Spectrum Technology

V1.0 2026/11/9

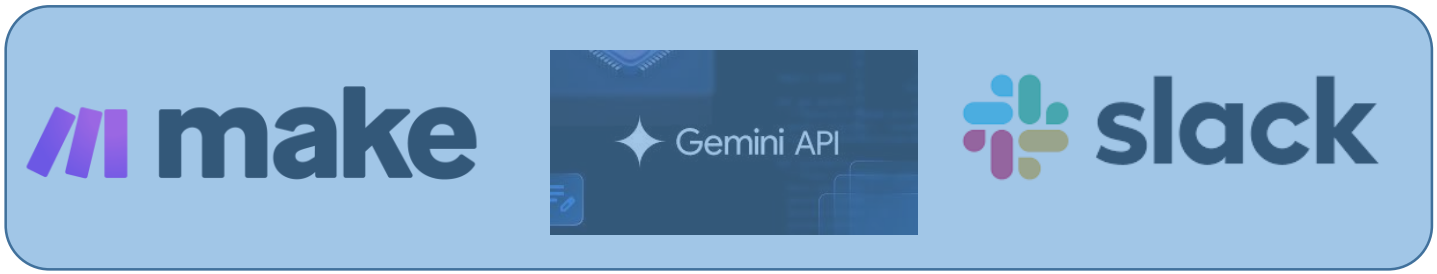
無償配布版

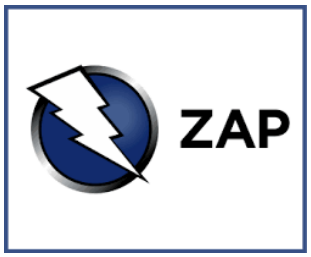
サイバー攻撃対策　脆弱性診断ツール

～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. ubuntu版設定	6
4. Vmware版設定	7
1. Openvas	
① 概要	9
② 設定	11
③ 運用	13
④ 対策	30
2. Make	
① 概要	32
② アカウント設定	33
③ 設定：openvas自動化	34
④ テスト：openvas自動化	56
⑤ 本番運用	61
3. ZAP	
① 概要	63
② 設定、実施	65
③ 結果	68
4. 運用のポイント	71
免責事項	73
IPアドレス確認	75

利用にあたっては、各自でリスクを判断して、実施してください。インストール後のトラブルについては、弊社は責任を負いかねます。

無償配布版のため、自動管理ツールは含まれていません。、目次とページは一致しません。

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　128GB Ubuntu24.04,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	500GB以上	vmwareの場合,80GB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.

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
①概要

- 診断方式

項目	外部からの診断	内部からの診断
視点	インターネット上の第三者（攻撃者）	社内ネットワーク・管理者権限を持つユーザー
必要な権限	なし（アンシグネチャ/非認証）	あり（SSH/SMBなどのログイン情報）
スキャン範囲	外部に公開されているサービス・ポートのみ	OS内部の全インストール済みソフト・設定
検出の深さ	浅い（表面的な応答から推測）	**非常に深い**（パッチの未適用まで正確に把握）
主な用途	外部攻撃からの入口チェック	資産管理・脆弱性管理・多層防御

出来る限り、内部診断で実施しましょう、MFA設定のものは、一時的に外すなどしましょう。

- 対象機器

カテゴリ	推奨されるスキャン方式	重点チェック項目
Webサーバー	外部 / 内部（非認証メイン）	SSL/TLS設定、Webアプリの応答、不要ポート
クライアント・サーバー	**内部（認証付きスキャン）**	OSパッチ未適用、ローカル権限昇格、脆弱な設定、不要なサービス
ネットワーク機器	外部 / 内部	開放ポート、ファームウェアの脆弱性、SNMP設定
DB・ミドルウェア	内部（非認証・認証）	アクセス制限（IP制限）、デフォルトパスワード
IoT・NAS・複合機	内部	初期パスワード、古いファームウェア、弱い認証

all rights reserved 2026 spectrum technology co.

Spectrum Technology

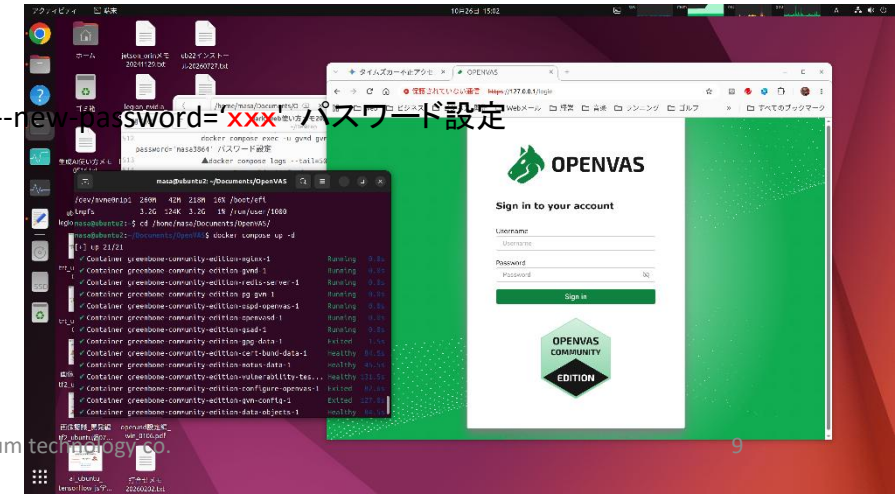
1.openvas ②設定

コマンド入力
cd /home/masa/Documents/OpenVAS
curl -f -O -L https://greenbone.github.io/docs/latest/_static/compose.yaml
docker compose -f compose.yaml -p greenbone-community-edition pull
docker compose -f compose.yaml -p greenbone-community-edition up -d
docker compose exec -u gvmd gvmd gvmd --user=admin --new-password='xxx'

- 準備
  - ubuntu22以上のマシンを準備
  - Dockerをインストール済
- インストール
  - $ cd /home/masa/Documents/OpenVAS配下へ
  - $ curl -f -O -L https://greenbone.github.io/docs/latest/_static/compose.yaml
  - $ docker compose -f compose.yaml -p greenbone-community-edition pull
  - $ docker compose -f compose.yaml -p greenbone-community-edition up -d

Vmwareはここから

- 設定
  - $ docker compose exec -u gvmd gvmd gvmd --user=admin --new-password='xxx' パスワード設定
- 起動
  - http://127.0.0.1:9392/
  - 右のブラウザが立ち上がる
  - 設定したユーザ、パスワードを入力



all rights reserved 2026 spectrum technology co.

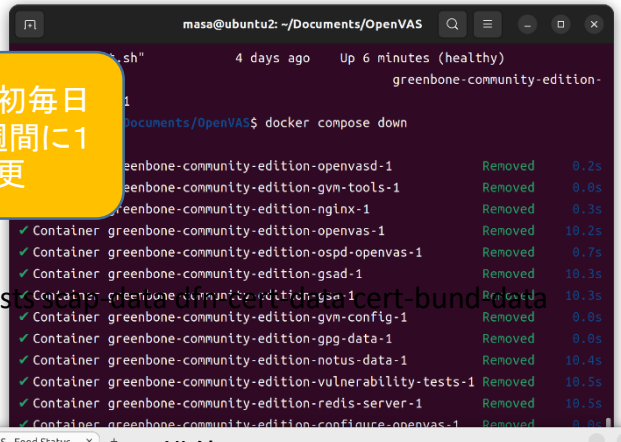
1.openvas ②設定

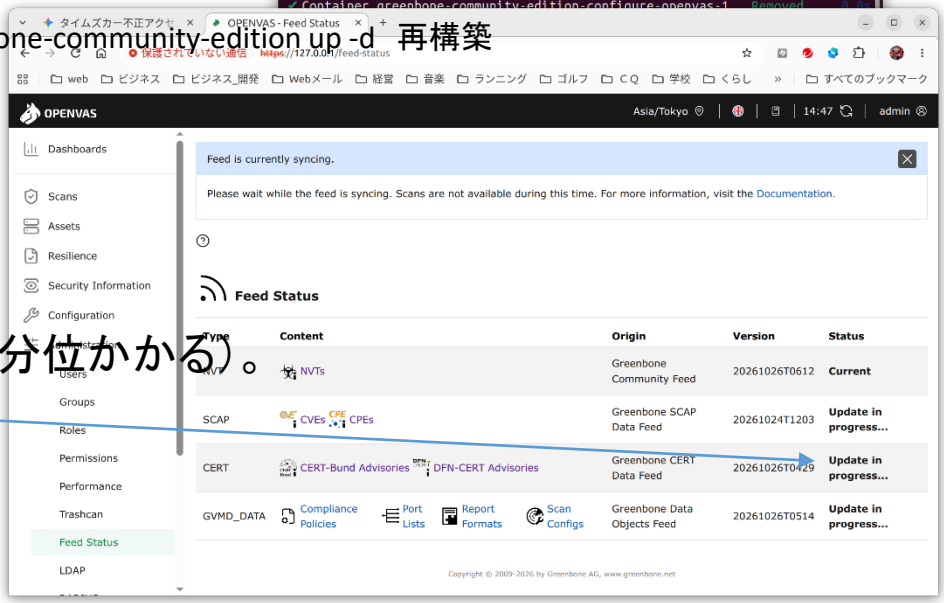
コマンド入力
cd /home/masa/Documents/OpenVAS
docker compose -f compose.yaml pull notus-data vulnerability-tests scap-data dfn-cert-data cert-bund-data report-formats data-objects
docker compose down　コンテナ削除
docker compose -f compose.yaml -p greenbone-community-edition up -d

- 準備
- 更新：脆弱性情報の更新
  - $ cd /home/masa/Documents/OpenVAS
  - $ docker compose -f compose.yaml pull notus-data vulnerability-tests scap-data dfn-cert-data cert-bund-data report-formats data-objects　30分位、イメージ更新
  - $ docker compose down　コンテナ削除
  - $ docker compose -f compose.yaml -p greenbone-community-edition up -d　再構築
- 起動
  - http://127.0.0.1:9392/
  - Admin>feed status
  - Updatingとなれば、更新中（30分位かかる）。

docker容量改善方法は、こちら

脆弱性の更新は、最初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

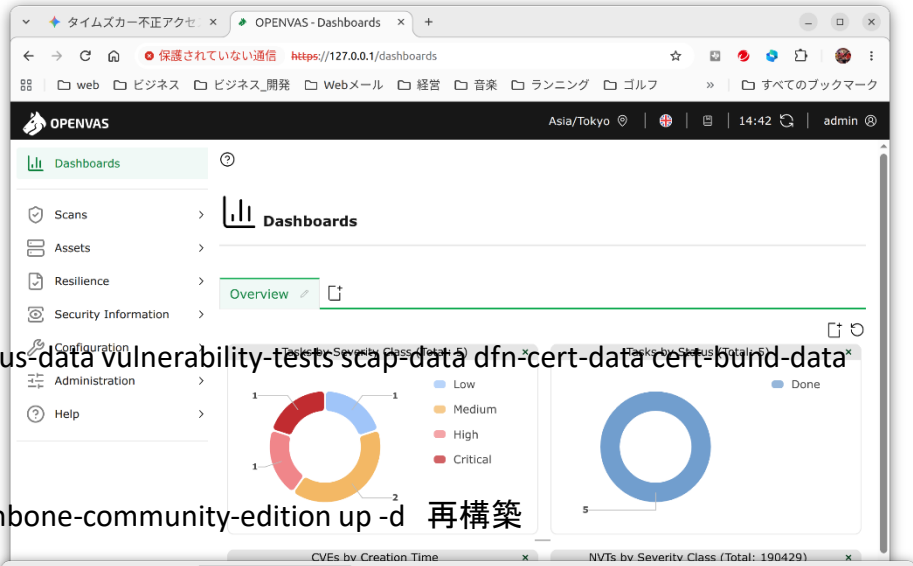
コマンド入力
cd /home/masa/Documents/OpenVAS
docker compose -f compose.yaml pull notus-data vulnerability-tests scap-data dfn-cert-data cert-bund-data report-formats data-objects
docker compose down　コンテナ削除
docker compose -f compose.yaml -p greenbone-community-edition up -d

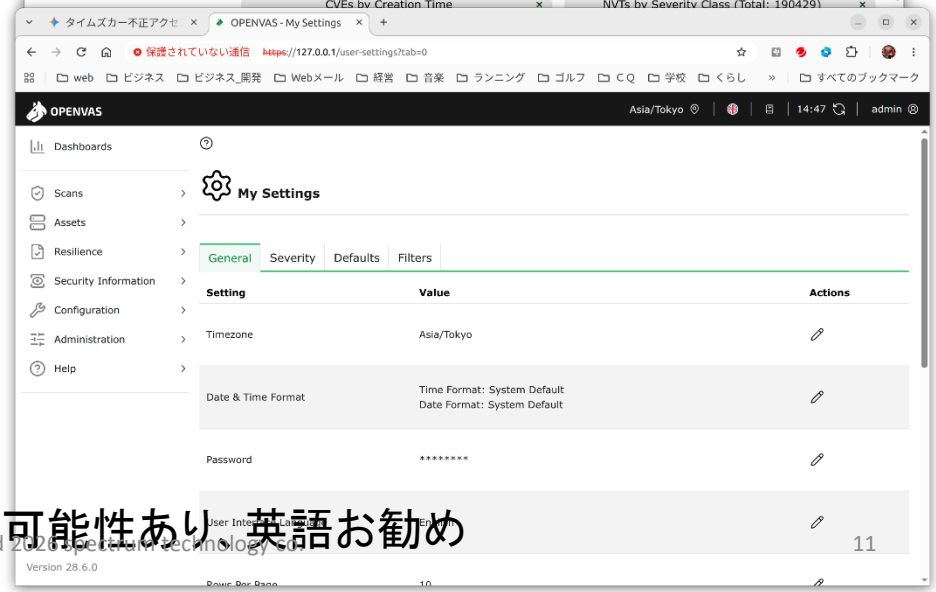
1.openvas
③運用

- 準備
- 更新：脆弱性情報の更新
  - $ cd /home/masa/Documents/OpenVAS
  - $ docker compose -f compose.yaml pull notus-data vulnerability-tests scap-data dfn-cert-data cert-bund-data report-formats data-objects
  - $ docker compose down　コンテナ削除
  - $ docker compose -f compose.yaml -p greenbone-community-edition up -d　再構築

docker容量改善方法は、こちら

- 起動
  - http://127.0.0.1:9392/
  - Dashboard
- 設定
  - 右上：setting
  - 時間：Asia>tokyoへ
  - 言語：日本語：誤翻訳になる可能性あり、英語お勧め



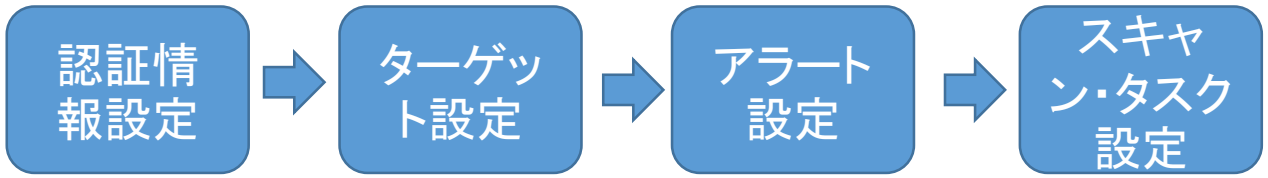


All rights reserved 2026 Spectrum Technology Co.,

1.openvas ③運用

項目	外部からの診断	内部からの診断
視点	インターネット上の第三者（攻撃者）	社内ネットワーク・管理者権限を持つユーザー
必要な権限	なし（アンシグネチャ/非認証）	あり（SSH/SMBなどのログイン情報）
スキャン範囲	外部に公開されているサービス・ポートのみ	OS内部の全インストール済みソフト・設定
検出の深さ	浅い（表面的な応答から推測）	**非常に深い**（パッチの未適用まで正確に把握）
主な用途	外部攻撃からの入口チェック	資産管理・脆弱性管理・多層防御

- 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（内部診断）

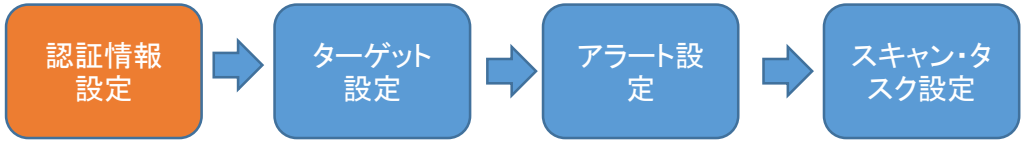
ターゲットのIPアドレス、ログイン情報

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

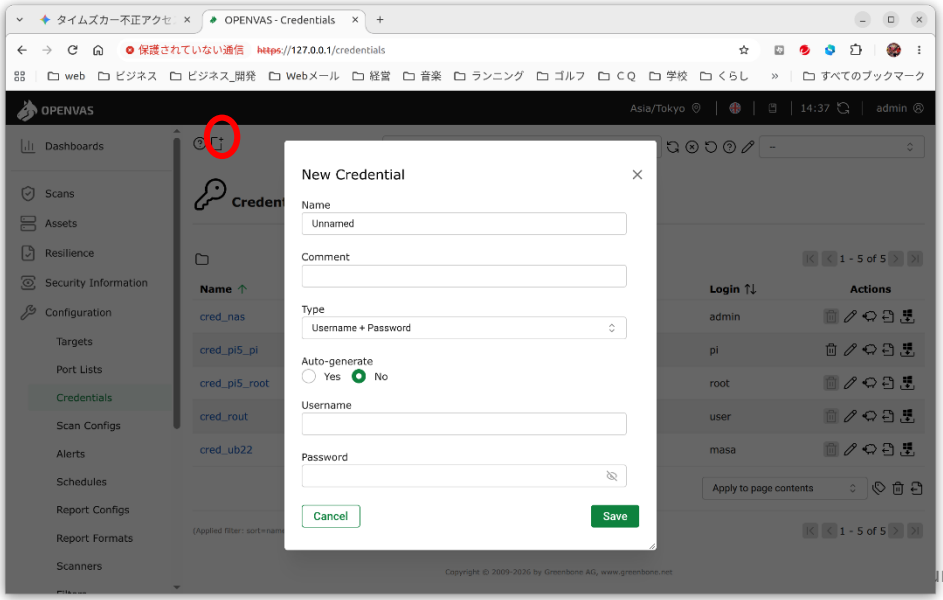
ターゲットを決めて、アラート、スケジュールなどを設定

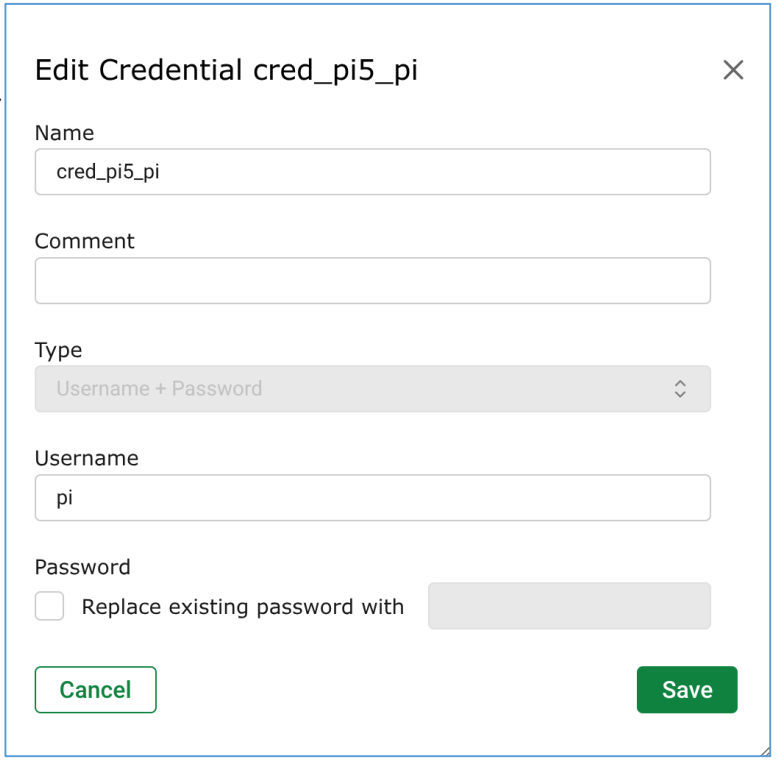
all rights reserved 2026 spectrum technology co.

1.openvas
③運用



- 起動
- スキャンフロー
- 認証設定
  - Configuration＞Credential　左上クリック
  - 名前、ユーザ、パスワードを入力



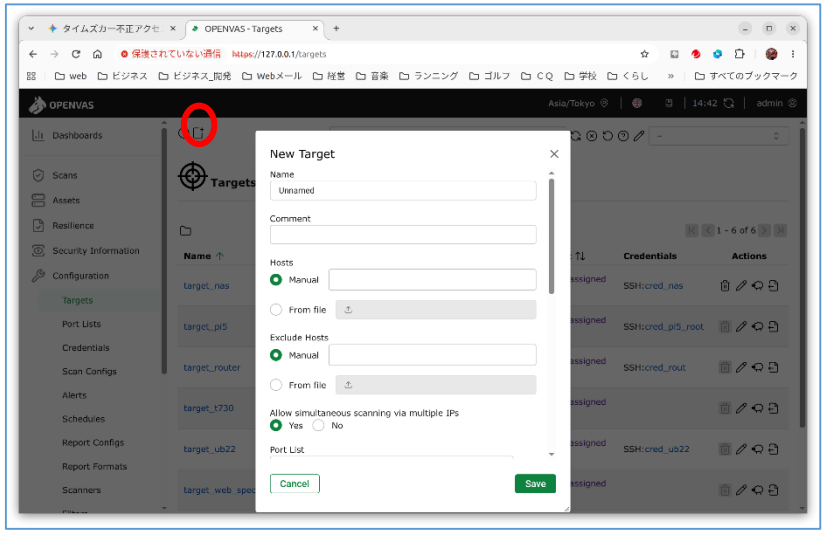


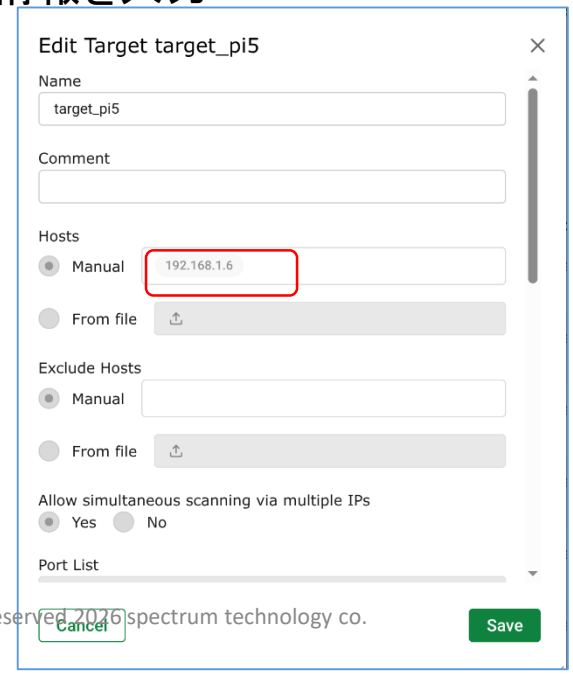
1.openvas ③運用

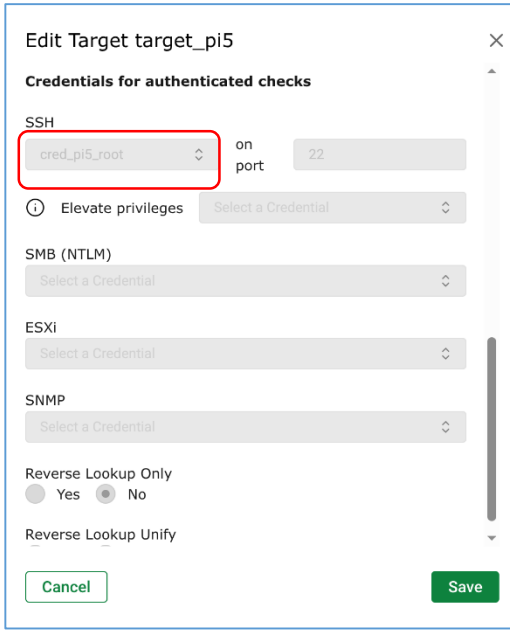
認証情報設定 → ターゲット設定 → アラート設定 → スキャン・タスク設定

- 起動
- スキャンフロー
- ターゲット設定
  - Configuration＞target　左上クリック
  - 名前、ip addr、ssh:前項の認証情報を入力

Ip addrは、softperfectを使って確認します。こちら参照



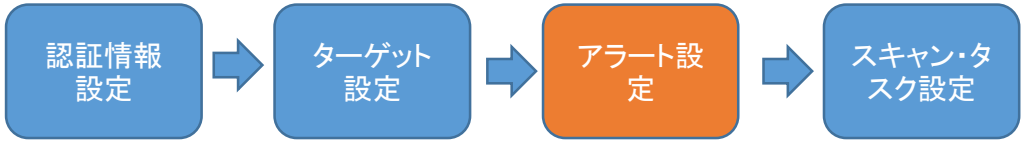




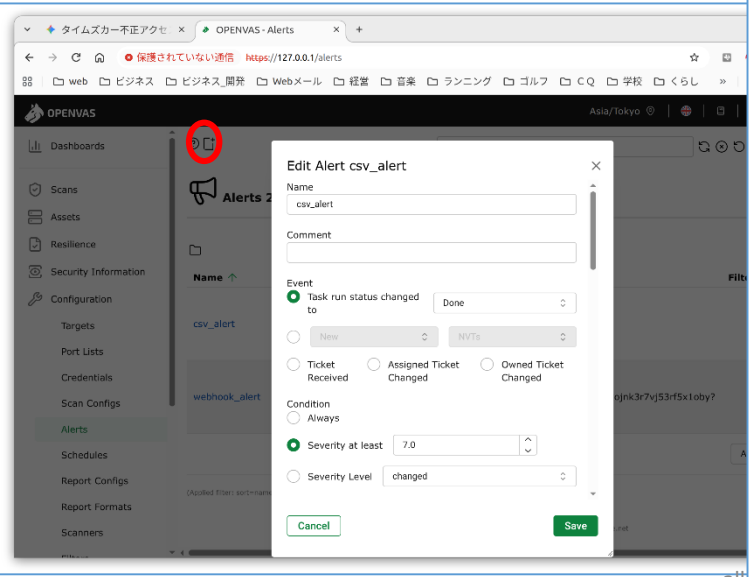
all rights reserved 2026 spectrum technology co.

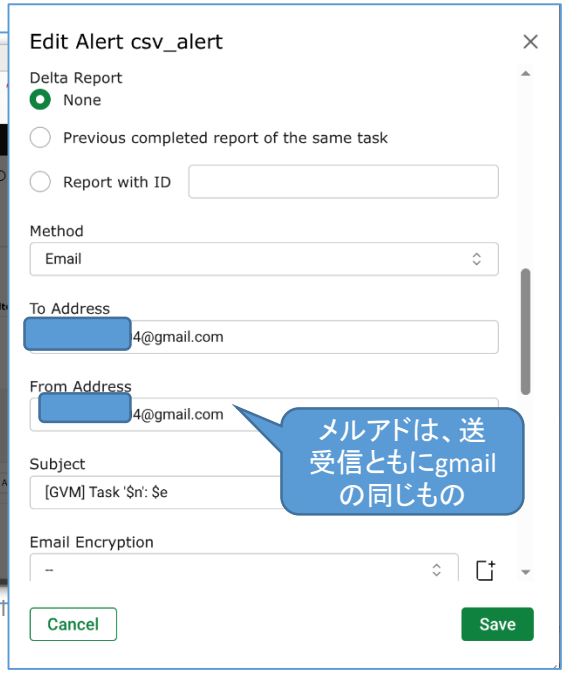
Spectrum Technology

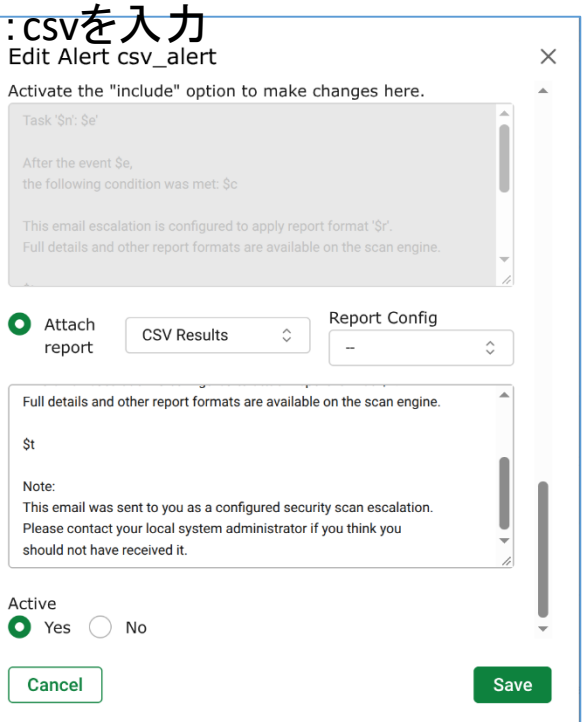
1.openvas ③運用



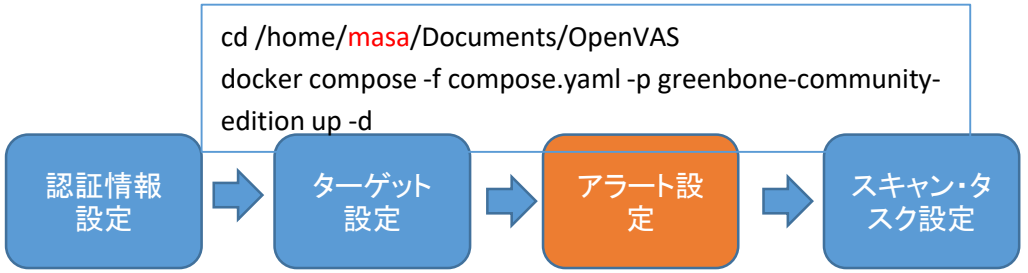
- 起動
- スキャンフロー
- アラート設定
  - Configuration＞alert　左上クリック
  - 名前、条件（severity:7.0)、通知方式：email, メルアド、添付：csvを入力







1.openvas ③運用



- 起動
- スキャンフロー
- アラート設定
  - Configuration＞alert　左上クリック
  - 名前、通知方式：email, メルアド、添付：csvを入力
  - Gmailを送信に使うための変更
  - 弊社提供のcompose.yamlの一部修正し、再ビルド
  - 再ビルド

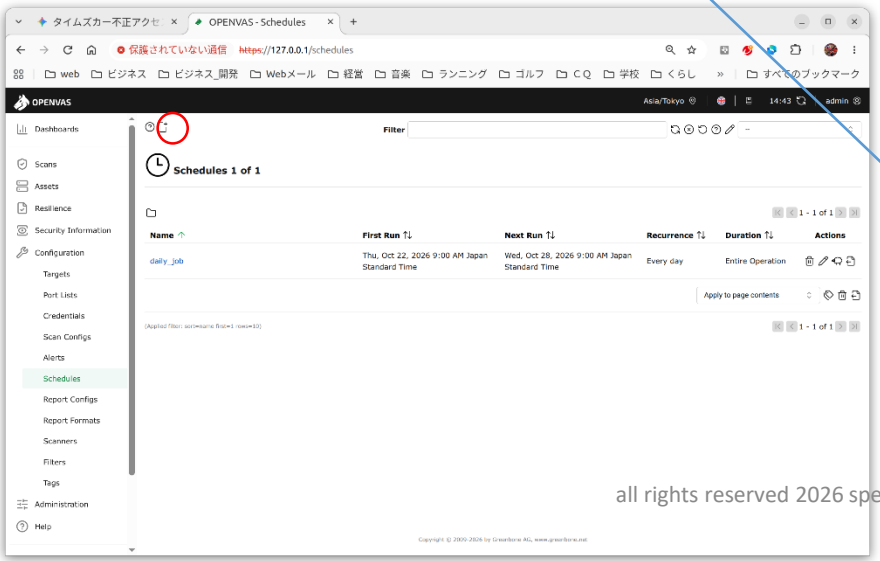
```
$ cd /home/masa/Documents/OpenVAS
$ docker compose -f compose.yaml -p greenbone-community-edition up -d
```

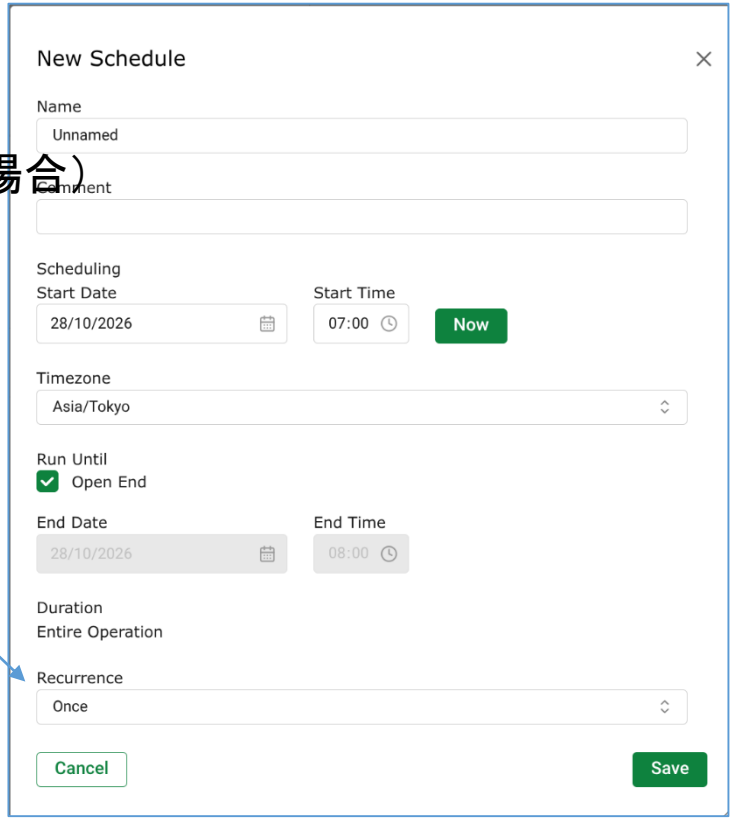
all rights reserved 2026 spectrum technology co.

1.openvas
③運用

認証情報設定 → ターゲット設定 → アラート設定 → スキャン・タスク設定

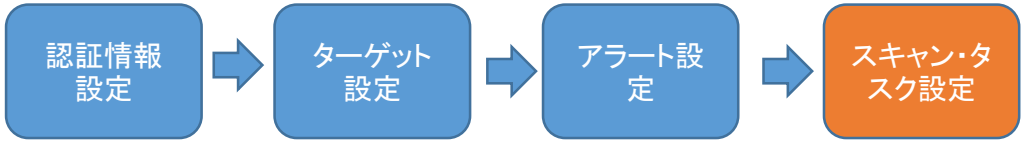
- 起動
- スキャンフロー
- スキャン・タスク設定
  - スケジュール：オプション（定期的に実施する場合）
  - Config＞schedule　左上クリック
  - 名前、開始スケジュール、周期を入力



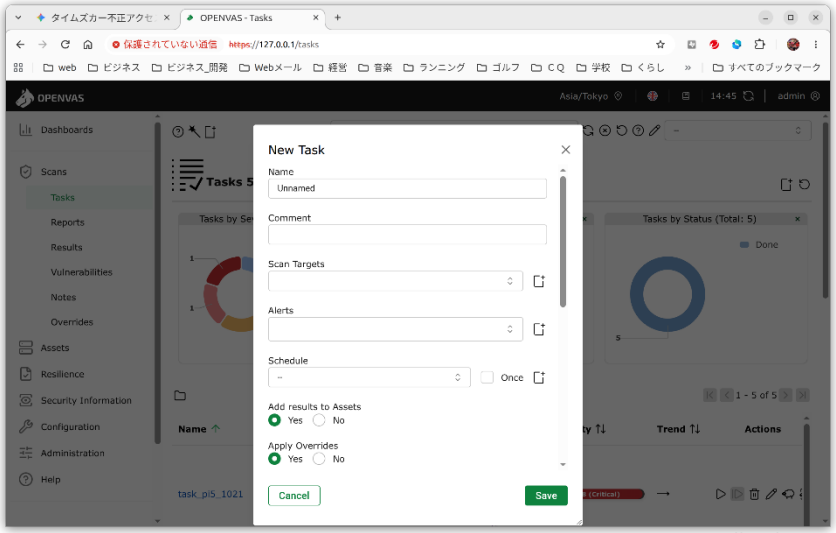


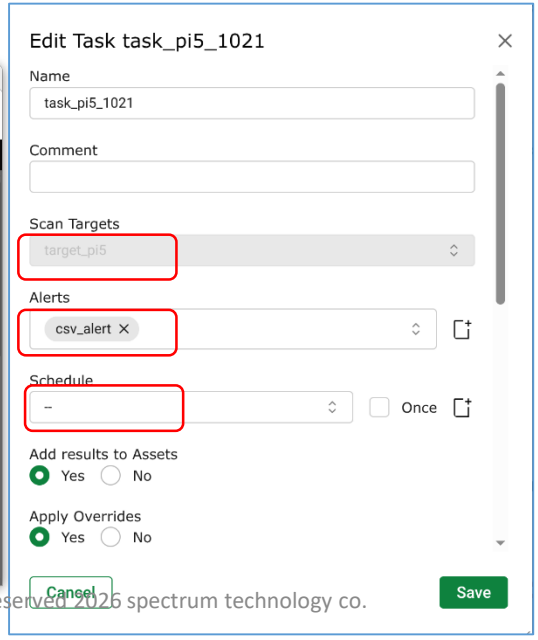
all rights reserved 2026 spectrum technology co.

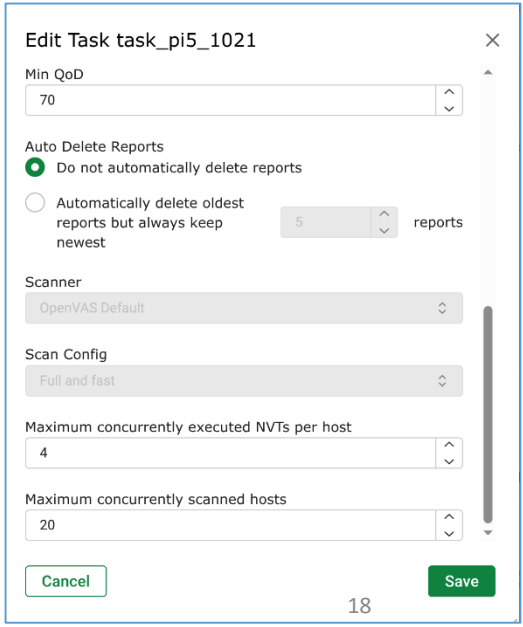
1.openvas ③運用



- 起動
- スキャンフロー
- スキャン･タスク設定
  - scan＞task　左上クリック
  - 名前、ターゲット、アラート、スケジュールを入力、他はデフォルト

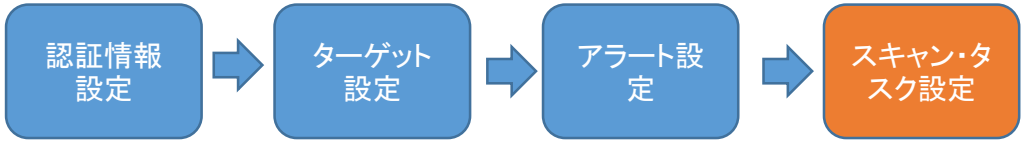






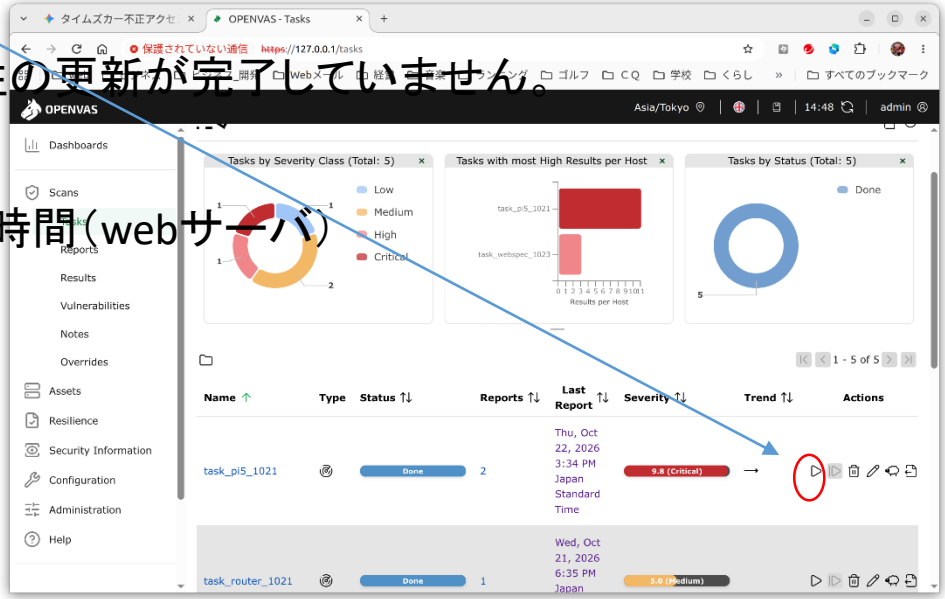
all rights reserved 2026 spectrum technology co.

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

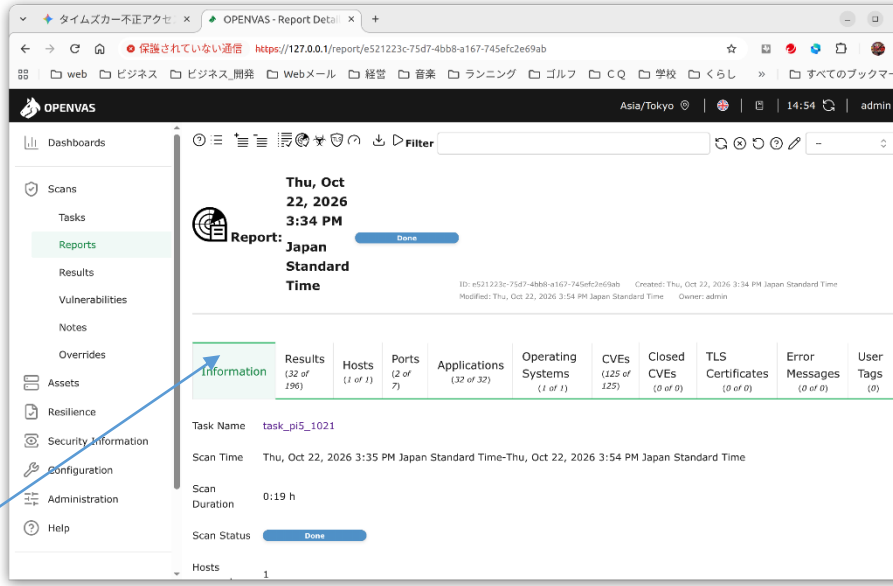


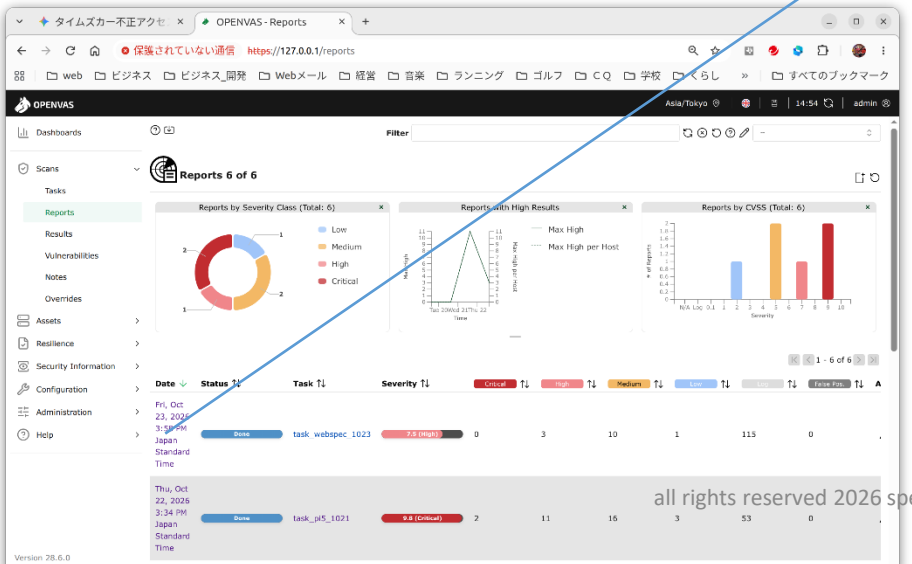
all rights reserved 2026 spectrum technology co.

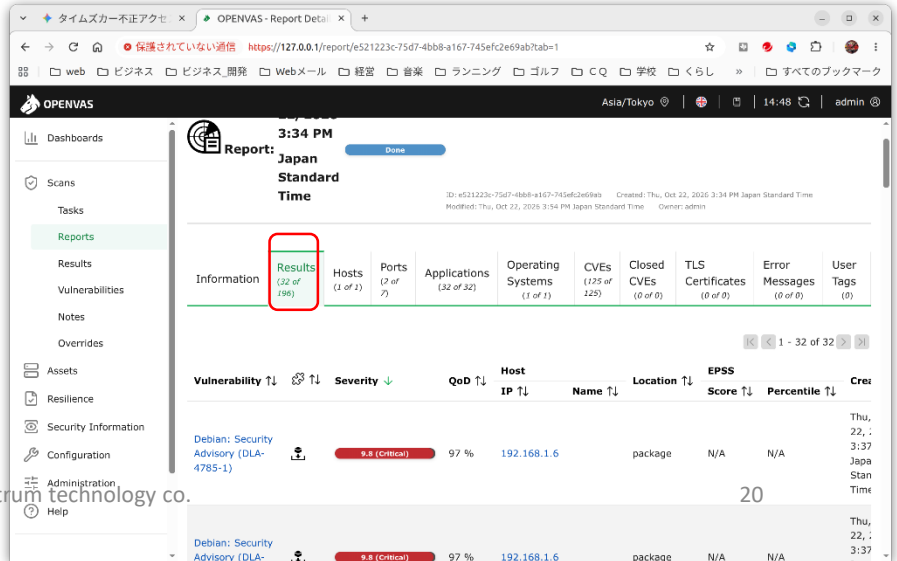
Spectrum Technology

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



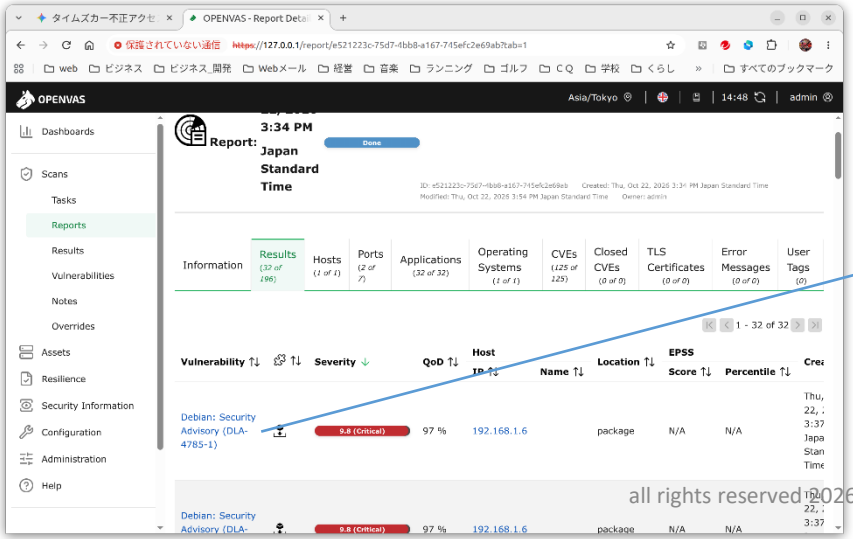




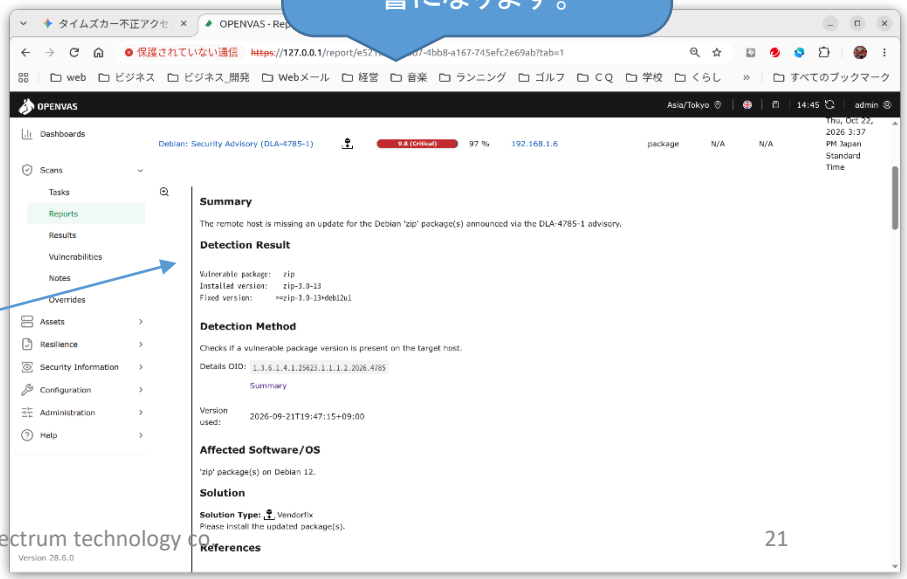
all rights reserved 2026 spectrum technology co.

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。

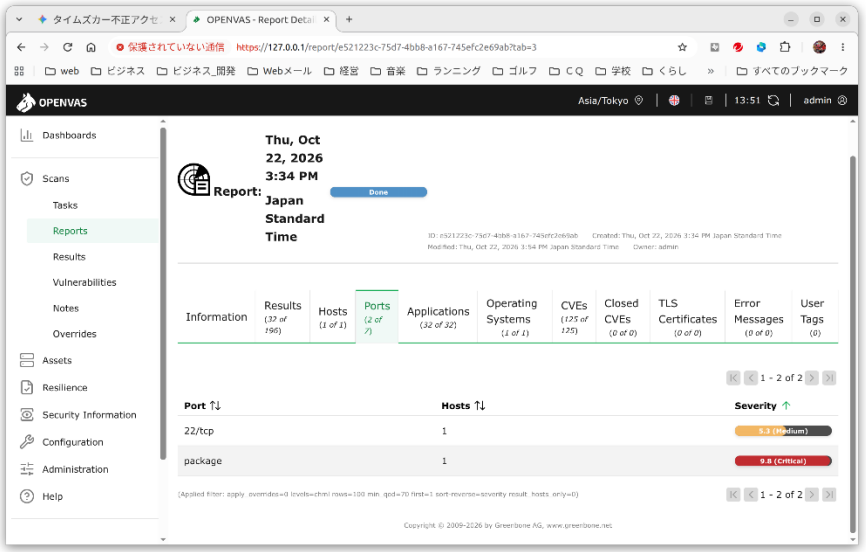


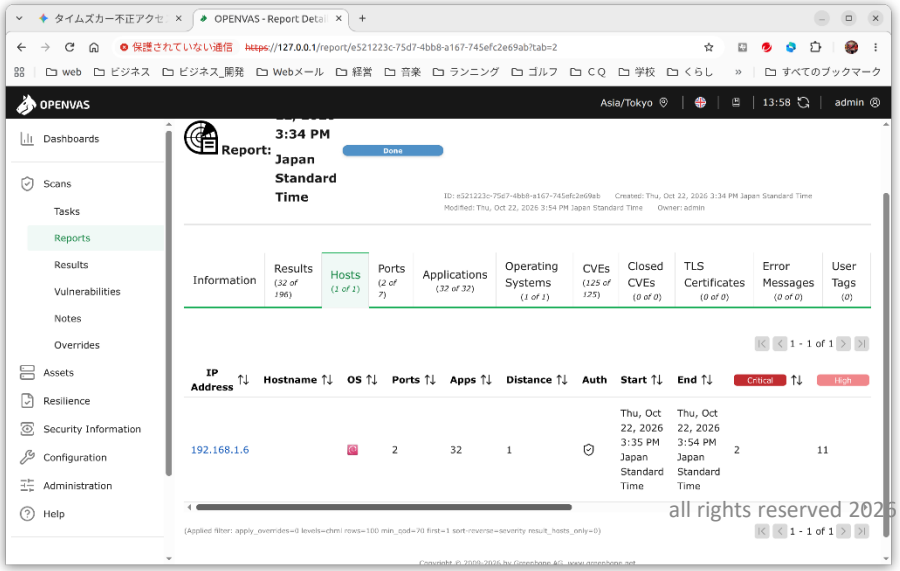
all rights reserved 2026 spectrum technology co.

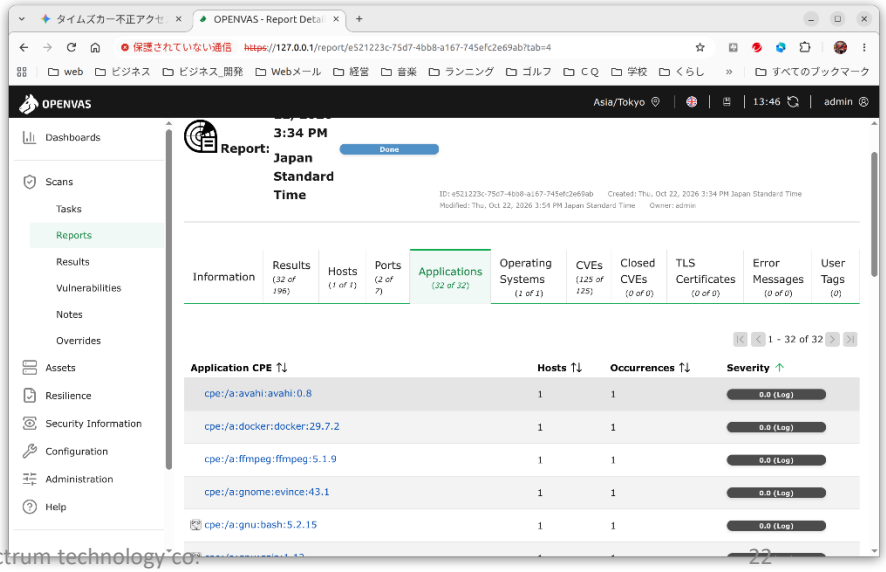
Spectrum Technology

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





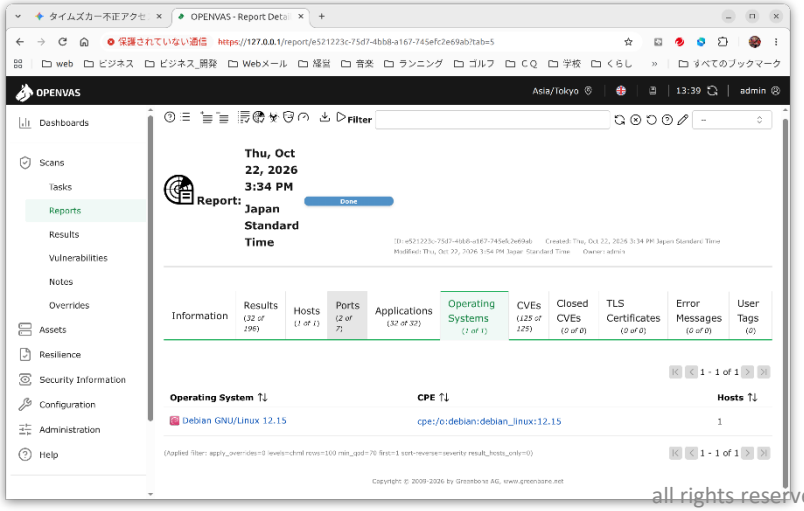


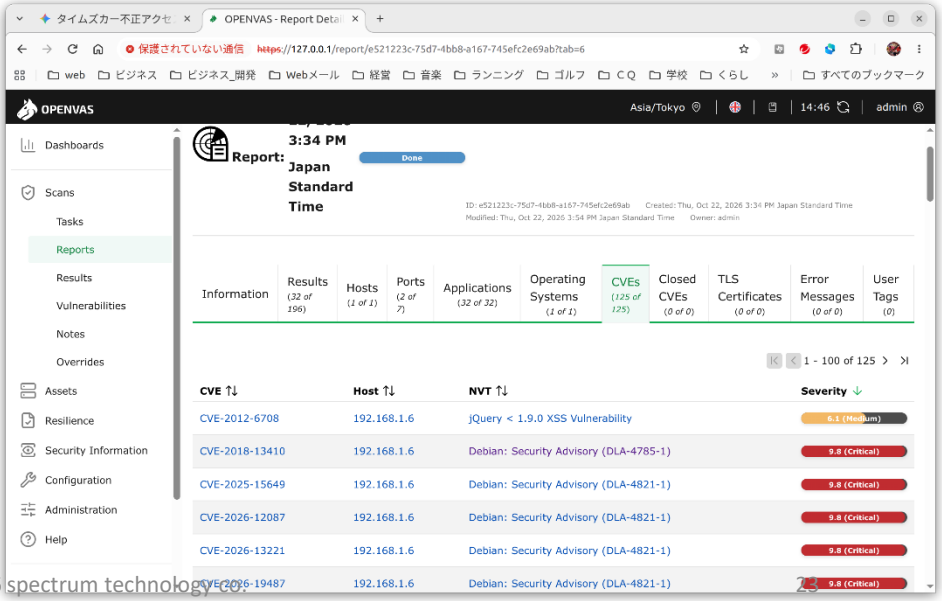
all rights reserved 2026 spectrum technology co.

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
  - Os, cve一覧

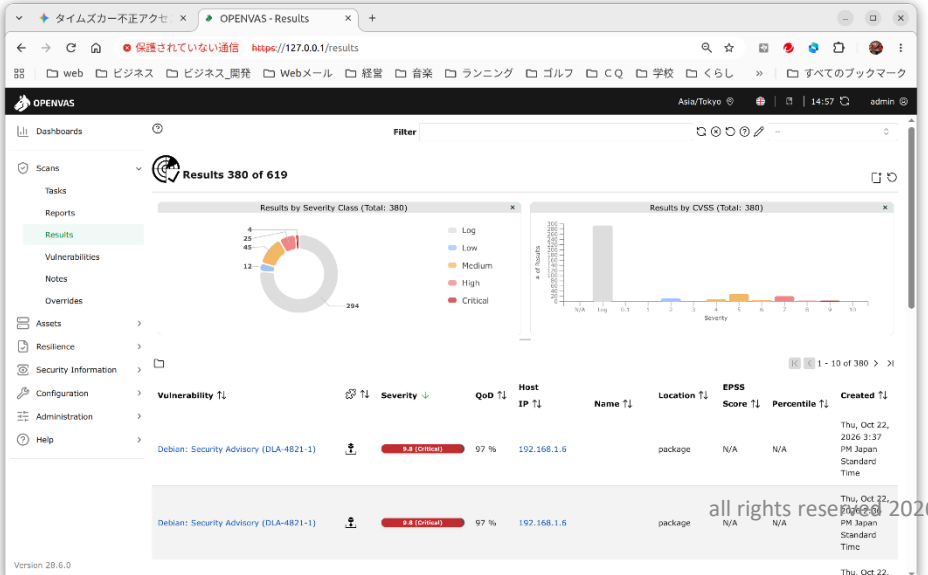


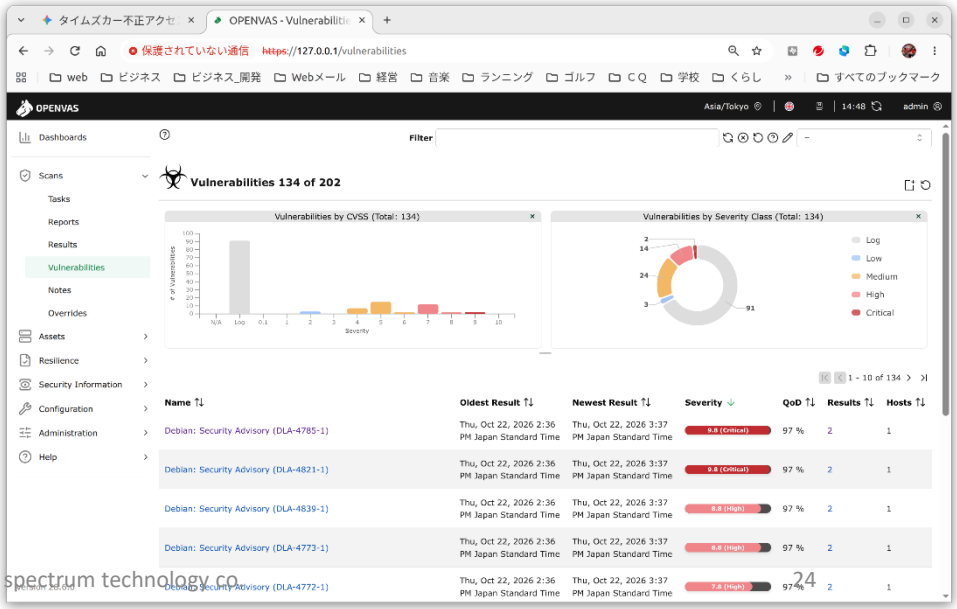


all rights reserved 2026 spectrum technology co.

1.openvas
③運用

- 起動
- スキャンフロー
- スキャン・タスク設定
- スキャン結果
  - Scan>result:全脆弱性一覧
  - Scan>vul:CVE一覧

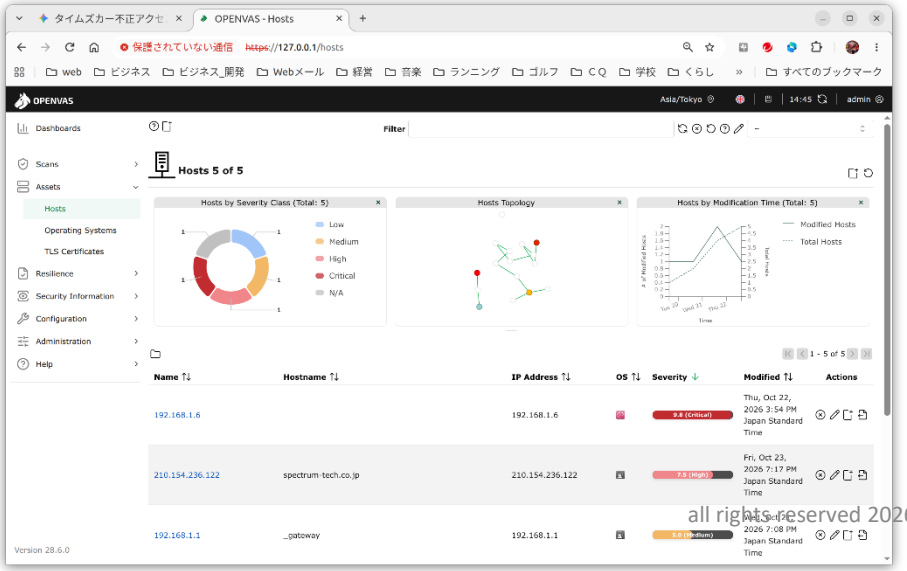


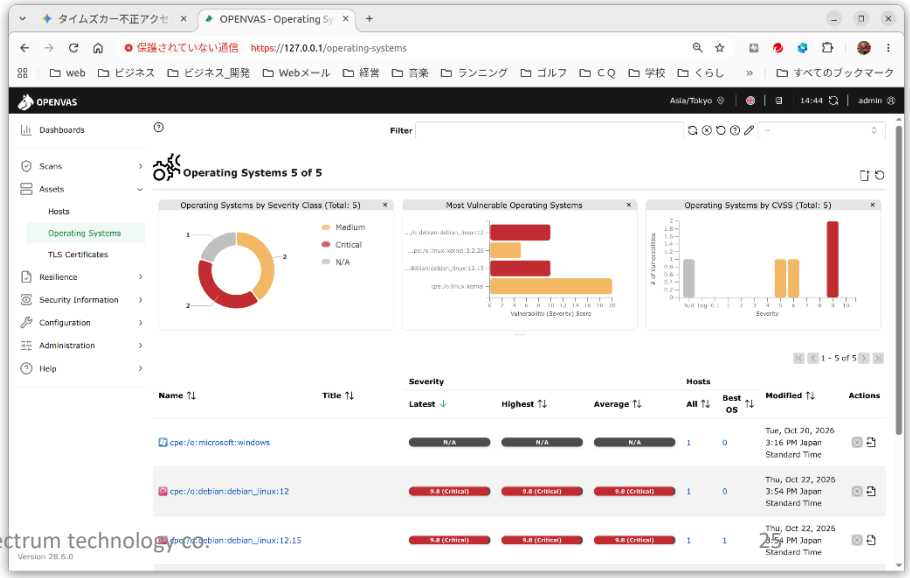


all rights reserved 2026 spectrum technology co.

1.openvas
③運用

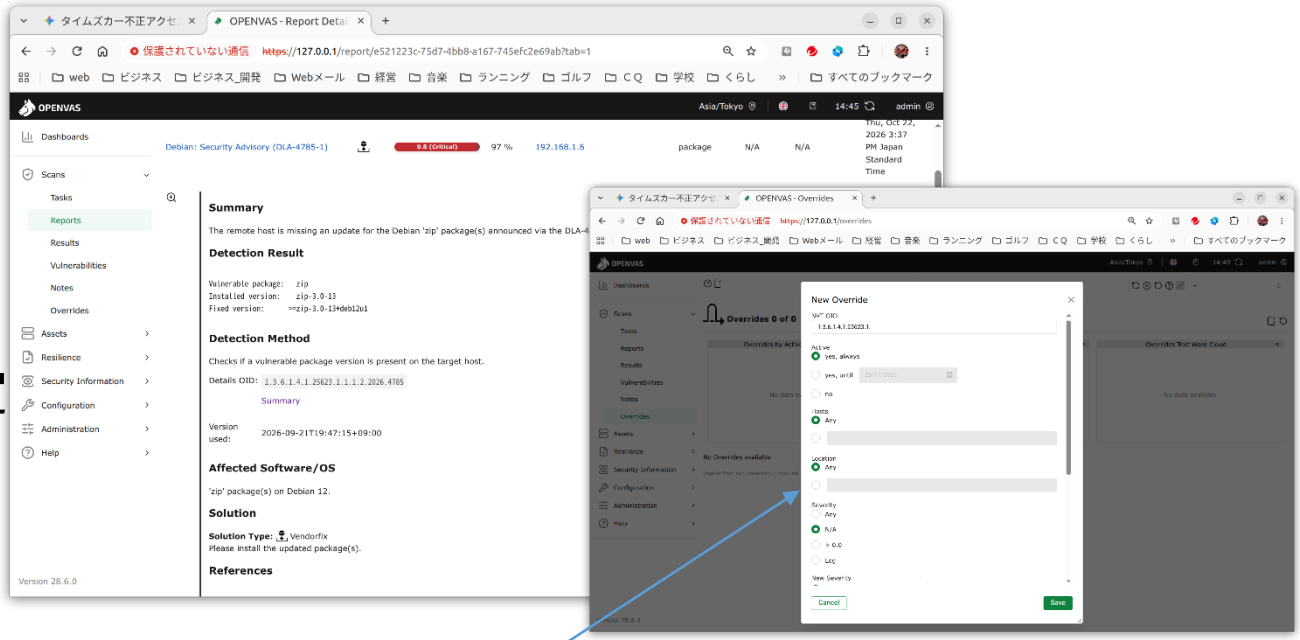
- 起動
- スキャンフロー
- スキャン・タスク設定
- 資産管理
  - Aseets>host:ホスト一覧
  - Assets＞OS:OS一覧





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
- ストレージの容量改善方法はこちら

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.

3.ZAP

①概要

- 診断方法

項目	外部からの診断（パブリック/インターネット側）	内部からの診断（プライベート/社内・認証後）
想定する視点	一般のインターネットユーザー、悪意ある外部の攻撃者	社員、VPN接続者、あるいは**「ログイン認証を突破した一般・管理者ユーザー」**
アクセス経路	グローバルIPやインターネット公開URLを経由	社内LAN、VPN、またはIP制限・Basic認証の内側
ZAPでのアプローチ	ログイン画面、お問い合わせフォーム、誰でも見られる公開ページに対する網羅的なスパイダー（クローリング）と攻撃テスト。	**ログイン後の管理画面、マイページ、ロール（権限）ごとの機能**に対して、各権限のアカウントでログインしたセッション（Cookieやトークン）をZAPに保持させてスキャンする。
主な目的	外部から不正侵入されるWeb上の入口（SQLiやXSSなど）の発見。	権限昇格の不備、内部ユーザーによる不正操作、セッション管理の脆弱性の発見

- 対象機器

カテゴリ	主な対象（ターゲット資産）	ZAP診断におけるポイント・注意点
① 公開Webサイト・ECサイト	コーポレートサイト、ECストア、オウンドメディア、ポータルサイト	不特定多数がアクセスするため、フォーム入力値の検証不備（XSS, SQLインジェクション）やディレクトリ構造の露呈を重点的にチェック。
② 認証・会員管理システム	ログイン画面、パスワード再設定機能、マイページ、会員登録フォーム	ブルートフォース耐性、セッションIDの予測可能性、CSRF、ログアウト後のセッション破棄不備などをチェック。
③ 業務Webアプリケーション	社内向けERP、グループウェア、チケット管理システム、受発注システム	社内ネットワーク（内部診断）からアクセスし、権限のないユーザーが他の機能やデータを閲覧・操作できてしまう「アクセス制御の不備（BOLA/IDOR等）」を検証。
④ Web API・モバイルアプリ用バックエンド	REST API、GraphQLエンドポイント、スマートフォンアプリの通信先API	GUIを持たないため、APIスキーマ（OpenAPI/Swagger定義等）をZAPに読み込ませるか、Proxy経由でリクエストをキャプチャしてファジングを実施。
⑤ 管理者向けコンソール（管理画面）	CMS（WordPress等の /wp-admin/）の管理画面、各種システムのバックオフィス	外部から推測されにくいURLになっているか、強固な多要素認証（MFA）やIP制限がかかっているか、脆弱性が放置されていないかを診断。

all rights reserved 2026 spectrum technology co.

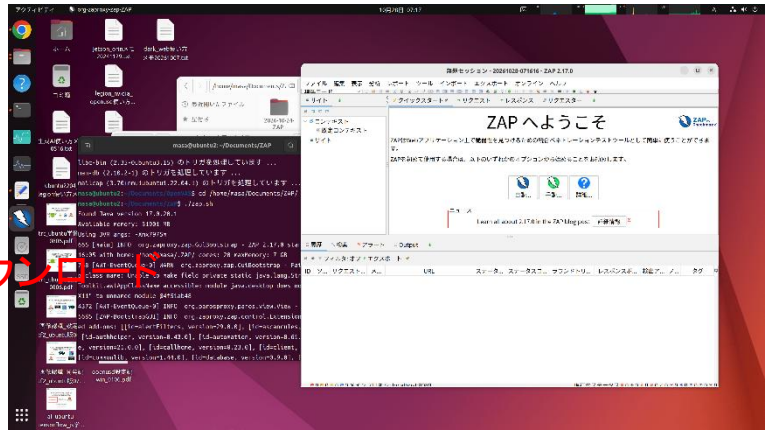
コマンド入力
cd /home/masa/Documents/ZAP
./zap.sh

3.ZAP
②設定、実施：外部診断

- インストール

  $ cd /home/masa/Documents/ZAP配下へ

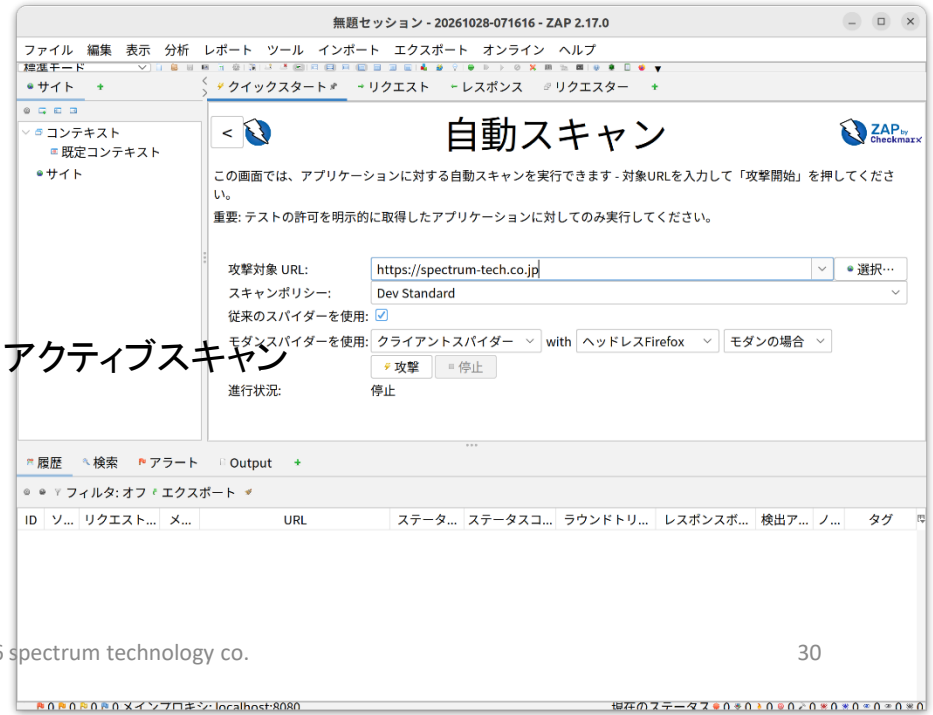
  https://www.zaproxy.org/download/ linux版をダウンロード



- 起動

  $ ./zap.sh

- 設定、実施
  - zapブラウザ自動起動
  - 自動（外部診断）＞ターゲットWeb入力
  - 攻撃スタート
  - スパイダーでスクロールして、全url検知し、アクティブスキャン
  - 対象によりますが、2時間位

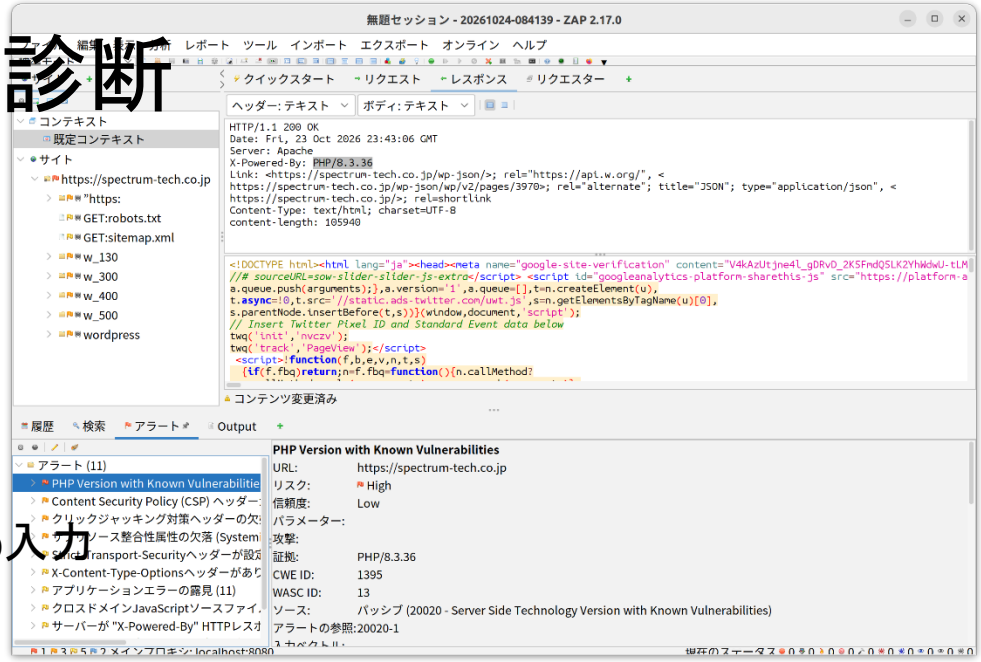


サイトに負荷がかかります、自社サイトのみで、負荷の少ない時間に実施のこと

all rights reserved 2026 spectrum technology co.

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

3.ZAP
②設定、実施：外部診断



- インストール
- 起動
- 設定、実施
  - zapブラウザ自動起動
  - 自動（外部診断）＞ターゲットWeb入力
  - 攻撃スタート
  - スパイダーでスクロールして、全url検知し、アクティブスキャン
  - 対象によりますが、2時間位
  - スキャン終了後、アラーム確認（リスク：高、中、小）
  - 上記は、10/22発生のphpの脆弱性で、対策実施後もアラームしています。内容はよく確認しましょう。わからない場合は、生成AIに問い合わせするのもよいでしょう

all rights reserved 2026 spectrum technology co.

Spectrum Technology

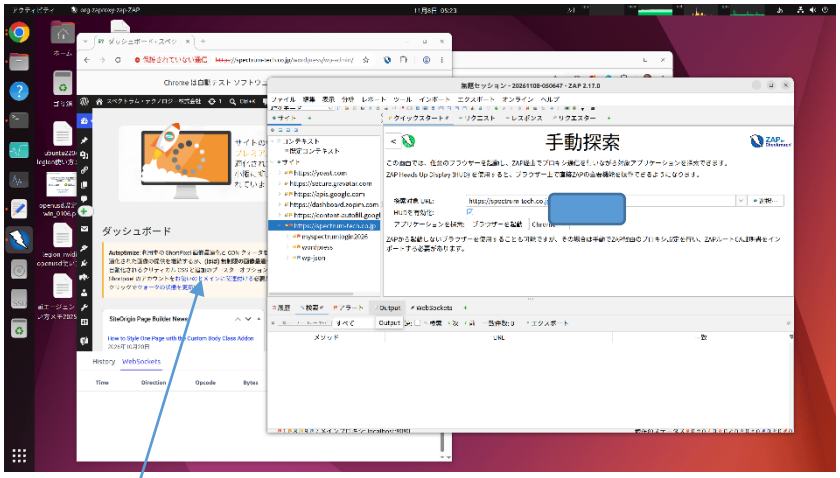
コマンド入力
cd /home/masa/Documents/ZAP
./zap.sh

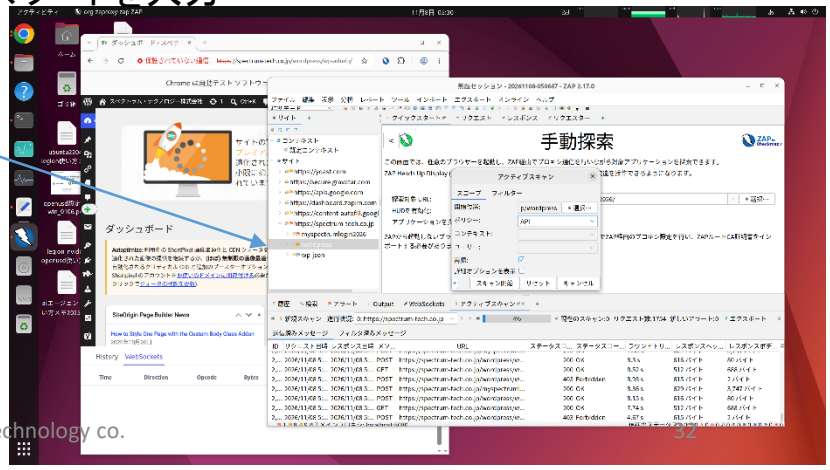
3.ZAP
②設定、実施：内部診断

- インストール
- 起動

  $ ./zap.sh

- 設定、実施
  - zapブラウザ自動起動
  - 手動（内部診断）＞ターゲットWeb（ログイン）入力
  - HUDを有効化：チェック
  - ログイン画面が起動、id,パスワード、ワンタイムパスワードを入力
  - zapに左横のタブに該当のurl（例wordpress)が表示
  - 右クリックで攻撃＞アクティブスキャンを実施
  - アクティブスキャンが開始、経過が%表示
  - 対象によりますが、1時間位





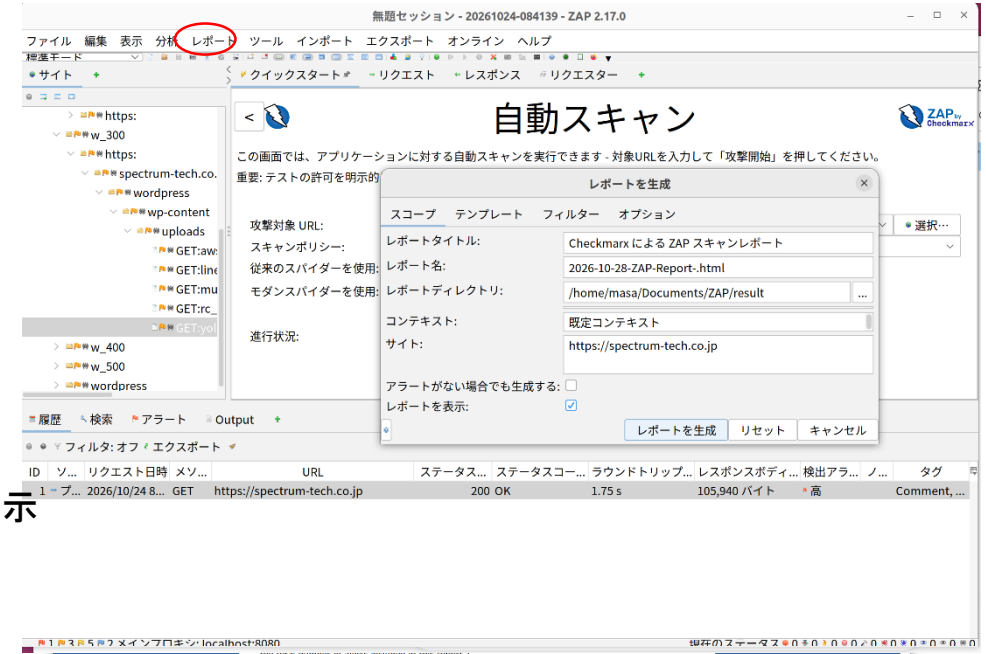
all rights reserved 2026 spectrum technology co.

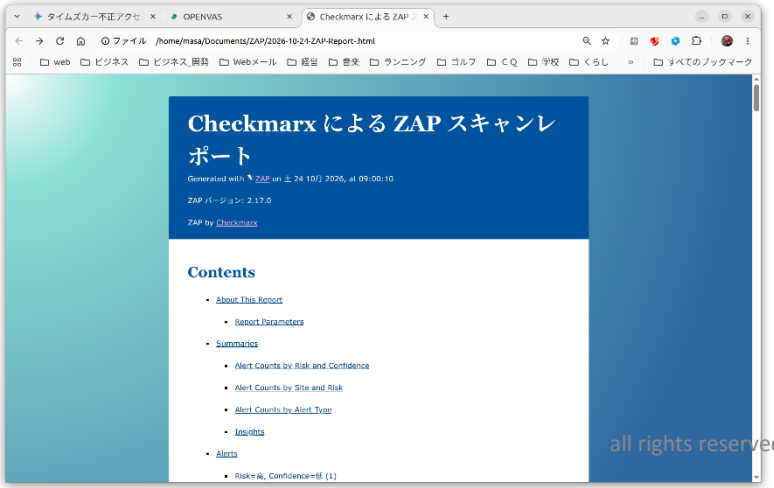
Spectrum Technology

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

3.ZAP
③結果：外部診断

- 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





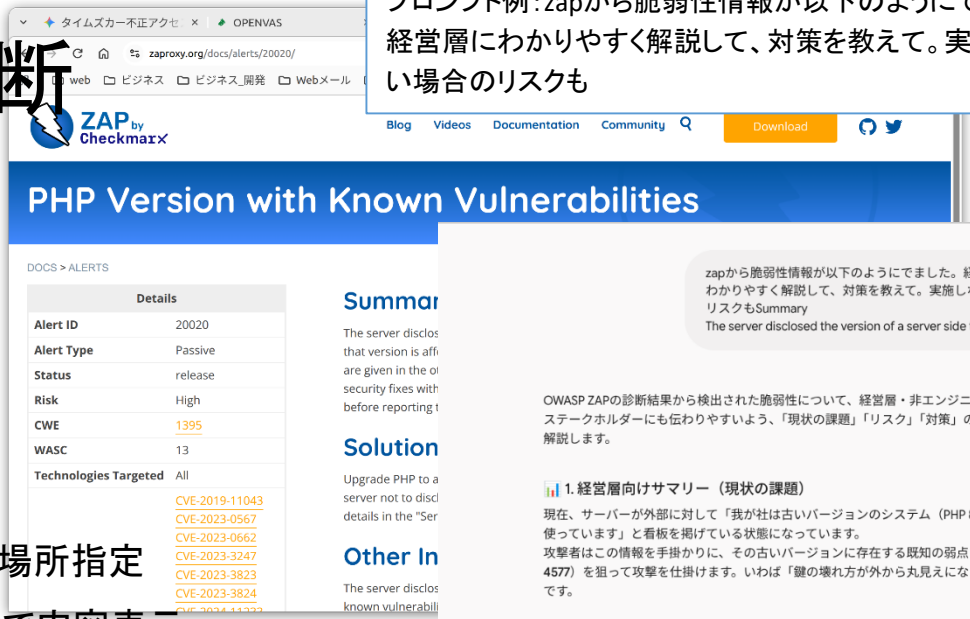


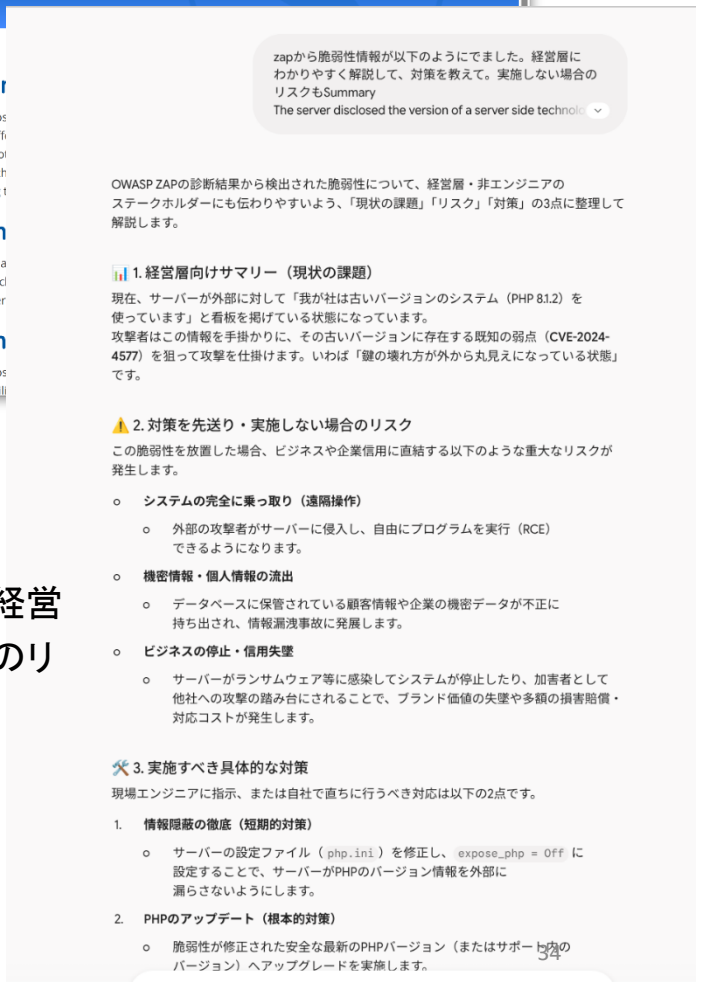
all rights reserved 2026 spectrum technology co.

3.ZAP
③結果：外部診断

- 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
  - 脆弱性確認し、個別の対策がでます。
  - 生成AIに問い合わせするのもよいでしょう。
  - プロンプト例：zapから脆弱性情報が以下のようにでました。経営層にわかりやすく解説して、対策を教えて。実施しない場合のリスクも

コマンド入力
cd /home/masa/Documents/ZAP
./zap.sh
プロンプト例：zapから脆弱性情報が以下のようにでました。経営層にわかりやすく解説して、対策を教えて。実施しない場合のリスクも





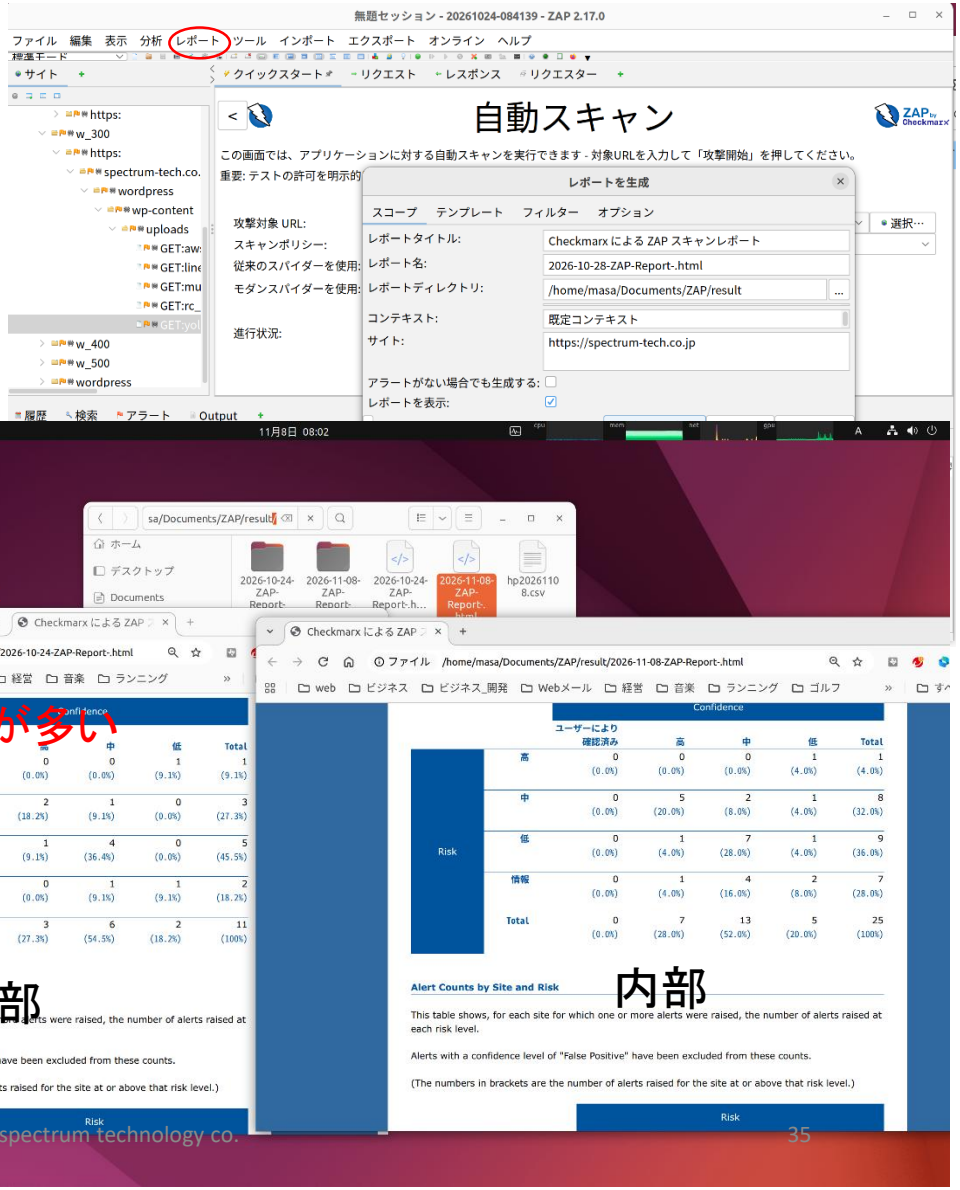
all rights reserved 2026 spectrum technology co.

Spectrum Technology

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

3.ZAP
③結果：内部診断

- 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
  - 内部診断の方が外部診断より件数が多い



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.