

gred セキュリティサービス

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

株式会社 セキュアブレイン

目次

1. gred セキュリティサービス 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. ウェブ解析機能解説	5
i. ウェブ解析	5
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. ファイル解析機能解説	13
i. ファイル解析	14
ii. 解析履歴	15
iii. 駆除ツール	15
d. 管理情報の変更	15
i. ユーザー管理	15
ii. ユーザー情報の変更	16
iii. パスワードの変更	16
iv. ログアウト	16
3. その他	16
a. テクニカルサポート	16
b. gred セキュリティサービス Web サイトの真正性について	16
c. サービスの申し込みについて	17
d. サービス内容の変更について	17
e. サービス期間終了時について	18
4. クローリング仕様の解説	19

5. FAQ..... 21

※ このドキュメントの内容は2010年7月1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. gred セキュリティサービス 概要

「gred セキュリティサービス」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しての SaaS 型ソリューションです。

「gred セキュリティサービス」は、販売形態に応じて「ウェブ解析」と「ファイル解析」の 2 つの機能、あるいは「ウェブ解析」のみの機能を提供します。

ウェブ解析機能

- SQL インジェクションや gumblar ウイルスの感染等に起因する、自社ウェブサイトの変更の有無を解析
 - ✧ 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ウェブ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を検知・報告
- 企業のウェブ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
- 解析対象となる、自社の URL を登録するだけでサービス利用が可能
- gred 証明書で自社ウェブサイトの安全性をアピール
- 問題発生時に自動的にページを切り替え

ファイル解析機能

- 仮想インターネット環境でファイルを実行し、詳細な解析レポートを数分で生成
- レポート内容
 - ✧ ファイルがマルウェアか否か
 - ✧ 作成/削除するファイルやレジストリ、ネットワーク上での挙動
 - ✧ 解析対象のファイルが行なった通信のイメージ図と表示する画面のキャプチャイメージ等
- マルウェアの場合には、フィックスツールを提供
- 数分でレポートを提供
- 管理コンソールから過去の解析結果を取得可能

2. 基本サービス概要

a. サービスの提供対象及び範囲

gred セキュリティサービスは、ウェブサイトを保有/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

イト以外への解析を提供するものではありません。

自社以外のサイトに対しての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. ウェブ解析機能解説

i. ウェブ解析

機能解説

ユーザーが事前に登録した「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 の改ざんをチェックします。

たとえば、`www.xxxxxx.com/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 `xxxxxx.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(例えば、`yyyyyy.com`)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。解析開始 URL と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 10 まで指定可能です。

解析の回数は、購入時のライセンスに応じて 1 日 4 回・8 回・24 回となります。解析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、解析作業はすべて gred 側のサーバにて行われます。

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、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。

gred セキュリティサービスは、1 週間に一度（月曜日）、1 週間のチェック状況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。

解析のアーキテクチャについて

gred セキュリティサービスは、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釈します。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。

gred セキュリティサービスは、HTML に改ざんによく利用されるような記述、た

¹ ライセンスの形態に応じて、300 ページあるいは 1000 ページのチェックが標準です。詳細な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。

例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（2010年7月現在）での、gred セキュリティサービスのエンジンが判断可能な問題は、以下の通りです。

- ・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
- ・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

例) Java スクリプトによる問題のあるサイトの場合：

- ・gred セキュリティサービスが、登録済みの「解析開始 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。

解析の順序について

ユーザーの指定した「解析開始 URL」から解析を開始します。Web 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。

複数の「解析開始 URL」が登録されている場合は、「解析開始 URL」が登録されている順番にて解析を行います。このプロセスを最大解析ページ数まで行います。

※Note: gred セキュリティサービスは、解析開始 URL のページからリンクをたどって、解析対象ドメインのページかどうかを確認していますが、同じ解析開始 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、複数の解析開始 URL を登録している場合、それぞれの解析開始 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** にて解析の結果、検知可能な問題は以下ようになります。

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カウントやパスワードを不正に入手しようとする場合。

1 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。

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。

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、2 か月分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解析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、対象の日にウェブ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。

「最近の解析結果履歴」は、1日に実施した解析結果をそれぞれ表示します。この項目は、1日の解析実施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 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、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。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」： 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、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、「レポートを表示する」ボタンを押下します。

月ごとの改ざんを通知者した回数とチェックしたウェブページ数の平均を表示し、解析結果の詳細も同様にリストします。

v. 解析内容の設定

ウェブの解析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」、「オプション機能」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解析する対象を階層レベルで指定することができます。

「メニュータイトル」とは、ページ上部の「ウェブ解析」と表示されているタブの下部にある「解析開始 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20文字までで設定する事が可能です。

「ウェブ解析対象階層の指定」は、解析を行うウェブ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

ウェブ解析機能では、ウェブ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。これを防ぐためにウェブ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、ウェブ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

ウェブサイトが「gred セキュリティサービス」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」をウェブ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、お客様のウェブサイトの 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。

ウェブページ上での **gred** 証明書をクリックすると、**gred** セキュリティサービス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、サイト訪問者がウェブサイトを開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 **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、ウェブ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. ファイル解析機能解説

ファイル解析機能は、実行ファイルの挙動を短時間で解析して詳細な解析レポートを生成します。解析レポートは、マルウェアか否かの判断、作成/削除するファイルやレジストリ、ネットワーク上での挙動、解析対象のファイルが行なった通信相手、およびその内容、通信のイメージ図、表示する画面のキャプチャイメージ等の詳細な情報を得ることができます。

解析したファイルがマルウェアだった場合には、必要に応じて駆除ツールを利用することが可能です。この駆除ツールはセキュアブレインのサポートより入手可能です。また、管理コンソールから、過去に解析したファイルの解析レポートを参照することも可能です。

新種のマルウェアが検体としてセキュリティベンダーに提出されてから、そのマルウェアの攻撃の詳細や、駆除ツール・パターンファイルが配信されるまでに数時間から数日かかるため、その間の被害の拡大は避けられません。特に標的型攻撃を受けている場合は、検体入手が困難な為、マルウェア自体の発見が遅れます。

『**gred** セキュリティサービス』は、パターンファイルを使用せず、不審なプログラムを仮想のインターネット環境で実際に実行し、その結果を元に解析を行います。これを動的解析といいます。

その為、他ウイルスベンダーの提供するレポートよりも更に詳細な解析レポートを生成することが可能です。『新種のマルウェアや標的型攻撃に対して何もできない』空白の時間（ゼロアワー）を劇的に短縮します。

i. ファイル解析

ファイル解析の画面より、解析を行いたいファイルをアップロードします。画面上の「参照」ボタンにてローカルのファイルを指定して、「解析する」ボタンを押下します。これにより **gred** セキュリティサービス側にデータをアップロードし、解析が開始されます。解析が開始した時点と完了時に、事前に登録した **email** アドレスにそれぞれ通知されます。

解析可能なファイルは、**Windows** 用 **32bit PE** プログラムファイル（通常の拡張子が **EXE**、あるいは **SCR** のファイル）で、単独のモジュール（他の **DLL** やその他のファイルが必要ない）と、**DLL** モジュール単体でのチェックが可能です。圧縮してアップロードする場合には、**ZIP** 形式にてアップロードください。また、**ZIP** のパスワードをつける場合には「**infected**」にしてください。

また、**DOS** の **COM** プログラム、**Microsoft Office** などのデータファイルを解析することはできません。

標準ではファイルの解析依頼は **30** 分毎に **1** ファイル、月間 **30** ファイルまでの解析が可能です。

解析結果は、**gred** セキュリティサービスの画面より確認可能です。（通知 **email** にもリンクが記載されています。）「ファイル情報」「詳細情報」「ネットワーク通信図」のセクションに分かれます。

「ファイル情報」： ファイル情報セクションには、「ファイル名」、解析の結果による「プログラムの分類」、「プログラムのサイズ」、「プログラムの作成日時」、「**MD5** のハッシュ値」、「**SHA1** のハッシュ値」が表示されます。

また、アンチウイルスでのスキャン結果も同時に表示します。アンチウイルスベンダーの定義ファイルが更新されると、チェック時に未検知だったファイルも検知することがあるために、アップロード時だけではなく定期的にファイルをスキャンし、その結果を表示します。

「詳細情報」： 詳細情報は、**Windows XP (SP2)** にて実際にプログラムを動作させた時のレポートが表示されます。実際に作成及び削除されるファイルや、レ

ジストリキー、改ざんされるファイル、作成されるミューテックス、検索するファイルやフォルダ、ファイルが通信する先や通信内容などの解析結果を表示します。

「ネットワーク通信図」： ファイルが通信を行う対象のアドレスなどを図表表示します。

ii. 解析履歴

画面の左側に、今まで解析を行った日付とファイルを表示します。これらのリンクをクリックすることによって過去の解析結果を得ることが可能です。

この履歴は、解析したファイルすべてを保存しています。

iii. 駆除ツール

プログラムの動作を解析した結果を元に、作成されるファイルやレジストリなどを復旧させるツールを提供することが可能です。これは無償で提供しています。

入手するためには、テクニカルサポートに対象のファイル名などをご連絡いただくことによって提供を行います。

駆除ツールは、ファイル解析の動的解析結果（レジストリやファイルの追加などの動き）に基づいて作成されます。そのため、すべての問題を解消するわけではありません。また、駆除ツールに関しての技術的サポートは提供しておりません。

d. 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

gred セキュリティサービス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、**gred** セキュリティサービス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。また、ユーザーによっては特定のウェブ解析のみのアクセス、ファイル解析のみのアクセスというように限定された機能のみ閲覧可能になる制限をつけることが可能です。

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（メールアドレス）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、ファイル解析の終了告知メール、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

gred セキュリティサービス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

gred セキュリティサービス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

gred 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。

- 電子メールでのお問い合わせ

電子メールアドレス：tech_support@securebrain.co.jp

※製品名、ご利用の OS 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. gred セキュリティサービス Web サイトの真正性について

gred セキュリティサービス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ウェブ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ウェブサイト (<http://www.securebrain.co.jp/products/client.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、**gred** セキュリティサービスにて導入している「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/server.html>

PhishWall クライアントの機能をさらにエンドユーザー向けに機能強化した Internet SagiWall もございます。

<http://www.securebrain.co.jp/products/sagiwall/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

gred セキュリティサービス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、解析開始 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

gred セキュリティサービスの契約期間が満了し、サービスの提供が終了した場合は、定期的なウェブ解析が停止し、ファイル解析の画面から解析対象のファイルを送れなくなります。

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

=====

gred セキュリティサービス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。

※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) で、?より前の部分が現在のページと同一の場合は除外されます。

(ただし、? がドメインの直下にある場合は例外で解析の対象となります。)

- <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。

ドメイン指定について

=====

- **gred** セキュリティサービスのクローラーは、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たどり先とします。

(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たどり先となります。

(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 はクローリング対象となります。

`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 はクローリング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.securebrain.co.jp/` や、`http://info.securebrain.co.jp/`、`http://www2.securebrain.co.jp/`等は、クローリング対象とはなりません。`http://hoge.www.securebrain.co.jp/`の場合にはクローリング対象となります。

PDF ファイルの扱い

=====

現状 (2010 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。

クローリング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、ウェブ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)も同様に解析を行います。

圧縮ファイルについて

=====

圧縮ファイル (zip, rar, 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

gred セキュリティサービスは、ウェブページをクロールすることですが、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、ウェブアクセスログにも残ります。ウェブサーバ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

gred セキュリティサービスでは、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、ウェブ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、gred セキュリティサービスでチェックし、発見が可能です。また弊社では、ウェブ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 PhishWalleX もご用意しています。

質問 3

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・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 gred セキュリティサービスは必要ですか？

回答

これらのツールで防御する範囲と gred セキュリティサービス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 gred セキュリティサービスです。

質問 4

ファイル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

gred セキュリティサービスは、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 4 回、ライセンスによって 8 回、24 回を選ぶことができます。
- ✓ ウェブ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

ウェブ解析は 1 日 4 回、1 社様あたり登録・チェックは 1 ドメインまで、最大 99 ページが解析対象となります。ファイル解析は、1 日当たり、1 ファイルとなります。1 日毎のキャリーオーバーはできません。これらの機能が 30 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 日のウェブ解析の回数（※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

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

ウェブ解析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 9

ウェブ解析は携帯対応していますか？

回答

現在のところ、対応しておりません。

質問 10

ファイル解析における解析結果の動作の OS のバージョンは何ですか？

回答

プログラムチェックの解析は、現在は Windows XP SP2 で行っています。

質問 11

ファイル解析はすべてのマルウェアを判定できますか？

回答

すべてではありません。exe ファイルと zip ファイルの中味を調査します。基本すべてが判定されますが、該当 OS での判定となりますので、該当以外の OS でマルウェアと判定された場合でも、該当の OS でマルウェアと判定されないことがあります。(現在の、判定基準の OS は XP_SP2)

質問 12

ウェブ解析では「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？

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 13

ファイル解析を依頼した結果の駆除ツールで全て駆除できますか？

回答

ご提供する駆除ツールは、プログラムを動的解析にて確認した挙動に基づくレジストリやファイルの改変を修正するものです。プログラムによっては様々なふるまいを見せるものがあるために、完全な駆除を行うことができない場合があります。また、駆除ツールに関してのサポートはご提供しておりません。

質問 14

認証を経た先に表示されるページを解析しますか？

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解析対象になっておりません。

質問 15

Flash で作成されたトップページからの解析はできますか？

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。

質問 16

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

gred セキュリティサービス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 17

クロスドメインスクリプトの検知と改ざん切替機能の関係

回答

昨今の Gumblar 等による改ざんは、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に改ざん切替機能を設定しており、クロスドメイン検知で切り替え機能を有効にしている場合、クロスドメインスクリプトを検知した時点でページ切替機能が発生します。予め、クロスドメインスクリプト機能の許可設定を行った上で、切替機能の設定を ON にしてください。(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)

質問 18

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

可能です。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。

