Web改ざん検知 オプション

※Web改ざん検知は、オプションサービスです。

■ Web改ざん検知とは

お客様のホームページに対する改ざんを検知する機能です。1日1回ホームページを自動で解析するので、タイムリーな発見が可能です。万が一改ざんを検知した場合は、管理者メールアドレス宛にアラート送信し、自動的に安全なページに切り替えることができます。

■ Web改ざん検知の注意事項について

- ご利用料金として、3,000円／月（税抜）を別途申し受けます。
- 改ざんの解析対象ページは、100ページ(共有SSLのページ除く)までとなります。
- 画像ファイル、動画ファイル、アクセス制限がかかっているページなどは解析の対象外となります。
- 改ざんを検知した際に安全なページに切り替えるには、予めWebサイトにスクリプトを書き込む必要があります。(お客様作業)
  ※ページの切り替え方法→「改ざん検知時のページ切り替え機能を設定する」(P.11)
- 「ウェブ解析開始URL」は初期設定値として以下を設定しています。

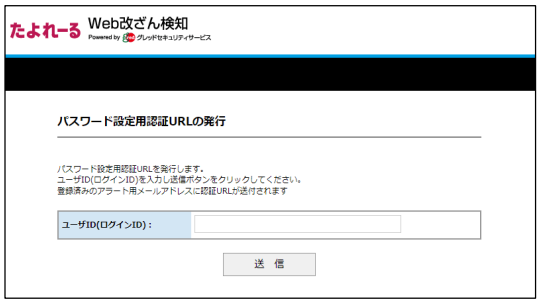
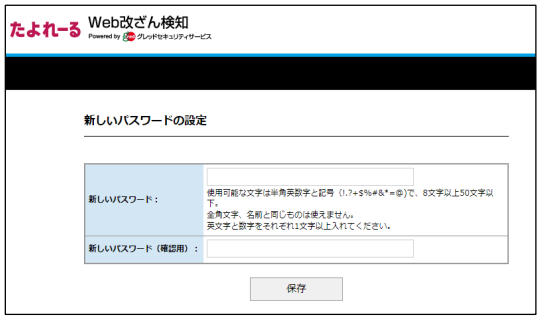
ウェブ解析開始URL(1)	http://www.お客様ドメイン名/
監視設定	有効

ウェブ解析開始URL(2)	https://共有SSL用のドメイン名/ または https://共有SSLのドメイン名/お客様ドメイン名/
監視設定	無効

追加・変更を希望される場合、サポートセンターまでお問い合わせください。
※各項目、初期設定値を含め5つまで設定が可能です。
※監視設定の変更方法→「監視のON/OFFと基本設定を設定する」(P.7)

- メンテナンスや障害情報は、Web改ざん検知のログイン画面でご確認いただけます。
  ※ログイン画面の表示方法→「Web改ざん検知にログインする」(P.3)

■ Web改ざん検知 お申し込みからご利用開始までの流れ

大塚商会	お客様	セキュアブレイン
契約処理	Web改ざん検知のお申し込み	
		メール配信 【Web改ざん検知】サービス登録完了のお知らせ
	パ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。  	
		メール配信 【Web改ざん検知】パスワード設定用認証URLのお知らせ
	新しいパスワードの設定 新しいパスワードを設定します。  	
		メール配信 【Web改ざん検知】パスワード設定完了のお知らせ
	ログイン ユーザーIDと設定した新しいパスワードでWeb改ざん検知にログインします。  	

■ Web改ざん検知にログインする

1 Web改ざん検知のログイン画面にアクセスします。
https://www.gred.jp/saas/alpha-mail/

Web改ざん検知のログイン画面が表示されます。

2 必要事項を入力し、「ログインする」をクリックします。

ユーザーID	ユーザーIDを入力します。
パスワード	パスワードを入力します。

※ユーザーIDは、gredセキュリティサービスから送信される下記メールに記載されています。初めて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。
下記メールに記載されている手順に従い、パスワードを設定してください。

■管理者の場合
「【Web改ざん検知】サービス登録完了のお知らせ」
■サブユーザーの場合
「【Web改ざん検知】サブユーザ登録のお知らせ」

パスワードを忘れた場合
パスワードの再発行が可能です。詳しい操作方法については「パスワードを再発行する」(P.15)をご覧ください。

3 Web改ざん検知画面が表示されます。

■ Web改ざん検知画面の画面説明

①ウェブ解析開始URL
選択したウェブ解析開始URLのページが表示されます。

②監視サイト検索
検索する監視サイトのタイトルまたはURLを入力し「検索する」ボタンをクリックすると、該当する監視サイトのページが表示されます。

③最終結果
最後に解析した日時が表示されます。また、解析結果がマークで表示されます。

SAFE	改ざんを検知しなかった場合
	改ざんを検知した場合
Warning	クロスドメインスクリプトを検知した場合 マーク下の「再チェックする」をクリックすると即時に解析が行われます。1日2回まで使用が可能です。
NOT FOUND	解析対象のページにアクセスができなかった場合
STOP	改ざん検知の処理を停止した場合

④過去の解析結果
当月と先月の解析結果がマークで表示されます。検知した場合、マークをクリックするとクリックした日付に検知したURLが表示されます。当月と先月以外の解析結果は、カレンダー下のプルダウンメニューで対象の期間を選択し表示してください。

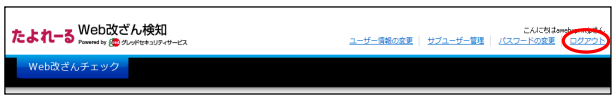
OK	改ざんを検知しなかった場合
	改ざんを検知した場合
	クロスドメインスクリプトを検知した場合
?	解析対象のページにアクセスができなかった場合

⑤本日の解析結果履歴
本日の解析履歴（1日分）が表示されます。検知した場合、クリックすると本日検知したURLが表示されます。

⑥最新情報の表示

最新のクロスドメイン一覧を見る	クリックすると、最新のクロスドメイン一覧が表示されます。
最新の解析URLのリストをダウンロード	クリックすると、最新の解析URLのリストがダウンロードできます。

■ ログアウトする



1 「ログアウト」をクリックします。

Web改ざん検知からログアウトします。

■ 解析履歴を確認する

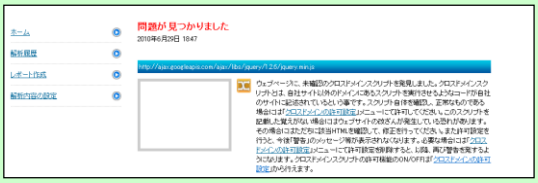
Web改ざん検知の解析履歴を確認します。過去60日分の解析履歴が一覧で表示されます。

1 「解析履歴」をクリックします。

2 解析履歴が表示されます。

解析日	解析日が表示されます。
解析完了時間	解析が完了した時間が表示されます。
解析結果	解析結果が表示されます。
ページ数	解析をしたページ数が表示されます。

検知した場合、上記項目をクリックするとクリックした日付に検知したURLが表示されます。

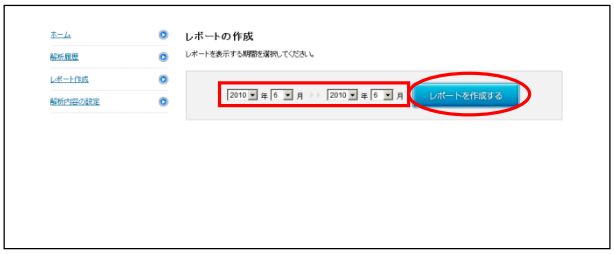


■ レポートを作成する

Web改ざん検知の解析結果をレポートとして印刷します。

1 「レポート作成」をクリックします。

レポートの作成画面が表示されます。



2 作成するレポートの期間を選択し、「レポートを作成する」をクリックします。

選択した期間のレポートが表示されます。

3 「レポートを印刷する」をクリックします。

表示されているレポートを印刷できます。

■ 解析内容の設定画面を表示する

1 「解析内容の設定」をクリックします。

2 解析内容の設定画面が表示されます。

■ 現在の利用状況を確認する

1 解析内容の設定画面を表示し、「現在の利用状況一覧を見る」をクリックします。

※解析内容の設定画面の表示方法→「解析内容の設定画面を表示する（P. 6）

2 現在の利用状況一覧画面が表示されます。

■ 監視のON/OFFと基本設定を設定する

Web改ざん検知の監視を有効にするかどうか、画面左上部に表示されるメニュータイトルと解析対象の階層を設定します。

1 解析内容の設定画面を表示し、「監視のON/OFFと基本設定」をクリックします。

※解析内容の設定画面の表示方法→「解析内容の設定画面を表示する（P. 6）

基本設定画面が表示されます。

2 必要事項を入力し、「変更する」をクリックします。

監視のON/OFF	Web改ざん検知の監視を有効にするかどうかを選択します。
メニュータイトル	メニュータイトルを入力します。
ウェブ解析対象階層の指定	解析対象の階層を入力します。 入力した階層以降はページが存在しても解析されません。

監視のON/OFFについて
「有効」と設定した場合、各種アラートメールが検知内容によって送信されます。
※アラートメールについて→「gredセキュリティサービスから配信されるメールについて」(P.17)

3 設定が反映されます。

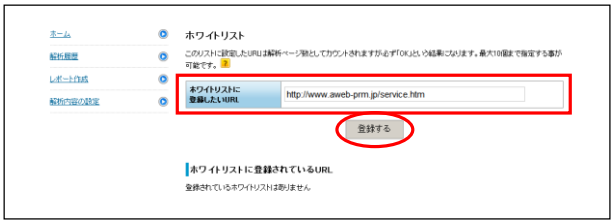
■ ホワイトリストを登録する

ホワイトリストとは
特定のページの解析結果を常に「改ざんを検知しなかった状態」として判断します。

1 解析内容の設定画面を表示し、「ホワイトリスト」をクリックします。

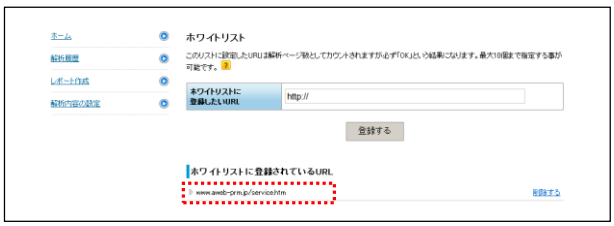
※解析内容の設定画面の表示方法→「解析内容の設定画面を表示する（P. 6）

ホワイトリスト画面が表示されます。



2 解析から除外したいURLを入力し、「登録する」をクリックします。

URLは最大10個まで登録することが可能です。



3 設定が反映されます。

登録したURLは解析対象ページとしてカウントされます。

■登録したホワイトリストを削除する

1. 削除するホワイトリストの「削除する」をクリックします。
2. 確認画面が表示されますので「OK」をクリックします。

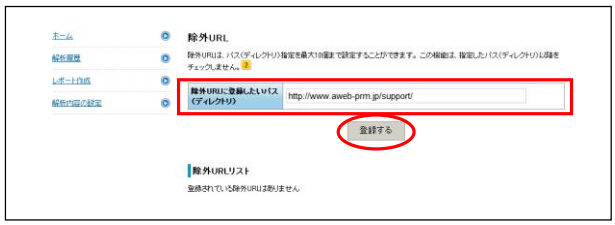
■ 除外URLを登録する

除外URLとは
特定のパス（ディレクトリ）を解析から除外します。設定したパス（ディレクトリ）以降はページが存在しても解析されません。

1 解析内容の設定画面を表示し、「除外URL」をクリックします。

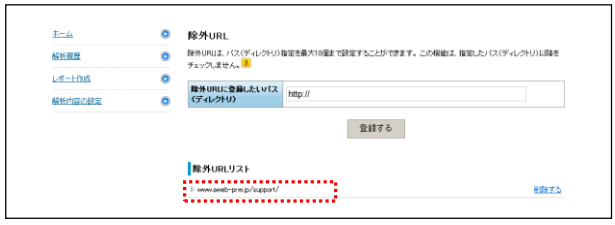
※解析内容の設定画面の表示方法→「解析内容の設定画面を表示する（P. 6）

除外URL画面が表示されます。



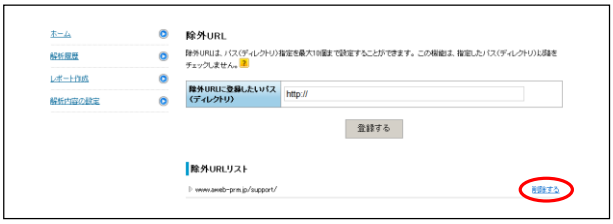
2 解析から除外したいパス（ディレクトリ）を入力し、「登録する」をクリックします。

登録したパス（ディレクトリ）は解析対象ページとしてカウントされません。



3 設定が反映されます。

■登録した除外URLを削除する



1. 削除する除外URLの「削除する」をクリックします。
2. 確認画面が表示されますので「OK」をクリックします。

■ クロスドメインスクリプトの検知を設定する

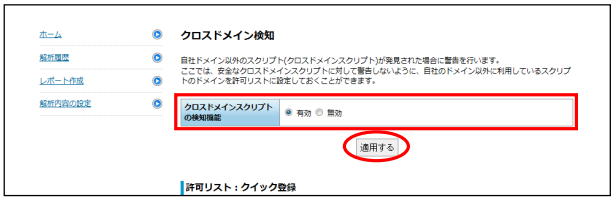
クロスドメインスクリプトの検知を有効にするかどうか設定します。

クロスドメインスクリプトとは
お客様ドメイン名以外のURLに対してのリンクやスクリプトの設定が行われているHTMLファイルの記述です。

1 解析内容の設定画面を表示し、「クロスドメイン検知」をクリックします。

※解析内容の設定画面の表示方法→「解析内容の設定画面を表示する（P. 6）

クロスドメイン検知画面が表示されます。



2 必要事項を選択し、「適用する」をクリックします。

クロスドメインスクリプトの検知機能	
有効	クロスドメインスクリプトの検知を有効にします。
無効	クロスドメインスクリプトの検知を無効にします。

「有効」と設定した場合、クロスドメインスクリプトを検知した際にアラートメールが送信されます。
※アラートメールについて→「クロスドメインスクリプト検知アラート」（P.20）

3 設定が反映されます。

■ 許可するクロスドメインスクリプトを登録する

ウェブ解析開始URL以外のクロスドメインをチェック対象から予め除外します。

1 解析内容の設定画面を表示し、「クロスドメイン検知」をクリックします。

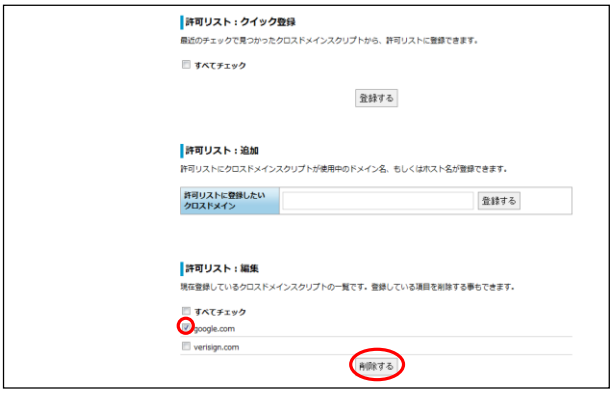
※解析内容の設定画面の表示方法→「解析内容の設定画面を表示する（P. 6）

クロスドメイン検知画面が表示されます。

2 許可するクロスドメインを入力し、「登録する」をクリックします。

3 設定が反映されます。

■登録したクロスドメインを削除する



削除するクロスドメインを選択し、「削除する」をクリックします。

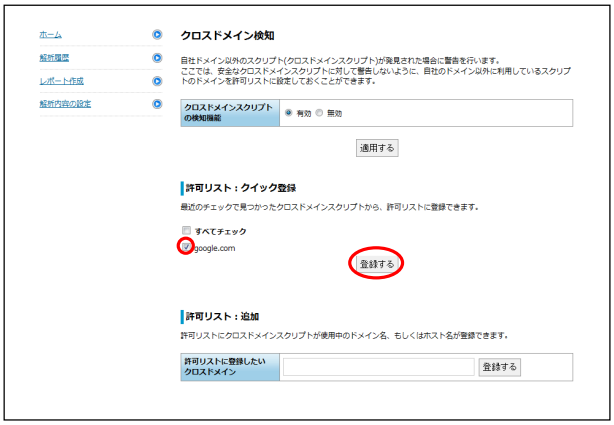
■ チェックで見つかったクロスドメインスクリプトを許可する

チェックで見つかったクロスドメインスクリプトを許可します。

1 解析内容の設定画面を表示し、「クロスドメイン検知」をクリックします。

※解析内容の設定画面の表示方法→「解析内容の設定画面を表示する（P. 6）

クロスドメイン検知画面が表示されます。



2 「許可リスト：クイック登録」から許可するクロスドメインスクリプトを選択し、「登録する」をクリックします。

3 設定が反映されます。

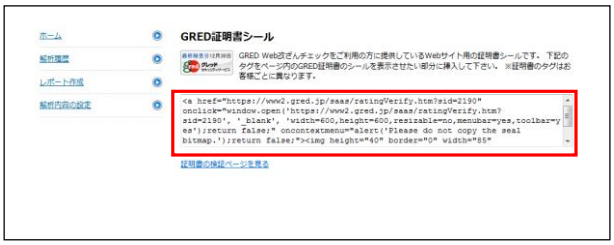
■ GRED証明書をホームページに表示する

GRED証明書をお客様のホームページに表示します。

1 解析内容の設定画面を表示し、「GRED証明書」をクリックします。

※解析内容の設定画面の表示方法→「解析内容の設定画面を表示する（P. 6）

GRED証明書画面が表示されます。



2 記載されているタグを全てコピーします。

コピーしたタグを、GRED証明書を表示したいホームページのソースに埋め込みます。

コピーしたタグ下の「GRED証明書の検証ページを見る」をクリックすると、GRED証明書のサンプルが表示されます。

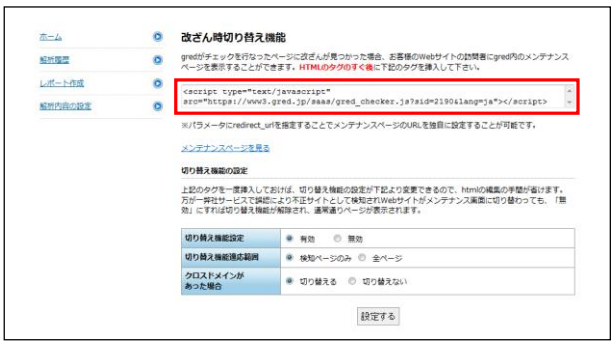
■ 改ざん検知時のページ切り替え機能を設定する

改ざんの検知時にメンテナンスページに切り替える設定をします。

1 解析内容の設定画面を表示し、「改ざん時切り替え機能」をクリックします。

※解析内容の設定画面の表示方法→「解析内容の設定画面を表示する（P. 6）

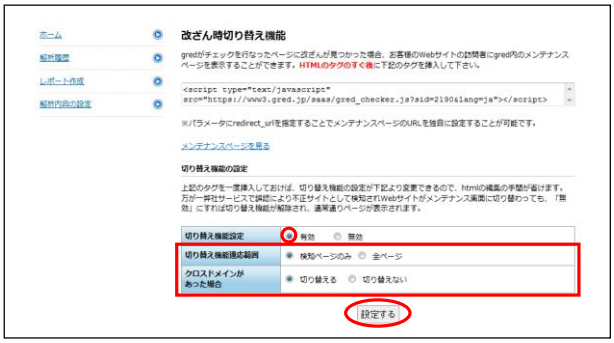
改ざん時切り替え機能画面が表示されます。



2 「改ざん時切り替え機能」に記載されているタグを全てコピーします。

コピーしたタグを、ページ切り替え機能を設定したいホームページのソースに挿入します。

任意のページをメンテナンスページにするには
コピーしたタグの「lang=ja」と「″」の間に以下を追加します。
&redirect_url=″任意のページのURL″



3 「切り替え機能設定」で「有効」を選択します。

設定項目が表示されますので、必要事項を選択し、「設定する」をクリックします。

切り替え機能適応範囲	検知時にメンテナンスページに切り替える適応範囲を選択します。
クロスドメインがあった場合	クロスドメインを検知した場合、メンテナンスページに切り替えるかどうかを選択します。

切り替え機能を解除するには
上記画面で「無効」を選択します。

4 設定が反映されます。

■ サブユーザーを作成する

Web改ざん検知を利用できるユーザーを作成します。（最大5つまで作成可能）

1 「サブユーザー管理」をクリックします。

サブユーザー管理画面が表示されます。

2 必要事項を入力し、「追加する」をクリックします。

サブユーザーご担当者名（お名前）	名前を入力します。
ログインID	ログインに使用するIDを入力します。
アラート用メールアドレス	改ざん検知時にアラートを送信するメールアドレスを入力します。
アラートメール通知	アラートメールを受け取るかどうかを選択します。
アクセスの権限	参照を許可する解析結果を選択します。

3 設定が反映されます。

登録したアラート用メールアドレス宛にパスワード設定用認証用URLが記載されたサブユーザ登録のお知らせが送信されます。
初めて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。
下記メールに記載されている手順に従い、パスワードを設定してください。
※サブーユーザ登録のお知らせについて→「サブユーザ登録のお知らせ」(P. 21)

■サブユーザーの設定を変更する

変更するサブユーザーの変更内容を選択し、「変更する」をクリックします。

■サブユーザーを削除する

削除するサブユーザーの「削除」をクリックします。

■ ユーザー情報を変更する

メールアドレスやアラートメールの受信有無などのユーザー情報を変更します。

1 「ユーザー情報の変更」をクリックします。

ユーザー情報の変更画面が表示されます。

2 必要事項を入力し、「確認する」をクリックします。

アラート用メールアドレス	改ざん検知時にアラートを送信するメールアドレスを入力します。
ご担当者名（お名前）	名前を入力します。
週間レポートメール通知	週間レポートメールを受け取るかどうかを選択します。
アラートメール通知	アラートメールを受け取るかどうかを選択します。

確認画面が表示されます。

3 「変更する」をクリックします。

4 設定が反映されます。

■ パスワードを変更する

Web改ざん検知にログインする際のパスワードを変更します。

1 「パスワードの変更」をクリックします。

パスワードの変更画面が表示されます。

2 必要事項を入力し、「変更する」をクリックします。

現在のパスワード	現在のパスワードを入力します。
新しいパスワード	新しいパスワードを入力します。
新しいパスワード（確認用）	再度、新しいパスワードを入力します。

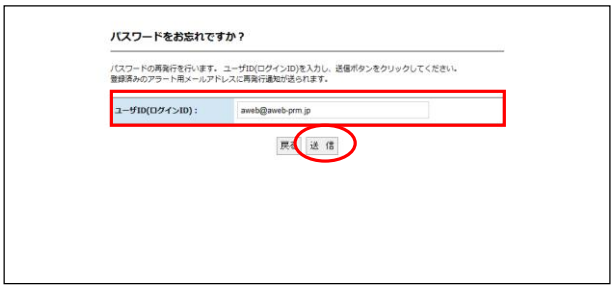
3 設定が反映されます。

■ パスワードを再発行する

Web改ざん検知にログインする際のパスワードを再発行します。

1 Web改ざん検知のログイン画面で「パスワードをお忘れの場合はこちらをクリック」をクリックします。

パスワードの再発行画面が表示されます。



2 ユーザIDを入力し、「送信」をクリックします。

3 登録されているアラート用メールアドレス宛にパスワード設定用認証用URLが記載されたメール（【Web改ざん検知】 パスワード設定用認証用URLの発行）が送信されます。

24時間以内に記載されているURLよりパスワードを設定して下さい。

■ gredセキュリティサービスから配信されるメールについて

gredセキュリティサービスから配信されるメールについてご案内します。

■サービス登録完了のお知らせ

アルファメール「Web改ざん検知」オプションをお申し込みいただき、ありがとうございます。
サービスの登録が完了しましたのでご連絡いたします。

「Web改ざん検知」ではお客様のWebページ改ざんを監視する「Web解析」機能を提供します。
「Web改ざん検知」管理画面へは、下記のユーザーID・パスワードでログインしてください。

■「Web改ざん検知」管理画面URL：https://www.gred.jp/saas/alpha-mail
■ユーザーID：xxxx@xxxx.xx.xx
■パスワード：下記参照

パスワードにつきましては、お手数ですがお客様にて以下の手順に沿って設定をお願いいたします。

（1）「パスワード設定用認証URLの発行画面」にアクセスします。

パスワード設定用認証URLの発行画面：
https://www.gred.jp/saas/xxxxxxxxxxx

（2）「パスワード設定用認証URLの発行画面」にて、上記のユーザーIDを入力し、「送信」ボタンをクリックします。

（3）「パスワード設定用認証URLのお知らせ」のメールが、本メールを受信しているアドレス宛に届きますので、メール本文中のURLにアクセスします。
※メールが届いてから24時間以内にアクセスしてください。
24時間を過ぎてしまった場合は、（1）の手順からやり直してください。

（4）「新しいパスワードの設定画面にてご利用になりたいパスワードを設定し、「保存」ボタンをクリックします。

（5）「パスワード設定完了のお知らせ」のメールが届きますので、管理画面URLへアクセスし、ユーザーIDと、手順4で設定されたパスワードでログインします。

※設定済みのパスワードをお忘れになった場合も、上記手順にてパスワードの再設定が可能です。

■－－
本メールは株式会社セキュアブレインの「gredセキュリティサービス」から自動で送信しています。
――
お問い合わせは　たよれーるコンタクトセンター
アルファメール担当
TEL ： 0120-xxx-xxx
https://www.alpha-web.jp/question/support.htm
――

Web改ざん検知のお申し込み時に、送信されます。

To	アルファメール管理者メールアドレス
From	gred@service.securebrain.co.jp
件名	【Web改ざん検知】サービス登録完了のお知らせ

■パスワード設定用認証URLの発行

パスワード設定用URLをお知らせします。
24時間以内に下記のURLにアクセスし、パスワードを設定してください。

■パスワード設定用認証URL：
[CURL]

※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、下記「パスワード設定用認証URLの発行画面」より改めて、パスワード設定の操作を行い、パスワード設定用認証URLを発行してください。

■パスワード設定用認証URLの発行画面：
https://www.gred.jp/saas/xxxxxxxxxxx

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ください。

■－－
本メールは株式会社セキュアブレインの「gredセキュリティサービス」から自動で送信しています。
――
お問い合わせは　たよれーるコンタクトセンター
アルファメール担当
TEL ： 0120-xxx-xxx
https://www.alpha-web.jp/question/support.htm
――

Web改ざん検知のお申し込み時、パスワードの再発行時、サブユーザー登録時に送信されます。

To	アルファメール管理者メールアドレス、またはアラート用メールアドレス
From	gred@service.securebrain.co.jp
件名	【Web改ざん検知】パスワード設定用認証URLのお知らせ

■パスワード設定完了のお知らせ

パスワードの設定が完了しました。
「Web改ざん検知」管理画面URLへアクセスし、ユーザーIDと、設定されたパスワードでログインの上ご利用ください。

■「Web改ざん検知」管理画面URL：https://www.gred.jp/saas/alpha-mail
■ユーザーID：xxxx@xxxx.xx.xx
■パスワード：お客様にて設定されたパスワード

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ください。

■－－
本メールは株式会社セキュアブレインの「gredセキュリティサービス」から自動で送信しています。
――
お問い合わせは　たよれーるコンタクトセンター
アルファメール担当
TEL ： 0120-xxx-xxx
https://www.alpha-web.jp/question/support.htm
――

Web改ざん検知のお申し込み時、パスワードの再発行時、サブユーザー登録時に送信されます。

To	アルファメール管理者メールアドレス、またはアラート用メールアドレス
From	gred@service.securebrain.co.jp
件名	【Web改ざん検知】パスワード設定完了のお知らせ

■TOPページ見た目の変化検知アラート

アルファメール「Web改ざん検知」オプションをご利用いただき、ありがとうございます。

システムが監視中のWebサイトでTOPページの見た目が変化した可能性を検知しました。

解析開始URL： ［解析開始URL］

詳細については下記URLをご参照ください。
https://www.gred.jp/saas/alpha-mail

改ざんされている可能性があるWebページの参照には十分ご注意ください。

■－－
本メールは株式会社セキュアブレインの「gredセキュリティサービス」から自動で送信しています。
――
お問い合わせは　たよれーるコンタクトセンター
アルファメール担当
TEL ： 0120-xxx-xxx
https://www.alpha-web.jp/question/support.htm
――

トップページで改ざんの可能性を検知した場合、送信されます。

To	アラート用メールアドレス
From	gred@service.securebrain.co.jp
件名	【Web改ざん検知】TOPページの見た目が変化した可能性を検知

■改ざん検知アラート

アルファメール「Web改ざん検知」オプションをご利用いただき、ありがとうございます。

システムがWebページ改ざんの可能性を検知しました。

解析開始URL：［ウェブ解析開始URL］

検知したページ：［検知したURL］
改ざんの内容：［フィッシング］の疑いのあるコンテンツが発見されました。

詳細については下記URLをご参照ください。
https://www.gred.jp/saas/alpha-mail/

改ざんされている可能性があるWebページの参照には十分ご注意ください。

■－－
本メールは株式会社セキュアブレインの「gredセキュリティサービス」から
自動で送信しています。
――
お問い合わせは　　たよれーるコンタクトセンター
アルファメール担当
TEL ： 0120-xxx-xxx
https://www.alpha-web.jp/question/support.htm
――

トップページ以外で改ざんの可能性を検知した場合、送信されます。

To	アラート用メールアドレス
From	gred@service.securebrain.co.jp
件名	【Web改ざん検知】Webページに改ざんの可能性を検知しました！

■改ざん検知アラート(マルウェア類似挙動の可能性)

アルファメール「Web改ざん検知」オプションをご利用いただき、ありがとうございます。

システムが監視中のWebページにリンクされた実行ファイル（EXE）のマルウェア類似挙動の可能性を検知しました。

マルウェア類似挙動の可能性を検知したURLをブラウザで直接アクセスするとマルウェアに感染する可能性があります。
詳細については下記URLをご参照ください。
https://www.gred.jp/saas/alpha-mail

監視中のWebサイト：［監視中のWebサイト］

検知URL：［検知したURL］

この検知はマルウェアとして検知するものではなく、あくまでもマルウェア類似の動きを検知したものです。
検知したファイルが正常なものである場合、ホワイトリストに登録することで以降の検知を 回避することができます。
ホワイトリストに登録するかどうかは、お客様にてご判断ください。

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ください。

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。改ざんされている可能性があるWebページの参照には十分ご注意ください。

■－－
本メールは株式会社セキュアブレインの「gredセキュリティサービス」から
自動で送信しています。
――
お問い合わせは　　たよれーるコンタクトセンター
アルファメール担当
TEL ： 0120-xxx-xxx
https://www.alpha-web.jp/question/support.htm
――

実行ファイルのマルウェア類似挙動の可能性を検知した場合、送信されます。

To	アラート用メールアドレス
From	gred@service.securebrain.co.jp
件名	【Web改ざん検知】実行ファイルのマルウェア類似挙動の可能性を検知

■クロスドメインスクリプト検知アラート

アルファメール「Web改ざん検知」オプションをご利用いただき、ありがとうございます。

システムがクロスドメインスクリプトを検知しました。

解析開始URL：［ウェブ解析開始URL］

クロスドメインスクリプト：［検知したクロスドメインスクリプト］

詳細については下記URLをご参照ください。
https://www.gred.jp/saas/alpha-mail/

改ざんされている可能性があるWebページの参照には十分ご注意ください。

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。改ざんされている可能性があるWebページの参照には十分ご注意ください。

■－－
本メールは株式会社セキュアブレインの「gredセキュリティサービス」から自動で送信しています。
――

お問い合わせは　たよれーるコンタクトセンター
アルファメール担当
TEL ： 0120-xxx-xxx
https://www.alpha-web.jp/question/support.htm
――

クロスドメインスクリプトを検知した場合、送信されます。

To	アラート用メールアドレス
From	gred@service.securebrain.co.jp
件名	【Web改ざん検知】Webページにクロスドメインスクリプトを検知しました！

クロスドメインスクリプト検知アラートは、サブユーザーには配信されません。

■ヘルスチェックアラート

現在監視中の下記URLで、Webサイトが正常に開けませんでした。

解析開始URL：［ウェブ解析開始URL］

エラー内容：
　検知したページ：［検知したURL］
内容：［アラートの内容］

詳細については、下記ページよりご確認ください。
https://www.gred.jp/saas/alpha-mail/

※トップページが開けない場合、Web改ざん検知が正常に行われません。
　この警告と検知を停止する場合は、管理画面へログイン後に、
　[解析内容の設定]-[基本設定]-[監視のON・OFF]にて、OFFを選択してください。
　管理画面URL：https://www.gred.jp/saas/alpha-mail/

■－－
本メールは株式会社セキュアブレインの「gredセキュリティサービス」から自動で送信しています。
――

お問い合わせは　たよれーるコンタクトセンター
アルファメール担当
TEL ： 0120-xxx-xxx
https://www.alpha-web.jp/question/support.htm
――

解析開始URLからの応答がない場合やリンク先ページのコンテンツが存在していない場合などに送信されます。

To	アラート用メールアドレス
From	gred@service.securebrain.co.jp
件名	【Web改ざん検知】お客様Webサイトが開けません

■週間レポート

［お客様名］様

アルファメール「Web改ざん検知」オプションをご利用いただき、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：0000/00/00 - 0000/00/00

登録Webサイト：［ウェブ解析対象ドメイン］

対象ドメイン名：［ドメイン名］

改ざんを通知した回数：［数字］回

チェックしたWebページ数（1回あたりの平均）：［数字］ページ

詳細な情報につきましては、以下の管理画面からご確認いただけます。週間レポート送信サービスの設定を変更される場合は、管理画面ログイン後「ユーザ情報の変更」から行ってください。

管理画面URL：https://www.gred.jp/saas/alpha-mail/

■－－
本メールは株式会社セキュアブレインの「gredセキュリティサービス」から
自動で送信しています。
――

お問い合わせは　たよれーるコンタクトセンター
アルファメール担当
TEL ： 0120-xxx-xxx
https://www.alpha-web.jp/question/support.htm
――

毎週月曜日、今週1週間のレポートが送信されます。

To	アラート用メールアドレス
From	gred@service.securebrain.co.jp
件名	【Web改ざん検知】週間レポート

■サブユーザ登録のお知らせ

アルファメール「Web改ざん検知」オプションをお申し込みいただき、ありがとうございます。

サブユーザ登録確認のお知らせです。

「Web改ざん検知」ではお客様のWebページ改ざんを監視する「Web解析」機能を提供します。
「Web改ざん検知」管理画面へは、下記のユーザーID・パスワードでログインしてください。

■「Web改ざん検知」管理画面URL：https://www.gred.jp/saas/alpha-mail
■ユーザーID：xxxx@xxxx.xx.xx
■パスワード：下記参照

パスワードにつきましては、お手数ですがお客様にて以下の手順に沿って設定をお願いいたします。

（1）「パスワード設定用認証URLの発行画面」にアクセスします。

パスワード設定用認証URLの発行画面：
https://www.gred.jp/saas/xxxxxxxxxxx

（2）「パスワード設定用認証URLの発行画面」にて、上記のユーザーIDを入力し、「送信」ボタンをクリックします。

（3）「パスワード設定用認証URLのお知らせ」のメールが、本メールを受信しているアドレス宛に届きますので、メール本文中のURLにアクセスします。
※メールが届いてから24時間以内にアクセスしてください。
24時間を過ぎてしまった場合は、（1）の手順からやり直してください。

（4）「新しいパスワードの設定画面にてご利用になりたいパスワードを設定し、「保存」ボタンをクリックします。

（5）「パスワード設定完了のお知らせ」のメールが届きますので、管理画面URLへアクセスし、ユーザーIDと、手順４で設定されたパスワードでログインします。

※設定済みのパスワードをお忘れになった場合も、上記手順にてパスワードの再設定が可能です。

■－－
本メールは株式会社セキュアブレインの「gredセキュリティサービス」から
自動で送信しています。
――

お問い合わせは　たよれーるコンタクトセンター
アルファメール担当
TEL ： 0120-xxx-xxx
https://www.alpha-web.jp/question/support.htm
――

サブユーザーの登録時に、送信されます。

To	ログイン用メールアドレス アラート用メールアドレス
From	gred@service.securebrain.co.jp
件名	【Web改ざん検知】サブユーザ登録のお知らせ