すべてのアイデンティティを管理：アイデンティティガバナンスをモダナイズするための5つのステップ

AIの急速な普及とクラウドの拡大が進む現代の情勢では、従来のネットワーク境界は弱体化しており、アイデンティティガバナンスがセキュアな環境に不可欠な基盤となっています。本チェックリストは、防御能力を監査し、人間アイデンティティと非人間アイデンティティの間に生じるセキュリティギャップを埋めるための戦略的ロードマップを提供するものです。最初のインベントリ作成からライフサイクル管理の自動化まで、これらの主要なカテゴリに対処することで、組織は、すべてのアイデンティティ（人間のユーザー、非人間アイデンティティ（NHI）、AIエージェント）をもれなく管理対象として記録し、最小特権の原則に基づいて管理しながら、リスクを継続的に監視するための措置を講じることができます。

すべてのアイデンティティを一覧化する

Identity Security Fabric全体で単一の信頼できる情報源を確立することで、シャドーAIや未管理のサービスアカウントによって生まれる、管理の目が届かない領域を減らすことができます。

- ☐ すべてのユーザー、非人間アイデンティティ（NHI）、AIエージェントを一覧化する
- ☐ 承認済みのアカウントだけでなく、あらゆる種類のシャドーアカウントも含める
- ☐ エージェントプラットフォーム（AWS Bedrock、Vertex AIなど）をスキャンする
- ☐ クラウド、オンプレミス、SaaSプラットフォーム全体で、すべてのアイデンティティ（ワークフォースと非人間）を特定する
- ☐ 有効な所有者が存在しない孤立アカウントや休眠アカウントを検出する
- ☐ 各アイデンティティがアクセスできるシステムやデータとの対応関係を明確にする

人間の担当者を割り当てる

すべてのデジタルエンティティを責任者に紐づけることで、すべての自動化されたアクションが、明確な業務上の目的や背景に基づいて実行されていることを担保できます。

- ☐ それぞれのアイデンティティ（人間ユーザー、非人間アイデンティティ（NHI）、AIエージェント）に対して、責任を持つ個人やチームを割り当てる
- ☐ 各アイデンティティの業務上の目的を文書化する
- ☐ 従業員の異動や退職時に、所有権が引き継がれるようにする
- ☐ 正当に割り当てられた有効な所有者が存在しないアイデンティティを検出し、利用停止にする

okta

最小権限を適用する

ゼロスタンディング特権（ZSP）モデルに移行することで、アクセス権が永続的にならず、認証情報が侵害された場合の影響を大幅に軽減できます。

- ☐ 必要最小限の範囲に限定してアクセス権を付与し、それ以上は付与しない
- ☐ 有効期間の長い永続的な認証情報の代わりに、ジャストインタイム（JIT）トークンを使用する
- ☐ APIキーや静的な認証情報がコードやパイプライン内にハードコーディングされないようにする
- ☐ 委任アクセスやサブエージェントのアクセス権は、保証元アイデンティティのスコープよりも狭くなるように制限する
- ☐ 不適切な権限の組み合わせを特定・修正して、職務の分離（SoD）を徹底する

アクセスレビューを標準化する

全種類のアイデンティティに対して一貫したアクセス認定基準を適用することで、常に権限が実際の業務ニーズと整合するよう継続的に検証できます。

- ☐ サービスアカウントとエージェントにも、従業員と同じレビューやアクセス認定の基準を適用する
- ☐ 高リスクのユーザーやエージェントに対して、定期的なアクセス権の再認定レビューを実施する
- ☐ 対象となるすべてのアイデンティティについて、SoD違反や権限の競合がないかを定期的に確認する
- ☐ 業務上正当な理由がなくなったアクセス権を取り消す
- ☐ 本来のスコープを超えて拡大した権限があればフラグを立てる
- ☐ 承認されたSoD例外を含め、すべての例外について文書化し、有効期限を設定する

ライフサイクル管理を自動化する

利用開始からオフボーディングまで、アイデンティティのライフサイクルを自動化することで、手動対応に頼ることなく、ビジネスのスピードに合わせてセキュリティを運用できるようになります。

- ☐ アイデンティティのプロビジョニングはすべて、所定の申請プロセスとワークフローに従って実施する
- ☐ ワークフローやタスク、または雇用関係が終了した際に、認証情報を自動的にプロビジョニング解除する
- ☐ 認証情報の有効期限を、役割やタスクの期間に応じて設定する
- ☐ 担当従業員のオフボーディング時には、エージェントのアクセス権を取り消すようにする
- ☐ 全種類のアイデンティティで、未使用アカウントや孤立アカウントの検出を自動化する

Lifecycle Management

新規作成・権限変更・削除に伴うプロセスを自動化し、手作業をなくしてセキュリティギャップを解消します。

okta

ガバナンス戦略を最適化する

ガバナンス態勢の刷新に向けて、セキュリティ主導のガバナンスに関する当社のeBookをご覧ください。サイロ化された手動プロセスから脱却し、エコシステム内の人間ユーザー、非人間アイデンティティ（NHI）、AIエージェントのすべてに対して、自動化されたレジリエンスを実現する方法をご紹介します。

今までに述べた要件の多くにすでに対応できている企業にも、これから環境の棚卸しを始める段階の組織にも、Okta Identity Governanceは、ガバナンス態勢を刷新するために必要な戦略的基盤を提供します。

サイロ化された手動プロセスから、統合されたIdentity Security Fabricへと移行することで、組織はすべての人間ユーザーや非人間アイデンティティ、AIエージェントのライフサイクル全体を自動化できるようになります。

静的な権限付与から脱却し、自動化された継続的なレジリエンスモデルを採用して、ビジネスのスピードを損なうことなく、最小権限と「ジャストインタイム」アクセスを適用しましょう。

Okta Identity Governanceの詳細を見る

Okta会社概要
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。