PRESS RELEASE

2010 年 6 月 18 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.11【2010 年 5 月分統計】

「危険なウェブサイト」の検知数が統計開始後の最高値を記録。ウェブサイトの改ざんが再び増加傾向に。

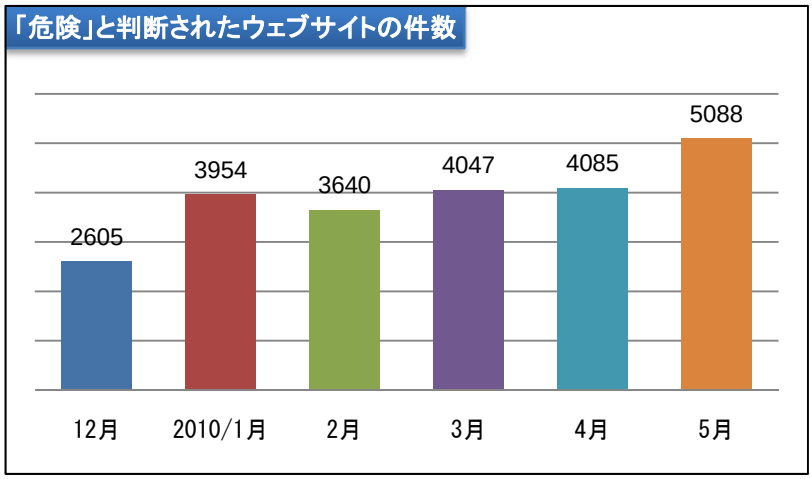
株式会社セキュアブレイン(本社:東京都千代田区、代表取締役社長 兼 CEO:成田 明彦、以下「セキュアブレイン」)はセキュアブレインが運用する、無料のウェブセキュリティサービス「gred(グレッド)でチェック」で収集した情報を基に、「セキュアブレイン先端技術研究所」(以下 先端技術研究所)で分析を行い、その結果を「セキュアブレイン gred セキュリティレポート」として公表します。「gred でチェック」は、インターネットユーザがウェブサイトの安全確認を行うことができる、無料のウェブセキュリティサービスです。確認したいウェブサイトの URL を入力するだけで、セキュアブレインが独自に開発した解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

目次

1　gred セキュリティレポート概要

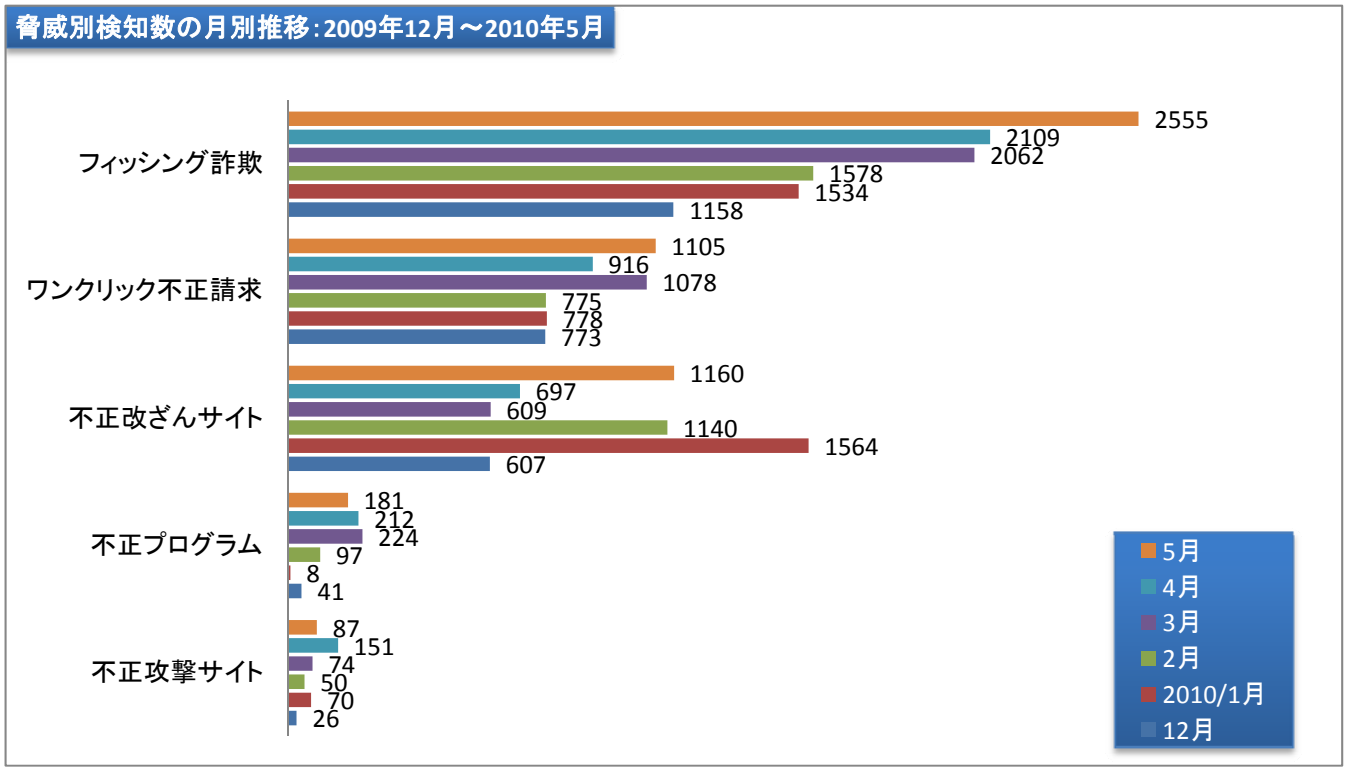
1.1　「危険」と判断されたウェブサイトの数

（2010 年 5 月）：5.088 件（図表 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 2）（単位：件）



1.3　「gred でチェック」月別総利用数（2009/12 月～2010/5 月）

月	12 月	2010/1 月	2 月	3 月	4 月	5 月
「gred でチェック」総利用数	40,697	70,999	55,927	54,995	55,025	58,365

- 「危険」と判断されたウェブサイトの件数は、5,088（前月比 124.6%、図表 1）。2009 年 5 月の統計開始後の最高値を前月に続き更新しました。
- 「フィッシング詐欺」の検知数が、前月に続き、今月も増加しました。2010 年 5 月の検知数 2,555 件（前月比 121.2%）は統計開始後の最高値です。

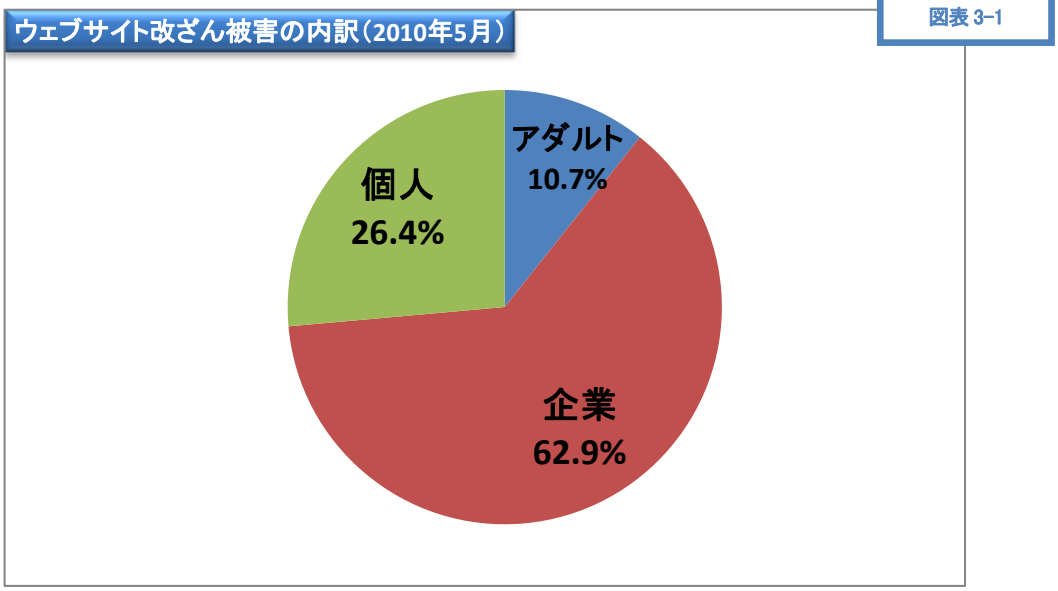
- 「ワンクリック不正請求」の検知数が 1,105 件（前月比 120.6%）となり、上昇傾向にあります。
- 「不正改ざんサイト」の検知数が 1,160 件（前月比 166.4%）となり、Gumblar（ガンブラー）による被害が大量に発生した、2010 年 1 月以来の高い数値になっています。

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 3-1、3-2）

図表 3-1



図表 3-2

	2010 年 5 月	2010 年 4 月	2010 年 3 月	2010 年 2 月	2010 年 1 月	2009 年 12 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	15.3% （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）	31.6% （1,248 件/3,954 件）	12.9% （336 件/2,605 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	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）	79.8% （1,248 件/1,564 件）	55.4% （336 件/607 件）

「企業」「個人」の比率には、大きな変化は見られません。しかし、「gred でチェック」で検知された悪質サイトに占める「Drive by Download タイプの攻撃」、また「不正改ざんサイト」として検知されたウェブサイトに占める「Drive by Download タイプの攻撃」について、いずれも増加しています。

3 「不正改ざんサイト」＋ αの攻撃に注意

- 「Drive by Download タイプの攻撃」では、改ざんしたウェブサイトに「不正な Java スクリプト」埋め込みによる、悪質ウェブサイトへの誘導、ウイルス等不正プログラムのダウンロード等の被害が代表的です。しかし、最近では「不正な改ざん」を行ったウェブサイトにワンクリック詐欺サイトやフィッシング詐欺サイト等の「不正なコンテンツ」を設置するケースが確認されています。
- 「Drive by Download タイプの攻撃」では、攻撃対象となるウェブサイト管理者の ID、パスワードを盗み、その管理権限が及ぶ範囲のウェブサイトのコンテンツに改ざんが行われています。攻撃する側が管理権限を有している事を悪用し、同一サーバに「ワンクリック詐欺」や「フィッシング詐欺」の不正なコンテンツをアップロードしたものと思われます。
- ウェブサイトの管理者は、既存のウェブサイトが改ざんされていないかを監視することに加えて、サーバに別のフォルダーが作られ、ワンクリック詐欺やフィッシング詐欺のコンテンツが埋め込まれていないかについても、監視しなければなりません。

3.1 「不正なコンテンツ」を設置された事例

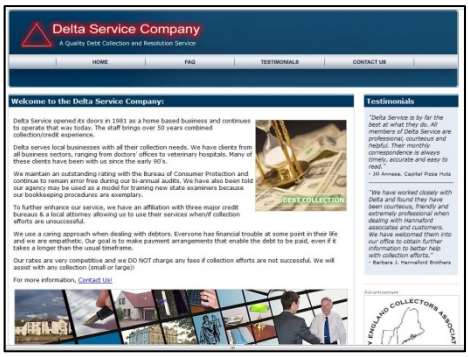
http://xxx.jp/

不正コンテンツ設置用に作られたフォルダー

http://xxx.jp/girl/girlxxx.html ← 不正なコンテンツ

日本の企業のウェブサイトに「ワンクリック詐欺」のコンテンツが埋め込まれた事例。コンテンツ設置用のフォルダーを作成し、そこにコンテンツを作成している。

http://xxxxservice.com/



http://xxxxservice.com/r.html ← 不正なコンテンツ。他にも「x.html」、「v.html」等のファイルが設置されていた。

米国の企業のウェブサイトに「フィッシング詐欺（薬品の違法販売）」を埋め込まれた事例。トップページと同じ階層にコンテンツを置いている。このケースでは、同一のコンテンツが複数のファイル名で設置されていた。

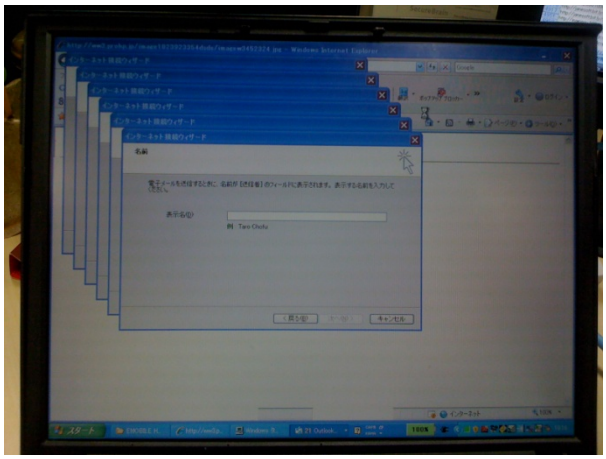
ウェブサイトの「不正な改ざん」による「不正なコンテンツ」の設置に管理者が気付かず、「不正なコンテンツ」が長期間にわたって残存してしまう事例も確認されています。防止する為には、コンテンツの常時、または定期的な監視を行わなければなりません。管理者が、目視でこれらのファイルが作成されたことに気付くことは極めて困難です。

4 「ブラウザクラッシャー」による攻撃について

4.1 「ブラウザクラッシャー」とは？

- 「gred でチェック」には「不正攻撃サイト」として多くの「ブラウザクラッシャーサイト」が報告されています。「ブラウザクラッシャーサイト」は一旦閲覧してしまうと、大量のダイアログや、常に画面上を移動するウィンドウ等を表示し、ユーザのブラウザの使用を妨げるような攻撃を行います。
- これらの攻撃により、CPU の使用率が断続的に 100%となってしまい、他の操作が行えない状態や、パソコンの強制終了による作業内容の消去等の被害が発生します。最悪の場合、OS の起動に悪影響を及ぼし、パソコンの再インストールが必要となる場合もあります。

4.1.1 大量のウィンドウが表示される「ブラウザクラッシャーサイト」の例



4.1.2 その他の「ブラウザクラッシャー」の種類

- ブラウザの変形（横長、縦長）
- ブラウザが振動
- 音楽が急に鳴りだす
- ブラウザ内の表示が真っ黒になる
- 巨大な画像を張り付ける
- メールソフトが自動的に起動する
- フロッピディスクドライブへの断続的なアクセスが発生する etc.

4.2 「ブラウザクラッシャー」の防止

「怪しいサイトを閲覧しない」「知らない人からのメールに記載されているリンクをクリックしない」「セキュリティソフトを使用する」等の、インターネット利用時の基本的な注意事項を実践することで、「ブラウザクラッシャー」による被害を防止することが可能です。

また、ブラウザのセキュリティ設定を強化することで、防止することも可能です。お使いのブラウザの設定を確認してください。

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