プロローグ

インターネットにある基本的なリスクやトラブルを知ろう

私たちは、スマホやパソコンを用いて、いつでもどこでもインターネットにつながり、便利なサービスを利用したり、世界中の人とコミュニケーションしたりできます。しかしインターネットには、注意したいリスクやトラブルがあります。まずは本書全体を通じて登場する基本的なリスクやトラブルについて知りましょう。

1 サイバー攻撃とは？

よく聞く「サイバー攻撃」とは？

サイバー攻撃は、誰がなんの目的でやっているのでしょう。

軍事スパイや産業スパイ？ それともハッカー？

いわゆるスパイ▶用語集 P.197の目的は、軍事機密や先進の研究内容など、自国や企業にとって有益な情報の入手です。それに対し、私たちが普段遭遇するサイバー攻撃は、主として個人情報や金銭など、攻撃する者にとって利益が得られることにつながることを目的としています。

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

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

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

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

2 ハッカーと攻撃者とは？

「ハッカー」の意味やさまざまな呼称

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。

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」▶用語集 P.201 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▶用語集 P.196 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」▶用語集 P.196 から転じて「クラッカー（cracker）」▶用語集 P.195 や攻撃者の意味を持つ「アタッカー（attacker）」▶用語集 P.194 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」▶用語集 P.193 ともいわれます。（本書ではこれらの人を「攻撃者」「悪意のハッカー」などと呼びます）

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。

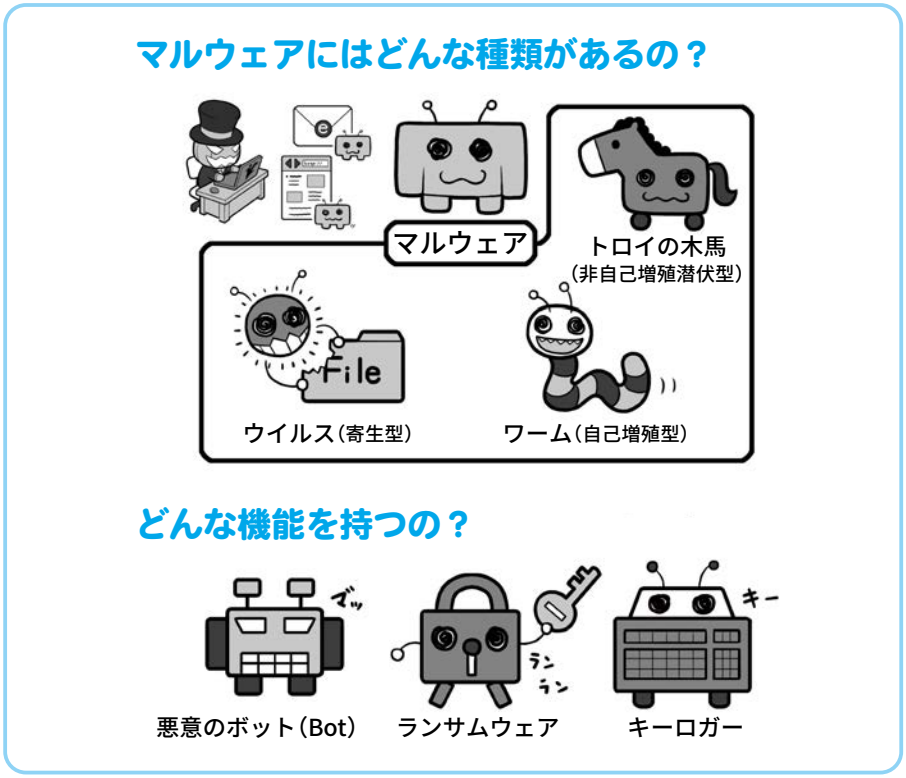
3 攻撃者が使う武器「マルウェア」とは？

3.1 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1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」▶用語集 P.203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」▶用語集 P.203「ランサムウェア」▶用語集 P.203「キーロガー」などの呼び方もあります。これは病原体の行動形態を表す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。



3.2 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▶用語集 P.194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▶用語集 P.200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。

3.3 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▶用語集P.203、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▶用語集P.191、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。

とくにIoT（Internet of Things）▶用語集P.191、「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）▶用語集P.198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▶用語集P.194＝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▶用語集P.194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」▶用語集P.201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

4 サイバー攻撃の具体例は？

4.1 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。

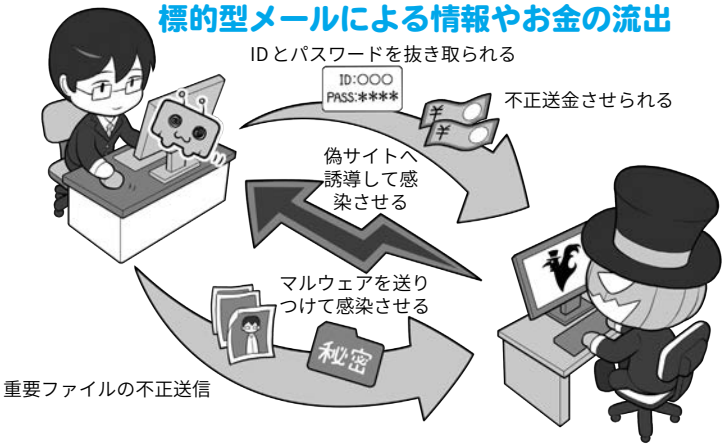
サイバー攻撃として代表的なものは、みなさんが普段業務に使っているパソコンやスマホなどが、マルウェア（他者を攻撃する不正なプログラム。一般的にはコンピュータウイルスとも呼ばれる）に感染し、インターネットを通じて機密情報やお金が、流出させられたり盗まれたりするものがあります。

パソコンなどの脆弱性（弱点。以下セキュリティホール）▶用語集 P.197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▶用語集 P.202（以下ウェブサイト）へ誘導するリンク▶用語集 P.204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。

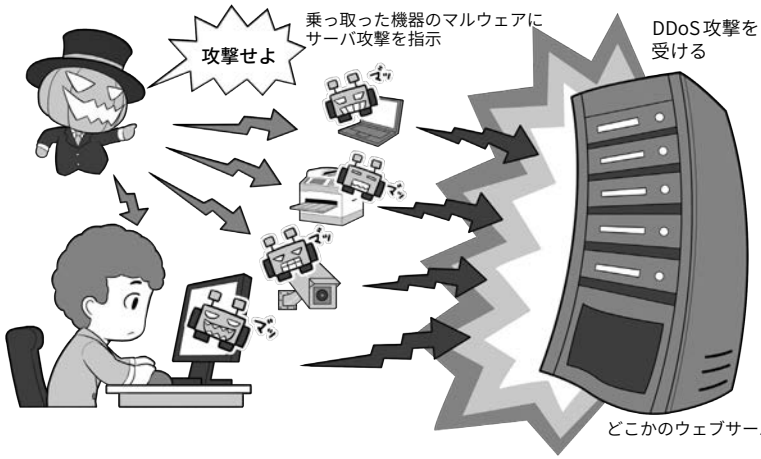
「マルウェアはともかく、リンクで？」と思うかも知れませんが、リンク先を開いてみれば有名銀行のネットバンキングと瓜二つの偽サイトになっていて、ID▶用語集 P.191とパ

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機器の乗っ取り～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。

スワードを入力させられ、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。

4.2 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）」▶用語集 P.190があります。BECとは、攻撃する相手や環境を事前によ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。

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。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よいと考えるかもしれません。

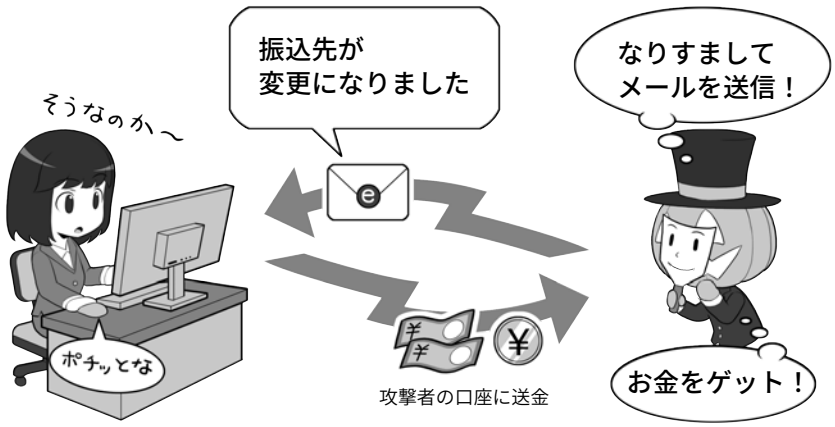
そうした特定の会社や団体を標的とした「サイバー攻撃」は、知らない間に所有するパソコンなどに入り込む不正アクセス、既に紹介したBEC、ランサムウェア他さまざまな手段で襲いかかってきます。

ちなみにBECは、国際比較したとき日本企業は被害報告が少ない傾向があります。日本企業では、多額の支払いには入念な確認を必要とするビジネスプロセスが構成されていることも被害が少ない要因の1つと考えられます。

ただしこれは、あくまで現時点の話であり、例えばビジネスプロセスが成熟していないスタートアップ企業などを狙ったBECが発生しないとも限らないため、注意を怠ってはいけません。

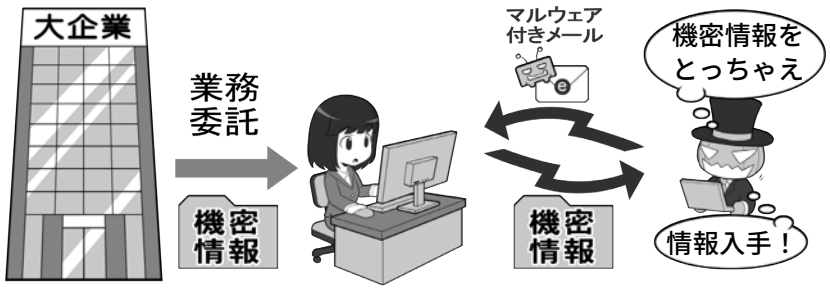
データが漏えいしたら発注元からは信用のならない取引先と判断されて取引が打ち切られることも十分に想定されます。とくに小さな会社やNPOなどにとってはまさに死活問題になり得るサイバー攻撃なのです。

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とりをしているか、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ほうが簡単と考えます。外注を受けていればしめたものと考えます。

5 攻撃者とはどんな人物なの？

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。ではその悪意を持った人々は何者なのでしょうか？

まず最もアマチュア的なものが、こどもの腕試しやスクリプトキディ▶用語集 P.197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。ただ単純に趣味や興味だけで攻撃を行う人は、最近のセキュリティ対策意識の高まりや法整備の状況から、攻撃を仕掛けることによるリターンよりもリスクのほうが上回り、その結果相対的に少なくなっているように見えます。

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。しかし金銭目的の攻撃者は多くの企業、個人に対して被害を及ぼしており、現在は組織化、相互連携を進める方向に進んでいます。単独で攻撃するよりは、チームを組んで得意な分野、技能を出し合い、利益の効率を上げようとしているのです。

次に企業が持つ先進技術や製品計画などを盗もうとする産業スパイ、兵器開発や軍事計画の情報を狙ったり敵対国に誤情報の拡散で混乱を起こしたりしようとする軍事的ハッカーなどです。明確な目標を持つ攻撃者のため、狙われるとコストを度外視して何度も執拗に攻撃を仕掛けてきます。

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。

6 どうやって攻撃されるの？

6.1 おも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2つの方向性があります。1つは技術的な攻撃、もう1つは心理的な攻撃です。

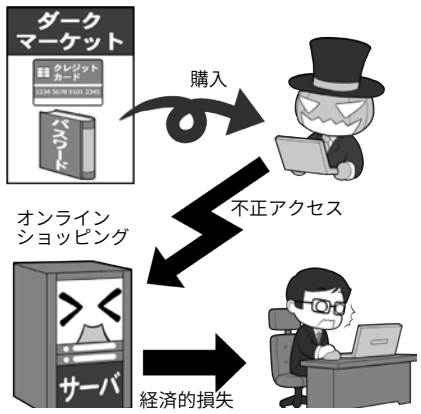
マルウェアを使ってパソコンやスマホ、あるいはシステム上のセキュリティホールを突く、技術的で「サイバー攻撃」の要素が強いものが前者。「ソーシャルエンジニアリング」▶用語集 P.198と呼ばれ、人間の心の隙を突く詐欺や「心理攻撃」の要素が強いものが後者です。本項では「サイバー攻撃」について解説します。

まずは、自分や自社が攻撃され自らが損害を受けるサイバー攻撃。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。

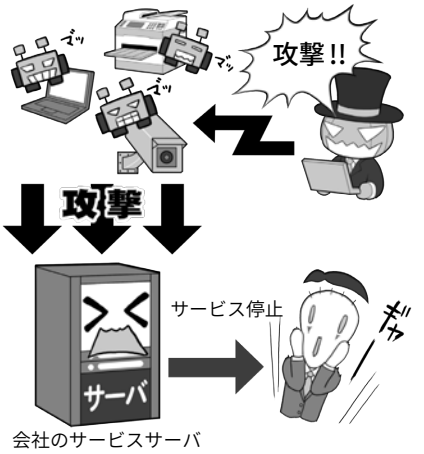
次に自分や自社が気付かないうちに攻撃される例です。インターネットでは日々、さまざまなウェブサービスが攻撃されアカウント情報の漏えいが発生しています。例えば個人用のアカウントのIDとパスワードを会社用にも使い回ししていると、どこかのサービスから漏れた情報によって会社のシステムへの不正侵入や不正利用を許すことにつながります。また、業務でインターネット上のクラウドストレージサービスに重要情報を保存していると、ここから情報流出が発生するかもしれません。この例では「自分自身はマルウェアなどに感染した形跡がなくても攻撃される」ことを知って下さい。

最後に、自社が攻撃されるだけでなく他者にまで損害を与える例です。攻撃者が多数のIT機器にマルウェアを感染させた上で、それらのIT機器からターゲットにした他者のコンピュータなどに通常では考えられない量のデータをターゲットに送りつけ使えない状態にする「DDoS攻撃」▶用語集 P.190、パソコンの中身を勝手に暗号化して、暗号化の解除と引き換えに身代金を要求して脅迫する「ランサムウェア」などが挙げられます。自社で業務遂行をできなくなると、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ます。また、業務が停止することで、業務に関連する顧客／サービス利用者にも間接的に経済的損失を与えます。

流出情報で乗っ取られて経済的損失



ボットネットからのDDoS攻撃で業務停止



ランサムウェアで暗号化して身代金要求

6.2 人の心の隙を突く心理的な攻撃～ソーシャルエンジニアリング

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、人間の心の隙をついた攻撃が存在することを認識し、予防する意識を持つことが重要です。

この狙った情報を、情報通信技術に限定せず心理的攻撃も組み合わせながら盗み出す攻撃を「ソーシャルエンジニアリング」と呼びます。

「ソーシャルエンジニアリング」は現実でもネットでも心の隙を突いてだます

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テクニックなのです。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」▶用語集 P.201「ネームドロップ」▶用語集 P.200「ギブアンドテイク」▶用語集 P.195 などにあたるでしょう。

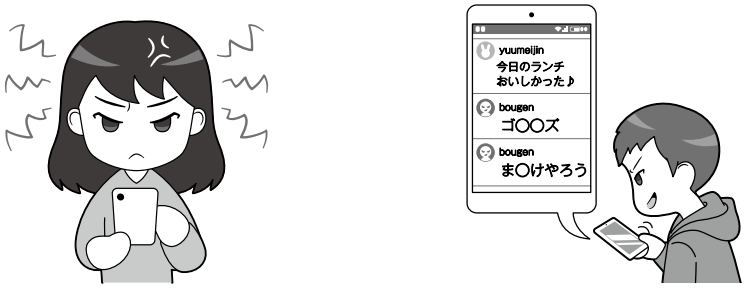
一方、ネットの世界のソーシャルエンジニアリングは、知り合いになりすまして「標的型メール」を送る場合、これらの「フレンドシップ」▶用語集 P.202 という手法の要素が使われています。ちなみに標的型攻撃メールにおいては、攻撃者が特定の組織へ攻撃を仕掛ける前に「トラッシング」▶用語集 P.200 と呼ばれるゴミ箱を漁る行為で、サーバやルータなどの設定情報、ID パスワードなどの情報を捨てられた資料から探ることがよくあります。

攻撃者は情報通信技術に限定せず心理的攻撃も組み合わせて攻撃を仕掛け、セキュリティを突破しようと試みます。

7 SNSやネットのコミュニケーションで注意したいことは？

7.1 SNSやネット上の誹謗中傷対策

SNSやネットで他人を傷つける発言をしてはいけません



SNS ▶用語集 P.192 は自由に自分の意見を発信できて便利ですが、議論が行き過ぎ感情的な発言をしてしまうことは誰にでもあります。SNS やネット上の過激な発言は、名誉毀損罪や侮辱罪などの犯罪となる場合もあります。対面でのコミュニケーションと同じように、他人を傷つけるような発言を SNS やネット上でも決して発信してはなりません。

総務省 HP ｜インターネット上の誹謗中傷への対策
https://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/hiboutyusyou.html
インターネット上の誹謗中傷への対応に関する政策パッケージの概要（PDF）
https://www.soumu.go.jp/main_content/000755959.pdf

サイバー攻撃のほかにも、私たちにとって身近なSNSやネットのコミュニケーションでは、気を付けたいトラブルがたくさんあります。とくにSNSは自分の発言を広く読んでもらい、自由に他の人と交流することができる便利なサービスですが、常に周りの人が自分と友好的な意見だとは限りません。議論が行き過ぎることもありますし、また、自分が気に入らない人に対しての表現がうっかり過激になってしまうこともあります。一方、誹謗中傷となるような批判的発言を多数人から受ける立場になってしまえば、精神的に極めて辛い立場に立たされることになり、残念ながら自らを傷つける行為を選ぶような人や事例も生じています。

SNSやネット上での誹謗中傷対策として、総務省では「インターネット上の誹謗中傷への対応に関する政策パッケージ」を発表しています。

その内容は、以下のとおりです。

- **ユーザーに対する情報モラル及びICTリテラシーの向上のための啓発活動**
- **プラットフォーム事業者の自主的取組の支援と透明性・アカウンタビリティの向上**（SNS事業者による削除等の自主的取組を支援すると共にその状況把握を行うものです。）
- **発信者情報開示に関する取組**（他者の権利を侵害する発言に対し削除や損害賠償などの権利行使を行う前提として、発信者を特定するための制度の整備です。）
- **相談対応の充実に向けた連携と体制整備**（誹謗中傷などの被害を受けた人が相談を行う窓口間の連携強化と相談員の増員などを行うものです。）

また、ネット上の過激な発言は、名誉毀損罪や侮辱罪などの犯罪となる場合もあります。名誉毀損罪と侮辱罪の違いは、事実の指摘があるかどうかですが、SNSやネット上で対象を過激に傷つけるような「ゴ〇〇ズ」や「ま〇けやろう」などの発言は侮辱罪にあたる可能性があります。侮辱罪の法定刑が令和4年7月7日より引き上げられています。それまで侮辱罪の刑は、拘留また科料という極めて軽く、例外的な場合を除き、逮捕がされない内容でしたが、今では、1年以下の懲役若しくは禁錮若しくは30万円以下の曝気又は拘留若しくは科料とされ、逮捕の可能性もあるものとなっています。誹謗中傷的発言をしないように注意しましょう。

7.2 SNSやネット上の犯罪やトラブル

SNSやネットでコミュニケーションする際、注意すべき犯罪もたくさんあります。

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

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

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

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

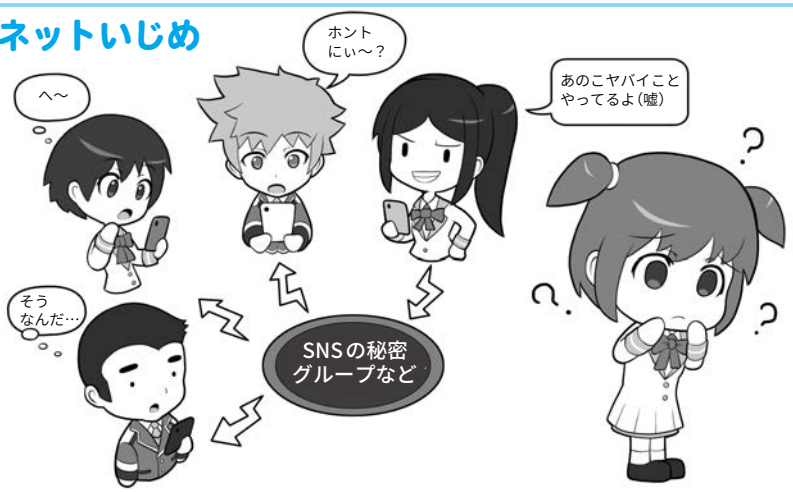
なりすましや誘拐・略取（連れ去り）

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

自画撮り（セクスティング）被害

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

ネットいじめ



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

各章ダイジェスト

プロローグ
インターネットにある基本的なリスクやトラブルを知ろう

私たちは、スマホやパソコンを用いて、いつでもどこでもインターネットにつながり、便利なサービスを利用したり、世界中の人とコミュニケーションしたりできます。しかしインターネットには、注意したいリスクやトラブルがあります。まずは本書全体を通じて登場する基本的なリスクやトラブルについて知りましょう。

→P.13〜26

第1章
まずはサイバーセキュリティの基礎を固めよう

サイバー攻撃を受けないようにするため、まずは基礎的なセキュリティの固め方を理解しましょう。スマホやパソコンを最新の状態にすること、安全なパスワードの管理方法、もしものときのバックアップの必要性など、攻撃する側からのサイバー攻撃を防ぐためにはどうすればよいかを学びましょう。

→P.27〜48

第2章
よくあるサイバー攻撃の手口やリスクを知ろう

基礎的なセキュリティを固めても、インターネットにつながる限りサイバー攻撃を受けてしまうリスクはあります。実際にサイバー攻撃を受けてしまうとどんな被害があるのでしょうか。乗っ取りやランサムウェアなど、よくある被害について学びましょう。

→P.49〜56

第3章
SNS・ネットとの付き合い方や情報モラルの重要性を知ろう

現代では、SNSを通じて、世界中の人たちと簡単につながりコミュニケーションできます。しかし、接する人がすべて自分と友好的であるとは限りません。SNSやネットでよくある危険やトラブルについて知り、対策や家族を守る方法を学びましょう。

→P.57〜78

第4章
災害・テロ、海外でのトラブル、普段とは違う環境のリスクに備えよう

災害・テロなど、非常時にもインターネットにつながり情報収集することは大切です。また、海外でインターネットを利用する際、日本では遭遇しないトラブルやリスクがあります。普段とは違う環境に備えるには、普段からどんな準備をしておくとよいか学びましょう。

→P.79〜90

第5章
スマホやパソコン、IoT機器を安全に利用するための設定を知ろう

スマホ・パソコンを中心に、安全を守るための設定について学びましょう。またIoT機器ならではの注意したいリスクについても解説します。どのように情報を守るか、どのように安全にインターネットを利用するか、具体的な設定方法を学び不安なく利用できるようにしましょう。

→P.91〜108

第6章
パスワードの大切さを知り、通信の安全性を支える暗号化について学ぼう

インターネットを安全に利用するには適切なパスワード管理が不可欠です。また通信の安全性を保つには暗号化技術が役立っています。パスワード管理、知っておきたい暗号化の必要性やしくみを学びましょう。

→P.109〜148

第7章
中小組織向け
セキュリティ向上が利潤追求につながることを理解しよう

人材・体制・資金などが限られた中小企業にとって、通常業務をこなしながらセキュリティ対策を講じるための負担は少なくありません。しかし、企業経営においてセキュリティ対策を省くことはできません。セキュリティ対策に投資すべき理由、テレワークを安全快適に利用するために必要なルール作り、企業だからこそ気を付けたいサイバー攻撃、そして最低限把握しておきたいセキュリティ関連の法律などを学びましょう。

→P.149〜172

付録
知っておくと役立つサイバーセキュリティに関する手引き・ガイダンス

本書の最後には、知っておくと役立つ手引きやガイダンスなどを紹介します。サイバー攻撃を受けた場合に相談できる公的機関の窓口、スキルアップしたい中小組織のセキュリティ部門担当者に役立つ情報、そして本格的な普及がはじまったマイナンバーカードなど、実践的な内容を解説します。
また、本章では、「一般国民向け」「中小組織向け」と中心となる対象読者を表すタグを付しています。

→P.173〜188

サイバーセキュリティ対策９か条

次のP.27からはじまる第１章より、NISCとIPAが提唱する「サイバーセキュリティ対策９か条」に即した、基礎的なセキュリティの考え方・対策を解説します。

1 OSやソフトウェアは常に最新の状態にしておこう

最新の攻撃情報に対抗するため、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ましょう。

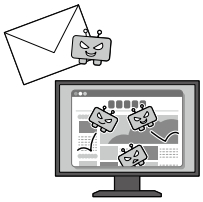
2 パスワードは長く複雑にして、他と使い回さないようにしよう

パスワードは長く複雑にし、機器やサービス間で使い回さないことを徹底して安全性を高めましょう。

3 多要素認証を利用しよう

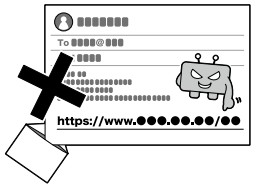
サービスへのログインを安全に行うために、認証用アプリや生体認証を使った多要素認証を利用しましょう。

4 偽メールや偽サイトに騙されないように用心しよう



フィッシング詐欺メールは年々手口が巧妙になっています。心当たりがあるものでもメールやメッセージのURLには安易にアクセスしないようにしましょう。

5 メールの添付ファイルや本文中のリンクに注意しよう



心当たりのない送信元からのメールに添付されているファイルやリンクはもちろん、ファイルやリンクを開かせようとするものには注意しましょう。

6 スマホやPCの画面ロックを利用しよう

スマホやパソコン(PC)の情報を守るには、まず待ち受け画面をロックすることが第一です。短時間であっても端末を手元から離す際はロックを忘れないようにしましょう。

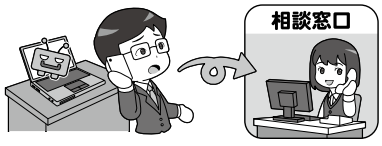
7 大切な情報は失う前にバックアップ(複製)しよう

大切な情報を失っても、バックアップから復元することで被害を軽減することができます。普段からバックアップして攻撃や天災に備えましょう。

8 外出先では紛失・盗難・覗き見に注意しよう

外出先でスマホやパソコンを使うときは、背後からの覗き見に注意しましょう。また、紛失・盗難の危険があるので、公共の場でスマホを放置することは絶対にやめましょう。

9 困ったときは１人で悩まず、まず相談しよう



インターネットでの被害に遭遇したら、1人で悩まず各種相談窓口に相談しましょう。