クラウドネイティブなWebアプリケーションのセキュリティ設計

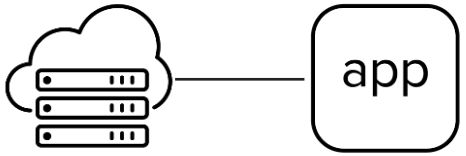
東京エレクトロン デバイス株式会社

近年のアプリケーションについて

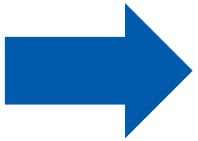
複雑化するアプリケーション

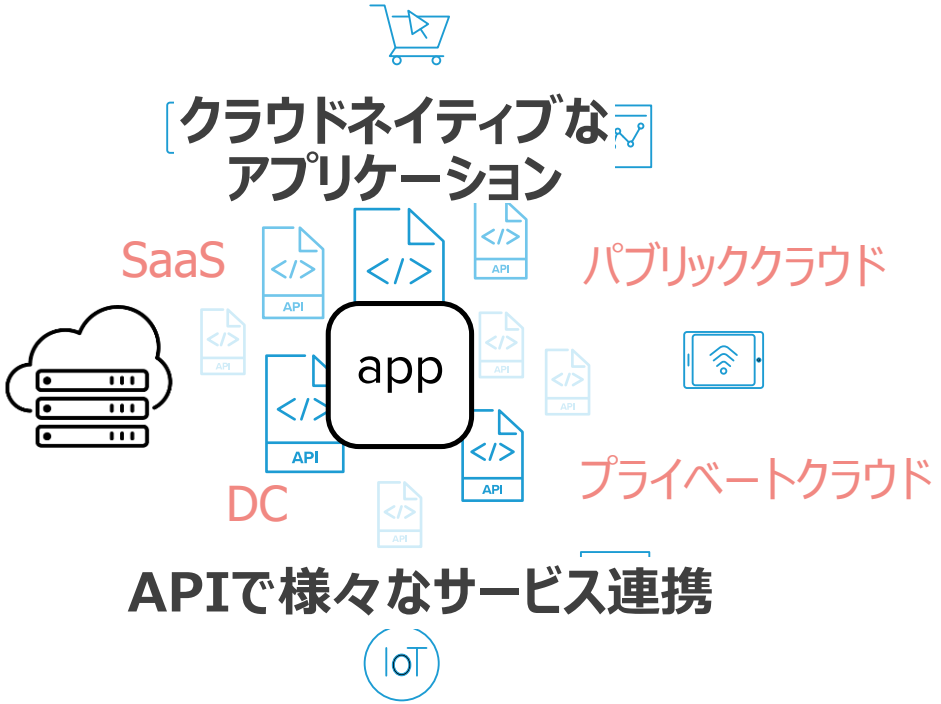
モノリシックなアーキテクチャからマイクロサービス化されたアーキテクチャへ

従来のアプリケーション



バックエンドサーバー連携





APIアーキテクチャが主流に

WAAP(Web Application and API Protection)とは

2017年に提唱された次世代のWebセキュリティ概念

Webアプリケーションやモバイルアプリでの API利用の増加に伴い、近年高度化するサイバー攻撃に対して
従来型のWAFだけでは対策は不十分
→APIの保護も考慮したセキュリティ対策が必要

WAAPをWAF市場の進化として定義し、以下の機能をコアとする。

DDoS対策	ネットワーク及びアプリケーションレベルのリソース保護
次世代WAF	アタックシグネチャ自動更新、クライアントの振る舞い学習
Bot対応	Bot及びツールの検証。振る舞いを把握し悪意のあるBotを検知
API保護	APIディスカバリとリクエスト毎の異常確認

クラウドネイティブなアプリケーションのセキュリテイの課題

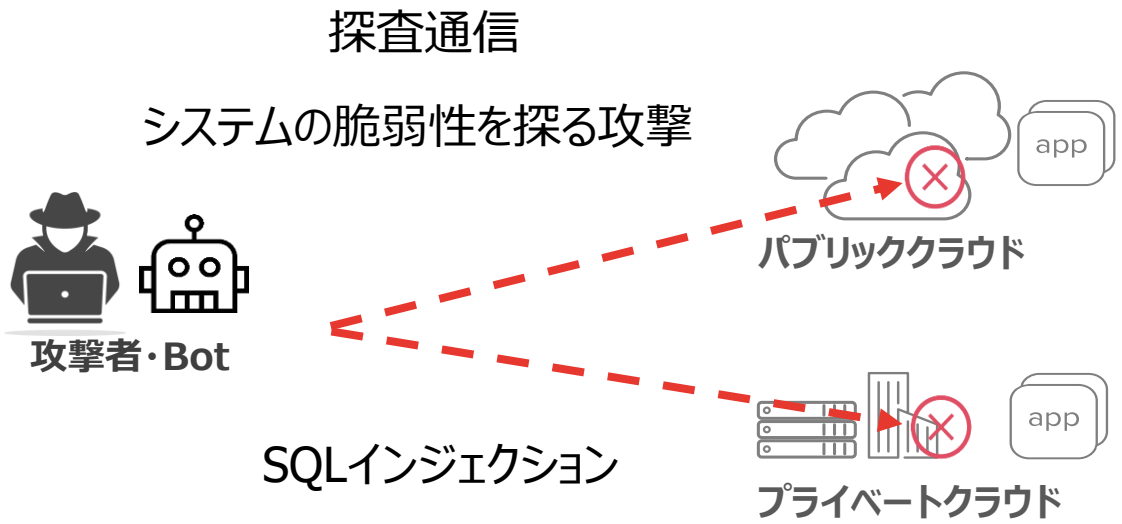
クラウドネイティブなアプリケーションのセキュリテイ

アプリケーション側（サーバー）でセキュリティ対策しているから大丈夫？

それでは不十分

なぜなら

- 攻撃がアプリ（サーバー）まで届いてしまうことも問題
  - 探査通信が行われ、脆弱性を探られてしまう
  - 攻撃をブロックするのにサーバーのリソースが使われる
  - DDoS攻撃をうけることで、環境内の帯域が圧迫される
- 新しい脅威や未知の脆弱性に対して、即時対応が困難
  - 新しい脅威が発生する度に、対応が必要



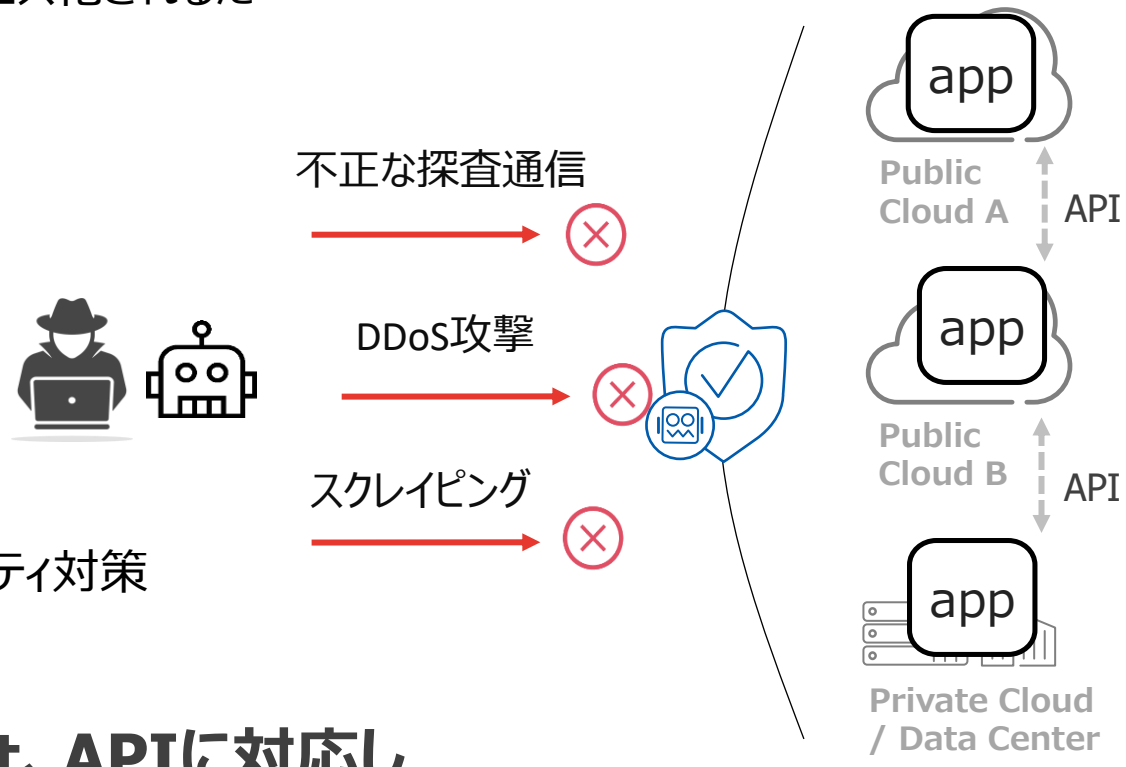
アプリケーション（サーバー）に攻撃が届かないようにするべき

クラウドネイティブなアプリケーションのセキュリテイ

どのようにアプリケーションを保護するか

クラウドネイティブなアプリケーションは、個々の機能がマイクロサービス化されるため、保護する環境が増えることを踏まえて、以下を考慮する

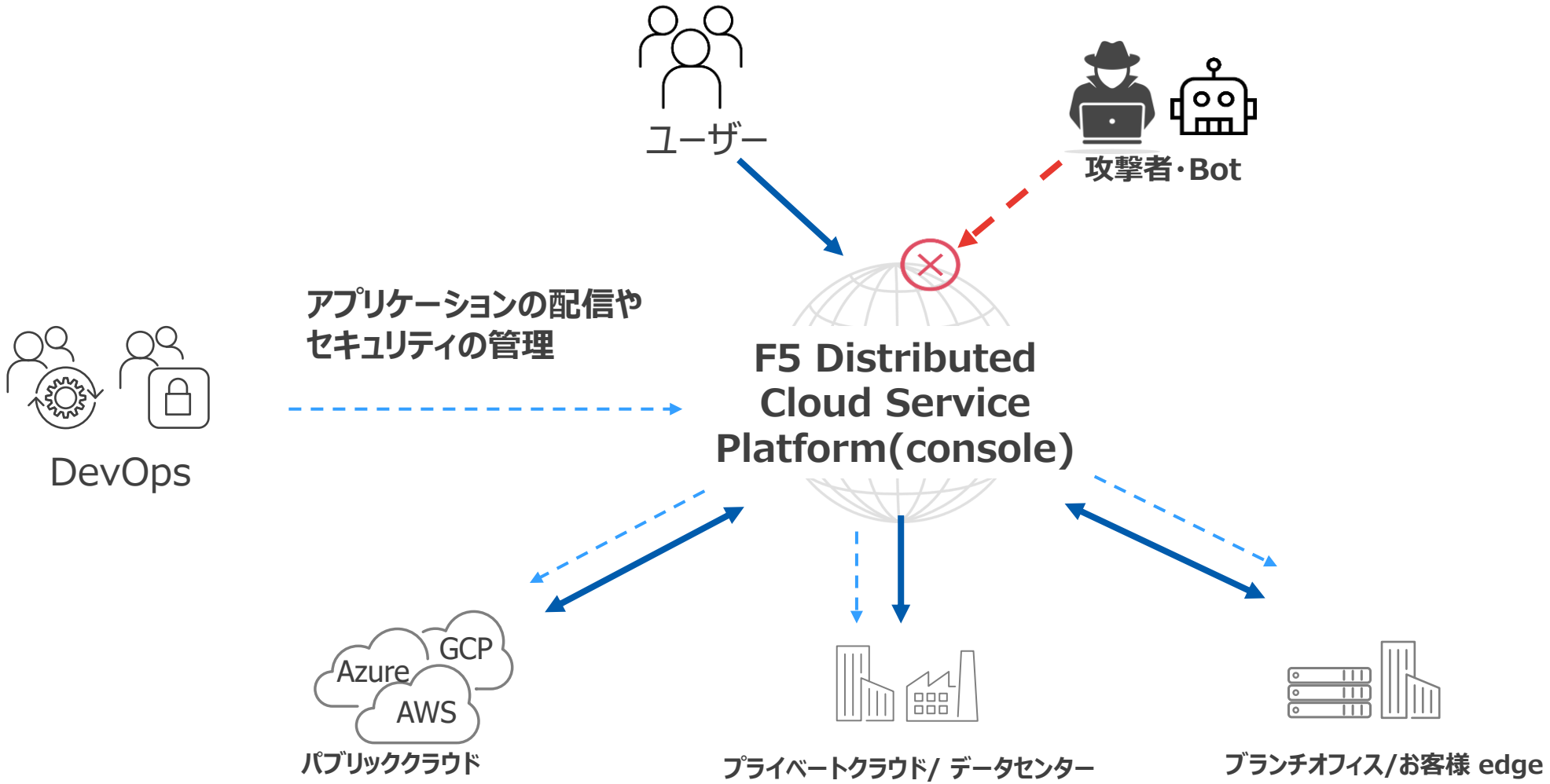
- 全ての環境のセキュリティポリシーを一元管理
- 各環境に攻撃通信を侵入させない
  - 帯域課金やリソースの消費
  - 探査通信をさせない
- WAFだけでなく、DDoS、Bot、API保護など包括的なセキュリティ対策



WAF、DDoS、Bot、APIに対応し
クラウドネイティブなアーキテクチャ（細分化されたサービスを包括的に守れる）セキュリティ対策が必要

クラウドネイティブなソリューション

F5 Distributed Cloud Services（F5 XC）で アプリケーションを保護・展開

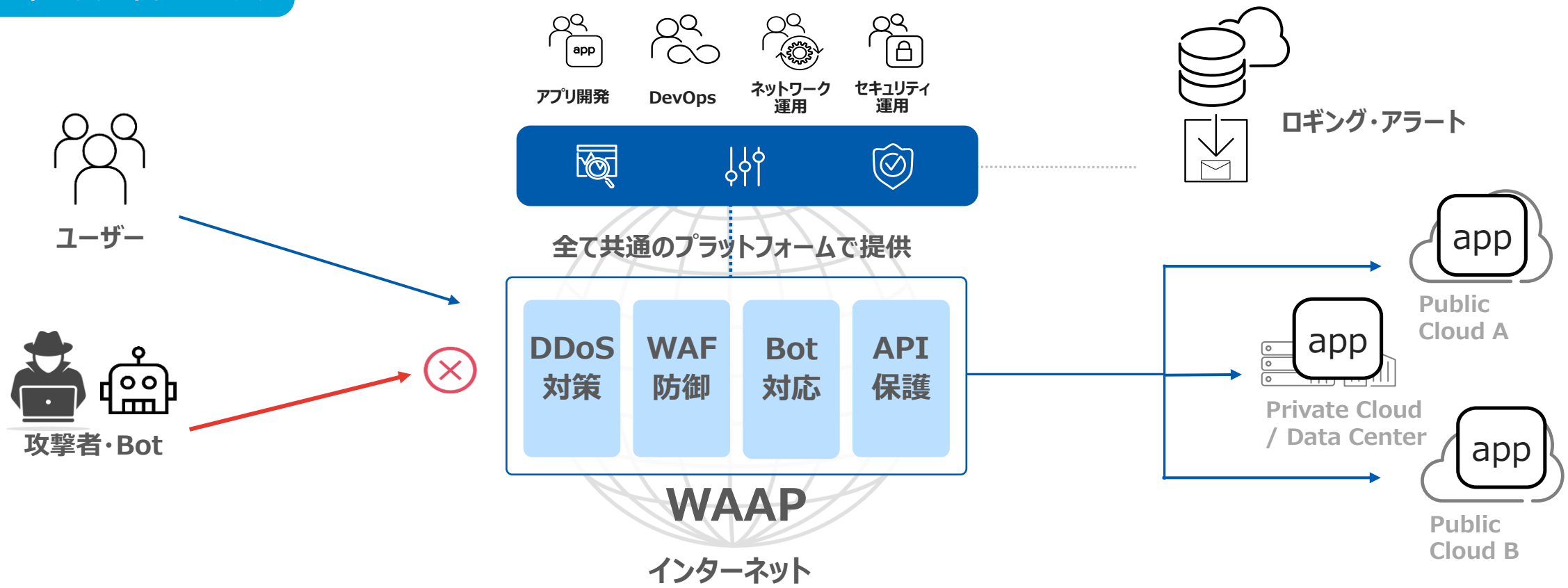


すべてのアプリケーションをF5 XC で統合管理

F5 XC WAAPについて

SaaS型
セキュリティサービス

クラウドネイティブなアーキテクチャ（細分化されたサービス）に対応したソリューション



1 WAF、Bot、DDoS対策をワンパッケージで提供

2 パッケージの帯域課金なし

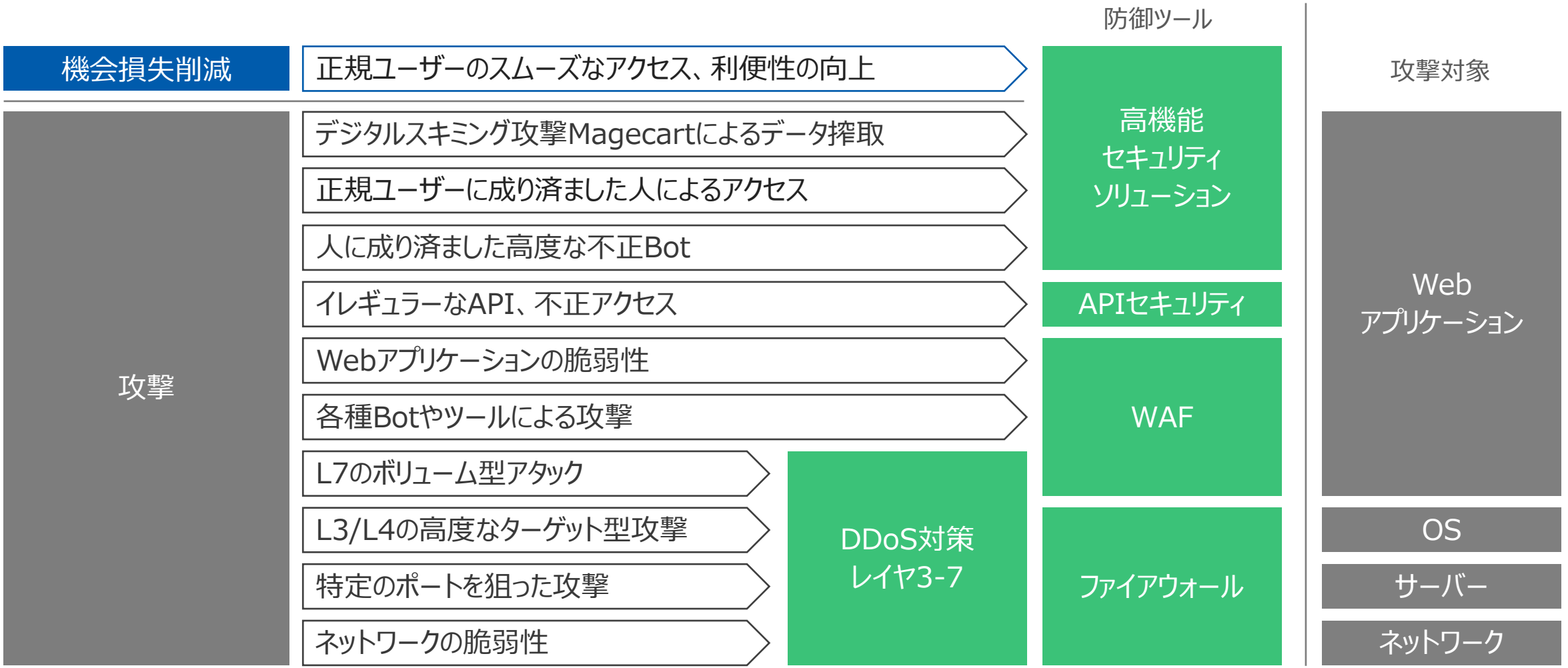
3 実績豊富なBIG-IP AWAFエンジンを搭載

4 機械学習による誤検知の自動削減を実現

F5 XC WAAPの階層型セキュリティ対策

全レイヤのセキュリティ機能を一つのコンソールで管理

使用当初は不要でも、問題発生時にすぐ使えることが重要です。



F5 XC WAAPの各機能について

F5XC DDoS対応ネットワーク

DDoSを最寄りのデータセンターで防御
日本においては、東京と大阪にスクラビングセンターを設置

DDoS攻撃がお客様サイトに届く前に止める仕組み

F5 XC WAFの特徴

常に最新のシグネチャーが適用されるWAFポリシー

1 攻撃検知・誤検知削減

- 実績豊富なBIG-IPのAWAFエンジンを採用
- 機械学習により誤検知を削減

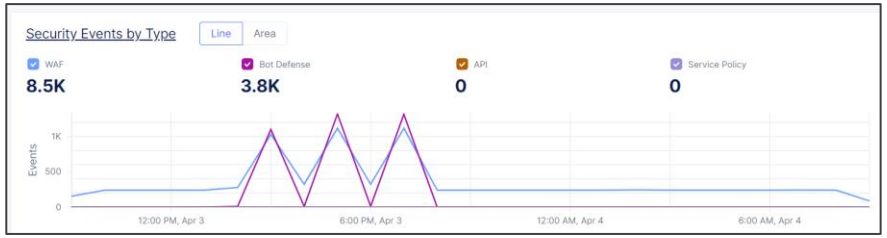
2 豊富なログと見やすいモニタリング画面

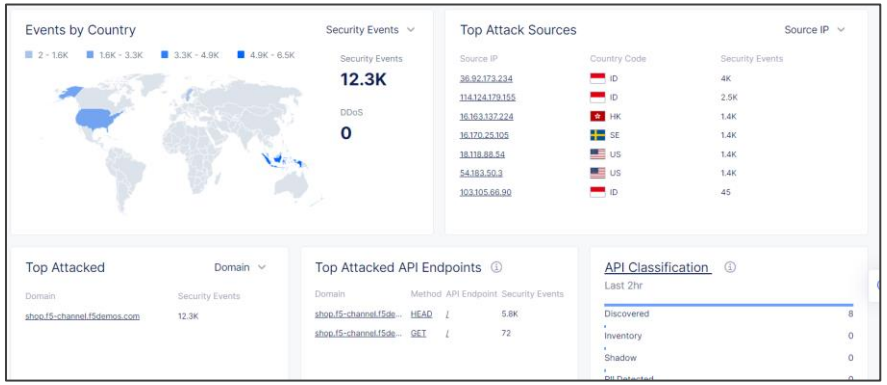
- ユーザーフレンドリーで見やすい管理画面
- ログ解析に必要なデータを提供

3 柔軟なWAF無効設定で誤検知を低減

- 管理画面のログからワンクリックで誤検知を解除
- 特定のシグネチャや攻撃タイプ毎にWAF無効
- 誤検知レベル毎のWAFポリシー有効化の設定

WAFの管理画面（サマリー）





管理画面のログ
ログを見ながら容易に除外ルールを適用

Signature ID 200100015

name	.htaccess access
attack_type	ATTACK_TYPE_INFORMATION_LEAKAGE
accuracy	high_accuracy
context	request
matching_info	Matched 9 characters on offset 7 against value: '/icons/.htaccess'.
state	Enabled

F5 XC Bot対策の特徴

- **シグネチャベースのBot保護**
- **Shape Bot DefenseによるBot検知機能の強化**

Bot検知と脅威の軽減
自動化された人間以外の攻撃を特定
Java ScriptやSDKで、キーボード入力やマウスの挙動などのデータ収集し、人の動きを装ったBotの攻撃から保護

悪意のあるボット種
ブラウザ以外のアクセス
トロイの木馬
バックドア
スパイウェア
脆弱性スキャン
DoS攻撃

様々なツール

adsarobot	DSurf15a
agdm79@mail.ru	EBrowse
BecomeBot	Educate Search VxB
BigCliqueBOT	EmailSpider
CheeseBot	ESurf15a
mailto:craftbot@yahoo.com	Fetch API Request
Nokia-WAPToolkit.* googlebot	Franklin Locator
Shockwave Flash" spam bot	FSurf15a
WISEbot"	Full Web Bot
Atomic_Email_Hunter	IBM EVV
atSpider	Indy Library
Bork-edition	ISC Systems iRc Search 2.1
bwh3_user_agent	Jorgee
China Local Browse	MFC_Tear_Sample
compatible ;	panscient.com
ContactBot	Wells Search II
ContentSmartz	WEP Search
DBrowse	その他…

F5分散クラウド

Bot検知

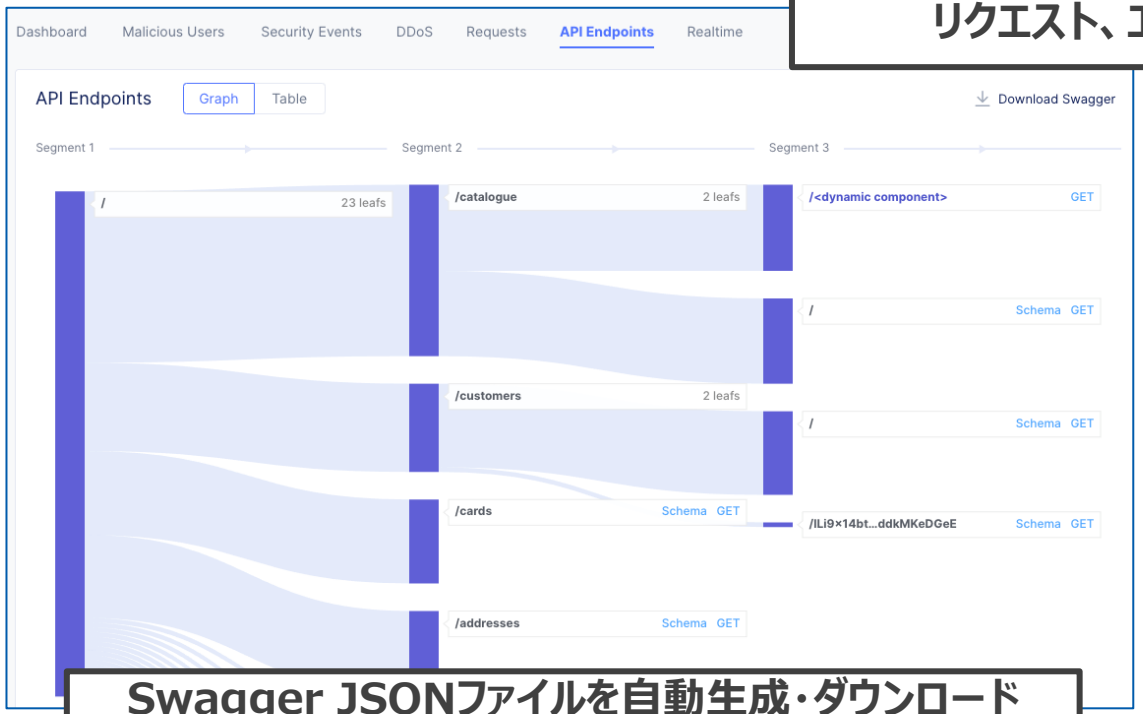
シグネチャデータベース

脅威レベルと対処を定義	
レベル	対処（例）
高	ブロック
中	レポート
低	無視

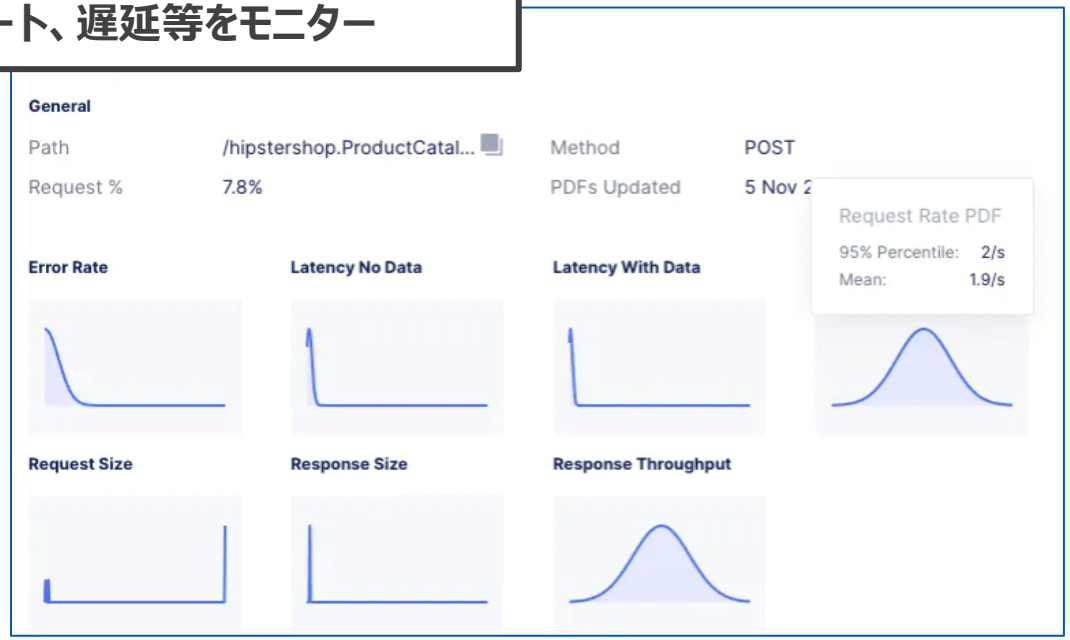
F5 XC API保護の特徴

機械学習を用いた動的なAPIエンドポイントの把握
- APIの発見と異常アクセスの可視化
Open API定義ファイルをベースとした、セキュリティポリシーの適用

サービス間のAPI連携、スキーマ構造を学習し可視化
リクエスト、エラーレート、遅延等をモニター

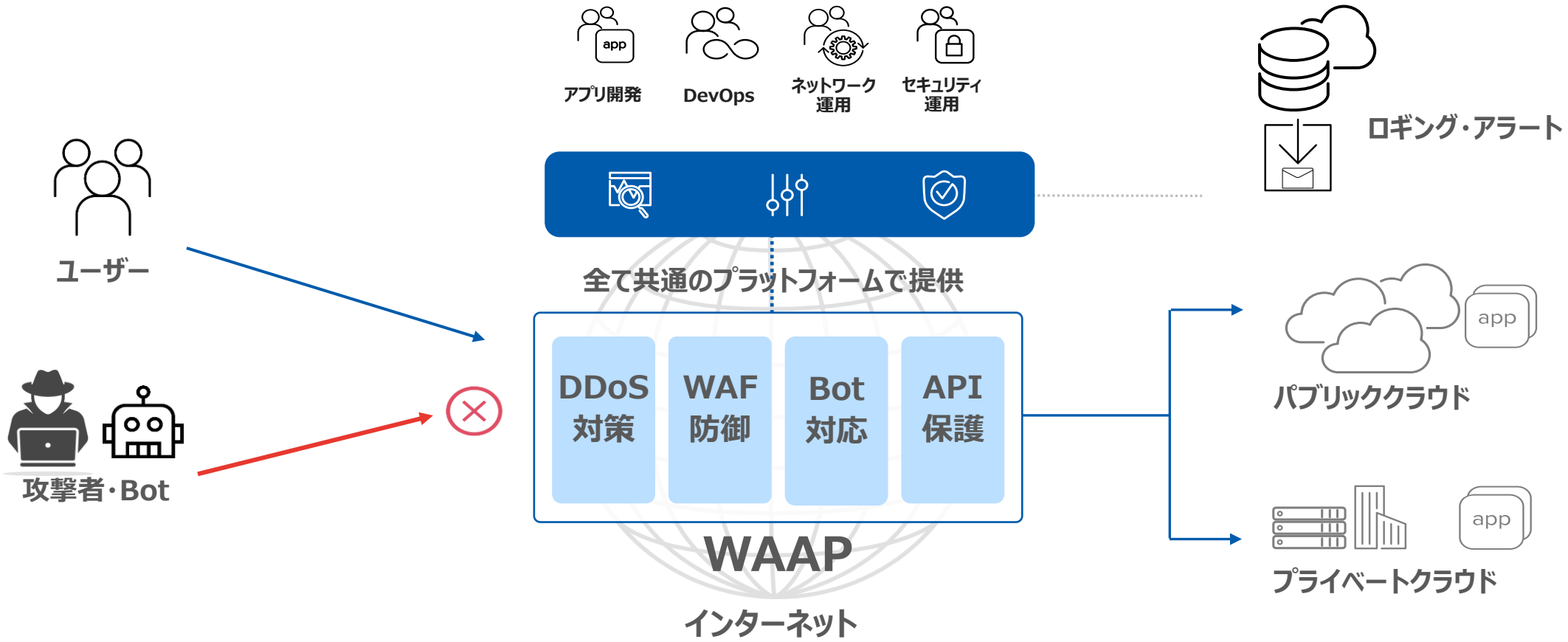


Swagger JSONファイルを自動生成・ダウンロード
Editorを使いAPIドキュメントの作成に利用可



リクエスト・レスポンスサイズ、受信遅延値、
リクエスト・エラーレートの異常検知

F5 XC WAAPでクラウドネイティブなアプリケーションを保護



1 常に最新のセキュリティポリシーが適用される

2 攻撃通信が自社環境に入ってくる前に止める

3 セキュリティポリシーの一元管理

4 DDoS、Bot、API保護なども含めた対策

まとめ

まとめ

- クラウドネイティブなアプリケーションを保護するためには、SaaS型のセキュリティソリューションの導入が有効
- 攻撃通信をお客様の環境に届けないような仕組みすることが大事
- F5 XC WAAPはGartnerにより提唱された次世代のWebセキュリティ概念に準拠したセキュリティソリューション
- DDoS保護、WAF、Bot対策、API保護などの全レイヤーのセキュリティ機能を一括で提供し１つのコンソールで管理可能
- オンプレミス、クラウドに存在するお客様環境のセキュリティを一元的に管理が可能
  - クラウドネイティブなアプリケーションを保護するのに最適