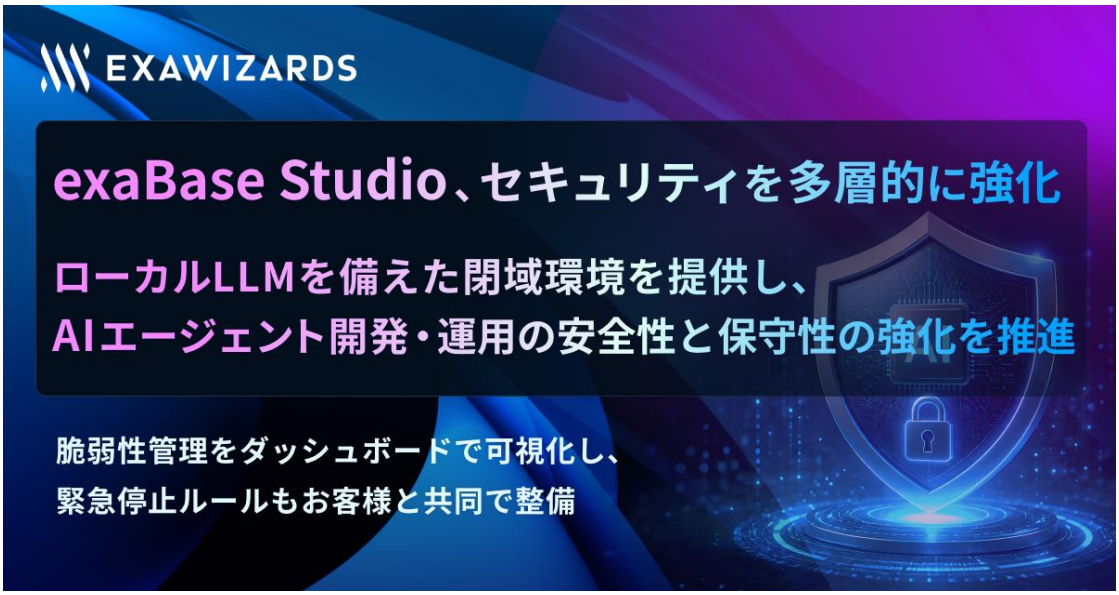
News Release

2026 年 11 月 11 日
株式会社エクサウィザーズ
（コード番号：4259 東証グロース）

exaBase Studio、セキュリティを多層的に強化
ローカル LLM を備えた閉域環境を提供し、AI エージェント開発・運用の安全性と保守性の強化を推進

～SaaS 版では脆弱性管理をダッシュボードで可視化し、緊急停止ルールもお客様と共同で整備～

株式会社エクサウィザーズ（東京都港区、代表取締役社長 CEO：春田 真、以下エクサウィザーズ）は、AI エージェントの開発・運用プラットフォーム「exaBase Studio」のセキュリティを多層的に強化します。プライベートクラウド版を中核として、インターネットから切り離したお客様専用の閉域環境に、AI エージェントの実行・統制基盤、AI 駆動開発環境、ローカル LLM をまとめて構築します。これにより、機密性の高い実データを外部に出すことなく AI エージェントの開発・検証を行え、稼働後の原因調査や保守も効率化できます。本ソリューションは、エクサウィザーズグループ 4 社が一体で提供します。
あわせて SaaS 版では、自社インフラのセキュリティ監視にクラウドセキュリティプラットフォーム「Wiz[*1]」を採用し、お客様が開発・実行するコンテナ環境を含めた脆弱性の継続的な監視体制を強化します。あわせて、exaBase Studio 上でお客様が自社環境の安全性ステータスを確認できるセキュリティダッシュボード機能を提供するとともに、重大な脆弱性発見時の緊急停止条件や対応方針について、お客様と協議しながら運用ルールを明確化します。
これらの取り組みを通じて、閉域環境での安全な AI 駆動開発・運用から、脆弱性の継続的な管理まで、企業のセキュリティ要件に応じた AI 活用を支援します。



☑ 背景：サイバー攻撃の高度化に伴い、AI サービスにも包括的なセキュリティ対策が必要に

近年、ソフトウェアの脆弱性を悪用した侵入やサプライチェーン攻撃、ランサムウェアなどによる被害が相次いでいます。さらに、生成 AI が攻撃対象の調査やフィッシング、マルウェア開発などに活用されるようになり、サイバー攻撃の高度化・効率化が進んでいます。企業にはこうした脅威の変化に応じた、より高度で継続的なセキュリティ対策が求められています。

同時に、AI の業務利用が広がる中で、アプリケーションだけでなく、ネットワーク、認証・認可、データ、LLM、開発環境までを含めた多層的なセキュリティ対策が不可欠となっています。

加えて、AI エージェントの活用を進める企業からは、別の課題も挙がっています。AI エージェントは実際の業務データや利用状況によって動作が変わるため、本番データを用いた検証が品質確保に不可欠です。しか

し機密性の高いデータを外部の LLM サービスや開発サービスに送信できず、実データでの開発・検証に踏み込めないという制約が生じています。
エクサウィザーズグループは、こうした脅威環境の変化と企業の実務上の制約の双方に応えるため、exaBase Studio のセキュリティを多層的に強化します。

☑ 閉域型 AI 基盤：exaBase Studio のプライベートクラウド版とローカル LLM・AI 駆動開発環境を統合
本ソリューションの最大の特長は、AI エージェントを動かす基盤だけでなく、それを開発・保守するコーディングエージェントと、両方が利用するローカル LLM までを、お客様専用の閉域環境にまとめて配置できる点にあります。
具体的には、Microsoft Azure や AWS などのお客様専用のプライベートクラウド環境に、MCP Gateway・MCP Registry・認証・認可サービスを備えた exaBase Studio、AI 駆動開発環境、専用 GPU 上のローカル LLM を構築し、閉域ネットワーク内で連携させます。インターネットから直接アクセスできる入口は設けず、お客様のセキュリティ要件に応じた環境を提供します。
これにより、機密性の高い本番データや実行ログを外部の LLM・開発サービスに送信することなく、AI エージェントの開発・検証から、稼働後の原因調査・修正・回帰評価までを AI 駆動開発によって効率化し、開発・保守にかかる負荷の低減を目指します。
本構成は、以下の 3 つの基盤で成り立っています。

（1）AI エージェント実行・統制基盤：MCP Gateway・認証認可を統合し、安全な業務システム連携を実現
exaBase Studio の AI エージェント開発・実行環境に、MCP Gateway、MCP Registry、AI Gateway、認証・認可サービスを組み合わせます。AI エージェントの実行環境を隔離し、LLM や業務システムへのアクセスを共通の仕組みで統制します。
また、AI エージェントごとに固有の ID を持たせる NHI（Non-Human Identity）への対応や、利用者の権限に基づいて外部 SaaS や業務システムにアクセスする認可方式にも対応できるよう設計しています。
これにより、既存の ID 基盤や、メール、チャット、文書管理などの業務サービスとの連携を想定した、安全で拡張性の高い AI エージェント実行環境を提供します。

（2）AI 駆動開発環境：本番データを活用した開発・検証から、稼働後の監視・保守までを効率化
コーディングエージェントを利用できる AI 駆動開発環境を、お客様のプライベートクラウド内に構築します。
開発段階で想定したシナリオだけでは、AI エージェントの品質を十分に確保することは困難です。本構成では、適切な権限管理の下で、閉域内に保持した本番データを用いて、動作検証、プロンプトや設定の調整、プログラム修正、回帰評価などを AI 駆動開発によって進められます。
本番稼働後も、コーディングエージェントが実行ログや関連するプログラム・設定を適切な権限の下で参照し、異常の分析、原因・影響調査、修正案の作成、テストの生成・実行などを支援します。

（3）ローカル LLM 基盤：AI エージェントの実行と AI 駆動開発の両方を、閉域内の LLM で支援
お客様専用の GPU 環境にオープンウェイトの LLM を配置し、AI エージェントの推論処理だけでなく、コーディングエージェントによる AI 駆動開発にも活用します。
これにより、本番データを海外の LLM サービスに送信できない企業に対しても、実データを活用した AI 駆動開発の選択肢を提供します。外部 LLM の利用に伴うデータ管理上の制約を軽減するとともに、AI 駆動開発に必要な LLM 利用コストの最適化にも取り組みます。

☑ SaaS 版：脆弱性の可視化と、お客様と連携したセキュリティ運用の強化
プライベートクラウド版による閉域型 AI 基盤の提供とあわせて、SaaS 版でも脆弱性管理とセキュリティ運用を高度化します。

（1）セキュリティステータスの可視化

exaBase Studio の SaaS 版では、お客様が開発したアプリケーションのコンテナを含め、クラウドセキュリティプラットフォーム「Wiz」による継続的な脆弱性検知・インフラ監視を実施しています。

今後は、exaBase Studio の機能の一環として、お客様が開発したアプリケーションや稼働コンテナの健全性・脆弱性に関するセキュリティステータスを、専用ダッシュボード上で確認できる機能を提供します。これにより、お客様との間でリスク情報を迅速に共有し、透明性の高いサービス運用を実現します。

（2）お客様と連携した脆弱性対応・緊急停止ルールの明確化

重大な脆弱性が発見された場合には、脆弱性の重大度だけでなく、外部からの到達可能性や実際の影響範囲、既存の防御策などを踏まえた対応判断が重要になります。

エクサウィザーズグループは、お客様との協議を通じて、脆弱性発見時のリスク評価、対応の優先順位、緊急停止・機能制限の判断条件、情報共有や復旧の方針などを事前に明確化する取り組みを開始します。
対応方針をあらかじめお客様と共有することで、セキュリティと業務継続性を両立したサービス運用を推進します。



図：exaBase Studio 異なる提供形態に応じた 2 つのセキュリティアプローチ

☑ エクサウィザーズグループの強み：AI エージェントの開発から運用・保守までを一体提供

エクサウィザーズグループ 4 社は、exaBase Studio を中核に、グループ各社が持つ AI 駆動開発、ローカル LLM、セキュリティなどの専門技術を組み合わせ、企業の AI 活用を総合的に支援します。

担う領域	会社・製品
業務設計、AI エージェント基盤の提供、全体統括	エクサウィザーズ（exaBase Studio、「一緒に設計」）
AI 駆動開発環境の構築、開発・テスト支援	Exa Frontier Edge
ローカル LLM 基盤の構築・運用	Exa Interaction Design Lab
AI セキュリティ診断・レッドチーミング	ExaSecurity

AI エージェントの設計・開発から、本番稼働後の監視、セキュリティ対策、保守・継続改善までをグループ一体で支援します。お客様が複数のベンダーや技術を個別に組み合わせ、それぞれと調整する必要はありません。

また、脆弱性への対応や本番稼働後の問題調査においても、AI エージェント基盤、開発環境、ローカル LLM などの各領域の専門家が連携し、安全かつ効率的なサービス運用を支援します。

☑ **今後の展開**

エクサウィザーズグループは、今後の展開として次の 3 点に取り組みます。

1. 対象業種の拡大

金融・製造・建設・公共など、機密性の高いデータの取り扱いや厳格なセキュリティ統制が求められる企業に向けて、exaBase Studio のプライベートクラウド版と、閉域型ローカル LLM 基盤・AI 駆動開発環境を組み合わせたソリューションの展開を進めます。

2. 対応プロセス全体の AI 活用

脆弱性の検知や AI エージェントの動作異常の把握にとどまらず、影響範囲の調査、対応策の検討、プログラムの修正、検証までを一連のプロセスとして AI で効率化する仕組みを整備します。人による判断・承認は維持したうえで、セキュリティ対策の精度向上と、開発・運用・保守の省力化を両立していきます。

3. 多数の AI エージェントを支える共通基盤化

企業内で稼働する AI エージェントが増加し、複数の業務システムを横断した自動化が進むことを見据え、認証・認可、実行管理、監査、セキュリティ対策を共通基盤として整備します。

エクサウィザーズグループは、各社の専門技術を結集し、企業が多数の AI エージェントを安全かつ効率的に開発・運用し、継続的に改善できる環境の提供を推進します。

なお、本件が 2027 年 3 月期業績に与える影響は軽微であります。

*1 Wiz, Inc. が提供するクラウドセキュリティプラットフォーム。本サービスでは、exaBase Studio のサービス提供基盤および稼働環境の安全管理・セキュリティ運用のために当社が導入・活用しています。

*2 記載されている会社名、製品・サービス名は、各社の登録商標または商標です。

【エクサウィザーズ 会社概要】

会社名　：株式会社エクサウィザーズ（証券コード 4259）
所在地　：東京都港区芝浦 4 丁目 2−8 住友不動産三田ファーストビル 5 階
設立　　：2016年2月
代表者　：代表取締役社長CEO　春田 真
事業内容：AIを利用したサービス開発による産業革新と社会課題の解決
URL：https://exawizards.com/

<広報に関するお問い合わせ先>
株式会社エクサウィザーズ　広報　メール：publicrelations@exwzd.com