Wi-Fi（無線 LAN）の安全な利用について

利用している端末を **Wi-Fi**（ **Wireless Fidelity** ）に接続することで、モバイル回線を使用しなくてもインターネット接続が可能となります。

いまや、街中のコンビニやカフェ、空港やホテルなど、人が気軽に出入りできる場所のほとんどで「**無料（フリー）Wi-Fi**」が提供されています。

しかし、便利な反面、**全てが安全に使えるというわけではありません。**悪意を持って提供された Wi-Fi スポットに接続してしまうと、通信内容の盗聴、ウイルス感染、危険なサイトに飛ばされる、不正アクセスに遭う等の被害を受けることがあります。パスワードが設定されていない、安全性の低い通信規格（WPA2 ではない規格）を使用しているなどの Wi-Fi スポットには特に気をつけてください。

✽利用しようとしているサービスのセキュリティを理解しよう

ウェブメールのログイン画面を見ている時に、ウェブブラウザのアドレスバーやウインドウの下の方（ステータスバー）に金色の鍵マークが表示され、URL が「**https://**」で始まるアドレスになっていることに気づいたことはありますか？

これは、**SSL（Secure Socket Layer）**というセキュリティの仕組みが働いていることを意味していて、**そのウェブページで送受信するデータを完全に暗号化している**ことを表しています。また、SSL は暗号化に加え、電子証明書により通信相手の本人性を証明し、なりすましを防止するなど、今日のインターネットの安心・安全を支えています。そのため、パスワードや暗証番号などの大切な情報も安心して扱うことができるのです。

パスワード等の個人情報に限らず、インターネット上に情報を送信する際に SSL が機能しているページがあれば、そちらを利用すると良いでしょう。

総務省『国民のための情報セキュリティサイト』（最終閲覧日：2020/2/25）
（https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/basic/structure/03.html）を編集して作成

ウイルス感染しないために

コンピュータウイルスの感染ルートはさまざまですが、ウイルス感染を防止するためには、次の３つが基本の対策になります。

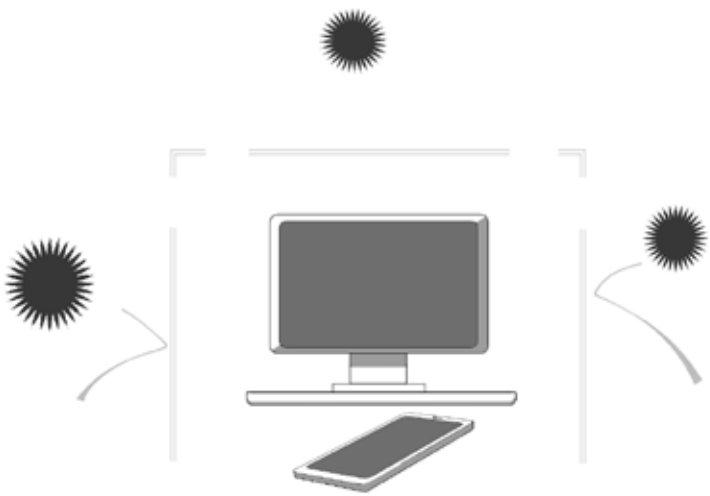
1. **ソフトウェアを更新する**
2. **ウイルス対策ソフトを導入する**
3. **怪しいホームページやメールに注意する**

インターネット普及率が高い現在では、ネットワークを利用して簡単にウイルスをばら撒けるため、電子メールやウェブペ ージによる感染が主流になっています。ネットワークを介して感染するウイ ルスの場合、PC から LAN ケーブルを抜くなど、ネットワークから物理的 に隔離すると、確実に感染拡大を防ぐことができます。
しかし、先決すべきは**ウイルスに感染しない環境づくりをすること**です。

新しい PC やスマホなどの通信機器を入手したら、一番最初に必ず**ウイルス対策ソフト**をインストールしましょう。
ウイルス対策ソフトは、一般的にコンピュータの電源がオンであるときには常に起動した状態になり、外部から受け取ったり送ったりするデータを常時監視することで、インターネットや LAN、記憶媒体などからコンピュータがウイルスに感染することを防ぎます。

また、ウイルス対策ソフトのバージョンは常に最新版を利用するよう心がけましょう。契約期間が切れて、ウイルス検知用データが更新できなくなってしまうと、コンピュータを十分に保護することができなくなってしまいます。ウイルス対策ソフトは、コンピュータを使用する上での必要な投資と考え、必ず継続的に更新するようにしましょう。

総務省『国民のための情報セキュリティサイト』（最終閲覧日：2020/2/25）
（https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/basic/privacy/03.html）を編集して作成

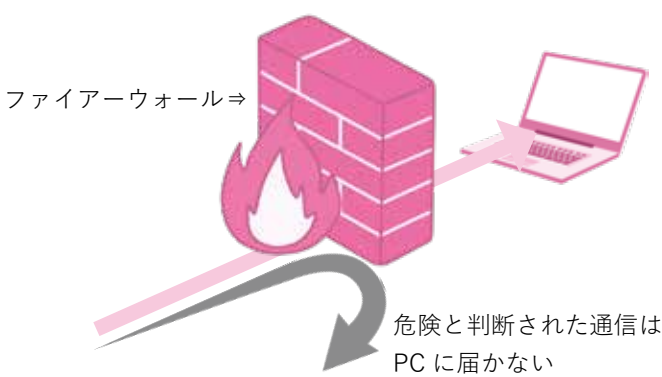


不正アクセスに遭わないために

インターネットに接続したPCには、外部から自分の意図しない攻撃の通信が送られてくる場合があります。こうした**不正アクセス**をさせないためには、まず外部からの不要な通信を許可しないことが大切です。
最近では、ノートPCなどを外部に持ち出すなどの機会が増えたため利用者のPCが直接の不正アクセスの対象になっています。このような被害を防ぐためには、通信の可否を設定できる**パーソナルファイアウォール**を導入し、運用するようにしましょう。

ただし、ファイアウォールなどによって権限のない者の通信を防いでいても、権限を悪用されると、不正アクセスをされることになってしまいます。そのようなことがないよう、**アカウント情報（ID、パスワードなど）の管理を十分に行い、権限を奪われることがないように注意**しなければなりません。

その他、不正アクセスをされる原因となる**脆弱性**への対策も必要になります。脆弱性が報告され、修正プログラムが配布されたら速やかに適用するようにしましょう。



総務省『国民のための情報セキュリティサイト』（最終閲覧日：2020/2/25）
（https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/basic/privacy/04.html）を編集して作成

個人情報の取扱について

個人のインターネット利用において問題となっているのが、個人情報の公開です。ブログやソーシャルネットワーキングサービス（SNS）を使って、個人が情報発信をする機会が増えていますが、自分の写真や連絡先をインターネット上に公開することには、危険も伴います。

インターネットで公開した情報は、いろいろな人が閲覧する可能性があります。そのため、インターネット上で、氏名、年齢、住所、電話番号、自分の写真といった作成者自身の**個人に関する情報を公開することの危険性**について、きちんと認識しておかなければなりません。

また、インターネット上の電子掲示板やホームページなど、誰でも見られる場所に他人の個人情報を公開することは、たとえ事前に許可を得たとしても、プライバシー保護の観点から慎重になった方が良いでしょう。

被害から身を守るためには、何よりもインターネット上では、むやみに個人に関する情報を公開しないようにすることが大切です。最近は、検索技術の向上により、たとえあるサイトで公開している情報が断片的なものであっても、インターネット上のさまざまな情報を組み合わせることで、**あなた個人を特定する情報を探し出すことができる可能性が高くなっています**。また、一度インターネット上に公開された情報が、コピーにより拡散していった場合、それを完全に削除することは困難です。

個人に関する情報の公開の判断は、非常に慎重に行うべきです。さらに、自分以外の家族や他人の個人に関する情報を、本人の許可なく掲載することは、厳に慎まなければなりません。

総務省『国民のための情報セキュリティサイト』（最終閲覧日：2020/2/25）
（https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/enduser/attention/02.html）を編集して作成

パスワードの設定と管理

他人に自分のユーザアカウントを不正に利用されないようにするには、適切なパスワードの設定と管理が大切です。
適切なパスワードの設定・管理には、以下の **3 つの要素**があります。

✤1．安全なパスワードの設定

安全なパスワードとは、他人に推測されにくく、ツールなどで割り出しにくいものを言います。

(1) 名前などの個人情報からは推測できないこと
(2) 英単語などをそのまま使用していないこと
(3) アルファベットと数字と記号が混在していること
(4) 適切な長さの文字列であること（**8 文字以上が望ましい**）
(5) 類推しやすい並び方やその安易な組合せにしないこと

✤2．パスワードの保管方法

せっかく安全なパスワードを設定しても、パスワードが他人に漏れてしまえば意味がありません。以下が、パスワードの保管に関して特に留意が必要なものです。

・パスワードは、**友達や先輩後輩などに教えないで、秘密にすること**
・パスワードを電子メールでやりとりしないこと
・パスワードのメモをディスプレイなど、他人の目に触れる場所に貼ったりしないこと
・やむを得ずパスワードをメモなどで記載した場合は、鍵のかかる机や金庫など安全な方法で保管すること

総務省『国民のための情報セキュリティサイト』（最終閲覧日：2020/2/25）
（https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/basic/privacy/01-2.html）を編集して作成

✽3. パスワードを複数のサービスで使い回さない（定期的な変更は不要）

パスワードはできる限り、複数のサービスで使い回さないようにしましょう。
あるサービスから流出したアカウント情報を使って、他のサービスへの不正ログインを試す攻撃の手口が知られています。もし重要情報を利用しているサービスで、他のサービスからの使い回しのパスワードを利用していた場合、他のサービスから何らかの原因でパスワードが漏洩してしまえば、第三者に重要情報にアクセスされてしまう可能性があります。

なお、利用するサービスによっては、パスワードを定期的に変更することを求められることもありますが、実際にパスワードを破られアカウントが乗っ取られたり、サービス側から流出した事実がなければ、パスワードを変更する必要はありません。むしろ定期的な変更をすることで、パスワードの作り方がパターン化し簡単なものになることや、使い回しをするようになることの方が問題となります。定期的に変更するよりも、機器やサービスの間で使い回しのない、固有のパスワードを設定することが求められます。

これまでは、パスワードの定期的な変更が推奨されていましたが、2017 年に、米国国立標準技術研究所（NIST）からガイドラインとして、サービスを提供する側がパスワードの定期的な変更を要求すべきではない旨が示されたところです（※１）。また、日本においても、内閣サイバーセキュリティセンター（NISC）から、**パスワードを定期変更する必要はなく、流出時に速やかに変更する**旨が示されています（※２）。

（※ 1）NIST SP800-63B（電子的認証に関するガイドライン）
（※ 2）https://www.nisc.go.jp/security-site/handbook/index.html

引用：総務省『国民のための情報セキュリティサイト』（最終閲覧日：2020/2/25）
（https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/basic/privacy/01-2.html）

迷惑メールへの対応

受信者が望んでいないにもかかわらず、一方的に送信されてくる電子メールのことを**迷惑メール**と呼んでいます。いわゆる「出会い系サイト」やドラッグなどの商品の宣伝などを内容とする電子メールが多く、**スパムメールとも呼ばれます**。

これらの電子メールは、昼夜を問わずに届けられ、電子メールをダウンロードするために時間がかかるなど、受信者側に大きな負担をかけるため、最近では社会問題のひとつになっています。また、いやがらせのために送りつけられる大量の無意味な電子メールも、迷惑メールの一種といえます。

迷惑メールの対策としては、ホームページのアンケートや電子掲示板などにメールアドレスをむやみに掲載しないことや、使用するメールアドレスは、わかりにくいものにするなどが考えられます。

引用：総務省『国民のための情報セキュリティサイト』（最終閲覧日：2020/2/25）

（https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/enduser/security02/10.html）

さらに注意が必要なのは、このような迷惑メールで送信される内容をうかつに信用してはいけないということです。これらの電子メールの中には、無限連鎖防止法に抵触するもの（いわゆるねずみ講）や詐欺行為を目的としているものもあります。

最近では、携帯電話やSNSのメッセージでの迷惑メールの急増が問題化しています。このような迷惑メールを受信しないようにするためには、

◆長く複雑なメールアドレスを使用する。
◆指定したドメインやメールアドレスからの電子メールのみ受信するように設定する。
◆必要以上に自分のアドレスを他人に漏らさない。
◆SNSのメッセージでの迷惑メールの場合は、利用しているSNSサービスの機能を使って、メッセージを拒否する、もしくは相手をブロックする。

など、利用者側でできる自衛策も大変有効です。携帯電話による迷惑メール対策の一環として実施してみましょう。

なお、受信者の望んでいない広告メールを送信する際には、「今後送信を必要としない場合にはこちらのメールアドレスまでご連絡ください」といった内容を記載することが法律で義務付けられていますが、その意思を伝える際には、**相手側に氏名・住所などの個人情報をむやみに開示しないように気を付けましょう。**悪意を持って、迷惑メールを送信してくる業者は、このような意思を伝えた際に、その送信元の電子メールアドレスが使われていることを確認できることにもなります。そして、その後も迷惑メールが送信され続けるという被害も起こっています。

総務省『国民のための情報セキュリティサイト』（最終閲覧日：2020/2/25）
（https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/enduser/security02/10.html）を編集して作成

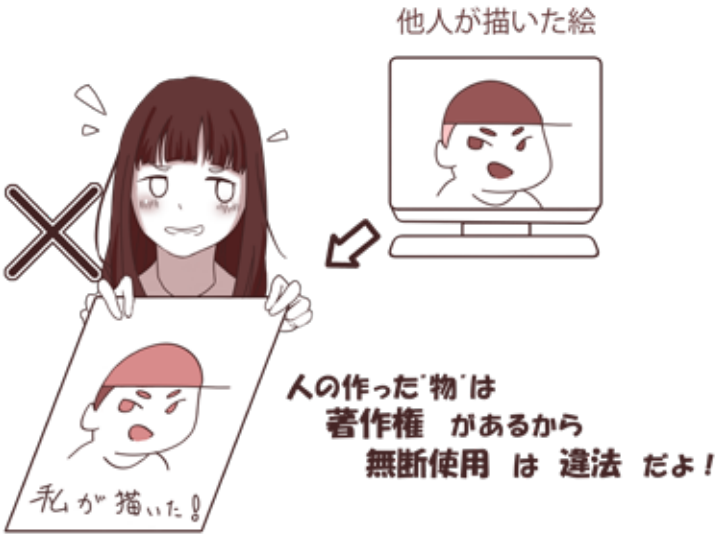
著作権侵害に注意

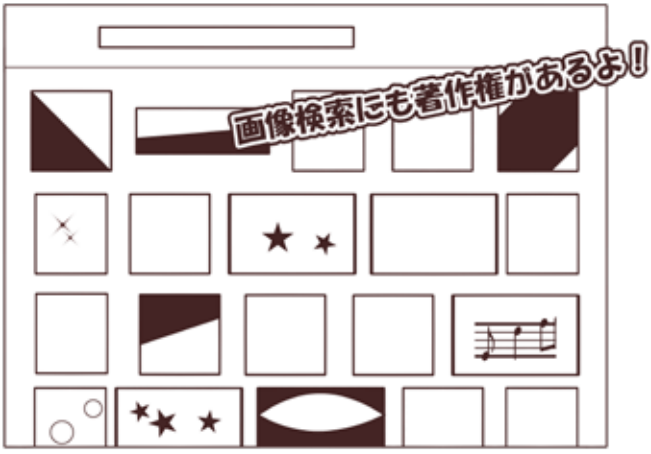
情報を発信する際には、著作権の侵害に注意しなければなりません。
写真、イラスト、音楽など、インターネットのホームページや電子掲示板などに掲載されているほとんどのものは誰かが著作権を有しています。
これらを、権利者の許諾を得ないで複製することや、インターネット上に掲載して誰でもアクセスできる状態にすることなどは、著作権侵害にあたります。また、新聞や雑誌などの記事にも著作権があり、引用の範囲を越えて掲載すると著作権侵害にあたるため、注意しましょう。

また、人物の写真などの場合は、撮った人などが著作権を有するだけではなく、写っている人に肖像権があるため、ホームページに掲載する場合にはこれらすべての権利者の許諾が必要になる場合があります。

情報を発信する際に、市販の素材集（絵や写真など）やインターネットに素材を提供しているホームページなどでは、これらを利用する場合に権利者による許諾の必要がない旨を記載されていることがあります。しかし、そのような素材であっても、商業利用については制限がかけられていることがあるため、必ず規約をよく読んでから利用するようにしましょう。

引用：総務省『国民のための情報セキュリティサイト』（最終閲覧日：2020/2/25）
（https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/enduser/attention/01.html）


他人が描いた絵
私が描いた！
人の作った"物"は
著作権 があるから
無断使用 は 違法 だよ！


画像検索にも著作権があるよ！

SNS 利用上の注意点

SNS は、Social Networking Service の略語です。
インターネット上では、日本中あるいは世界中のたくさんの人たちがさまざまな意見や思想を持ちながら活動しています。

今や、X（旧Twitter）・Instagram・Facebook といった SNS は、若者のみならずほぼ全世代に渡って利用されるものとなりました。時間や場所を問わず自分が情報を投稿したり、他人が投稿した情報を閲覧したりできるので、便利ですよね。
しかし、気軽に情報を発信できてしまうからこそ「人を誹謗中傷する内容を投稿しない」「位置情報の付いた写真を投稿しない」等、自他共に気をつけなければならないことがたくさんあります。（理由の一部は次ページ参照してください）

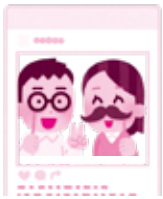
例え友人限定で情報を公開していたとしても、内容を他にコピー＆ペーストされてしまったら簡単に拡散されていきます。一度インターネット上に投稿した情報の完全回収は、不可能に等しいのです。

SNS 上とはいえ社会的マナーは必須です。犯罪に巻き込まれたり巻き込んだり、トラブルになることがないよう、**マナーを守って慎重に SNS を利用してください。**

大学生活の中で少しでも多く「情報」に関する知識を身に付け、社会に出る準備をしましょう。

✤気をつけるべき事例を３パターンご紹介します

・他人の写真を許可無く勝手に SNS 等のネットワーク上にアップロードするのは、プライバシーの侵害にあたり、違法行為となります。
どうしてもアップロードしたい場合には、
相手に許可を得てからにしましょう。

SNS に写真載せてもいい？＞  ＜いいよ！

・位置情報が登録されている写真は SNS にアップロードしないようにしましょう。例えば、旅行中であることが知られ空き巣に入られたり、知らない人に自分の活動域を把握されかねません。

今ここで遊んでいるのか…＞ 

・相手を誹謗中傷するような投稿をした場合は「人権侵害」となり、発言の責任を追及される可能性もあります。匿名で投稿したとしても、IP アドレス等で情報発信者を特定できてしまいます。