しぇあわふ

サービス仕様書

第 1.4 版

2021 年 3 月 11 日

KOANKEISO

興安計装株式会社

目　次

内容

改訂履歴

版数	更新日	更新内容	更新者
1.0	2020/4/9	初版作成	興安計装株式会社
1.1	2020/4/22	「３－１．WAF」マルウェア対策内容更新	興安計装株式会社
1.2	2020/5/28	ウィークリーレポートについて追記	興安計装株式会社
1.3	2020/7/3	DoS 対策、証明書更新、カスタムレポートについて追記	興安計装株式会社
1.4	2021/3/11	帯域プラン、レポートに関する注意点について追記	興安計装株式会社

はじめに

本仕様書は、興安計装株式会社（以下「当社」とする）が提供する「しぇあわふ」（以下「本サービス」とする）の提供を受ける者（以下「利用者」とする）に対する、本サービスの機能、サービス内容、その他の諸条件について記載するものです。

また、本仕様書は「しぇあわふサービス利用規約」の一部を構成するものとします。

本サービスにおけるお問い合わせは、さくらインターネット株式会社が提供するメールによるサポート窓口をご利用いただくか、技術情報にて公開されたナレッジをご参照ください。本サービスの製品 XGFirewall の開発元であるソフォス株式会社への直接の問い合わせを固く禁じます。

1. サービスについて

（1）サービス提供内容

提供項目	内容
Web サーバ保護	DNS 設定によるアクセス転送を介して、Web サーバに対する WAF、IPS、国別フィルタ機能を提供します。

（2）サービスプラン

本サービスでは、提供される回線の帯域によって 2 種類のプランを提供しています。

プラン名称	機能
200kbps プラン	平均帯域 200kbps を提供するプランとなります。
2Mbps プラン	平均帯域 2Mbps を提供するプランとなります。

※　2021 年 3 月 11 日より以前にしぇあわふにお申込みいただいたお客様については、200kbps プランを提供させていただいております。

（3）サービス提供範囲

本サービスで提供される機能は以下の通りです。

サービス項目	機能
WAF	Web サーバに対する各種攻撃トラフィックの遮断を行います。
IPS	シグネチャマッチングによる攻撃トラフィックの遮断を行います。
国別フィルタ	IP アドレスからアクセス元の国を判別し、ポリシーに則った通信制御を行います。
アクセス元通信制御	事前に利用者が定義したポリシーに従って、特定のアクセス元 IP アドレスからの通信制御を行います。
レポート	Web サーバ利用状況、WAF、IPS の 3 種類のレポートを提供します。 デイリー、ウィークリーのタイミングで提供が可能です。 カスタムレポートはオプションサービスとしてβ提供されます。
アップデート	本サービスにて提供されているセキュリティ機能に関わるソフトウェア、シグネチャの適切なアップデートを提供します。

本サービスで提供される各機能の詳細については３．提供機能の詳細をご参照ください。

（4）サービス利用条件

本サービスの利用条件は以下の通りです。

① ご利用環境

インターネット経由でアクセス可能な Web サーバーを対象とします。

※ HTTP、HTTPS のプロトコルに対応しております。

※ クライアントからのアクセスに使用されるポート番号は、個別に指定することが可能です。

※ IPv6 アドレスの Web サーバーには対応しておりません。

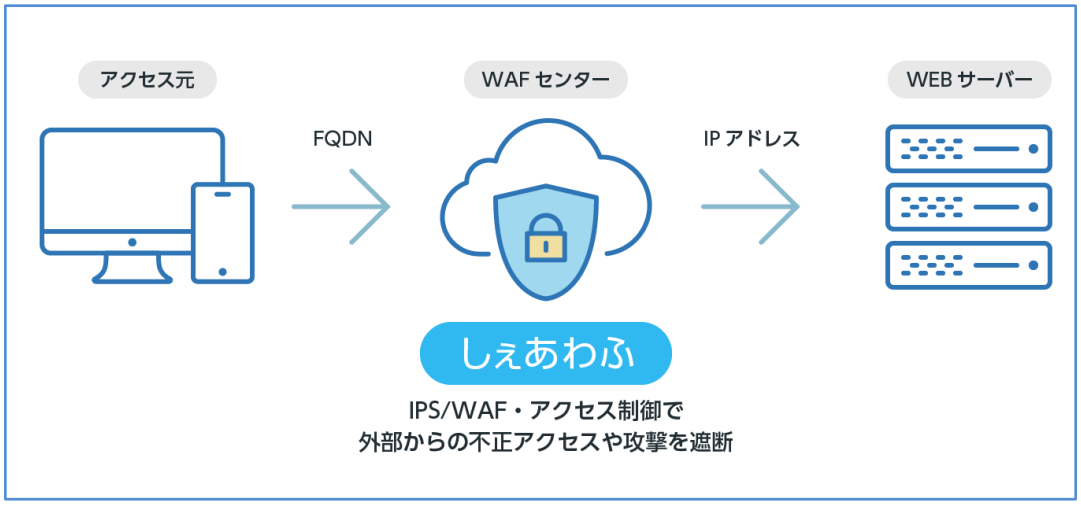
※ 利用者自身が DNS の編集権限を有していない、共通ドメインを利用した Web サイトではご利用いただけません。

※ Web サーバーと同じ FQDN でメール等その他のサービスを利用している場合、そちらのサービスが利用できなくなるため、Web サーバー専用の FQDN をご用意ください。

※ DNS を利用せず、直接 IP アドレスを公開している Web サイトではご利用いただけません。

② 導入構成

本サービスでは、保護対象 Web サイトの DNS 設定を変更することで、保護対象 Web サーバー宛の通信をクラウド上のセキュリティ装置に転送し、不正な通信の検査を行ったうえで保護対象 Web サーバーに転送します。



③ サイジング

本サービスを利用する Web サイトのサイジングについて、プラン毎の提供帯域を以下に記載します。提供帯域を超えるアクセスが発生した場合、サービス側で帯域制御を行う可能性がございます。

プラン名称	提供帯域
200kbps プラン	200kbps
2Mbps プラン	2Mbps

※　上記の提供帯域は参考値であり、回線状況によっては提供帯域内の利用であっても通信に遅延が発生する可能性があります。

④ 契約の範囲

本サービスでは、1 契約の範囲で同一の FQDN で運用される 1 つの Web サイトに対する防御を提供します。

※　共通のサーバーを転送先とする複数のドメイン名を 1 契約の範疇として登録することができます。

※　同一の Web サイトを冗長化・負荷分散する目的で運用される複数台のサーバーを転送先として登録することができます。

（5）サービスの構成

本サービスでは、複数のホストサーバーで構成されたリソースプールを共有するクラウド基盤上に構築されており、セキュリティ装置にて障害が発生した場合、フェールオーバー機能によって自動復旧する構成となっております。

本サービスでは、設備に対する DoS 対策として、サービス規定の閾値を超えた通信量のパケットを受信した場合、送信元 IP アドレス単位で通信の制限を行います。

具体的な閾値については設備保護の観点から公開はしておりません。

本サービスにおいてシステム障害が発生している場合も、保護対象 Web サーバーにてアクセス元の制限を行っていない状態であれば、Web サーバーの IP アドレスに対する直接のアクセスは可能です。

（6）サービス利用の流れ

本サービスご利用までの流れは以下の通りとなります。

提供ステップ	実施内容
①　申込書の提出	申込書にて、以下の情報を提供ください。 ・ 導入する Web サイトの FQDN ・ 導入する Web サイトの IP アドレス ・ 導入する Web サイトのリスニングポート ・ 保護対象 Web サイトへのアクセスを必ず許可、あるいは遮断したいアクセス元 IP アドレス ・ 国別フィルタにて通過、あるいは遮断対象としたい国情報 （HTTPS 利用サイトの場合） ・ 導入する Web サイトに設定されている SSL 証明書（サーバ証明書、中間証明書、秘密鍵）
②　開通設定	受領した情報からサービス側で開通設定を実施します。 通常、申込情報が揃った時点から 5 営業日程度で設定が完了します。
③　利用開始	サービス側より、利用者に設定いただく CNAME、IP アドレスの情報を含む開通案内をメールにてお知らせします。
④　DNS 設定の変更	利用者側で通知された情報をもとに DNS 設定を更新し、保護対象 Web サイト向けの通信を本サービス設備向けに切り替えます。 端末の hosts ファイルを更新することで、通信切り替え前に本サービスをテストいただくこともできます。

※　HTTPS 利用サイトがレンタルサーバや AWS 等のクラウドサービスにて発行された証明書を利用しており、提供が難しい場合は別途証明書の作成が必要となります。

※　Let’s Encrypt の証明書をご利用いただいている場合、しぇあわふ設備にインストールされた証明書は、サービス利用期間中は自動的に更新されます。なお、お客様が管理する保護対象サーバにインストールされた証明書の更新はしぇあわふサービス側では行われません。

※　サービス側の提供するセキュリティ装置の IP アドレスは、障害等の理由で変更される可能性があるため、DNS 設定では CNAME を利用することを推奨いたします。

※　DNS 設定の変更以降、保護対象 Web サーバーで受信するリクエストの送信元 IP アドレスは、本サービスが提供するセキュリティ装置のものとなります。

※　保護対象 Web サーバーで受け入れるアクセスを、本サービスが提供するセキュリティ装置からのものに限定することで、保護対象 Web サーバーの IP アドレスに対する直接の攻撃を防ぐことができます。

※　保護対象 Web サーバーに対するアクセス制限を行った場合、障害対応等の理由で本サービスが提供するセキュリティ装置の IP アドレスが変更になった場合に、保護対象 Web サーバーのアクセス制限設定を変更いただく必要がございます。

2．運用について

本サービスの運用について以下に記載します。

（1）メンテナンスについて

本サービスでは、サービス提供基盤のハードウェア、セキュリティ機能を提供するソフトウェア、シグネチャの更新等の理由で、定期・不定期のメンテナンスを行います。

また、障害やセキュリティ上のリスク対策等やむを得ない理由があった場合、緊急でメンテナンスを行う場合があります。なお、メンテナンスに関する個別の問合せは受け付けておりません。

メンテナンス種別	実施内容
定期メンテナンス	毎月 第 2 金曜日　AM 3:00 ～ 4:00 JST 毎月 第 4 金曜日　AM 3:00 ～ 4:00 JST 上記の時間帯、10 分程度のサービス断が複数回発生します。
不定期メンテナンス	不定期に発生するメンテナンスについては、原則夜間の実施となり、実施の 20 日以上前に実施内容を SNS に掲載いたします。
緊急メンテナンス	実施内容については、事後に SNS に掲載いたします。

※　定期メンテナンスの実施要領は固定となるため、SNS による告知はございません。

（2）障害について

本サービスでは、サービス提供基盤のハードウェア、セキュリティ機能を提供するソフトウェアに障害が発生した場合、障害対応状況、影響範囲、復旧見込みについて SNS への掲載を以って周知いたします。

（3）問合せについて

本サービスに関する不明点については、メールによるサポート窓口をご利用いただくか、技術情報にて公開されたナレッジをご参照ください。

（4）設定変更について

本サービスに関する設定、運用情報の変更については、別途提供されるヒアリングシートに変更内容を記載の上、メールによるサポート窓口を介してご依頼ください。

（5）証明書更新について

本サービスのご利用にあたって提供いただいたサーバ証明書の更新期限については、お客様ご自身で管理いただく必要がございます。

サーバ証明書期限切れの一ヶ月前を目途に、別途提供されるヒアリングシートに必要事項を記載の上、メールによるサポート窓口を介して更新作業をご依頼ください。

なお、Let's Encrypt 発行のサーバ証明書をご利用の場合は、しぇあわふ設備にアップロードされた証明書はサービス利用期間中は自動的に更新されるため、更新依頼は不要となります。

（6）ログについて

本サービスで提供する各種セキュリティ機能に関わる動作ログは、1 年間保持いたしますが、特別の理由がない限り、ログ情報の直接の開示は行いません。

3．提供機能の詳細について

本サービスが提供する機能の詳細は以下の通りとなります。

3－1．WAF

WAF 機能では、保護対象 Web サイトに対するアクセスを、以下項目の機能にて制御します。

機能項目	機能内容
Cookie 署名	Web サイトが発行する Cookie に対してセキュリティ装置にて署名を行い、不正に改ざんされた Cookie の悪用を遮断します。
フォームハードニング	Web サイト上のフォームを経由して送信された情報を検証・評価し、異常があった場合に要求を拒否します。
マルウェア対策	Web サイトに対してアップロードされるファイルについて、2 種類のエンジンによるスキャンを行い、マルウェアの送信を遮断します。 ※暗号化されたファイルのスキャンは行いません。
クライアントレピュテーション	Web サイトに対するアクセス元の IP アドレスをレピュテーションデータベースで検索し、評価の低いクライアントを拒否します。
プロトコル違反	プロトコルの RFC 標準仕様に反する要求を拒否します。
プロトコルアノマリー	プロトコルの標準的なパターンから逸脱した要求を遮断します。
要求の制限	一定の基準を超えた要求引数の量と範囲に対して制限を行います。
HTTP ポリシー	HTTP プロトコルにおいて通常利用されないオプションの仕様を制限することで、不要なリスクを低減します。
バッドロボット	ボットやクローラーからのアクセスを制限します。
共通攻撃操作	多くの攻撃に共通して利用されるコマンドの使用を検出し、遮断します。
SQL インジェクション攻撃	不正な SQL コマンドを利用した攻撃を遮断します。
XSS 攻撃	Web サイトを介した不正なスクリプトの利用を遮断します。
チェックの厳格化	禁止されているパストラバーサルの試行をチェックするなど、リクエストに関して厳重なセキュリティチェックを実行します。
トロイの木馬	トロイの木馬を利用している可能性のある通信を遮断します。
出力情報制限	サーバーから出力される情報の流出を制限します。

※　各機能項目による検出ロジックの詳細は非公開となります。

※　偽陽性の誤検知により、悪意のないアクセスを遮断する可能性がございます。

※　保護対象 Web サイトの構成によっては、可用性の確保のために特定の WAF ルールが使用できない場合がございます。

3－2．IPS

IPS 機能では、Snort による定義に従って保護対象 Web サイトへの不正な通信を遮断します。

※　保護対象 Web サイトが HTTPS を採用している場合、暗号化された通信に対してはパターンマッチングを行いません。

※　偽陽性の誤検知により、悪意のないアクセスを遮断する可能性がございます。

3－3．国別フィルタ

IP アドレスからアクセス元の国を判別し、事前に定めたポリシーに従って通信を制御します。

事前に想定された閲覧者に含まれない国からのアクセスを遮断することで、保護対象 Web サイトのリソースを最大活用でき、量的攻撃に対するリスクを最小化できます。

動作モード	内容
ホワイトリストモード	すべてのアクセスを遮断する設定をベースに、保護対象 Web サイトへの**アクセスを許可する国を設定**します。
ブラックリストモード	すべてのアクセスを許可する設定をベースに、保護対象 Web サイトへの**アクセスを遮断する国を設定**します。

※　アクセス元 IP アドレスによる国の判別に際しては、Maxmind 社の提供するデータベースを参照しています。

※　IP アドレスによる国の判別には誤判定が発生する可能性が存在するため、必ず通過させる必要がある／必ず止める必要があるアクセス元 IP アドレスについては、アクセス元通信制御機能への登録を推奨します。

３－４．アクセス元通信制御

アクセス元 IP アドレスを事前に指定することで、該当 IP アドレスからの通信を許可もしくは遮断することができます。

動作モード	内容
アクセス元ホワイトリスト	特定の IP アドレスから保護対象 Web サイトへの通信について、該当 IP アドレスをホワイトリストに設定することで、すべてのスキャンの対象外とすることができます。
アクセス元ブラックリスト	特定の IP アドレスから保護対象 Web サイトへの通信について、該当 IP アドレスをブラックリストに設定することで、完全に遮断することができます。

※　保護対象 Web サイトの IP アドレスに対する直接のアクセスについては制御することができません。

3－5．レポート

保護対象 Web サイトに関する以下のレポートを提供します。

レポート送信タイミングはデイリー、ウィークリーのいずれか、あるいは両方を提供できます。

オプションとしてβ提供されるカスタムレポートでは、以下項目を取りまとめて日本語化したレポートをマンスリーで提供いたします。

レポート名	内容
サーバー利用状況	・上位のアクセス元 IP アドレス
WAF 検知状況	・種類別のブロックされたリクエスト統計 ・上位の攻撃元 IP アドレス
IPS 検知状況	・攻撃カテゴリ別統計 ・攻撃対象プラットフォーム別統計 ・攻撃対象種類別統計 ・攻撃レベル別統計 ・遮断ルール別統計 ・上位の攻撃元 IP アドレス ・攻撃先アプリケーション別統計 ・攻撃元国別統計 ・遮断された攻撃 ・通過した攻撃

※　デイリーレポートは、前日分の通信内容を集計して毎日 AM4 時から生成され、利用者のメールアドレス宛に PDF ファイルの添付にて送信されます。

※　ウィークリーレポートは、前週分の通信内容を集計して毎週月曜日 AM1 時から生成され、利用者のメールアドレス宛に PDF ファイルの添付にて送信されます。

※　カスタムレポートは、前月分の通信内容を集計して月初 5 営業日を目途に生成され、利用者のメールアドレス宛に PDF ファイルの添付にて送信されます。

※　レポートを受信するメールアドレスは、申込書にて指定いただいたものを使用します。

※　レポートを受信するメールアドレスは、最大 5 つまで設定することができます。

※　WAF 転送先サーバをドメイン指定にてお申込みいただいた場合、レイヤー3 機能である IPS のレポートは提供されません。その場合も機能としての IPS は正常に機能します。

※　デイリーレポート、ウィークリーレポートは英語での提供となります。

※　カスタムレポートは日本語での提供となります。

※　レポートは「@owlook.jp」を送信元として送付されます。受信環境にて送信元アドレスによるフィルタ等ご利用の場合は上記ドメインを許可設定してください。

※　設備のレポートメール送信機能は監視されておりますが、伝送経路や受信環境の問題でメールが到達しない場合、サービス側で検知できない場合があるため、レポートメールが受信できない場合は個別にお問い合わせください。

3－6．アップデート

本サービスでは、セキュリティ機能を最適な状態に保つためのソフトウェアアップデート、シグネチャ更新を実施します。

以上