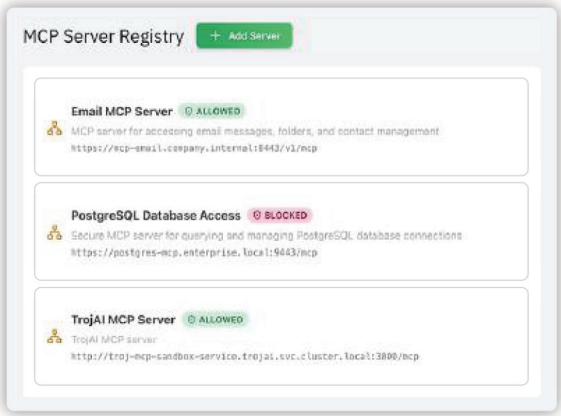
ソリューションブリーフ

# TrojAI Defend for MCP by A10 Networks

エージェントを確実に制御。企業向け MCP セキュリティ




## 企業向け MCP ランタイムセキュリティ

MCP（Model Context Protocol）は、AI エージェントが外部データ、ツール、サービスへ標準化された方法で接続するためのオープンプロトコルです。MCP は AI エージェントの自律的な動作を可能にする一方、新たなリスクも生み出します。MCP サーバー、ツール、接続が増えるたびに、従来のセキュリティ製品では監視・管理できない要素が追加され、新しい攻撃経路が開かれます。

TrojAI Defend for MCP は、MCP ワークフロー全体を可視化・制御します。MCP サーバーとツールのレジストリを提供し、プロンプトインジェクションなどの攻撃を含む悪意あるツール記述を検出するとともに、ツールの完全性を継続的に追跡します。これにより、企業はエージェンティック AI を安全に活用できます。

## すべての MCP サーバーを検出・保護

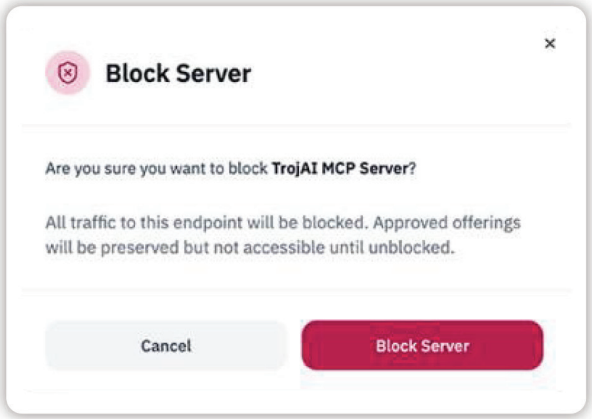
エージェンティック AI のワークフローで MCP の採用が進む中、稼働中のサーバーとその安全性を把握することは大きな課題です。さらに、各 MCP サーバーが複数の未検証ツールを呼び出せるため、リスクは一層高まります。

TrojAI Defend for MCP は、すべての MCP サーバーを検出・登録し、悪意ある第三者による不正アクセスやシャドー MCP を防止します。サーバーと関連ツールをレジストリで承認することで、危険なツールの無断利用を防ぎます。

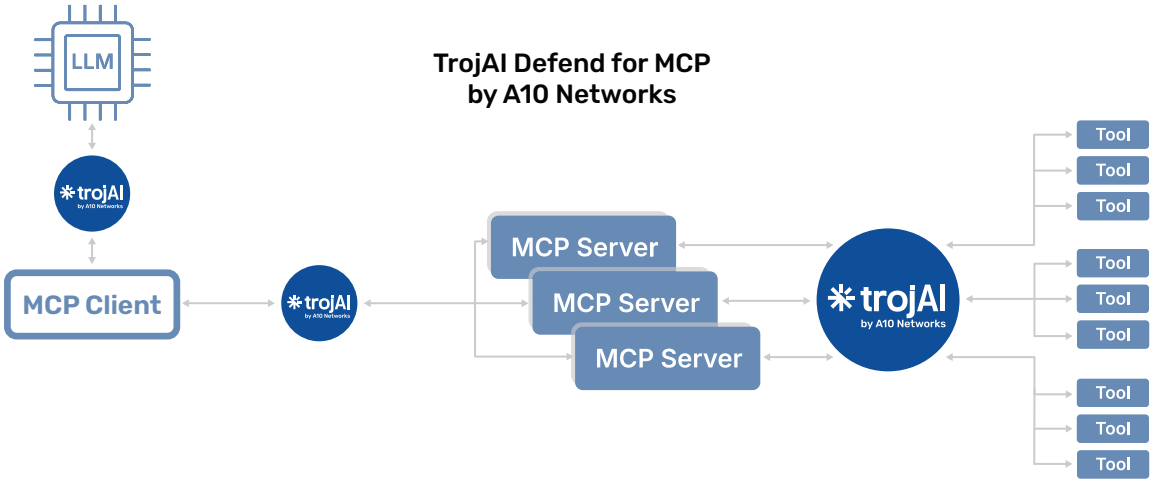
## 不正な MCP サーバーと改ざん攻撃を阻止

悪意ある、または未検証のサーバーは、不正な処理を行うツールや機密データを漏洩するツールを公開する可能性があります。攻撃者は、ツールの名前、説明、パラメータなど、一見無害なメタデータにプロンプトインジェクションを隠し、AI の挙動を変えることもできます。

TrojAI Defend for MCP は、各サーバーを出入りする MCP トラフィックを識別し、未登録または不正なサーバーをブロックします。隠れた通信経路を排除し、プロンプトインジェクションやデータ流出などの AI 攻撃から保護します。




© 2026 A10 Networks, Inc. All rights reserved.




## 改ざんを即座に検出

承認済みのMCPサーバーやツールも改ざんされ、信頼されたワークフロー内にリスクが持ち込まれる可能性があります。TrojAI Defend for MCPは、サーバーとツールの定義を継続的に検証し、差分や変更をリアルタイムで検出します。不正な変更を検知すると対象を隔離・ブロックし、改ざん、ポイズニング、ラグプル攻撃の拡散を防ぎます。

## MCPワークフローを守るAIポリシー

MCPがエージェンティックAIの基盤となる中、企業にはエージェントの実際の挙動を理解するポリシーが必要です。MCP固有のガードレールがなければ、プロンプトインジェクション、データ漏洩、不正なツール利用を見逃す可能性があります。

TrojAI Defend for MCPは、すべてのエージェント操作を検査・監査・保護する、包括的でカスタマイズ可能なポリシーを適用します。企業のデータ取り扱いルールへの準拠を徹底してガバナンスを強化し、コンプライアンスやインシデント対応に必要な詳細な監査証跡を保持します。

## 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-19217-JP-01 July 2026