

不正アクセス・個人情報漏洩対策ソリューション

修正までの時間差を突く不正アクセスから、公開 Web・API とリモート接続を保護

ThreatX by A10 Networks（ThreatX、WAAP）と A10 Cloud Access Controller（ZTNA）で、
外部に公開している Web・API とリモート接続の検査・認証を A10 に集約します。

国内で相次ぐ不正アクセスと情報漏えい

不正アクセスの公表

1,380

2026 年 9 月 1 日～10 月 30 日に国内で不正アクセスの被害を公表した組織

大規模な漏えい

76

そのうち、漏えい規模 **10 万件** 以上
100 万件 以上 **38**
1,000 万件 以上 **8**

脆弱性を突かれた侵入

82

不正アクセスのうち、公表文・報道で原因に「脆弱性」が明記されたもの

2026 年 10 月 7～13 日には、個人情報保護委員会・警察庁・金融庁・総務省・経済産業省・IPA・NICT・JPCERT/CC・国家サイバー統括室が相次いで注意喚起などを公表しました。被害は業種を問わず、会員・顧客情報が **1,000 万件** を超えて漏えいしたおそれのある事案も公表されています。

3 つの侵入経路

1 公開 Web・API

既知の脆弱性や、画面では使用しない内部 API が悪用され、顧客 DB から会員情報を大量に取得

2 VPN 機器

ランサムウェア被害の侵入経路の約 5 割が VPN 機器（警察庁 令和 8 年上半期・被害組織のアンケート）

3 委託先・SaaS

委託先の環境や SaaS の管理サイトへの不正ログインで、預けた情報が漏えい

修正の徹底と並行して必要な 3 つの対策

対策 1　外部公開面の把握と集約

公開している Web・API・管理画面を把握し、接続先を 1 か所に集約して同じ検査とログを適用

対策 2　振る舞いによる攻撃者の検知

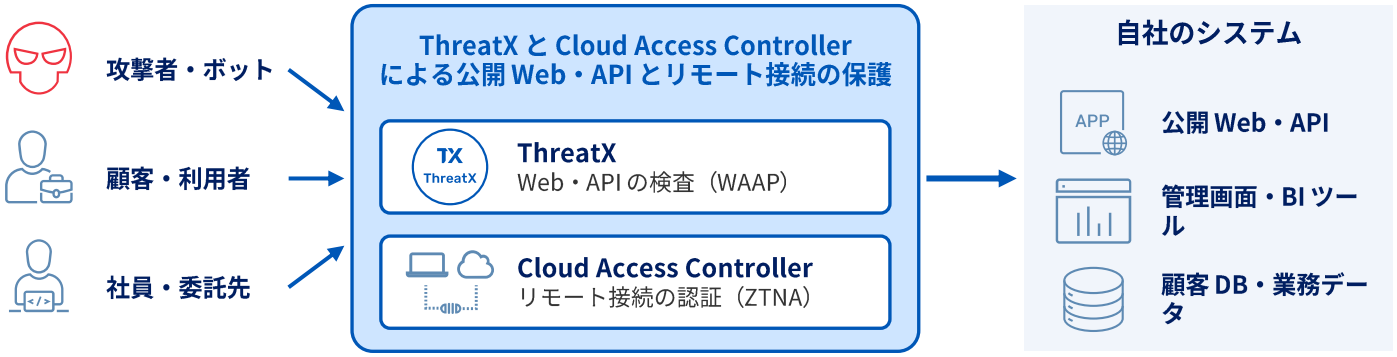
攻撃者の一連の振る舞いで判定し、既知の脆弱性への攻撃は修正版を適用するまでの間も遮断

対策 3　認証後に接続するリモート接続

VPN 機器を不特定多数に公開せず、ユーザーごと・アプリごとに認証してから社内へ接続

AI と既知の弱点　IPA「AI セキュリティ短信」2026 年 9 月号で確認された AI を利用した侵害は、いずれも露出したサービス・未修正の既知の脆弱性・窃取された認証情報という既知の弱点に帰着しています。

出典: A10 調べ（2026 年 9 月 1 日～10 月 30 日に国内で最初に公表された事案を、各組織の公表文・報道と民間の集計サイト（情報漏洩まとめ.site・SmartScope）の掲載情報をもとに集計。委託先の被害は公表した組織ごとに計上。漏えい規模は公表値で「最大」「可能性」「延べ」を含み、漏えいが確認されなかったと公表された事案は除く）。
国家サイバー統括室「不正アクセスによる漏えい等の事案を踏まえた各機関による注意喚起等について」（2026 年 10 月 14 日）、
警察庁「令和 8 年上半期におけるサイバー空間をめぐる脅威の情勢等について」（2026 年 9 月 10 日、VPN 機器は有効回答 36 件中 18 件）。記載の情報は 2026 年 10 月 30 日時点のものです。
IPA「AI セキュリティ短信」2026 年 9 月号（9 月 28 日公開）。



ThreatX
Web アプリケーションと API の保護（WAAP）

■ 攻撃者の振る舞いを追跡して自動で遮断
意思決定エンジン（Hacker Mind）が、攻撃者をエンティティ単位で追跡し、複数の攻撃ベクトルを横断した相関分析と機械学習で適応型リスクスコアを算出し、リスクが高まった攻撃者を自動で遮断

■ 把握していない API の発見（API Defender）
稼働中の通信から API を自動で一覧化し、管理から漏れた API や廃止したはずの API を可視化します

■ Web・API への攻撃の防御
OWASP Top 10、悪意あるボット、クレデンシャルスタッフィング、レイヤー 7 の DDoS への対策と、エンドポイント単位のレート制限。既知の脆弱性への攻撃も、修正版を適用するまでの間遮断

■ マネージド SOC
ThreatX の SOC が 24 時間 365 日監視し、ルールやポリシーの調整にも対応します

A10 Cloud Access Controller
ゼロトラストのリモート接続（ZTNA）

■ VPN 機器をインターネットに公開しない
外部からの接続は A10 のクラウドが受け、自社の VPN 機器や管理画面を不特定多数に公開する必要がありません

■ ユーザーごと・アプリごとの認証（ZTNA）
お客様の ID 管理基盤と連携し、認証したユーザーだけを許可したアプリへ接続します

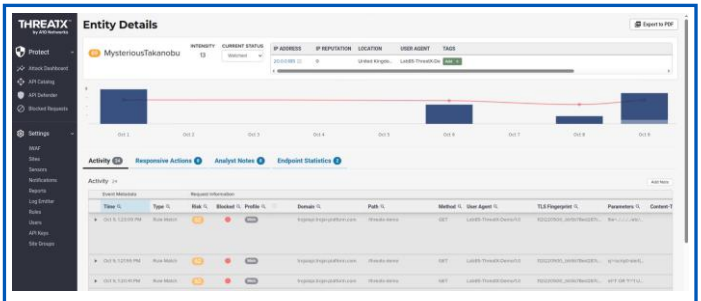
■ 端末へのエージェント導入が不要
クライアントに専用ソフトウェアは不要。既存のネットワークを変えずに段階的に導入できます

■ 通信の可視化とアクセスログ
SSL/TLS 復号、URL フィルタリング、アクセスログ保管。Site-to-Site／Client-to-Site の IPsec VPN にも対応

導入パターン

クラウド構成　ThreatX センサー（サービスとして提供）＋Cloud Access Controller
ThreatX は DNS（CNAME）の切り替えで導入し、機器の設置は不要。Cloud Access Controller はクラウドサービスで提供

オンプレミス併用構成　ThreatX センサー（コンテナ）＋Cloud Access Controller
ThreatX のセンサーを自社内に設置し、既存のドメインのまま検査。解析・SOC と Cloud Access Controller はクラウドで提供



ThreatX の管理画面（攻撃者ごとのリスクと記録）

攻撃者の振る舞いを追跡して自動で遮断
- 要求ごとに検査し、リスクの高い攻撃は要求単位で遮断
- 意思決定エンジン（Hacker Mind）が攻撃者ごとにリスクスコアを算出
- しきい値を超えた攻撃者を一定時間まとめて遮断（既定 30 分）
- 自動遮断が 3 回に達した攻撃者は、恒久的に拒否するリストへ登録

無料トライアル
ご用意しています

ThreatX の無料トライアルをご用意しています。
Cloud Access Controller も無料トライアルでお試しいただけます。
詳細は弊社営業までお問い合わせください。
A10ネットワークス株式会社　https://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。その他記載の商品およびサービスの名称は、それら各社の商標です。製品の仕様や機能は、変更する場合がございます。