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。

1 攻撃者に乗っ取られると起こることを知ろう

1.1 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▶用語集 P.182があなたのパソコンなどにサイバー攻撃▶用語集 P.182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▶用語集 P.188に感染させるか、流出したID▶用語集 P.177とパスワード▶用語集 P.186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。

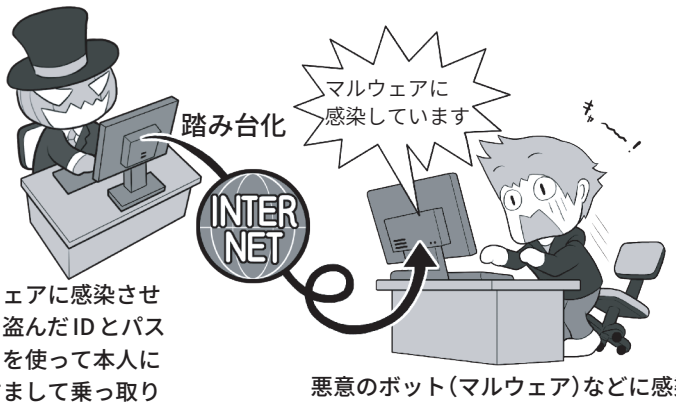
次に別のパソコンやサーバなどに侵入するとき、「踏み台▶用語集 P.188」にしてあなたのパソコンがやっているように見せかけたり、悪意のボット▶用語集 P.188によるボットネット▶用語集 P.188に接続させ、第三者へのDDoS攻撃▶用語集 P.176を行わせたりします。

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。

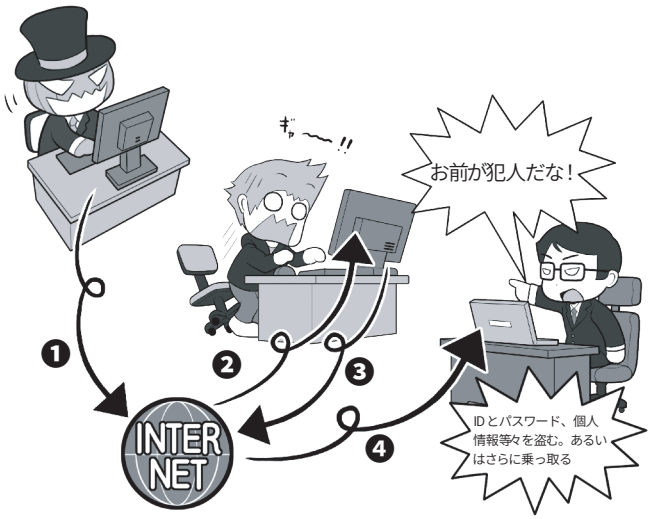
そうならないためにも、公衆衛生的なマナー意識を持って、パソコンなどのセキュリティはしっかり固めましょう。もしセキュリティソフト▶用語集 P.183が、マルウェアに感染していることを検出したら速やかにネットから切断し、実害の出ている攻撃に関して、警察などから協力の要請があった場合は証拠保全（第4章4（P.96）参照）を行いましょう。

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

乗っ取ったパソコンを踏み台にしてサイバー攻撃を行う



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

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

1.2 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▶用語集P.182、クレジットカードや銀行情報、ウェブ▶用語集P.180サービスやSNS▶用語集P.178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▶用語集P.180を使った不正送金▶用語集P.187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▶用語集P.184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。

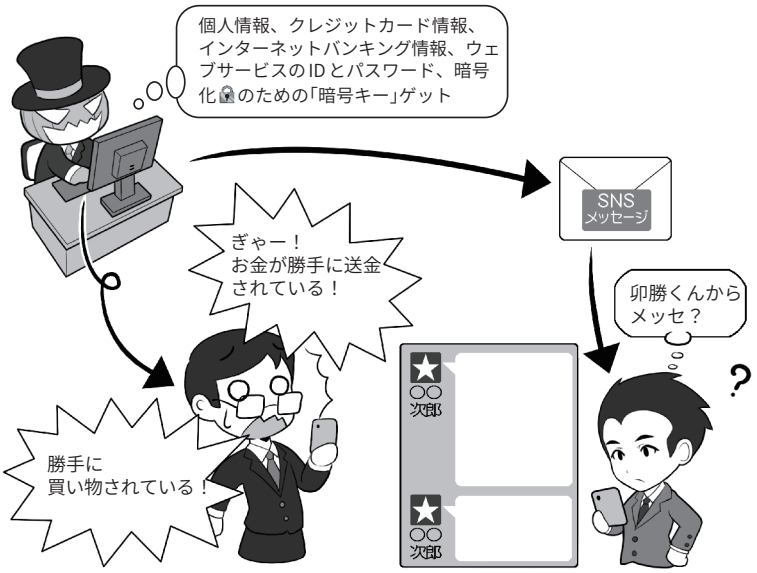
SNSのメッセージであなたになりすまし▶用語集P.185、友だちに対して「プリペイドカードを買って、アクティベーションコード▶用語集P.179を送ってくれ」と依頼して、電子マネーを騙し取る場合もあります。

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

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

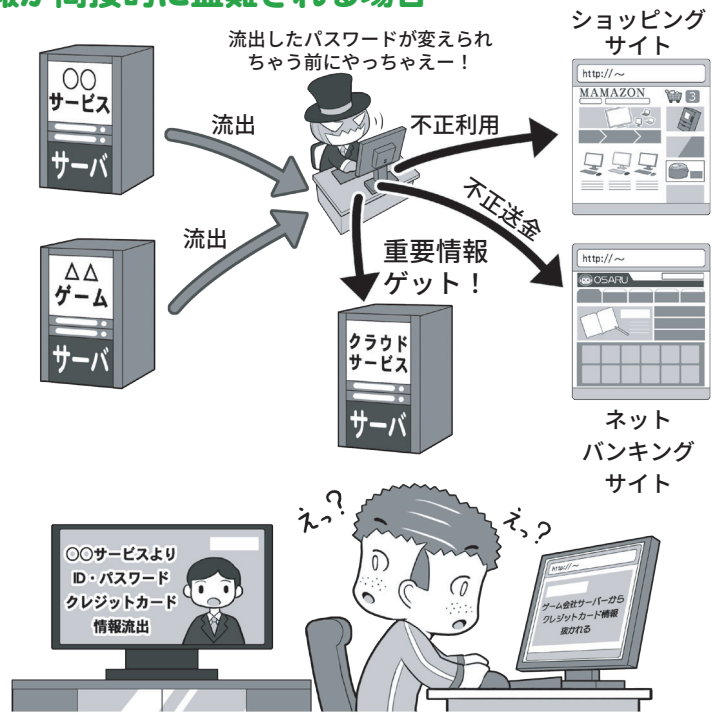
パスワード流出が判明したらパスワード設定のセオリー(第1章3 P.31-P.32)参照)にしたがってすぐに変更し、クレジットカード情報が流出したらカード会社に連絡してカードの番号を変更しましょう。

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。

1.3 乗っ取られた機器はサイバー攻撃に使われる

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

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

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

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

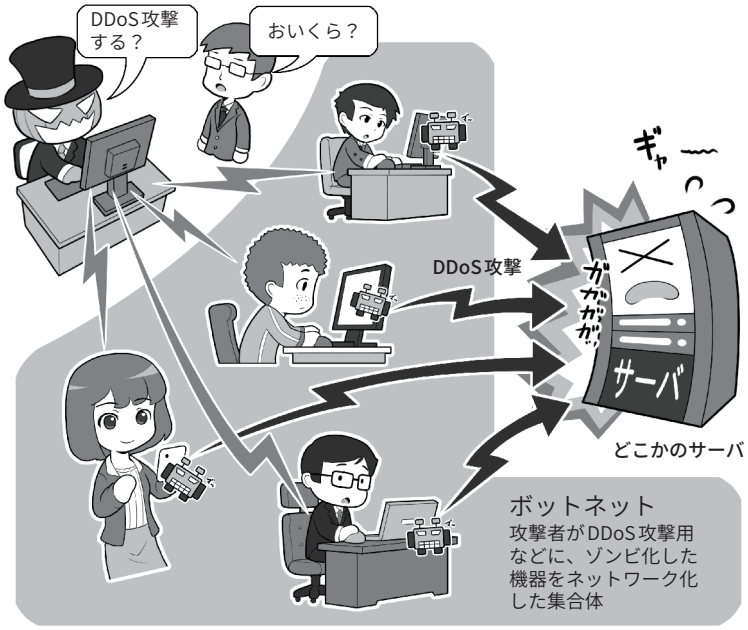
「ウォードライビング」といって、車で移動しながら、会社や事務所に設置されている、暗号化▶用語集 P.179されていない、もしくは暗号化や暗号キー▶用語集 P.180の設定の甘い無線LANアクセスポイント▶用語集 P.188を探し、見つけるとこれに侵入して利用する手法があります。

これはアクセスポイント▶用語集 P.179を「踏み台」にし、そこからインターネット上のさまざまなサーバやインフラ企業に攻撃をしかけるためです。

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

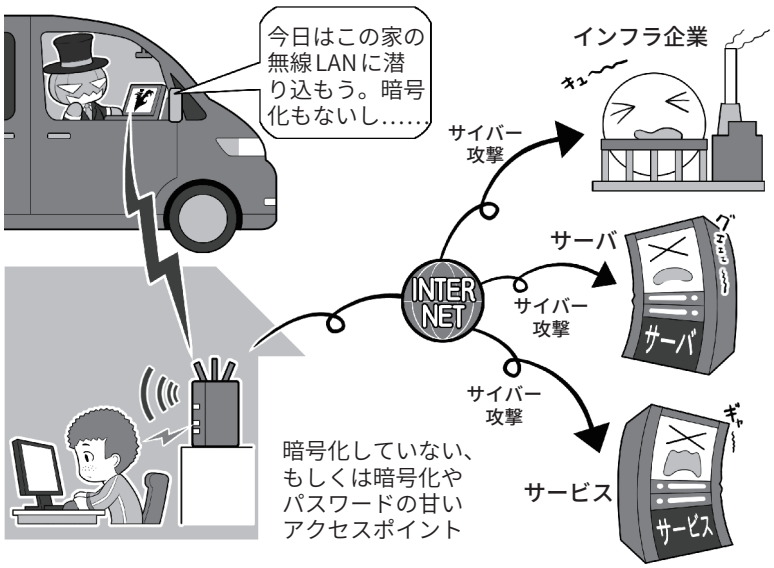
この場合、会社や事務所からサイバー攻撃が行われ、インフラ企業などで事故が発生したら社会的影響は大きいので、セキュリティを固めて侵入されないようにしましょう。

乗っ取られたマシンはボットネットとして貸し出される



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

無線LANに侵入され罪を押し付けられることも



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

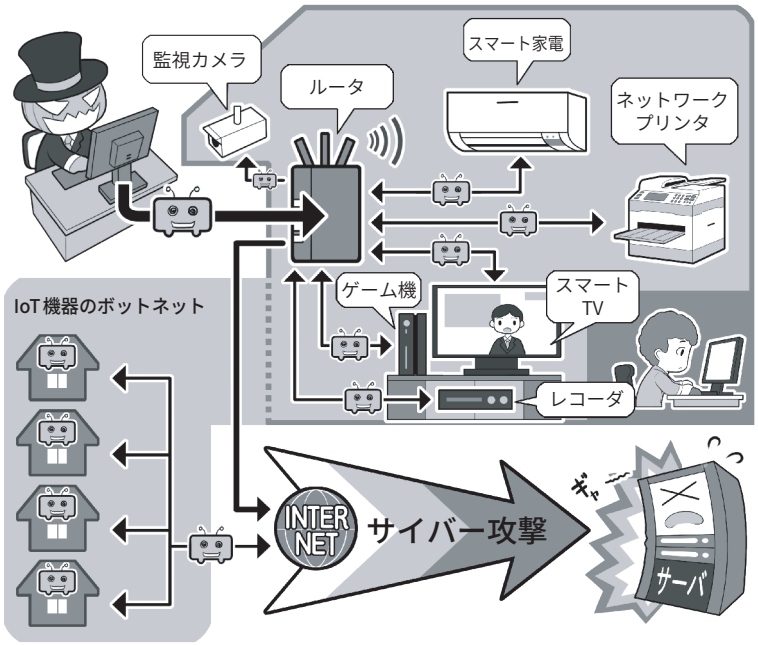
1.4 IoT機器も乗っ取られる。知らずにマルウェアの拡散も…

攻撃者によって乗っ取られるのはパソコンやスマホだけではありません。ネットにつながるIT機器はいずれも、乗っ取られて攻撃者の身代わりにされる「踏み台」化、DDoS攻撃のボットネットへの接続、マルウェアの拡散▶用語集P.180など、さまざまなサイバー攻撃に利用される可能性があります。とくにIoT機器は、監視カメラやネット対応電子機器などのように、普段私たちがあまりセキュリティについて気にかけないものであり、パソコンほどサイバー攻撃への対応能力も高くありません。そして1つの機種で生産台数が多い＝手間をかけずに多数を一気に攻撃できる「攻撃しやすい条件」が揃っているのです。最低でも、IoT機器の出荷時の「管理者用パスワード▶用語集P.181」などはパスワードセオリー(第1章 3 P.31-P.32)参照)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▶用語集P.184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▶用語集P.179試してみて」といった投稿を考えなしに拡散していると、その先はフィッシングサイトだったり、マルウェアのようなアプリだったりということもあり得ます。

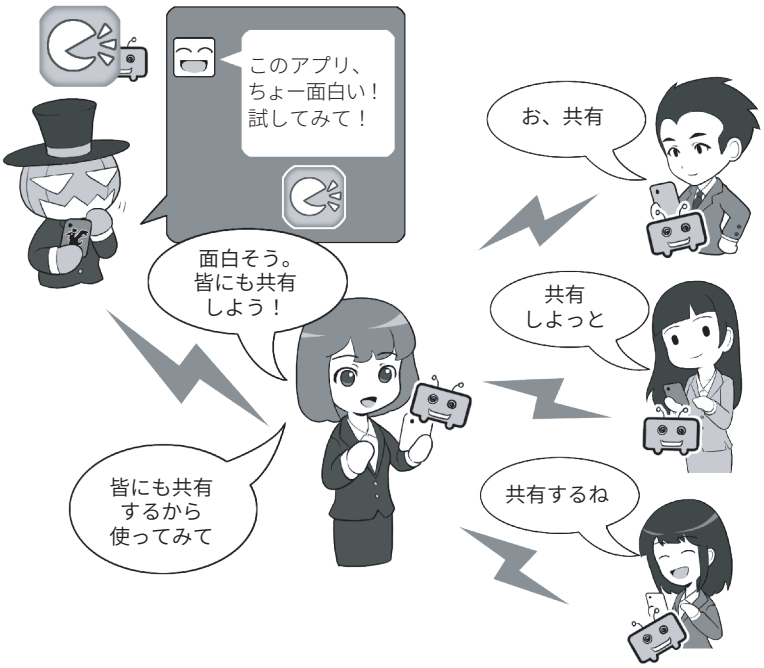
ネットでなにか行動する前には、必ず「それは本当に必要なのか」、「そうすることでなにか問題が発生する可能性はないのか」をいつも注意しましょう。

IoT機器も乗っ取られ攻撃に使われる



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

知らずにマルウェアの拡散に協力しているかも……



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

2 大きな脅威となっているランサムウェアを知ろう

パソコンなどのデータを暗号化し、ファイルを開けないようにして、身代金を要求するランサムウェア▶用語集 P.189。その大規模な感染に注目が集まっています。

例えば、2021年10月には、四国の病院で稼働しているシステムにランサムウェアが感染し、病院の診療を停止せざるを得なくなったうえ、復旧に2ヶ月以上を要するという事態になりました。また、「令和6年上半期におけるサイバー空間をめぐる脅威の情勢について」（警視庁）によれば、この数年ランサムウェアによる国内被害の報告件数は増加し、2020年下半期が21件だったのに対し、2024年上半期のランサムウェア被害は114件と5倍以上の数になっています。

これはあくまで「報告された件数」であり、報告されていない被害も相当数あると考えるのが妥当です。

近年では感染経路が多様化しており、メールを経由して不審なファイルをインストール▶用語集 P.180 させられるだけでなく、最近では、リモートデスクトップやVPN▶用語集 P.178 機器のぜい弱性▶用語集 P.183 を突いて、外部から侵入されるケースの割合が大きくなっています。

また、脅迫の手法についても、暗号化したデータの復号▶用語集 P.187 をもちかけて身代金を要求することに加え、盗んだデータを外部に公開するという脅しをかけ、さらなる身代金を要求するケースも出てきています。

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

こういったランサムウェアでは、身代金を支払ってもデータの暗号化を解除できなかったり、外部公開されたりするケースも多発しており、最悪の場合は端末を初期化▶用語集 P.182 しなければならず、大切なデータが失われることにもなりかねません。ランサムウェアに感染してこういった事態に陥らないよう、システムやアプリは最新の状態に保つ、データを常にバックアップ▶用語集 P.186 する、必要に応じてセキュリティソフト▶用語集 P.183 を利用するなどの対策をしっかり実施しましょう。また、不審なメールのリンク▶用語集 P.189 をクリックしない、あやしいウェブサイト▶用語集 P.180 からソフト▶用語集 P.184 やアプリをインストールしないよう意識することも重要です。ただ、最も大事なのは、企業や団体が、組織としての方針を示した上で、前述のような対策を徹底することです。

まずは「事前」に、ランサムウェアも含め、マルウェアに感染した場合の対応ポリシーや手順を策定するとともに、感染した場合には策定したポリシーや手順に則った対応をしてください。

なお、ランサムウェアによる攻撃や情報の無断公開は犯罪なので、対応手順などを検討する際には、警察への通報・相談なども視野に入れましょう。

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

ランサムウェアの被害を受けたら悩まずすぐに相談！

ランサムウェアによる攻撃や情報の無断公開はれっきとした犯罪です。被害を受けた場合は、警察への通報・相談などをしましょう。NISCとしてもランサムウェア対策のための対応手順や情報を公開しています。

警察庁 サイバー犯罪対策「ランサムウェア被害防止対策」
https://www.npa.go.jp/bureau/cyber/countermeasures/ransom.html
NISC「ストップ！ ランサムウェア　ランサムウェア特設ページ」
https://www.nisc.go.jp/tokusetsu/stopransomware/index.html

3 偽・誤情報、サイバープロパガンダに騙されないようにしよう

悪意を持った者が、なんらかの意図を持って、ネット上で偽のニュースを発信する「フェイクニュース▶用語集 P.187」。SNSなどで拡散され始めるとニュースサイトなどでも真贋不明のまま取り上げられ、それを真実だと思う人が多数現れてしまうということが起きています。フェイクニュースに代表されるように、ネット上ではあたかも正しい情報のように偽情報や誤情報が流通しています。SNSにも偽の情報も多く記載されていたり、名前等を偽っての投稿も多く見られます。

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

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

こういったフェイクニュースを、外国の国家機関や政治的意図を持った者などが「武器」として使い、他国の選挙における投票行動などに意図的に影響を及ぼす「サイバープロパガンダ」▶用語集 P.182も多く発生しています。

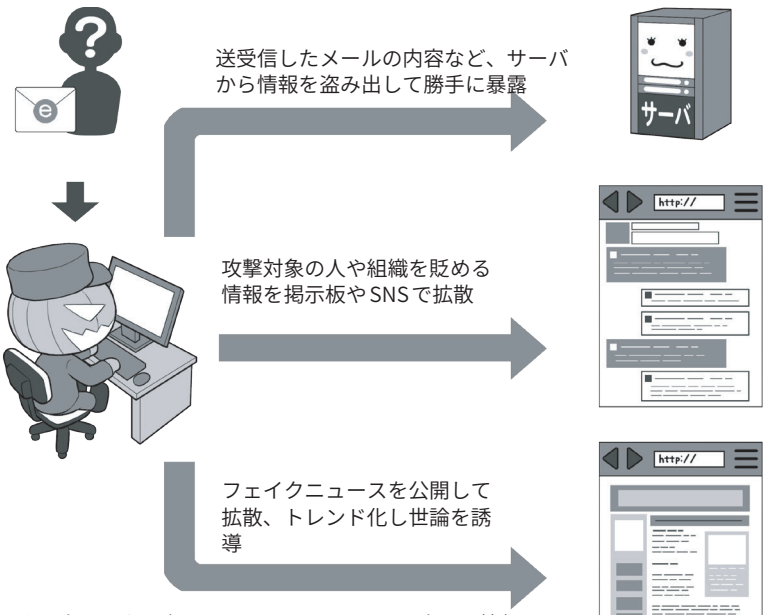
古くから国家が自国や他国に対して影響を及ぼすために行われてきたプロパガンダは、ネットを使うことでサイバープロパガンダとして、高度化かつ秘密裏になり、人々が気付かぬ間に、その考え方が操作される事態が起きています。

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

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

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

サイバープロパガンダが行われた例（米国）



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

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

コラム.1 最新の状態に保って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付けば、アップデート▶用語集P.179用のセキュリティパッチ▶用語集P.184を開発し公開します。

通常この競争に先行するのは攻撃者です。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▶用語集P.184」といいます。

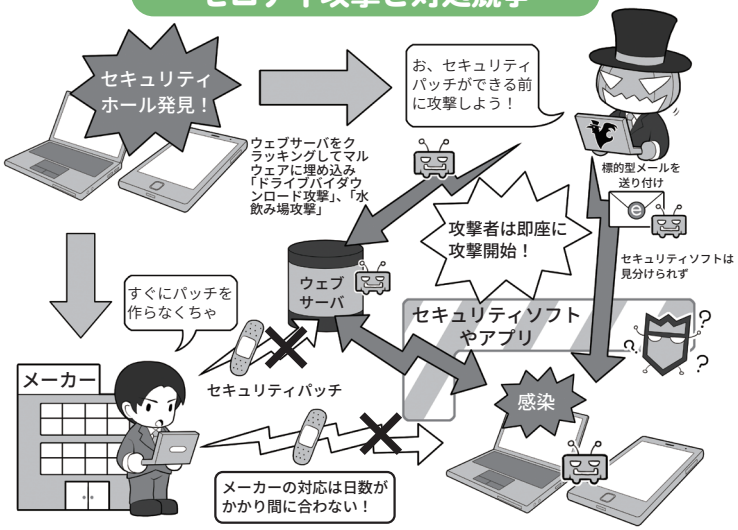
メールなどで送り付けられるマルウェアは、警戒していればある程度防げますが、動画、ウェブサイトやウェブ広告に仕込まれるマルウェアは、特定のウェブサイトを見ただけで感染することもあり、情報が無いままこの方法でゼロデイ攻撃を受けると実質的に防ぐことができません。

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▶用語集P.177のX(旧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、必要な対応を行うようにしましょう。メーカーがアップデート用のセキュリティパッチを提供するまでの緩和策を公開することもあるので、可能であればそのような対策を実施しましょう。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オフにする、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▶用語集P.179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▶用語集P.180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。

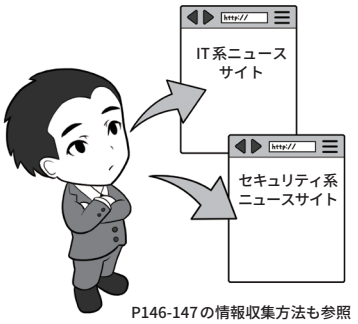
ゼロデイ攻撃とは？ 対処の例

ゼロデイ攻撃と対処競争



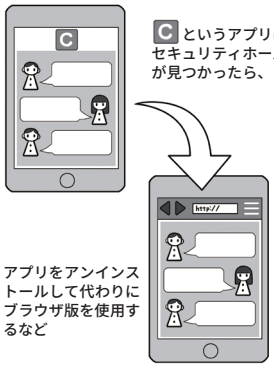
ゼロデイ攻撃に対抗するには？

ニュースサイトをこまめに見て情報収集



P146-147の情報収集方法も参照

別の手段でセキュリティホールを避ける

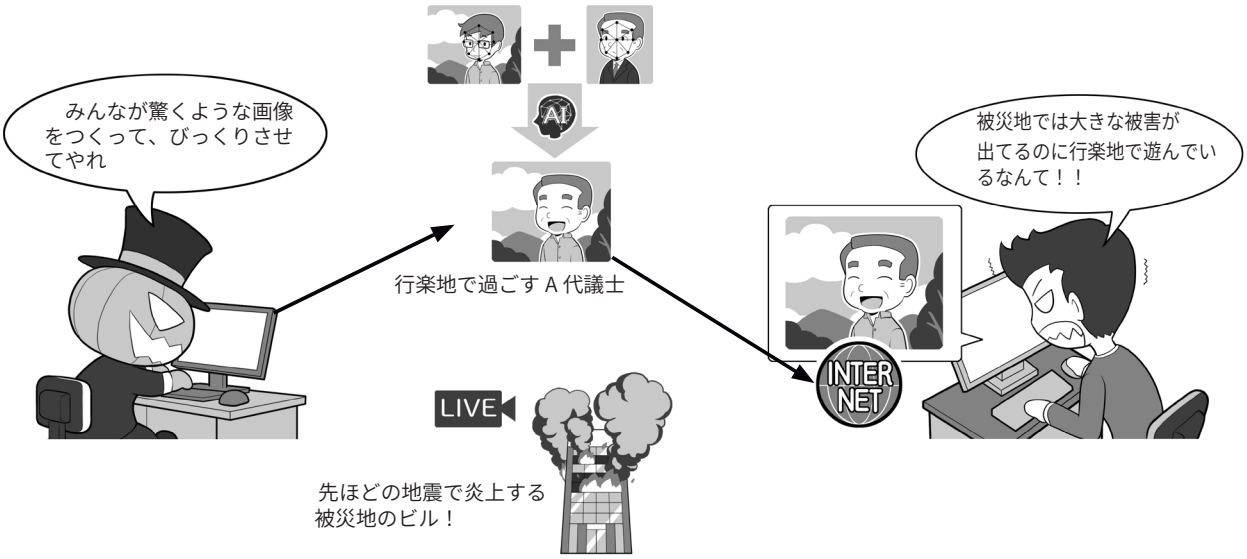


攻撃者とメーカーのゼロデイ攻撃に関する対応競争は、たいていの場合、攻撃者が先行します。攻撃者はメーカーが気付いていない段階でセキュリティホールの情報を入手し、対象の機種どれか1つでも攻撃に成功するなら攻撃を開始できますが、メーカーは情報を入手し精査した上でセキュリティパッチを開発し、攻撃可能と思われる機種すべてで、セキュリティパッチが正常に動作するか、充分な検証をしてからリリースしなければならないからです。

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.2　生成AIによるサイバー攻撃等への警戒や利用上の留意点

生成AIを用いたサイバー攻撃の高度化や一般化



以前の自動翻訳等では不自然さが残っていましたが、生成AIを用いることで、フィッシング詐欺のメールの文面と正規のメールの文面との間で見分けがつかないレベルになっています。また、精度の高い偽画像や動画が、簡単な指示で作成できるようになりました。

加えて、サイバー攻撃に使われるマルウェアなども、生成AIを用いることで、プログラミングの技術が乏しくても、作成できるようになってきていると言われています。

このように偽情報の作成の巧妙化や、サイバー攻撃の一般化が進んでいますので、インターネット上の過激な偽情報に騙されないよう注意したり、身に覚えがない、あるいは差出人が不明瞭なメール、SMSに対して、より警戒する必要があります。

2010年代からAIの活用が進められてきました。AIは大量のデータを機械学習▶用語集 P.181という手法によりモデルを構築し、このモデルに基づいて人が行う判断や処理などを高い精度で自動化するなどが期待されています。最近はさらに生成AI▶用語集 P.183の登場によりAIが身近になりました。生成AIはプログラミングなどしなくとも、簡単な日常の言葉を用いて、作成したり、処理してもらいたいことをAIに指示すると、AIでその意味をくみ取り、利用者の意に沿ったものを生成してくれます。例えば文章や画像、音楽、プログラムなどを生成してくれたり、表の作成などをしてくれたりします。

このように便利な生成AIですが、一方でサイバー攻撃にも利用されています。生成AIの文章も巧みになり、今では、偽メールや偽サイトを判別することが難しくなっています。さらには、海外では電話やウェブ会議で本人であることをなりすますために、生成AIにより音声や顔画像などを偽装し（ヴィッシング（ボイスフィッシング））、詐欺を行う事例も発生しています。

また攻撃に使うプログラム自体も、生成AIを用いて簡単に作ることができるようになっています。例えばランサムウェアの生成や、DDoS攻撃などを一種のクラウドサービスとして提供しているサイトなどもあり、多くの知識を有しない人でも巧妙な攻撃者に変貌できてしまいます。攻撃のために行うパスワード解析、暗号化解析でもAIを用いることで速やかに行われるようになっています。

生成AIを用いて偽情報などを配布するようなケースも増えています。特にディープフェイクと呼ばれる手法を使って偽の画像や動画を生成して、ネット上で公開して騒ぎをおこすほか、認証情報を作り出して攻撃するようなケースもあります。例えば著名人や政治家が発言していない内容を発言しているような

動画の生成や、災害時に、起きていない被害の画像を生成して混乱させるなどが実際に起きています。

さらには、他人の著作物や肖像を用いた精巧な違法なコンテンツを、生成AIを用いて作成し、頒布する等のケースや、テロ行為等への応用（違法薬物や爆弾などの危険物の製造）するケースも生じています。

このようにサイバー攻撃や偽情報・違法コンテンツの流通に生成AIが用いられ、より巧妙化・高度化、また一般化する傾向にあります。ですので、例えばメールについては、添付ファイルや文中のURL▶用語集 P.178は送信元の確信が取れない場合にはクリックせずに、アプリストアから改めてアクセスするなど、基本に忠実な対応を行うことが一層重要となります。

なお、生成AIについては、コンテンツの生成や利用での活用する場合も留意が必要です。生成AIを利用すると、利用者の注文に応じて、文章や画像などを生成するほか、利用者が投入したコンテンツを、注文に応じて改変できます。しかし、生成AIが生み出す文章や画像は、生成AIがネット上から収集し、学習したものをベースにしているため、元の著作物の権利者が予定した使い方とは限らず、知らない間に権利侵害をしてしまっている可能性があります。また他人の著作物を加工するのに生成AIを用いる場合には、一種の改変をしているため、著作権者の著作者人格権を侵害することになる危険性があります。

生成AIを用いた不適切な利用例

ネット上の他人の著作物からＡＩを用いて、勝手に新たな著作物を作成することや、これをネット上に上げることは著作権法に違反する可能性があります。また映像に写る本人の承諾なしに、画像をＡＩで生成し、配布することは、本人の肖像権を侵害する可能性があります。

そこで生成AIを通じてコンテンツを利用する場合には、利用の仕方や公開方法などが他人の権利を侵害していないことを十分確認し、そのリスクを把握したうえで、自己責任の下で利用するということ意識して使いましょう。また総務省から「上手にネットと付き合おう！安心・安全なインターネット利用ガイド」の、特集ページで「生成AIはじめの一歩～生成AIの入門的な使い方と注意点～」、消費者庁から「AI利活用ハンドブック～生成AI編～」なども公表されているので、参考にしましょう。