

情報セキュリティに関する Q&A

ウイルスによるデータの漏えいや、パスワードの詐取など、パソコンやインターネットの利用には様々な危険が隠れており、注意が必要です。

以下に、パソコンやインターネットを利用する上で注意すべき点を Q&A 形式でまとめています。疑問に感じることなどありましたら、ぜひ参考にしてください。

Q:学内のパソコンやメールで使用しているログイン ID を他の学生に貸しても良いのでしょうか？

A:ログイン ID は利用者を識別するためのものです。他の学生があなたのログイン ID で何らかの問題を起こした場合、問題を起こした学生だけでなく、管理者であるあなたの責任も問われることとなります。他人には絶対に貸さないよう管理してください。

Q:なぜ、パスワードに電話番号や生年月日を使用していけないのですか？

A:電話番号や生年月日は、比較的容易に情報を入手できるためです。アルファベットのみや数字のみのパスワードも、悪意のある者に割り出されてしまう可能性があります。英数字を混在させ、かつ6文字以上のパスワードを設定してください。

Q:入学時から同じパスワードを使用していますが、問題ないのでしょうか？

A:キー操作の盗み見やインターネット通信の盗聴などによって、万が一 ID・パスワードが漏えいしてしまった場合でも、パスワードを変更することによって、その ID を不正に使い続けられることを止めることができます。少しでも異常を感じたらすぐにパスワードを変更するよう心掛けてください。

Q:数分席を離れる程度であれば、パソコンをそのままの状態にしておいても良いのでしょうか？

A:たとえ数分であっても、席を離れる場合はコンピュータをログオフまたはシャットダウンをしてください。また、貴重品は常に身につけるようにしてください。

※ただし、荷物での席の確保は他の利用者の迷惑になりますのでご遠慮ください。

Q:出所のはっきりしないファイルや、見知らぬ相手からのメールに添付されていたファイルは、内容を確認するためにも開いた方が良いでしょうか？

A:出所のはっきりしないメールには、ウイルスや役に立つように見せかけて実際には被害をもたらすプログラムが混入されている可能性がありますので、安易に開かないようにしてください。判断に迷う場合は、情報メディアセンターまでご相談ください。

Q:持ち運び可能なパソコンを自宅の外で使用する際に注意することはありますか？

A:機器の盗難には十分注意し、席や車に置いたままにしないようにしてください。また、電車などへの置き忘れにもご注意ください。

Q:自宅やネットカフェなど、学外のパソコンで大学のシステムを利用する際に注意すべきことはありますか？

A:学内のパソコンに比べ、自宅のパソコンはウィルス感染によって悪意のあるプログラム、例えばキー操作の内容を記録してしまうようなプログラムが潜り込む可能性が高くなっています。自宅のパソコンには必ずウィルス対策ソフトを入れ、常に最新の状態に保つようにしてください。さらに、セキュリティアップデートを行い、OSを常に最新の状態にするよう心掛けてください。また、ネットカフェのパソコンは不特定多数の人が利用するため、悪意のあるプログラムが潜り込んでいる可能性が高くなっています。極力、ネットカフェのパソコンでは、他人に見られたくない情報は扱わないようにしてください。

Q:なぜ、自分のホームページにアニメのキャラクターや俳優の画像を掲載してはいけないのでしょうか？

A:著作権法により、著作物を無断でホームページにアップすることは禁止されています。たとえ自分で撮影した写真であっても、本人の許可を得ずに無断でインターネット上に公開することはトラブルのもとになります。これは芸能人の写真に限らず、一般人についても撮影および公開には許可が必要です。

Q:コンピュータウイルス、ワームとはいったい何ですか？

A:電子メールやホームページの閲覧によってコンピュータに侵入する特殊なプログラムです。パソコンの画面に何らかのメッセージや画像を表示するものから、悪意のあるものはパソコンに保存されている情報を勝手に消去したり、パスワードなどのデータを外部に送信したりします。また最近では、「あなたのパソコンからウイルスが発見されました」といった偽の警告を画面に表示させ、悪意のある Web サイトに誘導させるようなものも発見されています。

Q:トロイの木馬とは何ですか？

A:通常のプログラムを装ってコンピュータに侵入し、データを消去したり、データを外部送信してしまうプログラムです。見知らぬファイルや、無料でウイルスチェック行うなどのメッセージが表示されても安易に実行しないようにしてください。

Q:キーロガーとは、いったい何ですか？

A:キーボードの入力内容を記録するプログラムです。こっそりパソコンに仕掛けて、パスワードなどの情報を盗んだりします。

Q:フィッシング詐欺とは何ですか？

A:銀行などからのメールやホームページと見せかけ、暗証番号やクレジットカード番号を盗み取る詐欺のことです。銀行や企業は、暗証番号の確認をメールで行うことはありませんのでご注意ください。また、正規のホームページにそっくりな偽ホームページに誘導し、クレジットカード番号や暗証番号を入力させ、番号を盗み取る例も報告されています。不信なメールを受信したり、偽ホームページの疑いがある場合は、情報メディアセンターまでお知らせください。

情報セキュリティに関するお知らせや、コンピュータウイルスに関する注意喚起などをこちらのホームページに掲載していますので、定期的に確認してください。

愛知大学情報セキュリティ委員会ホームページ

<https://jsec.aichi-u.ac.jp/>

愛知大学公式ホームページのトップ画面最下や、情報メディアセンターのホームページにもリンクが設けられています。

以上