GRED Web 改ざんチェック Cloud ユーザーガイド

第 18 版

（2025 年 3 月 7 日）

株式会社 日立システムズ

変更履歴

Version	日付	備考
8	2020/5/20	V3.8 対応
9	2022/2/28	V3.11 対応
10	2022/5/31	機能変更対応
11	2022/8/1	GUI リニューアル対応
12	2022/9/1	V3.12 対応
13	2023/4/5	V3.13 対応
13.1	2023/6/2	V3.13.1 対応
14	2023/9/29	V3.14 対応
15	2024/4/1	V3.15 対応
17	2024/11/1	V3.17 対応
17.0.1	2024/12/4	V3.17.0.1 対応
17.1	2025/1/10	V3.17.1 対応
18	2025/3/7	V3.18 対応

目次

1. はじめに

本書は、「GRED Web 改ざんチェック Cloud」の導入のための手順と、導入後の設定や機能について解説しております。不明点がございましたら、販売元のお問合せ窓口までご連絡をお願いします。

2. GRED Web 改ざんチェック Cloud サービス概要

「GRED Web 改ざんチェック Cloud」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、日立システムズの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。

2.1 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

2.2 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送信します。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。

2.3 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。

3. 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。

3.1 ログイン・ログアウト

ログイン

管理画面 URL 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。

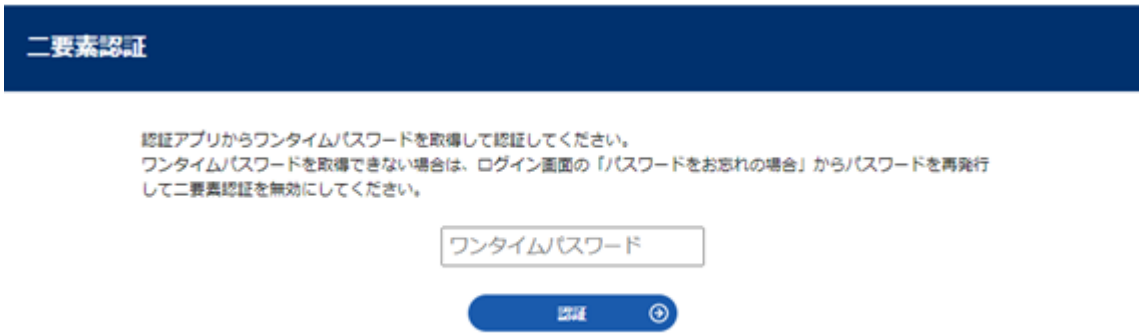
初めて管理コンソールにログインするには、お客様にてパスワードを設定する必要がございます。サービス開始後に送付される登録通知メールの手順に従い、パスワードを設定してください。パスワード設定後、パスワード設定完了の通知が届きますので、メールに記載しているログイン画面 URL よりログインして下さい。

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「3.9 お知らせ機能」を参照してください。

二要素認証

二要素認証を有効に設定することでIDとパスワードでの認証後にワンタイムパスワードを使用した二要素認証をします。スマートフォンにインストールした認証アプリからワンタイムパスワードを取得することでログインしてください。認証アプリは Google Authenticator または Microsoft Authenticator を利用してください。二要素認証の設定方法については「5.2 ユーザー情報の確認・変更」を参照してください。



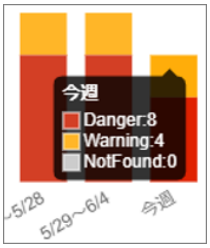
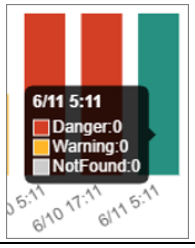
ログアウト

ヘッダーの右上にある『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。

3.2 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一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一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。

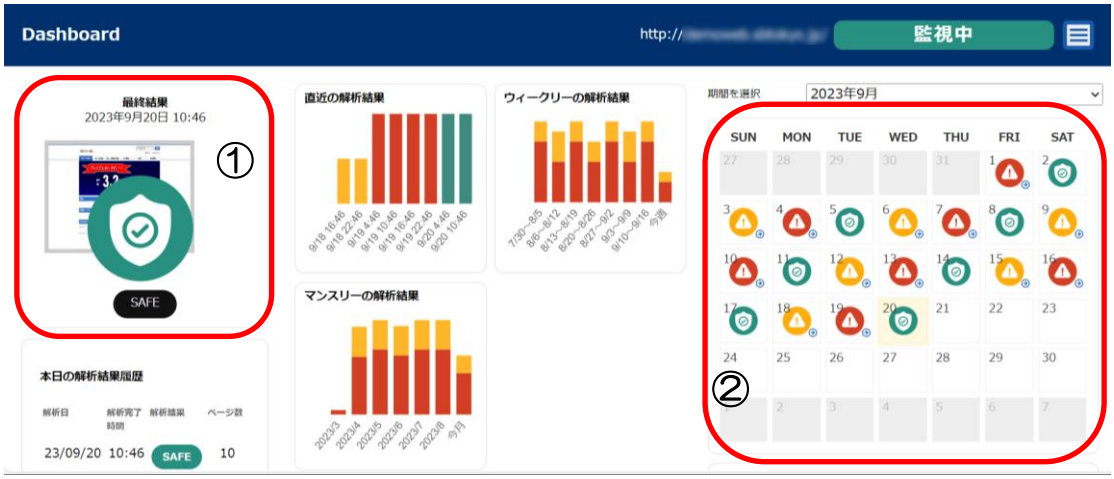
⑨	ツールチップ	各棒グラフにカーソルを合わせると解析結果の検知数が表示されます。 改ざん検知された場合  改ざん検知が無い場合 
⑩	ログイン履歴	前回のログイン日時を表示します。右側の「履歴」をクリックすると過去のログイン履歴を表示するページに遷移します。詳細は 6.5 の「ログイン履歴確認機能」を参照して下さい。
⑪	お知らせ	管理画面には最新のお知らせが表示されます。「一覧を見る」をクリックすると過去のお知らせを確認することができます。詳細は 3.9 の「お知らせ機能」を参照してください。

※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」参照して下さい。）

3.3 解析結果表示 緑（SAFE・安全）

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。

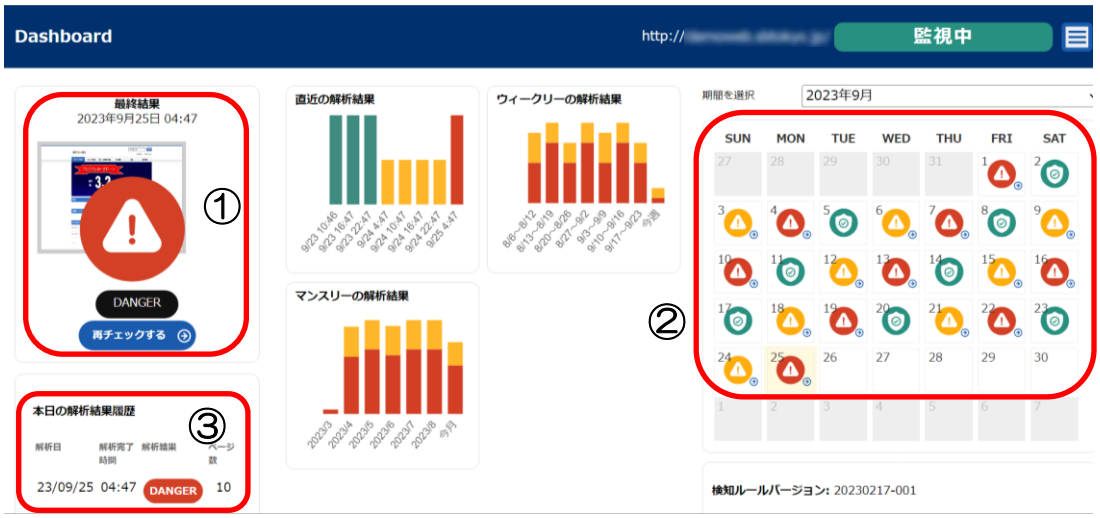


「SAFE」表示内容

	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  マークをカレンダー上に表示します。

3.4 解析結果表示 赤（DANGER・危険）

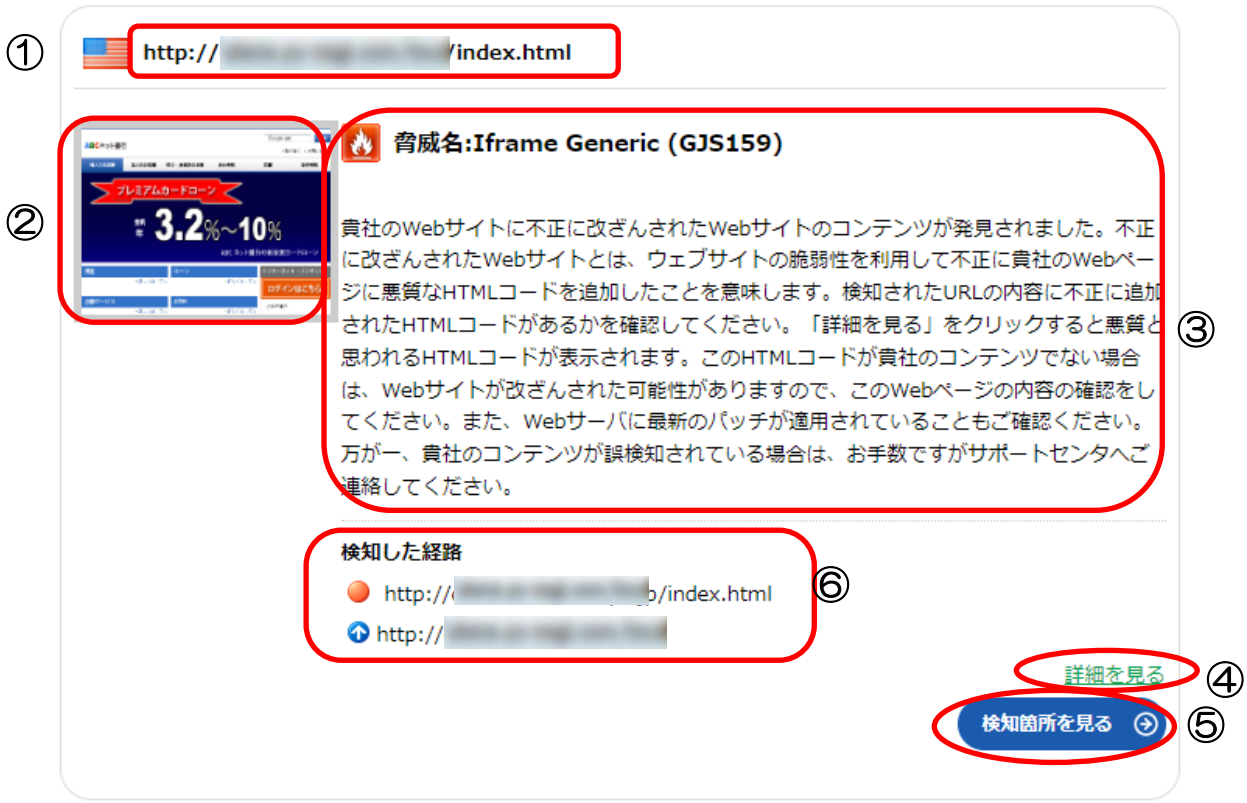
解析を行った結果、危険なサイトであると判定された場合、画面には赤の  マークが表示されます。



「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。



解析結果の表示内容

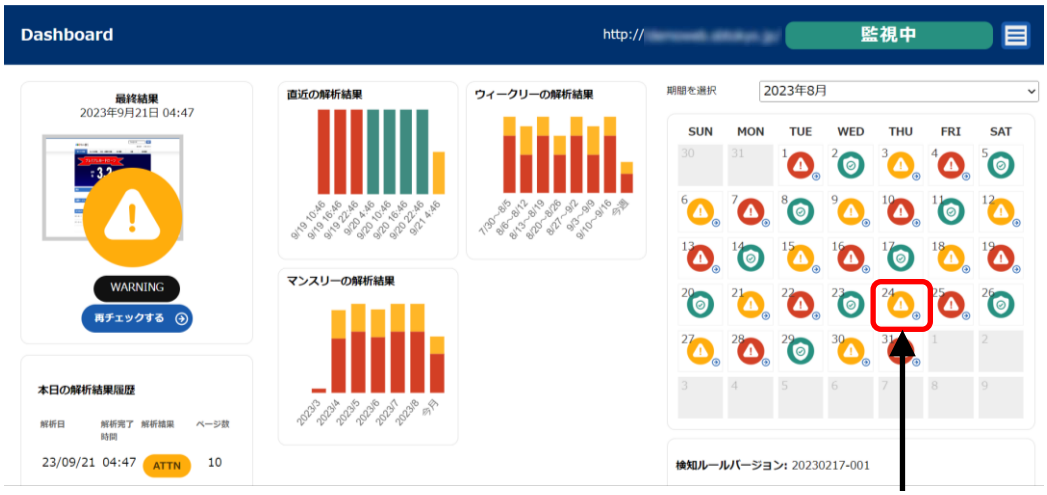
	項目名	内容
①	URL 表示	危険と判断された URL が表示されます。
②	判定画面	危険と判断されたサイトの画像が表示されます。
③	解析結果	どのような危険のあるサイトなのか表示します。
④	解析結果の詳細	問題のあるソースコードがハイライト表示されます。
⑤	検知した箇所を見る	検知箇所が可視化されます。
⑥	検知した経路	検知した箇所の経路が表示されます。 「脅威名」の名称が表示されている場合には、検知経路が表示されます。

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

3.5 解析結果表示 黄色（Warning・警告）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。

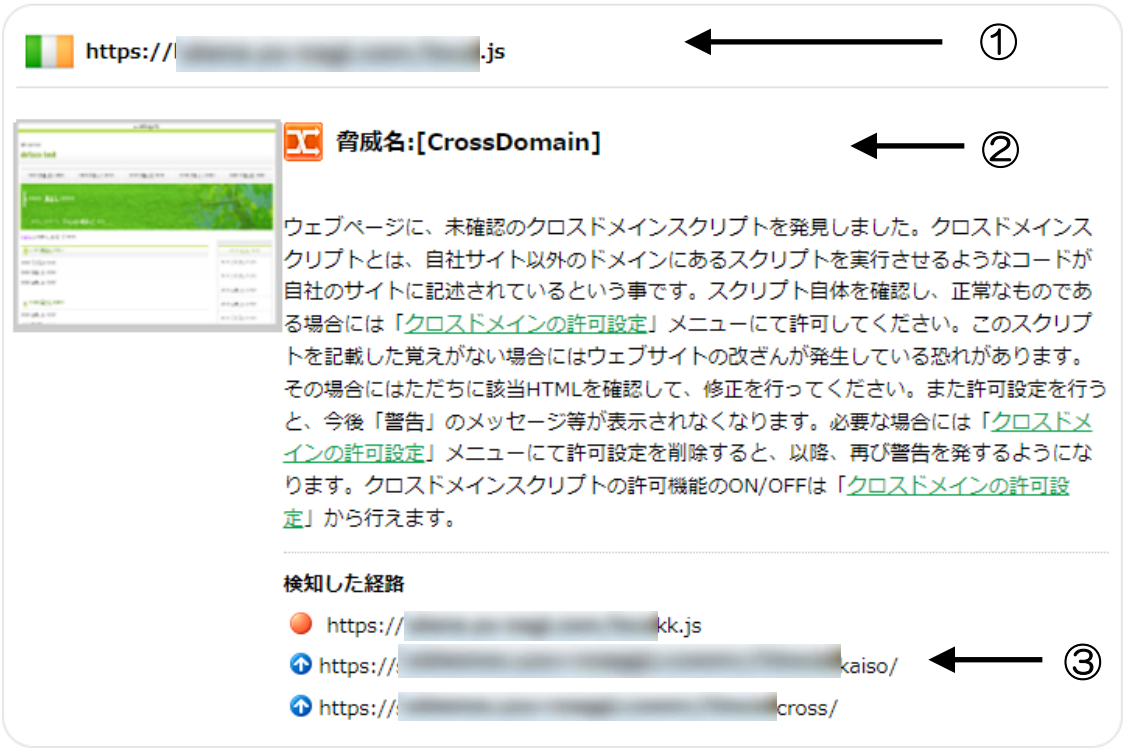


黄色のマークをクリックすると
詳細ページが表示されます。

■詳細ページ

注意が必要です

2022年5月4日 10:03



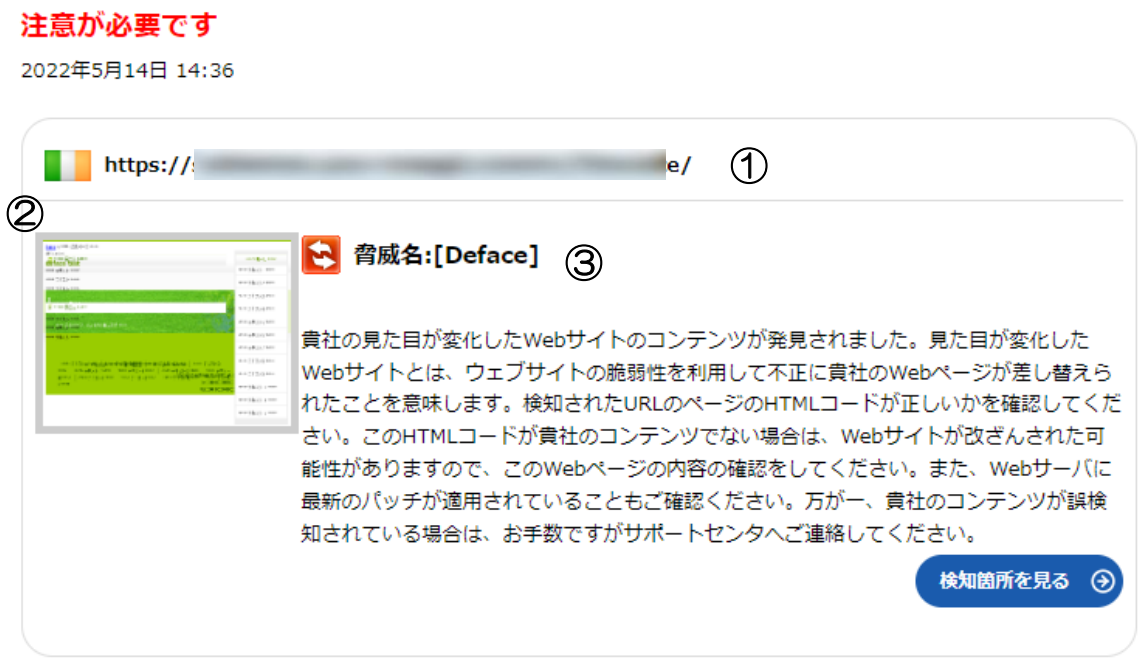
解析結果の表示内容

	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。）

3.6 解析結果表示 黄色（Warning・警告）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、検知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。

3.7 解析結果表示 黄色（Warning・警告）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。検知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。

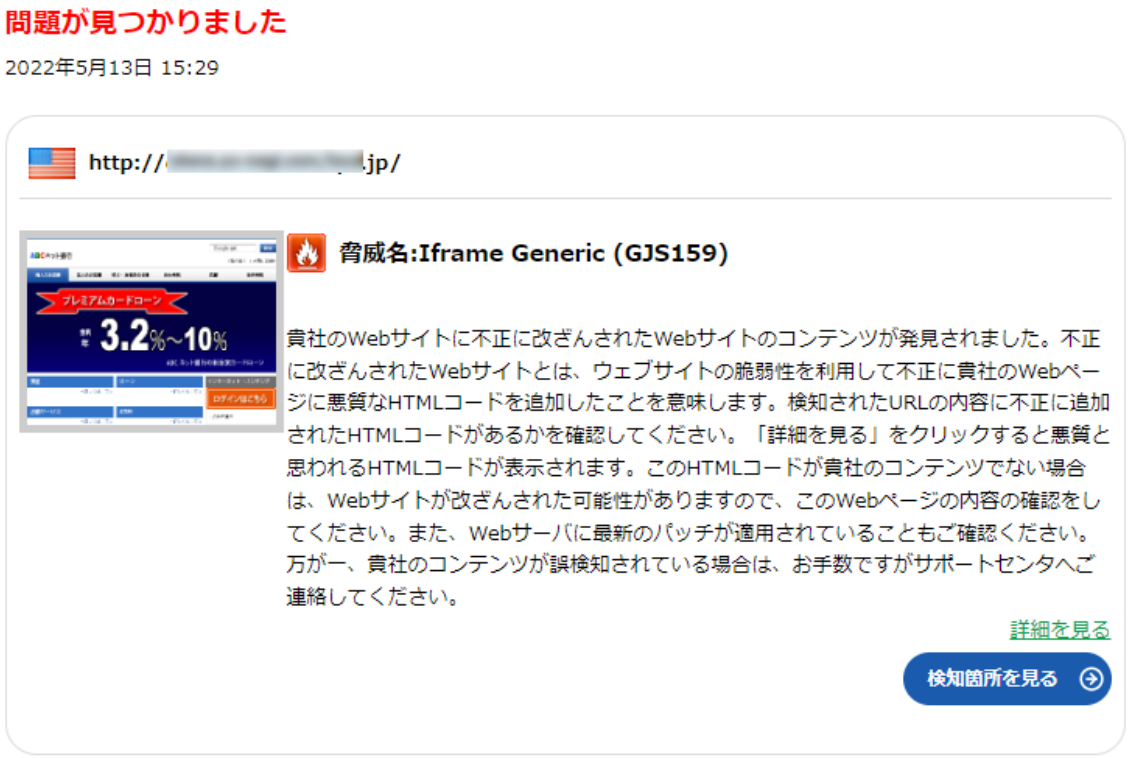
	項目名	内容
①	URL 表示	危険と判断された URL が表示されます。
②	概要	ファイルの概要
③	解析結果	挙動の詳細を表示します。

3.8 改ざん検知時のメール送信

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信されます。

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。
メール本文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 4 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。

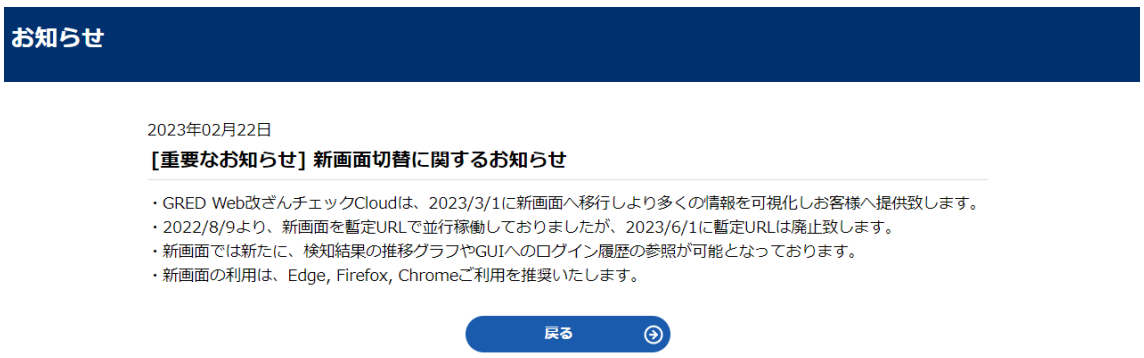
・Top ページのヘルスチェック検知時
・見た目変化検知時
・クロスドメインスクリプト検知時
・EXE 解析検知時

3.9 お知らせ機能

Gred Web 改ざんチェックからの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一件表示されます。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。

4. 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。

4.1 解析履歴

過去の解析を確認することができます。

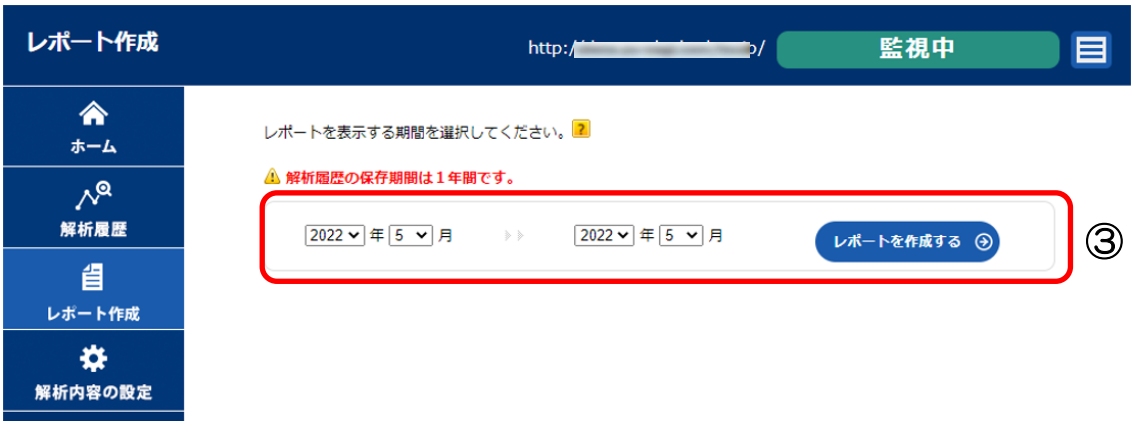
① 管理画面左上の  をクリックし、「**解析内容の設定**」に遷移します。

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。

4.2 レポート作成

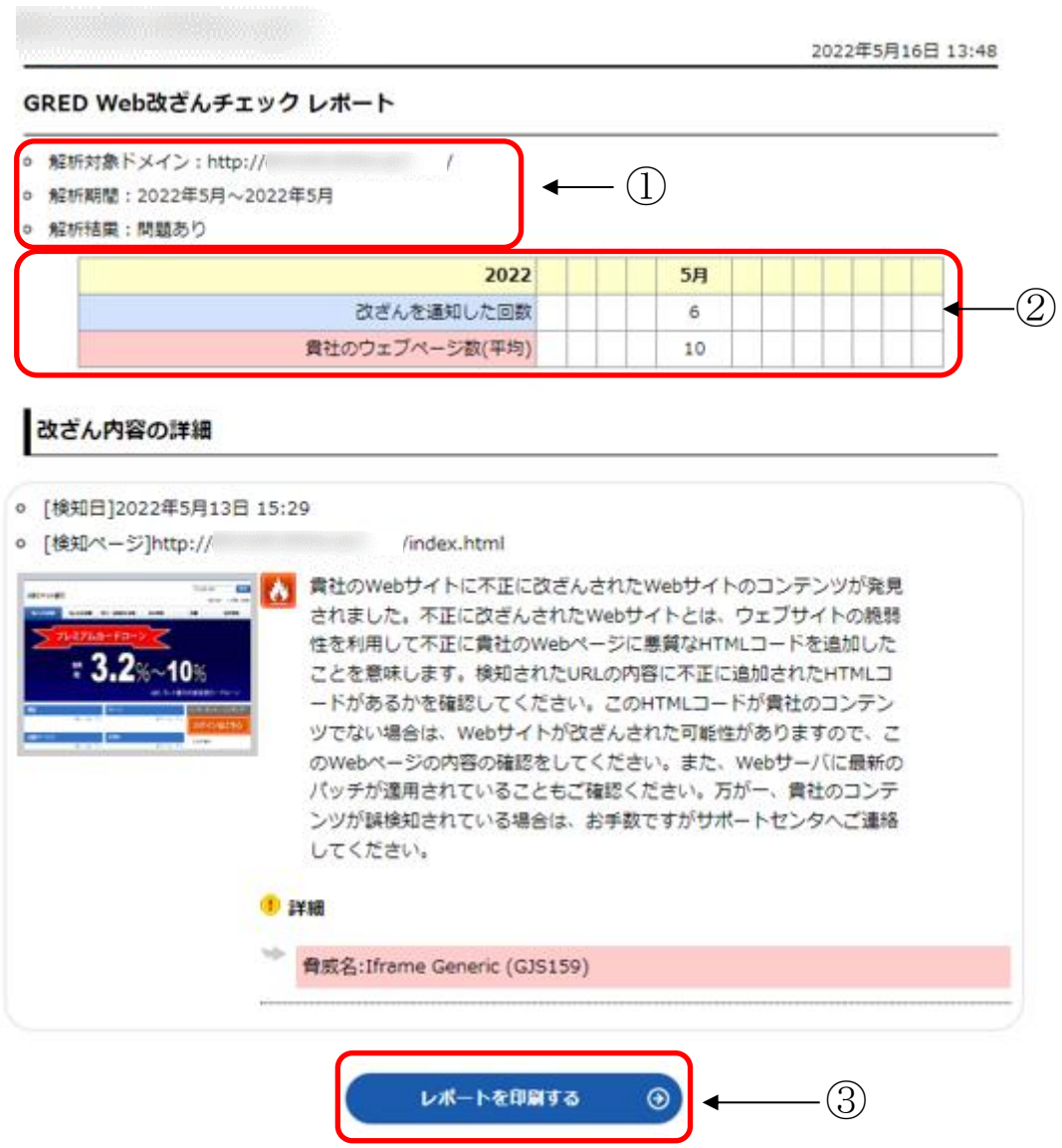
左側にある「レポート作成」をクリックします。
一定期間の解析結果の統計情報を見ることができます。



① 管理画面左上の  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。

4.3 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。

5. 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。

5.1 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。申込時に登録したメインユーザーのみサブユーザーの登録が可能です。

① ヘッダーの「**ユーザー情報**」をクリックします。

② 「**サブユーザーの情報**」をクリックします。

③ サブユーザーご担当者名（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。

※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。

5.2 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、二要素認証もここで変更できます。

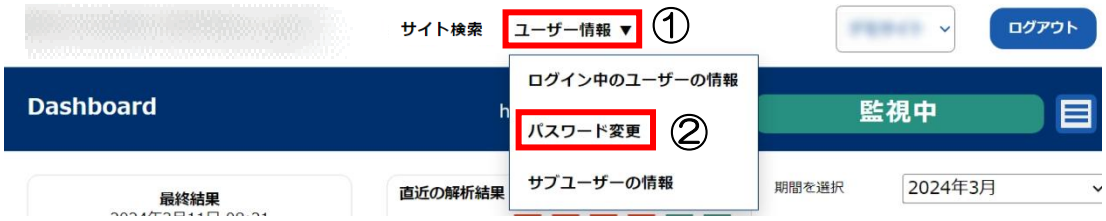
① ヘッダーの「**ユーザー情報**」をクリックします。
② 「**ログイン中のユーザーの情報**」をクリックします。
③ 設定変更などを行い、「**確認する**」をクリックします。
※「お知らせ通知」は申込時に登録したメインユーザーのみ設定できます。
④ 確認画面にて変更内容を確認し、「**変更する**」をクリックします。

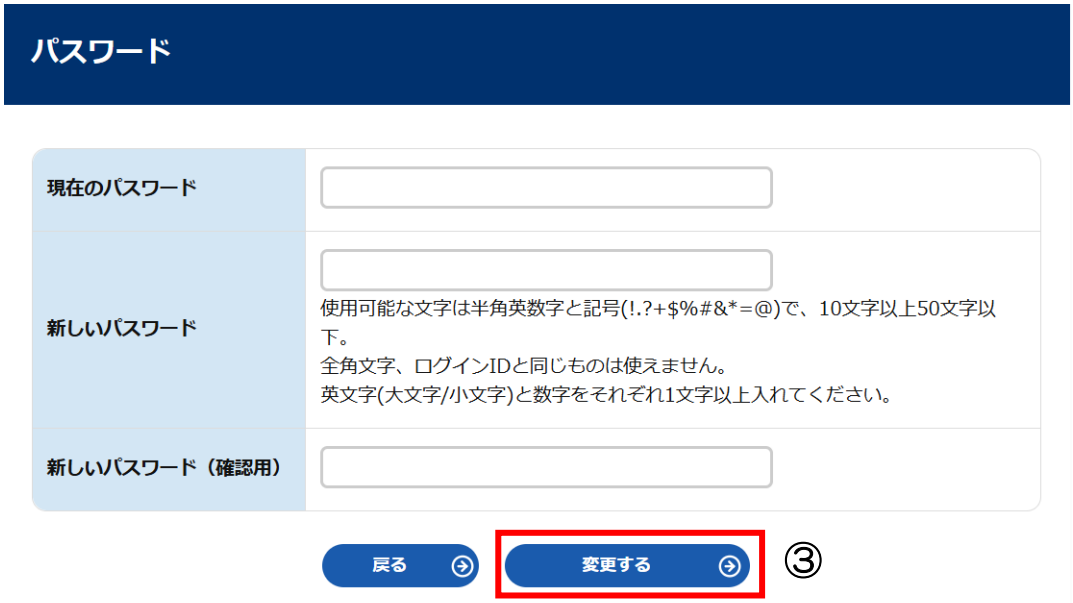
二要素認証を無効から有効へ変更すると以下の画面を表示します。

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。

5.3 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。





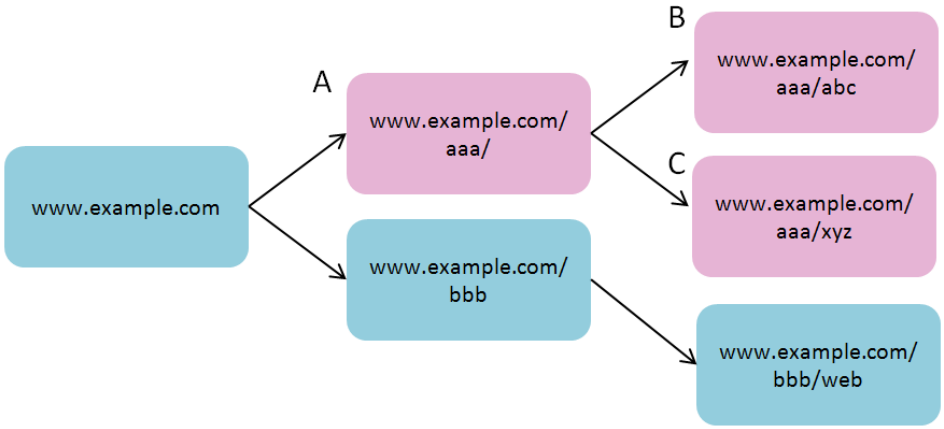
① ヘッダーの「**ユーザー情報**」をクリックします。

② 「**パスワード変更**」をクリックします。

③ 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。

5.4 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。

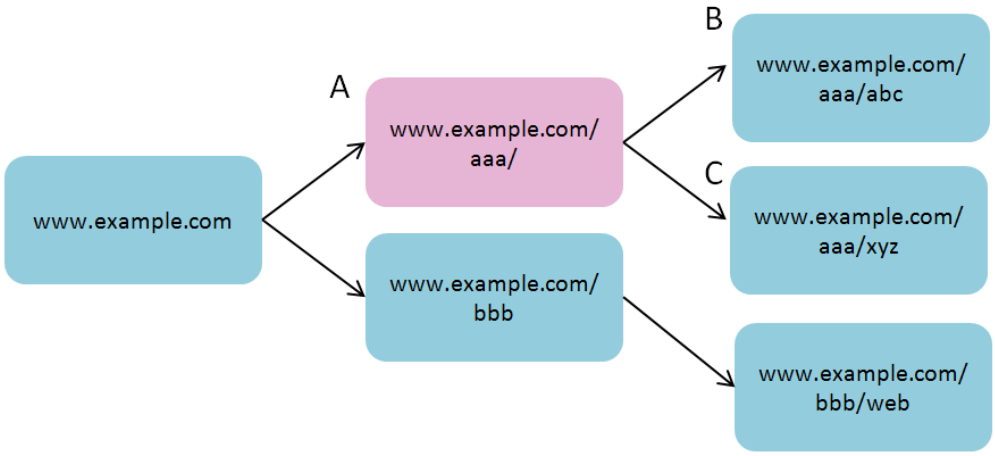
① 管理画面左上の  をクリックし、「**解析内容の設定**」に遷移します。

② 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。

5.5 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 管理画面左上の☰をクリックし、「**解析内容の設定**」に遷移します。
② 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。

5.6 監視の ON/OFF とウェブ解析対象階層の指定

GRED Web 改ざんチェック Cloud 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 画面左上の  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 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。

5.7 クロスドメインの許可設定

ウェブ改ざんチェックの「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 画面左上の  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の「**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。

5.8 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 管理画面左上の  をクリックし、「**解析内容の設定**」に遷移します。

② 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・HEAD タグのすぐ後など、出来るだけソースの上方に挿入する事をお勧めします。

■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。

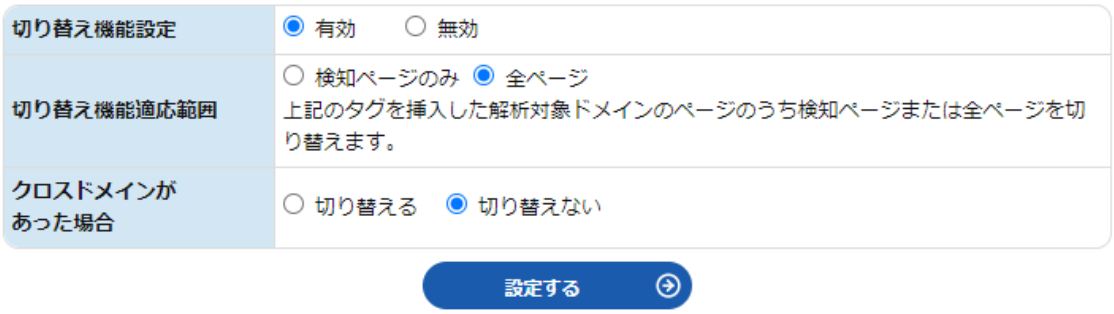
```
<script type="text/javascript" src="https://www3.gred.jp/saas/gred_checker.js?sid=[redacted]">
</script>
```

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】

※ウェブ改ざんチェックのサービスを終了した場合は、埋め込んだタグの削除をお願いします。

5.9 GRED 証明書の設定

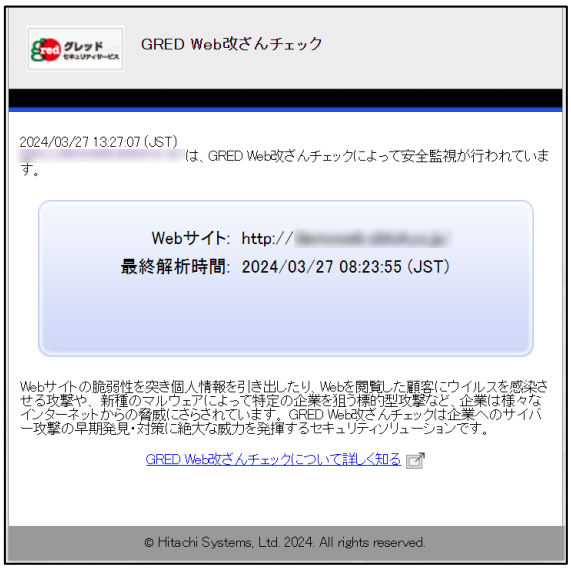
サイトが改ざんされていないことを証明できる「GRED 証明書」が利用できます。この証明書をサイトに表示し、クリックすると検証結果が表示されます。

① 管理画面左上の  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=[redacted]"
onclick="window.open('https://www2.gred.jp/saas/ratingVerify.htm?sid=[redacted]',
'_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=[redacted]" 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 ）

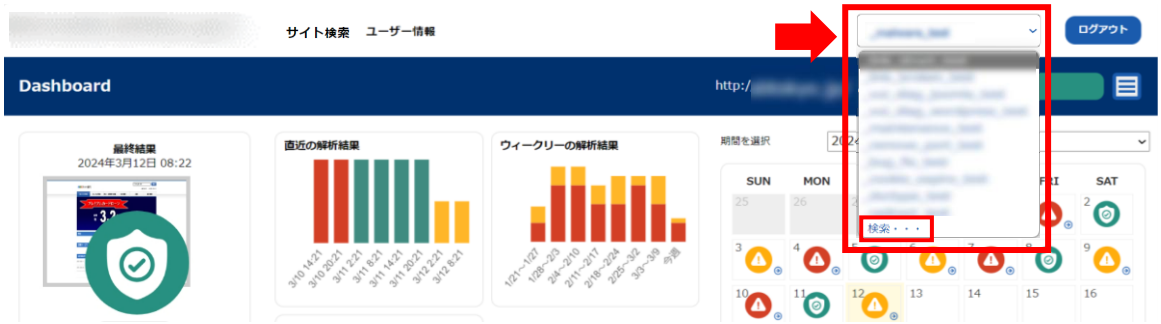
※GRED Web 改ざんチェック Cloud のサービスを終了した場合は、埋め込んだタグの削除をお願いします。

6. 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。

6.1 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。



ヘッダーの「サイト検索」からもアクセスが可能です。

6.2 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。

6.3 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「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。

6.4 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。

6.5 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