Biz メール＆ウェブ　Web 改ざん検知オプション

機能概要書

第 1.1 版

2024/7/11

◆目次

1. Web 改ざん検知概要

「Web 改ざん検知サービス」は、インターネットを利用している個人を含む企業や、Web サイトを利用して業務活動を行うユーザーに対して株式会社日立システムズが提供する GRED Web 改ざんチェックプラットフォームを利用した SaaS 型ソリューションです。

(1)Web 改ざん検知機能

・SQL インジェクションやガンブラー等に起因する、自社 Web サイトの改ざんの有無を解析
・マルウェアの埋め込み、悪意のあるスクリプトの埋め込み、オンライン詐欺サイトや Web サイトのコンテンツの不正な改ざんを検知
・サイトに存在するクロスドメインスクリプト（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）を検知・報告
・企業の Web サイトを自動で定期的に解析
・問題が検知されると、アラートメールで管理者に通知
・対象となる、自社の URL を指定するだけでサービス利用が可能
・GRED 証明書で自社 Web サイトの安全性をアピール
・問題発生時に自動的に安全なページに切り替え

(2)サービスの提供対象および範囲

Web 改ざん検知は、Web サイトを保有／運営している企業、またはマルウェアの対策を行いたい企業、若しくは個人を対象とするセキュリティサービスとなります。ただし当サービスは、対象となる顧客の自社及び自社において運営を行っているサイト以外へ提供するものではありません。

2. Web 改ざん検知機能

(1)解析について

お申し込み時に事前に登録した「解析開始 URL」からユーザーにより指定されているドメイン内のリンクをお申し込みプラン(10 ページから 10,000 ページ)に応じたページ数まで自動的にクローリングを行い、Web の改ざんの有無を解析します。

たとえば、www.ntt.com/index.html から複数のサイトにリンクがあり、お申し込み時に指定されている ntt.com のドメインである場合にはクローリングを行います。しかし、他のドメイン（たとえば、ocn.ne.jp)にリンクされている場合にはクローリングを行うことはありません。開始 URL 対象ドメインについてはサービス申し込み時に指定可能です。
改ざん解析の回数は、1 日 1 回となります。解析のタイミングは自動計算されます。

対象となる Web サーバー側の負荷としては、通常のユーザーが行う Web ブラウジングと同等の負荷となります。Web サーバー側には負荷をかけずに、解析作業はすべて GRED 側のサーバーにて行われます。
解析の結果、不正なサイトに改ざんがあった場合には、あらかじめ登録済みのメールアドレスに連絡することができます。また、管理画面上でもその旨を確認可能になります。
また、後述するレポート作成の機能にてデータを入手することも可能です。Web 改ざん検知は、1 週間に一度（月曜日）、1 週間の解析状況(1 週間で解析した回数、改ざんを通知した回数、クロスドメインスクリプトの検知回数、解析した Web ページ数[平均])を登録されたアラート用メールアドレスに報告をいたします。

(2)ホーム画面について
ホーム画面では、解析を行った最終結果と、過去の履歴のカレンダーが表示されます。この画面がログイン後の初期画面となっています。最終結果には取得したスクリーンショットと、問題がない場合には緑のアイコン、改ざん等が発生している場合には赤のアイコン、クロスドメインスクリプト等の注意が必要な場合には黄色のアイコンが表示されます。サイト改ざんを検知、あるいはクロスドメインスクリプトが検知された場合にはアイコンの下に「再チェックする」というボタンが表示されます。これは、通常のスケジュールとは別に、問題を修正した後に再度チェックを行いたい場合に利用します。1 日に 2 回まで利用する事が可能です。カレンダー側には、対象の日に Web がどのような状態であったのかを履歴として表示します。履歴表示も、緑・赤・黄のアイコンが表示され、赤・黄の場合にはクリックする事によって詳細履歴が表示されます。また、画面下部には「最新の解析結果履歴」リストと、「最新のクロスドメイン一覧を見る」、「最新の解析 URL のリストをダウンロード」ボタンがあります。
「最終結果」は、1 日に実施した解析結果をそれぞれ表示します。「最新のクロスドメイン一覧」ボタンは、最後の URL 解析結果によって見つかったクロスドメインスクリプトの一覧を表示します。クロスドメイン自体の URL と、そのスクリプトが見つかった URL を表示する事ができます。「最新の解析 URL のリストをダウンロード」ボタンは、最後の解析を行った対象 URL 全てをテキストファイルにてダウンロードを行う事が可能です。このリストをダウンロードし、どの URL に対して解析を行ったかを確認する事が可能です。

(3)解析履歴
解析履歴機能は、サービスを開始してからの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」: Web 解析を実施し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。Web 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」:解析対象のページ数を表示します。「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、2 ヶ月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。

(4)レポート作成

レポートの作成機能は、1 か月単位で解析結果と詳細を表示することができます。またブラウザの印刷機能を利用することによってレポートを印刷することも可能です。ドロップダウンボックスから、レポート表示の開始年月と終了年月を指定して、「レポートを作成する」ボタンを押下します。月ごとの改ざんを通知した回数と解析した Web ページ数の平均を表示し、解析結果の詳細(改ざんを検知したページの URL、改ざんの種類と説明、脅威名とソース)も同様にリストで表示します。

(5)解析内容の設定

Web の改ざん検知を行う場合の解析内容の設定を行います。項目として a. 基本設定、b. 除外設定、c. クロスドメイン設定、d. オプション設定があります。また、現在の設定等を一覧で表示する「現在の利用状況一覧」表示リンクがあり、これをクリックするとリスト形式で現在の設定が表示されます。

a. 基本設定

基本設定では、メニュータイトルと解析する対象を階層レベルで指定する事ができます。
「メニュータイトル」とは、ページ上部の「Web 改ざんチェック」と表示されているタブの下部にある「開始 URL」のタイトルです。デフォルトではお申し込みいただいた開始 URL が表示されています。これを全角 20 文字までで設定する事が可能です。「Web 解析対象階層の指定」は、解析を行う Web サイトの階層指定を行う事によって、サイト全体ではなく指定した部分のみ解析を行う事が可能になります。

例えば、100 階層まであるサイトの開始 URL から 3 階層までのみの解析を行う様な制限をかけたい場合に指定します。この設定をした場合には、指定階層に解析が達し、お申し込みプランに応じた最大ページ数に至らない場合でも解析が終了します。また、この項目の指定を行わない場合には「無制限」となり、階層構造は考慮せずにライセンスに応じた最大ページまで解析を実施します。

b. 除外設定

除外設定では、2 つの機能を提供しています。「ホワイトリスト」と「除外 URL」の設定です。それぞれ以下のような機能を提供します。

ホワイトリスト:

ホワイトリストは対象のページのアドレスを指定し、そのページの解析結果を必ず「OK」とします。そのページ内に他のページへのリンクがある場合もクロールし、解析を行います（指定したページのみ解析結果を「OK」とし、他のページは通常通りの解析対象となります）。この機能は、解析対象のページを単純に「OK」という判断にするだけであるため、解析対象のページとしてカウントされる事に注意してください。また、パス（ディレクトリ）指定はできません。ホワイトリストは開始 URL につき 10 ページまで登録可能です。

除外 URL:

除外 URL は、パス（ディレクトリ）を指定し、そのパス以降の解析を行いません。したがって、指定したパス以降は解析ページとしてカウントされません。除外 URL の指定は、必ずパス（ディレクトリ）の指定になります。ページのアドレスは指定することはできません。指定したパス以降が除外の対象となる事に注意してください。除外 URL は開始 URL に対して 100 個のパスまで設定可能です。

c. クロスドメイン設定

Web 改ざん検知では、Web サイト内に記述されている別ドメインのスクリプトを検知して警告を行う機能を提供しています。改ざんによって、意図しないドメインに設置されているスクリプトが埋め込まれている場合、ウイルスの配布や情報の漏えいなどが心配されます。これを防ぐために Web ページの解析実行時に、現在のドメイン以外のサイトに置かれているスクリプトへのリンクが存在した場合、警告を発します。警告はメールにて行われ、該当のスクリプト埋め込みに問題がない場合（意図して埋め込んだスクリプトである場合等）は、許可設定を行う事で警告を行わないようにすることが可能です。

クロスドメイン検知:

この設定項目では、検知の設定と許可しているリスト、クロスドメインスクリプトのクイック登録が表示されます。「クロスドメインスクリプトの検知機能」では、クロスドメインスクリプト検知の有効無効を設定します。「有効」を選択した場合には警告機能を有効にします。「無効」を選択すると、ページにクロスドメインスクリプトが存在しても警告を行いません。また、問題がないと判断するスクリプトを事前に登録することも可能です。「クロスドメインスクリプトを登録する」機能を利用して、事前に問題がないクロスドメインスクリプトを指定する事によって、警告を行わないようにする事が可能です。

「許可リスト」には、上記で事前に指定したクロスドメインスクリプトをリスト形式で一覧表示します。必要がないスクリプトは、リストから選択し削除する事も可能です。
「クロスドメインスクリプトのクイック登録」では、検知したクロスドメイン一覧が表示されます。問題がないと判断したスクリプトのチェックボックスをクリックし、「チェックしたクロスドメインを許可する」ボタンを押下することによって、許可リストに登録して警告を消すことが可能です。この表示には、チェックボックス横の「＋」ボタンを押下する事によってスクリプトが発見された URL も確認する事が可能です。もし意図しないスクリプトが埋め込まれていた場合には、該当の HTML を変更し、修正することによって問題を解決することができます。
※Note：このような改ざんがあった場合には、Web サイトのメンテナンス等に利用する
　　ユーザー名やパスワード等も変更することをお勧めします。

d. オプション設定

Web サイトが「Web 改ざん検知」にて解析されており、安全に利用することができるという証明として「GRED 証明書」を Web サイトに埋め込むことが可能です。また、改ざん検知時にサイト閲覧者が直接ページに訪れることを防止する、「ページ切り替え」の機能を提供しています。これらの機能は、お客さまの Web サイトの HTML に弊社から提供するスクリプトを埋め込むことによって可能になります。

GRED 証明書：
HTML の img タグにより GRED 証明書のイメージを埋め込みます。オプションページのスクリプトをお客さまのページへ「コピー＆ペースト」することによって掲載することが可能になります。Web ページ上での GRED 証明書をクリックすると、Web 改ざん検知の最新検証結果を別ウインドウにて表示します。

改ざん時切り替え機能：
改ざんが発生した場合、サイト訪問者が Web サイトを閲覧するだけでマルウェアがダウンロードされるといったような被害が発生する場合があります。このような事態になると、企業にとって信頼や利益を失うケースが珍しくありません。これを防ぐために、GRED が解析したページに改ざんが見つかった場合、お客さまのサイト訪問者に GRED にて用意している「メンテナンスページ」を表示することが可能です。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、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。HTML タグのすぐ後ろに、ページ内にあるタグを記述しておくことによって自動で画面を切り替える機能を提供します。このタグは、お客さま毎に異なるタグ内容になっています。切り替え機能では、下記の設定を行う事が可能です。

切り替え機能設定：有効・無効

改ざん検知時の画面切り替え機能を有効にするか無効にするかを選択します。

「有効」を選択した場合には、この機能が動作します。また、「有効」を選択した場合には、下記の「切り替え機能適用範囲」および「クロスドメインがあった場合」の設定項目が表示されます（「無効」を選択している場合には、2 つの機能スイッチは表示されません）。これを「無効」にした場合、改ざんやクロスドメインスクリプト検知時にスクリプトを挿入した画面でも切り替えが発生しません。

切り替え機能適用範囲：検知ページのみ・全ページ

「切り替え機能設定」を「有効」にした場合に表示され、切り替えを行うページの範囲を設定します。デフォルトは「全ページ」です。「全ページ」の場合、改ざん等が発生したページのみ切り替えるのではなく、スクリプトが設定されているページ全てで画面切り替えが行われます。「検知ページのみ」に設定した場合は、改ざん等が発生したページに閲覧者がアクセスした場合にのみページ切り替えが発生します。

※Note：切り替え機能を設定するスクリプトが埋め込まれている事が切り替えの機能を実装する事になります。スクリプトが設定されていないページでは画面切り替えの機能は実現できません。

クロスドメインがあった場合：　切り替える・切り替えない

「切り替え機能設定」を「有効」にした場合に表示され、クロスドメインスクリプト検知時の動作を設定します。「切り替える」を選択した場合、クロスドメインスクリプトがページ内にて検知された時に、ページの切り替え機能が動作します。「切り替えない」を選択した場合には、クロスドメインスクリプトの検知時にはページ切り替えが発生しません。

※Note：切り替え機能を設定するスクリプトが埋め込まれている事が切り替えの機能を実装する事になります。スクリプトが設定されていないページでは画面切り替えの機能は実現できません。

3. 管理情報の変更

登録時に入力した情報を変更することができます。

(1)サブユーザー管理

Web 改ざん検知の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可能です。

サブユーザーを登録すると、各ユーザーのログイン用メールアドレスに登録完了メールが送信されます。

Note：登録完了メールのみがログイン用メールアドレスに送られます。アラート等の
　　メールはアラート用メールアドレスに送信されます。

(2)ユーザー情報の変更

ユーザー情報は、「アラート用メールアドレス」と「名前」の変更ができます。ユーザーID は変更することができません。この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。

(3)パスワードの変更

Web 改ざん検知の管理画面にログインするためのパスワードが変更できます。

(4)ログアウト

Web 改ざん検知の管理画面からログアウトします。

4. その他

(1)Web 改ざん検知のアーキテクチャについて

Web 改ざん検知は、Web ブラウザが Web ページを取得することと同じように、ページをダウンロードして HTML に記述されているタグを解析します。この HTML のコード情報をもとにして、問題があるサイトになっているかどうかを判断します。

Web 改ざん検知は、HTML に改ざんによく利用されるような記述、たとえば自社サイトとは全く異なるドメインからファイルのダウンロードを行うようにしている場合や、自社ドメインと異なるサイトへのリダイレクト、実際のダウンロードに脆弱性を利用してユーザーに気付かせずに、ファイルを実行させようとしている場合に改ざんが発生しているという判断を行います。そのほかにもさまざまな判断を行って改ざんを検知します。

現時点(2024 年 7 月現在)での、Web 改ざん検知のエンジンが判断可能な問題は、以下の通りです。

・脆弱性を利用した攻撃を行うサイトへの改ざん
・脆弱な Web サーバーの不正改ざん
・ウイルスやワーム、スパイウェアなどが自動的にダウンロードされるサイトへの改ざん
・ガンブラー等によるサイトの不正改ざん
・フィッシングサイトへの改ざん
・ワンクリック詐欺サイトへの改ざん
・不正セキュリティソフトウェアのダウンロード
・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(見た目改ざん)
・Dark leech Apache Module による Web 改ざん

例)Java スクリプトによる問題のあるサイトの場合:
・Web 改ざん検知が、登録済みの「開始 URL」を開始ポイントとして Web ページをダウンロードする。
・ダウンロードした、HTML のタグを解釈し問題のあるような処理をしていないかどうかを確認する(たとえば、JavaScript が実行されている場合には JavaScript がどのような動作をしているのかを評価する)。
・不正な処理を行っている場合、たとえば不正なファイルをダウンロードしたり、他のサイトへ攻撃(通信)を行うようなコードが記載されている場合には問題のあるサイトとして検知する。

(2)改ざん解析の順序について
ユーザーの指定した「開始 URL」から解析を開始します。Web 改ざん解析機能は、ページに記載されているリンクをたどって解析を行います。リンク先のページが解析対象のドメインにあたる場合には解析対象になり、ページのカウントが行われます。

(3)検知可能な改ざんと検知できない改ざん
a. 検知可能な改ざん

脆弱性悪質サイトへの改ざん: 悪意をもった改ざんによりサイトを変更されて、来訪者の脆弱性を衝いた攻撃を仕掛けるサイト。

不正改ざんサイト:ガンブラーや SQL インジェクション、クロスドメインスクリプティングなどを利用して不正に改ざんされたサイト。

フィッシングサイトへの改ざん：悪意を持った改ざんによりサイトを変更されて、Web への来訪者のさまざまなサイトのユーザーカウントやパスワードを不正に入手しようとする場合。

ワンクリック詐欺サイトへの改ざん： 悪意を持った改ざんによりサイトを変更されて、クリックしただけで契約されたように見せかけて料金請求を求める不正。その他、改ざんによって不正なプログラム（例：ウイルス、ワーム、スパイウェアなどのマルウェアがサイトに埋め込まれて閲覧ユーザーにダウンロードさせるような場合）も検知します。

b. 検知できない改ざん

コンテンツの内容の変更：コンテンツに含まれる文章内容の一部を変更した場合。
たとえば、「インターネットでダウンロードしてきたファイルなど、開く前にチェックをするとウイルスなどの被害を未然に防ぐことができます」というような文章を、「Internet でダウンロードしたファイルなどを開く前にチェックすることによってウイルスなどの被害を未然に防ぐことができます」というように変更した場合や、コンテンツそのものの入れ替えや、更新した場合は検知を行いません。

(4)クローリング仕様

a. クローリングするページ

Web 改ざん検知にて実行されるクローラーは以下のリンクをたどり、データを取得します。

- <meta>タグの refresh に記載されている URL
- <script>タグの src に記載されている URL
- <frame>タグのリンク先
- <iframe>タグのリンク先
- <I ink>タグで参照しているスタイルシートファイル
- <a>タグ

※<a>タグ内のリンクが HTML や Java スクリプトでは無い場合にはクロールしません。スクリプト言語で書かれたファイル(cgi· php など）はクロール対象です。

※リンク先のページがパラメータ付き（？で値が後ろに付いている）の場合は、？より前の部分がクロール済みのページと同一の場合も、パラメータが異なる場合にはクロールします。

- <area>タグのリンク先
- <script>タグに含まれている".php",".cgi", ".asp",".aspx"等が含まれる文字列は URL に復元を試みてリンク先とします。
- <base>タグを考慮してリンク先 URL を生成します。

- リダイレクトされた場合にはリダイレクト元とリダイレクト先の URL を別のものとして考慮します。
- Java スクリプトなどからジャンプしているリンク先は他ドメインであってもクロールします。
- HTTP HEADER でリダイレクトしている URL はクロールします。
- HTML ファイル内で直接読み込まれている CSS ファイルは別ドメインであってもクロールします。

b. ドメイン指定について

- Web 改ざん検知のクローラーは、解析開始 URL のドメインを登録ドメインと解釈します。この場合、同じドメインのページだけたどります。
- ディレクトリも指定されている場合は、ディレクトリもマッチするものだけをたどり先とします。

ドメイン名は後方一致で確認します。
抽出した URL のドメインの後方に、指定されたドメインが含まれていれば該当ドメインであると判断します。
ディレクトリは前方一致で確認します。
ドメインと同時にディレクトリも指定されている場合、抽出した URL にある directory の先頭に、指定されたディレクトリが含まれている場合に該当したものであるという判断を行います。

これら、全ての条件も満たしたものをたどり先とします。

（例 1）
「www.ntt.com」がドメインとして指定されていれば、
http://www.ntt.com/index2.html は ntt.com が含まれており、条件を満たすため、たどり先となります。

（例 2）
「www.ntt.com/shop」がドメインとして指定されていれば、http://www.ntt.com
/shop/index.html はドメインが後方一致で該当し、ディレクトリは「shop」があるため前方一致となります。したがって、この URL はクローリング対象となります。http://blog.ntt.com/shop の場合、ドメインは後方一致しますが、ドメインが「blog」であるため、「www」と一致しません。したがって、この URL はクローリング対象とはなりません。

（例 3）
「www. ntt.com」がドメインとして指定されると、http://www.ntt.com/index.html はドメインが後方一致で該当し、この URL はクローリング対象となります。しかし、「www」が指定してあるため、たとえば http://blog.ntt.com/や、http://info.ntt.com/, http://www2.ntt.com/等は、クローリング対象とはなりません。http://hoge.www.ntt.com/の場合にはクローリング対象となります。

c. PDF ファイルの扱い

現状(2024 年 7 月現在)では PDF ファイルをダウンロードしていません。そのため、PDF ファイルを解析対象としてはいません。

d. クロールで取得したファイルの解析について

ダウンロードしたファイルは解析対象かどうかを判断した上で解析します。URL の拡張子、 Web サーバーからのレスポンスヘッダ、コンテンツの中身を参照して、Windows の実行ファイル(exe , dll , sys , drv , cpl , ocx , scr)はプログラムの解析を行います。HTML ファイルなどのテキストファイル(js , css)も同様にチェックを行います。

e. 圧縮ファイルについて

圧縮ファイル(zip , jar)はファイルを取得して解凍した上で、プログラムファイルが含まれていればプログラム解析を実施します。

5. 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。