AIWAF-VE
運用者教育資料

アプリケーション・セキュリティ事業本部

- Security for Developers -

2025/3/25

目次

1. WAF(Web Application Firewall)の概要
2. 管理者ページ
3. GUI
4. ログ照会
5. ポリシー設定– 共通
6. 保護対象WEBサーバ
7. ポリシー設定 – 基本設定
8. ポリシー設定 – Adminポリシー
9. ポリシー設定 – ドメイン別ポリシー
10. 環境設定
11. AIMANAGER WEB
12. Trouble Shooting

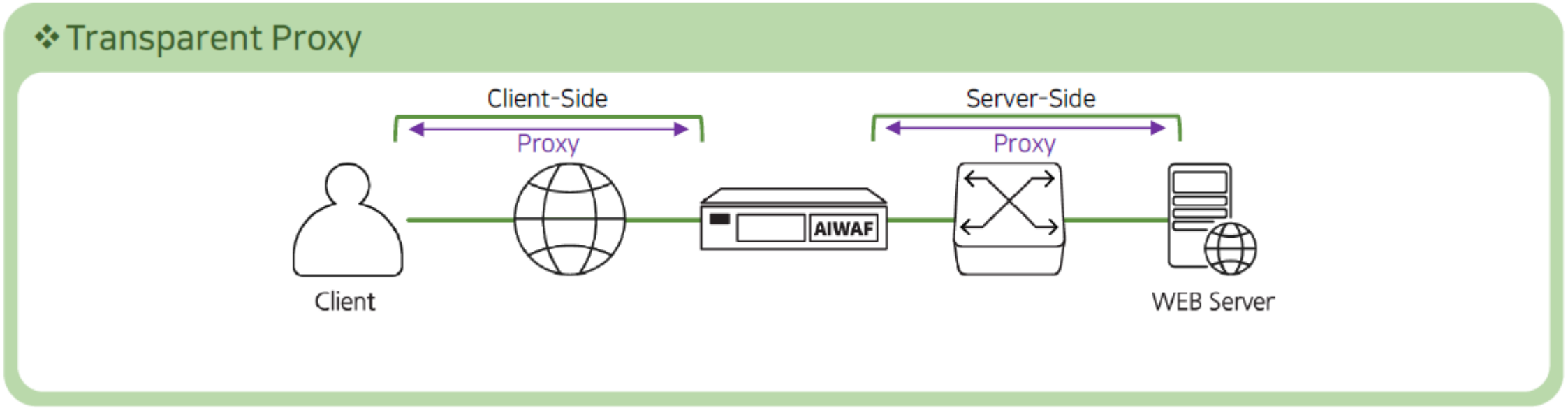
1．WAFの概要

●Web（HTTP/HTTPS）プロトコルを利用した攻撃に対応するセキュリティ機器

➢非Webプロトコルは、動作モードに応じてバイパス動作またはパケットをドロップします ●Transparent Proxy テクノロジーを使用して別の IP を付与せずにステルスモードで動作

➢AIWAFに基づいてClient-SideとServer-Sideセッションを別々に確立 ➢出発地と目的地のMAC、IP、ポートを切り替えて通信

➢ クライアントの立場ではサーバーのように、サーバーの立場ではクライアントのように動作



1．WAFの概要

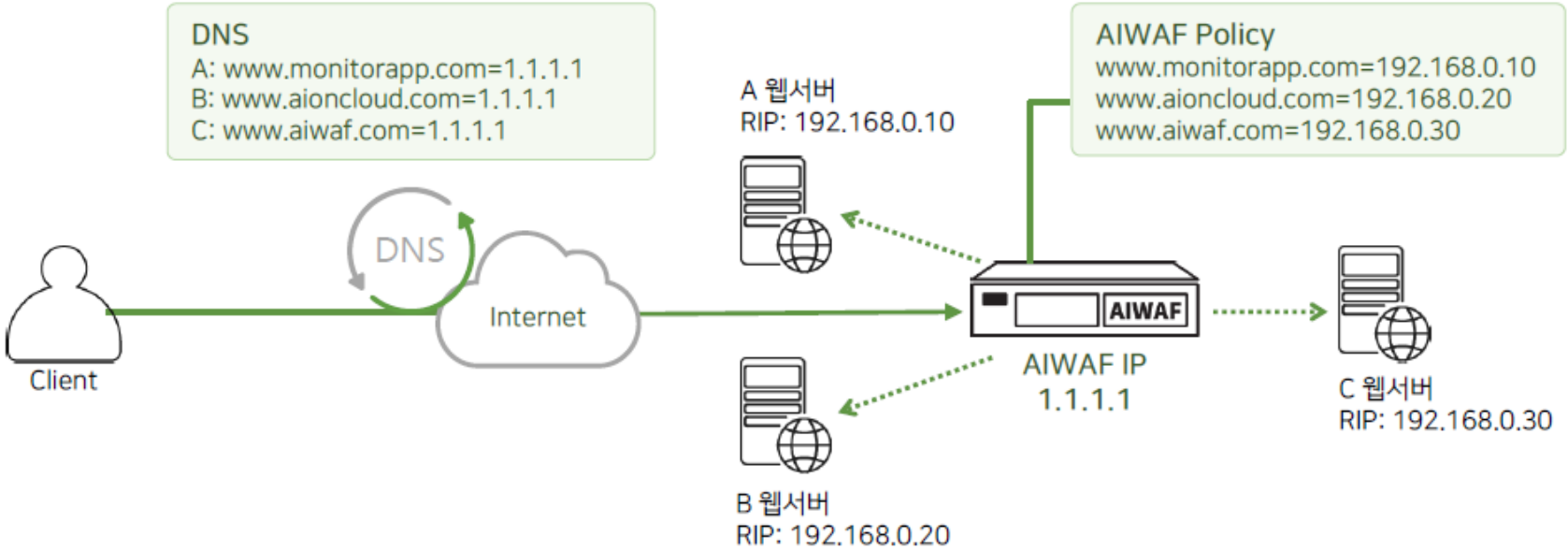
●リバース プロキシ (Reverse Proxy) Mode

➢ AIWAFが保護対象のWebサーバーに代わってProxyサーバーとして動作するモードです。

➢Webサーバーの外部への露出を防ぎ、Webサーバーが分散して配置されている環境で幅広い保護を提供します。

●AIWAFまたはWebサーバーの物理的な場所とは無関係に構成できます。

➢ AIWAF が物理的な場所に拘束されていないため、すべての Cloud 環境で構成でき、さまざまなVirtual環境で使用されます。



2. 管理者ページ

SSH接続

●管理者向けページの提供（SSH、GUI、AIMANAGER WEB）

●SSHの基本的なアプローチと情報[1/3]

➢ SSH接続

• Default SSH Port: 22

➢ CLI アクセスアカウント情報

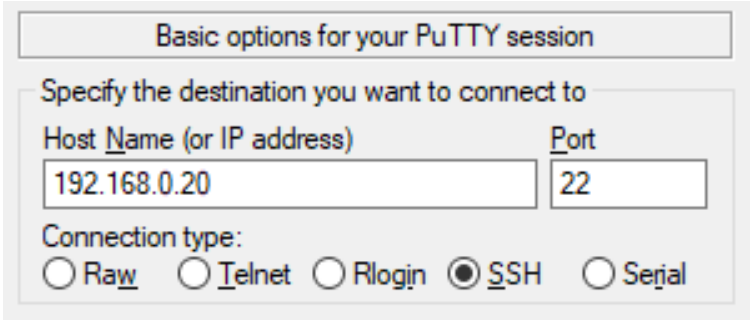
•デフォルトアカウント：aiadmin

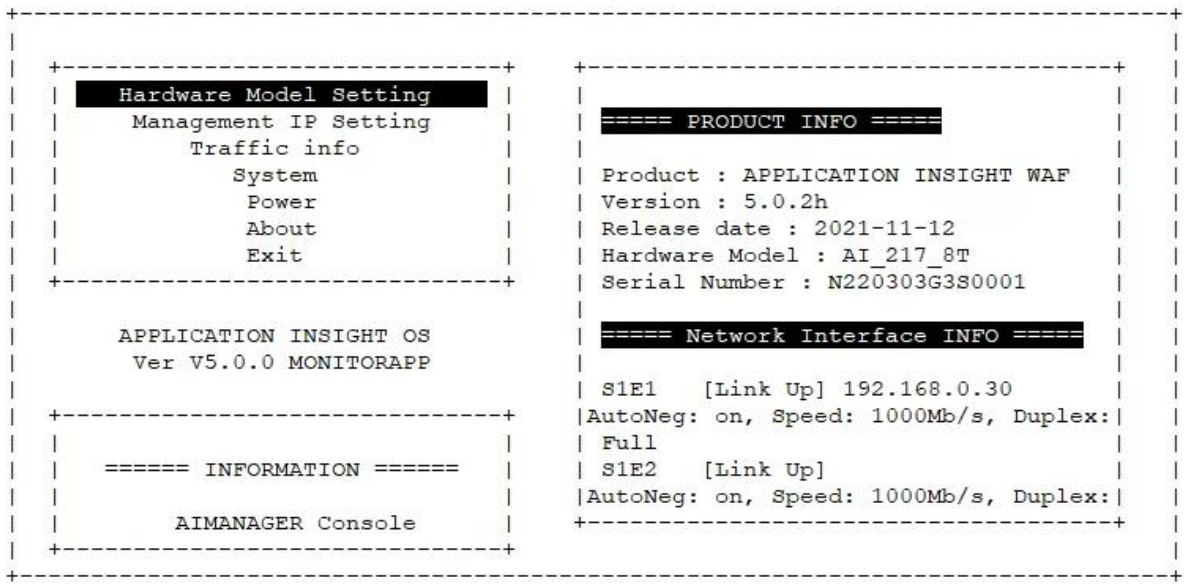
•パスワード：number1aiwaf

➢Root権限の取得

• aiadmin@AIOS50:~$ sudo su

•パスワード：aiadminパスワード入力



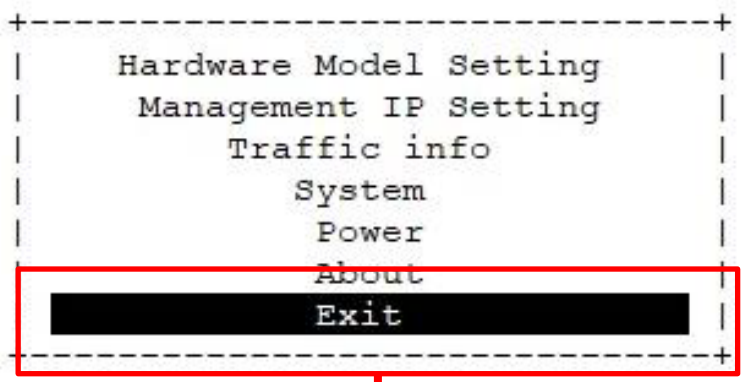


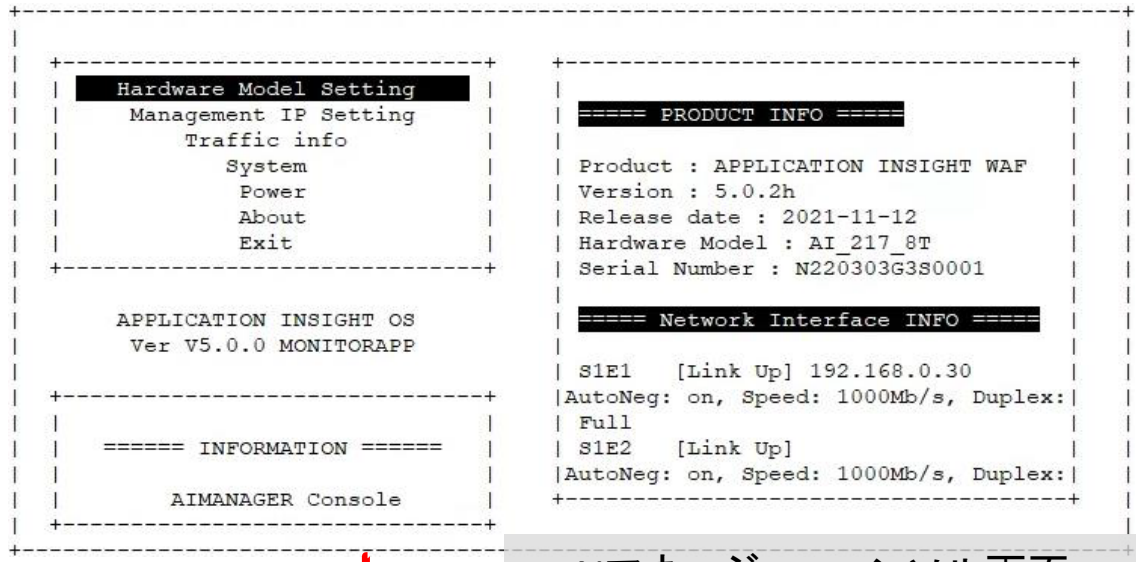
2. 管理者ページ

SSH基本接続方法及び情報

●Shell接続方法

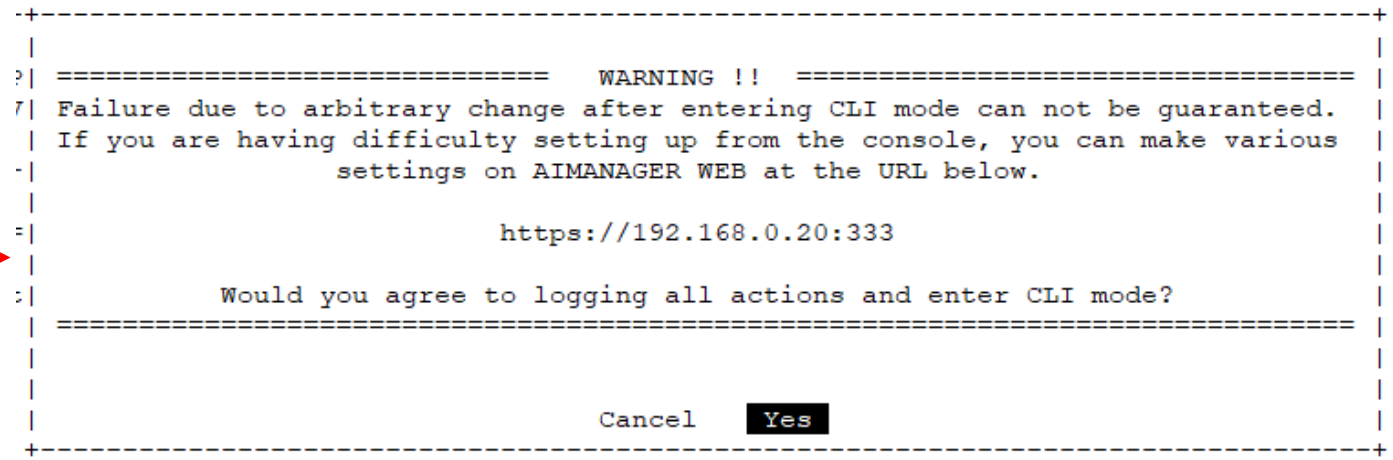
詳細の説明はAdminマニュアルを参照





AIマネージャーコンソル画面

EXITでShellへ



Shellに接続時警告を確認

2. 管理者ページ

SSH基本接続方法及び情報

●ルート権限取得

・sudo su コマンドでroot権限取得

・aiadminアカウントのパスワード入力

```
================================================================================
                          WARNING !!

        All actions in the current session wil

        user name      :  root
        session id     :  22350
        logging start_time : 2022-03-04 11:51:

Please end the session if you do not agree to
================================================

root@AIOS50:/home/aiadmin# sudo su
```

```
================================================================================
                                WARNING !!

        All actions in the current session will be logged.

        user name      :  aiadmin
        session id     :  12427
        logging start_time : 2022-03-04 11:53:29

Please end the session if you do not agree to logging your actions.
================================================================================

aiadmin@AIOS50:~$ sudo su
[sudo] password for aiadmin:
root@AIOS50:/home/aiadmin#
```

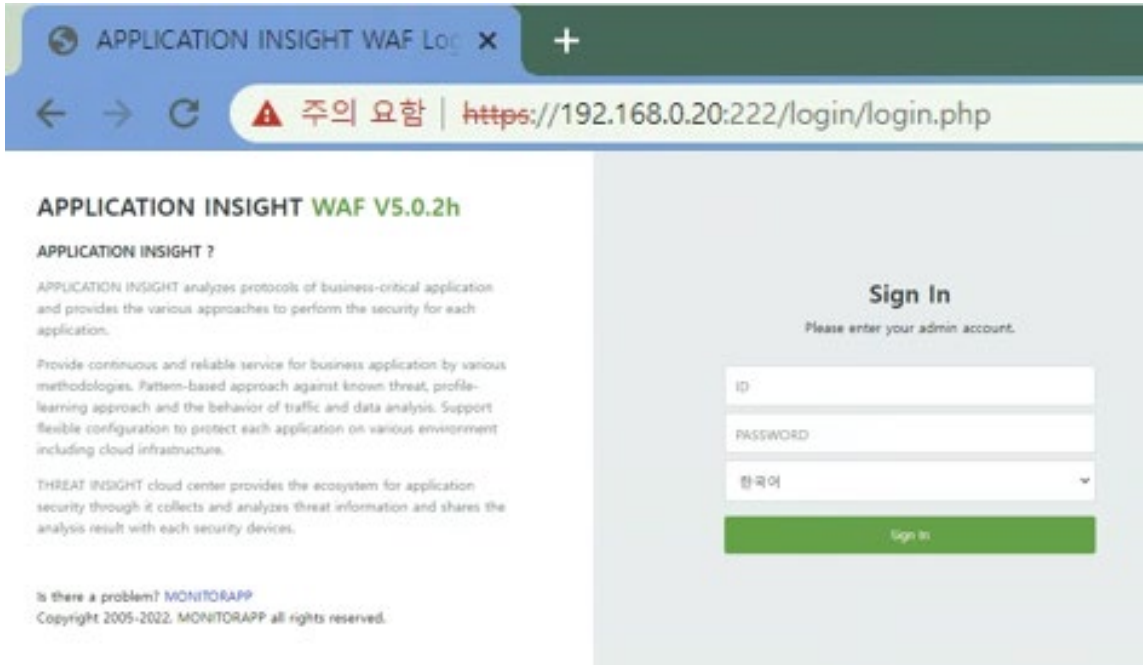
2. 管理者ページ

管理者ページ” GUIの基本接続情報

➢ AIWAF のポリシー設定やログ、監視など、全体的な機能の設定と管理ページ

➢ 管理ページ GUI アプローチ

- Default GUI Port: 222 (アクセス例: https://192.168.0.20:222)
- Default アカウント: administrator1
- Default パスワード : 1234qwer!



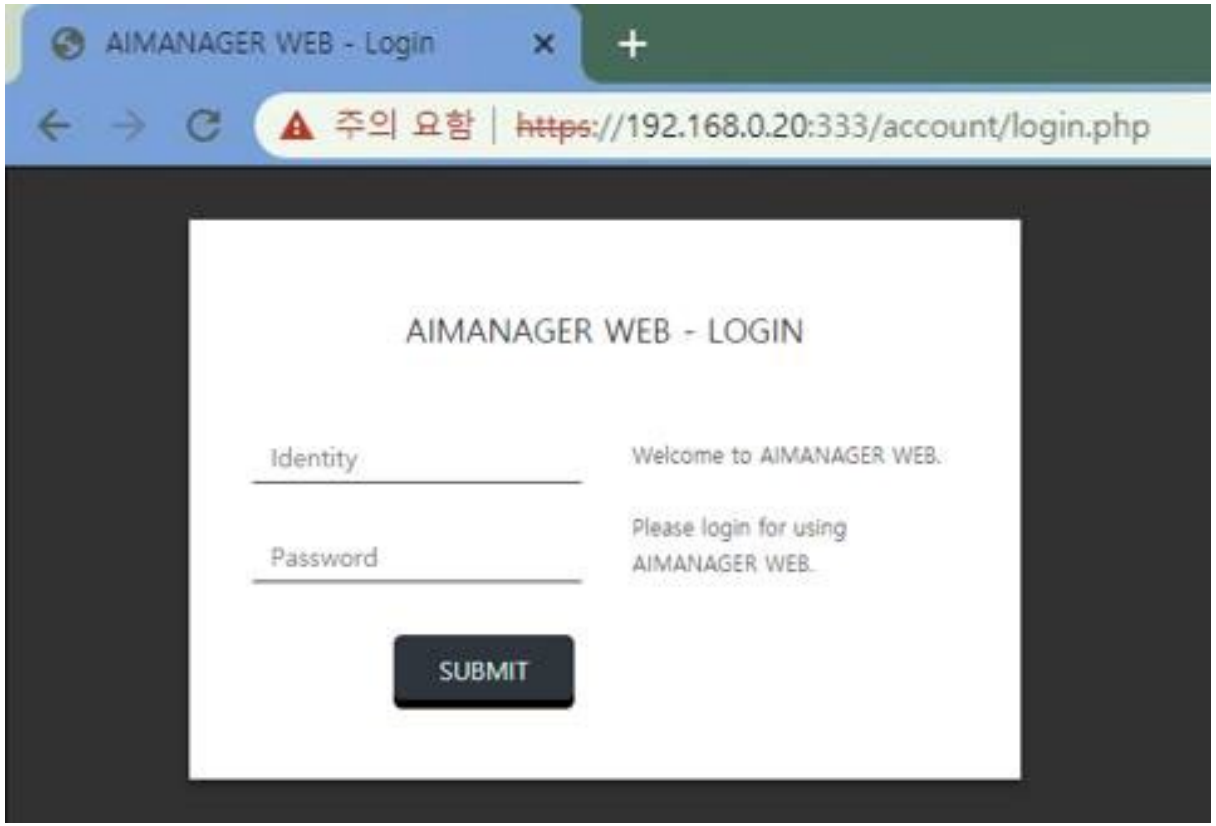
2. 管理者ページ

管理者ページ” GUIの基本接続情報

➢ AIWAFのエンジニアリングのためのWebページ

➢ AIMANAGER WEB GUI アプローチ

- Default GUI Port: 333 (アクセス例: https://192.168.0.20:333)
- Default アカウント: administrator
- Default パスワード: _appleader



3. GUI

ダッシュボード

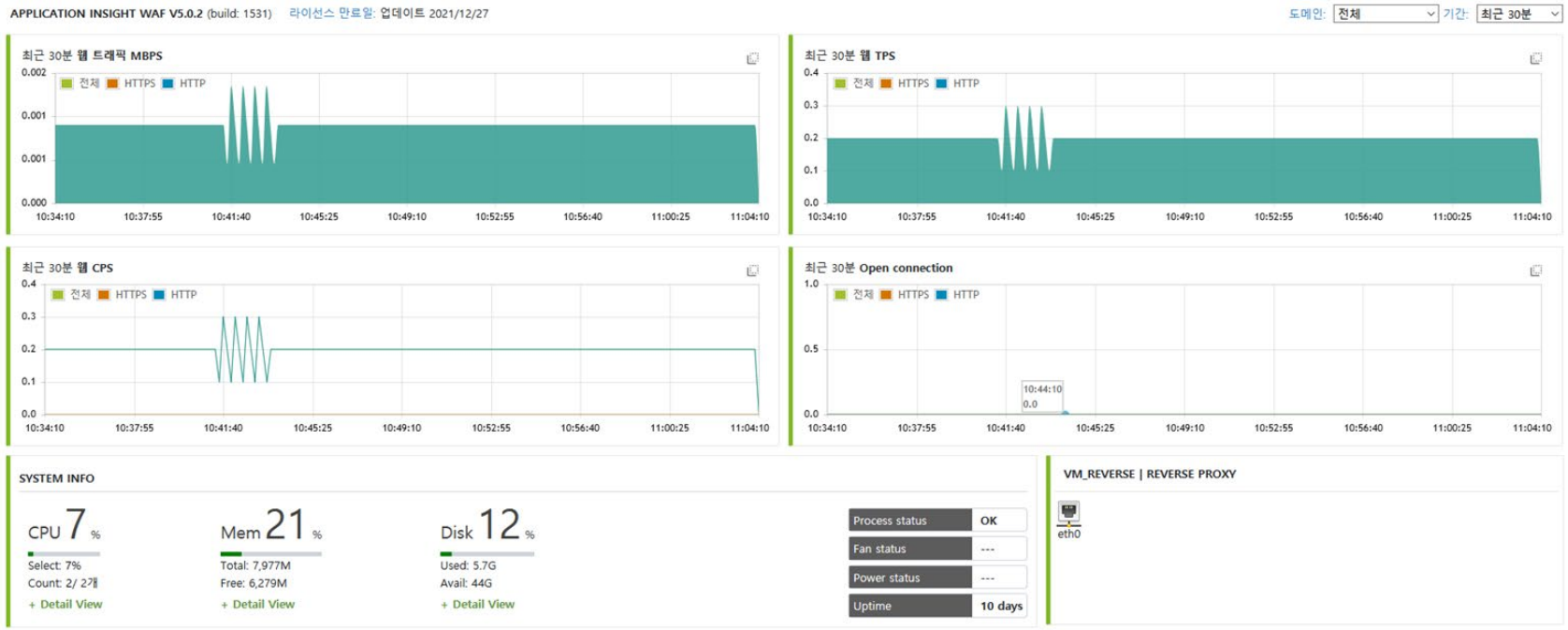
機器のトラフィック、リソース、バージョン、ライセンス情報などのステータス情報を提供する画面

➢Webトラフィック（Mbps）：AIWAFを通過するWebトラフィックの量を1秒あたりのメガビット数で表示します。

➢ Web TPS: AIWAF を通過するトラフィック量を連続処理単位数で表示

➢Web CPS：AIWAFを通過するWebトラフィックの量を1秒あたりの接続数として表示します。

➢Open Conncection：AIWAFを通過するWebトラフィックの瞬間接続数を表示します。



3. GUI

ダッシュボード

機器のトラフィック、リソース、バージョン、ライセンス情報などのステータス情報を提供する画面

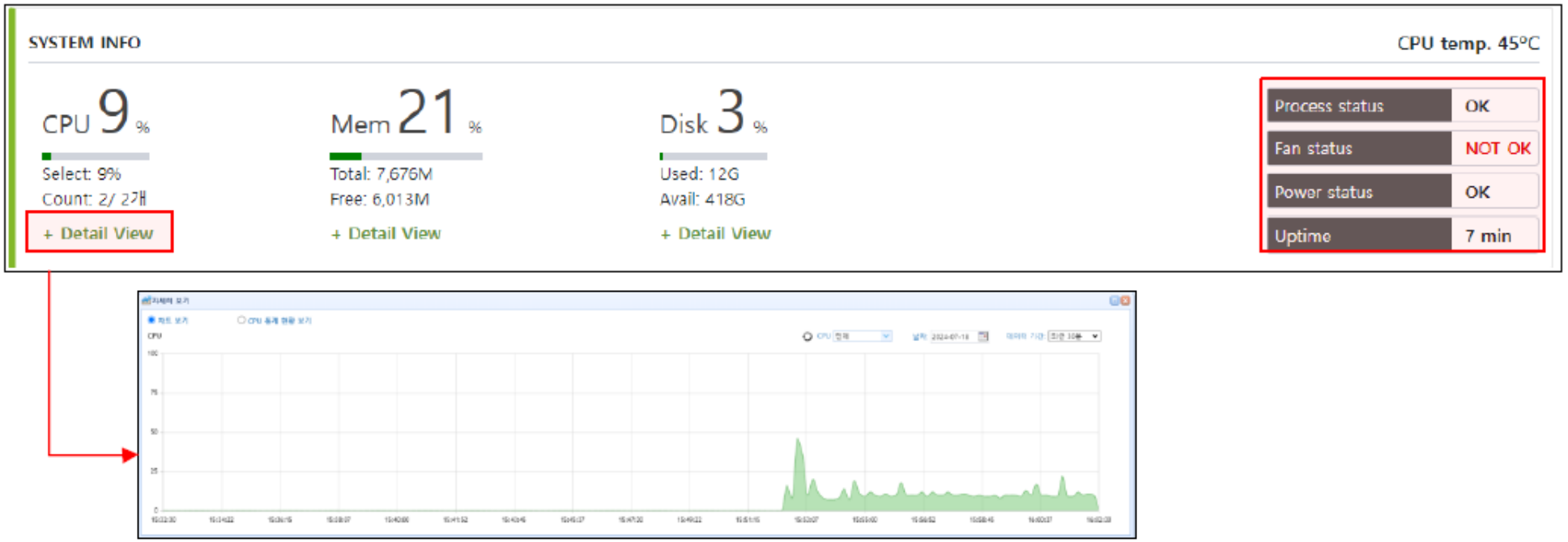
➢CPU、MEM、DISK使用量情報を確認可能

• Detail Viewで詳細情報を確認する

➢ プロセス状態、ファン状態、電源状態情報、アップタイム情報を確認可能

•正常：OK

•異常：NOT OK



3. GUI

ダッシュボード

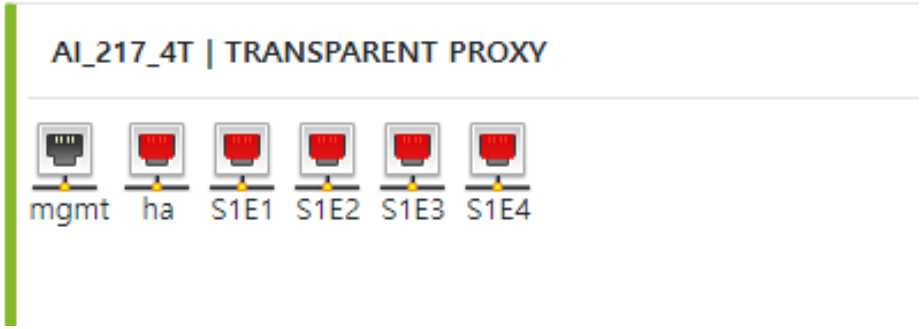
機器のトラフィック、リソース、バージョン、ライセンス情報などのステータス情報を提供する画面

➢ 機器のモデル名、動作モード、インタフェースの状態を確認可能

•グレード：スペック基準に応じて200、500、1000、2000、4000、8000の存在

•年式：Y17、Y20など、その機器のリリース年式を表示

•Q：40G_Fiber　G：10Gファイバー　F：1Gファイバー　T：1G UTP



➢ ファームウェアバージョン及び、ライセンス情報確認

APPLICATION INSIGHT WAF V5.0.2_2h (build: 4753)　ライセンス満了日: 更新 2031/09/09

4. ログ照会

検出ログの照会 [1/3]

➢違反したトラフィックを検出してログを収集する

➢ログ詳細を表示、条件検索機能を提供

➢フルまたは特定のログ Excel ダウンロードを提供

4. ログ照会

検出ログの照会 [2/3]

➢ ログ詳細表示機能で詳細情報を確認可能

➢検出時間、クライアント、サーバーIP、要求/応答データを確認可能

4. ログ照会

検出ログの照会 [3/3]

照会されたログ用にExcelをダウンロードできます

- 注意: 照会されたログの数によって Excel 生成時間に差があり、適切な照会期間の選択が必要

4. ログ照会

監査ログの照会 [1/3]

- システムの状態と変更に関するログ収集
- ログイン、ポリシー適用、プロセス異常、ライセンスなど
- フルまたは特定のログ Excel ダウンロードを提供

4. ログ照会

監査ログの照会 [2 /3]

➢ログ詳細表示機能で詳細情報を確認可能

➢検出時間、クライアント、サーバーIP、要求/応答データを確認可能

4. ログ照会

監査ログの照会 [3/3]

➢ 照会されたログに対して Excel をダウンロード可能

- 注意: 照会されたログの数によって Excel 生成時間に差があり、適切な照会期間の選択が必要

5. ポリシー設定共通

ポリシー適用・取消 [1/2]

➢ 政策変更時に「政策適用」を通じて最終適用が必要

➢ 「以前のポリシーへの復元」でポリシーの適用をキャンセル可能

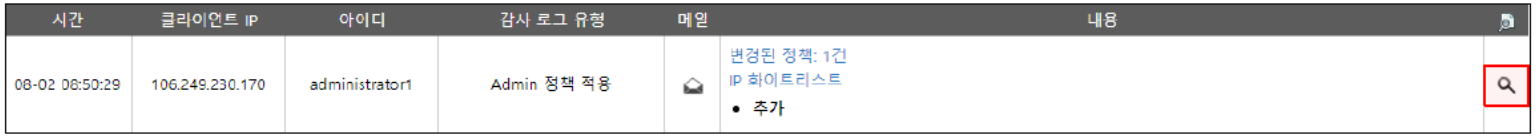
5. ポリシー設定共通

ポリシー適用·取消 [2/2]

➢ 適用されたポリシーは「監査ログ」で詳細内容確認可能

ポリシー復旧

➢ ポリシー復旧により以前のポリシー復旧可能



5. ポリシー設定共通

ポリシールール別処置

➢ ポリシー復旧により以前のポリシー復旧可能

- 検出：検出ログを作成してWebトラフィックを通過させます。
- ブロック：検出ログを作成した後、クライアントにブロックページを送信します。
- マスキング：検出ログを作成した後、検出された要求/応答Webトラフィックの一部をマスキング後に通過させます。
- クロッキング：検出ログを作成した後に応答Webトラフィックをブロックし、設定されたクロッキングページ（ブロックページ）を送信します。
- 許可：検出ログを作成したら、追加のWebトラフィックをサブルールとして調べます。

✓ クローキング設定時、通常のブロックと同じブロックページを送信する

(グループ/ブロックページ設定 ->ブロックページ)

5. ポリシー設定共通

共通オプション（1/2）

1. クライアント&サーバー適用時

•クライアントIP＆サーバーIPまたはクライアントIP＆サーバーURLはAND条件で動作します。

2. URL 部分の作成

•ポリシーにサーバーURLを作成するときにwww.monitorapp.com/policy/またはwww.monitorapp.com/policyで作成すると自動的にpolicy/*(asterisk)、 policy*(asterisk) の形で動作する。

3. 適用 & 例外

• ポリシー クライアント IP またはサーバ IP OR URL の場合

[適用]：指定されたターゲットのみがそのルールに反映されます

[例外]: 指定された対象外の該当ルールに反映

5. ポリシー設定共通

共通オプション（2/2）

4.最小長さと最大長さ

- 最小長：一致する最小長を意味し、パターンをabc、最小長を5に設定した場合

  abcだけがある場合検出不可、abcde 5byteが満たされなければ検出

  abcパターンを適用した後の最小長を1byteに設定しても、固定abcは満足する必要があります。

- 最大長：一致する最大長を意味し、空の値または大きすぎるサイズを設定した場合は、対応するサイズと一致する試みで

  負荷が発生します（最小長さと最大長さを同時に使用します。）パターンを polic で指定後最小長 6 最大長

  10 で指定する場合 policy までが 6byte その後policy1234まではブロック、 policy12345から11byteでマッチング不可

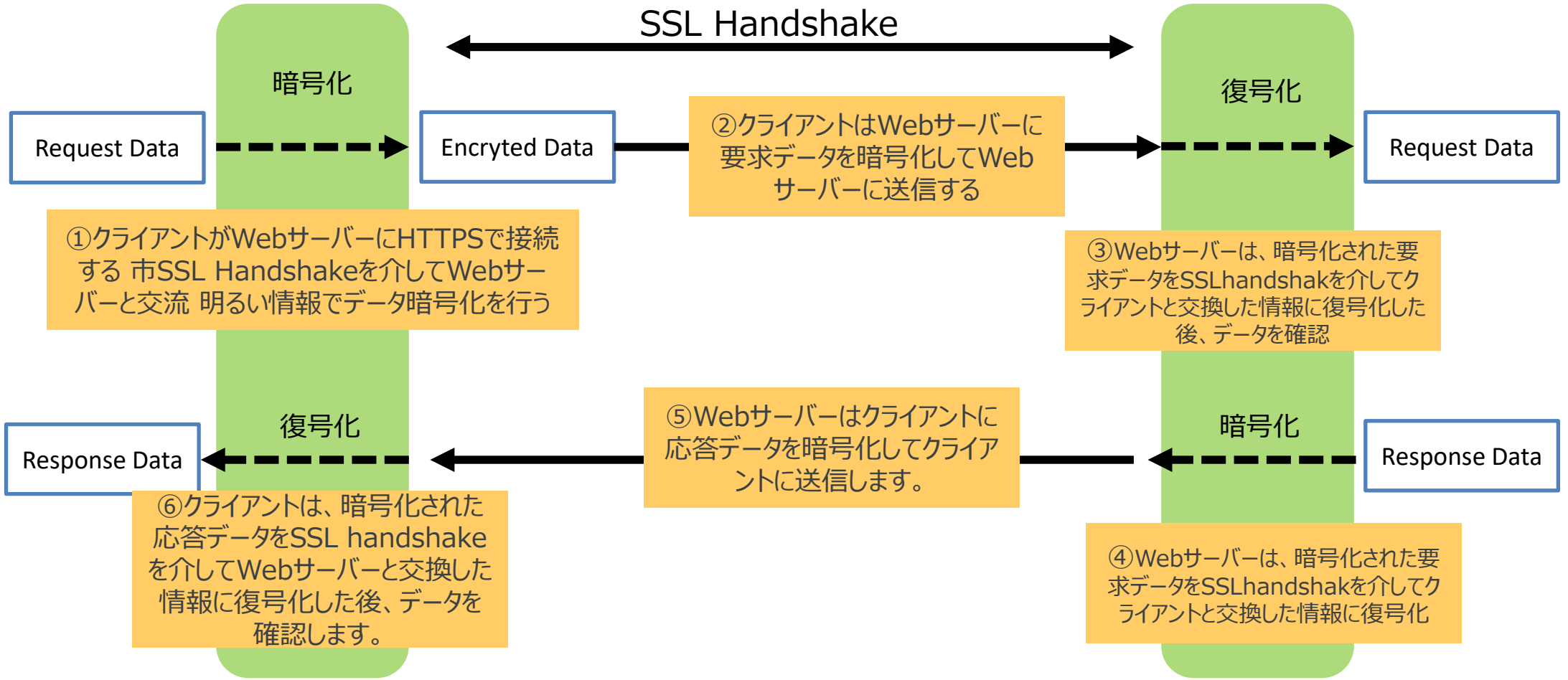
5.使用者定義パターンルールの「パターン」

- カスタムパターンルールのパターン部分では正規表現式使用可能。

6. 保護対象のWEBサーバ

保護対象のWEBサーバ

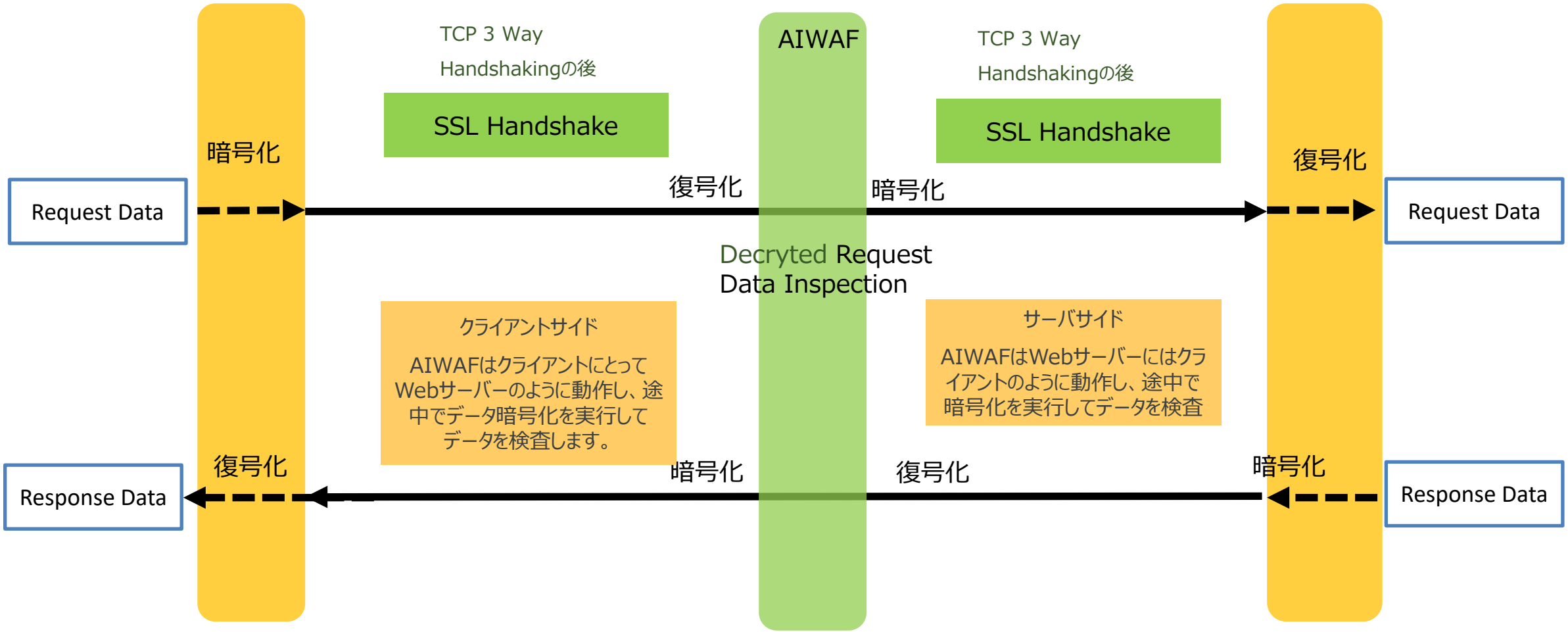
Proxy適用に対する理解



6. 保護対象のWEBサーバ

保護対象のWEBサーバ

AIWAFで保護するWebサーバーを登録し、その保護対象Webサーバーに流入する要求および応答トラフィックは、検出対象に含まれる。



6. 保護対象のWEBサーバ

保護対象のWEBサーバ

保護対象のWebサーバー設定ルールの追加

- ポリシー設定パス：製品UI>ポリシー設定>管理ポリシー>保護対象のWebサーバー

✓ 保護対象 Web サーバ登録時の留意事項

① Web サーバごとにプロトコルを指定して登録しなければならない。

②HTTPSプロトコル登録時にHTTPS証明書、アルゴリズムバージョンなどTLS Handshakeによって関連サービス障害問題が発生する可能性があるため、保護対象Webサーバに登録する前に、留意すべき事項をチェックする。

③ 保護対象サーバのIPとポートに関する情報が明確な場合、初期値であるALL(IP 0.0.0.0-255.255.255.255& Port 80)ポリシーが有効になっている場合は削除し、新規にルールを追加して使用する。 - 保護すべきサービスであるWebやHTTPではなく、任意のTCP 80を使用するサービスがある場合、不要なProxy動作による障害発生可能点を解消するためである。

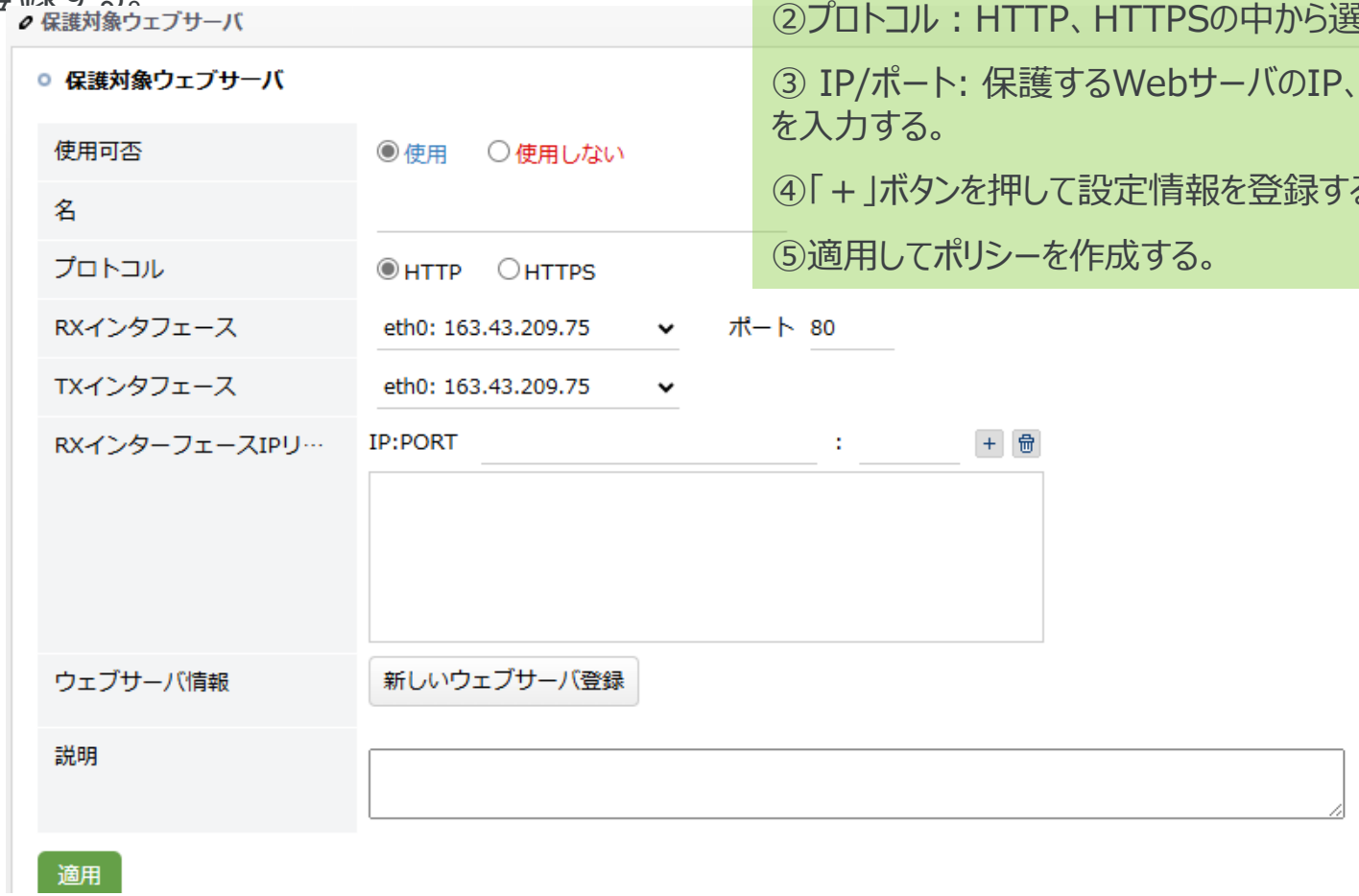
6. 保護対象のWEBサーバ

保護対象のWEBサーバ

HTTP保護対象のWebサーバーの追加「1/3」

ネットワーク動作モードが1）TP、SYN TP、ミラーリング、スニッフィングモードの場合

✓ 保護するWebサーバのIP、Port情報を登録する。



①名前：ルール名を設定する。

②プロトコル：HTTP、HTTPSの中から選択する。

③ IP/ポート: 保護するWebサーバのIP、PORTを入力する。

④「＋」ボタンを押して設定情報を登録する。

⑤適用してポリシーを作成する。

6. 保護対象のWEBサーバ

保護対象のWEBサーバ

HTTP保護対象のWebサーバーの追加「2/3」

•ネットワーク操作モードがリバースプロキシモードの場合[1/2]

✓ 保護するWebサーバのドメイン、IP、Port情報を登録する。

✓RX、TXインターフェースには、IP設定に追加されたインターフェースのみが有効になります。

①名前：ルール名を設定する。

②プロトコル：HTTP、HTTPSの中から選択する。

③RXインターフェース：クライアントサイドと通信するインターフェースを選択します。

④RXポート：クライアント要求を受信するポートを設定します。

⑤ TXインターフェース：サーバーサイドと通信するインターフェースを選択します。

⑥ RX インターフェース IP リスト以外の受信許可 IP: RX インターフェース IP 以外の IP を宛先とするパケットを受信した場合に転送することができる。AIWAFトップのLB などの機器がAIWAF RXインターフェースIPを目的地にせず、そのまま配信する場合に使用できる。

⑦ Web サーバ情報：保護対象 Web サーバのドメイン、IP、PORT 情報を登録する。

⑧適用してポリシーを作成する。

6. 保護対象のWEBサーバ

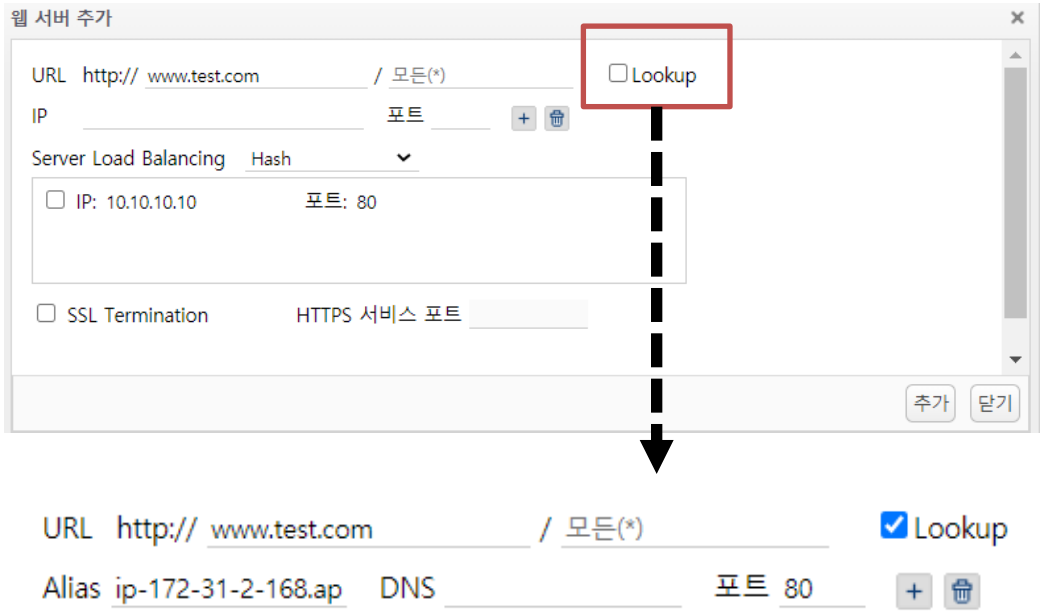
保護対象のWEBサーバ

HTTP保護対象のWebサーバーの追加「3/3」

•ネットワーク操作モードがリバースプロキシモードの場合[2/2]

✓ AIWAF が保護する Web サーバーに関する情報とポリシーを設定する。

✓「新しいWebサーバーを登録する」クリックすると、以下のようなウィンドウがポップアップ表示されます。



① Web サーバの URL を設定する。

②WebサーバのIP、Port情報を入力する。

③ サーバ負荷分散ロジックを選択する。(SLB機能)

- Hash: 新規接続クライアントの IP アドレスと Port で Hash key を生成してパスを指定します。一度確立されたセッションを維持することによって特定のクライアン特定のサーバーにのみ割り当てる方法です。

- Least Connection: 最小数の接続セッション(Open Session)持っているサーバーに優先的に割り当てる方式だ。

- RR（Round Robin）：順番に割り当てる方法で優先順位や対応応答時間に関係なく、すべてのサーバーに同じように順番に割り当てます。

- Latency: 遅延時間が最も少ないサーバーに割り当てる方法でLatencyは、保護対象のWebサーバーの登録後に変更すると有効になります。このオプションは、保護対象のWebサーバールールのすべてのWebサーバーに「製品UI>ポリシーを設定するチョン>ヘルスチェック対象設定」に登録されていなければうまい。

④ Lookup（オプション）：Alias情報でWebサーバ登録が必要な場合にチェックして設定する。

⑤SSL Termination設定（オプション）ができる。

⑥設定を押してWebサーバー情報を追加します。

6. 保護対象のWEBサーバ

保護対象のWEBサーバ

HTTPS保護対象のWebサーバーの追加「1/6」

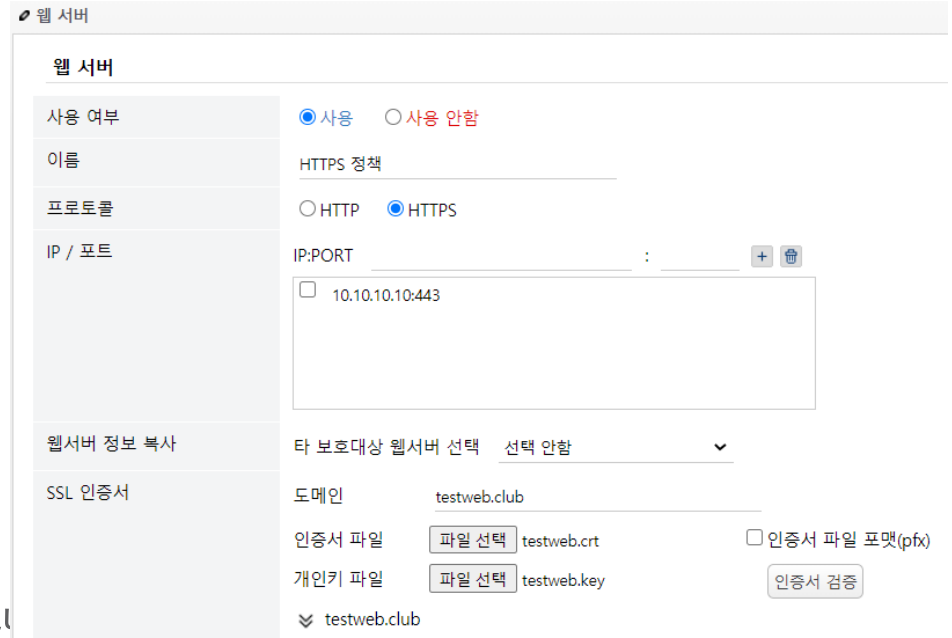
•ネットワーク動作モードがTP、SYN TP、ミラーリング、スニッフィング

モードの場合[1/6]

✓ 保護するWebサーバのIP、PORT、証明書、秘密鍵、暗号化アルゴリズム情報を登録する。

✓保護するWebサーバーの証明書と秘密鍵を事前に準備します。

▪ 暗号化されたパケットを復号化するために、クライアントはWebファイアウォールに登録された証明書で通信します



①Webサーバー情報のコピー（オプション）

- 既存に生成された他のHTTPS保護対象Webサーバルールの設定履歴を反映する。反映内訳は以下の通り。

✓ SSL証明書

✓ HTTP/2を使用するかどうか

✓ 未使用のSSLバージョン

✓ 暗号化アルゴリズムの優先権

✓ SSL情報

✓ マルチドメイン情報

②SSL証明書：保護対象WebサーバのSSL証明書に対して登録する。

システム運用を通し

7. ポリシー設定ー基本設定

運用モード「1/3」

➢ ポリシーバイパスモード

•ポリシーバイパスモードは、パケットドライバPacket Driverで保護対象に設定されているパケットに対してAI_SOCKにアップロードした後、メインエンジン（httpgw）にデータを転送します。メインエンジンは、配信されたデータに対してポリシー的にBypass処理して送信する。

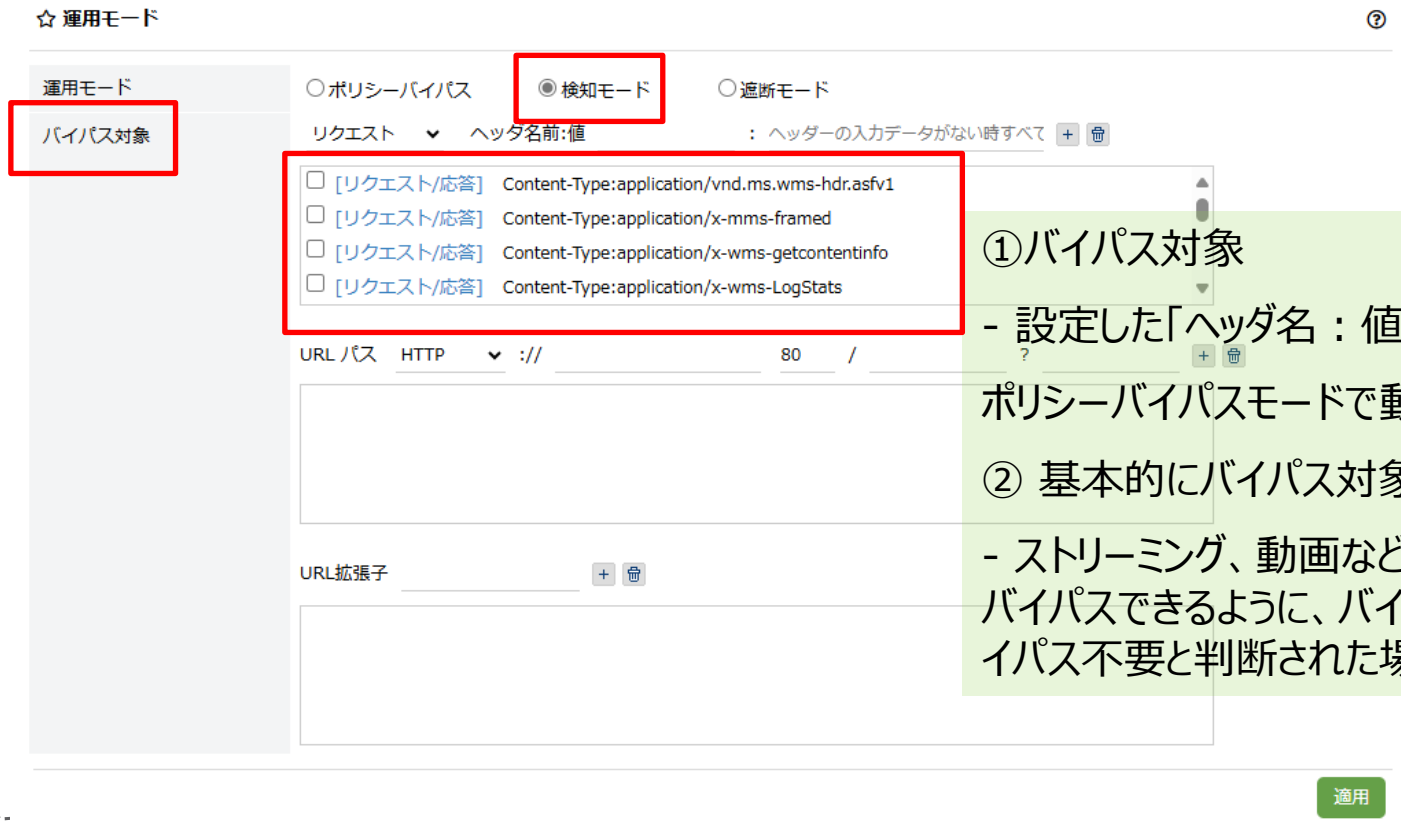
7. ポリシー設定ー基本設定

運用モード「2/3」

➢検出モード

•検出モードは、メインエンジン（httpgw）に渡されたデータにセキュリティポリシーを適用します。

•ポリシーに違反するデータは、検出機能のみを実行して検出ログを生成するモードです。したがって、動作モードが検出モードである場合、アクションが「遮断／クロック／マスキング／回復」に設定されているポリシーによって検出されたデータは「検出」として動作する。



①バイパス対象

- 設定した「ヘッダ名：値」、URLパスまたはURL拡張子にポリシーバイパスモードで動作します。

② 基本的にバイパス対象に含まれているヘッダ値

- ストリーミング、動画などAIWAFでInspectionが不要なデータに対してバイパスできるように、バイパス対象にヘッダ情報がリストアップされている。バイパス不要と判断された場合、該当項目を除去することができる。

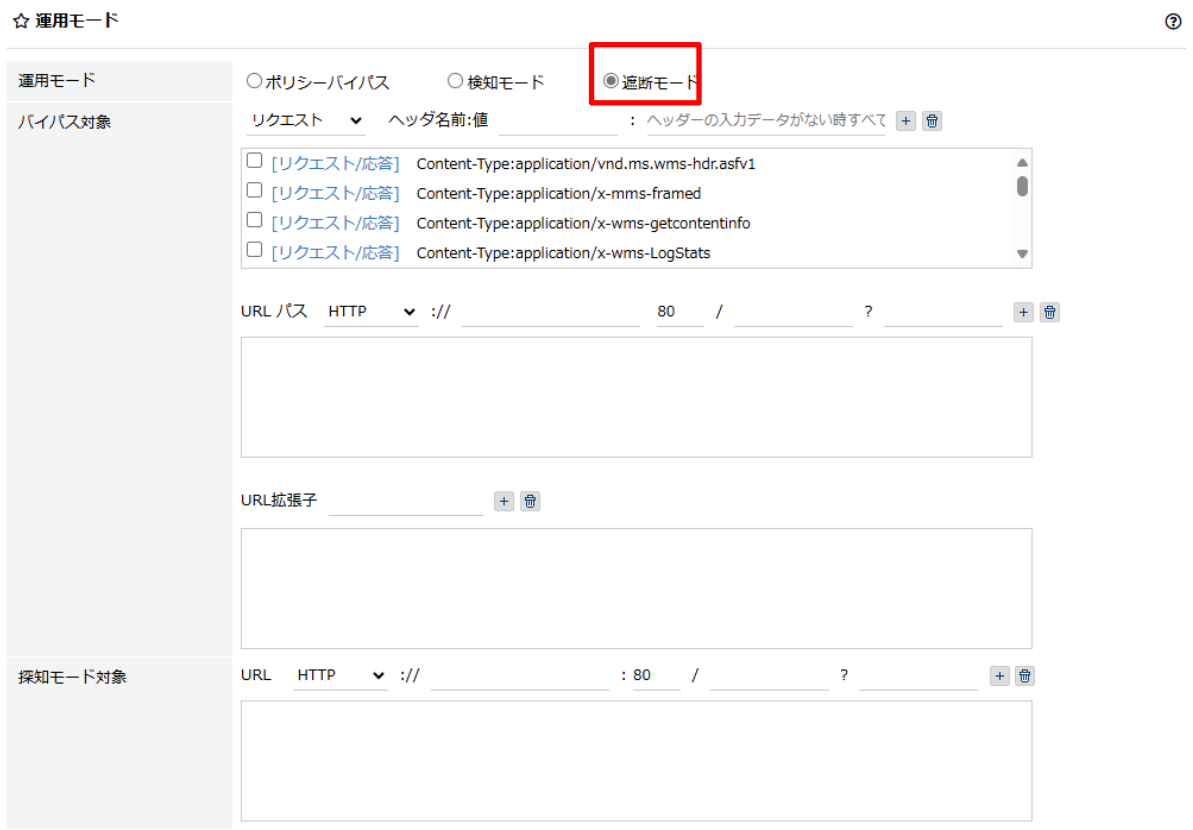
7. ポリシー設定ー基本設定

運用モード「3/3」

➢ 遮断モード

•検出モードは、メインエンジン（httpgw）に渡されたデータにセキュリティポリシーを適用します。

•ポリシーに違反しているデータに対して、アクションが「検出」の場合は検出として機能し、アクションが「ブロック/クロッキング/マスキング/回復」の場合、通常はブロック/クロッキング/マスキング/修復として動作します。



① 検出モード対象 - 設定したURLに対して検出モードで動作するようになる。

7. ポリシー設定ー基本設定

パターンアップデート

➢ 基本設定ーパターンアップデート設定

•オンライン/オフラインパターンの更新をサポートする。

•パターンは約1ヶ月周期で更新され、毎時間パターンサーバーと通信して更新状況を更新します。

•オフラインパターンファイルは「パートナーポータル」に通知され、必要に応じて「技術サポートチーム」に別途要求することができます。

•サーバーアドレス：api.monitorapp.com、ポート：443

7. ポリシー設定ー基本設定

ポリシー同期化設定

➢ 基本設定ーポリシー同期化設定

複数の機器を運用するときに登録されたポリシー同期リストに対応する機器間セキュリティポリシーをリアルタイムで同期する機能

2つのAIWAFがある場合、同期対象リストにそれぞれ相対IWAF IPを追加すると、どの機器でポリシーを変更して適用しても、常に2つの機器が同じポリシーを維持できます。

①自動同期：自動同期機能に設定します。 - ポリシー設定の変更時に自動的にポリシーを同期する - 通信不可同期対象自動削除

② コミュニティ：同期対象と同じコミュニティ値を設定する。コミュニティの値が異なると同期しません。

③対象メニュー：同期対象メニューを設定する。

④同期対象：同期を実行する相手AIWAFのIPを設定する。追加したAIWAFの「同期化状態確認」を確認し、「同期化執行」で同期を実行します。

✓ ポリシー同期設定時の注意事項

- 必ず同期対象機器と「バージョン」、「ビルド」が同一でなければならない。
- 相手機器と同期設定をして混同してポリシーを同期しなければならない対象のポリシーを受け取る場合が発生することがあるので注意する。

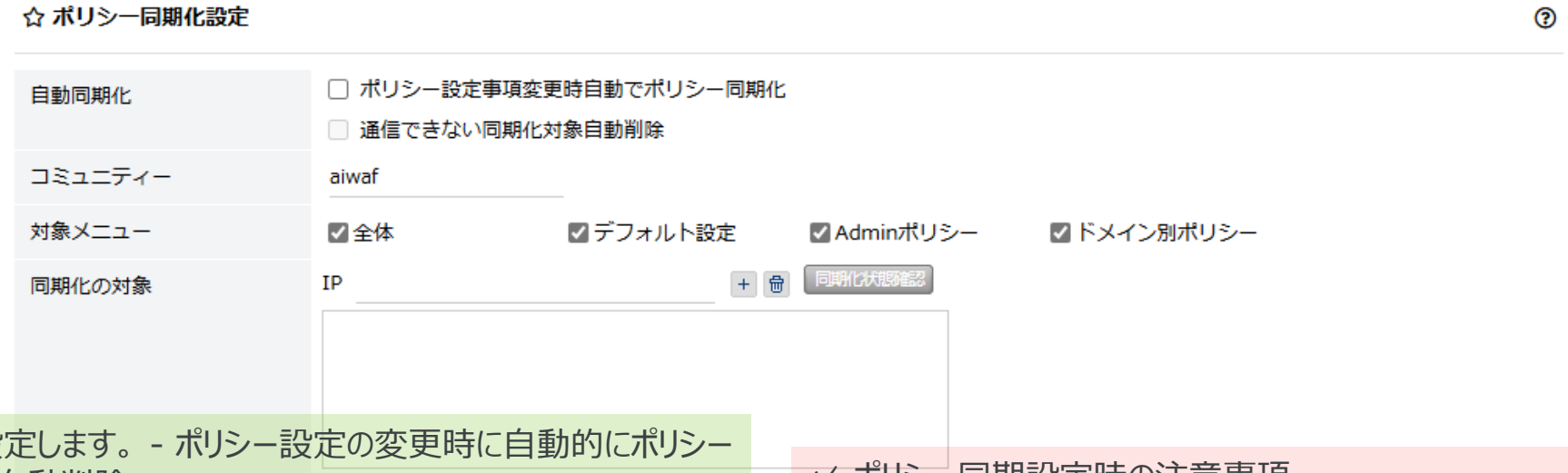
7. ポリシー設定ー基本設定

ポリシー同期化設定

➢ 基本設定ーポリシー同期化設定

複数の機器を運用するときに登録されたポリシー同期リストに対応する機器間セキュリティポリシーをリアルタイムで同期する機能

2つのAIWAFがある場合、同期対象リストにそれぞれ相対IWAF IPを追加すると、どの機器でポリシーを変更して適用しても、常に2つの機器が同じポリシーを維持できます。



①自動同期：自動同期機能に設定します。 - ポリシー設定の変更時に自動的にポリシーを同期する - 通信不可同期対象自動削除

② コミュニティ：同期対象と同じコミュニティ値を設定する。コミュニティの値が異なると同期しません。

③対象メニュー：同期対象メニューを設定する。

④同期対象：同期を実行する相手AIWAFのIPを設定する。追加したAIWAFの「同期化状態確認」を確認し、「同期化執行」で同期を実行します。

✓ ポリシー同期設定時の注意事項

- 必ず同期対象機器と「バージョン」、「ビルド」が同一でなければならない。
- 相手機器と同期設定をして混同してポリシーを同期しなければならない対象のポリシーを受け取る場合が発生することがあるので注意する。

8. ポリシー設定ーAdminポリシー

IPポリシー[1/2]

➢ IPポリシー - IPホワイトリスト（最大ルール登録数：制限なし）

•IPホワイトリストは信頼できるIPリストで、IPホワイトリストに登録されているクライアント/サーバーからのHTTP要求と応答については、いかなる検出ポリシーも実施せずに許可することになります。

•IPホワイトリストは、IPブラックリストよりも優先順位の上にあります。

•単一または帯域で登録可能で、クライアント、サーバーIPの2つの条件はAND条件で動作します。

・クライアントIPとサーバーIPがそれぞれLineにAND条件に設定されている

8. ポリシー設定ーAdminポリシー

IPポリシー[2 /2]

➢ IPポリシー - IPブラックリスト（最大ルール登録数：IP /ポート設定は複数個を含み、最大2048個のIPまで登録可能）

•信頼できないユーザーまたは攻撃者のリストとして、出発地/目的地IPのいずれかがIPブラックリストに該当する場合は、ポリシーを実行する前に検出またはブロックを実行します。

•単一または帯域で登録可能で、クライアント、サーバーIPの2つの条件はAND条件で動作します。

例外クライアントIP設定時

•IPポリシーから例外があっても、Webポリシールールで検出できます。

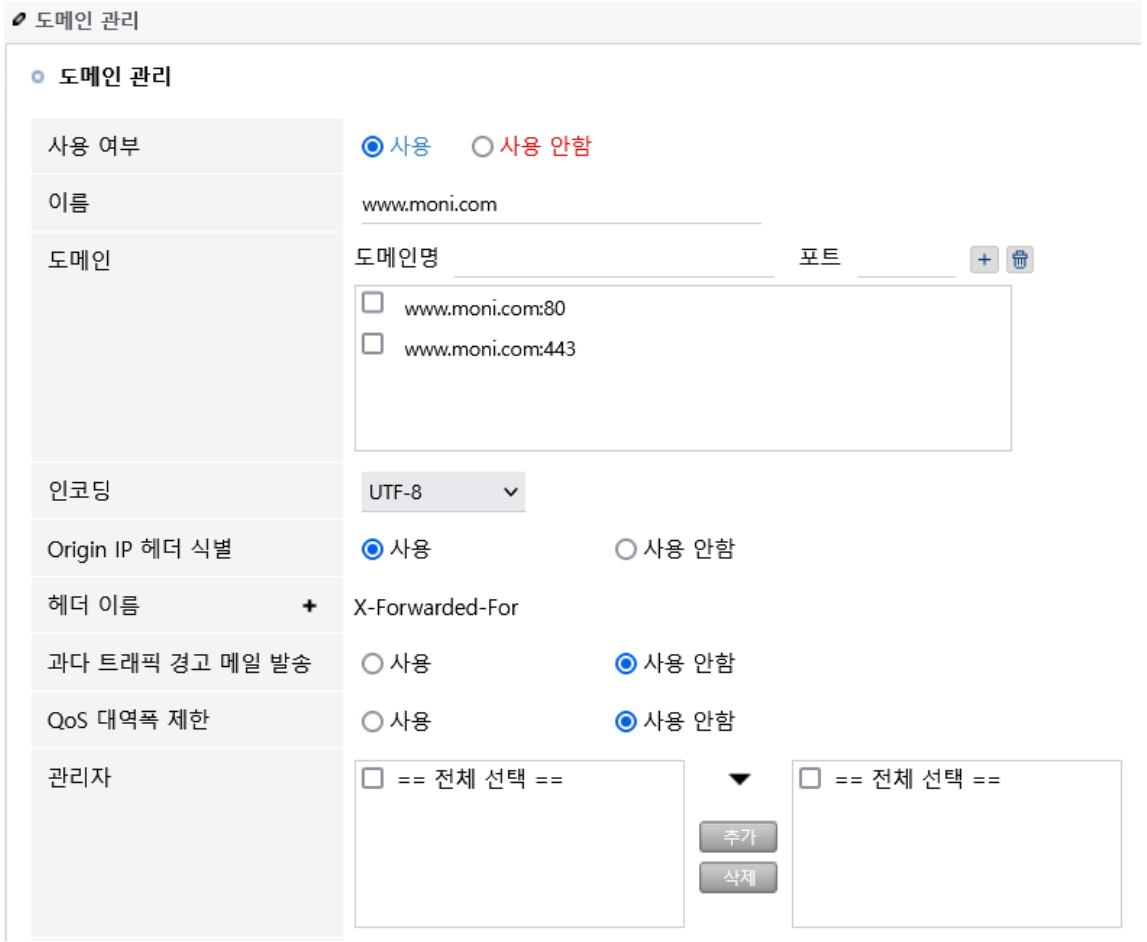
• Ex.）例外IPでもSQLインジェクションなど

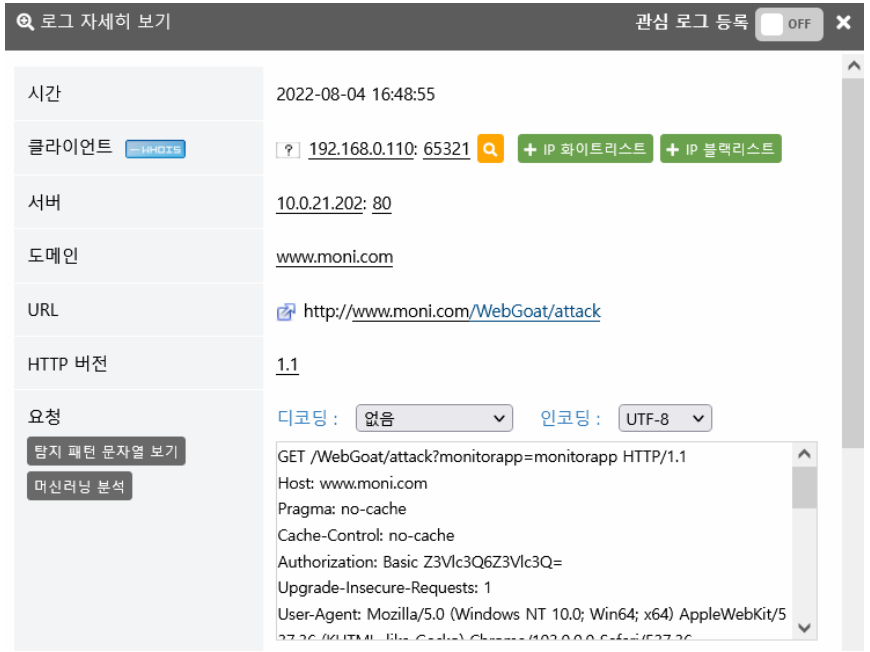
9．ポリシー設定ードメイン別ポリシー

ドメイン管理

➢ドメイン登録（最大ルール登録数：制限なし）[1/2]

•AIWAFのセキュリティポリシーをドメインごとに登録して管理できるメニューであり、許可された管理者のみが使用できます。





ドメイン固有のポリシーを照合するには、クライアント要求でHostヘッダーのドメイン情報と一致する必要があります。

9．ポリシー設定ードメイン別ポリシー

ドメイン管理

➢ドメイン登録[2/2]

- 全体的なポリシー適用順序は、インスペクション順序で適用される。
- 対応するインスペクション順序で、ドメイン固有のポリシー内のセキュリティポリシーに対するルールの適用順序を説明します。

９．ポリシー設定ードメイン別ポリシー

セキュリティーポリシーの適用優先順位[1/2]

➢ セキュリティポリシーの適用優先順位

•HTTPリクエストインスペクションシーケンス

✓ クライアントからの 1 つの要求データに対する AIWAF のインスペクション順序は以下の通りである。

MACホワイトリスト→IPホワイトリスト→ SSLオフロード/ターミネーション→運用モード（ポリシーバイパス）→運用モード（URL拡張子バイパス）→運用モード（ヘッダバイパス）→運用モード（URLバイパス）→CAPTCHA PAGEブロックルール→IPブラックリスト→優先ポリシー：URLアクセスルール→ポリシーリスト→国別リストプロキシ専用ポリシー）→HTTPリクエストフラッディング検出→不正クリック検出→国別IP検出→ドメインURLアクセスルール→URL拡張アクセス制御→POSTリクエスト承認→HTTPメソッド制限検出→HTTPオーバーフロー検出ポリシー（ヘッダ）→スキャナ/プロキシ/スパムボット検出ポリシー→AiLabs→スクリプト検出ポリシー→ディレック トーリアクセス検出→JSONオーバーフロー検出→脆弱性ページアクセス検出→SQLインジェクション攻撃検出→LDAPインジェクション攻撃検出→クロスサイトスクリプト検出→ヘッダ脆弱性検出ポリシー→CSRF攻撃検出→Webサー 脆弱性の検出→アプリケーションの脆弱性の検出→コマンドインジェクションの検出→システムファイルアクセスの検出→悪意のあるファイルアップロードの検出（パターン）→HTTPオーバーフロー検出ポリシー（ボディ）→文字セット制限の検出→悪意のあるファイルのアップロードの検出 （拡張子）→アプリケーションプロファイルの学習と検出→キーワードフィルタリングルール→カスタムパターン→隠しフィールド焼戻し→ハニーポットURL→Webシェルソリューション連動検出（ファイルアップロード、パターン）→プライバシー流入検出

９．ポリシー設定ードメイン別ポリシー

セキュリティーポリシーの適用優先順位[2/2]

➢ セキュリティポリシーの適用優先順位

・HTTPレスポンスインスペクションシーケンス

✓ Web サーバの 1 つの応答データに対する AIWAF のインスペクションシーケンスは以下の通りである。

運用モード（ポリシーバイパス、URL拡張子、URLバイパス）、IPホワイトリスト、URLホワイトリスト（リバースプロキシ専用ポリシー）→運用モード（ヘッダーバイパス）→強制ブラウジング検出→ヘッダークロッキング→検証なしリダイレクト検出→エラーページクロッキング→ディレクトリリスト検出→エラーページクロージング→ページ偽造検出→悪意のあるファイルアクセス検出→マルウェア流布検出→不正ログイン試行→コメントクローキング検出→ハニーポットURL→スクリプト検証→アプリケーションプロファイリング→個人情報の漏洩

10. 環境設定

管理者設定

➢管理者IDの追加/変更/削除ができ、管理者の権限、メニュー別権限、許可IP（製品UI ACL）を設定する。

•最高管理者：AIWAF製品UIで提供されるすべての機能を制限なく設定できます。(Root権限)

•フルマネージャ：フルマネージャは、トップマネージャによって設定されたメニュー固有の権限によって異なりますが、以下の権限に違いがあります。

✓他の管理者の設定はできず、このアカウントの設定のみ可能です。

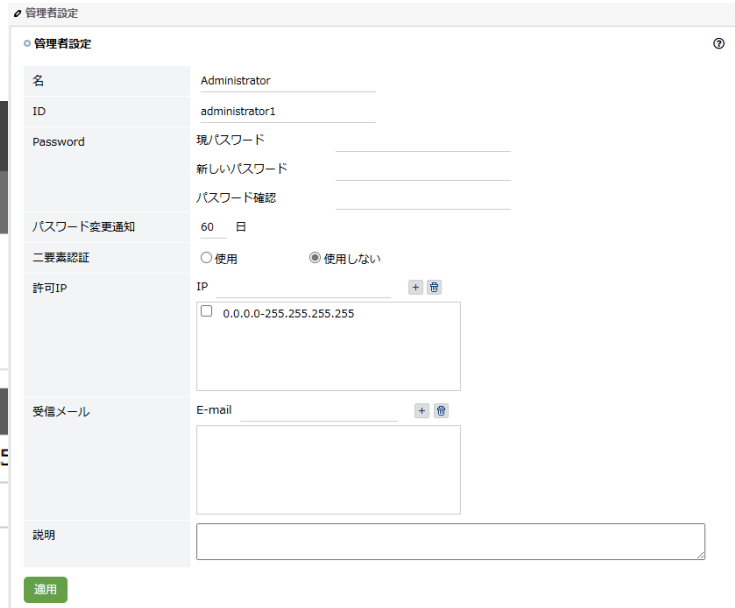
✓ 環境設定に対して読み取りのみ可能で修正は不可能。

•一般管理者：一般管理者また、最高管理者によって設定されたメニュー固有の権限によって異なりますが、管理者全体と以下の違いがあります。

✓「ドメイン別のポリシー>ドメイン管理>管理者」に追加したドメインのポリシーのみを管理できます。

✓特定のドメインからのトラフィックのみを監視できます。(全トラフィックの監視不可)

✓defaultドメインポリシーは管理できません。



10. 環境設定

ログ管理ーESM設定

➢UDP、TCP、SSL通信を使用してESMサーバーに送信するログフォーマットを設定できます。

•1）ESM、2）SIEMなどの統合ログサーバーにSYSLOGを送信し、セキュリティや管理などの分析、監視を可能にします。

•各ログの出荷フォーマットを設定できます。

• 通常 Well known port である UDP 514 (syslog のみ) を使用したが用途が多様化し、セキュリティ事故およびパケット損失の可能性があり、TCP、SSL/TLS プロトコルも活性化された。ESMログはシステムログ、Webトラフィックログは定期的に送信でき、その他のログはイベント発生ごとに送信します。

1）ESM：Enterprise Security Managementの略で、
中央から統合的にセキュリティシステムの現状を監視するシステムである。

2)SIEM: Security Information and Event Managementの略で、すべてのリソースの情報およびセキュリティイベントを統合的に管理するシステムである。製品ごとに機能に違いがあるだろうが、通常ESMよりも高度化された概念のシステムと見ることができる。

•送信されるログのエンコード形式は、UTF-8、EUC-KR、EUC-JP、SJIS、GB2312をサポートします。

①ログ転送周期：システムログ、Webトラフィックログの送信周期を 設定する。（10秒単位、10秒から60秒まで設定可能）

②エンコーディング：発送するログのエンコーディング形式を指定する。(UTF-8、EUC-JP、EUC-JP、SJIS、GB2312対応)

③サーバーアドレス - プロトコル：出荷ログのプロトコルを指定します。- IP, Port: ログを受信する宛先サーバの IP と Port を指定する。④ 検出ログフォーマット：検出ログの発生時間、製品バージョン、クライアント IP＆Port、サーバーIP＆Port、ドメイン、ルール名、要求データ、ホスト、パス、要求長などを送信します。

⑤監査ログフォーマット：監査ログの発生時間、監査ログの種類、監査ログデータなどを送信する。

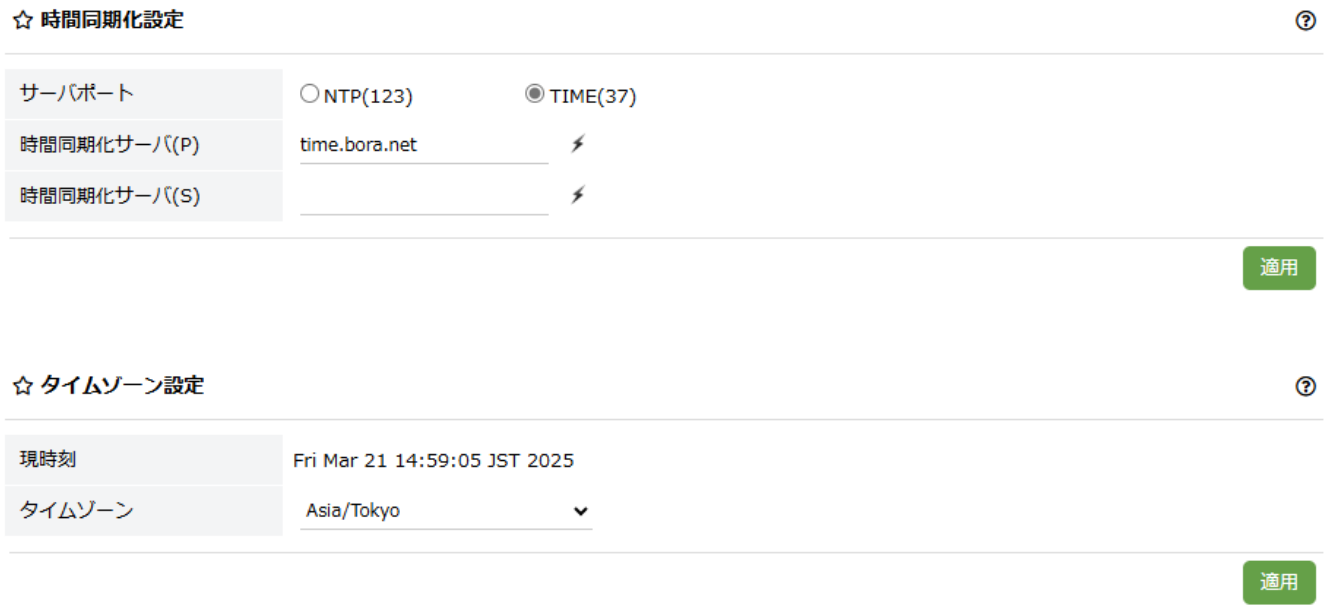
⑥トラフィックログフォーマット：BPS、TPS、CPS、Open CONECTION（CC）、接続者数、攻撃者数、攻撃件数などを発送する。

⑦システムログフォーマット：httpgwデーモンの状態、CPU使用率、リンク状態、メモリ使用率、ディスク使用率、ファン状態、電源状態などを発送する。

10. 環境設定

システム設定ー時間同期化

➢AIWAFは信頼されたNTP、TIMEサーバーから安全なタイムスタンプを提供し、同じ時間値を持つセキュリティ機能と一貫性のあるログデータを記録するために使用され、これらの情報を同期させる必要があります。



①サーバーポート：NTP UDP 123ポート/ TIME UDP 37ポートのうち1日

②時間同期サーバー（P）：PrimaryサーバーのIPまたはドメインを入力します。

③ 時刻同期サーバ(P): SecondaryサーバのIPまたはドメインを入力する。

※注意事項

•ログ情報はAIWAFに設定されている時間に基づいて記録されているため、システムの時刻が正確に一致していないと、ログDBに記録されているログの時刻情報が信頼できなくなるため、必ず時刻同期が必要です。

•crontabによって定期的に（デフォルト設定：毎日04:00分）、または管理者が望むとき（時間同期設定で適用ボタンをクリックしたとき）にNTP、TIMEサーバーから標準時間を提供してシステムに適用します。

10. 環境設定

システム設定ー環境設定同期化設定

➢2台以上のAIWAFを運用する場合、各製品の環境設定をリアルタイムで同期する機能です。

•管理者設定、システム設定、製品設定、ログ管理に対して同期が可能です。

•コミュニティは、同期するAIWAFなどのコミュニティに設定する必要があります。

•各環境設定に追加された機能などをエラーなく同期できるように、必ず同じバージョン、Buildバージョンでのみ環境設定同期設定を行う必要があります。

10. 環境設定

システム設定ーライセンス管理

➢AIWAFの製品ライセンスとアップデートライセンスを登録することができる。

❖製品ライセンスとアップデートライセンス

•製品ライセンス：製品ライセンスが異常であるか有効期限が切れた場合、セキュリティポリシー機能は機能せず、バイパス状態に移行または維持されます。

•アップデートライセンス：アップデートライセンスの有効期限が切れた場合、新しいパターンアップデートはできません。正式製品ライセンス登録日が13ヶ月以内であれば、アップデートライセンスファイルがなくても13ヶ月間はパターンアップデートが可能である。

❖正式ライセンスとデモライセンス

•正式ライセンス：正式に発行手続きをして発行した製品ライセンスです。

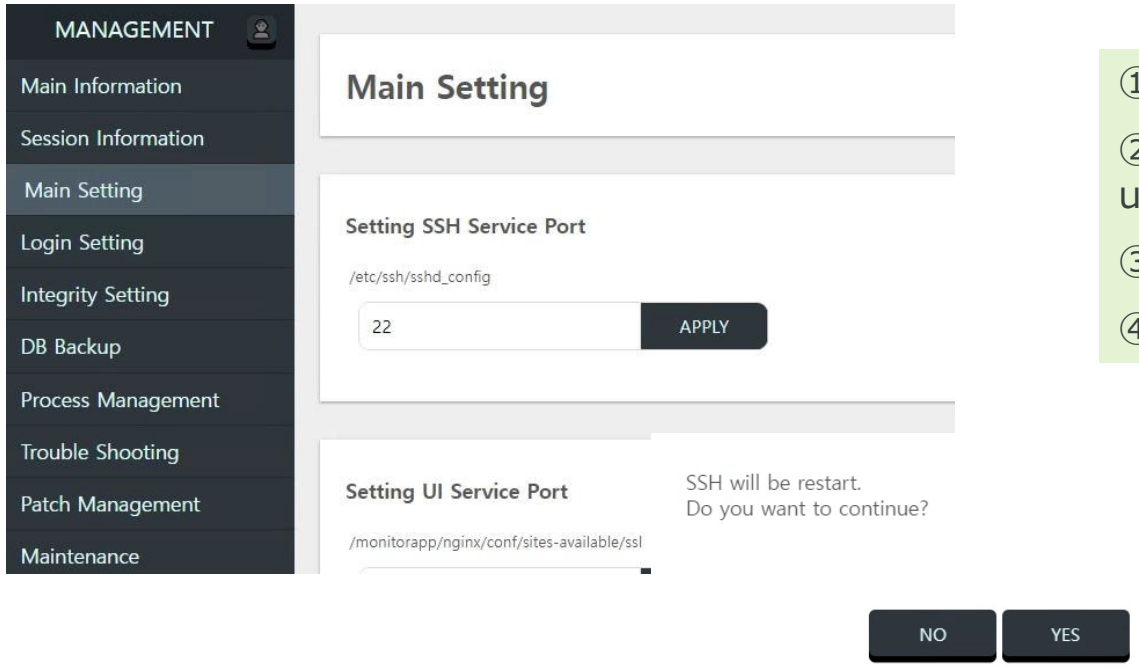
•デモライセンス：PoC、BMTなどの理由でデモライセンスが必要な場合に発行された製品ライセンスです。

11. AIMANAGER WEB

SSH Port 変更

➢初期のSSHは“TCP Port 22”で設定されているが、セキュリティー及び必要により変更できる。

AIMANAGER Web > Main Setting > Setting SSH Service Port



①AIMANAGER Webログイン後のMain Settingクリック

② Setting SSH Server Portの設定（特にない場合はunknown Portで設定を推奨）

③ APPLYクリック

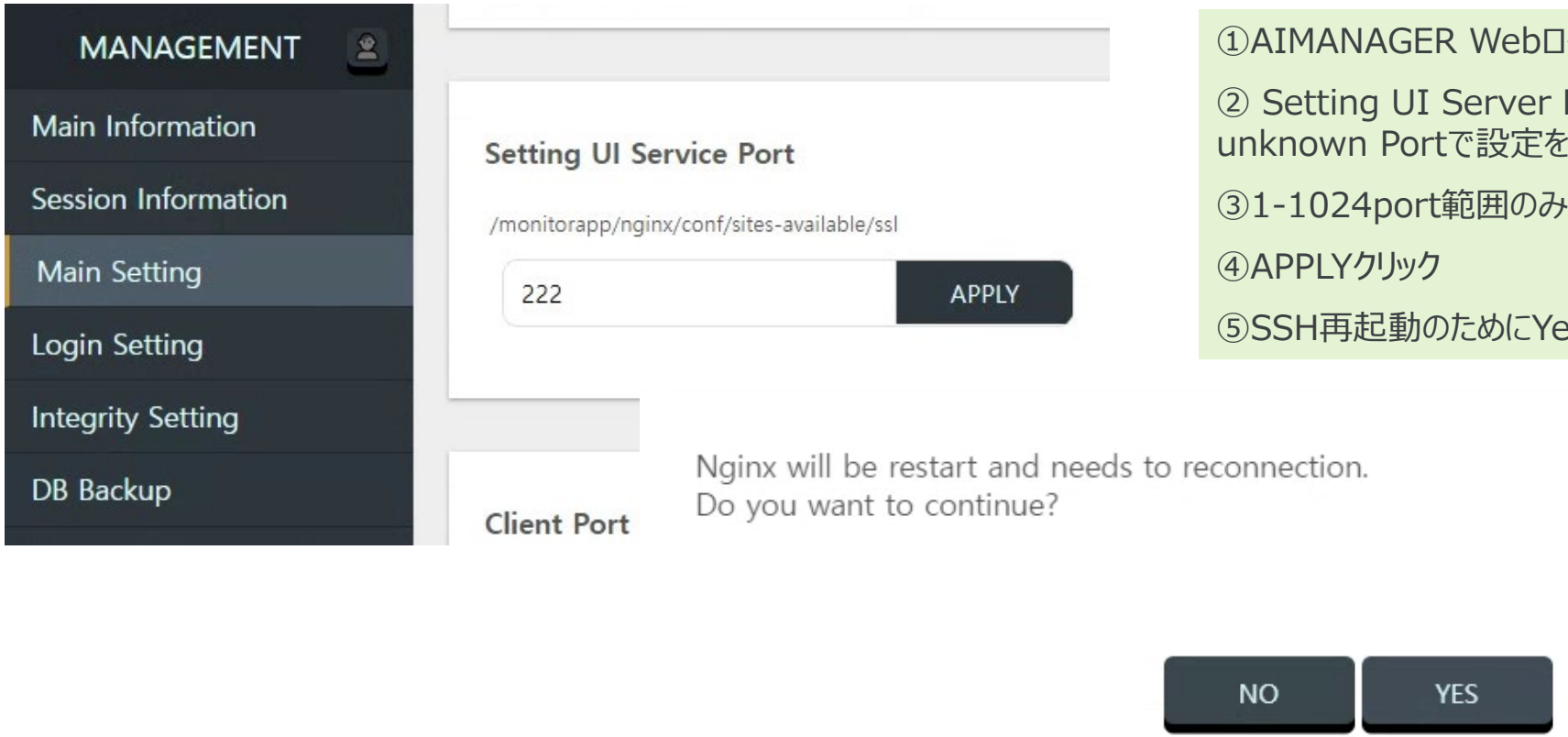
④SSH再起動のためにYesをクリック

11. AIMANAGER WEB

NGINX（WEB）Port 変更

➢初期のGUIは“TCP Port 222”で設定されているが、セキュリティー及び必要により変更できる。

AIMANAGER Web > Main Setting > Setting UI Service Port



①AIMANAGER Webログイン後のMain Settingクリック

② Setting UI Server Portの設定（特にない場合はunknown Portで設定を推奨）

③1-1024port範囲のみで設定可能

④APPLYクリック

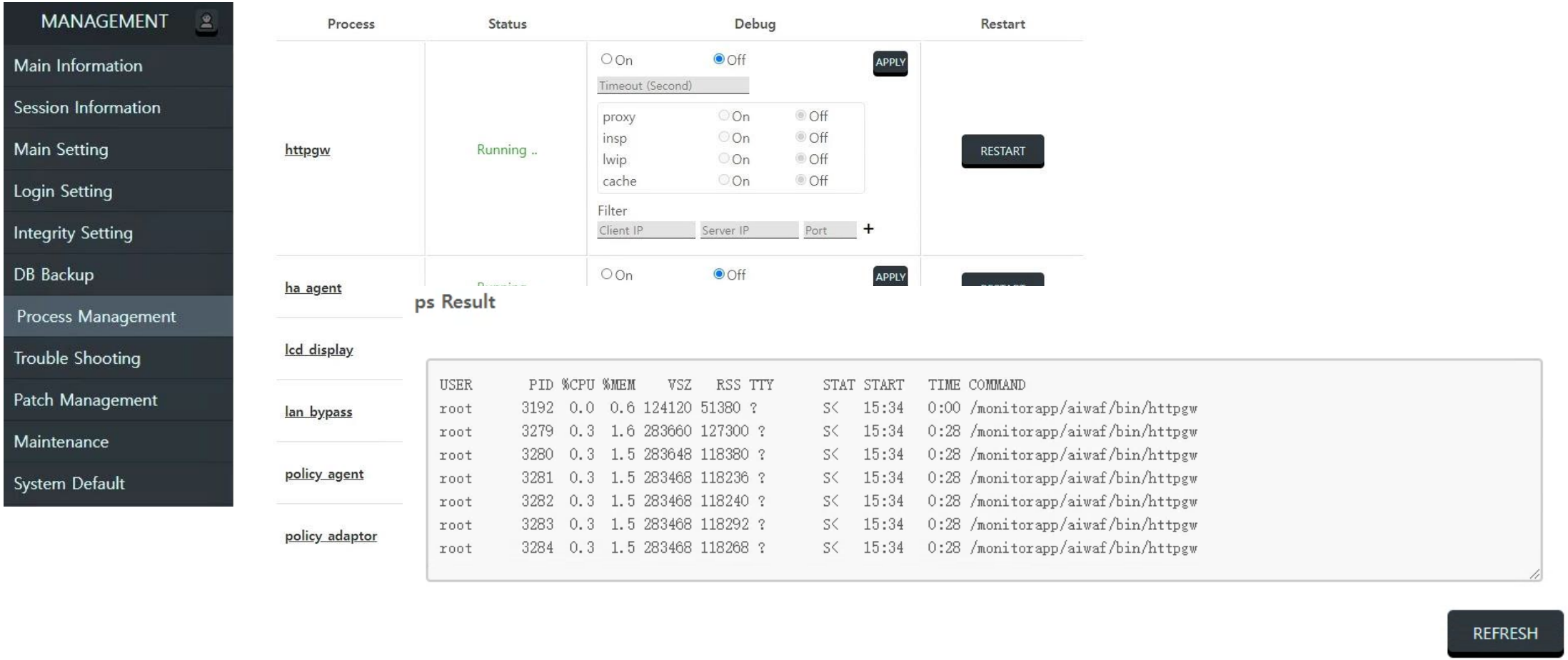
⑤SSH再起動のためにYesをクリック

11. AIMANAGER WEB

プロセス状態確認

➢AIMANAGER Webでプロセス状態チェック

AIMANAGER Web > Process Management



アイティーエム株式会社

URL：https://www.itmanage.co.jp/

お問合せフォーム：https://www.itmanage.co.jp/contact/