Secure Innovation

沖縄から日本、アジア、そして世界へ

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

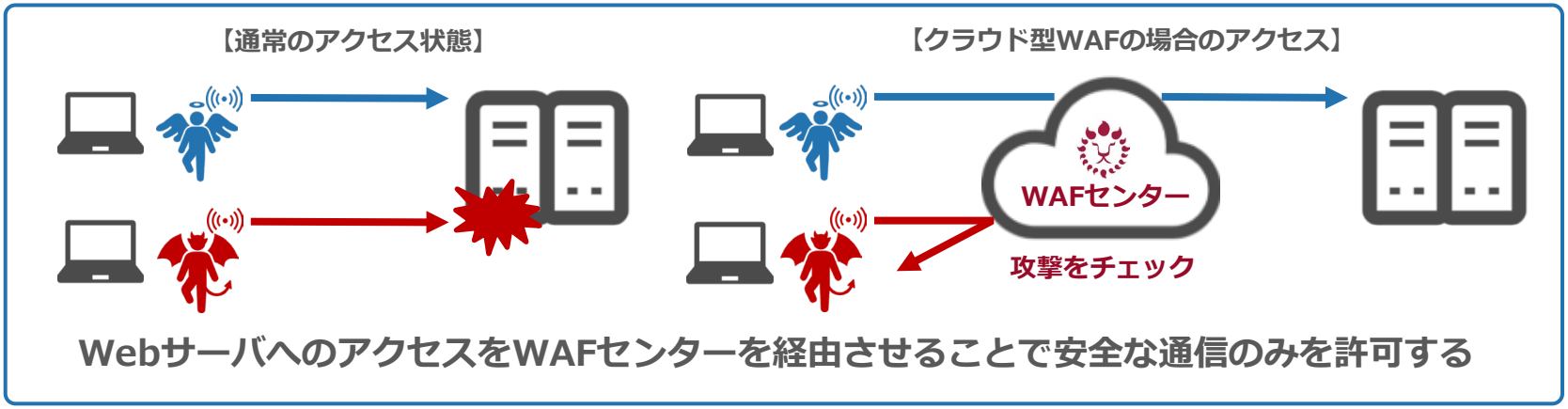
secuWAF

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、充分な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。**



WebサーバへのアクセスをWAFセンターを経由させることで安全な通信のみを許可する

secuWAFとは

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。

WAFの必要性

Secure Innovation
沖縄から日本、アジア、そして世界へ

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

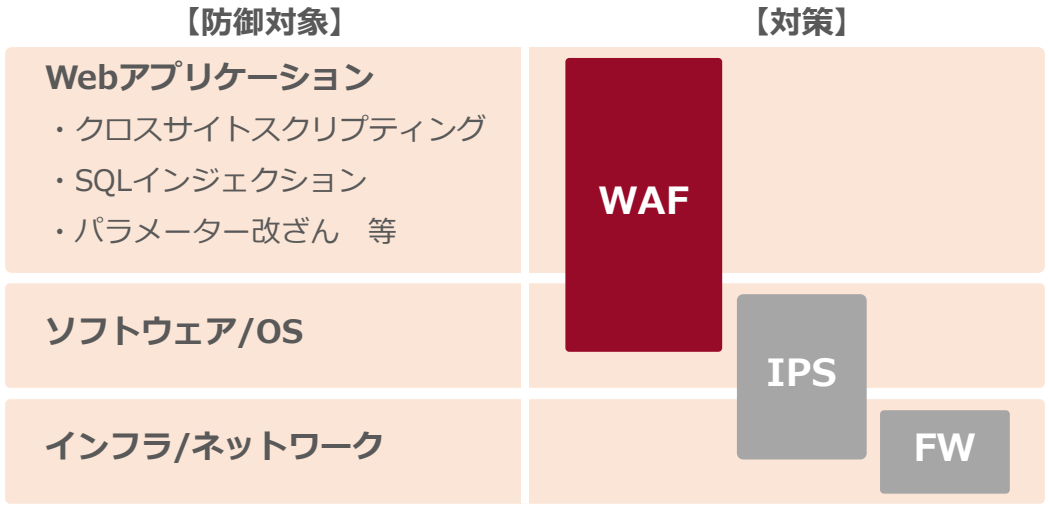
一般に公開されているWebアプリケーションなので、正規ユーザーと攻撃者を区別してアクセスさせることが難しい。

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～

Secure Innovation
沖縄から日本、アジア、そして世界へ

	クラウド型WAF（secuWAF）	アプライアンスWAF
費用	**安価**	**高額**
	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。
導入の手間	**非常に手軽**	**手間が大きい**
	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。
運用の手間	**ほぼゼロ**	**手間が大きい**
	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。
セキュリティ技術者	**不要** **（存在しているに越したことはないですが）**	**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。	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。
自由度	**低い** **（一般的なサービスは共通設定で利用）**	**高い**
	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。	ど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。

secuWAFの特徴

Secure Innovation
沖縄から日本、アジア、そして世界へ

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、アプライアンス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

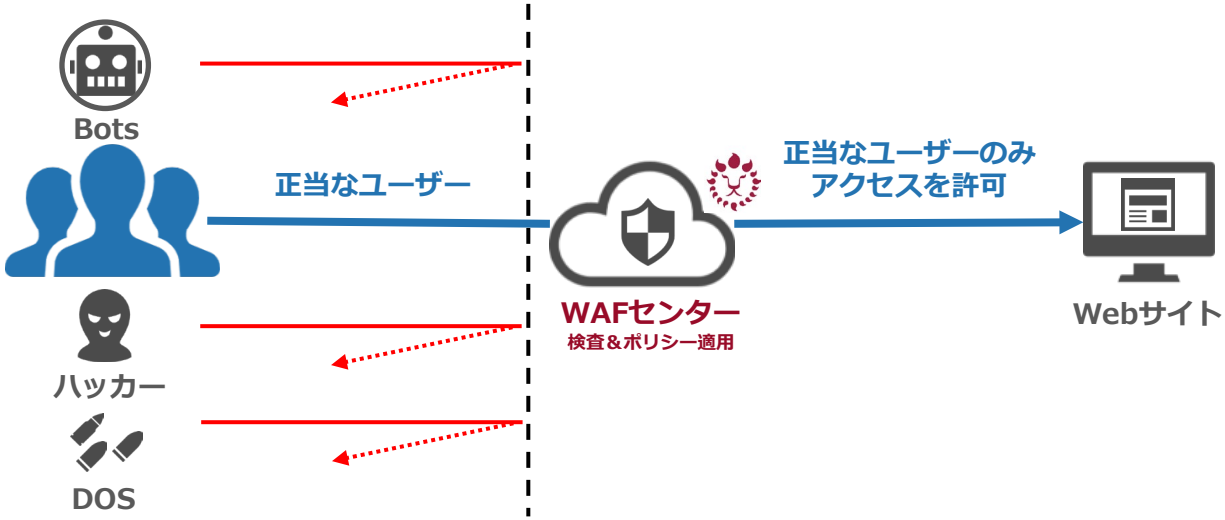
Secure Innovation
沖縄から日本、アジア、そして世界へ

	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出来ます。
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が、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が、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おります。
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いているサービスが多い中、secuWAFはオートスケール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

Secure Innovation
沖縄から日本、アジア、そして世界へ

強力なセキュリティ



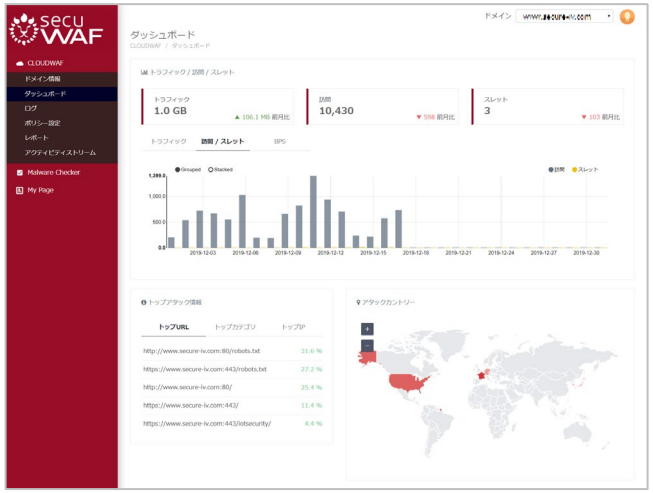
**最も脅威的なOWASPトップ10の脆弱性を突いた攻撃だけでなく、
その他の攻撃からもWebサイトを強固に防御します。**

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

Cloud WAF の主な機能②

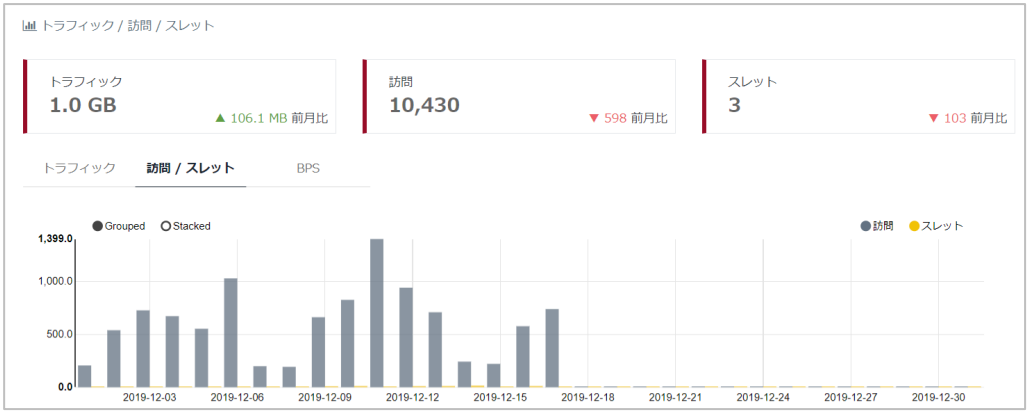
Secure Innovation
沖縄から日本、アジア、そして世界へ

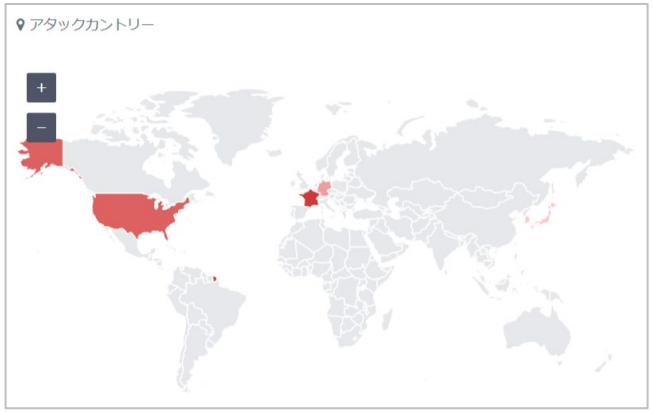
ダッシュボード



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

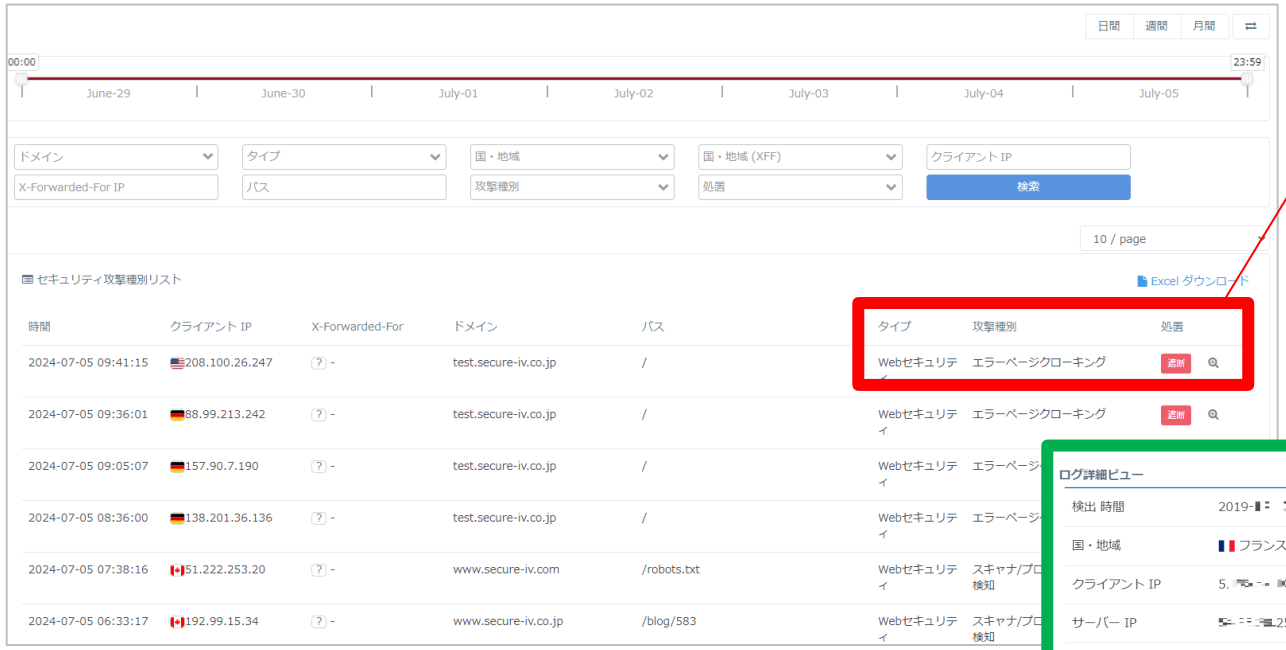
特に攻撃を受けるURLや
攻撃カテゴリーを表示。

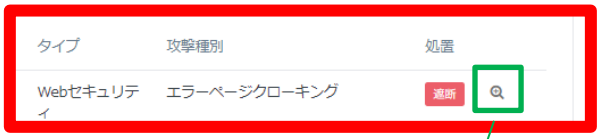
Cloud WAF の主な機能③

Secure Innovation
沖縄から日本、アジア、そして世界へ

セキュリティ攻撃種別

期間別の攻撃ログを検索・表示





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。

Cloud WAF の主な機能④

Secure Innovation
沖縄から日本、アジア、そして世界へ

ポリシー設定

個別設定

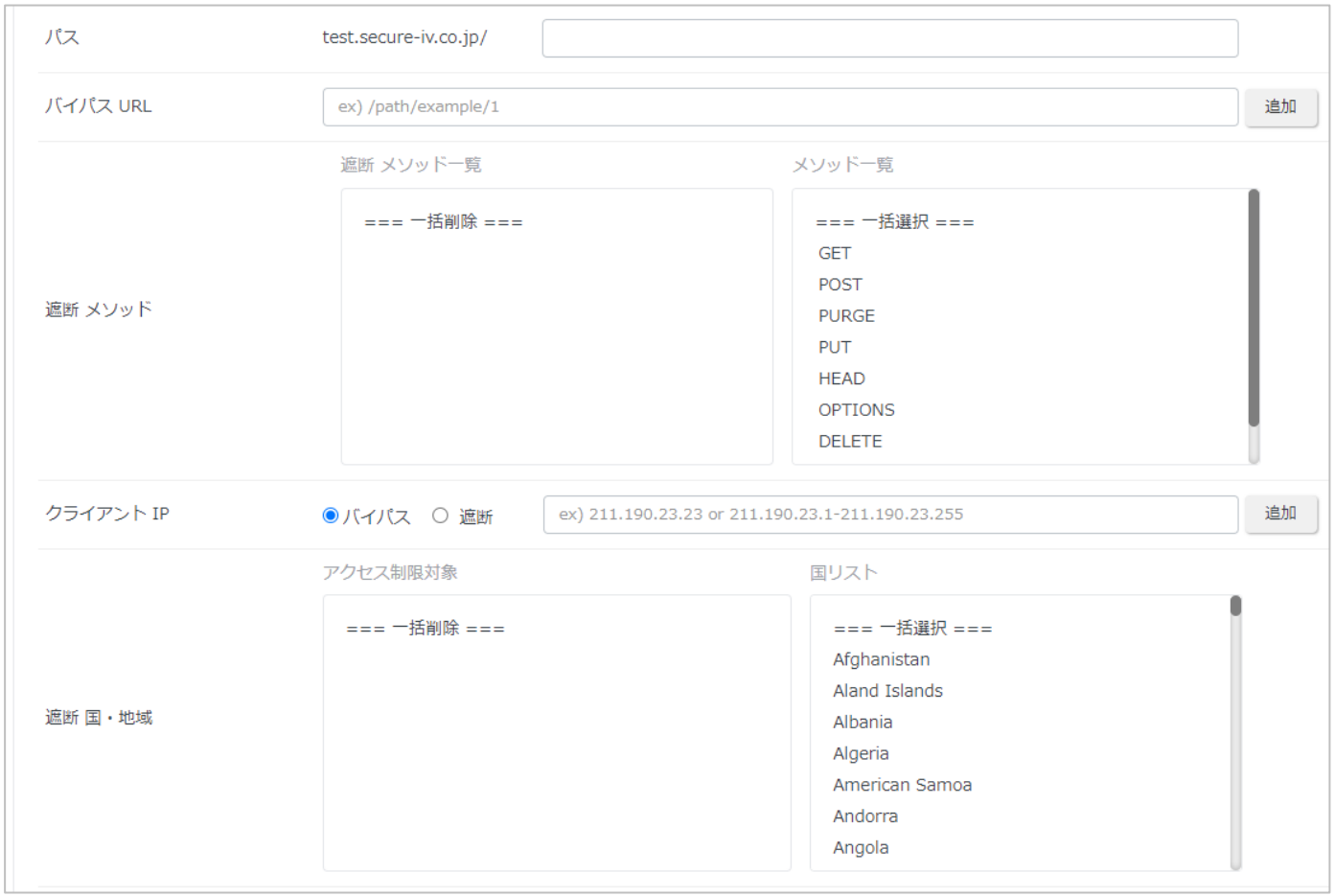
サイトごとに個別でポリシー設定が可能。
・防御項目の遮断/検知/OFF
・検出条件等の詳細内容（一部の項目）

Cloud WAF の主な機能⑤

Secure Innovation
沖縄から日本、アジア、そして世界へ

アクセス制御ルール

パス、バイパス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

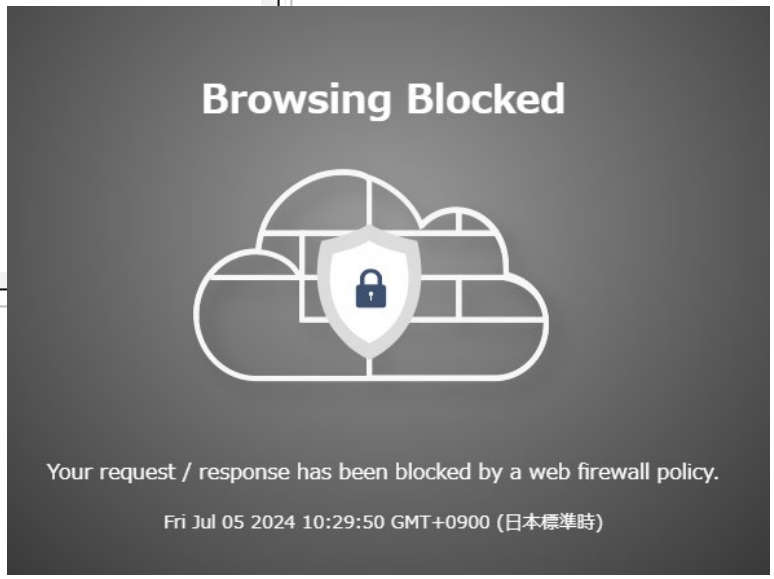


Cloud WAF の主な機能⑥

Secure Innovation
沖縄から日本、アジア、そして世界へ

遮断ページ

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



Cloud WAF の主な機能⑦

Secure Innovation
沖縄から日本、アジア、そして世界へ

その他機能

・他ドメインへ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

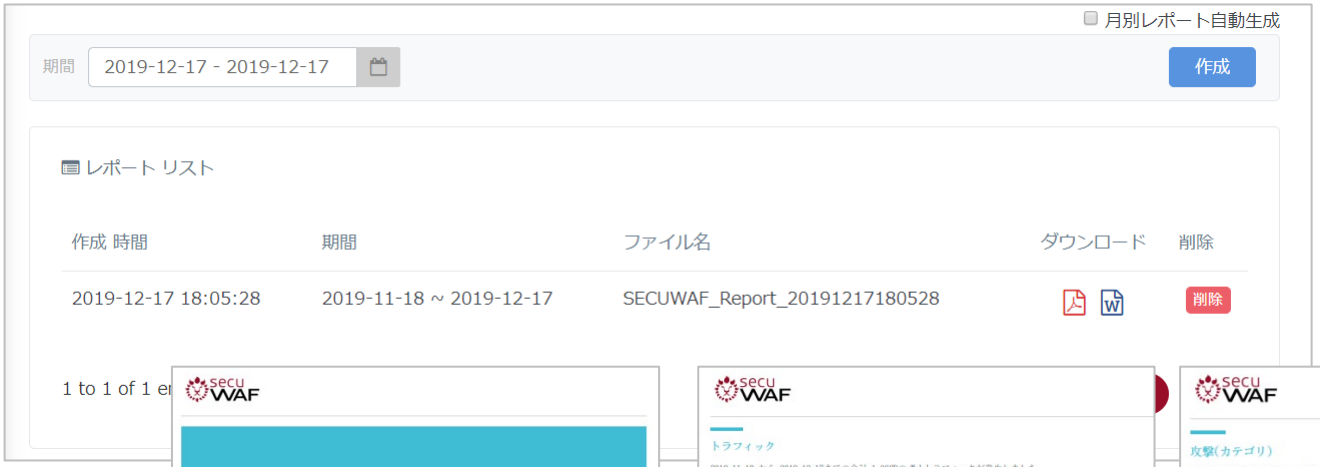
Cloud WAF の主な機能⑧

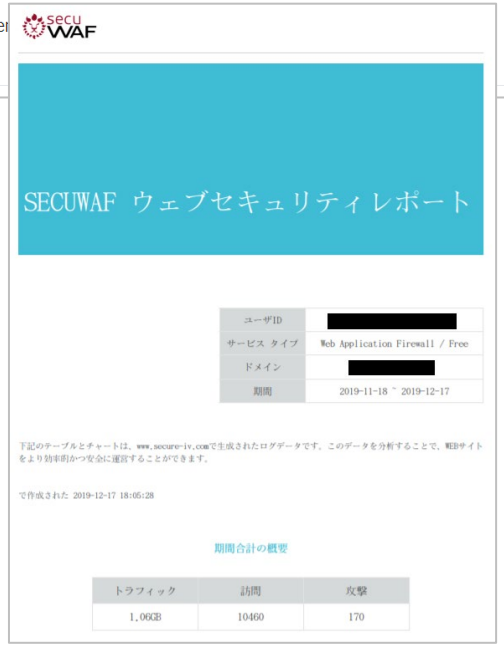
Secure Innovation
沖縄から日本、アジア、そして世界へ

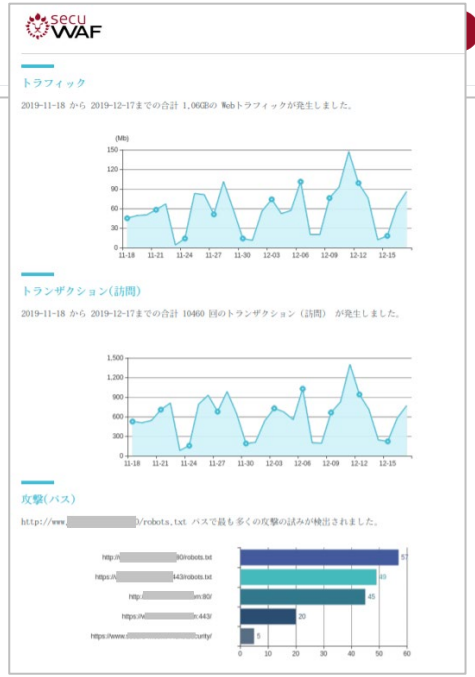
レポート

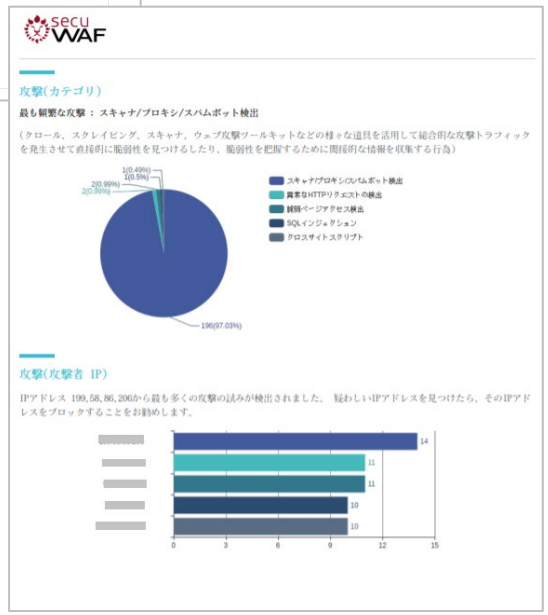
レポート生成

期間を指定してレポート生成（Word＆PDF)が可能。









MALWARE CHECKER の主な機能①

Secure Innovation
沖縄から日本、アジア、そして世界へ

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

Secure Innovation
沖縄から日本、アジア、そして世界へ

個別の巡回設定

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。

MALWARE CHECKER の主な機能③

Secure Innovation
沖縄から日本、アジア、そして世界へ

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

Secure Innovation
沖縄から日本、アジア、そして世界へ

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://[redacted]	0	0	7959	表示 ファイル 作成

1 to 1 of 1 entries

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カテゴリー	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.	プロトコール	アプリケーションプロトコール	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

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

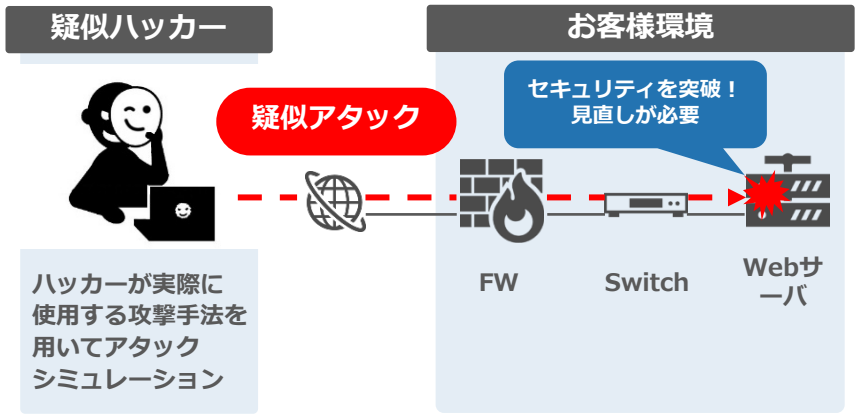
簡易Webアプリケーション診断サービスの内容

Secure Innovation
沖縄から日本、アジア、そして世界へ

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
バッファーオーバーフロー
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

Secure Innovation
沖縄から日本、アジア、そして世界へ

STEP 1 お客様側で、WebサイトからsecuWAFへの新規申込

STEP 2 サポートチームから保護対象のFQDN等の確認連絡を実施

STEP 3 サポートチームにてお客様のWebサイトをsecuWAFセンターに登録

STEP 4 サポートチームからお客様に対して、DNS情報を送付

STEP 5 お客様側にて、DNSの設定変更

START DNSの設定変更が反映され次第、secuWAFでの防御がスタート

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

Secure Innovation
沖縄から日本、アジア、そして世界へ

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	100B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

Secure Innovation
沖縄から日本、アジア、そして世界へ

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ト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

Secure Innovation
沖縄から日本、アジア、そして世界へ

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、ホワイトリスト/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が、 http://www.abc.jp/　　http://www.efg.jp/ 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。 http://www.abc.jp/123/　http://www.abc.jp/456/
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 http://www.abc.jp/site01/　http://www.abc.jp/site02/ 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

Secure Innovation
沖縄から日本、アジア、そして世界へ

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

Secure Innovation
沖縄から日本、アジア、そして世界へ

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）