



運用の手間なく 脅威からWebサイトを守る
クラウド型WAFセキュリティサービス



secuWAFとは

外部からのウィルスや脆弱性を突いた攻撃を遮断し、様々な脅威からWebサイトを守る

クラウド型WAFセキュリティサービス（WAF）です。

- ✓ クラウドサービスであるためお客様の手間を煩わせることなく、十分なWebサイトの防御が可能となります。
- ✓ 直感的なUIによるモニタリングやレポートが可能なことはもちろん、個別のカスタマイズ設定が可能なユーザーインターフェースも提供し、ユーザー個別のご要望にも対応が可能です。
- ✓ SOC側でお客様の防御状況をチェックし、個別の設定チューニングを行うサービスや防御対象サイトに定期的にアクセスしてWebサイトのマルウェア感染の有無を診断する機能も提供しております。





2つの機能と1つのサービスで 強固なWebサイトセキュリティを実現



Cloud WAF機能 <被害者にならないための対策>

WAF機能を活用し、Webサイトにおけるセキュリティリスクの最小化とパフォーマンスを向上させる。



マルウェアチェッカー機能 <加害者にならないための対策>

Webサイトを定期巡回。
未知の不正・脅威にも検知・分析をし、対処につなげる。



Webアプリケーション診断サービス

定期的な健康診断として、自社サイトの潜在的な脆弱性を把握。
自社サイトの本質的なセキュリティ強度の強化につなげる。

Webアプリケーションに潜む危険性

誰でもアクセス可能なWebアプリケーション

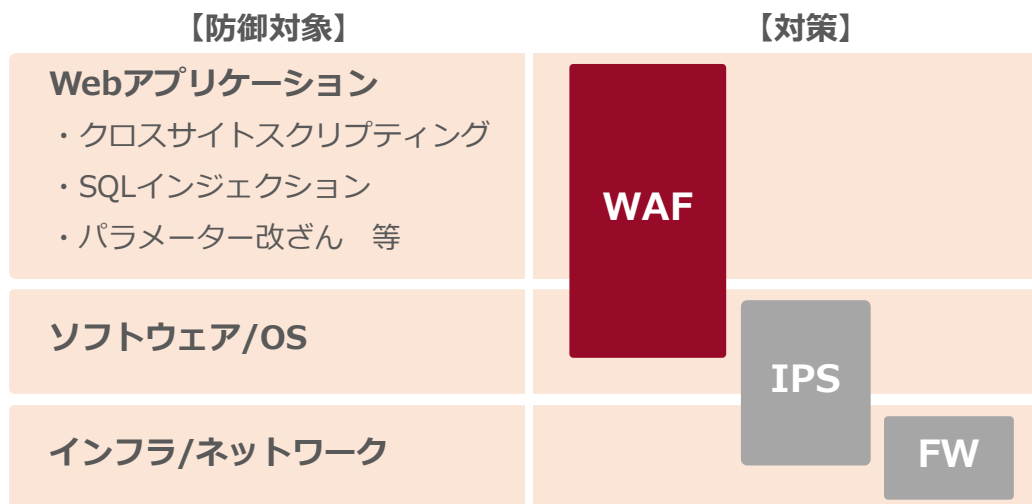
一般に公開されているWebアプリケーションなので、正規ユーザーと攻撃者を区別してアクセスさせることが難しい。

無くならないWebアプリケーションの脆弱性

コスト的・時間的な制約でセキュアプログラミングにも限界があり、
人の手で作られている以上は脆弱性は無くすることがほぼ不可能。（=人が自ら脆弱性を作り出しているとも言える状況）

これまでの一般的な対応策、FW・IPSをすり抜ける

SQLインジェクション／クロスサイトスクリプティングといった攻撃は、コードを分かりにくい形に変換した「難読化攻撃」とされており、FWのように、IPアドレスやポートの確認だけでは、検知できません。
また、IPS/IDSにおいては難読化されている攻撃に対する検知精度は低いと言われています。



クラウド型WAFの特徴

～“安価”で“手軽”に、“技術者不在”でもセキュリティ強化～

	クラウド型WAF (secuWAF)	アプライアンスWAF
	安価	高額
費用	機器の購入や複雑な初期設定が不要で、利用ボリュームによる月額15,000円～の料金プランなのでお手軽に利用することが可能。	機器購入・設計・構築等、高額な初期費用が発生。実際の運用後も保守費用や設定変更費用等のメンテナンス費用が必要。
	非常に手軽	手間が大きい
導入の時間	基本的にDNS設定を切替えていただくだけの簡単な作業で利用でき、申込みから数日で利用が可能。	サイトに合わせた細かいパラメーター設定やチューニングを実施していくのが一般的で運用に入るまで数か月掛かることもある。
	ほぼゼロ	手間が大きい
運用の時間	WAFの設定変更や新しい攻撃に対してのシグネチャの作成等は当社にて実施し、レポートも自動作成するためお客様に対応いただく作業はほぼありません。	受ける攻撃手法により設定変更が必要だったり、カスタムシグネチャを作る必要が出てくる場合もあり、レポートも自ら設定・作成する必要も出てくる。
	不要 (存在しているに越したことはないですが)	必要
セキュリティ技術者	保護対象Webアプリケーションのシステム構成とWAF機能の双方に精通した技術者が必要。	保護対象Webアプリケーションのシステム構成とWAF機能の双方に精通した技術者が必要。
	低い (一般的なサービスは共通設定で利用)	高い
自由度	クラウドサービス全体もしくは契約単位で統一の設定が一般的。ただし、 secuWAFは個別の設定が可能 です。	こういったことが出来るかは製品次第だが、個別の設定が可能。ただし、技術者のスキルにも依存する。

自動アップデートされる 強力なセキュリティ機能

自動アップデートされた最新のセキュリティ機能で様々な攻撃を防ぎ、新たな脅威を検出して早期対策を行うことが可能です。中には他のクラウドWAFサービスでは防げない攻撃も防御が可能です。



Webアプリケーション診断で 強度なセキュリティを継続支援

標準でWebアプリケーション診断（簡易診断）のチケットがついています。ページ数限定の簡易診断ではありますが、日々PCIDSSガイドラインに準じたWebアプリケーション診断を実施している専門エンジニアが診断を行います。



サイト入れ放題で 高い費用対効果を実現

どのプランもプラン内で定めたトラフィック内であれば保護対象とするWebサイトが入れ放題です。1契約で多くのシステムを一括防御が可能なため、費用対効果の高い対策が可能となります。



クラウドベースなのに 柔軟な個別設定

お客様自身での簡易設定のほか、SOC側による詳細設定も個別提供が可能です。入れ放題で導入した各Webサイト毎にも個別の設定が可能なため、アプリケーション製品に近い運用も可能となります。

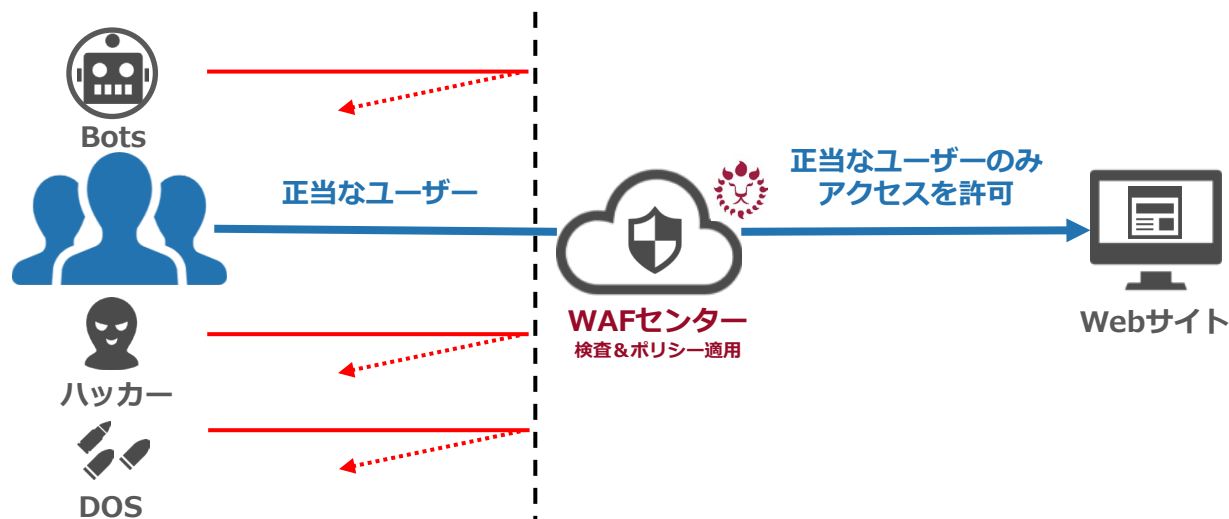


他サービスと比べた優位性

	secuWAF	他の一般的なクラウドWAFサービス	
独自ポリシー設定	○	△	クラウドサービス全体での共通設定で防御をしており、独自ポリシーの設定がNGなサービスがあるのに対し、secuWAFは独自ポリシーの設定が可能で、尚且つ、多くの設定をユーザー自身で行うことができます。
個別ポリシーの適用	○	×	secuWAFの場合はサイト入れ放題であっても、それぞれのサイトに対しての個別のポリシー設定が可能。それに対し、他のサービスは入れ放題プランで個別設定が可能であってもそれぞれのサイト個々の設定は不可で、全体に適用されます。
無料SSL証明書付与	○	△	secuWAFにて無料SSL証明書を発行してご利用いただけます。
http→https変換	○	×	対象サイト内のHTMLにhttpのリンクをhttpsに自動的に変換する機能を持っており、httpとhttpsとが混在するコンテンツをブロックするブラウザをご利用の場合の影響を回避します。
IPホワイトリスト	○	△	secuWAFではユーザー自身で除外IPの設定等が可能です。他サービスはその設定自体が不可であったり、依頼ベースでの対応となっています。
IPブラックリスト	○	×	ホワイトリスト登録はできても、ブラックリスト登録はNGなサービスが多い中、secuWAFはブラックリスト登録もユーザー自身で設定可能です。
URLホワイトリスト	○	△	secuWAFではユーザー自身で設定等が可能です。他サービスはその設定自体が不可であったり、依頼ベースでの対応となります。
シグネチャカスタマイズ	○	△	特定のプランのみでの対応をしている他サービスがある中、secuWAFは基本的に全プランで対応をしています。
レポート生成期間カスタマイズ	○	△	他のサービスでは決まった期間のみでのレポートが作成されるが、secuWAFでは期間指定をしたレポート生成が可能です。
WAF冗長構成	○	△	WAFシステムの事態の構成について、シングル構成であったり、オプションで冗長構成を提供しているサービスが多い中、secuWAFはオートスケーリング機能を実装したデフォルトで高負荷対策がされたサービスです。
Webサイト自体へのマルウェア感染検知	○	×	他サービスではWAF機能しか有していなかったり、他サービスとの組み合わせで提供しているが、secuWAFにおいては内部にMALWARE CHECKER機能を有しています（プランによっては標準提供）。
Webサイト自体のWebアプリケーション診断	○	×	一般的に他のクラウドサービスでは提供していないが、メイン事業の1つとして診断業務を提供しているためsecuWAFにおいては簡易診断を提供しています。

Cloud WAF の主な機能①

強力なセキュリティ

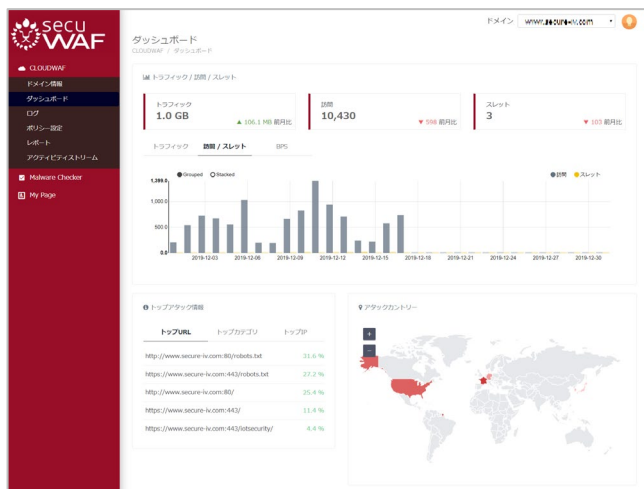


最も脅威的なOWASPトップ10の脆弱性を突いた攻撃だけでなく、
その他の攻撃からもWebサイトを強固に防御します。

- | | | |
|------------------|----------------------|-----------------|
| - SQLインジェクション | - ディレクトリアクセス検知 | - HTTPメソッド制限検知 |
| - XSS | - ヘッダ脆弱性 | - HTTP異常リクエスト検知 |
| - CSRF検知 | - 悪意のあるファイルアップロード検知 | - ディレクトリリスティング |
| - アプリケーション脆弱性検知 | - スキャナ/プロキシ/スパムボット検知 | - エラーページクローキング |
| - コマンドインジェクション検知 | - システムファイルアクセス検知 | - LDAPインジェクション |
| - 脆弱なページアクセス検知 | - Webサーバー脆弱性検知 | |

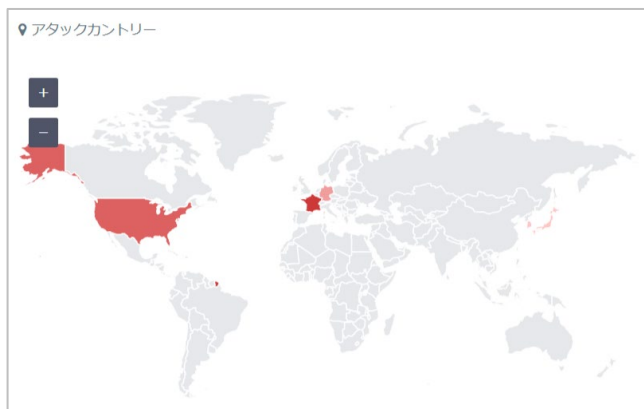
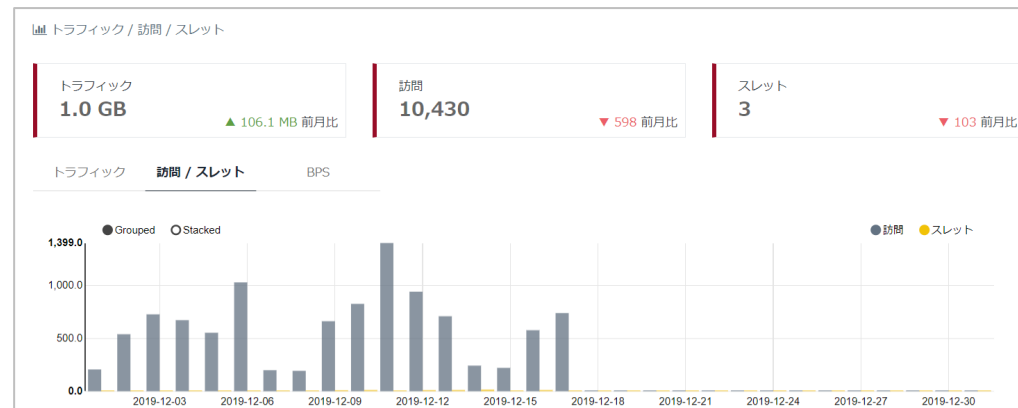
Cloud WAF の主な機能②

ダッシュボード



サマリー

脅威の数やトラフィックスループット等を視覚的に表示。



アタックカントリー

攻撃の多い国を表示。
必要に応じて国単位で通信をブロック。

トップアタック情報		
トップURL	トップカテゴリ	トップIP
http://www.secure-innovation.com/robots.txt		31.6 %
https://www.secure-innovation.com/443/robots.txt		27.2 %
http://www.secure-innovation.com:80/		25.4 %
https://www.secure-innovation.com/443/		11.4 %
https://www.secure-innovation.com/443/iotsecurity/		4.4 %

トップアタック情報

特に攻撃を受けるURLや
攻撃カテゴリーを表示。

Cloud WAF の主な機能③

セキュリティ攻撃種別

期間別の攻撃ログを検索・表示

00:00 23:59
June-29 June-30 July-01 July-02 July-03 July-04 July-05

ドメイン X-Forwarded-For IP パス 国・地域 (XFF) クライアント IP 攻撃種別 処置 検索

10 / page Excel ダウンロード

セキュリティ攻撃種別リスト

時間	クライアント IP	X-Forwarded-For	ドメイン	パス	タイプ	攻撃種別	処置
2024-07-05 09:41:15	208.100.26.247	(?) -	test.secure-iv.co.jp	/	Webセキュリティ	エラーページクローキング	遮断
2024-07-05 09:36:01	88.99.213.242	(?) -	test.secure-iv.co.jp	/	Webセキュリティ	エラーページクローキング	遮断
2024-07-05 09:05:07	157.90.7.190	(?) -	test.secure-iv.co.jp	/	Webセキュリティ	エラーページクローキング	遮断
2024-07-05 08:36:00	138.201.36.136	(?) -	test.secure-iv.co.jp	/	Webセキュリティ	エラーページクローキング	遮断
2024-07-05 07:38:16	51.222.253.20	(?) -	www.secure-iv.com	/robots.txt	Webセキュリティ	スキャナ/プロキシ検知	遮断
2024-07-05 06:33:17	192.99.15.34	(?) -	www.secure-iv.co.jp	/blog/583	Webセキュリティ	スキャナ/プロキシ検知	遮断

ログ詳細

検出されたログの詳細を表示。
攻撃の特定に活かすことが可能。

タイプ	攻撃種別	処置
Webセキュリティ	エラーページクローキング	遮断

ログ詳細ビュー

検出 時間 2019-11-11 11:11:11

国・地域 フランス

クライアント IP 5.1.1.1 : 17726

サーバー IP 5.1.1.1 : 443

検出 パターン スキャナ/プロキシ/スパムボット検出

検出 理由 AhrefsBot

リクエスト URL https://www.ahrefs.com/

リクエスト

```
GET /iotsecurity/ HTTP/1.1
Host: www.ahrefs.com
User-Agent: Mozilla/5.0 (compatible; AhrefsBot/6.1; +http://ahrefs.com/robot/)
Accept: */*
Accept-Encoding: deflate, gzip, br
```

リクエストデータ 長 184 byte

OK

Cloud WAF の主な機能④

ポリシー設定

個別設定

サイトごとに個別でポリシー設定が可能。

- ・ 防御項目の遮断/検知/OFF
- ・ 検出条件等の詳細内容（一部の項目）

test.secure-iv.co.jp

Webセキュリティ > セキュリティ

📌 セキュリティ 設定

» 詳細設定

SQLインジェクション

データベース(DB)と連動したウェブアプリケーションで攻撃者が入力フォームおよびURL入力欄にSQL文を挿入してDBから情報を閲覧(または操作)できる弱点

Off 検知 遮断

XSS

ページに悪意的なスクリプトを含めてウェブページを閲覧する接続者の権限で不適切なスクリプトが実行され、情報流出などの攻撃を誘発しかなない弱点

Off 検知 遮断

CSRF検知

外部入力動的ウェブページ生成に使用される場合、送信された動的ウェブページを閲覧する接続者の権限で不適切なスクリプトが実行される弱点

Off 検知 遮断

アプリケーション脆弱性検知

ウェブサーバー構築時、金銭的、時間的な負担により公開アプリケーションを多く利用しており、インターネットに公開された公開アプリケーションの各種脆弱性情報によりホームページ変造およびハッキング経路地として使用できる脆弱性

Off 検知 遮断

コマンドインジェクション検知

適切な検証手続きを経っていないユーザ入力値がオペレーティングシステムコマンドの一部または全部で構成され実行される場合、意図しないシステムコマンドが実行される弱点

Off 検知 遮断

個別ページアクセス検知	ウェブサイトの下位に内部文書やバックアップファイル、ログファイル、圧縮ファイルのようなファイルが存在する場合、ファイル名を暗号化してファイル名を採出し出し、直接アクセスしてハッキングに必要なサービス情報を取得したり、管理ページがインフラネットワークを通じてアクセス可能な場合、攻撃者のメタデータとなり、攻撃者のSQLインジェクション、Brute-Force攻撃など様々な形態の攻撃の口実を提供する脆弱性	Off	検知	遮断
ディレクトリアクセス検知	外部入力値に対して経路操作に使用できる文字をフィルタリングしないと、予期外のアクセス範囲領域に対する経路文字列構成が可能となり、システム情報漏洩、サービス障害などを誘発させる脆弱性	Off	検知	遮断
ヘッダ脆弱性	User-Agent、Rangeヘッダなどヘッダ情報操作を通じてウェブアプリケーションサーバーやOSシステム内に存在する知られていない脆弱性にアクセスし、遠隔命令実行やバッファオーバーフローを誘発する脆弱性	Off	検知	遮断
悪意のあるファイルアップロード検知	サーバー側で実行できるスクリプトファイル(asp,phpファイルなど)がアップロード可能で、このファイルを攻撃者がウェブを通じて直接実行させることができる場合、システム制御命令を実行したり外部と連携してシステムを制御できる脆弱性	Off	検知	遮断
スキャナ/プロキシ/スパムロボット検知	クロリング、スクラップ、スキャナー、ウェブ攻撃ツールキットなど多様なツールを適用し、機密的な攻撃トワックを発生させて直接的な損点を発生したり、脆弱性を把握するための脆弱性情報を収集する行為	Off	検知	遮断

システムファイルアクセス検知	知られていない位置のウィンドウズ、ユニックスウェブサーバーのシステムファイルと脆弱なPHPサーバーの脆弱なファイルやオブジェクトに脆弱なアクセスし、漏出したシステム脆弱情報や脆弱性情報を攻撃者に必要な脆弱情報として活用する脆弱性	Off	検知	遮断
Webサーバー脆弱性検知	アプリケーション(Apacheなど)のインストール中に生成されるインストールファイルや脆弱なファイルが存在したり、ウェブ上でWindowsログインウィンドウが露出するなど、システム上の設定不備によって発生する脆弱性	Off	検知	遮断
HTTPメソッド制御検知	ウェブサービス提供時に不要なMethod(PUT、DELETE、OPTIONSなど)許可により攻撃者によって脆弱なファイルをアップロードしたり脆弱な脆弱性ファイルの脆弱性になる脆弱性	Off	検知	遮断
HTTP異常リクエスト検知	セキュリティシステムは定期的で、多量な空白、多量な接続、空行文字、ノル文字挿入、HTTP異常リクエスト検知または異常な接続と検出規則に反する形状のトラフィックで検知してウェブサーバーに到達する攻撃的攻撃	Off	検知	遮断
ディレクトリリスティング	サーバー内のすべてのディレクトリまたは重要な情報が含まれたディレクトリに対してディレクトリスティングが可能な脆弱性、脆弱な脆弱性情報	Off	検知	遮断
エラーページクロッキング	ウェブサーバーに到達したエラーページを指定していない場合、エラーメッセージを通じてサーバーデータ情報と攻撃に必要な脆弱性が露出する脆弱性	Off	検知	遮断
LDAPインジェクション	LDAP (ディレクトリサービス)を統合・修正するアプリケーション(クエリー)を操作したクエリーを入力したりすることによって(スクリプト、個人情報などが露出する脆弱性、ウェブサイトでユーザ入力値がLDAPクエリーが実行される場合、LDAP脆弱性を悪用してシステムを攻撃する脆弱性	Off	検知	遮断

Cloud WAF の主な機能⑤

アクセス制御ルール

パス、パイパスURL、メソッド、クライアントIP、国・地域別の遮断設定ルールを追加可能

パス	test.secure-iv.co.jp/	
パイパス URL	ex) /path/example/1	追加
遮断 メソッド	遮断 メソッド一覧 === 一括削除 ===	メソッド一覧 === 一括選択 === GET POST PURGE PUT HEAD OPTIONS DELETE
クライアント IP	☒ バイパス ☐ 遮断	ex) 211.190.23.23 or 211.190.23.1-211.190.23.255
遮断 国・地域	アクセス制限対象 === 一括削除 ===	国リスト === 一括選択 === Afghanistan Aland Islands Albania Algeria American Samoa Andorra Angola

遮断ページをHTMLで編集可能であるため、お客様側で任意に表示内容を変更可能です。

Browsing Blocked



Your request / response has been blocked by a web firewall policy.

Fri Jul 05 2024 10:29:50 GMT+0900 (日本標準時)

Cloud WAF の主な機能⑦

その他機能

- ・ 他ドメインヘルールの同期が可能。
- ・ 月別レポート自動生成&メール送信が可能

test.secure-iv.co.jp のセキュリティルールを同期します。		同期する
セキュリティルール同期化	対象ルール	☐ アクセス制御 ☐ APIセキュリティ ☐ Webセキュリティ ☐ Bot 管理
	ドメインリスト	☐ www.secure-iv.com ☐ portal.secure-iv.com ☐ www.test.secure-iv.co.jp ☐ www.secure-iv.co.jp ☐ www.secuwaf.jp
セキュリティルールの初期化	設定されているセキュリティルールを最初の設定状態に戻します。	
		初期化する
月別レポート自動生成	毎月1日に先月のレポートを自動的に作成します。	On Off
レポートメール送信	自動的に作成された月次レポートを設定したメールアドレスへ転送します。	
	受取人	Email 追加
	全体 : 1 カウント	higa-yuk@secure-iv.com

Cloud WAF の主な機能⑧

レポート

レポート生成

期間を指定してレポート生成（Word & PDF）が可能。

月別レポート自動生成

期間 2019-12-17 - 2019-12-17 作成

レポートリスト

作成 時間	期間	ファイル名	ダウンロード	削除
2019-12-17 18:05:28	2019-11-18 ~ 2019-12-17	SECUWAF_Report_20191217180528	 	削除

1 to 1 of 1 reports

SECUWAF ウェブセキュリティレポート

ユーザーID	サービス	タイプ	ドメイン	期間
	Web Application Firewall / Free			2019-11-18 ~ 2019-12-17

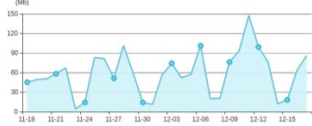
下記のテーブルとチャートは、www.secure-iv.comで生成されたログデータです。このデータを分析することで、脆弱サイトをより効率的かつ安全に運営することができます。

で作成された 2019-12-17 18:05:28

期間合計の概要		
トラフィック	訪問	攻撃
1,062B	10,460	170

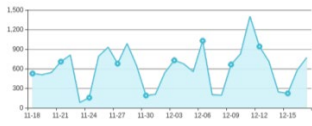
トラフィック

2019-11-18 から 2019-12-17までの合計 1,062B のトラフィックが発生しました。



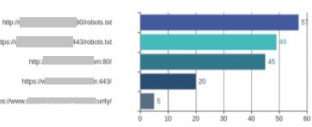
トランザクション(訪問)

2019-11-18 から 2019-12-17までの合計 10,460 回のトランザクション(訪問)が発生しました。



攻撃(バス)

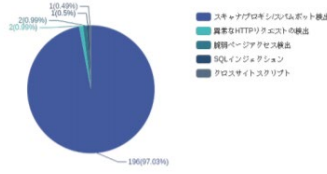
http://www.robots.txt バスで最も多くの攻撃の読みが検出されました。



攻撃(カテゴリ)

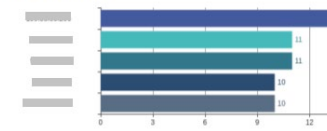
最も顕著な攻撃: スキャン/プロキシ/スパムボット検出

(タコール、ステレピング、スキャン、ウェブ攻撃ツールキットなどの種々な道具を活用して総合的な攻撃トラフィックを発生させて直接的に脆弱性を見つけるしたり、脆弱性を把握するために間接的な情報を収集する行為)



攻撃(攻撃者 IP)

IPアドレス 193.58.86.206から最も多くの攻撃の読みが検出されました。 疑わしいIPアドレスを見つけたら、そのIPアドレスをブロックすることをお勧めします。



MALWARE CHECKER の主な機能①

Webサイトへのマルウェア感染を検出



加害者になってしまわぬようWebサイトを定期巡回し、独自のマルウェア解析技術によりWebサイトがマルウェアに感染していないか検査をし、アラート通知をします。



1. パターンベース分析



2. 不審なイベントの発見



3. マルウェアの検出



4. 悪意のあるURL・コード抽出



5. マルウェア発生源の分析

MALWARE CHECKER の主な機能②

個別の巡回設定

http://

☐ **HTTP 認証**
HTTP認証が必要な場合は、このオプションを有効にして設定してください。

☐ **User Agent**
任意のUser Agent設定が必要な場合は、このオプションを有効にして設定してください。

自動診断周期
☐ 無し ☒ 1日 ☐ 1週間 ☐ 1か月

サイトマップ 再作成
☒ None ☐ 再作成

診断レベル
☒ Quick ☐ Normal ☐ Deep

クローリング深度
☒ 1 depth ☐ 2 depth ☐ 3 depth ☐ 4 depth ☐ 5 depth

サイト管理

定期巡回の頻度や階層のほか、
アラーム通知先等の個別設定が可能。

外部リンク
☒ 無効 ☐ 有効

例外 Regex 設定
Regex Value

アラーム設定
☐ 無し ☒ 電子メール

メール入力

☒ **アラーム**

電子メール

.com

MALWARE CHECKER の主な機能③

ダッシュボード

チェックしたURLの数や検出された脅威等のサマリーを表示



MALWARE CHECKER の主な機能④

診断ステータス

📄 診断結果

日付	URL	スレット	悪意のあるページ	すべてのURL	レポート
2019-12-18 10:50:04	http://cms.nahaken-okn.ed.jp/	0	0	7959	表示 ファイル 作成

1 to 1 of 1 entries

診断したそれぞれのURLや
レスポンス内容などの診断結果を表示

分析時間

分析スタート 2019-12-18 10:50:09

分析完了 2019-12-18 10:56:57

リクエスト/レスポンス

☐ スレットのみを見る

cms.nahaken-okn.ed.jp (101.102.227.73:80)

URI	レスポンスタイプ	レスポンスコード	URLカテゴリ	レスポンス長さ	時間
/?action=common_downlo...	text/html	200	unknown	1912	2019-12-18 10:55:53
/index.php?action=cabinet...	text/html	200	unknown	3757	2019-12-18 10:55:51
/index.php?action=cabinet...	text/html	200	unknown	114	2019-12-18 10:55:51
/index.php?action=cabinet...	text/html	200	unknown	977	2019-12-18 10:55:51
/index.php?action=cabinet...	text/html	200	unknown	114	2019-12-18 10:55:58
/index.php?action=cabinet...	text/html	200	unknown	2746	2019-12-18 10:55:58
/index.php?action=cabinet...	text/html	200	unknown	114	2019-12-18 10:55:58
/index.php?action=cabinet...	text/html	200	unknown	1363	2019-12-18 10:55:58
/index.php?action=cabinet...	text/html	200	unknown	114	2019-12-18 10:55:58
/index.php?action=commo...	text/css	200	unknown	6934	2019-12-18 10:55:58

First Prev **1** 2 3 4 5 6 7 Next Last

スレット情報

No.	プロトコル	アプリケーションプロトコル	カテゴリ	URI レピュテーション	時間
スレット検知情報なし					

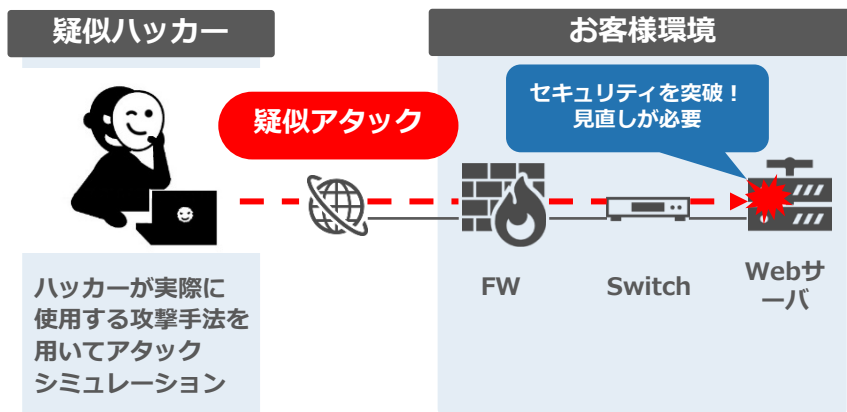
✓ OK

簡易Webアプリケーション診断 サービスの内容

簡易Webアプリケーション診断

Topページの脆弱性診断で、修正すべきところが丸わかり

お客様環境に対してリモート接続をして、疑似アタックを実施し、脆弱性の有無とその危険性レベルをチェック！

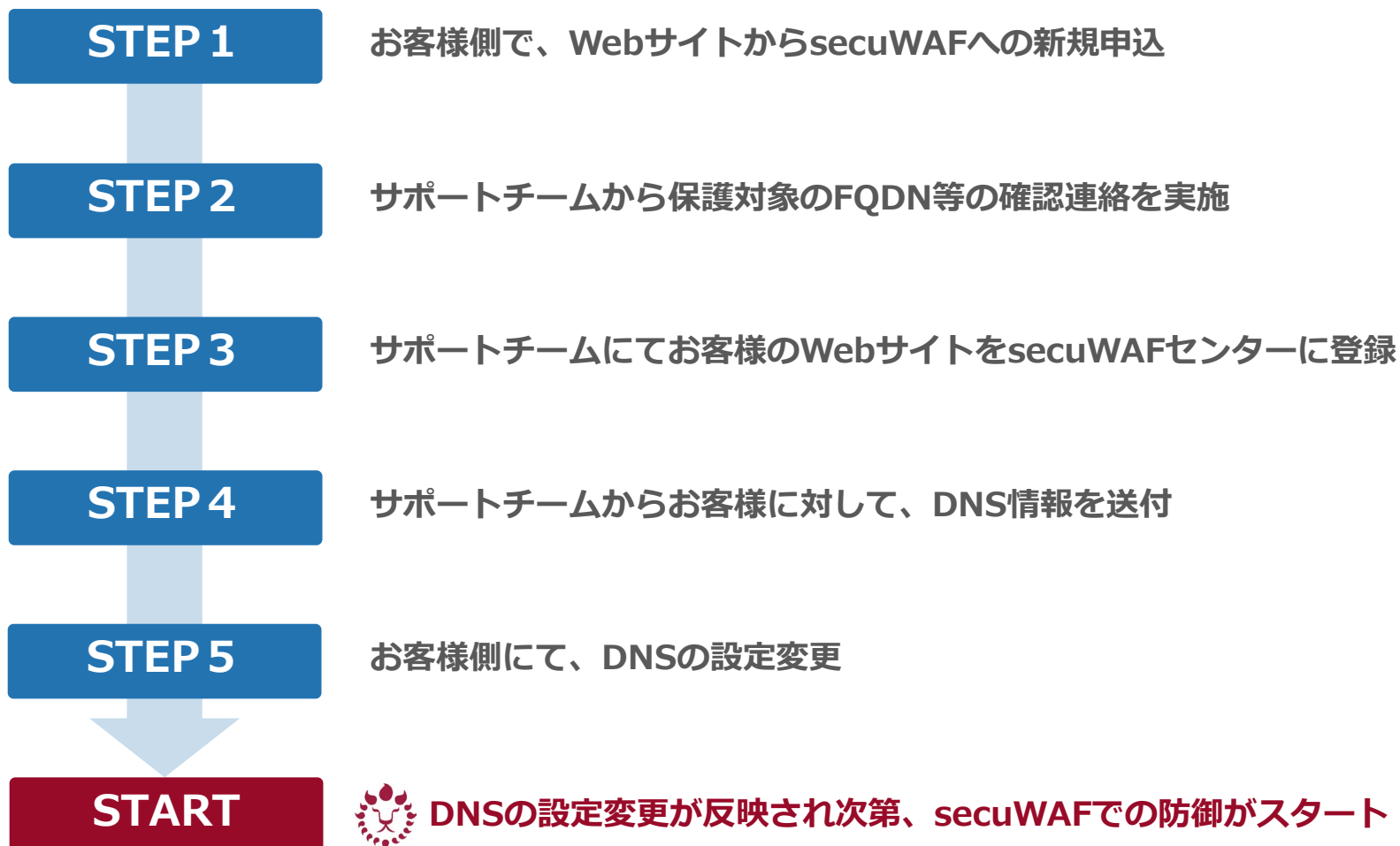


※簡易サービスのため、Topページのみとしております。
※プラットフォーム診断は、含んでおりません。

主な診断項目

SQLインジェクション
OSコマンドインジェクション
パラメータ操作による脆弱性
クロスサイトスクリプティング
セキュア属性の無いCookie
不要なエラーコードの表示
バッファオーバーフロー
クロスサイトリクエストフォージェリ
セッション管理に関する問題
プロトコルの不適切な適用
不要なエラーメッセージの表示
HTML5のクロスオリジン設定に関する問題
HTML5のレスポンスヘッダに関する問題
Sandbox属性の無いインラインフレーム
Webサーバ設定ミスによるサーバ情報、アプリ情報の漏えい
Webサーバのディレクトリやファイルの不適切な公開設定
Webサーバの既知の脆弱性

導入の流れ



お客様環境に手を加えることなく、簡単に導入可能

サービスプラン

どちらのプランもサイト入れ放題！複数サイトを一括して防御したい際は特に高いコストパフォーマンスを発揮します。

トラフィック総流量プラン(税抜き)

無償トライアル	10GBプラン	20GBプラン	50GBプラン	100GBプラン
5 GBまで	10 GBまで	20 GBまで	50 GBまで	100 GBまで
初期： ¥0 月額： ¥0 ・最長30日間	初期： ¥0 月額： ¥10,000 ・独自ポリシー設定可 ・CDN機能	初期： ¥0 月額： ¥15,000 ・独自ポリシー設定可 ・CDN機能 ・簡易診断	初期： ¥0 月額： ¥30,000 ・独自ポリシー設定可 ・CDN機能 ・簡易診断 ・MALWARE CHECKER	初期： ¥0 月額： ¥45,000 ・独自ポリシー設定可 ・CDN機能 ・簡易診断 ・MALWARE CHECKER

超過従量課金：基本プランの超過利用分に応じて料金が追加される設定も可能です（要事前申込）

従量課金	10GBプラン	20GBプラン	50GBプラン	100GBプラン
価格 / 1GB	800円	750円	600円	450円

帯域保証プラン(税抜き)

10Mbpsプラン	50Mbpsプラン	100Mbpsプラン	200Mbpsプラン	300Mbpsプラン
10 Mbpsまで	50 Mbpsまで	100 Mbpsまで	200 Mbpsまで	300 Mbpsまで
初期： ¥100,000 月額： ¥88,000 ・独自ポリシー設定可 ・簡易診断	初期： ¥100,000 月額： ¥125,000 ・独自ポリシー設定可 ・簡易診断	初期： ¥150,000 月額： ¥170,000 ・独自ポリシー設定可 ・簡易診断	初期： ¥150,000 月額： ¥265,000 ・独自ポリシー設定可 ・簡易診断	初期： ¥150,000 月額： ¥333,000 ・独自ポリシー設定可 ・簡易診断

※MALWARE CHECKERについては、オプションとして個別にご利用が可能です。

1FQDN、月当たり8,000円となります。トラフィック総流量プランでは、50GBより標準付帯サービスとなっております。

※標準付帯されているMALWARE CHECKERは1FQDN分のみですので、必要に応じて追加でお申し込みください。

※最低利用期間は6ヶ月間となりますが、別メニューとしてのご用意も可能ですので、ご相談ください。

【参考】FAQ①

Question		Answer	
Q1.	保護対象であるWebサイトのサーバがダウンした場合の挙動はどうなるか？	A1.	CLOUD WAF側の機能としてWebサーバダウン時にバランシングしたり、転送したりする機能は有しておりません。そのため、実際のWEBページは、「このウェブページにアクセスできません」等のWEBブラウザ固有のエラー画面が表示されます。
Q2.	WAF側に、ロードバランサのIPを設定することは可能でしょうか	A2.	WAFにロードバランサのIPを設定するのは可能です。
Q3.	MALWARE CHECKERのみの利用は可能でしょうか？	A3.	MALWARE CHECKERのみの利用も可能です。
Q4.	MALWARE CHECKERを並行して動かすことは可能でしょうか？	A4.	1 アカウントで複数サイトを登録した際は検査を同時並行して実行することはできません。指定の時間に他の検査が実行されている場合は前の検査が終わるまで開始を待ちます。
Q5.	secuWAFはGoogleアナリティクスに影響がありますか？	A5.	Google アナリティクスのようなブラウザ側でスクリプトを動かしてログを収集するものの場合は、影響ありませんが、念のため事前にお試しいただくことを推奨いたします。
Q6.	secuWAFはクラウド環境でも使用可能でしょうか？	A6.	secuWAFは、ウェブサーバーの種類（クラウドまたはオンプレミス）に関係なく使用できます。
Q7.	サポートしているプロトコルを教えてください。	A7.	secuWAFはウェブプロトコル（http / https)のみをサポートしています
Q8.	容量課金プランの場合、トラフィックのカウンターの考え方を教えてください。	A8.	保護対象Webサイトへ接続するインバウンドとアウトバウンドのそれぞれの通信（HTTP / HTTPS）トラフィックの合計です。 現在のトラフィック量についてはユーザー画面のダッシュボードから確認できます。
Q9.	容量課金プランの場合、プラン内のトラフィックを 使い切りそう な場合はどうなりますか？	A9.	プラン内のトラフィックの使用状況が80%程度になった場合にサポート部門より通知メールを送付し、上位プランへの検討をご案内しております。
Q10.	容量課金プランの場合、プラン内のトラフィックを 使い切った 場合はどうなりますか？	A10.	ご契約プランのトラフィック量を超えた場合は、自動バイパスするモードに変わり、WAFセンターを介さない通常アクセス（WAF導入前の状態）に戻るだけですので、サイトが閲覧できなくなるような影響がありません。 但し、ルートドメインの場合には自動バイパスモードを有効にするには条件がございますのでご要望の場合はお問合せ下さい。

【参考】FAQ②

Question		Answer	
Q11.	secuWAFのセキュリティ機能について教えてください。	A11.	secuWAFには、SQLインジェクション、クロスサイトスクリプト、スキャナー＆ボット等の大きく分類すると12種類のセキュリティ機能があります。また、管理画面上から各ポリシーの有効/無効を選択できる他、ホワइटリスト/ブラックリストへの登録が出来るなど、ユーザー自身で個別の設定が可能になっております。加えて、ブロックモード/検知モードへの切替えやWebサイトの簡易診断等、SOC側にご依頼いただくことで対応するものもございます。
Q12.	ルートドメインでの利用も可能でしょうか？	A12.	サブドメイン・ルートドメイン共にご利用は可能ですが、ルートドメインでのご利用の場合は自動バイパスモードを適用するには条件がある等、制約事項があるため、サブドメインでのご利用を推奨しております。
Q13.	DDOS攻撃の対応について教えてください。	A13.	HTTP GET(Post) Floods等のDOS攻撃については対応をしておりますが、複数のIPから分散して攻撃するようなDDOS攻撃には対応をしておらず、また、一般的にWAFでは防げないDDOS攻撃もあるため、CDNやIPSなどのご利用を推奨しております。
Q14.	secuWAF自体の負荷対策について教えてください。	A14.	オートスケール機能を実装した環境に環境に構築をしているため、負荷に応じて増強することで対応をしております。
Q15.	1契約で複数サイトで導入した場合のトラフィック量の確認方法について教えてください。	A15.	ダッシュボードで確認することが可能です。 以下のようにホスト（FQDN）が異なれば、ホスト毎の確認が可能です。 <code>http://www.abc.jp/</code> <code>http://www.efg.jp/</code> 以下のように同一ホストの場合、サブディレクトリ毎の確認はできません。 <code>http://www.abc.jp/123/</code> <code>http://www.abc.jp/456/</code>
Q16.	MALWARE CHECKERの定期巡回の範囲について教えてください。	A16.	MALWARE CHECKERは1ホスト（FQDN）に対して1契約となります。 以下のようにホスト内でサブディレクトリ毎にサイトがある場合も <code>http://www.abc.jp/site01/</code> <code>http://www.abc.jp/site02/</code> リンクを辿ってリンクがつながっていれば、同一ホストとして巡回され検知対象になります。ただ、TOPページからリンクがたどれない浮き島的なページは巡回されないため、検知対象にはなりません。 なお、リンクは最大、同一ドメインリンク5階層まで辿るよう設定が可能です。

【参考】FAQ③

Question		Answer	
Q17.	どのプランにしたら良いかわからないのでアドバイスが欲しい。	A17.	帯域保証プランの場合は、お客様がご利用中のログ管理ツールのほか、回線やクラウドサーバ等のサービスプロバイダーが提供する情報を参考にしてください。容量課金プランの場合は、ページ容量×月間PV数が分かりやすい計算となりますが、Webサイトの作りや導入済みの製品・サービスの内容によっては結果が大きく異なる可能性があるためあくまで参考値となります。無償トライアル等のご用意もありますので、お困りの場合はお問合せください。
Q18.	レポート出力可能な期間（=ログの保存期間）を教えてください。	A18.	管理画面とレポートで確認できるログの保存期間は3ヶ月となっております。
Q19.	MALWARE CHECKERで検知した際のアラート通知先は複数登録が可能でしょうか？	A19.	アラートメールは、ホスト毎に複数のメールアドレスを登録できます。
Q20.	CLOUD WAFについて、1契約でサブドメインとルートドメインの利用は可能でしょうか？	A20.	1契約内でサブドメインとルートドメインの双方を混同させてご利用いただくことは可能です。但し、双方に自動バイパス機能を有効にするためには条件があり、条件を満たさない場合は容量超過時に超過費用を頂戴するなどの影響があるため、混同させることは推奨しておりませんので、充分にご検討ください。

お問い合わせ

資料請求やお見積依頼など、お気軽にお問い合わせください。
担当からすぐにご連絡いたします。

お問い合わせフォーム

<https://www.secure-iv.co.jp/contact>



pr@secure-iv.com



098-943-2718

受付時間 9:00～18:00（土日祝祭日を除く）