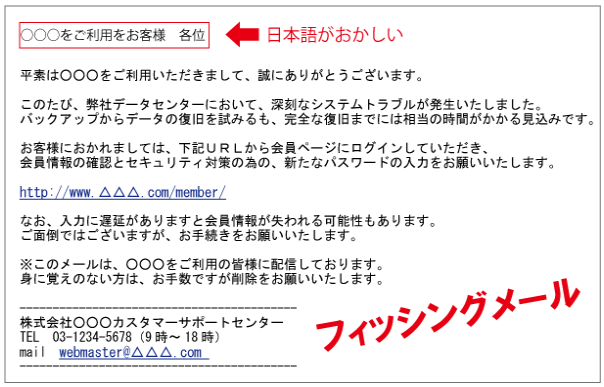
フィッシングサイトにご用心

窓口やATMが閉まっている土日や深夜でも、パソコンやスマホなどインターネットを通じて取引できる便利なネットバンキングですが、その便利さ故に不正送金事件の被害も年々増えています。

不正送金事件の被害は、主にネットバンキングのIDとパスワードが盗まれることにあります。
IDとパスワードが盗まれる手口には、
・フィッシングサイト（偽ホームページ）でIDとパスワードを入力
・コンピュータウイルスによる不正送信
などがあります。

▼フィッシングサイト（偽ホームページ）被害の例

まず銀行を名乗ったメールが届きます。
メールは主に利用者の不安を煽り銀行のホームページへログインを促す内容となっています。
メールに提示されたリンクをクリックすると、本物そっくりの偽ホームページ（フィッシングサイト）が表示され、入力したIDとパスワードは不正に収集されてしまうのです。
三菱東京UFJ銀行を名乗るメールが有名。



（三菱東京UFJ銀行）パスワード等を入力させる偽メールが届いても、絶対に入力しないでください！（2015年4月16日）

さらに最近では、本物のネットバンキングのホームページを開くと、IDとパスワードそして秘密の質問の入力を促すポップアップ画面を表示するウイルスが発見されています。
※銀行がこの3項目を同時に聞いてくることはありません。

▼ジョイメイト推薦の対策方法

（1）ネットバンキング専用のパソコンを用意する
（2）ネットバンキング専用のメールアドレスを用意する
（3）ネットバンキングに必要なこと以外はしない（ネットやメールを用途以外で使わない）
（4）ウイルス対策ソフトをきちんと導入する
（5）OSや関連ソフトの修正アップデートを適切に行う

ネットバンキング専用とするならば、
適切に管理されたWindows 7以降のパソコンでしたら特に高性能で有る必要はありません。
中古パソコン29,800円（税込）から販売いたしております。

※ただ単にウイルス対策ソフトをインストールしているからといって安心はできません。
犯人はいろいろなスキを付いて侵入を試みてきます。（メール、ダウンロード、ホームページなど）