クラウドWAF入門：初心者でも導入・運用できるF5のクラウドWAF（WAAP）ソリューション

東京エレクトロン デバイス株式会社

※本資料に掲載されている会社名・製品・サービス名・ロゴは各社の商標または登録商標です。
また、写真・ロゴマーク・その他の著作物に関する著作権はそれぞれの権利を有する各社に帰属します。

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

自己紹介

所属：

東京エレクトロン デバイス株式会社

CNBU プロダクト第一技術部

熊谷 敦文（くまがい あつふみ）

担当業務：エンジニア

趣味：フットサル、釣り、動画鑑賞（アニメ）、ゲーム、

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

目次

1. クラウドWAFとは

2. クラウドWAFの必要性について

3. WAFの導入ハードル

4. F5 XCのWAAPソリューションについて

※F5 XCとは、F5 Distributed Cloud Servicesの略です

5. 東京エレクトロン デバイス株式会社のサービスメニュー

6. まとめ

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

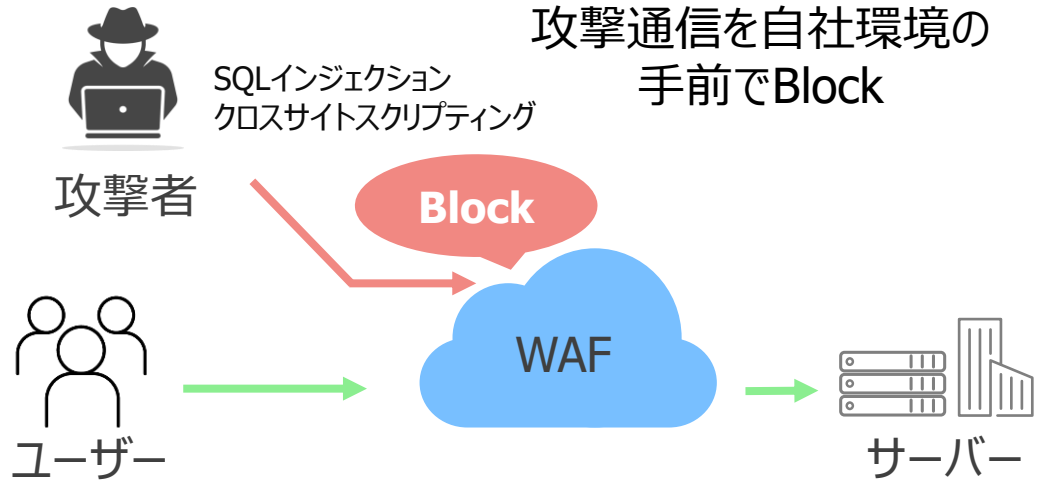
クラウドWAFとは

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

クラウドWAFとは

WAFとは、(Web Application Firewall) の略でWebサイトをはじめとしたWebアプリケーションへの攻撃を防御する製品・サービスです。
企業のアプリケーションに不正にアクセスし、個人情報の入手・改ざんなどの攻撃から保護します。

この機能をクラウド上で提供しているWAFをクラウドWAFと呼びます。
クラウドWAFは、攻撃通信を企業の環境の手前でブロックすることができます



クラウドWAFのメリット

- 簡単に導入できる
- 導入までの期間が短い
- 初期投資が少ない
- サイジング不要
- 運用時の負担が少ない

近年では、単純なWAFだけでなく、WAAPに相当する機能が求められている

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

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

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

クラウドWAFの必要性について

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

クラウドWAFが必要な3つのポイント

- サイバー攻撃からアプリケーションを保護
- 迅速な導入・運用効率の向上
- コンプライアンス遵守

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

クラウドWAFの必要性：サイバー攻撃からアプリケーションを保護

- ビジネスやサービスの中断、停止
- 損害賠償
- 情報の紛失・改ざん・漏えい
- ユーザーの離脱/機会損失
- 売上の減少
- 企業の社会的信用の低下
- 社内の業務効率の低下

1IPアドレス当たりのサイバー攻撃関連通信

図1. 1 IPアドレス当たりの年間総観測パケット数（過去10年間）

NICTER観測レポート2023
https://www.nict.go.jp/press/2024/02/13-1.html

安全なWebアプリケーション運用のために セキュリティ対策 が必要です

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

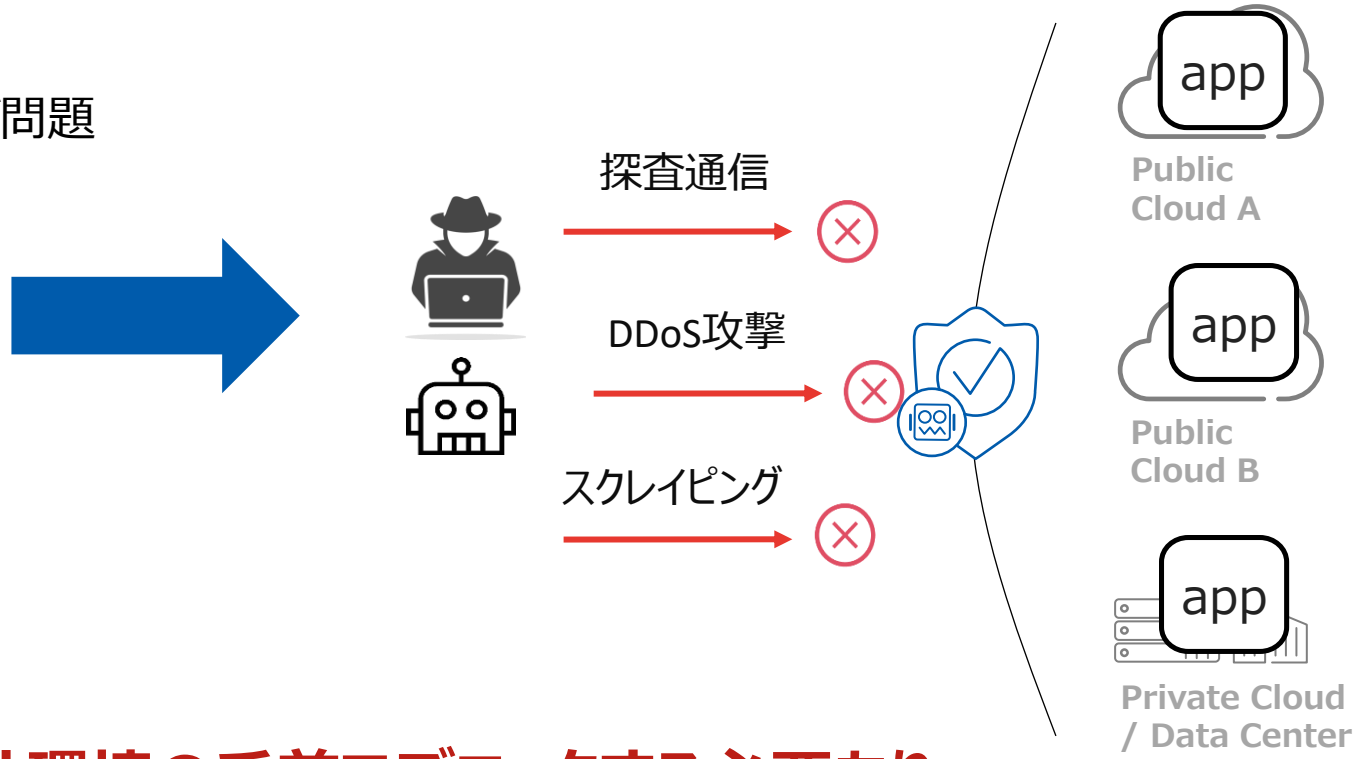
クラウドWAFの必要性：サイバー攻撃からアプリケーションを保護

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？

それだけでは不十分

攻撃がアプリ（サーバー）まで届いてしまうことが問題

- **探査通信により、脆弱性を探られてしまう**
- **サーバーのリソースが使われる**
- **帯域が圧迫される**



攻撃通信を自社環境の手前でブロックする必要あり

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

クラウドWAFの必要性：迅速な導入・運用効率の向上

サイバー脅威の迅速な対応が不可欠
コストとリソースの最適化
ビジネスの成長に合わせたセキュリティ

クラウドWAFのメリット

- 簡単に導入できる
- 導入までの期間が短い
- 初期投資が少ない
- サイジング不要
- 運用時の負担が少ない

具体的なメリット

- DNSの切り替えだけで導入可能（構成変更の必要なし）
- ハードウェアの準備が不要
- ハードウェアの購入やインフラの設置が不要。利用した分だけ支払い
- Traffic量が増大しても、クラウド側で自動でスケールアウト
- WAFのシグネチャのアップデート不要
- 緊急度の高い脆弱性に関しても、迅速にメーカーが対応

強固なセキュリティを実現しつつ、運用の効率化とコスト削減も実現

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

クラウドWAFの必要性：コンプライアンス遵守

DS-200 政府情報システムにおけるセキュリティ・バイ・デザイン ガイドライン（最終改定：2024年1月31日）
システム開発の企画工程からセキュリティを組み込むことを明記 https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/7e3e30b9/20240131_resources_standard_guidelines_guidelines_01.pdf

DS-310 政府情報システムにおけるクラウドサービスの適切な利用に係る基本方針クラウドスマート（最終改定：2023年9月29日）
クラウド・バイ・デフォルト原則に基づき、クラウドをスマート利用することやクラウドサービスを利用するメリットについて明記 https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/5167e265/20230929_resources_standard_guidelines_guideline_01.pdf

PCI DSS 4.0（2025年3月31日までが準拠するまでの猶予期間
要件6.4.2) 公開用Webアプリケーションに対して、Webベースの攻撃を継続的に検出・防止する自動化された技術的ソリューションを展開（**WAFの導入が必須**） 要件6.4.3) 消費者のブラウザに読み込まれ、実行されるすべての決済ページスクリプトを管理する（**Webスキミング対策が必須**）

クラウドサービスのメリットを生かしたセキュリティ対策の検討
業界によってはWAFの導入が必須

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

WAF導入のハードル

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

WAFを導入したいが、、、

WAFの定期的なアップデートやメンテナンス

DDoS、WAF、Bot対策、何からやればいいか分からない

パブリッククラウド、オンプレミスそれぞれにWAFを導入して管理するのは大変

従量課金制なので、コストが見積りにくい

攻撃の検知ログがたくさんあって探したいログが見つかりにくい

WAFは導入前後で知識が必要

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

F5 XC WAAPソリューション

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

F5, Inc.の提供するクラウドサービスです。

Distributed
Cloud Services

略称 F5 XC

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

F5 XC WAAPソリューションの特徴

WAFの定期的なアップデートやメンテナンス	→	SaaS型のWAF「F5 XC WAAP」 **シグネチャのアップデートなどはメーカーが実施**
DDoS、WAF、Bot対策、何からやればいいか分からない	→	次世代のWAF概念「WAAP」に対応したセキュリティソリューション **WAF、DDoS対策、Bot対策、API保護の機能** **これら機能をベースパッケージで提供**
パブリッククラウド、オンプレミスそれぞれにWAFを導入して管理するのは大変	→	**クラウド・オンプレミスのアプリケーションを一括して保護・管理**
従量課金制なので、コストが見積りにくい	→	予測可能なコスト 1年ベースのサブスクリプション **帯域・リクエスト数によらない価格体系**
攻撃の検知ログがたくさんあって探したいログが見つかりにくい	→	高機能で使いやすい管理ダッシュボード **管理画面のログからワンクリックで誤検知を解除**

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

F5 XC WAAPソリューションの特徴

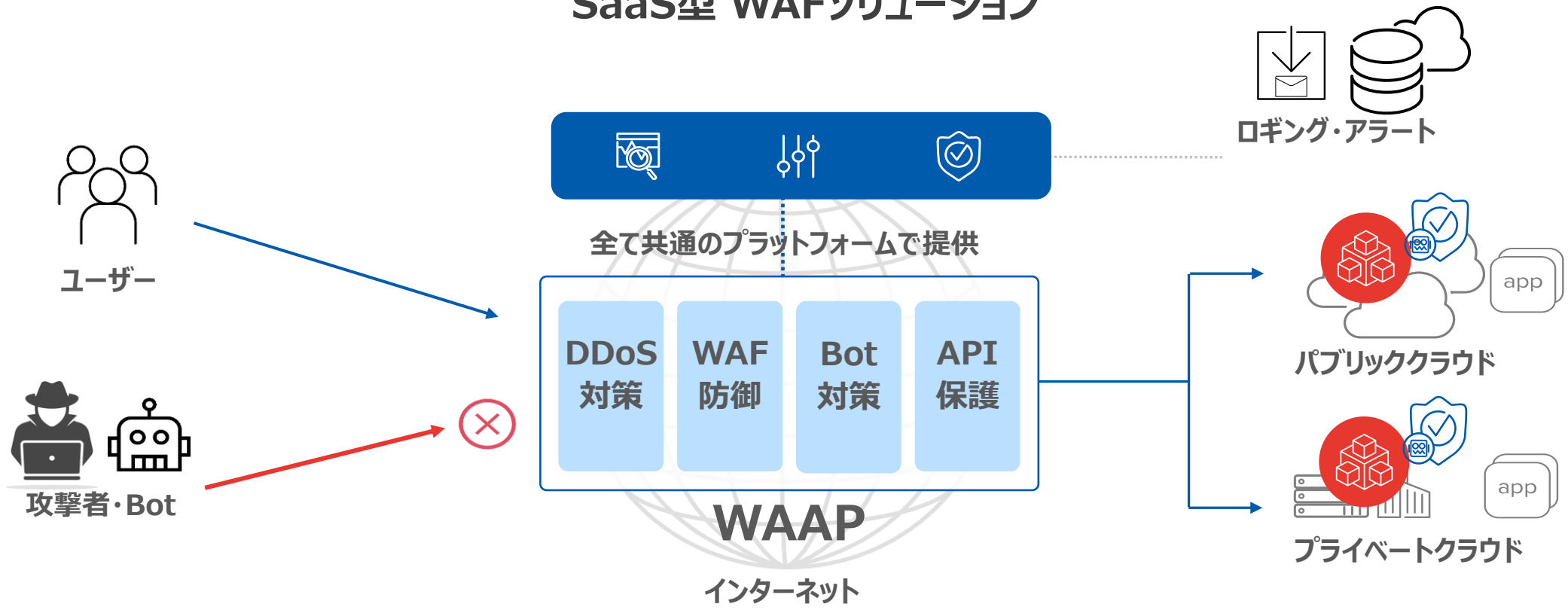
WAFの定期的なアップデートやメンテナンス	→	SaaS型のWAF「F5 XC WAAP」 **シグネチャのアップデートなどはメーカーが実施**
DDoS、WAF、Bot対策、何からやればいいか分からない	→	次世代のWAF概念「WAAP」に対応したセキュリティソリューション **WAF、DDoS対策、Bot対策、API保護の機能**
パブリッククラ それにWAF は大変		**護・管理**
従量課金制なので、コストが見積りにくい	→	予測可能なコスト 1年ベースのサブスクリプション **帯域・リクエスト数によらない価格体系**
攻撃の検知ログがたくさんあって探したいログが見つかりにくい	→	高機能で使いやすい管理ダッシュボード **管理画面のログからワンクリックで誤検知を解除**

WAF（WAAP）をはじめてみたいというお客様には最適なソリューション！

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

F5 XC WAAPソリューションについて

F5 XC WAAPは、WAAPの4つの機能に対応した SaaS型 WAFソリューション

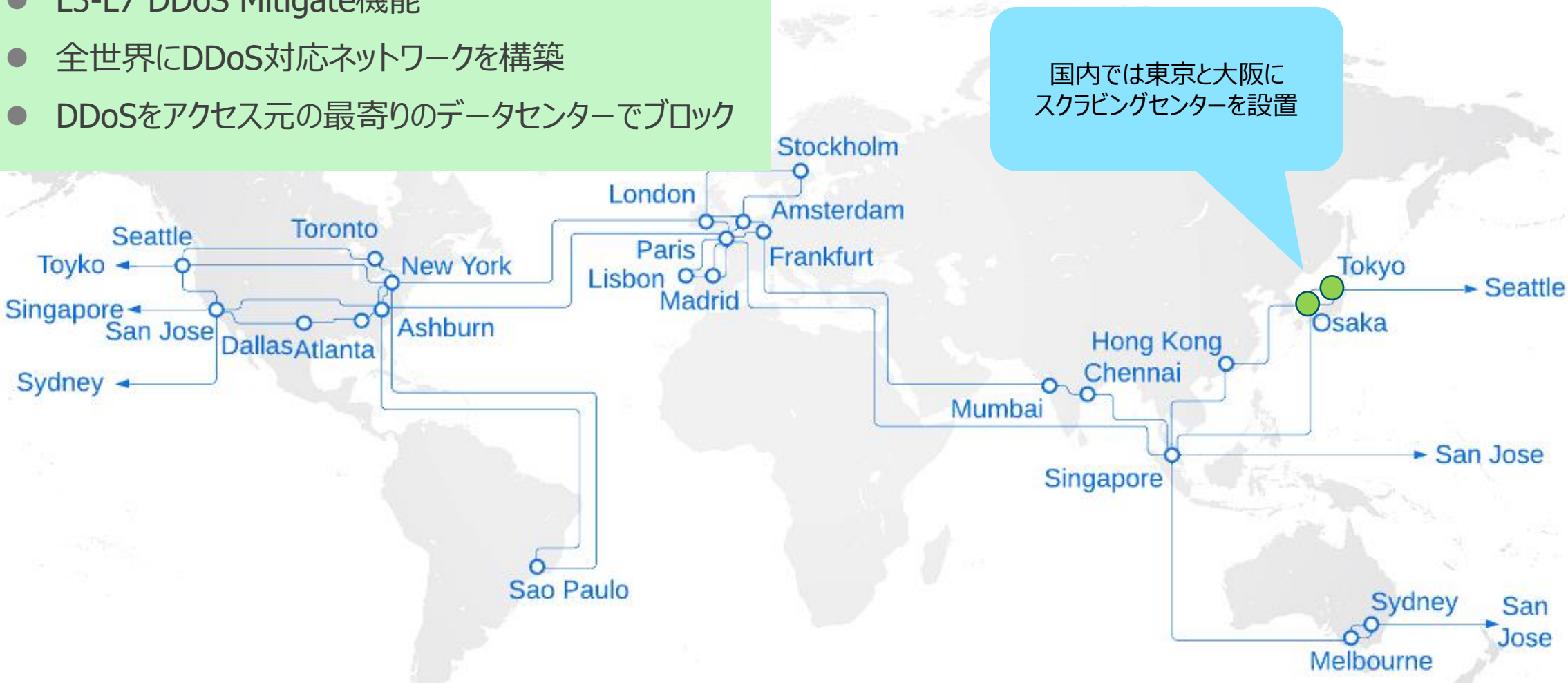


DNSの切り替えによるWAAPの適用
既存構成を変更することなく、迅速に導入することが可能

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

F5 XC DDoS Mitigate

- L3-L7 DDoS Mitigate機能
- 全世界にDDoS対応ネットワークを構築
- DDoSをアクセス元の最寄りのデータセンターでブロック



DDoS攻撃がお客様サイトに届く前に止める仕組み

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

F5 XC WAF機能

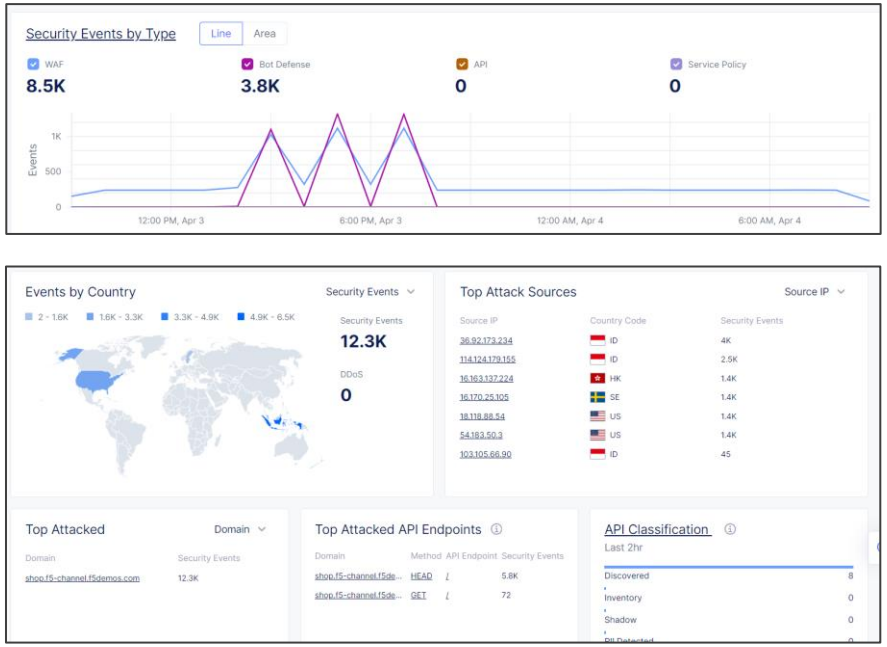
攻撃検知・誤検知緩和

- **実績豊富なBIG-IPのASM・AWAFエンジンを採用**
- 機械学習による誤検知緩和
- 誤検知レベル毎のWAFポリシー有効化の設定
- 管理画面のログから数クリックで誤検知を解除
- ステージング機能

豊富なセキュリティ機能

- シグネチャベースのポリシー設定
- IPレピュテーションによる送信元評価
- ジオロケーション/IPベースのブロック
- Threat Campaigns
- リクエストメソッド毎のアクセス制御
- Rate Limit

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

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

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

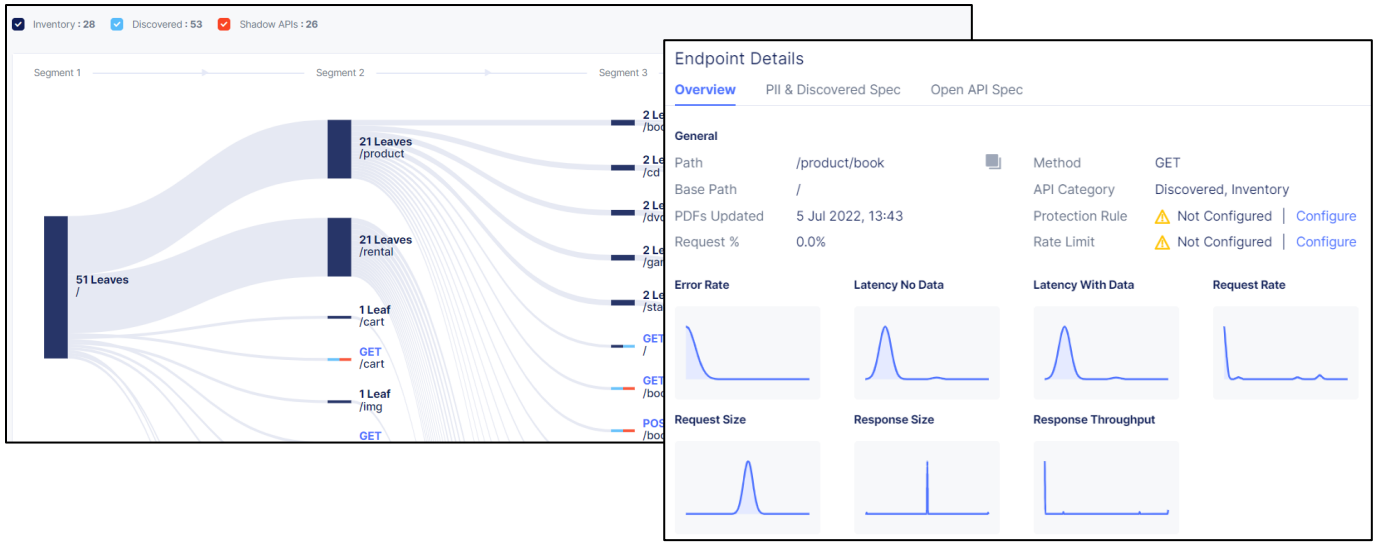
脅威レベルと対処を定義	
レベル	対処（例）
高	ブロック
中	レポート
低	無視

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

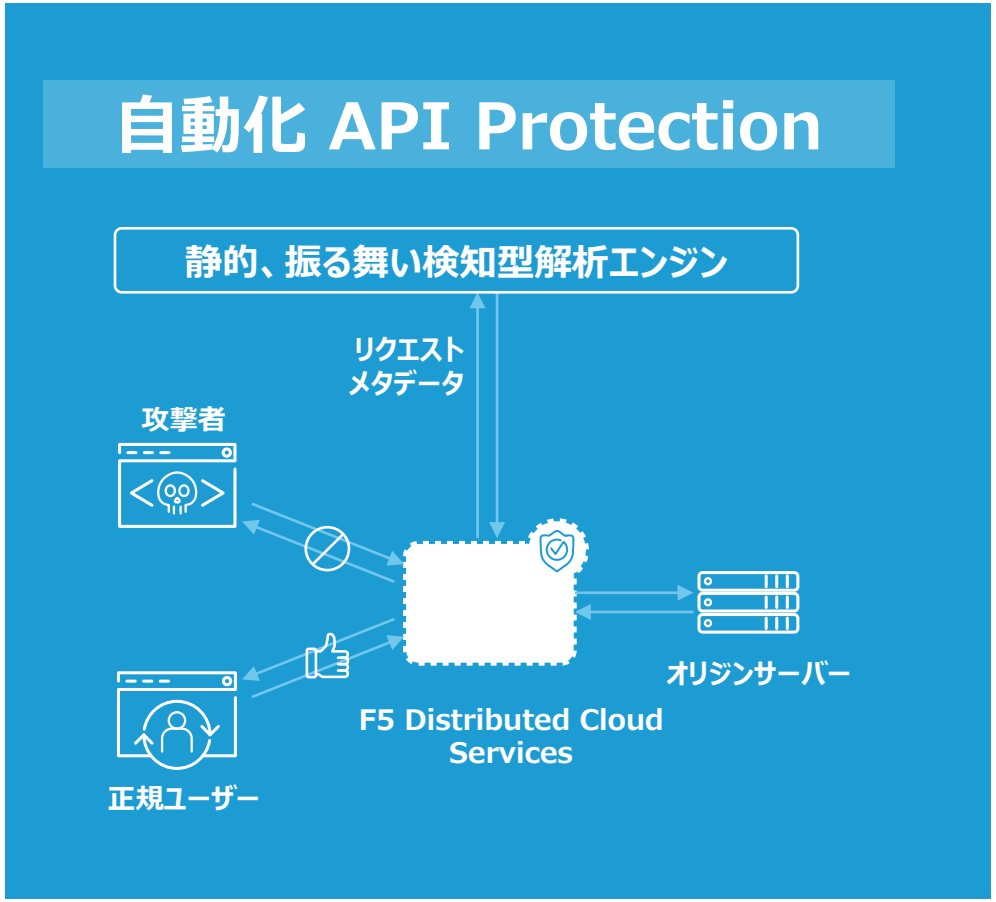
F5 XC API Protection

1 アタックシグネチャによるAPI保護

2 自動APIディスカバリーとポリシー管理によるAPI保護



- API通信を自動で可視化
  - APIスキーマを学習し、Swaggerファイルを自動生成
  - シャドーAPIの検知
- Swaggerファイルをベースにした API保護ポリシーの適用
  - 不審なリクエストをブロックし、データ漏えいを防止
- APIセキュリティポリシーの設定と導入にかかる時間を短縮



Copyright © Tokyo Electron Device LTD. All Rights Reserved.

F5 XC Client-Side Defense

Webスキミング対策：攻撃者/犯罪者による改ざんを防止するセキュリティサービス

PCI DSS 4.0 要件6.4.3）消費者のブラウザに読み込まれ、実行されるすべての決済ページスクリプトを管理する（Webスキミング対策が必須）

- JavaScriptの動作監視

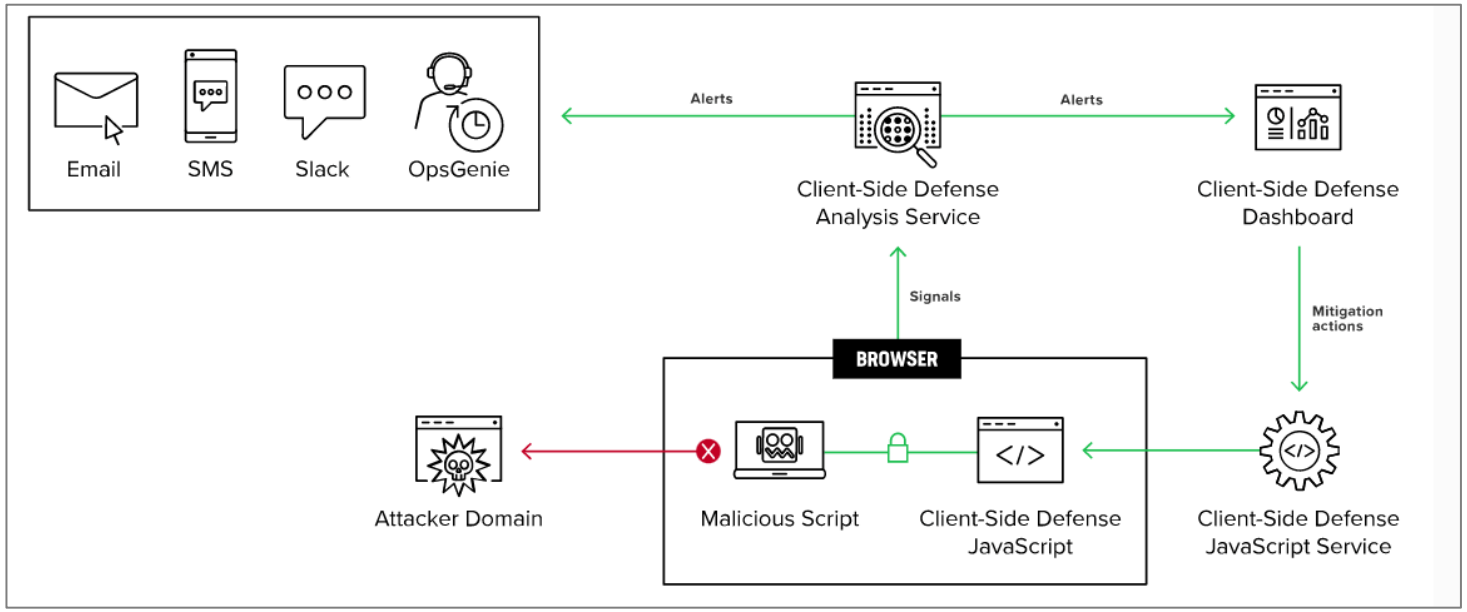
オリジンサーバーにCSDのJavaScriptを導入することで、クライアントのブラウザの動きをリアルタイムに監視し、不審な挙動を検出します。

- インサイトフルアラート

攻撃の影響に関する実用的な洞察を含むアラートを受け取ることができます。

- データ流出の軽減

簡単な操作でデータ流出を即座に停止します。

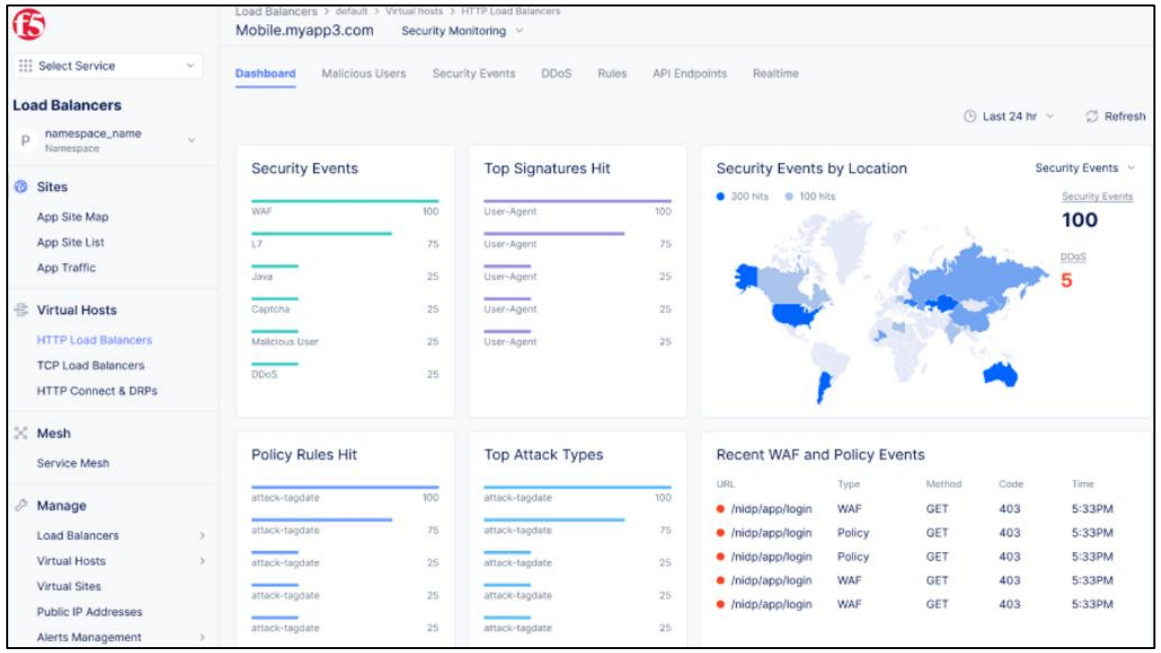


Copyright © Tokyo Electron Device LTD. All Rights Reserved.

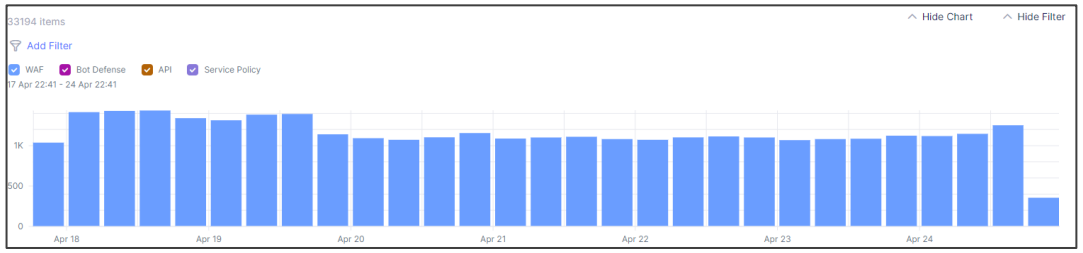
F5 XC WAAP コンソール画面

F5 XC の設定・モニタリングは1つのコンソールから実施可能
保護対象のアプリケーションへ一貫した管理を提供

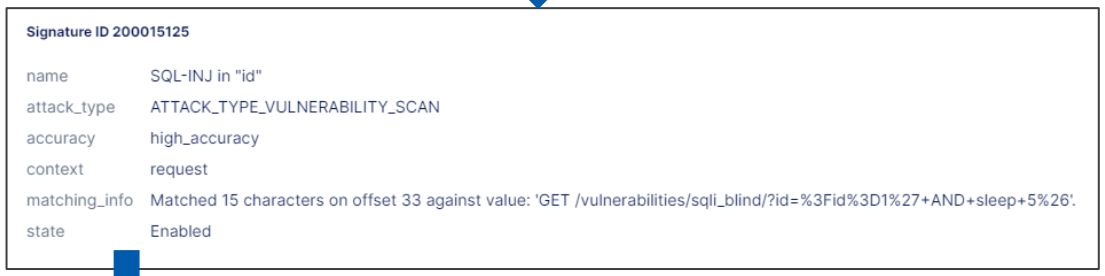
Dashboard Summary

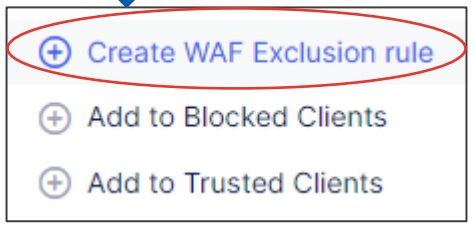


Security Eventsのチャート



Security ログ（一部）





ここから数クリックで、Signature IDやリクエストのパラメータなどの情報が入った除外ルールを自動で生成し、適用することが可能

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

東京エレクトロン デバイス株式会社のサービスメニュー

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

東京エレクトロンデバイスについて

- F5の日本法人が出来る前からの代理店
- 幅広い取り扱いラインナップ
  - **F5 BIG-IP**
  - **F5 NGINX**
  - **F5 Distributed Cloud Services**
- F5国内販売額9年連続No.1の一次代理店
- 自社検証環境を利用した技術支援(デモ/ハンズオンのご提供)
- 保守契約ユーザー向けの会員制サイト(FAQ/ドキュメント等)
- F5製品の重要情報をPush型でメール配信(脆弱性、既知の重大不具合及び改修情報、リリース情報等)

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

東京エレクトロン デバイス株式会社のサービスメニュー

WAFは導入前後で知識が必要

製品だけでは解決できない部分もサポートいたします

弊社が導入や運用をサポート

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

構築/支援 サービス

F5 XC WAAPに関しては、主に次の構築・支援サービスをご用意しております。

- PoC支援サービス
  - お客様が主体となって実施していただきます
  - 特定の目的に対して、F5XC WAAPで実現可能かどうかを確認する手法です
  - 弊社で操作レクチャを実施したのち、お客様主体で設定や検証を進めていただきます
  - 目標設定などの進め方については弊社がフォローします

- WAAP構築&WAFチューニングサービス
  - 弊社が主体となって実施するサービスです
  - お客様のご要件をヒアリングし、弊社がWAAP環境を構築します
  - 構築後、WAFのチューニングも実施します。

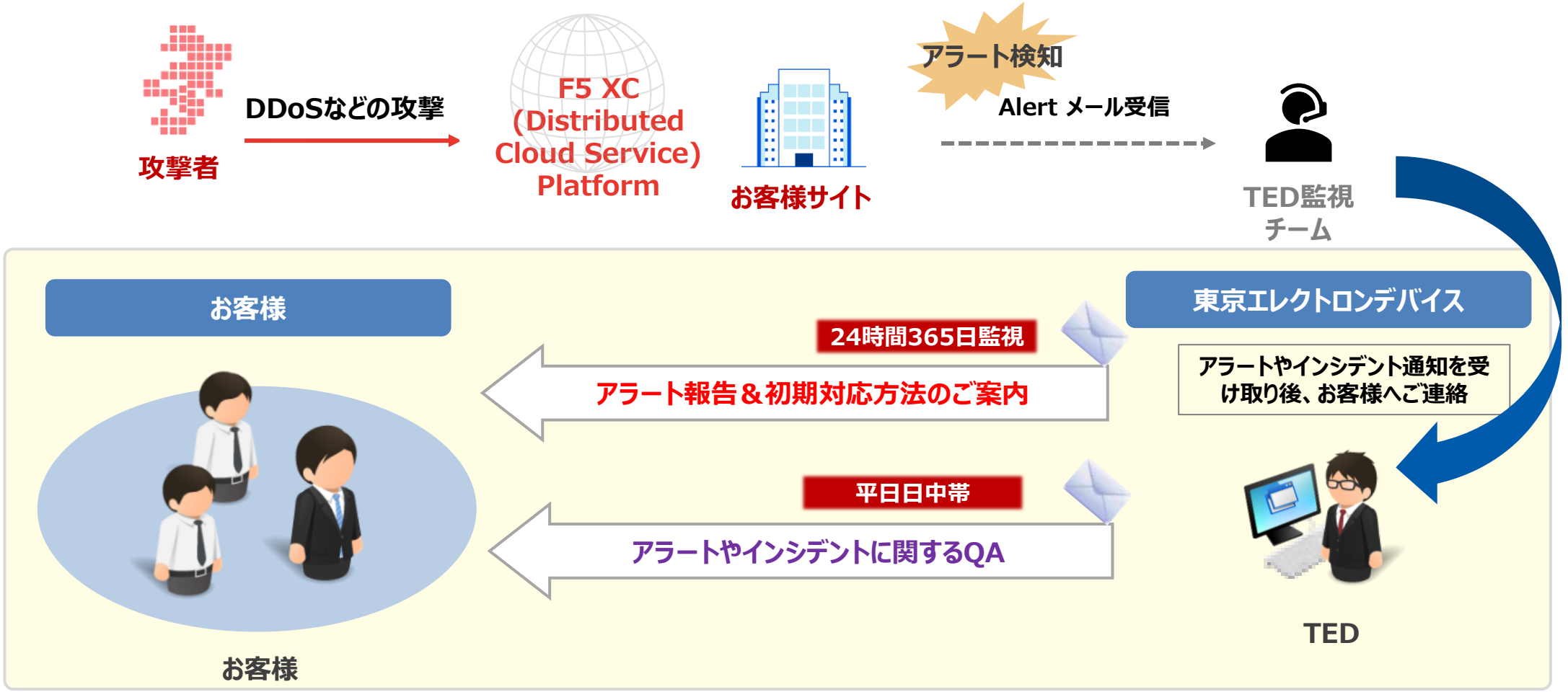
これ以外のご要望についてもお気軽ご相談ください
トレーニングやデモなども実施可能です

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

F5 XC WAAP アラート対応支援サービス

アラートに対する初期対応方法を支援するサービスです。

- システムアラート検知後、その旨をお客様にメールにて報告いたします（24時間体制）
- 平日日中帯でのヘルプデスクサポートとともに、アラートやインシデントに関するQA対応を実施します



Copyright © Tokyo Electron Device LTD. All Rights Reserved.

まとめ

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

まとめ

- クラウドWAFが必要な理由について、3つの観点でお話しました
  - サイバー攻撃からアプリケーションを保護
  - 迅速な導入・運用効率の向上
  - コンプライアンス遵守

- WAFの導入のハードルはいくつもありますが、F5 XC WAAPで以下のハードルを乗り越えることが可能です
  - WAFの定期的なアップデートやメンテナンス
  - DDoS、WAF、Bot対策、何からやればいいか分からない
  - パブリッククラウド、オンプレミスそれぞれにWAFを導入して管理するのは大変
  - 従量課金制なので、コストが見積りにくい
  - 攻撃の検知ログがたくさんあって探したいログが見つかりにくい

- WAFを導入したくても、何をしたらいいのか分からないという場合でも、弊社が構築/運用をサポートします

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

onnect Beyond

ご視聴ありがとうございました

東京エレクトロン デバイス株式会社

Copyright © Tokyo Electron Device LTD. All Rights Reserved.