

企業のAI活用をセキュアに支える「AI-SPMソリューション」を提供開始

NTTドコモビジネス株式会社(旧 NTTコミュニケーションズ株式会社、以下 NTTドコモビジネス)は、企業のAI活用の実態を踏まえ、AIに対するセキュリティ対策(Security for AI)の一環として、Wiz Cloud Japan 株式会社のCNAPP^{※1}製品である「Wiz^{※2}」を活用した「AI-SPM^{※3}ソリューション」(以下 本ソリューション)の提供を開始します。

1. 背景

近年、企業におけるAI活用は急速に進展しており、業務効率化や新たな価値創出の手段として注目されています。しかしながら、従来のサイバー攻撃手法とは異なるAI環境への攻撃に対しては、セキュリティ対策のベストプラクティスが確立されておらず、各企業が手探りで対策を進めているのが現状です。

その中でも、クラウド上にAI環境を構築する際に検討すべきセキュリティ上の主な課題である「AIリソースの可視化」、「設定ミスの検出」、「脆弱性対策」「機密情報や学習データの保護」への対策は急務です。

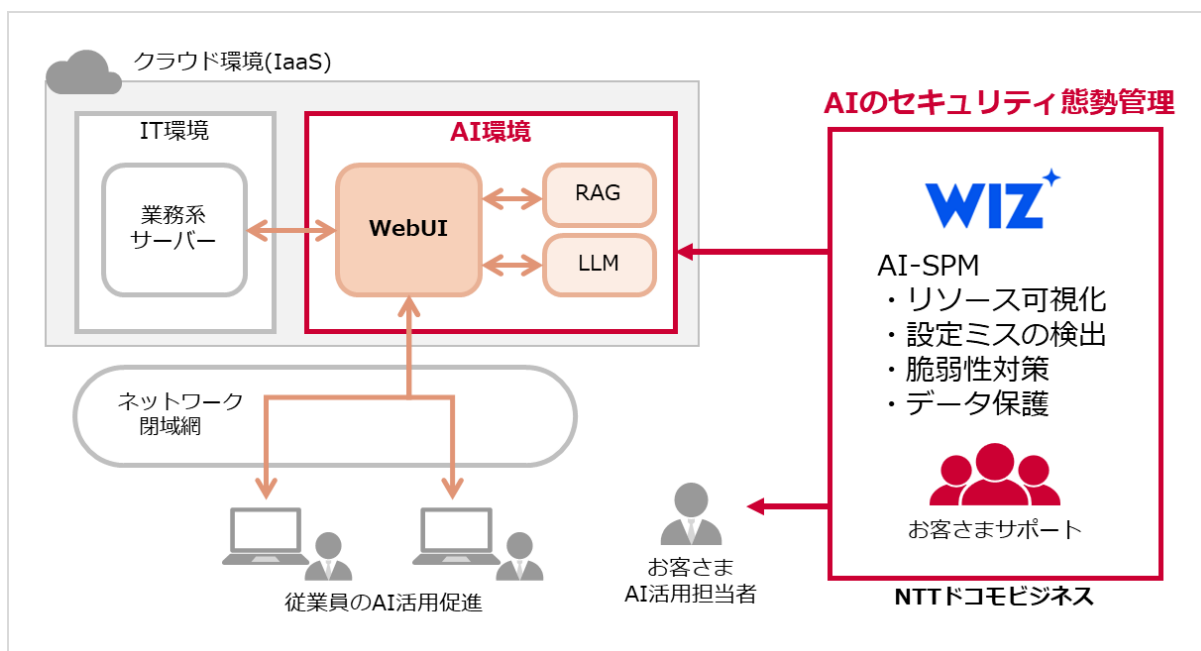
NTTドコモビジネスでは、AIに対するセキュリティ対策の一環として、CNAPP製品として定評のある「Wiz」を活用し、NTTドコモビジネスの運用ノウハウを組み合わせることで、お客さまのAI環境に対するセキュリティ強化を支援します。

2. 本ソリューションの概要

本ソリューションは、クラウド上にAI環境を構築するお客さまが対象になります。AI-SPMを活用し、クラウド環境にあるAI環境を構成するコンポーネント(仮想サーバー、ストレージ、AIモデルなど)の可視化を行います。加えて、各コンポーネントに脆弱性や設定ミスがないかの確認や、機密データへ適切なアクセス権が設定されているかを確認します。これにより、攻撃者による脆弱性をついた攻撃や設定ミスによる意図しない情報漏えいを防ぐことができます。あわせて、NTTドコモビジネスのこれまで蓄積してきたCNAPP製品の運用ノウハウを活かし、企業のAI環境の適切な態勢管理を実現し、各リソースが適切に利用されているか、設定ミスや脆弱性が存在していないか等を調査し、お客さまに対してアドバイザリーを行います。

主なユースケースとしては、クラウド上で、生成AIを活用して独自のチャットボット(Web UI)やAI環境を構築しているお客さまに対し、設定ミス、過剰な権限設定、脆弱性などを検出することを想定しています。

<提供イメージ>



3. 提供開始日

2025年11月6日

4. 利用料金

NTTドコモビジネス営業担当までお問い合わせください。

5. お申し込み方法

NTTドコモビジネス営業担当までお問い合わせください。

6. 今後の展開

NTTドコモビジネスは、今後、本ソリューションを拡大し、AI-SPMのみならず「Wiz」のさまざまなセキュリティ機能を活用し、お客様のクラウド運用を包括的に支援するメニューの拡充をめざします。

また、AIへアクセスする際のセキュリティ強化や、AIエージェントを活用したセキュリティ運用など、AIに関する各種セキュリティ強化支援を充実させていきます。

7. エンドースメント

Wiz Cloud Japan 株式会社 日本代表 山中直氏からのコメント

NTTドコモビジネスさまは、その卓越した技術力と高い革新性により、日本市場において確固たる信頼を築かれてきたパートナーです。Wiz Cloud Japan 株式会社は、NTTドコモビジネスさまの強力な販売ネットワークを通じて、当社の先進的なセキュリティ機能をより多くの企業様へお届けできることを、大変光栄に思っております。本パートナーシップは、クラウドセキュリティに関する複雑な課題に対し、的確かつスピーディに対応する力をさらに強化するものと確信しております。NTTドコモビジネス

スさまとともに、日本のお客様がより安全で効率的にクラウドを活用できる環境の実現をめざし、今後
も取り組んでまいります。

「NTT コミュニケーションズ株式会社」は 2025 年 7 月 1 日に社名を「NTT ドコモビジネス株式会社」に変更
しました。私たちは、企業と地域が持続的に成長できる自律・分散・協調型社会を支える「産業・地域 DX のプラット
フォーマー」として、新たな価値を生み出し、豊かな社会の実現をめざします。

つながり。驚きを。幸せを。



<https://www.ntt.com/about-us/nttdocomobusiness.html>

- ※1 : CNAPP(Cloud Native Application Protection Platform)は、クラウドネイティブアプリケーション保護プラット
フォームという、クラウドセキュリティの考え方であり、クラウドの設定ミス、脆弱性の発見、権限の過多、
マルウェアの検出を可能とします。
- ※2 : 「Wiz」とは、Wiz Cloud Japan 株式会社が提供する、クラウド環境のセキュリティを包括的に可視化・管理す
る CNAPP 製品です。
- ※3 : AI-SPM(AI Security Posture Management)とは、AI のセキュリティ態勢管理と呼ばれ、継続的に AI リソー
スの可視化や管理、リスク評価を行うことで、AI 特有の攻撃から保護し、企業の安全な AI 活用を推進する戦略
的アプローチです。
- ※4 : RAG (Retrieval-Augmented Generation)とは、大規模言語モデルによるテキスト生成時に、外部情報を活用
して推論の精度を高める技術のことです。
- ※5 : LLM (Large Language Models) とは、生成 AI などに活用される、自然言語をより正確に理解するためのモ
デルのことです。