

# 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にです。

# 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

監視中 DEMO WEB  
(http://demoweb.■■■■.jp/)

ホーム

解析履歴

レポート作成

解析内容の設定

### 解析履歴

⚠ 解析履歴の表示期間は2ヵ月です。

解析日	解析完了時間	解析結果	URI数
2016年09月25日	18:10	改ざんを発見しました	8
2016年09月24日	18:12	注意が必要です	9
2016年09月23日	18:14	問題はありませんでした	8
2016年09月22日	18:16	問題はありませんでした	8
2016年09月21日	18:17	注意が必要です	9
2016年09月20日	18:18	問題はありませんでした	8
2016年09月19日	18:19	改ざんを発見しました	8
2016年09月18日	18:20	注意が必要です	9

- ・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。

## 問題が見つかりました

<http://demoweb.████████.jp/>

以下のソースコード内のハイライト部に問題があります。

```
1 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1" >
2 <html xmlns="http://www.w3.org/1999/xhtml" xml:lang="ja" lang="ja">
3 <head>
4 <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
5 <meta http-equiv="Content-Style-Type" content="text/css" />
6 <meta http-equiv="Content-Script-Type" content="text/javascript" />
7 <meta http-equiv="imagetoolbar" content="no" />
8 <meta name="description" content="" />
9 <meta name="keywords" content="" />
10 <link rel="stylesheet" href="css/common.css" type="text/css" />
11 <script type="text/javascript" src="js/jquery.js"></script>
12 <script type="text/javascript" src="js/common.js"></script>
13 <title>ABCネット銀行</title>
14 </head>
15 <body>
16 <div id="top">
17 <div id="header">
18 <h1><a href="index.html"></a></h1>
19 <div id="serch">
20 <form action="http://www.google.com/cse" id="cse-search-box">
21 <input type="hidden" name="cx" value="" />
22 <input type="hidden" name="ie" value="UTF-8" />
23 <dl>
24 <dt><input type="text" name="q" size="21" /></dt>
25 <dd><input type="image" src="images/serch.gif" alt="検索" name="sa" value="検索" /></dd>
26 </dl>
27 </form>
```





# 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。

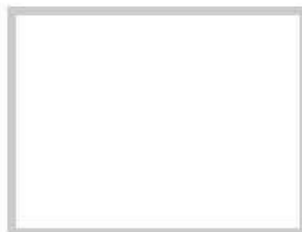
意図しないクロスドメインスクリプトが埋め込まれた際に、警告が送信され迅速に対処することが可能です。

**注意が必要です**

2016年9月6日 18:38



http://www. [redacted] /1.0/badge.js




## 脅威名:[CrossDomain]

ウェブページに、未確認のクロスドメインスクリプトを発見しました。クロスドメインスクリプトとは、自社サイト以外のドメインにあるスクリプトを実行させるようなコードが自社のサイトに記述されているという事です。スクリプト自体を確認し、正常なものである場合には「[クロスドメインの許可設定](#)」メニューにて許可してください。このスクリプトを記載した覚えがない場合にはウェブサイトの改ざんが発生している恐れがあります。その場合にはただちに該当HTMLを確認して、修正を行ってください。また許可設定を行うと、今後「警告」のメッセージ等が表示されなくなります。必要な場合には「[クロスドメインの許可設定](#)」メニューにて許可設定を削除すると、以降、再び警告を発するようになります。クロスドメインスクリプトの許可機能のON/OFFは「[クロスドメインの許可設定](#)」から行えます。

### クロスドメインが見つかった経路

 http://www. [redacted] /1.0/badge.js

 http://demoweb. [redacted] jp/

# 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](mailto:info@beyondjapan.com)