カリキュラム1

IT リテラシー・AI の基本

第2回：インターネットの基礎と安全な利用

～インターネットの仕組みとセキュリティを理解する～

目次

第 1 章.インターネットの基本概念

1. はじめに

この章では、インターネットの仕組みについて、初心者の方にもわかりやすく解説していきます。

私たちが毎日使っている SNS や動画視聴、インターネット検索、ネットショッピング、そしてオンラインゲーム。こうした便利なサービスは、すべてインターネットという巨大なネットワークの仕組みの上で成り立っています。

でも、その裏側で何が起きているのか、詳しく知っている人は意外と少ないかもしれません。

この講座では、インターネットで情報がどのように届くのか、どんなルールで動いているのか、そして安全に使うために気をつけるポイントまで、じっくりと解説していきます。

それでは一緒に、インターネットの世界をのぞいてみましょう！

2. パケット通信とインターネットの流れ

インターネットの基礎となる「パケット通信」と「インターネットの流れ」について

私たちが普段何気なく使っているウェブサイトの閲覧、動画の再生、メールの送受信、SNS の利用。これらはすべて、インターネットという巨大なネットワークを通じてデータをやり取りすることで成り立っています。

でも、そのデータはどのようにして世界中を行き来しているのでしょうか？ ここで登場するのが「パケット通信」という仕組みです。

インターネットでは、画像や動画、テキストといった大きなデータを一度にまるごと送るのではなく、「パケット」と呼ばれる小さなかたまりに分割して送信します。それぞれのパケットは、異

なる経路を通って目的地まで届けられ、最後にもう一度、ひとつのデータとして組み立てられます。

この方法には多くの利点があります。まず、ネットワークの混雑に応じてルートを変更できるため、効率よくデータを送ることができます。また、もし一部のパケットが途中で失われても、再送する仕組みがあるので、通信の信頼性が保たれるのです。

では、パケットは実際にどのような経路を通るのでしょうか？

たとえば、あなたが自宅のパソコンで動画サイトにアクセスしたとします。まず、そのリクエストはパケットとして、家庭用のルーターやモデムを経由し、インターネット・サービス・プロバイダー、いわゆる ISP のネットワークに送られます。

そこからインターネットのコアネットワークに入り、複数のルーターという中継装置を通って、目的のサーバーへと向かっていきます。サーバーに届いたパケットに対して、サーバー側は動画のデータを同じようにパケットとして分割し、再びインターネットを通じてあなたのパソコンへと送り返してくるのです。

この仕組みは、まるで郵便のように、住所に従って荷物を小分けにして届けるイメージです。ただし、パケットはそれぞれ別々のルートを選ぶことができるという点で、もっと柔軟でスマートな配送方法と言えるでしょう。

ここで重要なのが、「TCP/IP」という通信のための基本ルールです。

TCP は、送る順番の管理やデータの欠損チェック、再送の指示を出す役割を持ちます。一方、IP は送信先や送信元を指定するための“住所”、つまり IP アドレスの役割を担っています。

たとえば、あなたが見たい動画が正しく順番通りに再生されるのは、この TCP の働きによるものです。そして、世界中のどのサーバーと通信するかを決めるのが、IP アドレスの力です。

このように、TCP と IP が連携することで、信頼性が高く、効率的な通信が可能になっている

のです。

さらに、パケット通信はインターネットだけでなく、社内ネットワーク、スマートフォンのモバイル通信、そして最近では IoT 機器にも活用されています。つまり、私たちの身の回りのあらゆるデジタル機器が、パケット通信によって情報をやり取りしているのです。

この仕組みを知ることは、インターネットをより深く理解する第一歩です。たとえば、回線が遅い、動画が止まるといったトラブルの原因が、ネットワークのどこにあるのかを予測しやすくなります。

パケット通信は、インターネットの血液のような存在。目には見えませんが、日々無数のパケットが世界中を駆け回り、私たちの生活を支えてくれているのです。

3. IP アドレスとドメインの役割

次は「IP アドレス」と「ドメイン名」の役割について学んでいきましょう。

私たちが普段インターネットでウェブサイトを見たり、メールを送ったり、アプリを使ったりするとき、実は通信相手を正しく見つけ出すために必要な「住所」が使われています。それが「IP アドレス」です。

IP アドレスとは、インターネットに接続されたすべての機器に割り当てられている固有の番号のことです。たとえば、142.250.196.78 のような数字の列がそれです。これによって、あなたのスマホやパソコンがどこにデータを送ればいいのかを正確に判断することができます。

ですが、数字の羅列は覚えづらいですよね？ そこで登場するのが「ドメイン名」です。これは、人間にとって覚えやすい名前で、IP アドレスの代わりに使えるようになっています。

たとえば、「google.com」や「yahoo.co.jp」といった名前がドメイン名にあたります。私たちは URL を入力するときにこのようなドメイン名を使いますが、裏ではちゃんと IP アドレスに変換されているんです。

この変換を行っているのが「DNS」、つまりドメインネームシステムです。

DNS は、インターネット上にある「名前と番号の対応表」のようなものです。ドメイン名を入力すると、自動的に対応する IP アドレスが探し出され、そのアドレスを使って目的のサーバーに接続することができます。

たとえば、あなたが「www.example.com」というウェブサイトを見たいと入力すると、DNS がこのドメイン名に対応する IP アドレスを調べてくれます。そして、その IP アドレスに向けてデータのリクエストが送信される、というわけです。

このように、ドメイン名は「人間のための住所」、IP アドレスは「コンピュータのための住所」と言えます。

DNS は階層構造を持っていて、インターネット全体の中で効率よく検索できるように工夫されています。私たちが入力したドメイン名は、複数の DNS サーバを通じて、目的のアドレスが見つかるまでたどっていきます。まるで迷路の中を抜けて、正解の鍵を探すようなイメージです。

もう一つ大事なことがあります。それは、ドメイン名には種類があるということです。

たとえば、「.com」は商業用、「.net」はネットワーク用、「.org」は非営利組織用というように、それぞれ用途や目的に応じた種類があります。これらは「gTLD（ジェネリック・トップレベル・ドメイン）」と呼ばれます。

一方で、「.jp」や「.us」など、国や地域ごとに割り当てられたドメインもあります。これらは「ccTLD（カントリーコード・トップレベル・ドメイン）」と呼ばれます。

日本で使われる「.jp」や、アメリカの「.us」、イギリスの「.uk」などがその例です。つまり、ドメインを見るだけでも、そのサイトがどこに属しているのか、おおよその見当をつけることができます。

また、企業や団体では、自社名にちなんだドメインを取得することで、信頼性やブランドイメージを高めています。最近では「.tokyo」や「.shop」といった新しい TLD も登場しており、ドメインの世界もますます多様化しています。

IP アドレスとドメイン名の仕組みを知ることで、普段何気なく使っているインターネットの裏側にある、見えない仕組みへの理解が深まります。

たとえば、もしドメイン名に似せた偽サイトが表示されたときにも、「あれ、このドメイン名ちょっとおかしいな」と気づくことができるかもしれません。

正しいドメインを見分ける目を養うことは、インターネットを安全に使う第一歩です。IP アドレスや DNS のしくみを理解しておくと、ネットワークのトラブルにも強くなれます。

これらの知識を、ぜひ普段のネット利用の中でも意識してみてください。

4. URL の構造と読み解き方

ここでは、Web ページの住所ともいえる「URL」の構造について解説していきます。

URL とは「Uniform Resource Locator（ユニフォーム・リソース・ロケーター）」の略で、インターネット上の情報がどこにあるのかを示す“住所”のような役割をしています。

たとえば、次のような URL を見てみましょう。

https://www.example.com/news?article=123

この URL には 4 つの構成要素があります。

最初の「https://」は“スキーム”と呼ばれる部分で、どのような通信方法でアクセスするかを示します。「https」は、暗号化された安全な通信を意味します。

次の「www.example.com」は“ドメイン名”です。このドメイン名が、インターネット上のどのサーバーにアクセスするかを決める鍵となります。

その次の「/news」は“パス”と呼ばれ、サーバー内のどのページやファイルにアクセスするかを指定しています。

そして最後の「?article=123」は“クエリ”と呼ばれ、追加情報を伝えるために使われます。この場合、記事番号「123」を指定している、という意味になります。

このように、URL はただの文字列ではなく、非常に論理的に構成されています。それぞれの要素がどんな役割を持っているのかを知ることで、トラブル時の対応や、安全なサイトの見分けにも役立ちます。

また、最近ではスマホアプリでもリンクが共有されることが多くなってきました。リンクをタップする前に、URL のドメインやクエリ部分を確認する習慣を持つことも、セキュリティ対策としてとても大切です。

今後インターネットを利用する上で、URL の構造を理解しておくことはとても役立ちますので、ぜひ覚えておきましょう。

5. クライアント・サーバモデルと HTTP/HTTPS

「クライアント・サーバモデル」と「HTTP／HTTPS」の仕組みについて解説します。

インターネット上で情報をやり取りするとき、必ず登場するのが「クライアント」と「サーバ」という 2 つの役割です。

まず「クライアント」とは、皆さんが使っているパソコンやスマートフォンなど、情報を受け取る側の機器のことを指します。一方、「サーバ」は、情報を提供する側のコンピュータです。たとえば、Web ページや動画、メール、オンラインゲームのデータを保存し、必要に応じて配信する役割を持っています。

このように、クライアントとサーバがやり取りをしながら情報を交換する関係を「クライアント・サーバモデル」と呼びます。

たとえば、皆さんが Web ブラウザで「検索」をするとします。クライアントであるあなたのスマートフォンが、検索内容をリクエストとして送信します。このリクエストはインターネットを通じてサーバに届き、サーバがその検索結果をまとめて、レスポンスとしてクライアントに返す。これが、日々私たちが行っている Web の基本的な仕組みです。

このとき、やり取りのルールとして使われているのが「HTTP」や「HTTPS」という通信プロトコルです。

HTTP とは「HyperText Transfer Protocol（ハイパーテキスト・トランスファー・プロトコル）」の略で、Web ページの情報をやり取りするための決まりごとのようなものです。リクエストを送信し、レスポンスを受け取る際には、HTTP に従った形式でデータがやり取りされます。

ただし、HTTP にはひとつ問題があります。それは「通信内容が暗号化されていない」という点です。つまり、途中で誰かが通信内容をのぞき見ることが可能である、ということです。

たとえば、公共 Wi-Fi を使っているときに HTTP で送信したパスワードやメッセージが、悪意ある第三者に読み取られてしまうリスクがあるのです。

そこで登場するのが「HTTPS」です。「S」は「Secure（安全な）」の略で、通信内容を暗号化する機能が追加されたプロトコルです。

HTTPS を使うと、クライアントとサーバの間で交わされる情報がすべて暗号化されるため、第三者に盗み見られたり、改ざんされたりする危険性が大きく下がります。

最近では、ショッピングサイトやオンラインバンキングなど、個人情報を扱うサービスの多くが HTTPS に対応しています。また、Google などの検索エンジンも、HTTPS 対応サイトを優先して表示するようになってきており、Web の標準になりつつあります。

さらに、近年では Web ブラウザが HTTP のみのサイトに「保護されていません」という警告を表示するようになり、多くのサイト運営者が HTTPS への移行を急いでいます。

ブラウザで Web ページを表示するとき、URL の先頭が「https://」になっているかどうかをチェックすることで、そのサイトが暗号化されているかを確認できます。さらに、多くのブラウザでは、URL の左に鍵マークが表示されていることでも、安全性を判断できます。

このように、クライアントとサーバが適切に通信し、暗号化を用いて安全性を保つことが、快適で安心なインターネット利用につながっています。

私たちは普段、意識せずに Web サイトを閲覧していますが、その背後にはこうした通信のやり取りが常に発生しています。

この「クライアント・サーバモデル」と「HTTP／HTTPS」の仕組みを知ることで、インターネットをより深く理解でき、トラブル対応や安全確認にも役立つようになります。

6. 安全なインターネット利用のポイント

最後に、安全にインターネットを利用するためのポイントについてご紹介します。

インターネットはとても便利な道具ですが、正しい知識と注意がないと、思わぬトラブルに巻き込まれることもあります。ここでは、初心者でも実践できる大切な 3 つのポイントを確認しましょう。

1. 「URL をよく確認すること」です。とくに「https://」で始まっているかどうかをチェックしましょう。

「https」は安全な通信を意味しており、情報が暗号化されて送られます。逆に「http」だけのサイトは、通信内容が第三者に見られる危険性があります。また、URL のドメイン名が本物かどうかも大切です。たとえば「amaz0n.co」や「gooogle.net」など、一見すると本物に見える偽サイトもあるので注意しましょう。

2,「個人情報をむやみに入力しないこと」です。氏名、住所、電話番号、パスワード、クレジットカード情報などは、信頼できるサイト以外には絶対に入力しないようにしましょう。もし不安な場合は、入力前にそのサイトの評判や運営会社を調べると安心です。あわせて、不審なメールや SMS のリンクは、むやみに開かないようにすることも重要です。

3,「セキュリティ対策ソフトを導入すること」です。ウイルスやスパイウェア、不正アクセスなどの脅威から自分のパソコンやスマートフォンを守るために、信頼性の高いセキュリティソフトを使い、常に最新の状態に保つことが大切です。更新を怠ると、新しい脅威に対応できなくなるため、必ず自動更新を有効にしておきましょう。

また、パスワードの使い回しを避ける、多要素認証を活用するなど、日常のちょっとした心がけでも安全性を高めることができます。

インターネットは正しく使えば、とても便利で楽しいツールです。今日ご紹介したポイントを意識して、安全にインターネットを活用していきましょう。

7. まとめ

今回の講義では、インターネットの仕組みや安全な使い方について、基本的な内容を学んできました。

パケット通信、IP アドレスとドメイン、URL の構造、クライアント・サーバモデル、HTTP と HTTPS の違い、そして安全に使うための具体的なポイントまで、インターネットを正しく理解するための基礎を一通り確認しました。

これらは、普段何気なく使っているネットの裏側で実際に働いている仕組みです。仕組みを知ることで、トラブルを防ぎ、安心して活用できるようになります。今後は、今日学んだ内容を意識しながら、正しく・安全にインターネットを使いこなしていってください。

第2章安全なインターネット利用

1. はじめに

この章では、インターネットを安全に使うための基本的なポイントを学んでいきましょう。

今やスマートフォンやパソコンを使って、SNS を楽しんだり、ネットショッピングをしたりするのは当たり前の時代です。でも、その便利さの裏には、個人情報の流出やウイルス感染といった危険が潜んでいます。ちょっとした油断が、大きなトラブルに繋がることもあるのです。

今回は、そうしたトラブルを未然に防ぐための知識として、「安全なパスワードの作り方」や、「フィッシング詐欺などのネット犯罪を見分けるコツ」、そして「セキュリティソフトの役割と必要性」などについて、わかりやすく解説していきます。

誰もが安心してインターネットを使えるように、しっかりと学んでいきましょう！

2. パスワード管理

「パスワード管理」について、詳しく解説していきます。

私たちが日々使っているインターネットの世界では、たくさんの個人情報や大切なデータがやり取りされています。SNS、ショッピング、動画配信、クラウドサービス、オンラインバンキングなど、あらゆるサービスを利用するたびに、私たちはパスワードという“鍵”を使って自分の情報を守っています。

このパスワード、実は思っている以上に重要なんです。家の鍵と同じように、パスワードがしっかりしていなければ、誰かが簡単に中に入ってきてしまいます。つまり、パスワードが弱いと、あなたの大切な個人情報やアカウントが、見知らぬ誰かに盗まれてしまうリスクが高くなるのです。

では、実際にどんなパスワードが「危ない」のか、いくつか例を挙げてみましょう。

たとえば、「123456」や「password」といった単純な文字列。これは毎年、最も使われているパスワードのランキングに入っており、ハッカーにとっては最初に試すような典型的なパスワードです。

また、「tanaka2024」のように自分の名前と年号を組み合わせただけのものや、「abcd1234」といったキーボードの並び順に沿ったパターンも非常に危険です。これらは、短時間で自動的に試されてしまう可能性があるため、セキュリティとしては非常に弱いとされています。

では、どうすれば安全なパスワードを作れるのでしょうか。ここでは、信頼性の高いパスワードを作るための 4 つのポイントを紹介します。

1,「8 文字以上にする」ことです。最近では 12 文字以上を推奨するサービスも増えてきました。文字数が多いほど、突破されにくくなります。

2,「英大文字・小文字・数字・記号を組み合わせる」ことです。たとえば、「F!9gT$e7」といったように、さまざまな種類の文字を混ぜることで、予測されにくいパスワードになります。

3,「名前・誕生日・電話番号など、推測しやすい情報を使わない」ことです。SNS や履歴書、名刺など、さまざまなところから情報が流出する時代です。身近な情報をパスワードに使うのは避けましょう。

4,「同じパスワードを複数のサービスで使い回さない」ことです。もし一つのサービスでパスワードが漏れてしまったら、他のサービスにも一気にアクセスされてしまう危険があります。できる限り、サービスごとに異なるパスワードを設定しましょう。

ただし、たくさんの複雑なパスワードを自分で覚えるのは難しいですよね。そこで役に立つのが、「パスワードマネージャー」というツールです。

パスワードマネージャーは、安全にパスワードを管理してくれるアプリケーションで、一度マスターパスワードを設定すれば、あとは自動的に各サイトごとのパスワードを保存し、必要なときに呼び出してくれます。代表的なものには、ワンパスワード、ラストパス、ビットワーデンなどがあります。

これらのツールは、パスワードの生成もしてくれるので、自分で複雑なパスワードを考える手間も省けますし、入力の手間も軽減されます。

最近では、スマートフォンやブラウザにもパスワード管理機能が標準搭載されており、Google Chrome や Safari、Android や iOS の「キーチェーン」なども便利です。ただし、端末を紛失した場合や他人に使われた場合に備えて、スマホや PC にも必ずロックをかけておくことが大切です。

また、パスワードとセットで活用したいのが、「2 段階認証もしくは 2 要素認証」です。これは、パスワードに加えて、スマホに送られてくる確認コードや専用アプリの認証を通してログインする仕組みです。万が一、パスワードが漏れたとしても、不正アクセスを防ぐ最後の砦になります。設定に少し手間はかかりますが、安心を買うためのとても効果的な方法です。

では最後に、今日のポイントをまとめましょう。

1 つ目、パスワードは 8 文字以上、できれば 12 文字以上にし、できるだけ複雑な文字の組み合わせを使いましょう。
2 つ目、誕生日や名前などの個人情報は使わず、予測されにくいパターンを作ること。
3 つ目、使い回しはせず、サービスごとに異なるパスワードを設定すること。
そして 4 つ目、覚えきれない場合は、パスワードマネージャーを活用すること。

さらに、2 段階認証も積極的に導入して、セキュリティを高めましょう。

これで、パスワード管理に関する説明は終わりです。次のセクションでは、フィッシング詐欺やウイルスなどのリスクと、その対策について解説していきます。引き続き、しっかりと学んでいきましょう。

3. フィッシング詐欺とウイルスのリスク

インターネットを利用するうえで非常に重要なテーマである「フィッシング詐欺」と「ウイルス感染のリスク」について説明します。

スマートフォンやパソコンが生活に欠かせない道具となった今、私たちはさまざまな情報に囲まれて暮らしています。その一方で、悪意のある第三者が、私たちの個人情報を盗んだり、金銭を騙し取ろうとするケースが後を絶ちません。これらのネット上の脅威の中でも、特に注意すべきものが「フィッシング詐欺」と「ウイルス感染」です。

◯「フィッシング詐欺」

フィッシング詐欺とは、一見すると本物の企業やサービスから送られてきたように見せかけたメールや SMS、偽の Web サイトなどを使って、ユーザーの ID やパスワード、クレジットカード情報などの個人情報を盗み取ろうとする詐欺行為です。

たとえば、「〇〇銀行からのお知らせ」「Amazon のアカウントに異常があります」「あなたのアカウントは一時停止されています」といったタイトルでメールが届き、本文には「今すぐログインして確認してください」というリンクが記載されています。そのリンクをクリックすると、見た目は本物そっくりなログイン画面に誘導され、そこに自分の ID やパスワードを入力してしまうと、情報がそのまま詐欺グループに送られてしまうという仕組みです。

非常に巧妙な手口で、公式のロゴやデザインを完璧に真似しているため、よく見ないと本物かどうかの判断が難しい場合もあります。

では、こういったフィッシング詐欺を見抜くにはどうすればよいのでしょうか？

ここでは、いくつかのチェックポイントをご紹介します。

1，差出人アドレスが怪しいことです。

メールの差出人の名前は「〇〇銀行」や「Amazon」など本物っぽく表示されていますが、実際のメールアドレスを見ると、「@xyzservice.com」など、公式のドメインとは異なる不自然なものになっていることが多くあります。たとえば「@amazon.co.jp」ではなく「@amazonsupport.net」など、よく見ると違和感のある文字列が使われています。

2，日本語に不自然さがあることです。

本文の日本語に誤字脱字があったり、言い回しが不自然だったりすることもフィッシング詐欺の特徴です。特に海外の詐欺グループが自動翻訳などで作成したメールの場合、文法的に変な日本語が使われていることがよくあります。

3，不安をあおるような文言が多いという点です。

「アカウントが停止されました」「不正アクセスの可能性があります」「〇時間以内に対応しないと削除されます」といった、ユーザーの不安をあおるような言葉が繰り返されている場合は、冷静に一度立ち止まってください。焦ってクリックしてしまわないようにすることが大切です。

4，リンク先 URL をよく確認することです。

メールや SMS に記載されているリンク先 URL が、公式サイトのアドレスと少しでも異なる場合は、絶対にクリックしないようにしましょう。最近は「www.amazon.co.jp.xxxxxx.com」のように、本物のドメインが前についていても、実際には全く無関係な偽サイトであることもあります。

こういったフィッシング詐欺に遭わないためには、以下のような対策が有効です。

メールや SMS のリンクをすぐにクリックせず、まずは公式アプリや公式サイトにアクセスして情報を確認すること。ブラウザにブックマークした公式ページからログインするようにするのが安全です。フィッシング対策機能が付いたセキュリティソフトを導入しておくと、怪しいサイトへのアクセスをブロックしてくれます。スマホの場合は、設定で SMS の迷惑フィルターを有効にしておきましょう。

◯「ウイルス感染」

ウイルスとは、コンピュータやスマートフォンに侵入し、データを壊したり、勝手に情報を外部に送信したりする悪質なプログラムのことです。広い意味では、「マルウェア」と呼ばれることもあります。これは「malicious software」、つまり悪意あるソフトウェアの略語です。

■ウイルスに感染すると、次のような被害が起こる可能性があります。

パソコンの動作が極端に遅くなる。保存していたファイルや写真が勝手に削除されたり、暗号化されて開けなくなる。入力したパスワードやクレジットカード情報が外部に送信される。勝手にメールやメッセージが他人に送られる。端末が遠隔操作され、知らないうちに不正アクセスの踏み台にされる。

とくに最近多いのが「ランサムウェア」と呼ばれるタイプのウイルスです。これはファイルを暗号化して開けないようにし、「元に戻したければお金を払え」と脅してくる非常に悪質な手口です。

■こうしたウイルスは、どこから感染するのでしょうか。

原因としては、怪しいメールの添付ファイルを開いたとき、信用できないサイトからファイルをダウンロードしたとき、海賊版ソフトや動画、音楽などを違法に入手しようとしたとき、古いバージョンの OS やソフトウェアを使い続けているとき、などが挙げられます。

たとえば「請求書の確認」などと書かれた PDF や Word ファイルを開くだけでウイルスが起動することもあります。感染は、ほんの一瞬の油断から始まります。

■こうしたウイルス感染を防ぐためには、どうしたらよいのでしょうか。

セキュリティソフトを必ずインストールし、常に最新の状態に保つこと。OS やアプリ、ブラウザのアップデートを定期的に行うこと。不審なメールや添付ファイルは絶対に開かないこと。知らないサイトからソフトをダウンロードしないこと。定期的にウイルススキャンを実行する習慣をつけること。スマートフォンにもウイルス対策アプリを導入して、安全性を高めましょう。

フィッシング詐欺とウイルス感染は、誰にでも起こり得るネット上のリスクです。しかし、ちょっとした注意と習慣によって、被害を未然に防ぐことができます。

メールやリンクはすぐに信用せず、まずは落ち着いて差出人や URL を確認すること。セキュリティソフトを活用し、常に最新の状態を保つこと。不審なものには「触れない・開かない・ダウンロードしない」。これらを意識するだけで、あなたのデジタルライフはぐっと安全なものになります。

次のパートでは、ウイルス対策ソフトについて、もう少し具体的にご紹介していきます。引き続き、しっかり学んでいきましょう。

4. セキュリティソフトの基本知識

ここまで、フィッシング詐欺やウイルス感染など、インターネットを使う上での危険についてお話ししてきました。では、これらのリスクから自分の情報やデバイスを守るためには、どんな対策が有効なのでしょうか。

◯セキュリティソフトの導入です。

セキュリティソフトとは、ウイルスやマルウェアといった有害なプログラムを検出して除去したり、インターネット上の危険なサイトや不正なアクセスをブロックしてくれるソフトウェアのことです。いわば、あなたのパソコンやスマートフォンを守る、デジタルの番犬のような存在です。

では、実際にセキュリティソフトにはどんな機能があるのでしょうか。代表的な機能を、四つに分けてご紹介します。

1，ウイルスやマルウェアの検出と除去です。

これはセキュリティソフトの基本的な機能で、日々更新されるウイルスの情報データベースと照らし合わせながら、パソコンやスマホ内のファイルをスキャンし、怪しい動きをするファイルやプログラムを検出し、隔離したり削除したりしてくれます。最新の脅威にも対応するためには、ウイルス定義ファイルの自動アップデートをオンにしておくことが重要です。

2，危険なサイトへのアクセスをブロックする機能です。

最近では、フィッシング詐欺やマルウェアを仕込んだ Web サイトが増えています。こういったサイトにアクセスしようとすると、セキュリティソフトが警告を表示してアクセスを止めてくれるため、うっかりクリックしてしまっても、被害を未然に防ぐことができます。

3，個人情報の保護機能です。

これは、ネットバンキングやオンラインショッピングなど、個人情報を入力する場面で効果を発揮します。入力フォームにセキュリティレイヤーをかけたり、不審なプログラムが入力内容を盗み見ようとする動きを防ぐことができます。たとえば、キーボードの入力を記録するキーロガーへの対策や、金融機関専用の安全なブラウザを使う機能などがあります。

4，定期的なスキャン機能です。

セキュリティソフトは、普段の操作中もリアルタイムで監視していますが、それに加えて、定期的にシステム全体をスキャンして、潜在的なリスクをチェックする機能も備えています。スキャンの頻度は、毎日、毎週、月に一回など、自由に設定することができ、夜間など作業の邪魔にならない時間帯に自動で行うようにしておくと便利です。

これらの基本機能に加えて、最近のセキュリティソフトにはさらに便利な追加機能が搭載されています。

たとえば、保護者機能によって子どものインターネット利用時間や閲覧内容を制限するペアレンタルコントロール、SNS の個人情報保護、迷惑メールのフィルタリング、VPN 機能による通信の暗号化なども製品によって用意されています。

◯誤解されやすいポイントがあります。

「Windows のパソコンには、最初から Windows Defender というセキュリティ機能が入っているから、それで十分ではないか」と思う方もいるかもしれません。

確かに、Windows Defender は Windows10 以降の OS に標準で搭載されており、基本的なウイルス検出やファイアウォール管理ができます。しかし、市販のセキュリティソフトと比べると、検出精度やフィッシング詐欺への対応、使いやすさ、そしてサポート体制などにおいて差があるのも事実です。

特に、ネットバンキングの保護や個人情報漏えい対策、ランサムウェア対策などをしっかり行いたい場合は、有料のセキュリティソフトを検討することをおすすめします。

◯代表的なセキュリティソフトをいくつかご紹介します。

ウイルスバスター、ノートン 360、カスペルスキー、ESET、マカフィー、Bitdefender などがあり、それぞれに特徴があります。

動作の軽さを重視するなら ESET、ネットバンキングの保護を強化したい場合はカスペルスキー、複数の端末をまとめて保護したいならノートンや Bitdefender が選ばれています。（異なる見解もありますので、ご自身にてご判断下さい。）

また最近では、スマートフォン向けのセキュリティアプリも豊富に提供されており、Android や iPhone でも利用できます。特に Android は、アプリの自由度が高い反面、ウイルス感染のリスクもあるため、セキュリティアプリの導入をおすすめします。

最後に、セキュリティソフトを導入した後に忘れてはいけないのが、定期的なアップデートとスキャンの実行です。

インターネットの脅威は日々進化しています。昨日まで安全だったサイトやファイルが、今日は危険になっているということもあります。

自分の大切なデータを守るためにも、セキュリティソフトをうまく活用し、安心・安全なインターネットライフを送りましょう。

5. まとめ

◯インターネットを安全に利用するための基本的な知識について、一緒に学んできました。

今日のまとめとして、大切なポイントを 3 つに整理してお伝えします。

1,「強力でユニークなパスワードを使うこと」です。

パスワードは、あなたの大切な情報を守る“鍵”です。短くて単純なものは、簡単に突破されてしまいます。英大文字・小文字・数字・記号を組み合わせ、できるだけ長く、そして他のサービスと使い回さないようにすることで、セキュリティが大きく向上します。

2,「怪しいメールやサイトには注意すること」。

一見すると本物に見えるメールやウェブサイトでも、リンク先や差出人をよく確認すると、不自然な点が見つかることがあります。「今すぐログイン」や「アカウントが停止されました」など、焦らせるような文言には特に注意が必要です。不審なメッセージは開かず、公式アプリやブックマークから確認する習慣を持ちましょう。

3,「セキュリティソフトを常に最新の状態に保つこと」です。

セキュリティソフトは、私たちのパソコンやスマートフォンを見守ってくれる大切な存在です。ただし、入れただけでは十分ではありません。ウイルスの種類や攻撃手法は日々進化しているため、ソフトを常に最新バージョンに更新し、定期的にスキャンを行うことが必要です。

以上の 3 つのポイントを意識するだけでも、インターネット上の多くのトラブルを未然に防ぐことができます。

安全なネット環境をつくるためには、一人ひとりの意識がとても大切です。今日学んだことを、日常の中でもぜひ意識して実践してみてください。

次回は、「ソフトウェアの基本操作」について学びます。実際の画面を使いながら、操作の基本をわかりやすく解説していきます。

第3章情報検索と信頼できる情報の見極め

1. はじめに

この章では、インターネットを使って情報を調べる方法や、正確で信頼できる情報を見つけるコツについて学びます。エスエヌエスや検索サイト、AI チャットなど、情報を得る手段はたくさんありますが、その情報が本当に正しいか、自信を持って言えるでしょうか？今日は、検索のコツと情報の見極め方を一緒に身につけましょう。

2. Google 検索の活用

◯Google 検索をもっと上手に使うための方法をご紹介します。

普段何かを調べるとき、「キーワードを入れて検索ボタンを押すだけ」になっていませんか？
もちろんそれでも情報は出てきますが、必要な情報を正確に、早く探すためには、ちょっとしたテクニックが役立ちます。

その一つが、「検索演算子（けんさくえんざんし）」という機能です。これは、検索キーワードの前後に特定の記号や言葉をつけることで、検索結果を絞り込んだり、除外したりすることができる便利な方法です。

それでは、代表的な検索演算子をいくつかご紹介しましょう。

1，ダブルクォーテーションで囲む方法です。

キーワードを「“人工知能”」のように、二重引用符で囲むと、完全にその言葉通りの並びで検索されます。
たとえば「人工知能」の意味をそのまま探したいときに便利です。

2,「site:」です。

これは、特定のウェブサイトやドメイン内だけを対象に検索したいときに使います。

たとえば「site:go.jp コロナ対策」と検索すると、日本政府の公式ドメインである「go.jp」内から、“コロナ対策”に関連する情報だけが表示されます。

信頼性の高い情報を探すときにとても便利ですね。

3,「filetype:」です。

これは、特定のファイル形式の資料を探すときに使います。

たとえば「filetype:pdf 人工知能」と検索すると、PDF 形式の資料だけが表示されるので、学術的なレポートや配布資料などを探したいときに重宝します。

4,「-（ハイフン）」です。

これは除外したいキーワードの前に使います。

たとえば「AI -映画」と入力すると、“AI”に関する情報の中でも、“映画”に関するものを除外して表示してくれます。

ノイズになる情報を減らしたいときに役立つテクニックです。

このように、検索演算子を上手に使うことで、必要な情報にぐっと早く、正確にたどり着くことができます。ちょっとした工夫で、あなたの検索力は大きくアップします。

3. チャット AI による検索活用

◯近年急速に普及している「チャット型 AI」を使った情報検索の活用法について

従来の Google 検索では、キーワードを入力して、ずらりと並んだ検索結果の中から、自分で必要な情報を探し出す必要がありました。しかし、最近では ChatGPT や Perplexity AI といった「対話型の AI」を使えば、もっと効率的に情報を探すことができるようになってきました。

では、実際にどのように使えるのか、具体的に見ていきましょう。

1，ChatGPT

ChatGPT は OpenAI が開発した AI チャットサービスで、ユーザーが入力した質問や指示に対して、自然な日本語で回答を返してくれます。

たとえば、「AI の活用事例をまとめてください」と入力すると、ChatGPT は医療、教育、製造業、農業など、さまざまな分野から代表的な活用事例をピックアップして一覧にしてくれます。

ここで注目したいのは、“単なる情報の羅列”ではなく、ChatGPT が要点を整理し、簡潔にまとめてくれるという点です。情報の要約が非常に得意で、「何が重要なのか」「どんな順番で説明すると分かりやすいか」を考慮した返答をしてくれます。

さらに、ChatGPT のもう一つの利点は「対話型であること」です。

たとえば、「AI の活用事例を教えて」と聞いた後に、「それは日本国内の話ですか？」と補足の質問をすると、ChatGPT はそれをきちんと文脈として理解し、「日本国内の事例では、たとえば〇〇という企業が……」といったように、さらに具体的な情報を返してくれます。

このように、会話のキャッチボールをするような感覚で検索ができるので、従来のキーワード検索に比べて、格段に深い情報が得られる可能性があります。

2. Perplexity AI について

Perplexity AI は、ChatGPT のような対話型の AI であると同時に、情報源を明示してくれるのが大きな特徴です。

たとえば、「最近の日本のインフレ率について教えて」と聞くと、Perplexity は最新のニュース記事や政府の統計データを元に答えを出し、さらにその情報の出典 URL まで表示してくれます。

つまり、「この情報はどこから来たのか？」という信頼性のチェックが非常にしやすくなっているのです。

また、Perplexity AI はリアルタイム検索機能にも強く、直近のトレンドやニュースにも素早く対応してくれる点も魅力です。ChatGPT が“学習済みの知識”に基づいているのに対し、Perplexity は“今まさに報じられていること”にアクセスできるという強みがあります。

ここで忘れてはいけないのが、「AI の回答が必ずしも正しいとは限らない」ということです。

たしかに AI は便利で、情報を素早く整理してくれる優れたツールですが、時には誤った情報を出したり、情報の出所が曖昧だったりすることもあります。

たとえば、ChatGPT が提供する情報は、2023 年 4 月以前のデータが中心であり、最新のニュースや変更された制度などは含まれていないことがあります。また、Perplexity AI でさえも、検索エンジンのランキングに影響されて、信頼性の低い情報が上位に表示されることもあります。

ですから、AI が出してきた情報をそのまま信じるのではなく、「本当に正しいのか？」「出典は明示されているか？」「他の情報と照らし合わせて矛盾はないか？」といった視点で、自分自身で確認することがとても重要です。

AI は“情報検索のパートナー”として非常に優れた存在ですが、その最終的な判断を下すのは“私たち自身”であることを忘れないようにしましょう。

このように、ChatGPT や Perplexity AI は、現代の情報検索においてとても便利でパワフルなツールです。上手に活用しながら、情報の質と信頼性を見極める力を身につけていきましょう。

4. フェイクニュースや誤情報の見分け方

フェイクニュース」や「誤情報」の見分け方

では次にいきましょう。インターネット上にあふれる「フェイクニュース」や「誤情報」の見分け方について詳しくお話ししていきます。 現代は、誰もが自由に情報を発信できる時代です。SNSやニュースアプリ、ブログ、動画プラットフォームなど、情報が日々あらゆる形で流れてきます。私たちはそれを受け取る側として、真偽を見極めながら情報に接する必要がありますが、現実には多くの人が、意図的に操作された情報や誤解を招くニュースに振り回されてしまうことがあります。

どのようにして私たちは信頼できる情報と、そうでない情報を見分ければいいのでしょうか？

ここでは、実際に役立つ視点とチェックポイントを、できるだけわかりやすくお伝えします。 まず第一に確認したいのは、その情報の「出典」、つまりどこから来たのかということです。情報の信ぴょう性を判断するには、その出どころが公的な機関や大学、専門家であることが重要です。政府機関の公式サイトや医療機関、大学の研究チームなど、信頼性のある組織名が明記されていれば、情報の正確性は高いと判断できます。一方、「ある著名人がこう言っていた」「SNS で話題になっている」といった曖昧な引用や、発信元が不明な情報は、まずは疑ってかかるべきです。

次に、「他の信頼できるメディアでも同じ情報が掲載されているかどうか」を確認することが大切です。

たとえば、新聞、テレビ、専門誌、公共機関のウェブサイトなど、複数の情報源で同じ事実が確認できれば、信ぴょう性はさらに高まります。逆に、その情報が一部のサイトや SNS 投稿にしか存在していない場合は、慎重に扱う必要があります。 また、その情報を「誰が発信しているのか」も重要なポイントです。肩書きや所属が明確で、専門的な知識や経験を持っている人の発信であれば、比較的信頼できます。ですが、SNS や動画サイトでは、匿名の人物や、

特定の思想に偏った情報を意図的に流しているケースも少なくありません。

さらに、「タイトルや見出しの表現」にも注意を払いましょう。

「衝撃の事実発覚！」「ついに〇〇が暴かれた！」といった、強い言葉で感情をあおるような表現には、気をつける必要があります。こうしたタイトルはクリックを誘うことを目的としており、記事の中身と一致しないことも多々あります。興味を引くように仕掛けられた“煽りタイトル”は、真実よりもバズや再生数を優先して作られている可能性があるのです。

そして、「情報の鮮度」も忘れずに確認しましょう。

インターネットには、数年前の記事がそのまま残っていることがあります。制度や法律、研究成果は日々更新されています。古い情報を鵜呑みにしてしまうと、間違った判断を下してしまう危険もあります。情報の日付や、最終更新日をチェックするクセを身につけましょう。ここで、フェイクニュースや誤情報を見分けるためのチェックポイントをまとめておきます。

◯見分けるためのチェックポイント

1. 出典が信頼できる機関かどうか
2. 他の複数の情報源でも同じ内容が確認できるか
3. 発信者の名前・立場・専門性が明示されているか
4. 感情的な表現や煽りタイトルが使われていないか
5. 情報の掲載日や更新日が新しいか

これらを一つずつ意識して確認するだけでも、誤情報に惑わされるリスクは大きく下がります。とくに SNS では、「シェアされた数」や「いいね数」が多いからといって、それが真実とは限りません。むしろ、不安や怒り、驚きをあおるような情報の方が拡散されやすいため、表面的な人気に惑わされず、自分の判断基準を持つことが求められます。

最近では、AI 技術を使って生成された“ディープフェイク画像”や、捏造された音声・映像コンテンツも出回るようになっています。一見すると本物のように見える画像や動画であっても、それが信頼できる情報であるとは限らないという意識を持つことが大切です。

最終的に大切なのは、「誰かが言っていた」ではなく、「自分の目と考えで確かめる」という姿勢です。便利な時代だからこそ、私たち一人ひとりが“情報の受け手”であるだけでなく、“判断する主体”であるという意識を持つことが求められています。情報に振り回されず、落ち着いて調べ、比較し、自分なりの根拠を持って行動できる、そんな力を育てていきましょう。

5. 情報を多角的に精査する考え方

次に、最後のポイント、「情報を多角的に見る」という視点についてご紹介します。

インターネット上の情報は、まさに玉石混交。便利な一方で、正しいかどうかの判断が難しいこともありますよね。だからこそ、「一つの意見を、うのみにしない」この意識がとても重要なんです。

たとえば、ある健康法について調べたとしましょう。

そのとき、SNS の体験談だけを見て「これは絶対に効果がある！」と判断するのは、ちょっと危険かもしれません。

そうではなく、厚生労働省のような公的機関の見解、大学などの研究結果、さらに患者会や医療現場での実際の声などのように、異なる視点からの情報を比較することで、初めて見えてくる事実があります。

これは「三点チェック」とも呼ばれますが、「官」の立場、「学」の立場、そして「民」の立場。この三つを意識的に見ることで、情報の偏りを避け、より信頼できる判断ができるようになるんです。

さらに、技術ニュースについても同じことが言えます。

企業のプレスリリースにはメリットばかりが並んでいて、課題やリスクについては書かれていないことが多いものです。そんなときには、技術系の専門メディアの記事や、実際の開発者が書いた技術ブログを読んでみると、思わぬ発見があるかもしれません。

視点を変えることで、「見えていなかったものが見える」ようになるんです。

情報の信頼性を高めるためには、最低でも 2 つ、できれば 3 つの異なる情報源を比較してみてください。

もし、それらが同じ内容を伝えていれば、その情報はかなり信頼できる可能性が高いですし、逆に食い違っている場合には、「なぜ違うのか？」という問いから、さらに深い理解へとつながっていきます。

こうした「比較する力」や「問いを立てる力」が、情報を鵜呑みにしないための最大の武器です。

何よりも大切なのが、「自分の頭で考える」ことです。

どんなに便利な検索エンジンや AI チャットでも、それはあくまで“道具”です。最後に情報を選び、判断し、活用するのは、私たち一人ひとりです。

ネット社会の中では、「たくさんの情報がある」ことと「正しい情報が得られる」ことはまったくの別物。だからこそ、自分の“視点”を持ち、意識的に比較する習慣を身につけましょう。

情報は一方向から見ただけでは、その本質が見えにくいこともあります。まるで、ダイヤモンドのように、角度を変えてこそ光る側面があるんです。

ぜひ、これからネットで情報を得るときには、「これは本当かな？」と立ち止まり、別の角度からも見てみてください。その一手間が、あなたの判断力と信頼力を育ててくれます。

6. まとめ

それでは本日のまとめです。

Google 検索では“演算子”を使うことで、欲しい情報に素早くたどり着けます。

チャット AI は要約や比較が得意ですが、出典の確認が欠かせません。

また、フェイクニュースは「出典」「複数の情報」「感情的な表現」に注意をして見抜来ましょう。

情報を鵜呑みにせず、複数の視点から比較・精査する習慣を持ちましょう。

こうした力を身につけることで、インターネットの海から信頼できる情報を、自分の力で見つけられるようになります。

次回は、実際に検索しながら情報を比較・分析するワークを行います。

ご視聴ありがとうございました！

第4章　.Q&A セッション

Q1: パケット通信って何？動画とかメールって、どうやって届いてるの？

A: パケット通信とは、大きなデータを小さなかたまりに分けて送る仕組みです。

それぞれのパケットが別々のルートを通って、最後に元どおりに組み立てられます。

Q2: じゃあ、そのパケットを運ぶときのルールってあるの？

A: はい、TCP と IP という通信の基本ルールがあります。

TCP は順番やエラーのチェックを、IP は宛先を決める“住所”の役割をしています。

Q3: IP アドレスって、数字ばかりで覚えられないよ～。

A: そのために「ドメイン名」があります。

たとえば「google.com」のように、人が覚えやすい名前で、裏では自動的に IP アドレスに変換されているんですよ。

Q4: その変換って誰がしてるの？

A: DNS という仕組みが行っています。

ドメイン名から IP アドレスを探し出す、いわばインターネットの電話帳のようなものです。

Q5: URL って、ただの文字列じゃないの？

A: URL はインターネット上の住所です。

「https://」「ドメイン名」「パス」「クエリ」という 4 つの要素で構成されていて、それぞれに役割があります。

Q6: 「http」と「https」って、何が違うの？

A: 「https」の「s」は Secure（セキュア）の略で、通信が暗号化されて安全です。

個人情報を扱うサイトでは、「https」で始まっていることを確認しましょう。

Q7: クライアントとサーバって、どっちが主役なの？

A: クライアントは情報を受け取る側、サーバは提供する側です。

どちらも役割があり、やりとりすることで私たちはインターネットを利用できているんです。

Q8: 安全なパスワードって、どうやって作るの？

A: 8 文字以上で、英大文字・小文字・数字・記号を組み合わせると良いです。

名前や誕生日などは使わないようにしましょう。

Q9: パスワード、全部同じにしてるけど大丈夫かな？

A: 同じパスワードの使い回しは危険です。

1 つ漏れただけで他のアカウントも乗っ取られる可能性があるので、それぞれ別のものを使いましょう。

Q10: フィッシング詐欺って、どうやって見抜けばいいの？

A: 差出人のメールアドレス、文面の日本語、URL、そして「すぐにログインして」などの不安をあおる言葉に注意すると、見抜きやすくなります。

Q11: ウイルスに感染したら、どうなっちゃうの？

A: 動作が遅くなったり、データが壊れたり、情報が盗まれることもあります。

特にランサムウェアは、ファイルを人質にして金銭を要求してくる危険なウイルスです。

Q12: セキュリティソフトって、本当に必要なの？

A: はい、必要です。

ウイルス検出や危険サイトのブロック、個人情報の保護など、多くの機能で私たちを守ってくれる頼もしい存在です。

Q13: Google 検索って、もっと上手にできるの？

A: 検索演算子を使うと便利です。

「“完全一致”」「site:」「filetype:」「-除外」などを使えば、より正確な情報を早く探せます。

Q14: ChatGPT って、便利だけどウソ言ったりしない？

A: とても便利ですが、誤情報を出すこともあるので、出典の確認が大切です。

あくまで参考情報として活用しましょう。

Q15: フェイクニュースって、どうすれば見抜けるの？

A: 出典の確認、他のメディアとの比較、感情的な表現がないかを見ることが大事です。

情報の鮮度や発信者の信頼性もチェックしましょう。

【奥付】

発行日：2025 年 4 月
発行者：株式会社妙香
所在地：福岡県北九州市小倉北区香春口 2-6-1
デザイナー・プリンセス・KY 3F