

# 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

<b>1. はじめに</b> .....	<b>2</b>
<b>2. AIWAF-構築</b> .....	<b>2</b>
2.1 AIWAF-VE のデプロイする。.....	2
2.2 Web ユーザーインターフェースにアクセスする(UI).....	2
2.3 タイムゾーンと言語の設定.....	3
2.4 シグネチャーと位置情報 DB のアップデート.....	4
2.5 保護対象の WEB サーバ登録.....	4
2.6 ポリシー適用.....	6
2.7 セキュリティポリシー遮断モード構成.....	7
<b>3. 設定の完了</b> .....	<b>9</b>
<b>4. AIWAF-VE のテスト</b> .....	<b>10</b>
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。.....	10
4.2 STEP 2 : サンプルトラフィックを AIWAF-VE に送信する。.....	11
4.3 STEP 3 : 攻撃検出の検証。.....	11
<b>5. まとめ</b> .....	<b>12</b>

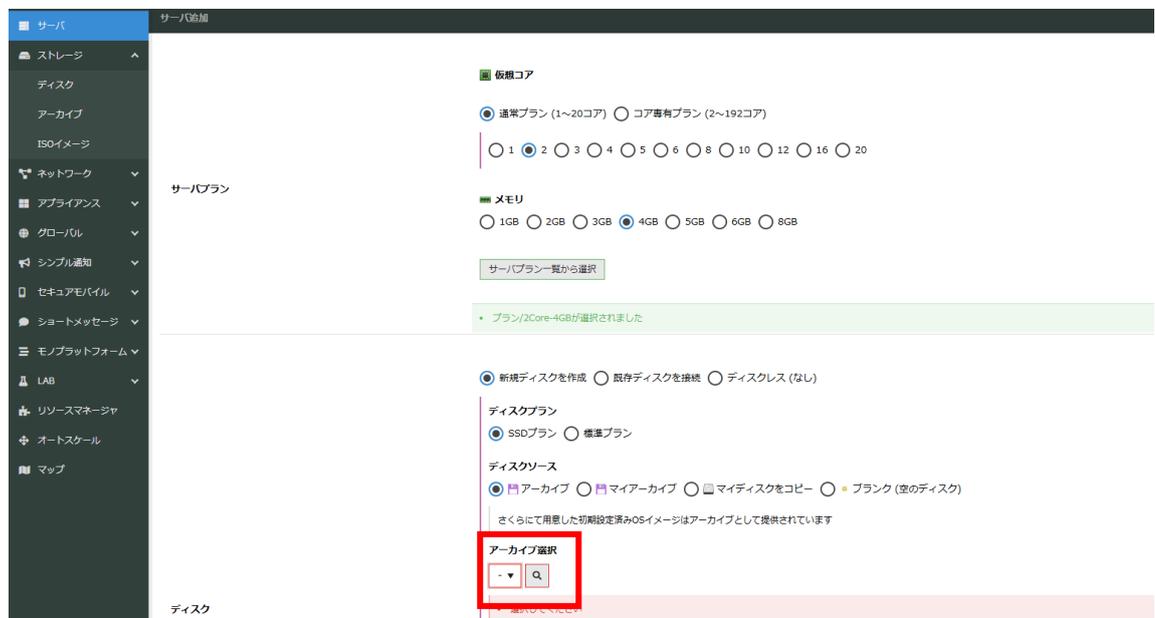
## 1. はじめに

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。

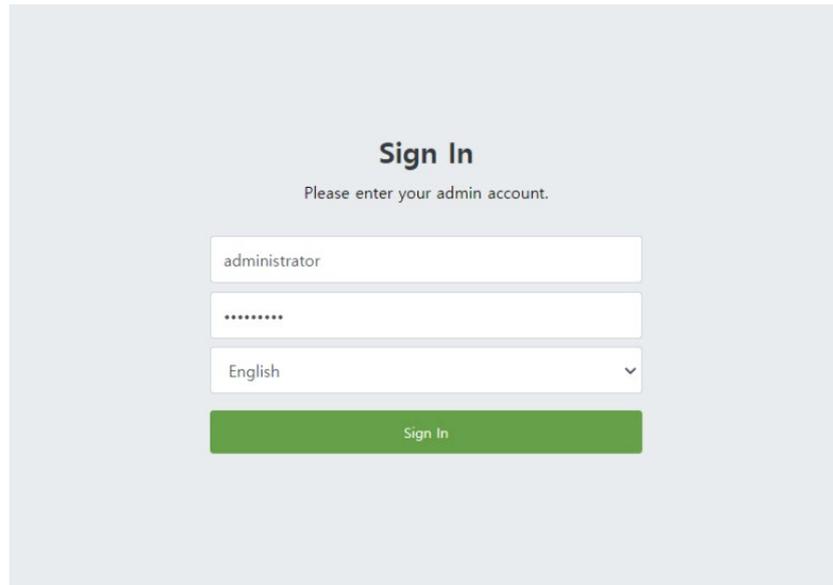


※アーカイブ名 : AIWAF-VE for さくらのクラウド v5.0.2

### 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](https://[VMに割り当てされたIP]:222)



Sign In

Please enter your admin account.

administrator

\*\*\*\*\*

English

Sign In

### 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



モニタリング ログ解析 レポート ポリシー設定 環境設定

管理者設定 システム設定 NIC設定 製品設定 ログ管理 サービス制御

◀

以下のタイトルをクリックして該当のメニューへ移動します

- IP 設定
- メール設定
- Telegram通知設定

### ☆ タイムゾーン設定

現時刻	Fri Mar 21 23:35:32 JST 2025
タイムゾーン	Asia/Tokyo

- 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

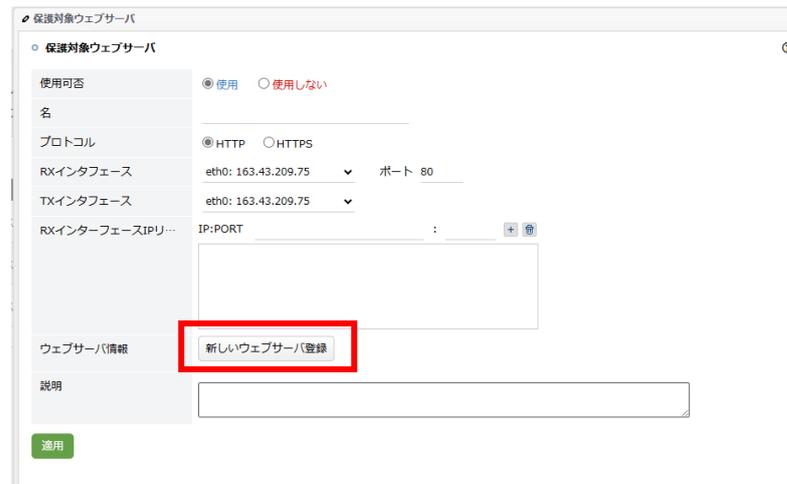
- [パターンアップデート]にアクセスするには、ポリシー設定 → デフォルト設定 → パターンアップデート設定 → オンライン パターンアップデートに移動する。
- チェックボックスに「現在のパターン バージョンは最新バージョンです」と表示されている場合、最新のパターンが適用されていることを示す。



## 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」→「保護対象ウェブサーバ」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。

The screenshot shows the 'Admin Policies' configuration page. The left sidebar lists various policy categories: Admin Policies, Protection Target Web Servers, IP Policies, DoS Policies, Priority Policies, URL Rewrite Policies, URL Encryption, and API Policies. The main content area is titled 'Admin Policies' and 'Policy Application/Cancel'. It contains a table with the following data:

ポリシー	変更事項
<input type="checkbox"/> 保護対象ウェブサーバ	0 件
<input type="checkbox"/> IPホワイトリスト	0 件
<input type="checkbox"/> IPブラックリスト	0 件
<input type="checkbox"/> セッション攻撃検知	0 件
<input type="checkbox"/> Slow DoS攻撃検知	0 件
<input type="checkbox"/> Slow Read攻撃検知	0 件
<input type="checkbox"/> URLアクセスルール	0 件
<input type="checkbox"/> 国別IP検知	0 件
<input type="checkbox"/> ユーザ管理	0 件
<input type="checkbox"/> ユーザ定義パターンルール	0 件
<input type="checkbox"/> 遮断ページ管理	0 件
<input type="checkbox"/> デフォルトSSL設定	0 件
<input type="checkbox"/> ヘルス・チェックURL	0 件
<input type="checkbox"/> URLリライトリクエストルール	0 件
<input type="checkbox"/> URLリライトレスポンスルール	0 件
<input type="checkbox"/> URLエンクリプション	0 件
<input type="checkbox"/> APIポリシー	0 件

At the bottom of the table, there are two buttons: 'ポリシー適用' (Apply Policy) and '以前ポリシーで復元' (Restore Previous Policy). The 'Apply Policy' button is highlighted with a red box.

- 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。

APPLICATION INSIGHT WAF

モニタリング ログ分析 レポート ポリシー設定 環境設定

デフォルト設定 Adminポリシー ドメイン別ポリシー ポリシー検証

☆ 運用モード

以下タイトルのクリックで該当のメニューへ移動します

- 運用モード
- ユーザ認証
- システム過負荷時に自動バイパス設定
- ログ圧縮
- パターン検知モード
- パス大小文字区別
- 保護対象ウェブサーバヘルス・チェック
- ウェブサーバエンコード設定
- 多重デコード検知設定
- ウェブシェルソリューション連動設定
- 悪性ファイル分析連携
- Threat Intelligence(AILabs) 連動設定
- パッシブミラー
- パッシブミラー-VXLAN

運用モード

ポリシーバイパス  検知モード  遮断モード

リクエスト ヘッダ名:値 : ヘッダの入力データがない時すべて

- [リクエスト/レスポンス] Content-Type:application/vnd.ms.wms-hdr.asfv1
- [リクエスト/レスポンス] Content-Type:application/x-wms-framed
- [リクエスト/レスポンス] Content-Type:application/x-wms-getcontentinfo
- [リクエスト/レスポンス] Content-Type:application/x-wms-LogStats

URL パス HTTP :// : 80 / ?

URL拡張子

検知モード対象 URL HTTP :// : 80 / ?

適用

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。

デフォルト設定 Adminポリシー ドメイン別ポリシー ポリシーのテスト

◀

以下のタイトルをクリックして該当のメニューへ移動します

- 運用モード
- ユーザ認証
- システム過負荷時に自動バイパス設定
- ログ圧縮
- パターン検知モード
- パス大小文字区別
- 保護対象ウェブサーバ(ヘルス・チェック)
- ウェブサーバエンコード設定
- 複数のデコード検出の設定
- ウェブシェルソリューション運動設定
- 悪性ファイル分析デバイス運動
- Threat Intelligence(AllLabs) 運動設定
- バックアップ ミラー
- バックアップミラー-VXLAN
- 全ポリシーのレスポンスデータ記録
- ユーザ定義CAPTCHAページ設定
- パターンアップデート設定
- Auto Scaling モード設定
- ポリシー同期化設定
- ポリシーバックアップ/復旧

☆ 運用モード

運用モード  ポリシーバイパス  検知モード  遮断モード

バイパス対象 リクエスト ヘッダ名前:値

- [リクエスト/応答] Content-Type:application/vnd.ms.wms-hdr.asfv1
- [リクエスト/応答] Content-Type:application/x-mms-framed
- [リクエスト/応答] Content-Type:application/x-wms-getcontentinfo
- [リクエスト/応答] Content-Type:application/x-wms-LogStats

URL パス HTTP :// \_\_\_\_\_ : 80 / \_\_\_\_\_ ? \_\_\_\_\_

URL拡張子 \_\_\_\_\_

検知モード対象 URL HTTP :// \_\_\_\_\_ : 80 / \_\_\_\_\_ ? \_\_\_\_\_

適用

デフォルト設定 Adminポリシー **ドメイン別ポリシー** ポリシーのテスト

ドメイン管理

ドメイン別ポリシー

**Default**

ポリシー適用/キャンセル

<input type="checkbox"/>	ドメイン	変更事項
<input type="checkbox"/>	Default	0件

総数: 1件

ポリシー適用 以前ポリシーで復元

- 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。))

デフォルト設定 Adminポリシー ドメイン別ポリシー ポリシーのテスト

ドメイン管理  
ドメイン別ポリシー  
Default  
バックアップ/復旧/コピー  
プロファイル検索  
ウェブアクセラレーション検索  
ブラックリスト目録

適用URL  ルール名  使用可否 全体 アクション 全体 メール 全体 リスク 全体 検索

ポリシーを使用するかどうか一括変更 使用 適用 政策措置一括変更 検知 適用 ポリシーの現状情報検索

脆弱性攻撃検知	ルール	検知	遮断
SQLインジェクション	ルール 1個	検知 0個	遮断 1個
LDAPインジェクション	ルール 1個	検知 1個	遮断 0個
クロスサイトスクリプト	ルール 1個	検知 0個	遮断 1個
TODO	ルール 1個	検知 1個	遮断 0個
CSRF検知	ルール 1個	検知 1個	遮断 0個
悪性ファイルアップロード検知	ルール 1個	許可 0個	検知 0個
悪性ファイル検出検知	ルール 1個	検知 1個	遮断 0個
コマンドインジェクション検知	ルール 1個	検知 0個	遮断 1個
ディレクトリ検出検知	ルール 1個	検知 0個	遮断 1個
脆弱なページアクセス検知	ルール 1個	検知 1個	遮断 0個
システムファイル検出検知	ルール 1個	検知 0個	遮断 1個
ウェブサーバ脆弱性検知	ルール 1個	検知 1個	遮断 0個
ヘッダ脆弱性検知	ルール 1個	検知 1個	遮断 0個
アプリケーション脆弱性検知	ルール 1個	検知 1個	遮断 0個
スキャナ/プロキシ/スパムボット検知	ルール 1個	検知 1個	遮断 0個
異常なリクエスト/レスポンス			
サーバデータ保護			
ユーザ定義検知			
暗号基礎保護ポリシー			
ウェブアクセラレーションポリシー			
グループ/遮断ページ設定			

- 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。

脆弱性攻撃検知

SQLインジェクション ルール 1個 検知 0個 遮断 1個

Header表示 適用

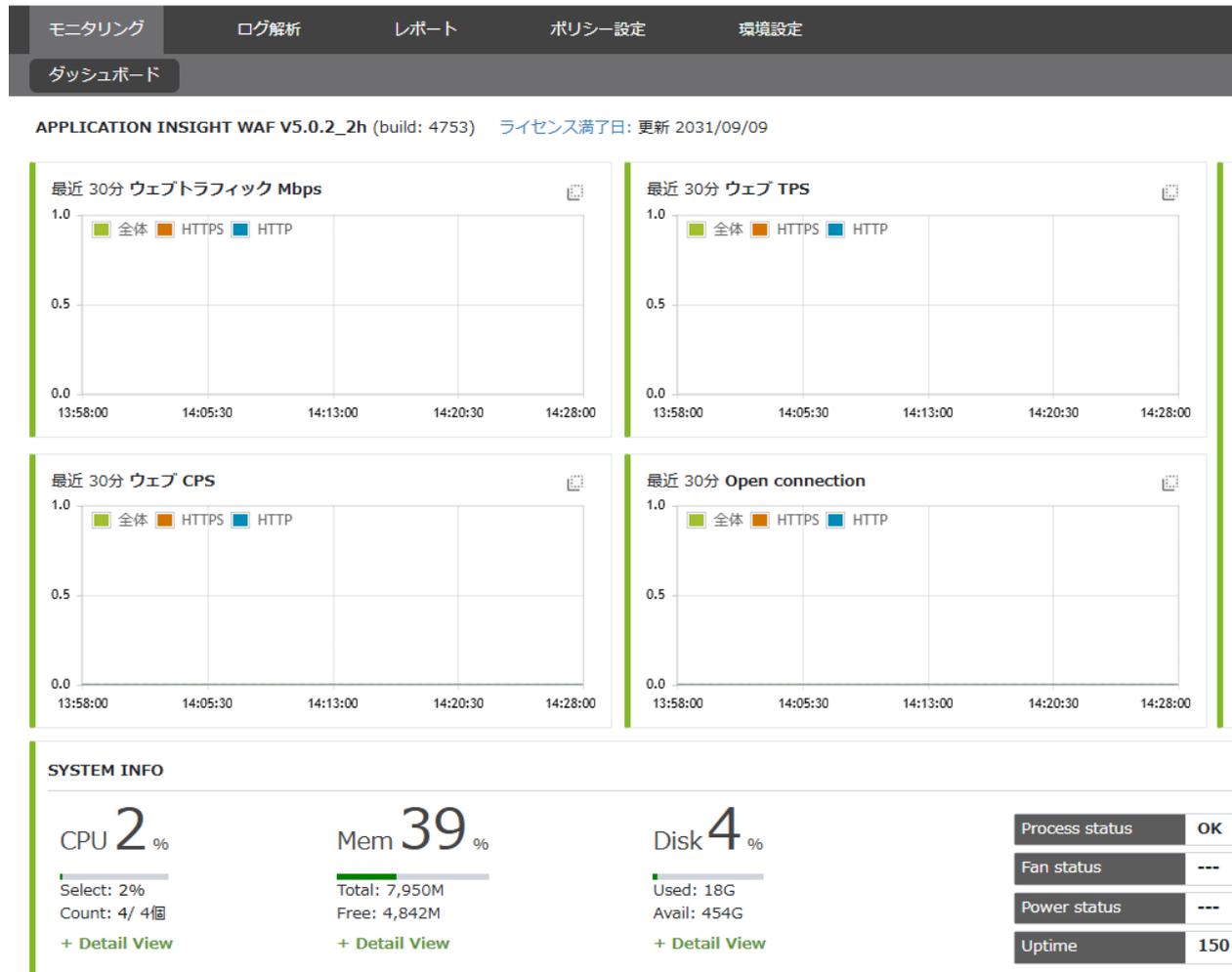
ルール名	クライアントIP	サーバURL	未使用パターン	スケジュール	説明	アクション	ログ	メール	リスク	変更
SQL Injection	全IP	全URL	0件	常時						

総数: 1件

- 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 保護機能に対しテストを行う。

### 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。

The screenshot shows the AIWAF-VE dashboard interface. At the top, there is a navigation menu with tabs: 'モニタリング', 'ログ解析', 'レポート', 'ポリシー設定', and '検出設定'. Below this, there are sub-tabs for search: '検知ログ検索', '監査ログ検索', 'ウェブサーバ状態検索', and 'ファイル分析ログ検索'. A green button labeled '全体削除' is visible. The main area shows a search filter for the period '2025-03-22 14:09 ~ 2025-03-22 14:39'. There are dropdown menus for time intervals (今日, 1週間, 1ヶ月, 2025-03-22 14:09 ~ 2025-03-22 14:39) and checkboxes for 'パターン探知モードログだけ検索' and '關心ログだけ検索'. A search button and a '検索条件の適用' button are present. Below the search area, there is a summary line: '攻撃ドメイン: - 個 | 攻撃者(Origin IP): - 個(- 個) | 攻撃件数: - 件'. There is also an '自動更新' dropdown set to '5 秒' and a '検索 15 行' dropdown. The table header includes columns: '時間', 'クライアントIP', 'Origin IP', 'サーバIP', 'ドメイン', '検知類型', 'ルール名', 'URL', 'リスク', 'アクション', and 'メール'. The table content is empty, with a message '情報がありません。' (No information found.) displayed below the header.

## 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