PRESS RELEASE

2010 年 5 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.10【2010 年 4 月分統計】

不正改ざんサイトの内訳に変化。より多くの個人ユーザが攻撃対象になる可能性。

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。

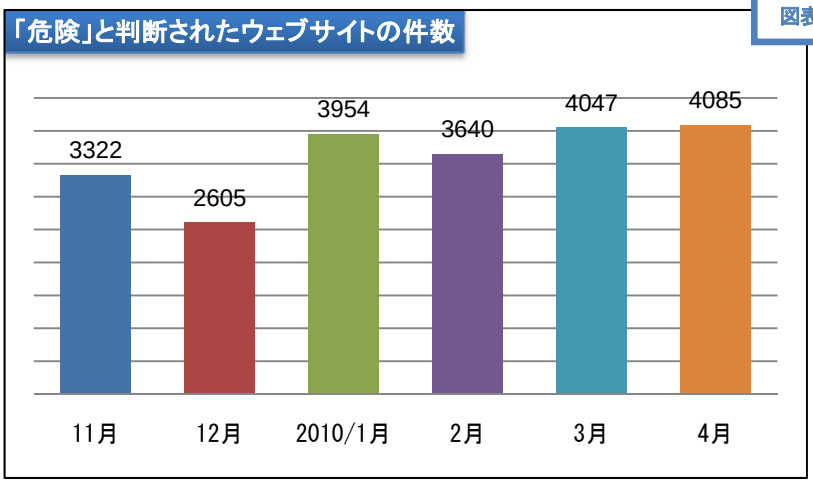
本レポートに含まれる内容

内容

1　gred セキュリティレポート概要

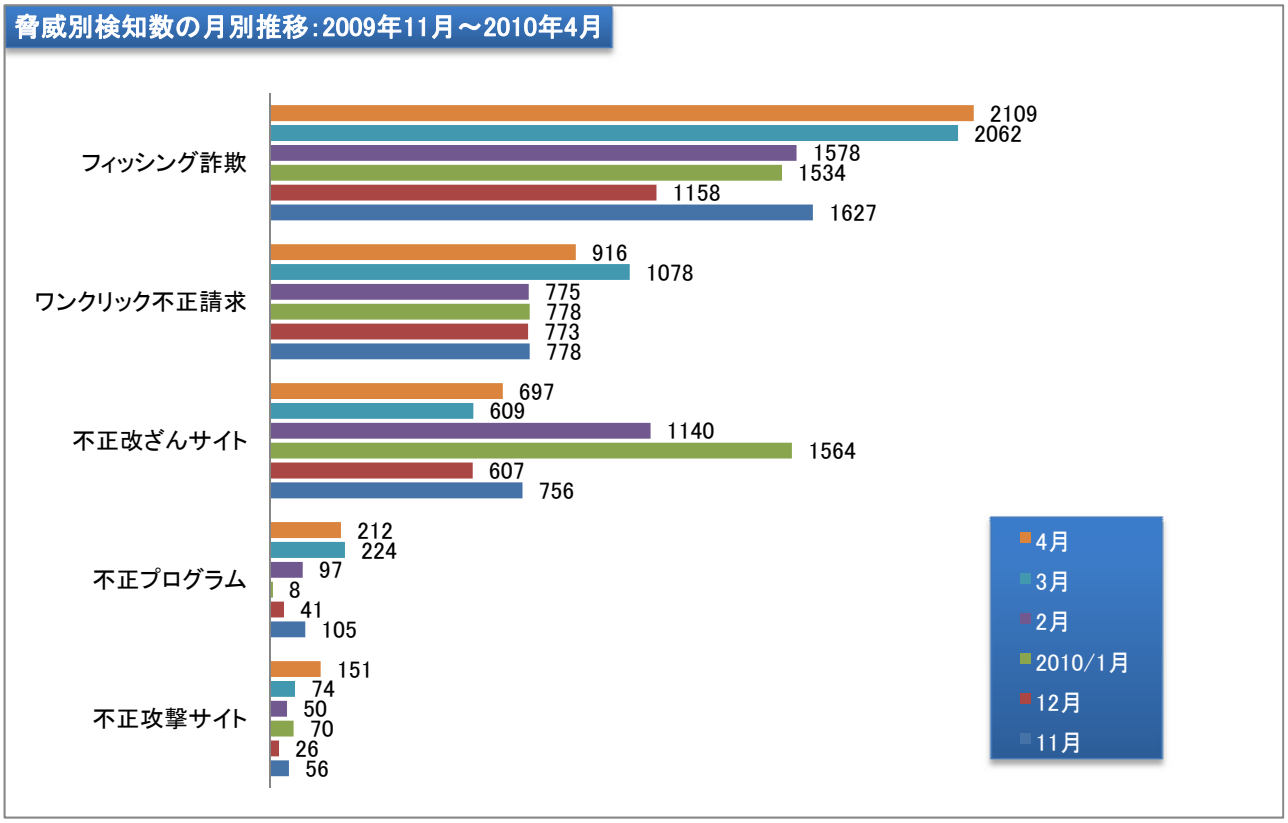
1.1　「危険」と判断されたウェブサイトの数（2010 年 4 月）：4.085 件（図表 1）

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）

図表 2.



1.3　「gred でチェック」月別総利用数（2009/11 月～2010/4 月）

月	11 月	12 月	2010/1 月	2 月	3 月	4 月
「gred でチェック」総利用数	39,330	40,697	70,999	55,927	54,995	55,025

- 「危険」と判断されたウェブサイトの件数は、4,085 件（前月比 100.9%、図表 1）。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
- 「不正攻撃サイト」は前月より増加しています。（前月比　204.1%）
- 「フィッシング詐欺」の検知数が、前月に続き、今月も増加しました。2010 年 4 月の検知数 2,109 件（前月比 102.3%）は統計開始後の最高値です。

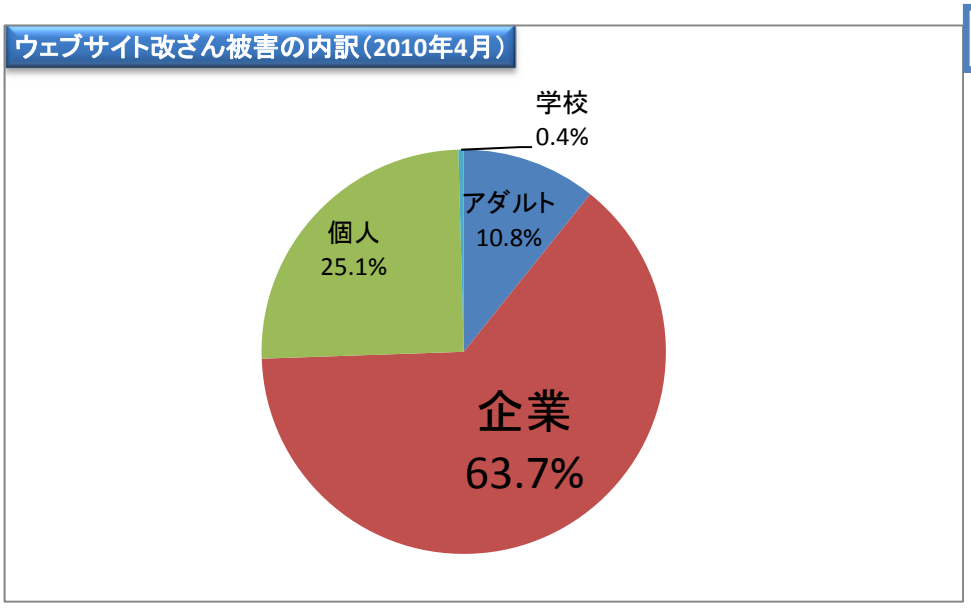
1.4　「gred でチェック」のチェック結果に表示される脅威の説明

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　「ウェブ改ざん」被害は前月に引き続き減少傾向

- 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 3-1

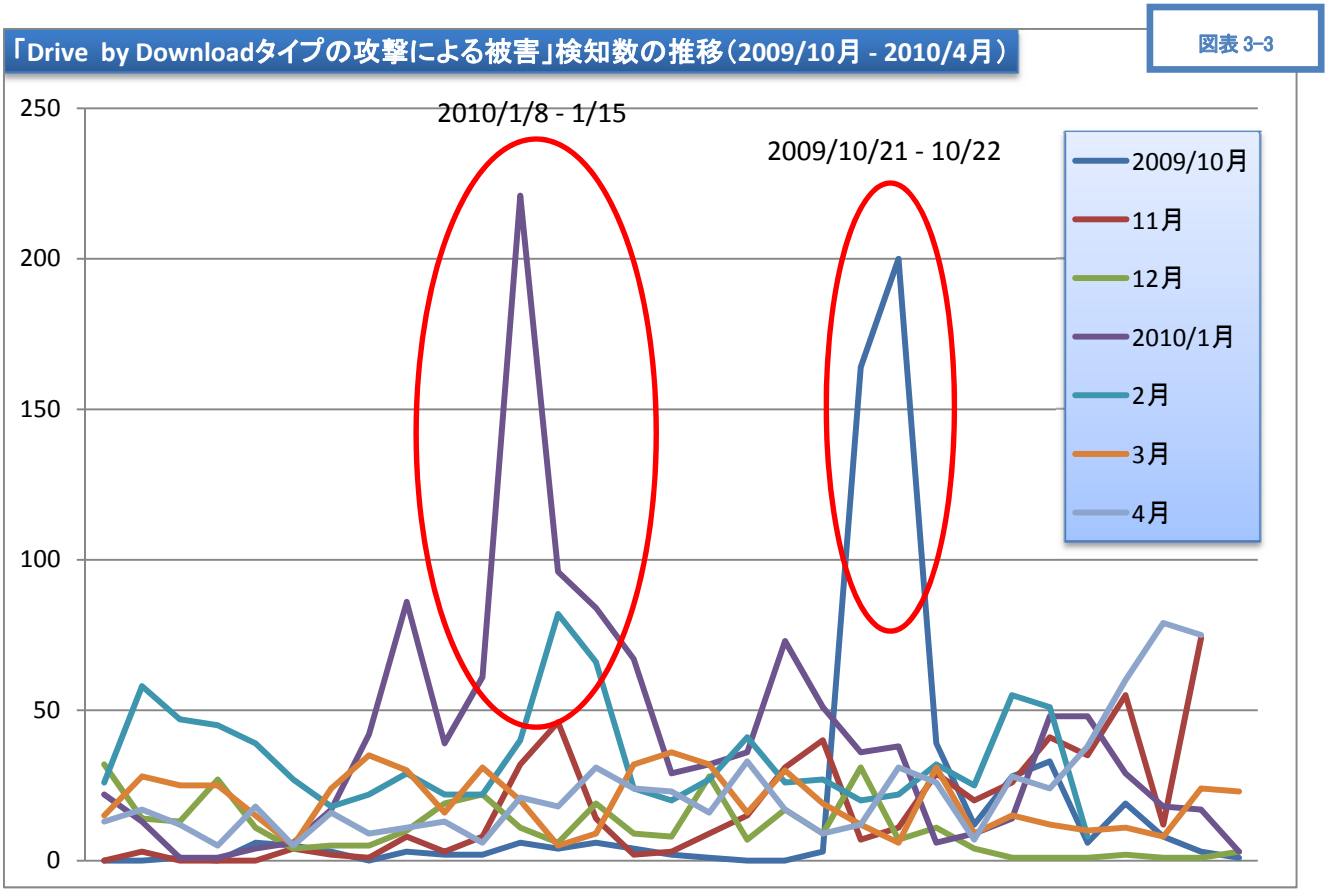


図表 3-2

	2010 年 4 月	2010 年 3 月	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占める「Drive by Download タイプの攻撃」の割合	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)	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「Drive by Download タイプの攻撃」の割合	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)	55.4% (336 件/607 件)	63.2% (562 件/889 件)
「Drive by Download タイプの攻撃」の中で、「企業ウエブサイト」が占める割合	74.6% (293 件/393 件)	76.2% (345 件/453 件)	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)

- 「Drive by Download タイプの攻撃」に関する数値は減少していますが、「ウェブサイトの不正改ざん」における攻撃手法の主役は、「Drive by Download タイプの攻撃」であることに変わりはありません。この攻撃は、自社のウェブサイトの改ざんにとどまらず、顧客や取引先、また自社のウェブサイトを閲覧したユーザへ被害が拡大します。その為、その修復に要する人員、時間、コストは図りしれません。また、この攻撃は、「セキュリティソフトによる検知が難しい」という特徴も併せ持っています。

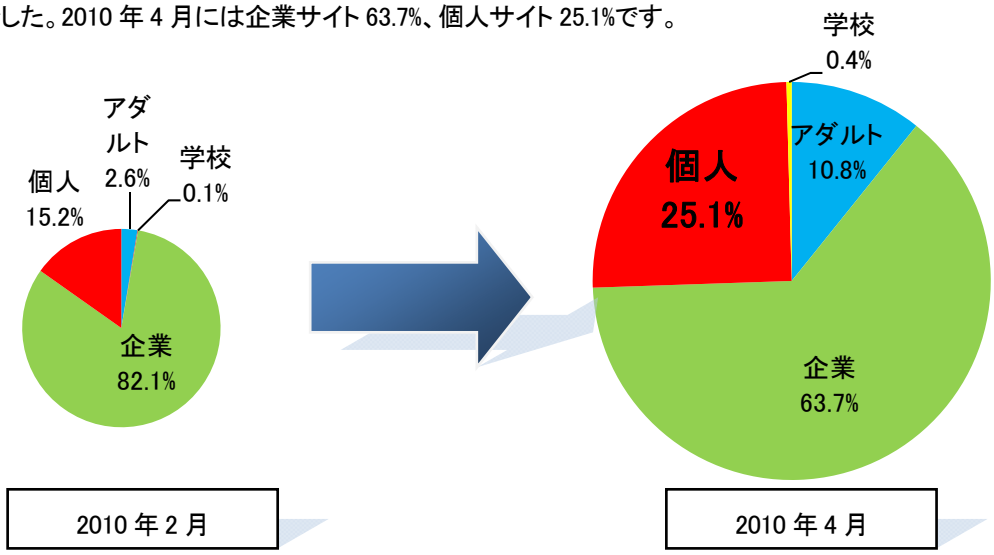
図表 3-3



- 「Drive by Download タイプの攻撃」による被害の検知数の増減を示しています。発生のピークの規模にばらつきがありますが、その発生時期についても周期性は確認できません。

2.1　「不正改ざんサイト」の内訳に変化、個人のブログが標的に

- 「不正改ざんサイト」の被害サイトの内訳にも変化が生じています。2010 年 2 月の時点では、企業サイト 82.1%、個人サイト 15.2%でした。2010 年 4 月には企業サイト 63.7%、個人サイト 25.1%です。



- 4 月に収集した「不正改ざんサイト」の情報を基に、各ウェブサイトのコンテンツについて調査を行ったところ、企業のウェブサイトでは、特に定まった傾向はありませんが、個人のウェブサイトでは 90%以上が「ブログ」でした。
  「平成 21 年版　情報通信白書（総務省）」によれば、インターネットの利用目的として「ブログの閲覧」をあげた人は、全体の 56.8%でした。
  2009 年 1 月末時点における、ブログの登録者数は約 2,695 万人。月間の閲覧数は約 205 億 PV です。（ブログ・SNS の経済効果の推計　平成 21 年 7 月　総務省　情報通信政策研究所）つまり、約 5 人に 1 人はブログを持っている計算になります。また 1 日に読まれているページ数は約 6 億ページになる計算です。
  個人が運営するブログでは、企業サイトほどのセキュリティ対策は行われていません。その為、改ざんに気がつかない。また、改ざんされたことが分かっても、修正方法が分からない為に放置してしまう。このようなことからを改ざんすることで、より多くのユーザに攻撃を行うことが可能です。攻撃を行う側がより多くの個人を攻撃対象としている可能性が伺えます。
  今後とも「不正改ざんサイト」の攻撃方法、攻撃対象の変化には注意を払う必要があります。

3　ワンクリック不正請求サイトでは、不正プログラムにも注意

3.1　ムービー再生ソフトを装ったプログラム。実は「ワンクリウェア」

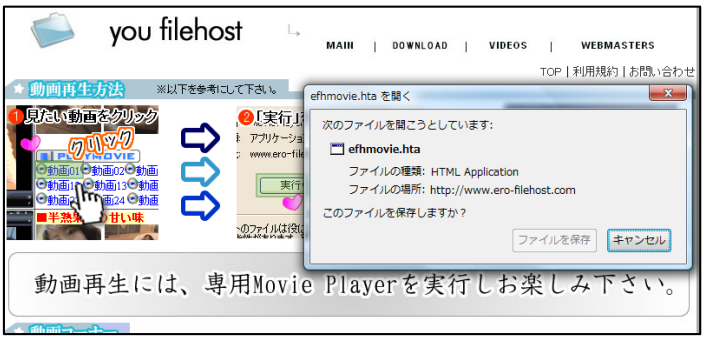
- 「ワンクリック不正請求サイト」は必ずしも、画面に「脅迫文章」を表示するだけではありません。ムービー再生ソフトを装った不正プログラムをダウンロードさせることで、パソコンの設定を変え、ブラウザが起動する度に「不正請求の画面」を表示させます。

■「ワンクリウェア」感染例

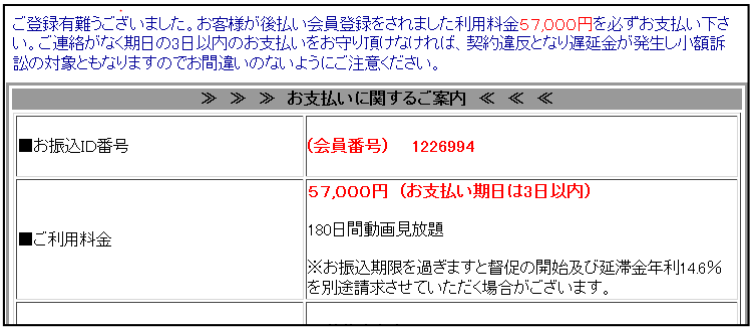
1. 「ワンクリック不正請求サイト」に多くみられる確認画面

2. 「専用の再生ソフト」が必要なことを伝える画面

3. ファイル（xxxx.hta）のダウンロード



4. 手順に従ってファイルを保存・実行してしまうとブラウザ起動時に不正請求画面が表示されます



ご登録有難うございました。お客様が後払い会員登録をされました利用料金57,000円を必ずお支払い下さい。ご連絡がなく期日の3日以内のお支払いをお守り頂けなければ、契約違反となり遅延金が発生し小額訴訟の対象ともなりますのでお間違いのないようにご注意ください。

≫ ≫ ≫ お支払いに関するご案内 ≪ ≪ ≪

■お振込ID番号	(会員番号)　1226994
■ご利用料金	57,000円 (お支払い期日は3日以内) 180日間動画見放題 ※お振込期限を過ぎますと督促の開始及び延滞金年利14.6%を別途請求させていただく場合がございます。

従来の「ワンクリウェア」では拡張子が「EXE」の実行ファイルが多くを占めていましたが、昨年から「HTA」タイプのものが増加しています。「HTA」は HTML 言語を利用してプログラムの作成することが可能です。この技術を悪用し、ブラウザが起動したときに「不正請求の画面」を出し続けます。

これらのプラグラムが一度実行されてしまうと、アンインストールや、設定を変更することは困難です。最悪の場合、OS の再インストールが必要な場合もあります。安易にソフトウェアのインストールを行うことは絶対に避けてください。

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、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

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」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