Takumi
by GMO

紹介・デモ ウェビナー

脆弱性診断とペネトレーションテスト
「AIでやる」リアルな運用やコストを解説



8.18（火）
12:00-13:00@online

Speaker
執行役員 豊田 恵二郎



豊田 恵二郎 @toyojuni

- GMO Flatt Security(株) 執行役員CCO / 共同創業者
- 東京大学工学部航空宇宙工学科卒
- 3人と3台で暮らしてます

開発・提供

GMO Flatt Security

バグハント × AI開発
世界トップクラスの
エンジニア集団

防衛省サイバーコンテスト(2023-2025) **3連覇**

Ubuntuへの脆弱性報告報奨金(単一の脆弱性) **$30,000**

その他脆弱性報告先実績
Google, Cloudflare, GitHub,
Salesforce, Microsoft, Meta

Canonical
at home
SBI DigiTrust
NTT DATA 株式会社NTTデータユニバーシティ
en
GLORY
CyberAgent
Cygames
SmartHR
Timee
TIER IV
TOKYO GAS
TREND MICRO
NIKKEI
PKSHA COMMUNICATION
pixiv
freee
Findy
FINATEXT HOLDINGS
Preferred Networks
MIZUHO みずほリサーチ&テクノロジーズ
MITSUI & CO. DIGITAL ASSET MANAGEMENT
MITSUBISHI ELECTRIC Changes for the Better 三菱電機インフォメーションシステムズ株式会社
LayerX

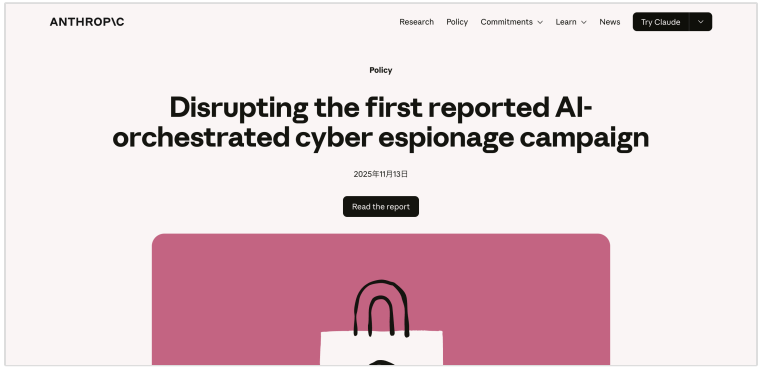
CHAPTER 01

はじめに

AIの進化が、攻撃側と守備側の前提を変えている

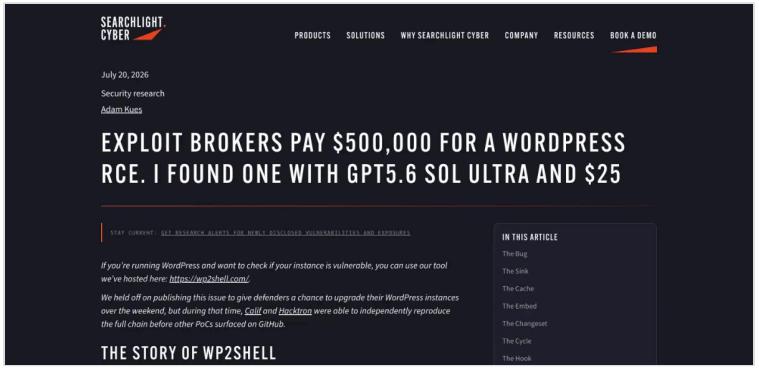
昨今、AIによる脅威はますます大きく、リアルなものに

25/11時点ですでに、Claude Codeを利用した攻撃が明るみに



出典：https://www.anthropic.com/news/disrupting-AI-espionage

GPT-5.6 Solによる WordPressの認証前RCE脆弱性発見



出典：https://slcyber.io/research-center/wp2shell-pre-authentication-rce-in-wordpress-core ／ https://slcyber.io/research-center/exploit-brokers-pay-500000-for-a-wordpress-rce-i-found-one-with-gpt5-6

大前提：攻撃者にも経済の力学が存在する

変わらないこと

攻撃者の狙いは依然として「金銭」「名誉」「情報」

- 高能力モデルの登場そのものは、攻撃の動機を増やさない
- 切れ味のよい包丁が出たから傷害事件が増える、は成立しない

変わること

攻撃が「割に合う」対象が増える

- 攻撃に必要な人件費・スキル下限・時間が下がる
- 従来は手間が勝り攻撃に値しなかった対象も、攻撃が合理的になる
- ユニットエコノミクスが成立する攻撃対象が自然と増える

結果として、狙われる対象の広がりと攻撃頻度の向上が起こりうる

攻撃者に起きたユニットエコノミクスの変化

	Before AI	AI時代では
コスト	人件費相当の費用がかかる	**低コスト**で攻撃できる
速度	人間が律速	**高速・高頻度**に攻撃できる
スキル下限	複雑な攻撃の実行には 相応のスキルを持った人材が必要	**誰でも複雑な攻撃**を実行できる

攻撃側がAIで加速・拡大する以上、
守り側も対策の高速化・高品質化が必須。

従来の手法では、AI時代の攻撃に対処しきれない

速度

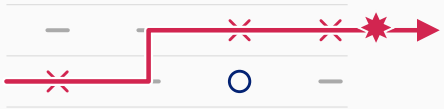
人手による診断では頻度が著しく低い



外部ベンダーのセキュリティエンジニアによる診断では、実施頻度が年に一度程度にとどまります。社内の専門家がこの分野に継続的にコミットすることも現実的ではありません。

精度

非LLMツールでは検知できる項目に限界がある



非LLMのツールは総当たりやパターンマッチ的な検知にとどまり、AIが対象の仕様やレスポンスに応じて実行する適応的な攻撃には及びません。結果、認証・認可をはじめとする重要部分に脆弱性が生じ得ます。

AI時代もプロダクトを守り抜くには

AIを使って
セキュリティ対策を内製化すべき



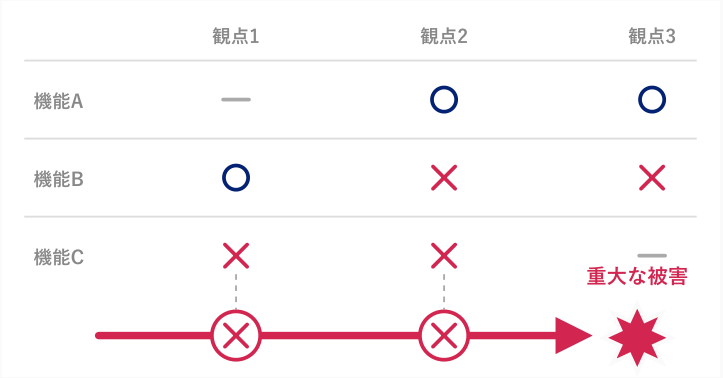
GMO Flatt Security

脆弱性診断

	観点1	観点2	観点3
機能A	○	○	○
機能B	○	×	×
機能C	×	×	○

- 定義した項目に沿って脆弱性がないか調べる
- システムの**機能・弱点が網羅的**にわかる

ペネトレーションテスト



- 実際にどこまで深く侵入できるか試す
- 起こりうる**実被害**と**事業インパクト**の最大値がわかる

脆弱性診断・ペネトレーションテストは AIによって安く、速く、高精度に

費用

数百万円 から

→ 数万円 に

従来の手法に比べ、AI利用では1回あたりの費用が格段に抑えられる

速度

数ヶ月 から

→ 数日 に

スタートから完了までの時間が大幅に短縮され、高頻度で実施できるように

精度

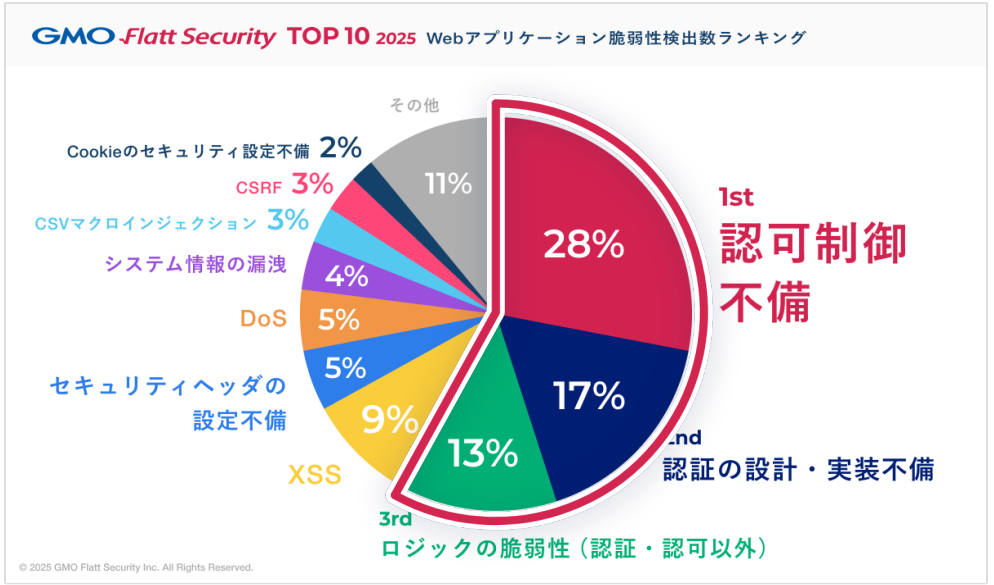
昨今のモデルでは

人間レベル に

脆弱性の検出水準が人間に等しいレベルに到達し、より実用しやすく

「人間レベルの精度」＝ アプリケーションの仕様を理解してロジックの脆弱性を検出できる水準

- 弊社の脆弱性検出数ランキングでも、OWASP Top 10 2025でもロジックの脆弱性は**1位**
- 従来、ロジックの脆弱性は人間でないと見つけられなかった（非LLMのDAST/SASTでは検出不可能）。
- Takumiはこのロジックの脆弱性を**検出できる**

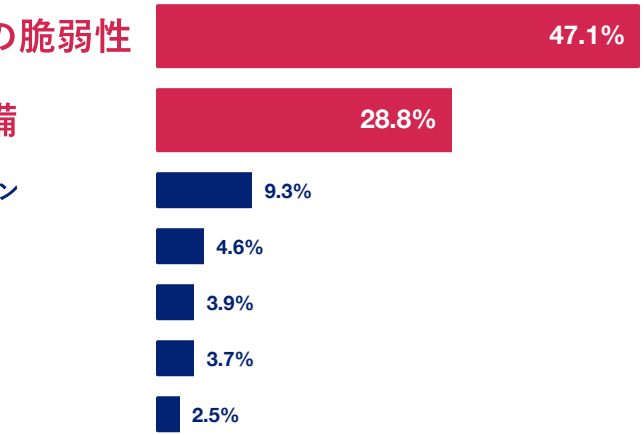


画像出典：GMO Flatt Security「Webアプリケーション脆弱性検出数ランキング TOP10 2025」https://blog.flatt.tech/entry/flatt_top10_2025

Takumiが検出する多くは、ロジックの脆弱性・認可の不備

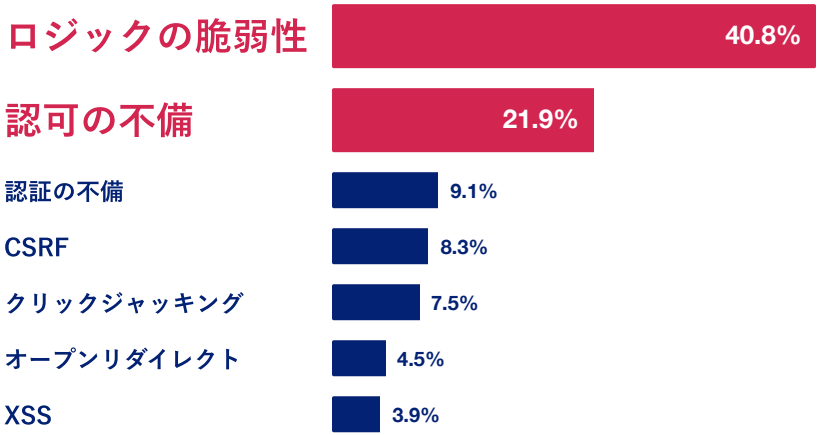


ホワイトボックス診断





ブラックボックス診断



2026年5月29日～2026年8月4日時点での集計。同一対象の複数回実行を含む延べ件数。

CHAPTER 02

Takumiの紹介

主な機能と強み

GMO Flatt Security

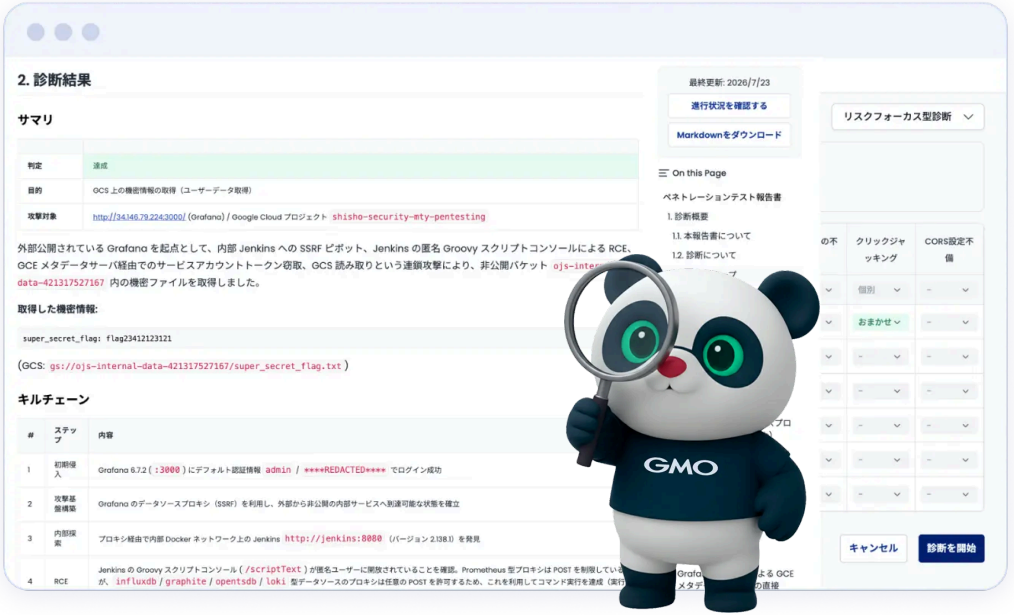
Takumiはこれまでにも数多くの脆弱性を検知

診断件数

800件以上

見つけた脆弱性の数

12,000件以上



診断・ペネトレーションテスト・ソフトウェアサプライチェーン対策を提供中



ホワイト/ブラックボックス診断

SAST/DASTで脆弱性を検出



脆弱性の自動修正

検出した脆弱性の修正パッチを自動生成



AI ペネトレーションテスト

ペネトレーションテストを自律的に実施



Takumi Runner

CI/CDワークフローの動作を可視化する実行基盤



Takumi Guard

悪性パッケージを検知してブロック



Takumi Images

既知脆弱性・マルウェア最小化コンテナイメージ

診断・ペネトレーションテスト・ソフトウェアサプライチェーン対策を提供中



ホワイト/ブラックボックス診断

SAST/DASTで脆弱性を検出



脆弱性の自動修正

検出した脆弱性の修正パッチを自動生成



AI ペネトレーションテスト

ペネトレーションテストを自律的に実施



Takumi Runner

CI/CDワークフローの動作を可視化する実行基盤



Takumi Guard

悪性パッケージを検知してブロック



Takumi Images

既知脆弱性・マルウェア最小化コンテナイメージ

セキュリティ診断機能：ホワイト / ブラックボックス診断から選択
修正まで一貫して対応可能



ホワイトボックス診断

ソースコードを静的に解析し
脆弱性を検出

- GitHub連携 or コードのアップロード
- 潜在リスクまで網羅的に洗い出す



ブラックボックス診断

実環境を動的に試し
脆弱性を検証

- URLとログイン情報を入力するだけ
- 実際に再現可能なリスクを検出



AIによる自動修正

パッチ / Pull Requestを
作成し脆弱性を修正

- 診断結果をふまえた修正タスクを作成
- GitHubにPull Requestも自動作成

本日提供開始



https://shisho.dev/docs/ja/r/202608-takumi-graybox

AIペネトレーションテスト機能：
起こりうる実被害と事業インパクトを明らかに

AIペネトレーションテスト

攻撃対象と達成したいゴールを設定すると
自律的に疑似攻撃を試みる



- 「機密情報の取得」「システムへの侵入」等をゴールに設定
- 攻撃の到達点を示すタイムライン、侵入マップ、レポートを出力

AIペネトレーションテスト機能は順次開放中です。利用開始の通知は右記より登録いただけます。 https://flatt.tech/takumi/features/pentesting

CHAPTER 03

Takumiの運用イメージ

導入事例と、実際の画面デモ

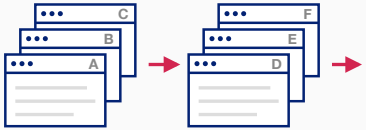
Takumiの運用事例

リリース前 / 年次診断の代わりのフルスキャン



リリース前や年次の診断など、重要なタイミングで**アプリケーション全体**を対象に検査。

リスクフォーカス型で複数プロダクトを定期診断



クレジット消費を調整しながら、**複数の製品**を優先度ベースで定期的にチェックする。

週次のcron実行で脆弱性をチェック



毎週の開発差分に対して自動で診断を実行。新たに混入した**脆弱性を継続的にチェック**する。

ホワイトボックス／ブラックボックス／グレーボックス診断の使い分け

ホワイトボックス診断



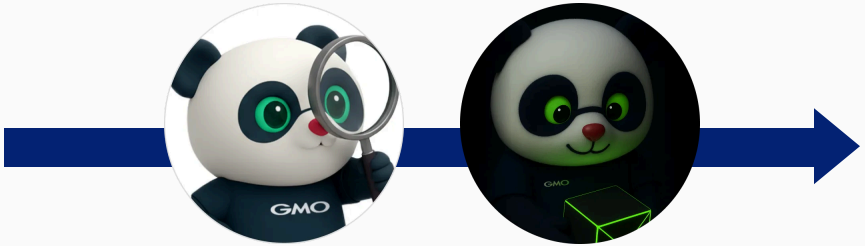
ソースコードがあれば診断可能

ブラックボックス診断



実環境があれば診断可能

グレーボックス診断



網羅的に
リスクを検出

悪用可能か
実環境で判定

- **ソースコード**・**実環境**の両方がそろっていれば診断可能
- 高い検出率と低い誤検知率を両立

クロール機能

対象アプリケーションをAIが自動巡回して画面や機能を把握。
診断対象となる機能を洗い出す。

機能 × 診断観点の一覧をマトリクス表示



リスクフォーカス機能

AIが各項目の優先度をチェックして、**優先度が高い項目**から診断。
クレジットの利用上限も指定できる。



デモ：診断・自動修正







きちんと時間をかけるからこそ
高精度のセキュリティ診断ができる



- 1回あたり**数時間**をかける
- 人間レベルの深い診断を実現

→ 重たい検査と軽い検査は違う。
使い所の見極めが重要

Q Takumiは開発フローのどこに入れるべき？

A 従来の脆弱性診断と同じくリリース前のゲートに向いている

軽くて速いレビューが必要。
小回りの効くエージェント等
が向いている

「世の中に出してOKか」
の門番になれる検査が必要。
Takumiがマッチしやすい

1. 要件を決める → 2. つくる・変える → 3. テストする → 4. 出荷し運用する



APIを用いて定期実行・自動化もできる

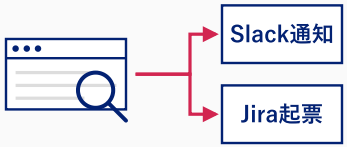
API機能で診断の実行・結果の取得を呼び出し、開発ライフサイクルに自由に組み込める。

CI/CDパイプラインに組み込んで自動実行



ステージング環境へのデプロイ後に**ブラックボックス診断を自動実行**するなど、パイプラインの一部に。

診断結果をふまえて後続処理を自動で進める



検出された脆弱性を**Slackへの通知やJiraへの起票**など、既存のワークフローに自動連携。

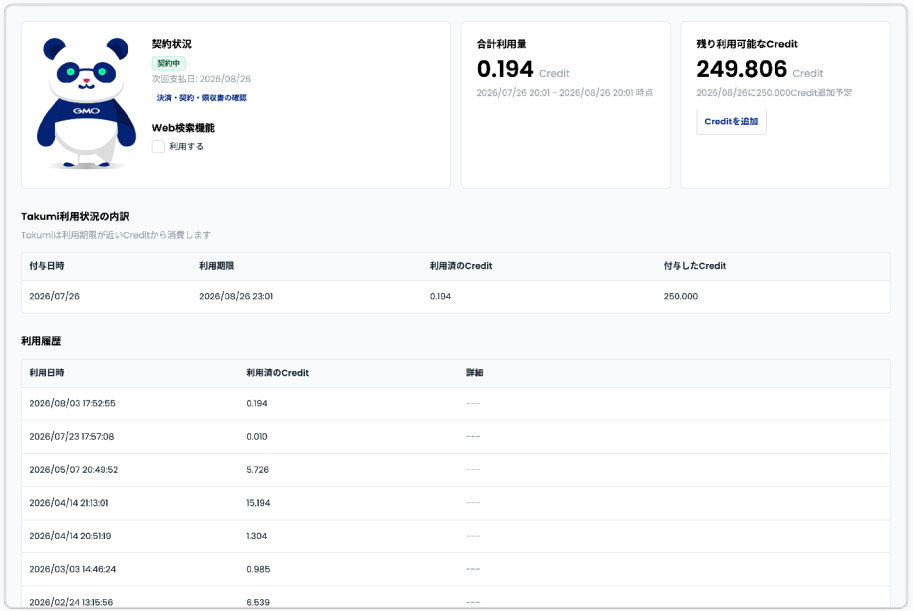
CHAPTER 04

Takumiの料金

月額制とクレジット消費の考え方

Takumiは月額プラン制

- **月額制** かつ **クレジット消費制**
- 上限を超えたら、
  クレジットの追加購入も可能
- 支払い方法はクレジットカード／
  請求書払いに対応



GMO Flatt Security

基本プラン

7万円 /月

＋

250 クレジット/月 付与

- Takumi Guard 15組織トークン
- Takumi Runner 実行時間 3,000分

＋

追加クレジット

280円 / 1クレジット

（ ＝ 基本料金と同じレート）

クレジットを消費して診断・修正等を行う



クレジット消費の利用イメージ

「機能 × 観点」の組み合わせ1セルあたり、おおよそ以下のクレジットを消費する（あくまで目安）。

診断の種類	消費クレジット（1セルあたり）
ブラックボックス診断	5〜8クレジット
ホワイトボックス診断	1〜3クレジット

- 対象機能の規模や、診断中にTakumiが発見した手がかりの数によって変動する
- クレジットの利用上限を指定することも可能（リスクフォーカス機能）

CHAPTER 05

コーディングエージェントとの比較

Takumiならではの利便性とは？

内製では構築コストが大きすぎる実装を、Takumiを通じて提供

網羅性

当社が規定する**診断項目に沿って**、抜け漏れなく網羅的に診断できる

安定性

ブラックボックス診断のような動的なチェックも安定して回る

モデル・ハーネスの最新性

最新モデルの追随やハーネス改善を当社セキュリティエンジニアが実施。**利用者様側での保守は不要**

ツールの準備

必要なツールが揃っており、手作業でのインストールが不要

コストの見通し

クレジット制で**消費金額を予測・制御**できる。トークン課金のように青天井にならない

安全性

サンドボックス環境で診断するため、安全に実行できる

Anthropicと戦略的パートナーシップ契約を締結済み



2026.7.28

GMOインターネットグループ、 Anthropic と戦略的パートナーシップ契約を締結

GMOインターネットグループ
Anthropicと
戦略的パートナーシップ契約
を締結

GMO INTERNET GROUP

GMOインターネットグループ株式会社（代表取締役グループ代表：熊谷 正寿）は、米Anthropic PBC（以下、Anthropic）と、2026年7月10日（金）、戦略的パートナーシップ契約を締結いたしました。

本契約において、GMOインターネットグループは、広く世間に安心・安全なAIを搭載したサービスを提供すること、グループ全体でハイパーオートメーション企業グループになるためにClaudeを徹底的に活用するといった、グループ内外両面に向けたAI活用を進めてまいります。

出典：https://flatt.tech/news/20260728_press

Takumiは、
当社の実務で鍛えられている

GMO Flatt Securityの
脆弱性診断・ペネトレーションテストに実践投入しながら、
アップデートし続けています。



お手元のコーディングエージェントで試してみるのもアリです

どんな脆弱性がみつかる？

使用感は？

実務で取り入れられそう？

Q Takumiを「外部の第三者」として扱えますか？

品質評価そのものとは別に、脆弱性診断サービスには「お墨付き」の側面があると認識しています。顧客から「外部の第三者による評価を受けていること」というセキュリティ要件が課されるシーンも引き続きあります。お墨付きのために別途人間の診断を受けるべきでしょうか。

A コストメリットがある方をご選択いただけます

お客様のスタンスと外部要件によるため、どちらが良いということはありません。「お墨付き」が必要な際には、**プロフェッショナルサービスとして当社の診断で対応**することも可能です。

CHAPTER 06

Takumiの未来・まとめ

これから予定している機能追加と全体のまとめ

AIペネトレーションテストの全ユーザーへの開放

AIペネトレーションテストの提供をさらに拡大予定。脆弱性から起こりうる**実被害の検証**をより手軽に。



📣 利用開始の通知登録はこちら

https://flatt.tech/takumi/features/pentesting

本日のまとめ

1 AIで攻撃コストが下がった

「割に合う」対象が広がる一方、人手診断と非LLMツールでは追いつきません。

2 人間レベルの高度な検査を自動で

認証・認可・その他ロジックの脆弱性も検出できる診断を実行します。

3 リリース前のゲートとして使う

「重たい検査」なので使い所が肝要。クレジット上限指定で計画的に。

4 月額7万円で250クレジット

月額7万円で毎月250クレジット付与。不足分は都度同レートで追加可能。

5 専門家の実装を皆様に提供

網羅性・安定性・最新性..... 当社の診断実務で使い込みながら改善しています。

本ウェビナー参加者さまへのご案内

初月無料 ＋250クレジットを ご利用いただけます

14万円相当のトライアルをご利用いただけます。ぜひTakumiをお試しください。



9/2（水）渋谷で開催。ぜひご参加ください



https://flatt.connpass.com/event/393895/

次回ウェビナーもあります！



https://flatt.tech/takumi/event/ai-devsecops-202608