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

「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 ポイゾニングによる 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していただけます。

■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。

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

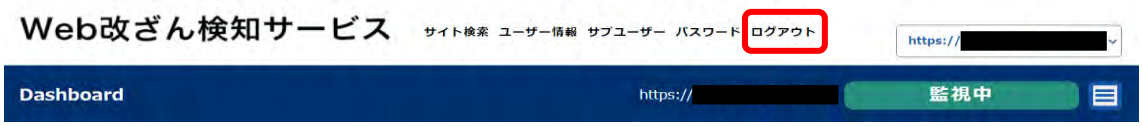
ログイン

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。

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。



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。

		改ざん検知された場合  改ざん検知が無い場合 
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）

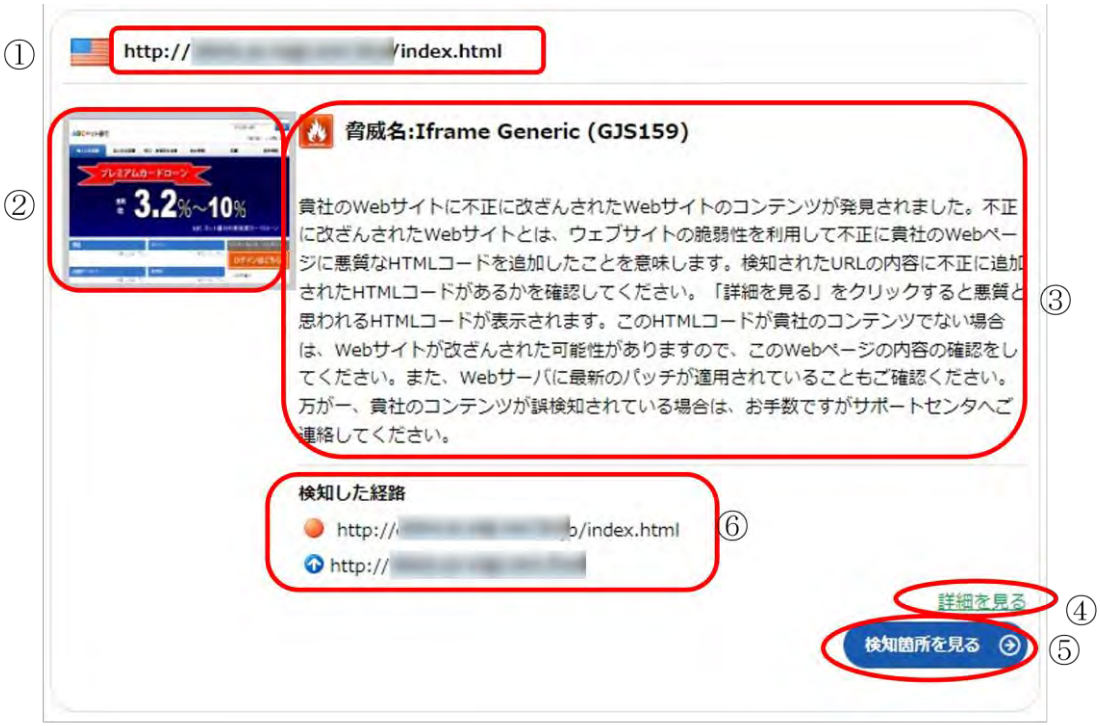
解析を行った結果、危険なサイトであると判定された場合、画面には赤の  マークが示されます。

「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。



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。

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。

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

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。

	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。

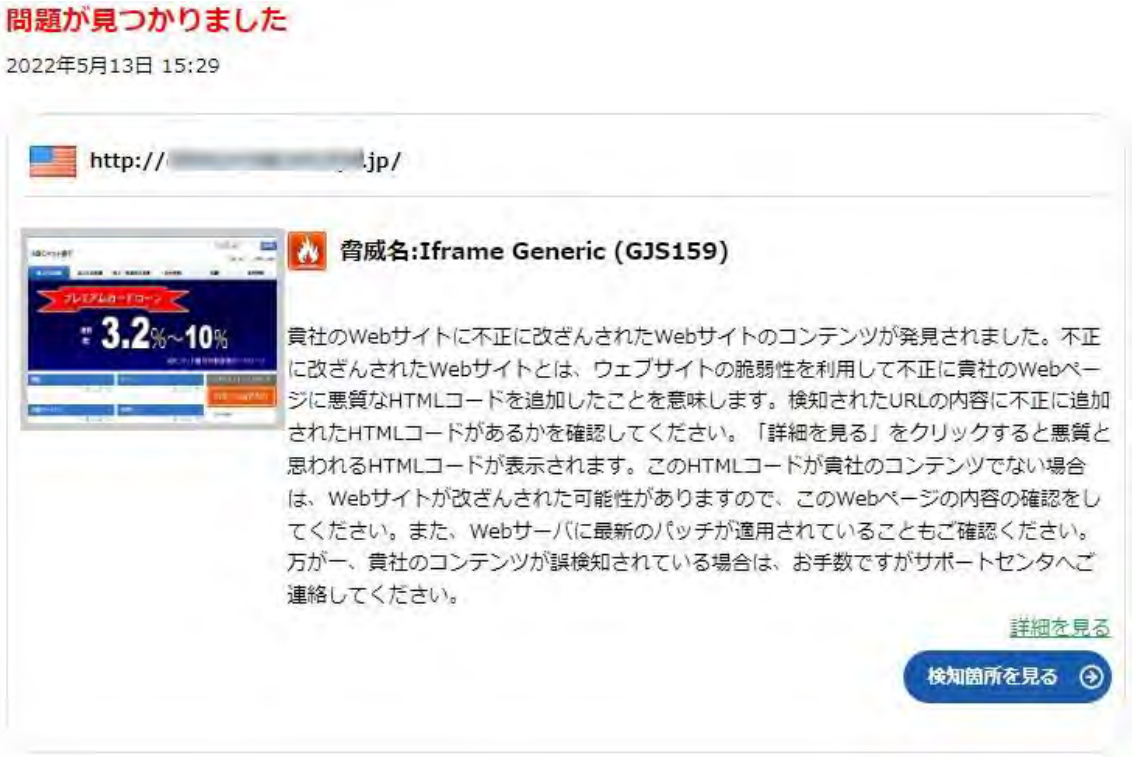
	項目名	内容
①	URL 表示	危険と判断された URL が表示されます。
②	概要	ファイルの概要
③	解析結果	挙動の詳細を表示します。

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



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。

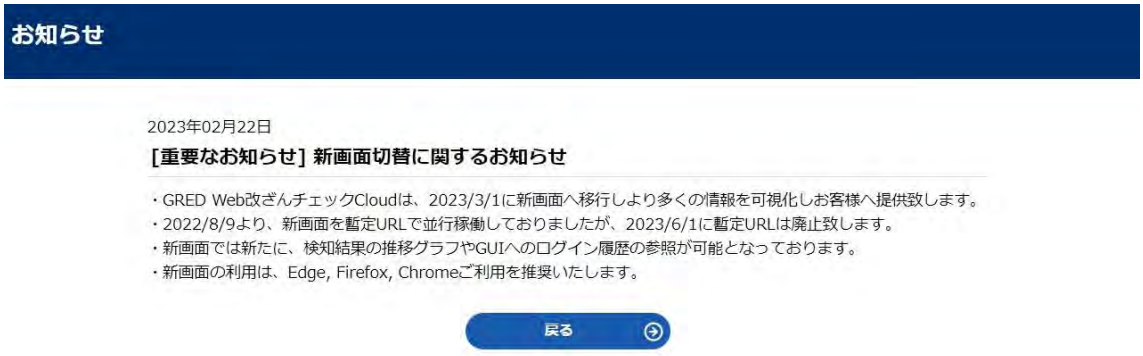
・Top ページのヘルスチェック検知時
・見た目変化検知時
・クロスドメインスクリプト検知時
・EXE 解析検知時
・タグ・JavaScript 変化検知時

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

■詳細ページ



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

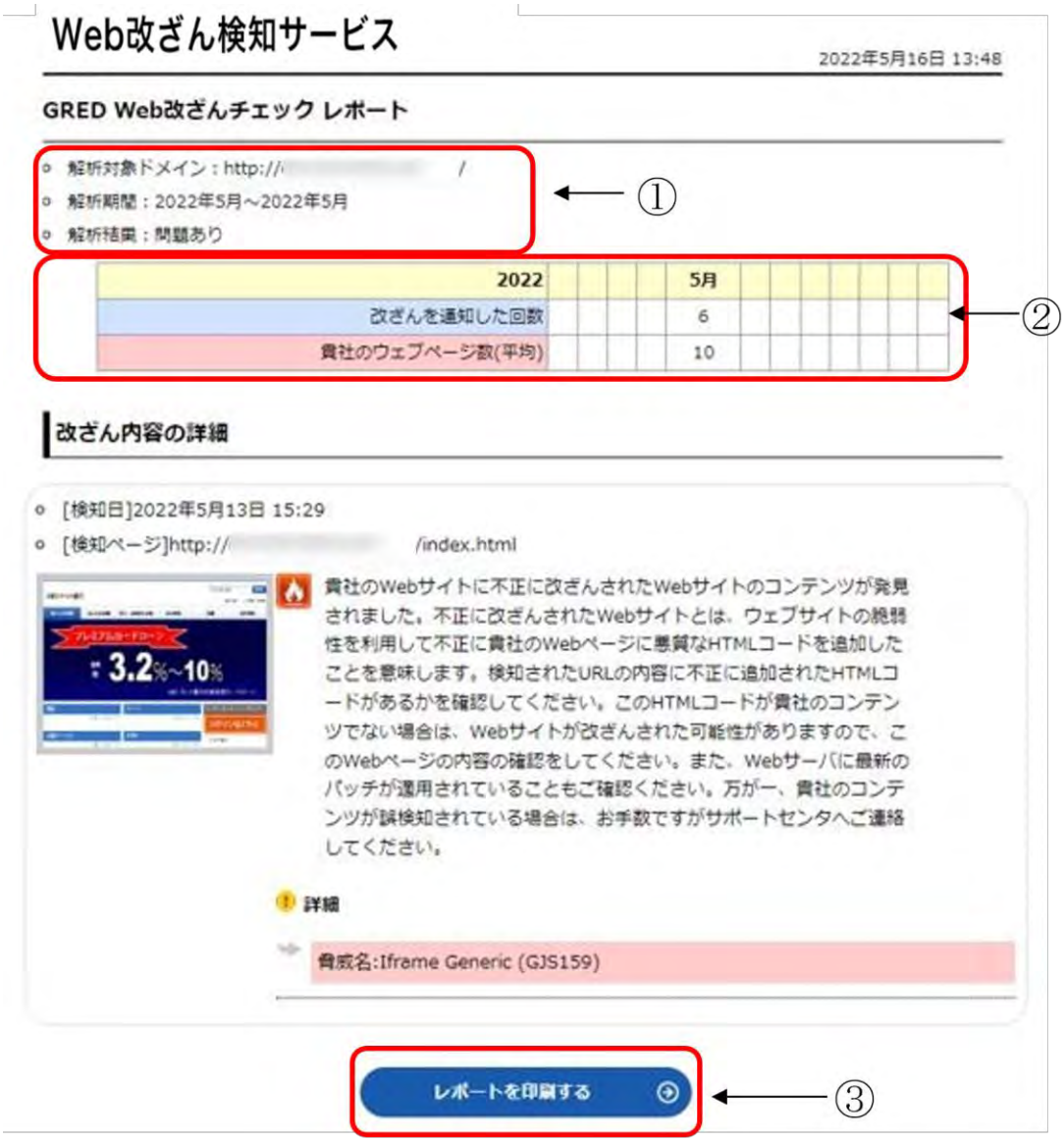
過去の解析を確認することができます。

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。

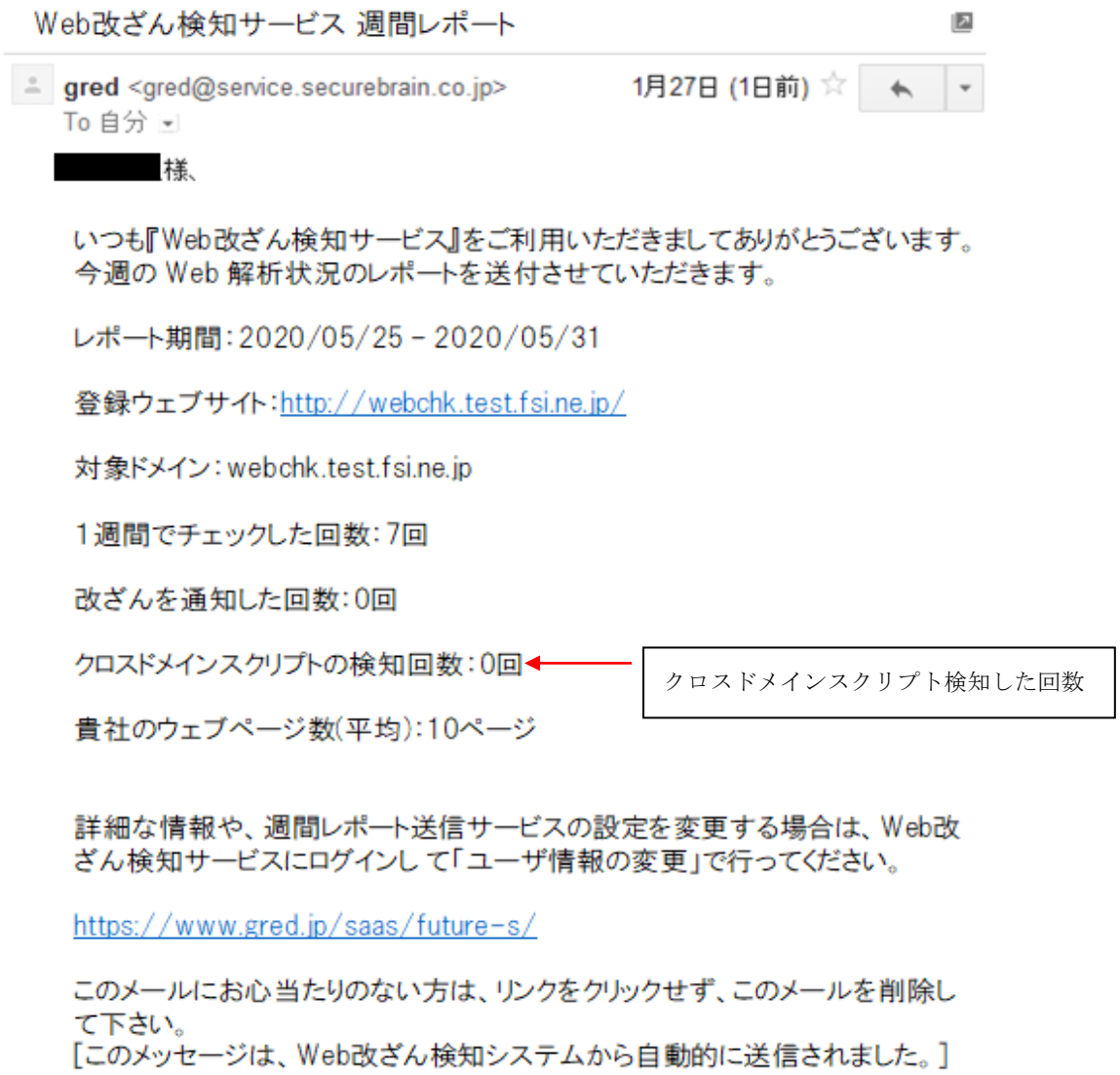
① 画面左上の  をクリックし、「解析内容の設定」に遷移します。
② 左側の「レポート作成」をクリックします。
③ 統計を出したい期間（1 か月単位）を指定し「レポートを作成する」ボタンをクリックすると、指定された期間の統計概要と月ごとの解析結果が表示されます。



	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。

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。



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。

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。

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。

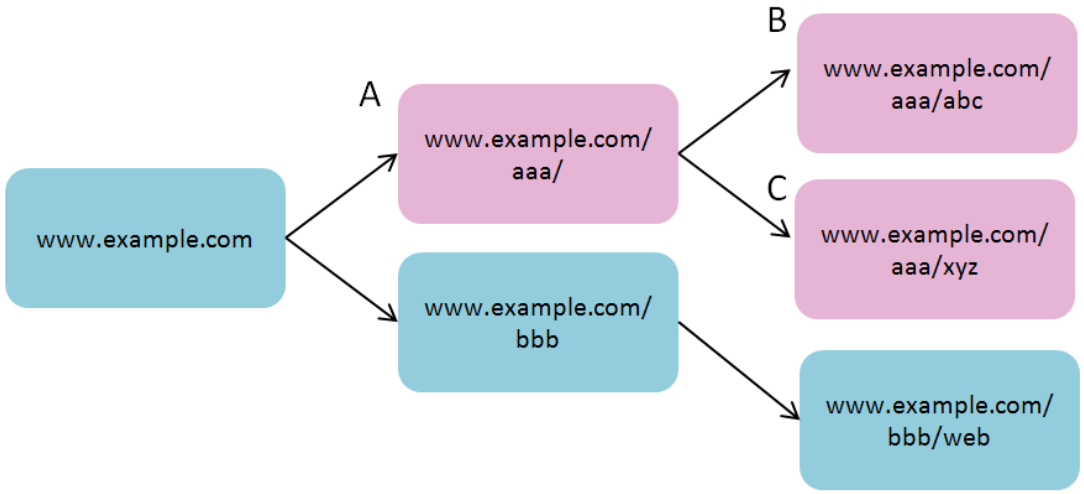
4.3 パスワードの変更

ログインパスワードの変更は、ここから行ってください。

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。

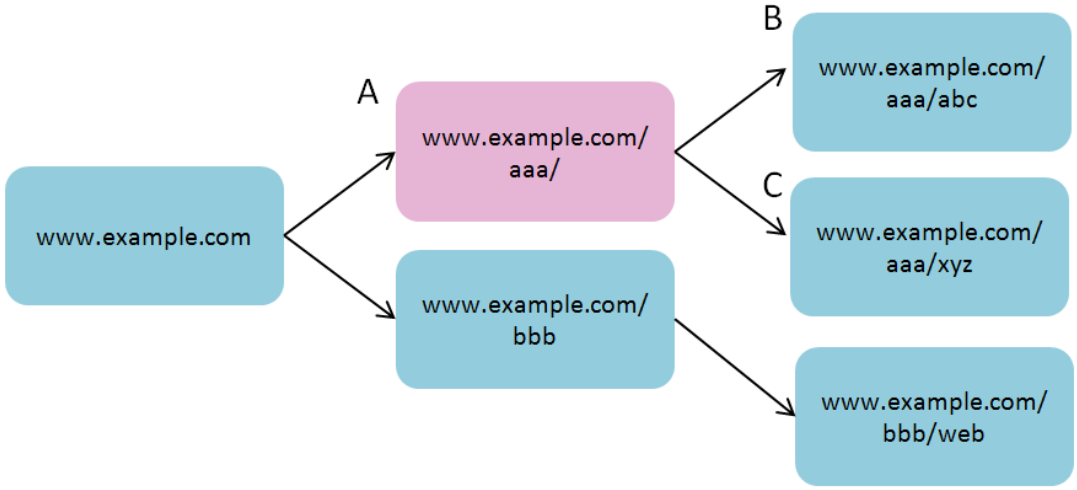


※A(www.example.com/aaa/)を指定した場合、B と C も解析対象から除外されます。

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リングします。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。

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。

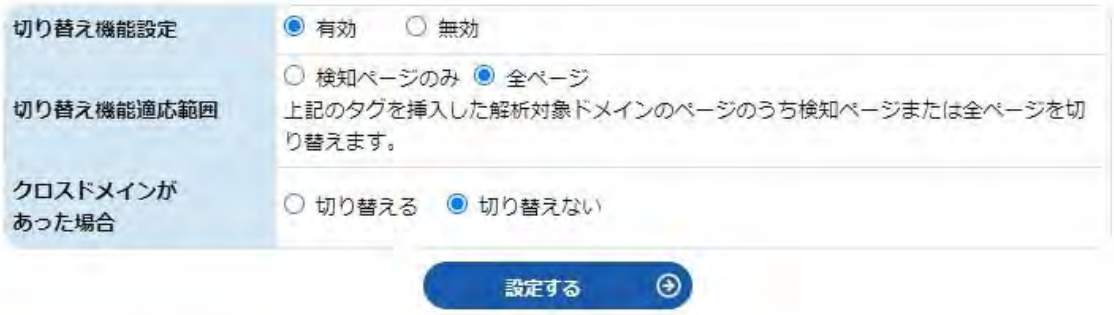
```
<script type="text/javascript" src="https://www3.gred.jp/saas/gred_checker.js?sid=[redacted]">
</script>
```

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。

「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。



・切換え画面サンプル

【メンテナンス画面】

※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=
onclick="window.open('https://www2.gred.jp/saas/ratingVerify.htm?sid=',
'_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=" 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。

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。

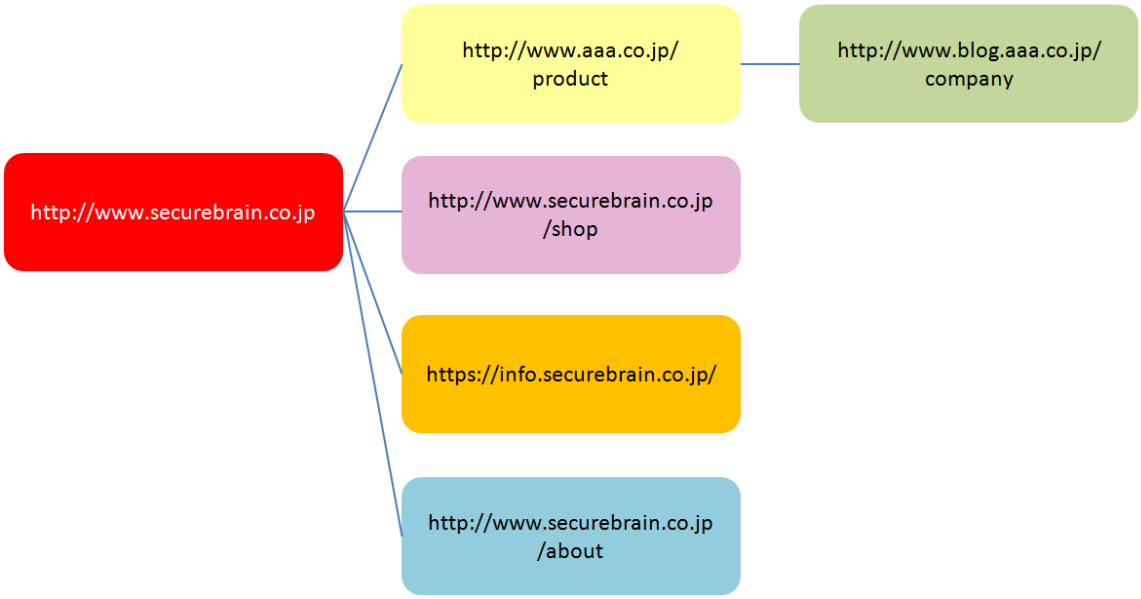
6. 解析する URL の絞り込み

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。

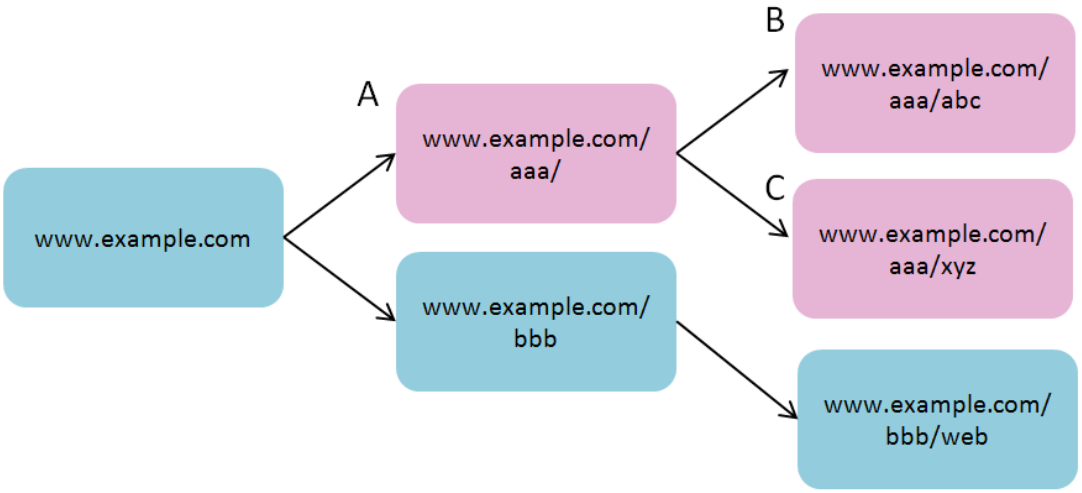
【設定方法①】対象ドメイン		解析対象
securebrain.co.jp	securebrain.co.jp が含まれる全てが対象になります。https サイトも対象になります。	
【設定方法②】対象ドメイン		解析対象
www.securebrain.co.jp	www.securebrain.co.jp が含まれる全てが対象になります。 https://info.securebrain.co.jp/は一致しないので対象外となります。	

【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。）**