

Web改ざん検知オプション 利用マニュアル

第2.3.1版 2024/7/11

NTTコミュニケーションズ株式会社

はじめに

Web改ざん検知サービスは、お客さまが作成、管理されているウェブサイトが安全で あることを確認するためのサービスとなります。解析対象のドメインと URL を登録 することにより、解析が実行され、改ざんが検出された場合は、ご登録いただく管理 者様にアラートメールが送信されます。

1.パスワードの発行

ここでは、
 管理画面へログインするためのパスワードを発行する手順をご案内します。

(1) 『サービス登録完了のお知らせ』メールに記載されている 「パスワード設定用認証URL発行」用のリンクをクリックします。

0000様
「GRED Web改ざんチェック」サービスへようこそ! 本サービスはWeb改ざんを検知し、迅速な対応を可能にするセキュリティサービスです。
この電子メールは、「GRED Web改ざんチェック」サービスの登録が完了したことをお伝えするものです
のです。 ログイン画面からログインするには、お客様がパスワードを設定する必要がございます。 本人確認のため、下記のURLにアクセスしパスワード設定用認証URLを取得しパスワードを設定して ください
認証URLの取得にはユーザIDが必要です。
パスワード設定用認証URL発行: https://www.gred.jp/saas/requestpw?partid=0 (1)
ユーザID : 0000 (2)

(2) 「パスワード設定用認証URLの発行」画面が表示されたら、 メールに記載されている [ユーザーID] を入力して [送信] をクリックします。

バスワード設定用認証URLの発行					
パスワード設定用 認証URLを発行します。ユーザID(ログインID)を入力 し送信ボタンをクリックしてください。登録済みのアラート用メールアドレス に認証URLが送付されます。					
ユーザID(ログイ>ID):					
	戻る 送信				

※『パスワード設定用認証用URLの発行』メールが送信されます。

(3) 『パスワード設定用認証用URLの発行』メールに記載されている 「認証URL」をクリックします。

0000様

パスワード設定用認証用URLをお知らせします。 24時間以内に下記のURLよりパスワードを設定して下さい。

パスワード設定用認証URL:

https://www.gred.jp/saas/ChangePwd.action?partid=0&lang=ja&key=Oukvw6daHJLdoexKBdLg sBUSTZKQNW1YfoPcdkgzn0iOtQdT%2FQRgcw%3D%3D

※上記URLの有効期限は24時間です。 有効期限切れとなった場合は、パスワード設定用認証URL発行画面より、 再度パスワード設定用認証URLを発行して下さい。

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。 本メールは、送信専用メールアドレスからお送りしています。

(4) 任意のパスワードを入力して [保存] をクリックします。



(5) 『パスワード設定完了のお知らせ』メールが送信されます。 メールに記載されている「ユーザーID」と、設定した「パスワード」で ログインしてください。

0000様

パスワードの設定が完了しました。 ログイン画面のURLをお知らせします。 ログインするには、設定完了したパスワードとユーザIDが必要です。

ログイン画面URL: https://www.gred.jp/saas/?partid=0

ユーザID : 0000

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。 本メールは、送信専用メールアドレスからお送りしています。

※ ログイン方法は「<u>2.管理画面へのログイン</u>」をご参照ください。

2.管理画面へのログインとログアウト

2.1 ログイン

『サービス登録完了のお知らせ』メールに記載されている[ユーザーID]と、 「<u>1.パスワードの発行</u>」で設定した[パスワード]でログインしてください。

ログインURL: <u>https://www.gred.jp/saas/bizmw</u>

	ユーザーIC パスワード	。 ログインする パスワードをお忘れの場合							
Bizメール&ウェブ Web改ざん検知オプション ^ッ	サイト検索 ユーザー情報 サブユーザー バス・	2-6 02				https://)	Herene	com 🗸
Dashboard	al Coutoff and	http:	5://	2	.com	/	監視	.中	
2023#2/9228 10:24	7 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2		SUNDAY 20 5 © 12 © 10 © 26 5 452/4	MONDAY 30 6 13 20 21 20 21 20 21 20 21 22 30	 TUESDAN 31 7 3 14 2 21 	WEDNES 1 8 15 22 3 11-001	2 3 2 3 2 3 2 4 2 2 2 4 2 4 2 4 2 4 2 4 2 4 2 4 2 4	FRIDAY 3 20 10 3 10 24 3 10	SATURDAN 4 3 11 3 18 3 25 31 11 19 3 19 3 10 4 10 4 10 10 4 10 4 10 10 4 10 4 10 10 4 10 4 10 4 10 10 10 10 10 10 10 10 10 10

- ログインする際の二要素認証を有効にする方法は、「<u>3.5 二要素認証</u>」をご参照く ださい。
- 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「<u>8.お知らせ機能</u>」をご参照ください。

管理画面からログアウトするには、画面上部の[ログアウト]をクリックします。

Bizメール&ウェブ Web改ざん検知オプション	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
Dashboard		
是放社田	直近の解析結果	ウィークリーの解析結果

3.ユーザーの管理

3.1 ユーザー情報の確認・変更

ユーザー情報を確認・変更する場合は、画面上部の[ユーザー情報]をクリックします。

以下の項目が変更可能です

- アラート用メールアドレス
- ご担当者名(お名前)
- ・ 週間レポートメール通知
- アラートメール通知
- お知らせ通知
- 二要素認証
- ※ [ユーザID(ログインID)] は変更できません。

W	SIZ メール & フェフ eb改ざん検知オプション	ユーザー情報 サプユーザー パスワード ログアウト		
Ч	ユーザー情報			
	ユーザー情報を変更します。 🔋			
	ユーザID(ログインID)	ma2rttum		
	アラート用メールアドレス	Transplan angent care		
	ご担当者名(お名前)	#~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~		
	週間レポートメール通知	● 有效 ○ 無効		
	アラートメール通知 🎴	● 有効 ○ 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	 ● 有効 ○ 無効 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 		
	二要素認証 🔼	◉ 有効 ○ 無効		
	※ユーザID(ログインID)は変更できま	せん。 戻る ③ 確認する ④		

二要素認証を有効にする場合は「3.5 二要素認証」をご参照ください。

3.2 サブユーザーの追加

サブユーザーを追加するには、画面上部の [サブユーザー] をクリックします。

※管理画面へアクセスが可能なサブユーザーを5名まで追加登録できます。 ※サブユーザーの登録は、お申込時に登録した初期ユーザーのみが実行できます。 ※ [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。

W	ミュメール&ウェブ eb改ざん検知オプション	ユーザー情報 サブユーザー パスワード ログアウト
ታ	ブユーザー	
	サブユーザーを追加します。 🖻	(1)
(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	※こちらのアドレスにサブユーザー登録完了の通知メールが届きます。
	アラートメール通知	● 有効 ○ 無効
	アクセスの権限	□全て選択 └. □ https:// .com
		<u>追加する</u> (2)
	サブユーザー情報の変更・削除	
		変更する

(1) 各項目を入力します。

(2)入力内容に間違いがないことを確認の上 [追加する] をクリックします。

※手順(1)で入力した「アラート用メールアドレス」宛に『サブユーザー登録の通知』メールが送信されます。通知メールの手順に従いパスワードを設定した後、ロ グインをお試しください。

3.3 サブユーザーの変更・削除

お申込時に登録した初期ユーザーが、登録済みのサブユーザーを変更・削除するには、 画面上部の [サブユーザー] をクリックします。

Bizメール&ウェブ Web改ざん検知オプション	ユーザー情報 サブユーザー パスワード ログアウト
サブユーザー	
サブユーザーを追加します。 🞴	
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	※こちらのアドレスにサブユーザー登録完了の通知メールが届きます。
アラートメール通知	● 有効 ○ 無効
アクセスの権限	□全て選択 └□http://www.example.com
	<u>追加する</u> ③
サブユーザー情報の変更・削除	:
Test-User01	
アラートメール通知 ® 有効 〇	無効
アクセスの権限 □ 全て選択 ^L ☑ http:/	//www.example.com
	変更する

■変更:該当ユーザーの情報を変更した後、[変更する]をクリックします。

※ サブユーザーが自身の情報を確認・変更する場合は、 「<u>3.1ユーザー情報の確認・変更</u>」をご参照ください。

■削除:該当ユーザーの欄に表示されている [削除] をクリックします。

3.4 パスワードの変更

パスワードを変更する場合は、画面上部の[パスワード]をクリックします。

Biz Web改	・ メール&ウェブ ざん検知オプション	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・	- ド	
	現在のパスワード	
	新しいパスワード	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。
	新しいパスワード(確認用)	
		戻る ③ 変更する ④

以下の理由でログインができなくなった場合は、ログイン画面の[パスワードをお忘れの場合]をクリックして、パスワードを再設定することが可能です。

- パスワードを紛失
- 二要素認証の認証アプリへ登録せずにログアウトした**
- 二要素認証の認証アプリの削除・デバイスの変更・紛失等によりログインで きなくなった**

**この場合、『新しいパスワードの設定』画面で、二要素認証を無効にしてください。

ユーザーID	Test-User04	
パスワード		
	ログインする	Θ
4	パスワードをお忘れの場合	

3.5 二要素認証

二要素認証を [有効] へ変更すると以下の画面が表示されます。



- 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、ログイン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や、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は、ログイン画面の「パスワードをお忘れの場合」をクリックして、パスワードを再設定してください。
- ※この際、『新しいパスワードの設定』画面で、二要素認証を無効にしてください。

新	新しいパスワードの設定				
	新しいパスワード	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。			
	新しいパスワード(確認用)				
	二要素認証	☑ 無効にする			
	保存 ③				

4. 解析画面

ホーム(Dashboard)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。
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。 ひざん検知:あり のanger.8 Warning:4 NotFound:0
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。
1	お知らせ	ホーム(Dashboard)には、最新のお知らせのタイトルが表示されます。 また、「一覧を見る」をクリックすると、過去のお知らせを確認できます。 詳細は 「 <u>8.お知らせ機能</u> 」をご参照ください。

4.1 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は、画面には「SAFE」と緑の マークで表示されます。



	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。

4.2 解析結果表示:赤(DANGER・危険)

解析した結果、危険なサイトであると判定された場合は、画面には赤のマーク 🙆 が表示されます。



	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。 マークをクリックすると、解析結果の内容を表示できます。 ※ 解析結果の内容については、 <u>次ページ</u> をご参照ください。
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 2 マークをクリックすると、下図のような「解析結果の内容」が表示されます。

http://	/index.html
■10×100 ■1	■ 2010 脅威名:Iframe Generic (GJS159) ③ 3 賞社の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。
	検知した経路 http:/// p/index.html ④ http:// 詳細を見る ⑤ 浅知箇所を見る ④

	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。 問題が見つかりました http:// / NFのソースコード内の//イライト部に問題があります。 ((DOCTYPE html PUBLIC **//WSC//DTD XHTML 1.0 Transitional//EN" " <u>http://mww.w3.org/TB/xhtml</u> ((DOCTYPE html PUBLIC **//WSC//DTD XHTML 1.0 Transitional//EN" " <u>http://mww.w3.org/TB/xhtml</u> ((DOCTYPE html PUBLIC **//WSC//DTD XHTML 1.0 Transitional//EN" " <u>http://mww.w3.org/TB/xhtml</u> ((DOCTYPE html PUBLIC **//WSC//DTD XHTML 1.0 Transitional//EN" " <u>http://mww.w3.org/TB/xhtml</u> ((DOCTYPE html PUBLIC **//WSC//DTD XHTML 1.0 Transitional//EN" " <u>http://mww.w3.org/TB/xhtml</u> ((thtml winhow" <u>http://mww.a3.org/TB/xhtml</u> ((doct ** thtp:-equive" Content-*Type" content="text/javascript" /> ((etta name="description" content="'/> ((etta name="descri		
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」が表示されている場合には、検知経路が表示されます。		

4.3 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。



解析結果カレンダー内の黄色マーク 0 をクリックすると、下図のような詳細ページが表示されます。

注意が必要です 2022年5月4日 10:03	.js
Lange	■ 育威名:[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「クロスドメインの作可設定」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学生している犯があります。 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「雪白」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。
	検知した経路 https:// kk.js ゆ https:// kaiso/ ゆ https:// cross/

	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。

4.4 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。

4.5 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 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。

5. 解析履歴

詳細設定ボタン
をクリックして遷移した画面の、左メニューから「解析履歴」
をクリックします。

※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。

*-1	▲ 解析履歴の表示期間は2	カ月です。		
٨Q	解析日	解析完了時間	解析結果	URL数
解析履歷	2022年05月16日	05:10	改ざんを発見しました	10
4	2022年05月15日	17:10	注意が必要です	10
ロレポート作成	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
解析内容の設定	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
		HOLD-K D		

6. レポート作成

詳細設定ボタン

言 をクリックして遷移した画面の、左メニューから「レポート作成」

をクリックします。

※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。

レポート作成	http:/// 監視	. ф	
☆ ホーム への 解析履歴 目 レポート作成	レポートを表示する期間を選択してください。 ④ 解析陶器の保存期間は1年間です。 2022 ▼ 年 5 ▼ 月 → 2022 ▼ 年 5 ▼ 月 レポートを作用	क्षेत्र अ	
	GRED Web改ざんチェックレホート ・ 枢桥対象ドメイン: http:// ・ 枢桥対象: 2022年5月~2022年5月 ・ 和析指果: 開墾あり 2022 5月 文ざんを遥知した回数 6 資社のウェブページ数(平均) 10		
	 (検知日]2022年5月13日 15:29 (検知ヘージ)http:// (検知ヘージ)http:// 		
	■ac2:irrame Generic (GJS159) レポートを印刷する ③		

	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。

7.解析内容の設定

解析内容の設定	https://	com/	監視中	
合 ホーム	▶ <u>現在の利用状況一覧を見る>></u>			
_∧ ^Q 解析履歴	基本設定	除外設定	クロスドメイン設定	
	▷ 監視のON/OFFと基本設定	D ATITEUZE D BARLUR	▷ <u>クロスドメイン検知</u>	
	オプション 5 • <u>GRED証明書</u> • 改ざん時切り替え機能 6			

① 基本設定

「監視のON/OFF」「メニュータイトル(全角 20文字 半角 40文字)」と「ウェブ 解析対象階層(何も記入しなければ無制限)」を指定できます。

基本設定	https://	.com/ 監視中 目
أ		
^@	監視のON/OFF	● 有効 ○ 無効
解析履歷	メニュータイトル	https:// (全角20文字 半角40文字) ※ページ上部の「ウェブ解析」タブの下に表示される部分です。
日 レポート作成	ウェブ解析対象階層の指定	発展目まで ※何も記入しなければ「無制限」です。
☆ 解析内容の設定		2275 •

② ホワイトリスト

このリストに設定した 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。最大 10個まで指定する事が可能です。



③ 除外URL

除外 URL は、パス(ディレクトリ)指定を最大 100個まで設定することができます。 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。



④ クロスドメイン検知

クロスドメインスクリプトの検知の有効/無効と、許可設定を行います。

※ウェブ解析機能では、改ざんによって意図しないドメインの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。

※ このリストに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「Warning」表示を「Safe」に変更します。

クロスドメイン検知	https://	/	監視中	
▲ ホーム 八 ^Q 解析履歴 目 レポート作成	目社ドメイン以外のスクリプト(クロスドメインスクリプト)が発見され ここでは、安全なクロスドメインスクリプトに対して警告しないように トのドメインを許可リストに設定しておくことができます。 クロスドメインスクリプトの検知機能 ● 有効 ○ 無効 違用する	クロスドメ 機能をON チェックを クリックしま	インスクリフ Nにするには 入れて、「適) ます。	パトの検知 は、有効に 応する」を
☆ 解析内容の設定	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 □ すべてチェック □ https://hogehogelololo.jp/kkkkkkkk.js	最近のチェ クロスドメー 一括で許可	ックで見つた インスクリプ Jすることが	かった トを 、できます。
	登録する (0		
	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 許可リストに登録したい クロスドメイン	個別に許す のクロスド 録する]を	可をする場合 メインを入り クリックします	合は、該当 カして[登 す。
	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 つすべてチェック いco.jp	登録してい ます。	る項目を[詳	削除]でき
	address (0		

⑤ GRED証明書

HTMLのimgタグによりgredシールのイメージを埋めこみます。ここに表示される お客さま専用のタグをページ内のgredシールを表示させたい部分に挿入してください。

GRED証明書シー	-JL https://	.com/	監視中		
合 ホーム	■##表目12月30日 GRED Web改ざんチェックをご利用の方に ジャパティース グをページ内のGRED証明書のシールを表示	提供しているWebサ たさせたい部分に挿入	イト用の証明書シールです。 して下さい。 ※証明書の会	。 下記の夕 タグはお客様	
	ごとに異なります。 (a href="https://www2.gred.jp/saaz/ratingVerify.htm?sid=" onclic sid=, blank, "width=800, height=800, regizablemo, memobar-yes, the saal binne, ")retwort n Jase;" X-(sin beight=800" berg="0" width="	k="window.ope too 85" 31			
信 レポート作成	onerror='javasoriptisro = 'https://www.gred.jp/gred_seal/seal.gif';' 証明書の検証ページを見る	GR ごと	ED 証明書の に異なります	タグはお裂 。	字さま
☆ 解析内容の設定					

この証明書をお客さま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でき、エンドユーザーに安心感を提供することができるので、 お客さまへの信頼を高める手助けとなります。ぜひご活用ください。

⑥ 改ざん時切り替え機能

解析を行なったページに改ざんが見つかった場合、お客さまのWebサイトの訪問者にGRED内のメンテナンスページを自動で表示することができます。

- ※ 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、お客さまのWebサイト が復旧するまでエンドユーザーの被害を防ぐことができます。
- ※この機能は、お客さまのWebサイトが安全な状態になると表示されません。
- ※ ウェブ改ざんチェックのサービスを終了した場合は、埋め込んだタグを削除してく ださい。
- ※切り替え後の画面サンプルは、次ページをご参照ください。

改ざん時切り替	え機能 https:	.com/	監視中	
ہ ہ–4	gredがチェックを行なった/ ージを表示することができま	ページに改ざんが見つかった場合、お客様のWe すす。 HTMLのタグのすぐ後 に下記のタグを挿み	bサイトの訪問者にgred内のメンテナンスペ して下さい。	
Q 解析履歴	<pre><sor <="" ipt="" pre="" si="" type="text/javasor ipt"></sor></pre>	ros"https://www.gred.jp/saas/gred_charker.js?sid= を指定することでリンテナンフルージの	切り替え機能のタグはお客さ	:ŧ
信 レポート作成	※ハウスージにredirect_un	218229 8222223777227772200	ごとに異なります。 お客さまのサイトのHTM	
☆ 解析内容の設定	切り替え機能の設定 上記のタグを一度挿入してま が一弊社サービスで誤認によ にすれば切り替え機能が解説	Sけば、切り替え機能の設定が下記より変更でき SD不正サイトとして検知されWebサイトがメン たれ、通常通りページが表示されます。	くhead>タグのすぐ後に挿 してください。	, 认
	切り替え機能設定	● 有效 ○ 無效		
	切り替え機能適応範囲	● 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 🕘		

切り替え後の画面サンプル

【メンテナンス画面】

ただい	いまメンテナ	ンス中です	す。
現在メンテナンスを行 ご迷惑をおかけいたし	うっているため、目的のサイ 、ますが、お時間をおいて後	トにアクセスすること ほどアクセスしてくた	こができません。 ごさい。
	623		

8. 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できます。

- ホーム(Dashboard)には最新のお知らせのタイトルが表示されます。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確認できます。



●お知らせはメールでも受け取ることができます。
 設定画面は「<u>3.1 ユーザー情報の確認・変更</u>」をご参照ください。

9. 注意事項

Web改ざん検知サービスは、ウェブサイトのコンテンツを診断するサービスとなります。改ざんを削除したり、コンテンツが安全な状態になるようにサイトの内容を修正、 改善するものではございません。

10. お問い合わせ先

Web改ざん検知オプションに関するお問い合わせはmw-option@ml.ntt.comまでご 連絡ください。