PRESS RELEASE

2012 年 1 月 30 日

報道関係各位

株式会社セキュアブレイン

セキュアブレイン gred セキュリティレポート Vol.30【2011 年 12 月分統計】

－ 標的型（APT）攻撃の原理と対策 －

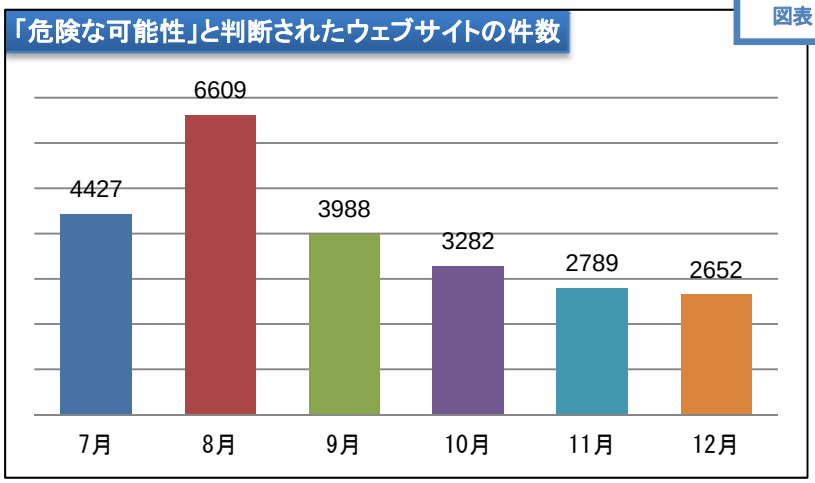
株式会社セキュアブレイン(本社：東京都千代田区、代表取締役社長 兼 CEO：成田 明彦、以下「セキュアブレイン」)はセキュアブレインが運用する、無料のウェブセキュリティサービス「gred（グレッド）でチェック」で収集した情報を基に、「セキュアブレイン先端技術研究所」（以下 先端技術研究所）で分析を行い、その結果を「セキュアブレイン gred セキュリティレポート」として公表します。「gred でチェック」は、インターネットユーザがウェブサイトの安全確認を行うことができる、無料のウェブセキュリティサービスです。確認したいウェブサイトの URL を入力するだけで、セキュアブレインが独自に開発した解析エンジンが、ブラックリストを使用せず短時間で解析し、そのウェブサイトの安全性を判定します。

内容

1　gred セキュリティレポート概要

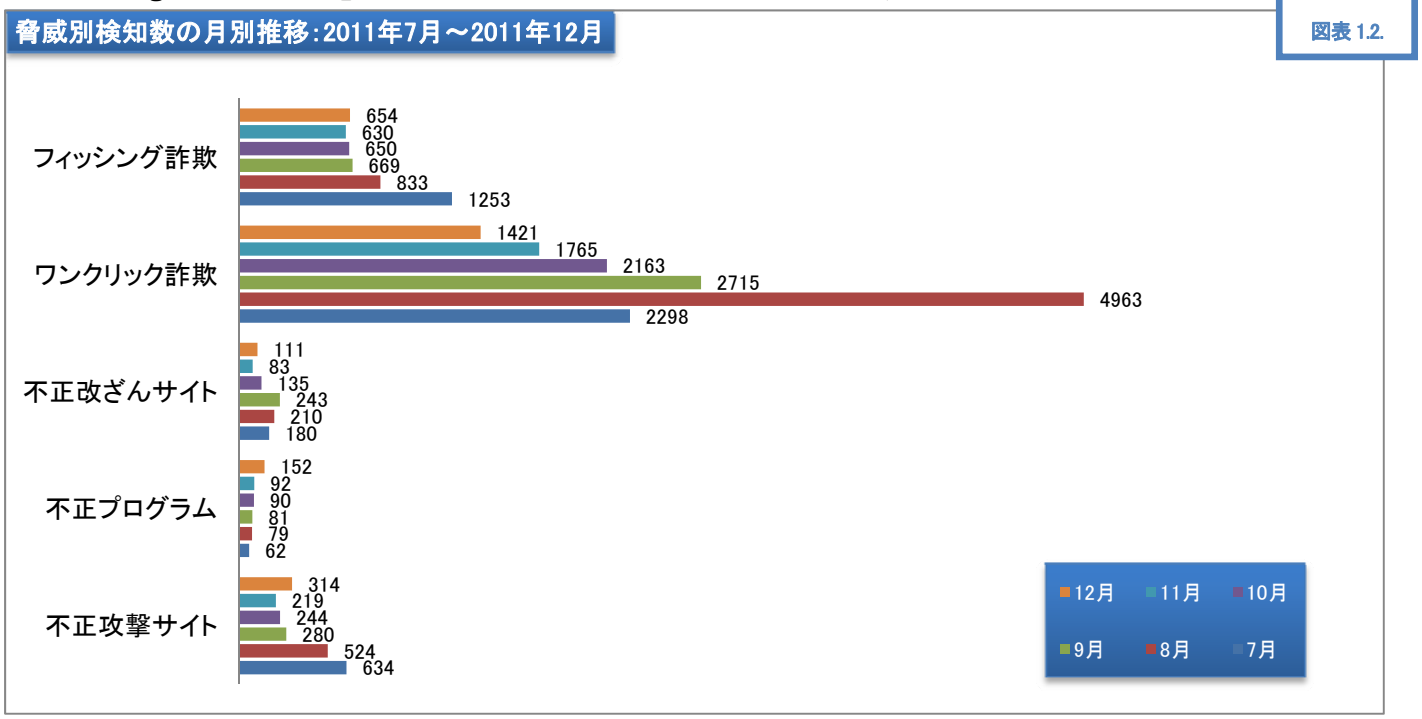
1.1　「危険な可能性のあるウェブサイト」と判断されたウェブサイトの数（図表 1.1.）

図表 1.1



1.2　「gred でチェック」で検知した脅威の月別推移（脅威別）（図表 1.2.）

図表 1.2.



1.3　「gred でチェック」月別総利用数（図表 1.3.）

図表 1.3.

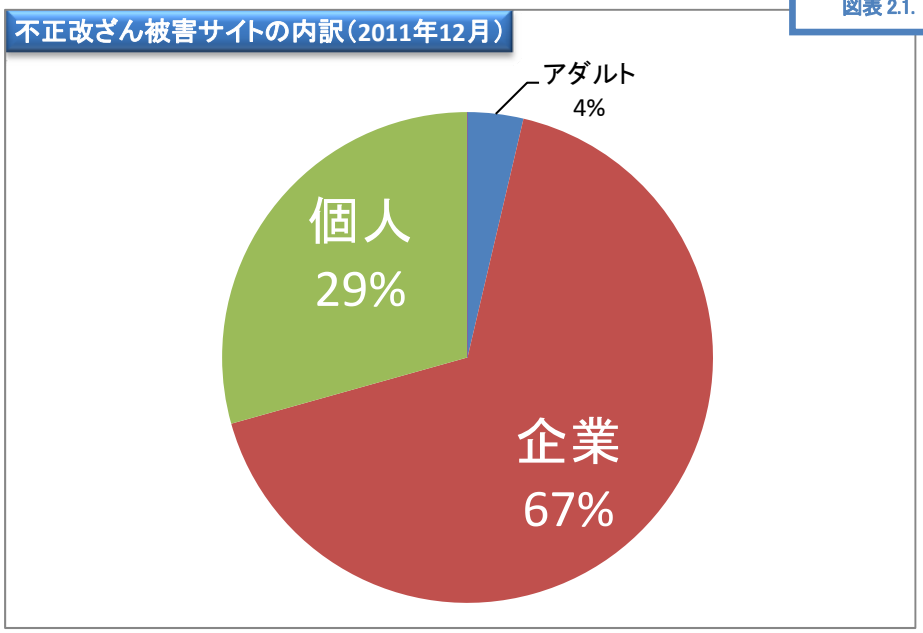
月	7 月	8 月	9 月	10 月	11 月	12 月
「gred でチェック」総利用数	38,006	44,272	41,269	41,897	39,618	38,938

「gred でチェック」のチェック結果に表示される脅威の説明

表示される脅威の名称	説明
フィッシング詐欺	本物そっくりに、偽造されたウェブサイトです。ユーザの ID や、パスワード等の個人情報を不正に取得します。
ワンクリック詐欺	ウェブサイト上のボタン等をクリックしただけで、契約が成立したように見せかけ、料金を不当に請求する詐欺を行っているウェブサイトです。
偽ソフトウェア（不正プログラム）	不当に料金を請求する、実際には機能しない、偽物のソフトウェアを配布しているウェブサイトです。
不正攻撃サイト	他のコンピュータに存在する脆弱性を突いて、攻撃を行うことを目的として作成されたウェブサイトです。
不正改ざんサイト	攻撃者によって、不正に改ざんされてしまった状態になっているウェブサイトです。
ウイルス（不正プログラム）	ウイルスが仕掛けられているウェブサイトです。閲覧すると感染被害の恐れがあります。
ワーム（不正プログラム）	電子メールやネットワークを利用し自己増殖する、ワームが仕掛けられているウェブサイトです。閲覧すると感染被害の恐れがあります。
スパイウェア（不正プログラム）	個人情報等をコンピュータから盗む、スパイウェアが仕掛けられているウェブサイトです。閲覧すると感染被害の恐れがあります。
その他のマルウェア（不正プログラム）	ウイルス、ワーム、スパイウェア以外の不正プログラムが仕掛けられているウェブサイトです。閲覧すると感染被害の恐れがあります。

2　数値で見る「不正改ざんサイト」の内訳（図表 2.1.、2.2.）

図表 2.1.



図表 2.2.

	2011 年 7 月	2011 年 8 月	2011 年 9 月	2011 年 10 月	2011 年 11 月	2011 年 12 月
「危険な可能性がある」と判断されたウェブサイトに占める「Drive by Download タイプの攻撃」の割合	2.2% （98 件/4,427 件）	0.7% （48 件/6,609 件）	1.9% （77 件/3,988 件）	1.7% （55 件/3,282 件）	0.9% （24 件/2,789 件）	1.3% （35 件/2,652 件）
「不正改ざんサイト」の検知件数に占める「Drive by Download タイプの攻撃」の割合	54.4% （98 件/180 件）	22.8% （48 件/210 件）	31.7% （77 件/243 件）	40.7% （55 件/135 件）	28.9% （24 件/83 件）	31.5% （35 件/111 件）

3　標的型（APT）攻撃の原理と対策　～解説者：　先端技術研究所　神薗　雅紀～

近年、標的型（APT）攻撃（以下　標的型攻撃）が猛威を振っています。特に防衛産業に関わる企業や官公庁が標的とされていますが、個人にとっても身近な脅威となってきました。ここでは標的型攻撃の原理と対策についてご紹介したいとおもいます。インシデントの内容を把握することはセキュリティ対策では重要です。攻撃の原理を理解した上で、効果的な対策を実施して頂けたら幸いです。

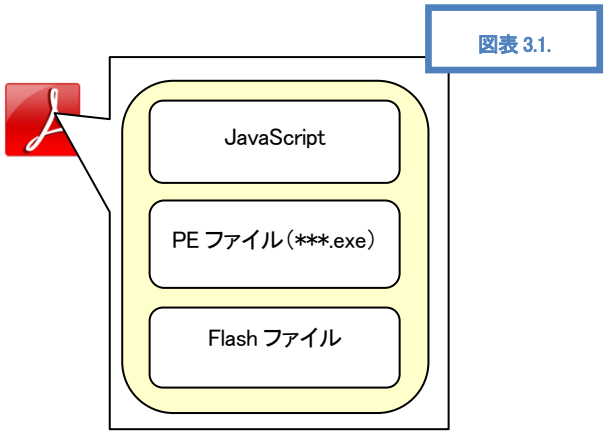
3.1　標的型攻撃の種類

標的型攻撃とは、サイバー攻撃の一種で、特定のターゲット（標的）に対して継続的な攻撃、または潜伏活動を行い、ソーシャルエンジニアリング等の様々な手法を駆使して情報搾取行為や妨害行為等を行う攻撃の総称です。標的型攻撃は多くの手法が確認されていますが、主にメールにマルウェアを添付し、ユーザに開かせることが第一ステップとなります。そして、添付されるマルウェアも様々なタイプが存在しますが、代表的なものにPDFタイプのマルウェアがあります。先に述べた防衛産業におきましても、内部の人間から送付されたように偽装したメールに PDF タイプのマルウェアが添付されていました。

3.2　標的型攻撃の原理と構造

ここでは標的型攻撃に利用されているPDFタイプのマルウェアの原理を紹介します。今回紹介する内容は、全てのマルウェアが当てはまるわけではありませんが、一般的に以下のような構造となっています。

- PDF タイプのマルウェアの構造
  - ✓　難読化された JavaScript
  - ✓　不正な PE ファイル（ファイルをダウンロードするダウンローダやボット）
  - ✓　不正な Flash ファイル　など



- 暗号化された Java Script が行っている処理

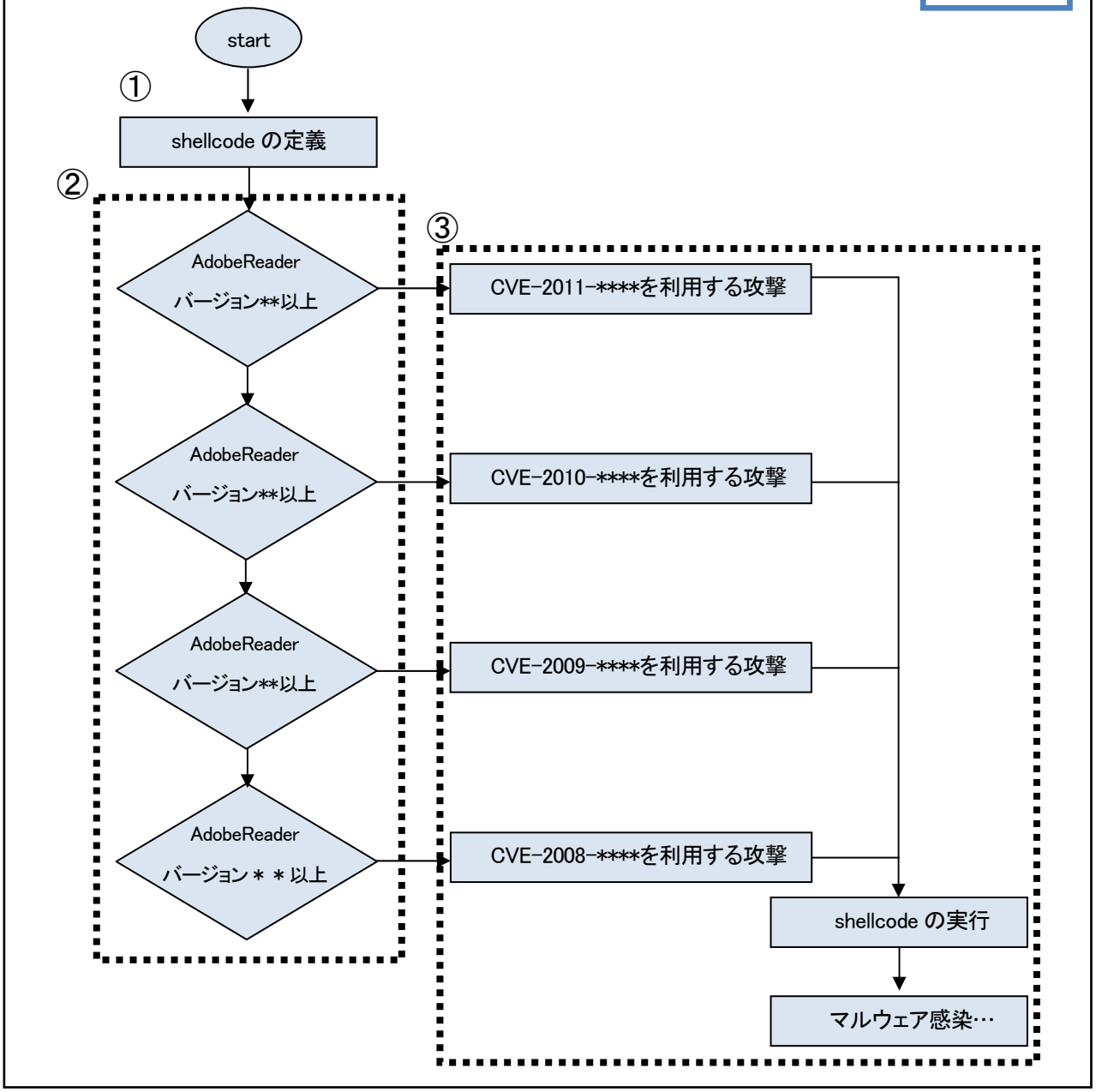
PDF タイプのマルウェアに含まれる JavaScript の難読化を解除すると、多くは以下のような構造となっています。代表的な JavaScript のフローと共にご説明いたします。

① 最初に、コンピュータの制御を奪うための shellcode を定義します。この shellcode は、具体的には PDF 内に組み込まれた PE ファイル（ボット）の実行や、バックドアなどを仕掛ける処理などが仕組まれています。

② 続いてユーザが利用している Adobe Reader のバージョンをチェックします。これは、「③Adobe Reader のバージョンに沿った攻撃」を行うための事前調査となります。より多くのユーザに、そして感染の確率を高めるために実施されていると想定されます。

③ 最後に Adobe Reader のバージョンに沿った攻撃を実施します。①の処理で定義された、コンピュータの制御を奪うための shellcode が実行され、マルウェアに感染するという流れとなります。

図表 3.2.



③における攻撃部分は、非常に多くの手法が存在します。主に「JavaScript for Acrobat API に定義されている脆弱性のある API を利用する攻撃」や「heap spray 攻撃」、そして「PDF 内に組み込まれた脆弱性が存在する Flash ファイルを実行する攻撃」等が挙げられます。最近の PDF マルウェアは、一つのマルウェアの中に 4 つから 5 つの脆弱性を利用するものが多くみられ、主に 2004 年～2011 年の間に報告された脆弱性が頻繁に検出されています。

3.3 ちょっとした作業で効果的な対策を！！

「2. 標的型攻撃の原理と構造」でご説明したとおり、標的型攻撃の攻撃内容の中心は JavaScript です。つまり JavaScript が機能しなければ感染しないことが理解できます。

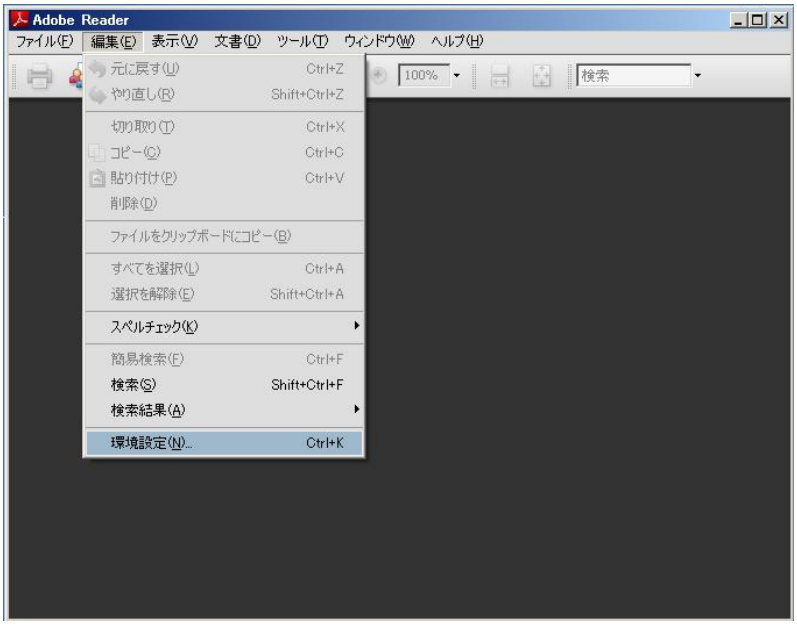
しかし、以下の点に関する疑問が発生します。

- *フォントの脆弱性や Flash の脆弱性を利用された場合は、JavaScript は使われないのではないか？*

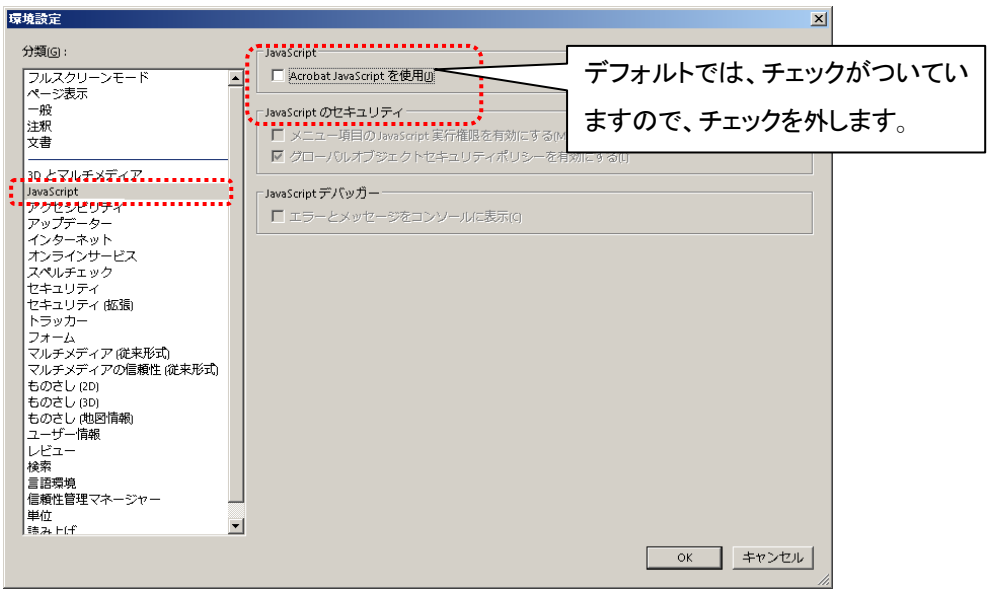
確かに、かつては JavaScript を使用せず脆弱性を利用するものも報告されていました。しかし最近の脆弱性は、基本的には

JavaScript と連携しています。また、フォントの脆弱性を利用するマルウェアも、その脆弱性を突くためにフォントを定義する必要がありますが、多くのマルウェアはフォントの定義処理に JavaScript を使っています。また、Flash の脆弱性を悪用した攻撃でも、JavaScript が事前に設定した制御（shellcode などと呼ばれる）を実行するトリガのみである場合が多くみられます。つまり、Adobe Reader の JavaScript 機能を OFF にすることで、端末の制御までは奪われず、マルウェアの感染までは実施されないため、標的型攻撃の抑止に効果的であると言えます。

- Adobe Reader の JavaScript 機能を OFF にする方法を以下に示します。



Adobe Reader「編集」→「環境設定」



「環境設定」画面の分類「JavaScript」を選択→Acrobat JavaScript を使用のチェックを外す

また、マルウェアの多くは過去に報告された複数の脆弱性を利用して端末に感染を試みます。OS と同様、アプリケーションもパッチやアップデートが非常に重要です。

4　セキュアブレインがご提供するセキュリティソリューションのご紹介

4.1　個人向けの対策

ブラウザ専用の詐欺対策ソフト「Internet SagiWall 」（インターネット・サギウォール）

従来のセキュリティ対策ソフトでは検知することのできない「危険なウェブサイトをブロックします。

［ブロックする悪質サイト］

- フィッシング詐欺サイト
- ワンクリック・ツークリック詐欺サイト
- ウイルス等不正プログラム配布サイト
- Gumblar などによって改ざんされたウェブサイト
- 偽ソフトウェア配布サイト

［機能詳細ページ］

http://www.securebrain.co.jp/sagiwall/index.html

【ご購入はこちら】セキュアブレインショップ

http://www.securebrain.co.jp/shop/index.html

※本製品は、BB ソフトサービス株式会社の製品です。

※Android 端末に対応した、「Internet SagiWall for Android」が「ソフトバンクモバイル」および「Android Market」より提供されています。

ソフトバンクモバイルのページ：http://mb.softbank.jp/mb/service/sagiwall/

Android Market のページ：https://market.android.com/details?id=jp.co.bbss.android.security.sagiwall_softbank

閲覧しようとしているウェブサイトの安全性を無料でチェック

セキュアブレインでは、閲覧しようとしているウェブサイトの安全性を、ブラックリストを使わずに判断する、セキュリティサービス「gred でチェック」（http://www.gred.jp）を無料で提供しています。

安い、軽い、安全、最新型ウイルス対策ソフト「gred アンチウイルス アクセラレータ Plus」

米国の研究機関による、ウイルス検知テストで『100%』の実力

全世界で 200 万人が使用！

軽さと高い安全性を実現した最新型ウイルス対策です。

［ gred アンチウイルス アクセラレータ Plus の機能］

- 圧縮ファイルのスキャン
- パッカーにより難読化されたファイルのスキャン
- CD、DVD、USB メモリ経由の脅威をブロック
- 電子メールスキャン
- ルートキットの検知と削除
- レジストリとファイルシステムの修復

［機能詳細ページ］

http://www.gredavx.jp/plus/index.html

【ご購入はこちら】セキュアブレインショップ

http://www.securebrain.co.jp/shop/index.html

4.2　企業向けの対策

月々9,000 円からご利用いただけるウェブサイト監視サービス「gred セキュリティサービス」

企業のウェブサイトの管理者は、自社のウェブサイトの安全性を、自動で定期的に監視するソリューションが必要です。セキュアブレインでは、企業のウェブサイトが不正に改ざんされていないかを定期的に監視し、問題が発見された場合には、即座に管理者に通知する、SaaS 型セキュリティサービス「gred セキュリティサービス」をご提供しています。

■「gred セキュリティサービス」無償トライアルお申込み URL

http://www.securebrain.co.jp/products/gred/trial.html

■「gred セキュリティサービス」の機能詳細説明 URL

http://www.securebrain.co.jp/products/gred/function.html

以上

セキュアブレインについて:

株式会社セキュアブレインは、インターネット上の脅威が多様化する中、「より快適で安心できるネットワーク社会を実現するために、一歩進んだ技術で貢献する」というビジョンのもと、信頼性の高いセキュリティ情報と高品質なセキュリティ製品・サービスを提供する日本発のセキュリティの専門企業です。詳細は、www.securebrain.co.jp をご覧ください。

◆ 本件に関する報道関係者さまからのお問い合わせ先 ◆

株式会社セキュアブレイン　広報担当:丸山　芳生(まるやま　よしお)

e-mail:info@securebrain.co.jp

電話:03-3234-3001、FAX:03-3234-3002　〒102-0083 東京都千代田区麹町 2-6-7 麹町 RK ビル 4F