*本プレスリリースは、米国で2026年4月16日（現地時間）に発表されたプレスリリースの抄訳版です。原文はこちらをご参照ください。

報道関係各位

プレスリリース
2026年5月19日
Rubrik Japan株式会社

Rubrik、エージェント型AIの導入加速で拡大するセキュリティギャップに警鐘

Rubrik Zero Labsの最新調査によると、日本企業が完全に可視化や復旧できないエージェント型システムの導入を急速に進める中、アイデンティティガバナンスの重大な欠如が浮き彫りに

セキュリティおよびAIオペレーション分野のリーダーであるRubrik（本社：米国カリフォルニア州パロアルト、CEO：ビプル・シンハ（Bipul Sinha）、以下 Rubrik）は本日、Rubrik Zero Labsの最新の調査レポートを発表しました。同調査では、企業におけるAIエージェント導入の動きが、そのセキュリティ対策の整備を上回るスピードで進んでいることが明らかになりました。また、組織がガバナンスに必要な制御を十分に備えないままエージェント型システムの運用を進めており、イノベーションとセキュリティの間にギャップが生じていることが判明しました。

本調査は、1,600人のITおよびセキュリティリーダーを対象に実施され、以下の結果が明らかになりました。

- 回答者の86%（日本：83%）は、今後1年以内にAIエージェントの急増が自社のセキュリティガードレールを上回ると予測しています。
- 自社のIT環境でアクティブなAIエージェントを完全に監視できていると回答したのはわずか23%（日本：38%）に留まりました。なお、レポートではこうした自己申告による数値は、実態より高く出ている可能性を指摘しています。その結果、すでに意思決定やアクションの実行、重要なデータと連携しているアイデンティティを十分に保護できない状況が生じています。

この課題は、アイデンティティの急増によってさらに深刻化しています。エージェントに紐づく非人間アイデンティティは、企業による追跡やガバナンスが追いつかない速度で増加しており、研究者はこれを「シャドーワークフォース」と呼んでいます。こうしたアイデンティティは、恒常的なアクセス権と限定的な監視のもとで運用される場合が多く、不正利用や侵害、横展開の新たな経路を生み出しています。

同時に、AIエージェントの運用に対する期待も揺らいでいます。調査では以下の点も明らかになりました。

- 回答者の80%以上（日本：86%）は、エージェント導入による効率化よりも、人手による管理負担の方が大きいと回答しています。また、88%（日本：84%）はシステム全体をリセットすることなくAIエージェントが行った特定のアクションを元に戻す機能を備えていないと回答しています。
- 復旧および予防は、主要な課題として浮上しています。エージェントによる脅威が拡大する中、約9割のリーダー（日本：88%）が復旧目標を達成することに懸念を表明しています。

脅威そのものも加速しています。回答者の約半数は、今後1年以内にはエージェント型システムが攻撃の大半を占めるようになると予想しており、攻撃者の手法が大きく変化していることが示されています。エージェント型システムは、攻撃までの時間を短縮し、攻撃規模が拡大させるとともに、内部リスクと外部からの侵害の境界を曖昧にしています。

Rubrikの最高トランスフォーメーション責任者であるカヴィサ・マリアパン（Kavitha Mariappan）は、次のように述べています。「AIの導入は、それを制御する能力を上回るスピードで進んでいます。企業は完全に可視化、管理、復旧できないシステムを導入し、対応に苦慮しています。私たちは、AIがリスクであるかどうかという議論する段階を超え、より厳しい現実に向き合う必要があります。意思決定が人間からマシンへと移行する中、すべてのリーダーにとって、自律化が進む環境において運用上の安全性を維持することは重要な課題です。」

企業の取締役会や経営陣にとって、その影響は即座に現れます。AI戦略は今やレジリエンス戦略と切り離せして考えることはできません。組織がコントロールの仕組みよりも導入スピードを優先し続けた場合、障害の封じ込めや復旧ができない環境を生み出すリスクがあります。

Renown Healthのバイスプレジデント兼最高情報セキュリティ・技術責任者であるスティーブン・ラミレス（Steven Ramirez）氏は、次のように述べています。「アイデンティティの検証は、人手によるボトルネックを生じさせることなく、AIによる自動化の恩恵を最大限に引き出すための基盤です。検証と可視性は、健全かつ安全なエージェント型システム導入の前提条件です。」

Rubrik Zero Labsのレポート「エージェントの現状：導入、リスクおよびその軽減策の理解（The State of the Agent: Understanding Adoption, Risk, and Mitigation）」は、AIシステムにおけるツール層、認知層、アイデンティティ層の各レイヤーにまたがる新たな攻撃ベクトルについて、技術分析とグローバル調査データを組み合わせたものです。本調査は、現在進行している変化として、セキュリティの焦点が単なる侵害の防止から、人間の介入を待たずに動作するシステムの制御維持へと移行していることを示しています。

Rubrik Zero Labsの調査レポートの全文は、こちらをご覧ください。
英語版はこちらからご覧ください。

Rubrik（ルーブリック）について
Rubrikは、セキュリティとAIオペレーションをリードする企業として、データ保護、サイバーレジリエンス、エンタープライズAIの活用推進を支える領域で事業を展開しています。Rubrik Security Cloudは、クラウド全体のデータ、アイデンティティ、ワークロードを保護、監視、復旧することで完全なサイバーレジリエンスを提供します。Rubrik Agent Cloudは、AIエージェントのアクションを監視・監査し、リアルタイムでガードレールを適用、精度向上のための微調整を行い、さらに誤動作を元に戻すことで、信頼できるAIエージェントの大規模導入を加速します。

Webサイト：https://www.rubrik.com/ja/

本件に関するお問い合わせ先：
Rubrik Japan 広報代理（ホフマンジャパン株式会社内）
担当: 張 / 西村 / 竹房 / 田中
Email: RubrikJP@hoffman.com