PRESS RELEASE

2011 年 6 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.23【2011 年 5 月分統計】

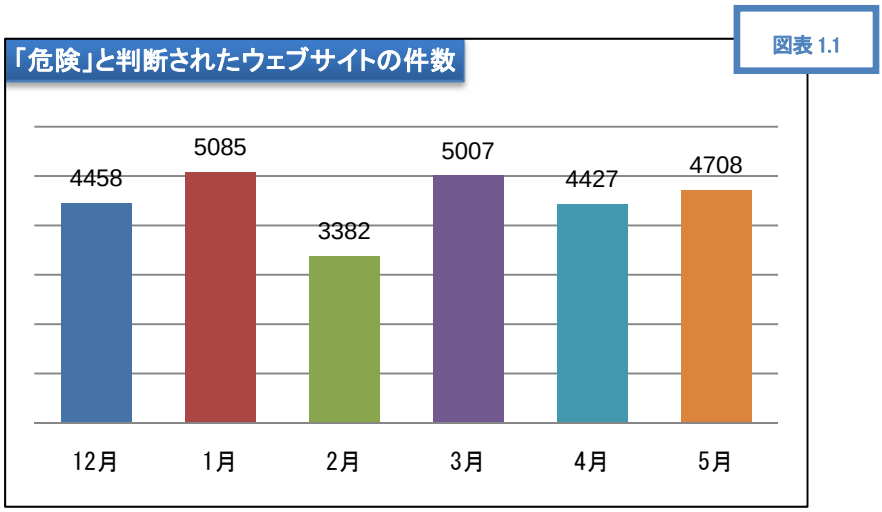
- 【SEO ポイズニング】SEO を悪用した不正サイト誘導のテクニック -

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。

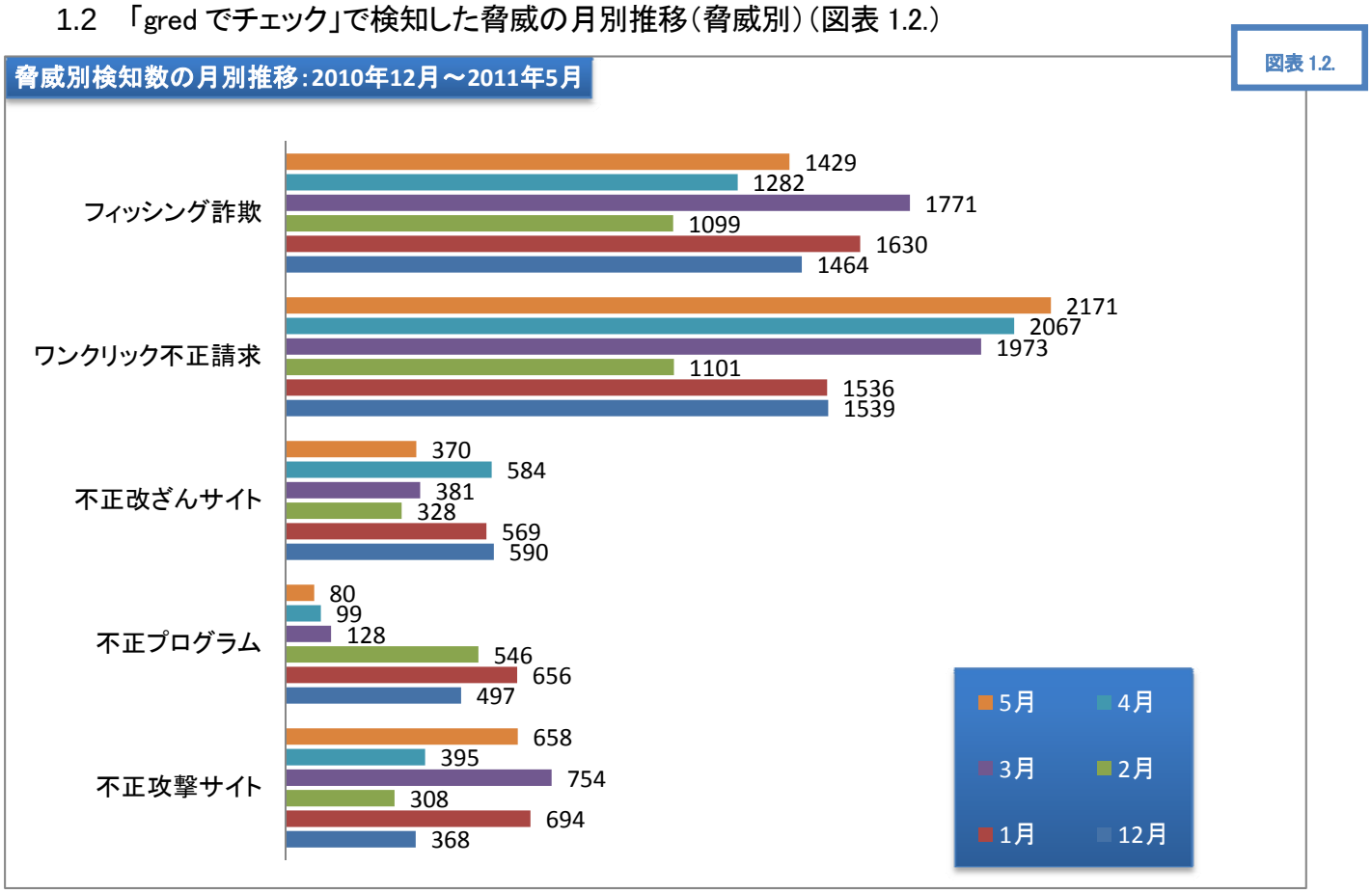
内容

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.）



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.）



1.3 「gred でチェック」月別総利用数（図表 1.3.）

図表 1.3.

月	12 月	2011/1 月	2 月	3 月	4 月	5 月
「gred でチェック」総利用数	43,060	46,034	37,106	40,451	39,165	42,236

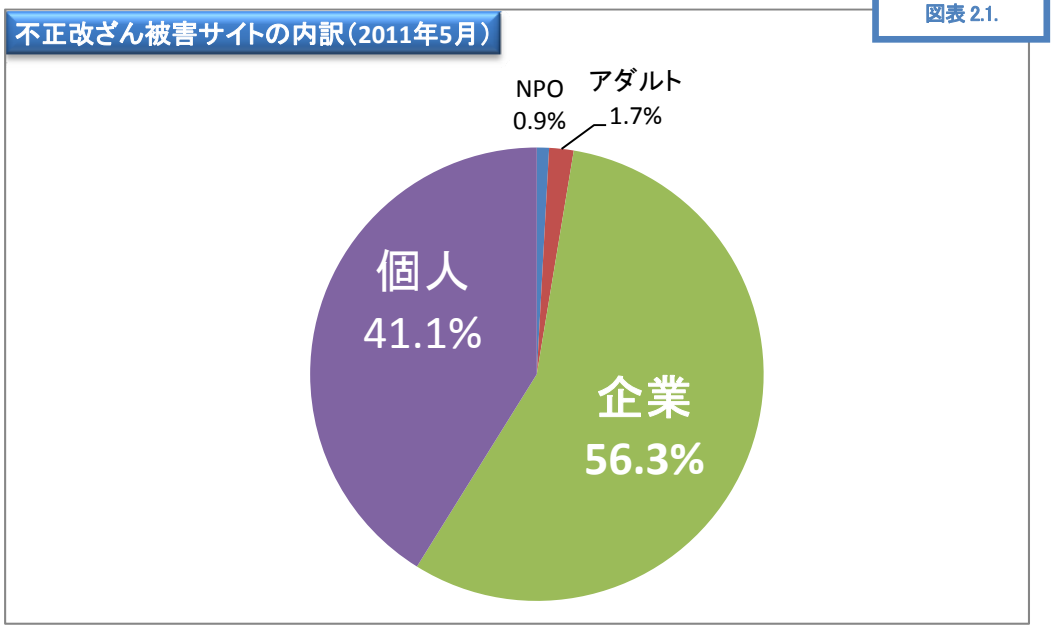
- 「危険」と判断されたウェブサイトの件数は、4,708 件（前月比 106.3%、図表 1.1.）
- 「フィッシング詐欺サイト」の報告件数が増加しています。1,429 件（前月比 111.5%、図表 1.2）
- 「ワンクリック不正請求」の報告件数が増加傾向。2,171 件は先月に引き続き過去最高を更新（前月比 105.0%、図表 1.2）
- 「不正攻撃サイト」の報告件数が大幅増。658 件（前月比 166.6%、図表 1.2）

「gred でチェック」のチェック結果に表示される脅威の説明

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 5 月	2011 年 4 月	2011 年 3 月	2011 年 2 月	2011 年 1 月	2010 年 12 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	4.4% （206 件/4,708 件）	6.1% （269 件/4427 件）	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）
「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	55.7% （206 件/370 件）	46.1% （269 件/584 件）	35.4% （135 件/381 件）	40.9% （134 件/328 件）	46.7% （266 件/569 件）	47.6% （281 件/590 件）

3 【SEO ポイズニング】SEO を悪用した不正サイト誘導のテクニック

（おことわり：本記事は、2011 年 6 月 6 日にセキュアブレインブログに掲載された記事（http://info.gred.jp/archives/1597201.html）を加筆修正したものです。）

近年、社会的に影響が大きい特定の事件・事故について検索すると、不正サイトが検索結果の上位に表示され、被害を受ける問題が多発しています。

「東日本大震災」の直後にも便乗した不正サイト（マルウェア配布サイト）、偽の義援金サイト（デマ情報）が作られました。

これらは、SEO （Search Engine Optimization＝検索エンジン最適化）を悪用し検索結果をできるだけ上位に表示させるテクニックが利用されており、「SEO ポイズニング」と呼ばれています。

SEO ポイズニングによる被害は、数年前から横行

「SEO ポイズニング」の実例

2009 年「サモアで起きた津波」 検索キーワード（samoa tsunami など）

2009 年「マイケル・ジャクソン氏の訃報」検索キーワード（Michael Jackson など）

2010 年「バンクーバー五輪 リュージュ選手の訃報」検索キーワード（Olympics Luge など）

過去の例においても、不正なウェブサイトに誘導され、マルウェアの感染、ボーガスウェアやスケアウェアなどによる被害が多発しました。

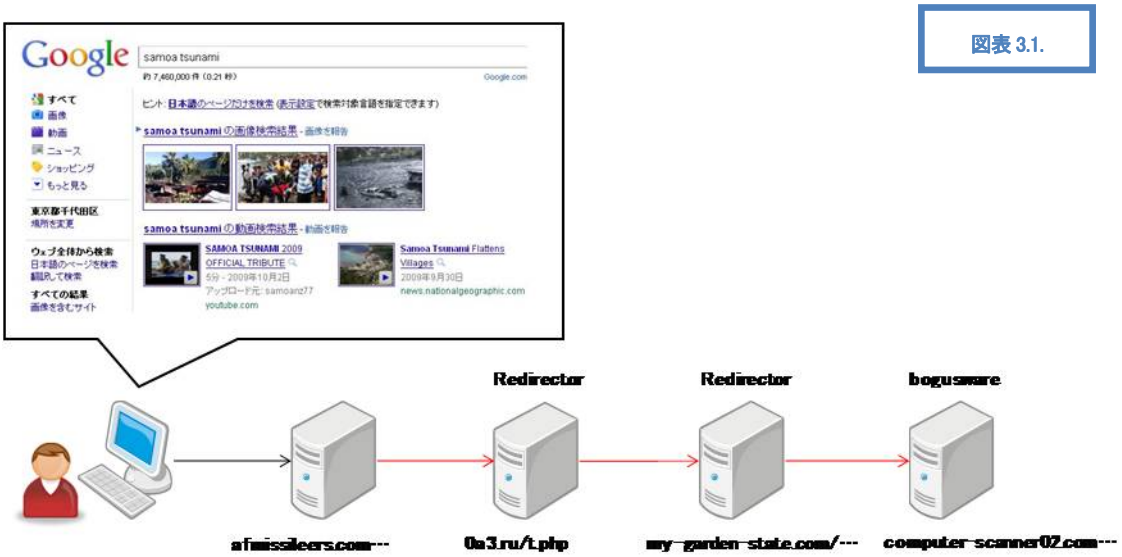
インパクトが大きい事件・事故・自然災害の発生後は、必ずと言っていいほど、僅かな時間で不正サイトが検索結果の上位に表示されています。これらの多くは、「SEO ポイズニング」によるものと考えられます。

SEO ポイズニングは攻撃への入り口？

SEO ポイズニングで検索上位に表示させた不正サイトを入口とし、最終的にウイルス配布サイト等の悪意のあるサイトへ誘導させる多段の誘導テクニックが利用されています。

2009 年「サモアで起きた津波」の際に調査した結果を以下に示します。

図表 3.1.



この攻撃は、最終的にはボーガスウェア（偽のアンチウイルスソフト）を配布しているウェブサイトへ誘導します。最初に Google にて「samoa tsunami」を検索キーワードとして検索し、検索結果の上位に表示されたサイトの URL が「afmissileers.com…」となります。

「afmissileers.com…」にアクセスすると、「0a3.ru/t.php」、「my-garden-state.com/…」と次々とリダイレクトされ、最終的にボーガスウェアを配布する「computer-scanner02.com…」に誘導されます。

ウイルス対策ソフトから逃れる手法も利用

また、最初の入り口となるサイトは HTTP referrer※1 を確認し、検索結果からアクセスしなければ、別の正規のサイトに誘導される仕組みになっています。

これは、セキュリティベンダーなどからの検知や解析から逃れるためだと推測されます。またこの他にも、同一 IP アドレスからの 2 回目のアクセスは別の正規サイトにリダイレクトさせます。

User-Agent※2 などを確認することで、ユーザが利用しているブラウザにより誘導サイトを振り分けるような不正サイトも存在します。

※1HTTP referrer

HTTP ヘッダの 1 つで、インターネット上の 1 つのウェブページまたはリソースから見て、それにリンクしているウェブページやリソースのアドレスを指す。リファラを参照することで、どこからそのページに要求が来たのかを知ることができる。

※2User-Agent

利用者があるプロトコルに基づいてデータを利用する際に用いるソフトウェアまたはハードウェアを指す。

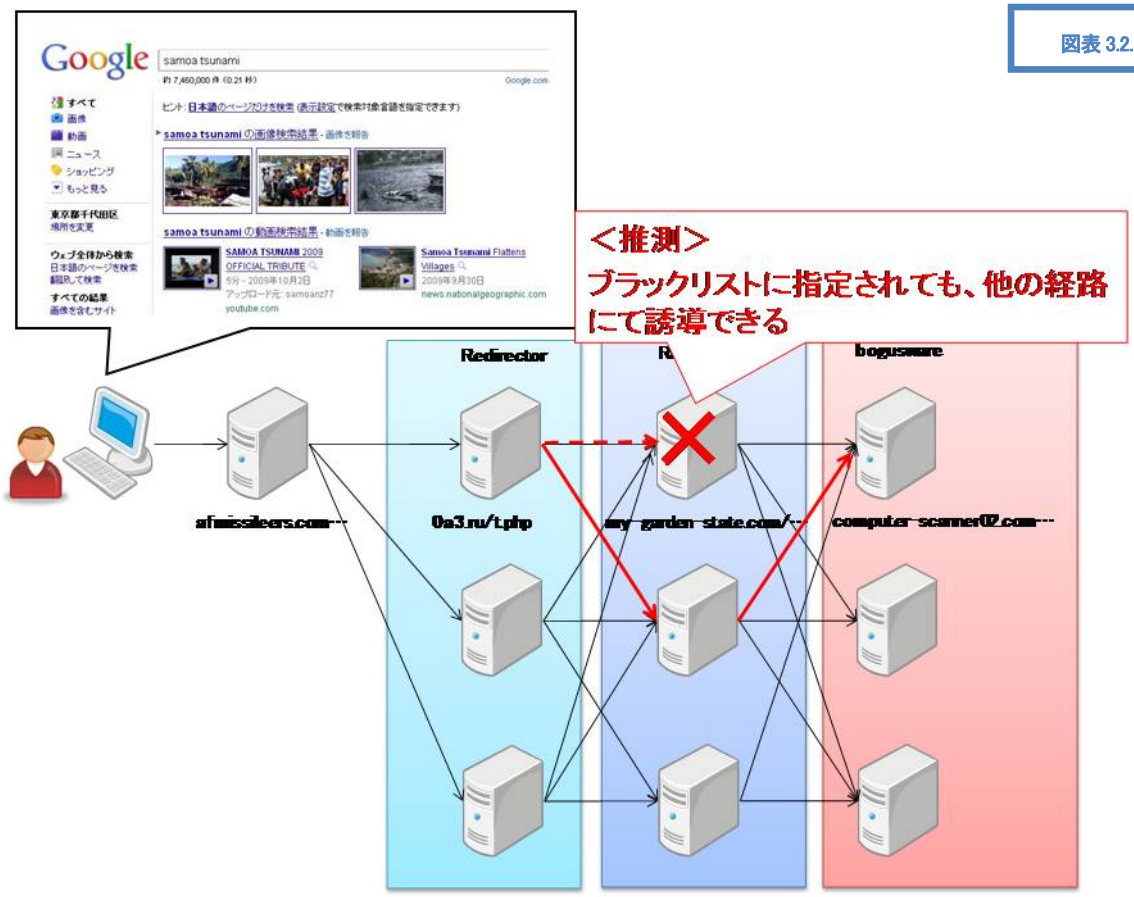
フリー百科事典『ウィキペディア（Wikipedia）』より

複数の誘導ルートを確立！

さらに、同じ PC から定点観測を行った結果、セキュリティベンダーが製品に導入している、ブラックリストによる検知を逃れる為に、以下のような構造になっていることが判明しました。

リダイレクトするサイトが複数存在、さらに最終的にボーガスウェアを配布するサイトも、複数存在しました。

図表 3.2.



この結果より分かることは、リダイレクトする不正なサーバがセキュリティベンダーなどによりブラックリストとして登録された場合でも、他のリダイレクトサーバに迂回させ、ボーガスウェアまで誘導することができることです。

この方法を利用すれば、悪意のある者が（別のキーワードの SEO ポイズニングを狙って）新たな攻撃を仕掛けようとした際、既存のリダイレクトサイトサーバ群を利用することで、即座に上記のような攻撃が可能になると推測されます。

最近の大きなニュースもすぐに多段のネットワーク環境による誘導テクニックが蔓延しているため、これらを構築するテクニックも確立されているのではないかと推測されます。

解説　セキュアブレイン　先端技術研究所　神薗　雅紀（かみぞの　まさき）

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。

ブラウザ専用の詐欺対策ソフト「Internet SagiWall （インターネット・サギウォール）

従来のセキュリティ対策ソフトでは検知することのできない「危険なウェブサイトをブロックします。

［ブロックする悪質サイト］

- フィッシング詐欺サイト
- ワンクリック・ツークリック詐欺サイト
- ウイルス等不正プログラム配布サイト
- Gumblar などによって改ざんされたウェブサイト
- 偽ソフトウェア配布サイト

［機能詳細ページ］

http://www.sagiwall.jp/product/detail.html

【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

安い、軽い、安全、最新型ウイルス対策ソフト「gred AV アクセラレータ Plus」

米国の研究機関による、ウイルス検知テストで『100%』の実力

全世界で 120 万人が使用！

軽さと高い安全性を実現した最新型ウイルス対策です。

[gred AV アクセラレータ Plus の機能]

- 圧縮ファイルのスキャン
- パッカーにより難読化されたファイルのスキャン
- CD、DVD、USB メモリ経由の脅威をブロック
- 電子メールスキャン
- ルートキットの検知と削除
- レジストリとファイルシステムの修復

[機能詳細ページ]

http://www.gredavx.jp/plus/index.html

【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