beyond セキュリティ対策

GRED

クラウド側WAFでサイバー攻撃を可視化・遮断するサービスです。
よくあるDDoS攻撃は当サービスがぴったりです。

GRED Web改ざんチェック Cloud

定期的にWebサイトの不正改ざんの有無を確認し、
不正な改ざんを検知すると、
管理者にアラートメールの配信と詳細レポートの提供を行います。

3つの検知エンジンで改ざん検知

■スクリプト変化検知エンジン
JavaScriptの変化を独自のアルゴリズムで分析し検知。

■リンクタグ変化検知エンジン
HTML内の特定タグの、src属性やhref属性の変化を検知。

■表層解析エンジン
監視対象ページにある実行ファイルが、
マルウェアと類似した動きをしている場合に警告をおこなう。

様々なWeb改ざんに対応

・サイバー攻撃などによるWeb改ざん

・脆弱性を悪用した攻撃をおこなうWeb改ざん

・ウイルスなどが自動的に
ダウンロードされるWeb改ざん

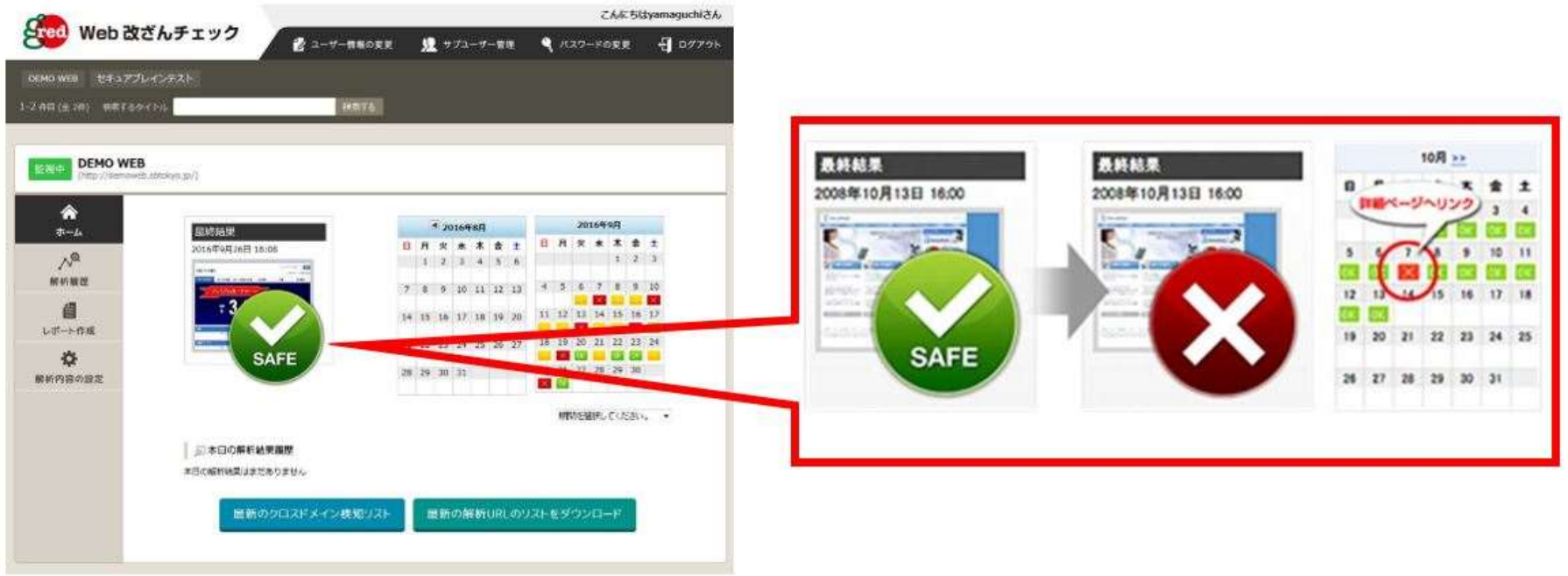
・政治意思や思想を誇示するために
意図的にページ書換えをおこなうWeb改ざん

・ドライブバイダウンロード攻撃の
踏み台に利用するためのWeb改ざん

・ガンブラーやDarkleech Apache Moduleによる
Web改ざん　など

Web改ざんを発見した場合

登録されている URL に改ざんがあった場合、管理コンソールトップページの「SAFE」の緑のマークが
「改ざんを発見」の赤のマークに変化し、アラート用に登録されたメールアドレスに改ざん発見の通知が届きます。



詳細はメールに記載されている URL をクリックするか、
トップページのカレンダーの赤い「×」アイコンをクリックすると確認できます。
詳細な解析レポートによって問題のある個所がすぐにわかるので、迅速な対処が可能になります。

改ざんを検知したソースコードのハイライト表示

詳細レポートの
「詳細を見る」をクリックすると、
改ざんを検知したページの
ソースコードが表示され、
問題のある箇所をハイライト表示します。

問題のある箇所をいち早く見つけることで、
より迅速な対応が可能になります。

リンクタグ・JavaScriptの変化検知時の詳細レポート

JavaScript の変化を見ることにより改ざんを検知する「スクリプト変化検知エンジン」と、
HTML 内の特定タグの src属性 や href属性変化を検知する「リンクタグ変化検知エンジン」を実装しているので、
「Webコンテンツデータの変化を検知」というタイトルでメールが配信され詳細を管理コンソールで確認することができます。

クロスドメインスクリプト管理・警告機能

クロスドメインスクリプト管理・警告機能は、
監視対象のWebサイト全体に含まれる
クロスドメインスクリプトを
一括して監視・管理することができます。

意図しないクロスドメインスクリプトが
埋め込まれた際に、
警告が送信され迅速に対処することが可能です。

GRED Web改ざんチェックのシール

本サービスをご利用の方には、「GRED Web改ざんチェックのシール」を提供します。
このシールを自社のWebサイトに表示すれば、
Web改ざんチェックによって守られている検証結果を表示させることができます。
「GRED Web改ざんチェックのシール」をWebページに配置してWebサイトが常に監視され、
安全であることをアピールし、Web閲覧者や顧客に安心を提供します。

サービス提供価格

種別	月額費用（税別）
基本プラン　改ざん解析：1日4回 1,000ページ	30,000円 / 1FQDN
追加プラン　改ざん解析：FQDN追加	10,000円 / 1FQDN
追加プラン　改ざん解析：ページ追加	10,000円 / 1,000ページ

※「基本プラン」は初回の設定手数料として、1プランあたり別途10,000円(税別)が必要です。
※「追加プラン」のみのご契約はできません。
※ 1プランでの運用可能ホスト数は「1FQDN」です。

サービスのお申し込み・ご不明点はお気軽にご連絡ください。

お問い合わせ

株式会社ビヨンド

TEL：0120-803-656

Email：info@beyondjapan.com