EG Secure Solutions

信頼の純国産WAF

SITEGUARDシリーズ製品概要

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	69名（2025年9月末時点）
役員	代表取締役　齊藤 和男
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】

弊社サービスラインナップ

EG Secure Solutions

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

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。

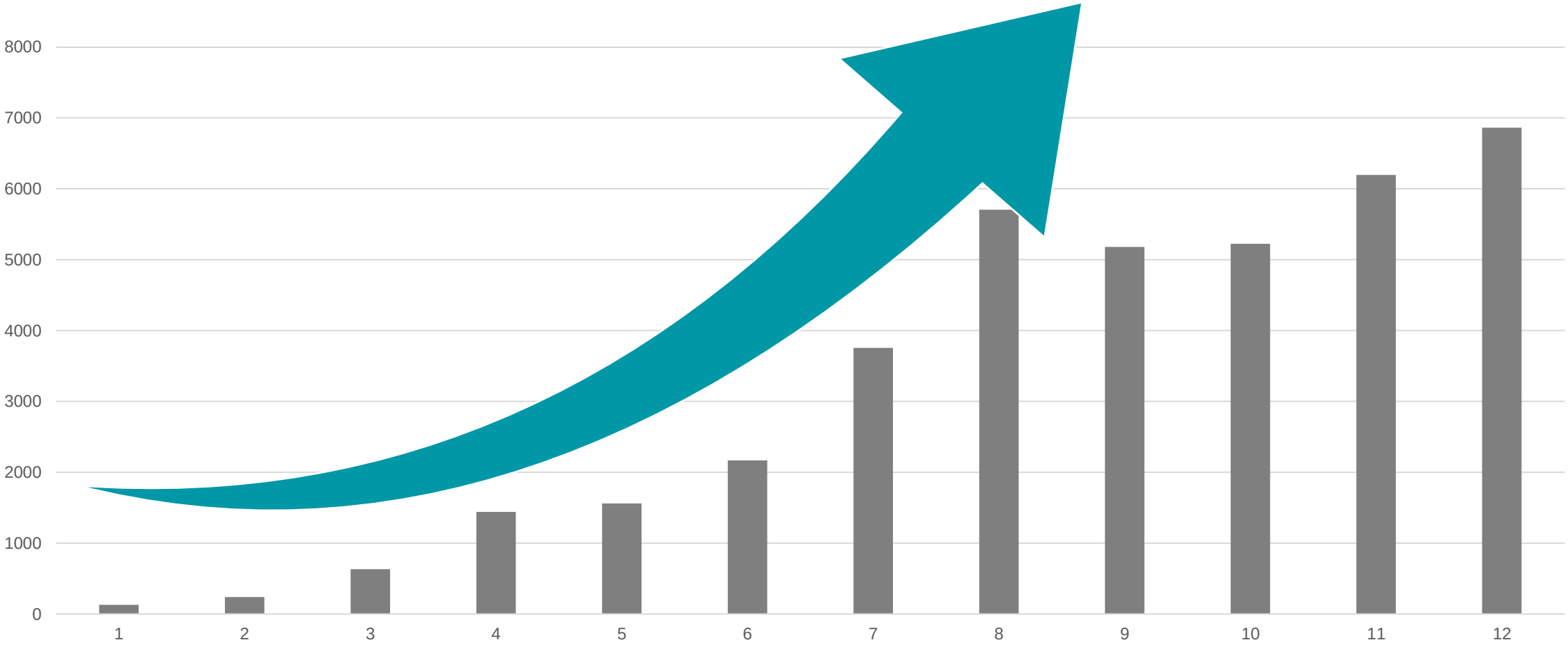
脆弱性診断やコンサルティング業務のかたわら、ブログや勉強会などを通じてセキュリティの啓蒙活動をおこなっている。

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。

サイバー攻撃の推移

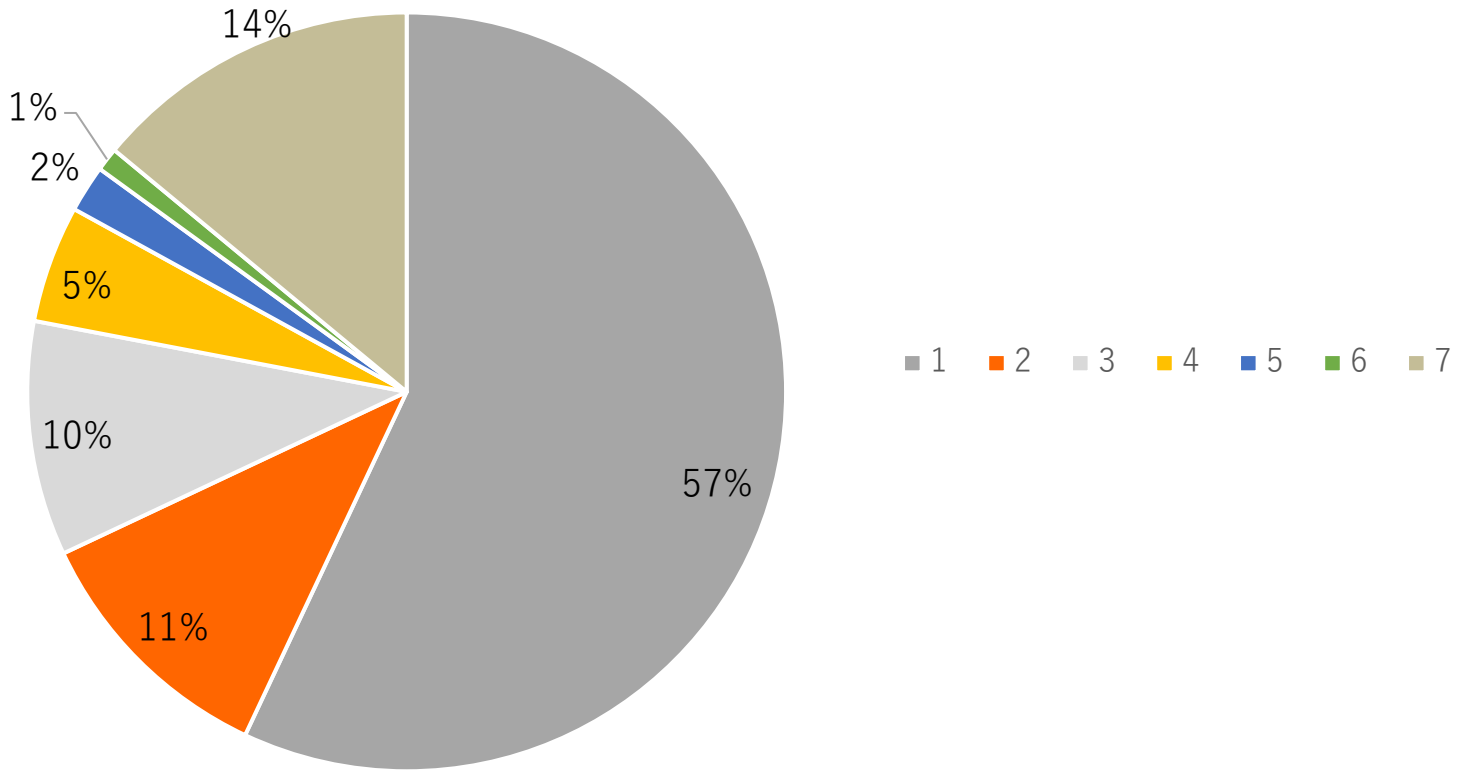
10年で50倍以上になっています

（パケット数　単位：億）



NICTERダークネット観測統計2025年より作成

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（2025年第4四半期）」

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

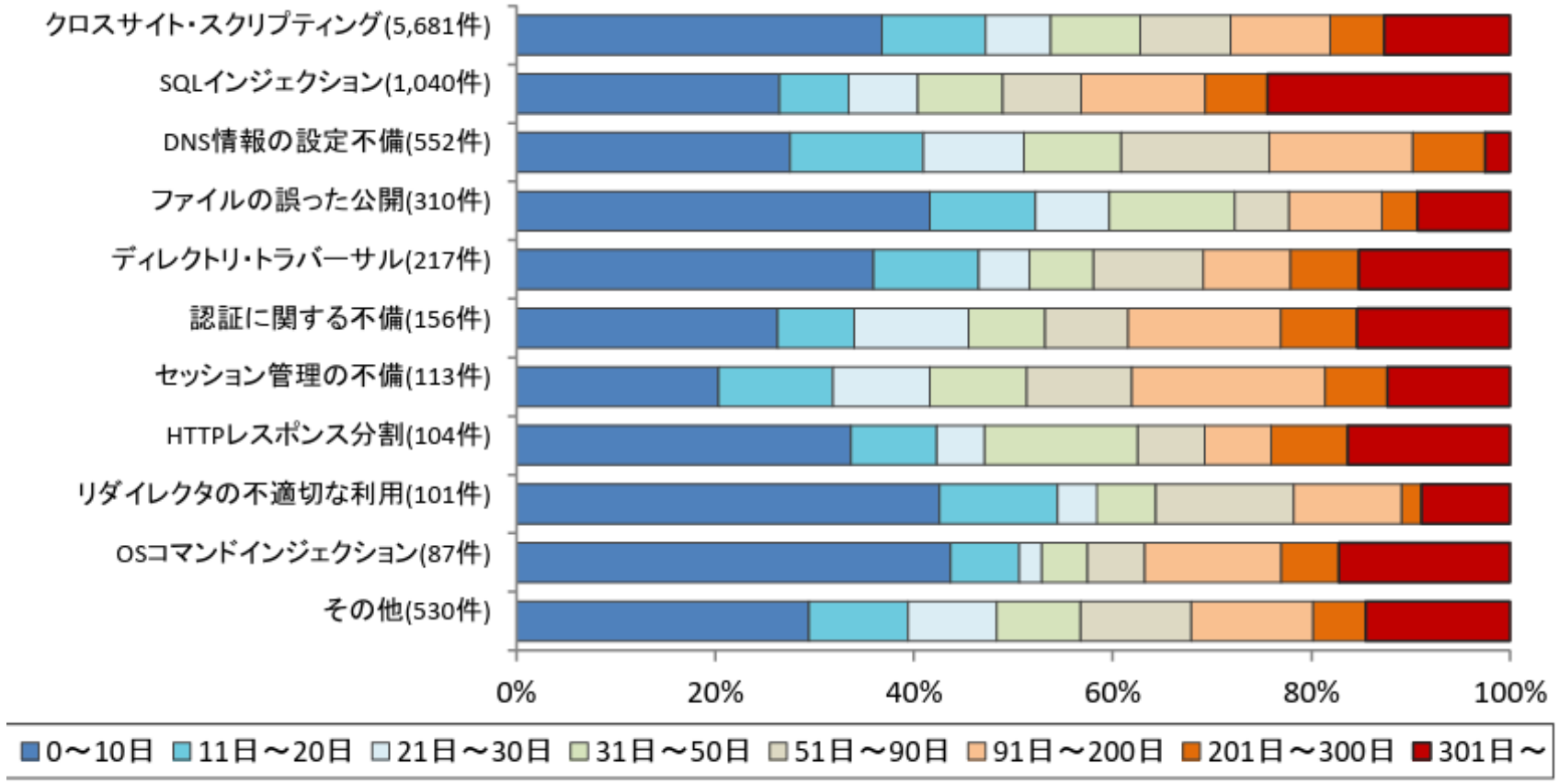
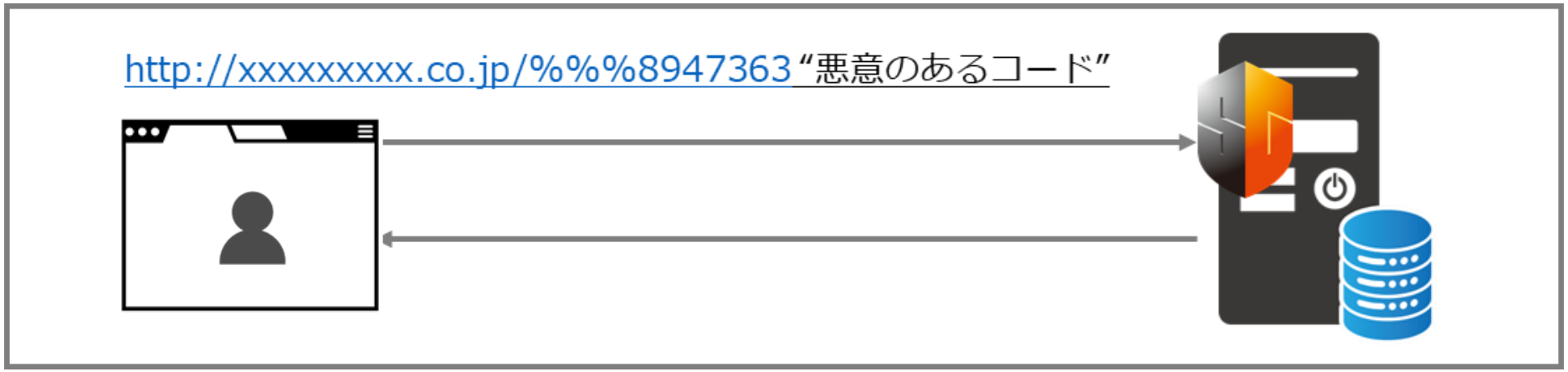


図2-21. ウェブサイトの修正に要した脆弱性種類別の日数の傾向

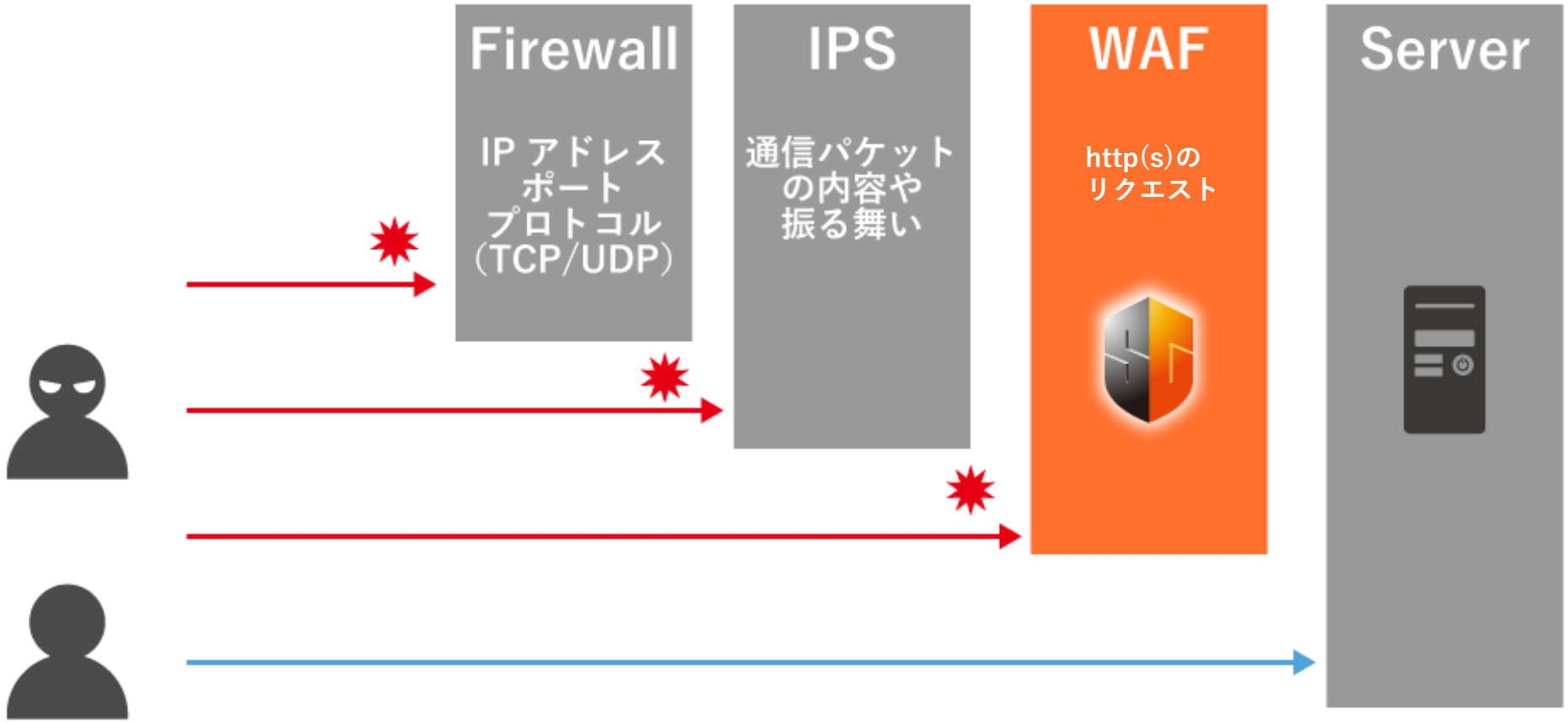
出典：情報処理推進機構（IPA）「ソフトウェア等の脆弱性関連情報に関する届出状況（2025年第4四半期）」

Web Application Firewall

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。



WAFはFirewallやIPS/IDSとは異なるレイヤーを防御します。



新しい脅威にすぐに対応できない

サイバー攻撃は常に新しい脅威にさらされています。WAFを導入することで、新しい脅威をWAF側で対応することが可能です。

脆弱性を修正できない

脆弱性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。

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。

いますぐ攻撃を防ぎたい

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助けとなります。

SiteGuardシリーズの特長

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

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

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

※2023年10月～2024年9月の間での当社調べ

SiteGuardシリーズ導入実績

- 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18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サーバー数百台や数万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

■サービスパートナー

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

SiteGuardシリーズラインナップ

クラウド型 WAF

SITEGUARD Cloud Edition

・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

ソフトウェア型 WAF

SITEGUARD Server Edition

・Webサーバー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
・管理するを増やさずに導入可能
・シンプルに導入が可能
・マネージドライセンスの提供も可能

ソフトウェア型 WAF

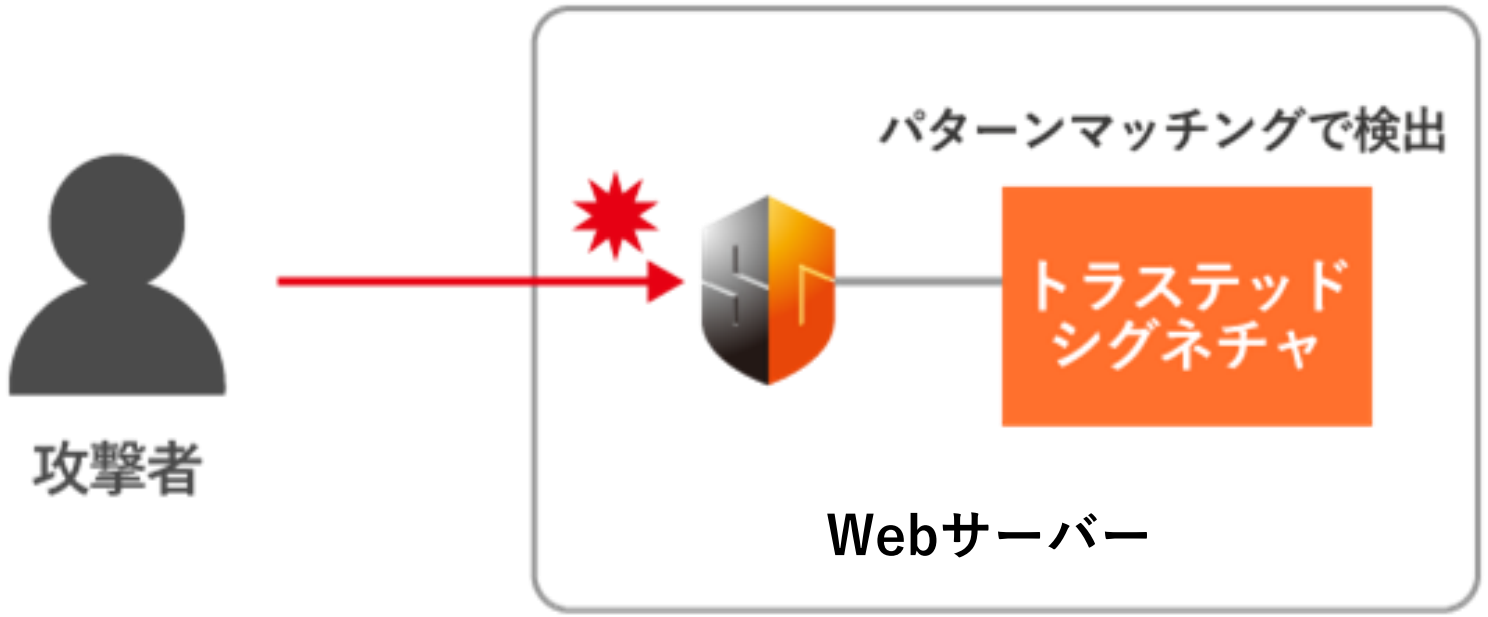
SITEGUARD Proxy Edition

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

SiteGuardシリーズの防御性能

- 攻撃パターンを定義したリスト（トラステッド・シグネチャ）を標準搭載
- SQLインジェクションやクロスサイトスクリプティングなど代表的な攻撃の多くに対応
- 独自の検査ロジックを組み合わせることで、高速且つ高い精度で攻撃を検出
- 検出時は設定（拒否、監視、フィルタ）に従い通信を処理
- トラステッド・シグネチャは定期的に更新しており、常に最新の脅威に対応

※ソフトウェア型は自動更新が可能（手動更新やオフライン更新も可能）



※Server Editionのイメージ（ウェブー上で保護）

SiteGuardシリーズ比較

項目	Cloud Edition	Server Edition		Proxy Edition
		マネージドライセンス	通常ライセンス/ プロキシライセンス	
■構成・運用・サポート				
導入構成	DNS切り替え	モジュール、Agent （プロキシも可）	モジュール （プロキシも可）	プロキシ
インストール	不要	必要	必要	必要
チューニング	AI自動チューニング マネージド（弊社）※1	マネージド（弊社）※1	必要	必要
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）
アップデート	不要	必要	必要	必要
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
24時間365日運用 ※2	あり	あり	非対応	非対応
■その他				
国単位でのアクセス制御	○	○	○	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
■CMS専用のトラステッド・シグネチャ搭載				
WordPress	○	別途有償	別途有償	ー
EC-CUBE		ー	ー	
Movable Type				

※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 クラウド上で提供しているマネージド環境について、障害対応および稼働監視を24時間365日運用で対応します。
（マネージドライセンスの場合は、マネージド環境の管理画面にアクセスができないなど、マネージド環境の障害対応になります。）

新しい脅威への対応スピード

主な注意喚起	概要	SiteGuardの対応日
2025年12月9日	React Server Componentsの脆弱性（CVE-2025-55182）	2025年12月10日
2024年7月5日	PHPの脆弱性（CVE-2024-4577）	2024年6月13日
2022年3月31日	JavaアプリケーションフレームワークSpringの脆弱性（CVE-2022-22963）	2022年3月31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。

防御可能な脅威と対応する機能

脅威	対応する機能	Cloud Edition	Server Edition	Proxy Edition
■ウェブアプリケーションの脆弱性を狙う攻撃				
SQLインジェクション	トラステッド・シグネチャ検査	○	○	○
クロスサイトスクリプティング				
OSコマンドインジェクション				
ディレクトリトラバーサル				
改行コードインジェクション（HTTPヘッダ、メールヘッダ）				
SSIインジェクション				
Xpathインジェクション				
LDAPインジェクション				
フォーマットストリング（書式文字列）				
PHPリモートファイルインクルード				
バッファオーバーフロー				
XXE（XML External Entity）				
不正なURLエンコード	URLデコードエラー検出	―	○	○
クロスサイトリクエストフォージェリ	セッション管理（CSRF防御）カスタム・シグネチャ検査	○※1	○※1	○
パラメータ改ざん	セッション管理（フォーム変数検査）カスタム・シグネチャ検査	○※2	○※2	○
クリックジャッキング	応答ヘッダフィールド追加	―	○	○
Cookie改ざん	Cookie保護（暗号化）	―	○	○
■DDoS/不正ログイン				
DDoS対策（L3/4/7）	DDoS対策機能	○	―	―
ブルートフォース（ログインアタック等）	カスタム・シグネチャ検査	○	○	○
■特定ミドルウェアやOS等の脆弱性　※3				
Apache Strutsの深刻な脆弱性	トラステッド・シグネチャ検査	○	○	○
Apache Killer				
ShellShock				
Slow HTTP DoS（Slowloris等）	タイムアウト機能	―	―	○
Hashdos	パラメータ数制限	―	○	○

※1 カスタム・シグネチャを使用したRefererヘッダ検査
※2 カスタム・シグネチャを使用したパラメータ検査
※3 特定ミドルウェアやOS等の脆弱性を悪用する、緊急度の高い攻撃にはトラステッド・シグネチャ検査で対応

クラウド型WAF

月額費用（SiteGuard Cloud Edition）

定額通信量	登録可能サイト数	平均帯域(参考値)	初期定価費用	月額定価費用
400GB	10FQDN	1.2Mbps	¥100,000	¥25,000
～1TB	10FQDN	3Mbps		¥50,000
～4TB	20FQDN	12Mbps		¥80,000
～10TB	50FQDN	30Mbps	¥200,000	¥170,000
～20TB	100FQDN	60Mbps		¥280,000
～40TB	200FQDN	120Mbps		¥520,000

・上記金額は全て税別です。
・本サービスは、”サービスを提供するインフラの運用管理”、”お客様からのご依頼によるチューニング作業” をマネージドサービスとして提供します。
・通信量を基準とした料金体系で、月額料金には1ヶ月分の定額通信量が含まれています。
・2か月連続で通信量を超過した場合、または、以下の割合を超えた場合は、通信量に応じた上位プランに移行していただきます。
【プラン変更対象となる通信量の割合】
400GB～10TBプラン：3割以上の超過、20TBプラン：2割以上の超過
なお、40TBプランは通信量の2割を超えた場合は、1GB単位で10円/GBにてご請求いたします。

例①）4TBプランで月間通信量が5.2TB以下だった場合は、4TBプランを維持。超過通信量の請求無し。
例②）10TBプランで月間通信量が13.1TBだった場合は、20TBプランへ移行。超過通信量の請求無し。
例③）40TBプランで月間通信量が48TB以下の場合は、超過料金の請求無し
例④）40TBプランで月間通信量が48.1TBだった場合は、超過通信量8.1TBを1GB単位で1GB/10円で請求、請求額8.1×10円=81,000円を月額料金と合わせて請求

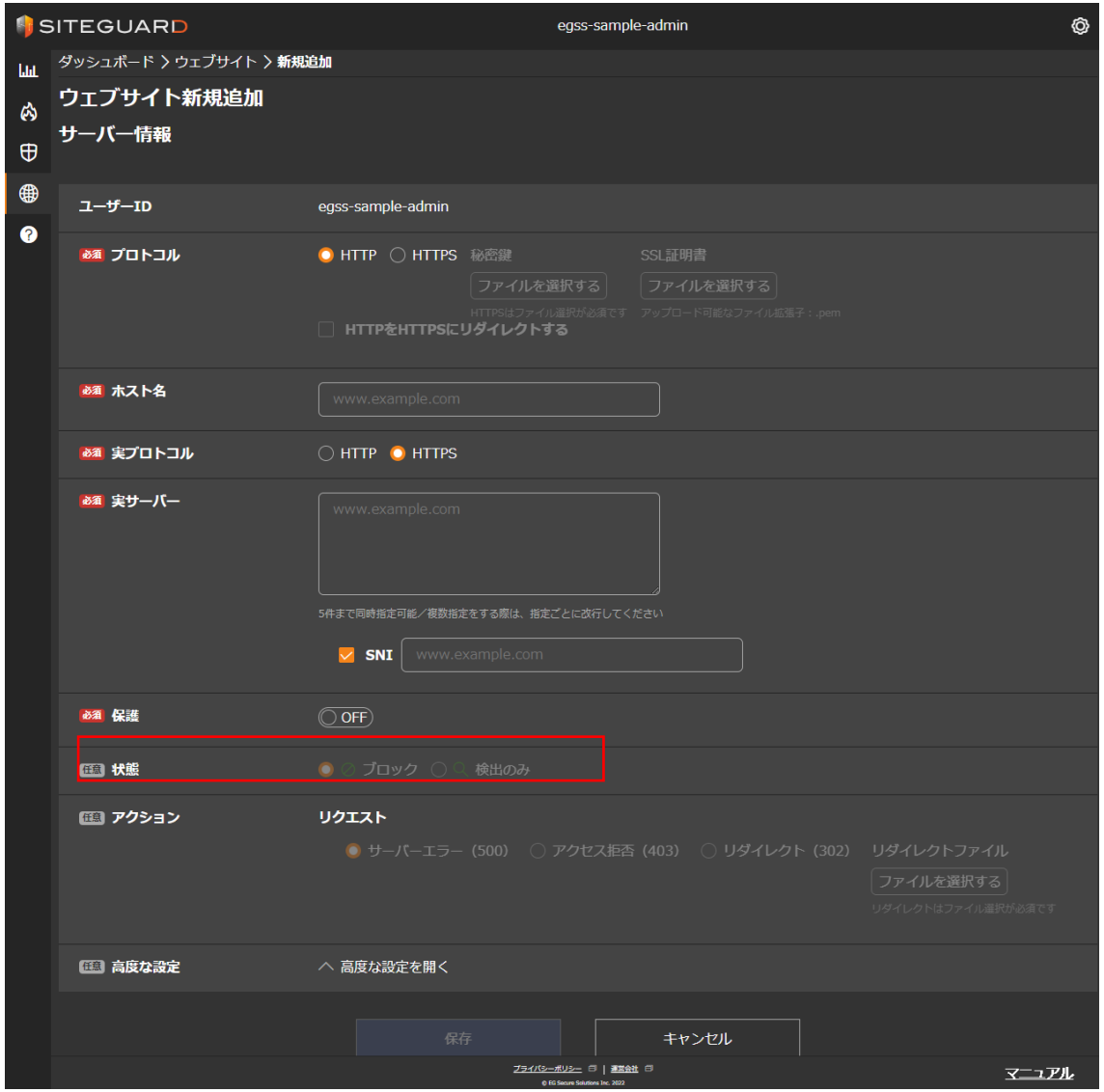
・上位プランへの変更は無償で承ります。下位プランへの変更は、変更先プランの初期費用が発生します。
・帯域の優先制御はなく、実際のスループットはベストエフォートになります。
・登録可能サイト数は10から最大200まで、プランによって異なります。
・プラン毎に性能（最大リクエスト処理数、CPU、メモリ）が異なります。多数のサイトを登録される場合には上位プランによるお申し込みを推奨します。
・本サービスのサポート内容は以下の通りです。
1）管理画面（サポートフォーム）によるテクニカルサポート（9:30-17:30/土日祝日・年末年始休暇は除く）
2）バージョンアップ、最新シグネチャデータの適用
3）緊急を要する障害復旧作業（24時間365日）

導入までの流れ

1. 利用申請書を入力して、SiteGuard営業窓口へお送り下さい。
1. ご記入頂いた内容をもとに、2営業日内に設定作業を行います。
1. 完了後、管理画面で使用するID/PASS、CNAMEなどをメールでご案内します。
1. 管理画面へログイン後、SSL証明書登録やWebサイト、実サーバー等の登録を行いDNSを切り替え次第、ご利用になれます。

監視設定　～テスト/本番運用の容易な切り替え

「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。



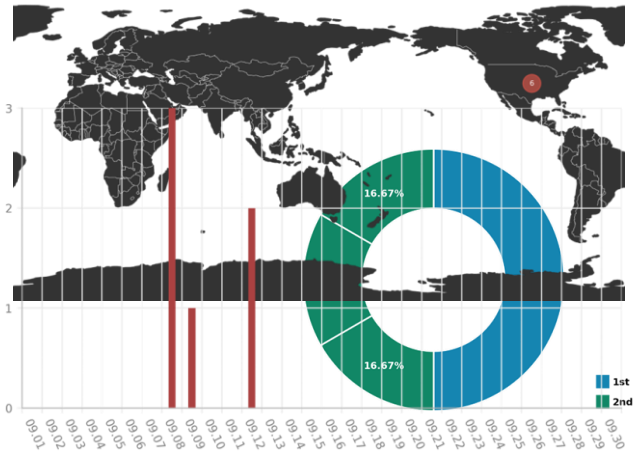
アクセス制御

・アクセス制御は、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・サイトごとに設定が可能となります。

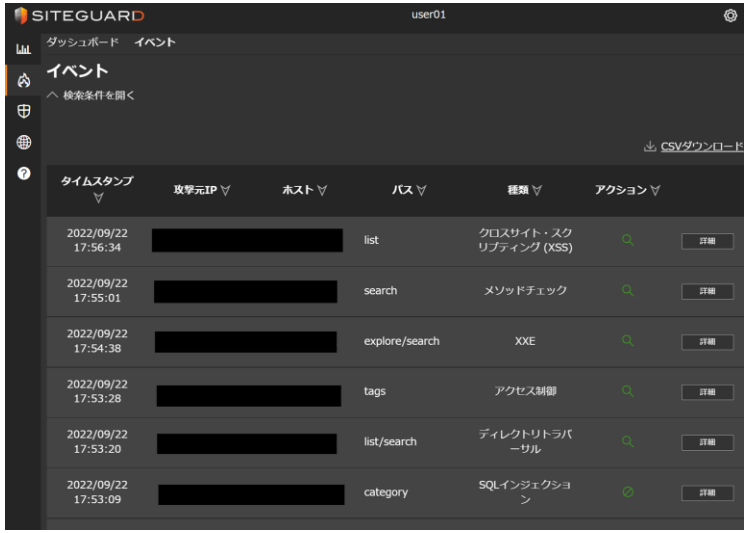
Web管理画面

【管理コンソールUI】

【レポート】



【検出ログ】



【国別フィルタ】

※画面は変更になる可能性があります。

NEW！

Cloud Edition 新機能

DDoS対策もAI自動チューニングも全プランに標準実装！
なのに、1サイトあたり2,500円～のクラウドWAFへ超進化

【防御力UP】

L7/4/3 DDoS対策を
「全プラン標準装備」

他社サービスでは高額な上位プランやオプション契約が必要になることが多い「L7 DDoS対策（HTTP Flood / Slow HTTP Attack等）」。Cloud Editionでは、これを全プランに追加費用なしで標準実装しました。OCI基盤のL3/L4対策に加え、WAF側でのL7対策が強化されています。

【運用力UP】

AI自動チューニングで誤検知対応の手間を大幅削減

WAF運用で最も手間のかかる「誤検知」の対応。新搭載の「AI自動チューニング機能」が、日々の検出ログから誤検知を自動で判定します。使えば使うほど通信傾向を学習し、シグネチャの検知精度が向上。専任のエンジニアがいなくても、手軽にセキュアな状態を維持できます。

※リリース初期は、AIが判定したチューニング結果を1日1回（平日）手動で適用いただく安心の運用サポート体制となります。今期中の完全自動化に向け順次アップデート予定です。

ソフトウェア型WAF

カスタム・シグネチャ

- お客様独自の検出ポリシーを細かな条件設定で柔軟に定義
- 特定のサイト・ページ・パラメータに対するシグネチャ検査の除外設定が可能
- 検出時の動作によりブラックリスト、ホワイトリストとして利用可能

活用例1	不正なホスト（Host:ヘッダ）宛のアクセスを禁止する
活用例2	不正なパラメータ値のアクセスを禁止する
活用例3	指定したページ宛の連続したアクセス（高頻度）を禁止する
活用例4	指定したパラメータについて、一部シグネチャの検出を除外する
活用例5	指定した接続元IPアドレスからのアクセスを安全とみなす

■検査可能な項目

URL、パス名、パラメータの名前、パラメータの値、接続元IPアドレス、接続先IPアドレス、応答メッセージ本文、要求メソッド、要求ヘッダ、応答コード、応答ヘッダ、送信ファイル名

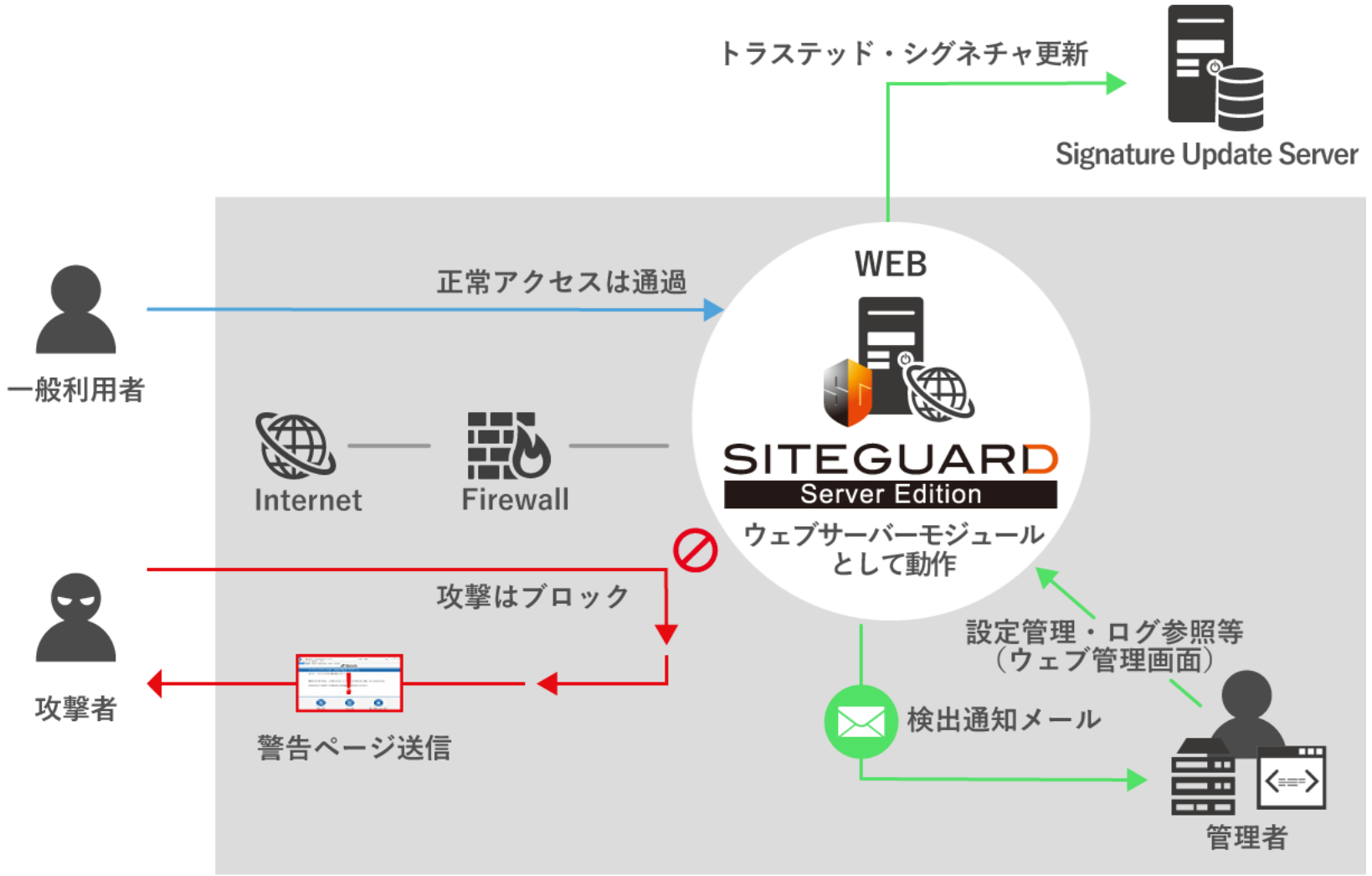
※応答メッセージ本文、応答コード、応答ヘッダはProxy Editionのみ可
※検査文字列は正規表現で柔軟に記述可

機能一覧

項目	Server Edition	Proxy Edition
■導入構成		
導入構成	モジュール・プロキシ	プロキシ
■防御機能		
トラステッド・シグネチャ検査（メーカー標準ブラックリスト）	○	○
カスタム・シグネチャ検査（ブラック・ホワイトリスト、頻度判定）	○	○
セッション管理（URL遷移検査、フォーム変数検査、CSRF防御）	ー	○
Cookie保護（シグネチャ検査、暗号化、secure属性設定）	○	○
応答ヘッダフィールド追加・削除	○	○
URLデコードエラー検出	○	○
パラメータ数制限	○	○
■管理機能		
攻撃検出時の動作設定（ブロック、モニタリング、フィルタ）	○	○
クライアントへ警告ページ送信（全文日本語編集可）	○	○
管理者へメール通知（全文日本語編集可）	○	○
ウェブ管理インタフェース（日本語、英語対応）	○	○
マルチインスタンス	ー	○
設定配信	○	ー
トラステッド・シグネチャ更新設定（自動、手動）	○	○
ロギング（syslog、ローカル）	○※1	○
レポート機能	○	○

※1：syslog対応はApache/Nginx版のみ実装。

運用負荷を抑えて攻撃をシャットアウト



※Server Editionの動作イメージ（Webサーバー上で保護）

推奨動作環境

	SiteGuard Server Edition	SiteGuard Proxy Edition
対応OS	● **Apache版** Red Hat Enterprise Linux 7※1/8/9/10 CentOS Stream 9/10 AlmaLinux 8/9/10 Oracle Linux 8/9/10 MIRACLE LINUX 8/9/10 Rocky Linux 8/9/10 Amazon Linux 2/Amazon Linux 2023 Ubuntu 22/24 FreeBSD 13/14 ・※1 Extended Life-cycle Support（ELS）に対応 ・x64に対応 ・Apache 2.2/2.4に対応 ・FreeBSD 13/14は、Apache 2.4のみ対応 ● **Nginx版** Red Hat Enterprise Linux 7※1/8/9/10 CentOS Stream 9/10 AlmaLinux 8/9/10 Oracle Linux 8/9/10 MIRACLE LINUX 8/9/10 Rocky Linux 8/9/10 Amazon Linux 2/Amazon Linux 2023 Ubuntu 22/24 FreeBSD 13/14 ・※1 Extended Life-cycle Support（ELS）に対応 ・x64（Nginx 1.20～1.29に）対応 ・Nginxをソースからコンパイル、インストールする必要があります。 ● **IIS版** Windows Server 2016/2019/2022/2025 ・各OS標準のIIS（10.0）に対応 ※マネージドライセンスは今後対応予定	Red Hat Enterprise Linux 7※1/8/9 CentOS Stream 9 AlmaLinux 8/9 Oracle Linux 8/9 MIRACLE LINUX 8/9 Rocky Linux 8/9 Amazon Linux 2 /Amazon Linux 2023 ・※1 Extended Life-cycle Support（ELS）に対応 ・x64に対応
CPU	Intel Pentium 互換CPU（2コア以上を推奨）	Intel Pentium互換CPU（4コア以上を推奨）
メモリ	2GB以上を推奨	4GB以上を推奨
HDD	空きが5GB以上（ログの保存期間等による）	空きが20GB以上（ログの保存期間等による）

※対応OSであれば仮想OSやクラウド上でもご利用いただくことができます。
※ウェブ管理画面の動作環境として、JDK/JRE 11以降が必要となります。
※IIS版をARR（Application Request Routing）環境でご利用いただく場合は、導入前の動作検証を推奨しています。

価格（ソフトウェアライセンス）①

■SiteGuard Server Edition 通常ライセンス

ライセンス数	新規標準単価	更新標準単価	新規月額換算	更新月額換算
1	¥252,000	¥252,000	¥21,000	¥21,000
2～5	¥216,000	¥216,000	¥18,000	¥18,000
6～10	¥192,000	¥192,000	¥16,000	¥16,000
11～25	¥186,000	¥186,000	¥15,500	¥15,500
26～50	¥180,000	¥180,000	¥15,000	¥15,000
51～100	¥168,000	¥168,000	¥14,000	¥14,000

■SiteGuard Server Edition マネージドライセンス

ライセンス数	標準単価	初期費用	月額換算
1	¥504,000	¥200,000	¥42,000
2～5	¥480,000		¥40,000
6～10	¥456,000		¥38,000
11～25	¥432,000		¥36,000

■SiteGuard Server Edition プロキシライセンス

ライセンス名	新規標準単価	更新標準単価	新規月額換算	更新月額換算
プロキシライセンス	OPEN	OPEN	OPEN	OPEN
プロキシライセンス（マネージド）	OPEN		OPEN	
初期費用（マネージド）	OPEN		―	

価格（ソフトウェアライセンス）②

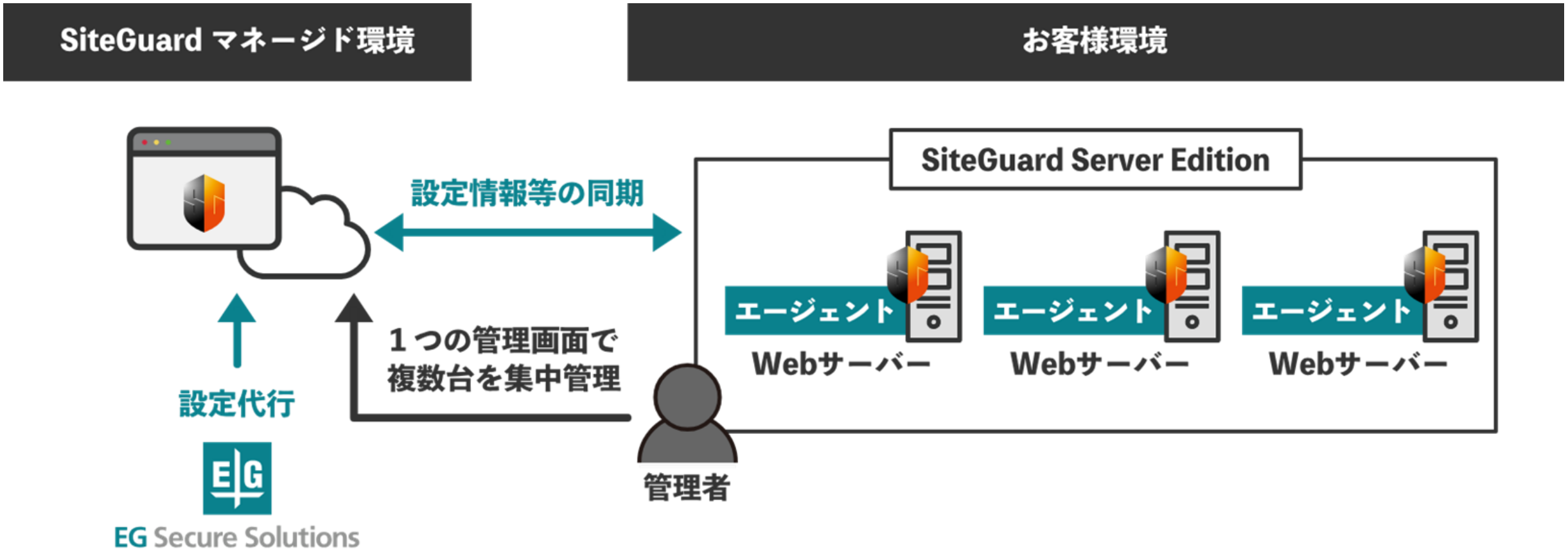
■SiteGuard Proxy Edition

ライセンス数	新規標準単価	更新標準単価	新規月額換算単価	更新月額換算単価
1	¥1,780,000	¥1,068,000	¥148,333	¥89,000

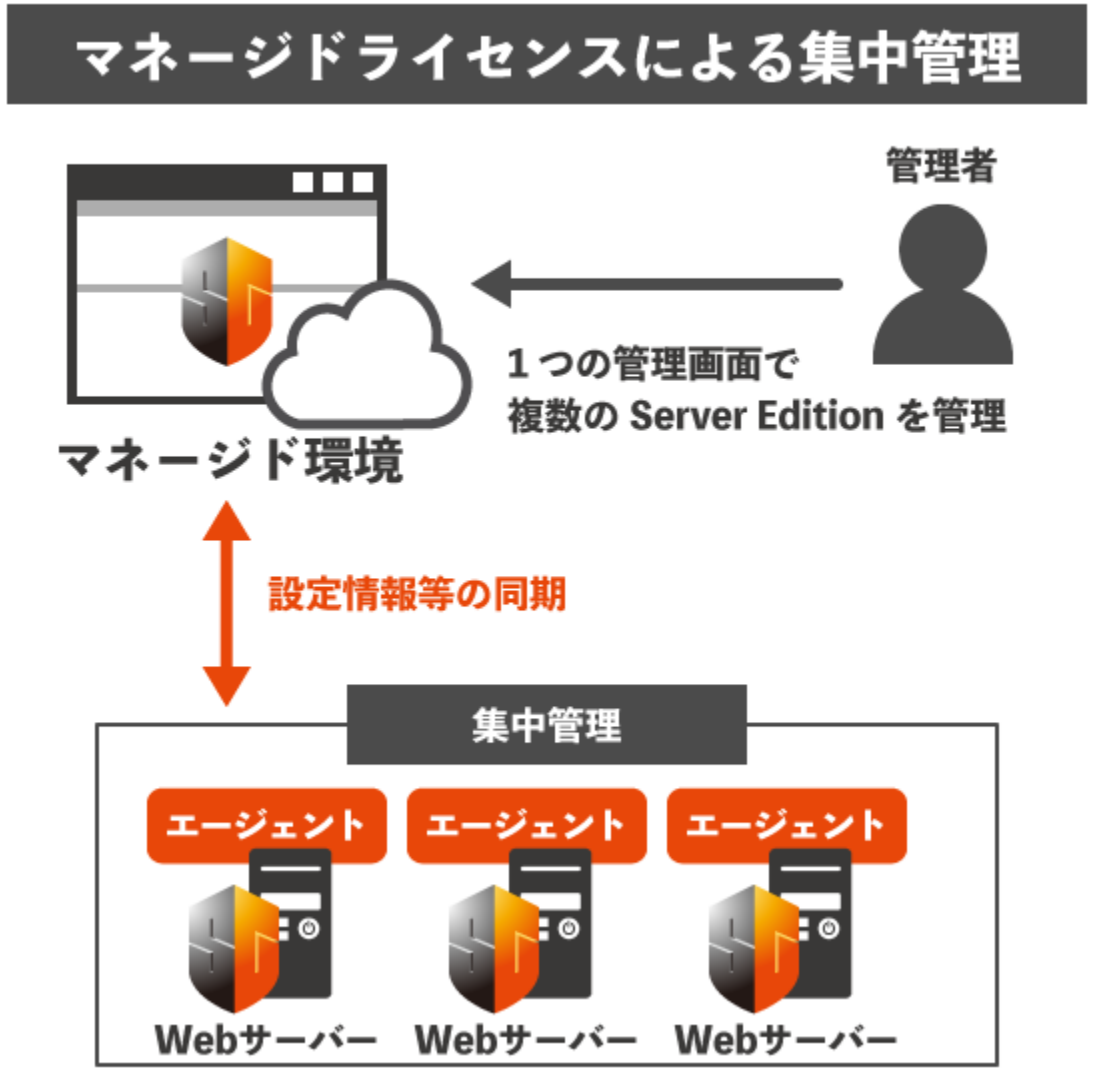
■備考

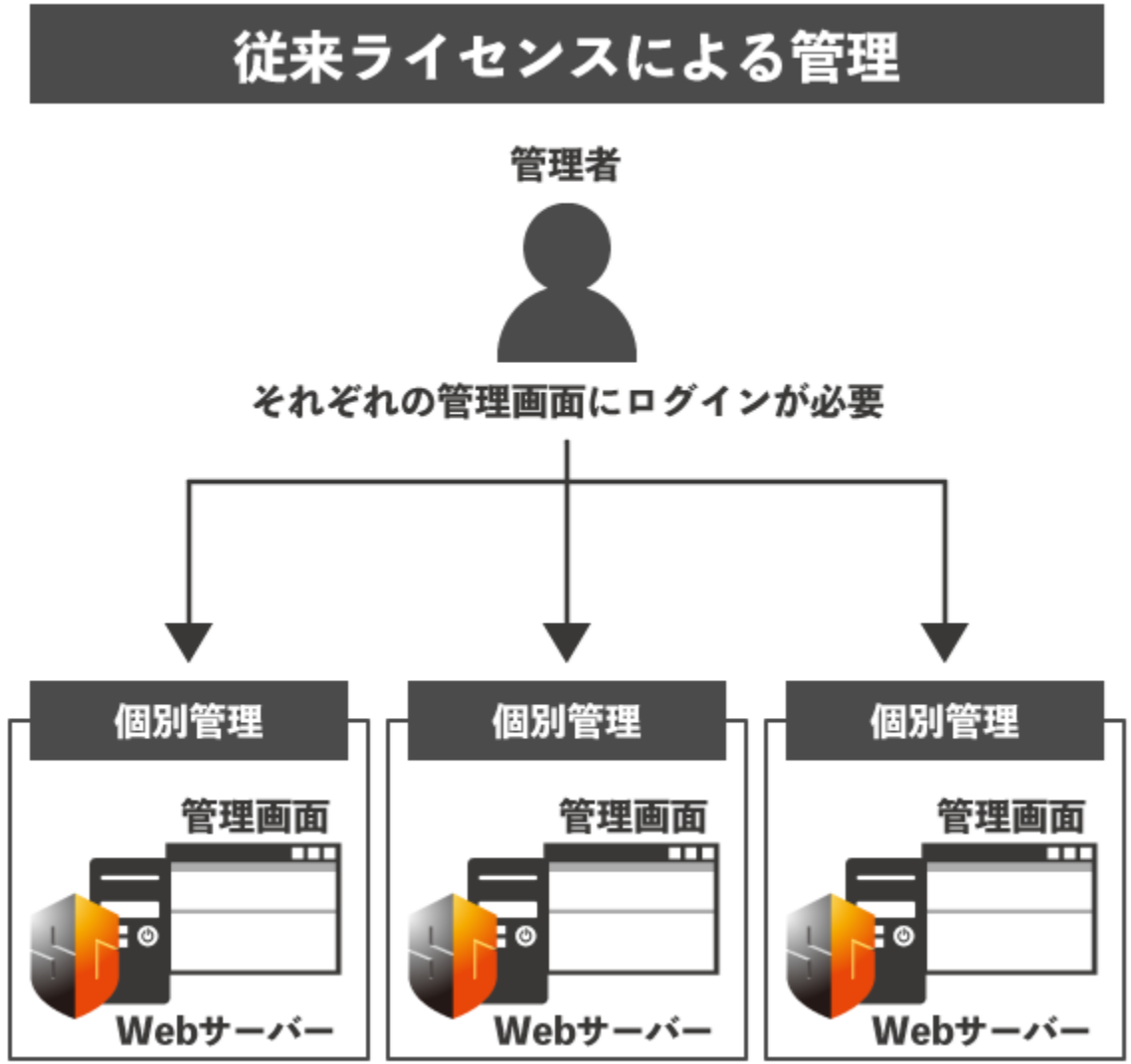
- 金額は1ライセンスあたりの単価（税別）です。
- 新規（更新）価格には、初年度（次年度以降）1年間の製品使用権とサポートサービスが含まれます。
- ライセンス数はインストールするOS（仮想OS含む）単位でカウントします。
- SiteGuard Server Editionをプロキシ構成（※）で利用する場合、「Server Edition プロキシライセンス」が必要です。お問い合わせ下さい。
  ※ホスト構成ではなく、前段のプロキシサーバー（Nginx/Apache等）へインストールして利用する構成
- Server Edition（プロキシライセンス除く）のボリュームディスカウントは、同一契約の合計ライセンス数に適用されます。
- マネージドライセンス、プロキシライセンス（マネージド）の初期費用は同一契約内であれば数量1となります。
  ライセンスを追加する場合には初期費用は不要となります。
- アカデミック価格適用対象の場合（「Server Edition プロキシライセンス」「Server Editionマネージドライセンス除く）は、価格が50%OFFとなります。
  [適用対象] 高等教育機関、各種大学校、初等中等教育機関、教育委員会、教育関連施設（教育センター/教育研究所/美術館/博物館/公民館/図書館等）
  公共職業能力開発施設および職業訓練法人、大学共同利用機関
- サポートサービスの内容は以下の通りです。
  1）テクニカルサポート（電話、E-Mail）
  2）最新のトラステッド・シグネチャデータのご提供
  3）最新のソフトウェアパッケージのご提供
- クラウド、ホスティング事業者様でサービス提供をご検討の際はお問い合わせ下さい。
- マネージドライセンスのWindows/IIS版は2025年中の提供予定となります。

マネージドライセンス構成イメージ

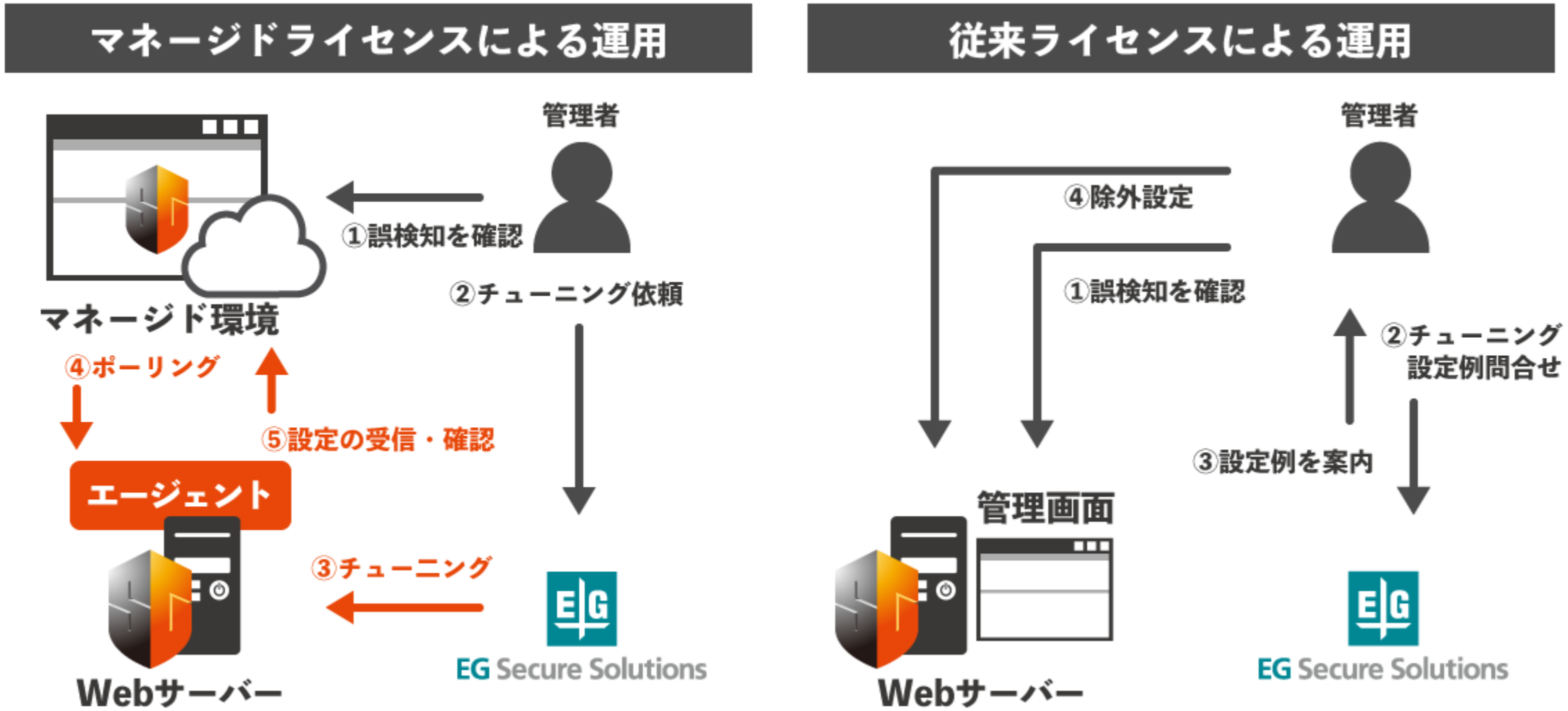


マネージドライセンス　統合管理





マネージドライセンス　設定代行



SiteGuard Server Editionプロキシライセンス

ApacheやNginxで構成したリバースプロキシがすでに存在している場合等、
リバースプロキシ上にホスト型WAF「Server Edition」を導入する場合のライセンスとなります。
※製品自体はServer Editionと同じとなります。

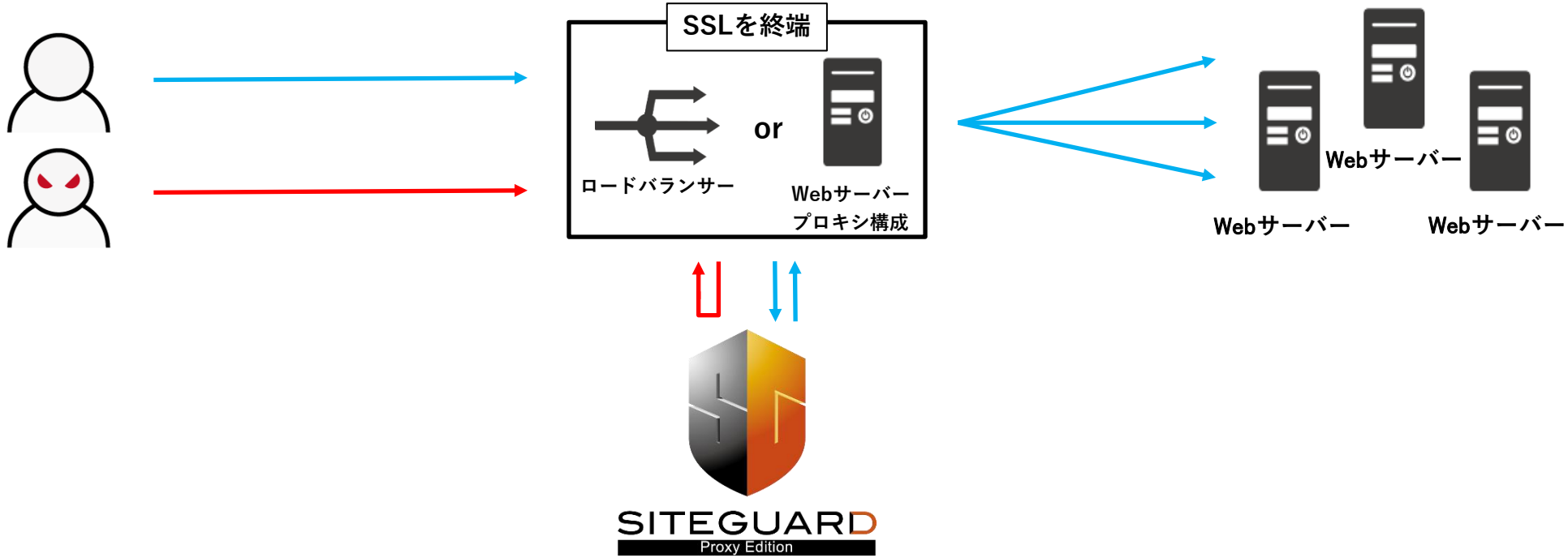
■構成イメージ

※Server EditionはWebサーバーのモジュールとして通信の検査・防御のみ行います。
※前段のプロキシ構成のWebサーバーはユーザー様側でご用意いただく形となります。

SiteGuard Proxy Edition

SiteGuard Proxy EditionはHTT。Pのプロキシサービスとして動作するためSSL処理は前段のロードバランサー等で終端いただく必要がございます

■Proxy Editionの多い構成



※Proxy EditionはSiteGuard Proxyとして通信の検査・防御のみ行います。
※プロキシサーバーはユーザー様側でご用意いただく形となります。

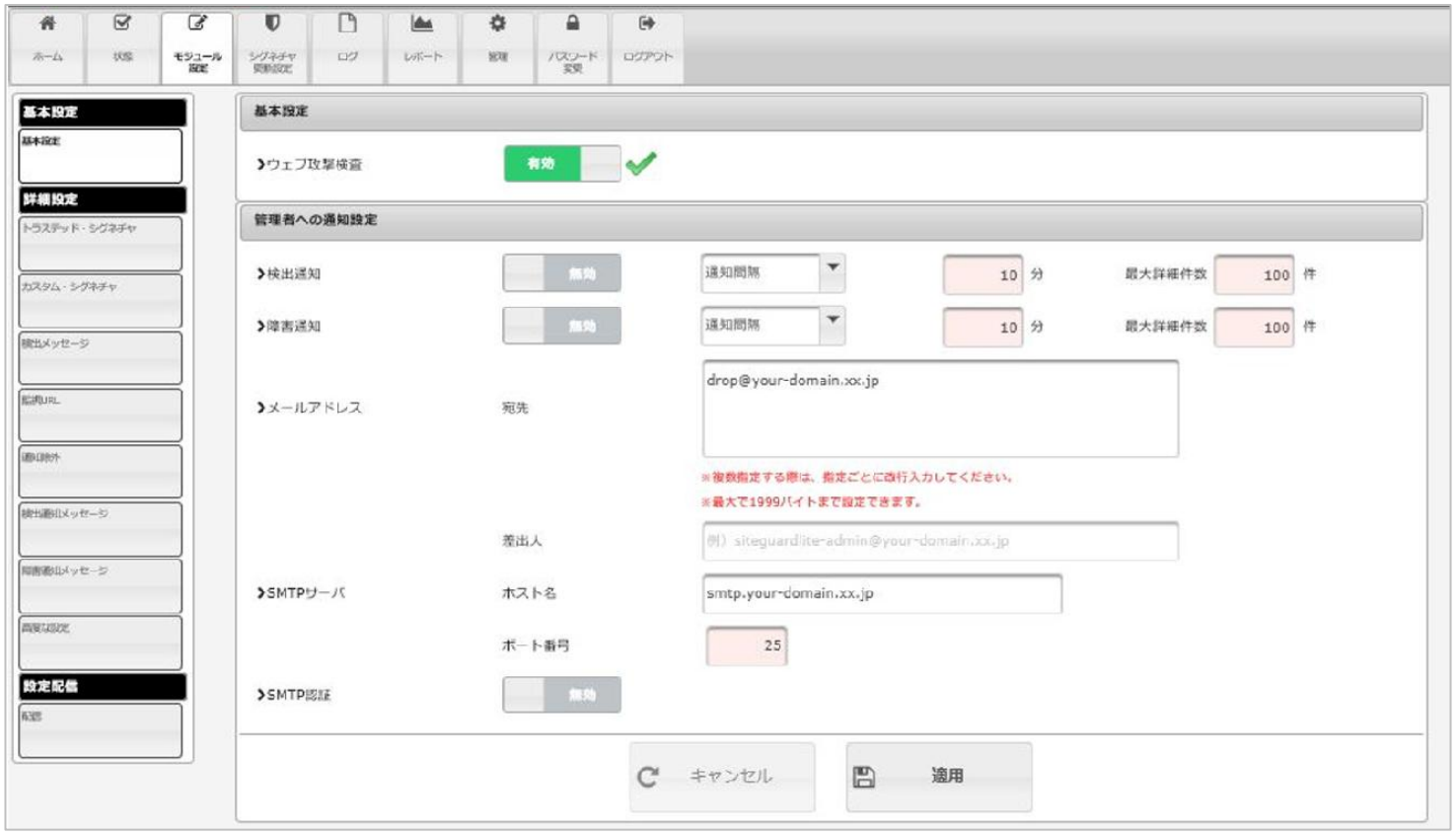
導入サービス

「SiteGuardシリーズ」は、簡単インストール・クイックスタート
セキュリティに詳しくない方でも導入・運用が可能！
そうはいっても専任の管理者が不在だし、導入・運用ともに心配・・・
そのようなお悩みを導入サービスが解決します。

導入サービス	SiteGuard Server Edition	SiteGuard Server Edition プロキシライセンス	SiteGuard Proxy Edition
導入サービス（標準）	¥600,000 (¥300,000)	-	OPEN（※ご相談下さい）
導入サービス（Lite）	¥400,000 (¥200,000)	OPEN（※ご相談下さい）	
構築支援サービス	-		¥2,000,000～ （※ご相談下さい）
WP Protect Service	¥200,000		-
製品アップグレードサービス	¥200,000		
製品トレーニングサービス	¥200,000		

- 金額は1台あたりの単価、（）内は2 台目以降の単価（いずれも税別）です。
- 導入サービス価格には、ソフトウェアライセンスは含まれておりません。
- 導入サービス（標準）とPE構築支援サービス、製品トレーニングサービスは別途訪問費用が必要です。
- 製品トレーニングサービスは、ご希望があればオンラインでも実施できます。
- 導入サービスおよびご提供条件の詳細につきましては、別途お問い合わせ下さい。

- ソフトウェアパッケージ、およびスクリプト実行による簡単インストール
- 設定管理はウェブ管理インタフェースベース
- ライセンス登録後、検査機能の有効のみで防御開始も可能



※画面はServer Editionのもの

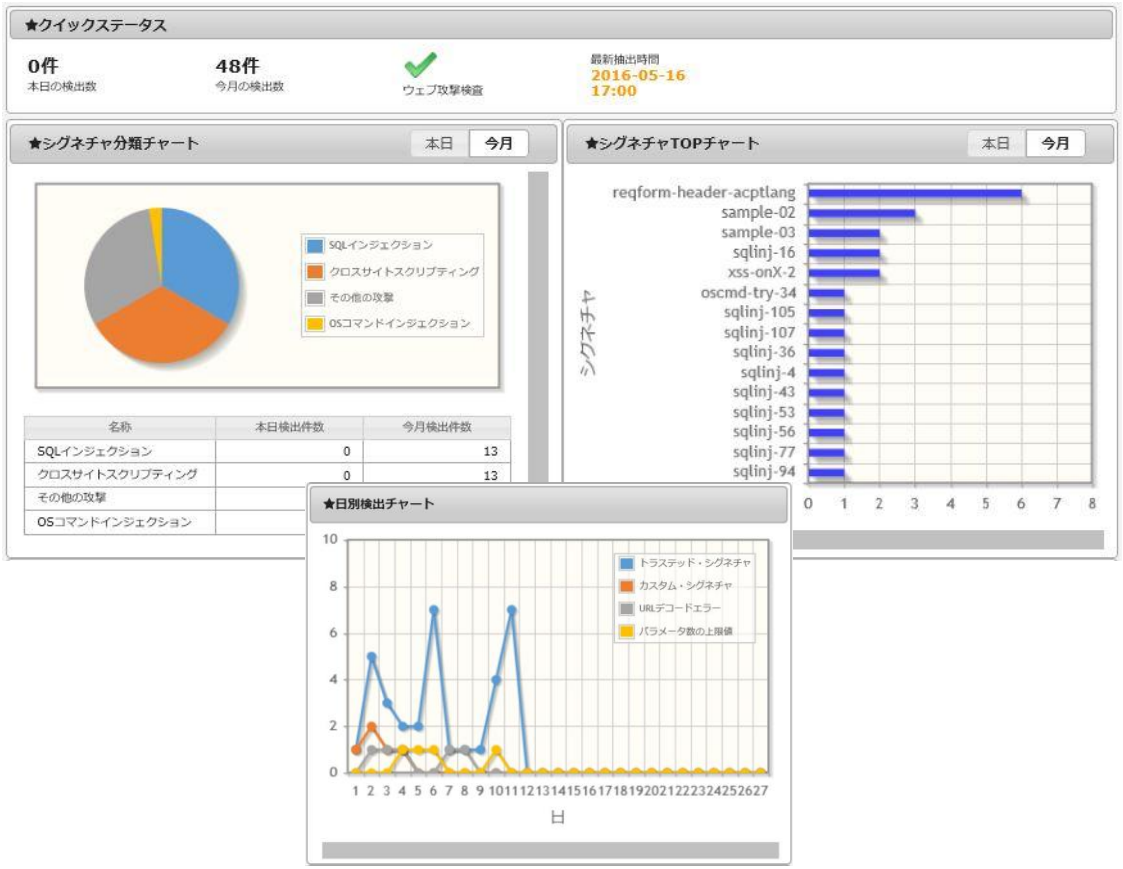
監視設定

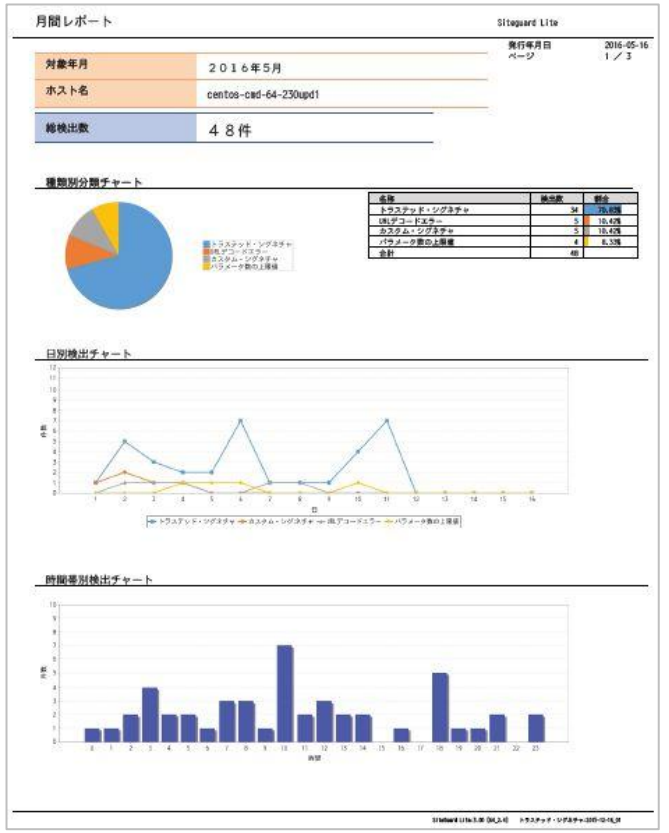
- 監視対象（攻撃を検出しても遮断せず、ログのみを取得）にするURLを登録
- 対象は正規表現で柔軟に記述可能
- 個別のシグネチャ設定を変更することなく、監視/拒否の切り替えを効率的に実施
- 複数サイトでの段階導入など、リスクを抑えた本番運用への移行を実現
- Server Editionでは、監視対象にする接続元IPアドレスを登録することも可能

※画面はServer Editionのもの

レポート

- 検出情報を集計して、内容をグラフィカルに表示
- 管理画面上でダッシュボードとして表示できるほか、PDF形式で外部出力可能
- Server Editionを複数台に導入している場合、親サーバー（設定配信機能の配信元）でレポートデータを収集し、統合レポートを作成することも可能





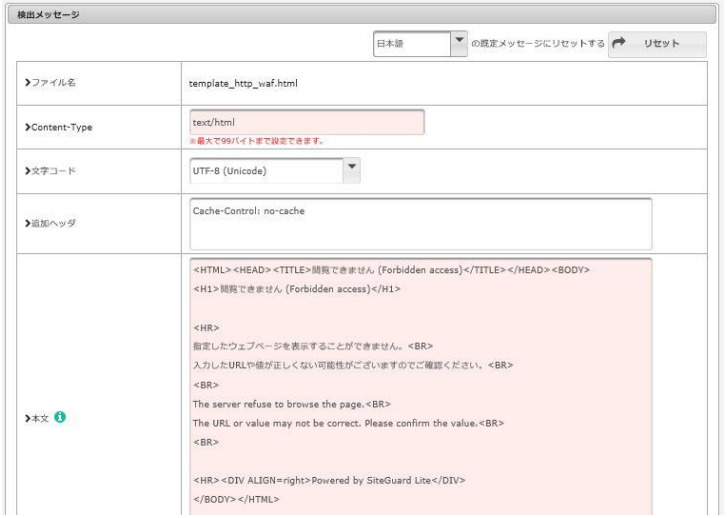
※画面はServer Edition

設定配信

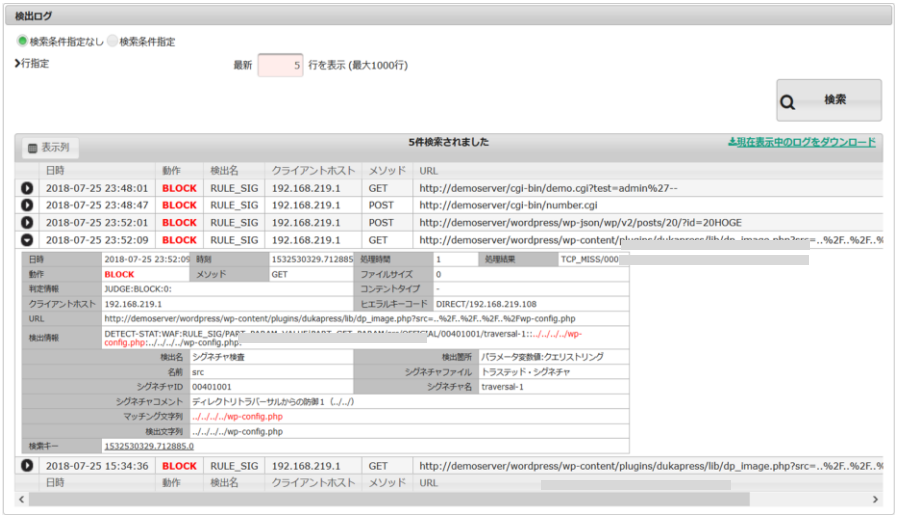
Server Editionを複数台に導入している場合、配信元の親サーバーを設定する事で複数の子サーバーへ設定の一括配信が可能

Web管理画面

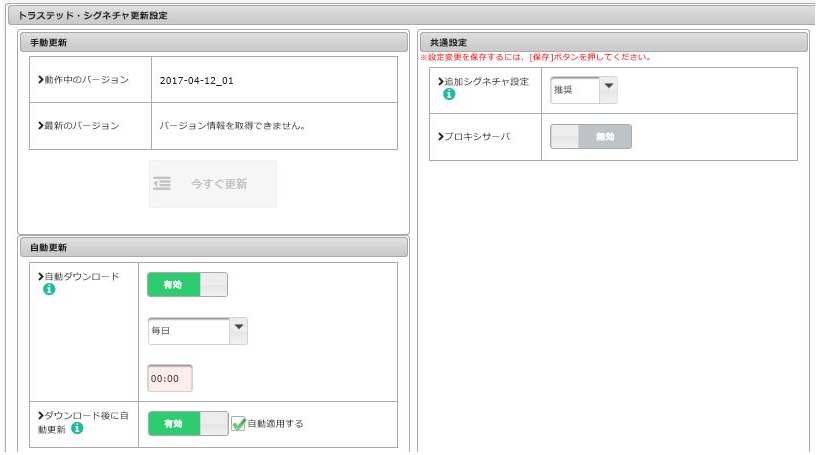
【検出メッセージの編集】



【ログ参照】



【シグネチャ更新設定】



【バックアップ・リストア、診断情報】

Web管理画面

【ホーム画面】

【トラステッド・シグネチャの設定】

【ログ参照】

【レポート出力・ダウンロード】