攻撃遮断くん
導入事例集

※掲載許可をいただいた企業様のみ掲載しております。

清水建設株式会社

清水建設株式会社は、1804年創業の日本を代表する大手総合建設会社です。建設事業、開発事業を主な事業とし、さらに各事業に付帯関連する建設資機材の販売及びリース、金融等の事業活動を展開しています。建設プロジェクトの全段階でお客様にとっての最善を提案し、実現しています。

写真：
情報システム部 システム運営グループ
グループ長 市橋 章宏（左）
井上 悠　（右）

導入前の課題	■ 清水建設が運用するWebサイトのセキュリティレベル統一 ■ 開発を外部委託しているシステムの安全性確保 ■ セキュリティ診断では対策として不十分な脆弱性への迅速な対応
導入後の効果	■ DNSの切り替えやサーバへのアクセス制御によるWebサイトのセキュリティレベル統一 ■ WAFを導入したサーバのセキュリティ評価が向上 ■ 契約帯域内での可用性の高さによる、予算管理工数の削減

清水建設株式会社（以下、清水建設）は日本を代表する建設会社です。高層ビル、商業施設、交通インフラやダムなど、あらゆるものの建設に携わり、国内だけでなく海外へと活躍のフィールドを広げています。2018年からは「深海未来都市構想（OCEAN SPIRAL）」や「環境アイランド(GREEN FLOAT)」といった近未来的な事業「シミズドリーム」が動き始めます。
海外でも活躍する清水建設では、Webサイトなど約60サイトへクラウド型WAF「攻撃遮断くん」を導入しています。

今回「攻撃遮断くん」の導入にあたり、丸紅情報システムズ株式会社（以下、丸紅情報システムズ）、JIG-SAW株式会社（以下、JIG-SAW、株式会社サイバーセキュリティクラウド（以下、サイバーセキュリティクラウド）が清水建設の「攻撃遮断くん」導入をサポートしました。
清水建設がクラウド型WAF「攻撃遮断くん」の導入に至った経緯、そして製品選定のポイントやWebセキュリティに対する考え方について伺いました。

全社のセキュリティレベル統一に向けた新しい施策

Q：WAF導入の経緯についてお聞かせいただけますでしょうか。

市橋：当社の情報システム部は社内向けのシステムや、外部に公開しているWebサイトなど清水建設の全システムを管理しています。例えば、分譲マンションをお客様に販売するWebサイトなどは、情報システム部以外の所管部署が直接発注し管理していたものもあります。自社開発から制作会社が開発しているシステムまで大小数十種類のサーバ全ての安全を確保する必要がありました。

一から情報システム部で設計・構築したサーバは、一般公開前にセキュリティ診断やネットワーク診断を実施し、安全を確保しておりますが、それ以外のサーバでは、セキュリティ診断が実施されていないものもあります。当社管理の全てのサーバに対するセキュリティ対策が不可欠なため、2年前から全システムに対して毎年セキュリティ診断を実施する規定を定めました。そして、セキュリティ強化の次なる一手として検討したのがWAFです。

毎年実施するセキュリティ診断への対策だけでは、次々に発生する脆弱性に対応しきれないと考えていました。そのため、恒常的にサーバを防御できるWAF導入を検討することしました。全社共通のWAFを導入することで、セキュリティレベルを統一することが目的です。

清水建設株式会社

重要なのは運用管理を専門家に任せられること

Q：どのような種類のWAFを検討していましたか？

市橋：クラウド型であることが第一条件でした。
当社にはクラウドありきの方針というわけではなく、当社で「実施したいこと」「目指したいこと」をもとに要件定義し、実現する手段としてクラウドやオンプレなどを対策案を検討してきました。
サイバー攻撃に対しては、アプライアンス型WAFで全ての攻撃に対応するのは難しいと考えています。攻撃検知があった際に「この検知は対処すべきか、もしくは誤検知か」「この後どのようなアクションをとれば良いか」といった対応が必要となりますが、次々に攻撃が来る状況下では、全ての攻撃に対応しきれません。巧妙化しているサイバー攻撃に対して、我々も成長しなくてはいけませんが、一朝一夕にはできません。クラウド型WAFのように専門家へ運用管理を任せられることは、ユーザー企業にとっては大きなメリットになります。

井上：WAFの運用管理をセキュリティの専門家に任せ、その上で、自社で対応しなければならない範囲を対応する。アプライアンス型のように全て自社で対応するよりも、クラウド型のほうが効率的なセキュリティ対策の実施が可能だと考えています。

市橋：今回は「スモールスタート」「ファーストスタート」ができることが重要でしたので、DNSを切り替えるだけで導入できるクラウド型WAFに最初から絞っていました。

井上：WAFの導入を検討した対象は、約100サイト弱です。WAFを導入するまでに時間がかかると、その間も攻撃受ける可能性があるため、導入できるものから少しでも早くWAFを導入しセキュリティ強度を高める必要がありました。

その他にも選んだポイントとして、導入のしやすさがあります。当社の課題として、導入するサイトの中には情報システム部以外の部署が管理しているサーバもあり、専用機器の設置やエージェントをインストールするとなると、敷居が高く導入が困難だったと思います。「攻撃遮断くん」は、DNSの切り替えやサーバへのアクセス制御だけで導入できたため、アプライアンス型などに比べると所管部署との調整も比較的簡単でした。

「攻撃遮断くん」の選定理由は手間なく運用管理できること

Q：WAFを比較する際、どのような点を重視していましたか？

井上：我々の仕事は、システムを運用・運営していくことです。WAFは導入して完了ではなく運用開始後の方が重要なため、システム運用面を一番重視していました。具体的には、「攻撃を受けた際に、どのように対応してもらえるのか」という点を、各社詳細に聞かせていただきました。24時間365日対応はもちろん、当社から何かあった際に問い合わせることができる、問い合わせた内容に柔軟に対応してもらえるといったサポート面を重要視してきました。

市橋：国産WAFというのもポイントです。世界中から攻撃が来ますが、日本は日本独特の攻撃があると考えています。また、何か問題あった際の対応は、国産のほうが早いと思っています。セキュリティ製品は、何かあった際の対応が早くないと一番困ります。また、我々ユーザー企業からすると、国産WAFは技術者が見えるため安心できます。

Q：「攻撃遮断くん」はどのように評価いただけましたか？

井上：「Webサイト入れ放題プラン」というサービスプランは、評価できたポイントです。導入対象が約100サイト弱ありましたので、１サーバ・１FQDNごとに課金されるコスト体系より、100Mbpsや200Mbpsといった帯域で運用できる方が分かりやすく、結果的に費用が抑えられていると感じています。

市橋：人気があるマンションの販売サイトは、販売開始時からすぐに完売となるとWebサーバも役割を終えてしまいます。当社のWebサイトは特別トラフィックが多いわけではありませんが、対象サーバの増減によりトラフィックに変動が出てきます。トラフィックが増えるたびに追加で帯域を申込むより、契約している一定の帯域内で自由に運用できるほうが予算管理しやすく、Webサイトの追加・削除も手続き不要で自由に設定できるというのも便利です。このような手続きも運用業務内のため、手間がかからないほうが運用しやすいです。

Q：その他に評価いただいた点はございますか？

市橋：丸紅情報システムズ様が窓口となって、あらゆる問い合わせに対応してくれたことです。丸紅情報システムズ様へ問い合わせれば、証明書の発行や更新はJIG-SAW様が、WAFはサイバーセキュリティクラウド様が対応してくれます。我々ユーザー企業にとっては、証明書の窓口、WAFの窓口や障害対応の窓口というように、問い合わせ窓口が何箇所もあるよりは、一箇所で一元対応していただけることは運用管理の手間が減ります。

清水建設株式会社

WAF導入後は脆弱性診断の結果が如実に向上！

Q：攻撃遮断くんの導入効果はございましたか？

井上：「攻撃遮断くん」導入後に例年通りセキュリティ診断を実施すると、WAFを導入したサーバは軒並み評価上がり、指摘事項が減っていました。脆弱性診断の結果が目で見て分かる成果ではないでしょうか。実際にレベルの低い攻撃からSQLインジェクションなどのレベルの高い攻撃まで、全て防いでくれています。

市橋： WAFを導入できていないサーバと比べると、診断結果は明らかです。WAFを導入したものは診断結果が如実に向上していました。予想外にも嬉しかったこととしては、一機も誤検知が無かったことです。WAF導入後の誤検知や過検知は、ある程度覚悟していましたが、今回、「攻撃遮断くん」導入後に誤検知による不具合の問い合わせは一度も受けていません。

Q：Webセキュリティ重要性について、どのように考えられていますか？

井上：最近のサイバー攻撃は巧妙化していて、Webサイトのコンテンツ内容に関わらず攻撃を受けるリスクがあると思います。例えば、踏み台にされてしまうと自社サーバが被害を受けるだけでなく他の企業へ被害が及ぶこともありますので、どんなWebサイトへもセキュリティ対策は必要であると考えています。

市橋：当社では各部門の責任者を集めて会議を行い、情報システム部で策定したガイドラインに従って必ずWAFを導入するよう、責任者対して説明しいきます。「サーバ上に取られて困る情報は無い」でなく、加害者にならないためにはどうすれば良いかを考え対策することが大切です。誰もが被害者になりたくないという意識は非常に強いため、情報にはアクセス制限や暗号化をしていますが、それだけでなく攻撃の踏み台にされて加害者にならないようにするという意識が重要だと考えています。

■ご協力企業様

丸紅情報システムズ株式会社

JIG-SAW株式会社

株式会社ソルクシーズ

株式会社ソルクシーズはクラウドサービス「Fleekdrive」をはじめとした自社サービスを提供する一方で、SI事業や金融業界の企業を中心としたソフトウェア開発事業などワンストップであらゆるITソリューションを提供しています。今後はIoTやフィンテック、AIといった新しい分野へ力を入れ、さらなる成長を目指しています。

事業支援部 情報化推進グループ
担当マネージャー
浅山 大輔 様

ソルクシーズのコーポレートサイトには2016年12月からクラウド型WAF「攻撃遮断くん」が導入されています。なぜコーポレートサイトへWAFを導入するに至ったのか、その理由と「攻撃遮断くん」の選定理由を、自社・グループ会社の業務システムやネットワークインフラ、情報セキュリティの企画から運用保守まで担当する浅山様にお伺いしました。

「会社の恥を晒すことはできない。」の意識からWAFの導入へ

Q：今回どのような理由でWAFを導入するに至ったのか、導入経緯をお聞かせください。

2016年6月に当社のコーポレートサイトをリニューアルしまして、当然多くの人に見ていただきたいという思いがありましたが、リニューアルして2~3カ月が経過した頃、サイバー攻撃によってコーポレートサイトが見られなくなってしまうということがありました。
当時「攻撃遮断くん」無料トライアル（旧サービス名：「攻撃見えるくん」）※1を実施しており、管理画面を見ると明らかに同じIPから攻撃が来ていたため、恐らくDoS攻撃であるということがわかりました。DoS攻撃は攻撃元のIPをブロックすれば防ぐことができるのですぐに対応できましたが、こういったツールを導入していないと、どれくらい攻撃が来ているかわかりません。DoS攻撃を受けたことで「サイバー攻撃は実際に来たし、当社にどれくらいサイバー攻撃が来ているかも気になるし心配だ」ということになり、すぐにセキュリティ対策を検討し始めました。
WAF導入以前からポートフィルタリングや、アプリケーション側ではSQLインジェクション等のセキュリティ対策を実施していましたが、許可された通信についてはサイバー攻撃かどうかわからないため、WAF等のセキュリティ製品の導入が必要と判断しました。

Q：「DoS攻撃では情報漏えい等の損害は出ていないと思いますが、予算をかけてコーポレートサイトへセキュリティ対策したのは何故ですか？

せっかくリニューアルしたサイトが見られなくなるのは当然良くないことですので、サイトリニューアルをきっかけに会社全体でセキュリティ対策の優先度が上がったということはあるかもしれませんが、やはり「コーポレートサイトは会社の顔である」という意識がサイトを担当している部署にも我々にもありますので、「会社の恥をさらすことはできない」というのが１番の理由です。

※1　2018年3月「攻撃見えるくん」の提供を終了し、2018年4月「攻撃遮断くん」無料トライアルの提供を開始

株式会社ソルクシーズ

導入の決め手は導入スピードとIPS＋WAFという特性から「攻撃遮断くん」を採用

Q：WAF選定時に、どのような要件があったかお聞かせください。

まず、攻撃状況を把握できるもので考えていました。どのような攻撃が一定期間にあったのか、その攻撃をちゃんとブロックしたのかということが一覧でわかるもの。また、既に攻撃を受けてしまっていたので短納期、そして低コスト。あとは、攻撃をブロックする際にはWAF側で何らかの処理が発生するため、ユーザーレスポンスに影響が少ないもの。この3点を重視していました。

Q：アプライアンス型・ホスト型を選ばなかった理由は何ですか？

当社のコーポレートサイトがクラウド環境にあることから、アプライアンス型は適さないため最初から考えていませんでした。また、サイトリニューアル前からサーバはクラウド上にありましたが、それはハードを持ちたくないという方針から始まっていて、ハードが増えるアプライアンス型はそれに逆行してしまいます。
そうなると、サーバへインストールするホスト型かクラウド型ということになります。
ホスト型の場合はサーバへインストールするのが手間である点、クラウド型の場合はDNSを切り替えなくてはいけないため、何か障害が起きたときに問題の切りわけが難しくなる点、そしてユーザーレスポンスに影響が出る可能性を懸念していました。

Q：「攻撃遮断くん（サーバセキュリティタイプ）」を導入された決め手をお聞かせください。

他社WAFも比較する中でコスト面におけるメリットもそうですが、無料トライアルを実施していたことによる導入スピードが一番ではないでしょうか。インストールする点ではホスト型と同じですが、既に使用しているアカウントや管理画面をそのまま使えるということでしたから。ただ既に利用しているという面で、別サービスへ導入していたIPSで対策できないかということで、WAF同士はもちろんですが、IPSとWAFについても比較をしていました。

OSやミドルウェアの脆弱性に関してはIPSの方が強く専門分野だと判断していたので、IPSもWAFも両方導入しようかという案も出ていました。しかし、「攻撃遮断くん（サーバセキュリティタイプ）」であればOSやミドルウェアの脆弱性を突く攻撃に対しても効果があるという特性がありましたので、IPSとWAFを導入して二重でコストをかけるよりも「攻撃遮断くん」だけで良いという判断をしました。また、両方導入した場合に競合するので、正常動作確認が求められることも避けたいところではありました。

IPSとWAFを比較した結果、Webアプリケーションのセキュリティ対策としてはIPSだけでは攻撃を防ぎきれないので、OSやミドルウェア、Webアプリケーションへの脆弱性をカバーできる「攻撃遮断くん」を選びました。「攻撃遮断くん」ではDNS切り替え型のようなレスポンスへの影響も出ないというところもポイントとなりました。

Q：「攻撃遮断くん」導入効果は感じられていますか？

導入して1年以上経ちますが、DoS攻撃や別の攻撃によるWebサイトの改ざんといった被害発生もなく、低コストで必要十分な安心感がシステム管理者として得られています。管理画面はメイン担当含めて3人程度が見ることがあり、主に部内で週に一度攻撃状況と攻撃を防いだ状況を共有し、月に一度本部長へ報告、その際に管理画面でレポートを出力して提出しています。例えば流行している攻撃があれば、当社には攻撃が来ていないかなどの攻撃状況の把握に管理画面は役立っています。

株式会社ソルクシーズ

WAFやIPS等のセキュリティは最低限かつ必須セキュリティ

Q：コーポレートサイトへセキュリティ対策する企業様はまだまだ少ないと感じていますが、コーポレートサイトへWAFを導入する重要性についてどう思われますか？

今ではインターネットは当たり前のインフラとなったというなかで、「会社の顔であるホームページが停止や遅延、ましてや改ざんされることによって見ていただいた方に被害を与えるような事態というのは絶対に避けるべきである。」という考え方を徹底するべきではないかと考えています。そのためにはWAFやIPSといった最低限かつ必須セキュリティではないでしょうか。余談ではありますが、例えば海外で「コーポレートサイトを見てマルウェアへ感染したことへの損害賠償請求」というような裁判が行われていれば、そう遠くないうちに日本でも行われるだろうし、そうなればコーポレートサイトへのセキュリティ対策の重要性は増してくるのかなと思っています。

メールによるサイバー攻撃を警戒　さらなるセキュリティ強化へ

Q：今後前向きに検討しているセキュリティ対策はございますか？

昨年の後半くらいから大手の銀行やECショップ等のメールに似せた標的型攻撃メールが流行っていて、当社にも結構な数のメールが届きました。実際に社員にも届いてしまい、幸いにもメールを開いて本文をクリックした社員はいなかったのですが、調べてみると当社のメールのフィルタリングをすり抜けるような仕組みで送信されていることが分かりました。このようなメールによるサイバー攻撃は今後も続くものであると思いますので、訓練を含めて社員への啓蒙活動に力を入れていきたいと考えています。

過去にニュースとなった個人情報や仮想通貨の流出の件などの多くはメール経由で感染した不正プログラムが原因と報道されていますし、メールというのは業務に関係してそうだなと思うとどうしても開いてしまいますよね。サイバー攻撃の２大経路というのはWebとメールですので、全Webサイトへのセキュリティ対策はもちろんのこと、メールに関してもしっかりとセキュリティ対策していかないといけないと思っています。

株式会社ファンコミュニケーションズ

Q：導入までの経緯をお聞かせください。

まず、コーポレートサイトのセキュリティを向上させようというプロジェクトがありました。
サイバー攻撃に対しては手動でIPアドレスをブロックして回避していたのですが、攻撃の頻度や種類も増えてきたため、
WAFサービスを探し始めたのが最初のきっかけです。

Q：「攻撃遮断くん」をお選びいただいた決め手は何でしょうか。

いくつかセキュリティサービスの候補を出したのですが、直接IPアドレスにくる攻撃には対応できないものがほとんどでした。
そこで御社の攻撃遮断くん（サーバセキュリティタイプ）ならそうした攻撃も防げて、
簡単に導入できるということでしたので、選ばせていただきました。
翌営業日から導入できる点と、申込までのフローが簡単だったのはよかったですね。
また、とりあえずトライアルでやってみようかなと思えたことも、攻撃遮断くん導入の
きっかけとなりました。
それから、やはり他社よりも低価格であることは非常に大きかったですね。
また、ひと月のデータなどを見てから導入を決めたのですが、その際のレポートもわかりやすかったです。
レポート内容がロボット的な集計だけではなく「こうしてブロックしたほうがいいですよ」と対応策も書いてあり、
人の手が入っている部分も気に入りました。

Q：「導入してよかった」と感じていただけた場面はございますか。

まずはサイバー攻撃が見える化されている点ですね。ログを見ればわかることをより視覚的に理解できます。
また、わかりやすいレポートをエクスポートできる機能があるので、エンジニアではない人に対しても説明がしやすいです。
こういった攻撃を受けているけれどもブロックしていますよ、という状況をわかりやすく伝えられることが
非常に良かったと思っています。

Q：弊社へのイメージやご要望をお聞かせください。

私たちの要望をヒアリングして、良いものは反映していこうという意識が伝わってきます。
例えば管理者機能だったりユーザー権限の付与など、こういう機能が欲しいですというお話しをしたら、
いつまでにリリースを目指していますというお返事をいただいたり、細かいことですが、請求書の形式などにも
柔軟に対応していただいたこともその一つです。
今後もさらなる新機能の実装に期待しております！

お問い合わせ

会社名	株式会社サイバーセキュリティクラウド
本社所在地	〒150-0031　東京都渋谷区東3-9-19 VORT恵比寿maxim3階
Webサイト	コーポレートサイト：http://www.cscloud.co.jp サービスサイト：https//www.shadan-kun.com
電話での お問い合せ	03-6416-1579（平日10:00～18:00）
メールでの お問い合わせ	sales@cscloud.co.jp