サイバー犯罪の〈傾向と対策〉

便利なインターネットサービスを安全に利用するために

個人情報や詐欺被害にご注意

ネットバンキング　ネットショッピング　ネットオークション

個人情報が狙われる❶ フィッシング

実在の企業・金融機関を名乗るメールで、システム変更によって新しいID・パスワードの登録が必要などと偽り、本物らしくデザインされた偽造のWebページへアクセスさせ、現在使用しているID・パスワードやカード番号・暗証番号などを入力させようとします。犯人たちは、そうして得た情報を元にカードを偽造し、現金を引き出したり、商品を購入したりします。巧妙に作られた偽造のメールやWebページにだまされないよう気をつけてください。

対策

❶メールにWebページへのリンクが貼られている場合は、そこをすぐにクリックせず、まず企業名・金融機関名などが正しく記入されているか、内容に不審な点はないかなど確認する。

❷メールに不審な点があった場合は、発信者であるはずの企業・金融機関に直接問い合わせて確認し、その上で手続きを行う。

❸メールのリンクページを開いたときは、表示されるURLやページの内容・デザインに注意し、偽造ページでないことを確認する。

個人情報が狙われる❷ スパイウェア

スパイウェアと呼ばれるソフトは、企業・金融機関を詐称して送られてきたCD-ROMやメールの添付ファイルとして、あるいはアクセスしたWebサイトからのダウンロードファイルという形でパソコンにインストールされ、ハードディスクに保存されている個人情報やキーボード入力情報、ディスプレー表示、接続カメラの映像などを、第三者のパソコンに送ります。こうして盗まれた個人情報によって銀行口座から預金が引き出されたり、クレジットカード決済で買い物されたりする被害が発生しています。

対策

❶不審なCD-ROMは使用しない。

❷メールの不審な添付ファイルは開かない。

❸OSメーカーのサポートサイトを利用してシステムをアップデートし、OSのセキュリティ機能を常に最新の状態に保つ。

❹スパイウェア駆除ソフトまたは駆除機能付きウィルス対策ソフトを常に最新の状態で使用する。

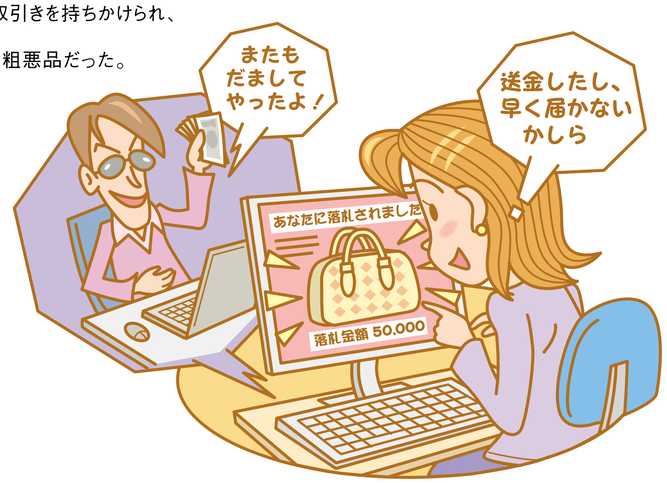
トラブルが多発 ネットオークション

インターネットオークション詐欺と呼ばれる次のような被害が発生しています。

❶落札し代金を振り込んだが、商品が届かない。

❷オークションの出品者からメールで直接取引きを持ちかけられ、代金を振り込んだが、商品が届かない。

❸送られてきた商品が破損している、または粗悪品だった。



対策

❶代金着払いまたはエスクローサービス（第三者が決済と発送を保証するサービス）など安全な取引き方法を指定する。

❷直接取引きには応じない。

❸出品者の銀行口座、振込みの記録、取引き時のWeb画面やメールを保存、または印刷しておく。

個人情報が狙われる❸ インターネットカフェ

インターネットカフェでパソコンを使用した後に、データを削除した場合でも、ハードディスクには情報が残ってしまい復元され、悪用される可能性があります。また、不特定多数の人が利用するインターネットカフェのパソコンには、不正なソフトがひそかにインストールされている危険性もあります。

対策

❶ID・パスワードや金融情報など、重要な個人情報は入力しない。

❷ネットバンキングなど金融関係のネットサービスには利用しない。

❸情報セキュリティ対策が十分でないインターネットカフェは利用しない。

情報を盗み見られる危険 無線LAN

無線LANルータのセキュリティ設定を適切に行っていないと、第三者に無線LANでやり取りしている情報を盗み見られる危険があります。また、セキュリティ設定を適切に行っていない無線LANルータを第三者が悪用し、不正アクセス等の犯罪を行う事案も発生しています。

対策

❶セキュリティ設定（無線LANでやり取りするデータの暗号化や利用者の制限）を必ず行う。

❷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。