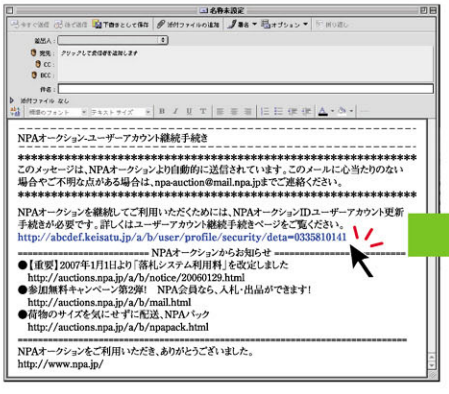
フィッシング

アクセスしたページがもし偽物だったら

フィッシング（phishing）は釣り（fishing）のことではありません。実在する金融機関や企業からのメールを装って「セキュリティを強化する。」などの口実をつけて言葉巧みに偽のホームページに誘導し、暗証番号、カード番号、ＩＤ、パスワードなどを入力させるという手口のことで、そうして得た情報をもとに偽造カードを作ったりネット決済に悪用して、現金を引き出されたり商品を購入されたりといった詐欺の被害に遭います。巧妙に造られた偽のホームページにだまされないように注意してください。

●メール閲覧画面
銀行などの実在する企業を装い、
ID･パスワードの変更などをうながす。



リンク先をクリックすると…

●ブラウザ画面
本物そっくりの“お客様”“会員”情報の
入力画面が開く。

偽の入力ページにアクセスし個人情報を入力させる。

対 策

- **メールやホームページで個人情報を聞かれても安易に答えない。**
- **不審に思ったら、104（電話番号案内）等で確認した電話番号に電話するなど、その金融機関等に直接問い合わせる。**
- **メール本文のURLをクリックしない。（直接入力するか、「お気に入り」等に登録しておく）**
- **フィッシングやスパムメール対策用のソフトウェアを適切に使う。**
- **フィッシングページを見つけたら、フィッシング110番（サイバー犯罪相談窓口）へ通報する。**

インターネットカフェ

消したつもりでも データは残る

不特定多数の人が利用するインターネットカフェ等のパソコンには、利用者の個人情報を盗むような不正なソフトがインストールされている危険性があります。実際にこの手口で個人情報を盗まれて悪用される事件が発生しています。

対 策

- **ID･パスワード、金融情報等の個人情報は入力しない。**
- **ネットバンキングなどのインターネット取引には利用しない。**

無線LAN

使用するときは セキュリティ設定を忘れずに

好きな場所からワイヤレスでネットワークに接続できる無線ＬＡＮは、使い勝手の良さから利用者が急増しています。無線LANを利用する場合には、セキュリティを適切に設定し盗聴や不正利用の被害に遭わないよう注意してください。

対 策

- **セキュリティ設定（暗号等）を必ず行う。**
- **使わないときはパソコンや無線LANルータの電源をOFFにする。**