フィッシング

フィッシングとは

「フィッシング」とは他人のクレジット番号やID，パスワードなどを詐取する行為のことである。金融機関や企業からのメールを装って不特定多数の人にメールを送信し，そこにリンクされている偽物のURLにアクセスをさせ，**個人情報**(→p.31)を入力させるなどして不正に入手しようとする行為をいう。

英語では（phishing）と書くが，これは，被害者を魚釣りのように“釣り上げる”（fishing）ことと，その手口が“洗練されている”（sophisticated）ことから「f」が「ph」に置き換えられたと言われている。

フィッシングの手口

フィッシングの手口は巧妙である。送信元を金融機関や企業の担当者名にして「下記のURLにアクセスしないと，あなたのアカウントは失効します」とか「あなたの使用中のカードに新たな機能が加わりました。すぐにログインして使用開始登録をしてください」などと書かれたメールが無差別に送りつけられる。

そのページには金融機関を装ったWebページへのリンクが載っており，クリックするとその金融機関のWebサイトが表示される。ここで表示されるWebサイトは本物をコピーして作られた全くの偽物である場合や，上半分が本物で下半分が偽物である場合，さらには本物のWebページが表示され，その上に個人情報入力用のポップアップウィンドウが表示される場合などがある。

金融機関のページを見て安心したユーザーが「新しいＩＤとパスワードを発行しますので，古いＩＤとパスワードを入力してください」と促され，ポップアップに表示された入力フォームに暗証番号やパスワード，クレジットカード番号などを入力・送信すると，犯人に情報が送信され，詐取されてしまうのである。

クレジットカード番号が詐取されると，勝手に商品を購入されたり，金品をだまし取られたりする。

オークションのＩＤやパスワードが詐取されると，知らないうちに架空の商品を出品したかのような**なりすまし行為**(→p.69)をされて，犯人が入札者から商品の代金をだまし取り，被害者はオークション詐欺の加害者のように仕立てられてしまうのである。

フィッシングへの対応

フィッシングへの対応策としては，送信者欄を信用しない，フォームの送受信にSSL(鍵マーク)が利用されているか確認する，メールに示されたリンク以外の電話番号やURLなどから案内が本物かどうかを確認する，などが挙げられる。

また，OSのアップデートを実行して，常に最新のセキュリティパッチの適用を行ったり，HTMLメールは必ずテキスト表示にしたり，ブラウザのセキュリティ設定で「インターネットゾーン」は“高”レベルに設定したりするなどのセキュリティ対策が必要となる。

さらに，このような対策に加えて，ネット上で起こっている様々な犯罪や詐欺まがい行為についての情報を集め，犯罪者の手口や事例を知っておくとともに，重要な個人情報は，慎重の上にも慎重に扱う姿勢が大切である。