

2010 年 3 月 24 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.8【2010 年 2 月分統計】

依然として続く、企業ウェブサイトの改ざん被害。

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。

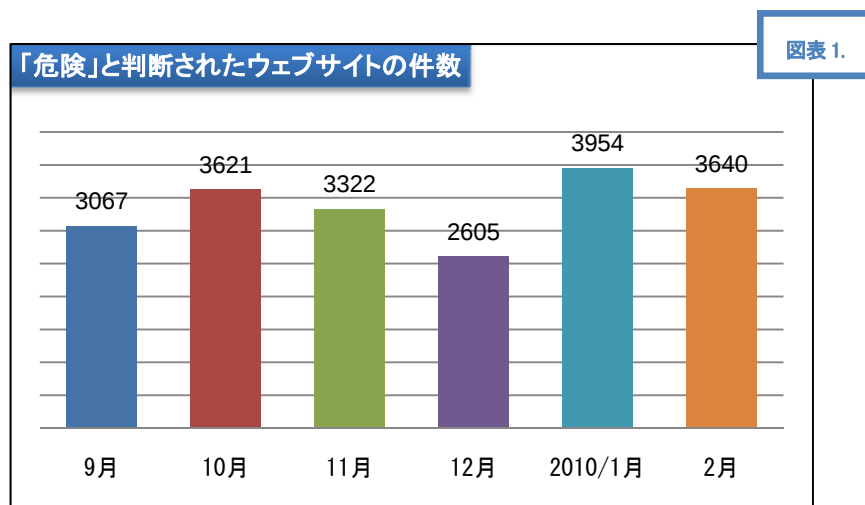
本レポートに含まれる内容

内容

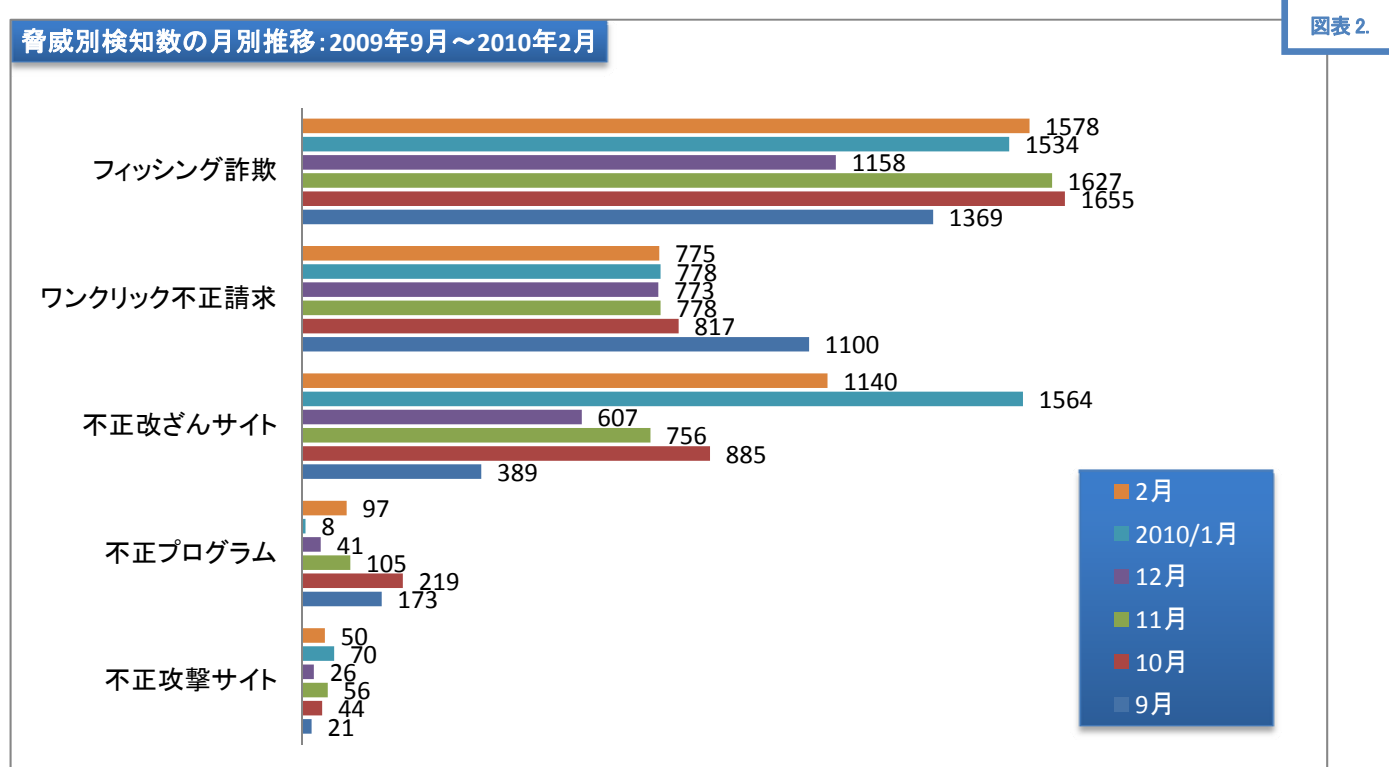
本レポートに含まれる内容	1
1 gred セキュリティレポート概要	2
1.1 「危険」と判断されたウェブサイトの数(2010 年 2 月):3,640 件(図表 1)	2
1.2 「gred でチェック」で検知した脅威の月毎の推移(脅威別)(図表 2)(単位:件)	2
1.3 「gred でチェック」月別総利用数(2009/10 月~2010/2 月)	2
1.4 「gred でチェック」のチェック結果に表示される脅威の説明	3
2 企業ウェブサイトの改ざん被害はさらに深刻度を増す	3
2.1 依然として続く、企業ウェブサイトへの攻撃	3
・ 数値で見る「ウェブサイト改ざん被害」(図表 3-1、3-2、3-3)	3
2.2 管理者は FTP アカウントの整理や運用ルールの整備が急務	4
3 大手日本語検索サイトのフィッシングサイトが急増	5
4 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
4.1 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
4.2 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（2010 年 2 月）：3,640 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（2009/10 月～2010/2 月）

月	2009/10 月	11 月	12 月	2010/1 月	2 月
「gred でチェック」 総利用数	39,569	39,330	40,697	70,999	55,927

- 「危険」と判断されたウェブサイトの件数は、3,640 件（前月比 92.1%）（図表 1 参照）
- 「不正改ざんサイト」の検知数は、前月より減少していますが、依然として高い数値を示しています。
- 2010 年 1 月の統計情報は、大手企業のウェブサイト改ざんの報道もあり、「gred でチェックの利用数」、「危険と判断された

ウェブサイトの件数」共に、過去最高でした。2010 年 2 月の統計では、前月よりは減少しているものの、多くの統計数値で、依然として高い数値が示されています。

- フィッシング詐欺の検知数が、2010 年 1 月から引き続き上昇傾向にあります。

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

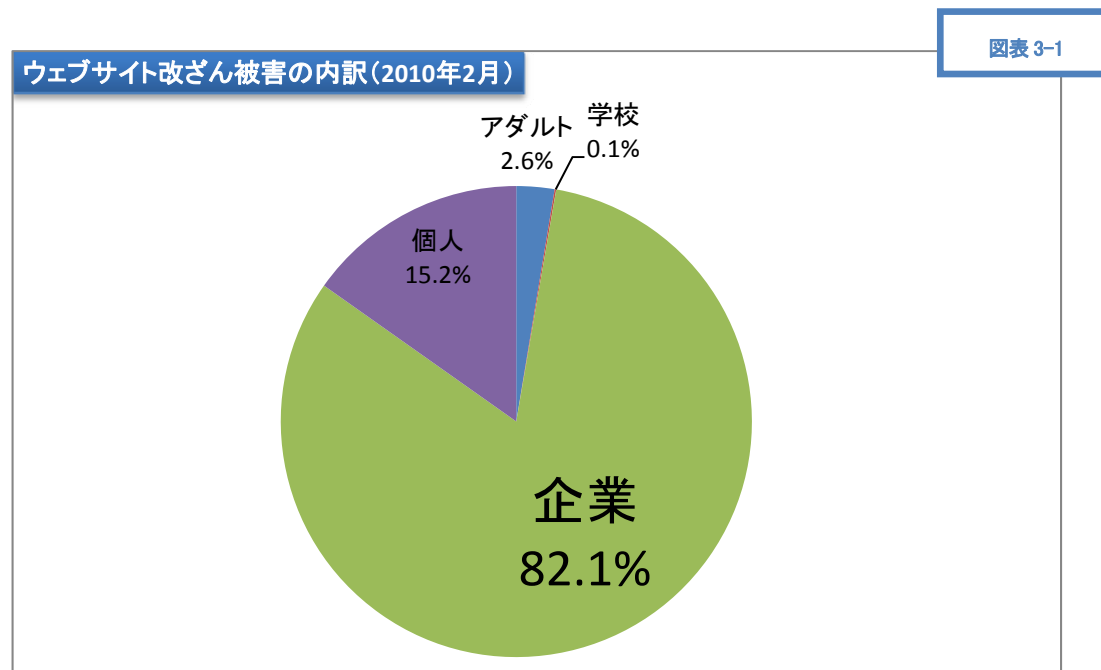
表示される脅威の名称	説明
フィッシング詐欺	本物そっくり、偽造されたウェブサイトです。ユーザの ID や、パスワード等の個人情報を不正に取得します。
ワンクリック不正請求	ウェブサイト上のボタン等をクリックしただけで、契約が成立したように見せかけ、料金を不当に請求する詐欺を行っているウェブサイトです。
偽ソフトウェア(不正プログラム)	不当に料金を請求する、実際には機能しない、偽物のソフトウェアを配布しているウェブサイトです。
不正攻撃サイト	他のコンピュータに存在する脆弱性を突いて、攻撃を行うことを目的として作成されたウェブサイトです。
不正改ざんサイト	攻撃者によって、不正に改ざんされて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 企業ウェブサイトの改ざん被害はさらに深刻度を増す

2.1 依然として続く、企業ウェブサイトへの攻撃

2010 年初頭から、「法人系ウェブサイト改ざん」の検知報告が急激に増加しました。2010 年 2 月に「gred でチェック」で「危険」と判断されたウェブサイトの数 3,640 件中、「不正改ざんサイト」の検知件数は 1,140 件(31.3%)、「Gumblar(ガンブラー)等の不正プログラムが関連した、ウェブサイトの改ざん被害」(以下「ウェブサイト改ざん被害」は、921 件(「不正改ざんサイト」報告件数の 80.8%、「危険」と判断されたウェブサイトの 25.3%)です。

- 数値で見る「ウェブサイト改ざん被害」(図表 3-1、3-2、3-3)

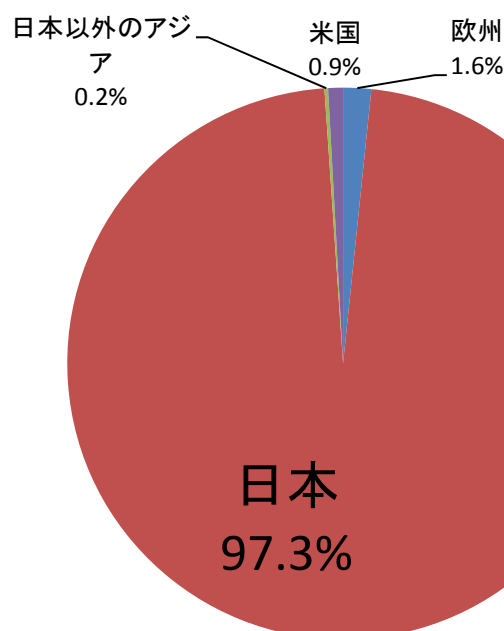


図表 3-2

	2010 年 2 月	2010 年 1 月	2009 年 12 月	2009 年 10 月
「危険」と判断されたウェブサイトにも占める「改ざん被害サイト」の割合	25.3% (921 件/3,640 件)	31.6% (1,248 件/3,954 件)	12.9% (336 件/2,605 件)	15.5% (562 件/3,621 件)
「不正改ざんサイト」の検知件数に占める「改ざん被害サイト」の割合	80.8% (921 件/1,140 件)	79.8% (1,248 件/1,564 件)	55.4% (336 件/607 件)	63.2% (562 件/889 件)
「改ざん被害サイト」の中で、「企業ウェブサイト」が占める割合	82.1% (756 件/921 件)	80.9% (1,009 件/1,248 件)	60.7% (204 件/336 件)	53.2% (299 件/562 件)

図表 3-3

改ざん被害サイトに使用されていた言語(2010年2月)



2.2 管理者はFTP アカウントの整理や運用ルールの整備が急務

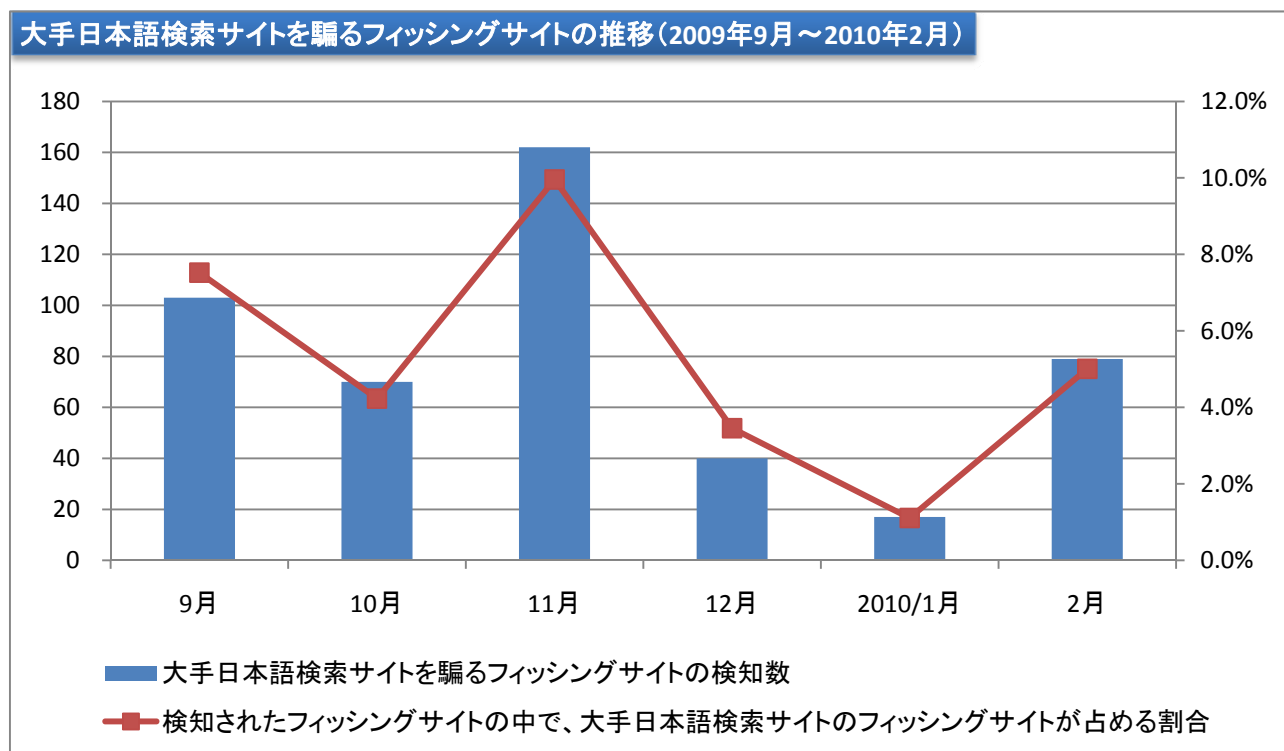
2010 年 2 月の統計では、前月同様「企業のウェブサイト」が「改ざん被害サイト」の大勢を占めています。検知数は減少していますが、割合としては上昇しており、「ウェブサイト改ざん」の対象が「企業ウェブサイト」中心であることが考えられます。また、ウェブサイトが使用している言語で「日本語」が占める割合も、前月と比較して 1 ポイントほど上昇しています。

インターネットユーザが「改ざん被害サイト」に遭遇する確率は、より一層高くなっています。「改ざん被害サイト」に遭遇したパソコンに脆弱性が存在する場合、Gumblar 等の不正プログラムに感染し、FTP の ID やパスワードの漏えい等の情報漏えいを引き起こします。その為、「改ざん被害サイト」の増加に比例して、不正プログラム感染被害を受けるパソコンが増加し、さらに「企業ウェブサイトの改ざん」増加に繋がるという構図が生まれています。

ウェブサイトのコンテンツ更新等の管理に一般的に使用されている「FTP」ですが、企業内で使用されていないアカウント、必要無い人に発行されているアカウントの有無の確認を行うと共に、ルールに基づいた運用が行われているか(または、運用ルールそのものが定められているか)を確認してください。

3 大手日本語検索サイトのフィッシングサイトが急増

2010年2月の統計では、フィッシングサイト検知数に占める「大手日本語検索サイトを騙ったフィッシングサイト」の割合が増加傾向にあります。フィッシングサイトの出現には「フィッシングメールの配信数や内容」「作成するフィッシングサイトの数」の要素が関係すると同時に、使用されるドメインやIPアドレスにも一貫性が見られず、いつ、どれくらいの数のフィッシングサイトが発生するかを予測することが困難です。



今後も「大手日本語検索サイトを騙るフィッシングサイト」の出現は継続されると思われます。フィッシングサイトによる個人情報漏えいの対策として、以下の点に注意してください。

- **知らない人からの、不審な電子メールには注意**

知らない人からのメールや不審なタイトルのメールには、注意してください。また、メールを開いてしまった場合でも、フィッシングメール等に含まれるURLリンクをクリックしないでください。本物のWebサイトに接続するように見せかけてフィッシングサイトに誘導します。頻繁に利用するWebサイトは、お気に入りや登録するなどして利用することをお勧めします。

- **WebサイトのURLや証明書を確認**

ブラウザに表示された内容だけでなく、「アドレスバーに表示されるURL」についても確認してください。本来のものとは異なるURLが表示されている場合には、そのウェブサイトの閲覧を中止する、または当該ウェブサイトの管理者や問い合わせ窓口へ、電話やメールで問い合わせをすることをお勧めします。また、多くの企業では、自社Webサイトの正当性を証明する「証明書」を導入しています。詳細については各企業のWebサイトで確認してください。

- **セキュリティ対策ソフトの導入**

フィッシングメールやフィッシングサイトを検知する機能を持ったセキュリティ対策ソフトを使用してください。

4 個人・企業それぞれに求められる、セキュリティ対策とは？

4.1 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、無料でご利用いただけるウェブセキュリティサービス「gred でチェック」(<http://www.gred.jp>)を提供し

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検知する「Internet SagiWall」(<http://www.securebrain.co.jp/products/sagwall/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/sagwall/index.html>

■「gred AV アクセラレータ」URL

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

4.2 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」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