メンテナンス手順書

-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

2025/3/20

目次

1. はじめに

本手順書は、AIWAF-VE の定期的なメンテナンス作業を円滑に実施するための手順を示します。適切なメンテナンスを行うことで、システムの安定性とセキュリティを維持します。

メンテナンスの項目は下記の通りにする。

- パッチの適用
- バージョンアップ
- ログのバックアップ
- ポリシーチューニング(誤探知・過検知対応)
- 高負荷・パフォーマンスのチューニング

2. メンテナンスの前準備

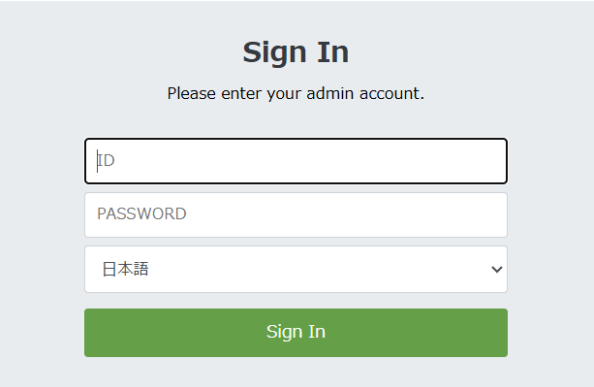
2.1 メンテナンス実施前の確認事項

- メンテナンス実施日時を事前に通知
- 影響範囲を明確化し、関係者と調整
- ログイン情報とアクセス権限の確認
- メンテナンスは主に AIWAF Web 管理コンソールと AIMANAGER WEB により行われる。

  Web 管理コンソール：AIWAF のポリシー設定、ログ、モニタリングなど全判的な機能に対する

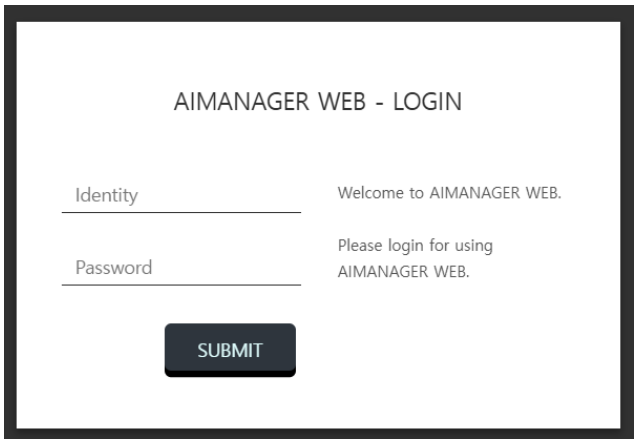
  設定及び管理する UI

  (接続 URL: https://[AIWAF IP]:222)



AIMANAGER WEB：AIWAF のエンジニアリングの為のページであり、

(接続 URL: https://[AIWAF IP]:333)

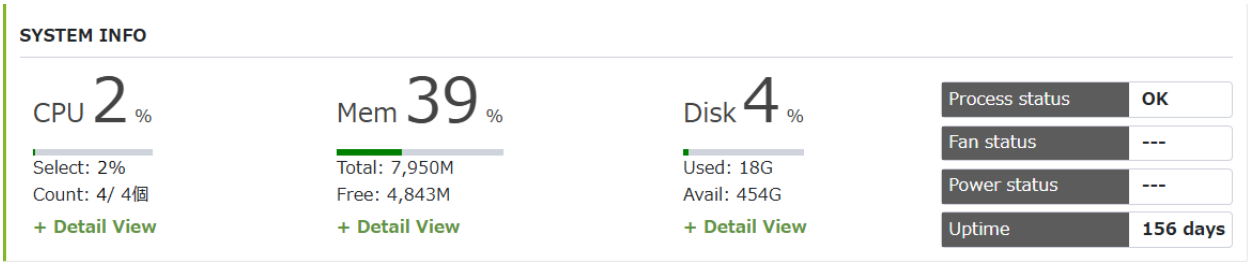


プロセス管理、セッション情報、パッチ管理などを行う。

3. メンテナンス手順

3.1 システム状態の確認

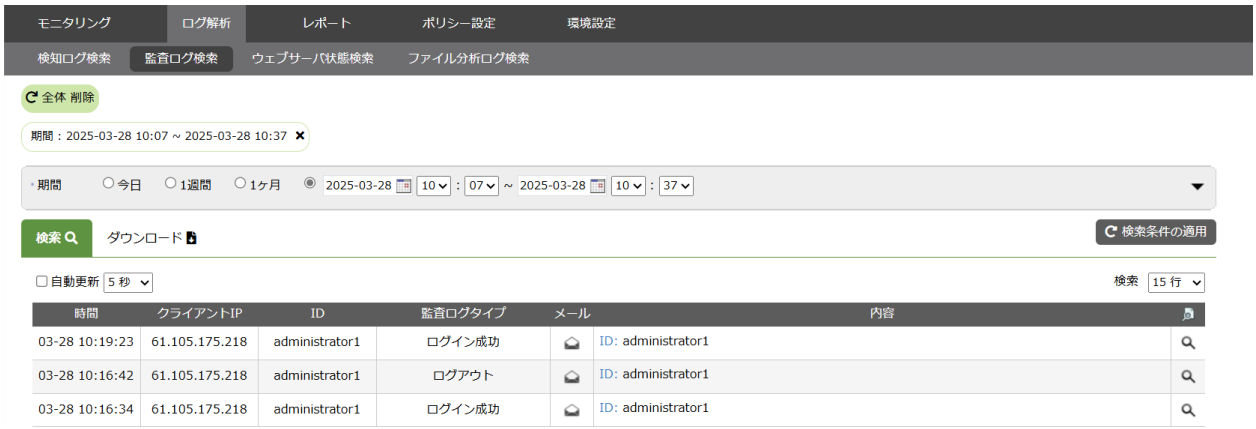
1. AIWAF Web 管理コンソールへログイン。
2. ダッシュボードで稼働状況を確認（CPU 使用率、メモリ使用量、ディスク使用量）



3. ログの確認(検知ログ、監査ログ)

- 検知ログ確認：ログ解析＞検知ログ検索

- 監査ログ確認：ログ解析＞監査ログ検索



3.2 バックアップの取得

1. 環境設定のバックアップ

- AIWAF Web 管理コンソールで[プログラム・環境設定]のバックアップ

  環境設定＞製品設定へ移動

  説明を記載し「バックアップ」ボタンをクリックでバックアップ実施

※バックアップを実施すると、バックアップリストに追加され、ダウンロード可能。

※定期バックアップ設定 mo

可能

2. ポリシーのバックアップ

- AIWAF Web 管理コンソールで[ポリシー]のバックアップを行う実施

  ポリシー設定＞ デフォールト設定＞バックアップ/復旧へ移動

  「すぐにバックアップしてから転送」をクリックすると、ポリシーがバックアップされ指定されたサーバに転送される。

※定期バックアップ設定可能

※ポリシーを復旧時には必ず、ファームウエア・Build バージョンが同一である必要がある。

3.3 ファームウェア・パッチの適用（必要時）

1. AIMANAGER UI に接続し Patch Management メニュー選択
2. Patch Management メニューから「パッチ」可能なバージョンを選択し適用を押下する。
3. パッチバージョンを確認する

4. 新しいバッチファイルを選択し、アップロードする
5. 「APPLY」をクリックし適用する
6. 再起動を行う

3.4 ログ・セキュリティ設定の最適化

1. 不要なログの削除: find /var/log/ -type f -mtime +30 -exec rm -f {} ¥;
2. ログローテーションの設定確認: /etc/logrotate.conf
3. WAF ルールの更新・最適化

- 最新の脅威情報を元にポリシーを更新。
- 設定変更後、適用テスト実施

4. メンテナンス後の確認

4.1 システムの動作確認

- Web サービスやアプリケーションの正常稼働を確認
- ログイン・アクセス制限の動作テスト
- ログを再度チェックし、エラーがないことを確認

4.2 関係者への報告

- メンテナンス完了の報告を実施
- 変更内容、問題点、対処方法を記録
- 次回のメンテナンス計画を更新

5. トラブルシューティング

5.1 サービス停止・アクセス不可

原因

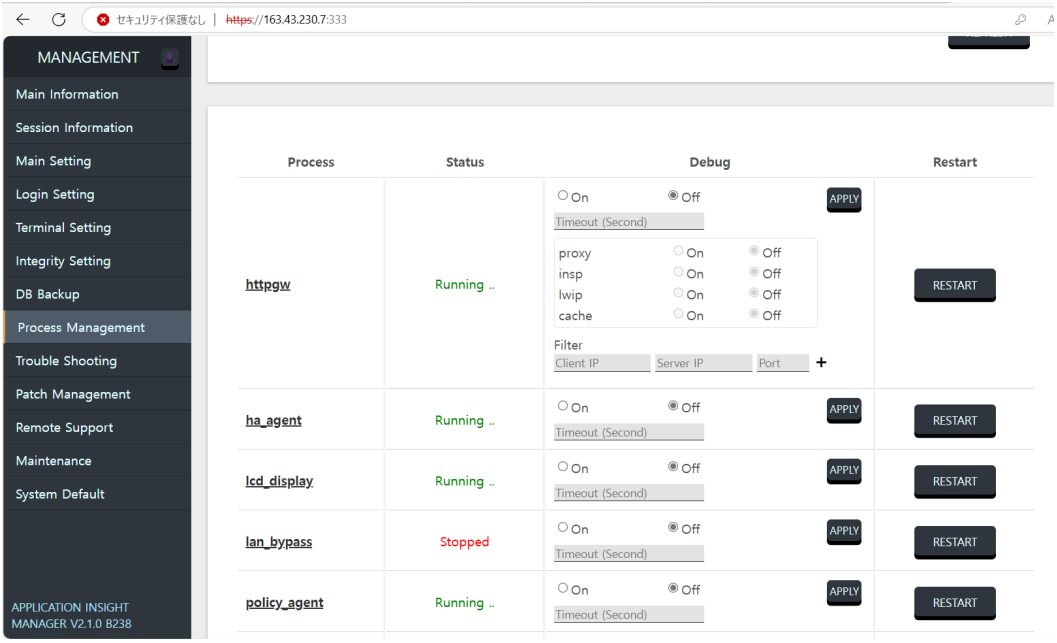
- WAF エンジンの障害
- 設定ミスによるブロック
- サーバリソースの不足
- ネットワーク障害
- アプリケーションサーバ側の問題

対処方法

① ステータス確認

- AIMANAGER ページに接続し、Process Management 状況を確認する。

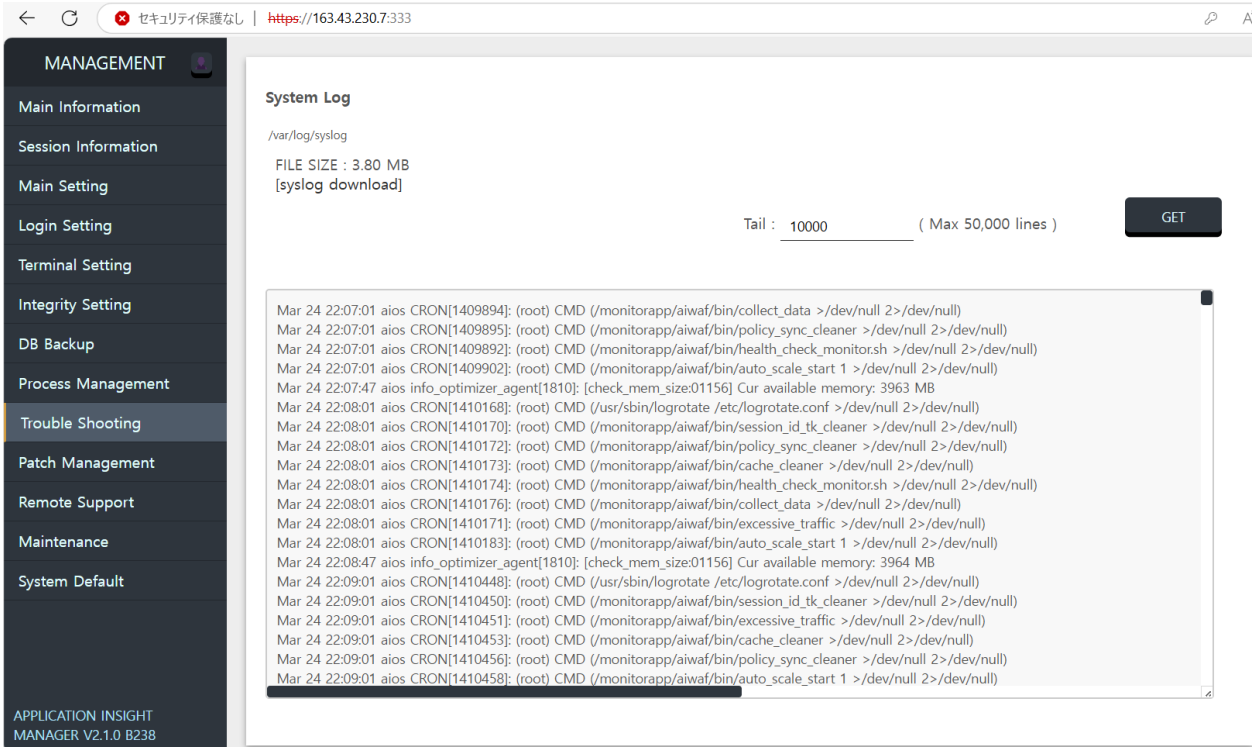
接続先 https://WAF の IP アドレス:333



② ログ確認

- システムログを確認し、システムの状況確認を行う

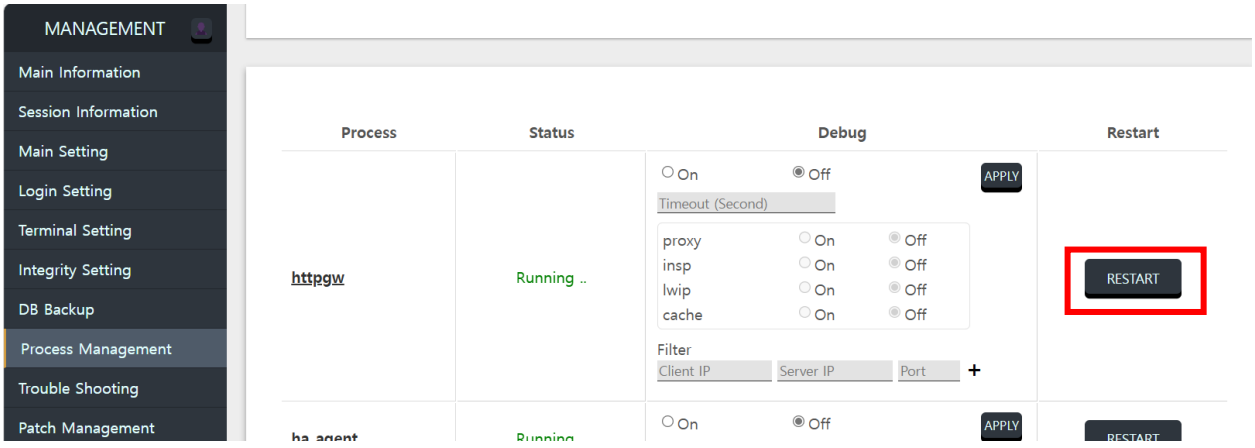
接続先 https://WAF の IP アドレス:333



③ サービス再起動

- WAF の再起動を行う

  接続先 https://WAF の IP アドレス:333

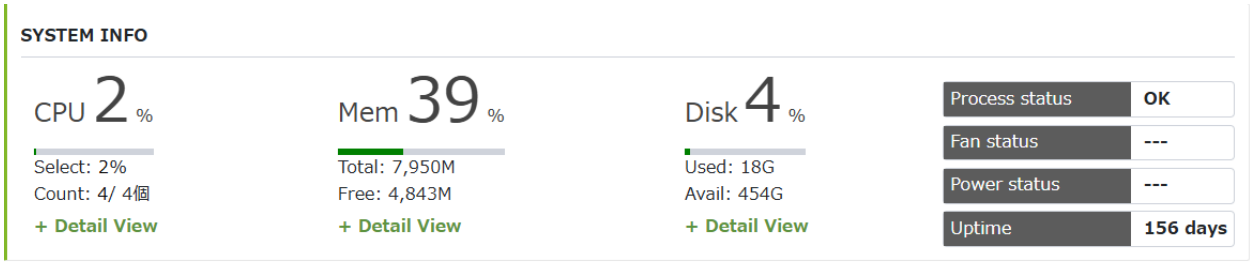


※httpgw をリスタートする。

④ リソース監視

- CPU、メモリ、ディスク使用量を確認し、過負荷が継続する場合リソース増設及びスケールアップを検討する。

Web 管理コンソール＞モニタリング＞ダッシュボード



5.2 誤検知

原因

- 正常なリクエストにに対し、攻撃と誤認された
- ルール設定に誤りがあった

対処方法

- Web 管理コンソールから、ホワイトリスト設定を確認
- 正常なリクエスト許可ルールを追加・削除を行う。

  [ポリシー設定] → [Exception Rules] から設定

5.3 検知漏れ

原因

- 攻撃パターンが最新ではない
- 必要なルールが適用されてない

対処方法

① ステータス確認

- 検知ログの分析：検知状況を確認し検知状況を確認する。

- AIWAF-VE のパターンアップデート

  ポリシー設定> 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でバージョン確認を行い、パターンアップデートを行う。

- ルールの追加

  ポリシー設定> Admin ポリシーに移動し必要なポリシーを選択し適用する

5.4 高負荷・パフォーマンス低下

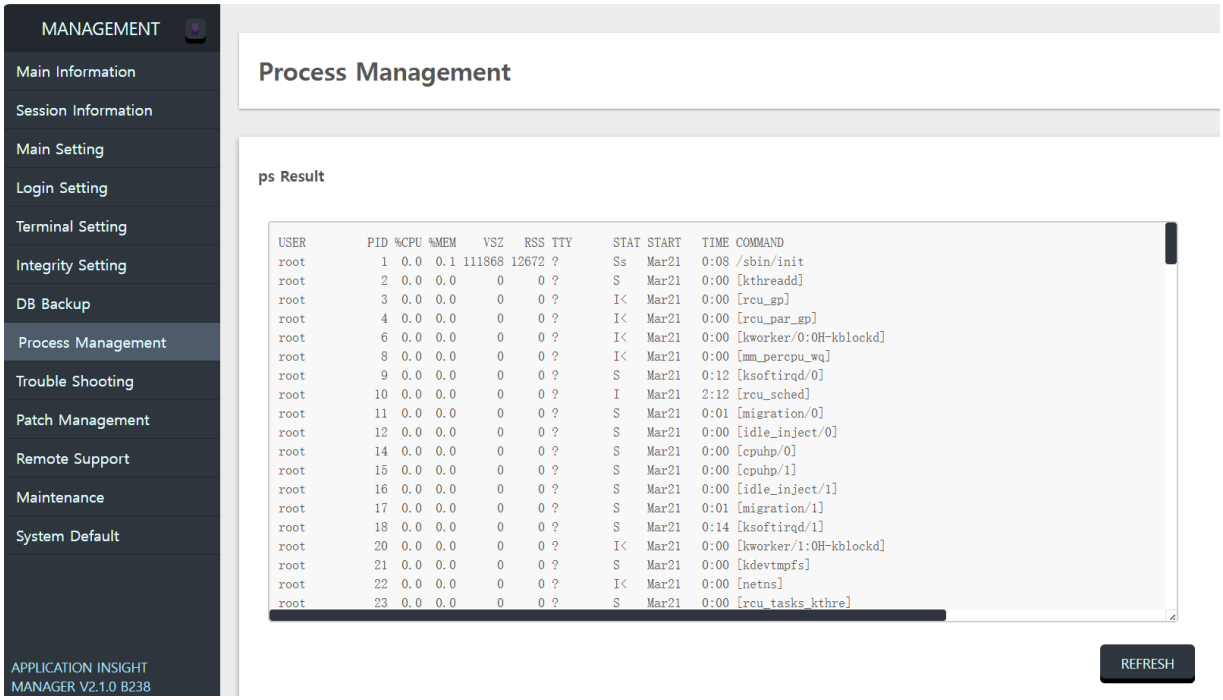
原因

- 不要なログの蓄積
- ネットワーク帯域の逼迫

対処方法

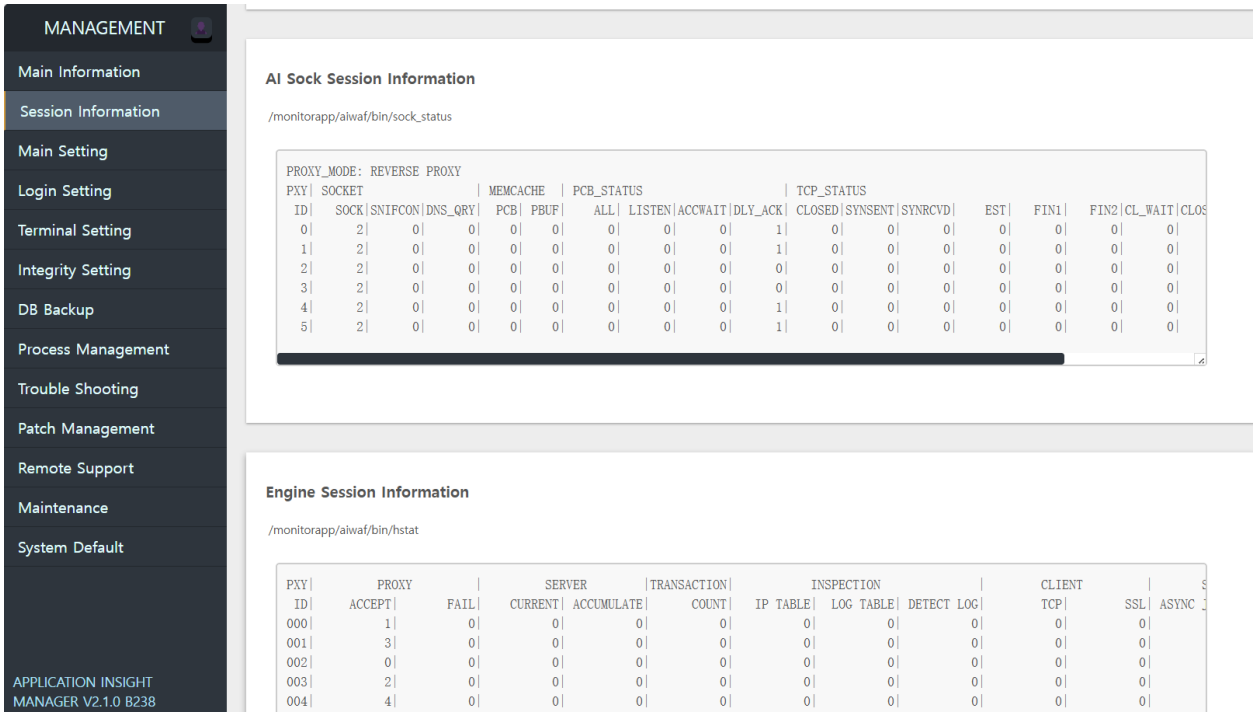
① リソース状況確認

- MANAGEMENT ページからプロセスの状況を確認



② エンジン・ソケットセッション情報確認

- MANAGEMENT ページからセッション情報を確認する。



③ ログを削除しディスクの空きを増やす。【ディスク容量が逼迫されている場合】

- SSH で接続し過去のテーブルを削除

  psql -U number1aiwaf aiwaf_db / 1234qwer!

  テーブル容量確認： ¥d+

  テーブル内容を空ける：truncate tablename_25xx

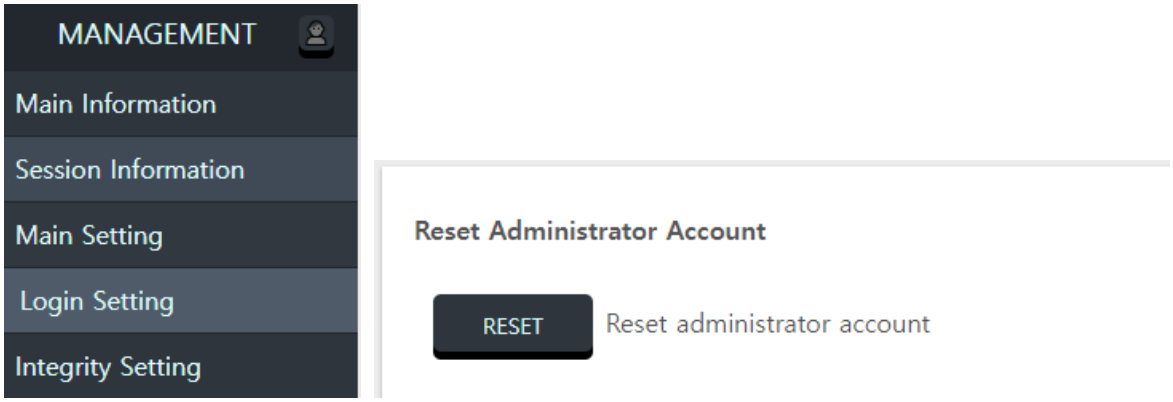
5.5 Web 管理コンソールのアカウント初期化

内容

Web 管理コンソールのアカウント情報を紛失した場合は、AIMANAGER WEB から初期アカウントに戻す方法

対処方法

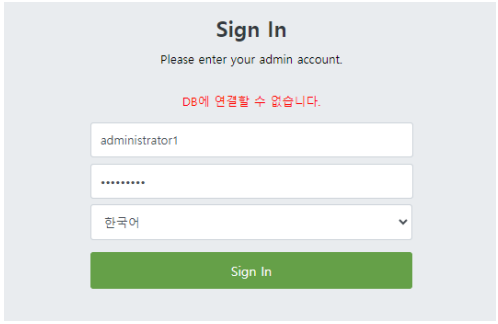
AIMANAGER Web > Login Setting > Reset Administrator Account をクリックで初期化
AIMANAGER Web の接続：https://[AIWAF サーバ IP]:333



5.6 AIWAF WEB 管理コンソールへログイン不可―DB へ接続できない

内容

AIWAF WEB 管理コンソールへログイン時「GUI ログイン不可 - DB に接続できません。」のメッセージが表示されログインできない場合



対処方法

AIWAF サーバの DISK 容量が高騰されている場合に発生する。
容量の確保の為、DB に接続し古いテーブルを削除し可用領域を確保が必要である。

SSH で AIWAF へ接続し古いテーブルを削除する。
Psql -U number1aiwaf aiwaf_db / 1234qwer!

テーブル容量確認
¥d+
該当の DB table の内容を削除する。
Truncate tablename_25xx

```
 public | detect_highlight_log          | table    | postgres     | 8192 bytes |
 public | detect_highlight_log_2408     | table    | number1aiwaf | 8192 bytes |
 public | detect_highlight_log_2409     | table    | number1aiwaf | 16 kB      |
aiwaf_db=# truncate detect_highlight_log_2409;
```

6. まとめ

本手順書に従い、定期的なメンテナンスを行うことで、AIWAF-VE の安定運用を確保できます。問題発生時は適宜ログを確認し、必要な対応を速やかに実施が求められます。

以上