PRESS RELEASE

2011 年 3 月 30 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.20【2011 年 2 月分統計】

－ 災害に関するチェーンメール、フィッシング詐欺が増加傾向。ご注意ください！ －

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。

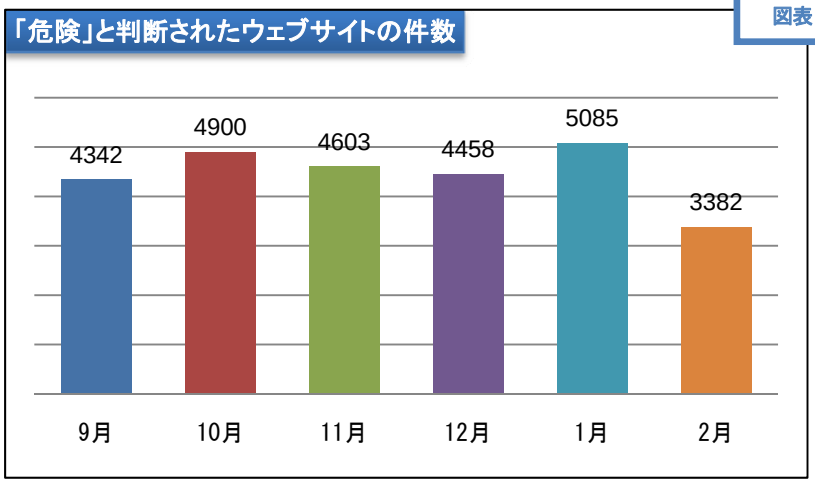
株式会社セキュアブレイン(本社：東京都千代田区、代表取締役社長 兼 CEO：成田 明彦、以下「セキュアブレイン」)はセキュアブレインが運用する、無料のウェブセキュリティサービス「gred（グレッド）でチェック」で収集した情報を基に、「セキュアブレイン先端技術研究所」（以下 先端技術研究所）で分析を行い、その結果を「セキュアブレイン gred セキュリティレポート」として公表します。「gred でチェック」は、インターネットユーザがウェブサイトの安全確認を行うことができる、無料のウェブセキュリティサービスです。確認したいウェブサイトの URL を入力するだけで、セキュアブレインが独自に開発した解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

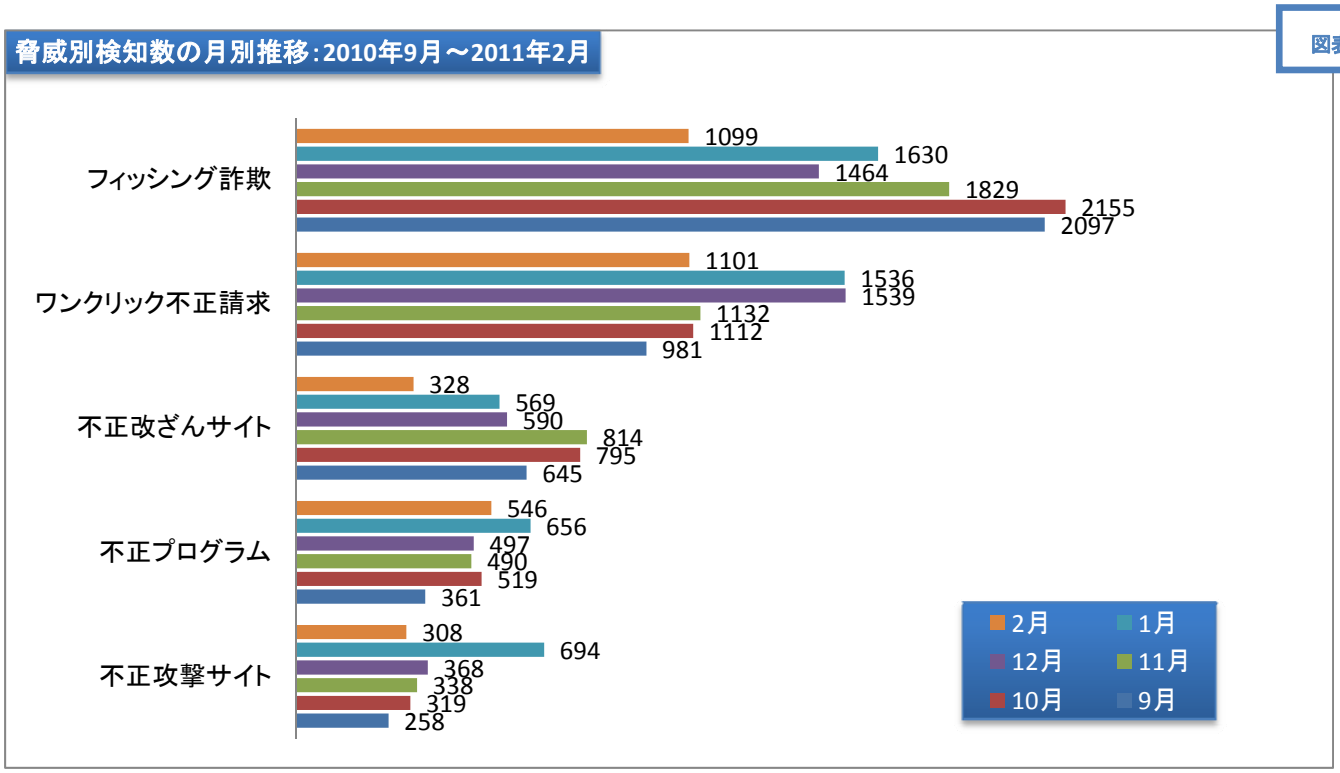
- 「危険」と判断されたウェブサイトの数（図表 1.1.）

図表 1.1



- 「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.



- 「gred でチェック」月別総利用数（図表 1.3.）

図表 1.3.

月	9 月	10 月	11 月	12 月	2011/1 月	2011/2 月
「gred でチェック」総利用数	49,565	49,720	44,901	43,060	46,034	37,106

- 「危険」と判断されたウェブサイトの件数は、3,382 件。（前月比 66.5%、図表 1.1.）

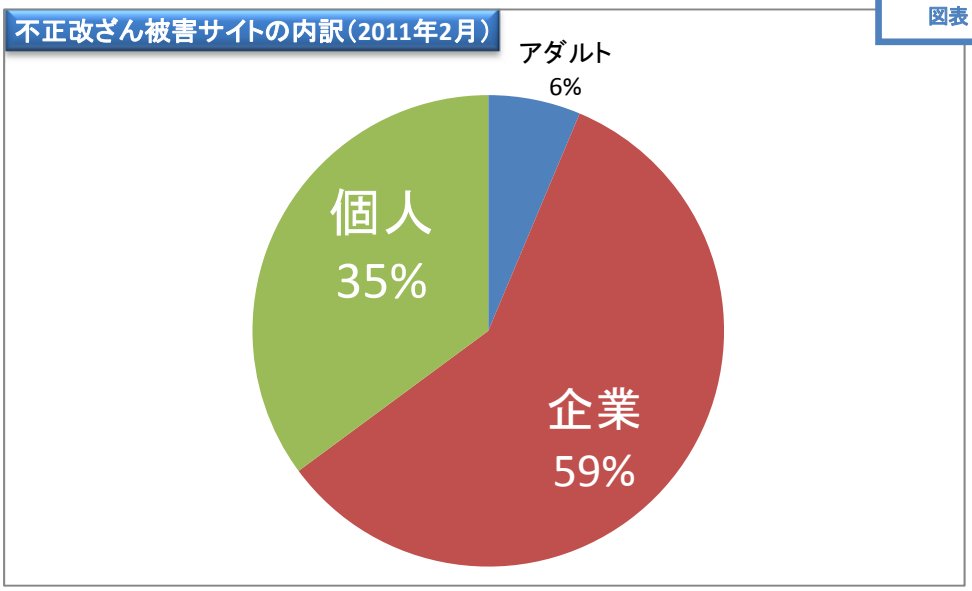
「gred でチェック」のチェック結果に表示される脅威の説明

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.

	2011 年 2 月	2011 年 1 月	2010 年 12 月	2010 年 11 月	2010 年 10 月	2010 年 9 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	**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）	5.2% （226 件/4342 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	**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）	35.0% （226 件/645 件）

3　東北地方太平洋沖地震に関するデマ情報にご注意ください

- 地震の翌日から出現したチェーンメールや悪質なウェブサイト

3 月 11 日以降、以下のチェーンメール、フィッシング詐欺サイト、偽情報が確認されており、セキュアブレインでは随時注意喚起を行っていますが、このレポートではそれらの情報を整理してお伝えします。

悪質なウェブサイトは今後も増える可能性がある為、インターネットを利用した情報収集には注意が必要です。

チェーンメールの実例

- 「コスモ石油工場爆発」に関するチェーンメール
  - 地震発生後の翌日に確認されました。文面は以下の様なものでした。

    ======以下、文面======

    コスモ石油工場勤の方から情報。

    外出に注意して、肌を露出しないようにしてくださ い！

    コスモ石油の爆発により有害物質が雲などに付着し、雨などといっしょに降るので

    外出の際は傘かカッパなどを持ち歩き、身体が雨に接触しないようにして下さい！！

    皆さんに知らせてください！！

    多くの人に回してください！！

    ======以上==========

- 原子力発電所の事故に関するチェーンメール
  - 事故により危険性が懸念されている「放射性物質」に関する情報と、対処法についての不確かな情報が記載されています。

    ======以下、文面======

    福島原発からの流れ始めた放射性物質、こちらへも影響があります。

    関東の方へ、風向きが今は西風、ときどき北風。北風だと飛ぶ。ヨウ素が主体の放射能、幼児は対処が必要。

    ★風向きに直角に逃げるのが一番。ほんの数日（雨が降らなければ、雨なら3か月）離れればいい。

    ★今日から流し始めた放射能なので明日の外出は避けて下さい！

    NHK ラジオでは，10km 圏内の被曝線量は 20-50mSv（ミリシーベルト）になると保安院ら試算していることを伝えている．これは，一般人の年間の制限値である 1mSv の 20-50 倍に達する．

    首都圏に飛んでくる放射能で、特に症状が出やすいのは、放射性ヨウ素による甲状腺異常です。

    体内に取り込むヨウ素は、一定量以上になると蓄積できずに排泄されるので、それを利用して放射性ヨウ素の被害を避けることが出来ます。

    もちろん、第一の対策は防塵マスクで放射能を体内に入れないことで、これが最も重要です。

    放射能の危険が迫ったら、間に合うようにヨウ素をとれば有効です。服用のタイミングは、放射能に襲われる直前がベスト。被ばく後でも 3 時間後で 50%の効果があるとされています。

    「食品で取るならトロロ昆布」

    食品でヨウ素をとるなら、副作用の心配はありません。特に多くヨウ素を含む食品は昆布で、ワカメの 4 倍くらい多く含んでいます。

    原発で事故が起こったと知ったら、食べやすいトロロ昆布などを多めに食べるのが、無理のない、健康的な対策です。

    ★トロロ昆布は、乾いたまま一度にたくさん食べると腸内で膨張して危険なので、お吸い物などに入れて食べましょう。

    ※万が一の時にはまず、防塵マスク、ぬれタオル・ハンカチで口鼻を覆って、吸い込まないように。

    ======以上==========

電力不足に関するチェーンメール

- 電力会社からの情報を騙り、情報の拡散を求めています。

  ======以下、文面======

  ■お願い■

  関西電力で働いている友達からのお願いなのですが、本日 18 時以降関東の電気の備蓄が底をつくらしく、中部電力や関西電力からも送電を行うらしいです。

  一人が少しの節電をするだけで、関東の方の携帯が充電を出来て情報を得たり、病院にいる方が医療機器を使えるようになり救われます！

  こんなことくらいしか関西に住む僕たちには、祈る以外の行動として出来ないです！

  このメールをできるだけ多くの方に送信をお願い致します！

  返信はいりません

  ======以上==========

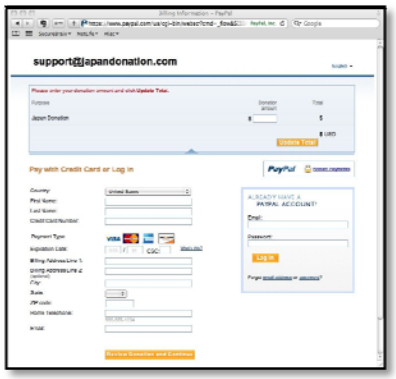
フィッシング詐欺サイトの実例

■ 義援金を募るフィッシング詐欺サイト

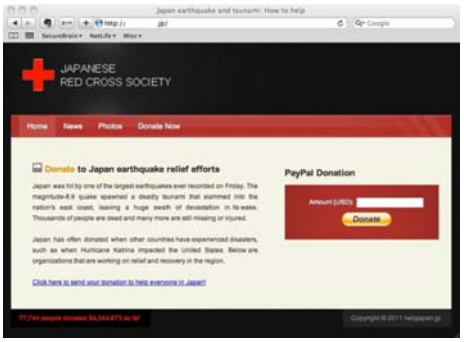
- 「Japan Donation」を名乗る英語のフィッシング詐欺サイトが確認されました。

  個人情報の入力画面

クレジットカード番号等の入力画面（オンライン決済サービスの大手である米国 Paypal を利用して支払いを行っています。）



■ 日本赤十字を騙ったフィッシング詐欺



日本赤十字社からも注意喚起が行われています。

http://www.jrc.or.jp/oshirase/l3/Vcms3_00002080.html

義援金や寄付金は、必ず信頼できるサイトを使うように注意してください。

偽情報、迷惑メールの実例

■ 原子力発電所の事故に関する偽情報

● 事故により漏れた放射能が 6 日～10 日間かけて、米国に到達するという偽の情報がインターネット上で確認されました。

Australian Radiation Services 社のロゴも入っているため、正式に発行した物に見えますが、Australian Radiation Services 社のウェブサイトでも注意喚起をも行われています。

http://www.australian-radiation-services.com.au

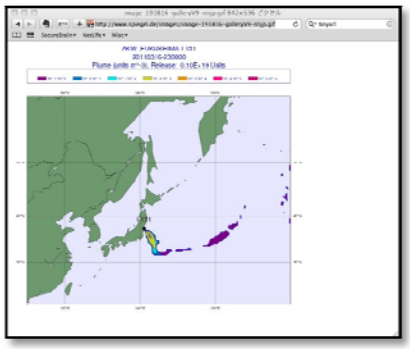
● Twitter 上で確認された「放射能の影響に関する紛らわしい情報」

==========以下文面==========

以下の様な Twitt を見たんだけど。RT ドイツが出したらしい、福島第一原発の放射能汚染シミュレーション http://bit.ly/xxxI1h

========== 以上 ==========

リンク先は、インパクトのある放射能汚染シミュレーション動画です。そのため、実際に放射能が流れている物ではありません。あくまでも、シミュレーションであり確かな情報ではありません。



このような情報に惑わされないようにしてください。必要以上の「リツイート」や「情報の転送」を行うことは、情報の錯綜を招きますので注意が必要です。

- ■ 緊急地震速報（エリアメール）を騙った悪質な迷惑メール
  - NTTドコモが緊急地震速報（エリアメール）を騙った悪質なメールに対して注意喚起を実施してます。
    NTTドコモの注意喚起：http://www.nttdocomo.co.jp/info/notice/page/110315_00_m.html

4　チェーンメール、フィッシング詐欺サイト、偽情報への対策について

- チェーンメールの特徴と対処方法について
  - チェーンメールには以下のような特徴があります。
    1. 天災、事故等に関連した、心配する内容を警告している。
    2. 情報の発信元が、電力会社や原子力発電所の職員等の関係者であることが記されている。
    3. 「皆さんに知らせてください。 」「多くの人に回してください」のような、告知の協力を求める文面が記載されている。

上記の様な要素が含まれた電子メールを受け取った場合、情報の告知協力を行う前に、関連する情報をインターネットで調べてください。

- フィッシング詐欺サイトへの対処方法について
  - 不審な電子メールに記載されている、URLリンクのクリックをしないでください。
  - セキュリティ対策を行ってください。
  - 義援金や寄付金は、必ず信頼できるサイトを使うように注意してください。

5　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