詐欺メール解読術

アドレス偽装の手口■クリックは避けよう

典型的なインターネット犯罪の一つに「フィッシング詐欺」があります。金融機関やネットサービス会社を装い、私たちを偽のページに誘導して個人情報を盗み出す手口です。詐欺を見破る手っ取り早い方法は「アドレスを読む」。うっかり被害に遭わないよう、その基本を解説します。（ライター　斎藤幾郎）

てくの生活入門

フィッシング詐欺の標的は、オークションや金融機関などの利用者。実在の企業を装った偽のウェブサイトを用意して誘導するのが一般的です。ユーザー名とパスワード、またはクレジットカード番号と名義といった情報を入力させて盗み、本人になりすまして決済などを行い、金銭的な利益を得ます。

誘導手段の大半は電子メール。「サービスが変わったので、確認のため下記をクリックして情報を入力してください」などと書いた下にリンクがあり、クリックすると、本物に見せかけた偽ページが表れます。

サービス提供元に電話して確認すれば確実ですが、メールに表示されたアドレスからも、リンク先が正しいかどうか見分けられます。偽ページからウイルスに感染することもあるので、クリックは危険。アドレス表記の仕組みを知っておけば、クリックせずに確認できます。

冒頭の「http://」から、最初に現れる「/」に囲まれた部分を見てください（図下）。この部分を「ドメイン名」といい、通信相手となるコンピューターが所属する組織を知る手がかりになります。

ドメイン名は「www.example.co.jp」のように、「.（ドット）」で区切られ、調べる際は後ろから見ます。欧米では住所を「建物名・番地・市町村・都道府県・国」といった順で表記しますが、ドメイン名も後ろにあるほど「大きなグループ」を示します。

一番右側が「com」や「gov」など3文字以上なら、会社や政府機関など組織の「分類」を意味します。その左の「.」のさらに左側にある名が公式に登録された組織の名前（社名やブランド名など）です。

図下のように、一番右側が2文字の場合は、「jp」なら日本、「hk」なら香港などと国や地域を示します。その左に組織の「分類」が続くもの（「co.jp」や「com.hk」など）と、登録した組織の「公式登録名」が続くものとがあります。2文字＋2文字と続いたら、2番目は組織の「分類」のことが多く、組織の「公式登録名」（例では「example」）はその左側にあります。

この公式登録名と「国・組織分類」から、正規のアドレスかどうか判別できます。例えば「www.asahi.com.example.co.jp」や「example.co.jp/www.asahi.com」は、朝日新聞の「asahi.com」に見せかけていますが、正体は「example.co.jp」。公式登録名（「example」）の左にある「.」のさらに左側や、「/」の右側は登録の必要がないことを悪用しています。

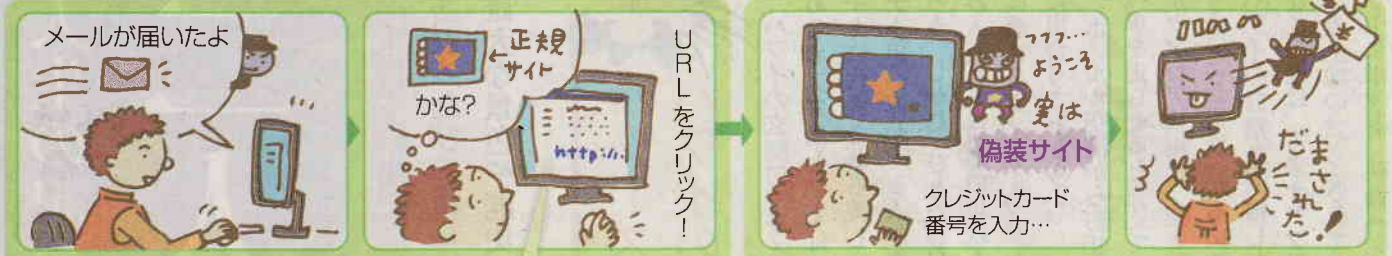
ウェブページ作成などに使われる「HTML」を使うと、メールに表示された文字列と全く異なるアドレスにリンクを設定できるので、メールの文面だけで判断してはいけません。

まずリンクにマウスを合わせ（クリックしない）、メールソフトに表示される情報を見ます。アウトルック・エクスプレスなど多くのソフトでは、ウインドーの左下に本当のリンク先のアドレスが出ます（図中）。

この方法では、長いアドレスの全部は見えません。リンクを「右クリック」して表れるメニューから、「ショートカットのコピー」（ソフトによっては「アドレスのコピー」）を選びます。「メモ帳」などのテキスト編集ソフトを起動し、その上で右クリックして「貼り付け」をすると、本当のリンク先のアドレスが確認できます。

重要な用件は、正規ページの目立つ場所でも告知するのが普通です。手作業で正規ページにアクセスして確認しましょう。アドレスが分からなければ、検索サイトでサービス名を入力して調べます。

詐欺メールでだまされる仕組み



詐欺メール文面(例)

いつもお世話になっております。お取り引きの関係で確認させていただきたい件がございますので、下記のURLから弊社ホームページにお進みのうえ、お手続きをお願いいたします。
http://example.co.jp.xxx.xxx/

正規サイトと見せかけて、偽装サイトに誘導し、情報を入力して盗む

- アカウント情報(ID、パスワード)
- クレジットカード番号、名義
- アメリカでは社会保障番号など

URL偽装の手口

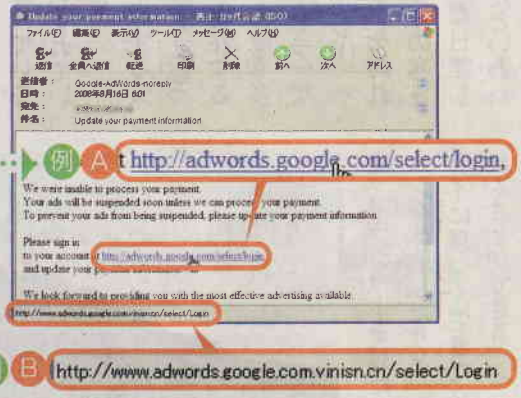
1 実在のドメイン名をサブドメインにして、本物のように見せかける
例 http://example.co.jp.xxx.xxx/

2 パスに正規のドメインを入れる
例 http://xxx.xxx/example.co.jp/

3 見間違えやすい、ミスタイプしやすいドメイン名を使う
例 vv(vを二つ並べてwと誤認させる)
例 lO(エルオー。10と誤認させる)

4 HTMLを悪用して、実際と異なるURLを表示させる

手口①②は、公式登録不要のドメイン部分や、パス部分を、利用者が登録せずに自由に設定できることを悪用して、正規のサイトに見せかける手法



メールの文面からはグーグルのアドレスに見えるが、マウスカーソルを当てて表示させたアドレス(B)は、左記①の手法を使った偽装アドレス

URLはこんなつくり

ドメイン名(「.」で区切る)　パス

http://www.example.co.jp/digital/techno/index.html

サブドメイン
利用者が自由に設定できる。公式登録不要

会社名や組織名など
利用者が設定できる。右側のドメイン(この例なら「example.co.jp」)と組み合わせて、公式登録が必要

国・組織の分類
1区画のものと2区画のものがある
1区画 com net gov org jp cn tv biz など
2区画 co.jp ne.jp go.jp or.jp co.uk など

グラフィック・なかのりか