EG Secure Solutions

事例から学ぶWAFの有効性

EGセキュアソリューションズ株式会社

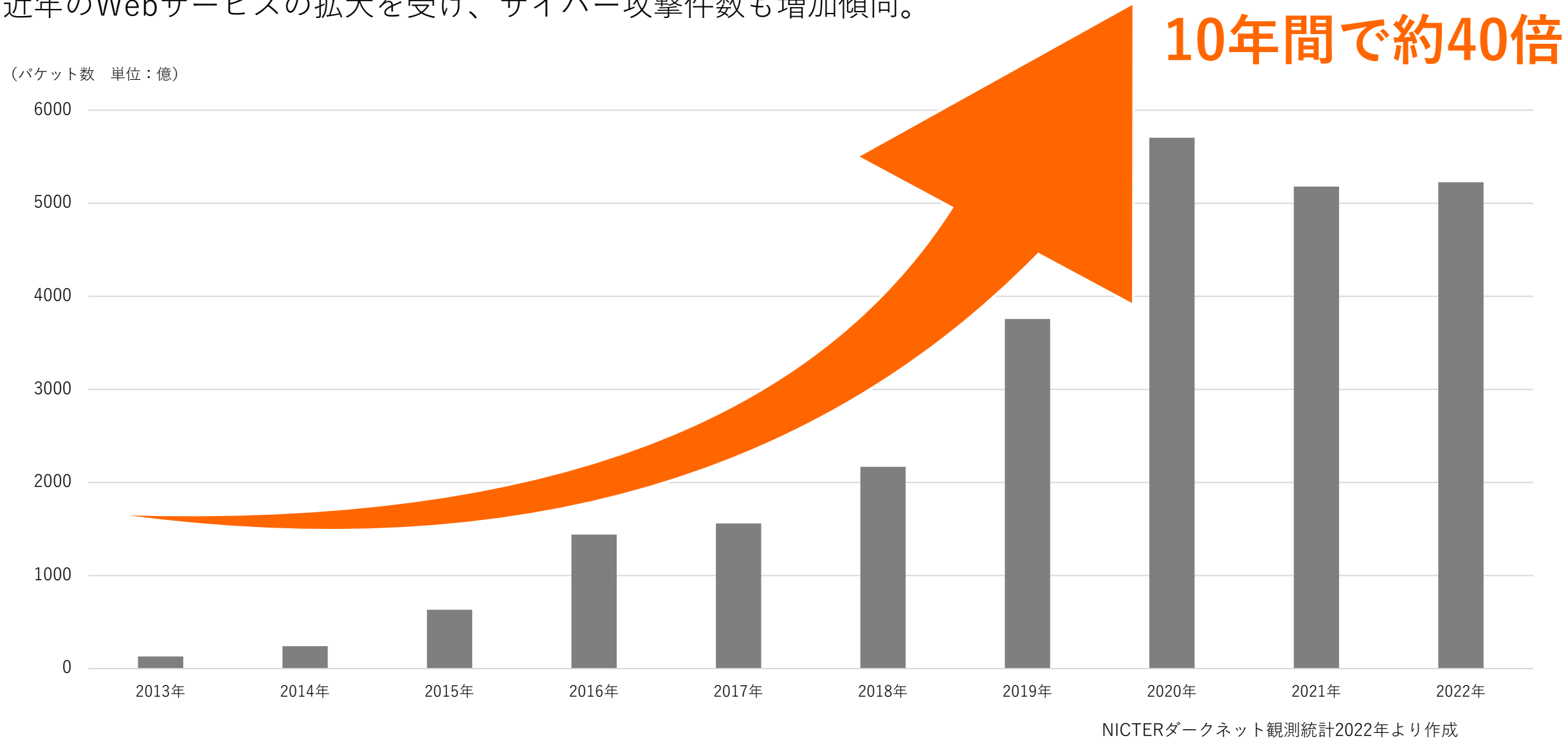
会社概要

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	1,000万円
従業員数	38名（2023年10月1日時点）
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】

※2023年10月1日現在

サイバー攻撃推移

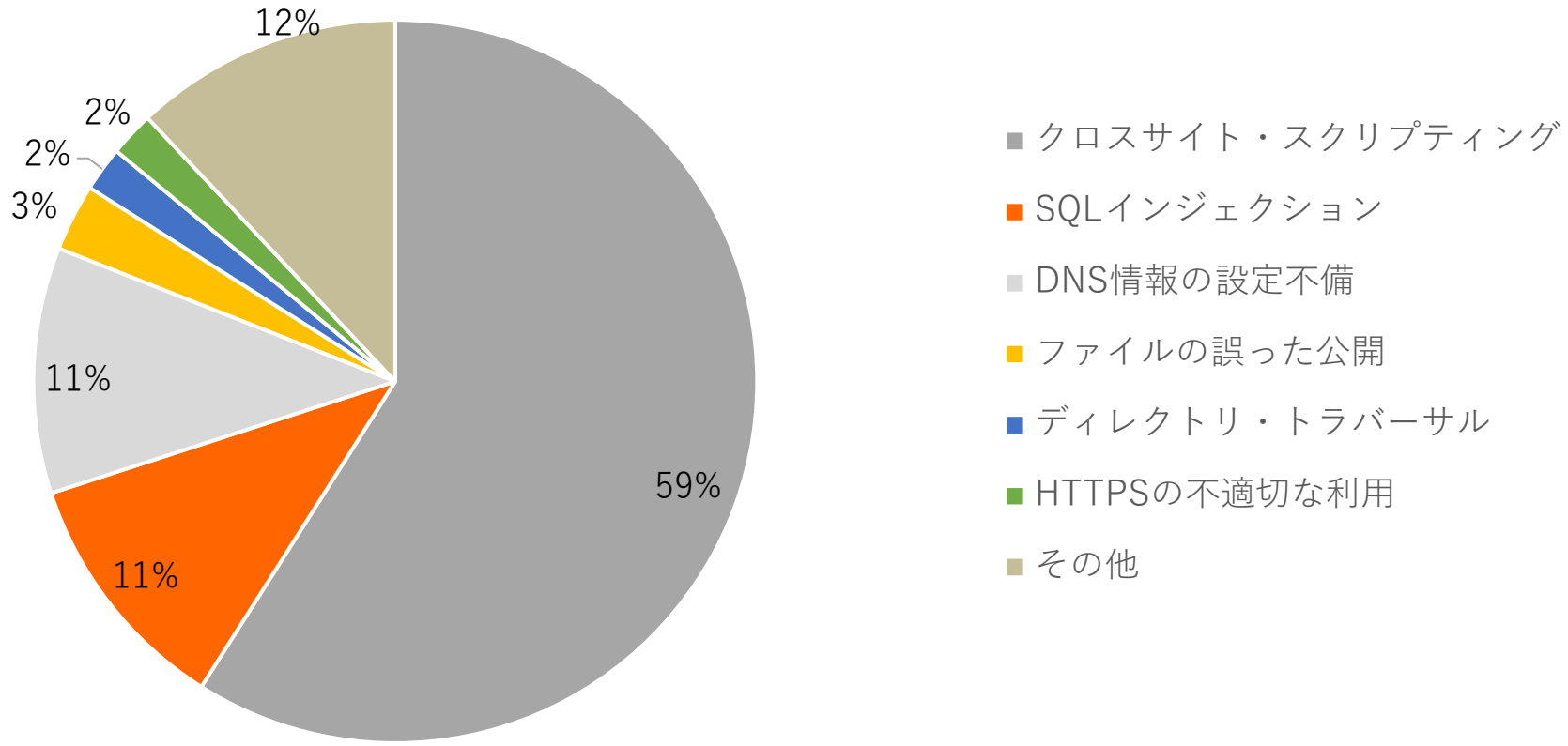
近年のWebサービスの拡大を受け、サイバー攻撃件数も増加傾向。



NICTERダークネット観測統計2022年より作成

重要インシデントの傾向

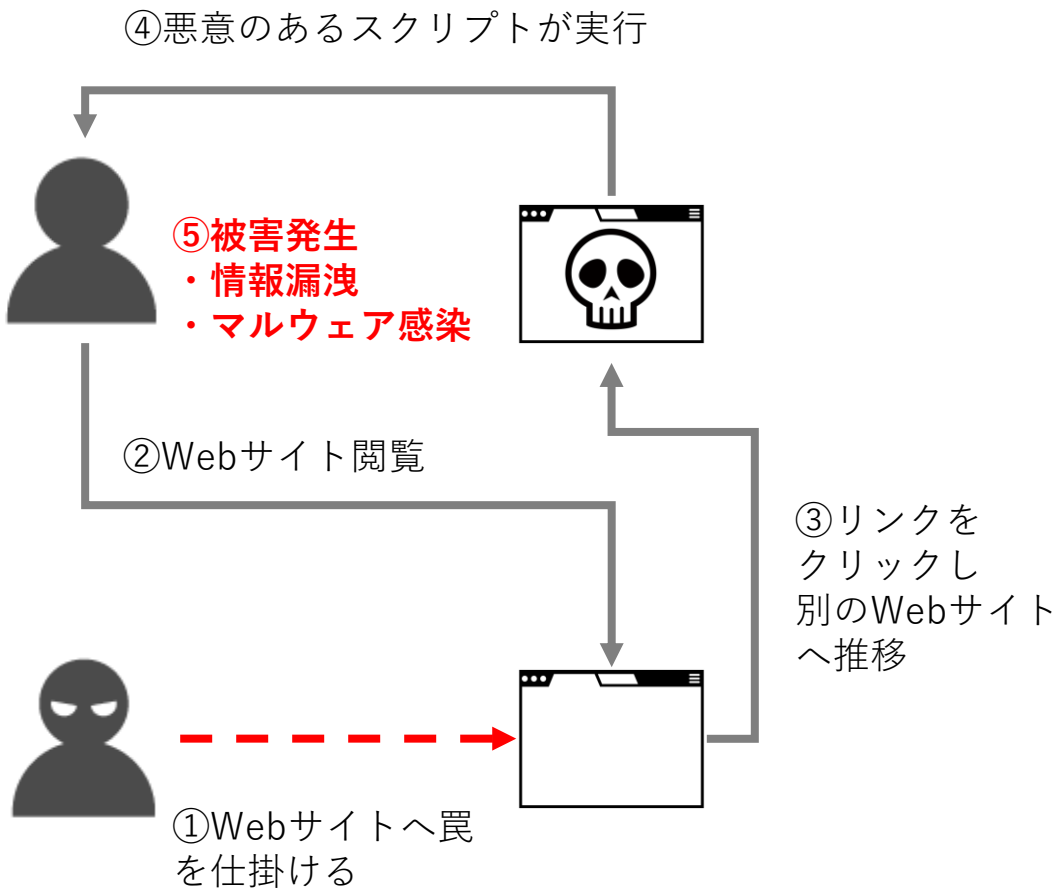
インターネットからの攻撃により発生した重要インシデントの内訳



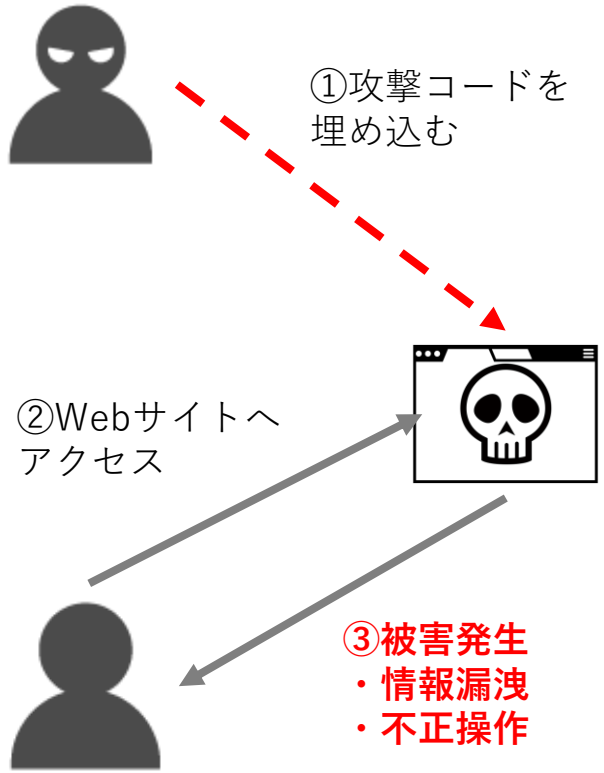
出典：情報処理推進機構（IPA）「ソフトウェア等の脆弱性関連情報に関する届出状況（2023年第2四半期）」

クロスサイトスクリプティング

■反射型XSS

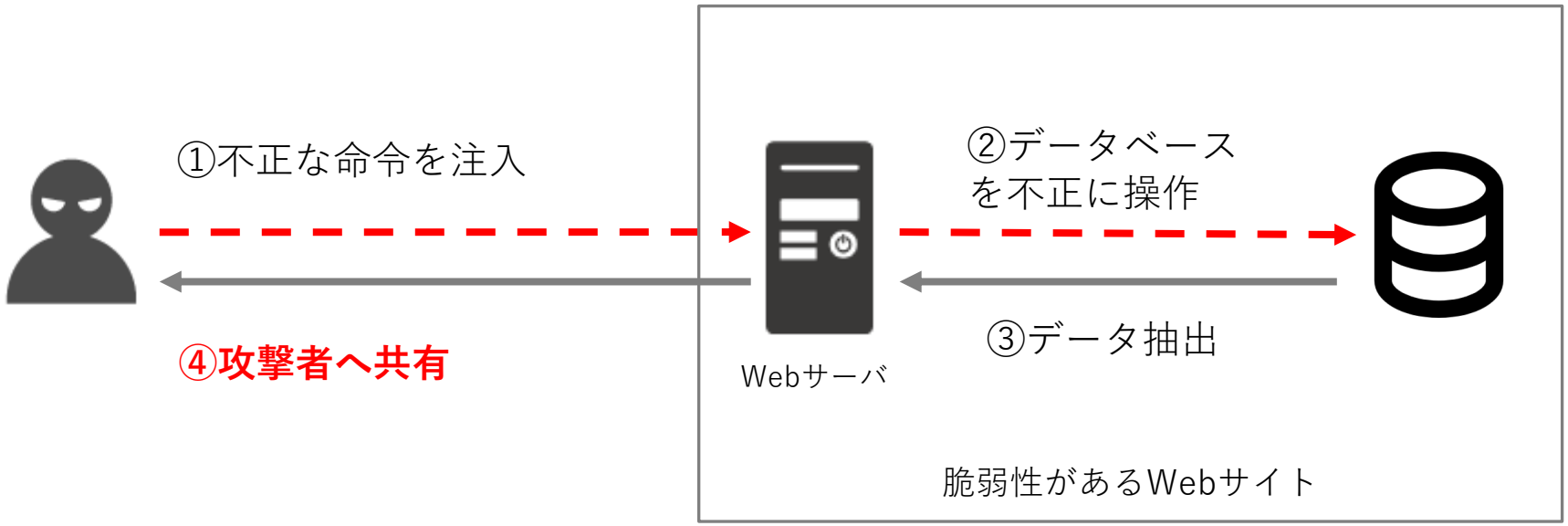


■持続型XSS（蓄積型XSS）



SQLインジェクション

Webアプリケーションが想定していないSQL文を実行させて、データベースを不正操作する攻撃方法



インシデント事例①

志布志市ふるさと納税サイトで情報流出 - 脆弱性検査で改ざん気付けず

鹿児島県志布志市は、同市のふるさと納税特設サイトが不正アクセスを受け、クレジットカード情報が流出し、不正に利用されたことを明らかにした。期間中にシステムのアップデートや脆弱性検査なども実施していたが、被害の発生に気づくことができなかったという。

同市によれば、2021年3月12日から同年12月29日にかけて、同市が運営する「志布志市ふるさと納税特設サイト」でクレジットカード決済を利用した寄付者に関する個人情報910件が流出した可能性があることが判明したもの。

クレジットカードの番号、有効期限、セキュリティコードのほか、メールアドレスやサイトのログインパスワード、電話番号などを第三者によって窃取された可能性がある。2023年4月6日にクレジットカード会社より情報流出の可能性について指摘があり問題が発覚した。6月26日の時点で65人で被害が確認されており、合計被害額は2万2000円としている。

同サイトは「EC-CUBE」をベースにシステムが構築されており、「EC-CUBE」の本体に存在したクロスサイトスクリプティングの脆弱性を突かれ、2021年3月12日にサーバ内に情報を窃取するプログラムを埋め込まれた。当時は「同4.0.2」が稼働していたという。

「EC-CUBE」に関しては、2021年5月に脆弱性「CVE-2021-20717」が明らかとなっている。「同4.0.5」および以前のバージョンが影響を受ける脆弱性で、同サイトで稼働していたバージョンとも重なるが、外部事業者の調査では、実際に悪用された脆弱性の特定には至らなかった。

（Security NEXT - 2023/06/26 ）

健康食品通販サイトに不正アクセス - 個人情報流出の可能性

健康食品や化粧品を取り扱う通信販売サイト「健康いきいきライフスタイル」が不正アクセスを受け、クレジットカード情報をはじめとする顧客の個人情報が外部に流出したことがわかった。

同サイトを運営するファインエイドによれば、クロスサイトスクリプティング（XSS）の脆弱性を突く不正アクセスがあり、クレジットカード決済処理時に個人情報を窃取するようアプリケーションが改ざんされたという。

同サイトを侵害されたことにより、2021年1月5日から2023年11月15日にかけて、同サイトを利用した顧客5193人に関する個人情報が外部に流出した可能性がある。

対象となるのは、氏名、住所、電話番号、メールアドレス、生年月日、性別、注文履歴。クレジットカードの名義、番号、有効期限、セキュリティコードなども含まれる。

2023年12月11日にクレジットカード会社から情報が流出している可能性について指摘があり問題が発覚。クレジットカードによる決済を停止するとともに、外部協力のもと調査を実施した。

（Security NEXT - 2024/02/01）

インシデント事例②

ほくせんカードの会員サイトにSQLi攻撃 - 顧客情報4.4万件が流出の可能性

クレジットカード事業を展開するほくせんは、クレジットカード会員向けサイトが不正アクセスを受けたことを明らかにした。顧客の個人情報や加盟店に関する情報が流出した可能性があるという。

同社によれば、クレジットカードの利用明細などを確認できる「ほくせんWebサービス」が、1月17日に「SQLインジェクション」の脆弱性を突く不正アクセスを受けたもの。

同社では同サイトを停止。外部事業者が調査を行ったところ、サーバ内に保存されていた加盟店に関する情報615件含む4万4559件の個人情報が外部に流出した可能性があることが判明した。

3万9310件については、「ログインID」「パスワード」「メールアドレス」が流出。さらに190件については、これら情報にくわえて、「氏名」「住所」「電話番号」「生年月日」「性別」「口座情報」「暗証番号」が含まれる。

これ以外にメールアドレス5059件が流出した可能性があるが、クレジットカードの番号、有効期限、セキュリティコードの流出については否定した。

（Security NEXT - 2022/05/20 ）

スニーカーフリマアプリで個人情報275万件が流出か

スニーカーフリマアプリ「SNKRDUNK」が不正アクセスを受け、会員の個人情報が流出した可能性があることがわかった。

同サービスを運営するSODAによると、データベースに対して不正アクセスが行われたことが6月7日に発覚。確認したところ会員情報275万3400件が外部に流出した可能性があることが明らかとなった。

氏名、住所、電話番号、生年月日、メールアドレス、購入情報、ハッシュ化されたパスワードなどが含まれる。10件に関しては口座情報が含まれていた。

約6割の顧客については、流出した項目が生年月日、メールアドレス、ハッシュ化されたパスワードのみに限られる可能性もあるという。

同社では、警察に被害を相談し、個人情報保護委員会へ報告を行った。対象となる会員に対しては、6月15日よりメールにて経緯の報告と謝罪を行っている。

セキュリティ対策としてウェブアプリケーションファイアウォール（WAF）を導入。脆弱性診断や不正アクセスの監視強化などを実施した。引き続き、調査を継続していくとしている。

（Security NEXT - 2022/06/15 ）

難しい脆弱性ゼロ

- セキュアプログラミングの徹底が難しい
- 脆弱性の修正には30日以上を要することが多い

【ウェブサイトの修正に要した脆弱性種類別の日数の傾向】

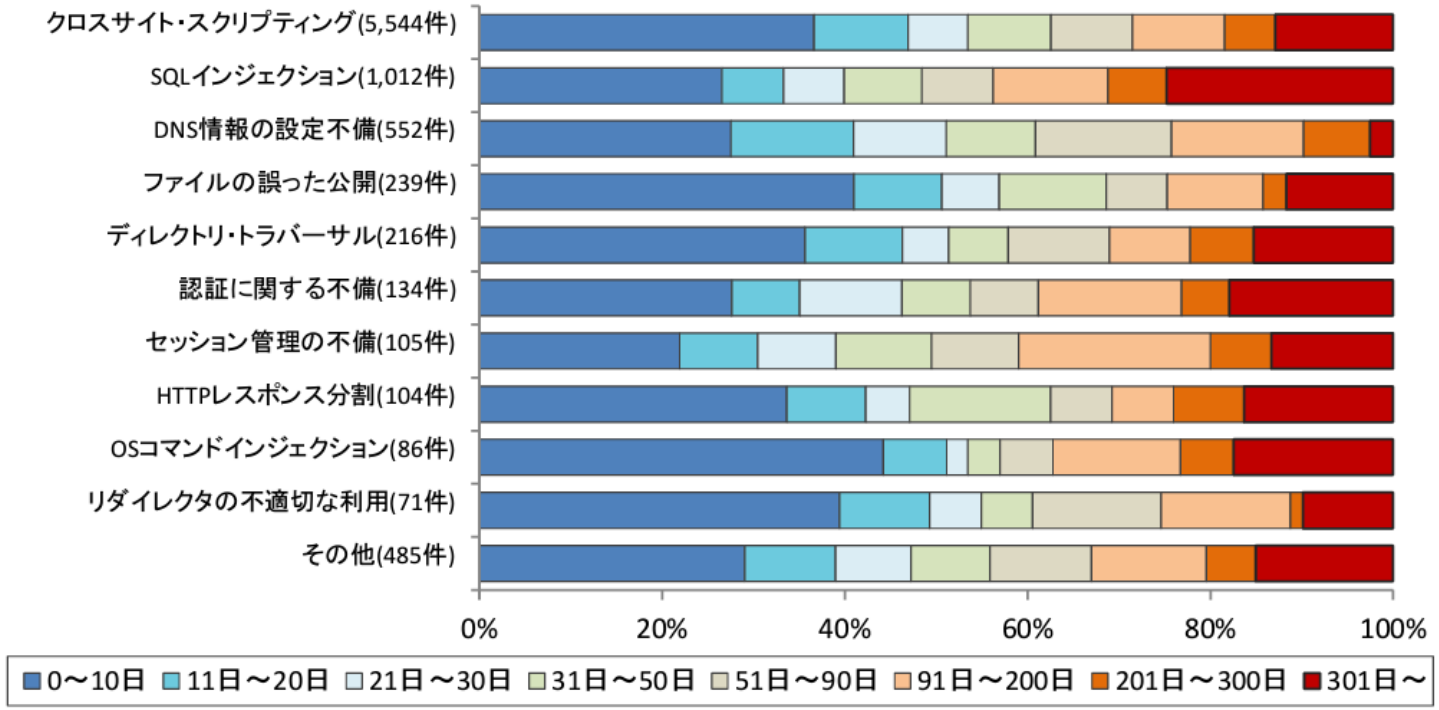


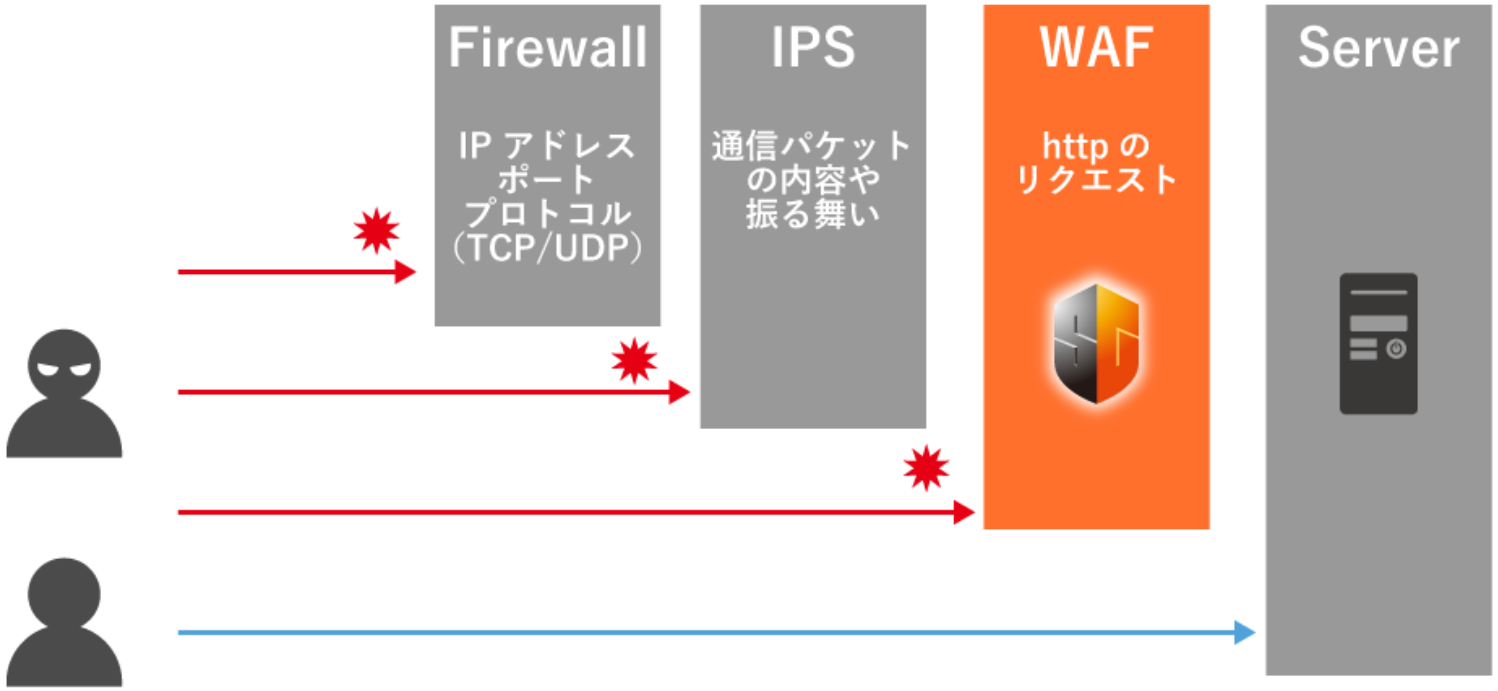
図2-21. ウェブサイトの修正に要した脆弱性種類別の日数の傾向

出典：情報処理推進機構（IPA）「ソフトウェア等の脆弱性関連情報に関する届出状況（2023年第2四半期）」

Web Application Firewall

（ウェブアプリケーションファイアウォール）

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。



Webサイトはなぜねらわれるのか

・Webを基盤とした各種サービスは、私たちの日常生活に欠かせない
・その利便性の反面、データベース内の情報窃取などの被害が後を絶たない
・セキュリティ上の欠点（脆弱性）を抱えているWebサイトが狙われている
・攻撃を受けると、直接的・間接的な被害が大きくなる可能性がある

①セキュリティ対策が甘く、効率的に目的を達成できる

②他の企業への攻撃の踏み台として利用できる

・ネットショップなどのWebサービスの個人情報奪取
・ホームページ改ざんによる金銭獲得
・興味本位のイタズラ・迷惑行為

WAF導入のメリット

IPA「情報セキュリティ10大脅威 2023[組織]」

順位	組織	前年順位
1位	ランサムウェアによる被害	1位
2位	サプライチェーンの弱点を悪用した攻撃	3位
3位	標的型攻撃による機密情報の窃取	2位
4位	内部不正による情報漏えい	5位
5位	テレワーク等のニューノーマルな働き方を狙った攻撃	4位
6位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	7位
7位	ビジネスメール詐欺による金銭被害	8位
8位	脆弱性対策の公開に伴う悪用増加	6位
9位	不注意による情報漏えい等の被害	10位
10位	犯罪のビジネス化（アンダーグラウンドサービス）	圏外

IPA「情報セキュリティ10大脅威 2024[組織]」

順位	組織	前年順位
1位	ランサムウェアによる被害	1位
2位	サプライチェーンの弱点を悪用した攻撃	2位
3位	内部不正による情報漏えい等の被害	4位
4位	標的型攻撃による機密情報の窃取	3位
5位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	6位
6位	不注意による情報漏えい等の被害	9位
7位	脆弱性対策情報の公開に伴う悪用増加	8位
8位	ビジネスメール詐欺による金銭被害	7位
9位	テレワーク等のニューノーマルな働き方を狙った攻撃	5位
10位	犯罪のビジネス化（アンダーグラウンドサービス）	10位

「Apache HTTP Server」のゼロデイ脆弱性、国内でも攻撃を観測

ウェブサーバ「Apache HTTP Server」にゼロデイ脆弱性「CVE-2021-41773」が明らかとなった問題で、国内でも攻撃が観測された。セキュリティ関係者が広く注意を呼びかけている。

問題の脆弱性「CVE-2021-41773」は、パストラバーサルの脆弱性。ドキュメントルート外のファイルでも、明示的にアクセス制限を行っていないと漏洩するおそれがある。9月16日にリリースされた「同2.4.49」で生じたもので、同バージョンのみ影響を受ける。

※Security NEXT

Log4jの脆弱性が大きな話題になった影響もあり、修正プログラム公開前のゼロデイ攻撃がランクイン

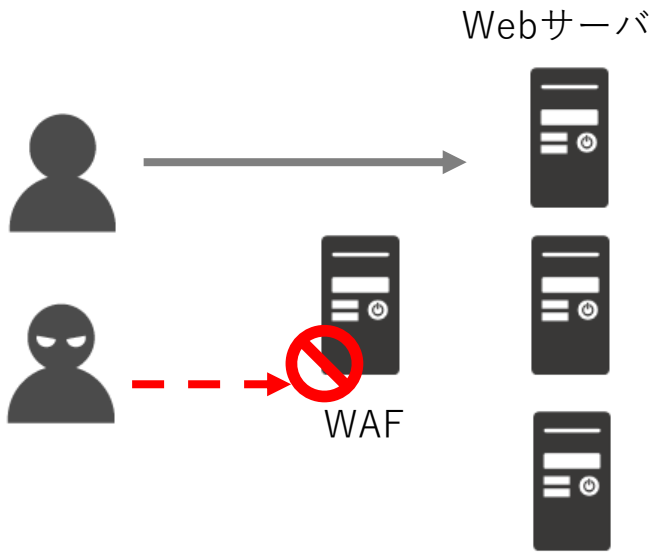
Log4jのように影響する範囲が広く、即座に対応することが難しいケースに備え、**WAFを導入**しておくことで、迅速な対応が可能。

WAFの種類

WAFにはいくつかの種類があるため、サイトの特性にあわせて選定ください。

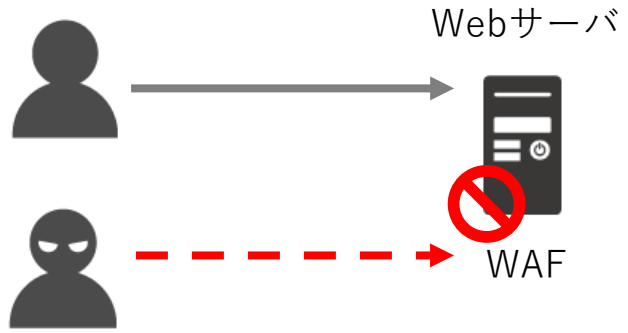
ゲートウェイ型

・Webサーバと独立して動作
・複数のWebサーバを保護できる
・Webサーバの環境に依存しない
・ネットワークの構成変更が必要



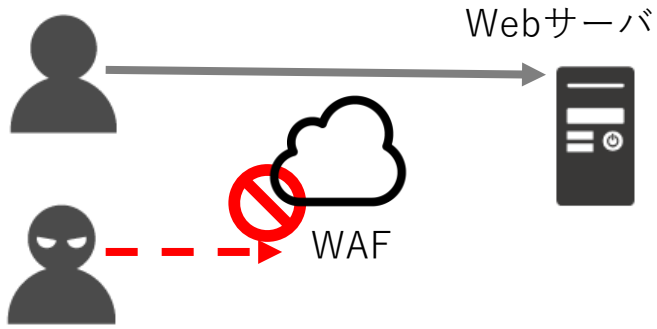
ホスト型

・Webサーバのモジュールで動作
・ネットワークの構成変更が不要
・シンプルな構成で導入できる
・利用料がサイト数や通信量に影響されない
・Webサーバ毎にインストールが必要



クラウド型

・クラウド上のWAFで動作
・運用管理を任せることができる
・DNSの切替、サイト登録が必要
・サイト数や通信量で費用が変動する



WAFの選定ポイント

お客様の環境や予算に合わせて選定ください。

ゲートウェイ型

・高機能で柔軟な設定をしたい
・サーバ台数が多い
・組織外に設置できない
・大規模サイト

ホスト型

・サイト毎に柔軟な設定をしたい
・サーバ台数は少ないが、サイト数や通信量が多い
・クラウド型でのデメリットが気になる（一時的なトラフィック増やメンテナンスによる通信断など）
・中小規模のサイト

クラウド型

・手軽にWAFを使いたい
・専任の管理者がいないため、外部に任せたい
・サーバ台数もサイトも少ない
・変動が少ないサイト
（例：コーポレートサイト）

■新しい脅威への対応
・対応できるWebアプリケーションへの攻撃手法。新しい脆弱性や国内で流行している脆弱性への対応の速さ

■サイトとの相性
・サイトの規模や特性、運用形態に見合っているか
・特定のサイト、アプリケーションに対応できるカスタマイズ性と柔軟性

■運用管理のしやすさ
・管理画面が直感的な操作があり、簡単で使いやすく、設定方法が煩雑でない
・定期的なアップデートや迅速なサポートなどの対応がある

SiteGuardシリーズ

SITEGUARD

SITEGUARD Cloud Edition クラウド型 WAF

・DNS切替のクラウド型WAF
・最短2営業日～ご利用開始
・ネットワーク構成変更不要
・初期登録とDNS切り替えのみ

SITEGUARD Server Edition ソフトウェア型 WAF

・Webサーバのモジュールとして動作するホスト型WAF
・ネットワーク構成を変更せずに導入可能
・管理するサーバを増やさずに導入可能
・シンプルに導入が可能

SITEGUARD Proxy Edition ソフトウェア型 WAF

・リバースプロキシとして動作するゲートウェイ型WAF
・Webサーバと独立した構成
・複数のWebサーバを集約
・保護対象毎に設定のカスタマイズが可能

SiteGuardシリーズの特徴

導入実績

国内WAF市場シェアNO.1 ※
導入サイト数150万サイト以上

※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

WAF市場初期より国産メーカーとして販売期間15年以上の実績と、導入サイト数150万サイト以上の導入実績があり、日本国内のWAF市場シェアNo.1です。

簡単導入・簡単運用

お客様環境に合わせたサービス・製品選択が可能

■クラウド型WAF
マネージドで運用負荷を軽減

■ソフトウェア型WAF
誤検知の際の除外ルールの設定例をサポートから案内可能

マネージドで提供しているクラウド型WAFはで運用負荷がかからないことはもちろんのこと、ソフトウェア型WAFではテクニカルサポートからチューニング内容の設定例を案内しており、運用が簡単です。またソフトウェア型WAFでは有償オプションで初期チューニングの提供も行っております。

低価格・高品質

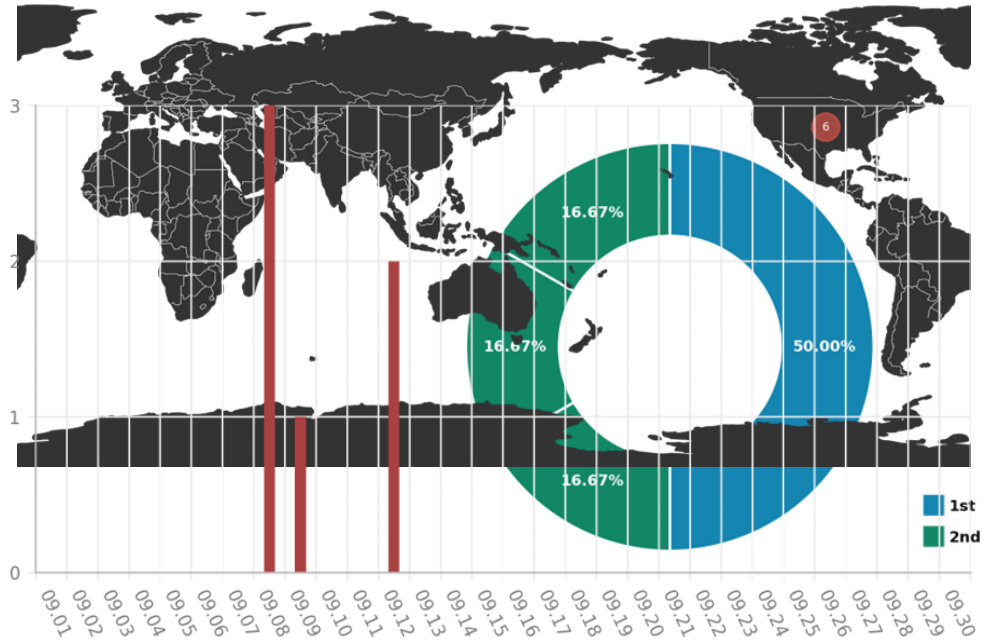
継続率99％以上、高い防御性能でコスト面も安心の価格設定

※2022年10月～2023年9月の間での当社調べ

デフォルト設定で高い防御性能があり、継続率は99%以上と
お客様から高い評価をいただいております。
価格はクラウド型月額2.5万円～、ソフトウェア型初年度25万2千円（月額換算2.1万円）～、次年度以降12万6千円～（月額換算1.05万円）～と安価にWAFの導入が可能です。

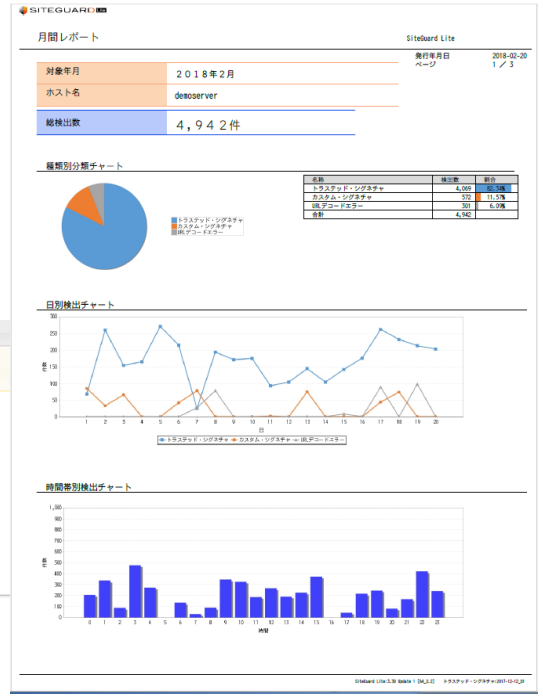
SiteGuard Cloud Edition

・DNSの切替で、ご利用環境（クラウド・オンプレ）を選ばずに導入可能
・WAFのチューニングもマネージドサービスで提供
・全プランに国別フィルタを標準搭載
（標準で、プランに応じて複数サイトが登録できるほか、レポートも利用可能）
・プランに応じた定額の通信量による課金（通信量超過の課金あり）



SiteGuard Server Edition/Proxy Edition

・デフォルト設定で、すぐに保護が可能
・シグネチャの個別のON/OFFのほか、カスタム・シグネチャで柔軟な設定が可能
・3大ウェブサーバーである「Apache」「Nginx」「IIS」に対応しているほか、
　プロキシとして動作するWAFを設置可能
・国産メーカーサポートならではの迅速、丁寧な回答でお客様をサポート



新しい脅威への対応スピード

SITEGUARD

主な注意喚起	概要	SiteGuardの対応日
2021年12月11日	Apache Log4jの任意のコード実行の脆弱性（CVE-2021-44228）	2021年12月10日
2021年10月6日	Apache HTTP Server の脆弱性（CVE-2021-41773, CVE-2021-42013）	2021年10月6日
2021年5月10日	EC-CUBEのXSSの脆弱性（CVE-2021-20717）	2021年5月10日
2020年8月14日	Apache Struts 2の脆弱性（S2-059）	2020年8月14日
2020年5月21日	Apache Tomcat の脆弱性 (CVE-2020-9484)	2020年5月21日
2019年6月20日	Oracle WebLogic Serverの脆弱性（CVE-2019-2729）	2019年6月20日
2018年8月23日	Apache Struts 2の脆弱性（S2-057）	2018年8月23日
2017年9月6日	Apache Struts 2の脆弱性（S2-052）	2017年9月6日
2017年7月10日	Apache Struts 2の脆弱性（S2-048）	2017年7月8日
2017年3月8日	Apache Struts 2の脆弱性（S2-045）	2017年3月7日
2017年2月6日	WordPressの脆弱性（REST API）	2017年2月6日

※主な注意喚起とは対象の脆弱性に関してJPCERT/CCや情報処理推進機構（IPA）等の外部機関が公表する注意喚起情報を指しています。

※SiteGuardシリーズの対応は、新規シグネチャのリリースまたは既存シグネチャでの対応に関する情報提供を含みます。

価格

ソフトウェア型 年間ライセンス

- 製品をインストールするOSの数でライセンスをカウント
- Proxy Edition 初年度1,780,000円、次年度更新534,000円
- Server Edition 初年度252,000円、次年度更新126,000円～（ボリュームディスカウントあり）
- アカデミック価格あり

クラウド型 月額サービス料金

- 毎月の通信量を基準に6プランを用意
- 各プラン毎に定額分の通信量を設定
- 400GBプラン 月額25,000円～
- 標準で複数サイトの登録に対応（400GBプランの場合、10FQDNまで）