

# F5 Advanced WAF

Web アプリケーションファイアウォール  
簡単セットアップガイド (v14.1 対応)

F5 Networks Japan



## 目次

1.	はじめに	4
1.1.	Adv.WAF 動作概要	5
2.	Adv.WAF ポリシー作成の概要	6
2.1.	[Step1] ベースとなる Adv.WAF ポリシーを作成する	7
2.2.	[Step2] シグネチャのチューニング (誤検知の対策)	8
2.3.	[Step3] File Type の設定を行う (強制ブラウジング対策)	8
2.4.	[Step4] 追加機能の要否検討	8
2.5.	最終的なチューニング	8
2.6.	[ご参考] 利用するセキュリティ機能の優先度	9
2.7.	[ご参考] Evasion (回避) テクニックとは	10
3.	スタンドアローン	11
3.1.	スタンドアローンのネットワークサンプル	11
3.2.	構成の概要	12
3.3.	初期設定	13
3.3.1.	管理ポートへの GUI アクセス	13
4.	ネットワークの設定	18
4.1.	VLAN の作成	18
4.2.	Self IP の設定	20
4.3.	ルーティングの設定	21
4.3.1.	デフォルトゲートウェイの設定	21
4.3.2.	Web アプリケーションサーバへのルーティング設定	21
5.	[Step1] ベースとなる WAF ポリシーを作成する	22
5.1.	Deployment Wizard による設定	22
5.2.	Virtual Server の設定の確認	25
5.3.	Learning and Blocking Setting の確認と変更	26
5.3.1.	Blocking Setting の設定変更	26
5.3.2.	Data Guard の無効化-2	27
5.4.	シグネチャの状態確認	28
5.4.1.	Attack Signature Configuration	28
5.4.2.	Attack signature List	29
5.4.2.1.	各シグネチャ状態の確認	29
5.4.3.	ステー징ログの設定	30
6.	シグネチャ動作の確認	31
6.1.	例: SQL インジェクション	31
6.2.	各シグネチャの Staging の解除	34
6.3.	Enforcement Mode を Blocking に変更	37
7.	[Step2] シグネチャのチューニング (誤検知の対策)	38
7.1.	誤検知の例	38
7.2.	[対策 1] 誤検知したパラメータをホワイトリスト化する (シグネチャ検知はしない状態にする)	39
7.3.	[対策 2] シグネチャの誤検知が発生したパラメータで、そのシグネチャを無効化する	41
7.4.	[対策 3] 誤検知したシグネチャを全体で無効化し、そのシグネチャで守りたいパラメータだけに適用する	43
8.	[Step3] File Type の設定を行う (強制ブラウジング対策)	47
8.1.	File Types の設定	47
8.1.1.	File Types の学習	47
9.	[Step4] 追加機能の要否検討	51
9.1.	Data Guard	52
9.2.	L7 DoS への対策 <ご参考>	54
9.2.1.	TPS-Based DoS	54
9.2.2.	Stress-Based DoS	57
9.3.	Brute Force の対策	58
9.3.1.	Brute Force 対策の設定	58
9.4.	CSRF (Cross Site Request Forgery) への対策	63
9.4.1.	CSRF 攻撃とは	63
9.4.2.	CSRF 対策の設定	64
9.5.	Threat Campaigns シグネチャ <ご参考>	68

9.6.	最終的なチューニング .....	69
9.7.	例:パラメータ・タンパリング .....	69
9.7.1.	攻撃例.....	69
9.7.2.	パラメータ・タンパリングの防御方法.....	71
9.7.3.	パラメータ・タンパリング対策の設定.....	71
9.8.	例:セッションハイジャック .....	75
9.8.1.	攻撃例.....	75
9.8.2.	セッションハイジャックの防御方法.....	76
9.8.3.	セッションハイジャック対策の設定.....	77
10.	Adv.WAF ポリシーの保存 .....	82
11.	レポートिंग .....	84
12.	IP Intelligence の設定 .....	85
13.	Geolocation の設定 .....	86
14.	ブロック時のレスポンスページの変更 .....	87
15.	シグネチャの運用 .....	88
15.1.	シグネチャセットとは .....	88
15.1.1.	シグネチャの属性.....	88
15.1.2.	シグネチャセットの割り当て方法 .....	90
15.1.3.	「Basic」シグネチャセット .....	91
15.1.4.	「Attack Type Specific」シグネチャセット.....	91
15.1.5.	「User-defined」シグネチャセット .....	91
15.2.	シグネチャセットの作成.....	92
15.3.	新しい Signature の更新 .....	94
15.3.1.	シグネチャが更新された直後の振る舞い.....	94
15.3.2.	シグネチャ更新の実行.....	95
15.4.	更新されたシグネチャのステージング状態確認 .....	98
15.5.	CVE 番号によるシグネチャの検索 .....	100
16.	[ご参考]ログの外部出力の設定.....	101
16.1.	Logging Profile の作成 .....	101
16.2.	Logging Profile の VS への適用.....	102
17.	冗長化 .....	103
17.1.	冗長化のネットワークサンプル .....	103
17.2.	Active 機の設定 .....	104
17.2.1.	VLAN、SelfIP の設定 .....	104
17.2.2.	Device の設定 .....	105
17.2.3.	時刻同期(NTP)設定 .....	106
17.3.	Standby 機(bigYYY.f5jp.local)の設定 .....	108
17.4.	デバイストラストの設定 .....	110
17.5.	デバイスグループの設定 .....	113
17.6.	トラフィックグループの設定.....	114
17.7.	ConfigSync.....	117
17.8.	Traffic-group-1 の Active/Standby の切替え .....	120
18.	おわりに .....	122

## 1. はじめに

本セットアップガイドにて F5 Advanced Web Application Firewall (以下、Adv.WAF) の設定方法についてご案内します。

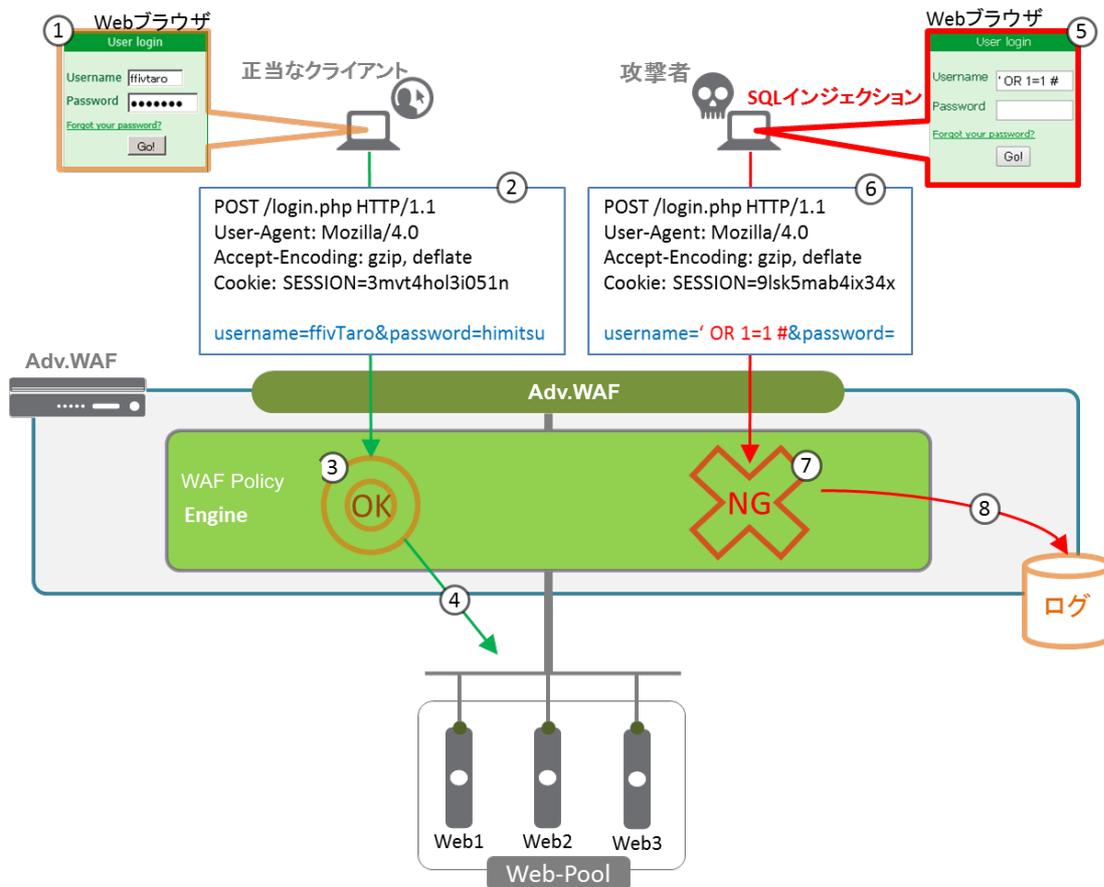
Adv.WAF は、Web アプリケーションファイアウォールです。Adv.WAF によって、Web アプリケーション特有の攻撃に対する防御が可能となります。また、L7 レベルの DoS 攻撃に対する防御機能も兼ね備えています。

Adv.WAF と Local Traffic Manager (以下、LTM) を一つの筐体内に実装することができるので、高度なサーバロードバランシングを行いつつ、Web アプリケーションファイアウォールとしても利用するということが一つのプラットフォーム上で実現できます。

本ガイドでは、Adv.WAF の設定をスムーズに進められるように、必要となる典型的なセットアップ手法を、豊富なスクリーンショットを交えて解説します。

## 1.1. Adv.WAF 動作概要

Adv.WAF の基本動作イメージを以下に示します。



SQL インジェクション攻撃の例:

- ① 正当なクライアントが、ブラウザのフォーム認証画面にユーザ名とパスワードを入力して「Go!」ボタンを押す。
- ② そのユーザ名とパスワードの値が入った HTTP リクエストが、Adv.WAF の VS へ送られる。
- ③ Adv.WAF は、そのユーザ名とパスワードをチェック。ポリシーに違反していないことを確認。
- ④ Adv.WAF は Web-pool へその HTTP リクエストを転送する。
- ⑤ 攻撃者が、ブラウザのフォーム認証画面で、ユーザ名として「' OR 1=1 #」と入力して「Go!」ボタンを押す。  
(SQL インジェクション攻撃)
- ⑥ ユーザ名の変数に値:「' OR 1=1 #」が入った HTTP リクエストが、Adv.WAF の VS へ送られる。
- ⑦ Adv.WAF は、そのユーザ名とパスワードをチェック。不正な値:SQL インジェクション攻撃であることを検知。
- ⑧ その攻撃をブロックし、ログとして記録する。

以降、このような Web アプリケーションを狙った攻撃を防御する設定方法を示します。

## 2. Adv.WAF ポリシー作成の概要

このセクションでは、Adv.WAF ポリシー作成ステップの概要を記載します。

ポリシー作成にはいくつかのアプローチがありますが、本ガイドの作成ステップにより、早く且つかなり高い精度で攻撃を防御できるポリシーが生成できます。

本ガイドでは、Web アプリケーションのセキュリティポリシーを素早く作成することを目的とした、Rapid Deployment Security Policy (以下、RDSP) をベースポリシーとして利用します。

---

### [Note]

Adv.WAF ポリシーの作成方法には他に、Policy Builder 機能 (自動的にパラメータ、URL、ファイル拡張子などを学習して、ポリシーを自動作成する機能)があります。しかし、以下の理由から本ガイドの対象外としています。

- 学習の期間として1ヶ月～3ヶ月を基本とする。(時間がかかる)
  - 自動的にポリシーが作られるので、どのような設定がなされたのかを管理者が把握しづらい (Adv.WAF の深い理解が必要)
  - 管理者が、自動的に生成されたポリシー設定の変更要否の最終判断をしなければならない (Adv.WAF の深い理解が必要)
-

## 2.1. [Step1] ベースとなる Adv.WAF ポリシーを作成する

### (1) Rapid Deployment Security Policy (RDSP) の利用

RDSP には以下のセキュリティチェック機能がデフォルトで含まれています。(v13.1.x 現在)

Performs HTTP compliance checks	HTTP プロトコル標準に合致しているかのチェック
Checks for mandatory HTTP headers	必要な HTTP ヘッダのチェック
Stops information leakage	情報漏えい停止
Prevents illegal HTTP methods from being used in a request	HTTP Request の中の違反 HTTP method を防御
Checks response codes	Response コードをチェック
Enforces cookie RFC compliance	Cookie が RFC 標準に合致しているかのチェック
Applies attack signatures to requests	攻撃シグネチャによる検知
Detects evasion technique	イベーション(回避)テクニックの検知
Prevents access from disallowed geolocations	無許可の地域からのアクセスを防御
Prevents access from disallowed users, sessions, and IP addresses	無許可のユーザ、セッション、IPアドレスからのアクセスを防御
Checks whether request length exceeds defined buffer size	定義済みバッファサイズ超過のチェック
Detects disallowed file upload content	無許可のアップロードファイルコンテンツの防御
Checks for characters that failed to convert	コンバートに失敗した文字のチェック
Looks for requests with modified ASM cookies	ASM Cookie が改ざんされたリクエストかどうかのチェック

その他、RDSP の設定において、以下 2 つについての無効化を検討します。

- ① 無効化を推奨する機能
  - Failed to convert character: 日本語サイトの場合、誤検知しやすいため。
- ② 無効化を検討すべき機能
  - Data Guard: パフォーマンスへの影響を考慮し、不要なら OFF にすべき。

### (2) シグネチャセットの割当て

利用するアプリケーションに応じて、最小限の攻撃シグネチャセットを適用します。

## 2.2. [Step2] シグネチャのチューニング（誤検知の対策）

誤検知が発生した場合に対して、以下 3 つの手段のいずれかを利用します。

- ① [対策 1] 誤検知したパラメータをホワイトリスト化する（シグネチャ検知はしない状態にする）
- ② [対策 2] シグネチャの誤検知が発生したパラメータで、そのシグネチャを無効化する（ホワイトリスト化する）
- ③ [対策 3] 誤検知したシグネチャを全体で無効化し、そのシグネチャで守りたいパラメータだけに適用する

## 2.3. [Step3] File Type の設定を行う（強制ブラウジング対策）

強制ブラウジング攻撃の対策として、File Type の設定を行います。

### (1) File Type の学習

Web アプリケーションページの巡回により、File Type を学習します。

### (2) File Type の設定

その学習結果を見て、以下 2 つのどちらの対応を取るかを判断し、設定します。

- ① Disallow File Type で対応する（利用しない File Type で、危険と判断されるものを指定する）
- ② Allow File Type で対応する（利用する File Type をすべて指定する）

## 2.4. [Step4] 追加機能の要否検討

以下の機能が必要かどうかを判断し、必要なものを有効にします。

- ① Data Guard（クレジットカード番号のマスキング）
- ② L7 DoS への対策
- ③ Brute Force への対策
- ④ CSRF への対策

## 2.5. 最終的なチューニング

[Step1]～[Step4]によって、Web アプリケーションへの攻撃はかなり高い精度で防御可能と考えます。

ここまでのステップで対応できない攻撃に対する対策としては、以下が考えられます。

- ① ホワイトリスト利用による詳細設定
- ② カスタマイズしたシグネチャ作成による対策
- ③ iRules による攻撃回避

上記①の手法については、サンプルとして 2 つの攻撃手法とその防御設定にて解説します。

上記②及び③については、大半のケースがお客様の環境依存となることから、ヒアリングを実施させて頂き、その情報を元に対策する必要がでてきます。

この対応については F5 コンサルティングサービスにてお受けいたしますので、必要となった際には弊社へご連絡ください。

## 2.6. [ご参考] 利用するセキュリティ機能の優先度

Adv.WAF のセキュリティ機能は豊富なので、どの機能を使えばよいか判断に迷うことがあります。

以下表は一つのガイドラインとして、一般的な Web アプリケーションで利用すべき機能の優先度を記載しました。

Web アプリケーション次第で利用すべき機能は異なりますが、目安として参考にしてください。

◎: ご利用を推奨する機能です。

○: 多くの Web アプリケーションで適用することが望ましいと考えられる機能です。

▽: 必要に応じて適用、という位置づけです。

	設定項目	推奨	コメント	
1	<b>Rapid Deployment Security Policy</b>	◎	一部、無効化を推奨する機能あり (既述)	
2	<b>シグネチャ</b>	◎	必要最小限のシグネチャセットのみを適用。	
3	ホワイトリスト	<b>File Type</b>	◎	Adv.WAF を通過させるファイルを指定。 ファイルタイプ数によっては Disallow の設定の方が、管理が楽だと思われる。
		URI	▽	これらはアプリケーションによっては数が膨大になる。 よって、例外処理が必要となるものだけ抜き出して設定したほうが良い。
		Parameter	▽	
		Header	▽	
4	<b>DoS</b>	○	多量のリクエストによるアプリケーションへの影響が懸念される場合	
5	<b>Brute Force</b>	○	不正ログインを防止したい場合	
6	Web Scraping	▽	ボットによる情報収集を拒否したい場合	
7	<b>CSRF</b>	○	CSRF による攻撃を守りたい場合	
8	Data Guard	▽	クレジットカード番号漏洩がありえる場合	
9	Session 管理	▽	ログイン後にしか表示しない画面を制限したい場合	

## 2.7. [ご参考] Evasion(回避)テクニックとは

RDSP によって有効になる機能のうち、Evasion テクニックとはどのようなものかがやや分かりにくいと思いますので、いくつかの具体的な攻撃をサンプルとして解説します。

- ディレクトリ・トラバーサル (Directory Traversal)

URL の一部ではない、「../」のような文字列を URL に組み込んで HTTP リクエストを送ってくる攻撃。  
例えば、攻撃者から「http://example.com/../../../../private\_file.txt」というリクエストが発せられたとき、システムは、Web アプリケーションがユーザに提供すべきではないファイルを返してしまうかもしれない。

この攻撃は、Web Server root をバイパスして、さまざまなファイルをリクエストすることを目的としている。  
この攻撃によって、システムファイル、またはプライベートディレクトリ・リソースが奪取される可能性がある。

- マルチプル・エンコーディング (Multiple Encoding)

複数回の%エンコーディング(URL エンコードともいう)を繰り返し実施することで、文字を隠蔽する攻撃。  
例えば、%エンコーディングによって、「<」は「%3c」に変換される。攻撃者は、これを攻撃に使うために、もう一度エンコードして隠蔽する。「%3c」をもう一度エンコードすると、「%253c」になる(「%」はエンコードすると「%25」になる)。

この攻撃によってメタキャラクタを隠蔽できるので、クロスサイトスクリプティングやディレクトリ・トラバーサル、SQL インジェクションなどのような攻撃を、一回のデコーディングでは検知できないようにすることが可能になる。

- ベア・バイト・デコーディング (Bare byte decoding)

ASCII 文字は 7 ビットで英数字と少数の記号を表現するコードであり、0x00~0x7F の 128 種類の文字を扱う。  
0x00~0x7F の範囲より上の 0x80~0xFF の範囲の文字(=最上位ビットが 1 の文字であった場合、ブラウザによっては最上位ビットが無視され、0x00~0x7F として扱われる。

例えば、メタキャラクタ:「<」は ASCII では「0x3C」なので、Web アプリケーションは「0x3C」の入力をエスケープすることでクロスサイトスクリプティング攻撃を防いでいる。しかし、「0xBC」が防がれていないと、ブラウザ上では「<」として処理され、クロスサイトスクリプティング攻撃が成立してしまう、という可能性がある。

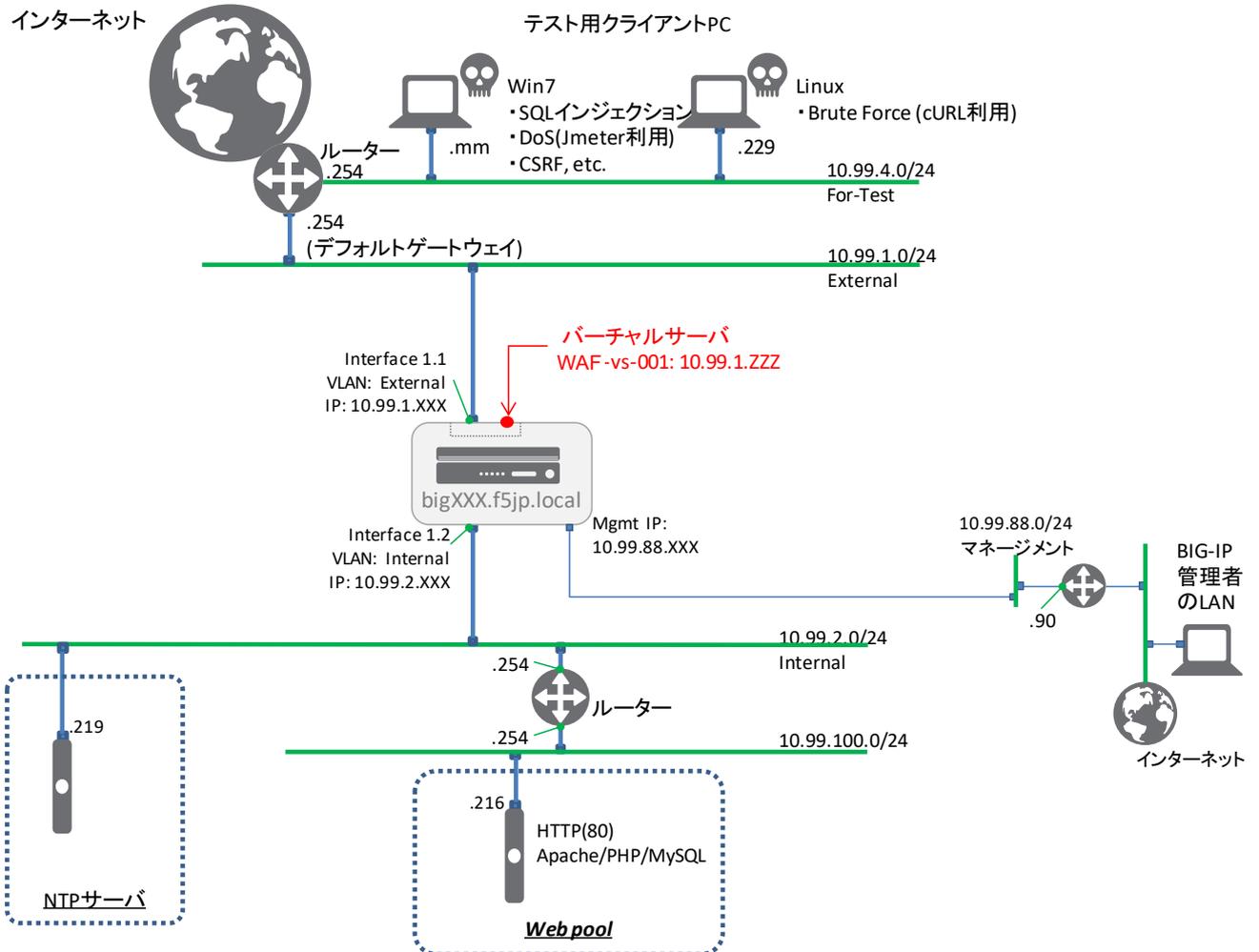
文字	US-ASCII		最上位ビットを 1 にセット	
	16 進	2 進	16 進	2 進
"	0x22	00100010	0xA2	10100010
<	0x3C	00111100	0xBC	10111100
>	0x3E	00111110	0xBE	10111110

Evasion テクニック検知を有効にすることで、このような既知の攻撃を防御することが可能となります。

### 3. スタンドアローン

#### 3.1. スタンドアローンのネットワークサンプル

まずは、冗長化しない状態を想定して、1台のみ設定していきます。



ここでは、Adv.WAF の Virtual Server は 10.99.1.ZZZ:80 を設定します。

プールメンバーには、以下の WEB サーバ: 10.99.100.216:443 を設定します。

Adv.WAF のデフォルトゲートウェイは、インターネット方向を想定したルーター:10.99.1.254 に設定します。

Web サーバのデフォルトゲートウェイは、Adv.WAF の Internal インタフェース宛(10.99.2.XXX)に設定します。

動作確認は、テスト用に設置した PC(図中の「テスト用クライアント」)から行うこととします。

## 3.2. 構成の概要

テスト用クライアント PC からバーチャルサーバ: WAF-vs-001 に対して、Web アプリケーションに対する攻撃を仕掛けます。Adv.WAF によって、その攻撃をどのように検知・防御するかを記載します。

本ガイドで攻撃対象となる Web アプリケーションは、Apache, PHP, MySQL で構成されたオークション用サイトを利用します。

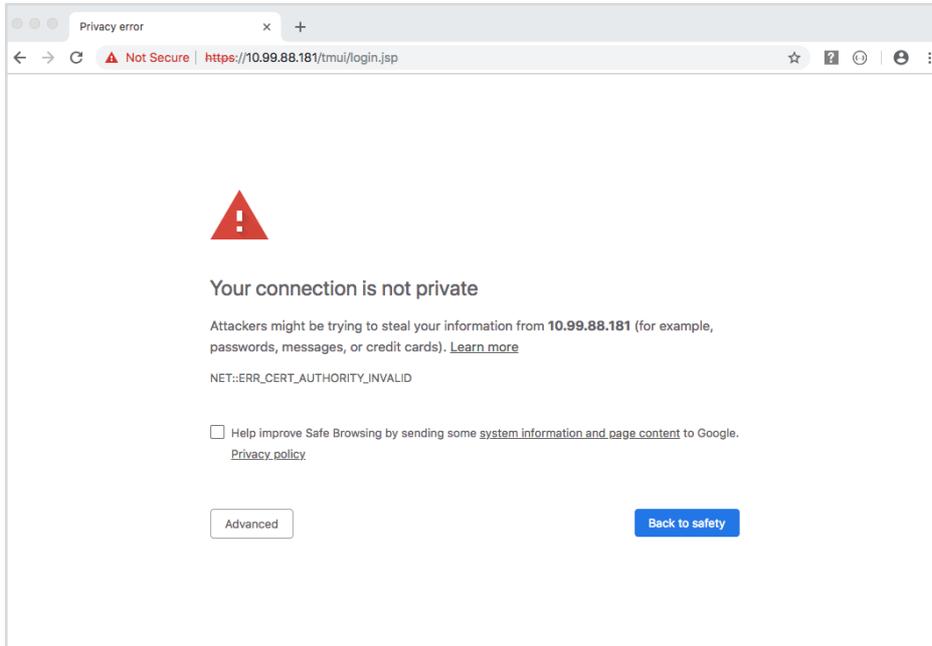
Web アプリケーションにログイン可能なユーザとして、F5 LAB 環境では 8 つ (f5user1~f5user8) を設定しています。また、本ガイドは、Adv.WAF の初期設定から LTM のサーバロードバランシング設定ができるまでの基本的な知識は習得済みである前提とします。

また、管理用のマネージメント IP アドレスは設定済みである前提とします。

### 3.3. 初期設定

#### 3.3.1. 管理ポートへの GUI アクセス

- (1) 管理用 PC から、設定した BIG-IP の管理 IP アドレスへ、HTTPS でアクセスします。デフォルトの証明書は、正式に取得した証明書ではないため、以下のような画面が現れますが、「続行する」を選択してください。



- (2) ログイン画面が現れますので、以下のデフォルトの ID と Password でログインしてください。

ID: **admin**

Password: **admin**



- (3) バージョン 14.0 より、デフォルトで BIG-IP のセキュアパスワードポリシーが有効となっています。パスワードポリシーを変更しない限り、v13.0 以前のデフォルトパスワードは利用できません。

F5LAB では以下のように設定し、Save ボタンを押します。

Current Password: **admin**

New Password: **ilovef5**

Confirm: **ilovef5**

- (4) 設定したパスワードでログインし直します。

- (5) 「Next」ボタンを押します。

(6) ライセンス画面が出ます。「Next」ボタンを押します。(ライセンスが BIG-IQ License Manager で管理されている場合は、Next ボタンはクリック出来ませんので、Resource Provisioning をクリックして下さい。)

~中略~

(7) プロビジョニング画面がでますが、デフォルトで選択されている LTM をはずし、ASM にチェックを入れて、Next ボタンを押します。(プロビジョニングにはしばらく時間がかかります。)

Module	Provisioning	License Status	Required Disk (GB)	Required Memory (MB)
Management (MGMT)	Small	N/A	0	1264
Carrier Grade NAT (CGNAT)	Disabled	Licensed	0	0
Local Traffic (LTM)	None	Licensed	0	2400
Application Security (ASM)	<input checked="" type="checkbox"/> Nominal	Licensed	20	1492
Fraud Protection Service (FPS)	None	Licensed	12	544
Global Traffic (DNS)	None	Licensed	0	148
Link Controller (LC)	None	Unlicensed	0	148
Access Policy (APM)	None	Licensed	12	494

~中略~

(8) Continue ボタンを選択します。

Hostname: bigip1 | Date: Jul 24, 2019 | User: admin  
IP Address: 10.99.88.181 | Time: 7:45 PM (PDT) | Role: Administrator | Partition: Common | Log out

ONLINE (ACTIVE)  
Standalone

Main | Help | About | Setup Utility >> Device Certificates

Setup Utility

- Introduction
- License
- Resource Provisioning
- Device Certificates
- Platform
- Network
- Redundancy
- VLANs
- NTP
- DNS
- ConfigSync
- Failover
- Mirroring
- Active/Standby Pair
- Discover Peer

**General Properties**

Name	server.crt
Certificate Subject(s)	localhost.localdomain, MyCompany

**Certificate Properties**

Public Key Type	RSA
Public Key Size	2048 bits
Expires	Jul 7 2029 08:07:39 GMT

**Unable to contact BIG-IP device**  
Thu Jul 25 2019 11:43:34

The BIG-IP Configuration utility makes periodic requests for status information in the background while you work. Unfortunately, the network connection to your BIG-IP system has been interrupted and the last status request failed.

**Instructions:**

1. Check your network connection. An interruption in your network connectivity or a change in network conditions may prevent you from accessing this BIG-IP system.
2. A system administrator may have initiated a system reboot. If this is the case, the BIG-IP system should become available after a few minutes.
3. The system may not be responding. The BIG-IP system may be writing a large configuration to disk, experiencing other difficulty, or may have been taken offline by an administrator.

**Elapsed Time:** 55 seconds

- ✔ **Waiting to establish a connection with the device...**  
If a connection is not reestablished after a few minutes, contact your system administrator.
- ✔ **Device connection has been restored.**  
A connection to your BIG-IP system has been reestablished.

(9) SSL 証明書の確認がされますが、デフォルトのまま、「Next」ボタンを押します。

Hostname: bigip1 | Date: Jul 24, 2019 | User: admin  
IP Address: 10.99.88.181 | Time: 7:47 PM (PDT) | Role: Administrator | Partition: Common | Log out

ONLINE (ACTIVE)  
Standalone

Main | Help | About | Setup Utility >> Device Certificates

Setup Utility

- Introduction
- License
- Resource Provisioning
- Device Certificates
- Platform
- Network
- Redundancy
- VLANs
- NTP
- DNS
- ConfigSync
- Failover
- Mirroring
- Active/Standby Pair
- Discover Peer

**General Properties**

Name	server.crt
Certificate Subject(s)	localhost.localdomain, MyCompany

**Certificate Properties**

Public Key Type	RSA
Public Key Size	2048 bits
Expires	Jul 7 2029 08:07:39 GMT
Version	3
Serial Number	be:77:a7:19:39:7d:ef:ee
Fingerprint	SHA256/E7:9C:EA:EA:EF:E3:C6:0F:8D:67:13:24:EC:FC:5D:DE:44:87:AC:5D:0D:7E:24:22:CE:E3:F0:F9:9F:8A:7F:9E
Subject	Common Name: localhost.localdomain Organization: MyCompany Division: MyOrg Locality: Seattle State Or Province: WA Country: --
Issuer	Self
Email	root@localhost.localdomain
Subject Alternative Name	

(10) ホスト名、タイムゾーン、Root/Adminそれぞれのパスワードを設定します。「Next」ボタンを押します。

Hostname: bigip1, Date: Jul 11, 2019, User: admin, Role: Administrator, Partition: Common, Log out

ONLINE (ACTIVE) Standalone

Activation Complete  
Configure your platform.

Main Help About Setup Utility » Platform

Setup Utility

- Introduction
- License
- Resource Provisioning
- Device Certificates
- Platform
- Network
- Redundancy
- VLANs
- NTP
- DNS
- ConfigSync
- Failover
- Mirroring
- Active/Standby Pair
- Discover Peer

**General Properties**

Management Port 1 Configuration:  Automatic (DHCP)  Manual

Management Port 1: IP Address(prefix): 10.99.88.181, Network Mask: 255.255.255.0 (/24), Management Route: 10.99.88.90

Management Port 2: IP Address(prefix):, Network Mask: Select..., Management Route:

Host Name: big181.f5jp.local (ホスト名を FQDN で指定)

Host IP Address: Use Management Port IP Address (タイムゾーンを指定)

Time Zone: Japan

**User Administration**

Root Account:  Disable login, Password: ....., Confirm: ..... (Root ユーザのパスワードを指定 ※F5 ラボ環境では指定の値を利用してください。実際は自社セキュリティポリシーに則ったものを利用してください。)

SSH Access:  Enabled

SSH IP Allow: \* All Addresses

Back Next...

(11) この後、Standard Network Configuration の「Next」を押すことでウィザード形式にて冗長化も含めた設定が可能ですが、ここではスタンドアロン構成にするため、Advanced Network Configuration の「Finished」ボタンを押します。

Hostname: big181.f5jp.local, Date: Jul 11, 2019, User: admin, Role: Administrator, Partition: Common, Log out

ONLINE (ACTIVE) Standalone

Main Help About Setup Utility » Network

Setup Utility

- Introduction
- License
- Resource Provisioning
- Device Certificates
- Platform
- Network
- Redundancy
- VLANs
- NTP
- DNS
- ConfigSync
- Failover
- Mirroring
- Active/Standby Pair
- Discover Peer

**Standard Network Configuration**  
Create a standard network configuration by configuring these features:

- Redundancy
- VLANs
- NTP
- DNS
- Config Sync
- Failover
- Mirroring
- Peer Device Discovery (for Redundant Configurations)

Next...

**Advanced Network Configuration**  
Create advanced device configurations by clicking **Finished** and navigating to the Main tab of the Configuration Utility.

Finished

## 4. ネットワークの設定

ネットワーク構成に合わせて、VLAN, VLAN インタフェースへの IP 設定およびルーティング設定を行います。

### 4.1. VLAN の作成

まず、VLAN を作成します。「Network」→「VLAN」で表示された画面の右上にある「Create」ボタンを押します。

#### (1) External VLAN の設定をします。

Hostname big181.f5.jp.local Date Jul 11, 2019 User admin  
IP Address 10.99.88.181 Time 4:35 PM (JST) Role Administrator Partition: Common Log out

ONLINE (ACTIVE)  
Standalone

Main Help About Network > VLANs : VLAN List >> New VLAN...

Statistics  
iApps  
DNS  
Local Traffic  
Acceleration  
Device Management  
Shared Objects  
Security  
Network

Interfaces  
Routes  
Self IPs  
Packet Filters  
Quick Configuration  
Trunks  
Tunnels  
Route Domains  
VLANs  
Service Policies

**General Properties**

Name external 名前(任意)を指定  
Description  
Tag

**Resources**

Interface: 1.2  
Tagging: Untagged  
Add  
1.1 (untagged) Interface:1.1  
Tagging:Untagged  
を選択し、Add をクリック  
Edit Delete

**Configuration:** Basic

Source Check  
MTU 1500

**sFlow**

Polling Interval Default  
Sampling Rate Default

Cancel Repeat Finished

## (2) Internal VLAN の設定をします。

Hostname big181.f5.jp.local Date Jul 11, 2019 User admin  
IP Address 10.99.88.181 Time 4:37 PM (JST) Role Administrator Partition: Common Log out

ONLINE (ACTIVE)  
Standalone

Main Help About Network » VLANs : VLAN List » New VLAN...

Statistics  
iApps  
DNS  
Local Traffic  
Acceleration  
Device Management  
Shared Objects  
Security  
Network

Interfaces  
Routes  
Self IPs  
Packet Filters  
Quick Configuration  
Trunks  
Tunnels  
Route Domains

**General Properties**

Name: internal 名前(任意)を指定

Description:

Tag:

**Resources**

Interface: 1.1  
Tagging: Untagged  
Add  
1.2 (untagged) Interface:1.2  
Tagging:Untagged  
を選択し、Add をクリック

Edit Delete

Configuration: Basic

Source Check

MTU: 1500

**sFlow**

Polling Interval: Default  
Sampling Rate: Default

Cancel Repeat **Finished**

## (3) 一覧では以下のような状態になります。

Hostname big181.f5.jp.local Date Jul 11, 2019 User admin  
IP Address 10.99.88.181 Time 4:39 PM (JST) Role Administrator Partition: Common Log out

ONLINE (ACTIVE)  
Standalone

Main Help About Network » VLANs : VLAN List

VLAN List VLAN Groups

Search Create...

<input type="checkbox"/>	Name	Application	Tag	Untagged Interfaces	Tagged Interfaces	Partition / Path
<input type="checkbox"/>	external		4094	1.1		Common
<input type="checkbox"/>	internal		4093	1.2		Common

Delete...

## 4.2. Self IP の設定

設定した VLAN それぞれに対して、IP アドレスを設定していきます。  
Adv.WAF 自身に設定する IP アドレスを、Self IP と呼びます。

「Network」→「Self IPs」で表示された画面の右上にある「Create」ボタンを押します。

### (1) External VLAN の Self IP を設定します。

Configuration

Name	external-ip	名前(任意)、
IP Address	10.99.1.181 10.99.1.XXX (F5 ラボの場合)	IP アドレス、
Netmask	255.255.255.0	サブネットマスク、
VLAN / Tunnel	external	VLAN を設定
Port Lockdown	Allow None	このアドレス上でのサービス (SSH/GUI アクセス等) を拒否
Traffic Group	<input type="checkbox"/> Inherit traffic group from current partition / path traffic-group-local-only (non-floating)	
Service Policy	None	

Cancel Repeat **Finished**

### (2) internal VLAN の IP 設定

Configuration

Name	internal-ip	名前(任意)、
IP Address	10.99.2.181 10.99.2.XXX (F5 ラボの場合)	IP アドレス、
Netmask	255.255.255.0	サブネットマスク、
VLAN / Tunnel	internal	VLAN を設定
Port Lockdown	Allow Default	このアドレス上でのサービス (SSH/GUI アクセス等) を許可
Traffic Group	<input type="checkbox"/> Inherit traffic group from current partition / path traffic-group-local-only (non-floating)	
Service Policy	None	

Cancel Repeat **Finished**

### (3) 一覧では、以下のような状態になります

Name	Application	IP Address	Netmask	VLAN / Tunnel	Traffic Group	Partition / Path
external-ip		10.99.1.181	255.255.255.0	external	traffic-group-local-only	Common
internal-ip		10.99.2.181	255.255.255.0	internal	traffic-group-local-only	Common

### 4.3. ルーティングの設定

#### 4.3.1. デフォルトゲートウェイの設定

(1) 「Network」→「Routes」で表示された画面の右上にある「Add」ボタンを押し、以下のように設定します。

Hostname big181.f5.jp.local Date Jul 11, 2019 User admin  
IP Address 10.99.88.181 Time 4:55 PM (JST) Role Administrator Partition: Common Log out

ONLINE (ACTIVE)  
Standalone

Main Help About Network » Routes » New Route...

Statistics  
iApps  
DNS  
Local Traffic  
Acceleration  
Device Management  
Shared Objects  
Security  
Network  
Interfaces  
Routes

Properties

Name Default-GW 任意の名称を入力

Description

Destination 0.0.0.0 左記の通りに入力

Netmask 0.0.0.0

Resource Use Gateway...

Gateway Address IP Address 10.99.1.254 ゲートウェイのアドレスを入力

MTU

Cancel Repeat Finished

#### 4.3.2. Web アプリケーションサーバへのルーティング設定

(1) Adv.WAF から Web アプリケーションサーバ: 10.99.100.0/24 へ到達するためのルーティング設定も行います。

Hostname big181.f5.jp.local Date Jul 11, 2019 User admin  
IP Address 10.99.88.181 Time 4:59 PM (JST) Role Administrator Partition: Common Log out

ONLINE (ACTIVE)  
Standalone

Main Help About Network » Routes » New Route...

Statistics  
iApps  
DNS  
Local Traffic  
Acceleration  
Device Management  
Shared Objects  
Security

Properties

Name Servers-Route 任意の名称を入力

Description

Destination 10.99.100.0 Web サーバのネットワークアドレスを入力

Netmask 255.255.255.0

Resource Use Gateway...

Gateway Address IP Address 10.99.2.254 ゲートウェイのアドレスを入力

MTU

Cancel Repeat Finished

(2) 一覧では、以下のような状態になります。

Hostname big181.f5.jp.local Date Jul 11, 2019 User admin  
IP Address 10.99.88.181 Time 5:01 PM (JST) Role Administrator Partition: Common Log out

ONLINE (ACTIVE)  
Standalone

Main Help About Network » Routes

Route List

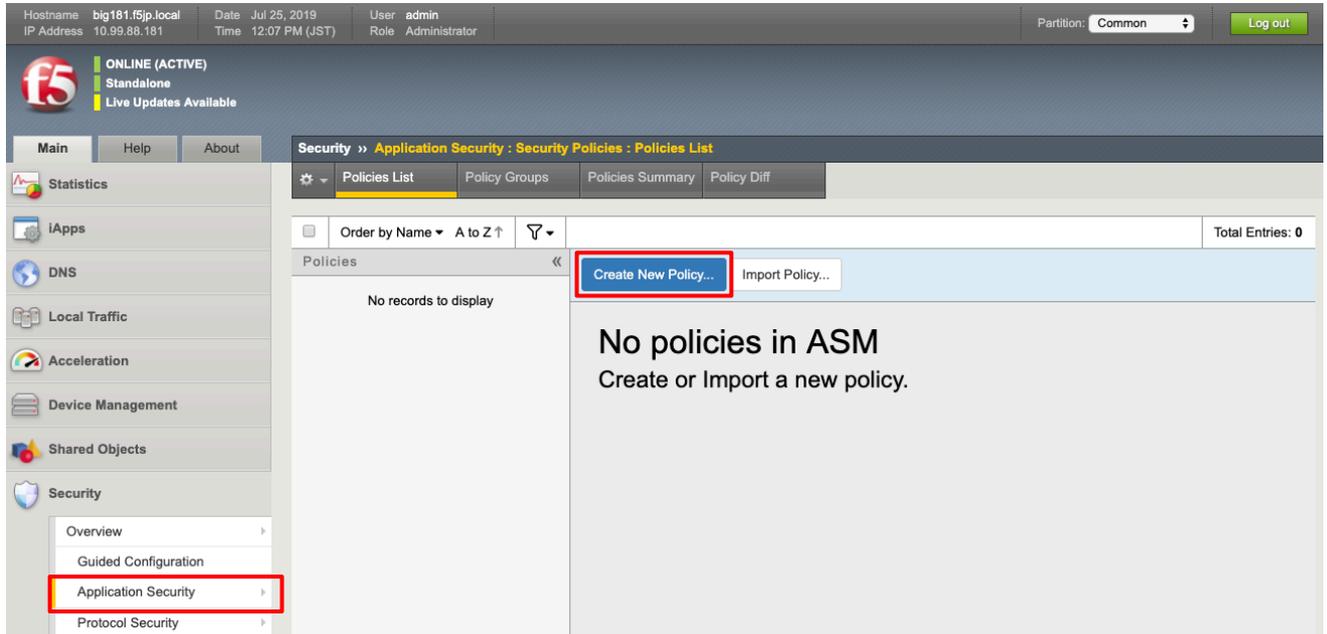
Name	Application	Destination	Netmask	Route Domain	Resource Type	Resource	Partition / Path
Default-GW	Default IPv4			Partition Default Route Domain	Gateway	10.99.1.254	Common
Servers-Route		10.99.100.0	255.255.255.0	Partition Default Route Domain	Gateway	10.99.2.254	Common

Delete...

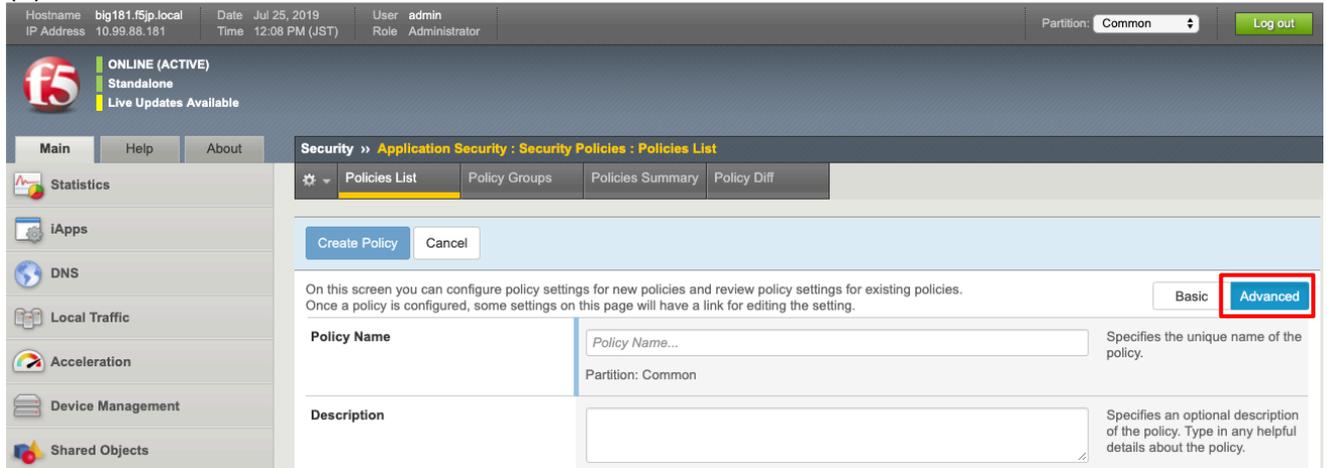
## 5. [Step1] ベースとなる WAF ポリシーを作成する

### 5.1. Deployment Wizard による設定

(1) 「Security」→「Application Security」→「Security Policies」で表示された画面中央の「Create New Policy...」ボタンを押します。



(2) 画面右上の「Advanced」を選択します。



(3) 下記のように必要事項を入力し、Create Policy ボタンを押す。

Security >> Application Security : Security Policies : Policies List

On this screen you can configure policy settings for new policies and review policy settings for existing policies. Once a policy is configured, some settings on this page will have a link for editing the setting. Basic

**Policy Name**  Specifies the unique name of the policy. **WAF のポリシー名 (任意) を記載**

Partition: Common

**Description**  Specifies an optional description of the policy. Type in any helpful details about the policy.

**Policy Type**   Select a policy type: **Security** for an application security policy that you can apply to a virtual server, or **Parent** that you can use in order to attach Security policies to it, inheriting its attributes. Parent policies cannot be applied to Virtual Servers.

**Policy Template**  Choose a policy template for this policy. **Rapid Deployment Policy を選択**

**Virtual Server**

Configure new virtual server...  Select an Existing Virtual Server if you already configured one. (An existing Virtual Server is displayed only if it has an HTTP Profile assigned to it and it is not under any Local Traffic Policy controlling ASM) and you would like to reuse it, or New Virtual Server if you have not associate the newly created :

**What type of protocol does your application use?**  **HTTP and HTTPS を選択**

**Virtual Server Name**  Note: 2 Virtual Servers will be created with "http\_" and "https\_" added as prefix to the selected name. **VS の名称 (任意) を入力**

**HTTP Virtual Server Destination**   **VS のアドレス、ポート番号 (80) を入力**

**HTTP Pool Member**  **プールメンバーのアドレス、ポート番号を入力**

**HTTPS Virtual Server Destination**   **VS のアドレス、ポート番号 (443) を入力**

**HTTPS Pool Member**  **プールメンバーのアドレス、ポート番号を入力**

**SSL Profile (Client)**  **clientsssl を選択**

**SSL Profile (Server)**

**Logging Profile**  **Log illegal requests を選択**

**Learning Mode**    Select how ASM handles the policy building process: **Automatic** will automatically accept learning suggestions once they reach 100%, **Manual** will require the administrator to accept every suggestion, and **Disabled** will cause that ASM does not create any learning suggestions. Note that an administrator can accept suggestions manually even in Automatic mode.

**Enforcement Mode**   Specifies how the system processes a request that triggers a security policy violation.

**Application Language**  Specifies the language encoding for the web application, which determines how the security policy processes the character sets.

**Auto-Added Signature Accuracy**  Accuracy for the signatures that are included in the template and for those to be added as a result of adding Server Technologies to the policy.

**Server Technologies**

Server Technology	Learnable	Associated
Apache Struts	Yes	<input type="button" value="Yes"/> <input type="button" value="No"/>
Apache Tomcat	Yes	<input type="button" value="Yes"/> <input type="button" value="No"/>
Apache/NCSA HTTP Server	Yes	<input checked="" type="button" value="Yes"/> <input type="button" value="No"/>
ASP	Yes	<input type="button" value="Yes"/> <input type="button" value="No"/>
ASP.NET	Yes	<input type="button" value="Yes"/> <input type="button" value="No"/>
BEA Systems WebLogic Server	Yes	<input type="button" value="Yes"/> <input type="button" value="No"/>
CGI CGI	Yes	<input type="button" value="Yes"/> <input type="button" value="No"/>

**WAF でのチェック対象テクノロジーを選択**  
F5 ラボでは、**Apache/NCSA HTTP Server**  
**MySQL**  
**PHP**  
の3つを利用する

**Signature Staging**   Displays whether the signature staging feature is active. **Signature Staging は Enable のまま**

**Enforcement Readiness Period**  days How many days, since they were last changed, both security policy entities and attack signatures remain in staging mode before the system suggests you enforce them.

**Policy is Case Sensitive**   Displays whether the security policy treats microservice URLs, file types, URLs, and parameters as case sensitive (Enabled), or not (Disabled)

**Differentiate between HTTP/WS and HTTPS/WSS URLs**   When enabled the security policy configures URLs specific to a protocol, meaning that the security policy differentiates between HTTP/WS and HTTPS/WSS URLs.

通常 Virtual Server は HTTPS のみ作成することが多いですが、ここでは後項のテストのために HTTP の Virtual Server も作成しています。

(4) ポリシーが作成されると以下のように表示されます。  
 Enforcement Mode が「Transparent」=攻撃をブロックしないモードになっていることを確認して下さい。

Security » Application Security : Security Policies : Policies List

Policies List    Policy Groups    Policies Summary    Policy Diff

Order by Created Time ▾ Newest ↓    Total Entries: 1

WAF-policy-001    http\_WAF-...

            ▾         ▾

Policy Properties    Inheritance Settings

On this screen you can configure policy settings for new policies and review policy settings for existing policies. Once a policy is configured, some settings on this page will have a link for editing the setting.       

<b>Policy Name</b>	WAF-policy-001 Partition / Path: /Common	Specifies the name of the policy.
<b>Description</b>	<input type="text" value="Rapid Deployment Policy"/>	Specifies an optional description of the policy.
<b>Policy Type</b>	Security	Specifies the type of the policy.
<b>Policy Template</b>	Rapid Deployment Policy	Specifies the template of the policy.
<b>Parent Policy</b>	None	Specifies the parent of the policy.
<b>Version</b>	2019-07-11 10:37:37 ⓘ Source Host Name: big181.f5jp.local Source Policy Name: /Common/WAF-policy-001	Displays additional information about policy version.
<b>Application Language</b>	Unicode (utf-8)	Specifies the language encoding for the web application, which determines how the security policy processes the character sets.
<b>Virtual Server</b>	<a href="#">http_WAF-vs-001 ⓘ</a> <a href="#">https_WAF-vs-001 ⓘ</a>	Displays the name of the protected virtual server, or virtual servers, which have assigned to them a security policy with Application Security enabled.
<b>Enforcement Mode</b>	Transparent <a href="#">View Learning and Blocking Settings ⓘ</a>	Specifies how the system processes a request that triggers a security policy violation.
<b>Policy is Case Sensitive</b>	Yes	Displays whether the security policy treats microservice URLs, file types, URLs, and parameters as case sensitive (Enabled), or not (Disabled)
<b>Differentiate between HTTP/WS and HTTPS/WSS URLs</b>	<input checked="" type="button" value="Enabled"/> <input type="button" value="Disabled"/>	When enabled the security policy configures URLs specific to a protocol, meaning that the security policy differentiates between HTTP/WS and HTTPS/WSS URLs.
<b>Event Correlation Reporting</b>	<input checked="" type="button" value="Enabled"/> <input type="button" value="Disabled"/>	When enabled, Event Correlation Reporting logs are collected.
<b>Mask Credit Card Numbers in Request Log</b>	<input checked="" type="button" value="Enabled"/> <input type="button" value="Disabled"/>	When enabled the security policy masks credit card numbers that appear in any part of requests.

## 5.2. Virtual Server の設定の確認

Deployment Wizard で設定した Virtual Server の設定を確認します。

### 5.2.1 Policies の確認

- (1) 「Local Traffic」→「Virtual Servers」で表示された、作成済み https 用 Virtual Server を選択します。  
その上に表示された「Resources」タブを選択します。  
WAF ポリシー作成の際に自動的に生成された Policy が割当てられていることが分かります。

The screenshot shows the F5 configuration interface. The breadcrumb path is Local Traffic >> Virtual Servers : Virtual Server List >> https\_WAF-vs-001. The 'Resources' tab is active, and the 'Policies' section is expanded, showing a single policy: /Common/asm\_auto\_i7\_policy\_https\_WAF-vs-001. The 'Virtual Servers' menu item in the left sidebar is also highlighted with a red box.

- (2) 「Security」タブの「Policies」をクリックします。  
生成した WAF ポリシーが割当てられていることが分かります。また、Log は、Log illegal requests が割当てられていることが分かります。

The screenshot shows the 'Security' tab selected. The 'Policy Settings' section is visible. The 'Application Security Policy' is set to 'Enabled... Policy: WAF-policy-001'. The 'Log Profile' is set to 'Log illegal requests'. Red boxes highlight these settings with the following annotations: '作成した WAF ポリシーが割当てられている' (The created WAF policy is assigned) and 'illegal のみをロギング' (Logging only illegal requests).

- (3) 作成済み http 用 Virtual Server も、(1)(2)と同様の内容を確認します。

### 5.3. Learning and Blocking Setting の確認と変更

Adv.WAF のセキュリティ機能の ON/OFF のほとんどは、Learning and Blocking Setting で設定します。

「Security」→「Application Security」→「Policy Building」→「Learning and Blocking Settings」で表示された画面を確認します。

Rapid Deployment Security Policy によって、いくつかの Violations の「Learn」と「Alarm」が有効になっていることを確認します。Enforcement Mode が Transparent なので、「Block」はすべてグレーアウトされています。

- 「Learn」…… Manual Traffic Learning 画面で、検知した攻撃を学習するモード
- 「Alarm」…… Event Logs 画面で、攻撃を検知したことを示すログを出力するモード
- 「Block」…… 攻撃をブロックするモード

#### 5.3.1. Blocking Setting の設定変更

(1) 日本語サイトの誤検知の防止策として、「Failed to convert character」を OFF にします。また、「Data Guard: Information Leakage Detected」もパフォーマンス面を考慮して OFF にします。

The screenshot shows the 'Learning and Blocking Settings' page for policy 'WAF-policy-001'. The 'Enforcement Mode' is set to 'Transparent'. Under 'Policy Building Settings', the 'Data Guard' section is expanded, showing a table of violations. Two rows are highlighted with red boxes: 'Data Guard: Information leakage detected' and 'Failed to convert character'. Both rows have checkboxes for 'Learn', 'Alarm', and 'Block' that are unchecked, and the word '外す' (Remove) is written in red to the right of each row. The 'General Settings' section is also expanded, showing a table of violations. The 'Failed to convert character' row is highlighted with a red box and has '外す' written in red. The 'Advanced' button is highlighted with a red box and labeled 'Advanced を選択'.

Learn	Alarm	Block	Violation
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Data Guard: Information leakage detected
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Failed to convert character
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Illegal Base64 value
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Illegal HTTP status in response
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Illegal session ID in URL
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Request length exceeds defined buffer size

(2) 変更後、「Save」ボタンを押します。

### 5.3.2. Data Guard の無効化-2

(1) 「Security」→「Application Security」→「Data Guard」で表示された画面で、「Data Guard」のチェックが外れていることを確認します。

The screenshot shows the F5 Security Center interface. At the top, the status bar displays: Hostname: big181.f5jp.local, IP Address: 10.99.88.181, Date: Jul 11, 2019, Time: 7:51 PM (JST), User: admin, Role: Administrator, Partition: Common, and a Log out button. The main navigation bar includes Main, Help, and About. The left sidebar contains various menu items: Statistics, iApps, DNS, Local Traffic, Acceleration, Device Management, Shared Objects, and Security. The Security menu is expanded, showing Overview, Guided Configuration, Application Security, Protocol Security, Network Firewall, DoS Protection, and Bot Defense. The main content area is titled 'Security >> Application Security : Data Guard'. Below this, there is a 'Data Guard' section with a 'WAF-policy-001' dropdown, a gear icon, a shield icon, and 'Learning Mode: Manual'. A warning icon indicates 'Changes not applied' and an 'Apply Policy' button. The 'Data Guard' table is as follows:

Data Guard		Save
Data Guard	<input type="checkbox"/> Enabled	
Credit Card Numbers	<input checked="" type="checkbox"/> Enabled	
U.S. Social Security Numbers	<input checked="" type="checkbox"/> Enabled	
Custom Patterns	<input type="checkbox"/> Enabled	
Exception Patterns	<input type="checkbox"/> Enabled	
Mask Data	<input checked="" type="checkbox"/> Enabled	
File Content Detection	<input type="checkbox"/> Check File Content Note: When file content is detected, the system will not enforce exception patterns and mask response data that match the file content.	
Enforcement Mode (Wildcards supported)	Ignore URLs in list: <input type="text"/> Add Example: /index.html <input type="text"/> Remove	
Save		

(2) 「Apply Policy」ボタンを押します。

This screenshot is identical to the previous one, but the 'Apply Policy' button in the top right corner of the configuration area is highlighted with a red box.

Attack Signature の状態確認及び変更は次の章で行います。

## 5.4. シグネチャの状態確認

### 5.4.1. Attack Signature Configuration

- (1) 「Security」→「Application Security」→「Policy Building」→「Learning and Blocking Settings」の「Attack Signatures」を選択します。

「Enable Signature Staging」にチェックが入っていることを確認します。

The screenshot displays the 'Attack Signatures' configuration page. At the top, there are navigation tabs for 'Traffic Learning' and 'Learning and Blocking Settings'. Below this, there's a dropdown for 'WAF-policy-001' and a 'Learning Mode: Manual' setting. The 'General Settings' section includes 'Enforcement Mode' (Transparent), 'Learning Mode' (Manual), 'Learning Speed' (Medium), and 'Enforcement Readiness Period' (7 days). The 'Policy Building Settings' section is expanded to show 'Antivirus' and 'Attack Signatures'. A table lists signature sets with columns for 'Learn', 'Alarm', 'Block', 'Signature Set Name', and 'Signature Set Category'. Below the table, there are settings for 'Auto-Added Signature Accuracy' (Medium Accuracy) and 'Enable Signature Staging' (checked). There's also a section for 'Updated Signature Enforcement' and 'Apply Response Signatures for these File Types'.

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Signature Set Name	Signature Set Category
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	PHP Signatures (High/Medium Accuracy)	User-defined
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	MySQL Signatures (High/Medium Accuracy)	User-defined
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Apache/NCSA HTTP Server Signatures (High/Medium Accuracy)	User-defined
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Generic Detection Signatures (High/Medium Accuracy)	Basic

## 5.4.2. Attack signature List

### 5.4.2.1. 各シグネチャ状態の確認

(1) 「Security」→「Application Security」→「Attack Signatures」をクリックします。

Signature Staging が Enabled なので、Learn/Alarm/Block が無効になり、「In Staging」の状態になっています。

The screenshot shows the Fortinet Security Manager interface. At the top, the status is 'ONLINE (ACTIVE) Standalone'. The navigation menu on the left includes Statistics, iApps, DNS, Local Traffic, Acceleration, Device Management, Shared Objects, Security, Network, and System. The main content area is titled 'Security >> Application Security : Attack Signatures'. A dropdown menu shows 'WAF-policy-001' and 'Learning Mode: Manual'. Below this, a table lists various attack signatures. The 'Staging' column for all signatures is set to 'Yes', indicating they are in Staging mode. The 'Learn', 'Alarm', and 'Block' columns are all set to 'No' or 'N/A', indicating these actions are disabled. The table has 7 columns: Signature Name, Signature ID, Staging, Learn, Alarm, Block, and Enabled. The total number of entries is 2565.

Signature Name	Signature ID	Staging	Learn	Alarm	Block	Enabled
"/phpinfo.php" access	200010015	Yes	Yes	No	N/A	Yes
"/pls/admin_/help" access	200010009	Yes	Yes	No	N/A	Yes
"/soap/.../spy/" access	200010002	Yes	Yes	No	N/A	Yes
"/xsl/demo/adhocsql/query.xsql" access	200010011	Yes	Yes	No	N/A	Yes
"dbase invalidation" Error Message	200009189	Yes	Yes	No	N/A	Yes
"dbm invalidation" Error Message	200009182	Yes	Yes	No	N/A	Yes
"Error processing SSI file"	200009178	Yes	Yes	No	N/A	Yes
"FileMakerPro Query Invalidation" Error Message	200009188	Yes	Yes	No	N/A	Yes
"Frontbase SQL invalidation" Error Message	200009181	Yes	Yes	No	N/A	Yes
"httpd.conf" access	200010016	Yes	Yes	No	N/A	Yes
"httpd.conf" access (Parameter)	200010042	Yes	Yes	No	N/A	Yes
"index of /" response	200100002	Yes	Yes	No	N/A	Yes
"Interbase SQL invalidation" Error Message	200009186	Yes	Yes	No	N/A	Yes
"Microsoft OLE DB Provider" Error Message	200009194	Yes	Yes	No	N/A	Yes
"MySQL SQL invalidation" Error Message	200009184	Yes	Yes	No	N/A	Yes
"open()" execution attempt	200003074	Yes	Yes	No	N/A	Yes
"php.ini" access (Parameter)	200010044	Yes	Yes	No	N/A	Yes
"php.ini" access (URI)	200010043	Yes	Yes	No	N/A	Yes
"style :expression (" (Headers)	200001152	Yes	Yes	No	N/A	Yes
"style :expression (" (Parameter)	200001151	Yes	Yes	No	N/A	Yes

- Staging (ステージング) モードとは:

Learn/Alarm/Block 設定が無効化され、攻撃を検知した場合には、「Manual Traffic Learning」で学習するだけの動作となるモードです。

### 5.4.3. ステージングログの設定

ステージングのログを Event Logs に出力するための設定を行います。

(1) 「Security」→「Event Logs」→「Logging Profiles」にて、Create ボタンを押し、以下のように設定します。

Logging Profile Properties

Profile Name	Log illegal and staging requests	任意の名前を入力
Description		
Application Security	<input checked="" type="checkbox"/> Enabled	Application Security の Enabled チェック
Protocol Security	<input type="checkbox"/> Enabled	
Network Firewall	<input type="checkbox"/> Enabled	
DoS Protection	<input type="checkbox"/> Enabled	
Bot Defense	<input type="checkbox"/> Enabled	

Configuration: Basic

Storage Destination: Local Storage

Storage Filter: Basic

Request Type:  Illegal requests only  
 Illegal requests, and requests that include staged attack signatures or staged threat campaigns  
 All requests

Cancel Create

Illegal requests, and requests that includes staged attack signatures or staged threat campaings を選択

(2) Virtual Server に(1)で作成したロギングプロファイルを追加して、既存のプロファイルをはずします。Update ボタンを押します。

Local Traffic » Virtual Servers : Virtual Server List » https\_WAF-vs-001

Properties Resources Security Statistics

Policies

Policy Settings

Destination	10.99.1.81:443
Service	HTTPS
Application Security Policy	Enabled... Policy: WAF-policy-001
Service Policy	None
IP Intelligence	Disabled
DoS Protection Profile	Disabled
Bot Defense Profile	Disabled
Log Profile	Enabled... Selected: /Common, Log illegal and staging requests Available: Log all requests, global-network, local-bot-defense, local-dos, Log illegal requests

Update

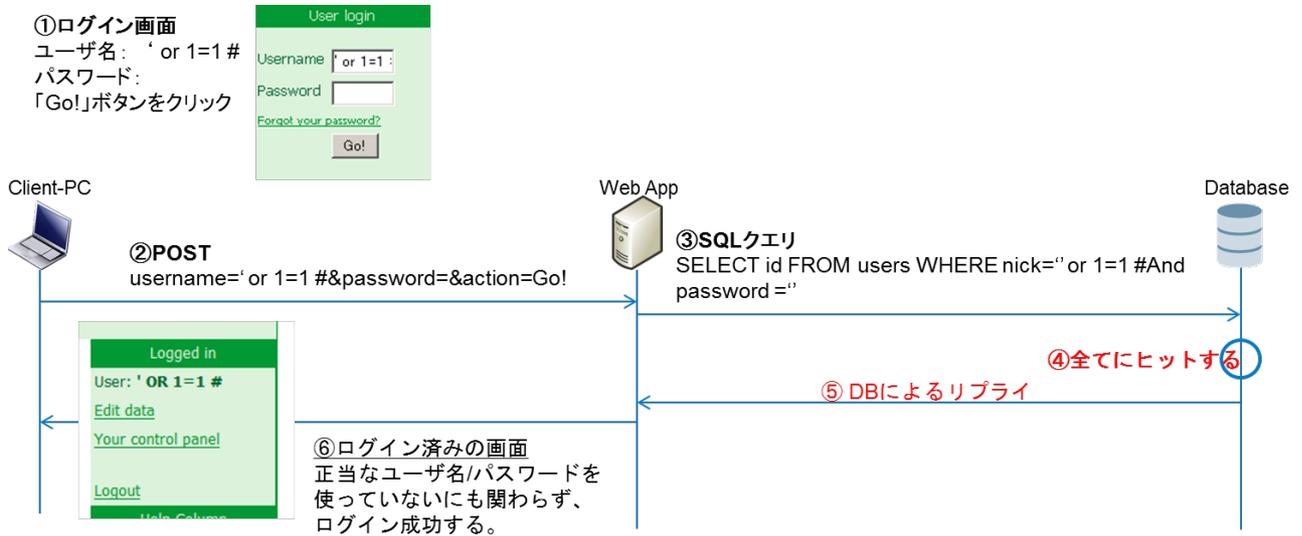
このステージングモードのまま、次項「シグネチャ動作の確認」を実施します。

## 6. シグネチャ動作の確認

### 6.1. 例:SQL インジェクション

シグネチャの動作を確認するにあたり、SQL インジェクション攻撃を例に取ります。

SQL インジェクションは、以下のような攻撃です。



- ① ユーザ名に「' or 1=1 #」と入力して「Go!」ボタンを押す。
- ② 結果、HTTP リクエスト:POST で、「username=' or 1=1 #&password=&action=Go!」を送る。
- ③ Web アプリケーションは、

```
SELECT id FROM users WHERE nick='username 値' And password ='password 値'
```

の SQL 文を生成し、データベースへ送る準備をしている。

ここに、HTTP リクエストで到着した値を埋め込むと、

```
SELECT id FROM users WHERE nick=' or 1=1 #' And password =''
```

の形になる。

この意味するところは、

「nick が空 または 1=1 ならば、users テーブルから id を取得する。#以降はコメントアウト。」となる。

- ④ この SELECT 文内の「1=1」は正しいので、データベースのすべてにヒットする。
- ⑤ データベースからリプライを受ける。
- ⑥ ログインに成功する。

Adv.WAF は、このような脆弱性を持つ Web アプリケーションを防御するためのシグネチャ群を持っています。この攻撃を例に、シグネチャの動作を確認していきます。

- (1) クライアント PC から、<https://10.99.1.ZZZ> へアクセスします。  
 ブラウザの Username 欄に、「' or 1=1 #」を入力し、「Go!」ボタンを押します。

The screenshot shows the homepage of 'Hack-it-yourself auction'. The navigation bar includes links for Home, Sell an item, Register now, Login, and Help. Below the navigation bar, there are search and browse fields, both with 'Go!' buttons. The page displays statistics: 35 REGISTERED USERS and 631 AUCTIONS. On the left, there is a 'Categories' sidebar with links to various product categories. The main content area is titled 'Last created auctions' and lists several recent auction items with their dates and IDs. On the right, there is a 'User login' section with a Username field containing the payload ' or 1=1 #', a Password field, and a 'Go!' button. A 'Forgot your password?' link is also present. Below the login section is a 'Help Column' with links for General Help, Bidding, and Registering.

- (2) 本 Web アプリケーションはこの脆弱性を持つため、ログインできてしまいます。

The screenshot shows the same homepage as in the previous image, but the user is now logged in. The navigation bar includes links for Home, Sell an item, Your control panel, Contact Us, Logout, and Help. The 'User login' section has been replaced by a 'Logged in' section, which displays 'User: ' or 1=1 #'. Below this, there are links for Edit data, Your control panel, and Logout. The 'Last created auctions' section remains the same. The 'Help Column' is also present, with links for General Help, Bidding, and Registering.

(3) 「Security」→「Event Logs」→「Application」→「Requests」で表示された画面で、「Staged」で SQL インジェクションが検出されていることを確認します。

Violation の Occurrences をクリックしても、Staged であることがわかります。また、シグネチャで検知したキーワードが確認できます。

ステージングを示しています。

クリック

(4) 上記画面の Suggestions の View...をクリックすると、Traffic Learning の画面でも Attack signature detected が確認できます。(「Security」→「Application Security」→「Policy Building」→「Traffic Learning」でもたどれます。)

WAF-policy-001 Learning Mode: Manual Apply Policy

Applied Filter: Support ID: 1478491023369051209; Violation: Attack signature detected Total Entries: 1

Suggestions

Attack signature detected 5% Parameter: \*

Accepted Action: Add SQL-INJ expressions like "or 1=1" (6) (Parameter) (disabled on the parameter) to Overridden Atta... 5%

Matched Parameter: \*

Matched Attack Signature: 200002476 - SQL-INJ expressions like "or 1=1" (6) (Parameter) \*

1 sample request out of 1 that triggered the suggestion on 2019-07-25 14:02:03

Average Request Violation Rating 2.0 At least 1 untrusted sources / 0 trusted source

Sample Requests

[HTTPS] /login.php

Triggered Violations

Violation: Attack signature detected Occurrences: 1

Request Details

Geolocation: N/A

Source IP Address: 10.99.88.90:49816

Session ID: 683dc34ec2b33949

Microservice: N/A

Time: 2019-07-25 14:02:03

Violation Rating: 2 Request looks like a false positive but requires examination

Attack Types: N/A

Decoded Request

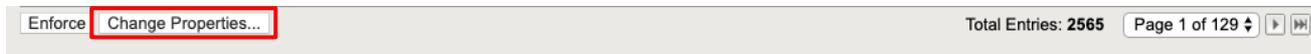
POST /login.php HTTP/1.1

Host: 10.99.1.81

## 6.2. 各シグネチャの Staging の解除

ステー징状態のままでは、攻撃を Event Log として記録してくれません。  
 よって、全シグネチャのステー징を解除 (=Learn/Alarm/Block 設定を有効に) します。

- (1)
- (2) 「Security」→「Application Security」→「Attack Signatures」で表示された画面下の「Change Properties」ボタンを押します。



- (3) 上図の「Change Properties」ボタンを押すと現れる画面で、以下のように設定し、「Apply Changes to...」ボタンを押します。



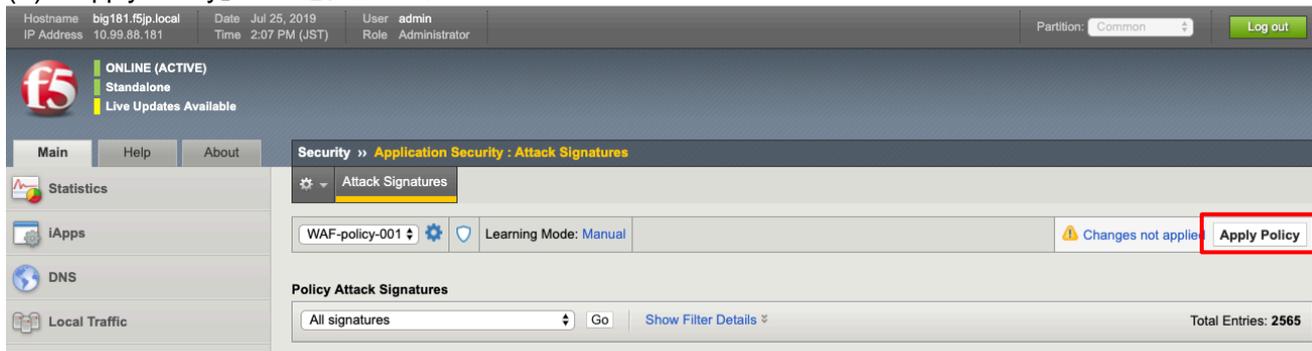
- (4) ステー징モード解除が完了するまで、少し時間がかかります。

- (5) 以下のイメージは、Staging モードが解除された状態です。  
 この段階では Enforcement Mode が Transparent なので、Block は N/A になっています。

A screenshot of the Fortinet Security Manager interface. The 'Attack Signatures' section is active, showing a list of signatures. The columns 'Staging', 'Learn', 'Alarm', 'Block', and 'Enabled' are highlighted with a red box. The 'Staging' column shows 'No' for all signatures, indicating that staging has been disabled. The 'Block' column shows 'N/A' for all signatures, indicating that the enforcement mode is transparent.

Signature Name	Signature ID	Staging	Learn	Alarm	Block	Enabled
"phpinfo.php" access	200010015	No	Yes	Yes	N/A	Yes
"pls/admin_help" access	200010009	No	Yes	Yes	N/A	Yes
"soap/...spy" access	200010002	No	Yes	Yes	N/A	Yes
"xsl/demo/adhocsql/query.xsql" access	200010011	No	Yes	Yes	N/A	Yes
"dbase Invalidation" Error Message	200009189	No	Yes	Yes	N/A	Yes
"dbm invalidation" Error Message	200009182	No	Yes	Yes	N/A	Yes
"Error processing SSI file"	200009178	No	Yes	Yes	N/A	Yes
"FileMakerPro Query Invalidation" Error Message	200009188	No	Yes	Yes	N/A	Yes
"Frontbase SQL Invalidation" Error Message	200009181	No	Yes	Yes	N/A	Yes
"httpd.conf" access	200010016	No	Yes	Yes	N/A	Yes
"httpd.conf" access (Parameter)	200010042	No	Yes	Yes	N/A	Yes
"index of /" response	200100002	No	Yes	Yes	N/A	Yes
"Interbase SQL invalidation" Error Message	200009186	No	Yes	Yes	N/A	Yes
"Microsoft OLE DB Provider" Error Message	200009194	No	Yes	Yes	N/A	Yes
"MySQL SQL Invalidation" Error Message	200009184	No	Yes	Yes	N/A	Yes
"open()" execution attempt	200003074	No	Yes	Yes	N/A	Yes
"php.ini" access (Parameter)	200010044	No	Yes	Yes	N/A	Yes
"php.ini" access (URI)	200010043	No	Yes	Yes	N/A	Yes
"style :expression (" (Headers)	200001152	No	Yes	Yes	N/A	Yes
"style :expression (" (Parameter)	200001151	No	Yes	Yes	N/A	Yes

(6) 「Apply Policy」ボタンを押します。



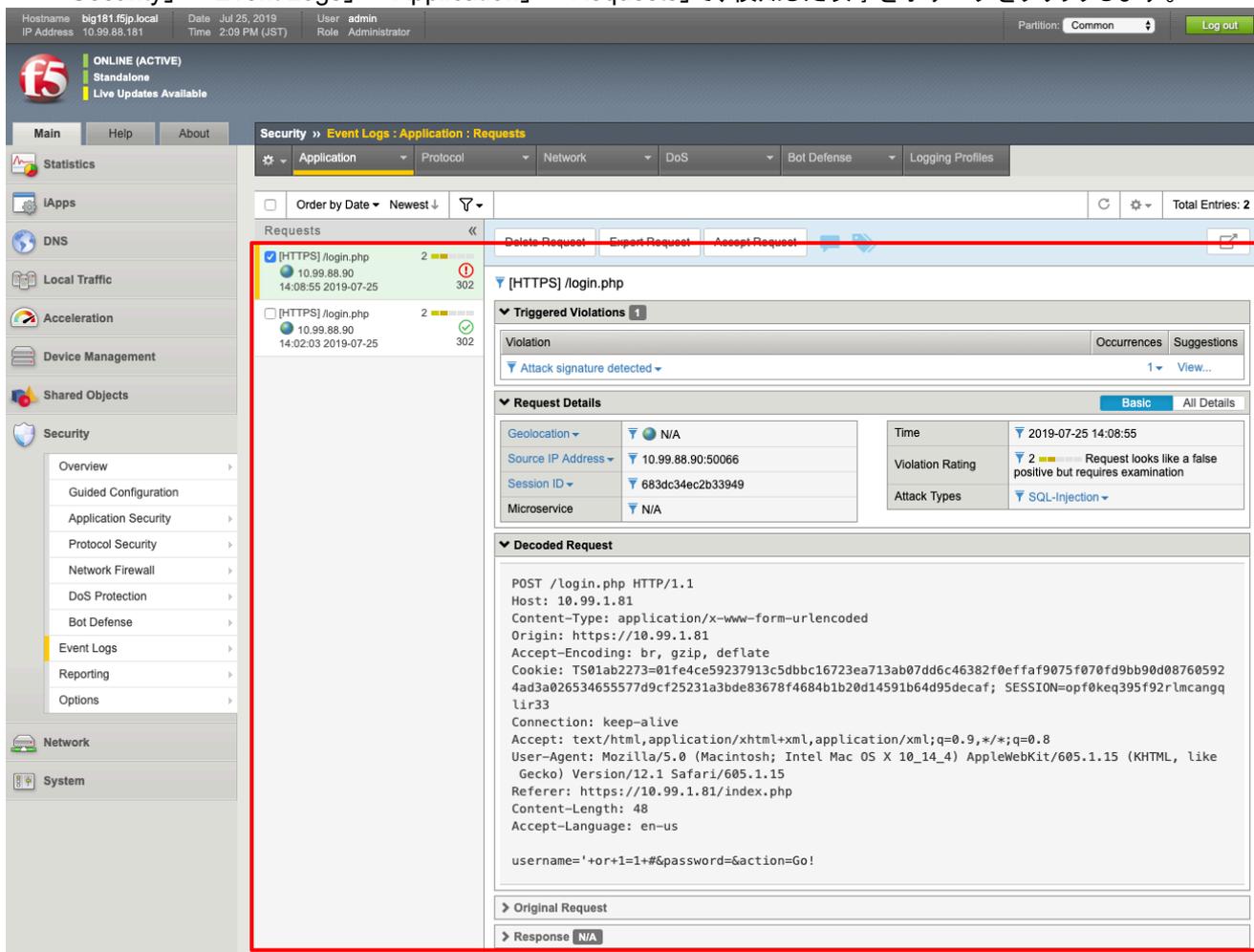
[Note]

「Policy Building Settings」-「Attack Signature Configuration」の「Enable Signature Staging」を OFF にすることも、全シグネチャの Staging を解除することはできます。しかし、その方法ですと問題になる場合があります。例えば、シグネチャの Update が行われた際には、その Update されたシグネチャだけはしばらく Staging で運用したい場合があります。この場合、この「Signature Staging」が Enabled でなければ、そのように動作してくれません。つまり、この「Attack Signature Configuration」の「Signature Staging」を OFF することで、「Staging 機能は全く使わない」という設定になる、ということです。よって、本ガイドでは、「Enable Signature Staging」は ON にしておき、各シグネチャの Staging を OFF にする、という方法を取ります。

尚、更新されたシグネチャだけをステージングモードとするための設定は、「シグネチャの運用」のセクションで解説します。

(7) もう一度、クライアントのブラウザから、同様の SQL インジェクション攻撃を実施します。

(8) Signature の Alarm が有効になっているので、攻撃を検知したことを示すログが出力されます。「Security」→「Event Logs」→「Application」→「Requests」で、検知した攻撃を示すログをクリックします。



(9) 「Attack Signature detected」をクリックすると、ヒットしたシグネチャの一覧が表示されます。

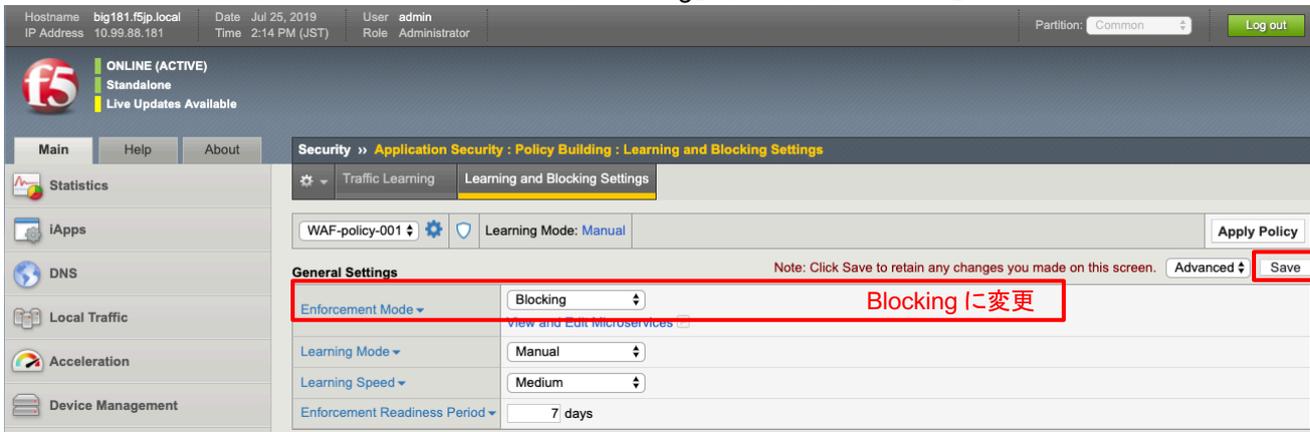
The screenshot shows a security dashboard with the following elements:

- Navigation:** Security » Event Logs : Application : Requests. Filter tabs include Application, Protocol, Network, DoS, Bot Defense, and Logging Profiles.
- Request List:** A table of requests for /login.php. The first entry is highlighted with a red box around an alarm icon, with the annotation "アラームのアイコンが表示されている。" (Alarm icon is displayed).
- Triggered Violations:** A section titled "Triggered Violations 1" containing a table with columns for Violation, Occurrences, and Suggestions. The entry "Attack signature detected" is highlighted with a red box and the annotation "クリック" (Click).
- Request Details:** A detailed view of the selected request, including:
  - Detected Keyword:** username="[redacted]#"
  - Attack Signature:** ID 200002476, Name "SQL-INJ expressions like 'or 1=1' (6) (Parameter)".
  - Context:** Parameter (detected in POST Data)
  - Parameter Level:** Global
  - Actual Parameter Name:** username
  - Wildcard Parameter Name:** \*
  - Parameter Value:** "[redacted]"
  - Applied Blocking Settings:** Alarm, LearnThe details section is annotated with "詳細が表示される" (Details are displayed).
- Decoded Request:** A raw HTTP request showing headers like Host, Content-Type, Origin, Cookie, and User-Agent, and a body with "username='+or+1=1+#&password=&action=Go!"
- Original Request:** A section for the original request.
- Response:** A section showing "N/A".

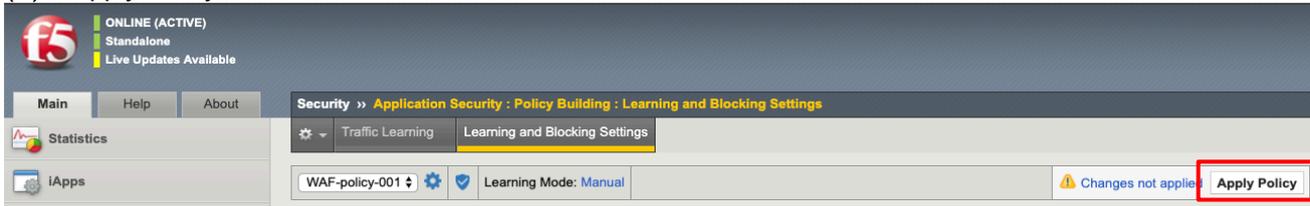
### 6.3. Enforcement Mode を Blocking に変更

攻撃をブロックする設定方法を示します。

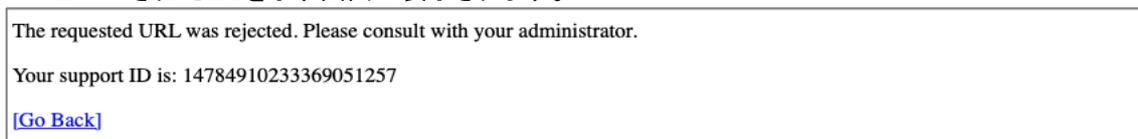
- (1) 「Security」→「Application Security」→「Policy Building」→「Learning and Blocking Settings」において、該当のポリシー名を選択し、Enforcement Mode を「Blocking」に設定変更し、「Save」ボタンを押します。



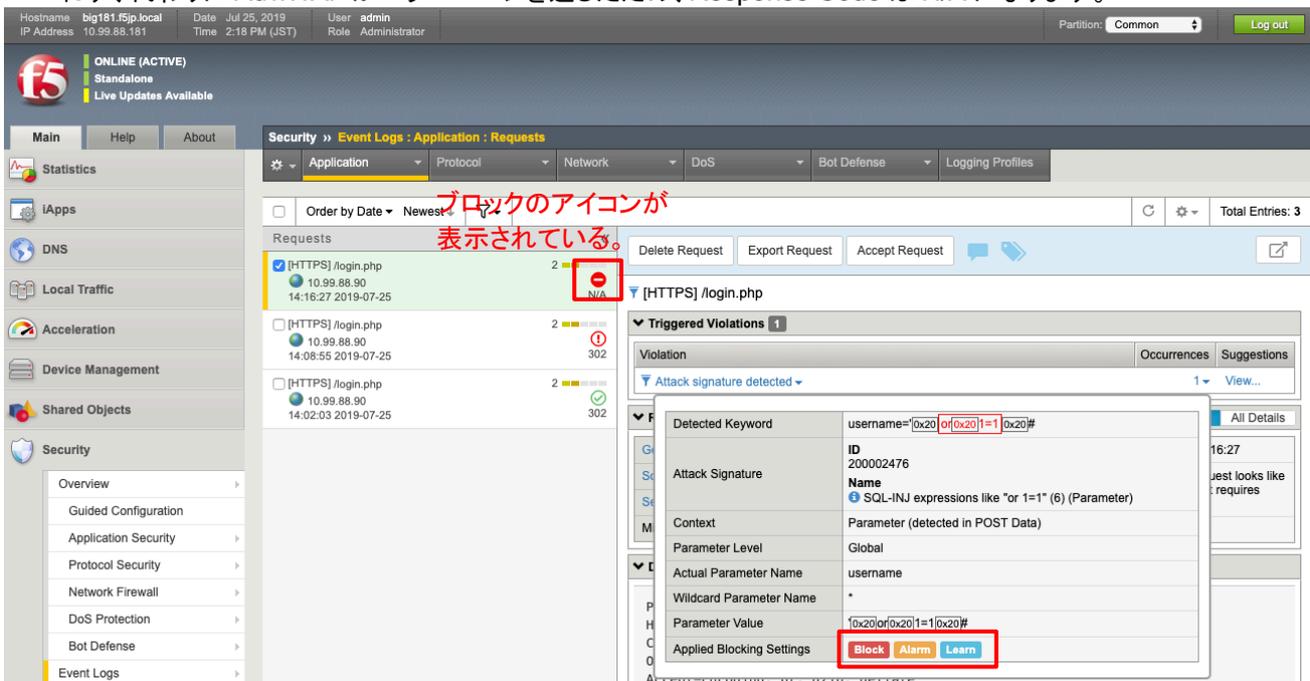
- (2) 「Apply Policy」ボタンを押します。



- (3) クライアント PC のブラウザからもう一度、同様の SQL インジェクション攻撃を実施します。Block されたことを示す画面が表示されます。



- (4) Event Logs を確認します。Block されているので、Pool Member の Web サーバからの HTTP レスポンスは返されず、代わりに Adv.WAF がエラーページを返したため、Response Code は N/A になります。



これで、その他の攻撃(クロスサイトスクリプティング等)に対しても、シグネチャがヒットした場合にはブロックされます。

## 7. [Step2] シグネチャのチューニング（誤検知の対策）

このステップでは、誤検知が発生した場合の対処方法を示します。

このステップで実施する内容は、Web アプリケーションの各パラメータの役割が全て把握できている場合を除き、運用開始前から全てを設定するのは難しいかもしれません。

その場合は、仮運用・本運用に入ってから、再度このチューニングを実施してください。

### 7.1. 誤検知の例

例えば、BIG-IP をオークションで売る、という場合を想定します。

Web アプリケーションに「f5userX」でログインし、上段の「Sell an item」をクリックしてください。

Item の説明に、代表的な例として SQL インジェクション攻撃を防御する機能があることを説明することにし、具体例として「' OR 1=1 #」を用いて説明したとします。

これは攻撃ではなく、ただ単に SQL インジェクションを説明しただけなのですが、[Step1]で行った、ただシグネチャを適用しただけの状態では、このフォームも対象となるため、攻撃とみなされます。

#### (1) 例) BIG-IP をオークションで売る例

**Hack-it-yourself auction**

Home **Sell an item** Register now Login Help

Search  Go! Browse  Gd Jul.02 2014, 08:10:39

39 REGISTERED USERS 636 AUCTIONS

**Sell an item**

Item title  任意

Item description (HTML allowed)  
The ASM can prevent a variety of web application attacks represented by SQL injection attacks.  
For example, when an attacker put ' OR 1=1 # into username form of a web page, the web application might permit the user to login. This attack is called SQL injection.

URL of picture (optional)

Or select the image you want to upload (optional)  C:\Users#test1001#D 参照... アプリケーションの作り上、Image のアップロードが必要。デスクトップ上の f5-logo.jpg を使ってください

（アプリケーションの作り上、その他にも必須とされている値があります。それらについては、本ガイドの手順には直接影響しないので、任意で入力してください。）

#### (2) Submit ボタンを押すと、攻撃として検知されてしまいます。

The requested URL was rejected. Please consult with your administrator.

Your support ID is: 10891647079625523681

[Go Back](#)

## 7.2. [対策 1] 誤検知したパラメータをホワイトリスト化する (シグネチャ検知はしない状態にする)

誤検知が発生したパラメータでは、Adv.WAF の全セキュリティ機能を無効化する=ホワイトリスト化する、という方法を示します。

(1) 誤検知が発生した通信の Event ログを表示します。

「Security」→「Event Logs」→「Application」→「Requests」で確認できます。

The screenshot shows the FortiWeb interface with the following details:

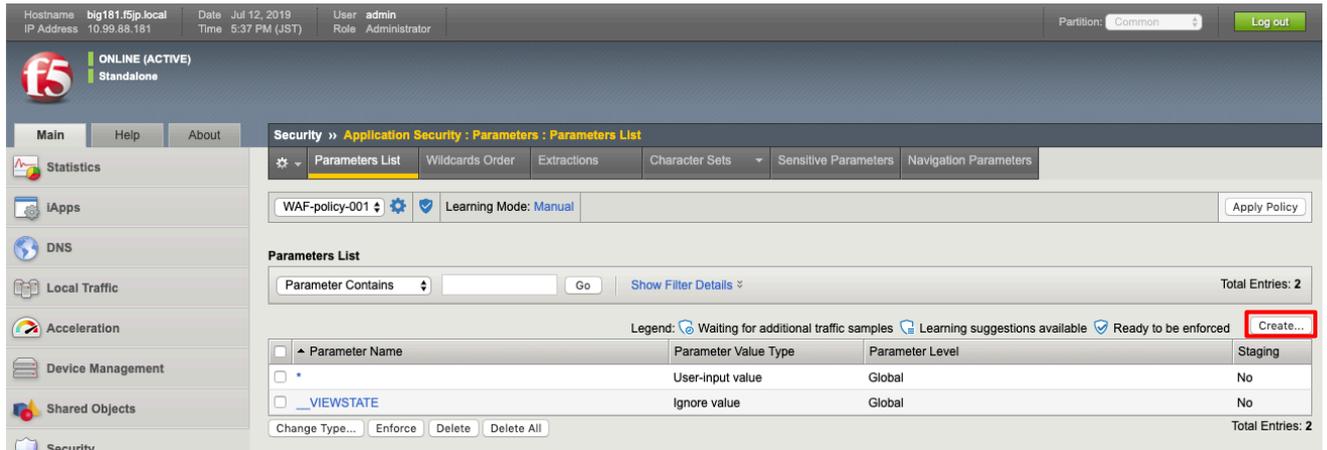
- Security > Event Logs > Application > Requests**
- Triggers Violations 1**
- Violation:** Attack signature detected (Occurrences: 1)
- Request Details:**
  - Source IP Address: 10.99.88.90:35000
  - Session ID: 8667f56032d7cd17
  - Microservice: N/A
  - Time: 2019-07-12 17:31:41
  - Violation Rating: 2 (Request looks like a false positive but requires examination)
  - Attack Types: SQL-Injection
- Request:** Request actual size: 3056 bytes.
 

```
POST /sell.php HTTP/1.1
Host: 10.99.1.81
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryPUkuYBsW0KzJ9sI
Origin: https://10.99.1.81
Accept-Encoding: br, gzip, deflate
Cookie: TS01ab2273=01c891b041770f2a4ccc3e45cddcf0b6600a7d54ade15ee1054a71149b12a0bc981197e80c8134d335b1c0874898bb27eca153285a033319aafbf4d198eed7e63b237a29f; SESSION=0ft6t0c1qs45mtlnb19hs6e3u4
Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_4) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1 Safari/605.1.15
Referer: https://10.99.1.81/sell.php?
Content-Length: 2355
Accept-Language: en-us
```

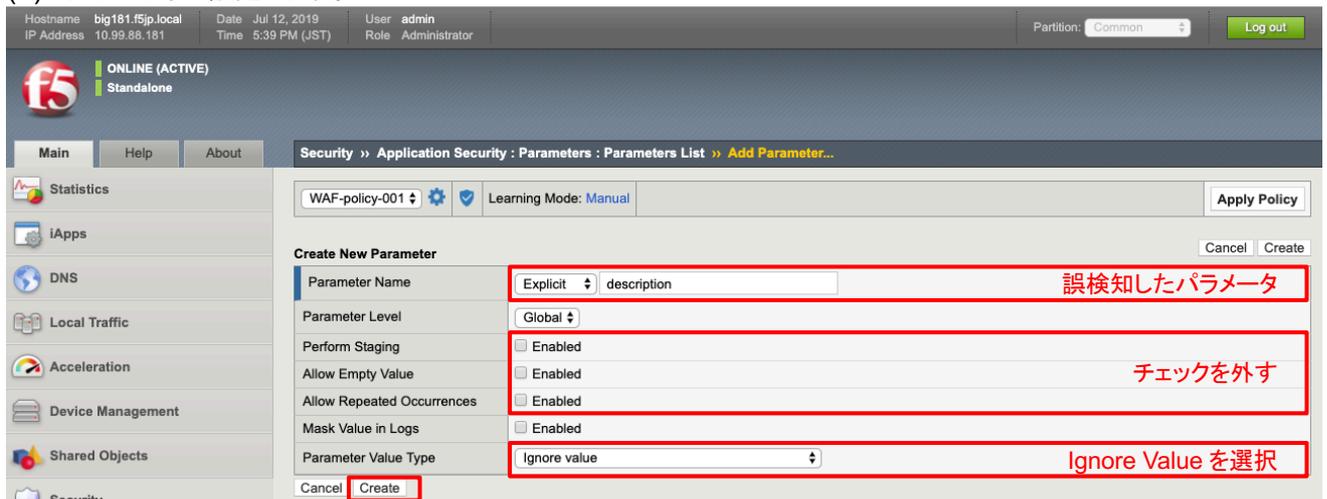
(2) 「Occurrences」をクリックして表示された画面を確認すると、誤検知したパラメータは、「description」であることが分かります。

Detected Keyword	0x20injection0x20attacks.0xd0xa0xd0xaF0r0x20example.0xd0xawhen0x20an0x20attacker1=10x20#0x200x20into0x20username0x20from0x20of0x20a0x20webpage.0x20the0x20w
Attack Signature ID	200002476
Attack Signature Name	SQL-INJ expressions like "or 1=1" (6) (Parameter)
Context	Parameter (detected in POST Data)
Parameter Level	Global
Actual Parameter Name	description
Wildcard Parameter Name	*

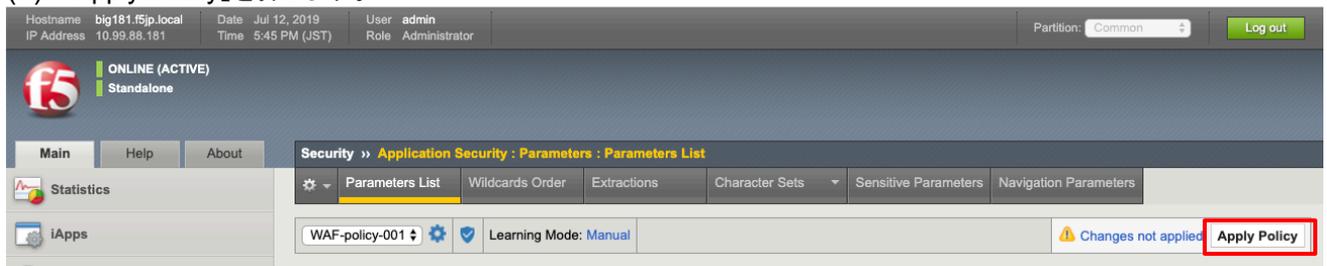
(3) 「Security」→「Application Security」→「Parameters」→「Parameters List」で表示された画面右上の「Create」ボタンを押します。



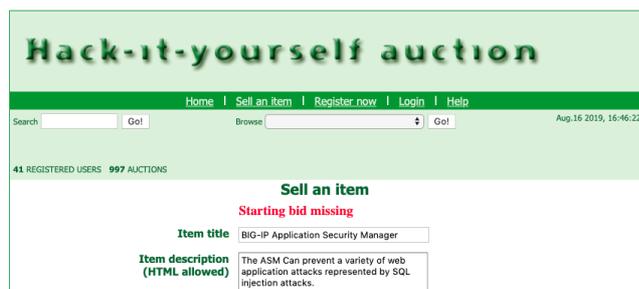
(4) 以下のように設定します。



(5) 「Apply Policy」を押します。



(6) クライアントのブラウザからもう一度、BIG-IP をオークションで売るための入力を試みます。今度は検知されず、次の画面に遷移します。(F5LAB アプリの作りにより、まずは左の画面がされ、全て入力した場合には右のような画面に遷移します。)



### 7.3. [対策 2] シグネチャの誤検知が発生したパラメータで、そのシグネチャを無効化する

誤検知が発生したパラメータで、その誤検知したシグネチャだけを無効化する方法を示します。

(1) もう一度、作成した「description」パラメータの設定画面を開き、以下のように設定します。

Hostname: big181.f5.jp.local | Date: Jul 12, 2019 | User: admin | IP Address: 10.99.88.181 | Time: 5:50 PM (JST) | Role: Administrator | Partition: Common | Log out

ONLINE (ACTIVE) Standalone

Security >> Application Security : Parameters : Parameters List >> Parameter Properties

Parameter Properties

Edit Parameter

Parameter Name: description (Explicit)

Parameter Level: Global

Perform Staging:  Enabled

Allow Empty Value:  Enabled

Allow Repeated Occurrences:  Enabled

Mask Value in Logs:  Enabled

Parameter Value Type: User-input value (1) User-Input-Value を選択

Data Type: Value Meta Characters Attack Signatures (2) Attack Signatures タブをクリック

Check attack signatures and threat campaigns on this parameter

Overridden Security Policy Settings:

Attack Signature	State
<input type="checkbox"/> SQL-INJ expressions like "or 1=1" (6) (Parameter)	Disabled (5) Disabled であることを確認

Global Security Policy Settings: << (4) 「<<」ボタンを押す >>

(3) 誤検知したシグネチャの ID を入力: 200002476 Total: 0

Cancel Update

[ご参考] Signature ID は以下になります。

Attack Signature	Signature ID 200002476
	Signature Name SQL-INJ expressions like "or 1=1" (6) (Parameter)

(2) 「Apply Policy」を押します。

ONLINE (ACTIVE) Standalone

Security >> Application Security : Parameters : Parameters List

Parameters List

Current edited security policy: WAF-policy-001 (blocking, modified)

Changes have not been applied yet Apply Policy

(3) クライアントのブラウザからもう一度、BIG-IP をオークションで売る入力をしてみます。

[対策 1]と同様、攻撃として検知されず、次の画面に遷移します。

(F5LAB アプリの作りにより、まずは左の画面がされ、全て入力した場合には右のような画面に遷移します。)

Hack-it-yourself auction

Home | Sell an item | Register now | Login | Help

Search: [ ] Go! Browse: [ ] Go!

41 REGISTERED USERS 997 AUCTIONS

Sell an item

Starting bid missing

Item title: BIG-IP Application Security Manager

Item description (HTML allowed): The ASM Can prevent a variety of web application attacks represented by SQL injection attacks.

Hack-it-yourself auction

Home | Sell an item | Register now | Login | Help

Search: [ ] Go! Browse: [ ] Go!

39 REGISTERED USERS 636 AUCTIONS

You can still make changes to your auction

Item title: BIG-IP Application Security Manager

Item description (HTML allowed): The ASM can prevent a variety of web application attacks represented by SQL injection attacks. For example, when an attacker put "' OR 1=1 #' into username form of a web page, the web application might permit the user to login. This attack called SQL injection. BIG-IP ASM can protect attacks against web application.

(4) [対策 3]を試しますので、作成した Parameter: description を削除してください。

Hostname: big181.f5jp.local | Date: Jul 12, 2019 | User: admin | IP Address: 10.99.88.181 | Time: 5:52 PM (JST) | Role: Administrator | Partition: Common | Log out

ONLINE (ACTIVE) Standalone

Apply Policy Configuration  
Operation completed successfully.

Security » Application Security : Parameters : Parameters List

Parameters List

WAF-policy-001 | Learning Mode: Manual | Apply Policy

Parameters List

Parameter Contains: [ ] Go | Show Filter Details

Total Entries: 3

Legend: Waiting for additional traffic samples Learning suggestions available Ready to be enforced | Create...

Parameter Name	Parameter Value Type	Parameter Level	Staging
* [ ]	User-input value	Global	No
[ ] __VIEWSTATE	Ignore value	Global	No
[ checked="" ] description	User-input value	Global	No

Change Type... Enforce Delete Delete All

Total Entries: 3

(5) 「Apply Policy」を押します。

Hostname: big181.f5jp.local | Date: Jul 12, 2019 | User: admin | IP Address: 10.99.88.181 | Time: 5:53 PM (JST) | Role: Administrator | Partition: Common | Log out

ONLINE (ACTIVE) Standalone

Security » Application Security : Parameters : Parameters List

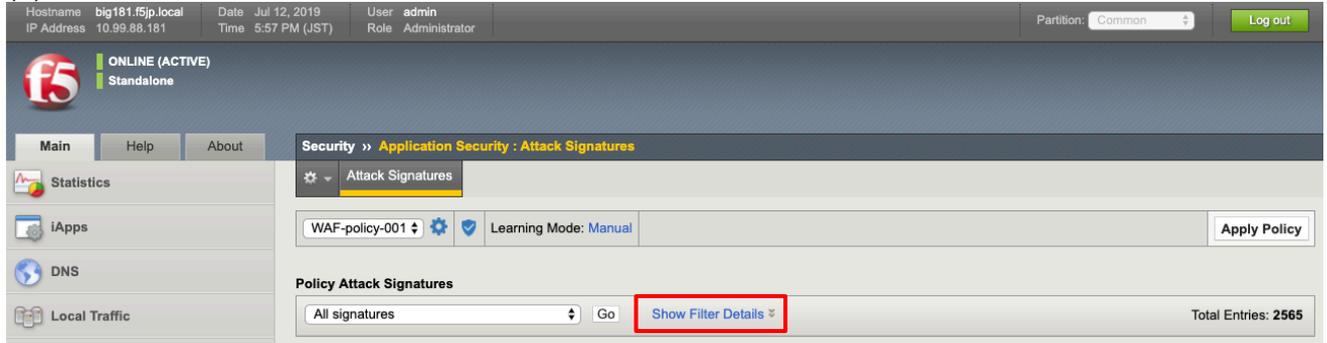
Parameters List

WAF-policy-001 | Learning Mode: Manual | Changes not applied | Apply Policy

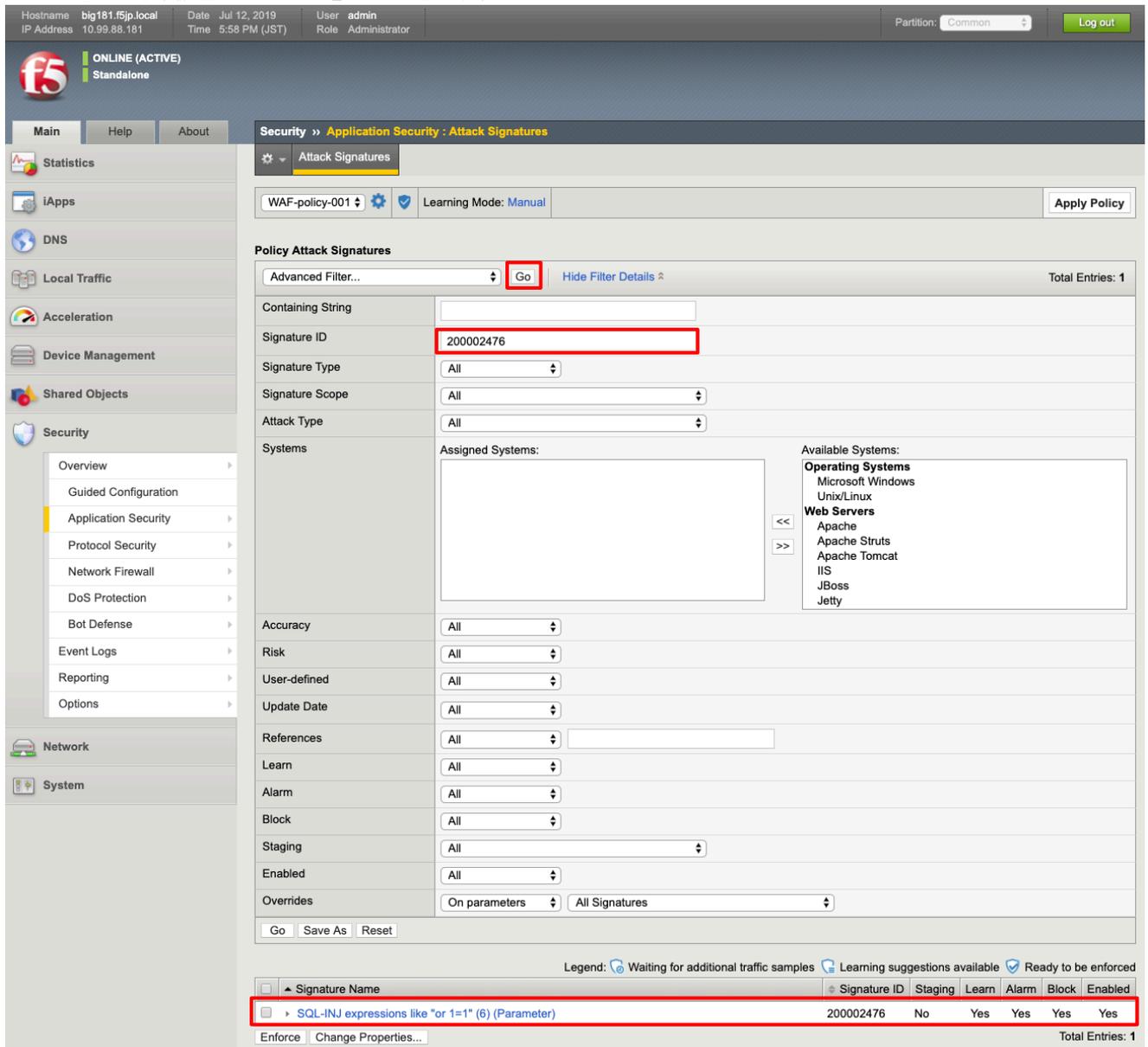
#### 7.4. [対策 3] 誤検知したシグネチャを全体で無効化し、そのシグネチャで守りたいパラメータだけに適用する

誤検知したシグネチャを全体で無効化し、特定のパラメータにだけそのシグネチャを適用する方法を示します。ここでは、「username」にのみ、そのシグネチャを適用します。

- (1) 「Security」→「Application Security」→「Attack Signatures」を選択します。
- (2) 「Show Filter Details」を選択します。



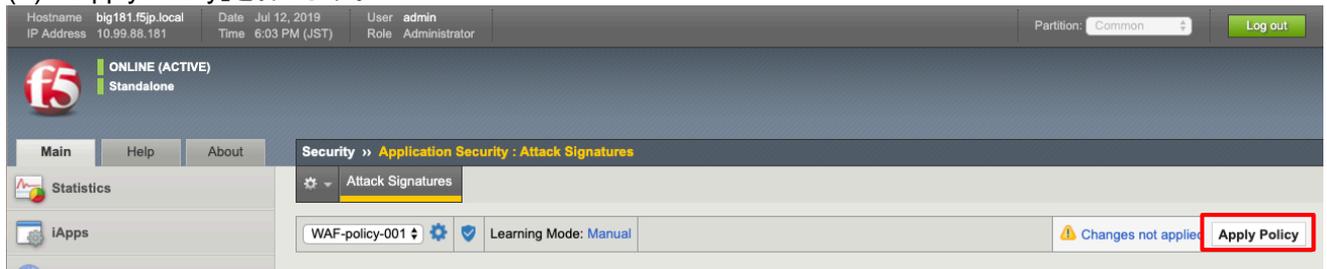
- (3) Signature ID に誤検知したシグネチャ ID (200002476) を入力し、Go を押すと、該当のシグネチャが下の方に表示されます。該当シグネチャをクリックします。



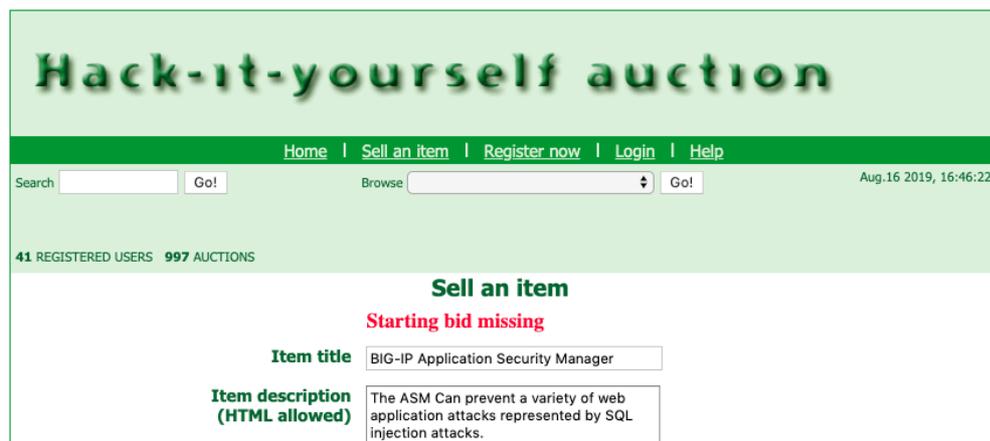
(4) Enable の Enabled のチェックを外し、Update ボタンを押します。



(5) 「Apply Policy」を押します。



(6) クライアントのブラウザからもう一度、BIG-IP をオークションで売るための入力を試みます。[対策 1][対策 2]と同様、攻撃として検知されず、次の画面に遷移します。



(7) しかし、username に「' OR 1=1 #」を入力して SQL インジェクション攻撃を実施すると、今度は通過してしまいます。以降、この対策を実施します。



- (8) 「Security」→「Application Security」→「Parameters」→「Parameters List」で表示された画面右上の「Create」ボタンを押すと、以下の画面が現れます。  
「username」パラメータを作り、以下のように設定します。

[ご参考] Signature ID は以下になります。

Attack Signature	<b>Signature ID</b> 200002476
	<b>Signature Name</b> SQL-INJ expressions like "or 1=1" (6) (Parameter)

- (9) 「Apply Policy」を押します。

- (10) クライアントのブラウザからもう一度、username に「' OR 1=1 #」を入力して SQL インジェクション攻撃を実施します。今度は SQL インジェクション攻撃を検知します。

The requested URL was rejected. Please consult with your administrator.

Your support ID is: 10891647079625523765

[\[Go Back\]](#)

- (11) クライアントのブラウザからもう一度、BIG-IP をオークションで売る入力を試みます。  
攻撃として検知されず、画面が遷移します。  
(F5LAB アプリの作りにより、まずは左の画面がされ、全て入力した場合には右のような画面に遷移します。)



## 8. [Step3] File Type の設定を行う（強制ブラウジング対策）

強制ブラウジングは、ユーザに開示するつもりのないファイル（例えば、バックアップ用ファイル（“XX.bak”と名づけたもの）やシステム用ファイル（XX.conf）などを攻撃者が取得する、という攻撃です。

この攻撃は、開示するファイルの種類を限定しておくことで防御できます。

以下にその設定方法を示します。

### 8.1. File Types の設定

#### 8.1.1. File Types の学習

- (1) 「Security」→「Application Security」→「Policy Building」→「Learning and Blocking Settings」で表示された画面で、「Illegal file Type」を探します。以下のように、Learn / Alarm / Block を有効にします。また、Learn New File Types において、「Always」を選択し、「Save」ボタンを押します。

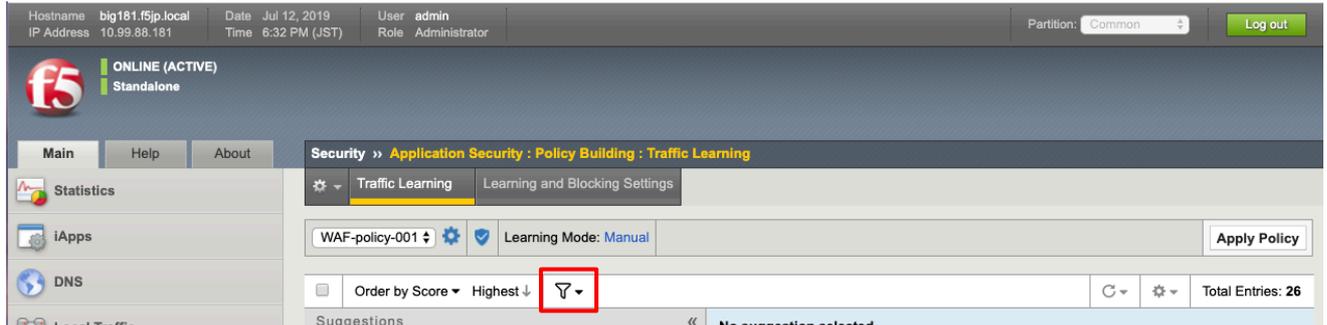
The screenshot shows the F5 Security Management console interface. The top navigation bar includes 'Main', 'Help', and 'About'. The main content area is titled 'Security >> Application Security : Policy Building : Learning and Blocking Settings'. Under 'Learning and Blocking Settings', the 'WAF-policy-001' is selected, and the 'Learning Mode' is set to 'Manual'. The 'Apply Policy' button is visible. The 'General Settings' section includes 'Enforcement Mode', 'Learning Mode', 'Learning Speed', and 'Enforcement Readiness Period'. The 'Policy Building Settings' section includes 'Antivirus', 'Attack Signatures', 'CSRF Protection', 'Content Profiles', 'Cookies', 'Data Guard', and 'Evasion technique detected'. The 'File Types' section is expanded, showing 'Learn New File Types' set to 'Always' and 'Maximum Learned File Types' set to 250. A table lists various file types with checkboxes for 'Learn', 'Alarm', and 'Block'. The 'Illegal file type' row has all three checkboxes checked. The 'Save' button is highlighted with a red box.

- (2) 「Apply Policy」ボタンを押します。

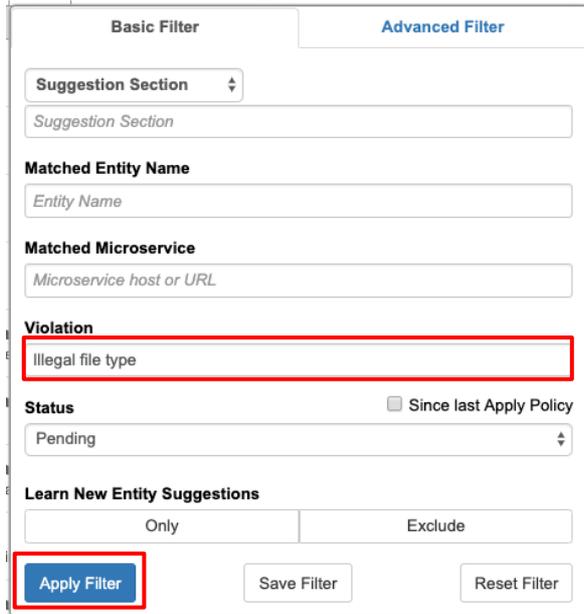
The screenshot shows the same F5 Security Management console interface as the previous one. The 'Apply Policy' button is now highlighted with a red box. A yellow warning icon and the text 'Changes not applied' are visible next to the button.

- (3) クライアントのブラウザのキャッシュを全部消してください。
- (4) クライアントのブラウザで、正当なユーザ（f5userX）でログインして、Web ページを巡回してください。

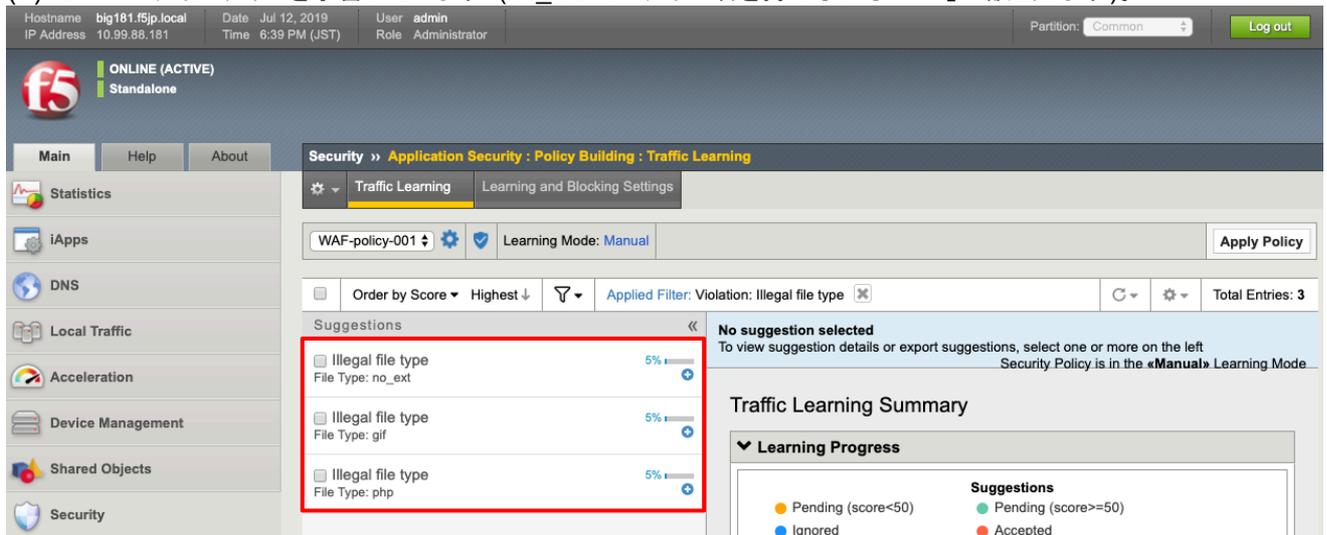
(5) 「Security」→「Application Security」→「Policy Building」→「Traffic Learning」で表示された画面で、Filtering アイコンをクリックします。



(6) Violation から illegal file type を選択し、Apply Filter を押します。



(7) 3つのファイルタイプを学習しています (no\_ext はファイル名を持たないもの:「/」が該当します)。



(8) すべてチェックを入れて、「Accept suggestions」ボタンを押します。

(9) 「Security」→「Application Security」→「File Types」→「Allowed File Types」で、Acceptしたファイルがここに表示されます。この学習済みのファイルだけを通過させる、という設定にしますので、「\*」を削除します。「\*」の先頭にチェックを入れ、「Delete」ボタンを押します。

Type	URL Length	Request Length	Query String Length	POST Data Length	Staging
<input checked="" type="checkbox"/> *	Any	Any	Any	Any	No
<input type="checkbox"/> gif	Any	Any	Any	Any	No
<input type="checkbox"/> no_ext	Any	Any	Any	Any	No
<input type="checkbox"/> php	Any	Any	Any	Any	No

(10) 「Apply Policy」ボタンを押します。

(11) クライアントのブラウザから、学習した以外のファイル、例えば Index.html へアクセスしてみます。

The requested URL was rejected. Please consult with your administrator.

Your support ID is: 10891647079625524117

[\[Go Back\]](#)

(12) 以下のような「強制ブラウジング」(Illegal file type)を示すログが出ます。

The screenshot shows the Fortinet Security Manager interface. The left sidebar contains navigation menus for Statistics, IApps, DNS, Local Traffic, Acceleration, Device Management, Shared Objects, Security, Network, and System. The main area displays 'Event Logs : Application : Requests'. A table lists several requests, with the first one selected. The details for this request show a triggered violation of 'Illegal file type'. The request details include the following information:

Violation	Occurrences	Suggestions
Illegal file type	1	View...

**Request Details**

Geolocation	N/A	Time	2019-07-12 18:46:09
Source IP Address	10.99.88.90:38636	Violation Rating	3 (Request needs further examination)
Session ID	9f91d9b2c2620414	Attack Types	Forceful Browsing
Microservice	N/A		

**Request**

Request actual size: 529 bytes.

```
GET /index.html HTTP/1.1
Host: 10.99.1.81
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Cookie: TS01ab2273=01c891b0419e1d8abd46047d42fb4cb4dfd3f7903434c5d154b6001091c76a9c7f28c626d0917d2421a69b7fa828ef2daab59068ffd564ff0b6794af51ac3f32d095ccca1; SESSION=vmalhnn2k2sseco30sqev3epg4
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_4) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1 Safari/605.1.15
Accept-Language: en-us
Accept-Encoding: br, gzip, deflate
Connection: keep-alive
```

(13) Occurrences をクリックします。html が違反として検知されていることが分かります。

File Type	html
Detection Cause	Illegal File Type
Applied Blocking Settings	Block Alarm Learn

(14) 本ガイドでは、学習したファイルのみ通過させる設定を例に取りましたが、実際の環境においては、以下 2 つのどちらかで対応してください。

① この学習した File Types だけを設定 (ホワイトリスト化) する。(本ガイドと同じ方法)

② 利用しないファイルを設定 (ブラックリスト化) する。

(ア) 学習したファイルがあまりに多すぎるから

(イ) 利用しないファイルは明確になっているから、など

この場合は、「Security」→「Application Security」→「File Types」→「Disallowed File Types」で指定します。

## 9. [Step4] 追加機能の要否検討

防御対象の Web アプリケーションに対して、「Step1」～「Step3」で設定した機能に加え、以下のセキュリティ機能が必要かどうかを判断します。

- ① Data Guard (クレジットカード番号のマスキング)
- ② L7 DoS への対策
- ③ Brute Force への対策
- ④ CSRF への対策
- ⑤ Threat Campaings シグネチャ

必要に応じて、追加で設定を実施してください。

以降、それぞれの設定方法を記載します。

## 9.1. Data Guard

クレジットカード番号の漏洩の危険性がある Web アプリケーションの場合、本機能により防御が可能です。HTTP レスポンスにクレジットカード番号が存在する場合、Adv.WAF はその番号をマスキングすることができます。

- (1) 「Security」→「Application Security」→「Policy Building」→「Learning and Blocking Settings」で表示された画面で、「Data Guard: Information leakage detected」を探します。  
以下のように、Learn / Alarm を有効にし、Block をはずし、「Save」ボタンを押します。

The screenshot shows the 'Learning and Blocking Settings' page for policy 'WAF-policy-001'. Under the 'Data Guard' section, the following table is visible:

Learn	Alarm	Block	Violation
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Data Guard: Information leakage detected
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Evasion technique detected (0 out of 8 subviolations are enabled)

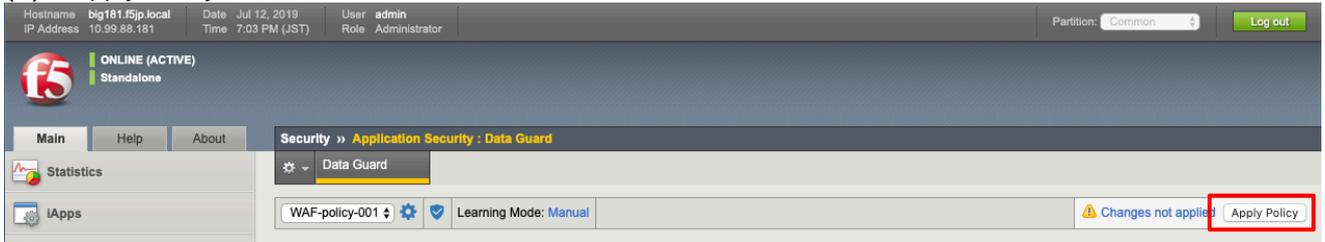
- (2) 「Security」→「Application Security」→「Data Guard」で表示された画面で、以下のように設定し、「Save」ボタンを押します。

The screenshot shows the 'Data Guard' configuration page. The 'Data Guard' section is expanded, showing the following settings:

- Data Guard
- Credit Card Numbers
- U.S. Social Security Numbers
- Custom Patterns
- Exception Patterns
- Mask Data
- File Content Detection

Red annotations highlight the 'Data Guard' checkbox (2), the 'Credit Card Numbers' checkbox (1), and the 'Save' button (3).

(3) 「Apply Policy」ボタンを押します。



(4) クレジットカード番号が登録されたユーザでログインします。  
「Your Control Panel」をクリックします。



(5) 以下のように、クレジットカード番号がマスキングされます。



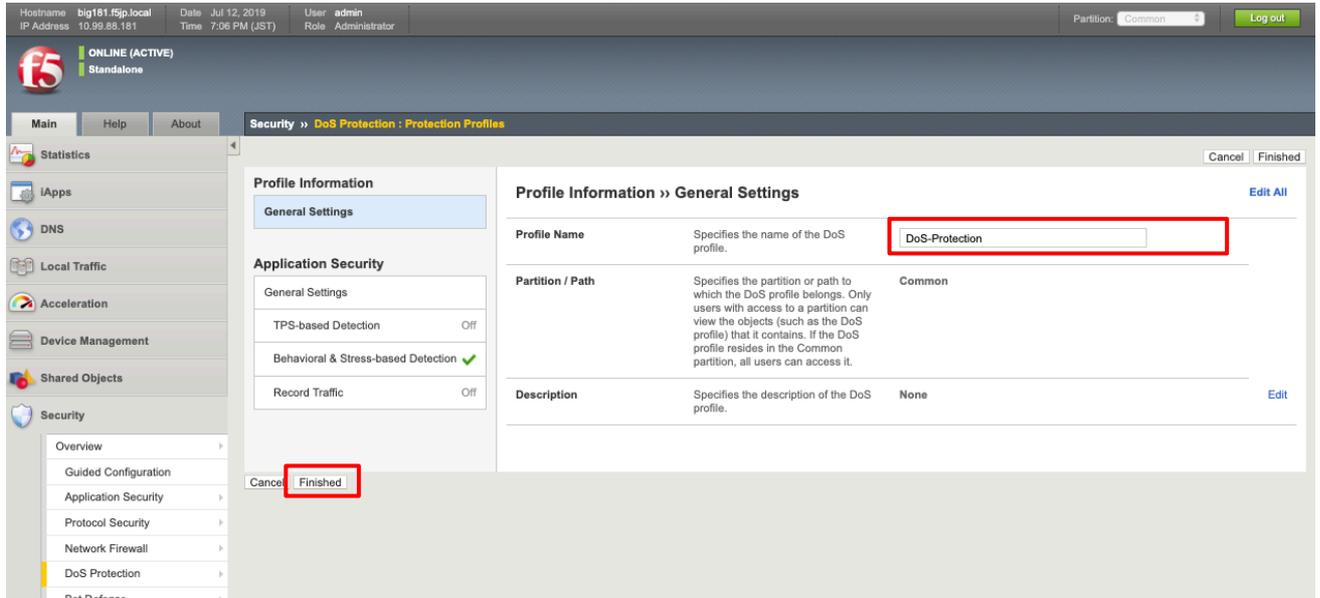
## 9.2. L7 DoS への対策 <ご参考>

DoS Protection 設定を行うことで、大量の HTTP リクエストが送り込まれてきていることを検知し、緩和することが可能です。

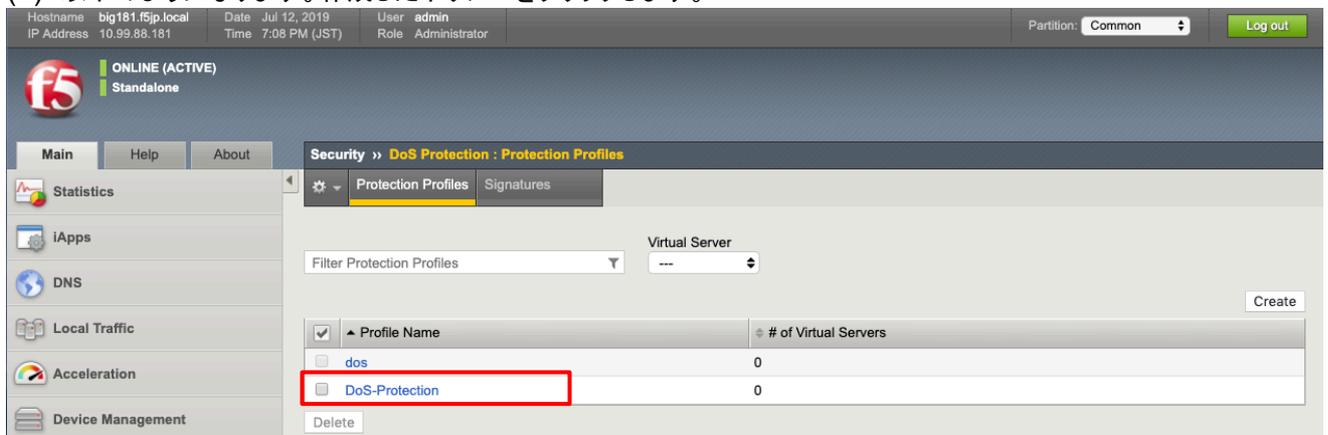
### 9.2.1. TPS-Based DoS

秒間の HTTP トランザクション数の変化で検知を行います。

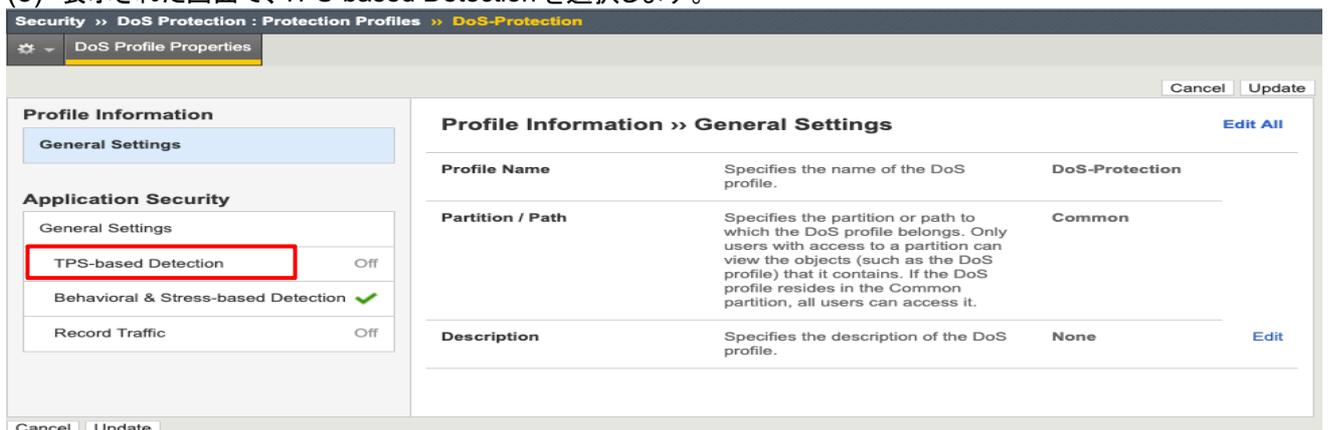
- (1) 「Security」→「DoS Protection」→「DoS Profiles」で表示された画面の右上にある「Create」ボタンを押し、現れた画面で Profile Name を設定し、Finished ボタンを押します。



- (2) 以下のようになります。作成したポリシーをクリックします。



- (3) 表示された画面で、TPS-based Detection を選択します。



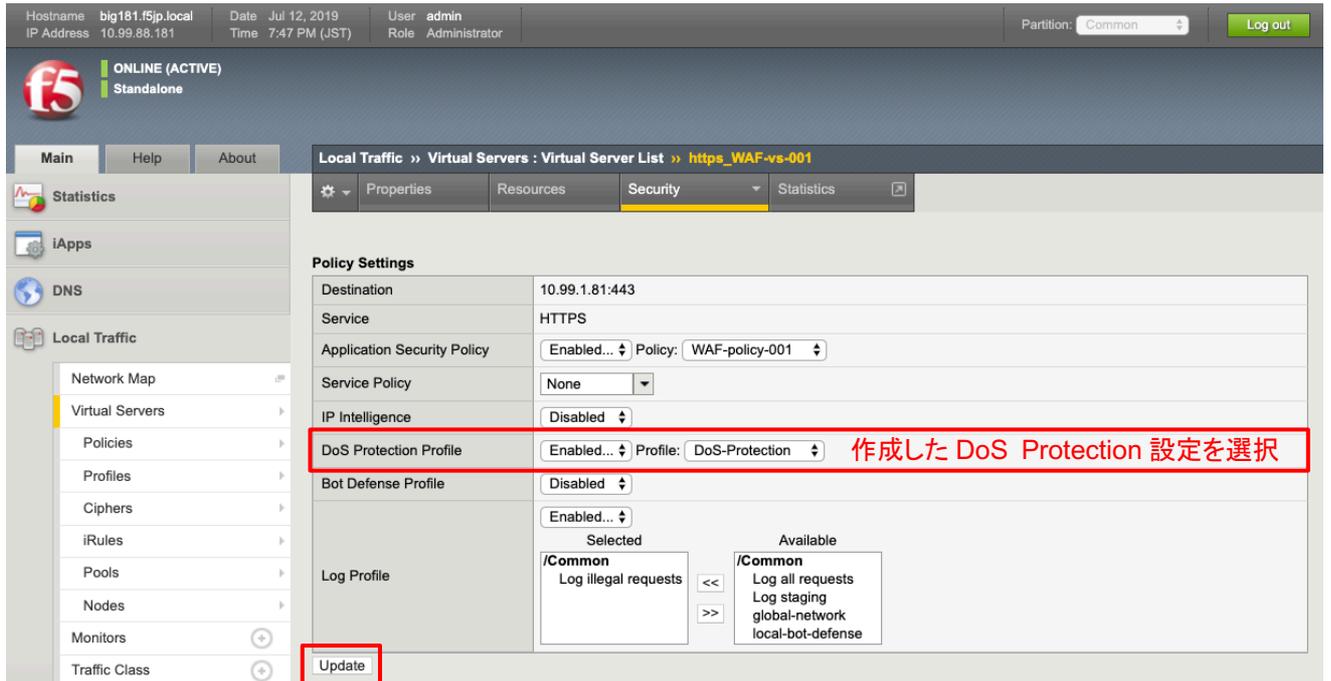
(4) Operation Mode で Blocking を選択します。

The screenshot shows the 'DoS Profile Properties' configuration page. On the left, there are sections for 'Profile Information' and 'Application Security'. The 'Application Security' section includes 'General Settings', 'TPS-based Detection' (Off), 'Behavioral & Stress-based Detection' (On), and 'Record Traffic' (Off). The main area is titled 'Application Security >> TPS-based DoS Detection'. It contains a description: 'This section configures the detection of DoS attacks based on high volume of incoming traffic.' Below this, the 'Operation Mode' is set to 'Blocking' (previously 'Off'). A red box highlights the 'Blocking' option in the dropdown menu. 'Cancel' and 'Update' buttons are visible at the bottom.

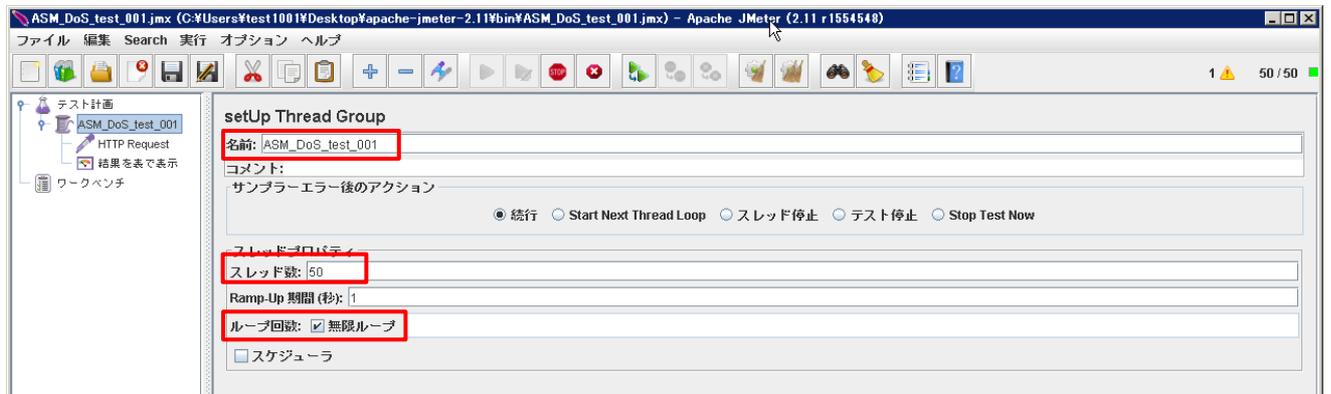
(5) 下記のように設定し、Update ボタンを押します。(検知しやすいように、値を小さめに変更しています。)

This screenshot shows the same configuration page with more settings highlighted. In the 'Application Security' sidebar, 'TPS-based Detection' is now checked and highlighted with a red box. The main area shows 'Operation Mode' set to 'Blocking'. Under 'How to detect attackers and which mitigation to use', three detection methods are listed: 'By Source IP', 'By Device ID', and 'By Geolocation'. The 'By Source IP' and 'By URL' sections are highlighted with red boxes. The 'By Source IP' section has 'Relative Threshold' set to 101% and 'Absolute Threshold' set to 20 TPS. The 'By URL' section has 'Relative Threshold' set to 101% and 'Absolute Threshold' set to 20 TPS, with 'Heavy URL Protection' checked. The 'Prevention Duration' section is also highlighted with a red box, showing an 'Escalation Period' of 30 seconds and a 'De-escalation Period' of 60 seconds. Red text labels 'By Source IP の設定', 'By URL の設定', and 'Prevention Duration の設定' are placed next to their respective sections. The 'Update' button at the bottom is also highlighted with a red box.

- (6) 「Local Traffic」→「Virtual Servers」で表示された Virtual Servers のうち、DoS プロテクションを実施したい Virtual Server を選択します。  
「Security」タブ→「Policies」で現れた画面で作成した DoS プロテクションポリシーを選択し、アップデートボタンを押します。

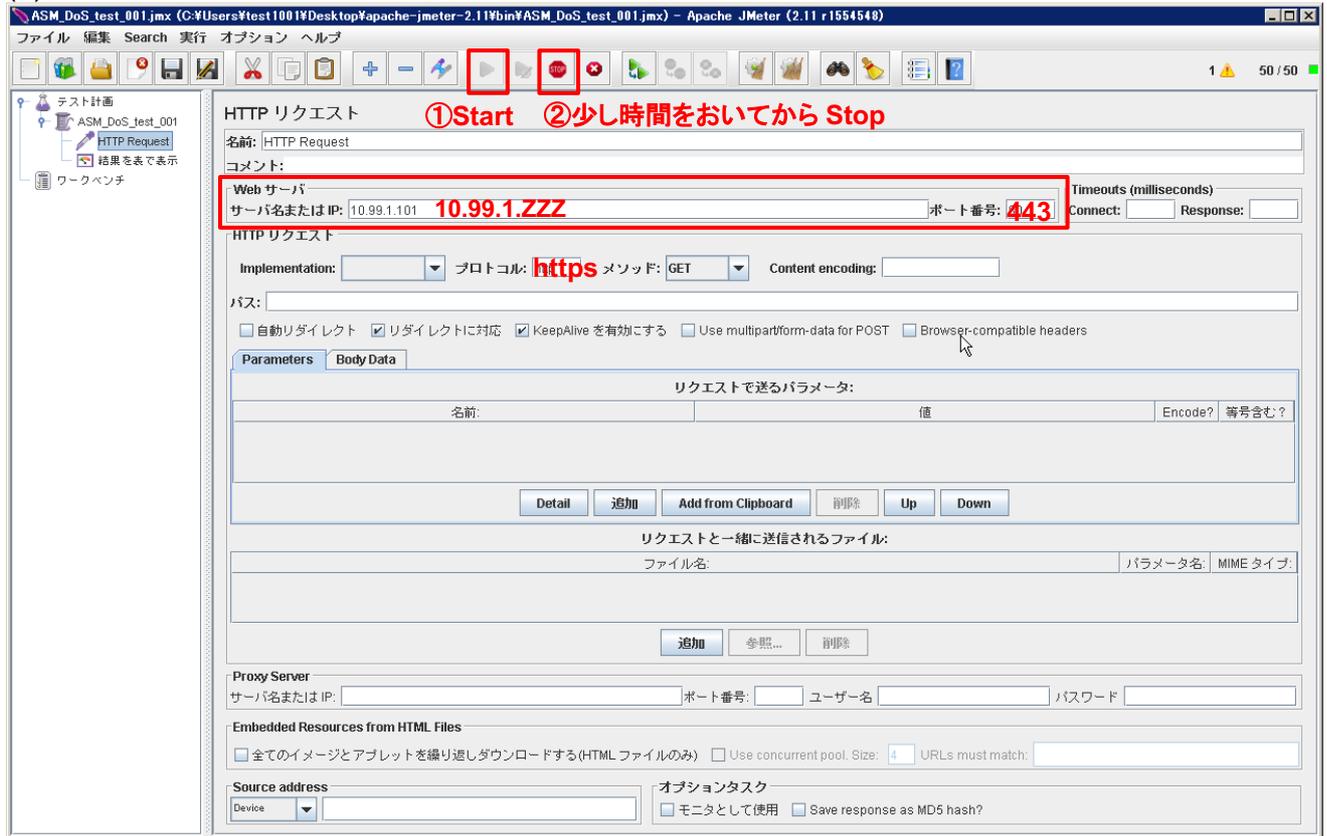


- (7) 本検証では、クライアント PC 上の JMeter を使って、多量の HTTP リクエストを生成します。  
スレッド:50

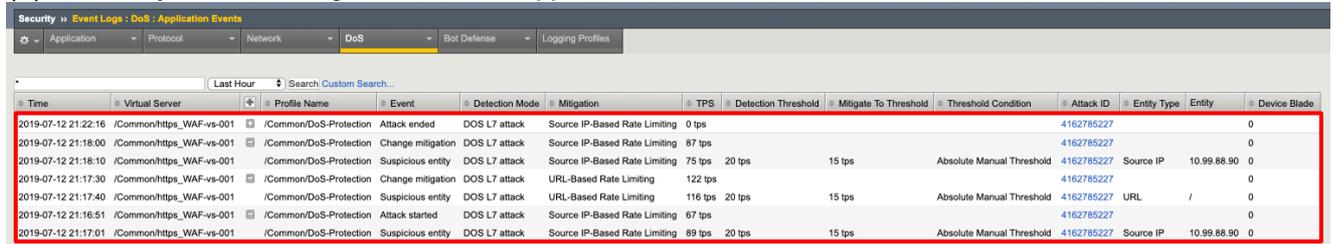


- ① 「テスト計画」を右クリックし、「Threads(Users)」の「setUp Thread Group」を追加。「無限ループ」にチェックを入れる。
- ② ①で作成した Thread Group を右クリックして、「サンプラー」の「HTTP リクエスト」を追加します。

(8) JMeter の HTTP リクエスト内容を設定し、リクエストを投げます。



(9) 「Security」→「Event Logs」→「DoS」→「Application Events」で、DoS 攻撃を検知していることを確認できます。



各 Attack ID をクリックすると、DoS Dashboard report を確認できます。

## 9.2.2. Stress-Based DoS

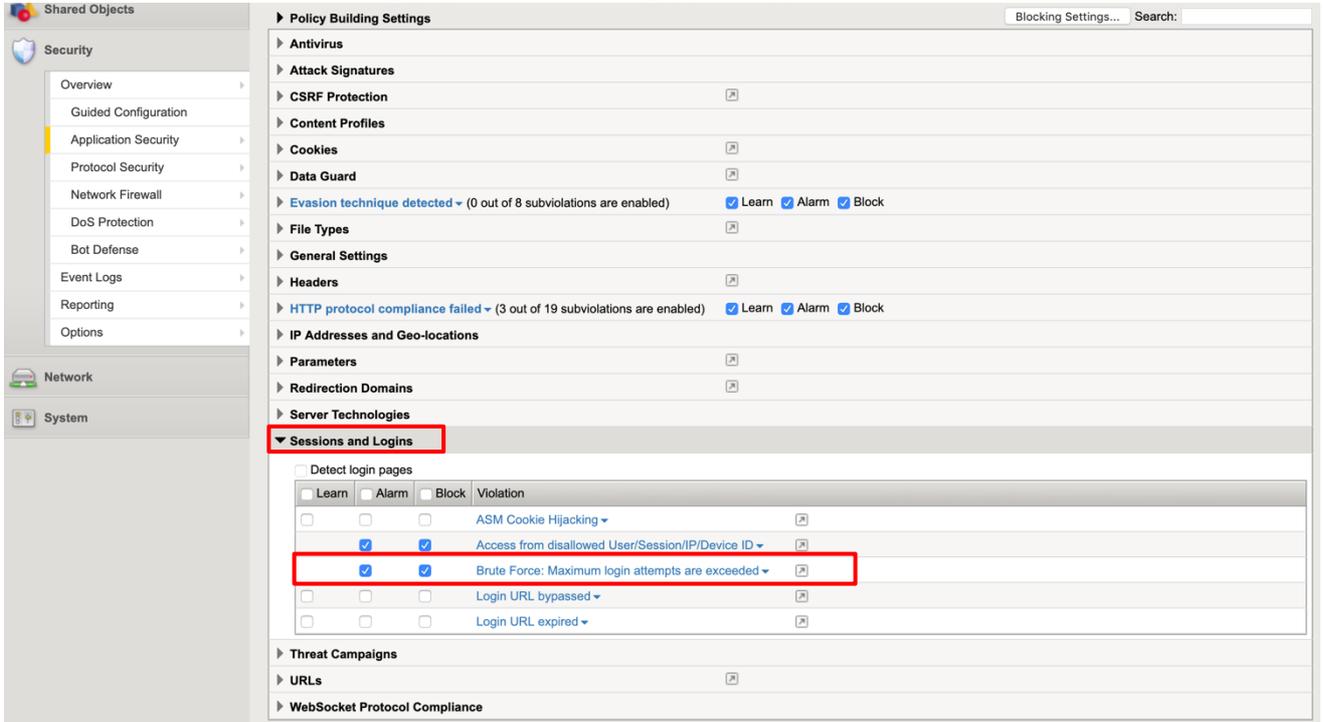
Stress-Based DoS は、TPS ベースと WEB サーバへのレイテンシをチェックする DoS 対策方法で、サーバのリソースをゆっくりと枯渇させるような攻撃の対策に有効です。

### 9.3. Brute Force の対策

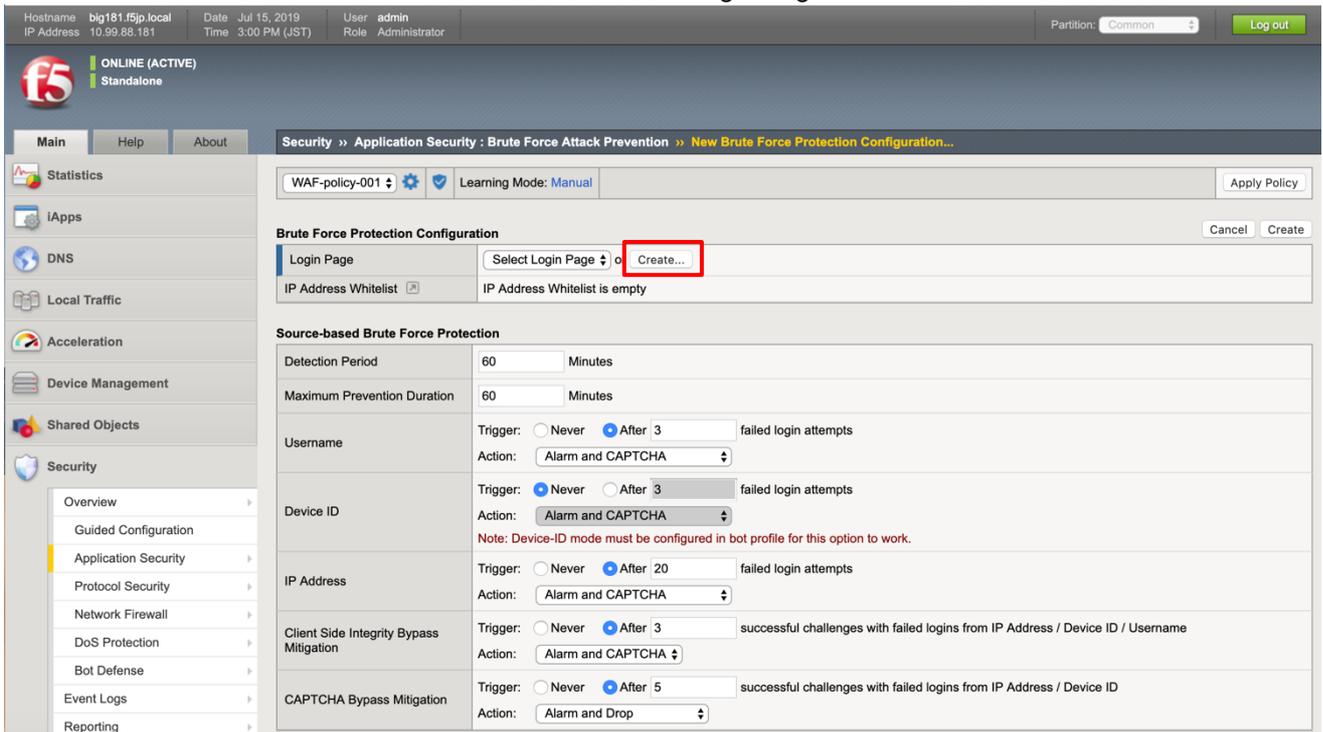
Adv.WAF は、ソース情報(ユーザ名、IP アドレスなど)ベースで Brute Force 対策を行っています。

#### 9.3.1. Brute Force 対策の設定

- (1) 「Security」→「Application Security」→「Policy Building」→「Learning and Blocking Settings」で表示された画面で、「Sessions and Logins」の「Brute Force: Maximum login attempts are exceeded」を探します。  
以下のように、Alarm/Block を有効となっていることを確認します。



- (2) 「Security」→「Application Security」→「Brute Force Attack Prevention」で表示された画面の右上にある「Create」ボタンを押すと、以下の画面が現れます。更に Login Page の「Create」ボタンを押します。



(3) 以下の画面が現れます。以下のように設定します。

### Create Login Page

**Login Page Properties**

Login URL	Explicit   HTTPS   /user_login.php	ユーザ名/パスワードを入力するページを指定
Authentication Type	HTML Form	
Username Parameter Name	username	ユーザ名のパラメータを入力
Password Parameter Name	password	パスワードのパラメータを入力

**Access Validation**

A string that should appear in the response	
A string that should <b>NOT</b> appear in the response	
Expected validation header name and value (for example, Location header)	
<b>NOT</b> Expected validation header name and value (for example, Location header)	
Expected validation domain cookie name	
Expected parameter name (added to URI links in the response)	本ガイドの Web アプリケーションは、認証が成功すると「302」のレスポンスコードを返すので、それを指定
Expected HTTP response status code	302
<b>NOT</b> Expected HTTP response status code	<input type="text"/> Add
	Delete

認証が成功したことが分かる、HTTP レスポンスのいずれかの値を入力

Cancel Create

- (4) 上記画面で「Create」ボタンを押すと、以下の画面に戻ります。  
 Source-based Brute Force Protection の値を必要に応じて変更します。  
 下記のように設定し、「Create」ボタンを押します。(下記設定は、検出しやすい値にしています。)

Security » Application Security : Brute Force Attack Prevention » New Brute Force Protection Configuration...

WAF-policy-001 [Settings] [Shield] Learning Mode: Manual [Changes not applied] [Apply Policy]

Brute Force Protection Configuration [Cancel] [Create]

Login Page [(HTTPS) /user\_login.php] [View Selected Login Page] or [Create...]

IP Address Whitelist [IP Address Whitelist is empty]

Source-based Brute Force Protection

Detection Period	5 Minutes	検証では検出しやすい値に設定
Maximum Prevention Duration	5 Minutes	
Username	Trigger: <input checked="" type="radio"/> Never <input type="radio"/> After 3 failed login attempts Action: Alarm and CAPTCHA	
Device ID	Trigger: <input checked="" type="radio"/> Never <input type="radio"/> After 3 failed login attempts Action: Alarm and CAPTCHA Note: Device-ID mode must be configured in bot profile for this option to work.	
IP Address	Trigger: <input type="radio"/> Never <input checked="" type="radio"/> After 3 failed login attempts Action: Alarm and CAPTCHA	a. 同じ IP アドレスで 3 回失敗すると、ログ出力し、ユーザに CAPTCHA を表示
Client Side Integrity Bypass Mitigation	Trigger: <input checked="" type="radio"/> Never <input type="radio"/> After 3 successful challenges with failed logins from IP Address / Device ID / Username Action: Alarm and CAPTCHA	
CAPTCHA Bypass Mitigation	Trigger: <input type="radio"/> Never <input checked="" type="radio"/> After 3 successful challenges with failed logins from IP Address / Device ID Action: Alarm and Blocking Page	b. CAPTCHA 入力に 3 回成功しても、同じ IP アドレスからの ID/PASSWORD の入りに失敗した場合は、ログ出力し、ユーザにブロックページを表示

Distributed Brute Force Protection

Detection Period	15 Minutes
Maximum Prevention Duration	60 Minutes
Detect Distributed Attack	<input type="radio"/> Never <input checked="" type="radio"/> After 100 failed login attempts
Detect Credential Stuffing	<input type="radio"/> Never <input checked="" type="radio"/> After 100 login attempts that match known leaked credentials dictionary
Mitigation	Alarm and CAPTCHA

[Cancel] [Create]

- (5) 「Apply Policy」ボタンを押します。

Hostname big181.f5jp.local Date Jul 15, 2019 User admin  
 IP Address 10.99.88.181 Time 3:19 PM (JST) Role Administrator Partition: Common [Log out]

f5 ONLINE (ACTIVE) Standalone

Main Help About Security » Application Security : Brute Force Attack Prevention

Brute Force Attack Prevention

WAF-policy-001 [Settings] [Shield] Learning Mode: Manual [Changes not applied] [Apply Policy]

Brute Force Configurations [Create...]

Login URL  
 [(HTTPS) /user\_login.php]

- (6) 登録したログインページにアクセスし、クライアント PC から、ユーザ名のみ入力し、「クエリ送信」ボタンを押します。  
これを 3 回以上繰り返します。

← → ↻ ▲ 保護されていない通信 | https://10.99.1.81/user\_login.php ☆ 👤 ⋮

# Hack-it-yourself auction

Home | Sell an item | Register now | Login | Help

Search   Browse   Jul.15 2019, 13:32:20

41 REGISTERED USERS 983 AUCTIONS

## User's login

Your name

Password

[Forgot your password?](#)

Home | Sell an item | Register now | Login | Help

Copyright 2000-2002, PHPAUCTION.ORG

- (7) 以下のように CAPTCHA が表示されます。Code を入力して、submit ボタンを押します。

This question is for testing whether you are a human visitor and to prevent automated spam submission.

What code is in the image?

Your support ID is: 1530498216676977362.

- (8) 更に 3 回以上、パスワード入力を誤る操作と CAPTHCHA 対応を返します。

- (9) 以下のようにブロック画面が表示されます。

The requested URL was rejected. Please consult with your administrator.

Your support ID is: 15304982166769773718

[\[Go Back\]](#)

(10) 「Security」→「Event Logs」→「Application」→「Requests」で、Brute Force 攻撃の検知の動作を確認します。

a. 同じ IP アドレスからの接続で入力を連続して誤り、CAPTCHA 表示をされた際のログサンプルログ

The screenshot shows the 'Requests' list with the following entries:

Request	Score	Severity
[HTTPS] /user_login.php 10.99.4.18 16:13:27 2019-07-15	5	N/A
[HTTPS] /user_login.php 10.99.4.18 16:13:27 2019-07-15	5	200
[HTTPS] /user_login.php 10.99.4.18 16:13:16 2019-07-15	5	200
[HTTPS] /user_login.php 10.99.4.18 16:13:03 2019-07-15	5	200

The selected request details are as follows:

Field	Value
Mitigated Action	Alarm and CAPTCHA
Client IP Address	10.99.4.18
Detected Failed Logins / Threshold	3 / 3 (at the time of attack detection)
Detection Period	5 minutes
Maximum Prevention Duration	5 minutes
Applied Blocking Settings	Block Alarm

b. CAPTCHA を複数回入力するものを入力を引き続き誤り、ブロック画面を表示された際のログサンプルログ

The screenshot shows the 'Requests' list with the following entries:

Request	Score	Severity
[HTTPS] /user_login.php 10.99.4.18 16:13:41 2019-07-15	5	N/A
[HTTPS] /user_login.php 10.99.4.18 16:13:27 2019-07-15	5	200
[HTTPS] /user_login.php 10.99.4.18 16:13:16 2019-07-15	5	200
[HTTPS] /user_login.php 10.99.4.18 16:13:03 2019-07-15	5	200

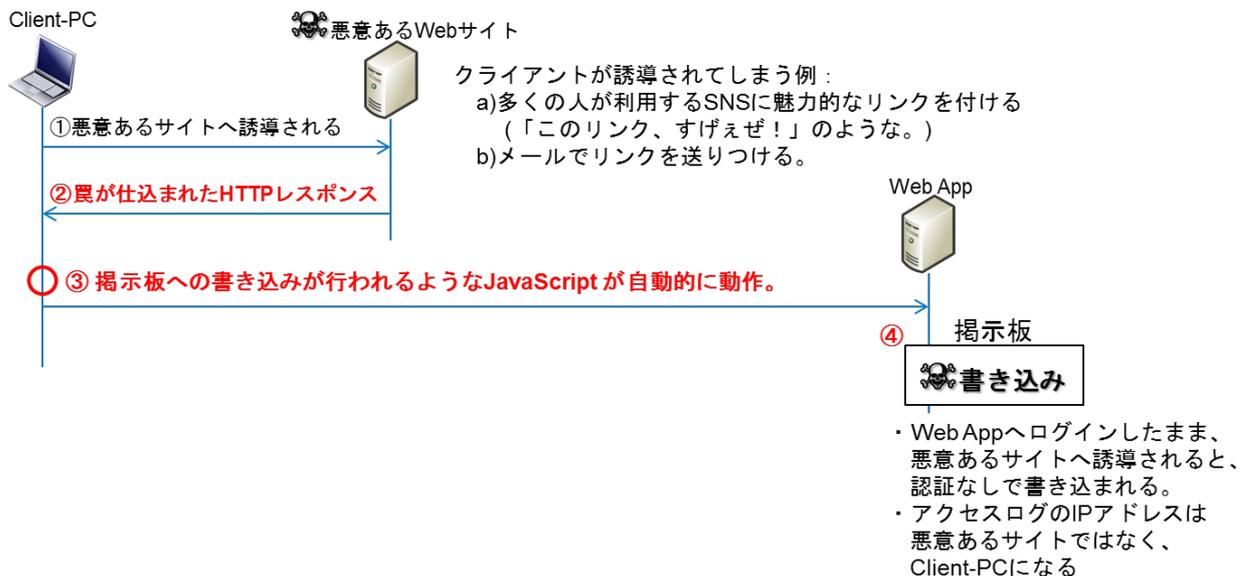
The selected request details are as follows:

Field	Value
Mitigated Action	Alarm and Blocking Page
Client IP Address	10.99.4.18
Detected Failed Logins / Threshold	6 / 3 (at the time of attack detection)
Detection Period	5 minutes
Maximum Prevention Duration	5 minutes
Total Passed CAPTCHA Challenges / Threshold	3 / 3
Applied Blocking Settings	Block Alarm

## 9.4. CSRF (Cross Site Request Forgery) への対策

### 9.4.1. CSRF 攻撃とは

CSRF は以下のような攻撃です。



- ① クライアントが何らかの形で悪意ある Web サイトへ誘導されてしまう。  
(ア) SNS 上に、魅力的な文面が書かれたリンク  
(イ) 不正なメールのリンク
- ② 罠（悪意ある JavaScript 等）が仕込まれた HTTP レスポンスを受け取ってしまう。
- ③ その HTTP レスポンスを受け取ったと同時に、掲示板への書き込みが行われる JavaScript が動作する。
- ④ Web サイトに、意図しない書き込みが行われる。

CSRF は、Web アプリケーションから見ると「正当なユーザからの HTTP リクエスト」と「悪意あるサイトによって作られた HTTP リクエスト」の区別がつかないため、シグネチャによる防御が難しい攻撃です。

よって、「正当なユーザからの HTTP リクエスト」と「悪意あるサイトによって作られた HTTP リクエスト」を区別できる方法を提供できれば、この攻撃を防御することができる、といえます。

Adv.WAF の CSRF 対策イメージ：

例えば、以下のようなリンクが実 Web サーバからの HTTP レスポンスの Body に存在していた、とします。

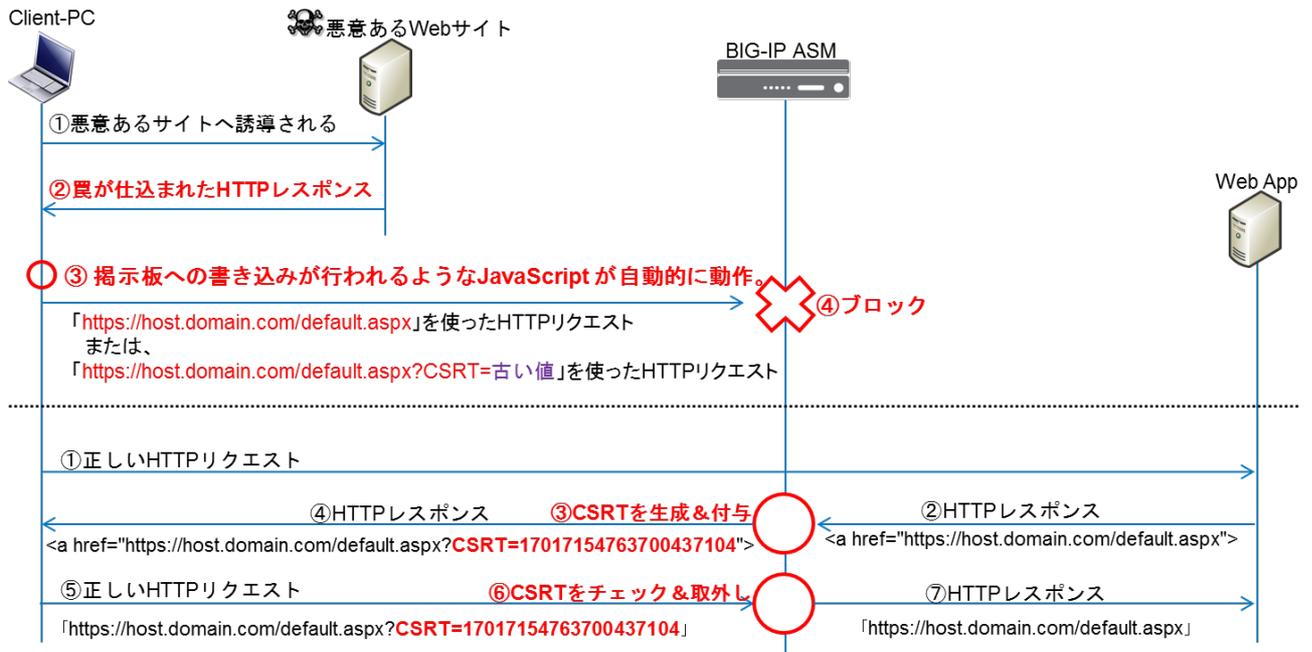
```
<a href="https://host.domain.com/default.aspx">.....(a)
```

Adv.WAF の CSRF プロテクト機能を有効にすることで、Adv.WAF はこの実 Web サーバからのリンクに、以下のような形で動的な値を Query String として加えます。

```
<a href="https://host.domain.com/default.aspx?CSRT=17017154763700437104">.....(b)
```

正当なユーザの HTTP リクエストの URI は、動的に変化する CSRT を持つ(b)を使います。

悪意あるサイトによる HTTP リクエストは、(a)を利用する、または、攻撃者が以前に取得した、古い値を持つ(b)を使うので、正当なユーザの HTTP リクエストと区別することができます。



(厳密には、Adv.WAF が HTTP レスポンスに埋め込んだ JavaScript によって、上記の CSRT 値を付与する方式を取っています。)

#### 9.4.2. CSRF 対策の設定

- (1) 「Security」→「Application Security」→「Policy Building」→「Learning and Blocking Settings」で表示された画面で、「CSRF Protection」を探します。  
以下のように、Alarm/Block を有効になっていることを確認します。

Security >> Application Security : Policy Building : Learning and Blocking Settings

Traffic Learning Learning and Blocking Settings

WAF-policy-001 Learning Mode: Manual Apply Policy

General Settings

Enforcement Mode Blocking

Learning Mode Manual

Learning Speed Medium

Enforcement Readiness Period 7 days

Policy Building Settings

Antivirus

Attack Signatures

CSRF Protection

Learn Alarm Block Violation

CSRF attack detected

CSRF authentication expired

Content Profiles

- (2) 「Security」→「Application Security」→「CSRF Protection」で表示された画面で、CSRF Protection にチェックをいれ、Save ボタンを押します。

Security >> Application Security : CSRF Protection

WAF-policy-001 Learning Mode: Manual Apply Policy

**CSRF Protection**

CSRF Protection  Enabled チェックを入れる

SSL Only  Enabled

Expiration Time  Enabled

Simple Edit Mode

URLs List for POST requests with CSRF token verification only (Wildcards supported)

New URL  Add

URL  \*

Delete Total Entries: 1

Save Note: Click Save to retain any changes you made on this screen.

- (3) 「Apply Policy」を押します。

Hostname big181.f5.jp.local Date Jul 15, 2019 User admin  
IP Address 10.99.88.181 Time 4:46 PM (JST) Role Administrator Partition: Common Log out

ONLINE (ACTIVE) Standalone

Main Help About Security >> Application Security : CSRF Protection

WAF-policy-001 Learning Mode: Manual Changes not applied Apply Policy

- (4) 例えば、「Login」をクリックしてみると、下図のように、csrftok 値が Query String として付与されていることが分かります。(ここでは、以降のテストを簡単に行うため、http の Virtual Server (http://10.99.1.ZZZ) に接続します。)

← → ↻ ⓘ 保護されていない通信 | 10.99.1.81/user\_login.php?csrftok=16555410474506134575

# Hack-it-yourself auction

Home | Sell an item | Register now | **Login** | Help

Search  Go! Browse  Go! Jul.15 2019, 14:06:23

41 REGISTERED USERS 983 AUCTIONS

## User's login

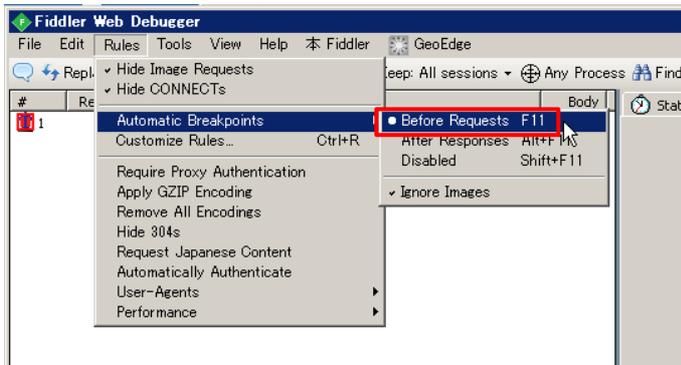
Your name

Password

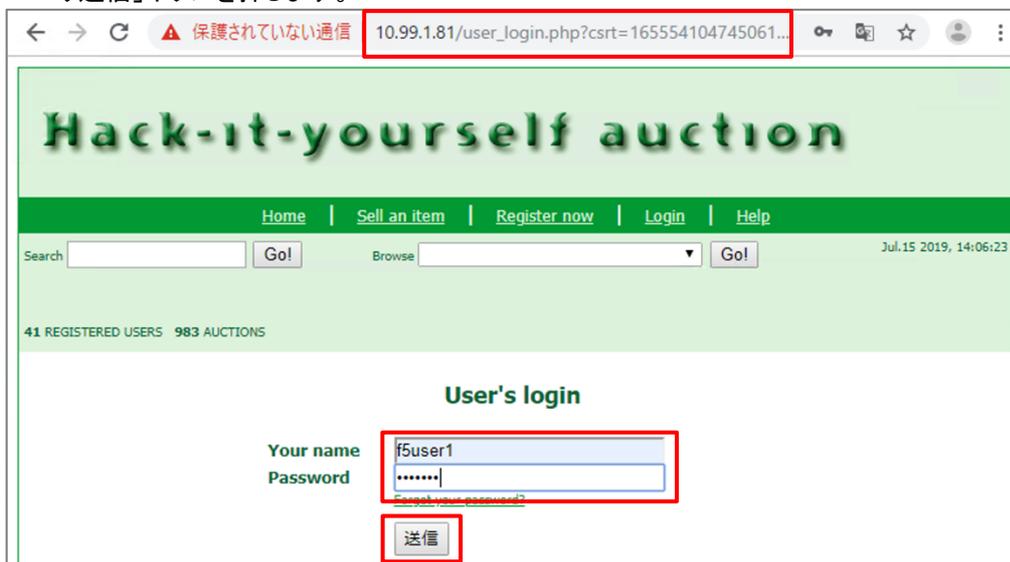
[Forgot your password?](#)

送信

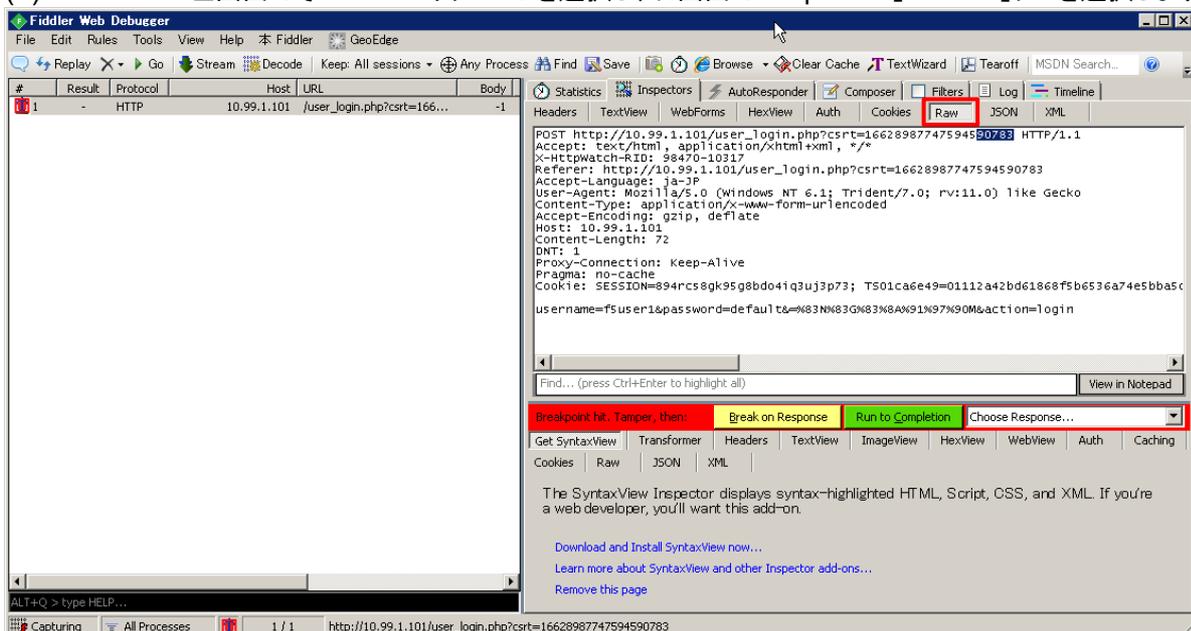
- (5) クライアントのブラウザから攻撃を模擬するために、Fiddler2 を利用します。  
Fiddler2 を起動し、「Rules」→「Automatic Breakpoints」→「Before Requests」を選択(有効に)します。
- (6) (https 通信の場合、「Tools」→「Options」の「HTTPS」タブにて、「Capture HTTPS CONNECTs」と「Decrypt HTTPS traffic」を有効にして、Fiddler が作成するルート証明書を許可し、その証明書をブラウザにインポートする必要があります。)



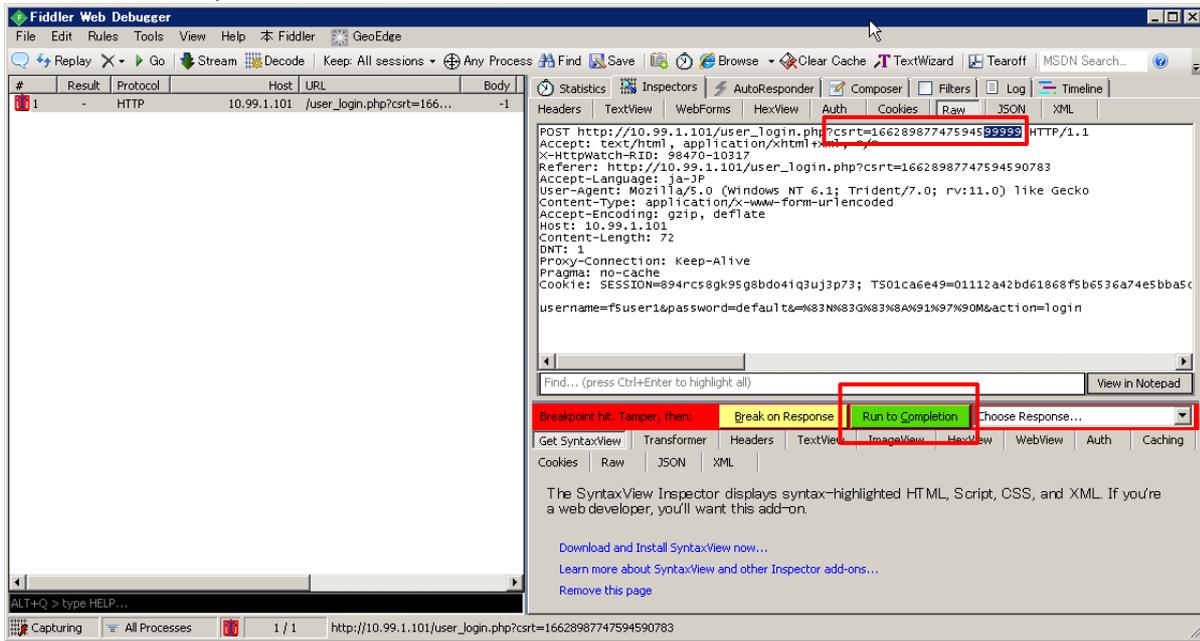
- (7) ここでは http の Virtual Server にアクセスし、ブラウザに正当なユーザ名 (f5userX) とパスワードを入力し、「クエリ送信」ボタンを押します。



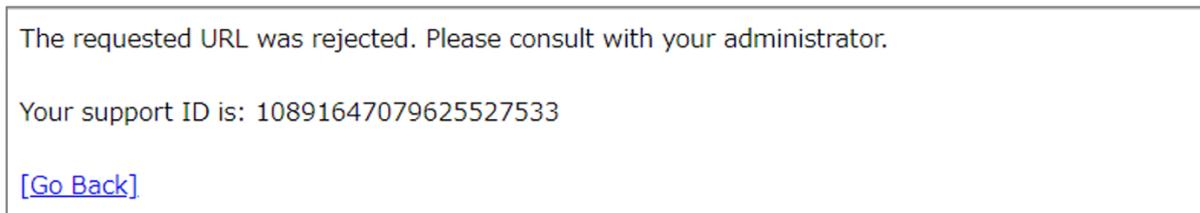
- (8) Fiddler2 がこの HTTP リクエストをインターセプトするので、先に進みません。
- (9) Fiddler2 の左画面でその HTTP リクエストを選択し、右画面で「Inspectors」→「Raw」タブを選択します。



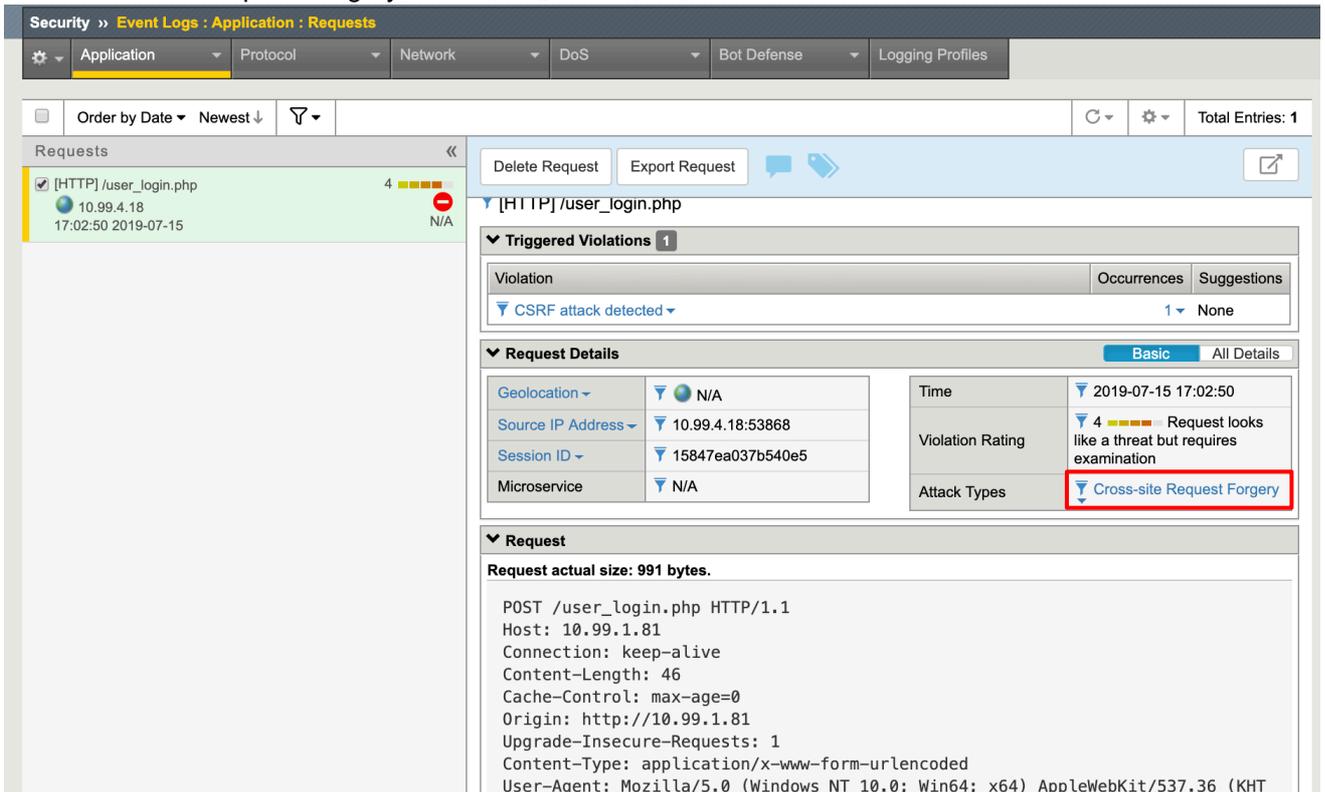
- (10)CSRT の値の末尾 5 桁を以下のように「99999」に書き換えてみます。  
 =古い CSRT 値を使って攻撃をしてきている、という想定です。  
 「Run to Completion」ボタンを押します。



- (11)Adv.WAF が期待する CSRT 値ではない HTTP リクエストが到達したため、攻撃として検知します。



- (12) Fiddler2 を終了し、「Security」→「Event Logs」→「Application」→「Requests」でログを確認します。  
 「Cross-site Request Forgery」として検知されています。



## 9.5. Threat Campaigns シグネチャ <ご参考>

※F5 ハンズオンでは実施しません

Web アプリケーションの脅威対策を行う上で、実際の攻撃とフォールスポジティブを見極めることに直面することがあります。シグネチャや WAF の様々な機能によって、既知の脆弱性に対する攻撃リクエストを評価すると同時に、悪意のないリクエストも評価されるため、管理者は WAF で検知されたアラートに対し、正常なリクエストか悪意のあるリクエストか判断を迫られることがあります。

この問題は、検査するデータがシングルポイントであることにあります。もっと多くの条件を元にリクエストを検査することによって、この問題を解決することができる場合があります。F5 はこの問題を解決する手法として、“Threat Campaigns シグネチャ”という独自のシグネチャを提供しています。Threat Campaigns シグネチャは、実際の攻撃キャンペーンを元に複数の条件をマッピングされたものになっています。

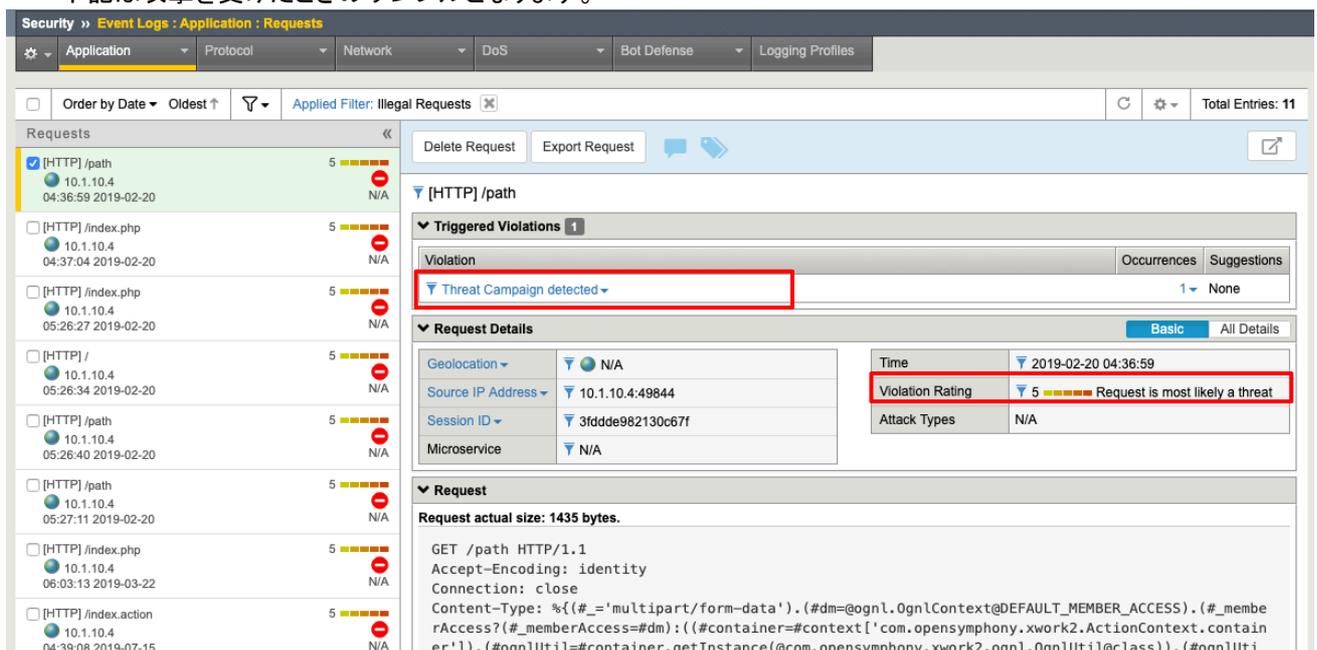
この項では、Threat Campaign の設定確認と、テキスト上にて攻撃サンプルログを確認します。

(注: Threat Campaigns はサブスクリプション形式のライセンスとなります。)

- (1) 「Security」→「Application Security」→「Policy Building」→「Learning and Blocking Settings」で表示された画面にて、Threat Campaigns の Alarm&Block 有効になっていることを確認します。



- (2) 攻撃を受けたと仮定して、「Security」→「Event Logs」→「Application」→「Requests」でログを確認します。下記は攻撃を受けたときのサンプルとなります。



Violation	Occurrences	Suggestions
Threat Campaign detected	1	None

Request Details	Basic	All Details
Geolocation	N/A	
Source IP Address	10.1.10.4:49844	
Session ID	3fdde982130c67f	
Microservice	N/A	
Time	2019-02-20 04:36:59	
Violation Rating	5	Request is most likely a threat
Attack Types	N/A	

Request actual size: 1435 bytes.

```
GET /path HTTP/1.1
Accept-Encoding: identity
Connection: close
Content-Type: %({_#_='multipart/form-data').(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).({_#_memberAccess?({_#_memberAccess=#dm}):((#container=#context['com.opensymphony.xwork2.ActionContext.container']).(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).(#ognlUtil
```

上記のイベントログを見ると、Violation Rating が“5: Request is most likely a threat”となっていることが分かります。これは Threat Campaigns シグネチャが実際の攻撃を元に作成されており、ほぼフォールスポジティブではないことを表しています。

## 9.6. 最終的なチューニング

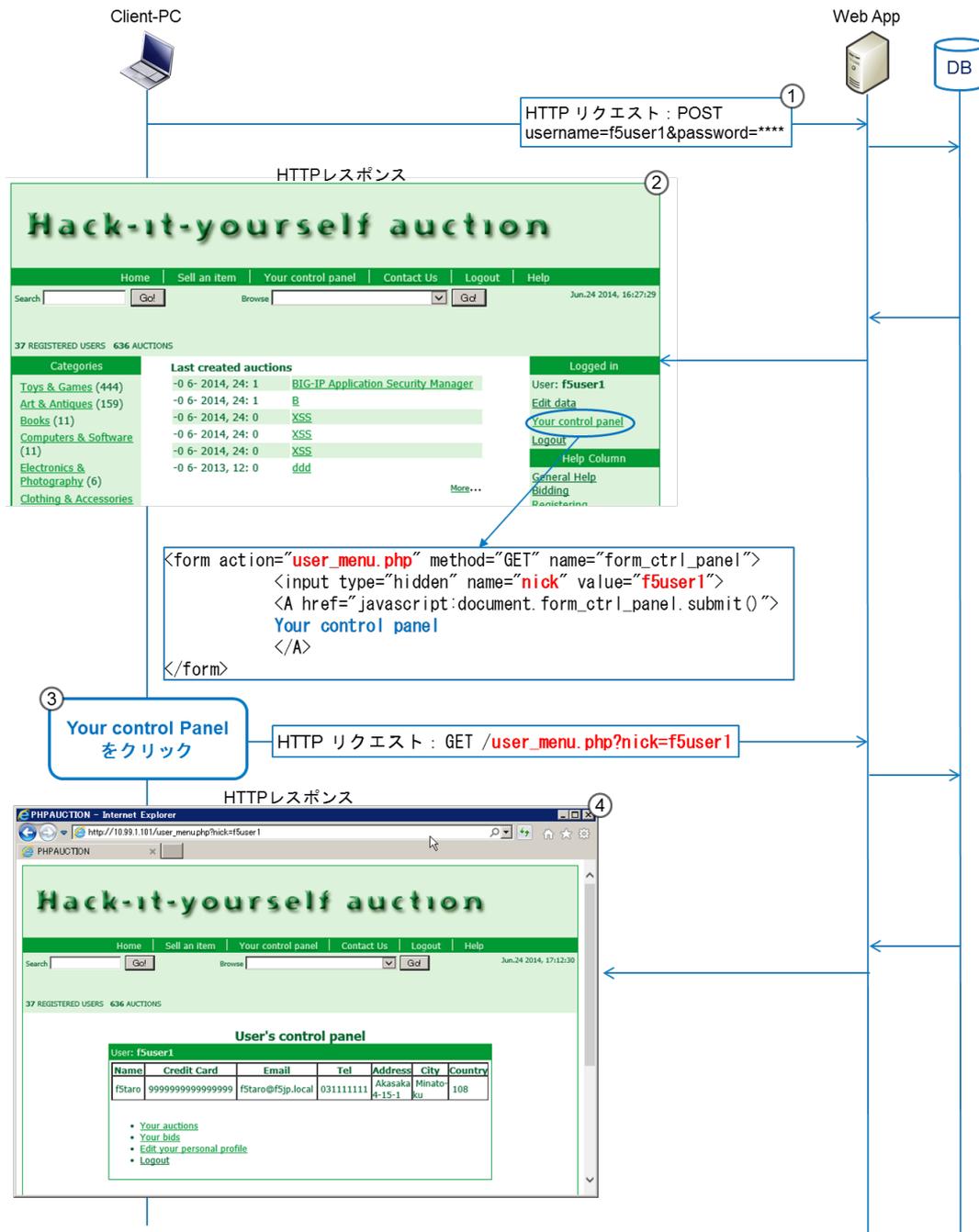
[Step1]～[Step4]では防御できない攻撃への対策として、2つの攻撃とその設定をサンプルとして、解説します。

## 9.7. 例：パラメータ・タンパリング

パラメータ・タンパリング攻撃とは、サーバから提供されたパラメータ値を改ざんすることで、Webアプリケーションが期待しない動作を引き起こすような攻撃です。以下に、この攻撃例を示します。

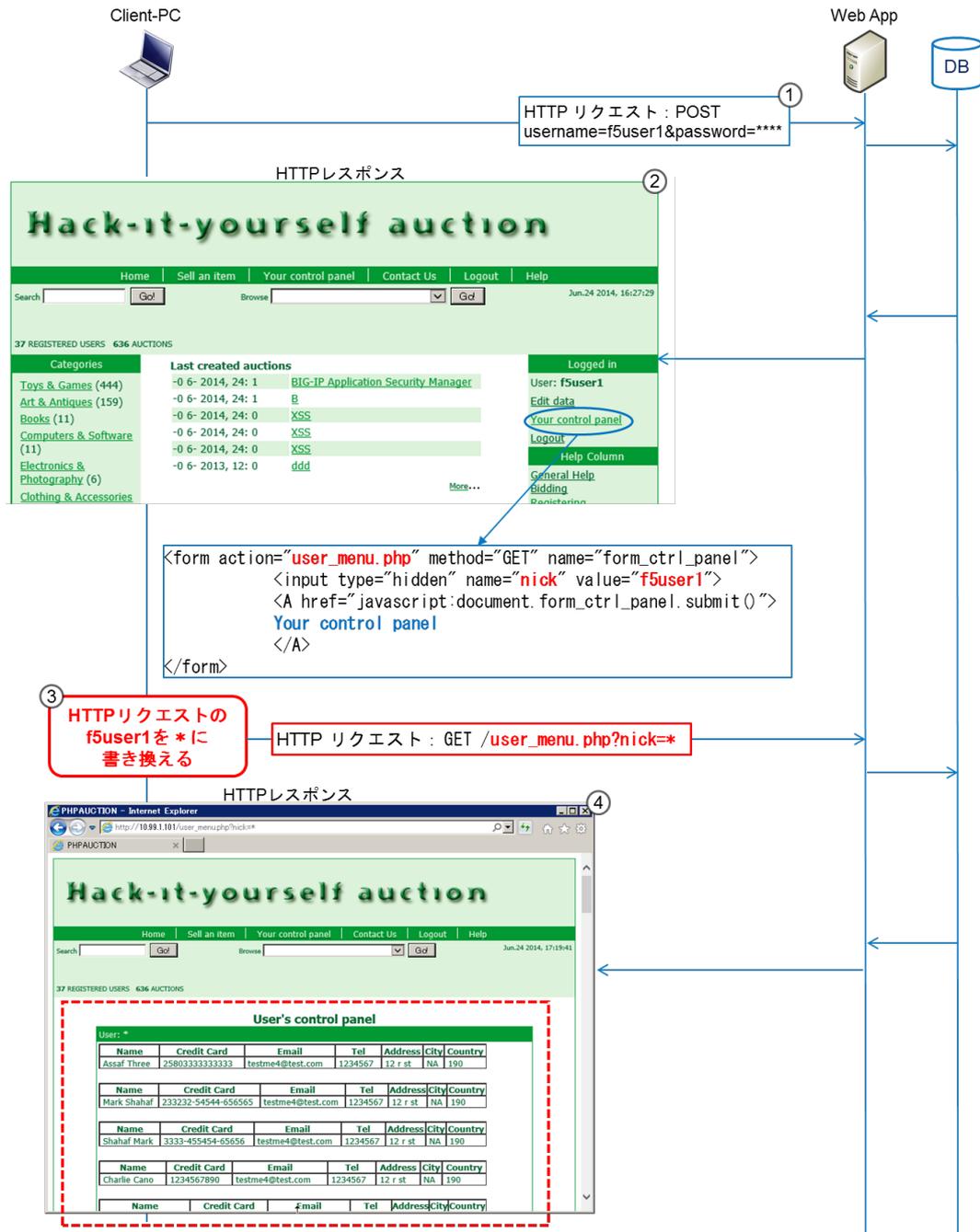
### 9.7.1. 攻撃例

#### (1) 正常な動作



- ① ユーザ名: f5userX でログイン。
- ② HTTP レスポンスページの「your control Panel」は、図中のような HTML と JavaScript で構成されている。
- ③ この「your control Panel」をクリックすると、「/user\_menu.php?nick=f5userX」の GET リクエストが送信される。
- ④ f5userX の情報が記載されたページが HTTP レスポンスとして返される。

## (2) パラメータ・タンパリング攻撃



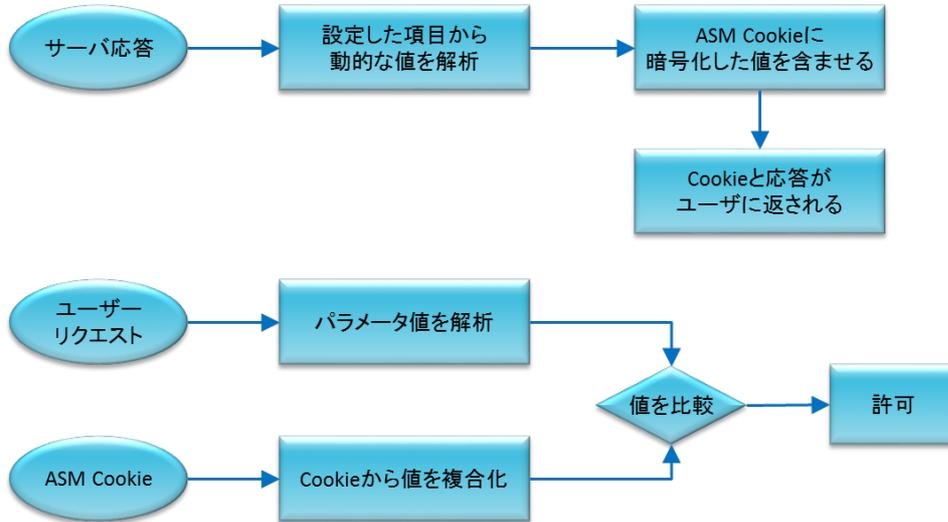
- ① ユーザ名: f5userX でログイン。
- ② HTTP レスポンスページの「your control Panel」は、図中のような HTML と JavaScript で構成されている。
- ③ この「your control Panel」をクリックすると、「/user\_menu.php?nick=f5userX」となるところを、攻撃者は f5userX を \* に書き換えて送信。
- ④ 全ユーザの情報が記載されたページが HTTP レスポンスとして返されてしまう(ようなことがあり得る)。

次に進む前に、Fiddler2 を使って本攻撃を実施してみてください。

### 9.7.2. パラメータ・タンパリングの防御方法

この攻撃に対しては、Web アプリケーション側から提供されたパラメータ値が、後の HTTP リクエストで改ざんされていないかどうかをチェックすることで防御できます。

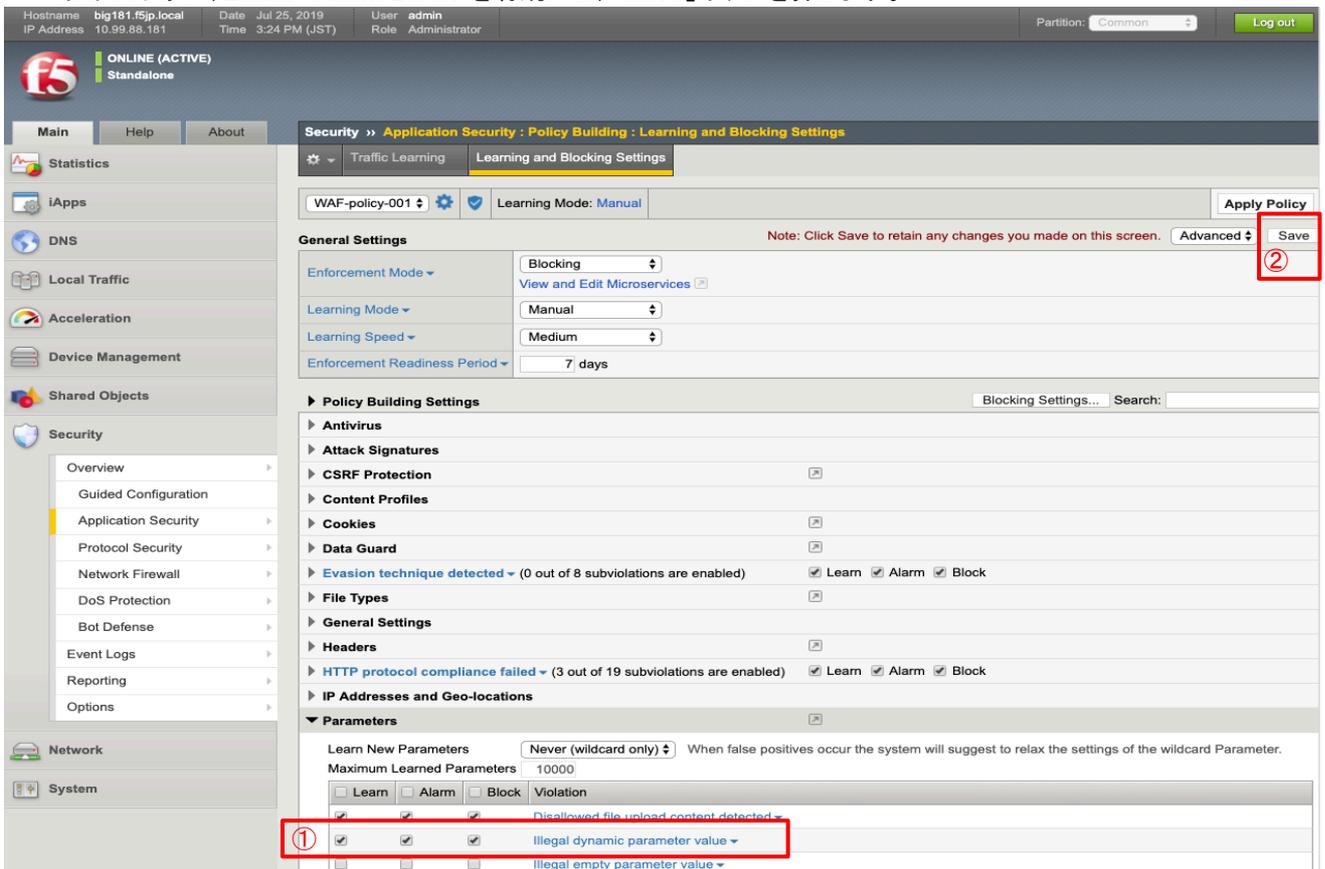
Adv.WAF は以下のようなフローにて、改ざんがなされていないかのチェックを行います。



### 9.7.3. パラメータ・タンパリング対策の設定

このようなパラメータ・タンパリング攻撃を防ぐ Adv.WAF の設定を示します。

- (1) 「Security」→「Application Security」→「Policy Building」→「Learning and Blocking Settings」で表示された画面で、「Parameters」カテゴリの「illegal dynamic parameter value」を探します。以下のように、Learn / Alarm/Block を有効にし、「Save」ボタンを押します。

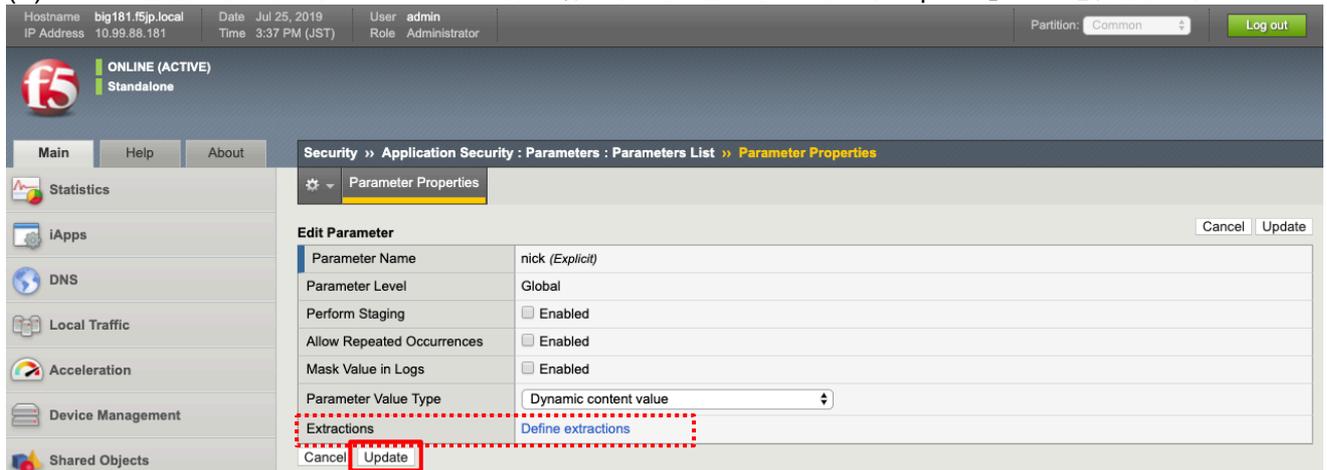


- (2) 「Security」→「Application Security」→「Parameters」→「Parameters List」で表示された右側の「Create」ボタンで現れた以下の画面で、以下のように設定します。

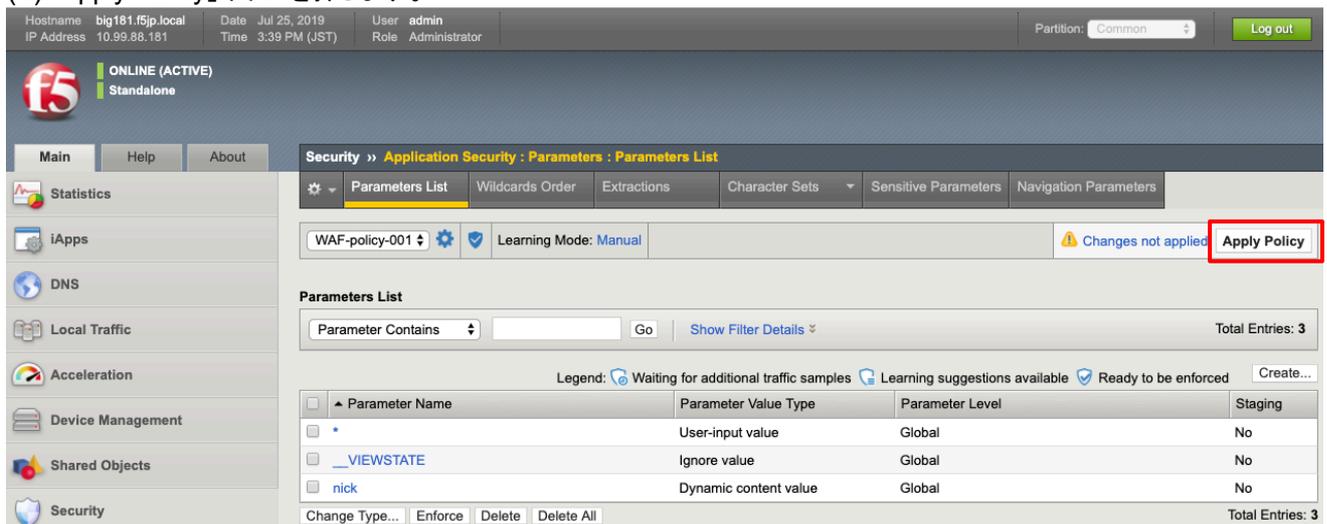
- (3) この動的パラメータ (nick)と関連するファイルタイプ(または URL)の指定を促す画面が出ます。「OK」を押します。

- (4) 本ガイドでは php ファイルタイプと関連付けることとします。以下のように設定します。

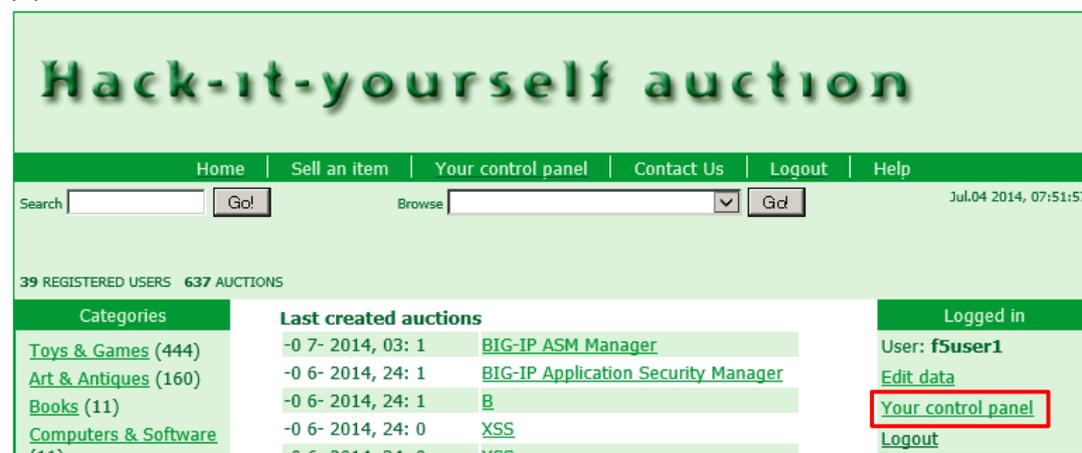
(5) 以下の画面に戻ります。Extractions の行が増えていることが分かります。「Update」ボタンを押します。



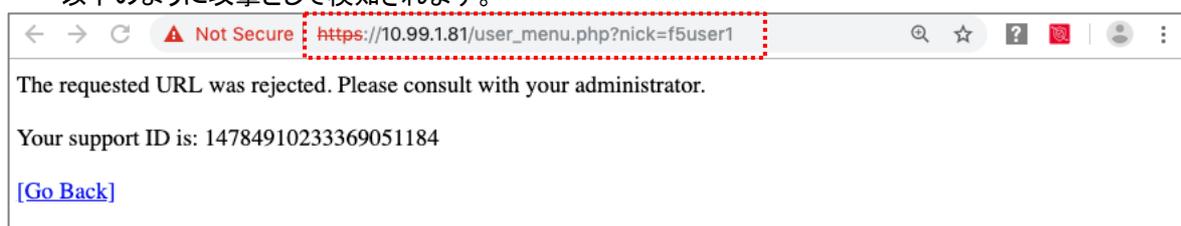
(6) 「Apply Policy」ボタンを押します。



(7) クライアントのブラウザで、正当なユーザ (f5userX) でログインします。



(8) 「Your Control Panel」をクリックし、以下のように「nick=\*」に書き換えて、Enter します。以下のように攻撃として検知されます。



(9) 「Security」→「Event Logs」→「Application」→「Requests」でログを確認します。  
「Parameter Tampering」として検知されています。

The screenshot displays the Fortinet Security Manager interface. The top navigation bar shows 'Security >> Event Logs : Application : Requests'. A sidebar on the left contains various system management options. The main content area shows a list of requests, with one entry for '[HTTPS] /user\_menu.php' selected. The details pane for this request shows a 'Triggered Violations' section with one violation: 'Illegal dynamic parameter value'. The 'Request Details' section shows the source IP as 10.99.88.90 and the attack type as 'Parameter Tampering'. The 'Request' section shows the actual request body, including the query string 'nick=f5user1'.

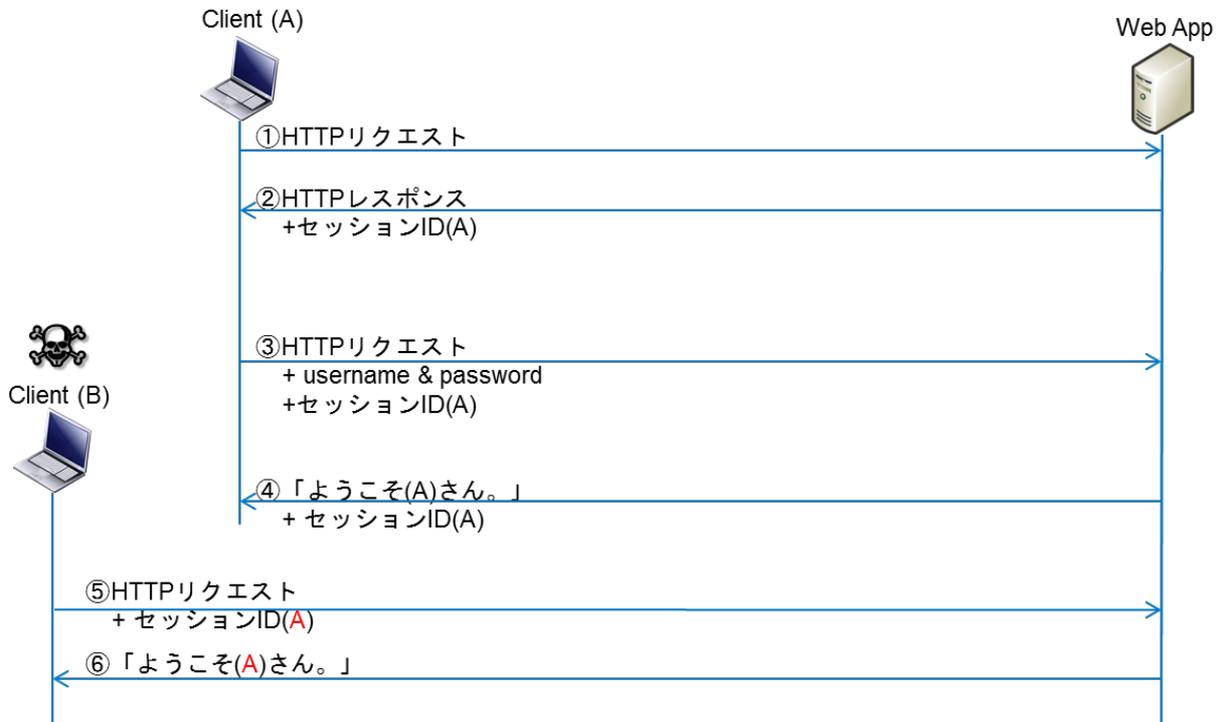
(10) 「Illegal dynamic parameter value」をクリックすると、以下の画面が現れます。  
パラメータ:「nick」で検知していることが分かります。

Parameter Location	Query String
Parameter Level	Global
Parameter Name	nick
Parameter Value	f5user1
Applied Blocking Settings	<span>Block</span> <span>Alarm</span> <span>Learn</span>

## 9.8. 例:セッションハイジャック

他人のセッション ID(Cookie)を模倣することで、そのユーザとしてログインする、という攻撃です。以下に、この攻撃例を示します。

### 9.8.1. 攻撃例

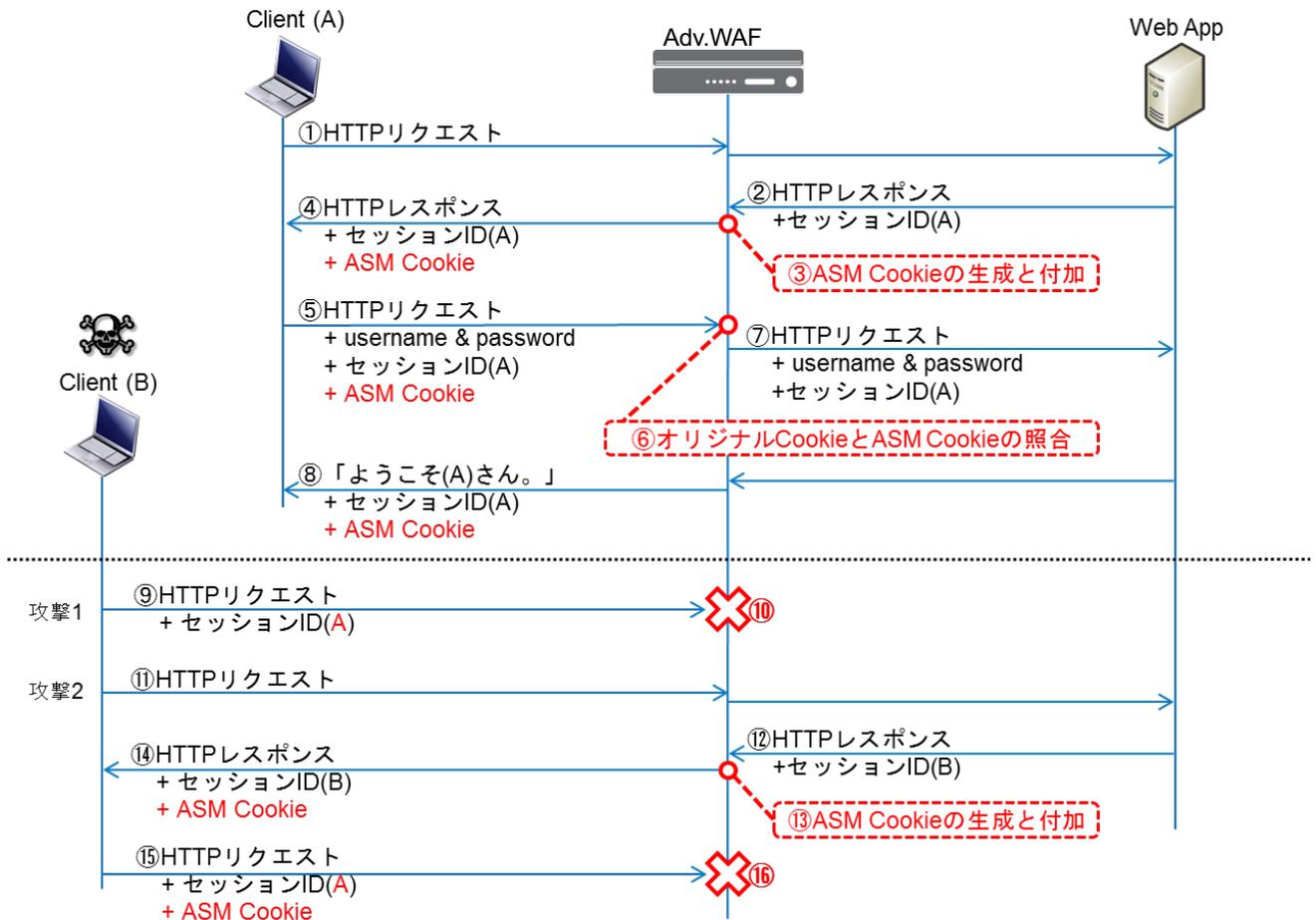


- ① Client(A)が Web App に HTTP リクエストを送る。
- ② Web App はセッション ID(A)をつけて、認証フォーム画面の HTTP レスポンスを送る。
- ③ Client(A)は、ユーザ名とパスワードを入力=POST リクエストを送る。
- ④ Client(A)用の画面が表示される。
- ⑤ Client(B)は、何らかの方法でセッション ID(A)を生成して、HTTP リクエストを送る。
- ⑥ ログイン情報を入力することなく、Client(A)の画面を見ることができる。

## 9.8.2. セッションハイジャックの防御方法

Adv.WAF では、Web アプリケーションから払い出されたセッション ID(Cookie)のハッシュ値を計算し、それを Cookie (ASM Cookie) として付与します。

クライアントから戻ってきたそのセッション ID(Cookie)のハッシュ値を計算し、ASM Cookie 値と同じであれば、改ざんされていない、と判断します。



- ① Client(A)が Web App に HTTP リクエストを送る。
- ② Web App はセッション ID(A)をつけて、認証フォーム画面の HTTP レスポンスを送る。
- ③ Adv.WAF は、セッション ID(A)のハッシュ値を計算。それを ASM Cookie として HTTP レスポンスに付与する。
- ④ Client(A)は、ASM Cookie が付与された HTTP レスポンスを受け取る。
- ⑤ Client(A)は、ユーザ名とパスワードを入力=POST リクエストを送る。
- ⑥ Adv.WAF は、セッション ID(A)のハッシュ値を計算。それを ASM Cookie 値と比較する。
- ⑦ 比較結果が同じであれば、改ざんされていないと判断し、Web App へ HTTP リクエストを転送する。
- ⑧ Client(A)用の画面が表示される。
- ⑨ [攻撃 1] Client(B)は、何らかの方法でセッション ID(A)を生成して、HTTP リクエストを送る。
- ⑩ ASM Cookie 値を持たないため、Adv.WAF で拒否される。
- ⑪ [攻撃 2] Client(B)が HTTP リクエストを送る。
- ⑫ Web App はセッション ID(B)をつけて、認証フォーム画面の HTTP レスポンスを送る。
- ⑬ Adv.WAF は、セッション ID(B)のハッシュ値を計算。それを ASM Cookie として HTTP レスポンスに付与する。
- ⑭ Client(B)は、ASM Cookie が付与された HTTP レスポンスを受け取る。
- ⑮ Client(B)は、セッション ID(B)をセッション ID(A)に書き換えて、HTTP リクエストを送る。
- ⑯ セッション ID(A)のハッシュ値と ASM Cookie 値が異なるため、ブロックされる。

### 9.8.3. セッションハイジャック対策の設定

このようなセッションハイジャック攻撃を防御する設定を示します。

- (1) 「Security」→「Application Security」→「Policy Building」→「Learning and Blocking Settings」で表示された画面で、「Learn New Cookies」にて「Selective」を選択し、「Learn and enforce new unmodified cookies」と「Modified domain cookie」の Learn / Alarm/Block を有効にし、「Save」ボタンを押します。

Hostname: big181.f5jp.local | Date: Jul 25, 2019 | User: admin | IP Address: 10.99.88.181 | Time: 3:52 PM (JST) | Role: Administrator | Partition: Common | Log out

ONLINE (ACTIVE) Standalone

Main | Help | About | Security >> Application Security : Policy Building : Learning and Blocking Settings

Traffic Learning | Learning and Blocking Settings

WAF-policy-001 | Learning Mode: Manual | Apply Policy

Note: Click Save to retain any changes you made on this screen. Advanced Save ④

**General Settings**

Enforcement Mode: Blocking | View and Edit Microservices

Learning Mode: Manual

Learning Speed: Medium

Enforcement Readiness Period: 7 days

**Policy Building Settings** | Blocking Settings... Search:

Antivirus

Attack Signatures

CSRF Protection

Content Profiles

**Cookies**

① Learn New Cookies: Selective | When false positives occur, the system will add/suggest to add an explicit Cookie with relaxed settings that avoid the false positive.

Maximum Learned Cookies: 100

②  Learn and enforce new unmodified cookies

	Learn	Alarm	Block	Violation
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Cookie not RFC-compliant
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Expired timestamp
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Illegal cookie length
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Modified ASM cookie
③ <input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Modified domain cookie(s)

Collapse many common Cookies into one wildcard Cookie after 10 occurrences

- (2) Apply Policy」ボタンを押します。

Hostname: big181.f5jp.local | Date: Jul 25, 2019 | User: admin | IP Address: 10.99.88.181 | Time: 4:49 PM (JST) | Role: Administrator | Partition: Common | Log out

ONLINE (ACTIVE) Standalone

Main | Help | About | Security >> Application Security : Policy Building : Learning and Blocking Settings

Traffic Learning | Learning and Blocking Settings

WAF-policy-001 | Learning Mode: Manual | Changes not applied | Apply Policy

**General Settings** | Advanced Save

- (3) クライアントのブラウザで、ユーザ (f5userX) ログインします。

- (4) 「Security」→「Application Security」→「Policy Building」→「Traffic Learning」で表示された「Enforce Cookie」をクリックすると、以下の画面が現れます。  
「SESSION」が、この Web アプリケーションのセッション ID(Cookie)です。

The screenshot shows the FortiGate web interface. The main content area displays a suggestion for 'Enforce Cookie' with a 5% progress bar. The suggestion is highlighted with a red box. Below the suggestion, the 'Matched Cookie: SESSION' is also highlighted with a red box. The interface shows a list of sample requests and a detailed view of a request for [HTTPS] /user\_login.php. The request details include Geolocation (N/A), Time (2019-07-25 17:55:43), Source IP Address (10.99.88.90:58904), Session ID (683dc34ec2b33949), and Microservice (N/A). The request body shows a GET request for /user\_login.php? HTTP/1.1 with various headers and a cookie value.

- (5) 「Enforce Cookie」にチェックを入れ、「Accept Suggestion」ボタンを押します。

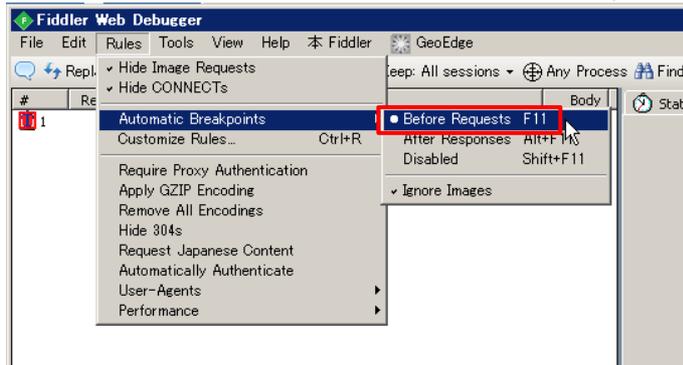
The screenshot shows the FortiGate web interface after the 'Enforce Cookie' suggestion has been accepted. The 'Accept Suggestion' button is highlighted with a red box. The suggestion is now marked as 'Accepted' and the policy is being enforced. The interface shows the same list of sample requests and a detailed view of a request for [HTTPS] /user\_login.php. The request details include Geolocation (N/A), Time (2019-07-25 17:55:43), Source IP Address (10.99.88.90:58904), Session ID (683dc34ec2b33949), and Microservice (N/A). The request body shows a GET request for /user\_login.php? HTTP/1.1 with various headers and a cookie value.

(6) 「Apply Policy」ボタンを押します。

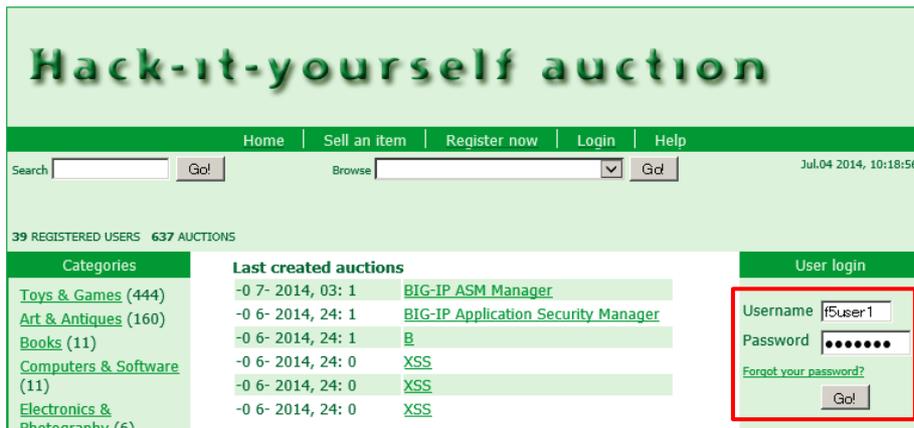


(7) クライアントのブラウザから攻撃を模擬するために、Fiddler2 を利用します。

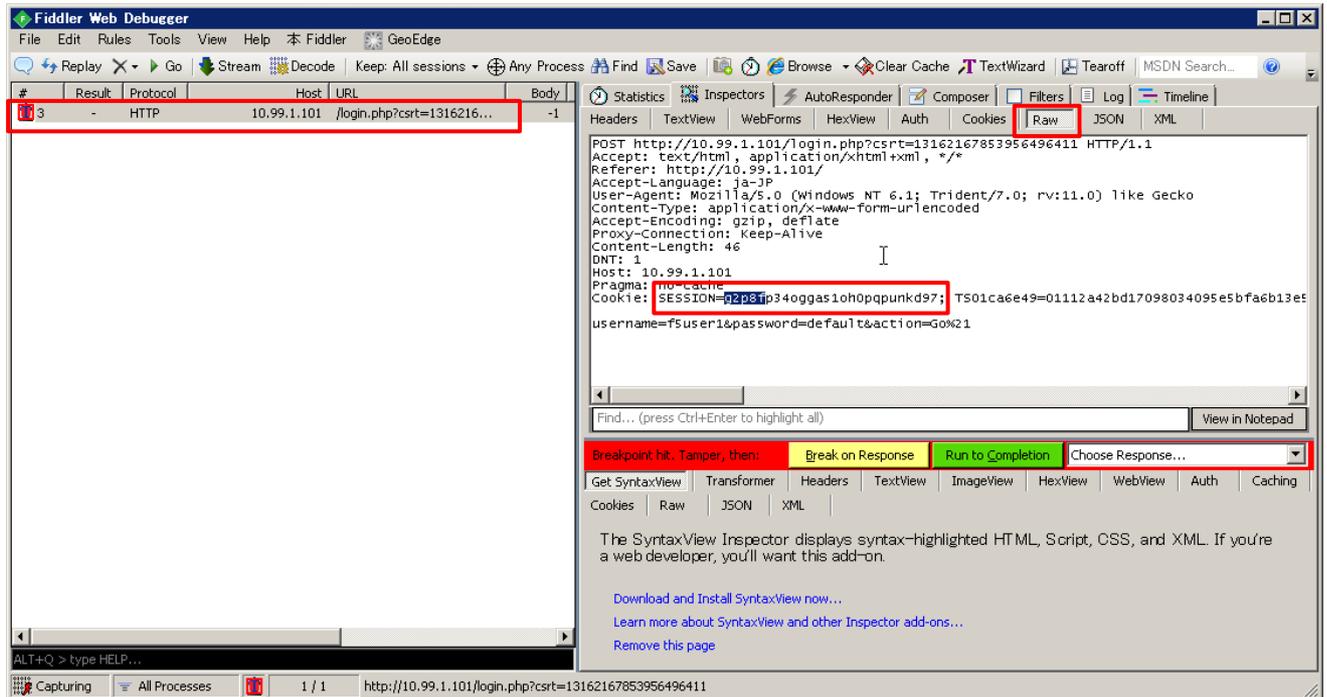
Fiddler2 を起動し、「Rules」→「Automatic Breakpoints」→「Before Requests」を選択(有効に)します。



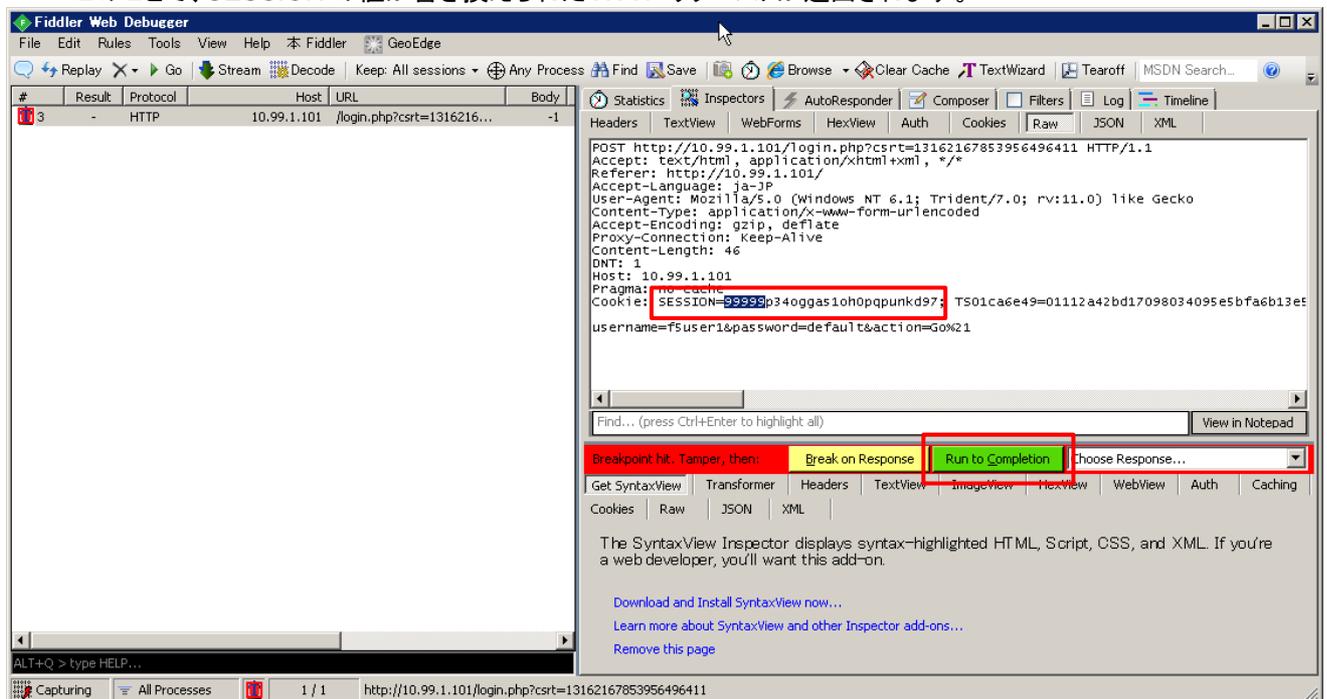
(8) ブラウザで http の Virtual Server にアクセスし、正当なユーザ(f5userX)とパスワードを入力し、「Go!」ボタンを押します。



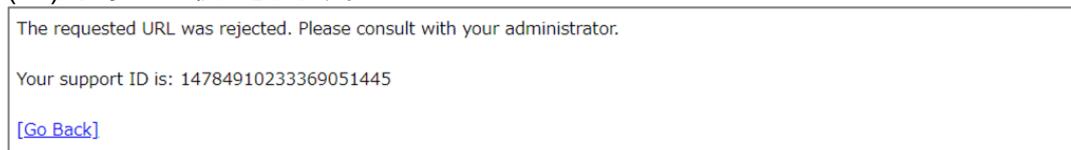
- (9) Fiddler2 がこの HTTP リクエストをインターセプトするので、先に進みません。  
Fiddler2 の左画面でその HTTP リクエストを選択し、右画面で「Inspectors」→「Raw」タブを選択します。  
「Cookie: SESSION=」を見つけます。



- (10) ここでは、SESSION 値の先頭五文字を、「99999」に書き換えてみました。  
「Run to Completion」ボタンを押します。  
このことで、SESSION の値が書き換えられた HTTP リクエストが送出されます。



- (11) 攻撃として検知されます。



Fiddler2 を終了するか、「Rules」→「Automatic Breakpoints」→「Disabled」を選択（無効に）します。

(12) 「Security」→「Event Logs」→「Application」→「Requests」でログを確認します。Modified domain cookie が検知されていることが分かります。

The screenshot shows the Fortinet Security Manager interface. The top navigation bar includes 'Main', 'Help', and 'About'. The main content area is titled 'Security >> Event Logs : Application : Requests'. A list of requests is shown, with one entry for '[HTTP] /login.php' from IP 10.99.4.18 at 18:50:55. This entry has a severity of 3 and a status of N/A. A red box highlights the 'Modified domain cookie(s)' violation in the 'Triggered Violations' section. The 'Occurrences' column for this violation shows '1' and the word 'クリック' (Click) is written next to it. Below the violation, the 'Request Details' section shows the source IP, session ID, and other request metadata. The 'Decoded Request' section shows the raw HTTP request, including headers and the body with a session cookie value.

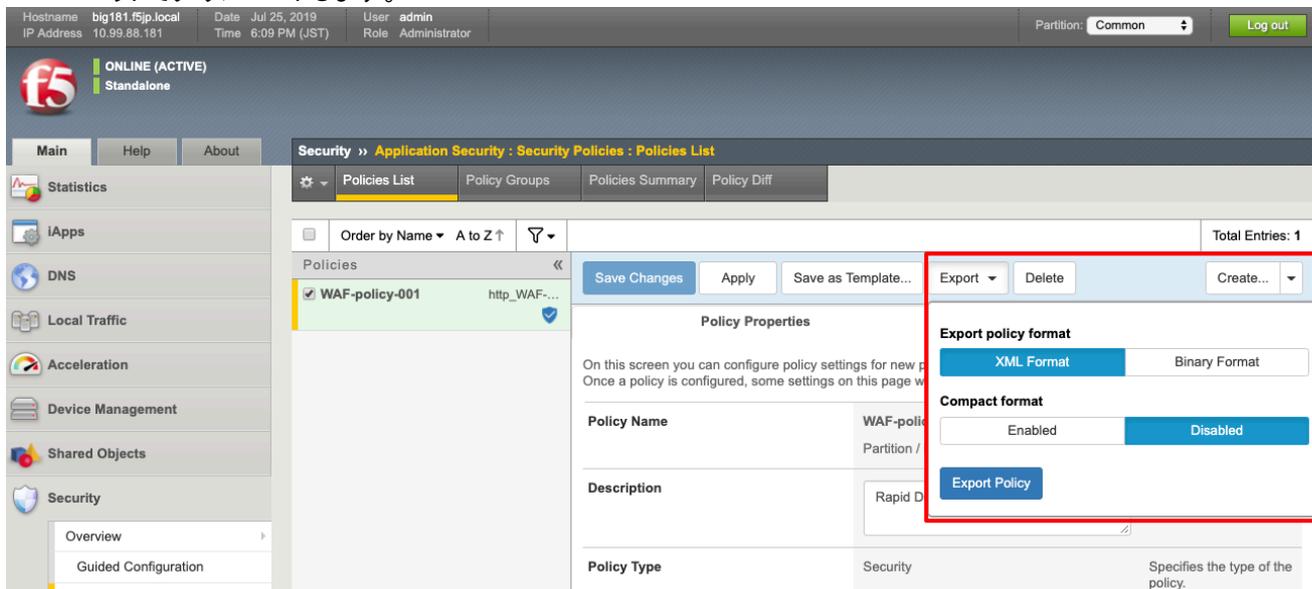
(13) Occurrences をクリックすると、以下のように SESSION の値がどのような値に書き換えられたか表示されます。

Cookie Name	SESSION
Cookie Value	99999kfakdsumrih0t60oapunh1
Reason	Modified Cookie
Applied Blocking Settings	<span>Block</span> <span>Alarm</span> <span>Learn</span>

## 10. Adv.WAF ポリシーの保存

作成したポリシーを保存することが可能です。また、保存したポリシーを import することも可能です。

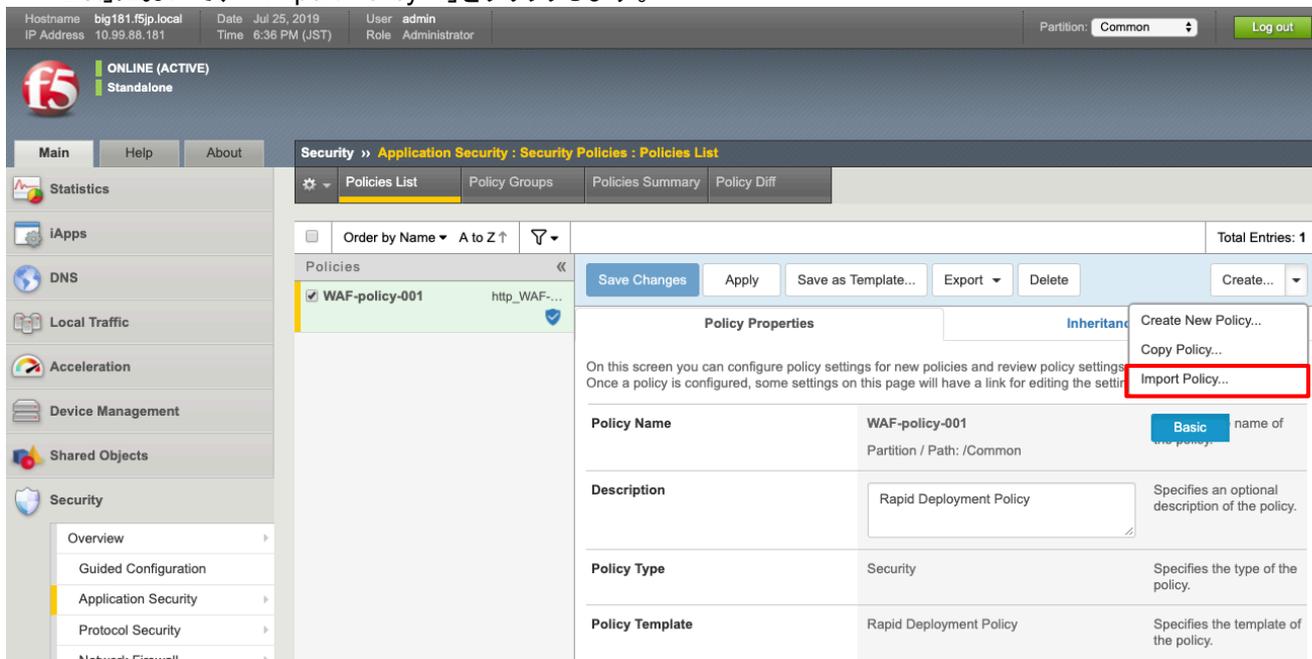
- (1) はじめに、作成したポリシーを保存します。「Security」→「Application Security」→「Security Policies」→「Policies List」をクリックすると以下の画面が表示されます。「Export」→「Export Policy」をクリックし、XML フォーマットでダウンロードします。



- (2) Downloads フォルダに以下のようにファイルが保存されています。

Name	Size	Kind	Date Added
Common_WAF-policy-001_2019-7-25_18-24-9_big181.f5jp.local.xml	906 KB	XML Document	Today 18:24

- (3) 次に、保存したポリシーを import します。「Security」→「Application Security」→「Security Policies」→「Policies List」において、「Import Policy...」をクリックします。



(4) 「Select File」をクリックします。

Hostname big181.f5jp.local Date Jul 25, 2019 User admin  
IP Address 10.99.88.181 Time 6:37 PM (JST) Role Administrator Partition: Common Log out

ONLINE (ACTIVE)  
Standalone

Main Help About

Security » Application Security : Security Policies : Policies List

Statistics Policies List Policy Groups Policies Summary Policy Diff

Import Policy Cancel

On this screen you configure basic settings of policy you are going to import.  
Note: Depending on the settings you configure, you may see only some of the screen elements described here.

Imported Policy File	Select File	Specifies the policy to import. Click the Browse button and search for it.
Import Target	New Policy Replace Policy	The imported policy file can act as a new policy (New Policy) or replace an existing policy (Replace Policy).
Replaced Policy	WAF-policy-001	Specifies that the policy you are importing will replace the selected policy.

(5) ExportしたポリシーのXMLファイルを選択し、「Import Policy」ボタンを押します。

Hostname big181.f5jp.local Date Jul 25, 2019 User admin  
IP Address 10.99.88.181 Time 6:38 PM (JST) Role Administrator Partition: Common Log out

ONLINE (ACTIVE)  
Standalone

Main Help About

Security » Application Security : Security Policies : Policies List

Statistics Policies List Policy Groups Policies Summary Policy Diff

Import Policy Cancel

On this screen you configure basic settings of policy you are going to import.  
Note: Depending on the settings you configure, you may see only some of the screen elements described here.

Imported Policy File	Select File Common_WAF-policy-001__2019-7-25_18-24-9_big181.f5jp.local.xml	Specifies the policy to import. Click the Browse button and search for it.
Imported Policy Name	WAF-policy-001	Specifies the unique name of the policy.
Imported Policy Type	Security	Specifies the type of the policy.
Imported Application Language	Unicode (utf-8)	Displays the language encoding of the policy that you are importing.
Description		Specifies an optional description of the policy. Type in any helpful details about the policy.
Import Target	New Policy Replace Policy	The imported policy file can act as a new policy (New Policy) or replace an existing policy (Replace Policy).
Replaced Policy	WAF-policy-001	Specifies that the policy you are importing will replace the selected policy. Note: The imported policy will replace your current "WAF-policy-001" policy associated with <a href="#">http_WAF-vs-001</a> , <a href="#">https_WAF-vs-001</a> Virtual Servers

(6) Import が成功すると以下の表示になります。Close ボタンを押します。

Creating a new Policy

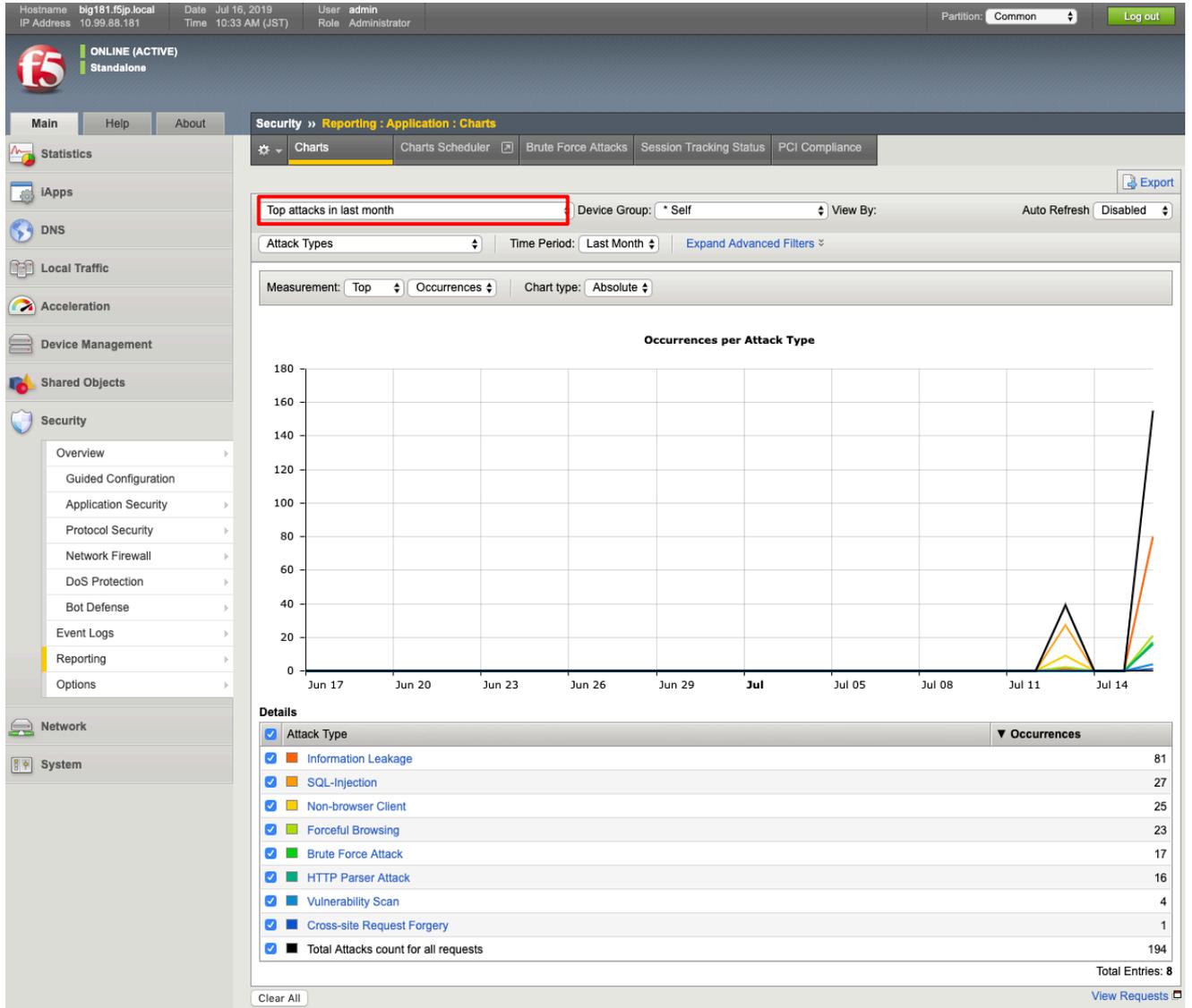
The operation was completed successfully. The security policy name is '/Common/WAF-policy-001'.

Close

## 11. レポーティング

Reporting 機能にて、グラフィカルなレポートを表示することが可能です。

- (1) 「Security」→「Reporting」→「Application」→「Charts」で表示された画面にて確認します。例えば、「Top attackers in last month」を選択すると、1ヶ月分の攻撃が表示されます。



他にも、「Top violations in last month」や「Top blocked URLs」など様々なパターンのレポートを表示可能となっています。

## 12. IP Intelligence の設定

※ F5 ハンズオンでは実施しません。

サブスクリプションライセンスの IP Intelligence を設定することで、悪意ある IP アドレスからの攻撃を Block することが可能です。Application Security 処理の前段で IP アドレスの評価が行われるため、CPU 負荷高騰を和らげる効果があります。WAF と L7DDoS において IP Intelligence を利用することが可能です。インターネットから悪意ある IP アドレスデータベースを取得するため、事前に DNS 設定が必要になります。

(1) 「Security」→「Application Security」→「IP Addresses」→「IP Address Intelligence」をクリックすると以下のように表示されます。

Hostname big181.f5.jp.local Date Jul 16, 2019 User admin  
IP Address 10.99.88.181 Time 10:46 AM (JST) Role Administrator Partition: Common Log out

ONLINE (ACTIVE)  
Standalone

Main Help About

Security >> Application Security : IP Addresses : IP Intelligence

IP Address Exceptions IP Intelligence

WAF-policy-001 Learning Mode: Manual Apply Policy

IP Intelligence Configuration

IP Intelligence  Enabled

Save Restore Defaults

IP Intelligence last updated: 2019-07-16 10:46:22

(2) 「IP Address Intelligence」の Enabled をクリックします。IP Intelligence を設定したいカテゴリをチェックします。

Hostname big181.f5.jp.local Date Jul 16, 2019 User admin  
IP Address 10.99.88.181 Time 10:49 AM (JST) Role Administrator Partition: Common Log out

ONLINE (ACTIVE)  
Standalone

Main Help About

Security >> Application Security : IP Addresses : IP Intelligence

IP Address Exceptions IP Intelligence

WAF-policy-001 Learning Mode: Manual Apply Policy

IP Intelligence Configuration

IP Intelligence  Enabled

IP Address Whitelist IP Address Whitelist is empty

IP Intelligence Categories

Category Name	Alarm	Block
Tor Proxies	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Mobile Threats	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Cloud-based Services	<input type="checkbox"/>	<input type="checkbox"/>
Anonymous Proxy	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Phishing Proxies	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Infected Sources	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Denial of Service	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Scanners	<input type="checkbox"/>	<input type="checkbox"/>
BotNets	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Web Attacks	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Windows Exploits	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Spam Sources	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Save Restore Defaults

IP Intelligence last updated: 2019-07-16 10:46:22

(3) Save ボタンをクリックし、Apply Policy をクリックします。

Hostname big181.f5.jp.local Date Jul 16, 2019 User admin  
IP Address 10.99.88.181 Time 10:50 AM (JST) Role Administrator Partition: Common Log out

ONLINE (ACTIVE)  
Standalone

Main Help About

Security >> Application Security : IP Addresses : IP Intelligence

IP Address Exceptions IP Intelligence

WAF-policy-001 Learning Mode: Manual Apply Policy

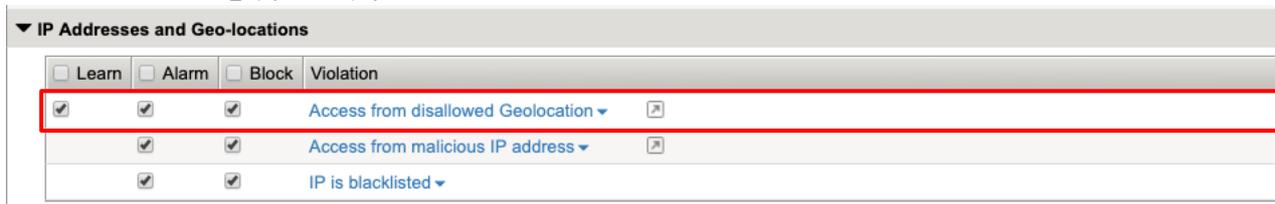
Changes not applied Apply Policy

上記の他、L7DoS Shun と IP Intelligence を組合せることによって、IP Intelligence の IP レピュテーション DB のリストを L7DoS 対策の shun list (Auto-blacklisting) として利用が可能です。

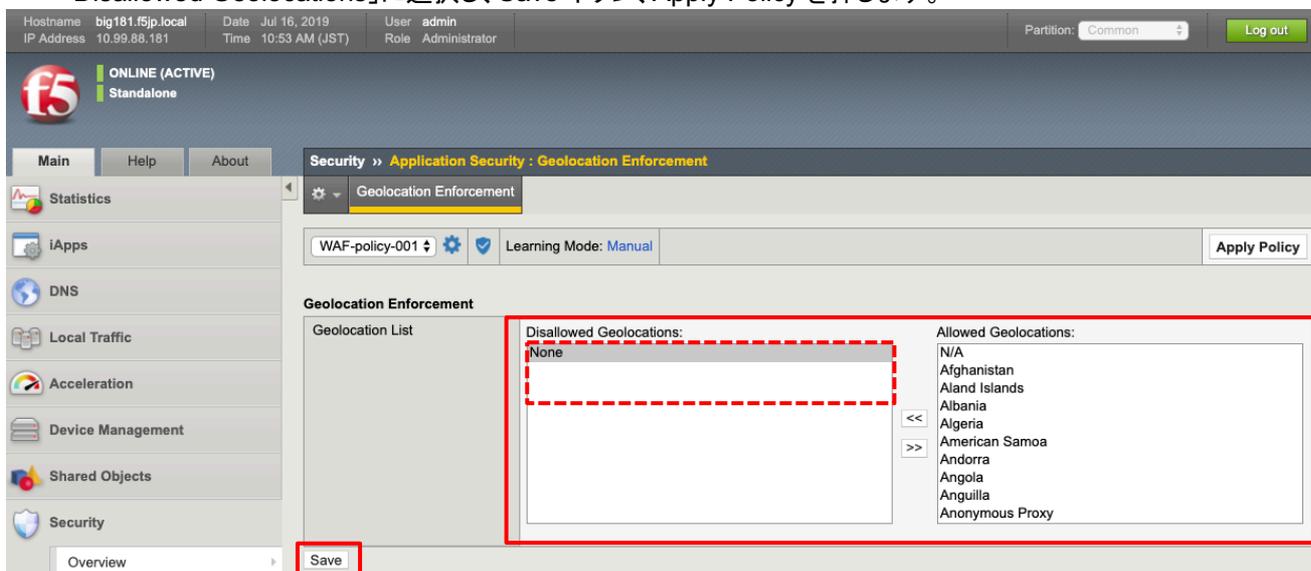
### 13. Geolocation の設定

Geolocation Enforcement の設定を行うことで、接続される予定のない国からの接続をブロックすることができます。

- (1) 「Security」→「Application Security」→「Policy Building」→「Learning and Blocking Settings」の「IP Addresses/Geolocations」において、「Access from disallowed Geolocation」の Learn/Alarm/Block がチェックされていることを確認します。



- (2) 「Security」→「Application Security」→「Geolocation Enforcement」にて、接続する予定のない国を「Disallowed Geolocations」に選択し、Save ボタン、Apply Policy を押します。



## 14. ブロック時のレスポンスページの変更

攻撃をブロックした際にユーザに返されるレスポンスページの内容を変更することが可能です。

(1) 「Security」→「Application Security」→「Policy」→「Response Pages」をクリックすると以下の画面が表示されます。デフォルトでは編集ができません。

The screenshot shows the F5 Security console interface. At the top, it displays system information: Hostname (big181.f5jp.local), Date (Jul 16, 2019), User (admin), and IP Address (10.99.88.181). The main navigation bar includes 'Main', 'Help', and 'About'. The left sidebar contains various system management options like 'Statistics', 'iApps', 'DNS', 'Local Traffic', 'Acceleration', 'Device Management', 'Shared Objects', and 'Security'. The 'Security' section is expanded to show 'Application Security', 'Protocol Security', 'Network Firewall', and 'DoS Protection'. The main content area is titled 'Security >> Application Security : Policy : Response Pages'. It shows the configuration for policy 'WAF-policy-001' in 'Manual' learning mode. A table lists various security features and their response types. The 'Response Type' dropdown is set to 'Default Response'. The 'Response Headers' and 'Response Body' sections are visible, showing a default rejection message.

(2) Response Type の中から Custom Response を選択します。

This screenshot shows the same configuration page as above, but with the 'Response Type' dropdown menu open and 'Custom Response' selected. The 'Response Headers' and 'Response Body' sections are visible, showing a default rejection message. The 'Response Type' dropdown is highlighted with a red box.

上記から Header や Body の内容を変更することが可能です。

## 15. シグネチャの運用

シグネチャの追加、変更、更新などについて記載します。

### 15.1. シグネチャセットとは

Adv.WAF でのシグネチャの割当ては、「シグネチャセット」という単位での割付を行います。そのシグネチャセットとはどういうものを説明します。

#### 15.1.1. シグネチャの属性

シグネチャセットを理解するには、まずシグネチャの属性について知る必要があります。

- (1) 「Security」→「Options」→「Application Security」→「Attack Signatures」→「Attack Signature List」で表示された一つのシグネチャをクリックして現れた画面で、Signature Name をクリックします。各シグネチャは全て、以下のような属性を持っています。

Security » Options : Application Security : Attack Signatures : Attack Signature List » Attack Signature Properties

Attack Signature Properties

Signature Properties	
Name	SQL-INJ expressions like "" or 1 --"
ID	200002419
Signature Type	Request
Signature Scope	Parameter, Cookie, XML, JSON, GWT, Plain Text
Attack Type	SQL-Injection
Systems	General Database
Accuracy	Low
Risk	High
User-defined	No
Revision	2
Last Updated	03/09/2014
Documentation	<a href="#">View</a>
References	<a href="http://www.owasp.org/index.php/SQL_injection">www.owasp.org/index.php/SQL_injection</a> <a href="http://www.webappsec.org/projects/threat/classes/sql_injection.shtml">www.webappsec.org/projects/threat/classes/sql_injection.shtml</a>

Cancel

Security » Options : Application Security : Attack Signatures : Attack Signature List » Attack Signature Properties

Attack Signature Properties

Signature Properties	
Name	SQL-INJ expressions like "or 1=1" (6) (Parameter)
ID	200002476
Signature Type	Request ①
Signature Scope	Parameter, Cookie, XML, JSON, GWT, Plain Text
Attack Type	SQL-Injection ②
Systems	General Database ③
Accuracy	High ④
Risk	High ⑤
User-defined	No ⑥
Revision	1
Last Updated	06/15/2017 ⑦
Documentation	<a href="#">View</a>
References	URL: <a href="http://www.owasp.org/index.php/SQL_injection">www.owasp.org/index.php/SQL_injection</a>

Cancel

この属性のうち、上記①～⑦の値のいずれか(またはその組合せ)で絞込みした、複数のシグネチャのグループをシグネチャセットと呼びます。

## (2) シグネチャセットの例: Generic Detection Signatures

ここでは、デフォルトで割当てられるシグネチャセット: Generic Detection Signatures を見てみます。「Security」→「Options」→「Application Security」→「Attack Signatures」→「Attack Signature Sets」で表示された複数のシグネチャセットの中から、「Generic Detection Signatures」を選びます。

Signatures Filter を見ると、Attack Type (上図の②) で絞り込みがなされたシグネチャセットであることが分かります。

The screenshot shows the configuration page for 'SQL Injection Signatures'. The 'Signatures Filter' section is highlighted with a red box, showing 'Attack Type' set to 'SQL-Injection'. A red annotation 'Attack Type で絞り込まれたグループ' points to this value. The 'Signatures' list includes: Blind NoSQL Injection Attempt (Header), Blind NoSQL Injection Attempt (Parameter), Joomla SQL Injection Probe, NoSQL Injection / \_active\_tasks (Header), and NoSQL Injection / \_active\_tasks (Parameter).

Signature Set Properties	
Name	SQL Injection Signatures
Type	Filter-based
Default Blocking Actions	Learn: Yes Alarm: Yes Block: Yes
Assign To Policy By Default	No

Signatures Filter	
Signature Type	All
Attack Type	SQL-Injection <span style="color: red;">Attack Type で絞り込まれたグループ</span>
Systems	All
Accuracy	All
Risk	All
User-defined	All
Update Date	All

Signatures	
Signatures	Blind NoSQL Injection Attempt (Header) Blind NoSQL Injection Attempt (Parameter) Joomla SQL Injection Probe NoSQL Injection / _active_tasks (Header) NoSQL Injection / _active_tasks (Parameter)

Cancel

このシグネチャセットは、以下3つのような、一般的な攻撃に対するシグネチャに絞り込まれています。

- ① General Database
  - 一般的なデータベースへの攻撃シグネチャ
- ② System Independent
  - 特定のシステムに限定されない攻撃シグネチャ
- ③ Various Systems
  - 特定のシステムまたはコードバージョンに依存していない、一般的な攻撃シグネチャ

よって、守るべき Web アプリケーションが使っているシステム (例: Apache や PHP など) が明確ならば、それらのシグネチャも追加で割当ててを推奨します。

詳細は「K10726: Overview of the attack signature Systems and Attack Type fields」を参照ください。

<http://support.f5.com/csp/article/K10726>

## 15.1.2. シグネチャセットの割り当て方法

ポリシーへのシグネチャ割り当ては、このシグネチャセット単位でしかできません。

- (1) 「Security」→「Application Security」→「Policy Building」→「Learning and Blocking Settings」の「Attack Signatures」において「Change」ボタンを押します。

Policy Building Settings

Blocking Settings... Search:

Antivirus

Attack Signatures

<input type="checkbox"/> Learn	<input type="checkbox"/> Alarm	<input type="checkbox"/> Block	Signature Set Name	Signature Set Category
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	PHP Signatures (High/Medium Accuracy)	User-defined
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	MySQL Signatures (High/Medium Accuracy)	User-defined
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Apache/NCSA HTTP Server Signatures (High/Medium Accuracy)	User-defined
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Generic Detection Signatures (High/Medium Accuracy)	Basic

Auto-Added Signature Accuracy: Medium Accuracy (also includes signatures with high accuracy)

Enable Signature Staging

Updated Signature Enforcement: Retain previous rule enforcement and place updated rule in staging

Note: Newly added signatures are always placed in staging regardless of this setting.

Apply Response Signatures for these File Types

Add

Delete

Change...

- (2) 一覧から必要なセットを選んで、Change を押します。この「Available Signature Sets」の中には、「Basic」、「Attack Type Specific」、「User-defined」の 3 つのカテゴリが存在しています。

Select Policy Attack Signature Sets

Assigned To Security Policy	Signature Set Name	Signature Set Category
<input type="checkbox"/>	All Response Signatures	Basic
<input type="checkbox"/>	All Signatures	Basic
<input type="checkbox"/>	Command Execution Signatures	Attack Type Specific
<input type="checkbox"/>	Cross Site Scripting Signatures	Attack Type Specific
<input type="checkbox"/>	Directory Indexing Signatures	Attack Type Specific
<input type="checkbox"/>	Generic Detection Signatures	Basic
<input type="checkbox"/>	Generic Detection Signatures (High Accuracy)	Basic
<input checked="" type="checkbox"/>	Generic Detection Signatures (High/Medium Accuracy)	Basic
<input type="checkbox"/>	HTTP Response Splitting Signatures	Attack Type Specific
<input type="checkbox"/>	High Accuracy Detection Evasion Signatures	Attack Type Specific
<input type="checkbox"/>	High Accuracy Signatures	Basic
<input type="checkbox"/>	Information Leakage Signatures	Attack Type Specific
<input type="checkbox"/>	Low Accuracy Signatures	Basic
<input type="checkbox"/>	Medium Accuracy Signatures	Basic
<input type="checkbox"/>	OS Command Injection Signatures	Attack Type Specific
<input checked="" type="checkbox"/>	OWA Signatures	Basic
<input type="checkbox"/>	Other Application Attacks Signatures	Attack Type Specific
<input type="checkbox"/>	Path Traversal Signatures	Attack Type Specific
<input type="checkbox"/>	Predictable Resource Location Signatures	Attack Type Specific
<input type="checkbox"/>	Remote File Include Signatures	Attack Type Specific
<input type="checkbox"/>	SQL Injection Signatures	Attack Type Specific
<input type="checkbox"/>	Server Side Code Injection Signatures	Attack Type Specific
<input type="checkbox"/>	WebSphere signatures	Basic
<input type="checkbox"/>	XPath Injection Signatures	Attack Type Specific
<input checked="" type="checkbox"/>	Apache/NCSA HTTP Server Signatures (High/Medium Accuracy)	User-defined
<input checked="" type="checkbox"/>	MySQL Signatures (High/Medium Accuracy)	User-defined
<input checked="" type="checkbox"/>	PHP Signatures (High/Medium Accuracy)	User-defined

Cancel Change

### 15.1.3. 「Basic」シグネチャセット

「Basic」カテゴリには、以下のようなシグネチャセット(一例)が存在します。  
それぞれ、各シグネチャが持ついずれかの属性でグループ化されています。

<b>Signature Set</b>	Generic Detection Signatures	All Signatures	All Response Signatures	OWA Signatures	WebSphere signatures
<b>Signature Type</b>	All	All	Response	All	All
<b>Attack Type</b>	All	All	All	All	All
<b>Systems</b>	General Database System Independent Various systems	All	All	ASP IIS Microsoft Windows Outlook Web Access WebDAV	Apache Apache Tomcat CGI General Database IBM DB2 IIS Java Servlets/JSP Lotus Domino Macromedia ColdFusion Microsoft SQL Server Microsoft Windows MySQL Oracle Other Web Server PHP PostgreSQL Proxy Servers SSI (Server Side Includes) Sybase/ASE System Independent Unix/Linux Various systems XML
<b>Accuracy</b>	All	All	All	All	All
<b>Risk</b>	All	All	All	All	All
<b>User-defined</b>	All	All	All	All	All
<b>Update Date</b>	All	All	All	All	All

### 15.1.4. 「Attack Type Specific」シグネチャセット

攻撃手法が限定されたシグネチャセットです。これらのセットは「Attack Type」で絞込みされています。

<b>Signature Set</b>	Command Execution Signatures	Cross Site Scripting Signatures	Directory Indexing Signatures	...	XXXX Signatures
<b>Signature Type</b>	All	All	All	...	All
<b>Attack Type</b>	Command Execution	Cross Site Scripting (XSS)	Directory Indexing	...	XXXX
<b>Systems</b>	All	All	All	...	All
<b>Accuracy</b>	All	All	All	...	All
<b>Risk</b>	All	All	All	...	All
<b>User-defined</b>	All	All	All	...	All
<b>Update Date</b>	All	All	All	...	All

### 15.1.5. 「User-defined」シグネチャセット

ユーザが設定(組合せ)変更可能なシグネチャセットです。  
いくつかのテンプレートが事前に用意されています。

## 15.2. シグネチャセットの作成

シグネチャセットは自分で作ることもできます。

例えば、「All Signatures」は Request だけでなく Response に対するシグネチャも入っているので、Request だけのシグネチャを作りたい、と仮定します。その例を以下に示します。

- (1) 「Security」→「Options」→「Application Security」→「Attack Signatures」→「Attack Signature Sets」で表示された画面の右上の「Create」ボタンを押すと、以下の画面が現れます。以下のように設定します。

Security >> Options : Application Security : Attack Signatures : Attack Signature Sets >> Create New Signature Set...

**Create Signature Set** Cancel Create

Name: Set-Signature-set-001 名前(任意)

Type: Filter-based

Default Blocking Actions:  Learn  Alarm  Block (affects only newly created policies)

Assign To Policy By Default:  Enabled (affects only newly created policies)

**Signatures Filter**

Signature Type: Request 「Request」を選択

Attack Type: All

Systems

Assigned Systems:

- Operating Systems
  - Unix/Linux
- Web Servers
  - Apache Struts
- Languages, Frameworks and Applications
  - Java Servlets/JSP
  - SSI (Server Side Includes)
- Database Servers
  - MySQL

Available Systems:

- jQuery
- Database Servers
  - CouchDB
  - General Database
  - IBM DB2
  - Microsoft SQL Server
  - MongoDB 必要なカテゴリを選んで「<<」を押す
  - Oracle
  - PostgreSQL
  - Redis

Accuracy: All

Risk: All

User-defined: All

Update Date: All

References: All

**Signatures**

Signatures: `"../namedfork/data" execution attempt (Headers)`  
`"../namedfork/data" execution attempt (Parameter)`  
`"../namedfork/data" execution attempt (URI)`  
`"/bin" execution attempt (Headers)`  
`"/bin" execution attempt (Parameter)`

Cancel Create

- (2) 「Security」→「Application Security」→「Policy Building」→「Learning and Blocking Settings」の「Attack Signatures」において、「Change」ボタンを押し、前項で作成したシグネチャセットを探します。以下のように該当のシグネチャセットを選択して、「Change」ボタンを押します。

Select Policy Attack Signature Sets

Assigned To Security Policy	Signature Set Name	Signature Set Category
<input type="checkbox"/>	All Response Signatures	Basic
<input type="checkbox"/>	All Signatures	Basic
<input type="checkbox"/>	Apache/NCSA HTTP Server Signatures (High/Medium Accuracy)	User-defined
<input type="checkbox"/>	MySQL Signatures (High/Medium Accuracy)	User-defined
<input type="checkbox"/>	PHP Signatures (High/Medium Accuracy)	User-defined
<input checked="" type="checkbox"/>	Set-Signature-set-001	User-defined

Cancel Change

～略

(3) 選択したシグネチャセットが追加されていることを確認して、「Save」ボタン、「Apply Policy」ボタンを押します。

Security » Application Security : Policy Building : Learning and Blocking Settings

Traffic Learning Learning and Blocking Settings

WAF-policy-001 Learning Mode: Manual Apply Policy

Note: Click Save to retain any changes you made on this screen. Advanced Save

**General Settings**

Enforcement Mode  [View and Edit Microservices](#)

Learning Mode

Learning Speed

Enforcement Readiness Period

**Policy Building Settings** Blocking Settings... Search:

**Antivirus**

**Attack Signatures**

<input type="checkbox"/> Learn	<input type="checkbox"/> Alarm	<input type="checkbox"/> Block	Signature Set Name	Signature Set Category
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Set-Signature-set-001	User-defined

Change...

Auto-Added Signature Accuracy

Enable Signature Staging

Updated Signature Enforcement

Note: Newly added signatures are always placed in staging regardless of this setting.

Apply Response Signatures for these File Types

Add

Delete

これで、作成したシグネチャセットの割当ては完了です。

### 15.3. 新しい Signature の更新

F5 から新しい Signature が出た場合、新しい Signature を Update することで新たな攻撃に対応することができます。Signature は定期的に更新されております。以下の記事を参考して下さい。

<https://support.f5.com/csp/article/K8217>

#### 15.3.1. シグネチャが更新された直後の振る舞い

シグネチャが更新された場合に、ステージングモードで運用するか、即座に Learn/Alarm/Block の設定が適用されるかの指定が可能です。

また、既存シグネチャの更新後の振る舞いについての指定も可能です。

- (1) 「Security」→「Application Security」→「Policy Building」→「Learning and Blocking Settings」の「Attack Signatures」で表示された画面で、希望する動作への設定変更を実施します。

Security >> Application Security : Policy Building : Learning and Blocking Settings

WAF-policy-001 Learning Mode: Manual Apply Policy

General Settings Advanced Save

Enforcement Mode Blocking View and Edit Microservices

Learning Mode Manual

Learning Speed Medium

Enforcement Readiness Period 7 days

Policy Building Settings Blocking Settings... Search:

新しく追加されたシグネチャをステージングにするかどうかの設定

Enforcement 状態 (Non-Staging) の既存シグネチャがアップデートされた場合、更新されたシグネチャも Non-Staging とします。

<input type="checkbox"/> Learn	<input type="checkbox"/> Alarm	<input type="checkbox"/> Block	Signature Set Name	Signature Set Category
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Set-Signature-set-001	User-defined

Auto-Added Signature Accuracy Medium Accuracy (also includes signatures with high accuracy)

Enable Signature Staging Enforce updated rule immediately for non-staged signatures

Updated Signature Enforcement  Retain previous rule enforcement and place updated rule in staging

Note: Newly added signatures are always placed in staging regardless of their accuracy.

Apply Response Signatures for these File Types

Add

Delete

Enforcement 状態 (Non-Staging) の既存シグネチャがアップデートされた場合、更新前のシグネチャは Non-Staging のままとし、更新されたシグネチャを Staging とします。  
更新されたシグネチャの Staging 期間が終了した際に、更新前のシグネチャが削除され、更新されたシグネチャが Non-Staging となります。

- (2) 変更後、「Save」、「Apply Policy」を押します。

### 15.3.2. シグネチャ更新の実行

※F5 ハンズオンでは実施しません

- (1) まず、DNS の設定を行います。「System」→「Configuration」→「Device」→「DNS」で表示された画面で、“DNS Lookup Server List”の Address に“10.99.2.218”を入力し、「Add」をクリックし、「Update」をクリックします。

The screenshot shows the F5 configuration interface for DNS settings. The breadcrumb path is System >> Configuration >> Device >> DNS. The left sidebar shows the navigation menu with 'System' > 'Configuration' selected. The main content area is titled 'Properties' and contains three sections: 'DNS Lookup Server List', 'BIND Forwarder Server List', and 'DNS Search Domain List'. In the 'DNS Lookup Server List' section, the 'Address' field contains '10.99.2.218' and the 'Add' button has been clicked, resulting in '10.99.2.218' being added to the list below. The 'Update' button at the bottom of the configuration area is highlighted with a red box.

- (2) 「System」→「Software Management」→「Live Update」で表示された画面で、現状の設定を確認します。以下のように表示されます。

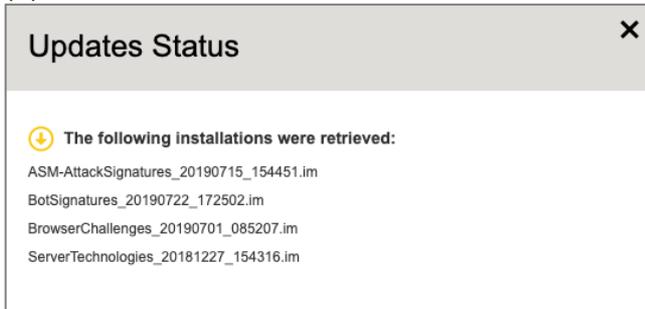
The screenshot shows the F5 Live Update configuration interface. The breadcrumb path is System >> Software Management >> Live Update. The left sidebar shows the navigation menu with 'System' > 'Software Management' > 'Live Update' selected. The main content area is titled 'Live Update' and contains several sections: 'Install All Updates', 'Check for Updates', 'Upload File', and 'Last Checked: 2019-07-25 14:36'. The 'Check for Updates' button is highlighted with a red box. Below this, there is an 'Updates Configuration' section with a 'Save' button. The 'Installation of Automatically Downloaded Updates' section has a 'Disabled' button selected. The 'Installation History' section shows a table with the following data:

Install Date	Update File Name	Status
N/A	ASM-AttackSignatures_20180508_142725.im	Currently Installed

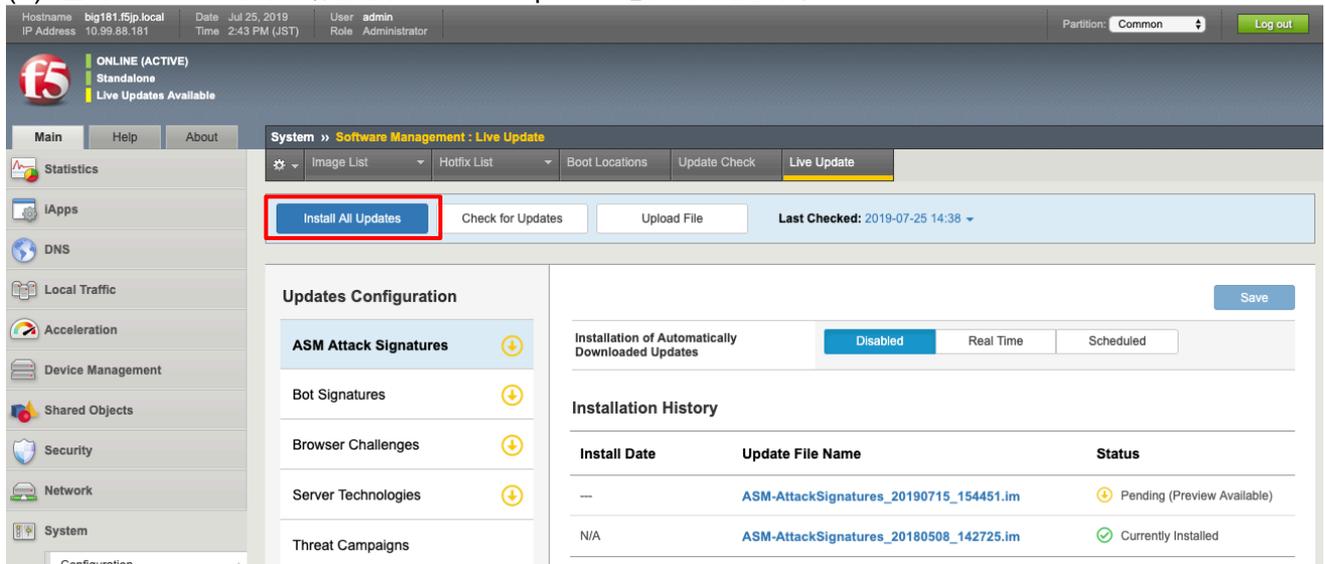
(3) 「Check for Updates」をクリックして、シグネチャ更新の有無を確認します。(チェックには数分かかります。)



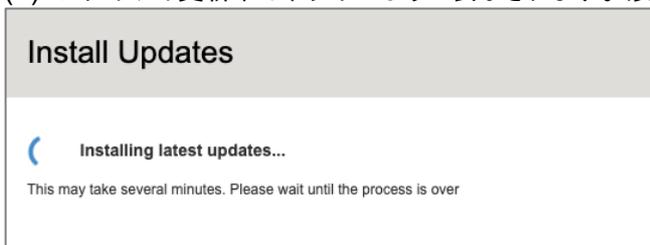
(4) 更新可能なシグネチャがある場合、以下のように表示されます。Xを押し、画面を閉じます。



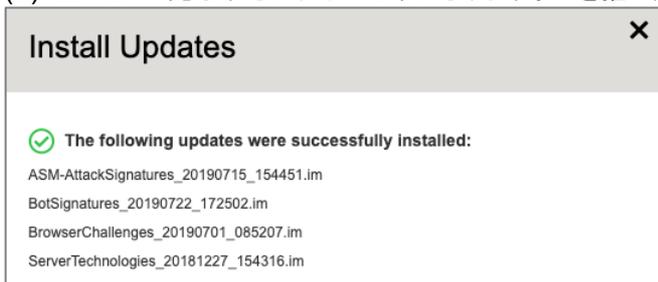
(5) 全てインストールしたい場合は、Install All Updates をクリックします。



(6) シグネチャ更新中は、以下のように表示されます。(更新には数分かかります。)



(7) Install が完了すると以下ようになります。Xを押し、画面を閉じます。



(8) Currently Installed ステータスのシグネチャをクリックします。

Hostname: big181.f5.jp.local | Date: Jul 25, 2019 | User: admin | Role: Administrator | Partition: Common | Log out

ONLINE (ACTIVE) Standalone

System » Software Management : Live Update

Image List | Hotfix List | Boot Locations | Update Check | **Live Update**

Install All Updates | Check for Updates | Upload File | Last Checked: 2019-07-25 14:38

**Updates Configuration**

- ASM Attack Signatures**
- Bot Signatures
- Browser Challenges
- Server Technologies
- Threat Campaigns

Installation of Automatically Downloaded Updates: Disabled | Real Time | Scheduled

**Installation History**

Install Date	Update File Name	Status
2019-07-25 14:48:07	ASM-AttackSignatures_20190715_154451.im	Currently Installed
N/A	ASM-AttackSignatures_20180508_142725.im	Previously Installed

(9) Update された Signature の情報が表示されます。各 Entity をクリックすると、該当するシグネチャー一覧が確認できます。

### Installation Details

Update File Name	ASM-AttackSignatures_20190715_154451.im
Create Date	2019-07-16 00:44:51
Install Date	2019-07-25 14:48:07
Readme	Added more signatures for JSP errors detection in the response (CR111472). Tuning for signature 200002289 (CR111344)... <a href="#">View Full Readme</a>
Status	Currently Installed

### Install Results

- Added Entities (492)
- Modified Entities (1849)
- Deleted Entities (87)

Install | Delete | Cancel

(10) Update がない場合は Install Updates をクリックしても以下のように表示されます。

### Updates Status

No updates found

## 15.4. 更新されたシグネチャのステージング状態確認

更新されたシグネチャがステージングになっているかどうかの確認方法を示します。

(1) 「Security」→「Application Security」→「Attack Signatures」で表示された画面の「Show Filter Details」をクリックします。

The screenshot shows the Fortinet Security Manager web interface. The top navigation bar includes 'Main', 'Help', and 'About'. The left sidebar contains various system management options like 'Statistics', 'iApps', 'DNS', 'Local Traffic', 'Acceleration', 'Device Management', 'Shared Objects', 'Security', 'Network', and 'System'. The main content area is titled 'Security >> Application Security : Attack Signatures'. Below this, there's a 'WAF-policy-001' dropdown and a 'Learning Mode: Manual' setting. A 'Policy Attack Signatures' section shows a dropdown set to 'All signatures' and a 'Go' button. A 'Show Filter Details' button is highlighted with a red box. Below this is a table of attack signatures with columns for Signature Name, Signature ID, Staging, Learn, Alarm, Block, and Enabled. The 'Staging' column for all entries shows 'Yes' with a blue checkmark icon. At the bottom right, it says 'Total Entries: 855' and 'Page 1 of 43'.

(2) 「Staging」で「Enabled」を選択して、「Go」ボタンを押します。

The screenshot shows a dialog box for configuring filter details. It has several dropdown menus: 'References' (All), 'Learn' (All), 'Alarm' (All), 'Block' (All), 'Staging' (Enabled), 'Enabled' (All), and 'Overrides' (On parameters). The 'Staging' dropdown is highlighted with a red box. At the bottom, there are three buttons: 'Go', 'Save As', and 'Reset'. The 'Go' button is also highlighted with a red box.

(3) 以下のように、追加分が「Staging」になっています。

Legend: Waiting for additional traffic samples Learning suggestions available Ready to be enforced

Signature Name	Signature ID	Staging	Learn	Alarm	Block	Enabled
▶ "/..namedfork/data" execution attempt (Headers)	200003067	Yes	Yes	No	No	Yes
▶ "/..namedfork/data" execution attempt (Parameter)	200003066	Yes	Yes	No	No	Yes
▶ "/..namedfork/data" execution attempt (URI)	200003068	Yes	Yes	No	No	Yes
▶ "/bin" execution attempt (Headers)	200003058	Yes	Yes	No	No	Yes
▶ "/bin" execution attempt (Parameter)	200003057	Yes	Yes	No	No	Yes
▶ "/bin" execution attempt (URI)	200003059	Yes	Yes	No	No	Yes
▶ "/email/sendmail.jsp" access	200010004	Yes	Yes	No	No	Yes
▶ "/etc" execution attempt (Headers)	200003055	Yes	Yes	No	No	Yes
▶ "/etc" execution attempt (Parameter)	200003054	Yes	Yes	No	No	Yes
▶ "/etc" execution attempt (URI)	200003056	Yes	Yes	No	No	Yes
▶ "/info/info.jsp" access	200010005	Yes	Yes	No	No	Yes
▶ "/proc/1/cgroup" access (Header)	200010083	Yes	Yes	No	No	Yes
▶ "/proc/1/cgroup" access (Parameter)	200010082	Yes	Yes	No	No	Yes
▶ "/proc/1/cgroup" access (URI)	200010084	Yes	Yes	No	No	Yes
▶ "/proc/self/enviro" execution attempt (Headers)	200003131	Yes	Yes	No	No	Yes
▶ "/proc/self/enviro" execution attempt (Parameter)	200003130	Yes	Yes	No	No	Yes
▶ "/proc/self/enviro" execution attempt (URI)	200003132	Yes	Yes	No	No	Yes
▶ "/usr" execution attempt (Headers)	200003061	Yes	Yes	No	No	Yes
▶ "/usr" execution attempt (Parameter)	200003060	Yes	Yes	No	No	Yes
▶ "/usr" execution attempt (URI)	200003062	Yes	Yes	No	No	Yes

Enforce Change Properties... Total Entries: 797 Page 1 of 40

通常はこのまま Staging モードで運用し、特に問題がないようでしたら、Learn/Alarm/Block モードに戻します。その場合には、もう一度この画面に戻り、同じように表示フィルタを実施します (Staging のみ表示します)。

(4) 「Change Properties」ボタンを押し、以下のように設定します。

### Change Properties Of Policy Attack Signatures

Enable	<span style="border: 1px solid red; padding: 2px;">Don't Change</span>
Perform Staging	<span style="border: 1px solid red; padding: 2px;">No</span>

Cancel Apply Changes to 797 Filtered Attack Signatures

(5) 「Apply Policy」ボタンを押して、適用します。

Hostname: big181.f5jp.local | Date: Jul 16, 2019 | User: admin | IP Address: 10.99.88.181 | Time: 12:33 PM (JST) | Role: Administrator | Partition: Common | Log out

**f5 ONLINE (ACTIVE) Standalone**

Main Help About | Security » Application Security : Attack Signatures

Attack Signatures

WAF-policy-001 Learning Mode: Manual

Changes not applied Apply Policy

## 15.5. CVE 番号によるシグネチャの検索

各シグネチャが CVE に対応しているか確認することが可能です。

- (1) 「Security」→「Options」→「Application Security」→「Attack Signatures」→「Attack Signature List」で表示された画面の「Show Filter Details」をクリックすると、以下のような画面が表示されます。References から CVE を選択し、CVE 番号を入力して「Go」ボタンを押します。

The screenshot shows the 'Attack Signatures List' configuration page in Fortinet's web interface. The 'References' field is set to 'CVE' and '2017-5638'. The 'Go' button is highlighted with a red box. Below the filters, a table lists various signatures, including several for CVE-2017-5638.

Signature Name	Signature ID	Signature Type	User-defined
Code Injection Java (Accessing attributes)	200004156	Request	No
Code Injection Java (Accessing attributes) (#_classResolver)	200004262	Request	No
Code Injection Java (Accessing attributes) (#_keepLastEvaluation)	200004265	Request	No
Code Injection Java (Accessing attributes) (#_lastEvaluation)	200004264	Request	No
Code Injection Java (Accessing attributes) (#_traceEvaluations)	200004263	Request	No
Code Injection Java (Accessing attributes) (#_typeResolver)	200004261	Request	No
Java code injection - Content-Type class github.com/joaoamatos/fjexboss	200004287	Request	No
Java code injection - Content-Type class org.jboss.console.remote.RemoteMBeanInvocation	200004286	Request	No
Java code injection - jexboss webshell	200004288	Request	No
Java code injection com.opensymphony (Header)	200003471	Request	No
Java code injection com.opensymphony (Parameter)	200003470	Request	No
Java code injection com.opensymphony (URI)	200003472	Request	No
JBOSS admin panel URL 3	200010106	Request	No
JSP Expression Language Expression Injection (URI)	200004281	Request	No
Object Graph Navigation Library Expression Injection (URI)	200004280	Request	No

上記の CVE 番号 (CVE-2017-5638) は、Apache Struts 2 の脆弱性に対応したシグネチャー一覧であることを表示しています。Adv.WAF では、1 つの CVE 番号に関連したシグネチャが複数存在していることがあります。

## 16. [ご参考]ログの外部出力の設定

※F5 ハンズオンでは実施しません

ログの出力を Adv.WAF 内部ではなく、外部サーバへのみ行う設定方法を示します。この設定により、Adv.WAF 内部でのログ出力のディスク I/O が発生しないため、その分パフォーマンスは良くなります。

### 16.1. Logging Profile の作成

(1) 「Security」→「Event Logs」→「Logging Profiles」で表示された画面右上の「Create」ボタンを押し、現れた画面で以下のように設定します。

The screenshot shows the 'Create New Logging Profile' configuration page in the F5 Security Management console. The page is divided into several sections:

- Logging Profile Properties:** Profile Name is set to 'WAF-logging-profile'. A red box highlights this field with the annotation '名前(任意)を指定'.
- Application Security:** The 'Application Security' checkbox is checked. A red box highlights this section with the annotation 'Application Security をチェック'.
- Configuration:** 'Storage Destination' is set to 'Remote Storage'. A red box highlights this field with the annotation 'Remote Storage を選択'.
- Server Addresses:** The 'IP Address' field is set to '10.99.2.201:514'. A red box highlights this section with the annotation 'ログ出力先サーバを指定'.
- Storage Format:** The 'Field-List' is set to 'Comma-Separated Values'. A red box highlights this section with the annotation '出力したい項目を選択'.
- Storage Filter:** The 'Request Type' is set to 'Illegal requests only'. A red box highlights the 'Create' button at the bottom of the page.

## 16.2. Logging Profile の VS への適用

- (1) 各バーチャルサーバへ、設定した Logging Profile を適用します。「Local Traffic」→「Virtual Servers」→「Virtual Server list」で表示された該当 VS をクリックし、「Security」タブの「Policies」をクリックすると、以下の画面が表示されます。作成した profile を選択して、Update ボタンを押します。

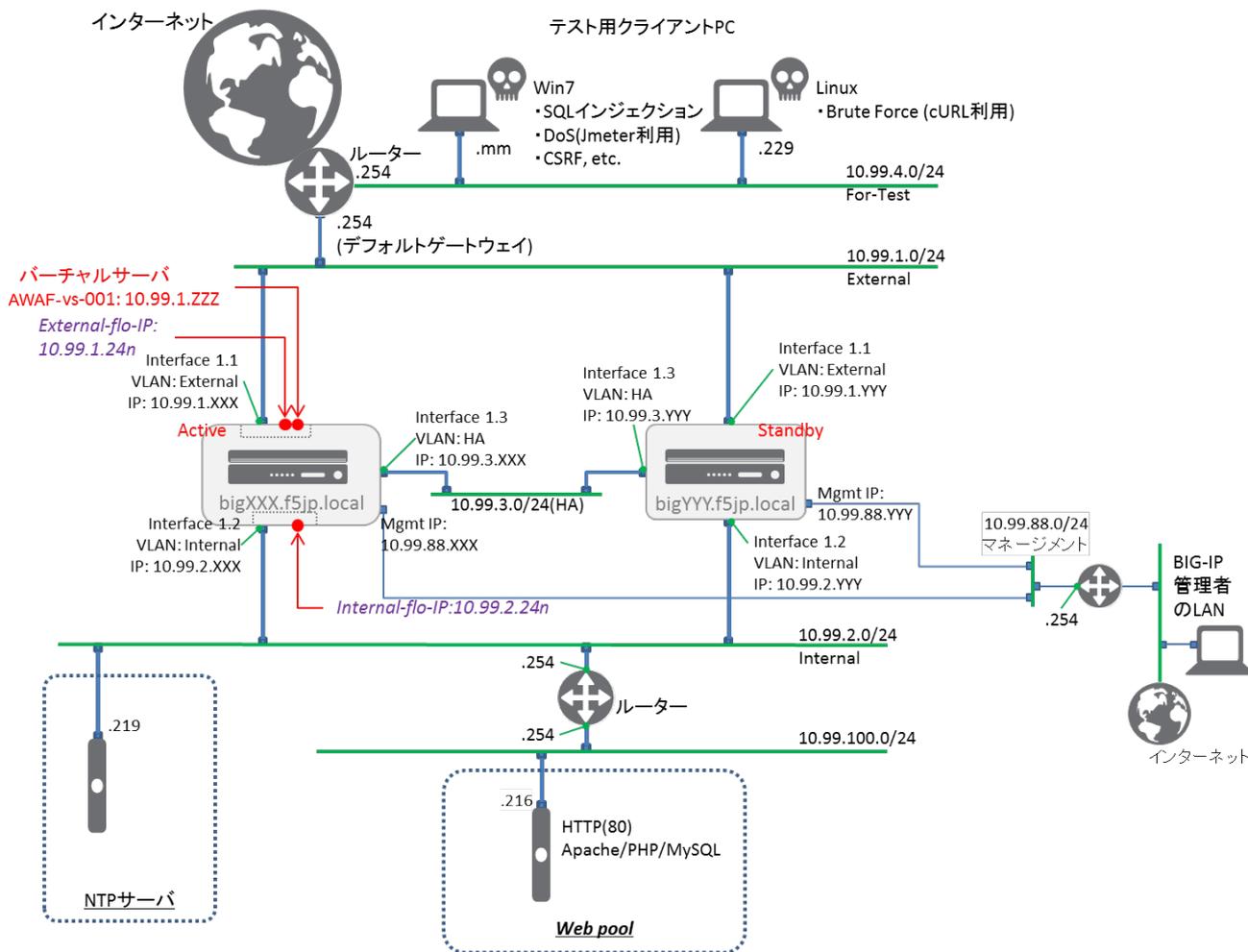
The screenshot shows the F5 management console interface. At the top, the status bar indicates the system is ONLINE (ACTIVE) and Standalone. The breadcrumb navigation shows the path: Local Traffic >> Virtual Servers : Virtual Server List >> https\_WAF-vs-001. The left sidebar contains navigation options: Main, Help, About, Statistics, iApps, DNS, and Local Traffic (with sub-items: Network Map, Virtual Servers, Policies, Profiles, Ciphers, iRules, Pools, Nodes, Monitors, and Traffic Class). The main content area is titled 'Policy Settings' and shows configuration for the selected Virtual Server. The 'Log Profile' field is highlighted with a red box, and a dropdown menu is open, showing a list of available profiles: /Common, WAF-logging-profile, Log illegal requests, global-network, local-bot-defense, local-dos, and Log illegal and staging requests. The 'Update' button at the bottom left of the configuration area is also highlighted with a red box.

Destination	10.99.1.81:443
Service	HTTPS
Application Security Policy	Enabled... Policy: WAF-policy-001
Service Policy	None
IP Intelligence	Disabled
DoS Protection Profile	Disabled
Bot Defense Profile	Disabled
Log Profile	Selected: /Common, WAF-logging-profile; Available: Log illegal requests, global-network, local-bot-defense, local-dos, Log illegal and staging requests

## 17. 冗長化

### 17.1. 冗長化のネットワークサンプル

もう一台 Adv.WAF を追加して、L3 構成の冗長化設定を行います。



Adv.WAF 間の HA (High Availability) VLAN は、冗長化の制御プロトコルをやり取りする専用の VLAN です。External や Internal VLAN を利用することも可能ですが、HA 専用の VLAN を追加することを推奨しています。

よって、本構成においては、HA VLAN を追加しています。

## 17.2.Active 機の設定

**管理(マネージメント)IP アドレスの 4 オクテット目の数字が大きい方が、デフォルトで”Active”となります。**  
F5Lab 環境では、bigXXX.f5jp.local が Active 機となります。

### 17.2.1. VLAN、SelfIP の設定

#### (1) HA VLAN の設定

「Network」→「VLANs」で表示された画面の右上にある「Create」ボタンを押し、HA 用 VLAN を設定します。

Hostname big181.f5jp.local Date Jul 25, 2019 User admin  
IP Address 10.99.88.181 Time 7:52 PM (JST) Role Administrator Partition: Common Log out

ONLINE (ACTIVE)  
Standalone

Main Help About Network » VLANs : VLAN List » New VLAN...

Statistics  
iApps  
DNS  
Local Traffic  
Acceleration  
Device Management  
Shared Objects  
Security  
Network

General Properties  
Name HA  
Description  
Tag

Resources  
Interface: 1.1  
Tagging: Untagged  
Add  
1.3 (untagged)  
Edit Delete

Configuration: Basic  
Source Check  
MTU 1500

sFlow  
Polling Interval Default  
Sampling Rate Default

Cancel Repeat Finished

名前(任意)を指定

ポート&Untagged を選択

#### (2) HA VLAN の IP 設定

「Network」→「Self IPs」で表示された画面の右上にある「Create」ボタンを押し、HA 用 VLAN の IP を設定します。

Hostname big181.f5jp.local Date Jul 25, 2019 User admin  
IP Address 10.99.88.181 Time 7:54 PM (JST) Role Administrator Partition: Common Log out

ONLINE (ACTIVE)  
Standalone

Main Help About Network » Self IPs » New Self IP...

Statistics  
iApps  
DNS  
Local Traffic  
Acceleration  
Device Management  
Shared Objects  
Security

Configuration  
Name HA-ip  
IP Address 10.99.3.181  
Netmask 255.255.255.0  
VLAN / Tunnel HA  
Port Lockdown Allow Default  
Traffic Group Inherit traffic group from current partition / path  
traffic-group-local-only (non-floating)  
Service Policy None

Cancel Repeat Finished

名前(任意)  
IP アドレス  
サブネットマスク  
VLAN を設定  
※1 必ず Allow None 以外を選ぶ

※1 Allow None を選ぶと HA の通信も止めてしまい、HA が組めません。(ここでは Allow Default を選びます)

## 17.2.2. Device の設定

(1) 次に、「Device Management」→「Devices」で、自分自身:bigXXX.f5jp.local(self)を選択します。

Hostname big181.f5jp.local Date Jul 25, 2019 User admin  
IP Address 10.99.88.181 Time 7:55 PM (JST) Role Administrator Partition: Common Log out

ONLINE (ACTIVE)  
Standalone

Main Help About

Device Management » Devices

Device List

Search

Status	Name	Address	Hostname	Version	Time Delta (sec)
	big181.f5jp.local (Self)	10.99.88.181	big181.f5jp.local	BIG-IP v14.1.0.6 (Build 0.0.9)	0

Overview  
Devices

(2) 「ConfigSync」を選択し、HA VLAN に指定した IP アドレスを選択し「Update」を押します。

Hostname big181.f5jp.local Date Jul 25, 2019 User admin  
IP Address 10.99.88.181 Time 7:56 PM (JST) Role Administrator Partition: Common Log out

ONLINE (ACTIVE)  
Standalone

Main Help About

Device Management » Devices » big181.f5jp.local

Properties ConfigSync Failover Network Mirroring

ConfigSync Configuration

Local Address 10.99.3.181 (HA) HA VLAN に設定した IP アドレスを選択

Update

(3) 「Failover Network」を選択し、「Add」ボタンを押します。

Hostname big181.f5jp.local Date Jul 25, 2019 User admin  
IP Address 10.99.88.181 Time 7:58 PM (JST) Role Administrator Partition: Common Log out

ONLINE (ACTIVE)  
Standalone

Main Help About

Device Management » Devices » big181.f5jp.local

Properties ConfigSync Failover Network Mirroring

Failover Unicast Configuration

Local Address Port VLAN

No records to display.

Delete

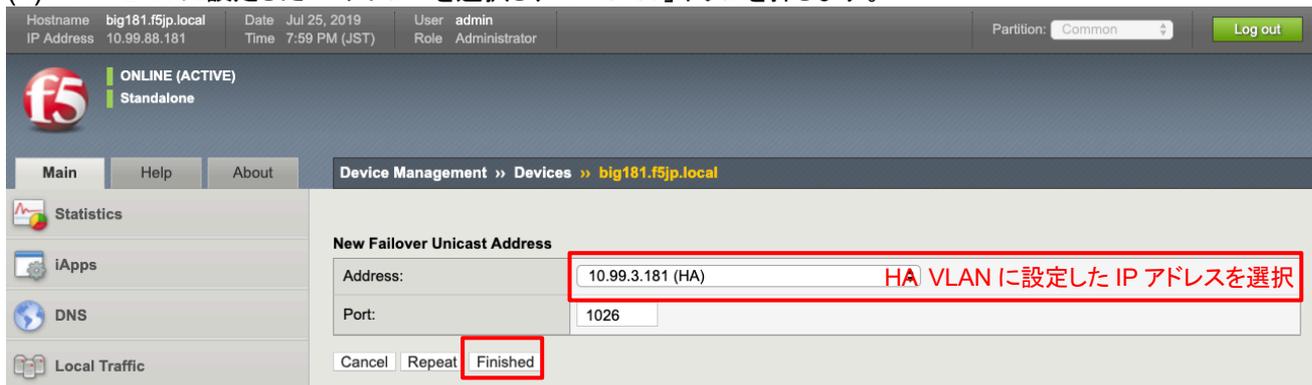
Failover Multicast Configuration

Use Failover Multicast Address  Enabled

Update

Add...

(4) HA VLAN に設定した IP アドレスを選択し、「Finished」ボタンを押します。

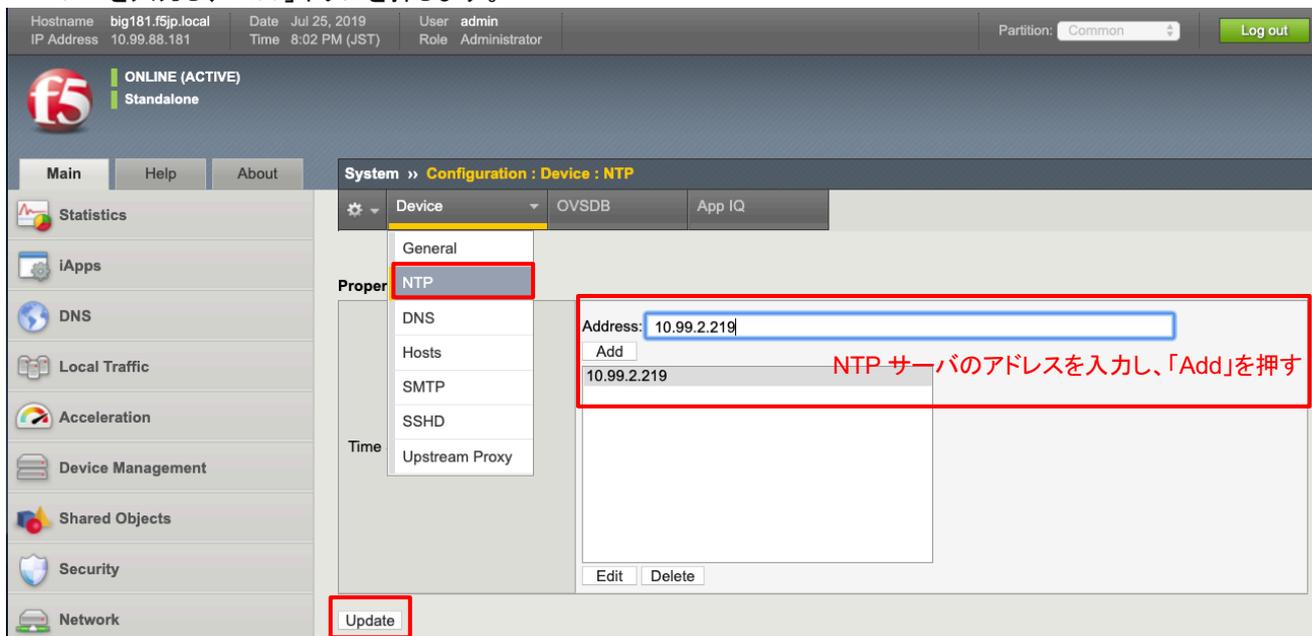


(5) 「Mirroring」を選択し、HA VLAN に指定した IP アドレスをプライマリに指定します。任意ですが、ここでは Secondary として、Observe VLAN に指定した IP アドレスを選択しています。選択後、「Update」を押します。



### 17.2.3. 時刻同期(NTP)設定

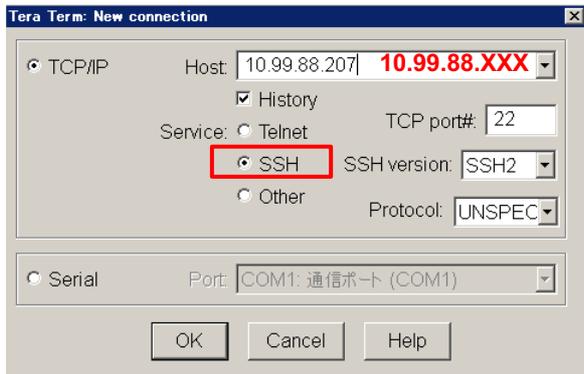
(1) 「System」→「Configuration」→「Device」→「NTP」を選択します。Address 欄に、NTP サーバの IP アドレスを入力し、「Add」ボタンを押します。



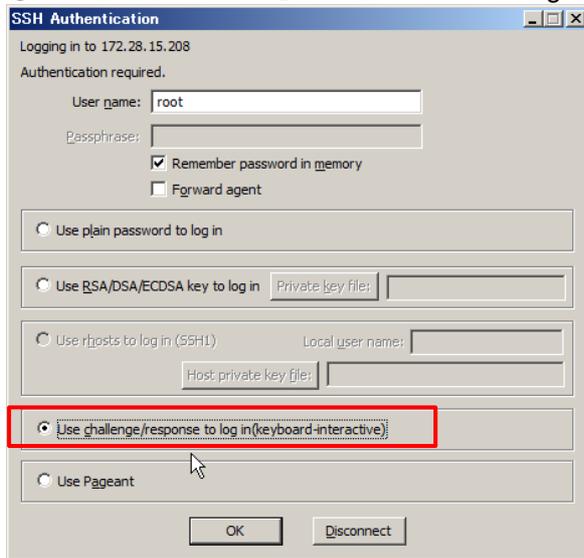
[ご参考] NTP 同期状態の確認

NTP 同期状態の確認は、コマンドラインから実施します。以下に、Tera Term を利用した場合の確認方法を示します。

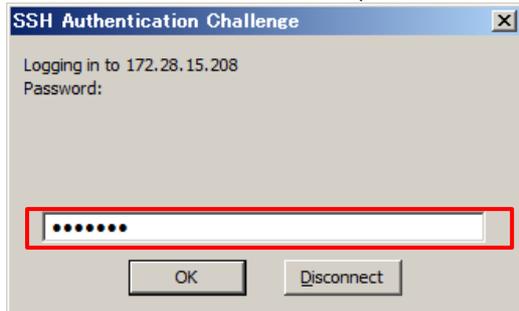
① SSH でログインします。



② User name に「root」を入力し、Use challenge/response to log in をチェックします。



③ パスワードを入力します。(デフォルト状態のパスワードは「default」です)



④ SSH アクセスが完了したら、「ntpq -np」を実行します。先頭に「\*」がついていれば、同期が完了しています。(同期完了状態になるまで、時間がかかる場合があります。)

```
[root@bigXXX:Active:Standalone] config # ntpq -np
remote          refid          st t when poll reach  delay  offset jitter
=====
*10.99.2.219    133.243.238.243  2 u  23   64    1   0.805 -0.003  0.933
```

### 17.3. Standby 機(bigYYY.f5jp.local)の設定

(1) Active 機での VLAN、Self IP、Devices の設定と同様の設定を Standby 機に対しても行います。

(2) Standby 機に設定する VLAN は以下のようになります。

The screenshot shows the Palo Alto Networks configuration interface for a Standby device. The page title is "Network >> VLANs : VLAN List". The table below lists the configured VLANs:

Name	Application	Tag	Untagged Interfaces	Tagged Interfaces	Partition / Path
HA		4092	1.3		Common
external		4094	1.1		Common
internal		4093	1.2		Common

(3) Standby 機に設定する Self IP アドレスは以下のようになります。

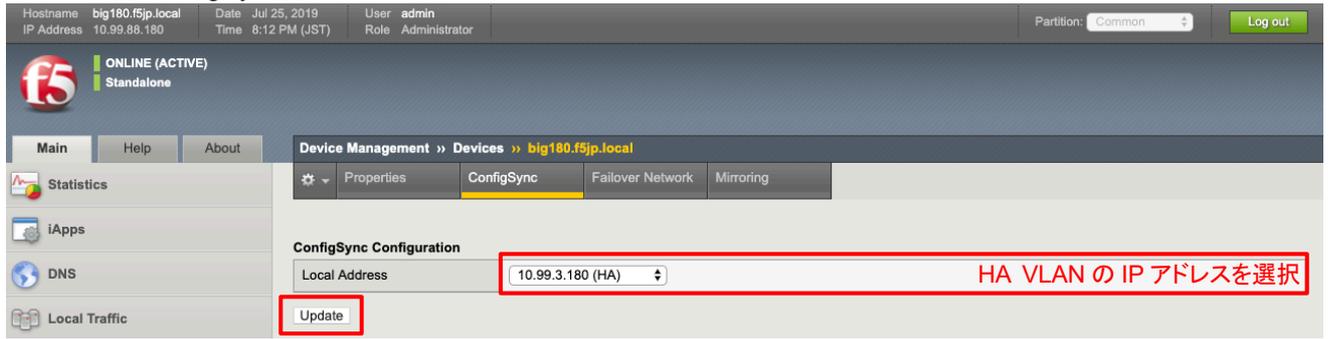
The screenshot shows the Palo Alto Networks configuration interface for a Standby device. The page title is "Network >> Self IPs". The table below lists the configured Self IP addresses:

Name	Application	IP Address	Netmask	VLAN / Tunnel	Traffic Group	Partition / Path
HA-ip		10.99.3.180	255.255.255.0	HA	traffic-group-local-only	Common
external-ip		10.99.1.180	255.255.255.0	external	traffic-group-local-only	Common
internal-ip		10.99.2.180	255.255.255.0	internal	traffic-group-local-only	Common

(4) NTP 設定を行います。

The screenshot shows the Palo Alto Networks configuration interface for a Standby device. The page title is "System >> Configuration : Device : NTP". The "Properties" section shows the NTP configuration form. The "Address" field is set to "10.99.2.219". A red box highlights the "Address" field and the "Add" button, with the text "NTP アドレスを入力し、「Add」ボタンを押す". The "Update" button is also highlighted with a red box.

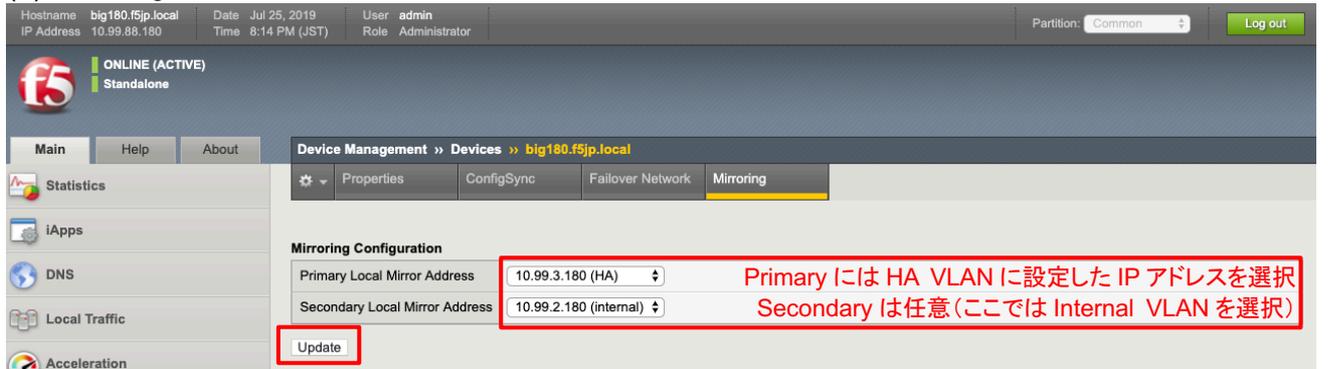
- (5) 「Device Management」→「Devices」で、自分自身 :bigYYY.f5jp.local(self)を選択し、Active 機同様に、Device Connectivity の設定を行います。  
 まずは ConfigSync を設定します。



- (6) Failover Network を設定します。



- (7) Mirroring を設定します。



## 17.4. デバイストラストの設定

- (1) デバイストラスト設定にて、冗長化する機器間で信頼関係を結びます。
- (2) 本項は、Active 機: bigXXX.f5jp.local からのみ、設定します。

(3) 「Device Management」→「Device Trust」→「Device Trust Members」を選択し、「Add」ボタンを押します。

The screenshot shows the F5 Device Management web interface. At the top, it displays system information: Hostname (big181.f5jp.local), IP Address (10.99.88.181), Date (Jul 25, 2019), Time (8:16 PM (JST)), User (admin), Role (Administrator), and Partition (Common). The main content area is titled 'Device Management >> Device Trust : Device Trust Members'. On the left sidebar, the 'Device Trust' menu item is highlighted with a red box. In the main content area, the 'Peer and Subordinate Devices' section has an 'Add...' button highlighted with a red box. Below this button is a table with columns for Name, Device Type, Hostname, Serial Number, and MAC Address, and a 'Delete' button.

(4) Standby 機: bigYYY.f5jp.local の IP アドレスと管理者 ID(Admin)とパスワードを指定します。「Retrieve Device Information」ボタンを押します。

The screenshot shows the 'Retrieve Device Credentials (Step 1 of 3)' form in the F5 Device Management interface. The form fields are: Device Type (Peer), Device IP Address (10.99.3.180, 10.99.3.YYY), Administrator Username (admin), and Administrator Password (\*\*\*\*\*). A red text box on the right side of the form contains the instruction: 'Standby 機の IP アドレスを指定し、管理者ユーザ名(admin)およびそのパスワードを指定します'. The 'Retrieve Device Information' button at the bottom of the form is highlighted with a red box.

(5) Standby 機 bigYYY.f5jp.local の証明書情報が表示されます。「Device Certificate Matches」ボタンを押します。

Hostname big181.f5jp.local Date Jul 25, 2019 User admin  
IP Address 10.99.88.181 Time 8:18 PM (JST) Role Administrator Partition: Common Log out

ONLINE (ACTIVE)  
Standalone

Main Help About Device Management » Device Trust

Statistics  
iApps  
DNS  
Local Traffic  
Acceleration  
Device Management  
Overview  
Devices  
Device Groups  
Device Trust  
Traffic Groups  
Shared Objects  
Security

**Retrieve Device Credentials (Step 1 of 3)**

Device Type	Peer
Device IP Address	10.99.3.180
Administrator Username	admin
Administrator Password	*****

**Verify Device Certificate (Step 2 of 3)**

Subject	/C=- -/ST=WA/L=Seattle/O=MyCompany/OU=MyOrg/CN=localhost.localdomain/emailAddress=root@localhost.localdomain
Management IP Address	10.99.3.180
Expiration	Sun Jul 07 09:58:27 JST 2029
Serial Number	f7a9fe1e30d862c1
Signed	Yes
SHA-1	1fe1449db6c43d38e3ec9a43622c375994785652
MD5	59f600ed4f12e09e9ed1e918b8a00f83

Cancel Device Certificate Matches

(6) Device Name を確認し、「Add Device」ボタンを押します。

Hostname big181.f5jp.local Date Jul 25, 2019 User admin  
IP Address 10.99.88.181 Time 8:19 PM (JST) Role Administrator Partition: Common Log out

ONLINE (ACTIVE)  
Standalone

Main Help About Device Management » Device Trust

Statistics  
iApps  
DNS  
Local Traffic  
Acceleration  
Device Management  
Overview  
Devices  
Device Groups  
Device Trust  
Traffic Groups  
Shared Objects  
Security  
Network

**Retrieve Device Credentials (Step 1 of 3)**

Device Type	Peer
Device IP Address	10.99.3.180
Administrator Username	admin
Administrator Password	*****

**Verify Device Certificate (Step 2 of 3)**

Subject	/C=- -/ST=WA/L=Seattle/O=MyCompany/OU=MyOrg/CN=localhost.localdomain/emailAddress=root@localhost.localdomain
Management IP Address	10.99.3.180
Expiration	Sun Jul 07 09:58:27 JST 2029
Serial Number	f7a9fe1e30d862c1
Signed	Yes
SHA-1	1fe1449db6c43d38e3ec9a43622c375994785652
MD5	59f600ed4f12e09e9ed1e918b8a00f83

**Add Device (Step 3 of 3)**

Name	big180.f5jp.local
------	-------------------

Cancel Add Device

(7) 承認されたデバイスとして登録された状態です。

The screenshot shows the f5 Device Management interface. At the top, it displays system information: Hostname: big181.f5jp.local, Date: Aug 7, 2019, User: admin, IP Address: 10.99.88.181, Time: 6:19 PM (JST), Role: Administrator, Partition: Common, and a Log out button. The main header shows 'ONLINE (ACTIVE)' and 'Changes Pending'. The navigation menu includes Main, Help, and About. The left sidebar contains Statistics, iApps, DNS, and Local Traffic. The main content area is titled 'Device Management >> Device Trust : Device Trust Members'. Below this, there are tabs for Local Domain, Identity, and Device Trust Members. The 'Peer and Subordinate Devices' section contains a table with columns: Name, Device Type, Hostname, Serial Number, and MAC Address. A single row is highlighted with a red border, showing the device 'big180.f5jp.local' with Device Type 'Peer', Hostname 'big180.f5jp.local', Serial Number '4217261b-71df-2705-64852db0043c', and MAC Address '00:50:56:97:fc:93'. A 'Delete' button is located below the table.

Name	Device Type	Hostname	Serial Number	MAC Address
big180.f5jp.local	Peer	big180.f5jp.local	4217261b-71df-2705-64852db0043c	00:50:56:97:fc:93

(8) 「Device Management」→「Devices」で見ると、(self)に加え、Standby 機: bigYYY.f5jp.local も表示されます。  
(ここは確認のみです。)

The screenshot shows the f5 Device Management interface. At the top, it displays system information: Hostname: big181.f5jp.local, Date: Aug 7, 2019, User: admin, IP Address: 10.99.88.181, Time: 6:20 PM (JST), Role: Administrator, Partition: Common, and a Log out button. The main header shows 'ONLINE (ACTIVE)' and 'Changes Pending'. The navigation menu includes Main, Help, and About. The left sidebar contains Statistics, iApps, DNS, Local Traffic, and Acceleration. The main content area is titled 'Device Management >> Devices'. Below this, there is a 'Device List' tab. A search bar is present above a table with columns: Status, Name, Address, Hostname, Version, and Time Delta (sec). Two rows are highlighted with a red border. The first row shows a device with status 'Offline' (represented by a red icon), Name 'big180.f5jp.local', Address '10.99.88.180', Hostname 'big180.f5jp.local', Version 'BIG-IP v14.1.0.6 (Build 0.0.9)', and Time Delta '0'. The second row shows a device with status 'Online' (represented by a green icon), Name 'big181.f5jp.local (Self)', Address '10.99.88.181', Hostname 'big181.f5jp.local', Version 'BIG-IP v14.1.0.6 (Build 0.0.9)', and Time Delta '0'.

Status	Name	Address	Hostname	Version	Time Delta (sec)
Offline	big180.f5jp.local	10.99.88.180	big180.f5jp.local	BIG-IP v14.1.0.6 (Build 0.0.9)	0
Online	big181.f5jp.local (Self)	10.99.88.181	big181.f5jp.local	BIG-IP v14.1.0.6 (Build 0.0.9)	0

## 17.5. デバイスグループの設定

- (1) デバイスグループは、デバイストラストで信頼関係を結んだ機器の間で、どの機器間で冗長化を行うかの指定です。デバイストラストは Adv.WAF × 3 台以上で構成することも可能で、例えば、(1)と(2)で冗長化を行い、(2)と(3)はコンフィグ同期のみ行う、という組合せが可能となっています。この組み合わせをデバイスグループで指定します。
- 2 台で冗長化を行う場合はデバイスグループの組み方をあまり意識する必要はありませんが、設定は必要です。

- (2) 「Device Management」→「Device Groups」から、デバイスグループを作成します。

Hostname: big181.f5jp.local Date: Aug 7, 2019 User: admin  
IP Address: 10.99.88.181 Time: 6:21 PM (JST) Role: Administrator Partition: Common Log out

ONLINE (ACTIVE)  
Changes Pending

Main Help About Device Management » New Device Group...

Statistics  
iApps  
DNS  
Local Traffic  
Acceleration  
Device Management  
Overview  
Devices  
Device Groups  
Device Trust  
Traffic Groups  
Shared Objects  
Security

**General Properties**

Name: Device-Group-001 **名前(任意)を設定**  
Group Type: Sync-Failover **「Sync-Failover」を選択**  
Description:

**Configuration:** Advanced

Members: Includes: /Common, big180.f5jp.local, big181.f5jp.local Available: **冗長化を行うデバイス(自分自身を含む)を選択**

Sync Type: Manual with Incremental Sync  
Maximum Incremental Sync Size (KB): 1024  
Network Failover:  Enabled **ネットワークフェイルオーバーを行うので、チェック**  
Link Down Time on Failover: 0.0 seconds

Cancel Repeat **Finished**

- (3) デバイスグループが作られた状態です。

Hostname: big181.f5jp.local Date: Aug 7, 2019 User: admin  
IP Address: 10.99.88.181 Time: 6:23 PM (JST) Role: Administrator Partition: Common Log out

ONLINE (ACTIVE)  
Changes Pending

Main Help About Device Management

Device Group List

\* Search Create...

<input checked="" type="checkbox"/>	Group Name	Type	ConfigSync	ConfigSync Status	Members
<input type="checkbox"/>	Device-Group-001 (Includes Self)	Sync-Failover	Manual	Awaiting Initial Sync	2

Delete...

## 17.6.トラフィックグループの設定

トラフィックグループは、デバイスグループ内で移動するオブジェクトの集合です。  
主に、Virtual Server と共有 IP(Floating IP)がトラフィックグループのオブジェクトです。

- (1) 「Device Management」→「Traffic Groups」を確認します。デフォルトで、「Traffic-group-1」という名前のトラフィックグループが存在しています。以降、この Traffic-group-1 に対して、Floating IP および Virtual Server を割当てていきます。

Hostname big191.f5jp.local Date Jul 26, 2019 User admin  
IP Address 10.99.88.191 Time 8:44 PM (JST) Role Administrator Partition: Common Log out

ONLINE (ACTIVE)  
Changes Pending

Main Help About

Device Management » Traffic Groups

Traffic Group List

Failover Status

Status	ACTIVE
Summary	1/1 active
Details	

Search Create...

Name	Active Device	Next Active Device	Failover Objects	HA Group	Failover Method	Partition / Path
traffic-group-1	big191.f5jp.local (Self)	big190.f5jp.local	1	None	HA Order	Common

Force to Standby... Delete...

デフォルトのトラフィックグループ

- (2) Floating IP (共有 IP)を追加設定します。Floating IP は、Active 機ダウン時に Standby 機が引き継ぐ、自身に設定された IP アドレス(Self IP)を指します。実サーバは、この IP アドレスをデフォルトゲートウェイに指定することで、Active/Standby の切り替わり発生時にも、即座に通信を再開できます。
- (3) Internal VLAN 側の共有 IP(Floating IP)を追加設定します。「Network」→「Self IPs」から設定します。ここで、Traffic-group-1 を選択することで、そのトラフィックグループに属させます。

Hostname big191.f5jp.local Date Jul 26, 2019 User admin  
IP Address 10.99.88.191 Time 8:46 PM (JST) Role Administrator Partition: Common Log out

ONLINE (ACTIVE)  
Changes Pending

Main Help About

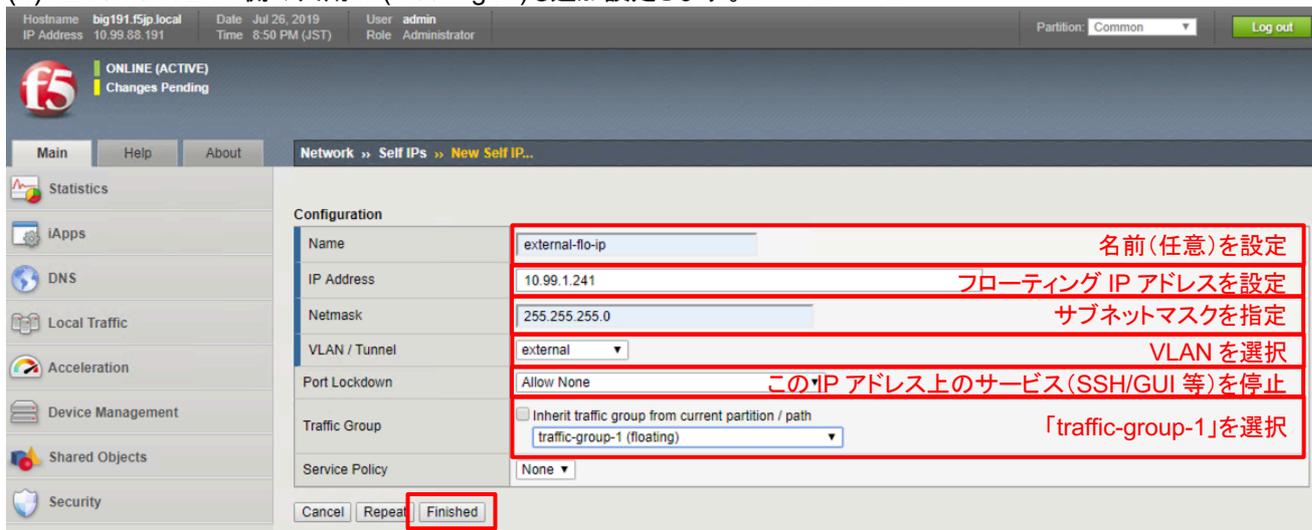
Network » Self IPs » New Self IP...

Configuration

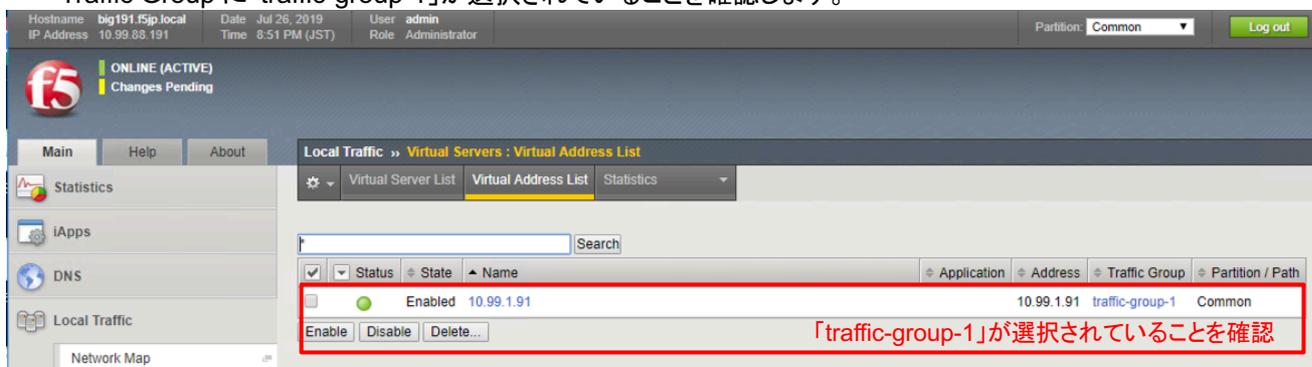
Name	internal-flo-ip	名前(任意)を設定
IP Address	10.99.2.241	フローティング IP アドレスを設定
Netmask	255.255.255.0	サブネットマスクを指定
VLAN / Tunnel	internal	VLAN を選択
Port Lockdown	Allow Default	この IP アドレス上のサービス (SSH/GUI 等) を許可
Traffic Group	traffic-group-1 (floating)	「traffic-group-1」を選択
Service Policy	None	

Cancel Repeat Finished

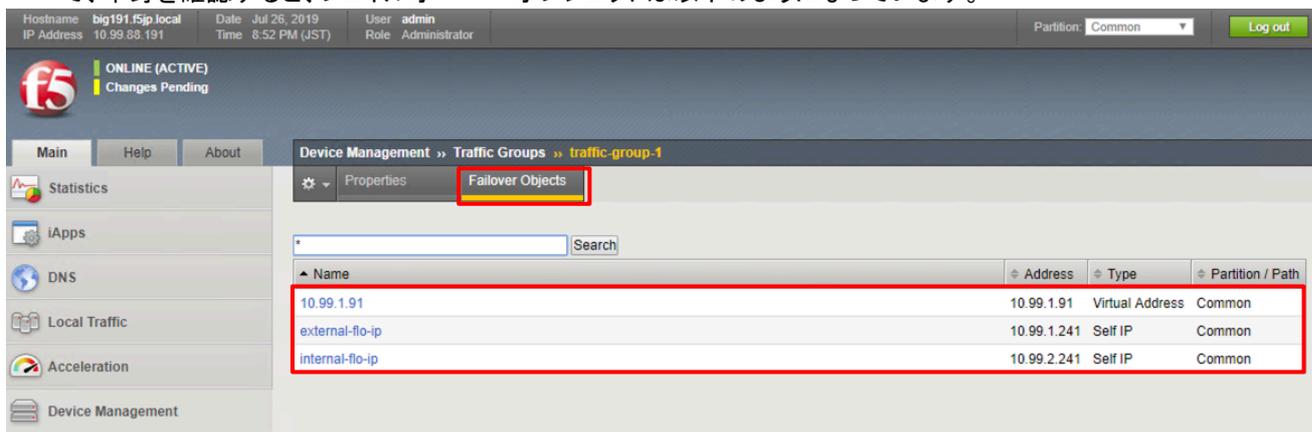
(4) External VLAN 側の共用 IP(Floating IP)も追加設定します。



(5) 「Local Traffic」→「Virtual Servers」→「Virtual Address List」を選択します。  
Traffic Group に「traffic-group-1」が選択されていることを確認します。



(6) 「Device Management」→「Traffic Groups」の Traffic-group-1 をクリック→「Failover Objects」タブをクリックして、中身を確認すると、フェイルオーバーオブジェクトは以下のようになっています。



- (7) **Adv.WAF 固有の設定です。** Adv.WAF ポリシーを同期するために必要となります。  
「Security」→「Options」→「Application Security」→「Synchronization」→「Application Security Synchronization」で表示された画面で、設定した Device-Group を選択し、「Save」ボタンを押します。

Hostname big191.f5jp.local Date Jul 26, 2019 User admin  
IP Address 10.99.89.191 Time 8:53 PM (JST) Role Administrator Partition: Common Log out

ONLINE (ACTIVE)  
Changes Pending

Main Help About

Security » Options : Application Security : Synchronization : Application Security Synchronization

Attack Signatures Threat Campaigns RegExp Validator Integrated Services Advanced Configuration Synchronization Preferences

Application Security Synchronization

Device Group	Device-Group-001
Device Group Members	/Common/big190.f5jp.local /Common/big191.f5jp.local
Device Group Type	Sync-Failover
Config Sync	Manual

Save

設定済みの Device-Group を選択

## 17.7. ConfigSync

Active 機: bigXXX.f5jp.local にのみ行った設定を、Standby 機: bigYYY.f5jp.local に同期するために、ConfigSync を行います。

「Device Management」→「Overview」を選択すると、3つの Device Group が作成されています。

I	device_trust_group	trust group に peer を設定すると、システムによって自動的に作成されます。peer の基本情報を Sync します。
II	datasync-global-dg	Adv.WAF 特有の Device Group で、システムによって自動的に作成されます。Script や暗号鍵を Sync します。
III	Device-Group-001 (任意の名前)	前項で作成したユーザ設定領域のデータを Sync します。

I は自動で Sync されますが、II と III はデフォルトでマニュアル Sync の設定となっています。II は初回設定時、または UCS ファイルからデータをリストアした後に Sync を実施する必要があります。III はマニュアル設定の場合、ユーザ設定領域の変更を行った場合に Sync を実施します。

(1) Device-Group-001 (任意の名前) を Sync します。アクティブ機(bigXXX.f5jp.local)を選択し、「Sync」ボタンを押すことで、コンフィグ同期が行われます。

The screenshot shows the F5 configuration interface. At the top, it displays the hostname 'big191.f5jp.local', date 'Jul 26, 2019', and user 'admin'. The main navigation bar includes 'Main', 'Help', and 'About'. The left sidebar contains various system management options like 'Statistics', 'iApps', 'DNS', 'Local Traffic', 'Acceleration', 'Device Management', 'Shared Objects', 'Security', 'Network', and 'System'. The main content area is titled 'Device Management >> Overview'. Under 'Device Groups', there are three entries: 'Device-Group-001' (Changes Pending, 2 Devices, Sync-Failover Group, Manual Sync, No successful group sync), 'datasync-global-dg' (Changes Pending, 2 Devices, Sync-Only Group, No successful group sync), and 'device\_trust\_group' (In Sync, 2 Devices, Sync-Only Group, Auto Sync, In sync on 7/26/2019 at 20:43:15). The 'Device-Group-001' section is expanded, showing a 'Changes Pending' message with a recommended action to synchronize 'big191.f5jp.local' to the group. Below this, the 'Devices' section lists 'big191.f5jp.local (Self)' as selected (indicated by a red box and the word '選択') and 'big190.f5jp.local' as 'Awaiting Initial Sync'. The 'Sync Options' section has two radio buttons: 'Push the selected device configuration to the group' (selected) and 'Pull the most recent configuration to the selected device'. A 'Sync' button is highlighted with a red box. At the bottom, the 'In Sync' section shows the status of the other two device groups.

(2) datasync-global-dg を Sync します。アクティブ機(bigXXX.f5jp.local)を選択し、「Sync」ボタンを押すことで、コンフィグ同期が行われます。

Hostname: big181.f5jp.local Date: Aug 7, 2019 User: admin  
IP Address: 10.99.88.181 Time: 6:45 PM (JST) Role: Administrator Partition: Common Log out

ONLINE (ACTIVE)  
Changes Pending

Main Help About

Device Management » Overview

Device Groups:

Sync Issues :

datasync-global-dg Changes Pending 2 Devices Sync-Only Group Manual Sync No successful group sync

Changes Pending  
Recommended action: Synchronize big181.f5jp.local to group datasync-global-dg

Devices: View: Basic

Recent Changes

big181.f5jp.local (Self) 選択 Awaiting initial Sync with Changes Pending Configuration Time : 8/7/2019 at 18:07:43

New Device Group Members

big180.f5jp.local Awaiting Initial Sync Configuration Time : Device has not synced with group

Sync Options:

Push the selected device configuration to the group  
Pull the most recent configuration to the selected device

Sync

In Sync:

Device-Group-001	In Sync	2 Devices	Sync-Failover Group	Manual Sync	In sync on 8/7/2019 at 18:28:40
device_trust_group	In Sync	2 Devices	Sync-Only Group	Auto Sync	In sync on 8/7/2019 at 18:28:40

(3) 以下のメッセージがでるので、「Sync and Overwrite」を選択します。

Confirm Sync and Overwrite

Push big181.f5jp.local configuration to datasync-global-dg?

Warning: The receiving devices may become OFFLINE for several minutes while the configuration is updated:  
big180.f5jp.local may become offline for several minutes  
big181.f5jp.local will remain online

Sync and Overwrite Cancel

(4) しばらく待つと、コンフィグ同期が完了し、各ステータスがグリーンになります。

Hostname: big181.f5jp.local    Date: Aug 7, 2019    User: admin  
IP Address: 10.99.88.181    Time: 6:47 PM (JST)    Role: Administrator    Partition: Common    [Log out](#)

**f5** ONLINE (ACTIVE)  
In Sync

Main    Help    About

Statistics  
iApps  
DNS  
Local Traffic  
Acceleration  
Device Management  
  Overview  
  Devices  
  Device Groups  
  Device Trust  
  Traffic Groups  
Shared Objects  
Security  
Network

Device Management » Overview

Device Groups:

**In Sync:**

▶ Device-Group-001	In Sync	2 Devices	Sync-Failover Group	Manual Sync	In sync on 8/7/2019 at 18:28:40
▼ datasync-global-dg	In Sync	2 Devices	Sync-Only Group	Manual Sync	In sync on 8/7/2019 at 18:07:43

In Sync  
All devices are in sync. There are no changes pending.

**Devices:** View: Basic

<input checked="" type="radio"/> big180.f5jp.local	In Sync	Configuration Time : 8/7/2019 at 18:07:43
<input type="radio"/> big181.f5jp.local (Self)	In Sync	Configuration Time : 8/7/2019 at 18:07:43

**Sync Options:**  
No sync options are available.

▶ device_trust_group	In Sync	2 Devices	Sync-Only Group	Auto Sync	In sync on 8/7/2019 at 18:28:40
----------------------	---------	-----------	-----------------	-----------	---------------------------------

## 17.8. Traffic-group-1 の Active/Standby の切替え

- (1) アクティブ機の「Device Management」→「Traffic Groups」から Traffic-group-1 を選択し、「Force to Standby」ボタンを押します。

The screenshot shows the Fortinet web interface for configuring a Traffic Group. The top status bar indicates the device is ONLINE (ACTIVE) and In Sync. The left sidebar shows the navigation menu with 'Traffic Groups' selected. The main content area displays the configuration for 'traffic-group-1'. The 'General Properties' section shows the name, partition, and current device. The 'Health Monitor' section shows the HA Group is set to 'none'. The 'Failover Configuration' section shows the failover method is 'Failover using Preferred Device Order and then Load Aware' and the failover order is 'Preferred Order'. The 'HA Load Factor' is set to 1. The 'Force to Standby' button is highlighted with a red box.

- (2) 確認のポップアップがでるので、「Force to Standby」ボタンを押します。

The screenshot shows a confirmation dialog box titled 'Force Traffic Group to Standby'. The dialog contains a question mark icon and the text 'Are you sure you want to force this Traffic Group to standby?'. At the bottom, there are two buttons: 'Force to Standby' and 'Cancel'. The 'Force to Standby' button is highlighted with a red box.

- (3) その結果、Active から Standby に変わります。

The screenshot shows the Fortinet web interface displaying the Traffic Group List. The top status bar indicates the device is ONLINE (STANDBY) and In Sync. The left sidebar shows the navigation menu with 'Traffic Groups' selected. The main content area displays the 'Failover Status' for 'traffic-group-1', showing the status as 'STANDBY' and the summary as '1/1 standby'. Below the status information is a table listing the traffic groups. The 'Force to Standby' button is highlighted with a red box.

Name	Active Device	Next Active Device	Failover Objects	HA Group	Failover Method	Partition / Path
traffic-group-1	big190.f5jp.local	big191.f5jp.local (Self)	3	None	HA Order	Common

(4) Standby だった Adv.WAF は Active になります。

The screenshot shows the F5 management console interface. At the top, the status is "ONLINE (ACTIVE)" and "In Sync", highlighted with a red box. The navigation menu includes "Main", "Help", and "About". The "Device Management" section is expanded to "Traffic Groups". The "Failover Status" section shows:

Status	ACTIVE
Summary	1/1 active
Details	

Below this is a search bar and a "Create..." button. A table lists the traffic groups:

<input checked="" type="checkbox"/>	Name	Active Device	Next Active Device	Failover Objects	HA Group	Failover Method	Partition / Path
<input type="checkbox"/>	traffic-group-1	big190.f5jp.local (Self)	big191.f5jp.local	3	None	HA Order	Common

Buttons for "Force to Standby..." and "Delete..." are visible at the bottom of the table.

(5) テスト用クライアントから、作成した Virtual Server へ Web ブラウザでアクセスし、Web 画面が表示されることを確認します。

(6) Traffic-Group-1 を、再度切替え、クライアントからの通信が復旧するかを確認してください。

## 18. おわりに

Adv.WAF セットアップに関しては以上で終了となります。

BIG-IP シリーズ製品ラインナップにおいては、ソフトウェアモジュールライセンスを追加することで、サーバ負荷分散はもちろんのこと、広域負荷分散やリモートアクセス機能、ネットワークファイアウォール機能など、アプリケーションアクセスを最適化する為の多彩な機能が使用できるようになります。

詳細は各種 WEB サイトにてご確認くださいか、F5 公式販売代理店にお問い合わせください。

<F5 ネットワークス WEB サイトの紹介>

F5 ネットワークスジャパン総合サイト

<https://f5.com/jp>

F5 のセキュリティ ソリューション

<https://f5.com/jp/products/security>

AskF5: ナレッジベース総合サイト(英語)

<http://support.f5.com/kb/en-us.html>

DevCentral: F5 ユーザコミュニティサイト(英語: アカウント登録が必要です)

<https://devcentral.f5.com/>

F5 公式販売代理店リスト

[https://www.f5.com/ja\\_jp/partners/jp-find-a-partner](https://www.f5.com/ja_jp/partners/jp-find-a-partner)

以上

更新日: 2019-10-15

---

本資料は設計・構築を補助するための情報提供を目的としています。内容についてできる限り正確を期すよう努めてはおりますが、いかなる明示または暗黙の保証も責任も負いかねます。本資料の情報は、使用先の責任において使用されるべきものであることをあらかじめご了承ください。この文書に記載された製品の仕様、ならびに動作に関しては各社ともにこれらを予告なく変更する場合があります。F5 製品の各機能やコマンドに関する正式な情報に関しては AskF5(<https://support.f5.com/>)の対応するハードウェアプラットフォーム、ソフトウェアバージョンに即してご確認ください。

本資料の著作権は、F5 ネットワークスジャパン合同会社にあります。本文中にある製品名は、各社の商標または登録商標です。

---