# Webサイト攻撃状況レポートサービス＆高PV安定化-インフラレッドのソリューション

2026年

# インフラレッド合同会社 会社概要

代表社員　加藤晋平

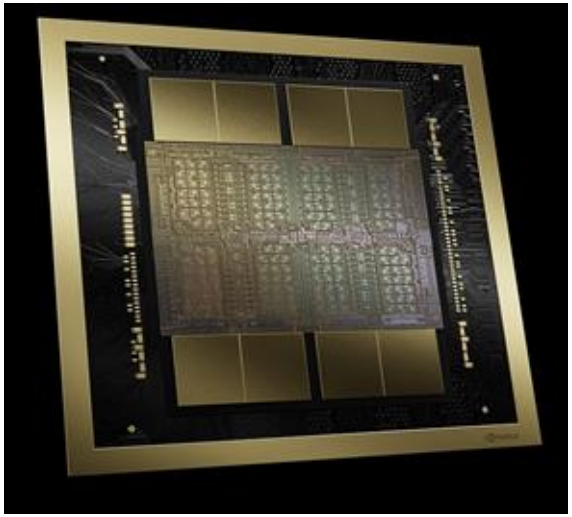
設立　2015年（創業2012年）

住所　福岡県福岡市

業務内容　海外IT製品の販売、技術支援、サイト構築支援、コンサルティング

**Webサイト攻撃状況レポートサービス**

New



nvidia blackwellプラットフォーム

# AIによる攻撃発見レポートサービス「ミツケル」

- お客様のログは全てインハウスのAIスーパーコンピュータにて解析
- クラウドAIを使わないため情報流出の恐れが最小
- サンプリングではなく全ログを調査する精査が可能
- 独自の複数モデルによる合議制で高精度の検出と読みやすいレポートを実現

ミツケル

Claude Mythos
フロンティアAI

# 攻撃状況　VS　脆弱性・防御側

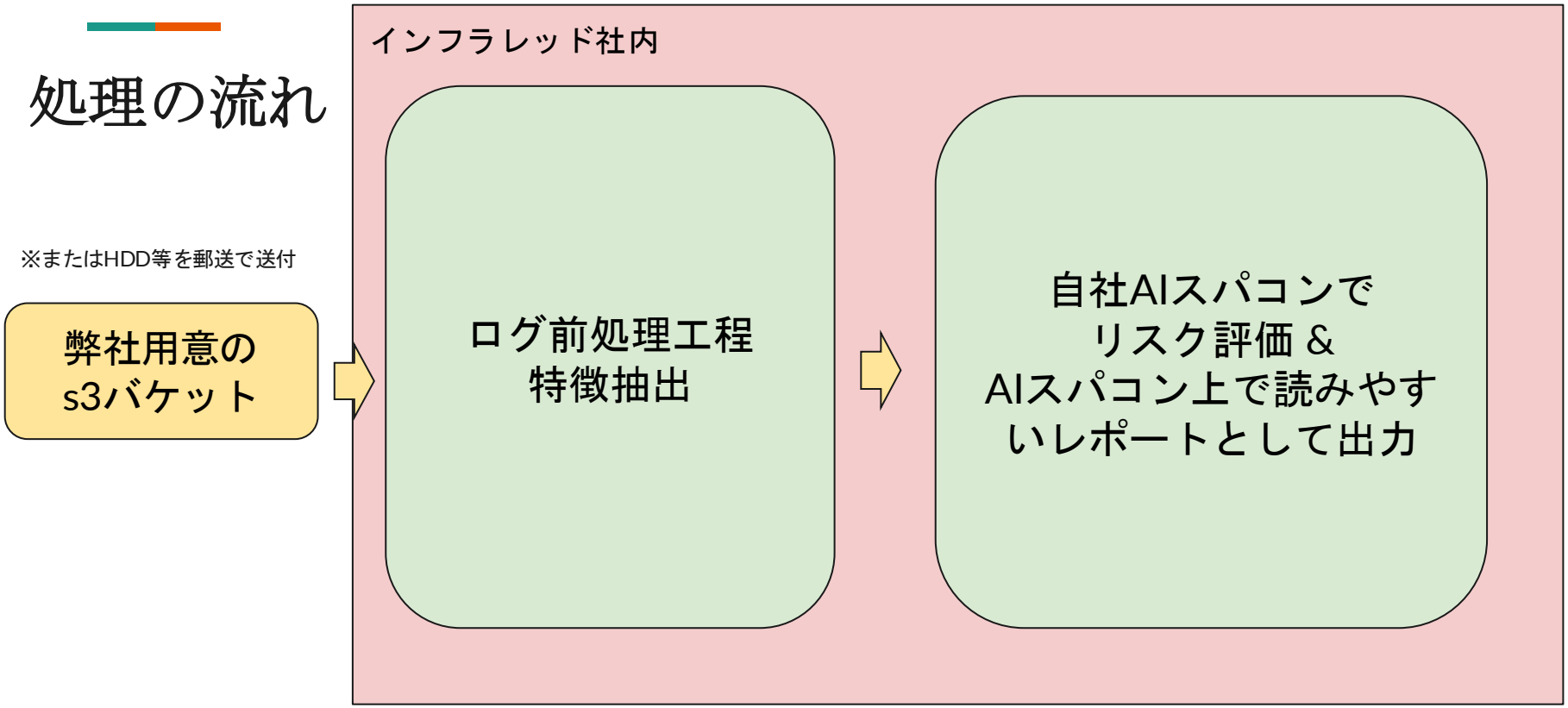
※脆弱性検査は進んでいるけど、
　そもそも今来ている攻撃の状況ってつかめてないですよね？

# レポート

- アクセスログを戴き（1週間から1ヶ月程度）、どのような攻撃がされているか、WAFが入っている場合にはそれでの打ち漏らしがどのようにあるかをレポート
  - 対策例の提示も（可能な場合）
- 3営業日程度でメールにてご報告
- ログ中のIPやJA4等のパターンを追いかけることで高精度な分析を可能にしている
- 現在はWebアクセスに特化しているが、リバースプロキシログやIoTログ等にて一般のWebアクセス以外の攻撃検出も原理的に可能

# 処理の流れ

※またはHDD等を郵送で送付



# サンプル


月次セキュリティ戦況レポート
対象: 匿名顧客　2026年3月　｜　ボット・攻撃アクセスの可視化と「次の一手」
① 安全度
② 攻撃は通った？
③ ボット負荷
④ 守りは大丈夫？
⑤ 何からやる？
▼ 実測データ
▼ 注目IP
— サマリー（前半2ページ） —
サイトのセキュリティ、今月どうだった？
今月の総合判定：警戒
月間 14,263,357 件 のアクセスを処理し、1,170,507
撃試行が確認されており、防御強化が必要です。
安全スコア
1
悪性IPおよ
脅威情報に
2
オリジンサ
WAF未導入
3
ボットおよ
既知の悪性ボ
40 / 100
40-59点: 警戒要
中リスク
※スコアは0〜100で表し、低いほど対処が必要
なことを示します
① 危険な攻撃は、サーバーまで通った？
攻撃アクセスのうち 約41.1%（10,222 件） がサーバーまで到達 — 現時点で情報漏洩は未確認
攻撃と分類されたリクエスト 24,855 件 のうち、入口の遮断を通り抜けてサーバーまで到達（200応答）した件数が 10,222 件 (約41.1%)、入口での遮断は 366 件、その他の応答（3xx/4xx/5xx 等の非200）は 14,267 件です。 下図は攻撃総数 24,855 件を内訳に分解したもので、到達率（約41.1%）の分母も同じ攻撃総数です。 応答サイズから空ページと推定されるものを含むが、応答本文は未取得のため漏洩の有無は未確定（要追加調査）。
き先（合計＝攻撃総数 24,855件）
14,267件
0
10,000
20,000
30,000
件数
入口で遮断
その他応答（非200: 3xx/4xx/5xx等）
サーバーまで到達（200応答）
漏洩確認
判定の限界：到達先の応答本文は未取得のため、空ページか否か・漏洩の有無はいずれも未確定（要追加調査）。
到達の多かったパス（上位3件）
パス
200応答件数
判定
/catalogsearch/advanced/result/
1,542
本文未取得・要確認
/page_cache/block/render/
900
空ページ判定
/catalogsearch/advanced/
684
本文未取得・要確認
全パス一覧 → 詳細1へ

— 詳細データ —

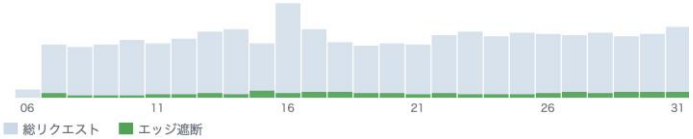
実測データ / CDN/WAFログ直接集計

## 月間トラフィック実績

このセクションの数値はCDN/WAFアクセスログから直接取得した確定値です。

| 月間総アクセス | エッジ遮断 | サーバー到達(200) | ユニーク IP |
|---|---|---|---|
| 14,263,357 | 1,170,507 | 10,635,160 | 41,267 |
| 件 | 遮断率 8.21% | 件 | 件 |

### 日次アクセス推移（CDN/WAFログ実測）




### 時間帯別アクセス分布（CDN/WAFログ実測・UTC）


時刻は UTC。深夜帯（UTC 22-04 時 = JST 07-13 時）の突出は帯域・地域の問題を示す場合あり。

### ボット分類内訳（ボット分類分析・実測値）

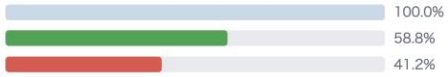
| 分類 | 割合（全リクエスト比） |
|---|---|
| 不審・未分類ボット | 38.3% |
| AI クローラ | 0.9% |
| 正規クローラ | 1.3% |

詳細6 / 攻撃パス実績

## 攻撃パス月次実績

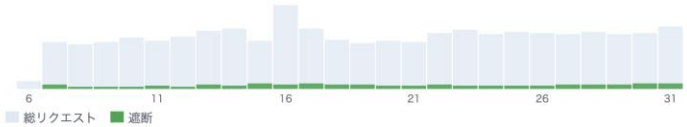
攻撃パス（インジェクション・認証試行・機密パス等）へのアクセスが遮断されたか、サーバーに到達したかを集計（CDN/WAFログ実測値）。

| 24,797 | 14,575 | 10,222 | 41.2% |
|---|---|---|---|
| 攻撃パスアクセス総数 | 遮断・その他（200以外） | サーバー到達（200） | 通過率 |




### 全トラフィック日次推移（参考）（ピーク日: 16, 31日）

下図は全リクエストの日次傾向（参考値）。




↑ フロント② 攻撃は通ったか に戻る

# 数億件のログを、AIが段階的に絞り込む

**生ログ** — 数億件
CDN / WAF から取得したアクセスログ

**何が起きているか**
リクエスト数・エラー率・帯域の統計集計

**正常に見えるが異常**
ベースラインとの乖離・協調ボット群の検出

**どのように異常か**
異常の種別・強度を分類し悪性 IP をスコアリング

**異常な IP は何者か** — 審問 5,500 回
異常なIPを AI が多角的に審問
（最大 500 件 × 11 回）

**だから何をすべきか** — 調査〜統合 多段
8 人の専門家 AI が調査・査読・統合し提言を生成
最大約4500回

**レポート** — 1 本
経営層・担当者向けの日本語レポート

全件を読んだ上で
絞り込み
AI専門家が調査する

1 レポートあたり
**約10,000**
**回の推論**

# 1 つの不審 IP を、3 種の AI が異なる問いで審問する

## 防御視点 専門家

脅威の検知・防御視点で分析

防御

**問い 1**
いつ、活動しているのか？

**問い 2**
何を取得しようとしたか？

**問い 3**
人間か、ボットか？どんな意図を持つか？

→

## 攻撃視点 専門家

攻撃者視点で侵害経路を推定

攻撃

**問い 1**
いつ、攻撃をしてきたか？

**問い 2**
どの脆弱性を狙ったか？

**問い 3**
どんな手口・ツールを使ったか？

**問い 4**
何を目的として攻撃しているか？

→

## 見解の要約

反論・検証して最終判定を下す

統合

**問い 1**
本当にそう言えるか？反証はないか？

**問い 2**
証拠と矛盾していないか？

**問い 3**
総合的に見て、何者と判定できるか？

**問い 4**
この結論を顧客にどう伝えるか？

1 IP あたり
**11**
**問い**

最大で
**5,500**
回の審問

# 8 人の専門家 AI が独立した視点で調査し、査読・統合する

## 調査 — 5 スペシャリスト

**脅威ハンター**
危険な攻撃は実際に通ったか

**フォレンジック調査官**
攻撃者は誰か・どこからか

**ボット解析官**
ボットに何をどれだけ抜かれたか

**脅威インテリジェンス分析官**
既知の脅威 IP が通ったか

**セキュリティ評価官**
WAF のどこが抜けたか

AI専門家
**8**

▼ 所見を受け取る

## 査読 — 2 専門家

**レッドチーム**
5 専門家の所見に
反論・矛盾点を突く

**ファクトチェッカー**
数値・分類の横断検証

最大で
**4,500**
回の審問

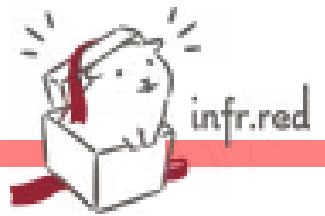
▼ 全知見を集約

## 統合 — 主席セキュリティアナリスト

**主席セキュリティアナリスト**
7 専門家の結論を統合し、
日本語レポートを生成

→ 日本語レポート

1 レポートあたり
**約10,000**
**回の推論**



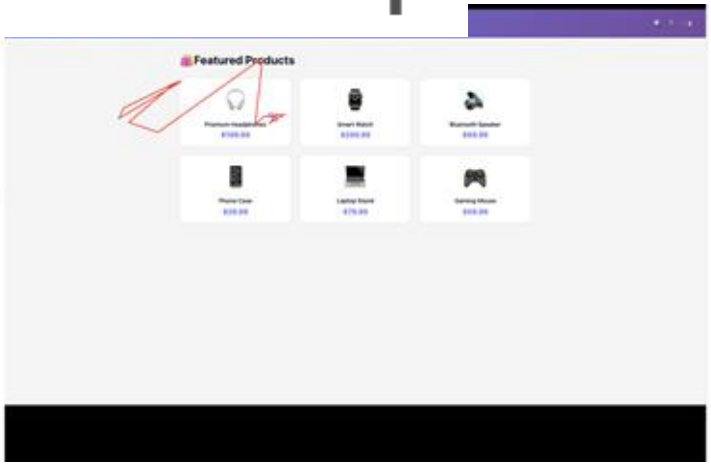
fastly

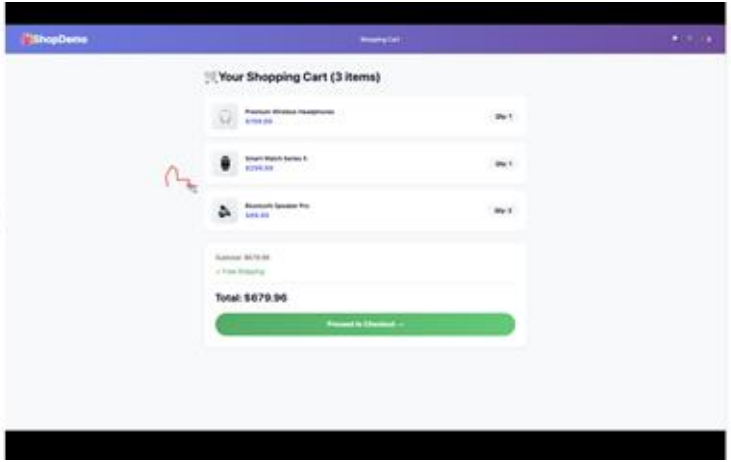
ファストリー、本日他のコマでご案内

# その他弊社のソリューション

WhaTap

顧客のブラウザ表示をプレイバックできる
「セッションリプレイ」機能を安価に提供



# 代表者紹介

加藤晋平

名古屋市出身、福岡市在住

2000年代前半はNW、サーバエンジニアとして活動、
その後EC構築、運用の領域に転身。
2012年インフラレッド創業（2015年法人化）

NWのバックグラウンドにより、
お客様体験の向上にNWやインフラがどう貢献できるか
を中心に考えている。