第2章

サイバー攻撃にあうと、どうなるの？最新の攻撃の手口を知ろう

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

1 攻撃者にIT機器を乗っ取られるとこんなことが起こる

1 被害に遭わない、そして加害者的立場にならないために

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

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

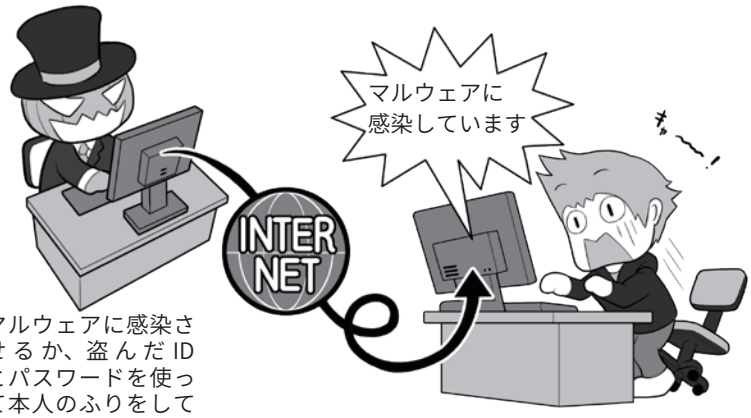
次に、別のパソコンやサーバなどに侵入するとき、「踏み台」にしてあなたのパソコンがやっているように見せかけたり、悪意のボットによるボットネットに接続させ、サイバー攻撃を行わせたりします。

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

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

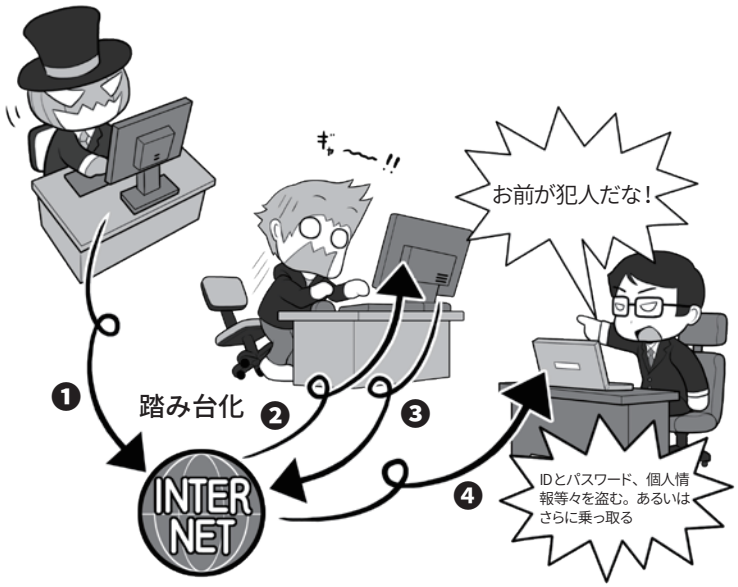
そうならないためにも、パソコンなどのシステムの状態は最新にし、セキュリティを固めましょう。もし、セキュリティソフトが、悪意のボットに感染していることを検出したら速やかに駆除します。一方、実害の出ている攻撃に関して、警察などから協力の依頼があった場合は証拠保全を行いましょう。

攻撃者によるパソコンなどの乗っ取り



攻撃者は、パソコンなどをマルウェアに感染させ乗っ取るほか、あなたのIDやパスワードがどこかから流出すると、それを入手して（あなたのふりをして）各種ウェブサービスやパソコンにログインを試みて、これを乗っ取ります。マルウェアであれば、セキュリティソフトで検出されるかもしれませんが、なんらかの正規の方法でログインされ、「本人」として遠隔操作用のマルウェアをインストールされると、その乗っ取りに気づくのは難しくなります。

乗っ取ったパソコンを踏み台にしてサイバー攻撃を行う



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

また、乗っ取りだけでなく、あなたのパソコンのメールソフトを使って、フィッシング詐欺のためのメールなどを送信する場合などもあります。

2 盗まれた情報は犯罪に使われる

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

例えば、銀行のインターネットバンキングから不正送金で、お金を勝手に盗み取るかもしれません。

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

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

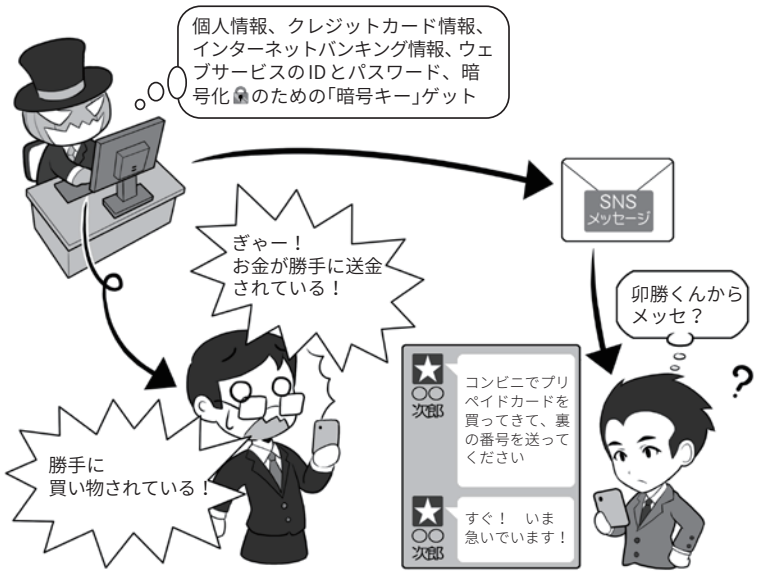
SNSのメッセージであなたになりすまし、友だちに対して「プリペイドカードを買って、アクティベーションコードを送ってくれ」と依頼し、電子マネーをだまし取る場合もあります。

自分が使っているパソコンなどのセキュリティをしっかり固めていても、情報を登録しているウェブサービスなどから、間接的に流出・盗難されることもあります。この場合でも同様に、攻撃者は盗んだ情報からなんらかの手段で、お金を手に入れようとします。

あなたに非がなくても流出は起こるのです。自分の環境のセキュリティを固めても、そのときは防ぎようがないので、不正利用などの兆候に気をつけてください。

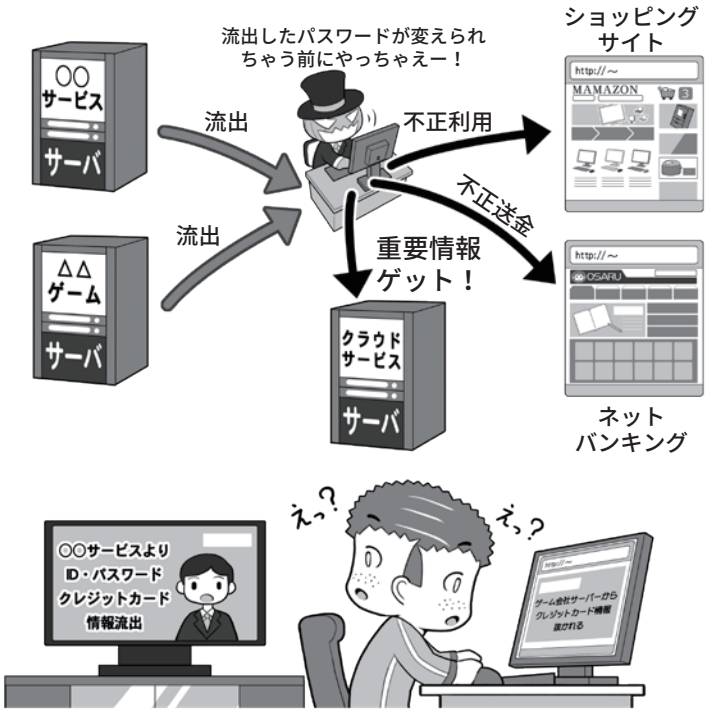
パスワード流出が判明したら、パスワード設定のセオリーにしたがいすぐに変更し、クレジットカード情報が流出したら、カード会社に連絡してカード番号を変更しましょう。

情報が直接盗難される場合



クレジットカード情報の流出などが起こった場合は、その被害は多岐におよびます。とりあえずカードが不正利用されていないかチェックします。パスワードの流出時は、各ウェブサービスのパスワードの変更を行いましょう。

情報が間接的に盗難される場合



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

3 乗っ取られたIT機器はサイバー攻撃に使われる

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

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

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

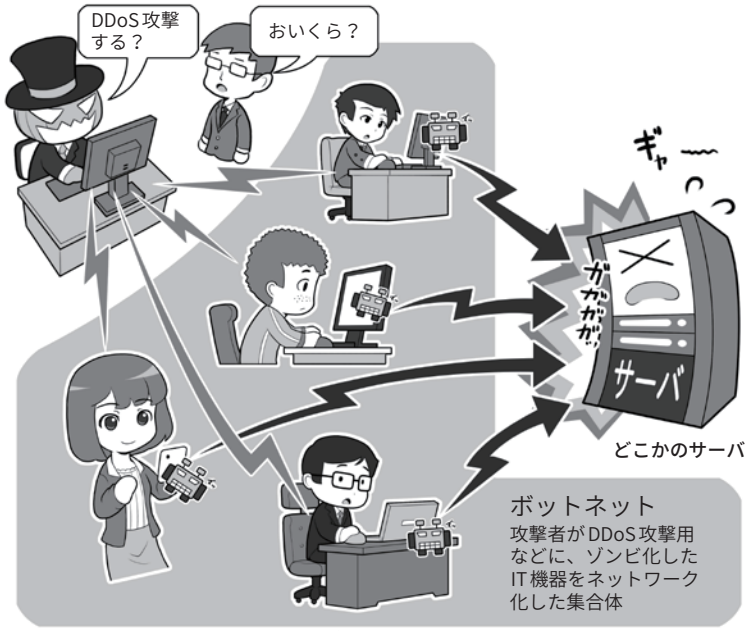
一方、「踏み台」的な攻撃はパソコンなどの乗っ取りによるものだけではありません。

「ウォードライビング」といって、車に乗って、会社や家の暗号化されていない、もしくは暗号化や暗号キーの設定の甘い無線LANアクセスポイントを探し、これに侵入する手法があります。

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

この場合、攻撃者に非があるのは当然ですが、自分の家からサイバー攻撃が行われ、インフラ企業などで事故が発生したら心中穏やかではありません。セキュリティを固めて侵入されないようにしましょう。

乗っ取られたIT機器はボットネットとして貸し出される

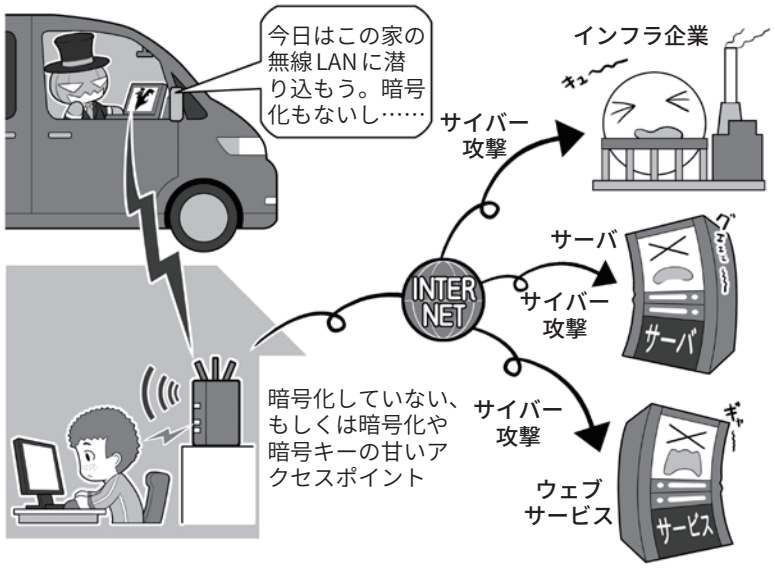


攻撃者によって、悪意のボットに感染させられ、遠隔操作されたパソコン(ゾンビPC)などの集合体がボットネットです。

攻撃者の命令で、一斉に特定のサーバなどにDDoS攻撃をしかけ、ダウンさせたり反応不能に陥れたりします。

ダークウェブ(P120)で時間あたりいくらで貸し出されることもあります。

無線LANに侵入され罪を押しつけられることも



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

4 IoT機器も乗っ取られる。知らずにマルウェアの拡散も…

攻撃者によって乗っ取られるのは、パソコンやスマホだけではありません。IoT機器と呼ばれるネットにつながる電子機器はいずれも、乗っ取られて攻撃の身代わりとなる「踏み台」、DDoS攻撃用のボットネットへの接続、マルウェアの拡散など、様々なサイバー攻撃に利用される可能性があります。

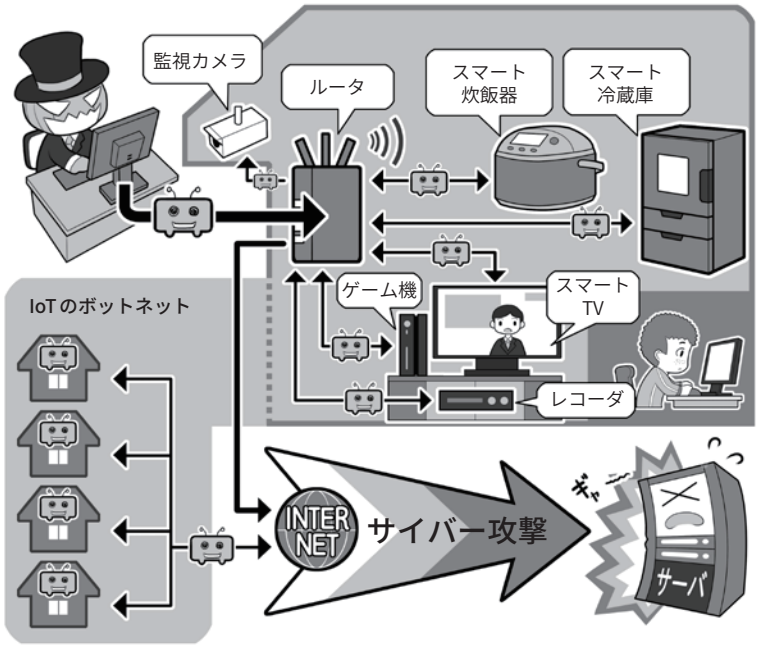
特に、IoT機器は監視カメラやスマート家電などのように、普段私たちがあまりセキュリティについて気にかけることがない機器であり、パソコンほどサイバー攻撃への対応能力が高くありません。そして、一つの機種で台数が多い＝手間をかけずに多数を攻撃できる、攻撃者にとって「攻撃しやすい条件」が揃っているのです。

最低でも、出荷時の「初期パスワード」はパスワード設定のセオリーにしたがって変更し、システムは最新に保ち、ネットにつなぐ必要がないものはむやみに接続しないようにしましょう。

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

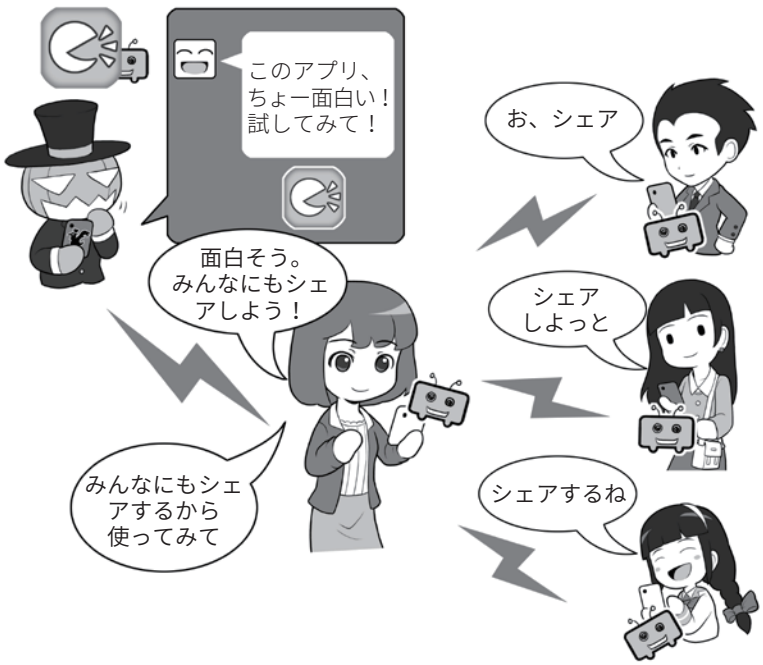
ネットでなにか行動する前には、必ず「それは本当に必要なのか」「なにか問題が発生する可能性はないのか」をいつも注意しましょう。

IoT機器も乗っ取られ攻撃に使われる



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

知らずにマルウェアの拡散に協力しているかも……



SNSで見た「面白い投稿」や「拡散希望の投稿」を、深く考えないで拡散すると、その投稿の先にはフィッシングサイトが用意されていたり、ゼロデイ攻撃のマルウェアが仕込まれていたり、アプリであればマルウェアが入ったものだったりするかもしれません。拡散する前に、よく考えて「シェアする必要がないものはシェアをしない」ようにしましょう。そうしないと、あなたが被害者ではなく、サイバー攻撃やマルウェアの拡散者になってしまうかもしれません。

コラム：大きな脅威となっているランサムウェア

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

企業のパソコンやサーバがランサムウェアに感染し、ビジネスに大きな支障が生じる事件が多発しています。

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

特に、イギリスでは国民に保険サービスを提供するいくつかの団体で端末が利用できなくなり、医療機関においても診療ができなくなったり、予定されていた手術ができなくなった事例もありました。

また、ある大手自動車メーカーでは、工場内の端末がWannaCryの亜種に感染し、生産が一時止まるといった影響が出ていました。

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いケースも多発しています。ランサムウェアのふりをしてデータを破壊することが目的と思われるものもあります。

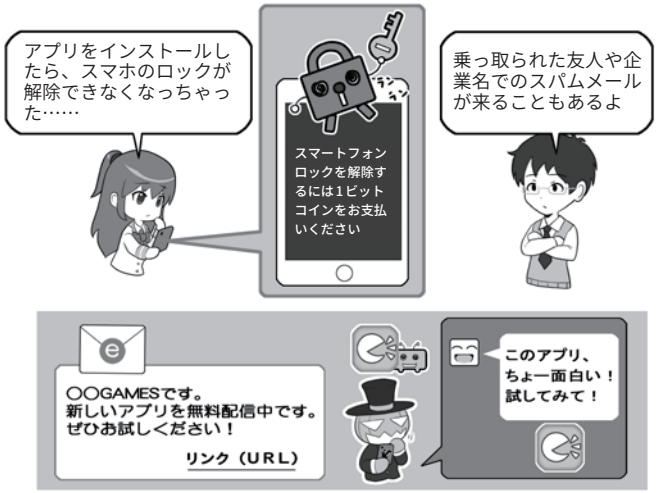
最近では、個人のスマホを狙ったランサムウェアも登場しています。最悪の場合は端末を初期化しなければならず、大切なデータが失われることにもなりかねません。

こういった事態を避けるため、システムやアプリは最新の状態を保ち、不審なメールのリンクをクリックしたり、あやしいウェブサイトからソフトやアプリをインストールしたりしないこと。データを常にバックアップし、必要に応じてセキュリティソフトを利用するといった対策をしっかり実施しましょう。

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。

不審なアプリのインストール要求に注意



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

コラム：仮想通貨の現在地1

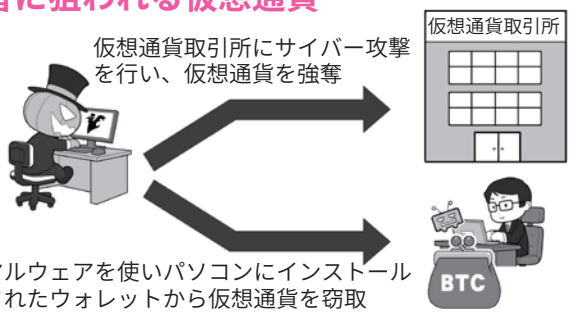
ビットコインなどの仮想通貨が広く流通しつつあります。投資などの面でも仮想通貨が現実世界での投資対象として使われ普及しつつあります。

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

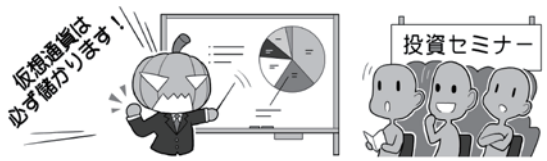
実際、仮想通貨は現実通貨に対する価値が乱高下することがあり、一般的な投資対象と比較してリスクが大きいようです。そして、まるで西部劇の世界のように、サイバー攻撃により仮想通貨を預かる取引所からの大規模な盗難や、個人のお財布(ウォレットという)から仮想通貨が盗まれるケースも頻発しています。

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

犯罪者に狙われる仮想通貨



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



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

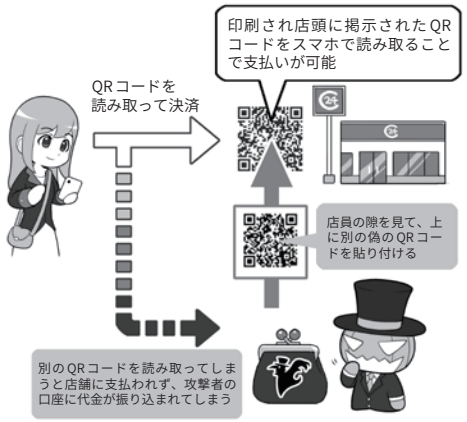
コラム：QRコード決済サービスで生まれた新たな詐欺

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

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

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

QRコード決済の詐欺の流れ



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

コラム：仮想通貨の現在地2

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

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

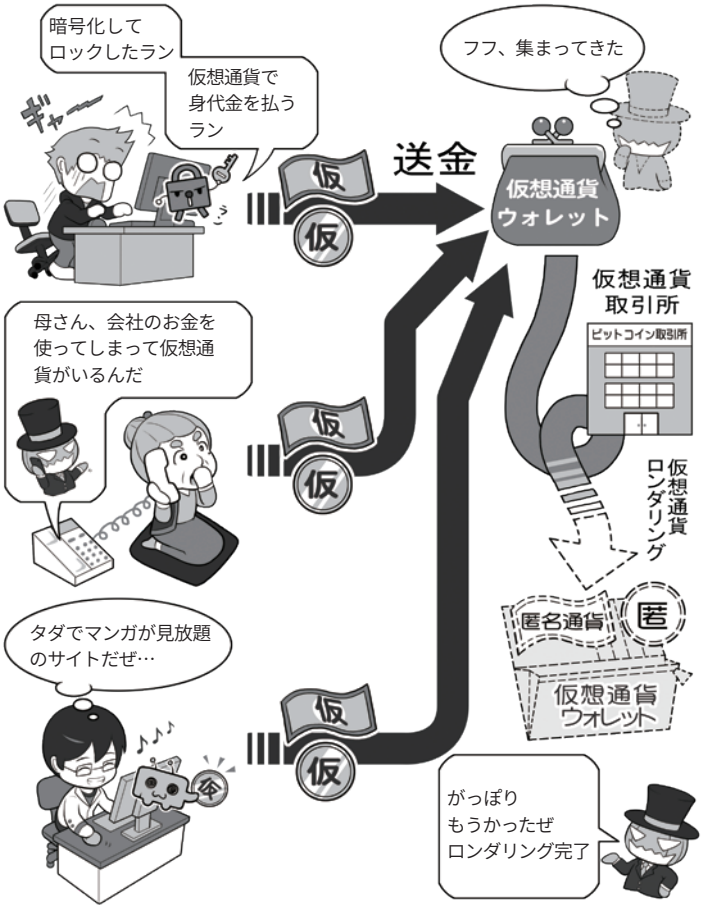
仮想通貨で要求する理由は、仮想通貨が全般的に「匿名性」が高く、不正に入手したり奪取したりしても、その後の追跡が困難だからです。また、一般に知られているビットコインなどの仮想通貨で受け取ったあと、支払先をばらばらに分散して追跡し難くし、その上で極めて匿名性の高い仮想通貨に換金（ロンダリング）して、追跡を逃れるなどの手法もあります。

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

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

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

著名な仮想通貨を匿名性の高い通貨にロンダリングして逃げる



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

コラム：フェイクニュースとサイバープロパガンダ

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

悪意を持った者が、なんらかの意図を持って、ネット上で偽のニュースを発信するもので、これが拡散され始めるとニュースサイトなどでも真贋不明のまま取り上げられ拡散され、結果的に見た人はそれを真実だと思ってしまうといったことが起きています。

フェイクニュースには、意図を持って発信している人のほかに、人々が注目するニュースをねつ造することで自分のウェブサイトの閲覧数を増やし、掲載した広告の収入でお金を稼ぐ商売としている人もいて、1つの悪意のビジネスモデルになりつつあります。

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

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

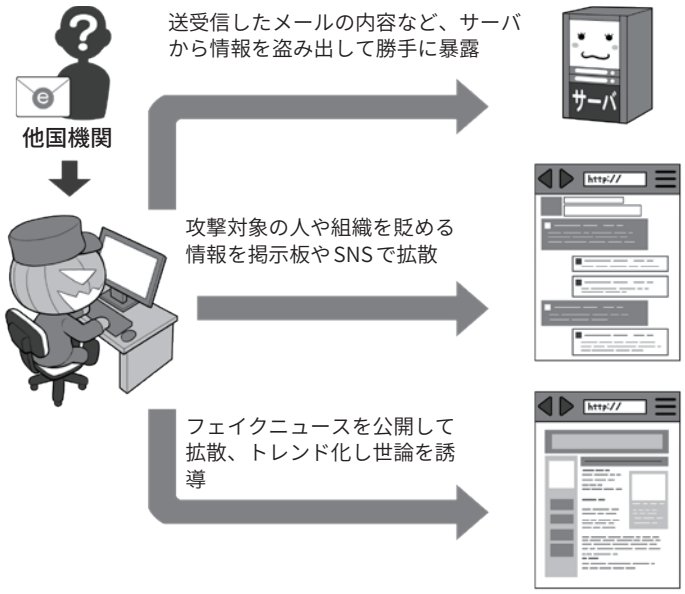
プロパガンダ自体は、古くから国家が自国や他国に対して影響を及ぼすために、行われてきた「人を思いどおりに動かそうとする情報の悪用法」ですが、これがネットを使うことで高度化かつ秘密裏になり、人々が気付かぬ間に、その考え方が操作される事態が起きているのです。

これを行うため、サイバー攻撃によって盗んだ政治家のメールを改ざんした上での暴露、国と密接な関係にあるメディアでの偽ニュースの発信、ボットを使ったSNSでの偽ニュースのトレンド化、政治的な争点になっている事柄の賛否両方にSNS上で広告を打つことで混乱を生み出し国民を分断、そして、SNS上で架空の人格のアカウントを作りインフルエンサー(有名人)に成長させ、他国の人々を自国に有利になるように扇動するなどといった、様々な手法を総動員してサイバープロパガンダが行われているのです。

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

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

サイバープロパガンダが行われた例(米国)



サイバープロパガンダでは、フェイクニュースや盗んだ情報のリークを種として、トロールと呼ばれる情報操作グループと「いいね」や「シェア」を押す自動のボットによりこれをトレンドにのせ、さらに、ターゲットの国の「自分にマッチした情報を好んでシェアする」人たちのSNS集団(エコーチャンバー)にこれを投げ込み、最終的にそのほか大勢に、さも「重要なニュースである」というイメージを与え、世論を操作します。

コラム：軍事スパイ、産業スパイに狙われてしまったら

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

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

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

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

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

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

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

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