F5 Advanced WAFによる進化する攻撃からのWebアプリケーション防御

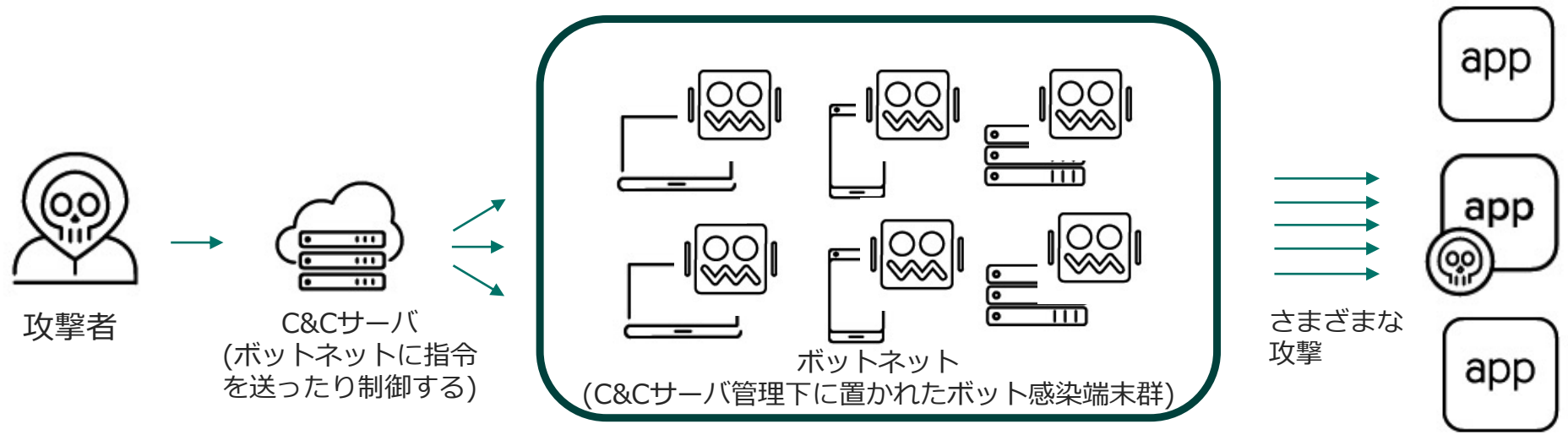
F5 BIG-IP 製品

株式会社 ネットワールド

背景 (1/6)

Background

- **ネット犯罪の裏にボット有り**
  ボットをご存知でしょうか。**ボット**は命令したタスクを自動実行するプログラムの総称です。企業サービスにも利用されており、商品の価格調査、子供のGPS位置確認、サポートサービスでのチャットによる自動応答など、良識を持って使われている事例も多くあります。
  しかしながら、ボットは単純な繰り返し処理を継続的に行うことを得意とし、悪用しやすい特徴があります。悪意ある技術者は、脆弱性のある複数デバイスを乗っ取り、ボットネットを形成し、リモートからボットに指令し、Webサービスに対する**DDoS攻撃**、**不正ログイン**、**クレジットカード情報搾取**といったネット犯罪に利用される事件が発生しております。Webアプリケーション防御において**ボット通信を識別する必要性**は高まっている状況です。



背景 (2/6)

Background

- **脆弱性公開直後の素早い攻撃をどう防ぐか**
  2017年に発生した**Apache Struts 2の脆弱性(CVE-2017-5638)**では、Apacheが脆弱性情報を公開してから、脆弱性を悪用した攻撃が発生するまでの期間が、極めて短く**1日半程度**でありました。脆弱性が判明しても、**パッチを適用するまでに悪用**されてしまえば、Webアプリケーションに深刻な影響が発生してしまう事例となりました。WAFを導入しシグネチャを適用すれば防御可能でしたが、同様にWAFベンダがシグネチャを短期間に開発できなければ、今後も攻撃が成功してしまうことになります。脆弱性が公開されてから、なるべく**短時間に防御できる仕組み**がWAFに求められています。

(日時は日本時間)

日付	時間	事象
2017年3月6日	19時ごろ	Apacheより、S2-045に関する情報が公開される。
2017年3月7日	午前	中国のウェブサイトでPoCが公開される。
2017年3月7日	13時ごろ	中国国内で攻撃を検知。
2017年3月7日	17時ごろ	日本国内で攻撃を検知。
2017年3月7日	21時ごろ	Apacheより、修正バージョンが公開される。
3月7日中にWAFベンダからシグネチャがリリースされた		
2017年3月8日	5時ごろ	保険特約料支払いサイトへの攻撃が発生。
2017年3月8日	11時ごろ	JPCERT/CCより早期警戒情報を公開。
2017年3月8日	14時ごろ	IPAより注意喚起情報を公開。
2017年3月8日	17時ごろ	都税支払いサイトへの攻撃が発生。
2017年3月8日	21時ごろ	Apacheより修正バージョンのアナウンスメール送信。
2017年3月9日	午前	JPCERT/CCが注意喚起を公表。
2017年3月9日	18:00	GMO-PGがS2-045を把握。対象サイトの調査を開始。
2017年3月9日	20:00	GMO-PGにて対象となるシステムの洗い出しが完了。
2017年3月10日	0:30	GMO-PGにて保険特約料支払いサイトと都税支払いサイトへの不正アクセス発生を確認。

Apache Struts 2の脆弱性(CVE-2017-5638)が公開されてから不正アクセスが開始されるまでの時系列
（引用：IPA WAF導入に向けた検討項目　https://www.ipa.go.jp/files/000072484.pdf）

背景 (3/6)

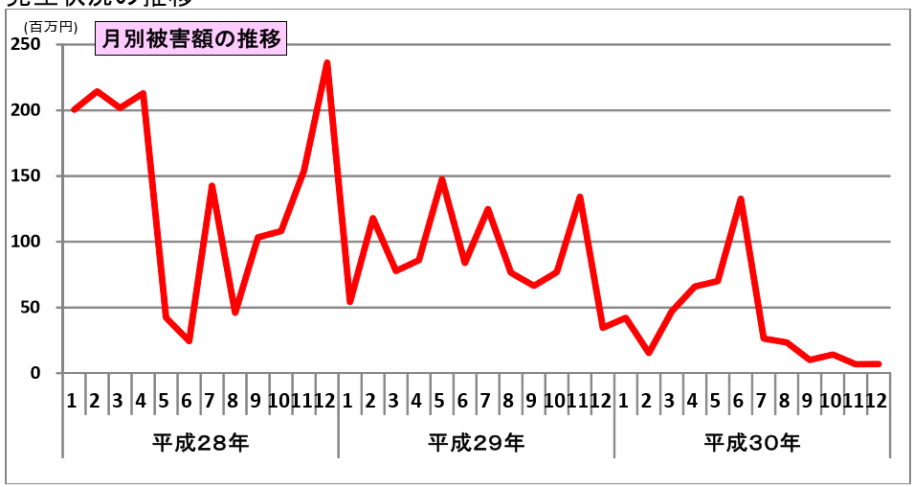
Background

- **WEBサイトの認証情報窃取マルウェア**
  毎日のようにマルウェア感染被害のニュースを耳にします。標的型攻撃による端末側のマルウェアも巧妙になり、感染に気づかずにWebページで入力したID/パスワードやクレジットカード情報等が抜き取られて、**インターネットバンキング不正送金**に利用される事件も発生しています。システム側で根本的な解決ができないものでしょうか。もっとWebシステムでの**アカウント情報の取り扱いのセキュリティを高めたい**という要望がございます。

引用：一般財団法人日本サイバー犯罪対策センター　マルウェア情報
https://www.jc3.or.jp/

3　インターネットバンキングに係る不正送金事犯の発生状況等

（1）発生状況の推移



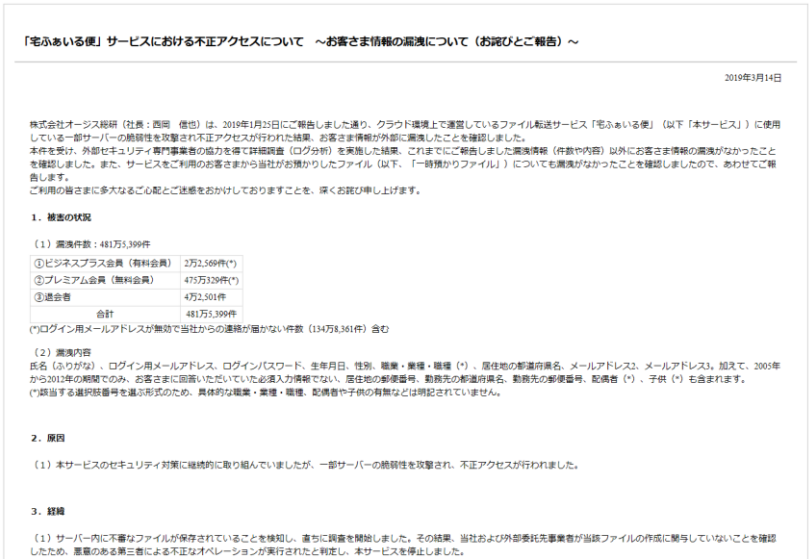
引用：警察庁　平成30年におけるサイバー空間の脅威の情勢等について
https://www.npa.go.jp/publications/statistics/cybersecurity/data/H30_cyber_jousei.pdf

背景 (4/6)

Background

- **ユーザアカウント情報の流出攻撃多発**
  毎月のように**ユーザアカウント情報の流出事件**をニュースで聞きます。**不正に取得されたユーザアカウント情報**は、他のWebサービスへの攻撃に利用されます。ボットによるスタッフィング（総当たり的に検証する）＝不正ログインを繰り返し試み、アクセス権を取得する攻撃を行います。クレデンシャルスタッフィング攻撃の成功率は一般的に**1～2%**はあると言われています。WAF側でも**クレデンシャルスタッフィング攻撃**への対策が必要となっております。

引用：株式会社 ファーストリテイリング グループ企業ニュース



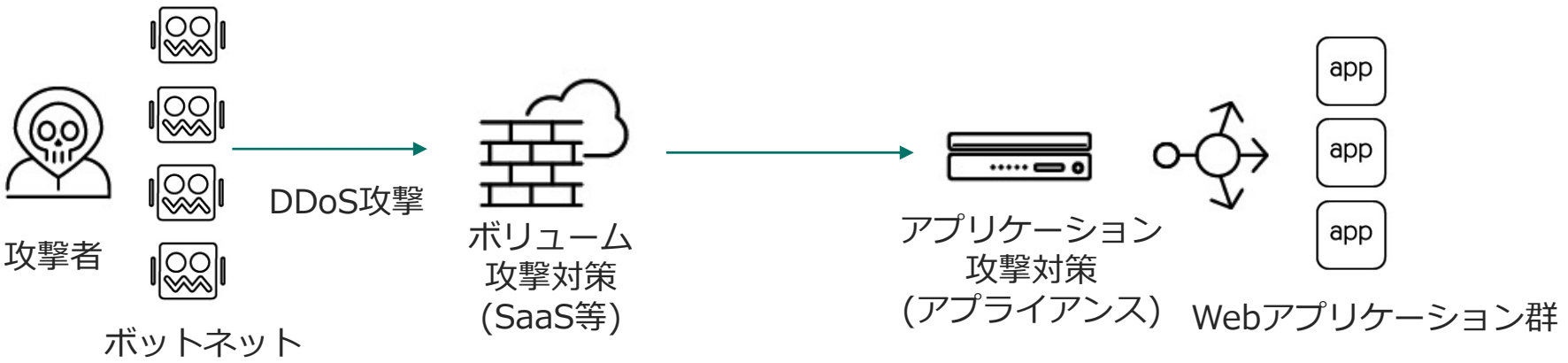
引用：株式会社オージス総研　お知らせ

引用：Facebook newsroom
セキュリティに関する重大なアップデート

背景 (5/6)

Background

- **多様化するDDoS攻撃**
  DDoS攻撃は大量のトラフィックによりサービスに負荷をかけて停止に追い込む攻撃です。
  しかしながら、実はその攻撃手法が**巧妙化**して、単純な通信量を増加させるネットワークおよびトランスポートレイヤー(L3 or L4) の攻撃からアプリケーションレイヤーにシフトし、L7プロトコルの利用した攻撃に変化してきています。
  HTTP GET Flood、Slow HTTP DoS Attackといった攻撃手法は、1つのTCPコネクション内でサーバへ負荷をかけるHTTP通信を繰り返す手法であるため、従来型のDDoS対策では検知できず、**HTTPプロトコル**を理解し、**ふるまい異常を検知**できなくてはなりません。攻撃の手法の進化にあわせて、**多層型防御(ボリューム攻撃対策+アプリケーション攻撃対策)**に変わっていく必要があります。



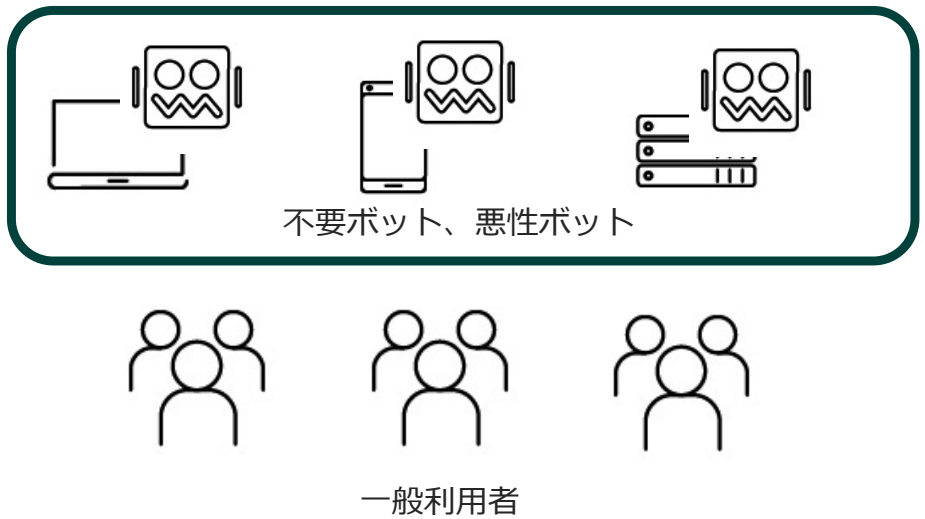
背景 (6/6)

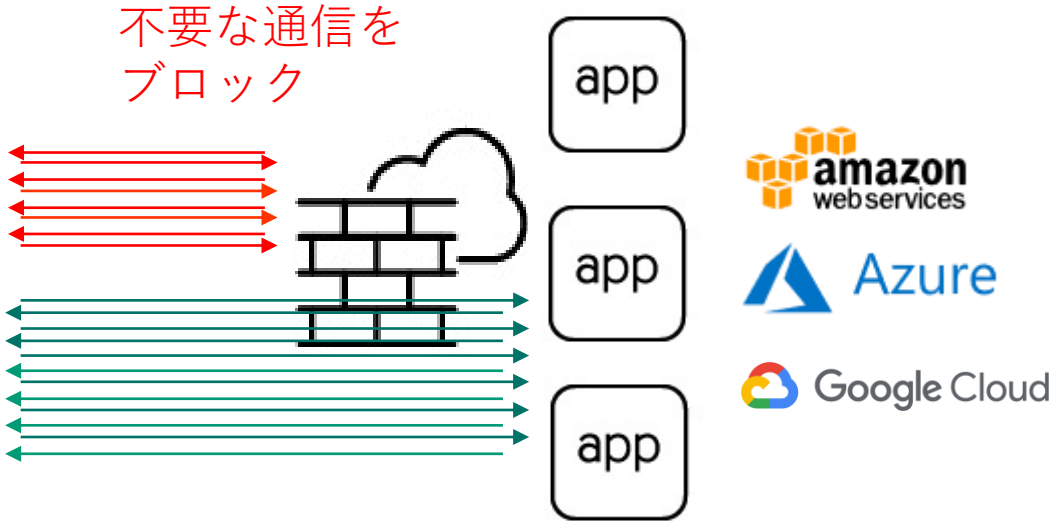
Background

- **ボットによって消費されるレスポンスデータ転送量によるクラウドサービス利用料**

ボットによって目には見えない**クラウドサービス利用料金**が掛かっていることをご存知でしょうか。一般的なクラウドサービスは、HTTPレスポンスデータ転送量に応じて料金が請求されております。ボットによるWebサービスへの通信量の**10～40%**になるという、試算がございます。

不要ボットや悪性ボットの通信を識別し、クラウドサービスの入り口で**ブロック**することが出来たら、クラウドの**コスト削減**を実現できます。長期間のコスト削減額を考えたら、WAF導入は効果的な投資になるのではないでしょうか。





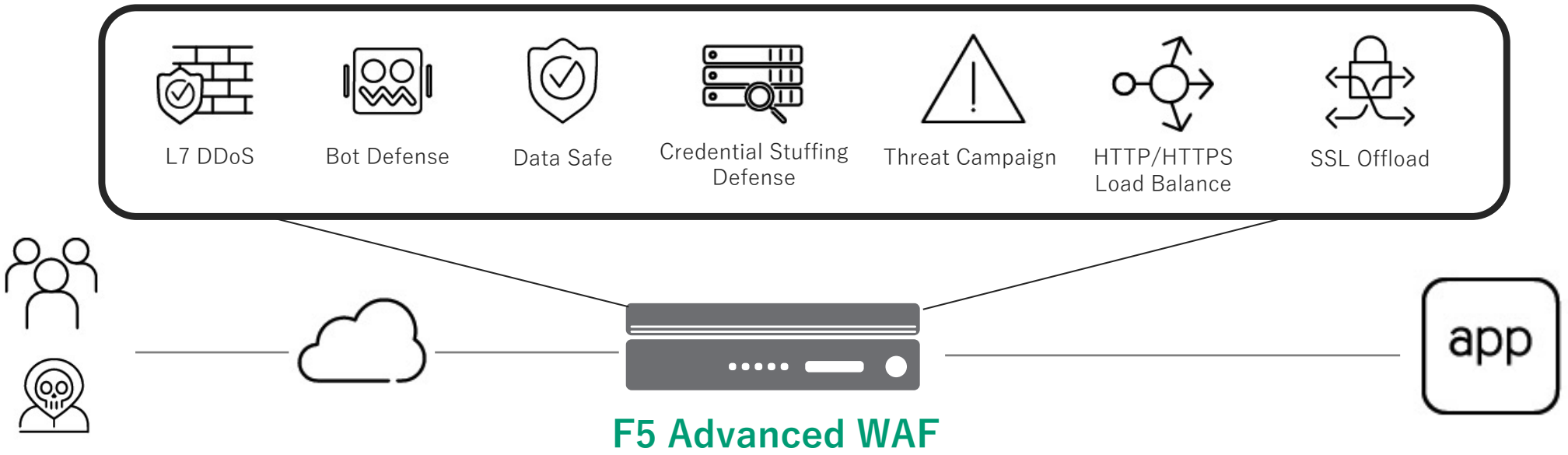
F5 Advanced WAF
– 概要/特徴 –

概要

Overview

- **F5 Advanced WAF(AWAF)**とは、BIG-IP製品で実績のあるWAF機能(ASM)に、**進化する脅威**に対応するため、独自で先進的な検知、防御機能を実装した新しいWAF製品になります。

　LTMで実績と信頼性の高い拡張された**HTTP負荷分散**+**SSL処理**機能も標準装備しており、Webアプリケーション環境でWeb Application Firewallとして**オールインワン**で利用できる製品となっております。



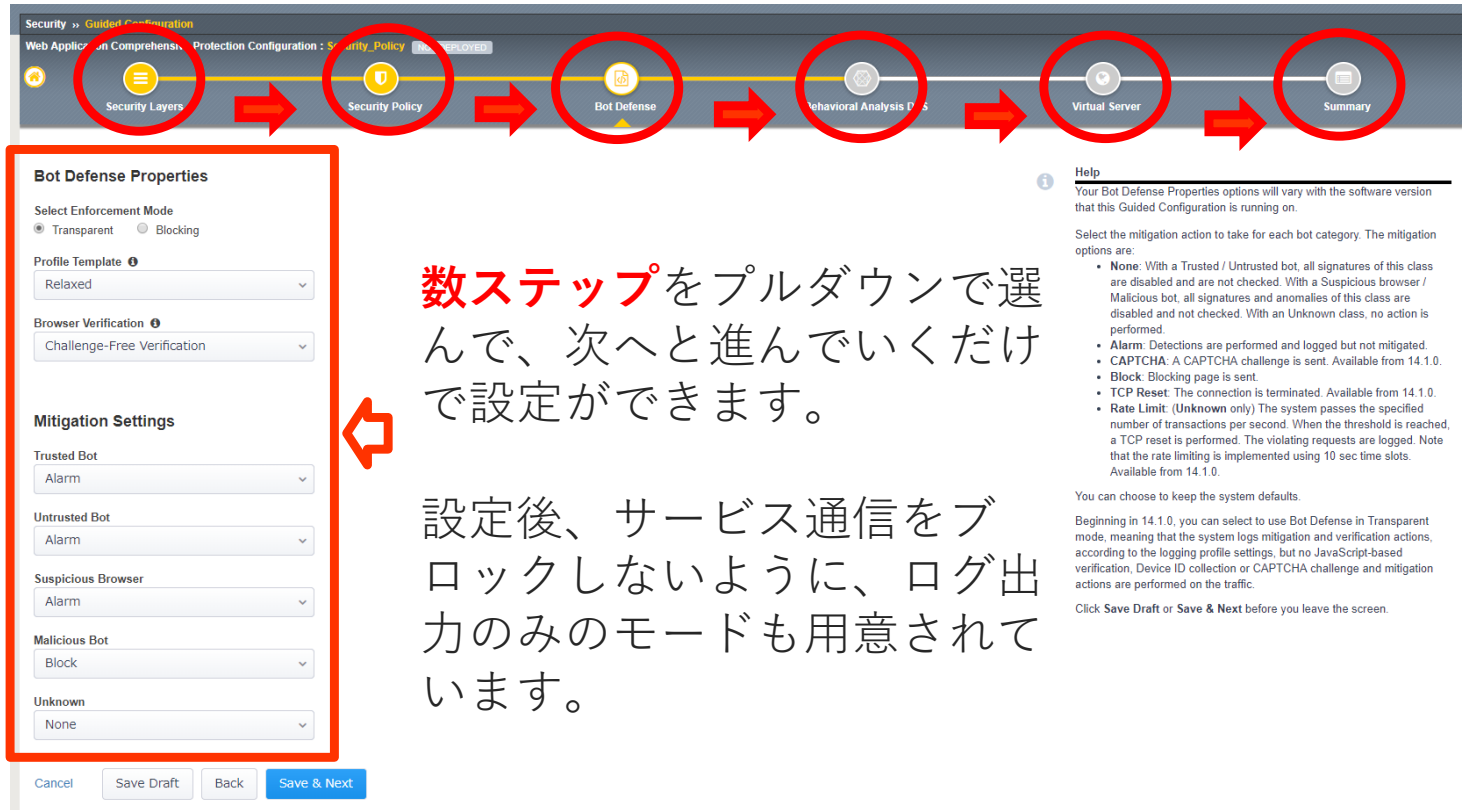
特徴（1/6）

Features

AWAF限定

- **WAF Guided Configuration：かんたんセットアップ**

  カテゴリされた機能に対してステップ化された設定を行うことでVirtual Serverや各種Profile, Security Policyが自動作成されます。WAF設定を行ったことのないアプリケーション管理者でも設定が行えます。
  短時間にセットアップを行いたいユーザへメーカ作成のテンプレート設定が用意されております。



数ステップをプルダウンで選んで、次へと進んでいくだけで設定ができます。

設定後、サービス通信をブロックしないように、ログ出力のみのモードも用意されています。

特徴（2/6）

Features

AWAF限定

サブスクリプション

- **Bot Signatures：ボット専用シグネチャ**

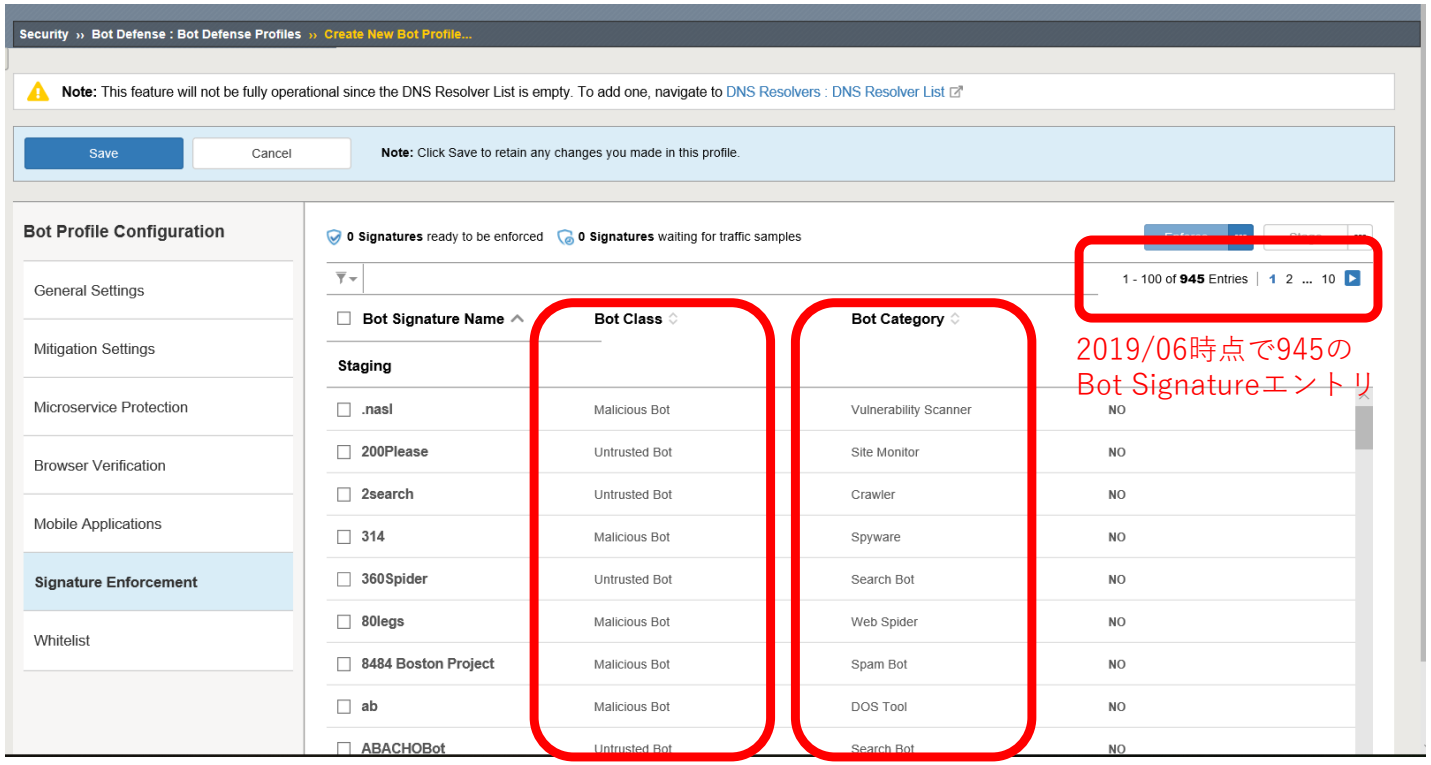
HTTPリクエスト ヘッダー内の特定のパターンを探すことによってボットを識別するシグネチャとなります。シグニチャは分類および調査目的のためにボットの種類を識別し、良性ボットと悪性ボットを区別しております。

①良性ボット:検索エンジンボット、インデックスクローラ、サイトモニタ

②悪性ボット：電子メールアドレスの収集、スパムの生成、スパイウェア、DoS Tool

ボット毎に許可/不許可を定義して、Virtual Serverへ適用することが可能です。

(※Bot Signatureの防御メカニズムでは、DNSの逆引き参照を利用するため、DNSサーバとDNSリゾルバの設定が必要となります。)



特徴（3/6）

Features

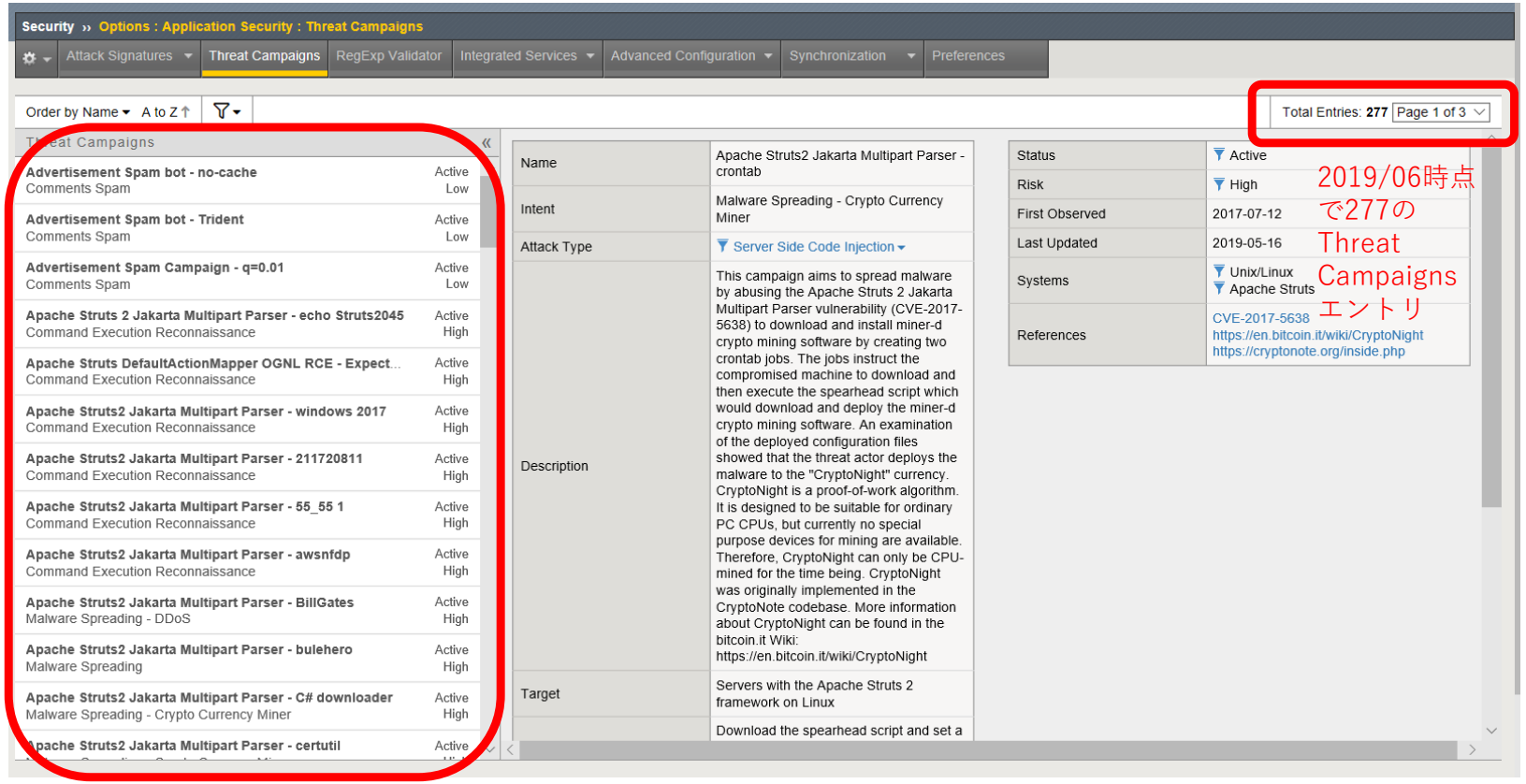
AWAF限定

サブスクリプション

- **Threat Campaigns Signatures: 緊急対策シグネチャ**

F5脆弱性専門チームがハニーポット等を用いて、現在進行形で世の中に流行している緊急性の高い攻撃のシグネチャを作成し、即座に(1日程度)配信するサービス。

誤検知が起こりにくいシグネチャ構造(多角的なポイント)となっているため、即座にブロッキングモードにすることを考えられている。攻撃が改変された場合には、随時シグネチャのアップデートが必要となる。



2019/06時点で277のThreat Campaignsエントリ

対策シグネチャの名前と深刻度を一覧で確認可能

特徴（4/6）

Features

AWAF機能UP

- **Behavioral DoS Protection: 高度なL7DDoS検知防御機能**

Behavioral DoS Protectionとは、機械学習とデータ分析を使用してトラフィックの動作を分析することにより、DDoS攻撃に対する自動保護を提供します。

例えば、ボットネットからのDDoS攻撃の場合、１つ１つのリクエストは完全に正当である可能性がありますが、一度に多数の要求を実行するとサーバーの速度が低下したりクラッシュしたりする可能性があります。

下記の機能にてL7 DDoS検知防御を行います。
①動作DoS機能は、サーバーを正常に保つのに疑わしいクライアント通信のトラフィック処理を遅くすることによって攻撃を軽減します。
②行動DoS機能は、リアルタイムの相関関係を確認し、サーバーの状態、攻撃、および緩和を検証するために、全体通信のフィードバックループを使用してサーバーの正常性と負荷を継続的に監視します。その後の異常はすべて監視され、システムは必要に応じて緩和策（スローダウンまたはブロック）を適用します。

特徴（5/6）

Features

ASM/AWAF共通

V14.1以降サポート

- **TLS fingerprint: 高度なTLSハンドシェイク攻撃防御機能**

TLS fingerprint機能とは、TLSハンドシェイクで見つかったシグニチャパターンの異常を識別し、特定のシグニチャパターンと一致するトラフィックをドロップする攻撃の検出および軽減機能です。
例えば、元々暗号スイート（RSAなど）を使用すると、少数のクライアントでTLS攻撃を行うとサーバ攻撃を効果的に実行できてしまいます。これは、ハンドシェイクの計算コストはクライアントよりもサーバーの方がかなり高くなるためです。

TLS fingerprint機能により、暗号化されたセッションのTLSハンドシェイクを完了するというオーバーヘッド処理無しで、DDoS攻撃を識別することができます。 TLSフィンガープリントを有効にすると、フィンガープリントエンジンはClient Helloメッセージを解析して、以下のハンドシェイクパラメータで異常を検知します。

①TLS version
②Cipher suites
③Compression options
④TLS extensions
⑤Elliptic curve extensions

特徴（6/6）

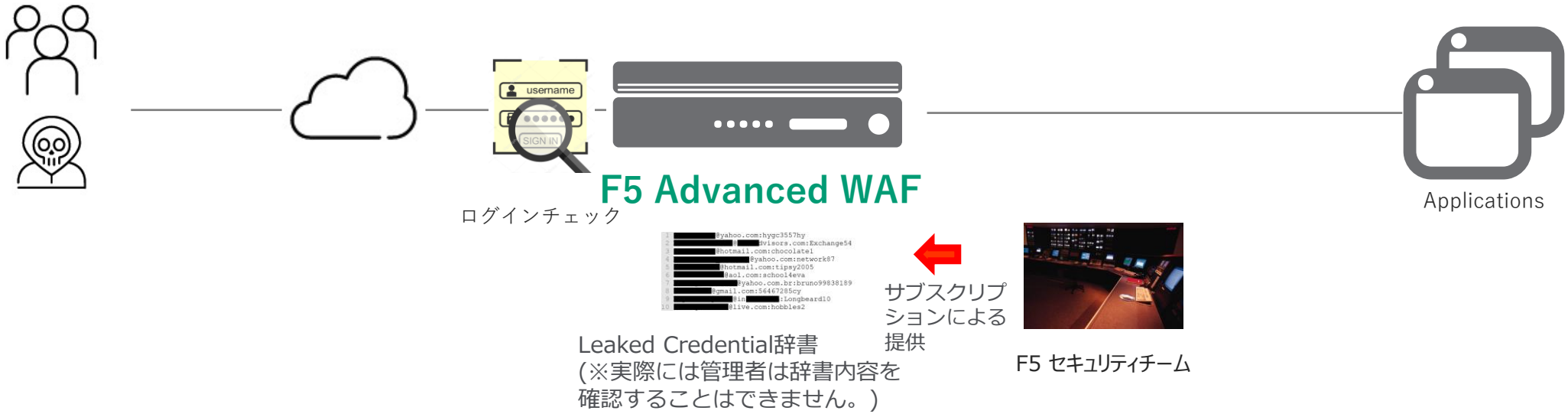
Features

AWAF限定

サブスクリプション

- **Credential Stuffing Protection: パスワードリスト型攻撃対策(リリース予定)**

Credential Stuffing Protection機能とは、F5独自に収集したLeaked Credential辞書(流出ID/パスワード)と、システムのログインにユーザID/パスワードが利用されるかチェックしており、使われた場合に警告と防御を行う機能です。



F5 Advanced WAF
– 構成例 –

構成例①

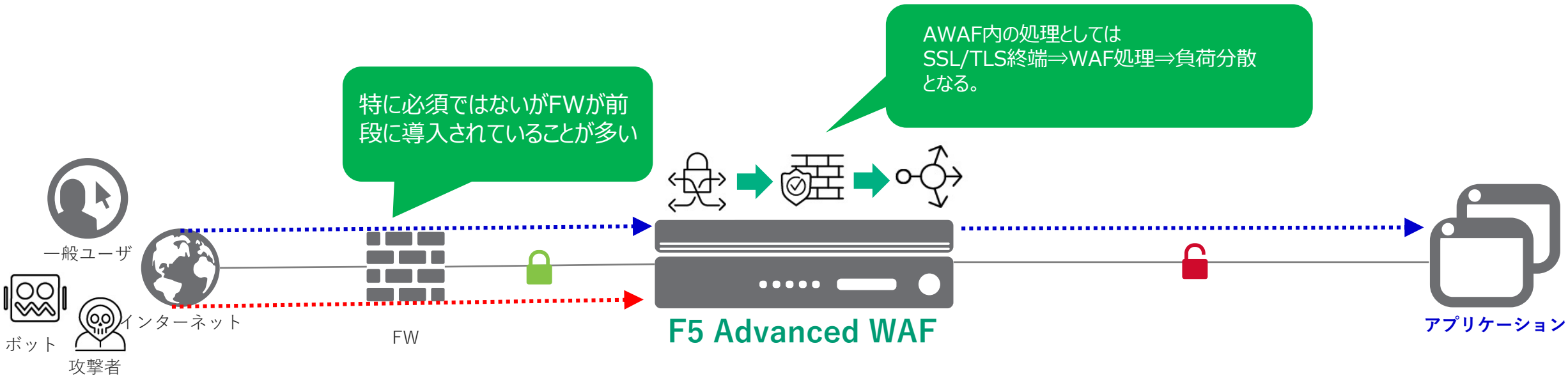
AWAF: フルプロキシ基本構成

Advanced WAF

- クライアントとサーバ間にインラインでAWAFを導入する構成(ワンアーム折り返しも可能)

メリット：従来のLTMにWAF機能がそのまま付加されるためトラフィックフローを理解しやすい。
：AWAFのすべての機能でアプリケーションを防御可能。
：アプリケーションへのすべての通信がAWAFとなるためセキュアな構成となる。

デメリット：AWAFが新規IPアドレスを持つことになるため、ネットワーク構成変更となることが多い。
：機器故障時に備えて冗長構成で導入が必須となる。



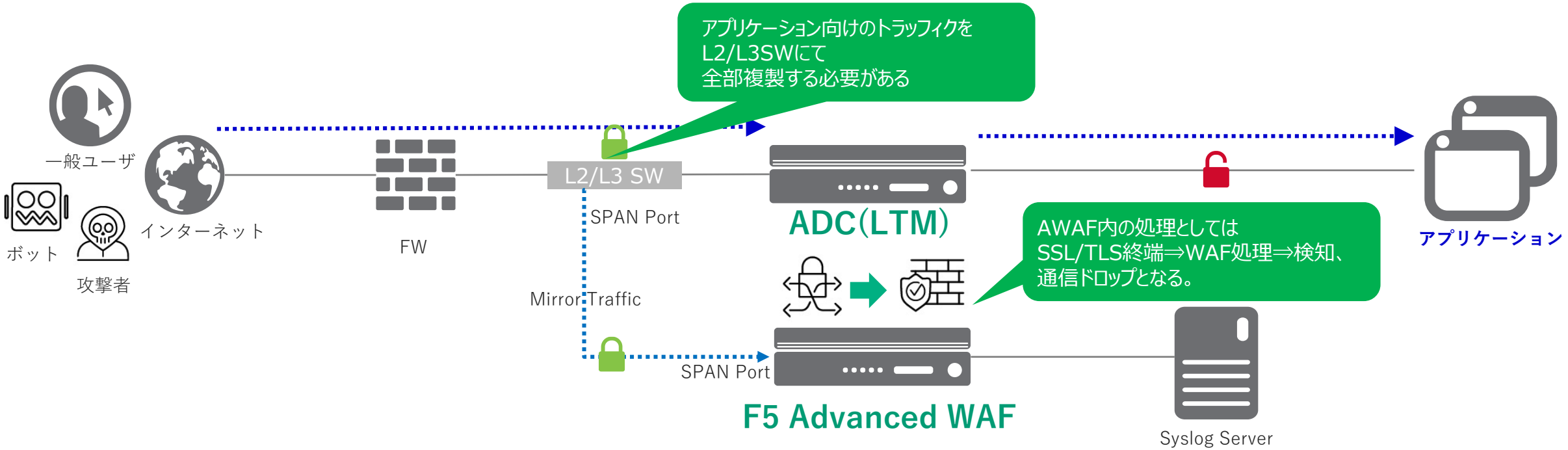
構成例②

AWAF: Passive Monitoring構成

Advanced WAF

- 複製したトラッフィクをAWAFで分析し、Syslogサーバへログ送付のみ実施する構成(検知のみ)

メリット：サービス通信をWAFに通過させない構成のため、誤検知によるサービス影響が無い。
　　：既存L2/L3SWがあればネットワーク構成を変更せずに導入が可能。
デメリット：AWAFは検知のみであるため、一部の機能が利用できない(バージョンによる差あり)
　　：シングル構成のみサポート可能。



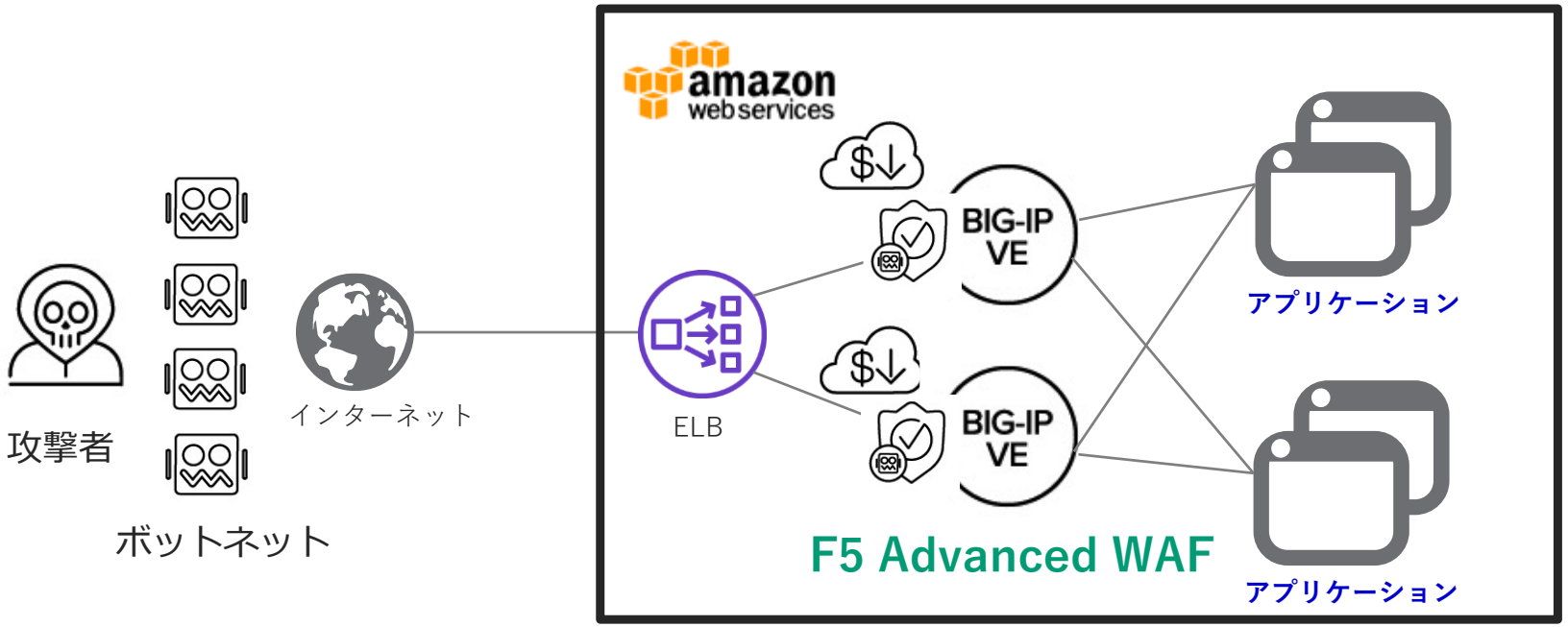
構成例③

AWAF: パブリッククラウドでのボットトラッフィク対策

Advanced WAF

- パブリッククラウド環境でELB配下にBIG-IP VEとして構築(ボット通信ブロック目的)

メリット：ボット通信をAWAFでブロックすることで、レスポンスデータ量に対して課金される
　　クラウドサービス利用料が下げられる。(もちろん同時にWAFでのセキュリティ対策も可能。)
　　：BIG-IPライセンスについても、BYOL(持ち込み)だけではなく従量課金(サービス)選択も可能。
デメリット：ハードウェアアプライアンスに比べて、コストパフォーマンスは低い。



F5 Advanced WAF
– その他 –

機種選定や動作検証について

Model selection and Verification

・**機種選定**については、お客様がご利用予定のスループット、SSL処理性能及びネットワーク構成やトラフィックフローによって必要となるスペックが異なるため、都度、ご相談頂きたいと考えております。

お気軽にお問合せ窓口にご相談ください。

・**動作検証**については、無償にてAWAF貸出検証機で実施が可能です。クラウド環境での仮想アプライアンスでの評価用ライセンスを試したい場合も、お気軽にお問合せ窓口にご相談ください。

お客様からよくあるご質問

ARU ARU

Q. AWAFの負荷分散機能での制限事項を教えてください。

A. HTTP 用途のLoad Balancing Method(Round Robin, Ratio, Least Connections, Weighted Least Connections, Ratio Least Connections)、Persistence(Cookie, Source Address, Host, Destination Address)をサポートしております。それ以外についてはサポートしておりません。
UDP Profileはご利用できません。L4負荷分散は可能です。

Q. HA構成は可能ですか。

A. はい。Active-Standbyモードをサポートしております。

Q. AWAFでサブスクリプションライセンスが必要な機能を教えてください。

A. IP intelligence(IPI), Credential Stuffing DB, Threat Campaign Signatureについては、
サブスクリプションライセンス(1年、3年)の購入が必要となります。
Anti Mobile SDKについては、Add-on ライセンスとしての購入となります。

Q. AWAFでは、iRulesは使えますでしょうか。

A. はい。iRulesは通常通りご利用可能です。ただし、HTTP負荷分散用途以外の構文についてはご利用する前に検証することをお奨めいたします。

本資料に関するご相談・ご質問などございましたらご連絡お待ちしております。

f5-info@networld.co.jp