Press Release

2010 年 8 月 27 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.13【2010 年 7 月分統計】

個人が運営するゲームサイトの改ざん被害が急増、ワンクリックサイトへの誘導手口はさらに狡猾に

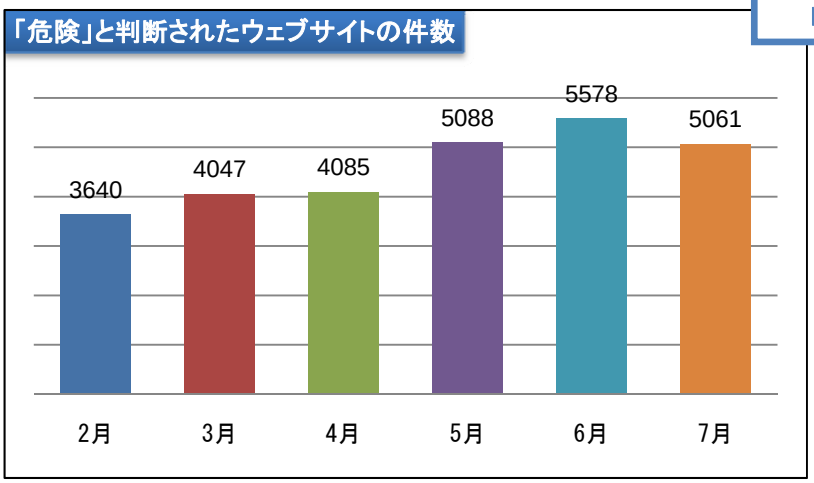
株式会社セキュアブレイン(本社:東京都千代田区、代表取締役社長 兼 CEO:成田 明彦、以下「セキュアブレイン」)はセキュアブレインが運用する、無料のウェブセキュリティサービス「gred(グレッド)でチェック」で収集した情報を基に、「セキュアブレイン先端技術研究所」(以下 先端技術研究所)で分析を行い、その結果を「セキュアブレイン gred セキュリティレポート」として公表します。「gred でチェック」は、インターネットユーザがウェブサイトの安全確認を行うことができる、無料のウェブセキュリティサービスです。確認したいウェブサイトの URL を入力するだけで、セキュアブレインが独自に開発した解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

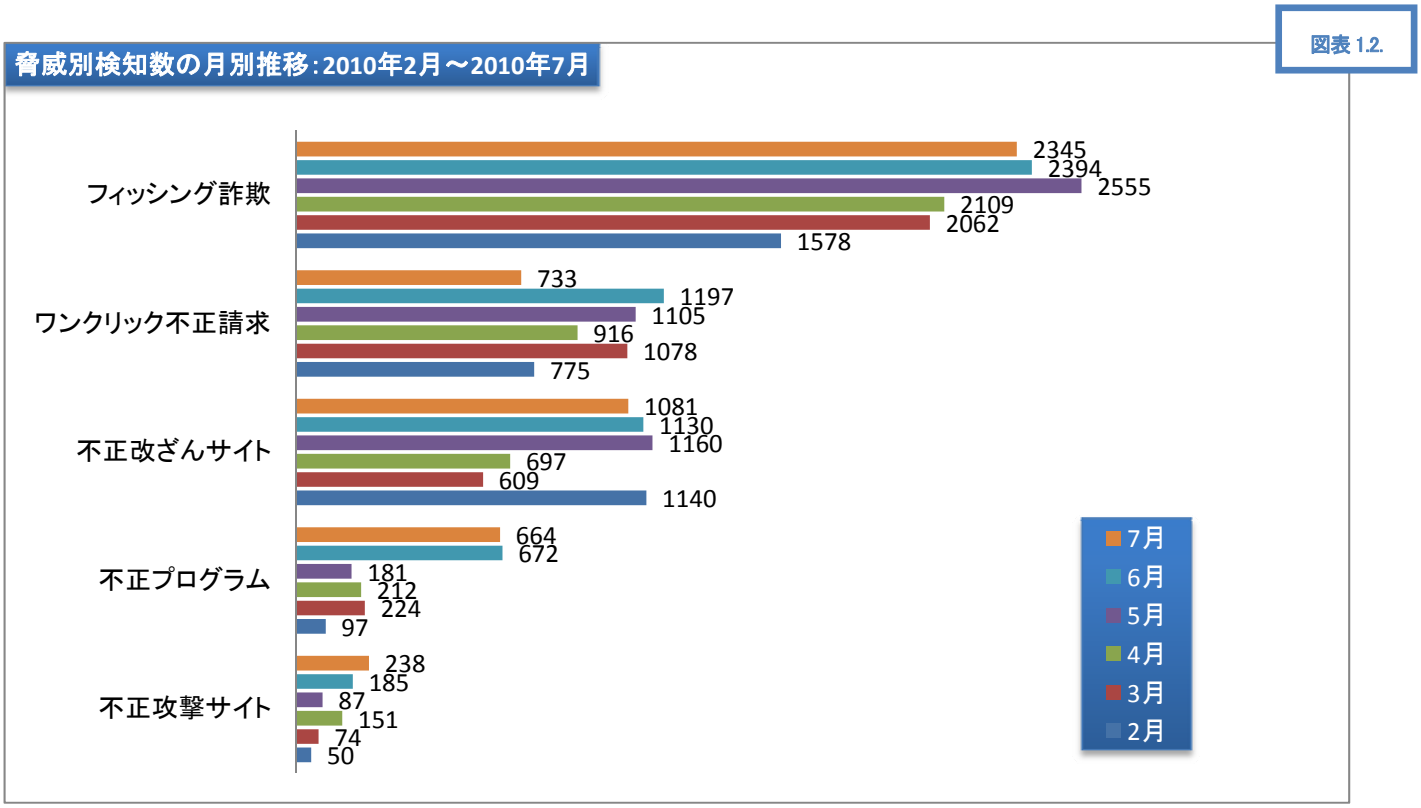
1.1　「危険」と判断されたウェブサイトの数（2010 年 7 月）：5,061 件（図表 1.1.）

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（2010/2 月～2010/7 月）（図表 1.3.）

図表 1.3.

月	2 月	3 月	4 月	5 月	6 月	7 月
「gred でチェック」総利用数	55,927	54,995	55,025	58,365	57,346	56,419

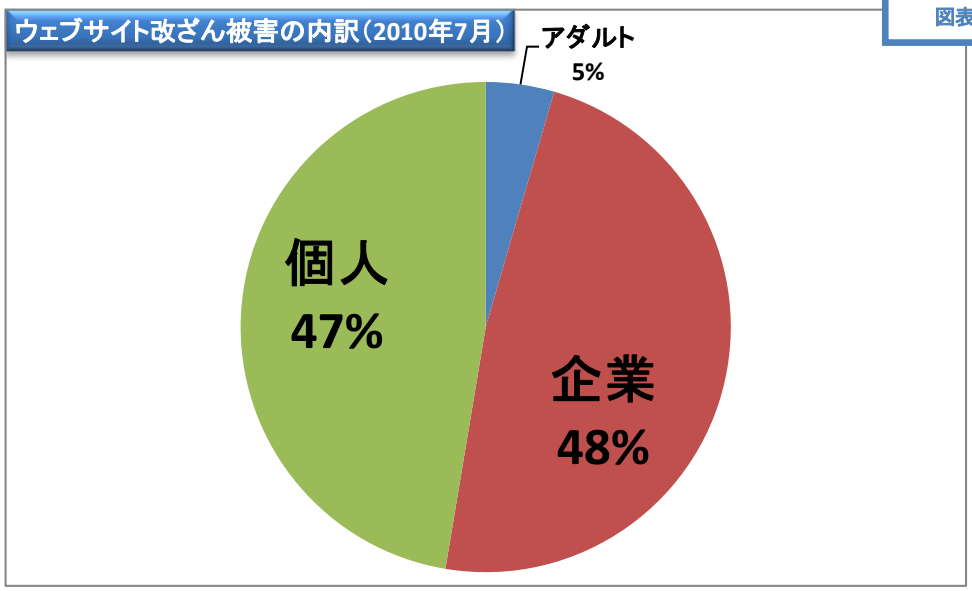
- 「危険」と判断されたウェブサイトの件数は、5,061 件（前月比 90.7%、図表 1）。2010 年の統計では、始めて減少傾向に転じました。

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.

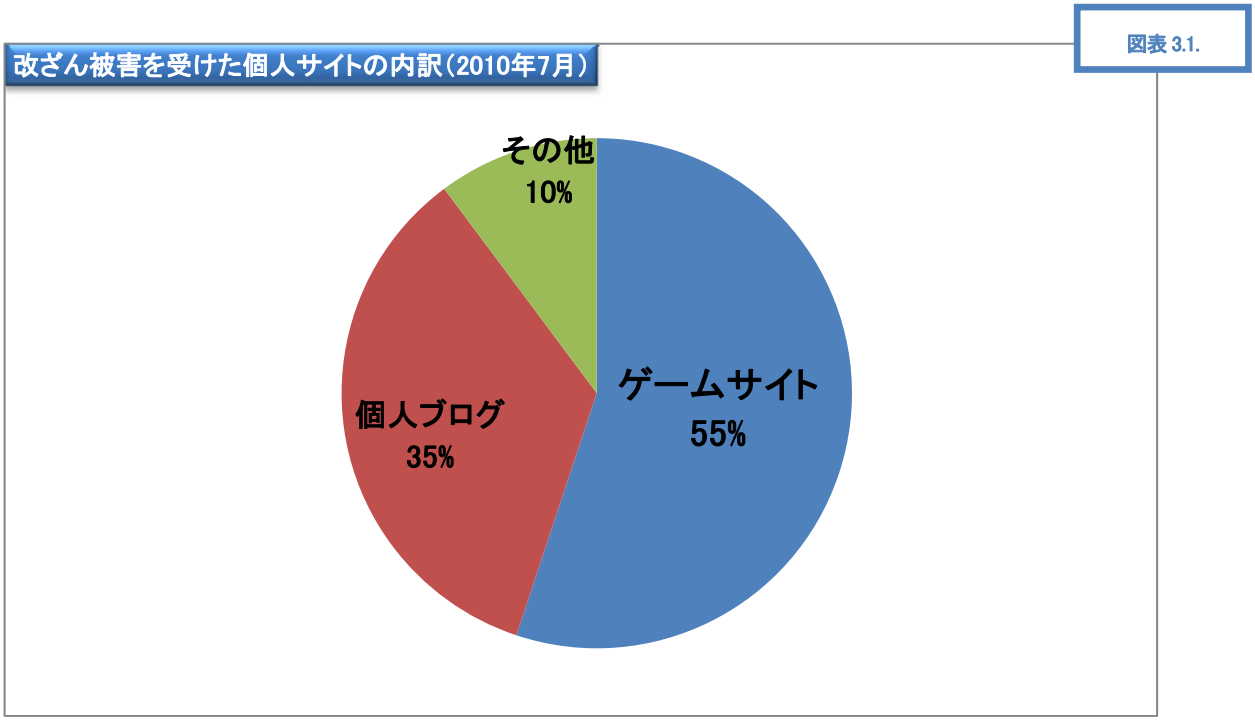


図表 2.2.

	2010 年 7 月	2010 年 6 月	2010 年 5 月	2010 年 4 月	2010 年 3 月	2010 年 2 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	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）	25.3% （921 件/3,640 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	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）	80.8% （921 件/1,140 件）

3　改ざん被害を受けた個人サイトの傾向について（図表 3.1.）

依然として、多くのウェブサイトが改ざん被害を受けています。「図表 2.1.」のグラフに記載されているように「個人サイト」が改ざんされる割合も増加しています。「gred でチェック」で検知された「不正改ざんサイト」をさらに追跡調査し、「改ざん被害を受けた個人サイトの傾向」を調査しました。



3.1　個人が運営するゲームサイトの被害が急増

「gred セキュリティレポート Vol.10【2010 年 4 月分統計】」では、改ざん被害を受けた個人サイトの 90%は「ブログ」サイトでしたが、今回の統計では、「ゲームサイト」へ被害が拡大している事が分かります。

「ゲームサイト」の被害は、1)「他のウェブサイトに誘導する様なコードが埋め込まれている場合」と 2)「閲覧者の PC に不正プログラムをダウンロードするような、直接攻撃を仕掛けるようなコードが埋め込まれている場合」の 2 種類に大別されます。オンラインゲームの運営者は日本に限らず、韓国、台湾、米国のサイトが見受けられます。これらのウェブサイトの多くは個人で運営されており、改ざんされたことに気づかず「放置」され、長期間にわたり被害が拡大する可能性があります。ゲームサイトの閲覧に際しては、十分な注意が必要です。

4　「ワンクリック不正請求」の傾向について

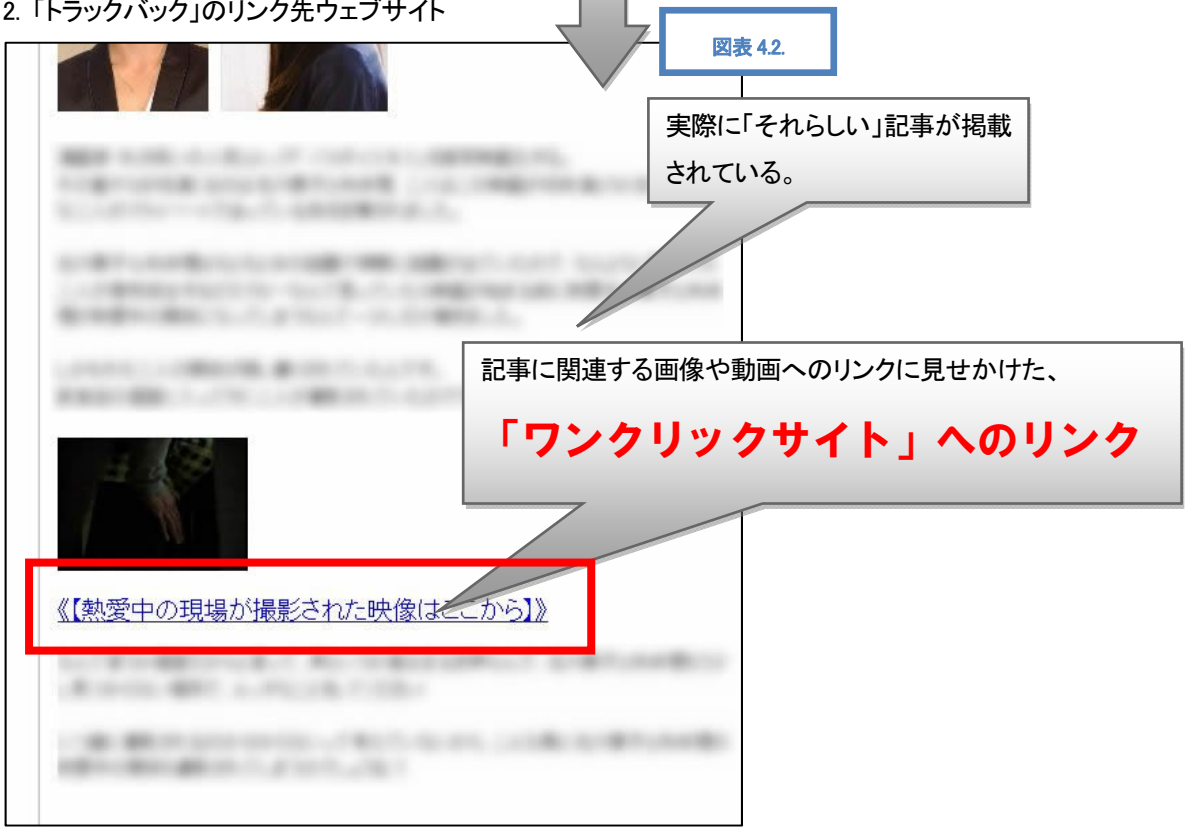
「ワンクリック不正請求」は、アダルトコンテンツ等の閲覧を行おうとした際に、「料金請求の画面」を表示させて、脅迫、金銭をだまし取る「インターネット詐欺の一種」です。詳細についてはセキュアブレインのウェブサイト「進化するインターネットの脅威」の「ワンクリック詐欺って何？」（http://www.securebrain.co.jp/products/sagiwall/menace.html）をご覧ください。

4.1　「ワンクリックサイト」へ誘導する狡猾な手口（図表 4.1. . 4.2.）

「ワンクリック不正請求を行っているウェブサイト」（以下　ワンクリックサイト）へ誘導する為の手法も多様化しています。以下では一般のウェブサイトや有名人ブログの「トラックバック機能」を悪用する手法を、注意喚起も含めてご説明します。

1. 悪質なウェブサイトへの「トラックバック」が掲載された、有名人のブログサイト

2. 「トラックバック」のリンク先ウェブサイト



4.2 有名人のブログのトラックバックを悪用した「ワンクリックサイト」への誘導手法の特徴（図表 4.3.）

- その有名人の活動と特に関係のない「トラックバック」が多数掲載されている。（図表 4.1.参照）
- 「トラックバック」の内容が「有名人の噂」や「ゴシップ記事」である。（図表 4.1.参照）
- リンク先の記事の中に「映像はこちら」「動画はこちら」のようなリンクがある。（図表 4.2.参照）
- ブログのエントリーが 1 日しかない（図表 4.3.参照）

このような状況は有名人のブログのみならず、一般のブログでも発生する可能性があります。ブログのトラックバックは、各ブログの運営者（そのブログを執筆している個人や企業）の責任において管理されます。その為、「トラックバックをすべて許可する」設定にしてしまうと、上記のような「悪質なトラックバック」が掲載され、ブログの閲覧者に被害が及ぶ可能性があるため、「トラックバックの設定」等に注意する必要があります。

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