

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.19【2011年1月分統計】

企業に集中する Drive by Download 攻撃

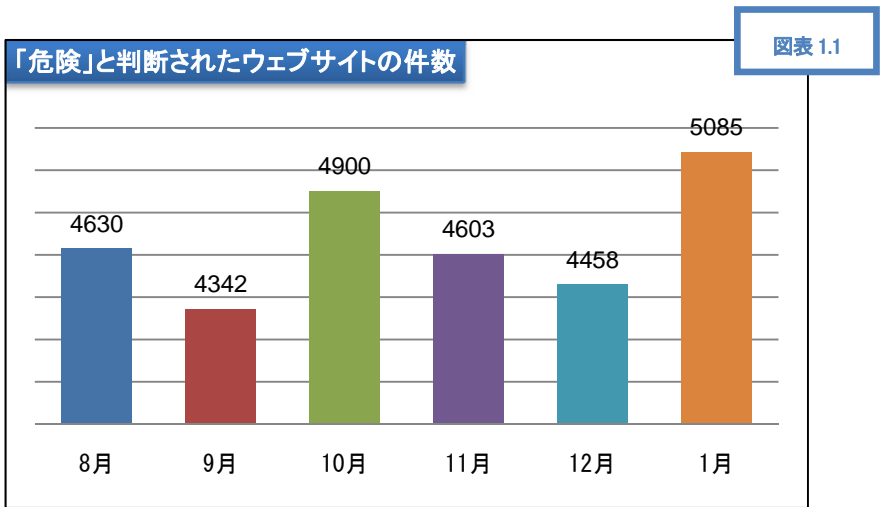
株式会社セキュアブレイン(本社:東京都千代田区、代表取締役社長 兼 CEO:成田 明彦、以下「セキュアブレイン」)はセキュアブレインが運用する、無料のウェブセキュリティサービス「gred(グレッド)でチェック」で収集した情報を基に、「セキュアブレイン先端技術研究所」(以下 先端技術研究所)で分析を行い、その結果を「セキュアブレイン gred セキュリティレポート」として公表します。「gred でチェック」は、インターネットユーザがウェブサイトの安全確認を行うことができる、無料のウェブセキュリティサービスです。確認したいウェブサイトの URL を入力するだけで、セキュアブレインが独自に開発した解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

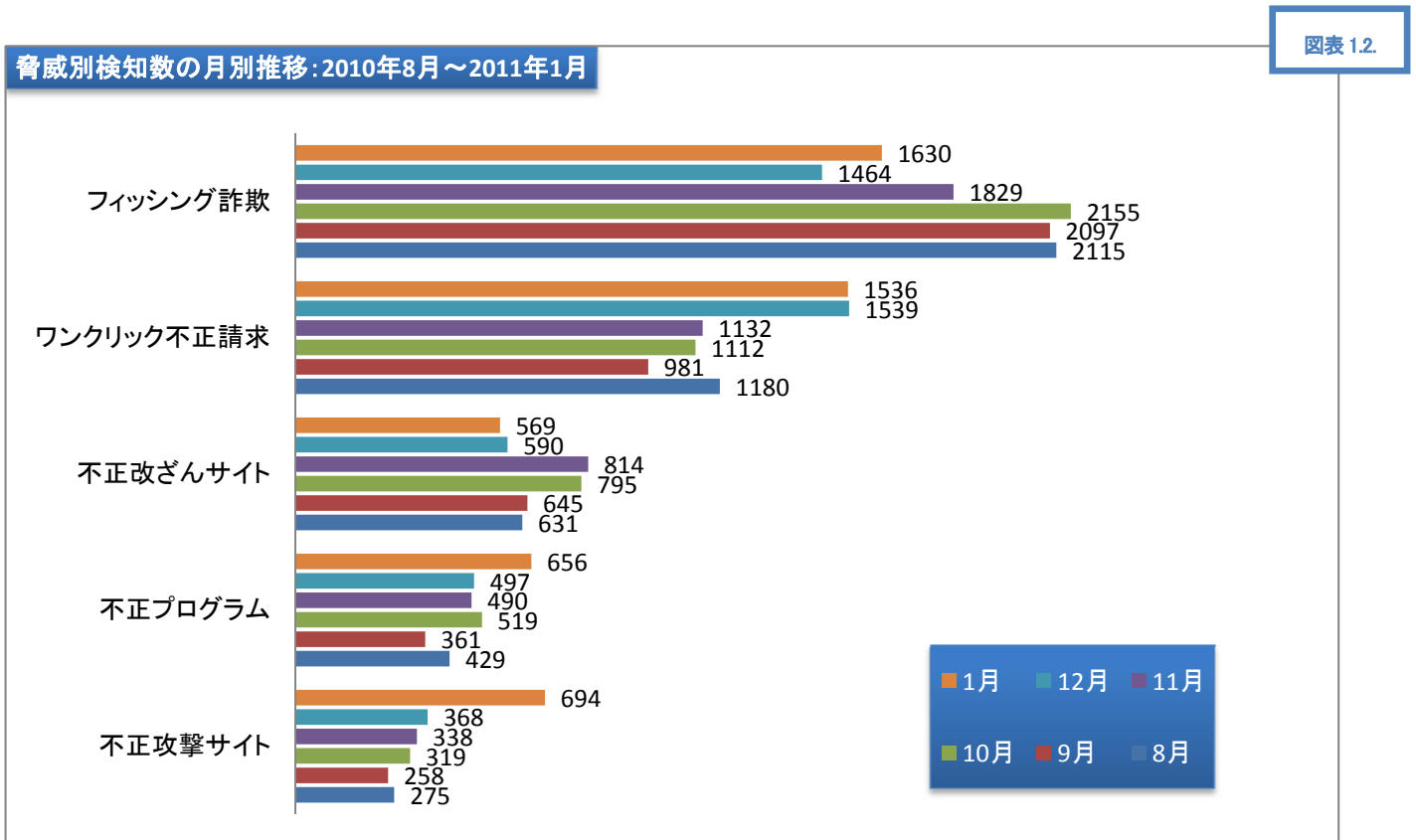
1	gred セキュリティレポート概要.....	2
1.1	「危険」と判断されたウェブサイトの数(図表 1.1.).....	2
1.2	「gred でチェック」で検知した脅威の月別推移(脅威別)(図表 1.2.).....	2
1.3	「gred でチェック」月別総利用数(図表 1.3.).....	2
2	数値で見る「不正改ざんサイト」の内訳(図表 2.1., 2.2.).....	3
3	Drive by Download 攻撃の対象はやはり企業に集中(図表 3.1., 3.2.).....	4
	依然として続く企業ウェブサイトの改ざん.....	4
4	「ショート URL」にご注意ください。.....	5
	「不正攻撃サイト」報告の 14.3%は「ショート URL」.....	5
	クリックする前に「gred でチェック」でリンクを無料チェック.....	5
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
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」.....	5
5.2	企業向けの対策:「gred セキュリティサービス」.....	6

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.)



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.)



1.3 「gred でチェック」月別総利用数(図表 1.3.)

図表 1.3 「gred でチェック」月別総利用数

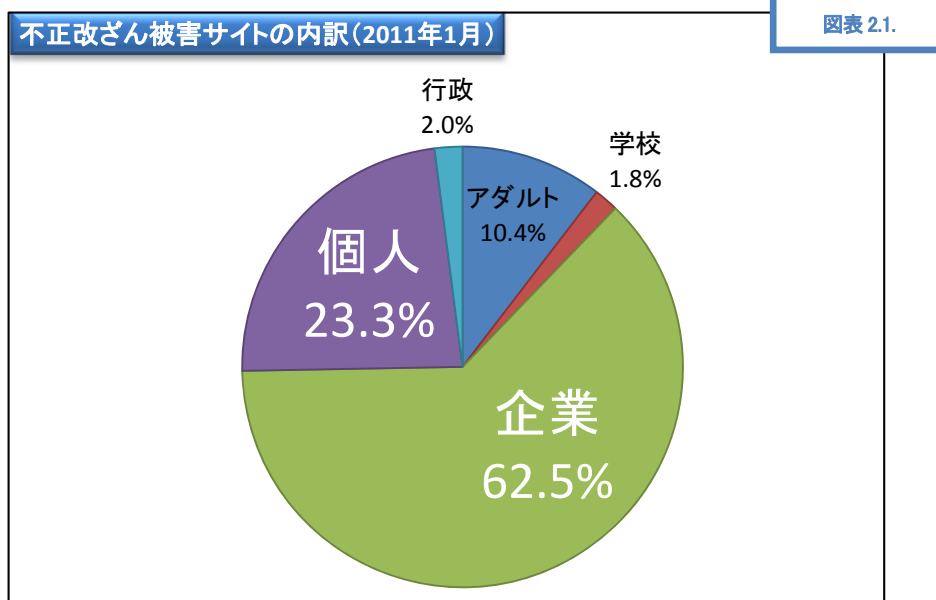
月	8月	9月	10月	11月	12月	2011/1月
「gred でチェック」総利用数	49,669	49,565	49,720	44,901	43,060	46,034

- 「危険」と判断されたウェブサイトの件数は、5,085 件。(前月比 114.1%、図表 1.1.)
- 「不正プログラム」の検知数が増加しています。(前月比 132.0%、図表 1.1.)
- 「不正攻撃サイト」の検知数が急増しています。(前月比 188.6%、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、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.

	2011年1月	2010年12月	2010年11月	2010年10月	2010年9月	2010年8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	5.2% (266 件/5,085 件)	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/4,342 件)	6.6% (305 件/4,630 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	46.7% (266 件/569 件)	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)

3 Drive by Download 攻撃の対象はやはり企業に集中(図表 3.1、3.2)

依然として続く企業ウェブサイトの改ざん

「Gumblar」に代表される「Drive by Download タイプの攻撃」は、依然として「企業のウェブサイト」に狙いを定めています。2010年1月に「Drive by Download タイプの攻撃」により、大量の「企業ウェブサイト」が改ざん被害を受けました。1年が経過した現在でも攻撃は継続し、さらに被害は拡大していると言えます。

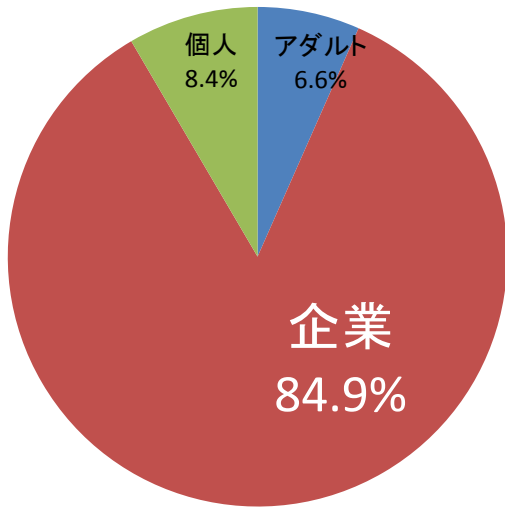
「不正改ざんサイト」サイトの中から、「Drive by Download サイト」について調査を行ったところ、「企業のウェブサイト」が全体の84.9%を占めました。(図 3.1)

「不正改ざんサイト」全体における、企業サイトが占める割合は62.5%(図表 2.1)ですので、「Drive by Download サイト」の攻撃対象として「企業のウェブサイト」が集中的に狙われている事が分かります。

また、この数値は2010年1月に確認された「Gumblar 被害サイトの内訳(2010年1月)」と比較しても9.0%上昇しています。企業のウェブサイト管理者は、自社ウェブサイトのセキュリティ対策についてより注意深く、また包括的に実施する必要があります。

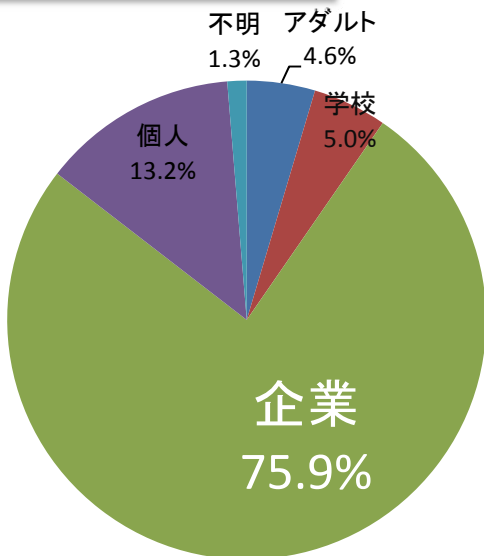
図表 3.1.

Drive by Downloadサイトの内訳(2011年1月)



図表 3.2.

Gumblar被害サイトの内訳(2010年1月)



※セキュアブレイン gred セキュリティレポート Vol.7【2010年1月分統計】「数値で見る Gumblar(ガンブラー)ウイルスの被害」より抜粋。

4 「ショート URL」にご注意ください。

「不正攻撃サイト」報告の 14.3%は「ショート URL」

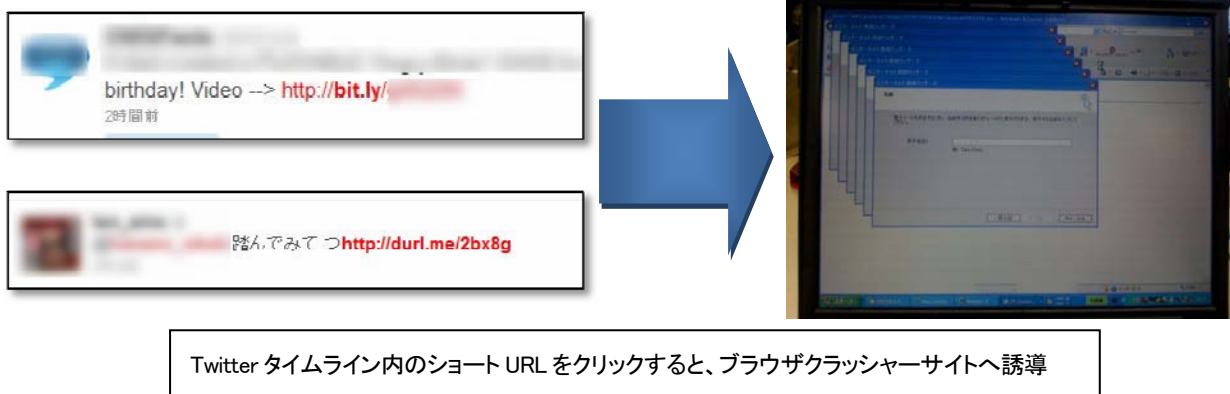
ショート URL は、書き込み可能文字数に制限のある「Twitter」のような掲示板で、「URL 情報」を紹介する際に利用するサービスです。最近では、その他の掲示板においても「ショート URL」を使用して「URL 情報」が書き込まれるケースが増加しています。

【ショート URL の例】



「ショート URL」の利便性が高い反面、「本当の URL 文字列」が分からない為、「危険なウェブサイト」に誘導する攻撃に悪用される恐れが指摘されています。

【ショート URL を悪用した攻撃例】



「不正攻撃サイト」の報告について URL を確認したところ、694 件の報告中 99 件 (14.3%) がショート URL による報告でした。インターネットユーザは「ショート URL」で作成されたリンクをクリックする際は注意が必要です。

クリックする前に「gred でチェック」でリンクを無料チェック

株式会社セキュアブレインが提供する、無料のウェブサイトの検査サービス「gred でチェック」(<http://gred.jp>)は「ショート URL」にも対応しています。「Twitter」「Facebook」「mixi」等の掲示板に記載されている「ショート URL」をクリックする前に、「gred でチェック」(<http://gred.jp>)でリンク先の URL の安全性を確認することをお勧めします。

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.sagwall.jp/index.html>)も提供しています。危険なウ

ウェブサイトを開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 東京都千代田区麴町 2-6-7 麴町 RKビル 4F