Press Release

2010 年 11 月 29 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.16【2010 年 10 月分統計】

特定のホスティング会社で集中的に改ざんサイトを検知。攻撃者の準備行動か？
フィッシング詐欺のお手伝い？騙し取ったお金の運び屋「Mule（ミュール）」とは？

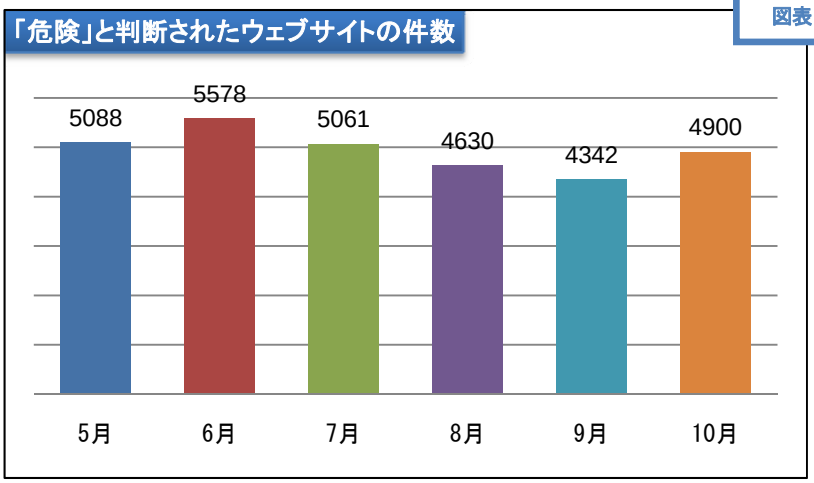
株式会社セキュアブレイン(本社：東京都千代田区、代表取締役社長 兼 CEO：成田 明彦、以下「セキュアブレイン」)はセキュアブレインが運用する、無料のウェブセキュリティサービス「gred（グレッド）でチェック」で収集した情報を基に、「セキュアブレイン先端技術研究所」（以下 先端技術研究所）で分析を行い、その結果を「セキュアブレイン gred セキュリティレポート」として公表します。「gred でチェック」は、インターネットユーザがウェブサイトの安全確認を行うことができる、無料のウェブセキュリティサービスです。確認したいウェブサイトの URL を入力するだけで、セキュアブレインが独自に開発した解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

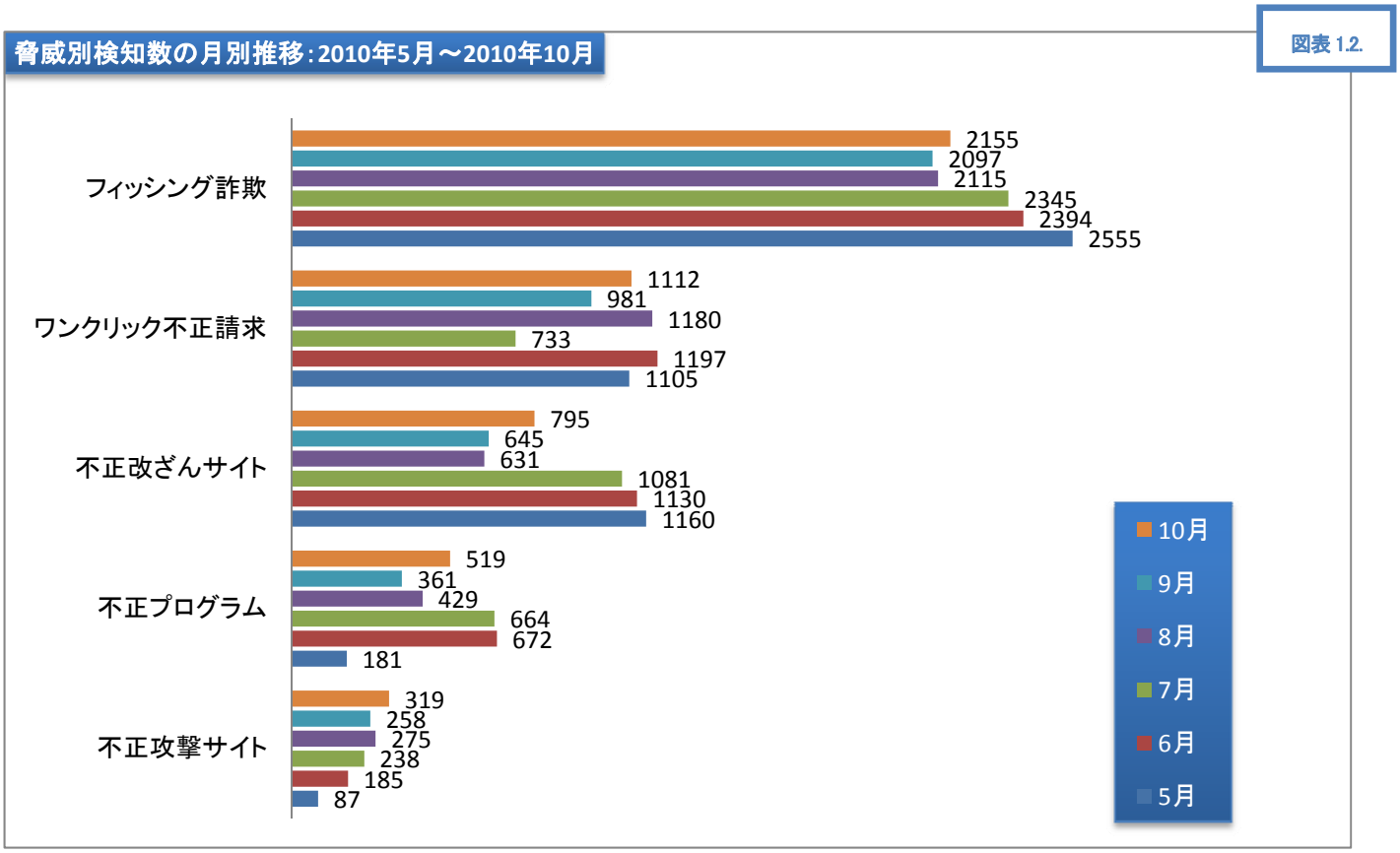
1.1　「危険」と判断されたウェブサイトの数（図表 1.1.）

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	5 月	6 月	7 月	8 月	9 月	10 月
「gred でチェック」総利用数	58,365	57,346	56,419	49,669	49,565	49,720

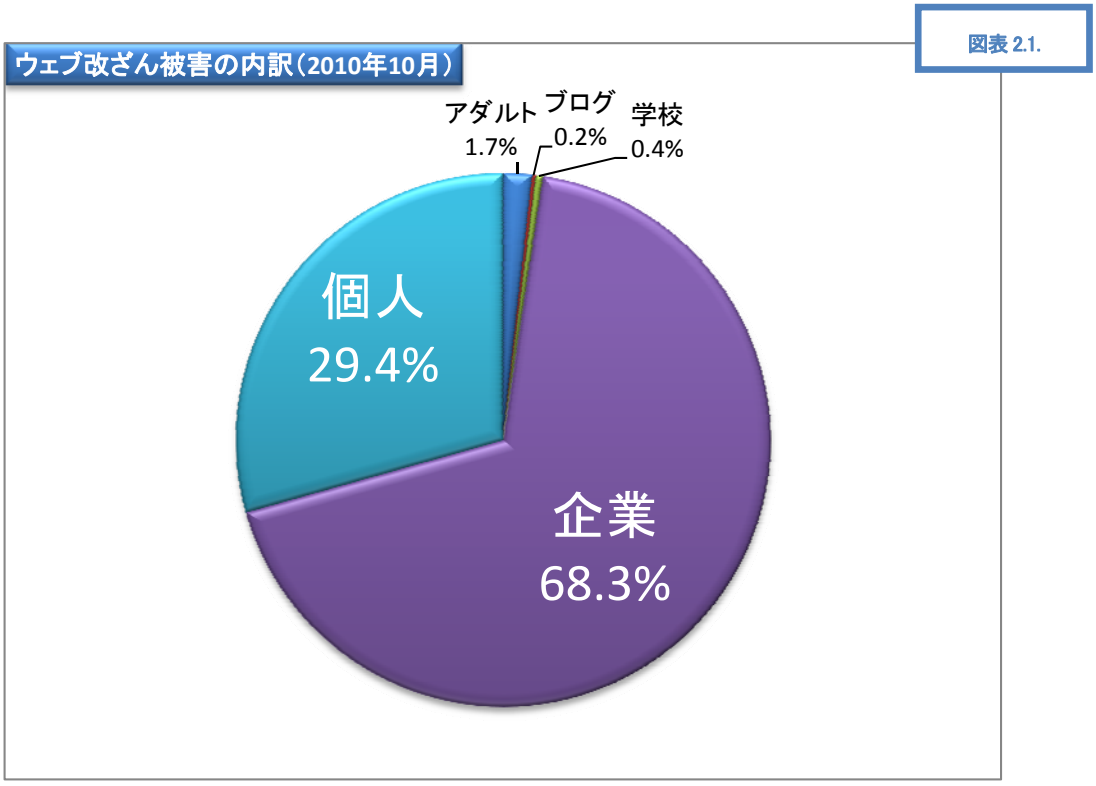
- 「危険」と判断されたウェブサイトの件数は、4,900 件（前月比 112.9%、図表 1.1.）。6 月の統計以来、4 カ月ぶりに前月より増加しています。

「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.

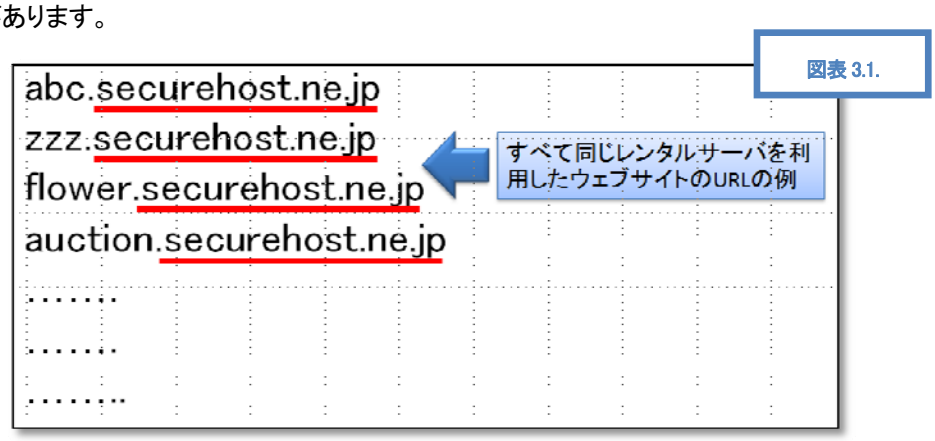
	2010 年 10 月	2010 年 9 月	2010 年 8 月	2010 年 7 月	2010 年 6 月	2010 年 5 月
「危険」と判断されたウェブサイトに占める「Drive by Download タイプの攻撃」の割合	7.0%（344 件/4,900 件）	5.2%（226 件/4342 件）	6.6%（305 件/4,630 件）	15.0%（759 件/5,061 件）	14.6%（813 件/5,578 件）	15.3%（781 件/5,088 件）
「不正改ざんサイト」の検知件数に占める「Drive by Download タイプの攻撃」の割合	43.3%（344 件/795 件）	35.0%（226 件/645 件）	48.3%（305 件/631 件）	70.2%（759 件/1,081 件）	71.9%（813 件/1,130 件）	67.3%（781 件/1,160 件）

3　特定のホスティング会社で集中的に不正改ざんが発生（図表 3.1）

レンタルサーバ事業社の無料期間を悪用

「gred でチェック」で収集された「不正改ざんサイト」の URL を調査したところ、特定のレンタルサーバを利用していると思われる改ざんサイトが多数発見されました。

レンタルサーバを利用して構築されているウェブサイトでは、以下のように URL のドメインを表記する部分が同一になる場合があります。



今回の調査では、特定のドメイン表記を持った URL が多数報告されていました。その数は全体の 11.1%（38 件/344 件）にものぼります。

このような現象には、主に以下 2 つの理由が考えられます。

1. 特定のレンタルサーバのユーザを狙って、管理者 ID、パスワードを盗み取り悪用した。
2. 悪意を持った人物が、不正なウェブサイト構築を目的として、大量にレンタルサーバを申込んで悪質なサイトを立ち上げた。

上記「2」については、サーバレンタル料の発生や申込者の登録情報等の課題があるように思われますが、攻撃者はレンタルサーバの「トライアル期間」を悪用しています。レンタルサーバ事業社は、利用者向けに「2 週間の無料利用期間」等のトライアルメニューを用意しています。攻撃者はこのサービスで一定期間サーバをレンタルし、フィッシング詐欺サイト、ウイルス配信サイト等の悪質なサイトを立ち上げ、攻撃に利用していると思われます。トライアルの申し込みに際しては、本人確認や事業者の確認を取らずに受け付けてしまう場合もあります。また海外の事業者の同様のサービスを悪用する事例も確認されています。

レンタルサーバ利用時のセキュリティ対策に注意

レンタルサーバを使用していると、そのサーバに関するセキュリティ対策は、レンタルサーバ事業社がすべて提供するという、間違った認識を持っている利用者も多いようです。

レンタルサーバ事業社が、一部のセキュリティサービスを提供している場合もありますが、ウェブの改ざん対策等のサービスはすべての事業社が提供しているわけではありません。また、たとえ提供していても「オプション」になっているような場合もあります。ウェブサイトを運営する企業は、自社で利用しているサービスの内容を再度確認すると共に、ウェブサイトの改ざん対策について、対策を講じていく必要があります。

4　フィッシング詐欺の片棒を担ぐことになってしまうかもしれない？

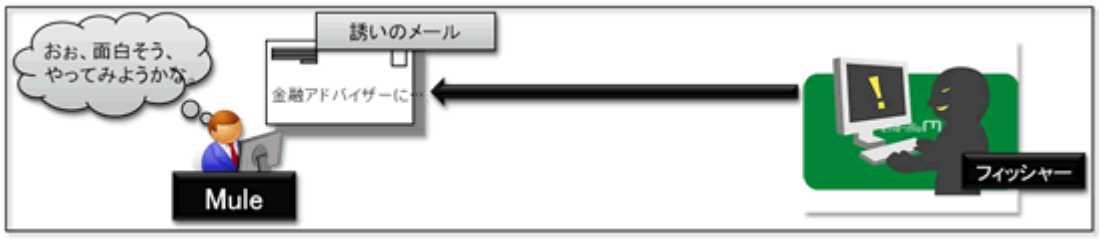
「当社の金融アドバイザーになっていただけませんか？」こんな表題のメールを受信したことはありませんか？本文には「金融の知識は必要ありません」「あなたの口座に振り込まれるお金を送金するお仕事です」「簡単な作業で手数料をお渡しします」のような意味のことが書かれています。

注意してください。これはフィッシャー（フィッシング詐欺を行う人、またはそのグループ）が、収集したインターネットバンキングの ID やパスワードを使って現金を得る為に利用する「Mule（ミュール）：運び屋」を探すメールです。

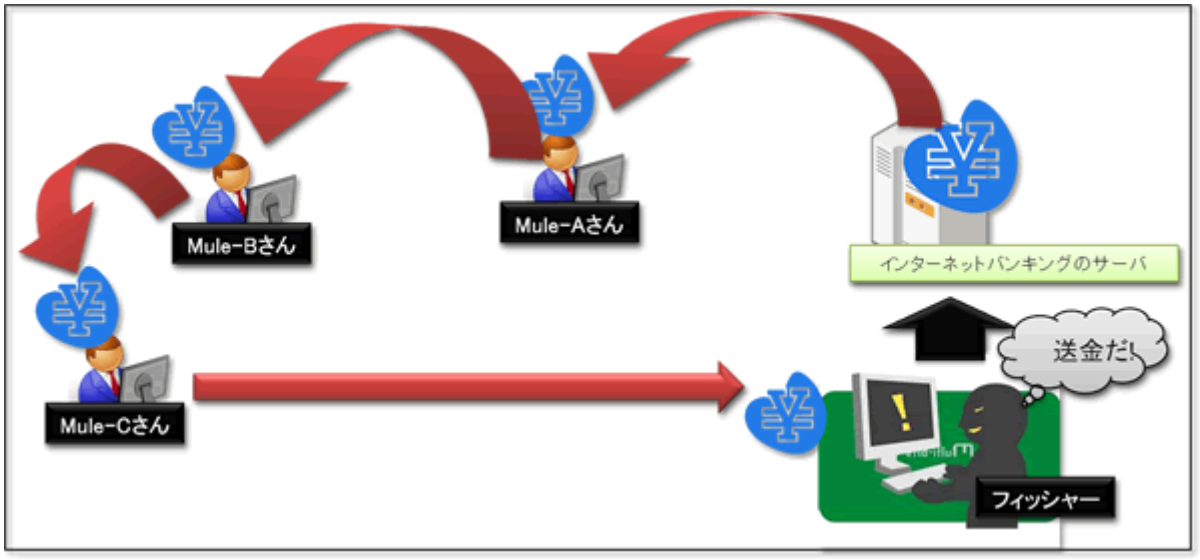
搾取した ID・パスワードをそのまま使って、フィッシャーの口座にお金を振り込んでしまうと、フィッシャー自身が特定されてしまう恐れがあります。しかし、一旦引き出したお金を「Mule」の口座を経由させることで、捜査機関の追跡は難しくなります。「Mule」はフィッシャーとは全く関係の無い「第三者」です。

Mule が介在するフィッシング詐欺の構図

「Mule の採用活動」

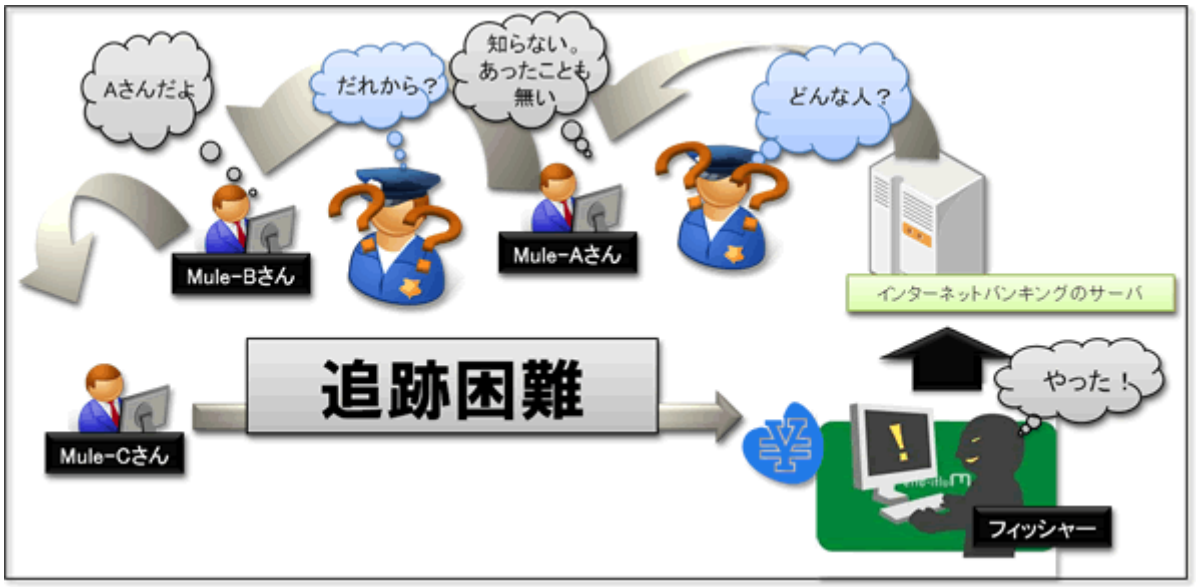


「Mule を利用した送金の流れ」



メールで口座情報をやり取りし、送金・振込の指示もすべてインターネット経由で行い、面識はおろか名前、性別すら知らない者同士が、フィッシャーの呼びかけで集まっています。もちろん「Mule」は送金・振込の本当の目的は知らされていません。

「追跡が困難」



依頼人や送金先の人物と面識がない為、警察等の捜査機関が「Mule」と思われる人物を特定しても「フィッシャー」までたどり着くことは非常に困難です。

また、「Mule」は同一国内にいるとは限りません。多少の語学力があれば、海外送金も可能です。このような状況が、より「フィッシャー」の追跡を困難にします。

「Mule」を誘うメールは無差別に配信される為、そのようなメールの誘いには乗らないよう、最新の注意を払ってください。

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.sagiwall.jp/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.sagiwall.jp/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