

| 次世代サイバー攻撃対策ソリューション

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 + Gemini APIによる全自動セキュリティ運用

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

なぜ今、中小企業に高精度な脆弱性診断が必要か

個人情報漏洩
多発

セキュリティ専門人材の不足

診断結果の英訳理解や優先順位付けが困難で放置リスクが発生。

従来ツールの高いコストハードル

商用ツールは高額であり、予算の限られた中小企業には導入困難。

本ツールの導入効果

0人手、**約2000円/月**(*1運用費)

Gemini AIによる日本語解釈&自動運用

診断結果の抽出から Slack 通知・Google Sheets 記録まで全自動化を実現。

*1)約80回/月スキャンを想定

脆弱性診断ツール 全体像

ハードウェア

CPU



16GB RAM

gpu搭載が望ましい

+

USBメモリ



OS

ubuntu



USBメモリ(ubuntu版)
販売価格:55,000円(税込)

USBメモリ(vmware版)
販売価格:66,000円(税込)

通知関係



windows環境でも動作

脆弱性診断系



OpenVAS

Open Vulnerability Assessment Scanner



自動管理系

make



Google Sheets

AI系



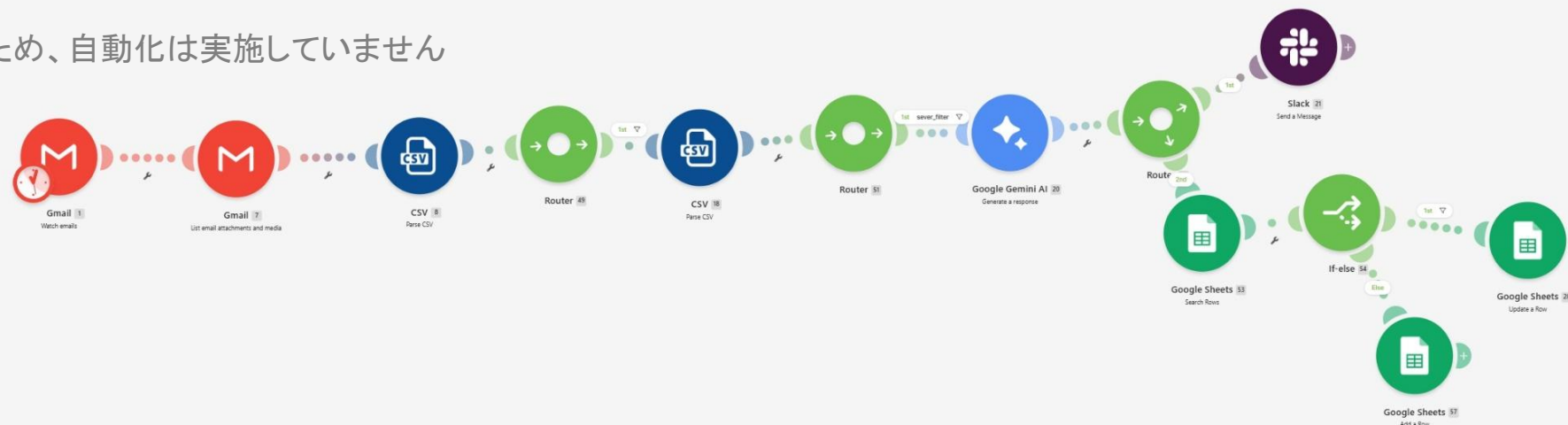
お客様準備

弊社提供

ソリューションの全体像とシームレス連携

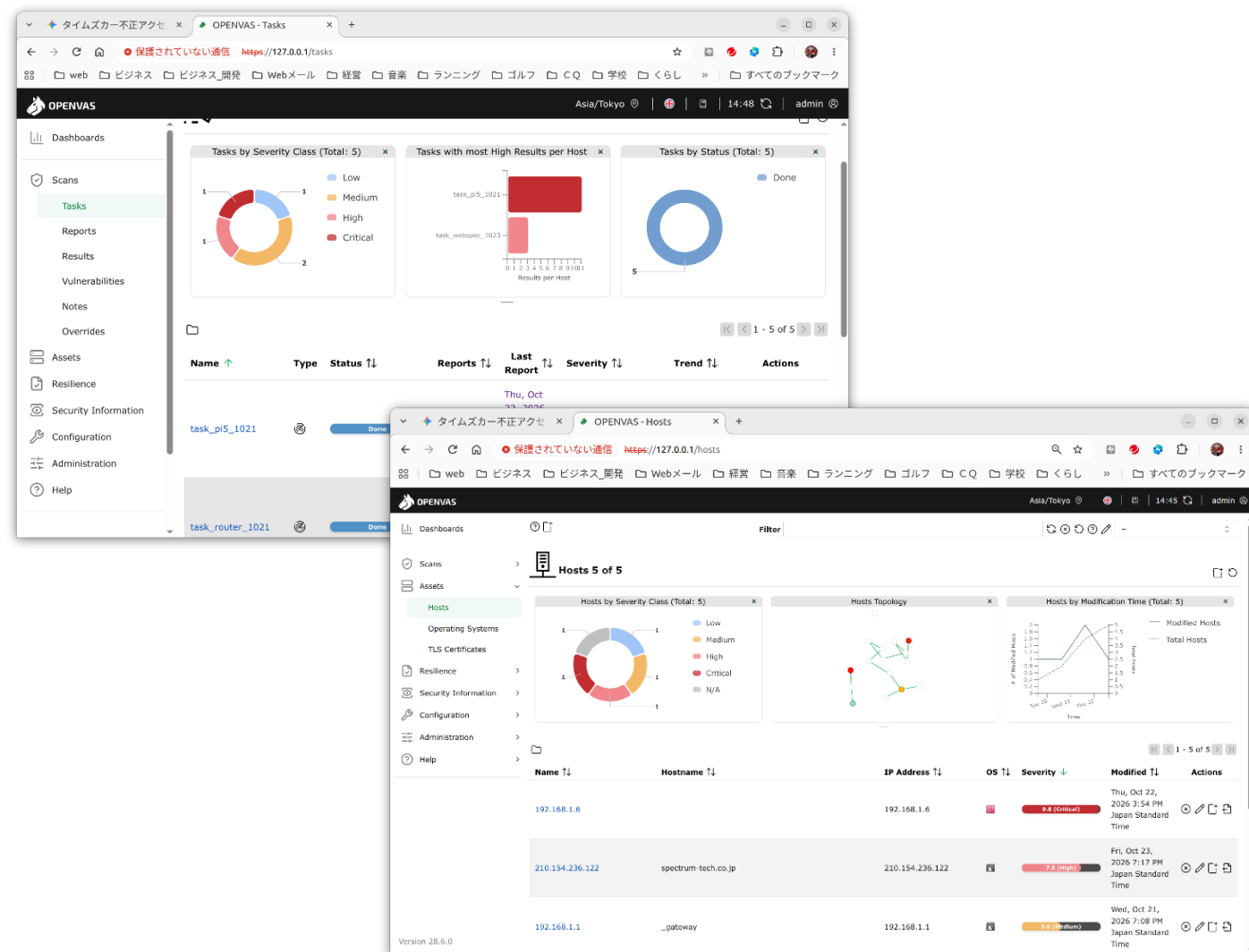


*1)ZAPは件数が少ないため、自動化は実施していません



OpenVAS : 網羅的なネットワーク・サーバー・クライアント診断

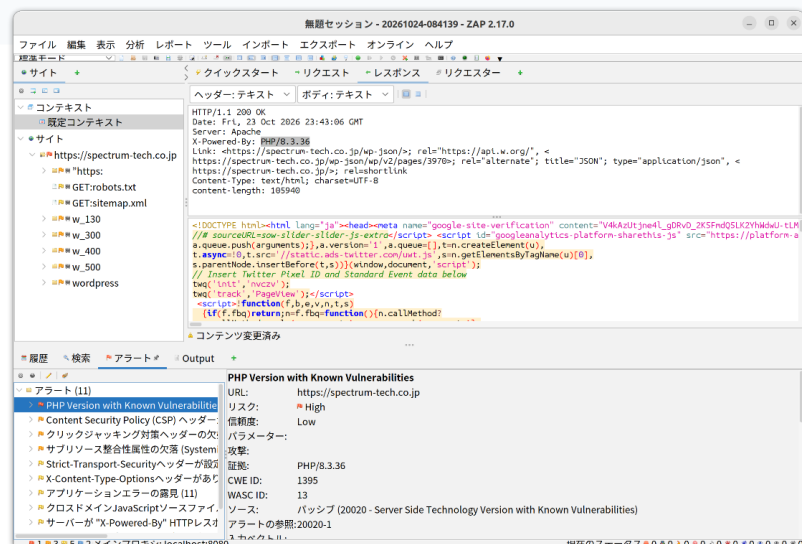
- 1 数万件以上のNVTデータベース
CVE等の最新セキュリティ情報を常時自動更新。
- 2 CVSSに基づくリスクスコアリング
危険度スコアで今優先すべき対策を明確化。
- 3 認証スキャンによる詳細検査
SSH/SMB認証設定でOS内部の既知バグも検出。



OWASP ZAP : Webアプリケーション特化スキャン

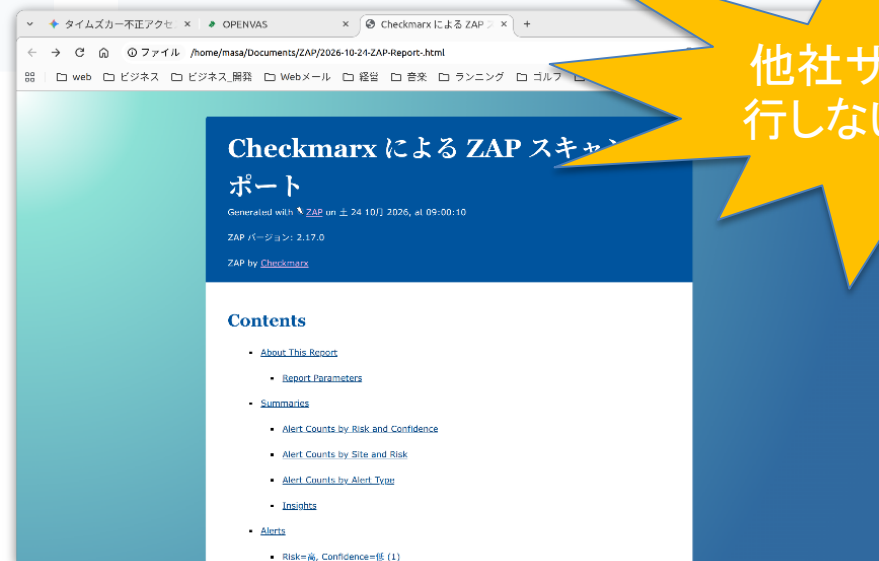
インフラ・NW層診断 (OpenVAS)

- ✓ 対象: クライアント、サーバーOS、ネットワーク機器
- ✓ 検知: 不正開放ポート、ミドルウェア脆弱性
- ✓ 定期実行: 定常監視による予防保守



Webアプリ層診断 (OWASP ZAP)

- ✓ 対象: 自社Webサイト、顧客向けシステム
- ✓ 検知: SQLインジェクション、XSS、認証不備
- ✓ 自動、手動: 自動又は手動スキャンを選択



他社サイトには実行しないでください

Gemini AIによる分かりやすい要約レポート例

オリジナル

date	ip	cvss	severity	NVT name	summary	solution	os
2026-10-22T06:54:40.000Z	192.168.1.6	9.8	Critical	Debian: Security Advisory (DLA-4785-1)	The remote host is missing an update for the Debian 'zip' package(s) announced via the DLA-4785-1 advisory.	Please install the updated package(s).	zip' package(s) on Debian 12.

Gemini ai出力

test 内を検索する

☆ # openvas

メンバーを招待する

メッセージ canvas を追加する +

対象環境: 192.168.1.6 (OS内部パッケージ: perl) / CVSS: 9.8 (Critical)

【緊急セキュリティレポート】 放置厳禁の脆弱性が検出されました

1. どこが危ないか (概要)
サーバー内の「動画や音声処理する部品」に重大な欠陥があり、悪意のあるデータを読み込ませただけで外部から内部に土足で侵入されてしまう状態です。

2. 放置した場合のリスク
***サーバーの乗っ取り・遠隔操作:** 攻撃者にシステムを完全に掌握され、不正アクセスの踏み台にされる恐れがあります。
***機密情報の漏洩:** サーバー内に保存されている顧客情報や社内データが外部へ流出する可能性があります。
***ウイルス感染・業務停止:** ランサムウェア（身代金要求型ウイルス）を仕込まれ、システムが暗号化・破壊されて業務が全面停止するリスクがあります。

3. 今すぐやるべき対策アクション

【緊急度: 高】
Debian OSの対象ソフトウェア（gst-plugins-bad1.0 パッケージ）を最新版へアップデート（セキュリティ修正パッチの適用）してください。

【担当者への指示】
社内システム担当者、または保守ベンダーへ至急以下の対応を依頼してください。
「対象サーバー（192.168.1.6）にて、Debianセキュリティ勧告（DLA-4839-1）の修正パッケージ（gst-plugins-bad1.0）の適用作業、および適用後の動作確認を実施してください（作業イメージ: `apt update && apt --only-upgrade install ...` 等によるパッケージ更新と関連プロセスの再起動）。」

対象環境: 192.168.1.6 / CVSS: 8.8 (High)

ハード概要

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
必要なハードウェア: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

ソフト概要

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

導入後の運用ポイント・推奨サイクル

段階的なスキャン頻度

導入当初は毎日、運用安定後は週1回へ最適化。

データベース更新

最新CVE情報を定期同期し未知のリスクに対処。

進捗管理と修復確認

対策実施日をGoogle Sheetへ記録し次回確認。

コスト管理

Gemini apiは従量制です。
制限を設けるなど、注意してください

openvas											
ファイル 編集 表示 挿入 表示形式 データ ツール 拡張機能 ヘルプ											
メニュー 100% 123 デフォルト											
id_key											
1	id_key	date	ip	cvss	severity	NVT name	summary	solution	os	対応	進捗
2										【緊急セキュリティレポート】放置 ★ 1. どこが危ないか (概要) サーバーの頭脳の中で働く基本プログラム ★ 2. 放置した場合のリスク **外部からのサーバー乗っ取り** 悪意 **機密情報・個人情報漏洩** サーバ **ランサムウェア感染・システム全停 ★ 3. 今すぐやるべき対策アクション 【緊急度: 最高 (即時対応)】 Debian OSの管理パッケージ (perl) を 【担当者への指示】 1. "社内IT担当者または保守ベンダーへ" IPアドレス "192.168.1.6" のサーバ 2. "作業手順イメージ" ・業務影響の少ない時間帯を調整のう ・パッケージ更新コマンド (apt-get i 対象環境: 192.168.1.6 (OS内部バツ未対応	
3	192.168.1.6_Dr2026-10-22T06:192.168.1.6				9.8 Critical	Debian: Security	The remote host Please install the perl package(s)			【緊急セキュリティレポート】放置 ★ 1. どこが危ないか (概要) サーバー内でファイルを圧縮・解凍す ★ 2. 放置した場合のリスク 深刻度スコアが "9.8" "10.0" と最高レ **サーバーの完全な乗っ取り** 外部の **機密情報・個人情報漏洩** 保存さ **ランサムウェア (身代金要求ウィル **他社へのサイバー攻撃の「踏み台」 ★ 3. 今すぐやるべき対策アクション 【緊急度: 高】 該当サーバーのOS (Debian) における 【担当者への指示】 社内インフラ担当者または保守ベンダー 1. 対象サーバー (192.168.1.6) にて、	

まずはお気軽にご相談ください

御社のネットワーク環境に合わせた最適な脆弱性診断・自動管理ツールの導入
をご提案いたします。

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

担当: 村上