AIエージェントのアイデンティティセキュリティ準備状況早見表

企業は現在、システムやクラウド環境、顧客向けアプリケーションへのAIエージェントの導入に熱心に取り組んでいます。しかし、準備態勢は、導入に対する熱意に必ずしも追いついていません。**組織の91%**がすでにAIエージェントを活用している一方で、**ほぼ50%は正式な監督体制を欠いており**、ガバナンスや制御に関連した新たな課題が生まれています。

こうした非人間アイデンティティ（NHI）は、パワフルな新機能を実現する一方で、同等にパワフルなリスクももたらします。強固なアイデンティティフレームワークがなければ、AIエージェントは攻撃対象領域を広げていき、従来の制御方法では管理できないセキュリティ上の欠陥を生み出します。

AIエージェントを安全かつ大規模に統制するには、**初期のパイロット段階から完全な本番環境への展開まで、エージェントのライフサイクル全体を保護する、アイデンティティ優先のセキュリティ基盤**を整える必要があります。

このAI準備状況早見表を利用すると、AIエージェントのエコシステム全体で**大規模に可視性を維持し、制御を徹底して、コンプライアンスを検証するための**アイデンティティセキュリティ手法を手軽に確認できます。

大部分の組織がすでにAIエージェントを活用している一方、50%近くで正式な監視体制が整っていません。

AIエージェントのエコシステムで中核となるアイデンティティセキュリティの手法

すべてのエージェントを管理する	組織全体で、AIエージェントに対して一元的な可視性と制御を確立する
01. AIエージェントとNHIを検出・追跡する	すべての環境で稼働しているAIエージェントと関連サービスアカウントを継続的に検出・追跡します。これにより、管理されていないアイデンティティが既存のガバナンスや監視の制御下を外れて動作することを防ぎます。
02. エージェント登録を一元化する	検出したエージェントを登録し、所有権や許可を割り当てます。登録の一元化により、AIシステム全体での答責性・可監査性・可視性が向上します。
03. AIエージェントのアイデンティティのガバナンスを一元化する	一元化されたアイデンティティシステムを通じて、プロビジョニング・認証・認可・プロビジョニング解除を管理します。統合プラットフォームにより、断片化を解消し、ポリシーの一貫性を向上させ、スケーラビリティをサポートします。
04. AIエージェントのアクティビティをリアルタイムで継続的に監視する	AIエージェントに関連した認証アクティビティ、APIの呼び出し、行動パターンをリアルタイムで監視します。リアルタイムの可視性により、不正利用や異常、侵害された認証情報をすばやく検知できます。
05. システム全体でAIエージェントの操作をログ記録・監査する	認証イベントやアクセス試行、エージェントが開始した操作を記録・監査します。確実なログ記録により、インシデント対応、コンプライアンスの検証、ガバナンスの徹底を支えます。

すべてのエージェントを保護する

組織の意図に沿って、安全かつ予測可能に動作するAIエージェントを導入する

06.

エージェントのセッションを検証済みの人間のアイデンティティに結び付ける

エージェント操作が行われる前に、人間のアイデンティティを検証・確立し、帰属性・答責性・信頼性を確保します。

07.

トークンや認証情報、シークレットを専用のボールトで保護する

長時間有効のトークン、認証情報、シークレットは、エージェントに埋め込むのではなく、切り離されたセキュアなボールトに保管します。有効期間の短いトークンを実行時に発行し、影響範囲を狭め、漏洩を防ぎます。

08.

認可チェックとヒューマンインザループに基づく制御を徹底させる

エージェントに、許可された場合のみ行動できる権限を付与し、リスクの高い操作については人間の承認を義務づけます。

09.

AIエージェントに最小権限アクセスを適用する

エージェントの行動範囲を、認可されたリソースと認可された操作のみに制限します。リクエスト時の評価に基づいて認可されるため、行動範囲が、限定された予測可能なものになります。

準備から実践へ

AIエージェントのエコシステムを制御しませんか。AIアイデンティティセキュリティコンプライアンスチェックリストを確認し、次のステップに役立てましょう。