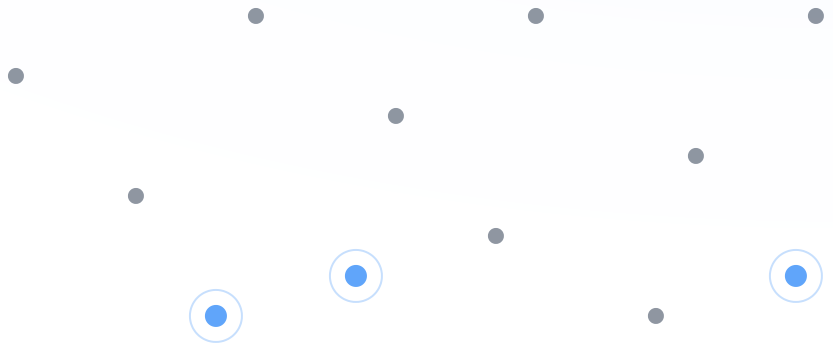
PentaTrail

見えない資産が、最大の脆弱性になる

AIネイティブの CTEM / ASM プラットフォーム

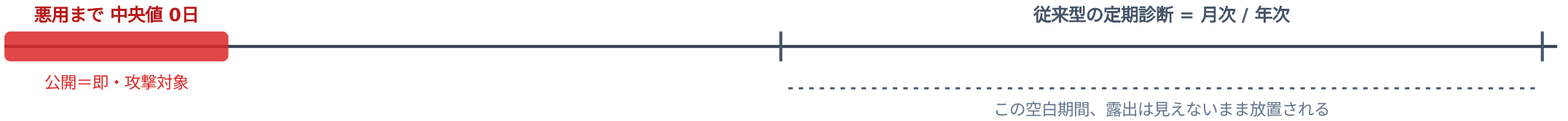
外部に公開されたドメイン・IP・ポート・クラウドバケット。管理台帳に載っていない資産こそ、攻撃者が最初に狙う場所です。攻撃者と同じ視点で、あなたの攻撃面を継続的に監視します。



なぜ今か

露出を放置できる時間は、もうゼロになった

脆弱性の「公開 → 大規模悪用」の時間差が消えつつあります。年に一度の診断では、もう追いつきません。



0日

公開から悪用までの猶予

エッジ機器の KEV（悪用が確認された脆弱性）の、公開から大規模悪用までの中央値／ Verizon DBIR 2025

84%

外部公開機器からの侵入

ランサム侵入経路が VPN・リモートデスクトップ等の外部公開機器／ 警察庁 2025年上半期

73%

管理外資産が原因

未把握・管理外の資産に起因するインシデントを経験した責任者の割合／ Trend Micro・CSO Online 2025

経済産業省「サプライチェーン強化に向けたセキュリティ対策評価制度（SCS）」が2026年度末に開始予定。取引先から客観的な説明を求められる場面が増えています。

BLIND SPOTS

いま、組織が直面している3つの死角

把握できない外部資産

クラウド移行・M&A・部門ごとのサブドメイン。IT資産台帳だけでは、外部露出の全体像を掴めません。攻撃者に見えているものが、自分には見えていない。

属人化するセキュリティ運用

スキャン結果の解釈、優先度判断、経営層への報告 ── すべてが特定の担当者に依存。人が変われば、対応品質もリスク判断も変わります。

説明できないリスク

「うちは安全なのか？」と問われたとき、直感ではなく数字で答えられるか。定量的な根拠でリスクを説明する力が求められています。

→ **PentaTrail は、この3つの死角を埋めます。** 外部資産を自動で洗い出し、危険な順に並べ、経営に数字で報告するまでを一気通貫で。

CTEM FRAMEWORK

見つけて終わりにしない ── CTEM 全5段階を回し続ける

CTEM（継続的脅威エクスポージャー管理）は、外部から見える弱点を継続的に発見・評価・対処する枠組み。一度きりの診断ではなく、5段階を回し続けて攻撃面を縮小します。

1 SCOPING
範囲確定
監視対象のドメイン群を確定

2 DISCOVERY
自動発見
外部資産を確定的に洗い出す

3 PRIORITIZE
優先順位
危険な順に並べ替える

4 VALIDATION
実証
本当に悪用できるか確かめる

5 MOBILIZE
対処・報告
直しきり、経営に見せる

継続的に反復 ── 攻撃面は毎日変わる

プラン別カバー範囲	① 範囲確定	② 発見	③ 優先順位	④ 実証	⑤ 対処・報告
ASM（見つける・狙われやすさ）	✓	✓	危険度づけ	—	AIガイダンス閲覧
CTEM（実証・直す・報告）	✓	✓	✓	✓	✓

DISCOVERY ／ 発見

推測ではなく、技術的な裏付けで"見えない資産"を洗い出す

管理台帳に載っていない資産こそ、攻撃者が最初に狙う場所。PentaTrail は公開情報源から、技術的に裏付けのある資産だけを確定的に発見します。AIの推論には依存しません。

確定的な手がかりから 公開情報源

- DNS
- CT Log（証明書）
- WHOIS
- 逆引き IP

AIの推論に依存せず、**技術的に裏付けのある手がかり**だけを使用。推測で資産を"でっち上げ"ません。

→

"見えない資産"を発見 台帳の外まで

- ドメイン・サブドメイン
- IP アドレス
- 開放ポート
- 技術スタック
- クラウド資産・バケット
- 公開 URL

シャドーIT・未管理サブドメインまで。**毎日スキャン**し、翌日には新しい資産や開いたポートも検知します。

PRIORITIZATION

CVSSスコアだけで、並べない

見つかる脆弱性は毎週数百件になりえます。全部には手が回らない。PentaTrail は2段階で並べます。まず深刻度（CVSS）・悪用確率（EPSS）・検出根拠の確かさ（エビデンスグレード）から**脅威ディスカバリレベル**を算出。これに業務影響（BI）を掛けて**脅威エクスポージャーリスク**を出し、「まず直すべき順」を示します。

TDL **脅威ディスカバリレベル**

深刻度（CVSS）× 悪用確率（EPSS）× 検出根拠の確かさ（エビデンスグレード）。悪用実績（KEV）で補正し、技術的な脅威の高さを 1〜5 で表します。

エビデンス **エビデンスグレード**

A＝検証済み / B＝直接テスト / C＝CPEマッチ / D＝バックポート疑い。推測ではなく、検出根拠の確かさで危険度を上げ下げします。

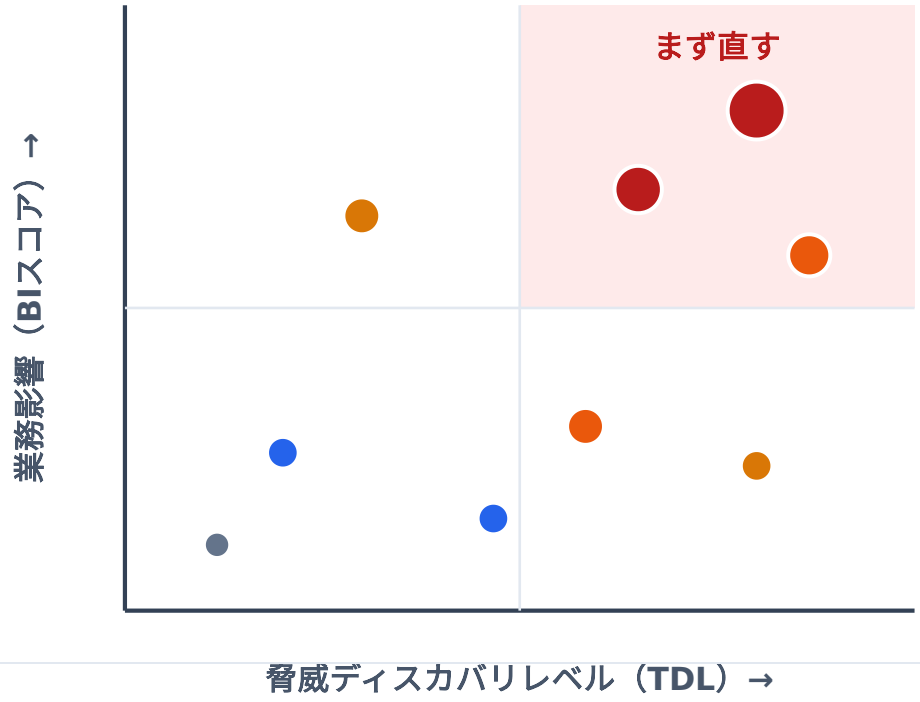
業務影響 **BIスコア**

用途・データ種別・可用性で資産の重みを算定。決済システムとテスト環境では、同じ脆弱性でも重みが変わります。

脅威ディスカバリレベル × 業務影響 ＝ 脅威エクスポージャーリスク → S〜D の5バンド:

S	A	B	C	D
緊急	高	中	低	情報

脅威エクスポージャーリスク ＝ 脅威ディスカバリレベル（TDL）× 業務影響（BI）



同じCVSSでも、決済システムとテスト環境では優先度が変わる。

VALIDATION ／ 実証

「見つかった」で終わらせない ── 本当に悪用できるかを AI が実証する

CVSS の理論値だけでは、実際に危ないかは分かりません。AIディープスキャンが、脆弱性候補ごとに検証コードを自動生成して非破壊でテストし、攻撃が"成立するか"を確かめます。

AIが検証コードを自動生成

CVEごとにAIが実証コードを生成し、対象ホストに安全な方法でテストします。

非破壊で実証

DNS検証で所有を証明したドメインに限定。システムに影響する操作は一切採用していません。

攻撃"成立／未成立"を確定

理論値ではなく、実際に攻撃が成立するかで判断。危険度の裏付けになります。

誤検知を減らす

"本当に危ないもの"だけに、限られた対処リソースを集中できます。

MOBILIZATION ／ 対処

見つけて終わりにしない ── AIが「どう直すか」まで示す

脆弱性を見つけて放置しない。AIが脆弱性ごとに対処方針を生成し、対応状況を追跡、PDFで配布まで。少人数のチームでも、直しきれます。

AIが対処方針を生成

脆弱性ごとに「影響・対処方針・暫定緩和策」を自動生成。何を、どの順で直すかが分かります。

属人化しない運用

担当者のスキルや異動に左右されず、一定品質のガイダンスを常に得られます。

PDFでそのまま配布

現場の担当者にも経営にも、ワンクリックで共有できます。

対応状況を追跡

未対応 → 対応中 → 対応済みを台帳で管理し、やり残しを防ぎます。

MCP で連携

承認した外部ツール（AIエージェント）から攻撃面データを直接読み書きできます。

実際の AI対処ガイダンス ── 脆弱性ごとに影響・対処方針・暫定緩和策を生成し、対応状況を追跡。ワンクリックで PDF 化。

EXECUTIVE REPORTING

経営の「3つの問い」に、数字で答える

取締役会がセキュリティ責任者に問うのは、突き詰めると3つ。PentaTrail は、そのどれにも一枚のダッシュボードで答えます。

1. **我々は安全か？**
   セキュリティスコア（400点満点）と危険度分布で、いまの態勢を示す
2. **改善しているか？**
   スコアトレンド（前回比）で、取り組みの成果を追跡
3. **新しい脅威は？**
   変更検知（新規資産・開放ポート）で、直近の変化を捉える

> 業務影響度別の脅威分布まで示せるので、セキュリティ投資のROIを定量的に説明できます。

実際の経営ダッシュボード ── セキュリティスコア・脅威エクスポージャーリスク・危険度分布（S〜D）・AIによるCISO向けインサイトを一枚で。

USE CASES

あらゆるシーンで、攻撃面を管理

外部攻撃面の継続監視から、M&A デューデリ・取引先評価への対応まで。少人数のチームでも、継続的に回せます。

外部攻撃面の継続監視
シャドーIT・未管理サブドメインを自動発見し、変化を追跡

クラウド露出チェック
AWS/GCP/Azure の公開バケットや意図しない公開リソースを検出

M&A デューデリジェンス
買収先の外部資産を1枚のスコアレポートで経営層に提示

少人数セキュリティ運用の補完
1人情シスでも、継続的な攻撃面管理を回せる

取引先セキュリティ評価への対応
取引先評価制度（SCS）など高まる要求に、自社の外部露出を客観的な証跡で提示

→ これらすべてを、**1つの契約で。** ドメイン3つ・5ユーザー込み（サブドメイン無制限）、追加費用はかかりません。

PRICING

シンプルな2プラン ── 含まれる機能で選ぶ

	ASM ¥40,000 /月 見つけて、監視して、危険な順に並べる	CTEM ¥68,000 /月 実際に確かめ、直しきって、経営に見せる
外部資産の自動発見 Discovery	✓	✓
日次スキャン・変更検知 Monitoring	✓	✓
危険度づけ（KEV / EPSS / BI） Prioritization	✓	✓
AI 対処ガイダンスの閲覧 Mobilization	✓	✓
脆弱性の実証（Validation） Validation	—	✓
対処タスクの運用・追跡 Mobilization	—	✓
経営報告レポート（スコア・トレンド） Reporting	—	✓
MCP 連携	✓	✓
共通：ドメイン3つ・5ユーザー込み（サブドメイン無制限）	✓	✓

表示価格はすべて税抜・月額です。攻撃面が広い会社ほど、1資産あたりの負担は軽くなります。

COMPANY

会社紹介

会社名	株式会社ペンタコン研究所（Pentacon Research, Inc.）
代表取締役	平舘 一哉
設立	2026年2月
資本金	1,000万円
本店所在地	東京都中央区日本橋茅場町二丁目17番6号
事業内容	1. 情報セキュリティ分野における SaaS の企画・開発・提供 2. 情報セキュリティ分野における調査・分析・コンサルティング 3. 情報システム・クラウド・AI 関連技術の研究開発

代表取締役 ／ CEO

平舘 一哉　Kazuya Hiradate

野村総合研究所入社後、NRIセキュアで 20年以上 サイバーセキュリティ事業に従事。マネージドセキュリティサービス事業やコーポレートセキュリティ管理部門で部長を歴任。その事業開発およびガバナンスの知見を、AI駆動開発の設計思想として PentaTrail に実装しています。

MISSION ／ 使命

見えないリスクに気づける力を、すべての組織に。

AI駆動開発による徹底した省力化と、コーポレートセキュリティの実務経験に裏打ちされた技術力で、続けられるセキュリティを届けます。

VISION ／ 目指す姿

セキュリティが空気のように溶け込む社会へ。

誰もがセキュリティを意識せずとも、サイバー空間の安全を享受できる世界を実現します。

GET STARTED

まずは自社の攻撃面を、外から確かめる

最短5分で登録でき、数時間で初回の攻撃面が見えます。

登録 5分 → **自動発見** 数時間 → **確認** その場で可視化

無料で試す | pentatrail.co/ctem

スマホで読み取る

14日間、無料。 AIネイティブの CTEM / ASM プラットフォーム