条件に基づいてサブスクリプションを付与することで、コストをより適切に管理できます。

OktaでAmazon Q Businessを最大限に活用



Oktaを使用したAmazon Q Businessラボの構成

非人間アイデンティティをセキュアに活用

AIは、記録的な速さで、将来の優位性という仮説的存在から、現在の必須要素へと変化しました。競争力を維持しようとする組織なら当然、AIエージェントのような最新ツールを最大限に活用する必要があります。しかし、NHIを効果的に利用できるかどうかは、組織がNHIを保護できるかどうかによって決まります。

Oktaでは、AIを活用したワークフローが統合アイデンティティ・プラットフォームで実行されます。このプラットフォームは、リスクをもたらす分断化を解消し、セキュリティ・エコシステムの基盤を強化します。これらはすべて、Oktaのアイデンティティ・セキュリティ・ファブリックによって実現されます。

これが、AWSとOktaが連携して、次世代のインテリジェント・オートメーションのためのセキュアな基盤を提供している理由です。AWSでAIエージェントを展開する場合でも、チーム全体でAmazon Qを活用する場合でも、Oktaのアイデンティティ・プラットフォームが、アイデンティティの安全性、ガバナンス、監査可能性の確保を支援します。

セキュリティ戦略をOktaのアイデンティティ・セキュリティ・ファブリックに統合する方法の詳細は、当社チームにお問い合わせください。
Okta Platformの実際の動作をご確認いただけます。