Press Release

2010 年 9 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.14【2010 年 8 月分統計】

オンライン広告配信サービス利用者における改ざん被害が拡大、「ワンクリック不正請求」サイトは多言語化の兆し

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、そのウェブサイトが「安全(Safe)」か「危険(Danger)」を判断します。

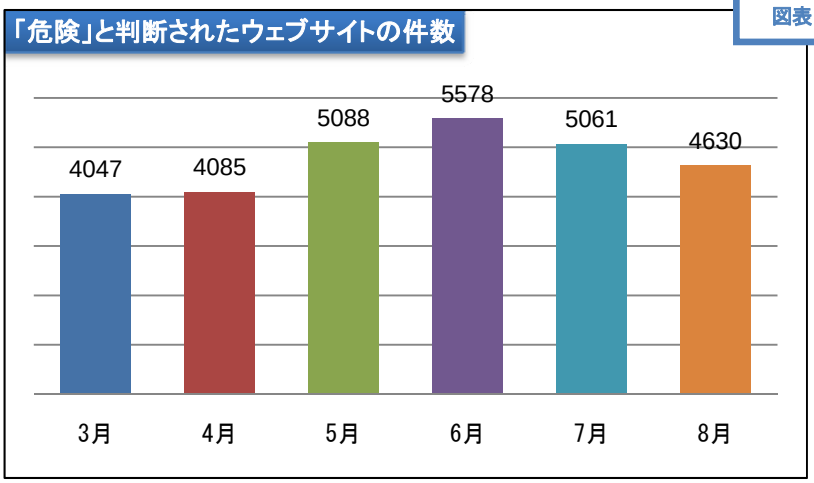
内容

1 gred セキュリティレポート概要 2
1.1 「危険」と判断されたウェブサイトの数(2010 年 8 月):4,630 件(図表 1.1.) 2
1.2 「gred でチェック」で検知した脅威の月毎の推移(脅威別)(図表 1.2.)(単位:件) 2
1.3 「gred でチェック」月別総利用数(2010/3 月～2010/8 月)(図表 1.3.) 2
1.4 「gred でチェック」のチェック結果に表示される脅威の説明 3
2 数値で見る「不正改ざんサイト」の内訳(図表 2.1., 2.2.) 3
3 オンライン広告配信サービス利用者における改ざん被害が拡大 4
3.1 サービス提供会社のサーバへ行われた攻撃の概要 4
3.2 ウェブサイトを運営している企業は継続的な安全確認を 5
4 多言語化される「ワンクリック不正請求」サイト 6
5 個人・企業それぞれに求められる、セキュリティ対策とは? 7
5.1 個人向けの対策:「gred でチェック」「Internet SagiWall(インターネット・サギウォール)」「gred AntiVirus アクセラレータ」 7
5.2 企業向けの対策:「gred セキュリティサービス」 7

1　gred セキュリティレポート概要

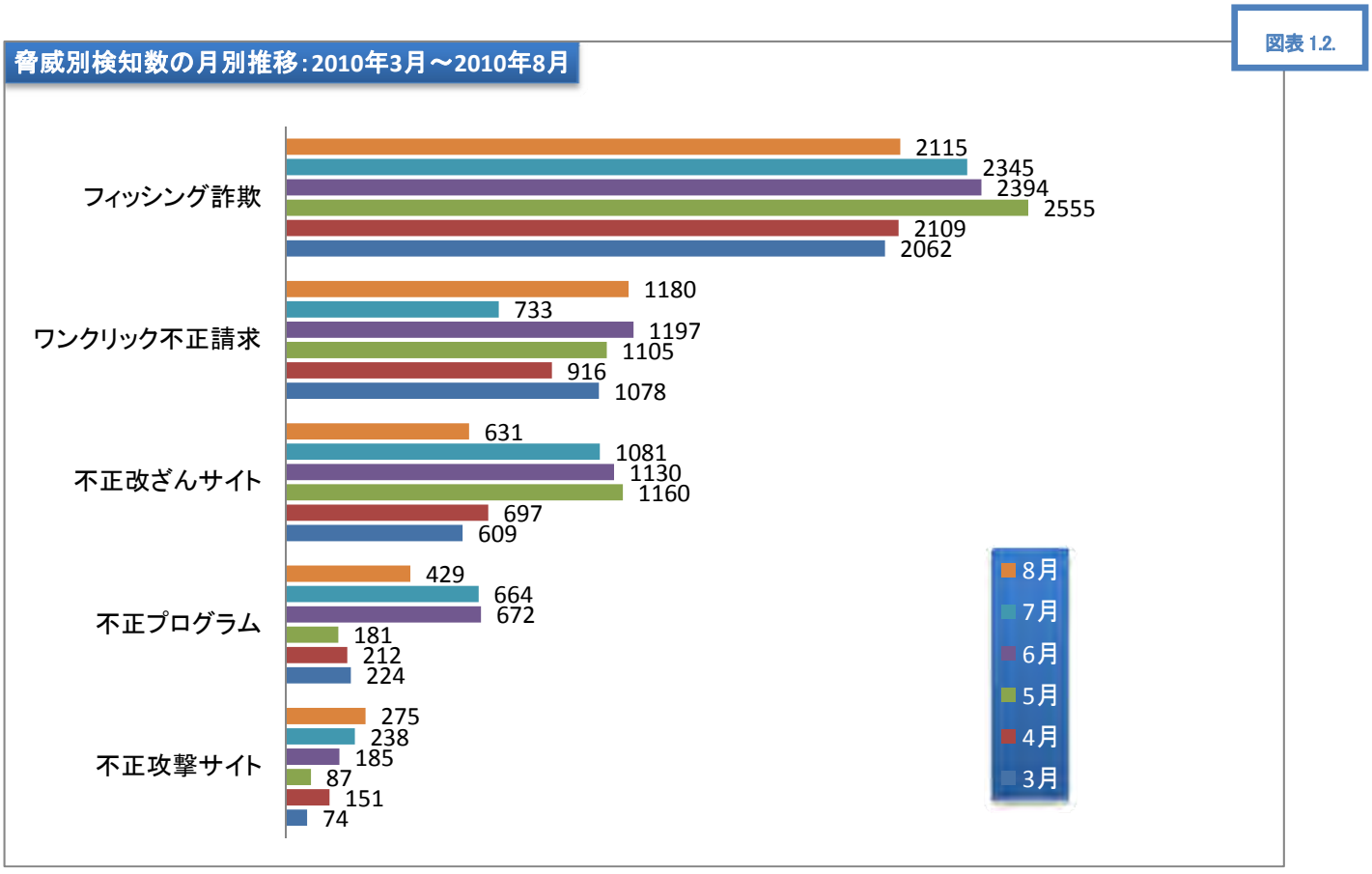
1.1　「危険」と判断されたウェブサイトの数（2010 年 8 月）：4,630 件（図表 1.1.）

図表 1.1



1.2　「gred でチェック」で検知した脅威の月毎の推移（脅威別）（図表 1.2.）（単位：件）

図表 1.2.



1.3　「gred でチェック」月別総利用数（2010/3 月～2010/8 月）（図表 1.3.）

図表 1.3.

月	3 月	4 月	5 月	6 月	7 月	8 月
「gred でチェック」総利用数	54,995	55,025	58,365	57,346	56,419	49,669

- 「危険」と判断されたウェブサイトの件数は、4,630 件（前月比 91.5%、図表 1.1.）。7 月の統計に引続き減少傾向です。
- 「ワンクリック不正請求」の検知数が 1,180 件（前月比 161.0%　図表 1.2.）となり急増しています。

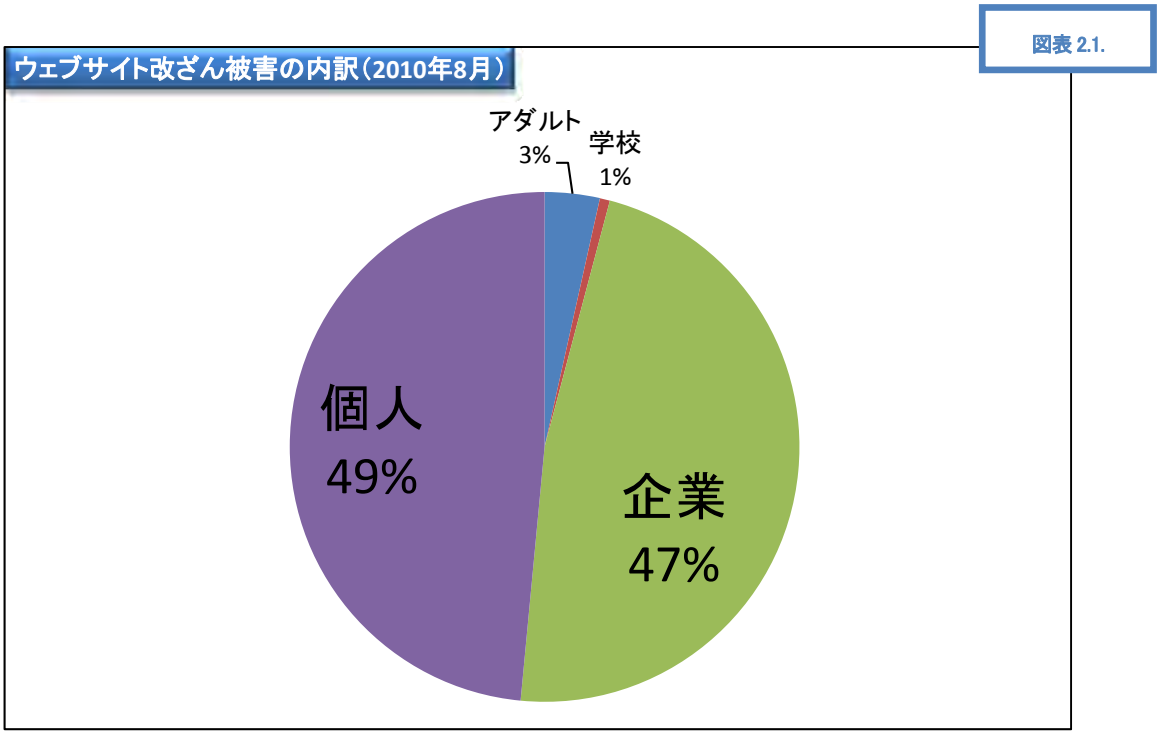
- 「フィッシング詐欺」「不正改ざんサイト」「不正プログラム」は減少傾向です。
- 「不正攻撃サイト」は 275 件（前月比 115.5% 図表 1.2.）となり増加傾向にあります。

1.4 「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。
ワンクリック不正請求	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.

	2010 年 8 月	2010 年 7 月	2010 年 6 月	2010 年 5 月	2010 年 4 月	2010 年 3 月
「危険」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	6.6% （305 件/4,630 件）	15.0% （759 件/5,061 件）	14.6% （813 件/5,578 件）	15.3% （781 件/5,088 件）	9.6% （393 件/4,085 件）	11.2% （453 件/4,047 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	48.3% （305 件/631 件）	70.2% （759 件/1,081 件）	71.9% （813 件/1,130 件）	67.3% （781 件/1,160 件）	56.4% （393 件/697 件）	74.4% （453 件/609 件）

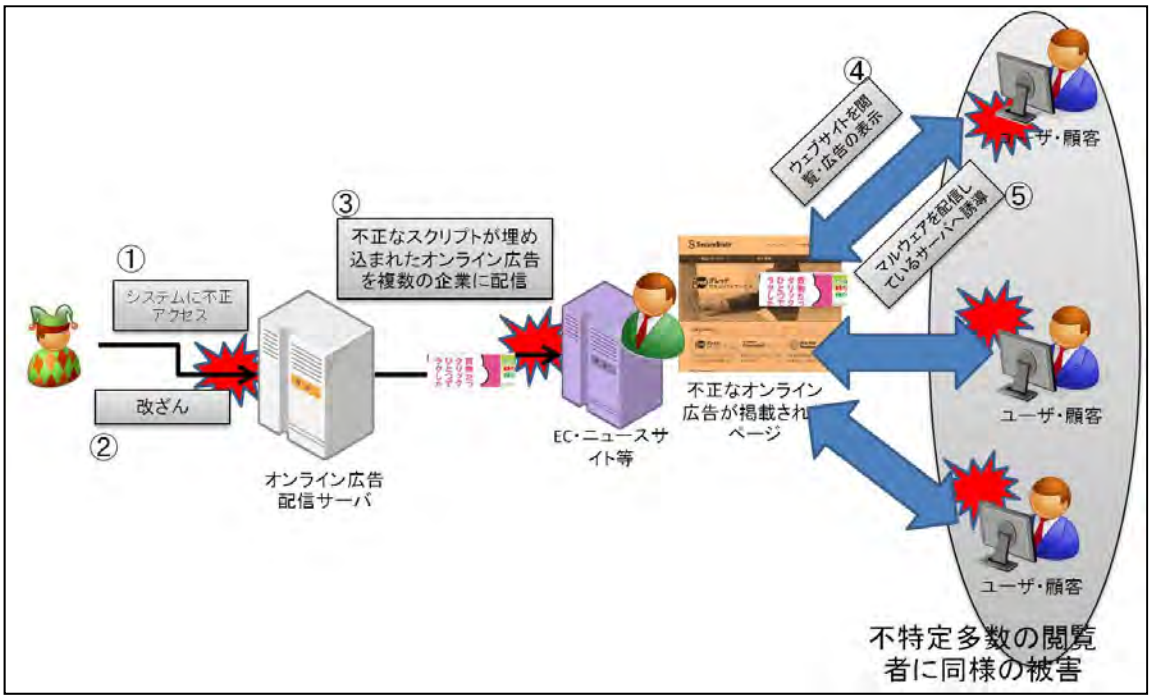
3　オンライン広告配信サービス利用者における改ざん被害が拡大

9 月 24 日以降、オンライン広告配信サービス提供会社（以下　サービス提供会社）が不正アクセス等の攻撃を受け、提供するオンライン広告が改ざんされ「不正なスクリプト」が埋め込まれる被害が発生しています。「改ざんされたオンライン広告」を掲載したウェブサイトは、「不正なスクリプト」により、閲覧したユーザを「マルウェアを配信している悪質なウェブサイト」に誘導します。オンライン広告配信サービスの利用者が、オンライン広告に含まれる「不正なスクリプト」を独自に検知することは困難です。

3.1　サービス提供会社のサーバへ行われた攻撃の概要

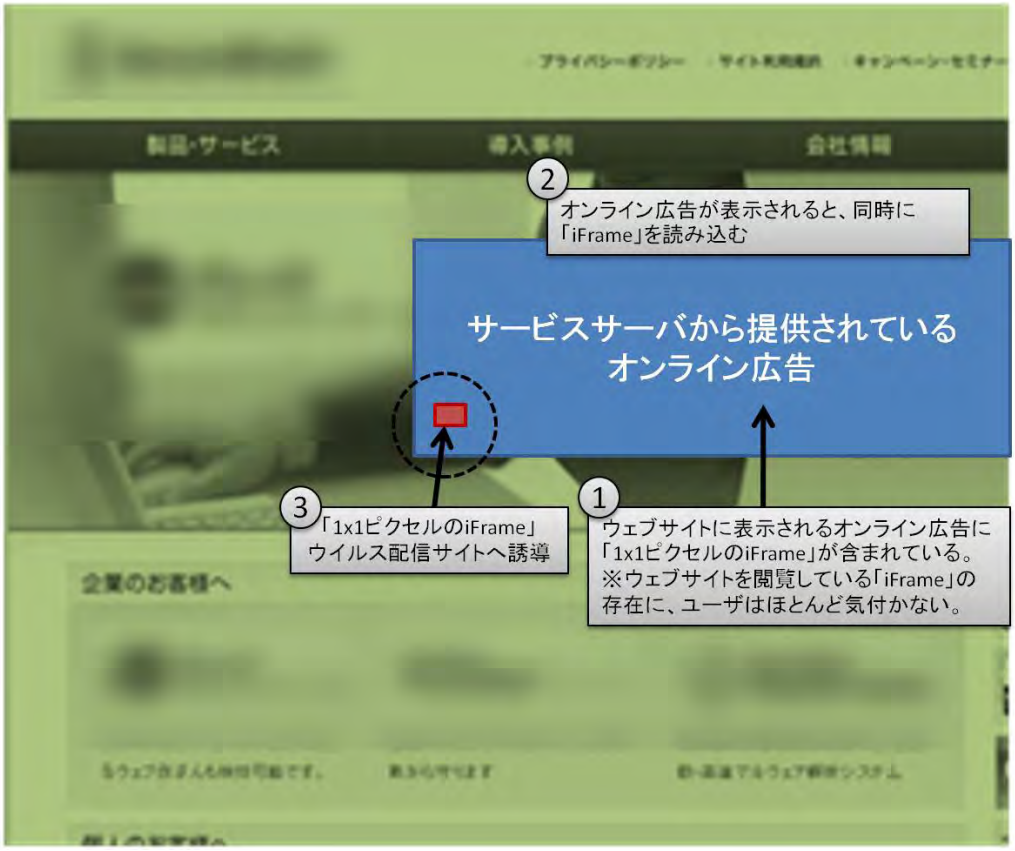
1. オンライン広告の配信サービスを提供するサーバ（以下　サービスサーバ）が第三者により不正アクセス、および改ざん被害を受ける
2. サービスサーバより配信されている一部のオンライン広告に「不正なスクリプト」が埋め込まれた状態になる
3. サービス提供会社のサービス利用者（主に EC サイト、ニュースサイト等）のウェブサイトに「不正なスクリプト」を含んだオンライン広告が掲載される
4. 「不正なスクリプト」を含んだオンライン広告が掲載されたウェブサイトを閲覧したユーザが、「マルウェアを配信しているウェブサイト」に誘導され被害に遭う

図 1：サービスサーバへの攻撃に起因して、ユーザへの被害が及ぶまで



※サービス提供会社を利用している複数のウェブサイトに対して、上記「図 1」の③～⑤までのプロセスが発生し被害が拡大しました。

図２：攻撃手口の詳細



※ウェブサイトを閲覧したユーザが、マルウェア配信サイトに誘導されている事を気付かせないために、上記のような手法を取っている事が考えられます。

3.2　ウェブサイトを運営している企業は継続的な安全確認を

自社ウェブサイトのコンテンツやサービス充実の為の外部サービスは、運用管理の軽減、人的リソースの削減等のメリットがあり、多くの企業が利用しています。今回被害を受けたオンライン広告配信サービスもそのひとつです。しかし、運用管理を外部に委託するということが、そのサービスに潜むリスクの対処についても委託するということにはなりません。むしろ、リスクの管理については、自社で責任を取らなければなりません。

サービスを利用する場合には「便利だから」「コストが削減できるから」というメリットだけでなく、そこに潜むリスクや問題が生じた場合の対処について、十分に配慮したうえで利用を開始すると同時に、定期的にその安全性を確認する為のシステムやサービスを採用して、継続的な安全の確保に努めなければなりません。

4　多言語化される「ワンクリック不正請求」サイト

「ワンクリック不正請求」は、従来日本国内を中心として被害が広まっていました。しかし、最近では、日本語で存在していたページを別の言語に翻訳しているコンテンツが確認されています。

従来「日本語」で存在していたコンテンツが、URL は同じまま「日本語」から「中国語」に変わっているものが確認されています。

【部分的に日本語と中国が混在している「ワンクリック不正請求」サイト】

図表 4.1.

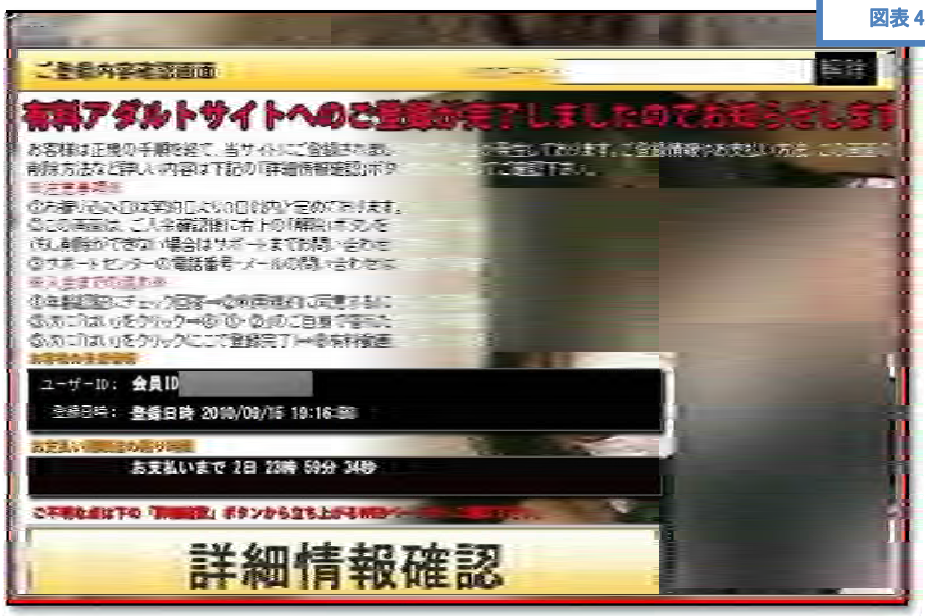
【日本語と中国語で同様のコンテンツと思われるページが存在する例】

●中国語版

図表 4.2.

●日本語版

図表 4.3.



部分的に「日本語」の記載が残存、「不正請求」している金額の振込先に関する情報が無い等、ウェブサイト自体は不完全な状態であることが伺えます。しかし、オンライン犯罪の国際化に繋がり、より悪質な手口、大規模な被害の発生も予想されます。「ワンクリック不正請求サイト」等のオンライン犯罪の動向には今後も注意が必要です。

5　個人・企業それぞれに求められる、セキュリティ対策とは？

5.1　個人向けの対策：「gred でチェック」「Internet SagiWall（インターネット・サギウォール）」「gred AntiVirus アクセラレータ」

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。

また、ウイルス対策を無料で強化する、コミュニティ型ウイルス対策製品「gred AntiVirus アクセラレータ」（http://www.securebrain.co.jp/products/gredavx/index.html）もダウンロード提供を行っています。

また、ウェブサイトのコンテンツやリンク先等複数の要素を解析し、オンライン詐欺サイトや不正プログラム等を配布している危険サイトをブラックリストを使わずに検知する「Internet SagiWall」（http://www.securebrain.co.jp/products/sagiwall/index.html）も提供しています。危険なウェブサイトを閲覧してしまった場合、瞬時に画面を遮断し警告画面を表示します。

■「gred でチェック」URL

http://www.gred.jp

■「Internet SagiWall」の製品紹介 URL

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

■「gred AV アクセラレータ」URL

http://www.securebrain.co.jp/products/gredavx/index.html

5.2　企業向けの対策：「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」は、ブラックリストを使わずに、ウェブサイトの「今の状態」をリアルタイムに判断します。

「gred セキュリティサービス」の「無償トライアル版」は、自社ウェブサイトの URL、アラートメール送信先等の情報を登録するだけで、すぐにサービスを利用開始することができます。「gred セキュリティサービス」は、検査対象となるウェブサイトのコンテンツを、ダウンロードして検査を行いますので、ウェブサイトへの負荷はほとんどかかりません。

■「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