４．ネットワーク犯罪に巻き込まれないために

二十年前には大学や研究機関でしか利用できなかったインターネットに、今では携帯電話やパソコンを通じて誰もがアクセスできるようになりました。インターネットのおかげで私たちの生活は便利になりましたが、その反面、知らない間に犯罪の被害者や加害者になる可能性が高くなっています。この章では、安全にインターネットを使うための基本的なポイントを紹介します。

アカウントとパスワード、個人情報の扱いに注意しましょう

ネットワーク上では「アカウントとパスワード」が「あなたがあなたであること」を証明します。パスワードが盗まれてしまうと、誰かがあなたになりすまして悪用するおそれがあります。逆にあなたが友人のアカウントとパスワードを知ってしまった場合、無断で利用することは法律に違反するので気をつけましょう。また、ネットワーク上で実名・住所・電話番号・所属といった個人情報が悪意のある第三者に知られると、犯罪の被害に遭う可能性が高くなります。取扱いには充分な注意が必要です。

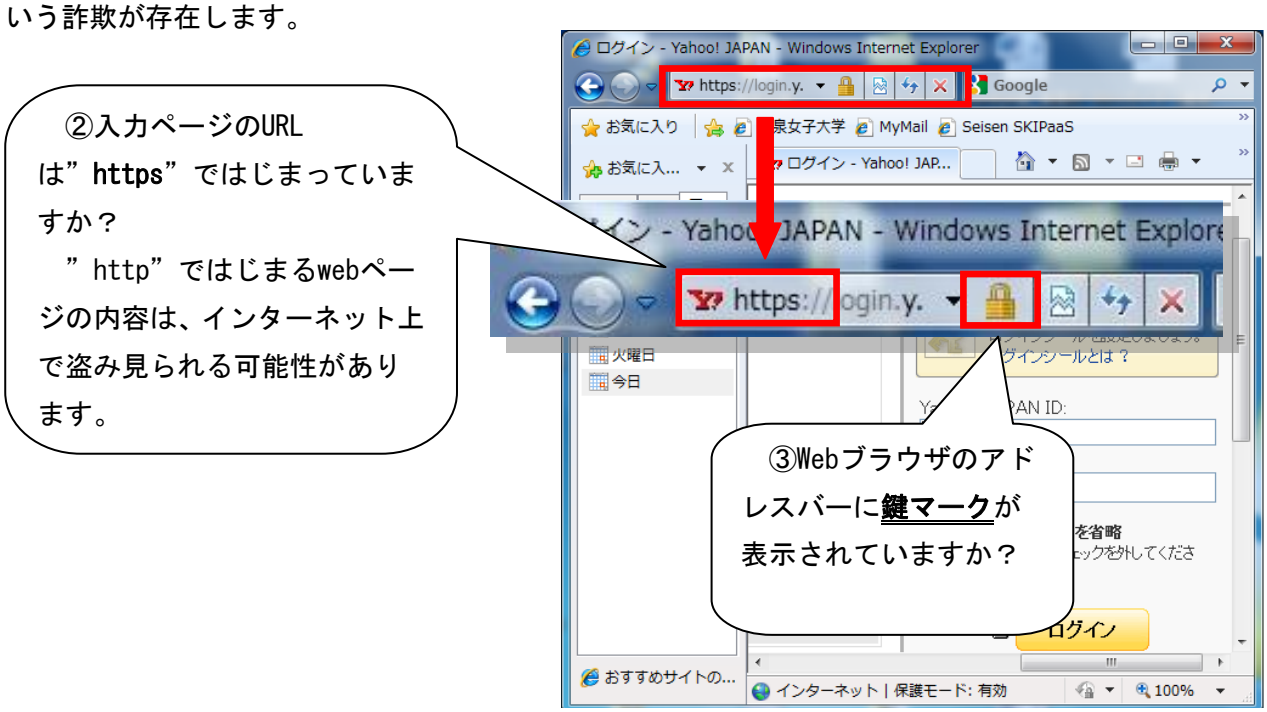
1) アカウントとパスワードを他人に知られないように管理しましょう

手帳に書いたり、友達や彼氏に教えたりしていませんか？　また、名前や誕生日、LANアカウントと同じにしたりしていませんか？パスワードが漏えいすると、本人になりすましてメールを送られたり、高額の商品を買われたりする恐れがあります。

2) アカウントとパスワードを入力する web ページが「安全である」ことを確認しましょう

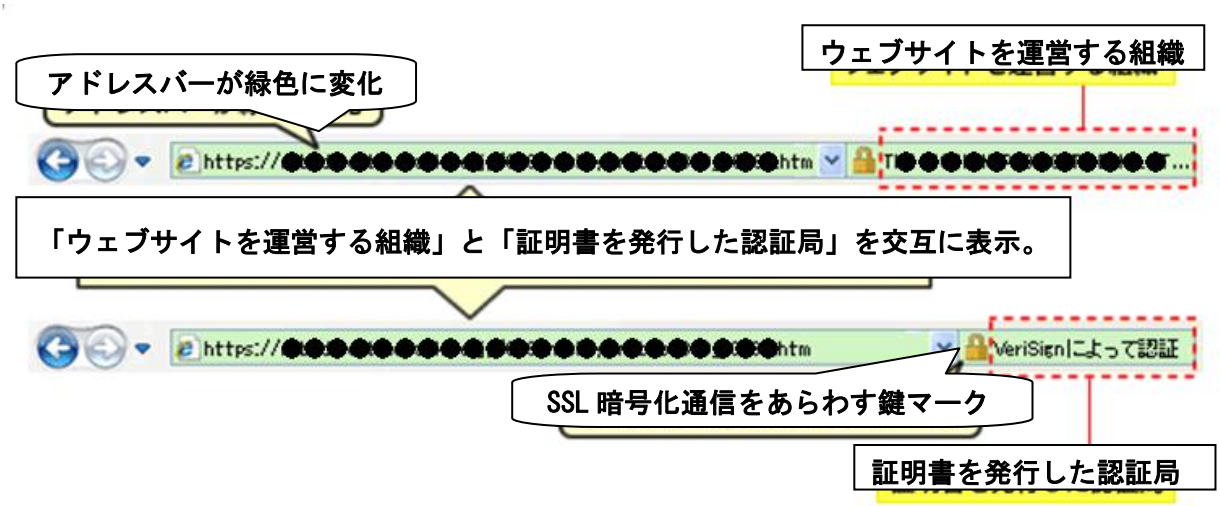
①ドメイン名は正しいですか？

ショッピングサイトや銀行などのwebページを複製してパスワードを入力させる「フィッシング」という詐欺が存在します。



④アドレスバーの色にも注意しましょう。

正規のサイトの場合はアドレスバーが緑色に変化します。



アドレスバーが赤色になり、「フィッシングwebサイト」と表示された場合は正規のサイトではなく、フィッシングサイトですので、
個人情報を入力しないようにしましょう。

アドレスバーが赤色になる機能はInternet Explorerの機能であり、EV SSLサーバ証明書の機能ではありません。Microsoft社にフィッシングサイトとして報告されたサイトを閲覧した場合にアドレスバーが赤色になります

3) 運営元が信頼できる相手かどうか考えましょう

姓名判断や相性占いなど、巧みなうたい文句で個人情報を入力させ、集めた情報を名簿として販売する業者が存在します。その名簿は架空請求詐欺などの犯罪に使われる可能性があります。実名・住所・生年月日・電話番号といった個人情報を入力するときには、特に注意しましょう。

コンピュータウイルスに気をつけましょう

コンピュータウイルスはメールやwebページ閲覧を通してパソコンに侵入する特殊なプログラムです。感染すると自分のパソコンが壊れたり自分の個人情報が漏れたりするだけでなく、他人のパソコンをウイルスに感染させたり、攻撃をしかけるために使われたりする可能性があります。

1) ウィルス対策ソフトを導入し、正しく使いましょう

インターネットの世界では次々に新しいウイルスが生みだされています。対策ソフトを導入したうえで、ウイルス検知データを定期的に更新するように設定しましょう。また、USBメモリやSDカードなど、持ち運び用のメディアも感染していないかチェックしましょう。

2) ソフトウェアを最新の状態に保ちましょう

パソコンに入っているOS（WindowsOS、MacOSなど）、Webブラウザ（IE、Safariなど）、AdobeFlash、AdobeReader、Java Runtime など、毎日利用しているソフトウェアでセキュリティホールと呼ばれる不具合が見つかることがあります。不具合が見つかった場合、メーカーからはパッチと呼ばれる修正プログラムが提供されますが、パッチを実行せずに放置していると、たとえウイルス対策ソフトを入れて正しく使っていても、ウイルスに感染してしまう可能性があります。自分の利用しているソフトの名前とメーカーを把握し、不具合情報に注意しましょう。

ネットワーク上でのふるまいに気をつけましょう

インターネット上の情報は世界中の誰でもアクセスすることができるため、軽い気持ちで行ったことがとんでもない被害をもたらすことがあります。webページやブログ、SNSやプロフィールサイトなどで不特定多数を相手に発信する場合には、充分に注意しましょう。

1) 著作権や肖像権を侵害していませんか？

持っているCDをMP3に変換してwebサイトに置いたり、素材サイトの写真を自作だと偽って配信したり、メールの内容を送信者に断りなくブログに載せたり、引用の範囲を超えて本の内容を転記したり、街中で見かけたアイドルの写真を掲示板に投稿したりしていませんか？他人の著作や肖像にはそれぞれ固有の権利があり、許諾を得ずに公開すると訴えられたり罰せられたりすることがあります。

2) 他人のプライバシーを侵害していませんか？

友人の本名や住所、顔写真、あるいは個人が特定できるような悪口や噂話を掲示板やプロフィールサイトに載せていませんか？ブログを開設している場合には、コメントに個人情報や誹謗中傷が投稿されていませんか？不用意に公開された個人情報をもとにストーカー被害などが生じたり、プライバシーの侵害で罪に問われたりする可能性があります。

■■　ネットトラブル実例集 ～ありませんか、こんなこと～ ■■

Case1

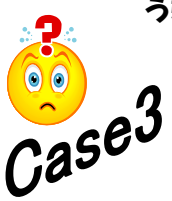
最近、読んだ覚えのないメールに既読メールがついている。
また、ネット閲覧の履歴に知らないページが入っている。

誰かがあなたのアカウントでログインしている可能性があります。すみやかにパスワードを変更しましょう。

Case2

「サイトの利用料金を払っていないのですみやかに支払え。」、というハガキが裁判所から来た。利用したかどうか覚えがないが、親に知られると怒られそうなので、払おうと思う。

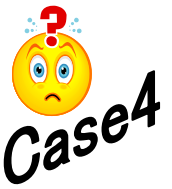
裁判所からいきなりハガキが来ることはありません。架空請求詐欺の可能性がありますので、決して支払ってはいけません。



Case3

難病の子どもを救うために、献血募集のメールをできるだけ多くの人に回すよう頼まれた。

チェーンメールという迷惑行為の一つです。ネットワークに大きな負荷をかけるだけでなく、デマの温床ともなりますので、応じてはいけません。



Case4

クレジットカードの請求明細に見知らぬ支払いがある。

Web ショッピングや店舗での買い物を通じて、クレジットカードの情報が盗まれた可能性があります。至急、カード会社に連絡してください。

Case5

他大学の友達と喧嘩した腹いせに、喧嘩の詳細や相手の悪口をツイッターでしゃべった。

内容の真偽を問わず、名誉毀損にあたる可能性があります。また、しゃべった自分の身元が特定された場合、社会的に大きなダメージを被ります。一時の怒りに我を忘れないようにしましょう。

もっと詳しく知りたい場合は…。

清泉女子大学「ネットトラブル SOS ページ」や別紙「情報倫理の手引き」、
総務省の「国民のための情報セキュリティサイト」等を参考にしましょう。

また、インターネットを利用していて「おかしいな」「気になるな」と感じたことがあれば、
４号館１階　情報環境センター窓口　までご相談ください。

清泉女子大学「ネットトラブル SOS ページ」
http://campus.seisen-u.ac.jp/sos/