

SB C&S、Zenity とディストリビューター契約を締結 AI エージェント向けセキュリティプラットフォームの 日本国内における取り扱いを開始

「新しいテクノロジーをいち早く、より使いやすい仕組みやかたちにして全国にお届けする」というソフトバンク創業以来の役割を担う SB C&S 株式会社（以下「SB C&S」）は、Zenity, Inc.（本社：米国ニューヨーク州、CEO：Ben Kliger、以下「Zenity」）とディストリビューター契約を締結し、Zenity が提供する AI エージェント向けセキュリティプラットフォームの日本国内における取り扱いを開始します。



近年、生成 AI の活用が広がる中、企業では AI エージェントを業務プロセスに組み込み、データへのアクセスや各種ツールとの連携、タスクの自動実行などに活用する動きが進んでいます。一方、AI エージェントはユーザーに代わってさまざまなシステムやデータへアクセスし、自律的に処理を実行するため、従来のセキュリティツールでは、AI エージェントが「何を行っているのか」「なぜその処理を行っているのか」「どのデータへアクセスしているのか」「どのようなアクションを実行しているのか」を十分に可視化できない場合があります。

今回、SB C&S が取り扱う Zenity のセキュリティプラットフォームは、SaaS や独自開発環境、エンドポイントなどに存在する AI エージェントを可視化し、その設定や権限、実行時の挙動を継続的に把握することで、企業における AI エージェントの安全な利用を支援するソリューションです。AI エージェントのプロンプト、ツール、ID、権限、データアクセスなど、各エージェントの実行状況をエンドツーエンドで可視化しつつ、リスクのある設定、過剰な権限、攻撃経路を特定します。また、ポリシーに基づく制御や実行時の脅威検知・対応により、AI エージェントの開発から利用時まで一貫して保護します。

SB C&S は、Zenity 製品の取り扱いを通して企業が AI エージェントを活用する上で必要となる可視性とガバナンス、セキュリティ対策の整備を支援します。また、全国約 1 万 5,000 社の販売ネットワークと、これまで培ってきたセキュリティ分野の知見を生かし、日本企業における AI エージェントの安全な導入の実現に貢献します。

【主な特長】

- ・ AI エージェントの利用状況とリスクを可視化
環境内で稼働する AI エージェントを継続的に把握し、プロンプトやツール、データアクセスなどの実行

状況をステップ単位で可視化します。また、AI エージェントの攻撃経路や MCP (Model Context Protocol) 連携、サプライチェーンの依存関係などを確認し、設定不備や過剰なアクセス権限、ポリシー違反などのリスク把握を支援します。

- ・ **ポリシーに基づく AI エージェントの制御**

AI エージェントの実行内容やコンテキストに応じて、組織のセキュリティポリシーを適用します。AI エージェントがアクセスできる環境やリソースを制限するとともに、特定の処理に必要な最小限の権限のみを付与することで、不要な常時権限を削減します。

- ・ **実行時の脅威を検知し、インシデント対応を支援**

AI エージェントの実行時の挙動を継続的に監視し、プロンプトインジェクション、ツールの不正利用、未承認のアクションなど、AI エージェント特有の脅威を検知・封じ込めます。インシデント発生時には、最初のプロンプトからツール呼び出し、データアクセス、結果として実行されたアクションまで、AI エージェントの一連の実行過程を再構築し、原因の特定、影響範囲の把握、対応を支援します。

【製品の詳細】

<https://zenity.io/>

【製品に関するお問い合わせ】

sbcasgrp-security-marketing@g.softbank.co.jp

Zenity, Inc. VP Business Development, Harrison Johnson 氏からのエンドースメント

企業では、AI エージェントの実験段階から、重要な業務プロセスへの導入へと急速に移行しています。日本はこの変化において重要な市場であり、SB C&S は、その規模、セキュリティに関する専門知識、顧客基盤を生かし、企業による AI エージェントの安全な導入を支援できるパートナーです。Zenity の AI Agent Security Platform を日本の企業に届けるため、共に取り組めることを大変うれしく思います。

Zenity, Inc.について

Zenity は、自律型 AI 向けの AI Security Platform を提供し、SaaS、クラウド、エンドポイントなど、AI エージェントが稼働するあらゆる環境を保護します。Gartner から AI Agent Governance 分野の「Company to Beat」に選出されており、AI エージェントとそのエクスポージャーの把握から、意思決定レイヤーにおける Runtime Boundaries の適用、エージェント活動への対応まで、エージェントのライフサイクル全体にわたってセキュリティチームに可視性と制御を提供します。エージェントの意図、意思決定、アクション、アクセス、相互作用を把握することで、セキュリティや制御を損なうことなく、企業による自律型 AI の安全な拡張を支援します。詳細は <https://www.zenity.io/> をご覧ください。

- SoftBank およびソフトバンクの名称、ロゴは、日本国およびその他の国におけるソフトバンクグループ株式会社の登録商標または商標です。
 - その他、このお知らせに記載されている会社名および製品・サービス名は、各社の登録商標または商標です。
-