# インターネットの
# 安全・安心ハンドブック

NISC 内閣サイバーセキュリティセンター
National center of Incident readiness and Strategy for Cybersecurity

知る・守る・続ける
サイバーセキュリティ普及啓発

ネットワークビギナーのための
情報セキュリティハンドブック Ver 4.03

# インターネットの
# 安全・安心ハンドブック



サイバーセキュリティ普及啓発

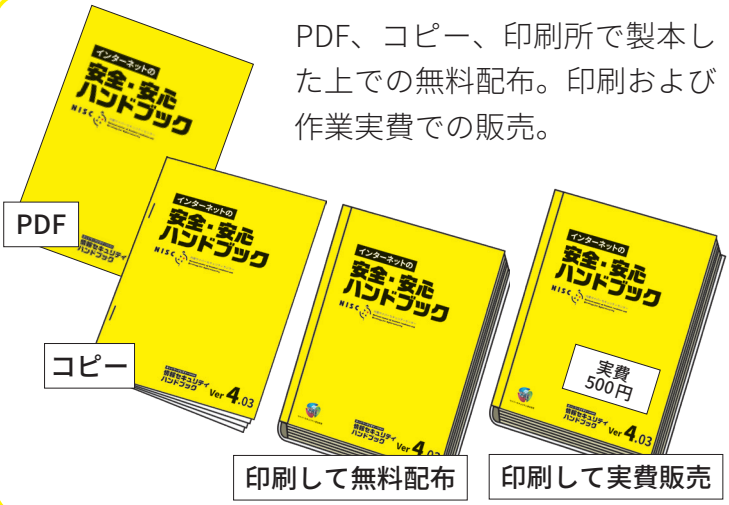
ネットワークビギナーのための
情報セキュリティハンドブック Ver 4.03

NISC 内閣サイバーセキュリティセンター
National center of Incident readiness and Strategy for Cybersecurity


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

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

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



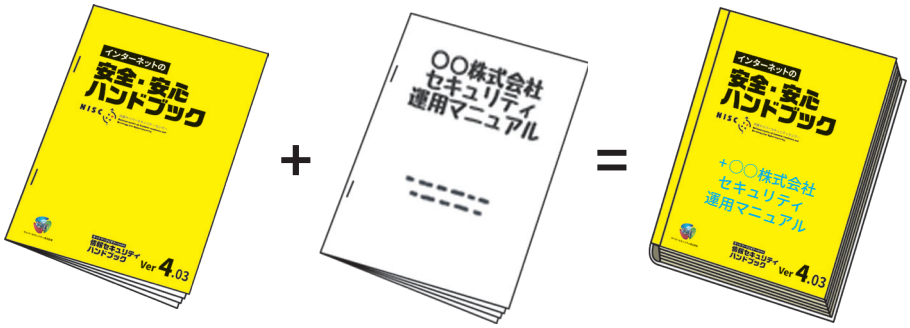

PDF、コピー、印刷所で製本した上での無料配布。印刷および作業実費での販売。

ページ単位、イラスト単位での利用、配布(ネット配布含む)


分割して配布、必要部分だけを抜粋して配布


ウェブサイトにダウンロードサイトのリンクを設置※


使用する団体名を表紙に入れて利用




自団体のセキュリティ資料と合体しての配布

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

# インターネットの安全・安心ハンドブック　活用法

## ● 学校の授業で

「インターネットの安全・安心ハンドブック」では、まず、中高生の方とその先生方に、この本を、セキュリティ意識を高めるための教材として使っていただきたいと思います。

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

## ● ご家庭で

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

また、第5章では、子ども達がSNSを気軽に利用すると、どういうったトラブルが発生するのか、SNSをとおして見知らぬ人と友だちになると、どういったことが起こるのか触れていますので、ご家族で一緒になって確認し合ってください。

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

## ● 災害時に備えて

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

### 学校の授業で

P21「第1章．基本のセキュリティ～ステップバイステップでセキュリティを固めよう~」


P41「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」


P51「第3章．パスワード・Wi-Fi・ウェブ・メールのセキュリティを理解して、インターネットを安全に使おう」


P107「第5章．SNSやインターネット関連の犯罪やトラブルから、自分や家族を守ろう。災害に備えよう」


### ご家庭で

P108「5-1-1 SNSやネットの楽しみと気をつけること」


P118「5-2-1 アニメ・マンガ・音楽の違法なシェア。パクリなどの著作権侵害」


### 災害時に備えて

P132「5-3-4. 大災害やテロに備える」


P135「5-5-4. 徒歩帰宅。海外での災害やテロに備えて」

# 目次

**※ご注意**

本書では、初心者の方にサイバーセキュリティ関連の問題を理解してもらうために、実際のケースと比較してわかりやすく簡略化したり、内容を理解しやすいように関連する事項の一部を省略したりして記述している場合があります。ご了承ください。

このハンドブックを読んで、よりサイバーセキュリティに関する理解を深めていきたいと思う方は、ぜひステップアップして、様々な専門誌や最新の記事にチャレンジしていただけると幸いです。

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

# はじめに～サイバーセキュリティは「公衆衛生」の時代に～

みなさん、はじめまして。私たちは内閣サイバーセキュリティセンター(NISC)です。日本の政府機関で国のサイバーセキュリティ政策を担当しています。

突然ですが、「ウイルス」という言葉をご存じですか？病気の原因としてのウイルスを思い浮かべましたか？それとも「コンピュータウイルス」？

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

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


※NISC特務第１チームは架空の団体です。

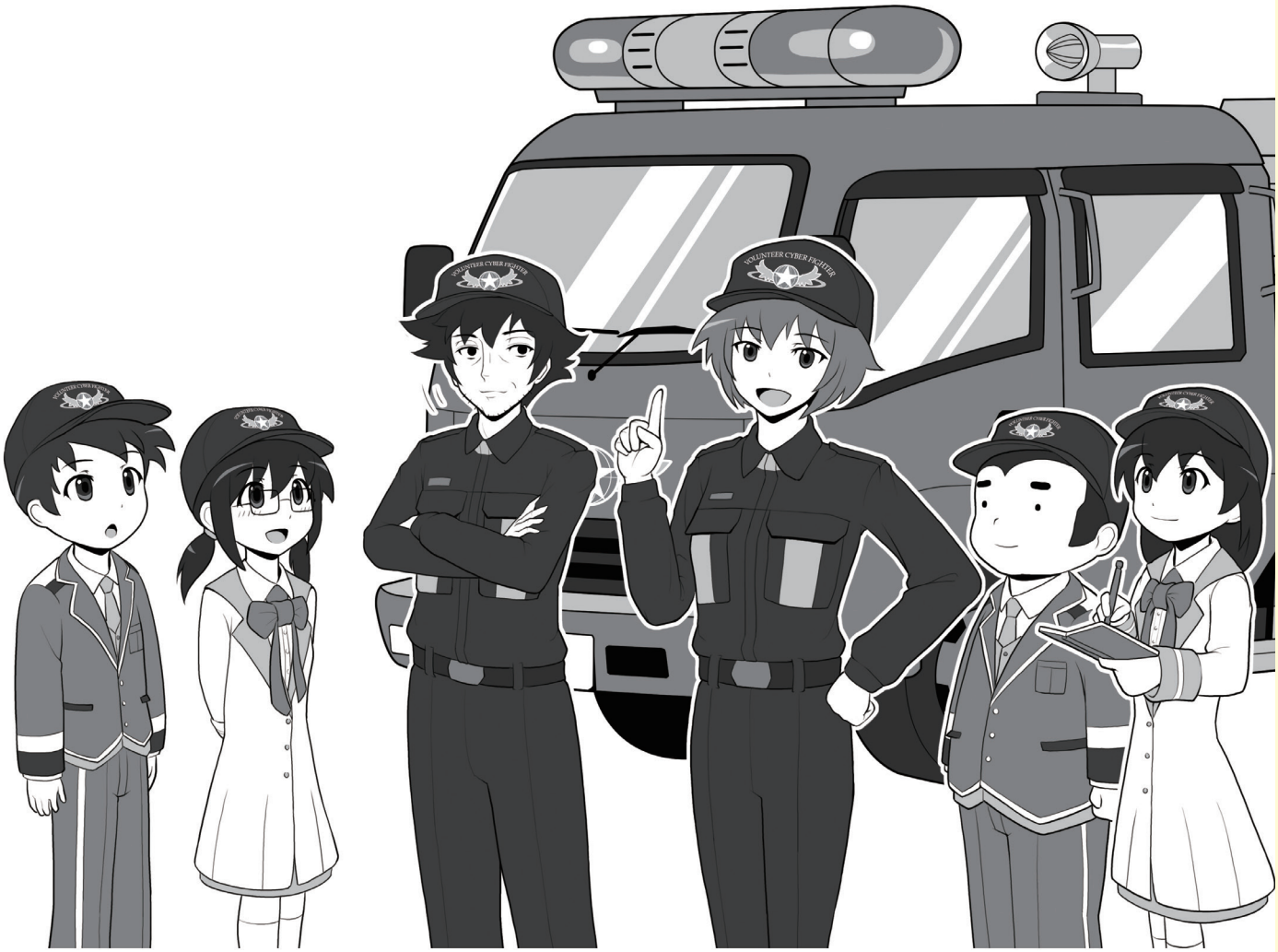
今、日本の街角が綺麗で、病気による大災害が発生しないのも、国民全員が長年取り組んだ「公衆衛生」意識と活動の賜物なのです。

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

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

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

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




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

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

# Black Hat the Cracker

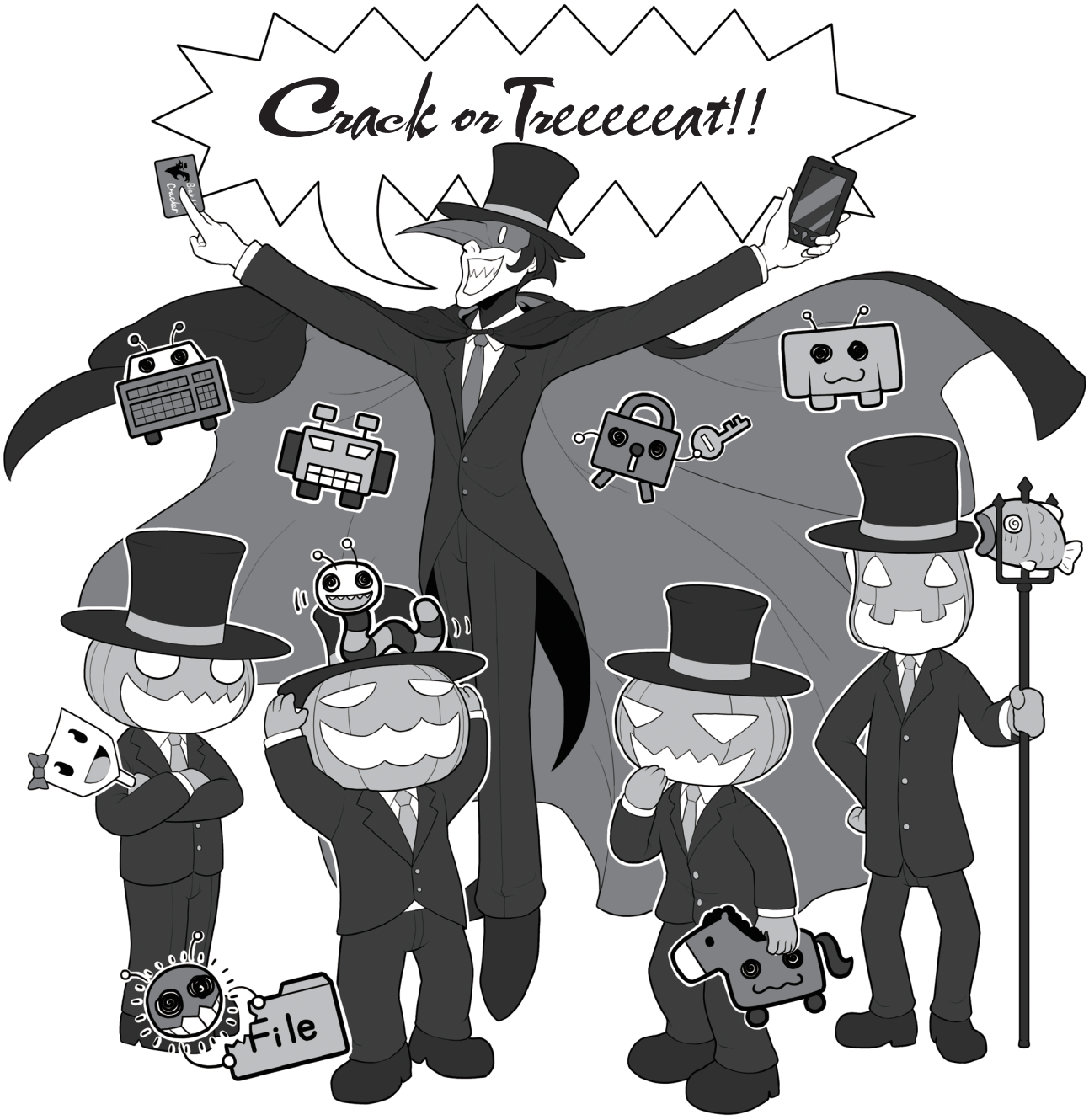
サイバー空間(インターネット)には、悪意をもってこれを利用し、自らの利益のためには平気で他人の情報や財産を奪い、また、サイバー攻撃を通じて自己誇示するといった、様々な悪事を働く者がいます。

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

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

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

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



# プロローグ

# サイバー攻撃ってなに？

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

## 悪意を持った人たちは、いったいなにを狙っているの？

# 1 サイバー攻撃のイメージ

## 1 サイバー攻撃って誰がやっているの？どうするの？


サイバー攻撃は、誰がなんの目的でやっているのでしょう。

軍事スパイや産業スパイ？ それともハッカー？

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

スパイは、目標の達成が絶対条件なので、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を試みます。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持っています。例えば、「ここはセキュリティがしっかりしているので手間がかかる(≒費用がかかる)のでやめよう」「ここなら手間がかからない(≒安くすむ)からここから盗もう」というように、攻撃しやすい方に流れる傾向があり、セキュリティレベルを高めることで、ある程度攻撃を受けにくくすることができるのです。完璧に防ぐことは難しくても、努力をすれば被害に遭う確率を減らせると考えていいでしょう。

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

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

## コラム：攻撃者とハッカーとクラッカー

### ハッカー


そもそも、「ハッカー」とはコンピュータの知識と技術に精通した人を尊敬して呼ぶ名前で、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。

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

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

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

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

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

# コラム：攻撃者が使う武器「マルウェア」

## ● どんな種類があるの？

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

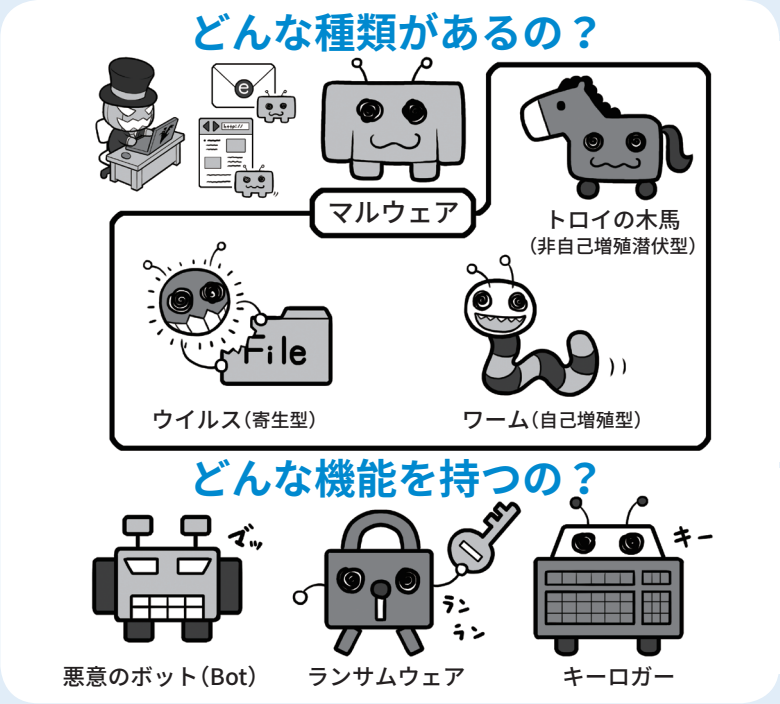
攻撃者がサイバー攻撃を行う場合、相手のコンピュータをなんらかの悪意のプログラムに感染させ、これをコントロールする方法がよく用いられます。この攻撃に使われるプログラムをまとめて「ウイルス」と呼びがちです。

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

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

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

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




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

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

## ● どのような機能を持つものがあるの？

マルウェアを機能別に分けると、このようなものがあります。

- **悪意のボット（Bot）**

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

- **ランサムウェア**

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

- **キーロガー**

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

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

ですね。

### ● どんなものが感染したり、感染させたり、悪さをするようになるの？

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

そして「マルウェアはコンピュータが感染する悪意のプログラム」です。

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

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

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

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

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

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

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

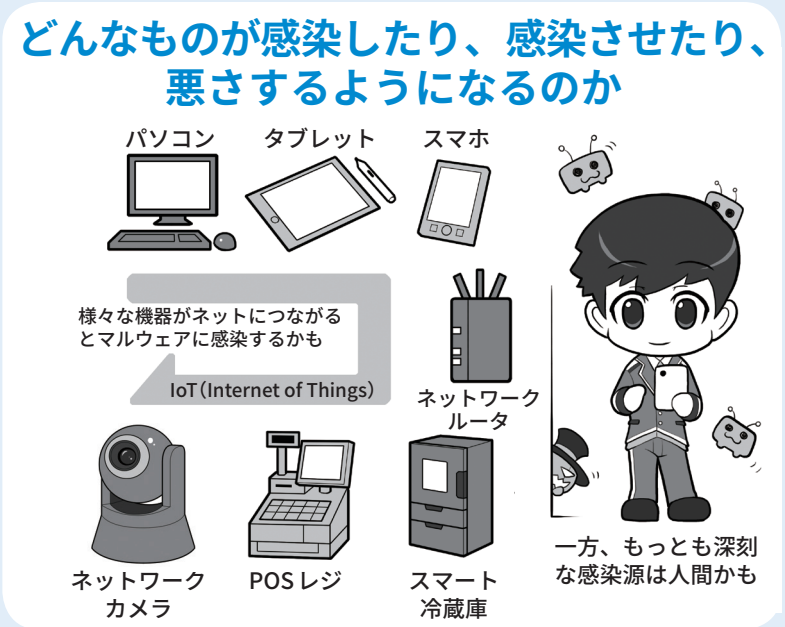
これを実現するのが後ほど説明する「標的型(電子)メール」など、心の隙を突くタイプの攻撃です。問題はこの心の隙が、コンピュータのセキュリティホールのように簡単にはふさげないことにあります。セキュリティ意識は、本人が必要性を認識しないと向上しないからです。

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

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

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

まずは、防ぐための知識を得て行動をおこしましょう。



## 2 サイバー攻撃の例

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

攻撃者はマルウェアを添付した電子メール(以下メール)をあなたに送ったり、マルウェアを仕込んだウェブサイト(ホームページ)に誘導したりして、あなたのパソコンなどをマルウェアに感染させます。そして、画像や重要情報を気づかれないように盗ませたり、盗んだIDとパスワードで勝手に物を購入し、換金したりもします。

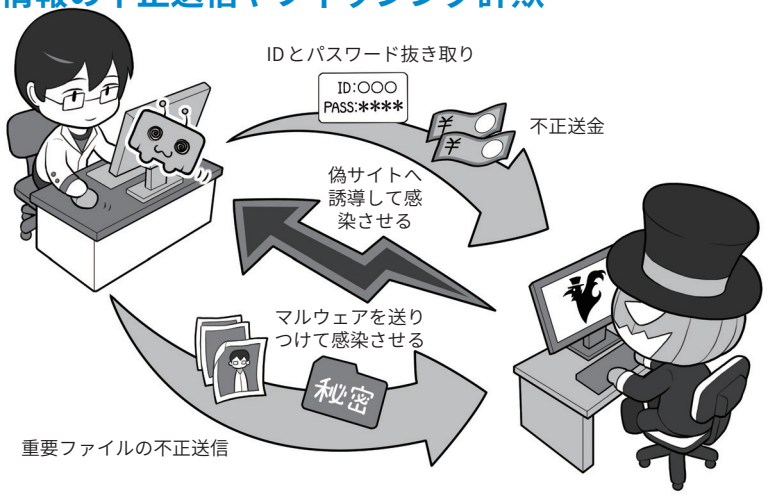
また、メールやSMS(ショートメッセージ)で偽の銀行サイトに誘導し、お金を不正送金させる、「フィッシング詐欺」などを行うこともあります。

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

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

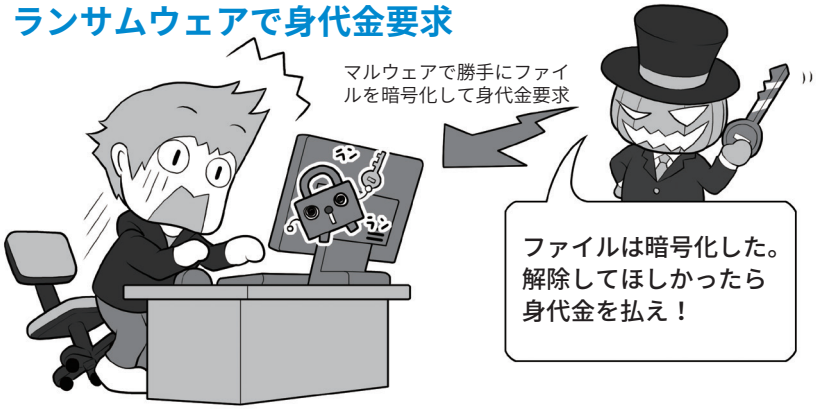
攻撃者はこの攻撃用の不正な仕組みを時間制で貸し出して、対価としてお金を稼ぐこともあります。

### 情報の不正送信やフィッシング詐欺



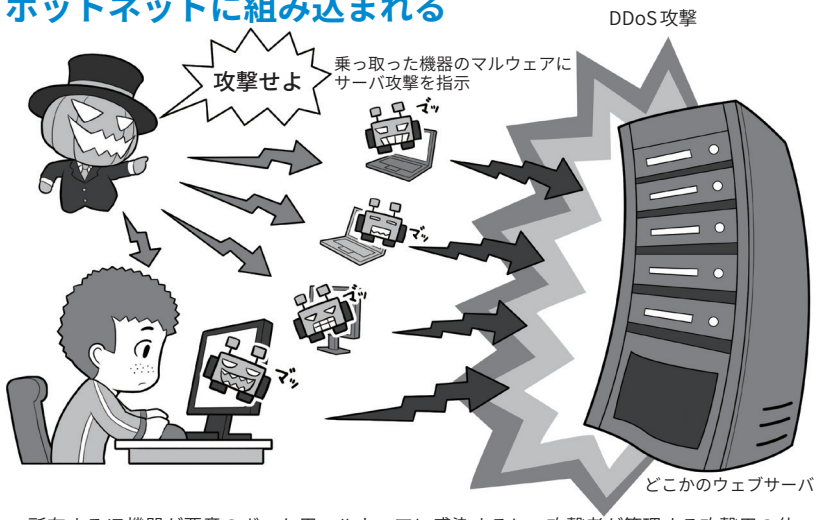

攻撃者は、あなたから重要情報やお金を盗むために、マルウェアに感染させて重要ファイルを不正に送信させたり、偽のメールで偽の銀行サイトなどに誘導する「フィッシング詐欺」を行って不正送金させたりします。どういう方法でだまされてしまうのか、一度調べてみましょう。

### ランサムウェアで身代金要求




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

### ボットネットに組み込まれる




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

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

# 3 サイバー関連の犯罪やトラブル

サイバー攻撃のほかにも、ネットを使った犯罪やトラブルはたくさんあります。

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

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

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

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

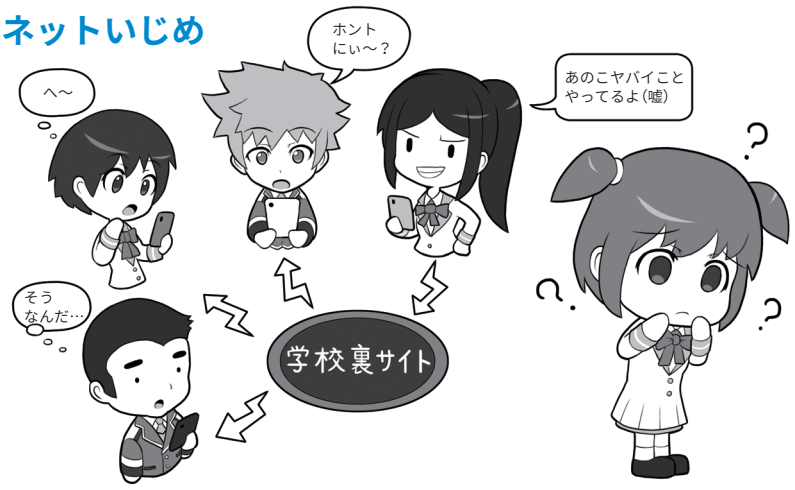
## なりすましや誘拐・略取(連れ去り)


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

## 自画撮り被害(セクスティング)


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

## ネットいじめ




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

# 4 一見サイバー攻撃に見えない「ソーシャルエンジニアリング」攻撃

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

関係機関が常に注意喚起をしていますが、未だに多くの方が被害に遭っています。

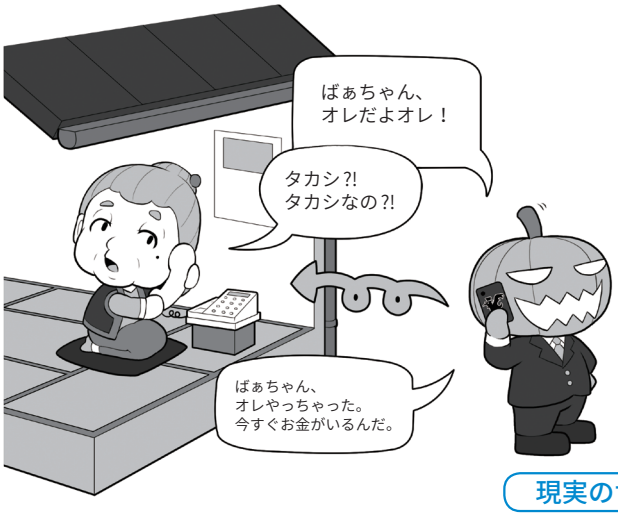
パソコンに例えると、セキュリティホールを必死に埋めようとしているのになかなか埋まらず、目の前で次々とサイバー攻撃が行われてしまっているような状況です。

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

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

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

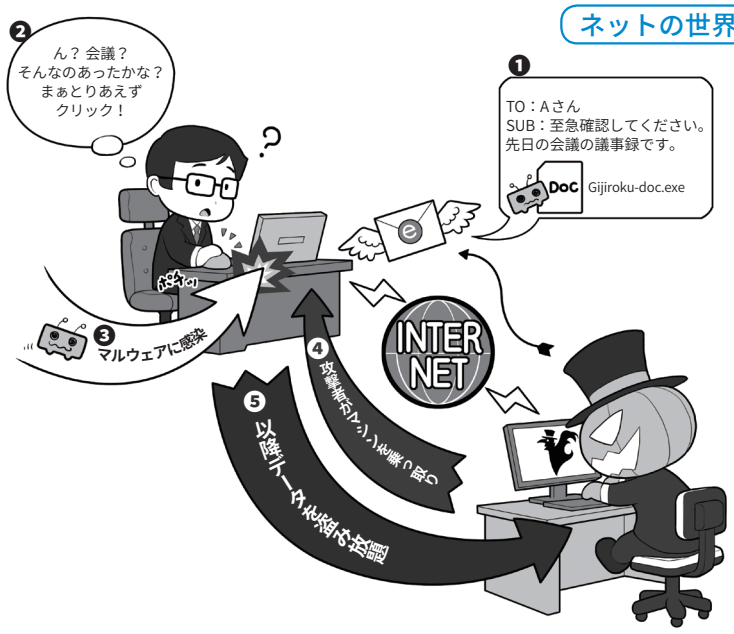
## 「ソーシャルエンジニアリング」は現実でもネットでも「心の隙」を突いてだます




現実の世界

この2つの共通点は人間の「心の隙」を突いた点

ネットの世界




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

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「フレンドシップ」という手法に当てはまります。

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

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