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

知る・守る・続ける
サイバーセキュリティ普及啓発

ネットワークビギナーのための
情報セキュリティハンドブック
Ver 4.20

協力
総務省 経済産業省 IPA 独立行政法人 情報処理推進機構

CC BY NC SA

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

知る・守る・続ける
サイバーセキュリティ普及啓発

協力
総務省 経済産業省 IPA 独立行政法人 情報処理推進機構

ネットワークビギナーのための
情報セキュリティハンドブック
Ver 4.20

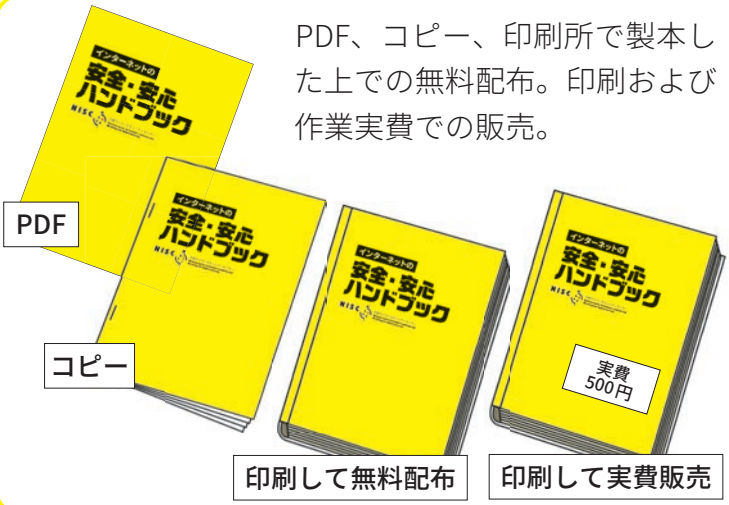
CC BY NC SA

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

「インターネットの安全・安心ハンドブック」は、下記のようにご活用いただけます。

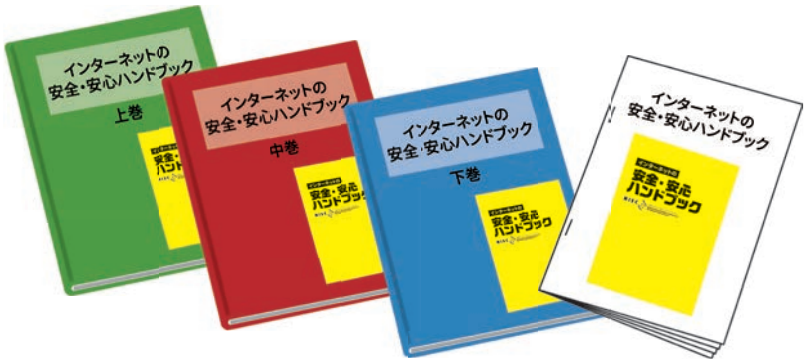
本冊子の著作権は内閣サイバーセキュリティセンター(NISC)に留保されますが、内容に改変を加えないことを条件に、多様な形でご活用いただくことができます。

※製本用印刷データが必要な場合は下記までお問い合わせください
security_awareness@cyber.go.jp
※合本やプリンタでの印刷にはNISCウェブサイト掲載のPDF版をお使いください



PDF、コピー、印刷所で製本した上での無料配布。印刷および作業実費での販売。

ページ単位、イラスト単位での利用、配布(ネット配布含む)



分割して配布、必要部分だけを抜粋して配布

ウェブサイトにダウンロードサイトのリンクを設置※

使用する団体名を表紙に入れて利用

自団体のセキュリティ資料と合体しての配布

※ダウンロードサイトURL
https://www.nisc.go.jp/security-site/handbook/index.html

インターネットの安全・安心ハンドブック　活用法

● 学校の授業で

「インターネットの安全・安心ハンドブック」は、中高生の方とその先生方に、セキュリティ意識を高めるための教材として使っていただけるように作成されています。

第1章の基本のセキュリティを踏まえつつ、第2章のサイバー攻撃に遭うとどういったことが起こるのか、そして、第3章のセキュリティを守るための各技術をマスターして、それをさらに、まわりの方やご家族にも広めてください。

● ご家庭で

ご家庭でのセキュリティの守り方については、各章に記述がありますので、ぜひご参照ください。

また、第5章では、子ども達がSNSを気軽に利用すると、どういったトラブルが遭遇するのか、SNSをとおして見知らぬ人と友だちになると、どういったことが起こるのかについて触れていますので、ご家族で一緒にお読みになってください。

子ども達だけでなく、お年寄りを守るためのテクノロジーの使い方のアイデアも掲載していますので、ご活用ください。

● 災害時に備えて

第5章の家族を守るセクションには、災害時に関する記述があります。大規模災害時に、どうやって情報を活用して身を守るのか、デジタル世代のサバイバル技術についての知識を得た上で、「もし災害が起こったらどうするか」、ご家族で計画を立ててみてください。

学校の授業で

P25「第1章．基本のセキュリティ～ステップバイステップでセキュリティを固めよう～」

P45「第2章．サイバー攻撃にあうと、どうなるの？最新の攻撃の手口を知ろう」

P55「第3章．パスワード・Wi-Fi・ウェブ・メールのセキュリティを理解して、インターネットを安全に使おう」

P113「第5章．SNSやインターネット関連の犯罪やトラブルから、自分や家族を守ろう。災害に備えよう」

ご家庭で

P114「5-1-1. SNSやネットの楽しみと気をつけること」

P124「5-2-1. アニメ・マンガ・音楽の違法なシェア。パクリなどの著作権侵害」

災害時に備えて

P138「5-5. 大災害やテロに備える」

P141「5-5-4. 徒歩帰宅、海外での災害やテロに備えて」

目次

※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、様々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。

はじめに～サイバーセキュリティは「公衆衛生」の時代に～

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。我々は日本の政府機関で、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、「ウイルス」という言葉をご存じですか？病気の原因としてのウイルスを思い浮かべましたか？それとも「コンピュータウイルス」？

現実の世界では、ウイルスに感染して病気にかかった人がいると、病院に行かせたり、場合によっては隔離して適切な治療をし、ほかの人にうつらないようにもします。そうしないと、家庭や職場の人たちみんなが病気になって、最後は社会全体の活動に大きな問題が発生してしまうからです。

それを知っているから私たちは、マスクをし、手洗いをし、ワクチンを接種し、上下水道を整備し、家の中や町をきれいにして「公衆衛生」に努めるわけです。

※NISC特務第１チームは架空の団体です。

今、日本の街角が綺麗で、病気による大災害が発生しないのも、国民全員が長年取り組んだ「公衆衛生」意識と活動の賜物なのです。

さて、コンピュータやインターネットの世界にも、「ウイルス」が存在します。ウイルスだけでなく細菌や、原虫、寄生虫に相当するトロイの木馬やワームといったものもありますし、また、生活の安全を脅かす、悪意をもった人たちが暗躍しています。それは、さながら、社会システムが未発達で公衆衛生意識が低く、治療が未成熟で知識も十分ではない、はるか昔の時代のようです。

そして、そのインターネットの世界は、今や私たちの現実の世界と複雑に絡み合っていて、インターネットで発生するトラブルは、現実世界の私たちの生活にまで、多大な影響を及ぼしつつあるのです。

いま私たちに求められているのは、この新しい世界の状況をきちんと理解して、そこを安全に利用し、楽しめる生活空間とするために、インターネットの世界の公衆衛生の意識や防犯意識を確立して、行動に移すことです。

その活動は、私たちだけではできません。国民全員参加で初めて成し遂げることができるのです。さぁ、その第一歩を始めましょう。

一人ひとりがサイバーセキュリティを担うことで、安全なネット社会をつくることができます

ネットにいる悪意を持った人たちは、みなさんの手の中にあるスマホや家にあるパソコンを狙ってきます。しかし世の中にあるすべてのスマホやパソコンを守るためには工夫がいります。街の安全が防犯活動や、それによって醸成される防犯意識、あるいはなにかあったときに、みんなが助け合うという意志によって守られるように、私たちと一緒にネットを守って下さい。

Black Hat the Cracker

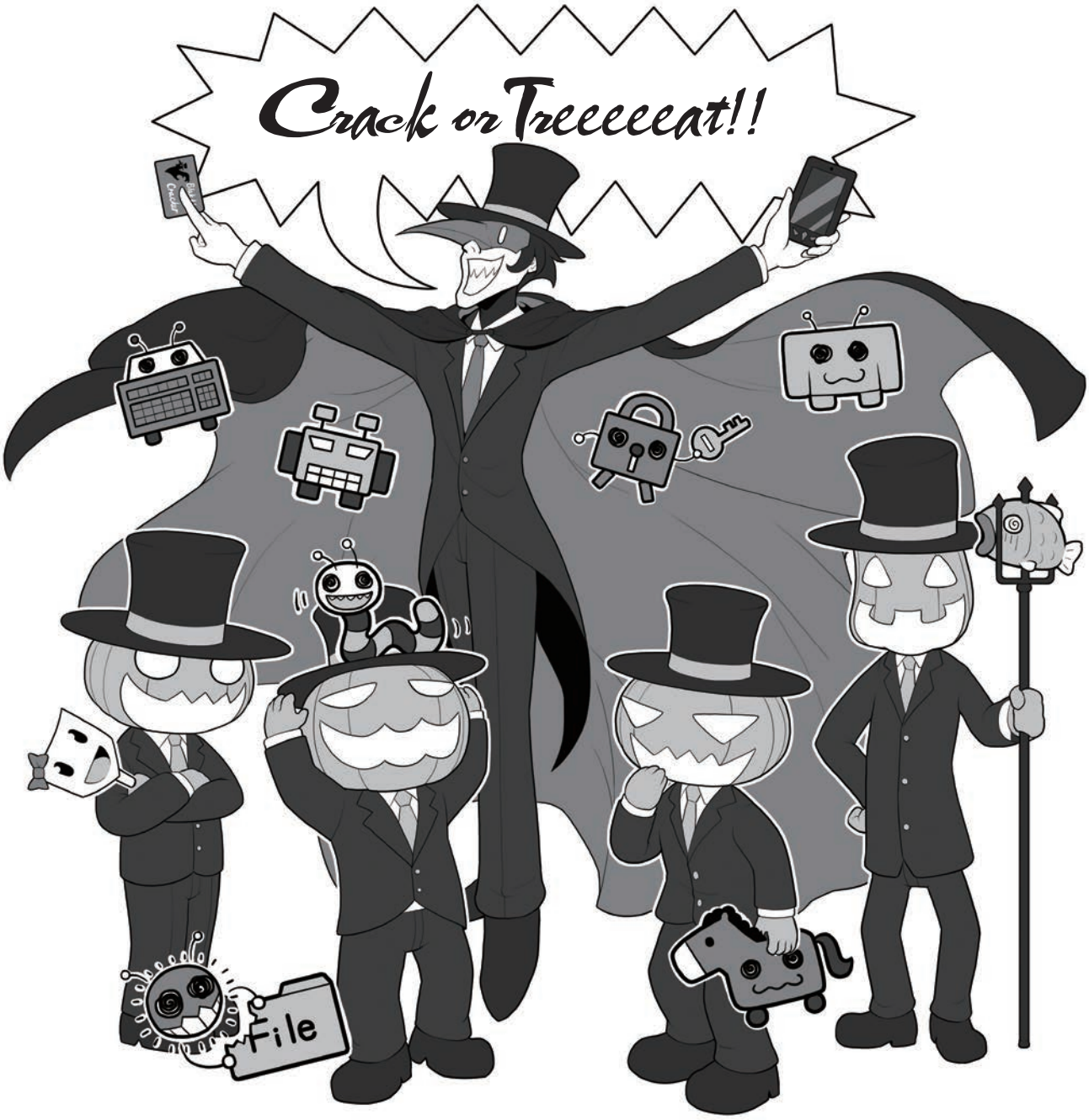
サイバー空間(インターネット)には、悪意をもってこれを利用し、自らの利益のためには平気で他人の情報や財産を奪い、また、サイバー攻撃を通じて自己誇示するといった、様々な悪事を働く者がいます。

この本では、その者たちの仮の姿として、「ブラックハット・ザ・クラッカー」と、その手下たち「ブラックパンプキン」、そして、様々な「マルウェア」が登場します。

ときに、彼らが普通の人の仮面をかぶったり、あるいは普通の人々が彼らの仮面をかぶったりして、悪事を働くこともあります。

解説のイラストでは、そのあたりもきちんと描き分けていきたいと思いますので、ぜひつぶさに見ていて下さいね。

彼(彼女?)の正式名称「ブラックハット・ザ・クラッカー」の由来については、「コラム：攻撃者とハッカーとクラッカー」の項目でお話ししましょう。



プロローグ

サイバー攻撃ってなに？

サイバー攻撃という言葉を聞いて、なにを思い浮かべますか？
どんなことが起こるの？誰がやっているの？なにを狙っているの？
まず、サイバー攻撃とはどのようなものなのか、それを知ってもらいましょう。

悪意を持った人たちは、いったいなにを狙っているの？

1 サイバー攻撃のイメージ

1 サイバー攻撃って誰がやっているの？どうするの？

サイバー攻撃は、誰がなんの目的でやっているのでしょう。

軍事スパイや産業スパイ？ それともハッカー？

いわゆるスパイの目的は、軍事機密や先進の研究内容など、自国や企業にとって有益な情報の入手です。それに対し、私たちが普段遭遇するサイバー攻撃は、主として個人情報や金銭など、攻撃する者にとって利益が得られることにつながることを目的としています。

スパイは、目標の達成が絶対条件であり、ありとあらゆる手段で攻撃を行うため、どんなにセキュリティが厳重でも侵入してきます。それは、やっかいな存在で、現状完璧には防ぐことができません。

一方、利益目的のサイバー攻撃は、攻撃する者にとってはビジネスとしての性格を帯びています。例えば、「ここはセキュリティがしっかりしているので手間がかかる(≒費用がかかる)のでやめよう」「ここなら手間がかからない(≒安くすむ)からここから盗もう」というように、攻撃しやすい方に流れる傾向があり、セキュリティレベルを高めることで、ある程度攻撃を受けにくくすることができるのです。完璧に防ぐことは難しくても、努力をすれば被害に遭う確率を減らせると考えていいでしょう。

サイバー攻撃への対処は、ヒーローが登場する勧善懲悪のアニメのように、きっちり解決をしたり、あるいは0と1のデジタルのようにかっちりと防いだりすることはできません。まずは安全を確保する手段を、石垣を築くように地道に積み上げる必要があるのです。

これから、私たちが説明していくサイバーセキュリティに関するお話は、この考え方に沿っていることを覚えておいてくださいね。

コラム：攻撃者とハッカーとクラッカー

ハッカー

そもそも、「ハッカー」とはコンピュータの知識と技術に精通した人を尊敬して呼ぶ名前で、悪事を働く人という意味ではありません。

その用語を自分で使うとき、あるいは報道など見るとき、どのような意味で使われているのかを気にかけましょう。

専門ではない新聞や雑誌、テレビでは、サイバー攻撃を行う者をよく「ハッカー」と称しがちです。しかし、実はこの呼び方はあまり正しくありません。

ハッカーとは、もともとはコンピュータに精通しその方面の高い知識と技術を持つ人を指すある種の尊称であり、イコール悪事を行う攻撃者ではありません。そして、彼等がその技術を駆使して行う作業を「ハッキング」や単に「ハック」といいますが、これも本来は悪事とイコールではありません。

ただし、こういった知識や技術をもって悪事を行う人も存在するため、それらを善意の人と区別する意味で、「ブラックハットハッカー」や「ブラックハッカー」、あるいは防御しているものを割って侵入することを意味する「クラッカー（cracker）」や攻撃者の意味を持つ「アタッカー（attacker）」と呼ぶのです。一方、日本語で「ハッカー」と安易に呼ばない場合は「悪玉ハッカー」や「悪意のハッカー」ともいわれます。

逆に、善意に基づいて高い知識や技術を使う人を「ホワイトハットハッカー」や「ホワイトハット」「ホワイトハッカー」といい、日本語では、「善玉ハッカー」や「正義のハッカー」と呼びます。

本書では、この本来の意味に基づいた用語でお話を進めますので、みなさんにもぜひ覚えていただき、日常の生活でも正しい名称が広く用いられるようご協力ください。

コラム：攻撃者が使う武器「マルウェア」

● どんな種類があるの？

先ほどのハッカーやクラッカーの例と同じように、今ひとつ正しく用いられていないのが、「コンピュータウイルス」や、単に「ウイルス」という用語です。

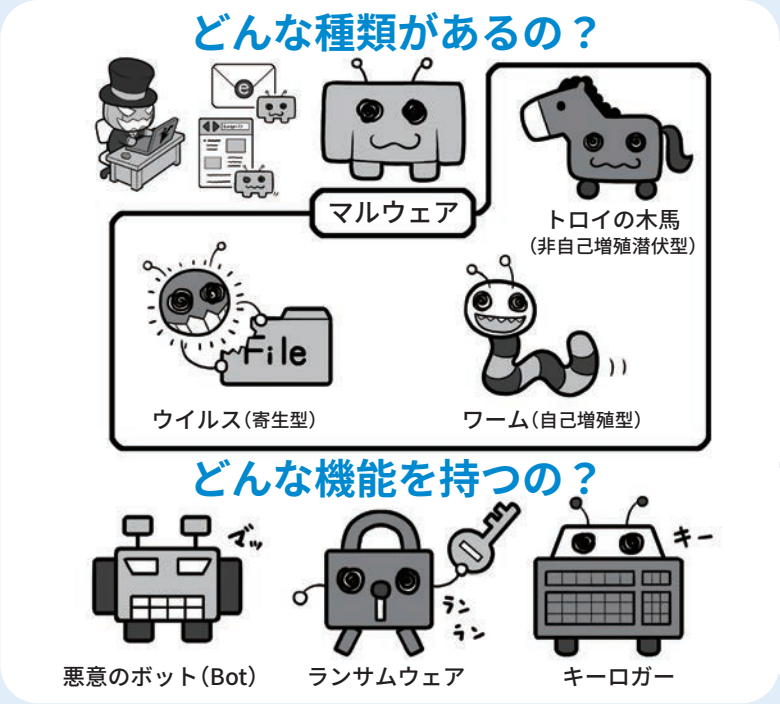
攻撃者がサイバー攻撃を行う場合、相手のコンピュータをなんらかの悪意のプログラムに感染させ、これをコントロールする方法がよく用いられます。この攻撃に使われるプログラムをまとめて「ウイルス」と呼びがちです。

しかし、攻撃用プログラムは本来「マルウェア」もしくは「不正なプログラム」と呼ぶのが正しく、「ウイルス」とはそのマルウェアの中の一種で、コンピュータ上のファイルが感染し、そのファイルに寄生して活動するタイプのものを指す限定的な名称なのです。

現実世界に例えるなら、「マルウェア」とは病気を起こす原因の総称「病原体」にあたり、「病原体」の一種で細胞に寄生しないと増殖できないものを「ウイルス」と呼ぶのと同様です。

そして、病原体にはウイルスのほかにも、単独で存在することができる細菌、原虫や寄生虫などがあります。マルウェアにも同様に、独立していて非自己増殖型の「トロイの木馬」と呼ばれるものや、独立型かつ自己増殖型の「ワーム」があります。

また、機能による分類としては「ボット」「ランサムウェア」「キーロガー」などの呼び方もあります。これは、病原体の行動形態を表す症状の名前のようなものです。



ただ、一般に広がった「ウイルスという言葉がマルウェアと同じ意味で使われる」事実もあるため、その整合性を取るために「広義のウイルス」といった言い方も存在します。

みなさんには、この部分もぜひ覚えていただいて、正しい呼び方を広めてもらうと同時に、新聞、雑誌やテレビで「ウイルス」と使われている時は、それが「広義のウイルス＝マルウェアの意味」なのか「狭義のウイルス＝ファイルに寄生する感染プログラム」なのかを文脈から読み取って、正しく理解してもらえるとうれしく思います。

● どのような機能を持つものがあるの？

マルウェアを機能別に分けると、このようなものがあります。

- **悪意のボット（Bot）**

ボットとはRobotの略で、悪意のものは感染すると攻撃者にコンピュータが乗っ取られ、別のコンピュータへの攻撃などに使われる。

- **ランサムウェア**

感染すると、コンピュータ上のファイルが暗号化された上で、攻撃者から元に戻すための身代金を要求される。

- **キーロガー**

比較的古いマルウェアで、感染するとキーボードの入力を記録して攻撃者に送信する。攻撃者はこれを利用してパスワードなどを盗む。

また、例えば、「トロイの木馬」は、最初にコンピュータに侵入する時は害がないようなふりをして、侵入したらマルウェアの本性を現したり、外部からボットやランサムウェアを呼びこんだりして悪事を働き始める特性を持ちます。これは、「トロイアの木馬」という神話から取った名称

ですね。

● どんなものが感染したり、感染させたり、悪さをするようになるの？

マルウェアに感染するものといえば、おそらく真っ先にパーソナルコンピュータ(以下パソコン)やスマートフォン(以下スマホ)、タブレットなどを想像するでしょう。

そしてマルウェアは「コンピュータが感染する」悪意のプログラムです。

しかし、実際には、ご家庭で使っている無線LAN(Wi-Fi)アクセスルータ、ネットワークプリンタ、ネットワークカメラ、スマートテレビ、スマート冷蔵庫、はてはPOSレジなども感染するそうです。こういった機器はコンピュータではないのになんで感染するのでしょうか。

この「コンピュータが感染する」と「コンピュータじゃないものまで感染している」ことの矛盾を解く鍵は、「現代の電子機器は、コンピュータに見えないものでも、実はコンピュータが内蔵されている」というところにあります。

こういった機器が、インターネットにつながりデータをやりとりする以上、マルウェアに感染する可能性があるわけです。

特に、IoT(Internet of Things)「モノのインターネット」の時代が訪れ、私たちの周りに存在する様々な電子機器がコンピュータ化し、インターネットにつながるようになると、今より多数の機器が感染する可能性があります。

しかし、こういった悪意の攻撃によってマルウェアに感染してしまうかもしれないことよりも、もっと深刻な問題があります。それは、人間の心の隙を突いたサイバー攻撃です。

機器を強制的にマルウェアに感染させるためには、セキュリティホール(脆弱性)と呼ばれるプログラム上の弱点が必要です。セキュリティホールがあるということは、家の鍵が壊れているようなものです。しかし、日々セキュリティのアップデート(修正)が行われ、大抵のセキュリティホールはすぐにふさがれます。

そういった場合でも、持ち主をだまして自らマルウェアをインストールさせれば、外から無理矢理侵入せずとも、内側から簡単に悪事を働くことができてしまいます。

これを実現するのが後ほど説明する「標的型(電子)メール」など、心の隙を突くタイプの攻撃です。問題はこの心の隙が、コンピュータのセキュリティホールのように簡単にはふさげないことにあります。セキュリティ意識は、本人が必要性を認識しないと向上しないからです。

どんなにサイバー攻撃に対する防御を固めても、人間をだます攻撃手法はいくつも存在し、こちらはなかなか防げない。このこともよく知ってください。

そして、被害者が友人や職場の仲間に次々に感染を広げていって、様々な機器が持ち主の知らぬところで乗っ取られ、勝手に攻撃者によるサイバー攻撃に使われることもあるのです。

そう、被害者であるはずのあなたが、いつの間にか攻撃に参加させられ、時に加害者的立場になることもあるのです。

まずは、防ぐための知識を得て行動をおこしましょう。

2 サイバー攻撃の例

では、先ほど紹介したサイバー攻撃が、実際にはどのように行われるのか、いくつかの例をあげて見てみましょう。

攻撃者はマルウェアを添付した電子メール(以下メール)をあなたに送ったり、マルウェアを仕込んだウェブサイト(ホームページ)に誘導したりして、あなたのパソコンなどをマルウェアに感染させます。そして、写真や重要情報を盗んだり、アカウントを乗っ取って勝手に物を購入したりもします。

また、メールやSMS(ショートメッセージ)を使って偽の銀行サイトに誘導し、お金を不正送金させる「フィッシング詐欺」などを行うこともあります。

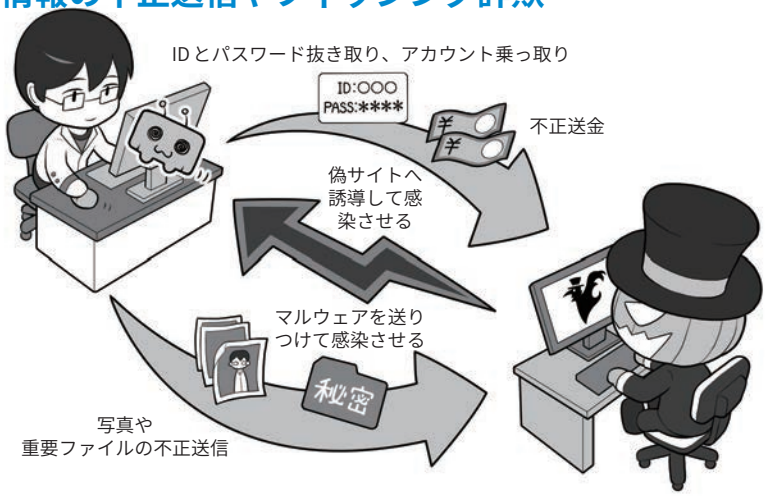
もっと直接的に、あなたにお金を要求することもあります。「ランサムウェア」に感染させ、あなたのパソコンなどのデータを勝手に暗号化し、「暗号化を解除してほしければ身代金を払え」と脅迫してくるのです。

ほかにも、感染させたパソコンや機器を、ボットネットと呼ばれるネット上の不正な仕組みに勝手に組み込み、所有者が知らないうちに、どこかのウェブサーバに大量のアクセス要求を送って反応できなくする、「DDoS攻撃*1」などに利用することもあります。持ち主は知らないうちに攻撃に協力してしまうことになるわけです。

攻撃者はこの攻撃用の不正な仕組みを時間制で貸し出して、対価としてお金を稼ぐこともあります。

*1 DDoS攻撃：Distributed Denial of Service attackの略。多数の機器からサーバなどに攻撃をしかけ通信能力を超えさせ使えない状態にする

情報の不正送信やフィッシング詐欺

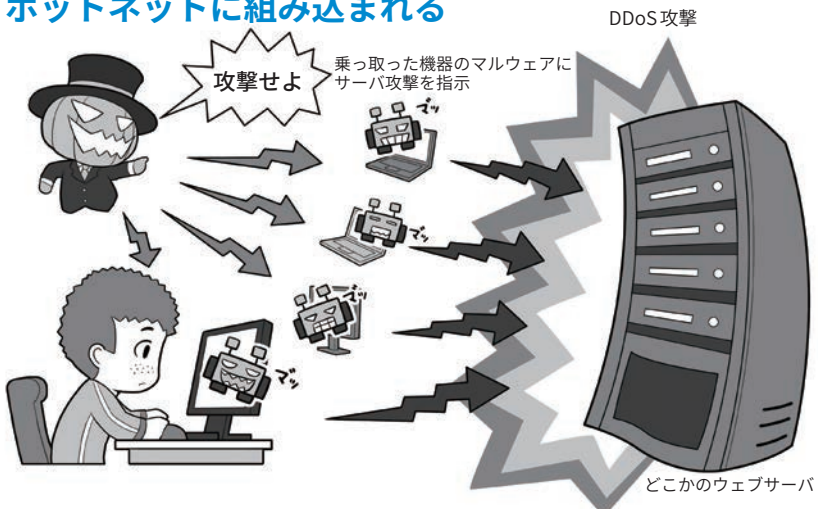


攻撃者は、あなたから情報やお金を盗むために、マルウェアに感染させて重要ファイルを不正に送信させたり、偽のメールで偽の銀行サイトなどに誘導する「フィッシング詐欺」を行って不正送金させたりします。どういう方法でだまされてしまうのか、一度調べてみましょう。

ランサムウェアで身代金要求

ランサムウェアに感染すると、パソコンなどのファイルが暗号化され、解除するために身代金を要求されます。しかし、身代金を払っても解除するキーをもらえるとは限りません。普段からシステムやデータのバックアップを取って、元の状態に戻せるように備えましょう。どうやって侵入されるのか、実例の記事を探して学んでみましょう。

ボットネットに組み込まれる



所有するIT機器が悪意のボット用マルウェアに感染すると、攻撃者が管理する攻撃用の仕組みであるボットネットに接続され、あなたが知らないところでサイバー攻撃に参加させられることになります。気づかずに加害者的立場になってしまうかもしれません。

3 サイバー関連の犯罪やトラブル

サイバー攻撃のほかにも、ネットを使った犯罪やトラブルはたくさんあります。

例えば、「なりすましや誘拐・略取」。SNSなどで未成年と同じ年齢や性別になりすまして近づき、その上で相手を誘い出して誘拐や略取などに及ぶケース。あるいはSNSで家出などをした子どもの書き込みを見付けて、自宅などに連れ込むケースもあります。

また、同じようにネットで未成年のふりをして近づき、相手の警戒心を和らげて、「私も送るからあなたも送って」と裸の写真を要求して、入手したらその写真を使って相手を脅迫するケースもあります。

このような、子どもたちが自分自身の裸の写真を撮り、交換し合うことによって起こる被害を「自画撮り被害(セクスティング)」といいます。一度自分のスマホなどに記録された写真は、誰かに渡さなくても流出の危険がありますし、相手に渡してしまえばネットに流され、その後ずっと自分を苦しめ続ける可能性があることを考えなくてはいけません。これは、子どもに限らず、交際していた相手が別れたことの腹いせに、裸の画像をインターネットに流す犯罪「リベンジポルノ」としても問題になっています。

そのほかにもSNSへの投稿やSNSのグループチャットで、誰かの悪口をいったりする「ネットいじめ」は、やっている本人たちは軽い気持ちでも、時に相手を激しく追い込んで悲劇を招いたりするので、現実世界のいじめ同様、絶対にやってはいけないことです。

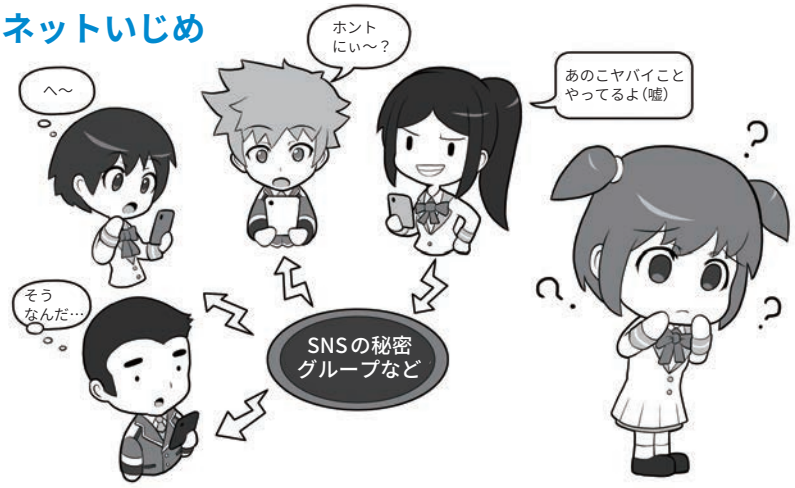
なりすましや誘拐・略取(連れ去り)

SNSなどであなたに近寄るために、年齢や性別を偽っている人がいます。同じ歳や性別になりすまし油断させて近づき、誘い出して誘拐や略取に及ぶかもしれません。基本的に実際に会ったことがない人がSNSで近づいてきたら、「そういう人かもしれない」と考え友だちにならないように！

自画撮り被害(セクスティング)

「自画撮り被害(セクスティング)」は、裸の写真などを送ってしまうことで起こります。もしその相手が写真をネットで売ったり、あなたを脅すためにやっていたりしたらどうでしょう。一度ネットに流出した写真は完全に消し去ることは困難です。絶対にやってはいけません。

ネットいじめ



現実のいじめはもちろんのこと、ネットを使ったいじめもやってはいけません。ネットはみんなの未来を創るためのものであって、苦しめるためのものにしてはいけないのです。

4 一見サイバー攻撃に見えない「ソーシャルエンジニアリング」攻撃

さて、「サイバー攻撃」ではなく一般的な犯罪で、みなさんがよく耳にするものにはなにがあるでしょう。たぶん「オレオレ詐欺」「振り込め詐欺」など、人をだましてお金を巻き上げる「特殊詐欺」があげられると思います。

関係機関が常に注意喚起をしていますが、未だに多くの方が被害に遭っています。

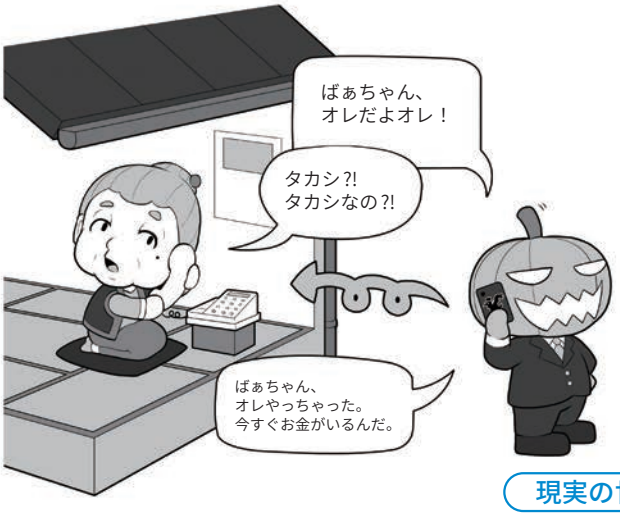
パソコンに例えると、セキュリティホールを必死に埋めようとしているのになかなか埋まらず、目の前で次々とサイバー攻撃が行われてしまっているような状況です。

それが終わらない理由は、人間の「心の隙」というセキュリティホールを突いた攻撃だからであり、人間のセキュリティホールは対策が難しいためです。そして、サイバー攻撃でも、この人間の心の隙を突くものがたくさんあります。

例えば、大企業ですらだまされる「ビジネスメール詐欺(BEC)」の発端になる「標的型メール」。送りつける相手をよく調査・分析した上で、本人宛かつあたかも仕事の関係のメールに見える文面に、マルウェアなどを添付して送り付け、本人がうっかりファイルを開くと感染させられてしまうのです。

こういった攻撃による被害を軽減するためには、多くの人々がサイバーセキュリティ知識を持つことに加えて、「心の隙」についても詳しくなり、サイバー攻撃だけでなく、こういったハイブリッドな攻撃に関する危機意識が、みんなの心の中に常識として根付くようになることが重要なのです。

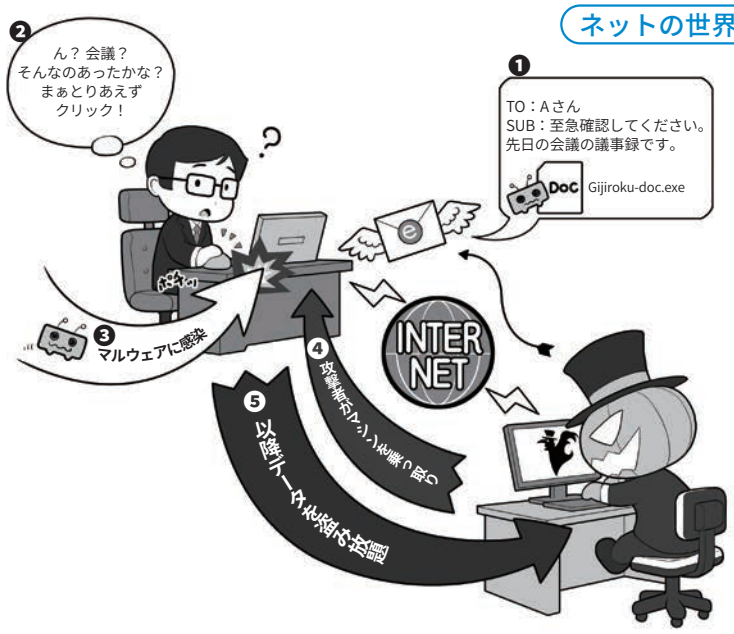
「ソーシャルエンジニアリング」は現実でもネットでも「心の隙」を突いてだます



現実の世界

この2つの共通点は人間の「心の隙」を突いた点

ネットの世界



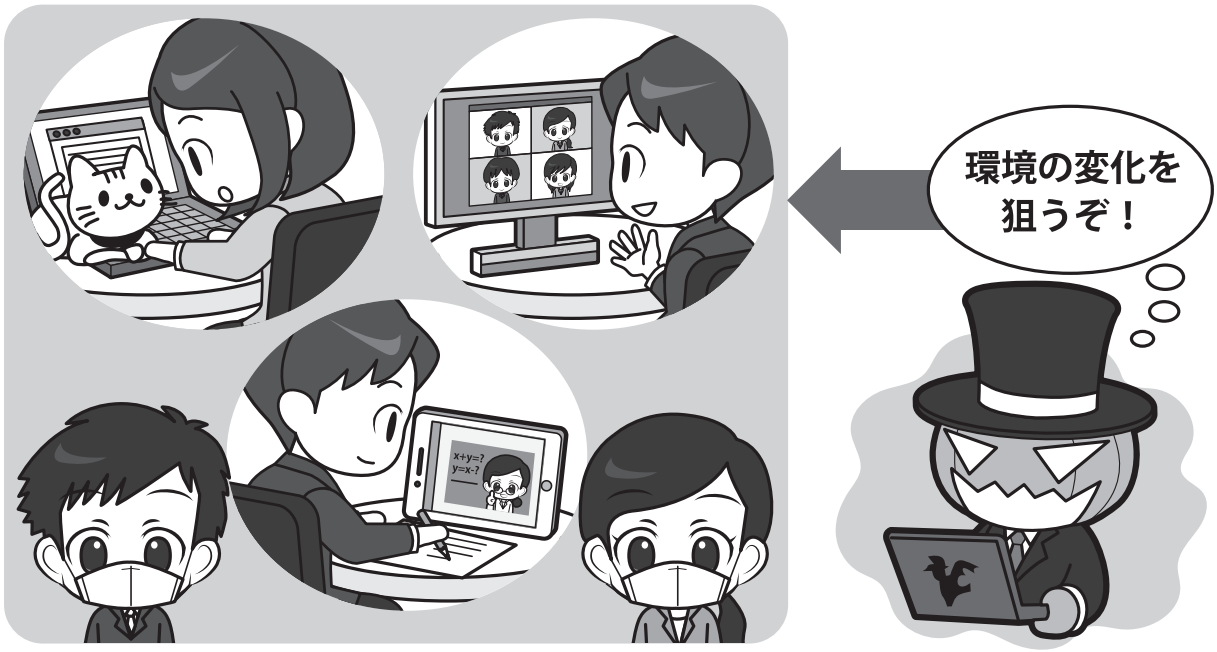
振り込め詐欺の場合は、例えば、まず相手に「身内が事故やトラブルを起こして大変だ！」と思い込ませ、電話をかけている人間が誰か確かめるなどの、相手が本来持っている冷静な判断能力を奪います。せかしたり、弁護士や警察官に扮した人物を登場させたり、お金を払えば助かると交換条件を出したりといった心理的な揺さぶりは、古典的なソーシャルエンジニアリングの、「ハリーアップ」「ネームドロップ」「ギブアンドテイク」というものにあたります。

一方、ネットの世界のソーシャルエンジニアリングは、知り合いになりすまして「標的型メール」を送る場合「フレンドシップ」という手法に当てはまります。

現実世界でもネットの世界でも、相手の心の隙を突けばどんなセキュリティでも破ることができます。そのだますテクニックが「ソーシャルエンジニアリング」なのです。ぜひ、そういうテクニックがあることを覚えてください。

この心の隙を突く攻撃は広い意味で「ソーシャルエンジニアリング」と呼ばれマニュアル化されています。覚えておいてください。

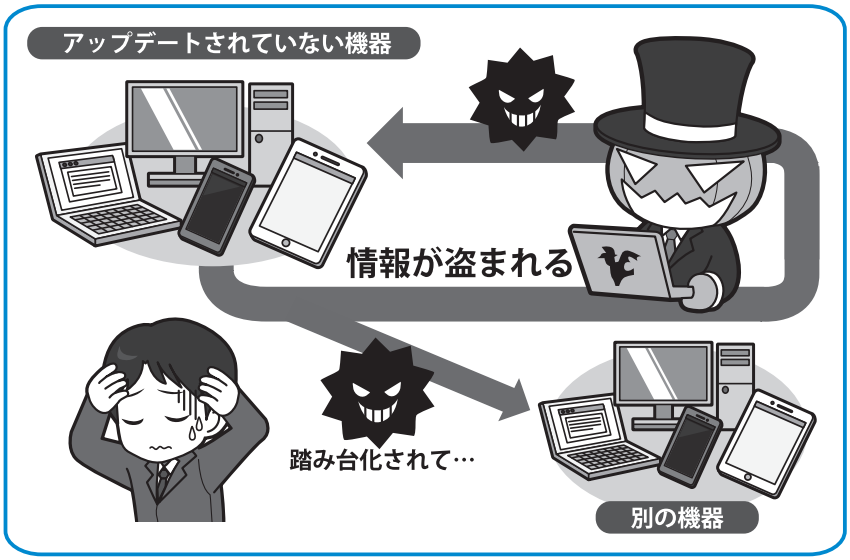
2 テレワーク・オンライン授業における注意点



新型コロナウイルス感染症の影響等により、従来のようにオフィスや学校に行かずに、自宅や外出先でテレワークを行ったりオンライン授業を受けたりする機会が増えています。物理的にもネットワーク的にも意識しなくても守られていた環境から、自分が意識して自分のことを守らなければならない環境に変化しています。こういった環境の変化にはリスクはつきものです。

悪い事を考える人達は、そのような環境の変化を利用し、様々な手法を使用してあなたを狙ってきます。

あなたを狙う攻撃者は、アップデートされていない機器、パッチが当たっていない機器を狙ってきます。このような機器は脆弱性（ぜいじゃくせい）と呼ばれる「プログラム上の弱点」が存在しているため、その弱点を突いた攻撃を受けた場合、機器の中の情報が盗まれてしまったり、機器がマルウェアに感染し踏み台にされ、別の機器に感染を広げてしまうきっかけになる可能性があります。テレワークを行ったりオンライン授業を受けたりする以前は、会社や学校に行くことで端末に自動的にパッチが当てられたり、会社や学校の担当者がアップデートを手伝ってくれたりしていたかもしれません。しかし、テレワークやオンライン授業が進み、自分の使用する端末のセキュリティ状態は自分で責任をもって管理やチェックしないといけないことも増えました。



☆合わせてこちらも確認してみよう！
第１章　基本のセキュリティ～ステップバイステップでセキュリティを固めよう～
２．環境を最新に保つ、セキュリティソフトを導入する・・・P28

あなたを狙う攻撃者は、あなたを焦らせたり不安にさせる内容や実際のやり取りの返信などを装ったメールやSMSを送ってくることがあります。またテレワークやオンライン授業が増え、すぐに相談できずにどうしていいかわからないと悩む機会も増えたと思います。

こういったメールはとても精巧に作成されているため、本物か偽物かを見分けるのは非常に困難です。本文内にURLリンクが記載されていたり、ファイルが添付されているメールやSMSには注意するようにし、もしこのようなメールやSMSを受信した際には一呼吸置いて冷静に判断するようにしましょう。

サイバーセキュリティ対策に「絶対」はありません。万が一の時に備えて、緊急時の連絡先や相談先、連絡手段をいつでも確認できるように準備しておきましょう。大事なのは、所属している組織（会社や学校）のセキュリティ報告窓口まで速やかに報告することです。

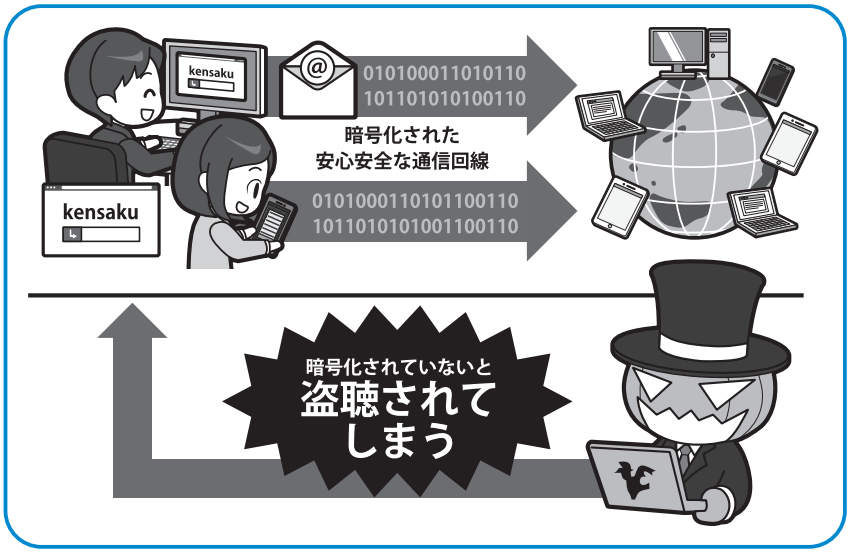
本物か偽物か『見分ける』のが困難になっている

＜注重すべきメールの内容＞
- 本文内にURLリンクが記載されている
- メールにファイルが添付されている
- メールを読んだだけで完結しない内容

＜どうすればいいか＞
- まずは偽物じゃないかと疑ってみる
- いきなりURLにアクセスしたり、添付ファイルを開封したりしない
- そのメールに思い当たることがあるか確認する
- 知り合いや周りの人に相談する

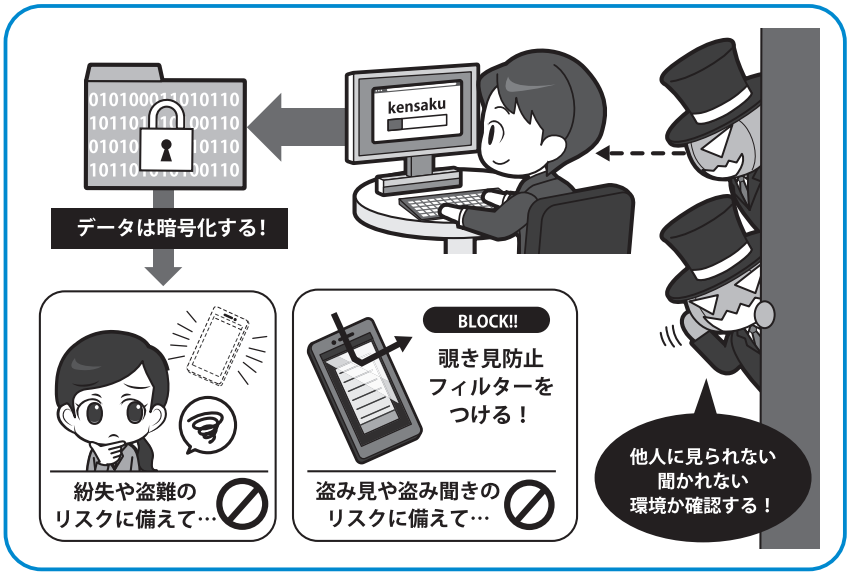
☆合わせてこちらも確認してみよう！
第２章　サイバー攻撃にあうと、どうなるの？　最新の攻撃の手口を知ろう
１．攻撃者にIT機器を乗っ取られるとこんなことが起こる・・・P46

オンラインで作業をする場合、必ず無線、有線問わず通信回線を利用します。その通信回線がセキュリティ的に安心安全に使用できるかの確認を行いましょう。もしその回線が暗号化されていない場合、悪意のある第三者に通信内容が盗聴され解読されてしまう可能性があります。そうならないように暗号化された回線を利用するようにしましょう。



☆合わせてこちらも確認してみよう！
第３章　パスワード・Wi-Fi・ウェブ・メールのセキュリティを理解して、インターネットを安全に使おう
２．通信を守る、無線LANを安全に利用する・・・P70

社外や自宅外で作業を行う場合にも注意が必要です。自分の情報を盗み見ようとしたり、盗み聞きしようとしている人がもしかしたら近くにいる可能性があります。情報を漏えいさせないためにも、社外や自宅外で作業をする場合は、PC等の画面を盗み見られないようモニターに覗き見防止シートを貼ったり、電話やオンライン会議をする場合は、他の人に話の内容を聞かれることのない個室等の環境で実施したりするようにしましょう。



また組織外にノートPCやスマートフォンを持ち出すということは、紛失や盗難のリスクもあるということです。万が一の事を想定し、端末内の記憶装置やデータは暗号化しておくようにしましょう。

☆合わせてこちらも確認してみよう！
第４章　スマホ・パソコンのより進んだ使い方やトラブルの対処の仕方を知ろう
１．スマホのセキュリティ設定・・・P98

オンラインでの会議やオンライン授業が増えたことで、本来の会議参加者ではない人が無断で会議に参加して音声を乗っ取る、会議内容とは関係のない画像を共有する等の妨害行為を行うケースも見受けられます。そういった事態に陥らないよう、オンライン会議や授業を行う際には、必要に応じて会議参加のためのパスワード設定を行う等、適切な対策を実施しておきましょう。また、オンライン会議中に映り込む背景などに、組織外の第三者に知られてはいけない情報が意図せず映り込んでしまう可能性があります。必ずミーティング前に、参加者の画面にどのように映るのかをチェックしておく、背景をぼかす設定等をONにしておく等の確認をしておきましょう。

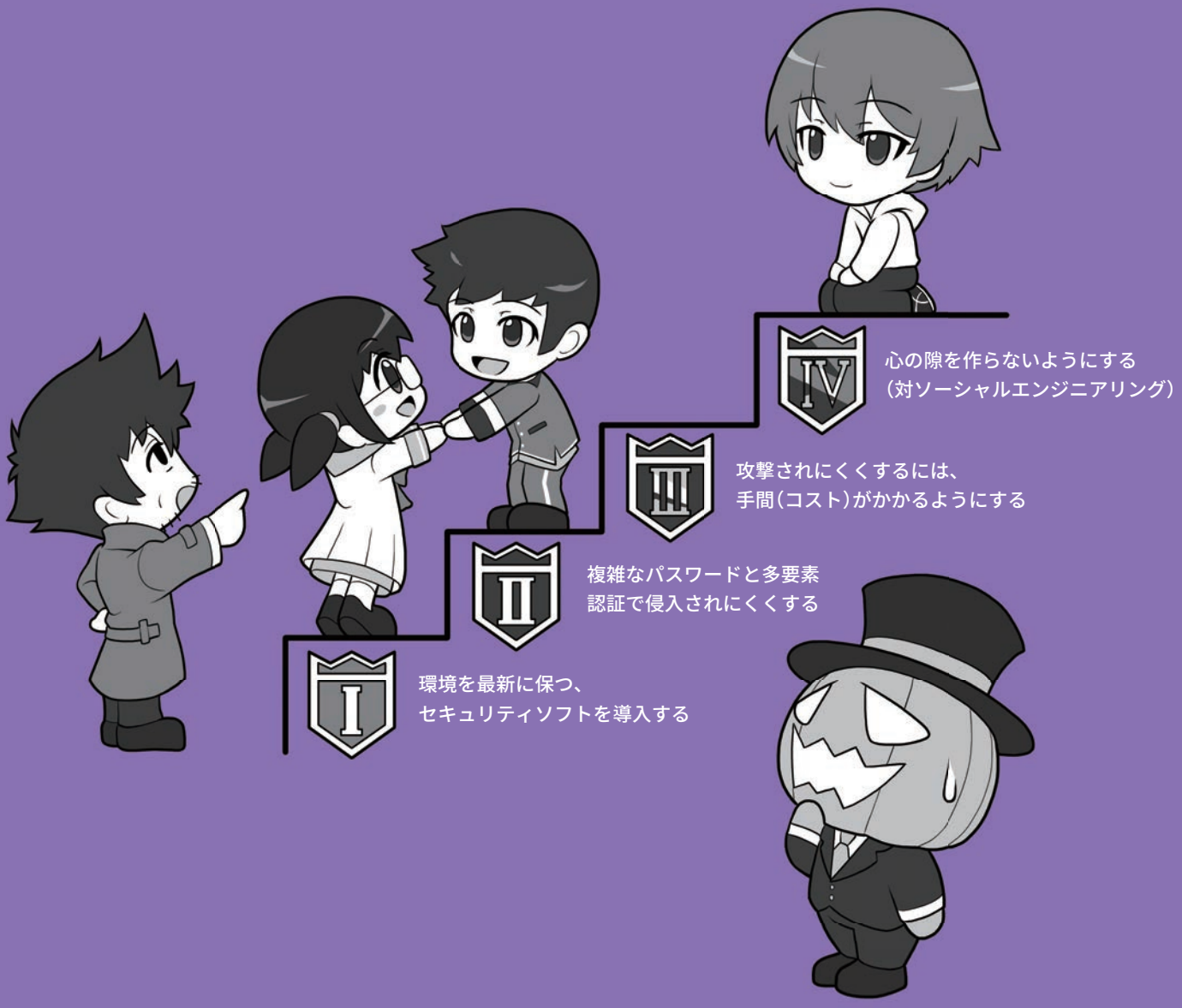
☆合わせてこちらも確認してみよう！
第５章　SNSやインターネット関連の犯罪やトラブルから、自分や家族を守ろう。災害に備えよう
１．SNSやネットとのつきあい方、守り方・・・P114

第1章

基本のセキュリティ

～ステップバイステップでセキュリティを固めよう～

サイバー攻撃を受けにくくするための、簡単なセキュリティの固め方を理解しましょう。
また、パスワードの管理の仕方や、攻撃する側が攻撃したくなくなるにはどうすればいいかを学びましょう。
人間の心の隙を突く、ソーシャルエンジニアリング攻撃などについても勉強しましょう。



1 4つのポイントで セキュリティを守る

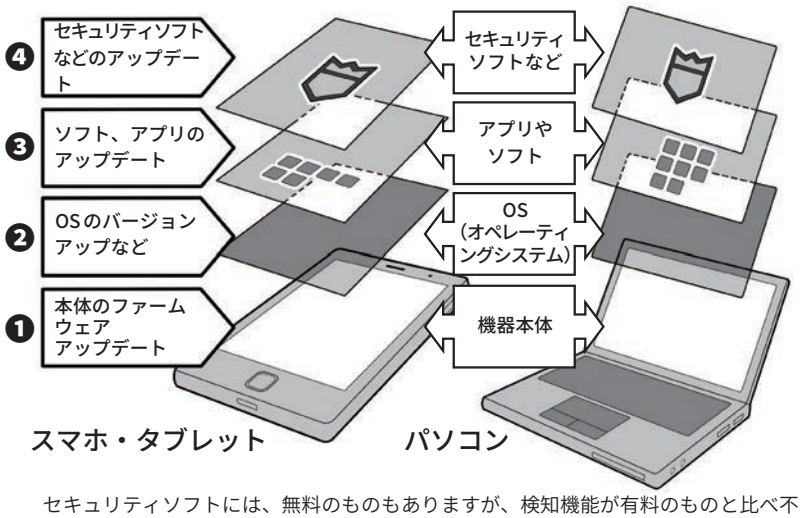
1 システムを最新に保つ。セキュリティソフトを入れて防ぐ

サイバー攻撃を防ぐための第一歩は、パソコンやスマホのシステムを最新の状態に保つことです。

①に機器の本体の「ファームウェアのアップデート」。②に、私たちが操作するインターフェースを提供している「オペレーティングシステム（以下OS）のバージョンアップやアップデート」。③に、セキュリティホールになりやすい「ソフトやアプリのアップデート」を行います。

パソコンの場合、それに加えマルウェア検出などを行う④「セキュリティソフトの導入とアップデート」です。なお、スマホの場合、導入は必要性に応じてなので、P30を参照してください。これらを常時更新して　セキュリティ上の穴をふさぎます。

様々な段階でセキュリティを守る



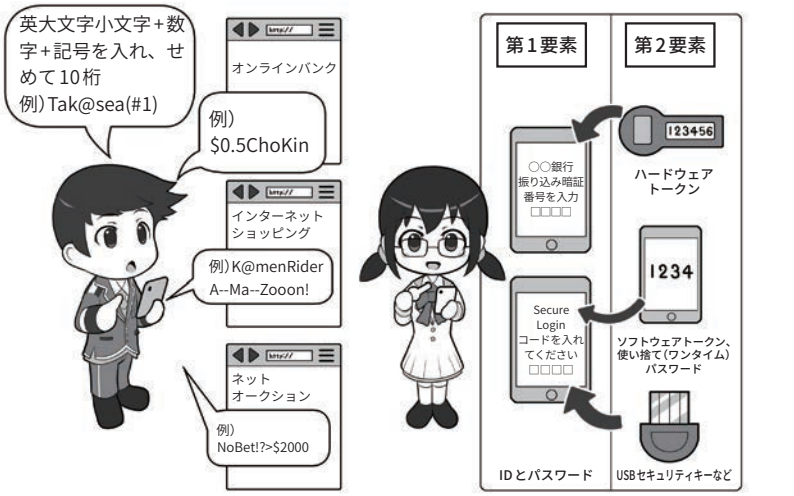
セキュリティソフトには、無料のものもありますが、検知機能が有料のものと比べ不十分なものや、セキュリティソフトを名乗りながら、実はマルウェアのような挙動をするものもあるので注意してください。どれを導入するか迷った場合は、プロバイダなどが提供するセキュリティパックか、信頼できるメーカーのソフトを導入しましょう。多少のコストがかかってもセキュリティ向上は安全への投資なのです。

2 複雑なパスワードと多要素認証で侵入されにくくする

次に、サイバー攻撃で的になりやすいのはパスワードです。攻撃者がこれを入手するには「見つけ出す」のと「盗む」攻撃方法があります。まず簡単にやられないように、購入時に設定されていたパスワードは必ず変更し、複雑なパスワードをウェブサービスや機器ごとに別々に設定しましょう。設定したパスワードを盗まれないように保管することも重要です。

続いて、仮にパスワードを盗まれてもサービスや機器が乗っ取られないように、多要素認証などさらなる防御手段を追加しましょう。

複雑なパスワードや多要素認証でセキュリティを守る



ウェブサービスや機器間で、使い回しのない英大文字小文字・数字・記号が入った複雑なパスワードを使う

使い捨てパスワードや多要素認証の導入、ネットに流出しない現物としてのセキュリティキーなどを利用する

3 攻撃されにくくするには侵入に手間(コスト)がかかるようにする

サイバー攻撃を行う攻撃者は、プロフェッショナルであるスパイを除けば、ビジネスとしての効率が重要なので、より手軽に侵入できる対象を選ぶ傾向にあります。

警備や戸締まりがしっかりしている場所に泥棒が入らず、鍵がかかっていない留守の家に空き巣が入るのは、その方が危険性(コスト)が低く手軽だからです。

サイバー攻撃でも同じように、侵入するまでに幾重にも防御がしてあると、攻撃者にとっては手間(コスト)がかかって面倒な、あるいはそもそも侵入できない対象となり、攻撃されにくくなります。

そのためには、システムを最新の状態に保ちセキュリティホールをふさぎ、セキュリティソフトを導入し、複雑なパスワードや多要素認証が必要になるわけです。

守りを何重にもして侵入されにくくする

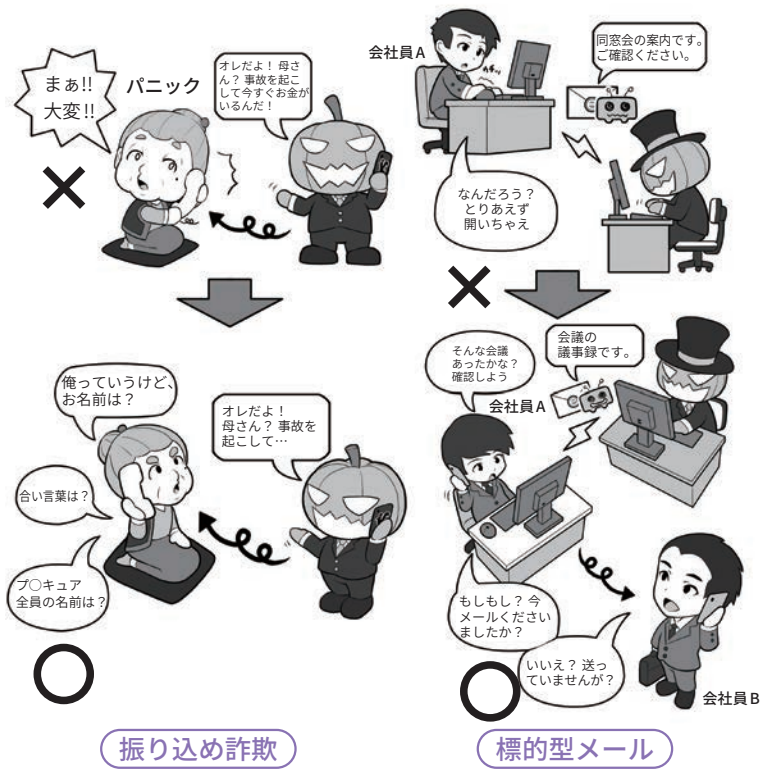
4 心の隙を作らないようにする(対ソーシャルエンジニアリング)

しかし、それでも、ソーシャルエンジニアリングという、人間の心の隙を突く攻撃を受けて攻撃者に操られ、家の鍵を中から開けるような状況になってしまうことがあります。それを防がなければ、いくらシステムのセキュリティを高めても意味がありません。システム面と心理面の防御は車の両輪なのです。

振り込め詐欺のあやしい電話なら合い言葉で防御する。あやしい電子メールやメッセージを使った標的型のサイバー攻撃なら、疑わしい通信手段とは別の通信手段で送信者に情報を確認するなどの対処法があります。

これは、項目の2にもあった多要素認証と同じ考え方で、攻撃を防ぐシンプルかつ有効な手段です。

心の隙を作らない。攻撃をうけつけない



2 環境を最新に保つ、セキュリティソフトを導入する

1 セキュリティソフトを導入して守りを固めよう

単純なウイルス対策ソフトがマルウェアを見つける方法は、おもに「手配書」方式になっています。

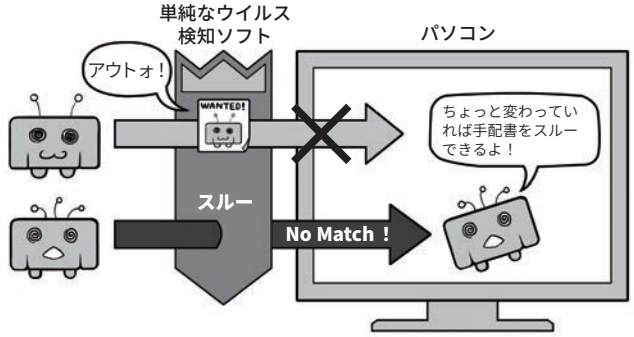
手配書方式とは、あらかじめ検出したいマルウェアの特徴を、対策ソフト開発社からそれぞれのパソコンなどに送信しておき、マッチしたものを駆除する方式です。

しかし、現在では攻撃者が、発送先ごとに送りつけるマルウェアを微妙に変えたり、狙いを定めて専用に作ったりする場合もあるので、この方法では見つけ出すことが難しくなりつつあります。

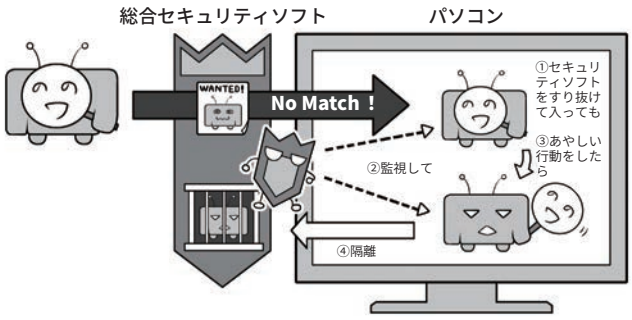
そこで、単純ではない最近の総合セキュリティソフトでは、「手配書」方式に加えて、パソコンに入ってしまった後も監視を続け、不審な行動を取れば隔離なり駆除をする、「ふるまい検知」や、機能的に怪しい部分を検出する「ヒューリスティック分析」機能を持つものが出てきています。これにより、未知のマルウェアにもある程度は対処できるわけです。

しかし、それでも対処しきれないものもあります。システムのセキュリティホールが発見されると、それが修正される前に攻撃する「ゼロデイ攻撃」を行うマルウェアです。この場合は、手配書も間に合わないので、現状では、決定的に有効な手段がほとんどありません。しかし、そういったことを踏まえても総合セキュリティソフトを導入することには多くのメリットがあります。ぜひ導入してパソコンの守りを固めましょう。

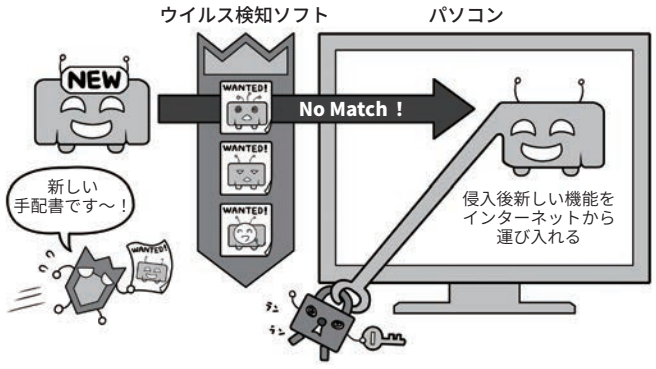
単純なウイルス検知ソフト



進化したセキュリティソフト（総合セキュリティソフト。ふるまい検知、ヒューリスティック分析あり）



手配書が間に合わないゼロデイ攻撃も



2 パソコン本体とセキュリティの状態を最新に保とう

パソコンのセキュリティを最新に保つためには、各種のアップデート処理が不可欠です。

最近の機種では、たいていの場合、OS関連のアップデートは自動で行われるか、利用者にアップデートを促す通知が出るようになっています。ただ、深刻なセキュリティホールが発見され、緊急でアップデートを行ったほうがよいこともあります。セキュリティ関連ニュースサイトなどでそういった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されます。

次に、サイバー攻撃で狙われやすいソフトの更新を重点的に行いましょう。Adobe Flash Player、Adobe Acrobat Reader、Oracle Javaや各種のウェブブラウザはよく使用されるため、攻撃のターゲットになりやすいのです。

また、本体機器そのものを動かす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、自分の機器にファームウェアアップデートがあった場合、どういうようにその情報を入手するべきかを、確認して気を配ってください。

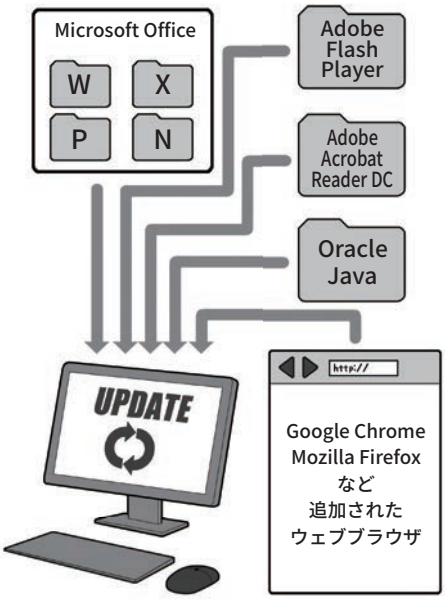
セキュリティソフトも、基本的にはインストールすると自動更新されるようになりますが、なるべく日に一度は意識的にセキュリティソフトの画面を見るようにしましょう。これは、セキュリティの状態を確認する意味もあります。

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

本体のファームウェアも更新

OSと基本ソフトの更新

重要ソフトも更新



セキュリティソフトも更新

ここであげられている重要ソフトは、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、そのためほとんどのパソコンで利用されています。

例えば、社会インフラがテロ攻撃などで狙われやすいのは、テロリストが少ないコストで多大な影響を与えることができるからで、こういった重要ソフトが狙われやすいのも同じ理屈なのです。ですから、利用する側も重要ソフトのアップデートがあったら速やかに適用して、攻撃者が攻撃できないようにしましょう。重要ソフトを使っていない場合は、削除してしまってもいいでしょう。

別項目でも登場したボットネットも、攻撃して乗っ取れる機器がなければ成立しないように、穴を作らない一人ひとりの行動が安全なネットを作るのです。

3 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が必要です。

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、また、自動アップデート機能も充実しています。機器そのもののソフトウェアの更新でも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でも、更新の通知が出たら、マメにアップデートするようにしましょう。

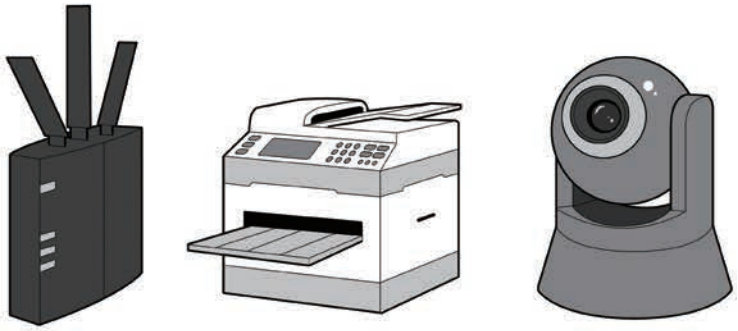
そのためには、本体のファームウェア(ソフトウェア更新やシステムアップデート)やOSの更新が、設定メニュー上のどこにあるのか更新手順を確認しておきましょう。また、アプリの更新が自動になっているかも確認しましょう。

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、また、その設定でも更新時に権限変更で、所有者による確認が必要な場合は自動で実行されないため、気づくと更新されていないアプリがたくさんたまっていることもあります。意識してアップデート画面に行き、更新作業を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スマート家電やIoT機器などは、こういった通知がなく、アップデートが公開されても気づかず、セキュリティホールが開いたままになっていることもあります。週1回でも月1回でも、アップデートファイルが公開されているかチェックしましょう。特に、ネットワークカメラなどは適切に管理しないと不正に利用されることがあります。

アプリやセキュリティソフトの更新は基本的に自動にし、まめにチェック

ネットにつながる家電もファームウェア更新する設定ページの初期パスワードも変更しておくこと



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

スマート家電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。このときの初期パスワードは必ず購入時から変更しておきましょう。不正アクセスされ、カメラなどでは覗き見される原因になります。

4 ソフトやアプリは原則公式ストアから。権限にも気をつける

本体やシステムを最新の状態に保っても、防ぎにくい攻撃があります。それは、まだマルウェアとして認識されていない悪意あるソフトウェアへの感染です。

基本的に、セキュリティソフトなどがマルウェアを検出するためには、過去に収集されたデータが必要になります。このデータが多ければ多いほど、マルウェア検出の精度は高まるのです。

これとは逆に、セキュリティソフト会社がまだ知らないマルウェア、あるいは検体が充分に収集されていないマルウェアは、検知ソフトなどでの発見が難しくなります。

攻撃者が、チェック体制のしっかりしている公式ストア経由ではなく、私たちをメールなどで誘導し、不審な場所から導入させようとする理由もそのためです。

そのような手に引っかかって、マルウェアに感染してしまわないように、「ソフトは信頼できる場所から、アプリは公式ストアから導入する」ことが推奨されるわけです。

特に、スマホの場合、iOS 機器は公式のストア以外からはアプリを導入できない仕組みになっていますが、Android 機器の場合は公式ストアやベンダー・メーカーのストア以外からもアプリをインストール可能です。それを利用し攻撃者がメールや SMS などであなたを誘導して、公式ストアでない場所から不明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。

そのほか、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、すべてセキュリティ上危険なものと判断するようにし、最初から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、基本的に公式ストアからのみインストールするようにして、そのほか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。

コラム：必要ならばスマホには セキュリティパックを検討しよう

スマホの場合、その誕生が比較的最近であることもあり、設計思想自体にセキュリティの概念が盛り込まれていて、パソコンなどと比較して、セキュリティアプリなどが担う役割は大きくはありません。

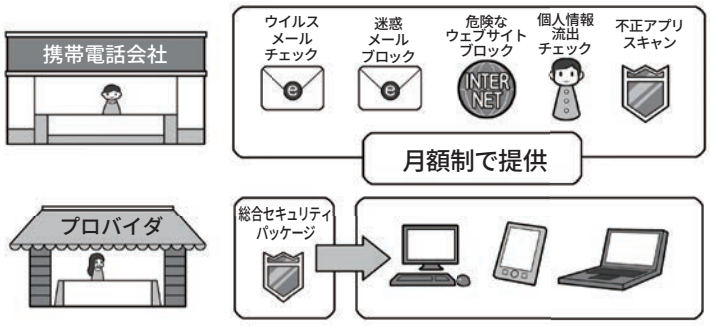
しかし、チェックするべき点を見落とし、気づかないうちにインストールされる不正なアプリの検出や、また、そういったものの侵入経路になるメールの排除、危険なウェブサイトのブロック、あるいは個人情報の流出チェックなど、セキュリティ全般にかかわる機能を補助的に導入したい場合もあるかもしれません。

そういった場合は、携帯電話会社やプロバイダなどが、セキュリティアプリを含め、セキュリティ機能をまとめて提供するパッケージを、内容を充分に精査した上で導入してもいいでしょう。

また、メーカーが作ったスマホのセキュリティ思想は、定められた利用方法から外れると、とたんに脆弱になり攻撃されやすくなるので、Android の「root 化」や iOS の「JailBreak」といった改造は絶対にやってはいけません。

そして、高機能化するスマート家電など IoT 機器についてもスマホと同様にセキュリティ対策が必要になります。P45 も参照して、万全の対策を講じていきましょう。

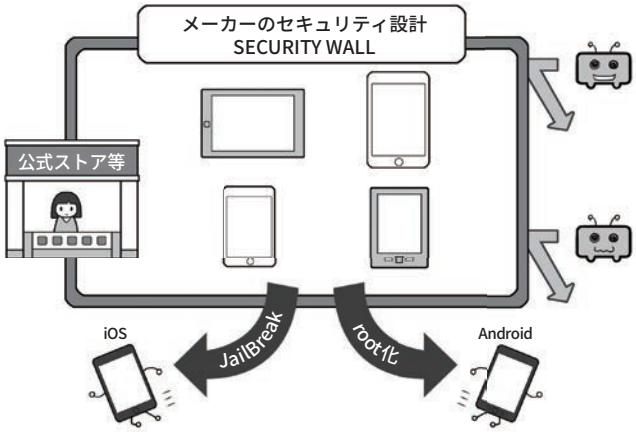
必要性を感じるなら、スマホには セキュリティパック導入を検討しよう



上記のようなサービスをまとめて複数台に月額制で提供

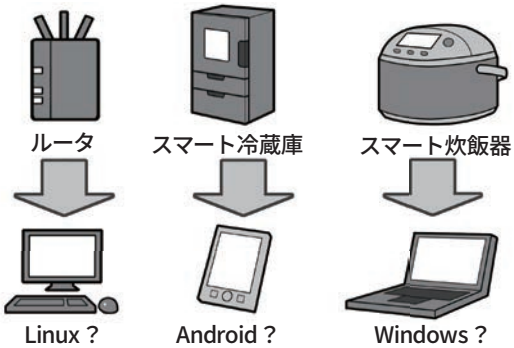
携帯電話会社からは、セキュリティ関係の機能がパッケージ化されて提供され、インターネットプロバイダも、同様のサービスを提供しています。自分が求める機能があるかを精査して、必要性を感じる場合は導入を検討しましょう。

スマホのセキュリティを改造してはいけません



スマホのセキュリティ思想は、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。「root 化」や「JailBreak」といったソフトウェアの改造は、規約違反である場合もあり、セキュリティ上も脆弱になるので非常に危険です。やってはいけません。

スマート家電や IoT 機器の中にはパソコンやスマホがある？



スマート家電や IoT 機器は、一見ただの機械に見えて、実は内部に Linux、Android、Windows などのコンピュータが入っていることがあります。乗っ取られ、サイバー攻撃に利用されるの可能性もあるので、なんらかのセキュリティ対策が必要です。

コラム：パソコンやスマホを最新の状態に保っても防げない攻撃がある。それがゼロデイ攻撃！

一般的には、システムやソフトにセキュリティホールが見つかると、攻撃者はこの穴を攻撃するためのマルウェアを急いで開発し始めます。メーカーもこの穴に気づけば、アップデート用のセキュリティパッチを開発し公開します。通常この競争に勝つのは攻撃者です。このようにセキュリティホールが発見されてからメーカーによって修正されるまでの期間を狙って攻撃することを「ゼロデイ（ZERO DAY）攻撃」といいます。

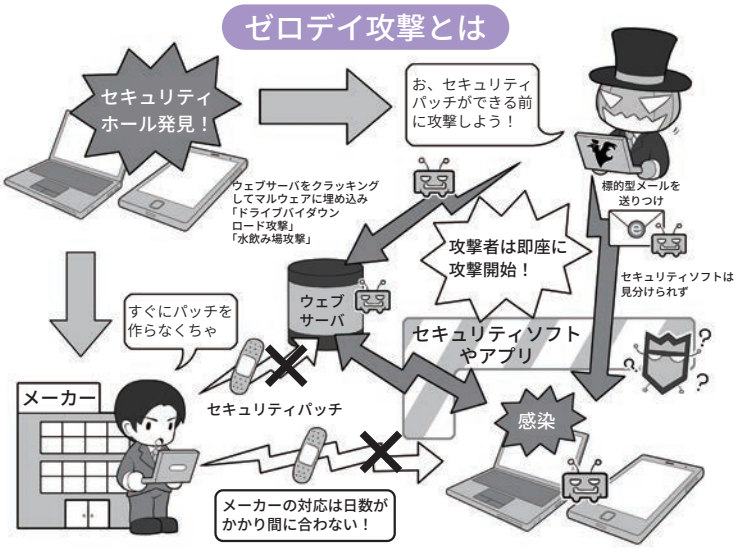
メールで送りつけられるマルウェアは、警戒していればある程度防ぐことができるのですが、動画、ウェブサイトやウェブ広告に仕込まれるマルウェアは、特定のサイトを見ただけで感染することもあり、情報がないままこの方法でゼロデイ攻撃を受けると実質的に防ぐことができません。

特に、最近では攻撃者がお金を支払ってまで、マルウェアの仕込まれた動画ウェブ広告を大手サイトに出してサイバー攻撃をしかけてくるため、その規模も非常に大きくなってきています。これは、広告を出すコストが、不正に入手できるお金に見合っているということを意味しています。

被害を少しでも避けるためには、セキュリティ情報サイトやSNS（NISCのtwitter「内閣サイバー（注意・警戒情報）」など）をこまめにチェックして、例えば、動画系のマルウェアが登場したら動画の自動再生機能をOFFにする、スマホ用アプリであればセキュリティホールが修正されるまでアンインストールするなどの対応をしましょう。アプリを提供するサービスは、アプリを使用しなくてもウェブブラウザで利用可能なこともあるので、普段からスマホなどでもウェブブラウザ経由での利用にも慣れておきましょう。

ゼロデイ攻撃とは？ 対処の例

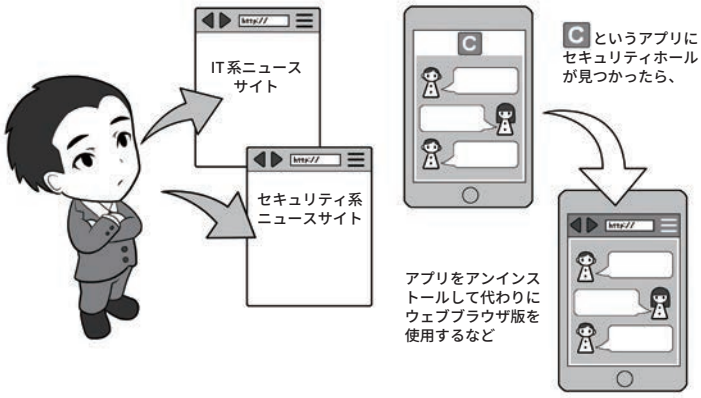
ゼロデイ攻撃とは



ゼロデイ攻撃に対抗するには？

ニュースサイトをこまめに見て情報収集

別の手段でセキュリティホールを避ける



攻撃者とメーカーのゼロデイ攻撃に関する対応競争は、たいていの場合攻撃者が先行します。攻撃者はメーカーが気づいていないセキュリティ情報を入手し、対象の機種どれが一つでも攻撃に成功するなら攻撃を開始できますが、メーカーは情報を精査した上で、対象となっている機種すべてで充分なセキュリティ対応をしなくてはいけないからです。

ですから、利用者もそれを前提として備え、対処行動をする必要があります。そうすることが結果として自分を守ることになるわけです。

3 複雑で長いパスワードと多要素認証で侵入されにくくする

1 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る方法のほかに、なんらかの手段でIDとパスワードを解明し、機器やサービスを乗っ取るものもあります。

パスワードは、ウェブサービスなどが保管しているものが流出して使われる「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試す「辞書攻撃」などにより探し当てる方法や、IoT機器購入時のパスワードを変更せず乗っ取られる場合もあります。

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26文字の記号を入れると88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、攻撃し続ければ理論上は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」にして防ぎます。ログイン用パスワードであれば入力ごとに時間がかかるので、英大文字小文字＋数字＋記号混じりで10桁以上を安全圏として推奨します。しかし、より桁数を増やして安全性を高めるに超したことはありません。

ログイン用パスワードは英大文字小文字＋数字＋記号で10桁以上

「ログインに使うパスワードは、英大文字小文字＋数字＋記号で10桁以上」の理由

数字のみだと→100億通り

英大文字小文字＋数字＋記号（26個として）だと→
約2785京97兆6009億通り

数字だけで10桁と、英大文字小文字＋数字＋記号で10桁では雲泥の差がある。
そして、これほど多量な組み合わせは、機械入力でも事実上突破不可能。

英大文字小文字＋数字＋記号混じりの組み合わせ数

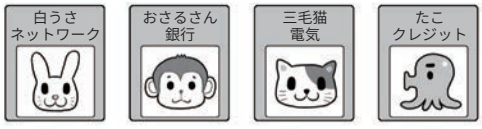
アルファベット（大）＋アルファベット（小）＋数字＋記号（例）
26　＋　26　＋　10　＋26＝88

数字	英大文字	英小文字	記号	合計		5	6	7	8	9	10
10				10	数	100,000	1,000,000	10,000,000	100,000,000	1,000,000,000	10,000,000,000
10	26			36	数英	60,466,176	2,176,782,336	78,364,164,096	2,821,109,907,456	101,559,956,668,416	3,656,158,440,062,976
10	26	26		62	数英大小	916,132,832	56,800,235,584	3,521,614,606,208	218,340,105,584,896	13,537,086,546,263,552	839,299,365,868,340,224
10	26	26	26	88	数英大小記	5,277,319,168	464,404,086,784	40,867,559,636,992	3,596,345,248,055,296	316,478,381,828,866,048	27,850,097,600,940,212,224

2 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、それを複数の機器やサービスで使い回していては意味がありません。1カ所から漏れればすべてログイン可能になります。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つけるのも、1つ漏れれば推測されます。それぞれに別々のパスワードを設定し、使い回しをしないことが大切です。

同じパスワードを使い回さない。似たパスワード、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	たこ クレジット	
×使い回し	PASSPPOI	PASSPPOI	PASSPPOI	PASSPPOI	全部同じ
×おしりだけ違う	PASSPPOI1	PASSPPOI2	PASSPPOI3	PASSPPOI4	推測しやすい
×法則性あり	USAGIPPOI	OSARUPPOI	NEKOPPOI	TACOPPOI	法則性がばれたらおしまい

3 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、テキストファイルなどで保存しておけば、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。

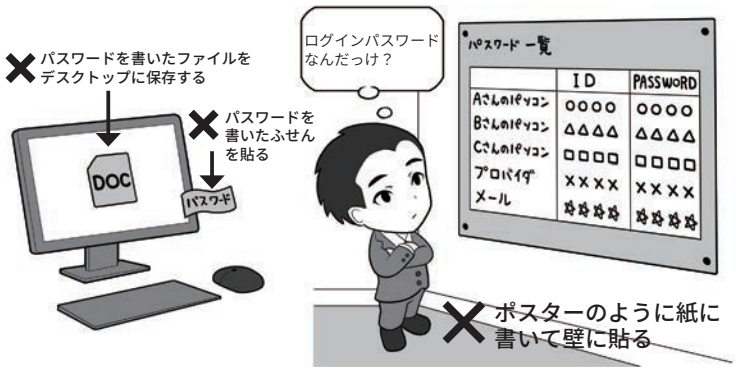
パソコンで、ウェブブラウザに覚えさせる「自動入力」機能も要注意です。あなたが席を離れた隙に、誰かがパソコンを勝手に操作するかもしれません。それに、ノートパソコンなら本体ごと盗まれてしまいます。またもしマルウェアに感染して外部からパソコンを攻撃者に遠隔操作されてしまった場合、ブラウザに登録しているパスワードリストを奪われてリスト型攻撃に使用されてしまう可能性もあります。パスワードは、基本的に利用する場所で保管してはいけないのです。

サービス毎に設定した個別に複雑なパスワードはどのように保管すればいいでしょう。

一つは、紙のパスワード管理ノートに書いて、パソコンとは別に保管する方法。もう一つはスマホのパスワード管理アプリを利用する方法があります。なお、後者の場合、クラウドでデータを保管する機能の利用は熟考し、過去にセキュリティ上のトラブルがあったアプリは避けましょう。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。

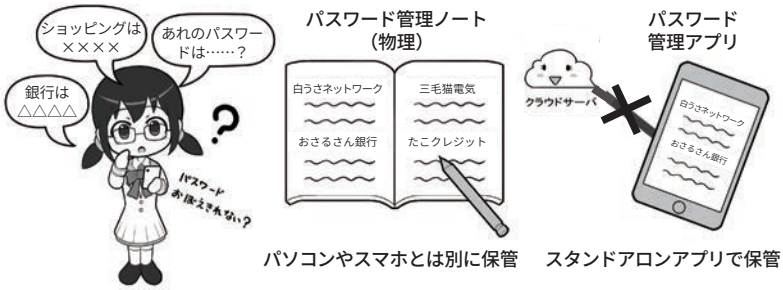
スマホでもパスワードを使う場合もリスクはありますが、こういったアプリは後述のPINコードや指紋認証＋暗号化で情報がガードされます。盗まれても落としても、簡単に他人が使ったりすることはできません。ただ、管理しているパスワードは、必ずバックアップを忘れないようにしましょう。落としたスマホが戻るとは限りませんから。

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。

パスワードは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。アプリの機能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。

ウェブブラウザの自動入力にパスワードを覚えさせない

4 秘密の質問にはまじめに答えない。多要素や生体認証を使う

各種のウェブサービスには、パスワードを忘れてしまった場合の本人確認、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るものです。

この秘密の質問には、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」とか「ペットの犬の名前は」のように、生活に密着したものからしか選べなくなっています。しかし、こういった個人情報はSNSが普及した現在、ネットで簡単に見つけられることもあり、セキュリティ上、安全とはいえなくなっています。

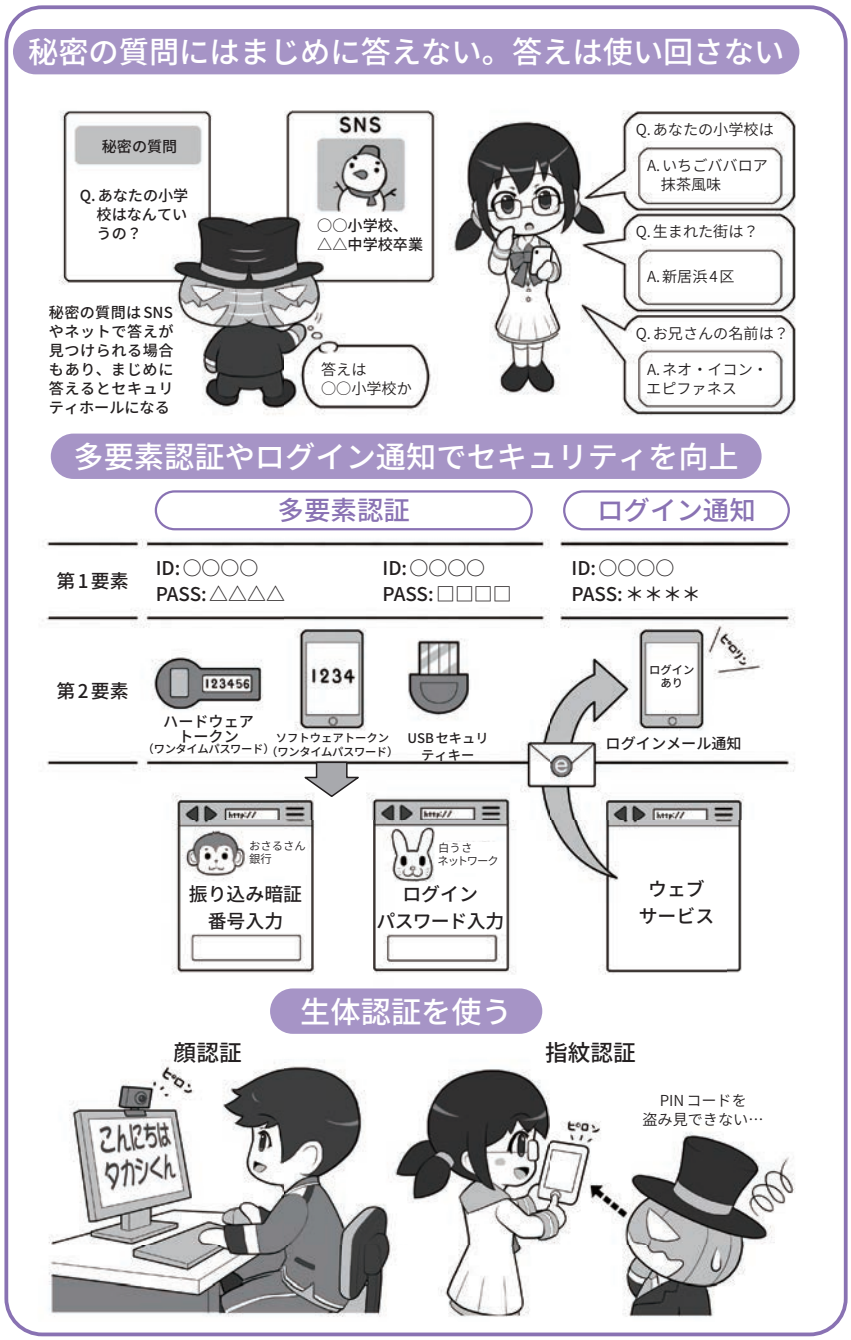
ですから、秘密の質問に答えを設定する場合、まじめに答えず、あえて全く関係ない答えを使い、SNSなどから推測できないようにし、その上で忘れないように管理アプリなどに保存しましょう。

また、ウェブサービスに安全にログインするために、二要素以上を使う多要素認証方法が提供されていれば必ず設定しましょう。これらの方法では、通常のパスワードのほかに、そのときに一度きり使用する使い捨て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。（SMSやメールで送信する方式もありますが、安全面で非推奨です）

そのほかにも、USBセキュリティキーなどで物理的に確認する方法や、不審なログインがあったときに、メールで利用者に通知するサービスがあれば活用しましょう。

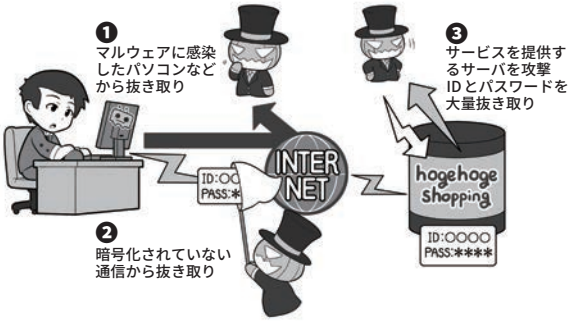
また、最近の機器では3次元の立体的な顔形状や、虹彩や指紋で本人確認をして機器のロック状態を解く生体認証機能もあります。

生体認証は本人のみが使える反面、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るなど善し悪しですが、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。なお、生体認証はたいていは通常のPINコードの入力の替わりなので、スマホでは失敗すると通常のPINコード入力に戻ります。本体を盗まれてこの方式でロック解除されないよう、PINコードには誕生日などの個人情報は使わないようにしましょう。



コラム：パスワードはどうやって漏れるの？どう使われるの？

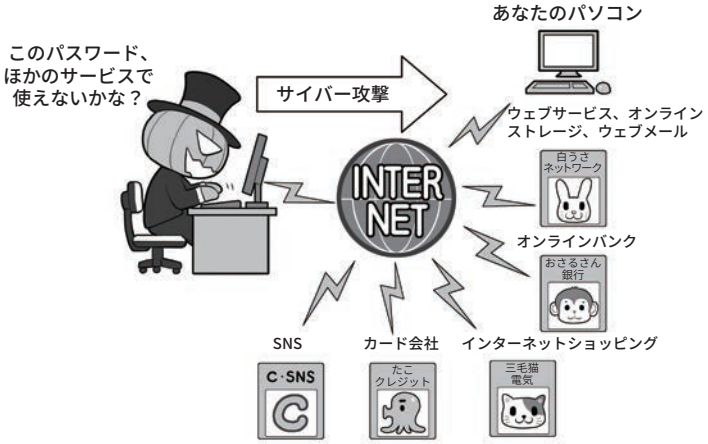
様々なIDとパスワードの抜き取り方法



攻撃者にIDとパスワードが抜き取られる方法は、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ほかに、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。

攻撃者は盗んだIDとパスワードを使い、様々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様々な方法で試します。

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、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？

一つには、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るケースなどがあります。

ここで知っ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。IDやパスワードを普段入力してしないから安心、とはいい切れません。

IDとパスワードを盗み取った攻撃者は、それで別のウェブサービスなどが乗っ取れないか、様々な場所で試します。

あなたが、複数のサービスで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が一気に乗っ取られます。あとは、オンラインショッピングで勝手に物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してしまうわけです。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 攻撃されにくくするには、手間(コスト)がかかるようにする

サイバー攻撃を行う攻撃者は、軍事や産業スパイ、名をあげること自体を目的に採算度外視でやる悪意のハッカーなどではない場合、なんらかの利益が目的の行動が多いということができるでしょう。

彼等にとってのサイバー攻撃はビジネスであり、ビジネスはコストパフォーマンス、つまりいかに手間をかけず大きな利益を生むかが重要です。

そういった攻撃者の視点から見ると、攻撃されにくい環境を作るにはどうしたらいいかが見えてきます。

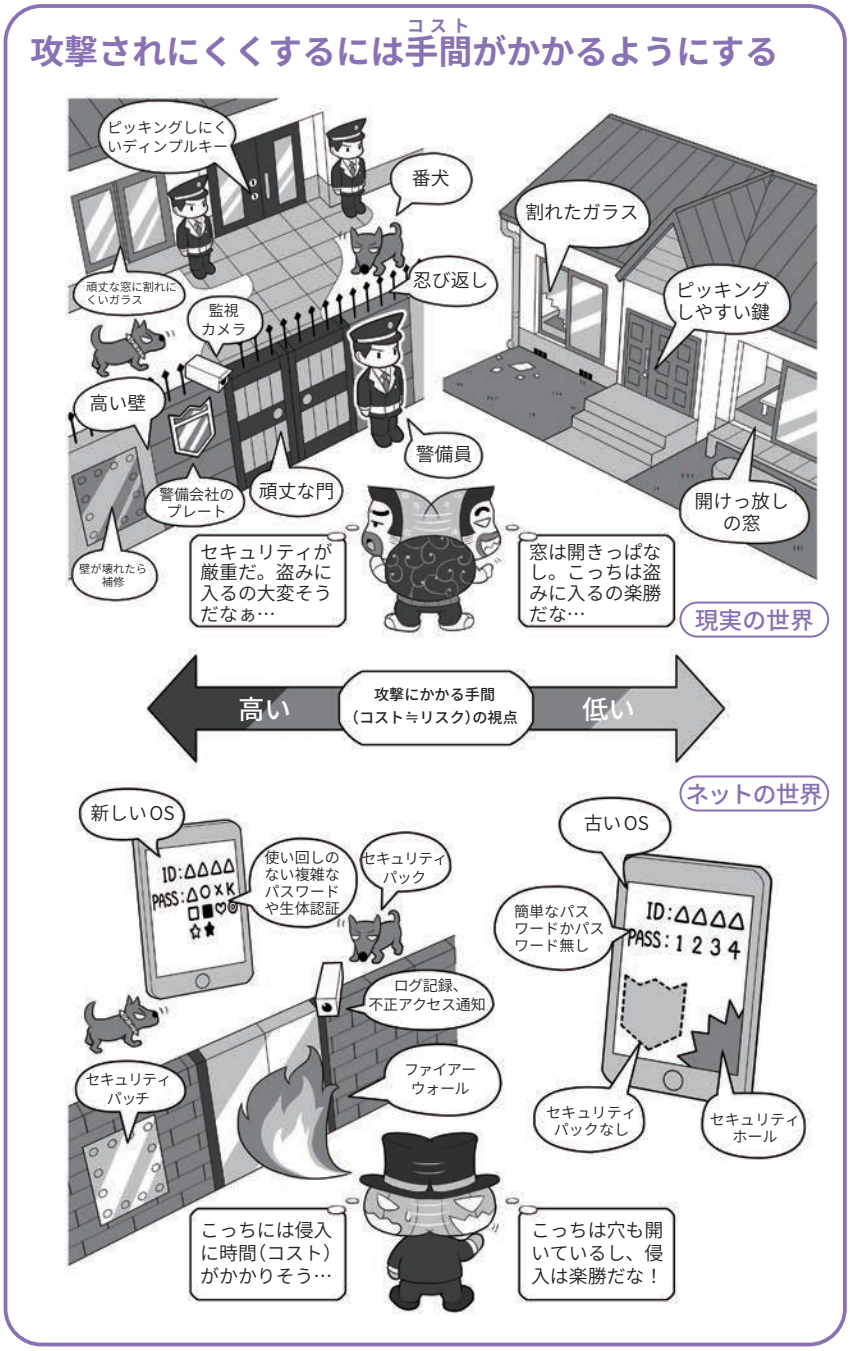
例えば、現実世界では、泥棒は防犯がしっかりしていて警戒が厳重な家よりも、鍵をかけなかったり窓を開けっ放しで外出したりするような家の方に侵入します。その方が、彼等にとって安全、つまり手間(コスト)がかからないからです。

これは、ネットの世界でも同様です。侵入するまでに幾重にも難関があり、侵入を試みたら形跡を記録され(ログ)、場合によってはしかるべき管理者に通知が行き、パスワードを破ろうとしても複雑で突破できない。システムも最新で、攻撃するにもセキュリティホールが見あたらない。セキュリティソフトも導入されている。さらに、ファイルを盗めても複雑な暗号化がされていれば、解読までに何百年もかかってしまい使えない。普通の攻撃者なら敬遠します。

横を見たら、セキュリティホールは放置、パスワードは非常に簡単だったり無しだったり、ファイルそのものも暗号化されておらず、パスワードを使っていても、たくさんのウェブサービスで全部同じものを使い回している。

これならば、どっちに行くのがビジネスとしてコストパフォーマンスがいいか明らかですよね。

こういった攻撃者の視点を持ち、侵入することがとても面倒くさく、攻撃したくなくなるような環境を構築するのが安全への近道です。一方、単純な利益目的でない場合、すこし対策が変わってきます。



金銭などの利益目的ではない攻撃の例としては、相手そのもの、つまり未成年者略取や、いかがわしい写真の入手などを目的とするものがあります。

現実の世界で、面と向かって「いかがわしい写真を撮らせてください」といったら、たいていの人は拒否して逃げ出すでしょう。それが、ネットの世界だと許容してしまう理由は、攻撃者がネットを利用して、警戒心をもたれないような人間になりすまし、相手をうまくだましてしまうからです。

ですから、SNSや掲示板などのウェブサービスで知らない人物が近づいてきたら、注意して絶対に個人情報は教えないようにしましょう。現実の知り合いでもないのに会おうと誘われた場合は、基本的に会わないか、会う必要がある場合は必ず保護者同伴で行きましょう。

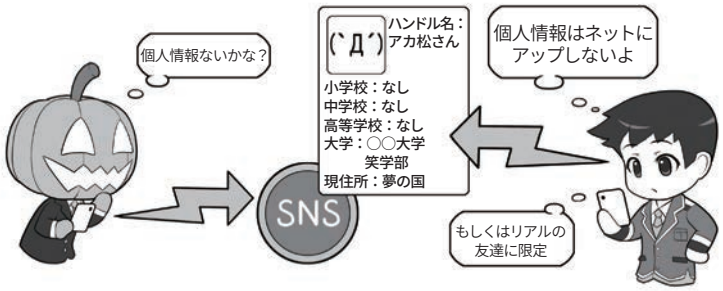
そして、少しでも変だなと思ったり、最初と話が違ったりした場合、それは人をだます「心理的な」テクニックかもしれません。警戒し、その場から立ち去りましょう。

あまり聞いたことがないかもしれませんが、そういった「人をだます心理的なテクニック(≒ソーシャルエンジニアリング)」は体系化されマニュアルのようになって存在するのです。

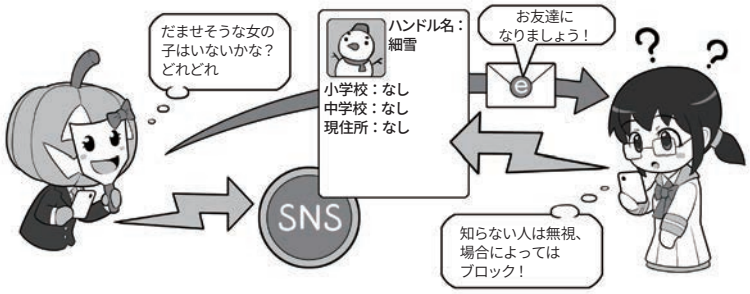
この人をだますテクニックは、なにも上記のような例だけでなく、私たちも日常生活の様々なシーンで直面しているのです。

例えば、「振り込め詐欺」や「標的型メール」。どんなにセキュリティを固めても、本人がだまされ結果として犯罪者に操られてしまうと、すべては無意味になってしまいます。厳重に注意しましょう。

金銭目的ではない攻撃にも備えよう



個人情報はネットに上げない！



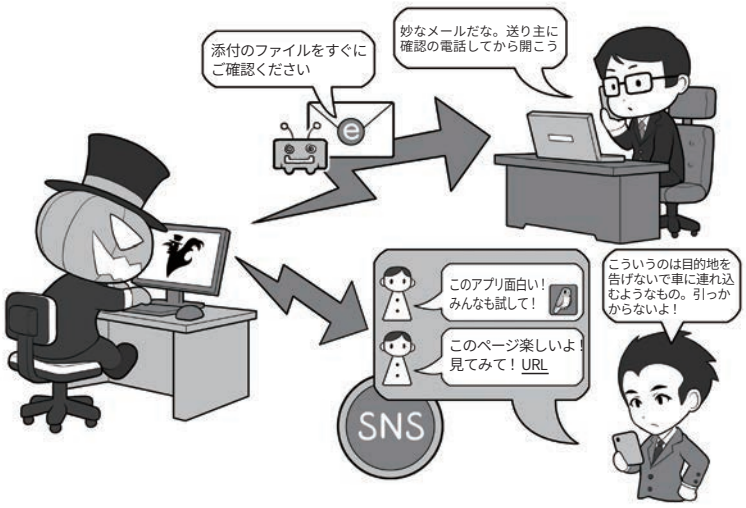
リアルで知り合いじゃない人とはネットで友達にならない！

未成年がSNSを利用する場合、写真や自分の個人情報を記載しないようにしましょう。また、投稿内容も原則的に一般に公開せず、SNSで友達になった人のみが見られる設定にしましょう。

SNSで、知らない人が友達になろうとリクエストを送ってきても、会ったことがない人はスルーするか基本的にお断り(ブロック)しましょう。

それは、現実の世界で自分の個人情報を書いた名札をつけて歩いたり、名前もわからない初めて会った人に、ついていったりするのと同じぐらい、たいへん危ないことなのです。

攻撃者に操られて、内側から鍵を開けてしまわないように、心がまえを持とう



不審なメールに気をつけ、怪しいときは開かず送信者に確認する癖をつけましょう。ネットやSNSの引っかけは、セキュリティ関係のニュースをこまめに見ていると、次第に傾向がわかるようになります。訓練しましょう。

5 心の隙を作らないようにする（対ソーシャルエンジニアリング）

心の隙を突く攻撃、ソーシャルエンジニアリングには、「トラッシング（ゴミ箱あさり）」など相手に直接接触せずにやるものや、「ネームドロップ（権威があるように見せて聞き出す）」「ハリーアップ（急がせて聞き出す）」など、相手が正常に判断できない状況に追い込んで必要な情報を聞き出したり、相手に自分が求める行動を行わせたりするものがあります。

振り込め詐欺をはじめ詐欺全般には、こういった「人間の心の隙を突くソーシャルエンジニアリングの手法がよく用いられている」といわれています。

そして、デジタル世代のソーシャルエンジニアリングも、また、人間の心の隙を突くものなのです。

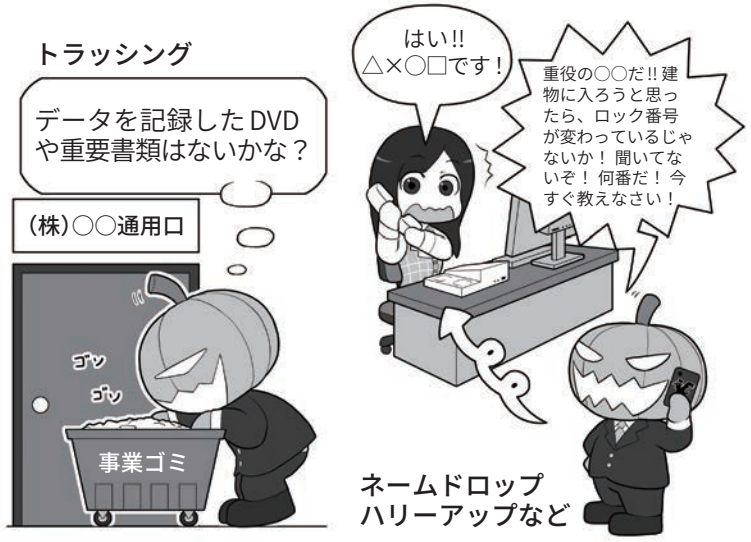
例えば、相手に直接接触せず情報を入手するものとしては、電車で座席に座っている人のスマホ操作を見て「PINコード」やパターンロック形状を盗む「ショルダーハッキング」、カフェなどのテーブルに放置されているスマホの画面に残る指の脂跡からパターンロックを見破る方法などがあります。事前に、ロック解除の手段を特定してから機会を見てスマホを盗めば、個人情報が丸ごと手に入ります。

また、メールで相手の心理的な隙を攻撃するのが「標的型メール」です。詐欺師が詐欺にかける相手をよく調べてから行動するように、標的型メールでは攻撃者が相手の名前、所属、身分、同じような会社でやりとりするメールのパターンなどを入手して、通常の仕事のメールと見分けがつかないほど精緻なものを送ってきます。そうして、会社のネットワークに侵入されたり経営層のふりをして送金を迫るビジネスメール詐欺（BEC）が行われたりするのです。

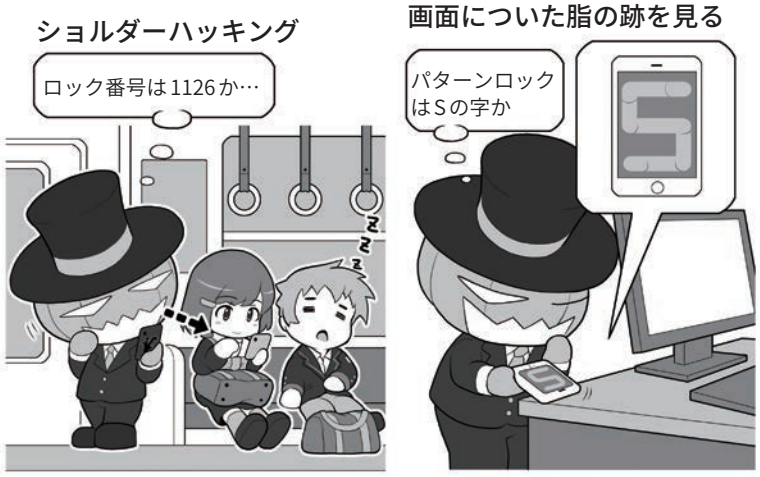
精緻な「標的型メール」がライフルによる狙撃のように狙った獲物だけを撃つものだとすると、「スパムメール」は広範囲を攻撃する手法として今でもよく使われます。

心の隙を作らないようにする（対ソーシャルエンジニアリング）

古典的なソーシャルエンジニアリング



デジタル世代のソーシャルエンジニアリング



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つけましょう。

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。

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

これには、フィッシング(=詐欺)メールを疑う手がかりがたくさんあります。まず、口座を持っていない人はそこで気づけるでしょう。表示しているリンクも、よく見ると、URLの末尾が日本を示すjpではなくgqになっています。しかし、こういったものでも一定の割合で引っかかる人がいます。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。「悪意はないが拡散してしまう例」の画面を見てください。このSNSアカウントが友達のアカウントだった場合、きっと本当に「このアプリが面白いと思って薦めているかも」と、あまり不審に思わないでしょう。

しかし、友達は知らなくても、実はこのアプリがマルウェア入りだったり、あるいは拡散する間は無害でも、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。

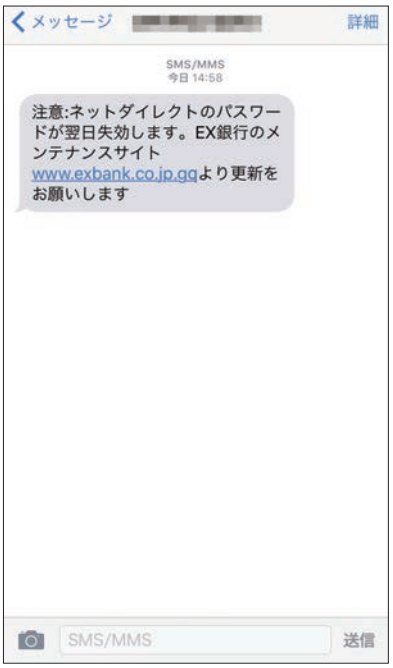
これが、他人の発信ならば警戒できますが、親しい友達や家族だった場合、警戒するでしょうか？

対抗策としては、こういったお薦め系のものは一つの線引きを持って接するようにしましょう。

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(ショートメッセージ)を使った例



悪意はないが拡散してしまう例

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つきあってよ」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。

コラム：クリックしてはいけない！フィッシング詐欺の傾向

近年、フィッシング詐欺の攻撃でもっとも目を引いたのは、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（ショートメッセージ）を送りつけて、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だま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つけてください」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。

その考え方からいえば、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考えられるので、同様に注意してください。

ほかにも、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「だまされないぞ」と身構えているのとは違う方向や、災害時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、送信元アドレスを確認したり、メッセージ中のリンクのアドレスをよく見ることなどで詐欺を見抜くこともできますが、それらは偽装することも可能なので、確認するだけで安全とはいい切れません。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。

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（https://www.antiphishing.jp/）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。

フィッシング詐欺はいろんな方法がある

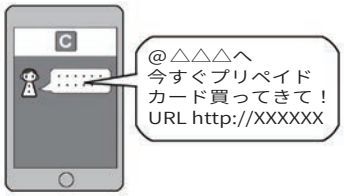
SMS（ショートメッセージ）

電話番号宛てに送る

電子メール（eメール）

メールアドレス宛に送る

メッセージ（アプリなど）



アプリのアカウント宛に送る

ゲーム内のメッセージ機能

ゲームのユーザー宛に送る

「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つけましょう。

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。

コラム：映画「ザ・ハッカー」にみるソーシャルエンジニアリング

ケビン・ミトニック（左）

ケビン・ミトニックは車で走りながら電話一本で人をだまし、情報を手に入れる段取りをします。

シモムラ・ツトム（右）

シモムラは、当初、後手に回りますが、そこから巻き返してミトニックを追い込んでいきます。

「ザ・ハッカー」は1999年に公開された、ハッカー対ハッカーの戦いを描いた、実話ベースの映画です。

原作はその登場人物のうちの一人「シモムラ・ツトム」が共著した『Takedown』という小説です。

相手のハッカー「ケビン・ミトニック」にも『欺術（ぎじゅつ）』などの著書があります。

原作では、シモムラがホワイトハット的に、ミトニックがクラッカー的に描かれていますが、映画では、その勧善懲悪的な雰囲気よりも、ハッカーとハッカーの意地とテクニックのぶつかり合いに重点を置いて描かれています。

この映画の注目するべきポイントは、「ハッカーの技術」とはなにかという部分です。特に、「凄腕ハッカーは目的のためならデジタルの世界に留まらない」ということに驚愕します。みなさんの中の「ハッカー像」が変わると思います。

ミトニックは劇中で、「ソーシャルエンジニアリング」を駆使し、人をだまして情報を手に入れたり、コンピューターセンターに堂々と入り込んで暗号解析をしたりします。

私たちの日常で、「要人のメールや個人情報が、電話が原因で盗まれた」といったニュースを目にすると、情報管理が緩いんだなと思ったりしますが、この映画を観れば、人間というものがどれぐらいあっけなくだまされ、どれぐらいあっけなく情報を流出させるのかを実感することができます。

見たほとんどの人は、「あんなことやられたら、絶対に逃げられない」といいます。

残念ながら、現在日本では、この作品を販売している会社がありません。中古のDVDを手に入れるか、有料のネット配信サービスで見つけたらぜひご覧になってください。

心の隙への攻撃にポイントを置いた、セキュリティの教材にもおすすめです。

ミトニックさんは現在では、ホワイトハットとして社会に貢献されています。罪を償って守る側に回ったミトニックさんはかなりクールですよ。

コラム：スパムメールとその由来

スパムおにぎり、スパムの味噌汁、スパムのソテー、スパムのポークオムレツは単品で存在しますが、スパムの姿煮はないだろ！　ドヤッ！（スパムの姿煮は執筆担当の夢です）

かつて、メールソフトを開くと、うんざりするほど広告や勧誘、フィッシングなどをする「スパムメール(spam mail)」が送信されてきていて、メールを見るのに滅入る(おっと失礼)時代がありました。

この、うんざりする多量のメールを「スパム(spam)」と呼ぶ由来はなにか。諸説ありますが、有力なのはソーセージの中身を缶詰にしたスパム(SPAM)と、これをネタにした英国のコメディ集団「モンティパイソン」のコントでしょう。

実際のコントの内容は、文字では表現できないナンセンス系なので、動画サイト検索で探し「考えるより感じろ」で味わってみて下さい。

そして、このコントの劇中での「スパム推しのウザさ」が当時のスパムメールの「ウザさ」とつながり、「spam mail」と呼ばれるに至ったのでしょう。

なお、SPAMを生産しているホーメルフーズ社は商品を大文字、スパムメールを小文字と表記することで、迷惑メールがスパムメールと呼ばれることを容認しています。

さて、とはいえ日本人にこのうんざり感を説明するのは難しいので、某グルメマンガをリスペクトしつつ、日本風にアレンジしたイラストを描いてもらいました。

「めいる百軒」と書かれた定食屋ののれんをくぐって、「おやじ！おまかせ定食！」と注文したら、これが出てきたと思って下さい。滅入るでしょ。

ところで、SPAMはすごくおいしいですよ！　姿煮以外は沖縄でお目にかかれます。ただ、さすがの沖縄でも、この完全スパム定食には出くわしたことはありませんけど(^o^)

第2章

サイバー攻撃にあうと、どうなるの？最新の攻撃の手口を知ろう

サイバー攻撃に遭うと、どんなことが起こるのでしょう。
また、サイバー攻撃では、あなたがいつも被害者とは限りません。
ときには気づかず加害者になってしまうこともあります。
そうならないように、サイバー攻撃の攻撃パターンを知ってこれに備えましょう。

1 攻撃者にIT機器を乗っ取られるとこんなことが起こる

1 被害に遭わない、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状態にします。

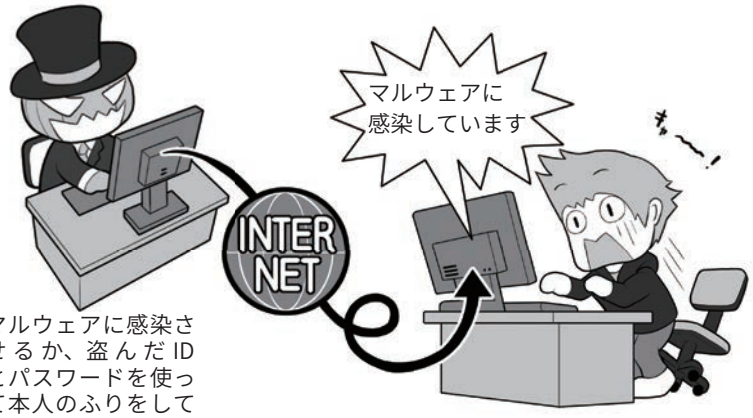
次に、別のパソコンやサーバなどに侵入するとき、「踏み台」にしてあなたのパソコンがやっているように見せかけたり、悪意のボットによるボットネットに接続させ、サイバー攻撃を行わせたりします。

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、もし重要な社会インフラに対して攻撃が行われ、実際に被害が出てしまったら、あなたは思い悩んでしまうでしょう。

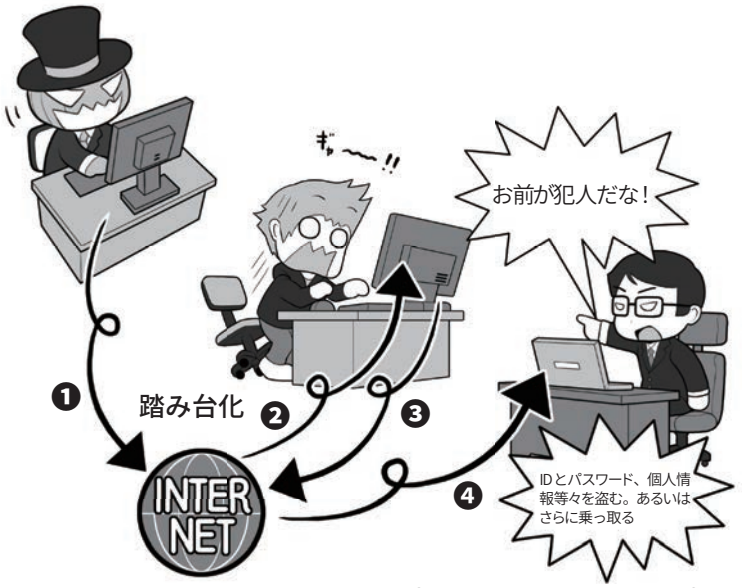
そうならないためにも、パソコンなどのシステムの状態は最新にし、セキュリティを固めましょう。もし、セキュリティソフトが、悪意のボットに感染していることを検出したら速やかに駆除します。一方、実害の出ている攻撃に関して、警察などから協力の依頼があった場合は証拠保全を行いましょう。

攻撃者によるパソコンなどの乗っ取り



攻撃者は、パソコンなどをマルウェアに感染させ乗っ取るほか、あなたのIDやパスワードがどこかから流出すると、それを入手して（あなたのふりをして）各種ウェブサービスや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」として遠隔操作用のマルウェアをインストールされると、その乗っ取りに気づくのは難しくなります。

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ほかの人のパソコンなど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ソフトを使って、フィッシング詐欺のためのメールなどを送信する場合などもあります。

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から不正送金で、お金を勝手に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方法もあります。

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。

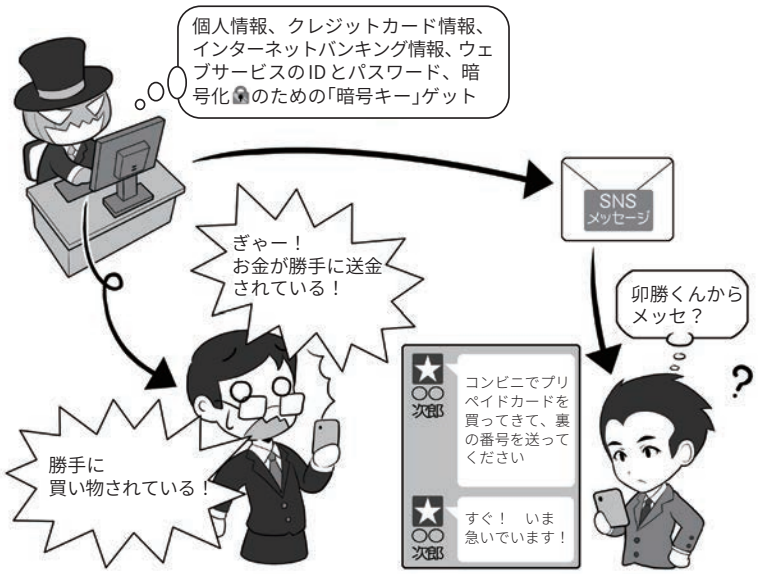
SNSのメッセージであなたになりすまし、友だちに対して「プリペイドカードを買って、アクティベーションコードを送ってくれ」と依頼し、電子マネーをだまし取る場合もあります。

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。この場合でも同様に、攻撃者は盗んだ情報からなんらかの手段で、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つけてください。

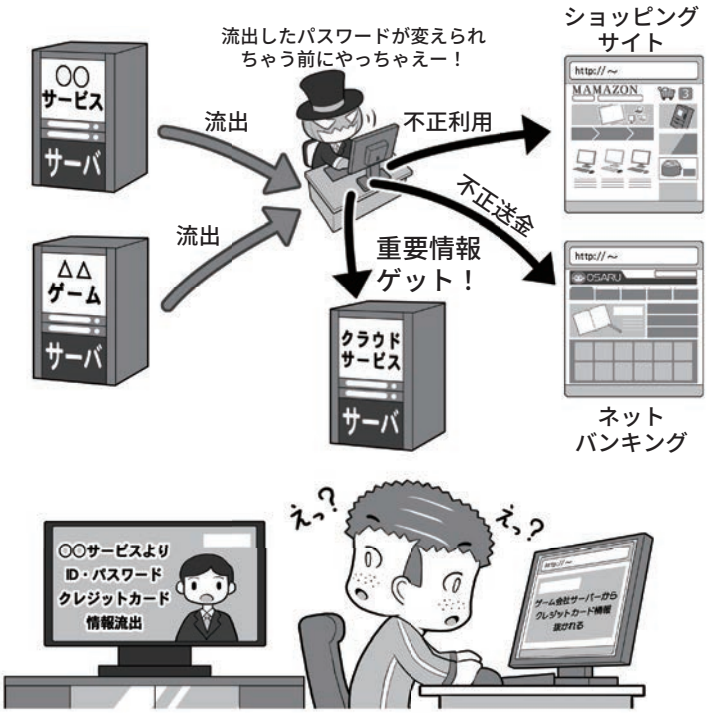
パスワード流出が判明したら、パスワード設定のセオリーにしたがいすぐに変更し、クレジットカード情報が流出したら、カード会社に連絡してカード番号を変更しましょう。

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、その被害は多岐におよびます。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す。パスワードの流出時は、各ウェブ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、ほかのサービスへの被害拡大はありませんが、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。

3 乗っ取られたIT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IT機器は、「ゾンビ化」といい、攻撃者に操られる状態となって様々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)」に使われるほか、「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。

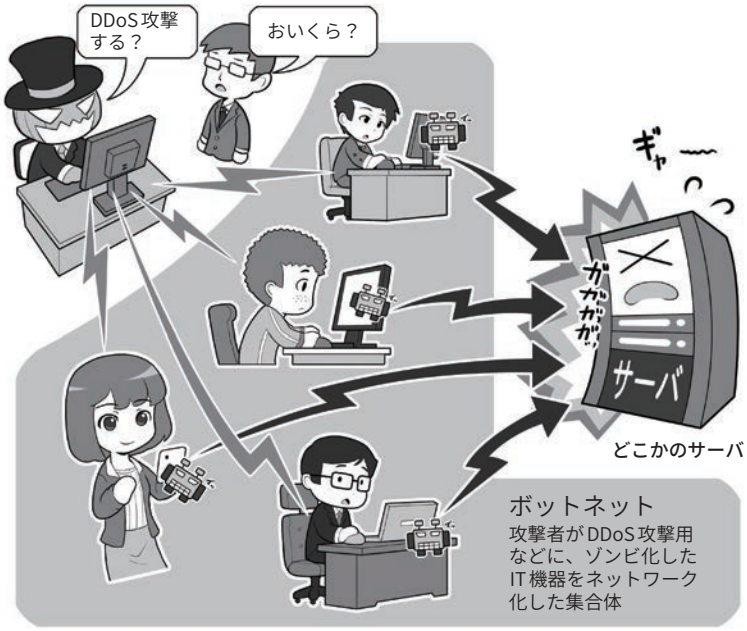
一方、「踏み台」的な攻撃はパソコンなどの乗っ取りによるものだけではありません。

「ウォードライビング」といって、車に乗って、会社や家の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、これに侵入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様々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、あなたを身代わりにして、攻撃がばれたときの追跡を逃れる方法です。

この場合、攻撃者に非があるのは当然ですが、自分の家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心中穏やかではありません。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IT機器はボットネットとして貸し出される

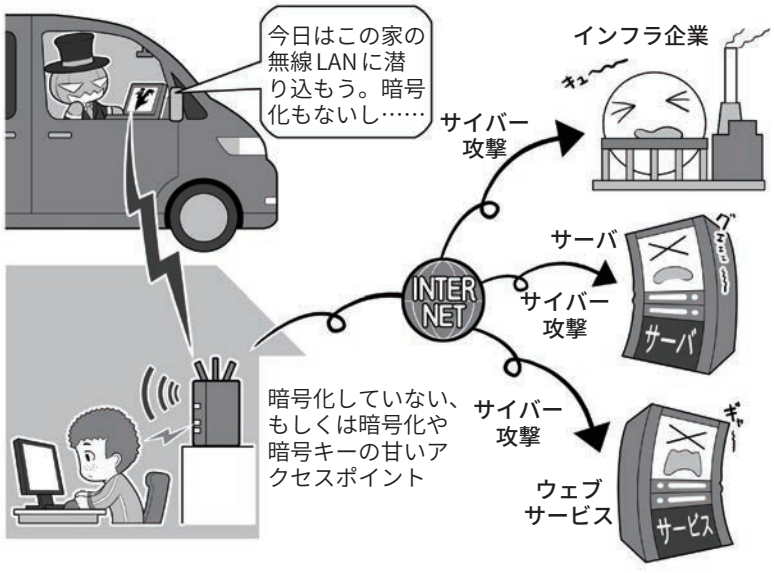


攻撃者によって、悪意のボットに感染させられ、遠隔操作されたパソコン(ゾンビPC)などの集合体がボットネットです。

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(P126)で時間あたりいくら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つけられることも



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。

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。IoT機器と呼ばれるネットにつながる電子機器はいずれも、乗っ取られて攻撃の身代わりとなる「踏み台」、DDoS攻撃用のボットネットへの接続、マルウェアの拡散など、様々なサイバー攻撃に利用される可能性があります。

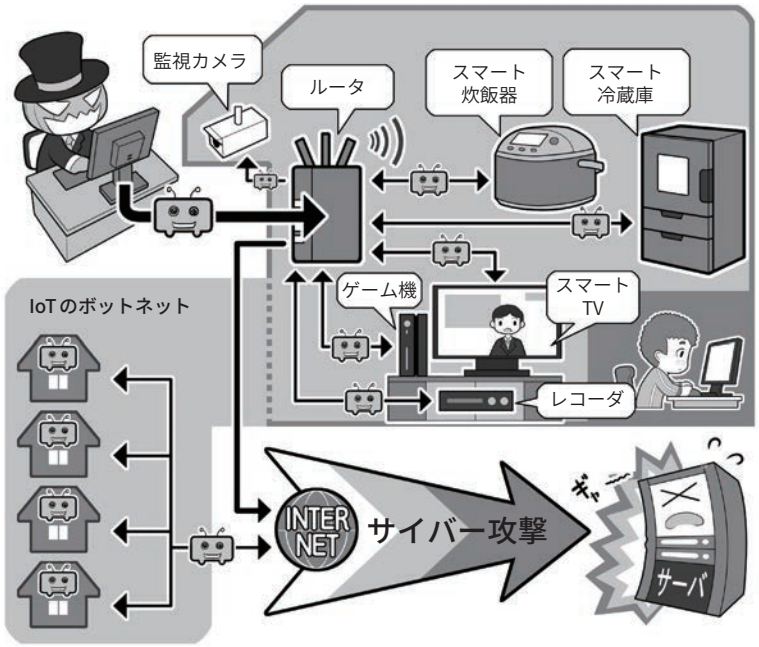
特に、IoT機器は監視カメラやスマート家電などのように、普段私たちがあまりセキュリティについて気にかけることがない機器であり、パソコンほどサイバー攻撃への対応能力が高くありません。そして、一つの機種で台数が多い＝手間をかけずに多数を攻撃できる、攻撃者にとって「攻撃しやすい条件」が揃っているのです。

最低でも、出荷時の「初期パスワード」はパスワード設定の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、マルウェアの拡散元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、マルウェアアプリだったりします。

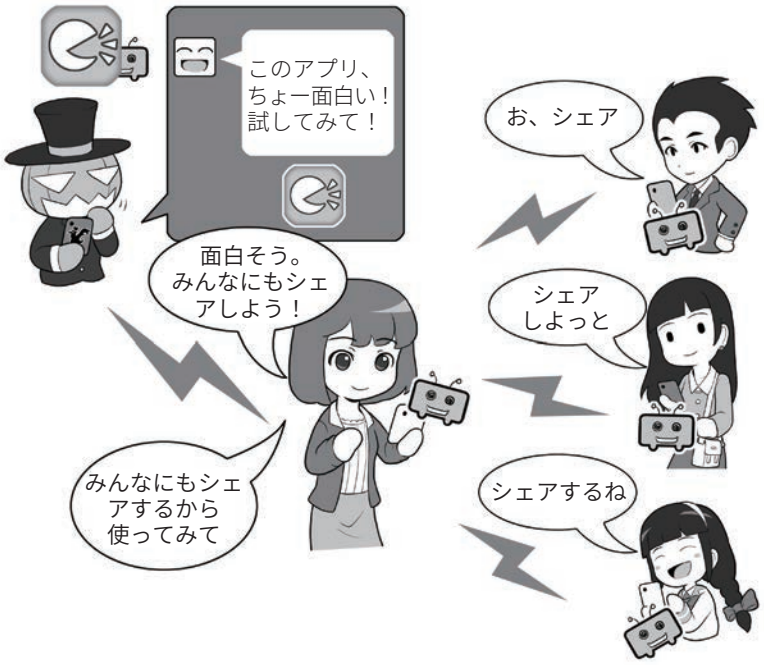
ネットでなにか行動する前には、必ず「それは本当に必要なのか」「なにか問題が発生する可能性はないのか」をいつも注意しましょう。

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もっています。攻撃者はそれらを乗っ取って様々なサイバー攻撃に使います。IoT機器は、最低でも「出荷時の管理者用パスワードの変更」「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」などの対応をしましょう。

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、その投稿の先にはフィッシングサイトが用意されていたり、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するかもしれません。拡散する前に、よく考えて「シェアする必要がないものはシェアをしない」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ません。

コラム：大きな脅威となっているランサムウェア

パソコンなどのデータを暗号化し開けないようにして、身代金を要求するランサムウェア。その大規模な感染に注目が集まっています。

例えば、2017年5月には、「WannaCry」と呼ばれるランサムウェアを使った大規模なサイバー攻撃が行われ、百数十カ国の20万台以上のコンピュータが感染したといわれています。

近年では感染経路が多様化しており、メールを経由して不審なファイルをインストールさせられるだけでなく、脆弱性の存在しているVPN機器を経由して外部から侵入されるケースも見受けられます。

また、脅迫の手法についても、暗号化したデータの復号をもちかけて身代金を要求することに加え、盗んだデータを外部に公開するという脅しをかけ、さらなる身代金を要求するケースも出てきています。

日本の大手企業がこのような新たな経路や手法により、被害を被った事例もありました。

こういったランサムウェアでは、身代金を支払ってもデータの暗号化を解除できなかったり、外部公開されたりするケースも多発しており、最悪の場合は端末を初期化しなければならず、大切なデータが失われることにもなりかねません。

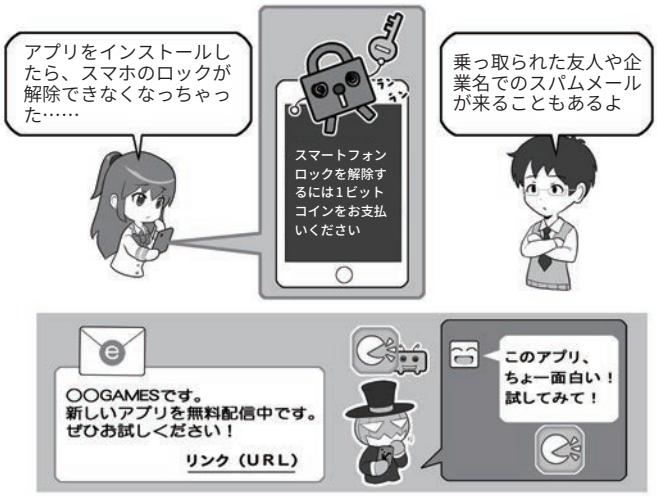
ランサムウェアに感染してこういった事態に陥らないよう、システムやアプリは最新の状態に保つ、データを常にバックアップする、必要に応じてセキュリティソフトを利用するなどの対策をしっかり実施しましょう。また、不審なメールのリンクをクリックしない、あやしいウェブサイトからソフトやアプリをインストールしないよう意識することも重要です。

万一ランサムウェアに感染した場合、まずは所属する組織のポリシーに則り対応してください。

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、感染すれば仕事などをする上で極めて重要なファイルも人質に取られてしまいます。バックアップは常にしておきましょう。

不審なアプリのインストール要求に注意



公式ストアでもマルウェアは発見されていますが、もっとも注意すべきは、それ以外の場所からのインストールです。こういったアプリは、不審なメールのリンクや、SNSの共有などでも回ってきます。大きなダメージを被る可能性もありますので注意しましょう。少なくともアプリのインストールは公式ストアからのみにしましょう！

コラム：仮想通貨の現在地1

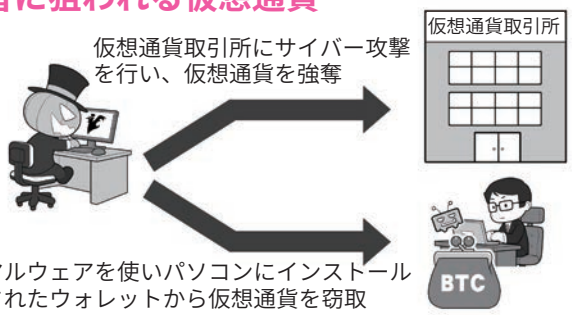
ビットコインなどの仮想通貨が広く流通しつつあります。投資などの面でも仮想通貨が現実世界での投資対象として使われ普及しつつあります。

しかし、注意しておきたいのは、仮想通貨の多くは国家発行の通貨と異なり価値の裏付けを行う者がおらず、最悪の場合、突然価値が0になり得るおそれがあることです。

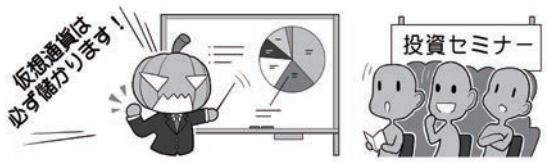
実際、仮想通貨は現実通貨に対する価値が乱高下することがあり、一般的な投資対象と比較してリスクが大きいようです。そして、まるで西部劇の世界のように、サイバー攻撃により仮想通貨を預かる取引所からの大規模な盗難や、個人のお財布(ウォレットという)から仮想通貨が盗まれるケースも頻発しています。

また、「仮想通貨は必ず儲かる」といった、投資詐欺も登場したこともあり、その特性や取り巻く環境を理解せずに手を出すことは、非常に危険性が高いと理解しましょう。

犯罪者に狙われる仮想通貨



仮想通貨を巡るサイバー攻撃も続発しています。実際、大手仮想通貨取引所がサイバー攻撃を受け、大きな金銭的被害が生じた事例があるほか、仮想通貨の窃取を目的としたマルウェアも登場しています。



仮想通貨をネタにした投資詐欺が増えています。どのようなものであっても、「必ず儲かる」という話はありえませんので、くれぐれもご注意を。

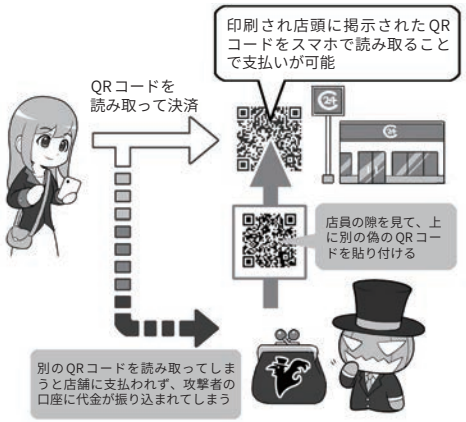
コラム：QRコード決済サービスで生まれた新たな詐欺

ITを活用して金融サービスを実現する、FinTechと呼ばれる取り組みが世界的に広まっています。具体的なFinTechサービスとしては、収入と支出、現預金などをスマホのアプリを使ってすばやく把握できるサービスや、スマホで手軽に決済できるサービスなどがその代表例として挙げられます。

そうしたサービスの1つとして、広まる兆しを見せているのが、QRコードを使った決済サービスです。店舗などで商品を購入する際、掲示されたQRコードをスマホで読み取り処理を行うと代金を支払うことができるというサービスです。中国などが先行し、最近は国内でも広く利用されています。

確かに便利なサービスですが、中国では印刷されたQRコードを別のものに貼り替え、代金を横取りする詐欺も過去に発生しました。日本でもQRコードを使った決済サービスが普及しつつありますが、今後同様の詐欺が発生する可能性もあるので注意が必要です。

QRコード決済の詐欺の流れ



まず、犯罪者が店舗に掲示されたQRコードの上に、別のQRコードを貼り付けます。利用者がそのQRコードを使って決済を行うと、代金は店主ではなく犯罪者の口座に振り込まれてしまうという流れです。

コラム：仮想通貨の現在地2

「仮想通貨の現在地1」のほかにも、近年は仮想通貨にまつわる大小様々なトラブルが度々発生し、世間を騒がせています。

一つは、ランサムウェアなどでパソコン・スマホのデータを暗号化した上でロックして、そのロックを解いて欲しければ身代金を払えと脅し、支払いをビットコインなどの仮想通貨で要求するものです。

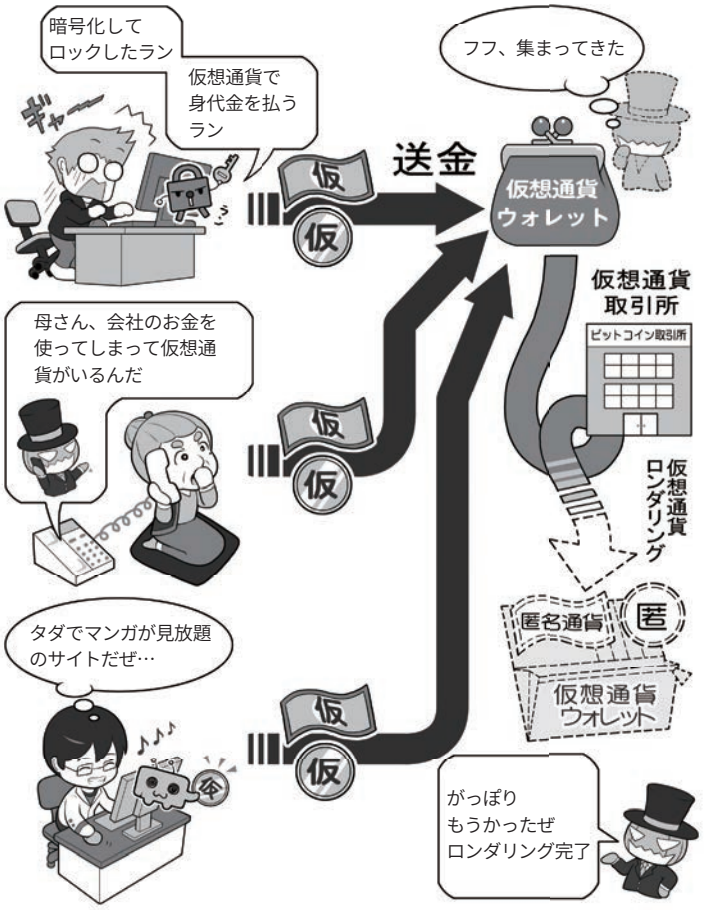
仮想通貨で要求する理由は、仮想通貨が全般的に「匿名性」が高く、不正に入手したり奪取したりしても、その後の追跡が困難だからです。また、一般に知られているビットコインなどの仮想通貨で受け取ったあと、支払先をばらばらに分散して追跡し難くし、その上で極めて匿名性の高い仮想通貨に換金（ロンダリング）して、追跡を逃れるなどの手法もあります。

こういった手法は、詐欺などで利用されるケースもあるので、「仮想通貨での支払い」ときたら、まず警戒する方がいいでしょう。

仮想通貨を入手するには売買するほかに、自分のパソコンなどで複雑な演算を解いて、その報酬として入手する方法もあります。これを、パソコンなどの保有者に断りなく、勝手に行う攻撃もあります。不正にマンガなどを閲覧できるウェブサイトに行くと、その裏で勝手に仮想通貨を得る演算をさせられた例がありました。そもそも、そういったウェブサイトを見るべきではありませんが、それと同時に、特定のサイトを開いたら突然パソコンの動作が遅くなった、といった場合には注意が必要です。

仮想通貨は最近、全世界における演算による電力消費が中堅国1国分よりも多くなり、規制も厳しくなりつつあることで価値の下落が進んでいます。1項にあった、「必ず儲かる」といった話に引っかからないのと同様に、仮想通貨関連でだまされないように、上記の図の内容にもご注意ください。

著名な仮想通貨を匿名性の高い通貨にロンダリングして逃げる



仮想通貨はもともと匿名性が高いのですが、攻撃者はそれをさらに匿名性が高い仮想通貨にロンダリングすることで、追跡を困難にして逃げます。

コラム：フェイクニュースとサイバープロパガンダ

デマと似たようなものとして、「フェイクニュース」という言葉が注目集めています。

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もので、これが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拡散され、結果的に見た人はそれを真実だと思ってしまうといったことが起きています。

フェイクニュースには、意図を持って発信している人のほかに、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、1つの悪意のビジネスモデルになりつつあります。

検索エンジン企業やSNS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。

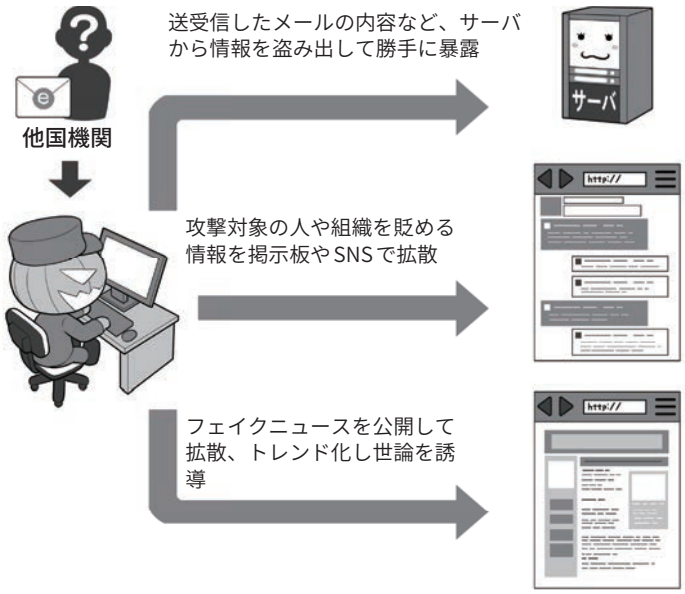
プロパガンダ自体は、古くから国家が自国や他国に対して影響を及ぼすために、行われてきた「人を思いどおりに動かそうとする情報の悪用法」ですが、これがネットを使うことで高度化かつ秘密裏になり、人々が気付かぬ間に、その考え方が操作される事態が起きているのです。

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、国と密接な関係にあるメディアでの偽ニュースの発信、ボットを使ったSNSでの偽ニュースのトレンド化、政治的な争点になっている事柄の賛否両方にSNS上で広告を打つことで混乱を生み出し国民を分断、そして、SNS上で架空の人格のアカウントを作りインフルエンサー(有名人)に成長させ、他国の人々を自国に有利になるように扇動するなどといった、様々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。

私たちが希望を持つインターネットでは、一方でそういった悪意をもった人々が暗躍しているということを理解し、手元に来た情報をそのまま鵜呑みせず、また、短絡的にシェアなどの共有をせず、一呼吸置いてその真贋を見極めたり、本当にシェアなどの拡散をするべきか冷静に判断したりすることが求められています。

なぜなら、サイバープロパガンダには、私たちが「深く考えず情報を拡散する習性」までもが組み込まれているからです。悪意のある人の駒にならないように気を付けましょう。

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、トロールと呼ばれる情報操作グループと「いいね」や「シェア」を押す自動のボットによりこれをトレンドにのせ、さらに、ターゲットの国の「自分にマッチした情報を好んでシェアする」人たちのSNS集団(エコーチャンバー)にこれを投げ込み、最終的にそのほか大勢に、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。

コラム：軍事スパイ、産業スパイに狙われてしまったら

スパイではない攻撃者は、コストパフォーマンスでターゲットを選ぶ傾向がありますが、では、逆にスパイはどのように行動するのでしょう。

軍事スパイや産業スパイの場合、入手するべき情報は絶対であり、侵入しにくいからといって別の情報にすることや諦めることはできません。

こういった攻撃者の場合、活動するための資金は自分でまかなわなくても、国家だったり軍だったり、あるいは産業スパイでも、独立して活動して情報を売る者でなく、スポンサーの企業から活動資金を得ている者なら、コストパフォーマンス度外視で攻撃をしかけられるわけです。

興味がある方は、一般のスパイの教本をお読みになると、目的のためにはどれぐらい容赦ないことをするのか理解できるでしょうし、それが理解できれば、あとはネットの世界のサイバー攻撃に置き換えればいいわけです。

なお、ネットが全盛になる前のスパイ活動は、相手国の新聞や雑誌など公開されているものから情報収集するオシント、人間関係を調べたり尾行したり、交友関係を持って情報を聞き出すヒューミント、そして、通信を傍受や盗聴して情報を入手するシギントがありました。

ネット社会の現代では、SNSを見ればある程度ヒューミント的な情報は入手できますし交友関係も丸わかりです。また、シギントもマルウェアに感染させてメールを盗み見たりファイルを奪取したり、スマホの通話を盗聴できたりもします。

少なくとも、相手がSNS好きの人間なら一般人でも楽にヒューミントもオシントもでき、これがサイバー時代のインテリジェンスといったところでしょうか。

要職にある方々は、SNSなどに不必要に情報を流さないようにしましょう。あなたの行動のすみずみまで、その情報は誰かに見られていますよ。

第3章

パスワード・Wi-Fi・ウェブ・メールのセキュリティを理解して、インターネットを安全に使おう

私たちの、安全なインターネット生活を支えるパスワード、Wi-Fi(無線LAN)・ウェブ・メール。
それらを安全に利用したり、その内容を盗聴や流出から守る暗号化など、
セキュリティについての理解を深めましょう。
初心者向けとしてはやや難しい項目ですが、なるべく平易な言葉で解説していきますので、
ぜひ読んで、セキュリティへの理解を深めてください。

1 パスワードを守る、パスワードで守る

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。

なお、こういった役割を担うものには、ほかに「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。

2 3種類の「パスワード」を理解する

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や、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使われているもの（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、実に様々なものがあります。P34でご紹介したのは、上記のうちの2にあたります。

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。

3 「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

P34では、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」として、英大文字小文字＋数字＋記号混じりで少なくとも10桁以上を推奨しました。

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桁以上で良いとしています。

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）」と呼びます。「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。

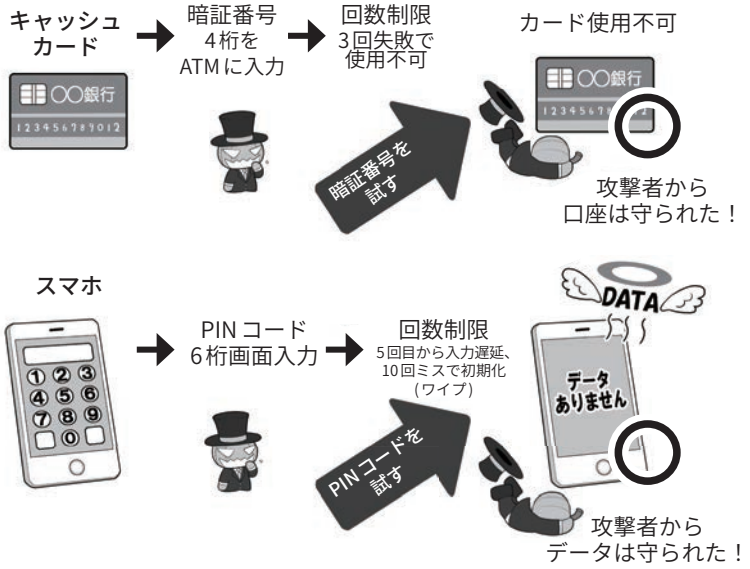
一方、「ログインパスワード」は、通常「PIN コード」のようにワイプまでする機能がついていることはほぼありません。数回失敗すると入力間隔が開く、一定時間入力をロックするなどのペナルティを受ける場合もありますが、ペナルティがないものも多いのです。

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。

本書の推奨どおり、英大文字小文字＋数字＋記号 26 種＝88 種類の文字を使い、10桁のパスワードを作ったとすると、その組み合わせは約2785 京個（京は兆の上の単位）、1秒5回の制限で「総当たり攻撃」をした場合、全部を試すまでに約1760億年かかるわけです。

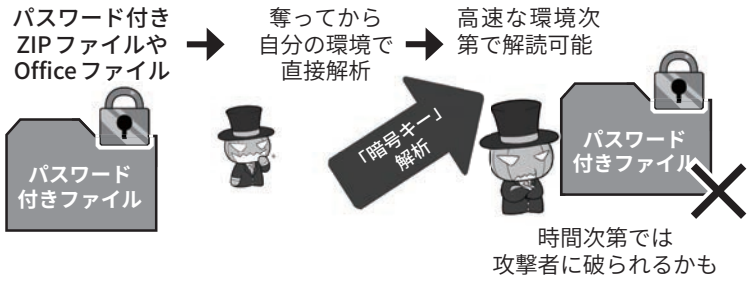
3種のパスワードを理解する

①「PIN コード」の例



②「ログインパスワード」の例

③「暗号キー」の例

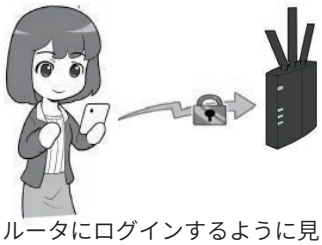


わかりにくい例

「ログインパスワード」か「暗号キー」か分からない例

暗号化された記憶装置 (ハードディスクや SSD) の救済に関して、「ログインパスワード」なのか「暗号キー」なのか分からないものを求められたら「暗号キー」と考えましょう。

無線 LAN アクセス時にパスワードのように入力する文字列



ルータにログインするように見えますが、ログインパスワードではありません。「暗号キー」を自分の機器に設定しているだけなので、「暗号キー」の基準で設定します。

※この図は一例であり、実際の機器の条件とは異なります。

これならば、100年以内に探り当てられる確率は非常に小さく、事実上不可能といえるわけです。

このような攻撃の想定を、セキュリティ用語的には「オンラインアタック(攻撃)」といいますが、ここでは「『ログインパスワード』への攻撃」と呼ぶことにします。

4 「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、自分のペースで暗号化解除(解読)の高速攻撃ができます。

この攻撃の対象となるのは、「複数のファイルをまとめたパスワード付き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。

こういったものでは、「パスワード」と思って設定しているものが、実はパスワードではなく、中身を読まれないようにするための暗号化に使われる鍵=「暗号キー」となっている場合が多いのです。

ZIPやMicrosoft Officeのファイルは、パスワードが設定されていると、開くときにパスワード入力画面が出るので、入力遅延の防御があるように見えますが、実はその画面はZIPやOfficeのプログラムが提供しているもので、ファイルそのものは単なる暗号化されたデータにすぎないのです。

そのため、パスワード入力画面を使わなくても直接ファイルに対して暗号化解除の攻撃が可能であり、遅延による防御はありません。

このような暗号化解除は、「暗号キー」が短いと、スーパーコンピュータを使うまでもなく、普通に市販されているゲーム用パソコンの性能で十分可能です。そういったパソコンの、グラフィックボードに搭載されているGPUというプロセッサーを駆使すれば、ZIPファイルに対して40億回/秒の暗号化解除の攻撃が可能というデータすらあります。

この場合、先ほどの約2785京個の組み合わせがある場合でも、解読までにかかる期間は78.5万年に短縮、8桁のものになると103年、8桁で記号抜きの62種の文字だと6年、英大文字小文字だけだと2年となり、GPUの性能が向上すればそのうち、数日単位で可能になるでしょう。それは、もう「解読可能な領域」といえます。

そのため本書では、「暗号キー」には、完全にランダムで英大文字小文字＋数字＋記号混じりで15桁以上のものを推奨し、これを基準とします。

ZIPのパスワードに、15桁ものランダムな文字列を使うのは、覚えられなくて無理だと思われるでしょうが、8桁程度のパスワードでは破られてしまうので、暗号化したつもりでも攻撃者の前では意味がないのです。

なお、このような想定の攻撃をセキュリティ用語的には「オフラインアタック(攻撃)」と呼びますが、ここでは「『暗号キー』への攻撃」と呼ぶことにします。

5 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」のほかにも様々な手法があります。

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、かつほか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」を利用するのも一つの手です。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。

ただ、指紋認証などの生体認証も100%安全とはいい切れません。最近では、どこかで撮影した相手の指の写真から、3Dプリンターで偽の指紋を作って認証を突破したり、顔を印刷した紙を加工して、それを使って顔認証を突破したりする実験も行われています。

また、指紋認証が携帯電話に登場したときから、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。最近では、親が寝ている間に子どもが勝手に認証し、ゲームに課金していたという例もありました。

したがって、勝手に認証される可能性がある環境では、「PINコード」入力が必要になるよう、わざと生体認証を数回失敗させて、それ以上勝手に生体認証できない状態にするなどの工夫が必要です。

生体認証はこのほかにも、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。

「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。この暗号キーが、事実上漏れた状態になる話は、P64以降で詳しく説明します。

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

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

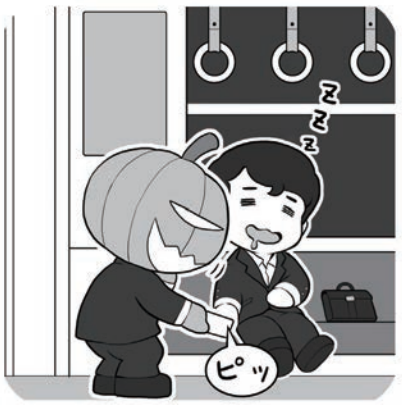
辞書攻撃（ディクショナリアタック）

パスワードでよく使われる単語を使って試す

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）

指紋認証が破られることも…



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PINコード入力が必要な状態にしましょう。

6 多要素認証を活用する。ただしSMS認証は避ける

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二要素認証以上の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。

もっとも一般的なものは、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（ショートメッセージ）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成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、または生体認証を推奨します。

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ので、より快適なパスワード管理を求めるならば活用しましょう。

また、パスワードをネット経由で送信しない方式の採用も推進されています。より安全な利用のために、アンテナ高く情報収集しましょう。

7 二段階認証と二要素認証と多要素認証の安全性

ウェブサービスのアカウント乗っ取りを防ぐための追加の認証。

この認証のために用いる要素には下図にあるように、「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。

この要素を、二つ用いて行うものを二要素認証、それ以上に用いて行うものを多要素認証などと呼びます。

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等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。

従って、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、例えば攻撃者がこれを突破しようとすると、物理世界で窃盗や脅迫を行わなければならず、ネットの影に隠れたまま行える犯罪よりもリスクが高くなり、安全性が高まります。

それでも、「知っていること」と「持っているもの」の組み合わせであるキャッシュカードが、オレオレ詐欺などであっさり奪われたり、P76に解説しますが、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絶対安全と思い込まないで下さい。

常に「自分は、狙われているかもしれない」「攻撃されているかもしれない」「もしかしたら、これは攻撃かもしれない」という危機意識を持つようにして下さい。

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

ソフトウェアトークン
（ワンタイムパスワード生成）

USB
セキュリティ
キー

生体認証
（指紋認証など）

アプリから認証

推奨できないもの

SMS（ショートメッセージ）や
メールでワンタイムパスワード送信

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

8 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、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。

ただし、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、その原因も特定しましょう。

原因が、マルウェアなどでパソコン側から情報が流出し続けている場合、その穴を解明しないまま放置していると、パスワードを変更しても意味がありません。

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。

9 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と言えるので利用は再考しましょう。

10 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。どう管理すればいいのでしょう。

本書では、「スマホ用のパスワード管理アプリ」か「物理的な紙のノート」の利用を推奨します。

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

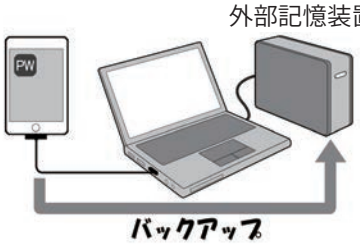
ウェブブラウザにはパスワードを保存しない

ウェブブラウザにパスワードを保存すると、席を離れたとき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

一見分かりにくい専用の紙のノートに二重で

管理アプリのデータは、暗号化した外部記憶装置にバックアップ



紙のノートに二重に記入したり、スマホのパスワード管理アプリを使って、パソコン経由で外部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ノートも売られています。

ものを優先しましょう。

紙と比較した場合、スマホはネットに接続されているので、攻撃者にクラッキングされる可能性は捨てきれませんが、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。

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し、管理アプリも独自に暗号化するので二重に暗号化された金庫での保管に等しくなります。加えてスマホは、事前にきちんと設定しておけば、紛失や盗難に遭っても遠隔操作でロックして操作できなくしたり、場合によってはワイプ(消去)して情報流出を避けたりできるという、紛失に対する三重四重のセキュリティが設けられています。

一方、紙のノートを推奨する理由は、あたりまえではありますが、紙のノートはネットに接続できないからです。接続できなければネット経由のサイバー攻撃も不可能です。奪うには現実世界で「盗む」という行動を起こさなければならず、攻撃者が姿を現すリスクがあることが抑止力になるからです。

11 パスワード情報をクラウドで保管する善し悪し

パスワード管理アプリや、同様の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。

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ことも管理することもできません。

また、パスワード管理アプリのデータがスマホ上にある限りは「PINコード」方式で守られますが、クラウドのバックアップデータが流出すれば、マシンパワーにものをいわせた高速なオフラインアタック、暗号化解除の攻撃が可能になるからです。

銀行の口座からお金が盗まれれば、自分にミスがない限り銀行が補填してくれますが、クラウドから流出した情報は実質的に回収不可能です。これは、「お金は補填が可能だが、重要情報の秘密性は戻らない」からなのです。

パスワード管理方法のメリットデメリット

	利便性	盗まれたときの対策	ネット経由のセキュリティ	データの管理者
紙のノート	△ 持ち歩き可でも落とすと読まれる	× 家にあると盗まれにくいが、盗まれると対応できない	○ 攻撃不可	本人
スマホアプリ	○ ロックしたまま持ち歩き可	○ バックアップがあれば復元可能	△ 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、一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。

12 ノートやスマホを失くした場合のリカバリ考察

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。ただ、スマホの場合、パソコンでスマホのデータを丸ごと暗号化してバックアップをしておけば、紛失しても代替機をパソコンに接続し「復

元」を指示するだけで、環境やパスワード管理アプリの内容を含めて、すべて元の状態にできるものもあります。

また、スマホを丸ごとバックアップしなくても、パスワード管理アプリのデータを、パソコン経由で暗号化された外部記憶装置などにバックアップし、普段は接続せず適切に保管しておけば、復旧は容易です。アプリによっては紙に印刷して保管する機能もあります。

なお、クラウドサービスのメリットとデメリットを理解した上で、クラウドを使った複数機種での連携機能、自動バックアップやそれに付随するリカバリ機能を利用するのは一つの選択肢といえます。

紙のノートの場合は、紛失したときに備え2冊同じものを作り、一つは金庫に保管するなどのバックアップ手段を取りましょう。

紙のノートによるパスワード管理は、平文で書いてあるものを持ち歩いて紛失してしまった場合、中を見られないような制限はかけられませんので、一見してもパスワードが分からない、専用のノートを利用するのが安全でしょう。

13 注意するべきソーシャルログイン

機器やウェブサービスのパスワードは、使い回しをしないのが絶対です。しかし、膨大な数のパスワードを暗記するのは非現実的なので、必然的にパスワード管理アプリやパスワード管理のノートを使う必要があります。

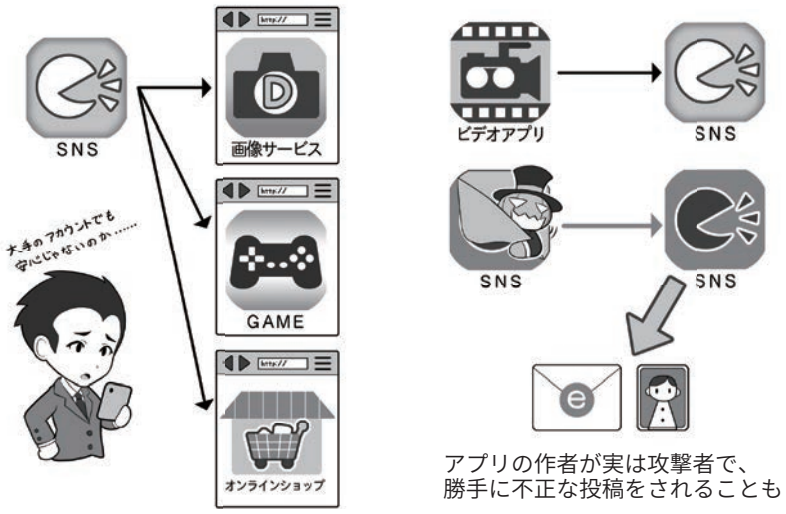
この手間は、情報漏えい対策のために「パソコンのウェブブラウザにIDやパスワードを覚えさせる機能(＝自動入力)」を使わないならなおさらです。

これを解決する策として、「ソーシャルログイン」という方法が用いられて来ました。これは、IDとパスワードの管理がしっかりしたウェブサービスのアカウントで、ほかのウェブサービスにログインして利用するというものです。

しかし2018年時点で、最大手SNSサービスから、ソーシャルログインで用いられる身分証明の証(トークン)が流出するトラブルがあったため、本書では、ソーシャルログインを非推奨として、基本的にそれぞれのサービスは別々のIDとパスワードを設定することのみを推奨することとします。

トークンが流出すると、IDとパスワードが流出しなくても、ソーシャルログインを設定していたサービスに根こそぎアクセスして

ソーシャルログインとサービス・アプリ連携の違い



ソーシャルログインは、堅牢なサービスのアカウントを別のサービスの鍵に使え便利ですが、大本のアカウントの認証情報が漏れる事案が発生したため、それぞれのサービスに別々のパスワードを使用する基本対応を推奨します。

アプリなどの連携は定期的に棚卸ししよう

自分が意識的に連携をしていなくても、ネット経由で回ってきた「面白いアプリ」を利用したら、いつの間にか連携されていたということもあります。また、そのときは問題がなくても更新時に権限の拡張を求めてきて、結果的に個人情報を「合法的に」奪うアプリも存在しています。

アプリ連携やアプリの権限は、定期的に棚卸をして、不必要なものや不審なものは連携解除するか、削除するようにしましょう。

しまえる可能性があるからです。

一方、それぞれのウェブサービスを利用するときに、別々のIDとパスワードを入力する手間を省くために、パスワード管理アプリが進化し、ウェブサービスやアプリのログイン時に、自動的に入力してくれる機能も登場してきました。多要素認証などの使い捨てパスワード入力も楽になっています。

それらを活用し、パスワードの使い回しをせず、ストレスなくルールを守るようにしましょう。

14 権限を与えるサービス連携にも注意

ソーシャルログインと混同されやすいものに、SNSに関する機能で「サービス・アプリ連携」というものがあります。

例えば、AというSNSにBというサービスやアプリから、投稿を認めるといったものです。具体例としては特徴的な機能を持つカメラアプリにSNSへの写真付き投稿を認めるといったものがあります。

これは、ソーシャルログインとは別の性格の機能ですが、ときに「連携するアプリやサービスに投稿を認める(＝権限を与える)」という部分が、攻撃者の手段として利用されることもあるので、利用は避けるようにしましょう。

SNSを利用していると、自分が意識しないうちに誤操作をし、知らずにサービス・アプリ連携していることもあります。

定期的に使用しているSNSアカウントの「連携を確認できる画面」を開いて、知らないアプリや止むを得ず使ったサービス・アプリの連携があれば解除しましょう。

コラム：暗号化の超簡単説明

暗号化とは、自分と相手だけが読めて他人は読めないという、セキュリティを保つ技術です。

暗号化というと非常に難しく感じるかも知れませんが、大丈夫、その心配にはあたりません。

ただ、暗号化の内容を詳しく書くとそれだけで本になってしまうので、ここではその概念だけをごく簡単に説明します。

1．暗号化とは「魔法をかけて手紙などの内容を読めないようにする」ことです。

2．暗号化の魔法にはいくつもの系統(方式)があり、魔法をかけるには呪文(「暗号キー」)を決めて使います。

3．魔法の呪文(「暗号キー」)がばれると、魔法が解けて内容が読めてしまいます。

4．古い系統の魔法の中には、その仕組みに不備があり、呪文が分からなくても解けてしまうものがあります。

初歩としては、このぐらいの理解があれば大丈夫です。

使用する暗号方式が安全かどうかは、魔法研究の専門家に任せましょう。車がどうやって動くのか知らなくても、安全な利用ができるのと同じです。

大切なのは、正しい使用法を知ることと、専門家が「危険が発生した！」という情報を発信したらキャッチし、迅速に避けるように行動することです。

右のイラストでは、具体的に危険が発生する例を描いていますので、是非覚えておいてください。

まず第一歩は、「正しく使うこと」からです。

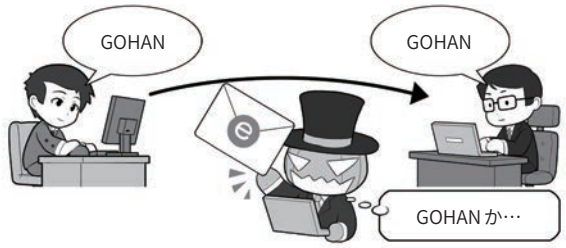
Cipher Disk(シーザー暗号)

もっとも原始的な暗号は、シーザー暗号といわれるものです。文字をずらして記述するだけのシンプルなもので、仕組みさえ分かればアルファベットなら26回試すまでに暗号が解けてしまいます。

上の図は、その暗号を解きやすくするためのCipher Disk（暗号円盤）です。現代の暗号は複雑な演算を伴うために、人力での解読はほぼ不可能です。

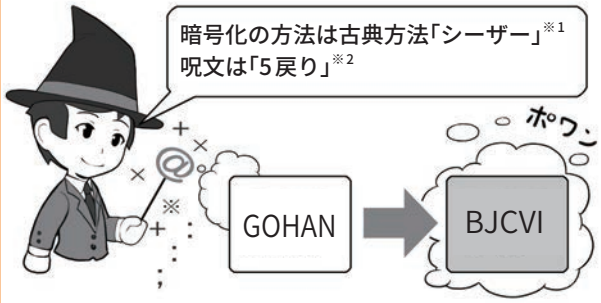
暗号化ってなに？

平文での通信は読めてしまう



暗号化していないと、攻撃者はどこでも盗んで読み放題

暗号化の魔法は内容を読めなくする



※1：暗号化方式　※2：「暗号キー」

暗号化したものを送れば攻撃者が読めない

※ただし、攻撃者が「シーザー暗号」を読めない場合

事前に決めておいた方法（暗号化方法）と呪文（「暗号キー」）で暗号文を復元（復号）する

暗号が破られる場合

暗号化方法の種類はいろいろ

シーザー暗号化方法
×　古い、危険すぎ

「WEP」方法
×　解読されるからだめ

「WPA」方法
○　呪文が長ければ安全

暗号破られる例①　呪文がバレている

暗号破られる例②　方法が古くて解読可能！

暗号破られる例③　呪文が簡単すぎて解読される

※このページは、抜き出して個別に使用することを想定して、本文と一部内容が重複しています。ご了承ください。

コラム：パスワードの管理と流出チェックについて

ここでは、パスワードの管理に関する最新の動向を踏まえて、本文でも紹介したテクニックを詳しく解説しましょう。攻撃者から身を守るためには、最新の技術で先手を打つのも一つの対策だからです。

パスワードに関して、2018年には約16億件のパスワードが流出したというニュースが流れました。また、有名ホテルチェーンが顧客情報約5億件を流出させたニュースも報じられました。こうして流出したIDとパスワードは、必ずといっていいほど不正アクセスに使われます。そういった攻撃から身を守るには手段は2つ。1つは、流出しても被害を最小限にとどめるため、サービス毎に別々の長くて複雑なパスワードを設定すること。もう一つはそもそもパスワードを盗めないようにすることです。

● パスワード管理アプリの高度な利用

パスワードに関して、NISCでは、「人は必ずヒューマンエラーを起こす」ことを前提に対処方法を考えます。例えば、パスワードの管理は数が多くなるほど覚えにくく、使い回しをせずサービス毎に別々のものを考えるのは面倒で、対策せずに強要すると、そのうちワンパターン化したり、同じ物の使い回しが起きたりするのではないかと考えます。

これを解決するため、総合的にパスワードを管理する、スマホの「パスワード管理アプリ」などを推奨します。パスワード管理アプリは、単にパスワードを保管してくれるだけではなく、条件を設定するとそれに合わせた長くて複雑なパスワードを自動的に生成してくれるほか、最近では、ウェブブラウザでのサービスログイン時に、自動的に起動してIDとパスワードを入力したり、アプリ起動時にもIDとパスワードを入力してくれたりするように進化しているものもあります。パスワードを、いちいち管理アプリを見て入力したり、カット＆ペーストしたりする手間も省きつつ、みなさんの負担を軽減する傾向にあるのです。

また、パスワード管理アプリの中には、多要素認証で利用する使い捨てパスワードを発生するためのQRコードを、アプリ内に読み込めるようになっているものもあります。多要素認証で使い捨てパスワードを利用する設定にすると、サービスそれぞれが別々の「ソフトウェアトークンアプリ」をインストールさせるように見えて、実は必要なのはこのQRコードを読み込ませることだけなので、パスワード管理アプリに読み込んで、一括して管理するようにできるのです。

加えて、パスワード管理アプリによってはスマートウォッチとの連携を行っているものもあります。これらのアプリでは、スマートウォッチにインストールされた連携用のパスワード管理アプリ上で、登録しているIDとパスワード、多要素認証用の使い捨てパスワードを発生させることもできるので、パソコンでウェブサービスへのログインに際して、スマホを立ち上げなくても、手元でログインに必要な情報をすべて確認できます。

これらを使って、楽に個別のパスワードを管理しましょう。どういったアプリが条件を満たすのか評価記事などを参考に検索して、利用するときは責任関係がしっかりとする有料のものを選択しましょう。無料のアプリには情報を抜き取ることを目的とするものも紛れ込んでいるからです。

● パスワードを無くすFIDO

主としてパスワードが流出するのは、サービス側で保管しているIDとパスワードを含めた個人情報が、多量にまとめて盗まれるケースです。したがって、サービス側に盗むべきパスワードがない場合は、この攻撃は成功しません。そのためにパスワードそのものを無くすことを目指すのがFIDOアライアンス（Googleやマイクロソフト、NTTドコモといったIT企業や通信会社、信販会社、通販会社などが加盟）が進めるFIDOという方法です。この方法では、利用者が「本人」

であるという認証をパソコンやスマホなどそれぞれの機器の上で行い、利用するサービスへは「本人だと認証しました」という情報のみをやりとりするのです。本人だと認証する方法は、USBセキュリティキー、指紋や顔認証などの生体認証です。

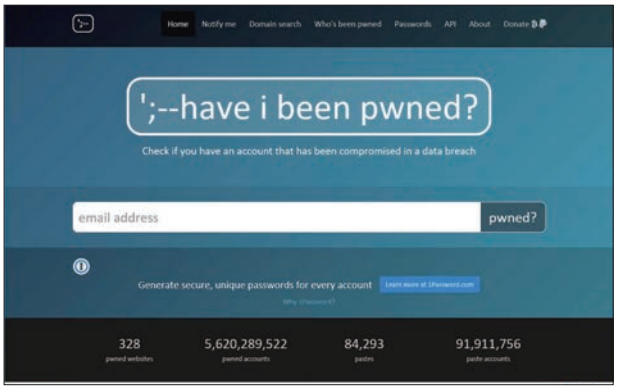
現在Googleのサービスの一部で利用が始まっているほか、最近はAndroidスマホ本体のFIDO2対応や、WindowsへのログインWindows Helloに対応した端末などがFIDO2に対応しています。

今後これらの方式が普及してきた場合、積極的に選択することも検討しましょう。少なくともGoogleの社内では、FIDO2対応USBセキュリティキーを採用することで、フィッシング詐欺の被害がゼロになったと報告されています。

パスワード管理と認証の新しいトレンド

ハードウェアメーカーが推奨し、密接に連携するパスワード管理アプリと対応スマートウォッチや、FIDO対応機器。これらの導入がセキュリティの向上に役立ちます。

流出IDとパスワードチェックサイト「Have I Been Pwned?」（私、漏洩してる？）



メールアドレス流出チェックURL：https://haveibeenpwned.com/
パスワード流出チェックURL：https://haveibeenpwned.com/Passwords/

ほかにもFirefox Monitorなどで、同等の機能が提供されています。
実績もありセキュリティ業界において評価は高いですが、あくまでも民間のサービスなので、その点を理解して利用しましょう。

● パスワード流出を能動的に検知する

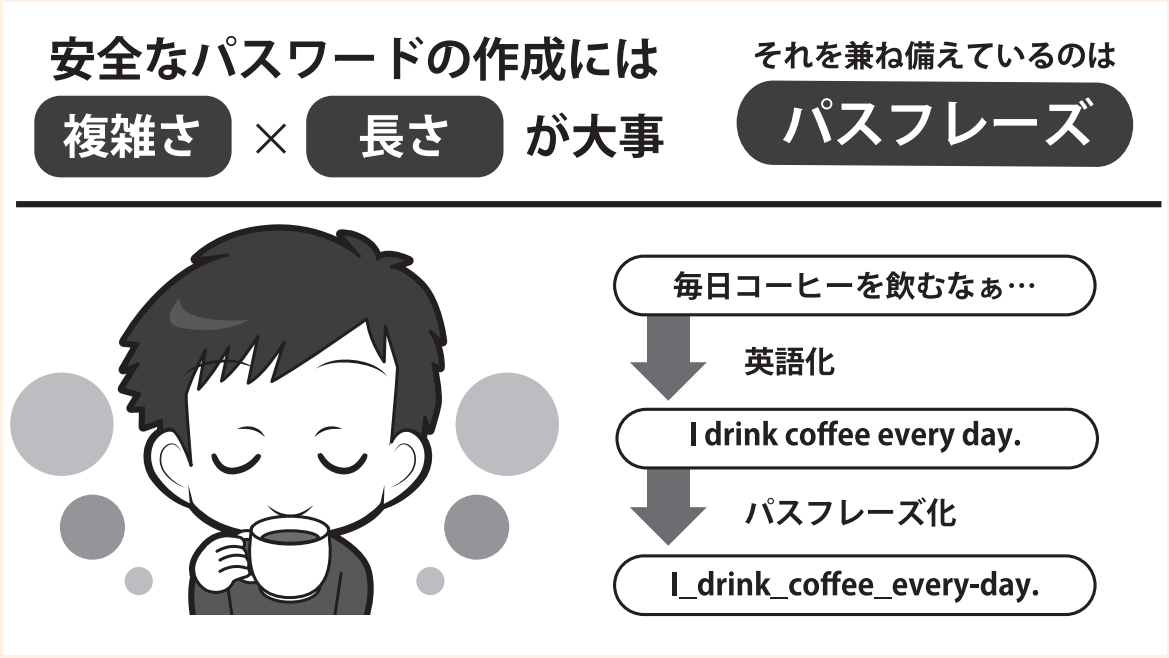
パスワードの流出は、登録しているサービス側から流出の事実が通知されるほかにも、流出情報の検索サイトを利用すれば能動的に調べられます。

セキュリティ識者のトロイ・ハントさんが、流出したIDとパスワード情報を収集し検索できるようにした「Have I Been Pwned?」は、各国政府によって政府系メールアドレスの流出チェックなどにも使われていますし、個人でもウェブサイトで自分のIDとパスワードが過去に流出していないかチェックできるほか、アドレスを事前に登録しておくと流出時に警告のメールが送られてきます。

また、パスワードを入力して、そのパスワードが「流出した履歴あり」と出た場合、それは、あなたの情報の流出であってもほかの人の情報の流出であっても、以降パスワードリスト攻撃の対象になるので変更しておきましょう。

根っこは同じデータベースを用いますが、ウェブブラウザを提供しているFirefoxもFirefox Monitorとして同様のサービスを提供しているほか、パスワード管理アプリでもパスワードの安全性チェックに採用する動きが見られます。今後こういった流出情報のチェックサービスは増えていくと予測されるので積極的に活用して、攻撃される前に対処するようにしましょう。

コラム：パスフレーズを使う生活がくるかも？しれない



パスワードの安全性を高める為には複雑で長いパスワード（英大文字小文字＋数字＋記号で10桁以上）を設定することが大切です。（P34「パスワードの安全性を高める」参照）

安全なパスワードの作成には「複雑さ」と「長さ」の両方がしっかりと兼ね備えられていないといけません。その両方を兼ね備えつつ、作成する際にあまり悩まずに作成でき、かつ本人が覚えやすいものとして、パスフレーズが利用される場合があります。

パスフレーズとは、文字列を使ったパスワードの事です。例えば毎日コーヒーを飲む人であれば「I drink coffee every day」を「I_drink_coffee_every-day」とパスフレーズ化するということです。自分だけしか知ることのできない情報を文章化することで、ある程度の複雑さと長さの両方を兼ね備えた、覚えやすいパスワードを作成する、という考え方です。

なお、パスフレーズを作成する時、使用する時は、パスワードと同じ点に注意する必要があります。

いくら自分だけしか知ることのできない情報であっても、上述の例のようにごく簡単な単語や固有名詞を使ってパスフレーズを作成してしまうと、第三者からすぐに推測されたり、割り出されてしまう可能性が高まります。また、複数のサイトで同じパスフレーズを使い回してしまうと、どこかのサイトから流出してしまった場合、第三者にその情報を使用され不正アクセスされてしまう可能性があります。また多要素認証や生体認証も合わせて設定できる場合は積極的に導入するようにしましょう。

サイト名：
ID／ユーザー名：
パスワード：

メールアドレス：
メモ：

サイト名：
ID／ユーザー名：
パスワード：

メールアドレス：
メモ：

サイト名：
ID／ユーザー名：
パスワード：

メールアドレス：
メモ：

サイト名：
ID／ユーザー名：
パスワード：

メールアドレス：
メモ：

サイト名：
ID／ユーザー名：
パスワード：

メールアドレス：
メモ：

サイト名：
ID／ユーザー名：
パスワード：

メールアドレス：
メモ：

サイト名：
ID／ユーザー名：
パスワード：

メールアドレス：
メモ：

サイト名：
ID／ユーザー名：
パスワード：

メールアドレス：
メモ：

サイト名：
ID／ユーザー名：
パスワード：

メールアドレス：
メモ：

2 通信を守る、無線LANを安全に利用する

私たちが、日常的にインターネットで送信するIDやパスワード、送受信するメールの文面やウェブサイトで閲覧する内容は、常に攻撃者の盗聴や盗み見の危険にさらされています。

攻撃者は、そうした情報を不正に入手して売却したり、様々な手段を駆使して直接お金を手に入れるために利用したりします。これを阻止するためには、通信している情報の暗号化が必要なのです。

そもそも、インターネットはその始まりにおいては、暗号化など全くされておらず、情報をそのままの状態(平文)で送受信するシステムでした。

インターネットは、蜘蛛の巣状に接続し合ったサーバ間で、どこかの経路が遮断されても迂回して通信を続ける、そういう面では先進的ではあったのですが、攻撃者などの悪意の存在を前提に構築されてはいなかったからです。

その後、インターネットの発展にしたがって、悪意を持ったものが現れ、コンピュータウイルスの開発や、パスワードを破って侵入しての情報の奪取、通信中の情報の盗聴が行われるようになり、それぞれ対策が必要になりました。

コンピュータウイルスにはウイルス対策ソフトが、パスワード破りには複雑なパスワードや二要素以上の多要素認証などが、そして、通信中の情報の盗聴には暗号化が、攻撃者への防御として普及していくわけです。

1 それぞれの状況に合わせた暗号化の必要性

一口に通信の暗号化といっても、様々な状況に合わせた、それぞれの暗号化があります。

私たちが通信すること一つをとっても、有線LAN、LTEなどの携帯電話回線、Wi-Fiなどの無線LAN、多様な通信手段があります。

このうち、攻撃者にとって、手軽に行いやすい攻撃の一つとして無線LAN通信の盗聴があります。

無線LANでは、その名のとおり通信機器が無線(電波)を使って通信するので、盗聴に際してなにか工作する必要はありません。通信が暗号化されていなければ、無線LANに対応したパソコンを持って電波が届く範囲にいるだけで、簡単に盗聴することが可能です。

なお、有線通信も暗号化されていなければ、通信経路上のどこかで情報を盗聴することが可能です。

さらに、攻撃者が利用者のふりをしてメールサーバやパソコンに侵入すれば、中にたまったメールや、内蔵記憶装置などの中の情報も盗み見し放題です。

パソコンがマルウェアに感染して、記憶装置の中の暗号化されていないファイルが流出し、見放題になるという事件もありました。

そういった状況を避けるためには、仮に盗聴されたり、侵入されたり、流出してしまっても、通信内容や重要なファイルの中身が見られないように、それぞれのシーンに応じた適切な暗号化をする必要があります。

その対策をあげていくと数え切れないのですが、このセクションでは、まず私たちの生活でもっとも身近な無線LAN通信の暗号化について説明しましょう。

2 無線LAN通信(Wi-Fi)の構成要素

インターネットに接続した無線LANアクセスポイントさえあれば、いちいちLANケーブルをつながなくても、気軽にインターネットを楽しめる無線LAN通信(Wi-Fi)。

家庭で利用する無線LANでも、外出時に利用する公衆無線LANでも、セキュリティがしっかりしていなければ、通信中に送信したIDやパスワード、データすべてを攻撃者に盗まれる危険性があります。

それを理解するために、まずは無線LAN通信を構成する要素を理解しましょう。

最初は、無線LAN通信を提供する「無線LANアクセスポイント」になる機器。一般には「無線LANアクセスルータ」「Wi-Fiルータ」あるいはシンプルに「ルータ」などと呼ばれます。この機器で無線LAN通信を提供する際、最低限以下の3つを設定します。

① 識別名「SSID(Service Set Identifier)」
②通信内容を暗号化するための「暗号化方式」

③その暗号化のための鍵となる「暗号キー」(設定上は暗号化キーと書かれる)

「暗号キー」は、利用者が無線LANアクセスポイントに接続するときパスワードのように使われるほか、通信内容を暗号化するときと、元に戻す復号(元の平文に戻す)のときの鍵として使われます。

ここまでが、無線LANアクセスポイントの構成要素です。

スマホやパソコンが無線LANを利用して通信するときは、利用する機器の無線LAN(Wi-Fi)設定で、SSIDを手掛かりに目的の無線LANアクセスポイントを見つけ、必要な場合は暗号化方式を選択し、「暗号キー」を入力して接続します。

なお、災害時や公益目的で、誰でも無線LANを利用できるように、「00000JAPAN(ファイブゼロジャパン)」を筆頭に「暗号化無し」で提供されている無線LANアクセスポイントもあります。この場合は利用時に暗号化方式も「暗号キー」も必要ありません。

次に、無線LANの危険要素について説明します。危険なポイントは以下の2つになります。

①「通信が暗号化されていないか、されていても安全ではない場合」
②「暗号化の鍵(「暗号キー」)が公開か漏れている場合」

3 暗号化無しや、方式が安全ではないものは危険

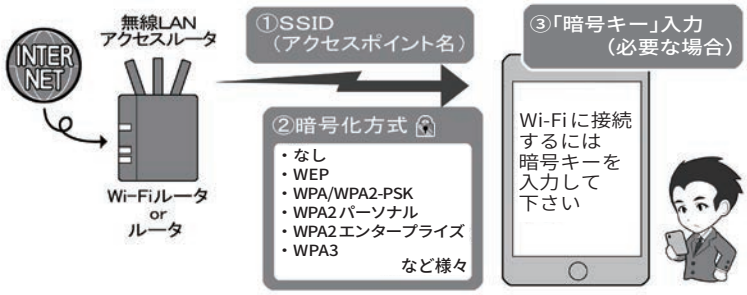
無線LANの利用において、通信が暗号化されていないものは、内容が平文で送受信されているので、別の手段での暗号化を行わないま

それぞれの状況に合わせた暗号化

通信の暗号化　**ファイルの暗号化**

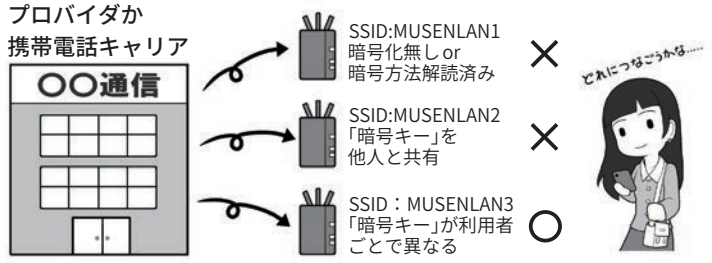
暗号化には、電話、メール、ウェブ閲覧などの「通信の暗号化」と、ファイルやパソコンの記憶装置などの「ファイルの暗号化」があります。

暗号を使う無線LANの構成要素



暗号化を伴う無線LAN通信には暗号化方式と「暗号キー」の設定が必要となります。「暗号キー」は機器に接続するときにパスワードのように使われます。

公衆無線LANが安全とは限らない



信頼がおける企業や団体でも、提供しているWi-Fiが安全とは限りません。アクセスの利便性のため暗号化無しで提供される場合もあるからです。

「暗号キー」共有は接続しちゃダメ

暗号化方式が安全でも、「暗号キー」を見知らぬ他人と共用するものは、すべて危険です。こういった方式は、公衆無線LANやホテル、公共機関、インターネットカフェやレストランなどで広く使われています。

提供する側が善意で行っていても、攻撃者は善意で行動しません。攻撃できる環境があると判断するだけです。

安全な通信のため、自前で暗号化を行うテクニックがなければ利用不可です。

ま使っていると、攻撃者に内容を盗聴されてしまいます。

そのため、まず「暗号化無し」のアクセスポイントは基本的には利用しないようにしましょう。

災害時など、例外的に使用する場合は、後述の「10 公衆無線 LAN が安全でない場合の利用方法」を参照してください。安全な利用には最低限、別の手段での暗号化が必要だと覚えておいてください。

暗号化無しの通信は、拡声器で遠くの人と話しているようなもので、耳を傾ければその場にいる誰もが内容を知ることができます。

また無線 LAN 通信が暗号化されていても、その暗号化方式がすでに破られていて安全ではない場合、上記と同様に、攻撃者は通信を盗聴して内容を解読することができるので、これも危険です。使用しないようにしましょう。

これは、「英語でしゃべればわからないだろう」と思ったら、周りにいた人も英語が理解できて、内容がばれるイメージです。

危険である暗号化方式の具体例としては、「WEP」という名前のものや、方式の名称の中に「TKIP」と含まれるものが該当します。

一方、暗号化方式として安全とされるのは WPA-PSK(AES)、WPA2-PSK(AES)、WPA2-EAP、WPA2- エンタープライズ、IEEE 802.1x、SIM 認証、そして、無線 LAN の多くの問題点を解決するために作られた WPA3、それらの記述があるものです。安全な方式の詳細は P69 を参照してください。

4 暗号化方式が安全でも「暗号キー」が漏れれば危険

暗号化の方式自体が安全でも、通信を暗号化するための「暗号キー」が漏れていると、通信を盗聴した攻撃者が通信内容を復号したり、同じ SSID と「暗号キー」を使って偽の無線 LAN アクセスポイントを作り、本物のアクセスポイントになりすまして通信内容を根こそぎ奪う、中間者(Man-in-the-middle)攻撃を行ったりすることができるようになります。

イメージとしては、破られていない暗号化方式は誰も知らない言語で、「暗号キー」が辞書。しかし、辞書がほか人の手に渡っていると、たとえ知られていない言語でも解読されてしまうし、その情報をもとに通信する相手になりすますこともできる、というものです。

この至極単純な、「暗号キーが漏れていれば暗号化された通信を復号し解読できる」ということも、よく覚えておいてください。

5 家庭内での安全な無線 LAN の設定(暗号化方式)

家庭内で無線 LAN を使用する場合、先ほど説明した安全な暗号化方式である WPA-PSK(AES)、WPA2-PSK(AES)、WPA3 を利用し、「暗号キー」を P54 の基準にしたがって、完全にランダムで充分に長くして、さらに、その「暗号キー」を「家族だけが知っている」状態に保てれば、ほぼ安全に使用することができます。

これを実現するため、無線 LAN 機器設置時には、まず機器を購入したときの初期の「暗号キー」は変更しましょう。上記のとおり、家族だけしか知らない「暗号キー」に変更しなければなりません。メーカーによっては「暗号キー」が共通だったり、付け方に規則性があるかもしれないからです。

また、極端な考え方をすれば、その機種がメーカーから手元につくまでに、初期の「暗号キー」を見たものがいないともいい切れません。

なお、SSID を変更する場合、自分や家族の名前、家族を想起させる語句は使わないようにしましょう。あなたが攻撃のターゲットの場合、攻撃するべき無線 LAN を特定させるヒントになるからです。

家庭用無線 LAN アクセスルータは、標準で 2 つ以上の SSID を持てるものが多く、そのうちの一つには、WEP などのもはや安全でない古い暗号化方式が設定されている場合があります。これは、主に古いゲーム機などが接続できるようにするためだったりします。

しかし、こういった設定はセキュリティ上の穴となるので、設定を変更し、安全な暗号化方式にするか、安全でない暗号化方式の設定のものはすっぱりと停止しましょう。また、接続する古い機器が安全でない暗号化方式しか選べないならば、使用は諦めましょう。

同様に、来客用に簡便な「暗号キー」や、問題のある暗号化方式を使った接続設定があれば、これも停止しましょう。来客に家族用の SSID に接続させるのも安全ではありません。「暗号キー」が「家族だけが知っている状態」ではなくなってしまうからです。

どうしても来客用に一時的にアクセスポイントを開放したい場合は、2 つの SSID の一つを来客専用にし、2 つのアクセスポイントの間で、お互いのアクセスポイント

に接続した機器が見えないような分離状態に設定してから提供しましょう。そして、来客が帰宅したら、そのSSIDは利用停止しましょう。

6 家庭内での安全な無線LANの設定（そのほか）

無線LANアクセスルータには、ウェブブラウザを使って本体の設定画面にアクセスするための、機器管理用のIDやパスワードがあります。それは、管理者アカウントとも呼ばれます。

こちらのパスワードも、必ず購入時のものから変更しましょう。このパスワードはログイン画面から使用するものなので、「ログインパスワード」の基準に従い変更しましょう。

この設定画面が、もし家の中からだけでなくインターネット側からアクセスできるようになっていたら、アクセスできないように変更しましょう。また、設定画面が無線LANで接続した機器からアクセスできず、有線LANからのみアクセスできる設定にしましょう。この設定をする理由は、家の外にいる攻撃者が姿を隠した上で無線LANに接続し、設定内容を変更したりしてしまわないようにするための予防策です。

無線LANアクセスルータにルータ本体と機器のボタンを押すだけで簡単に接続できる「WPS」「AOSS」「無線LANらくらくスタート」といった名称のもの、もしくは類似の機能がある場合は利用不可にしましょう。この設定をONにしていると、目を離したすきに、利用してほしくない人物が、ボタ

家庭でのWi-Fiの利用

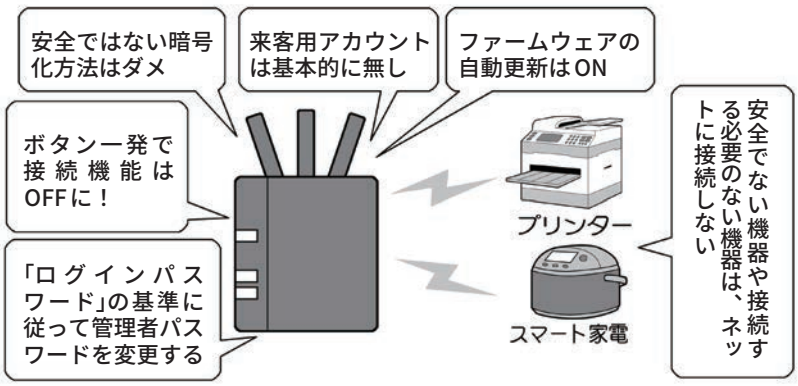
①出荷時の管理者パスワード、「暗号キー」の変更

出荷された機器は、厳密にいえば誰かの手によって梱包されているので、出荷時の「暗号キー」が見られている可能性があります。必ず変更しましょう。

②「暗号キー」は家族のヒミツ

家庭で使える暗号化方式は、「暗号キー」を家族のみの秘密にすることが、安全に使うための絶対条件です。ほかの人には教えないようにしましょう。

③ルータと機器の安全な運用



家庭で無線LANや有線LANを使用する場合、注意したり設定を変えたりしなければならない点がたくさんあります。必ずチェックして安全な状態を作りましょう。また、基本的に接続する必要がない機器を、むやみに家庭のLANに接続しないようにしましょう。

ン一発で手元の機器を無線LANに接続できてしまうからです。

どうしても利用する場合は、設定画面からそのときだけONにして使用し、設定後はOFFにします。

UPnP（Universal Plug and Play）の設定も、不用意に家庭内のLANの機器をインターネット上に公開してしまう可能性があるので、OFFにします。そして、ネットに接続する必要のない機器は、無線・有線にかかわらず、そもそもLANに接続しないようにしましょう。

無線LANアクセスルータの設定画面に、本体ファームウェアの自動アップデート機能がある場合はONにしておきましょう。それによりメーカーがルータの不具合（バグ）などを修正した場合、自動で更新が行われセキュリティが最新の状態に保たれます。

もし自動アップデートの設定がない場合は、自分のスマホに定期的な通知を作り、それにしたがってファームウェアが更新されていないかチェックし、公開されていれば更新処理を行いましょう。

なお、昔に書かれたセキュリティの解説記事によっては、「SSIDを隠すステルス設定」や、接続できる機器をLAN機器の番号で制限する「MACアドレス規制」を対策として推奨していたりします。

しかし、ステルスになったSSIDも簡単に探し出すことが可能ですし、MACアドレスは盗聴可能かつ詐称可能ですので、これらの対策を行っても安全性は向上せず、むしろ利便性が悪くなるので、設定する意味はないでしょう。

無線LANアクセスルータは、家庭のセキュリティの要です。お使いのルータに上記のようなセキュリティの設定がない場合や、安全な暗号化方式の設定がない古い機器の場合は、速やかに利用を停止し最新のものに買い換えるようにしましょう。

7 公衆無線LAN利用時の注意

公衆無線LANの安全な利用は、家庭用の無線LANの安全な利用と少し事情が異なります。

例えば、公衆無線LANで「WPA-PSK（AES）/WPA2-PSK（AES）」の方式の無線LANが提供されていた場合、暗号化方式自体は安全でも、別の危険があります。

上記の名称の中のPSKの部分はPre-Shared Keyの略です。利用にあたり「暗号キー」を事前に共有する方式のことで、この方式では家庭内の利用のときと同様に、複数の人で同じ「暗号キー」を使うことになります。これを公衆無線LANに当てはめると、全く知らない人と、同じ「暗号キー」を一緒に使うことになるわけです。

その設定を使って通信を行うと、「暗号キー」を知っている攻撃者により、通信内容を直接盗聴されたり、なりすまし無線LANアクセスポイント（偽アクセスポイント）をしかけられ、通信内容が盗聴される可能性を避けられません。

しかし、この方式を含め安全でない暗号化方式は、街中のカフェやレストラン、ホテル、あるいはインターネットプロバイダや携帯電話キャリが提供する公衆無線LANでも広く使用されています。これらのアクセスポイントはすべて危険ということになります。

こういった危険なアクセスポイントを使用する場合、無線LAN通信の暗号化とは別の暗号化機能で対処する方法もがあります。それについては後述します。一方、安全な暗号化方式の選択で安全性を確保する方法もあります。

8 個別の「暗号キー」を用いる方式の公衆無線LAN

公衆無線LANにおいて通信の安全を確保する方法は、危険な暗号化方式などを使わないことは当然として、「暗号キー」を他人と「共有しない」で個別の「暗号キー」を用いる方式を利用することです。

この方法は、公表されている公衆無線LANアクセスポイントの情報の中で「WPA2-EAP、WPA2-エンタープライズ、IEEE 802.1x、SIM認証」といった用語が含まれるものを選択するのです。

携帯電話キャリアなどは、いくつかの異なる暗号化方式の公衆無線LANを提供している場合があり、ウェブサイトなどで、それぞれのSSIDが採用している暗号化方式が、きちんと掲示されている場合があります。

利用前にそこをチェックし、上記の方式名を頼りに、安全な接続ができる公衆無線LANのSSIDを探してから利用しましょう。

「WPA2-EAP、WPA2-エンタープライズ、IEEE 802.1x、SIM認証」などが公衆無線LANとして安全である理由は、これらの方式の無線LANアクセスポイントを利用する場合、公衆無線LANサービスの提供者が、利用する一人ひとりの機器、または、利用者を識別して個別の認証を行い、個別の「暗号キー」を用いて通信を行うからです。

そのため、他人と同じSSIDに接続しても、自分の「暗号キー」を他人に知られることがないのです。

一例を挙げると、「SIM認証」と呼ばれる方式では、それぞれのスマホなどに入っているSIMカードの情報を用いて認証＝接続許可を出すわけです。SIMは1枚1枚別々の情報が入っているので、誰かと「暗号キー」が被ることなく安全な通信が確保されるわけです。

9 公衆無線LANに関して新規に購入したスマホなどで行うこと

新規契約や機種変更、携帯電話会社の乗り換えなどをして、携帯電話キャリアで新しいスマホを手に入れたら、まずやるべきことがあります。

そのスマホには、携帯電話キャリアで提供している様々な方式の公衆無線LAN用の自動接続設定が、安全性に関係なくまとめて導入されていることがあるからです。

購入後、細かい設定をしなくても自動的に公衆無線LANに接続できるので便利と思われがちですが、この状態では、意図せず「安全でない方式の公衆無線LAN」に、接続してしまう可能性があります。

新しいスマホなどを手に入れたら、まず接続される可能性があるアクセスポイントの暗号化方式を調べましょう。安全でない公衆無線LANのアクセスポイントに接続してしまった場合、無線LAN接続を切断して、その接続用のプロファイルも削除し、できれば二度とそのアクセスポイントに自動接続されないようにしましょう。

また、知らない公衆無線LANア

公衆無線LAN通信の表示の意味

①スマホやパソコンの画面から見た無線LAN暗号化

接続	Android	iOS、mac OS	Windows
×（暗号化無し）			
△（暗号化有り）			 ＊1

②詳細な区分けから見た無線LAN暗号化

接続	ネットワークの種類	暗号化キー（「暗号キー」）		解説
×	暗号化無し		なし	暗号化無しは論外
×	WEP		事前入手	解読済み。使用は不適切
×	WPA-PSK WPAパーソナル	（TKIP）	事前入手	TKIPには暗号化にセキュリティ上の不安あり。AESは暗号解読不可能とされているが、「暗号キー」が事前に存在し、利用者はみな同じものを共有するので、暗号解読の可能性あり
△		（AES）	事前入手	
×	WPA2-PSK WPA2パーソナル	（TKIP）	事前入手	
△		（AES）	事前入手	
○	WPA2-EAP＊2 WPA2エンタープライズ	（AES）	SIM認証（端末個別）＊2 個別パスワード、クライアント証明書認証（利用者個別）	SIM認証ではSIMの情報を認証に用い、個別の「暗号キー」が利用されるので通信内容の不正な解読は困難。ほかにも利用者を個別に認証するEAP-TTLS,EAP-TLSなどの方式もある

上の表は、Android、iOS、mac OS X、Windowsなどで、無線LANアクセスポイントを選択するときの画面に表示されるアイコンの例になります。それぞれ2種類のアイコンしかありません。そして、このアイコンは、各アクセスポイントが信頼できるかを表しているのではなく、単純に「暗号化されているかどうか」だけを表しています。

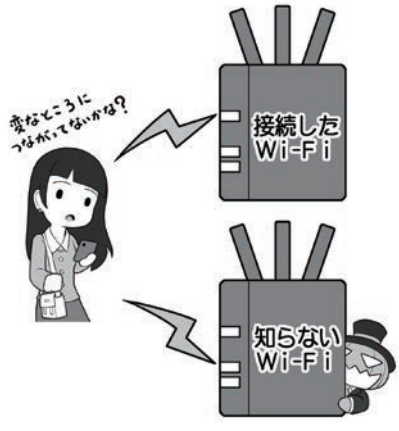
下の表は、暗号化方式のそれぞれの安全性とその理由を書き出したものです。この2つの表を比較すると、すでに暗号化が破られており、利用が推奨されていない「WEP」が、表示アイコン上は暗号化に分類されていることがわかります。アイコンは暗号化の有無を表しているので、これは正しい表示ですが、アイコンは安全性の担保ではないと認識して下さい。Androidは、接続したアクセスポイントをタップすると「セキュリティ」の項目でネットワークの種類の暗号化方式などを確認できます。Windows、mac OS Xは調べるのに手間がかかります。iOSでは、簡単に確認する手段がありません。

なお、WPA3が普及すると、これらの問題点のかなりが解消されるようになります。

＊1：Windowsでは、バージョンによってアイコンに「セキュリティ保護あり」と表示される場合もあります。

＊2：例としてはNTTドコモでアクセスポイントの名称（SSID）が「0001docomo」、auで「au_Wi-Fi2」、ソフトバンクで「0002softbank」のものがWPA2-EAPの方式です。各携帯電話キャリア提供の無線LANアクセスポイントの一部で、自動接続になっているため意識することはありません。そのほかの安全性が確保されていないと判断したアクセスポイントに接続されている場合は、接続を切ることが推奨されます。

新しいスマホを購入したら…



携帯電話キャリアなどで購入したスマホには、無料提供されている公衆無線LANの設定が入っています。しかし、すべての公衆無線LANが安全とは限りません。それぞれの暗号化方式を調べ、安全でないものに接続したら切断するようにしましょう。

また、知らないアクセスポイントに接続した場合も切断しましょう。攻撃者が設置したものだったり潜んでいたりすることがあります。

クセスポイントなどに勝手に接続されてしまった場合は、同様に設定を削除して、以降自動で接続されないようにしましょう。

10 公衆無線LANが安全ではない場合の利用方法

しかし、いつでも安全な状態の公衆無線LANを利用できるとは限りません。先ほど少しだけお話しした観光客用や、災害時に設置される「00000JAPAN」などの「暗号化無し」の公衆無線LANしか利用できない状況も考えられます。

しかし、「暗号化無し」もしくは「危険な状態」で提供されている無線LANアクセスポイントを不用意に利用すると、攻撃者から見れば獲物が絶好の狩り場に飛び込んできた状況になってしまいます。

対策は、「無線LANの暗号化に頼らず、自前で通信を暗号化して盗聴対策をする」ことです。

もし、この言葉の意味が理解できない場合は、ここからはややハードルが上がりますので、無理をせず自前の携帯電話回線、もしくはパソコンならばスマホをルータ代わりに利用する「テザリング」の範囲で、手軽かつ安全にインターネット接続することをおすすめします。

11 自前の暗号化による盗聴対策

自前の暗号化で盗聴対策をする第一歩は、ウェブブラウザでのインターネット閲覧では「https://」から始まるもののみ、メールでは「SSL/TLS」を使った通信設定になっているもののみ、スマホなどのアプリでは暗号化通信でサーバに接続するもののみ使うことです。

前者2つに関しては、後ほどそれぞれ詳しく説明します。

スマホアプリに関しては、アプリの通信全体を暗号化するトレンドに向かいつつありますが、現状、提供している会社によっては通信を暗号化しているかどうか明確にしていないものも多く、技術者でもない限りは自分で確認することは困難です。

アプリが通信を暗号化しているかどうかは、調査結果など公開されている情報から確認するか、多くの人が使用していてかつ盗聴や情報流出のトラブルがないもの、という選択しかありません。

もしくは、通信の全暗号化を商品として表明しているアプリに限定して利用することです。

12 まとめて暗号化するVPN、現状は過信できないが今後に期待

こういった個別の面倒な対策ではなく、まとめて一気に対策をする方法もあります。それは、VPN（Virtual Private Network：仮想プライベートネットワーク）の個人利用です。

VPNとは、元々は一つの会社の離れた事業所間をインターネットを使いながら接続する技術です。まるで会社内のLANで接続されているように、秘密を守りつつ互いに通信することができます。VPNはインターネットを使って事業所間を接続してますが、その通信が外部から盗聴できないように暗号化して秘密を守っているのです。

この方式を「事業所から事業所」ではなく、「個人の機器から安全な場所にある出口サーバ」に置き換えて利用するのが、VPNの個人利用です。

この場合、通信は自分のスマホやパソコンから、少なくとも安全な場所にあるとされる出口サーバまで、無条件ですべて暗号化されるので、どのようなソフトやアプリでも、また、その間の公衆無線LANの暗号化方式が安全でなかったり、そもそも全く暗号化されていなかったりしても、攻撃者に盗聴される心配は少なくなります。

ただ、このVPNの使い方はまだ、一般の利用者が豊富な選択肢の中から選び、ボタン一つで簡単に使える程にはこなれていません。現状は、一部プロバイダが有料サービスで提供していたり、あるいは有料アプリで提供されていたりする程度で、無料で安全性が高く手軽に使えるものは、自分で設定画面を書き換える必要があるなど、導入にスキルが求められます。

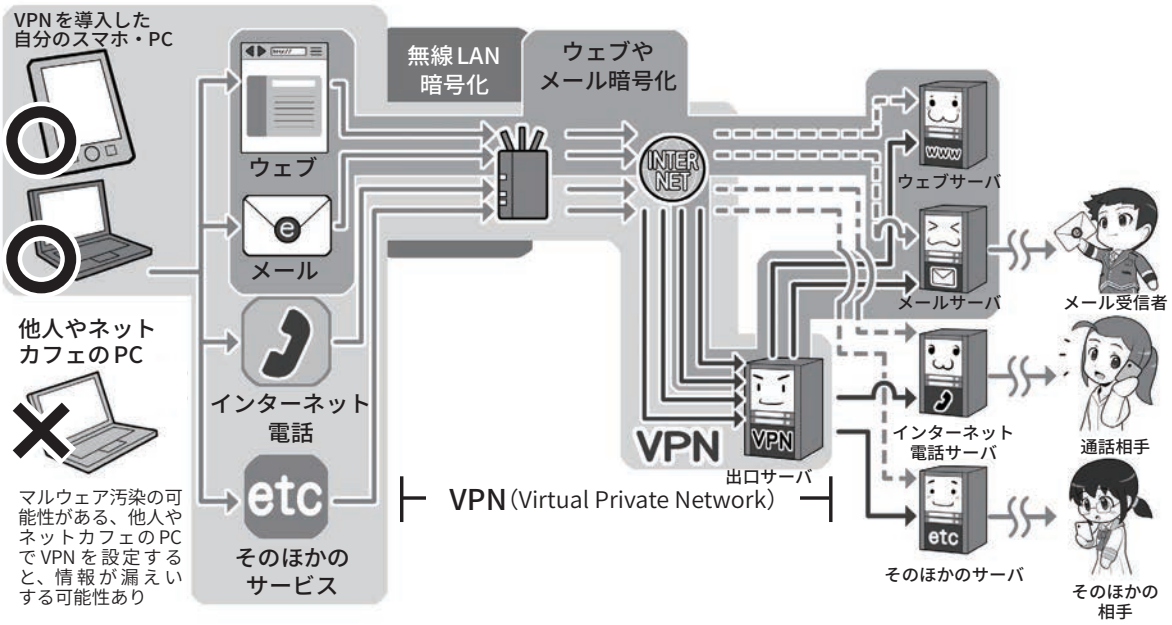
また、利用するVPNのサービスによっては、誤ったアクセスポイントに誘導されたり、VPN接続が切れると暗号化されていない状態に移行して通信を継続したりしてしまうものもあるなど、2020年の春の時点でも、まだ決定版的なサービスがありません。

どうしてもVPNを利用したい場合は、そういった問題点に関する各VPNサービスのテスト結果を公開しているウェブサイトがあるので、そこできちんと問題点に対応しているVPNサービスを探し、導入するようにしましょう。

なお、VPNが通信を暗号化するのは出口サーバまでなので、その先の通信の暗号化が行われない点は注意しましょう。

様々な場所から安全なアクセスを可能にするVPN

①詳細なVPNのイメージ

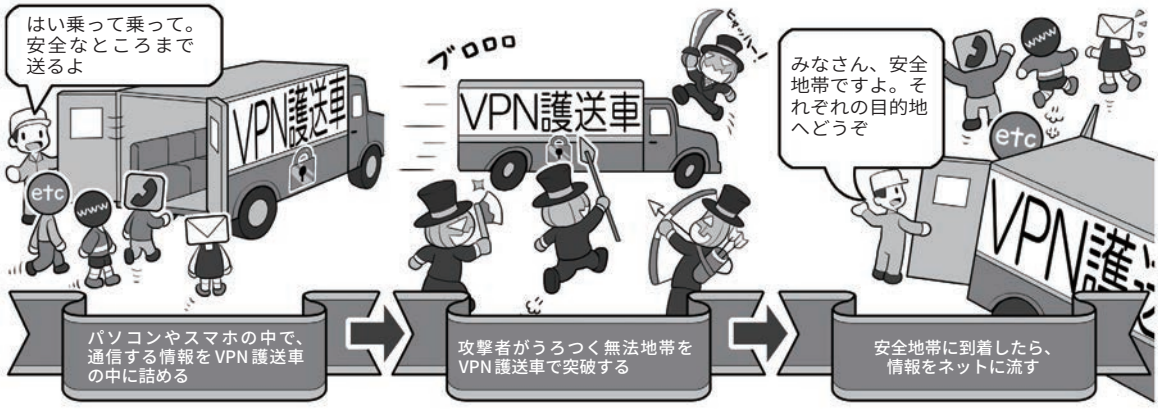


VPN を図で説明すると、上のように入り組んでよく分からなくなってしまうので、簡単な図を下に用意しました。くじけそうな方は、まず下をご覧ください。

上の図では、左から右に向かって通信を行う場合、無線 LAN の暗号化、ウェブやメールの暗号化、VPN とそれぞれ暗号化の守備範囲があることが分かります。

無線 LAN の暗号化は範囲が短く、ウェブやメールの暗号化は文字どおり用途が限定されます。VPN はすべての通信を暗号化し、かつ広範囲にカバーしてくれます。しかし、その範囲は利用者の機器から安全と思われる場所に設定された出口サーバまで限定なので、その先の目的のサーバまでは暗号化されない区間が残ります。VPN さえあればすべて安全というわけではないのです。

②簡単なVPNのイメージ



VPN を簡単なイメージで説明すると、この図のようになります。スタート地点（自分のパソコンやスマホの中）でデータを護送車に乗せて全部まとめて暗号化、危険地帯を突破し、信頼がおける安全な場所（出口サーバ）に着いたらデータを解放します。VPN は暗号化されていない無線 LAN を利用するのにも役に立ちますし、危険性があると思われる通信回線の盗聴、検閲や監視がある国からの安全な通信にも役立ちます。

また、災害時などに利便性を優先して提供される、暗号化無しの公衆無線 LAN を利用する場合でも役に立ちます。ただし、そもそもだれが運営しているのかよく分からないような無線 LAN アクセスポイントには、多分に攻撃者が潜んでいる可能性があるので、攻撃の手段は予測できず、VPN を使えたとしても積極的な利用は推奨しません。

3 ウェブサイトを安全に利用する、暗号化で守る

1 無線LANの暗号化とVPNの守備範囲

インターネット通信の基本は、「平文」での送受信です。ウェブサイトを見るときに、ウェブブラウザ上部のアドレスバーと呼ばれるウェブサイトの住所(URL)を入れる欄内が①http://で始まっている、②「保護されていない通信」や「安全ではありません」と表示されている、③先頭に注意喚起のⓘや🚫のマークがある場合、その通信は平文で送受信されています。

平文での通信は、通信の途中、攻撃者によっていつでも盗聴や改ざんされ、すべてもしくは一部が偽の情報に書き換えられる可能性があります。そうさせないためには、ウェブサーバとの通信の暗号化が必要になります。

前項では、通信の暗号化を行うために、無線LAN通信の暗号化と、VPNが登場しました。

利用者が目的のウェブサーバなどと通信するとき、無線LAN通信の暗号化では、利用者の機器から無線LANアクセスポイントまでの、すべての通信が暗号化されます。一方、無線LANアクセスポイントから、目的のウェブサーバまでの通信は、無線LAN通信ではないので暗号化されません。

一般の利用者向けのVPNサービス(以下VPN)では、利用者の機器からインターネット上の安全な場所にある出口サーバまで、無線であっても有線であってもすべての通信を暗号化します。しかし、出口サーバから目的のウェブサーバまでの通信は暗号化してくれません。

それぞれの守備範囲があり、攻撃できるポイントが残るわけです。

では、無線LANやVPNでは暗号化してくれない区間の通信の暗号化や、前項にあった、なんらかの理由で無線LAN通信の暗号化やVPNが使えない状況で安全に通信をしたい場合、どのような対処方法があるのでしょうか。

代表的なものとしては、ウェブサイト閲覧やメール送受信、通信の目的に限定して、利用者のそれぞれのソフトやアプリから目的のサーバまでを暗号化するやり方があります。

2 すべての通信と、その一部であるウェブサイトとの通信

無線LAN通信の暗号化とVPNでは、暗号化対象を「すべての通信」と書きましたが、ウェブサイトを閲覧するための通信の暗号化は、その「すべての通信」の中の一部「ウェブサイト閲覧に関する通信」に限定した暗号化になります。

通信には、ウェブサイト閲覧やメール送受信のほかに、インターネット電話、一部のアプリや特殊な機器など、目的などに応じて多様な通信が存在します。

例えるなら、すべての通信は「テレビの電波放送」という大きなくくり。これに対してウェブサイトを閲覧する通信は、その中の一つのチャンネルにあたります。そして、通信には様々なチャンネルが存在するわけです。

インターネットの通信では、このチャンネルにあたるものを「ポート」と呼び、ウェブサイトの閲覧の通信は、通常「ポート80」「80番ポート」という名称で、文字どおり80番のポートで行います。

80番ポートを使って送受信される通信は、基本的に暗号化されていない平文で、仮にこの状態でIDやパスワード、個人情報などを送信すると、通信を盗聴している攻撃者は特になんの工夫をしなくても情報を盗むことができます。また、情報が送受信ともに改ざんされ、偽の情報で取引などをさせられる可能性もあるのです。

それを避けるため、ウェブサイトを安全に閲覧する通信の暗号化が普及しました。それが「SSL(Secure Sockets Layer)/TLS(Transport Layer Security)」(以下SSL/TLS)という暗号化通信です。

暗号化していないウェブサイト閲覧では、URLが「http://」から始まるのに対して、SSL/TLSの通信では「https://」で始まります。後ろに追加されたsは「secure=安全な」の意味のsなのです。

3 httpsで始まる暗号化通信にはどんなものがあるか

先ほどのチャンネルの話に戻ると、httpsは通常ポート443を使

用します。つまりテレビのチャンネルを443にあわせたら、放送にはモザイクがかかっていて、有料放送契約者だけがモザイクを解除して見ることができる、というイメージです。

https://から始まるウェブサイトにアクセスすると、通信相手が誰であるかが後ほど説明する電子証明書によって証明され暗号化通信が始まり、アドレスバーに暗号化を示す鍵マークが表示され、問題がないという意味で、左ページの②や③の表示がなくなります。

この状態になると、「一応は」、IDやパスワードなどを入力しても大丈夫で、「表示される情報も改ざんされていない」ということになります。しかし、なぜ「一応は」かというと、最近ではこの状態でも安全とは限らないからです。

httpsによる暗号化通信を行うためには、まず、httpsで通信するサーバを作りたい企業や団体のサイト運営者が、認証局という機関に、書類で自分の会社の情報とサーバのドメイン名を提示して、ネット上で身元を明らかにする電子証明書の発行を申請します。

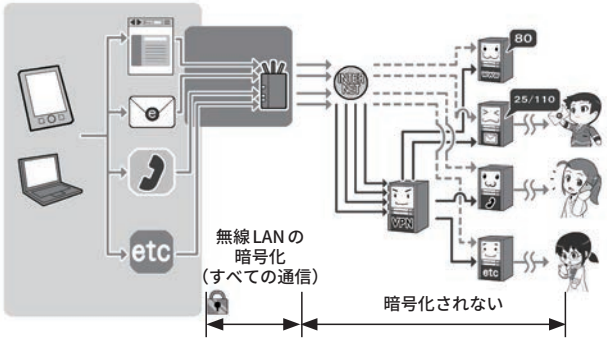
認証局は審査の上、その企業や団体が実在することを確認できれば、「SSL証明書(SSLサーバ証明書)」という電子証明書を発行します。

「SSL証明書」を取得した企業や団体は、httpsで通信するサーバに「SSL証明書」を設定し、利用者がアクセスしたときに、その「SSL証明書」によって、該当のドメインの運営主体と証明することで、互いに安心して暗号化通信が始められるようになります。

しかし、SSL証明書の中には実在性確認をせず、簡単なオンライ

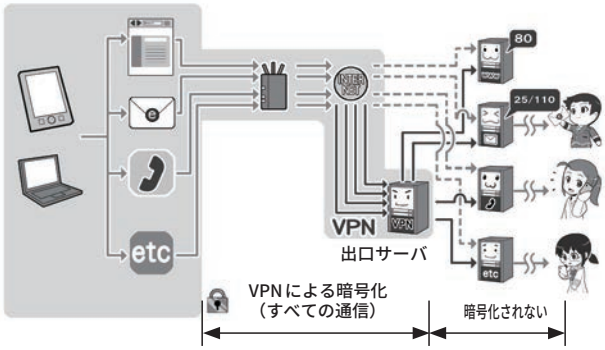
それぞれの暗号化の守備範囲

無線LANの暗号化



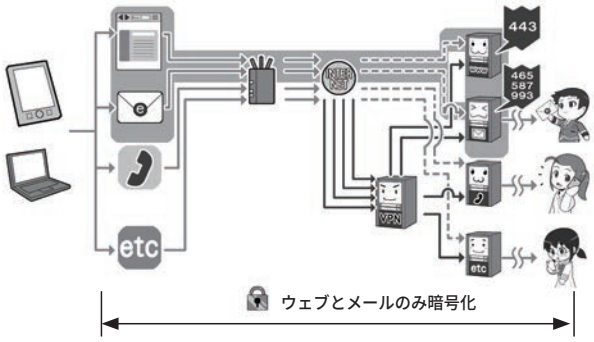
無線LANの暗号化は、利用者の機器から無線LANアクセスポイントまでのすべての通信を暗号化します。

VPNによる暗号化



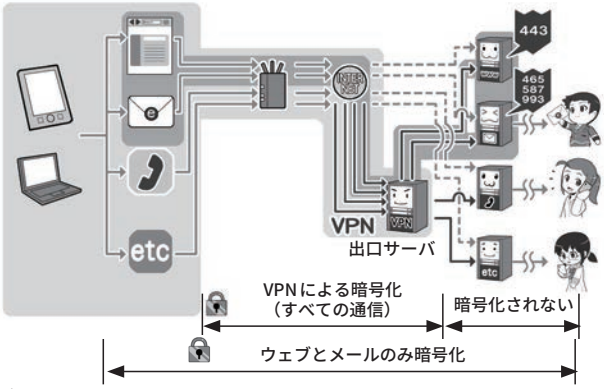
VPNは利用者の機器から、安全とされる「出口サーバ」までの区間で、すべての通信を暗号化します。

ウェブサイト、メールの暗号化



ウェブやメールの暗号化は、利用者のウェブブラウザやメールソフトから目的のサーバまでの区間で、ウェブとメールの通信だけを暗号化します。

VPN＋ウェブメールの暗号化



ウェブやメールの暗号化とVPNを組み合わせて利用することももちろん可能です。この場合暗号化される通信範囲は広くなります。

ンでの確認だけで機械的に発行し、企業や団体名すら証明書に記載しないものもあります。そのような「SSL証明書」は誰でも取得できてしまいます。

攻撃者は、そういった審査の甘い認証局を使って、詐欺サイトのための「SSL証明書」を取得して、暗号化通信をする詐欺サイトを立ち上げます。

そして利用者に、「あ、暗号化しているから大丈夫」と油断させ、パスワードやクレジットカード番号を入力させ盗むという事例が発生するようになったのです。

4 より厳格な審査の「EV-SSL証明書」

そういった問題に直面して、より審査を厳しくした「EV-SSL証明書」が登場しました。

「EV-SSL証明書」の審査では、証明書を発行する認証局も、外部の監査により基準を満たした者に限定して発行権限が与えられ、証明書を受ける側の企業なども、法的な存在の証明や、管理責任者や役員など複数人への聴取など、従来よりも厳格に審査が行われます。

これにより、「法的・物理的実在性」と「正当性」、結果としての「安全性」などが担保され、詐欺サイトなどの排除が行えるようになったわけです。

この「EV-SSL証明書」に対応したブラウザでは、アドレスバーが緑色になったり、企業名や団体名を表示したり、証明書に会社の所在地が表示されるなど、利用者がより確認しやすい表示が行われるようになりました。

しかし、現在はこういった表示を取りやめ、本項の最初に掲示したような表示に戻ったブラウザもあります。

その理由は、「EV-SSL証明書」特有の表示を行っても、利用者の行動に変化はなかったからとされ、平たく言えば、「利用者はそのようなものを確認しなかった」ということでした。

5 アドレスバー警告表示と、常時SSL化の流れ

また、そもそもウェブの通信が改ざんされないように「常時SSL化」「暗号化されている状態を標準とすべき」という流れもあり、「利用者が通信をきちんと暗号化しているウェブサイトの運営主体を確認しやすくする」方式から、「通信を暗号化していないウェブサイトを『危険である』と警告する」方法にブラウザを取り巻く動向が変化しました。

そして、本項の冒頭にあったように、暗号化されていないウェブサイトにアクセスしたときは、ブラウザが「安全ではない」と表示したり、警告表示のマークをつけたりするようになったのです。

なお、現在でもパソコンのブラウザなどでは、鍵マークをクリックすると証明書内容が表示されます。

「EV-SSL証明書」を利用しているサイトの場合は、その証明書の詳細まで表示すると、証明書を持っている企業や団体の所在地も表示されるので、そのサイトが自分が見ようとしているサイトかどうか判断する手掛かりになります。

スマホの場合は、鍵マークをクリックしても証明書が表示されない場合があるので、残念ながら普遍的に安全性を確認できる方法ではありません。

6 有効期限が切れた証明書は拒否する

なお、電子証明書には有効期限があり、失効したものは安全ではないと考えるべきです。

有効期限に問題があるなどの理由で、ウェブブラウザやセキュリティソフトが警告を発する場合、そのウェブサイトには接続しないようにしましょう。

きちんとセキュリティに対して必要な手続を行っている会社ならば、証明書の失効前に更新の処理を行い、新しい証明書に差し替えるはずです。

それを行わない企業は、セキュリティに対して必要な措置をしていないと判断し、したがってそのウェブサイトは安全に利用できないと考えるべきでしょう。

7 ほかにも証明書に関する警告が出るウェブサイトは接続しない

証明書が失効している警告以外にも、証明書に関する警告が表示される場合があります。

詳しく分類すると多岐にわたるので、すべては記述しませんが、以下のような例が該当します。

1. 証明書の使い方を間違っている場合
2. 証明書の署名アルゴリズムに問題がある場合
3. 証明書を発行した認証局になんらかの問題がある場合
4. 「オレオレ詐欺」のように認証

局でないのに認証局と偽って証明書を発行し、それを使っている場合（通称：オレオレ証明書）

いずれの場合も、「安全ではない通信」の元凶となります。

証明書の有効期限の問題と同様に、ウェブブラウザやセキュリティソフトが「証明書に関する警告」を発した場合、そのウェブサイトとの通信は安全でないと判断し、利用しないようにしましょう。

さて、ウェブサイトを安全に利用するには、通信面のほかにも気をつけるべきポイントがあります。

ほかのセクションとも重複しますが、ウェブを使うというくくりで少し触れておきましょう。

8 ウェブサービスのログインは多要素認証を選択する

ウェブサービスを安全に利用するには通信の暗号化も大切ですが、ウェブサービスにログインするIDやパスワードの管理と運用も大切です。

通信を暗号化しても、スマホやパソコンがマルウェアに感染してしまえば、通信する前の段階で情報が盗まれてしまいますし、ウェブサービスのIDやパスワードが盗まれると、攻撃者がウェブサービスに勝手にログインして、悪さをすることができるからです。

これを避けるため、P22でも触れたように、ウェブサービスへのログインは、使い捨てパスワード（ワンタイムパスワード）を含む、二要素以上の多要素認証を利用して、仮にパスワードが盗まれた場合でも攻撃者が簡単にログインできないようにしましょう。不審な

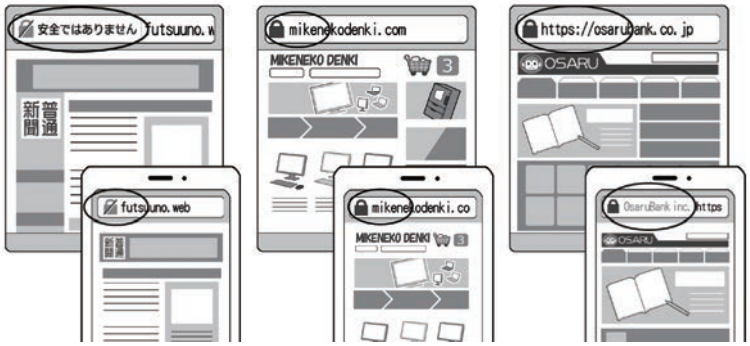
httpsの暗号化通信で情報を守る

個人情報の入力は基本的には……

ダメ ✕ 暗号化無し（httpと表示される）安全ではないと表示される ⓘや🔒マークがある

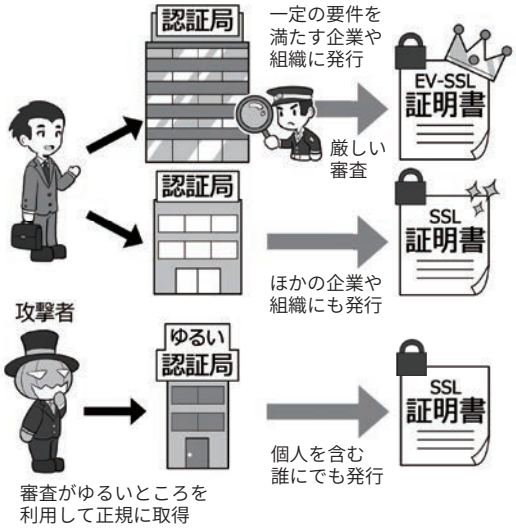
注意 △ SSL（暗号化あり）（httpsと表示される 🔒マークが表示される）

より安全 ○ EV-SSL（暗号化あり）（🔒マークと、一部のブラウザでは文字が緑になる）



個人情報の入力をする場合、暗号化は必須となります。厳しい認証局の審査を伴うEV-SSLのウェブサイトを利用する方が、より安全であると判断しましょう。特に、お金関連のサイトはEV-SSLの方がより推奨されます。

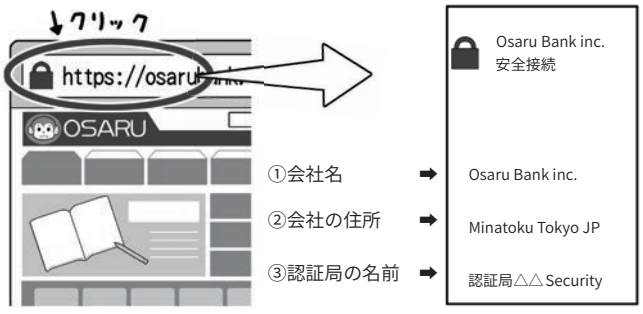
攻撃者が不正に取得した証明書に注意



SSL証明書には、ウェブサイトを運営する企業や組織が実在することを認証局が審査して証明してくれるものと、その機能がないものがあります。SSL証明書は元々、サーバ設置者の身元証明のためのものですが、最近では実在証明がなくても証明書を取得できる手があるので、攻撃者が攻撃サイト用に取得することもあります。

EV-SSLのhttpsサイトは、より厳密なので不正取得は困難ですが、上記のとおりただのhttpsサイトは運営者が不明な場合もあるので、要注意です。

証明書の内容をチェックする



パソコンなどの場合は簡単に証明書の内容をチェックすることができます。会社名や認証局の名前、EV-SSLに対応したウェブブラウザならば会社の大まかな住所も表示されます。また、一部ブラウザである緑文字のURL表示はEV-SSL証明書の証でもあるので覚えておきましょう。

ログインがあった時にログイン通知を受けとれる機能があれば利用して、攻撃を即座に察知できるようにしましょう。

また、近年、ウェブサービスへのログインに関して、そもそも「ネットを通じて認証のためにパスワードを送信する」という構造そのものが危険だという考え方も出てきています。正当な利用者である認証は、手元の機器の中で行い、パスワードなどは送信せず、「本人であることを確認できた」という認証情報だけをサーバに送って、ウェブサービスを利用可能にする、FIDOなどの方式も一部で採用が始まっています。

今後の動向に注目して、必要に応じて採用するようにしましょう。

9 多要素認証すら破る「中間者攻撃」

ウェブサービスの安全な利用のためには、二要素以上の多要素認証を利用するべきと第3章の1で書きましたが、それすらやぶる攻撃もあります。

例えば、パソコンから二要素認証に対応したインターネットバンキングを利用する際、銀行のサイトにIDとパスワードでログインするときや送金操作時に、使い捨てのパスワードがスマホに送られて来て、これをパソコンからサイトに入力するとしましょう。

このとき、銀行のサイトだと思っていたものが偽サイトだとしたらどうなるでしょう。攻撃者が、私たちが偽サイトに入力した内容を本物のサイトに中継して、画面の内容をリアルタイムに模倣していたとしても、気付かないまま送金の操作をしてしまうでしょう。

攻撃者が通信を中継しながら、送金先を別の銀行口座に差し替えていたら、二要素認証を使っていても不正に送金されてしまいます。

このような、通信経路の中間で双方の通信を中継しながら裏をかく手口は「中間者攻撃」と呼ばれています。たとえ多要素認証を採用していても、この中間者攻撃をすべて防ぐことはできません。

結局、偽サイトによる攻撃は、利用者自身で自分がどこのウェブサイトを見ているのか、注意して確認する以外に対策はありません。では、どのように注意すればよいのでしょうか。

本物のサイトが、前ページの図にあるようにEV-SSL証明書を使っている場合には、パスワードを入力する直前に、ウェブブラウザ画面のアドレスバーの鍵マークから証明書を表示して、自分の利用している企業や団体名や所在地とあっているか確認する方法もあります。

ただ、先ほど説明した通り、攻撃者が偽のSSL証明書を取得していることを考えると、鍵マークなどの有無だけでは判断できません。

また、アドレスバーのURLを見て自分が知っているウェブサイトとドメイン名が同じかを確認します。

「ドメイン名」とは、例えば「https://www.example.co.jp/foo/bar.html」のうち「example.co.jp」の部分のことです。

ただ、これを確認するのも簡単ではなく、攻撃者は利用者が見間違うのを狙って、「https://www.example.co.jp.foo/bar.html」という、似たURLで偽サイトをつくることがあります。このURLのドメイン名は「co.jp.foo」であり、「co.jp」とは全く違うところなのですが、「.」と「/」の違いを見抜けないと気がつきにくいのです。

最近のウェブブラウザでは、URL中のドメイン名部分がどこなのかを強調表示してくれるものや、アドレスバーにドメイン名部分しか表示しないようにしているウェブブラウザもありますので、そういうブラウザでは見分けがつきやすいでしょう。

その場合でも、URLの一部をアルファベットに似た別の言語の文字を使ってURLを偽装する手口もあります。

こう言った状況を総合的に鑑みると、自分が利用するウェブサービスは、基本的にあらかじめブックマークしておいて、訪れる際も、詐欺に用いられやすい偽サイトへの誘導に使われるメールやメッセージのリンクは利用せず、直接ブックマークから訪れるか、スマホの場合は公式のアプリを利用するのが安全でしょう。

もうひとつ注意したいのは、野良Wi-Fiや、公衆無線LANを利用する時に同名のSSIDに偽装した攻撃者のアクセスポイントに誤って接続してしまうケースです。安全でないアクセスポイント（P69の図で接続が×や△になっているもの）に接続している場合には、DNSハイジャックといって、通信経路を誘導する情報が改ざんされ、ブックマークから正規のサイトへ接続しようとして、ブラウザ上も正規のサイトに接続しているように見えても、偽サイトに誘導される場合があります。野良Wi-Fiや運営主体の分からない公衆無線

LAN、同名のSSIDのアクセスポイントがある場合の利用は避けるようにしましょう。

10 ウェブサイトを使ったサイバー攻撃に対応する

スマホやパソコンがマルウェアに感染したことによる、パスワードなどの情報流出。

事態が起こるまでには、マルウェアに感染する経路が必ずあり、それがウェブブラウザであることもよくあるケースです。最近では、ウェブブラウザでウェブサイトを「見る」だけで感染させる攻撃も発生しています。

攻撃者があなたに、マルウェアを仕込んだウェブサイトのURLをメールやアプリのメッセージで送り、あなたがリンクをクリックして悪意のあるウェブサイトを見てしまう場合(フィッシングメール)や、あなたの行動パターンを調べて、よくアクセスするウェブサイトに、事前にマルウェアを仕込んでおく水飲み場攻撃、さらにわざわざお金を払ってマルウェアが含まれた動画広告などを目的のウェブサイトに出すという方法(マルバタイジング)もあります。攻撃は不特定多数を対象に行われる場合もあります。とくに、広告を使うものは、攻撃者は広告費以上のお金を稼がなければならず、攻撃は無差別に不特定多数に対して行われ、被害者も大変多くなります。

この「見る」だけで感染するサイバー攻撃は、未知のセキュリティホールが突然狙われる場合もあるのですが、ネットでセキュリティホールが公表され、メーカーがそのソフトやアプリを修正するまでの「穴が開いたまま」の期間を狙って攻撃する「ゼロデイ攻撃」で行われる場合も多くあります。

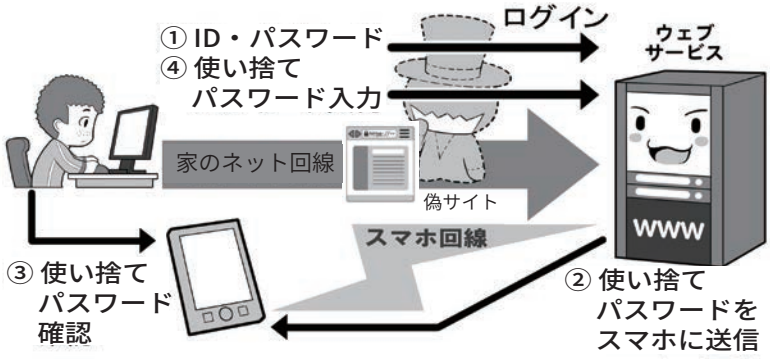
また、見るだけでなく、あなたの心の隙を突き、巧妙に誘導して「自らクリックやインストールさせる」といった攻撃もあり、この場合はセキュリティホールがなくても攻撃ができてしまいます。

なお、セキュリティホールを狙ったサイバー攻撃に対する基本の対策は、システムの状態を最新に保つことですが、セキュリティホールの修正など対応が間に合わない場合は、あなたが意識して攻撃を避けるほか対処法はありません。

さらに、利用者を巧妙にだましシステムのセキュリティ設定を変えさせて、自らアプリなどをインストールさせる攻撃に至っては、誰にでもある人間の心の隙を、自分が理解しなければ防げません。

そういった場合に備えて、「不審なメール文中のリンクは開かない」「なにかをインストールさせようとするものは拒否する」「ニュースなど情報を常時ウォッチして、特定のウェブサイトやアプリを使った攻撃が判明したらそのサイトやアプリに近づかない」「SNSやウェブサービスの動画や広告は自動再生しないように設定する」などの防御策を積み上げて守りましょう。

間に入ってなりすます中間者攻撃



中間者攻撃では、利用者とサーバの間に攻撃者の偽サイトが入ります。攻撃対策として二要素認証を使っていても、改ざんされた情報を見せられたまま処理が進むので、防御が意味をなさないこともあります。

ウェブを使ったサイバー攻撃の例

4 メールを安全に利用する、暗号化で守る

1 メールにおける暗号化

次は、メールを安全に使う方法についてです。

「ウェブを安全に利用する」の項目で書いたとおり、メールの送受信もすべての通信の中の一部です。

そして、メールの内容を盗聴されないためには、暗号化の区間が限定される無線LANの暗号化やVPNではなく、メールが送受信中常に暗号化していることが大切です。特に、メールはウェブと異なり、私的な内容が含まれるからです。

メールの送受信では、使用するスマホやパソコンなどのソフトやアプリから、メールサーバまで、送信と受信に別々の通信チャンネルを利用します。

2 送信の暗号化と受信の暗号化

メールは、昔はどちらも暗号化されていない平文で通信が行われており、送信を行うSMTPと呼ばれる通信が25番ポート、受信のうちPOPと呼ばれる通信が110番ポート、IMAPと呼ばれる通信が143番ポートを利用していました。

それが、後になって、平文でのメール送信による盗聴の危険性を回避するため、465番ポートを使って、SSL/TLSによる暗号化を組み合わせてSMTP over SSL（SMTPs）が普及しました。これと併せて、メール受信側の暗号化も普及し、POPがPOP over SSL（POPs：995番ポート）、IMAPがIMAP over SSL（IMAPs：993番ポート）で提供されるようになりました。

現在では、多くのプロバイダメール、携帯電話キャリアメール、フリーメールサービスで、この暗号化によるメール送受信サービスが標準になっています。

設定が「面倒くさくない」ように、スマホなどでは工夫されていて気付きませんが、最近では、特に意識しなくても自動的に暗号化で通信を行うようになっています。

一方、パソコンのメールソフトでは、依然として手動での設定が必要な場合もあるので、パソコンメールを使っている人は一度、自分のメールソフトのメール送受信サーバの設定がきちんと上記の暗号化ポートや類似の方式を利用しているか、もしくはSSL/TLSなどの文字がある設定になっているかをチェックしてみてください。

特に、パソコンで古くからメールを利用し、メールソフトの設定を全然いじっていない場合、暗号化されていない昔の設定のままになっていることもあります。

多くのメールアカウントを持っている人は、一度メールアカウントの棚卸（たなおろし）をし、暗号化されていない設定があれば、暗号化した方式に切り替え、暗号化した方式がないものしか提供されていないメールサービスは安全でないと考え、安全なメールサービスに乗り換えるようにしましょう。

3 メールにおける暗号化の守備範囲

先ほども少し触れましたが、メール送受信の暗号化は、スマホやパソコンのソフトやアプリなどから、送受信用のメールサーバまでの間を暗号化します。

しかし、目的のウェブサイトの情報を直接閲覧するのと異なり、メールの送受信は自分が利用しているメールサーバから相手のメールサーバまで、複数の中継メールサーバによってバケツリレーのように、受け渡しによる送受信が行われる場合があります。

遠方の誰かに手紙を送ると、複数の郵便局を転送された後に、相手に配達されるのに似ています。

そして、残念ながら、このバケツリレー中の送信はいまだ平文で行われていることもあるのです。

自分や相手が契約しているメールサーバまでの経路をそれぞれ暗号化しても、その先のバケツリレーの区間で平文での送信が行われていれば、内容を盗聴されてしまったり、改ざんされてしまったりする可能性が残ります。

とはいえ、この転送中の通信の暗号化は、大手メールサービス提供会社の努力により進み、改善されつつあります。

ただ、途中の経路をすべて暗号化しても、それぞれのメールサーバで一旦暗号化が解かれますので、バケツリレーの途中のメールサーバに盗聴しようとする攻撃者がい

たら、内容を読まれてしまう余地があります。

現代でも外国に郵便を送ると、国や地域によっては手紙が開封されて中を見られてしまったりすることがあり得るのに似ています。通信の秘密が保障されるかは、国や地域によるからです。

それを避けたい場合は、安全な国内だけで手紙をやり取りするように、メール送受信を暗号化したサービスの中だけでやり取りする方法もあります。

4 メール本文の暗号化

ところで、メールの暗号化には、送受信の暗号化ではなく、メールの本文そのものを暗号化する手段もあります。

これには、「S/MIME」や「PGP」という方法があります。これらの方法を使うと、メールのバケツリレーの途中で攻撃者が盗み見しようとしても、そもそも本文が暗号化されているため読めません。

メール本文の暗号化には、公開鍵暗号方式の「公開鍵」と「秘密鍵」を使います。この方法を使うときは、事前の準備として、自分用の秘密鍵と公開鍵を作成しておく必要があります。

相手が自分の「公開鍵」で暗号化したメールを、受信して復号するには自分の「秘密鍵」を使い、相手にメールを送る際は相手の「公開鍵」で暗号化して送信します。

そして、これを成立させるためには、お互いの公開鍵を安全かつ確実な方法で交換しておく必要があります。

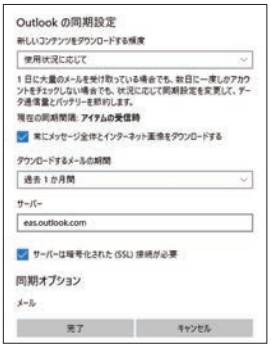
特に、S/MIMEを使う場合は、お金を払い認証局が発行する証明

メールの送受信は暗号化されているか

メールソフトやアプリが暗号(SSL/TLS)利用することになっているか？

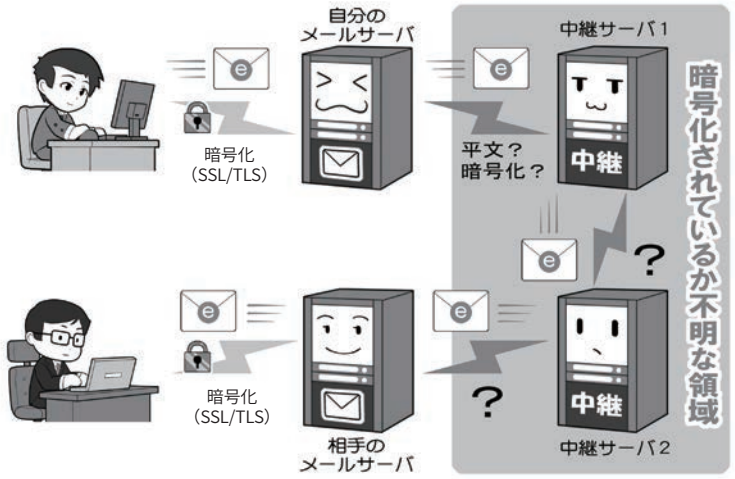
メールソフトの例

メールアプリの例



メールアカウントが設定された状態で、メールソフトやメールアプリの、サーバの詳細設定画面を開き、暗号化を利用する設定になっているかを確認します。「受信ポート 587 や 993 の使用」「送信ポート 465 の使用」「パラメータとして SSL 使用が ON」などになっているかがチェックポイントです。これらは暗号化通信が設定されている目印です。

しかしSSLの通信は自分のサーバまで



メールの暗号化設定は、利用者の機器から契約しているサーバまでの区間のみの暗号化が担保され、メールが送信相手の利用しているサーバに到達するまで経路は担保されておらず、平文で送信される区間がある可能性が残ります。

暗号化している同じサービスを利用する

メールを安全に利用する一つの方法としては、暗号化通信を採用した一つのメールサービスを、送信相手とともに利用する方法があります。通信の秘密が守られる国内だけで手紙をやり取りするのと同じ概念です。

書を入手し、自分の公開鍵の正当性を証明する必要があります。事前の準備も必要で、相手も同じことをする必要があるので負担にもなります。

なお、メールの本文を暗号化しても、メールのヘッダ部分、つまり、件名部分や、宛先と差出人のアドレスなどは、平文で送られることになるので、注意が必要です。

S/MIME や PGP を使うと、盗聴を防ぐことができるだけでなく、仮にメールの本文が改ざんされても、受信者側で改ざんの有無を調べることができるようになります。また、他人がなりすました偽のメールではないかを確認することもできます。これを実現する機能を「デジタル署名」と呼びます。

上記のとおり S/MIME は大変優れた機能なのですが、事前の準備に手間がかかり、また、大手のメールソフトが対応してないものもあって、残念ながらあまり利用されていません。詳しい方法の説明はここでは省略しますので、各自で調べてみましょう。

一方、利用者ではなくメールサービス側で成りすましを防ぐものとして、認証チェックをする SPF、DKIM、そして、これに引っかかった場合の対処を決める DMARC などがあります。これは、送信者の書面上のメールアドレスと実際にメールが発信されたサーバのドメインをつきあわせて、合っていなければメールを受け取らないなどの対応ができるものです。これらを採用したメールサービスがあれば、積極的に利用を検討してもいいでしょう。それが安全な技術の普及への一助になります。

5 怪しいメールとはなにか

メールを安全に使うために、メールを使ったサイバー攻撃にも触れておきましょう。

サイバーセキュリティの標語などでは、よく「怪しいメールを不用意に開かないように」といったものを見ます。これは、「標的型メール攻撃」に代表されるフィッシング（詐欺）メールを使った攻撃に関する注意喚起をしています。この攻撃は、攻撃者が特定の個人を狙って仕事などのメールを装い、マルウェアの添付や、マルウェアを仕込んだウェブサイトのリンクを送り付けるものです。相手が添付ファイルやリンクを不用意に開くと「ゼロデイ攻撃」などを受け、不正なプログラムをインストールされたり、パソコンなどを乗っ取られたりするのです。

実際には、特定の個人を狙った標的型攻撃だけでなく、不特定多数を狙った「スパムメール」でも同様の手口が使われます。誰でも攻撃対象になりうるわけです。

これらの手口は、昨今のセキュリティ環境の向上で「開くだけ」「見るだけ」で感染させることが難しくなったため、少なくとも相手を「感染させるためになにがしかの行動を起こさせる」ことで感染率を上げています。それが、偽装したマルウェアをインストールさせたり、偽装サイトへのリンクをクリックさせたりする手法なのです。

こういった攻撃を避け、マルウェアなどに感染しないようにするためには、まず**「送られてきたメールの文面を見るだけで完結しないものは、すべて『怪しいメール』として警戒する」**ことが必要です。

送られてきたメールの差出人が知り合いでも、実は全く違う所から送られて来ていたり、あるいは間違いなく知っている相手から送られてきたメールでも、実は相手のパソコンが乗っ取られていて、そのパソコンから送ってきたりしていることもあります。知り合いからのメールだから安全とはいえないと覚えて下さい。

少なくとも、送られてくることが事前に知らされていない添付ファイルや、「今すぐ確認を！」といったように、緊急に文中の添付ファイルやリンクを開くことを要求するメールなどは、警戒する必要があります。次項目の偽装添付ファイルにも気をつけてください。

発信者に、送信されてきたメールについて「メールではなく電話などの別通信経路」で問合せをしたり、銀行・行政サービス・インターネットプロバイダ・サービスなどから送られてきた場合は、文中のリンクを開くのではなく、公式のウェブサイトやアプリを直接開き、本当に該当の情報が掲載されているかを確認し、もし個人情報に関わる問題であれば、ウェブサービス側に電話で問い合わせたりするなどの対応をしましょう。

6 マルウェア入りの添付ファイルに気をつける

「怪しいメール」の一つのパターンである、マルウェア入りの添付ファイルとはどういったものなのでしょう。

例を挙げると、業務を装ったメールに「報告書」などの一見文書ファイルなどに見える形で添付されるものや、ZIP ファイルというファ

イルを圧縮した形で添付されてくるものなどがあります。

そして実際は、こういったファイルは本当の文書などではなく、なんらかのマルウェアを含んだ不正なファイルであり、あなたがファイルをクリックして開くと感染するしかけになっています。

通常パソコンでは、ファイルはアイコンで表示され、アイコンには文書ファイルであれば文書ファイルを示す画像がつけられます。

しかし、このファイルのアイコンというものは、簡単に変更可能であり、文書ファイルに見せかけたマルウェアを作ることも可能で、事実そういった手法が使われます。

また、ファイル名は、文書ファイルであれば「文書名.doc」、ZIPファイルであれば「ファイル名.zip」というように、文書の名前の後ろに「拡張子」といって、そのファイルがどういった種類のファイルであるかを示す文字列が付け加えられます。(表示されていない場合は、ファイル拡張子を表示する設定に変更してください)

マルウェアが実行形式ファイル(プログラム)の場合、Windowsなら拡張子は「.exe」となり、exeと表示されれば「メールで実行形式ファイルが送られてくるのはおかしい」と気付く人もいます。

これを隠すために、攻撃者はファイルの名前を「houkokusyo.doc.....exe」というような長いファイル名にして、後半が省略され画面上で見えないように細工し、「houkokusyo.doc...」の部分だけが表示されるようにして、その上でアイコンを偽装するといったことを行います。

そういった手法に引っかからな

ウェブメールの送受信は暗号化されているか

ウェブブラウザでメールを送受信する場合は、ウェブブラウザの暗号化のチェック項目を参考にしてください。

一般的には「SSL 証明書」や「EV-SSL 証明書」を持ち、暗号化通信を示す鍵マークがついていることで、暗号化されているかどうか、信頼性があるかどうかなどがわかります。

心配な場合は、パソコンなどでは鍵マークをクリックすることで、そのサーバを運営している主体を確認することができます。

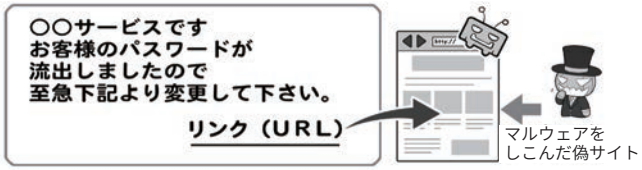
安全性を確認をした上で、「ログインパスワード」などを入力します。

怪しいメールとはなにか

①仕事のメールを装う

サイバー攻撃に使われる怪しいメールとは、まず「見ただけでは完結しない」メールです。リンクをクリックさせたり、添付ファイルを開かせたり、なにかをインストールさせようとしたりします。

②銀行、カード会社、オンラインショッピングサイト、プロバイダ関係を装うメール



また、自分が利用しているウェブサービスの名称で、緊急にどこかのウェブサイトを見させようとするのも、よく使われる手口です。

本当の仕事仲間のメールでも攻撃は来る

自分の知り合いや仕事仲間からのメールと思っても、安心はできません。なりすまして仕事仲間の名前を名乗っているだけでなく、攻撃者がその人のパソコンを乗っ取って、知り合いや仕事仲間の本物のメールソフトから攻撃をしかけてくることもあるからです。

いためにも、繰り返しになりますが、「送られてきたメールの文面を見るだけで完結せず、なにか行動させようとするメール」は、すべて「怪しいメール」として警戒することを心がけてください。

また、こういった攻撃手法は常にブラッシュアップされ進化していくので、定期的に検索エンジンやニュースなどで攻撃の手口を検索をして、最新の攻撃手法の情報を入手してください。

セキュリティソフトメーカーやフィッシング対策協議会、専門機関、識者などのSNSアカウントをフォローすると、最新の情報を入手しやすくなります。

7 メールアドレスのウェブサービスなどからの流出

「標的型メール」や「スパムメール」による攻撃には、送り先となるメールアドレスが必要です。

メールアドレスを、無差別に生成し送り付ける方法もありますが、ウェブサービスなどから流出した大量のメールアドレスを使って送られる場合も多くあります。

また、会社内で標的型メールによって感染した端末があると、そこから社内のメールアドレスが流出して、さらなる標的となる場合もあります。こういった情報は、攻撃者によって直接、攻撃メールの送付先として使われるだけではなく、インターネットの闇サイト（ダークウェブ）などで名簿として売買されることもあります。

攻撃のメールが送られてきたら、もちろん警戒するべきですが、それ以前にもできることがあります。

セキュリティ識者のトロイ・ハント氏が運営する、「Have I been pwned」というウェブサイトなどでは、メールアドレスやパスワードなどの流出情報を、すべてではないものの検索できるようになっており、そこで自分の情報が流出した形跡がないかを、ある程度チェックできるのです。

では、流出が判明したら、速やかに対処するのは当然として、流出に備えてメールアドレスにどのような工夫ができるのでしょうか。

8 流出・スパム対策としての、変更可能メールアドレスの利用

解決策としては、親しい人とやり取りをする大事なメールアドレスと、ウェブサービスや通信販売サイトなどに登録するメールアドレスを別にし、後者にはメールアドレスを気軽に変更・追加・削除したり、仮想メールアドレスが貰えるものを使う方法があります。

これは、「メールのサブアドレス」や「使い捨てメールアドレス」「捨てアド」と呼ばれるもので、ウェブサービスなどからメールアドレスが流出してしまっても、すぐに変更するかメールアドレスごと削除して、攻撃メールが送られてくるのを避けることができます。

思い入れがあり変えられないアドレスと違い、ウェブサービスなどに登録するアドレスは、すっぱりと変えたり捨てたりできるものを使いましょう。

一つのサービスからの流出によって、ほかのサービスに登録しているメールアドレスを変更するのが面倒なら、無限に近いサブアドレスを作れるサービスもあるので、それを利用してサービス毎に別々のアドレスを登録しましょう。

余談ですが、この方式でなら、攻撃者からスパムメールなどが来たときに、どのサービスから流出したかを知ることもできます。

なお、親しい人に限定して使っているアドレスでも、相手がマルウェアに感染して流出させる可能性もあります。さすがにその場合までは対処することができません。

ただ、逆に自分が流出させて迷惑をかけてしまう可能性もあるので、セキュリティを固め、自分から流出させないようにしましょう。

9 通信の安全と永続性を考えたSNSやメールの利用

メールの送受信での秘密を確保する手段として、送信者と受信者が「メールの送受信を暗号化している同じサービスを使う」方法について触れましたが、この「閉鎖された空間による安全性の確保」は、「すべての通信の暗号化を宣言しているSNSサービスを使ったメッセージのやり取り」にも当てはまります。

この場合、上記のメールサービスの利用と同じく、サービス全体が一つのセキュリティ方針で守られるので、安全性は確保されます。

ただし、SNSの運営企業によっては、すべての通信を暗号化しているかどうかを明確にしていない場合もあり、一般の利用者が自力で暗号化の状況を調べるのは容易ではありません。

現状では、検索エンジンで「自分が利用しているSNSの名前」＋「暗号化」などと入力して調べるか、暗号化を明言しているSNSサービ

スを選ぶしか方法がありません。本来であれば全SNSサービスが、暗号化とセキュリティの向上に対応してほしいところです。

この閉じた空間による安全性の確保は、確かに安全な通信に有効な手段である一方、様々な機器がつながりあって情報をやり取りする、「インターネット」の思想とは逆の発想でもあります。

本来は、多様なサーバがつながりあってバケツリレーが行われるメールであっても、すべての過程で暗号化が行われ、安全性が確保されることが理想なのです。

一方、現状では問題が残るメールですが、SNSと比較したメリットもあります。

メールは特定の企業サービスとは紐付かないインターネットの仕様なので、様々なメールソフトを使い、どのメールサーバに接続しても基本的には利用可能なのです。

一社によって提供され、栄枯盛衰（えいこせいすい）によってサービス終了する可能性があるSNSに対して、メールは永続性の点で有利といえます。

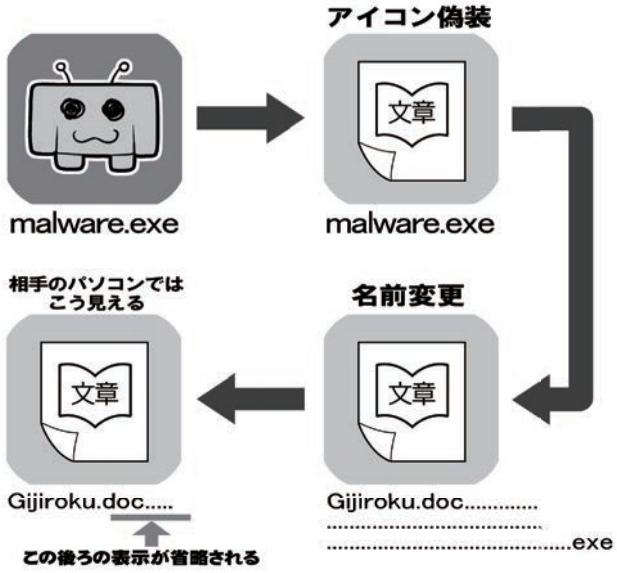
事実、インターネットの初期から様々なOSやメールソフトを乗り換えても、きちんとメールの内容を引き継ぎ、ごく初期のメールをきちんと見られる状況にしている人が少なからずいます。

SNSや各種通信サービスなどは、サービス終了時にデータのエクスポート(出力)の対応をすることもありますが、それらは保存されるデータであって、データが生きていた環境はサービス終了とともに終わってしまうわけです。その分、メールにはない、様々な華やかな機能を楽しむこともできます。

SNSとメール、どちらがいいかは人それぞれです。それぞれにメリットとデメリットがあるのでよく機能を理解して、自分に合ったものをうまく利用しましょう。

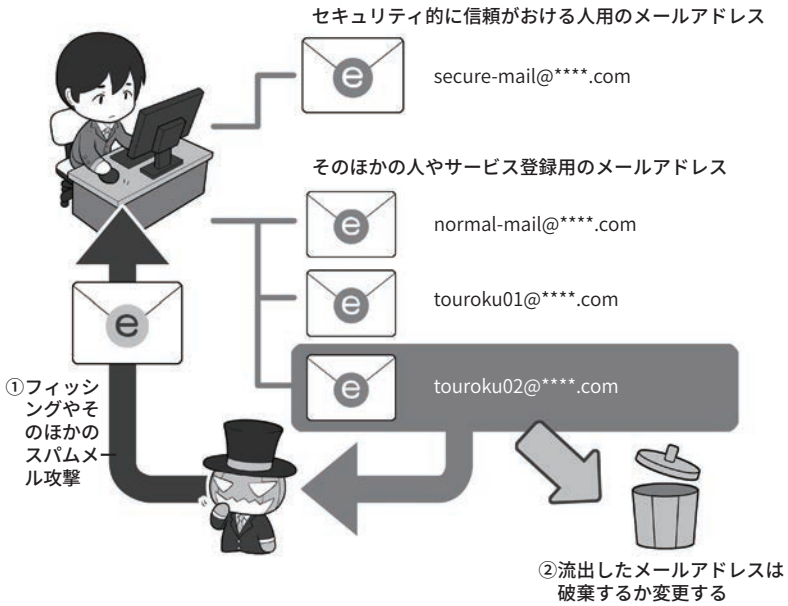
マルウェア入りファイルの偽装

マルウェア入りファイルの偽装



攻撃メールに添付されてくるファイルは、一見するとただの文章ファイルに見える場合もあります。しかし、ファイルのアイコンも名前も偽装したり、別のものに見せかけることは可能なのです

メールアドレスを変えてスパムメールから逃げる



メールアドレスの流出は、ウェブサービス側で管理しているものが攻撃者によって盗まれたり、ウェブサービス側の内部の人間が持ち出して売却したり、セキュリティ意識のない人がマルウェア感染して流出させることなどで起こります。愛着を持って長く使いたいメールアドレスは、むやみに人に教えたりウェブサービスに登録したりしないようにしましょう。流出してしまった場合に備えて、変更したり捨ててしまえるメールアドレスを活用しましょう。

5 データファイルを守る、暗号化で守る

もう一つ、通信にまつわる安全で考えなければならないのは「ファイルの暗号化」です。

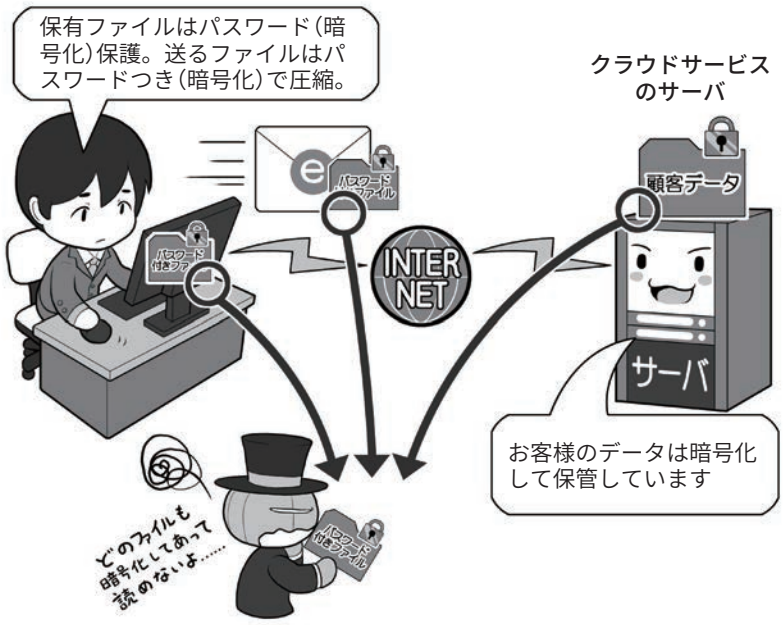
例えば、メールの添付ファイルが盗まれたり、保存しているファイルがマルウェアで流出したり、サーバに不正アクセスされて盗み見されても、また、ファイルの入った物理的な記録メディアを紛失しても、確実に適切な方法と鍵（暗号キー）で暗号化してあるならば、攻撃者が解読できなくなり、情報を流出から守ることができます。

ただ、ファイルの暗号化は攻撃者に盗まれると、高速なコンピュータを使って長い時間をかけて執拗に解読を試みられる可能性があります。「暗号キー」は基準にしたがって、長く複雑なものを設定しなければなりません。

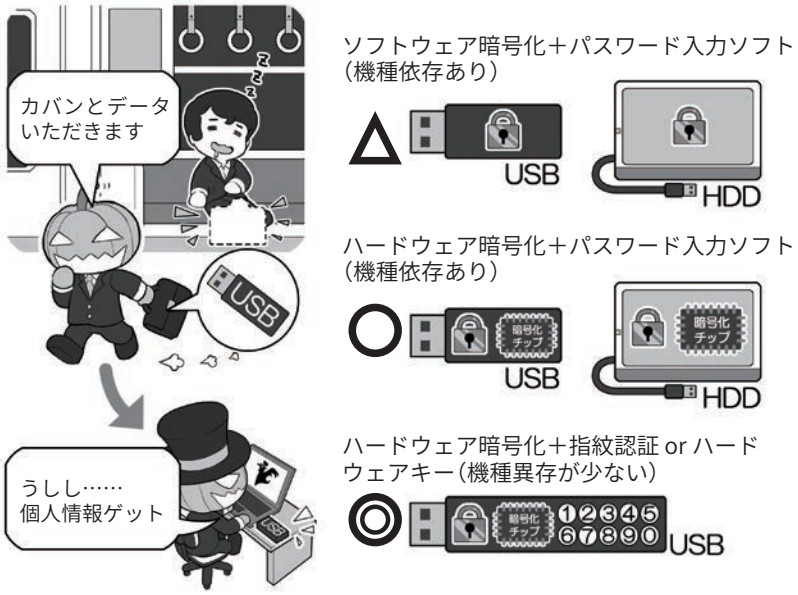
機密情報を持ち運ぶ場合は、ファイル単位の暗号化よりも、装置全体の暗号化機能が付いた外部記憶装置やUSBメモリの利用を推奨します。可能であれば、高速に暗号処理が可能で様々な攻撃に対策された暗号化チップが内蔵されたものを選択しましょう。そうすることで、ファイル単位の暗号化が不確実になった場合のトラブルも避けられます。

USBメモリの場合、汎用性と安全性を両立した、ハードウェアキーでパスワード認証をするタイプもあります。これらは、専用の認証ソフトウェアを必要としないので、利用するOSの依存度が少ないのと、ハードウェアキーの入力が「PINコード」と同じようになっており、入力を間違えると「ロック」や「データ消去」の保護機能があるほか、内部の「暗号キー」が十分に長く複

データの暗号化は保険



データを持ち運ぶときは必ず暗号化メディアを使う



＋「強制暗号化」＋「暗号化方式AES256bit以上」
＋「パスワード一定回数入力ミスで完全ロック（アクセス不能）」
あれば…「書き込み時ウイルスチェック（USBメモリ内機能）」

盗まれたメディアはリモートワイプができないので、より高度なセキュリティが求められます。しかし、それよりも重要情報を持ったまま飲酒したり、電車で寝たりすることは言語道断です。本来は暗号化よりもモラルが第一です。

雑なものが自動で生成され、この「暗号キー」の利用に「PIN コード」の入力を求めることで安全性を確保しています。

データの暗号化で重要になってくるのは「暗号キー」の運用です。

「暗号キー」は、英大文字小文字＋数字＋記号で、完全にランダムな15桁以上を基準としていますが、完全にランダムな場合、暗記することは困難になりますし、また、スマホのパスワード管理ソフトやパスワードノートを見て打ち込むのも一苦労になります。

かといって、パソコン上に保存したり付箋で貼っていたりすると「パスワードを利用場所に保管しない」というセオリーに反します。

現状は、単純で楽な解決方法はありません。ただ、暗記を前提にするのであれば、自分だけが知っているマイナーな曲の歌詞などからローマ字打ちで15桁よりかなり長くなる部分を抜き出し、一部を独自のルールで記号や数字に置き換えるなどの対策が考えられます。

また、暗号化したファイルを誰かとメールで受け渡しする場合、相手と「暗号キー」を共有する方法にも気をつけなければなりません。

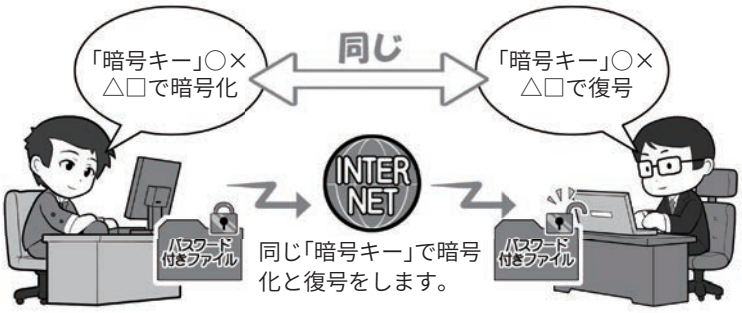
別送信であっても、暗号化ファイルと「暗号キー」を同じメールアドレスに送れば、メールが流出すると２つが揃ってしまいます。

「暗号キー」はメールでは送信せず、現実に会ったときに決めておくか、それができず、出先で突発的に送信が必要になった場合は、電話などで伝達するか、通信が暗号化されている「別系統の送信経路」で送るようにしましょう。

また、「暗号キー」には先ほども少し登場した、対になった２つの暗号キー（公開鍵と秘密鍵）を使ってやりとりする方式（公開鍵暗号方式）があります。この鍵は手で入力するのではなくパソコンが自動的に使うためのものですので、直接目にすることはないかもしれません。

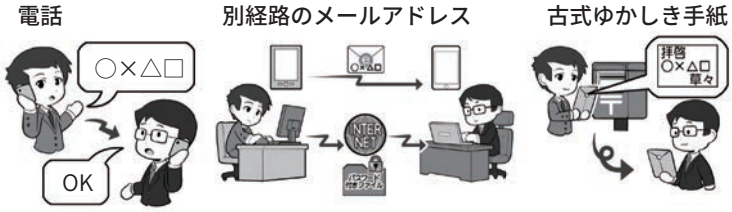
この方式を利用している具体例としては、P85 で紹介した「S/MIME」や「PGP」や、同じように目にすることはありませんが、Wi-Fi 通信の暗号化などがあります。

「暗号キー」が１個の方式（共通鍵暗号方式）



同じ「暗号キー」で暗号化と復号をします。

安全な「暗号キー」の受け渡しの例



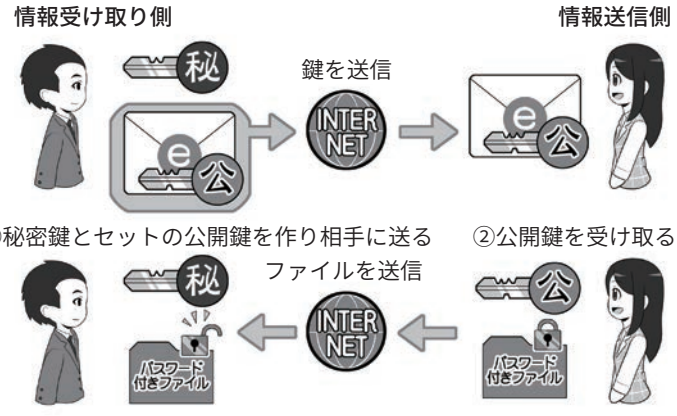
直接会ったときに「暗号キー」を渡したり、電話で直接伝えたりします。

盗聴やマルウェア感染を考え、スマホ対スマホなど別経路で送信します。

アナログだが一つの方法で、銀行などが利用しています。

どの場合であっても「暗号キー」の秘匿が重要です。

「暗号キー」が２個の方式（公開鍵暗号方式）



共通鍵暗号方式と異なり、「暗号キー」を送信しても大丈夫なのがポイントです。この方式では、「暗号キー」は手入力では使いません。メール送受信の影で使われていたりします。

コラム：究極の防御手段「ネットにつながない」エアギャップ

小さな会社の仕事などで、業務上どうしても個人情報などの入った顧客データベースを管理しなければならないが、マルウェアによる感染は怖いし、セキュリティを固められているか自信がない。

そんなときは、重要な情報の入ったパソコンを、極力ネットにつながずスタンドアロンパソコンとして使用するという手があります。

このネットにつながっているパソコンとスタンドアロンのパソコンの間、マルウェアが電子的に越えることができない壁を「エアギャップ（空気の隙間）」と呼び、立派な防御手段の一つとなっています。

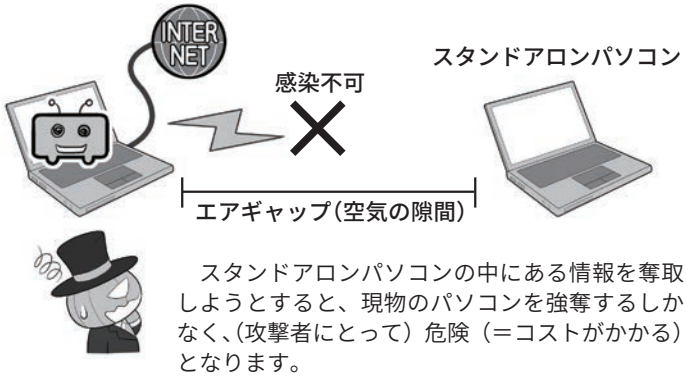
もし攻撃者が、このスタンドアロンのパソコンに入っているデータが欲しければ、物理的に事務所に忍び込まなければならず、それは、攻撃者にとって危険でコストがかかることであり、抑止力になるわけです。

ただ、データの盗難目的ではなく、破壊などが目的のマルウェアの場合は、USBメモリを介して感染させるという手法があります。それらを避けるには、きちんと管理できる人間以外がうかつにUSBメモリを挿せないように、パソコン側に鍵つきのUSB端子キャップなどを使いましょう。

余談ですが、この方式の場合、スタンドアロンパソコンが仮に感染しても、外部との通信ができないためデータの持ち出しは困難なのですが、パソコン内でのわかりきった場所にある少量の情報であれば、光るもの（LEDやパソコンのモニタ）、音、消費電圧の上下などを使って、外に向かって信号を送ることは可能であり、攻撃者がこれを観測できれば情報の奪取も可能となります。要するにこれらのものを使ってモールス信号を打つといわれればイメージがわくでしょうか。

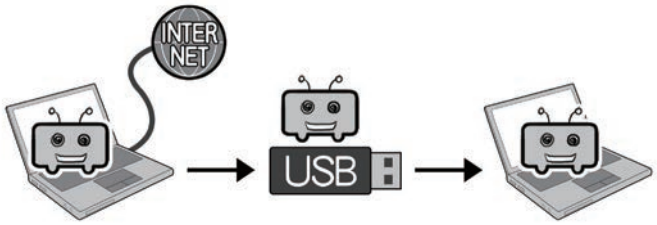
話題を戻して、エアギャップをインターネットバンキン

有線でも無線でも、つながっていないパソコンにはマルウェアは感染しない



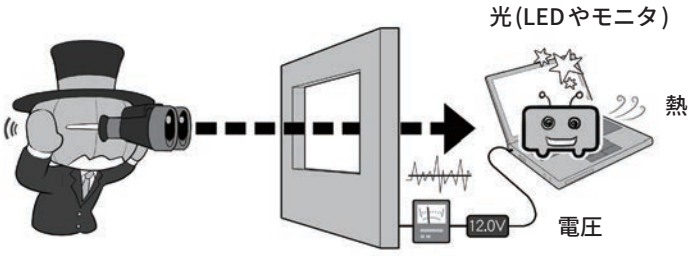
スタンドアロンパソコンの中にある情報を奪取しようとすると、現物のパソコンを強奪するしかなく、（攻撃者にとって）危険（＝コストがかかる）となります。

しかし、USBメモリを介して感染することも



かつて、イランで核燃料施設にあるスタンドアロンパソコンを感染させ、機器を暴走させた手法（Stuxnet型）です。ただし、攻撃者がマルウェアをネット経由で直接操作できないのと、データを抜き出すのは困難なマルウェアです。

ネットに接続していなくても、少量のデータであれば盗める



Stuxnet型で感染したパソコンに、あらかじめ特定のデータの内容を、デジタル信号の形で、光、音、電圧差などを使って発信させることは可能です。それを受信することができれば情報の奪取も可能です。ただし、通信速度は遅いので大容量のデータを盗み出すことは困難です。

グの不正送金の例に当てはめてみましょう。

インターネットバンキングのセキュリティの向上と、攻撃者の技術向上はいたちごっこであり、銀行などによって様々なセキュリティ対策が講じられますが、絶対に安全ということはありませんし、今後も難しいでしょう。

それは、攻撃者との技術競争的な問題もありますが、セキュリティに人間の心の隙という防御しにくい要素が含まれていることと、攻撃者がネットの闇に姿を潜めていて、現実世界でそこまでたどり着き、相手を捕まえることが容易ではないからです。

このうち、人間の心の隙に関しては一朝一夕に対策を講じることは難しいのですが、攻撃者がネットの闇から出てこなくてはならない方法で防ぐ手段はあります。すごくシンプルな方法でおどろくかもしれませんが、ようは取引をネットで行わなければいいだけなのです。

インターネットバンキングは確かに便利ですが、現在では、コンビニを含めあらゆる所にATMが設置され24時間稼働していますし、24時間送金可能なものもあります。したがって、多量の送金処理を毎日行うのでなければ、インターネットバンキングを使うのは「便利」ですが「必須」ではありません。

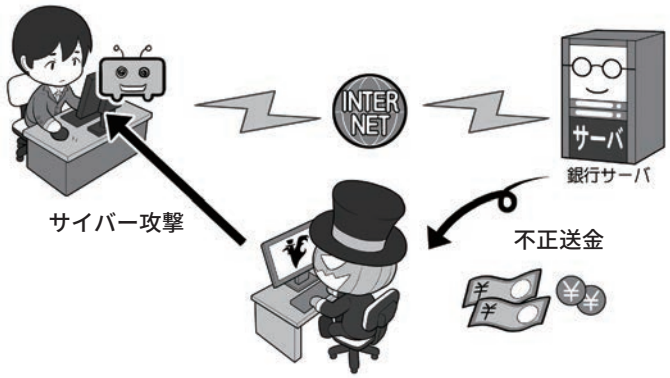
そして、ネットを利用しない場合、攻撃者が不正にお金を奪おうと思えば、現実世界でキャッシュカードとあなたの身柄を抑えて、暗証番号を聞き出さなければなりません。

そのようなことをすれば、当然のように顔もばれますし、リスク(コスト)も非常に高くなるので、攻撃者としてそういった手段は選びにくくなるでしょう。

このように、ときにはネットにつながない、ネットを利用しないという「ある種のエアギャップ」という選択肢をとることも防御の一つなのです。

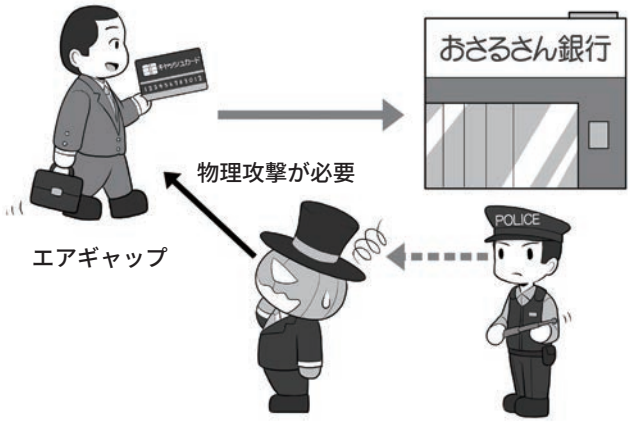
ネットにつなぐのは、「便利」の物差しだけで考えるのではなく、「利便性」と「危険性」を天秤の両側に乗せ、総合的に安全な選択肢をとるべきでしょう。

オンラインで銀行口座が狙われるなら



ネットを使って銀行口座から不正送金が行われるのは、そもそも送金処理をネットで行っていることと、攻撃者がネットの闇に潜んでいて、世界のどこにいるかわからず、検挙しにくいこともあります。

インターネットバンキングを止めるという手も



ネット経由ではなく、現実世界で送金処理を行うようにすると、当然ネットを使った不正送金はできませんし、お金を引き出す情報や鍵を持っているあなたと攻撃者の間には、エアギャップが存在することになります。無理矢理カードと暗証番号を手に入れようとすると、現実世界で窃盗や強盗をしなければならず、監視カメラなどにも映るので、リスク(コスト)がかかるようになります。このリスクが防御となるわけです。

コラム：「無料」ということの対価はなにか

インターネットでは、よく「無料」という言葉を見かけます。無料のメールサービス、無料のウェブサービス、無料の動画公開サービス、無料のアプリなどなど。

しかし、お店などの試食コーナーの図を見てもらうとわかりますが、私たち利用者の側から一見無料に見えても、サービスが提供されるときは必ず「コスト（費用）」がかかっています。そして、正常な企業であれば、コストが回収できないビジネスは行いません。そこにはなんらかの採算が取れるシステムが存在し、私たちが見えないところでお金が回って提供されているわけです。

その方法の一つは、広告による収益モデルです。広告主がウェブなどに広告バナーを出し、サービス会社はそれを資金源に運営するわけです。

広告システムがもう少し進むと、ウェブサービス会社が私たちのウェブ上での行動パターンや、趣味や属性などの情報を収集し、一見匿名の情報の形にして、これを広告主に提供、広告主は自社製品にマッチした人物向けに絞り込んで広告を打つなどして、より効果的な宣伝を行います。

このパターンでは、匿名とはいえ平たくいえば「私たちの情報」がサービスの対価として支払われているわけです。

また、先行投資といって、当初無料で提供し、サービスに馴染んだら、その後有料化してコストを回収するマネタイズを行う型もあります。

そして、最後にもっとも気をつけたいのが善意の無料サービスです。誰かがウェブサービスやアプリなどを開発し無料で提供するのですが、明示

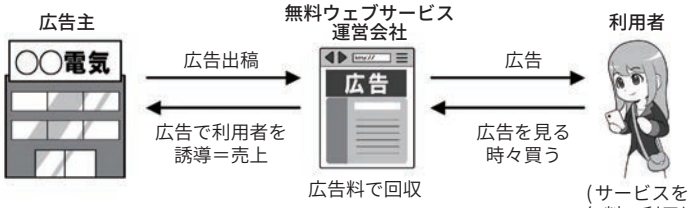
試食サービスのコストの例

（ソーセージを売る場合）

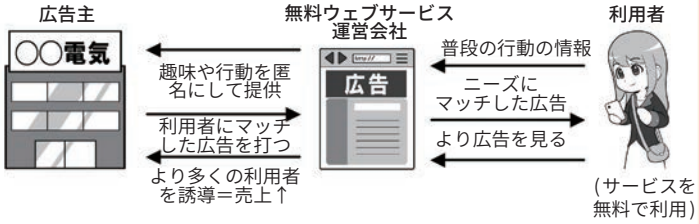
・食べる側は一見無料だが、人件費、光熱費、材料費は必ず発生し、どこかで誰かが必ず支払っている
・お店全体の売上や直接的なソーセージの売上の一部としてなど
・運営主体もしっかりして、コストも回っているので食べても大丈夫

無料ウェブサービスの例

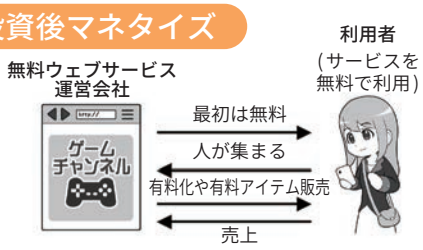
①無差別広告で運営



②利用者の情報を利用し、ターゲットに合わせた広告で運営



③先行投資後マネタイズ



④善意の無料サービス（ただし責任能力なし）

的ではなくても「責任は一切取りませんよ」という状態のものです。この場合コストは、提供する側のポケットマネーなどでまかなわれ、ビジネスとしては成立していないので、セキュリティに対して割くべきコストや労力がおろそかになりがちです。そして、ここが弱点として攻撃者に狙われ、利用される可能性があるわけです。

公衆無線LANの無料サービスの例も考えてみましょう。

政府機関・施設や自治体などが提供するものは、運営費とセキュリティの費用が、実は税金でまかなわれています。

携帯電話会社が提供する場合は、支払料金の中からまかなわれているので「追加料金無料」といった方がいいでしょう。

対価を払って利用する場合は、当然その支払料金が運営管理費用やセキュリティ費用にあてられます。

今回も問題なのは、「善意の無料サービス（ただし責任能力なし）」です。

小さなお店などで無線LANが提供されている場合、それは、仕事用のものを開放しているだけかもしれません。そして、無料で使っている以上利用者とは契約関係もなく、安全性を求める権利もないわけです。

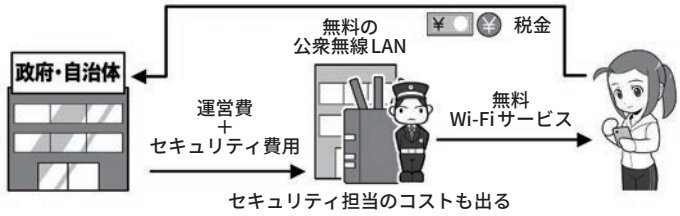
攻撃者は、このような所を狙って罠をしかけてきます。運営費もセキュリティ費用もないならば、誰も日常的に攻撃者の有無をチェックしないからです。

このような理由があるので、「運営主体がはっきりしていない、責任能力の無い無料の公衆無線LANは使用しない方がいい」というわけです。

無料という言葉には注意。費用の出所がはっきりしない場合、あなたが個人として高いツケを払わされることになるかもしれませんよ。

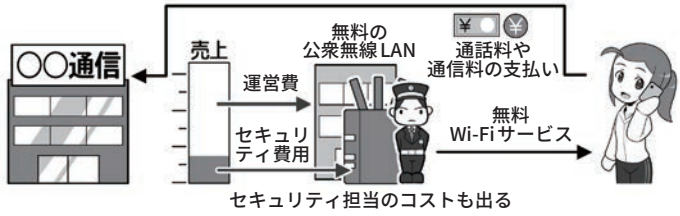
無料の公衆無線LANサービスの例

①一見無料だが税金などでまかなっているから無料



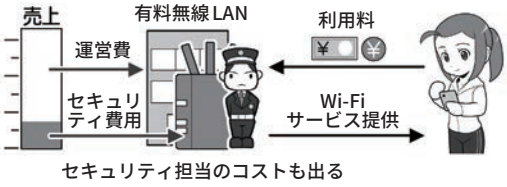
トラブルがあると議会などで取りあげられ問題となることもあります。責任能力もあります。

②企業が収入の中から払っているから（追加料金）無料



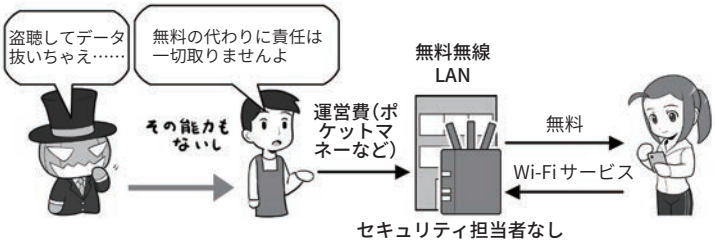
トラブルが起きれば責任問題となり、本業にも影響が出ます。責任能力もあります。

③対価を支払って利用する（有料）



対価をもらったサービスなので、トラブルが起きれば責任問題となります。

④善意の無料サービス（ただし責任能力なし）



対価はもらっていないので、トラブルは自己責任といわれたり、実質的に責任はとってもらえません（その能力もありません）。

コラム：クラウドサービスからのデータ流出。原因は？

クラウドサービスとは、「従来自分の手元で保存していたデータなどを、インターネット上のどこかに雲のように存在しているサーバに保存し、どの機器からでも、意識せず利用できる」サービスで、その雲的なイメージを指してクラウド（cloud）と呼ばれます。

最近では、スマホを利用していると、意識しないうちに写真などがクラウドサービスにバックアップされていることもあります。それに、ウェブブラウザがあればどこからでもアクセスできるメールサービスも、クラウドサービスの利用ともいえます。

ここで問題なのはクラウドサービスからの情報流出です。

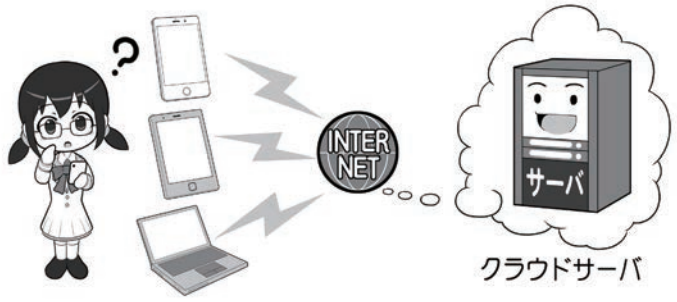
自分が管理している情報に様々な環境からアクセスできるという事は、正しい設定が行われていないと、意図していない第三者からもアクセスできてしまう可能性があるということです。実際に、クラウドサービス上に保存されているデータに、誰でもアクセス可能な状態が標準設定であることに気づかず、保存しているプライベートなスケジュール情報やメモ、写真や画像などの重要なデータが不特定多数に公開されていたというケースも発生しています。

そのような事態に陥らないためにも、クラウドサービス上に保存されるデータの公開設定がどうなっているかに加え、そのデータやファイルを、クラウドサービス上に保存することの適否をしっかり確認するようにしましょう。

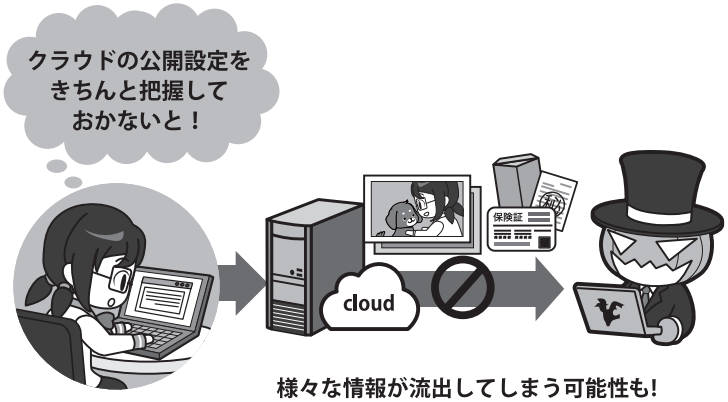
また情報流出するケースとして、利用者のパスワードが各種攻撃で破られ、クラウドから情報や写真を抜き取られるケースがあります。ここでの攻撃とは、「リスト型攻撃」「辞書攻撃」、そして、個人情報からの推測などです。ほかのサービスとIDとパスワードを使い回ししていて、侵入される場合もありますが、パスワードは誕生日やニックネームから推測した」という攻撃者の証言もよくあります。

こういった流出事故を起こさないためには、まずIDとパスワードを使い回ししないこと。 推測されるほど簡単なものにしないこと。多要素認証や、不正なアクセスがあった場合通知されるサービスを利用すること。そして何より、「流出して困る情報はクラウドサービスにアップロードしない・（自動で）されないようにする」ことです。

データはどこに保存されている？



スマホなどを使っていると、意識せずにクラウドサービスにデータをバックアップしていることもあります。



クラウドサービスの設定内容をきちんと把握しておかないと、初期設定で「外部公開」という設定がオンになっている場合があり、意図せず外部からクラウドサービス上に保存しているデータを見られたり盗まれてしまう可能性があり注意が必要です。

第４章

スマホ・パソコンのより進んだ使い方やトラブルの対処の仕方を知ろう

ここではパソコン・スマホの扱い方を中心に、安全を守る方法について勉強しましょう。
どのように情報を守るか、どのように安全にネットを利用するか、セキュリティを守るための技術を
障害物競走のように楽しめれば、みなさんのスキルアップになるでしょう。

1 スマホのセキュリティ設定

1 スマホにはロックをかけよう。席において離れたり、人に貸したりするのは×

スマホの情報を守る第一歩は、待ち受け時にロックすることです。

ロックにはPINコードによるロック、パターンロック、生体認証によるロック、また、最近では特定の機器（普段身につけているスマートウォッチなど）や、GPSに連動して特定の場所（自宅など）で自動的にロックを解除できる機能もあります。

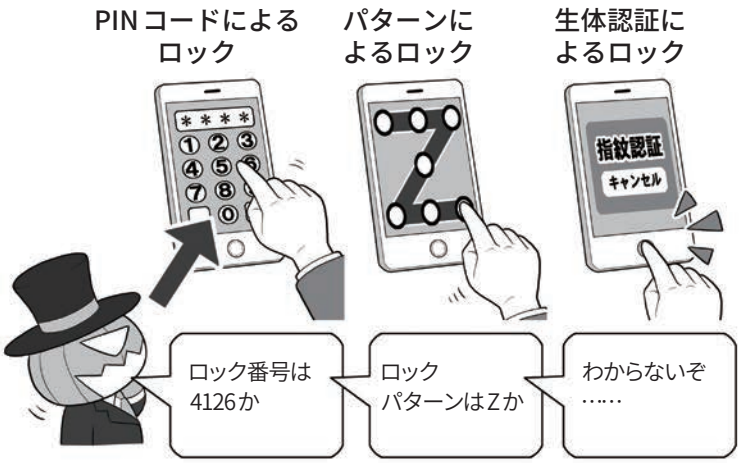
ただ、自分が明示的に指示をしないロック解除は、うっかり端末を無防備にすることもあるので、基本的にはなんらかの動作をして解除する方式にしましょう。周りから覗かれPINコードを盗まれる危険性の排除や、入力の面倒くささを省く点からは、生体認証を利用するのが便利です。

一方、生体認証にも弱点があります。お面や写真から復元した偽の指で指紋認証を破る研究や、「寝ているときに自分の指を勝手に使われ認証突破される」こともあります。生体認証だから安全と過信しないようにしましょう。

そして、各種のロック機能を設定しても、スマホのロックを解除を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、あるいは貸してしまったりすれば、一瞬で情報を盗んだり、乗っ取ったりすることが可能です。

スマホは、持ち歩く情報の金庫だと思って、必ず自分のそばに置き、こまめにロックをかけた状態　にしましょう。

スマホ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恐れがあります（特に、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、一瞬で盗み見アプリをインストールされたりすることがあります。注意しましょう。

2 情報漏れを防ぐ①

SNS用のアプリなどには、本体のロックとは別にアプリ用のPINコードなど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。守りが二重になります。一部の機種では、指紋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ているわけで、手間をかけさせ侵入を諦めさせるセオリーに沿っているわけです。

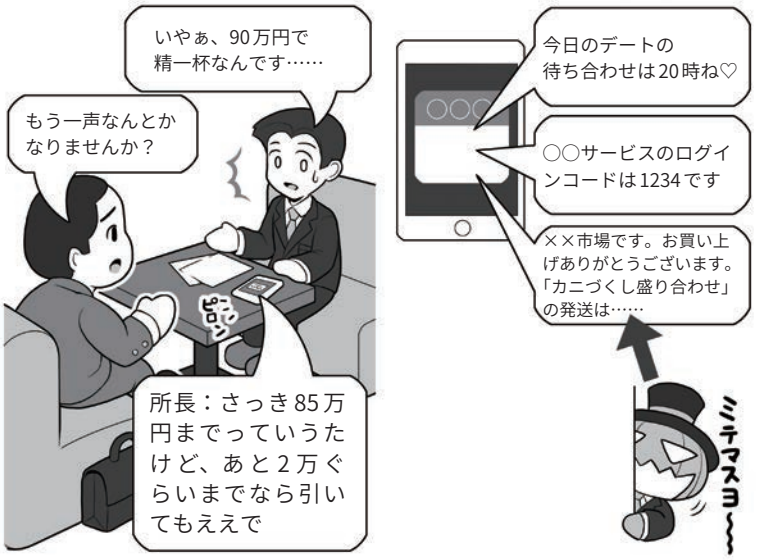
なお、アプリのPINコードを設定する場合は、スマホロック解除のPINコードと異なるものにしましょう。PINコードの使い回しはセキュリティがないのと一緒になってしまいます。PINコードも異なってこそ意味があるのです。

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。でも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、うっかり内部の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ます。

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確認メールも見られてしまうことがあり得ます。そうするとIDとパスワード＋ロックのかかったスマホだけでも、「正常に」ウェブサービスのセキュリティをパスできてしまうわけです。

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……。情報の扱いには気をつけましょう。

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、スマホを席に残してはいけません。なお、勝手に人のスマホのロック解除をすることはサイバー攻撃です。

3 情報漏れを防ぐ②

直接スマホを盗まれる以外の情報漏れのケースには、攻撃者による無線LANを使った盗聴があります。スマホから無線LANのアクセスポイントの間の、情報通信を盗聴するものです。これを防ぐには通信内容の暗号化が重要です。

暗号化のセクションの繰り返しになりますが、無線LAN利用時のチェックポイントとしては、

1. **無線LAN通信が暗号化されていて、かつその暗号化方式が安全であるか。**
2. **きちんと暗号化されていても、その通信で利用する「暗号キー」が他人に漏れていたり、共用になっていないかどうか。**

などがあります。

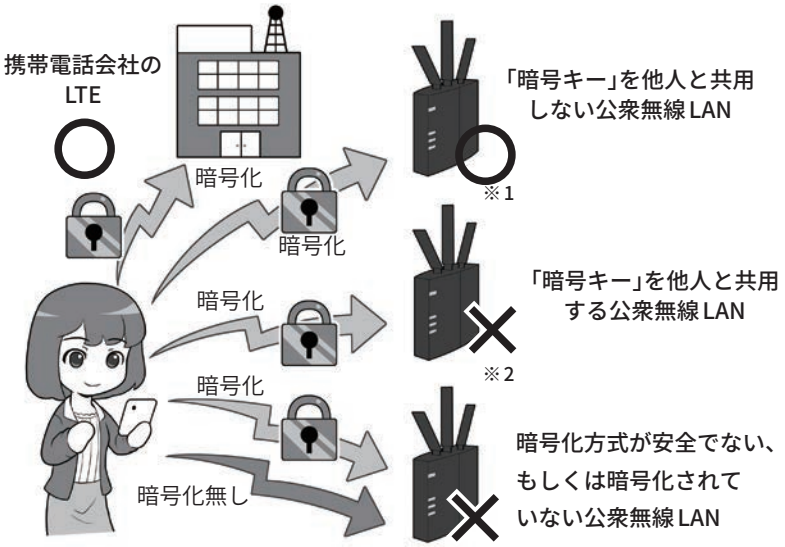
企業によって提供されている公衆無線LANであれば、上記の無線LANの安全性をきちんと理解して提供する能力があるかどうかをチェックしましょう。トラブルを発生させて「謝るだけ」の企業より、情報漏れの芽を摘み「万全の安全性のもとにきちんとサービスを提供する」企業の方が、はるかに優秀で信頼に足るのです。

その点をよく調べた上で、利用する公衆無線LANの企業を選択するのも、重要な情報漏れの防御策です。

次に、万が一、スマホを落としてしまった場合に、情報流出させない方法も考えましょう。

まずは、スマホのデータが暗号化されているかチェックです。古い機種では、初期状態で暗号化されていないことがあります。本体と記録メディアいずれも暗号化して、落としてしまっても簡単には利用できないようにしましょう。暗号化は本体のロックとセットとなり、必然的にロック機能もONにする必要があります。

屋外ではむやみに公衆無線LANを使用しない



そもそも、自分と「契約関係がない」ものは非常時以外は基本的に使わず、また、その中でも運営主体がわからない無線LANアクセスポイントは絶対に使用しないようにしましょう。

※1 携帯電話会社やプロバイダが提供していても、「暗号キー」が共用でないとは限りません。きちんとチェックしましょう。

※2 暗号キーが貼り出してあるような公衆無線LANは、「暗号キー」が他人と共有になり危険です。使わないようにしましょう。

無線LAN暗号化などに関するより詳しい説明は、P70からを参照して下さい。

盗難されたときのために中を見られないように暗号化しよう

本体もメディアも暗号化。最近では、暗号化が標準のものがほとんどですが、必ず確認しましょう。

スマホを落としたときの次の対策としては、リモートロック、位置情報確認やリモートワイプ機能を使える状態にしましょう。

iOSでは、iCloudの「iPhoneを探す」、Androidでは、「スマートフォンを探す」として、それぞれ該当の機能があり、パソコンや同じアカウントを紐付けたほかの端末から操作ができるようになっています。無料なので必ず試してマスターしておきましょう。

リモートロックとは、遠隔操作でスマホをロックして使えなくする機能です。スマホの所在がわからなくなったら、なによりもまずスマホをロックしましょう。

次に、「位置情報」を確認しましょう。事前にこの機能を使ってスマホの位置確認ができるかどうかを試し、確実に使えるように設定しておきましょう。ただし、子どもの端末などの監視目的では、絶対に使わないようにしましょう。この理由は後ほどご説明します。

建物の中などでは、明確な場所が特定できない場合もありますが、現在のスマホのおおよそのありかが地図上に表示されます。

見つかった場所が、自分が訪れたお店や、遺失物として届けられた警察などなら、連絡をして取り戻す段取りをします。一方、そうではない場合は、最後の手段として情報漏れ防止のために「リモートワイプ」機能でスマホの中身を全部消すことも考えましょう。ただし、リモートワイプをすると、位置情報を取ることができなくなりますので、情報を守るための捨て身の手段になります。

そして、仮にスマホが戻ってこなくても、本体を買い直したらすぐに復旧できるように、スマホの中身は定期的にバックアップしておきましょう。

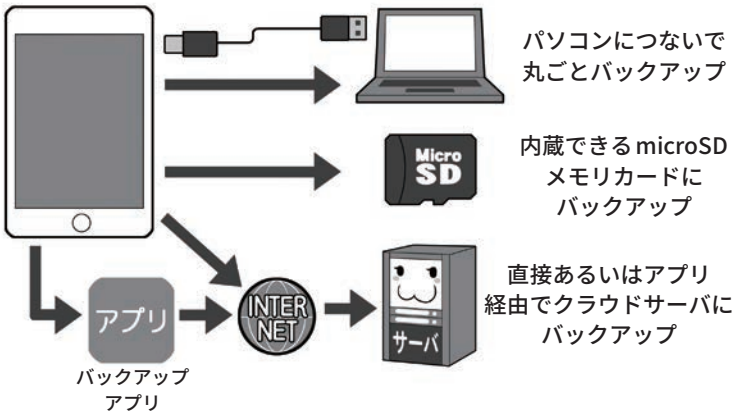
機種によっては、パソコンでバックアップすると、新しいスマホをつないでボタン一発指示するだけで復元できるものもあるので、機種選定時に調べておきましょう。

紛失や盗難時のために準備をしておこう

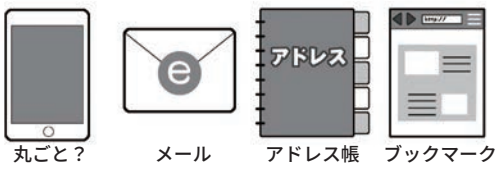
※リモートワイプすると、位置情報が確認できなくなるので、リスクが少ないならばロックだけ行い、遺失物として警察に相談するなどの手段をとりましょう。

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



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。

4 スムーズな機種変更と、予期せぬデータ流出の防ぎ方

スムーズな機種変更を行うためには、その前に機種変更手段を調べておくことが重要になります。

バックアップの項目でも書きましたが、「丸ごとバックアップ」「データごとにバックアップ」「アプリを使用してバックアップ」など様々な方式があります。このあたりは自分で調べるとともに、実際に機種変更やデータの移行をしたことがある人に聞いたり、記事を見たりしつつ、どの方法が便利だったり簡単だったか、アドバイスを求めるといいでしょう。

最近では、データがスマホ自体の中（ローカル）にあるだけでなく、インターネットのどこか、利用者から見て姿が見えない雲のような存在のサーバ（クラウド）に保存されている場合もあり、機種によっては移行のためのバックアップ作業という概念そのものがないこともあります。

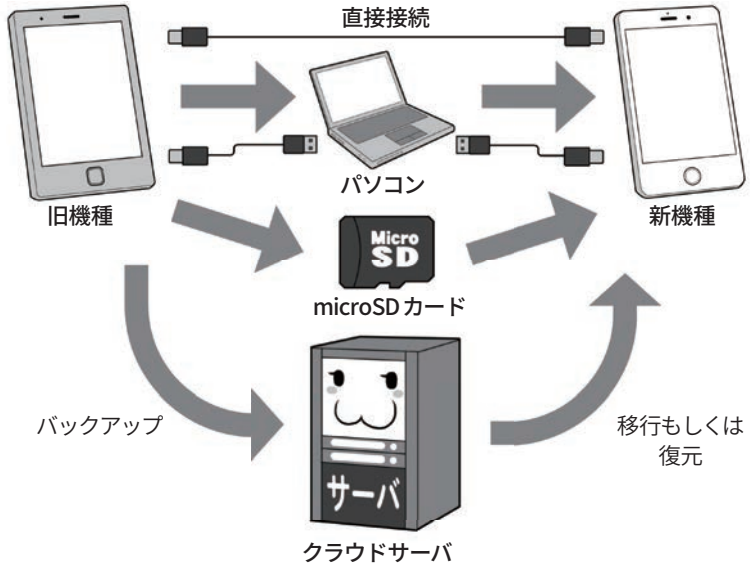
また、本体のデータ移行処理とは別に、機種変更に際して、特定の機能の移行処理をしておかなければならないものもあります。

例えば、いわゆる「おサイフケータイ」に関する機能では、一旦情報をサーバ側に預け、かわりにパスワードを受け取り、スマホから機能を削除して、その後新しい機種でログインして貰ったパスワードを使い機能を復元する処理が必要になるものもあります。

一部のSNSでは、旧機種がアクセス可能なまま新機種がアクセス可能になって、複数台から同時アクセスできないように、移行処理の前に一度手続きを踏んで、旧機種からSNSにアクセス権を削除してから、新しい機種でアクセスするための利用開始の手続きをするものもあります。

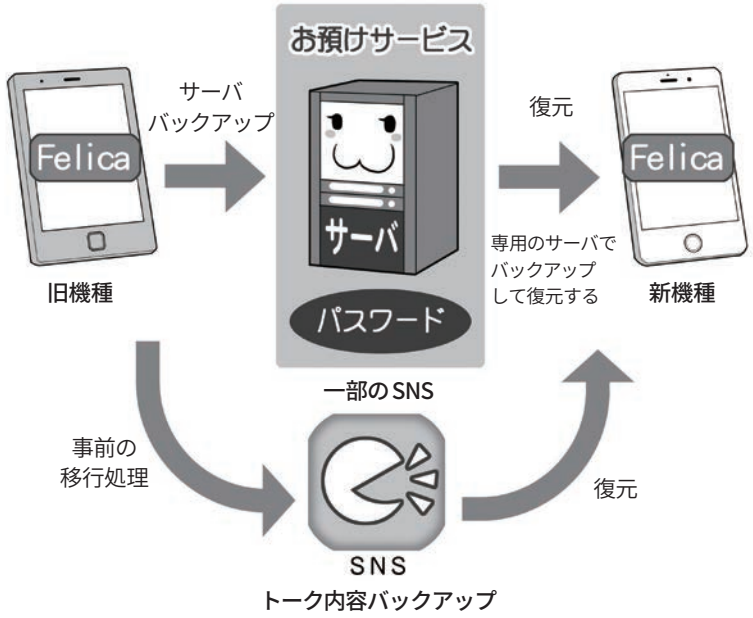
いずれの場合も、機種変更の移行処理にあたって、移さなければならない機能を紙などに書き出し、それが網羅されているかどうかをチェックしてください。さもないと、電子マネーが旧機種とともに消えてしまって取り戻すのが困難になることもあります。

データの移行は事前に手段を調べる



移行処理は事前に目的の機種でどういった移行手段が使えるのか調べておきます。

おサイフケータイや、SNSデータなどの移行



次は、機種変更をした後の情報流出を防ぐ処理です。

機種変更した前のスマホには、個人情報である住所録、撮りためた写真、今までやりとりしたメールなど、あなたの情報が全部詰まったままになっています。売却、譲渡や廃棄する場合、データを必ず消去しなければなりません。さもないと、知られたくないメールや写真が流出したり、住所録にある友人宛にフィッシングメールが送られてくるかもしれません。

また、修理に出す場合でも、モラルの低い修理会社が、芸能人のスマホから写真を抜き出して流出させた例があるので、必ずデータをすべてバックアップをした上で、本体のデータは消去してから修理に出したほうが安全でしょう。

手順としては、各種サービスはアプリもウェブもすべてログアウト。続いて、それぞれのスマホにある「初期化」や「データ消去機能」を使って内部のデータを消去します。

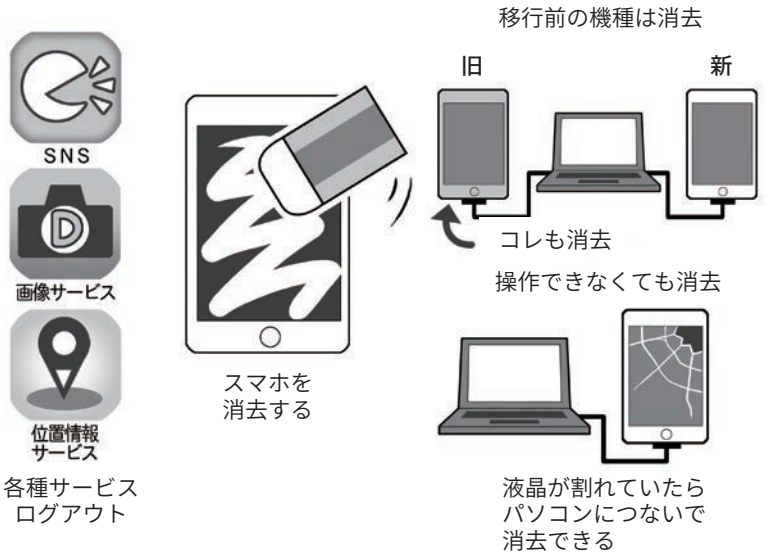
一部のスマホでは、紛失時に探せるように設定した「位置情報を確認するためのサービス」を事前にログアウトしておかないと修理などに出せないものもあるので、消去の前に確認してください。

落としてしまって液晶が割れ、操作ができない場合、消去することもできないと思いがちですが、パソコンに接続することで消去することが可能ですので、あきらめず必ず行いましょう。

業務用に使用しているスマホなどで、万が一にでもデータが復元される可能性を排除したい場合は、各携帯電話会社や家電量販店などで、スマホを物理的に破壊してくれるサービスを利用して、データを読み出せないようにしてしまいましょう。

余談ですが、業務用などで情報漏えいのリスクを少しでも排除したいなら、中古品を使ったりしないようにしましょう。中古販売店が良心的でも、プロの組織が仕込むようなマルウェアやバックドアには対処できない可能性があります。それを排除するには信頼できる国で生産された、正規ルートの新品を購入して使いましょう。

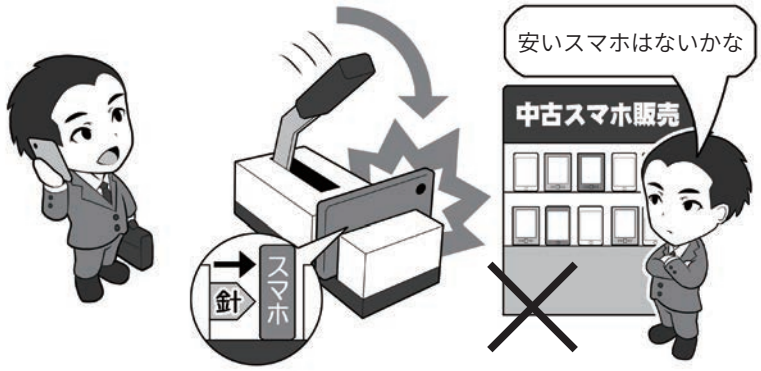
転売、譲渡、廃棄のときは必ずデータを消去する



消去する前には、利用しているサービスはすべてログアウトして、サーバなどに情報を預けなければならないもの（おサイフケータイ）などは預けましょう。SNS で移行処理が必要なものは行っておきます。その後、移行処理をして、移行後きちんと復元できたら、前の機種を売却・譲渡や廃棄する場合は、必ずデータを消去しましょう。

液晶が割れて操作できなくても、パソコンにつなげば消去することはできます。

業務用のスマホは物理的に破壊する。心配ならば新品で情報流出の可能性を排除する



仕事に使うスマホを廃棄する場合は、物理的に破壊する機械がある場所に持ち込んで破壊しましょう。大手携帯電話会社での回収も信頼できます。

一方、中古で購入したスマホに攻撃者がスパイウェアを仕込んでいて、企業の情報が流出しても、販売したものにその責任を取る能力はないでしょう。ましてやオークションでの購入などではなおさらです。前所有者の残債で購入後使用不能になるケースもあります。業務用に使用するなら IT 機器は新品を利用しましょう。

2 パソコンのセキュリティ設定

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、まず復旧のときに必要になるリカバリメディアを作成しましょう。

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外付けDVDドライブやUSBメモリで作成します。

また、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」が必要になる場合があります。本体の裏側などにシールで貼られているか、付属しているリカバリメディアに貼り付けられているので、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。

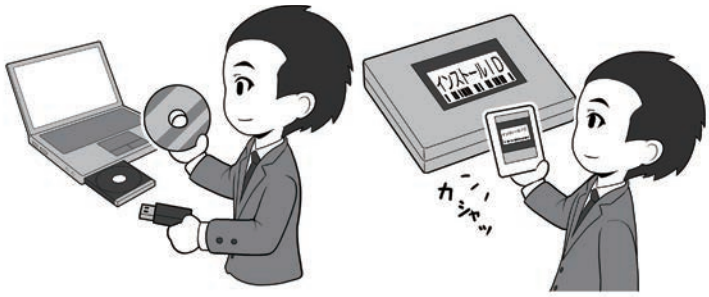
次に、セキュリティの設定をします。初期設定時にIDと「ログインパスワード」の設定を必ず行いましょう。また、マニュアルにしたがって起動用「BIOSパスワード」や「ファームウェアパスワード」といった、電源を入れた段階で入力することを求められるパスワードを設定しましょう。

これを設定しておくと、盗難されてもそもそも電源を入れることができなくなり、盗難時の情報流出をより防ぐことができます。

生体認証を使用する場合は、パスワードのセオリーにしたがって「ログインパスワード」を設定した上で、生体認証の登録を行い、セキュリティを高めつつログインの手間を省きましょう。

生体認証機能が無い場合はパスワードをしっかり設定しましょう。

パソコンを買ったらまずリカバリメディアを作る



DVD-R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、セオリー通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きます。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。

2 暗号化機能などでセキュリティレベルを高める

パソコンを盗まれたときに、情報が流出しないように、攻撃者に嫌がらせ、ではなく、セキュリティレベルを上げましょう。

会社のパソコンは、泥棒などが盗んで帰れないように、ワイヤーロックという盗難防止用のワイヤーで、くくりつけて移動できないようにしてあります。

こういった場合、攻撃者は情報だけでも入手すべく、パソコンの内部記憶装置(ハードディスクやSSD)だけを盗む場合もあります。

そうやって盗んでも情報が漏れないようにするため、内蔵記憶装置には暗号化処理を行いましょう。

この場合の「暗号キー」は「ログインパスワード」と共用になっているものもあるので、その場合はより複雑な「暗号キー」のセオリーに従い、15桁以上に設定します。

きちんとした複雑さと長さの「暗号キー」で暗号化された記憶装置は、盗んで別のパソコンにつないで暗号化を解除しようとしても、解読が非常に困難であり、情報流出を防ぐ力になります。

また、スマホにあるロック機能やリモートワイプも、業務用でかつLTEなどの通信回線を内蔵している一部パソコンでは可能です。

特に、こういった用途を前提に開発をされている機種は、相手から電源が入っているように見えない状態で記憶装置の中身を初期化することもでき、重要情報を持ち出す必要がある場合は有効な防御手段となります。

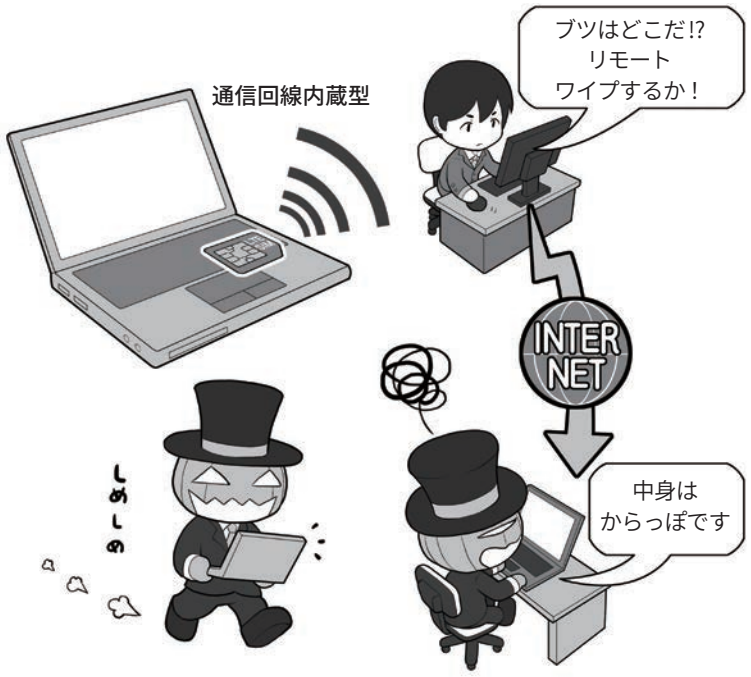
なお、スマホほどの精度ではありませんが、こういったパソコンでは、GPS無しでも盗まれた機器の現在地を探索することができるので、置き忘れのままや届け出られてる場合は取りに行き、盗まれている場合は情報を添えて警察に相談しましょう。

盗難にそなえての記憶装置の暗号化

OSの機能や暗号化チップなどを使って記憶装置を暗号化する

暗号化のための専用のTPMチップで暗号化されている記憶装置は、「暗号キー」が元の本体のTPMチップ内に残されているので、記録装置を盗み出しての暗号化解除がさらに困難になります。

パソコンでもリモートワイプはある



業務用の一部パソコンでは、起動をさとられないステルス状態でリモートワイプなどが可能です。盗んだ相手が気づく前に処置することができます。

もちろん、そもそも盗まれないようにするのが第一ですが。

3 マルウェア感染に備え、3-2-1のバックアップ体制を整える

マルウェアに感染しにくいようにするには、システムやソフトウェアを最新の状態に保つこと、セキュリティソフトを導入し同様に最新の状態に保つことが重要です。しかし、それでも感染してしまったとき、素早く復旧させるためには、定期的なバックアップが重要です。

バックアップは「3-2-1ルール」といって、少なくとも3個以上の複製、2種類以上の記録メディア、1個は遠い場所に保管することを推奨します。具体的には、パソコン＋バックアップ用外部記憶装置＋クラウドサーバといった形です。

メインのバックアップ用記憶装置は外付けで、最低でも内蔵記憶装置の3〜4倍の容量にし、何世代分かのバックアップを可能にいましょう。また、昨今顕著な、パソコンの中のファイルを勝手に暗号化し、解除するには身代金を要求する「ランサムウェア」に対抗するために「定期的にバックアップをしつつ、普段は本体に接続しておかない」という、やや煩雑な対応が必要です。こうすることで、バックアップ用記憶装置もろとも暗号化されることを防げます。

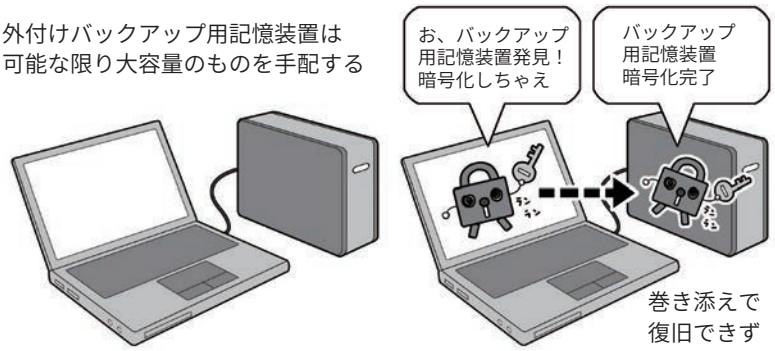
また、特に重要なデータは、信頼できるクラウドサーバ上にセキュリティを固めた上でバックアップして、地震だけでなく仮に自宅が風水害などに遭っても、復旧できるようにしておきましょう。

ランサムウェアをはじめ、こういったマルウェアの感染はネット経由だけだと思われがちですが、それだけとは限りません。

例えば、仕事相手の会社の人から「資料をコピーしてくれ」と渡されたUSBメモリにマルウェアが仕込まれていたり、パーティでプレゼントされたデジタルカメラに仕込まれていたりというケースも実際に存在します。注意しましょう。

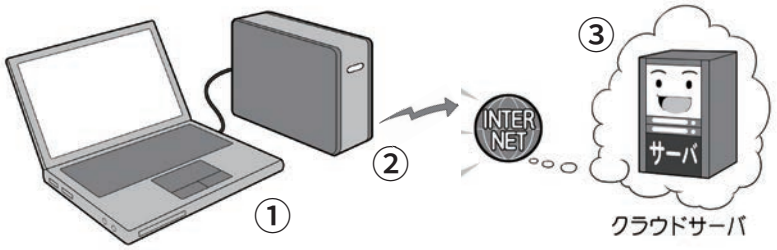
バックアップの体制を整える

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



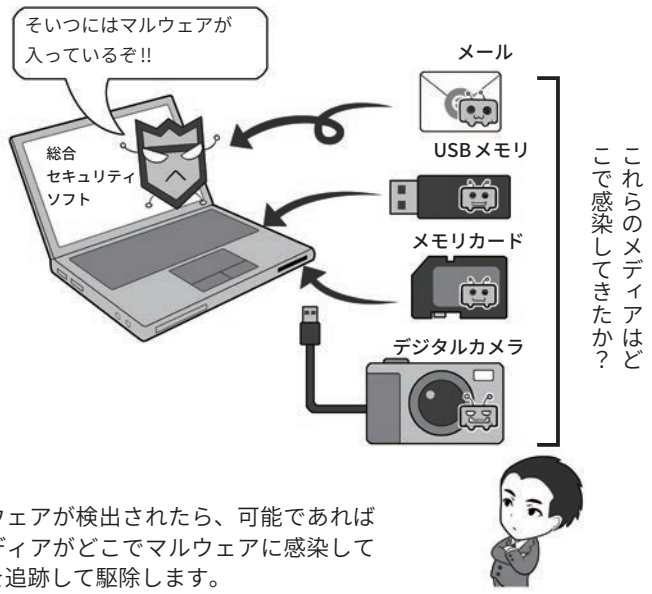
環境を整えたらバックアップを開始します。ソフトの導入や、環境を変更したらバックアップします。システムのアップデート後もバックアップします。ただし、バックアップ用記憶装置を常に接続しておくとランサムウェア感染で巻き添えになって、復旧に使うためのデータも失われてしまいます。

バックアップは3媒体、2種類、1個は遠い場所



本体＋バックアップ用外部記憶装置＋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で、攻撃者に乗っ取られないようにしましょう。

様々なマルウェア感染源に注意する



マルウェアが検出されたら、可能であればそのメディアがどこでマルウェアに感染してきたかを追跡して駆除します。

4 売却や廃棄するときはデータを消去する

スマホの廃棄と同様に、パソコンの廃棄でも、個人情報、メールや写真などの情報流出を防ぐため、記憶装置に含まれるデータを絶対に読み出せない形で確実に消去しなければなりません。

ハードディスクが正常に読み書きできる状態で、パソコン本体にディスク消去機能があるならそれを使い消去。無い場合は消去用のソフトウェアを利用。裸のディスクで保管していた場合などは本体に接続して消去するか、消去用の専用機器などを利用しましょう。

データの最低限の消去は、ディスク全域に無意味な情報を複数回書き込むことで、記録されていた情報の残留の可能性を消す方法が考えられます。例えば、かつて米国国防総省や軍などでは、この方式で3〜4回以上の繰り返し上書きによる消去を推奨していました。

なお、SSDはデータの管理方式がハードディスクとは異なるので、この方法では消えず、注意が必要です。生産メーカーの専用ソフトや破壊装置を使う必要があります。

故障して正常に読み出せない、あるいは機密性を求められるものの場合は、本体から取り出し物理的に、もしくは磁気的破壊する必要があります。

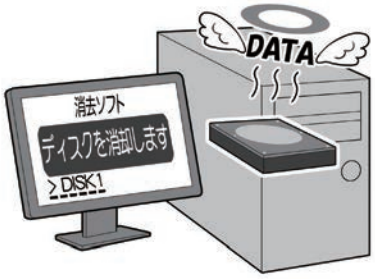
有料ではありますが、家電量販店などに破壊サービスがあります。これらは自分が見えるところで破壊してくれるので確認しましょう。

企業などで多量に廃棄する場合は、きちんと安全が確保された環境で、ディスクを読み出し不可能な状態に破壊するか、破壊用の専用機器やハードディスクやSSDでも粉砕できるシュレッダーの導入も検討しましょう。機密性を確保し情報漏洩を防止する投資です。

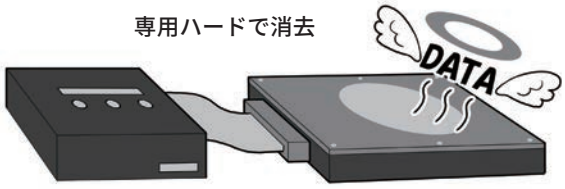
記憶装置の中のデータは必ず消去する

内蔵機能で消去

消去ソフトで消去



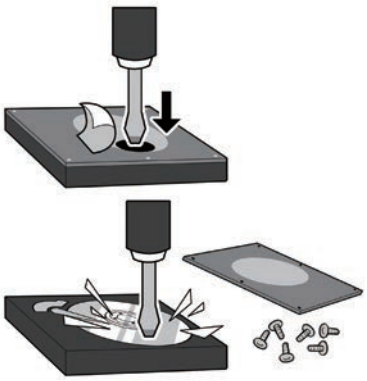
専用ハードで消去



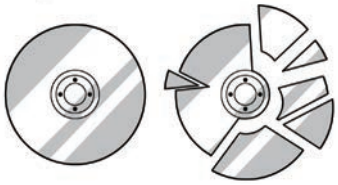
最低3回以上の繰り返し消去(データ上書き)処理をするモードを選択します。

動作不能、あるいは機密性確保には破壊する

ハードディスクは破壊用の穴を使うか、分解してディスクを取り出し壊す

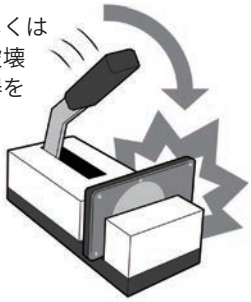


中のディスクを割るか、穴を開ける



目の前で破壊してくれる店に持ち込む(有料)

物理的もしくは磁気的に破壊できる機器を購入する(企業など向け)



ガラス製のディスクならば、割れれば OK です。金属製ならば、ドリルを利用して穴を開け読み出し不能にします。壊れて動かなくても、記録ディスクだけをほかに移植して読み出すという手段があるので確実に破壊しましょう。SSD は中のメモリチップを物理的に破壊するのが理想です。

5 盗難や紛失のとき、スマホとパソコン、どっちが安全？

盗難や紛失という視点から見たときに、スマホとノートパソコンとデスクトップパソコン、どれがより安全なのでしょう。

置かれている環境にもよりますが、「盗まれた後」までを、その要素に入れて考えてみます。

図のとおり、人目に付きやすいスマホは、当たり前ですが盗みやすい。その代わり盗難時の不正なロック解除は困難。また、基本的に通信機能があり、落とした後の位置情報の確認や盗まれたときのリモートロックやリモートワイプ機能といったセキュリティ機能が標準で備わってます。

ノートパソコンは、ログインパスワードの試行に制限が無い場合もあり。一方、PIN コードや指紋認証型もあり。盗難された場合に場所を特定し取り戻すには LTE などの「通信機能内蔵」が現実的な最低条件となり、現状ではほとんどの機種で利用できないので、盗難や紛失した後の探知が困難です。

デスクトップパソコンは、基本的に屋内にあるので、空き巣に入られるのでもなければ盗まれたり人目についたりすることが少なく、また、大きいので目立たないように持ち運びは困難。したがって盗まれる機会が少ないので、盗難後の探知機能は必要ないといえばありません。代わりに、設置場所の戸締まりや監視カメラの設置で安全性を高められるので、その分は補えるでしょう。

結果として、「実質的に盗難紛失時のリカバリ手段のないノートパソコン」が、盗難紛失に最もリスキーといえるかもしれません。

そうなった場合のために、せめてデータを読み出すことができない起動用パスワードや記憶装置暗号化の手段を講じておきましょう。

要素から安全性のポイントを検証する

	盗まれにくい	人の目につきにくい	ロック解除が困難	LTE などの内蔵通信機能	GPS を使った位置情報	リモートロック リモートワイプ
スマホ（タブレット） 	×	×	○ 生体認証 PIN コード 多数失敗でロック	○	○	○
ノートパソコン 	△	△	△ 失敗しても ロック無しも ○ 生体認証 PIN コード	△※1	△※2	△※3
デスクトップパソコン 	○	○	△ 失敗しても ロック無しも	×	×	×

※1　LTE などの無線 WAN 通信機能を内蔵しているものが対象
※2　LTE など内蔵機のみ。ノートパソコンの場合は GPS が内蔵されていなくても、通信基地局を使ったおよその位置確認が可能な場合もある
※3　LTE など内蔵機のみ。リモートロック、リモートワイプを本体が起動していないように見せつつ行うことは、専用に設計された機種のみ可能

コラム：ダブルラインでトラブルに備える

インターネットを閲覧していると、突然サーバが無反応になることがあります。そのときどうやって対処するのがいいのでしょう？

使用しているパソコンやスマホが原因なのか、無線LANか、それともウェブサーバ自身がダウンしているのか。それを特定し、別経路でのアクセスを確保するのです。

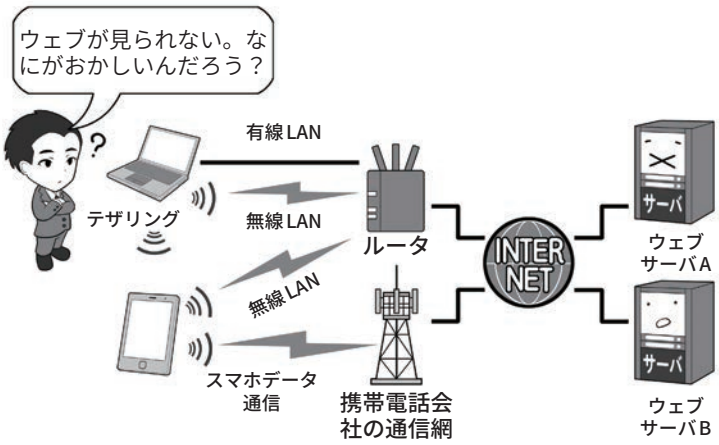
それには主要な機器の二重化(ダブルライン化)が有効です。パソコンで見られないならスマホで確認。無線LANがダメならば有線で。ルータがおかしいならLTEで。Aというサーバがダメならば Bへアクセスして、トラブルが発生した部位の機器を避けるなどの処置をしましょう。

また、所有する特定の機器がマルウェアに感染したり、セキュリティホールが明らかになったアプリなどを避けてサービスを利用したりする場合も、同様の考え方になります。

特定の機種へのサイバー攻撃が流行っているなら別機種で、ウェブブラウザにセキュリティホールがあるなら別のブラウザで。問題があるものを避けて利用するわけです。

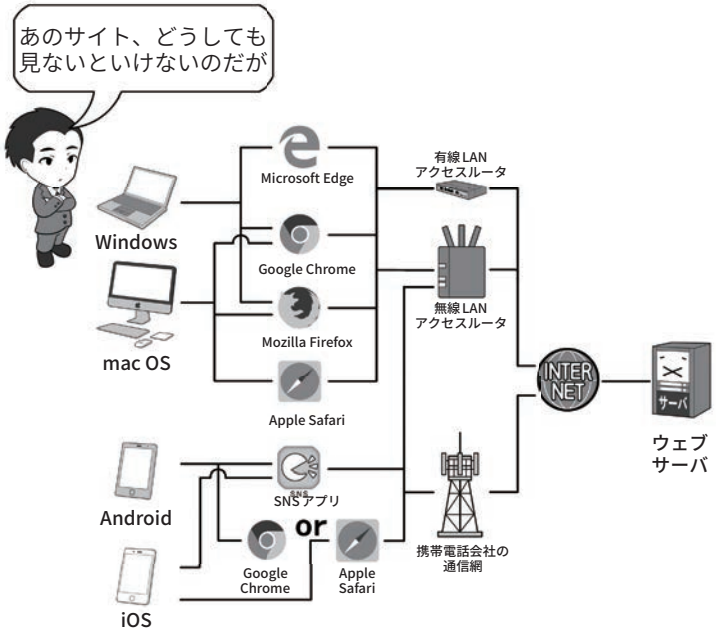
複数台の機材を持つ場合は、機材のタイプを分散することも備えとしては有効でしょう。生物界でも特定の品種に偏った生物は、一つの病気(ウイルスなど)で一気に絶滅に追い込まれる可能性があります。

通信状態がおかしいときに問題点を絞り込む手段



自分から見ると、インターネットのウェブサーバを見る機器、ルータまでの通信方法、インターネットまでの通信方法、そして、目的のサーバまで切り替えることで、どの部分にトラブルがあるかを絞り込めます。なお、すべてを切り替えてもネットが表示されない場合は、しばらく時間をおいて確かめましょう。いずれかの場所で通信が集中し混雑して通信ができなくなっている可能性があります。

パソコンがマルウェアに感染したり、ブラウザがセキュリティホールで使えないときの回避手段



Windows にトラブルが発生したら mac OS で、特定のウェブブラウザにトラブルが発生したら別のウェブブラウザで、スマホのアプリにトラブルが発生したらウェブブラウザ経由で利用するなどの回避手段を設けるのも、一つの防御手段です。

ここでは、簡略化して描いているため、上のイラストを含めインターネットの部分で二重化が収束してしまっているように見えますが、そもそもインターネットは通信経路上にあるサーバが攻撃で破壊されても、迂回して通信が確保されるようになっているので、通信が断絶するトラブルがあった場合、自然と迂回路が形成され通信が確保されるはずです。

雑草のような多様な環境を　作って、力強く備えましょう。

3 それでも攻撃を受けてしまったときの対処

1 兆候に気をつけて、被害が出たら対処

ここまでお伝えしてきた内容を的確に実行してもらえれば、定型化されているサイバー攻撃のかなりの部分は防げるでしょう。

しかし、それで安心してはいけません。人間の心の隙を突く攻撃をしかけられたり、セキュリティホールの発見に対してパッチなどの提供が間に合わない状態で、ゼロデイ攻撃をしかけられたら、防ぐことが難しいからです。

ですから、攻撃を受けたときの兆候を敏感に察知する能力を身につけ、これに対処するスキルを磨きましょう。

攻撃の兆候の中からいくつかの例をあげてみます。

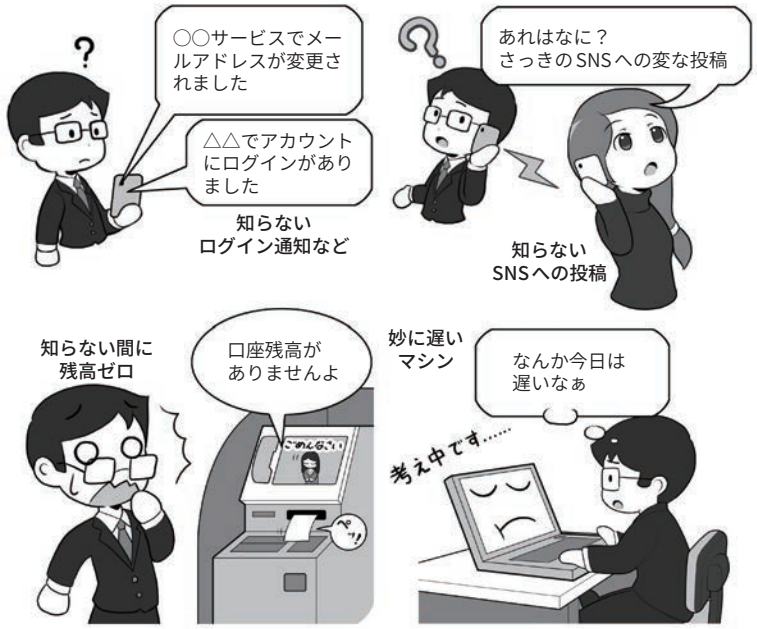
アカウントの乗っ取りは、知らないログイン通知やログインの履歴、ログインしている機器の一覧に知らないものがあったり、あるいはSNSで自分が知らない投稿やアプリ連携などがあります。

銀行口座関連も、ログイン通知があればそれを受け察知し、通帳や取引履歴を見てチェック。クレジットカードはたとえ少額の送金であっても検証しましょう。

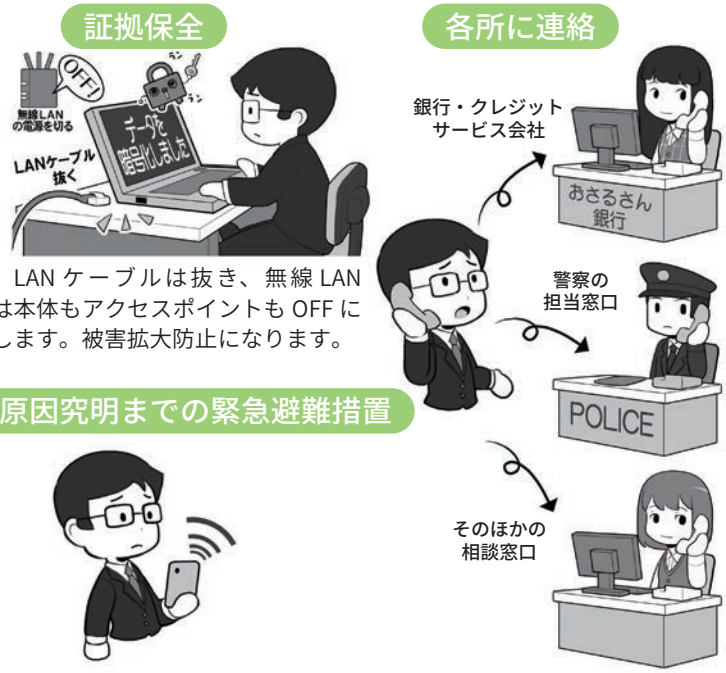
そして、マシンが乗っ取られている場合などは、動作が普段より遅かったり重かったりすることがあります。

もしマルウェアの感染の疑いや、アカウント乗っ取り、情報の流出や不正送金など、実害が判明した

セキュリティソフトが検知しなくても、兆候に敏感になれ



実被害が出ているときは証拠を保全して通報



LANケーブルは抜き、無線LANは本体もアクセスポイントもOFFにします。被害拡大防止になります。

原因究明までの緊急避難措置

感染したマシンで、メールでの連絡や仕事のやりとりは×。感染経路やマルウェアの種類などが判明するまで、同一LAN内、同種の機器の利用も避け、別の種類の機器、別の種類の回線を使います。家のパソコンが感染したら、スマホなどの通信回線を使用するなどの暫定的な回避策を行いましょう。

ら、とりあえずは有線でも無線でもネットにつながる回線を切断して本体の電源はそのままにして、証拠保全を図りましょう。通信を切断するのは拡散防止のためと外部の攻撃者との通信を絶つためで、本体の電源を切らない理由はパソコンなどのメモリ上の証拠を消してしまわないためです。

その後、必要に応じて各種サービスに取引を一旦止めてもらう連絡をし、必要に応じて相談窓口などに連絡して対処方法を相談しましょう。実害があれば警察の担当部署に被害届を出しましょう。

問題の解明やマルウェアの駆除が終わるまでは、連絡や仕事のやりとりは、感染したと思われる機器とは別種の機器を用いて行いましょう。同種の機種は同じLANに接続していたことで、感染し攻撃を受けている可能性が否定できないからです。

マルウェアが発見されただけで実害が出ていない場合、セキュリティソフトなどで駆除できる場合は駆除します。駆除できない場合は機器を初期化してバックアップから復元し、再びネットに接続して使用し始める前に、まずは感染や乗っ取りの原因と思われるものをクリアにしましょう。

システムやセキュリティソフトは最新の状態にし、不審なメールや添付ファイルなどが原因だったならばメールを削除、セキュリティホールになるサポート期限切れの古い機器は買い換え、ソフトやアプリはアンインストールし、アプリやサービス連携の棚卸(たなおろし)をして、知らないものを解除しましょう。

なお、どこかのウェブサービスからパスワードなどが流出した結果、アカウントを乗っ取られてパスワードまで変えられた場合は、自分で再設定はできないので、サービス側に連絡してアカウントを取り戻す処理をしてもらいましょう。

そして、こういったとき、なんだかんだで一番頼りになるのが、ITに詳しい友だちだったりします。あなたが困っているときにその友だちが復旧を手伝ってくれたとしたら、いつかはあなたが「ITに詳しい友だち」になって、誰かを助ける番になってください。

一人、また一人と、こういったセキュリティに詳しい人が増え、みんなでサイバー攻撃に立ち向かう姿勢が広まることは、きっとネットの安全を守る力になります。

実被害が出ていない場合

マルウェアの駆除

セキュリティソフトなどを最新にしてフルスキャンをかけて駆除します。

バックアップから復元

セキュリティソフトで対処できない場合は、本体を初期化してバックアップから復元します。

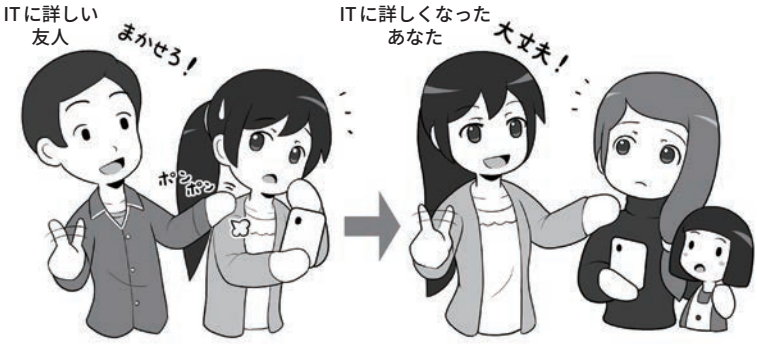
システムチェックする

古いソフト、サポート終了しているソフトおよびアプリは削除します。

サービスやアプリ連携の棚卸(たなおろし)

SNSのサービス連携機能は見直しをします。

そんなとき頼りになるのは……



ITに詳しい友人に対処を手伝ってもらうとともに、一緒に勉強しましょう。その相手が動いてくれる時間には、労力分のお礼をすること忘れずに。

そして、将来同様なケースがおきたら、あなたが困っている人に「ITに詳しい友だち」として手を差しのべて、力になってあげてください。

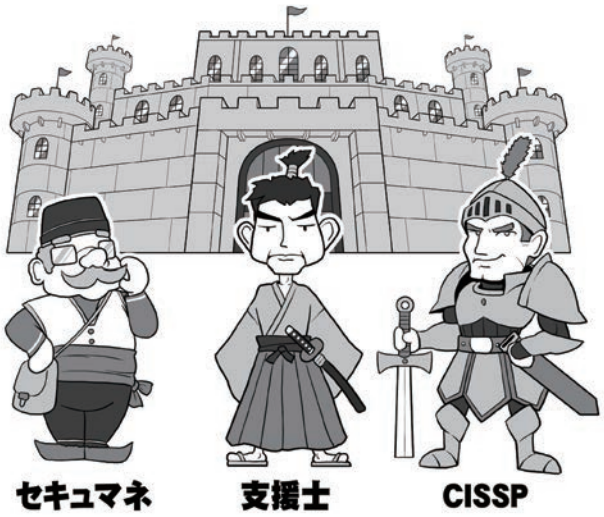
コラム：セキュリティの資格取得を目指そう

セキュリティについて深く知りたい、もっと詳しく学びたいと考えているのであれば、オススメしたいのが資格の取得を目指した勉強です。すでにセキュリティ関連の資格は数多く存在していて、自分自身のレベルや目的に合わせて選択できる環境が整っているほか、資格取得のための勉強を進めることで、体系立てて知識を獲得できるメリットがあります。

そうしたセキュリティ関連の資格として、比較的取り組みやすいものの1つに「情報セキュリティマネジメント試験」があります。これは、脅威から継続的に組織を守るための基本的なスキルを認定する試験であり、業務で個人情報を取り扱ったり、情報管理を担当したりするすべての人を対象としています。情報セキュリティについて、基礎知識からバランスよく学習したいと考えているのであれば、まずはここからチャレンジするのも1つの方法です。

さらに、高度な試験としては、「情報処理安全確保支援士」やグローバルで普及している「CISSP」(Certified Information Systems Security Professional)などがあります。情報処理安全確保支援士はサイバーセキュリティに関する実践的な知識や技能を有する専門人材の育成や確保を目的とした国家資格制度であり、情報セキュリティに関する高度な知識と技能を持つことを証明することができます。一方、CISSP は(ISC)^2(International Information Systems Security Certification Consortium)が認定を行う、国際的な情報セキュリティのプロフェッショナル認証資格です。これらの資格取得に向けた勉強を積み重ねれば、自身のスキルアップにもつながるでしょう。

数多くあるセキュリティ資格



現在、セキュリティに関する資格試験は数多くあり、自分のレベルや目的に合わせて取得することが可能です。情報セキュリティに特化した試験にチャレンジする前に、IT に関する全般的な知識が問われる「IT パスポート試験」を受けてみてもよいでしょう。そして、支援士の「士」は騎士や武士の「士」。現代の騎士や武士としてセキュリティを守りましょう。

セキュリティを網羅的に学ぶことができる

資格取得を目指して勉強する大きなメリットは、その領域に関する知識を段階的かつ網羅的に学べることにあります。また、自分の知識レベルを判断する上でも、こうした試験は大いに役立ちます。

第5章

SNSやインターネット関連の犯罪やトラブルから、自分や家族を守ろう。災害に備えよう

SNSやインターネットを使う上で、どんなふうにしたら自分や家族を守れるの？
具体的にどんなことが起こり、そのときどのようにしたら自分や家族を守ることができるのか、
一緒に考えてみましょう。
海外での利用の注意点や、災害時に情報を生かしてどうやって身を守るかを知りましょう。

1 SNSやネットとのつきあい方、守り方

1 SNSやネットの楽しみと気をつけること

私たちは、インターネットの普及により、「距離とその移動に必要だった時間が消えた世界」を手に入れることができました。

昔は、遠い国の人と連絡を取り合うには、手紙を書いて何週間も返事を待ったり、電話をかけるにしても料金が高く気軽にかけられなかったり、あるいは顔を見るために旅行するにしても、大変な手間とお金がかかったものです。

しかし今では、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、映像つ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。

そして、IT技術の進歩は言葉の壁すらも崩しつつあります。まるで世界が一つになったような時代が訪れ、人の意識そのものが変わっていくかもしれません。

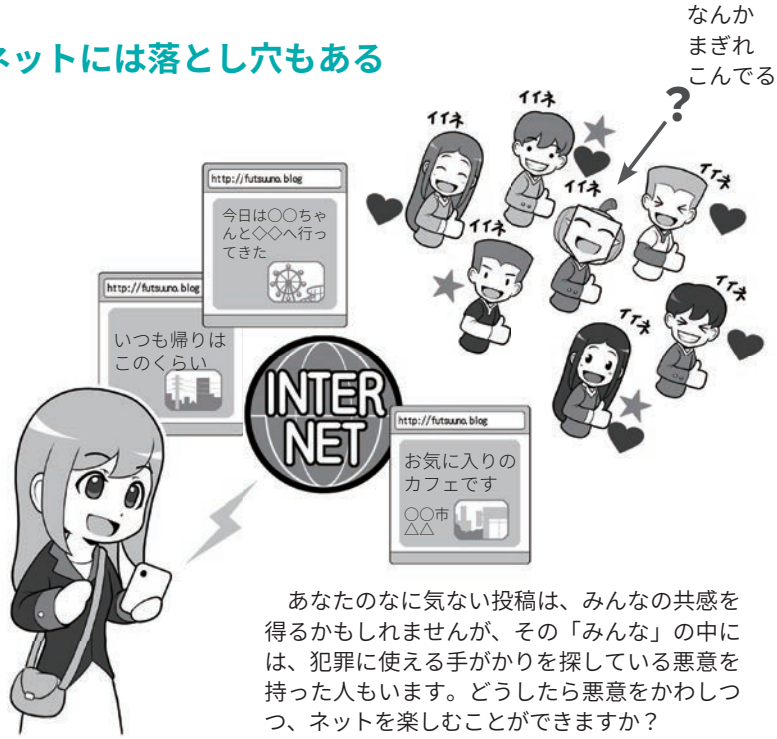
一方、あなたが世界中の人にメッセージを発信するとき、それを受け取る人々の中には悪意を持った人がいることも忘れてはなりません。ネットを使ったコミュニケーションは人と人の意識のつながり合いを容易にしますが、同時に自分の意識の壁の中に、そういった悪意をもった人間がするりと入ってきやすくなるのです。

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、新しいつきあい方」を作り上げなければならないでしょう。悪意のあるものを鋭く見分けて、善意のコミュニケーションの世界を作っていくことができるように。

ネットやSNSによるコミュニケーション

ネットやSNSで、距離を超えて世界とつながることができます。そして、時間を越えて様々なことを知ることもできるのです。

ネットには落とし穴もある



あなたのなに気ない投稿は、みんなの共感を得るかもしれませんが、その「みんな」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、ネットを楽しむことができますか？

2 SNSやネットの怖さ、こんなことが実際に起こっている

では、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の人でした。「○○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。こんな風に誘拐や略取が行われます。

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。

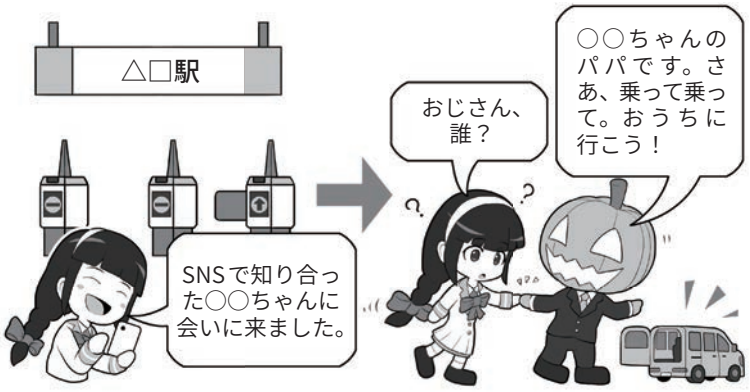
闇サイトなどを興味本位に覗いたりしていると、犯罪勧誘といって、顔も知らない人があなたを犯罪に誘ってくることもあります。

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。

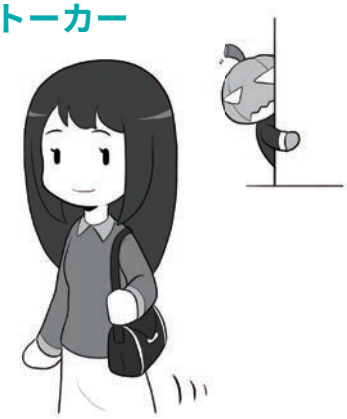
交際している相手が、「誰にも渡さないから」とあなたの裸の写真を要求してきて、信頼して渡したら、別れた後にその画像がネットに流出してしまうかも。それは、「リベンジポルノ」といって、相手が嫌がらせのために、写真をネットに投稿する行為ですが、その意図がなくても、相手のスマホがマルウェアに感染して流出してしまうかもしれません。その写真は、消えない「デジタルタトゥー」(デジタルの入れ墨)として、以降あなたの人生に、ずっと影を落とし続けることになるかもしれません。

このほかにも、SNSやネットでは、様々なトラブルが発生することがあります。トラブルのことをよく知って、決して巻き込まれないようにしましょう。

誘拐や略取



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。

3 SNSやネットとのつきあい方の基本

自分からネットの怪しげな場所に近づかないなら、あとは日常的に注意しなければならないのは、システムなどを最新の状態に保ちサイバー攻撃を受けないようにすることと、SNSやネットで悪意がある人に個人情報や画像が渡り、あなた自身が狙われたり、攻撃の対象にならないよう、投稿する内容には気をつけることです。

例えば、SNSを利用する場合、個人情報はサービスの規約などで必須のもの以上は記入しないようにしましょう。その上で、投稿の公開範囲の設定は、友だち限定にしましょう。そのほか個人情報を守る仕組みが提供されている場合は、それらを有効活用しましょう。

実際に会ったことがない人が、突然お友だちになりたいといってきても、即座にOKせず家族などに相談しましょう。誰かの友だちなら、実際に会ったときの印象や、どういった人かを教えてもらい検討の材料にしましょう。また、その人の過去の発言などを良く見て、二面性などを含め判断しましょう。

そして、一度も会ったことがないのに、本名や連絡先をたずねたり、いきなり実際に会おうなどと誘ってきたりしたときは、基本的にお断りしましょう。文化活動や物の売買など、なんらかのきちんとした理由で会う必要があるときは、大人や保護者同伴で行き、その際でも本名や住所などは極力教えないようにしましょう。

SNSやネットへ投稿をする場合は、普段の立ち回り先や生活のパターンの情報などは避けるようにしましょう。些細なことですが、一枚の写真に写っている背景だけで、自宅を特定される場合もあるので注意しましょう。

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。

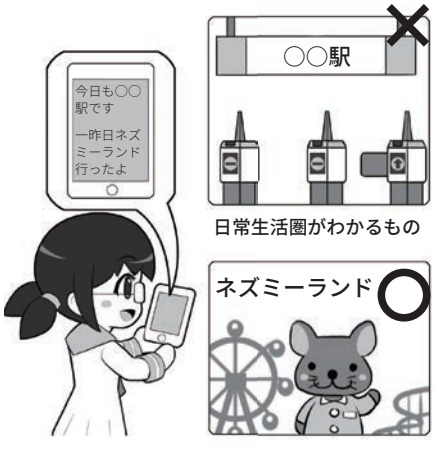
会ったことがない人とむやみに友だちにならない

会ったことない人が友だちになろうと近づいてくるときは、その中に悪意をもったものがいることを知りましょう。基本的には友だちにならず、必要ならよく吟味したり、相手について調べたりしてから判断しましょう。

現実世界で会おうとする人を警戒する。出会い系に近づかない

実際に会ったことがない人は、プロフィールの年齢や性別が本当なのかわかりませんし、これを偽って近づいてきた人と会い、被害に遭った例もあります。また、よく事件が起こる出会い系サイトなどには、絶対に近づかないようにしましょう。

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、デジカメで「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 存在するデータは流出することがある。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じゃ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、様々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ういった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、信頼できる友人に秘密の写真をシェアしたあと、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。

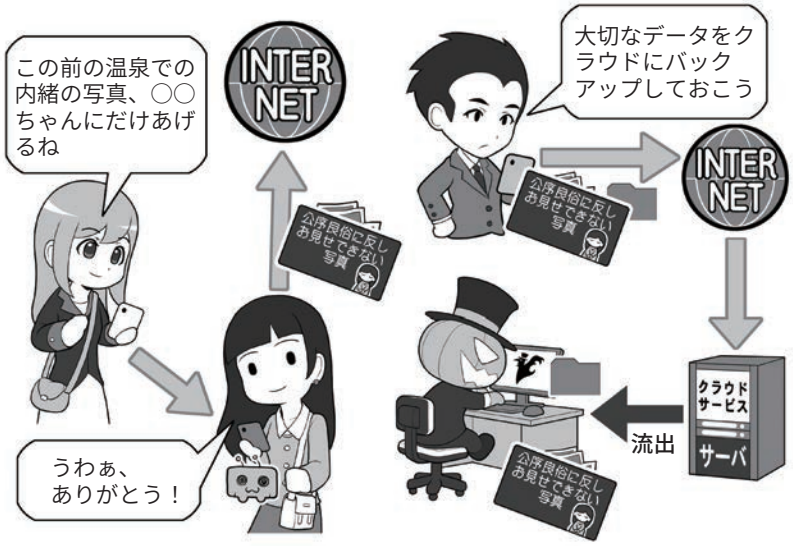
相手が、自分と同じレベルのセキュリティ知識を持ち、実践しているとは限らないですし、また、それを強要もできません。

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した場合、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、少なくとも2カ所から流出する可能性が存在するようになります。事実、クラウドからセレブの写真が流出する事件も発生しています。

問題がある画像は、なにかということに関する意識の差でも問題は起こります。例えば、若気の至りで公序良俗に反することをして、これを、その場ののりでSNSに投稿したとします。その写真が大炎上を起こしたとしたら、もしかしたらあなたの人生のあらゆる局面での歩みを妨げるものとなってしまうかもしれません。

流出したら問題になることは、しない、させない、(助長する意味ではなく)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。

コラム：子どもにスマホを持たせるとき、「スマホ契約書」という提案

子どもがスマホを使いたいと要望してきたので、人生の課題を設定してそれをクリアしたら契約書付きで提供するようにした、というニュースがありました。

契約書というと物々しいですが、スマホ利用のルールを口頭ではなくきちんと明文化し、それをお互いが確認し合うことで、利用する子どもも「それをないがしろにしてはいけないことだ」ということを強く認識するというわけです。厳しいという意見もあると同時に、一歩階段を上り大人として扱われたことを喜ぶ子ども自身の意見もあるようです。

契約書の内容は、「家族からの連絡にきちんと返信すること」や、「朝受け取って夜親に返すこと」、「実際に会ったことがない人はアプリで友だちにならないこと」などがあります。

また、SNSを使ったトラブルになりそうな「面と向かっていわないことはSNSでもいわないこと」とか、海外の例では、「恥ずかしい写真を交換したいといわれてもやってはいけない」といった項目もありました。これは、SNS上での炎上の芽を摘んだり、未成年が同年代になりすました人間に裸の写真を要求された上で脅されたり、あるいは同級生同士で交換したものが流出したりする、セクスティングなどを未然に防ぐ意味で重要です。

それと同時に、インターネット上の情報は必ずしも正しいとはいえず、フェイクニュースやデマが存在すること、情報は裏を取って初めて本当の情報となること、ときにスマホを置いて現実の世界へと飛び出し、自然や様々な動物に興味を持つことなどを書いた項目もありました。

些細なことですが、夜になったら親に返し、朝になったら渡してもらうといった項目は、友だちとメッセージをやり取りして眠れない、勝手に眠ると仲間はずれにされるといったことにして、「うちは夜になると親に返さないといけないからごめんね」とスパッといえ、一つのいい対処方法でもあるといえるでしょう。

「スマホ　契約書」で検索して、実際の契約書や記事を見てください。スマホのルール作りの一助になるかもしれません。

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、ルールを時々見返したり、いったいわないにならない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と自律を促しましょう。

コラム：GPS、位置情報、ジオタグの管理

私たちが普段なにげなく使っているスマホは、実は相当に高機能で、10数年前ならばすべて別々の機器だったものが、まとまって小さなボディに収まっています。

例えば、電話、音楽プレイヤー、デジカメ、ビデオカメラ、そして、GPSレシーバーなど。

とくに昔は、GPS衛星からの電波をキャッチして、緯度経度で構成される位置情報を測るには、大きな専用のレシーバーが必要でした。今はスマホの地図アプリを開いて「現在地」と押せば、即座に自分がいる場所を示してくれます。

しかし、便利になった代わりに、油断すると意図せずこういった情報を公開してしまっていることもあります。

例えば、スマホで写真を撮影するときに位置情報を記録するようにしておくと、撮影場所の情報が「ジオタグ」という形で写真に保存されます。

ジオタグが記録されている写真を、写真アプリなどで見返すと、地図上の撮影したポイントに写真を配置して見ることができ、時系列順に並んだたくさんの写真からわざわざ探さなくても、思い出の場所で撮った写真を即座に見つけることができます。

これは便利ですが、写真にジオタグをつけたままSNSに投稿すると、SNSによっては撮影場所が公開されてしまうことがあります。その写真が自宅で撮影したものだったりすると、世界中に自宅の場所が公開されてしまうのです。

また、位置情報はSNSの投稿時に位置情報を公開する設定にしておくと、文字だけの投稿をしたつもりでも、写真を撮った場所まで文字で公開されてしまいます。

生活圏の位置情報を公開してしまうトラブルは、GPSにまつわるものだけではなく、普段立ち寄る店の名前を投稿したり、周りの風景が映り込んだ写真を投稿したりするだけで、いともたやすく「撮影場所が特定される」ことがあります。

そして、これらの「位置情報」もしくは「位置情報に相当する情報」は、ストーカーにとっては絶好の手がかりになります。

ネットは知らない人と「距離とその移動に必要な時間」を超えて知り合える場所ですが、トラブルが発生すれば、それは距離を越えて現実世界の我が身に即座に襲いかかってきます。

位置情報を含む個人情報の管理は、しっかり行いましょう。

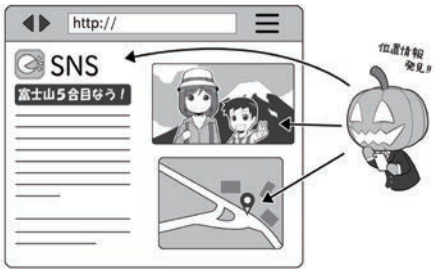
写真には位置情報が含まれることも

スマホによっては購入時の設定で、写真に位置情報を記録するようになっている場合もあります。必要なければ機能をOFFにしましょう。

位置情報は思い出を見返すのに便利

画像アプリによっては地図上に写真がドロップされ、思い出の場所を拡大すると、そこで撮影した写真を見ることができます。写真を一から探さなくていいので便利です。

位置情報はストーカーの手がかりになる



写真に付加された位置情報、投稿時の位置情報だけでなく、場所の名前や、場所が特定できる写真からはあなたの居場所が分かります。ストーカーにとっては絶好の手がかりになるので、投稿前後に必ずチェックしましょう。

コラム：SNSやSNSのグループを使ったいじめに備える（いじめ経験者からのアドバイス）

いじめは公共の目がある場よりも、人々の目が届きにくい比較的閉鎖された空間で起こりやすく、学校はときにその条件に当てはまります。

ネットが普及する以前であれば、コミュニケーションは言葉や暴力など、実際の行動となって現れていたので、それでもまだ目につく可能性がありました。

しかし、ネットの普及によって、そのいじめの一部がSNS上で匿名で、あるいはSNSの外から見えないグループ内で行われるようになると、いじめの実状を目にする方法が少なくなりました。

また、昔であれば学校から離れた別のコミュニティをもつことで、自分が自分らしくいられる場所を確保し、バランスを保つことができました。今はスマホを始終持ち歩くので、学校から離れ別のコミュニティに行き、スイッチを切り替えることも難しくなります。スマホを持っているとそれを通じて四六時中、学校のコミュニティにつながり続け、その中でのいじめは生活すべてにおいて、その影を落とし続けてしまうからです。

物理的ないじめはもちろん、SNSやネットを使ったいじめを受けているときは親に相談し、画面キャプチャーやコピー、録音などで証拠を集め、それを添えて恐れずに、専門の窓口に相談しましょう。

また、学校以外の自分の居場所やコミュニティをもつことで、「学校の中の自分ではない自分」という時間をもち、その中でのアイデンティティを確立しましょう。

いじめに遭うのは辛いことですが、自分が否定されない別の空間をもつことができれば、心を休める場所と時間をもてます。その場所にいるときは、いっそスマホの電源をOFFにして、目の前に集中して過ごしてみましょう。

（空手道場で生き延びられたNISCのおじさんより）

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

ネットも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。

証拠を集めて相談しよう

いじめの告発をするときは、きちんと証拠がある方がトラブルの説明がしやすくなります。

自分らしくいられる別の場所をもとう

ネットに関係がない場所を探して、学校以外に自分の居場所を作りましょう。

コラム：モラルを逸脱すると炎上を生む

ネットのニュースなどを見ていると、「炎上」という言葉を良く目にします。

炎上とは、特定の人物がSNSなどに投稿した内容が不適切であるとして拡散され、多くの人から集中的に非難を受けることを指します。

例えば、特定のお店に関していいがかりのような投稿や嘘の書き込みをしたり、飲食店などで働いている人が芸能人のプライベートでの来店を投稿したり、引っ越し業者が業務上知り得た情報で引っ越した女性にアプローチをしたり、あるいは未成年が飲酒ありの大宴会をした投稿をするなどなど。

多くの場合は、世間一般の「モラル」に照らし合わせて、おかしいと思われるものに対して炎上は発生します。

問題は、その炎上の結果、炎上させた本人が非難されるだけでなく、嫌がらせをされたお店が閉店してしまったり、雇っていた会社が謝罪したりと、周辺に多大なる影響を及ぼしたり、また、本人にも損害賠償責任が発生したり、名誉棄損で訴えられたり、内定が取り消しになったりということが起こる点です。

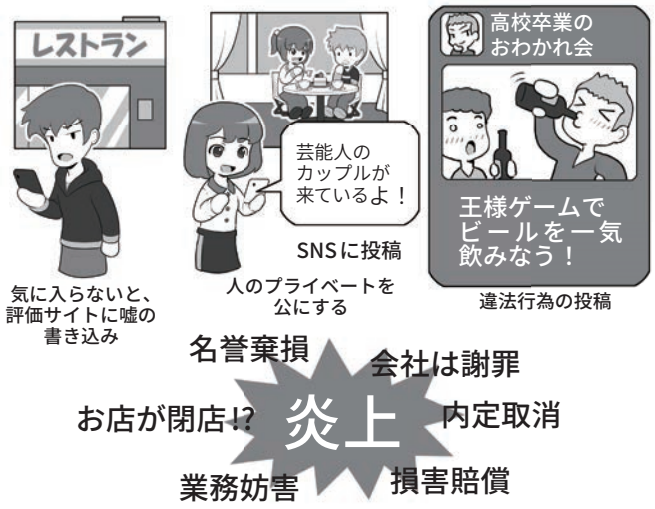
この「炎上」をおこさないためには、投稿する人が「世間とのモラルと自分の意識のギャップを埋める」か、「投稿をしないか」しか解決策はありません。

ネットで炎上を見たら、その顛末を見て、どのような書き込みがどのような経緯で炎上を生み、どのような結果を招くか、どこに意識のずれがあったのか調べてみましょう。

また、ネットの掲示板などを利用して、自分の投稿を多人数のふりをしてはやす「自作自演」や、焚きつけるアオリ行為、誰かのふりをするなりすましの書き込みなども、状況によっては犯罪や名誉棄損の対象となる場合があります。

「こんなことになると思わなかった」という言い訳は昔からよく聞きますが、そういったところでもとには戻りません。現実世界とネットでのコミュニケーションの差、SNSの情報拡散の特徴などを、興味を持って調べて、騒がしくない穏やかな生活を送って下さい。

モラルを逸脱することが炎上を生む



自作自演やアオリ行為、嘘の書き込み

コラム：屋外でのゲームを安全に楽しむ。ながらスマホは×！

ここ数年のスマホのパワーアップにより、昔ならば専用ゲーム機が必要だった複雑なゲームでも、スマホで軽く動かせるようになりました。

それに伴い、従来から存在していた「位置情報ゲーム」と呼ばれるジャンルに、リアルタイムの地図情報や動く3Dキャラクター、カメラ映像にAR（拡張現実）を重ねたものも登場してきました。

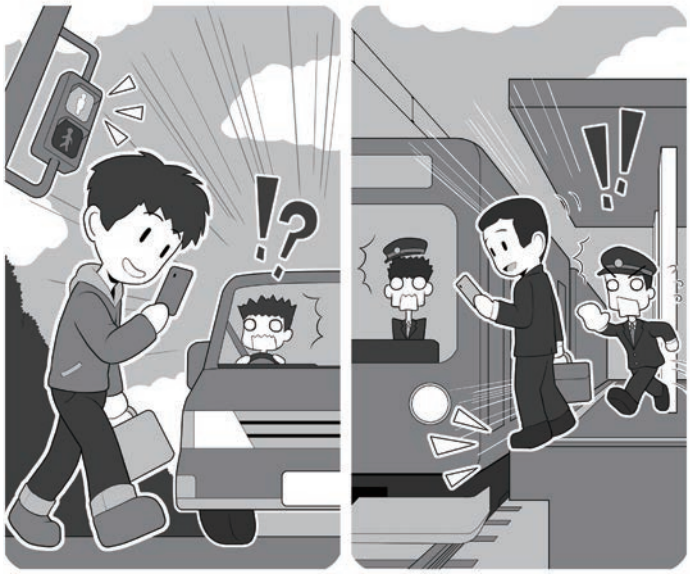
スマホを持って現実世界に飛び出して、モンスターを捕獲したり、様々な場所に行ってご当地でアニメキャラクターと写真を撮ったり、あるいは全国の駅を巡るといったゲームが登場しています。

そういったゲームでは、みんなが安全に楽しく遊び、幸せになるために守らなければならないルールがあります。

まず、屋外でゲームをするとき「ながらスマホ」をするのは危険です。場所やものを探すゲームでは、ついついスマホの画面を見ながら歩いてしまいますが、わずかの時間スマホを見ているだけで誰かにぶつかったり、線路に落ちそうになったり、車にはねられそうになったりすることはありえます。また、わざとぶつかってくる「スマホ当たり屋」によって怪我をしたり、難癖をつけられ金銭を要求されるということも起こっています。

移動中は、画面を見ずに遊べる方法が提供されているこ

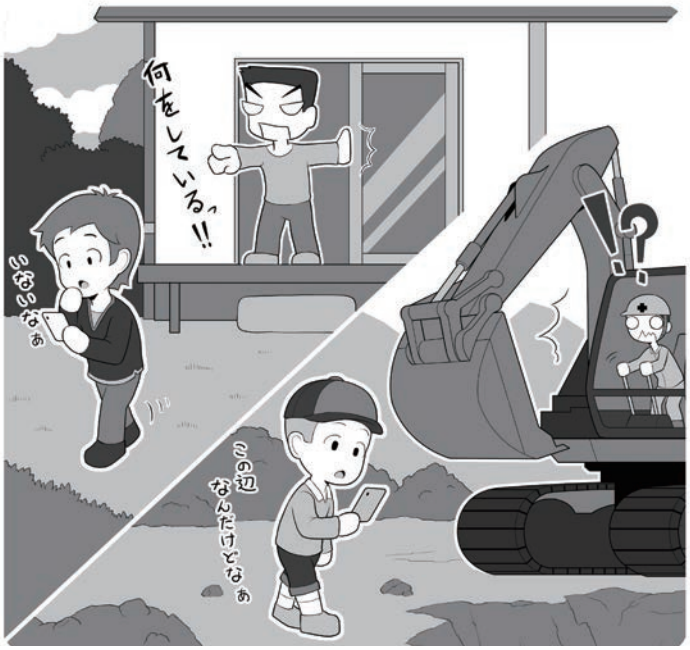
歩きスマホは自分も周りの人も危険



自分は大丈夫と思っていても、歩きスマホは大変危険な行為です。歩いているうちに車道に出て事故に遭ったり、駅のホームから転落することもあります。

また、歩きスマホをしている人を避けようとして、自転車や車に乗っている人が事故を起こしてしまう可能性もあります。歩きスマホはやめましょう。

私有地や危険な場所には入らない



スマホを使ったゲームをしていると、それに集中するばかりに、危険な場所に立ち入ったり、他人の家の敷地の中に入ってしまうこともあります。

危険な場所での事故や、海外では発砲トラブルも起きています。ゲームはゲーム、命をかけるものではなく、楽しむものです。モラルを持って楽しみましょう。

ともあるので、よく調べてみましょう。

また、自転車を運転しながらの操作や、当然のことながら自動車を運転中のスマホ操作は論外です。周りを見ないで運転する乗り物は、周りからすると命を奪いかねない大変な脅威ですし、条例や法律に違反する場合もあります。

また、ゲームに熱中していて誰かの家の敷地や私有地に入り込んでしまうと、これは「不法侵入」に当たります。

ただ、そういった不法行為の問題としてではなく、単純に「自分の家の庭に、知らない人が入ってきたらびっくりするよね」というように、相手の立場に立って考えましょう。そういった考え方ができるようになれば、ほかのシチュエーションでも生かせるはずです。

自分の街に、たくさん人が来て賑わうのはウェルカムですが、迷惑行為があると「もう来なくてよい」となり、誰もハッピーになりません。

また、危険な場所に入り込んでケガをすれば、救助する人員や救急車、場合によってはヘリコプターが必要になります。常識的に考えて、その場所が危険であると思われるなら、例えゲームのプレイエリアが設定されていても、近づかないようにしましょう。

こういったモラルや安全を守りながら楽しめるなら、現実世界でプレイするゲームは様々な場所にたくさんの人を呼び、ときには災害に遭った地域の復興支援にも役立つことがあります。

それが成功するかどうかは、みなさんに心持ちひとつにかかっていますよ。

運転中のスマホはダメ。車は凶器になります

運転中のながらスマホは違反です。運転している車はルールを守って使わないと一瞬で人の命を奪う凶器になるということを考えましょう。

位置ゲームを活用すれば、いいこともあるよ

スマホを使った位置ゲームは、上手く使えば地域活性化や復興支援に使える素晴らしいアイテムです。安全に使い、安全に楽しみ、そして、ゲームとともに様々な場所を巡って、旅を楽しみましょう。

2 サイバー関連でやってはいけないこと

1 アニメ・マンガ・音楽の違法なシェア。パクリなどの著作権侵害

インターネットは、基本的に様々なものを共有する場です。しかし、著作権者の許可を得ずに、ネットにアップロードされた、映画、アニメ、テレビ番組、音楽、マンガなどの作品を、そうと知ってダウンロードするのは違法行為です。

また、同様に上記のような作品を、著作権者の許可を得ずにインターネットサーバにアップロードして配信する行為も違法です。

違法アップロード、ダウンロードは作品が生み出される環境を破壊し、結果として作品が生まれなくなります。許可を得て公開されているものを利用しましょう。

こういった違法行為以外にも、ネットでは「パクリ」といわれるカジュアルな著作権侵害がよく行われています。

例えば、他人がSNSに投稿した写真や文章を、自分のもののふりをして勝手に投稿するのは著作権侵害ですし、SNSによっては利用規約違反になりアカウントを停止される場合もあります。

また、他人がウェブで発表した小説や写真などの、一部もしくは全部を自分のもののように偽って公開することも著作権侵害です。

パクリで一瞬だけ注目を集めても、いずれ身元が特定されるなどして「パクった人だ」とネットに記録されてしまうでしょう。

ネットには距離が存在しない分、今まで会うことができなかった人に作品を届られる世界です。誰かの作品ではなく自ら作品を生み出して世界に届けましょう。

違法アップロード、ダウンロードは刑罰の対象にも……

＊1：有料の作品が違法にアップロードされているものと知っていた場合

他人の投稿や作品を盗む「パクリ」

2 ゲームの不正行為。恋人や家族でもプライバシーは守る

ゲームの不正コピーやチート行為もやってはいけないことです。

それ自身、規約違反で場合によっては犯罪として摘発されますし、「自分ひとりぐらいやっていても大丈夫」という人たちが増えていけば、楽しんでいるゲームそのものが生まれてくる環境を破壊してしまうことになります。

ゲームを作る人はゲームを売ることで利益を上げ、生活をし、また、新しいゲームを世の中に生み出してくれます。この利益の循環があるからこそ、ゲームを遊ぶ側は楽しい時間を過ごせるのです。

しかし、誰かが不正行為でこの「利益の循環」を回らなくしてしまうと、やがてゲームを作る人々は生活できなくなり、結果としてゲームがこの世に生み出されなくなってしまいます。

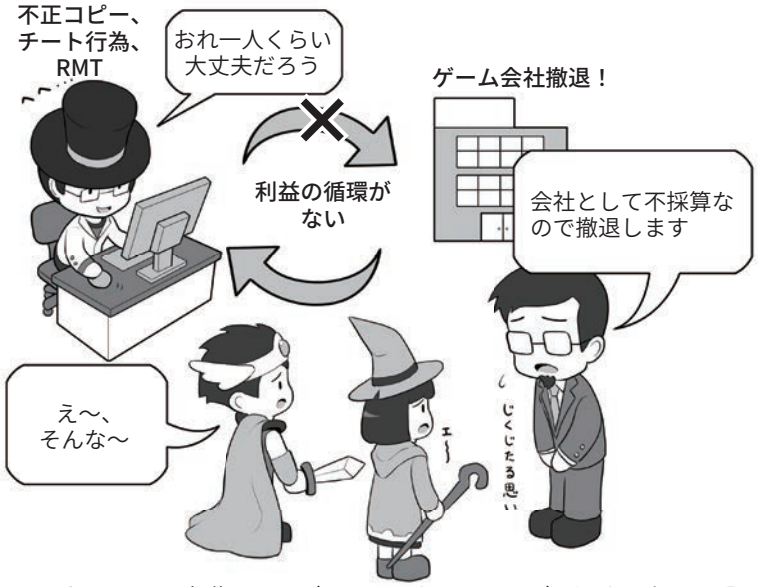
楽しみのある世界がいいですか？ない世界がいいですか？

私たちは信頼関係をもって楽しい世界を盛り上げていく人たちが大好きです。

信頼関係は普段の生活でも大切です。例えば、プライバシー。あなたが席を立っている間に勝手にスマホの中身を見られてしまったり、あるいは親があなたの部屋に勝手に入り込んで、パソコンに保存している日記を見ていたらどうでしょう。特に、「信頼している」人の行為は人を深く傷付けます。

また、「信頼関係」の名のもとに自分のプライバシーを守ってほしかったら、自分も誰かにとって、信頼を裏切らない人物にならなければいけません。

ゲームの不正行為は犯罪になることも…



不正コピー、チート行為、RMT（リアルマネートレード）など、ゲームの販売や運営を妨げたりする行為は、場合によっては犯罪として摘発されますが、それよりも積もり積もってゲームを生み出す会社やシステムの崩壊を引き起こしてしまうことが問題です。

その結果、みんなが楽しめる世界が奪われてしまうのです。利用者を信頼している制作者の人たちを裏切ってはいけません。

恋人や家族の間でも信頼関係は大事、でしょ

例えば、あなたの恋人や親がスマホの中を勝手に見たり、内緒でパソコンを開いて勝手に日記を見ていたりしたら、信頼関係はなくなってギスギスしてしまうでしょう。それにスマホやパソコンに対する安心感を失ってしまうかもしれません。

自分が「信頼」を守ってほしいと考えるなら、相手に対しても守らないとフェアではありません。信頼を守って笑顔の関係を作りましょう。

というようなことを真顔でいちいちいわれるよりも、お互いのことを思い合って、信頼し合い、笑顔で生活できる社会になった方がいいですよね。「いい笑顔」を守りましょう。

3 クラッキングはクールじゃない！

インターネット上には、「ダークウェブ」という、通常は見ることがないネットの陰の部分が確かにあります。そこには、アングラなありとあらゆるものを売るマーケットが存在し、悪意のハッカーがクラッキング用のツールを売っていたり、DDoS攻撃のためのゾンビ化した機器群を時間あたりいくらで貸し出したりもしています。

近年、若い子どもたちがここに足を踏み入れ「インターネットは匿名だからばれないだろう」とツールを購入したり入手したりして、ランサムウェアによるサイバー攻撃や不正送金などを行い逮捕された例もあります。

では、果たしてそれは、本当にばれないのでしょうか。

インターネットは当初、悪意が存在することを想定していない空間でした。しかし、そこに悪意が芽生え、犯罪に利用されるようになり、各国の捜査機関も日々こういった犯罪に対応する技術力を向上させています。

事実、「そういう事件があった」と報道されるのは、匿名でばれないと思った者たちを、捜査機関が地道な解析などで追い詰め、犯人を特定しているからです。

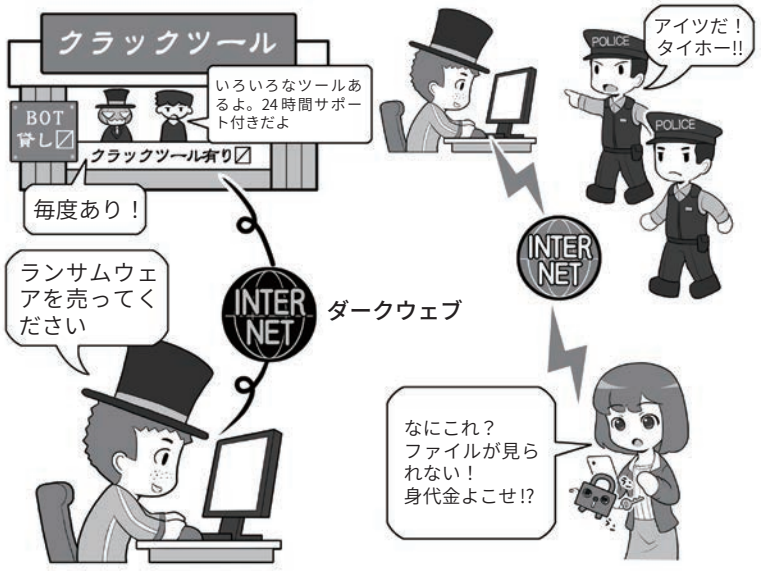
「有名になりたかった」「腕試しをしたかった」「小遣い稼ぎで」

そういう言い訳をしつつクラッキングを行っても、しょせんは自己満足であって、その行為は誰もハッピーにしません。有名になったところで、その悪名がネットに刻まれるだけで誰も尊敬はしてくれません。実名が流出して、その後の人生にずっと影響しつづけることだってあるのです。

それよりも、腕と技術力で多くの人々をハッピーにし、ネットの偉人として名前を刻む方が「かっこいい」でしょう？

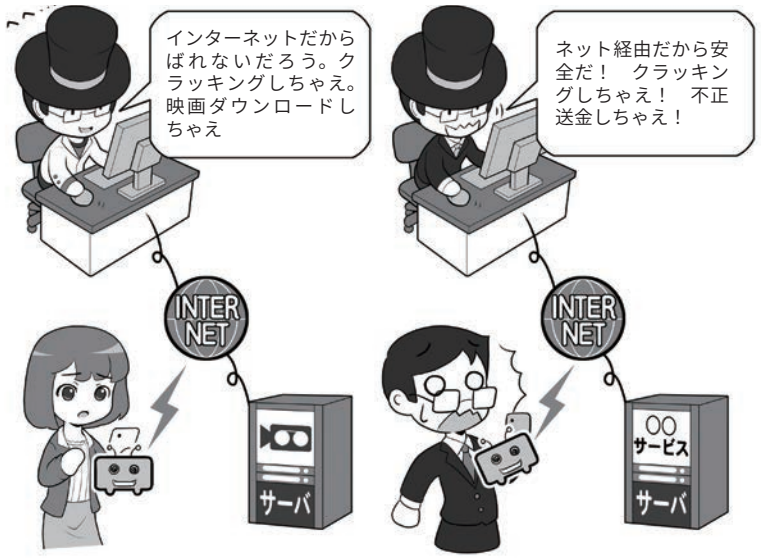
ネットでは、現実よりも名前が長く残るかもしれませんよ。

クラッキングツールに手を出さない



現実世界でもネットでも、広く知られている「安全でない場所」や「怪しい場所」は、当然のことながら捜査する側もよく調べ、必要ならば対策を講じています。「匿名性が高い」はずなのに「捕まったこと」が記事になるということは、なにを意味するでしょう？ネットでも危険場所には近づかないようにしましょう。

インターネットだからばれないと思うのは……



本人は軽い気持ちで始めているつもりでも、クラッキングは様々な法律や利用規約に違反します。そして、見つからないと思っていても、現実世界に生きる私たちは、現実世界に生きている痕跡を完璧に消すことはできません。

コラム：法律に違反することをしてはいけません。気軽に考えてはダメ

サイバー犯罪というと、それなりの年齢の悪意のハッカーを想像するかもしれませんが、非常に幼い子ども達が行い児童相談所に通告されたり、未成年が書類送検されたりしている事件もあります。

見てはいけないウェブサイト、危険なサイトをフィルタリングするだけでなく、コンピュータやスマホを使う際、どういうことをしてはいけないのか、きちんと家族で話し合っておく必要があります。下記の例などを参考に事例を調べて、共有してみてください。

他人のアカウントへの不正なログインや乗っとりをした場合

不正アクセス禁止法
不正アクセス行為の禁止

第三条、第十一条
→三年以下の懲役または
百万円以下の罰金

コンピュータウイルスの作成や保管をした場合

刑法
不正指令電磁的記録作成等

（作成、提供、供用）
第百六十八条のニ
→三年以下の懲役または
五十万円以下の罰金

（取得、保管）
第百六十八条の三
→二年以下の懲役または
三十万円以下の罰金

児童ポルノの所持・提供をした場合

児童買春、児童ポルノ禁止法
児童ポルノ所持、提供等

（所持）
第七条第一項
→一年以下の懲役または
百万円以下の罰金

（特定少数者への提供）
第七条第二項
→三年以下の懲役または
三百万円以下の罰金

● アカウント乗っ取り

2011年　奈良県の小学4年生の女子児童が、会員制の交流サイトでサービス上の通貨の提供を条件に、別の女子中学生のIDとパスワードを聞き出し、本人になりすましてログイン、その女子中学生のアカウントを乗っ取ったもの。小学生の女子児童は不正アクセス禁止法違反の容疑で補導され、児童相談所に通告された。

● ウイルス保管と提供

2017年12月、動画サイトなどに掲載されていた動画を参考にコンピュータウイルスを作成、これを保管、提供したなどの理由で、大阪に住む小学3年生の男子児童が不正指令電磁的記録提供などの非行内容で児童相談所に通告された。またこれをダウンロードした京都、山梨などに住む児童も不正指令電磁的記録取得の非行内容で児童相談所に通告された。児童は「友だちを驚かせたかった」などと述べた。

● 同級生の少女の裸の画像を拡散

2018年4月、同級生が高校生の少女に裸の画像や動画を撮影させ、これをSNSに投稿することを強要し、そののち拡散した。16歳から17歳の男女4人の児童は、児童買春・児童ポルノ禁止法違反（製造、提供など）の疑いで書類送検された。

コラム：成人年齢18歳引き下げに伴って注意が必要なこと

2018年6月に民法が改正され、約140年ぶりに成人年齢が20歳から18歳に変更されることとなりました。この改正により、2022年4月1日以降は、18歳になると成人になり、また、すでに18歳、19歳になっている人は、この日をもって成人となります。

さて、成人すると、なにが変わるのでしょう。すぐに思いつくのは、飲酒や喫煙、ギャンブルなどがありますが、これらは、成人年齢が変更されても20歳以上のままで変更はありません。最も大きな変化は、「親権者の親権に服さなくなる」ことです。

未成年者は、親権者の同意なく契約行為ができませんが、今回の改正で、18歳になれば成人になりますから、自らの意思で契約行為をすることができます。

例えば、携帯電話の購入では、回線の利用契約が必要ですが、保護者が契約した上で、利用者を未成年者としたり、保護者の同意のもと未成年者が契約したりすることになっています。これも施行後は、18歳以上ならば自身で契約できるようになります。また、青少年インターネット環境整備法で携帯電話会社に提供が義務付けられているフィルタリングも、その提供が契約事項に含まれているため、これまでは未成年者は親権者の同意がなければ自分の意思で解除をできませんでしたが、施行後は18歳ならばそれも可能になります。

ソーシャルゲーム、オンラインゲームでの課金やオンライン通販などでの購入も契約行為です。親権者の同意のない課金は、未成年者による契約を理由に取り消しを申し出ることが可能でしたが、施行後は18歳になれば成人ですので、未成年であることを理由に取り消しはできません。日頃から課金などをしている場合には、自身で課金額などを確認し、支払える範囲内に収めておくよう心掛けましょう。

さらに、高齢者だけでなく成人したばかりの若者をターゲットに、SNSなどで甘い言葉や人間関係を作って勧誘するような手口が国民生活センターからも報告されています。18歳成人化を控えて、従来よりもより低年齢層にターゲットが広がるおそれもありますので、日頃からこうした甘い言葉や見知らぬ人からの誘いには注意しておきましょう。

18歳成人化の対象者

対象者	成人になる日	成人年齢
2002年4月1日以前の生まれ	20歳の誕生日	20歳
2002年4月2日～2003年4月1日生まれ	2022年4月1日	19歳
2003年4月2日～2004年4月1日生まれ	2022年4月1日	18歳
2004年4月2日以降の生まれ	18歳の誕生日	18歳

変わるもの・変わらないもの

変わるもの	変わらないもの
・携帯電話の契約 ・ローンを組む ・クレジットカードをつくる ・賃貸契約を結ぶ ・10年有効のパスポート取得 ・結婚　など	・お酒を飲む ・タバコを吸う ・競馬、競輪、オートレース、競艇の投票券(馬券等)を買う ・大型・中型自動車運転免許の取得　など

コラム：デジタル遺産相続

近年、生活の中にIT機器やウェブサービスが深く入り込むにつれ、それぞれで必要となるIDとパスワードの数は増加する一方です。

また、例えば家族の中でITに詳しい人が一人だったり、あるいは互いになにを利用しているか話していなかったりした場合、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。

特に、問題になりやすいのは負の遺産で、FX(外国為替証拠金取引)で取引をしたまま亡くなった場合、取引が継続されていて、その後相場が大きく変動して、知らないうちに莫大な負債(不足)を抱え込んだという例もあります。

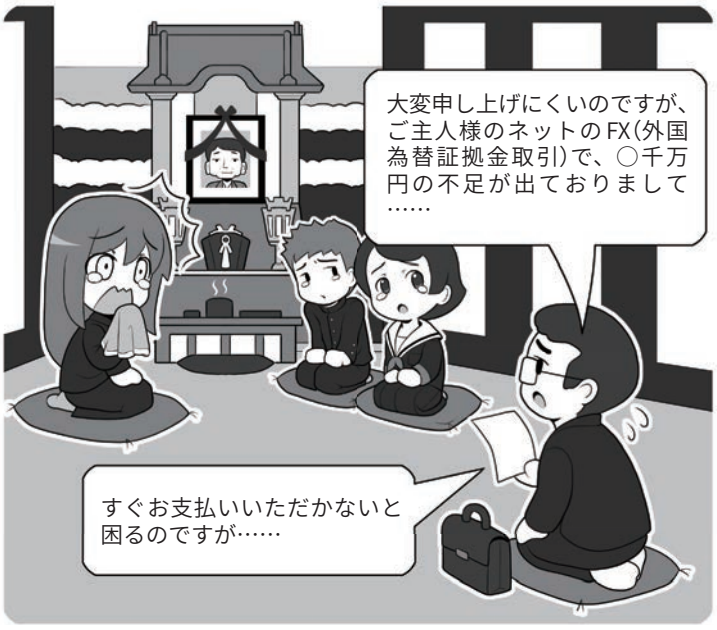
イラストのように、極端な話しになるかどうかはさておき、「立つ鳥跡を濁さず」にするためには、残された人が迷わないように、万が一のときに備えて管理情報のありかを残しておきましょう。

どういったサービスを利用していたかの一覧や、もし亡くなったらどのような処理をしたらいいか。IDやパスワードなどをパスワード帳に書き残すか、スマホのパスワード管理アプリを利用している場合は、その解除のためのPINコードなどを、ノートや遺言書に残すか、家族と共有しておきましょう。

SNSのウェブサービスなどは、本人が亡くなった場合、特定の人を管理者に指定できる機能が提供されている場合もあります。調べてみましょう。

残された家族が美しい思い出に浸りながらあなたを偲ぶことができるように、きちんと整理をしておきましょう。

きちんと伝えておかないと、突然負の遺産が現れることも



これは極端なたとえですが、お金のやりとりが発生するサービスをそのままにしておくと、支払いや負債が残された家族にかかってくる場合があります。

なにをやっていたかをパスワードを含めて書き残す

お金のやりとりが発生するものは支払いや負債が発生する可能性があり、ブログや電子メールアカウント、デジタル写真サービスは乗っ取られる可能性があります。誰かが相続し管理をするか、きちんと終了させる必要があります。パスワード帳などに書き残すのも一つの方法です。

3 デジタルテクノロジーで家族を守る

1 子ども達を守る

子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。

子どもたちが犯罪に当たる行為をするとき、本人達はそれが「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。

その上で、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、子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、子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。セキュリティ設定の変更などはあっという間にクリアしてしまうでしょう。

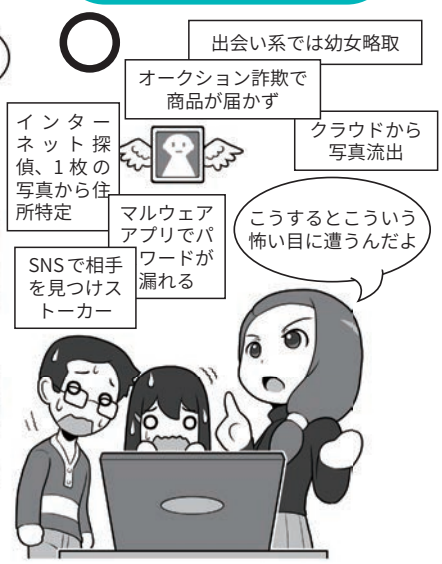
ですから、叱ったり、とがめたり、あるいは取引のようにするのではなく、その必要性を共有し、特に位置情報の共有は監視のために使わないことを約束し、そして、約束を守りましょう。

また、子どもからルールの変更

本当は怖いインターネット

理由をいわずに禁止するのは命令

ネットでなにが起こるかを一緒に見る



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。子どもだけでは、対処できないトラブルがあることを知ることは重要です。

自分だけは大丈夫と思わせない

保護者機能や位置情報を活用する

意識を共有したら、実例を示して子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。

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お子さん達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、簡単な携帯電話とGPSと防犯ブザーが合体したキッズケータイは、子どもたちが意識しないで使え、あるい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をすることができる年代になったら、位置情報を送信したり、必要な情報をメールやSNSを通じてシェアする方法を、一緒に覚えるのもいいでしょう。

幼いお子さんの姿が見えなくなって、一番困るのは迷子になってしまうことです。また、親とでもお友だちとでも、待ち合わせ場所などで誰かを探すようなそぶりをしていると、知らない人物から「一緒に探してあげる」というような声をかけられる隙になります。目的の場所に迷わずたどり着け、必要であれば待ち合わせをし、迷わず会うことができるスキルを身につけると役に立つでしょう。

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、今後地下街や屋内などにビーコンと呼ばれる機械の設置により、屋内でも位置情報の交換が可能となると考えられます。

そのほかにも、電車やバスの乗り換え案内アプリ、徒歩ナビゲーションの活用などを覚えることで、どこかではぐれても、家に帰り着くスキルを一緒に学びましょう。

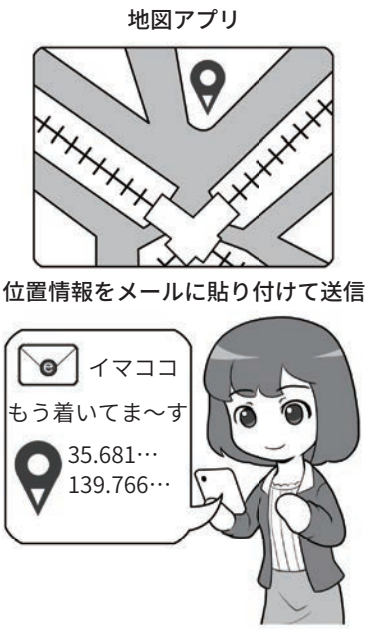
見守りメール

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いいでしょう。

GPSつきキッズケータイ

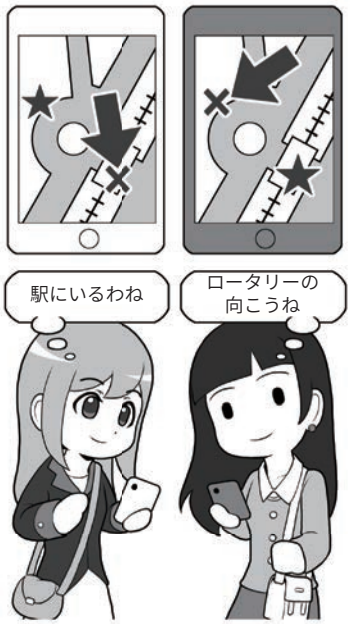
連れ去りや変質者に遭遇したときに使用する、防犯ブザーと簡単な通話機能が一体になった携帯電話です。簡単な操作で登録された特定の人物への通話なども可能です。

位置情報メール



「位置情報を共有」→「メール」などで設定すると、現在地を簡単にメールで送ることができます。これを相手宛に送れば、相手のスマホで地図アプリが起動して位置を確認できます。

位置情報シェアアプリ



本当に親しい友人とは、常時位置情報を確認し合えるアプリを利用するのもいいでしょう。そうすることでいちいちメール送信せずに位置情報を共有できます。

2 お年寄りを守る

離れて暮らしているお年寄りと連絡を取り合うのに、テレビ電話機能に対応したスマートテレビや大きなタブレット、液晶付きスマートスピーカーをプレゼントして、ときどき映像つき電話をして声だけでなく顔を見せるのもいいでしょう。

また、一人暮らしのお年寄りの見守りのために、よく相談をした上でウェブカメラの設置をしたり、毎日部屋の中を動いて電化製品やガスを使用しているかをメールで連絡してくれるサービスも存在するので、こちらも相談し、納得してもらった上で利用したりするのも一つの手でしょう。

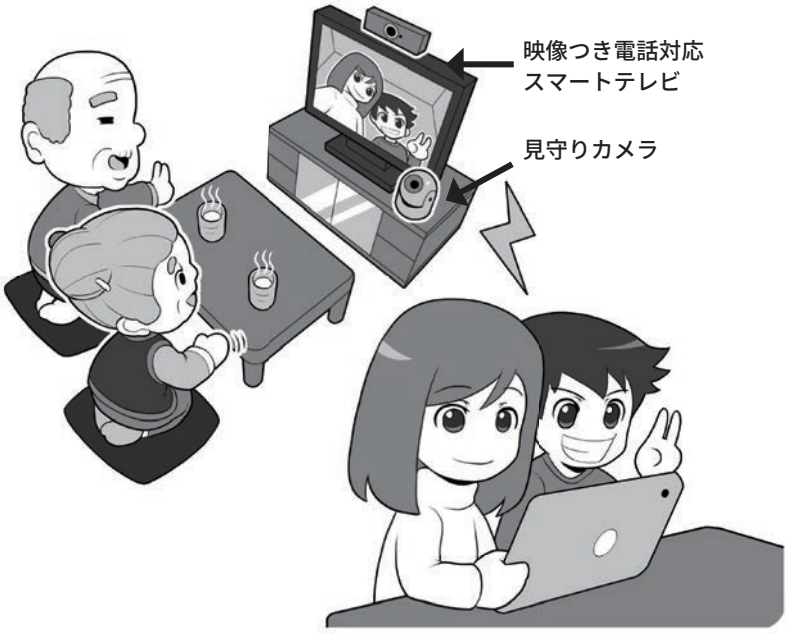
一番いいのは会いに行くことですが、離れて住んでいて頻繁に会えないならば、そういうときこそインターネットの「距離とその移動に必要だった時間が消えた世界」という能力を生かしましょう。

また、「自分は大丈夫」と思っているお年寄りほど、あっさりと振り込め詐欺などに引っかかってしまうものです。振り込め詐欺は電話で顔が見えない状況で、相手を不安に陥れ正常な判断ができなくなることを利用しています。

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、だまされることを回避できるかもしれません。

そのテレビ電話機能のためではありませんが、お年寄りには使いやすい簡単操作のスマホを渡すのも一つのアイデアです。または、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同じ機種を渡しておくのも一つの考え方です。

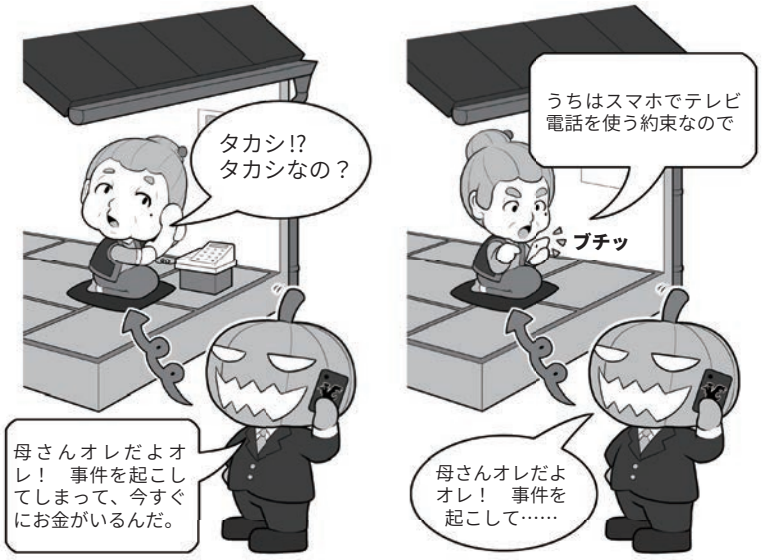
映像つき電話やITサービスの活用



お年寄りにとって子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、一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、利用を検討してもいいでしょう。

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、かかってきた電話を受けることはできるものです。子どもや孫から連絡を取るときは必ずTV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。

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することができるので、予定どおりに旅行しているかもチェックすることができます。

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、どのようにしたらいいかのアドバイスも的確にできるでしょう。

そん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られたりした場合も、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することもできます。

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に出て徘徊し、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。

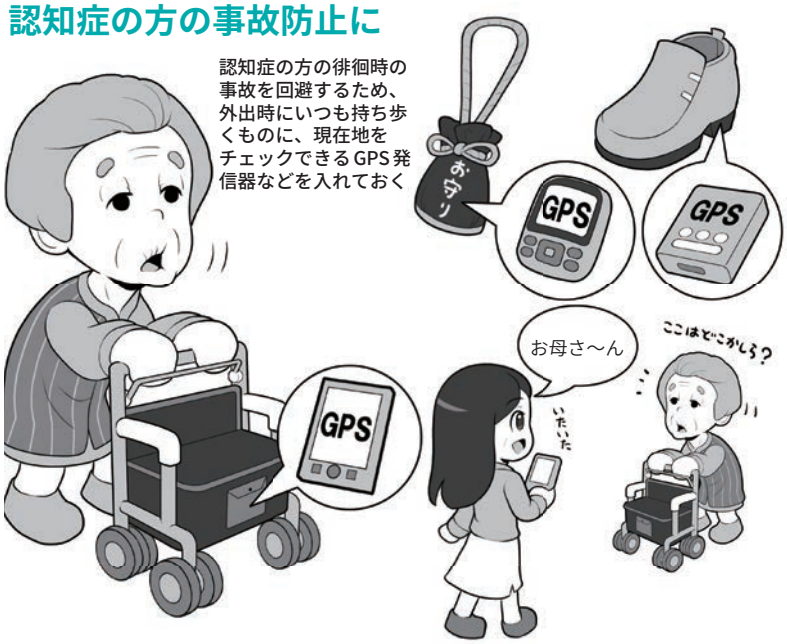
お年寄りによっては、持ち慣れない機器を持つことを嫌がる場合もありますので、機器を入れる場所の工夫は必要ですが、事故などを未然に防げる可能性が少しでも高くなるならば、検討してみると　いいでしょう。

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、そもそも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ういった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。

4 屋外・海外でのネットワーク利用

1 一見なにもないように見えて、危険がいっぱい

例えば、国内でも国外でも、あなたが屋外のカフェでパソコンを開いてウェブを見たりメールをやりとりしたりするとします。カフェには無料の無線LANアクセスポイントがあって快適にネットに接続することができます。うららかな日差し、さえずる鳥の声、実に平和そのものだし、ちょっとお店に入ってケーキでも選んでこようかな？

さぁこのカフェには、どんなサイバーセキュリティ上の危険があると思いますか？

まず日本では、よくスマホで席取りをしてレジに行くのを見かけますが、海外では、貴重品は肌身離さず持つことをおすすめします。日本と同じ治安レベルとは限らないので盗難される可能性があります。日本でも油断はなりません。

また、席に置きっぱなしにしたパソコンへ目を離した一瞬に、USBメモリを差し込んでマルウェアに感染させることもできます。

所持品が盗まれなくても、肩越しや場合によっては双眼鏡や望遠レンズを使って、スマホやパソコンのロック解除用PINコードを盗み見されるかもしれません。

お店の無線LANアクセスポイントの暗号化は、本当に安全な方式ですか？パスワード(暗号キー)を店内に貼り出していませんか？通信を盗聴されたり、ウェブサービスにログインするIDやパスワードを盗まれたり、不正なサイトへ誘導されたりするかも知れません。そのために攻撃者が店のアクセスポイントと全く同じ名前の偽のアクセスポイントを設置して、あなたを待ち構えているかもしれませんよ。

気をつけてくださいね。

2 インターネットカフェの利用

海外旅行に出かけるときになるべく荷物を減らそうとすると、仕事での渡航でないなら、パソコンはお留守番になるでしょう。

最近では、スマホもありますし、長いメールを書く必要があるなら、インターネットカフェに行って、ウェブメールを利用すれば、ホテルでもなんでも予約できるし…、なんて思ってはいませんか？

インターネットカフェは、国内外を問わず便利ではありますが、これを使ってメールやなんらかのウェブサービスのIDとパスワードの入力、あるいはクレジットカード情報の入力は、絶対に避けることをおすすめします。

海外のインターネットカフェのパソコンは、管理が充分ではないことがあるほか、攻撃者にとっても狙いやすいターゲットでもあります。キーロガーというマルウェアを仕込んで、利用者が入力したIDやパスワードなどの個人情報を抜き取って攻撃者に送信してしまうことがあるのです。

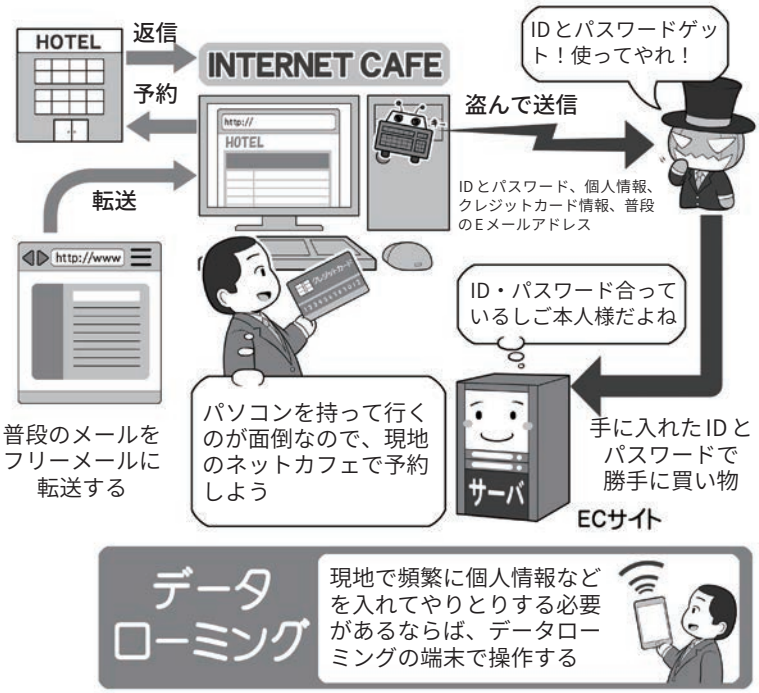
お店の人がシステムを最新に保ち、セキュリティソフトも入れ管理しているから、そんなソフト仕込めないよ、と思ったら甘いのです。キーロガーにはハードウェア版もあり、数秒あればパソコンの本体の後ろ、キーボードのUSB端子と本体の間に装着でき、あとは無線LAN経由でデータを送信できるものもあります。今まで利用したパソコンの後ろをいちいち確認したことはないでしょう？

また、自分のパソコンやタブレットを持ち込んで店のWi-Fiを使用する場合は、自前の暗号化ができないなら利用はおすすめしません。もし現地で頻繁にデータ通信を利用するならば、データローミングや現地の定額SIM（次頁参照）の使用をおすすめします。

インターネットカフェのマシンには、キーロガーなどが仕込んである前提で利用する

インターネットカフェは、基本的に情報を検索するだけに利用します。IDとパスワード、個人情報、クレジットカード情報は絶対に入力しないように。自分の持ち込みパソコンなどを利用する場合は、自前の通信の暗号化ができるならOKです。

共用のパソコンで重要な情報をやりとりしたら攻撃者に漏れる可能性あり



インターネットカフェで普段利用しているウェブメールを使うのは危ないと考え、フリーメールアドレスを作成しそこにメールを転送しても、結局予約のやりとりなどを現地で行うことになるのなら、情報流出の危険性はかわりません。

現地でそういった情報を入力することが多いのならば、タブレットなどでデータローミングを行うか、自前の暗号化+公衆無線LANを使うようにしましょう。

3 海外でスマホやタブレットを活用するために

スマホやタブレットを海外旅行にもっていって現地で使う場合、日本で契約している携帯電話会社が提供するローミングサービスを使って、現地の携帯電話回線提供会社と契約せず、データ通信を利用する方法があります。

ローミングサービスは国内よりは割高で、また、音声とデータ通信は別々に料金設定されていることもあるので、利用した場合いくらかかるのかをよく確かめてから使いましょう。さもないと途轍もない料金請求が届く場合があります。最近は手頃な1日あたり料金定額などのプランも存在します。

また海外では、電話を受けただけでも電話料金がかかる会社もあります。着信が無料ではない場合、電話を受けたらいくらかかるのかもチェックしておきましょう。さもないと、不意の長話で高額な請求が来てしまうかもしれません(くどい?)。

データ通信が使えなくも、短い文章のやりとりをする方法にショートメッセージ(SMS)がありますが、これも利用可能かどうかと、利用できる場合の料金を調べておきましょう。電波整備状況がよくなくデータ通信が使えない場合の文字通信手段になります。

ローミングサービスを電話で利用するメリットは、海外にいても自分の電話番号にかかってきた通話を受けられることです。

もし、長期で滞在する場合などで、その間電話番号が変わってもいいならば、現地携帯電話会社のSIMを購入して利用する方法もあります。SIMには目的別に音声のみ、音声＋データ通信、タブレット用にデータ通信のみなどのSIM

海外で電話やデータ通信を使う

普段の電話番号で着信できるようにする

音声利用：
マイ端末で(音声)
ローミング

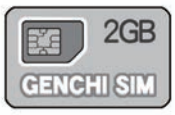
データ通信利用：
マイ端末で
データローミング

電話番号が現地のものになってもいい

音声利用：海外はSIMフリー
相当のマイ端末か、SIMフリー
端末＋現地SIM

データ通信利用：海外はSIM
フリー相当のマイ端末か、SIM
フリー端末＋現地SIM

現地SIMは現地空港などでも買えるが……



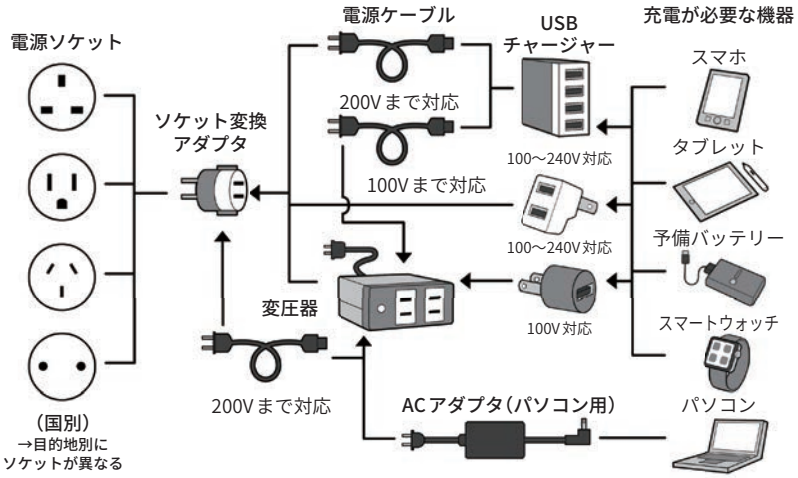
- 日本で買えることも(SIMのサイズに注意)
- 事前使用設定を済ませておく
- 音声の料金、データ通信の上限容量をチェック
- 月額料金が発生せず、チャージすれば保存可能なものもある。何回も訪れるなら選択肢に
- 料金は従量制か、上限のある定額制か確かめる

外国語が苦手だからメールでやりとりしようと思ったら

海外では意外とデータ通信できず、音声のみのエリアも多いのです。データ通信できても遅い場合もあります。データ通信速度を確保できないことを想定して、地図アプリの地図データなどは日本で事前にダウンロードしておきましょう。

電源・充電方法の確保

ソケットと電源のボルト数はまちまち。理想的にはすべて100〜240V対応であること



USBチャージャーのUSB端子は、充電する機器の数だけ差し込み口はあるか、全体の電源容量は足りているか、タブレット用には充電能力は足りしているかチェック。200V系の国へ訪問するときは、ACアダプターだけでなくケーブルまでもが200V対応かをチェックします。

が存在します。

普段の端末は日本からの着信専用にして、別途SIMフリーの端末を用意し、これに現地のSIMを入れて使用する方法もあります。

海外のSIMを使う場合の注意点は、利用する端末が「SIMフリー」か同様の状態であることを確かめることです。日本の携帯電話会社で販売されてる端末は、その会社のSIMしか使えない設定になっていることがあるからです。ただ、多くの端末では、国内では制限があっても海外ではどのSIMでも使える「SIMフリー」相当になっているものもあり、また、条件を満たせば携帯電話会社が有料でSIMフリーに改修する「SIMロック解除」を行ってくれます。

また、忘れがちなのが充電に関することです。充電器の対応電圧と、充電器にケーブルがある場合はこのケーブルの対応電圧が訪問国の電気事情にあっているか確認して、必要に応じ変圧器を用意、また、現地の様々なタイプの電源ソケットの形状に対応できるソケット変換アダプターも用意しておきましょう。

次に、せっかくスマホなどを海外に持っていくのなら、海外で使える機能や役立つ機能を準備していきましょう。

まずは翻訳系です。文字を入力するのではなく、音声で入力、翻訳結果も音読してくれるアプリなどもあります。また、逆に相手にしゃべってもらってそれを翻訳することもできるので、音声を使って現地の人と理解を深め合うことができるでしょう。

次は翻訳カメラ。海外で街並みやメニューなどを撮影すると、文字部分を認識し翻訳して表示するものです。こちらもいちいち辞書アプリなどに文字を入力する手間が省けますので、海外の旅をより楽しむことができるでしょう。

地図系のアプリのインストールと、現地の地図のダウンロードも重要です。前述のコラムでも書きましたが、海外では場所によっては日本のように通信網が充実しておらず、データ通信があっても遅いか、場所によっては全く使えないこともしばしばです。そんな中で、現在地を確認しなければならない状態になったとき、オフラインでも使えるように、地図をスマホにダウンロードできるものを準備しておきましょう。

海外でITを活用する

翻訳アプリ

翻訳カメラ

地図ソフト、GPSナビ

(音声)ローミングの注意点

- 海外では通話を受けても料金がかかる場合もある
- ローミング時の料金はいくらかかるのかチェックしておく
- SMS(ショートメッセージ)が利用できるかどうかと、その料金

データローミングの注意点

- 必要がないなら、データローミングの設定を必ず切る
- つながるからと放置しておくと、莫大な請求金額がくる場合がある

海外利用におけるSIMフリーとは

手持ちのスマホなどが海外でも使えるか

- 目的の国でのローミングに対応しているか、実際使用されているか。現地の会社の周波数帯(バンド)に合っているか
- 海外のSIMが使用可能か(≒SIMフリー)

日常使っているスマホなどを、SIMを入れ替えて使う

- ○ 現地SIMなら料金も手頃なものがあり、電話料金も安い
- ✕ 日本から普段の番号につなげない。滞在期間中の電話番号を教えておく必要あり

SIMフリー端末の入手とは

- 日本では、特定の会社のSIMのみ利用可能だが、海外では、どれでもOK(海外では「SIMフリー」相当)
- お金を払うと携帯電話会社がSIMフリー状態に改修してくれる(SIMフリー)
- そもそも電気店やメーカーから直接SIMフリーのスマホを買う(SIMフリー)

普段使っていないSIMフリー機を使う

- ○ 手頃なSIMフリー機を入手するか、使わなくなったものをSIMフリー化しておく
  現地SIM使用、料金も手頃
- ○ 普段使用の機種は電話を受けるだけのローミング。日本の電話番号でかけられる
- ✕ 2台持ちは面倒

5 大災害やテロに備える

1 まずは自分の身の安全を確保する

大地震・各種の自然災害・テロなどが発生したり、なんらかの避難勧告が発表されたら、決してその場に留まって写真を撮ったりSNSに投稿したりせず、速やかに安全な場所に避難しましょう。

海や川の近くでの大地震ならば、急いでできるだけ高い場所に避難しましょう。昨今の豪雨・水害などの自然災害の例を見ると、避難勧告前に自主的に避難場所に移動することが安全です。

災害時に現場で写真を撮ったり、実況放送のようにレポートすることは、あなたの仕事ではありません。無事家族の元に帰ることが使命です。それを最優先に考えて、まずは命を守る行動をしましょう。

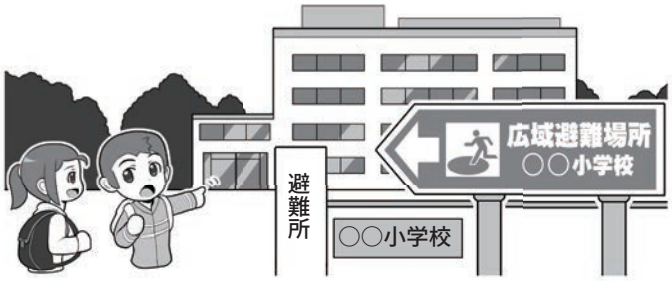
避難場所に到着し、そこが安全であると確認できたら、安否確認の連絡や情報収集をしましょう。

安否確認サービスは様々なものがあるので、家族や友だちと事前にどのサービスを利用するかを決めておきましょう。また、災害時はスマホの電話やウェブの閲覧などは混み合ってつながりにくくなります。災害時に通話が優先される公衆電話や、データ通信量の少なくてすむ、メールやSNSなどのサービスを使いましょう。

なお、スマホアプリの通話機能もメールなどより通信容量を多く使います。譲り合い、少ないデータ通信ですむ手段を利用しましょう。

命を脅かすものから速やかに逃げる

安否の連絡や情報収集は安全な場所に着いてから



自然災害時は避難勧告が出る前でも、自主的な避難が命を守る行動になります。まずは身の安全を確保し、その後、安否の連絡や情報確認を行いましょう。

そして安否連絡や安否確認サービスに登録

安否確認の方法は、複数の候補を事前に家族などで決めておいて、それらを利用するようにしましょう。災害時には、スマホを含む一般の電話は通話がつながりにくくなります。電話連絡をする場合は、公衆電話か避難所に設けられる災害時用の電話を利用しましょう。なお、インターネットが使えなくなった場合の避難手順や安否確認方法も検討しておきましょう。

2 電池をもたす、情報収集をする

災害時などに街中なのにスマホが圏外になったら、それは通信会社の基地局が機能しなくなった印です。そのまま電源をONにしておくと、スマホはつながらない基地局に接続しようとして貴重な電池を消耗してしまいます。

そういったときはスパッとスマホの電源を切るか、スマホの中身を見る場合でもフライトモード（機内モード）にして少しでも電池の消費を抑えましょう。

電波が回復しても、電話よりはデータ通信であるメールやSNSを利用しましょう。災害時はその方がつながりやすく、電池の消費も少なくてすみます。次に、いつ充電できるかわからない状況では、とにかく電池の節約を心がけましょう。モバイルバッテリーを日常的に持ち歩くのもいいでしょう。

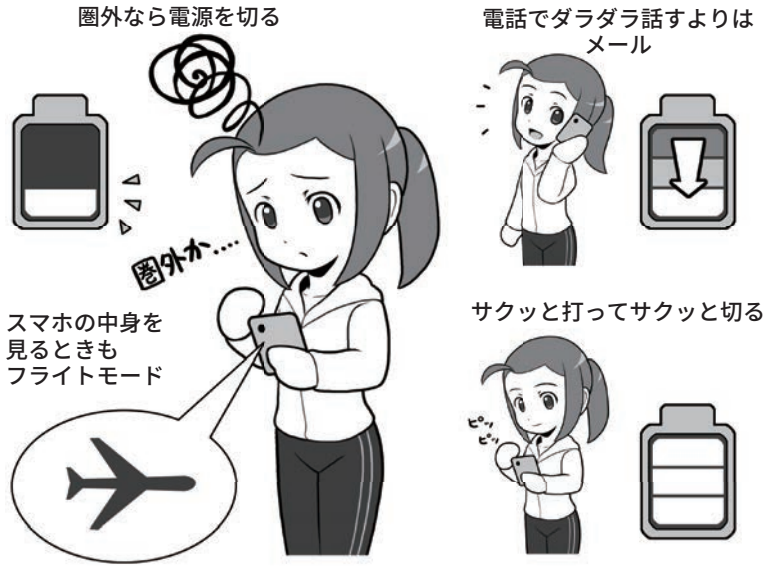
災害直後は情報が錯綜しますが、一定時間が経過すると救援物資や脱出ルートなどの情報がネットに発信され、やがて整然とした情報発信が行われるようになります。

しかし、だらだらとウェブを見て回って情報を収集しても電池を消費するだけなので、メールやSNSで、情報の収集と整理に長けた家族や親しい友人に助けを求め、信憑性や関連性の高い情報、必要としている情報だけを整理して送ってもらうのもいいでしょう。

東日本大震災では、旅行で被災地に訪れているときに震災に遭い、帰ることができなくなった方たちが、SNSを通じて被災地から地元に帰るためのルートの確認や車両手配、バスの予約などをしてもらった例もあります。

ぜひ、そういった事例をみんなで話し合って、いざというときにどうするか、ということを相談しておいてみてください。

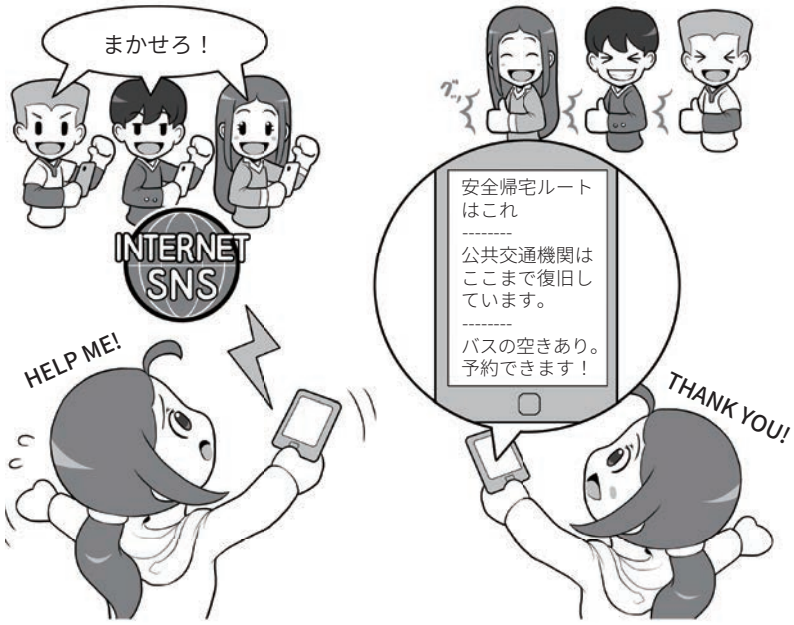
電池をもたすテクニック



圏外ならば電源を切るか、スマホの内容の閲覧時もフライトモードを利用します。電波が回復したら災害用の超省電力モードがあれば活用してもいいでしょう。

電話で長く話すよりも、メールをさくっと打って電源を切った方が電池を消費しません。充電器にもなるモバイルバッテリーを持ち歩くのも役立ちます。

情報収集に協力してもらう



情報収集に長けた家族や友人に相談して、いざというときは情報収集や必要なものの手配をお願いできるようにしておきましょう。自分一人では、気づかない情報も外から見ていると気づく場合もあります。

3 ラジオ、車載テレビを使った情報収集

大災害時に電波がきちんと飛んでいる状態でも、目的のサーバに接続しようとすると、反応がない場合があります。

それは、サイバー攻撃のDDoS攻撃のように、多くの人が特定のサーバに集中して接続することで、サーバの反応が間に合わなくなり、ギブアップの状況になっているためと思われます。

この問題は災害時には避けがたく、双方向通信のメディア、つまり私たちがサーバに接続してサーバが返信するというプロセスを前提としているインターネットでは、どうすることもできません。

こういったときに力を発揮するのが、「片方向通信メディア」である、ラジオやテレビです。これらのメディアは送信局が一方的に情報を発信して私たちが受信するだけなので、アクセスが集中し反応できなくなるということはありえません。

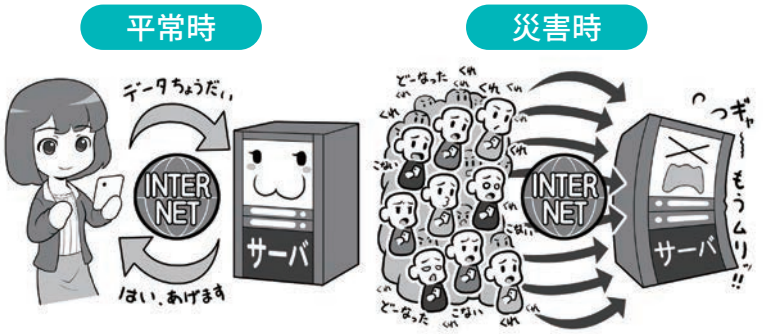
比較的近距離の範囲の放送をするテレビやFMラジオなどは、大震災時などに送信局や送信施設が自分の被災地域に含まれる可能性があります。しかし、一局で広範囲に電波を送信できるAMラジオや短波放送ならば、災害時に放送が中断する可能性がテレビやFMと比較して少なくなります。

これが災害用の持ち出し袋にAM放送を受信できるラジオを入れる理由でもあります。

トラブルに対しては、複数の手段で備えるのが基本ですから、普段は聴くことがなくても、災害用持ち出し袋にはAMラジオを入れることを検討しましょう。

また、車の中ならAM/FMのラジオ、一部は車載テレビでテレビ放送が受信できます。

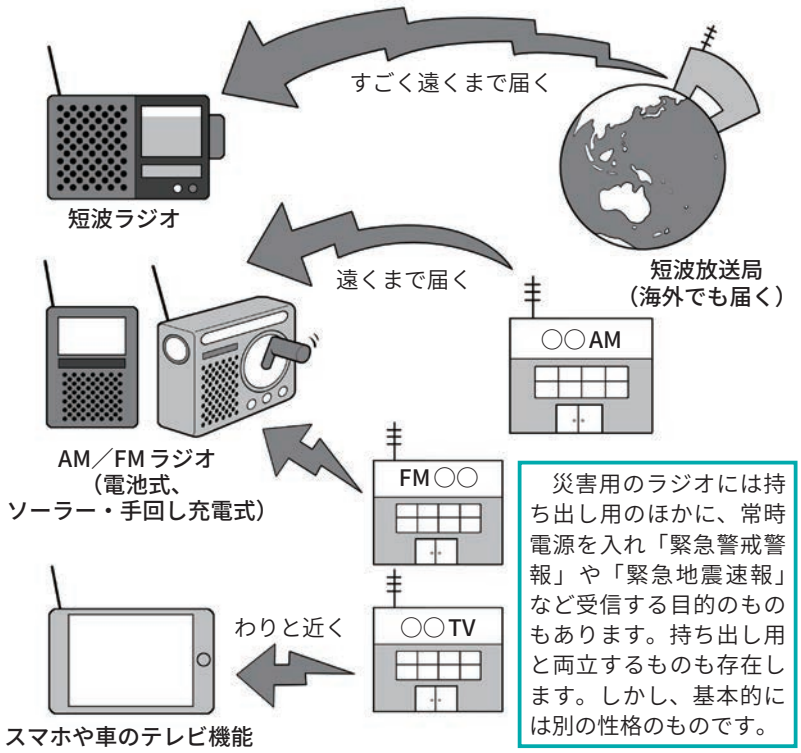
災害時のアクセス集中によるサーバの沈黙(双方向通信)



インターネットでは、私たちのリクエストにサーバが答えることで情報が表示可能になります。しかし、一気にリクエストが集中するとサーバの処理能力を超えるため、反応が返ってこなくなります。これがアクセス集中です。

災害時でも沈黙しないラジオやテレビ(片方向通信)

ラジオ・TVは一方的に送信できるので大丈夫



災害用のラジオには持ち出し用のほかに、常時電源を入れ「緊急警戒警報」や「緊急地震速報」など受信する目的のものもあります。持ち出し用と両立するものも存在します。しかし、基本的には別の性格のものです。

片方向通信の機器は、対応する受信機を持っているすべての人が受信可能です。FMやテレビは、放送局も被災して発信できなくなる可能性もありますが、AMはかなり遠くまで届くので、別の地域の放送を拾うこともできる場合もあります。短波に至っては海外まで届きますが、逆に地域別情報発信には不向きです。ラジオは消費電力が少なく、ソーラー充電や手回し式充電型も実用的です。なお、ワンセグTV搭載のスマホは少なくなりましたが、カーナビはフルセグテレビ受信可能なものもあることをお忘れなく。

4 徒歩帰宅、海外での災害やテロに備えて

災害時は、原則としては政府や各自治体・消防などの指示に従うべきですが、ときに徒歩帰宅をするという選択肢を取らざるを得ない場合もあります。スマホには、学校や仕事場から自宅までの道中、災害時に役立つ情報を掲載した帰宅支援マップやアプリを入れておくと役立つでしょう。日没時や降雨時の避難場所などもわかります。

また、その場合に備え、家族と落ち合う集合場所や、帰宅手順を話し合っておきましょう。長期大規模停電で通信できない状況まで想定して、プランを立てましょう。

災害時には、スマホの電池が命綱になる場合もあるので、普段からACアダプター体型のモバイルバッテリーや、車の電源を活用できるようにカーチャージャー、ケーブルなどを持ち歩きましょう。

海外での災害やテロに備える場合は、事前に外務省の「海外安全ホームページ」で渡航先の情報を確認し、渡航が推奨されない場所には行かないようにしましょう。

また、渡航前に外務省の海外安全情報配信サービス「たびレジ」に登録し、リアルタイムで渡航先の安全状況が把握できるようにしましょう。万が一災害が起こった場合に、緊急時の安否確認などがすみやかに行えるように、SMSでメッセージを受け取れるようにしましょう。「海外ではどういう風にデータ通信をするか」を前提に考えつつ、特にデータ通信しない場合でも、いざというとき、最低限上記のSMSメッセージは必要なんだと覚えておきましょう[*1]。

災害時に徒歩帰宅をする場合は

帰宅マップ


予備電池


ACアダプタ

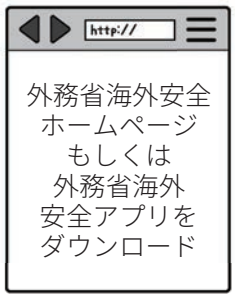
USB
カーチャージャー


タブレット対応か
チェックする
（2Aなど）

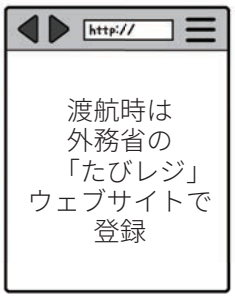
災害時は政府方針で、最大3日（72時間）程度現地に待機を求められる場合もあるので、スマホなどの情報機器を使う場合、電池を持たす準備が重要です。ACアダプター機能付きのモバイルバッテリーの携帯や、車で充電できるようにUSB端子のついたカーチャージャーを必要に応じて携帯しましょう。また、自分の機器の充電に対応しているかもチェックしておきましょう。条件に合わないと充電できないこともあります（おもに2Aや2.1A対応と書かれている給電能力）。

海外での災害やテロに備える場合は

渡航前後に現地の情報を確認する



外務省たびレジに登録する




緊急時は
SMSで連絡

たびレジ簡易登録にメールアドレスを登録する

＊1：SMSは基本的には通常の携帯電話回線（インターネット電話ではない）を利用していれば、データ通信を利用していなくてもメッセージを受け取ることができます。

注）「外務省海外安全アプリ」では、約120ページの「海外安全虎の巻」が同梱されていたり、海外安全にかかわる外務省のウェブサイトなどを簡単に分類し、手早くアクセスできるようになっていたりするので、ぜひダウンロードしておきましょう。

コラム：情報の取り扱いは国によって異なる。要らぬトラブルに巻き込まれないように

インターネットは国境を越えて世界の人々を繋ぎ、理想的には皆同じ基準で、平等にその恩恵を享受できるべきです。しかし、現実的にそれぞれの国の中ではローカルルールによって、様々な制約を受ける場合があります。

訪問国のルールを理解せず、自国の常識でネットを利用などすると、思わぬトラブルに遭遇することもあるので注意が必要です。

ここでは、あなたが他国を旅行やビジネスで訪れると想定して、遭遇するトラブルを、あくまでフィクションとしてですが考察してみましょう。

1．入国まで

あなたがA国に訪れたいと考えました。ビザは免除されていますが、テロ対策の点から、事前に入国登録することが求められました。項目には「利用しているSNSアカウントを全て記入せよ」というものがありました。

これはSNSアカウントの書き込みから、テロを起こす過激思想を持っていないかを判断するために利用するようですが、日本ではちょっとした冗談の書き込みでも、A国ではそう受け取られず、入国を拒否されそうになりました。

入国したら、今度は入国審査で、利用しているスマホやパソコンのパスワードを開示せよと言われました。様々なウェブサービスのアカウントの分もです。書き出したものの一覧を見ると、係官は鼻で笑い、ロックを外された機器は別室に持って行かれ、コピーを取られました。あなたは長い間待たされたあげく、今度は取調室に呼ばれます。

そして、スマホに保存していた特殊な嗜好のマンガや写真の所持を指摘され、法律違反で逮捕され、起訴され、懲役判決を受けるかもしれないと言われました。私たちの国では問題無くても、そういったものが法律的あるいは宗教的に許されない国も、世界にはあります。

2．入国してから

やっとの事で入国することはできましたが、パソコンは没収されてしまいました。

スマホは戻ってきたものの初期化され、ローミングでの通信も著しく遅く通信に支障が出るので、値段も手頃だった、現地で販売しているその国の携帯電話会社のSIMカードを購入しました。代金はクレジットカードで支払います。

ところが、スマホを元の状態にリカバリーしようとアプリストアを見ると、普段使い慣れているエンドツーエンド暗号化のSNSのアプリがありません。そうやらその国では、使い慣れたSNSアプリが禁止されているようです。かわりにVPNを使おうとしたら、度々VPN機能がOFFになります。やっとの事で見つけた通信暗号化するメッセージアプリをインストールしたら、今度は通信ができなくなりました。

3．撮影していると…

携帯電話会社のお店に駆け込んで、通信ができなくなったといったら、別のSIMを買うことをすすめられました。仕方が無いので、再度購入します。

回線が復活したので観光に戻って、現地での様子でも写真で撮って送ろうと、車での移動中や観光地で撮影をして、日が暮れたのでホテルに戻りました。

夕食を終えて部屋でくつろいでいると、突然部屋に警察官が入ってきて連行されます。軍事施設を撮影した容疑で逮捕されたのです。そんな場所を撮影した記憶は全くないのですが、確かに撮影したと言われ、またしてもスマホを取り上げられました。

同行者が速やかに大使館に連絡をしてくれたので、数日後やっとのことで釈放されました。

4．日本の常識は通じない

取り調べの過程で所持品も色々と没収されてしまったので、足りないものを翌日配達のオンラインショップで買おうと、アカウントを取得しクレジットカードを設定し、不正利用が怖いので、SMS経由

でワンタイムパスワードを利用する二要素認証を設定しました。

翌日、家族に帰国の日程を報告するべくスマートフォンで電話しようとすると、また通じなくなっていました。

仕方ないのでホテルの電話で連絡し、準備を整えてチェックアウトしようとしたら、クレジットカードも使えなくなっていました。

クレジットカード会社に問い合わせすると、昨日利用したオンラインショップで、一度に多量の購入があったので、利用を停止したとのことでした。

二要素認証を設定していたのに、なんで使われてしまったか調べたところ、電話番号を乗っ取るSIMハイジャックと言う攻撃に遭っていたことが判明しました。

5．帰国してからも

なんとか帰国してからしばらくすると、クラウドサーバに上げていた、子どもの成長記録のうち、いくつかが勝手に削除されていることに気付きました。

写真の内容によっては、サーバが置かれた国のルールに従って、「児童ポルノ」と判断され、国際的に手配される可能性があるかもしれないという話もありました。

また、サーバに保管していた書類が流出した形跡もありました。その国では情報は検閲され、その過程で機密情報が流出することもあるようでした。

インターネットは世界を繋ぎますが、実状として、訪問した国のルールや物理的なサーバの所在国のルールが適用されます。

自国の慣習をそのまま持ち込んだり、よく考えずに利用したりせず、必ず調べてから利用しましょう。またクラウドサーバの所在地は必ず確認し、重要な情報は自国にサーバのあるサービスを利用しましょう。

要らぬトラブル

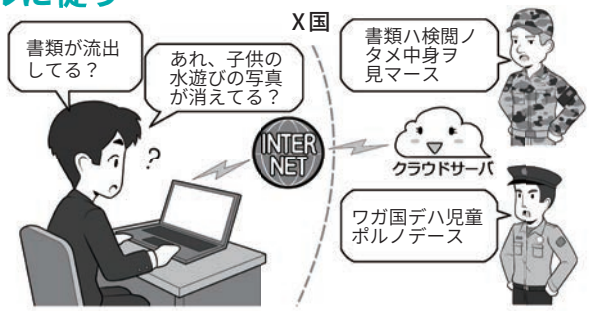
①自国で問題ない写真がアウトなことも

我が国の常識がそのまま外国の常識や法、宗教的規範に合致するとは限りません。そのルールに反すると、最悪の場合実刑を受けることもありえるのです。

②他国ではどこでも撮影していいとは限らない

また、軍事的にセンシティブな国では、関連施設にカメラを向けるだけで、スパイ容疑をかけられて拘束されることもあります。ルールを調べてから渡航しましょう。

③クラウドサーバのデータは所在地の国のルールに従う



クラウドサーバにあるデータは、サーバの実際の所在地や提供する企業のルールに従って、その内容が検閲され、その結果情報が流出する可能性もあります。要注意です。

コラム：デマに踊らされない！　ソースを探せ！　確かめよう！

昔からデマというものはありました。事件のときに拡散するものや、都市伝説のように長く語り継がれるものなど。

当時は、人から人への口伝えですから、自分が聞いた話を再度確かめようと思っても、すべて遡って大本の発言者までたどるのは至難の業ですが、その分「うわさ」ということを前提とした「不確かさ」「あやしさ」がありました。

ところが、インターネットが普及した現代では、デマは「距離とその移動に必要だった時間が消えた世界」で、恐ろしいスピードで拡散します。しかも、SNSなどの場合「何人の人がその情報を共有したか」ということが数字でついて回るので、それが何万人にもなると、デマであっても妙な信憑性があります。その代わり、ネットではソースをたどることができますので、怪しいと思って調べると、元の発言をした人間が、発言を消して逃亡してたなんてこともあります。

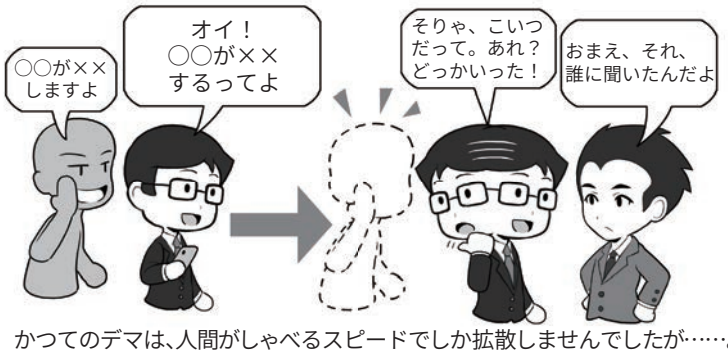
この構造は、「意図的なデマの拡散」にも使われます。デマになりそうな話題を使ったマルウェアへの感染誘導や、フィッシング詐欺を狙った釣りかもしれません。場合によっては、誰かを傷つけ名誉棄損となるものかもしれません。

情報が勢いをつけて手元に飛び込んできても、その勢いに飲まれて拡散に加担せずに、情報の信憑性を確認する余裕を持ってください。

そして、ほとんどの場合、後で冷静になって考えると、それはあなたが拡散する必要が、特にないものなのです。

それに災害時には本業の人ですら間違った発信をしてしまうミスもあるのでご注意を！

昔から出所が不確かなデマはあった

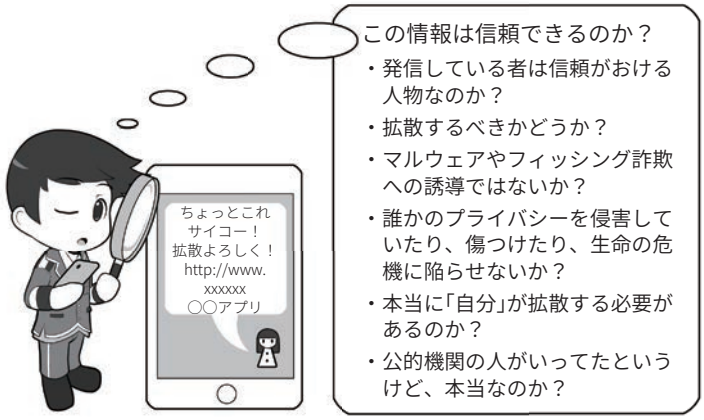


かつてのデマは、人間がしゃべるスピードでしか拡散しませんでしたが……。

ネットでは加速して飛び込んでくるが……

現在は、ネットの特性で「拡散数」を伴って加速して飛び込んできます。しかし、その数を真実かどうかの尺度にしてはいけません。元ネタが嘘だったり、意図的に流布してから消して逃げたりすることもあるからです。

情報はよく吟味することが必要



コラム：災害時の情報収集について（本年の振り返り）

近年は、様々な自然災害が発生し、その中で様々なデマが飛び交い、正確な情報収集の難しさを浮き彫りにしました。悪意のデマではないとしても、不正確な情報の拡散も多く見受けられました。拡散する方々は善意で行っているのですが、情報源（ソース）がはっきりしないものの拡散は状況を混乱させます。物事の正確さ担保するためには、「現場」を知る責任がある方の「公式な情報発信」以外は、むやみに拡散するべきではありません。特に、「誰かに聞いた」という伝聞は、たとえそれが「通信会社の人に聞いた」「役所がの人が言っていた」というものでも、公式発表ではないかぎり、「不正確」である可能性が高くなります。「伝聞情報」には気をつけて、「本当に拡散するべきか」良く考えてください。

また、災害時の救助要請をSNSで行う方法が、広く一般に認識されたことが確認されました。これも本人、もしくや直接依頼された家族などの代理人が行うことは大変有効な手段ともいえますが、上記と同様に伝聞の情報を拡散したり、あるいは本人が救助された後も救助要請が残されたままだったりすると、それが一人でも多く助けようとする方の妨げにもなります。それ以外にもSNSの情報を見て、直接関係がない人が善意で電話での救助要請を行うなどのケースがあったようです。

こういった情報は、本当に必要な情報収集への「雑音（ノイズ）」となる可能性があるので控えましょう。

また、最近は様々な災害時用のアプリが登場し、安否確認の方法も増えてきていますが、これらは連絡を取り合う人と、事前になにを使うか決めておかなければ意味を成しません。きちんと利用するサービスの確認をしておきましょう。

なお、2018年に北海道を襲った地震では、全道が長期間にわたって停電する事態が発生しました。携帯電話網もスマホも使えなくなる可能性が垣間見えた災害でした。そういった場合どういう手段で連絡を取り合うかも確認しておきましょう。

災害時の避難所などでは、自治体や電気通信事業者の取組により、無料で使えるWi-Fi「00000JAPAN」などが立ち上がることがありますが、このWi-Fiは接続しやすさを優先するため、暗号化されていないことを覚えておき、利用時はIDとパスワードの入力を避け、もし利用したい場合はVPNなど自前で通信を暗号化する知識を得ておきましょう。

災害時の救助関係発信はわかりやすく確実に

公的機関の災害時の窓口は、あくまでも110番119番の電話ですが、SNSで救助関係の発信をするときは、住所やGPS情報を付けましょう。

災害時は必要がない情報の拡散はひかえる

平成30年7月（西日本）豪雨時の不要不急拡散TOP3

…災害時に拡散しなくてもよいのでは？

5 ネットを使わない移動トレーニング（現代版オリエンテーリング）

災害時に、スマホの電池が切れてしまったり、あるいは旅行先でスマホを落としてしまったり、誰かに盗られてしまったりしたシチュエーションを想定して、スマホを使わずに自力で自宅に帰り着くためのトレーニングを、遠足のような遊びの一環としてチャレンジしてみましょう。

例えば、地図とコンパスやGPS受信機を持って、地図を読んで現在の場所を特定し、ハイキングルートを抜けて駅の場所を目指したり、駅に到着したら鉄道路線図から自宅までの経路を割り出したり、駅に設置されている時刻表をめくって自宅までの電車の時刻を書き出してみたりしましょう。

こういったことは、実はオリエンテーリングという野外スポーツのアレンジで、慣れると面白いゲームとして取り組むことができます。目的地を自宅ではなく、遠くの親戚の家へ訪問する機会にトライしてみるのもいいかもしれません。

地図が読めるようになると、コンパスがあるだけでも結構なんとかなるものですよ。

さて、最近はスマホになんでも記録できてしまうため、自宅の電話番号や家族の電話番号を覚えていないケースもあります。緊急に連絡を取る必要のある大切な番号は暗記して、公衆電話を見つけてコインやテレホンカードで電話をかける訓練をしてみましょう。公衆電話が見つからない場合は、お店などで聞いて探すところから始めるなど、いろいろなサバイバルを試してみてもいいでしょう。

ゲームとして帰宅サバイバルを楽しむ

地図の地形や記号などを読んで、現在地の特定にチャレンジしてみよう

ゲームとしていろいろなことにチャレンジしよう

GPS 情報からの現在地の地図の落とし込みや経路探索をしよう

電車の路線図を見て、自宅までの経路を決め、切符を買ってみよう

こういったことを経験しておくと、災害に遭ったときにスムーズに行動にすることができます。

大災害でもそんなことは起こらない？　いえ、こういったことは、どこまで「まさか」と思うことを想定できるかが、サバイバルの鍵になるのです。

エピローグ

来たるべき新世界へ

みんなが守るインターネット、その未来にはなにがあるの？
そのインターネットに、新しいテクノロジーが組み合わさって進化を遂げていったとき、
私たちはどのような世界を実現し、その先になにを見るのでしょうか。
少しだけ、未来を想像してみましょう。

1 ネットの「今」と、これからをどう守っていくか

インターネットというのは、今の40歳代後半の大人から考えると「便利な道具」であり、現実世界をサポートする存在といったイメージでしょう。それは、逆に今のようにネットがなかった「不便な時代」を知っているから比較ができるからでもあります。

しかし、生まれたときからインターネットが存在している環境で育った子どもたちは、インターネットを道具としてではなく、現実世界と一体として感じている場合もあります。

例えば、ネットへの接続が高速化して、ものを思い出すのとさほど変わらないスピードで情報端末から目的の情報を引き出させるようになった今、「いつでもネットから引き出せる情報」を、「少し思い出すのに時間がかかる記憶」ぐらいのようにあつかい、あまり脳に記憶することにこだわらないようになっている。そんな風に感じることはありませんか？機器がさらに進化して、考えれば答えが分かるようになれば、その「区別」すら感じなくなるかもしれません。

また、現物の本や紙ではない、ネット上のファイルやデータの受け渡しは、もはや「渡す」という概念ですらなく、スマホ一つで共有するだけ。あとは誰がどこからでも遅延なく「リアルタイムで共有」どころか「編集」までできてしまいます。現実世界に軸足をおいた人々にはもはや感覚的にわからない、次元を超えた情報管理です。

ただ、そういったネットのメリットの部分はものすごいスピードで進化していますが、インターネットの世界はまだ生まれてから年数が経っていないため、世界として見たとき、それ以外の、特に安全を守る社会システムのインフラや秩序構築などは充分に確立されていません。

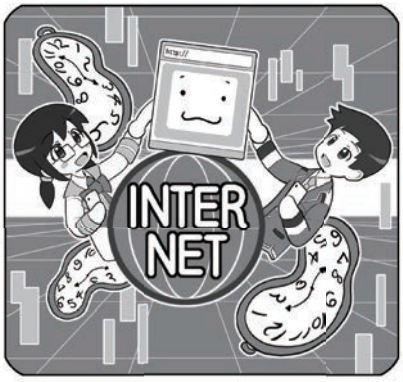
このネットの秩序に関しては、実はネットが生まれたごく初期に、現実世界から積極的にネットに移民してきた開拓意識旺盛な「ネチズン」と呼ばれた人々により、文章化されていない暗黙のモラルとして存在したこともありました。

しかし、その後ネットが一般化し、様々な人がネットに移り住んできたことによりネットは多様性を帯び、その人たちを含んだ新た

ネットは現実世界のオプションではない

インターネットの中の世界を、現実世界のオプションや便利な道具と捉える人もいますが、実際はそれに留まらない存在です。それは、現実世界と重なった新世界です。

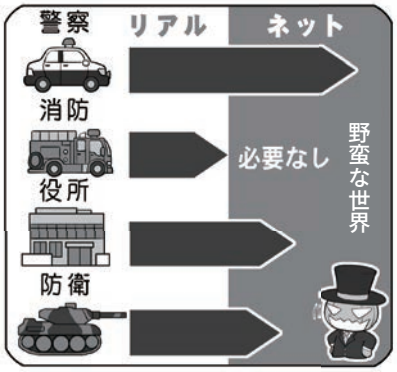
ネットは距離と移動時間の概念がない世界



ネットには距離という概念がなく、また、それによって消費されていた時間が必要でなくなる新しい世界です。子どもたちはこれを単に「そういうものだ」と自然に捉えて利用しています。

現実世界と同じ「社会インフラ」がまだ整っていない

新世界に人が先に進出して、社会のシステムや秩序の構築が間に合わない状態では、「力こそ正義」となりがちです。ある意味「生きぬく能力がない人には危険な世界」といえます。



ネットの世界には消防は必要ありませんが、そのほかのインフラは必要です。サイバー警察、電子政府、サイバー防衛などが次第に整いつつあります。しかし、国民全体の協力が必要です。

な秩序の構築が間に合わないまま、現在に至ります。そうして秩序が振り出しに戻ると、ネットの暗部では「強いやつが奪い、奪われるヤツが悪い」という、力こそ正義の、大開拓時代のようになったのです。

ネットが本当の意味でみんなが安心して使えるようになるには、ネットに必要がない消防はのぞき、警察や役所、場合によっては防衛などの秩序を作るシステムが対応しなければならず、それにはまだしばらく時間がかかります。

それでも、秩序が形作られる片鱗は見えつつあります。

警察組織などは、インターネットの匿名性を悪用して犯罪を行う攻撃者を、地道な努力と解析で追跡し、特定するための技術を磨きつつあります。

私たちが現実世界の住人であり、完全にはネットの中だけで生きていくことができません。ネットの闇に隠れても、攻撃者が人であれば、現実世界での痕跡を完全に消すことはできないのです。

しかし、そういった公的な能力の向上とともに大切なのは、ネットを利用するすべての人たちが、ネットを守ろうという意識を共有し、協力しあうことです。

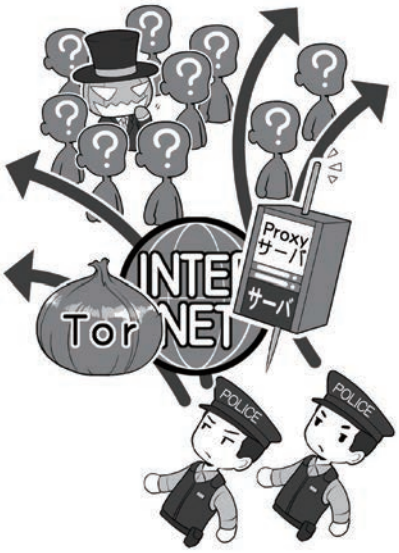
現実世界の秩序が、警察だけでなく国民一人ひとりの防犯意識や、公衆衛生運動、その他の啓発活動の結果、成り立っているように、ネットも、会社や学校の中や、友だちや家族の間で、どうやったら秩序のある世界にしていけるのか、そのためにはなにができるのかを考えることで、初めてネット上の「秩序」「防犯意識」「公衆衛生」が醸成され、「社会全体としてセキュリティを向上する」というベクトルを持つことができるのです。

ネット上の社会インフラの構築と、みんなのセキュリティ意識の向上、それは車の両輪であり、いずれかが欠けてしまっても、安全なネットは成り立ちません。

そうして、ネットが安全な「社会」になることができたとき、子どもたちをネットから遠ざける必要がなくなり、もっとネットの世界とともに進化し、より自由な発想で、新しい才能を開花させることができるようになるのでしょう。

そのためにも、ぜひみなさん一人ひとりが、それぞれの立場でネットの世界のセキュリティを守る知識をもち、これを行う人になってほしいと思います。

匿名の通信は追跡が困難だが…



ネットでは意図的に、正体を隠す環境を悪用し犯罪が行う者たちがいます。匿名通信するネット、匿名のSNS、防弾サーバ、成りすましの利用などです。

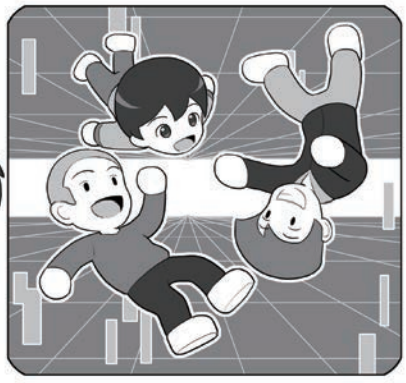
それでも徐々に技術は向上

最近では、「バレないと思った」という犯人を捕まえたり、ネットの闇に隠れる攻撃者を追跡する能力が向上しつつあります。

取り締まりは大切だが「防犯意識」醸成も大事

犯罪を起こしたら、きちんと検挙することは抑止力になります。しかし、みんながセキュリティを守ろうという「防犯意識」を醸成することも大切です。

デジタルネイティブの子どもたちに安全な世界を



デジタルネイティブの子たちが犯罪に巻き込まれず、ネットの世界で才能を開花させられるように、ネットの安全を守らなければなりません。

2 デジタルネイティブと未来

パーソナルなコンピュータの歴史が始まってからまだ30年しか経っていないこともあり、世の中にはまだ「パソコン」や「ネットワーク」が存在しなかった時代を知る世代の人がたくさんいます。

その人々の一部は、世界にパソコンが生まれ、ネットワークが生まれ、やがてインターネットの誕生と大規模なネットワーク化により「距離とその移動に必要だった時間が消えた世界」が生まれたとき、その世界に未来を見ました。

やがて、その先進的な開拓者たちは、移民のように生活の軸足を新たな世界に移し「デジタルイミグラント(デジタル移民)」と呼ばれるようになりました。

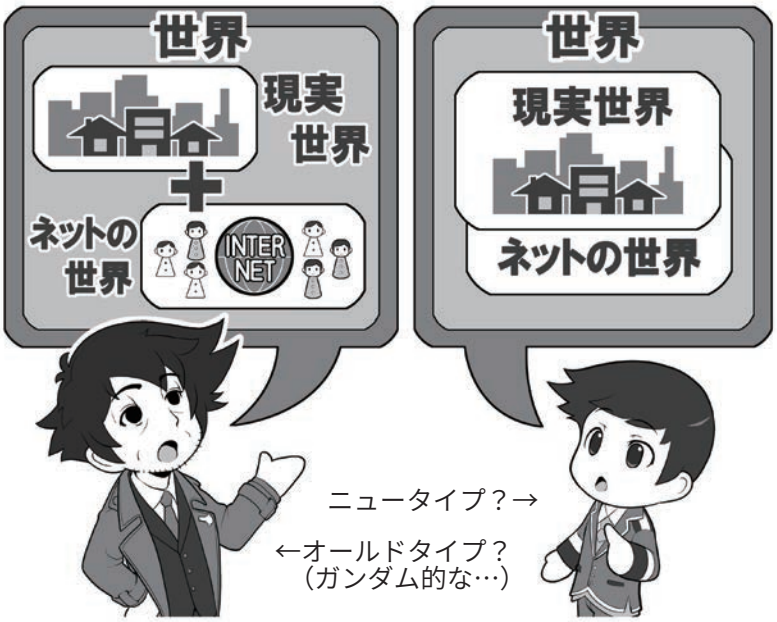
これは、現実世界にたとえるならば、古い世界に息苦しさを感じていた人々が、新大陸に夢を思い描き、そこに移住し、新しい社会を築き始めたようなものでした。

しかし、インターネットが大衆化したWindows 95から20年、初代スマホと呼べる存在であるiPhoneが誕生から10年の時が過ぎると、多種多様な人々がその世界に移住してきました。「距離とその移動に必要だった時間が消えた世界」にも子ども達が生まれ、ネットを無意識に使いこなす「デジタルネイティブ」と呼ばれる世代が形成されるようになってきました。

そういった世代が社会の中心となると、いままで距離と時間の概念によって形成されていた世界の国の人たちとの意識の壁が、技術力とともにあっけなく解決されていくかもしれません。

海外で生まれた子ども達が、多言語をネイティブのように操り、様々な国の考え方を当然のように理解するように、すべてを楽々と越えていくでしょう。

デジタルイミグラントとデジタルネイティブ



デジタルイミグラントは手紙に対するメールのように、ネットを現実世界のオプションとして捉えて「便利になった」と考えますが、デジタルネイティブには現実とネットの世界は一体であり、メッセージは一瞬で届く「距離とその移動に必要だった時間が消費されない」コミュニケーションを当たり前と捉えています。

技術の進化で文化の壁をあっさりと乗り越えていくかも

自動翻訳つきテレビ電話は、すでに一部の言語で始まっています。スマホの翻訳アプリでは、発音した言葉を翻訳してしゃべってくれます。言葉という壁、それに伴う意識の壁も、あっさりと壊される日がくるかもしれません。

3 バーチャル空間を超えて世界へ

デジタル機器の進化は、さらにネットと私たちの融合を進めるかもしれません。

例えば、仮想の3次元空間を目の前に実現するバーチャルリアリティシステムは、驚くべき没入感をもち、まるで自分がその空間に存在しているかのように感じさせてくれます。

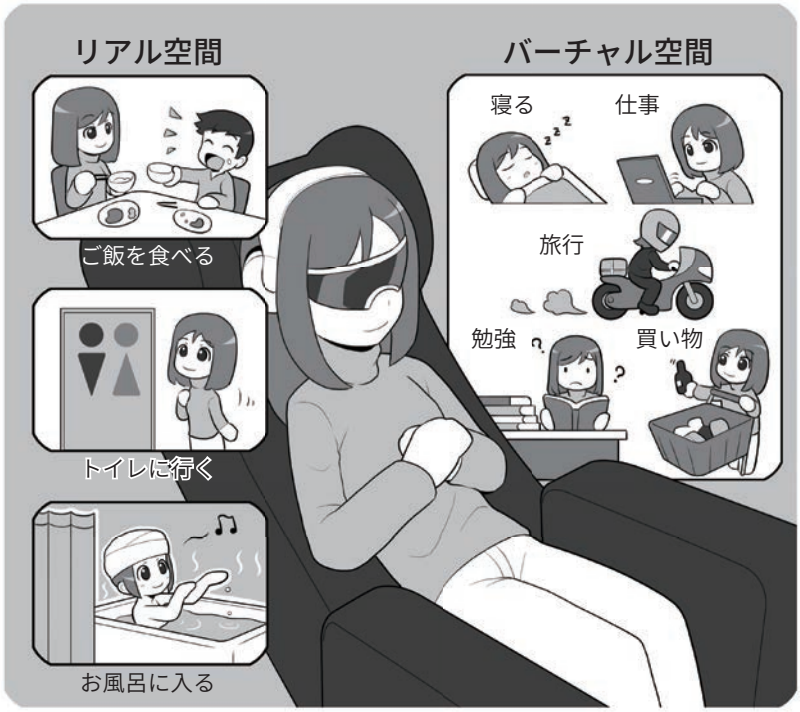
仮想空間を使って生活することを前提に考えると、現実の世界でしかできないことは意外に少なく「ご飯を食べる」「おトイレに行く」「お風呂に入る」といった生理現象と清潔さに関するものだけになるかもしれません。

そんな世界が来るはずがないと思うかもしれませんが、実は私たちは毎日「夢」で同じような経験をしています。夢の中の出来事を現実の出来事と混同してしまうことがあるように、「経験」とは必ずしも現実世界だけのものではなく、脳にとっては、どれも等しく同じ経験なのかもしれません。

そして、こういった技術がさらに進化を遂げれば、自分の部屋からネット経由でアクセスして、世界各所で「アバターのロボット」をレンタルして、実際にそこに訪れるのと同じように、世界の国々を旅してみたり、その国の人とコミュニケーションをしてみたり、あるいは学校で学ぶことができるようになるかもしれません。

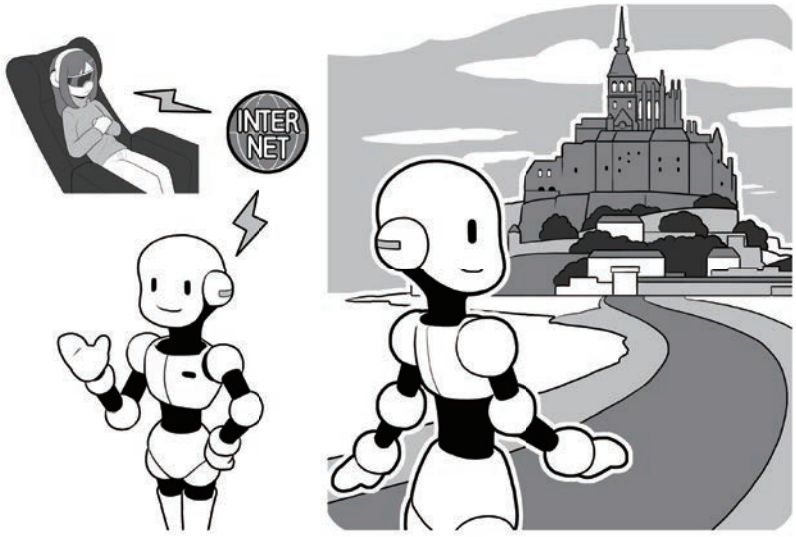
それは、体が不自由な人、あるいは病気でベッドから起き上がれない人たちにとっても、社会参加することができるツールにもなるでしょうし、私たちが世界の様々な国の人々との相互に理解しあう　ことにも役に立つでしょう。

リアルである必要は意外と少ない



ゲームに出てくるような素敵な空間で旅行したり、机を広げて仕事や勉強をしたり、お店があれば買い物をしたりなどバーチャル空間で実現できることはたくさんあります。私たちが夢の世界でやっていることも、現実世界ではないという意味では同じです。一方、ご飯やトイレ、お風呂はバーチャル空間ではできません。残念ながら100%ネットの海に漕ぎ出すことはできません。

バーチャル空間だけでなく、社会参加やネットの向こうの現実世界を旅することも



なんらかの事情でベッドから起き上がることができなくても、ネットを通じて「アバター（自分の代わりのロボット）」を使い社会参加し、世界中の様々な国を旅して、コミニュケーションすることができるようになるでしょう。

4 おわりに

さて、フィクションとして少しだけ、インターネットとデジタルテクノロジーの進化の果てについて語りました。

しかし、これは、実現できない未来ではなく、それぞれの要素はすでに種としてこの世界に存在しています。あとはその種の健やかな成長を待つだけです。

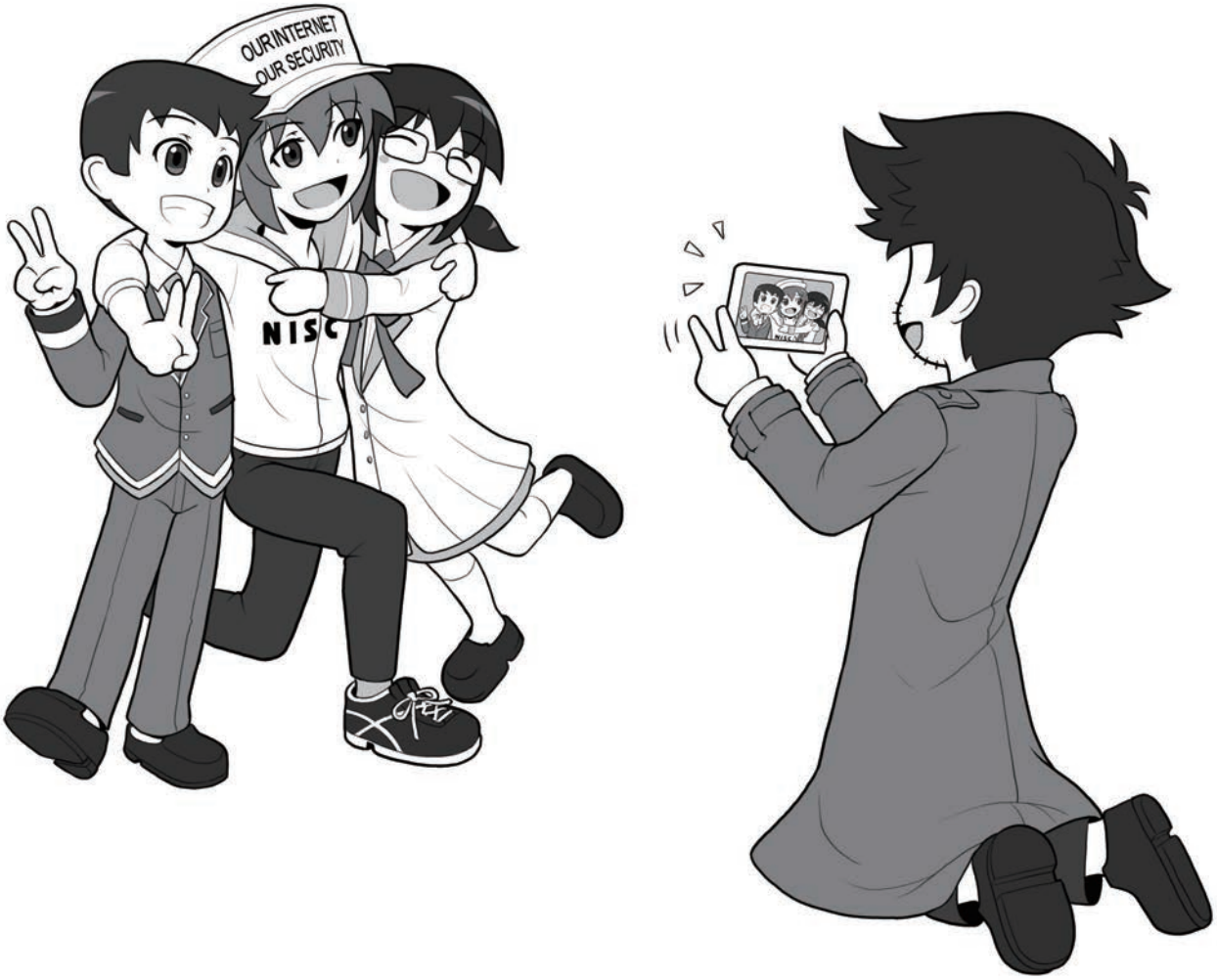
一方、このフィクションには語られなかった部分があります。それは、インターネットに潜む影、攻撃者(≒クラッカー)や悪意のハッカーの存在です。

もし、あなたがネットでショッピングを楽しんでいるときに、悪意のハッカーによる詐欺に遭ったとしたらどう思うでしょう。買い物はもう嫌と思うかも知れません。

インターネットは「距離とその移動に必要だった時間が消失した世界」ですから、悪意あるものは、いつでも何処でも現れて、あなたに悪事を働くかもしれません。

私たちがネットに素晴らしい未来を見いだし、ネットの果てに人としての進化があると思ったとしても、それは安全なネット空間があってこそ実現可能なのです。

古来、人は距離とその移動に消費する時間によって、行動する範囲とその可能性を制限されてきました。ほんの少し前までは、自分



の村から出たことがないという人もたくさんいたのです。しかし、ネットは距離という概念を消失させ、それによって失われていた時間を、あなたの可能性に転化します。羽を得て自由になる。想像するとわくわくしませんか？

それによって生まれる、人間という存在の新たな可能性を見てみたいと思ったならば、ぜひインターネットを安全で安心できる場所にするために、私たちの活動に参加してください。私たちと一緒にネットの未来を守っていきましょう。

さる著名なハッカーが、来たるべき未来に「ネットは広大だわ」という意味深い言葉を残しています。

広大なネットは可能性であると同時に、広大であるが故に政府や関連機関、セキュリティ関係企業だけで守り切ることはできるものではありません。

みなさん、一人ひとりがネットを守る私たちの仲間となって、私たちと共に未来を創ってくれることが必要なのです。

私たちは、みなさんのことを待っていますよ。

可能性の未来でお会いしましょう。

2021年12月
内閣サイバーセキュリティセンター一同

用語集

AES（エー・イー・エス）
暗号化方式の一要素。利用する無線LANの暗号化方式にAESという文字が入っている、WPA-PSK(AES)やWPA2-PSK(AES)という方式は、「暗号キー」を共有しない範囲では安全とされる。また、無線LANに限らずファイルや記憶装置の暗号化方式としても用いられ、数字＋bitで記述される「鍵長」の数字が大きいほど、不正な解読が困難とされる。WPA3はこれ以上の安全性をもつ

BIOSパスワード（バイオス・パスワード）
Windowsマシンなどで電源投入時に、OSが立ち上がる前に入力を求められるパスワード

DDoS攻撃（ディードスこうげき）
Distributed Denial of Service Attack。攻撃者などがゾンビ化した多量のパソコンなどから、攻撃目標に一斉に多量の問合せなどを行い、攻撃対象のサーバなどを反応が追いつかず利用できない状況にする攻撃。何種類かの類型がある

ECサイト（イーシー・サイト）
Electronic Commerceサイト。インターネット上にある商品販売店舗。オンラインショッピングサイト

GPS（ジー・ピー・エス）
Global Positioning System。多数の人工衛星で構成される衛星測位システム。この衛星からの電波を使い計算を行うことで、現在地を測定することができる。主として米国が運用しているが、2018年春より日本版GPS「みちびき」が運用開始

ID（アイ・デイー）
機器やウェブサービスなどを利用するときに、利用者を識別する文字列。「ログインパスワード」とセットで、正統な利用者であることを証明する

IMAP（アイマップ）
Internet Message Access Protocol。メールサーバからメールを受信するための通信上の規格。POPと異なるのは、メールがサーバ上にメールを残した状態で管理できるので、ウェブブラウザがあればどこからでもアクセスできるウェブメールなどで使われることが多い。メールソフトでも利用可能。通常はVer.4のIMAP4が使われる

IoT（アイ・オー・ティー）
Internet of Things.。「モノのインターネット」ともいわれる。コンピュータの入った電子機器をなんでもかんでもネットにつなげてしまおうというイメージの考え方。しかし、IoT機器製造業者がすべてネットワークセキュリティに詳しいとは限らず、攻撃者から見て乗っ取って踏み台にしやすい機器を増やす原因ともなっている

JailBreak（ジェイルブレイク）
AppleのiPhone、iPadなどで規約に反した改造を行い、公式ストアでは認められていないアプリなどをインストールする行為。製造メーカーが設計したセキュリティ思想から逸脱するため、マルウェアへの感染や乗っ取りなどの攻撃に遭う確率が高くなるため、大変危険な行為。やっちゃだめ、絶対

Linux（リナックス）
Windows、macOSとも別の、基本的には「みんなで作る無料のOS」。一般の人も利用可能だが、サーバや工業機器やIoT機器など、あまりコンピュータであることを意識しない電子機器でよく使われている。様々な種類のLinuxが存在するほか、私たちが普段使っている著名なOSの元になっている場合もある

LTE（エル・ティー・イー）
Long Term Evolution。携帯電話の最近の通信規格。携帯電話回線を提供する会社が個別に名称

をつけている場合もあるが、おもに４Ｇと呼ばれるタイプのものの総称。高速な無線通信回線ネットワークとしてWANと呼ばれることもある。さらに高速な5Gが登場しつつある

microSD（マイクロエスディー）
パソコンやスマホなどで使われる、小型のメモリカード。SDカードの超小型版

NISC（ニスク）
National center of Incident readiness and Strategy for Cybersecurity。→内閣官房内閣サイバーセキュリティセンター。内閣府ではない。

Office製品（オフィスせいひん）
Microsoft Officeなどに代表される、ワープロ、表計算、プレゼン用ソフトなどの総称。

OS（オー・エス）
Operating System。
→オペレーティングシステム

「PINコード」（ピンコード）
狭い意味では、スマホなどを利用するときに打ち込む、暗証番号のようなもの。複数回入力を間違うと明示的な入力遅延や入力画面がロックされるなどの規制がかかるものを指す。間違えすぎると強制的にデータを消去する「ワイプ」機能があるものも。本書では、機器やサービス利用時に、4から6桁以上の数字で打ち込むもので入力ミスでペナルティがあるものとして定義

POP（ポップ）
Post Office Protocol。メールサーバからメールを受信するための通信上の規約。IMAPと異なり、基本的にはメールをメールサーバからダウンロードして管理する。ただし、メールソフトの側で「メールサーバ」に残すという設定をした場合は、複数のメールソフトからダウンロードすることも可能。通常はVer.3のPOP3が使われる

POSレジ（ポスレジ）
Point of Salesレジ。販売した段階でその情報が送信され、集中管理されるシステム。内部にはコンピュータが入っており、ネットに接続されているのでマルウェアに感染する事例もある。IoT機器

RMT（リアル・マネー・トレード）
Real Money Trade。ゲームなどで出現したレアな装備を、現実世界の通貨で売買すること。ゲームの規約違反となっていることもある。また、販売に関して詐欺や様々なトラブルの発生もしている。レア武器は自力で出しましょう

root化（ルートか）
Androidスマホなどで本来提供されていない、機器の管理者権限を奪取する改造。通常インストールできないアプリなどがイントール可能となる。これを行うことはメーカー本来のセキュリティ設計思想を逸脱しサイバー攻撃に弱くなるため、行ってはいけない

SIM（シム）
スマホなどで携帯電話回線を利用するために挿入する小型のカード。電子的なeSIMもある。

SIM認証（シムにんしょう）
公衆無線LANなどで、「暗号キー」を他人と共用しないように、それぞれの利用者によって異なるSIMの情報を使って認証を行う方式

SIMフリー（シムフリー）
スマホなどの端末が、特定の携帯電話会社のSIMだけでなく、どの会社のSIMでも利用できるようになっている状態。逆に使えないように制限されている状態はSIMロックという。ただし、SIMフリー端末であっても、どの会社の回線でも利用可能とは限らない。携帯電話会社が提供している周波数とスマホが使える周波数などが合っている必要がある。

SMS（ショートメッセージ）
Short Message Service。スマホなどで電話番号宛てで送受信できるテキストメッセージ。携帯電話回線契約があればデータ通信契約が無い状

態でも送受信できる。一方、電話番号が無い場合や、データ通信専用SIMでSMSが提供されていない契約では、送受信できない。SMSがオプションとして提供されている場合もある

SNS（エス・エヌ・エス）
Social Networking Service。会員制のサービスで、メッセージのやりとりやブログ風の発信などを行う。アカウントを作らないと閲覧できないものと、アカウントがなくてもウェブブラウザから閲覧できるものなど、様々な形態がある

SSD（エスエスディー）
Solid State Drive。従来パソコンなどで用いられてきた大容量補助記憶装置であるハードディスク（HDD）に代わり、回転や可動部分がなく、半導体メモリだけでこれを代替する機器。HDDより小容量で比較的高価だが高速。→補助記憶装置

SSL（エス・エス・エル）
→SSL/TLS

SSL/TLS
（エス・エス・エル／ティー・エル・エス）
Secure Socket Layer / Transport Layer Security。データを暗号化して送受信する方法で、SSLのほうが古く、これを改訂して進化させたものがTLS。SSLがTLSの元になったこともあり、未だにSSLと呼ばれたり、SSL/TLSと書かれたりするが、古い資料やバージョンを明記しているものを除けば同義の意味と考えていい

SSL証明書
（エス・エス・エルしょうめいしょ）
SSLで通信を行うサーバの身分証明書のようなもの。認証局が審査を行って発行する。最近は審査がいい加減だったり、無料で発行する認証局の登場により、安全であることの目安とはならない状況になりつつある。より審査の厳しいEV-SSL証明書も存在する

Stuxnet（スタックスネット）
イランの核燃料施設を攻撃するために用いられたマルウェア。USBメモリを経由しエアギャップを越えて感染するように設計されている。攻撃するだけであれば、人の手を使いエアギャップを越えることは可能であることを示した例

TKIP（ティーキップ）
Temporal Key Integrity Protocol。暗号化方式の一つだが難しく考えないで、無線LANアクセスポイントの暗号化方式にこの文字が入っていたら、危険と考え利用を避ける

TLS（ティ・エル・エス）
→SSL/TLS

TPM（ティー・ピー・エム）
Trusted Platform Module。パソコンなどの内蔵記憶装置の暗号化を加速するチップ。「暗号キー」を秘匿し、本体が盗難された場合でも解読を困難にする。内蔵記憶装置だけが盗まれた場合は、TPMは本体に残るので「暗号キー」は秘匿され、当然解読がより困難になる

UPnP
（ユニバーサル・プラグ・アンド・プレイ）
Universal Plug and Play。ルータに内蔵されている機能で、家や会社のLAN側にある機器を、難しい設定抜きでインターネット側からアクセス可能にする。LAN内の機器がインターネット側からアクセスされ、「踏み台」にされることもあるので、利用しない方が安全

URL（ユー・アール・エル）
インターネットのウェブサイトの住所を示す文字列

USB（ユー・エス・ビー）
Universal Serial Bus。パソコンなどに周辺機器を簡単に接続するための規格

USBセキュリティキー（ユー・エス・ビー・せきゅりてぃ・キー）
USB端子に接続して、機器やウェブサービスの正統な利用者であることを証明する物理的な鍵

の役割を果たすもの。NFC、Bluetoothに対応しているものもある

USBチャージャー（ユー・エス・ビー・チャージャー）
USB経由で機器を充電できるようにするためのもの。AC電源、乾電池や充電池、車の電源ソケットを利用して充電できるものがある

VPN（ブイ・ピー・エヌ）
Virtual Private Network。仮想プライベートネットワーク。業務用としてはインターネットを利用しながらセキュリティを守りつつ、独立したネットワーク間をLANのように接続する。一般の利用者用には、自分の機器からインターネット上の安全とされる出口サーバまでの区間の通信をすべてまるっと暗号化するサービス

WAN（ワン）
Wide Area Network。LANと対になる言葉で、広域な無線通信回線ネットワークを指す。LTE（4G）やWiMAXがこれに含まれる

WEP（ウェップ）
Wired Equivalent Privacy。暗号化方式の一つだが、容易に解読可能で安全ではない。無線LANアクセスポイントの暗号化方式にこの文字が入っていたら危険と考え利用を絶対に避ける

Wi-Fi（ワイ・ファイ）
→無線LAN

Wi-Fiルータ（ワイ・ファイ・ルータ）
→ルータ

WPA（ダブリュー・ピー・エー）
Wi-Fi Protected Access。無線LANの暗号化方式の一つで、WPA-PSK(AES)と書かれたもので、「暗号キー」を他人と共有しない限り安全。一方TKIPと入っていれば利用を避ける。公衆無線LANでこの方式を採用している場合は、「暗号キー」を他人と共有する場合もあるので注意

WPA2（ダブリュー・ピー・エー・ツー）
Wi-Fi Protected Access 2。WPAをより強力にしたもので、AESが標準となった。「暗号キー」を他人と共有しない範囲では、安全とされている。もしTKIPと入っているものがあれば利用は避ける。公衆無線LANでこの方式を採用している場合、「暗号キー」を他人と共有する場合は危険

WPA3（ダブリュー・ピー・エー・スリー）
Wi-Fi Protected Access 3。WPA2で近年発見された特殊な脆弱性や、そのほか無線LANにまつわる問題点の多くを解消する暗号化方式

アオリ行為
SNSやブログなどを使って、他人の発言を取り上げ、批判的なコメントをして「炎上」状態にしようとすること

アクセスポイント
無線LANで通信するために、使用している機器を接続する先、およびその機器

アクティベーションコード
ソフトウェアをインストールしたり、コンビニなどで売っている、音楽サービスやゲームなどへのチャージカードを、利用可能にするために用いる。認証処理をするために入力時に機器がネットに接続されている必要がある場合もある。

アタッカー
→攻撃者

アップデート
セキュリティ改善要素が含まれているかどうかは関係なく、ソフトウェアやアプリの更新

アップデートファイル
アップデートを行うためのインストールファイル

アバター
ゲームやSNSなどで自分の代わりの役割を担う仮想のキャラクター。あるいは現実世界で代理をになうロボット

アプリ
パソコンやスマホなどで、なんらかの機能を実現するプログラム。おもにスマホで使われ、一部パソコンでも使われている名称

アプリ連携
複数のアプリ間で機能を連携すること。カメラアプリにSNSアプリの投稿機能を連携し、カメラアプリから直接写真付き投稿を行えるようにするなど。権限を渡すことになるので、攻撃者のサイバー攻撃の手口になるため利用は非推奨

アンインストール
インストールしてあるプログラムやアプリを機器から削除すること

暗号化
文章などを正統な利用者以外が通常の手段では読めないように加工すること

暗号化キー
暗号化と復号のために利用する鍵となる文字列。短く複雑でない暗号化キーは総当たりによって探り当てられやすい。また、なんらかの理由で流出したり、意図せず共有すると、キーを入手したものによって暗号化した内容が復号される。本書では、「暗号キー」という

暗号化チップ
暗号化をより高速に行うための、専用のチップ。≒TPM

暗号化方式
暗号化の方式。一部の古い方式では、「暗号キー」がなくても解読できるものもある。暗号化するときには利用する暗号化方式の安全性に注意が必要

暗号化メディア
暗号化されたメディア。SSDやHDD、USBメモリなどのメディアを暗号化する

「暗号キー」
本書では、暗号化と復号に使う鍵の名称として定義

インストール
プログラムやアプリを、スマホやパソコンに導入し、使える状態にすること

インターネットバンキング
インターネットを使って銀行の取引を行うサービス

インターフェース
パソコンやスマホを利用するための操作画面や操作方法

ウイルス定義ファイル
セキュリティソフトがマルウェアを検出するための定義情報が入ったファイル。実世界でいえば顔写真付きの手配書のようなもの

ウェブサーバ
ネット上でウェブサイトを表示するためのサーバ

ウェブブラウザ
ネット上で公開されているウェブサーバを閲覧するためのソフトウェアやアプリ

オフラインアタック
攻撃者が暗号化されたデータなどを入手し、入力制限がない環境で解読攻撃を行うもの。おもにネットに接続しないでできる攻撃なので、オフラインという。＝オフライン攻撃

オペレーティングシステム
パソコンやスマホの機器の上で動作し、利用者に操作用のインターフェースを提供するソフトウェア。Windowsパソコンの Windows。Apple社パソコンの mac OS、Androidスマホの Android OS、iPhoneの iOSなど

オレオレ証明書
通信の暗号化に際し本来認証局に申請して発行してもらう証明書を、勝手に発行して暗号化通信に利用するもの。この証明書を利用しているウェブサイトにウェブブラウザでアクセスすると、警告が表示される。接続してはいけない

オンラインアタック
攻撃者がウェブサービスなどに、不正にログインを試みる攻撃など。ネットを経由した攻撃が主なのでオンラインという。＝オンライン攻撃

オンラインストレージ
ネット上に存在するデータ保管用のサーバ

記憶装置
コンピュータ内部や、外部バスに接続され、データを保存する装置。ハードディスクやSSD

ギブアンドテイク
ソーシャルエンジニアリングの手法で、相手になにかのメリットを与えることで、その代償として自分の目的の情報を引き出す手法

クラウドサーバ
インターネット上に存在する、データなどを保存しておくサーバ。おもに「機器の記憶装置と同等に利用できる」「特別なサービスを利用している意識はないが使えている」「でもどこにあるかわからない」雲のような存在感からCloudと呼ばれる。これに対して転送を意識して使用するものは「オンラインストレージ」と呼ばれやすい。スマホなどでは、設定をよく確認しないと、知らないうちに、写真などのバックアップに使ってしまっていることもあるので注意

クラッキング
攻撃者が他者のアカウントや機器、サーバなどに不正に侵入すること。セキュリティを割って入るの「割る」のCrackから来ており、クラッキングを行う攻撃者をクラッカーとも呼ぶ

検体
セキュリティ会社などがセキュリティソフトでマルウェアを排除できるように、そのマルウェアを解析するための実物のサンプル

攻撃者
悪意を持ってサイバー攻撃やそれに付随する攻撃を行うもの。悪意のハッカー。ブラックハットハッカー。本書では、「ハッカー」そのものは悪意があるかどうかとは関係がないので、特に攻撃を行うものとして「攻撃者」とする。＝アタッカー。≒クラッカー

虹彩
目の中にある円盤状の膜で、人によって違っており、生体認証の要素として使われる

公衆無線LAN
街中や店舗などで、不特定多数に対して インターネット接続環境を提供する無線LANのこと

サービス連携
パソコンなどを使って複数のサービスの間で連携をすることをサービス連携と呼ぶ。その中で特にスマホ上でアプリによって連携をすることをアプリ連携と呼ぶ場合があるが、内容は同じ

辞書攻撃
「ログインパスワード」などによく使われる文字列を集めて辞書化したものを使い、不正に他人のアカウントにログインできないかを試みる攻撃

侵入テスト
会社や組織のネットワークに、外部から不正侵入することができないか行うテスト。ペネトレーションテストともいう

スタンドアロン
ネットワーク（つながっていること）と対になって使われる言葉で、ネットワークにつながっておらず単独で存在すること。ただし、ネットにつながっていて、かつほかの機能や機器と連携しないで動作する場合もスタンドアロンと表現することもある

ステルス状態
パソコンなどが起動していないように見えて、実際は動作している状態

スパムメール
元々はインターネットの初期、不特定多数に対して多量に送られてきた広告メールなどの迷惑メールを指した。攻撃者がこの方法を用いてマルウェア感染などを狙う攻撃をしたり、詐欺サイトに誘導するフィッシングメールなどに利用することもある。この場合はスパムメールでありフィッシングメールでもあることになる。サイバー攻撃に用いられる場合は、特定の誰かを狙った少量の「標的型攻撃（標的型メール）」に対して不特定多数を狙うため「ばらまき型攻撃」と呼ばれることもある

スマートウォッチ
スマホと連動したり、単独でネットに接続してなんらかの情報をやり取りできる腕時計型の機器

スマート家電
単独でネットに接続して、なんらかの情報をやり取りしたり、動作の指示を受け付けられる家電機器。IoT機器

セキュリティアプリ
スマホなどのセキュリティを確保することに貢献するアプリ

セキュリティホール
パソコンやスマホのシステム上、攻撃者が不正な侵入などを行える状態になっているプログラム上の「穴」のこと

セキュリティキー
→「暗号キー」

セキュリティソフト
パソコンなどのセキュリティを確保することに貢献するソフトウェア

セキュリティパック
パソコンやスマホなどのセキュリティを向上するために、複数の機能がパッケージになって携帯電話キャリアなどから提供されているもの

セキュリティパッチ
パソコンやスマホのシステム上に開いた、セキュリティの「穴」を塞ぐために、メーカーなどから提供される修正プログラム。パッチワークのパッチから来ている

ゼロデイ攻撃
セキュリティホールが公になってから、メーカーなどがその穴を塞ぐための修正プログラムを提供するまでの期間に行われる攻撃。この期間に攻撃を受けると、防ぐ手段はないため、利用者自身が「避ける手段」を講じる必要がある

総当たり攻撃
攻撃者が「ログインパスワード」や「暗号キー」を破るために、すべての文字などの組み合わせを試す攻撃

ソーシャルエンジニアリング
対人（アナログ）、サイバーを問わず、人間の心の隙を突き、相手に自らの望むような行動をさせるテクニック。対人の代表的な例が「オレオレ詐欺」などの特殊詐欺、サイバーの代表的な例が「標的型メール」やBECなど

ソーシャルログイン
特定のSNSやウェブサービスのIDを使って、ほかのSNSやウェブサービスにログインし利用可能にする規格。特定の身分証明書で、ほかのサービスを利用できるイメージ。新しいサービスを利用するためにいちからアカウントを作る手間を省くことができる。OpenIDとほぼ同義だが、ほかにもソーシャルログインに見える機能は存在する。鍵となるアカウント情報が流出すると連鎖的に乗っ取られるため、本書では、非推奨

ソース
「情報ソース」の意味で、発信された情報の発信元。

発生した事象そのものを明確に見たり聞いたり体験した上で発信しているものを一次ソースという。伝聞などで発信しているものを二次ソース、三次ソースと呼び、次第に信憑性が低くなったり、本来の意味とは別の意味で使われている可能性が高くなる

ソフト
ソフトウェア(≒プログラム)の略。対になる言葉は機器を意味するハード(ハードウェア)

ソフトウェアトークン
二段階認証などで使われる使い捨てパスワード(ワンタイムパスワード)を出力するトークンを、ソフトウェアで実現しているもの。例えば、ソフトウェアトークンを出力するスマホ用アプリ

多要素認証
サービス利用時に行う利用者認証を、3つの要素(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)のうち、2つ以上の要素を用いて行うもの。3つの要素すべてを使う場合などもあり得る

チート行為
ゲームなどで本来認められた方法では、なく不正な方法によるプレイ。また、はそれによって利益を得る行為

通知ウインドウ
パソコンなどで、なんらかの通知を出す表示のこと

通知機能
エラー発生、メール受信、そのほかのアラートなどを利用者に通知する機能

使い捨てパスワード
二段階認証などで用いられる、利用するたびに更新されるパスワード。ワンタイムパスワード

ディクショナリアタック
→辞書攻撃

データローミング
ローミングに関して、データ通信のローミングを行うこと

テザリング
パソコンなどで、スマホなどを経由してインターネット接続をする方法。スマホをルータとして利用する方法など

デジタルイミグラント
現実世界からデジタル世界に、移民のようにその生活の一部を移し、これを使いこなす世代。おもにパソコンが普及していない時代に生まれた人が多い

デジタルネイティブ
生まれた時代に既に十分にネットが普及しており、現実世界とデジタル世界を垣根なく一体に使いこなす世代

ドライブバイダウンロード攻撃
いずれかのウェブサイトを訪れただけで、なんらかのプログラム(この場合はマルウェア)のインストールが発生する攻撃

トラッシング
ゴミ箱に捨てられた紙などから重要な情報を探し出すソーシャルエンジニアリングのテクニック

内閣サイバーセキュリティセンター
正式名称は「内閣官房内閣サイバーセキュリティセンター」。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。国民への情報セキュリティ意識の啓発も行う。通称NISC。なお、内閣府と内閣官房は違う組織ですってば。おーぼーえーてー！

二段階認証
利用者認証を2回に分けて行うもの。多要素認証と異なり、同じ認証の要素で2つの段階に分けて認証する場合もそう呼ぶ。一方、異なる要素を組み合わせて2回認証を行う場合は二要素認証とも呼ぶ。同じ要素2回よりは異なる要素2回の方がセキュリティレベルは高くなる

認証局
申請に基づきSSL証明書の発行を審査する機関

ネームドロップ
業務上の上司や立場が上の人間を装って要求を実行させるソーシャルエンジニアリングの手法

ネチズン
ネットをよく利用する人物を指す、国内ではやや古い呼称。ネットワーク市民(Network Citizen)の略

ネットワーク暗証番号
通信事業者のサービスを利用する際に、利用者が本人であることを認証するための暗証番号

ネットワークカメラ
おもに、ネットワーク上に設置された監視カメラ。セキュリティ上は、おもにインターネット上から直接存在が見えるものを指し、サイバー攻撃の対象となりやすい。IPカメラとも呼ばれる。IoT機器

ネットワークキー
無線LANでアクセスポイントへの接続や通信の暗号化に使われる鍵。本書では、「暗号キー」に分類している

ネットワークルータ
家庭内や会社内のLANをインターネットに接続するための窓口的役割を担う機器。無線LAN機能を内蔵している場合は「無線LANネットワークルータ」「無線LANアクセスルータ」と呼ばれる

野良Wi-Fi
野良猫のように誰が飼い主か分からない無線LANアクセスポイント。おもに、暗号化されておらず誰でも利用できる状態になっているもの。暗号化されていない時代に設置されてそのままのものもあるが、攻撃者が情報を詐取するために設置しているものもある。災害時や観光目的に、運営主体がはっきりして設置される暗号化無しの無線LANアクセスポイントは別

バージョンアップ
アップデートファイルなどを適用して、ソフトウェアやアプリのバージョンが向上すること。セキュリティ関係の更新が含まれることもあり、積極的に適用するべきもの

バーチャル空間
仮想空間とも呼び、おもに3Dなどで利用可能なネット上の世界。ゲームなどが現在の主流。VRメガネなどを利用するもののほか、通常のモニターで見るものを指す場合もある

バーチャルリアリティ
仮想空間をあたかも現実世界のように感じさせる技術

ハードウェアトークン
二段階認証などで用いられる使い捨てパスワードを、専用の物理機器として提供するもの

パスコード
一部のアプリなどでPINコードと同じ役割をするものを指す言葉

パスワード
利用しようとしている人が、その機器やサービスの正規の利用者であることを証明する、合い言葉のような文字列

パスワードリスト攻撃
→リスト型攻撃

パターンロック
スマホをロック解除するときに、画面上に表示される複数の点を、あらかじめ登録したパターンでなぞり、ロックを解除する機能

バックアップ
パソコンやスマホの情報を別途保存しておき、機器が故障したり紛失や盗難したりした場合に、復元するためのもの。機器の情報の一括バックアップと、目的のデータ毎のバックアップがある

バックドア
機器やシステムに設けられた、正規のログイン方法ではないアクセス方法。攻撃者がシステムに侵入して、再度侵入するために不正に設置する場合や、システム開発者や管理者が管理の手間を省くために設置し、正規のリリース後をそれをわざと残したり忘れたりしている場合も

パッチ
≒セキュリティパッチ

パラメータ
機器やソフトウェアの設定上の要素

ハリーアップ
ソーシャルエンジニアリングの手法で、相手を急かすことで正常な判断をできなくなるようにして、目的の要求を通すこと

秘密の質問
ウェブサービスなどでパスワードを忘れてしまい、再度パスワードを設定し直すときなどに本人である確認をするため、あらかじめ設定しておく質問。ただし、質問はサービス側が用意したものがほとんどで内容も個人情報にまつわるものが多いため、正直に答えているとSNSなどで探し当てられることも

ヒューミント
スパイの諜報活動で、ターゲットの交友関係を調査すること

ヒューリスティック分析
手配書方式のマルウェア検知方法を避ける攻撃が普及してきたため、マルウェアのプログラム上の特徴ではなく、マルウェアの挙動によって判断する方法。別称「ふるまい検知」

標的型メール
攻撃者がターゲットを定めて、マルウェアなどに感染させるために、個人宛のフィッシングメールを送り付けてくる攻撃。ターゲットの名前だけでなく、業務上のメールと見分けがつかない内容や、場合によっては業務上のつきあいがある人間の名前、あるいはその人間のメールソフトを乗っ取って送られてくることもある

ファームウェア
利用する機器のソフトウェアやアプリではなく、機器自身を動かすプログラム。ソフトウェアやアプリだけでなく、更新されたら必ずアップデートしなければならないもの

ファームウェアパスワード
パソコンの電源投入時に入力を求められるパスワードの名称の一つ。これを入力しないと、そもそも起動することができない。「起動パスワード」

ファイアウォール
パソコンなどのネット接続部に存在するプログラムで、内部から外部へのアクセスは通し、外部からの不正なアクセスを防ぐ壁の役割をする。また、企業などでは専用の機器として存在する

フィッシングメール
攻撃者がターゲットから、お金につながる情報や個人情報を盗み取るための詐欺メール。フィッシング(phishing)は洗練された(sophisticated)＋釣る(fishing)から来ている。嘘の情報を餌にして釣り上げるというイメージ

フィルタリングサービス
青少年がネットにアクセスするに当たって、不適切なウェブサイトを閲覧しないようにするサービス

復号
暗号化されたデータを、暗号キーを使って元に戻すこと

不正アクセス通知
利用しているウェブサービスなどに、不正なアクセスが試みられると、スマホなどに通知が送信されてくるサービス

踏み台
攻撃者がサイバー攻撃を行う際、正体を隠すためにコントロール下においたパソコンなどを一旦経由すること。≒ゾンビ化

フライトモード
スマホなどを飛行機で移動中に使えるように、外部に電波を発しない状態にするモード。それに伴い電池の消費が少なくなるので、災害時の省電力モードとしても利用できる

ブラウザ
→ウェブブラウザ

ブラウザ版
SNSなどで、アプリではなくウェブブラウザを使ってアクセスするために提供されているもの

フリーメール
無料で提供されるメールサービス。広告などが表示されるか、利用者の利用情報を提供する代わりに無料で利用できる

フレンドシップ
ソーシャルエンジニアリングのテクニック。友情を持って接することで要求を断りにくくする

プロダクトキー
OSなどをインストールするときに、正統な利用者であることを証明するための文字列。パソコンにインストールされた状態で販売されるものは本体にシールで貼ってあり、店頭などで単体で販売される場合はパッケージ内部に封入されている。紛失すると再インストールすることができなくなる

プロバイダ
インターネットの接続環境を提供する企業。インターネット回線と提供する企業が同一の場合と、別々の場合がある

ベンダー
ソフトウェアやハードウェアなどの製品を販売する企業

ポート
パソコンやスマホがネットを通じて相手とデータを送受信するための窓口。それぞれに数字が振られ、これを「ポート番号」という。また、送信するものを「送信ポート」、受信するものを「受信ポート」と呼ぶ

ホームページ
→ウェブサイト

補助記憶装置
→記憶装置

ボット
ロボット(robot)の短縮形。様々な作業を自動化したプログラムのことでTwitterで自動的に呟くものが有名。「悪意のボット」となると、パソコンやIoT機器などを乗っ取ってゾンビ化するためのプログラムを指す

ボットネット
悪意のボットにコントロールされた機器で構成される集合体。パソコン、スマホ、IoT機器などが、コントロール用のサーバによって管理され、DDoS攻撃などに利用される

マネタイズ
なんらかの手段で得たモノや情報、システムをお金に換えたり、それを用いて稼いだりすること

マルウェア
攻撃者が目的とする機器を攻撃するために利用する不正なプログラム

マルバタイジング
マルウェアを含んだ広告を用いるサイバー攻撃。攻撃者がウェブサイトを閲覧したものを感染させるために広告ネットワークにお金を払って出稿する

水飲み場攻撃
攻撃者が目的とする相手(個人もしくは企業の構

成員など)を、マルウェアに感染させるために、あらかじめ訪問しそうなウェブサイトにマルウェアを仕込んで待つこと。砂漠などで動物が水があるところによってくる様子からつけられている

無線LAN
ネットで用いられる通信に、無線の信号を用いるもの。LANはLocal Area Networkの略で、通常は会社や家など小さい単位で用いる。インターネットとはルータを境にネットワーク的には分離されている(データの行き来は可能)。これに対して広範囲を対象とするネットワークはWAN(Wide Area Network)と呼ぶ

無線LANアクセスポイント
無線LANを利用するために、無線LANアクセスルータによって提供される接続環境、もしくはその機器。本書では環境を指している

無線LANアクセスルータ
無線LANアクセスポイントを提供する機器

無線WAN通信機能
WANとはLANのLocal Area NetworkにするWide Area Networkの意味。通信電波の供給範囲が広いものを指し、おもに携帯電話のLTEなどによる通信ネットワークなどを指す

ランサムウェア
パソコンやスマホなどのファイルを暗号化したりロックしたりして使えなくし、「解除してほしかったら身代金(ransom)を払え」と要求してくるマルウェア

リカバリメディア
あらかじめOSがインストールされたパソコンで、不具合が起きたときのOS再インストールのため、購入後作成するべきインストール用のメディア

リスト型攻撃
ウェブサービスなどから流出したパスワードのリストなどを使って、ほかのサービスでログインを試みる攻撃

リモートワイプ
遠隔操作でスマホやパソコンの中身を消去すること

ルータ
インターネットなどを利用するために利用者が接続・経由する機器。会社や家庭で利用する無線LANアクセスルータのほか、高速なWANの回線を利用して、おもに屋外などでノートパソコンなどを接続して利用するモバイルルータがある。また、有線だけで利用する有線ルータもある

ローミング
携帯電話などで、回線提供会社と個別の契約を結ばないで、ほかの会社の契約をもって音声通話を利用すること

ログ
その機器で行われた活動を記録したデータ。通信に関するものは「通信ログ」という

ログアウト
機器やサービスの利用している状態を終了すること。ウェブサービスの場合、利用していたウェブブラウザを終了してもログイン状態は継続される場合があるので、明示的にログアウトの操作をする必要がある

ログイン
機器やサービスに接続し、パスワードなどを入れることで利用できる状態にすること

「ログインパスワード」
本書では機器やサービスを利用状態にするために入力するパスワードとして定義

ロック
攻撃者による不正なログインなどが試みられ、機器やウェブサービスへログインできなくなった状態。自分の意志でその状態にすることもある。ロックをした画面をロック画面という

索引

ま行

ら行

下記の商標・登録商標をはじめ、本ハンドブックに記載されている会社名、システム名、製品名は一般に各社の商標または登録商標です。
なお、本ハンドブックでは文中にて、TM、®は明記しておりません。

Adobe、Acrobat、Adobe Reader、Adobe Flash PlayerはAdobe Systems Inc.の米国およびその他の国における商標または登録商標です。
Firefoxは、Mozilla Foundationの米国およびその他の国における商標または登録商標です。
Google、Android、Google Chromeは米国Google Inc.の米国およびその他の国における商標または登録商標です。
iOSは、Apple Inc.の米国およびその他の国における商標または登録商標であり、ライセンスに基づき使用されています。
Linuxは、Linus Torvalds氏の米国およびその他の国における商標または登録商標です。
MacおよびmacOS、Safariは、Apple Inc.の米国および他の国における商標または登録商標です。
Microsoft、Office、Word、Excel、PowerPointおよびWindowsは米国Microsoft Corporationの米国およびその他の国における商標または登録商標です。
OracleとJavaは、Oracle Corporation およびその子会社、関連会社の米国およびその他の国における商標または登録商標です。

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「みんなでしっかりサイバーセキュリティ」：https://www.nisc.go.jp/security-site/index.html
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Twitter: @cas_nisc
内閣サイバー（注意・警戒情報）Twitter:@nisc_forecast
内閣サイバーセキュリティセンター NISC LINE公式アカウント：@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

2019年1月18日　Ver 4.00発行
2019年3月5日　Ver 4.01発行 (誇示脱字修正、用語表記統一修正)
2019年3月18日　Ver.4.02発行 (配色ミス修正、誤字脱字修正、レイアウト統一修正)
2019年3月20日　Ver.4.03発行 (誤字脱字修正)
2020年3月31日　Ver.4.10発行
2021年12月31日　Ver.4.20発行

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　総務省　経済産業省　独立行政法人情報処理推進機構(IPA)

インターネットの安全・安心ハンドブック（旧情報セキュリティハンドブック）は、サイバーセキュリティ普及・啓発に利用する限りにおいては多様な形でご活用いただけます。
著作権は内閣サイバーセキュリティセンターが保有しますので、利用に際しては著作権者を表示してください。
クリエイティブコモンズライセンス 表示 - 非営利 - 継承 4.0 国際 (CC BY-NC-SA 4.0)
また、その際は、内閣サイバーセキュリティセンターウェブサイトのご意見・ご感想のページ（https://www.nisc.go.jp/mail.html）からご一報願います。

【活用例】
■ PDF・コピー・製本の無料配布または印刷および作業実費での販売
■ ページ単位・イラスト単位での利用
■ 分割しての配布、必要部分だけを抜粋して配布
■ 自団体のウェブサイトにリンクを設置
■ 表紙に使用する団体名を入れて利用
■ 自団体のセキュリティ資料と合本して配布

Copyright © 2021 National center of Incident readiness and Strategy for Cybersecurity.