Press Release

2011 年 1 月 31 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.18【2010 年 12 月分統計】

当社の「セキュリティ講座」ページを模倣した悪質なページが登場。インターネット利用者へ注意喚起

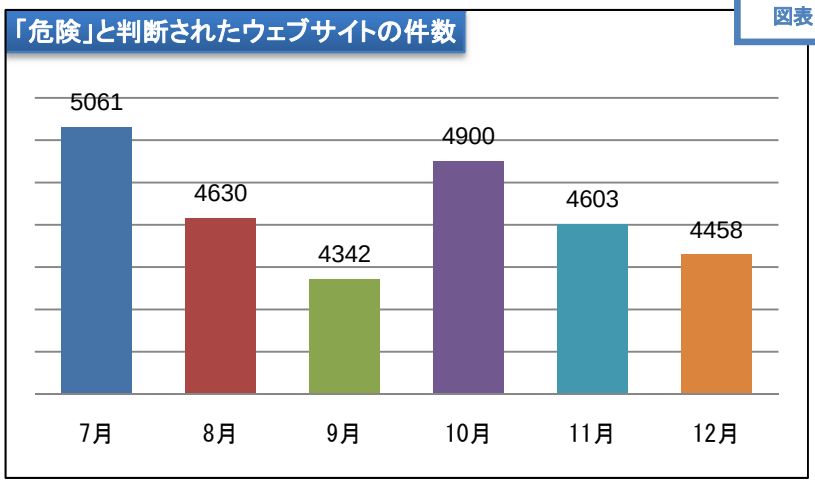
株式会社セキュアブレイン(本社:東京都千代田区、代表取締役社長 兼 CEO:成田 明彦、以下「セキュアブレイン」)はセキュアブレインが運用する、無料のウェブセキュリティサービス「gred(グレッド)でチェック」で収集した情報を基に、「セキュアブレイン先端技術研究所」(以下 先端技術研究所)で分析を行い、その結果を「セキュアブレイン gred セキュリティレポート」として公表します。「gred でチェック」は、インターネットユーザがウェブサイトの安全確認を行うことができる、無料のウェブセキュリティサービスです。確認したいウェブサイトの URL を入力するだけで、セキュアブレインが独自に開発した解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

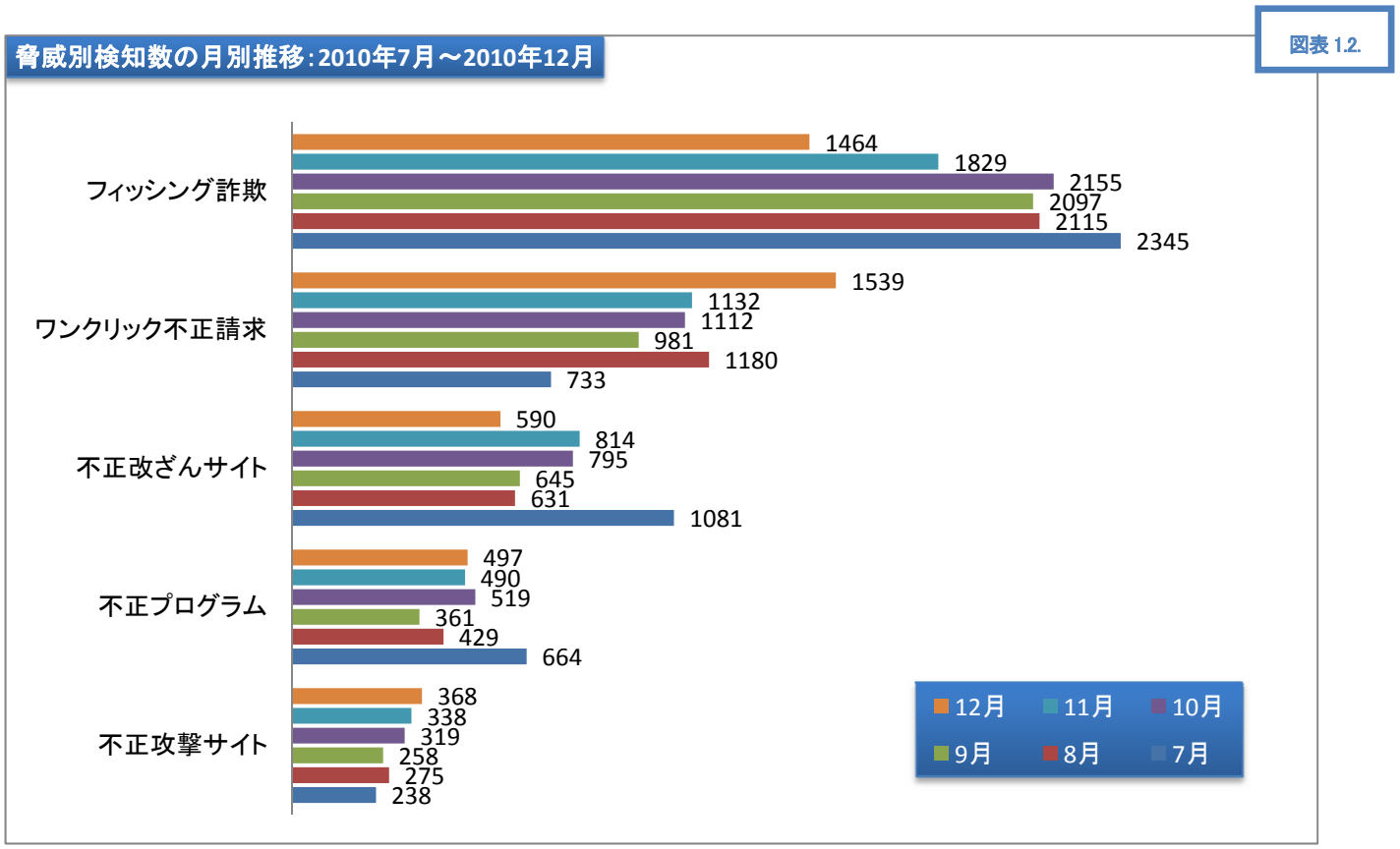
1.1　「危険」と判断されたウェブサイトの数（図表 1.1.）

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	56,419	49,669	49,565	49,720	44,901	43,060

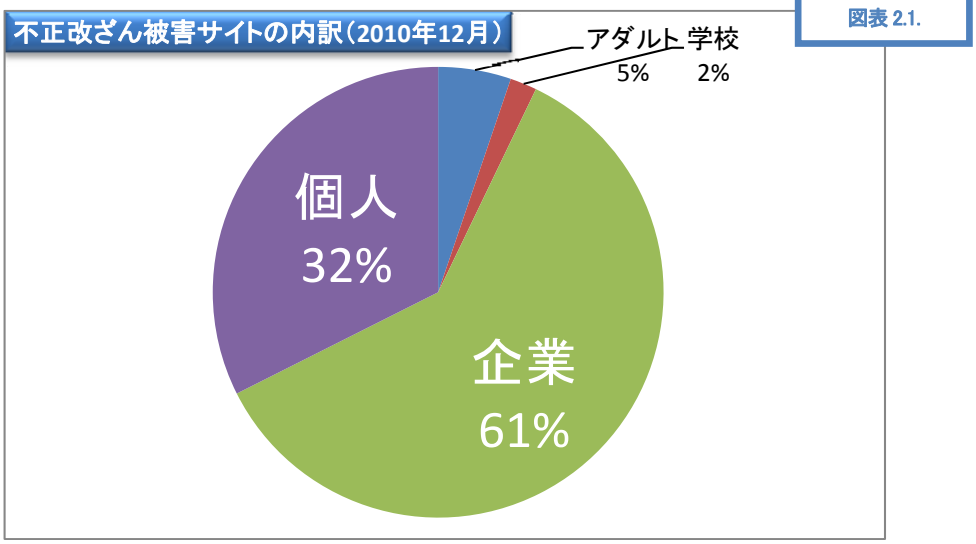
- 「危険」と判断されたウェブサイトの件数は、4,458 件。（前月比 96.8%、図表 1.1.）
- 「ワンクリック不正請求」の検知数が急増しています。（前月比 136.0%、図表 1.1）
- 「不正攻撃サイト」の検知数が僅かですが上昇傾向にあります。（図表 1.1）

「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 12 月	2010 年 11 月	2010 年 10 月	2010 年 9 月	2010 年 8 月	2010 年 7 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	6.3% （281 件/4,458 件）	13.3% （610 件/4,603 件）	7.0% （344 件/4,900 件）	5.2% （226 件/4342 件）	6.6% （305 件/4,630 件）	15.0% （759 件/5,061 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	47.6% （281 件/590 件）	74.9% （610 件/814 件）	43.3% （344 件/795 件）	35.0% （226 件/645 件）	48.3% （305 件/631 件）	70.2% （759 件/1,081 件）

3　セキュアブレインの「セキュリティ講座」ページを模倣した悪質なページが存在。（現在は閉鎖）

2011 年 1 月 15 日、当社の「セキュリティ講座」ページのコンテンツを盗用し、「ワンクリック不正請求」に関する不正確な記載を行っている悪質なウェブサイトが発見されました。

当該ウェブサイトのコンテンツは既に削除されています。

<<当社のコンテンツ>>（図表 3.1,）

<<盗用されたコンテンツ>>（図表 3.2,）

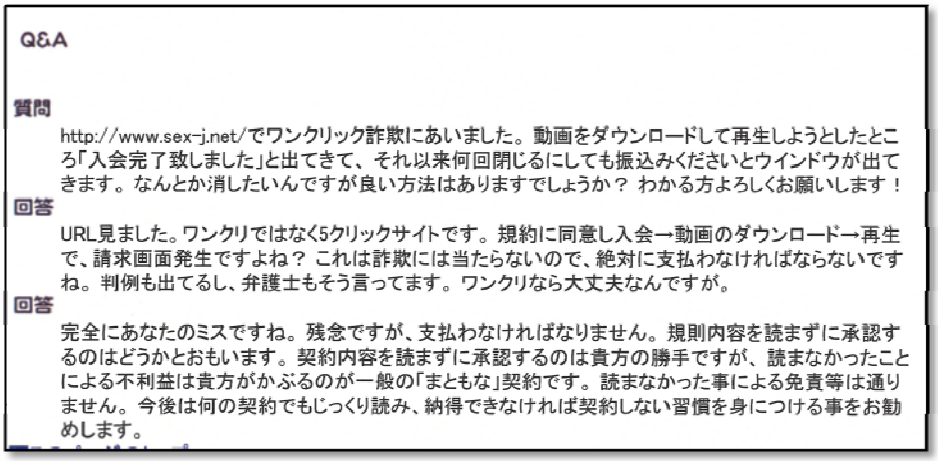
当該ウェブサイトでは、上記以外のページについても盗用を行っています。また、「ワンクリック不正請求」の危険性を説く他のウェブサイトについても盗用が行われている事が判明しています。

巧妙に「詐欺行為」を正当化

このウェブサイトでは、コンテンツを盗用したページ以外に、「ワンクリック不正請求」サイトのスクリーンショットや Q&A を使って、その正当性を主張する内容も確認されています。

また、別の「ワンクリック不正請求」の危険性を啓発する他のサイトでも、同様にコンテンツを盗用する事例が報告されています。

<<「ワンクリック不正請求」を正当化するようなコンテンツ>>（図表 3.3,）


Q&A

質問

http://www.sex-j.net/でワンクリック詐欺にあいました。動画をダウンロードして再生しようとしたところ「入会完了致しました」と出てきて、それ以来何回閉じるにしても振込みくださいとウインドウが出てきます。なんとか消したいんですが良い方法はありますでしょうか？ わかる方よろしくお願いします！

回答

URL見ました。ワンクリではなく5クリックサイトです。規約に同意し入会→動画のダウンロード→再生で、請求画面発生ですよね？ これは詐欺には当たらないので、絶対に支払わなければならないですね。判例も出てるし、弁護士もそう言ってます。ワンクリなら大丈夫なんですが。

回答

完全にあなたのミスですね。残念ですが、支払わなければなりません。規則内容を読まずに承認するのはどうかとおもいます。契約内容を読まずに承認するのは貴方の勝手ですが、読まなかったことによる不利益は貴方がかぶるのが一般の「まともな」契約です。読まなかった事による免責等は通りません。今後は何の契約でもじっくり読み、納得できなければ契約しない習慣を身につける事をお勧めします。

「脅し」に負けない為に…

アダルトコンテンツ等を閲覧した際に「突然」請求画面が表示され、「脅し」の様な文章が表示されるウェブサイトは、「ワンクリック不正請求」である可能性が高いです。脅しの文章には、アクセスした人の住所や連絡先の情報が、ウェブサイトの運営者に伝わってしまっているような記載がありますが、それらの個人情報は自分自身で入力しない限り、相手に伝わることはありません。

当社では、「ワンクリック不正請求」をはじめとした、インターネット上の不正な行為や、危険なプログラムについての情報をわかりやすく説明したページを公開しております。http://www.sagiwall.jp/knowledge/

4　ウェブ改ざん被害の長期放置について

13.9%のウェブサイトでは複数月に渡って放置

2010 年 7 月～2010 年 12 月（6 ヶ月）に報告された「不正改ざんサイト」URL を調査したところ、全体の 13.9%の URL が複数の月に渡って報告されていることがわかりました。詳細については以下の図表 4.1,をご覧ください。

（図表 4.1,）

継続月数	件数
6 ヶ月報告	2 件
5 ヶ月報告	2 件
4 ヶ月報告	6 件
3 ヶ月報告	35 件
2 ヶ月報告	131 件
連続無し	1,088 件

複数の攻撃者が、ひとつのウェブサイトを攻撃？

複数月に渡って報告がされているウェブサイトを詳細に調査すると、埋め込まれている不正スクリプトが変化していることが判明しています。（図表 4.2,）

サイト	確認日時	改ざんタイプ
ウェブサイト A	2010/5/31	Gumblar.8080
	2010/7/2	Gumblar.X
	2010/12/13	終了確認（約 6 か月感染）
ウェブサイト B	2010/5/27	Gumblar.X
	2010/11/21	Gumblar.X,MSTMP
	現在（7 ヶ月以上感染中）	Gumblar.X,MSTMP
ウェブサイト C	2010/7/2	Gumblar.8080
	2010/12/13	Gumblar.X
	2010/12/16	Gumblar.X, Gumblar.8080
	現在（6 ヶ月以上感染中）	Gumblar.X, Gumblar.8080
ウェブサイト D	2010/12/15	MSTMP
	現在（1 ヶ月以上感染中）	MSTMP

「改ざんタイプ」に変化している原因としては、以下のようなことが考えられます。

- 感染サイトの情報が売買されて、複数からの攻撃が行われている
- 1 人（1 グループ）が同じサイトに攻撃
- テストサイトとして利用している？

また、タイプが変化するだけではなく、同じタイプでも「異なるウェブサイトを呼出す」ように、不正スクリプトの内容が変化しているものも確認されています。

「改ざん被害サイトの長期放置」については、以下のような原因が考えられます。

- 根本的な対策が不十分な為、再感染している。
- 感染していることに気付いていない（対応する気がない）
- 管理されていないウェブサイト（放置サイト）の存在

ウェブサイト改ざんの攻撃手法が細分化、多様化するにつれ、「ブラックリスト」を活用した検知は困難になります。その為「ブラックリスト」を使用せずに、「改ざん」を検知するソリューションが必要となります。また、改ざんを長期間放置することは、自社のウェブサイトを閲覧したユーザに及ぶ被害を放置している事になり、企業の信頼性を大きく損なうことになります。特に EC を行っている企業にとっては自社の売上に直接影響する、大きな損害を受ける恐れもあります。

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」（https://www.gred.jp/avx/download.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.sagiwall.jp/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.sagiwall.jp/index.html

■「gred AV アクセラレータ」URL

http://www.gredavx.jp/

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