



AIセキュリティとガバナンス Qualys Total AI 2.0

クオリスジャパン株式会社
更新日：2026年9月



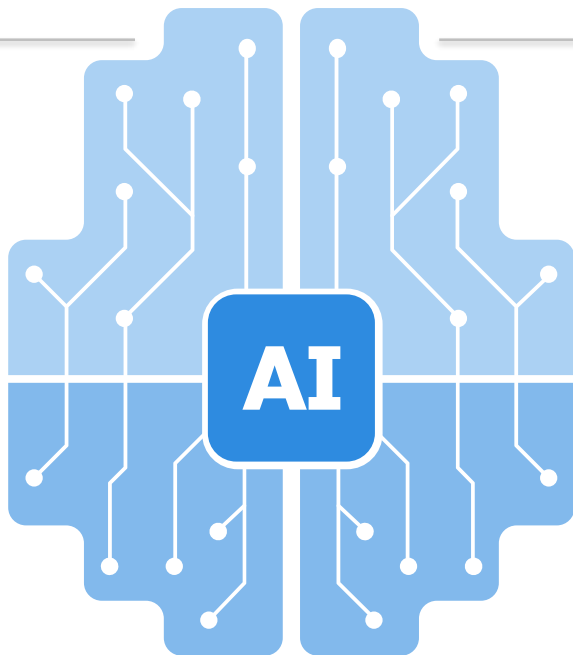
AI利用における課題

Workforce

- 日常業務に浸透する**ChatGPT、Copilot、Gemini**
- **シャドーAI利用**による管理外リスクの増加
- **機密データ**の意図しない外部共有
- **利用状況・コンプライアンス遵守状況**の可視化不足

Developers

- **AIコーディングアシスタント**の急速な普及
- AI生成コードのレビュー不足により、**脆弱性や品質問題**が本番環境へ持ち込まれるリスク
- **AIが組み込まれた開発・運用プロセスの拡大**
- 生成コードに潜む脆弱性の**継続的な監視**が必要



Workload

- AI活用の拡大に伴い、**GPUや機械学習基盤**が急増し、管理・可視化が困難に
- **公開モデルエンドポイントの露出**による攻撃対象領域の拡大
- AI関連**ソフトウェアのパッチ管理**の複雑化
- **モデルAPIやデータストレージの誤設定**によるリスク増大

Dev & Pipeline

- **AI生成コード**の活用拡大に伴う品質・安全性リスク
- **OSSモデル、AIライブラリ、データセット**など外部コンポーネントの信頼性確保
- **学習データの汚染**によるモデル品質・判断精度への影響
- **モデル配布基盤**を標的としたサプライチェーンリスクの増大

AIは至る所で利用されていますが、そのほとんどを可視化できていません

攻撃者の関心は運用中のAI・クラウド環境へ移行

脆弱性を見つけて修正するだけでは不十分。実行中の環境を継続的に監視・保護する必要がある

77%

の従業員が生成AIのプロンプトにデータを貼り付けており、その**82%は管理外のアカウントによるものです。**

ENTERPRISE USAGE TELEMETRY

12,520

インターネットに公開されたMCPサーバ — **その大半で認証機能が未実装です。**

INTERNET-WIDE SCAN

+340%

プロンプトインジェクション攻撃が前年比で増加 — **OWASP LLMリスクの第1位に**

OWASP LLM TOP 10

82%

企業の環境内には、すでに**正体不明のAIエージェントが存在**しています。

CLOUD SECURITY ALLIANCE SURVEY

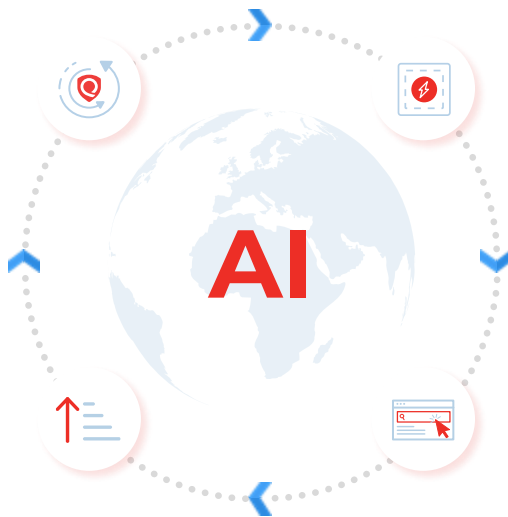
昨年まではセキュリティチームが安全に無視できた4つの数字ですが、今は無視できません

Qualys TotalAIの紹介

LLM、MCP、エージェント、AIワークロード、およびAI脆弱性の統一リスクビューのための単一のプラットフォーム

AI環境全体を可視化

AIパッケージ、LLM、MCPサーバー、
AIIエージェント、GPUを自動検出し、
AI資産を包括的に管理・把握



生成AIを安心して活用するために

LLM for OWASP Top 10ベースの安全性・セキュリティ診断を実施。
機密情報の漏えい、モデルのバイアス、プロンプトインジェクション、Jailbreak攻撃への耐性を継続的に検証します。

AI環境の脆弱性を継続的に可視化・対策

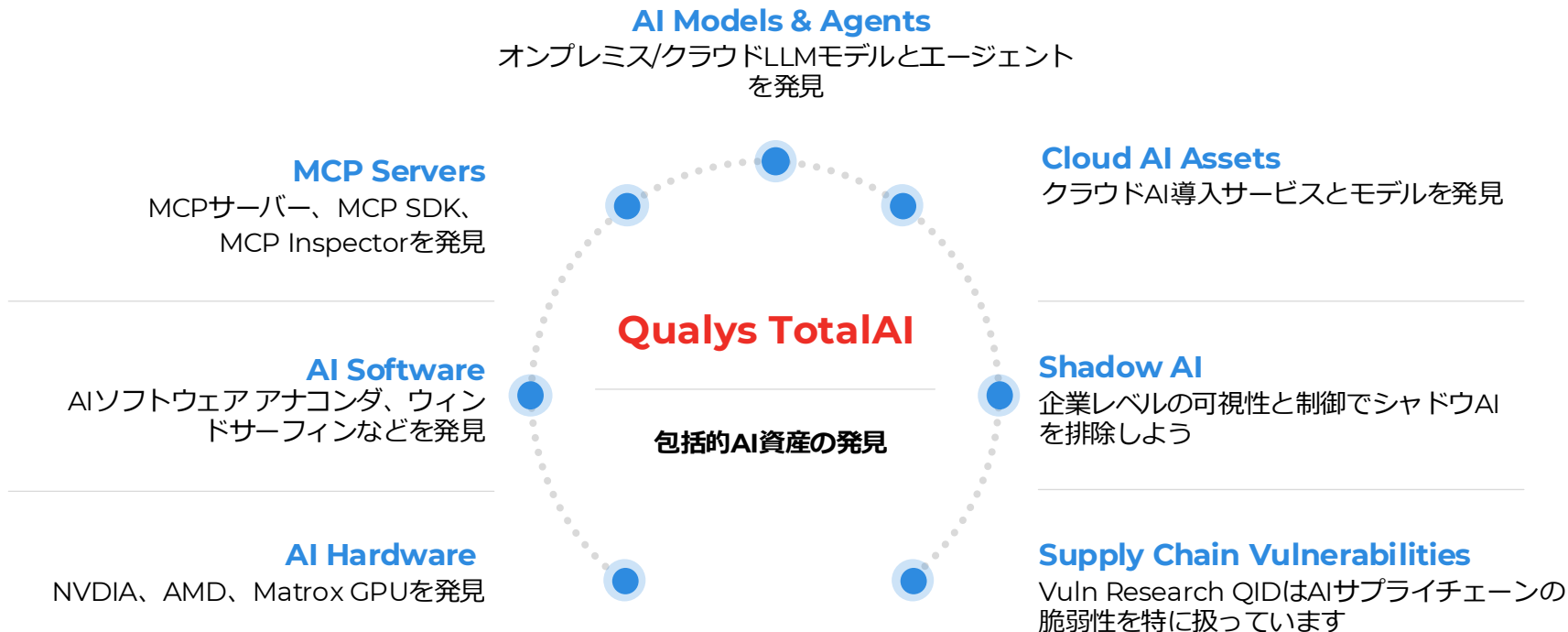
1,000種類以上のAI関連脆弱性を検出し、TruRiskによる優先順位付けを実施。モデルや学習データの窃取につながるリスクを効率的に低減します。

報告およびコンプライアンス

GDPRやPCIなどの規制要件への準拠状況を可視化し、違反リスクを低減。経営層向けのLLMセキュリティレポートにより、AIガバナンスを強化します

既存のQualysエージェント、スキャナー、CSAM、VMDB、TotalAppSec、TotalCloudを活用し、AIセキュリティを加速させる

フルAIスタックの包括的なディスカバリー



Total AI2.0の主な機能

完全なAI資産発見

AIワークロード、LLM、MCP、AIエージェント、AIコードリポジトリ、AI SaaSアプリ、AIソフトウェア、ハードウェアなど、クラウド、オンプレミスエンドポイント、SaaS - シャドウAIを含む完全なAIインベントリを構築します。

AIリスクポスチャーマ管理(AI-SPM)

AIの脆弱性、設定ミス、過剰なアクセスなど、AIに関するあらゆる状況を把握できます。モデル、エージェント、クラウドサービス、コントロール間のリスクを関連付けることで、ビジネスへの影響が最も大きいAIの脆弱性や有害な組み合わせを優先順位付けて表示します

AI Red Teaming

攻撃者目線でAIに擬似攻撃を仕掛け、セキュリティの脆弱性や有害な応答の有無を事前検証する技術。OWASPテスト、プロンプトインジェクション、Jail Break、機密・個人情報の保護、誤情報や有害出力の防止を目的とします。

エージェントアプリケーションを管理する

コードや認証ポリシーからワークロード、ランタイムに至るまで、エージェント型AIのライフサイクル全体にわたって管理します。TotalAIは、eBPFカーネルの可視化とMCPモニタリングを組み合わせることで、エージェントの動作を追跡し、権限を検証し、コードからランタイムまでのセキュリティを実現します。

育成型GenAI およびAI SaaS

従業員のブラウザや組み込みSaaSアプリにおける、隠れたAIやデータ漏洩のリスクを明らかにします。TotalAIはプロンプトのアクティビティを監視し、機密データの移動を追跡し、SaaS構成を評価することで、ガバナンスのギャップを解消し、AIの利用を安全に保ちます。例：Claude、ChatGPT

承認後のAI監視

AIのリスクは、導入後も続きます。モデル、コンテナ、ブラウザ、MCPパスウェイを継続的に監視し、姿勢のずれ、不審なアクティビティ、データ漏洩を検出します。テストから本番環境まで、AIが承認された範囲内で動作していることをリアルタイムで証明します。

MCPとエージェントAIセキュリティ

MCPサーバーを検出してスキャンすることで、AIエージェントとエンタープライズシステム間の接続を保護します。TotalAIは、ツールポイズニング、引数インジェクション、認証情報漏洩を検出し、エージェントが安全でない動作を実行するのを防ぐための完全な可視性を提供します。

AIコンプライアンスとガバナンス

さまざまなコンプライアンスフレームワークへのマップ検索 - EU AI法、MITRE ATLAS、OWASP トップ10

エージェントの発見はフルライフサイクルを通じたもの：コードからランタイムまで

AIエージェントが開発者リポジトリから本番作業へ移行する方法、そしてセキュリティ管理が適用される場所



私たちはエージェントAIアプリケーションをエンドツーエンドで発見し、保護します

なぜQualysがAIセキュリティ市場を変革する独自のポジションにあるのか？



Benefits of Qualys ?



価値までの高速タイム:

VMDR、CSAM、スキャナーを使ったQualysプラットフォームでの摩擦のないディスカバリー

シームレスなクラウドおよびAppSecコネクタ統合AI資産、クラウドサービス、LLMエンドポイントの迅速なオンボーディングを可能にします

スケールとエンタープライズがバナンス向けに構築大規模環境をサポートするように設計されています

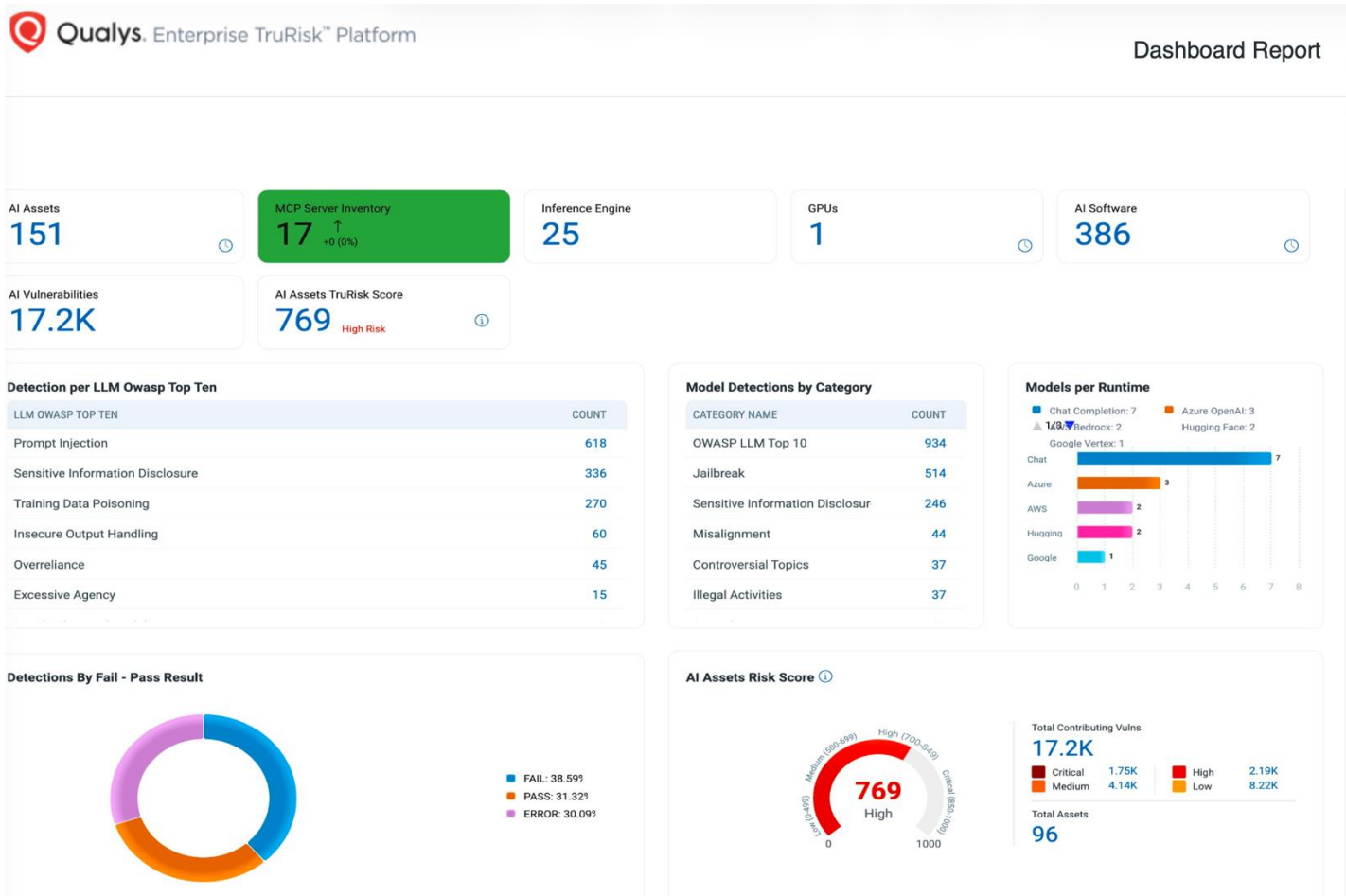


高価値アドバンテージ:

新しいエージェントやツールは不要Qualysクラウドプラットフォーム上でネイティブに動作

運用オーバーヘッドの低さ最小限のセットアップ、迅速な展開、そしてセキュリティチームの負担軽減

Total AI ダッシュボード





補助資料



AIライフサイクル – 在庫管理から修復までの一貫したストーリー

Stage	Customer Question	TotalAI Capability	Metric
Discover	What AI do I have?	AI Discovery	
Assess	What is risky?	AI-SPM	Per workload /yr
Prioritize	What should I fix first?	TruRisk for AI	
Validate	Which SaaS?	Workforce AI(AI SaaS)	Per AI-active user /yr
Validate	Is it resilient?	AI Red Teaming	LLM -Per model MCP – per MCP endpoint
Protect	Can attackers exploit it?	Runtime Protection	Per workload / yr
Remediate	How should I reduce the risk?	TruRisk Eliminate	
Govern	Is it compliant?	AI Governance	

AIガバナンスとコンプライアンス準備

AI監査の準備はできていますか？



EU Act Readiness Assessment



NIST AI RMF



MITRE ATLAS



ISO 42001





Qualys®

| De-risk Your Business

製品およびDemoリクエストなどは
sales-jp@qualys.comまでお問い合わせください。