
Web 改ざん検知サービス ユーザーガイド

第 3 版

(2023 年 8 月 8 日)

株式会社フューチャースピリッツ



目次

1. Web 改ざん検知サービスの概要	3
1.1 検知可能な改ざん	3
1.2 改ざんを発見した場合	3
1.3 改ざん検知時のページ切り替え	4
2. 管理コンソールの見方、使い方	5
2.1 ログイン・ログアウト	5
2.2 ダッシュボード画面	6
2.3 解析結果表示 緑 (SAFE)	8
2.4 解析結果表示 赤 (DANGER)	8
2.5 解析結果表示 黄色 (Warning) クロスドメインスクリプト検知	11
2.6 解析結果表示 黄色 (Warning) TOP ページの見た目変化検知	13
2.7 解析結果表示 黄色 (Warning) タグ・JavaScript の変化検知	14
2.8 解析結果表示 黄色 (Warning) EXE 解析検知	15
2.9 改ざん検知時のメール配信	16
2.10 お知らせ機能	17
3. 解析履歴	18
3.1 解析履歴	18
3.2 レポート作成	19
3.3 週間レポートメール	21
4. 各種設定	22
4.1 ユーザー管理	22
4.2 ユーザー情報の確認・変更	23
4.3 パスワードの変更	25
4.4 除外 URL の登録	25
4.5 ホワイトリストの登録	26
4.6 監視の ON/OFF とウェブ解析対象階層の指定	28
4.7 クロスドメインの許可設定	29
4.8 改ざん検知時のページ切り替え機能の設定	30
4.9 GRED 証明書の設定	32
5. その他の機能・サービス	34
5.1 解析サイトの検索	34
5.2 オンデマンドチェック機能	34
5.3 GRED 証明書	35
5.4 パスワードをお忘れの場合	36
5.5 ログイン履歴確認機能	36
6. 解析する URL の絞り込み	37
6.1 解析開始 URL と対象ドメイン設定について	37
6.2 解析する URL の絞り込み (除外 URL の登録)	38

6.3	解析する URL の絞り込み（ウェブ解析対象階層の指定）	39
-----	------------------------------------	----

1. Web 改ざん検知サービスの概要

「Web 改ざん検知サービス」は、お客様の Web サイトが改ざんの被害にあっていないかを定期的に確認するサービスです。監視対象となる URL を登録するだけで、システムが自動的にリンクを辿り、各ページの解析を行います。


改ざん発見時には、アラート送信と詳細なレポートを生成する機能を提供します。

※「Web 改ざん検知サービス」は、株式会社セキュアブレインが提供する「GRED（グレッド）Web 改ざんチェック」を利用したサービスです。

1.1 検知可能な改ざん

- ・サイバー攻撃等による Web サイトの改ざん
- ・脆弱性を悪用した攻撃を行う Web サイトへの改ざん
- ・ウイルスなどが自動的にダウンロードされる Web サイトへの改ざん
- ・政治意思や思想を誇示するために意図的にページを書き換える改ざん
- ・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
- ・SEO ポイズニングによる Web 改ざん

1.2 改ざんを発見した場合

改ざんを発見した場合、管理者にアラートメールを配信します。詳細はそのメールに記載されている URL をクリックするか、管理コンソールトップページのカレンダーの赤い  のアイコンをクリックすると確認いただけます。



■ 詳細レポート

詳細レポートには、改ざんを検知した URL、改ざんの種類とその説明、悪質コードの脅威名とソースを表示します。このレポートにより、迅速な対応が可能になります。

問題が見つかりました

2022年5月13日 15:29

改ざんを検知したページのURL

改ざんの種類と説明

脅威名:Iframe Generic (GJS159)

貴社のWebサイトに不正に改ざんされたWebサイトのコンテンツが発見されました。不正に改ざんされたWebサイトとは、ウェブサイトの脆弱性を利用して不正に貴社のWebページに悪質なHTMLコードを追加したことを意味します。検知されたURLの内容に不正に追加されたHTMLコードがあるかを確認してください。「詳細を見る」をクリックすると悪質と思われるHTMLコードが表示されます。このHTMLコードが貴社のコンテンツでない場合は、Webサイトが改ざんされた可能性がありますので、このWebページの内容の確認をしてください。また、Webサーバに最新のパッチが適用されていることもご確認ください。万が一、貴社のコンテンツが誤検知されている場合は、お手数ですがサポートセンターへご連絡してください。

詳細を見る

検知箇所を見る

より詳しい情報を表示（ソースコードを表示）

検知箇所をリンク構造で表示

1.3 改ざん検知時のページ切り替え

改ざんが見つかった場合、自動で安全なページ（GRED 内のメンテナンスページ）に切り替えることができます。この改ざん検知時のページ切り替え機能を設定しておくと、お客様の Web サイトが復旧するまで、エンドユーザーへの被害を防ぐことができます。この機能は、お客様の Web サイトが安全な状態になると表示されません。



2. 管理コンソールの見方、使い方

各種設定、サービスの提供は、管理コンソールより行います。

2.1 ログイン・ログアウト

ログイン

<https://www.gred.jp/saas/future-s/>にアクセスし、ログイン画面に、ID とパスワードを入力し、「ログインする」をクリックします。

Web改ざん検知サービス



Copyright (c) 2019 SecureBrain Corporation. All Rights Reserved.

システムメンテナンスや障害の詳細情報は、ログイン後に確認いただけます。
詳細は「3.10 お知らせ機能」を参照してください。

ログアウト

ヘッダーの上部にある『ログアウト』ボタンをクリックすると、ログアウトされます。

Web改ざん検知サービス

サイト検索 ユーザー情報 サブユーザー パスワード **ログアウト**

[https://\[redacted\]](https://[redacted])

Dashboard

[https://\[redacted\]](https://[redacted])

監視中



2.2 ダッシュボード画面

正しくログインが完了すると、ダッシュボード画面へ遷移します。ダッシュボード画面では、最新の解析結果と過去の解析結果の統計情報（直近、ウィークリー、マンスリー）の棒グラフと解析履歴（1 年分）をカレンダーで表示します。



	項目名	内容
①	最終結果	最新の解析結果を表示します。詳細は 3.3 以降の「解析結果表示」参照して下さい。
②	本日の解析結果履歴	最新の解析結果を表示します。
③	直近の解析結果	直近の 8 回分の解析結果（解析毎の検知数の累計）を棒グラフで表示します。
④	ウィークリーの解析結果	今週を含めて 8 週間分の解析結果の累計を 1 週間ごとの棒グラフで表示します。
⑤	マンスリーの解析結果	今月を含めて 8 か月分解析結果の累計を 1 か月ごとの棒グラフで表示します。
⑥	解析結果カレンダー	解析の結果を、それぞれ安全、警告、危険のマークをカレンダー上に表示します。カレンダー上部の「期間を選択」リストボックスで表示する年月の切り替えが出来ます。
⑦	解析サイトリスト	解析サイトが複数ある場合にはリストで表示されます。リストボックスに表示される解析サイトを選択すると表示対象の解析サイトの切り替えが出来ます。
⑧	詳細設定ボタン	各解析サイトの解析履歴、詳細設定画面に遷移します。
⑨	ツールチップ	各棒グラフにカーソルを合わせると解析結果の検知数が表示されます。

		<p>改ざん検知された場合</p>  <p>改ざん検知が無い場合</p> 
⑩	ログイン履歴	前回のログイン日時を表示します。右側の「履歴」をクリックすると過去のログイン履歴を表示するページに遷移します。詳細は 6.11 の「ログイン履歴確認機能」を参照して下さい。
⑪	お知らせ	管理画面には最新のお知らせが表示されます。「一覧を見る」をクリックすると過去のお知らせを確認することができます。詳細は 3.10 の「お知らせ機能」を参照してください。

※アイコンと棒グラフの色について
(詳細は 3.3 以降の「解析結果表示」を参照して下さい。)



2.3 解析結果表示 緑 (SAFE)

解析した結果、安全なサイトであると判定された場合、画面には「SAFE」と緑で表示されます。



「SAFE」表示内容

	項目名	内容
①	判定結果	安全なサイトであることを示す「SAFE」が表示されます。
②	解析結果カレンダー	解析の結果、安全なサイトと判断された場合には緑色の🟢のマークをカレンダー上に表示します。



2.4 解析結果表示 赤 (DANGER)


解析を行った結果、危険なサイトであると判定された場合、画面には赤の🔴マークが表示されます。

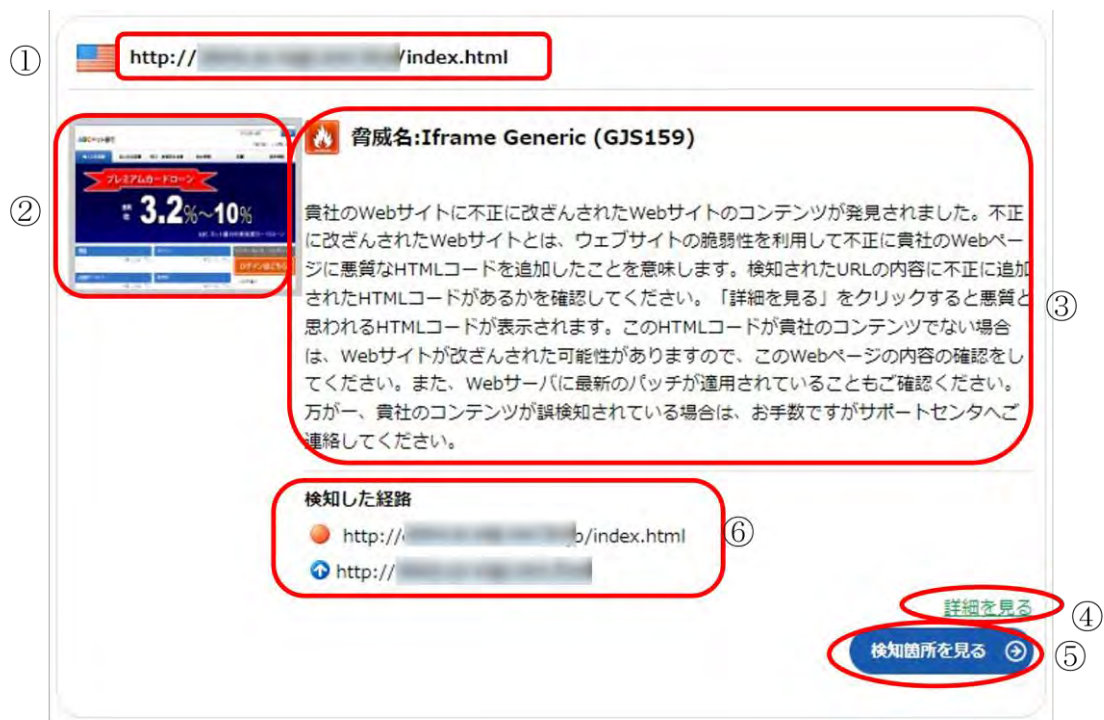


「DANGER」表示内容


	項目名	内容
①	判定結果	危険なサイトであることを示す赤い🔴が表示されます。

②	解析結果カレンダー	解析の結果、危険なサイトと判断された場合には赤色の  マークをカレンダー上に表示します。  のマークをクリックすると、解析結果の内容を表示することができます。
③	最新の解析結果	最新の解析結果を表示します。危険なサイトだと判断された場合には赤く表示され、解析結果には危険の内容が表示されます。

解析結果カレンダーの  をクリックすると、解析結果の内容が表示されます。



① [http://\[redacted\]/index.html](http://[redacted]/index.html)

② 

③ **脅威名:Iframe Generic (GJS159)**
 貴社のWebサイトに不正に改ざんされたWebサイトのコンテンツが発見されました。不正に改ざんされたWebサイトとは、ウェブサイトの脆弱性を利用して不正に貴社のWebページに悪質なHTMLコードを追加したことを意味します。検知されたURLの内容に不正に追加されたHTMLコードがあるかを確認してください。「詳細を見る」をクリックすると悪質と思われるHTMLコードが表示されます。このHTMLコードが貴社のコンテンツでない場合は、Webサイトが改ざんされた可能性がありますので、このWebページの内容の確認をしてください。また、Webサーバに最新のパッチが適用されていることもご確認ください。万が一、貴社のコンテンツが誤検知されている場合は、お手数ですがサポートセンタへご連絡してください。

④ [詳細を見る](#)

⑤ [検知箇所を見る](#)

⑥ **検知した経路**
[http://\[redacted\]/index.html](http://[redacted]/index.html)
[http://\[redacted\]](http://[redacted])

解析結果の表示内容

	項目名	内容
①	URL 表示	危険と判断された URL が表示されます。
②	判定画面	危険と判断されたサイトの画像が表示されます。
③	解析結果	どのような危険のあるサイトなのか表示します。
④	解析結果の詳細	問題のあるソースコードがハイライト表示されます。
⑤	検知した箇所を見る	検知箇所が可視化されます。
⑥	検知した経路	検知した箇所の経路が表示されます。 「脅威名」の名称が表示されている場合には、検知経路が表示されます。

また、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。

問題が見つかりました

http://[redacted] /

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/xhtml2
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" />
26         </dl>
27       </form>

```

2.5 解析結果表示 黄色（Warning）クロスドメインスクリプト検知

許可設定をしていないクロスドメインスクリプトを検知すると、管理コンソールホームのマークが黄色の「Warning」（警告）に変化します。

The dashboard displays the following information:

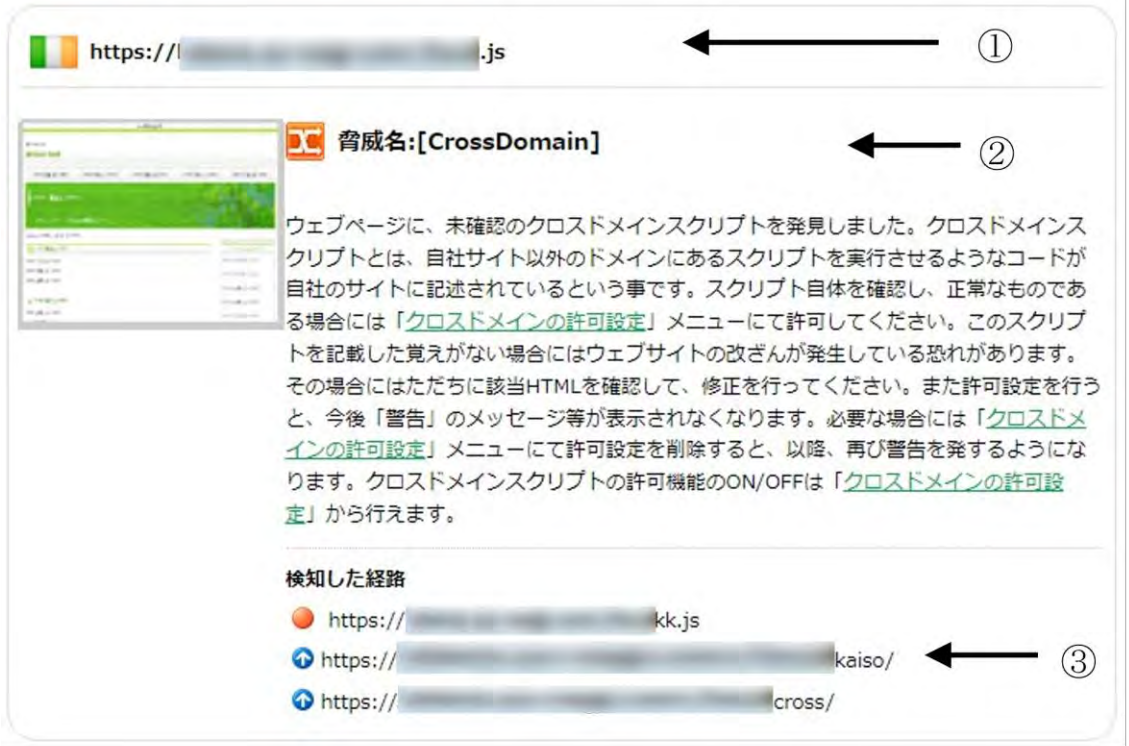
- Summary:** Shows a yellow warning icon and a 'WARNING' status.
- Recent Analysis Results:** A bar chart showing analysis results for various domains.
- Weekly Analysis Results:** A bar chart showing analysis results for the current week.
- Calendar:** A calendar for May 2022. A red box highlights a yellow warning icon on May 27, with an arrow pointing to it.
- Today's Analysis Results:** A table showing analysis results for the current day.

黄色のマークをクリックすると
詳細ページが表示されます。

■詳細ページ

注意が必要です

2022年5月4日 10:03



解析結果の表示内容

	項目名	内容
①	URL 表示	クロスドメインを検知した URL が表示されます。
②	解析結果	クロスドメインの許可設定の説明
③	クロスドメインの経路	クロスドメインが見つかった経路を表示します。

「クロスドメインの許可設定」から自社のドメイン以外に利用しているスクリプトのドメインを設定しておくことによって、解析結果の「Waning」表示を「SAFE」に変更します。（設定の方法は、「5.7 クロスドメインの許可設定」をご覧ください。）

2.6 解析結果表示 黄色（Warning）TOP ページの見た目変化検知

Top ページのコンテンツが著しく変化した場合に、「Top ページの見た目が変化した可能性を検知」というタイトルでメールが送信され、詳細を管理コンソールで確認することができます。



	項目名	内容
①	URL 表示	危険と判断された URL が表示されます。
②	判定画面	危険と判断されたサイトの画像が表示されます。
③	解析結果	どのような危険のあるサイトなのか表示します。

2.7 解析結果表示 黄色（Warning）タグ・JavaScript の変化検知

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」を実装しました。「タグ/JavaScript 変化検知」という項目で表示されます。詳細は管理コンソールで確認することができます。

注意が必要です

2022年5月16日 10:47



	項目名	内容
①	URL 表示	タグ/JavaScript の変化を検知した URL が表示されます。
②	概要	タグ/JavaScript の変化の概要
③	変化したタグ/JavaScript	変化したソースコードを表示します。

2.8 解析結果表示 黄色（Warning） EXE 解析検知

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行う「表層解析エンジン」を実装しました。「ファイルのマルウェア類似挙動の可能性を検知」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。

注意が必要です

2022年5月16日 11:27



	項目名	内容
①	URL 表示	危険と判断された URL が表示されます。
②	概要	ファイルの概要
③	解析結果	挙動の詳細を表示します。

2.9 改ざん検知時のメール配信

危険なサイトを検知すると、管理コンソールのアイコンが赤または黄色に変わると同時に登録いただいたメールアドレスに解析結果が送付されます。

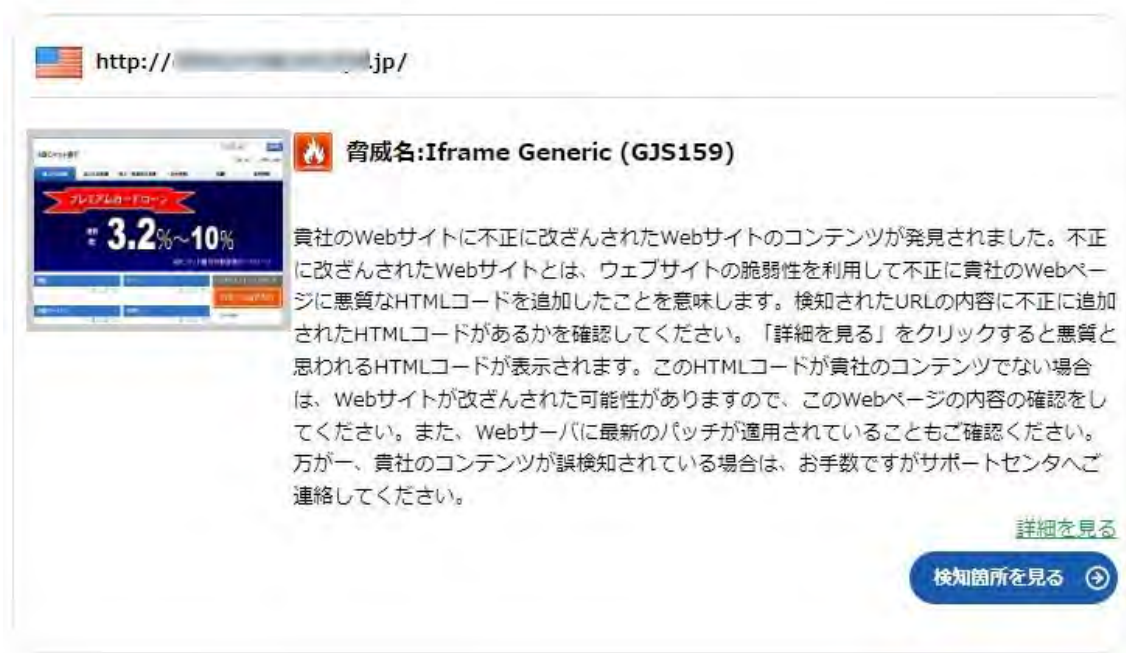
メール本文には、検知したページの URL と内容が表示されます。

「詳細については下記 Web サイトをご参照ください。」と表示された下のリンクをクリックすると詳細ページにジャンプします。改ざんされている可能性があるウェブページの参照には十分ご注意の上、確認してください。

詳細ページ

問題が見つかりました

2022年5月13日 15:29



改ざん検知以外のアラートメールは以下 5 種です。

なおアラートメールは、管理コンソールから「メールを送信する」、「送信しない」を選択することができます。

- ・ Top ページのヘルスチェック検知時
- ・ 見た目変化検知時
- ・ クロスドメインスクリプト検知時
- ・ EXE 解析検知時
- ・ タグ・JavaScript 変化検知時

2.10 お知らせ機能

Web 改ざん検知サービスのシステムに関するお知らせやメンテナンスなどの情報を確認することができます。

管理画面には最新のお知らせが 1 件表示されます。タイトルをクリックすると詳細画面へ遷移します。「一覧を見る」をクリックすると、過去のお知らせ一覧が確認できます。

■ 一覧ページ

お知らせ一覧		
掲載日	カテゴリー	タイトル
2023年02月22日	重要なお知らせ	新画面切替に関するお知らせ
2022年12月28日	重要なお知らせ	定期システムメンテナンス スケジュールのお知らせ
2022年09月30日	重要なお知らせ	定期システムメンテナンス スケジュールのお知らせ
2022年09月09日	重要なお知らせ	システムメンテナンスのお知らせ
2022年08月08日	重要なお知らせ	新画面に関するお知らせ
2022年06月30日	重要なお知らせ	定期システムメンテナンス スケジュールのお知らせ
2022年04月14日	重要なお知らせ	システムメンテナンスのお知らせ
2022年04月01日	重要なお知らせ	定期システムメンテナンス スケジュールのお知らせ
2022年03月07日	重要なお知らせ	システムメンテナンスのお知らせ
2022年01月01日	重要なお知らせ	定期システムメンテナンス スケジュールのお知らせ

■ 詳細ページ

お知らせ

2023年02月22日

[重要なお知らせ] 新画面切替に関するお知らせ

- ・ GRED Web改ざんチェックCloudは、2023/3/1に新画面へ移行しより多くの情報を可視化しお客様へ提供致します。
- ・ 2022/8/9より、新画面を暫定URLで並行稼働しておりましたが、2023/6/1に暫定URLは廃止致します。
- ・ 新画面では新たに、検知結果の推移グラフやGUIへのログイン履歴の参照が可能となっております。
- ・ 新画面の利用は、Edge, Firefox, Chromeご利用を推奨いたします。

戻る

お知らせはメールでも受け取ることができます。

設定方法は「5.2 ユーザー情報の確認・変更」を参照してください。

3. 解析履歴

解析履歴やレポートの確認方法をご説明します。


3.1 解析履歴

過去の解析を確認することができます。

The screenshot shows the '解析履歴' (Analysis History) page. The page header includes the URL 'http://...' and a '監視中' (Monitoring) status. The left sidebar contains navigation links: 'ホーム' (Home), '解析履歴' (Analysis History), 'レポート作成' (Report Creation), and '解析内容の設定' (Analysis Content Settings). The main content area displays a table of analysis results. The table has four columns: '解析日' (Analysis Date), '解析完了時間' (Analysis Completion Time), '解析結果' (Analysis Result), and 'URL数' (URL Count). The table lists several analysis results, with some highlighted in red and others in yellow. A red box highlights the 'ダウンロード' (Download) button at the bottom of the table, with a note indicating that it downloads the analysis history for the last 2 months.

解析日	解析完了時間	解析結果	URL数
2022年05月16日	05:10	改ざんを発見しました	10
2022年05月15日	17:10	注意が必要です	10
2022年05月15日	05:10	注意が必要です	10
2022年05月14日	17:10	問題はありませんでした	10
2022年05月14日	05:10	問題はありませんでした	10
2022年05月13日	17:10	改ざんを発見しました	10
2022年05月13日	15:29	改ざんを発見しました	10


③ ダウンロード ※ 2ヵ月分の解析履歴をダウンロードします

- ① 画面左上のをクリックし、「解析内容の設定」に遷移します。
- ② 左側の「解析履歴」をクリックします。
- ③ 解析日、解析完了時間、解析結果、ページ数を新しいものから順に表示します。赤、黄色の項目はクリックすると、詳細ページにジャンプします。「ダウンロード」をクリックする事で、CSV 形式のファイルでダウンロード可能です。

3.2 レポート作成

左側にある「レポート作成」をクリックします。
一定期間の解析結果の統計情報を見ることができます。



- ① 画面左上のをクリックし、「解析内容の設定」に遷移します。
- ② 左側の「レポート作成」をクリックします。
- ③ 統計を出したい期間（1 か月単位）を指定し「レポートを作成する」ボタンをクリックすると、指定された期間の統計概要と月ごとの解析結果が表示されます。

Web改ざん検知サービス

2022年5月16日 13:48

GRED Web改ざんチェック レポート

解析対象ドメイン: http:// /

解析期間: 2022年5月~2022年5月

解析結果: 問題あり

2022

5月

改ざんを通知した回数

貴社のウェブページ数(平均)

6

10

改ざん内容の詳細

[検知日]2022年5月13日 15:29

[検知ページ]http:// /index.html

貴社のWebサイトに不正に改ざんされたWebサイトのコンテンツが発見されました。不正に改ざんされたWebサイトとは、ウェブサイトの脆弱性を利用して不正に貴社のWebページに悪質なHTMLコードを追加したことを意味します。検知されたURLの内容に不正に追加されたHTMLコードがあるかを確認してください。このHTMLコードが貴社のコンテンツでない場合は、Webサイトが改ざんされた可能性がありますので、このWebページの内容の確認をしてください。また、Webサーバに最新のパッチが運用されていることもご確認ください。万が一、貴社のコンテンツが誤検知されている場合は、お手数ですがサポートセンタへご連絡してください。

詳細

脅威名:Iframe Generic (GJS159)

レポートを印刷する

	項目名	内容
①	統計概要	解析したサイトと期間、解析結果
②	統計詳細	月別の統計結果
③	印刷	レポートを印刷します。

20

Copyright © FutureSpirits Co.,Ltd All rights reserved.

3.3 週間レポートメール

週に1度（月曜日）に、1週間の解析結果をメールでお知らせします。

Web改ざん検知サービス 週間レポート

gred <gred@service.securebrain.co.jp> 1月27日 (1日前) ☆

To 自分

様、

いつも『Web改ざん検知サービス』をご利用いただきありがとうございます。
今週の Web 解析状況のレポートを送付させていただきます。

レポート期間: 2020/05/25 - 2020/05/31

登録ウェブサイト: <http://webchk.test.fsi.ne.jp/>

対象ドメイン: webchk.test.fsi.ne.jp

1週間でチェックした回数: 7回

改ざんを通知した回数: 0回

クロスドメインスクリプトの検知回数: 0回

貴社のウェブページ数(平均): 10ページ

詳細な情報や、週間レポート送信サービスの設定を変更する場合は、Web改ざん検知サービスにログインして「ユーザ情報の変更」で行ってください。

<https://www.gred.jp/saas/future-s/>

このメールにお心当たりのない方は、リンクをクリックせず、このメールを削除して下さい。
[このメッセージは、Web改ざん検知システムから自動的に送信されました。]

クロスドメインスクリプト検知した回数

4. 各種設定

各種機能の追加・変更等の設定方法をご説明します。

4.1 ユーザー管理

新しいユーザー（サブユーザー）を追加します。 管理画面へアクセスが可能なユーザーを 5 名まで追加登録できます。申込時に登録した初期ユーザーのみサブユーザーの登録が可能です。名前、ログイン ID は、半角英数字及び記号（@#%&?!）8 文字以上です。メールアドレス、アラートメールの受け取りの有無、アクセスの権限を入力して、「追加する」をクリックしてください。

① ヘッダーの「サブユーザー」をクリックします。

② サブユーザーのご担当者名（お名前）、ログイン ID、アラート用メールアドレス、アラートメールの受け取りの有無、アクセスの権限を入力し、「追加する」をクリックします。

※サブユーザーのご担当者名（お名前）、ログイン ID は半角英数字及び記号（@#%&?!）8 文字以上です。

※ログイン ID は、一度設定しますと変更はできませんのでご注意ください。

※弊社管理用として、サブユーザー（xxx@future-s.com）を事前に設定しております。
削除されないようご注意ください。

4.2 ユーザー情報の確認・変更

アラート用メールアドレス、名前の変更が行えます。

また、週間レポートメール、アラートメールの受け取りの有無、お知らせ通知、二要素認証もここで変更できます。

Web改ざん検知サービス

① ユーザー情報

サブユーザー パスワード ログアウト

ユーザー情報

ユーザー情報を変更します。 ②

ユーザーID(ログインID)	<div style="background-color: black; width: 100px; height: 1.2em;"></div>
アラート用メールアドレス	<div style="background-color: black; width: 150px; height: 1.2em;"></div>
ご担当名(お名前)	<div style="background-color: black; width: 150px; height: 1.2em;"></div>
遅延レポートメール通知	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
アラートメール通知 ③	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
お知らせ通知 ※アラート用メールアドレス に通知されます。	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効 <div style="margin-top: 5px;"> 重要なお知らせ [有効の場合は送信します] 機能追加・変更 サービス・システム仕様変更 メンテナンス など </div>
二要素認証 ④	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効

※ユーザーID(ログインID)は変更できません。

② 確認する

Web改ざん検知サービス

ユーザー情報 サブユーザー パスワード ログアウト

ユーザー情報

ユーザID(ログインID)	<input type="text"/>
アラート用メールアドレス	<input type="text"/>
ご担当者名(お名前)	<input type="text"/>
週間レポートメール通知	<input type="checkbox"/> 有効
アラートメール通知	<input type="checkbox"/> 有効
お知らせ通知	<input type="checkbox"/> 有効 [通知内容] -重要なお知らせ
二要素認証	<input type="checkbox"/> 無効

戻る 3 変更する

- ① ヘッダーの「ユーザー情報」をクリックします。
- ② 設定変更などを行い、「確認する」をクリックします。
※「お知らせ通知」は申込時に登録した初期ユーザーのみ設定できます。
- ③ 確認画面にて変更内容を確認し、「変更する」をクリックします。二要素認証を無効から有効へ変更すると以下の画面を表示します。

ユーザー情報

ユーザー情報を変更しました。

QRコードまたは登録用コードを使用して認証アプリ(Google AuthenticatorまたはMicrosoft Authenticator)へ登録してください。

⚠ 認証アプリへ登録する前に別ページへ遷移したり画面を閉じたりしないでください。

認証アプリへ登録せずにログアウトした場合は、ログイン画面からパスワードを再設定して二要素認証を無効にしてください。認証アプリの削除やデバイスの変更・紛失等によりログインできなくなった場合も、ログイン画面からパスワードを再設定して二要素認証を無効にしてください。



登録用コードを表示する

認証アプリへ登録完了



こちらの画面で QR コードまたは登録用コードを使用して認証アプリ（Google Authenticator または Microsoft Authenticator）へ登録してください。次回以降のログイン時には、ID とパスワードに加えて認証アプリで取得するワンタイムパスワードを使用してログインしてください

認証アプリへ登録せずにログアウトした場合は、ログイン画面からパスワードを再設定して二要素認証を無効にしてください。 認証アプリの削除やデバイスの変更・紛失等によりログインできなくなった場合も、ログイン画面からパスワードを再設定して二要素認証を無効にしてください。

4.3 パスワードの変更

ログインパスワードの変更は、ここから行ってください。

Web改ざん検知サービス

ユーザー情報サブユーザーパスワードログアウト

パスワード

現在のパスワード

新しいパスワード

新しいパスワード（確認用）

使用可能な文字は半角英数字と記号（`!~$%&'()*+,-./:;<=>?@`）で、8文字以上50文字以下。
全角文字、名前と同じものは使えません。
英文字と数字をそれぞれ1文字以上入れてください。

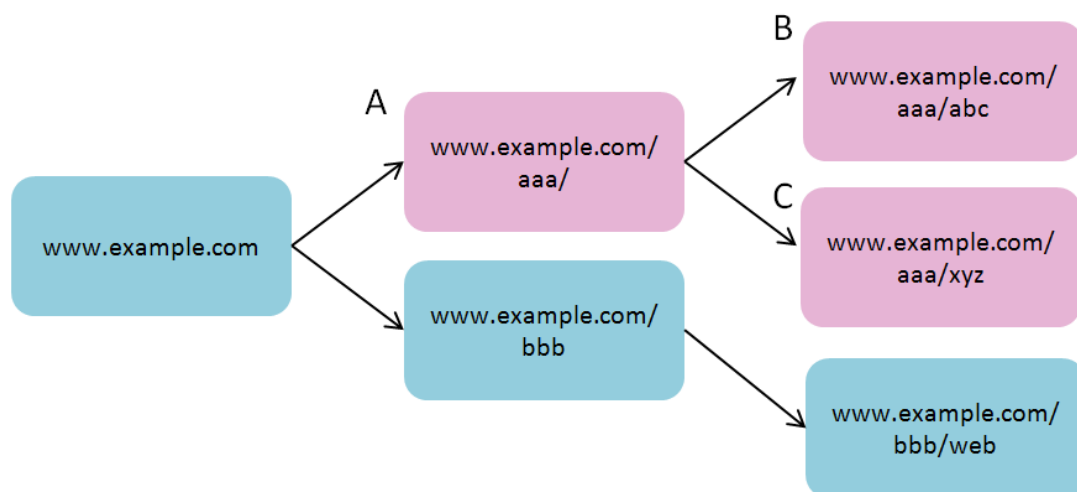
戻る

変更する

- ① ヘッダーの「パスワード」をクリックします。
- ② 現在のパスワードと新しいパスワードを入力し、「変更する」をクリックします。


4.4 除外 URL の登録

除外 URL の設定は、パス（ディレクトリ）指定を最大 100 個まで行うことができます。この機能は、指定したパス（ディレクトリ）以降をチェックしません。



※**A**(www.example.com/aaa/)を指定した場合、**B**と**C**も解析対象から除外されます。

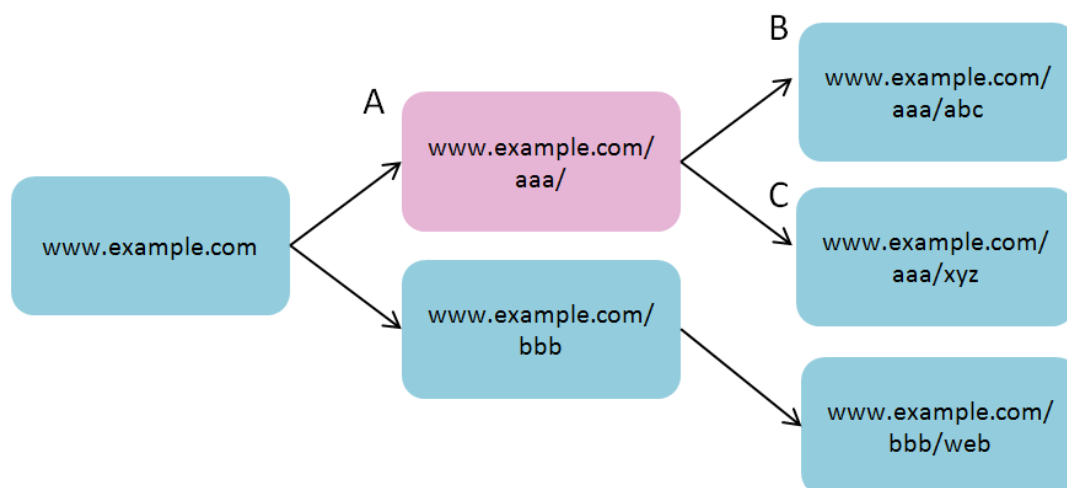


- ① 画面右上のをクリックし、「解析内容の設定」に遷移します。
- ② 画面中央のメニューから「除外設定」内の「除外 URL」をクリックします。
- ③ 「除外 URL に登録したいパス (ディレクトリ)」欄に任意の URL を入力し「登録する」をクリックします。

4.5 ホワイトリストの登録

ホワイトリストは、あらかじめ問題が無い事がわかっている URL を指定して、常に「OK」という判断を行うリストです。最大 10 個まで指定することが可能です。


このリストに指定した URL は解析ページ数としてカウントされますが、必ず「OK」という結果になります。ページにリンクがあった場合には、そのリンクから先もクロールします。ただし、このリストに指定したページのみ「OK」となる事に注意してください。



※A(www.example.com/aaa/)を指定した場合、このページは必ず「OK」という解析結果となります。 B と C は通常通り解析が行われます。



}


- ① 画面右上の  をクリックし、「解析内容の設定」に遷移します。
- ② 画面中央のメニューから「除外設定」内の「ホワイトリスト」をクリックします。
- ③ 「ホワイトリストに登録したい URL」欄に任意の URL を入力し「登録する」をクリックします。

4.6 監視の ON/OFF とウェブ解析対象階層の指定

Web 改ざん検知サービス自体の監視の ON/OFF を管理コンソールで行うことができます。また、解析対象の階層数を指定する事により、解析ページ数の調整が可能です。指定された階層以降はページが存在していても解析を行わず、解析対象ページ数としてもカウントいたしません。

監視の ON/OFF の設定



- ① 画面右上のをクリックし、「解析内容の設定」に遷移します。
- ② 画面中央のメニューから「基本設定」内の「監視の ON/OFF と基本設定」をクリックします。
- ③ 「監視の ON/OFF」欄の有効または、無効にチェックを入れて「変更する」ボタンをクリックします。
- ④ 「ウェブ解析対象階層の指定」欄に解析対象の階層数を入力し「変更する」をクリックします。

4.7 クロスドメインの許可設定

Web 改ざんチェックの「クロスドメインスクリプト管理・警告機能」は、自社サイト外に誘導するスクリプトがウェブページに埋め込まれた場合に「警告」を行います。あらかじめ任意で埋め込んだ外部に飛ばすスクリプトは、許可リストに登録してください。

解析内容の設定 https:// 監視中 ①

ホーム
解析履歴
レポート作成
解析内容の設定

現在の利用状況一覧を見る>>>

基本設定
監視のON/OFFと基本設定

除外設定
ホホワイトリスト
除外URL

クロスドメイン設定
クロスドメイン通知 ②

クロスドメイン検知 https:// 監視中 ①

ホーム
解析履歴
レポート作成
解析内容の設定
簡易脆弱性診断

クロスドメインスクリプトの検知機能 ☒ 有効 ☐ 無効 ③

適用する

許可リスト：クイック登録

最近のチェックで見つかったクロスドメインスクリプトから、許可リストに登録できます。

☐ すべてチェック
☐ https://hogehogelololo.jp/xxxxxxxxx.js ④

登録する

許可リスト：追加

許可リストにクロスドメインスクリプトが使用中のドメイン名、もしくはホスト名が登録できます。


許可リストに登録したい
クロスドメイン 登録する

許可リスト：編集

現在登録しているクロスドメインスクリプトの一覧です。登録している項目を削除する事もできます。

☐ すべてチェック
☐ www.securebrain.co.jp ⑤


削除する

- ① 画面右上のをクリックし、「解析内容の設定」に遷移します。
- ② 画面中央のメニューから「クロスドメイン設定」内の「クロスドメイン検知」をクリックします。
- ③ クロスドメインスクリプトを「有効／無効」の設定ができます。いずれかにチェックを入れます。
- ④ 「許可リスト：クイック登録」では見つかったクロスドメインスクリプトが表示されます。許可する場合は、ボックスにチェックを入れて「登録する」ボタンをクリックしてください。
- ⑤ 「許可リスト：編集」では登録している項目を削除することもできます。削除したい URL のチェックボックスにチェックを入れ、「削除する」ボタンをクリックします。

4.8 改ざん検知時のページ切り替え機能の設定

改ざんが確認された場合に、自動でページを切り替える機能が利用できます。



- ① 画面右上のをクリックし、「解析内容の設定」に遷移します。
- ② 画面中央のメニューから「オプション」内の「改ざん時切り替え機能」をクリックします。
- ③ お客様専用のタグが生成されます。 <html>タグのすぐ後に取得したタグを挿入して下さい。

■ タグのサンプル ※切り替え機能のタグはお客様ごとに異なります。

```
<script type="text/javascript" src="https://www3.gred.jp/saas/gred_checker.js?sid=1234">
</script>
```

お客様独自のメンテナンスページを表示させる場合には末尾に【&redirect.url=” 挿入したいメンテナンスページの URL “】を追加してください。

・切り替え機能設定

ページ切り替え機能の有効／無効を設定します。

切り替え機能設定 ☐ 有効 ☒ 無効

設定する

「有効」を選択すると切り替えに関するオプションが表示されます。

切り替え機能設定 ☒ 有効 ☐ 無効

切り替え機能適用範囲 ☐ 検知ページのみ ☒ 全ページ
上記のタグを挿入した解析対象ドメインのページのうち検知ページまたは全ページを切り替えます。

クロスドメインがあった場合 ☐ 切り替える ☒ 切り替えない

設定する

・切換え画面サンプル

【メンテナンス画面】

ただいまメンテナンス中です。

現在メンテナンスを行っているため、目的のサイトにアクセスすることができません。
ご迷惑をおかけいたしますが、お時間をおいて後ほどアクセスしてください。


もどる

※Web 改ざん検知サービスを解約した場合は、埋め込んだタグの削除をお願いします。

4.9 GRED 証明書の設定

サイトが改ざんされていないことを証明できる「GRED 証明書」が利用できます。この証明書をサイトに表示し、クリックすると検証結果が表示されます。



- ① 管理画面右上の  をクリックし、「解析内容の設定」に遷移します。
- ② 画面中央のメニューから「オプション」内の「GRED 証明書」をクリックします。
- ③ お客様専用のタグが生成されます。そのタグをページ内の GRED 証明書を表示させたい部分に挿入して下さい。

■ タグのサンプル※GRED 証明書のタグはお客様ごとに異なります。

```
<a href="https://www2.gred.jp/saas/ratingVerify.htm?sid=1^1^"
onclick="window.open('https://www2.gred.jp/saas/ratingVerify.htm?sid=1^1^',
'_blank', 'width=600,height=600,resizable=no,menubar=yes,toolbar=yes');
return false;" oncontextmenu="alert('この画像はコピーできません。');return
false;"><img height="40" border="0" width="85" src="https://www2.gred.jp
/saas/seal.gif?sid=1^1^" onerror = "javascript:src = 'https://www.gred.jp
```

[gred証明書の検証ページを見る](#)





表示内容

Web サイト名:

最終解析完了時間:

(最後にチェックした時間が表示されます)

解析結果:

(最後に解析を行った結果が表示されます)

※Web 改ざん検知サービスを解約した場合は、埋め込んだタグの削除をお願いします。

5. その他の機能・サービス

各種設定、サービスの提供は、管理コンソールより行います。

5.1 解析サイトの検索

複数の解析サイトを1つの管理コンソールで管理している場合、確認したい解析サイトの検索ができます。解析サイトが10以上ある場合に「検索・・・」リンクが表示され、クリックすると該当する解析サイトの管理コンソールへのリンク一覧が表示されます。



5.2 オンデマンドチェック機能

改ざんを検知し、修復を行った際に、問題がないか確認できるよう、即時チェックを行う機能です。1日に2回まで使用可能です。



5.3 GRED 証明書

この証明書をお客様のサイトに表示すれば、GRED によって守られている検証結果を表示させることが出来ます。HTML の `img` タグにより GRED 証明書のイメージを埋めこみます。タグをページ内の GRED 証明書を表示させたい部分に挿入して下さい。エンドユーザーが GRED 証明書をクリックすると、ポップアップ画面が表示され、そのページについて GRED での解析結果が表示されます。

GRED 証明書のタグの入手方法は「5.9 GRED 証明書の設定」をご覧ください。



クリックすると
以下の画面が開
きます。



5.4 パスワードをお忘れの場合

パスワードをお忘れによりログインできない場合に、ログインフォームの下にある『パスワードをお忘れの場合』リンクからパスワードを再設定することができます。あわせて二要素認証の設定を無効化することもできます。

Web改ざん検知サービス



ユーザーID

パスワード

ログインする

[パスワードをお忘れの場合](#)

Copyright (c) 2019 SecureBrain Corporation. All Rights Reserved.

5.5 ログイン履歴確認機能

これまでのログイン日時とそのログインを行った環境の IP を表示します。1 ページに最大 100 件が表示され、最長で過去 1 年分のログイン履歴を表示することができます。

ログイン履歴

⚠ ログイン履歴の表示期間は最長1年です。

ログイン日時	ログインIPアドレス
2022年07月15日 15:31:47	192.168.1.1
2022年07月15日 14:11:27	192.168.1.1
2022年07月15日 13:42:53	192.168.1.1
2022年07月14日 16:33:35	192.168.1.1
2022年07月14日 16:29:09	192.168.1.1
2022年07月14日 16:28:41	192.168.1.1

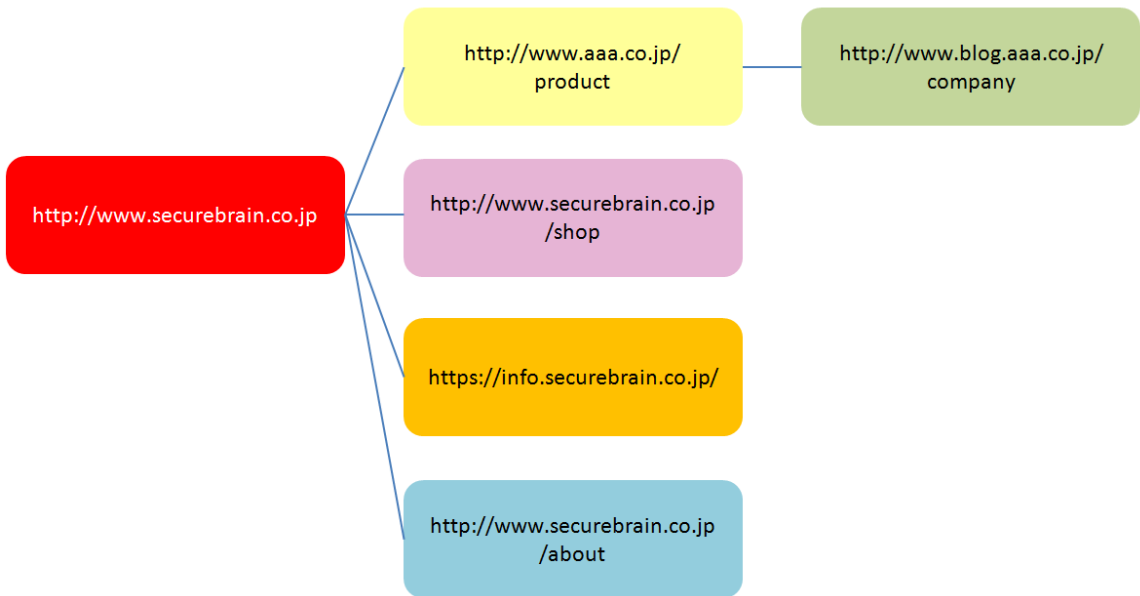
6. 解析する URL の絞り込み

6.1 解析開始 URL と対象ドメイン設定について



「Web 改ざん検知サービス」は、開始 URL からリンクをたどって解析をします。
解析したい Web サイトの開始 URL を決定してください。また、サブドメインのサイトも解析したい場合は、サブドメインも登録してください。1URL、5 ドメインまで設定可能です。

以下の例をあげて、対象ドメインの設定によって、解析対象がどのように変わるかを説明します。

各サイトのリンク状況は下記図の線で表しています。



ここでは解析開始 URL を「`http://www.securebrain.co.jp`」として説明します。

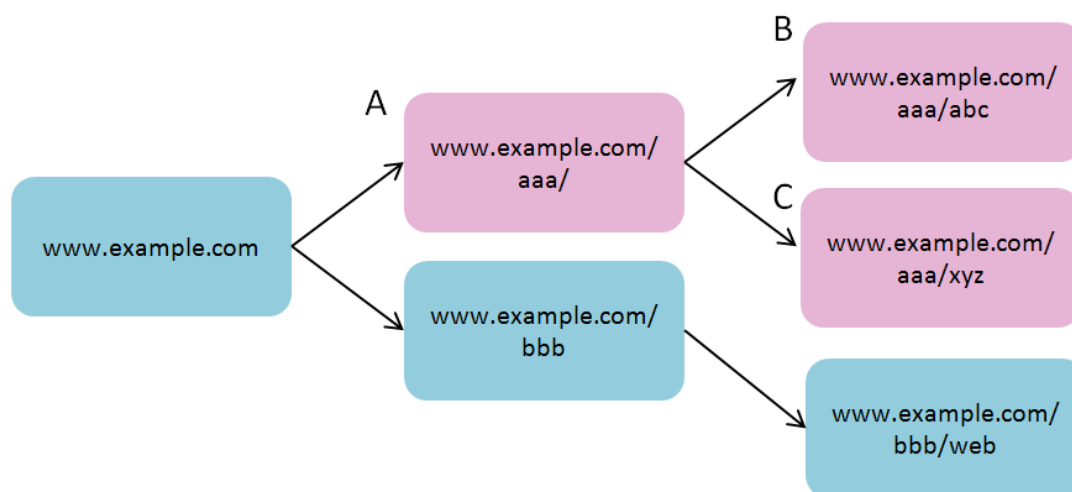
【設定方法①】対象ドメイン		解析対象
securebrain.co.jp	securebrain.co.jp が含まれる全てが対象になります。https サイトも対象になります。	
【設定方法②】対象ドメイン		解析対象
www.securebrain.co.jp	www.securebrain.co.jp が含まれる全てが対象になります。 https://info.securebrain.co.jp/は一致しないので対象外となります。	

【設定方法③】対象ドメイン		解析対象
securebrain.co.jp/shop	ディレクトリも設定することが可能です。一致したディレクトリのみ対象となります。	
【設定方法④】対象ドメイン		解析対象
securebrain.co.jp aaa.co.jp	対象ドメインを複数選択すると、それぞれのドメインが含まれる全てが対象となります。	
【設定方法⑤】対象ドメイン		解析対象
securebrain.co.jp www.aaa.co.jp	http://www.blog.aaa.co.jp は一致しないため対象外となります。	

6.2 解析する URL の絞り込み（除外 URL の登録）

除外 URL の設定が可能です。解析 URL 数を調節する際にお使いいただけます。パス（ディレクトリ）指定を最大 100 個まで行う事ができます。この機能は、指定したパス（ディレクトリ）以降をチェックしません。（この機能は、契約後、お客様が管理コンソールから設定します。設定方法は、「5.6 監視の ON/OFF とウェブ解析対象階層の指定」をご覧ください。）

※A(www.example.com/aaa/)を指定した場合、B と C も解析対象から除外されます。



6.3 解析する URL の絞り込み（ウェブ解析対象階層の指定）

解析対象の階層数を指定する事により、不要なページのスキャンを防止いたします。
指定された階層以降はページが存在していても解析を行わず、解析対象ページ数としてもカウントいたしません。（この機能は、契約後、お客様が管理コンソールから設定します。設定方法は、「5.6 監視の ON/OFF とウェブ解析対象階層の指定」をご覧ください。）