# デジサート クラウド型 WAF サービス仕様書

2023 年 7 月版

販売元；

デジサート・ジャパン合同会社

サービス提供元；

株式会社 セキュアスカイ・テクノロジー

# 目次

# 1 はじめに

## 1.1. 本資料について

本資料はデジサート クラウド型 WAF（以下本サービス）のサービス仕様を説明するものです。

※本サービスは、サービス提供元である株式会社セキュアスカイ・テクノロジー（以下「SST 社」）のウェブアプリケーションファイアーウォール（以下 WAF）である Scutum を利用して提供されています。

## 1.2. 用語の説明

a. FQDN

ホスト名とドメイン名を省略せずにつなげて指定した記述形式のことです。

b. ブロック機能

不正と思われる通信を WAF にてブロックする機能。ブロックが行われると通信を実施しているクライアントのブラウザにブロック画面が表示されます。

c. モニタリング機能

疑わしい通信ではあるが、誤検知の可能性がある、もしくは攻撃だとしても危険性がそれほど高くない場合の通信を、ブロックせずに攻撃ログに残す機能。

モニタリング機能のログについては、サービス提供元の担当者が確認後にログを表示させる場合があるため、通信が発生したタイミングとログが表示されるタイミングとの間にずれが生じる場合があります。

d. 防御ロジック

WAF を通過する通信に対してブロック、モニタリングすることを決める基準となるルール。必要に応じて FQDN 毎にカスタマイズします。また新しい攻撃が発見された場合等に随時更新されます。

シグネチャだけではなく、複数のロジックを組み合わせ、ブロック、モニタリングを行います。

e. オリジンサーバ

WAF を導入する対象となる、お客様が運用しているウェブサーバ。

f. API 機能

API（Application Programming Interface）のうち、これを経由することにより、本サービスの特定の機能、情報にアクセスすることができます。

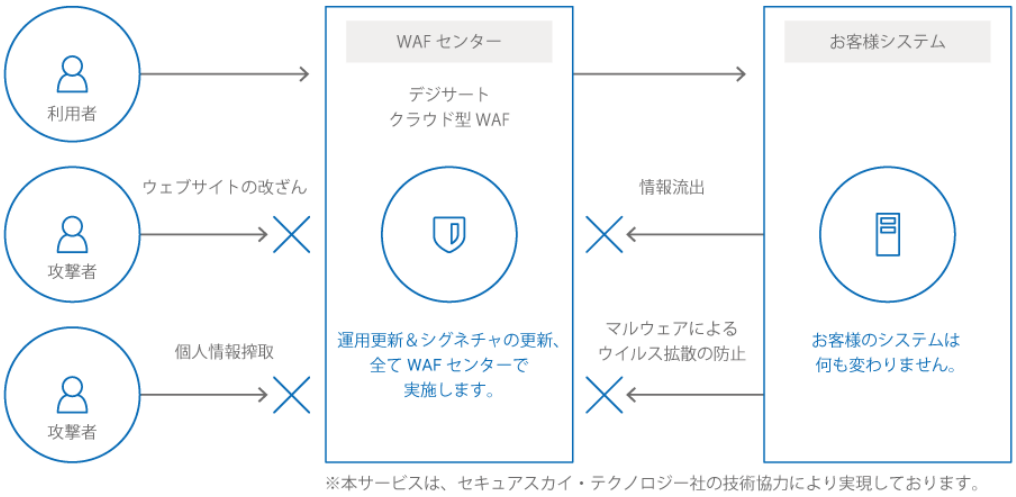
g. API キー

ユーザIDおよびパスワードによりログインした者に対して発行するアクセスキー、トークン等の認証情報であって、これを利用することにより、本サービスのAPI機能を利用することができます。

# 2 サービス概要

## 2.1. デジサート　クラウド型 WAF について

本サービスは、お客様のウェブサイトへのエンドユーザからの通信を、クラウド上で提供される WAF を経由させることにより、不正な通信を防御するサービスです。SST 社が管理するセンターを経由する形で WAF の機能を提供します。




**デジサート　クラウド型 WAF サービスイメージ**

# 3 ウェブアプリケーションファイアウォール機能

## 3.1. ブロック、モニタリング機能

本サービスを利用するウェブサイトに対して、あらかじめ登録されている不正な通信パターンを検出した場合、該当通信を遮断もしくは記録する機能（通信自体は遮断されません）。ブロック（もしくはモニタリング）する基準は本サービスで提供する防御ロジックとなります。この防御ロジックは定期的に更新されます。

※ブロック（もしくはモニタリング）する主な攻撃は下記となります。

| 区分 | 名称 |
|---|---|
| 認証 | 総当り<br>パスワードリスト攻撃 |
| クライアント側での攻撃 | クロスサイトスクリプティング<br>クロスサイトリクエストフォージェリ（導入時に調整が必要です。調整内容によっては有償となる場合があります。） |
| コマンド実行 | バッファオーバーフロー<br>OS コマンドインジェクション<br>SQL インジェクション<br>XPath インジェクション<br>書式文字列攻撃<br>LDAP インジェクション<br>SSI インジェクション |
| 情報公開 | ディレクトリインデクシング<br>情報漏えい<br>パストラバーサル<br>リソース位置を推測 |
| 特定ミドルウェア/フレームワーク等を狙った攻撃 | Apache Struts1＆2 の脆弱性を利用した攻撃<br>GNU bash の脆弱性を利用した攻撃(CVE-2014-6271)<br>SSL3.0 の脆弱性を利用した攻撃（CVE-2014-3566）<br>WordPress 4.7. 1 の REST API 脆弱性 |
| マルウェア対策 | ドライブバイダウンロード（ガンブラーによるメール拡散）攻撃 |
| プラットフォームへの攻撃 | プラットフォームの脆弱性をついた DoS 攻撃<br>（ApacheKiller、hashDoS など）<br>少数 IP アドレスからの DoS 攻撃<br>（大量正常通信、Slowloris、SYN flood 攻撃など） |

※ 防御ロジックの内容は非公開としております。

※ 上述の攻撃について、100%の防御を保証するものではありません。

## 3.2. ログ機能

ブロック、モニタリングされた通信をログとして保存する機能です。ログの内容はお客様管理画面にて提供されます。ログは一覧と詳細で提供されます。機密情報保護の観点から詳細ログについては一定期間後消去されます。

## 3.3. 特定 URL 除外機能

本サービスを利用するウェブサイト中の WAF 機能を利用したくない箇所を URL 単位で除外する事ができます。本機能はお客様管理画面にて提供されます。

## 3.4. IP アドレスの拒否／許可の設定機能

本サービスを利用するウェブサイトへの特定 IP アドレスからの通信を拒否することができます。ホワイトリスト、ブラックリストによる設定が可能です。本機能はお客様管理画面にて提供されます。

## 3.5. SSL/TLS 通信機能

本サービスでは SSL サーバ証明書にて暗号化されている通信についても防御することが可能です。本機能を利用する場合は SSL サーバ証明書がクラウド上にも必要になります。

SSL サーバ証明書はお客様管理画面から設定していただきます。（API 経由でも更新可能です。）

## 3.6. ウェブサーバの設定

お客様が運用しているウェブサーバの IP アドレスに変更があった場合、WAF の転送先を管理画面より変更できます。ウェブサーバやセンターの移行の際にお客様側で自由に WAF を設定変更することが可能です。

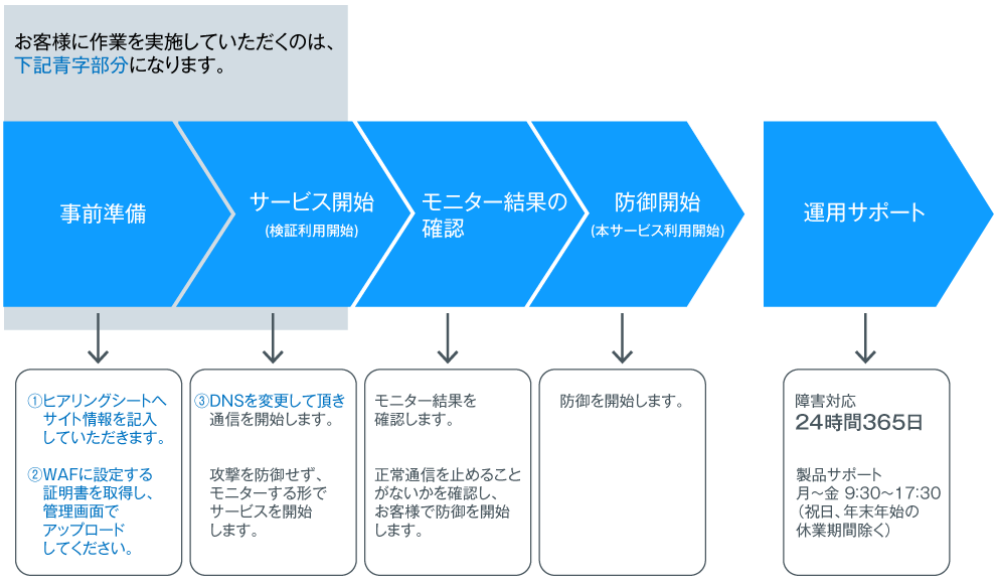
## 3.7. API 機能

お客様管理画面で利用できる機能の一部を API にて利用することができます。利用にあたってはお客様管理画面より、API キーを発行する必要があります。

# 4 運用管理機能

## 4.1. 初期設定及び導入作業

本サービスの初期設定及び導入は以下の流れとなります。




※ DNS 設定は CNAME による変更が必要になります。(A レコードでも変更が出来れば、WAF の利用は可能ですが、障害対応時などにお客様側での作業が必要となります。後述の「6.4 DNS の変更について」を併せてご参照ください。)

※ なお、DNS 設定の変更がいただけないお客様にはサービスの提供ができません。

## 4.2. お客様管理画面の提供

### 4.2.1. お客様管理画面とは

サービス利用者にお客様専用の管理画面(ウェブサイト)を提供します。WAF を利用されるサイト(FQDN)毎に管理アカウント(ユーザ ID) を提供します。

お客様管理画面の操作方法詳細に関しては以下の弊社ウェブサイト上に掲載する管理画面マニュアルを参照ください。

[デジサート クラウド型 WAF ポータル]

https://www.digicert.com/jp/waf/waf-portal

### 4.2.2. お客様管理画面にて提供する機能

| | |
|---|---|
| 1 | 防御ログの閲覧 |
| 2 | ログ統計機能（攻撃元 IP アドレス top5, 攻撃種別 top5、ダウンロード） |
| 3 | WAF 防御 on/off 機能 |
| 4 | IP アドレスの拒否/許可の設定 |
| 5 | 除外 URL の設定 |
| 6 | SSL サーバ証明書の更新 |
| 7 | SSL の設定 |
| 8 | 管理画面用パスワード変更 |
| 9 | メールアドレス変更 |
| 10 | ウェブサーバの設定 |
| 11 | API の設定 |

### 4.2.3. ユーザ ID・パスワード、メールアドレスの設定変更

お客様管理画面のユーザ ID・パスワードを弊社より発行致します。パスワード、連絡先メールアドレスはお客様自身で変更することが可能です。変更申請は、管理画面よりいつでも実施可能です。

## 4.3. 契約者設定情報の変更

契約者設定情報（以下「設定」）の変更が必要になった場合、お客様の申請に従い、設定変更を行います。

- 設定情報には、管理画面へアクセスを許可された担当者ウェブサイト自体の情報が管理されています。
- 変更申請はメールにて 24 時間 365 日受付けます。
- 設定変更申請は WAF の管理者として登録頂いた方からのみの受付となります。
- 設定変更実施希望日時をご指定される場合は、変更実施希望日の 7 営業日前までに申請ください。
- 申請受領後、受付連絡を実施し、内容を確認した後に申請受領連絡を行います。
- 受領連絡にてお伝えした実施日時で設定変更を行います。
- 設定変更後メールにて完了を連絡します。

## 4.4. 防御ロジックの更新

WAF は不正な通信を防御ロジックにて防御します。ウェブアプリケーションの脆弱性に対する主要な攻撃の多くをカバーしています。新たな脆弱性についても、随時防御ロジックを更新して対応します。誤検知等の確認は十分に行いますが、誤検知が発生しないことを保証するものではございません。

## 4.5. システム監視

サービス提供元の SST 社にてシステムの稼働状況を 24 時間 365 日監視いたします。万一障害が発生した場合の対応については、後述の「5 障害時の対応について」をご参照ください。

# 5 障害時の対応について

## 5.1. システム障害の基本方針

WAF は構成される機器や回線などを冗長化しているため、サービスが長時間利用できない状況は想定しておりません。ただし、想定外の事態が起こり、サービスが長時間利用できない状況が発生した場合は以下に説明する内容にて対応を実施します。

## 5.2. 障害の定義

WAF を利用しているウェブサイトにおいて、WAF の不具合に起因して Web サイトが複数回更新しても画面の表示に時間がかかる、もしくは正常な画面が表示されない場合を障害と定義します。

## 5.3. 障害時の対応

WAF システムに障害が発生し、一定時間以上回復が見込めない場合は、お客様にて DNS を変更することにより WAF を切り離し、Web サイトの通信を継続させることが可能です。

前項 5.2 の状態が継続する時間に合わせて以下の報告を行いますので、DNS 変更の実施についてはお客様にてご判断ください。

約 10 分経過時 ： サービスプロバイダにて障害速報を以下のウェブページに掲載します。

URL ： https://support.scutum.jp/ （サービス提供元である SST 社のサイト）

約 30 分経過時 ： 該当のお客様ウェブサイト(FQDN)ごとの連絡先メールアドレスに、障害が発生している旨をメールにて通知します。

※復旧の連絡については、安定稼働確認後、上記ウェブページへの更新情報の掲載、個別でのメールまたはお電話の、いずれかの方法で実施させていただきます。

## 5.4. 注意事項

WAF は、DNS を CNAME で設定していただくことを前提に障害対応を設計しています。

WAF では、冗長化している 2 系統のサーバに対して DNS ラウンドロビン(※)により通信しますが、片側でサーバダウン等の不具合が発生した場合、弊社にて不具合を検知してから約 5 分で正常稼働しているもう一方に通信を寄せる対応を行います。

ただし DNS が A レコードで設定されている場合には、上記の対応を行うことができないため DNS ラウンドロビンによる動作となり、表示に遅延等が発生する場合があります。このようなケースでは、片側の不具合発生検知から約 30 分経過時に通知を行いますので、DNS 変更の実施についてはお客様にてご判断ください(後述の「6.4 DNS の変更について」を併せてご参照ください)。

※　DNS ラウンドロビン

1つのドメイン名に複数の IP アドレスを割り当てる負荷分散技術です。ご利用のブラウザにより挙動は異なりますが、1つの IP アドレスで接続に失敗した場合、もう一方の IP アドレスに接続し直します。この際、ご利用ブラウザやサーバダウンの状態により挙動は異なり、接続できない、もしくは著しく遅延が発生する場合がございます。

# 6 お問合せ

## 6.1. お問合せ先

**デジサート　クラウド型 WAF　緊急お問い合わせ**（24 時間年中無休）

サービス開始後の WAF の障害等に関する緊急のご連絡は以下へご連絡ください。

電話：03-4578-1365　音声ガイダンス後に[2]を選択

**デジサート クラウド型WAF　サポート　月～金　9:30～17:30(祝日、年末年始の休業期間除く)**

サービスの利用等に関するご質問は、以下のメールアドレスまでご連絡ください。

E-mail：cloud_waf@digicert.com

【重要】サポートへのお問合せ時には、会社名・ご担当者様情報・ご契約 FQDN をご連絡ください。

# 別紙 サービスご導入にあたっての注意点(重要)

## (1) ソース元 IP の変更について

ソース元 IP アドレスが全て WAF サービスのものとなります。貴社サイトにて、ソース元 IP アドレスを使用している場合はご注意ください。

ソース元 IP 使用例

・アクセス解析

・ソース元 IP を利用した Web アプリケーションによる表示変更

・ソース元 IP を利用したロードバランシング 等

本来のソース元 IP アドレスは、HTTP ヘッダ内の「X-Forwarded-For」パラメータを通じて提供されます。

## (2) レスポンスの低下について

Hop 数が増えるため、レスポンスはわずかに低下いたしますが、影響が体感されないよう注意を払っています。しかし、環境により差が出る可能性もあるので、hosts ファイル経由の動作確認を推奨します。

特に、5～10MB 以上のデータのアップロード、ダウンロードがある場合、体感速度が遅延もしくはタイムアウトする可能性があります。そのような不具合が生じる場合、「これらのオペレーションのみ」が WAF を経由しない構成になるようご検討ください。

## (3) 使用できるプロトコルについて

WAF サービス経由の通信は、HTTP、HTTPS のみに対応しております。

同一サーバで FTP、SSH、SMTP 等をご使用されている場合、同一 FQDN での利用はできません。FTP サービス用に別のホスト名（ftp.example.com など）をご用意いただくか、接続の際に IP アドレスを直接設定ください。

なお、MX レコードと CNAME を同じサブドメインに指定できない為、WAF の DNS 変更は A レコードで実施して頂く形となります。

競合する MX レコードの例は、以下のようなものです。

メールアドレス：××@www.digicert.com

FQDN：www.digicert.com

## (4) DNS の変更について

弊社では、以下の理由から CNAME での変更を推奨しています。

・データセンターの移行などアクセスする IP を変更する可能性があるため

・万が一のデータセンター障害時等の際に、弊社側での DNS 変更が可能となるため
（前述の「5 障害時の対応について」を併せてご参照ください）

A レコードでの変更も可能ですが、その場合、上記の対応時にお客様側での作業が必要となります。

※御社 DNS の TTL の設定値により、サーバ切り替え時のコントロールが可能になります。なお、短い設定にすると DNS の切戻し時の即時性は上がりますが、サーバ負荷も上がるのでご注意ください。

## (5) F/W の設定について

WAF サービスを導入することにより、ソース元 IP アドレスが全て WAF サービスのものとなります。

オリジンサーバ側の F/W 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、その設定を解除してください。

## (6) F/W での制限について

オリジンサーバ側の F/W で WAF サービス以外からのアクセスを禁止することで、よりセキュアな環境が構築できます。F/W で制限をした場合、ドメイン名でなく IP アドレスにてアクセスを実施した場合についても防御が可能となります。

尚、万が一の WAF サービス側のデータセンター障害時に、お客様側で DNS を変更いただく場合は、同時にこの F/W の制限を元に戻していただく必要がございますのでご注意ください。

## (7) SSL 通信をご利用の場合について

本サービスでは、暗号化された通信を WAF サービス内で復号し、通信内容を確認し、その後、再度暗号化しお客様 Web サーバへ送信する形になりますので、SSL サーバ証明書のライセンスが追加で必要になります。

WAF は冗長構成で複数のシステムを利用していますので、FQDN あたり 2 ライセンスのご利用をお願いしています。

## (8) 正常通信の誤検知について

WAF サービスは、正常通信の誤検知が発生しないように作られていますが、絶対に誤検知が発生しないことを保証するものではありません。

ただ、SQL インジェクション等の攻撃については、SQL 文が実際に構文として成立しているかどうかもチェックする上、防御ロジックの作成は日本で行っていますのでダブルバイトでの不要な誤検知が発生することはありません。

なお、新たな防御ロジックの追加時やサービスの開始時には、ブロックはせず、ログだけをとる形でスタートし、正常通信を確認した上でサービスを開始します。

### (9) 保護対象サイトが DDoS 攻撃を受けた場合について

WAF サービスでは大量の DDoS 攻撃を受けた場合、サービス停止の恐れがあります。その際には他のサービス利用者への影響を抑えることを想定して、攻撃対象サイトを退避環境に一時的に移行します。このための設定情報は、サービスご契約時の一連のご案内に含みます。