

高千穂交易、サイバー攻撃に悪用される脆弱性を AI で検証する「XBOW」を販売開始**～HackerOne 米国 1 位の実績を持つ自律型 AI、悪用可能な脆弱性を継続検証～**

高千穂交易株式会社（本社：東京都新宿区、代表取締役社長：井出尊信、証券コード：2676、以下「当社」）は、XBOW 社（本社：米国ワシントン州シアトル）とリセラー契約を締結し、自律型ペネトレーションテスト・プラットフォーム「XBOW」の国内での販売を開始することを発表いたします。XBOW は自律型オフensive・セキュリティ企業であり、同名のプラットフォーム「XBOW」は、AI が自律的に Web アプリケーション、API への侵入テストを実行し、実際の攻撃者と同じ手法で悪用可能な脆弱性のみを証拠付きで報告するプラットフォームです。

AI を悪用した攻撃が高度化し、アプリを解析して API やバックエンドを直接狙う攻撃「A2B（App-to-Backend）攻撃」への懸念も高まるなか、当社は本製品の取り扱い開始により、特定時点の診断にとどまらない「AI による継続的な攻撃者視点の検証」を国内企業に提供します。開発スピードにセキュリティテストが追いつかないという課題に対し、開発サイクルに合わせた継続的なセキュリティテストを実現するとともに、「実際に攻撃が成立する脆弱性」から優先的に対処できる体制づくりを支援します。

**【XBOW を取り扱い開始する背景】**

生成 AI やコーディング支援 AI の普及により、企業のアプリケーション開発・更新が加速する一方、攻撃者側も AI を活用し、人間を大きく上回る速度で脆弱性の探索と悪用を試みています。そのため、年に一度の人手によるペネトレーションテストや、既知パターンに基づく脆弱性スキャンだけでは変化し続ける攻撃対象領域を十分にカバーすることが難しくなっています。

また、AI を用いてスマートフォンアプリなどを解析し、API の仕様や認証情報を特定したうえで、アプリを介さずに API やバックエンドを直接狙う A2B 攻撃が特に問題となっています。こうした攻撃は、アプリ・API・バックエンドそれぞれの弱点を組み合わせで成立することが多く、一度の診断だけでは、開発・リリースの度に变化する攻撃経路を捉えきれません。検出された脆弱性の一覧を得るだけでは不十分であり、そのうち実際に攻撃が成立するものはどれかを見極め、優先して修正すべき箇所を特定することが求められています。

こうした状況を踏まえ、当社は、これまで注力してきたサイバーセキュリティ事業において、防御・検知に加え、攻撃者視点でシステムを能動的に検証する「オフensive・セキュリティ」領域を強化するため、「XBOW」の取り扱いを開始します。海外の先進技術を発掘してきた知見と、国内での導入・サポート体制を生かし、日本企業の継続的なセキュリティ検証を支援します。

【XBOW について】（URL：<https://xbow.com/>）

XBOW は、2024 年 1 月に設立された自律型オフensive・セキュリティ企業です。同社が提供する「XBOW」は、AI が人間のペネトレーションテスターのようにアプリケーションを調査し、攻撃経路を組み立て、実際に悪用可能かどうかを独立した検証プロセスで確認します。2025 年には、バグ Bounty プラットフォーム「HackerOne」の米国リーダーボードにおいて、自律型システムとして史上初めて人間のセキュリティ研究者を上回り 1 位を獲得。2026 年 3 月には 1 億 2,000 万ドルのシリーズ C 資金調達を実施し、評価額は 10 億ドルを超えています。現在は世界 200 社を超えるセキュリティチームに導入されています。

創業者兼 CEO の Oege de Moor 氏は、英オックスフォード大学でプログラム解析を研究する計算機科学の教授を務めた

後、コード解析技術「CodeQL」を開発した Semmle 社を創業しました。同社が 2019 年に GitHub に買収された後は、研究開発部門 GitHub Next を率い、AI コーディング支援の先駆けとなった GitHub Copilot と、開発者向けセキュリティ機能 GitHub Advanced Security を世に送り出しています。AI とコード解析、セキュリティを知り尽くしたチームによる開発が、XBOW の検証精度と実用性を支えています。

【XBOW の主な特徴】

1. 実際に悪用可能な脆弱性のみを証拠付きで報告

独立した検証プロセスが再現性と悪用可能性を確認します。誤検知を抑え、対応すべき脆弱性と優先順位を明確にします。

2. AI エージェントが攻撃経路を自律的に探索・攻撃

対象の URL や仕様書、API ドキュメントを渡すだけで、エンドポイントや認証フローを自動でマッピングします。複数の AI エージェントが並行して実際に攻撃を試み、単体では見落とされがちな、複数の弱点を組み合わせた攻撃経路（アタックチェーン）まで検証します。

3. 1～2 日程度で実施できる、継続的・オンデマンドなペネトレーションテスト

従来は数週間かかっていたペネトレーションテストを 1～2 日程度で実施することができます（対象の規模・範囲により異なります）。変更やリリースのたびに、必要なときにオンデマンドで検証でき、本番公開前に危険な脆弱性を把握できます。

4. Web・API からモバイルアプリまで検証対象を拡大

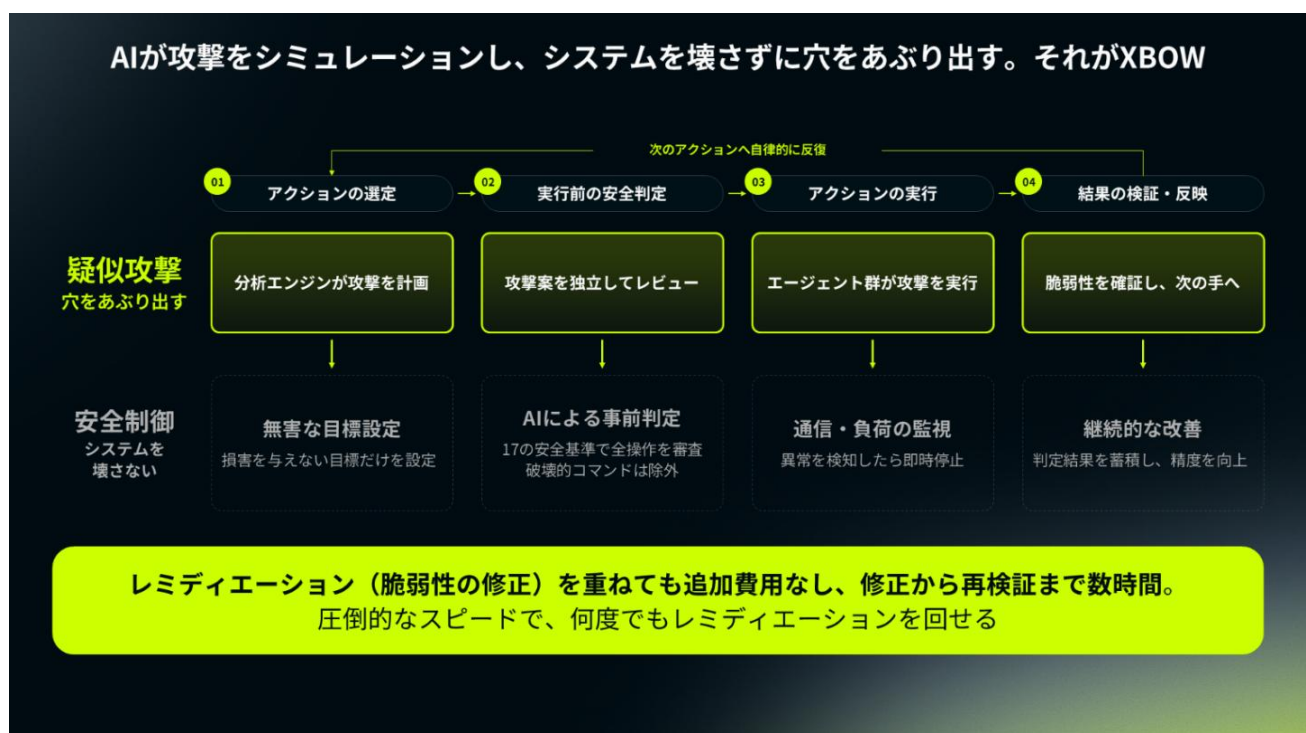
Web アプリケーション・API・バックエンドにまたがるリスクを攻撃者と同じ視点で確認できます。

5. 開発者がすぐ修正に移せるレポート

攻撃経路、再現手順、修正方針をセットで提示します。開発チームの手戻りを減らし、経営層・監査への報告に活用できます。

6. スコープ定義と監査ログによるガバナンス

テスト範囲を組織側で定義でき、実行されたすべての操作を記録・追跡可能。SOC 2、ISO 27001、PCI DSS、NIS 2 など各種コンプライアンス要件への対応に必要な検証と証拠の取得を支援します。



【今後の展開】

当社は、Web アプリケーションや SaaS、スマートフォンアプリを自社で開発・運用する IT・SaaS 企業を中心に、製造業、金融・保険業、小売・EC 業界など、アプリケーションの安全性確保が事業継続に直結する幅広い業種に向けて「XBOW」を提供します。既存のセキュリティ製品や運用サービスと組み合わせ、企業が開発スピードを維持しながら、攻撃者視点で継続的に検証できる体制づくりを支援します。2030 年度までに 100 社への導入を目指します。

【XBOW 社 創業者兼 CEO Oege de Moor 氏からのコメント】

攻撃者はすでに AI を活用して機械並みのスピードで脆弱性を発見・悪用しており、防御側もそれと同等のスピードで対応する必要があります。XBOW は熟練した攻撃者と同様の方法でアプリケーションを継続的にテストし、実際に悪用可能な脆弱性を特定する自律型攻撃型セキュリティプラットフォームです。これにより、セキュリティチームは優先度の高い脆弱性を優先的に修正することができます。高千穂交易は先進的な技術をいち早く見極め、導入から運用に至るまで日本の顧客を支援してきた長い実績があります。今回、同社と提携し日本全国の企業に自律型攻撃型セキュリティを提供できることを光栄に思います。

【XBOW 社 APAC Account Executive 時本 舜介氏からのコメント】

現在、世界中の組織が AI を駆使する攻撃者からの激しい脅威に直面しています。攻撃者が AI を武器化する今の時代において、真に修正すべき脆弱性に優先順位をつけるための有効な解決策は、攻撃者と同じ手法を用いて、悪用可能な問題を検出し、早期修正することです。すでに 200 を超える組織が XBOW に信頼を寄せている理由です。

この度、高千穂交易株式会社とのパートナーシップを通じ、当社のプラットフォームを日本市場に展開できることを大変嬉しく思います。同社の卓越した技術的先見性とお客さまサポートにおける豊富な実績を活かし、日本全国の企業様へオフェンシブ・セキュリティソリューションを迅速にお届けすべく、協業できることを光栄に存じます。

※記載されている会社名、製品名は、各社の商標または登録商標です。

【製品の詳細】

<https://www.takachiho-kk.co.jp/prod/security/xbow/>

【製品のお問い合わせ先】

<https://www.takachiho-kk.co.jp/contact/network/>

高千穂交易株式会社について（Web サイト：<https://corp.takachiho-kk.co.jp/>）

高千穂交易は、「技術の力と、人へのやさしさで、空間に『新しい必要』をつくる。」をパーパスに掲げる 1952 年創業の技術商社です。ビジネスセキュリティ（商品監視、入退室管理、サイバーセキュリティなど）、エレクトロメカニクス（半導体・機構部品）の事業領域で、コンサルティングから開発・設計、設置、保守サービスまでをワンストップで提供しています。

【お問い合わせ先（報道機関窓口）】

高千穂交易株式会社 経営企画室 久我

TEL:03-3355-1201 / E-mail：pr@takachiho-kk.co.jp

〒160-0004 東京都新宿区四谷 1-6-1 YOTSUYA TOWER 7 階