



Google Cloud 環境でのセキュリティ強化 WafCharm で実現！

専任不要・運用工数をかけないサイバー攻撃対策

坂口 龍一

株式会社サイバーセキュリティクラウド 営業部部長

会社紹介

世界有数のサイバー脅威インテリジェンスと AI 技術を活用し、
全世界に安心安全なサイバー空間を創造するサービスを提供します。



世界中の人々が安心安全に使える
サイバー空間を創造する



サイバー
セキュリティ



AI



自己紹介



株式会社サイバーセキュリティクラウド
営業部 部長

坂口 龍一

前職までは一貫して法人顧客向けの IT 商材の営業に従事し
インサイドセールスからフィールドセールスまでを幅広く経験。

現在は CSC の営業部長として部全体のマネジメントや
パートナー企業とのアライアンス構築に従事。



インターネット上の脅威

直近の被害事例

日本経済新聞 2022 / 3 / 1 記事より引用

ランサムウェア犯行グループの活性化

- 標的型攻撃の二重脅迫にも使用
- 破壊型ランサムウェアの存在

RaaS (Ransomware as a Service) の登場

⇒ 攻撃の実施がより容易に



<https://www.nikkei.com/article/DGXZQOFD0119F0R00C22A3000000/>

※ 日野自動車とダイハツ工業も同じ理由で同日、国内の工場を一部停止

Emotet の復権

| 2021 年 11 月頃から Emotet※ の活動再開を確認

- これまで大半は添付ファイル (Microsoft Word や Excel に仕込んだマクロ) を利用していた⇒最近では URL ダウンロード タイプも
- Emotet 本体には不正なコードをあまり多く含まない

| Emotet で開けられた「穴」を使った様々な犯行

- 情報を外部に持ち出される
- 他のマルウェア (ランサムウェアとか) 打ち込まれる
- 内外への拡散の「踏み台」にされる など

※ Emotet (エモテット): 2014 年に発見された非常に強い感染力を持つマルウェア。不正メールの添付ファイルが主要な感染経路で、情報窃盗に加えて他のウイルスの媒介も行う。

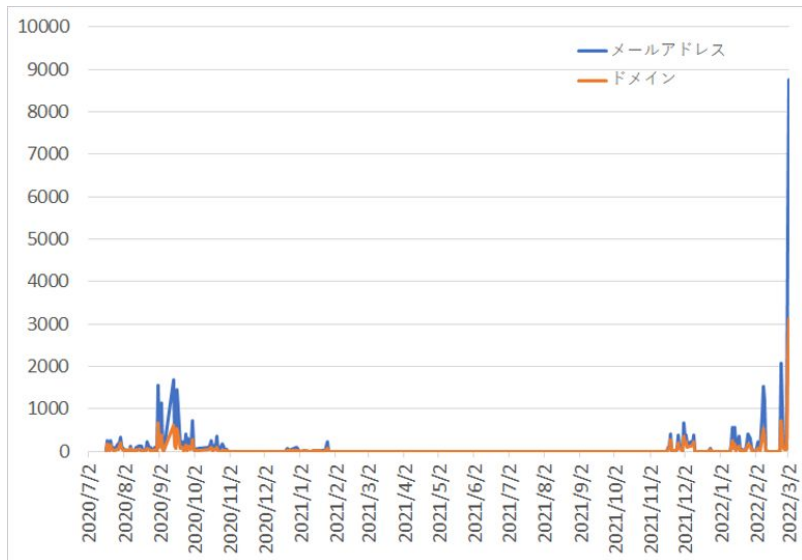
一度侵入されれば他のウイルスにも次々と感染してしまうため、甚大な被害に発展する危険性が高いマルウェアとして知られている。

直近の Emotet 動向

※ 2022 / 3 / 3 時点

国内の日々の新規の感染数は過去ピークの 5 倍以上

- 2021 年 1 月に一度は無効化されたが、さらに強力になって復活した



2022 年 3 月に入り、Emotet に感染しメール送信に悪用される可能性のある .jp メールアドレス数が 2020 年の感染ピーク時の約 5 倍以上に急増。国内感染組織から国内組織に対するメール配信も増加。

2022 年 3 月 3 日、なりすましの新たな手法として、メールの添付ファイル名やメール本文中に、なりすまし元の組織名や署名などが掲載されるケースもあり。Emotet が感染端末内のメーラーのアドレス帳から窃取したとみられる情報が用いられていると考えられる。

IPA: マルウェア Emotet の感染再拡大に関する注意喚起

<https://www.jpcert.or.jp/at/2022/at220006.html>

ISMS, PCIDSS,...認証をとれば安心なのか

| 決済代行企業のクレジットカードを含む情報流出

- プリペイド式電子マネー、クレジットカード決済、コンビニ決済など を扱うフィンテック企業

1. 社内管理システムに不正ログインがあった
2. アプリケーションへの SQL インジェクション攻撃があった
3. バックドアが設置されていた

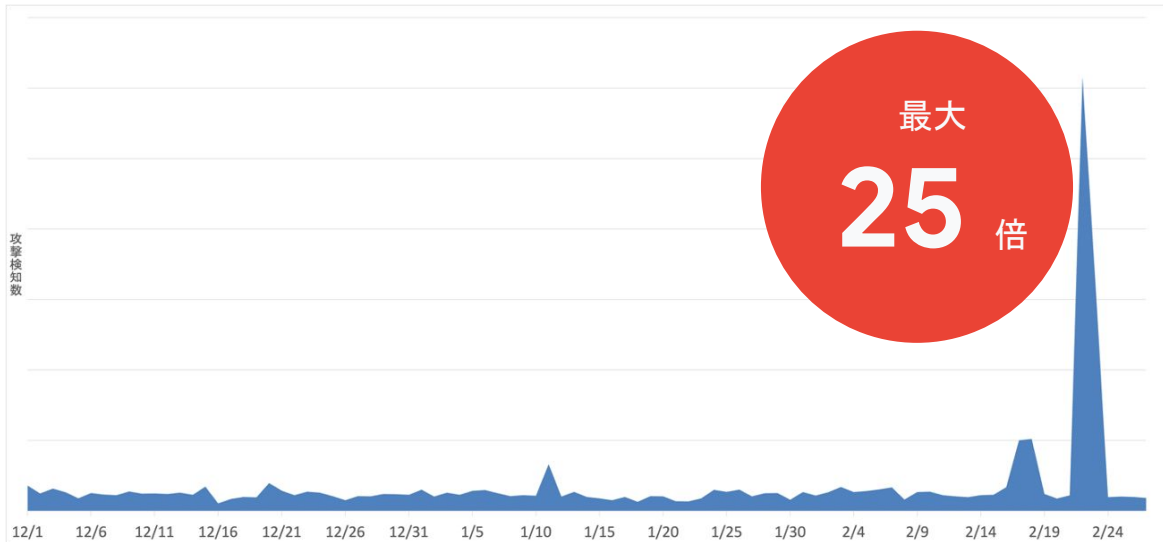
PCI DSS 準拠、ISMS 認証取得、プライバシーマーク取得



認証を取得しても、絶対安全な証明にはならない

Web サイトへの侵入数が増加

直近 3 ヶ月平均と比べて最大 25 倍もの攻撃を検知



- 上智大 Web サイトが改ざん、不正なサイトに閲覧者を誘導 (2022 / 2 / 26)
- 琉球大学移転事業 Web サイトが改ざん (2022 / 3 / 2)

※不審な攻撃者による不正アクセス、正確には BOT や脆弱性スキャンツールなどによる攻撃の検知

参考: 株式会社サイバー セキュリティクラウド調べ「サイバー攻撃検知レポート 2021」

政府からの関心も高まっている

| 金融庁の実態調査・通達

- 2020 年度に報告を受けたシステム障害は約 1500 件
- 2022 年は日銀と連携し、地方銀行のサイバー攻撃へのリスクを重点調査
- 同 2 月 24 日、全国の金融機関にサイバー セキュリティ対策強化を求める通達

| 2022 年 2 月 23 日 経済産業省から注意喚起

- 「昨今の情勢を踏まえ、サイバー攻撃事案の潜在的なリスクが我が国においても高まっていると考えられるため、企業の経営者等に対し、サイバー セキュリティの取組の一層の強化を促す」

※経済産業省 ニュース リリース <https://www.meti.go.jp/press/2021/02/20220221003/20220221003.html>



脅威への対抗

脅威に対抗するための対策案

| ランサムウェアも Emotet もマルウェア

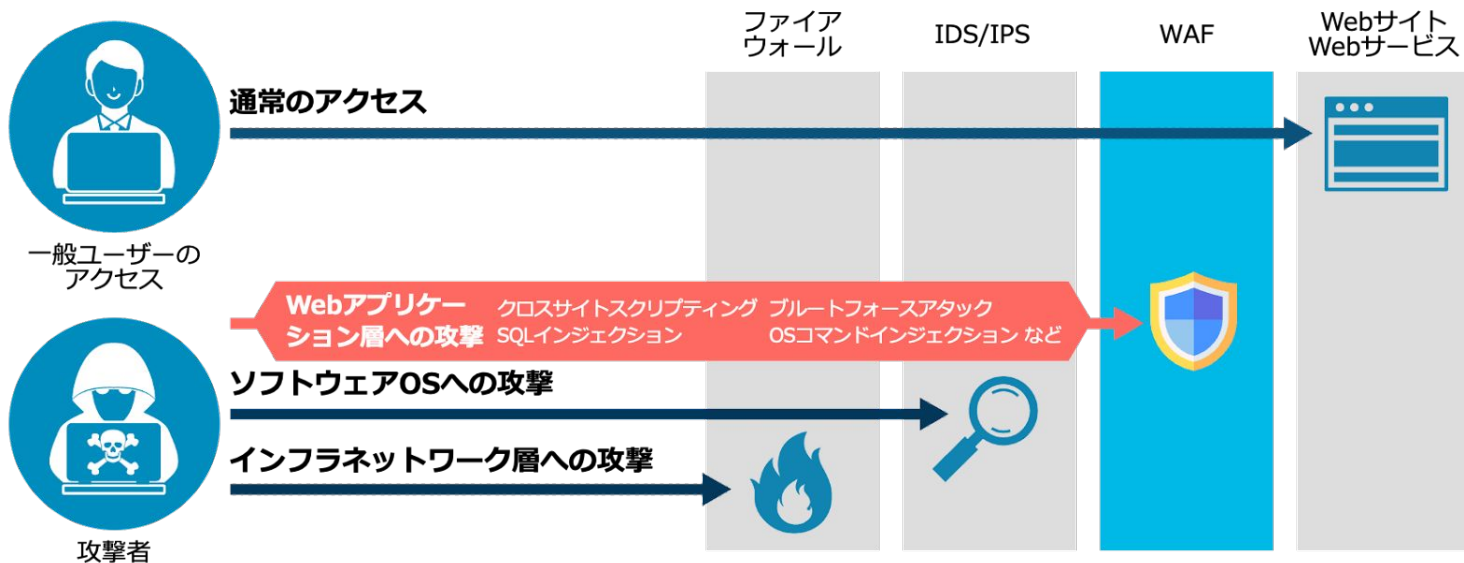
- ならば重要なのはマルウェア対策の基本

| マルウェアは脆弱性狙いが基本

- 攻撃者より先に、内部の脆弱性の有無を把握し、穴を埋める
 - ⇒ 脆弱性診断、脆弱性管理ツール
- 対応が追い付かない＝入口で防ぐ
- メール添付や URL リンク＝メール セキュリティ、アンチウイルス等
- Web サイト狙い ⇒ **WAF (Web Application Firewall)**

WAF とは？

従来の FW や IDS / IPS では防ぐ事ができない不正な攻撃から
Web アプリケーションを防御するファイアウォール

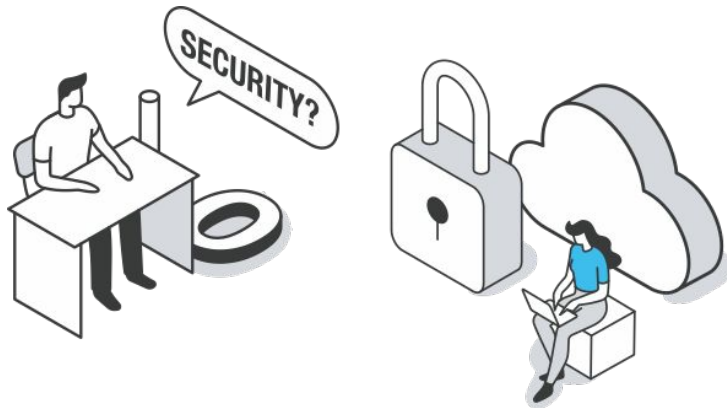




パブリック クラウドを利用する上で 考えるべき セキュリティ対策

パブリック クラウドのセキュリティ対策は不要？

パブリック クラウド※1は誰でも簡単に導入できる上に、大手企業が提供している場合が多いため、セキュリティ対策はすべてサービス提供者が対応してくれると誤解している場合も見受けられる。しかし、パブリック クラウドを利用する場合、**サービス利用者がセキュリティ対策を行わないといけない範囲**がある。



※1 パブリック クラウド: クラウド コンピューティング環境を、企業や組織をはじめとした不特定多数のユーザにインターネットを通じて広く提供するサービス。特定の利用者のみにアクセス権を限定した専用のクラウド環境をプライベート クラウドと言う。

パブリッククラウドの「責任共有モデル」

パブリッククラウドサービスでは、サービス提供者とサービス利用者のそれぞれが運用管理の責任を負う範囲が予め決められている。

Google Cloud では、「**アプリケーション レベルでのデータ制御**」は利用者(顧客)の責任」であることを掲示。

例えば、Google Cloud の IaaS ※2を利用する場合、サービス提供者の Google はセキュリティグループとしてファイアウォールの機能を提供するが、ファイアウォールの構成自体はサービス利用者が責任を負う範囲となる。

Google Cloud における責任共有モデルに対応する説明

(<https://cloud.google.com/security/?hl=ja> より抜粋)

Google Cloud プロジェクトの安全性確保

Google はお客様のプロジェクトの安全性を一部担いますが、セキュリティに対する 責任は Google 単体ですべてを担えるものではなく、お客様の協力が不可欠です。

機密データの管理

データの重要性はその性質により異なります。Google Cloud は、安全なアプリケーションの構築に必要な基本機能を提供していますが、これらのデータの 適切な移動やアクセスをアプリケーションレベルで制御するのはお客様の責任です。これには、エンドユーザーが企業ネットワークやパブリッククラウド インフラストラクチャの外 で重要な情報を共有しないよう防ぐ対策(データ損失防止)も含まれます。

各パブリッククラウドの責任範囲の定義例

責任共有モデル | AWS: <https://aws.amazon.com/jp/compliance/shared-responsibility-model/>

クラウドにおける共同責任 - Microsoft Azure | Microsoft Docs:

<https://docs.microsoft.com/ja-jp/azure/security/fundamentals/shared-responsibility>

※2 IaaS: Infrastructure as a Service。コンピュータ(仮想マシン)やネットワークなどのインフラ部分を提供するサービス。

Google Cloud Armor とは？

Google Cloud Armor は、DDoS 攻撃に対する防御や、IP アドレスによる通信制限、OWASP (Open Web Application Security Project) の ModSecurity に基づいた **WAF ルール等のセキュリティ機能を有効化することができる** 機能。

また、防御するだけでなく、どのような攻撃が行われたのかをテレメトリとして収集し、分析することが可能。



パブリック クラウドWAFのメリット・デメリット

- パブリック クラウドのサービス提供者は、それぞれのサービスに適した専用の WAF を提供している場合があり、Google Cloud では「Google Cloud Armor」。
- これらの専用の WAF は、パブリック クラウドに適した形で提供されているため簡単に導入可能。
- 一方で、WAF を使うには専門知識と専任で対応するリソースが必要で、自社で運用するには負荷が高いという課題がある。

パブリック クラウド提供の WAF のメリット

- ❑ 使った分だけの課金で安い
- ❑ すぐに導入できる
- ❑ ネットワーク構成の変更が不要
- ❑ 障害ポイントが増えない



パブリック クラウド提供の WAF のデメリット

- ❑ サイバー攻撃を分析・ルールの設定・検証が必要
- ❑ 日々発見される新規脆弱性への対応が必要
- ❑ 正しい通信をブロックしてしまう誤検知への対応が必要
- ❑ 上記を対応できる人材が必要

難点となる“セルフサービスでの運用”



便利なパブリッククラウド WAF ですが、
1点だけ難点となるのが

“セルフサービスでの運用”





パブリック クラウド WAF の課題、
解決できます！

サイバーセキュリティクラウドの提供サービス

自社で開発した SaaS 型セキュリティ サービスを全世界に提供しています。

クラウド型WAF

攻撃遮断くん



導入社数 / 導入サイト数

国内 No.1 ※1

AWS WAF/Azure WAF/
Google Cloud Armor
自動運用サービス

Waf Charm



導入ユーザ数

国内 No.1 ※2

aws marketplace

AWS WAF
Managed Rules



導入ユーザ数

**76カ国
2167** ※3
ユーザー以上

脆弱性管理
トータルソリューション

SIDfm™

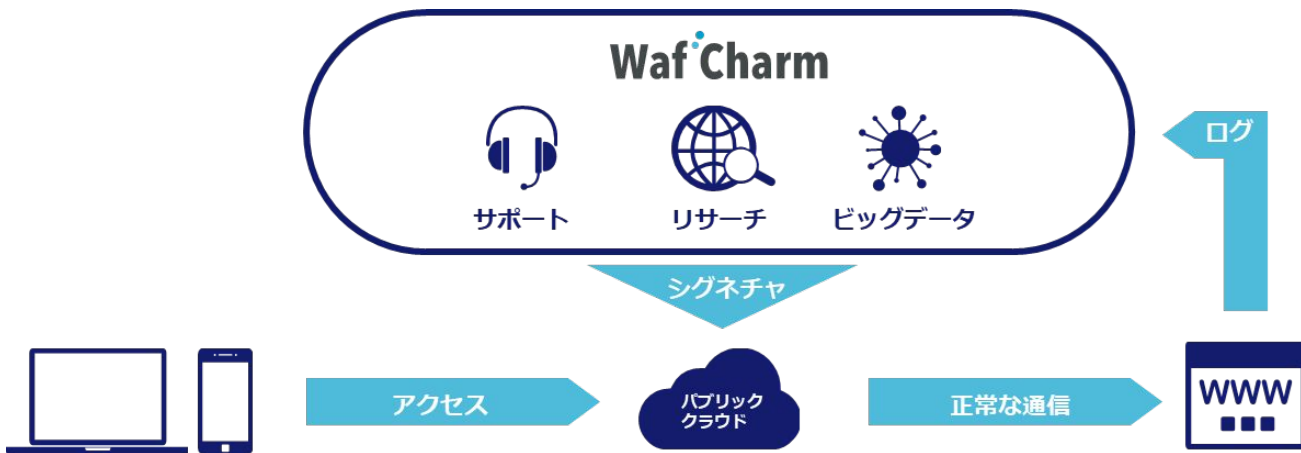


脆弱性情報配信サービスシェア
脆弱性情報提供実績
脆弱性オリジナルコンテンツ数

3部門国内 No.1 ※4

WAF 自動運用サービス「WafCharm」でお悩みを解決

WAF 自動運用サービス「WafCharm」とは、パブリック クラウド WAF のルールを最適化させる WAF 自動運用サービスです。WafCharm を利用することで、専任のセキュリティ エンジニアを必要とすることなく Google Cloud Armor などのパブリック クラウド WAF 運用を円滑に行うことができます。



3 大クラウドプラットフォームに対応

| AWS WAF、Azure WAF に加えて、
Google Cloud Armor に対応した「WafCharm for Google Cloud」を提供

| 3つのパブリッククラウドに対応したことで、世界シェア 65% のパブリッククラウドの WAF の自動運用をサポート可能に。

Google Cloud

AWS

Azure

WafCharm の特徴 1

強力な防御性能

WafCharm がお客様の環境に最適なルール(シグネチャ)を作成・設定を行います

お客様ごとに最適な防御をご提供

- CRS で不足しているルールを追加し、
防御性能の UP
- カスタマイズ可能
- シグネチャ新規作成も可能

数百ものシグネチャでより強力に

- 設定しているルールでは漏れる可能性も
- 漏れたものは数百ものシグネチャで
再マッチング
- 再マッチングで攻撃認定したものは
Blacklist に自動適用



面倒なルール作成は WafCharm におまかせ

WafCharm の特徴 2

楽な WAF 運用の実現

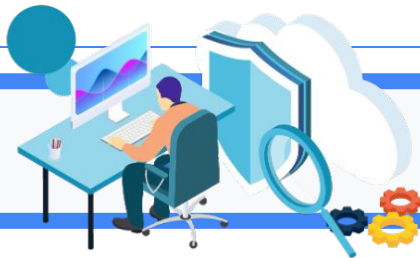
導入から新規の脆弱性対応までWAFを手放しで運用できます。

導入も運用も楽に

- 専用機器設置や DNS 切り替えなど
不要で導入もスムーズ
- お客様に代わってアクセスログを分析し、IP リストを
自動運用

新たな脆弱性にもお客様は対応不要

- 当社専任のセキュリティリサーチャーが監視
- 新規シグネチャを迅速に作成し、
即時適用。シグネチャでの対応が難しい場合は迅速にご案内します。



導入もスムーズ、運用も手放しで OK

WafCharm の特徴 3

日本のお客様を熟知した安心のサポート

日本のお客様を熟知した安心のサポートで誤検知時も安心

何か困ったらサポートへ

- 日本人による日本語サポート
- 24 時間 365 日の技術サポート※1
- 継続率 99% を誇るサポート

柔軟なサポート体制で安心

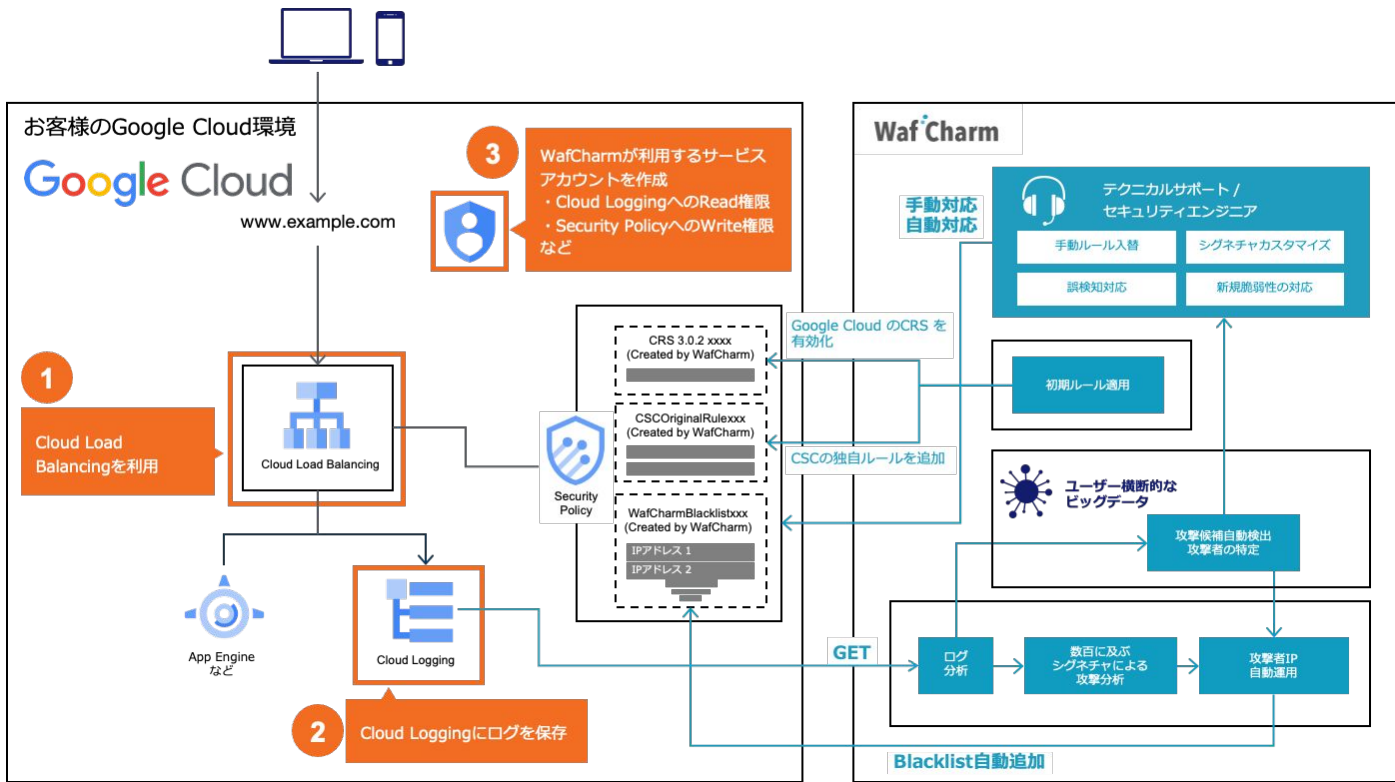
- 誤検知対応
- ルールの手動入れ替え
- カスタマイズにも柔軟に対応※1

※1 エントリープランを除く



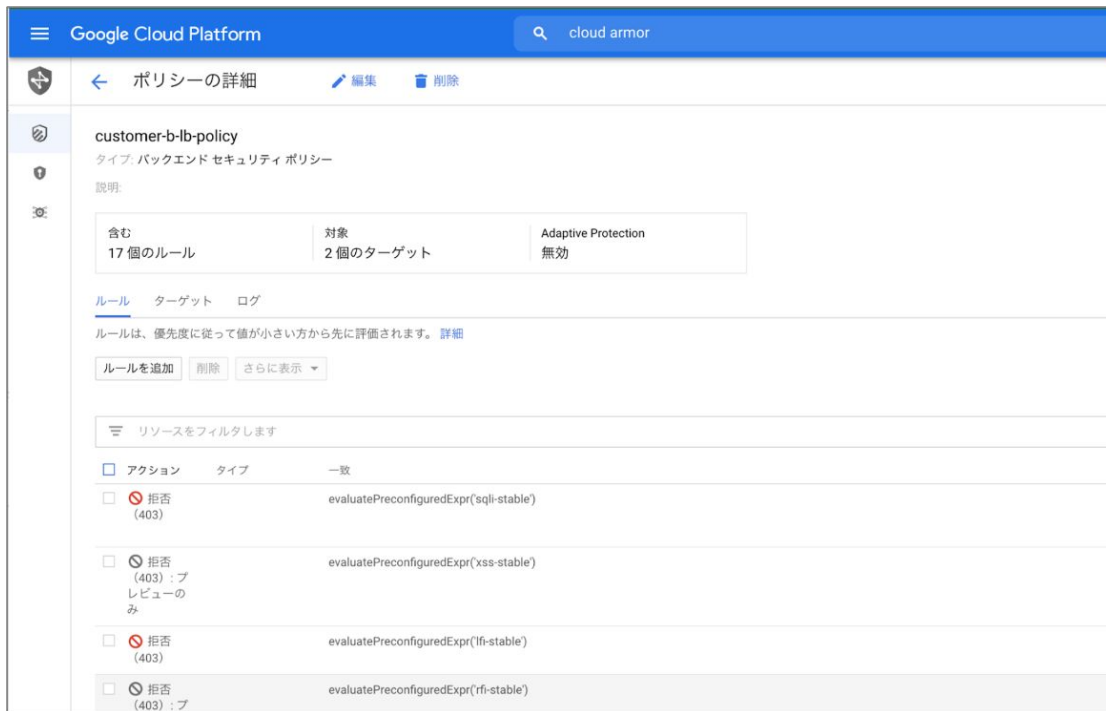
万全のサポートで、運用開始後も安心

WafCharm システム アーキテクチャ (Google Cloud 版)



プレビュー設定

Google Cloud Platform Console から該当のポリシーをプレビューに設定変更可能です。



Google Cloud Platform

cloud armor

← ポリシーの詳細 編集 削除

customer-b-lb-policy
 タイプ: バックエンドセキュリティ ポリシー

説明:

| | | |
|----------------|-----------------|---------------------------|
| 含む 17 個のルール | 対象 2 個のターゲット | Adaptive Protection 無効 |
|----------------|-----------------|---------------------------|

ルール ターゲット ログ

ルールは、優先度に従って値が小さい方から先に評価されます。詳細

ルールを追加 削除 さらに表示 ▼

リソースをフィルタします

| アクション | タイプ | 一致 |
|---------------------------------------------|-----|-----------------------------------------|
| <input type="checkbox"/> 拒否 (403) | | evaluatePreconfiguredExpr('sql-stable') |
| <input type="checkbox"/> 拒否 (403) : プレビューのみ | | evaluatePreconfiguredExpr('xss-stable') |
| <input type="checkbox"/> 拒否 (403) | | evaluatePreconfiguredExpr('lfi-stable') |
| <input type="checkbox"/> 拒否 (403) : プレビューのみ | | evaluatePreconfiguredExpr('rfi-stable') |

提供機能

| | 提供サービス | 備考 |
|-------------------|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| ルール関連 | 初期シグネチャ | Google Cloud Armor の予備領域に CRS に含まれないルールを追加展開 |
| | 新規脆弱性対応 | 適宜お知らせメールを発報 |
| | Geoルール作成 | 弊社サポートへ依頼にて対応 |
| Security Policy関連 | シグネチャ再マッチングによる IP 制御 | Google Cloud Armor 標準装備のシグネチャでは通過してしまう攻撃を判別し、攻撃者 IP アドレスをブラックリスト運用。 |
| | サイバーセキュリティクラウドの IP レピュテーションによる IP 制御 | 弊社サイバーセキュリティクラウドが作成した IP レピュテーションをユーザーの Google Cloud Armor に展開。 |
| | Whitelist 設定 | |
| サポート | 24時間365日 テクニカルサポート | <ul style="list-style-type: none"> ●シグネチャのカスタマイズ（ボディを検知するルール作成は対応不可） ●シグネチャの入れ替え ●誤検知対応 ●その他Q&A |

WafCharm 料金プラン

Web サイトのアクセス(リクエスト数)に合わせてプランを選択可能。

| 無料トライアル | エントリー | ビジネス | エンタープライズ |
|---------------|--------------------|---------------------|---------------------|
| 30日間無料 | 5,000 円/月 ~ | 50,000 円/月 ~ | 95,000 円/月 ~ |

料金詳細 / 機能比較

(税抜)

| | | 無料トライアル | エントリー | ビジネス | エンタープライズ |
|---------------|--------------------------|---------|--------------------|----------------------------|------------------------|
| 月額料金 A+B+C | (A) WAF設定ユニット料金 | 30日間無料 | 5,000円 | | |
| | (B) プラン料金 (ウェブリクエスト数) ※1 | 30日間無料 | 無料 (50万件まで) | 45,000円 (1,000万件まで) | 90,000円 (1億件まで) |
| | (C) ウェブリクエスト数追加料金 | 30日間無料 | 500 円/ 10万件 | 500 円/ 100万件 | 250 円/ 100万件 |
| メールサポート | | ○ | ○ | ○ | ○ |
| 手動ルール入替 | | ○ | ○ | ○ | ○ |
| 24/7サポート | | - | - | ○ | ○ |
| 電話サポート | | - | - | ○ | ○ |
| シグネチャカスタマイズ | | - | 都度お見積り(約2万円~/回) | ○ | ○ |
| 支払い方法 | | - | クレジット払い (月末締翌月払い) | クレジット払い、請求書払い (月末締翌月払い) | |

お得

※1 ウェブリクエストは WafCharm の1アカウント単位で合算されます。

※ 別途AWS WAF, Azure WAF, Google Cloud Armor の利用料金が掛かります。

導入実績

多くのお客様に導入いただき、AWS WAF の自動運用サービス導入ユーザー数国内No.1 を達成しております。

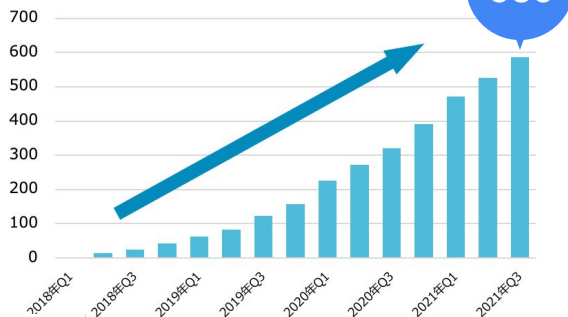


AWS WAF 自動運用サービス
導入ユーザー数

国内 **No.1**

日本マーケティング リサーチ機構調べ 調査概要:2020 年 7 月期 実績調査

WafCharm 課金ユーザー数



導入企業様
一例





Waf Charm

無料トライアル
実施中！



Google Cloud

Thank you.

