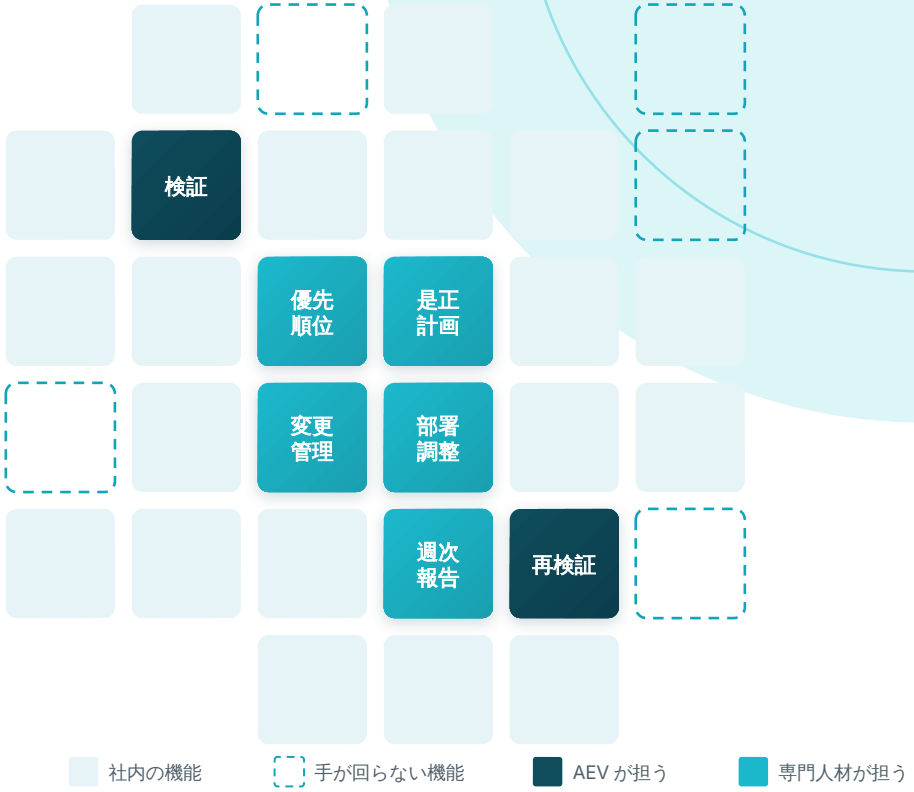
Confidential

SERVICE GUIDE

サイバー脆弱性対応代行サービス

自律型 AI ペネトレーションテストで見つけた穴を、専門人材が是正まで運び、防御力を高める。

検証から優先順位・是正計画・変更管理・部署調整まで、
脆弱性対応をひとつながりでお引き受けします。



AI セキュリティ株式会社

Copyright(C)2026 AI セキュリティ株式会社

Confidential

本資料の構成

本資料は 6 章と Appendix で構成し、まずサイバー脆弱性対応代行サービスの全体像・価値・体制をご説明します。
その後、プランと進め方、背景、会社紹介へと続き、 AEV の仕組みは Appendix にまとめています。

01 サービス概要
お悩み・全体像・サイクル
P5 〜 10

02 サービスの価値
3 つの価値・手法比較
P11 〜 20

03 業務と体制
推進担当・業務・事例
P21 〜 28

04 プラン・進め方
メニュー・導入の流れ
P29 〜 34

05 背景
攻撃と IT 環境の変化
P35 〜 42

06 会社紹介
当社の概要・メンバー
P43 〜 47

07 Appendix
AEV の仕組み・安全設計
P50 〜 61

サービスを知る | 導入を考える | 背景と当社を知る | 補足

Copyright(C)2026 AI セキュリティ株式会社

Confidential

WHAT IS ｜ サイバー脆弱性対応代行サービスとは

自律型 AI ペネトレーションテストから是正までを ひとつながりで担い、防御力を高めるサービスです。

Check Point の自律型 AI ペネトレーションテスト「 AEV 」が毎週、攻撃者の目線で侵入を検証し、その結果を起点に、当社の専門人材が優先順位・是正計画・変更管理・部署調整までを担います。見つけることと直すことを分けずに進め、企業の防御力を継続的に高めます。

提供するもの

是正の完了までの対応

検証結果の報告で終わらず、塞がったことを確かめるまでを社内の一員として回します。

提供のかたち

AEV ＋ 社員代替

AEV の毎週の検証と、セキュリティ社員代替サービスの専門人材を組み合わせて提供します。

いま求められること

変化に追いつく脆弱性対応

AI で攻撃は速くなり、自社の環境も日々変わります。年 1〜2 回の検証では追いつけません。

Copyright(C)2026 AI セキュリティ株式会社

Executive Summary

自律型 AI ペネトレーションテストと是正の推進をひとつにつなぎ、脆弱性を計画的に減らして、企業の防御力を高めます。

Check Point の AEV が毎週、外部から侵入できる箇所を証拠つきで示し、当社の専門人材がその結果を起点に是正の完了までを推進します。
「見つける」と「直す」が同じリズムで回り続けることで、脆弱性が計画的に減っていく状態をつくります。

01 何を提供するか

AEV による毎週の侵入検証と、検証結果を起点に脆弱性の是正を推進する専門人材（推進担当）を、ひとつのサービスとして提供します。

02 どう提供するか

推進担当がお客様の一員として参画し、優先順位・是正計画・変更管理・関係部署との調整を担います。3 つのメニューから体制を選べます。

03 なぜ必要か

AI で攻撃は速く大規模になり、自社の IT 環境も毎週変わります。年 1〜2 回の検証と、手が回らない是正では追いつけなくなっています。

本資料では、サービスの中身・価値・体制・プランを先にご紹介し、後半で背景となる環境変化をご説明します。

Copyright(C)2026 AI セキュリティ株式会社

CHAPTER 01 | サービス概要

Service Overview

サービスの全体像

自律型 AI ペネトレーションテストから
是正までをひとつながりで担います。

IN THIS SECTION

このセクションの内容

この章のページ

こんなお悩みはありませんか P6

検知・復旧と並行して、防御力を高めたい方へ P7

Service Overview ｜サービスの全体像 P8

脆弱性対応のサイクル P9

検出から是正までの絞り込み P10

Copyright(C)2026 AI セキュリティ株式会社

こんなお悩みはありませんか

AI を使った攻撃が広がり、脆弱性を「見つける力」と「直しきる力」の両方が問われるようになっています。
検知や復旧の強化と並行して、侵入口を減らす防御そのものも強くしたいという声を多く伺います。

「外部から指摘されてから、慌てて直すことが続く」

公表や指摘のたびに、
業務を止めて緊急対応している。



セキュリティの責任者

「検証が年 1〜2 回では、合間の穴が見えない」

事業部門が導入した SaaS や
自作アプリは把握できていない。



脆弱性管理のご担当

「直すべきことは分かるが、調整して進める人がいない」

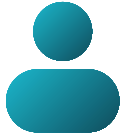
変更管理や部署間の調整に
手が回らず、是正が止まっている。



インフラ・運用のご担当

「検知や復旧と並行して、防御力も高めたい」

検知・復旧の強化を進めながら、
侵入口そのものも減らしたい。



CISO ・経営層

これらのお悩みは、 AEV による毎週の検証と、是正を推進する専門人材の組み合わせで解消できます。

Copyright(C)2026 AI セキュリティ株式会社

検知・復旧と並行して、防御力を高めたい方へ

検知や復旧への意識が高まり、ゼロトラストへの取り組みも進むなか、侵入口を減らす防御の重要性は変わりません。
本サービスは、検知・復旧の強化と並行して、外部から突ける穴を毎週塞ぎ、防御力を高めたい企業に適しています。

本サービスが強める領域 | 並行して強化が進む領域（EDR ・ SOC ・バックアップ など）

GOVERN	IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
統治	識別	防御	検知	対応	復旧
方針・体制	資産とリスクの把握	侵入口を減らす	侵入に気づく	封じ込める	事業を戻す

01 侵入される前に塞ぐ

AEV が毎週、外部から突ける穴を証拠つきで見つけ、
専門人材が是正の完了まで運びます。
攻撃が成立する前に、侵入口そのものを減らします。

公開資産の弱点 | 漏洩した認証情報 | 設定ミス

02 ゼロトラストの前提を固める

ゼロトラストの考え方でも、外部に公開した
資産の弱点を減らすことは前提です。
入口に残る穴を毎週確かめ、足元を固めます。

VPN | 管理画面 | API

03 検知・復旧の強化と両立する

検知や復旧の取り組みは、そのまま進められます。
入口で防げる攻撃が増えるほど、SOC の
アラートや対応の負荷も小さくなります。

SOC | EDR | バックアップ

※ 機能の区分は NIST サイバーセキュリティフレームワーク（CSF）2.0 の 6 つの機能にもとづきます。

Copyright(C)2026 AI セキュリティ株式会社

Service Overview

検証から是正までを ひとつながりで担い、 防御力を高めます

サイバー脆弱性対応代行サービスの全体像

AEV ＋ 社員代替　派遣・業務委託　毎週のサイクル

AEV が毎週、外部から侵入できる箇所を証拠つきで示し、専門人材がその結果を起点に是正を推進します。

背後には当社の管理者・技術支援チームがあり、個人の力量に頼らない形で是正の流れを維持します。



Copyright(C)2026 AI セキュリティ株式会社

脆弱性対応のサイクル

AEV が毎週「どこが突けるか」を示し、当社の推進担当が「どう直すか」を計画・調整・実行まで運びます。
検証と是正が同じリズムで回り続けることで、脆弱性が計画的に減っていく状態をつくります。



このサイクルを、毎週回し続けます

AEV が「どこが突けるか」を示し、推進担当が「どう直すか」を是正の完了まで運びます。

AEV が担う工程　推進担当（専門人材）が担う工程

脆弱性の「潰し込み」を推進する人を、検証のリズムと一緒にご提供します。

Copyright(C)2026 AI セキュリティ株式会社

検出から是正までの絞り込み

AEV で本当に悪用できるものに絞り込めても、是正が完了しなければリスクは残り続けます。
最も滞りやすいのは、人手と部門間の調整が必要な「直す」工程です。



01 見つける｜脆弱性スキャン・資産の把握

検出結果は対応の速さを上回って増え続け、
どこから手を付けるべきかが見えにくくなります。

02 絞り込む｜ AEV による実証

「本当に悪用できるもの」が証拠つきで分かり、
優先して対応すべき対象が明確になります。

03 直す｜是正の計画と実行

変更管理、関係部署との調整、パッチ適用、再検証まで。
人手と調整が必要で、最も滞りやすい工程です。

本サービスは、 AEV で絞り込んだ結果を当社の推進担当が「是正の完了」まで運びます。

Copyright(C)2026 AI セキュリティ株式会社

CHAPTER 02 | サービスの価値

Service Value

柔軟性・計画性・安全性

本サービスがもたらす 3 つの価値と、
従来の手法との違いです。

IN THIS SECTION

このセクションの内容

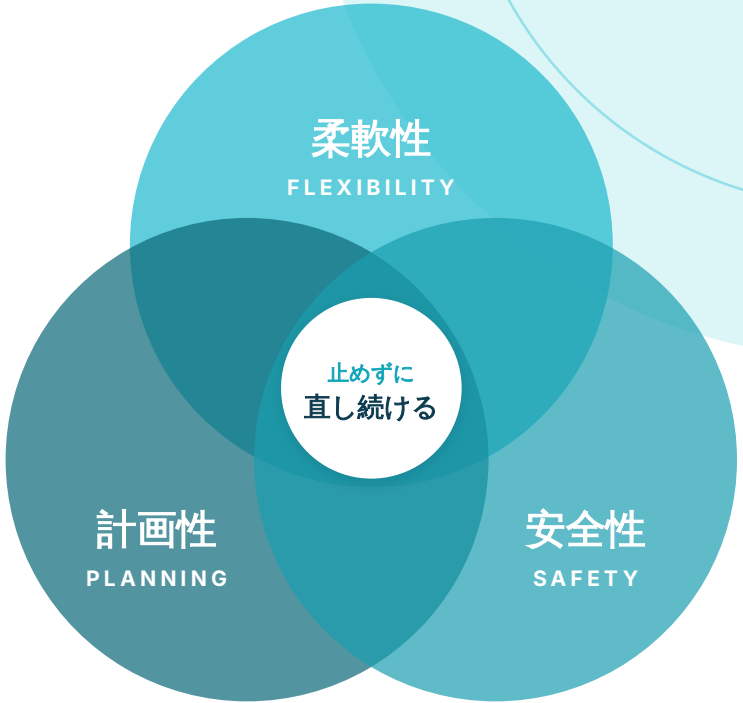
この章のページ

- 本サービスがもたらす 3 つの価値 P12
- 価値① 柔軟性 | 年 52 回の検証 P13
- 価値② 計画性 | 先に見つけて計画に載せる P14
- 価値③ 安全性 | 止めずに検証して直す P15
- 従来の診断手法との違い P16
- AI を活用した攻撃者への対策 P17
- 自律型 AI ペネトレーションテストとの違い P18 〜 19
- 自律型 AI ペネトレーションテスト（ AEV ）のまとめ P20

Copyright(C)2026 AI セキュリティ株式会社

本サービスがもたらす価値は、柔軟性・計画性・安全性の 3 つです。

3 つが重なることで、検証して終わりではなく、
業務を止めずに直し続けられる状態が生まれます。



01 柔軟性 Flexibility
年 52 回の検証で、攻撃や環境の変化に追いつく

02 計画性 Planning
先に見つけて、自社の計画とタイミングで直す

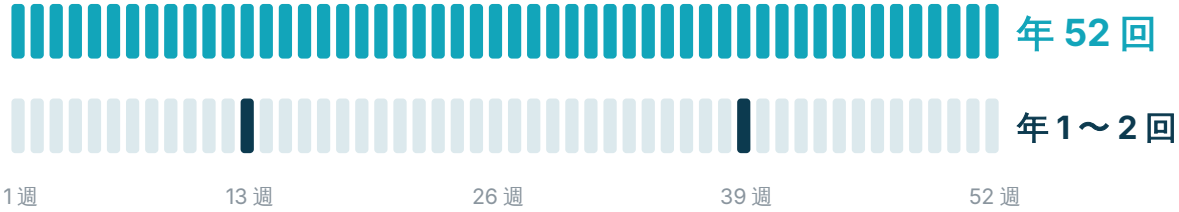
03 安全性 Safety
本番に負荷をかけず、変更管理に沿って直す

Copyright(C)2026 AI セキュリティ株式会社

価値① 柔軟性｜年 52 回の検証で変化に追いつく

同じ予算で人手のペネトレーションテストを行う場合、実施できるのは年 1〜2 回程度が一般的な目安です。
本サービスでは、 AEV の毎週の検証を 1 年を通じて続け、攻撃や IT 環境が変わるたびに確かめ直せます。

同じ予算で、 1 年間（ 52 週）に実施できる検証



1 攻撃の進化に追随する

AI モデルの進化に合わせて高度化する攻撃手法を、検証側も取り込み続けます。

2 自社の変化を捉える

事業部門が導入した SaaS や自作アプリなど、新しく増えた資産も翌週の検証で確かめます。

3 SaaS の更新を捉える

利用中の SaaS が機能を更新しても、外部から見える状態を毎週確かめ直せます。

Copyright(C)2026 AI セキュリティ株式会社

価値② 計画性｜先に見つけて自社の計画に載せる

外部から指摘されてから直す運用では、そのたびに業務を止めて緊急対応を行うことになります。
自分たちで先に突き止めておけば、緊急度の高いもの以外は自社の計画とタイミングで直せます。

緊急対応

外部から指摘されてから直す

脆弱性の公表・外部からの指摘 → 業務を止めて緊急に調査 → 調整が不十分なまま適用 → 影響の確認が後追いになる

計画対応

自分たちで先に見つけて直す

毎週の検証で先に発見 → 優先度を判定し計画に組み込む → **週末のメンテナンス時間に適用** → 再検証で塞がったことを確認

「やっていない状態」で見つかる前に、自分たちで見つけて、自分たちのタイミングで直す。

※ 緊急度・重要度が特に高い脆弱性は、計画を待たずに即時の対応をご提案します。

Copyright(C)2026 AI セキュリティ株式会社

価値③ 安全性｜業務を止めずに検証し、直す

検証も是正も本番環境で行う以上、業務を止めないことがすべての前提になります。
AEV の安全設計と、推進担当による変更管理の両面から、止めずに検証して直す運用を支えます。

検証の安全性

AEV の安全設計

1. **負荷をかけない**
   検証に必要な最小限のリクエストのみを送信します。
2. **データを変えない**
   データの削除や設定変更を行わない、非破壊の検証です。
3. **総当たりをしない**
   認証の試行を制限し、アカウントのロックを防ぎます。
4. **AI が三重にレビュー**
   実行前に、独立した AI が各検証の安全性を審査します。

是正の安全性

推進担当による変更管理

1. **段階的に直す**
   まずバーチャルパッチで守り、計画的に本修正へ進めます。
2. **手続きに沿う**
   お客様の変更管理のルールに沿って申請・承認を進めます。
3. **事前に知らせる**
   SIEM のアラート増加などを、関係部署へ事前に連絡します。
4. **再検証で確かめる**
   是正後に再検証し、塞がったことを確認します。

※AEV の安全設計は、 Check Point 社の公開情報・ご紹介資料にもとづきます。

Copyright(C)2026 AI セキュリティ株式会社

従来の診断手法との違い

AEV は、年に数回実施する深いペネトレーションテストを置き換えるものではありません。
テストとテストの合間を埋める継続的な検証として今の取り組みを補い、穴が残る期間を短くします。

観点	脆弱性スキャン	人手のペネトレーションテスト	AEV ＋ 本サービス
実施の頻度	月次〜四半期	年 1〜数回	週 1 回（年 52 回）
悪用できるかの確認	△ 理論上のリスク一覧	◎ 専門家が実証	◎ 証拠つきで実証
結果が出るまで	○ 数時間〜数日	△ 数週間	◎ 100 アセット約 1 時間
業務ロジックの深い検証	× 対象外	◎ 得意とする領域	△ 人手のテストと併用
是正までの推進	× 対象外	△ 報告書まで	◎ 推進担当が是正まで

◎ 優れる　○ 対応　△ 一部対応　× 対象外　※一般的な傾向を当社で整理したものです。

「年数回の深い検証」と「毎週の検証＋是正の推進」を組み合わせることで、合間に生まれる穴を減らせます。

Copyright(C)2026 AI セキュリティ株式会社

AI を活用した攻撃者への対策

偵察・侵入

AEV （ Agentic Exposure Validation ）

- 漏洩 ID
- CVE
- 非 CVE
- 設定ミス

推論・検証ループ
- 関連付け
- 仮説生成
- 安全なプローブ設計
- 独立した安全性レビュー
- 実環境での検証
- 立証／方向転換／棄却

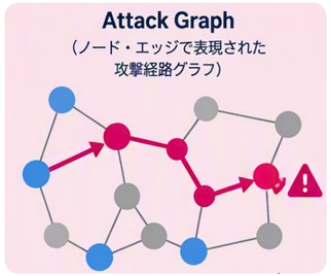
CVE のみならず漏洩情報や非 CVE 、設定ミスの組み合わせによる**未知の疑似攻撃**を自律的に考え外部侵入検証

AI を使った疑似攻撃の実施
AI を使った攻撃者への対策として
一番優先度高いソリューション

侵入経路

Attack Path 製品

- ID
- CVE
- 設定ミス



あくまでも重大な脆弱性や重大な設定ミスから派生した攻撃経路の理論的な発見

対象サーバー ソースコード脆弱性

AI を使ったソースコードスキャン



ミュトスや GPT Cyber などを使ったソースコードスキャン

Copyright(C)2026 AI セキュリティ株式会社

出典： Check Point Software Technologies Ltd.

自律型 AI ペネトレーションテストと従来型ペネトレーションテストの違い

ミュトスのような AI を使う攻撃者には、より高度な AI で高頻度に検証することが有効な対策です。
自律型 AI ペネトレーションテストと従来型の違いを、 9 つの観点で比較しました（ 1/2 ）。

項目	自律型 AI ペネトレーションテスト Agentic Exposure Validation （ AEV ）	従来型ペネトレーションテスト	ミュトスなどの Frontier AI を利用した特別なペネトレーションテスト
攻撃設計能力	◎ **ミュトスを超える攻撃性能** チェックポイントの製品品質保証で実績のある脆弱性発見能力	X 人手や経験やソフトウェアパターンによる攻撃設計のバラツキ	○ Frontier AI を活用したミュトスレベルの攻撃性能
CVE に依存しない攻撃パターン	◎ 人間では気付けない軽微なミスや非 CVE の組み合わせ（**未知攻撃**）も実施	X CVE 中心　従来型攻撃への対応のみ	◎ 人間では気付けない軽微なミスや非 CVE の組み合わせ（未知攻撃）も実施
攻撃のアップデート	◎ **成功した攻撃パターンを学習　実施機会が非常に多く攻撃アップデート大 CVE はリアルタイム　モデルは数ヶ月に 1 回アップデート　チェックポイント全製品で収集した脅威情報活用**	X 人間もしくはソフトウェアのパターンアップデートの限界	○ 単一モデルのアップデートに依存セキュリティベンダーが提供していないことが多く高度なセキュリティ情報の活用ができない
攻撃回数	◎ 200 アセットを場合により **1 万回**を超える攻撃回数	X 人手で実施するので回数が限定的	◎ Frontier AI を用いた非常に多くの攻撃回数
テスト実施回数 / 年	◎ 最短毎週　**52 回** / 年	X 1 回もしくは 2 回 / 年	X 1 回もしくは 2 回 / 年　コスト準備計画などから制約あり

Copyright(C)2026 AI セキュリティ株式会社

出典： Check Point Software Technologies Ltd.

自律型 AI ペネトレーションテストと従来型ペネトレーションテストの違い

ミュトスのような AI を使う攻撃者には、より高度な AI で高頻度に検証することが有効な対策です。
自律型 AI ペネトレーションテストと従来型の違いを、 9 つの観点で比較しました（ 2/2 ）。

項目	自律型 AI ペネトレーションテスト Agentic Exposure Validation （ AEV ）	従来型ペネトレーションテスト	ミュトスなどの Frontier AI を利用した特別なペネトレーションテスト
実施時間	◎ 100 アセットあたり **1 時間**	X 数日 ~ 週間	◎ Frontier AI を用いて短時間に高速
テスト準備	◎ **IP アドレスとドメインリストの登録のみ** あとは自動実行	X ヒアリングやドキュメントの提出 複数回の打ち合わせ	X ヒアリングやドキュメントの提出 複数回の打ち合わせ
本番環境への実行	◎ 本番に定期的に実行するために AI を確実にコントロール **1000 社を超える実績**	◯ テストを綿密に計画準備することにより実行可能　工数大	X 本番システムに影響を与える可能性あり　厳密な計画や事前テストが必要
見つかった問題への対処	◎ **Threat Exposure Management** と組み合わせることにより**分単位での対処**を本番への影響を確認しながら自動的に実現するように拡張することが可能	X 見つかった問題を分析して対処する方法を整理し実施するまでに非常に多くの時間と工数がかかる	X 見つかった問題を分析して対処する方法を整理し実施するまでに非常に多くの時間と工数がかかる

Copyright(C)2026 AI セキュリティ株式会社

出典： Check Point Software Technologies Ltd.

自律型 AI ペネトレーションテスト（ AEV ）のまとめ

AI を使った攻撃者への対策	• 最新の **FrontierAI** を利用した **SaaS 型 AI 自律型**ペネトレーションテストソリューション • 外部からの**侵入テストに特化**　一番優先度の高い外部からの攻撃可能性を特定 • **脅威情報や機密情報、 ASM ツール**のモジュールで情報を統合し高度なテストが可能 • 最新の攻撃者の攻撃手法、 CVE 、ソフトウェア仕様、漏洩情報、複数の AI モデルを**自動アップデート** • CVE のみならず設定ミス、非 CVE や漏洩情報の組み合わせによる **AI による未知攻撃**に対応
テスト時間パターン	多いときで**1万を超えるテストパターン**で 100 アセットを**約 1 時間で高速テスト**が可能
本番への適用	**本番にも負荷をかけることなく安心安全**にテストを実施することが可能
運用負荷	**IP アドレスやドメイン名の情報のみ**で自動的自律的にテスト　他に準備は必要なし
Why AEV	数年にわたりチェックポイントの**脆弱性を最小化した実績**ある製品品質保証 AI がベース
コスト	高度な外部侵入ペネトレーションテストと**同等コスト**で**年 52 回**実施可能

現在、無償診断を実施中です。詳しくは当社の担当営業までお問い合わせください

Copyright(C)2026 AI セキュリティ株式会社

出典： Check Point Software Technologies Ltd.

CHAPTER 03 | 業務と体制

Operation

業務と体制

推進担当（専門人材）が担う業務と、
人材例・ご支援事例をご紹介します。

IN THIS SECTION

このセクションの内容

この章のページ

- 推進担当（当社社員）が担うこと P22
- 業務プロセス | AEV 起点の脆弱性対応 P23
- 1 週間の稼働イメージ P24
- 推進担当の人材例 | 脆弱性管理・対応 P25
- 安心してお任せいただくための 6 つの特徴 P26
- ご支援事例 | 脆弱性対応の定常化 P27
- ご支援事例 | AEV の導入 P28

Copyright(C)2026 AI セキュリティ株式会社

推進担当（当社社員）が担うこと

当社の社員がお客様の一員として脆弱性の潰し込みを推進し、是正が止まらない状態をつくります。
検証結果を受け取るだけで終わらせず、社内の変更管理や関係部署との調整まで一緒に動きます。

1 今週の検証結果を出す

毎週の AEV の結果を読み解き、実証された箇所と前週からの変化を、今週の結果として整理します。

2 優先順位を決める

業務への影響や公開範囲を踏まえ、すぐ直すもの・計画に載せるもの・様子を見るものに仕分けます。

3 是正の方法を決める

パッチの適用、バーチャルパッチ、設定変更など、直し方とその実施時期を是正計画にまとめます。

4 変更管理を進める

お客様の変更管理の手続きに沿って申請を準備し、承認から実施までの段取りを進めます。

5 関係部署と調整する

SIEM のアラート増加が見込まれる場合の事前連絡など、運用・アプリ担当・ベンダーとの調整を担います。

6 直ったことを確かめる

是正後は AEV で再検証し、塞がったことを確認して是正の状況を毎週ご報告します。

※ 担う範囲はプランにより異なります。契約形態は派遣または業務委託（準委任）です。派遣の場合、指揮命令はお客様が行います。

Copyright(C)2026 AI セキュリティ株式会社

業務プロセス | AEV 起点

AEV 起点の脆弱性対応

起点：毎週の AEV 検証結果｜担い手：推進担当（専門人材）

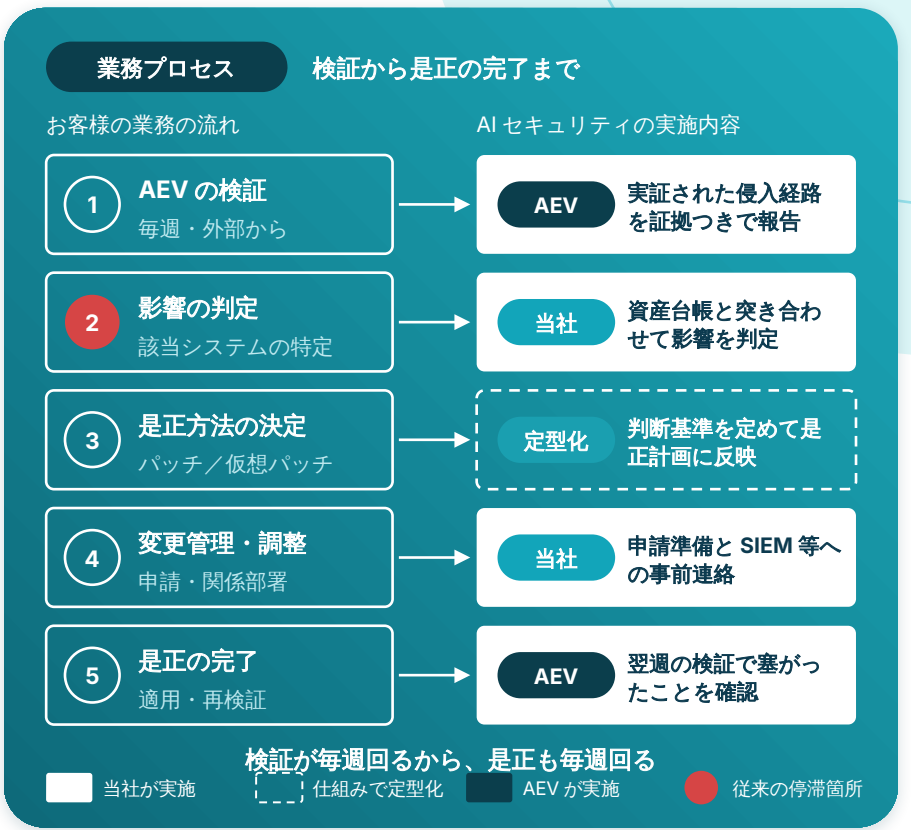
毎週の検証結果を起点に、是正の完了までを社員と同じように回します。

検証の結果を受け取っても、影響の判定や関係部署との調整が後回しになり、是正が止まりがちでした。
推進担当が判定から再検証までを定常業務として担います。

専門人材が担うこと

- 01 検証結果の読み解きと影響範囲の判定
- 02 是正計画の策定と変更管理・部署調整の推進
- 03 是正状況の週次報告と未対応の追跡

成果指標 実証された脆弱性の是正までの日数／残件数



Copyright(C)2026 AI セキュリティ株式会社

WEEKLY OPERATION

1週間の稼働イメージ

月曜の検証結果から、
週末の是正までを1週間で回します。

AEV が毎週検証し、推進担当が平日に判定・計画・
申請・調整を進め、お客様のメンテナンス時間に
是正を行います。翌週の検証で効果を確かめます。

週あたりの稼働の目安（標準スターター Menu ）

AEV 週1回 ＋ 専門人材 5日 ＋ 管理者 約2.5日

このサイクルで回る基本業務の例

- 検証結果の判定
- 是正計画
- 変更管理
- 週次報告

1週間の稼働イメージ

AEV が週1回検証し、専門人材が毎日終日、管理者も毎日約半日で業務を管理

	月	火	水	木	金	週末
AEV	検証					
専門人材	結果整理	優先順位	変更管理	部署調整	週次報告	是正立会
管理者	約 4h	約 4h	約 4h	約 4h	約 4h	

AEV　専門人材　管理者　必要に応じて

翌週の検証で、前週に是正した箇所が塞がったことを確認。
曜日の割り当ては一例で、変更管理のルールに合わせて設計します。

Copyright(C)2026 AI セキュリティ株式会社

推進担当の人材例｜脆弱性管理・対応

脆弱性の影響評価から優先度付け、パッチ適用の調整まで、見つかった後を確実に進める人材です。
以下は人材プールに登録されている代表的なプロファイルで、ご要件に合わせて最適な人材をご提案します。



K・M

影響評価からパッチ適用の調整まで一貫対応

脆弱性管理 | 資産台帳 | パッチ調整

簡易経歴

- 製造業の情報システム部門で脆弱性情報の収集・影響評価を担当
- 公開資産・ VPN 機器の台帳化と、拠点・保守ベンダーとの適用調整をリード
- 高リスク脆弱性の対応日数を指標化し月次で報告

保有資格

情報処理安全確保支援士／ Security+



S・Y

診断結果をもとに優先度付けと改善を推進

脆弱性診断 | CVSS/EPSS | 優先度付け

簡易経歴

- セキュリティファームで Web ・プラットフォーム診断を多数実施
- CVSS ・ EPSS と資産の重要度を組み合わせた優先度基準を整備
- 診断結果の説明会と、開発部門との改善計画づくりに対応

保有資格

OSCP ／情報処理安全確保支援士



D・I

公開資産とアタックサーフェスの把握

ASM | 外部スキャン | VPN 機器

簡易経歴

- 外部公開資産の調査（ ASM ）と台帳との突き合わせを担当
- VPN 機器・リモートアクセス機器のバージョン管理を定例化
- 緊急脆弱性の公表当日に該当有無を判定する体制を構築

保有資格

情報処理安全確保支援士／ PenTest+



E・N

サーバー・端末のパッチ運用

パッチ運用 | Intune | 例外管理

簡易経歴

- SIer でサーバー・端末のパッチ適用計画と検証を担当
- Intune ・ WSUS による配信運用と適用率の月次報告を整備
- 適用できない機器の例外承認と代替策の管理を運用

保有資格

LPIC-2 ／情報処理安全確保支援士

※ 個人が特定されないよう、イニシャルと経歴の要旨のみ記載しています。ご提案時は職務経歴書・面談録画・ Q&A の 3 点セットをご提示します。

Copyright(C)2026 AI セキュリティ株式会社

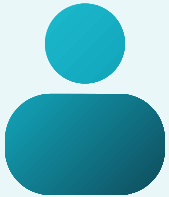
安心してお任せいただくための 6 つの特徴

外部の人材への不安は「誰が来るか分からない」「権限が見えない」「ノウハウが残らない」の 3 つです。
当社はこれらへの対応を契約に明記し、お客様の社員と同じルールのもとで運用します。

01 判定結果を提案時にお出しします
技術判定シートを提出。交代時も同じ基準

02 全員に本人確認と対面面接を行います
パートナー経由も同じ基準。報酬は本人口座へ

03 関わる人を全員お知らせします
再委託は、ご承認なしには行いません



お客様の現場に入る人

04 権限はお客様の管理下に置きます
お客様の端末・ ID ・操作ログで。当社も毎月確認

05 入場と退場の記録をお渡しします
誓約書、権限削除と貸与品回収の記録

06 月次の作業記録と引継ぎ文書を残します
契約が終わっても、ノウハウが社内に残ります

誰が来て、何をしたかが分かる専門人材として、お客様の社員と同じように働きます。
北朝鮮 IT 労働者への注意喚起（警察庁ほか、 2026 年 7 月）以降、本人確認も問われるようになりました。

Copyright(C)2026 AI セキュリティ株式会社

ご支援事例　脆弱性対応（社員代替）

脆弱性対応の定常化

お客様：大手損害保険グループ | 体制：派遣契約（社員代替）

社員と同じ指示系統で、脆弱性対応を毎月回る形にしました。

脆弱性情報の収集から修正依頼までを担当者１名が
兼務し、影響の判定が後回しになっていました。
判定と修正推進を担い、定常業務にしています。

AI セキュリティが担ったこと

01　脆弱性情報の収集と影響範囲の判定

02　優先度付けと各システム担当への修正依頼

03　対応状況の月次報告と未対応の追跡

成果　修正までの日数／未対応の脆弱性の件数



Copyright(C)2026 AI セキュリティ株式会社

ご支援事例　AEV の導入（モデルケース）

AEV による毎週の検証の立ち上げ

想定するお客様：金融・保険業｜メニュー：簡易トライアル Menu （AEV 中心）

外部公開資産を毎週検証し、「いま突ける穴」が見える状態をつくります。

脆弱性診断は年 1 回で、その間に増えた公開資産や
設定変更は確認できていない状態を想定しています。
まず AEV の検証を定着させ、是正の代行へと広げます。

当社が担うこと

- 01　対象資産（IP ・ドメイン）の棚卸しと検証範囲の設計
- 02　AEV の初期設定と毎週の検証サイクルの立ち上げ
- 03　検証結果の読み解きと月次報告会の運営

成果指標　実証された侵入経路の件数／是正着手までの日数

導入プロセス　対象の整理から月次報告まで

	お客様の業務の流れ	AI セキュリティの実施内容
1	対象資産の整理 IP ・ドメインの一覧	お客様　対象と除外リストをご提示
2	AEV の設定 範囲・頻度の設定	当社　検証範囲と実施頻度を設計
3	毎週の検証 外部から自動で	AEV　実証された侵入経路を報告
4	結果の読み解き 優先度の判断	当社　業務影響を踏まえて仕分け
5	月次の報告 是正の判断材料	定型化　報告様式を定めて継続

検証が定着したら、是正の代行へ広げる

※ 本ページは AEV のみを導入する場合の流れを示したモデルケースです。実際の導入事例が確定し次第、差し替えます。

Copyright(C)2026 AI セキュリティ株式会社

CHAPTER 04 | プラン・進め方

Plan & Process

プラン・進め方

3つのメニューと、
ご導入までの流れです。

IN THIS SECTION

このセクションの内容

この章のページ

ご提供メニュー P30

メニュー別の対応範囲 P31

ご導入までの進め方 P32

無償診断のご案内 P33

よくあるご質問 P34

Copyright(C)2026 AI セキュリティ株式会社

ご提供メニュー

AEV の毎週の検証に、推進担当（専門人材）の体制を組み合わせた 3 つのメニューをご用意しています。
推進担当の部分は社員代替サービスの標準プランに準拠し、稼働量や期間は柔軟に調整できます。

LIGHT

簡易トライアル Menu

推進担当 **180 万円／月（税別）**
＋ AEV ライセンス

体制の構成

AEV	毎週の検証
専門人材	0.5 人月　リモート常駐
管理者	0.1 人月　品質管理

こんなお客様に
- まずは検証結果の判定から始めたい
- 是正計画づくりを任せたい
- 小さく始めて効果を確かめたい

STANDARD　RECOMMEND

標準スターター Menu

推進担当 **450 万円／月（税別）**
＋ AEV ライセンス

体制の構成

AEV	毎週の検証
専門人材	1.0 人月　リモート常駐
管理者	0.5 人月　品質・継続性

こんなお客様に
- **検証から是正までを毎週回したい**
- **変更管理・部署調整まで任せたい**
- **是正の進み具合を毎週見たい**

PREMIUM

戦略的拡張 Menu

推進担当 **個別お見積**
＋ AEV ライセンス

体制の構成

AEV	毎週の検証・対象拡大
専門人材	複数名　常駐も可
管理者	専任　体制に応じて

こんなお客様に
- パッチ適用の作業まで任せたい
- 複数システムを並行で進めたい
- 経営層への報告まで整えたい

金額は柔軟に調整できます　**AEV**｜対象資産数に応じて　**稼働量**｜週の稼働日数・時間を増減　**期間**｜1か月単位で開始・見直し

※AEV のライセンスは年額 1,000 万円〜（200 アセットまで）が目安で、丸紅情報システムズ様を通じてご提供します。推進担当は当社と派遣または業務委託（準委任）でご契約いただきます。

Copyright(C)2026 AI セキュリティ株式会社

メニュー別の対応範囲

AEV による毎週の検証と結果のご報告は、すべてのメニューで共通してご提供します。
メニューの違いは、変更管理や是正の作業など、是正のどこまでを当社が担うかにあります。

対応項目	簡易トライアル Menu	標準スターター Menu	戦略的拡張 Menu
AEV による毎週の検証	○	○	○
検証結果の読み解き・週次報告	○	○	○
影響の判定・優先順位づけ	○	○	○
是正計画の策定	○	○	○
変更管理・関係部署との調整	△（一部）	○	○
パッチ・バーチャルパッチの適用作業	—	△（ご相談）	○
複数システムの並行対応・常駐	—	—	○
経営層向けのご報告	—	△（ご相談）	○

○ 対応　△ 一部対応・ご相談　— 対象外

Copyright(C)2026 AI セキュリティ株式会社

ご導入までの進め方

まずは無償診断で現在の状態を把握し、その結果を見たうえで次の進め方をご判断いただけます。
毎週の検証と是正の体制づくりは、診断結果やお客様のご体制に合わせて段階的に進めます。

STEP 1

1

無償診断の実施

外部から見える資産を対象に、
現在の状態を AEV で診断します。

お願いしたいこと

IP アドレス・ドメイン名のご提示

STEP 2

2

結果のご報告

実証された侵入経路と証拠、
優先して対応すべき点を
ご説明します。

お願いしたいこと

関係部署のご参加

STEP 3

3

メニューの決定

対象資産・体制・変更管理の
ルールを伺い、メニューと
運用の設計を決めます。

お願いしたいこと

体制とルールのご共有

STEP 4

4

毎週の運用開始

推進担当が参画し、検証と
是正のサイクルを毎週
回し始めます。

お願いしたいこと

ご担当窓口の設定

推進担当の人数や関わり方は、運用開始後も状況に合わせて見直せます。

Copyright(C)2026 AI セキュリティ株式会社

無償診断のご案内

攻撃者の AI が貴社の環境で何を見つけるのかを、先に知るところから始められます。
ご準備いただくのは、診断の対象とする IP アドレスやドメイン名の一覧だけです。

ご準備いただくもの

IP アドレスや
ドメイン名だけ

貴社の外部の攻撃対象領域を、
攻撃者と同じ目線で診断します。

01 実施する内容

攻撃者のように推論する AI エージェントが、外部から見える資産を検証します。
本番業務を妨げるような手法は使いません。

02 お渡しするもの

実際に悪用できると確認された箇所を、証拠とともにご報告します。
すぐ対応に移せる形で、優先して対応すべき点を整理します。

03 診断後のご相談

結果をもとに、毎週の検証と是正の体制をご提案します。
推進担当の関わり方も、結果に合わせて具体化します。

現在、チェック・ポイント社による無償診断を実施中です。

※ 無償診断の実施条件・対象範囲は、お申し込みの際にあらためてご案内します。

Copyright(C)2026 AI セキュリティ株式会社

よくあるご質問

Q 本番環境に影響はありませんか？

検証は必要最小限のリクエストによる非破壊の手法で行い、実行前に独立した AI が安全性を審査します。

Q 社内ネットワークも検証できますか？

AEV の対象は外部から見える資産です。社内の資産は、脆弱性診断など別の手段との組み合わせをご提案します。

Q 今のペネトレーションテストは不要ですか？

今のテストを補う位置づけです。業務ロジックの深い検証は人手のテスト、毎週の確認は AEV が担います。

Q 推進担当はどのような人材ですか？

脆弱性管理・脆弱性対応の経験を持つ専門人材です。 12,000 名の人材プールから、ご要件に合う人材をご提案します。

Q 契約形態はどうなりますか？

ライセンスは丸紅情報システムズ様経由、推進担当は当社との派遣または業務委託（準委任）のご契約です。

Q 社内にセキュリティ担当が少なくても始められますか？

はい。戦略的拡張 Menu では、パッチ適用の作業まで含めて当社が体制ごとご支援します。

Copyright(C)2026 AI セキュリティ株式会社

CHAPTER 05 | 背景

Why Now

背景

AI による攻撃の変化と、
変わり続ける IT 環境です。

IN THIS SECTION

このセクションの内容

この章のページ

- なぜ今、「 AI で検証し、人が直す」のか — P36
- AI 時代の攻撃と検証のギャップ — P37
- 日本でもサイバー攻撃・緊急対応が相次ぐ — P38
- 攻撃者はすでに AI を活用している — P39
- 事例：ソフトバンク社長が語った危機感 — P40
- 自社の IT 環境も、毎週のように変わっている — P41
- 不正アクセス・情報漏洩対策の緊急対応における課題 — P42

Copyright(C)2026 AI セキュリティ株式会社

WHY NOW

なぜ今、「AI で検証し、人が直す」のか。

AI によって攻撃は速く大規模になり、自社の IT 環境も毎週変わっています。
いま必要なのは、変化に合わせて検証し続けることと、
見つかった脆弱性を是正まで運ぶ人手です。



Copyright(C)2026 AI セキュリティ株式会社

AI 時代の攻撃と検証のギャップ

攻撃は AI によって速く大規模になり、軽微な設定ミスの組み合わせまで狙われるようになりました。
人手による年数回の検証だけでは、増え続ける脆弱性や設定ミスに追いつけなくなっています。



01 人の操作なしで自律的に悪用

最先端の AI モデルは、悪用可能な脆弱性や設定ミスを大規模かつ自律的に見つけられる段階にあります。

02 CVE 以外も侵入口になる

軽微な設定ミスや漏洩した認証情報の組み合わせでも、外部からの侵入口として見つけられてしまいます。

03 新しい AI モデルのたびに新たな脆弱性

モデルが更新されるたびに、対処済みのシステムから新たな脆弱性が見つかる状況が生まれています。

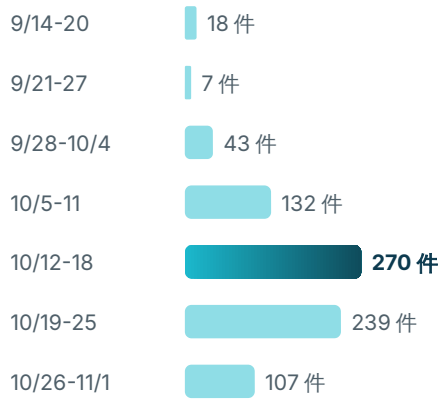
※ 図は概念図です。

Copyright(C)2026 AI セキュリティ株式会社

9 月後半以降、日本でもサイバー攻撃・緊急対応が相次ぐ

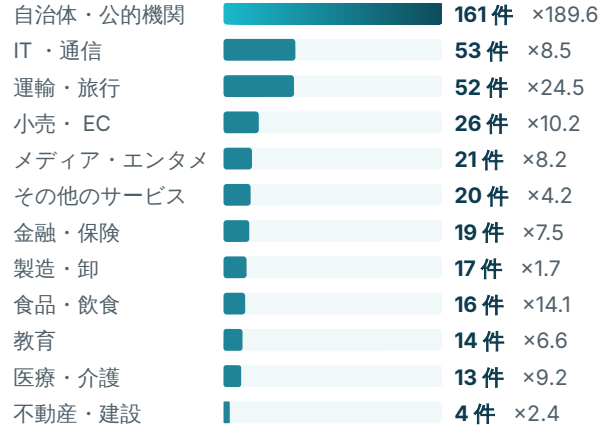
2026 年 9 月後半以降、国内でも情報漏えいや不正アクセスの公表が短期間に相次いでいます。
攻撃の入口と影響は多様化しており、事業継続のリスクは高い水準が続いています。

公表件数（週次）



業種別の公表

直近 30 日・線はふだん（1〜7 月）の 30 日あたり・倍率は参考値



急増の構図

1. **攻撃量**
   AI を利用し自動探索・大量配信
2. **侵入口**
   フィッシング／公開脆弱性
3. **事業影響**
   ランサムウェア・情報漏えい

「検知後の対応」だけでは遅い

公開資産・メール・ ID を横断し、
予防／迅速な修正／事業継続を一体で見直

攻撃の入口・影響は多様化

- **DDoS** サービス停止
- **ランサムウェア** 業務・供給停止
- **脆弱性悪用** 外部公開資産
- **メール／ ID** 不正アクセス

入口の多様化と「止まる・漏れる・広がる」事業影響への備えが急務

Copyright(C)2026 AI セキュリティ株式会社

出典： Check Point Software Technologies Ltd.

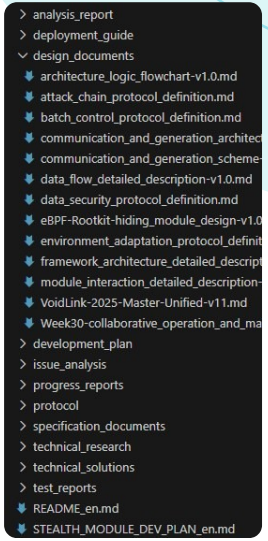
攻撃者はすでに AI を活用している

Check Point Research は、攻撃者が消し忘れた開発環境を発見し、その中身を分析しました。
AI が作成した計画書や仕様書が残されており、攻撃者がすでに AI を使える環境にあることが分かります。

Markdown の残骸： AI が作成した計画とスプリント

- 多数の .md ファイルが「残骸」として残されていた
- 高度に構造化された **LLM 形式のドキュメント**：スプリント計画、仕様書、コーディング標準

AI に対して「これは Red Team 用のツールだ」と説明することで、安全機能を巧みに回避



多くの報道機関から今回の不正アクセスに AI が使われている可能性
すべての攻撃で AI が使われている決定的な証拠はない
ただし攻撃者が AI をすでに使える環境にあるのが事実その対策が必要

Copyright(C)2026 AI セキュリティ株式会社

出典： Check Point Software Technologies Ltd.

事例：ソフトバンク社長が決算会見で語った危機感

大手通信事業者の社長でさえ、 AI による攻撃のスピードに「人の手では対応し切れない」と語っています。
診断・パッチ適用・稼働確認のサイクルを、速く継続的に回すことが求められています。

ソフトバンク 宮川社長（ 2026 年 11 月 9 日 決算説明会）

「 AI を使った攻撃が多くなっており、攻撃スピードが非常に速いので、人の手では対応し切れないのではないかと思っています。」

「正直もう疲れ切っている状態なんですが」

新しい AI モデルが公開されるたびに自社システムを試験すると、ほぼ必ず新たな脆弱性が見つかると述べています。

月 6 億〜 7 億件

偵察行為の件数（直近）

2025 年度の月平均約 3 億件から、毎月増加

7 分

子会社へのランサムウェア攻撃の犯行時間

アラート後に人が会議で判断する運用から、先に遮断する運用へ切り替え

1万 500 件 → 3 万 5000 件

自社システムの診断で見つかった脆弱性

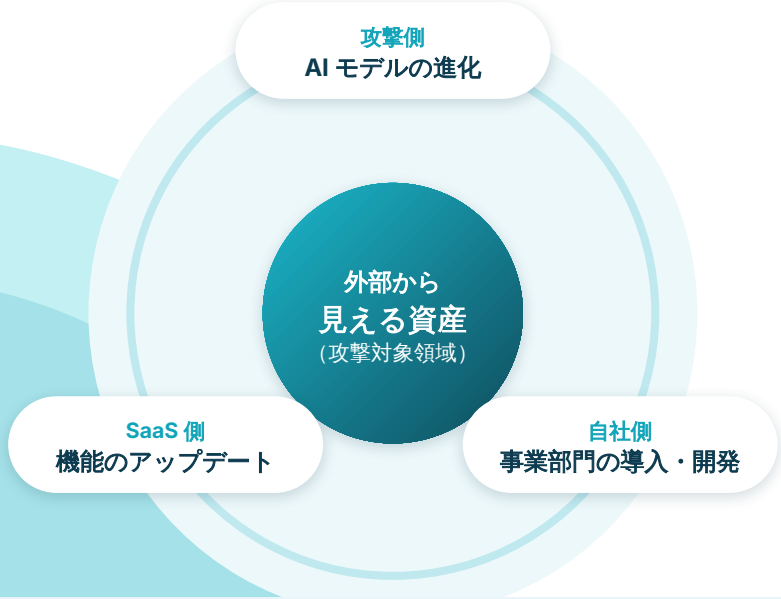
約 700 システムで 1万 500 件を 3 か月で修正後、最新 AI で再診断し 3 万 5000 件

※出典： ITmedia ビジネスオンライン（ 2026 年 11 月 9 日）「ソフトバンク宮川社長『正直もう疲れ切っている』」をもとに当社作成

Copyright(C)2026 AI セキュリティ株式会社

自社の IT 環境も、毎週のように変わっている

攻撃者だけでなく、守る側の自社の IT 環境も、事業部門の取り組みによって毎週のように変わっています。
デジタル化が進むほど外部から見える資産は増え、弱点が広がるのは自然なことです。



01 攻撃側：手法は毎週のように高度化

攻撃者が AI を使い、新しいモデルの登場に合わせて
攻撃の手法も高度化し続けています。

02 自社側：セキュリティ部門が知らない資産

事業部門が自ら SaaS を導入したり、 kintone などで
アプリを作ったりと、把握されない資産が増えます。

03 SaaS 側：サービスそのものも変わる

「 SaaS is Dead 」とも言われるなか、 SaaS 各社は
生き残りをかけて機能のアップデートを重ねています。

年 1〜2 回の検証では、検証した時点の「スナップショット」しか確認できません。

Copyright(C)2026 AI セキュリティ株式会社

不正アクセス・情報漏洩対策の緊急対応における課題

不正アクセスや情報漏洩を防ぐには、外部侵入につながる「入口」と「弱点」を把握して塞ぐことが重要です。
ただし、６つの対策を自社だけで毎週続けるには、ツールと人の両方が必要になります。

1 外部公開資産の把握

Web 、サーバー、 VPN 、クラウド、 API など、外部からアクセス可能な資産を把握する

攻撃者から見た場合の外部公開資産把握できていますか？
ASM

2 外部に露出した情報の把握

漏洩資格情報・機密情報、フィッシングサイト、なりすましドメインを確認する

自社の情報の漏洩機密情報や攻撃者の情報の把握できていますか？
脅威情報の活用

3 脆弱性の確認と対応

CVE や未適用パッチなどの既知の脆弱性を確認し、優先的に修正する

利用しているソフトの脆弱性把握し対応できていますか
脆弱性管理

4 設定・認証・権限の見直し

設定ミス、不要な公開・アカウント、弱い認証、過剰な権限を確認・是正する

現在の設定の状況把握できていますか危険な設定把握できていますか？
設定ドキュメント

5 外部からの侵入可否の検証

脆弱性診断やペネトレーションテストで、実際に外部から侵入できないかを確認する

外部からの侵入のペネトレーションテストできていますか？
ペネトレーションテスト

6 侵入兆候の確認

ログやアカウントを確認し、すでに不正アクセスされていないかを確認する

CVE のみならず非 CVE や設定ミス、漏洩情報の組み合わせによる侵入を想定して
全ての情報を網羅的にすべて洗い出し攻撃者が攻撃してくる一番危険な侵入先を特定することができますか？
新しい攻撃者や攻撃手法、ソフトウェア仕様に合わせて例えば毎週全部チェックするためにツールや組織、人材はお持ちですか？

Copyright(C)2026 AI セキュリティ株式会社

出典： Check Point Software Technologies Ltd.

CHAPTER 06 | 会社紹介

Company

会社紹介

AI 時代のセキュリティ対策を担う
当社の概要と経営陣・中核メンバーです。

IN THIS SECTION

このセクションの内容

この章のページ

AI 時代のセキュリティ対策を担う会社 P44

代表取締役社長 CEO　堀居 隆生 P45

代表取締役 COO　市川 貴大 P46

中核メンバー P47

Copyright(C)2026 AI セキュリティ株式会社

AI 時代のセキュリティ対策を担う会社

当社は AI 推進とセキュリティ強化を両輪とする総合型ファームとして、 AI 時代のセキュリティ対策を担います。
コンサルティングから導入、人材のご提供まで、皆さまの持続的な企業価値の向上をご支援します。

COMPANY

AI セキュリティ株式会社 AI Security Inc.

代表者 代表取締役 CEO 堀居 隆生
代表取締役 COO 市川 貴大

本 社 東京都新宿区四谷 1-9-16 三宅ビル 4F

許認可 有料職業紹介 13- ユ -314622 ／ 労働者派遣 派 -13-317530

累計支援企業数
200 社

従業員数
120 名
※ パート・業務委託込

創業期
2021 年 9 月設立
※4 期目に決算期変更

当社の特徴

1. **Glasswing 採択ベンダーと提携**
   CrowdStrike ・ AWS ・ Cisco （ Splunk ）等
2. **国内最大手 SIer と強連携**
   AI×Security 領域で独占的に推進中
3. **プライム上場から急成長企業まで**
   業種を問わず累計 200 社を支援
4. **社内に AI Security 研究組織**
   大手ファーム・ SIer 出身者が在籍

出身企業

Deloitte. デロイトトーマツ / accenture / pwc / NRI SECURE / IBM / EY / NEC Orchestrating a brighter world / HITACHI Inspire the Next / CTC / baycurrent / Simplex Inc. / IIJ / GMO CYBER SECURITY IERAE / BANK OF AMERICA

所属団体

JNSA 特定非営利活動法人 日本ネットワークセキュリティ協会 / 一般社団法人 AIガバナンス協会 AI Governance Association

取得認証

ISO27001 （ ISMS ）
JISQ15001 （ P マーク）

Copyright(C)2026 AI セキュリティ株式会社

AI 活用と安全性を両立させる 新たなセキュリティ基盤づくりに 挑んでいます

堀居 隆生 Takao Horii

代表取締役社長 CEO ／ AI セキュリティ株式会社

経歴・実績

- 大学時代に学生起業を経て事業売却を経験。
- ソフトバンク株式会社にて倍率 50 倍の中期インターンシップを経験。
- X Mile 株式会社に創業期メンバーとして参画し、西日本エリア拠点責任者を務める。
- PwC Japan 有限責任監査法人のインターン期間中にインド（バンガロール）へ渡航し、大手企業・スタートアップとの商談 20 件を獲得。内定者代表挨拶を務め、新卒で Cyber Security 領域の新規事業立案組織に参画。
- X-couture 株式会社を創業者兼 COO として立ち上げ、パリコレ出展ブランド『 yoshiokubo 』と共創で楽天ファッションウィークを企画。デジタルドレス事業を展開し、ランウェイ衣装をフォトグラメトリで 3DCG 化し NFT ドレスを販売。
- **2021年 AI セキュリティ株式会社を創業**



CEO Message

「 Secure today, Design tomorrow 」——
今日を守り、明日を築く。これが私たちのスローガンです。

不確実性の高いこの時代において、信頼されること。
その信頼を、未来への跳躍に変えていくこと。
その両立を、皆様と共に実現していきたいと考えています。

Copyright(C)2026 AI セキュリティ株式会社

AI 活用と安全性を両立させる 新たなセキュリティ基盤づくりに 挑んでいます

市川 貴大 Takahiro Ichikawa
代表取締役 COO ／ 共同創業者 ／ AI セキュリティ株式会社

経歴・実績

- 早稲田大学法学部卒業（司法予備試験短答式合格）
- 在学中に、小売店の廃棄寸前のお惣菜をフードシェアするスタートアップを創業し法人売却を経験。
- 学生時代、ドローンスタートアップの Terra Drone 株式会社に中期インターンとして参画。
- 大学卒業後、 PwC に入社し、クラウド安全性評価 ISMAP の制度設計と要求事項の検討に関与。
  並行して、 Cyber Security 領域の新規事業立案組織に参画し、 API 安全性評価を企画し採択。
  コンサルティング案件においては、官公庁を中心としたセキュリティ支援案件を複数推進。
- X-couture 株式会社を創業者兼 CEO として立ち上げ、
  パリコレ出展ブランド『 yoshiokubo 』と共創で楽天ファッションウィークを企画。
  デジタルドレス事業を展開し、ランウェイ衣装をフォトグラメトリで 3DCG 化し NFT ドレスを販売。
- **2021年 AI セキュリティ株式会社を創業**



COO Message

「挑戦の隣に、いつも、私たちがいる。」——
挑戦が生まれるのは、いつも最前線だからこそ、
守る者が立つのも最前線であるべきだと考えています。
そしてセキュリティを、誰もが憧れる仕事に。
そして、挑戦の隣に、いつも、私たちがいる。
それが、私たちの誓いです。

Copyright(C)2026 AI セキュリティ株式会社

大手ファーム・グローバルセキュリティベンダー出身の中核メンバーが在籍

大手 Consulting ファームにて PMD を務めたメンバーや、グローバルセキュリティベンダーにて責任者を務めたメンバー、官公庁対応・事業会社としてのセキュリティ戦略・管理に従事した布陣にて、お客様への価値提供を推進しております。



コンサルティング＆ソリューション事業統括本部 事業統括本部長

和田 Benjamin 真治

Apple Inc.、 NRI セキュアテクノロジーズ株式会社に従事し、セキュリティ戦略策定と Digital Identity に強みを有する



Account Sales 本部
本部長

前田 和則

Symantec 社にて営業本部長・執行役員を歴任した後に、 Accenture では Managing Director として Security Consulting 部門を立ち上げ



Partner
兼 Security Evangelist

河北 将弥

KPMG アソシエイトパートナーとして東京大学の松尾研究室に出向し、 AI×Security 領域にて市場動向調査・政府機関との推進を実施



コンサルティング＆ソリューション事業統括本部 ゼロトラスト推進事業部長

江口 真

NTT 研究所、 Zscaler Inc の TAC マネージャー、 Illumio 社のプリンシパルを歴任し、ゼロトラスト領域とマイクロセグメンテーション領域に強みを有する



コンサルティング＆ソリューション事業統括本部 プリンシパル

渡辺 英治

EMC/RSA の後にシスコシステムズ（ Splunk Inc ）では、 Professional Service 部門を責任者として立ち上げ、 SIEM やログ監視に強みを有する



コンサルティング＆ソリューション事業統括本部 Sec for AI 推進事業部長

河太 優治

中央省庁に約 20 年間従事し、楽天㈱では AI ガバナンス部門長に就任し、 AI ガバナンス及び Incident 対応に強みを有する

Copyright(C)2026 AI セキュリティ株式会社

Confidential

まずは、貴社の外部の攻撃対象領域を AEV で診断してみませんか。

攻撃者の AI が何を見つけるのかを先に知ることから、計画的な脆弱性対応が始まります。

01 診断対象のご相談

対象とする IP アドレス・ドメイン名の
範囲をご一緒に確認します。

02 無償診断の実施

AEV で外部の攻撃対象領域を検証します。
本番業務を妨げる手法は使いません。

03 結果のご報告とご提案

証拠とともに結果をご説明し、
毎週の検証と是正の体制をご提案します。

ご不明な点やご相談は、当社の担当営業までお気軽にお問い合わせください。

Copyright(C)2026 AI セキュリティ株式会社

Secure today, Design tomorrow

見つけて、直して、
防御力を高め続ける。

サイバー脆弱性対応代行サービスは、自律型 AI ペネトレーションテストと是正の推進をひとつながりで担い、
お客様の防御力を継続的に高めていきます。

AI セキュリティ株式会社

労働者派遣事業 許可番号：派 -13-317530

Copyright(C)2026 AI セキュリティ株式会社

APPENDIX | AEV の仕組み

Appendix

AEV の仕組み

本サービスの検証を担う
Check Point AEV の仕組みと安全設計です。

IN THIS SECTION

このセクションの内容

この章のページ

- AEV とは・ AEV の役割 P51 ～ 52
- 検証プロセスと検証の仕組み P53 ～ 54
- フロンティア AI への取り組みと BLAST P55
- AEV の対象範囲 P56 ～ 57
- 本番環境における安心安全な実行の約束 P58 ～ 59
- AEV を実施する流れとレポート P60 ～ 61

Copyright(C)2026 AI セキュリティ株式会社

AEV （ Agentic Exposure Validation ） とは

AEV は、攻撃者のように推論する AI エージェントが、外部から侵入できるかを証拠つきで確かめる仕組みです。
理論上のリスクを並べた一覧ではなく、実際に悪用できる箇所とその経路が具体的に分かります。

01 外部から見える資産を対象に検証

必要なのは IP アドレスやドメイン名だけです。
資産・ CVE ・漏洩した認証情報などをもとに分析します。

02 攻撃者のように推論する AI エージェント

Check Point の脅威インテリジェンスと照合し、
業務を妨げない手法で「本当に悪用できるか」を確認します。

03 短時間で多数の攻撃パターンを実施

100 アセットを約 1 時間で、場合により 1 万を超える
攻撃パターンで検証します。結果はすべて証拠つきです。

検証結果のイメージ

実証済み	**管理画面への到達経路を確認** 到達の手順と応答の記録を証拠として提示
防御済み	**既知の脆弱性は遮断を確認** 既存の防御で対処でき、追加の対応は不要
除外	**実証できなかった検出結果** 報告から除き、確認すべき件数を絞り込み

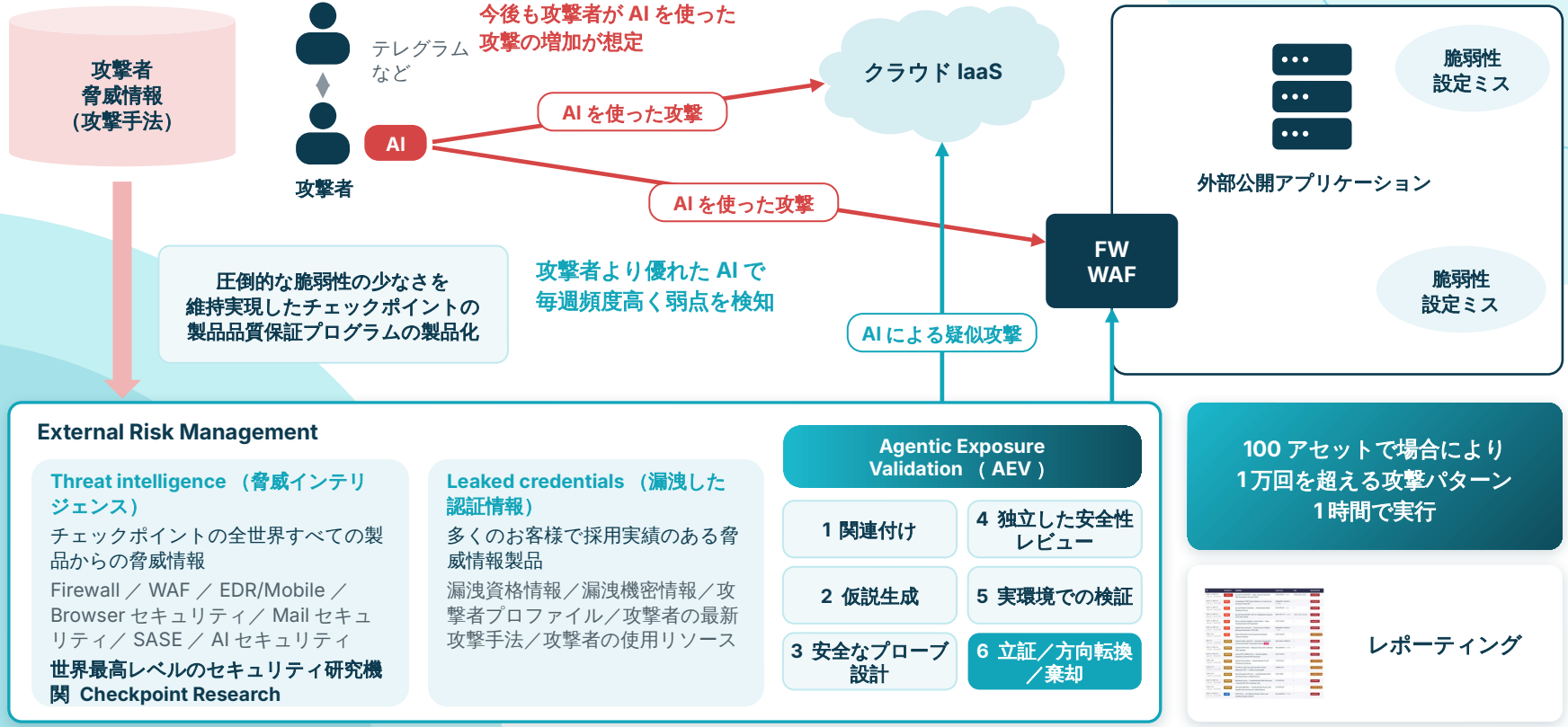
※ 説明用のイメージです

届く結果はすべて証拠つき。すぐ対応に移せます。

※AEV ： Check Point Software Technologies 社の Agentic Exposure Validation 。製品の仕様は同社の公開情報・ご紹介資料にもとづきます。

Copyright(C)2026 AI セキュリティ株式会社

攻撃される前に、 AI で弱点を見つけ出す AEV



Copyright(C)2026 AI セキュリティ株式会社
出典： Check Point Software Technologies Ltd.

AEV の検証プロセスと検証対象

AI エージェントが分析・照合・確認・実証の 4 段階を自律的に進め、悪用できるものだけを証拠とともに示します。
検証の対象は Web アプリケーションに限らず、 API や VPN などを含む外部から見える資産の全体です。

STEP 1
分析
資産・技術・ CVE ・
認証情報を把握

STEP 2
照合
脅威インテリジェンス・
攻撃者の行動と照合

STEP 3
確認
既存の防御で対処
できているかを確認

STEP 4
実証
攻撃者の思考を再現し、
証拠を提示

検証の対象（外部から見える資産）

Web アプリケーション | API | VPN | 管理コンソール | クラウド | 証明書・ DNS | 公開ポート・サービス

手がかりにする情報：漏洩した認証情報、ソースコードの露出、 CVE 、ダークウェブの情報 など
対象外：社内ネットワーク・端末などの内部限定資産、侵入後の横展開（内部は別の統制で補完します）

※AEV ： Check Point Software Technologies 社の Agentic Exposure Validation 。製品の仕様は同社の公開情報・ご紹介資料にもとづきます。

Copyright(C)2026 AI セキュリティ株式会社

Frontier AI を利用した AEV の仕組み

脅威インテリジェンス

ダークウェブインテリジェンス
侵害フォーラム、ランサムウェアリーク、攻撃者の通信

認証情報 & インフォスティーラー
漏洩パスワード、スティーラーログ、アクティブセッション

ソースコード露出
公開リポジトリ、 API キー、 Git 履歴のシークレット

CVE & エクスプロイト
検出技術にマッピングされた既知の脆弱性

攻撃対象領域の発見

組織の全資産
ドメイン、サブドメイン、 IP 、クラウドリソース

公開ポート & サービス
公開インターフェース、管理パネル、 API

証明書 & DNS データ
TLS 証明書、 CNAME チェーン、ダングリングレコード

技術 & インターフェース
フレームワーク、 CMS 、バージョンフィンガープリント

AEV エージェント型検証エンジン

1. **相関分析 & 優先順位付け**
   資産と脅威情報を照合 — CVE を技術に、認証情報を ID テナントに紐付け
2. **攻撃パターンの特定**
   攻撃チェーンを推論：クレデンシャルスタッフィング、サブドメイン乗っ取り、 API バイパス、情報抽出
3. **プローブの作成 & 検証**
   安全な読み取り専用の実証コードを作成 — 実行前に独立した AI がレビュー
4. **対象への実行**
   本番環境にプローブを送信 — 証拠を取得：抽出データ、発行トークン、認証情報の確認
5. **実証、方向転換、または削除**
   実証済み → 証拠付きで報告。ブロック → 新たな攻撃ベクトルへ転換。未実証 → 削除

対象組織

- API プローブ → HTTP Web アプリ
- クラウド乗っ取り → S3 クラウド基盤
- 資格情報総当たり → IAM ID 管理
- Swagger の悪用 → DEV 開発 / ステージング
- ファームウェア抽出 → VPN ネットワーク

Copyright(C)2026 AI セキュリティ株式会社

出典： Check Point Software Technologies Ltd.

フロンティア AI への取り組みと BLAST

フロンティア AI の登場で、脆弱性が見つかってから悪用されるまでの時間は大きく縮まりつつあります。
Check Point は、製品の品質保証に使う独自のテストシステム「 BLAST 」を AEV にも活用しています。

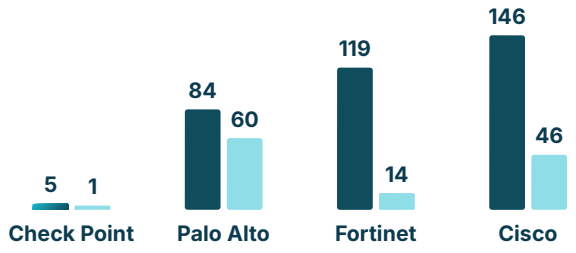
Frontier AI モデル準備プログラム (製品品質保証)

1. AI による脆弱性の発見
2. モニタリングの強化
3. 修正展開の高速化
4. ベストプラクティスの実践

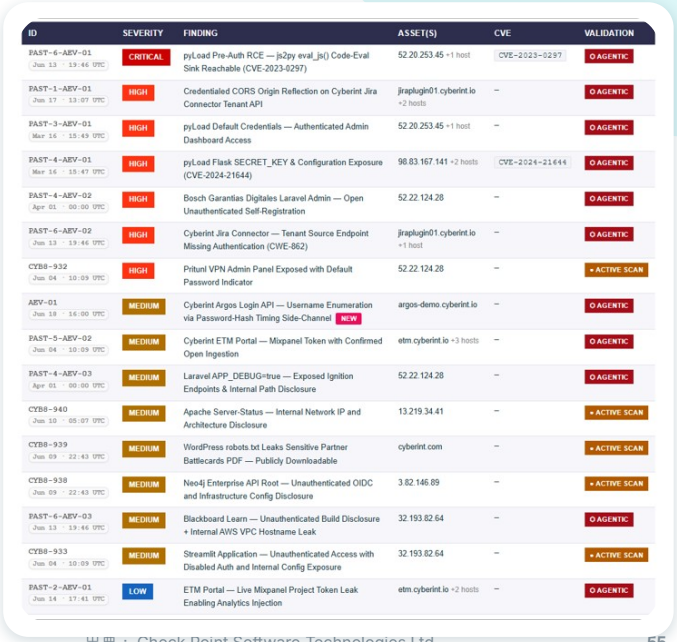
独自のテストシステム
BLAST による分析
Business Logic Application Security Testing

成果＆推奨アクション
修正 Jambo Hotfix を公開

■ “Critical & High” ソフトウェアの脆弱性数 （ 2020- ）
■ “Critical & High” の脆弱性修正までの平均時間 (Day) （ 2020- ）



BLAST を活用した Agentic Exposure Validation （ AEV ）



出典： Check Point Software Technologies Ltd.

Copyright(C)2026 AI セキュリティ株式会社

AEV の対象範囲（ 1/2 ）

AEV の主な検証範囲（外部からの悪用可能性を安全に実証）

1 外部公開資産

Web
例： Web サイト、 Web アプリケーション

API
例： REST API 、 GraphQL

VPN
例：リモートアクセス

管理コンソール
例：運用管理画面

クラウド
例：
SaaS 、 IaaS 、 PaaS

2 弱点

既知 CVE
例： CVE-2023-XXXX

設定不備
例：不要な機能の公開、デフォルト設定

認証回避
例：認証の不適切な実装

漏えいキー／トークン
例： API キー、クラウド認証情報

非 CVE の組合せ
例：設定不備＋仕様の悪用

3 偵察・自動スキャン

通常の自動化
例：ポートスキャン、サービス・バージョン検出、既知の脆弱性スキャン

AI 支援
例：ターゲットの分析、攻撃手法の選択・最適化、公開情報の相関分析

4 初期アクセス

Web からの侵入
例：脆弱性の悪用、認証バイパス

API の悪用
例：不適切な認可、トークンの悪用

VPN の侵入
例：認証回避、既知の脆弱性

管理コンソールの侵入
例：認証情報の悪用、設定不備の悪用

クラウド環境への侵入
例：漏えいキーの利用、権限の誤設定

AEV 単独では不十分／補完統制が必要

内部環境・エンドポイント等は別の統制で対応 = AEV で検証範囲外

5 権限拡大・横展開

権限昇格
例：ローカル権限の取得、クラウド権限の拡大

横展開
例：内部ネットワークへの移動、他システムへの侵害、認証情報の横取り

6 情報窃取・暗号化・サービス停止

情報窃取
例：機密データ、個人情報、知的財産

暗号化
例：ランサムウェアによるデータ暗号化

サービス停止
例：システムの破壊、業務停止、 DoS 攻撃

エンドポイント・モバイル・内部限定資産（例）

エンドポイント（例：社内 PC 、サーバー）
モバイル（例：スマートフォン、タブレット）
内部限定資産（例：社内システム、閉域ネットワーク）

Copyright(C)2026 AI セキュリティ株式会社

出典： Check Point Software Technologies Ltd.

AEV の対象範囲（ 2/2 ）

証拠

HTTP リクエスト／レスポンス、到達性、単一の安全な認可確認、無害な実行シグナル

例：ステータスコード、公開情報の取得、認可された範囲での安全な操作

安全制約

読み取り中心、 DoS ・ファジング・ブルートフォースなし、認可スコープ限定

例：データの変更・削除を行わない、システムに影響を与える負荷をかけない、事前に合意した範囲内での検証

関連するアプローチの違い

Scanner （スキャナー）

存在／バージョン

- サービスの存在確認
- ソフトウェアのバージョン検出
- 既知の脆弱性の有無を列挙
- 悪用可否は検証しない

Attack Path （アタックパス）

理論的経路

- 複数の弱点をつないだ攻撃シナリオ
- 到達可能性の理論的な分析
- 実際の悪用可否は検証しない
- 主に設計・リスク分析に利用

AEV （自動化された露出検証）

外部からの悪用可能性を安全に実証

- **実環境での到達性と悪用可能性を検証**
- **安全な方法での限定的な実証**
- **証拠（リクエスト / レスポンス等）を取得**
- **対応の優先順位付けに活用**

実施しない攻撃例

- 有効な資格情報を用いた通常ログイン
- MFA 疲労攻撃、セッション／ OAuth トークン窃取
- 悪意ある内部者
- 内部限定資産、侵入後の横展開、EDR 無効化
- DDoS 、ファジング、ブルートフォース

Copyright(C)2026 AI セキュリティ株式会社

出典： Check Point Software Technologies Ltd.

AEV の本番環境における安心安全な実行の約束（ 1/2 ）

5 つのリスクに対する安全設計

1 可用性とデータ整合性の保護

サービス停止（ Availability Risk ）やデータの書き換え・設定変更（ State Change Risk ）を防止する制御が組み込まれています。

2 認証情報とスコープの厳格管理

アカウントロック（ Credential Risk ）の回避、許可範囲外へのアクセス（ Scope Risk ）、および検証内容の漏洩（ Disclosure Risk ）を防ぎます。

Safety Floor （解除不能な 5 つの安全原則）

RULE 1	RULE 2	RULE 3	RULE 4	RULE 5
DoS 攻撃・負荷攻撃の禁止	**データ変更・書き込みの禁止**	**ブルートフォース（総当たり）の禁止**	**内部ネットワークスキャンの排除**	**Read-Only 検証の徹底**
負荷をかけず、検証に必要最小限のリクエストのみを送信します。	データの削除や設定変更を一切行わない非破壊的なアプローチを徹底します。	認証試行は 1 回のみに制限し、パスワードの総当たりによるロックアウトを防ぎます。	インターネット公開資産のみを対象とし、 RFC1918 （プライベート IP ）へのスキャンは行いません。	攻撃の「可能性」を証明するだけで、実際の攻撃コードの実行は行いません。

Copyright(C)2026 AI セキュリティ株式会社

出典： Check Point Software Technologies Ltd.

AEV の本番環境における安心安全な実行の約束（ 2/2 ）

「証明」と「悪用」の境界線

攻撃カテゴリ	AEV が実施すること（証明）	AEV が絶対に行わないこと（悪用・破壊）
API キー漏洩	キーが有効かどうかの確認	大量データ取得、不正課金、状態変更
SQL Injection	SQLi の実行可能性の確認	DB 全件取得、テーブル列挙、データ削除
リモートコード実行 (RCE)	コマンド実行可能性の確認	任意コマンド実行、マルウェア設置、永続化
認証バイパス	保護されたページへ到達可能が確認	—

3 段階の AI レビュープロセス

Stage 1 ： Self Challenge

生成 AI 自身が、手順が安全範囲内か、誤検知ではないかを自ら検証します。

Stage 2 ： Independent AI Review

別の AI モデルが客観的に審査し、危険と判断された場合は即座に却下・削除します。

Stage 3 ： Adversarial Judging

疑いの目を持つ第 3 の AI が、エビデンスの妥当性を再評価し、誤検知を徹底排除します。

運用上の安全制御

トラフィックの自動減速・停止機能

通常 1〜3 リクエストの少量通信で行い、システム遅延を検知すると自動で減速、または停止します。

禁止されたアクション

権限昇格、横展開（ラテラルムーブメント）、 DNS 変更、 OT/ICS への攻撃などは、いかなる場合も実行されません。

Copyright(C)2026 AI セキュリティ株式会社

出典： Check Point Software Technologies Ltd.

AEV を実施する流れ

AEV は、 Check Point の External Risk Management ツール上で対象範囲を設定して実行します。
お客様のご準備はアカウントの作成と対象の提示だけで、テストは 24 時間、レポートは 2 週間でお届けします。

1. AEV 機能を有効化

Account Settings より Active Exposure Validation 及び Agentic Exposure Validation を有効化

お客様 ユーザーアカウントの作成

2. AEV の対象範囲を設定

Account Settings より AEV 実施の対象範囲を設定
「全資産」「特定の資産」が選択可能

お客様 ドメイン名や IP アドレスの提供
（除外リストの提供）

チェックポイント 疑似攻撃に利用する IP アドレスの提示

3. 結果の出力

External Attack Surface タブ、 AEV より結果が出力される
Download Findings Report よりレポート出力が可能

チェックポイント レポートの提出

テストは 24 時間で実施　レポート報告に 2 週間

Copyright(C)2026 AI セキュリティ株式会社

出典： Check Point Software Technologies Ltd.

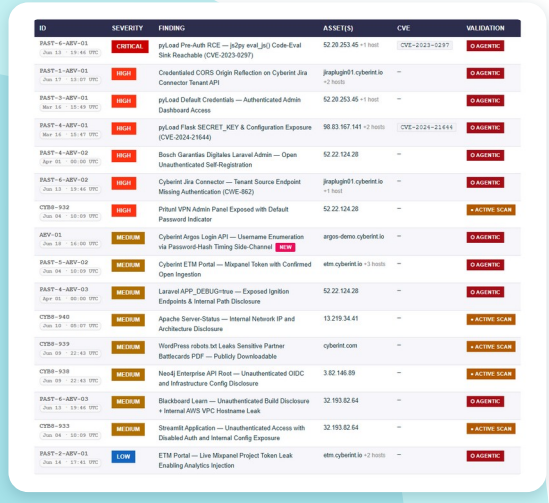
レポートイメージ

サマリ

14 DOMAINS	767 SUBDOMAINS	542 IPS	11 LEAKED CREDENTIALS	16 ALERTS ANALYSED	7 AEV RUNS

1 CRITICAL	6 HIGH	8 MEDIUM	3 LOW	18 TOTAL DISTINCT

課題一覧



ID	SEVERITY	FINDING	ASSET(S)	CVE	VALIDATION
PAST-6-AEV-01 Jun 13 · 19:44 UTC	CRITICAL	pyLoad Pre-Auth RCE — js2py eval_js() Code-Eval Sink Reachable (CVE-2023-0297)	52.20.253.45 +1 host	CVE-2023-0297	O AGENTIC
PAST-1-AEV-01 Jun 17 · 11:07 UTC	HIGH	Credentialed CORS Origin Reflection on Cyberint Jira Connector Tenant API	jiraplugin01.cyberint.io +2 hosts	–	O AGENTIC
PAST-3-AEV-01 Mar 14 · 15:43 UTC	HIGH	pyLoad Default Credentials — Authenticated Admin Dashboard Access	52.20.253.45 +1 host	–	O AGENTIC
PAST-4-AEV-01 Mar 14 · 15:47 UTC	HIGH	pyLoad Flask SECRET_KEY & Configuration Exposure (CVE-2024-21644)	98.83.167.141 +2 hosts	CVE-2024-21644	O AGENTIC
PAST-4-AEV-02 Apr 01 · 00:00 UTC	HIGH	Bosch Garantías Digitales Laravel Admin — Open Unauthenticated Self-Registration	52.22.124.28	–	O AGENTIC
PAST-6-AEV-02 Jun 13 · 19:46 UTC	HIGH	Cyberint Jira Connector — Tenant Source Endpoint Missing Authentication (CWE-862)	jiraplugin01.cyberint.io +1 host	–	O AGENTIC
CYBR-932 Jun 04 · 10:09 UTC	HIGH	Pritunl VPN Admin Panel Exposed with Default Password Indicator	52.22.124.28	–	• ACTIVE SCAN
AEV-01 Jun 18 · 16:00 UTC	MEDIUM	Cyberint Argos Login API — Username Enumeration via Password-Hash Timing Side-Channel NEW	argos-demo.cyberint.io	–	O AGENTIC
PAST-5-AEV-02 Jun 04 · 10:09 UTC	MEDIUM	Cyberint ETM Portal — Mixpanel Token with Confirmed Open Ingestion	etm.cyberint.io +3 hosts	–	O AGENTIC
PAST-4-AEV-03 Apr 01 · 00:00 UTC	MEDIUM	Laravel APP_DEBUG=true — Exposed Ignition Endpoints & Internal Path Disclosure	52.22.124.28	–	O AGENTIC
CYBR-940 Jun 10 · 08:07 UTC	MEDIUM	Apache Server-Status — Internal Network IP and Architecture Disclosure	13.219.34.41	–	• ACTIVE SCAN
CYBR-939 Jun 09 · 22:43 UTC	MEDIUM	WordPress robots.txt Leaks Sensitive Partner Battlecards PDF — Publicly Downloadable	cyberint.com	–	• ACTIVE SCAN
CYBR-938 Jun 09 · 22:43 UTC	MEDIUM	Neo4j Enterprise API Root — Unauthenticated OIDC and Infrastructure Config Disclosure	3.82.146.89	–	• ACTIVE SCAN
PAST-6-AEV-03 Jun 13 · 19:46 UTC	MEDIUM	Blackboard Learn — Unauthenticated Build Disclosure + Internal AWS VPC Hostname Leak	32.193.82.64	–	O AGENTIC
CYBR-933 Jun 04 · 10:09 UTC	MEDIUM	Streamlit Application — Unauthenticated Access with Disabled Auth and Internal Config Exposure	32.193.82.64	–	• ACTIVE SCAN
PAST-2-AEV-01 Jun 14 · 17:41 UTC	LOW	ETM Portal — Live Mixpanel Project Token Leak Enabling Analytics Injection	etm.cyberint.io +2 hosts	–	O AGENTIC

課題詳細（攻撃経路）



CVEについて

CVE-2023-0297

攻撃経路

課題詳細（対処策例）



私たちが何を試し、何を試さなかったか

緩和策

再現方法

出典： Check Point Software Technologies Ltd.