EG Secure Solutions

Web Application Firewall 導入ガイド

～Webアプリケーションを守る第一歩～

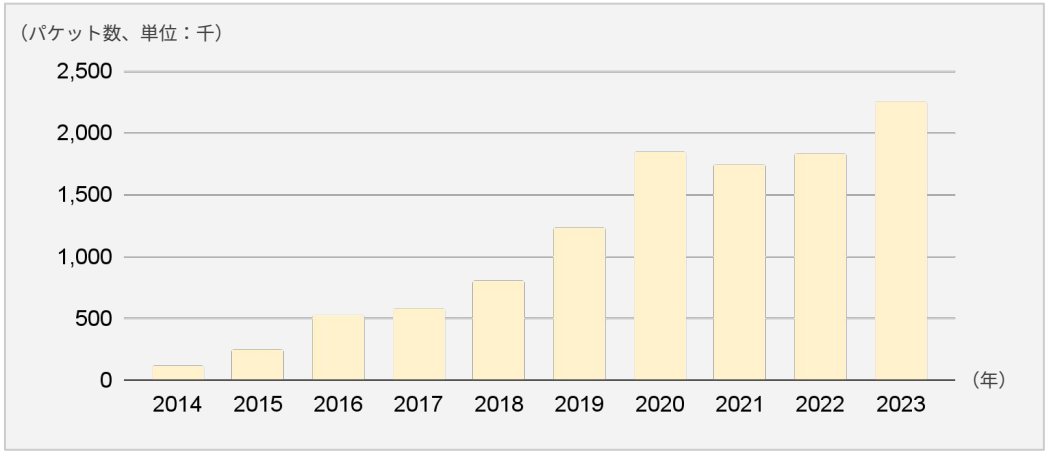
クラウド型／ソフトウェア型の純国産WAF

SITEGUARD

なぜWAFが必要なのか？

増加するWebアプリケーションへの攻撃

昨今、Webアプリケーションを標的とした攻撃は深刻な問題となっています。特に、ECサイトや顧客情報を扱うシステムへの攻撃は、データ漏洩や金銭的被害に直結するため、組織にとって重大なリスクとなっています。サイバー攻撃は年々高度化・巧妙化しており、従来の対策だけでは十分な防御が難しくなってきています。



サイバー攻撃のパケットは10年間で約20倍

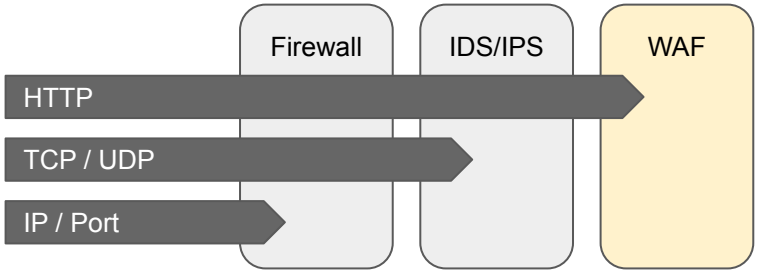
NICTERのダークネット観測網において観測されたサイバー攻撃関連通信の1 IPアドレス当たりのパケットが10年間で約20倍に増加

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）
出展：国立研究開発法人情報通信研究機構「NICTER観測レポート 2023」

なぜWAFが必要なのか？

ファイアウォールだけでは不十分

従来のファイアウォールは、IPアドレスやポート番号による制御が主な機能でした。しかし、現代のWebアプリケーション攻撃の多くは、正規のHTTP/HTTPSトラフィックを利用して行われるため、従来の対策では防ぎきれません。



WAFが導入されていれば防ぐことができる脅威

IPA 情報セキュリティ10大脅威 2025 [個人]	IPA 情報セキュリティ10大脅威 2025 [組織]
インターネット上のサービスからの個人情報の窃取	ランサム攻撃による被害
インターネット上のサービスへの不正ログイン	サプライチェーンや委託先を狙った攻撃
クレジットカード情報の不正利用	**システムの脆弱性を突いた攻撃**
スマホ決済の不正利用	内部不正による情報漏えい等
偽警告によるインターネット詐欺	機密情報等を狙った標的型攻撃
ネット上の誹謗・中傷・デマ	リモートワーク等の環境や仕組みを狙った攻撃
フィッシングによる個人情報等の詐取	地政学的リスクに起因するサイバー攻撃
不正アプリによるスマートフォン利用者への被害	分散型サービス妨害攻撃（DDoS攻撃）
メールやSMS等を使った脅迫・詐欺の手口による金銭要求	ビジネスメール詐欺
ワンクリック請求等の不当請求による金銭被害	不注意による情報漏えい等

出典：IPA（独立行政法人 情報処理推進機構）「情報セキュリティ10大脅威 2025https://www.ipa.go.jp/security/10threats/10threats2025.html

なぜWAFが必要なのか？

各業界のセキュリティガイドラインでWAF導入が基本要件となっています

日本検査機器工業会(JIMA)　：自工会/部工会・サイバーセキュリティガイドライン（車業界）

PCI SSC（PCI Security Standards Council）：PCIDSS v4.0

総務省　：自治体情報セキュリティクラウド

Webアプリケーションの脆弱性を悪用した攻撃の対策として有効

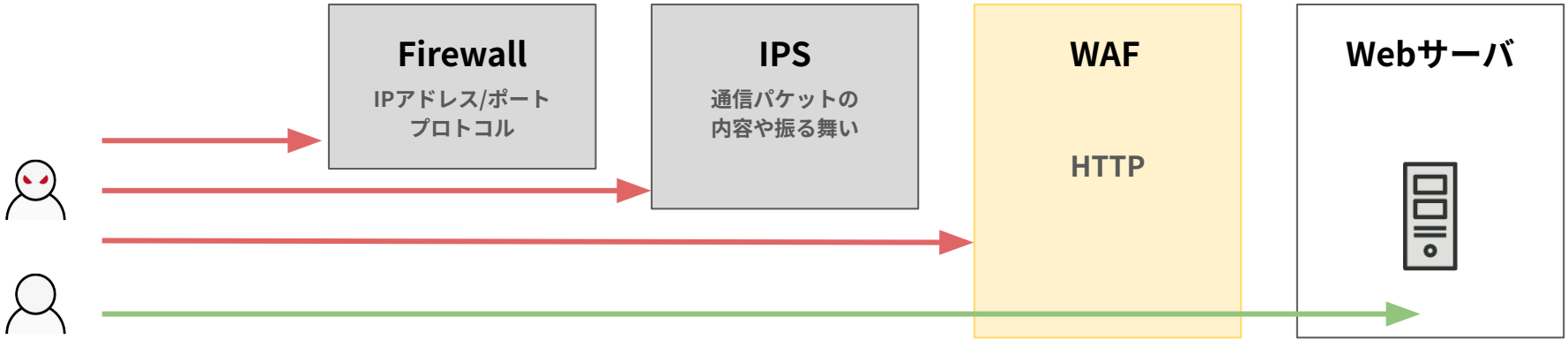
1. 大手住宅メーカー　：SQLインジェクションの攻撃を受け、会員制サイトの個人情報が数十万件漏洩した。
2. 外資系コーヒー店　：不正アクセスで決済アプリケーションが改ざんされ、数万件のクレジットカード情報が流出した。
3. 大手コンビニエンスストア：ブルートフォース攻撃により大量の不正アクセスが発生し、数百名のアカウントが被害を受け、数千万円の損害が報告された。

これらの攻撃はWAFで防ぐことができます

WAFの基本を理解する

WAFとは何か

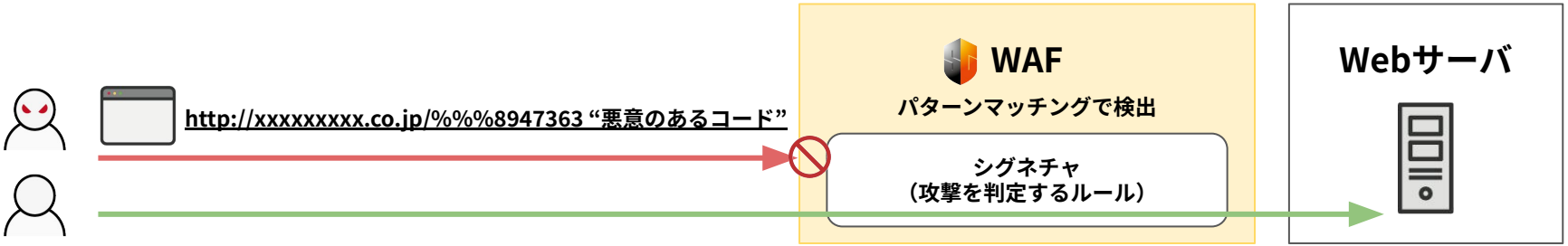
WAFはWebアプリケーションの保護に特化したセキュリティ対策で、HTTPプロトコルでやり取りされるデータを検査し、Webアプリケーションの脆弱性を悪用する不正アクセスからWebサイトを保護します。不正なパターンやシグネチャとのマッチング、異常な振る舞いの検知による制御などを組み合わせて、HTTPトラフィックを検査し多層的な防御を実現します。



WAFの基本を理解する

WAFによる防御の基本

WAFは、シグネチャ検査によって攻撃を検出します。HTTP リクエスト（リクエストライン、ヘッダ、本文）や HTTP レスポンス（ステータスコード、ヘッダ、本文）を解析し、既知の攻撃パターンと照合することで不正なアクセスを防ぎます。シグネチャには「ブラックリスト」と「ホワイトリスト」の二種類があります。ブラックリストは既知の攻撃パターンをブロックし、ホワイトリストは安全な通信のみを許可する方式です。一般的に「シグネチャ」とはブラックリストを指し、WAF 製品に標準搭載されるため、利用者は一から防御ルールを作成せずに統一的なセキュリティ対策を適用できます。



WAFの基本を理解する

WAFができること・できないこと

できること

- HTTP/HTTPSトラフィックの詳細な検査
- 既知の攻撃パターンの検知とブロック
- カスタムルールによる柔軟な防御設定
- リアルタイムの監視とログ記録

できないこと

- アプリケーションの脆弱性そのものの修正
- 内部犯行の完全な防止
- すべての未知の攻撃の防御

WAFの導入が有効なケース

脆弱性をすぐに修正できない

脆弱性の存在を把握しながらも運用上の理由からアプリケーションを修正できない場合があります。脆弱性の修正とWAF を併用することで現実的かつ効果的な対策が可能です。

今すぐ攻撃を防ぎたい

不正アクセスにより、ウェブサイトが実害を被ると対策完了までサービスの再開は困難です。ダウンタイムは機会損失に直結します。緊急対応的なWAF の活用は迅速なサイト復旧の大きな助けとなります。

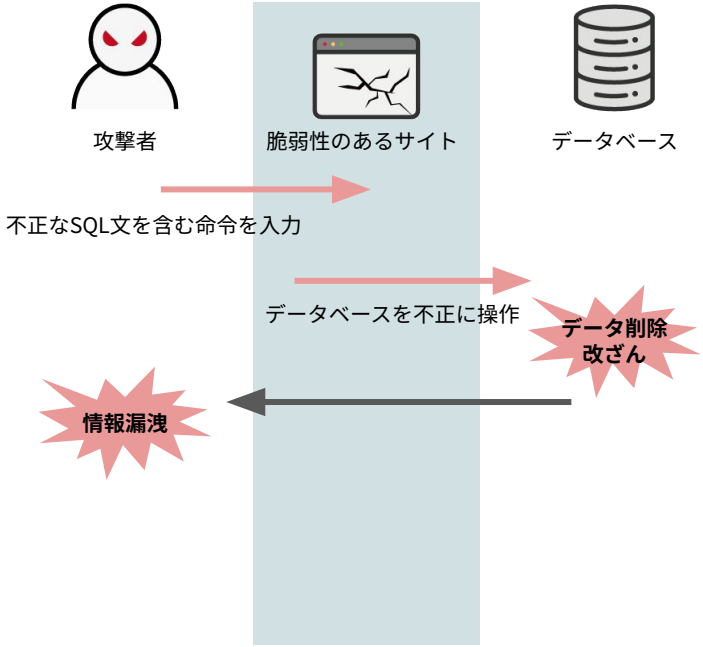
保険的対策をしたい

情報流出等の事故が起きてしまうと、直接・間接的に莫大なコストが発生します。事前対策としてWAF を利用することで、万が一のリスクを低減することができます。

WAFで防御できる代表的な脅威・攻撃手法とインシデント事例

SQLインジェクション

データベースを狙った攻撃の代表格であるSQLインジェクションに対し、WAFは入力値のチェックとフィルタリングを行います。データベースの不正操作に対して高い防御効果を発揮します。



事例: 2024年1月 地方自治体の住民情報システム侵害事案

住民情報システムの検索機能の脆弱性を突いたSQLインジェクション攻撃により、約12,000件の個人情報が流出。WAFによる入力値の検証があれば、不正な検索クエリを事前にブロックできた可能性が高いケースでした。この事例では、基本的な入力値チェックの欠如が重大な情報漏洩につながりました。

WAFで防御できる代表的な脅威・攻撃手法とインシデント事例

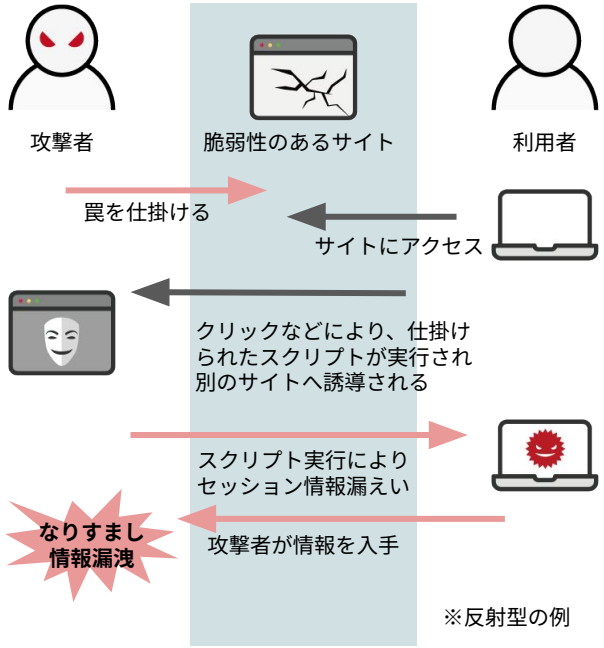
クロスサイトスクリプティング(XSS)

ユーザーのブラウザ上で悪意のあるスクリプトを実行させるXSS攻撃に対し、WAFはHTMLタグやJavaScriptコードの無害化（サニタイズ）を行います。反射型、格納型のXSS攻撃に対応します。

事例: 2023年11月 大手ECサイトでのアカウント乗っ取り事件

商品レビュー機能にXSS脆弱性が存在し、悪意のあるJavaScriptコードが埋め込まれました。これにより、レビューページを閲覧したユーザーのクッキー情報が攻撃者に送信され、アカウントの乗っ取りが発生。約5,000アカウントに影響が及びました。XSS対策に大きな防御効果を発揮するWAFが導入されていれば防げた事例です。

※格納型の事例



※反射型の例

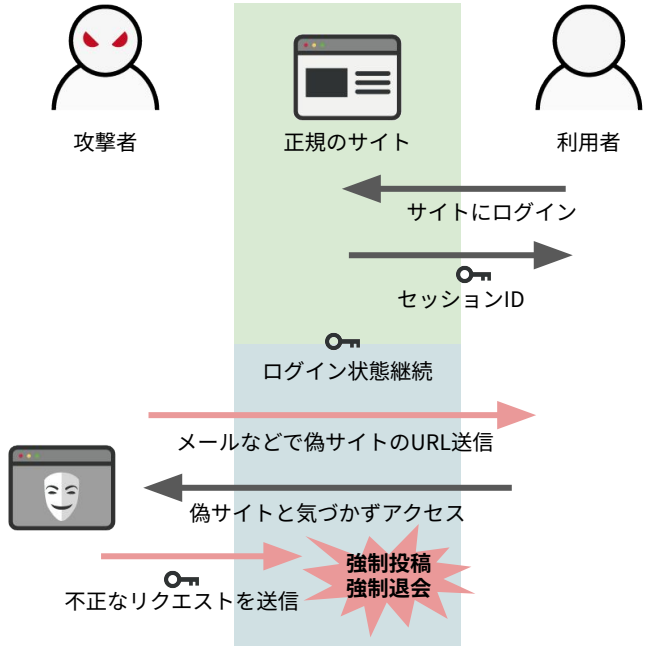
WAFで防御できる代表的な脅威・攻撃手法とインシデント事例

クロスサイトリクエストフォージェリ(CSRF)

ユーザーの意図しない操作を強制させるCSRF攻撃に対し、WAFはリファラーチェックやトークン検証などの対策を提供します。正規のフォームからの送信かどうかを確認し、不正なリクエストをブロックします。

事例: 2023年8月 仮想通貨取引所での不正送金事案

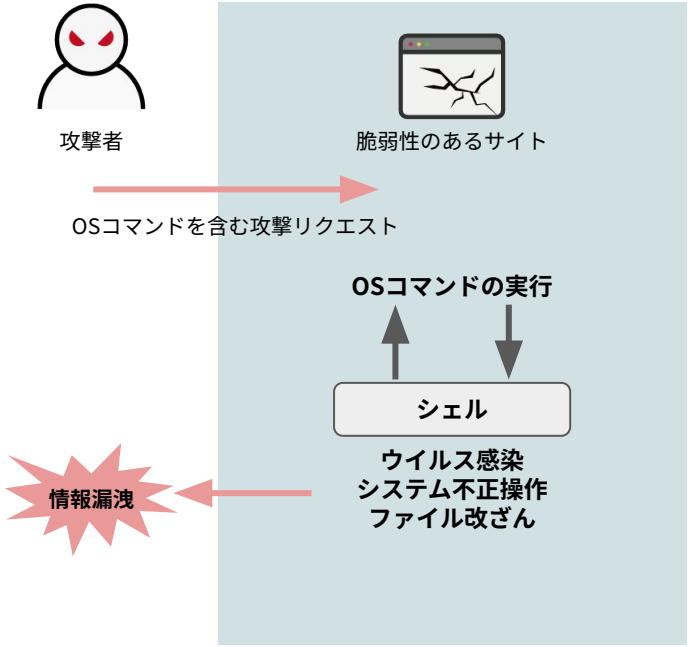
攻撃者が巧妙に細工したWebページをユーザーに閲覧させ、ユーザーが意図しない仮想通貨送金を実行させました。被害総額は約2億円に上りました。WAFが導入されていれば防げた可能性が高い事例です。



WAFで防御できる代表的な脅威・攻撃手法とインシデント事例

OSコマンドインジェクション

システムコマンドの不正実行を狙う攻撃に対し、WAFは特殊文字やコマンド文字列のフィルタリングを行います。不正なコマンド実行による情報漏えいや改ざん、不正操作に大して大きな防御効果を発揮します。



事例: 2023年10月 クラウドサービス事業者でのシステム侵害

PDFファイル生成機能に存在した脆弱性を利用し、システムコマンドが不正実行されました。この攻撃により、クラウドサーバー上の顧客データにアクセスされ、約23,000件の機密情報が流出。WAFによるOSコマンドインジェクション対策で防御可能でした。本事例では、入力値の不適切な処理が重大なセキュリティ事故につながりました。

WAF導入のメリット

インシデント事例から得られる重要な教訓

1. 基本的な脆弱性が依然として多く悪用され続けており、その被害規模は年々拡大傾向にあります。
2. 技術的対策の遅れが重大な被害につながっており、予防的対策の重要性が増しています。
3. WAFによる多層防御アプローチは、これらの攻撃に対する効果的な対策となります。
4. インシデント発生後の対応コスト（損害賠償、信用回復、システム改修等）は、予防的対策のコストを大きく上回ることが多いです。

これらの事例が示すように、WAFの導入は現代のWebセキュリティ対策において必須の要素となっています。特に、アプリケーションの改修が困難な場合や、ゼロデイ攻撃への対応が必要な場合に、WAFは非常に効果的な対策となります。

WAF導入のメリット

セキュリティ対策の効率化

WAFの導入により、複数の脆弱性に対する対策を一元的に管理できます。シグネチャの自動更新により、最新の脅威に対しても常に最適な防御を維持できます。

開発工数の削減

アプリケーションコードの修正を必要とせず、セキュリティ対策を実装できるため、開発者の負担を軽減できます。運用面での対策強化に加え、レガシーシステムのセキュリティ強化にも効果的です。

インシデント対応時間の短縮

リアルタイムの監視とログ記録により、セキュリティインシデントの早期発見と迅速な対応が可能です。攻撃の詳細な分析データを基に、効果的な対策を講じることができます。

ビジネスリスクの低減

データ漏洩や改ざんによる損害、信用失墜などのビジネスリスクを軽減できます。セキュリティ投資としてのROIも期待できます。

WAF選定のポイント

WAF導入前の検討事項

1

自社システムの現状把握

保護対象となるWebアプリケーションの構成、トラフィック量、使用している技術スタックなどを整理します。既存のセキュリティ対策との関係も確認が必要です。

2

保護すべき資産の特定

重要度の高いデータや機能を特定し、優先順位付けを行います。個人情報、決済情報、機密情報など、特に厳重な保護が必要な資産を明確にします。

3

予算と人員の確保

導入コスト、運用コスト、必要な人員体制を試算します。クラウド型とアプライアンス型で異なるコスト構造を比較検討します。

4

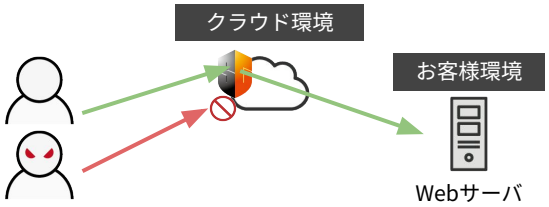
運用体制の検討

WAFの運用・管理を担当するチームの編成、必要なスキルの確認、教育・トレーニング計画の策定を行います。外部ベンダーとの役割分担も明確にします。

WAF選定のポイント

クラウド型

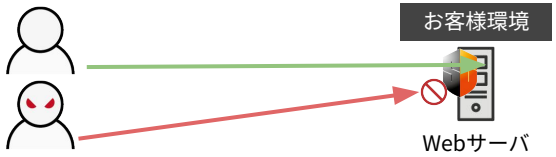
・DNSの切替で通信経路を変更する構成
・物理的なネットワーク構成を変更する必要なく導入が容易



メリット	初期投資が少ない、運用負担が軽い、スケーラビリティが高い
デメリット	レイテンシーの懸念、カスタマイズ性に制限

ソフトウェア型

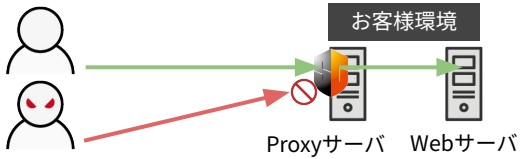
・Webサーバーのモジュールとして動作
・ネットワーク構成を変更せずに導入可能



メリット	導入が簡単、運用コストが低い、詳細なカスタマイズが可能
デメリット	運用負担が大きい

プロキシ型

・通信を中継するリバースプロキシとして動作
・1台のWAFで複数のWebサーバを保護



メリット	運用コストが低い、詳細なカスタマイズが可能
デメリット	導入と運用負担が大きい、レイテンシーの懸念

純国産WAF「SiteGuard」シリーズについて

SiteGuardシリーズ16年以上の実績

・保護対象数のサイト数は150万サイト超
・継続率99%以上
・WAF市場初期より国産メーカーとして販売期間16年以上
・IPA発行「WAF読本」へ監修協力するなど公的機関からの信用を獲得
・官公庁や金融機関をはじめ規模・業種問わず幅広い環境での導入実績
・Webサーバ数百台や数万VMなど大規模環境で安定稼働する品質
・高い運用性が求められる大手レンタルサーバーの多くで標準採用

※2023年12月期_指定領域における市場調査
※調査機関：日本マーケティングリサーチ機構

導入実績

SAKURA internet
KDDI Web Communications
KAGOYA JAPAN
GMOペパボ株式会社
GMO CLOUD
IDCFrontier
お名前.com レンタルサーバー
MIC 株式会社南日本情報処理センター
i2ts
ejworks.com
AIR Internet Service
株式会社 日立システムズ
UNICIDEX
TETRABIT
KIS
PLAYING NETWORK
UserSide

純国産WAF「SiteGuard」シリーズについて

エディション	Cloud	Server		Proxy
		マネージドライセンス	標準ライセンス／ プロキシライセンス	
導入構成	DNS切替え	モジュール、エージェント	モジュール	モジュール
インストール、アップデート	不要	必要	必要	必要
チューニング	マネージド（弊社）※1	マネージド（弊社）※1	セルフ（お客様）	セルフ（お客様）
シグネチャ更新	マネージド（弊社）※1	セルフ（お客様）	セルフ（お客様）	セルフ（お客様）
サポート	管理画面 （サポートフォーム）	電話・メール	電話・メール	電話・メール
DDoS対応	○※2	ー	ー	ー
国単位でのアクセス制御	○	ー	ー	ー
オートスケール機能	○	ー	ー	ー
SSL証明書（Let’s Encrypt）の自動取得・更新	○	ー	ー	ー

※1 平日のサポート業務時間（9:30-17:30）で対応。時間外は翌営業日での対応となります。
※2 ネットワークベースの攻撃（L3/4）に対応しています。

純国産WAF「SiteGuard」シリーズについて

1週間の無料トライアル環境をご利用いただけます

1. フォームからお申込み
2. 1～2営業日で環境をご用意
3. 1週間のトライアル
4. そのまま本番移行も可能

管理コンソールUI

評価のポイント

Point 1 - まずはログを取得

監視設定
「状態」を検出のみにすることで攻撃を検出しても遮断せず、ログのみを取得することが可能です。

Point 2 - 自社の運用に合わせてルールを設定

アクセス制御
アクセス制御機能でお客様独自のルールを登録することが可能です。国別フィルタや管理者IPを安全とみなすなど、グループ・サイトごとに細かく設定が可能です。

EG セキュアソリューションズについて

会社概要

名称	EGセキュアソリューションズ株式会社（英語表記：EG Secure Solutions Inc.）
所在地	〒105-0001 東京都港区虎ノ門1-2-8 虎ノ門琴平タワー 8F
設立	2008年4月2日
資本金	10,000,000円
従業員数	41名（2024年3月末時点）
役員	代表取締役　高谷 康久
株主	イー･ガーディアン株式会社100%(東証プライム/証券コード:6050)
取引銀行	三井住友銀行 丸の内支店
事業内容	・セキュリティ製品の開発、販売、サポート ・情報セキュリティ、情報システムに関する監査、コンサルティング ・情報セキュリティに関する調査、研究、執筆 ・情報セキュリティ関連の教育及びコンテンツ制作
取得資格	ISMS-AC【IS 575950/ISO 27001:2013】 情報セキュリティサービス基準【020-0012-20】

取締役ＣＴＯ　徳丸 浩

EGセキュアソリューションズ株式会社　取締役CTO
イー・ガーディアン株式会社　CISO
独立行政法人情報処理推進機構（IPA） 非常勤研究員 技術士（情報工学部門）

X：@ockeghem
著書:「 体系的に学ぶ 安全なWebアプリケーションの作り方
脆弱性が生まれる原理と対策の実践（ソフトバンククリエイティブ） 」

1985年京セラ株式会社に入社後、ソフトウェアの開発、企画に従事。1999年に携帯電話向け認証課金基盤の方式設計を担当したことをきっかけにWebアプリケーションのセキュリティに興味を持つ。2004年同分野を事業化。

2008年独立して、Webアプリケーションセキュリティを専門分野とするHASHコンサルティング株式会社（現EGセキュアソリューションズ株式会社）を設立。
脆弱性診断やコンサルティング業務のかたわら、ブログや勉強会などを通じてセキュリティの啓蒙活動をおこなっている。

2023年イー・ガーディアングループのCISOに就任。セキュリティレベル向上だけでなく、活動を通して得たノウハウをサービスやセミナーコンテンツにも還元し、広くセキュリティの啓蒙活動に邁進。

SiteGuardお問い合わせ窓口

sg-sales@eg-secure.co.jp
03-6257-3927
https://www.eg-secure.co.jp/siteguard