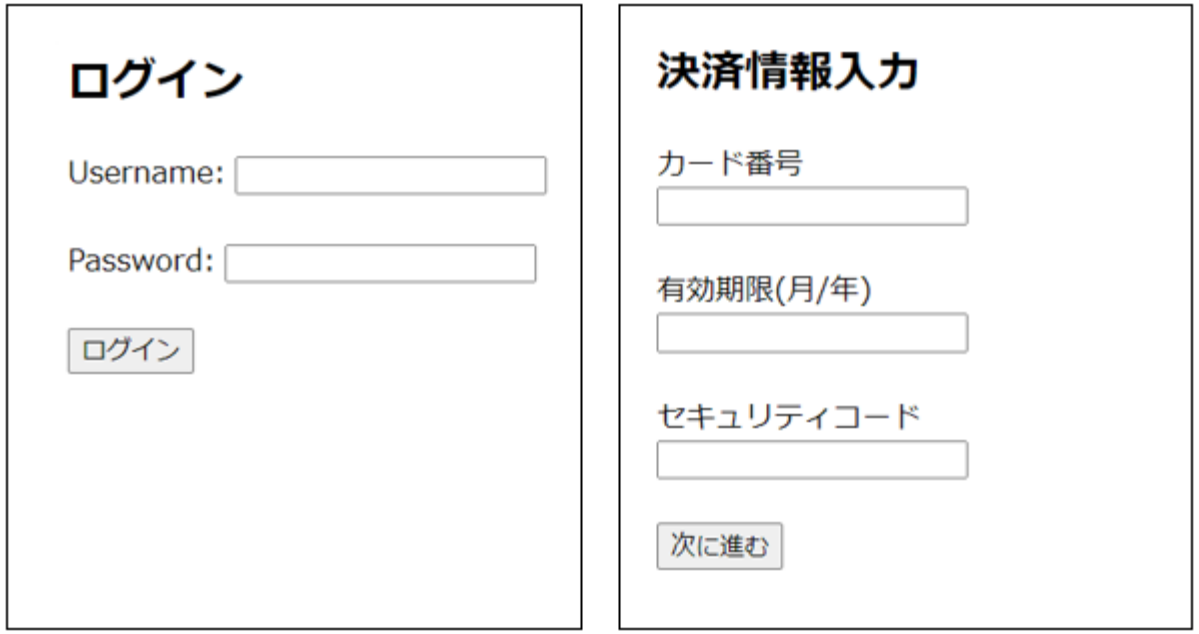
WAFだけでは守れない！
Webスキミング攻撃の脅威に対抗する
これからの対策

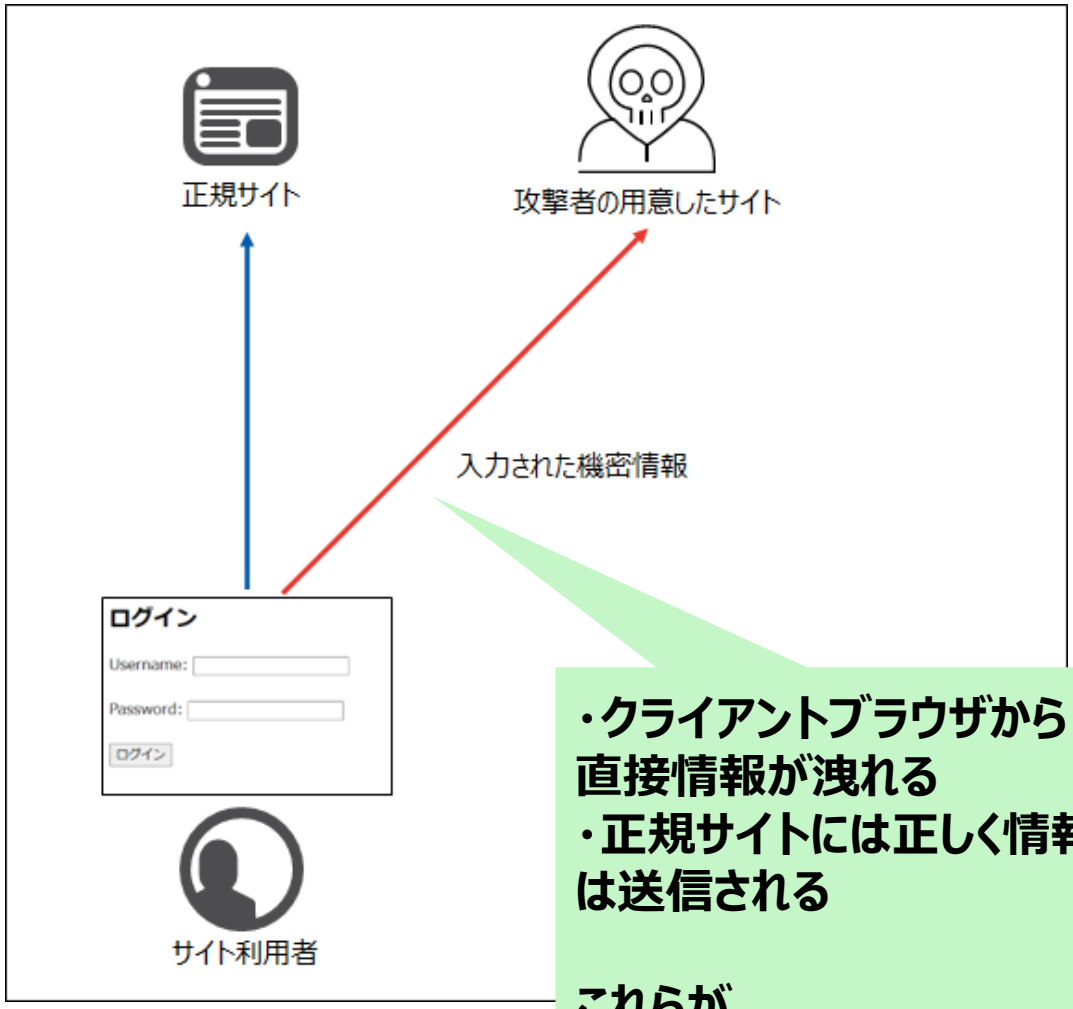
東京エレクトロン デバイス株式会社

Webスキミングの概要と脅威

Webスキミング攻撃の概要



- ウェブアプリケーションの脆弱性等を悪用し、
  ターゲットサイトに不正なコードを挿入する事で
  サイトの「入力フォーム」上に入力された情報を盗む攻撃手法



・クライアントブラウザから
直接情報が洩れる
・正規サイトには正しく情報
は送信される

これらが、
この攻撃のポイント！

Webスキミング攻撃によって漏えいする可能性のある情報

- ユーザー名＆パスワード
- クレジットカード情報
- 住所や電話番号をはじめとしたさまざまな個人情報…

Webサイトのフォーム上で入力される情報はすべて漏えいする危険性がある

情報セキュリティ10大脅威 2024

◢ 情報セキュリティ10大脅威 2024 [個人]

「個人」向け脅威（五十音順）	初選出年	10大脅威での取り扱い（2016年以降）
インターネット上のサービスからの個人情報の窃取	2016年	5年連続8回目
インターネット上のサービスへの不正ログイン	2016年	9年連続9回目
クレジットカード情報の不正利用	2016年	9年連続9回目
スマホ決済の不正利用	2020年	5年連続5回目
偽警告によるインターネット詐欺	2020年	5年連続5回目
ネット上の誹謗・中傷・デマ	2016年	9年連続9回目
フィッシングによる個人情報等の詐取	2019年	6年連続6回目
不正アプリによるスマートフォン利用者への被害	2016年	9年連続9回目
メールやSMS等を使った脅迫・詐欺の手口による金銭要求	2019年	6年連続6回目
ワンクリック請求等の不当請求による金銭被害	2016年	2年連続4回目

＜攻撃手口＞

以下の手口でクレジットカード情報を入手し、不正利用を行う。[1]

◆ **フィッシング詐欺**

メールやSMS等を使い、受信者を騙してフィッシングサイトに誘導し、クレジットカード情報等を詐取する。詳細は個人 1 位「フィッシングによる個人情報等の詐取」を参照。

◆ **正規の決済画面を改ざんし入力情報を詐取**

EC サイト（ショッピングサイト）の脆弱性を悪用し、正規ウェブサイトの決済画面を改ざんする。改ざんした決済画面に被害者を誘導し、クレジットカード情報を入力させる。入力されたクレジットカード情報を攻撃者が詐取する。

＜攻撃手口＞

◆ **サービスの脆弱性や設定不備を悪用**

攻撃者は、適切なセキュリティ対策が行われていないショッピングサイト等に対して、脆弱性や設定不備を悪用して、ウェブサイト内の個人情報等の重要情報を窃取する。

また、攻撃者はウェブサイトの脆弱性を悪用してウェブサイトを改ざんする場合もある。サービスの利用者が改ざんに気づかず情報を入力してしまうと、その情報は攻撃者に窃取される。

いずれもWebスキミングの攻撃手法となる

出典：独立行政法人 情報処理推進機構
https://www.ipa.go.jp/security/10threats/10threats2024.html

近年の被害事例

- ECサイトの事例①
  196日間 (2021年8月10日から2022年2月22日の期間)
  クレジットカード情報 **1万6093件**の漏えい
- ECサイトの事例②
  102日間 (2021年8月28日から同年12月8日の期間)
  クレジットカード情報 **7409件**の漏えい
- ECサイトの事例③
  1037日間 (2021年3月17日から2024年1月18日の期間)
  個人情報**2万132件**、クレジットカード情報**3958件**の漏えい
- ECサイトの事例④
  247日間 (2023年3月11日から同年11月13日の期間)
  クレジットカード情報**5447件(4851人)**の漏えい
- ECサイトの事例⑤
  1057日間 (2021年2月24日から2024年1月17日の期間)
  個人情報**3万8664件**、クレジットカード情報**1万3879件**の漏えい
- ECサイトの事例⑥
  1035日間 (2021年7月20日から2024年5月20日の期間)
  クレジットカード情報 **5万2958名**の漏えい

いずれも長期間にわたって攻撃の被害にあっている

PCIDSS v4.0.1変更点について

- **PCIDSS**
  クレジットカード会員情報を保護するために策定された技術的および運用上の要件についてを提供するグローバル基準
- 現在有効なPCIDSS v4.0.1ではWebスキミング攻撃対策とされる要件が追加

➢ 消費者のブラウザに読み込まれて実行されるすべての決済ページ **スクリプトを包括的に管理することが義務化(要件6.4.3)**

具体的には以下の実装が求められる。

①各スクリプトが認可されたものであることを確認する方法

②各スクリプトの完全性を保証する方法

③各スクリプトが必要な理由が記載された全スクリプトの目録

個人情報保護法規則・ガイドライン改正

- 2024年4月1日に施行された個人情報保護法規則及びガイドラインの改正では、「Webスキミング攻撃」を意識した個人情報として扱う情報と報告義務の拡大が実施

改正の問題意識「Webスキミング」

安全管理措置・漏えい等報告が改正される背景となった「Webスキミング」（図1）とは、典型的にはECサイトに仕掛けられる攻撃手法です。現行の個人情報保護法規則では、漏えい等報告の対象は、個人情報取扱事業者側でデータベース化された個人情報（＝個人データ）が漏えいした場合のみとなっており、Webスキミングによって漏えいした個人情報は報告対象外でしたが、利用者側から見れば、攻撃者に個人情報を取得されてしまっては、個人情報取扱事業者を経由しているか否かに関わらず生じる被害は同様なため、利用者から攻撃者に直接情報が流出してしまった事象に関しても個人情報保護委員会への報告が必要であるとして今回の改正が行われたと考えられます。

出典：一般財団法人 日本情報経済社会推進協会
https://www.jipdec.or.jp/library/report/20240227-r01.html

Webスキミング攻撃の厄介なところ

- Webサイトのサービス自体は正常に利用出来てしまう
  このため、**Webサイト運営側や利用者も攻撃の発生に気が付く事が難しい**

- **クライアントブラウザから直接情報が漏えいするため、**
  情報非保持化や暗号化保存といったポリシーが対策にならない

- **ECサイト以外のWebサイトも攻撃対象になりえる**
  B to BのシステムがWebスキミング攻撃の被害にあった事例も

- **WAFでは検知・防御が困難**
  一般的なWAFはWebサイトへのリクエストをスキャンして攻撃を検知・防御する対策
  サイトへのリクエストは正常トラフィックであるため攻撃の発生は検知出来ない

Webスキミング攻撃の厄介なところ

- Webサイトのサービス自体は正常に利用出来てしまう
  この
-
  性
-
  E
-
  ニ
  また、Webサイトの改ざんを検知する機能が無いこともほとんど

Webスキミング攻撃には専用の対策が必要

Webスキミング対策
Client-Side Defense

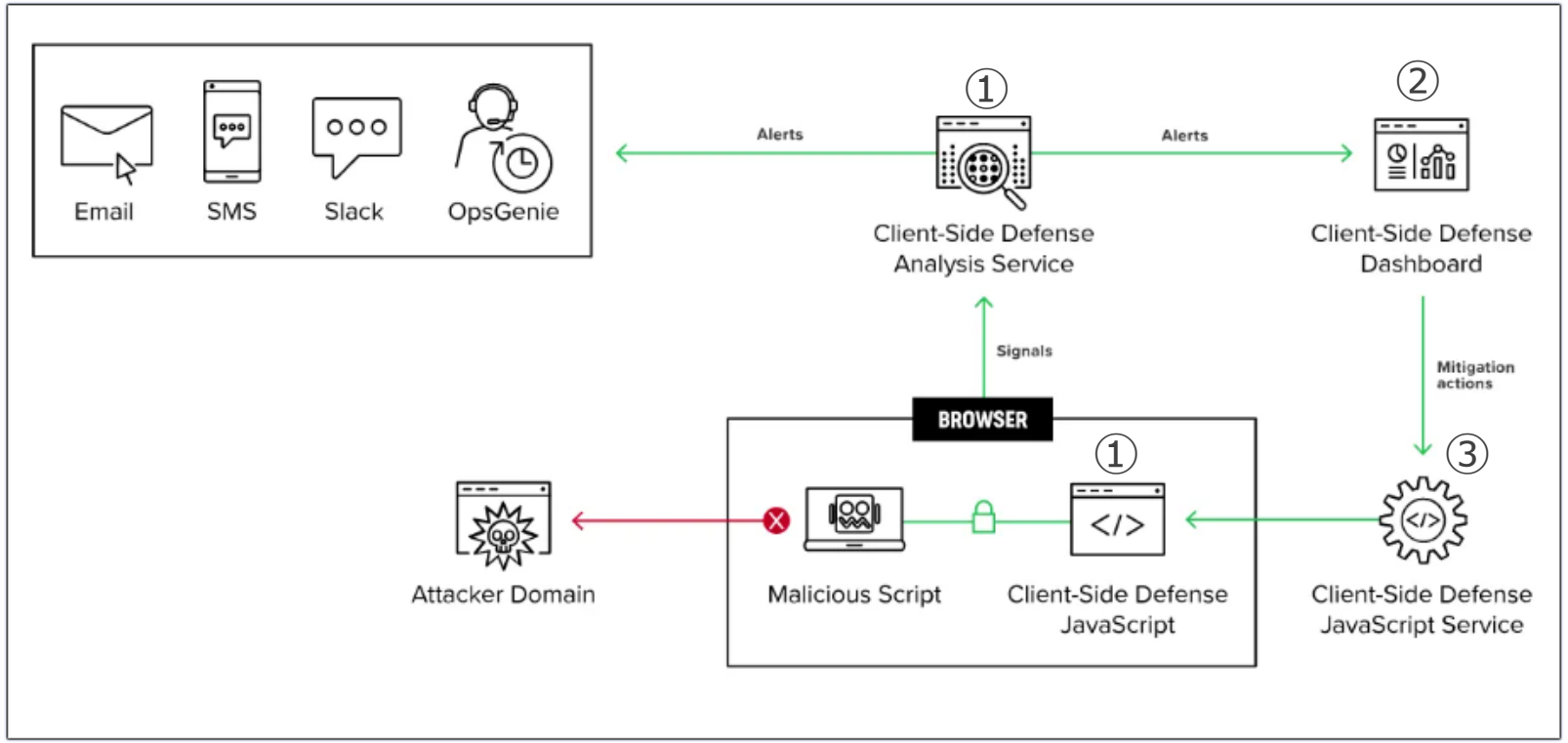
F5 Distributed Cloud Client-Side Defense(略称 CSD)

- **F5社が開発したWebスキミング対策用セキュリティSaaS型ソリューションです。**
  F5社のクラウドWAF「F5 XC WAAP」の機能として提供されています。

①「JavaScriptの動作監視」
→JavaScriptをリアルタイムで監視し
　不審な挙動を検出

②「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る

③「データ流出の軽減」
→簡単な操作でデータ流出を即座に
　停止する



CSD設定方法

対象ドメインを登録後、CSD(Client-Side Defense) JSの場所をwebページソースに追記

F5 Distributed Cloud

F5 Distributed CloudがCSD JSの場所を発行

サンプル　スクリプトタグ

```
<script  src="https://[redacted]/__imp_apg__/js/volt-
[redacted]pdoshj-f5bbbfb1.js" id="_imp_apg_dip_"
_imp_apg_cid_="volt[redacted]pdoshj-f5bbbfb1"
_imp_apg_api_domain_="https://[redacted]m"></script>
```

ヘッダータグ内挿入
※他のスクリプトやJSタグよ
先にロードされるように設定

```
<head>

</head>
```

保護対象サイトにJSを自動的に挿入する機能も提供

CSD 検出･保護の流れ

1)JavaScriptの接続先をモニタ

1．ページが読み込まれCSD JSが
JavaScriptの接続先ホストを収集

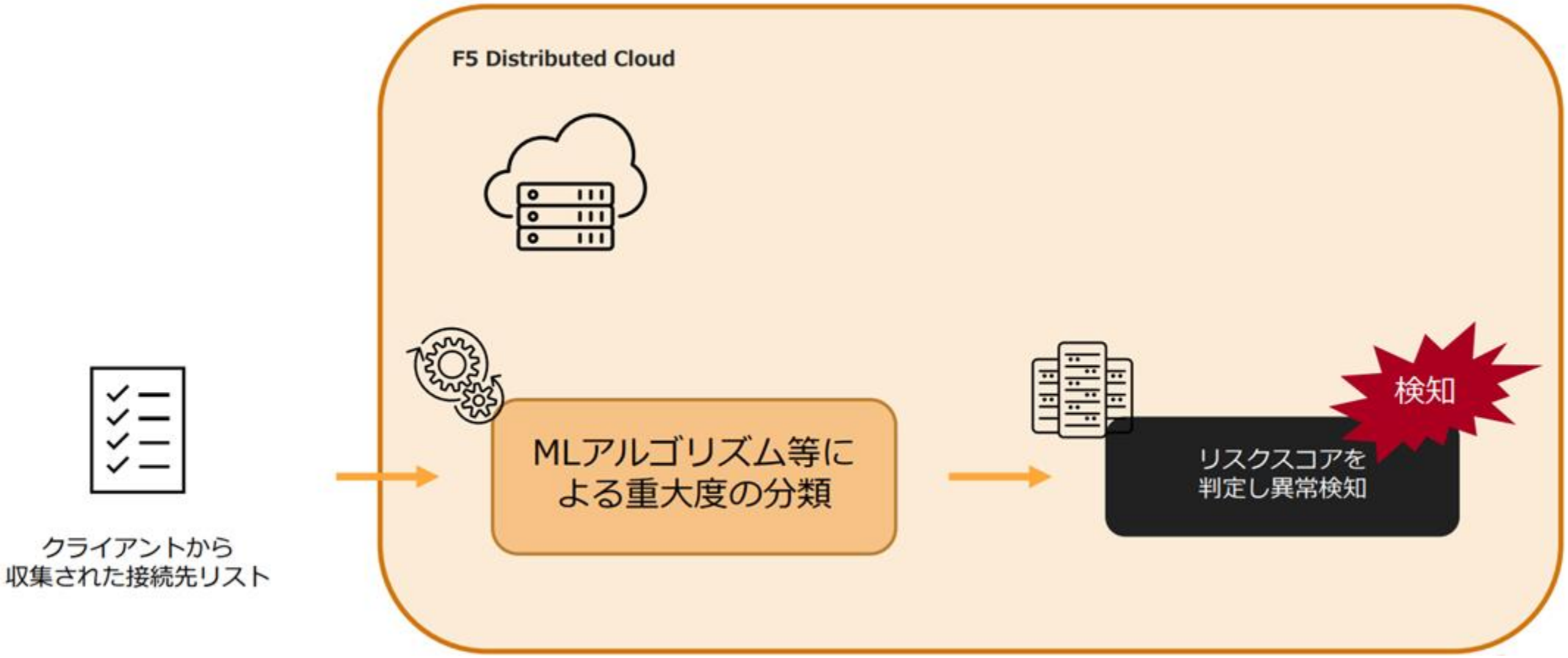
2．ページが実行するJavaScriptの接続先ホスト名を
暗号化してF5 Distributed Cloudへ送信

個人情報は収集するデータに含まれません

- ユーザー名、電子メール、クレジットカード番号など、ユーザーがアプリケーションに入力するデータを取得することはありません。

CSD 検出･保護の流れ

2)不正なサイトへの接続検知

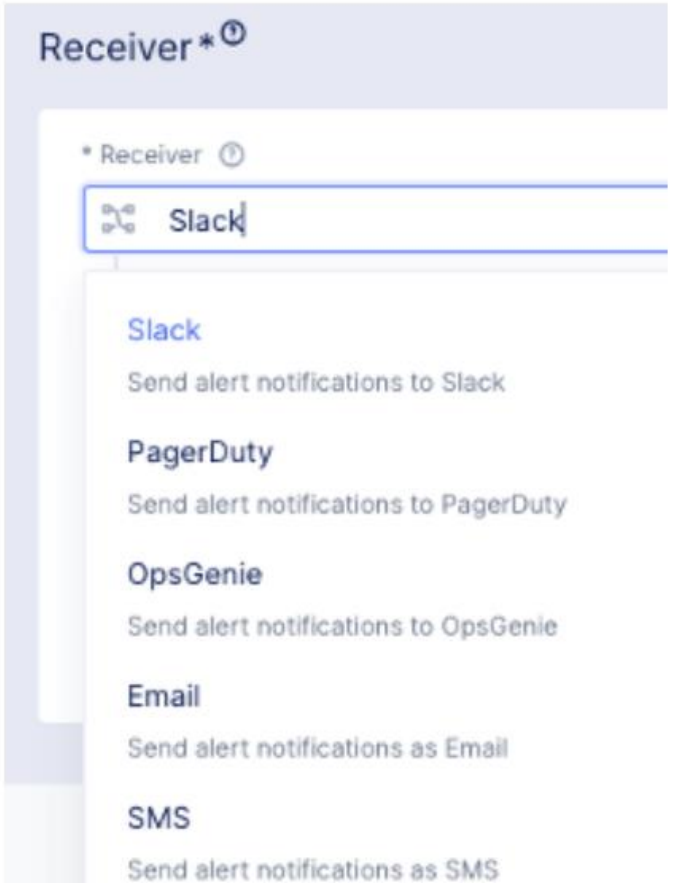


CSD 検出･保護の流れ

3)お客様へのアラート

お客様（登録済みの連絡先）へお知らせ

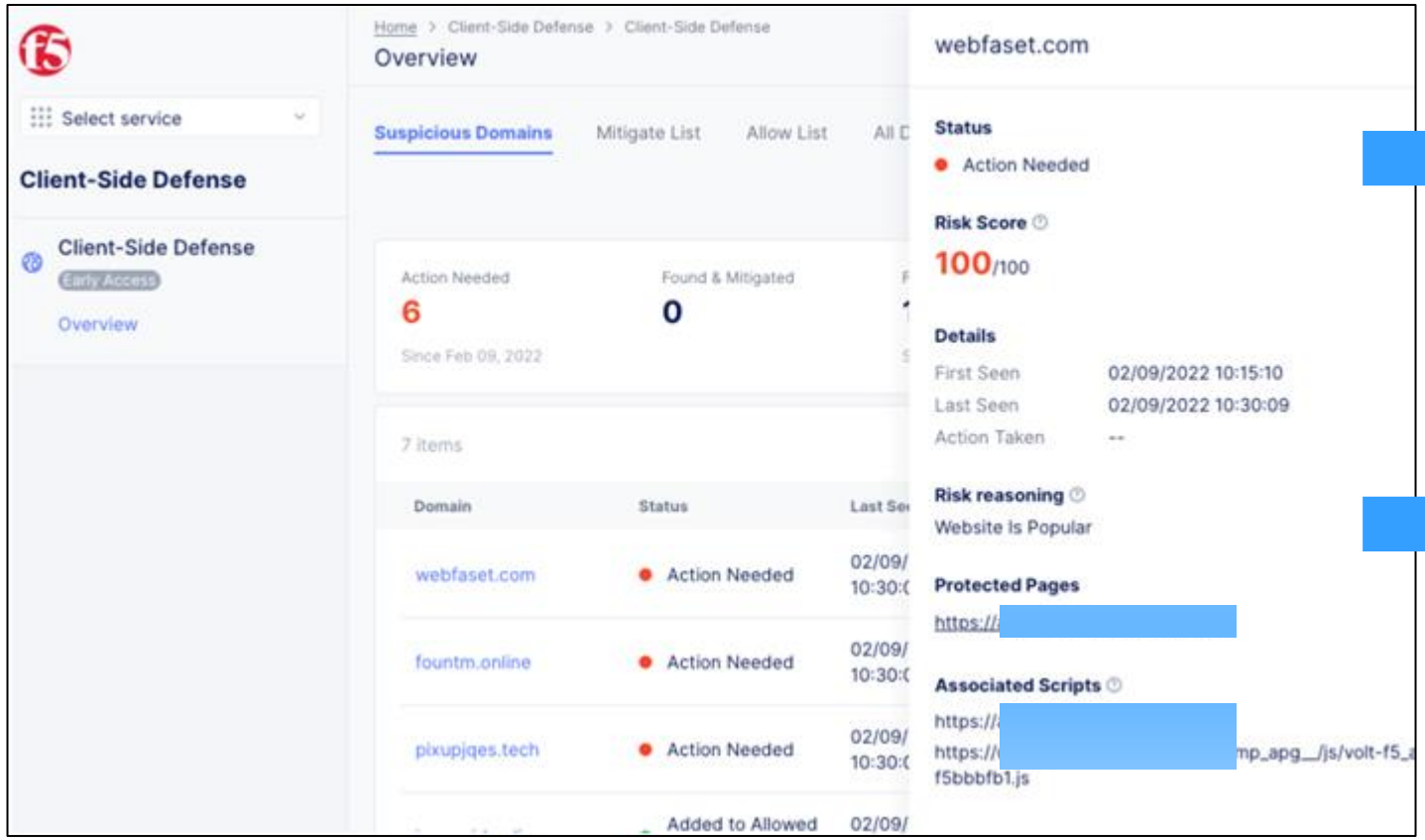
連絡先の登録



CSD 検出・保護の流れ

4)必要な対策の実施

ダッシュボードを確認



接続許可と判断

問題ない接続先と判断し、
Allow List に追加

不要な接続と判断

不正な接続とし判断し、
Mitigate Listに追加

F5の「Client-Side Defense」の機能まとめ

1. Client-Side DefenseのJSが挿入されたWebサイト上で動作するスクリプトの動作を監視
2. サービスのダッシュボード(Webコンソール)上で検知されたスクリプトをリスト化
   スクリプト目録の機能を提供
   ・スクリプトの動作、スクリプトが検知された日時・スクリプトの動作が変更された日時を確認可能
   ・一覧から信頼済みスクリプトとして登録する際にコメントを挿入する事が可能
3. スクリプトによるリスクの高い外部サイトへの情報を送信検知した場合管理者へアラート
4. スクリプトの動作を停止する事が出来る。

F5 XC WAAPとは

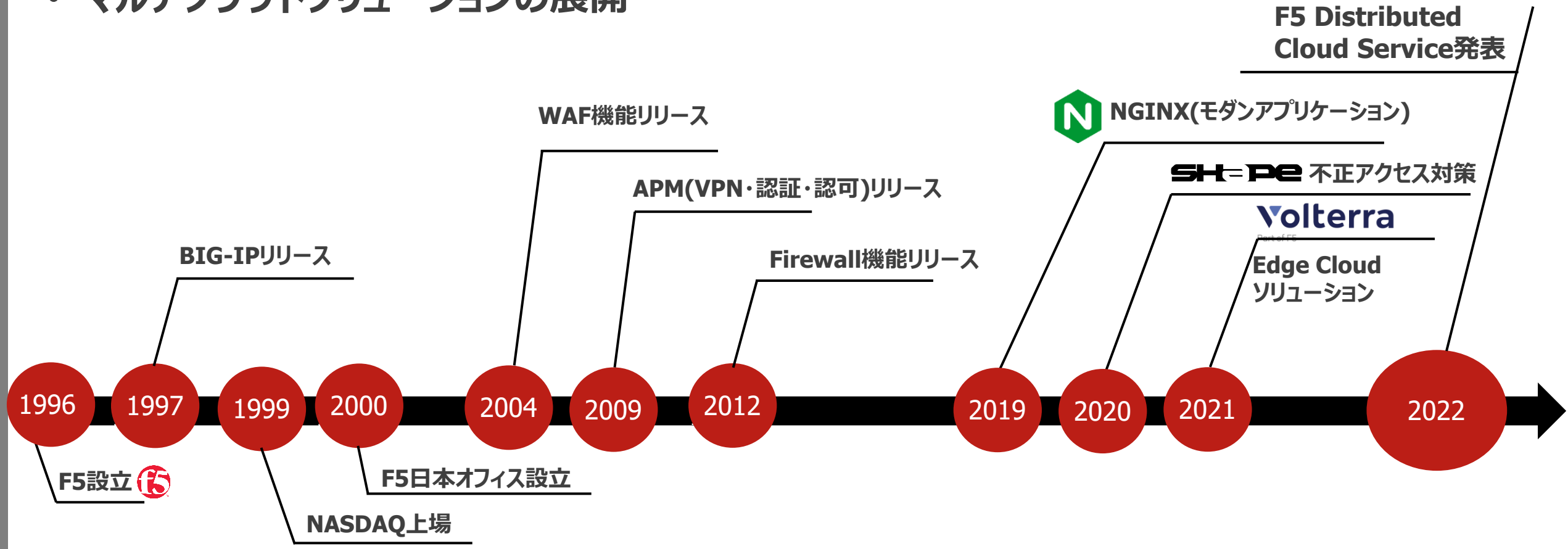
F5, Inc.の提供するクラウドサービスです。

Distributed Cloud Services

略称 F5 XC

F5のトランスフォーメーション

- アプリケーションを高速に安全に配信するためのソリューションを提供
- 早期よりセキュリティへの取り組みに着手
- マルチクラウドソリューションの展開



F5 XCの主な機能

マルチサイト・クラウドネットワーク接続（MCN）

マルチクラウドネットワーク接続など

SaaS型セキュリティサービス
WAAP

DDoS保護、WAF、Bot対策、API保護、Webスキミング対策などのマルチレイヤーのセキュリティ対策

マネージドK8s
アプリケーションサービス

オンプレミス、マルチクラウド、Edgeなどのあらゆる環境にアプリケーションをデプロイ

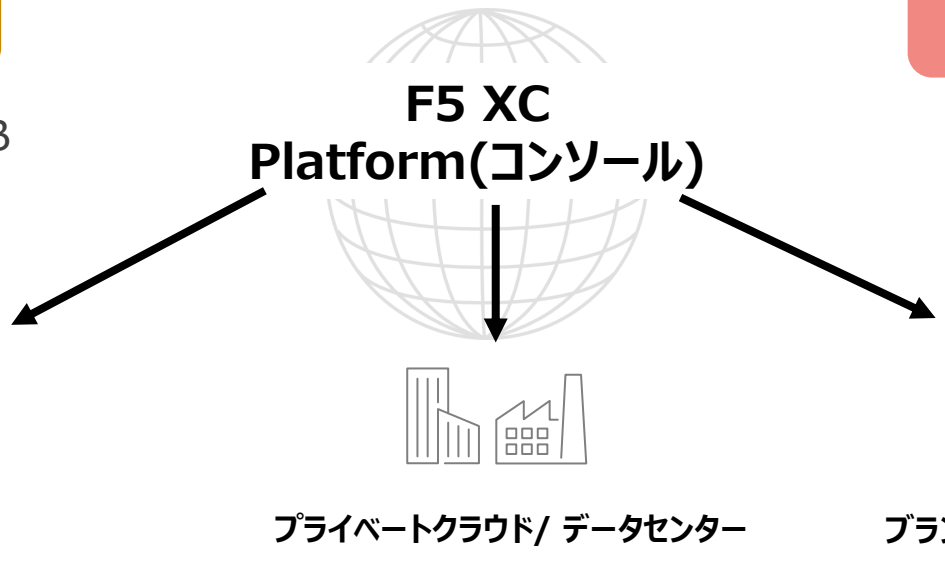
SaaS型　DNS

プライマリDNS・セカンダリDNS・GSLB

Web/API 脆弱性診断

CDN

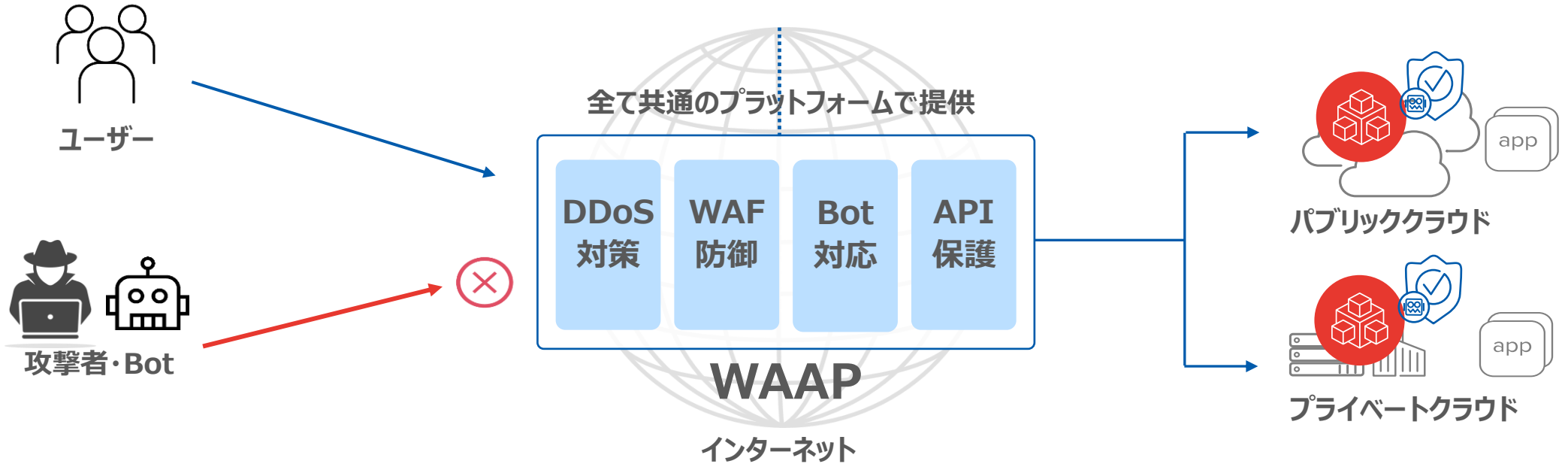
コンテンツキャッシュ



様々なサービスを提供することで、アプリケーションの課題を解決

F5 XC WAAP

- シンプルな操作と堅牢な防御を両立したソリューション
- DNSの切り替えによる迅速な導入



DDoS、WAF、Bot対応、API保護などのすべてのレイヤーのセキュリティ機能を提供

ベースパッケージだけで非常に幅広い機能・サービスを利用可能

WAF	• WAF機能 (アタックシグネチャ、バイオレーション) • IPレピュテーション • Threat Campaigns • **Client-Side Defense** **※月間100万リクエスト** **オプションで対応リクエスト数を追加可能**
Bot対策	• Bot Defense Basic （シグネチャベース）
DDoS対策	• L3-L7レベルの ボリューム型攻撃検知・緩和
API保護	• シグネチャベースによるAPI保護 • API Protection(月間50万リクエスト) • API Auto Discovery（1アプリ）
DNS	• DNS Zone管理（250 Zone）
DNS Load Balance	• DNSロードバランサー（50レコード） • ヘルスチェックの設定数 （200個まで）
Load Balancer	• 1つのLoad Balancer (32 FQDNまで対応可能) • ジオロケーション/IPベースのブロック
WEB/API 脆弱性診断	• Webアプリ向け自動ペネトレーション テストサービス（月間３アプリ）

ベースライセンスだけのご購入で
これらの機能を全て利用できます

F5XC WAAPの特徴

- **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
    - 本日ご紹介したClient-Side Defenseもベースパッケージ内に含まれます。

- 実績のあるWAF機能
  - 豊富な実績に基づいて提供されるWAF機能
  - さまざまなレポートと**容易なチューニング機能を提供**

- **予測可能なコスト**
  - 1年ベースのサブスクリプション・帯域課金によらない価格体系
  - ベース機能はドメイン(FQDN数)による課金
  - DDoS対策も標準機能に含まれているため、DDoS発生による追加コストも抑えられる
    (AWSなどのパブリッククラウド利用時のトラフィック課金対策)

- **Aレコードによる切り替えに対応**
  - オプションでお客様に固定グローバルIPアドレスを払い出し可能

東京エレクトロンデバイス F5XCサービスメニュー

F5 XC デモ

セキュリティ機能を中心にオンライン形式で実施しています。
セキュリティ以外の内容についても随時ご相談ください。

構築支援メニュー

PoC支援・構築支援サービスをご用意しています。
お気軽にご相談ください。

日本語サポート

弊社経由でご契約いただいた場合は、当社日本語でのヘルプデスクサポートがつきます。
※現状、メーカーダイレクトは英語サポートのみ

アラート通知サービス

F5XCのセキュリティアラートを当社でモニターし、
日本語に翻訳して初期対応方法を含めてお客様にメールでご案内するサービスです。

WAAPならびにClient-Side Defenseともに弊社販売実績がございます。

onnect Beyond

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