A10

AIを守る。安心して使い続けるために。

A10 AI Firewall

生成AI・AIエージェントを、開発から本番環境まで保護



AI Firewall（アプライアンス版）

AI Firewall（ソフトウェア版）

生成AIの活用で、こんなお悩みはありませんか？

- ☑ AI利用ガイドラインが守られているか監視したい
- ☑ 機密情報・個人情報の入力や情報漏えいを防ぎたい
- ☑ AIからの不適切・危険な回答をブロックしたい
- ☑ AIアプリケーションを公開する前に安全性を検証したい
- ☑ AIエージェントやMCPの利用まで含めて管理・保護したい

A10 AI Firewallが、AIの「事前検証」と「実行時防御」を一つに。

① 攻撃を試す (Red Teaming)

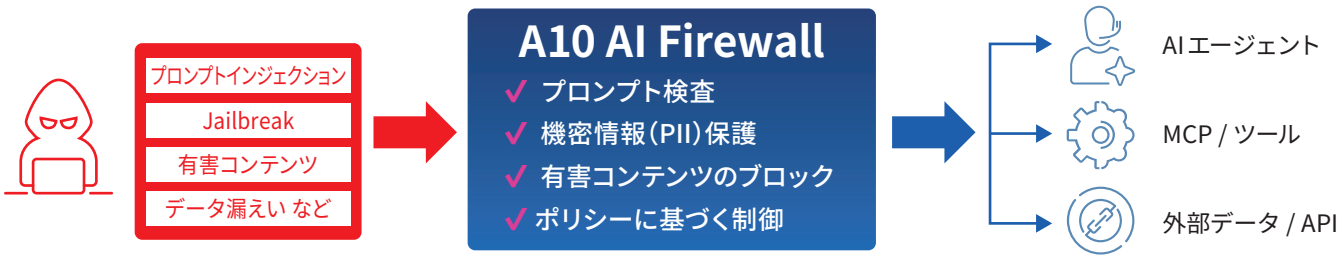
AIモデル・AIエージェントの弱点を事前に発見

② リアルタイムに守る (Runtime Guardrails)

プロンプトとレスポンスをリアルタイムに検知・制御

③ エージェントまで守る (Agent / MCP Protection)

AIエージェントやMCPサーバーツールの利用を可視化・制御



利用環境や運用要件に合わせて選べる、2つのA10 AI Firewall

アプライアンス版

すぐに導入しやすい

AIセキュリティ機能を搭載済み。
専用アプライアンスだから、シンプルに導入。

A10 AI Firewall（Thunderシリーズ・アプライアンス版）



対応 ②

- ✓ AI Firewall機能をハードウェアに搭載
- ✓ 設置するだけで導入が可能
- ✓ 低遅延・高スループットでAIトラフィックを保護
- ✓ 企業・自治体など幅広い環境で利用可能

こんなお客様に
- 生成AIを安全に使いたいが、複雑な設計・構築は避けたい
- 企業・自治体・教育機関など、早期に導入したい

ソフトウェア版

柔軟に設計・高度に制御

きめ細かなポリシー設定と高度なAIセキュリティ。
大規模・複雑なAI環境にも柔軟に対応。

A10 AI Firewall（ソフトウェア版）



対応 ① ② ③

- ✓ 柔軟なポリシー設定・カスタマイズが可能
- ✓ Red Teamingによる継続的な検証
- ✓ AIエージェント・MCPの詳細な制御
- ✓ 大規模・複雑なAI環境に対応

こんなお客様に
- AIアプリケーションやAIエージェントを幅広く展開したい
- きめ細かな制御・高度なカスタマイズを行いたい企業

A10 AI Firewallの主な機能

- ・AI Red Teaming（事前検証）
- ・Runtime Guardrails（実行時防御）
- ・Agent/MCP Protection（エージェント保護）
- ・カスタムポリシー（柔軟な制御）
- ・可視化・レポート（セキュリティ分析）

AIの利用をコントロールし、ビジネスの力に。

A10 AI Gateway

AIへのアクセスを一元管理し、安全・効率的なAI活用を実現



AI活用が広がるほど、こんな課題が増えていませんか？

- ☑ シャドウAI対策でAIの利用状況を可視化したい
- ☑ OpenAI、Anthropic、Googleなど複数のAIモデルを使い分けたい
- ☑ AIサービスの利用料金を削減したい
- ☑ アプリごとにAPIや認証情報を管理するのが大変
- ☑ ユーザー/用途に応じて利用できるAIモデルを制御したい
- ☑ AIへの入出力に共通のセキュリティポリシーを適用したい

A10 AI Gateway でAI利用を一元管理。 AI Firewall でAI利用を安全に。

社内ユーザー | AIアプリケーション | AIエージェント | 業務システム

A10 AI Gateway
AIのアクセス・利用をコントロール

- モデル選択・ルーティング
- アクセス制御・認証管理
- 利用状況の可視化・コスト管理
- ガバナンス・レート制御

A10 AI Firewall
AIの入出力を検査し、安全に

- プロンプトインジェクション対策
- 機密情報 (PII) 保護
- 有害コンテンツのブロック
- AIエージェント・MCP保護

OpenAI | Anthropic | Google (Gemini) | その他のLLM | オンプレミス/プライベートLLM

A10 AI Gateway の主な機能

- **マルチモデル対応**
  複数のLLMを柔軟に利用
- **ルーティング・負荷分散**
  最適なモデルへ自動振り分け
- **アクセス制御・認証管理**
  ユーザー/アプリごとに制御
- **利用状況の可視化**
  利用量・コストを把握
- **ガバナンス・ポリシー適用**
  組織のルールに基づく制御
- **A10 AI Firewall 連携**
  共通のセキュリティポリシーを適用

A10 ネットワークス株式会社
〒106-0032 東京都港区六本木三丁目2番1号 住友不動産六本木グランドタワー 33階 TEL.03-4520-5700 www.a10networks.co.jp a10networks.co.jp/contact