

# 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

<b>1. はじめに</b> .....	<b>2</b>
<b>2. メンテナンスの前準備</b> .....	<b>2</b>
2.1 メンテナンス実施前の確認事項.....	2
<b>3. メンテナンス手順</b> .....	<b>3</b>
<b>4. メンテナンス後の確認</b> .....	<b>7</b>
4.1 システムの動作確認 .....	7
4.2 関係者への報告 .....	7
<b>5. トラブルシューティング</b> .....	<b>8</b>
5.1 サービス停止・アクセス不可.....	8
5.2 誤検知 .....	10
5.3 検知漏れ.....	10
5.4 高負荷・パフォーマンス低下 .....	12
5.5 Web 管理コンソールのアカウント初期化.....	13
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.....	14
<b>6. まとめ</b> .....	<b>15</b>

## 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

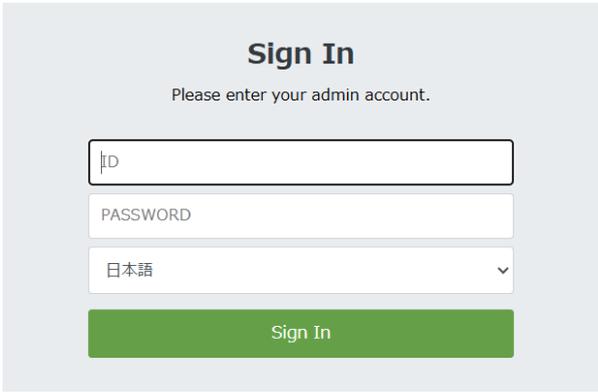
## 2. メンテナンスの前準備

### 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

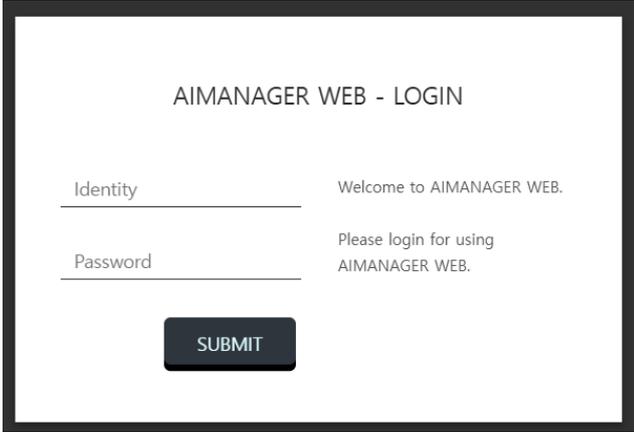
(接続 URL: [https://\[AIWAF IP\]:222](https://[AIWAF IP]:222))



The screenshot shows a 'Sign In' form with the following elements:

- Title: Sign In
- Instruction: Please enter your admin account.
- Input fields: ID, PASSWORD
- Language dropdown: 日本語
- Sign In button

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](https://[AIWAF IP]:333))



AIMANAGER WEB - LOGIN

Identity \_\_\_\_\_ Welcome to AIMANAGER WEB.

Password \_\_\_\_\_ Please login for using  
AIMANAGER WEB.

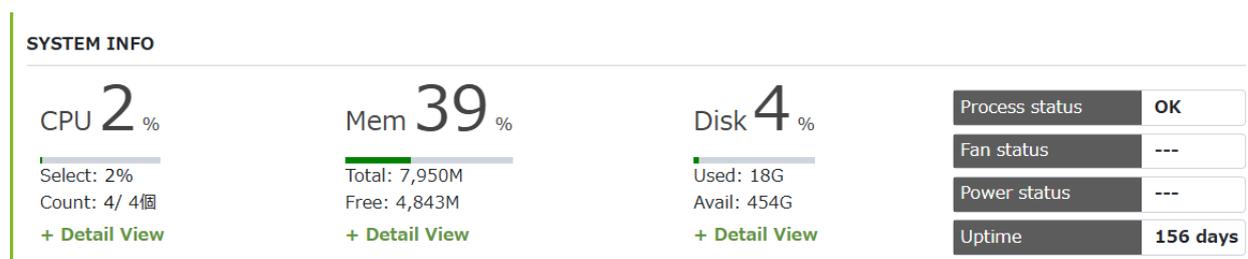
**SUBMIT**

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

Monitoring | Log Analysis | Reports | Policy Settings | Environment Settings | 2025-03-28

検知ログ検索 | 監査ログ検索 | ウェブサーバー状態検索 | ファイル分析ログ検索

全体削除

期間: 1ヶ月

期間: 今日 | 1週間 | 1ヶ月 | 2025-03-21 10:02 ~ 2025-03-28 10:32

検索 | ダウンロード | チャート | ピボットチャート | 検索条件の適用

攻撃ドメイン: - 個 | 攻撃者(Origin IP): - 個(- 個) | 攻撃件数: - 件 | TODO

自動更新: 5秒 | 検索: 15行

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	メール
03-07 11:43:42	163.43.24...	163.43.23...	163.43.158...	Default	SQLインジェクション	SQL Injection	http://test.jonmot.store/	高	停止	通知
03-07 11:43:12	163.43.24...	163.43.23...	163.43.158...	Default	SQLインジェクション	SQL Injection	http://test.jonmot.store/	高	停止	通知
03-07 11:41:02	163.43.24...	163.43.23...	163.43.158...	Default	SQLインジェクション	SQL Injection	http://test.jonmot.store/	高	停止	通知

- 監査ログ確認 : ログ解析 > 監査ログ検索

Monitoring | Log Analysis | Reports | Policy Settings | Environment Settings

検知ログ検索 | 監査ログ検索 | ウェブサーバー状態検索 | ファイル分析ログ検索

全体削除

期間: 2025-03-28 10:07 ~ 2025-03-28 10:37

期間: 今日 | 1週間 | 1ヶ月 | 2025-03-28 10:07 ~ 2025-03-28 10:37

検索 | ダウンロード | 検索条件の適用

自動更新: 5秒 | 検索: 15行

時間	クライアントIP	ID	監査ログタイプ	メール	内容
03-28 10:19:23	61.105.175.218	administrator1	ログイン成功	通知	ID: administrator1
03-28 10:16:42	61.105.175.218	administrator1	ログアウト	通知	ID: administrator1
03-28 10:16:34	61.105.175.218	administrator1	ログイン成功	通知	ID: administrator1

### 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、ファームウェア・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

Patch

Current Version Info

```
Product: APPLICATION INSIGHT WAF
Version: V5.0.2_2h
Release_date: 2024-09-05
AIOS: V5.0.0_L402
Build: 4753
Lib_build: 391
Synap_version: v4.28.0.1
```

Upload Patch file :  ファイルが選択されていません

Online Patch :

4. 新しいパ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>

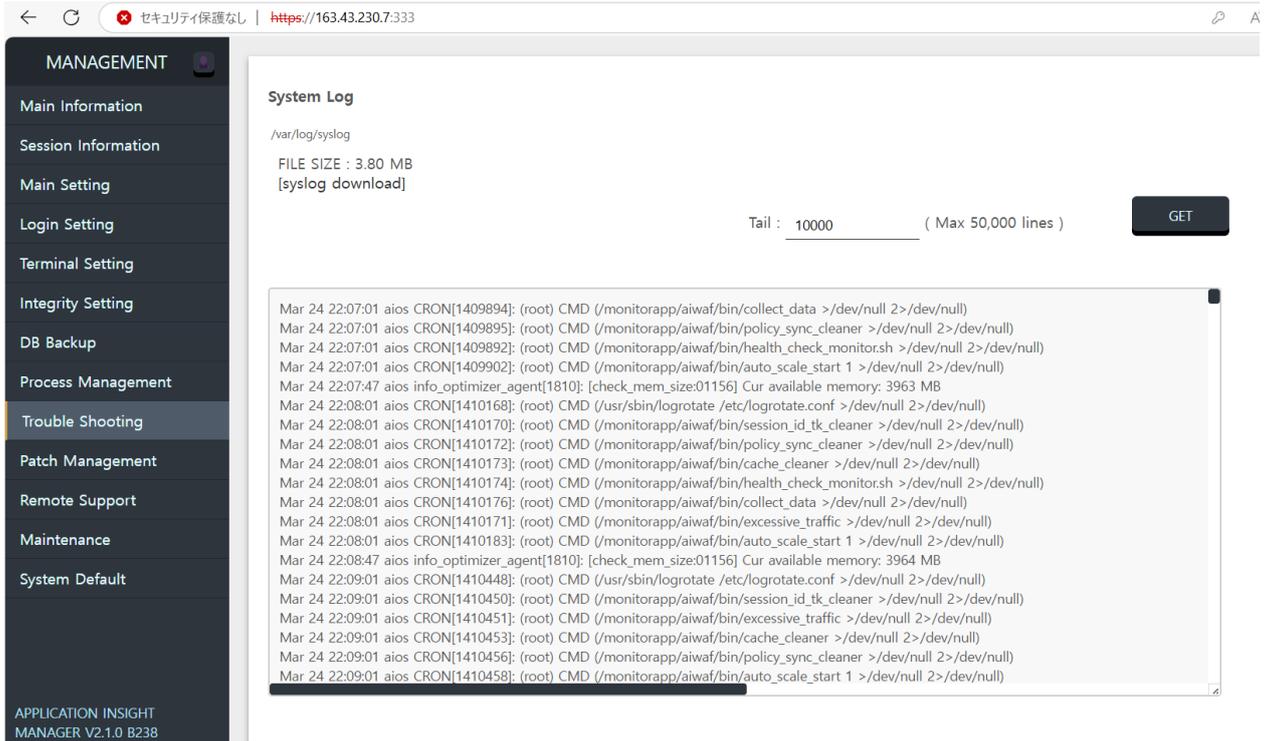
The screenshot shows the AIMANAGER interface with a sidebar menu on the left and a main content area. The sidebar menu includes: MANAGEMENT, Main Information, Session Information, Main Setting, Login Setting, Terminal Setting, Integrity Setting, DB Backup, Process Management (highlighted), Trouble Shooting, Patch Management, Remote Support, Maintenance, and System Default. The main content area displays a table with the following data:

Process	Status	Debug	Restart
httpgw	Running ..	<input type="radio"/> On <input checked="" type="radio"/> Off Timeout (Second) [input type="text"/> proxy <input type="radio"/> On <input checked="" type="radio"/> Off insp <input type="radio"/> On <input checked="" type="radio"/> Off lwip <input type="radio"/> On <input checked="" type="radio"/> Off cache <input type="radio"/> On <input checked="" type="radio"/> Off Filter Client IP [input type="text"] Server IP [input type="text"] Port [input type="text"] +	APPLY RESTART
ha_agent	Running ..	<input type="radio"/> On <input checked="" type="radio"/> Off Timeout (Second) [input type="text"]	APPLY RESTART
lcd_display	Running ..	<input type="radio"/> On <input checked="" type="radio"/> Off Timeout (Second) [input type="text"]	APPLY RESTART
lan_bypass	Stopped	<input type="radio"/> On <input checked="" type="radio"/> Off Timeout (Second) [input type="text"]	APPLY RESTART
policy_agent	Running ..	<input type="radio"/> On <input checked="" type="radio"/> Off Timeout (Second) [input type="text"]	APPLY RESTART

##### 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

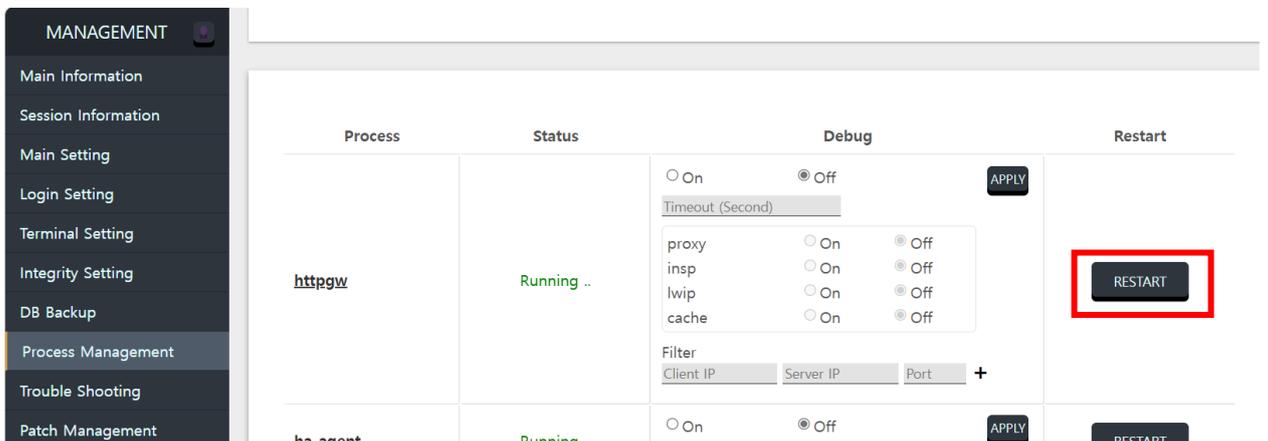
接続先 <https://WAFのIPアドレス:333>



### 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>

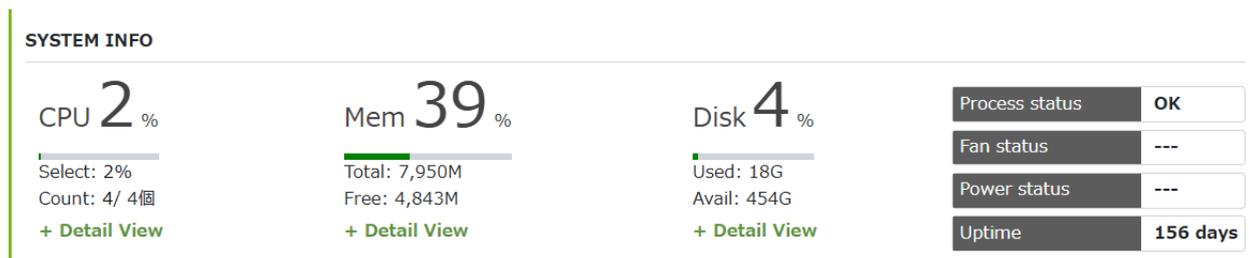


※httpgw をリスタートする。

### 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いない

### 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

MANAGEMENT

Main Information

Session Information

Main Setting

Login Setting

Terminal Setting

Integrity Setting

DB Backup

Process Management

Trouble Shooting

Patch Management

Remote Support

Maintenance

System Default

APPLICATION INSIGHT  
MANAGER V2.1.0 B238

### Process Management

ps Result

USER	PID	%CPU	%MEM	VSZ	RSS	TTY	STAT	START	TIME	COMMAND
root	1	0.0	0.1	111868	12672	?	Ss	Mar21	0:08	/sbin/init
root	2	0.0	0.0	0	0	?	S	Mar21	0:00	[kthreadd]
root	3	0.0	0.0	0	0	?	I<	Mar21	0:00	[rcu_gp]
root	4	0.0	0.0	0	0	?	I<	Mar21	0:00	[rcu_par_gp]
root	6	0.0	0.0	0	0	?	I<	Mar21	0:00	[kworker/0:0H-kblockd]
root	8	0.0	0.0	0	0	?	I<	Mar21	0:00	[mm_percpu_wq]
root	9	0.0	0.0	0	0	?	S	Mar21	0:12	[ksoftirqd/0]
root	10	0.0	0.0	0	0	?	I	Mar21	2:12	[rcu_sched]
root	11	0.0	0.0	0	0	?	S	Mar21	0:01	[migration/0]
root	12	0.0	0.0	0	0	?	S	Mar21	0:00	[idle_inject/0]
root	14	0.0	0.0	0	0	?	S	Mar21	0:00	[cpuhp/0]
root	15	0.0	0.0	0	0	?	S	Mar21	0:00	[cpuhp/1]
root	16	0.0	0.0	0	0	?	S	Mar21	0:00	[idle_inject/1]
root	17	0.0	0.0	0	0	?	S	Mar21	0:01	[migration/1]
root	18	0.0	0.0	0	0	?	S	Mar21	0:14	[ksoftirqd/1]
root	20	0.0	0.0	0	0	?	I<	Mar21	0:00	[kworker/1:0H-kblockd]
root	21	0.0	0.0	0	0	?	S	Mar21	0:00	[kdevtmpfs]
root	22	0.0	0.0	0	0	?	I<	Mar21	0:00	[netns]
root	23	0.0	0.0	0	0	?	S	Mar21	0:00	[rcu_tasks_kthre]

REFRESH

- 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。

MANAGEMENT

- Main Information
- Session Information
- Main Setting
- Login Setting
- Terminal Setting
- Integrity Setting
- DB Backup
- Process Management
- Trouble Shooting
- Patch Management
- Remote Support
- Maintenance
- System Default

APPLICATION INSIGHT  
MANAGER V2.1.0 B238

### AI Sock Session Information

/monitorapp/aiwaf/bin/sock\_status

PROXY_MODE: REVERSE PROXY																	
PXY   SOCKET				MEMCACHE				PCB_STATUS				TCP_STATUS					
ID	SOCK	SNIFCON	DNS_QRY	PCB	PBUF	ALL	LISTEN	ACCWAIT	DLY_ACK	CLOSED	SYNSENT	SYNRCVD	EST	FIN1	FIN2	CL_WAIT	CLOS
0	2	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0
1	2	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0
2	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	2	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0
5	2	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0

### Engine Session Information

/monitorapp/aiwaf/bin/hstat

PXY		PROXY		SERVER			TRANSACTION			INSPECTION			CLIENT		
ID	ACCEPT	FAIL	CURRENT	ACCUMULATE	COUNT	IP	TABLE	LOG	TABLE	DETECT	LOG	TCP	SSL	ASYNC	
000	1	0	0	0	0	0	0	0	0	0	0	0	0	0	
001	3	0	0	0	0	0	0	0	0	0	0	0	0	0	
002	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
003	2	0	0	0	0	0	0	0	0	0	0	0	0	0	
004	4	0	0	0	0	0	0	0	0	0	0	0	0	0	

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`

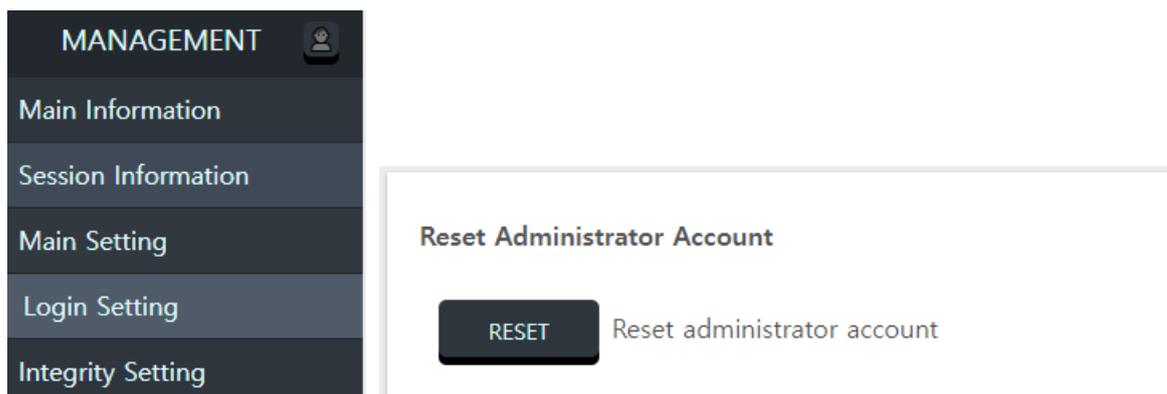
## 5.5 Web 管理コンソールのアカウント初期化

### 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

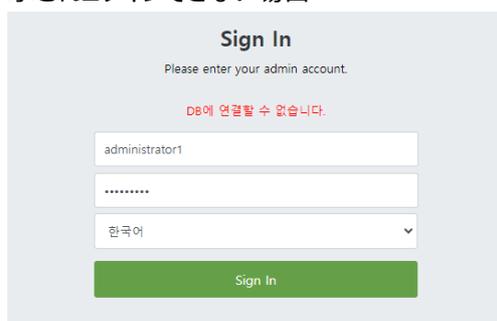
AIMANAGER Web > Login Setting > Reset Administrator Account をクリックで初期化  
AIMANAGER Web の接続： `https://[AIWAF サーバ IP]:333`



## 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