ネットショッピングやネットバンキングをご利用の皆さまへ

金融情報を盗み取られないために。

スパイウェア

もっとも要注意！
個人情報を盗み取る悪質ソフト

スパイウェアは、コンピュータウィルスのようにコンピュータに入り込み、打鍵（タイピング）、画面表示、ハードディスク等から個人情報を取得して、悪意のある者に送付します。

こうして盗まれた個人情報が悪用されて、銀行口座からお金を引き出されたり、クレジットカード決済で買い物をされたりする被害が発生しています。

スパイウェアは不審なソフトウェアのインストール、悪質なサイトやメールの添付ファイルなどから侵入することが多いので注意が必要です。

対策

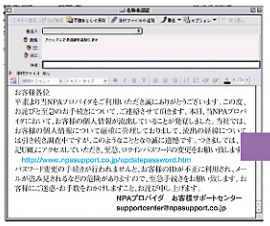
- 不審なCD-ROMやソフトウェアは使わない。
- 使っているOSのアップデートをきちんと行う。
- ウイルス対策ソフトを適切に使う。

フィッシング

アクセスしたページがもし偽物だったら

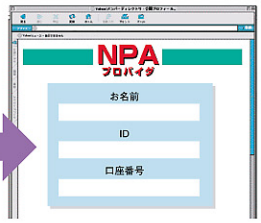
フィッシング（phishing）は釣り（fishing）のことではありません。実在する金融機関や企業からのメールをよそおって「セキュリティを強化する。」などの口実をつけて言葉巧みに偽のホームページに誘導し、暗証番号、カード番号、ＩＤ、パスワードなどを入力させるという詐欺の手口のことで、そうして得た情報をもとに偽造カードを作ったりネット決済に悪用して、現金を引き出されたり商品を購入されたりといった被害に遭います。巧妙に造られた偽のホームページにだまされないように注意してください。

●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。
- 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。

増えています！

インターネット・オークション詐欺

次のような被害が発生していますので、ご注意ください。

- ○　オークションで落札し、代金を振り込んだが、商品が送られてこない。
- ○　オークションで落札できなかったが、メールで直接取引を持ちかけられ、これに応じ代金を振り込んだが、商品が送られてこない。
- ○　自分のオークションIDを他人に不正に利用され、架空商品を出品された。このため、落札者から苦情が来ている。

・取引時のホームページやメールを印刷しておくよう心がけましょう。

利用する際の注意点

- 取引する時には、相手の住所・氏名・電話番号などをよく確認する。
- 相手の銀行口座の控え、振込の控え等を保管しておく。
- エスクローサービスや代金着払いなど安全な方法で取り引きする。
- オークション外での直接取引には応じない。
- パスワードは簡単なものを設定しない。