

1. サービスの実施
乙は甲に対し、本書記載の条件に従って、上記のサービス(以下「本サービス」という)を実施します。
2. 本サービス実施の前提条件
 - (1) 本サービスの利用はサービス提供者が定める「GREDセキュリティサービスの利用規約」(以下「利用規約」という)に同意のうえ、当該利用規約を遵守することを前提とします。また、サービス提供者が別途定める申込み手続きがあるときは、これに従うものとします。
 - (2) 本サービスは、セキュアブレイン株式会社(以下「サービス提供者」という)が運営・提供するものであり、サービス提供者から直接本サービスの実施に関する通知、連絡等がなされる場合があります。
3. 本サービスの内容
本サービスの詳細は、利用規約に記載のとおりとします。
4. 本サービスの緊急停止
 - (1) 乙またはサービス提供者が著しい負荷や障害がシステムに与えられ正常な本サービス提供を行えないと判断した場合、本サービスの全部または一部を緊急停止する場合があります。甲の利用が合法的でかつ技術的に問題がなく、本契約または利用規約に定めるいずれの禁止事項にも抵触しない場合であっても、甲は、本サービスの緊急停止を認めるものとします。
 - (2) 乙またはサービス提供者は、本サービスの利用に伴うシステムの稼働が甲に著しい損害を与える可能性を認知した場合、甲に通知なく、システムの緊急停止を行う場合があります。甲は、このような緊急停止があることをあらかじめ承認するものとします。
 - (3) 乙およびサービス提供者は、原則として甲からの本サービスの緊急停止の要請を受け付けません。
 - (4) 本サービスの緊急停止ができなかったことによって、甲が損害を被った場合でも、乙またはサービス提供者は一切の損害賠償を負いません。
6. 最低利用期間
 - (1) 本サービスの最低利用期間は、実施開始日から1か月とします。ただし、実施開始日が月の途中である場合は、翌月1日から起算するものとします。
 - (2) 最低利用期間中に本サービスの全部または一部を解約する場合、甲はその残存期間の契約金額相当額を違約金として乙に支払うものとします。なお、解約日が月の途中である場合、残存期間は翌月1日から起算するものとします。
7. 利用規約の改定
 - (1) 利用規約は、相当の期間を設けて予告のうえ、甲の了承を得ることなく変更されることがあるものとし、この場合、本サービスの提供条件は変更後の利用規約によるものとします。
 - (2) 利用規約の最新版は、以下URLに掲載されるものとします。
<http://www.gred.jp/saas/other/agreement.html>

以 上

GRED Web 改ざんチェック

サービス仕様書兼機能概要書

(初 版) 2009/02/27

(第 2 版) 2009/03/16

(第 3 版) 2009/06/24

(第 4 版) 2009/12/01

(第 5 版) 2009/12/02

(第 6 版) 2010/02/16

(第 7 版) 2010/05/20

(第 8 版) 2010/07/01

(第 9 版) 2011/12/14

(第 10 版) 2012/04/10

(第 11 版) 2012/08/28

(第 12 版) 2013/04/01

(第 13 版) 2013/09/05

(第 14 版) 2013/09/30

(第 15 版) 2013/12/05

(第 16 版) 2014/07/17

(第 17 版) 2014/12/04

(第 18 版) 2015/09/07

株式会社 セキュアブレイン

目次

1. Web 改ざんチェック 概要	4
2. 基本サービス概要	4
a. サービスの提供対象及び範囲	4
b. Web 解析機能解説	4
i. Web 解析	4
ii. ホーム	8
iii. 解析履歴	8
iv. レポート作成	9
v. 解析内容の設定	9
c. 管理情報の変更	13
i. ユーザー管理	13
ii. ユーザー情報の変更	14
iii. パスワードの変更	14
iv. ログアウト	14
3. その他	14
a. テクニカルサポート	14
b. Web 改ざんチェック Web サイトの真正性について	14
c. サービスの申し込みについて	15
d. サービス内容の変更について	15
e. サービス期間終了時について	15
4. クローリング仕様の解説	16
5. FAQ	18

※ このドキュメントの内容は2015年9月7日現在の情報です。内容について、断りなく修正及び改定することがございます。

このドキュメントの著作権は、株式会社セキュアブレインが所有しております。このドキュメントの一部または全部の内容について、複製・引用など断りなく行うことは禁止いたします。

1. Web 改ざんチェック 概要

「Web 改ざんチェック」は、Internet 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する SaaS 型ソリューションです。

Web 改ざんチェック機能

- SQL インジェクションや gumblar 等に起因する、自社 Web サイトの改ざんの有無をチェック
 - ✧ 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チェック
- 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 を登録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. 基本サービス概要

a. サービスの提供対象及び範囲

Web 改ざんチェックは、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。

自社以外のサイトに対するチェックを検討されている場合には、弊社営業までご連絡いただけますようお願いいたします。

b. Web 改ざんチェック機能解説

i. Web 改ざんチェック

機能解説

ユーザーが事前に登録した「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ライセンスに応じた¹ページ数まで自動的にクローリングを行い、Web の改ざんの有無をチェックします。

¹ 1000 ページのチェックが標準です。1000 ページ以上のライセンスに関しては、販売店あるいはセキュアブレインへご連絡ください。

たとえば、www.securebrain.co.jp/index.html から複数のサイトにリンクがあり、それが指定されている securebrain.co.jp 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、gred.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 1 対象ドメインについてはサービス申し込み時にそれぞれ 5 まで指定可能です。

改ざんチェックの回数は、購入時のライセンスに応じて 1 日 1 回・4 回・8 回となります。チェックのタイミングは回数に応じて自動計算されます。

対象となる Web サーバ側の負荷としては、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 サーバ側にはストレスをかけずに、チェック作業はすべて GRED 側のサーバにて行われます。

チェックの結果、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、管理コンソール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 改ざんチェックは、1 週間に一度 (月曜日)、1 週間のチェック状況 (1 週間でチェックした回数、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、チェックした 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。

Web 改ざんチェックのアーキテクチャについて

Web 改ざんチェックは、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チェックします。

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 改ざんチェックは、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の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 (2015 年 9 月現在) での、Web 改ざんチェック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

- ・gumblar 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（見在目改ざん）
- ・Darkleech 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 改ざんチェックが、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行っていないかどうかを確認する。（たとえば、Java Script が実行されている場合には Java Script がどのようなことを行っ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のダウンロードを行ったり、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。

改ざんチェックの順序について

ユーザーの指定した「開始 URL」からチェックを開始します。Web 改ざんチェック機能は、ページに記載されているリンクをたどってチェックを行います。リンク先のページがチェック対象のドメインにあたる場合にはチェック対象になり、ページのカウントが行われます。

複数の「開始 URL」が登録されている場合は、「開始 URL」が登録されている順番にてチェックを行います。このプロセスを契約ページ数まで行います。

※Note: Web 改ざんチェックは、開始 URL のページからリンクをたどって、対象ドメインのページかどうかを確認していますが、同じ開始 URL からのリンクをたどってチェックする場合には一度チェックした URL はカウントしません。しかし、複数の開始 URL を登録している場合、それぞれの開始 URL に同じページがリンクされている場合が考えられます。その場合には同じページを複数回カウントします。クローリングの仕様に関しては同様に第 4 章も参照ください。

検知可能な改ざんと検知できない改ざん

1) GREDにてチェックの結果、検知可能な問題は以下ようになります。

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： *gumblar* 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 への来訪者の様々なサイトのユーザーア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。

2) 検知ができない改ざんは以下のようなものが考えられます。

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。

ii. ホーム

ホーム画面では、チェック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、通常のライセンスに応じた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。

「最新の解析結果履歴」は、1日に実施したチェック結果をそれぞれ表示します。この項目は、1日のチェック回数に応じてリストが更新されます。

「最新のクロスドメイン一覧」ボタンは、最後の URL チェック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、最後のチェックを行った対象 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、チェックをどの URL に対して行ったかを確認する事が可能です。

iii. 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。Web サーバ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」： チェック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、2週間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。

iv. レポート作成

レポートの作成機能は、1か月単位でチェック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、「レポートを表示する」ボタンを押下します。

月ごとの改ざんを通知した回数とチェックした Web ページ数の平均を表示し、チェック結果の詳細（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）も同様にリストします。

v. チェック内容の設定

Web のチェックを行う場合の設定を行います。項目として「基本設定」、「除外設定」、「クロスドメイン設定」、「オプション」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。

1) 基本設定

基本設定では、メニュータイトルとチェック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」ごとのタイトルです。デフォルトでは「web1」、「web2」等のように表示されています。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チェック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 階層までのみのチェックを行う様な制限をかけたい場合に指定します。

この設定を行った場合には、指定階層にチェックが達し、購入ライセンスに

応じた最大ページ数に至らない場合でもチェックが終了します。

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チェックを実施します。

2) 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、そのページのチェック結果を必ず「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、チェックを行います。（※指定したページのみチェック結果を「OK」とします。他のページは通常通りのチェック対象となります。）

この機能は、チェック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、チェック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1つの開始 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、そのパス以降のチェックを行いません。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、1つの開始 URL に対して 10 個のパスまで設定可能です。

3) クロスドメイン設定

Web 改ざんチェック機能では、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検知の許可」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。「検知する」を選択した場合には警告機能を有効にします。「検知しない」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。

4) オプション機能

Web サイトが「Web 改ざんチェック」にて改ざんチェックを行っており、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、お客様の 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。

GREED 証明書：

HTML の `img` タグにより GREED 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様のページへ COPY/PASTE 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 GREED 証明書をクリックすると、Web 改ざんチェック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、GREED がチェックを行なったページに改ざんが見つかった場合、お客様のサイト訪問者に GREED 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ことで、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可能です。

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、お客様毎に別の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「設定する」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「設定する」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。

c. 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。

i. ユーザー管理

Web 改ざんチェック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 改ざんチェック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。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、メール内容にパスワードが記載されています。

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。

ii. 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、週刊レポートメールが送信されます。また、この画面にて週刊レポートメール、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。

iii. パスワードの変更

Web 改ざんチェックの管理コンソールにログインするためのパスワードが変更できます。

iv. ログアウト

Web 改ざんチェックの管理画面からログアウトします。

3. その他

a. テクニカルサポート

Web 改ざんチェックをご利用いただくユーザーは、サービスに関する技術的なお問い合わせについて、土日祝祭日を除く 9:00～12:00 13:00～17:00 の間、電話および電子メール（電子メールは 24 時間お送りいただけることが可能です。上記営業時間外に電子メールをいただきました場合は、翌営業日にご連絡差し上げます。）にて受けることができます。

ただし、問題の内容によっては回答にお時間を頂くこともございます。

テクニカルサポートへのコンタクト先は以下のとおりです。

- メールフォームによるお問い合わせ

URL : <https://www.securebrain.co.jp/form/gredss/sbformmail.php>

※必要項目を記載の上、ご連絡いただきますようお願いいたします。

- お電話によるお問い合わせ

電話番号 : 0120-988-131

※ダイヤル後、アナウンスに従い『1』を押してください。

※営業時間 月～金、9:00～12:00 13:00～17:00 土日祝祭日を除く

b. Web 改ざんチェック Web サイトの真正性について

Web 改ざんチェックの管理コンソールには、「PhishWall サーバ」が導入されています。ユーザーがアクセスする管理コンソールの Web が真性であることを、弊社の PhishWall クライアントにて確認することが可能です。

PhishWall は Web サーバと PC の間で認証情報をやり取りすることにより、参照している Web サイトが真正である（偽装されていない）ことを、PC 側から認証するソリューションです。

真正な場合にはブラウザ上のクライアントに緑のシグナルで目立つように表示します。閲覧者はひと目でそのホームページが本物であることを確認でき、安心して Web サイトを利用していただくことが可能です。

この PhishWall クライアントはセキュアブレインの Web サイト (<http://www.securebrain.co.jp/products/phishwall/install.html>) から無償でダウンロードできます。セキュリティ強化のために、PhishWall クライアントをぜひ導入してください。

また、Web 改ざんチェックにて導入している「PhishWall サーバ」についての詳細な情報は、以下の URL をご参照いただくか、弊社営業までご連絡いただけますようお願い申し上げます。

<http://www.securebrain.co.jp/products/phishwall/index.html>

c. サービスの申し込みについて

弊社または、販売代理店所定の申込様式をご用意しております。詳細につきましては弊社営業、または販売代理店へのお問い合わせください。

d. サービス内容の変更について

Web 改ざんチェック申込時の登録内容を変更したい場合には、（例：対象ドメインの変更追加、開始 URL の変更追加など）販売代理店または、テクニカルサポートにて承ります。

（テクニカルサポートへのご連絡先は、上記「テクニカルサポート」の項目をご参照ください。）

e. サービス期間終了時について

Web 改ざんチェックの契約期間が満了し、サービスの提供が終了した場合は、定期的な Web 改ざんチェック機能が停止します。履歴を参照するためにログインは可能です。（ログイン用のアカウントは自動的に削除されません。）

サービスを継続される場合には、販売代理店または弊社営業までご連絡ください。

4. クローリング仕様の解説

クローリングするページ

=====

Web 改ざんチェック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
- <link>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。

ドメイン指定について

=====

- Web 改ざんチェックのクローラーは、指定がない場合、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。

- ドメインの指定がされている場合には、該当ドメインであればたどり先とします。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。

- 比較方法

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とり先とします。

(例 1)

「securebrain.co.jp」がドメインとして指定されていれば、

http://www.securebrain.co.jp/index2.html は securebrain.co.jp が含まれているので条件を満たすためとり先となります。

(例 2)

「securebrain.co.jp/shop」がドメインとして指定されていれば、

http://www.securebrain.co.jp/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 はクロール対象となります。

http://www.securebrain.co.jp/blog の場合、ドメインは後方一致しますが、ディレクトリが「blog」であるため、「shop」と一致しません。したがって、この URL はクロール対象とはなりません。

(例 3)

「www.securebrain.co.jp」がドメインとして指定されると、

http://www.securebrain.co.jp/index.html はドメインが後方一致で該当し、この URL はクロール対象となります。

しかし、「www」が指定してあるため、たとえば http://blog.securebrain.co.jp/ や、http://info.securebrain.co.jp/、http://www2.securebrain.co.jp/等は、クロール対象とはなりません。http://hoge.www.securebrain.co.jp/の場合にはクロール対象となります。

PDF ファイルの扱い

=====
現状（2015年9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。

クローラで取得したファイルのチェックについて

=====
ダウンロードしたファイルはチェック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。

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. FAQ

質問 1

Web 改ざんチェックは、Web ページをクローラするとのことですが、自社のサイトは、レンタルサーバです。サーバに負荷が掛かるのが心配ですが、大丈夫ですか？

回答

検索エンジンがコンテンツを自動巡回するように、GRED が Web 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、Web アクセスログにも残ります。Web サーバに対しては通常のブラウザからの Web アクセスと同様のふるまいを行いますので、負荷は必要以上にかかりません。

質問 2

Web 改ざんチェックでは、フィッシング対策はできますか？

回答

スクリプトを埋め込まれることにより、Web ページが改ざんされフィッシングサイトとなるケースも報告されています。このようなケースでは、Web 改ざんチェックでチェックし、発見が可能です。また弊社では、Web サイトの真正性を保証する

フィッシング詐欺対策ソリューションとして PhishWall もご用意しています。

質問 3

自社で管理している Web サイトは、ファイアウォール・IDS・ウイルスチェック・ファイルの改ざん検知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 改ざんチェックは必要ですか？

回答

これらのツールで防御する範囲と Web 改ざんチェック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 改ざんチェックです。

質問 4

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。

回答

GREED Web 改ざんチェックは、SaaS 型なのでインストール・設定作業が不要です。簡単登録でかつ異常時のメールお知らせ機能があるので、毎日のログイン作業も不要です。

- ✓ 変更された箇所を日本語のレポートとして報告します。
- ✓ チェック間隔は標準 1 日 1 回、4 回、ライセンスによって 8 回を選ぶことができます。
- ✓ Web サーバの種類を選びません。

質問 5

無償トライアル版での制限事項を教えてください。

回答

Web 解析は 1 日 1 回、1 社様あたり登録・チェックは 1 ドメインまで、最大 10 ページが解析対象となります。これらの機能が 14 日間ご利用になれます。

質問 6

無償トライアル版と正式版との違いを教えてください。

回答

正式版では、以下の機能が追加されます。

- ✓ 1 日の Web 改ざんチェックの回数（※申込時の選択によって決定）
- ✓ 複数ドメイン登録
- ✓ 複数ユーザー登録機能
- ✓ GREED 証明書・改ざん時のページ切り替え機能
- ✓ クロスドメイン検知機能

今後、さらなる機能強化を図ってまいります。

質問 7

ログインするための ID とパスワードを忘れました。

回答

TOP ページ「パスワードをわすれたら」から確認いただけます。ID は、ページ下部「お問い合わせ」からお問い合わせ可能です。

質問 8

ユーザーID・パスワードの文字列に制限はありますか？

回答

ユーザーID・パスワードの文字列に制限は以下の通りです。

〈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 文字以内
- ・ 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(@)

質問 9

Web 改ざんチェックにおける評価対象ファイルをおしえてください

回答

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ます。

質問 10

携帯用サイトに対応していますか？

回答

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サイトは検知をすることができます。

質問 11

Web 改ざんチェックは「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？

回答

弊社で開発したエンジンのコアではブラックリストを使用していません。ただし、PhishTank 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。

質問 12

認証を経た先に表示されるページをチェックしますか？

回答

現在のところベーシック認証などの認証を行った後に表示されるページはチェック対象になっておりません。

質問 13

Flash で作成されたページはチェックできますか？

回答

現在の仕様では **Flash** に埋め込まれたリンクからはチェック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、チェックが可能となります。

質問 14

クロスドメインスクリプトを検知しました、対処方法を教えてください。

回答

Web 改ざんチェックにログイン後クロスドメインの許可設定を行います。最近見つかったスクリプト一覧から許可するものを選択します。許可するものが正規のものであるか予め確認をお願いいたします。

質問 15

SSL のページに GRED のスクリプト（証明書・ページ切替機能）を挿入したい
と思います、可能でしょうか？

回答

スクリプトの後半部分の `src="http://www.gred.jp/saas/seal.gif?sid=***`
部分の `src` 以下の `http` を `https` に変更して貼り付けしてください。