GRED Web改ざんチェック Cloud

Webサイトへのマルウェア
インジェクションに備える
早期警告システム

（ホワイトペーパー 2021年3月版）

SecureBrain

概要

最近では、ビジネスをする上でWebサイトを持たないことはもはや選択肢にありません。公式なオンラインプレゼンスがなければ、利益獲得機会の大きなシェアを失うリスクがあります。

しかし、Webサイトの管理を難しくする複雑な事情があります。サイバーセキュリティに関して言えば、ハッカーはオンラインプレゼンスを脅かす脅威となっています。最小限のノウハウしか持たないハッカーでも、マルウェアをWebサイトに仕込むことができるのです。マルウェアの存在は、企業とその顧客のプライバシーを危険に晒します。

このようなケースは、顧客の安全を脅かすだけでなく、企業のイメージを低下させる可能性もあります。調査によると、2019年にはすでに62%の消費者が、Webサイトや小売店と共有しているデータの安全について確信が持てなくなっています。企業側は、自社のブランドがこのように否定的なイメージで結び付けられることを望みません。結局のところ、企業のWebサイトはその企業の状況の反映なのです。Webサイトは、毎日の業務と同じようにスムーズに稼働する必要があります。

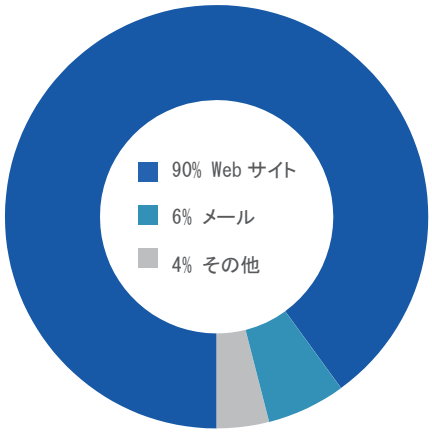
もしWebサイトが信頼されなければ、顧客はその企業もブランドとしても信頼しなくなります。

サイバー犯罪の最も一般的な形態の一つは、Webサイトにマルウェアをインジェクションする攻撃です。最新のGoogle透明性レポートによると、50,000以上のWebサイトがマルウェアの存在により安全ではないと見なされていますが、従来のWebサイトセキュリティ対策では、効果的に攻撃を防ぎ、悪意あるソフトウェアからWebサイトを保護することができません。

GRED Web改ざんチェック Cloudは、安心してWebサイトを運営するために必要なサービスです。このサービスは、Webサイトが攻撃を受けた場合にWeb管理者にアラートを発することができる早期警告ソリューションです。このクラウドベースのソリューションは、継続的にセキュリティチェックを実行して、Webサイトにマルウェアが侵入していないかどうかを常に確認することができます。

脅威とリスク:
一般的な Web サイトマルウェアインジェクション

マルウェアの伝播



「最近のマルウェアのほとんどは、改ざんされた Web サイトを介して拡散しています」

USA トゥデイ(2013)

Malwarebytesの最近の調査で、マルウェアインジェクションの対象が個人から組織や企業へとシフトしていることが明らかになりました。ここ数年、消費者からのマルウェアの報告数は2%減少しています。その結果、企業でのマルウェアの検知件数は10%以上増加しています。最近の傾向を踏まえると、一般的なWebサイトマルウェアインジェクションに精通しておくことが最も重要です。

マルウェアがWebサイトに侵入する方法はいくつかあります。ドライブバイダウンロード(DBD)はユーザの同意なしに悪意のあるプログラムをデバイスにダウンロードするマルウェア攻撃の一種です。この種のマルウェアは、デバイスをハイジャックして情報や活動を追跡できるだけでなく、デバイスを完全に無効にすることもできます。

特に企業にとってDBDが要注意なのは、DBDが正規のWebサイトに侵入するからです。ハッカーは、SQLインジェクション、CMSの脆弱性、HTMLコンテンツの改変などを通じて、Webサイトの管理者が知らないうちにWebサイトを介して消費者を攻撃することができます。

ハッカーはDBD以外にも、不正なJavaScript、Webサーバモジュール、Webサイト改ざんなどの手段を使用して、Webサイトに侵入できます。

現状：従来のWebサイトセキュリティ

マルウェアは、コンピュータが誕生して以来ずっと存在していました。実際、最初のマルウェアが発見されたのは、40年近く前の1982年です。したがって、Webサイトのセキュリティ確保も新しい概念ではありません。

従来のWeb管理者は、いくつかの手段を使用して、管理対象のWebページに悪意のあるソフトウェアが仕込まれないよう保護してきました。これらの手段は一般的な脅威に対しては有効ですが、より高度なマルウェアに立ち向かうには力不足です。最も一般的な従来のWebサイトセキュリティ対策として、次のようなものがあります。

Web アプリケーション ファイアウォール（WAF）

Webアプリケーションファイアウォール（WAF）は間違いなく、今日の市場で利用可能な最もポピュラーなWebサイトセキュリティ対策の1つです。この種のセキュリティメカニズムでは、HTTPトラフィックがサーバに到達する前にそれを解析することで、脅威をフィルタリングします。

WAFを効果的に利用するには、時間と労力がかかります。このセキュリティ対策を機能させるには、特定のフィルタを設置する必要があります。WebサイトにWAFを設定する作業は非常に面倒です。さらに、WAFの検知システムは限定的で複雑なので、ハッカーはWAFを簡単にバイパスしてしまいます。

Web コンテンツ完全性チェック

Webコンテンツ完全性チェックはファイル完全性監視とも呼ばれ、最近のアップロード、編集、削除を検知してWebサイトを監視します。このセキュリティ対策は、Webサイトのファイルのログを取得し、サイトの現在のバージョンと比較することで機能します。この手法は、Webサイトの改ざんの脅威を発見するのに有効です。

現在のほとんどのWebサイトには、動的コンテンツがあふれています。残念ながら、Webコンテンツ完全性チェックは静的なHTMLページに対してしか機能しません。

脆弱性診断

従来のWeb管理者は、侵入チェックと脆弱性チェックを使用して、管理対象のWebページに脆弱性を持たせないようにしてきました。このセキュリティ対策は効果的ではありますが、最も経済的というわけではありません。コストが高いため、企業は推奨される期間内にこれらのチェックを終わらせることができません。こうした不備があるため、Webサイトはマルウェア攻撃に対して脆弱性を残したままになってしまいます。

SOC アウトソーシング

Webサイトのセキュリティオペレーションセンター（SOC）のアウトソーシングは、その効果を確実にするための方法です。このサービスを提供する第三者企業は、結局のところ、この分野のエキスパートです。SOCをアウトソーシングすることで、専門的な知識はもちろんのこと、Webサイトを運営する側の負担を軽減することができます。これにより、最小限の労力でセキュリティを保証することができます。

ただし、SOCアウトソーシングには多額の費用がかかります。特に小規模な企業にとって、セキュリティ対策のアウトソーシングをすることは最も費用対効果の高い解決策とは言えないかもしれません。

Webサイトのセキュリティを確保する手段として従来の対策を使用することに、何も問題はありません。ただし、Webサイトの完全性を本当に守るためには、従来の対策だけでは不十分です。攻撃を受けた場合に情報を得て、侵入の影響を最小限に抑えるには、早期警告システムを備えておくことが重要です。

防衛の強化:
GRED Web 改ざんチェック Cloud

従来のWebサイトセキュリティ診断の欠点は、検知から対処までの間のダウンタイムにあります。これらの保護対策の定期的な実施には欠陥があるため、マルウェアがWebサイト上に長期間にわたって存在し、対処されるまでに時間がかかることがあります。その時点で、すでに攻撃によって、当該企業のオンラインプレゼンスと検索エンジンのステータスや、そのWebサイトを閲覧した人のPCに損害が生じている可能性があります。

企業がその業務と顧客の機密情報を守るためには、継続的な検査を実施し、早期にマルウェア警告を表示するアプリケーションが必要です。

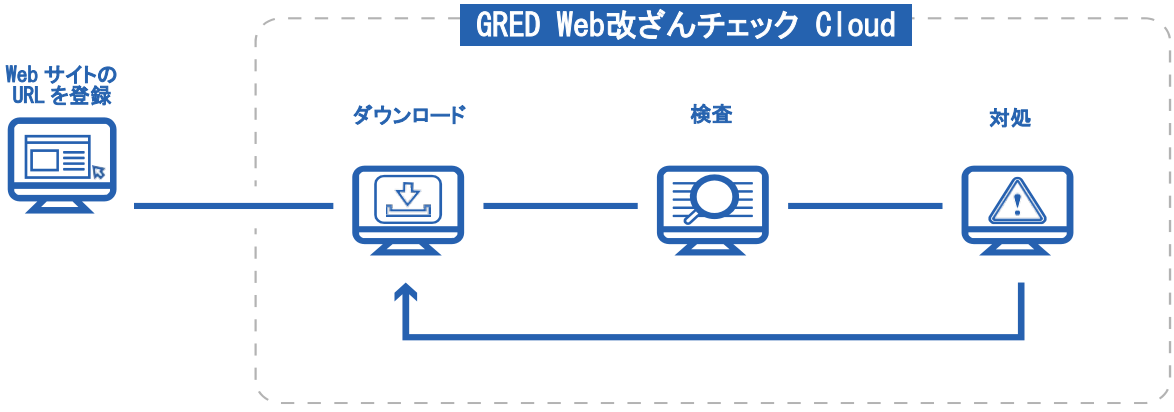
GRED Web 改ざんチェック Cloud とは

セキュアブレインのGRED Web改ざんチェック Cloudは、Webサイトへのマルウェアインジェクションに特化して設計されており、企業の業務品質を向上させることができる有用なツールです。Webサイトを年中無休で1日24時間週7日監視するために作られた早期警告システムです。

GRED Web改ざんチェック Cloudが提供するサービスは、完全にクラウド化されており、Webサイトへのインストールが不要で、ハードウェアの購入もソフトウェアのダウンロードも必要ありません。

シンプルで、効果的で、まさに企業にとって必要なソリューションです。

GRED Web改ざんチェック Cloudのしくみ



GRED Web改ざんチェック Cloudの特長は、完全に自動化されていて1日24時間週7日稼働していることです。
Web管理者であれば誰でも、GRED Web改ざんチェック Cloudを簡単に操作できます。

管理者は最初に、自社のWebサイトのURLを**GRED Web改ざんチェック Cloud**に登録する必要があります。登録が終わると、Webサイト全体の解析を実施します。この解析は、「ダウンロード」、「検査」、「Webポータル」の3つのパートに分けて行われます。

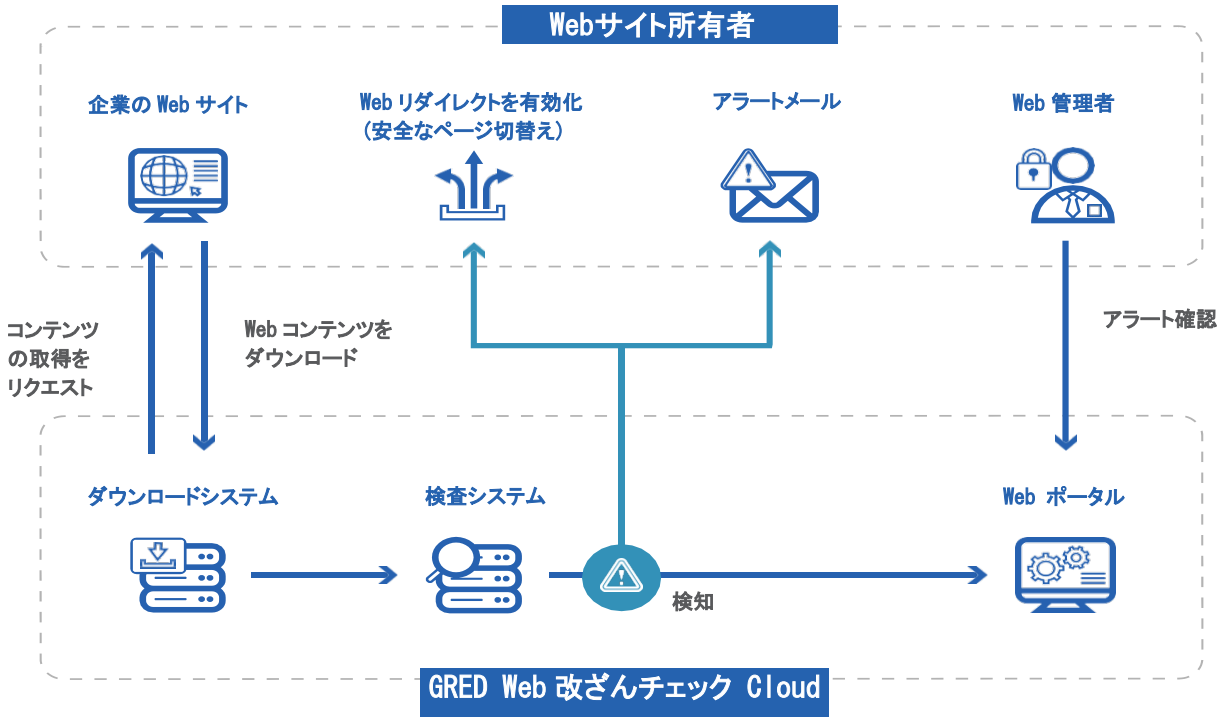
ダウンロード段階では、**GRED Web改ざんチェック Cloud**がWebサイト全体を解析します。ハイパーリンクを使用してすべてのページをナビゲートし、マルウェアの検査が必要な情報をダウンロードします。

すべてのページを取得し終わると、検査段階に入ります。静的解析を使用して、**GRED Web改ざんチェック Cloud**はすべてのページをチェックし、悪意のあるソフトウェアを探します。アプリケーションがマルウェアを検知すると、管理者にアラートメールを送信し、管理者はWebポータルで詳細を確認する事ができます。その後の検知したページを安全なページにリダイレクトしWebサイトの訪問者を保護します。

もっと深く理解する:
GRED Web 改ざんチェック Cloud の詳細

GRED Web改ざんチェック Cloudは、管理者や企業のオーナーが簡単にWebサイトを管理・監視できる有用なツールです。この製品の特長は、Webサイトをマルウェアや他の悪意あるソフトウェアから保護するシステムにあります。

ここで、企業の運営にとって本製品がいかに重要かを理解するために、**GRED Web改ざんチェック Cloud**を必要不可欠なものにしている3つのシステムについて、詳しく見ていきましょう。



ダウンロードシステム

WebサイトをGRED Web改ざんチェック Cloudデータベースに登録した後、アプリケーションはダウンロードシステムに進みます。

この段階で、GRED Web改ざんチェック Cloudは閲覧者と同じ方法でサイトをスキャンします。次に、サーバ側のスクリプト処理やデータベースの検索から生成された動的情報を含む、入手可能なすべてのWebコンテンツをダウンロードします。この段階では、アプリケーションがHTMLページ、URLリンク、そして最も重要なのは、Webサイトの閲覧者にマルウェアを感染させる可能性のあるEXEやZIPリンクのチェックも実施します。

ダウンロードは、すべてのWebコンテンツが常にカバーされていることを確認するために継続的に行われます。次に、GRED Web改ざんチェック Cloudは検査に進みます。

検査システム

検査システムは、ダウンロードシステムで収集されたデータをふるいにかけ、ウェブサイト内に潜むハッカーが仕込んだ悪意のあるソフトウェアを見つけ出します。

この段階では、GRED Web改ざんチェック Cloudは、サイトを破壊する可能性のあるスクリプトを起動してトリガーとします。その際に、大規模なホワイトリストデータベースを使用して、既知の安全なスクリプトと、信頼できない未知のスクリプトを区別します。このデータベースにより、GRED Web改ざんチェック Cloudでは、スクリプトが損害を与える前にスクリプトを特定することができます。

静的解析と動的解析

GRED Web改ざんチェック Cloudは、静的解析による検査を実施します。このアプリケーションでは、いくつかの理由からこの種の検査を選択しています。

従来、マルウェア検知には、静的解析と動的解析の2つの方法があります。どちらも広く使用されていて、それぞれ長所と短所があります。

動的解析では、マルウェアを実行してその動作を観察し、その目的や、マルウェアが引き起こす被害の深刻度、攻撃を回避するために講ずべき措置を判断します。この種の解析は、幅広いマルウェアを検知できますが、非常に時間がかかることでも知られています。

一方、静的解析は、マルウェアを特定するためにスクリプトを実行する必要がありません。その代わりに、各マルウェアのバイナリコードに特有のシグネチャを見つけます。静的解析は、ほとんどのWebサイトに埋め込まれる一般的なマルウェアを、動的解析よりはるかに迅速に検知します。これは、悪意のあるソフトウェアの検知と検査において、より効率的な手段であると言えます。

検査システムの対象リスト

GRED Web改ざんチェック Cloudでは、静的解析を使用してWebサイト上に存在するさまざまなマルウェアを検知します。そのためにシグネチャベースの検査を実行するため、GRED Web改ざんチェック Cloudが得意とするのは、一般的な種類のマルウェアの検知です。これに当てはまる脅威やシナリオには次のものが含まれますが、それだけに限定されるわけではありません。

- DBDダウンロードトリガJavaScriptおよびiframe
- 不正なJavaScript
- 信頼できないドメインからのスクリプト実行
- 疑わしいEXEファイル/ZIPファイル
- Webサイトコンテンツの改ざん
- フィッシング
- ボーガスウェア
- Google検索エンジンのブラックリスト
- 行政機関発行のブラックリスト
- セキュリティ団体発行のブラックリスト

Webポータル

検査システムがWebサイト上のマルウェアを検知すると、Webポータルが特定された脅威への対応を実行します。Webポータルによる処理は二段構えになっています。まず、脅威の詳細を示すレポートを作成するために十分なデータを収集します。攻撃の詳細と、被害を受けたWebサイトに注入された特定のスクリプトについて説明します。

Webポータル上のレポートとは別に、管理者に現在の状況を知らせるメールが送信されます。

Webポータルシステムは、**GRED Web改ざんチェック Cloud**の不可欠な要素です。これにより、Webサイトの所有者は、脅威が検知されてから数分以内に脅威に対処することができます。このアプリケーションは、Webサイトとその閲覧者に対するマルウェアの影響を最小限に抑えます。

ページ切り替え機能

Webサイトを適切に保守せず危険な状態を放置していると、瞬時に見込み客を失うことになります。従来のマルウェア検知の方法では、Webサイトの閲覧者がマルウェアの存在を管理者に報告するまで、悪意のあるソフトウェアが放置されます。この状態は企業の評判を傷つけるだけでなく、見込み客と彼らのデータを深刻なセキュリティリスクにさらすことになります。

GRED Web改ざんチェック Cloudの機能の1つに、改ざん時のページ切り替え機能があります。検査システムがWebサイト上のマルウェアを検知した場合、アプリケーションは自動的に閲覧者を安全なWebページにリダイレクトします。したがって、管理者がすぐに問題解決に着手できない場合でも、それ以上マルウェアの被害者が増えることはありません。

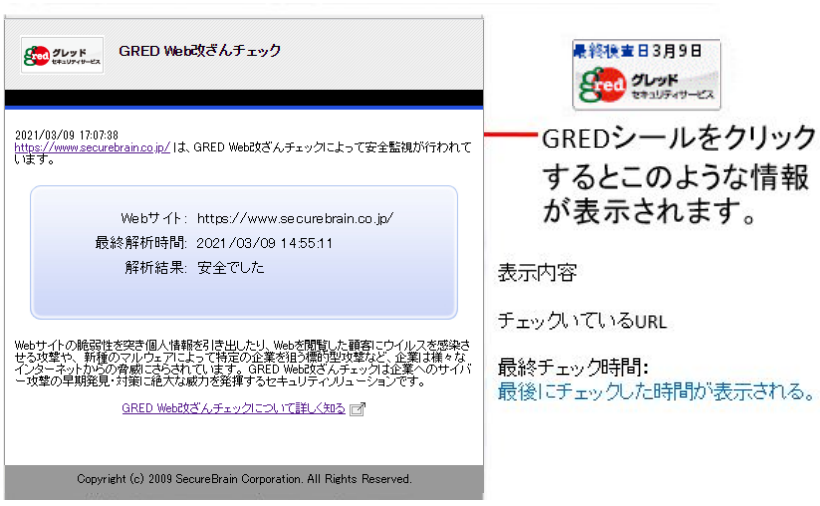
このページ切り替え機能は、Webサイト管理者がWebサイトにスクリプトタグを挿入するだけで利用できます。Webポータルからページ切り替えを有効にしたり無効にしたりすることができます。

シール機能

GRED証明書

GRED Web改ざんチェック Cloudは、自社のWebサイトにGRED証明書シールを表示することもできます。このシールは、そのWebサイトが適切に保守されていてマルウェアが存在せず安全であることを、閲覧者に保証します。

閲覧者はこのシールをクリックできます。すると、そのWebページのセキュリティレーティングだけでなく、最新の検査の日付も表示されます。**GRED Web改ざんチェック Cloud**は、オンラインでの評判を上げたい企業にとって必須のソリューションです。



GRED Web 改ざんチェック Cloud その他の機能

GRED Web改ざんチェック Cloudのコア機能の他にも、高度なマルウェアに対してWebサイトの守りを固めるための機能がいくつか用意されています。

クロスドメインスクリプト検知

GRED Web改ざんチェック Cloudは、許可していない外部スクリプトを検知します。この種の攻撃は、閲覧者を標的にして実際のWebページを悪意のあるスクリプトを実行するための道具にするため、特に注意する必要があります。

改ざん検知

Webサイトの改ざんは、ハッカーが所有者の知らないところでWebサイトのコンテンツを変更、削除、追加することで発生します。この種の脅威は、ブランドの評判を傷つけるだけでなく、そのWebサイトが危険であることを世間に知らせてしまいます。

GRED Web改ざんチェック Cloudは、Webサイトのトップページのコンテンツが著しく変化した場合にその攻撃を検知し、管理者に通知します。

特定タグの属性変化の監視

GRED Web改ざんチェック Cloudではビジュアルコンテンツ以外でも、WebサイトのJavaScriptコードの変化と、HTMLコンテンツ内のドメインリンクの変化も監視する機能を備えています。これには、アンカータグなどのタグの編集も含まれます。

簡易脆弱性診断

GRED Web改ざんチェック Cloudは、Webサイトの脆弱性診断を効率化できます。このアプリケーションは、WordPress脆弱性診断、ポートスキャン診断、そしてJoomla診断を実行できます。

ヘルスチェック検知

Webサイトが頻繁にダウンすると、ビジネスチャンスを逃す可能性があります。**GRED Web改ざんチェック Cloud**はスキャンを実行し、登録されているすべてのページの可用性を確認できます。

リンク切れ検知

Webサイト内にリンク切れがないようにすることは、検索エンジンのランキングを維持する上で重要なことです。Googleなどの検索エンジンは、存在しないリンクを含むページにペナルティを課します。**GRED Web改ざんチェック Cloud**は、リンク切れを検知するだけでなく、置換や編集が必要なリンクをレポートします。

実行ファイルのチェック

たとえば、Windowsの実行可能ファイル(.exeファイル)は、マルウェアを配信する手段としてよく利用されます。**GRED Web改ざんチェック Cloud**では、これらのファイルをチェックして、悪意のあるソフトウェアの有無を調べます。

GRED Web改ざんチェック:
販売と価格

GRED Web改ざんチェック Cloudは、日本発のセキュリティベンダーであるセキュアブレインが販売しています。価格設定は、検査の頻度や検査・保守の対象となるWebページの数によって異なります。

中小企業から多国籍企業まで、あらゆる規模の企業の予算とニーズに合わせたパッケージがあります。

現在、ボリュームディスカウントとOEMが可能です。OEMパートナーは、GRED Web改ざんチェック CloudのWebポータルをヘッダーとフッターに自社のロゴを付けてリブランディングすることができます。2021年の時点で、30社以上の企業が**GRED Web改ざんチェック Cloud**のOEMを選択しています。

GRED Web改ざんチェック Cloudの機能の詳細と、2週間のトライアルについては、
https://www.securebrain.co.jp/products/gred/index.html をご覧ください。

企業を守る GRED Web 改ざんチェック Cloud

ハッカーがWebサイトに侵入する方法はさまざまです。コンテンツの改ざんから情報の窃取まで、Webサイトを無防備に放置した結果は重大かつ深刻です。顧客を獲得することになるか、失うことになるか、その違いをもたらす問題です。GRED Web改ざんチェック Cloudのような早期警告検知システムの導入は、企業にとって価値のある投資です。

自社のイメージを守る

企業のWebサイトは、その企業の状況を反映します。Webサイトはオンラインでの企業の名刺のようなものです。したがって、マルウェアが仕込まれたWebサイトは、その企業が信頼できないと世間に知らせていることになります。

それに対して、**GRED Web改ざんチェック Cloud**はWebサイトを訪れるすべての閲覧者をさまざまな一般的マルウェアから保護します。シール機能は、閲覧者がWebサイトをクリックするたびにシステムが保護されているという安心感を提供しています。企業にとって、評判ほど重要なものはありません。**GRED Web改ざんチェック Cloud**は、企業が築き上げた評判を守ります。

高価な修復を回避

マルウェアがWebサイト内に潜む時間が長くなればなるほど、Webサイトの所有者と閲覧者が被る損害が大きくなることは、コンピュータの専門家でなくても分かります。

早期発見が大切であることは言うまでもありません。**GRED Web改ざんチェック Cloud**のようなプログラムは、損害を最小限に抑えます。さらに、ページ切り替え機能によって、それ以降のマルウェア感染を防ぎ、問題を封じ込めます。

このセキュリティサービスを利用すれば、Webサイトの修復に高額な費用を注ぎ込む必要がなくなります。

顧客基盤を拡大

GRED Web改ざんチェック Cloudを活用して信頼できるWebサイトを実現すれば、マルウェアの感染や拡散のリスクなしで顧客基盤を拡大できます。GRED Web改ざんチェック Cloudは、より多くのチャンスと契約獲得へと続く道を提供します。

付録:
Web ポータルのスクリーンショット

アラートメールを受信

Web ポータルで詳細を確認

注入されたコードを表示

Web ポータルのログイン画面

カレンダーを見るとチェックの結果がひと目で分かります。赤い日付はアラートを示しています。

注入されたスクリプトを自動的に特定

セキュアブレインについて

約20年に及ぶ経験を積み重ねてきたセキュアブレインは、日本の大手セキュリティソフトウェアプロバイダとして認知されるようになりました。
東京に本拠を置く当社は、国内外を問わずあらゆる種類の企業に多様なセキュリティ対策の選択肢を提供することを目指しています。

セキュアブレインは、Webサイトのマルウェア検知と保護において最先端の技術を提供するために、独自の研究センターを運営しています。
当社の研究者チームは、オンラインWebサイトの新たなセキュリティリスクの特定と、現在と将来の脅威に対するソリューションの開発に専念しています。

株式会社セキュアブレイン
〒102-0094　東京都千代田区紀尾井町3-12 紀尾井町ビル7F
電話:03-3234-3001、FAX:03-3234-3002
e-mail:　sales@securebrain.co.jp
https://www.securebrain.co.jp/

SecureBrain

https://www.securebrain.co.jp/