AIWAF-VE 構築ガイド

-さくらのクラウド_AIWAF-VE-

アイティーエム株式会社
アプリケーション・セキュリティ事業本部

2025/3/25

目次

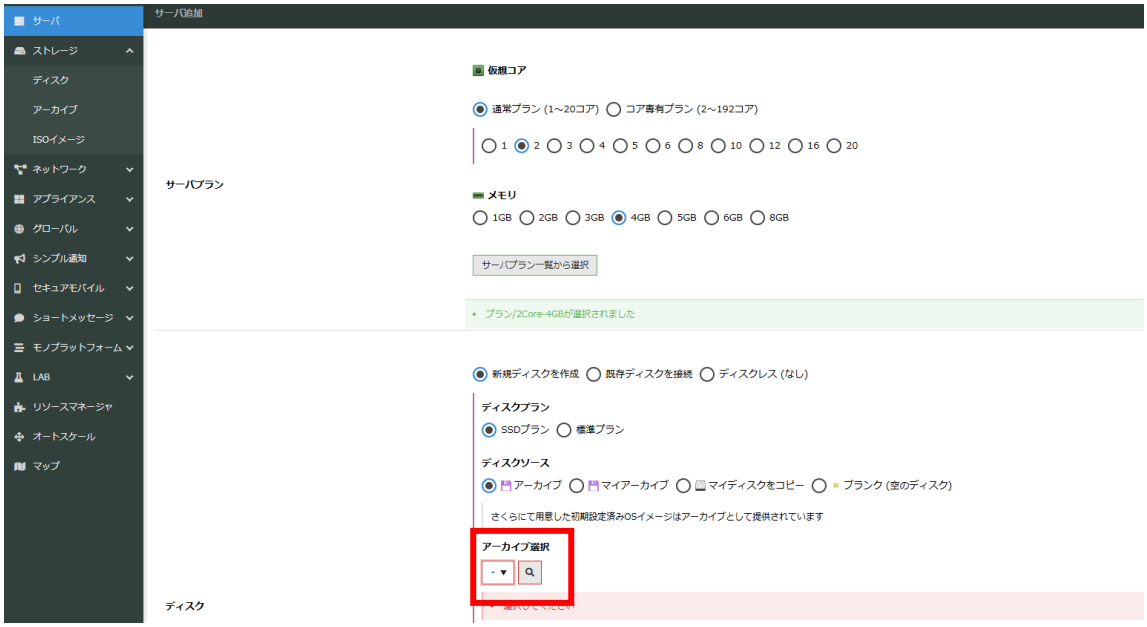
1. はじめに

本ガイドは、さくらのクラウド上で AIWAF-VE を構築する方法について具体的に説明します。

2. AIWAF-構築

2.1 AIWAF-VE をデプロイする。

- さくらのクラウドのサーバメニューから AIWAF-VE パブリックアーカイブ用して AIWAF-VE の VM を生成する。
- VM 生成時、プランに適合する vCore,Memory を選択する。

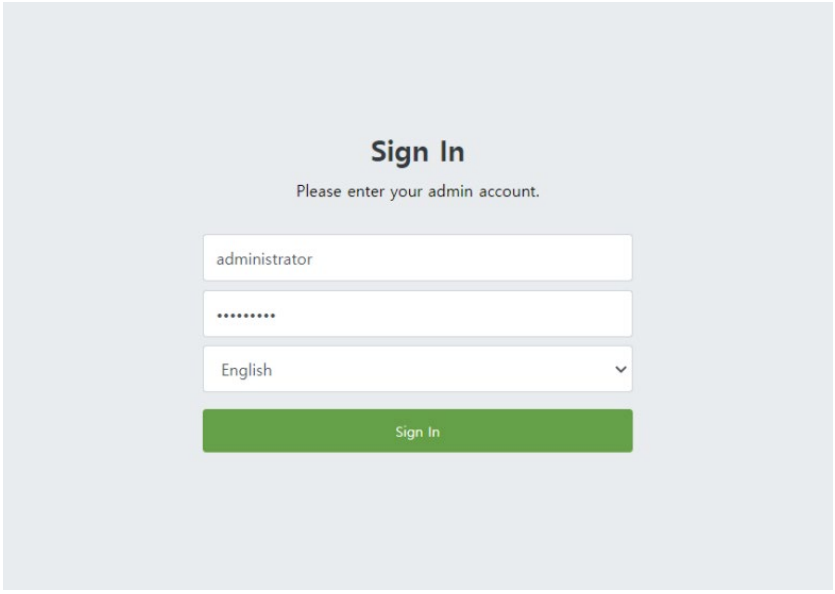


※アーカイブ名：AIWAF-VE for さくらのクラウド v5.0.2

2.2 Web ユーザーインターフェースにアクセスする(UI)

- 生成された VM の IP を確認し、WEB ブラウザで下記のように入力して AIWAF GUI にアクセスする。

  ※https://[VM に割り当てされた IP]:222



接続画面(ログイン)

- サインインする前に言語を選択する。（サポートされている言語：英語、日本語、韓国語）
- 提供された ID とパスワードでログインする。（初期設定 ID：administrator、PW：_appleader）
- 初のログイン後はセキュリティのため、デフォルトの ID・パスワードを変更し、アクセスを許可する IP を指定してください。(パスワード変更メニューの場所: 環境設定 → 管理者設定 →「変更」ボタンクリック)

2.3 タイムゾーンと言語の設定

- タイムゾーンの設定を行う。

  環境設定 > システム設定 > タイムゾーン設定

- 言語の設定を行う。

  環境設定 > 製品設定 > 言語設定

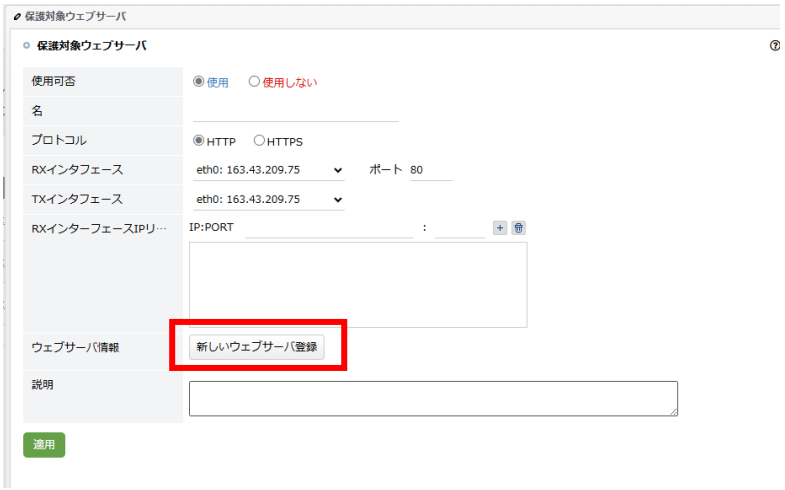
2.4 パターンと位置情報 DB のアップデート

- [パターンアップデート]にアクセスするには、ポリシー設定 → デフォルト設定 → パターンアップデート設定 → オンライン パターンアップデートに移動する。
- チェックボックスに「現在のパターン バージョンは最新バージョンです」と表示されている場合、最新のパターンが適用されていることを示す。

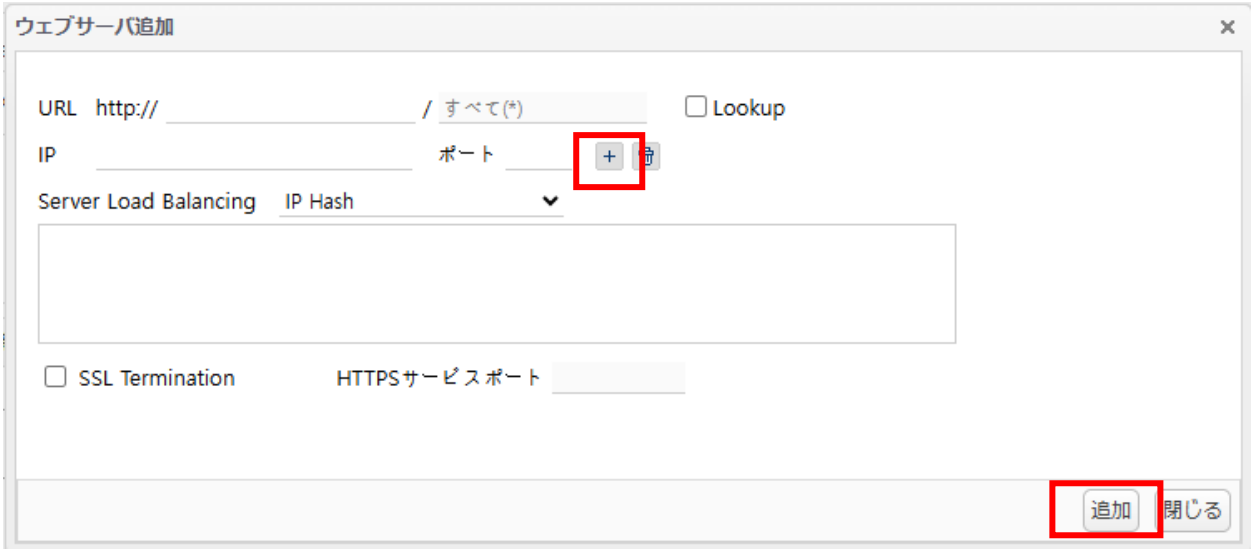
2.5 保護対象の WEB サーバ登録

- HTTP WEB サーバの登録する

「ポリシー設定」→「Admin ポリシー」→「保護対象ウエブサーバ」に移動し、「ルール追加」をクリックする。



- Web サーバの名を入力し、「新しい Web サーバーを登録」をクリックする。
- 保護される URL、IP アドレス、ポート番号を入力して'＋'をクリックする
- 動的 IP を持つサーバの場合は、エイリアス登録に Lookup オプションを使用する。



- 入力した値が正しく適用されていることを確認したら、「追加」をクリックして続行する。

- 入力 WEB サーバ情報を確認した後、「適用」をクリックして Web サーバの登録は完了です。

  ※HTTPS サーバ登録は「証明書ファイル」、「秘密鍵ファイル」の登録する必要あり。

2.6 ポリシー適用

- Web サーバを登録し、必要な各ポリシーを変更した後は、 [Admin ポリシー] セクションで [ポリシーの適用] を押下し、ポリシーを適用する。

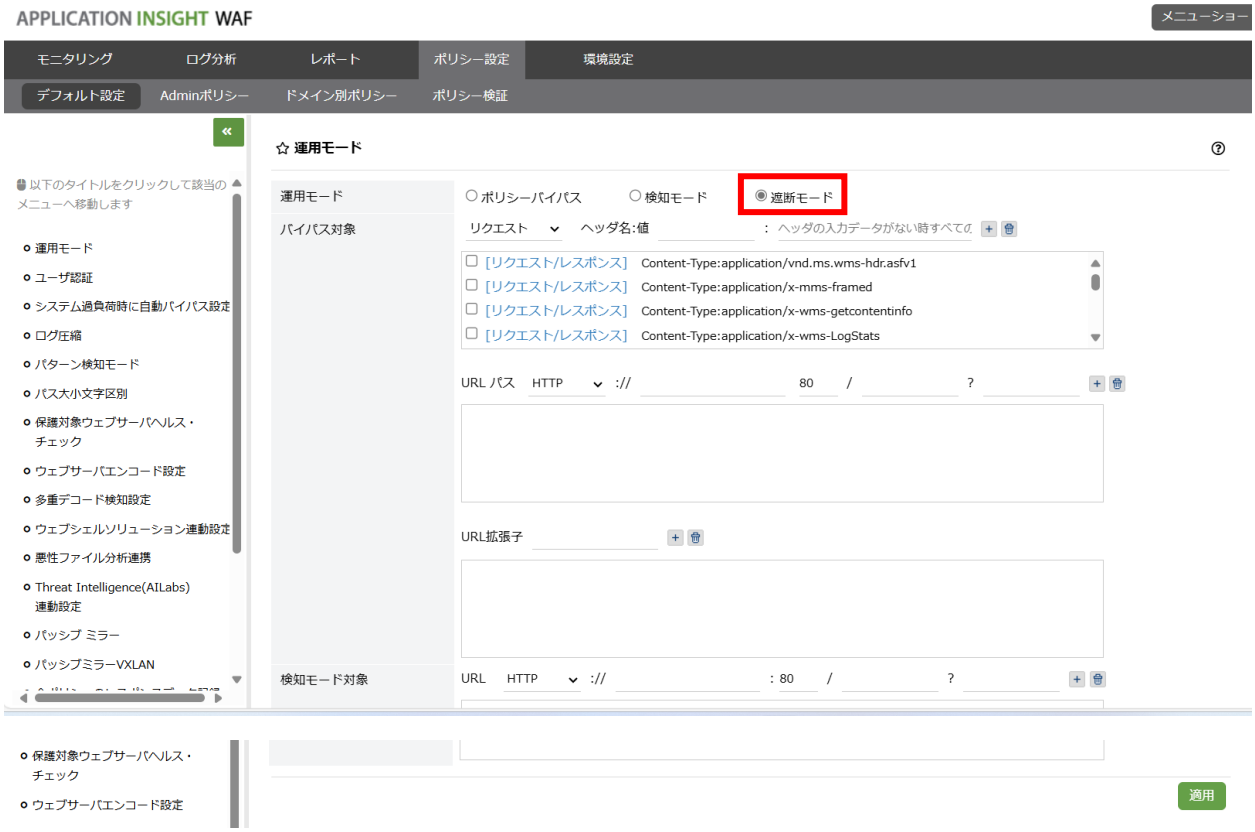
  ※各ポリシーの設定方法については、Admin マニュアル　5．ポリシー設定を参照してください。

- 登録された WEB サーバに必要なポリシーに項目を設定し「ポリシー適用」をクリックする。(ポリシー適用をクリックしないと適用されない。ポリシー適用により、以前のポリシーはバックアップされる)

- アクセスするには：ポリシー設定 → Admin ポリシー → ポリシー適用/キャンセル →「ポリシーの適用」をクリックします。

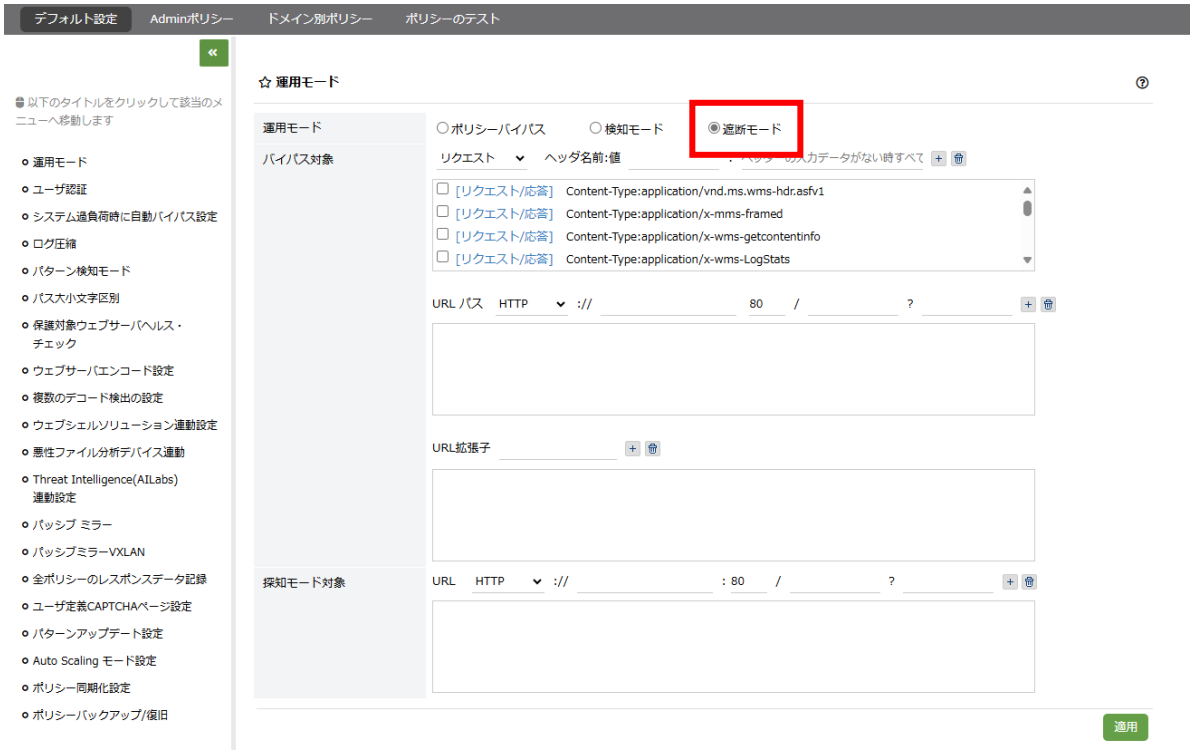
2.7 セキュリティポリシー遮断モード構成

デフォルト設定が検知モードになっている為、遮断機能を適用する為にはモード変更が必要。

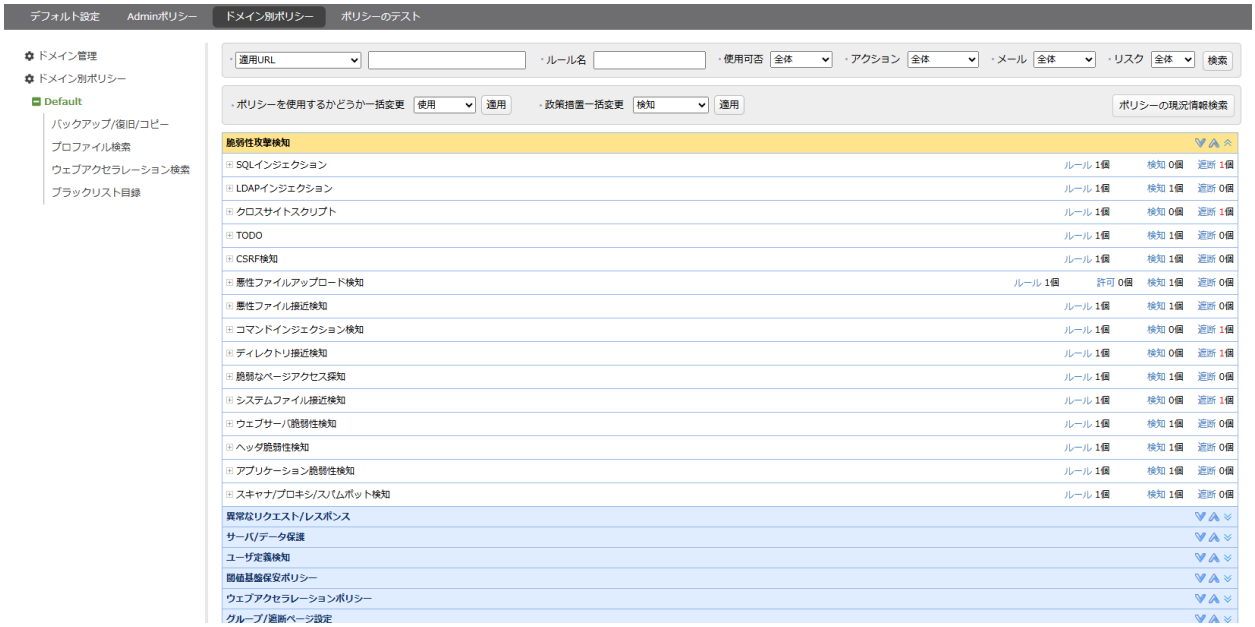


ポリシー設定 → デフォルト設定 → 運用モードに移動し「遮断モード」を選択する。

選択後「適用」を押下し続行する。



- 遮断モードを完全に適用するには、ドメインごとに個別のセキュリティポリシーの検出設定をブロックに変更する必要
- ポリシー設定 → Admin ポリシー → ポリシーの適用/キャンセル →「ポリシーの適用」をクリックします。
- 「デフォルト」をクリックして、各セキュリティポリシーを管理する。(デフォルトページは、ユーザーが登録した Web ページに適用される基本ルール設定を指します(5-1、5-2)。)

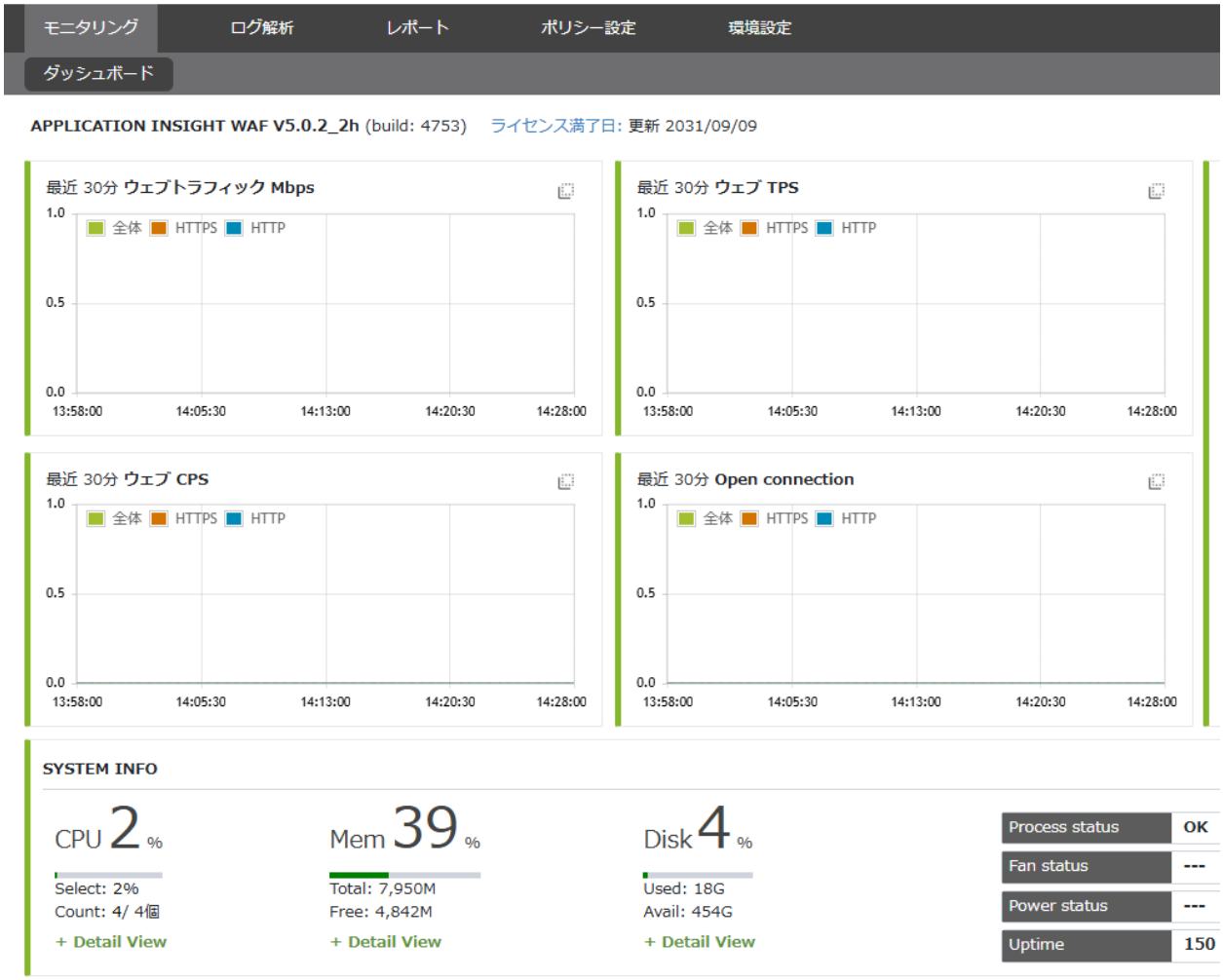


- すべてのデフォルトルールは「検出」に設定されている。変更したいルールをクリックすると検知情報が表示される。

- ルールの右側にあるアクションタブの赤い盾は、「遮断」モードを表します。これをクリックすると「検知」に変わる(緑盾)。
- 必要に応じ、遮断・検知の選択を行う
- 設定が終われば、「適用」押して設定を完了する。

3. 設定の完了

- モニタリング－＞ ダッシュボードでトラフィック情報を確認する。



4. AIWAF-VE のテスト

- 設定された WAF 保護機能い対しテストを行う。

4.1 STEP 1：テストトラフィックを AIWAF-VE にリダイレクトする。

- Windows 管理者としてメモ帳を起動します。
- メモ帳で、[ファイル] に移動して [開く] を選択し hosts ファイルを開く。

  ※Windows の hosts ファイルのパス: C:¥Windows¥System32¥drivers¥etc¥hosts
- hosts ファイルに Web サーバのドメイン名と AIWAF-VE の IP を登録する。

  例: [AIWAF-VE IP] [ドメイン] (例: 192.168.10.110 www.yourdomain.com)

- 登録が hosts ファイルに Web サーバのドメイン名と AIWAF-VE の IP を登録する。
- hosts ファイルを保存する。

※当手順はクライアント側の OS が Windows の場合を想定しています。
他 OS のクライアントでテストされる場合は OS に準じホスト設定行ってください。

4.2 STEP 2：サンプルトラフィックを AIWAF-VE に送信する。

- インターネットブラウザを開く。
- URL アドレス入力に次の値を入力。

例＞URL: http://www.yourdomain.com/?monitorapp=monitorapp

4.3 STEP 3：攻撃検出の検証。

- ダッシュボードから、ログ分析＞検知ログ移動し攻撃の検出記録を確認する。

5. まとめ

本ガイドに従い、AIWAF-VE の初期導入が可能となります。

詳細な設定に対する問い合わせについては、サービスのサポート担当へ問い合わせお願い致します。

以上