



これが見破るポイントだ

特集2

フィッシング防衛術

「登録しているユーザー情報をすぐに更新してください。こんなメールにはご用心。詐欺師が仕掛けたわなかもしれない。うのみにするとだまされる。詐欺師が狙うのは疑う心を持たないユーザー。ちょっとした警戒心と知識さえあれば、見破るのは簡単だ。」
(勝村 幸博)

© Patrik Giardino/CORBIS

インターネットでは、さまざまな詐欺が横行している。詐欺師たちは、あの手この手で金銭や個人情報をだまし取ろうとしている。その代表例が「フィッシング詐欺」だ。

フィッシング詐欺(以下、フィッシング)の目的は、ネットバンキングやネットオークションといったサービスで使われているユーザーIDやパスワードなどを詐取すること。フィッシングは、これらの情報を盗むために、実在する企業をかたった偽メールや偽サイトを駆使する。

偽のメールで釣り上げる

具体的な手口は次の通り(次ページ右上図)。詐欺師はまず、インタ

ーネットでサービスを提供している企業・組織をかたった偽メールを不特定多数に送信する(同図)。

偽メールには、本物そっくりに作った偽サイトへのリンク(URL)が記載されている。偽メールにだまされたユーザーがリンクをクリックすると、ユーザーのWebブラウザには、偽サイトのログイン画面などが表示される(同図)。ここでユーザーがパスワードを入力すると、それらは偽サイトに送信されて、詐欺師の手に渡る。

以上のように、偽メールをエサにして、ユーザーを偽サイトに「釣り上げる」ため、フィッシングと命名されている。なお、英語のつづりは

魚釣りの「fishing」と区別するために、「phishing」とされている。

偽メールの中には、偽サイトに誘導する代わりに、パスワードなどをメールに記載して返信するよう要求するものもある。こういった手口もフィッシングと呼ぶことが多い。

偽メールは毎月2万種類

フィッシングが出回り始めたのは2003年のこと。以降、世界中で深刻な被害をもたらしている。特に被害が大きいのは米国。このため米国の金融機関やセキュリティベンダーなどは、フィッシング対策の業界団体「アンチ・フィッシング・ワーキング・グループ(APWG)」を結成。フ

ィッシングに関する報告を受け付けるとともに、対策情報などを提供している。

そのAPWGによると、毎月2万種類以上の新しい偽メールと、1万以上の新しい偽サイトが世界中から報告されているという(右下図)。これだけでも十分多いように思えるが、「APWGのデータは、企業やユーザーからの報告に基づいているので、実際のフィッシングの件数はもっと多いはず」(フィッシング対策ソフトを開発販売するセキュアブレインの星澤裕二氏)。

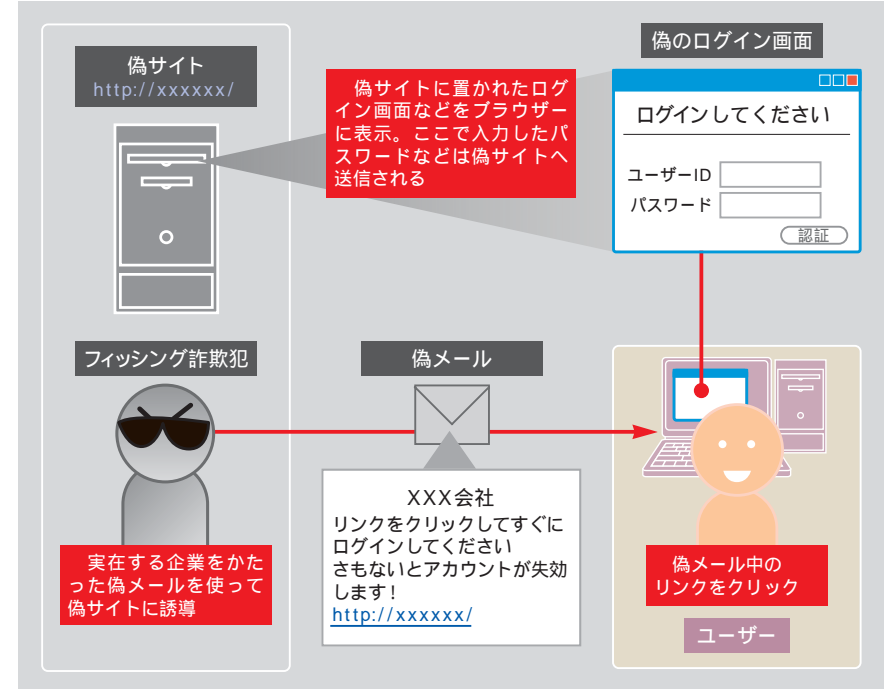
対岸の火事ではない。日本語のフィッシングも2004年ごろから複数出回り始め、2004年6月には警察庁が、7月には経済産業省が広く注意を呼びかけている。

しかしそのかいもなく、2006年になると、国内でも被害が顕在化。フィッシングで盗んだパスワードを悪用した「不正アクセス行為の禁止等に関する法律(いわゆる、不正アクセス禁止法)」違反の検挙件数が急増したのだ。2004年にはゼロ、2005年にはたった1件だったフィッシング関連の検挙件数が、2006年には220件になった(次ページ左上図)。

狙いはオークション詐欺

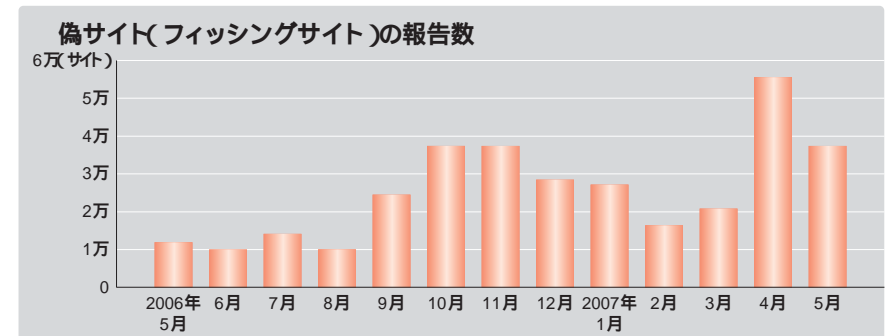
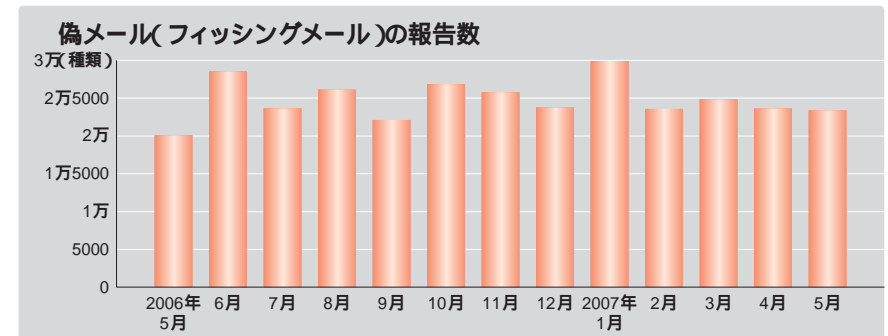
国内ユーザーを狙ったフィッシングとしては、「ヤフーをかたるものが最も多い」(セキュアブレインの星澤氏)。これは、今回取材した専門家の一致した意見。国内のセキュリティベンダーやソフトメーカー、金融機関などで組織されるフィッシング対策の業界団体「フィッシング対策協議会」では、たびたび注意を喚起

偽メールで偽サイトに誘導



フィッシング詐欺の基本的な流れ。詐欺を企てる人物は、実在する企業や組織のWebサイトとそっくりの偽サイトを用意。次に、そのサイトへのリンクを記述した偽メールを送信する。偽メールや偽サイトを信用してパスワードなどを入力すると偽サイトに送信され、詐欺犯に盗まれる。盗まれた情報は、別の犯罪に悪用されたり転売されたりする

全然減らないフィッシング詐欺



フィッシング対策の業界団体である米アンチ・フィッシング・ワーキング・グループ(APWG)に報告された、月ごとの偽メールの種類と偽サイトの数。月ごとにばらつきはあるものの、2万種類以上の偽メールと、1万以上の偽サイトが毎月新たに確認されている