Spectrum Technology

V1.0 2026/10/26

抜粋版

サイバー攻撃対策　脆弱性診断ツール

～AIを活用した中小企業向け脆弱性診断、自動管理ツール～

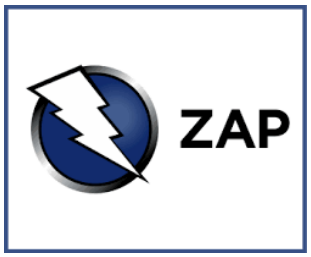
openvas/zap+make+geminiAPI











スペクトラム・テクノロジー株式会社

https://spectrum-tech.co.jp

sales1@spectrum-tech.co.jp



all rights reserved 2026 spectrum technology co.

Spectrum Technology

脆弱性診断ツール　目次

	ページ
• 脆弱性診断ツール　全体像	3
• ハード・ソフトウエア概要	
1. ハード概要	4
2. ソフト概要	5
3. ハードウエアの設定	6
1. Openvas	
① 概要	8
② 設定	9
③ 運用	11
④ 対策	28
2. Make	
① 概要	30
② アカウント設定	31
③ 設定：openvas自動化	32
④ テスト：openvas自動化	54
⑤ 本番運用	59
3. ZAP	
① 概要	61
② 設定、実施	62
③ 結果	64
4. 運用のポイント	66
免責事項	67

抜粋版のため、目次と本文はちがいます

all rights reserved 2026 spectrum technology co.

Spectrum Technology

脆弱性診断ツール　全体像

OS

ubuntu

vmware

ハードウエア

CPU

intel AMD

16GB RAM

gpu搭載が望ましい

＋

USBメモリ



通知関係

slack

脆弱性診断系

OpenVAS

Open Vulnerability Assessment Scanner

ZAP

自動管理系

make

Google Sheets

AI系

Gemini API

お客様準備

弊社提供

all rights reserved 2026 spectrum technology co.

Spectrum Technology

1. ハード概要

①. 必要なハードウエア仕様

品名		仕様	備考
USBメモリ（ubuntu版）		USB3.0　32GB openvas等プログラム一式	
USBメモリ（vmware版）		USB3.0　64GB Ubuntu22.04,openvas等プログラム一式	windows環境でも動作
必要なハードウエア：お客様準備			
PC本体	cpu	Intel i7 gen 7 AMD Ryzen 5	
	メモリ	16GB以上	
	Disk	256GB以上	vmwareの場合,50GB以上
	GPU	RTX4060以上	搭載が望ましい

all rights reserved 2026 spectrum technology co.

2. ソフト概要

提供するソフトウエアの概要です。

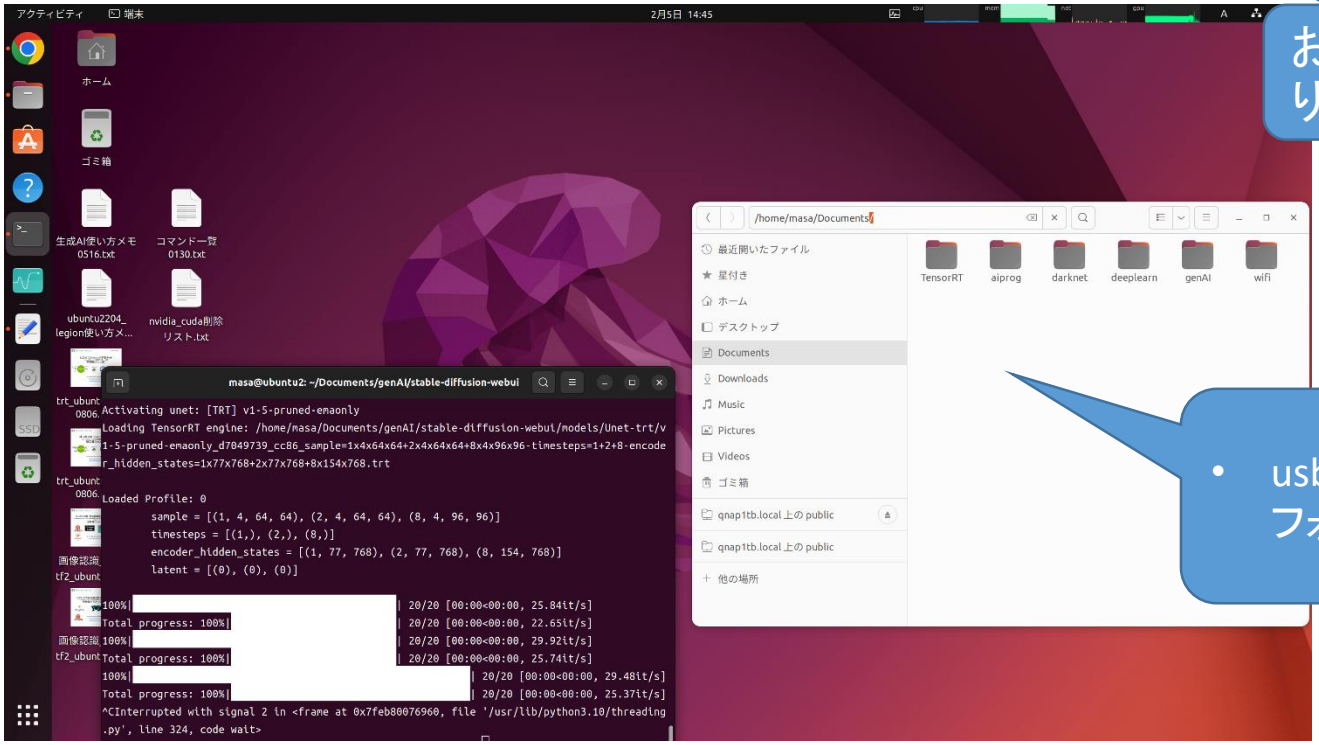
区分	ソフト名	バージョン	備考
OS	ubuntu	22.04以上	他のlinuxでも動作
仮想化	vmware	Workstation pro 25H2	window環境で動作、脆弱性診断ツールはプレインストール
脆弱性診断	openvas	25.0.8	ネットワーク、クライアント、サーバなど。dockerで動作
	zap	2.17.0	Webアプリ特化
自動管理	Make	ブラウザ	
	Gemini api	3.8 flash	診断結果の分析、対策立案:日本語化 他にclaudeなども利用可能
	Google sheet		診断結果、対策管理
通知	slack		通知

all rights reserved 2026 spectrum technology co.

3. ハードウエアの設定

① USBのデータ読込

- 添付のUSBのデータを読込ます。
- 例：cd /home/masa/Documents



お客様毎に異なります

- usbのデータを、Documentsフォルダにコピペ

all rights reserved 2025 spectrum technology co.

openvas

all rights reserved 2026 spectrum technology co.

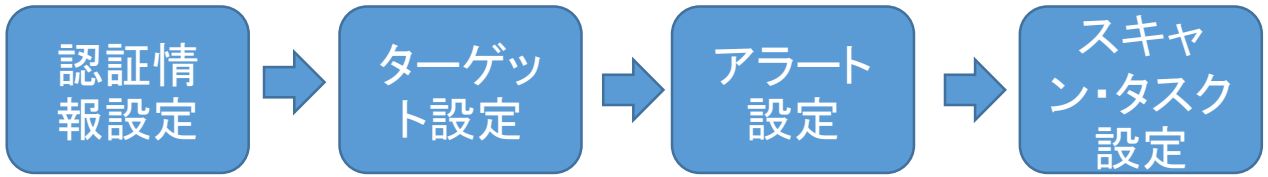
1.openvas
①概要

- openvasとは？
  - OpenVAS は、ネットワーク、サーバー、OS、ミドルウェアなどに存在する既知の脆弱性を網羅的にスキャン・診断し、一元管理するためのオープンソースの脆弱性管理プラットフォームです。定期的なシステム点検（健康診断）を行い、外部から攻撃される可能性のある「穴」を早期に発見・修復するために使用します。
  - https://openvas.org/
  - https://greenbone.github.io/docs/latest/index.html
- 特徴
  - 膨大な脆弱性データベース（NVT）
    - 数万件以上の脆弱性テスト項目（CVEや各種セキュリティアドバイザリに対応）を保有し、常に最新のシグネチャにアップデートされます。
  - 網羅的な自動スキャン
    - 単なるポートスキャンにとどまらず、稼働しているサービス、OSのバージョン、設定ミス、既知のバグを総合的にチェックします。
  - リスクの可視化とスコアリング（CVSS）
    - 発見された脆弱性を深刻度（CVSSスコアベース）に応じて分類・数値化し、どの脆弱性から優先して対策すべきかを分かりやすく提示します。
  - 豊富なレポート機能
    - 診断結果を PDF や XML、HTML などの形式で出力でき、インベントリ管理やセキュリティ監査の報告書としてそのまま活用できます。
  - 定期実行による継続的な監視
    - スキャンのスケジュール設定が可能なため、システム変更や新規アプリ追加に伴う新たな脆弱性の発生を継続的にモニタリングできます。
  - コストパフォーマンス：無償
    - 商用（有償）のエンタープライズ向け脆弱性スキャナーに匹敵する高度な機能を、オープンソースかつオンプレミス環境でコストを抑えて構築できます。

all rights reserved 2026 spectrum technology co.

1.openvas
③運用

- 起動
  - http://127.0.0.1:9392/
- スキャンフロー
  - 脆弱性のスキャンを実施するための全体のフロー
  - https://docs.greenbone.net/GSM-Manual/gos-25.0/en/
  - ネットワーク機器、サーバ、クライアントのフローは以下のとおり



ターゲットのログイン情報（ユーザ、パスワード）、詳細に分析するため

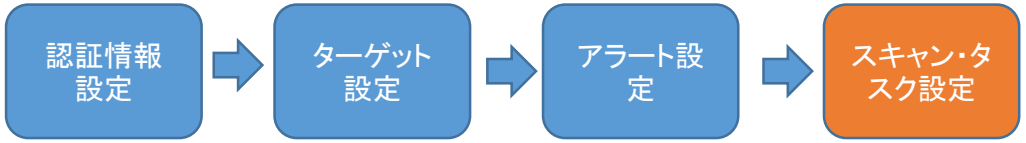
ターゲットのIPアドレス、ログイン情報

リスクの高い脆弱性が発見された場合、メール、CSVで出力。Makeでの自動化につながります

ターゲットを決めて、アラート、スケジュールなどを設定

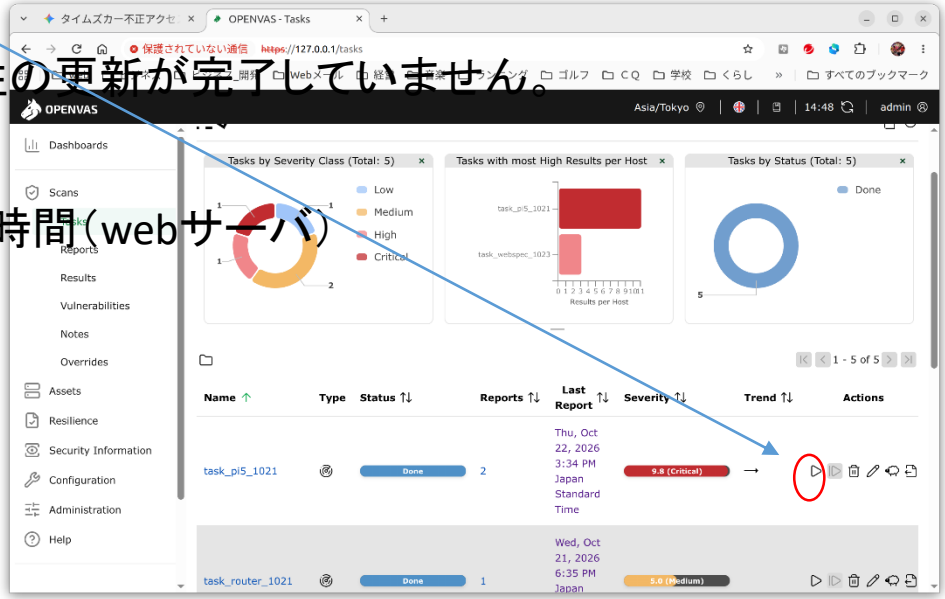
all rights reserved 2026 spectrum technology co.

1.openvas ③運用



- 起動
- スキャンフロー
- スキャン・タスク設定
- スキャン実施
  - Scan>task:該当タスク、実行ボタン
  - 実行ボタンがグレイの場合は、脆弱性の更新が完了していません。
  - こちらを確認してください。
  - 該当の機器によりますが、30分から2時間（webサーバ）

スキャンの実施頻度は、脆弱性の状況による。最初は、毎日でもよいが徐々に1週間に1回など頻度を変更

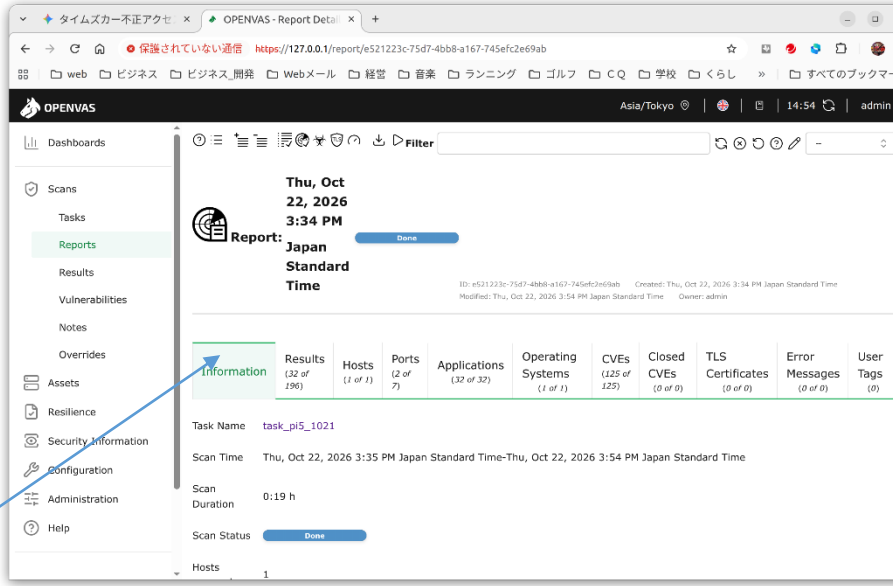


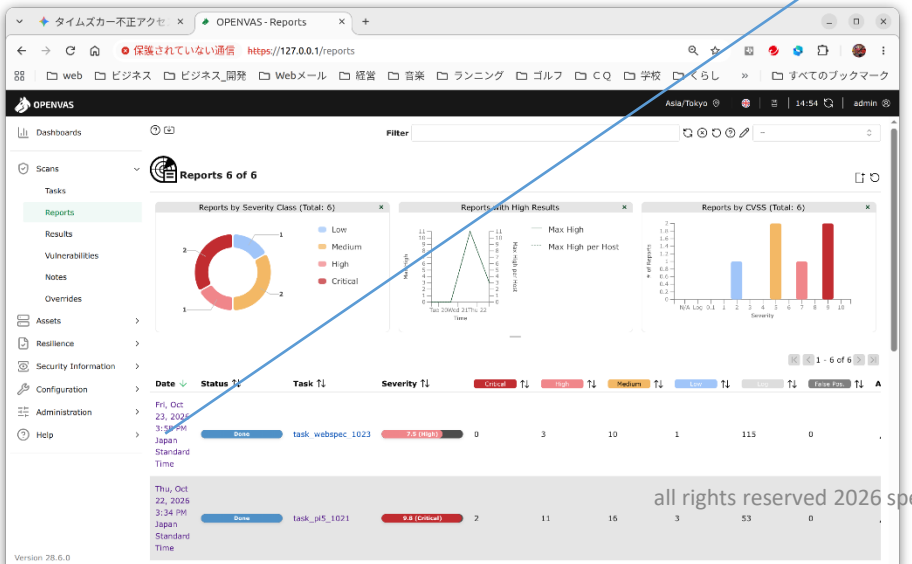
all rights reserved 2026 spectrum technology co.

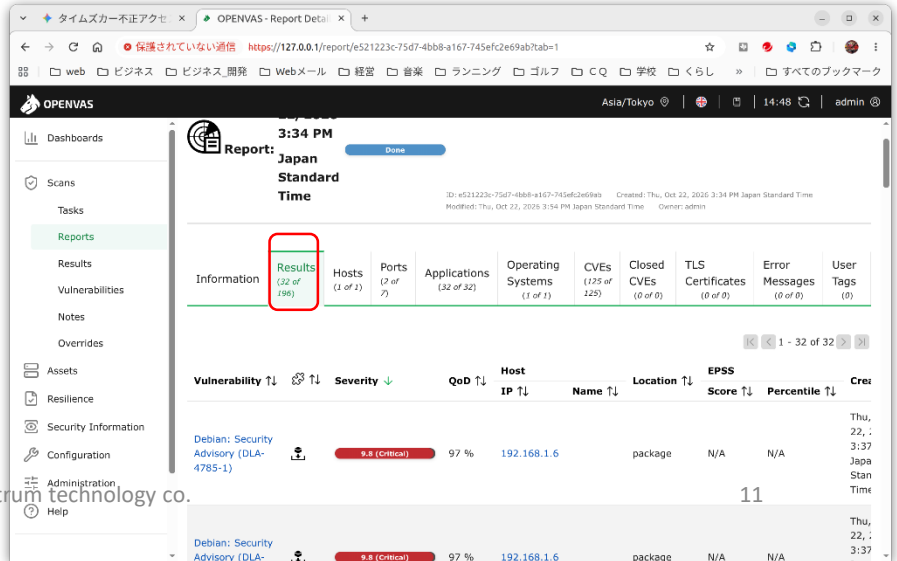
Spectrum Technology

1.openvas
③運用

- 起動
- スキャンフロー
- スキャン・タスク設定
- スキャン報告書
  - Scan>report:脆弱性などの報告が出力
  - 一覧から該当の報告、概要、結果





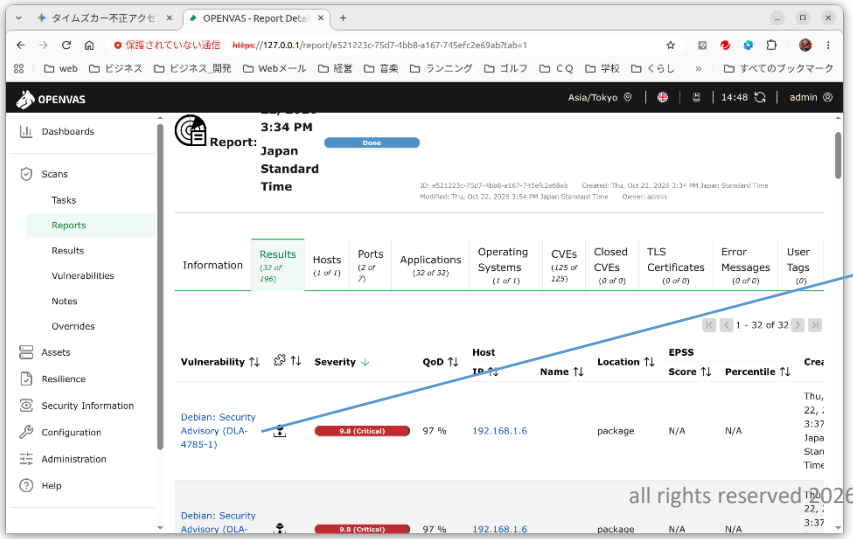


all rights reserved 2026 spectrum technology co.

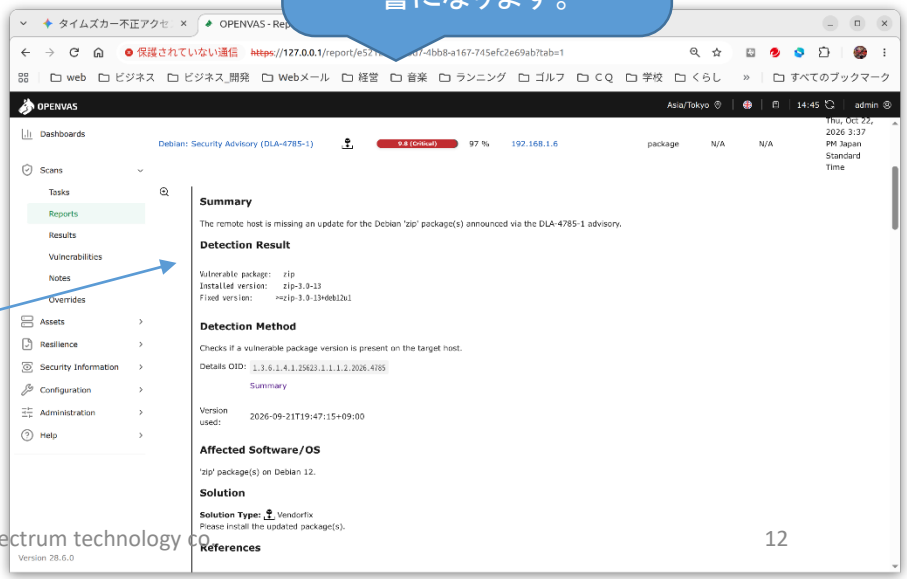
Spectrum Technology

1.openvas
③運用

- 起動
- スキャンフロー
- スキャン・タスク設定
- スキャン報告書
  - Scan>report:脆弱性などの報告が出力
  - 結果、詳細



脆弱性の詳細と、対策が表示。Makeの自動化で、日本語対応の報告書になります。

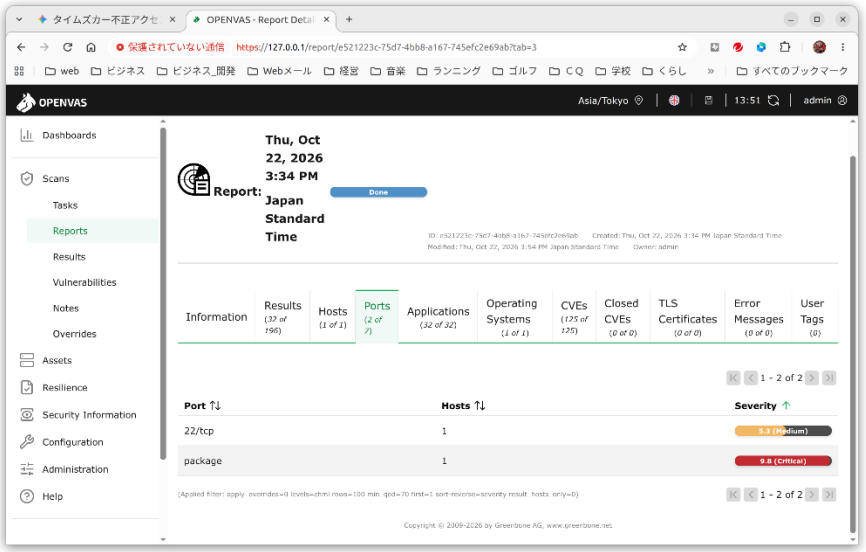


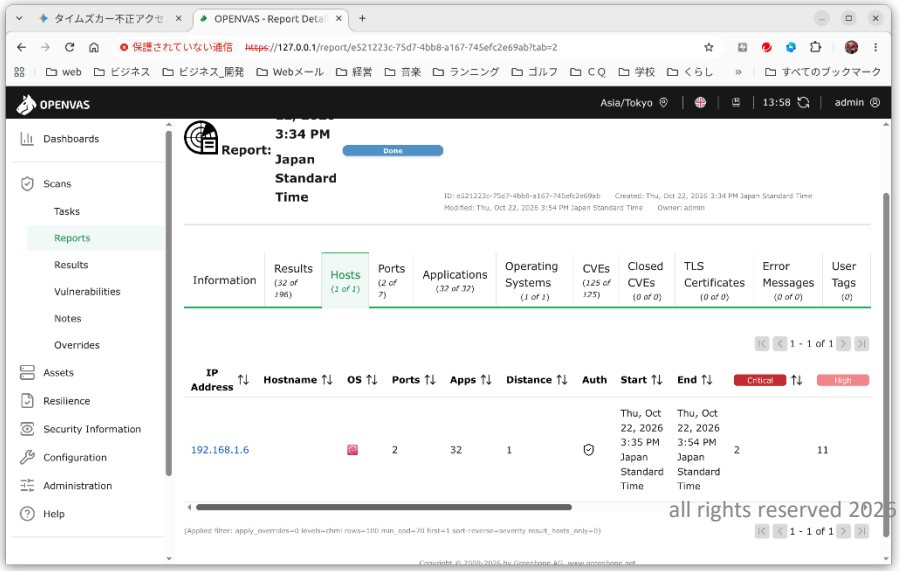
all rights reserved 2026 spectrum technology co.

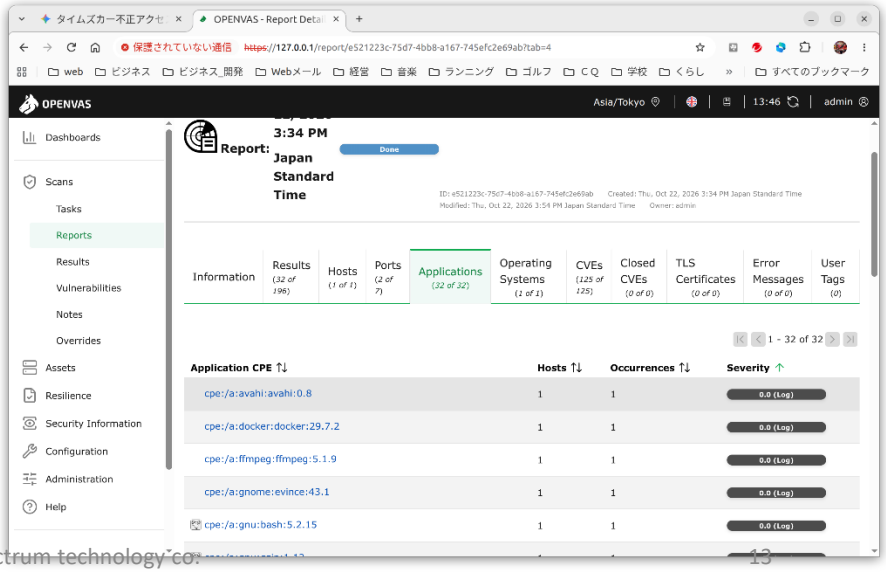
Spectrum Technology

1.openvas
③運用

- 起動
- スキャンフロー
- スキャン・タスク設定
- スキャン報告書
  - Scan>report:脆弱性などの報告が出力
  - ホスト、使用ポート、アプリ

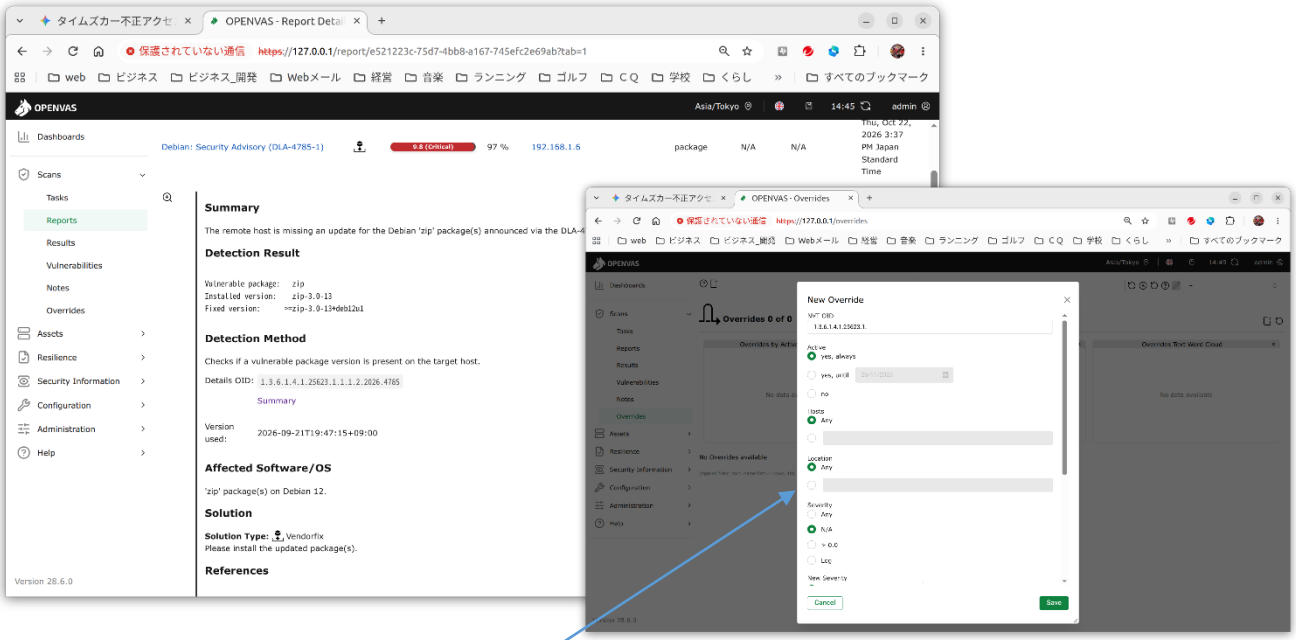






all rights reserved 2026 spectrum technology co.

1.openvas ④対策



- 起動
- スキャンフロー
- スキャン・タスク設定
- スキャン結果
- 対策
  - 各脆弱性に対して、各ホストに、記載している対策を実施。
  - 右上の脆弱性の場合は、パッケージの更新。Makeの自動化ツールでは日本語で対策のコマンドまで記載（gemini AIが対策を記載）。
  - 対策実施すると2回目は脆弱性のリストからなくなる。自動化ツールで対策実施日などを記入して管理
  - 参考：scan>override:脆弱性を対処済とすることもできるが、基本は、各対策を実施すること

all rights reserved 2026 spectrum technology co.

make

all rights reserved 2026 spectrum technology co.

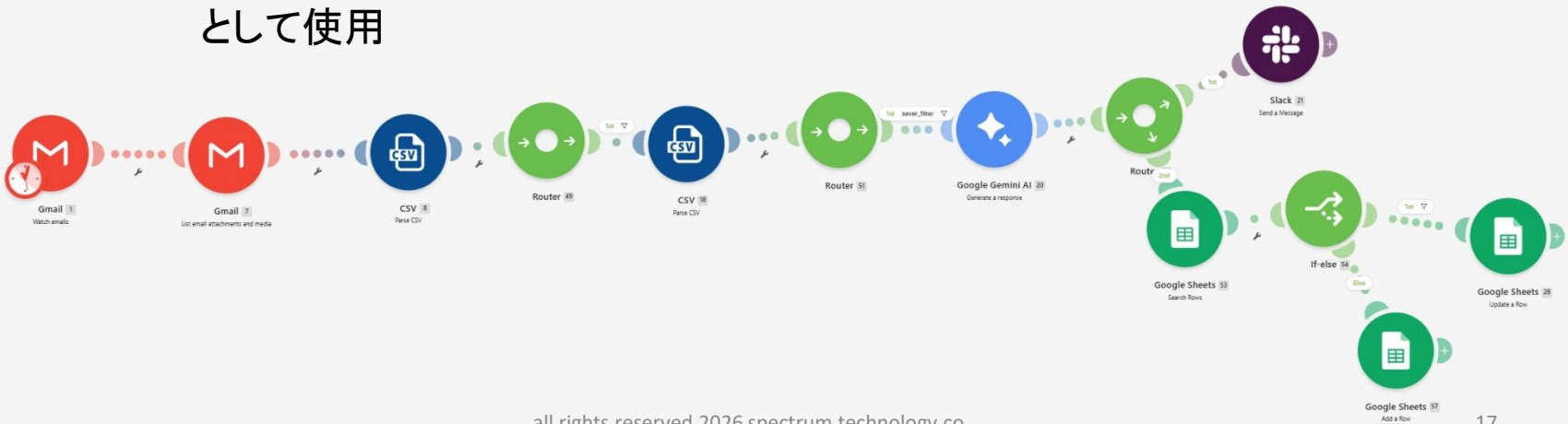
2.Make
①概要

- makeとは？
  - Make.comは、ノーコードで業務やアプリ間の連携を自動化できるクラウド型オートメーションプラットフォームです。旧名称「Integromat」からリブランディングされ、視覚的なワークフロー編集が特徴です。
  - https://www.make.com/en
- 特徴
  - ブラウザ上でフローチャートのように処理を組み立てます。
  - プログラミング不要で、ドラッグ＆ドロップ操作が中心です。
  - 個人～企業まで利用でき、無料枠から有料プランまで複数の料金プランがあります。

all rights reserved 2026 spectrum technology co.

2.Make
③設定：openvas自動化

- 準備
  - Gmail、google sheet,slackアカウントなど
- 下記の図のように設定します
  - Openvasからのgmail+csv添付ファイルを取り込み。重要なものだけに絞り込み
  - GeminiAPIで脆弱性内容、対策を分析し、日本語化
  - その内容をslack通知、及びGoogle sheetに保存、進捗管理として使用



all rights reserved 2026 spectrum technology co.

2.Make

④テスト：openvas自動化

- 連携テスト
  - openvas出力：スキャンし、csv出力
  - Gmailでcsvが添付されていることを確認
  - MakeのGmailのところで入力を確認。
  - 全体がokであれば、右肩に数字がでます。エラーはエラー表示



all rights reserved 2026 spectrum technology co.

2.Make

④テスト：openvas自動化

- 連携テスト
  - openvas出力：スキャンし、csv出力
  - Gmailでcsvが添付されていることを確認
  - MakeのGmailのところで入力を確認。
  - 全体がokであれば、右肩に数字がでます。エラーはエラー表示
  - Slackでの表示：わかりやすく解説しています

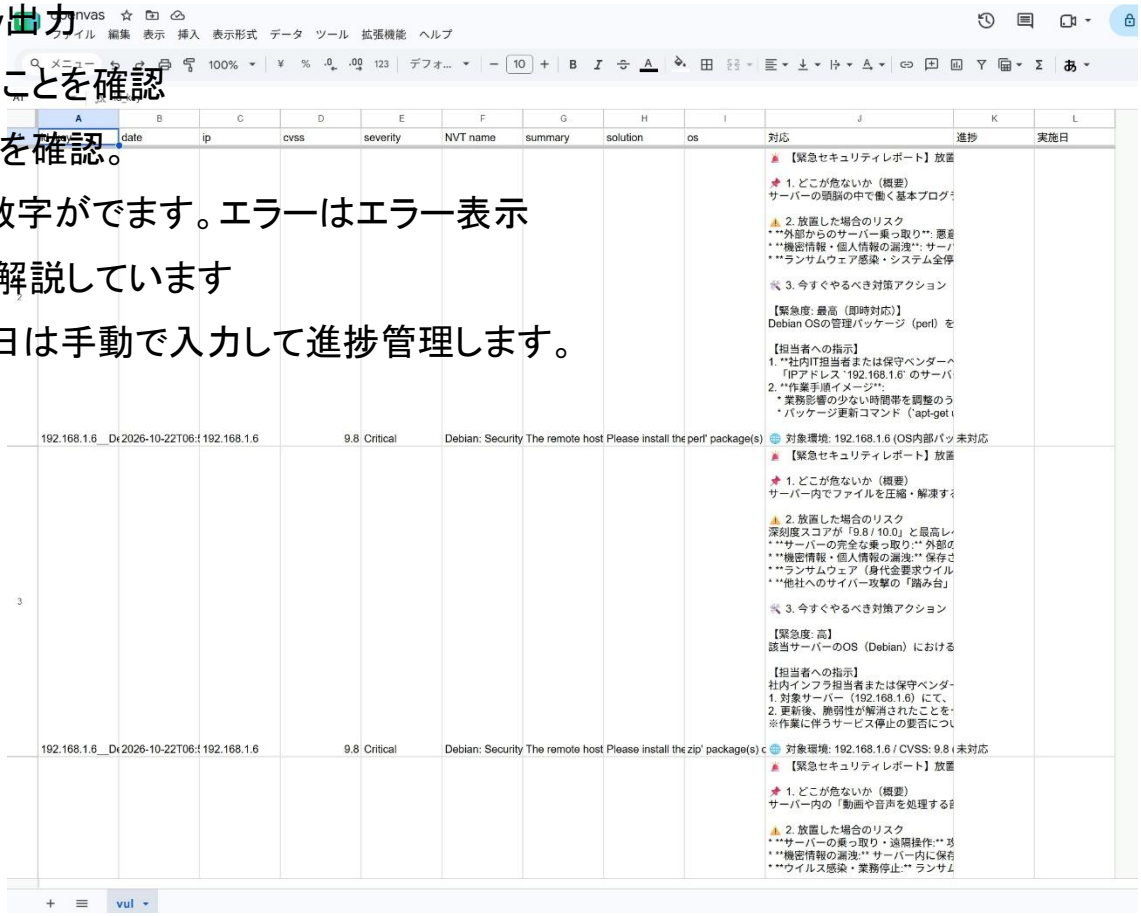


All rights reserved 2026 spectrum technology co.

2.Make

④テスト：openvas自動化

- 連携テスト
  - openvas出力：スキャンし、csv出力
  - Gmailでcsvが添付されていることを確認
  - MakeのGmailのところで入力を確認。
  - 全体がokであれば、右肩に数字がでます。エラーはエラー表示
  - Slackでの表示：わかりやすく解説しています
  - sheetでの表示。進捗と実施日は手動で入力して進捗管理します。

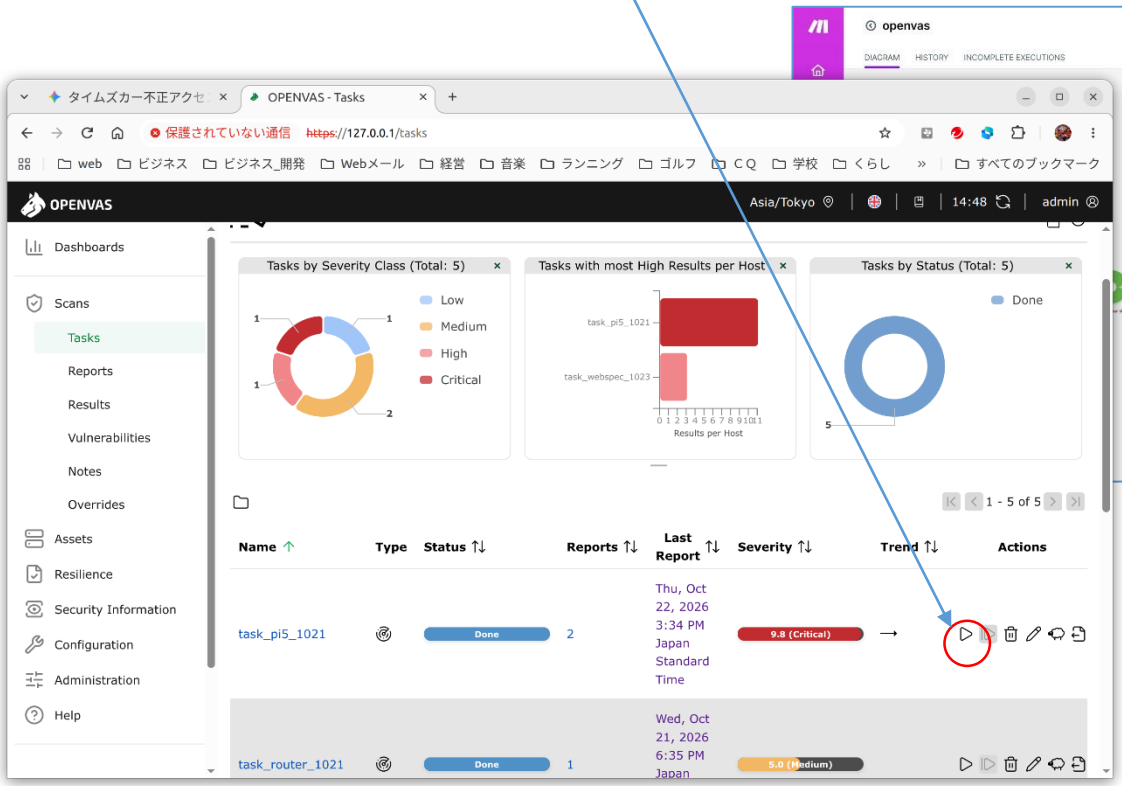


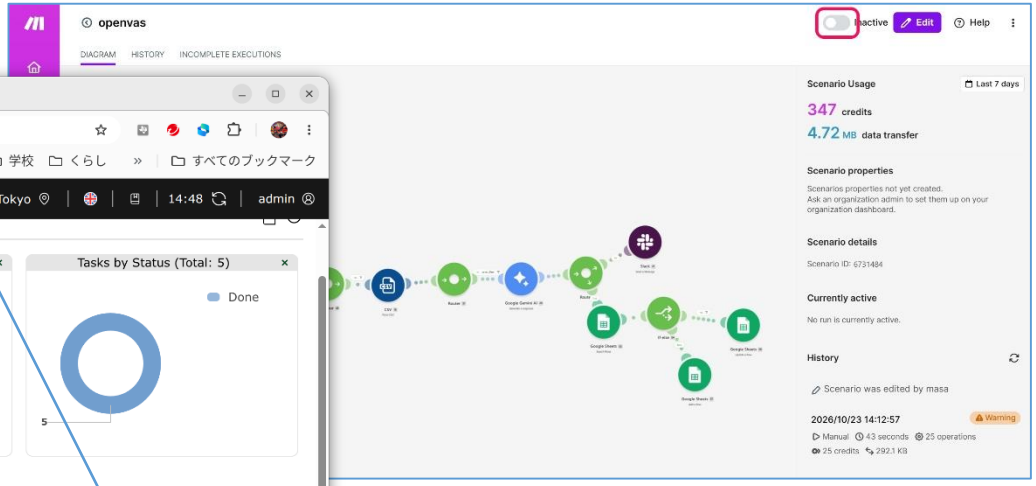
all rights reserved 2026 spectrum technology co.

2.Make

⑤本番運用

- 本番運用
  - Make>openvasシナリオ：activeへ
  - Openvasのscan>taskを稼働へ、又はスケジュール化





all rights reserved 2026 spectrum technology co.

ZAP

all rights reserved 2026 spectrum technology co.

3.ZAP
①概要

- ZAPとは？
  - OWASP ZAP（Zed Attack Proxy）は、世界的に有名なセキュリティコミュニティ「OWASP」が開発・提供している、オープンソースの Webアプリケーション用ダイナミック脆弱性スキャナー（DAST）です。WebサイトやWebアプリに対して実際にHTTPリクエストを送り、画面の裏側にある入力フォームやAPIの脆弱性（SQLインジェクションやクロスサイトスクリプティングなど）を網羅的に検出・診断するために使用します。
  - https://www.zaproxy.org/getting-started
- 特徴
  - 「自動スキャン」と「手動（プロキシ）パトロール」の両立
    - 自動でサイト内を巡回するクローラー機能だけでなく、ブラウザの通信を ZAP 経由（プロキシ）にすることで、人間の手でログイン操作や複雑な画面遷移を行いながら、その裏の通信を丸ごとテスト対象にできます。
  - リフレッシュされたセッション・リダイレクトの正確な処理
    - ログイン画面や複雑なセッション管理、302リダイレクトなどを伴うモダンなWebアプリであっても、セッションを維持したまま正しく奥までスキャンを進められます。
  - 多様なプラットフォームと拡張性
    - GUI版（デスクトップアプリとして視覚的に操作可能）だけでなく、コマンドラインや Docker コンテナとしても実行できるため、CI/CDパイプラインや自動化スクリプトへの組み込みも容易です。
  - 豊富なアドオンとコミュニティサポート
    - 活発なオープンソースプロジェクトであるため、新しい攻撃手法や脆弱性に対応するアドオンが日々追加されています。
  - 完全無料（オープンソース）
    - 商用の高額なWeb脆弱性検査ツールに匹敵する高度な機能を、コストを一切かけずに利用できます。

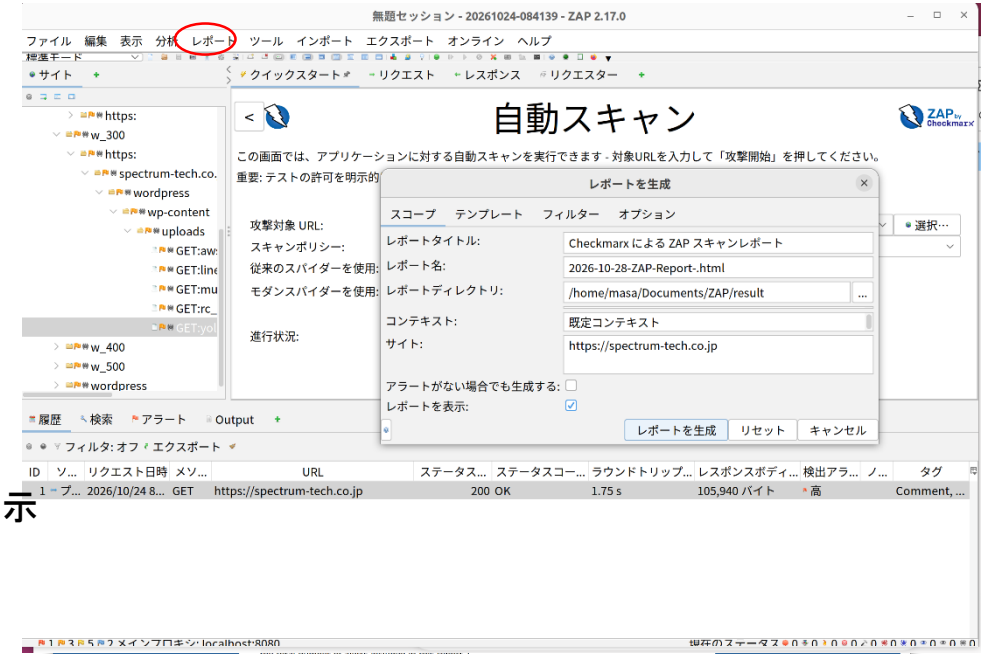
all rights reserved 2026 spectrum technology co.

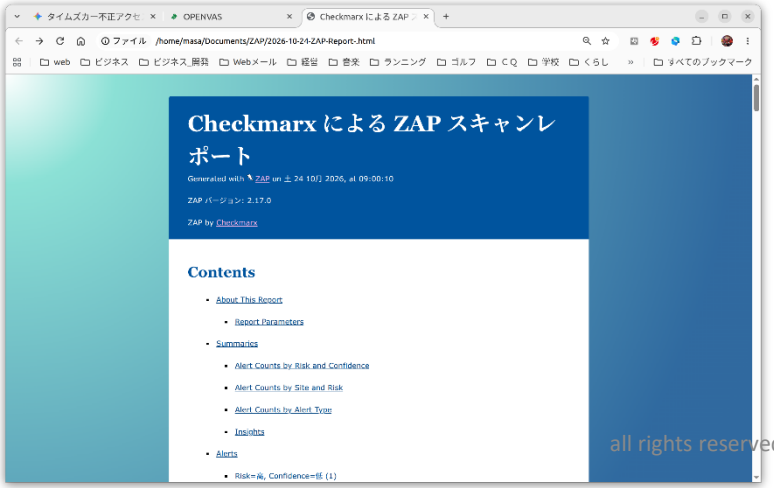
Spectrum Technology

コマンド入力
cd /home/masa/Documents/ZAP
./zap.sh

3.ZAP
③結果

- インストール
- 起動
- 設定、実施
- 結果
  - スキャン後、レポート出力：保存場所指定
  - Htmlが出力されるので、クリックで内容表示
  - 脆弱性確認







all rights reserved 2026 spectrum technology co.

4.運用のポイント

① アプリの使い分け

- Openvas:ネットワーク機器、サーバ、クライアントに適用に、ユーザ認証で内部まで入り脆弱性の調査を行う
- Zap：公開している自社のwebアプリに適用：負荷がかかるので、空き時間などに実施。他社のwebには実施しないこと

② 課金

- Openvas:無料
- Zap:無料
- Make:無料（1000クレジット/月）：1回のopenvasの調査結果で、約100クレジット、10回まで、有償（core $9,1万クレジット/月）100回まで、他に上位の契約あり
- Gemini api:有償（$5/月：最低）、10円/1回（csv,15件）、80回/月
- 合計：make+gemini:$9+$5=$14/月（80回/月）

③ 調査頻度

- 当初は脆弱性の更新頻度が分からないため、２－３日に1回。その後慣れたら1週間に1回程度。
- また、openvasはスケジュールすると自動で調査可能

all rights reserved 2026 spectrum technology co.

免責事項

本脆弱性診断・・自動管理ツールの販売にあたって、免責事項は、以下のとおりです。

第1条（免責事項・保証の否認）

- 本ツール（OpenVAS、OWASP ZAP、Make、Gemini API等を用いた自動診断・管理システムを含みます）は、システムやWebアプリケーションに存在する既知の脆弱性を検知・分析するための補助ツールであり、**システム全体の安全性や、すべての脆弱性の検出・不正アクセスの完全な防止を保証するものではありません。**
- 弊社は、本ツールの利用、または利用できなかったことに関して、ユーザーまたは第三者に生じた直接的、間接的、偶発的、特別、結果的損害（システムの停止、データの消失、業務の中断、利益の損失等を含みますが、これらに限定されません）について、法令上の定めがある場合を除き、一切の責任を負いません。

第2条（利用対象の限定とユーザーの責任）

- ユーザーは、本ツールを「自社が所有・管理するシステム」または「事前に所有者から明示的な許可を得た正当な権限を持つターゲット」に対してのみ使用するものとします。
- 許可のない第三者のシステムやネットワークに対して本ツール（特にOWASP ZAP等のアクティブスキャンや侵入テスト関連機能）を実行した場合、不正アクセス禁止法や関連法令に抵触する恐れがあります。これに違反して生じたトラブルや法的紛争について、弊社は一切の責任を負わず、すべての責任はユーザー自身が負うものとします。

第3条（システムへの影響に関する注意）

- 脆弱性診断（スキャン）の実行は、対象となるサーバーやネットワーク機器に対して一時的な負荷をかける場合があります。負荷による回線の圧迫、サービスの遅延、またはシステムの一時的な停止等が生じた場合、弊社はその損害について一切の責任を負いません。本番環境で実施する際は、必ず負荷の少ない時間帯を選択するなど、ユーザーの責任において十分な配慮を行うものとします。

第4条（AIおよび外部サービスの出力に関する免責）

- 本ツールに組み込まれている生成AI（Gemini API等）による解析結果、日本語要約レポート、および対策案は、AIが自動生成するものであり、その内容の正確性、完全性、有用性、および特定の脆弱性に対する効果を完全に保証するものではありません。
- AIの出力結果や推奨される対策コマンド等の適用は、必ず専門知識を持つ技術者の判断と検証のもとで行うものとし、適用結果に起因して生じた不具合や障害について、弊社は責任を負いません。
- Make、Slack、Google Sheetsなどの外部SaaS・API側の仕様変更、障害、料金改定、またはサービス停止に起因して本ツールの機能の一部または全部が利用できなくなった場合、弊社は一切の責任を負いません。

第5条（アップデートおよびデータベースの性質）

- 本ツールで利用する脆弱性データベース（NVT、CVE情報等）は外部のオープンソースコミュニティやセキュリティ機関に依存しており、すべての新種・ゼロデイ脆弱性がリアルタイムで反映されるものではありません。

all rights reserved 2026 spectrum technology co.