小さな中小企業と NPO 向け

情報セキュリティハンドブック

内閣サイバーセキュリティセンター（NISC）

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

協力
総務省　経済産業省　中小企業庁　IPA 独立行政法人 情報処理推進機構

Ver 1.10

小さな中小企業とNPO向け

情報セキュリティハンドブック

内閣サイバーセキュリティセンター（NISC）

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

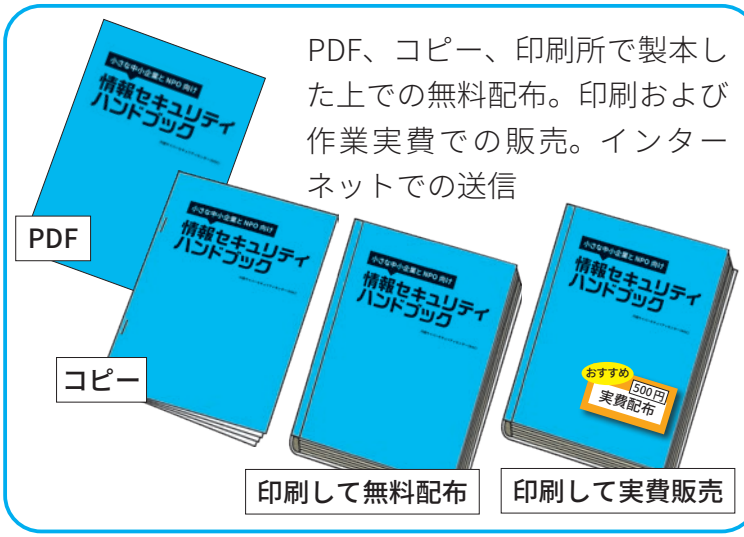
協力
総務省　経済産業省　中小企業庁　IPA 独立行政法人 情報処理推進機構

Ver 1.10

「情報セキュリティハンドブック」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けます。

※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。インターネットでの送信

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用サイトのリンクを設置※

社名団体名を表紙に入れて利用

自社や団体のセキュリティ資料と合体しての配布

※ダウンロード用ウェブサイト URL https://www.nisc.go.jp/security-site/blue_handbook/index.html

情報セキュリティハンドブックの活用法

● 会社・団体の研修で

「情報セキュリティハンドブック」は、まず「サイバーセキュリティってなに？」と思われる方々の基礎知識習得の教材として、研修などで使っていただきたいと思います。

「個人」と「セキュリティ部署のある企業や団体」の中間に位置するみなさんに、その両面から知っておいていただきたいことをこの1冊にまとめてあります。

まずは目を通して、セキュリティ全体の地図を描き、できるところから取り組んでみて下さい。

● サイバーセキュリティ知識の向上に

基礎的な知識を習得できたら、本書の後半には、サイバーセキュリティの知識を深めるためのセクションをもうけています。

守るべき項目を知るだけでなく、なぜ守らなければならないかを深く理解することができます。

姉妹書として、ご家庭やお子様向けに「インターネットの安全・安心ハンドブック」もご用意していますので、ご活用ください。

● IT技術を生かしてセキュリティコストを捻出

また、災害時の対応や、IT技術を生かしてセキュリティコストを捻出するための、いくつかのアイデアを掲載しています。インターネット時代の特性を生かして、フットワーク軽く活躍していただきたいと思います。

会社・団体の研修で

P15「プロローグ．サイバー攻撃ってなに？」

P21「第1章．まずは情報セキュリティの基礎を固めよう」

P45「第2章．パソコン・スマホ・IoT機器のより進んだ使い方やトラブルの対処の仕方を知ろう」

P65「第3章．被害に遭わないために、加害者にならないために」

サイバーセキュリティ知識の向上に

P113「第6章．セキュリティをより深く理解してインターネットを安全に使う」

姉妹書「インターネットの安全・安心ハンドブック」

IT技術を生かしてセキュリティコストを捻出

P87「第4章．会社を守る、災害に備える、海外での心構え」

P99「第5章．ITを使った効率化によるセキュリティコスト捻出」

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、さまざまな専門誌や最新の記事にチャレンジしていただけると幸いです。

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

前書き

サイバーセキュリティは全員参加!セキュリティは「公衆衛生」の時代に

小さな中小企業、そしてNPOのみなさん、こんにちは。

この本はサイバーセキュリティにあまり詳しくない、個人として事業を営む方、セキュリティ担当者のいない小さな会社、任意団体、非理営利団体(NPO)の方に向けて作りました。

突然ですがみなさん、「インターネット」ってなんだと思いますか？

「一昔前は郵便やファックスで書類を送っていたのが、メールやメッセージを使って一瞬で相手に届けられるようになった」「昔は高かった国際電話が、無料でかけられるようになった」

そんな便利な道具のイメージですか？いえいえ。インターネットはそんな「便利な道具」のような存在ではありません。

インターネットとは、デジタル化できるものに限るという条件付きではありますが、「距離とその移動に必要だった時間が消え、そのためにかかっていたお金(コスト)が必要ない」、現実世界とは異なる新しい世界なのです。

今、私たちは距離の概念がある物理的な世界と、距離の概念が無いインターネットの世界が重なり合ったところに生きています。

では距離の概念が無いことはどういうメリットを生むのでしょう。先ほどの話のように、相手が世界中のどこにいても一瞬で連絡を取ることができます。連絡だけではなく、デジタル化できるものであれば、情報でも写真でも動画でも、さまざまな形で相手とつながることもできます。

一方デメリットとしては、実は多くの面で私たちを守ってくれていた「距離」の壁がなくなり、インターネットにまつわるありとあらゆるトラブルや、世界中に散らばる悪意の人々が、私たちのすぐそばにいるようになってしまったことがあげられます。

物理的な世界では、世界のどこかで事件や事故、災害が起こっても、すぐには私たちに影響を及ぼしませんでした。感染力の高い病気でも同じです。国内でも、比較的トラブルの起こりやすい都会ではなく、地方に住んでいれば、さまざまなトラブルに遭うことが少なかったのも事実です。これが距離の壁なのです。

しかし、インターネットの世界には距離の概念は存在しないので、インターネット上のどこかで起こっている災害や、子ども達への魔の手、悪意の人による攻撃、コンピュータウイルスによる感染は、インターネット

を利用するすべての人々が、日常的に直面する問題になりました。

「地方にあるから、小さい会社や団体だから、インターネットを通じた悪意の人たちの攻撃は、自分たちには関係ないよ」

それは「物理的な世界」の考え方で、「インターネットの世界」では通用しない甘い考えなのです。

距離の概念が無い以上、攻撃する側は、インターネット上に存在し、自らを守る意識が薄く攻撃しやすい人や場所から、ただ冷淡に攻撃するだけなのです。

ですから、こういったインターネット経由の攻撃である「サイバー攻撃」を防ぐには、攻撃する側から見て私たちが「攻撃しにくい存在」になる必要があり、そのためにはサイバーセキュリティ意識と知識の向上が不可欠なのです。

本書では「サイバーセキュリティってなに？どこから手を着けていいかわからないよ」という方々向けに、サイバーセキュリティについてなるべく平易な言葉を使って分かりやすく、解説しています。

まずはここからスタートして、一通りの知識を身につけ、その上で、各省庁や外郭団体で提供している、サイバーセキュリティに関する詳しい資料に読み進み、会社や団体を守って下さい。

また、本書ではインターネットを怖がるだけでなく、その「距離の概念が無い」特性をビジネスに上手く活用することで、サイバーセキュリティに対するコストを捻出できるように、仕事の上でのインターネットの効率的な利用の仕方も解説しています。

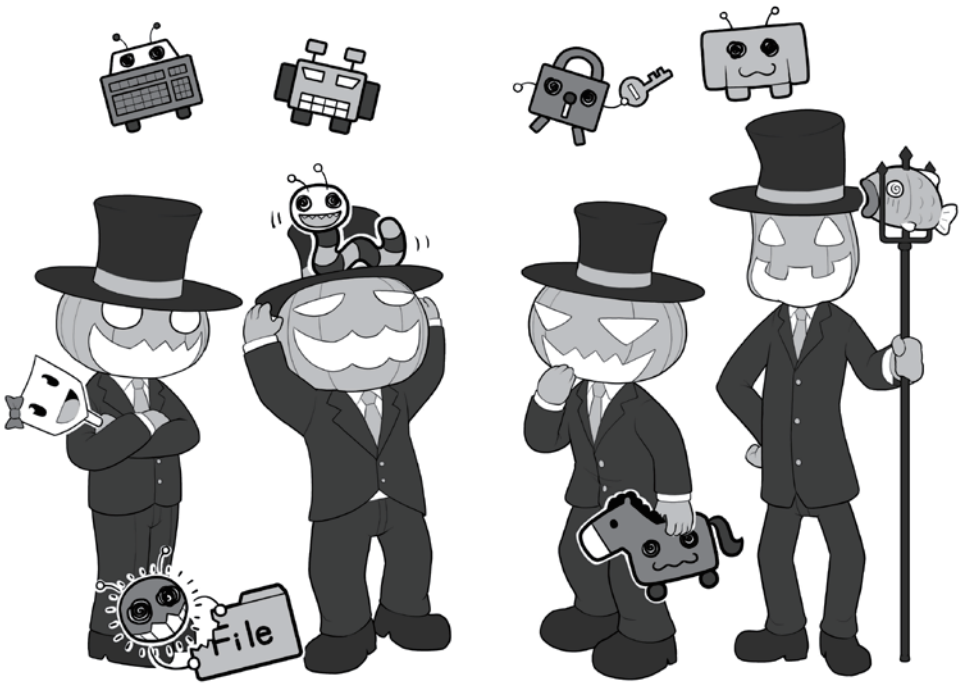
社会が真に衛生的で安全なのは、すべての人たちが「公衆衛生」意識を持ってこれに取り組んでいるからです。

サイバーセキュリティにまつわる社会の安全も、国民全員の意識と正しい知識が深まり、そして「公衆衛生」のレベルまで高められることによって成し遂げられます。

ぜひ全員が手を取りあって、インターネット時代の「公衆衛生」を構築し、安心で安全な新しい世界を作り上げましょう。

みなさんが楽しみながら学んで、より良い成長を遂げる一助となれば、NISCほか本書に協力した各省庁のメンバー一同もうれしく思います。

令和2年3月31日



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

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

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

解説のイラストではその辺りをきちんと書き分けて行きますので、じっくり見て下さいね。

コラム：ハッカーと攻撃者

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、イコール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。

● ホワイトハッカーとブラックハッカー

サイバーセキュリティが専門でない新聞や雑誌、テレビでは、サイバー攻撃を行う悪意の人たちを「ハッカー」と呼びがちです。しかし、この呼び方はやや正確ではありません。

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直接結びつくものではありません。

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「クラッキング」から転じて「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。（本書ではこれらの人を「攻撃者」と呼びます）

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解説しますので、みなさんにもぜひ覚えてもらって、日常の生活でも正しい名称が広く用いられるように協力してくださいね。

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。

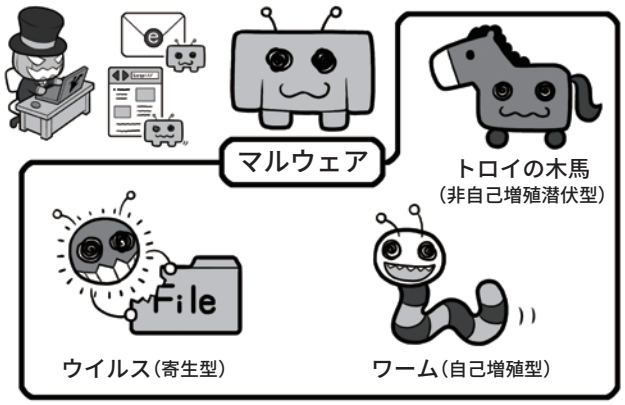
しかし、悪意のプログラムは本来「マルウェア」もしくは「不正なプログラム」と呼ぶのが正しく、「ウイルス」とはその中の一種で、コンピュータ上のファイルが感染し、そのファイルに寄生して活動するタイプのものを指す限定的な名称なのです。

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他にも、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、独立していてかつ自己増殖型の「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。

マルウェアにはどんな種類があるの？



どんな機能を持つの？

これは病原体の行動形態を表す病気の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」といったいい方も存在します。

みなさんには、このことも覚えていただいて、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」と使われているときは、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？

マルウェアの主な機能をあげるとこのようになります。

- **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コンピュータが攻撃者に乗っ取られ、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とき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ます。

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。

「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」

この表現も間違いではありません。しかし、実際には、会社などで使っている無線LAN(Wi-Fi)アクセスルータ、ネットワークプリンタ、監視カメラ、スマートテレビ、ネット接続医療機器、変わったところではPOSレジ、なども感染するそうです。コンピュータではないのになぜ感染するのでしょうか。

この「コンピュータが感染する」と「そう見え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、コンピュータを内蔵している」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ありとあらゆる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。

ただし、こういった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＝修正対応が行われ、たいてい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、所有者をだまして自らインストールさせれば、外から無理矢理侵入せずとも、簡単に悪事を働くことが可能なようにしてしまえるのです。

これを実現するのが後ほど説明する「標的型メール」など、人間の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塞（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。

サイバー攻撃に対するIT機器の防御をいくら固めても、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、さまざまな機器が持ち主の知らぬところで乗っ取られ、攻撃者によるサイバー攻撃に勝手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、ときに加害者の立場に立たされることもありうるのです。

まずは防ぐための知識を得て行動をおこしましょう。

どんなものが感染したり、感染させたり、悪さするようになるのか

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

プロローグ

サイバー攻撃ってなに？

サイバー攻撃と聞いて、どんなことを想像しますか？
誰がやっているの？攻撃されるとどういったことが起こるの？
まずは最初に、サイバー攻撃とはどういったものか、それによってどういった影響が出るのか、知ってください。

1 サイバー攻撃の具体例

1 どんな攻撃があるのか?

サイバー攻撃というと、まるで小説や映画の世界の話かと思っていませんか？実はあなたの会社や団体などの、すごく身近なところでも日常的に起こっていることなのです。

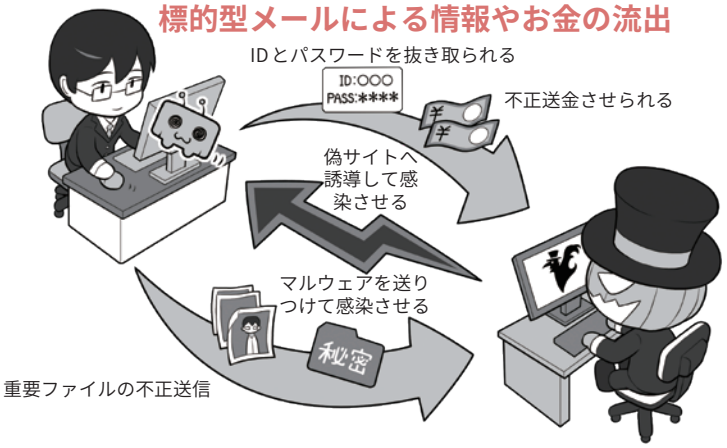
サイバー攻撃として代表的なものは、みなさんが普段業務に使っているパソコンやスマホなどが、マルウェア(他者を攻撃する不正なプログラム。一般的にはコンピュータウイルスとも呼ばれる)に感染し、インターネットを通じて機密情報やお金が、流出させられたり盗まれたりするものがあります。

パソコンなどの脆弱性(弱点。以下セキュリティホール)を突き、知らないうちに感染させるものもありますが、その機器の所有者をだまして悪意の罠に飛び込ませたりするものもあります。例えば、電子メールに悪意のホームページ(以下ウェブサイト)へ誘導するリンクや、添付ファイルに偽装したマルウェアを含ませ開かせるわけです。

メールのリンクや添付ファイルを開いて確認するといった作業は、ビジネスパーソンであれば毎日やっていることであり、そんな行動が、攻撃の糸口につながっているのです。

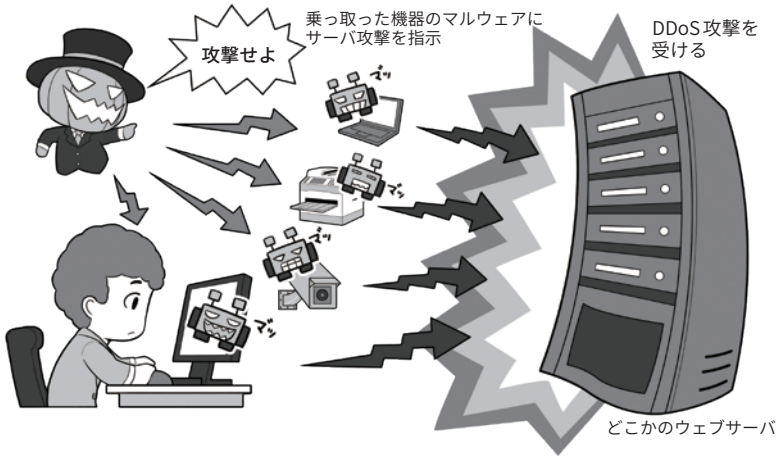
「マルウェアはともかく、リンクで？」と思うかも知れませんが、リンク先を開いてみれば有名銀行のネットバンキングと瓜二つの偽サイトになっていて、IDとパスワードを入力

標的型メールによる情報やお金の流出



攻撃者はあなたから重要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。

パソコン、IoT機器が乗っ取られ攻撃に悪用される



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。

ランサムウェアに感染して業務停止

ランサムウェアに感染すると、パソコンなどのファイルを暗号化され、解除するためには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、実例の記事をさがして学んでみましょう。

させられ、それを使われ会社や団体の口座から不正送金されてしまい、被害に遭うケースも発生しています。

また、会社や団体のパソコンやIoT機器などがマルウェアに感染すると、情報流出だけでなく勝手に操作され、他の会社などへのサイバー攻撃に利用されることもあります。被害者のはずが突然加害者的立場になり、それらの事例が明らかになると社会的信用を失うかもしれません。

パソコンなどのデータを暗号化して読めないようにして、身代金を要求されるマルウェアも急増しています。身代金を払ってもデータが元どおりにならない場合もありますし、業務遂行ができなくなるので、なによりも事前の対策が大切です。

2 会社や団体が狙われるとどうなる?

他にも電子メールが使われる事例としては「BEC（ビジネスメール詐欺）」があります。BECとは、攻撃する相手や環境を事前に良く分析して行われる、企業などを対象としたビジネス用の詐欺メール攻撃です。

実際に報道された事例では、ある航空会社の担当者に航空機のリース料の支払いを求める電子メールが届き、誤って応じて数億円の被害がでたという話がありました。

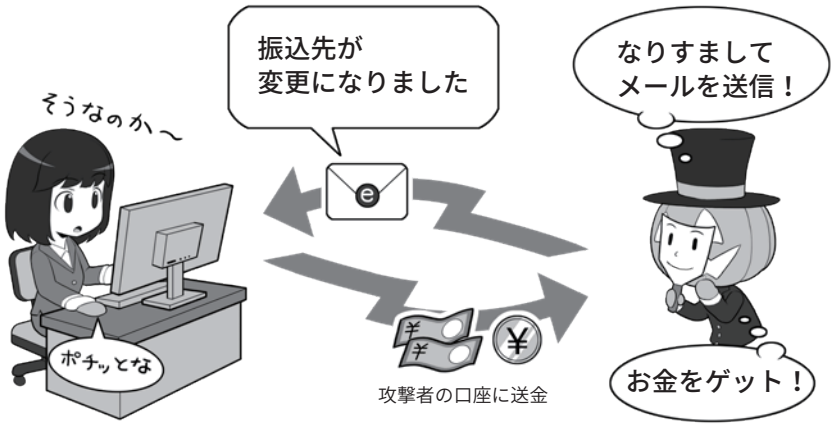
ここまで規模が大きくなくても、事前に支払い関係のメールを盗まれ分析され、取引先を装ったそっくりのメールが届けば、疑わずに振り込んでしまうことも十分に考えられることでしょう。

また、企業には株価に影響を及ぼす社外秘の情報というのは必ず存在しています。悪意を持ったものにとっては、そうした情報は宝の山です。例えばそういった情報を大企業から直接盗めなくても、セキュリティの甘い関連企業があれば、そこから盗んで売ればいいと考えるかもしれません。

そうした特定の会社や団体を標的とした「サイバー攻撃」は、知らない間に所有するパソコンなどに入り込む不正アクセス、既に紹介したBEC、ランサムウェアほかさまざまな手段で襲いかかってきます。

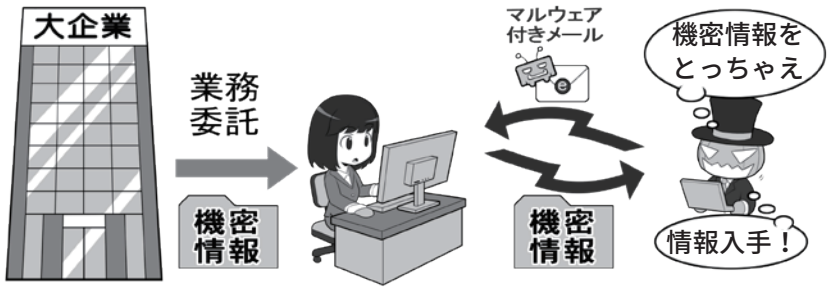
その結果としてデータが漏えいしたら、発注元からは信用のならない取引先と判断されて取引が打ち切られることも十分に想定されます。こういった攻撃から身を守ることは小さな会社やNPOなどにとってまさに死活問題といっても過言ではないでしょう。

取引先のふりをしてメールで送金請求



単純に「お金を送れ」といわれてもだまされる人はいませんが、取引先の企業の人になりすました攻撃者が、通常の請求書発行の業務として口座番号の変更を連絡してきたら、見分けることはできるでしょうか？そういった攻撃を行うために、攻撃者は事前にメールサーバから業務メールを盗み、日常どういったやり取りをしているか、といったことまで下調べた上で攻撃してくることもあります。

取引先の情報流出で業務停止



攻撃者は情報を盗み出そうと思った場合、セキュリティの厳しい大企業よりも、セキュリティの甘い小さな会社を狙った方が簡単と考えます。外注を受けていればしめたものと考えます。

2 誰が攻撃するの?

攻撃者(アタッカー、クラッカー)とはどんな人物なのか

悪意のハッカー

産業スパイ

国家的ハッカー

コスト優先 ← → **目標達成優先**

一口に攻撃者といってもそのカテゴリはいくつかに分かれます。
興味本位、自己顕示欲、腕試し、愉快犯などのアマチュア的な者、一般的な攻撃者(悪意のハッカー)ともいえる金銭目的でビジネスとして攻撃を行っている者、プロフェッショナルで産業的に目的の情報を狙う産業スパイ、そして国家のバックアップを受けながら他国の軍事機密や、政治的な情報を盗み出したり、果てはSNSなどを使って相手国に不利益を与えるプロパガンダなどの工作活動を行う国家的ハッカー(State sponcered hacker)などがいます。
これらは、必ずしも明確に分かれているわけではありません。国家、運営する主体、あるいはスポンサーによって、そのボーダーは曖昧です。
ただ、一般的な悪意のハッカーはビジネスとしてハッキングを行うので、攻撃のコストに対して収入が見あわないほどセキュリティを固めれば避けられやすくなります。
一方、後者二つは「コストは考えず目標の達成が必須」なので、狙われた場合その攻撃を避けるのは困難です。

ここまでで、漠然と悪意を持った者＝攻撃者が存在することがイメージできたと思います。ではその悪意をもった人々は何者なのでしょうか?

まずもっともアマチュア的なものが、子どもの腕試しやスクリプトキディと呼ばれる者です。こういった人物は「自分の力量を試す」「自己顕示欲を満たす」「興味本位」で攻撃を行います。ネットの見えにくいところでサイバー攻撃用のツールが販売されていることもあり、よく考えずにこれらを購入し、違法性を認識せず使う者もいるので侮れません。

次に金銭目的で行動する悪意のハッカーがいます。彼らはマルウェアを開発する能力や、身を隠す能力がありますが、活動は主に「金銭目的」のビジネスであり、仕事にコストパフォーマンス、つまり攻撃に手間をかけずに多く稼げることを望むので、防御のしようがあります。

次に明確に目標を持ち、企業の技術情報などを盗もうと考えている産業スパイ、そして国家へのなんらかの利益を目的として情報機関や軍と一体に動く国家的・軍事的ハッカーやスパイなどがいると考えられます。これらはプロフェッショナルです。

産業スパイであれば、企業が持つ先進技術や製品計画などを盗み、それを自社の製品に生かそうと活動します。軍事的ハッカーであれば兵器開発や戦略に生かせる軍事機器の設計図や軍事計画を狙ったり、誤った情報の拡散で敵対国に混乱を起こします。

これらの者は活動資金を企業や国などのスポンサーが出すために採算度外視で活動し、狙われるとコストの壁で攻撃を避けるのは困難です。

このように攻撃者といっても一様ではなく、愉快犯的な行動から、国の命運を左右する軍事目的まで多種多様なのです。しかし、いずれにしてもしっかりとしたセキュリティ対策が、防御を行うための入口なのはいうまでもありません。

3 どう攻撃されるの？

1 主にマルウェアなどを使って「技術的」に攻撃

では攻撃者は具体的にどう攻撃をしてくるのでしょう。大きく分けると二つの方向性があります。一つは技術的な攻撃、もう一つは心理的な攻撃です。

マルウェアを使ってパソコンやスマホ、あるいはシステム上のセキュリティホールを突く、技術的で「サイバー攻撃」の要素が強いものが前者。「ソーシャルエンジニアリング」と呼ばれ、人間の心の隙を突く詐欺や「心理攻撃」の要素が強いものが後者です。P12の説明もそういう目で見ると少し違ってくるでしょう。

ではまず、起こりうる攻撃の切り口から説明しましょう。

サイバー攻撃の1つ目の例は、自分や自社が攻撃され自らが損害を受けるものです。

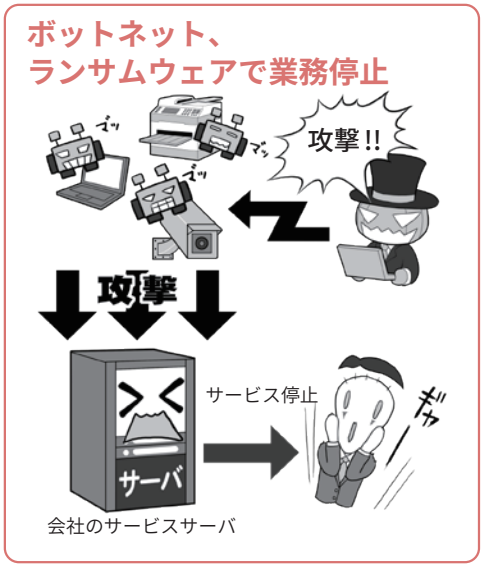
代表的なのはマルウェアによる攻撃です。攻撃者はメールや偽サイトなどにマルウェアを仕込み、利用者が添付ファイルを開いたり、メールのリンクから不正なページを開いたりすると、会社のパソコンがこれに感染し、その結果社内システムに侵入されます。そうなると社内システム用のIDやパスワードが盗まれ、機密情報の流出が発生します。また、これらは乗っ取ったメールアカウントを使って、なりすましのメールが送る攻撃にもつながります。

2つ目は、自分や自社が気付かないうちに攻撃される例です。インターネットでは日々、さまざまなウェブサービスが攻撃されアカウント情報の漏えいが発生しています。例えば個人用のアカウントのIDとパスワードを会社用にも使い回ししていると、どこかのサービスから漏れた情報によって会社のシステムへの不正侵入や不正利用を許すことにつながります。また、業務でインターネット上のクラウドストレージサービスに重要情報を保存していると、ここから情報流出が発生するかもしれません。この例では「自分自身はマルウェアなどに感染した形跡がなくても攻撃される」ことを知って下さい。

3つ目の例は、自社が攻撃されるだけでなく、他者に損害を与える例です。

マルウェアに感染してIT機器が乗っ取られ、他者を攻撃するボットネットに利用されたり、パソコンの中身を暗号化されるランサムウェアで業務遂行ができなくなると、自らが被害に遭うだけでなく、関連する他社にも損失を与えたり、また、店舗などの事業を行っていると、これが停止することで、そのサービスを使っていた利用者にも間接的に経済的損失を与えます。

一方、サイバー攻撃といっても心理的攻撃の性格が強いもの、マルウェアを使わない攻撃もあります。



2 人の心の隙を突き「心理的」に攻撃

さて「サイバー攻撃」ではない一般の犯罪で、みなさんがよく耳にするものはなんしょう。

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」でしょうか。関係機関が日夜注意喚起を行っていますが、未だに多くの方が被害に遭い続けています。

それが終わらない理由は、こういった特殊詐欺が人間が生まれながらにして持っている「心の隙」というセキュリティホールを突いた「心理的攻撃」だからです。人間のセキュリティホールはなかなか埋められず、対策することが難しいからです。そしてサイバー攻撃でも、この人間の心の隙を突いたものが多くあります。

例えば先ほど紹介した、BECの発端になったなりすましの詐欺メール。この攻撃の入口は、相手の心の隙を突き、シンプルに「数行の文字で」だましただけです。

また、送りつける相手をよく調査・分析した上で、送り付けられる偽装ファイルやリンクは、結果的にマルウェアを利用しますが、人間の心の隙を突く手法です。

こういった心理的誘導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意識を向上させるだけでなく、「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険を認識し、予防する「サイバー公衆衛生意識」を広く持つようになることが重要なのです。

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」と呼ばれます。覚えておいてください。

「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

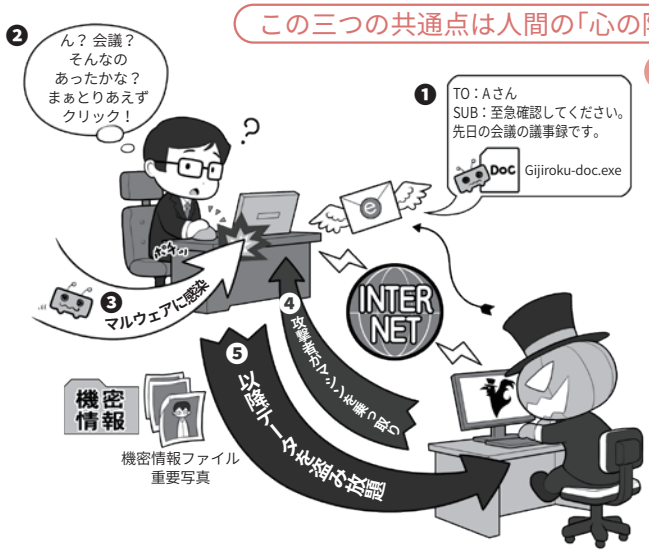
上はビジネス上のソーシャルエンジニアリング、下は振り込め詐欺の例ですが、こうやって見ると、実は2つの詐欺の本質的な部分は同じだと分かります。

これらは上手く人間の心の隙を作り出し、自らの望みどおりに相手を操る体系化されたテクニックなのです。

現実の世界

この三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！」と頭を混乱させ、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して、さらに追い込みます。

こう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（≒心理的交渉テクニック）の、「ハリーアップ」「ネームドロップ」「ギブアンドテイク」などにあたるでしょう。

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、これらの「フレンドシップ」という手法の要素が使われています。

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。その人をだますテクニックを体系化したものが「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。

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

第 1 章

まずは情報セキュリティの基礎を固めよう

サイバー攻撃はどうやって防いだらいいのでしょうか？

政府および関係機関では、セキュリティを固める基礎的指標として、一般国民向けには NISC（内閣サイバーセキュリティセンター）が「情報セキュリティ対策 9 か条」を出しています。一方、企業向けには IPA（情報処理推進機構）が「情報セキュリティ 5 か条」を出しています。

この本をお読みのみなさんは、一般国民とセキュリティ担当者がいる企業の中間に位置しますので、この二つを組み合わせる形でセキュリティを守ることを目標としてみましょう。

0 まずは情報セキュリティの基礎８項目を理解しよう

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

現在、政府系機関が掲げるサイバーセキュリティ対策の指針としては、一般国民向けにNISC（内閣サイバーセキュリティセンター）が「情報セキュリティ対策９か条」を、企業向けにはIPA（独立行政法人 情報処理推進機構）の「情報セキュリティ5か条」を出しています。本ハンドブックはこの中間に位置し、セキュリティ担当者がいない小さな会社やNPO向けに作られているので、この2つを包括する形で８つの基礎的項目にまとめ、解説していきます。

なお、各指針の対比は右頁下の表を参照して下さい。

項目はIPAの指標から見ると３つが加わった形になっています。IPAの指標は対策をはじめる端緒として最も基本的な事項に絞られており、巧妙な攻撃の場合は防ぎきれないこともあるため、それを前提に、また攻撃されたらどうしたら良いか、対策を立てる必要もあるからです。

●情報セキュリティの８項目の概略

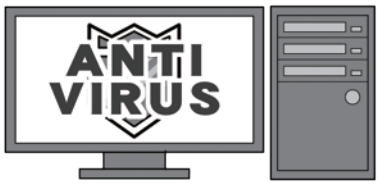
まず**「① OS[*1]やソフトウェアは常に最新の状態にしよう」**とはいわゆるアップデートのことです。

IT機器にはセキュリティホールと呼ばれる弱点が日々見つかっています。一見、大丈夫そうに見えてもそれは「ただセキュリティホールが発見されていない」だけ。OSやソフトウェアメーカーが提供している修正用アップデートを常に適用し続け、

①OSやソフトウェアは常に最新にしよう！

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

②ウイルス対策ソフトを導入しよう！



OSだけで防ぎきれないときの保険として対策ソフトも導入を。

③パスワードを強化しよう！

マルウェアなどによるサイバー攻撃だけでなくて、IDとパスワードを破って正規の利用者のふりをして、パソコンやIT機器を乗っ取ることも可能です。だから、破られないために安易なパスワードは使わず、十分に長くて複雑なものを使いまわしせずに使いましょう。

④共有設定を見直そう！

クラウドストレージサービスにデータを保存するのは便利だけど、共有設定をきちんとしないと、他人からデータや写真が見放題になってしまうのだぞ！

⑤脅威や攻撃の手口を知ろう！

攻撃を防ぐ一番の方法は攻撃者の攻撃方法を知り、それに対策を立てることです。

しかし、その情報は日々新しくなっていくので、OSやソフトをアップデートするように、人の頭の中のセキュリティ知識も、最新攻撃情報を収集してアップデートしていきましょう。

*1 OS: オペーレーティングシステム。パソコンやスマホの基礎的ソフトウェアで、機器の操作画面を提供するもの。各種ソフトウェアやアプリはこの上で動作する。

攻撃の糸口となる穴を塞ぎます。

「②ウイルス対策ソフトを導入しよう！」を実行すると、こういったセキュリティホールを突いてパソコンを乗っ取るマルウェア(≒ウイルス)を検知し、その侵入を防いでくれます。この対策ソフトも、攻撃者の新たな手段に対抗するため、常に更新し続ける必要があります。

「③パスワードを強化しよう！」。IT機器やインターネットサービスの乗っ取りは、マルウェアを使った攻撃に限らず、攻撃者が流出情報などからIDとパスワードを入手し、これを使って行われることもあります。そのため、安全に保管することによって流出による被害を防ぎ、推測しにくいように強化し攻撃を防ぎます。

「④共有設定を見直そう！」は、例えばインターネット上に重要なファイルを保存しておいた場合、これをうっかり誰でも見られる状態にしていると、パスワードによる保護なども効かず、容易に盗まれてしまいます。そういった情報流出を起こさないために、ファイルの共有設定を確認することで情報を守ります。

「⑤脅威や攻撃の手口を知ろう！」とは、攻撃者が常に新たな攻撃手段を開発するのに対抗するため、情報収集を怠らないことです。

●＋3のセキュリティ向上

そして**「⑥常にバックアップを取ろう！」**は、正常な状態のファイルを複製して保管しておくことで、仮に攻撃を許して重要なファイルを失ってしまっても、バックアップから復元することにより、被害を軽減します。

次に**「⑦人間にもセキュリティホールがあることを知ろう！」**で、心理的な弱点を学び、さらに自分だけで対処できないときに**「⑧困ったら各種相談窓口にすぐに相談しよう！」**を実行できるように、IPAなどの相談窓口をあらかじめ調べて、被害に遭ってもお手上げになってしまわないように備えましょう。

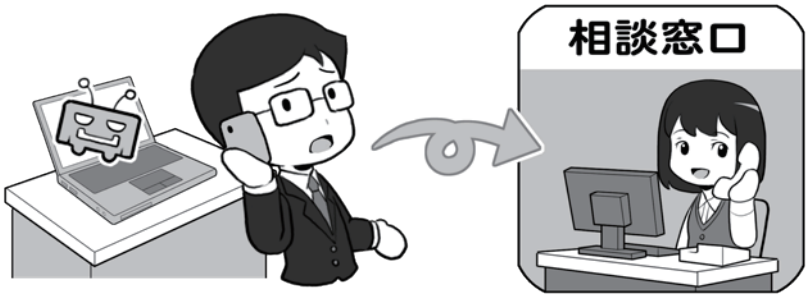
⑥常にバックアップを取ろう！

たとえ攻撃されても、適切にバックアップしておけば、すぐに復旧できます。

⑦人間にもセキュリティホールがあることを知ろう！

セキュリティの穴は人間の心にもあいています。攻撃者はどちらも攻撃してきます。

⑧困ったら各種相談窓口にすぐ相談しよう！



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

本書8項目と「情報セキュリティ5か条」「情報セキュリティ対策9か条」

IPA情報セキュリティ5か条	NISC情報セキュリティ対策9か条
1. **①OSやソフトウェアは常に最新の状態にしよう！**	1. OSやソフトウェアは常に最新の状態にしておこう
2. **②ウイルス対策ソフトを導入しよう！**	5. ウイルス対策ソフトを導入しよう
3. **③パスワードを強化しよう！**	2. パスワードは貴重品のように管理しよう
	3. ログインIDとパスワード絶対教えない用心深さ
	8. 外出先では紛失・盗難に注意しよう(紛失に備えてパスワードで保護しよう)
4. **④共有設定を見直そう！**	
5. **⑤脅威や攻撃の手口を知ろう！**	4. 見に覚えのない添付ファイルは開かない
	6. オンラインショッピングでは信頼できるお店を選ぼう
⑥．常にバックアップを取ろう！	7. 大切な情報は失う前に複製しよう
⑦．人間にもセキュリティホールがあることを知ろう！	
⑧．困ったら各種相談窓口にすぐ相談しよう！	9. 困ったときは一人で悩まず、まず相談

守るべき項目がなるべく少なくなるように、二つの指標をまとめて、○付きの数字の項目に集約しています。網掛けの部分はこのために本書が新しく起こした項目です。

1 ①OSやソフトウェアは常に最新の状態にしよう！

1 パソコン本体とセキュリティの状態を最新に保とう

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

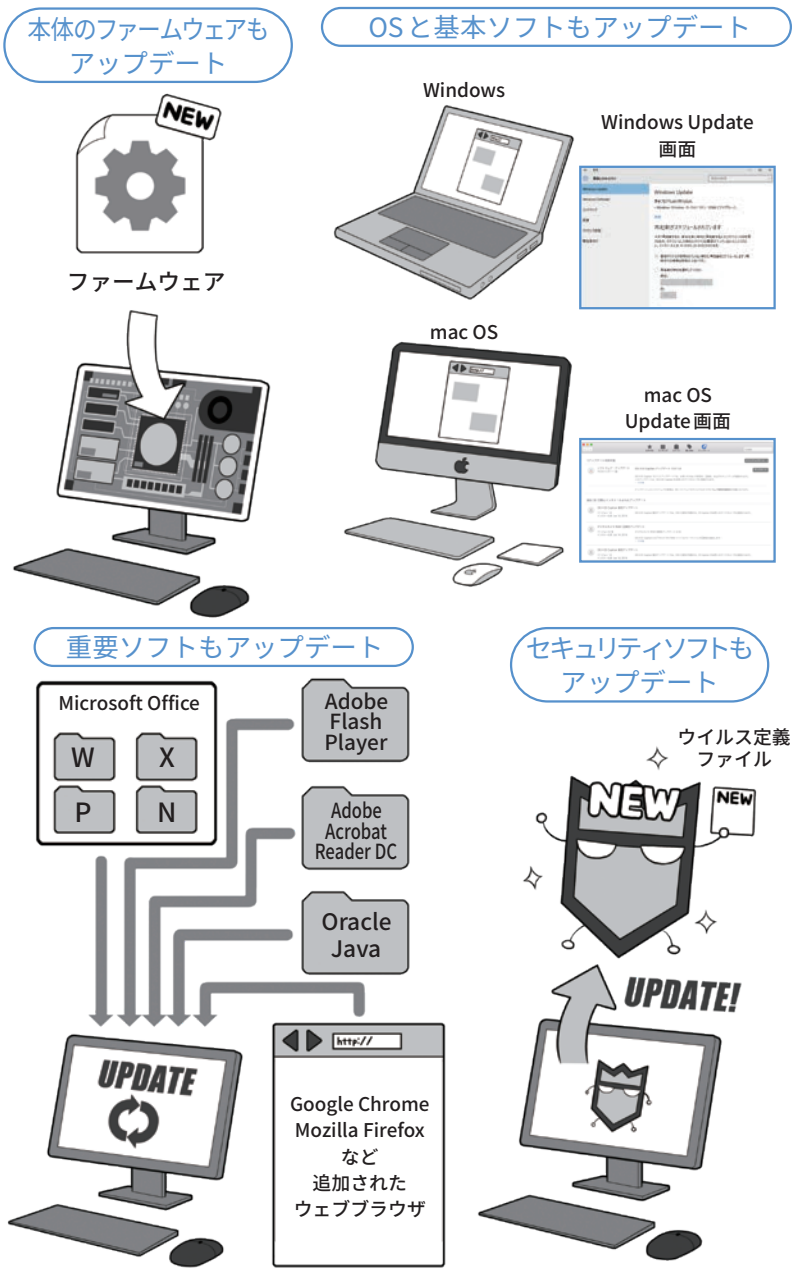
最近の機種では、OS関連のアップデート処理は自動で行われるか、アップデートを行うよう通知が出るようになっています。しかし、ときとして緊急でアップデートを行ったほうがよいこともあります。セキュリティ関連ニュースサイトなどでそういった情報が流れていたら、自主的に更新処理をかけるようにしましょう。Office製品などOSのメーカーが作っている重要なソフトもここで同時にアップデートします。

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社のFlash PlayerやAcrobat Reader、Oracle社Javaや各種のウェブブラウザは攻撃のターゲットになりやすいのです。

また、機器そのものの基本プログラムを更新するファームウェアアップデートにも気を配りましょう。こちらの更新通知は、自動で出る機器と出ない機器があるので、自分の機器用のアップデート情報は、どのようにすれば入手できるか、事前に確認して気を配ってください。

セキュリティソフト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、日に一度は意識的にセキュリティソフトの画面を見ましょう。これに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



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。

社会インフラがテロ攻撃などで狙われやすいのは、攻撃者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(更新)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。インストールしてあるが使っていない重要ソフトは削除(アンインストール)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、そもそも攻撃して乗っ取れる機器がなければ成立しないように、攻撃できる穴を作らない一人ひとりの行動が、安全なインターネットを作るのです。

2 スマホやネットワーク機器も最新に保とう

スマホも同様に各種のアップデートの適用が必須です。

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

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

スマホアプリの自動更新は、設定によっては無線LAN接続時のみ自動で行うことになっている場合もありますが、その設定でも更新時に権限変更で確認が必要な場合は自動更新されないこともあるので、気がついたら未更新のアプリがたくさんたまったままになってしまっていることもあります。日に一度は意識してアップデート画面に行き、更新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IoT機器やスマート家電などは、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、攻撃者に不正に利用されることが大いにあります。

アプリやセキュリティソフトの更新は基本的に自動更新にしつつ、まめにチェック

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

無線LAN
アクセスルータ

ネットワーク対応プリンタ

監視カメラ

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

2 ②ウィルス対策ソフトを導入しよう！

1 セキュリティソフトを導入して守りを固めよう

悪意のハッカーが攻撃に使うマルウェア。単純なウイルス検知ソフト、あるいは対策ソフトの場合、このマルウェアを見つける方法は、主として「手配書」方式になっています。

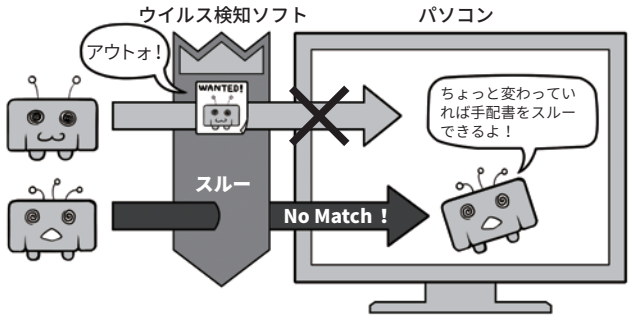
手配書方式とは、あらかじめ検出したいマルウェアの特徴を、検知ソフト開発元からそれぞれのパソコンなどに送信しておき、マッチしたものを駆除する方式です。

しかし、現在では攻撃者が、攻撃のターゲットごとに送信するマルウェアを微妙に変えたり、狙いを定めた相手には専用のマルウェアを開発し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困難になりつつあります。

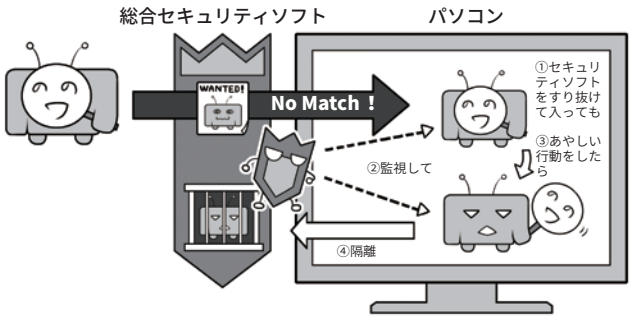
そこで最近の総合セキュリティソフトでは「手配書」方式に加えて、パソコンに入ってしまった後も監視を続け、不審な行動を取れば隔離や駆除を行う、「ふるまい検知」や、機能的に怪しい部分を検出する「ヒューリスティック分析」機能を持つものが出てきています。これにより未知のマルウェアにもある程度は対処できるわけです。

それでも対処しきれないものもあります。システムの穴であるセキュリティホールの発覚後、それに対して開発元からセキュリティパッチが配布され、穴が塞がれる前に攻める「ゼロデイ攻撃」を行うマルウェアです。この場合は手配書なども間に合わないので、現状では決定的に有効な対抗措置がほとんどありません。しかし、そういったことを加味したとしてもパソコンに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。

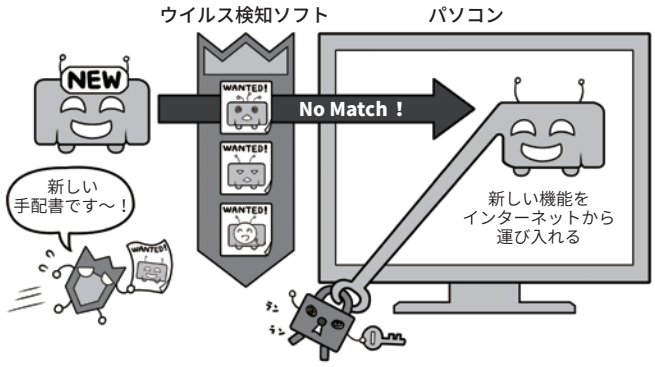
単純なウイルス検知ソフト



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 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、その誕生がパソコンなどと比較して近年ということもあり、設計思想自体により多くセキュリティの概念が盛り込まれています。したがってセキュリティを担うアプリは存在しても、それが担う役割はあまり大きくありません。

利用にあたって、そもそも不正なアプリをインストールしない、インストールするようにだまされない、インストールできる環境を作らないようにすれば、ある程度のセキュリティは確保できるのです。

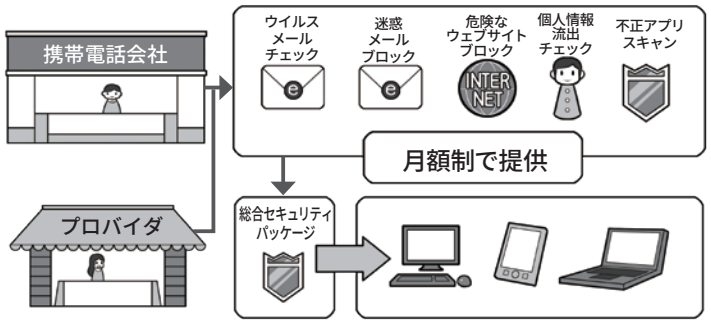
しかし、チェックするべき点を見落としてしまったり、だまされて気づかないうちに不正なアプリをインストールしてしまったりした場合の検知や、詐欺メールの検知、不正なアプリが仕込まれているウェブサイトのブロック、あるいは個人情報の流出チェックなど、セキュリティ全般にかかわるサポート機能を補助的に導入したいかもしれません。

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、精査した上で導入してもいいでしょう。

なお、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。

また、高機能化するスマート家電など IoT 機器についても他と同様にセキュリティ対策が必要になります。P58 も参照して、万全の対策を講じていきましょう。

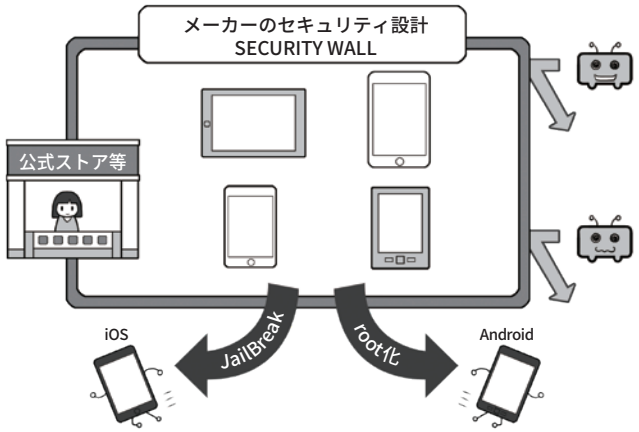
必要性を感じるなら、スマホには セキュリティパック導入を検討しよう



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

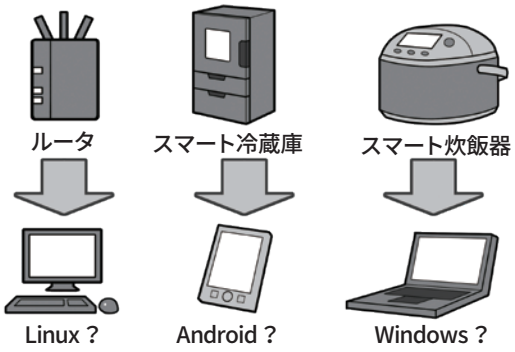
携帯電話会社からはセキュリティ関係の機能がパッケージ化されて提供され、インターネットプロバイダも同様のサービスを提供しています。自分が求める機能があるかを精査して、必要性を感じる場合は導入を検討しましょう。

スマホの改造をしてはいけません



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 というコンピュータシステムや、Android、Windows マシンが入っています。乗っ取られ、サイバー攻撃に利用されるなど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。

3 ③パスワードを強化しよう！

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て乗っ取る方法のほかに、なんらかの手段でIDとパスワードを解明し、サービスや機器を乗っ取る方法もあります。

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

総当たり攻撃を防ぐには、探り当てるまでに膨大な時間がかかるようにするのが一番の防御手段で、それには1桁の文字の種類と桁数による組み合わせを増やします。

例えば数字だけなら1桁10通りしかありませんが、英字を入れると36通り、英大文字小文字を入れると62通り、これに26文字の記号を入れると約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、理論上攻撃し続ければいつかは成功するのですが「時間がかかり事実上不可能な状態」にして防ぐのです。

ログイン用パスワードであれば入力ごとに遅延がかかるので、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、より組み合わせ数を増やし安全性を高めるにこしたことはありません。

ログイン用パスワードは英大文字小文字＋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」の10乗だと→100億通り

（英大文字小文字＋数字＋記号（88個として））の10乗だと→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、それを複数のサービスや機器の間で使い回していれば意味がありません。1カ所から漏れればすべてログイン可能になってしまうからです。

複雑なパスワードを1つ決めて、あとはおしりに数字や規則性のある文字をつけるのも、2つ以上漏れれば推測されます。それぞれに複雑なパスワードを設定し、使い回しをしないことが大切です。

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	1個漏れたら一網打尽
×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、テキストファイルにまとめておけばマルウェアに感染したときに流出し、多くのアカウントが一気に乗っ取られるかもしれません。

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

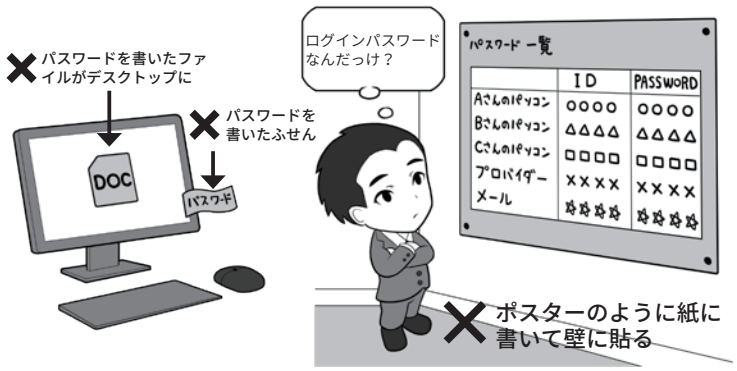
しかし、多くのサービスで複雑なパスワードをそれぞれ設定したら、とても覚えきることはできません。ではどうしたらいいでしょう。

一つは、パスワードを管理する紙のノートに書いてパソコンとは別に保管する方法。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です。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、過去に情報流出にまつわるトラブルのあったアプリやサービスは利用を避けるようにしましょう。それは他人の手元にIDやパスワードを保管することや、流出の危険が逆に増すことを意味するからです。

利用するところで保管するべきでないなら、スマホでパスワードを管理する場合リスクはありますが、こういったアプリは後述のPINコード(P114参照)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。

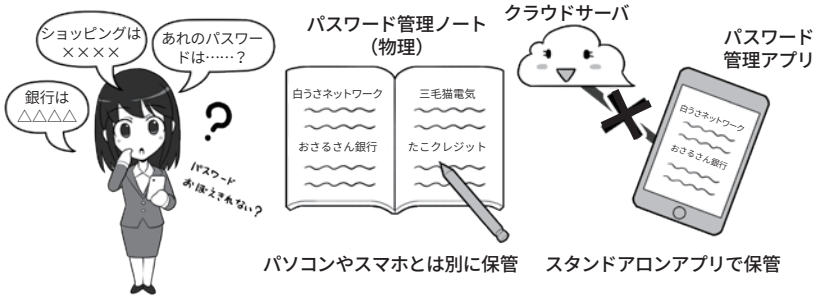
ただ、管理しているパスワードは、必ずバックアップするのを忘れないようにしましょう。落としたスマホが戻るとは限りませんから。

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。内部の人間が勝手に使うリスクもあります。

パスワードは紙のノートに書いて保管するか、パスワード管理アプリで守る



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

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

パスワードなどの自動入力は便利ですが、仕事場などであなたがパソコンをロックしないまま席を離れると、他人が各種サービスにログインし放題になります。

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や、あるいはいつもと違うログインがあった場合の本人確認のために「秘密の質問」と呼ばれる機能があります。これはあらかじめ利用者が、自分しか知らない質問と答えを設定しておいて、合い言葉的にこれに答え、本人であることを証明するものです。

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、こういった個人にまつわる情報はSNSが普及した今、ネット上で簡単に見つけられることもあり、セキュリティの観点からは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はあえてまじめに答えず、SNSの情報などから推測できないようにし、忘れないようにパスワード管理アプリなどに保存しましょう。

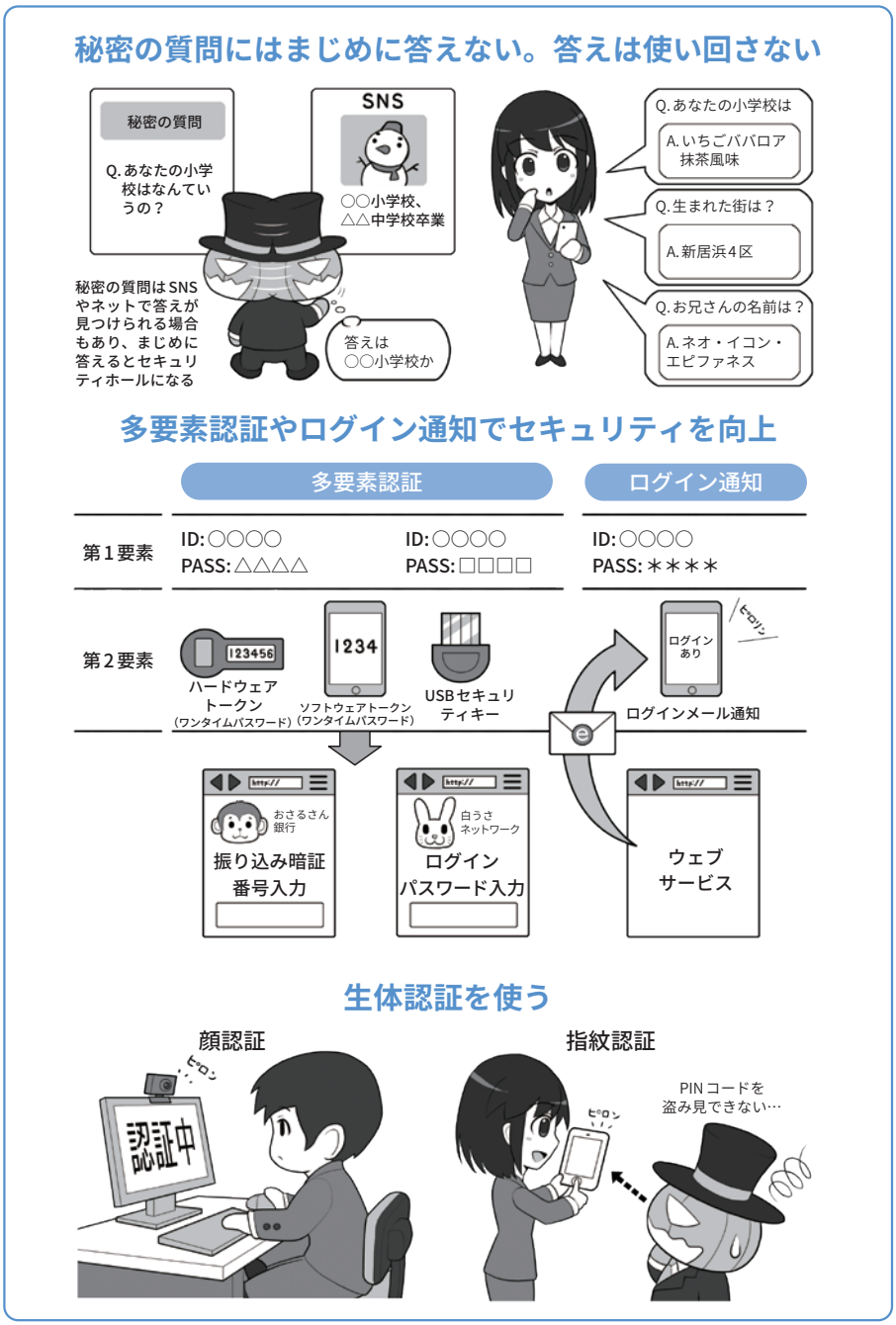
また、サービスへのログインを安全に行うために、二要素以上を使って認証作業をする多要素認証などの方法が提供されていれば必ず設定しましょう。これらの方法では通常のパスワードの他に、使い捨てにする別のパスワードを、ハードウェアトークンや生成アプリで作り、ログイン時に利用者に入力させます（メールやSMS・ショートメッセージを利用する方式もありますが、これらは安全面で非推奨です）。

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

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

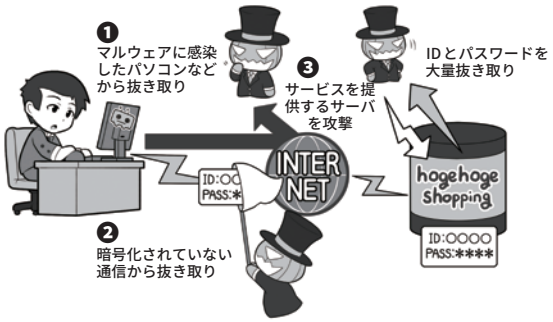
生体認証は本人のみが使える反面、指紋認証などは寝ている間に勝手にロック解除されることがあるなど善し悪しですが、肩越しの盗み見などよる暗証番号（PINコード）の盗難には強い機能でもあります。

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、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？

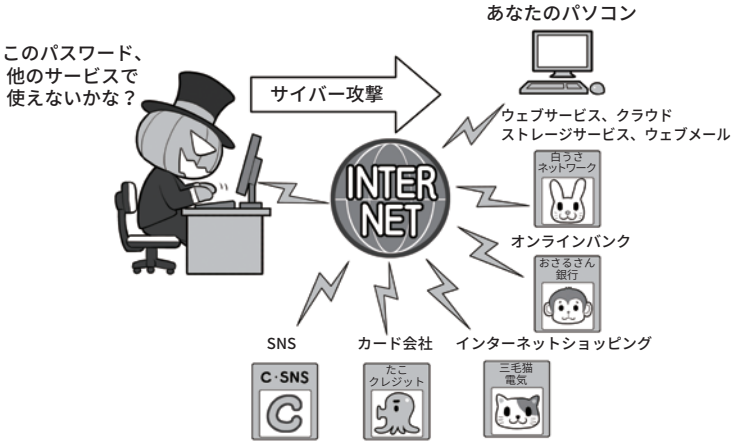
さまざまなIDとパスワードの漏えいパターン



攻撃者にIDとパスワードが漏えいする事態は、機器がマルウェアに感染したり、自分が通信する過程で抜き取られたりするほかに、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。

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



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

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

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

では実際はどのように漏れてしまうのでしょう？

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漏えいするケースなどがあります。

先ほど説明しましたが覚えておいてほしいのは、自分がマルウェアなどに感染していなくても、漏れてしまうケースがあるということです。したがってIDやパスワードを普段入力していないから安心、ともいい切れません。

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

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

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

もしパスワード流出が判明したら、まずはすぐにパスワードを変更しましょう。

4 ④共有設定を見直そう!

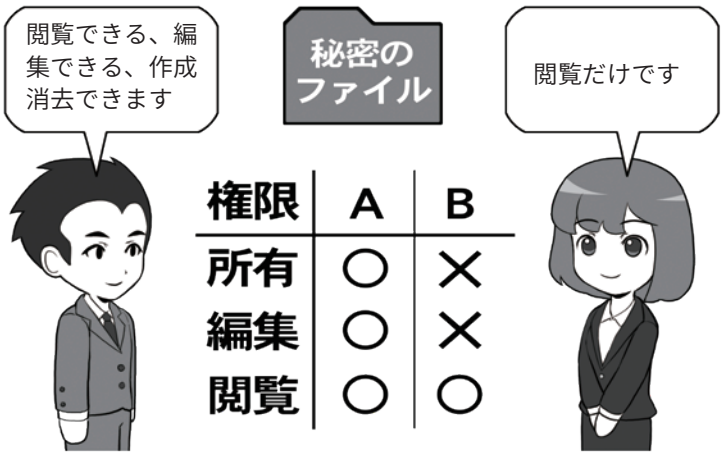
共有設定とは、私たちがIT機器上やインターネット上で使用するファイルや情報、あるいは機器そのものに関して、自分だけでなく誰かと共同で利用するときに、機密性を保つために必要な設定です。

共有設定には、ファイルの管理を例にあげれば、単純に見られるか見られないかを意味する「閲覧」、そのファイルを編集して内容を書き換えることができる「編集」、そしてファイルそのものを作ったり削除したりできる「所有」などの、大まかに3つの権限があります。

会社内でファイルをUSBメモリのような媒体にコピーしなくても受け渡しをしたりすることを可能にするために、社内にネットワーク(LAN:Local Area Network)を引いている企業であれば、ファイルを管理するサーバ(NAS: Network Attached Storage)上にある文章ファイルなどを見られる人を制限したり、あるいは誰かがうっかりファイルを消してしまわないように、こういったファイル毎の所有者設定や、同様の意味を成す資格設定をしっかりしておく必要があります。

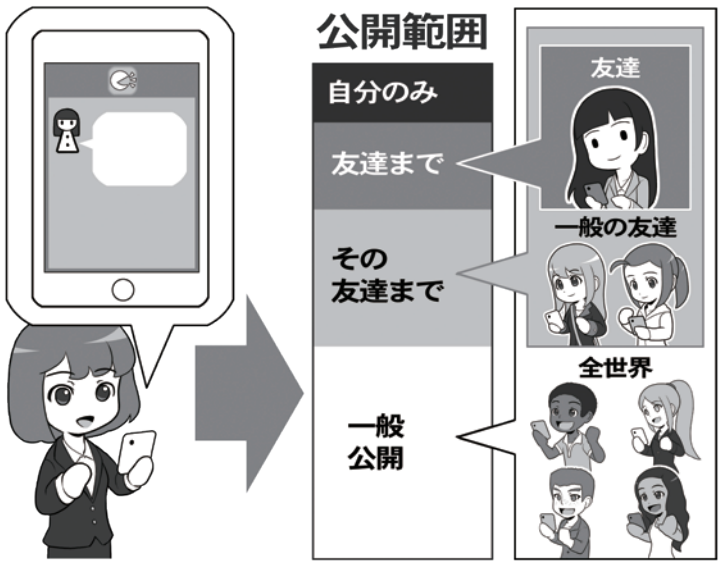
SNSやクラウドストレージサービスのようなインターネット上のサービスに関する共有設定の場合も上記と似ていますが、こちらの場合はだいたいは「公開設定」と呼ばれることが多いようです。つまり、どこまでの人が見たり開いたりしていいかを設定するわけです。

共有設定ってなんだろう？



物理的な手帳は、それが誰の持ち物で誰にも見せていいかといったことは、特に意識せずに使っています。しかし、ネットワーク上にあるファイルなどは、特に設定しない場合は、「基本的に誰でも見られる」状態になっているので、それでは困る場合、これに対してアクセスを制限する権限を設定する必要があります。それらが「所有」「編集」「閲覧」の権限です。

SNSの共有設定



SNS上に投稿した情報も、基本がオープンなSNSの場合、そのサービスに登録している人すべてが見られる「一般公開」の状態になっています。それが嫌な場合は、投稿内容やプロフィールに対して「公開範囲」を設定する必要があります。ただし、SNSでは限定公開していても、誰かがその内容をコピーして改めて一般公開すると、すべての人が見られるようになります。

例えばSNSへの投稿であれば、公開範囲として「自分だけ」「友だちまで」「友だちの友だちまで」「(一般)公開」などがあります。プライベートな写真などをインターネット上のファイルストレージサービスにアップロードしておいたのに、間違って一般公開にしていると、全世界の人

がそれを見ることができるようになってしまうわけです。

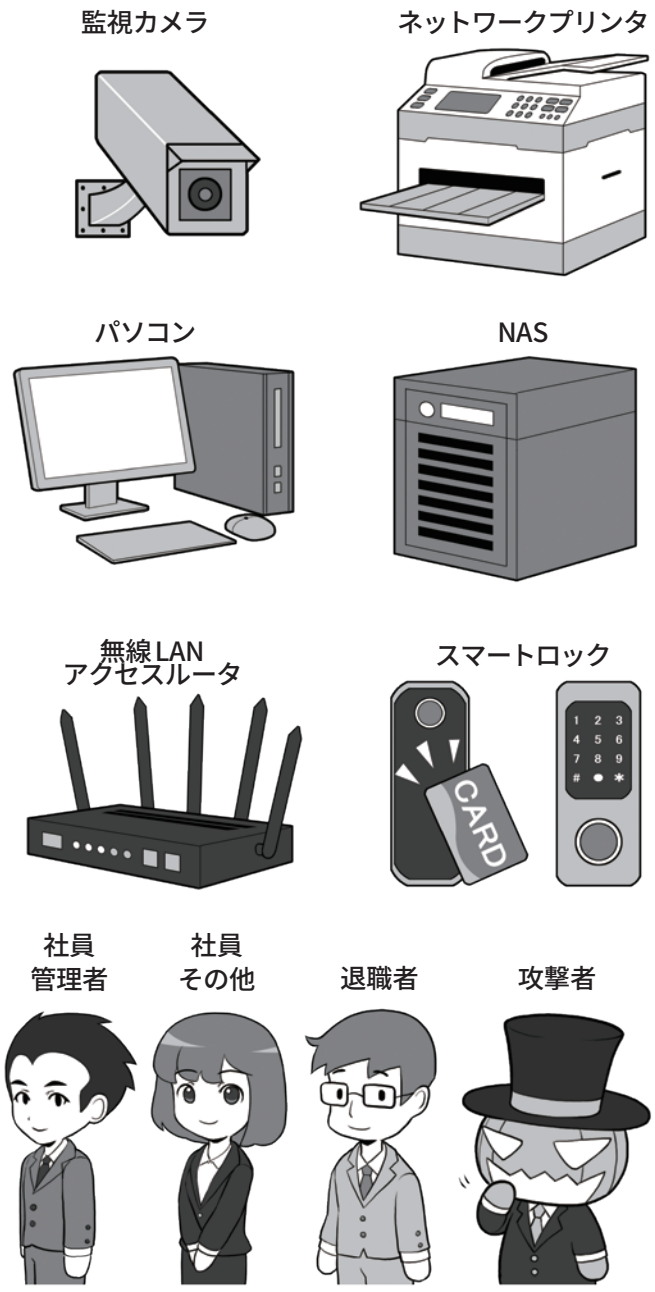
LAN上のNASでもストレージサービスでも、共有設定はファイル単位やフォルダ単位で設定できるので、その整合性に気を付けないといけないことと、例えば臨時で誰かに特定のファイルを公開したい場合、設定ではなく「見たり編集したりできる」リンクを送信することで共有することができるものもあり、この場合、そのリンクを知っている人は誰でも同じ権限を持つので、送信後の管理に特に注意が必要です。

IT機器そのものの利用にも、同様の設定があり、こちらの場合は共有というよりも利用できる権限設定です。機器を管理し設定を変更できる「管理者」や、利用するだけの「利用者」や「ゲスト」などがあり、これらは機器に対してログインするときのIDとパスワードで管理されるので、資格管理をしっかり行って下さい。

権限設定繋がりでいえば、会社の建物や特定の部屋に入るための権限を設定している場合も、同じようにきちんとした管理が必要です。例えば人事情報がある場所は人事の人間しか入れないようにしておく必要がありますし、社員の異動や退職が発生した場合、資格の無い人が立ち入りできないように、きちんと設定変更をしたり、入出用にICカードや鍵などを使っている場合は、回収する必要があります。

また、こういったシステムもIT機器を使っている場合は他のシステムと同じように、常にアップデートする必要があり、それを怠ると攻撃者がシステムをクラッキングした上で建物に物理的に侵入することもあります。なお、攻撃者は人間の心の隙を突くソーシャルエンジニアリングで社員をだまし、例えば建物管理や防犯システムの業者のふりをして、堂々とやってくるかもしれないのでそちらも注意しましょう。人間の心理も攻撃の対象なのです。

機器の共有設定



会社や団体の事務所で使用する機器も、ネットワークに繋がっている場合、基本的には誰でも利用できる設定になってることが多いのです。したがって特定の人のみが利用できるようにしたい場合は、それぞれの機器および利用者に対して権限を設定する必要があります。

建物などの立ち入りにIT機器による権限を設定している場合は、異動や退職などによってその人物の権限が変更されたり失ったりした際に、それに合わせてきちんと権限を変更するか、権限を執行するためのカードなどを回収しなければなりません。

これを怠ると、退職者が勝手に建物に立ち入ったり、あるいはなんらかの方法で攻撃者がそのカードを入手すると、なんの工作もしないで建物に侵入してしまえます。

また、機器に対する資格設定をしていない場合、攻撃者が無線LAN経由などで建物内のLANに侵入した場合、各種機器やファイルを管理しているNASなどに、なんなくアクセスしてしまえます。複数の人が働く職場ではこういった権限設定は特に重要です。

5 ⑤脅威や攻撃の手口を知ろう!

1 脅威や攻撃の手口を知ろう

「敵を知り己を知れば百戦危うからず」という孫子の諺(ことわざ)がありますが、サイバーセキュリティ上、危うい状況に陥らないためには、自らのセキュリティ環境が脅威にきちんと対応できてるか知り、また、攻撃者の手口を知ることが重要です。知らないことが、サイバー攻撃による被害がなくならない本質でもあるのです。

それを理解できれば、なにが必要かがわかり、さらにどのような情報が必要か地図が描けます。そうやってサイバー攻撃の危険性(ソーシャルエンジニアリングのような人間の心の隙を突くような攻撃を含め)を知ることが、一番の対策となるのです。

では、どのようにしたら情報を入手できるのでしょう？まずはセキュリティソフトを提供している企業の発信に注意を払いましょう。そうした企業はSNSなどで最新の攻撃情報をいち早く配信していることが多いので、著名な企業のアカウントを複数フォローするといいでしょう。

次にOSを作っているメーカーなどのアカウントです。ただし、そのアカウントが発信するのは自社製品に関する情報のみですが、有益な情報も多くあります。

もっと横断的な情報が欲しい場合は、IPAやNISCなどの政府機関のアカウントやメールマガジン、セキュリティや詐欺関連の対策機関の公式アカウント、セキュリティ系雑誌の記事を追いかけるようにしておけば、大規模なサイバー攻撃の兆候やセキュリティホールの発覚をいち早く察知することができ、その対策を立てることが容易になります。

攻撃者の攻撃手段を知ることで学ぶ

セキュリティ企業のブログやセキュリティ系のウェブ記事を見ていると、攻撃者の新しい攻撃手段について、かなり素早く教えてくれます。ニュースをキャッチするほかに、それがどういった意味を持つのか知りたい場合は、セキュリティー系ブログや記事が参考になります。

公的機関、OS企業、セキュリティ企業の情報を聞く

本当にヤバいサイバー攻撃が発生するとこんな感じに

上図に書かれているようにして、広範囲にアンテナを張ると、本当にヤバい攻撃が発生した場合は、各種ソースがその性格にかかわらず、一斉に同じ話題について発信し始めます。記事を理解するだけでなく、こういった波を肌で知ると、攻撃の危険度を察知し身構えたり回避策をとったりできます。

2 より能動的に情報収集しよう

そうした必要最低限の情報だけでなく、世界で起きているサイバー攻撃のトレンドなどを知りたいなら、海外のセキュリティ関連企業や機関、サイバーセキュリティに関する情報を提供しているウェブメディア、セキュリティ識者のSNSやブログなど参照するといいでしょう。

ただし、こうした情報は能動的に収集した上で取捨選択をする必要があり、さらに必ずしも毎日アップデートされるわけではありません。このため初めは熱心に情報を収集していても、だんだんと飽きてきてあまり見に行かなくなるかもしれません。

しかし、油断しているときにこそ、自分にも関係するような攻撃が起こるのが世の常です。

そこで、RSSと呼ばれる仕組みを利用して、攻撃情報を楽に収集できるようにしましょう。RSSは気になるウェブサイトやブログを登録しておけば、記事の更新があれば時系列で情報を串刺しして表示してくれます。

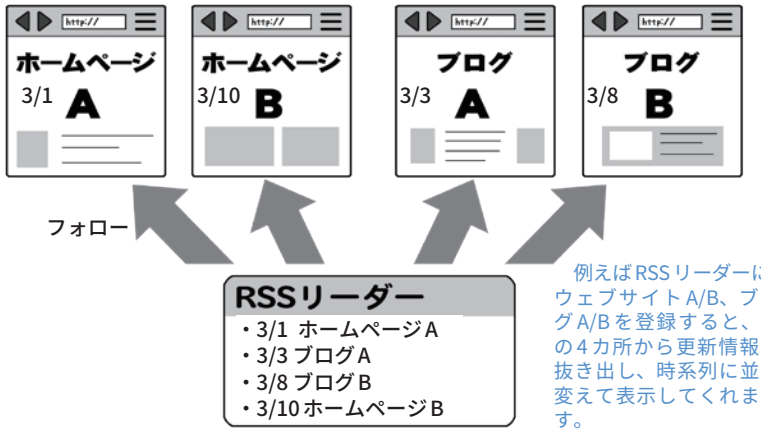
そうしたRSSを簡単に閲覧できるのが、RSSを管理できるウェブサービスとスマホ用のRSSリーダーと呼ばれるアプリの組み合わせです。それらを利用すると、まるでSNSを閲覧する感覚で、毎日世界中のどこかで起きているサイバー攻撃情報やトレンドが読むことができ、否が応でもセキュリティに関しての知識が蓄積されるでしょう。

常にアンテナの感度を上げていれば、新しいセキュリティホールが発覚したとき、自社に影響がないかが分かります。そうした感覚を持つことがサイバー攻撃に対する最大の備えなのです。

RSSってなんぞや

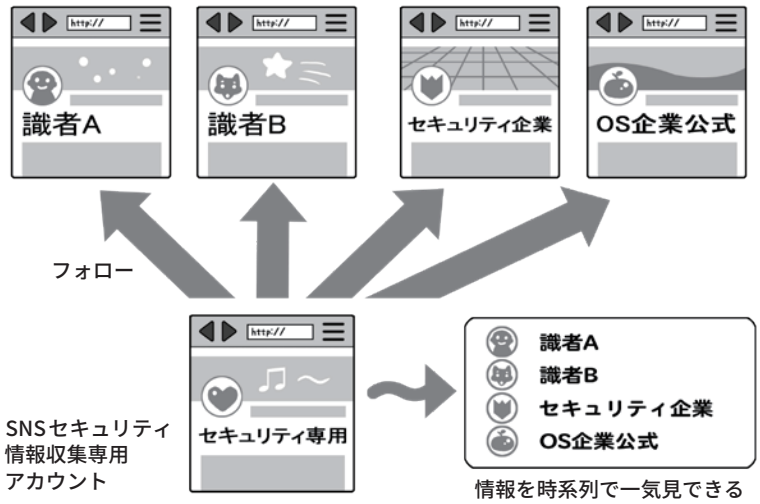
RSSとは平たくいえば、ウェブサイト上の更新情報を、見出し、もしくは概略付きで、時系列に、ウェブサイトの裏の見えない所で発信しているものです。規格（フォーマット）が決まっているので、RSSリーダーに登録すると複数の情報源を串刺しして見ることができます。

RSSは情報を串刺しして一気見できる



例えばRSSリーダーに、ウェブサイトA/B、ブログA/Bを登録すると、その4カ所から更新情報を抜き出し、時系列に並び変えて表示してくれます。

SNSも同様



RSSリーダーの感覚は、SNSで複数のアカウントをフォローすると、素の表示ではフォローしているアカウントの発信が時系列で並ぶのと一緒です。それと同じことをウェブサイトやブログでやると考えると分かりやすいでしょう。

なお、RSSリーダーはインターネット上のサービスで、それ自身がスマホアプリを出している場合もありますし、RSSリーダーに対応した個別のアプリも存在するので、それを導入すると、SNSの流し見と同じ感覚でセキュリティ情報をチェックできます。もちろんSNS上にある、セキュリティ関係のアカウントをフォローしてもOKです。セキュリティ情報収集専用のSNSアカウントを作ってフォローしておくと、個人的なSNS活動と混ざらないでいいでしょう。

良い情報源を集めこの2つを常時チェックしておくと、かなり情報を素早くキャッチできます。

なお、こういったウェブサイトやアカウントで発信される情報は、必ずしも一次情報ソースではないので、真偽を確かめたい場合は一次情報ソースを探すよう心がけて下さい。

6 ⑥常にバックアップを取ろう！

1 何をするにもバックアップを取ろう

各種のサイバー攻撃や、パソコン・スマホの故障などからいち早く復旧して事業を継続するには、システムやデータのバックアップが不可欠です。特に近年は感染するとファイルを暗号化して身代金を要求するランサムウェアの流行により、バックアップの重要性が格段に上がっています。

バックアップの方法は主にパソコンやスマホのOSの種類により異なっています。

パソコンの場合には、macOS搭載の機器のように、外付けの補助記憶装置（ハードディスクやSSD。以降記憶装置）を接続するだけでバックアップが行え、復旧もシステムとデータすべてをほぼ全自動で行えるものもあります。これに対してWindows搭載機器では、基本的にはデータをバックアップする考え方で、システムの復旧とデータの復元は、別に行うようになっています。

スマホの場合も機種ベンダーによる差もありますがほぼ同様です。

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

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

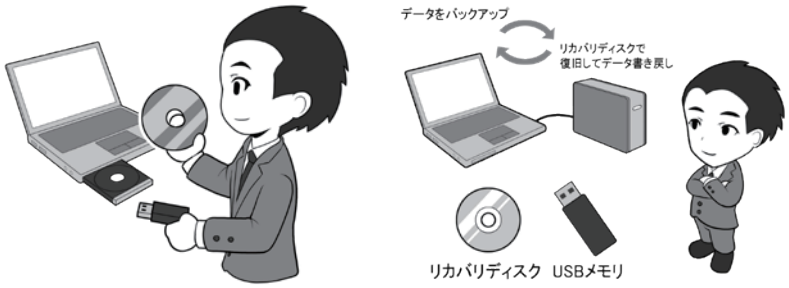
macOS機器のバックアップと復元

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

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

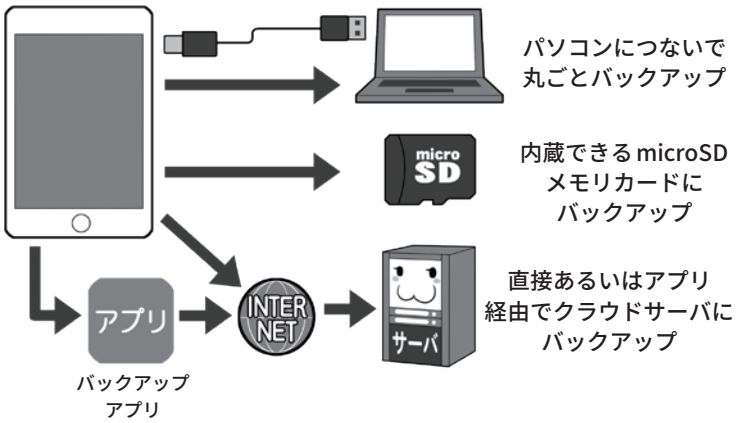
ですから基本的なそれぞれのOSの立ち位置や性格と考えて下さい。善し悪しや優劣はありません。

Windows機器のバックアップと復元

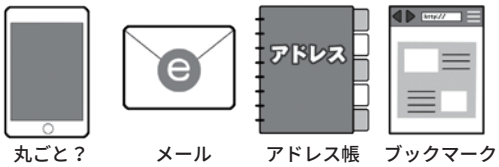


スマホもバックアップは定期的に取ろう

バックアップの方法はいろいろ



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。

2 ランサムウェアや天災にも対応できるバックアップ体制

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

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

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

また、最近は大雨による水害で、事務所にあったパソコンと外付け記憶装置が両方とも水没して復旧が困難になるという話もありました。

これに対応する手段としては、バックアップの「3-2-1ルール」というものがあります。

バックアップは本体を含め3個以上、2種類以上の媒体、そして1個は遠隔地に置くというものです。

遠隔地とは、現実的には「クラウドサーバ」などの利用を意味します。会社に同時に災害に遭わなそうな支社などがある場合は、そこにバックアップをおいてもいいでしょう。

クラウドサーバは最近では手頃になりましたが、それでも本体の全データをバックアップできる容量は高価です。したがって、事業継続に必要な重要なデータを選別してバックアップすることになるでしょう。

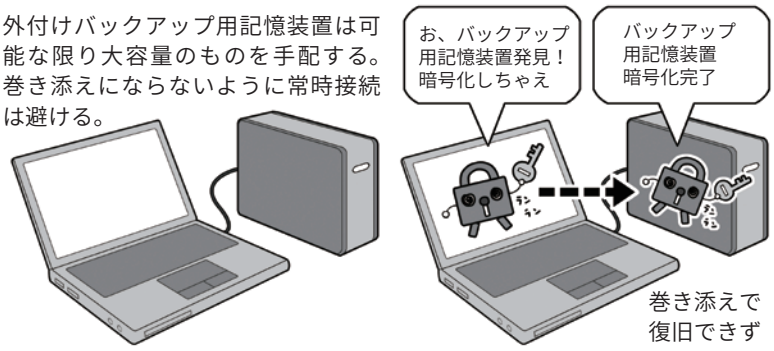
なお、最近のクラウドでのバックアップはランサムウェアの巻き添えになりにくい規格のものもあるので、利用にあたっては調べてみましょう。

ランサムウェア感染はビジネスにも影響

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

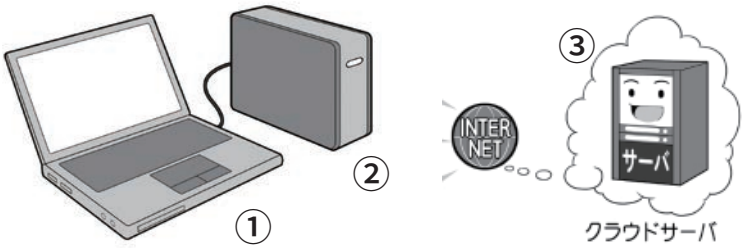
バックアップの体制を整える

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



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

バックアップは3個以上、2種媒体以上、1個は遠い場所



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

7 ⑦人間にもセキュリティホールがあることを知ろう!

デジタル世代のサイバー攻撃対策というと、機器やシステムで対抗することがクローズアップされがちですが、それはいってみれば会社の物理的な警備を固めるようなものです。

しかし、どんなに警備を固めても、内部の人間が心の隙を突かれて、攻撃者を招き入れてしまえば、全く役に立ちません。

機器やシステムのセキュリティと、心の隙を突く「ソーシャルエンジニアリング」に対抗する人間のセキュリティは、車の両輪なのです。

古典的なソーシャルエンジニアリングは、人間の「急かされたり驚いたり、パニックになると正常に判断ができなくなる」状態や、「油断」を直接的に攻撃してきました。

デジタル世代のソーシャルエンジニアリングは、それに加えBECなどの例に見られるように、相手が姿を現さず、メールなどを使って攻撃が行われます。こちらの方が、「姿を現すことによって物理的に発見されるリスクを軽減できる」からです。

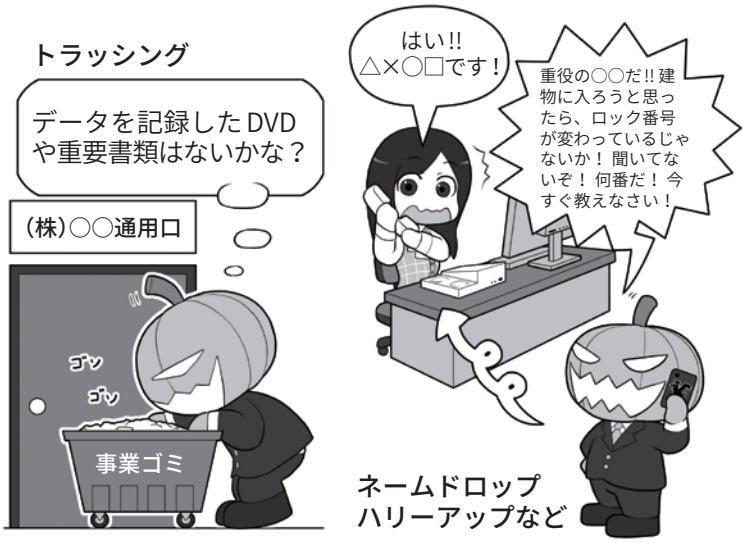
右下の図では、マルウェアを仕込んだウェブサイトに誘導する、リンクを含んだメッセージや、内部の人間になりすまして、偽装したマルウェアを開かせようとする攻撃例を掲載していますが、これらはいずれも相手の「油断」を突いているわけです。

心の隙を突くソーシャルエンジニアリング攻撃を防ぐには、ソーシャルエンジニアリングにはどういったパターンがあるのかと、それが実際に私たちに対する攻撃で使われる場合、どういった手口があるのかを知り、送られてきたとき「あの手だ！」と気づけたり、「なにか怪しい」と察知できるようにスキルを向上する必要があります。

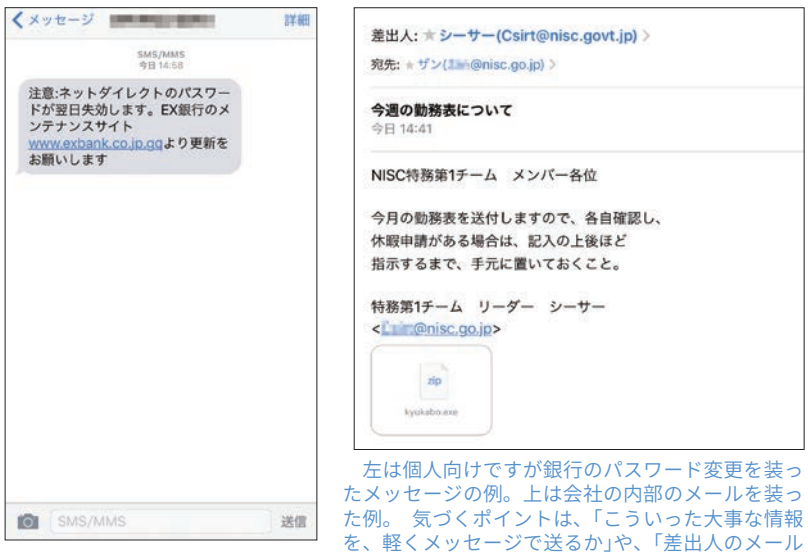
まずは、私たちには避けがたい心の隙があることを認識しましょう。

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



左は個人向けですが銀行のパスワード変更を装ったメッセージの例。上は会社の内部のメールを装った例。 気づくポイントは、「こういった大事な情報を、軽くメッセージで送るか」や、「差出人のメールアドレスが『政府のメールアドレスではない』です。

8 ⑧困ったら各種窓口にすぐ相談しよう!

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

ITに詳しい社員などがいればその人を中心に対処しましょう。

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

次に、連絡するには状況を把握しなければならないので、なるべく分かる範囲で5W1Hのように分けて事象を記録しましょう。いつから始まったのか、どのようなことがあったのか、誰が作業していたのかなどです。当然のことながらその間、攻撃が行われたと思われるパソコンなどの機器は使わず、その他の機器や紙のメモで記録します。

サイバー攻撃を受けたときに相談するサービスを契約している場合はそちらに相談し、無い場合は、IPAの「情報セキュリティ安心相談窓口」のウェブサイトを検索して、類似の例がないか調べてから、電話やメールで相談しましょう。

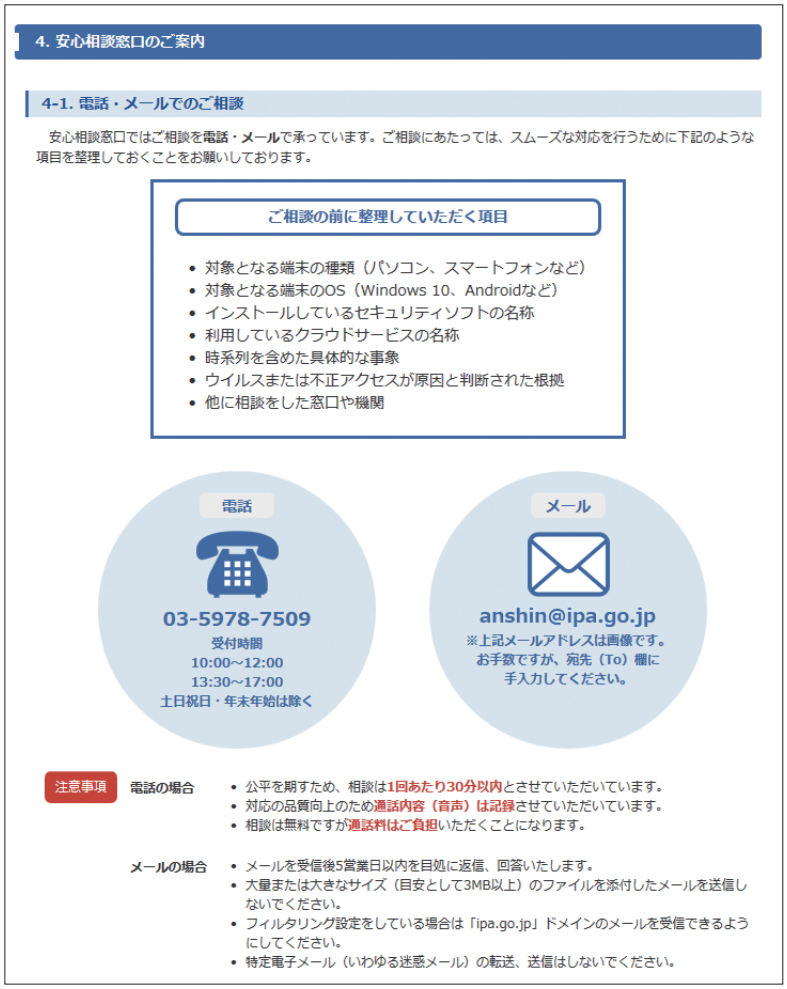
情報を消されたり、なにか機器を故障させられたり、あるいは情報を盗難されるなど、明確な被害がある場合は、各都道府県警のサイバー犯罪相談の窓口などに相談しましょう。

そして自社や団体で扱っている個人情報を盗まれたり消されたりしてしまった場合、「望ましい対応」として、原因究明や再発防止策の策定、そして「努力義務」として個人情報保護委員会などへの速やかな報告が求められます。

従来はファックスや郵送での報告ですが、令和元年3月からは、ウェブサイトからフォーム入力による方法で報告できるようになりました[*1]。

各種連絡窓口のウェブサイトなど

●IPA「情報セキュリティ安心相談窓口」
https://www.ipa.go.jp/security/anshin/index.html#4-1



●警察庁「都道府県警察本部のサイバー犯罪相談窓口等一覧」
https://www.npa.go.jp/cyber/soudan.htm

●個人情報保護委員会「漏えい等の対応（個人情報）」
https://www.ppc.go.jp/personal/legal/leakAction/

*1：詳しい報告先や対応方法は個人情報保護委員会ウェブサイトをご覧下さい。

9 総合的に攻撃のコストがかかるようにして防ごう!

サイバー攻撃を行う攻撃者は、例外的な軍事や産業スパイ、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、なんらかの利益目的の行動が多いのです。

それは彼等にとってのビジネスであり、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、鍵をかけてい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。

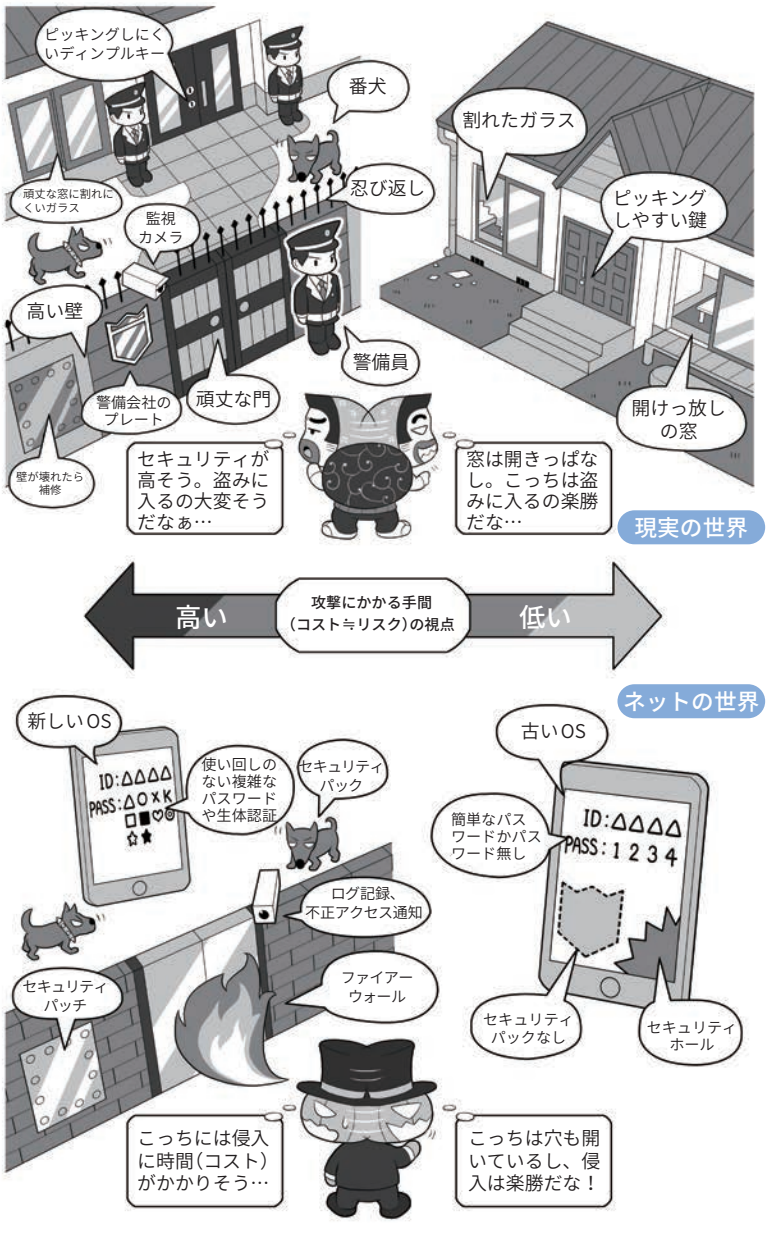
これはネットの世界でも同様です。侵入するまでに幾重にも難関があり、侵入を試みたら形跡を記録され(ログ)、場合によってはしかるべき管理者に通知が行き、パスワードを破ろうとしても複雑で突破できない。システムも最新で攻撃するにもセキュリティホールが見あたらない。セキュリティソフトも導入されている。さらにファイルを盗めても複雑な暗号化がされていれば、解読までに何百年もかかってしまい使えない。普通の攻撃者なら敬遠します。

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、ファイルは暗号化されておらず、さらにパスワードはたくさんのサービスで全部同じものを使い回している。

これならば攻撃者にとってどっちに行くのがコストパフォーマンスがいいか明らかでしょう。

ですから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。

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



コラム：それでも間に合わないゼロデイ攻撃

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攻撃可能な状態になってから、メーカーによって修正され攻撃不可能になるまでの期間をゼロデイとよび、この期間を狙って行われる攻撃を「ゼロデイ（ZERO DAY）攻撃」といいます。

メールなど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、特定のウェブサイトを見ただけで感染することもあり、情報が無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。

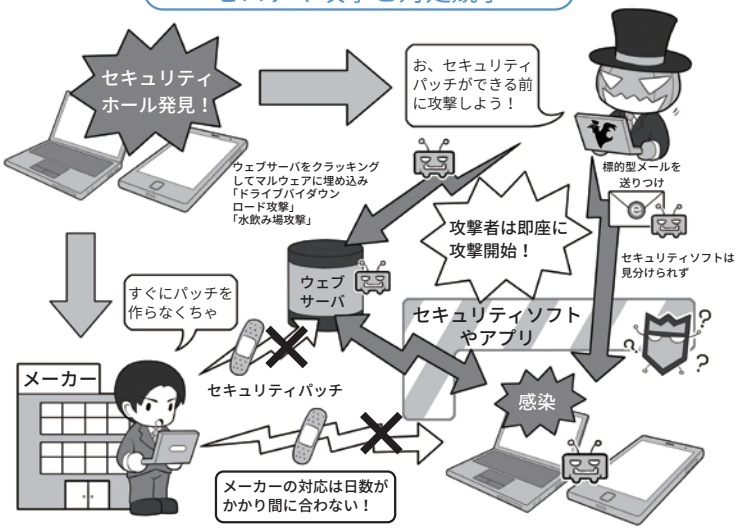
ときには、攻撃者がお金を支払ってまで、マルウェアの仕込まれた動画ウェブ広告を大手サイトに出してサイバー攻撃をしかけてくるため、その規模も非常に大きくなってきています。これは広告を出すコストが、不正に入手できるお金に見合っているということを意味しています。

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。

アプリを提供しているウェブサービスは、アプリが使用できない状況でも、ウェブブラウザでウェブ版が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

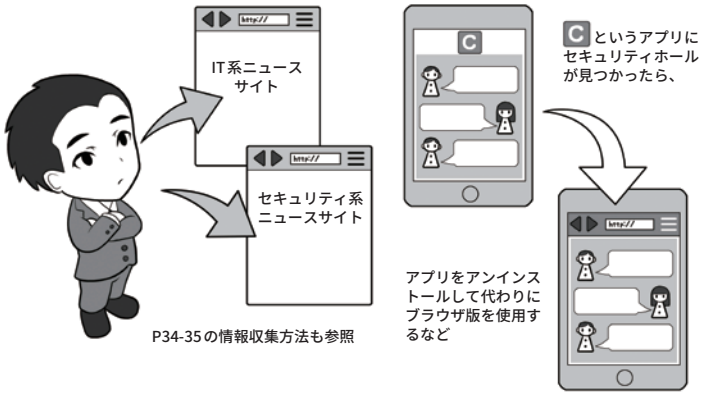
ゼロデイ攻撃と対処競争



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



P34-35の情報収集方法も参照

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段階でセキュリティホールの情報を入手し、対象の機種どれか一つでも攻撃に成功するなら攻撃を開始できますが、メーカーは情報を入手し精査した上でセキュリティパッチを開発し、攻撃可能と思われる機種すべてで、セキュリティパッチが正常に動作するか、充分な検証をしてからリリースしなければならないからです。

ですから利用者もそれを前提として備え、ゼロデイ攻撃を想定して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からです。

コラム：IPA「中小企業の情報セキュリティ対策ガイドライン」紹介

1 中小企業の情報セキュリティ対策ガイドラインとは

IPA（独立行政法人情報処理推進機構）は安全で利便性の高いIT社会の実現を目指して、情報セキュリティ対策など各種の取組みを行っている経済産業省所管の実務実施機関です。

そのIPAが発行している「中小企業の情報セキュリティ対策ガイドライン」（以下「対策ガイドライン」）は、ITを何らかの形で経営に活用している中小企業であれば、必ず参照しておくべき指針です。

この対策ガイドラインは、中小企業の経営者に対し、対策の必要性に気づいてもらい、情報セキュリティ対策に全く取り組んでいない状態から、徐々にステップアップし、しっかりとした社内ルールと体制を作って組織的な情報セキュリティのマネジメント体制を構築する道筋を提供することを目的に編集されています。

ウェブサイトにおいてPDFの電子ファイル版で無償配布されているほか、印刷版も有償で提供されています。

この対策ガイドラインの構成は、大きく本編と付録に分かれ、さらに本編は、第1部の「経営者編」と第2部の「実践編」で構成されています。

「経営者編」では、経営者が情報セキュリティの必要性を認識し、自らの責任で考え、実行しなければならない事項について説明されています。

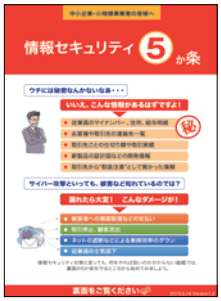
「中小企業の情報セキュリティ対策ガイドライン」とその付録

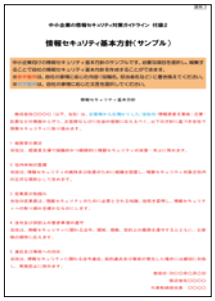
「中小企業のセキュリティ対策ガイドライン」には本編と、各企業が取り組まなければいけないチェック項目や、自社のセキュリティ資料を作るためのひな型、そしてクラウドの安全利用のための手引きが含まれます。

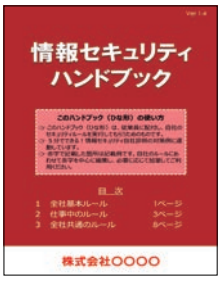
中段左から「情報セキュリティ対策5か条チラシ」、中段中「情報セキュリティ基本方針」のサンプル、中段右「5分でできる自社診断」、下段左「情報セキュリティハンドブック」のひな型、下段中「情報セキュリティ関連規程」のサンプル、そして下段左が「中小企業のためのクラウドサービス安全利用の手引き」となっています。

特にひな型やサンプルは、まずは文章中の項目を自社の組織や社員名に書き換えればいいように作られています。

このほかにやや専門的になりますが、EXCEL用の「リスク分析シート」があります。







中小企業の情報セキュリティ対策ガイドライン	https://www.ipa.go.jp/security/keihatsu/sme/guideline/index.html

対策を怠ることで企業が被る不利益や、経営者などが問われる法的な責任、社会的な責任などが、事例や主な関係法令の条項と処罰とともに説明されています。そして経営者が認識しておかなければならない「3原則」と、経営者自ら、または、従業員に指示して実行しなければならない「重要7項目の取組」が記述されています。

「実践編」では、具体的にどのように対策を進めていくかについて記述されています。

規模の小さな会社や、これまで十分な情報セキュリティ対策を実施してこなかった企業などでも、

すぐにできることから開始して、ステップバイステップで、企業それぞれの事情に適した対策が実施できるように、進め方を説明しています。

本ハンドブック第1章の冒頭にある「基礎8項目」のなかで引用されている「情報セキュリティ5か条」は、対策ガイドライン実践編の冒頭で紹介しています。

この5か条は、まず取り組んでいただきたい基本的な対策を最小限にまとめられたものです。ぜひここから対策をスタートしてください。

こののち、実践編では、現状を知り改善するステップ、本格的に取り組むステップについて解説しています。

それぞれのステップは、中小企業の実態や情報セキュリティ対策のありかたを熟知している有識者により検討された内容となっています。

「付録」は実践編に取り組む際に使用するひな型やシート類です。構成は以下のとおりです。

- **情報セキュリティ対策5か条チラシ**
- **情報セキュリティ基本方針(サンプル)**
- **5分でできる自社診断**
- **情報セキュリティハンドブック(ひな形)**
- **情報セキュリティ関連規程(サンプル)**
- **中小企業のためのクラウドサービス安全利用の手引き**
- **リスク分析シート**

5分でできる自社診断の25項目

診断編

診断項目	No	診断内容	チェック 実施している	一部実施している	実施していない	わからない
Part 1 基本的対策	1	パソコンやスマホなど情報機器のOSやソフトウェアは常に最新の状態にしていますか？	4	2	0	−1
	2	パソコンやスマホなどにはウイルス対策ソフトを導入し、ウイルス定義ファイル※1 は最新の状態にしていますか？	4	2	0	−1
	3	パスワードは破られにくい「長く」「複雑な」パスワードを設定していますか？	4	2	0	−1
	4	重要情報に対する適切なアクセス制限を行っていますか？	4	2	0	−1
	5	新たな脅威や攻撃の手口を知り対策を社内共有する仕組みはできていますか？	4	2	0	−1
Part 2 従業員としての対策	6	電子メールの添付ファイルや本文中のURLリンクを介したウイルス感染に気をつけていますか？	4	2	0	−1
	7	電子メールやFAXの宛先の送信ミスを防ぐ取り組みを実施していますか？	4	2	0	−1
	8	重要情報は電子メール本文に書くのではなく、添付するファイルに書いてパスワードなどで保護していますか？	4	2	0	−1
	9	無線LANを安全に使うために適切な暗号化方式を設定するなどの対策をしていますか？	4	2	0	−1
	10	インターネットを介したウイルス感染やSNSへの書き込みなどのトラブルへの対策をしていますか？	4	2	0	−1
	11	パソコンやサーバーのウイルス感染、故障や誤操作による重要情報の消失に備えてバックアップを取得していますか？	4	2	0	−1
	12	紛失や盗難を防止するため、重要情報が記載された書類や電子媒体は机上に放置せず、書庫などに安全に保管していますか？	4	2	0	−1
	13	重要情報が記載された書類や電子媒体を持ち出す時は、盗難や紛失の対策をしていますか？	4	2	0	−1
	14	離席時にパソコン画面の覗き見や勝手な操作ができないようにしていますか？	4	2	0	−1
	15	関係者以外の事務所への立ち入りを制限していますか？	4	2	0	−1
	16	退社時にノートパソコンや備品を施錠保管するなど盗難防止対策をしていますか？	4	2	0	−1
	17	事務所が無人になる時の施錠忘れ対策を実施していますか？	4	2	0	−1
	18	重要情報が記載された書類や重要なデータが保存された媒体を破棄する時は、復元できないようにしていますか？	4	2	0	−1
Part 3 組織としての対策	19	従業員に守秘義務を理解してもらい、業務上知り得た情報を外部に漏らさないなどのルールを守らせていますか？	4	2	0	−1
	20	従業員にセキュリティに関する教育や注意喚起を行なっていますか？	4	2	0	−1
	21	個人所有の情報機器を業務で利用する場合のセキュリティ対策を明確にしていますか？	4	2	0	−1
	22	重要情報の授受を伴う取引先との契約書には、秘密保持条項を規定していますか？	4	2	0	−1
	23	クラウドサービスやウェブサイトの運用等で利用する外部サービスは、安全・信頼性を把握して選定していますか？	4	2	0	−1
	24	セキュリティ事故が発生した場合に備え、緊急時の体制整備や対応手順を作成するなど準備をしていますか？	4	2	0	−1
	25	情報セキュリティ対策（上記1～24など）をルール化し、従業員に明示していますか？	4	2	0	−1

※1 コンピュータウイルスを検出するためのデータベースファイル「パターンファイル」とも呼ばれる
※2 重要情報とは営業秘密など事業に必要で組織にとって価値のある情報や顧客や従業員の個人情報など管理責任を伴う情報のことです

A 実施しているの合計点	B 一部実施しているの合計点	C わからないの合計点
点	点	マイナス(−)　点
A+B+C 合計	点	

診断の後は次ページ以降を読んで対策を検討してください。

3

付録「5分でできる自社診断」の中にある、診断のための25項目。それぞれの項目に答えることで自社のセキュリティレベルが診断できます。
先々どういったセキュリティ項目を満たしていかないといけないか、というビジョンを持つためには目を通しておくといいでしょう。
情報セキュリティ対策支援サイトでもオンラインで診断ができます。

https://security-shien.ipa.go.jp/learning/

これらのうち、「5分でできる自社診断」は、25問のチェック項目に回答することで自社の対策状況を把握することが出来るというものです。「基本的対策」、「従業員としての対策」及び「組織としての対策」という構成になっており、「基本的対策」は前述の「情報セキュリティ5か条」と同じになっています。

これに加え、「従業員としての対策」では、電子メール利用時や情報を格納した機器等の持ち出し、管理、バックアップなどの13項目、「組織としての対策」では、従業員教育や、取引先との契約時の秘密保持、緊急時の体制整備、ルール化など7項目が設けられています。これら25項目により、情報セキュリティ対策の実施状況を点数化し

100点満点でどの程度の達成状況か、また、どのような項目が弱点かを測ることができ、対策に取り組むうえでのポイントを見える化することが出来ます。

同じく、付録に収録されている「情報セキュリティ基本方針」や「情報セキュリティ関連規程」のサンプルは、それぞれ、自社の状況や方針に沿って記述を選択、あるいは書き換えることで自社固有のものに仕上げることが可能です。また、「情報セキュリティハンドブック」(ひな型)は、社内ルールに合わせて書き換えができますので、従業員ひとりひとりへのルール徹底に役立ちます。

2 情報セキュリティ対策自己宣言「SECURITY ACTION」

「SECURITY ACTION(セキュリティ アクション)」制度は、中小企業が情報セキュリティ対策に自発的に取り組むことを社の内外に宣言する制度です。

IPAのほか、商工団体、中小企業に関係する士業団体などが連携して創設し、IPAが運用を行っています。

情報セキュリティ対策を始めたくても「なにをすれば良いかわからない」、「経営者が重要性を認識してくれない」という中小企業の実態(IPAが実施した実態調査より)を踏まえ、まず何をすべきか、より良くするために何をすべきか、ということを示し、実際に取り組んでいることを中小企業に自己宣言してもらおう、というのがこの制度の趣旨です。

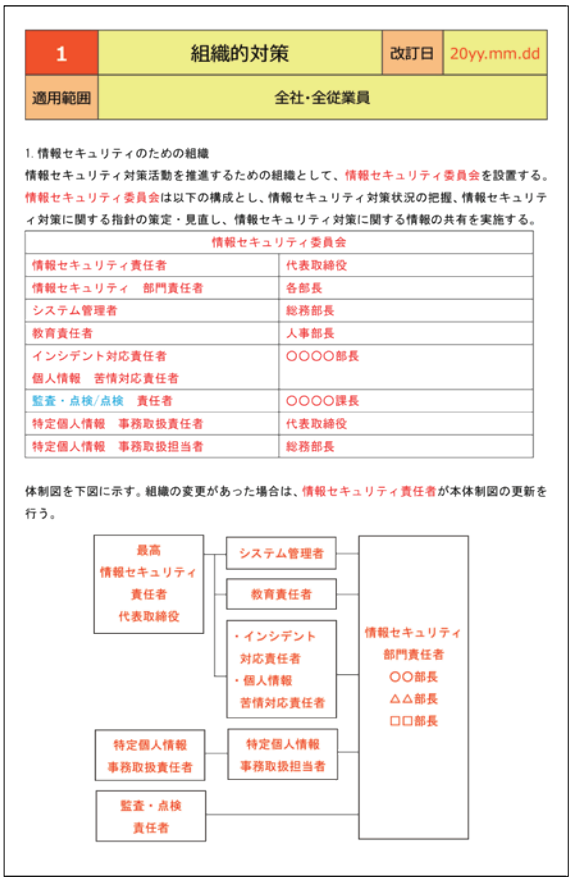
SECURITY ACTIONは、現在「一つ星」と「二つ星」の2段階があります。一つ星は「情報セキュリティ対策5か条」に取組むことを宣言するもの、二つ星は、「5分でできる自社診断」で自社の状況を把握するとともに情報セキュリティ基本方針を定めてウェブサイト上などで外部に示したことを宣言するものです。これらは、「中小企業向け情報セキュリティ対策ガイドライン」と同調しています。

この宣言をすることにより、社内意識の醸成、また、社外からは取組みを評価され、信頼の獲得と向上につながるなどの効果が期待できます。

まずはじめる、その一歩としてSECURITY ACTIONを宣言してはいかがでしょうか？

(執筆：IPA)

情報セキュリティ関連規定のサンプル



1	組織的対策	改訂日	20yy.mm.dd
適用範囲	全社・全従業員		

1. 情報セキュリティのための組織

情報セキュリティ対策活動を推進するための組織として、情報セキュリティ委員会を設置する。情報セキュリティ委員会は以下の構成とし、情報セキュリティ対策状況の把握、情報セキュリティ対策に関する指針の策定・見直し、情報セキュリティ対策に関する情報の共有を実施する。

情報セキュリティ委員会	
情報セキュリティ責任者	代表取締役
情報セキュリティ　部門責任者	各部長
システム管理者	総務部長
教育責任者	人事部長
インシデント対応責任者 個人情報　苦情対応責任者	○○○○部長
監査・点検/点検　責任者	○○○○課長
特定個人情報　事務取扱責任者	代表取締役
特定個人情報　事務取扱担当者	総務部長

体制図を下図に示す。組織の変更があった場合は、情報セキュリティ責任者が本体制図の更新を行う。

付録「情報セキュリティ関連規程」のサンプルの中の「組織内対策」のページ。

用意されたサンプルの中の赤字の部分を自社の情報に書き換えていくことで、自社の「情報セキュリティ関連規程」が完成するようになっています。

関連規程といってもなにを盛り込んでいいかわからないといったことが、このサンプルをなぞることで解決されます。

ウェブサイトに掲載するSECURITY ACTIONのマーク

セキュリティ対策自己宣言

セキュリティ対策自己宣言

SECURITY ACTIONの条件を満たした上で、これらのマークをウェブサイトに掲載することで、外部の企業などに対して自社のサイバーセキュリティに対する取り組みの「本気度」を示すことができます。

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

第 2 章

パソコン・スマホ・IoT 機器のより進んだ使い方やトラブルの対処の仕方を知ろう

パソコン・スマホ・IoT 機器の扱い方を中心に、それらの機器のセキュリティを固める手段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、難しく考えず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つながるでしょう。

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

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

なお、Windowsではリカバリメディアなどを使ったときに「プロダクトキー」の入力が必要になる場合があります。プロダクトキーは本体の裏側や付属しているリカバリメディアにシールが貼り付けられているので、紛失に備えスマホなどで写真に撮っておくか、メモに書き写して保管しておきます。

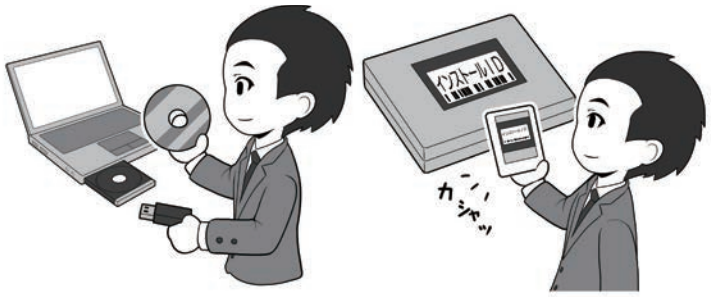
次に、セキュリティの設定をします。初期設定時にIDと「ログインパスワード※1」の設定を必ず行いましょう。また、マニュアルにしたがって起動用「BIOSパスワード」や「ファームウェアパスワード」という、電源を入れた段階で入力することを求められるパスワードも設定しましょう。

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

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生体認証でログインの手間を省きましょう。

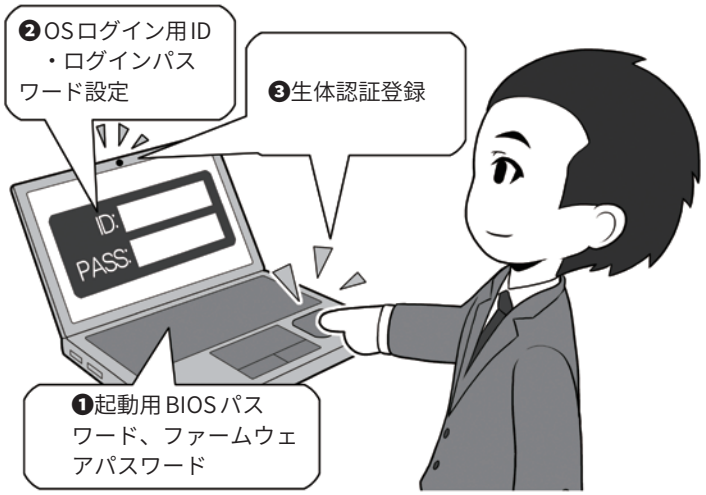
生体認証機能が無い場合はパスワードをしっかり設定しましょう。

パソコンを買ったらまずリカバリメディアを作る



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

起動用のパスワードや生体認証登録をしよう



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

※1 パスワードにはいろいろな種類があるので、詳しくはP114以降を参照

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、パソコンなどの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、机などに固定して、持ち運べないようにしましょう。

こういった状態だと、盗みに入った泥棒はパソコンの中の情報だけでも入手すべく、パソコンを壊して中の記憶装置であるハードディスクやSSDだけを盗む可能性もあります。

そのように盗まれても情報が漏れないようにするため、記憶装置は暗号化処理を行っておきましょう。

なお、暗号化機能付き外付け記憶装置の場合、使用開始時に入力するのは暗号化の鍵になる「暗号キー」になっているので、「ログインパスワード」より複雑な「暗号キー*2」のセオリーに従い、英大文字小文字＋数字＋記号で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、仮に盗んで別のパソコンに繋いでも、解読が非常に困難であり、情報流出を防ぐ力になります。

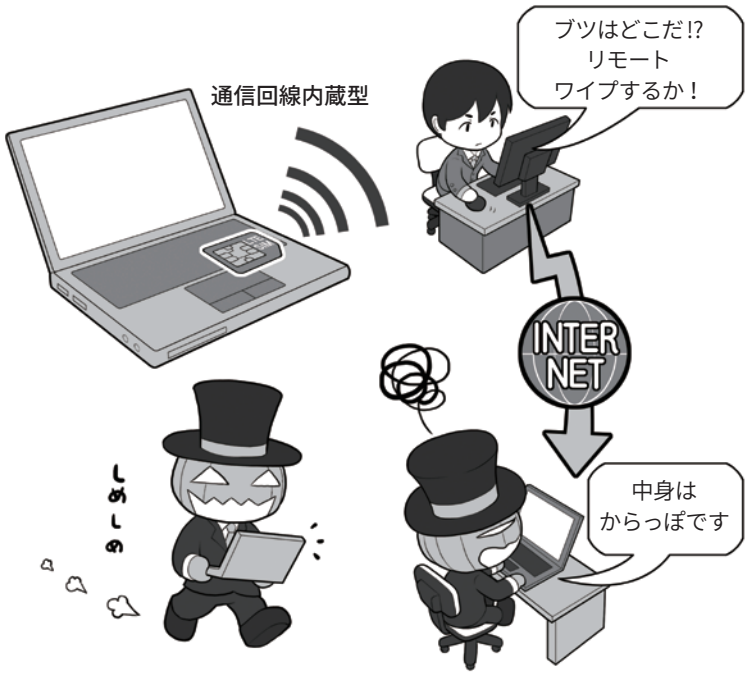
また、スマホにあるリモート(遠隔)ロックやリモートワイプは、業務用かつLTEなどの通信回線を内蔵している一部のパソコンでも可能です。特にこういった用途を前提に開発をされている機種は、相手から電源が入っているように見えない状態で記憶装置の中身を消すこともでき、重要情報を持ち出す必要がある場合は有効な防御手段となります。

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もできるので、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。

盗難にそなえて記憶装置の暗号化

TPMチップ(暗号化チップ)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、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



業務用の一部機種では、起動をさとられないステルス状態で、リモートワイプ(遠隔操作でパソコンの中身を消去)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。

※2 暗号キーに関しても、詳しくはP114以降のパスワードに関する項目を参照

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

マルウェアの感染に負けない環境を整え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、定期的なデータの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、本体含め3個以上の複製、2種類以上の記録メディアで、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。

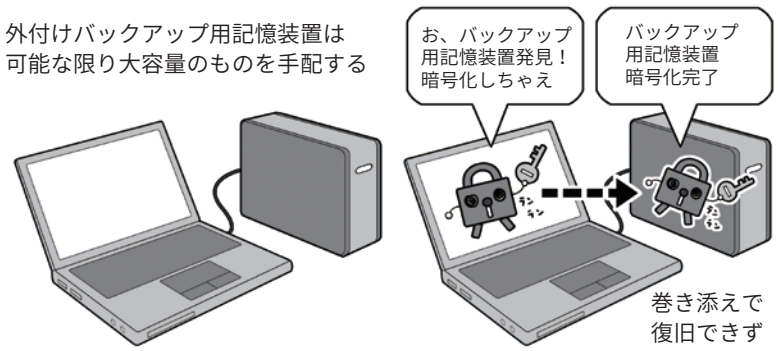
メインのバックアップ用記憶装置は外付けで、最低でも内蔵記憶装置の3〜4倍の容量にして、何世代分かのバックアップを可能にすることが理想です。昨今顕著になってきた、パソコンの中のファイルを勝手に暗号化し、解除するには身代金を要求するマルウェア（ランサムウェア）に備えるために「定期的にバックアップをしつつ、普段は本体に接続しておかない」という、やや煩雑な対応が必要です。こうすることでバックアップ用記憶装置もろとも暗号化されてしまうことを防げます。

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、重要なデータが巻き添えにならない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。

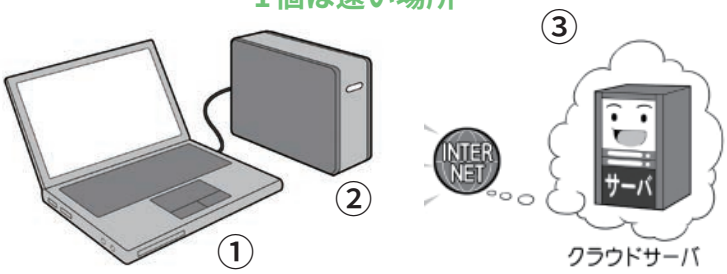
例えば、仕事相手の会社の人から「資料をコピーしてくれ」と渡されたUSBメモリにマルウェアが仕込まれていたり、パーティでプレゼントされたデジタルカメラに仕込まれていたりというケースも実際に存在します。注意しましょう。

バックアップの体制を整え、普段は接続しない



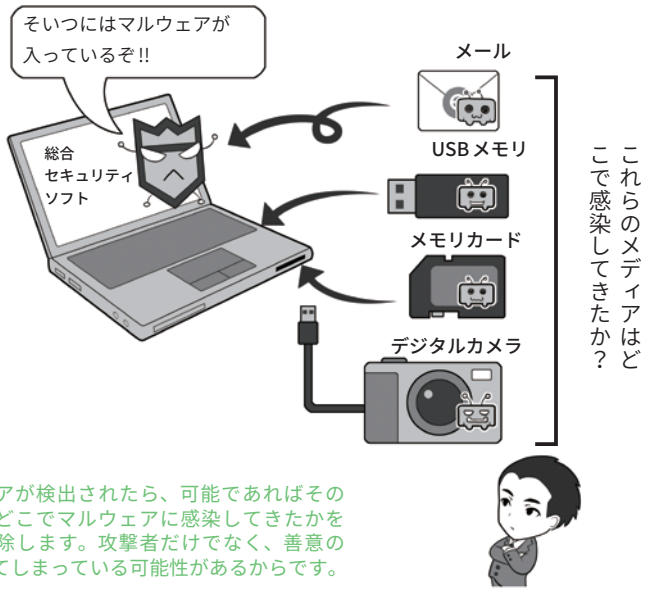
環境を整えたらシステムのバックアップを開始します。なにかソフトウェアの導入時や、環境を変更したときもバックアップします。システムのアップデート後もバックアップします。ただし、バックアップ用記憶装置を常に接続しておくとランサムウェアに感染して巻き添えで暗号化され、復旧に使うためのデータも失われてしまうので注意が必要です。

バックアップは3個以上、2種類以上の記録メディア、1個は遠い場所



このルールは、①本体＋②バックアップ用記憶装置＋③クラウドサーバで条件を満たせます。クラウドサーバは多要素認証、USBセキュリティキーなどを使って攻撃者に乗っ取られないようにしましょう。暗号化が可能なら暗号化して、共有設定をしっかり確認しましょう。

さまざま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。攻撃者だけでなく、善意の人が感染してしまっている可能性があるからです。

4 売却や廃棄するときはデータを消去する

パソコンの廃棄にあたっては、機密情報などの情報漏えいを防ぐために、内蔵記憶装置のデータを復元できない形で消去しなければなりません。特に個人情報などを扱う場合は、個人情報保護の観点から、廃棄時は確実に情報を消去する努力義務が求められています。

内蔵記憶装置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。記憶装置単体で保管していた場合などは本体に接続して消去するか、専用の機器などで消去。

データの最低限の消去は記憶装置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。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。ハードディスクの場合これに従わないと、消えたように見えたデータを復旧できる可能性が残るのです。

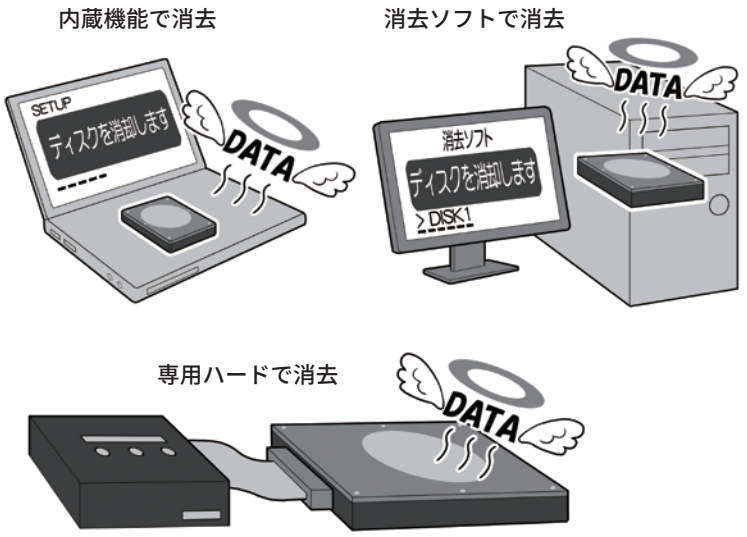
なお、SSDはデータの管理方式がハードディスクとは異なるので、生産メーカーの「Secure Erase」用ソフトを探してこれらを利用するなどの方法があります。

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、物理的もしくは磁気的に破壊する方法もあります。

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、安全が確保された環境でハードディスクを読み出し不可能に破壊するか、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。情報漏えい防止の投資です。

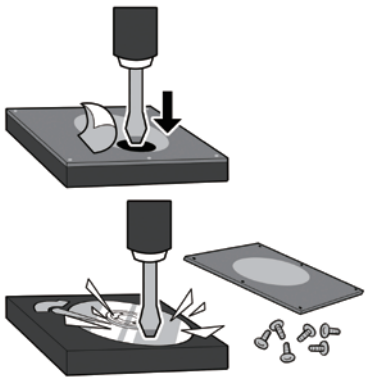
記憶装置の中のデータは必ず消去する



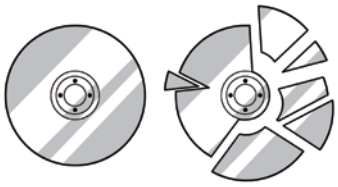
ハードディスクは、いずれの場合も最低3回以上の繰り返し消去（データ上書き）処理をするモードを選択します。SSDはメーカー製の消去用ソフトなどを使います。

動作不能、機密性確保には破壊する

①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

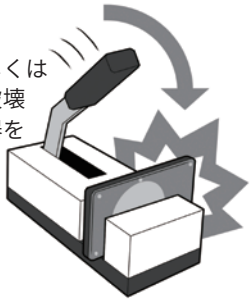


中のディスクを割るか、穴を開ける



②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他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。

2 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。席に置いて離れたり、人に貸したりするのは×

スマホの情報を守る第一歩は、待ち受け画面にロックをかけることです。

ロックには「PINコード※3」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、最近では特定のウェアラブル機器（普段身につけているスマートウォッチなど）を着けている場合や、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ができる機能もあります。

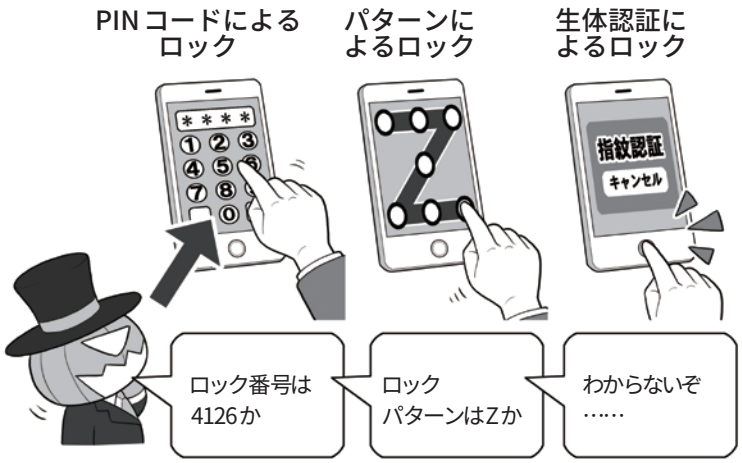
ただ、自分が明示的に指示をしないロック解除は、うっかり端末を無防備にしてしまうこともあるので、基本的にはなんらかの動作をしてからロック解除する方式にしましょう。その点では、生体認証は周りから覗かれPINコードを盗まれる危険性の排除をしつつ、入力の面倒くささを省くので便利な機能です。

なお、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、「寝ているときに勝手に指を使われ認証突破される」こともあります。過信はしないようにしましょう。

そしてセキュリティ向上のため各種のスマホロック機能を設定しても、そのスマホをロック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。

スマホは自分のすべての情報が詰まった持ち歩く金庫だと思って、必ず肌身離さず自分のそばに置き、使わないときはこまめにロックをかけた状態にしましょう。

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おそれがあります（特にロックを設定しなかったり、ロック解除したままの状態で放置）。

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

※3 PINコードに関しても、詳しくはP114以降のパスワードに関する項目を参照

2 情報漏えいを防ぐ①

SNS用のアプリなどでは、本体のPINコードなどとは別に、アプリ専用のPINコードが設定できるものもあります。盗難などの際、SNSの内容を見られたくなければ、このアプリPINコードも設定しましょう。情報の守りが二重になります。一部の機種では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というセオリーに沿っているわけです。

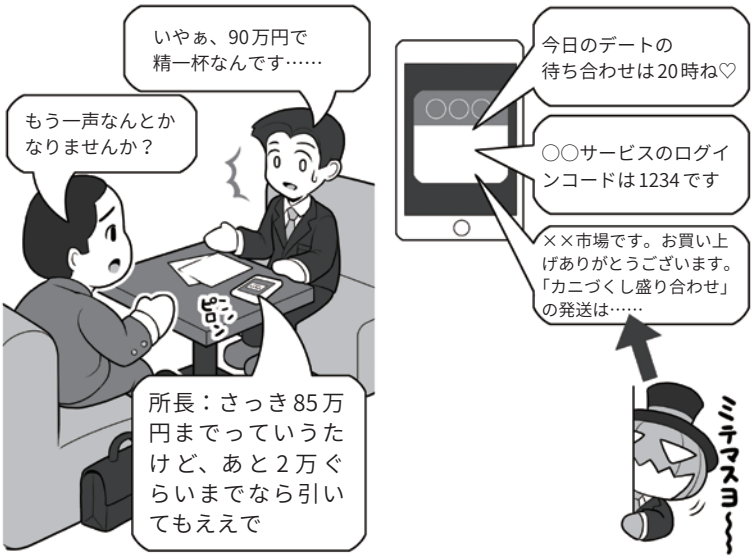
なお、アプリのPINコードを使う場合は、スマホロック解除のPINコードと異なるものを設定しましょう。PINコードの使い回しはセキュリティがないのと一緒になってしまいます。PINコードもそれぞれ異なってこそ意味があるのです。

スマホをロックしていても情報漏れが発生することもあります。

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

また、同様にロック画面にメールの内容を表示していると、せっかくセキュリティ向上のために設定した多要素認証のパスワードメールも見られてしまうことがあり得ます。そうすると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、自分が席を離れるときにスマホを残してはいけません。なお、勝手に他人のスマホのロック解除をすることは、れっきとしたサイバー攻撃です。

3 情報漏えいを防ぐ②

直接スマホを盗まれる以外の情報漏えいには、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。

P126からの無線LANの暗号化のセクションで詳しく説明しますが無線LAN利用時に注意すべき点は、

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。**

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、上記の安全性をきちんと理解してた上で、セキュリティが担保されているか精査しましょう。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ります。

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。

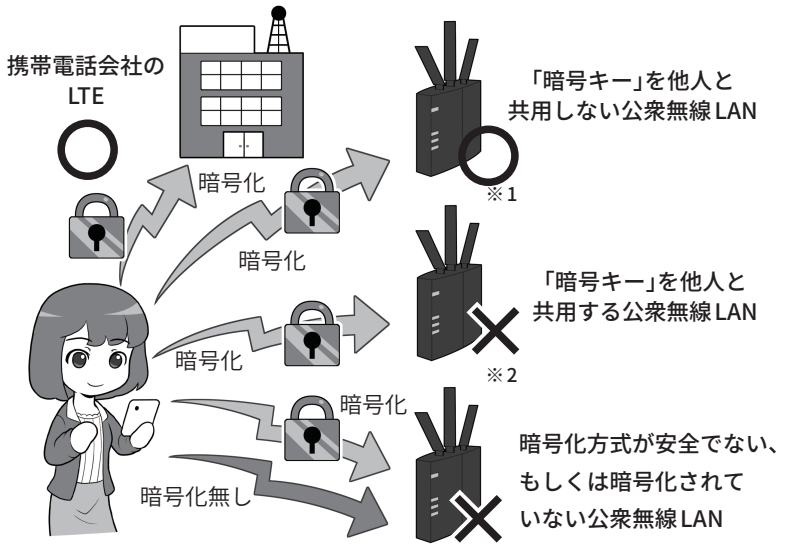
次に、業務中に万が一、スマホを落としてしまった場合に、情報を流出させない方法も考えましょう。

まずはスマホの中身が暗号化されているかチェックします。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。

スマホを落としてしまったときの対策のためには、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

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」ものは基本的に使わず、また、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、P126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。

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他のスマホやタブレット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不正利用されないよう、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、職員や会員の監視目的では絶対に使わないようにしましょう。それはプライバシーの侵害になります。

この機能は、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、自分が訪れた場所や、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、取り戻せそうになく、特に仕事上の問題がある場合は、最後の手段として情報漏えい防止のために「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。

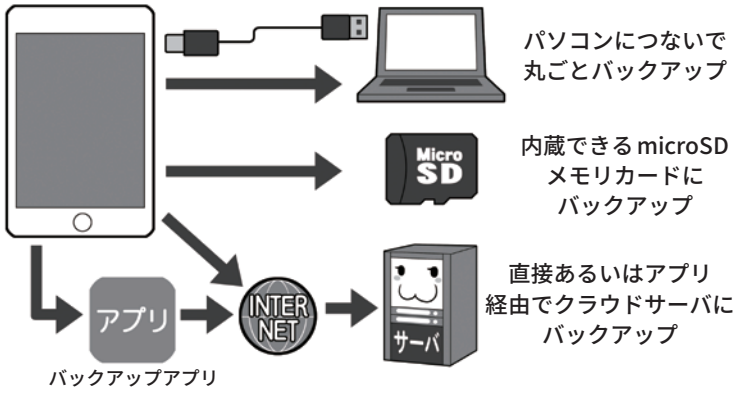
機種によってはパソコンでバックアップすると、新しいスマホをつないでボタン一発指示するだけで復元できるものもあるので、機種選定時に調べておきましょう。

紛失や盗難時のために準備をしておこう

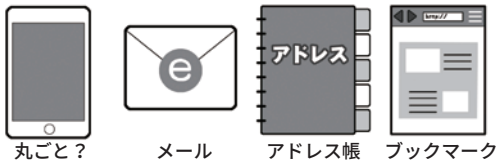
リモートワイプすると位置情報が確認できなくなるので、リスクが少ないならばロックだけ行い、遺失物として警察に相談するなどの手段をとりましょう。

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順を調べておくことが重要になります。

機種変更にはバックアップが重要ですが、「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」などさまざまな方式があります。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、記事を見たりして、どの方法が便利か、アドバイスを求めるなど、検討するといいでしょう。

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クラウドサーバ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。

一方で、本体のデータ移行手段とは別に、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。

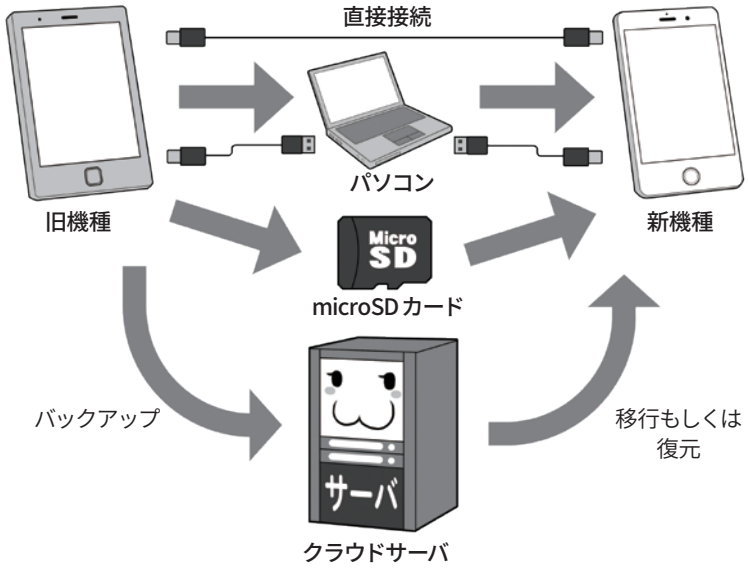
例えば、いわゆる「おサイフケータイ」に関する機能では、一旦情報をサーバ側に預け、かわりにパスワードを受け取り、スマホから機能を削除して、その後新しい機種でログインし、そのパスワードを使い機能を復元する処理が必要になるものもあります。

一部のSNSでは、旧機種がアクセス可能なまま新機種からのアクセスが有効になって、同時に複数台からアクセスできてしまうようにならないように、移行処理の前に一度手続きを踏んで、旧機種からアクセス権を削除したのち、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方式のものもあります。

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やアプリを書き出し、それぞれの移行手順がどうなっているか調べ、利用したいものがきちんと移行できるか確認をしてください。

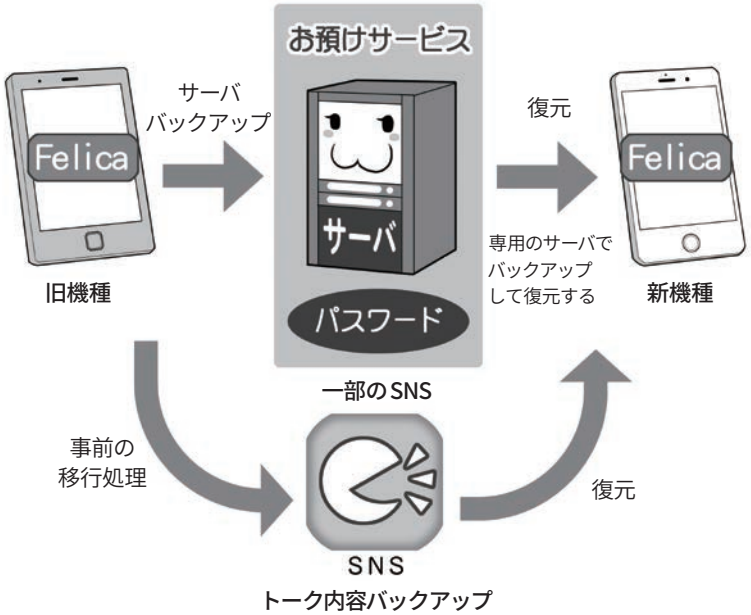
さもないと、電子マネーが旧機種とともに消えてしまって取り戻すのが困難になった、なんていうこともありえます。（職員の実話です）

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漏えいを防ぐ処理です。

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、あなたや会社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、必ずデータを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、住所録にある取引先に詐欺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。

手順としてはデータをバックアップした上で、各種サービスはアプリもウェブ版もすべてログアウトします。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。

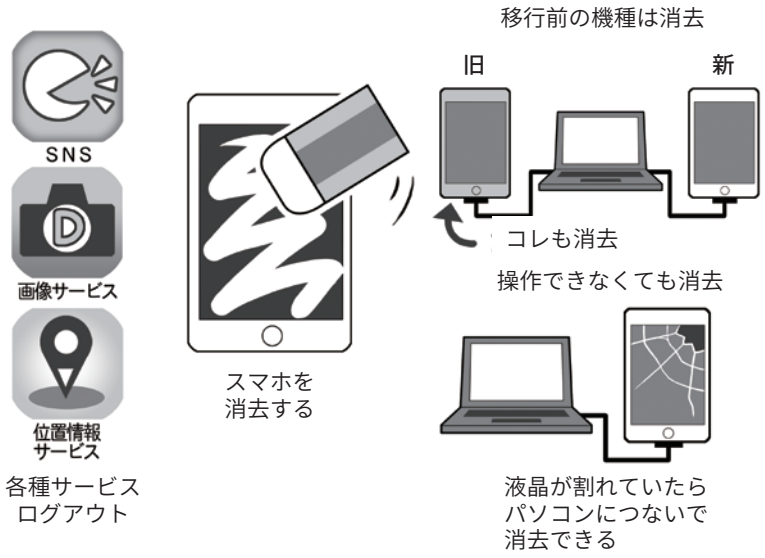
一部のスマホでは、紛失時に探せるように設定した「位置情報を確認するためのサービス」を事前にログアウトしておかないと修理などに出せないものもあるので、消去の前にログアウトを確認してください。

落としてしまって液晶が割れ操作ができない場合、消去作業を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。

なお、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、中古品を購入したりしないようにしましょう。中古販売店が良心的でも、入荷以前に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。それを避けるため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

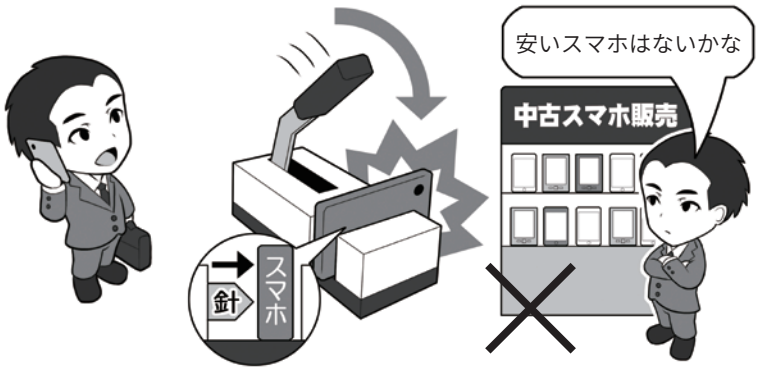


消去する前には、利用しているサービスはすべてログアウトして、サーバなどに情報を預けなければならないもの（おサイフケータイなど）は預けましょう。

SNSで移行前手続が必要なものは行い、その後移行処理をして、移行後きちんと復元できたら、旧機種を売却・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、パソコンに繋げば消去することは可能です。一部機種ではマウスを接続して操作することも可能です。

業務用のスマホは物理的に破壊する。心配ならば新品を購入し、スパイウェア混入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、販売した会社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。

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。

お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く、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います。

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ます。一方、PIN コードや指紋認証型もあります。盗難された場合に場所を特定し取り戻すにはLTE などの「通信機能内蔵型」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と、建物の施錠やワイヤーロックによる固定も可能であり、仮に盗難したとしてもノートパソコンと比較して目立たないように持ち出すのは困難です。したがって、盗難後の探知機能もノートパソコンのようには必要ないといえます。さらには、入出管理システムや監視カメラの設置、物理 IC カードを用いた未使用時のロックなどで盗難への安全性を高められます。

結果として「盗難紛失時のリカバリ手段や防御手段の少ないノートパソコン」が、盗難紛失に対し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、せめて窃盗犯が勝手に起動してデータを読み出すことができないように、BIOS 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 ×(回線非搭載)	△※2 ×(回線非搭載)	△※3 ×(回線非搭載)
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。本体が起動していないように見せつつ、リモートロック、リモートワイプを行うことには、専用設計された機種が必要

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原因を解明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。

ネットを仕事に使っているなら、通信ができなくなるのは死活問題。速やかにトラブルを特定し、別経路でのアクセスを確保するテクニックを身につけましょう。

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。

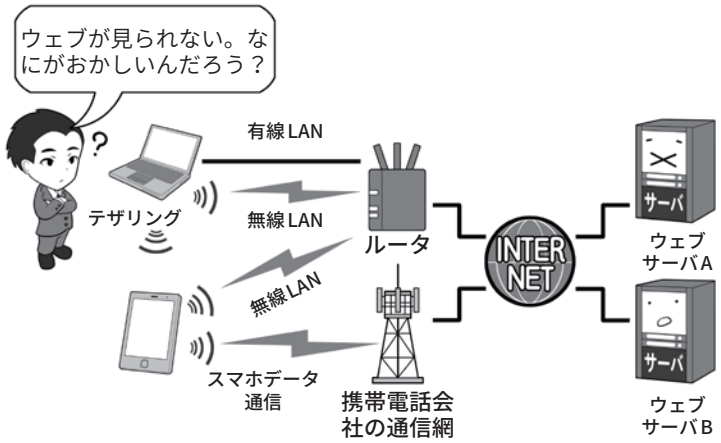
また、所有する特定の機器がマルウェアに感染したり、セキュリティホールが明らかになったアプリなどを避けてサービスを利用したりする場合も、同様の考え方になります。

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。問題があるものを積極的に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。

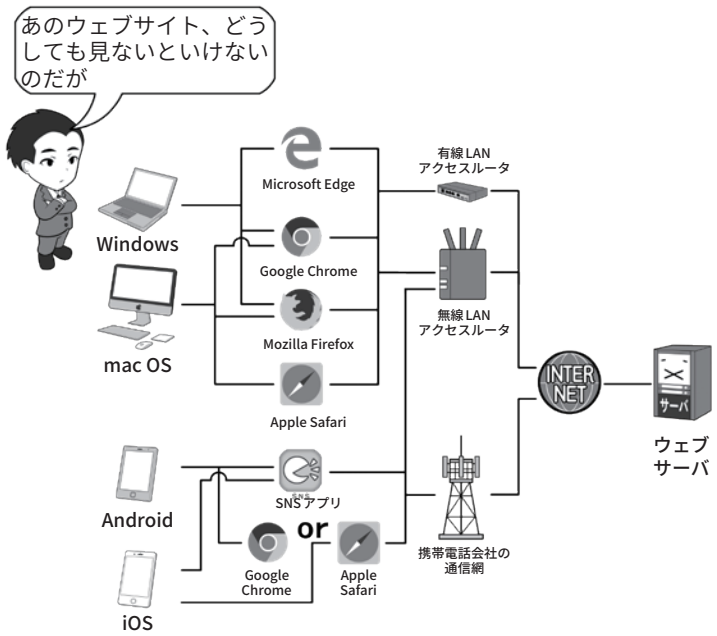
雑草のような多様な環境を作って、力強く備えましょう。

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版サービスを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なのです。

3 IoT機器のセキュリティ設定

1 流行のIoT機器だが、落とし穴も…

IoT（Internet of Things）機器とは、従来ネット接続しなかった電気機器が、インターネットに接続可能になったものを指します。例えば、従来の監視カメラはネットに接続する機能を持っていませんでしたが、IoTの監視カメラは撮影した映像をネット経由でスマホなどに送信して危険を通知するなどの機能を備えており、より便利に使うことができます。

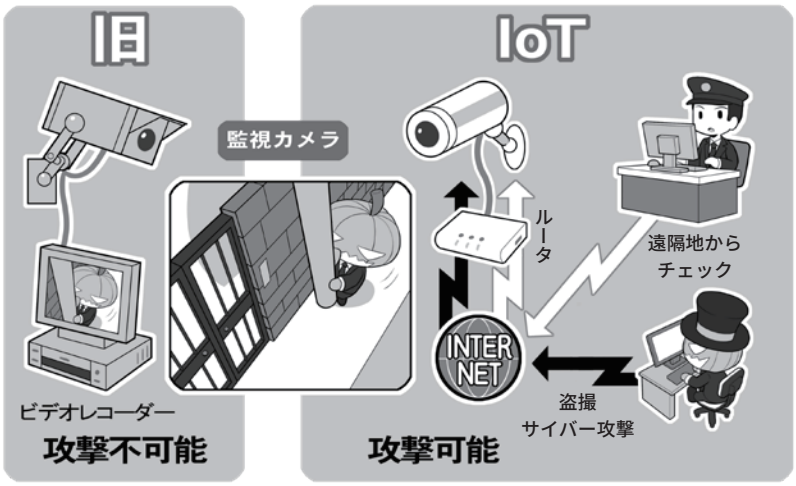
いつでもどこでも情報を受け渡しできることが喜ばれ、現在は猫も杓子もネットに繋ぐ、IoT機器ブームのような体裁になっています。

注意したいのはインターネットにつながるということは、インターネット上にいる、世界中の攻撃者から攻撃対象になりうるということです。例えばIoTの監視カメラであれば、攻撃者がセキュリティホールを突いて乗っ取り盗撮カメラとしても使うことができるわけです。

これを避けるためには、セキュリティを固めファームウェアを最新にすることなどが必要になります。

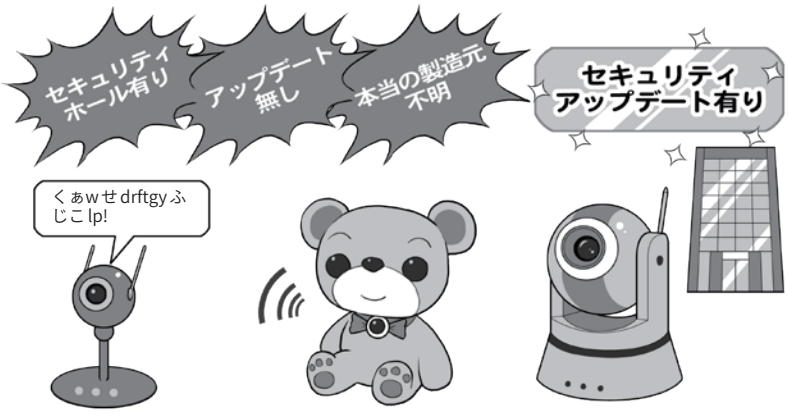
もう1つ留意したいのは、IoT機器の販売がブームとなり、さまざまな企業が参入する状況でありながら、その企業すべてがサイバーセキュリティについて詳しかったり、防御することに十分留意して設計を行っているわけではない点です。中には明らかにスパイカメラのように、情報を不正に外部に送信するようになっているものすらあります。

IoT機器に進化するとセキュリティ上のリスクも生む



従来の監視カメラは有線接続された録画機器でしか確認できませんでしたが、IoT機器化することで、遠隔地からチェックできたり、問題が発生すればスマホで通知や映像を受け取ることもできるようになりました。しかし、代わりにサイバー攻撃を受ける可能性も生まれたのです。

市場が広がったがセキュリティ上危険ない商品も増えた



他国語での声が聞こえるホームカメラ（製造元がよく分からないものも）

盗聴・盗撮の脆弱性が指摘された、カメラ付きぬいぐるみ

ネットワーク製品を出してきたセキュリティ企業製

IoT機器がブームになることで、従来ただの電気製品だったものにネットワーク機能が搭載され、市場にネットワーク機器があふれかえる様になりました。しかし、このように登場したIoT機器は、ネットワークのセキュリティの知識が乏しい企業による、ブームに乗っただけの商品の場合もあり、セキュリティホールがあっても対処されず、アップデートが提供されるウェブサイトも不明、それどころか、本当の製造元はどこの国の何という企業なのか判らないものもあります。ネットワークに接続する製品は、セキュリティのリテラシーが高い企業のものを購入しましょう。

IoT機器はきちんとしたネットワーク機器を生産した実績がある企業のものを優先して選択することが現状の安全策です。

2 購入後は初期パスワード変更などの設定を

前項のように悪意を持った設計と思われる製品はさておき、その他にも攻撃者の危険にさらされる可能性のある要素は対処しておきましょう。

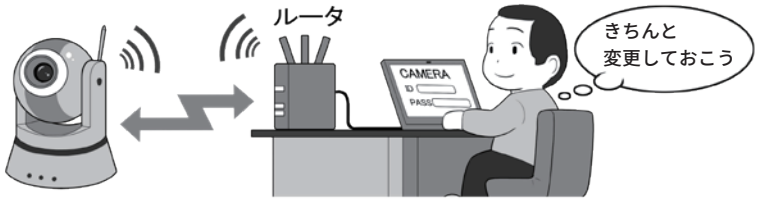
まず、ウェブブラウザで機器の設定画面にアクセスするための、管理者用パスワードは出荷時の状態から必ず変更しましょう。機種によってはそのモデルすべてで同じパスワードが設定されていたりするものもあり、格好の攻撃対象となります。それが自社に設置したカメラだった場合、どういったトラブルが起こりうるか、想像して下さい。

また、ネットワークの設定も適切に行う必要があります。IoT機器を意図せずインターネットに公開する可能性のある「UPnP」などの機能は基本的にオフにして、必要な機能を精査して使うようにすべきです。これは社内などのネットワークと外部のインターネットの境目にあるルータでも同様に設定します。

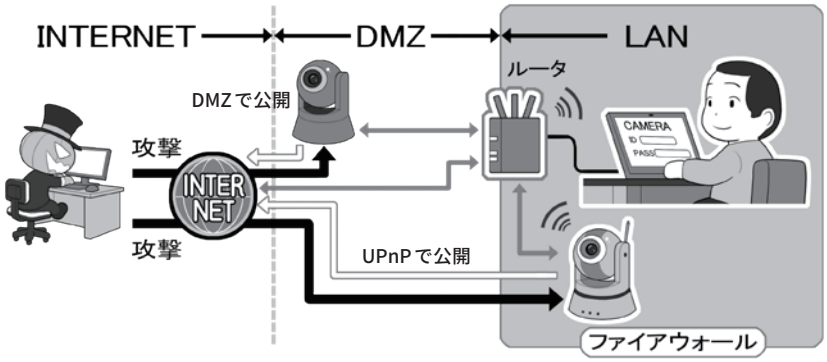
IoT機器は記憶容量が少なく、パソコンなどのように総合セキュリティソフトをインストールできませんので、きちんと管理しなければなりません。そのためにルータ自体がIoT機器に対応した、包括的なセキュリティ機能を持つ「ホームネットワークセキュリティルータ」などの製品も市販化されています。外部からの攻撃だけでなく、IoT機器が勝手に外部に情報を送信しないように、監視できる体制を整えましょう。

ただ、いうまでもないことですが、IoT機器に関する一番のセキュリティ対策は、ネットワークに接続する明確な理由のない機器は、そもそも接続しないことです。

初期の管理者パスワードは変更する

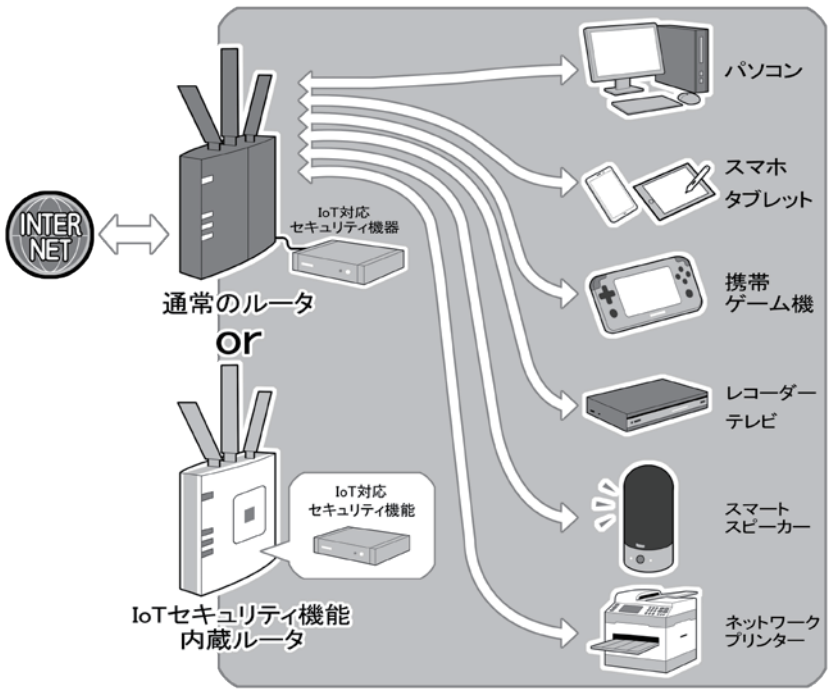


IoT機器を導入したら不正アクセス防止のため、まず初期の管理者用パスワードは変更しましょう。大抵の場合、ウェブブラウザ経由でIoT機器にアクセスして変更するようになっています。



そのほかにも、インターネットに対してLAN内部の機器を公開してしまう可能性のある、UPnP機能はオフにして、インターネット側(DMZ)にIoT機器を設置することもやめましょう。いずれも攻撃者からIoT機器へのアクセスが容易になるからです。

小さい会社などならホームセキュリティ機能内蔵ルータも



IoT機器はパソコンやスマホと異なって、記憶容量が小さいためセキュリティソフトなどを導入することがほぼできません。したがってサイバー攻撃に弱く、また、モニターなどがないため機器の状態をチェックしづらく、乗っ取られてもこれを察知することが難しいのです。そういった状態を察知するために、最近ではIoT機器に対する監視機能を持った装置を、インターネットの玄関口になるルータに接続したり、あるいはルータ自身の中にそういった機能を内包するものがあるので、これらの導入を検討しましょう。こういった装置はIoT機器などLAN内の機器を監視し、不自然な点があれば連携したスマホのアプリなどで確認できます。

コラム：究極の防御手段、エアギャップ

小さな会社やNPO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、セキュリティ上の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、十分な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そのパソコンにUSBメモリを挿せないように、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。

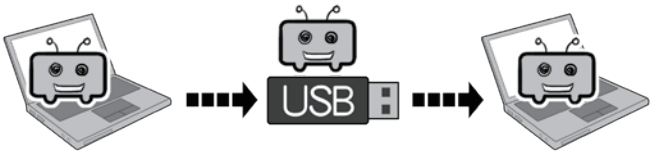
要するにこれらのものを使ってモールス信号を打つことで送信する、といわれればイメージが湧くでしょうか。

話題を戻してエアギャップを

有線でも無線でも、つながっていないパソコンは（基本的に）マルウェアに感染しない

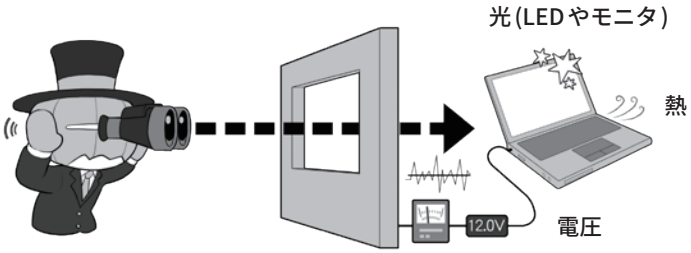
スタンドアロンパソコンの中にある情報を奪取しようとすると、現物のパソコンを強奪するしかなく、（攻撃者にとって）危険（＝コストがかかる）となります。

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。

インターネットバンキングの不正送金の例にあ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、日々さまざま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えませんし、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るため、その情報をたぐって現実世界の攻撃者の場所までたどり着き、証拠を固めた上で相手を捕まえることが容易ではないからです。

特に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、一方で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、要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りとあらゆる所にATMが設置され24時間稼働していますし、24時間送金可能な手段もあります。

したがって、多量の送金処理を毎日行うのでもなければ、インターネットバンキングを使うことは「便利」ではあっても「必須」ではありません。

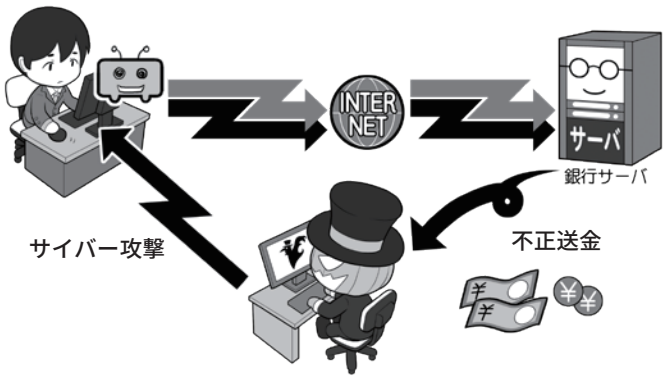
そしてネットを利用しない場合、攻撃者が不正にお金を奪おうと思えば、現実世界でキャッシュカードとあなたの身柄を抑えて、暗証番号を聞き出さなければなりません。

そのようなことをすれば当然のように攻撃者の顔もばれますし、現実世界に移動の痕跡も残ります。したがってリスク(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。

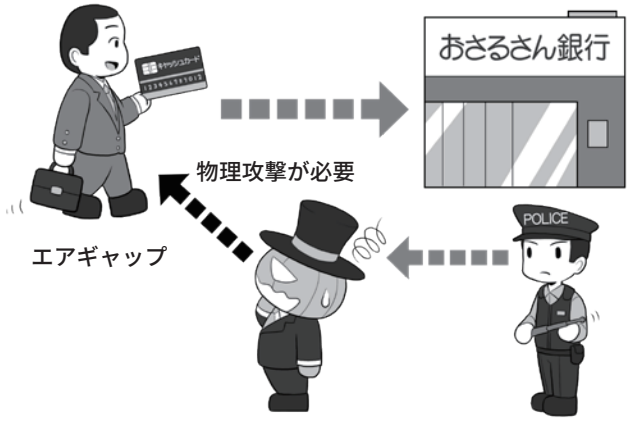
ネットにつなぐのは「便利」の物差しだけで考えるのではなく、「利便性」と「危険性」を天秤の両側に乗せ、総合的に安全な選択肢をとるべきでしょう。

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完結していること、攻撃者がネットの闇に潜んでいられること、そのため国内はおろか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、無料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。広告主がウェブサイト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、趣味や行動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。

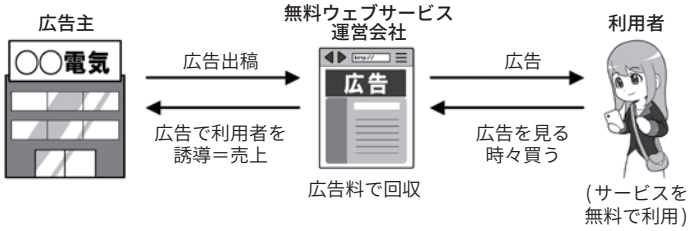
また、先行投資といって、当初無料で提供し、利用者がサービスに馴染んだら、その後有料化してコストを回収するマネタイズを行う型もあります。

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

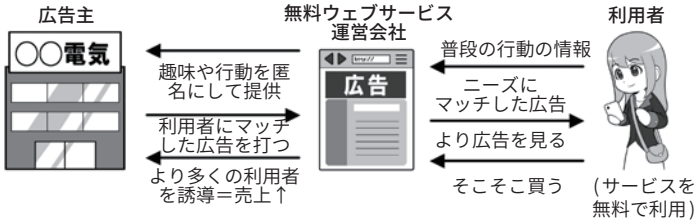
試食コーナーのサービスコスト の例

無料ウェブサービスの例

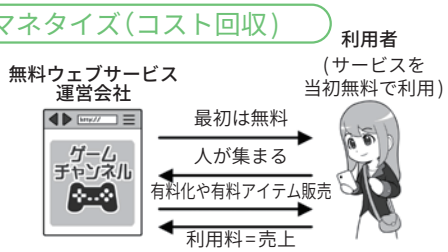
①無差別広告で運営



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（コスト回収）



④セキュリティ意識の低い善意の無料サービス

アプリなどを開発し無料で提供するのですが、明示的ではなくても「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。

そして今回も問題なのは「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、それは自宅用や仕事用のものを無料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、利用する側は安全性を求める権利もないわけです。

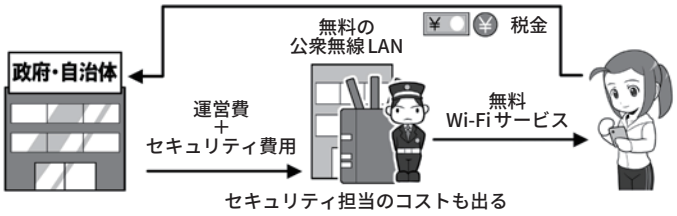
そして攻撃者はこのような所を狙って罠をしかけてきます。運営費もセキュリティ費用もないならば、誰も日常的に攻撃者が忍び込み罠を張っているかどうかなどチェックしないからです。

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、セキュリティ意識の低い、無料の公衆無線LANは推奨されない」というわけです。

無料という言葉には注意が必要です。運営されてる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。

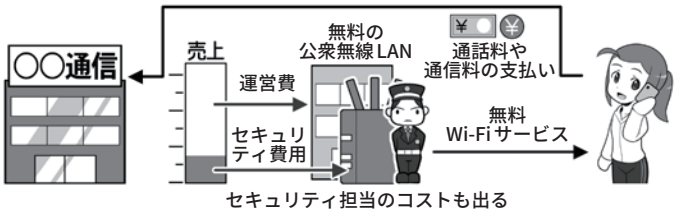
無料の公衆無線LANサービスの例

①一見無料だが税金などでまかなっている間接的に有料



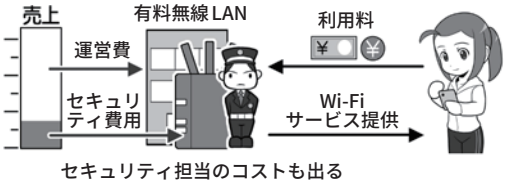
トラブルがあると議会などで取りあげられ問題となることもあります。責任能力もあります。

②企業が収入の中から払っているから（追加料金）無料



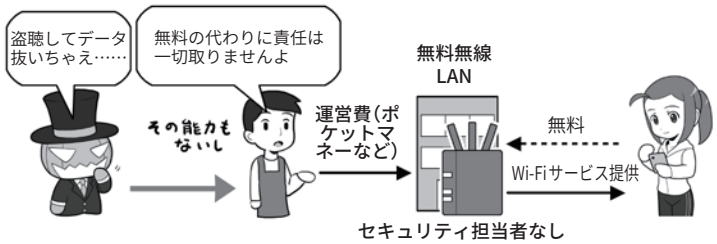
トラブルが起きれば責任問題となり、本業にも影響が出ます。責任能力もあります。

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セキュリティ意識の低い善意の無料サービス



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

コラム：クラウドストレージサービスからのデータ流出。原因は？

クラウドストレージサービスとは、「従来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、雲のように存在しているサーバに保存し、ネットに繋がったどの機器からでも、意識せずに利用できる」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。

実際には、サーバは雲や霞ではなく、どこかに歴然と存在していますし、この概念自体は昔から存在しているので、「意識せずに使える」≒「便利である」ことを「クラウド（雲）」と例えたあたりが、ポピュラーになったポイントでしょう。実際はそれぞれのサービス名で呼ばれています。

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バ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の機器からでもアクセスできるメールサービスも、クラウドの利用ともいえます。

パスワード管理アプリ※4の記事では、クラウドを利用することに関して厳しく書いていますが、クラウドサービスは、その性格を理解した上で利用するなら大変便利なものなのです。

一方、問題なのはクラウドストレージサービスからの情報流出です。攻撃者がシステムを攻撃して大規模に情報を奪取することもないとはいいませんが、ニュースを賑わす話のほとんどは、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たケースです。

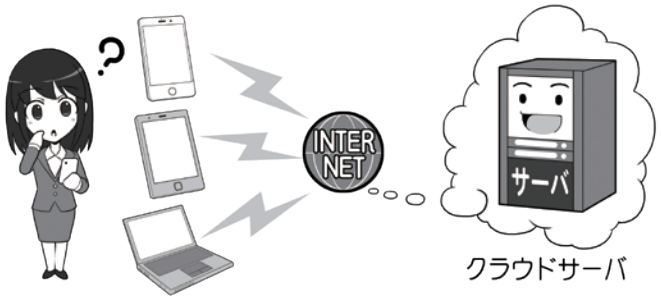
ここでの攻撃とは、「リスト型攻撃」「辞書攻撃」※5、そして個人情報からの推測などです。

他のサービスとIDとパスワードを使い回していて、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。そして、推測されるほど簡単なものにしないこと。セキュリティの強化を目的として多要素認証などや、不正なアクセスがあった場合通知されるサービスを可能な限り導入すること。そして「流出して困る情報は、セキュリティを固めずにクラウドサーバにアップロードしない・（自動で）されないように設定する」ことです。

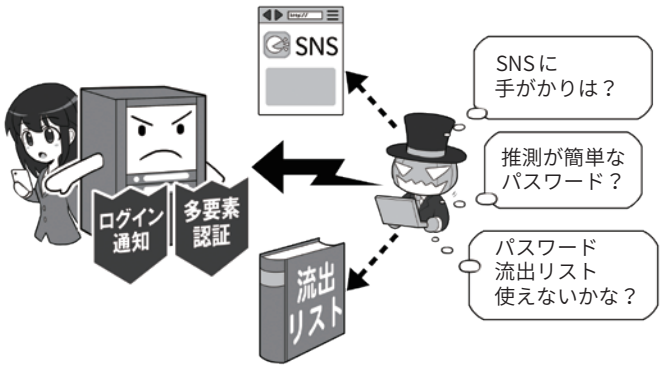
クラウドは大変便利ですが、きちんと利用目的とセキュリティを固めて利用しなければ、攻撃者の格好の的になると、理解してから利用しましょう。

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、全く意識せずにクラウドサーバにデータをバックアップしていることもあります。よく分からない場合は、一度調べてみましょう。「クラウド」という名前ではなく、それぞれのサービス毎の名前をつけられている場合もあります。

パスワードが甘いと流出するかも



攻撃者はクラウドサービスのパスワードを破るために、さまざまな攻撃を試みます。「ログインパスワード」の基準でパスワードを設定するなど、パスワード設定の基本を守るとともに、サービス間で使い回しをせず、多要素認証の設定や不正なログインがあった場合に通知を受け取れる設定を活用しましょう。

※4 P29,P118,P119参照　※5 P116参照

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

第 3 章

被害に遭わないために、加害者的立場にならないために

サイバー攻撃に遭っても、被害は自分や会社が持つお金や情報を奪われてしまうだけと思っているかも知れませんが、実はそれだけではありません。

攻撃者に乗っ取られた IT 機器が、第三者への別のサイバー攻撃に利用されたり、フィッシングメールの発信元に使われ、油断をした知り合いや取引先が二次被害に遭ったりするからです。

そういう被害を拡散しないためにも、公衆衛生的なマナーとして、セキュリティをしっかり固めなければならないのです。

1 攻撃者に乗っ取られるとこんなことが起こる

1 被害に遭わないために。そして加害者的立場にならないために

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

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

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

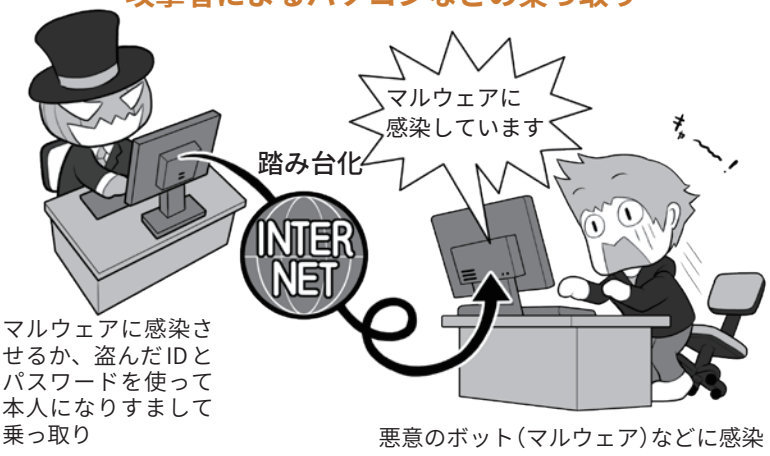
こうすることで、万が一サイバー攻撃がばれたとしても、最初にあなたが調べられ、その間に攻撃者は証拠隠滅などをして姿をくらますことができるわけです。

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

そうならないためにも、公衆衛生的なマナー意識を持って、パソコンなどのセキュリティはしっかり固めましょう。

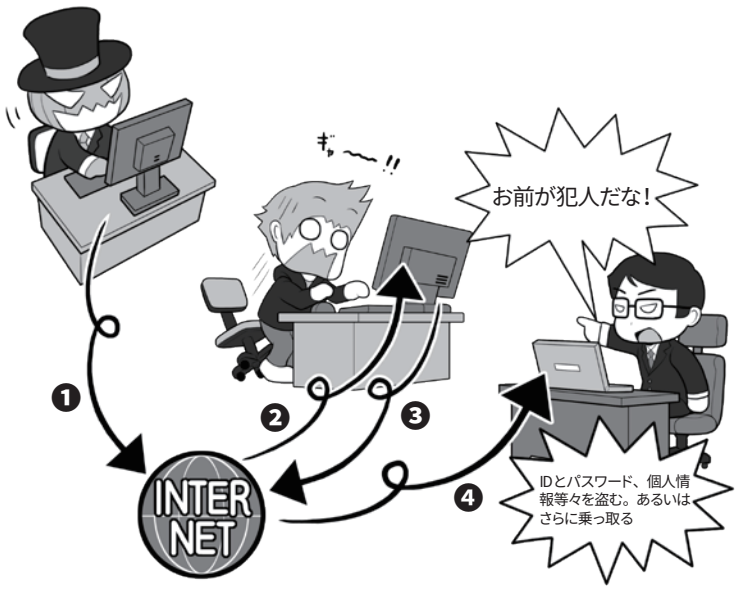
もしセキュリティソフトが、マルウェアに感染していることを検出したら速やかにネットから切断し、実害の出ている攻撃に関して、警察などから協力の要請があった場合は証拠保全(P82参照)を行いましょう。

攻撃者によるパソコンなどの乗っ取り



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

乗っ取ったパソコンを踏み台にしてサイバー攻撃を行う



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

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

2 盗まれた情報は犯罪に使われる

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

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

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

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

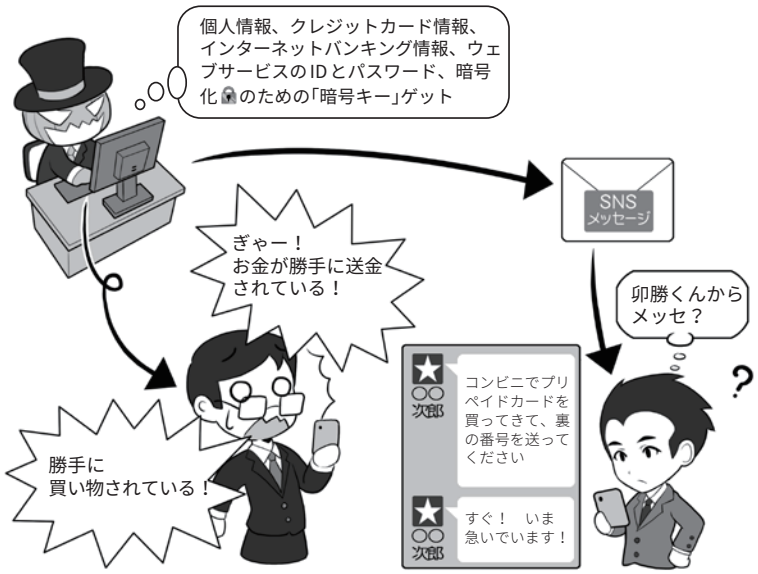
SNSのメッセージであなたになりすまし、友だちに対して「プリペイドカードを買って、アクティベーションコードを送ってくれ」と依頼して、電子マネーをだまし取る場合もあります。

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。

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

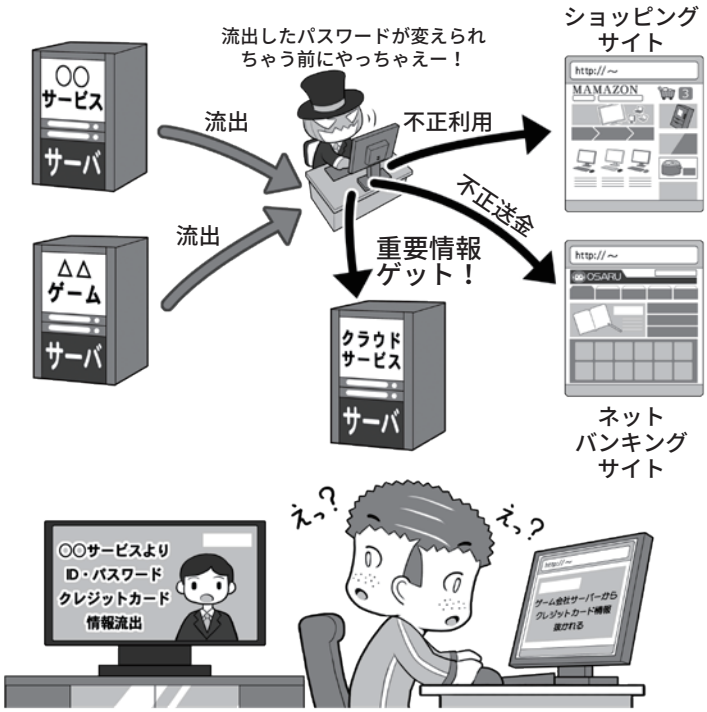
パスワード流出が判明したらパスワード設定のセオリー(P28参照)にしたがってすぐに変更し、クレジットカード情報が流出したらカード会社に連絡してカードの番号を　変更しましょう。

情報が直接盗難される場合



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

情報が間接的に盗難される場合



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

3 乗っ取られた機器はサイバー攻撃に使われる

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

サイバー攻撃の「踏み台（身がわり）」に使われるほか、「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。

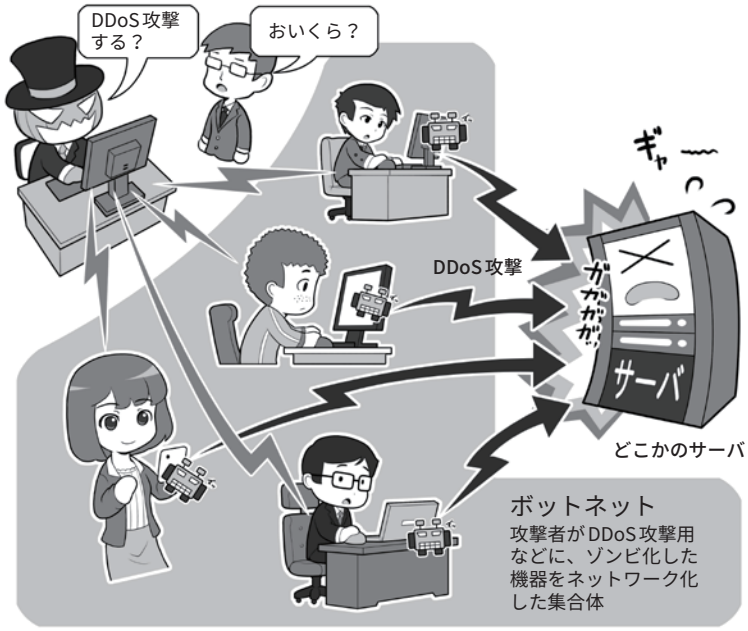
このボットネットによる攻撃は、攻撃者が自分の技術や主張を誇示する行動などにも使われますが、ボットネットを利用して攻撃を行いたい人物に、時間あたりいくらで貸し出されたりもします。攻撃者は乗っ取った人の財産（パソコンなど）を勝手に貸し出し、違法にお金を稼いでいるわけです。

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、会社や事務所に設置されている、暗号化されていない、もしくは暗号化や暗号キーの設定の甘い無線LANアクセスポイントを探し、見つけるとこれに侵入して利用する手法があります。

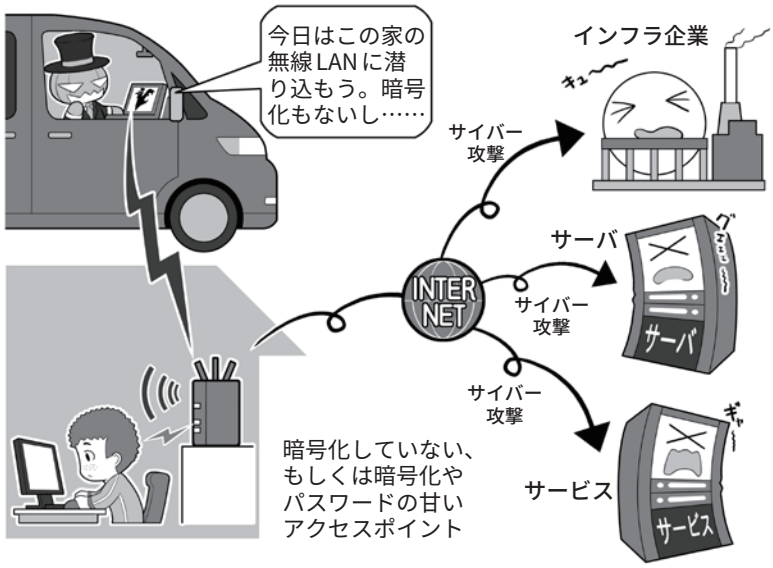
これはアクセスポイントを「踏み台」にし、そこからインターネット上のさまざまなサーバやインフラ企業に攻撃をしかけるためです。攻撃をしかけてきているのは「踏み台」がある場所と見せかけて身代わりにし、攻撃がばれたときの追跡を逃れるためです。

乗っ取られたマシンはボットネットとして貸し出される



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

無線LANに侵入され罪を押しつけられることも



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。

この場合、攻撃者に非があるのが当然ですが、会社や事務所からサイバー攻撃が行われ、インフラ企業などで事故が発生したら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。

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IT機器はいずれも、乗っ取られて攻撃者の身代わりにされる「踏み台」化、DDoS攻撃のボットネットへの接続、マルウェアの拡散など、さまざまなサイバー攻撃に利用される可能性があります。

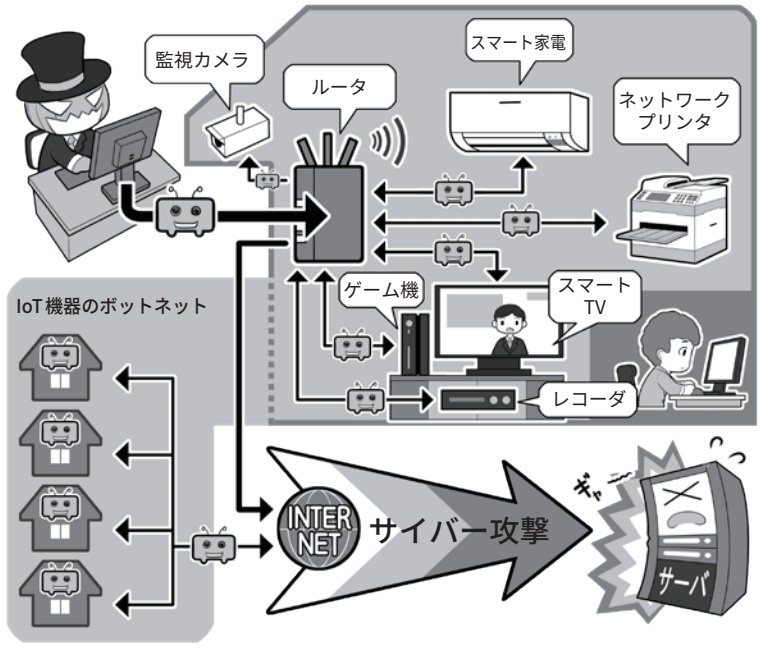
特にIoT機器は、監視カメラやネット対応電子機器などのように、普段私たちがあまりセキュリティについて気にかけないものであり、パソコンほどサイバー攻撃への対応能力も高くありません。そして一つの機種で生産台数が多い＝手間をかけずに多数を一気に攻撃できる「攻撃しやすい条件」が揃っているのです。

最低でも、IoT機器の出荷時の「管理者用パスワード」などはパスワードセオリー(P28 ,P114)にしたがって変更し、システムは最新に保ち、ネットにつなぐ必要がないものはむやみに接続しないようにしましょう。

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

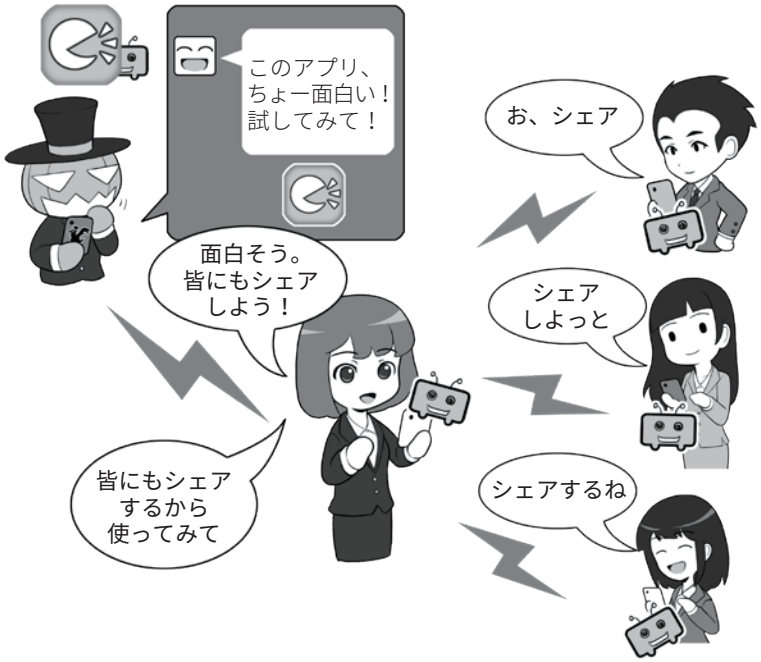
ネットでなにか行動する前には、必ず「それは本当に必要なのか」「そうすることでなにか問題が発生する可能性はないのか」をいつも注意しましょう。

IoT機器も乗っ取られ攻撃に使われる



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

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、その投稿にあるリンクの先にはフィッシングサイト用意されていたり、ゼロデイ攻撃のマルウェアが仕込まれていたり、アプリであればマルウェアが入ったものだったり、そのときは違っても、のちのちそう変化するアプリかもしれません。拡散する前によく考えて「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ないからです。

5 サプライチェーン攻撃の踏み台にならないように

P66やP68に書いたような、アカウントの乗っ取りとともに、気を付けなければならないのが「サプライチェーン攻撃」です。

「サプライチェーン攻撃」とは攻撃者が、セキュリティが堅牢な大企業を直接狙わず、その企業の業務上や製品調達上の関係があり、かつセキュリティが堅牢でない企業を狙うなどして、攻撃を仕掛ける手法です。

業務上繋がりがある場合は、乗っ取った企業の従業員のアカウントから、メールをダウンロードして、取引先の相手の氏名やメールアドレスを盗み出し、日常的にやり取りしている文面を模倣して、マルウェア付きのフィッシングメールを送り付けます。

場合によっては、その人物のアカウントそのものからメールを送る場合もあるため、受け取る側はフィッシングメールを疑う手掛かりがなく、引っかかってしまう可能性が高くなります。

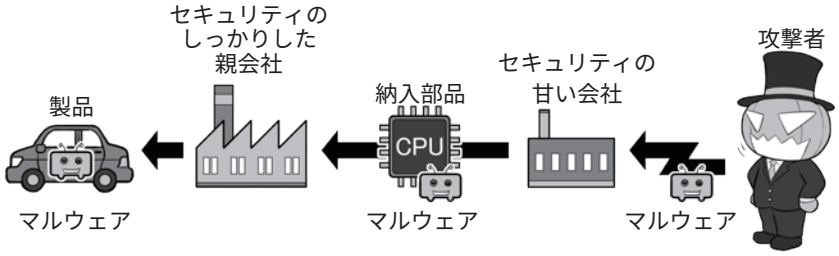
また電子機器を生産している企業などでは、生産しているIT部品にマルウェアやバックドアを仕込み、これを大企業に納入させることで、大企業が生産している製品を乗っ取る環境を整えるなどします。

例えば大企業に納入する部品がネットワーク部品で、大企業が生産する最終製品がパソコンだったとしたら、どのようなことが可能になるか、想像してみて下さい。

まさに諺の「将を射んと欲すればまず馬を射よ」と同じ作戦なのです。

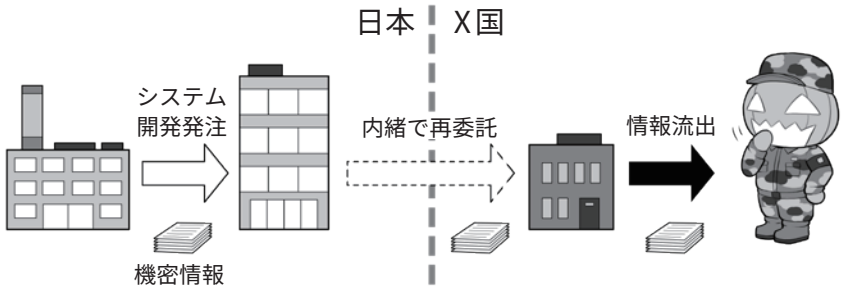
小さな中小企業や団体だから、サイバーセキュリティなど関係ないなどと考えず、こういった攻撃に遭うと、責任を負わせられることがあることを認識しましょう。

①サプライチェーン攻撃とは



サプライチェーン攻撃とは、最終的な攻撃目標を生産している、セキュリティが堅牢な企業を狙うのではなく、そのサプライチェーン(供給の連鎖)の工程の、弱い企業や弱い場所を狙って攻撃を仕掛け、最終的な攻撃目標に、マルウェアなどを仕込む手法を指します。イラストでは車(ハードウェア)が狙われていますが、ソフトウェアであっても同様ですし、考え方として誰かのアカウントを乗っ取るときにも使われます。

②オフショア開発とは



オフショア開発とは、ソフトウェアの開発するときに、受託した企業が依り開発コストが安い海外の企業などに再委託することを指します。しかしこの再委託先が我が国と同じ倫理感や法治の概念を持たず、モラルが低い場合、サプライチェーン攻撃を仕掛けられる場合があります。問題は受託企業が発注企業に内緒で再委託している場合あり、発注者はセキュリティ上、開発がどこで行われるか、契約で定め、掌握する必要があります。

●データの不正国外通信と思わぬオフショア開発

明示的なサプライチェーン攻撃以外にも、気付かぬ所で情報の漏えいを起こすケースにも気を付けましょう。

使用するIT機器が、利用者の意に沿わぬ形で情報を勝手に国外に漏えいさせるケースもあります。

通信機器やドローンに関連したサイバー攻撃が取り沙汰されているほか、外部から不正にIT機器へのアクセスが可能となるバックドアの設置も話題になっています。

機器を購入するときは、当該の会社の製品が、類似のトラブルを起こしていないか、入念に調べてから手配しましょう。

また外部にプログラムやIT機器の開発を委託する場合、詳細が開示されないうちに、情報の取り扱いが厳密でない外国に対して、「オフショア開発」で業務が再委託されるケースがあります。

こういった場合、発注者のあずかり知らぬ所で、情報漏えいやシステム上にバックドアを仕込まれてしまう可能性があるので、契約時にはそういったことがないように、取り決めをしておきましょう。

6 問題が起きると事業継続に影響を及ぼす

攻撃者によるサイバー攻撃だけでなく、十分に気を付けなければならないのは内部の人間、およびそれに準じる人間によるサイバー犯罪です。

現実にあった例を下敷きに説明しましょう。

とある会社で営業機密や顧客情報の流出が発覚しました。その犯人は過去にその会社に在籍していた人物で、特に複雑なハッキングをせずに、在籍時のアカウントを使ってアクセスし、情報を抜き取ったのでした。

退職者のアカウント管理をきちんと行っていなかったために発生したケースと言えます。

また、回線を使った侵入すら行わないケースもあります。

とあるサービス業から顧客情報が約数千万件流出するという事件が発覚しました。

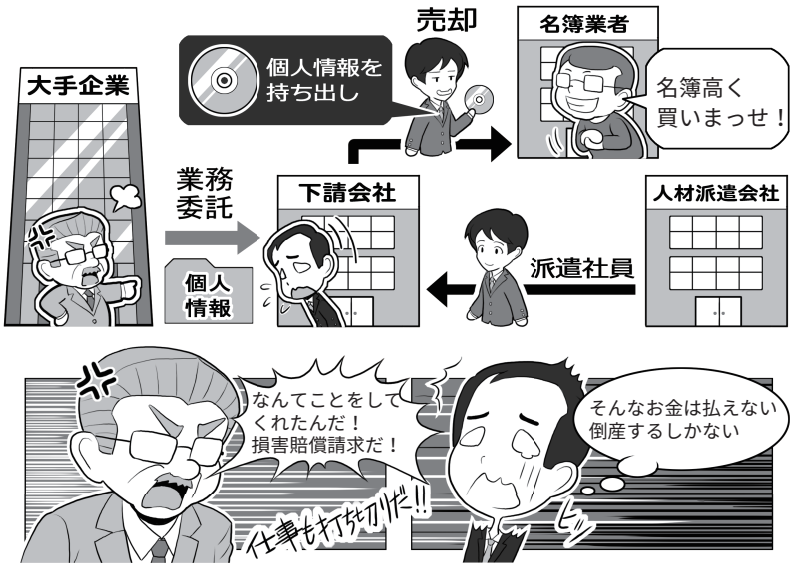
その会社自身が流出に気付いたものではなく、流出した名簿を使って顧客にダイレクトメールが届くようになったことで、間接的に数千万件の顧客情報流出が発覚したものです。

情報流出は親会社から業務委託された情報処理系の子会社から、外部の派遣社員のエンジニアが顧客データを持ち出し、名簿業者に不正に転売した結果起きたものでした。

本件は、クラッキングなどを行ったサイバー攻撃によるものではありませんが、内部犯行者によるれっきとしたサイバー攻撃でした。

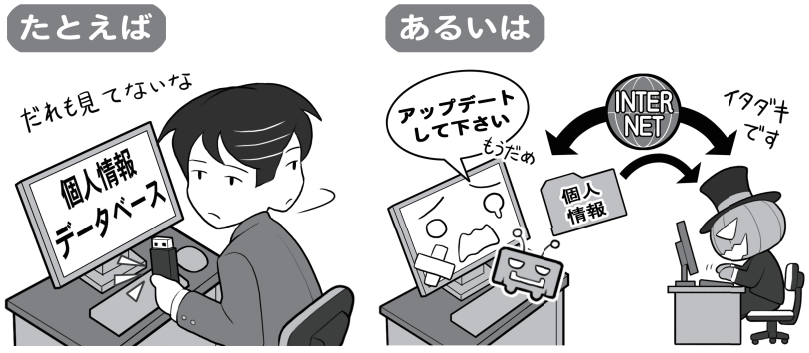
これにより親会社は顧客に数百億円相当の補償を行い、また、子会社は事業継続が困難となって翌年に解散。犯人は当然のことながら逮捕、責任を負うべき立場にいた役員が引責辞任となりました。

受託事業の機密情報を流出させてしまった



受託事業で預かった機密情報や個人情報なども、IT機器を導入していると、目立たずあっという間に持ち出されたり、流出してしまったりします。上記のイラストでは、外部から来た派遣社員の例ですが、ソーシャルエンジニアリングを使って会社に入り込んだり、社員を騙して送らせたり、あるいは外部からサイバー攻撃を行い社内や団体内のコンピュータなどを乗っ取って流出させたり、その可能性はいくらでもあります。こういったトラブルが発生したとき、相手先や顧客への不利益はもちろん、会社として受ける損害は計り知れません。

なぜこれがサイバー攻撃なのか？



外部の人間が機密情報の入ったパソコンに、USBメモリを挿して情報をコピーして持ち出した。ネットワーク越しに受けるサイバー攻撃だけでなく、こういった物理的な盗難も広義のサイバー攻撃です。サイバー攻撃とはネット経由に限らず現実世界も含むのです。

盗難されたデータはその先で、また、別のサイバー攻撃を生みます。例えば盗んだ名簿が現実世界の名簿屋やダークウェブ上のダークマーケットで販売されると、その名簿を買った別の攻撃者が、スパムメールなどを使ったサイバー攻撃に用いる可能性があるのです。

このケースでは親会社と子会社の関係でしたが、これが資本関係のない契約企業だった場合、損害賠償請求が行われたかも知れません。

ましてやこれが、社員数名しかいない中小企業だったら、金銭的賠償は不可能でしょうし、NPOだった場合は、高い意識を持って始めた事業であっても、情報流出を起こしたことで信頼を失い、その目的の達成を断念せざるを得ない事態に陥ったでしょう。

2 よくある攻撃の手口と対策

1 標的型メール攻撃の具体例と対策

「お盆休み明けに出社して、すぐにメールを開くと、提携先の会社のAさんから、次回のミーティングに関してのレジュメが添付されてきていた。ミーティングは当分先だったのではと思いつつ、このファイルをクリックして開いたが、レジュメは表示されなかった。ファイルが壊れているのかな…。まぁいいか。」

はい。アウトです。こんな話は、どこの会社や団体でも見るありふれた光景でしょう。しかし、この話には3つのポイントがあります。

1つは、長い連休中にはセキュリティアップデートや、総合セキュリティソフトの更新が行われている可能性があります。日常的な業務を始める前に、まずアップデートして連休中に見つかったシステムのセキュリティホールや新しいマルウェアに対応できる状態にしましょう。

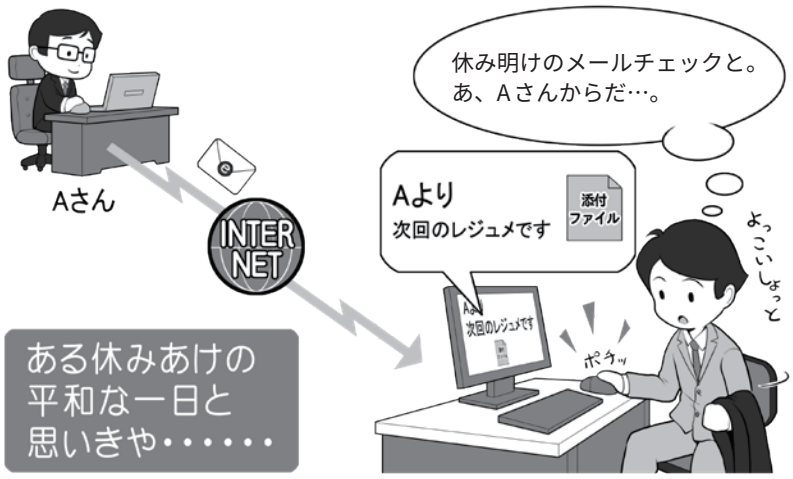
2つめに、どこかの会社のAさんが、本当にAさんか確かめるのは、ややレベルが高いとしても、少なくともこの時期にAさんからメールが来たことに疑問を持っています。そういうときは連休中にAさんのメールが乗っ取られた可能性を考えて、メールではない手段(電話など)でAさんに添付ファイル付きのメールを送ったか確認しましょう。

3つめ、添付されているファイルをいきなり開き、きちんと見られなかった点で、マルウェアの可能性を考えていません。ひらけなければ疑問を持つべきですし、開いた場合でもなにかをインストールしろとか、あなたに許可を求めるものは、総じて疑うべきです。

それに原則的なルールは、「メールを見ただけで完結しないものはすべて疑え」です。

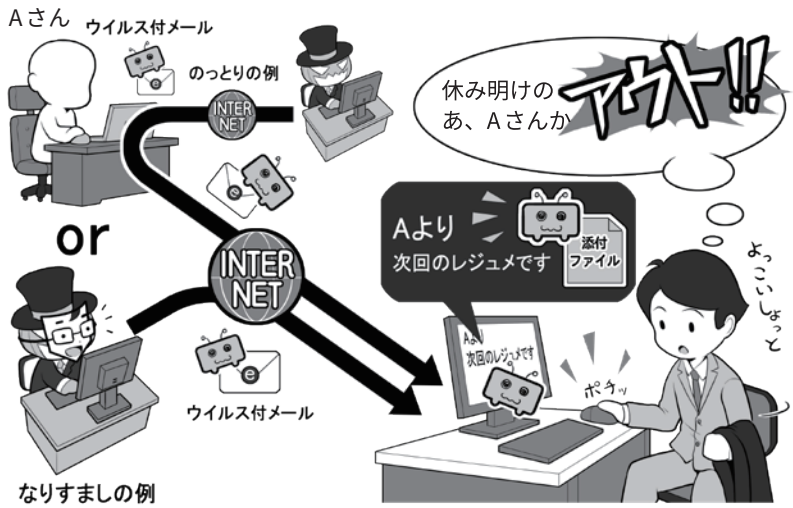
それは添付ファイルでもメールの文中の外部ウェブサイトへのリンクでも同じです。

こんなシチュエーションだと思っていたら…



休み明けに出社して、普段どおりにパソコンを立ち上げ、メールを開いて読む。しかし、この一連の流れには攻撃に対する視点が欠けています。攻撃者だったらどう攻撃するかという視点です。休み明けということは、何日間かパソコンを立ち上げていない時間が存在し…

実はこんなシチュエーションかも…



その間には、新たなセキュリティホールが発見され、攻撃者が攻撃するためのマルウェアを開発して、取引相手になりすましたり、アカウントを乗っ取ったりして、そのマルウェアを送ってきているかも。メールを開く前にまず、アップデートしてシステムを最新の状態にします。

2 フィッシング攻撃の傾向と対策

「オンラインショッピングの会社からメールで、『あなたのアカウントが攻撃され、一時的に利用停止になった。下記からログインして、停止を解除して下さい』という内容のものが送られてきた。リンクを開くといつもどおりのそのショッピングサイトのロゴとデザインのウェブサイトが表示されたので、IDとパスワードを入力して、停止を解除した。」

あなた宛に名指しで送られてくるメールなどと違い、個人名がなく不特定多数に送られることが多いのが、ばらまき型のフィッシングメールです。余談ですがフィッシングとは釣り Fishing ではなく、詐欺の意味の Phishing から来ています。

上記の話は有名なので知っている方も多いと思いますが、ねつ造された偽物のウェブサイトは、最近では本物と見分けが付きません。

あなたがIDとパスワードを入力すると、それをだまし取って勝手にオンラインショッピングサイトで買い物をし、商品を転売するなどしてお金を手に入れるわけです。

このメールも文面を見ただけで完結しないので疑うべきですし、パソコンの場合は、リンクのURLやジャンプした先のウェブサイトのアドレスが本当にその企業のものかチェックすることである程度回避できます。ウェブサイトが本当にその企業のものか確かめる方法は、P134 の SSL 証明書の項目を見て下さい。

なお、こういった警告が来た場合、メールのリンクは使用せず、ウェブブラウザで検索し直接そのショッピングサイトなどを訪れてみて下さい。本当にアカウントが停止されているならば、警告が表示されるでしょう。

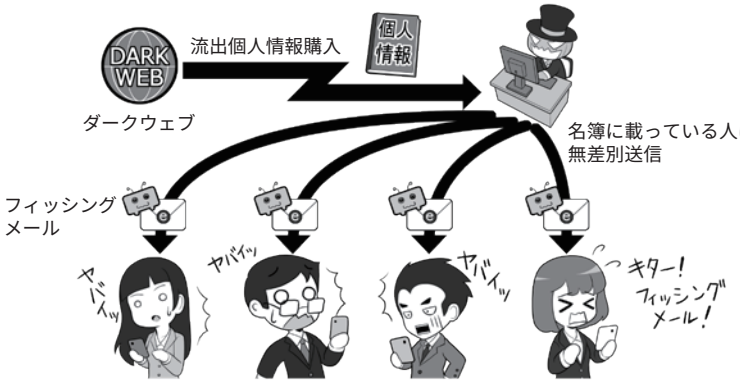
一方で、そのウェブサイトがショッピングサイト相当の暗号化 (https) に対応していて、一見そのショッピングサイトと同じ名前を掲示していても、実は「アルファベットに似た別の言語の文字」を使用している場合もあります。

具体的にはロシア語などで使われるキリル文字は、アルファベットと似た字形のものがありますが、インターネットでは別の文字として扱われるので、同じにURLに見えて別のウェブサイトを作れるのです。

すぐに対処しようと思ったら…

SMSやメールで「パスワードが流出しました。至急変更を！」という連絡がきても、ちょっと待ちましょう。それは本当に自分が使っているサービスから送られてきていますか？

実際はこういうワナだった！



攻撃者はどこかのウェブサービスなどから流出したメールアドレスなどをを買って、IDとパスワードを盗む攻撃をしかけてきます。反応するとアカウントを乗っ取られるかも。

それには解りにくくなる工夫も

この部分が見た目同じ文字を使う外国語だったりすると、一見、見分けが付かないことも

メールのリンクを開いて、飛んだ先のウェブサイトがそのサービスの本物のページとは限りません。似たような単語を使った別のウェブサイトの場合もあるのです。よく確認しましょう。

3 不正アクセスの傾向と対策

「ある朝、会社に出社したら、取引先から『お宅に渡した当社の機密情報がネットで公開されているじゃないか、どういうことだ！』というクレームの電話が来ていました。それを受けて調べるみると、社員で共有用に使っていた社外のクラウドストレージサービスのIDとパスワードが何者かに破られて、社外からアクセスをされ、情報が流出していました……。でもなぜIDとパスワードが漏れたんでしょう…。」

この問題は複合的で、「①なぜIDとパスワードが漏れたのか」だけでなく、「②なぜ漏れたIDとパスワードでクラウドストレージサービスにアクセスできたのか」、最後に「③なぜクラウドストレージサービスから情報流出を許してしまったのか」の要素があります。

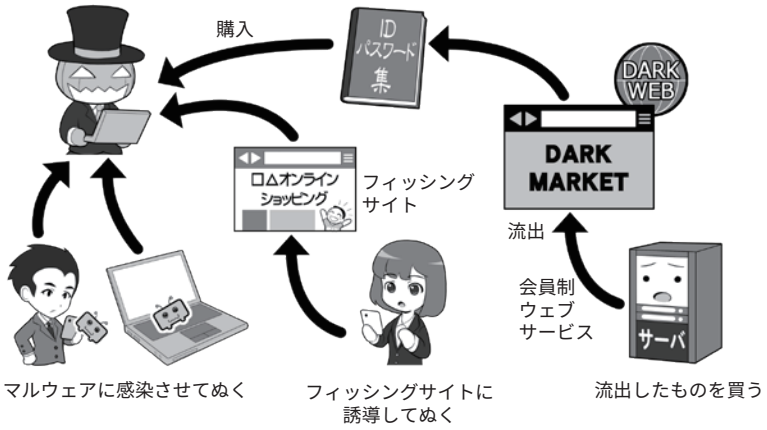
①のIDとパスワードの流出はマルウェアの感染やウェブサービスからの流出などがあり、自分で防げるものと防げないものがあります。自分で防ぐには、セキュリティをきちんと固めるだけです。一方、ウェブサービスからの流出は、多要素認証を導入していないセキュリティ意識が低いサービスを避けるなど、消極的手段はありますが、最終的には自分でどうにかすることはできません。

どうにかできないをカバーするには、②のなぜクラウドにアクセスできたかの問題ごと封じます。この場合は個人と業務用でパスワードの使い回しをしていたことが原因なのでこれを防ぐのです。たとえ漏れても被害が発生しないようにするには、一つはパスワードの使い回しを絶対にしないこと。もう一つは、多要素認証を導入して、漏れてもIDとパスワードだけではアクセスできないようにすることです。

③でさらにクラウドにアクセスを許しても情報流出を許さないためには、アクセスできる人間を限定することや、重要情報を見られる人間を共有設定で限定すること、そして、機密情報などは例えファイルとして流出しても、その内容を閲覧できないように、ファイルごとに暗号化を施すことです。

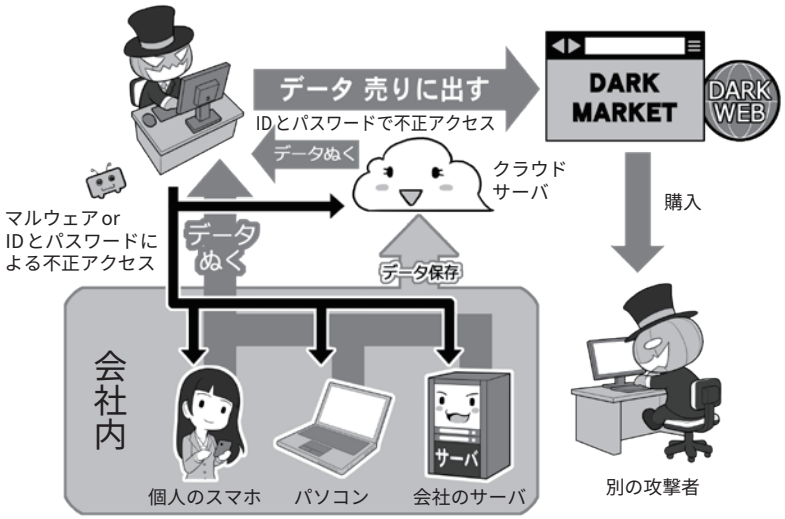
不正アクセスを行うために攻撃者は…

①IDとパスワードを狙う



攻撃者は不正アクセスを行うために、IDとパスワードを収集します。前ページのように偽のウェブサイトに誘導して抜く方法の他にも、マルウェアに感染させて抜く、流出した情報をダークウェブにあるマーケットで購入して集めるなど、さまざまな手法があります。それを使って別のウェブサービスや業務上のサービスに不正アクセスを行おうとします。このとき、IDとパスワードの使い回しをしていると、侵入されてしまう危険性が跳ね上がります。

②データを狙う



不正アクセスができたら、今度はあなたが持っている機器、使っている機器から情報を抜き取ります。それをダークウェブのマーケットを経由して誰かに販売するかもしれません。クラウドサーバ上にあるデータも、アカウントを盗まれればアクセスされて、保管しているデータを盗まれるでしょう。盗まれたデータが受託した業務に関連するものだった場合、自社だけでなく発注元企業に被害が及び、また個人情報だった場合、顧客などに不利益を与える結果になります。アカウント情報を盗まれないように、細心の注意を払いましょう。

4 不正送金の傾向と対策

お金を直接狙うサイバー攻撃は、別項でも紹介した航空会社のリース料詐欺のように、取引先のふりをして振り込み口座を変更させるBECや、不審なメールやメッセージから銀行にそっくりのウェブサイトに誘導して、IDとパスワードを抜いたり、実際にインターネット上で送金するときにその通信の中間に割り込んで、目的の口座に振り込ませる「中間者攻撃」と呼ばれるものなどがあります。

警察庁の発表によれば平成29年の不正送金事件の発生件数は425件、被害総額は約10億8,100万円となっており、依然として少なくない額の被害が発生していることが分かります。

「会社の口座を確認したら、空になっていた。」こうなってしまっては回収できたとしても時間を要するでしょう。会社の運転資金までやられてしまえば、事業継続は困難になります。

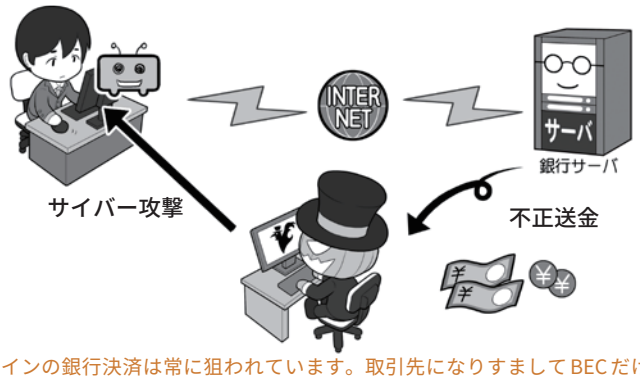
幸いにして情報の流出などと異なり、銀行の場合は過失が無いことが認められれば、銀行側が補填してくれることもあります。クレジットカードの不正利用なども同様です。

一方、場合によっては補填が行われないのが、仮想通貨を奪取する詐欺です。仮想通貨は通貨といいながら、平たくいえば暗号化された情報なため、不特定多数をフィッシングメールでマルウェアに感染させ、情報を奪取することも行われています。

これらに対処する特別な方法はなく、今までの3項目であるような基本的な対処方法と、もう一つは同様の手口の情報を、アンテナを高くしニュースやネットの記事、SNSなどから集めて、いざ攻撃されたときに、「似たような話を聞いたことがある。不信だ」と気付くようになることです。

なお、不正送金が疑われる事象があった場合は、速やかに銀行やクレジットカード会社に相談しましょう。

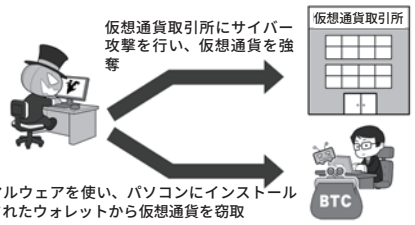
オンライン決済は常に狙われている



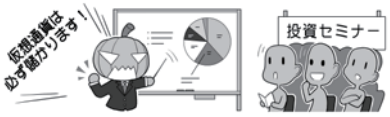
オンラインの銀行決済は常に狙われています。取引先になりすましてBECだけで誤った口座に送金させる手口や、偽サイトでIDやパスワードを奪う方法、そしてなんらかの手段で決済の中間に割り込んで振込先を自分の口座にすり替えてしまう中間者攻撃。

多要素認証、パスワードなどの厳重保管、BECやフィッシングメールに騙されないスキル、そして総合セキュリティソフトなどを導入している場合は、決済専用のブラウザを使うなどの防御手段があります。

犯罪者に狙われる仮想通貨



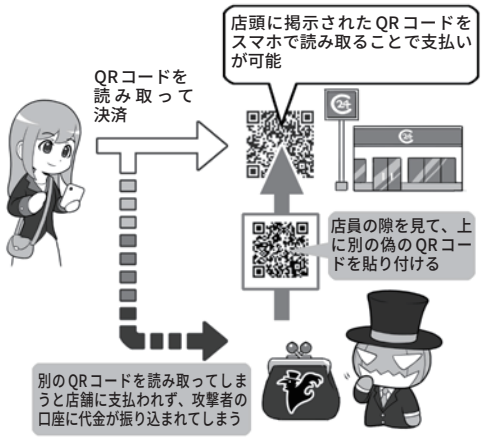
仮想通貨を巡るサイバー攻撃も続発しています。実際、大手仮想通貨の取引所がサイバー攻撃を受け、大きな金銭的被害が生じた事例があるほか、仮想通貨の窃取を目的としたマルウェアも登場しています。



題材を仮想通貨にした「必ず儲かる」系のセミナーも開催されています。仮想通貨に限らず、「必ず儲かる」という話は詐欺のケースが多いので、信用しないようにしましょう。

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。

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。

5 ランサムウェアの傾向と対策

「始業時間に会社に来てパソコンを起動すると、『このパソコンは乗っ取った。データはすべて暗号化したから、データを返して欲しければ身代金を払え』というメッセージが出て、送金期限までのカウントダウンが始まった……」

これがランサムウェア（ランサム＝身代金）と呼ばれるマルウェアの典型的な手口です。大事なデータが入ったパソコンが使えなくなれば、業務が停止し納期に間に合わなくなり取引先のお客様に迷惑をかけ、その結果、会社としての信用を失うおそれもあります。

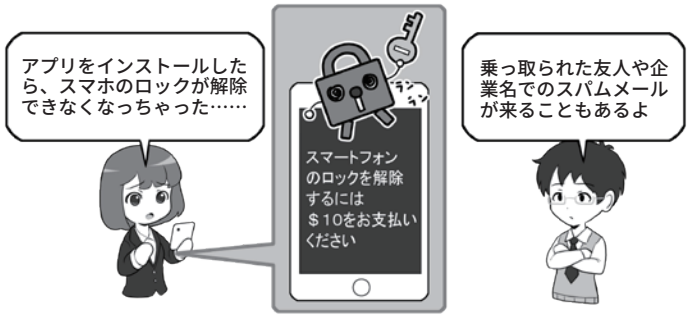
ランサムウェアへの対処方法はシステムを常に最新の状態に保つことと、仮に攻撃されても、感染したシステムを初期化しバックアップから復旧できる体制を整えることです。

身代金を支払ってもデータが復元される保証はないですし、攻撃者を助長するだけなので避けましょう。

ランサムウェア感染はビジネスにも影響

ランサムウェアはパソコンなどの中のファイルを勝手に暗号化するため、感染すれば仕事上の極めて重要なファイルも人質に取られてしまいます。バックアップは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



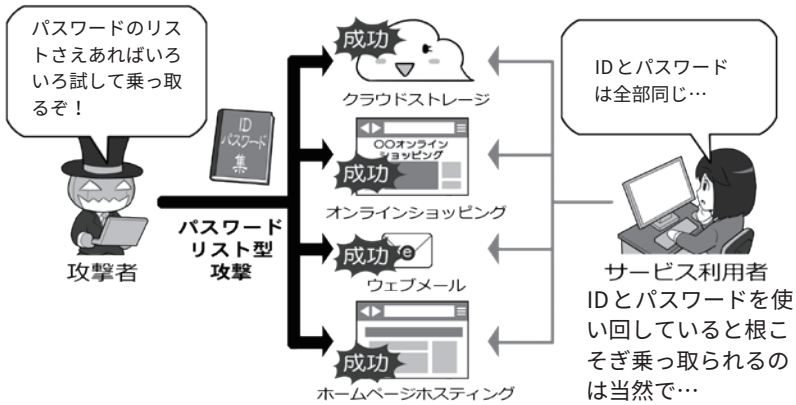
スマホの場合、公式ストアでもマルウェアは発見されていますが、ほとんどの場合はそれ以外の場所から、アプリなどをインストールさせる手法です。こういったアプリは不審なメールのリンクや、添付ファイルなどでも回ってきます。大きなダメージを被る可能性もありますので、十分に注意しましょう。少なくともアプリのインストールは公式ストアからのみにしましょう！

6 ウェブサービスへの不正ログイン

先ほどの情報流出の件でも登場しましたが、クラウドストレージサービス、オンラインショッピング、メール、ウェブサイト運用など、ウェブサービスと総称されるインターネットのサービスは、常に攻撃者からの乗っ取りの危険にさらされています。常にこれを阻むことを考えましょう。

IDやパスワードの使い回しをしないことと、さらにサービスを利用する際に、多要素認証などやUSBセキュリティキーなどを用いて、攻撃者が不正ログインしにくくなる環境を整備しておきましょう。

パスワードを使い回しをしていると攻撃に



つい面倒くさがってIDとパスワードを使い回ししていると、どこか一つでも流出が起これば、同じIDとパスワードを使用しているサービスが根こそぎ乗っ取られる場合があります。また、別々のパスワードを使っていても、そのパスワードがよく使われるような簡単なものだった場合、そういったパスワードをまとめたリストが流通していて、それを使ってアカウントを乗っ取る攻撃が行われます。一部を変えただけなど、似たようなパスワードも非常に危険です。

7 ウェブサイト改ざん

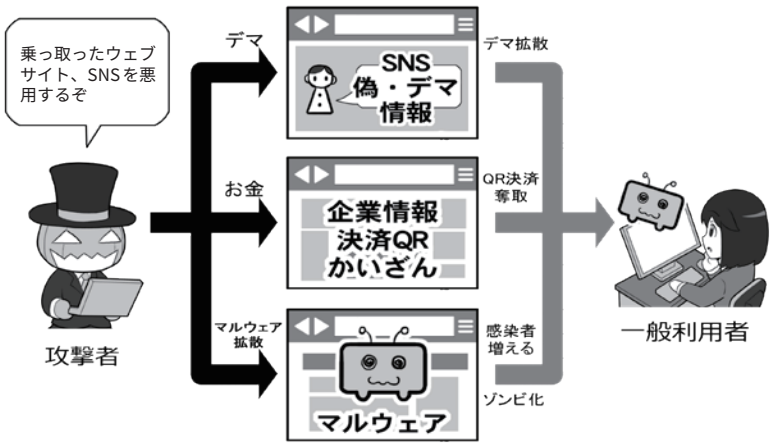
会社や団体のウェブサイトは、ホスティングサービスと呼ばれる、専用の業者のサーバを利用していることも多いと思います。

これらのサービスはセキュリティを自分で管理する代わりに、ホスティングサービスに外注している形になり、特殊なカスタマイズを施さなければある程度のセキュリティは確保されています。

一方、正規のIDやパスワードが流出し、それを使って不正アクセスされ乗っ取られると、改ざんされ偽の情報を発信したり、マルウェアなどを埋め込まれ、不特定多数にサイバー攻撃をしてしまったりします。

認証情報はきちんと管理し、多要素認証などで容易に不正アクセスできないように設定しましょう。

ウェブサイトを乗っ取られると攻撃の拠点に



IDとパスワードの流出による不正アクセスや補修されていないセキュリティホールを突かれ、自社や団体のウェブサイトを運用しているサーバが乗っ取られると、攻撃者はそのウェブサイトを使ってサイバー攻撃を行います。

例えば偽の情報を発信する、公開されている企業の情報を改ざんする、あるいはそのウェブサイト自身をマルウェアの発信元にして、ウェブサイトを訪問した人のIT機器をマルウェアに感染させ、乗っ取ったIT機器をどんどん増やしていくかも知れません。

また、ウェブサイトではなくても、利用しているブログサービス、SNSアカウントを乗っ取ると、そこでデマを発信したり、フェイクニュースを掲載するかもしれません。

海外では、ニュースサイトのSNSアカウントが乗っ取られ、重大なフェイクニュースが発信され、株価に影響を及ぼす事件もありました。たかがウェブサイト、たかがSNSではないのです。

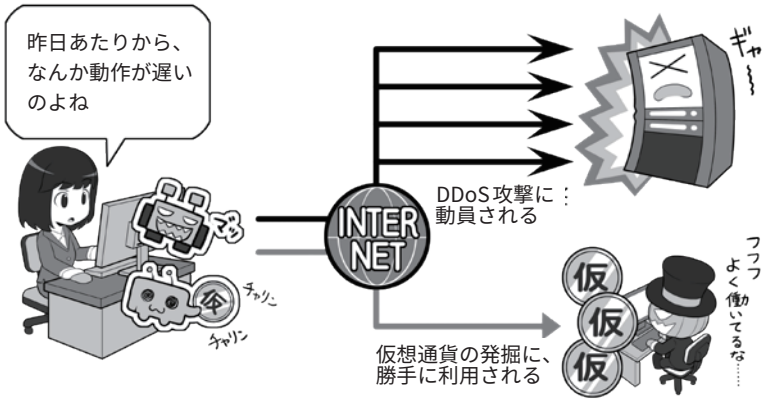
一方、WordPressなどのウェブサイト作成ソフトは、それ自身をアップデートしないで使用すると、発見されたセキュリティホールを悪用されるので、きちんとアップデートしましょう。

8 DDoS攻撃

DDoS(Distributed Denial of Service)攻撃とは、複数のIT機器からウェブサーバに対して大量のデータを送りつけて応答不能にするサイバー攻撃です。DDoS攻撃を受けると、利用しているインターネットサービス、いずれもが処理能力オーバーで機能しなくなり、ウェブサイトならばアクセスできなくなります。これに関しては、ウェブホスティングサービスに任せ、事実上利用者にできることはないのが実状です。

一方、自分の会社や団体のIT機器などが乗っ取られDDoS攻撃に利用されている場合は、利用停止、ネット切断、通報の判断、周りを含めマルウェアの駆除、バックアップからの復旧などをする必要があります。

乗っ取ったIT機器は直接的サイバー攻撃などに



マルウェアに感染させられたIT機器は、自分が被害に遭うだけに留まらず、他のIT機器やサーバに対して直接的なサイバー攻撃に駆り出されることもあります。例えば不正な情報リクエストを集中させ、相手のサーバが反応できない状態に追い込むDDoS攻撃などを行います。また、IT機器の動作がおかしいときには、気付かないうちに仮想通貨の発掘に利用されている場合もあります。普段と比べて動作が遅い、不審な挙動をするなどといったときは注意しましょう。

DDoS攻撃に限らず、総合セキュリティソフトが反応しない場合、マルウェアの感染を検知するのは、「なにか動作が遅い。おかしい」といった、正常動作時との差なので、そういった点にも気を配りましょう。

9 まずはサイバーセキュリティ以前のモラル教育から

顧客情報を狙う攻撃者の視点から、情報を手に入れる手段を考えると、狙った社員の心の隙を突くソーシャルエンジニアリング方法などが考えられます。例えばSNSで相手を見つけて「名簿高く買うよ」とそそのかす方法などが考えられます。

ただ、情報流出が起こるのは狙われたケースだけではありません。「列車内に鞄ごとPCを置き忘れる」「顧客情報の入ったUSBメモリを落とす」「車内に置き忘れた生徒の成績表の入った記憶装置を盗まれる」「全顧客にメールを送信しようとしたら全顧客の宛名が見える形で送信してしまった」など顧客情報の流出の報道は枚挙(まいきょ)に遑(いとま)がありません。

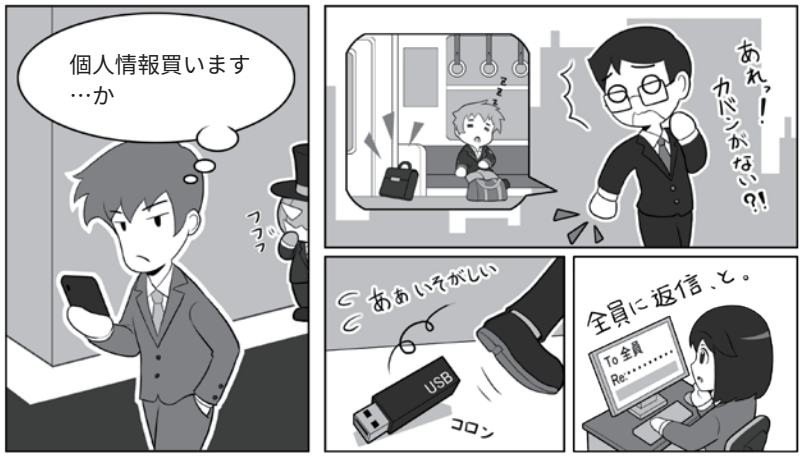
「それってサイバー攻撃なの？」といわれれば、直接的にはサイバー攻撃ではないかもしれません。しかし、流出したものがダークウェブなどで販売されれば、サイバー攻撃に繋がります。

こういった内部犯行や情報流出を防ぐには、防御手段をとった上でモラル教育をきっちり行うことです。それは本書の対象となる小さな会社やNPOでも変わりません。

例えば内部犯行防止に、必要がないときに顧客情報を扱う部屋に人を入れないよう、部屋や建物に施錠をしているでしょうか。アルバイトや社員に、きちんと情報モラル教育をしているでしょうか。

あるいは、仮に置き忘れや紛失、盗難が起こってしまっても、完全な情報流出が起こらないようにするリカバリ手段を講じたり、問題が起こったらどう対処するか、その段取りを考え訓練したりしているでしょうか。

情報流出の可能性はたくさんある



流出の可能性は情報を扱う人を狙ってそそのかすことだけではありません。機密情報を入れたパソコンをカバンごと電車やタクシーの中に置き忘れる、生徒の成績などが入ったUSBメモリを落とす、多数の人に一斉メールを送ろうとしたら、互いのメールアドレスが分からないBCC欄ではなく、見えてしまうTOやCC欄に入れて送信してしまった、などなど。パソコンやスマホ、IT機器は便利な反面、ミスを犯すときも一瞬で多量に失います。要注意です。

サイバーセキュリティにつながる予防策

内蔵記憶装置暗号化　暗号化USBメモリ　資格のない人にはさわらせない共有設定　必要ない人が立ち入らないように施錠

現実世界、ネットの世界、両者に共通する情報流出の防御手段は、機密情報を扱うパソコンや記録媒体は暗号化した上で、その部屋や建物には必要がない人が入れないようにすること、施錠をきちんと行うこと、パソコンなども使用しない場合はロッカーにしまって鍵をかけること、ハッキングを受けないようにネットワークには接続せずにスタンドアロンで使用すること、使用できる人の資格設定をきちんと行い、資格がない人には触れないようにすることなど、できる事はたくさんあります。

大切なのは情報モラル教育

こう言った機器やシステム的防御策だけでなく、同等に大切なのは、情報に触れる社員や会員に対する情報モラル教育です。機密情報の取り扱いだけでなく、最近ネットを賑わせる、問題のあるSNS投稿などを起こさないように、ネットリテラシーを含んだ勉強会や教育を行う事が、求められています。

情報流出というと、攻撃事例だけに注目をしてしまいがちですが、他にも情報流出は起こりえますし、一方で情報管理の基礎を守ればそれらを防ぎ、被害を抑え込むリカバリ手段も打てるのです。

そういったサイバー攻撃以前の備えの必要性を忘れないようにした上で、一般的なサイバー攻撃の事例を知りましょう。

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、では逆に職業的な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。

また、こういった攻撃者の場合、活動するための資金を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。

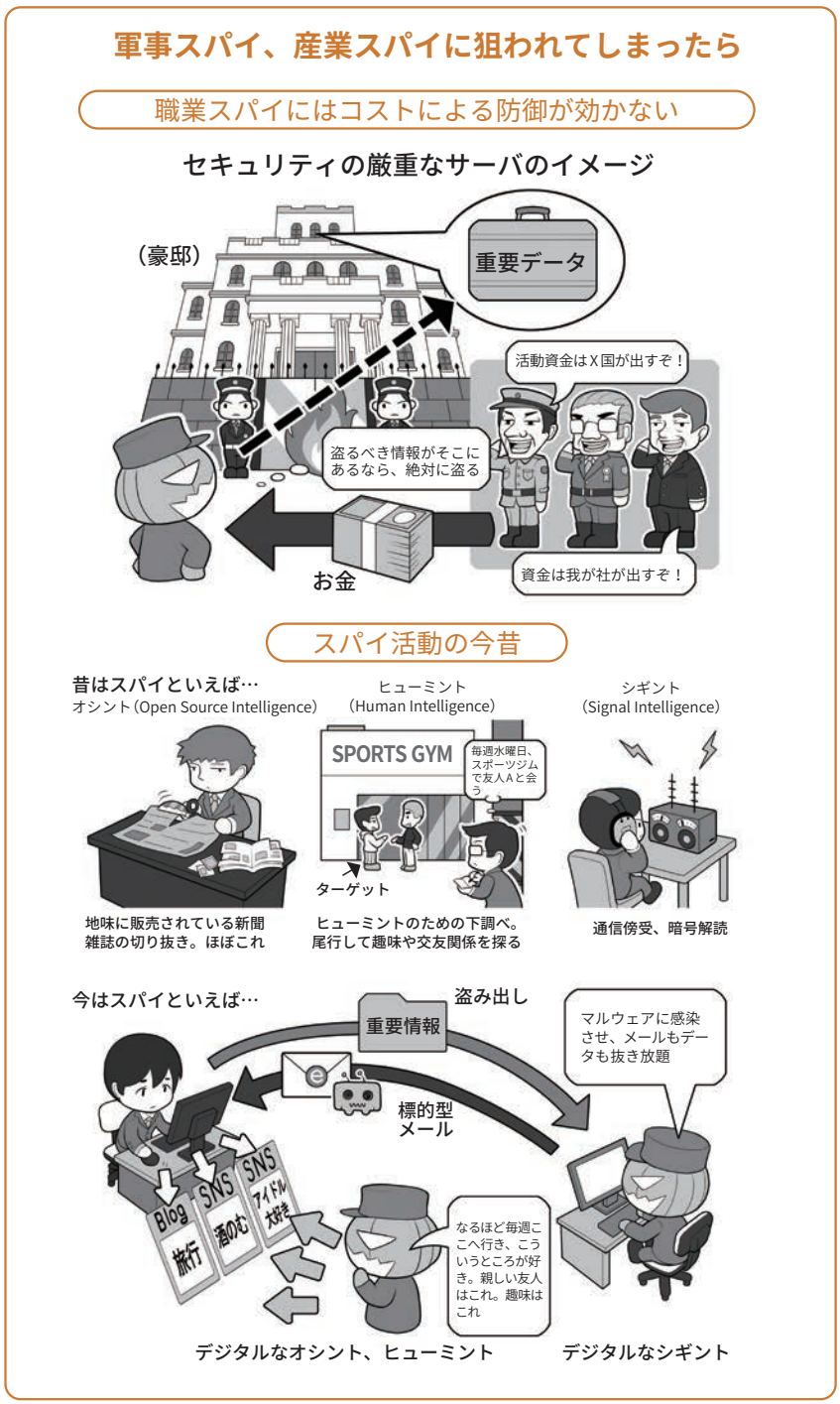
興味がある方は一般のスパイの教本をお読みになると、目的のためにはどれぐらい容赦ないことをするのか理解できるでしょうし、それが理解できれば、あとはネットの世界のサイバー攻撃に置き換えればいいわけです。

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情報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などがありました。

ネット社会の現代では、SNSを見ればある程度オシントで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。シギントもターゲットのスマホをマルウェアに感染させれば、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、旅行先の状況を盗撮できたりもします。

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低コストインテリジェンス(諜報活動)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。



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、現実的には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。

その国のルールを理解せず、自国の常識でネットを利用すると、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、あなたが他国に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ていました。通信しようとしたらローミングでは著しく遅いので、値段も手頃な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、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、やっとのことで数日後釈放されました。

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購入します。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入力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も確認し、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

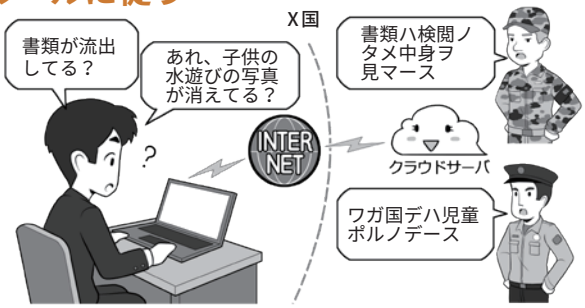
①自国で問題ない写真がアウトなことも

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法に従って、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。

3 それでも攻撃を受けてしまったときの対処

1 兆候に気を配りつつ、被害が出たら対処

ここではサイバー攻撃の兆候を日常の業務上で察知するという切り口と、そこからの対処行動を説明しましょう。

まず、システムを最新の状態にしたのち総合セキュリティソフトを入れたとしても安心してはいけません。セキュリティホールの発見に対してアップデートなどの提供が間に合わない状態で、攻撃をしかけられたら、防ぐことが難しいからです。（ゼロデイ攻撃）

備えるだけでなく、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る意味はここにあります。

攻撃の兆候の中からいくつかの例を挙げてみましょう。

アカウントの乗っ取りの兆候は、知らないログイン通知やログイン履歴、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での自分が知らない投稿やアプリ連携などがあります。

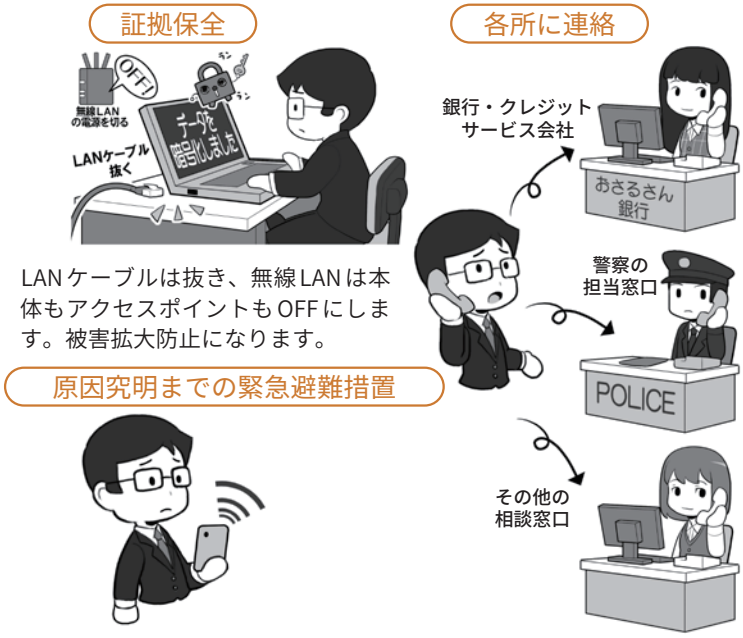
銀行口座関連も、ログイン通知があればそれを受け察知したり、通帳や取引履歴を見てチェック。クレジットカードはたとえ少額であっても利用履歴を検証しましょう。

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、実害が判明したら、とりあえずは有線でも無線でもネッ

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。会社や事務所のパソコンなどが感染したら、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。

トにつながる回線から切断した上で、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マルウェアの拡散防止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、必要に応じて各種金銭取引関係のサービス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。

侵入経路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、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再度最新の状態か確認し、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りかねないサポート期間切れの機器やソフト、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、知らないものや不要なものを解除しましょう。

なお、どこかのウェブサービスなどからパスワードが流出した結果、ウェブサービスのアカウントを乗っ取られてパスワードを変えられてしまった場合は、自分で再設定することはできないので、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。

ところで、攻撃が明白でない状況で疑心暗鬼になりそうなとき、頼りになるのが、気軽に話せる IT に詳しい知人だったりします。相談することで現在おかれている状況が明白になってきたら、各種の相談窓口の連絡や、関係機関への届け出を行いましょう。

そのときあなたが誰かに助けられたら、次は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。

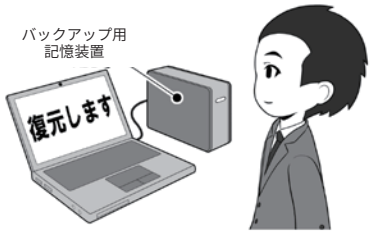
実被害が出ていない場合

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。



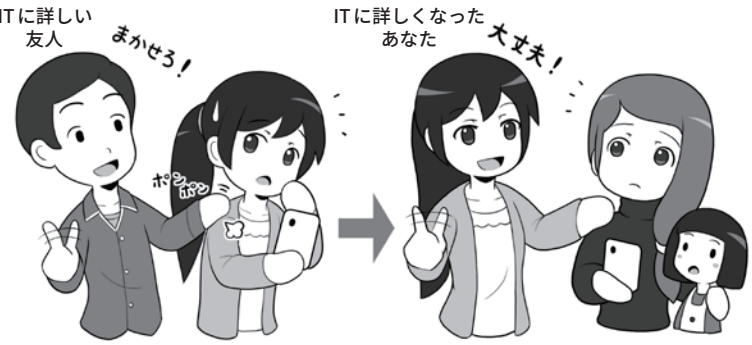
システムチェックする

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ます。

そんなとき頼りになるのは……



ITに詳しい知人に意見をもらうとともに、自らも勉強しましょう。
そして将来同様のケースがおきたら、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。

2 情報関係機関への相談や届け出

前項ではサイバー攻撃を受けた場合の概念的な流れを説明しました。

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

まず、とりあえずサイバー攻撃を受けたらどこに相談したらいいのか。その道に明るいアドバイスをもらえる人もいない場合はどうすればいいのでしょう。

代表的なものとしてIPAによる「情報セキュリティ安心相談窓口」があります。同名のウェブサイトを検索すると、「良くある質問」や、過去のサイバーセキュリティに関するレポートなどが掲示されているので、一通り目を通し、それでも解決しない場合は、電話やメールで問合せしてみるといいでしょう。

「標的型メール攻撃」に関しては「標的型サイバー攻撃特別相談窓口」が個別に設けられています。詳しい情報を提供すると、より速やかに的確な対応ができるようになっています。それとは別に、義務ではありませんが、「ウイルスの届け出」「不正アクセスの届け出」を受け付けているので、可能であれば届け出ましょう。そうすることで他の人が攻撃に遭うのを避けることが可能になります。

地域の商工会議所がサイバー攻撃対応支援サービスの一環として、有料の相談窓口を設けている場合もあります。なお業種によって、例えば医療機関でのサイバー攻撃に関しては、厚生労働省が、医政局 研究開発振興課医療技術情報推進室で連絡を受け付けています。

IPA情報セキュリティ安心相談窓口	https://www.ipa.go.jp/security/anshin/index.html
電話での相談	03-5978-7509（受付時間 10:00～12:00、13:30～17:00、土日祝日・年末年始は除く）
メールでの相談	anshin@ipa.go.jp
FAXでの相談	03-5978-7518
郵送での相談	〒113-6591 東京都文京区本駒込2-28-8 文京グリーンコート センターオフィス16階 IPAセキュリティセンター 安心相談窓口

IPA安心相談窓口で対応出来ない例

なお、IPA安心相談窓口では、下記のような相談は受け付けていません。

- 直接来訪しての相談や面談
- 契約・支払いに関する相談
- 法的解釈に関する相談
- 個別の端末調査や犯罪調査に関する相談
- 特定の製品やサービスの紹介
- 特定企業への改善や指導に関する相
- パソコンの具体的な操作方法や手順等の案内
- 他組織への連絡や通報などの仲介

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

●サービス提供または購入などの契約に関するトラブルで困っている場合

消費者ホットライン（消費者庁）
http://www.caa.go.jp/region/shohisha_hotline.html

国民生活センター
http://www.kokusen.go.jp/

●犯罪行為に関する被害届や捜査について相談をしたい場合

都道府県警察本部のサイバー犯罪相談窓口等一覧
https://www.npa.go.jp/cyber/soudan.htm

●法的トラブルの相談をしたい場合

法テラス
https://www.houterasu.or.jp/
インターネット上での違法・有害情報に関し相談したい場合

違法・有害情報相談センター
https://www.ihaho.jp/

社団法人 コンピュータソフトウェア著作権協会不正コピー情報受付
https://www2.accsjp.or.jp/piracy/

●インターネット上の違法情報を通報したい場合

インターネット・ホットラインセンター
https://www.internethotline.jp/

●迷惑メールの受信に関して困っている場合

財団法人 日本データ通信協会迷惑メール相談センター
https://www.dekyo.or.jp/soudan/ihan/

財団法人 日本産業協会電子商取引モニタリングセンター
http://www.nissankyo.or.jp/e-commerce/

●フィッシングサイトの発見または被害に関して困っている場合

フィッシング対策協議会
https://www.antiphishing.jp/registration.html

警察庁 フィッシング110番
https://www.npa.go.jp/cyber/policy/phishing/phishing110.htm

●インターネットに繋がらないなどのトラブルで困っている場合

利用プロバイダまたはパソコンのメーカー・購入店の各サポート窓口

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

3 警察機関への相談や届け出。そして経営ガイドライン

サイバー攻撃では前項のように、自分が攻撃を受けたことに関する相談の他に、実際に情報を盗難されたり、なんらかの被害を被ったり、あるいは法律で禁止されている不正アクセスなどに該当する場合は、警察への相談や通報が必要となります。

まずは都道府県警察本部のサイバー犯罪相談窓口に相談することを最初に考えるといいでしょう。

その場合でも5W1Hのように「なにがどうなってどういったことが起こっているのか」を、紙に書くなどして整理して明確にし、漠然とした相談にならないようにしましょう。警察がなんらかの捜査をする場合は、そのための情報や証拠が必要となります。

データ損失や不正送金など実害が発生した場合は、やたらにその機器を操作せず、まず相談窓口に相談して対処方針を決めるといいでしょう。

特に緊急を要する場合を除き、余裕があればその前に、警察庁の「インターネットの安心安全相談」の、「相談窓口」でキーワードでの検索や、事例検索ができるようになっているので、そちらを参照して見てはどうでしょうか。

さてそういった相談窓口を知っておいた上で、大切なのはサイバー攻撃を受けたときにパニックになってどうしていいか分からなくならないようにすることです。

経済産業省とIPAが共同で出している「中小企業の情報セキュリティ対策ガイドライン」では、問題が発生したことを想定してシナリオを作っておくことを薦めています。このガイドラインを読むことで、サイバーセキュリティに関するトラブルがの発生に「どう備えるか」ということに対するアイデアが得られるので、ぜひ一度目を通して、自分の会社や団体なりの対応マニュアルを作ってみて下さい。

警察庁サイバー犯罪対策プロジェクト	https://www.npa.go.jp/cyber/
警察庁 インターネット安全・安心相談	https://www.npa.go.jp/cybersafety/
各都道府県のサイバー犯罪相談窓口等	https://www.npa.go.jp/cyber/soudan.htm

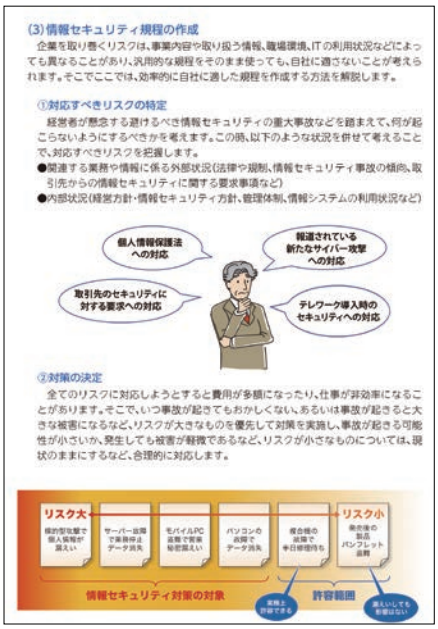

都道府県警察本部のサイバー犯罪相談窓口等一覧

都道府県	相談電話	上段はサイバー犯罪対策掲載、下段は情報・相談等メール等受付掲載
北海道	011-241-9110(祝)	http://www.police.pref.hokkaido.lg.jp/info/seian/cyber-bouhan-hiroba/main/information.html https://www.police.pref.hokkaido.lg.jp/consult/soudan/request/request.html（全）
青森	017-735-9110(祝)	http://www.police.pref.aomori.jp/seianbu/bzan/cyber/index.html http://www.police.pref.aomori.jp/keimubu/kouhou/dou.html（全）
岩手	019-654-9110(祝)	http://www2.pref.iwate.jp/~hp0802/cshirase/cyber/index.html http://www2.pref.iwate.jp/~hp0802/e-mail/form.html（全）
宮城	022-266-9110(祝)	http://www.police.pref.miyagi.jp/ho/cyber/index.html http://www.police.pref.miyagi.jp/ho/toa/soudankujou.htm（専）
秋田	018-865-8110(専)	http://www.police.pref.akita.jp/kenkei/cyber/body.html http://www.police.pref.akita.jp/kenkei/cyber/madoguti.html（専）
山形	023-642-9110(祝)	http://www.pref.yamagata.jp/ou/kensatsu/800016/cyber/hightec.html http://www.pref.yamagata.jp/ou/kensatsu/800016/cyber/advise.html（全）
福島	024-525-3311(祝)	http://www.police.pref.fukushima.jp/onegai/youhou/hightech2/cyber_top.html http://www.police.pref.fukushima.jp/onegai/youhou/hightech2/soudann_mdw.html（全）
警視庁	03-5805-1731(専)	http://www.keishicho.metro.tokyo.jp/kurashi/cyber/index.html http://www.keishicho.metro.tokyo.jp/sodan/madoguchi/sogo.html（全）
茨城	029-301-8109(専)	http://www.pref.ibaraki.jp/kenkei/a01_safety/index.html http://www.pref.ibaraki.jp/kenkei/a01_safety/cyber/taisyo/04_contact.html（専）
栃木	028-627-9110(祝)	http://www.pref.tochigi.lg.jp/keisatu/seikatu/nethanzai.html https://s-kantan.com/pref-tochigi-u/offer/userLoginDispNan.action?tempSeq=702（全）

各都道府県警の、サイバー犯罪相談窓口の一覧。
代表の電話番号の場合やサイバー犯罪相談等専用電話番号の場合もあるので、どの電話番号にかけているのかをよく確認しましょう。
ウェブサイト上のサイバー犯罪に関する情報は、表記されているアドレスだけでなく、他のページにも記載されている場合があります。

「中小企業の情報セキュリティ対策ガイドライン」

IPAによる「中小企業の情報セキュリティ対策ガイドライン」は小さな会社やNPOでも役立つ内容が記載されています。ぜひ手に取って役立つ部分を探してみましょう。



https://www.ipa.go.jp/security/keihatsu/sme/guideline/index.html
情報セキュリティ自社診断シートなどもあるので参考になります。

コラム：実践的サイバー防御演習「CYDER」

専任のセキュリティ担当者がいない中小企業の場合、サイバー攻撃から身を守る手段は、主として「攻撃を受けにくくなる」ようにすることや、自社のウェブサイトを持つ場合でも、ウェブホスティングサービスを利用することで、セキュリティに割く労力をアウトソースすることといった対応が現実的です。

しかし、サイバー攻撃に対して「立ち向かう」ことが求められる状況も出てきます。では実際にどうやって立ち向かえばいいのでしょう。

そこでお薦めするのが、国立研究開発法人情報通信研究機構(NICT)が提供している実践的サイバー防御演習「CYDER(CYber Defense Exercise with Recurrence)」です。

CYDERの受講者は、事前オンライン学習によって攻撃手法や対策技術に対する理解を深め、集合演習(ハンズオン＆グループワーク)を通じて、一連のインシデントハンドリングを体験することにより、組織で役立つセキュリティポリシーやコミュニケーションの重要性を学ぶことができます。CYDERは全国で100回程度開催しており、2018年度より民間企業の方も受講可能となりました。

特に小さな組織では、情報システム担当者を専任で配置することが困難な場合があります。しかし、サイバー空間では、組織の規模に関係なく、攻撃されるリスクにさらされています。経営者一人で対策を考えるのではなく、CYDERのようにコンパクトにまとまった訓練の機会を積極的に利用すると良いでしょう。組織のサイバー攻撃対応力をつけることが、有事に備えることにつながるのです。ぜひ活用してください。

実践的サイバー防御演習「CYDER」	https://cyder.nict.go.jp/

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

第4章

会社を守る、災害に備える、海外での心構え

サイバー攻撃ではなく、大災害やテロに遭った場合、どのようにして事業継続をしたり、あるいは社員や会員の安全を確保して、会社や団体としての身を守る行動ができるのでしょう。

ここではそういった災害に遭った場合の事業継続と海外での活動に関して、ITの側面からアドバイスできることを紹介します。

1 災害時の会社のために事業継続計画(BCP)を作ろう

1 打たれ強くあるために、どこでも作業できる能力

激しい天災に見舞われる我が国では、災害時にどのように事業継続を行うか、人・モノ・金などの面から事業継続計画(BCP)を、きちんと考えておかなければなりません。その備えがないと、災害時に廃業の憂き目にあう可能性も高くなります。

中小企業庁では、「中小企業BCP策定運用指針」のウェブサイト※内で、20項目による「BCP取り組み状況チェック」項目を設けています。ここではIT関連のアイデアから、その項目を達成するのに役立つと思われるものを紹介します。

もっとも役に立つのは、ネットがあればどこでも仕事ができるスキルや環境作りです。

生産設備などがあってその場で離れられない職種ではなく、オフィスでの作業を行う業種・職種の人は、インターネットの利点をフルに生かせます。データを主としてクラウドサービス上に保存し、あとはアクセスするパソコンなどの機器とネット環境があれば、基本的にはどこからでも作業を行うことができます。

また、作業に利用するソフトを、パッケージ版ではなくクラウド版で購入しておくと、災害にあってパソコンが壊れてしまっても、避難先でノートパソコンを購入して、ネットからソフトをダウンロードすれば、かなりのレベルで作業環境を復旧することができます。

最近ではこういったソフトは、クラウド上のデータの閲覧や軽微な修正に関しては、タブレットやスマホからブラウザを使って行えるようになっているので、スマホさえ手元にあれば、とりあえずは手も足も出ない状況にはならないでしょう。

注意するべき点は3点。1点目はそういったクラウドのデータにアクセスしての作業は、ネットカフェなどでも可能ですが、不特定多数の人が触るパソコンは攻撃者が触っている可能性も高いので、そういった場所でのIDやパスワードを入力する作業はやってはいけないこと。

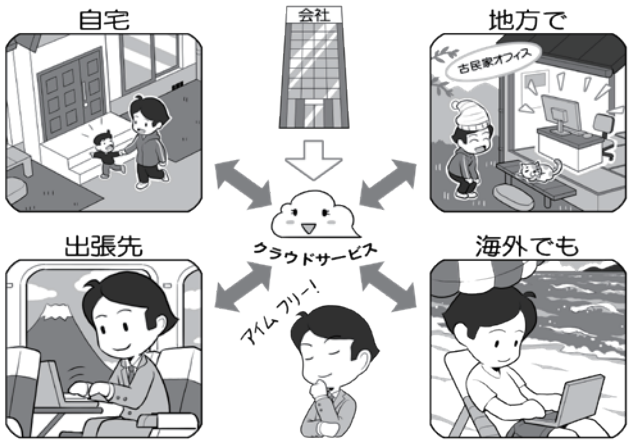
2点目。災害時には被災者が通信を円滑に行えるよう暗号化されていない無線LANが各所で提供されます。これも攻撃されやすいポイントなので、使用する場合はVPNを使うこと。

3点目として、専門用語ではBYOD(Bring Your Own Device)というのですが、災害時であっても個人が所有する機器で業務を行っていると、うっかりマルウェアに感染すれば仕事の情報も漏えいする可能性があります。複数台持つのは面倒ですが、セキュリティを鑑み、業務用には別の機器を用意しましょう。

なお、「このどこからでも作業できるというスキル」は、別段災害時のためだけのものではありません。テレワークといって在宅でも作業ができるようにしたり、出産子育て時にも離職しないで仕事を続けられるようにしたり、あるいは地方に出かけて現地のコワーキングスペースを利用することで自由度高く働き、社員や会員のクオリティオブライフを向上させることもできます。

勿論、ためらいなく出張できるフットワークの軽い企業・団体になるには環境作りが重要です。

クラウドを活用できれば打たれ強くなる



インターネットとは「距離の概念がない世界」です。これはイコール「どこにでもあるが、どこにでもない」と、少し哲学的な考え方になりますが、うまく使いこなせば、物理的な世界の制約を受けないだけでなく、物理的な世界の災害のダメージを受けにくくなることでもあります。

その一つのポイントは、クラウドをうまく使いこなした仕事の仕方だといえます。

※ 中小企業庁 中小企業BCP策定運用指針ウェブサイト https://www.chusho.meti.go.jp/bcp/index.html

2 人的損失をリカバリする能力

もう1つの備えは、社長や代表者、従業員や会員に人的被害が発生した場合にどう対処するかです。

例えば、社長や代表者が事故で亡くなってしまった場合のことを想定してみましょう。

小規模の企業や団体では専任のIT担当者がおかれておらず、社長や代表者が管理者を兼ねているという例は決して少なくありません。そうした企業や団体では、業務用のIDとパスワードなどの管理をどうするかが、事業継続の鍵になる可能性があります。執筆現在でまだ調査中ですが、管理者が亡くなり、100億単位の資金にアクセスできなくなったという事例も発生しています。

このため、普段から社長や代表者の他にデジタルデータなどの副管理者を置くなどの手段を取っておくといいでしょう。いわば人的なバックアップ体制です。

そのなかで大切なのは、上記のとおり業務に使われるウェブサービスのIDやパスワードなどの管理です。

もし代表者が管理している場合、そのデータがスマホに保存されていて、その人しか解除するPINコードを知らなかったとすると、場合によっては事業継続が困難になります。

先ほども述べましたが、そういった意味では管理用の機器は、個人の機器と分離するということが重要ですし、そのPINコードなども複数人が持つことが重要です。

また、それが難しい場合は、例えばクラウドでもアクセス可能なパスワード管理アプリを利用し、そのマスターパスワードやPINコードを、弁護士に託し、なんらかの理由で本人による事業継続が困難であると判明した場合は、弁護士に情報を開示してもらうのです。それは昔、貸金庫の鍵を弁護士にも持っていてもらったのと同じです。

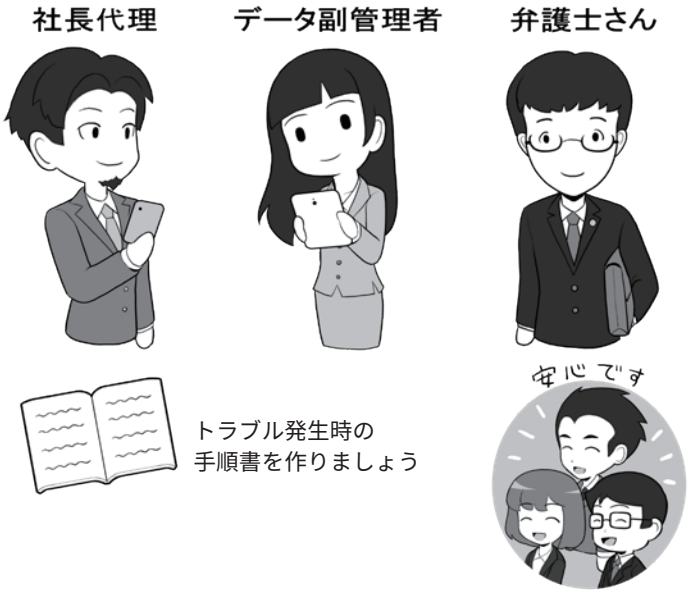
このように災害に遭った場合、どのように事業継続するか、そのバックアップ体制を考えましょう。

具体的に事例をあげ、それにしたがってどのように解決するか、シナリオを作り、それを社内や団体の中で共有しておくといいでしょう。すべては「想定外」にならない想像力がものをいいますから。

1人しか管理者がいないと…

デジタル化のメリットは、逆に管理者になにかあった場合「物理的な手掛かりがない」ことにも繋がります。また、セキュリティをきっちり固めることは、その入口の鍵をなくすとすべてにアクセス出来なくなる可能性もあります。したがって、トラブルが起こったらどうやってリカバリーするか、あるいはデータのバックアップだけでなく、人的なバックアップをどうするかをきちんと考えておかなければなりません。

万が一に備えて人のバックアップ



トラブルに対処する手順書は、物理的な災害による建物や機材の棄損、サイバー攻撃の対処などだけでなく、人的な損害に対するリカバリーも定めましょう。また、人的なバックアップをすることで、重要なデータへのアクセスする資格を複数の人が持つ場合は、だれがアクセスしたかが明確に分かる仕組みにするか、外部の信頼がおける弁護士さんなどに業務を依頼することなどを検討しましょう。

2 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

次は大災害やテロに遭った場合、個々人がどうやって身を守るかです。

最近では各種の自然災害やテロなどが発生すると、その状況をネットにアップする人がいます。しかし、なんらかの災害・テロの発生や避難勧告が発表されたら、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。

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。無事家族や同僚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。

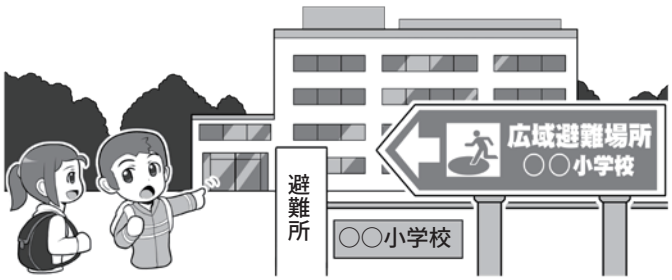
避難場所に到着し、そこが安全であると確認できたら、安否確認の連絡や情報収集をしましょう。

安否確認サービスはさまざまなものがあるので、事前に家族や同僚たちと、どのサービスを利用するかを決めておきましょう。また、災害時は電話やウェブサイト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、なるべくデータ通信量の少なくてすむ、メールやSNSのメッセージ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優先しましょう。

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や同僚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、街中なのにスマホが圏外になったら、それは通信用の基地局が被害にあって壊れている印です。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のメールやSNSを利用しましょう。災害時はその方がつながりやすく、また、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るようにしましょう。いざというときに備えてACアダプター一体型の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。

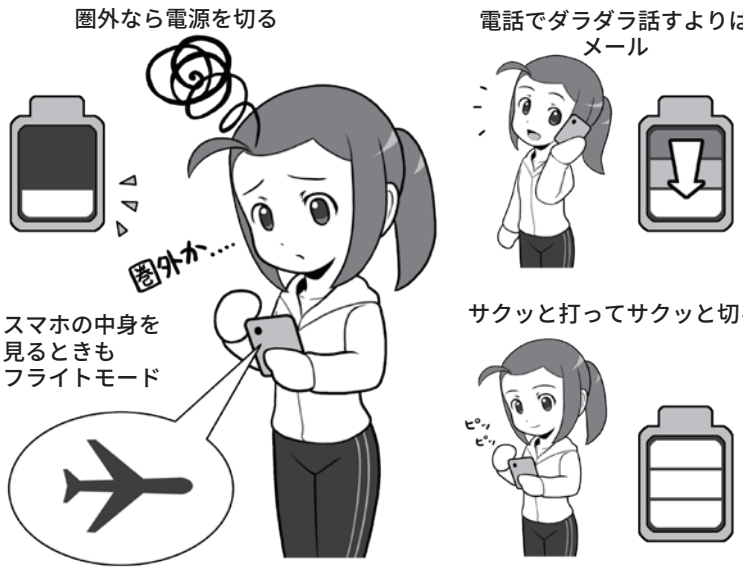
災害直後は情報が錯綜しますが、一定時間が経過すると救援物資や脱出ルートなどの情報がネットに掲載され、やがて整然とした情報発信が行われるようになります。

しかし、だらだらとウェブサイトを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や遠隔地にいる同僚に助けを求め、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、帰宅できなくなった方たちが、SNSを通じて友人に被災地から家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。同僚たちと検討してみましょう。

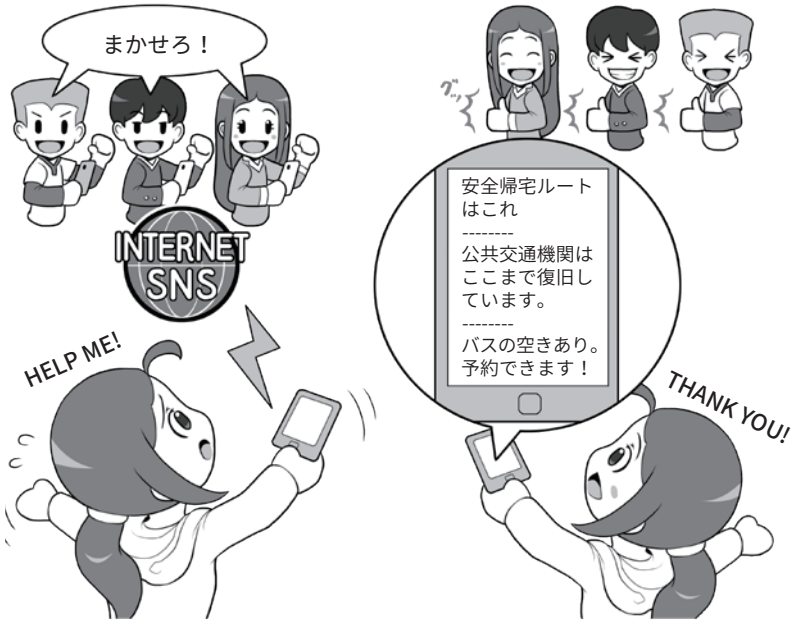
ぜひそういった事例をみんなで話し合って、いざというときにどうするか、ということを相談しておいてみてください。

電池をもたすテクニック



電波が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。ACコンセントがあれば充電器にもなる一体型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・同僚に相談して、いざというときは情報収集や必要な交通手段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、通信用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可能性があります。

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TV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、私たちは受信するだけなので、ウェブサーバのように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。

比較的近距離を放送のエリアとするテレビや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と同じように被災して活動できなくなってい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、FMと比較して少なくなります。

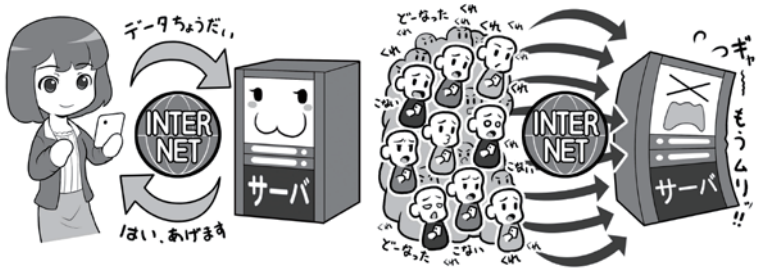
これが災害用の持ち出し袋にAM放送を受信できるラジオを入れる理由でもあります。

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。なお乾電池は、定期的に液漏れをチェックしましょう。

また、自分が持っていないと意外と忘れがちですが、車の中ならAM/FMのラジオ、一部はテレビも受信できます。

災害時のアクセス集中によるサーバの沈黙(双方向通信)

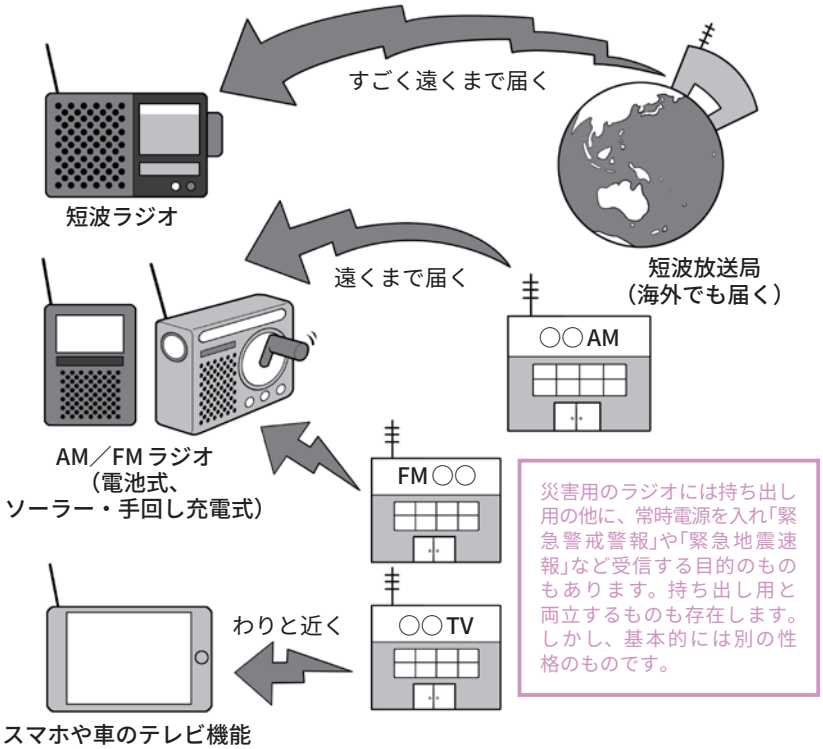
平常時　　災害時



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、情報が閲覧可能になります。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による沈黙(サーバーダウン)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他に、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こともありますが、AMではかなり遠くまで届くので別の地域のものを拾うことができる場合もあります。短波にいた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、ワンセグ搭載のスマホは少なくなりましたが、通常のテレビ受信可能な車のカーナビが増えてい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きましょう。日没時や降雨時の避難場所などもわかります。

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アダプター一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、充電用ケーブルなどを持ち歩きましょう。

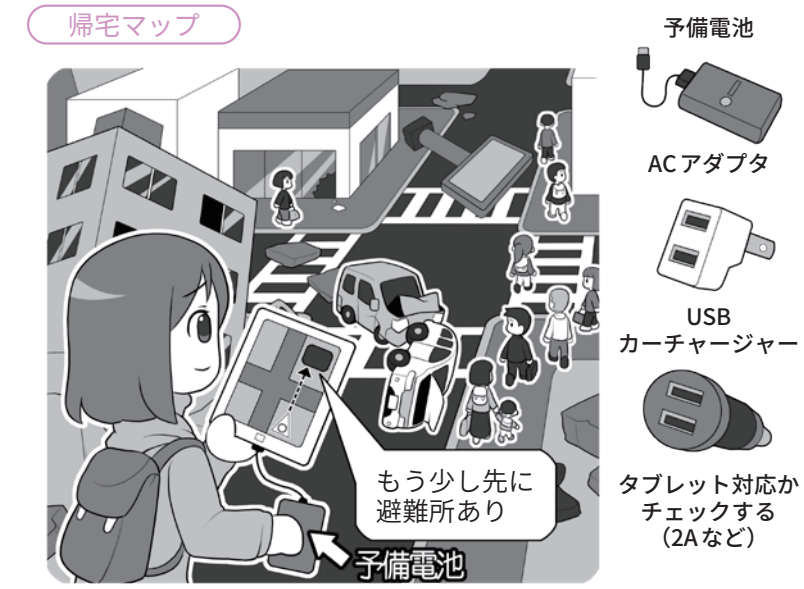
海外出張や旅行時の災害やテロに備える場合は、事前に外務省の「海外安全ホームページ」で渡航先の情報を確認し、渡航が推奨されない地域には行かないようにしましょう。

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、ショートメッセージ(SMS)を受け取れるようにしましょう。

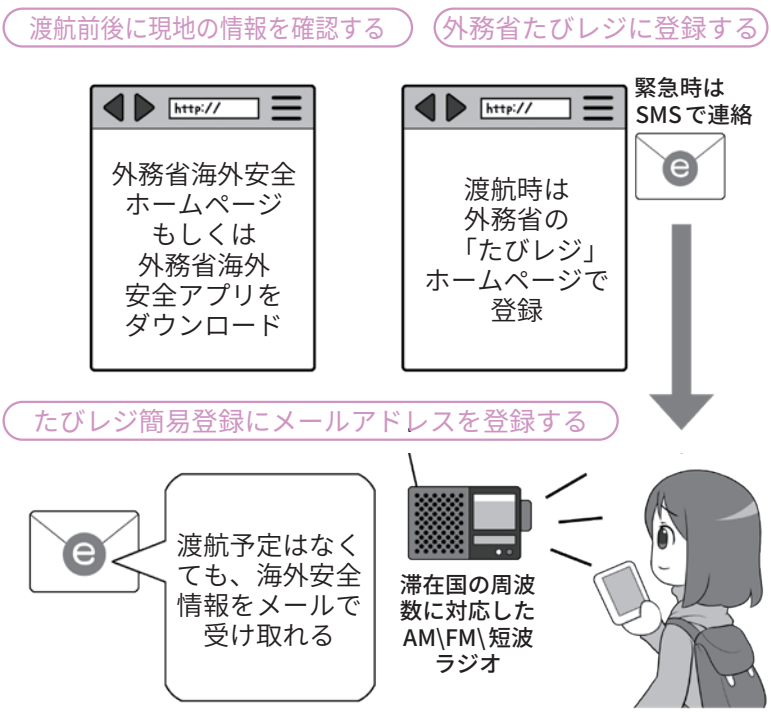
「海外ではどういう風にデータ通信をするか」を前提に考え、特にデータ通信しない場合でも、いざというとき、慣れない土地で身を守るためには、最低限上記のSMSメッセージは必要なんだと覚えておきましょう[*1]。

災害時に徒歩帰宅をする場合は



災害時は、政府方針で最大3日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大切です。ACアダプター一体型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(主に2Aや2.1A対応と書かれている給電能力が推奨)。

海外での災害やテロに備える場合は



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ホームページ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。

*1：ショートメッセージ(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。

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出張や旅行に持って行き現地で使う場合、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を交わさないまま、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、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、利用したらいくらなのかをよく確かめておきましょう。さもないと払い切れ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。

データ通信が使えなくも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、貴重な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(高額ですが)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。

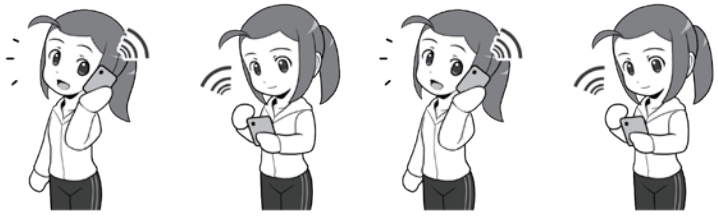
もし長期で滞在する場合などで、

海外で電話やデータ通信を使う

海外携帯電話会社

普段の電話番号で着信できるようにする

電話番号が現地のものになってもいい



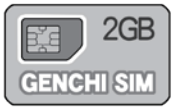
音声利用：マイ端末で(音声)ローミング

データ通信利用：マイ端末でデータローミング

音声利用：海外はSIMフリー相当のマイ端末か、SIMフリー端末と現地SIM

データ通信利用：海外はSIMフリー相当のマイ端末か、SIMフリー端末と現地SIM

現地SIMは現地空港などでも買えるが……



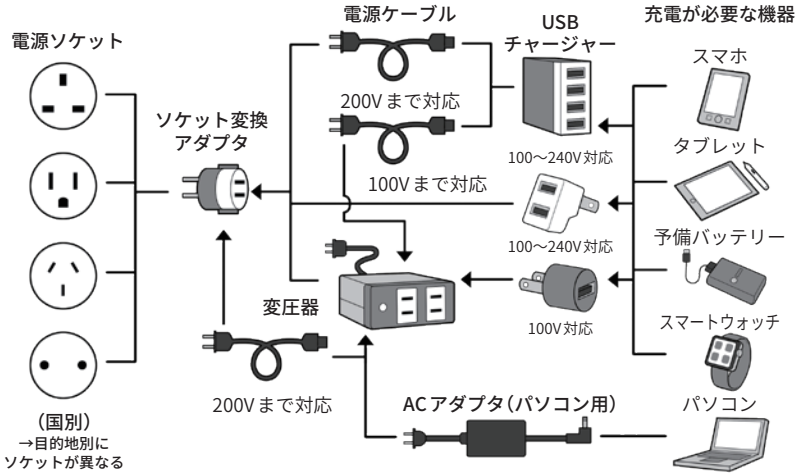
- 日本で買えることも(SIMのサイズに注意)
- 事前使用設定を済ませておく
- 音声の料金、データ通信の上限容量をチェック
- 月額料金が発生せず、チャージすれば保存可能なものもある。何回も訪れるなら選択肢に
- 料金は従量制か、上限のある定額制か確かめる

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くことを推奨します。

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、ケーブルまでもが200V対応かをチェックします。

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認することです。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」を行ってくれる場合もあります。

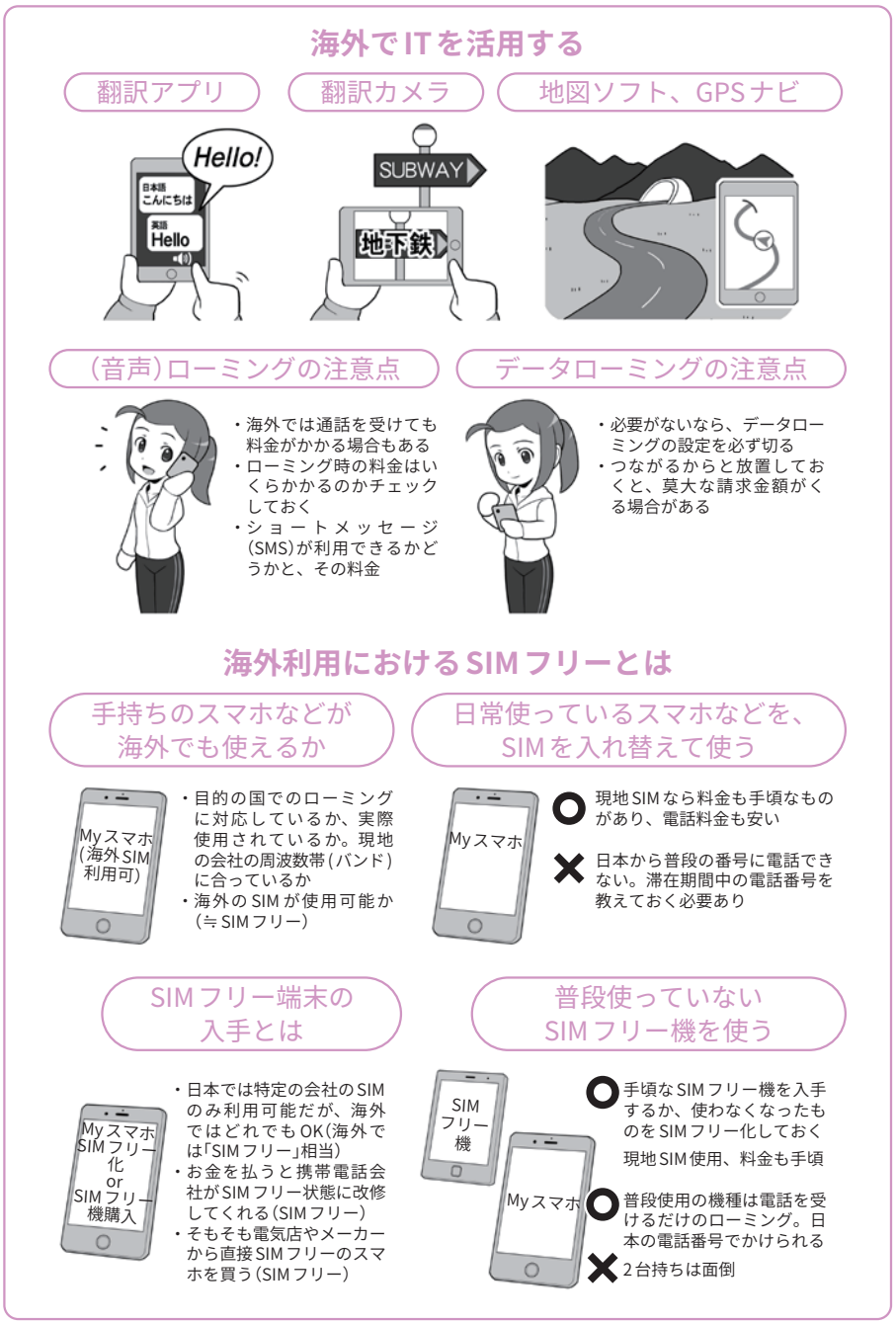
忘れがちなのが充電に関することです。充電器の対応電圧と、充電器にケーブルがある場合はこのケーブルの対応電圧が訪問国の電気事情にあっているか確認して、必要に応じ変圧器を利用し、現地のさまざまなタイプの電源ソケットの形状に対応できるソケット変換アダプターを用意しておきましょう。

次に、せっかくスマホなどを海外に持っていくのなら、海外で使えるアプリや役立つアプリ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、該当の地域の地図データを、あらかじめスマホ本体にダウンロードしておけるものを準備して行きましょう。



コラム：デマに踊らされない!

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。

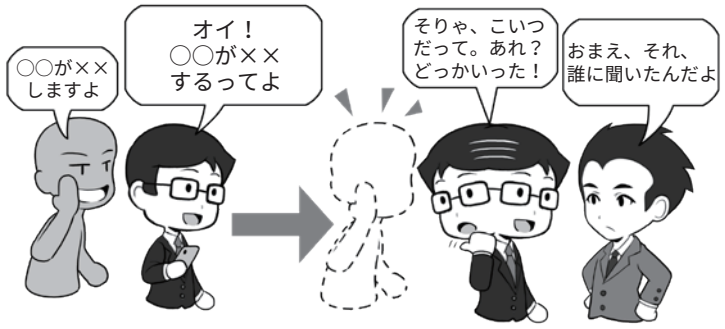
当時は人から人への口伝えでした。自分が聞いた話を再度確かめようと思っても、すべて遡っておおもとの発言者までたどるのは至難の業で、その分「うわさ」ということを前提とした「不確かさ」「あやしさ」がありました。

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な時間が消えた世界」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」ということが数字としてついて回るので、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いたなんてこともあります。

そしてこの構造は「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。

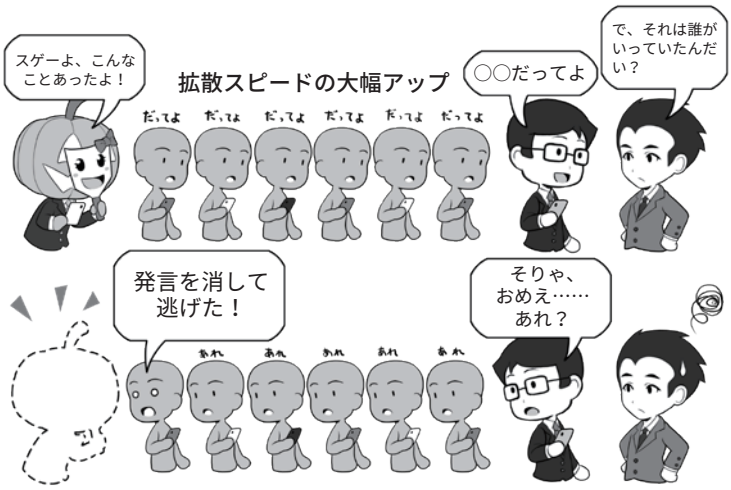
情報が勢いをつけて手元に飛び込んできても、その勢いに飲まれて拡散に加担せずに、情報の信憑性を確認する余裕を持ってください。

昔から出所が不確かなデマはあった



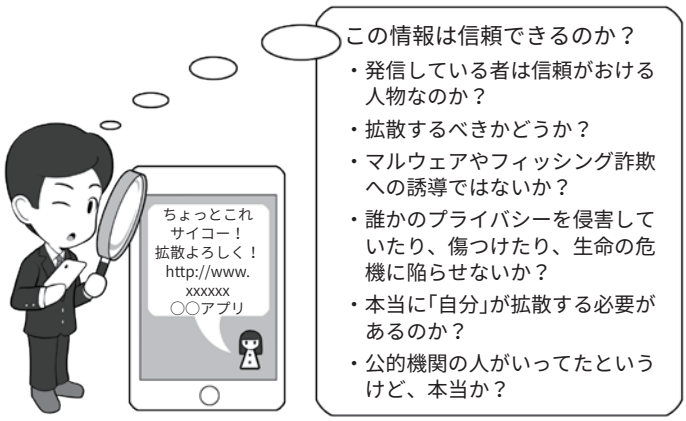
かつてのデマは、人間がしゃべるスピードでしか拡散しませんでしたが……。

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



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は、特にないものなのです。

災害時には本業の人ですら間違った発信をしてしまうこともあるので、業務では特に情報の取扱いには注意を！

コラム：モラルを逸脱して炎上しないために

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です。

例えば未成年が飲酒ありの大宴会をしたり、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社員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。

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が発生します。

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すことです。また、本人にも損害賠償責任が課せられ、会社にも評判による業績への影響が発生し、経済的損失を伴うことです。

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、「投稿をさせないか」しか解決策はありません。

しかし、社員や会員が成人だった場合どうすればいいのでしょうか。本来ならば成人として持っていてしかるべきモラルともいえるのです。

ただ、現実問題として「炎上」が発生していることを鑑み、これを避けることを目的に、情報モラル教育を実施し、あるいはみんなで勉強会をやって意識あわせをしてみるのはどうでしょう。

ネットでの炎上例を挙げ、どのような書き込みがどのような経緯で炎上を生むのか、みんなで考え、そのような結果を招かないように、意識のずれをすりあわせるのです。

SNSは上手く使えば会社や団体に取って、コストのかからないいい宣伝告知手段です。それが上手く使えるように、みんなで勉強しましょう。

コラム：経営者のデジタル相続「終活ノート」

事業継続に関する項目では、災害時などに経営者や代表者が行動できなくなった場合の事業継続の問題を取り上げました。それにより当面の事業を行うための備えに関して記述したわけです。

しかし、それ以外にも長期的には備えておかないといけないことがあります。本人が代表者として、あるいは個人として行っていた契約は、それをきちんと解除するか相続しないと、思わぬ負債を生み続けるからです。

特に大きな金銭的問題になりやすいのは、金融商品を放置することです。

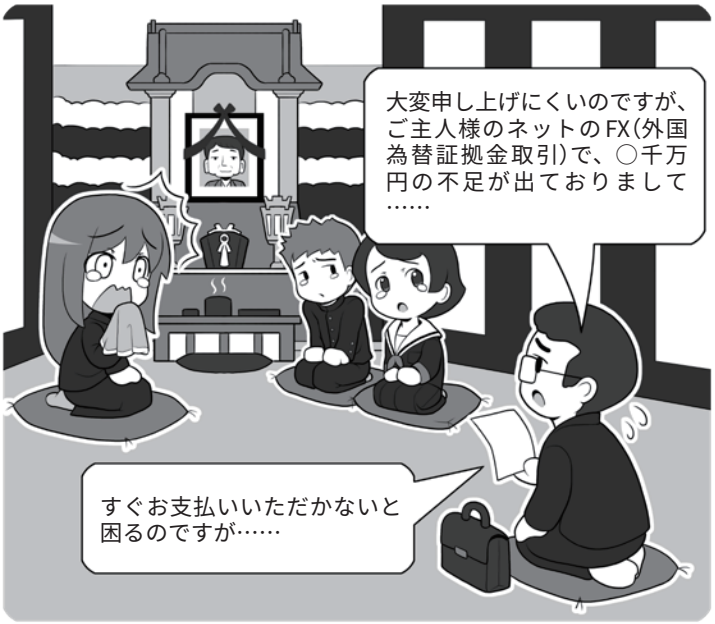
「FX(外国為替証拠金取引)で取引をしたまま亡くなった場合、取引が継続されていて、その後相場が大きく変動して、知らないうちに負債が発生した」

「仮想通貨の取引をしていたようだが、どこにあるのか分からない。金額によっては相続税を払わなければならないのに…」

そういったことが起こらないように、IDとパスワードの管理を引き継ぐ準備だけでなく、どこに対してどのような契約を結び、どういう支払いをしているか、どういう金融商品や不動産などを持っているか、それをどうして欲しいか、そういったものをまとめておく、終活ノートを作っておきましょう。

こういった取引は以前であれば郵送で行われたので、郵便物をめくっていけば大抵のことは分かったのですが、最近ではメールなどデジタル的にやり取りすることが多く、管理するパソコンをパスワードで厳重にガードしてしまうと、その概要を掴むことすらできなくなってしまうからです。

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会社や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、イコール支払いや負債が発生し続ける可能性があり、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。「終活ノート」にきちんとまとめていくことをお薦めします。

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

第5章

IT を使った効率化による セキュリティコスト捻出

サイバーセキュリティを固めるために資金を投入したいのだが、そのための余裕がない、ということも考えられるでしょう。

しかし、インターネットを利用することによる効率化を上手く取り入れれば、その分で浮かせたコストを、セキュリティ用の投資に回すことができます。

具体的な例をいくつかご紹介しましょう。

1 社内・社外のセキュリティ向上

1 セキュリティ思想を取り入れ、負のコストを発生させない

業績を圧迫するコストとは、どうやって発生するのでしょう。一つは業務を遂行する上で支払わなければいけないお金が増えるときです。もう一つは、イレギュラーな事態が発生して、そのリカバリのために人、お金、時間を割くときです。

この後者のロスというのは、なにか問題が発生してそれに誰かが掛かり切りになり、その期間中「利益を生む」ことができなくなることで発生する完全なる負のコストです。

ただ、トラブルを根本的に防ぐことは難しいので、その発生を予期して備え、利益を生まない負のコストによる業績の下ブレをなくす努力をするわけです。

サイバー攻撃による突発的なトラブルは、まさしくこの例に当てはまります。したがってサイバーセキュリティを強化して備えるメリットはここにあるのです。

「セキュリティを強化する」といわれても「正直うちが攻撃されるなんて万に一つもないだろう」というのが小さな会社やNPOの運営者の本音ではないでしょうか？

その考え方が甘いのは、はじめにお話したとおりです。攻撃者は冷酷にセキュリティが甘い所から、企業や団体の規模にかかわらず攻撃してきます。サイバー攻撃の数も被害額も年々増加傾向にあるのです。

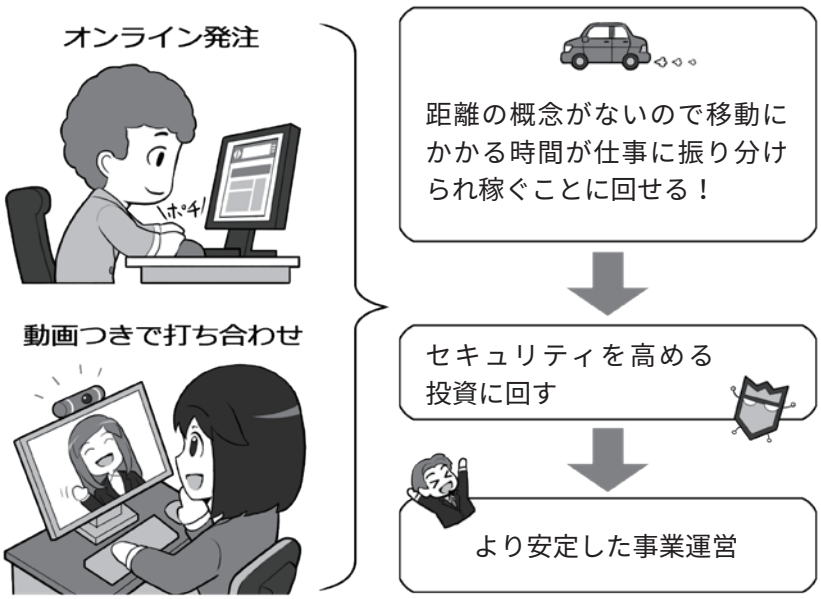
近年では「セキュリティ・バイ・デザイン」という考え方が一般的になりつつあります。企業のITシステムや業務プロセスなどを設計する段階でセキュリティ対策を組み込んでおき、サイバー攻撃による不測の事態に備えるのです。

小さな会社やNPOも例外ではありません。持続的な運営を行うために、きちんと備えましょう。

負のコストの発生例

利益を生むためのコストは必要ですが、備えをしなかったために発生し、そのリカバリのために多大なるマンパワーを割くことは「利益を生まない」完全なる負のコストです。そういったことを起こらないように準備するコスト（費用）は、実は利益を生むための投資なのです。

インターネットの利点を生かしてコストを減らす



インターネットのメリットを生かして、利益を生まない負のコストを減らし、その分をセキュリティの為の投資に使いましょう。距離とその移動に必要だった時間がなくなるという点を生かしましょう。多くの場合、無駄な移動とそのための時間をなくすことから始まります。

2 インターネットの特性を生かして投資資金を捻出する

しかし、「セキュリティに事前に備えるといわれてもそんな資金ないよ…」という経営者の方も少なくないのではないでしょうか？

ならばインターネットの特性を生かしコストを減らす手段もあります。

例えば、私たちが家から会社に出勤する場合、通勤時間と運賃が必要になります。しかし、インターネットとは「距離とその移動に必要だった時間が消えた世界」です。デジタル化できないものを除き、すべてこのインターネットの利点を生かすことで、時間や移動費をカットでき、それが「コストを減らす＝利益を生む」わけです。

また、この考え方で「在宅勤務」を評価して見て下さい。視点を変えるとそのメリットが分かるでしょう。

コストの視点を持って、インターネットの特性をあてはめると、業務上の様々なものでコストを削減でき、そこで浮いた分をセキュリティへの投資に回すことで、不必要な「負のコスト」を発生させない、仕事の質を高める「さらなる投資」にすることができるわけです。そして下ブレの無い経営も安定するのです。

さらに、今使っている業務にまつわる環境が、本当に現在の事業にとって効率を上げているかを再検討しましょう。

ITを導入する目的は、本来従業員の生産性を上げることのはずです。しかし、検証すると、オフィスに導入している業務システムが業務の効率を上げているどころか下げているという例も少なくありません。

逆転の発想で、各種IT機器や広いオフィスが本当に要るのか、専用の机がいるのか、いるとしたらなぜなのかを検証しましょう。

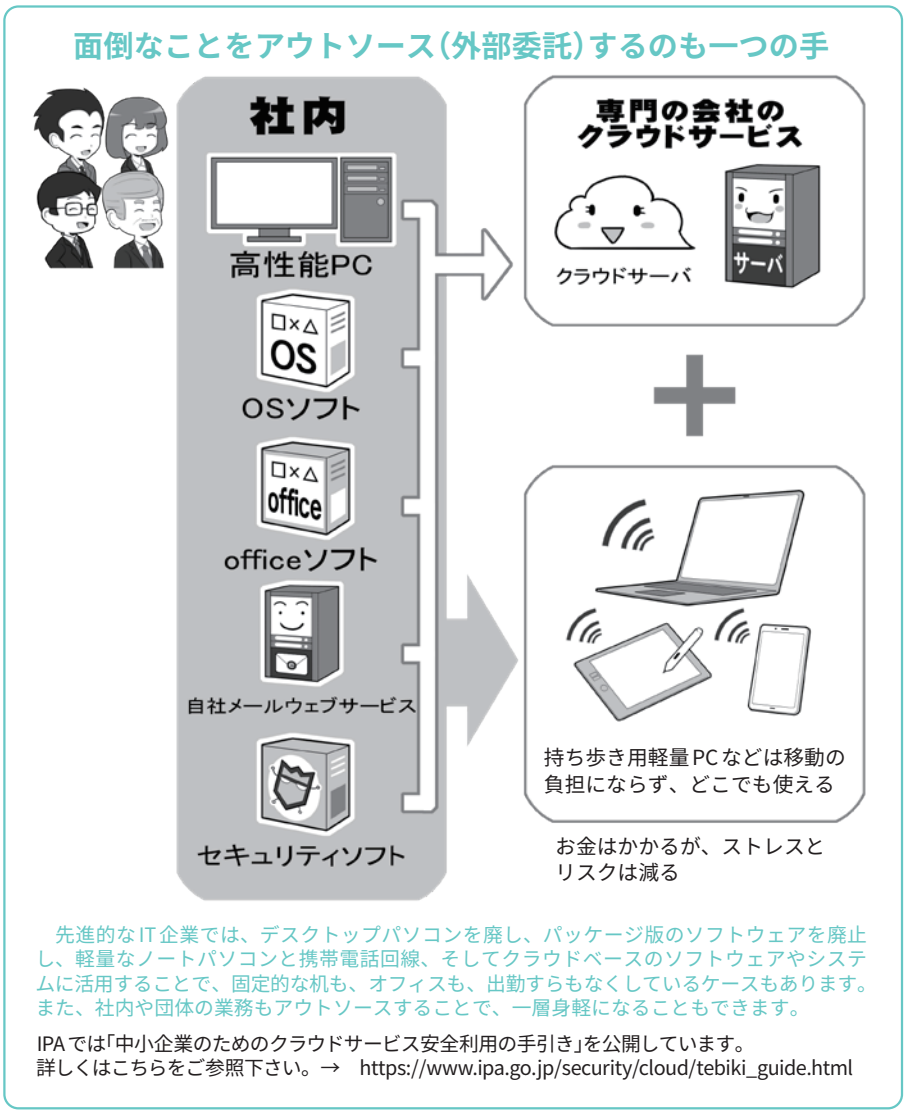
机が必要なのは書類を置くスペースが必要だからで、書類をデジタル化できれば固定の机はいらなくなるといった発想です。

また、近年では企業の業務システムをクラウド業務スイートに切り替えるケースが増えています。クラウド業務スイートは、業務用ソフト、クラウドストレージ、ウェブサーバなどが一つのパッケージとして提供され、どこからでもノートパソコンなどでアクセスして業務が行えます。

これにより従来は会社に縛られていた従業員にテレワーク環境を提供したり、スマホを利用して安全に業務連絡を行うことが可能になったりします。

そうしたシステムでは、事務所経費や事務コストを抑えつつ、小規模の事業者でも大規模な企業と同じレベルのセキュリティを確保できるのです。

そのように業務効率を改善すれば会社の業績も改善され、さらに高いレベルのセキュリティを実現する投資に回すことができるようになる、それが企業や団体にとっての生存戦略の一つになるのです。



先進的なIT企業では、デスクトップパソコンを廃し、パッケージ版のソフトウェアを廃止し、軽量なノートパソコンと携帯電話回線、そしてクラウドベースのソフトウェアやシステムに活用することで、固定的な机も、オフィスも、出勤すらもなくしているケースもあります。また、社内や団体の業務もアウトソースすることで、一層身軽になることもできます。

IPAでは「中小企業のためのクラウドサービス安全利用の手引き」を公開しています。
詳しくはこちらをご参照下さい。→　https://www.ipa.go.jp/security/cloud/tebiki_guide.html

2 適切な個人情報の取り扱いのために

個人情報の取扱いに関することは、「負のコスト」を発生させないための重要な要素です。

個人情報の保護に関する法律（いわゆる個人情報保護法）では、以前は5千人以下の個人情報しか管理していない事業者は対象外でしたが、平成27年の法改正により平成29年5月から管理数に関係なくすべての事業者が対象となっており、すべての事業者がその管理には細心の注意を払うことが必要になりました。

これは中小企業だけでなく、個人事業主、NPO法人、あるいは町内会・自治会、学校の同窓会なども対象となり個人情報を取り扱う際のルールを遵守することが義務づけられます。

個人情報保護法では個人データを第三者に提供する場合、本人の同意を得る必要があると規定しています（第23条）。

これに違反しますと、個人情報保護委員会から指導などを受け、会社の社会的信用を損なう可能性があります。

個人情報保護委員会では、平成29年6月に「はじめての個人情報保護～シンプルレッスン～」として、「中小企業向け『これだけは！』10のチェックリスト」を公開しています。

その中では、特にパソコンでのデータの保管は、システムを最新に保つ、セキュリティソフトを入れる、ログインパスワードの設定やデータを暗号化するといった事項が掲載されています。この本で書かれているセキュリティ事項をクリアしていれば大丈夫ですが、より安全に保護するためには、個人情報を取り扱うパソコンを明確にし、不必要にネットにつなげたり、USBメモリを使ってデータを抜き出すことができないようにすることが必要です。

また、使用していないときは、個人情報を記録したパソコン、もしくはデータが自動的に暗号化される外付け記憶装置を使っている場合はそれを、物理的に鍵がかかるロッカーなどに保管して、流出事故を起こして完全なる負のコストを発生させないようにしましょう。

巻末資料 中小企業向け「これだけは！」10のチェックリスト

分類	No	チェック項目	ポイント	関連ページ
取得・利用	1 ☐	取り扱っている個人情報について、利用目的を決めていますか？	目的は具体的に。 ○「新商品のご案内の送付のため」 ×「当社の事業のため」	P4
	2 ☐	その利用目的は、本人に通知するか公表していますか？	取得の状況からみて利用目的が明らかなら、通知・公表は不要。	P4
保管	3 ☐	（組織的安全管理措置） 個人情報の取扱いのルールや責任者を決めていますか？	個人情報の保管場所や漏えい発生時の社内の報告先は決まってますか？	P5・6
	4 ☐	（人的安全管理措置・従業者監督） 個人情報の取扱いについて従業員に教育を行っていますか？	個人情報の保管場所等のルールは周知できていますか？	P5・6
	5 ☐	（物理的安全管理措置） 個人情報が含まれる書類や電子媒体について、誰でも見られる場所・盗まれやすい場所に放置していませんか？	不要になった情報は適切に廃棄・削除することも大切。	P5・6
	6 ☐	（技術的安全管理措置） パソコン等で個人情報を取り扱う場合、セキュリティ対策ソフトウェア等をインストールして最新の状態にしていますか？	ログイン時にパスワードを要求したり、ファイルにパスワードをかけることも大切。	P5・7
	7 ☐	個人情報の取扱いを委託する場合、契約を締結する等、委託先に適切な管理を求めていますか？	委託先にも安全管理を徹底してもらうということ。	P5
提供	8 ☐	本人以外に個人情報を提供する場合、本人に同意をとっていますか？	法令に基づく場合（警察や裁判所からの照会等）や、委託に伴う提供には同意不要。	P7
	9 ☐	本人以外に個人情報を提供したり、本人以外から個人情報を受け取る際、相手方や提供年月日等について記録を残していますか？	法令に基づく場合（警察や裁判所からの照会等）や、委託に伴う提供には記録不要。	P7・8
開示請求等	10 ☐	本人から自分の個人情報を見せてほしいと言われたり、訂正してほしいと言われた際には、対応していますか？	開示等の請求に対応する人は決まっていますか？	P9

※このチェックリストは、主に中小企業を対象に、個人情報保護法を遵守できているかどうか確認する際の参考に作成したものです。個人情報保護法のルールの詳細は、本シンプルレッスンの関連ページや、個人情報保護委員会のガイドラインを参照してください。

出典：個人情報保護委員会ウェブサイトより https://www.ppc.go.jp/files/pdf/1711_simple_lesson.pdf

3 取引先の監督を徹底

自社のセキュリティを高めていたのに、大事なデータを渡していた関連会社や取引先がずさんな管理を行なっていて、個人情報を流出させてしまった……。

そんなときに「関連会社がやったから……」というのでは、国民や社会の理解を得ることができないのは、これまでの情報流出の事例を見ても明らかです。

自社が持っている個人データの取り扱いを、利用目的の達成に必要な範囲内において委託する。そのことに伴って取引先に当該個人データを提供する場合には、本人の同意に基づき取引先に提供する場合と異なり、記録義務はありませんが、一方で取引先を監督する義務を負います。

具体的には

1．プライバシーマークを取得するなど、きちんと個人情報を取り扱える能力のある業者を選定すること

2．取扱の内容を契約書に明記すること

3．契約の内容が守られているか定期的に監査すること

が義務づけられます。

詳しくは個人情報保護委員会のウェブサイトなどを参照して欲しいのですが、こういったことをきちんと行うことが、個人情報を厳密に扱う姿勢として委託先に示されることで、不正な個人情報の流出への抑止力になると考えて下さい。

P71で紹介したように、企業のグループ内であっても同様で、問題が発生したときに「関連会社が」とか、「委託先が」といって責任を逃れることは許されず、会社や団体の社会的な義務を果たし、また、流出した情報に関してはきちんとした責任を負わなければなりません。

流出がおきれば、実際のお金としての負のコストや、それに対処するためにマンパワー、信用喪失が見えないコストとして、自分たちに跳ね返ってくるのです。

取引先が自分と同じリテラシーを持つとは…

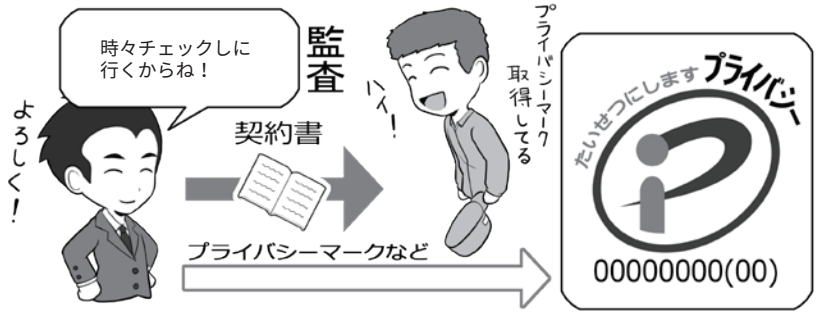
個人情報やプライバシーに関して、きちんと管理しなければならないことであるという意識は広がりつつありますが、それは自社や自団体の中だけにはなっていませんか？

その意識は取引先や委託用務先まで徹底されてるでしょうか？

自社や自団体と委託先は別ではなくて、例えば宛名を渡して発送業務を行う場合でも、その個人情報にまつわる監督責任が発生します。また、委託先が自社や自団体と同じリテラシーを持つと安易に考えないで、確認を怠らないようにしましょう。

専門性のある委託先に業務をアウトソースしてコストを抑えるのはよいことですが、抑えるべきポイントは抑えましょう。

自分たちも相手もトラブルにならないために



個人データを取り扱う業務を委託する場合は、委託先を監督する義務が発生し、一定条件を満たしプライバシーマークを取得しているかなどを確認し、個人データの取り扱いに関して契約書に明記し、その内容が守られているか定期的に監査するなどの対応が必要となります。

なお、プライバシーマークに関しては一般財団法人日本情報経済社会推進協会(JIPDEC)のウェブサイトの、プライバシーマーク制度のページに詳しく記載されているので、参照してみてください。また、実際に取得する場合は、職種によってはそれぞれの職種の団体を通じて取得申請をする場合があります。

日本国内であっても海外の方の個人情報を取り扱う場合は、EUのGDPR(一般データ保護規則)など、さらに注意が必要な法制度がありますので、業務を行う前に精査しましょう。

・プライバシーマーク制度(一般財団法人日本情報経済社会推進協会)
https://www.jipdec.or.jp/project/pmark.html

・GDPR(General Data Protection Regulation: 一般データ保護規則) 個人情報保護委員会
https://www.ppc.go.jp/enforcement/cooperation/cooperation/GDPR/

4 テレワークとアウトソーシング

1 テレワークの活用

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えた世界」です。したがって、ネット上でやり取りできる業務形態であれば、その特性をフル活用できるわけです。

ポイントは、やり取りするデータが「デジタルの情報」にできること。また、移動に必要な時間やコストによって失われていた仕事の機会を取り込むことです。

オフィスに出勤しなくても、メールや業務用の文章、表、プレゼン資料、チラシ、印刷物、写真、ビデオにまつわる作業はすべて可能です。「オフィスで顔をつきあわせないとコミュニケーションが取れない」という方も、大きなテレビやモニターを活用したテレビ電話を使えば、ニュアンスを含めたコミュニケーションが取れますし、それは1対1に限らず、多人数でも可能です。

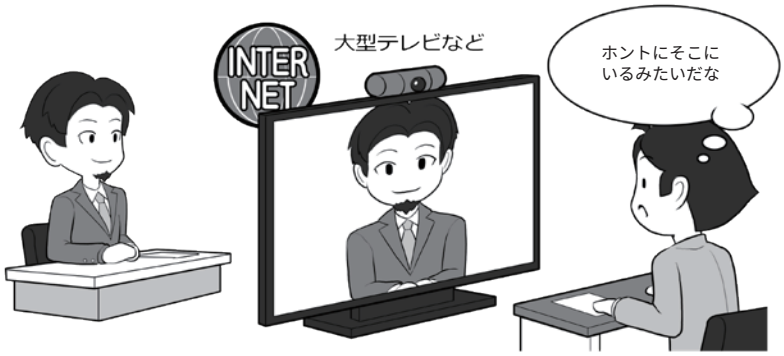
現在はクラウドを有効活用する業務用ソフトウェアがセットになった「スイート」が発達しているので、世界中のどこからでも、同じデータを共有して作業をすることができます。必要なものをしいてあげれば「高速なインターネット回線」でしょう。

機会を取り込むという面では、物理的距離の制約がありませんから、世界中のどこにいる人とでも会社を作ったり、腕に覚えがある人を見つけて一緒に仕事することができます。結婚、出産、子育て、Uターン、Iターンなどで、引越したり通勤が困難になったりした場合でも、自宅にいながら空いた時間を活用して仕事を続けることもできます。

さらに、世界中にあるコワーキングスペースや、サテライトオフィスを活用して、旅行しながら仕事をすることも可能ですし、そうでない方にはあまり切迫感が感じられないかもしれませんが、花粉症の方や、梅雨、寒さが苦手の方は、その季節だけ、花粉が飛ばない地方、梅雨がない地方、温暖な気候の地方に行って、仕事をすることもできます。

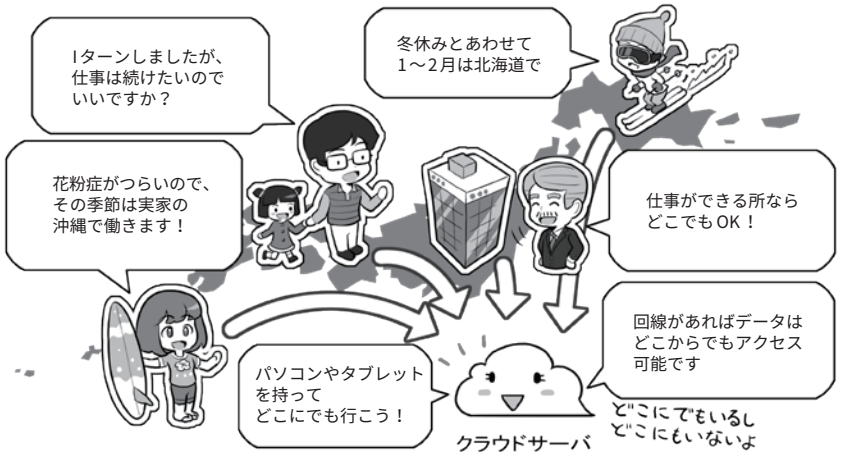
場にとらわれない働き方ができる、ということを前提に、仕事の仕方を組み直してみるといいでしょう。

大きなモニターを使ったコミュニケーションの活用



ビジネスは顔をつきあわせるのが基本とは昔からよく言われることですが、大きなモニターに表示されるリアルタイムの等身大映像は、そういったコミュニケーションに迫ります。最初は実際に訪問し挨拶を交わし、メールや電話ではニュアンスが伝わらないと思ったら、こういったコミュニケーションを導入する提案をしてみましょう。手元で作業ファイルを共有しながらコミュニケーションすることもできます。

ネットがあればどこでもテレワークできる



業種、職種にもよりますが、オフィスがあってそこに出勤しなければならない理由を、逆に考えてみましょう。顔を合わせなければいけない、きちんと仕事をしているか分からないといった要因は、ネットを使って映像をつないでおくと言ったことでも十分に管理できます。それよりはネットの特性を生かし、社員や会員のモチベーションを上げる選択から組み立ててみましょう。いろんなところにいるがゆえに、生まれるアイデアもあります。

2 効率的なアウトソーシング

もう一つのインターネット時代のメリットは、気軽に専門的な業務をアウトソーシング（外部委託）できることです。

従来であれば、なにかモノを発注する、業務を委託するといった場合、物理的な距離に縛られました。しかし、現在では、自分が望むサービスをインターネット上で検索すると、さまざまな専門の業者を、オンラインで見つけることができます。

例としてあげると、例えばチラシやパンフレット、および印刷物全般などは、オンラインの印刷業者がウェブサイトを設けており、そこで目的のものを探して紙質などを指定すると、どれぐらいの部数がどれぐらいの印刷日数で、いくらぐらいでできるかが明確になっています。

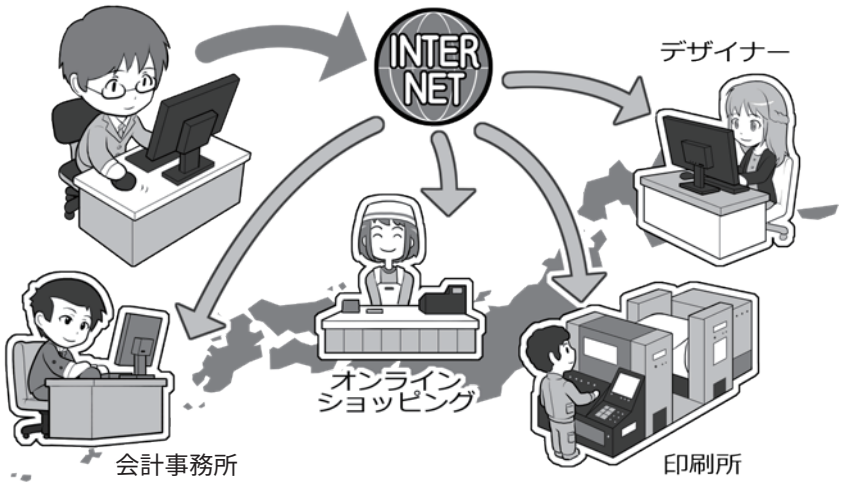
あとはこれらの業者が、印刷原稿として受け付けている形式のデータを作るスキルがあれば、24時間365日印刷物が発注できるわけです。

また、経理処理なども会計ソフト会社がオンライン対応になることで、取っておいたレシートをスキャナやスマホの撮影機能経由で提供されているクラウドサービスにダイレクトにアップロードすると、基本的な伝票入力が行われた状態で会計ソフトに返ってくるようになっているものもあります。

仕事で使う資材でも、図面を送信すれば、金属板をレーザーでカットして穴開けまでしてくれたり、簡単な折り曲げ加工をしてくれるもの、あるいは従来ならば専門店でしか購入できなかったものが、オンラインで購入できるようになっているので、まずは、ダメ元だとおもって検索をしてみましょう。

そうすることで、いままでの業務の効率化が行え、必要だったコストや時間を省くことができます。

どこにいる人とでも仕事ができる

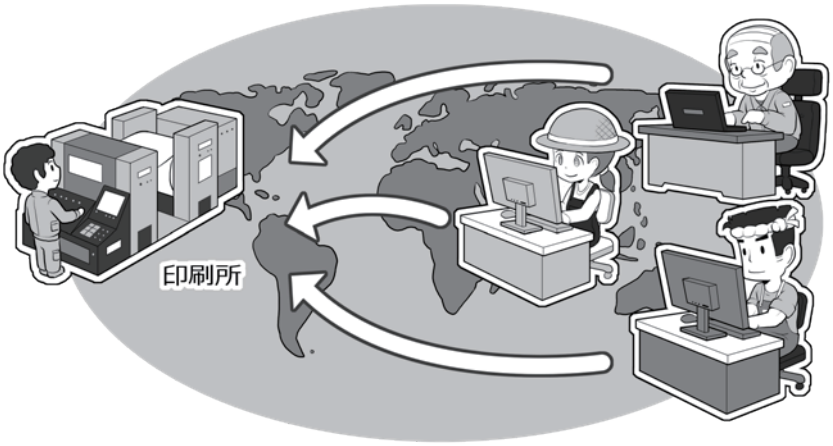


社員がどこにいても仕事ができるのと同様に、地方に住んでいる専門分野の人たちと仕事をする制約も少なくなります。場所ではなく求める技術を基準にフリーランスの人を探して仕事を依頼することもできますし、自社で原稿だけを作り、制作や印刷といった後工程の業務を、遠方のプロにオンラインで発注することもできます。場合によっては特定の業務を行う自分の手間と発注のコストを計算して比較して、それをアウトソーシングすることで、自社や自団体が自らが得意とする分野に注力して能力を向上し、逆に選んでもらえるプロになりましょう。

セキュリティ系業務もアウトソースできる

日常的なサイバーセキュリティに関する業務も、専門業者にアウトソースすることが可能です。どういった企業に依頼したらいいか判断しにくい場合に備えて、経済産業省とIPAでは一定の基準を設け、これを満たした企業のリストを公開しています。詳しくはP148を参照してください。

製品を扱うなら全世界が市場



自社や自団体が何かの製品や物品をつくって販売や提供する場合も、ネットを活用すればその対象が全世界になるといっても過言ではありません。昔であれば距離の壁に阻まれ小さなマーケットに閉じ込められていた地方都市の小さな会社でも、ネットの時代の特性を活かして、世界的にビジネスを行えるようになった例もあります。

もちろん発信する情報を翻訳したり、時には海外の方とコミュニケーションする必要もありますが、そういった言語的な問題はいずれIT技術で解決されるでしょう。とくに伝統技術などは「存在が知られていない」ことが、海外でのチャンスを逃がしていることもあるのです。

5 フリー素材とコンテンツ利用のスキル

インターネット上の素材を利用する上で、知っておくべき概念として、いわゆる「フリー素材」とよばれているものがあります。

「ネットにあがっているモノは著作権が無く勝手に使っていい」ということではなく、ネット上では「誰もが自由に使えるように、著作権者の好意で提供されているさまざまなコンテンツ」があり、これを見つけることができるということです。

この点を良く理解せず、確認しないままコンテンツを勝手に使ってしまい、その結果炎上案件となると、不必要な負のコストを生んでしまうことになります。

一口に「コンテンツ」といっても、その中身はプログラムや画像、映像、動画、音、音楽など多岐にわたり、また、その内容も、完全な著作権フリー（著作者を明記せず、その用途も私的、業務的を問わず、販売も可能）といったものから、著作権は明記しなければならないものや、私的利用のみ可や、改変していいかの可否、業務で使ってもいいが販売は不可、著作権保護期間切れなどさまざまなものがあります。

このあたりは「クリエイティブ・コモンズ・ライセンス」というプロジェクトがポピュラーです。

クリエイティブ・コモンズ・ライセンスではそれぞれ「どう使っていいか」が、マークなどで明記されているので、その範囲で活用させてもらいましょう。

人によっては、どこで使ったか教

クリエイティブ・コモンズ・ライセンスとは

すべての著作物には著作権があり、著作権は守られなければなりませんが、インターネットには著作権者によって「条件を満たせば比較的自由に使って良い」とされているコンテンツが多く存在します。そのルールを示しているのが、クリエイティブ・コモンズという国際的非営利組織とそのプロジェクトの、クリエイティブ・コモンズ・ライセンスです。

クリエイティブコモンズライセンスでは、その条件をわかりやすくするためにマークを定めています。

クリエイティブ・コモンズ・ライセンスの表示あることを示し、すべての著作権が保護される©All Rights Reserved から、著作権保護期間が終了しパブリック・ドメインになる間の Some Rights Reserved の条件を、下のマークと合わせて示す。

パブリックドメインを意味し、著作権の保護期間切れを示す。つまり自由に使ってよいコンテンツである事を意味する。(PD)と表記される例もある

この場合、「表示ー非営利ー改変禁止」となり、クレジット表記をした上で、非営利目的で改変しない限りにおいては、再配布が可能、という意味になる。

「表示」(BY)を意味し、著作者のクレジット表記などをすることを条件とする。営利目的での使用可。改変も可。再配布可。

「非営利」(NC)と意味し、非営利目的の使用に限って利用が許可される。非営利であれば、改変、再配布も可。

「改変禁止」(ND)を意味し、オリジナルのまま使用することを条件とし、改変や切り抜きレタッチなどはできない。そのままであれば営利目的での使用も可。

「継承」(SA)を意味し、改変を行った場合は元のライセンス条件を継承することで再配布を認める。条件を守れば営利目的の利用も可。

参考：クリエイティブ・コモンズ・ジャパン　ウェブサイト
https://creativecommons.jp/
クリエイティブ・コモンズに関して、詳しくは上記ページを参照してください。

無断使用は著作権侵害で賠償も

インターネットでは「パクリ」と呼ばれる著作権物の無断使用が散見されます。無断で使ってもばれないだろうといった軽い気持ちや、時には自らの作品と偽って公開しているものもいます。しかし、私たちが普段インターネットの検索エンジンを使って、世界中のウェブサイトにある情報を検索できるように、画像などが使われている場所も検索できます。そもそもそういった行為は著作権に関する法律に違反していますし、無断使用に対する使用料請求が行われますので、きちんと許可を取って使用するか、上記のようなコンテンツを使いましょう。

えて欲しいという方もいるので、その場合は、コンテンツを使わせてもらったお礼としてモチベーションを上げてもらえるように、感謝を伝えましょう。

なお、著作権には保護期間があり、これを過ぎると基本的には自由に使うことが出来ます。

コンテンツを入手したら、次に知っておくと便利なのが、制作するコンテンツにおける「レイヤーの概念」です。レイヤーとはアニメ製作における「セル」と呼ばれるものと同じ概念で、透明な板にそれぞれ別個にコンテンツを並べて重ねることで、それぞれ自由に拡大したり、変形することが自由にできるのです。

自分が作りたいコンテンツに似たものを見つけたら、そのコンテンツをこのレイヤーの要素に分解したらどうなるのかを考えてみましょう。

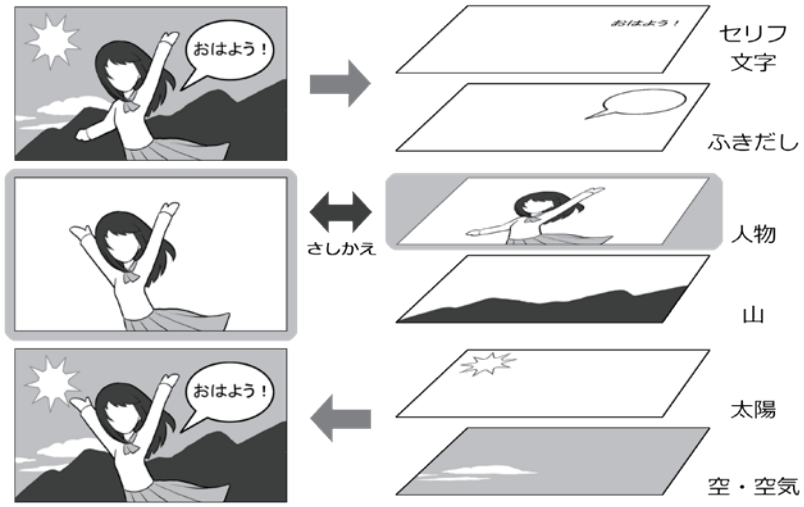
例えば吹き出しがある人間の画像があったとしたら、背景、人間、吹き出し、文字をそれぞれ別にレイヤーとすることで、文字だけを修正する、背景だけを差し替える、人間のサイズを変えるといったことが簡単にでき、一度作ったコンテンツの調整が手軽に行えます。

そして最後に知っておくのは「ペイント(絵)系」と「ベクトル系」という概念です。同じレイヤーを持った画でもペイント系はそれぞれの要素が画になっていて、そのレイヤーの中では不可分です。拡大縮小変形はできますが、それぞれのレイヤの中、例えば人物の顔を変更する場合は書き直す必要があります。

一方、ベクトル系は、数学でいうところのベクトルで描かれた線と、その線で囲まれたエリアを塗ったものの集合体であり、レイヤーの中の要素も自由自在に変更できます。例えば人物の眉だけをちょっと動かしたり、目を大きくしたりといったことも可能です。

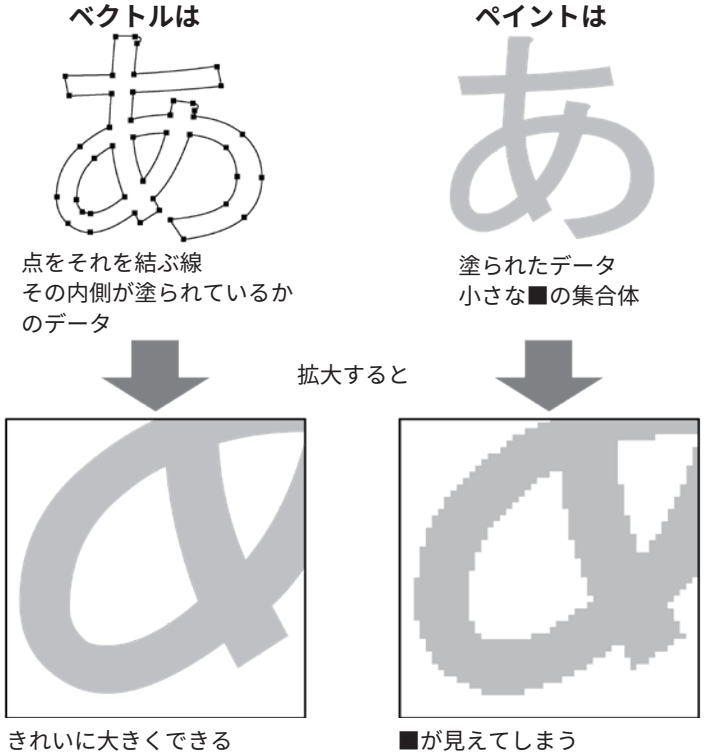
コンテンツを作る際に、この概念を知っているだけで、かなり制作効率が上がり、制作にかかる自分のコストが少なくなり、その分の時間が自由になるので、まず自分が作りたいものを見つけたら、どういった要素にしたがって作られているのか、見抜く能力を養いましょう。

レイヤーとはアニメのセル画のようなもの



画像や印刷物は、紙にペンで書くようにイメージすると修正は難しいのですが、アニメのセル画と同じ考え方をするレイヤーという概念を学ぶと、微調整や修正は簡単になります。レイヤーの一部だけに手を加えれば、全体を書き直さなくても手早く修正可能です。

ベクトルとペイント系の差とは



ベクトルで書かれたものは文字でも絵でも、大きさを修正しても細部が荒くなりません。ただし、微細なタッチの表現はできません。一方、ペイント系は微細な塗りの美しさはありますが、描かれた解像度のドット以上の情報がないので、拡大すると細部が階段状に荒くなります。

6 情報発信とプロモーション

ショップやレストランや一般の方向けのお店を始めたときに、重要になるのは顧客をつかむことです。どんなに腕に自信がある料理でも優良な商品でも、顧客に辿り着かなくてはビジネスはスタートしません。

そうしたときもインターネットの「距離とその移動に必要な時間がいらない」ことが役に立ちます。きちんと情報発信を行えば、理論的には世界中の人にアプローチできます。

情報発信で効果的なのはウェブサイトやブログ、さらにはSNS。ネット上に情報を発信し、検索サイトからの流入などでお客さんに見つけてもらうプロモーションです。

現在のインターネットでのプロモーションとは、平たくいえば「検索エンジンのより高い位置に登場する」ことと「SNSで情報をシェア(拡散)してもらう」ことです。

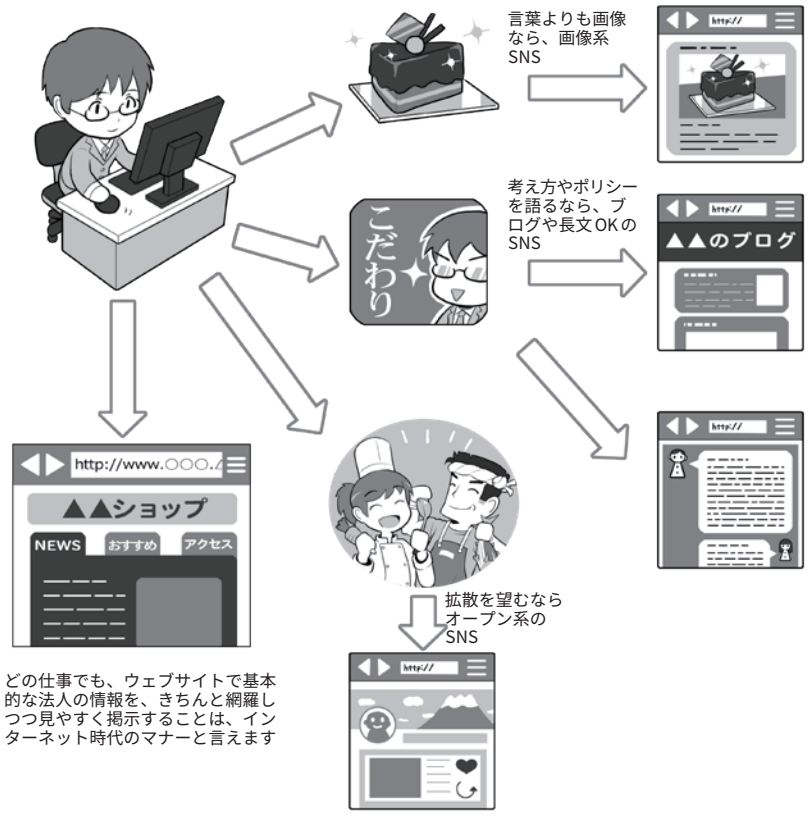
検索エンジンに取り上げられるにはSEO(Search Engine Optimization)という技術があります。大切なことは、きちんと整って必要な情報が揃った、センスのいいウェブサイトを作ることです。

それを見た顧客が「いいウェブサイトだな」と情報を共有してくれる数は、SEO上重要な要素だからです。

ブログも同様ですが、こちらの場合は共有してもらうためのセンスもさることながら、きちんと定期的に更新する「継続は力なり」も重要です。

きちんと更新することで顧客が繰り返し訪れてくれ、それによって「良く見られていること」も、同様

プロモツールは使いよう



どの仕事でも、ウェブサイトで基本的な法人の情報を、きちんと網羅しつつ見やすく掲示することは、インターネット時代のマナーと言えます

省コストのプロモーションには、ウェブサイト、ブログ、SNSはうってつけですが、全部をやる必要はありません。特に、SNSにはそれぞれ個性と客層があり、画像系、考え方やポリシーを述べる系、そしてオープンで拡散することを目的とする系などなどがあり、活用し始める前に自分たちにはどれがふさわしいかを調べ、広くやるよりはコンスタントに継続してコンテンツを提供できるようにしましょう。また、会社や団体の情報、所在地、責任者、ポリシー、決算情報がかかれたウェブサイトの開設は、インターネット時代のマナーです。

センスはどう磨く？

著作権切れの文学作品を公開しているウェブサイトや、国会図書館などがある

海外の美術館や博物館などでは、著作権切れの作品をパブリックドメインで公開している

画像共有サイトや検索エンジンでクリエイティブコモンズ作品を検索することができる

昔はお金がかかったセンス磨きですが、今は「距離の概念が無い」インターネットの特性を生かして、様々な有益なコンテンツが無料で提供されています。著作権が切れた名作文学を公開しているウェブサイト、所蔵品を閲覧できるようにしている美術館や図書館、画像系のSNSではプロカメラマンや世界各国の観光関連機関が、素晴らしい画像を公開しています。

そういったものを閲覧したり、SNSでアカウントをフォローして日々見続けるだけで、センスやどういったものが受け入れられやすいかといった感性が養われます。

にSEO上の重要な要素だからです。継続は力なりはSNSでも同じです。

写真が主体のSNSなら写真に重きをおき、短いコメントが主体のSNSならウィットがある短い文章で共有したくなるようにします。

その中でくどくならないように、自分のビジネスを売り込むわけです。

この写真とウィットのある文章は重要で、写真は「センスの良い写真を見る」ことを続け、それを自分のカメラで撮影して真似してみる、模倣からスキルを向上させます。幸いにデジタルカメラは繰り返し撮影してもお金はかかりませんし、トライした結果はすぐ出るので、最近ではカメラマンの修行期間は10分の1以下になっているぐらいです。

ウィットのある文章も同じ。良いと思うモノをたくさん読みましょう。

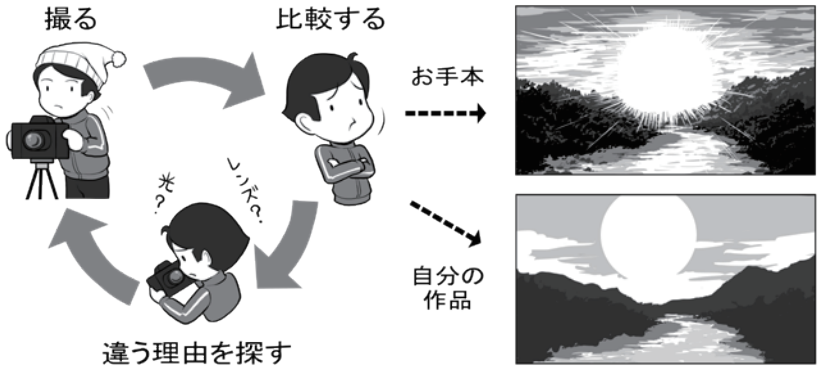
しかし、模倣しているときはビジネスのアカウントで投稿せず、自分なりのスタイル(型)やオリジナリティができたらデビューしましょう。

また、地味な作業ですが、地図系のサービスに自社の情報を掲載したり、自社や自店の情報を検索して、業種でまとめているサービスを見つけたら、ウェブサイトや連絡先、営業時間などを登録したり、自分のビジネスの商品の写真をアップロードして、タグ着けをしてみましょう。

無料でできることでも、かなりのプロモーションができるはずです。

それらを整えてまだ情報発信をしたい場合はSNSの広告も検討しましょう。SNSはターゲット層を絞りんで、比較的安価に広告を打つこともできるので、そういったサービスを利用して、顧客へのリーチを図るのもいいでしょう。

そして、まずはリスペクトしてトライする



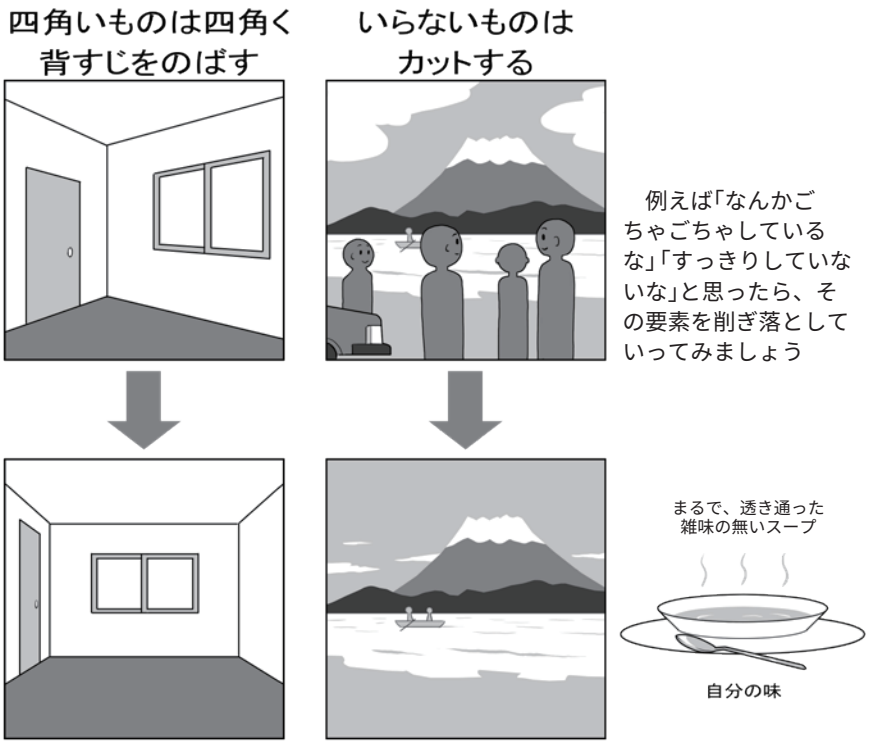
センスが磨けたら次は実践です。デジタル機器のメリットは、どれだけトライアンドエラーを繰り返しても、ほとんどお金がかからないことです。写真であればさまざまな設定を変えて何万枚の写真を撮っても、充電代しかかかりません。また、自分が作ったものを評価して欲しければ「距離の概念がない」インターネットで、多くの人に見てもらうことができます。

例えば文章を書く能力を向上したければ、小説やエッセーなどを書いて小説投稿サイトやSNSなどに投稿すると、評価やコメントがもらえます。イラストやマンガは画像共有サイトや画像系SNS、写真や動画は画像系のSNSや動画共有サイトが使えます。

製品を作っている場合は、写真や動画を使ってアピールすることもできます。コメントや評価を参考にしつつ、作品や製品の価値向上を行うことができるでしょう。

また、文章、画像、映像はマネタイズといって、公開して収入を得る方法も整いつつあります。製品もオンラインショッピングのサイトを使うことで、マーケットが広がります。

センスの一つのアイデア：余分なものは削ぎ落す



試行錯誤をするときの一つのアイデアは、「引き算」といわれます。つまり、作ったものから余分なものを引き算して、訴えたいことをクリアにする訳です。これは例えばスープを作るときに、灰汁をとって整ったらふきんで濃し、徹底的に雑味を取り除いて澄んだスープを作るのに似ています。

文章ならば余分な部分を削る、写真はそぎ落とす、動画ならば切り詰める、製品や作品を見せる場合でも、見た人が写真を通して目移りせずに製品や作品の主題に自然に導かれるようにするにはどうしたらよいか、試行錯誤してみましょう。

そしてプロモーションをする上で大切であり、少ない人数でも無理なくできる「写真を撮る」というテクニックは、磨いておくとさまざまなシーンで役に立ちます。人間は視覚的な情報のほうが、より記憶に残りやすいからです。

コラム：プロのテクニックを盗む

仕事をしてより利益を上げたり、成果を上げたりしたいと思った場合、大切なことはその道のプロフェッショナルになることです。しかし、アマチュアのスタートラインに立ったとき、プロはさながら高い山の頂に立っているようで、そこに辿り着く道筋が見えず、くじけてしまいそうになります。

また、プロはプロとして仕事をして食べていくために、昔アマチュアだった自分がそこに辿り着いたテクニックを、つまびらかには語ってくれません。まさしく他の人がその場所に容易に辿り着けないことこそが、プロの飯の種だからです。

プロへ辿り着く一つの道は、プロの仕事の要素を見破ることです。

先ほども出てきました、レイヤーの概念や、ベクター系の編集ソフトの概念があると、チラシ一つ作るにしても、何回でもやり直しできます。例えば文字一つを修正しようと思っても、全部一枚の紙に描いていたら頭を抱えますが、そういった編集ソフトを使っていれば、数秒で済みます。

写真を撮ったら暗かったと思っても、画像編集ソフトで補正する方法を知れば、粘って一発で撮らなくても少し手を加えて望みの明るさや色にしたり、映り込んだ邪魔なものをキュキュッと消してしまったり、人物を切り抜いて好みの背景に載せ替えることもお手のものです。

このように、なにを使えばどういったことができるんだ、という知識を持った上で、読み解いていくと、プロのプロたらしめている部分の、かなりの要素を追い込み迫ることができます。

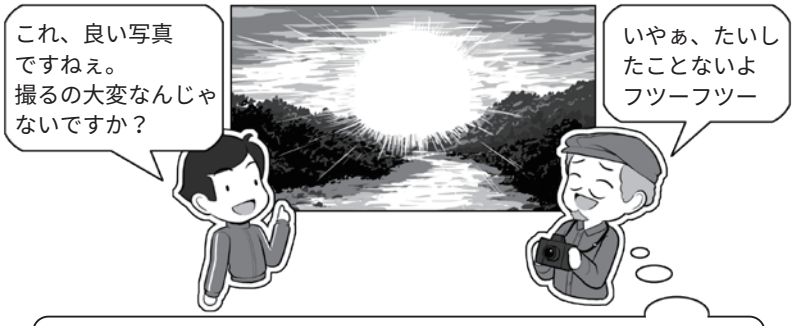
その上で、例えば芸術系の仕事なら「センス」があり、料理などの仕事なら「味覚」が、その他全般、オリジナリティとなる「美学」があるのかも知れません。

しかし、そういった美学であっても、インターネットの時代には、デジタル化できる部分では、過去の多くのプロである作家の作品を、距離と時間を越えて見ることができます。

特に海外で盛んな、美術館などのアーカイブをひたすら見続けるのも手です。

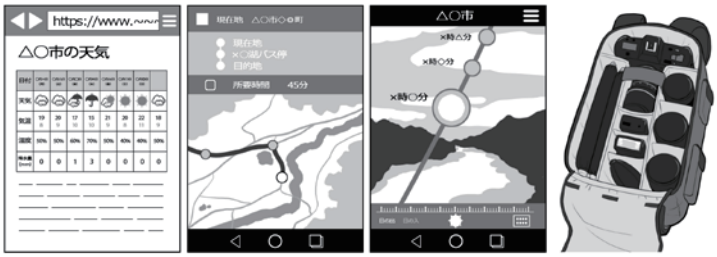
そういった「どこになにがあるか探しだし、見つけて自分のものにする」というテクニックは、インターネットの時代にこそ加速します。時代の力を生かして、新世代のプロを目指してみましょう。

プロの仕事の謎を解明し身につける



- 撮影する場所
- 光の角度
- 日の出の時間
- 例年の天気データ
- 一番きれいに写る機材とセッティングの選択
- 目的地に予定どおりの時間に着くタイムテーブル
- 前日までの降雨による湿度
- 場所取り
- 当日の温度
- 製品を撮る場合は光の当てかた

これができるのがプロのプロたるゆえん



天気予報・開花予想サービス　地図・ナビゲーションサービス　GPS連動天体移動AR日の出日没時間データ　機材の評価はショッピングサイトで

例えば、ある場所である日に思い描いたとおりの写真を撮るために、プロは上のような要素を総合的に判断して行っています。しかし、それはプロにとって当たり前なので、外に向かっては「普通だよ」「たいしたことしてないよ」というわけです。この差が私たちにとって「プロのような写真が撮れない」と思ってしまう理由です。

しかし、上記のような要素は、現在インターネット上の各種サービスを使えば、その多くが机の前に居ながらにして調べることができます。要素を調べ、インターネット上のサービスを活用できるものは活用する。そしてプロの仕事に近づく。これは別段写真に限らず、様々なプロフェッショナルな仕事に当てはまることなのです。

コラム：ヘルスケアと経営者の効率化

中小企業にとってサイバー攻撃も事業継続への不安要因の1つですが、経営者や代表者、業務の鍵になる従業員がいなくなってしまうのも避けたい事態です。

災害以外にもそういった要素はあり、それが「健康」です。最近ではその健康状態もデータ化して見える化することで、ある程度防ぐ手立てが生まれつつあります。

一年に一度は人間ドックを受診したりすることはもちろんですが、それと同時に日々の健康管理としてスマートウォッチやスマート血圧計、スマート体重計などのヘルスケアIoT機器を活用して、自分の健康状態を記録しましょう。

スマートウォッチには脈拍を計測できる機能を持つ製品があり、脈拍に異常があれば通知してくれたりします。それによって不整脈や、脈拍の上昇など心臓に異常が発生しているなどの兆候を、視覚的に察知することが可能です。

また、スマート体重体組成計やスマート血圧計を利用すれば、いちいち自分で記録しなくても日々の体重や血圧を記録してデータ化してグラフで見ることで、その推移を観察することが可能です。

今後、糖尿病などに対応するため、血糖値も手軽に計測できるようになるのではといわれていますが、まずは食べ物に関連したカロリー管理に取り組んでみましょう。

スマホの健康管理アプリの中には食事の写真を撮るだけでカロリー計算してくれるものもあり、また、摂取しなければいけないビタミンなどの栄養素ごとにグラフが表示されるので、そのグラフを満たすようにバランス良く、そして楽しんで食事の記録を取っていきましょう。

最近ではこうしたヘルスケア機器に明るい医師も増えつつあるので、そういった医師の場合、デジタル化された情報を示すことで、話が早くなる場合もあります。

ヘルスケアはIT業界でも重要なテーマとなっているので、新しい情報をアンテナを高くキャッチし、上手く活用して、健康な状態を守りつつ、安定した事業継続に取り組んで下さい。

自分だけで判断せず、適時医師に相談するという前提ですが、様々なヘルスケアIT機器は、基礎的な自分の健康状態を把握するのに役立ちます。

見える化されたデータは、少なくとも異変を察知する手がかりになりますし、自分が保つべき基礎的な指針に、向かっているのか離れているのかといったことが明白になります。

今後ヘルスケア製品が進化すると、データが常時医師に送信され、病気にかかった際にすぐに数値をチェックしてもらえるようになっていくでしょう。

コラム：認定情報処理支援機関（スマートSMEサポーター）について

認定情報処理支援機関（スマートSMEサポーター）とは、経済産業省の外局である中小企業庁が運営する、中小企業のIT活用を支援するITベンダーなどを中小企業等経営強化法に基づいて「情報処理支援機関」として認定する制度です。

近年、IT技術の進展や通信回線の高速化によって、サーバーなどの設備を持たなくてもソフトウェアの利用が可能なクラウドサービスの提供が増えてきました。

クラウドサービスは、設備やソフトウェアを購入する必要が無いため、初期導入コストが低く、しかも経営指導の専門家などとも情報共有がしやすく、クラウドサービス同士を組み合わせて活用することができるなど、中小企業にとっても数々のメリットがあります。

一方で、セキュリティ実装状況や保存したデータの取扱い条件などに関する情報提供が、クラウドサービスを提供するITベンダーによって異なり、中小企業にとっては分かりにくい部分がありました。

中小企業庁では、専門家との検討により、①クラウドサービスの安全・信頼性に関する情報、②セキュリティ対策状況、③利用者のサポート体制、④利用終了時のデータの取扱い、などの確認すべき項目を定めて、スマートSMEサポーターの認定申請時にITベンダーから申告させ、認定後には中小企業庁が特設サイトにて公開しています。

上記の項目の詳しい確認方法については、IPAが「中小企業のためのクラウドサービス安全利用の手引き」で解説していますので、参照下さい。

便利なITツールでも、利用者がデータを取り出せなかったり、セキュリティ対策がおろそかでは、安心して使い続けることができません。

スマートSMEサポーターとして公開されている情報を参考にして、クラウドサービスなどの中小企業にとって生産性向上に役立ち安全・安心に使えるITツールを上手に選んで活用しましょう。

● Smart SME Supporter 情報処理支援機関検索
https://smartsme.secure.force.com/smartsmesearch/

情報処理支援機関検索

情報処理支援機関として認定された、みなさんの生産性を高めるITツールを提供するITベンダーが検索出来ます。
本書ではコンテンツを作る業種を例に挙げましたが、この検索を用いることで、業種別、サービス別、そして地域別に、必要としているベンダーの情報を得ることが出来ます。
例えば、「東京都」で「飲食・サービス」業で、「予約」システムを提供してくれる会社を知りたい、というように検索します。

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

第6章

セキュリティを より深く理解して、 インターネットを安全に使う

インターネットを安全に利用するには、守っておくべきルールがありますが、なぜそういったルールがあるのか。

セキュリティにまつわるいくつかの項目を掘り下げて知ると、より理解が深まり、能動的な行動を取ることができます。

ここでは、パスワード、無線LAN、ウェブサイト、メール、データの暗号化の項目を深掘りして説明しましょう。

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単独で用いられるもの(ZIPファイルのパスワード、WordやExcel、PowerPointの保護パスワード、Wi-Fi機器の暗号化キー、暗号キー、パスフレーズ、セキュリティキー、ネットワークキー)**

一口にパスワードといっても、上記のとおり、実に様々なものがあります。P30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

P30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、「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。

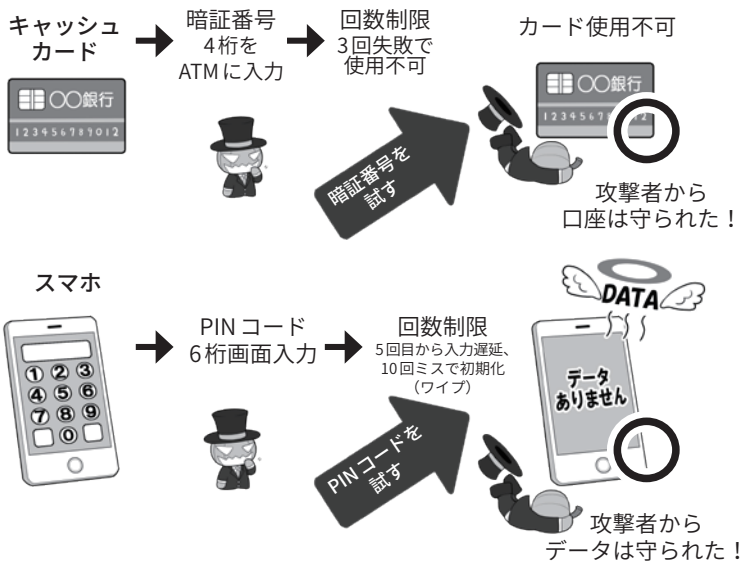
一方、「ログインパスワード」は、通常「PIN コード」のようにワイプまでする機能がついていることは、ほぼありません。数回失敗すると入力間隔が開く、一定時間入力をロックするなどのペナルティを受ける場合もありますが、ペナルティがないものも多いのです。

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。

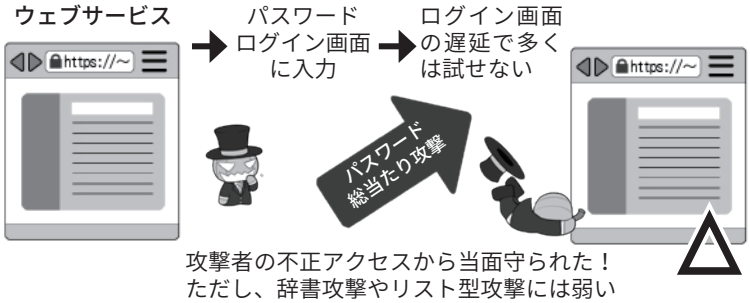
本書の推奨どおり、英大文字小文字＋数字＋記号26種＝88種類の文字を使い、10桁のパスワードを作ったとすると、その組み合わせは約2785京個（京は兆の上の単位）、1秒

3種のパスワードを理解する

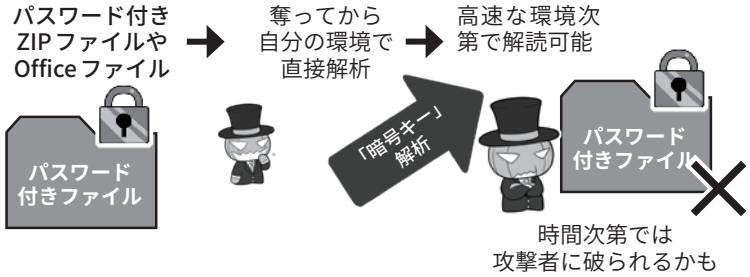
①「PIN コード」の例



②「ログインパスワード」の例



③「暗号キー」の例

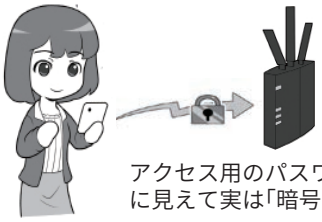


わかりにくい例

「ログインパスワード」か「暗号キー」か分からない例

内蔵記憶装置暗号化の救済に関して、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る。そういった場合は「暗号キー」と考える。

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るが、ログインパスワードではない。「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」の基準で設定する。

※この図は一例であり、実際の機器の条件とは異なります。

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。

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、自分のペースで高速な暗号化解除(解読)の攻撃ができます。

この攻撃の対象となるのは、「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なレベルの難易度なのです。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や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。

もっとも一般的な方法は、なんらかの手段で入手する、その場限りの「ワンタイムパスワード」の入力を追加する方法です。

ログインに当たって、サービス提供者から、SMS（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、または生体認証方式を推奨します。

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。

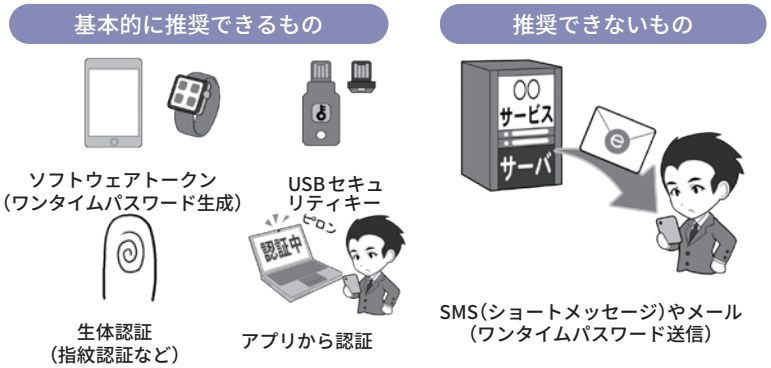
スマートウォッチによっては、スマホのパスワード管理アプリと連携して、手元でIDとパスワードを確認したり、ワンタイムパスワードを発生させたりできるので、より快適なパスワード管理を求めるならば活用しましょう。

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

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

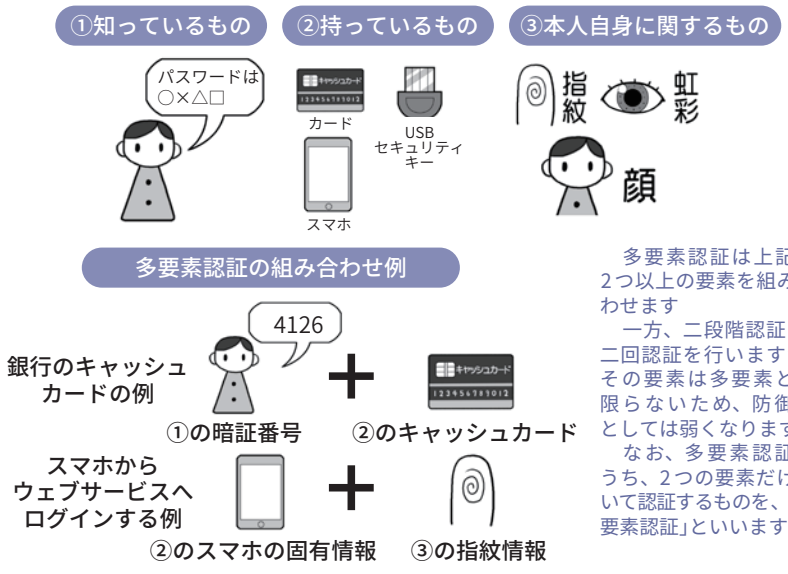
7 二段階認証と二要素認証と多要素認証の安全性

現時点で推奨できる多要素認証要素



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？



多要素認証は上記の2つ以上の要素を組み合わせます

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

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

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。

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た上で、実際にパスワードを破られアカウントを乗っ取られたり、サービス側から流出したりした事実がないのならば、基本的にパスワードを変更する必要はありません。

むしろ、パスワードの基準を定めず、定期的な変更のみを要求することで、パスワードが単純化したり、ワンパターン化したり、サービス間で使い回しするようになることの方が問題となります。

一方、アカウントが乗っ取られたり、流出の事実を知った場合は速やかにパスワードを変更し、その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、今日では、セキュリティ意識が低いと言えるのでそのサービスの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。

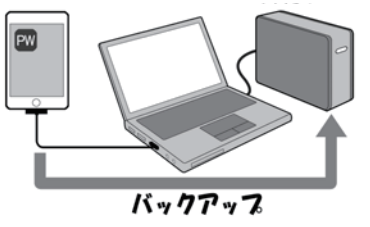
ウェブブラウザにはパスワードを保存しない

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

パスワード管理方法の例

一見分かりにくい専用の紙のノートに二重で

管理アプリのデータは、暗号化した記憶装置にバックアップ



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

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、パスワード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。

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
 外付け記憶装置へバックアップ			○ 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。

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。

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「ログインパスワード」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。

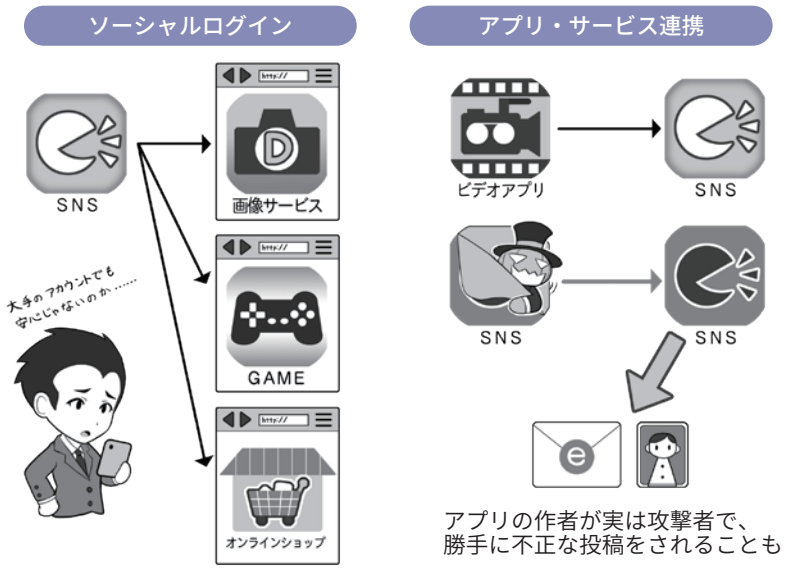
この手間は、情報漏えい対策のために「パソコンのウェブブラウザにIDやパスワードを覚えさせる機能（＝自動入力）」を使わないならなおさらです。

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しまえる可能性があるからです。

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。

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。二要素以上の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、攻撃者による攻撃の手段として利用されることもあり、また実際にメールアドレスや氏名が流出した例も存在しますので、利用は避けるようにしましょう。

また、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。

使用する暗号化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)

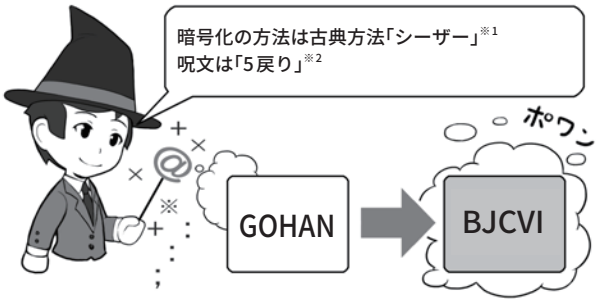
もっとも原始的な暗号は、シーザー暗号といわれるものです。文字をずらして記述するだけのシンプルなもので、仕組みさえ分かればアルファベットなら26回試すまでに暗号が解けてしまいます。
上の図は、その暗号を解きやすくするためのCipher Disk(暗号円盤)です。現代の暗号は複雑な演算を伴うために、人力での解読はほぼ不可能です。

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

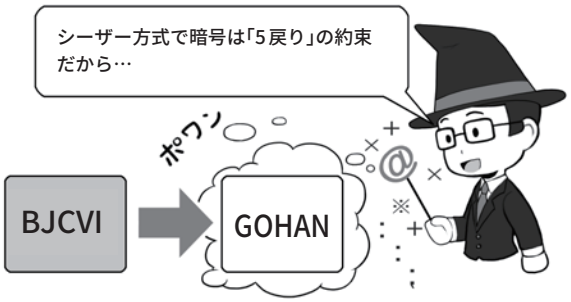


※1：暗号化方式　※2：「暗号キー」

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

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。

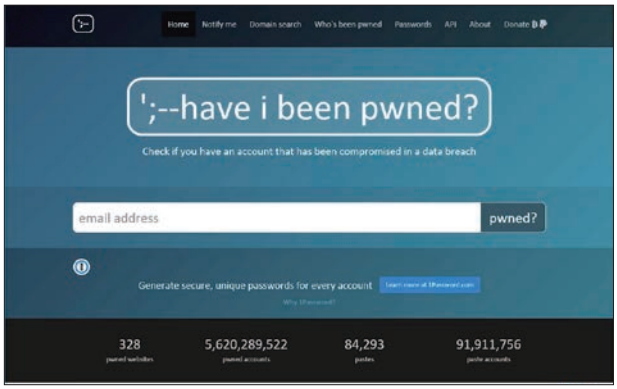
また、パスワードを入力して、そのパスワードが「流出した履歴あり」と出た場合、それは、あなたの情報の流出であってもほかの人の情報の流出であっても、以降パスワードリスト攻撃の対象になるので変更しておきましょう。

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。

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、漏えいしてる？）



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。

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内容や添付ファイル、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、さまざま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となります。

そもそもインターネットは、その始まりにおいて暗号化などが全くされておらず、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、世の常として悪意を持ったものたちが現れ、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、さまざまな状況に合わせた、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など、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対象の一つとして無線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、盗聴に際して特になにか物理的な工作を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居るだけで、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、インターネット上に投稿されたあげく、世界中から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。

その対策をつぶさに挙げていくと数限りないのですが、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

インターネットにつながった無線LANアクセスポイントさえあれば、いちいちIT機器にLANケーブルをつながなくても、手軽にインターネットを利用できる、無線LAN(Wi-Fi)による通信。

会社で利用する無線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知っておきましょう。

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の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。

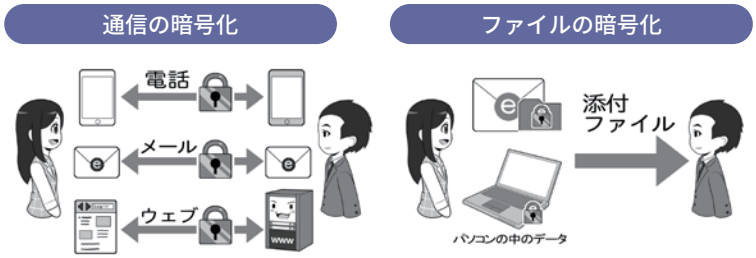
なお、災害時や公益目的で、誰でも無線LANを利用できることを目的にとして、「00000JAPAN（ファイブゼロジャパン）」のように「暗号化無し」で提供されている無線LANアクセスポイントもあります。（その安全性は別として）

この場合は利用時に暗号化方式の設定も「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。

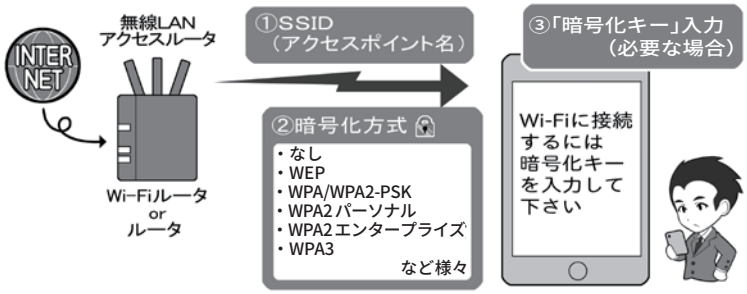
①「通信が暗号化されていないか、されていても安全ではない場合」
②「暗号化の鍵（「暗号キー」）が公開か漏れている場合」

それぞれの状況に合わせた暗号化



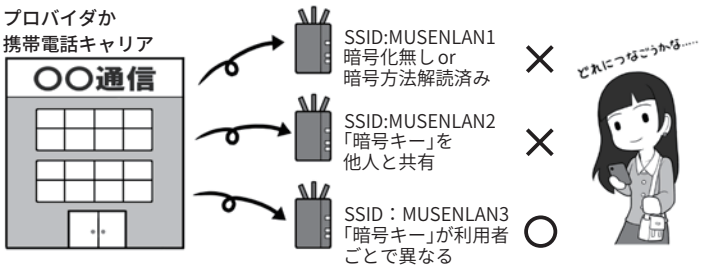
暗号化には、電話、メール、ウェブサイト閲覧などの「通信の暗号化」と、ファイルやパソコンの内部記憶装置などの「ファイルの暗号化」があります。

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、提供している公衆無線LAN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。

安全な通信をするために、自前で暗号化を行うテクニックがなければ利用してはいけません。

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、なんらかの別の手段での暗号化を行わないまま使っていると、攻撃者に盗聴され、即座に内容を知られてしまいます。

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、例えるなら拡声器を使って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るのです。

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、周りに居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登場しつつあるWPA3、それらの記述があるものです。安全な方式の詳細はP131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、辞書が他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 会社などでの安全な無線LANの設定(暗号化方式)

会社などで無線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)かWPA2-PSK(AES)、WPA3を利用し、「暗号キー」を基準にしたがって、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「社員や会員だけが知っている」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「暗号キー」は関係者だけしか知らないものに変更しなければ安全が確保できません。

メーカーによっては「暗号キー」が同一機種で共通だったり、付け方に規則性があるかもしれないからです。

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、無線LANアクセスポイントの名前となるSSIDを変更する場合、会社や団体の名前、社員や会員個々人を想起させる語句は使わないようにしましょう。会社や団体、もしくはあなたが攻撃の対象の場合、攻撃するべき無線LANが特定されるヒントになるからです。

小さい会社などで使う家庭用無線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。接続する古い機器が、安全でない昔の暗号化方式しか選べない場合は、利用を諦め買い換えましょう。

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。

来客に社内用のSSIDに接続させるのも安全ではありません。「暗号キー」が「社員・会員だけが知っている状態」では無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 会社などでの安全な無線LANの設定（その他）

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であり、「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。

設定画面は無線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

会社内での無線LANの利用

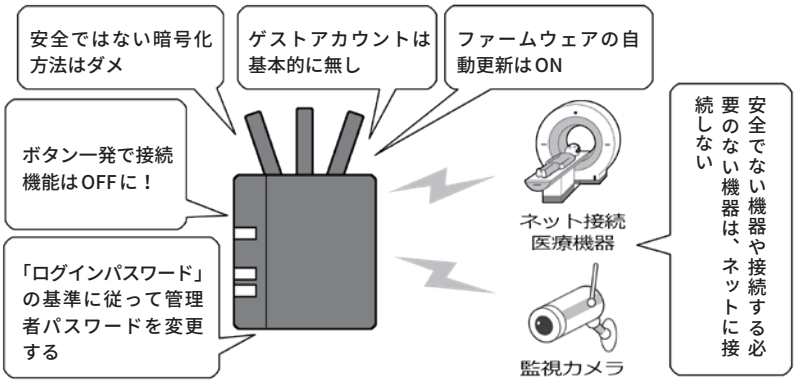
①出荷時の管理者パスワード、「暗号キー」の変更

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」は社員・会員だけの秘密

家庭で使える暗号化方式は、「暗号キー」を社員・会員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。部外者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



会社や団体で無線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LANに接続しないようにしましょう。

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来訪者が、ボタ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に戻しておきましょう。

UPnP（Universal Plug and Play）の設定も、不用意に社内の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アラームを作り、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、社内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、社内・団体内用の無線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、この方式では社内などの利用と同様に、複数の人が同じ「暗号キー」を使うことになります。これを公衆無線LANにあてはめると、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。

その設定の状態で無線LAN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）を使った攻撃をしかけられ、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潜在的に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ます。

利用前にそのページをチェックし、上記の暗号化方式のキーワードを頼りに、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、これらの方式を採用した

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、自分用の「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、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さまざまな方式の公衆無線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

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、利用者は皆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。他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どう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。

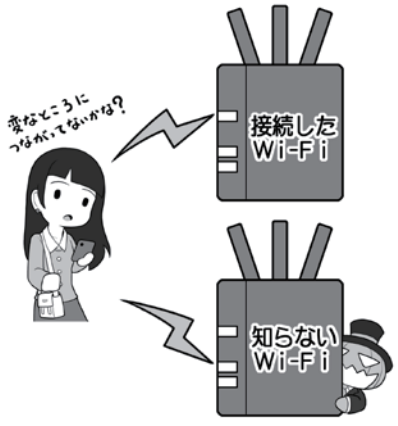
下の表は、暗号化方式のそれぞれの安全性とその理由を書き出したものです。この2つの表を比較すると、すでに暗号化が破られており、利用が推奨されていない「WEP」が、表示アイコン上は暗号化に分類されていることがわかります。アイコンは暗号化の有無を表しているのでこれは正しい表示ですが、アイコンは安全性の担保ではないと認識して下さい。Androidは、接続したアクセスポイントをタップすると「セキュリティ」の項目でネットワークの種類の暗号化方式などを確認できます。Windows、mac OS Xは調べるのに手間がかかります。iOSでは簡単に確認する手段がありません。

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。その他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。

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、切断した上で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

なお、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通信でサーバに接続するもののみを使用する方法です。

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、調査記事など公開されている情報で確認するか、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機密性を保って接続する技術です。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。

これを「事業所から事業所」ではなく、「個人のIT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。

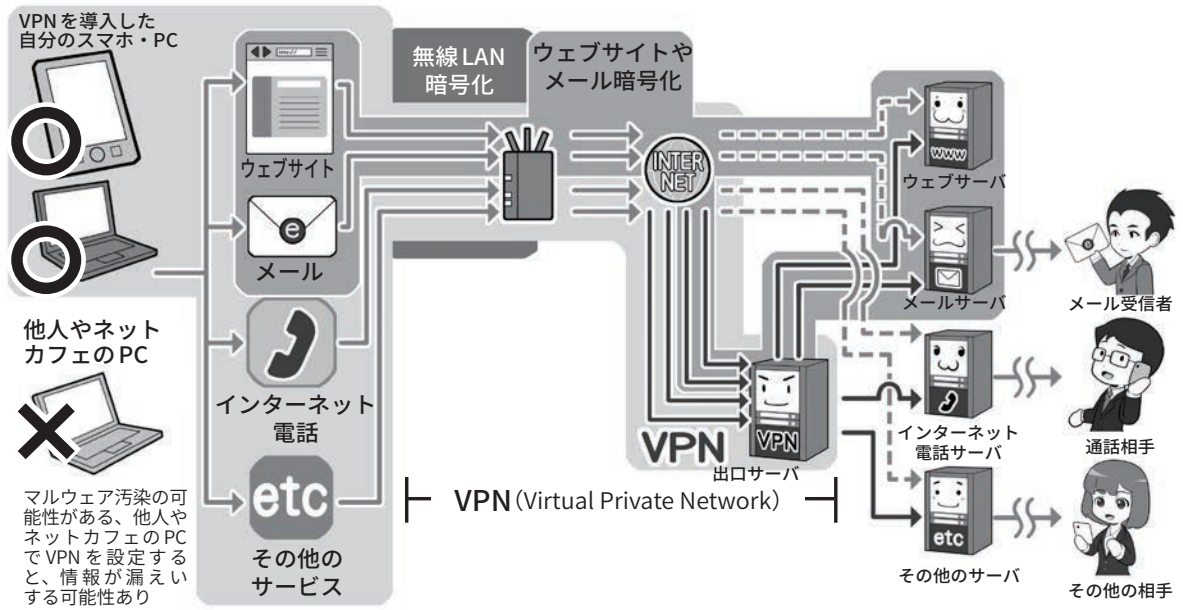
利用するVPNのサービスによっては、誤ったアクセスポイントに誘導されたり、VPN接続が切れると暗号化されていない状態に移行して通信を継続したりしてしまうものもあるなど、2020年の春の時点でも、まだ決定版的なサービスがありません。

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であり、その先の通信の暗号化が行われない点は注意が必要です。

さまざま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



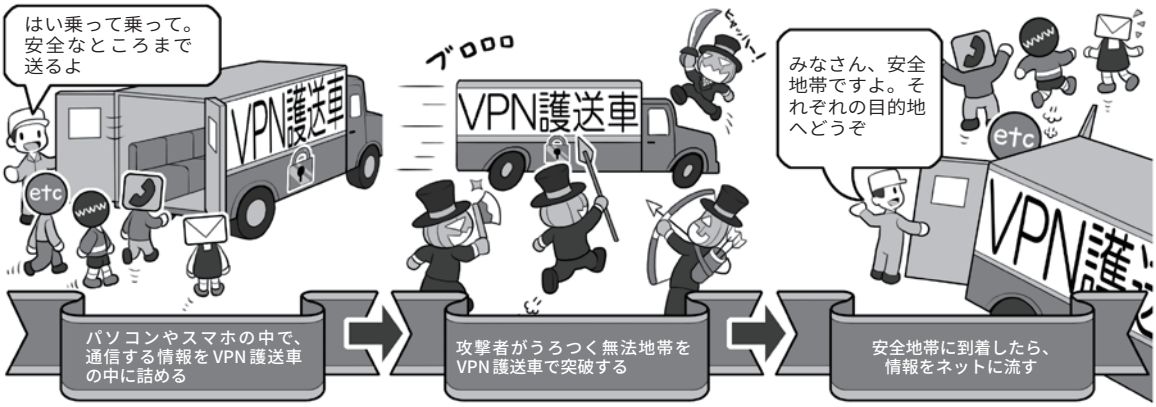
VPNを図で説明すると、上のように入り組んでよく分からなくなってしまうので、簡単な図を下に用意しました。くじけそうな方はまず下をご覧ください。

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、ウェブサイトやメールの暗号化、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、ウェブサイト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であり、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には限界があり、従って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、通信をする用途に限定して、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個別に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たり盗まれたり、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るか、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。

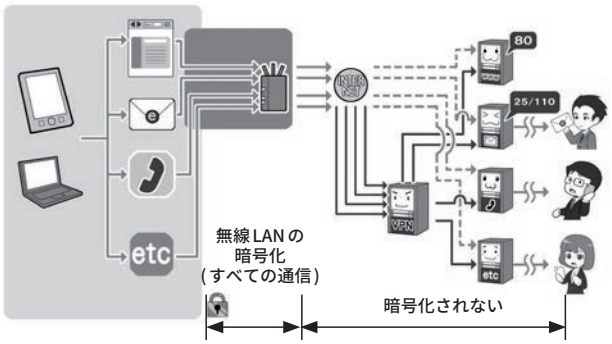
https による暗号化通信を行うためには、まず、https で通信するサーバを作りたい企業や団体のサイト運営者が、認証局という機関に、書類で自分の会社の情報とサーバのドメイン名を提示して、ネット上で身元を明らかにするための電子証明書の発行を申請します。

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

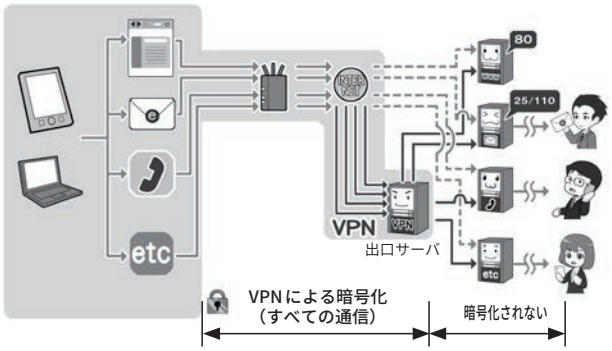
それぞれの暗号化の守備範囲

①無線 LAN の暗号化



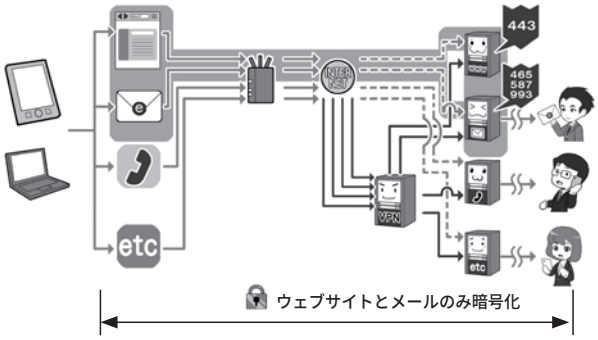
無線 LAN の暗号化は、利用者の機器から無線 LAN アクセスポイントまでのすべての通信を暗号化します。

②VPN による暗号化



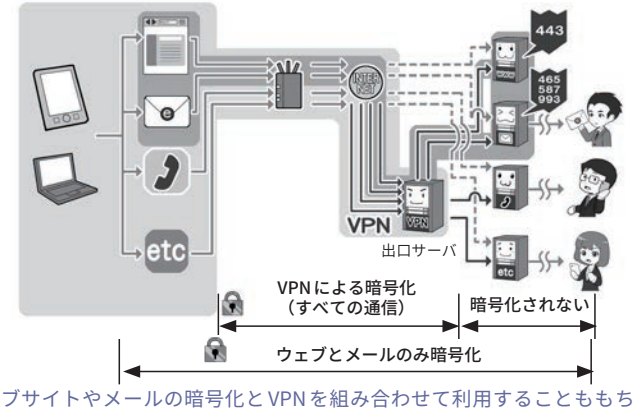
VPN は利用者の機器から、安全とされる「出口サーバ」までの区間で、すべての通信を暗号化します。

③ウェブサイトやメールの暗号化



ウェブサイト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、ウェブサイトとメールの通信だけを暗号化します。

④VPN ＋ウェブメールの暗号化



ウェブサイト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。

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。

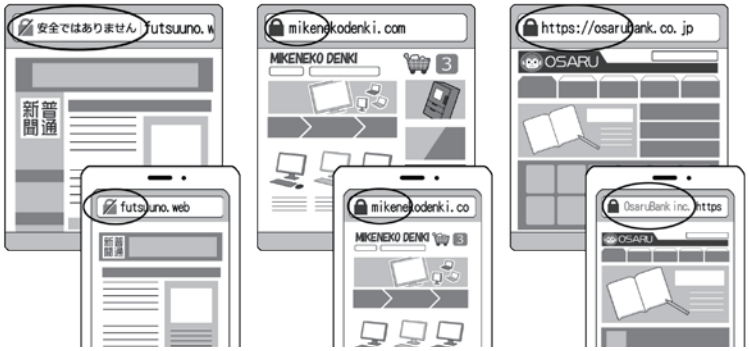
httpsの暗号化通信で情報を守る

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

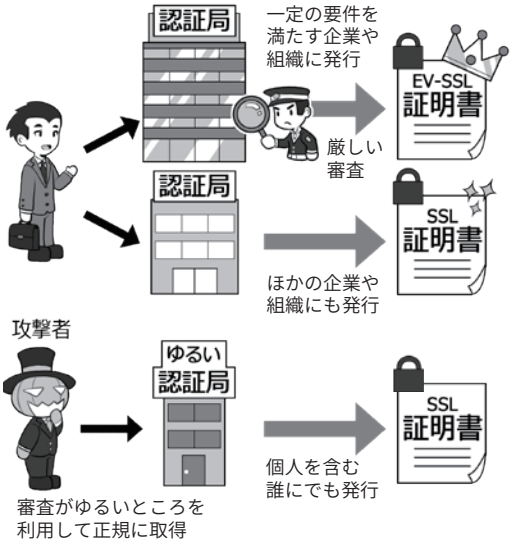
注意 △ SSL（暗号化あり）（httpsと表示される🔒マークが表示される）

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。

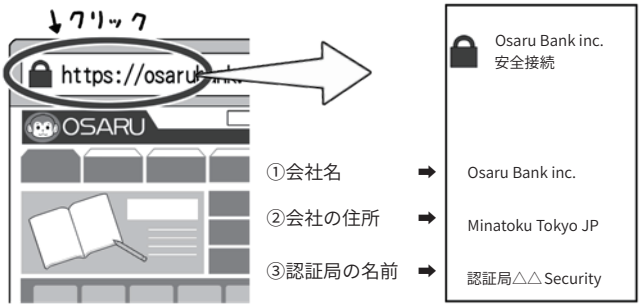
攻撃者が不正に取得した証明書に注意



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。

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本章頭で書きましたが、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偽装URLも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、直接ブックマークを開いてクリックして訪れるか、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、実際は偽サイトに誘導されてしまう場合があります。

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。

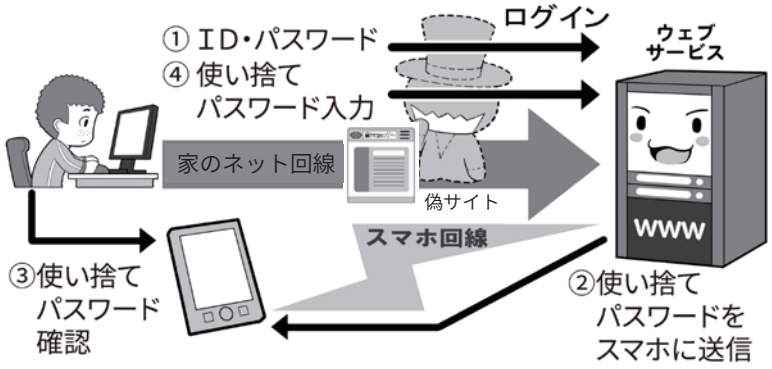
攻撃者があなたに、マルウェアを仕込んだウェブサイトのURLをメールやアプリのメッセージで送り、あなたがリンクをクリックして悪意のあるウェブサイトを見てしまう場合（フィッシングメール）や、あなたの行動パターンを調べて、よくアクセスするウェブサイトに、事前にマルウェアを仕込んでおく水飲み場攻撃、さらにわざわざお金を払ってマルウェアが含まれた動画広告などを目的のウェブサイトに出すという方法（マルバタイジング）もあります。

また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、母数を多くとる分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。

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。

ウェブサイトを使ったサイバー攻撃の例

①偽メールなどによる誘導　②水飲み場攻撃による感染

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の存在を、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。

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

次は電子メールを安全に使う方法についてです。

「ウェブサイトを安全に利用する」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、メールの内容を盗み見されないためには、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サイトと異なり、ほとんどが私的な内容になるからです。

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

メールも、昔は送受信どちらも暗号化されていない平文で通信が行われていました。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基本になっています。

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この暗号化で通信を行うようになっているのです。

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変えていない場合、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。

メールアカウントをたくさん持っている人は、一度メールアカウントの棚卸(たなおろし)をし、設定を見て暗号化されていないアカウントがあれば、暗号化している方式に切り替え、暗号化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、そもそも安全ではないと考え、暗号化方式が提供されている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な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、内容は読まれてしまう余地はあります。

それは現代でも外国に郵便を送ると、国や地域によっては検閲で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否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」という方法と「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、もともと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。

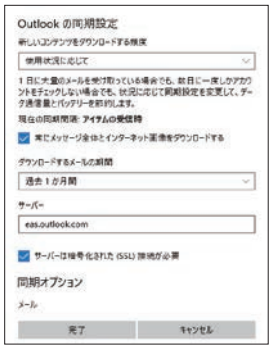
そしてこれを成立させるためには、

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
暗号通信（SSL/TLS）利用することになっているか？

メールソフトの例

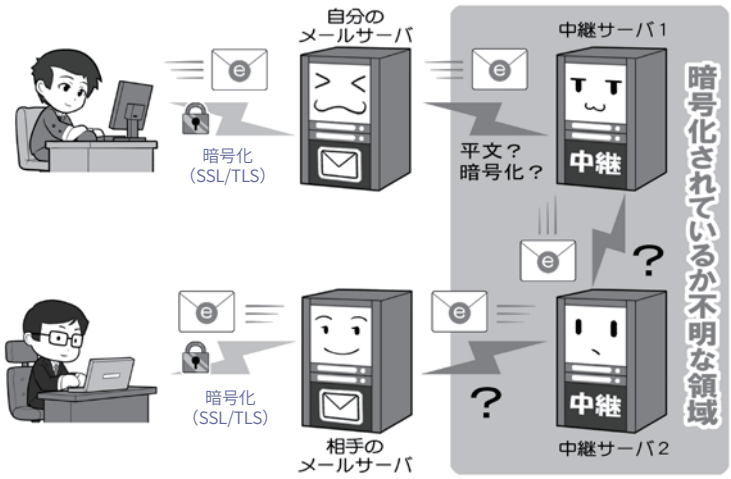
メールアプリの例



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。

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、仮にメールの本文を改ざんされても、受信者側で改ざんされていないか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。これを実現する技術を「デジタル署名」と呼びます。

上記のとおりS/MIMEは大変優れた機能ですが、事前の準備に手間がかかり、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。

なお、利用者ではなくサービス側でメールの成りすましを防ぐ技術として、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し注意喚起しています。

この場合、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うかつに開くと「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ばらまき型の「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こともあり、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、偽装広告へのリンクをクリックさせたりする洗練された手法なのです。

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、緊急に文中のリンクや添付ファイルを開くことを要求するメールなどは、かなり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・ウェブ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。

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、拡張子は「.exe」となり、exe と表示されれば「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、文章ファイルに見える「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いためにも、繰り返しになりますが、

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。

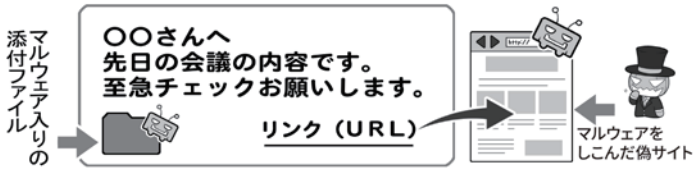
一般的には「SSL 証明書」や「EV-SSL 証明書」を持ち、暗号化通信を示す鍵マークがついていることで、暗号化されているかどうか、信頼性があるかどうかなどがわかります。

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。

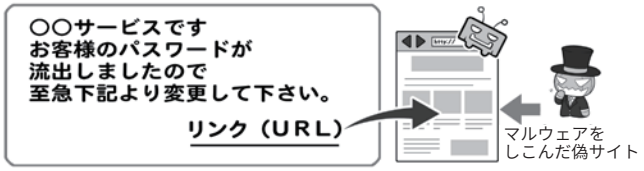
怪しいメールとはなにか

①仕事のメールを装う



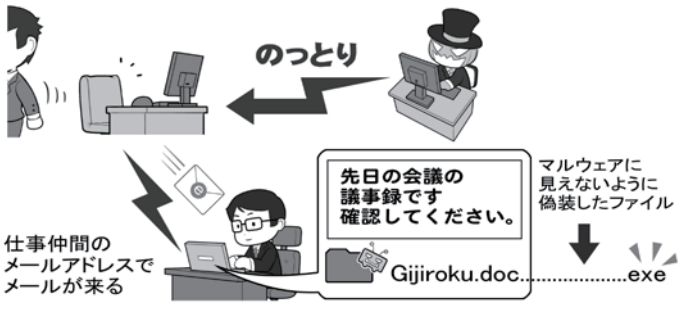
サイバー攻撃に使われる怪しいメールとは、まず「見ただけでは完結しない」メールです。リンクをクリックさせたり、添付ファイルを開かせたり、なにかをインストールさせようとしたりします。

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。名前を語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。

「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。

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 ウェブサービスなどからのメールアドレスの流出

「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。

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）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場合、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、複数の仮想メールアドレスを作れ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他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ば、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あれば、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（右下図参照）。

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、まずは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」にもあてはまります。

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、さまざまなシステムや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、さまざま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。

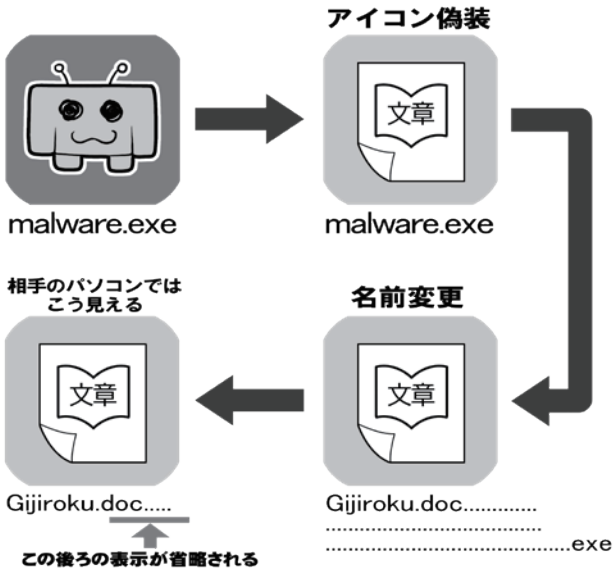
1社によって提供され、栄枯盛衰（えいこせいすい）によってサービス終了する可能性があるSNSに対して、メールは永続性の点で有利といえます。

事実、インターネットの初期からさまざまなOSやメールソフトを乗り継いでも、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、さまざまな華やかな機能を楽しむこともできます。

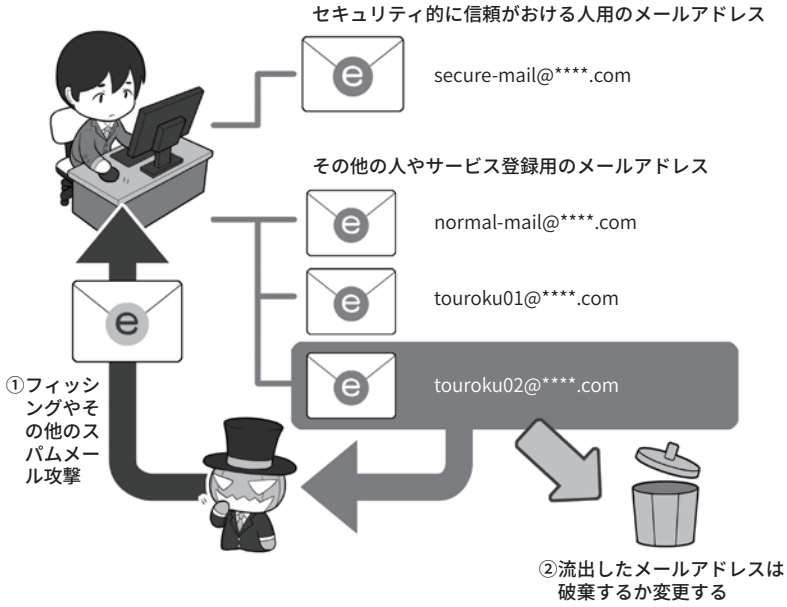
SNSとメール、どちらがいいかは人それぞれです。それぞれにメリットとデメリットがあるのでよく機能を理解して、自分に合ったものをうまく利用しましょう。

マルウェア入りファイルの偽装



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。

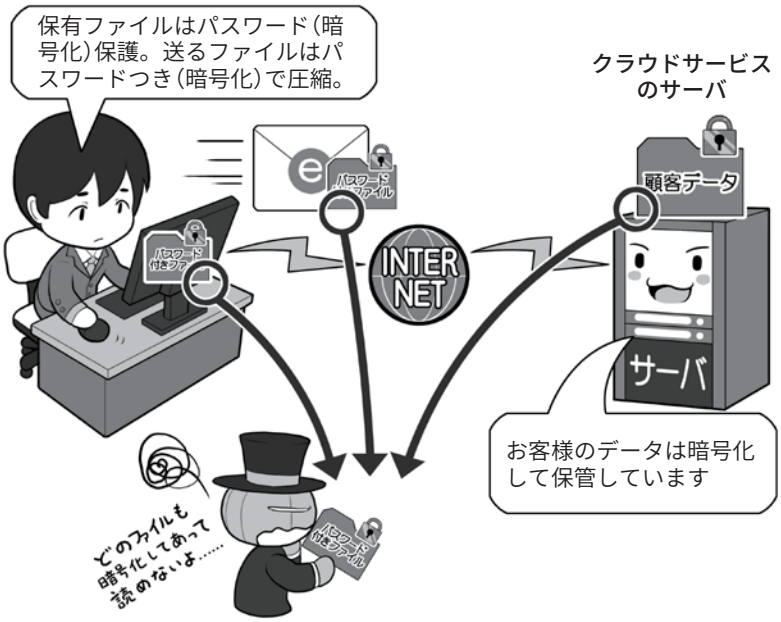
例えば、メールの添付ファイルが盗まれたり、保存しているファイルがマルウェア感染で流出したり、サーバに不正アクセスされて盗み見されても、また、ファイルの入った物理的な記録メディアを紛失しても、確実に適切な方法と鍵（暗号キー）で暗号化してあるならば、攻撃者が解読できなくなり、情報を流出から守ることができます。

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執拗に解読を試みられ続ける可能性があります。したがって「暗号キー」の基準にしたがって、長く複雑なものを設定しなければなりません。

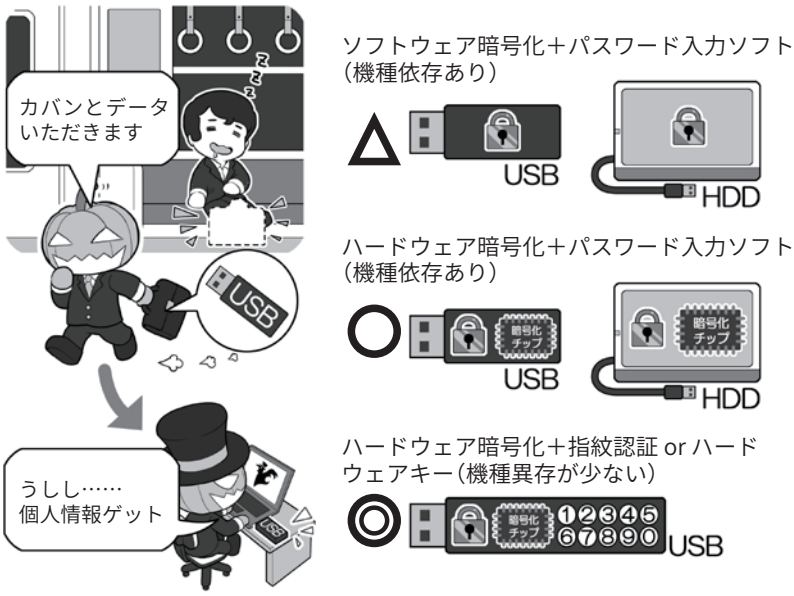
機密情報を持ち運ぶ場合は、ファイル単位の暗号化よりも、装置全体の暗号化機能の付いた外付け記憶装置やUSBメモリの利用を推奨します。可能であれば、高速に暗号処理が可能でさまざまな攻撃に対策された暗号化チップが内蔵されたものを選択しましょう。そうすることで、ファイル単位の暗号化が不確実になった場合のトラブルも避けられます。

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PINコード相当の認証をするタイプもあります。これらは専用の認証用ソフトウェアを必要としないので、

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。

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を「PINコード」方式と同じにすることで、入力を間違えると「ロック」や「データ消去」の保護機能があります。内部では「暗号キー」として十分に長く複雑なものが自動で生成され、この「暗号キー」の利用にのみ「PINコード」の入力を求めることで利便性と安全性を両立しています。

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、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、独自のルールで一部記号や数字に置き換えて使用するなどの方法が考えられます。

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。

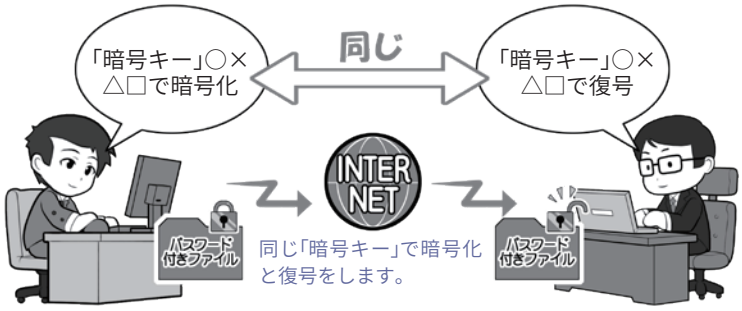
別送信であっても、暗号化ファイルと「暗号キー」を同じメールアドレスに送れば、メールが一気に流出すると2つが揃ってしまいます。

「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。

さらに、「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、こういったシーンでは目にしません。

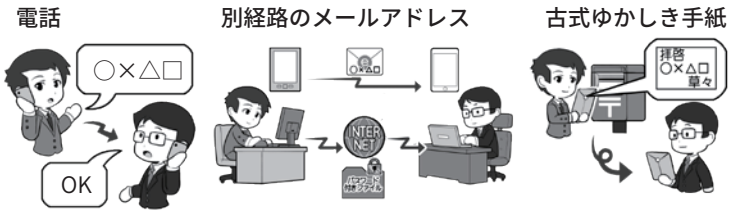
ただ、この方式は、P142で紹介した「S/MIME」や「PGP」や、同じように目にすることはありませんが、無線LAN通信の暗号化など、見ていないところでファイルも暗号化しています。

「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



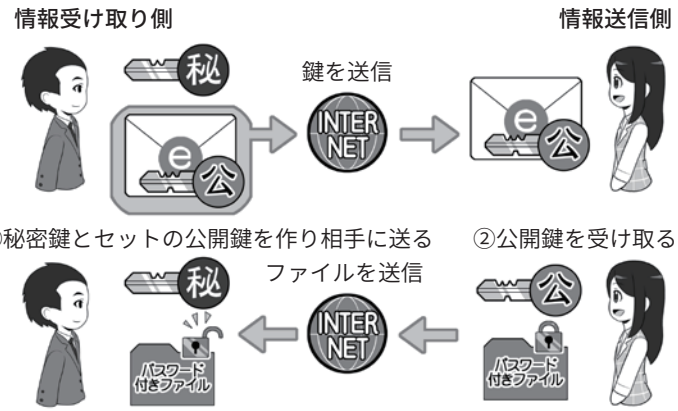
直接会ったときに「暗号キー」を渡したり、電話で直接伝えたりします。

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：IPAのより深いセキュリティ設定資料

ITの特徴は、多くの人の目的に合致するように柔軟に作られていることで、機器であれソフトであれ多くの設定項目が用意されており、それを調整することでより自分の目的に適した使い方が可能になります。基本的には標準設定のままでも十分使えるようになっていますが、まずはそのままで生産性を上げることを目指すのが大事です。しかし、将来的にもっとセキュリティ性を高めて安全に使いたいと思う時期がやってきます。

そうしたときにはIPA（独立行政法人情報処理推進機構）のウェブサイトに紹介されているマニュアルなどが参考になります。「情報漏えいを防ぐためのモバイルデバイス等各種設定マニュアル」ではパソコンやスマホをより安全に使うための設定が紹介されています。「SSL/TLS暗号設定ガイドライン」ではウェブサイトを作成し公開するときに、適切な暗号化通信の運用について解説しています。

「IT製品の調達におけるセキュリティ要件リスト活用ガイドブック」では、経済産業省が公開している「IT製品の調達におけるセキュリティ要件リスト」に対し、これを実際にどのように活用するかの辞書的な役割を担うものです。

「IT製品の調達におけるセキュリティ要件リスト」は「国際標準に基づくセキュリティ要件」に適合することが認証されたセキュリティ製品のリストで、それをどう活用するかが解説されています。

いずれも、本書に書かれているセキュリティ知識を習得した上で、次のステップに進む手引きとなる資料です。

情報漏えいを防ぐためのモバイルデバイス等各種設定マニュアル
https://www.ipa.go.jp/security/ipg/documents/dev_setting_crypt.html
SSL/TLS暗号設定ガイドライン～安全なウェブサイトのために（暗号設定対策編）～
https://www.ipa.go.jp/security/vuln/ssl_crypt_config.html
IT製品の調達におけるセキュリティ要件リスト活用ガイドブック
https://www.ipa.go.jp/security/it-product/guidebook.html

コラム：セキュリティ系業務のアウトソース

小さな会社やNPOのみなさんがより責任ある立場になっていくためには、本格的にサイバーセキュリティに取り組む必要があります。ただし、小さな会社やNPOにとって、それらを自ら習得するのは困難です。そういった状況で、インターネットの特性を生かし、専門の企業にアウトソースすることで、堅牢性を担保するのも一つの手でしょう。

しかし、みなさんにとっては「どういった企業が信頼できるのか」というところからのスタートになると思いますので、そういったシーンに向けて、経済産業省とIPAでは「情報セキュリティサービス基準適合サービスリスト」を公開しています。つまり、一定の基準を満たしたセキュリティ系企業のリストを公開しています。

リスクアセスメントを行う「情報セキュリティ監査」、ウェブサイトやシステムの弱点を見つける「脆弱性診断」、被害に遭ったときの鑑識的業務を行う「デジタルフォレンジック」、そして日々の問題無く業務行えるか常にチェックをする「セキュリティ監視・運用」の、それぞれのリストがあります。

情報セキュリティサービス基準適合サービスリスト（IPA）
https://www.ipa.go.jp/security/it-service/service_list.html
情報セキュリティサービス基準及び審査登録機関基準（経済産業省）
http://www.meti.go.jp/policy/netsecurity/shinsatouroku/touroku.html
情報セキュリティサービス基準（経済産業省）
http://www.meti.go.jp/policy/netsecurity/shinsatouroku/zyouhoukizyun.pdf

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

エピローグ

デジタル世代の小さな会社とNPOの未来

インターネット時代に小さな会社やNPOのみなさんが仕事をやり遂げていくために、参考になる内容はありましたか？

本書が少しでもみなさんの力になれたならうれしく思います。

次世代でも輝くみなさんを想像しつつ、しめくくりのメッセージを。

おわりに　～デジタル世代の中小企業・NPOとは?

小さな会社のみなさん、NPOのみなさん、本書の内容はいかがだったでしょうか？

通常、企業向けのサイバーセキュリティにまつわる本や資料は、かなり技術的でかっちりとして、手軽には読みにくいものになっています。それは会社や団体の中にセキュリティを理解する担当者がいて、その人に向けて「こうしなければならない」といった内容を、整然と詳しく伝えているからです。

また、サイバーセキュリティに関する記事も世の中にたくさんありますが、それらはかなりの部分、全くの個人か、先ほどの企業のセキュリティ担当者に向けてのものであり、その中間にあたる、従業員のいる個人事業主、セキュリティ担当者のいない小さな会社、そして任意団体や非営利団体(NPO)の方たち向けには作られていないのが現状です。

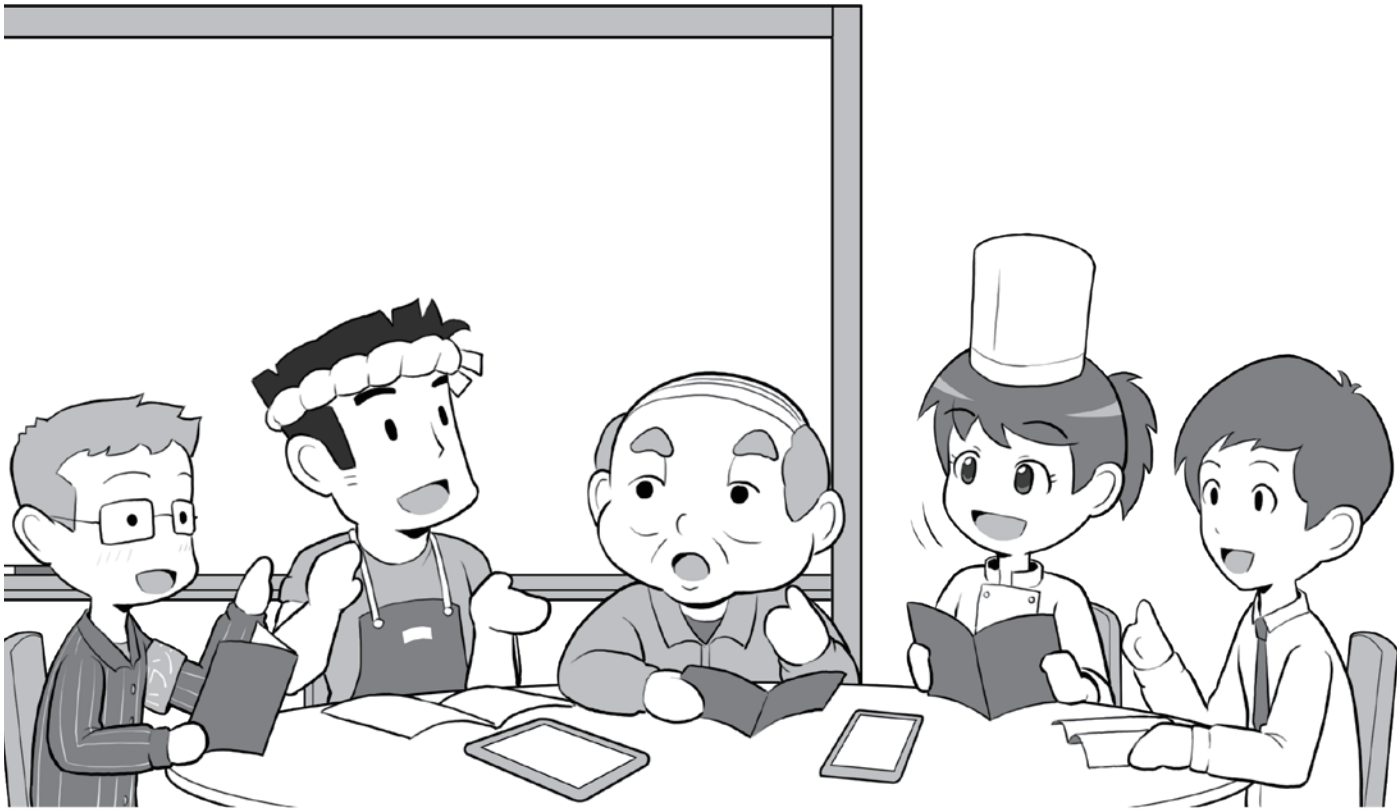
しかし、悪意をもって攻撃をするものたちは、みなさんを避けてくれはしません。

それに対抗するためには、小さな会社やNPOのみなさんの中にある「そもそもサイバーセキュリティってなに？」「最低限なにをしなければならないの？」という疑問を解消し、「サイバーセキュリティへの理解や投資が、結果的には未来の利益になる」ということを知ってもらうことからスタートするべきであり、それを実現するためには、なるべく分かりやすく、気軽に読めるものがいいのではないかと考え、この本を作りました。

この本が、みなさんがサイバーセキュリティを理解するためのお役に立てたならうれしく思います。

さてインターネット世代の小さな会社やNPOはどうなっていくのでしょう。

もちろん企業やNPOとしての目



標を達成する過程で、大きな会社や著名なNPOになることも一つの答えかもしれませんが、もう一つの方向性は、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」に合わせて進化して、このメリットをフル活用し、機敏に姿を変え、柔軟性を生かしてことにあたり、どこにいても仕事を行え、そして仕事と家庭を両立し、クオリティ・オブ・ライフ、すなわち生活の質を向上させる、そんな存在を目指すのもいいのではないかと思います。

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。しかし、インターネットの出現によってこの制約から放たれる、人間の可能性は無限大です。そんな未来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して活動できる場所にしていくため、私たちとともに、インターネット世界の未来を守って下さい。

私たちがインターネットに素晴らしい意義を見出し、その果てに人としての進化があると証明するためには、安全で安心なインターネット空間の実現が不可欠なのです。

そして広大なインターネットは可能性の宝庫であると同時に、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は守り切れないのです。

みなさん一人ひとりがインターネットを守る私たちの仲間となって、私たちとともに未来を守ってくれる存在になることを望みます。

私たちは、みなさんのことを待っています。可能性の未来でお会いしましょう。

2019年3月15日

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

BCP（ビー・シー・ピー）
Business Continuity Planningの略。事業継続計画の意味で、災害時に被害を最小限に抑えて事業を継続するために、あらかじめ人・モノ・金などのポイントから計画を立て、また、これを訓練することが望まれる。中小企業庁に詳細なウェブサイトがある

BEC（ベック）
Business Email Compromiseの略。ビジネスメール詐欺。攻撃者がビジネス用のメールを装い、企業の担当者をだまして、不正送金や機密情報の流出などが行われる攻撃

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

BYOD（ビー・ワイ・オー・ディー）
Bring Your Own Deviceの略。社員が個人の所有機材を会社の業務で使用すること

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

DMZ（ディーエムゼット）
DeMilitarized Zone。非武装地帯の意味。インターネットにつながるLAN用ルータに接続した機器のうち、LAN側ではなくインターネット側に設置したかたちにする仮想的なエリア。自前の公開用サーバやインターネット側から参照する監視カメラなどを設置する。DMZにあるIT機器はインターネットから直接見えるため攻撃されやすい

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、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」ともいわれるが、あらゆるものをネットにつなげる考え方。しかし、IoT機器製造業者が全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し、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

● 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であるが、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。さまざまな種類の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、主に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の略称　→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桁から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格。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。

● 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ストール可能となる。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

● RSS（アール・エス・エス）

Really Simple Syndication もしくは Rich Site Summaryの略。ウェブサイトの見えない部分で更新情報を掲載し、RSSリーダーで複数のサイトの更新情報を集約して見る事ができる。更新情報やタイトルだけで無く、仕様によっては要約文が提供される場合もある

● 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（エス・エム・エス、ショートメッセージ）
Short Message Serviceの略。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、さまざまな形態がある

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、電子的な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

SSL（エス・エス・エル）
→SSL/TLS

SSL/TLS（エス・エス・エル／ティ・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。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・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）

Uniform Resource Locatorの略。普段目にするものとしてはhttp://やhttps://などから始まる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・セキュリティキー）

USB端子に接続して、機器や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、およびそこから認証用のワンタイムパスワードなどを送信するもの。BluetoothやNFCに使うタイプも存在する

● 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

● WAN（ワン）

Wide Area Network。LANに対になる言葉で、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避ける

● Wi-Fi（ワイ・ファイ）

→無線LANおよびその通信

● Wi-Fiルータ（ワイ・ファイ・ルータ）

ルータに無線LANアクセスポイント機能を付けたもの。無線LANアクセスルータ。→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とされる。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、その他無線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。セキュリティの向上を含む場合もあるが、単に機能向上の場合もある。セキュリティ向上のみを行う場合は、セキュリティパッチと呼ばれる場合が多い

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。主にスマホで使われ、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り、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

アタッカー
=攻撃者

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

● 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

ウェブサイト、ホームページの略称。そもそもはインターネット上のウェブサイトを指す、World Wide Web(WWW,W3)の略

● ウェブサイト

ネット上で文章ファイル風に情報を表示する場所。主としてウェブブラウザなどで閲覧する。ウェブサーバ上で運営される

● 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イトを閲覧するためのソフトウェアやアプリ

● エアギャップ

有線無線を問わず、ネットに接続しないことでサイバー攻撃を受けなくする防御方法。間に空気が挟まることから来ている。実効性を高めるためには、接続しないだけで無く、接続できる端子を塞ぐなどの措置も必要

● 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。主にネットに接続しないでできる攻撃であり、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
≒クラウドストレージサーバ

● 記憶装置

パソコンやスマホの中にあるプログラムやデータを保存するメモリ。CPU に直結されデータをやり取りするメインメモリが主記憶装置、何らかの結線を使って接続しデータをやり取りするものが補助記憶装置という。ハードディスクや SSD などはこれにあたる。総括して記憶装置

● 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

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を指す。主に「機器の記憶装置と同等に利用できる」「利用している意識はないが使っている」「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。このうちファイルを保存し共有することを目的とするものを「クラウドストレージサービス」と呼ぶ。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。一方、共有が主たる目的でない場合もあり、クラウドサービスあるいは単純にクラウドという場合もある

クラッカー
P12 コラム参照　≒　攻撃者

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無いので、特に攻撃を行うものとして「攻撃者」とする。P12 コラム参照　＝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ウェブ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

スクリプトキディ
ハッカーのレベルになく、自分で作らず購入したマルウェアや簡単なスクリプトを使って悪事を働く、初心者攻撃者。「スクリプトを使うお子さま」の意

スタンドアロン
ネットワーク（繋がっていること）と対になって使われる言葉で、ネットワークに繋がっておらず単独で存在すること。ただし、ネットに繋がっていて、かつ他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

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

● 脆弱性
＝セキュリティホール

● 生体認証
パソコンやスマホなどを利用する時の本人確認を、指紋、虹彩、静脈、顔の形など、本人の生体の一部分を用いて認証すること

● 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。＝脆弱性

● セキュリティキー
無線LANに関するものの場合→「暗号キー」、物理的なものの場合→「USBセキュリティキー」

● 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。アップデートファイルに含まれる場合もある

● 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、全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心理テクニック。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、他のSNSやウェブサービスにログインして、利用可能にする規格。特定の身分証明書で、他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、他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。なお、プログラムを作るための設計ファイルもソース（もしくはソースコード）と呼ばれる

● 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
多要素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

● 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、その他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
多要素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

● 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、内閣府ではないってば。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
主にネットワーク上に設置された監視カメラ。セキュリティ上は主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設置したか分からない無線LANアクセスポイント。主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。バージョンの整数が上がるものをメジャーアップデート、小数点以下が上がるものをマイナーアップデートなどと呼ぶ

● ハードウェアトークン
多要素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。本書で言う「ログインパスワード」のみを指す場合と、暗証番号(PINコード)などや無線LANを利用する時に入力する「暗号キー」を含む場合がある。本書では明確に分けて記述している

● 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

● ハッカー
P12のコラム参照

● 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。更新された部分だけを追加してバックアップしていく方式は「差分バックアップ」とも呼ばれる

● 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個人情報にまつわるもののため、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などを調査すること

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 ≒BIOS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

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
CPUにケーブルなどを介して接続されデータを記録する記憶装置。ハードディスクやSSDなど。これに対してメインメモリと呼ばれCPUに直結するものを主記憶装置という。→記憶装置

ボット
ロボット(robot)の短縮形。さまざま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。パソコンやIoT機器などの機器が、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社員など)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た

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に対するWide Area Networkの意味。通信電波の供給範囲が広いものを指し、主に携帯電話の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、他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

● リンク
ウェブサイトやメール中にある、クリックすると所定のウェブサイトにジャンプする(リンクする)状態に設定されている文字列をさす。有意な文字列に設定されている場合もあれば、リンク先のURLの文字列に設定されている場合もある。表示されているURLとは別の場所へのリンクを設定できるため、表示されているものがイコールリンク先だとは思わないこと

● 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アクセスルータの他、高速なWANの回線を利用して、主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
携帯電話などを海外で使用するとき、その国の携帯電話会社と別途契約を結ばないまま、音声通話を利用できる状態にすること。同様のことをデータ通信に対して行う場合は「データローミング」という

● 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。また、自らの機器を紛失したときに、誰かが勝手に操作できないようにした状態。これを遠隔操作で行うことを、リモートロックや遠隔ロックという

● ロック画面
スマホを他者が勝手に操作できないような状態にした画面

● ワンタイムパスワード
＝使い捨てパスワード

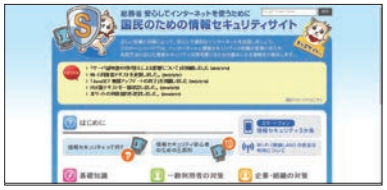
情報セキュリティ関連ウェブサイト一覧

情報セキュリティ関連のウェブサイト

● みんなでしっかりサイバーセキュリティ

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

● 国民のための情報セキュリティサイト



総務省
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/
総務省が運営する、情報セキュリティに関する基礎的なことを学べるサイト。企業向けの対策についても触れられている。

● ここからセキュリティ！

独立行政法人情報処理推進機構（IPA）
https://www.ipa.go.jp/security/kokokara/
IPA が運営する情報セキュリティを学べるサイト。さまざまなサイトのコンテンツを集約して分類されている。ポータルサイト的存在。

● 情報セキュリティ 安心相談窓口

独立行政法人情報処理推進機構（IPA）
https://www.ipa.go.jp/security/anshin/index.html
IPA が国民に向けて開設している、一般的な情報セキュリティ（主にウイルスや不正アクセス）に関する窓口。

● 情報セキュリティ

独立行政法人情報処理推進機構（IPA）
https://www.ipa.go.jp/security/
IPA が解説するサイトで最新のセキュリティ情報や、情報セキュリティ啓発コンテンツなどを提供している。

● 情報セキュリティ対策支援サイト

独立行政法人情報処理推進機構（IPA）
https://security-shien.ipa.go.jp/
IPA が中小企業における情報セキュリティ対策の水準向上の支援を目的として設置したサイト。「学びたい」「始めたい」「続けたい」を支援する。

● インターネットの安全・安心ハンドブック

内閣サイバーセキュリティセンター（NISC）
https://www.nisc.go.jp/security-site/handbook/index.html#ebook
各種電子書籍版の一覧がある（無料配信）

●Andoid アプリ版（無料配信）

Google Play で手に入れよう

●iOS アプリ版（無料配信）

App Store からダウンロード

NISC の SNS による情報発信

● Twiter

内閣サイバー（注意・警戒情報）

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

● FaceBook

内閣サイバーセキュリティセンター NISC

https://www.facebook.com/nisc.jp/
NISC の活動の紹介や、サイバーセキュリティに関するお役立ち情報を原則1日1回、コラムの形で発信している。

● Twiter

内閣サイバーセキュリティセンター（NISC） 公式アカウント

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

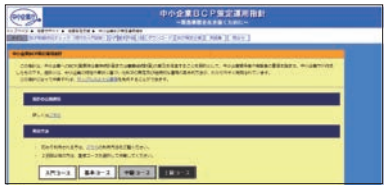
● LINE

内閣サイバーセキュリティセンター（NISC） セキュリティ関連情報

LINEID: @nisc-forecast
原則1日1回、サイバーセキュリティに関するお役立ち情報をコラム形式で発信している。

本書に掲載したサイトなど

● 中小企業 BCP 策定運用指針



中小企業庁
https://www.chusho.meti.go.jp/bcp/index.html

● 漏えい等の対応（個人情報）

個人情報保護委員会
https://www.ppc.go.jp/personal/legal/leakAction/

● 中小企業の情報セキュリティ対策ガイドライン

独立行政法人情報処理推進機構（IPA）
https://www.ipa.go.jp/security/keihatsu/sme/guideline/index.html

● 5分でできる自社診断の25項目

独立行政法人情報処理推進機構（IPA）
https://security-shien.ipa.go.jp/learning

● SECURITY ACTION セキュリティ対策自己宣言

独立行政法人情報処理推進機構（IPA）
https://www.ipa.go.jp/security/security-action/

● 情報処理支援機関検索（スマート SME サポーター）

中小企業庁
https://smartsme.secure.force.com/smartsmesearch/

IPA 安心相談窓口で対応出来ない案件の窓口

● 犯罪行為に対する被害届や相談をしたい

警察庁
https://www.npa.go.jp/cyber/soudan.htm
各都道府県の警察本部のサイバー犯罪の相談窓口と情報発信サイトの一覧

● 法的トラブルの相談をしたい

法テラス
https://www.houterasu.or.jp/

● インターネット上違法情報の通報

インターネット・ホットラインセンター
https://www.internethotline.jp/

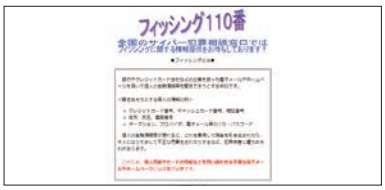
● 迷惑メールの受信に関して困っている

財団法人 日本データ通信協会迷惑メール相談センター
https://www.dekyo.or.jp/soudan/index.html

● フィッシングサイトの発見または被害に関して困っている①

フィッシング対策協議会
https://www.antiphising.jp/registration.html

● フィッシングサイトの発見または被害に関して困っている②



警察庁フィッシング 110 番
http://www.npa.go.jp/cyber/policy/phishing/phishing110.htm

災害時関連のウェブサイト

● 防災情報のページ

内閣府
http://www.bousai.go.jp/
災害時などに政府発表の情報が逐次公開される。また防災関連会議の情報や、大規模地震対策の計画なども公開されている。

● 防災情報提供センター

国土交通省
http://www.mlit.go.jp/saigai/bosaijoho/
リアルタイムの雨量情報他、ハザードマップ、傘下の気象庁発信の情報や、知識を学べる情報なども提供されている。

● 災害用伝言板（web171）

NTT東日本、NTT西日本
https://www.web171.jp/
災害発生時に設置される「災害用伝言ダイヤル」を、ウェブ経由から利用できるようにしたのがweb171。ウェブ経由でも共有できる。

● 災害・防災情報

国土交通省
http://www.mlit.go.jp/saigai/
災害時の状況や復旧状況を、国土や交通インフラの面から提供。情報は逐次更新され、地震、火山、風水害、雪害時などの状況が発信される。

● 気象庁 ホームページ

気象庁
https://www.jma.go.jp/jma/index.html
天気予報や気象全般に係わる情報、警報注意報、地震・津波・火山などの緊急時の情報、そしてさくらの開花状況まで提供される。

● 安否情報まとめて検索

J-anpi
https://anpi.jp/top
災害時にさまざまな形で提供される安否確認情報を、横断検索して確認をしやすくするためのシステム。NTTとNHKが提供。

● 公衆電話 設置場所検索

NTT東日本
https://service.geospace.jp/ptd-ntteast/PublicTelSite/TopPage/

● 公衆電話 設置場所検索

NTT西日本
https://www.ntt-west.co.jp/ptd/map/

● 公衆電話インフォメーション：公衆電話の種類と利用方法について

NTT西日本
https://www.ntt-west.co.jp/ptd/mag_public_kind.html

いじめ対策関連

● 子供（こども）のSOSの相談窓口（そうだんまどぐち）

文部科学省
http://www.mext.go.jp/a_menu/shotou/seitoshidou/06112210.htm
子供が自分自身で抱える不安や悩みを相談できる相談窓口を集約してあるサイト。

● インターネット人権相談窓口へようこそ！

法務省
http://www.moj.go.jp/JINKEN/jinken113.html
差別、いじめ、嫌がらせ等人権に関する問題で困っている方が気軽に相談できる

● ここにもあります！相談できる窓口が。「いじめ」しない させない 見逃さない

政府広報オンライン
https://www.gov-online.go.jp/useful/article/201505/2.html
さまざまな「いじめ」がある最近の現状と、大人と子どもができる「いじめ」へのかかわり方について解説された記事を掲載。

その他のTwitterアカウント

- 首相官邸（災害・危機管理情報）@Kantei_Saigai
- 内閣府防災　@CAO_BOUSAI
- 総務省消防庁　@FDMA_JAPAN
- 気象庁　@JMA_kishou
- IPA(ICATalerts)　@ICATalerts
- JPCERTコーディネーションセンター @jpcert
- フィッシング対策協議会 @antiphishing_jp
- Twitterライフライン @TwitterLifelin

索引

アルファベット

あ行

か行

さ行

た行

な行

は行

ま行

ら行

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
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

小さな中小企業とNPO向け 情報セキュリティハンドブック

2019年3月26日　Ver 1.00発行
2020年3月31日　Ver 1.10発行

制作・著作　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　中小企業庁　独立行政法人情報処理推進機構(IPA)
イラスト　ＫＯＴＡ