

報道関係各位

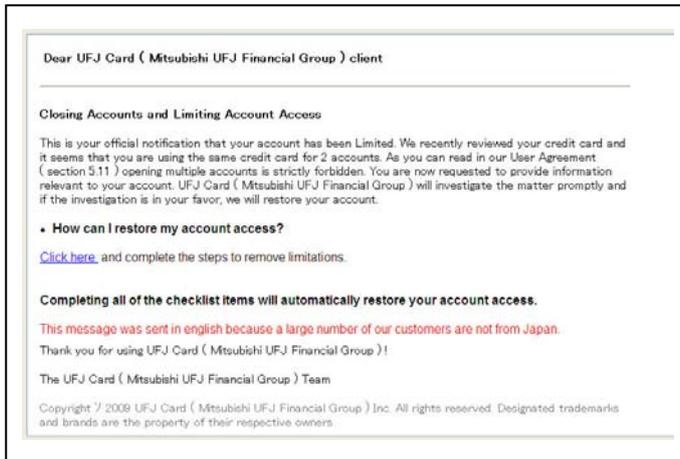
## セキュアブレイン、UFJカードを騙るフィッシングメール、フィッシングサイトが出現しているとして注意を喚起

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、UFJカードを騙るフィッシングメール、フィッシングサイトが出現しているとして、注意を呼びかけています。

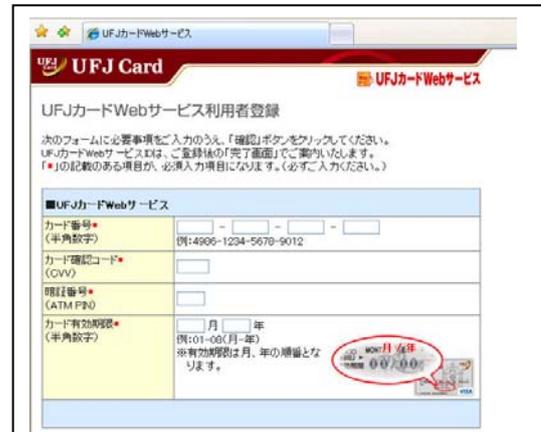
### 概要:

今回セキュアブレインが発見したフィッシングメールは英語で記載されています。フィッシングメールからリンクされたウェブサイトは日本語のものです。UFJカードのウェブサイトには同様のデザインのページが存在しています。このフィッシングサイトのサーバは米国にホスティングされており、UFJカードのロゴや内容を極めて酷似させ偽装しているものと言えます。

弊社では下記のフィッシングメール及びフィッシングサイトを確認しています。これらは、2009年4月14日にセキュアブレインへ報告があったものです。



(UFJカードのフィッシングメール)



(UFJカードのフィッシングサイト)

フィッシングメールは、「UFJ Card ( Mitsubishi UFJ Financial Group )」の件名で英語での HTML メールで送られてきており、メール上の「Click here」をクリックするとフィッシングサイトへリンクしています。メールの文面はカードの期限が切れるので、個人情報(カード番号やパスワードなど)の確認が必要になったというもので、メール中のリンクから Web サイトにログインし、個人情報を再入力しないとサービスが利用できなくなるという個人情報の再入力を求める内容になっています。

今後も複数のフィッシングメール、フィッシングサイトが発生する恐れがあります。メールのタイトル、および内容の両方に注意を払ってください。

## 対策:

UFJ カードでは、カード番号やパスワードなどの重要な情報をメールで尋ねることは、ありません。同様の内容のメールが来てもリンクをクリックすることや、情報を安易に入力しないよう注意を呼びかけています。

セキュアブレインでは、ユーザにできるフィッシング対策として推奨する項目を次のように挙げています。

- ・メールの中のリンクは安易にクリックしない
- ・目的のサイトにはブラウザの「お気に入り」からアクセスするか直接正しく入力してアクセスする
- ・個人情報を送信する前に鍵マークを確認する
- ・サーバ証明書で本物のサイトかどうかを確認する
- ・アドレスバーの URL を確認する
- ・ブラウザには最新のパッチをあてる
- ・専用の対策ソフトを使う

なお、セキュアブレインの個人向け無料ウェブセキュリティサービス「gred(グレッド)」 [www.gred.jp](http://www.gred.jp) では、このフィッシングサイトが検知可能ですのでご利用ください。



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](http://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: [yoshio\\_maruyama@securebrain.co.jp](mailto:yoshio_maruyama@securebrain.co.jp)

電話: 03-3234-3001、FAX: 03-3234-3002 東京都千代田区麴町 2-6-7 麴町 RKビル 4F