クラウド型 WebApplicationFirewall（WAF）

攻撃遮断くん

サービス仕様書

（公開版）

Ver.1.2.0

株式会社サイバーセキュリティクラウド

目次

1. 本書の目的

クラウド型 WebApplicationFirewall（WAF）攻撃遮断くん（以下、本サービスと記します）の仕様に関して説明する資料となります。

2. 用語の定義

本文書で使用する用語を説明します。

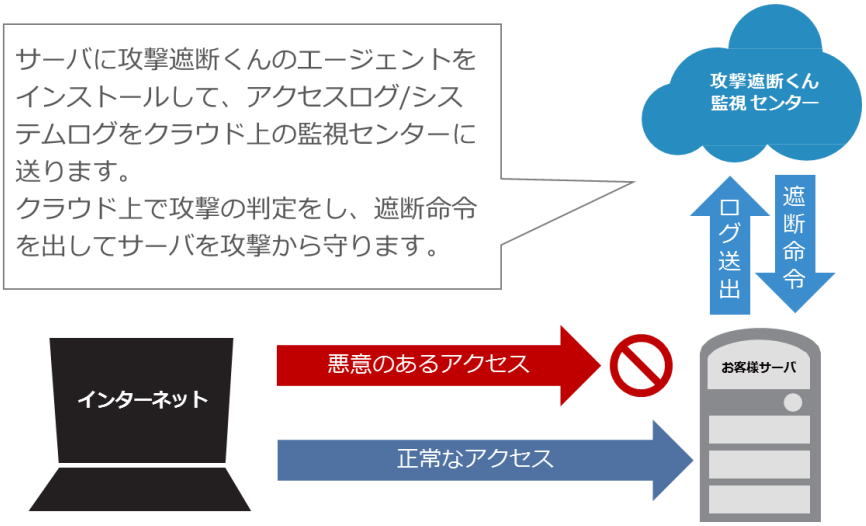
用語	説明
お客様	本サービスのサービス利用約款に基づく契約を弊社と締結し、本サービスの提供を受ける者。本サービスは法人または法人に準ずる団体に限りご利用できます。またお客様の委託を受け作業を代行する者も同様に定義しております。
攻撃遮断くん	本サービスで使用する、サーバや Web アプリケーションへのあらゆるサイバー攻撃を遮断するセキュリティサービス(有償)です。
攻撃遮断くん サーバセキュリティタイプ	攻撃遮断くんにおける、クラウド型 IPS+WAF のサーバセキュリティサービスプランです。
攻撃遮断くん WEB セキュリティタイプ	攻撃遮断くんにおける、SaaS 型 WAF タイプの WEB セキュリティサービスプランです。
攻撃遮断くん DDoS セキュリティタイプ	攻撃遮断くんにおける、DDoS 特化型 WAF タイプの WEB セキュリティサービスプランです。
企業アカウント	お客様の請求先単位・管理画面の提供の単位で発行される ID およびパスワードです。

3. サービス概要

本サービス「攻撃遮断くん」はクラウド型 WAF（Web Application Firewall）です。
Web アプリケーションの脆弱性を悪用した各種攻撃から Web サイトを守り、管理画面から攻撃の状況を確認することが可能です。また、月次で専門家によるコメントつきの月次レポートが届き、お客様の大切な web サービスの状況を確認することができます。
（WEB セキュリティタイプ・DDoS セキュリティタイプ：1 サイトプランは月次レポートが有償オプションとなります。）

【サーバセキュリティタイプ】

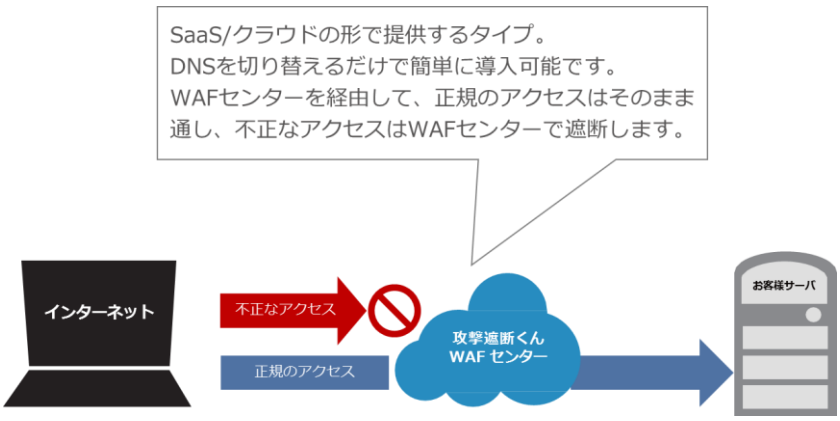
専用ハードウェアは必要なく、エージェントをインストールすることで、管理画面を用いて運用をいたします。サーバの一時停止やネットワーク構成を変更することなく、サービス開始が可能です。



【WEB セキュリティタイプ】

お客様のシステムに変更を加えることなく、DNS の切替えだけで短期間で WAF の導入が可能です。シグネチャを更新することでアップグレードし、攻撃を遮断いたします。

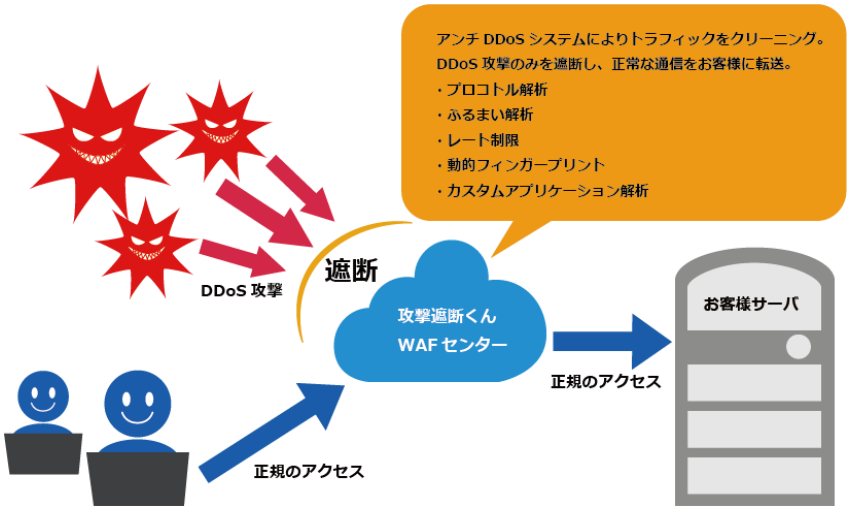
シグネチャ更新や運用は、全て「攻撃遮断くん」側で対応します。



【DDoS セキュリティタイプ】

お客様のシステムに変更を加えることなく、DNS の切替えで WAF の導入が可能です。様々なロジックで解析するアンチ DDoS システムにより、サーバの手前で攻撃を遮断し、サーバダウンによるサービス障害を防ぎます。

シグネチャ更新や運用は、全て「攻撃遮断くん」側で対応します。



4. サービス仕様

4.1 提供機能について

主な提供機能は以下となります。

項目	詳細
サイバー攻撃可視化機能 攻撃遮断くん/サーバセキュリィタイプ、WEB セキュリティィタイプ・DDoS セキュリティィタイプ:Web サイト入れ放題プラン:使い放題プラン）	24 時間 365 日、お客様に対する攻撃の閲覧が可能です。リアルタイムで確認が可能です。
サイバー攻撃防御機能	国内データセンターにて運用を行い、24 時間 365 日サイバー攻撃を防御します。
検知遮断の報告機能 （攻撃遮断くん　サーバセキュリティィタイプ、WEB セキュリティィタイプ・DDoS セキュリティィタイプ:Web サイト入れ放題プラン）	お客様ごとの管理画面で、お客様に対する攻撃の閲覧および遮断履歴の閲覧がリアルタイムで確認可能です。
システムの保守運用作業	システムの保守・運用作業を行います。
システムのバージョンアップ	システムのバージョンアップを行います。
シグネチャの最新アップデート	クラウド上でシグネチャを常に最新バージョンへアップデートします。常に最新の脅威に対応することが可能です
管理画面の提供	サービス毎に貴社環境の設定が確認できます。 Web/DDoS セキュリティィタイプに関しては、転送先の設定や SSL 証明書の設定(更新含む)が可能です。 監視センターとの接続状況の確認も可能です。
攻撃遮断くん攻撃ログ月次レポート	お客様へお渡しする管理画面上で、お客様に対する攻撃の日付・時間帯別・攻撃種別集計、検出攻撃割合等のログをダウンロードすることが可能です。 ※弊社より月次レポートを送付するサービスでは御座いません。 ※WEB セキュリティィタイプ・DDoS セキュリティィタイプ:1 サイトプランはオプション機能となります。
DDoS 対策 （攻撃遮断くん　DDoS セキュリティィタイプ）	WAF では防御できない DoS/DDoS 攻撃を、お客様ネットワークより上位のネットワーク側で検知/軽減することにより、サーバやネ

	ットワーク機器、インターネット回線までを含めた防御が可能です。
サイバー保険付帯 （攻撃遮断くん　WEB/DDoS セキュリティタイプ:1 サイトプラン内~500kbps プランは除く）	10Gbps 以上の DDoS 攻撃・ゼロデイ攻撃に起因して、お客様に損害が発生した場合に、その損害を補償します。 ※保険は自動付帯となります

4.2 サーバセキュリティタイプ仕様

4.2.1　防御対象の攻撃

攻撃手法
ブルートフォースアタック
SQL インジェクション
クロスサイトスクリプティング
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
コマンドインジェクション
LDAP インジェクション
ファイルインクルード攻撃
ＵＲＬエンコード攻撃
各種 OS・ミドルウェアへの脆弱性を突いた攻撃
その他の WEB 攻撃全般

4.2.2 システム・ソフトウェア要件

サーバセキュリティタイプはお客様のサーバへエージェントをインストールしてご利用いただくサービスとなります。インストールには root 権限を必要とします。

4.2.2.1 推奨サーバースペック

エージェントをインスールする際に必要となる容量は以下の通りです。攻撃の検知・遮断の最中でもサーバへの負荷は 1%以下となります。

- 2GB RAM デュアルコア CPU
- 12GB の HDD 空き容量

4.2.2.2 対象 OS

導入可能 OS 一覧
Linux の全てのディストリビューション（RHEL、CentOS、Debian、Amazon Linux、etc）
FreeBSD (all versions)
OpenBSD(all versions)
NetBSD(all versions)
Solaris 2.7, 2.8, 2.9, 10 and 11
AIX 5.3, 6.1 and 7.1
HP-UX 10, 11, 11i
Windows Server 2003, 2008 and 2012

4.2.3 サービス提供フロー

各プランに応じて提供フローが異なります。

① 【攻撃遮断くん/サーバセキュリティタイプ】使い放題プラン

使い放題プランをご希望される場合は弊社までご連絡ください。
契約内容を確認後、ご連絡いたしますので管理画面よりお客様専用の企業アカウントを発行してください。
企業アカウント承認後に登録に必要な手順をメール致しますので、手順に従い必要情報をご登録ください。ただし IP アドレスの登録は行わないでください。
契約後に専用の基盤をご用意し、10 営業日以内に完了のご連絡を致します。
基盤構築完了後、管理画面より IP アドレスのご登録を行ってください。
発行されたエージェントキーを使用してエージェントのインストールを行ってください。

② 【攻撃遮断くん/サーバセキュリティタイプ】ベーシックプラン

弊社管理画面よりお客様専用の企業アカウントを発行してください。
企業アカウント承認後に登録に必要な手順をメール致しますので、手順に従い必要情報をご登録ください。
発行されたエージェントキーを使用してエージェントのインストールを行ってください。

4.2.4 運用サポート

① シグネチャカスタマイズ

誤検知や特定の条件での除外、パラメータの調整等サポート窓口で対応致します。

② サーバ移行

・IP アドレスが変更される場合は新規にエージェントキーを発行してご対応ください。
導入については問題ございませんが、契約について確認するため別途ご連絡ください。

・IP アドレスを変更しない場合は現在のエージェントキーを使用しての対応が可能です。
サーバのなりすまし防止のため整合性をとっており、サーバが変更された際に、設定の変更作業が発生するためご連絡ください。

③ 検知(IDS)モード／遮断(IPS)モード切替

遮断モードと検知モードの切り替えが可能です。管理画面のマニュアルをご確認ください。

4.3 Web セキュリティタイプ・ DDoS セキュリティタイプ仕様

4.3.1 防御対象の攻撃

攻撃手法
SQL インジェクション
クロスサイトスクリプティング
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
コマンドインジェクション
LDAP インジェクション
ファイルインクルード攻撃
ＵＲＬエンコード攻撃
その他の WEB 攻撃全般
DoS 攻撃/DDoS 攻撃（DDoS セキュリティタイプのみ）
ミドルウェアなどの脆弱性を突いた攻撃 （Apache Struts2 の脆弱性など）

4.3.2 転送仕様

① 対応プロトコル

HTTP および HTTPS に対応しております。
※HTTP2 には対応しておりません。

② ポート番号仕様
HTTP 80 HTTPS 443 ですが、お申し込み時にご指定いただけます。

③ 送信元 IP アドレス
導入いただく WAF センター基盤の IP アドレスでのアクセスに変わります。

④ レイテンシ
約 50 ミリ秒

4.3.3 導入要件

① 導入いただく FQDN に関する DNS 設定が変更可能であること
DNS の設定変更(CNAME もしくは A レコード)が可能であること。なお、メールサーバや FTP サーバ等で FQDN を共有されている場合はご注意ください。

② HTTPS をご利用の際は SSL 証明書のご用意が可能であること
通常はサーバに設定していただいている SSL 証明書(サーバ証明書、中間証明書、秘密鍵)をご提供ください。レンタルサーバや AWS の Amazon Cetification Manager 等で証明書が発行されており提供が難しい場合は別途証明書を作成いただき提供をお願いしております。
証明書のコピーを取り出す方法に関しては証明書会社様やサーバ業者様にご確認をお願いします。※別途取得に費用が掛かる可能性がございます。

③ 接続クライアントが SNI (Server Name Ingication) に対応しているか把握していること
通常では、SNI 非対応クライアントには対応しておりません。別途オプションでのお申し込みが必要となります。

④ クライアント証明書には対応しておりません。

⑤ CDN(Content Delivery Network)をご利用されている場合には事前にご相談ください。

4.3.4 サービス提供フロー

① 【攻撃遮断くん/WEB セキュリティタイプ、DDoS セキュリティタイプ】 入れ放題プラン
ご使用する帯域に応じてプランが変わりますので必要帯域をお調べください。

※帯域はピーク時の情報をお調べください。
必要情報をヒアリングシートに記載いただきご連絡ください。
HTTPS 通信をご使用の場合は証明書情報（証明書、中間証明書、秘密鍵）が必要となります。
情報を元に専用の基盤を構築し、**10 営業日以内**にご連絡いたします。
完了時に、CNAME の FQDN 名および IP アドレスを提供致します。
お客様にて DNS 情報を切り替えて頂きます。

② 【攻撃遮断くん/WEB セキュリティタイプ、DDoS セキュリティタイプ】 1FQDNプラン
ご使用する帯域に応じてプランが変わりますので必要帯域をお調べください。
※帯域はピーク時の情報をお調べください。
必要情報をヒアリングシートに記載いただきご連絡ください。
HTTPS 通信をご使用の場合は証明書情報（証明書、中間証明書、秘密鍵）が必要となります。
4 営業日以内に設定完了のご連絡を致します。
完了時に、CNAME の FQDN 名および IP アドレスを提供致します。
お客様にて DNS 情報を切り替えて頂きます。

4.3.5 設定確認／動作検証

・Hosts ファイルを使用したアクセス確認
ご使用の PC の hosts ファイルに対象 FQDN の接続先情報を設定することで確認ができます。
別途ご案内します手順に従い、hosts ファイルを編集しアクセス確認を行ってください。

4.3.6 運用サポート

① 管理画面の提供
管理画面にて検知状況をご確認いただけます

- 入れ放題プラン
  専用基盤の IP アドレス毎に検知状況を確認するタイプと
  FQDN 毎に検知状況が確認できるタイプをお選びいただけます。

- 1FQDNプラン
  FQDN 毎に検知状況が確認いただけます。

② カスタマイズ

- 入れ放題プラン

  シグネチャカスタマイズに対応しております。検知状況をご確認後、別途ご相談ください。

  IP アドレス制御のカスタマイズに対応しております。ホワイトリストについては管理画面より登録可能です。その他をご希望の場合は、別途ご相談ください。対応可否を確認します。

  ※FQDN 毎の表示に変更した場合、お客様自身での編集ができない項目が発生します。ご不明な場合はご連絡ください。

- 1FQDNプラン

  シグネチャカスタマイズに対応しておりません。

  IP アドレス制御のカスタマイズはホワイトリストのみ対応可能です。管理画面から登録できませんので設定をご依頼ください。

③ 障害発生時

WEB セキュリティタイプ、DDoS セキュリティタイプ トラブル時

トラブルが発生していると思われる場合は DNS を切り戻してください。

4.3.7 導入時の注意点

以下、WEB セキュリティタイプ・DDoS セキュリティタイプ導入時の注意点となります。

① ソース（送信元）IP アドレスの変更について

ソース IP アドレスが全て、「攻撃遮断くん WAF センター」 の IP アドレスになります。御社サイトにて、ソース IP アドレスを使用した作業を実施している場合はご注意ください。

ソース IP アドレス使用例

・アクセス解析

・ソース IP アドレスを利用した WEB アプリケーションによる表示変更

・ソース IP アドレスを利用したロードバランシング

② ファイアウォールの設定について

ファイアウォールで同じ IP アドレスからの同時接続数を制限している場合は、その設定を解除願います。

③ ファイアウォールでの制限について

「攻撃遮断くん」 を導入することにより、ソース IP アドレスが全て、「攻撃遮断くん WAF センター」 の IP アドレスとなります。その為、ファイアウォールで、「攻撃遮断くん」 以外か

らのアクセス禁止することで、よりセキュアな環境が構築できます。
・ファイアウォールで制限をした場合のメリット
FQDN ではなく、IP アドレスを指定してアクセスした場合も、制御が可能となります。
・ファイアウォールで制限をした場合のデメリット
万が一、データセンター障害発生時に、DNS の変更と同時にお客様側でファイアウォールの変更を実施していただきます。

④ SEO への影響について
特に問題ありません。基本的には IP アドレスを移転するときと同様の処理になります。

⑤ Google アナリティクスなどのビーコン型アクセス解析ツールへの影響について
影響はありません。