ソリューションブリーフ

TrojAI Detect by A10 Networks

エージェント主導のレッドチーミングで AI リスクを可視化

AI モデルを自動でレッドチーム検証

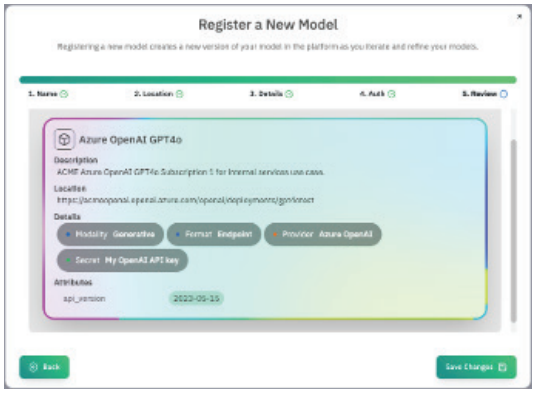
AI は企業を変革する可能性を持つ一方、安全に導入されなければ現実的なリスクとなります。AI モデルが期待どおりに動作することを確認することは、今や重要な経営課題です。従来のセキュリティ対策では、新しい AI 脅威に十分対応できません。AI モデル、アプリケーション、エージェントを守るには、AI 固有の要件に対応したソリューションが必要です。

TrojAI Detect は、AI、ML、生成 AI モデル向けのレッドチーミング・ソリューションです。開発・構築段階でリスクや欠陥を検出し、AI モデル、アプリケーション、エージェントの完全性と安全性を確保します。

構築段階で AI の挙動を保護

パブリック、プライベート、カスタムのいずれの AI モデルを利用する場合でも、導入前にセキュリティと安全性を評価する必要があります。十分なテストを行わなければ、モデルに潜むリスクや欠陥を把握できません。

TrojAI Detect は AI モデルを自動でレッドチーム検証し、挙動が操作され得るかを判定します。脆弱性とバイアスの両方を特定し、安全で信頼できる AI モデルを実現します。



モデルを自動管理

現代の AI 環境では、モデルが複数の環境に分散し、各種サービスや API に組み込まれたり、シャドー AI 環境で気づかれないまま稼働したりしています。

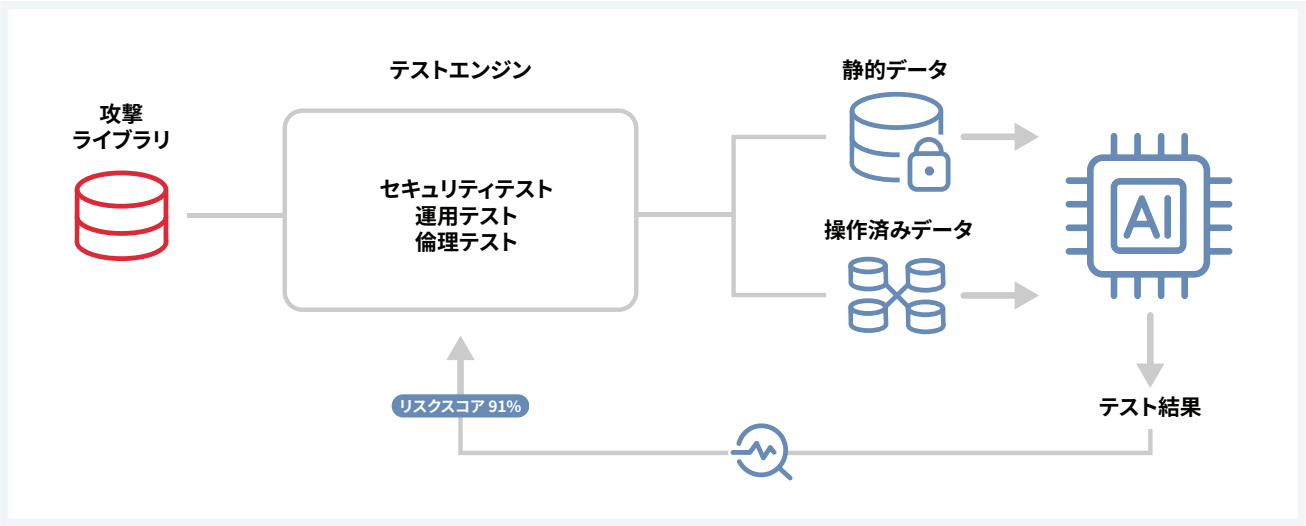
TrojAI は、稼働場所を問わず、すべてのモデルを自動管理する集中型モデルレジストリを提供します。モデルの追加、詳細設定、セキュリティテスト結果の追跡を一元化します。

敵対的攻撃から保護

高度な AI モデルにも、隠れた脆弱性が存在します。TrojAI は 150 種類以上の攻撃と操作手法を標準搭載し、カスタム攻撃にも対応します。高度なユースケースを柔軟かつ詳細に検証できます。

- **攻撃ライブラリ：**本番データセットを含む定義済み／カスタム攻撃を活用し、幅広いユースケースを検証
- **データ操作：**データセットを操作、変更、破損させ、追加の攻撃条件を設定
- **評価：**ブロックリスト、類似性に基づく拒否判定、LLM コンテンツモデレーションなどで AI の挙動を評価

© 2026 A10 Networks, Inc. All rights reserved.



リスクの優先順位付けと軽減

AI モデルの脆弱性を検出しても、修正されるまではリスクが残ります。TrojAI Detect が潜在的なリスクを特定すると、その情報をランタイム保護のための強固なポリシー作成に活用できます。

業界標準への準拠

規制対応には多大な時間とリソースが必要です。TrojAI Detect は、OWASP Top 10 for LLMs、MITRE ATLAS、NIST などのフレームワークへ自動的にマッピングし、主要な業界標準との整合を支援します。

TrojAI Detect の主な特長：

- **エンタープライズ規模のプラットフォーム：**表形式データ、NLP、LLM に対応。150 種類以上のセキュリティテストを利用でき、カスタムテストも容易に作成
- **敵対的攻撃の検知：**導入前に AI モデルの入力と出力をテストし、幅広い攻撃手法から保護
- **迅速で柔軟な導入：**任意のクラウド上の任意のモデルに導入可能。セルフホストまたはクラウドサービスに対応

A10 Networks / A10 ネットワークス株式会社について

A10 Networks(NYSE: ATEN) は、オンプレミス、ハイブリッドクラウド、エッジ環境における、ビジネスクリティカルなシステムを保護、最適化、拡張する、セキュアなアプリケーションおよびネットワークソリューションを提供しています。

A10 のポートフォリオは、世界中の大企業、サービスプロバイダー、クラウドプラットフォームが、パフォーマンス、信頼性、サイバー脅威からの保護を実現しながら、AI および次世代アプリケーションの需要に対応できるよう支援します。

A10 Networks は 2004 年に設立されました。米国カリフォルニア州サンノゼに本社を置き、世界で 7,000 社以上のお客様にサービスを提供しています。

A10 ネットワークス株式会社は A10 Networks の日本子会社であり、お客様の意見や要望を積極的に取り入れ、革新的なアプリケーションネットワーキングソリューションをご提供することを使命としています。

詳しくはホームページをご覧ください。

URL：https://www.a10networks.co.jp/

X(旧 Twitter)：https://twitter.com/a10networksjp

Facebook：https://www.facebook.com/A10networksjapan

About A10

A10Networks.co.jp

お問い合わせ

A10networks.co.jp/contact

A10ネットワークス株式会社

www.a10networks.co.jp

©2026 A10 Networks, Inc. All rights reserved. A10 ロゴ、A10 Networks は米国およびその他各国における A10 Networks, Inc. の商標または登録商標です。その他上記の全ての商品およびサービスの名称はそれら各社の商標です。 A10 Networks は本書の誤りに関して責任を負いません。A10 Networks は、予告なく本書を変更、修正、譲渡、および改訂する権利を留保します。製品の仕様や機能は、変更する場合がございますので、ご注意ください。 商標について詳しくはホームページをご覧ください。 www.a10networks.com/a10-trademarks

Part Number: A10-SB-19215-JP-01 July 2026