Bizメール＆ウェブ　Web改ざん検知オプション

FAQ（よくあるご質問）

第1.1版

2024/6/28

◆目次

1. ホーム画面について

Q

改ざん・クロスドメイン検知時の画面はどのような表示になりますか。

A

改ざん検知された場合、ログイン後のページでカレンダーの表示が赤く×印表記となります。×印をクリックすると改ざんの詳細説明を見ることができます。本日の解析結果履歴からも詳細説明を確認することができます。

クロスドメインが検知された場合、ログイン後のページでカレンダーの表示が黄色の「！」マークでWarning表示されます。カレンダー及び本日の解析結果履歴からクロスドメイン検知の検知元URLなどの情報を確認することができます。

2. 解析について

Flashで作成されたページは解析できますか。

現在の仕様ではFlashに埋め込まれたページからは解析がスタートできません。Flash表示後のページを指定いただくことで、解析が可能となります。

Web改ざん検知は、クロスサイトスクリプティング(XSS)対策にも効果がありますか。

入力フォームがあるウェブページには、スクリプトを挿入される危険があります。ウェブ解析では、ウェブサイトを定期的に巡回しますので、一早くスクリプトの埋め込みなどのチェックが可能となります。

Web改ざん検知では「ブラックリストを用いない」とありますが、本当に一切、どこのブラックリストも併用していないのでしょうか。

Web改ざん検知のエンジンのコアの部分ではブラックリストを使用していません。ただし、 Phish Tank APIとGoogle APIは、100%ブラックリストです。拡張機能としてブラックリスト機能も持っていますが、緊急対応（検知できない物があって、エンジンの更新に時間がかかる場合）に一時的な目的で使用できるようになっています。 弊社エンジンの悪質サイトを検出するコアのロジックとしては、悪質なサイトの様々な特徴をベースにして判定します。そのため、新しく改ざんされたサイトや新種の詐欺サイトなどをブラックリストの更新をしなくても判定することが可能になっています。

Web改ざん検知は、ウェブページをクロールするとのことですが、サーバーに負荷が掛かるのが心配ですが、大丈夫ですか。

検索エンジンがコンテンツを自動巡回するように、Web改ざん検知がウェブサイトを定期的に巡回してサイトの状態を評価します。また、アクセスログにも残ります。ウェブサーバーに対しては通常のブラウザからのウェブアクセスと同様の動作を行いますので、負荷は必要以上にかかりません。

ウェブ改ざんチェックツールとしてtripwireが有名ですが、違いを教えてください。

Web改ざん検知のウェブ解析は、SaaS型なのでインストール設定作業が不要です。
異常時のメールお知らせ機能がありますので、毎日のログイン作業も必要ありません。変更された箇所を日本語のレポートとして報告します。

サイトからダウンロードされるファイルの評価対象ファイルを教えてください。

評価対象のファイルはファイル名の拡張子などで決定していません。サイトからダウンロードしたWebコンテンツは全てチェックし解析します。

解析する順序やルールはありますか。

解析開始URLからリンクを辿り解析を行います。リンクを辿りながら、いくつかのスレッドに分岐して解析を行います。回線のスピードや解析の進捗などで解析の順序や解析ページ数が一定でない場合もございます。

改ざんがあった場合の表示について教えてください。

登録されているURLに改ざんがあった場合、トップページの「SAFE」の緑のマークが「改ざんを発見」の赤のマークに変化します。また、アラート用に登録されたメールアドレスに改ざん発見の通知が届きます。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、トップページのカレンダーの赤い「X」アイコンをクリックすると確認していただけます。

改ざんやクロスドメインが見つかると確認のために2回／日、手動で再チェックができますが、いつまでたっても最新の結果が表示されません。なぜですか。

仕様上、ブラウザの再読み込みボタンもしくはF5ボタンを押さないと更新されません。恐れ入りますが、最新の結果を確認するためには、ブラウザの再読み込みボタンで、再度読み込みを実施してください。

携帯対応はしていますか。

携帯でしかアクセスできないサイトに関しては、対応しておりません。パソコンからアクセスできる携帯サイトは解析をすることができます。

再チェックの終了時間の目安を教えてください。

サーバーの稼働状況にもよりますが、解析完了は、おおよそ100ページで1分とお考えください。

自社で管理しているウェブサイトは、ファイアウォール・IDS・ ウイルスチェックの対策をしています。これで十分だと思います。それでもWeb改ざん検知は必要ですか。

これらのツールで防御する範囲とWeb改ざん検知がチェックする範囲は明確に異なります。プロトコル単位で防御するのが前者なら、個別のアプリケーションレベルで防御するのが Web改ざん検知オプションのウェブ解析です。

3. 解析内容設定

クロスドメイン検知の許可設定について

クロスドメインが検知された時に、許可リストに登録することで、次回の解析からクロスドメインは検知されませんが、複数解析するURLがある場合は、そのすべてにおいて登録をする必要があります。
登録は、解析内容の設定＞クロスドメイン検知＞クロスドメインスクリプトのクイック登録から行うことができます。

ホワイトリストとは何ですか。

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個まで指定する事が可能です。 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。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。

例えば、「http://www.-gredsampleurl-jp/shop/index.html」を指定した場合、このページは必ず「OK」というチェック結果となります。このページに別のページへのリンクがあった場合はクロールされます。その場合、リストに設定されていなければ通常通りウェブ解析が行われます。

ホワイトリストとページ切り替えの関係を教えてください。

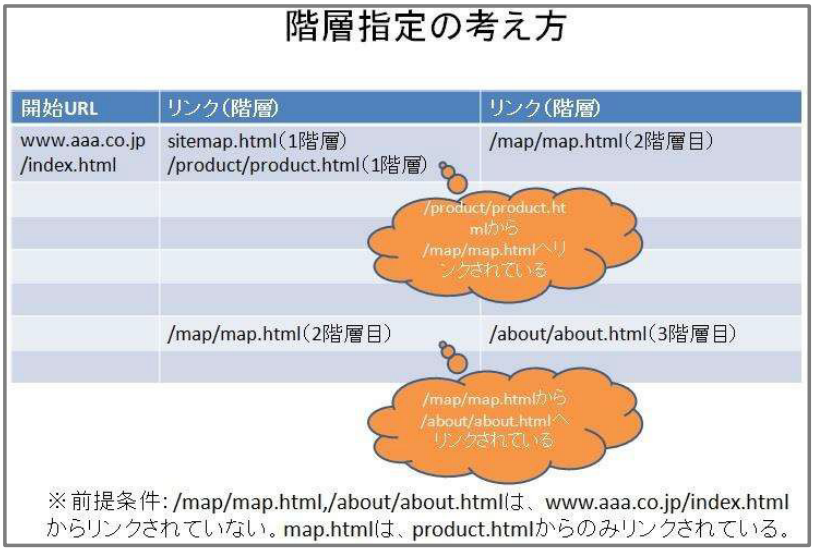
ホワイトリストは、常に「Safe」と判定します。改ざん時切り替え機能のスクリプトを挿入している場合でも、切り替えは発生しません。

ホワイトリストと除外リストを同時に登録しました、どちらが優先されますか。

ホワイトリストが優先されます。ホワイトリストは、改ざんされていても、「Safe」と表記します。また、解析ページ数としてもカウントされます。

階層指定ができますが、その考え方を教えてください。

解析開始URLから解析が始まりますが、その解析開始URLにリンクされているページを1階層目とします。以降リンクを辿る度に、1階層増えていく計算となります。



除外URLとは何ですか。

除外URLとは、ディレクトリ（パス）を指定し、指定されたパス以降を解析（クロール）しない機能です。 この機能は、1つの対象サイトに10迄設定可能で、除外URL指定されたパス以降を解析ページとしてはカウントせず、たとえ指定パス以降に設置されているページ内にリンクがあったとしても解析を行う事はありません。

例えば、「http://www.-gredsampleurl-.jp/blog/」と指定した場合、/blog/以降に設置してあるページは解析の対象とはなりません。

除外URLとページ切り替えの関係を教えてください。

除外URLとして登録すると、解析を行いません。改ざん時切り替え機能やクロスドメインの切り替えのスクリプトを挿入しており、改ざんもしくはクロスドメインのスクリプトが挿入されていても、実際は解析を行いませんので切り替えは発生いたしません。

4. 解析履歴 レポート

レポートの作成

期間を指定して、レポートを作成することができます。このレポートには、解析対象ドメイン・解析期間・解析結果・改ざんを通知した回数・ウェブページ数（平均）・解析結果詳細が表示されます。
またレポートを印刷することも可能です。
クロスドメイン検知の回数などクロスドメインに関する内容は、このレポートに含まれません。

解析の結果レポートの印刷について。

Web改ざん検知では、過去の解析結果をレポートとして表示し印刷することができます。トップページの左メニューの「レポート作成」のリンクをクリックするとレポート作成の期間選択画面になります。
ここで必要なレポート期間(1ヶ月単位）を選択し「レポートを表示する」ボタンをクリックすると、下にレポートが表示されます。印刷は結果のみを印刷することができます。

解析履歴の見方

解析履歴機能は、サービスを開始してからの解析結果を一覧表示します。表示項目としては、以下のようになります。

「解析日」:ウェブ解析を行った日付を表示します。
「解析完了時間」:解析を終了した時間を表示します。
「解析結果」:「問題はありませんでした」あるいは、「改ざんを発見しました」、
クロスドメインスクリプトが存在します」という表示を行います。ウェブサーバーのダウンなどによってページの取得ができない場合には「コンテンツかページが取得できませんでした」という表示がされます。
「ページ数」:解析を行った対象となるページの数を表示します。
「改ざん」が発生した場合には、リスト形式の行が赤でハイライトされます。同じく「クロスドメインスクリプト」が見つかった場合には、リスト形式の行が黄色になります。この履歴は、60日分まで表示されます。それ以前の履歴はレポート機能にて参照してください

5. ページ切り替え

Q

改ざん時の切り替え機能について教えてください。

A

弊社指定のタグをウェブページに埋め込んでいただき、改ざん時の切り替え機能をONにしていただくと、万が一ウェブページが改ざんされ、弊社システムが改ざんを検知した場合、改ざんされたページは、ユーザーに閲覧されず、弊社指定のウェブページに切り替わります。

この機能は、改ざんされたページのみを切り替えることも、タグを挿入した全ページを切り替えることもできます。また、クロスドメインがあった場合でも切り替えることができます。
これらの設定は、オプション機能＞改ざん時切り替え機能　から設定が可能です。

Q

改ざん時切り替え機能のタグの貼り方を教えてください。

A

ウェブページの<htm|>タグのすぐ後ろ（直下）に貼り付けてください。登録ドメインと同じドメインである必要があります。

Q

改ざん時切り替え機能のスクリプトは、SSLのページでも機能しますか。

A

はい、機能します。ただし、登録ドメインと同じドメインである必要があります。

Q

ホワイトリストとページ切り替えの関係を教えてください。

A

ホワイトリストは、常に「Safe」と判定します。改ざん時切り替え機能のスクリプトを挿入している場合でも、切り替えは発生しません。

Q

クロスドメインスクリプトの検知とページ切り替え機能の関係を教えてください。

A

Gumblar（ガンブラー）や8080と呼ばれる改ざんは、ページにクロスドメインスクリプトが挿入されて問題のあるファイルが自動的にダウンロードされる事により感染が広がっています。クロスドメインスクリプトを検知したページ切り替え機能を設定している場合、クロスドメインスクリプトを検知した時点でページ切り替え機能が発生します。あらかじめクロスドメインスクリプト機能の許可設定を実施した上で、ページ切り替え機能の設定をONにしてください（ページ切り替え機能のタグを挿入する前に、クロスドメインスクリプト機能の確認をお願いいたします）。

Q

開始URL変更時には以前の改ざん時切り替えタグは有効ですか。

A

いいえ、改ざん時切り替え機能のタグは、開始URLを変更した場合、張り替えていただく必要があります。開始URLを変更した際にはご注意いただきますようお願いいたします。

Q

解約した後の改ざん時切り替えスクリプトについて

A

Web改ざん検知オプションを解約した際には、弊社で提供した改ざん時の切り替えスクリプトを、貴社のウェブページより速やかに削除をお願いいたします。

6. GRED証明書

gred証明書とは何ですか。

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。

gred証明書は、SSLページも利用はできますか。

はい、利用できます。

開始URL変更時には以前のgred証明書タグは有効ですか。

いいえ、gred証明書のタグは、開始URLを変更した場合張り替えていただく必要があります。開始URLを変更した際にはご注意いただきますようお願いいたします。

解約時のgred証明書のタグについて

Web改ざん検知オプションを解約した際には、弊社で提供したgred証明書のタグを、貴社のウェブページより速やかに削除をお願いいたします。

7. ユーザー情報／サブユーザー情報管理

申込時に登録したユーザー以外にユーザーを追加したいのですが。

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。この機能は、Web改ざん検知申込時に初期登録したユーザーのみ利用できます。
それぞれ、ログイン用メールアドレス、アラート用メールアドレスを登録することができます。
このユーザー管理で登録されたユーザーは、各ユーザーのアラート用メールアドレスにメールが送信され、メール内容にパスワードが記載されています。

サブユーザーとは何ですか。

このページでは、サブユーザーとして、Web改ざん検知の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。登録は、申込時に登録した初期ユーザーのみ登録が可能です。

「サブユーザーご担当者名（お名前）」は、パスワード変更時にも必要となる情報です。大切に保管をお願いいたします。
「ログイン用メールアドレス」は一度設定しますと変更はできません。
「アラートメールアドレス」は、「ログイン用メールアドレス」と同一でも構いません。

ユーザーID.パスワードの文字列に制限はありますか。

〈ユーザーID〉

・8文字以上50文字以内

・半角英数字

・使用可能な記号：スペース、ダッシュ（ － ）、アンダースコア（ _ ）、スラッシュ（ / ）、
ピリオド（ . ）、アット・マーク（ ＠ ）

〈パスワード〉

・8文字以上50文字内

・半角英数字

・使用可能な記号：ビックリマーク（！）、ピリオド（ . ）、疑問符（？）、プラス（＋）、ドル（ $ ）、
パーセント（%）、シャープ（ # ）、アンバサンド（&）、アスタリスク（＊）、イコール（＝）、アット マーク（@）

※ユーザーIDは一度登録した場合、変更はできません。

パスワードを忘れました、何か必要な情報はありますか。

パスワードを変更するには、登録したメールアドレスが必要です、また、パスワードの修正を行う過程で担当者名が必要です。担当者名は、サービス登録時のメールに記載されています。担当者名が分からない場合、ご利用のログインID・会社名・アラートメール登録アドレスを明記の上「Web改ざん検知お問い合わせ窓口」mw-option@ml.ntt.comまでご連絡ください。

Q

ユーザー情報の変更

A

ユーザー情報の変更では、「アラート用メールアドレス」と「ご担当者名（お名前）」の変更ができます。「ログイン用メールアドレス」は変更することができません。「アラートメールアドレス」に、改ざん時の警告メール、週間レポートメールが送信されます。

また、この画面にて週間レポートメール、アラートメール（クロスドメイン検知メールを含む）を受け取る、受け取らないという指定をすることができます。「ご担当者名（お名前）」は、パスワードを再設定する際に必要な情報となります。情報は大切に保管をお願いいたします。

8. その他

登録した解析開始URLを変更したいのですが。

お客さまご自身で変更はできません、恐れ入りますが「Web改ざん検知お問い合わせ窓口」mw-option@ml.ntt.comまでご連絡ください。解析開始URLを変更する場合、過去の解析履歴は、削除されます、ご了承いただきますようお願いいたします。

ログインページ推奨ブラウザ

ログインページへログインする場合、最新のブラウザを利用してログインをお願いいたします。ブラウザのバージョンによっては、表示されないなどの現象が報告されております。

また、ブラウザの設定の、TLS1.0を有効にすることで表示される場合もございます。 Internet Explorerの場合、インターネットオプション＞詳細設定＞セキュリティ の項目をご確認ください。

Web改ざん検知オプションを解約したいのですが。

お申し込みの営業担当者または「Web改ざん検知お問い合わせ窓口」mw-option@ml.ntt.comまでご連絡ください。