

情報セキュリティ 10 大脅威 知っておきたい用語や仕組み

目次

はじめに.....	3
1 章. 理解は必須！	5
1.1. 脆弱性（ぜいじゃくせい）	6
1.2. 多段階認証、多要素認証	7
1.3. キャッシュレス決済、スマホ決済.....	8
1.4. 写真の位置情報.....	10
1.5. ドメイン名.....	11
1.6. アプリ利用に必要な権限	13
1.7. 「アップデート」「更新」「修正プログラムの適用」	14
2 章. 知っていますか？.....	16
2.1. リスクベース認証.....	17
2.2. オンライン本人確認（eKYC）	18
2.3. Cookie（クッキー）	19
2.4. VPN (Virtual Private Network).....	21
2.5. 3D セキュア	22
2.6. CAPTCHA（キャプチャ） 認証.....	23
3 章. あっていますか？あなたの意識。	24
3.1. HDD（ハードディスク）のデータ消去	25
3.2. その他の IT 用語.....	26

はじめに

パソコンやスマートフォン、およびそれらを使ったインターネット上のサービスは、社会に深く浸透しており、日常生活とは切っても切れない生活基盤の一部となっています。様々な製品やインターネット上のサービスが次から次へと登場してきますが、それらをトラブルなく安全に利用するためには、製品の取扱説明書やサービスの契約内容、利用規約等をよく読んで、その仕組みや注意するポイントをよく理解することが大切です。しかし、新しい言葉や聞きなれない用語も多く、全てを調べ理解するのはなかなか大変だと思います。

本書では、パソコンやスマートフォン、インターネットを安全に利用するための対策をとる上で、ぜひ知っておきたい用語や仕組み(技術名称やサービス名称等)をいくつかピックアップし、それらについての概要やよくある疑問点等を解説します。

◆ 解説する用語や仕組みの一覧

■1章 理解は必須！ ～ここでこっそりチェック～

- ・脆弱性(ぜいじゃくせい) ⇒ **1.1.**
- ・多段階認証、多要素認証 ⇒ **1.2.**
- ・キャッシュレス決済、スマホ決済 ⇒ **1.3.**
- ・写真の位置情報 ⇒ **1.4.**
- ・ドメイン名 ⇒ **1.5.**
- ・アプリ利用に必要な権限 ⇒ **1.6.**
- ・「アップデート」「更新」「修正プログラムの適用」 ⇒ **1.7.**

■2章 知っていますか？ ～できれば理解しましょう～

- ・リスクベース認証 ⇒ **2.1.**
- ・オンライン本人確認(eKYC) ⇒ **2.2.**
- ・Cookie(クッキー) ⇒ **2.3.**
- ・VPN(Virtual Private Network) ⇒ **2.4.**
- ・3D セキュア ⇒ **2.5.**
- ・CAPTCHA(キャプチャ)認証 ⇒ **2.6.**

■3章 あっていますか？あなたの意識。～改めて確認しましょう～

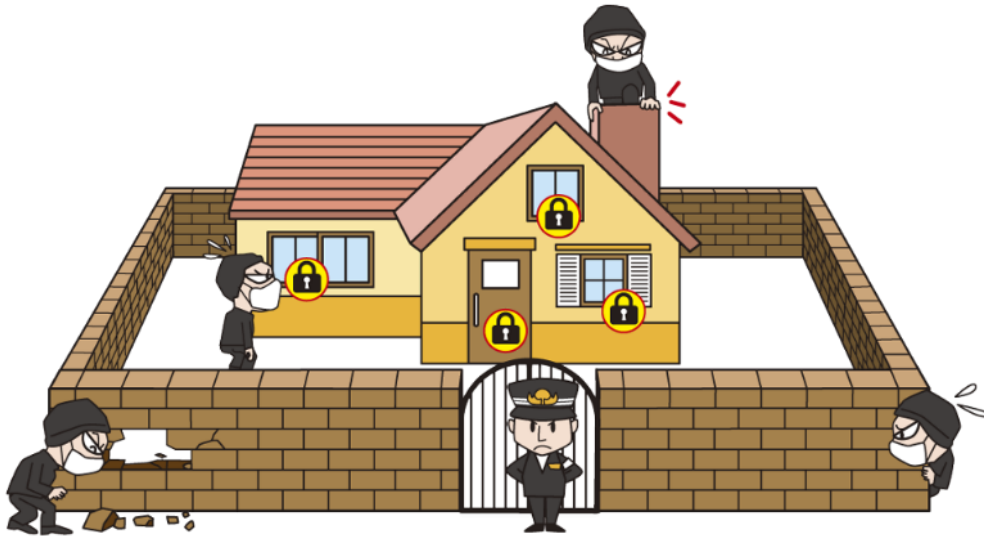
- ・HDD(ハードディスク)のデータ消去 ⇒ **3.1.**
- ・その他の IT 用語 ⇒ **3.2.**

◆ **本書を読んでいただきたい読者**

- ・主に家庭でパソコンやスマートフォンを利用する方
- ・パソコンやスマートフォンでインターネットを利用する方
- ・パソコンやスマートフォン、インターネットを利用する上でわからない用語等が多い方

1章. 理解は必須！
～ここでこっそりチェック～

1.1. 脆弱性(ぜいじゃくせい)



世の中に出回っている製品やインターネット上のサービス等には脆弱性が含まれている場合があります。脆弱性とはなにか、脆弱性がある製品やサービスとはどういうことか、どのように対策すればよいのか等を正しく理解し、向き合っていく必要があります。

◆ 脆弱性とは

ある製品やサービスに含まれる、セキュリティ上の弱点のことを指します。脆弱性を悪用されると、製品やサービス利用者の情報が漏えいしたり、製品やサービスの機能を不正利用されたりします。

どんなに安全な製品やサービスを開発しようとしても、開発元が意図せずに脆弱性が存在してしまうことが多々あります。また、製品の発売時点やサービスの開始時点では脆弱性がなかった(気づかなかった)としても、内在していた脆弱性が後々発見されたり、技術や環境が変化することで脆弱性が新たに顕在化したりする場合があります。

◆ 脆弱性がよく発見される製品は危険？

犯罪者に悪用されてしまうような脆弱性が含まれている製品やサービスを使用することはたしかに危険なことと言えます。ただし、脆弱性のない製品やサービスを開発することは非常に難しく、どんなものにも脆弱性はつきものです。

例えば日々多くの脆弱性が発見され、頻繁にアップデートを実施している製品やサービスが危険なのかという一概にそうとは言えません。良い製品・サービスであり広く普及しているため脆弱性が発見されやすいが、製品提供元のサポートが手厚いので頻繁にアップデートされているとの見方もあります。逆にあまり利用されていない製品やサービスの場合は、一見脆弱性がなさそうに見えても、単に脆弱性が発見されていないだけの場合もあります。

◆ 脆弱性対策は最新版にアップデート

脆弱性を放置することは非常に危険です。利用している製品に脆弱性が発見されたら速やかに最新版にアップデートしましょう。また製品を選択する場合には、その製品の機能や価格だけではなく、脆弱性が発見された場合にはきちんと対応してくれるのか(製品をアップデートしてくれたり、脆弱性対策の方法を公開してくれたりするのか)どうか、サポートの手厚さやサポート期限等も考慮して製品を選択することが肝要です。

1.2. 多段階認証、多要素認証



インターネット上のサービスを利用するにあたり ID とパスワード等でログインして利用するものがあります。ID やパスワードが犯罪者に漏れると、こういったサービスに不正ログインされてしまい様々な被害につながります。不正ログイン対策として多段階認証や多要素認証を推奨するサービスが増えてきました。

◆ 多段階認証とは

認証する回数を 1 回ではなく 2 回以上に分けて行うことを多段階認証といいます。例えばサービスにログインする際に、1 つ目のパスワードを入力して認証した後、2 つ目のパスワードを入力して複数の段階で認証することでセキュリティを高めようとする方式です。家の鍵を 2 つかけるのと似たイメージです。当然ながらパスワードが 2 つとも漏れてしまえば第三者に不正ログインされてしまうおそれがあります。

◆ 多要素認証とは

認証するための要素を大別すると 3 つの要素があり、これらを認証の 3 要素としています。それぞれ、「記憶」、「所持」、「生体情報」を指します。これら複数の要素で認証することを多要素認証といいます。(2 つの要素で認証することは二要素認証ともいいます。)例えば「記憶」とはパスワードや PIN コード等の「覚えている情報」、「所持」はキャッシュカードや OTP (ワンタイムパスワード) トークン等の「所持して

いるもの」、「生体情報」は静脈や指紋、顔の情報等の「身体的特徴等」を指します。

例えばログイン画面でパスワードを入力後、自身の携帯電話にワンタイムパスワードが記載された SMS が送信され、そのワンタイムパスワードを入力することでログインするサービスです。パスワードを 2 回入力するため、一見多要素認証ではないように思えますが、SMS は電話番号宛に送信されるので、携帯電話を所持している人にしか見られない性質を生かして多要素認証の要件を満たしています。

◆ 不正ログイン対策のため多要素認証を

自身が利用しているサービスに不正ログインされないように、積極的に多要素認証を利用しましょう。ただし、多要素認証も万全ではありません。例えば SMS で送信されてくるワンタイムパスワードを窃取しようとするフィッシングの手口も出てきています。そういった手口に騙されないよう十分に注意して操作することも重要です。

1.3. キャッシュレス決済、スマホ決済



2022年のキャッシュレス決済比率は36.0%にもおよび、経済産業省は2025年までにこれを4割程度にするという目標を掲げてキャッシュレス決済の推進に取り組んでいます。¹ キャッシュレス決済に関するキャンペーンやテレビCMを目にするのも珍しくない社会になりつつあります。

◆ キャッシュレス決済とは

キャッシュレス決済とは、現金（貨幣や紙幣）を用いない決済方法を指します。現金の持ち歩きや、現金の取り出し、おつりの受け取り等の手間が省けるため、スムーズな決済が可能という利点があります。インターネットショッピングやインターネット上のサービス（オンラインゲーム、動画配信、電子書籍等）の決済方法にキャッシュレス決済を使えば、商品購入やサービス利用、その決済までをすべてインターネット上で完結できるため、非常に便利です。

◆ キャッシュレス決済の種別

現金を渡して決済する以外の方法はキャッシュレス決済と言えるため、その種別は多岐に渡ります。決済方法の名称を付ける際、用いる端末から名づけたり、その技術的な仕組みから名づけたりしてきたことで、様々な用語が乱立しています。日常生活においては種別の名称を全て覚える必要はありませんが、自分が利用している、もしくは利用しようとしている決済方法の特徴やリスクを理解しておく、

より安全に利用できます。ここでは代表的な決済方法をいくつか紹介します。

・クレジットカード決済

クレジットカードを使って決済する方法です。買い物をする店舗にて読み取り機でカード情報を読み取って決済したり、インターネットショッピングでクレジットカード情報を入力して決済したりする方法があります。

（Visa、MasterCard、JCB、等）

・非接触型決済

NFC や FeliCa 等の通信技術を用い、ICカードを読み取り機にかざすことで決済する方法です。

（Suica、Edy、WAON、nanaco 等）

・キャリア決済

商品購入やサービス利用の支払い金額を、月々キャリアに支払っている携帯電話料金や通信料金とまとめてキャリアに支払うことで決済する方法です。

(ドコモ払い、auかんたん決済、ソフトバンクまとめて支払い、等)

・モバイル決済

フィーチャーフォン(ガラケー)やスマートフォン等のモバイル端末を利用して決済する方法の総称です。

・スマホ決済

モバイル決済の中でもスマートフォンを利用する方法をスマホ決済と言います。さらにその中でも、スマートフォンに専用のアプリをインストールし、そこに表示される QR コードやバーコードを店舗側で読み取ったり、逆に店舗側の QR コードを自分のスマートフォンで読み取ってから支払い金額を入力したりすることで決済する方法をコード決済と分類しています。

様々な企業が〇〇ペイのような名称のサービスを展開しており、スマホ決済の認知度は飛躍的に上昇しました。

◆ キャッシュレス決済の不正利用も横行

キャッシュレス決済はいまや広く普及しています。それゆえ犯罪者や犯罪者グループ等による不正利用も横行しています。キャッシュレス決済の種別は多岐に渡りますし、同じ種別の中でもサービスごとに仕様や使い方等、細かい部分は異なってくるため、それに応じて不正利用の手口も幅広くなり狙われやすくなっている状況です。

例えば、クレジットカード決済はクレジットカード情報を知っていれば本人ではなくても決済できるため、犯罪者はクレジットカード情報を窃取し、不正利用しようと狙っています。キャリア決済はキャリアの自分のアカウントに不正ログインされると不正利用されてしまうため、犯罪者はアカウントの認証情報(アカウントの ID やパスワード)を窃取しようと狙っています。また、スマホ決済も同様に自分のアカウントに不正ログインされると不正利用されるおそれがあります。これらの決済方法を利用する場合は、使う決済方法の認証の仕組みをよく理解したうえで、日々アカウントの認証情報を適切に管理することがとても重要です。

特に新しいサービスについては犯罪者が不正利用できないかと狙ってくるおそれについて意識しておくことが肝要です。

IPA では「情報セキュリティ 10 大脅威 2020」から「スマホ決済の不正利用」を 1 つの脅威として取り上げており、10 位以内を維持し続けています。また、クレジットカードの不正利用についても被害額が 2014 年から 2022 年まで増え続けています。²

それぞれの内容や対策について「情報セキュリティ 10 大脅威」の解説書でさらに詳しく解説していますので、そちらも参照して適切な対策を講じ、キャッシュレス決済を安全に利用しましょう。

参考資料

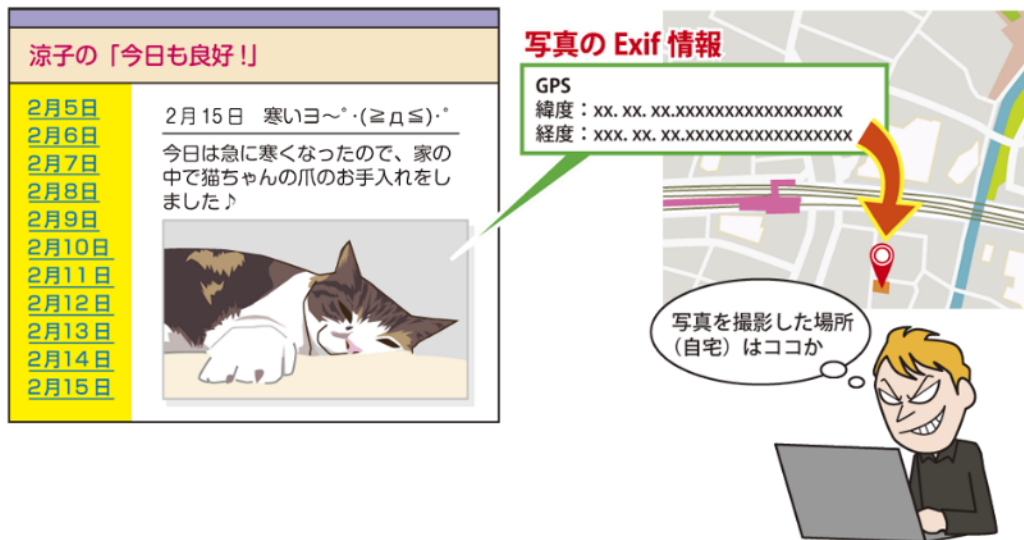
1. 2022年のキャッシュレス決済比率を算出しました(経済産業省)

<https://www.meti.go.jp/press/2023/04/20230406002/20230406002.html>

1. クレジットカード不正利用被害の集計結果および数値の訂正について(一般社会法人日本クレジット協会)

https://www.j-credit.or.jp/download/news_202300000195.pdf

1.4. 写真の位置情報



スマートフォンのカメラ機能が飛躍的に向上し続けています。旅行先での写真撮影やペットの写真撮影、自撮り等、スマートフォンやデジタルカメラで写真撮影をしている方は多いと思います。そんなスマートフォンやデジタルカメラで撮影した写真には実は様々な情報が含まれており、その中には撮影した場所の位置情報等も含まれていることは知っていましたか？

◆ スマートフォンの写真に含まれる情報

スマートフォンやデジタルカメラで撮影した写真は、Exif(イグジフ)というデータ形式で保存されています。Exif形式のデータには、写真としての画像データ以外にも、撮影日時や撮影機器のモデル名、カメラの設定、写真を撮影した場所の位置情報(GPS 情報)等の様々な情報が付加されています。

◆ 写真から様々な情報が漏えい？

スマートフォンやデジタルカメラで撮影した写真に含まれている情報で特に注意が必要なのは、撮影した場所の位置情報です。

例えば、子育ての写真やペットの写真等、自宅で撮影した写真の中には自宅の位置情報が含まれていることとなります。つまり写真で住所が特定できます。それ以外にも、子供の運動会の様子を撮影した写真であれば、通っている学校の位置情報が含まれているので、学校の所在地や学校名が特定できます。こういった写真を安易に第三者に渡したり、イ

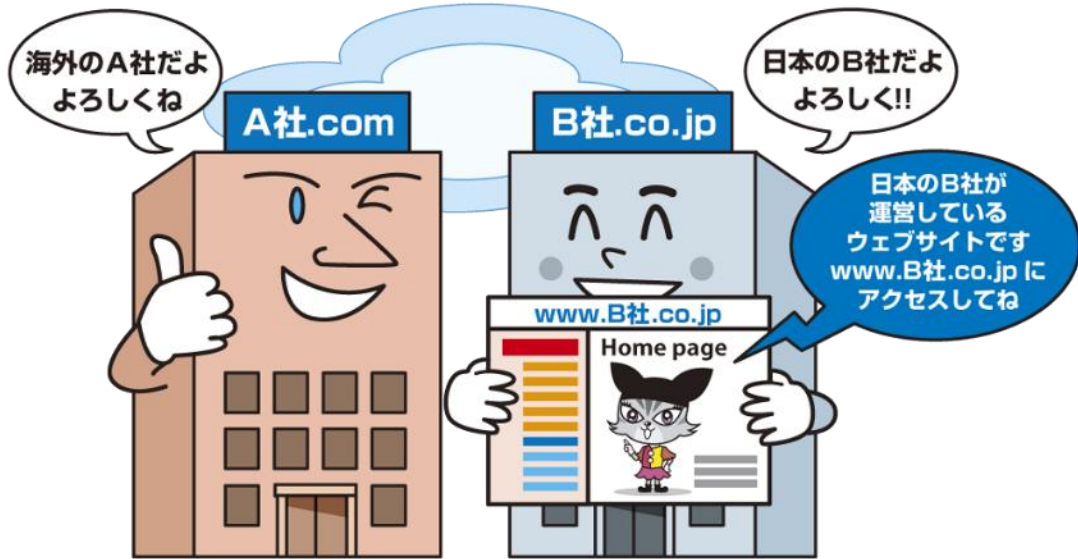
ンターネット上に公開したりすると、意図せぬ個人情報の漏えいにつながります。

◆ 撮影した写真を SNS で公開

スマートフォンで撮影した写真を Twitter や Instagram、LINE 等で不特定多数に公開する人が多くいます。ではこの場合、位置情報を公開していることになるのでしょうか？

実はよく利用されている SNS 等では、写真をアップロードする際に Exif 内の写真データ以外の付加情報をサービス側で削除してくれています。ただしこれはサービス側の仕組みに依存していることとなります。自身がサービスを利用する際には、Exif の情報がどのように扱われるか(アップロード時に位置情報等を削除してくれるか等)は、サポートサイトの記載をよく読む等してきちんと把握してサービスを利用することが肝要です。また、Exif 情報は自分で削除することもできます。例えばスマートフォンの場合は Exif 情報を削除するアプリもあるので必要に応じて探してみましょう。

1.5. ドメイン名



インターネットを利用している中で「ドメイン名」という言葉を聞いたことはありませんか？ウェブサイトの閲覧やメールを利用する際にも使われるインターネットにおける重要な仕組みのひとつです。閲覧するウェブサイトの URL (サイトアドレス) や受信したメールの送信元メールアドレスが本物なのか偽物なのか等を見分ける対策の中でも出てくる言葉なのでぜひ知っておきましょう。

◆ ドメイン名とは

インターネット上で主に組織の名前等を表すものです。閲覧するウェブサイトの場所や、メールを送信する際の送信先メールアドレス等にドメイン名が使用されています。例えば、IPA のドメイン名は「ipa.go.jp」です。

◆ ウェブサイト閲覧とドメイン名

ウェブサイトを閲覧した際に、ウェブブラウザ(以降ブラウザと表記)の上部にあるアドレスバーに、どこのウェブサイトのどのページを見ているかを示す URL と呼ばれる文字列が記載されています。その一部分にドメイン名が使用されています。

URL がウェブサイトのインターネット上の住所のようなもので、ドメイン名が組織の名前のようなものと考えるとわかりやすいと思います。例えば、IPA ウェブサイトのトップページの URL は「https://www.ipa.go.jp」で、その後ろの部分「ipa.go.jp」がドメイン名になっています。

ドメイン名は「.(ドット)で区切られていて、

後ろから「トップレベルドメイン」「第 2 レベルドメイン」「第 3 レベルドメイン」と分かれています。ドメイン名で組織の種別や国、組織名等が表現されているので、ドメイン名を見ることでこの国のどんな分野の組織なのかをある程度判断することに使えます。組織名を表す部分 (IPA のドメイン名を例にすると「ipa」の部分) は使用者が任意の文字列を自由(ただしドメイン管理団体への申請先着順)に指定できます。組織名以外にも製品名やサービス名等が指定される傾向にあります。

また、IPA の URL における「www」の部分はホスト名(サイト名)を表しています。同じ組織で複数のウェブサーバーやウェブサイトを運営したい場合はホスト名を変えます。ちなみに、ウェブサイトを見ていると「www」というホスト名を多く見かけると思います。これは「World Wide Web」の略で、簡単に言えばウェブサイトを実現するためのインターネット上の仕組みを指します。昔から慣習的に使われているので、一目でウェブサイトであることがわかりやすいようにホスト名を「www」として

いるウェブサイトが多いです

◆ ドメイン名の種別

様々なドメイン名がありすべてを覚えるのは大変かもしれないですが、代表的なドメイン名についていくつかご紹介します。

・「.com」

世界の誰でも使用できるトップレベルドメイン。世界の商業組織等で使用しています。

・「.co.jp」

日本の商業組織等で利用しています。

・「.ed.jp」

日本の 18 歳未満を対象とする教育機関等で利用しています。

・「.ac.jp」

「.ed.jp」を利用する条件には合致しない日本の教育機関で利用しています。

・「.or.jp」

日本の民間の非営利法人、公的な国際機関や在日公館等で利用しています。

・「.go.jp」

日本の政府機関や各省庁所轄の組織等で利用しています。

・「.jp」

日本に住所がある個人や組織が誰でも取得できる汎用的なドメイン名です。

等

◆ ドメイン名を知ってどうするのか

犯罪者が本物そっくりな偽物のウェブサイトを作ってそこに利用者を誘導し、個人情報等を入力させて情報を詐取する手口(フィッシング)が年々増加しています。

ウェブサイトの URL 内のドメイン名を見て、本物のウェブサイトなのかを判断できますが、それを逆手に取って本物のドメイン名と視覚的に見分けづらいドメイン名をつけることで、

ウェブサイトが本物か偽物かをわかりにくくする手口もあります。例えば、組織名等を表す部分が任意の文字列を指定できることを利用します。

あなたは以下の違いに気づけますか？

(例 1)

本物のドメイン名:「■■■m.jp」

偽物のドメイン名:「■■■rn.jp」

(例 2)

本物のドメイン名:「■■■.co.jp」

偽物のドメイン名:「■■■-co.jp」

例 1 では「m」(エム)を「rn」(アールとエヌ)に置き換えて「m」に見せかけています。

また、「.jp」ドメイン名を使用して、「.co.jp」や「.go.jp」等に似せたドメイン名を作成する手口もあります。

例 2 では見えにくい「-」(ハイフン)を入れることで同じドメインに見せかけています。

このように誤認識させるようなドメインをドッペルゲンガードメインと呼びます。メール内に記載した URL を誤認識させることで、偽のウェブサイトへアクセスさせるフィッシングに悪用します。また、メールアドレスのドメイン部分をタイプミスしたらドッペルゲンガードメインを準備した攻撃者にメールが送られるので、重要情報が攻撃者の手に渡るおそれもあります。

ドメイン名に着目してウェブサイトが本物か偽物かを判断することは大事ですが、このような騙しの手口もありますので注意が必要です。騙されないようにするためにも、ウェブサイトへアクセスする際には、あらかじめ自分が利用するウェブサイトをブラウザのブックマーク(お気に入り)に登録しておき、そこからアクセスする方法も有効です。

1.6. アプリ利用に必要な権限



スマートフォンは電話をするための機器というだけでなく、生活のためのツールや財布のような役割が大きくなりつつあります。そのために、スマートフォンに保存している情報は大切な思い出の写真やクレジットカード情報、電子マネーの情報等、多岐に渡っています。そんなスマートフォンにインストールするアプリは、保存されているどんな情報にアクセスでき、その情報を何に使うのか？それを理解してスマートフォン使わないと、いつの間にか「誰か」に情報を盗み取られていることもあり得るのです。

◆ スマホアプリの権限とは？

そもそも、人ではないアプリに対して「権限」と言われてもピンと来ない方もいると思います。「スマートフォンとアプリ」は「会社と社員」に例えて考えるとわかりやすいです。例えば、会社のお金を管理しているのは経理部です。経理部の仕事では会社のお金の情報を見たり、他社とやり取りしたりしないと仕事できません。そこで会社は経理部に、お金の扱いに関する権限を与えているのです。これをスマートフォンに置き換えてみましょう。〇〇ペイというアプリを使ってコンビニで買い物をするとしましょう。そのためにはクレジットカード情報や銀行口座にアクセスできないと支払いができません。そこで、利用者が〇〇ペイには銀行口座やクレジットカード情報にアクセスする権限を与えているのです。必要な権限はアプリの種類によって異なりますが、例えば連絡先、画像、動画、位置情報へのアクセス権限や、スマートフォンの機能を利用する権限等があります。

◆ リスクを軽減するためには？¹

- ・アプリは公式マーケットから入手する
世の中には優良なアプリだけでなく、不正なアプリも存在します。公式マーケットからインストールすることで不正なアプリをインストールするリスクが軽減できます。
- ・アプリに権限を安易に与えない
アプリのインストール時、起動時、他のアプリやサービスとの連携時には権限を求められることがあります。その際に、求められたから許可するのではなく、何をするのに必要な権限なのか一度考えましょう。例えば、地図アプリを利用して「位置情報にアクセスしようとしています」と表示が出た場合、不思議には思わないでしょう。しかし、「画像にアクセスしようとしています」と表示が出たら画像を何に使うのか不思議に感じませんか？
表示された内容についてちょっと考えてみるだけでもリスクを軽減することができます。

参考資料

1. 情報セキュリティ10大脅威2017 ～1章 情報セキュリティ対策の基本 スマートフォン編～(IPA)
<https://www.ipa.go.jp/security/10threats/ps6vr7000000bi1p-att/000059213.pdf>

1.7. 「アップデート」「更新」「修正プログラムの適用」



個人におけるスマートフォンの保有率は2021年には74.3%¹となり、PCだけでなくスマートフォンも生活の一部になっており、サービスを受けるためにはスマートフォンが必要である機会が増えました。PC やスマートフォンを使用していると、ソフトウェアやアプリの「アップデート」や「更新」、「修正プログラムの適用」という言葉を目にしたことがあるのではないのでしょうか。これらは適切なセキュリティ対策を行う上で大切なものですので正しく理解し、実行する必要があります。

◆ 言葉の意味

「アップデート」「更新」「修正プログラムの適用」「バージョンアップ」という言葉があります。類似した言葉が複数ありますが、本書では総じて「アップデート」と呼称して説明します。

PC やスマートフォンを利用するうえでのアップデートとは、ソフトウェアやアプリを、より新しい状態に変更することを指します。

更新の内容次第ではバージョンと呼ばれる数値が、例えば 1.1 から 1.2 になるように変更になることがあります。これをバージョンアップと呼びます。バージョンとは本で言うところの第〇版と同義です。このバージョンアップをするために必要な部品が「修正プログラム」と呼ばれています。本で言うところの、「修正した新しい文章」のようなイメージです。

◆ 「アップデート」をする機会

PC をシャットダウンする際に「更新してシャットダウン」という言葉を見たことがあるのではないのでしょうか。他にも、ソフトウェアを起

動した際に「最新版に更新しますか？」のような表示がされることがあります。

スマートフォンを利用している場合、iPhone や iPad ではアップデートができるアプリに関して、App Store で「アプリのアップデート」と表示されます。Android アプリでは、Play ストアで「利用可能なアップデート」が表示されます。

これらの表示はどれもソフトウェア、アプリの開発者が最新版をリリースした時に、その情報を PC やスマートフォンが検知して表示しています。表示が出た時はアップデートを行うようにしましょう。

◆ ソフトウェアやアプリの「アップデート」方法

ソフトウェアやアプリのアップデート方法にはいくつかの種類がありますので紹介します。

- ①自動的にアップデートされるもの
- ②PC やスマートフォン上で最新版がリリースされたことの通知があるもの
- ③最新版のリリース有無を Web サイトで

チェックする必要があるもの

④自動的にアップデートするか設定できるもの
以上のような種類があります。

例えば Google Chrome では自動アップデートを有効にするか無効にするかを設定できます。これを有効にしていると、最新版のアプリがリリースされた場合は、Google Chrome のウィンドウを一度閉じて、再度 Google Chrome を立ち上げることで自動的にアップデートされます。

最新版がリリースされたときに通知があるものの例としては Windows Update や Apple iOS が該当します。Windows OS の PC であればシャットダウンする際に「更新してシャットダウン」と表示されたり、mac や iPhone であれば「ソフトウェア・アップデートのポップアップが表示されたりします。それを確認した利用者がアップデートを行います。

こういった自動アップデートや通知を表示する機能が無いソフトウェアやアプリの場合は利用者自身がサポートページ等を確認しなければなりません。

◆ アップデートとは具体的に何をしているのか？

アップデートと聞くと、「新しい機能ができた」と考える方もいるかと思いますが、実はそれだけではありません。不具合の修正やセキュリティ対策をしていることもあります。つまり、アップデートしないことはセキュリティ対策が十分ではないままに利用していることとなります。

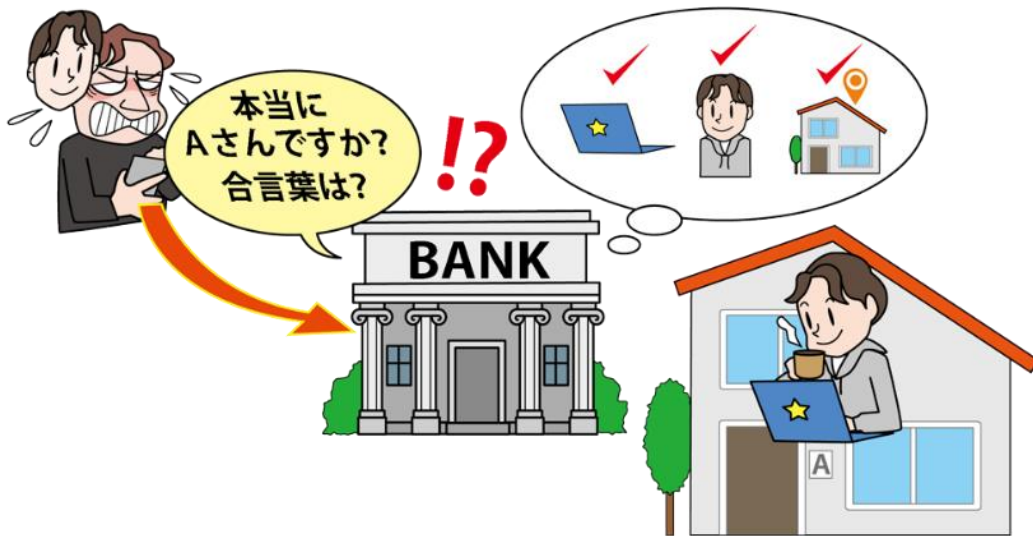
また、アップデートがある時は、そのソフトウェアのサポートページにアップデートの内容が書かれていることが一般的です。内容を確認し、「セキュリティ対策」や「脆弱性を修正」等の記載があった場合は特に迅速にアップデートを実行するようにしましょう。

参考資料

1. 令和3年通信利用動向調査の結果(総務省)
https://www.soumu.go.jp/johotsusintokei/statistics/data/220527_1.pdf

2章. 知っていますか？
～できれば理解しましょう～

2.1. リスクベース認証



インターネット上のサービスを利用するにあたり、自分が利用しているサービスを第三者に不正ログインや不正利用されないようにすることが重要です。そのために様々な認証方式(多要素認証、リスクベース認証等)がサービス側から提供されており、利用者側はそれらを正しく理解して利用することが望まれます。

◆ リスクベース認証

インターネット上のサービスを利用するために、まずはサービスの自身のアカウントに ID やパスワード等を用いてログインします。この時、ID やパスワードが第三者に漏れてしまうと、その情報を使って自身のアカウントに不正ログインされ、なりすまされてしまうおそれがあります。そこで、第三者が正規の利用者になりすましている可能性を考慮し、必要に応じて追加で認証を行う方式がリスクベース認証です。追加で認証を行うかどうかの判断基準として、利用者の使用している端末の OS、IP アドレス、ブラウザ等の情報がいつもと異なっていないかを確認する方式等があります。

◆ どのように追加の認証を行うか

追加の認証として使われるものは様々ですが、例えばあらかじめ「秘密の質問」や「合言葉」を登録しておき、リスクベース認証を行う場合にはサービス側が各利用者に対してそれらの情報入力を要求する方式があります。それ以外にも、あらかじめ登録しているメールア

ドレスにワンタイムパスワードを送信し、その情報を入力させてリスクベース認証を行うことで、多要素認証の要件も満たす方式もあります。どのようにリスクベース認証を実装するかについては各サービスの方針によって様々です。一例として、現在インターネットバンキング等でよく使われている方式は「秘密の質問」や「合言葉」です。

◆ リスクベース認証のメリット・デメリット

リスクベース認証は、利用者がいつもと同じ環境(IP アドレスや使用する端末、ブラウザ等)からサービスを利用する場合は追加の認証が発生しないため、利用者に負担をかけずにセキュリティを高めることができます。その一方で、利用者のネットワーク環境や使用する端末等が日々異なるような場合は、都度リスクベース認証が発生し、負担が大きくなることも考えられます。サービスによっては信頼できる端末(自分が利用する端末)を複数登録することができる場合もあるので、仕様を理解して適切に利用しましょう。

2.2. オンライン本人確認 (eKYC)



例えばインターネットバンキングの口座等を開設する際、インターネットから必要な情報を入力して申し込みをした後に、別途本人書類(身分証の写し等)を郵送するように案内されて不便に感じたことはないでしょうか。これを解消する方法としてオンライン(インターネット上)で本人確認を完結できることも増えています。

◆ 法改正でオンライン本人確認が可能に

銀行口座等を開設する際には本人確認が必要です。以前は本人確認のために利用者が身分証の写し等を銀行に郵送し、その後銀行から取引関係書類を転送不要郵便で利用者が受け取る手順を踏む必要がありましたが、2018年11月30日に「犯罪収益移転防止法」の一部が改正され、インターネット上のみで本人確認ができるサービスが増えました。これにより利用者が本人確認書類を郵送する手間が削減し、郵送に要する時間も省略できることで、より便利でスムーズに本人確認ができるようになりました。

◆ オンライン本人確認の方法

オンライン本人確認の方法にはいくつかありますが、例えば写真付き本人確認書類(運転免許証等)を写真撮影し、その画像データをウェブサイト上から送信(アップロード)する方法がわかりやすいかと思います。例えばスマートフォンを持っていれば写真撮影から画像データの送信までスマートフォン1台で可能

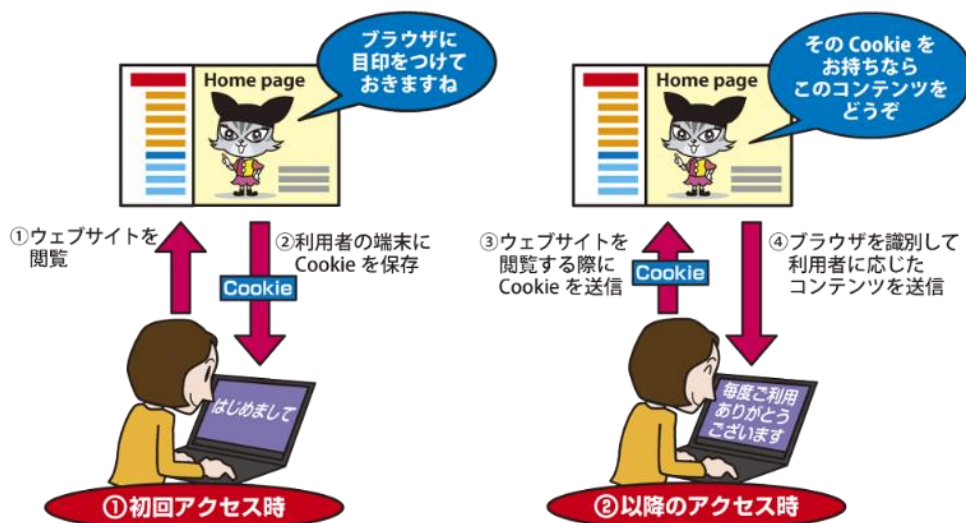
です。日々スマートフォンでインターネットを使っている方々には利用しやすいのではないのでしょうか。また、各サービス事業者がオンライン本人確認用のスマホアプリを提供している場合もあります。写真の撮影機能や撮影した画像データをサービス事業者へ送信する機能があり便利です。

◆ オンライン本人確認の今後について

オンライン本人確認はまだ新しい仕組みであるため、撮影された画像の真贋の判定や直近で撮影された写真なのかの確認等、サービス事業者にとって様々な課題があります。また、新しい技術の登場はそれを悪用する攻撃者を生み出すおそれがあります。そのため、オンライン本人確認の手法は今後も変化していく可能性があります。

利用者としてはサービス事業者からの案内を注視したり、アプリを更新して最新の状態に保ったり等、利用者ができる範囲での対応を心がけましょう。

2.3. Cookie (クッキー)



インターネットでウェブサイトを開覧するにあたり、Cookie(クッキー)という言葉を目にしたことはないでしょうか。主にログインを必要とするインターネット上のサービスで、ウェブサイト閲覧者の状態を管理することに利用されます。また、インターネット上の広告において、閲覧者が興味を持っていそうな分野の広告表示する、ターゲティング広告等にも利用されます。

◆ Cookie(クッキー)とは

インターネット利用者がウェブサイトを開覧した際、閲覧者のウェブブラウザ(以降ブラウザと表記)に対してウェブサイト側がテキスト形式の特定の情報(閲覧者ごとに割り当てられるID等)を保存することができます。この情報をCookieと言います。閲覧者のブラウザがCookieを持った状態でウェブサイトを開覧すると、ブラウザは自動的にCookieを送信し、ウェブサイト側はそのCookieを見てどの閲覧者(どのブラウザ)からのアクセスであるかを判断できるため、各閲覧者に応じたコンテンツを返すことができます。

閲覧者が利用しているブラウザに目印をつけるようなイメージです。

◆ Cookieはどのように使われるか

例えば、ウェブサイトにログインした後に別のサイトを見て、再度ログインしていたウェブサイトを見ると、ログインした状態が保持されている場合があります。これはウェブサイト側がどの閲覧者であるかを判別しているから可

能なことであり、このように閲覧者の状態を管理する方法にCookieが使われています。

◆ ターゲティング広告

ウェブサイトを開覧すると様々な広告が表示されます。時には自分が調べていた商品の広告が頻繁に出てくるようになる場合もあります。これはターゲティング広告と呼ばれるものです。今までに自分が閲覧したウェブサイトに関連の深い分野の広告が表示されるため、自身の行動が追跡されている(ウェブサイト閲覧履歴が知られている)のではないかと不安に感じる方も多いと思います。

ターゲティング広告を実現するための手段のひとつとしてCookieが用いられていますが、Cookieの中に個人を識別できる情報やウェブサイトの閲覧履歴がそのまま保存されているわけではありません。広告事業者は様々なウェブサイトに広告を出します。閲覧者があるウェブサイトとそこに掲載されている広告を開覧した場合に、広告事業者はそのウェブサイトのURLとブラウザのCookieを収集

しています。その情報を蓄積していくと、どの閲覧者(ブラウザ)がどのウェブサイト(広告事業者が広告を出しているウェブサイト)を閲覧したかの履歴になるので、それを利用して閲覧者が興味のある分野等を推測することができます。

◆ Cookie の取り扱いについて

Cookieの内容を見ることで、Cookieを発行する事業者側がウェブサイト閲覧者の傾向をある程度把握できることから、閲覧者個人に関連する機微な情報となり得ます。

Cookieのみでは通常個人の識別はできませんが、例えばログインして利用するインターネット上のサービス等で、別途個人を識別できる情報を登録する場合は、その登録情報とCookieを照合することによって、あるCookieを持っている閲覧者は誰であるのかをサービス事業者側では特定できることとなります。

世界的にも規則や法整備が進められており、欧州でのGDPR(一般データ保護規則)施行の影響もあり、個人に関する情報やプライバシーを保護しようとする動きはますます強くなってきています。それに伴い、ウェブサイトを閲覧する際に、Cookieを使用することの同意を求めるポップアップを表示するウェブサイト等が増えてきました。サービスに登録する個人情報や、送信したCookieの取り扱いはサービス事業者に委ねることになるため、利用するサービスの利用規約等をよく読み、それらの情報の取り扱い方を把握して、情報を預けて問題ないかを判断することが重要です。

◆ 利用者におけるCookieの管理

Cookieはインターネット上のサービス利用を便利にするために必要なものですが、サービス事業者の取り扱いによっては個人の機微な情報が第三者に知られてしまうおそれもあります。

Cookieは、利用者がブラウザで設定することで、自身で管理できます。例えばCookieを使わない(無効化する)設定をしたり、PCが保持しているCookieを削除したりできます。Cookieを利用したターゲティング広告については、Cookieを削除することで広告事業者に情報が渡ることを防げるので、定期的にブラウザのCookieを削除することを検討するのも良いと思います。

設定方法は使用しているブラウザの種別によって変わりますので、自分が利用しているブラウザにおけるCookieの設定方法を確認してみましょう。

2.4. VPN (Virtual Private Network)



新型コロナウイルス対策の1つであったテレワークが一般的な勤務形態の1つとなり、自宅からインターネットを通じて会社のシステムを利用して仕事をする機会が増えてきた方も多いのではないのでしょうか。自宅と会社間で通信をするにあたり、通信内容を改ざんされたり、盗聴されたりしない適切なセキュリティ対策をとることで、安全性の高い環境を準備することが求められます。

◆ VPN (Virtual Private Network) とは

主に個人でインターネットへのアクセス等の通信を行う場合、多くの利用者で物理的に同じ設備を共有する公衆回線を利用しています。一方、組織で通信を行う場合は重要なデータを扱うことが多く、公衆回線よりも通信の安定性や高いセキュリティを求められるため、拠点間で専用の設備を使用した専用回線を用いて通信を行う場合もあります。ただし、専用回線を導入するには公衆回線と比較して大きなコストがかかります。そこで、VPN (Virtual Private Network) と呼ばれる技術を用いて通信を暗号化することで、公衆回線をあたかも専用回線であるかのように利用することができ、専用回線を敷くよりも安価で、公衆回線よりも安全性の高い通信環境を実現できます。近年テレワークへ移行する組織が増えていますが、テレワーク環境を組織で整備するにあたり、比較的安価で安全性の高い通信環境が求められることから、VPN を利用するケースが増えています。

◆ VPN はどのように実現するか

VPN を実現する方法はいくつかありますが、例えばテレワークで自宅の PC から自分の会社のシステムを利用する場合、会社側に VPN 用の機器を、そして自宅の PC には VPN 用のソフトウェアを導入し、それらの VPN 用の製品を介して通信を行います。その通信は公衆回線(インターネット)を経由しますが、VPN 用の製品間はトンネルで繋がっているようなイメージになり、インターネットに接続している他の利用者からは、そのトンネル内の通信内容は見ることができないようになります。

◆ VPN は安全？

一般的に VPN を利用することで安全性の高い通信が可能ですが、仮に VPN 用の製品に脆弱性が存在する場合は、それを悪用した攻撃が行われるおそれもあります。利用している VPN 製品に脆弱性がないかの確認や発見された脆弱性への対策は日々継続して実施する必要があります。

2.5. 3D セキュア



3D セキュアとは、インターネット上でクレジットカード決済を行う際に、正規の利用であるかを確認する本人認証サービスの名称です。不正利用を防ぐために用いられる仕組みです。

◆ 「3D」とは？

「3D」と聞くと「3次元」が最初に頭に浮かび、何か立体的に表れる物を利用するのではと想像する方もいるのではないのでしょうか？3D セキュアにおける3Dは「3つのdomain(領域)」という意味を表します。3つの領域とは、クレジットカード発行会社、加盟店管理会社、そしてこの2つを仲介する領域を指します。本書ではインターネット上における「ドメイン名」も解説していますが、この「ドメイン」とは異なる、一般的な意味として用いられています。

◆ 3D セキュアを使うとどうなるの？

3D セキュアを適用していると、もしもクレジットカード情報を盗まれてしまったとしても、その情報だけでは不正に利用することができなくなります。

従来はクレジットカードを利用するために必要な情報は全てカード本体に記載されていました。つまり、カード本体やその情報が盗まれてしまうと不正に利用されてしまいます。

一方、3D セキュアを使うとクレジットカードだけでは認証できない追加認証が行われます。例えば、指紋や顔等の生体情報や、ワンタイ

ムパスワードを用いた認証です。生体情報もワンタイムパスワードを受け取る方法もあらかじめ登録しておく必要があります。このように、生体情報やワンタイムパスワードを受け取る機器といったクレジットカード以外の要素を持ち合わせていないと決済できなくすることで不正利用を防止しています。

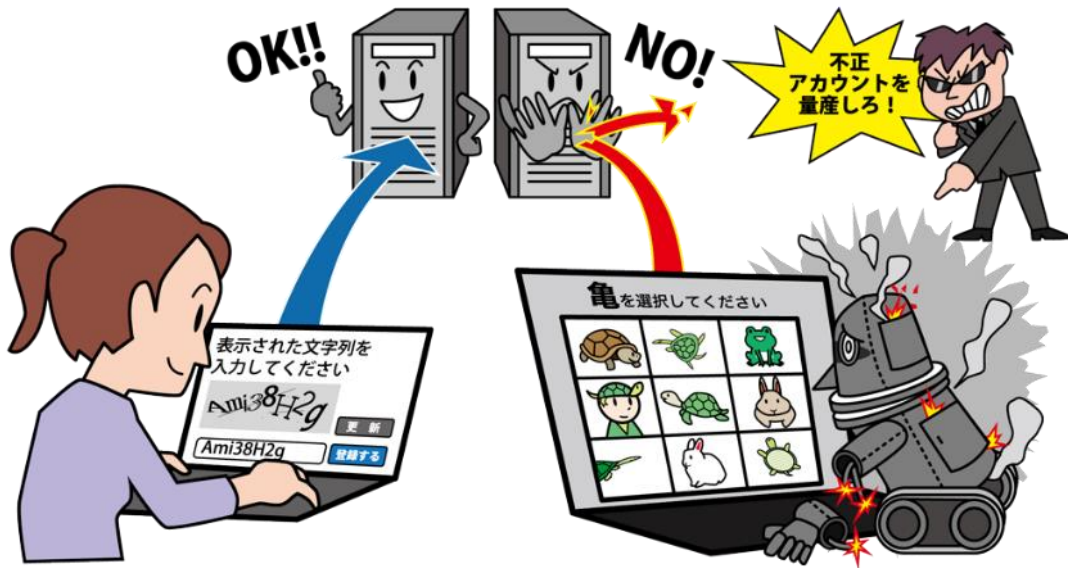
◆ 3D セキュアの利用方法

クレジットカードを発行する際に3D セキュアに対応しているカードブランドであり、事前にカード会社で必要な手続きを行っていただければ利用する準備は完了です。また、3D セキュアに対応していないECサイトでの決済時には利用できないため、注意が必要です。

◆ 3D セキュアの動向

2023年3月、経済産業省がクレジットカード・セキュリティガイドラインを改訂し、2025年3月末までにEMV3-Dセキュア(3Dセキュア2.0)の導入を原則全てのEC加盟店に求めています。クレジットカード利用者は3Dセキュアを理解し、利用することで自身の財産を守りましょう。

2.6. CAPTCHA(キャプチャ)認証



インターネットを閲覧している際に「私はロボットではありません」という文字が表示されて、チェックボックス(☑)をつけたり、表示された画像内にあるいびつな文字列の入力を求められたりしたことはないでしょうか？これらは操作しているのが人間であることを確かめる仕組みであり、CAPTCHA 認証(キャプチャ認証)と言います。

◆ CAPTCHA 認証とは？

CAPTCHA とは、Completely Automated Public Turing test to tell Computers and Humans Apart の頭文字を取った略語です。キャプチャと聞くと画面を画像として保存することを想像する方もいらっしゃるかもしれませんがそれとは別物で、人間とコンピュータを区別するテストを意味します。このテストのことをチューリングテストと言ひ、CAPCHA 認証はその1つです。

◆ なぜ CAPTCHA 認証をするの？

サーバへの攻撃手法に DoS 攻撃、DDoS 攻撃と呼ばれる、大量アクセスを発生させる手法があります。この攻撃を受けるとシステムの処理が遅くなったり、停止したりするおそれがあります。また、大量な迷惑メッセージの投稿をしたり、大量な不正ユーザー登録を行い、それを悪用したりするおそれもあります。このような大量に操作を行う攻撃はロボットで行われるため、ロボットでは対応できない操作をさせることで被害を防ぐ CAPTCHA 認証を行ひ

ます。

◆ CAPTCHA 認証の種類

CAPTCHA 認証はログイン認証のように、ID とパスワードを入力するといった1パターンではなくいくつかの種類があります。その一部を紹介します。

- ① チェックをさせる
「私はロボットではありません」のような文言と共にチェックボックスを表示させ、利用者にチェックを選択させる
- ② 文字列を入力させる
いびつな文字列を表示して、利用者に入力させる
- ③ 画像を判別させる
画像をいくつかに分割させ、例えば「車」が写っているものを利用者に選ばせる
- ④ パズルを解かせる
パズルの1ピース欠けた画像と最後のピースを表示させ、利用者完成させる

他にも種類はありますがいずれもロボットでは判別しにくいものになっています。

**3章. あっていますか？あなたの意識。
～改めて確認しましょう～**

3.1. HDD(ハードディスク)のデータ消去



日々利用しているパソコンの HDD(ハードディスク)には様々な情報が含まれています。パソコンを廃棄したり誰かに譲ったりすることを考えた場合、HDD 内に含まれている情報は第三者に見られないように安全に削除したいと思いますか？

◆ パソコンのデータ(ファイル)削除

通常パソコンのファイルを削除する場合には、削除するファイルのアイコンをドラッグ & ドロップでごみ箱に移したり、ファイルのアイコンを右クリックして「削除」を選ぶ等でごみ箱に移したりしていると思います。実は、ファイルをごみ箱に移してごみ箱を空にする操作は、ファイル自体を削除しているのではなく、ファイルの保管場所情報を削除しているだけです。一見ファイルは見えなくなるのですが、実際には HDD の中には残っている状態です。

◆ パソコンのデータ復元ソフト

パソコンには、ごみ箱で削除したファイルを復元するための、データ復元ソフトというものがあります。誤って重要なファイルをごみ箱で削除してしまった場合でもファイルを復元できる可能性がある有用なソフトです。ただし見方を変えると、自身が利用していたパソコンを第三者が再利用する際、自身で消したはずのデータを第三者がデータ復元ソフトを使用して復元してしまうおそれもあります。

◆ パソコンのデータ消去ソフト

パソコン内のデータを消去する、データ消去ソフトというものがあります。これを使用すると、データを強制的に上書きすることで、復元ソフトでも復元できないように元のデータを削除することができます。そのため、安心してパソコンを廃棄したり、第三者に譲ったりできるようになります。なお、最近では HDD のみではなく SSD を搭載したパソコンが増えてきましたが、SSD 用のデータ消去ソフトもあります。

◆ パソコン廃棄時のデータ消去

2013 年に小型家電リサイクル法が施行後、パソコンを廃棄するには家電量販店のパソコン回収サービスを利用する方法等が一般的です。この場合、自身でデータ消去ソフトにてデータを消去してから回収してもらったり、家電量販店のデータ消去サービス等でデータを消去してもらったりといった方法があります。これら以外にも無料の回収サービスを利用する方法もありますが、適切にデータ消去を実施してくれるかサービス内容をよく確認することが大切です。

3.2. その他の IT 用語

◆ 踏み台

「踏み台」という言葉を聞いて、どんなことを想像しますか？一般的には、高い所にある物を取るときに足場にする台のことを指し、これを想像する方が多いと思います。しかし、IT用語としての「踏み台」は全く別の意味を持ちます。攻撃者は自分の端末やアカウントから直接標的への不正アクセスや迷惑メールを発信するとは限りません。自分と標的の間に中継地点を用意して攻撃することがあります。この中継地点を「踏み台」と呼びます。この中継地点にはあなたのPCやメールアドレスが使われてしまうこともあるのです。

それでは、どのような状況で中継地点にされてしまうのでしょうか？例えば、PC、スマートフォン等にインストールしたソフトウェアやアプリに脆弱性が見つかり、修正プログラムが公開されているにもかかわらずアップデートをしていない状況が挙げられます。攻撃者に脆弱性を悪用され、PC やスマートフォンの操作権限を奪われたり、利用しているサービスのアカウントに対する認証情報を窃取されたりすることで不正に利用されてしまいます。攻撃者は踏み台を使うことで、自身の身元を隠し、PCやスマートフォンの所持者に嫌疑がかかるようにするのです。

◆ マルウェア

あなたはニュースや新聞等で「マルウェア」という言葉を聞いたことがありますか？マルウェアとは 2 つの単語「malicious」と「software」からなる造語であり、「悪意のあるソフトウェアやプログラム」の総称です。これにはいくつかの要素が含まれており、「ウイルス」や「ワーム」、「トロイの木馬」がそれに当たります。ウイルスやワームと聞くと人間が感染するウイルスや、ミズのような虫を想像してしまうかもしれませんが、IT用語としてのウイルスやワーム、トロ

イの木馬もその正体はプログラムなのです。

いずれも PC やスマートフォン等に悪影響を及ぼすものであることには変わりはないのですが、その働き方が異なっているため、分けて呼ばれています。

例えば、ウイルスは自身だけでは活動ができません。アプリやソフトウェアのプログラムの一部を悪意のあるプログラム書き換えて動作します。

ワームはウイルスと違い、アプリやソフトウェアの一部を書き換えるのではなく、自身が悪意のあるプログラムとして動作することができます。

トロイの木馬は無害なプログラムに偽装してインストールさせ、PC やスマートフォンに入り込んだ後で悪意の動作をします。

マルウェアとはこういった悪意のあるプログラムを総称しているのです。

なお、「情報セキュリティ 10 大脅威」では、便宜上、多くの人に馴染みがある「ウイルス」という名称を使用しています。

◆ 炎上

「〇〇さんが炎上している」という言葉を見聞きしたことはありませんか？これらは誰かが本当に燃えている訳ではありません。主に SNS を使用して、発信者の言動に批判が殺到している状態を「炎上」と言います。

また、炎上するという事は注目が集まっている状態でもあるため、それを利用して商売に繋げるケースがあり、炎上商法と呼ばれています。

一度炎上してしまうと問題となった発信を削除しても批判が止まらなかったり、削除したことさらに批判を受けたりするおそれもあります。

モラルに反することや過激な内容を SNS で発信しないこと、感情任せではなく発信する前

に一度冷静になって内容に問題がないかを確認すること、などの対応が必要です。

添えられていたとしても本当の情報なのか疑ってみるようにしましょう。

◆ スクショ(スクリーンショット)/キャプチャ

スクショ(スクリーンショット)やキャプチャは、いずれもスマートフォンやPC等の画面に表示された内容を画像として保存することを言います。

スクリーンショットを保存する方法は使用している機器によって異なりますが、自身が使用している機器の名称とスクリーンショットというキーワードで検索することで大抵は手順が紹介されているページが見つかります。

自身が記録しておきたいときはもちろん、使用しているPCやスマートフォン、アプリが何らかのエラーになり、サポート窓口やITに詳しい友人などに問い合わせる際にそのエラー画面のスクリーンショットも添えることで素早い解決につながります。

◆ フェイクニュース/デマ

フェイクニュースやデマはいずれも嘘の情報のことを指します。テレビ番組やインターネット上の信頼できるニュースサイトであれば故意に嘘の情報を発信することはありません。

一方で、SNS上の個人の発信やブログ記事には真偽が定かではないものも含まれており、デマが出回ることも多く、これは故意に嘘の情報を発信していることや、誤った情報が含まれていることなどのおそれがあります。文字だけの発信であれば、疑うであろう情報も、これに画像が添えられると信じてしまいがちです。さらに、巧妙に加工した画像を使うことで、嘘の情報を本当の情報のように発信していることもあります。SNSの発信は画像や動画も

情報セキュリティ 10 大脅威

知っておきたい用語や仕組み

2023 年 5 月 30 日 発行

[著作・制作] 独立行政法人情報処理推進機構 (IPA)

[イラスト制作] 株式会社 創樹

[事務局・発行] 独立行政法人情報処理推進機構

〒113-6591

東京都文京区本駒込二丁目 28 番 8 号

文京グリーンコートセンターオフィス

<https://www.ipa.go.jp/>