インターネットの
安全・安心ハンドブック

NISC 内閣サイバーセキュリティセンター
National center of Incident readiness and Strategy for Cybersecurity

一般利用者向け 抜粋版

Ver 5.10

知る・守る・続ける
サイバーセキュリティ普及啓発

協力
警察庁 National Police Agency
総務省
経済産業省
IPA 独立行政法人 情報処理推進機構

目次

はじめに

みなさん、はじめまして。私たちは内閣サイバーセキュリティセンター(NISC) です。日本の政府機関で、国のサイバーセキュリティ政策を担当しています。突然ですが、世界中のコミュニケーションの手段と聞いたら、みなさんは何を思い浮かべるでしょうか？手紙、会話、写真、プレゼント、などいろいろなものを連想されるかもしれません。

その中でも、形は見えないけれど現代においては「インターネット」という技術が主役の1つだろう、と何となく意識されている方も多いのではないでしょうか。

インターネットによりコミュニケーションのスタイルは大きく変わりました。インターネットが普及していない昔は、どんな場所にも設置されていた公衆電話で連絡を取ることは普通でしたが、インターネットが身近になると小型化された携帯電話、いわゆるガラケーが普及しました。当時のインターネットの通信速度では、ガラケーを使って短い文章、すなわちメッセージを送る形のコミュニケーションが主流でした。

そして現代、インターネットの通信速度も安定し、大半の国民がパソコンだけでなく、スマホを所有しています。スマホは単なる電話機ではなく、「持ち歩ける小さなパソコン」と呼べるほど多機能なもので、基本的には常にインターネットに接続しています。多くの人がスマホやパソコンからチャットしたり、SNSで写真を送りあったり、映像付きのインターネット電話を使ったりして、家族や友人とのコミュニケーションを楽しんでいます。コミュニケーションの用途以外にも、調べたいことがあればブラウザでウェブサイトを検索したり、オンラインストアで買い物をしたりして、インターネットにつながったサービスに多くの人が慣れ親しんでいます。またクラウドと呼ばれるインターネット上のサーバから業務上必要なデータの保存・共有をしたり、コロナ禍で普及したテレビ会議アプリでリモート会議をしたりと、仕事で多用している人もいるでしょう。さらには社会保障や税関係など、スマホやパソコンがあればできる行政機関への申請・申告も増えています。

もはや現代において、スマホやパソコンからインターネットにつながり、民間企業・公的機関問わず、無料・有料含めて、さまざまなサービスを利用することは、家庭や職場、学校と生活のあらゆる場面で求められています。多様なサービスにつながり多くのコミュニティが形づくられ、インターネット上には1つの社会領域といえる「サイバー空間」が形成されています。

そのような便利で欠かすことのできないサイバー空間は、地域や老若

男女問わず、全国民が参画する基礎的なインフラであると呼べ、私たちが社会経済活動を営む上で重要かつ公共性の高い場として位置付けられるものです。

しかし、このサイバー空間、便利さもあれば、問題もあります。

世界中の人と距離を超えてつながるため、中には、自らの利益や自己顕示のために平気で他人の情報や財産を奪おうと悪事を働く者ともつながってしまいます。そのような悪事を働く者は、ありとあらゆる手段を用いて、スマホやパソコン、ルータなどのIT機器に対して、「マルウェア」という不正なプログラムを送りつけようとしています。インターネットにつながるということは、常にそのようなサイバー攻撃のリスクにさらされているのです。

また、SNSなどで自分の発言を広く読んでもらい自由に他の人と交流できることは、インターネットにつながることで享受できるメリットの1つですが、接する人が常に自分と友好的な意見であるとは限りません。感情的になり、誹謗中傷といえるような発言が飛び交うことも珍しくありません。しかし、SNSでの発言から、精神的に追い詰められ、自らを傷付ける行為を選んでしまう人や事例も残念ながら生じています。面と向かって言えないような他人を傷付ける発言は、インターネット上でも決して発信してはいけないのです。

サイバー空間が、人々のくらしと密接につながり基礎的なインフラとなりつつある中、国民全員が、誰一人取り残されずその恩恵を享受していくためには、国民一人ひとりが能動的にサイバー空間における攻撃や脅威の存在を知り、サイバーセキュリティに関する素養・基本的な知識を身に付けていくことが必須です。スマホやパソコンを使ってインターネットにつながるときは、みんなが常にサイバーセキュリティ対策を心掛けるべきなのです。

そのため本書では、サイバー攻撃の手口やリスク、そして被害とはどんなものがあるのかをイメージしやすくなるように、身近な具体例を取り上げながら解説しています。そして、被害を受けないようにするにはどんな対策をすればよいのか？また被害を受けてしまった場合はどんな対処をすればよいのか？についても、具体的な手順や頼れる相談窓口を紹介しています。

ほかにも、

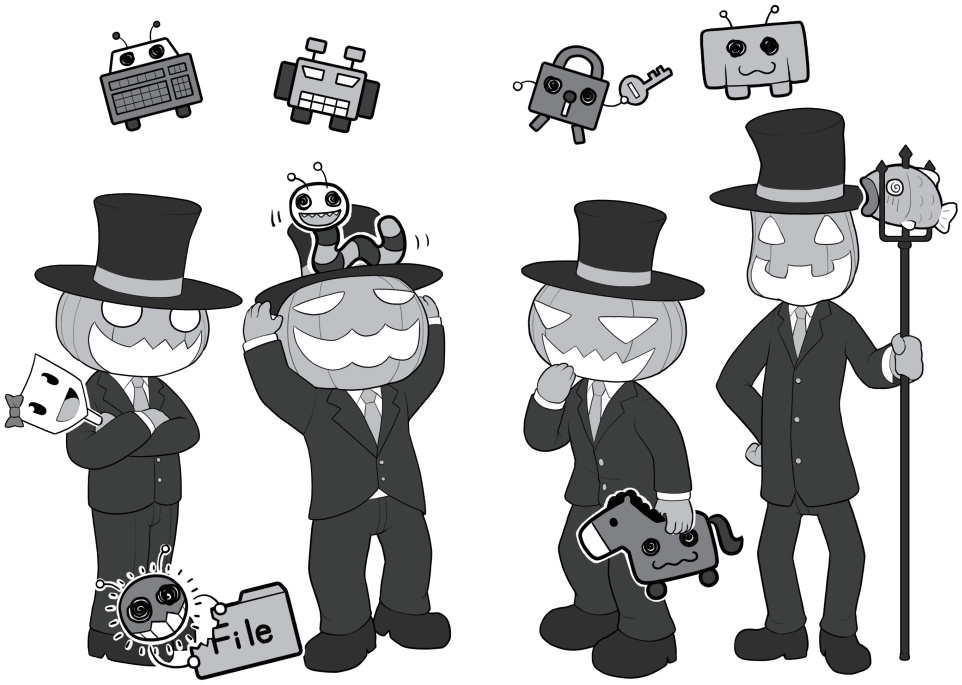
- **サイバー攻撃を防ぐための基本となるパスワードの適切な管理**
- **こどもやシニアが安全にインターネット上のサービスを利用するための方法**
- **SNSなどで多くの人と交流する際に気を付けたいマナーや法律**
- **スマホやパソコンを不安なく利用するための設定**

このイラストはインターネット上の悪意の人たちである攻撃者と、彼らが使う武器である「コンピュータウイルス（正確にはマルウェア）」をキャラクターにしたものです。

サイバー空間（インターネット）を悪意を持って利用し、自らの利益のためには他人の情報や財産を容赦なく奪い、ときにサイバー攻撃を通じて自己顕示欲を満たすといった、さまざまな悪事を働きます。

また、彼らが普通の人の仮面を被り、あるいは普通の人々が彼らの仮面を被ることもあります。

解説のイラストではそのあたりをきちんと描き分けていきますので、じっくり見てくださいね。

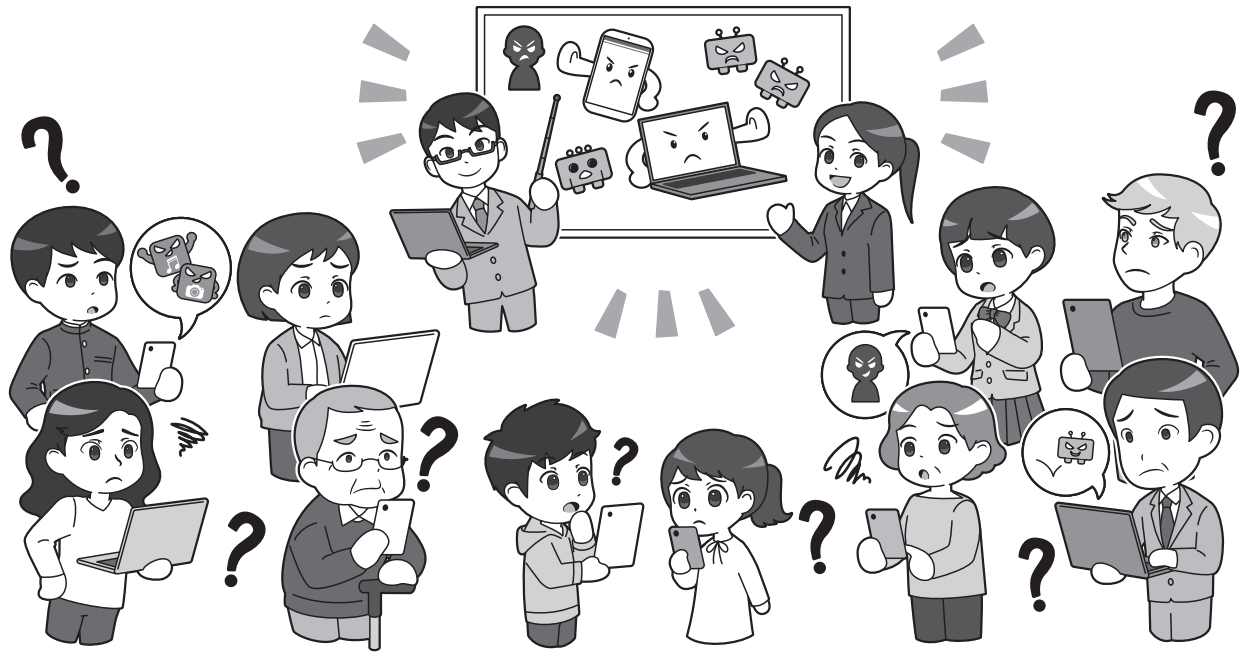


- **インターネットにおける通信の安全性を支える暗号化の基本**
- **中小企業等のセキュリティ部門担当者に役立つ情報**

など、サイバーセキュリティ対策に必要な内容を幅広く取り上げ、いずれも読む前には専門知識を必要としない形でやさしく説明しています。本書を読んで、安全・安心なサイバー空間を一緒に作っていきましょう。

また、NISCでは、本書だけにとどまらず、「みんなで使おうサイバーセキュリティ・ポータルサイト」を運営して、サイバーセキュリティの普及啓発や人材育成に取り組んでいます。

ポータルサイトでは、こども、シニア、企業の一般社員・経営者など対象者別に適したセキュリティ施策の紹介や、セキュリティ施策におけるセミナーやイベントの実施状況などを公開しています。本書やポータルサイトをご覧いただき、国民一人ひとりのサイバーセキュリティ対策の意識を高められれば幸いです。



「みんなで使おうサイバーセキュリティ・ポータルサイト」

https://security-portal.nisc.go.jp/

※ご注意

本書では、初心者の方にサイバーセキュリティ関連の問題を理解してもらうために、実際のケースと比較してわかりやすく簡略化したり、内容を理解しやすいように関連する事項の一部を省略したりして記述している場合があります。ご了承ください。

このハンドブックを読んで、よりサイバーセキュリティに関する理解を深めていきたいと思う方は、ぜひステップアップして、さまざまな専門誌や最新の記事にチャレンジしていただけると幸いです。

なお、登場する人物、および、団体は架空のものであり、実在するいかなる人物・団体とも関係はありません。

1 最低限実施すべきサイバーセキュリティ対策を理解しよう

攻撃者（悪意のハッカー）による攻撃を防ぐには、まずはパソコンやスマホの基本的なセキュリティを固め、また、トラブルが発生したときの対処手段を知ることが重要です。

現在、政府機関が掲げるサイバーセキュリティ対策の指針としては、NISC（内閣官房内閣サイバーセキュリティセンター）が「サイバーセキュリティ対策９か条」を公開しています。一般国民の誰もが最低限実施すべき対策をまとめており、本ハンドブックもこの９か条に則ってサイバーセキュリティ対策を解説していきます。

まず「**① OS やソフトウェアは常に最新の状態にしておこう**」はいわゆるアップデートのことです。 IT 機器にはセキュリティホールと呼ばれる弱点が日々見つかっています。一見、大丈夫そうに見えてもそれは「ただセキュリティホールが発見されていない」だけ。OSやソフトウェアメーカーが提供している修正用アップデートを常に適用し続け、攻撃の糸口となる穴を塞ぎます。

「**②パスワードは長く複雑にして、他と使い回さないようにしよう**」は、安全性の高いパスワードを設定する際の留意点、同じパスワードの使い回しの危険性、パスワードの適切な管理方法について解説します。

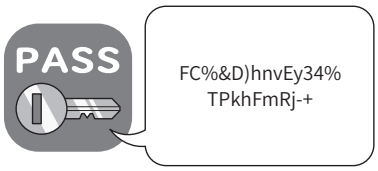
「**③多要素認証を利用しよう**」は、サービスへのログインを安全に行うために、二要素以上を使って認証作業をする多要素認証について解説します。認証用アプリや生体認証を利用するとログインの安全性を高められます。

「**④偽メールや偽サイトに騙されないように用心しよう**」は、フィッシング詐欺メールが多様化しており攻撃が複雑になっていることや、信頼できるサイト以外からアプリをインストールする危険性を解説します。

①OSやソフトウェアは常に最新の状態にしておこう

OS やソフトウェアを最新に状態にする理由は、最新の攻撃情報への対策が盛り込まれているからです。

②パスワードは長く複雑にして、他と使い回さないようにしよう



安全なパスワードの作成方法はもちろん多要素認証の重要性を説明します。

③多要素認証を利用しよう

認証用アプリや生体認証を利用したより安全性の高い多要素認証について説明します。

④偽メールや偽サイトに騙されないように用心しよう

多様化・複雑化するフィッシング詐欺メールや、信頼できるサイト以外からアプリをインストールする危険性について解説します。

「**⑤メールの添付ファイルや本文中のリンクに注意しよう**」は、「Emotet」のように、マルウェア添付メールで広がる感染、標的型メールやスパムメールの実例を挙げ、具体的リスクについて解説します。

「**⑥スマホや パソコン の画面ロックを利用しよう**」は、スマホやパソコン(PC)の情報を守るにはまず待ち受け画面をロックすることが第一であることを解説します。また、生体認証を使用したロックの利点や、安易に他人へ端末を渡す危険性についても触れます。

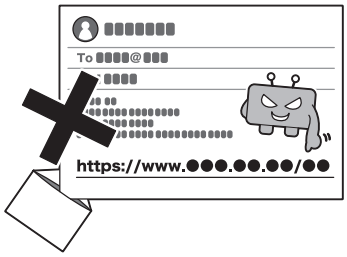
「**⑦大切な情報は失う前にバックアップ(複製)しよう**」は、普段からバックアップをとっておくことがどれほど重要か解説します。正常な状態のファイルをバックアップして保管しておくことで、仮に攻撃を許して重要なファイルを失ってしまっても、バックアップから復元することにより、被害を軽減します。とくに昨今増加しているランサムウェア攻撃に対してもバックアップを準備しておくことは有効です。

「**⑧外出先では紛失・盗難・覗き見に注意しよう**」は、勤務先や外出先でスマホやパソコンを使う際、覗き見されるショルダーハッキングなどのリスクなどについて解説します。また、飲食店などで離席時に端末を置いていく人を時折見かけますが非常に危険な行為です。公衆の場でスマホやパソコンを利用するときに注意すべきことについて把握しましょう。

「**⑨困ったときは１人で悩まず、まず相談しよう**」は、サイバー攻撃などインターネットの被害で自分だけでは対処できないときには、積極的に警察や IPA などの窓口へ相談する重要性を解説します。あらかじめ窓口を調べておくことで、困ったときにすぐに相談できるようになります。

*「サイバーセキュリティ9か条」https://security-portal.nisc.go.jp/guidance/cybersecurity9principles.html

⑤メールの添付ファイルや本文中のリンクに注意しよう

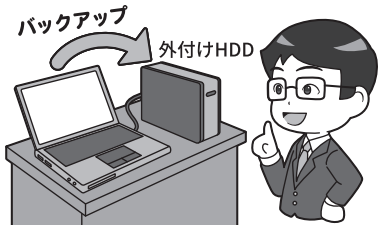


被害がなくならない「Emotet」、標的型メール、スパムメールの実例を紹介

⑥スマホやパソコンの画面ロックを利用しよう

スマホやパソコン（PC）の情報を守るにはまず待ち受け画面をロックすることが第一。そして生体認証が推奨

⑦大切な情報は失う前にバックアップ(複製)しよう

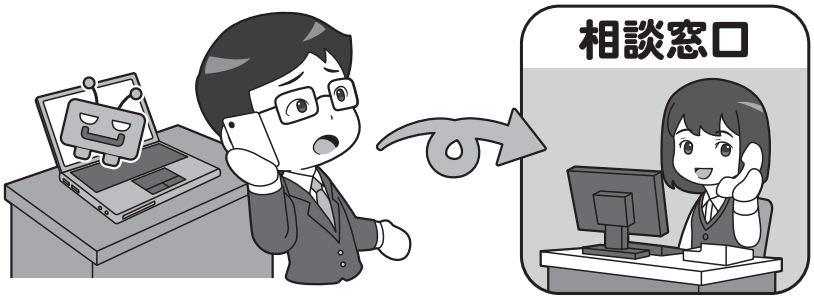


たとえ攻撃されても、適切にバックアップしておけば、すぐに復旧できます。

⑧外出先では紛失・盗難・覗き見に注意しよう

公衆の場における、ショルダーハッキングのリスク、スマホやパソコンの紛失・盗難など、利用時の注意すべきことを把握しましょう。

⑨困ったときは１人で悩まず、まず相談しよう



攻撃されたとき、どうしたらよいか分からないからとそのまま放置せず、相談窓口に相談しましょう。また、実質的な被害が出ている場合は、警察などの関係機関に報告した方がよい場合もあります。いざというとき慌てないように、あらかじめ連絡先を調べておきましょう。

①OSやソフトウェアは常に最新の状態にしておこう

①.1 パソコン本体とセキュリティの状態を最新に保とう

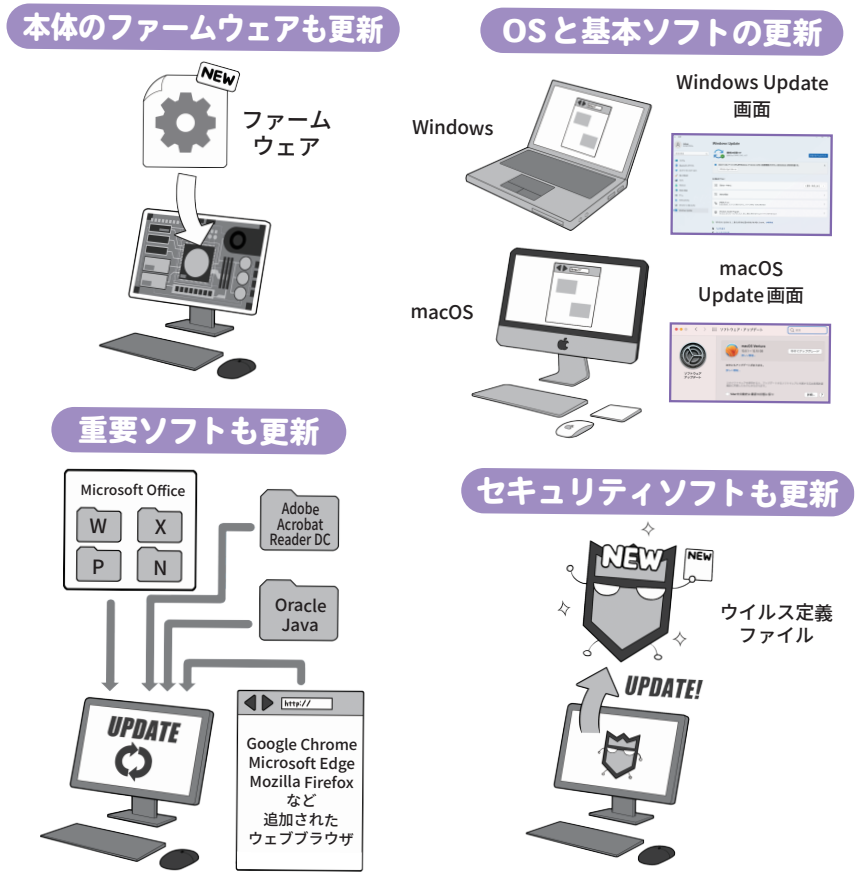
悪意の攻撃からパソコンを守る第一歩は、セキュリティを最新に保ち、各種のアップデート（バージョンアップ）を行うことです。

最近の機種では、OS関連のアップデート処理は自動で行われるか、アップデートを行うよう通知が出るようになっています。しかし、緊急でアップデートを行った方がよいときもあります。セキュリティ関連ニュースサイトなどでアップデートを促す情報が流れていたら、自主的に更新処理をかけるようにしましょう。Office製品などOSのメーカーが作っている重要なソフトもここで同時にアップデートします。

次に、サイバー攻撃で狙われやすいソフトウェアの更新を重点的に行いましょう。Adobe社Acrobat ReaderやOracle社Javaまたはその実行環境、そしてGoogle Chromeをはじめとする各種のウェブブラウザや、ブラウザの機能を拡張するプラグインは攻撃のターゲットになりやすいのです。

また、機器そのものの基本プログラムを更新するファームウェアアップデートにも気を配りましょう。こちらの更新通知は、自動で出る機器と出ない機器があるので、機器のアップデート情報は、どのようにすれば入手できるか、事前に確認して気を配ってください。セキュリティソフトをインストールしている場合は、最新のウイルス定義ファイルに自動更新されるよう設定しておきましょう。

本体もOSもセキュリティソフトも重要ソフトもアップデート



OSやファームウェアなどは、ほとんどのパソコンで利用されており、社会でいえば鉄道や電気ガス水道のような社会インフラに相当します。

利用する側もアップデート（更新）が必要になれば速やかに適用して、攻撃者が攻撃できないようにしましょう。インストールしてあるが使っていないソフトは削除（アンインストール）してしまってもよいでしょう。

ボットネットも、そもそも攻撃して乗っ取れる機器がなければ成立しないように、攻撃できる穴を作らない1人1人の行動が、安全なインターネットを作り社会インフラを支えるのです。

なお、OSやソフトウェア、ファームウェアは、開発者がアップデートの期限を設定するものが多く、この期限を過ぎるとアップデートが提供されなくなります。

アップデートが提供されなくなったOSやソフトウェアは、セキュリティホールが見つかっても修正用アップデートが提供されず、攻撃に対して非常にぜい弱なので、使用しないようにしてください。

①.2 スマホやネットワーク機器も最新に保とう

スマホも同様に各種のアップデートの適用が必須です。スマホの場合、比較的アップデートの通知がわかりやすくなっており、自動アップデート機能も充実しています。機器本体のファームウェアのアップデートでも、OS のアップデートでも、いつも使用している一般のアプリのアップデートでも、更新の通知が出たら、マメに適用するようにしましょう。

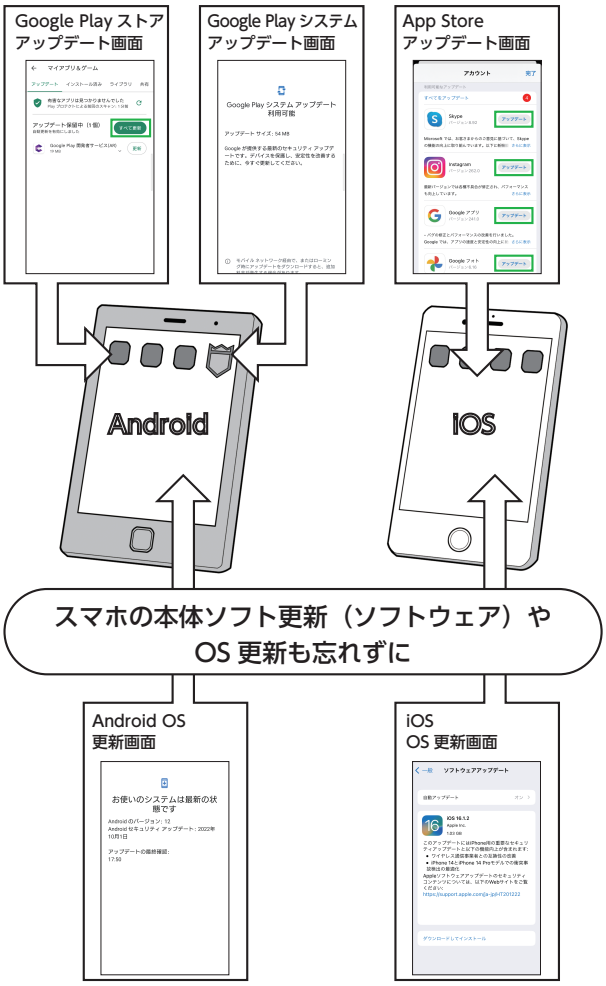
そのためには、本体のファームウェア（ソフトウェア更新やシステムアップデートと書かれることも）や OS の更新が、設定メニュー上のどこにあるのかと、更新の手順を確認しておきましょう。アプリの更新が自動になっているかも確認しましょう。すでに保守期間等がすぎて、ファームウェア等が更新できない場合には、以降の安全性が確保されないため、買い替え等も検討しましょう。

スマホアプリの自動更新は、設定によっては無線 LAN 接続時のみ自動で行うことになっている場合もありますが、その設定でも更新時に権限変更で確認が必要な場合は自動更新されないこともあるので、気が付いたら未更新のアプリがたくさんたまったままになってしまっていることもあります。日に一度は意識してアップデート画面に行き、更新するように心がけましょう。

また、ネットワークにつながるルータや IoT 機器、スマート家電、ネットワークカメラなどもぜい弱性を狙った攻撃の対象となるため、ファームウェアが自動更新されるよう設定しておきましょう。近時は国際情勢の影響もあり、更新されていないネットワーク機器を狙う攻撃が増加しました。

ルータはここ数年で自動更新機能搭載のものが普及してきているので、可能であれば買い換えましょう。

アプリやセキュリティソフトの更新は自動更新にしつつ、まめにチェック



ネットにつながるIT機器（ルータやIoT機器）もファームウェア更新や管理者用初期IDとパスワードの変更をしておくこと

無線 LAN アクセスルータ　ネットワーク対応プリンタ　ネットワークカメラ

IoT 機器のファームウェアの更新は、通常はウェブブラウザで本体にアクセスして行います。このときの管理者用 ID とパスワードは、必ず購入時の初期のものから変更しておきましょう。同じ機種で共通だった場合など、不正アクセスされ乗っ取られてサイバー攻撃に使われます。

②パスワードは長く複雑にして、他と使い回さないようにしよう

②.1 パスワードってなに？

私たちが、スマホやパソコンなどのIT機器や、各種のウェブサービスを使う上で、欠かせないのが「パスワード」です。

機器やウェブサービスを利用するときに、正当な利用者や持ち主である自分だけが利用でき、他人が利用できないようにするための鍵の役割を果たすものです。

パスワードは、いわば「家の鍵」や「金庫の鍵」。これを適切に守らなければ、家や車、金庫を勝手に開けられてしまうように、パソコンやスマホ、ウェブサービス上にある私たちの個人情報やメール、銀行口座が攻撃者に不正にアクセスされ、情報が流出したり、お金を盗まれたりしてしまいます。

②.2 パスワードの安全性を高める

サイバー攻撃には、相手の機器をマルウェアに感染させて乗っ取る方法の他に、なんらかの手段でIDとパスワードを解明し、サービスや機器を乗っ取る方法もあります。

パスワードは利用しているウェブサービスなどから大量流出したものが使われる「リスト型攻撃」、文字の組み合わせをすべて試す「総当たり攻撃」、パスワードによく使われる文字列を利用する「辞書攻撃」などにより探し当てる方法や、IoT機器のパスワードを購入時のまま利用していると乗っ取られることもあります。

総当たり攻撃を防ぐには、探り当てるまでに膨大な時間がかかるようにするのが一番の防御手段で、それには1桁の文字の種類と桁数による組み合わせを増やします。例えば数字だけなら1桁10通りしかありませんが、英字を入れると36通り、英大文字小文字を入れると62通り、これに33文字の記号を入れると95通りになります。これに桁を増やして、累乗で組み合わせを増やすわけです。総当たり攻撃は、理論上攻撃し続ければいつかは成功するのですが「時間がかかり事実上不可能な状態」にして防ぐのです。長いが覚えやすいパスワードにするか、短いが複雑なパスワードにするかは、好みの問題ともいえますが、最近では、桁数をできるだけ長くする方が安全であると言われています。さらにより安全にしたい場合には記号を入れることで安全性を高めるに、こしたことはありません。

ログイン用パスワードは、長くすることでより安全に

「数字＋英大文字＋英小文字」の８桁だと→約218兆通り
「数字＋英大文字＋英小文字」の12桁だと→約32垓通り

同じ文字種でも、パスワードを長く設定することで推認されにくくなります。

数字＋英大文字＋英小文字の組み合わせ数（例）

数字	英大文字	英小文字	合計	８桁（通り）	12桁（通り）	８桁と12桁の比較（倍）
10	26	ー	36	2,821,109,907,456	4,738,381,338,321,616,896	1,679,616
10	26	26	62	218,340,105,584,896	3,226,266,762,397,899,821,056	14,776,336

②.3 機器やサービス間でのパスワード使い回しは「絶対に」しない

複雑なパスワードを使っても、それを複数のサービスや機器の間で使い回していれば意味がありません。1カ所から漏れればすべてのサービス等でログイン可能になってしまうからです。複雑なパスワードを1つ決めて、あとはおしりに数字や規則性のある文字を付けるのも、2つ以上漏れれば推測されます。それぞれに複雑なパスワードを設定し、使い回しをしないことが大切です。但し実際にすべての規則性のないパスワードを記憶することは、難しいため、次ページに示すような形で適切なパスワード管理をすることが重要です。

同じパスワードを使い回さない。似たパスワード、単純な法則性のあるパスワードも×

	白うさ ネットワーク	おさるさん 銀行	三毛猫電気	
×使い回し	PASSPPOI	PASSPPOI	PASSPPOI	1個漏れたら一網打尽
×単純な法則性あり	USAGIPPOI	OSARUPPOI	NEKOPPOI	法則性がばれたらおしまい

②.4 秘密の質問は注意する

ウェブサービスの中には、パスワードを忘れてしまった場合や、あるいはいつもと違うログインがあった場合の本人確認のために「秘密の質問」と呼ばれる機能で対応しようとするものがあります。これはあらかじめ利用者が、自分しか知らない質問と答えを設定しておいて、合い言葉的にこれに答え、本人であることを証明するものです。

しかしこの秘密の質問は、自分で質問を作れるものもありますが、多くは「生まれた市は」、「ペットの犬の名前は」と回答が類推しやすいものが大半です。

SNSが普及した今、SNSの過去の投稿から簡単に見つけられることもあり、安全性が高いとはいえません。

秘密の質問に答えを設定する場合は推測できないものにし、忘れないようにパスワード管理アプリなどに保存しましょう。

②.5 パスワードを適切に保管する

使い回しをせず充分な複雑さと長さを持ったパスワードは、総当たり攻撃では突破されにくくなります。

しかし、適切に管理しておかず、別の方法で盗まれてしまってはひとたまりもありません。

例えばパソコンや壁に貼っていれば、誰かがそれを見て覚えてしまいますし、テキストファイルにまとめておけばマルウェアに感染したときに流出し、多くのアカウントが一気に乗っ取られるかもしれません。

パソコンでウェブブラウザにパスワードなどを覚えさせる「自動入力」機能も要注意です。あなたが席を離れた隙に、誰かがブラウザでウェブサービスを利用してしまうかもしれません。それにノートパソコンならば本体ごと盗まれることもあります。パスワードは基本的に利用する場所で保管してはいけないのです。

しかし、多くのサービスで複雑なパスワードをそれぞれ設定したら、とても覚えきることはできません。ではどうしたらよいでしょう。

具体的にはいくつかの方法が挙げられます。例えば、パスワードを管理する紙のノートに書いてパソコンとは別に保管する方法や、アプリのメモ帳や表計算ソフト等で管理するなどで管理する方法が挙げられます。またスマホのパスワード管理アプリを利用したり、ブラウザのパスワード管理機能を利用したりする方法なども挙げられます。なお、紙で管理する場合以外は、クラウドでデータを保管する機能の利用は熟考し、過去に情報流出にまつわるトラブルのあったアプリやサービスは利用を避けるようにしましょう。それは他人の手元にIDやパスワードを保管することや、流出の危険が逆に増すことを意味するからです。

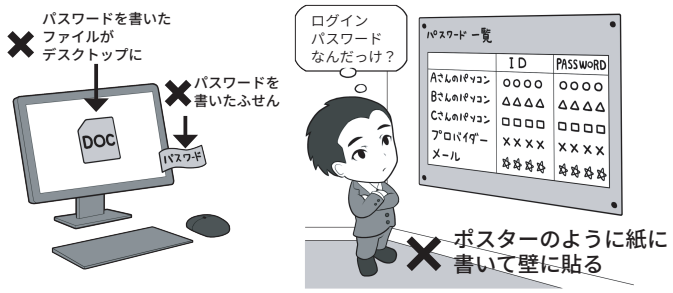
利用するところで保管するべきでないなら、スマホでパスワードを管理する場合リスクはありますが、こういったアプリは後述のPINコードや生体認証＋暗号化で情報がガードされます。盗まれても落としても、簡単に他人が使ったりすることはできません。

ただ、管理しているパスワードは、必ずバックアップするのを忘れないようにしましょう。

なお、紙で保存する場合には、紛失に備えて、予備を作成・保管しておき、その予備を参考にしながら早急にパスワードを変更することが必要です。また、パスワードを記録する際には、盗み見した者が記録されたパスワードを使用して、すぐに悪用できてしまう可能性を少しでも下げる工夫を施しておくと、より安全にパスワードを保管できます。

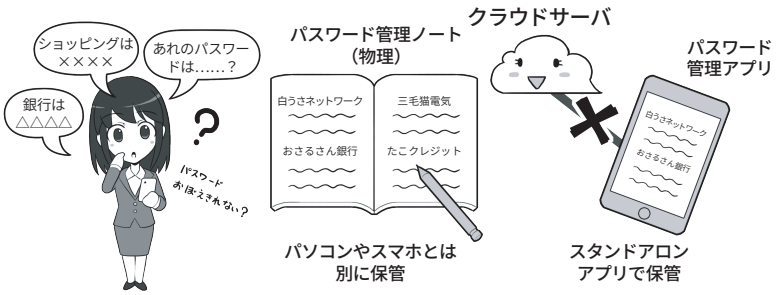
具体的には「実際には含まれない余分な文字を混ぜてノートに記録する」、「実際のパスワードは前後どちらかに2,3桁程度、暗記できる数の文字が追加されたものに設定して、すべての文字はノートに書き残さない」などがあります。

パスワードを使用する場所に置かない。パソコンの中も×



オフィスの中ならば外の人は見ないと判断するのは×。出入りの業者が見たり、外から双眼鏡で見たりすることもできるのです。内部の人間が勝手に使うリスクもあります。

パスワードは紙のノートに書いて保管するか、パスワード管理アプリで守る



クラウド保管＝ダメというわけではなく、それは利便性との兼ね合いです。アプリのバグや過去のトラブルは、アプリ名＋「トラブル」などで検索します。

③多要素認証を利用しよう

③.1 可能な限り多要素や生体認証を使う

サービスへのログインを安全に行うために、二要素以上を使って認証作業をする多要素認証などの方法が提供されていれば必ず設定しましょう。

例えば、最近の機器では顔、虹彩、指紋で本人確認をして機器のロック状態を解く、生体認証機能もあります。

生体認証は本人のみが使えて安全性が高く、肩越しの盗み見などよる暗証番号(PIN コード)の盗難には強い機能でもあります。ただ指紋認証などは寝ている間に勝手にロック解除されることがあり得るので過信は禁物です。

なお、生体認証はたいていは通常の PIN コードの替わりなので、スマホでは失敗すると通常の PIN コード入力に戻ります。誕生日などの個人情報を PIN コードにすると予想がされやすく、本体を盗まれてロック解除される可能性が上がるため使わないようにしましょう。

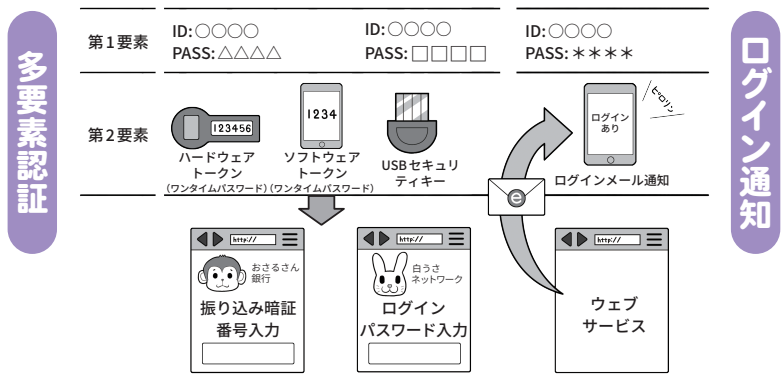
また通常のパスワードの他に、使い捨てにする別のパスワードを、ハードウェアトークンや生成アプリで作り、ログイン時に利用者に入力させます。なお、メールや SMS (ショートメッセージ。以降 SMS) を利用する方式もありますが、これらはその送信方法などによっては安全面で十分とは言えない場合があります。例えばウェブ上のサービスに対して、特定のスマホに対して SMS が送信される場合にはスマホを所持している人しかわからない情報なので、二要素認証として位置づけられますが、ウェブサービスに登録しているメールアドレスに送信される場合、安全性は低いと言えます。

その他、認証システムによっては、スマホなどへのプッシュ通知を多要素認証に組み入れることがあります。

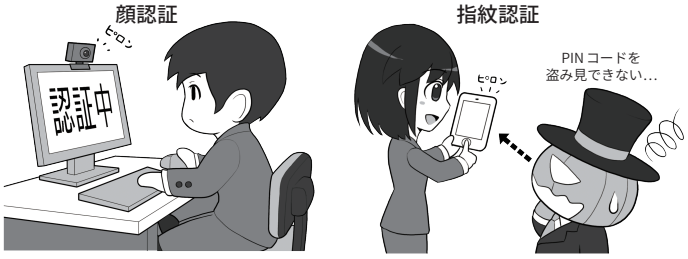
攻撃者がパスワードなどでの認証を成功させた場合にもプッシュ通知が送られるので見知らぬプッシュ通知には回答してはいけません。

その他にも、USB セキュリティキーなどで利用者を確認する方法や、不正アクセスの兆候を知る手段として、サービスに不審なログインがあったときにメールで利用者に通知を送る機能も存在するので、あれば活用しましょう。

多要素認証やログイン通知でセキュリティを向上



生体認証を使う

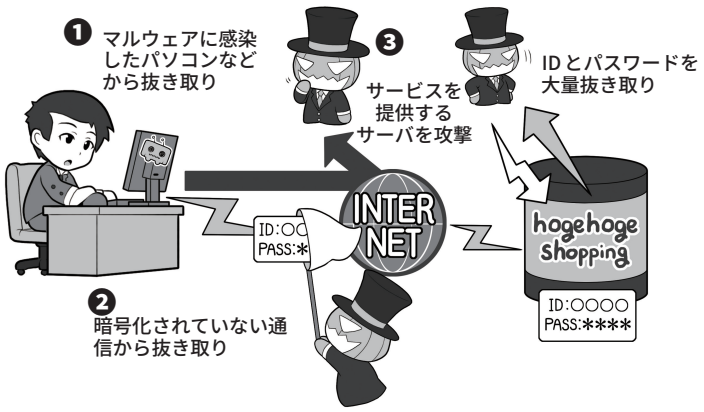


③.2 パスワードはどうやって漏れるの？どう使われるの？

さまざまなIDとパスワードの漏えいパターン

攻撃者にIDとパスワードが漏えいする事態は、機器がマルウェアに感染したり、自分が通信する過程で抜き取られたりする他に、利用しているサービス側からも流出するケースもあります。

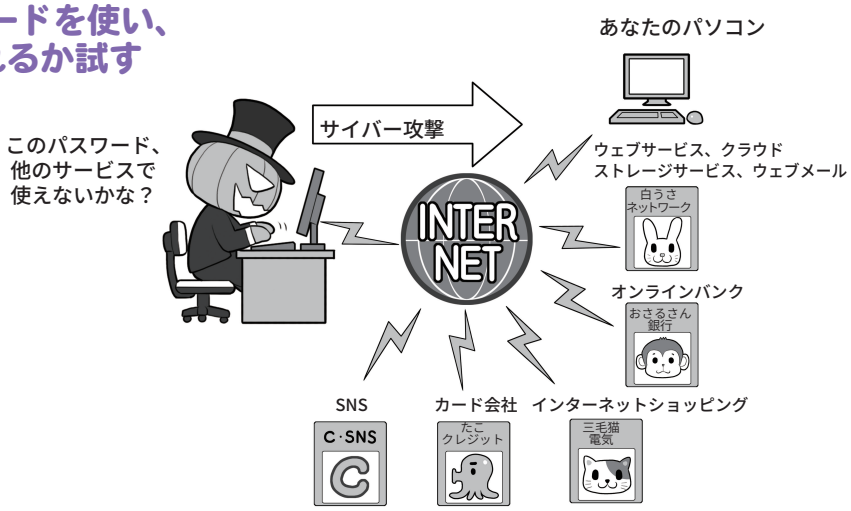
ニュースや通知でサービス側から流出が判明した場合は、速やかにパスワードを変更するなどの対応を取りましょう。



攻撃者は入手したIDとパスワードを使い、さまざまなサービスを乗っ取れるか試す

IDとパスワードをなんらかの手段で手に入れた攻撃者は、これをどこか別のサービスで使えないかさまざまな方法で試します。

こういった攻撃を成功させないために、パスワードの使い回しや、似たパスワード、パターンのあるパスワード、個人情報などから推測できるパスワードを利用するのはやめましょう。



私たちがパソコンやスマホ、あるいはSNSやウェブ上のサービスを利用するときに入力するIDやパスワード。サイバー攻撃でこれらの情報を盗まれると、かなり深刻な被害を起こしかねないものです。

では実際はどのように漏れてしまうのでしょう？

1つには、自分のパソコンなどがマルウェアに感染し、そのマルウェアがパスワードを盗み取って攻撃者に送信するケース。次に、ウェブサービスなどにログインするときに、私たちが利用する機器からウェブサービスまでの経路上のどこかで盗み取られてしまうケース。そして、ウェブサービス側でログインを認証するために控えとして持っているIDやパスワードが、攻撃者によって盗み取られ漏えいするケースなどがあります。

先ほど説明しましたが覚えておいてほしいのは、自分がマルウェアなどに感染していなくても、漏れてしまうケースがあるということです。

したがってIDやパスワードを普段入力していないから安心、とも言い切れません。

そしてIDとパスワードを盗み取った攻撃者は、それを使ってどこか別のウェブサービスなどが乗っ取れないか、さまざまな場所で試します。

あなたが複数のウェブサービスの間でIDとパスワードを使い回していたり、あるいは似た形のパスワードを使ったりしていると、これらのサービスのアカウントを一気に乗っ取られます。

乗っ取られると、あとはオンラインショッピングで勝手にものを買われてしまったり、現金は送れなくてもなんらかの送金システムが利用できる場合は、それを使ってお金を奪い取られたりされてしまうわけです。

もしパスワード流出が判明したら、まずはすぐにパスワードを変更しましょう。

④偽メールや偽サイトに騙されないように用心しよう

④.1 多様化する偽メールに注意しよう

サイバー攻撃を行う際に、攻撃者は偽メール、偽サイトを使うことが多いです。

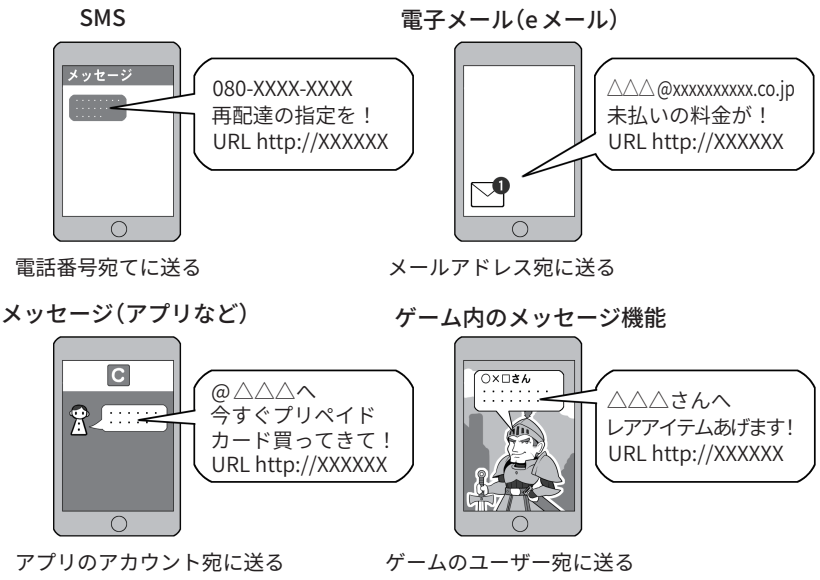
偽メールには、スマホ宛の偽SMSやSNSで使用可能なメッセージ機能なども含みます。メール・SMSからの誘導を受けて、アプリをダウンロードするのは原則としてやめましょう。

近年、フィッシング詐欺の攻撃で最も目を引いたのは、宅配業者の不在通知詐欺です。宅配業者を名乗って「配達に行ったが不在だった。下記のリンクから確認して欲しい」というようなSMSを送り付けて、利用者をリンク先の偽サイトに誘導し、そこでIDとパスワードなどを詐取するというものです。

実は、この業者は「SMSで不在通知を行なわない」のですが、それを知らない人たちはまんまと騙されてしまったわけです。関係機関で日々、「不審なメールに気を付けてください」というアナウンスをしているのですが、SMSとメールは違うものと思われてしまったのかもしれません。

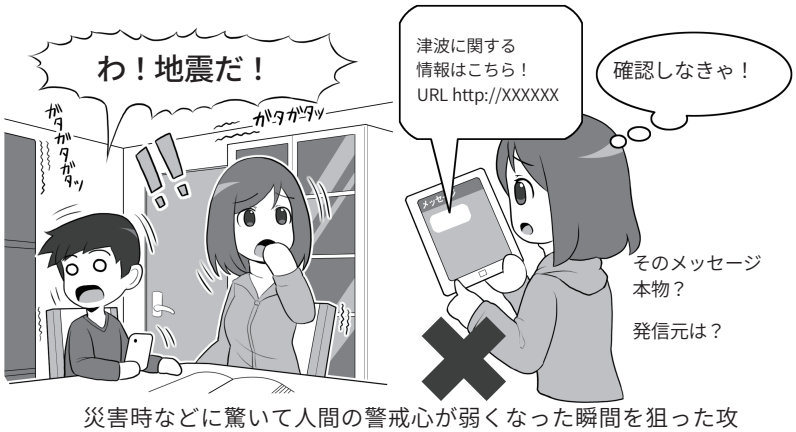
偽メールについても、国税庁を装ったりETCサービスを装ったりと、騙られる送信元にバリエーションが増えてきていますが、偽メールであることには間違いありません。また、すぐにアクセスしないとあなたの口座やアカウントが使えなくなる、一定の違約金が発生する等、不安を煽ることで一層、冷静な対応を妨げるものも多く存在します。そして誘導される偽サイトは短時間で消去される場合が多く、攻撃者が証拠をなるべく残さないようになっています。こういったメッセージを使った詐欺には、SMSやメールだけでなく、SNSのメッセージ機能、あるいはゲーム内のメッセージ機能を使った攻撃も実際に発生していますので、偽メールと同様に注意してください。心当たりのないものは無視し、心当

フィッシング詐欺はいろんな方法がある



「怪しいメール」といわれたら「メール」だけでなく似たような機能全般に気を付けましょう。

驚くと人間は警戒心を忘れる



災害時などに驚いて人間の警戒心が弱くなった瞬間を狙った攻撃もあります。注意しましょう。

フィッシング対策協議会 https://www.antiphishing.jp/
内閣サイバーセキュリティセンター X(旧 Twitter) @nisc_forecast

たりがあるものでも、そのメールやメッセージのURLなどにアクセスするのではなく、メールは通知と割り切って、そこに記載されているリンクは踏まないよう、心がけてください。

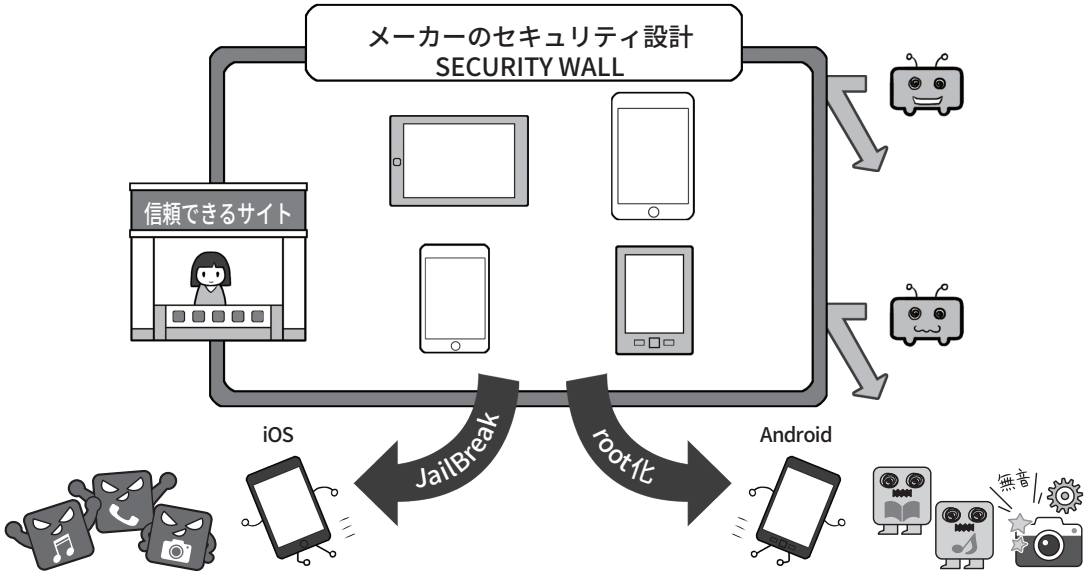
他にも、地震が発生したときに、気象庁を名乗って津波に関する迷惑メールが送られた例もありました。いずれも私たちが「騙されないぞ」と身構えているのとは違う方向や、災害時などで正常な判断が行えない状況を狙っています。

こういった詐欺メールは年々手口が巧妙になっており、送信元アドレスやメッセージ中のリンクを確認しただけで、詐欺と見抜くことは極めて難しくなっています。基本は「見るだけで完結しない情報はすべて疑え」です。情報を確認する場合は、正規のウェブサイトのURLを直接入力して見るか正規のアプリから行いましょう。検索結果上位に表示されるウェブサイト」であっても信頼性は必ずしも高くないこともありますので、注意が必要です。公式のアプリであると信じて偽サイトからダウンロードしたアプリにマルウェアが仕込まれていたという事例もありますので、注意が必要です。

また、日々巧妙になる手口を少しでも知るにはフィッシング対策協議会のウェブサイトや内閣サイバーセキュリティセンターのX(旧Twitter @nisc_forecast)をフォローするとよいでしょう。最新の事例をすぐに確認できます。

④.2 信頼できるサイト以外からアプリをインストールすることは控えよう

信頼できるサイト以外からのダウンロードやスマホの改造は控えましょう



スマホのセキュリティはメーカーが想定する利用方法を守っていることが前提条件です。信頼性が確保されていないアプリをインストールすることは危険が伴う可能性がありますし、「root化」や「JailBreak」といった改造は規約違反である場合もあります。いずれもセキュリティ上、ぜい弱になるので非常に危険で、やってはいけません。

スマホにインストールするアプリも同様に注意しなくてはいけません。

インストールしようとするアプリがどのような動作を行うものかをあらかじめ確認できればよいのですが、個人で、アプリの中身を分析し、不審な動作などがされないことを確認することは簡単なことではありません。そのような確認作業を自分ではなく信頼できる第三者がしてくれれば少し安心できます。

例えばスマホのＯＳ事業者が運営するアプリストアから配信されるアプリに関しては、配信前にアプリストア運営者が審査しているので一定程度のリスクは軽減されます。

また、アプリストア間の競争を促進するための「スマートフォンにおいて利用される特定ソフトウェアに係る競争の促進に関する法律」が令和7年中に全面施行されますので、今後、様々なアプリストアが登場することが予想されます。ただし、同法の下でも、一定の要件を満たす場合は、スマホのＯＳ事業者が、セキュリティ、プライバシー、青少年保護等のために必要な措置を引き続き採ることが

できます。

ユーザーには、アプリを利用する際の安全や安心を確保するためには一定のコストがかかることと、アプリの審査を行っている信頼できるアプリストアを使うという観点が不可欠です。スマホのOS事業者以外の事業者が運営するアプリストアについても、このような観点から信頼できるアプリストアを利用することも重要です。

このほか、アプリストア以外からアプリを入手する方法としては、おもにブラウザを介してアプリを直接ダウンロードする方法(以下、「サイドローディング」)があります。

サイドローディングについては、信頼できるサイトからのダウンロードと、セキュリティ設定の適切な管理が必要となります。一方で、信頼できるサイトのような偽サイトに誘導するフィッシングメールなどによる攻撃が行われる可能性がありますので、十分注意しましょう。

スマホの改造は規約違反になる場合もあり、セキュリティ上、ぜい弱になるので非常に危険です。スマホを標準にはない設定に変更できる改造を「root化」、「JailBreak」と呼びますが、これらの行為はセキュリティレベルを下げることになります。

スマホには、個人に関する重要な情報がたくさん保存されているため、リスクの高いアプリをインストールし、重要な情報が漏えいしてしまうと、取り返しがつきません。例えばスマホの場合、攻撃者が用意したサイトに偽メールや偽SMSなどであなたを誘導して、不適切なアプリをインストールさせ、端末を乗っ取ったり、端末内の情報を盗んだりする可能性があります。

Android機器の場合、使用しているアプリで別のアプリをインストールする設定が最初からオフになっております。不明なアプリをインストールしないためにも、スマホのＯＳ事業者以外の信頼できるアプリストアを利用したいとき以外には、この設定はオフのままにしておくようにしましょう。

また、Android機器でもiOSでも、アプリのインストール時や初回起動時に、同意を求められる「権限」には充分注意してください。権限とはインストールするアプリに対して、スマホのどの機能の利用を許可するか、という確認です。単なるカメラアプリなのに住所録にアクセスするものや、撮影する必要がないのにカメラにアクセスするもの、著しく多くの項目にアクセスしようとするものなどは要注意の例です。項目別に許可を却下するか、そうできない場合、そのアプリは導入しないようにしましょう。また、最初は無害に見えて、導入後のアップデートで権限の増加の許可を求めるものも、その変更項目に注意してください。

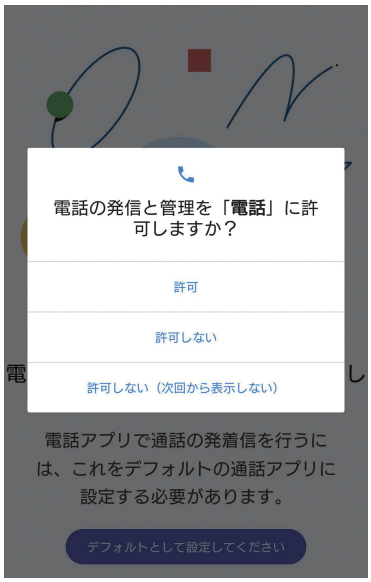
有用なアプリの開発者から、攻撃者が当該アプリを買い上げて、後からアプリをマルウェア化してしまう攻撃もあります。その他、アプリ間での機能連携やウェブサービス間で連携して、間接的に権限を奪取するものもあるので「連携」という言葉にも充分注意してください。

「不明のアプリ」という言葉に注意

• Android

項目や文言は、使用するAndroidのバージョンやスマホメーカーによって異なりますが、アプリのインストール時に「不明なアプリ」と表示されたり、最初からオフに設定されている「不明なアプリ」に関する項目を変更させようとするものは、セキュリティ上危険な可能性が高いものです。スマホのＯＳ事業者以外の信頼できるアプリストアを利用したいとき以外にはオフの設定のままにしておくようにしましょう。アプリは、基本的にアプリストアからのみインストールするようにして、その他の場所からは避けましょう。

導入時や起動時の権限付与に注意



• Android、iOS（画面はAndroid）

アプリのインストール時や、起動時にさりげなく表示されるため、多くの人が無意識に「承認」や「同意」してしまっていますが、これは、「アプリがスマホのこれらの情報に自由にアクセスできる許可」を求めている画面です。

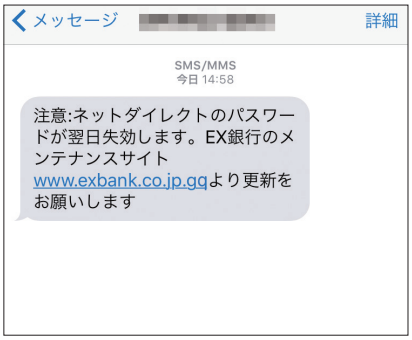
個別に却下することができない場合もあるので、その際は導入しないようにしましょう。そして、そもそも不必要な権限を求めるアプリは怪しいと警戒しましょう。

⑤メールの添付ファイルや本文中のリンクに注意しよう

標的型メールとスパムメールの例

標的型メールの例

スパムメールの例 SMSを使った例



添付ファイルやリンクは、標的型攻撃でもよく使われますし、今でもときどき復活しては、猛威を振るう「Emotet」も、マルウェアを添付したメールを受信者が開き、添付ファイルを実行することで感染が成立します。

心当たりのない送信元からのメールに添付されているファイルやリンクは、信用できないものとして、原則、開かないようにするとともに、機器の設定などを堅牢に保ち、感染の隙を作らないようにしましょう。例えば、一般社団法人全国銀行協会や一般社団法人クレジットカード協会からは、フィッシング詐欺に遭わないようにするための注意が示されており、SMSやメールを受信した場合には、必ず公式のページから対応することを、推奨しています。

スパムメールでの攻撃は、引っかかる率が少なくとも、その攻撃の母数を大きく取ることで攻撃者にとっての利益回収のパフォーマンスを上げています。

例えば、「スパムメールの例」の画面は、実際にSMSに送り付けられた、銀行を名乗るフィッシングメールを模したものです。

送信元とされる金融機関やカード会社の口座を持っていない人であれば、フィッシング(＝詐欺)メールだと気付くことができるかもしれませんが、現在もこういった攻撃に引っかかる人が相当数いるのが実態です。その先が詐欺サイトではなく、ゼロデイ攻撃のマルウェアが埋め込まれたウェブサイトならば、開いただけで感染してしまうでしょう。

また、もっとやっかいなのが、攻撃者ではなく、善意でマルウェアを拡散させてしまう人々です。友人から「このアプリ面白いよ！」と薦められたら、多くの人はあまり不審に思わないでしょう。

しかし、友人は知らなくても、実はこのアプリにマルウェアが仕込まれていたり、あるいは感染時点は無害でも、後に権限を拡大して個人情報を抜き取るかもしれません。

これが、他人の発信ならば警戒できますが、親しい友達や家族だった場合、警戒できるでしょうか？

対抗策としては、こういったお薦め系のものは1つの線引きを持って接するようにしましょう。メールの文面など、目の前に見ている情報で完結しないものは一律に警戒するのです。動画が面白いとかお金が儲かる方法があるとかだけでなく、リンクでジャンプするとか、添付ファイルを開かせるものは一律に避ける。

それは、現実世界で「ちょっと向こうまで付き合ってよ」とか「ちょっとこの車に乗ってよ」といって連れて行かれるのに等しいと思いましょう。

さらに、「リンクでジャンプしないけど検索エンジンで調べて見る分にはいいよね」、と思っても、攻撃者はそうやって検索エンジンからやってくる人向けに、二段構えでマルウェアを仕込んだウェブサイトを用意していることもある、と覚えておいてください。

⑥スマホやパソコンの画面ロックを利用しよう

⑥.1 スマホやパソコンには必ず画面ロックをかけよう

スマホやパソコン(PC)の情報を守る第一歩は、待ち受け画面にロックをかけることです。

ロックには「PIN コード」によるロック、パターンロック、指紋や顔など生体情報を用いた認証によるロックなどがあります。ロック機能は「誰かにスマホを持ち去られるなど、手元からスマホが離れたとき」に情報を確実に守るためのしくみの1つです。

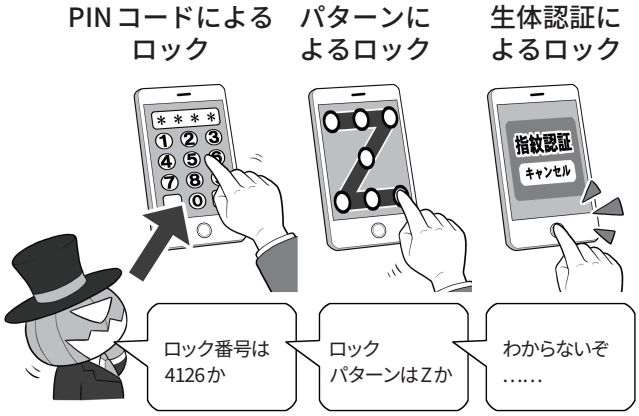
とくに生体認証は周りから覗かれPIN コードを盗まれる危険性の排除をしつつ、入力の面倒くささを省くので便利な機能です。

指紋認証や顔認証が代表的ですが、その他にも、スマートウォッチなど特定のウェアラブル機器を着けたり、GPS に連動して自宅など特定の場所にいたりすることで自動的にロックを解除できるものもあります。

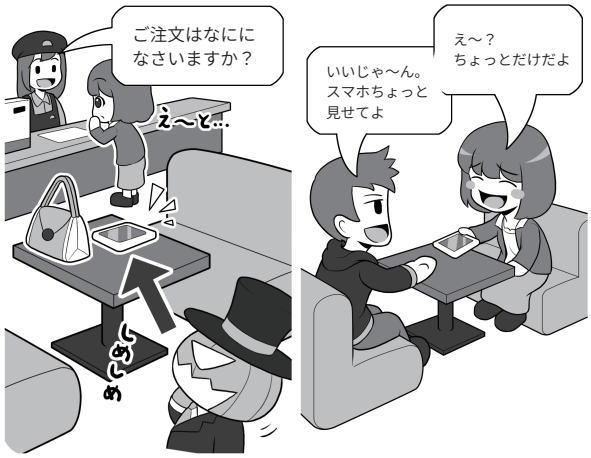
ただし、気を付けておきたいのは、セキュリティ向上のためのロック機能を設定しても、そのパソコンやスマホをロック解除したまま置いてその場所を離れたり、ロックを解除して他人に見せたり貸したりすれば、一瞬で情報を盗み、乗っ取ることが可能です。画面ロックは、情報を保護するための強力なツールですが、ロック解除するための認証方法がぜい弱だと意味がなくなります。ロックがかかっているから安心とそれだけに頼り切りにならず、ロックを解除するための機能や、スマホやパソコンの管理にも留意しましょう。

スマホやパソコンは自分のすべての情報が詰まった持ち歩く金庫だと思って、必ず肌身離さず自分のそばに置き、使わないときはこまめにロックをかけた状態にすることが重要です。

スマホやパソコンにはロックをかけよう



席において離れたり、人に貸したりしないようにしよう



スマホを席に置いたままでは、本体も情報も盗まれるおそれがあります（とくにロックを設定しなかったり、ロック解除したままの状態で放置）。

スマホを貸すと、プライバシーを覗かれたり、一瞬でスパイアプリのようなものをインストールされたりすることがあります。むやみに渡してはいけません。

⑥.2 よくある情報の漏れ方と対策

SNS用のアプリなどでは、本体のPINコードなどとは別に、アプリ専用のPINコードが設定できるものもあります。盗難などの際、SNSの内容を見られたくなければ、このアプリPINコードも設定しましょう。情報の守りが二重になります。一部の機種では生体認証をアプリのロック解除に利用できるものもあるので、セキュリティを向上させても快適な利用の妨げにはなりません。

一方、攻撃する側から見ると、スマホのロックをなんらかの方法でパスできたとしても、また、別の関門が待ち構えることになります。手間をかけさせ侵入を諦めさせるというセオリーに沿っているわけです。

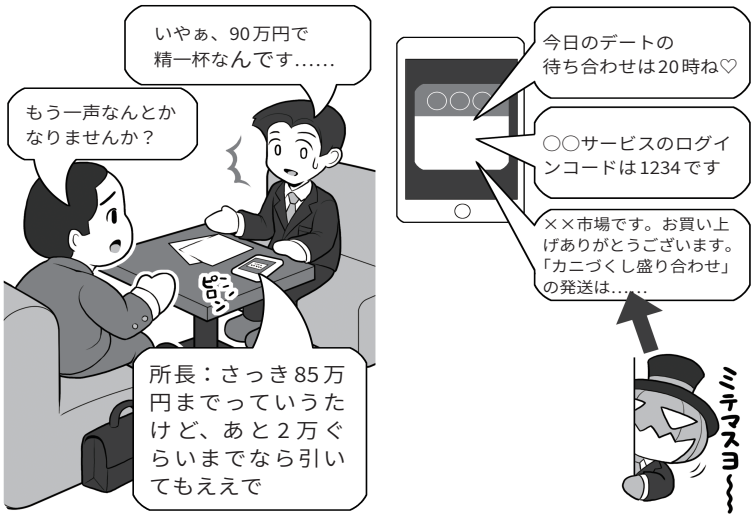
なお、アプリのPINコードを使う場合は、スマホロック解除のPINコードと異なるものを設定しましょう。PINコードの使い回しはセキュリティがないのと一緒になってしまいます。PINコードもそれぞれ異なってこそ意味があるのです。

スマホをロックしていても情報漏れが発生することもあります。

例えば自分だけで使っているときは便利なメールの通知機能。ロック画面にメールの内容を表示していると、誰かと会話中や商談中に、うっかり内部情報を見られてしまったり、あるいは差出人が分かるだけで、状況によっては知られると問題のある情報を提供してしまうことになりかねません。

また、同様にロック画面にメールの内容を表示していると、せっかくセキュリティ向上のために設定した多要素認証のパスワードメールも見られてしまうことがあり得ます。そうするとスマホやメールアドレスの正当な持ち主であることを確認する役割を果たせず、画面をのぞき見ただけの第三者によって認証が突破できてしまいます。

待ち受け画面に表示する通知はよく検討する



ロック画面だけでなく、普段使用している画面に通知ウインドウとして表示される場合でも、同じく情報を見られてしまう原因になります。スマホを使って説明しているときに、不適切なメールの内容が表示されることも……。情報漏えいには気を付けましょう。

アプリごとにPINコードをかけられる場合はかける

本体のロックを解除されても、SNSのアプリに別のPINコードがあれば、流出の危険性は低くなります。それでも、自分が席を離れるときにスマホを残してはいけません。なお、勝手に他人のスマホのロック解除をすることは、れっきとしたサイバー攻撃です。

⑦大切な情報は失う前にバックアップ(複製)しよう

⑦.1 何をするにもバックアップを取ろう

各種のサイバー攻撃や、パソコン・スマホの故障などからいち早く復旧して事業を継続するには、システムやデータのバックアップが不可欠です。またランサムウェアの流行により、バックアップの重要性が格段に上がっています。バックアップを取ることで、ランサムウェア攻撃や、様々なシステムへの破壊や影響があった場合に、被害を最小限にとどめる有効な手段となります。

またバックアップは、いざというときに元に戻せることが必要です。定期的にバックアップファイルが使える状態にあることの確認はもちろん、バックアップから元のシステムに戻すための手順の整備や訓練なども行うことも重要です。

バックアップの方法はおもにパソコンやスマホの OS の種類により異なっています。

パソコンの場合、macOS 搭載の機器のように、外付けの補助記憶装置(ハードディスクや SSD。以降記憶装置)を接続するだけでバックアップが行え、復旧もシステムとデータすべてをほぼ全自動で行えるものもあります。

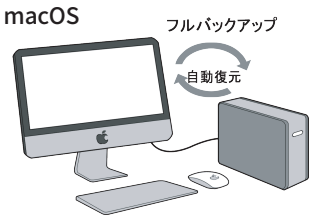
Windows 搭載機器では、基本的にはデータをバックアップする考え方で、システムの復旧とデータの復元は、別に行うようになっています。

スマホの場合も機種ベンダーによる差もありますがほぼ同様です。

iOS 搭載機器はパソコン上に専用の同期ソフトを導入して全体をバックアップします。機器を紛失した場合にも、新しい機器を接続すると自動で復元が行えます。

Android に関しては標準ではパソコンに全体をバックアップする機能はないので、Windows に似た、データのみをバックアップする形で行います。

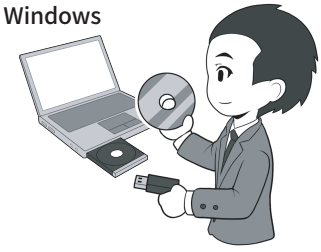
macOS機器、Windows機器のバックアップと復元

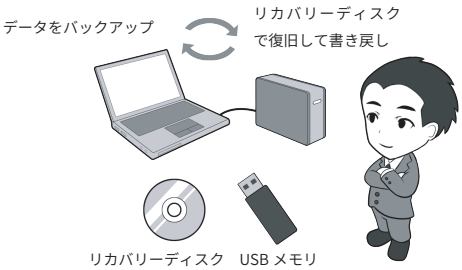


mac OS 機器はまるごとバックアップ、まるごと復元の性格が強く、Windows は基本的には OS を復元後、別途データを書き戻すイメージと考えるとよいでしょう。

実際は他にも専用のソフトウェアを導入したり、細かい設定を変えることで、バックアップの方法を変える手段はあります。

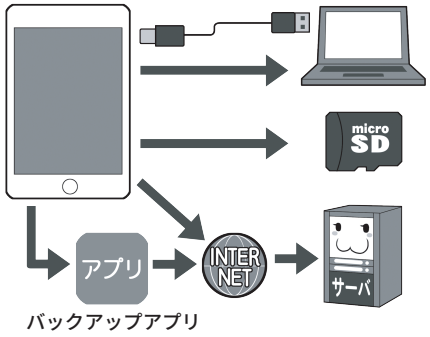
ですから基本的なそれぞれの OS の立ち位置や性格と考えて下さい。善し悪しや優劣はありません。





スマホもバックアップは定期的に取ろう

バックアップの方法はいろいろ

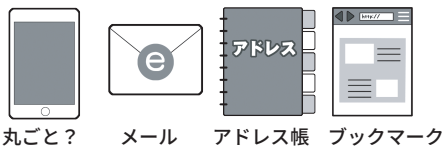


パソコンにつないで丸ごとバックアップ

内蔵できる microSD メモリカードにバックアップ

直接あるいはアプリ経由でクラウドサーバにバックアップ

なにがバックアップできるか確かめる



なにがバックアップできるのか確かめて、機種やバックアップ方法を選択します。また、取得したバックアップを用いてシステムがちゃんと復元できるか確認してください。

⑦.2 ランサムウェアや天災にも対応できるバックアップ体制

ランサムウェアなどの、データを破壊することが多いマルウェアの対策にはバックアップが有効ですが、では実際にどう運用するのでしょう。

ランサムウェアはパソコンなどが感染すると、そのパソコンに繋がっている記憶装置すべてを暗号化してしまいます。仮にバックアップしていても、常時接続したままにしていると、その外付け記憶装置まで巻き添えで暗号化されることもあります。

そのため、バックアップ自体はマメにしておくべきですが、常時接続はしておかないという、かなり難しい運用が求められます。

また、最近は大雨などの異常気象や地震等の災害により、事務所にあったパソコンと外付け記憶装置が両方とも使用不能となり、復旧が困難になることもあります。これに対応する手段としては、バックアップの「3-2-1ルール」というものがあります。バックアップは本体を含め3個以上、2種類以上の媒体、そして1個は遠隔地に置くというものです。特に重要なファイルのバックアップは、使いやすい状態におくなどの選択も重要です。

遠隔地とは、現実的には「クラウドサーバ」などの利用を意味します。クラウドサーバは最近では手頃になりましたが、それでも本体の全データをバックアップできる容量は高価です。したがって、事業継続に必要な重要なデータを選別してバックアップすることになるでしょう。なお、会社に同時に災害に遭わなそうな支社などがある場合は、そこにバックアップをおいてもよいでしょう。

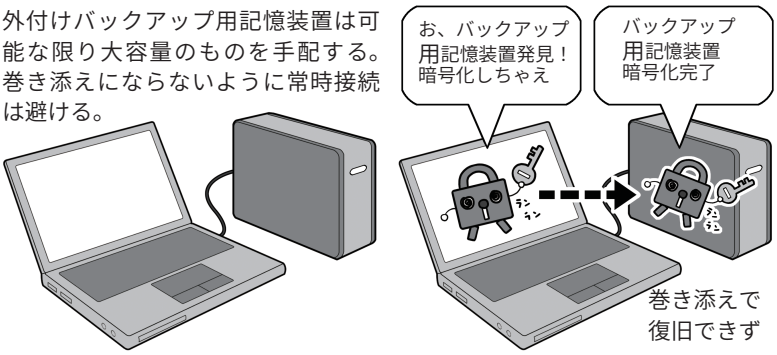
なお、ランサムウェアに対しては、変更不能な形でのバックアップが有効です。例えばDVDやBDなどのメディアで追記不能な形で記録したり、イミュータブル(変更不能)という機能に対応したクラウドサービスなども有効なので、利用にあたっては調べてみましょう。

ランサムウェア感染はビジネスにも影響

ランサムウェアはパソコン内のファイルを勝手に暗号化するため、感染すれば仕事上の極めて重要なファイルも人質に取られてしまいます。バックアップはまめにしておきましょう。

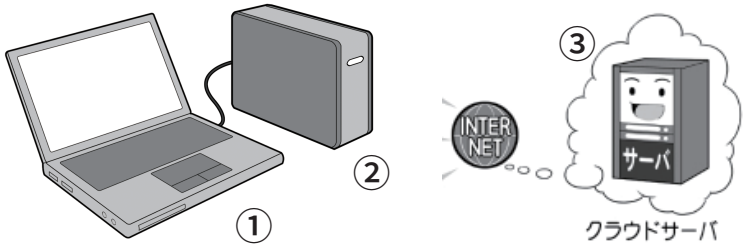
バックアップの体制を整える

外付けバックアップ用記憶装置は可能な限り大容量のものを手配する。巻き添えにならないように常時接続は避ける。



環境を整えたらバックアップを開始します。なにかソフトの導入や、環境を変更したらバックアップします。システムのアップデート後もバックアップします。ただし、バックアップ用記憶装置を常に接続しておくとランサムウェア感染で巻き添えになって、復旧に使うためのデータも失われてしまいます。

バックアップは3個以上、2種媒体以上、1個は遠い場所



本体＋バックアップ用記憶装置＋クラウドサーバで条件を満たします。クラウドサーバは多要素認証などで、攻撃者に乗っ取られないようにしましょう。

⑧外出先では紛失・盗難・覗き見に注意しよう

勤務先や外出先でスマホやパソコンを使う際に、誰かにスマホやパソコンを覗き見られている、そう感じたことはありませんか？

友人知人と冗談の範囲で「何やってるの～？」と１回２回茶化すくらいならまだしもあまりに覗き見の頻度が高かったり、あるいは見知らぬ人に何も言わずにずっと横や後ろから覗き見られてたりしているようならば要注意です。

見られている内容が機密情報であったり、秘匿したい個人情報であったりする場合には、あなたの情報が漏れる心配があります。

「見られても大したことない情報しか自分のスマホやパソコンには保存してないよ」と心配しない人も多いかもしれませんが、覗き見している人はあなたの情報もさることながら、あなたがやりとりしている相手がターゲットかもしれません。

「ロックをかけてあるから大丈夫」と思っても、ロックを解除する方法がすでに相手の手に渡っている懸念もあります。例えば、相手に直接接触せず情報を入手する方法として、電車で座席に座っている人のスマホ操作を見て PIN コードやパターンロック形状を盗む「ショルダーハッキング」、カフェなどのテーブルに放置されているスマホの画面に残る指の脂跡からパターンロックを見破る方法などがあります。飲食店などで席の確保にスマホなどを置き去りにする行為を時折見かけますが、紛失・盗難・覗き見、いずれの被害に遭ってもおかしくない非常に危険な行為です。このような行為は、すぐにやめましょう。

外出時は自分のスマホやパソコンが他人から見られる可能性は高い

外出時は、使用しているスマホやパソコンを他人から覗き見されないよう注意が必要です。また、うっかり紛失して盗難されれば、大事な情報が盗まれるリスクは大きく高まるので、よく注意しましょう。

スマホ使用時によく狙われるソーシャルエンジニアリング

ショルダーハッキング

公共の場でロック解除をするときは、背後などから見られていないか気を付けましょう。

画面についた脂の跡を見る

スマホを席に残しておいたり、席取りのためにテーブルに置いて離れたりしてはいけません。

⑨困ったときは１人で悩まず、まず相談しよう

自ら、あるいは第三者からの連絡でサイバー攻撃に気付いた場合は、直ちに処置を取り、その後必要な各種窓口に相談しましょう。

あらかじめ対応者を決めてあるならば、その人を中心に対応するか、決めていない場合には、IT に詳しい社員などがいたらその人を中心に対処しましょう。

一番最初にするべきは電源を落とさないままインターネットから切断することです。これはマルウェアなどの拡散を防ぎつつ、後々警察に連絡をする場合の証拠保全になります。

次に、連絡するには状況を把握しなければならないので、なるべく分かる範囲で 5W1H のように分けて事象を記録しましょう。いつから始まったのか、どのようなことがあったのか、誰が作業していたのかなどです。

当然のことながらその間、攻撃が行われたと思われるパソコンなどの機器は使わず、その他の機器や紙のメモで記録します。

サイバー攻撃を受けたときに相談するサービスを契約している場合はそちらに相談し、無い場合は、IPA の相談窓口に相談しましょう。

ランサムウェアによりデータを暗号化されて脅迫されたり、情報を消されたり、何か機器を故障させられたり、あるいは情報を盗難されたりなど、明確に被害がある、もしくは被害に遭ったおそれがある場合は、各都道府県警のサイバー犯罪相談の窓口などに相談しましょう。

そして自社や団体で扱っている個人情報を盗まれたり消されたりしてしまった場合、個人情報保護委員会などへの速やかな報告、原因究明や再発防止策の策定などが求められます。ウェブサイトからフォーム入力による方法で報告できます。

*** 詳しい報告先や対応方法は個人情報保護委員会ウェブサイトをご覧下さい。**

各種連絡窓口のウェブサイトなど

IPA「情報セキュリティ安心相談窓口（個人向け）」

https://www.ipa.go.jp/security/anshin/about.html
電話番号：03-5978-7509（受付時間：10時～12時　13時30分～17時
※土日祝祭日、年末年始除く）
メールアドレス：anshin@ipa.go.jp

IPA「サイバーセキュリティ相談窓口（企業組織向け）」

https://www.ipa.go.jp/security/support/soudan.html
メールアドレス：cs-support@ipa.go.jp

都道府県警察「サイバー犯罪等に関する相談窓口」

https://www.npa.go.jp/bureau/cyber/soudan.html

消費者庁「「消費者ホットライン」188」

https://www.caa.go.jp/policies/policy/local_cooperation/local_consumer_administration/damage/
電話番号：188

個人情報保護委員会「漏えい等の対応とお役立ち資料」

https://www.ppc.go.jp/personalinfo/legal/leakAction/

2 攻撃者に乗っ取られると起こることを知ろう

2.1 被害に遭わないために。そして加害者的立場にならないために

攻撃者があなたのパソコンなどにサイバー攻撃をしかけるのは、お金や情報を盗むだけでなく、あなたのパソコンなどをサイバー攻撃の道具にする目的である場合もあります。

手順としては、あなたのパソコンなどをマルウェアに感染させるか、流出したIDとパスワードを使いパソコンに侵入し、自由にコントロールできるようにします。

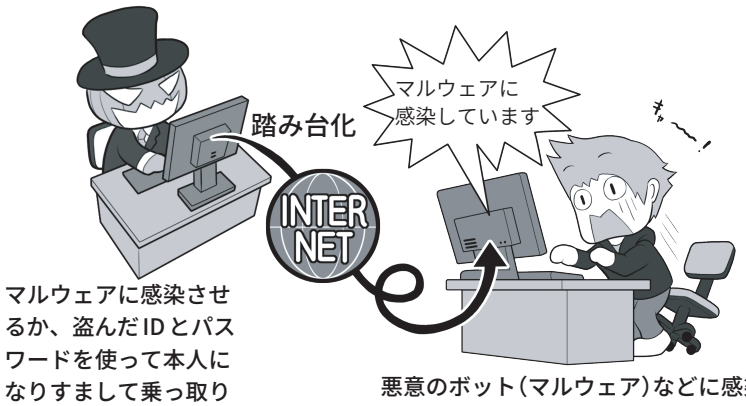
次に別のパソコンやサーバなどに侵入するとき、「踏み台」にしてあなたのパソコンがやっているように見せかけたり、悪意のボットによるボットネットに接続させ、第三者へのDDoS攻撃を行わせたりします。

こうすることで、万が一サイバー攻撃がばれたとしても、最初にあなたが調べられ、その間に攻撃者は証拠隠滅などをして姿をくらますことができるわけです。

こういった場合でも、入念に調査すれば乗っ取られていた事実が分かるでしょうが、もし攻撃が重要な社会インフラに対して行われ、実際に被害者が出てしまったら、あなたは思い悩んでしまうでしょう。

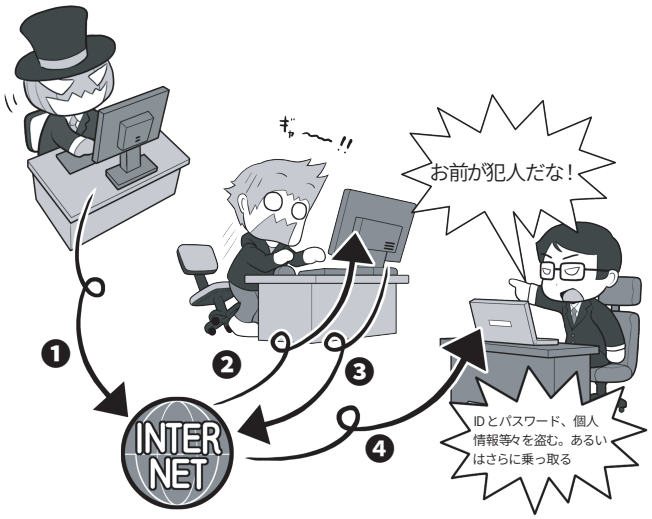
そうならないためにも、公衆衛生的なマナー意識を持って、パソコンなどのセキュリティはしっかり固めましょう。もしセキュリティソフトが、マルウェアに感染していることを検出したら速やかにネットから切断し、実害の出ている攻撃に関して、警察などから協力の要請があった場合は証拠保全を行いましょう。

攻撃者によるパソコンなどの乗っ取り



攻撃者は、目的のパソコンなどをマルウェアに感染させ乗っ取る他、流出したあなたのIDやパスワードを利用しあなたになりすまし、各種サービスやリモートでパソコンにログインを試みて、これを乗っ取ります。マルウェアであればセキュリティソフトで検出されるかもしれませんが、なんらかの正規の方法でログインされ、「本人」としてリモートコントロール用のソフトをインストールされると、その乗っ取りに気付くのは困難になります。

乗っ取ったパソコンを踏み台にしてサイバー攻撃を行う



攻撃者は乗っ取ったパソコンなどに対して❶インターネットを通じて、❷乗っ取ったパソコンに指示を出し、❸あなたのパソコンがやっているように見せかけて（踏み台化）、❹他の人のパソコンに攻撃をしかけます。攻撃者はこうすることで自分の存在を隠して、安全にサイバー攻撃を行えるわけです。

また、乗っ取りだけでなく、あなたのパソコンのメールアドレスを使って、他者にフィッシング詐欺のためのBEC（ビジネスメール詐欺）のメールなどを送信する場合などもあります。

2.2 盗まれた情報は犯罪に使われる

攻撃者は、あなたのパソコンなどを乗っ取って、個人情報、クレジットカードや銀行情報、ウェブサービスや SNS の ID とパスワードなどを盗むと、それを犯罪に使います。

例えば銀行のインターネットバンキングを使った不正送金で、口座からお金を盗み取るかもしれません。

銀行のインターネットバンキングは多要素認証でガードがされているから大丈夫と思っても抜け道はありますし、あなたの情報を売ってお金を得る手段もあります。

流出したクレジットカードを使いオンラインで勝手に買い物をして、それを受け取り現金化する、といった事件も起きています。

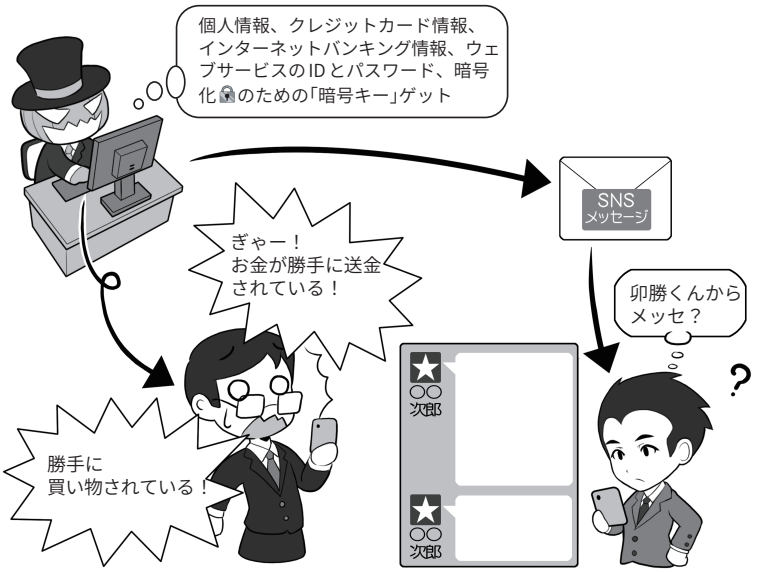
SNS のメッセージであなたになりすまし、友だちに対して「プリペイドカードを買って、アクティベーションコードを送ってくれ」と依頼して、電子マネーを騙し取る場合もあります。

自分が使っているパソコンなどのセキュリティをしっかり固めていても、情報を登録しているウェブサービスなどから、間接的に流出・盗難されることもあります。

この場合でも同じように、攻撃者は盗んだ情報からなんらかの手段を用いて、お金を手に入れようとします。あなたに非がなくても流出は起こるのです。自分の環境のセキュリティを固めてもそのときは防ぎようがないので、不正利用などの兆候に気を付けてください。

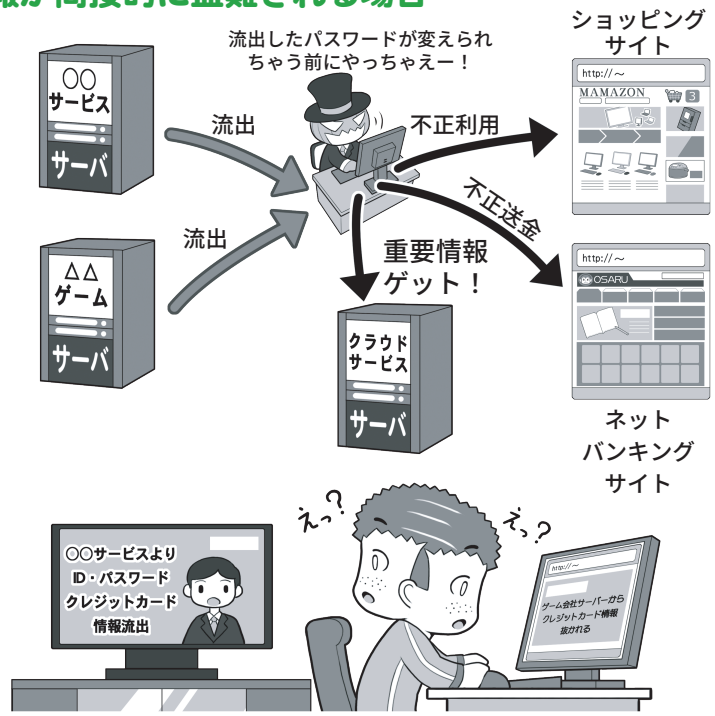
パスワード流出が判明したらパスワード設定のセオリーにしたがってすぐに変更し、クレジットカード情報が流出したらカード会社に連絡してカードの番号を変更しましょう。

情報が直接盗難される場合



クレジットカード情報の流出などが起こった場合は、その被害は多岐に及びます。とりあえずカードが不正利用されていないかチェックしましょう。パスワードなどの流出が判明したら、該当するサービスのパスワードの変更を行いましょう。

情報が間接的に盗難される場合



特定のサービスから ID やパスワードが流出しただけならば、ID とパスワードの使い回しをしていない限り、他のサービスへの被害拡大はありません。しかし、使い回しをしている場合や、クレジットカード情報が漏れた場合、その被害は多岐にわたる可能性があります。楽観的に考えずに迅速に対処しましょう。

2.3 乗っ取られた機器はサイバー攻撃に使われる

サイバー攻撃で攻撃者に乗っ取られたパソコンなどの機器は、「ゾンビ化」といい、攻撃者に操られる状態となって、さまざまなサイバー攻撃に使われることがあります。

サイバー攻撃の「踏み台（身がわり）」に使われる他、「悪意のボット」に感染した機器は、持ち主の知らないところでボットネットというゾンビ化したIT機器の集合体に加えられ、攻撃者の命令で特定のサーバに一斉にアクセス要求をするDDoS攻撃などに使われます。

このボットネットによる攻撃は、攻撃者が自分の技術や主張を誇示する行動などにも使われますが、ボットネットを利用して攻撃を行いたい人物に、時間あたりいくらで貸し出されたりもします。攻撃者は乗っ取った人の財産（パソコンなど）を勝手に貸し出し、違法にお金を稼いでいるわけです。

一方、「踏み台」的な攻撃はパソコンなどの乗っ取りによるものだけではありません。

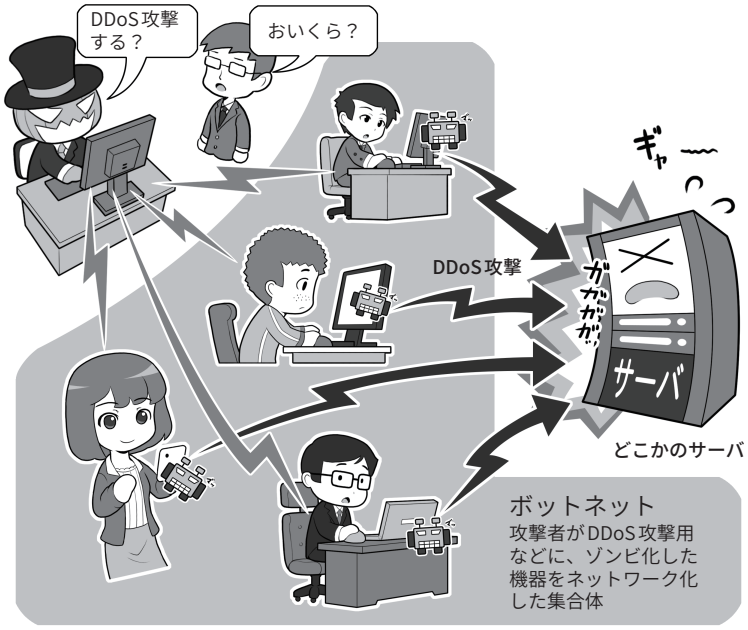
「ウォードライビング」といって、車で移動しながら、会社や事務所に設置されている、暗号化されていない、もしくは暗号化や暗号キーの設定の甘い無線LANアクセスポイントを探し、見つけるとこれに侵入して利用する手法があります。

これはアクセスポイントを「踏み台」にし、そこからインターネット上のさまざまなサーバやインフラ企業に攻撃をしかけるためです。

攻撃をしかけてきているのは「踏み台」がある場所と見せかけて身代わりにし、攻撃がばれたときの追跡を逃れるためです。

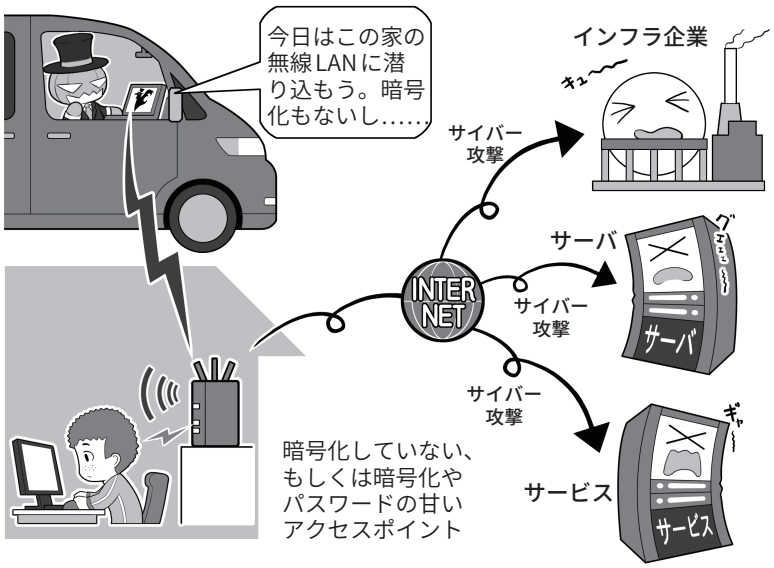
この場合、会社や事務所からサイバー攻撃が行われ、インフラ企業などで事故が発生したら社会的影響は大きいので、セキュリティを固めて侵入されないようにしましょう。

乗っ取られたマシンはボットネットとして貸し出される



攻撃者によって悪意のボットに感染させられ、コントロールされたパソコン（ゾンビPC）などの集合体がボットネットです。攻撃者の命令で、一斉に特定のサーバなどにDDoS攻撃をしかけ、ダウンさせたり反応不能に陥れたりします。ダークウェブなどで時間あたりいくらという形で貸し出されることもあります。

無線LANに侵入され罪を押し付けられることも



車で街を徘徊して、侵入可能な無線LANアクセスポイントを探すことを「ウォードライビング」といいます。こういった侵入を許し「踏み台」にされないためには、無線LANアクセスポイントのセキュリティ設定をきちんと見直しましょう。それが、自分の身の回りでできるサイバー攻撃阻止の第一歩です。

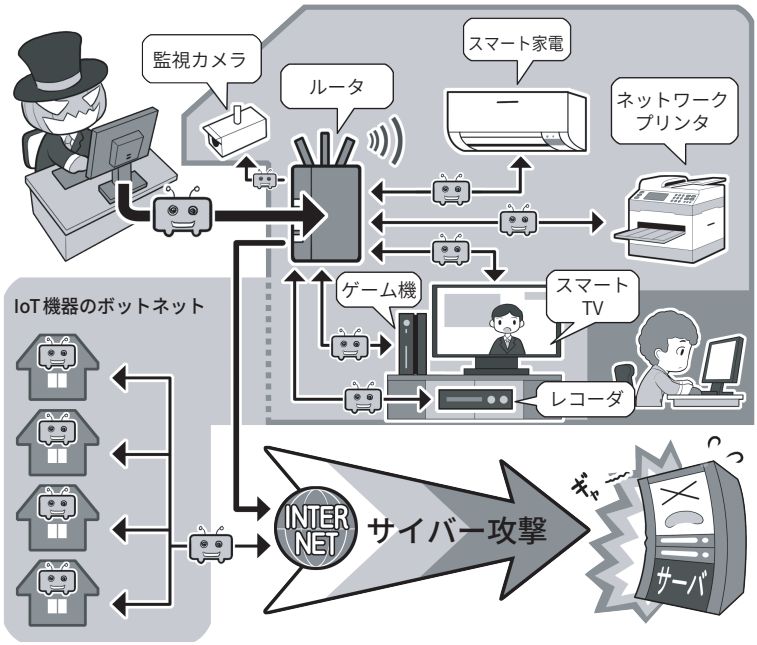
2.4 IoT機器も乗っ取られる。知らずにマルウェアの拡散も…

攻撃者によって乗っ取られるのはパソコンやスマホだけではありません。ネットにつながるIT機器はいずれも、乗っ取られて攻撃者の身代わりにされる「踏み台」化、DDoS攻撃のボットネットへの接続、マルウェアの拡散など、さまざまなサイバー攻撃に利用される可能性があります。とくにIoT機器は、監視カメラやネット対応電子機器などのように、普段私たちがあまりセキュリティについて気にかけないものであり、パソコンほどサイバー攻撃への対応能力も高くありません。そして1つの機種で生産台数が多い＝手間をかけずに多数を一気に攻撃できる「攻撃しやすい条件」が揃っているのです。最低でも、IoT機器の出荷時の「管理者用パスワード」などはパスワードセオリーにしたがって変更し、システムは最新に保ち、ネットにつなぐ必要がないものはむやみに接続しないようにしましょう。

また、サイバー攻撃に協力してしまうのはなにもパソコンやIoT機器だけとは限りません。人間は最大のセキュリティホールともいわれ、マルウェアの拡散源となることもあります。SNSなどで「この記事が面白いよ」、「このアプリ試してみて」といった投稿を考えなしに拡散していると、その先はフィッシングサイトだったり、マルウェアのようなアプリだったりということもあり得ます。

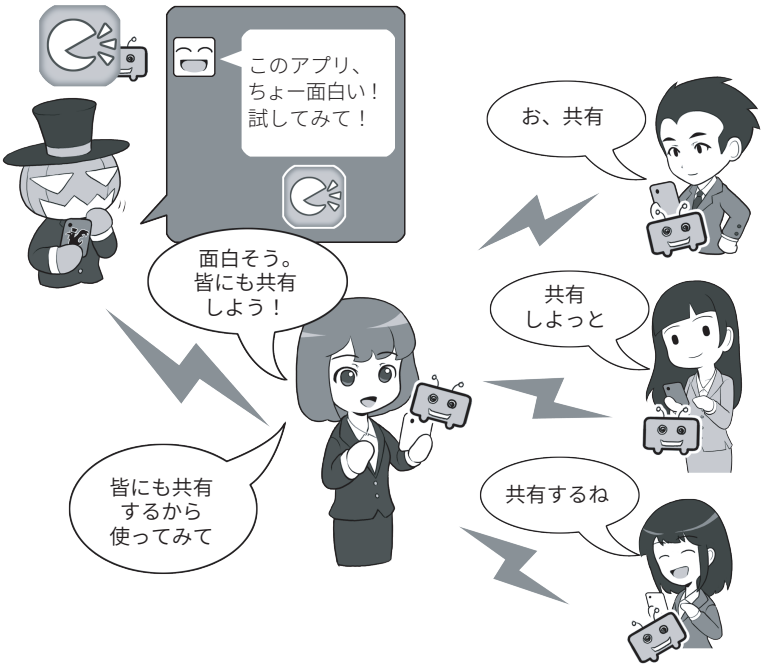
ネットでなにか行動する前には、必ず「それは本当に必要なのか」、「そうすることでなにか問題が発生する可能性はないのか」をいつも注意しましょう。

IoT機器も乗っ取られ攻撃に使われる



IoT機器は攻撃者から見ると、乗っ取りやすい要素を多く持っています。攻撃者はそれらを乗っ取ってさまざまなサイバー攻撃に使います。IoT機器は最低でも「出荷時の管理者パスワードの変更」、「システムの状態を最新にする」、「必要のない機器はネットにつながない」などの応をしましょう。

知らずにマルウェアの拡散に協力しているかも……



SNSで見た「面白い投稿」や「拡散希望の投稿」を深く考えないで拡散すると、その投稿にあるリンクの先にはフィッシングサイト用意されていたり、ゼロデイ攻撃のマルウェアが仕込まれていたり、アプリであればマルウェアが入ったものだったり、そのときは違っても、のちのちそう変化するアプリかもしれません。拡散する前によく考えて「共有する必要がないものは共有をしない」ようにしましょう。そうしないと、あなたが被害者ではなく、サイバー攻撃やマルウェアの拡散者になってしまうかもしれないからです。

3 偽・誤情報、サイバープロパガンダに騙されないようにしよう

悪意を持った者が、なんらかの意図を持って、ネット上で偽のニュースを発信する「フェイクニュース」、SNSなどで拡散され始めるとニュースサイトなどでも真贋不明のまま取り上げられ、それを真実だと思う人が多数現れてしまうということが起きています。フェイクニュースに代表されるように、ネット上ではあたかも正しい情報のように偽情報や誤情報が流通しています。SNSにも偽の情報も多く記載されていたり、名前等を偽っての投稿も多く見られます。

フェイクニュースには、意図を持って発信している人の他に、人々が注目するニュースをねつ造することで自分のウェブサイトの閲覧数を増やし、掲載した広告の収入でお金を稼ぐ商売としている人もいて、悪意のビジネスモデルになっています。

検索エンジンやSNSを運営する企業などは、こういった情報がニュースのランキングに登場しないように工夫をしたり、善意の団体と協力して偽の情報の場合は否定するなど処置を行ったりしていますが、いまだ根本的な解決には至っていません。

こういったフェイクニュースを、外国の国家機関や政治的意図を持った者などが「武器」として使い、他国の選挙における投票行動などに意図的に影響を及ぼす「サイバープロパガンダ」も多く発生しています。

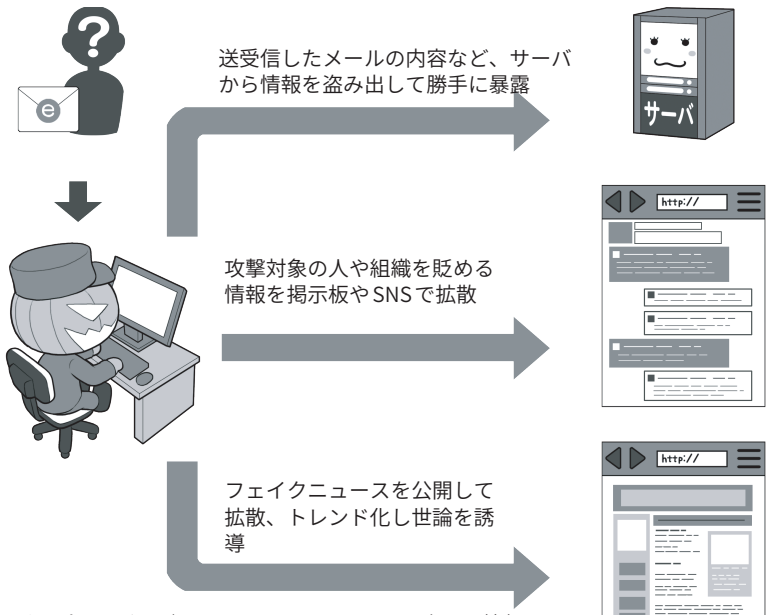
古くから国家が自国や他国に対して影響を及ぼすために行われてきたプロパガンダは、ネットを使うことでサイバープロパガンダとして、高度化かつ秘密裏になり、人々が気付かぬ間に、その考え方が操作される事態が起きています。

これを行うため、サイバー攻撃によって盗んだ政治家のメールを改ざんした上での暴露のほか、メディアによる偽ニュースの発信、SNSでの偽ニュースのトレンド化、などといった、さまざまな手法を総動員してサイバープロパガンダが行われているのです。

私たちが便利に利用しているインターネットでは、一方でそういった悪意を持った人々や不確実な情報を拡散している人が多数いるということを理解し、フェイクニュースやサイバープロパガンダ発の情報への対抗には、情報の受け手が「疑わしいときは一次情報を調べる」、「他の情報と比べてみる」、「情報の発信元を確かめる」などの基本行動を取る、もしそれが「無理」となったら、身近にいる信頼できる人に聞いてみたり、それすら難しい場合には「一旦情報から距離を置いて、冷静になって考える」などの方法が有効です。

なぜならこれらは、私たちが「深く考えず情報を拡散する習性」により、不正確な情報や悪意ある情報を拡散してしまうからです。これらを防止できるように注意しましょう。

サイバープロパガンダが行われた例（米国）



サイバープロパガンダでは、フェイクニュースや盗んだ情報のリークを種として、これをトレンドにのせ、さらに、「自分にマッチした情報を好んで共有する」人たちのSNS集団（エコーチェンバー）にこれを投げ込み、最終的にその他大勢に、さも「重要なニュースである」というイメージを与え、世論を操作します。

総務省「インターネット上で流通する真偽の不確かな情報」
https://www.soumu.go.jp/use_the_internet_wisely/special/fakenews/
政府広報「インターネット上の偽情報や誤情報にご注意！」
https://www.gov-online.go.jp/article/202403/entry-5920.html

4 SNSなどのネットとの付き合い方、守り方を知ろう

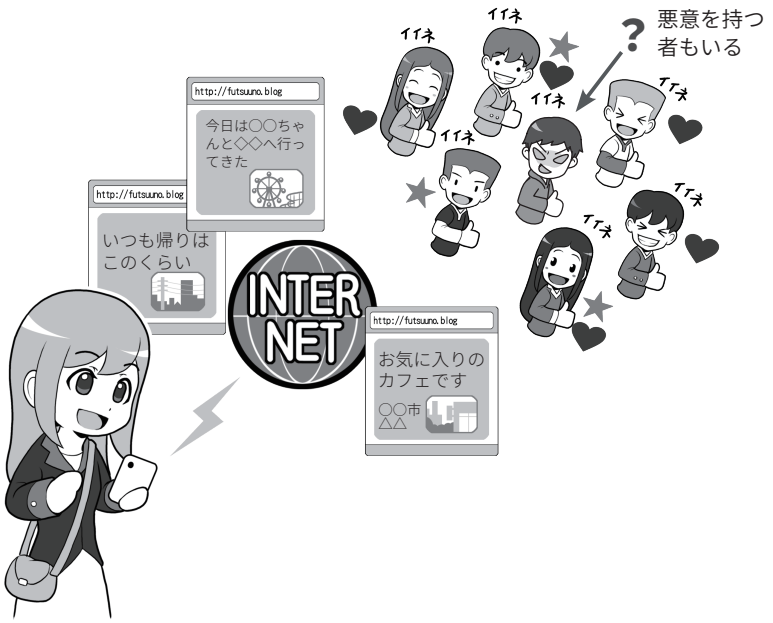
4.1 SNSなどのネットの楽しみ方と気を付けること

インターネットやスマホの普及により、今では、まるで隣に座っているかのようにチャットしたり、SNSで写真を送りあったり、映像付きのインターネット電話を使えば無料で顔を見ながらコミュニケーションができます。

一方、あなたがメッセージを発信するとき、それを受け取る人々の中には悪意を持った人や全く考え方が違う人がいることも忘れてはなりません。ネットを使ったコミュニケーションは人と人の意識のつながり合いを容易にしますが、同時に悪意を持った人等との接触も容易になるのです。

私たちは、ネットの世界をよく知って「この時代に合わせた、新しい付き合い方」を作り上げなければならないでしょう。悪意のあるものをしっかりと見分けて、善意のコミュニケーションの世界を作っていくことが必要です。

SNSやネットのコミュニケーションには落とし穴もある



SNSやネットのコミュニケーションは、距離を超えて世界中の人とつながることができます。なに気ない投稿は、多くの人の共感を得るかもしれませんが、その中には、犯罪に使える手がかりを探している悪意を持った人もいます。どうしたら悪意をかわしつつ、SNSやネットを楽しむことができますか？

4.2 SNSやネットの怖さ、こんなことが実際に起こっている

SNSやネットではどのようなトラブルに遭う可能性があるのでしょう。

SNSなどで、実際に会ったことがない同じ年ぐらいの子と友だちになり、どこかで会う約束をしたとします。しかし、待ち合わせ場所に行ってみると来たのは本人ではなくて別人でした。「○○ちゃんが待っているから連れて行ってあげる」といわれ、車に乗せられそうになりました。こんな風に誘拐・略取が行われます。

SNSに家の近くや普段立ち寄る場所、自分の写真などを上げていると、その情報からあなたを特定して、リアルのストーカーがやってくるかもしれません。

闇サイトなどを興味本位に覗いたりしていると、犯罪勧誘といって、顔も知らない人があなたを犯罪に誘ってくることもあります。最近では闇バイトが社会問題ともなっており、明らかな犯罪加担行為でない、一見、割のいい軽作業のような表現で勧誘し、本人情報を取られて脅されるケースもあります。闇バイトについて勧誘された、関わってしまった、不安があるなどの場合には、警

察庁で相談窓口なども開設しているので、適宜相談しましょう。

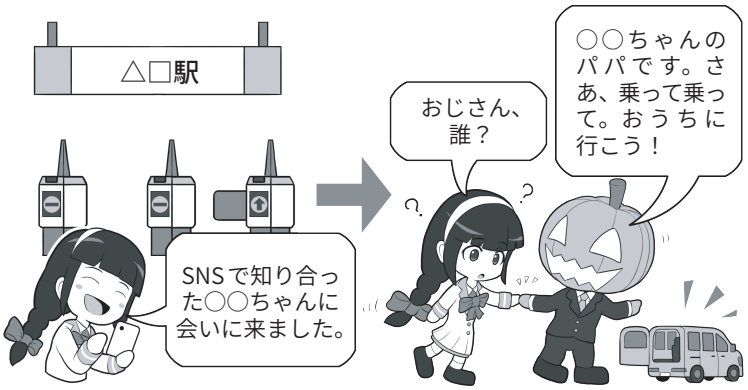
SNSのグループなどで、周りの雰囲気に流され、特定の人物のありもしない書き込みに同調したり、傷つけたり、仲間はずれにしたりする「ネットいじめ」をしたりされたりしてしまうかもしれません。

交際している相手が、「誰にも渡さないから」とあなたの裸の写真を要求してきて、信頼して渡したら、別れた後にその画像がネットに流出してしまうかも。それは、「リベンジポルノ」といって、相手が嫌がらせのために、写真をネットに投稿する行為ですが、その意図がなくても、相手のスマホがマルウェアに感染してネットに広く流出してしまうかもしれません。その写真は、消えない「デジタルタトゥー」(デジタルの入れ墨)として、以降あなたの人生に、ずっと影を落とし続けることになるかもしれません。

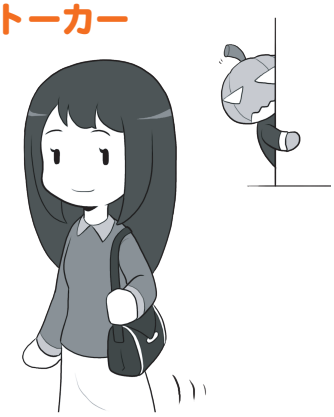
また、SNSを活用した詐欺が増えています。例えば、「SNS投資詐欺」は、インターネット上に著名人の名前・写真を悪用した嘘の投資広告を出したり、「必ずもうかる投資方法を教えます」などとメッセージを送ったりして、SNSへ誘導し、投資金などの名目で多額の金額を騙し取るものです。また、「ロマンス詐欺」は、SNSやマッチングアプリなどを通じて出会った者と、実際に直接会うことなくやりとりを続けることで恋愛感情や親近感を抱かせ、これを利用して、暗号資産の購入、架空の投資を促したり、必要な資金と称して、お金を振り込ませたりするものです。具体的な手口などは、警察庁が「SNS型投資・ロマンス詐欺」で公表しているので参考にしましょう。

この他にも、SNSやネットでは、さまざまなトラブルが発生することがあります。発信相手や情報の内容をネットだけではない複数のソースを確かめ、トラブルに決して巻き込まれないようにしましょう。

誘拐・略取



ストーカー

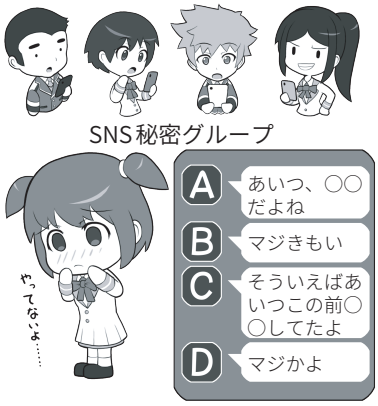


SNSで得た情報をもとに人物を特定し、リアルの世界でストーカーされる場合もあります。

犯罪勧誘

闇サイトなどと呼ばれる怪しいサイトで、面識がない者同士が集まって、犯罪を行うために仲間を探しています。

ネットいじめ



ノリでいじめに加わった結果、悲しい出来事が起きてしまったら、自分はそのときどう思うでしょう。

リベンジポルノ・デジタルタトゥー

元交際相手に、裸の写真をネットに投稿されるかも。ネットに広がった写真は消すことができません。

4.3 SNSやネットとの付き合い方の基本

SNSには、「いいね!」などの他の人からの反応や、コメントをもらうことができる機能があります。「いいね!」をたくさんもらえると嬉しい反面、少ないと気落ちすることもあるでしょう。また、否定的なコメントが来ることもあるかもしれません。人の価値観はそれぞれ違うので、それらに一喜一憂したり、振り回されたりしないようにしましょう。

また、SNSには投稿者に直接ダイレクトメッセージを送れる機能があるものもあります。知らない人からのダイレクトメッセージには注意しましょう。

さらに、多くのSNSでは投稿の公開範囲を自由に設定できます。設定範囲によっては友達以外の人が見ることがあるかもしれません。従って、氏名、住所、電話番号、学校や勤務先などの情報をむやみにプロフィールに掲載しないようにしましょう。個人情報を悪用されたりする場合やストーカーなどの被害に合うことも考えられます。

自分の投稿を不特定多数の人が見られる設定になっている場合は、自分の顔写真や居場所が特定される場合があるので、投稿には十分注意が必要です。また、知らない人だけでなく、友達の顔写真もむやみに投稿すると個人の特定や肖像権の問題が生じる場合がありますので、慎重に行いましょう。SNS利用に関しては総務省から「安心・安全なインターネット利用ガイド」(https://www.soumu.go.jp/use_the_internet_wisely/)で上手なネットとの付き合い方が示されているので、参考にしましょう。

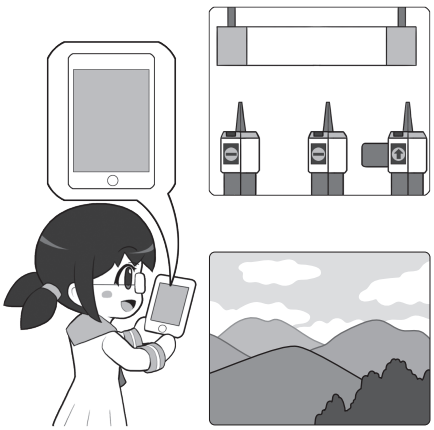
「いいね!」が少なくても気にしない

「いいね!」は、人それぞれの主観です。年齢も学校も大人なら仕事も異なります。多様な価値観があることを理解して、「いいね!」の数を気にしないようにしましょう。

個人情報は基本的に公開しない

一度流出した個人情報は、絶対にネットから消し去ることができませんし、ときに個人の居場所を特定する情報になります。悪意がある人にとって、手がかりになる情報はネットに載せないようにします。

個人が特定される情報はSNSなどに投稿しない



自分自身の写真や、日常的な生活圏がわかる情報を投稿しないようにしましょう。友人のみに公開としていても、その人が共有したら一般に公開されることもあります。また、スマホで「位置情報あり」で撮影していると、見えなくても写真に位置情報が記録されるので注意しましょう。

4.4 モラルを逸脱すると炎上を生む

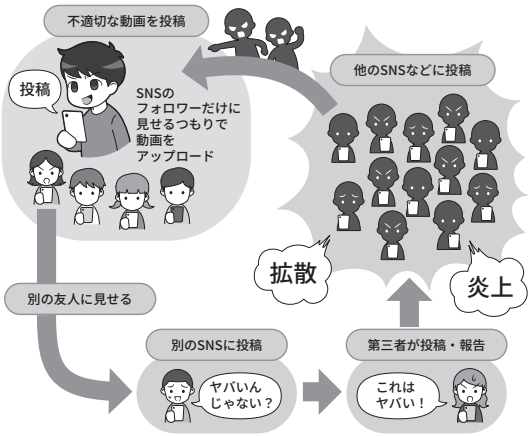
「炎上」とは、不適切なSNS投稿が拡散され、多数の人から非難を受ける現象を指します。その例には、誹謗中傷の書き込み、プライベート情報の無断投稿、未成年の飲酒投稿などが含まれます。炎上は、世間一般のモラルに反すると判断された場合に発生し、投稿者本人だけでなく、関係する店舗や企業にも多大な影響を与え、店舗の閉店、企業の謝罪、損害賠償請求や名誉毀損での訴訟、解雇や内定取消、さらには悪質な場合には業務妨害などの犯罪として捜査される結果をもたらすこともあります。

炎上を防ぐには、自分の投稿が広く読まれることを意識し、批判を受けない内容かどうかを慎重に考える必要があります。自信がない場合は投稿を控えるのが賢明です。また、ネットでの炎上事例を他人事とせず、自分に置き換えて考えることが重要です。炎上は些細なきっかけで起こり得るため、SNSの拡散力や影響を理解し、その場の勢いなどでの軽率な投稿を避けるべきです。

さらに、「自作自演」や「なりすまし」なども状況次第で犯罪や名誉毀損に該当する可能性があるほか、軽い気持ちで行った行為が取り返しのつかない結果を招くことがあります。ネットでの投稿の意味を十分理解し、SNS等の利用を心がけることが大切です。

モラルを逸脱することが炎上を生む

よくある「炎上」の流れ



①発信者が自分のフォロワーなどだけが見るだろうと安易に考え不適切な内容を投稿

②投稿を見たユーザーが問題と感じて元とは違うSNSなどにその内容を投稿

③フォロワーが多いインフルエンサーが該当の投稿を発見して批判的内容を投稿

④インフルエンサーのフォロワーなどがさらに批判的投稿を行い元の不適切な投稿が拡散

⑤マスコミなどに取り上げられることによりさらに拡散

といった流れが考えられます。

③の段階にまで至ると、拡散速度が加速度的に増大し、なかなか沈静化しません。炎上が一旦生じると、発端の問題投稿をした投稿者の個人情報まで特定され、また、元の投稿の拡散も相まって炎上状態が沈静化した後も、ネット上に問題の情報が残り続けます。

4.5 望まない情報流出、流出したら消すことは難しい

個人情報や写真も、スマホなどの中から出さなければ大丈夫ではないかと思われるかもしれませんが、望まない情報流出の罠は、さまざまなところに隠れています。

スマホやパソコンの中に存在しているデータは、写真でもメールでも住所録でも、すべてマルウェアの感染などによって流出する可能性があります。

自分が、セキュリティについて学んでそのような可能性を少なくできても、現状では、サイバー攻撃を完璧に防ぐことはできないので油断してはいけません。

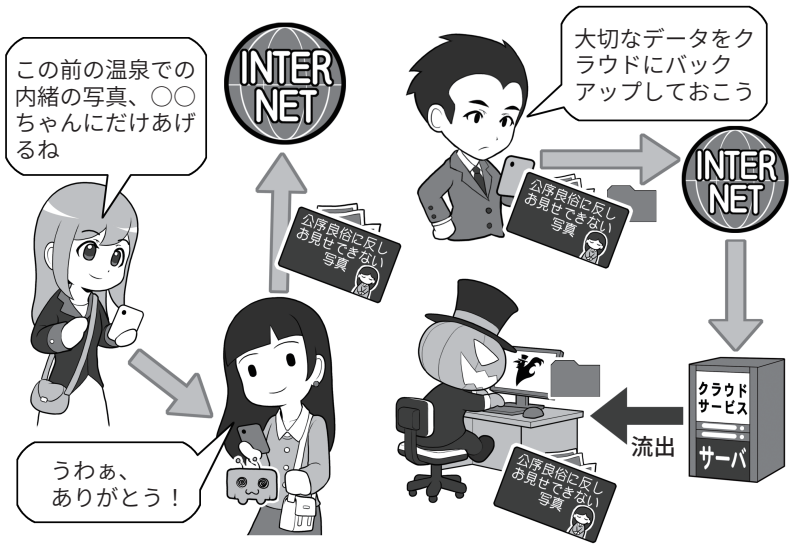
それに、例えば、信頼できる友人であっても、秘密の写真を共有した場合、その友人のスマホなどがマルウェアに感染して流出する可能性もあります。相手が、自分と同じレベルのセキュリティ知識を持ち、実践しているとは限らないですし、また、それを強要もできません。

したがって、流出を確実に阻止したい情報は、ネットワークから切り離して管理し、他人とは共有しないなどの対応が必要です。

さらに、秘密の写真などをクラウドサービスにバックアップのつもりで保管する場合、データが自分の手元と他人の管理下に複数存在するため、流出する可能性のある場所が増えることになります。事実、クラウドから有名人の写真が流出する事件も発生しています。

流出したら問題になることは、しない、させない、撮らない、投稿しないようにしましょう。

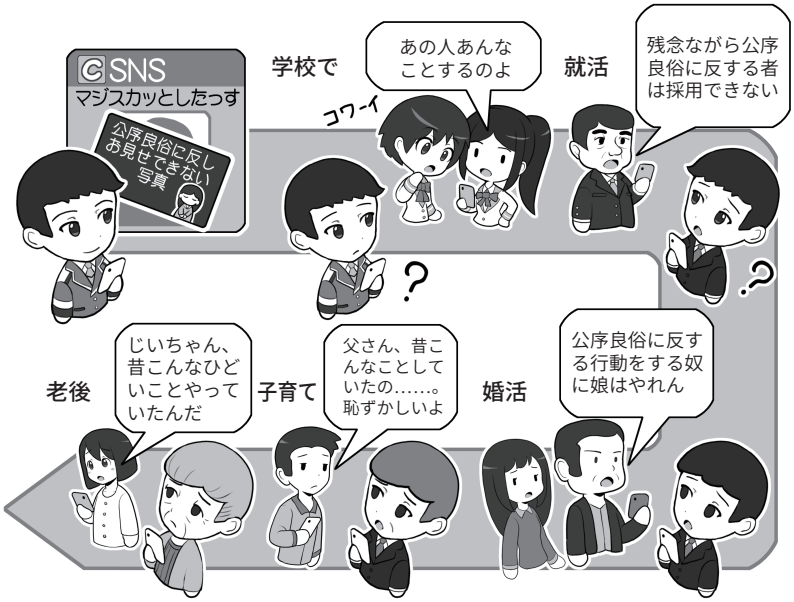
存在するデータは必ず流出することがあると考える



自分が流出させなくても、渡した相手がマルウェアに感染して流出させてしまうかもしれません。

パスワードの使い回しなどで、クラウドサービスからデータを抜かれて流出してしまうかもしれません。

投稿したデータは一生ついてまわるかも



上記は極端な例ですが、たとえ若気の至りが少年法によって許されて、その後、裁判所などに申し立ててプロバイダに情報の削除の依頼をしても、ネットに拡散した情報のすべてを消し去ることはできず、人生の節目であなたを苛むかもしれません。

まず、問題になることはしないことです。そして、（助長する意味ではなく）ネットに投稿するものはよく考えてから投稿しましょう。

5 便利なサービスや機能を利用して家族を守ろう

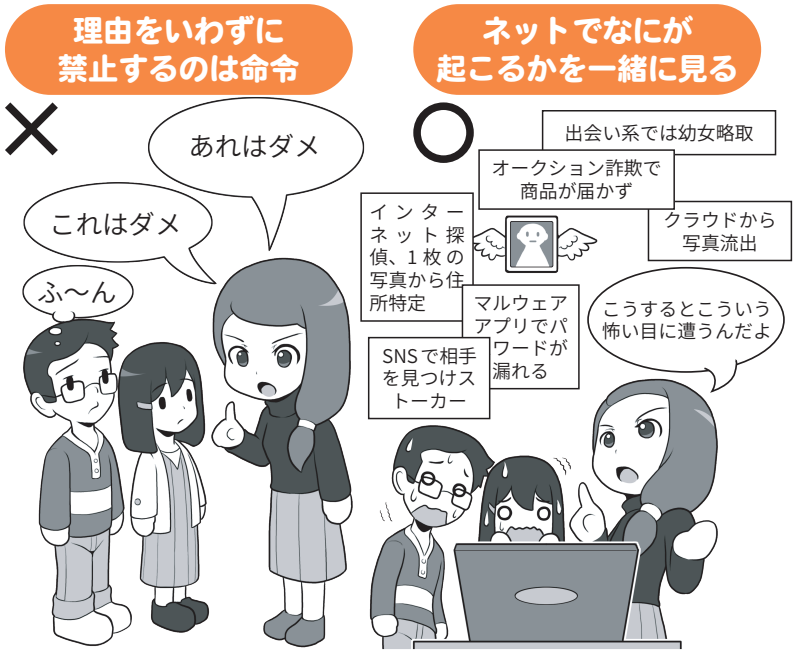
5.1 こどもを守る

こどもをインターネット関連の犯罪から守るには、理由を述べずにあれもダメこれもダメと頭ごなしに禁止せず、まず可能な限りどういった犯罪がどのように行われるのかを知らせましょう。

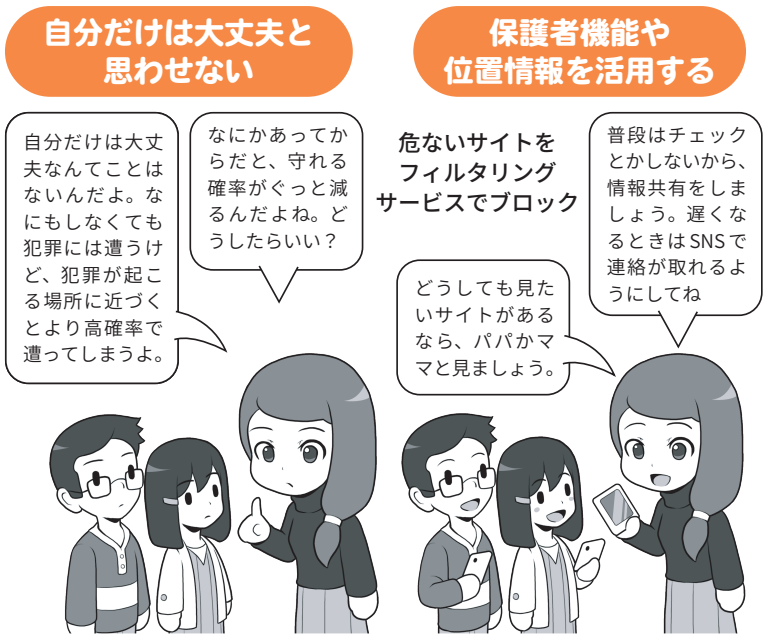
こどもたちが犯罪に当たる行為をするとき、本人たちはそれが「犯罪になると思っていなかった」という例もあります。知ることが抑止することにもつながります。

サイバー犯罪に遭うという視点からも、問題点や危険性、また、それによってどれぐらいの範囲にトラブルが広がるのか、きちんと共有することが必要でしょう。

本当は怖いインターネット



頭ごなしに禁止せず、インターネット関連のトラブルの実例を見ながら、なぜダメなのかを「理解」しあって共通の認識を作ります。こどもだけでは、対処できないトラブルがあることを知ることが重要です。



意識を共有したら、実例を示してこどもたちに答えを出してもらいましょう。自分で出した答えは自らのルールとなるからです。

5.2 こどもに対する情報モラル教育の重要性

SNSやネット上のリスクは、学校に通う児童・生徒に対しては、昨今のGIGAスクール構想による情報モラル教育の効果もあり、一定程度は理解が進んでいると思われます。

GIGAスクール構想を推進した文部科学省が告示している小〜中〜高校の学習指導要領によると、「情報モラル」は学習の基盤となる資質・能力の1つである「情報活用能力」にも含まれると定め、SNSやネット上のリスクについての理解などを含め、情報モラル教育の重要性が示されています。

一方で、児童・生徒の保護者には、情報モラル教育の重要性やその教育が求められる背景として存在するSNSやネット上のリスクを十分に理解できていない人も少なくないでしょう。こどもと保護者とのサイバーセキュリティに関する知識格差を埋めるためにも、保護者もSNSやネットのリスクは知っておきましょう。

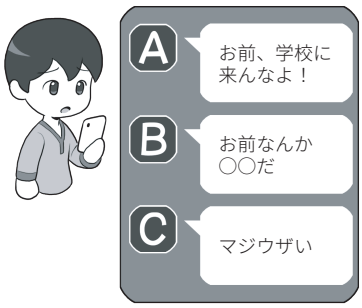
また、ネットの普及により、いじめはSNS上などで表面化しにくく巧妙化しました。悪口の書き込みやSNSグループからの排除といった形で行われ、大人からも発見しにくい場合があります。お子さんがネットいじめに遭った場合は、教師に相談し、画面ショットなどの証拠を保存することが重要です。

GIGAスクール構想により、児童・生徒1人一台の端末が配布され、ICT教育が進む一方で、これらの端末がネットいじめの手段になる可能性もあります。SNSでの誹謗中傷やパスワード流出によるトラブルを防ぐため、アカウントの適切な管理が必要です。このような環境下では、環境整備の本来の目的を踏まえつつ、ネットリテラシー教育の強化と、いじめ防止の仕組みを整えることが求められます。

いじめは閉鎖された場所で起きやすい

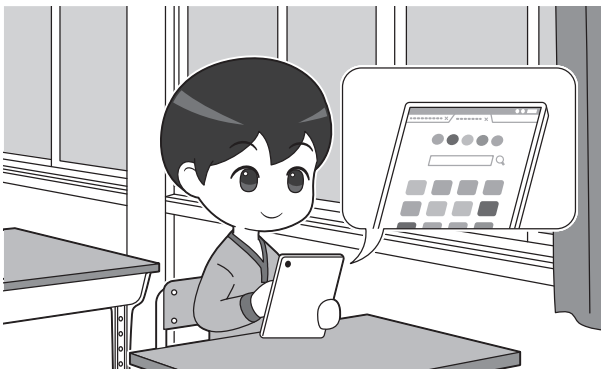
公共の空間では人の目がある

ネットは他人から見えにくい



人の目は、ときに抑止力になりますが、ネットの中は人目が少なく、その分いじめは陰湿でエスカレートしがちです。

GIGAスクールでICT教育環境が充実!!



コロナショックも影響し、2020年から急速に推進されたGIGAスクール構想により、全国の小中学校では児童・生徒1人1台の端末普及が実現しました。

GIGAスクールの端末は、学校のルールを守り、学習など正しい目的で使う

残念ながら、配布された端末を用いてSNSで他人への悪口を書き込むネットいじめが問題になりました。同じパスワードの使い回しにより、勝手に友達のアカウントになりすまし、誰が悪口を書いたかわからない事態になるなど、いじめの早期発見が難しくなってエスカレートする可能性があります。

5.3 こどもにスマホを持たせるとき「スマホ契約書」の提案

こどもがスマホを欲しがる際、利用に関する家庭内ルールを明確に定めることが、トラブル防止に重要です。総務省が実施した「我が国における青少年のインターネット利用に係るペアレンタルコントロールの効果的な啓発に関する調査結果」では、家庭内ルールと保護手段を併用することでトラブルのリスクを軽減できることが示されています。また、こども家庭庁が実施している「青少年のインターネット利用環境実態調査」からは、親とこどもでルールの認識が食い違うケースが多いことが分かり、ルールを確認し合い事前に取り決めておく必要性が浮き彫りになっています。

家庭内ルールを「契約書」という形で明文化することで、親子双方が約束を強く意識できるようになります。契約書はこどもに「一人前」として認められている感覚を与え、ルールを守る意識を高める効果もあります。具体的なルールとしては、「食事中にスマホを見ない」、「夜10時以降は使わない」など家庭ごとの方針のほか、「SNSでは誰に読まれても問題ない内容だけを投稿する」、「恥ずかしい写真を送らない」、「知らない人から、実際に会いたいなどの誘いが来た場合は親に相談する」など、ネットトラブルを防ぐための内容を含めると良いでしょう。

契約書作成の際には、親子で十分に話し合い、こどもが実行可能な具体的なルールを設定することが大切です。また、ルールを破った際の対応策も取り決めておく必要があります。さらに、一度作成した契約書は、こどもの成長や環境の変化に応じて定期的に見直し、更新することが重要です。

家庭内ルール作りの参考として、文部科学省が提供する「話し合っていますか？家庭のルール」教材が役立ちます。このように、ルールの明文化と更新を通じて、親子の信頼関係を深めながら、スマホ利用における健全な習慣を築いていくことが求められます。

口約束は忘れてしまいやすい？

ルールは決めても、口約束だけで見返せないと、あやふやになってしまいがちです。結果的に感情的なやりとりを生みます。

契約書を作り、責任ある人として接する

契約書は固いイメージもありますが、ルールをときどき見返すことができる他、言った言わないにならないというメリットもあります。

なにより相手を責任ある人間としてあつかうことで、ルールを自ら決めたことの自覚と守ることへの自律を促しましょう。

5.4 こどもを守るためのサービス

スマホには、こどもに有害と思われるサイトを閲覧できないようにするフィルタリング機能や、アプリの使用も含めて、こどものスマホ自体を管理するペアレンタルコントロールの機能があります。これらの機能を契約書の内容と合わせて、こどもの年齢に応じて適切に使うことで、こどもに対するスマホやネットの安全性をより高めることができます。

そのため、セキュリティソフトやフィルタリングサービス、緊急時のための位置情報共有の必要性を一緒に確認しましょう。

いざというとき、こどもを助けに行くためには、位置情報は非常に有効な手段です。一方、こどもたちは過度に位置情報に関することを追求されると、共有を切ってしまうかもしれません。こどもでもセキュリティの設定などはすぐに変更してしまうでしょう。こどもに対しては、セキュリティの必要性をわかりやすく説明しましょう。とくに位置情報の共有は監視のために使わないことを約束し、そして、約束を守りましょう。

また、こどもからルールの変更やどうしても見たいウェブサイトなどを言い出しやすい雰囲気を作り、それについて一緒に話し合って勉強する姿勢を示しましょう。スマホやIT機器は絆を断絶するためのツールではなく、より太く結ぶためのツールなのです。

スマホが使えないほど幼いこどもたちを守るサービスや機器も、いろいろと登場しています。

学校を離れたときや駅を通過したときに、親のスマホにメールが送信される見守りメールサービスや、メッセンジャーアプリ、簡単な通話機能

安全を守るさまざまな方法

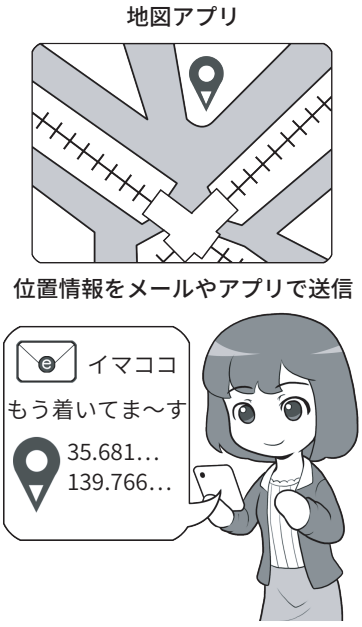
見守りメール

見守りメールは、鉄道会社や一部の学校などが提供しているものがあるので、自分が住んでいるエリアでサービスが行われているかを調べてみるとよいでしょう。

GPS付きキッズケータイ

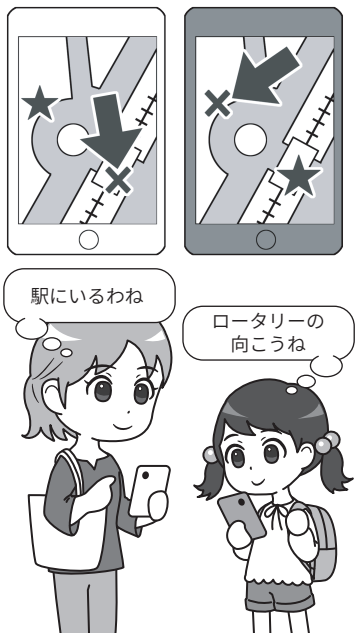
連れ去りや変質者に遭遇したときに使用する、防犯ブザーと簡単な通話機能が一体になったスマホです。簡単な操作で登録された特定の人物への通話なども可能です。

位置情報の送信



地図アプリの位置情報共有機能を利用して、メールやメッセンジャーアプリから現在地を簡単に相手へ送信できます。受信した相手も自分のスマホの地図アプリを起動すれば位置を確認できます。

位置情報共有アプリ



位置情報共有アプリは位置情報を相手へ送信する手間を省いて共有でき便利ですが、不用意に必要以上の人と位置情報の共有をしないことが重要です。

とGPSと防犯ブザーが合体したキッズケータイは、シンプルな操作方法を理解したら、いざというときの強い味方になります。

また、ある程度スマホの操作ができる年齢になったら、位置情報を送信したり、必要な情報をメールやSNSを通じて共有する方法を、一緒に覚えるのもよいでしょう。

位置情報共有アプリは便利ですが、悪用されストーカーなどの被害に遭う可能性もあり、刺傷事件に至ったケースもあります。位置情報を共有するのは、こどもが幼いうちは親のみにしておくようにするとよいでしょう。また、ある程度の年齢になっても不用意に必要以上の人と位置情報の共有をしないことが重要です。

なお、現在は建物の中で迷子になると位置情報や何階にいるかなどの情報は共有できませんが、今後地下街や建物内などにビーコン（Beacon）と呼ばれる装置が普及することで、屋内でも位置情報の交換が可能となると考えられます。

また、どこかではぐれても、電車やバスの乗り換え案内や徒歩ナビゲーションなどのアプリを利用して、家に帰り着く方法をこどもと一緒に学びましょう。

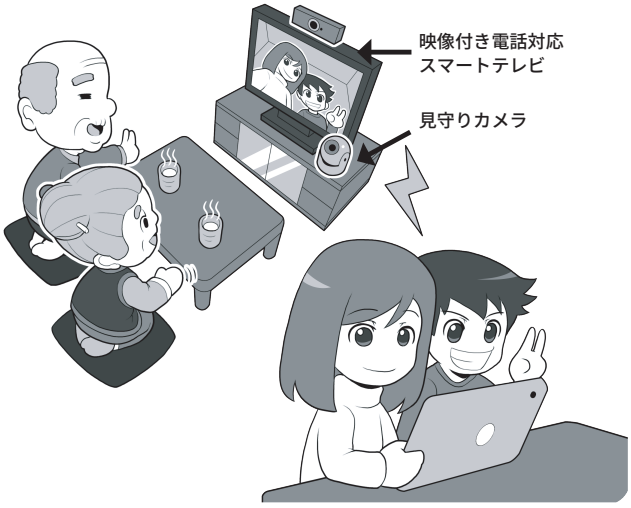
5.5 お年寄りを守る

お年寄りも、最近ではパソコンやスマホなどを使う方が増えています。ただ、これまでに馴染みがなかったことから、操作に不慣れだったり、インターネットの危険性等にうとい方もいます。特にソーシャルエンジニアリングを用いた詐欺は、「振り込め詐欺」のようにネット以外の方法でも被害が増大しています。

振り込め詐欺は電話で顔がみえない状況で、相手を不安に陥れ、さらに即断が必要な状況に追い込むなど、被害者に正常な判断を行わせなくするように仕向けています。これに対抗するために、例えば、ご両親に連絡するときは、通話アプリのTV電話機能を使うと決めておけば、顔が見えない状況で丸め込まれ、騙されることを回避できるかもしれません。

高齢者の方がスマホなどを使い始める際に、操作などを会得するのを支援するため、国では「デジタル活用支援推進事業」（https://www.digi-katsu.go.jp/）を行っており、高齢者等が身近な場所で身近な人からデジタル活用について学べる講習会を設けたり、役立つ学習資料等を提供したりしています。また、いざ操作を勉強する段になって教えてあげやすいように、自分が持っているものと

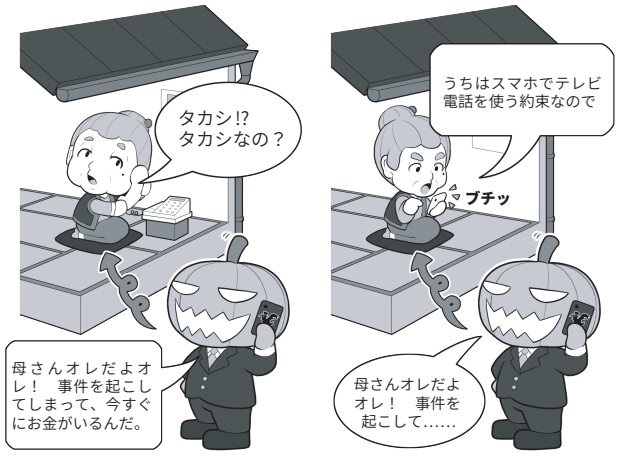
映像付き電話やITサービスの活用



お年寄りにとってこどもや孫たちの顔を見るのは、なによりの楽しみでしょう。会いに行ってあげるのが一番ではありますが、なかなか訪ねて行けないときは、顔を見てコミュニケーションを取れるツールを活用しましょう。

また、1人暮らしのお年寄りに万が一のことがあったときのために、日々生活状況を確かめられるサービスも存在しますので、利用を検討してもよいでしょう。

IT機器を使った振り込め詐欺対策



電子機器の操作に不慣れなお年寄りでも、スマホの電話機能ならよく使うでしょう。こどもや孫から連絡を取るときは必ずテレビ電話を用いるという方法を使えば、顔が見えない状況で不安に陥れる「振り込め詐欺」などの予防にもなります。同じスマホを渡してあげれば、操作を教えることも簡単です。

同じ機種を渡しておくのも1つの考え方です。

ご両親の海外旅行時に、きちんと目的地に着けているか、迷ったりしていないか心配な場合は、事前に相談して位置情報共有サービスや移動履歴が残るサービスを設定して旅に出てもらいましょう。

こうすることで、今どこにいるかを確認できるので、予定どおりに旅行しているかもチェックできます。また、仮に旅先で迷子になってしまっても現在地がすぐわかれば、どのようにしたらよいかのアドバイスも的確にできるでしょう。

そのようなことはあまりあってほしくありませんが、もしスマホを紛失したり盗まれたりした場合も、操作するための情報を共有しておけば、スマホをロックしたり所在地を確認したりできます。

認知症を患っているお年寄りは、家族の見ていないときに外で徘徊し、事故に遭ってしまうことがあります。

また、一緒に外出した後で目を離した隙にいなくなってしまい、本人も自分がどこにいるのかわからず、その結果、行方不明になってしまうケースもあります。

そういった場合に備えて、GPS発信器を使った位置情報サービスを契約したり設定したりしておくと、間をおかず探し出すことができます。

もちろん目を離さないことが重要なのですが、ご自身にリカバリする能力がない状況では、万が一に備えた方が安心でしょう。

持ち慣れない機器を持つことを嫌がるお年寄りの方も少なくないので、機器を携帯してもらうの際に工夫は必要ですが、事故などを未然に防げる可能性が少しでも高くなるならば、検討してみるとよいでしょう。

位置情報の共有（安否確認）

スマホの位置情報の共有設定をし、現地でもインターネット接続サービスを利用できるようにしておくと、世界中どこにいても現在地を確認することができます。年輩の方自身が位置情報を使いこなせなくても、電話やSNSのメッセージ機能などを使ってサポートすることができます。

※現地でデータ通信できるように、データローミングの利用や海外用のSIMを手配する場合は、渡航前に準備や設定を済ませておきましょう。また、現地に着いたときに確認するべき事項を紙などに書いて、事前に説明しておきましょう。海外で購入したSIMの使用は最初の設定をしないと、インターネット接続もできない場合がありますので注意が必要です。

認知症の方の事故防止に

普段押して歩くカートや、お守りに入れて持たせたり、物を持ちたがらないお年寄りには、靴の中に入れられる機器も存在するのでそのようなものを利用したりします。しかし、これらはなにかあったときのバックアップの手段で、普段から目を離さないことがなにより大切です。

最後に例えばその方が亡くなると、資産や負債を含めて、どういったものが残されたのかわからない場合もあります。残された人が困らないように、万が一のときに備えて管理情報のありかを残したり、PINコードをノートや遺言書に残したりするなど、残った家族が分かるようにしてもらいましょう。

6 スマホのセキュリティ設定を知ろう

6.1 スマホにはロックをかけ、席に置いて離れたり、人に貸したりするのは×

スマホには必ず画面ロック（以下「ロック」という）をかけてください。

ロックにもPINコードによるロック、パターンロック、指紋や顔など生体情報を用いた認証によるロックなどがあります。過信は禁物ですが、生体認証は周りから覗かれPINコードを盗まれる危険性の排除をしつつ、入力の面倒くささを省くので便利な機能です。

そしてセキュリティ向上のためのロック機能を設定しても、そのスマホをロック解除したまま置いてその場所を離れたり、ロックを解除して他人に見せたり貸したりすれば、せっかく施したセキュリティ対策が台無しになります。他人の手に渡れば、情報を盗まれ、乗っ取られる危険性が上がります。

スマホは大事な情報が詰まった貴重品、肌身離さず自分のそばに置き、使わないときはこまめにロックをかけましょう。

また、スマホだけでなくアプリにもロック機能があれば積極的に設定しましょう。

安全性を高めるには、スマホとは別のPINコード、または別のロック機能を選ぶとよいです。

しかし、ロックを設定しているからといって十分ではありません。

ロック中の待ち受け画面に表示される通知内容にも気を配りましょう。

とくに、待ち受け画面でメールの内容を表示できる設定にしていると、メールアドレスによる多要素認証を設定している場合、パスワードが記載されたメールの内容が待ち受け画面で確認でき盗み見られてしまう可能性があります。

待ち受け画面に表示する通知はよく検討すべきでしょう。

スマホには必ず画面ロックをかけよう

本来は、上記の例のようにスマホを手放してはいけません。しかし、ロックをかけておけば、最低限のセキュリティは保てます。普段からスマホには必ずロックをかけて、肌身離さず持っておきましょう。

待ち受け画面の通知にはなるべく重要な情報は表示させないようにしよう

上記の例のように「こんな場所だし、大丈夫だろう」と油断してはいけません。待ち受け画面の通知は覗き見のリスクが高いので、重要な情報は表示されないようにしたほうがよいです。

7 パソコンのセキュリティ設定を知ろう

7.1 パソコンを買ったら初期設定などを確実に

パソコンを購入したら、まず復旧のときに行うリカバリの方法を確認し、必要があればリカバリメディアを作成しておきましょう。

リカバリメディアがDVDなどで付属している場合は必要ありませんが、最近の機種ではコストダウンの影響で添付されないものや、そもそもDVDドライブなどを搭載していないものも多いので、マニュアルなどにしたがってDVD-RディスクやUSBメモリで作成します。

なお、Windowsではリカバリメディアなどを使ったときに「プロダクトキー」の入力が必要になる場合があります。

プロダクトキーは本体の裏側や付属しているリカバリメディアにシールが貼り付けられているので、紛失に備えスマホなどで写真に撮っておくか、メモに書き写して保管しておきます。

次に、セキュリティ設定をします。

初期設定時にIDと「ログインパスワード」の設定を必ず行いましょう。

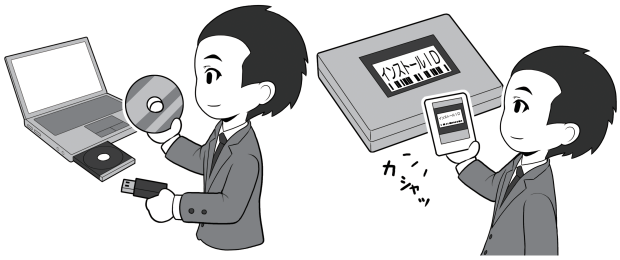
また、マニュアルにしたがって起動用「BIOSパスワード」や「ファームウェアパスワード」という、電源を入れた段階で入力が求められるパスワードも設定しましょう。

これを設定しておくと、盗難されてもOSの起動ができなくなり、盗難時の情報流出をより強固に防ぐことができます。

これらのパスワードは、「ログインパスワード」のセオリー通り複雑で安全性の高いものを設定してください。

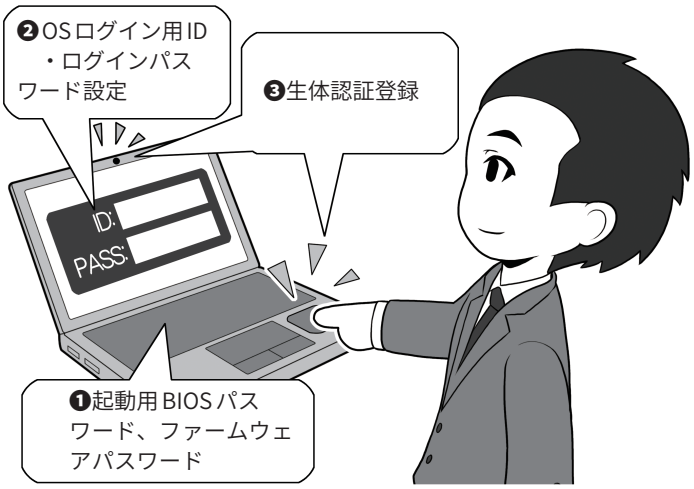
生体認証を使用すると、パスワードの桁数が多くても毎回入力する必要がなくなるので、ログイン操作が楽になるメリットがあります。

パソコンを買ったらまずリカバリメディアを作る



DVD-Rディスクや USB メモリでリカバリメディアを作り、本体裏などにあるプロダクトキーを撮影し保存します。メディアが添付されていれば作る必要はありません。

起動用のパスワードや生体認証登録をしよう



「ログインパスワード」はセオリーどおり複雑なものを設定し、その上で生体認証を使いログインの手間を省くようにします。盗難や不正利用防止のため BIOS パスワードなども設定しましょう。BIOS パスワードなどは「ログインパスワード」相当に設定します。

8 パスワードを守ろう、パスワードで守ろう

8.1 3種類の「パスワード」を理解する

パスワードの役割を担うものには、他に「暗証番号」などや、通信している情報やパソコン・スマホの中のデータを暗号化して、他人や攻撃者が読めないようにする、「暗号化と復号の鍵＝暗号キー」というものもあります。

この3つは、性格や役割が異なるのですが、よくまとめて「パスワード」と記述されることがあるのと、暗証番号、パスワードと暗号キーは、等しく攻撃の対象になるために、ここでは一括して扱います。私たちは、機器やウェブサービスを利用するとき、あるいはファイルを開くときに入力するものを、まとめて「パスワード」と呼び、同じような役割をするものと思いがちです。

しかし、セキュリティ上の性質から、「パスワード」とまとめて呼ばれるものは、大きく3つに分けて理解する必要があります。

1. 銀行のキャッシュカードやクレジットカードの利用時、スマホのロック解除時に使用し、通常4桁から6桁以上の数字だけで構成されることが多いもの（暗証番号やPIN、PINコード、パスコード。通信事業者のネットワーク暗証番号などを含む）
2. パソコンやデジタル機器、ウェブサービスなどの利用時にIDとセットで入力し、英大文字小文字、数字、記号を用い複雑さと一定以上の長さが推奨されるもの（狭い意味でのパスワード、ログインパスワード）
3. パスワードと呼ばれていることもあるけれど、本当はファイルや通信内容を暗号化しまた復号するための暗号鍵として単独で用いられるもの（ZIPファイルのパスワード、WordやExcel、PowerPointの保護パスワード、Wi-Fi機器の暗号化キー、暗号キー、パスフレーズ、セキュリティキー、ネットワークキー）

一口にパスワードといっても、上記のとおり、実にさまざまなものがあります。この本では、以降、この3つを混同しないように、

1を「PINコード」
2を「ログインパスワード」
3を「暗号キー」

と呼びます。

8.2 「PINコード」と「ログインパスワード」に求められる複雑さの違い

機器やウェブサービスを利用するとき、「ログインパスワード」桁数が多い方が安全に資します。

一方、同様に使う「PINコード」は、メーカーが数字のみの4桁から6桁以上でよいとしています。

この2つは、両方とも機器やウェブサービスを利用するときに使用するのに、求められる長さや複雑さに差があるのはなぜでしょうか。

そもそもパスワードに「複雑さ」が求められる理由は、攻撃者が制限のない状態でパスワードの文字列を総当たりで試すと、時間はかかるが「いつか必ず探り当てることが可能」だからです。これは、どんな複雑な「ログインパスワード」でも変わりません。

こうやって力業（ちからわざ）でパスワードを探り当てる攻撃を「総当たり攻撃（ブルートフォース攻撃）」と呼び、「ログインパスワード」を守る第一歩は、いかにこれを成功させないかにあります。

スマホの「PINコード」の場合は、数回間違うと「入力遅延」といって一定時間「PINコード」を入力できないようになり、さらに「10回間違えば以降PINコード入力不可にする（ロック）」、「場合によっては機器を初期化する（ワイプ）」ことで「総当たり攻撃」を不可能にし、攻撃者による不正利用を防ぎます。

さらに、厳しいキャッシュカードなどでは、3回間違うと以降カードが利用できなくなりますが、これも同じ考え方です。

「PINコード」では、こういった厳しい制限を設けることで「総当たり攻撃」を不可能にし、4桁から6桁以上の数字でも攻撃者から機器やサービスを守れるのです。

一方、「ログインパスワード」は、通常「PINコード」のようにワイプまでする機能がついていることは、ほぼありません。数回失敗すると入力間隔が空く、一定時間入力をロックするなどのペナルティを受ける場合もありますが、ペナルティがないものも多いのです。

この「ログインパスワード」は、ウェブサービスのログインページや、パソコンやIoT機器のログイン画面に入力するもので、こういった入力画面では、ネット経由でロ

グインを試みた場合、どう頑張っても1秒に数回～数十回程度しか入力することができず、これだけで実質的に高速な攻撃を防ぎます。

8.3 「暗号キー」に求められる複雑さ

上記の「ログイン画面」に入力する「ログインパスワード」とは異なり、「暗号キー」の場合は、攻撃者が暗号化されたデータを盗んで持ち帰り、ログイン画面の遅延などなく、自分のペースで高速な暗号化解除（解読）の攻撃ができます。

この攻撃の対象となるのは、「1つ、または複数のファイルを圧縮したパスワード付きZIPファイル」、「パスワードを設定したMicrosoft Officeのファイル」、「暗号化されたUSBメモリ」や「パソコンから取り出された内蔵補助記憶装置（ハードディスクやSSD。以下記憶装置」、あるいは「暗号化された無線LAN通信の内容」などです。

「暗号キー」が短いと、市販されているゲーム用パソコンの性能で暗号化解除は十分可能です。またこれらの性能が向上すれば、非常に短時間で解除されるような日がいずれ訪れても不思議ではありません。

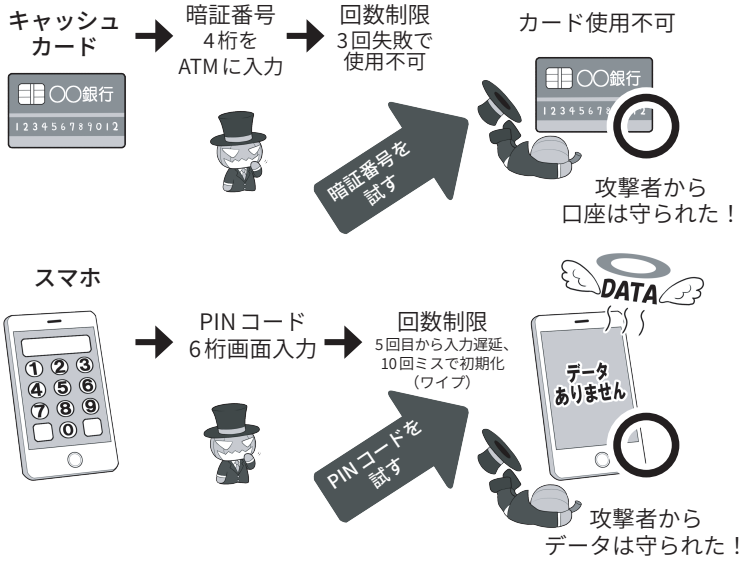
8.4 総当たり攻撃以外のパスワードを破る攻撃や生体認証を使った防御

パスワードなどを破る攻撃には、「総当たり攻撃」の他にもさまざまな手法があります。

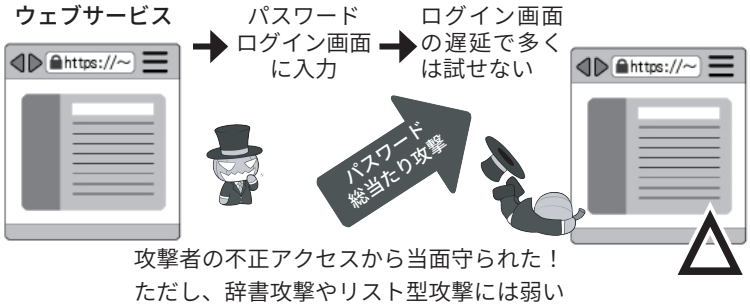
パスワードでよく使われる言葉などを集めた、専用の辞書を利用する「辞書攻撃（ディクショナリアタック）」、ウェブサービスなどから流出した名簿やIDとパスワードのリストを入力して試す「リスト型攻撃（ア

3種のパスワードを理解する

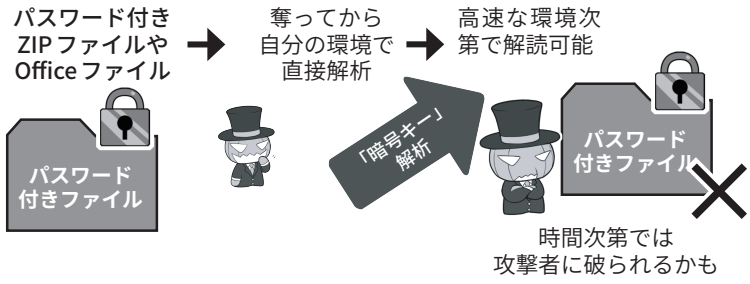
①「PINコード」の基準で安全性を保てる例



②「ログインパスワード」の基準で安全性を保てる例



③「暗号キー」の基準で安全性を保てる例

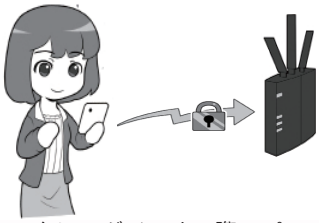


一見、安全性を保つための基準がわかりにくい例

内蔵記憶装置暗号化の救済が必要になる場面

「ログインパスワード」基準の複雑さで安全性を保てそうに思えるが、実際には入力遅延による防御が働かないので「暗号キー」の基準を採用すべき。

無線LANアクセス時に入力するパスワードを決める場面



ルータにログインする際のパスワードは「ログインパスワード」でよさそうだが、「暗号キー」の基準で設定した方がよい。

※この図は一例であり、実際の機器の条件とは異なります。

カウントリスト攻撃・パスワードリスト攻撃)」など。

これらに対する防御のためにも、「ログインパスワード」には意味のある単語や、自分に関連の深い語句やよく使われるパスワードは避け、推奨する基準に従い、充分に複雑で、かつ他の機器やウェブサービスで使い回していないものを設定しましょう。

「PIN コード」は、入力を間違え続けると「入力遅延」や「ロック」機能があるため、「総当たり攻撃」などの手法が有効ではありません。

しかし、「PIN コード」の強さは「盗み見や、推測されないこと」が前提ですので、入力するときは周りに気を配り、また、自分の個人情報など推測しやすいものは使わないようにしましょう。

現に、ATM でお金を下ろすときに「暗証番号(PIN コード)」を肩越しに覗き盗み取る手口は、「ショルダーハッキング」としてよく知られています。

「PIN コード」の盗み見などを防ぐためには、指紋認証や顔認証などの「生体認証」を利用するのも1つの手です。それらなら肩越しに見られても、攻撃者が容易にまねをすることはできないからです。

「暗号キー」は、攻撃に遅延がないので、「総当たり攻撃」を含めすべての攻撃が有効です。また、攻撃されるまでもなく、そもそも「暗号キー」が漏れていれば暗号化された中身が解読され、ひとたまりもありません。

8.5 多要素認証を活用する

ID とパスワードでの認証に、さらにチェック機能を追加するのが多要素認証と呼ばれる機能です。これを利用することで、パスワード流出時の乗っ取りをより困難にします。

最も一般的な方法は、なんらかの手段で入手する、その場限りの「ワンタイムパスワード」の入力を追加する方法です。ログインに当たって、サービス提供者から、SMS や電子メールで送られてくるものを利用する方法や、スマホのアプリを使って生成するソフトウェアトークンや専用の小さな乱数を発生するハードウェアトークンを利用する方法、そして物理的な USB セキュリティキーや生体認証を用いる方法があります。このうち、SMS 方式は海外で乗っ取りからのなりすましで破られた例があり、電子メールも経路上で奪取される可能性があるので、自分で種類を選択できる場合は、トークン、USB セキュリティキー、または生体認証方式を推奨します。

生体認証は代表的な指紋認証のほか、目の虹彩の模様によって認証する「虹彩認証」、手や指の静脈のパターンで認識する「静脈認証」などがあり日々進化しています。それぞれの特徴やセキュリティ上のメリットをよく検討して利用しましょう。

但し生体認証も 100%安全とは言い切れません。最近では、どこかで撮影した相手の指や顔の写真から、3D プリンターや AI を用いて偽の指紋などを作って認証を突破する実験もなされています。また本人が寝ている間に、勝手に指を押し当てて認証を突破するという話があります。したがって、生体認証だから、絶対安心と過信しないことが重要です。

ソフトウェアトークンは、専用のアプリを利用するものと、QR コードを使って情報を読み込むものがあり、後者はパスワード管理アプリで一括して管理できる場合もあるので、活用しましょう。

スマートウォッチによっては、スマホのパスワード管理アプリと連携して、手元で ID とパスワードを確認したり、ワンタイムパスワードを発生させたりできる機種もあります。

また、パスワードをネット経由で送信せず、USB セキュリティキーや生体認証を用いて端末内で本人確認をし、認証したという情報だけを送信する FIDO などの方式の採用も推

パスワードを破る手段は色々

総当たり攻撃(ブルートフォース攻撃)

すべての文字列の組み合わせを試す

辞書攻撃(ディクショナリアタック)

パスワードでよく使われる単語を使って試す

リスト型攻撃(アカウントリスト/パスワードリスト攻撃)

名前や ID とパスワードの流出リストを使う

あくまでも代表的なものの例ですが、簡単なパスワードやよく使われるパスワードだったり、使い回しをしていたり、流出したのに放置していると、攻撃者に楽々突破されます。パスワードはしっかり管理しましょう。

(本当は、図のように人力ではなくプログラムなどで自動的に行われます)

進されています。より安全な利用のために、アンテナ高く認証にまつわるセキュリティ情報を収集しましょう。

8.6 二段階認証と二要素認証と多要素認証の安全性

この認証のために用いる要素には右図にあるように、「知っていること」、「持っているもの」、「本人自身の一部」などの種類があり、このうち最初の認証に用いなかった要素と組み合わせて、二要素以上を用いた認証方式を構成することが重要です。複数の要素を使用するものを多要素認証、その中でもとくに2つの要素を使用するものを二要素認証と呼びます。本冊子では、その意味で推奨する認証方式を「二要素以上の多要素認証」という表現をします。

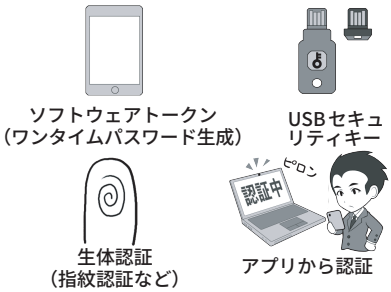
一方、アカウント認証に関する記事などでよく用いられる言葉に「二段階認証」というものがあります。これは、認証のプロセスを二段階に分けて行うものであり、構成する要素とは関係がありません。したがって、二段階認証であっても一要素認証もあれば、一段階認証であっても二要素認証の場合もあり、前者よりは後者の方が安全性が高まります。

また要素のうち、「持っているもの」、「本人自身の一部」は、物理的な存在であるため、実物が必要という点で、安全性が高まります。

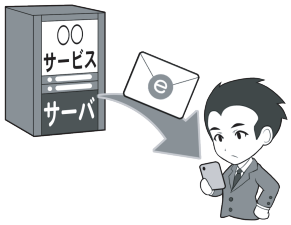
それでも、キャッシュカードが、振り込め詐欺などであっさり奪われたり、多要素認証すら破る「中間者攻撃」も存在したりするため、多要素認証だからそれだけで絶対安全とは限りません。

現時点で推奨できる多要素認証要素

基本的に推奨できるもの



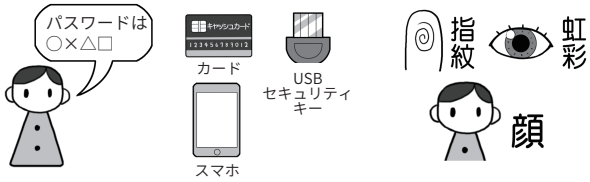
推奨できないもの



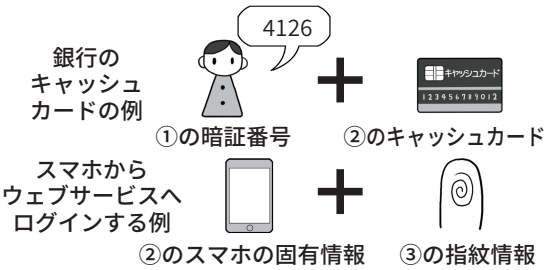
SMSを使ったワンタイムパスワード受信は、海外でSIMハイジャックという攻撃により破られた例があります。また、メールも同様にパスワードを「送信する」をいう点で攻撃の余地が多くなります。

多要素認証の構成要素は？

①知っているもの　②持っているもの　③本人自身に関するもの



多要素認証の組み合わせ例



多要素認証は上記の2つ以上の要素を組み合わせます

一方、二段階認証は、二回認証を行いますが、その要素は多要素とは限らないため、防御力としては弱くなります。

なお、多要素認証のうち、2つの要素だけ用いて認証するものを、「二要素認証」といいます。

指紋認証が破られることも…

極端な例ではありますが、高度なハッキングをしなくても、酔っ払って寝ているあなたの指に押し当てるだけで指紋認証は突破できてしまいます。

指紋認証だから、絶対安心と過信しないようにしましょう。

場合によっては、機器を再起動したり、わざと数回指紋認証を失敗して、強制的に生体認証ができない状態にする対策も検討しましょう。

8.7 パスワードの定期変更は基本は必要なし。ただし流出時は速やかに変更する

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があります。しかし、前出のように十分に複雑で使い回しのないパスワードを設定した上で、実際にパスワードを破られアカウントを乗っ取られたり、サービス側から流出したりした事実がないのなら

ば、基本的にパスワードを変更する必要はありません。

むしろ、パスワードの基準を定めず、定期的な変更のみを要求することで、パスワードが単純化したり、ワンパターン化したり、サービス間で使い回しするようになることの方が問題となります。企業などでパスワードに関するルールを定める場合にも、利用者に対して定期的な変更を求めないようにすることが原則として必要となります。

一方、アカウントが乗っ取られたり、流出の事実を知った場合は速やかにパスワードを変更し、その以降の被害を避けるため原因も特定しましょう。

また、アカウントが完全に乗っ取られてしまったら、ウェブサービスに連絡して復旧しましょう。

一方、自分の使用機器からではなく、ウェブサービスなどの側からパスワード流出が起きた場合は、速やかにパスワードを変更の上、流出の原因となった点の対策が行われたかを確認しましょう。

サービス側からパスワード強制リセットの通知や、再設定のリクエストが来たら、次項の便乗攻撃に注意しつつ、同様に速やかにパスワードを変更しましょう。

8.8 パスワード流出時の便乗攻撃に注意

サービス側から、パスワード再設定の通知がメールなどで送られて来た場合、まずそれが本当にサービス側から送られてきたものかどうか、該当のサービスのウェブサイトやニュースサイトでチェックし、事実の確認をしましょう。サービス側を装ったパスワードリセットの通知は、流出事故に便乗したフィッシング詐欺などのよくある攻撃パターンです。パスワードを奪う攻撃者の罠かもしれません。通知のメールにパスワードリセットのリンクなどが貼られていても、うかつにクリックしたりせず、リセットする場合も直接公式サイトやアプリからしましょう。

なお、ウェブサービスを利用するときは、パスワードが流出した場合に簡単にアカウントを乗っ取られないように、必ず二要素以上の多要素認証を設定しておきましょう。これが提供されないサービスは、セキュリティ意識が低い可能性があるのでそのサービスの利用は再考しましょう。

8.9 適切なパスワードの保管

さて、日常的にインターネットを利用していると、ID とパスワードは無限に増えていきます。どう管理すればよいのでしょう。

スマホのパスワード管理アプリを導入する場合は、ネットにデータを置く「クラウド連携（バックアップ）機能」を安易に利用せず、まずはスマホ内だけで管理する「スタンドアロン」状態で利用できるものを優先しましょう。

利用規約を守り、システムを最新に保っている限りは、スマホのセキュリティは十分に高い設計となっていますし、また、紛失や盗難に遭っても、最新のスマホはデータを暗号化した状態で保存しています

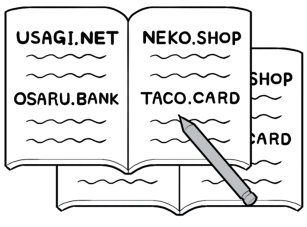
パスワード管理アプリや、同様の

ウェブブラウザにはパスワードを保存しない

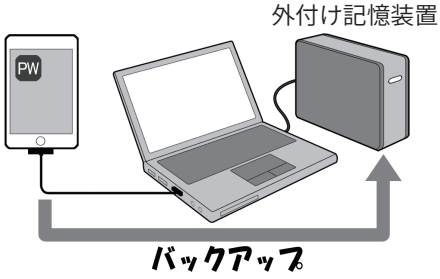
ウェブブラウザにパスワードを保存すると、席を離れた隙に勝手に利用されたり、パソコンをクラッキングされた際に根こそぎ盗まれる可能性があります。

パスワード管理方法の例

一見分かりにくい
紙のノートに二重で



管理アプリのデータは、暗号化した記憶装置にバックアップ



紙のノート二冊に記入したり、スマホのパスワード管理アプリを使って、パソコン経由で暗号化した記憶装置にバックアップする方法があります。紙のノートは一見内容が分からないようにできる専用のパスワードノートも売られています。

機能を持つソフトには「クラウド連携機能」やクラウドを用いた「バックアップ機能」があり、これを利用すると複数端末でパスワード情報を共有できたり、明示的にバックアップ処理をしなくても自動でクラウド上にバックアップデータが作られたりします。

この機能を無条件で推奨しない理由は、「重要な情報が複数箇所に存在すれば、流出する可能性がその分増える」からです。またサービスとして提供されている以上、利用者が意図しない形でサービスが終了してしまうリスクもあります。

加えて、クラウドサービスを利用する場合、他人の手元でデータが保管されますが、利用者には、そのサービスが運用しているシステムのセキュリティレベルの実態を知るがわからないことがあります。

クラウドサービスを利用する場合には上記のリスクを理解して、安全なものを選択する必要があります。

さて、パスワードを記録したスマホも紙のノートも、紛失してしまうと困るのは同じです。いずれの方法を採用した場合でも、その特徴を踏まえてリスクが小さく使いやすい形でバックアップを取ることが重要です。

パスワード管理方法のメリットデメリット

	盗難・紛失対策	ネット経由のセキュリティ	データの管理者
 紙のノート	○ 持ち歩かず自宅などの安全な場所に保管する	○ 攻撃不可	本人
 スマホアプリ	△ 盗難・紛失のリスクが高め。バックアップが必要	△ セキュリティレベルによる	本人
 外付けＨＤＤへバックアップ		○ ただし普段は接続しない	本人
 クラウドサーバにバックアップ		△ サービス側のセキュリティレベルによる	事業者

パスワードの管理方法とバックアップ方法を、１つの表で同列にまとめていますが、一番右列のデータの管理者の項目をよく見て下さい。クラウドサービスを使ったバックアップは便利ではありますが、データの管理者は自分ではなくなります。また、クラウドサービスのセキュリティがどのレベルなのかは、自分では容易に判断できません。

パスワードに関してのみは多少の不便さはあっても、自らの責任において管理するのか、それとも他人の手を借りるのか、クラウドはそれに伴うメリットとデメリットをよく勘案して利用しましょう。

付録01 サイバー攻撃を受けた場合①
～情報関係機関への相談や届け出

会社や団体として、相談したり必要に応じて届け出を行うものとしてはどのようなことを知っておくとよいのでしょうか。

まず、とりあえずサイバー攻撃を受けたらどこに相談したらいいのか。

代表的なものとして一般利用者向けには、IPAによる「情報セキュリティ安心相談窓口」があります。

同名のウェブサイトを検索すると、「良くある質問」や、過去のサイバーセキュリティに関するレポートなどが掲示されているので、一通り目を通し、それでも解決しない場合は、電話やメールで問合せしてみるとよいでしょう。

企業組織向けには「サイバーセキュリティ相談窓口」があります。

各種インシデント発生時の初動対応に関する相談や、標的型サイバー攻撃に関する相談、その他の情報セキュリティに関する一般的な相談が可能です。

それとは別に、義務ではありませんが、「ウイルスの届け出」、「不正アクセスの届け出」を受け付けているので、可能であれば届け出ましょう。

そうすることで他の人が攻撃に遭うのを避けることが可能になります。

地域の商工会議所がサイバー攻撃対応支援サービスの一環として、有料の相談窓口を設けている場合もあります。

なお業種によって、例えば医療機関でのサイバー攻撃に関しては、厚生労働省が、医政局特定医薬品開発支援・医療情報担当参事官室で連絡を受け付けています。

情報セキュリティ10大脅威

https://www.ipa.go.jp/security/vuln/10threats.html
※脆弱性対策（IPA公開資料一覧ページ）https://www.ipa.go.jp/security/vuln/index.html

ランサムウェア対策特設ページ

https://www.ipa.go.jp/security/anshin/ransom_tokusetsu.html

IPA情報セキュリティ安心相談窓口(個人向け)

URL	https://www.ipa.go.jp/security/anshin/about.html
電話での相談	03-5978-7509 （受付時間 10:00～12:00、13:30～17:00、土日祝日・年末年始は除く）
メールでの相談	anshin@ipa.go.jp
FAXでの相談	03-5978-7518
郵送での相談	〒113-6591 東京都文京区本駒込2-28-8 文京グリーンコート センターオフィス18階 IPAセキュリティセンター 安心相談窓口

IPAサイバーセキュリティ相談窓口(企業組織向け)

URL	https://www.ipa.go.jp/security/support/soudan.html
メールでの相談	cs-support@ipa.go.jp

また、IPAでは、その年のサイバーセキュリティ上の懸念される脅威を「情報セキュリティ10 大脅威」として公開しています。

個人編と組織編に分けて公表されており、脅威の内容に加えて、参考事例や注意するポイントがまとまった内容となっています。

さらに、組織を狙った脅威として急激に増えているランサムウェアに関しては、「ランサムウェア対策特設ページ」が用意されています。

万が一、企業や組織でランサムウェアの被害に遭った場合、まずこのページをご覧いただき、迅速かつ正確な対応を進めていきましょう。

IPA 安心相談窓口で対応出来ない例

なお、IPA 安心相談窓口では、下記のような相談は受け付けていません。

- 直接来訪しての相談や面談
- 法的解釈に関する相談
- 電磁波や電波に関する不安・苦情
- インターネットサービスの品質や役務不履行に関する相談
- 契約・支払い方法に関する相談
- 個別の依頼に基づく端末やログの調査、マルウェアの解析、その他調査行為全般の依頼
- 特定の製品やサービスの紹介またはそれらに対する良否の質問
- 他組織への連絡や通報などの仲介
- 犯罪者の検挙、事件捜査の要望

一方、IPA ではなく他の機関が開設している窓口で対応出来る場合もあります。それぞれの窓口の受け付ける事柄を、ウェブサイトなどでよく確認してご相談ください。

●サービス提供または購入などの契約に関するトラブルで困っている場合
消費者ホットライン（消費者庁）
https://www.caa.go.jp/policies/policy/local_cooperation/local_consumer_administration/hotline/

●国民生活センター
https://www.kokusen.go.jp/

●法的トラブルの相談をしたい場合
法テラス
https://www.houterasu.or.jp/

●インターネット上での違法・有害情報に関し相談したい場合
違法・有害情報相談センター
https://ihaho.jp/

●不正コピーや違法アップロードを見かけた場合
社団法人 コンピュータソフトウェア著作権協会不正コピー情報受付
https://www2.accsjp.or.jp/piracy/

●インターネット上の違法情報を通報したい場合
インターネット・ホットラインセンター
https://www.internethotline.jp/

●迷惑メールの受信に関して困っている場合
財団法人 日本データ通信協会迷惑メール相談センター
https://www.dekyo.or.jp/soudan/ihan/

●インターネットに繋がらないなどのトラブルで困っている場合
利用プロバイダまたはパソコンのメーカー・購入店の各サポート窓口

IPA「他の機関が開設している相談窓口等」より
https://www.ipa.go.jp/security/anshin/external.html

付録02 サイバー攻撃を受けた場合②
～警察機関への相談や届け出

警察庁では、サイバー事案に関す通報、相談及び情報提供の全国統一オンライン受付窓口を設置しています。

この窓口からはサイバー事案に関する

〇通報(都道府県警察に対し、サイバー事案に関する通報を行うもの。)
※被害に遭った具体的な事実の通知を伴う場合

〇相談(都道府県警察に対し、サイバー事案に関するアドバイスを求めるもの。)

〇情報提供(都道府県警察に対し、サイバー事案に関する情報を提供するもの。)

を行うことができます。

下記リンクでは、「よくある相談事例と対応方法」についても紹介しています。

通報・相談をする前に解決できる内容があるかもしれませんので、ご参考にしてください。

爆破予告、殺人予告、自殺予告等の人命に関わる事案は最寄りの警察署に通報(緊急を要するものは１１０番)してください。

また、被害届を出される場合は、最寄りの警察署等に連絡をお願いします。

サイバー事案に関する相談窓口	https://www.npa.go.jp/bureau/cyber/soudan.html

NISC関連ウェブサイト、SNS一覧

■ 内閣官房内閣サイバーセキュリティセンター(NISC)公式ウェブサイト

https://www.nisc.go.jp/
日本政府のサイバー政策の策定や政府機関へのサイバー攻撃の検知と調査を行っている機関。国民へのサイバーセキュリティ意識の啓発も行う。通称「NISC」。

■ みんなで使おうサイバーセキュリティ・ポータルサイト

https://security-portal.nisc.go.jp/
NISCが運営する、サイバーセキュリティ関連の情報を発信する普及啓発用サイト。本ハンドブックの配布も行っている。

NISCのSNSによる情報発信

■ X(旧Twitter)
内閣サイバー(注意・警戒情報)

https://x.com/nisc_forecast
フィッシング詐欺・マルウェアなどの注意喚起情報やソフトウェアの更新情報を発信している。

■ X(旧Twitter)
内閣サイバーセキュリティセンター公式アカウント

https://x.com/cas_nisc
NISCの取組やサイバーセキュリティに関連する情報を発信している。

■ Facebook

https://www.facebook.com/nisc.jp/
NISCの活動の紹介や、サイバーセキュリティに関する情報を発信している。

我が家のスマホ利用のルール

(保護者の名前_____)様

私は、以下の約束を守ってスマホを使います。もし、約束を破った場合、指定された期間(_____)、スマホを返します。この約束は、 ____年____月____日 ～ ____年____月____日までの 1年間を期間とし、1年経ったら見直しをお願いします。

A. ルールを守る

- □ 歩きスマホや自転車運転中のスマホ、その他禁止されている場所でスマホの使用はしない。
- □ 学校でのルールを守る。授業中はスマホを見ない。
- □ 写真撮影についてルールを守る。撮影してはいけない場所での撮影や、勝手に人の写真を撮ったりしない。
- □ 食事中や入浴中はスマホを使わない。

B. お金や健康

- □ 使い過ぎに注意する。使う時間は、____:____～____:____まで。
- □ それ以外でどうしても使う必要がある場合は、あらかじめ相談する。
- □ スマホの利用料を払ってもらっていることを理解し、課金が発生するサービスを利用する場合は、承諾をもらってから使う。その場合も、上限と定められた金額を守る。

我が家のスマホ利用のルール

C. ネットの利用

☐ フィルタリングが自分を守るために設定されていることを理解する。勝手に解除したりせず、必要な場合は、予 め相談する。

☐ だらだらスマホはせず、時間を決めてネットを見る。

☐ 違法なサイトで、音楽、アニメ、漫画を見ない。

☐ あやしいサイトやリンクは見ないし、開かない。

D. SNS の利用

☐ ネットで知り合った人と直接会わない。また、写真を送るように頼まれても写真を送らない。困ったら相談する。

☐ ネットは誰が見るか分からないことをきちんと理解した上で発言する。また、知らない人に見られたら困る内容をアップしない。

☐ 自分が言われて嫌なことは人に対しても言わない。

この条件でのスマホの利用を許し、それぞれ 1 通ずつ保管します。

年　月　日　こども：＿＿＿＿＿＿＿＿ ㊞

保護者：＿＿＿＿＿＿＿＿ ㊞

内閣官房内閣サイバーセキュリティセンター (NISC)ウェブサイト：https://www.nisc.go.jp/
NISC「みんなで使おうサイバーセキュリティ・ポータルサイト」：https://security-portal.nisc.go.jp/
内閣サイバーセキュリティセンター 公式X: @cas_nisc
内閣サイバー（注意・警戒情報）X:@nisc_forecast
NISC Facebookページ: https://www.facebook.com/nisc.jp

インターネットの安全（あんぜん）・安心（あんしん）ハンドブック

一般利用者向け 抜粋版

2023年3月1日　Ver.5.00発行
2025年3月11日　Ver.5.10発行

NISC 内閣サイバーセキュリティセンター
National center of Incident readiness and Strategy for Cybersecurity

制作・著作　内閣官房　内閣サイバーセキュリティセンター (NISC)
協力　警察庁　総務省　経済産業省　独立行政法人情報処理推進機構(IPA)
改訂検討会メンバー：猪俣 敦夫（主査：大阪大学 教授, CISO）
上沼 紫野（LM虎ノ門南法律事務所 弁護士　一般社団法人 安心ネットづくり促進協議会 理事）
加賀谷 伸一郎（独立行政法人情報処理推進機構（IPA）セキュリティセンター 普及啓発・振興部 副部長）
酒井 正幸（特定非営利活動法人日本ネットワークセキュリティ協会（JNSA）　中小企業支援施策ワーキンググループサブリーダー）
櫻澤 健一（一般財団法人 日本サイバー犯罪対策センター（JC3）業務執行理事）
松下 孝太郎（東京情報大学 総合情報学部 総合情報学科 教授）
宮本 久仁男（株式会社NTT データグループ技術革新統括本部Cloud ＆ Infrastructure技術部 情報セキュリティ推進室NTTDATA-CERTセキュリティマスター）