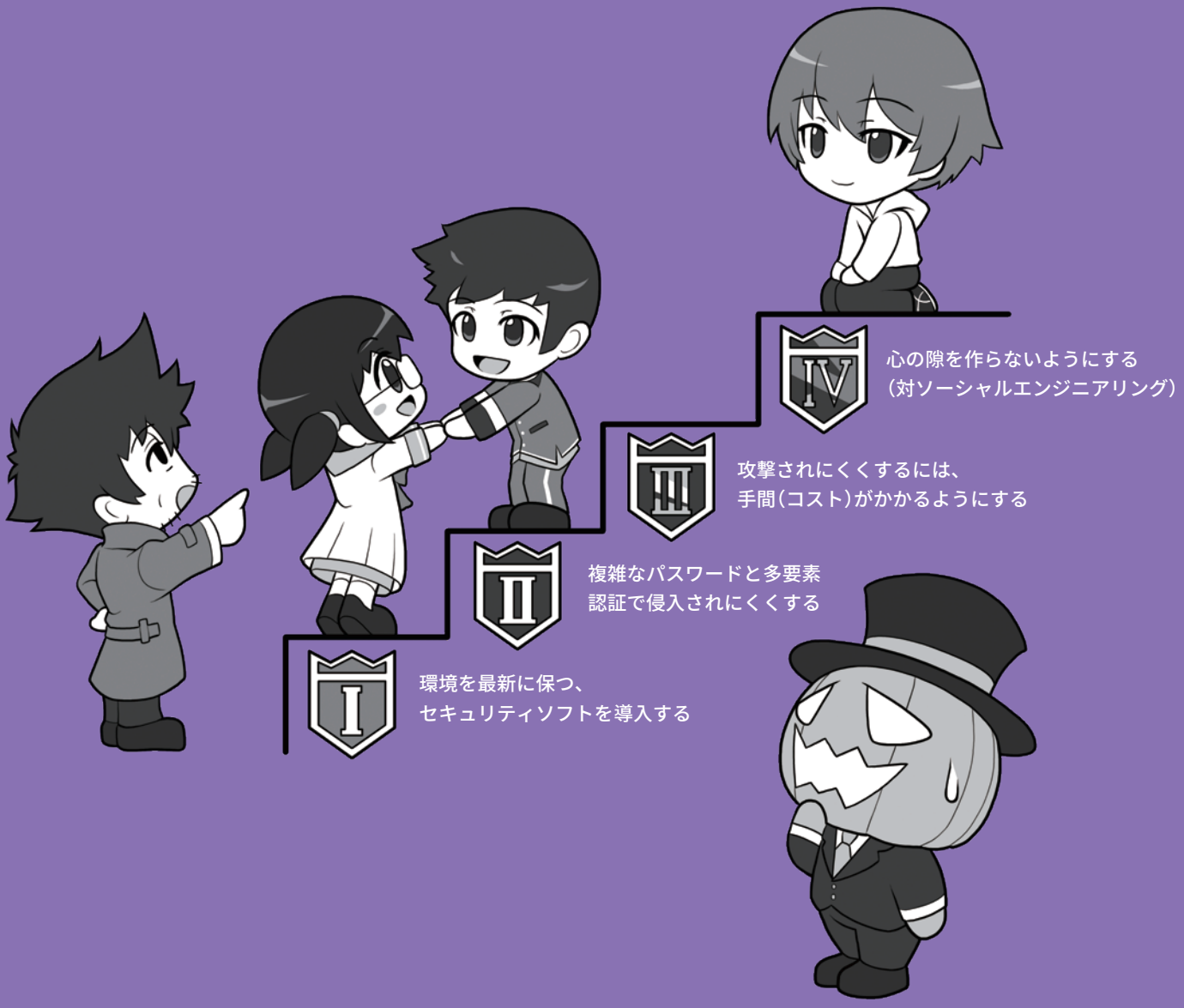
第1章

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～

サイバー攻撃を受けにくくするための、簡単なセキュリティの固め方を理解しましょう。
また、パスワードの管理の仕方や、攻撃する側が攻撃したくなくなるにはどうすればいいかを学びましょう。
人間の心の隙を突く、ソーシャルエンジニアリング攻撃などについても勉強しましょう。



1 4つのポイントで セキュリティを守る

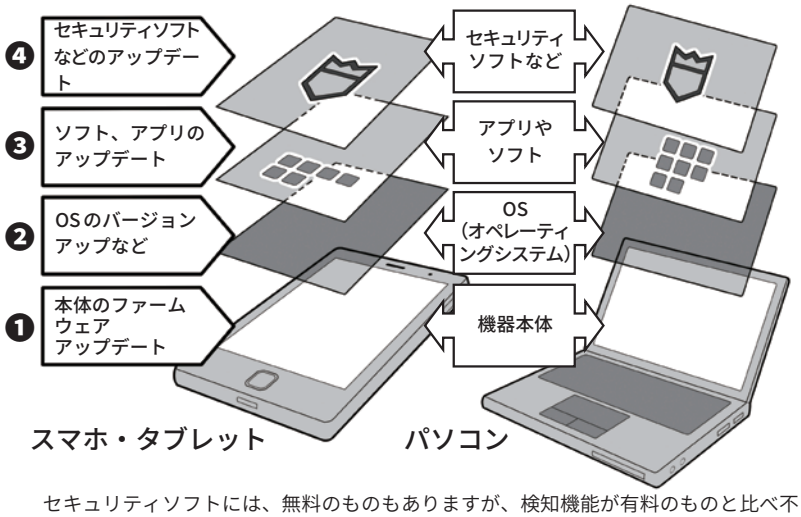
1 システムを最新に保つ。セキュリティソフトを入れて防ぐ

サイバー攻撃を防ぐための第一歩は、パソコンやスマホのシステムを最新の状態に保つことです。

①に機器の本体の「ファームウェアのアップデート」。②に、私たちが操作するインターフェースを提供している「オペレーティングシステム（以下OS）のバージョンアップやアップデート」。③に、セキュリティホールになりやすい「ソフトやアプリのアップデート」を行います。

パソコンの場合、それに加えマルウェア検出などを行う④「セキュリティソフトの導入とアップデート」です。なお、スマホの場合、導入は必要性に応じてなので、P26を参照してください。これらを常時更新して　セキュリティ上の穴をふさぎます。

様々な段階でセキュリティを守る



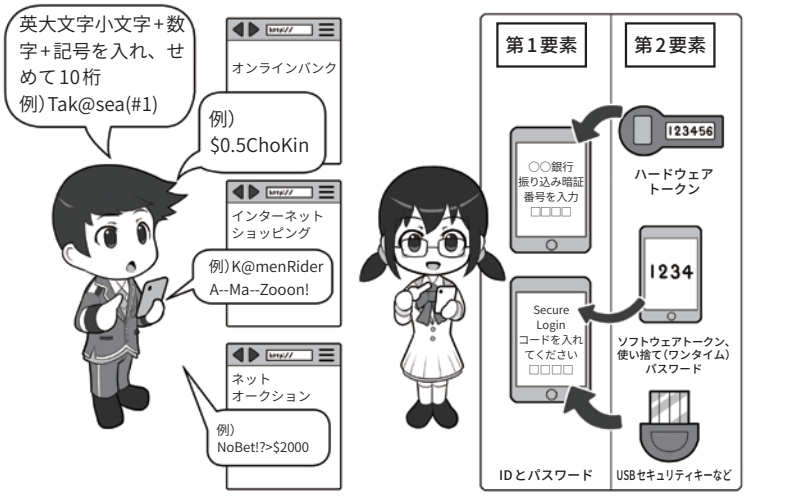
セキュリティソフトには、無料のものもありますが、検知機能が有料のものと比べ不十分なものや、セキュリティソフトを名乗りながら、実はマルウェアのような挙動をするものもあるので注意してください。どれを導入するか迷った場合は、プロバイダなどが提供するセキュリティパックか、信頼できるメーカーのソフトを導入しましょう。多少のコストがかかってもセキュリティ向上は安全への投資なのです。

2 複雑なパスワードと多要素認証で侵入されにくくする

次に、サイバー攻撃で的になりやすいのはパスワードです。攻撃者がこれを入手するには「見つけ出す」のと「盗む」攻撃方法があります。まず簡単にやられないように、購入時に設定されていたパスワードは必ず変更し、複雑なパスワードをウェブサービスや機器ごとに別々に設定しましょう。設定したパスワードを盗まれないように保管することも重要です。

続いて、仮にパスワードを盗まれてもサービスや機器が乗っ取られないように、多要素認証などさらなる防御手段を追加しましょう。

複雑なパスワードや多要素認証でセキュリティを守る



ウェブサービスや機器間で、使い回しのない英大文字小文字・数字・記号が入った複雑なパスワードを使う

使い捨てパスワードや多要素認証の導入、ネットに流出しない現物としてのセキュリティキーなどを利用する

3 攻撃されにくくするには侵入に手間(コスト)がかかるようにする

サイバー攻撃を行う攻撃者は、プロフェッショナルであるスパイを除けば、ビジネスとしての効率が重要なので、より手軽に侵入できる対象を選ぶ傾向にあります。

警備や戸締まりがしっかりしている場所に泥棒が入らず、鍵がかかっていない留守の家に空き巣が入るのは、その方が危険性(コスト)が低く手軽だからです。

サイバー攻撃でも同じように、侵入するまでに幾重にも防御がしてあると、攻撃者にとっては手間(コスト)がかかって面倒な、あるいはそもそも侵入できない対象となり、攻撃されにくくなります。

そのためには、システムを最新の状態に保ちセキュリティホールをふさぎ、セキュリティソフトを導入し、複雑なパスワードや多要素認証が必要になるわけです。

守りを何重にもして侵入されにくくする

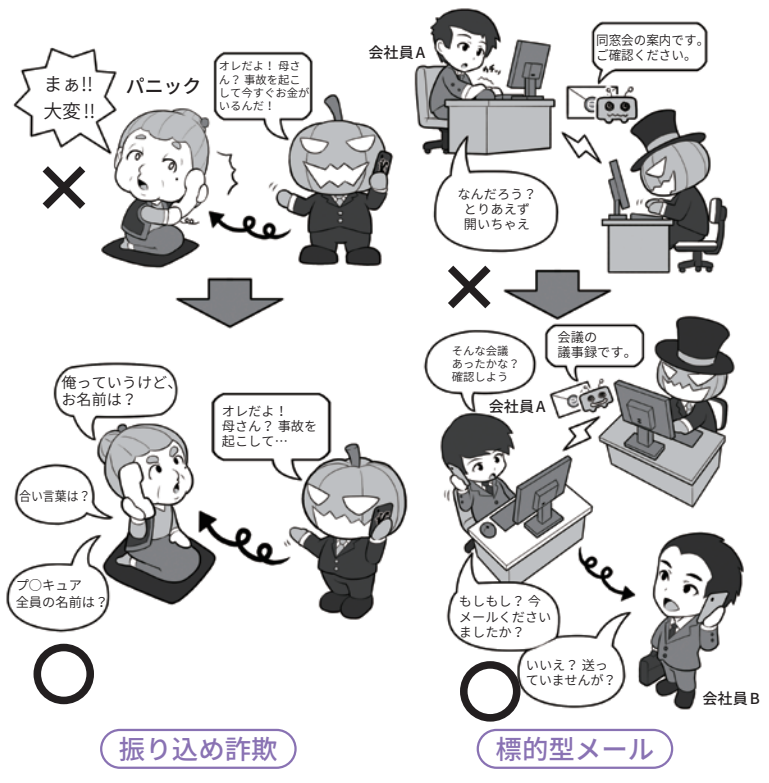
4 心の隙を作らないようにする(対ソーシャルエンジニアリング)

しかし、それでも、ソーシャルエンジニアリングという、人間の心の隙を突く攻撃を受けて攻撃者に操られ、家の鍵を中から開けるような状況になってしまうことがあります。それを防がなければ、いくらシステムのセキュリティを高めても意味がありません。システム面と心理面の防御は車の両輪なのです。

振り込め詐欺のあやしい電話なら合い言葉で防御する。あやしい電子メールやメッセージを使った標的型のサイバー攻撃なら、疑わしい通信手段とは別の通信手段で送信者に情報を確認するなどの対処法があります。

これは、項目の2にもあった多要素認証と同じ考え方で、攻撃を防ぐシンプルかつ有効な手段です。

心の隙を作らない。攻撃をうけつけない



2 環境を最新に保つ、セキュリティソフトを導入する

1 セキュリティソフトを導入して守りを固めよう

単純なウイルス対策ソフトがマルウェアを見つける方法は、おもに「手配書」方式になっています。

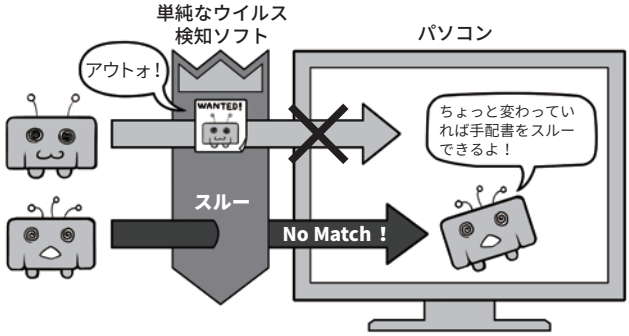
手配書方式とは、あらかじめ検出したいマルウェアの特徴を、対策ソフト開発社からそれぞれのパソコンなどに送信しておき、マッチしたものを駆除する方式です。

しかし、現在では攻撃者が、発送先ごとに送りつけるマルウェアを微妙に変えたり、狙いを定めて専用に作っ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難しくなりつつあります。

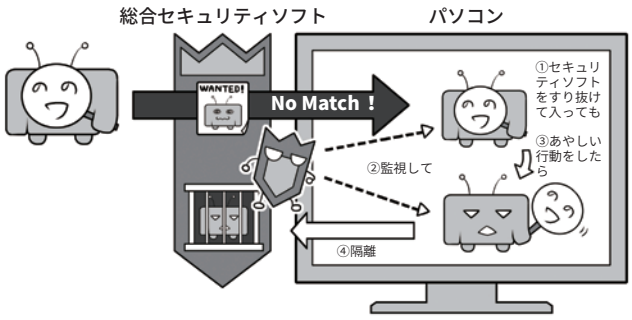
そこで、単純ではない最近の総合セキュリティソフトでは、「手配書」方式に加えて、パソコンに入ってしまった後も監視を続け、不審な行動を取れば隔離なり駆除をする、「ふるまい検知」や、機能的に怪しい部分を検出する「ヒューリスティック分析」機能を持つものが出てきています。これにより、未知のマルウェアにもある程度は対処できるわけです。

しかし、それでも対処しきれないものもあります。システムのセキュリティホールが発見されると、それが修正される前に攻撃する「ゼロデイ攻撃」を行うマルウェアです。この場合は、手配書も間に合わないので、現状では、決定的に有効な手段がほとんどありません。しかし、そういったことを踏まえても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。

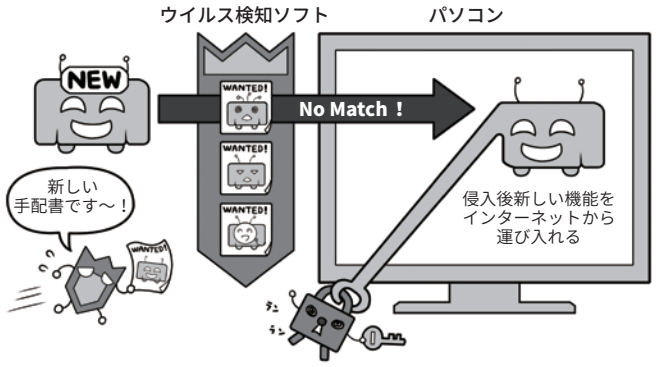
単純なウイルス検知ソフト



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 パソコン本体とセキュリティの状態を最新に保とう

パソコンのセキュリティを最新に保つためには、各種のアップデート処理が不可欠です。

最近の機種では、たいていの場合、OS関連のアップデートは自動で行われるか、利用者にアップデートを促す通知が出るようになっています。ただ、深刻なセキュリティホールが発見され、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されます。

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 Flash Player、Adobe Acrobat Reader、Oracle Javaや各種のウェブブラウザはよく使用されるため、攻撃のターゲットになりやすいのです。

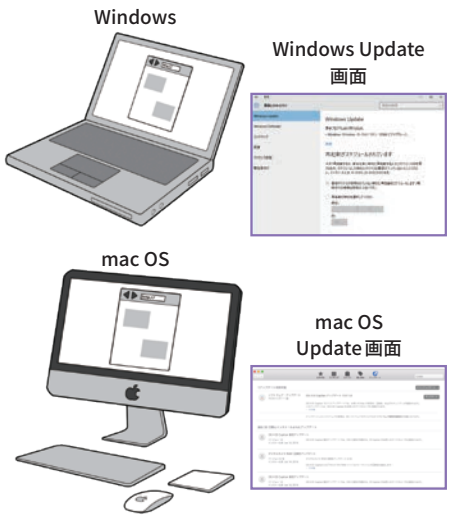
また、本体機器そのものを動かすプログラムを更新する、ファームウェアアップデートにも気を配りましょう。こちらの更新通知は、自動で出る機器と出ない機器があるので、自分の機器にファームウェアアップデートがあった場合、どういうようにその情報を入手するべきかを、確認して気を配ってください。

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、なるべく日に一度は意識的にセキュリティソフトの画面を見るようにしましょう。これは、セキュリティの状態を確認する意味もあります。

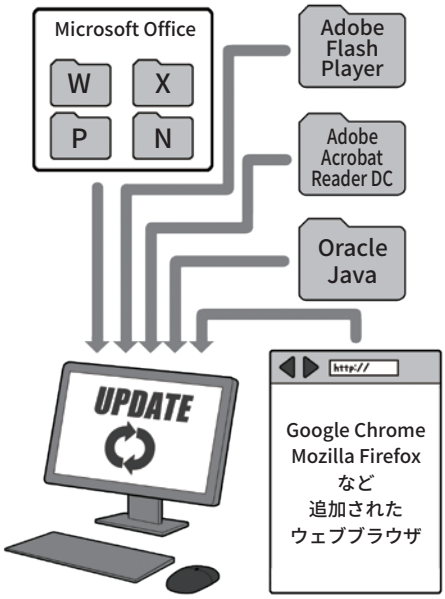
本体もOSもセキュリティソフトも重要ソフトもアップデート

本体のファームウェアも更新

OSと基本ソフトの更新



重要ソフトも更新



セキュリティソフトも更新

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。

例えば、社会インフラがテロ攻撃などで狙われやすいのは、テロリスト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。重要ソフトを使っていない場合は、削除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、攻撃して乗っ取れる機器がなければ成立しないように、穴を作らない一人ひとりの行動が安全なネットを作るのです。

3 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が必要です。

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、また、自動アップデート機能も充実しています。機器そのもののソフトウェアの更新でも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でも、更新の通知が出たら、マメにアップデート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)やOSの更新が、設定メニュー上のどこにあるのか更新手順を確認しておきましょう。また、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、また、その設定でも更新時に権限変更で、所有者による確認が必要な場合は自動で実行されないため、気づくと更新されていないアプリがたくさんたまっていることもあります。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スマート家電やIoT機器などは、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不正に利用されることがあります。

アプリやセキュリティソフトの更新は基本的に自動にし、まめにチェック

ネットにつながる家電もファームウェア更新する設定ページの初期パスワードも変更しておくこと

無線LANアクセスルータ　ネットワーク対応プリンタ　ネットワークカメラ

スマート家電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。このときの初期パスワードは必ず購入時から変更しておきましょう。不正アクセスされ、カメラなどでは覗き見される原因になります。

4 ソフトやアプリは原則公式ストアから。権限にも気をつける

本体やシステムを最新の状態に保っても、防ぎにくい攻撃があります。それは、まだマルウェアとして認識されていない悪意あるソフトウェアへの感染です。

基本的に、セキュリティソフトなどがマルウェアを検出するためには、過去に収集されたデータが必要になります。このデータが多ければ多いほど、マルウェア検出の精度は高まるのです。現実世界で、病気の検体が多ければ多いほど、より確実な対応方法を得られるのと同じです。

これとは逆に、セキュリティソフト会社がまだ知らないマルウェア、あるいは検体が充分に収集されていないマルウェアは、検知ソフトなどでの発見が難しくなります。

攻撃者が、チェック体制のしっかりしている公式ストア経由ではなく、私たちをメールなどで誘導し、不審な場所から導入させようとする理由もそのためです。

そのような手に引っかかって、マルウェアに感染してしまわないように、「ソフトは信頼できる場所から、アプリは公式ストアから導入する」ことが推奨されるわけです。

特に、スマホの場合、iOS機器は公式のストア以外からはアプリを導入できない仕組みになっていますが、Android機器の場合は公式ストアやベンダーメーカーのストア以外からもアプリをインストール可能なので、攻撃者がメールなどであなたを誘導して、公式ストアでない場所からインストールさせるもの、あるいはインストールの過程で「不明なアプリ」などといった言葉を見る方法は避けましょう。

また、AndroidでもiOSでも、アプリのインストール時や初回起動時に、同意を求められる「権限」には充分注意してください。権限とはインストールするアプリに対して、スマホのどの機能の利用を許可するか、という確認です。

単なるカメラアプリなのに住所録にアクセスするものや、撮影する必要がないのにカメラにアクセスするもの、著しく多くの項目にアクセスしようとするものなどは要注意の例です。項目別に許可を却下するか、そうできない場合、そのアプリは導入しないようにしましょう。また、最初は無害に見えて、導入後のアップデートで権限の増加の許可を求めるものも、その変更項目に注意してください。

そのほか、アプリ間での機能連携やウェブサービス間で連携して、間接的に権限を奪取するものもあるので「連携」という言葉にも充分注意してください。

基本的にアプリを公式ストアではない場所からインストールしない。権限付与にも気をつける。

「不明のアプリ」という言葉に注意

・Android

項目や文言は、使用するAndroidのバージョンやスマホメーカーによって異なりますが、アプリのインストール時に「不明なアプリ」と表示されたり、設定内の「不明なアプリ」に関する項目を変更させようとするものは、すべてセキュリティ上危険なものと判断して下さい。

アプリは、基本的に公式ストアからのみインストールするようにして、そのほかの場所からは避けましょう。

導入時や起動時の権限付与に注意

・Android、iOS（画面はAndroid）

アプリのインストール時や、起動時にさりげなく表示されるため、多くの人が無意識に「承認」や「同意」してしまっていますが、これは、「アプリがスマホのこれらの情報に自由にアクセスできる許可」を求めている画面です。

個別に却下することができない場合もあるので、その際は導入しないようにしましょう。そして、そもそも不必要な権限を求めるアプリは怪しいと警戒しましょう。

コラム：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、その誕生が比較的最近であることもあり、設計思想自体にセキュリティの概念が盛り込まれていて、パソコンなどと比較して、セキュリティアプリなどが担う役割は大きくはありません。

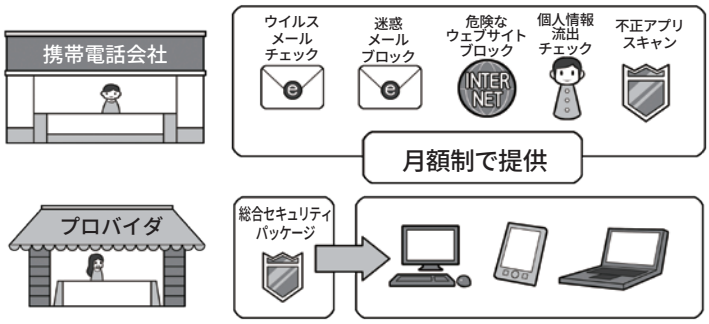
しかし、チェックするべき点を見落とし、気づかないうちにインストールされる不正なアプリの検出や、また、そういったものの侵入経路になるメールの排除、危険なウェブサイトのブロック、あるいは個人情報の流出チェックなど、セキュリティ全般にかかわる機能を補助的に導入したい場合もあるかもしれません。

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、内容を充分に精査した上で導入してもいいでしょう。

また、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。

そして、高機能化するスマート家電など IoT 機器についてもスマホと同様にセキュリティ対策が必要になります。P45も参照して、万全の対策を講じていきましょう。

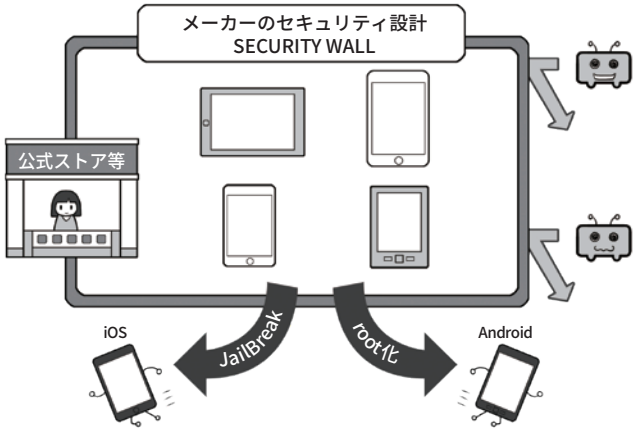
必要性を感じるなら、スマホには セキュリティパック導入を検討しよう



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

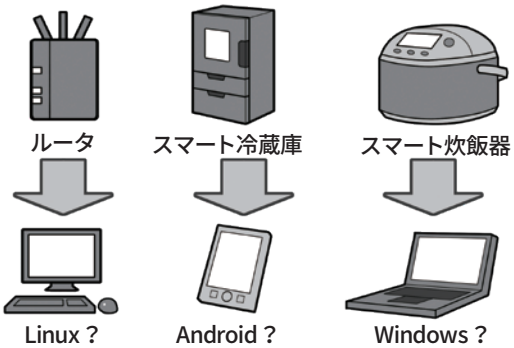
携帯電話会社からは、セキュリティ関係の機能がパッケージ化されて提供され、インターネットプロバイダも、同様のサービスを提供しています。自分が求める機能があるかを精査して、必要性を感じる場合は導入を検討しましょう。

スマホのセキュリティを改造してはいけません



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、Android、Windows などのコンピュータが入っていることがあります。乗っ取られ、サイバー攻撃に利用される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。

コラム：パソコンやスマホを最新の状態に保っても防げない攻撃がある。それがゼロデイ攻撃！

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からメーカーによって修正されるまでの期間を狙って攻撃することを「ゼロデイ（ZERO DAY）攻撃」といいます。

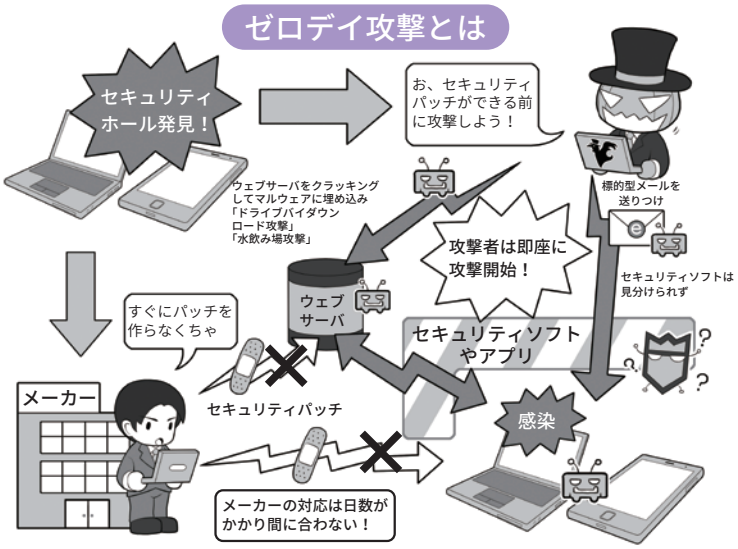
メールで送りつけられるマルウェアは、警戒していればある程度防ぐことができるのですが、動画、ウェブサイトやウェブ広告に仕込まれるマルウェアは、特定のサイトを見ただけで感染することもあり、情報がないままこの方法でゼロデイ攻撃を受けると実質的に防ぐことができません。

特に、最近で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。アプリを提供するサービスは、アプリを使用しなくてもウェブブラウザで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も慣れておきましょう。

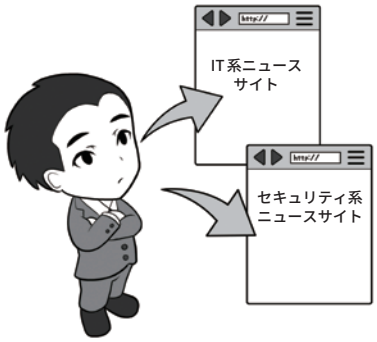
ゼロデイ攻撃とは？ 対処の例

ゼロデイ攻撃とは

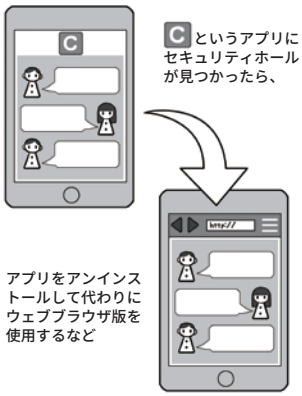


ゼロデイ攻撃に対抗するには？

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



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セキュリティ情報を入手し、対象の機種どれが一つでも攻撃に成功するなら攻撃を開始できますが、メーカーは情報を精査した上で、対象となっている機種すべてで充分なセキュリティ対応をしなくてはいけないからです。

ですから、利用者もそれを前提として備え、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わけです。

3 複雑で長いパスワードと多要素認証で侵入されにくくする

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、機器やサービスを乗っ取るものもあります。

パスワードは、ウェブサービスなどが保管しているものが流出して使われる「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試す「辞書攻撃」などにより探し当てる方法や、IoT機器購入時のパスワードを変更せず乗っ取られる場合もあります。

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、攻撃し続ければ理論上は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」にして防ぎます。ログイン用パスワードであれば入力ごとに時間がかかるので、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、より桁数を増やして安全性を高めるに超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

数字のみだと→100億通り

英大文字小文字＋数字＋記号（26個として）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、それを複数の機器やサービスで使い回していては意味がありません。1カ所から漏れればすべてログイン可能になります。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、1つ漏れれば推測されます。それぞれに別々の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	全部同じ
×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、テキストファイルなどで保存しておけば、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。

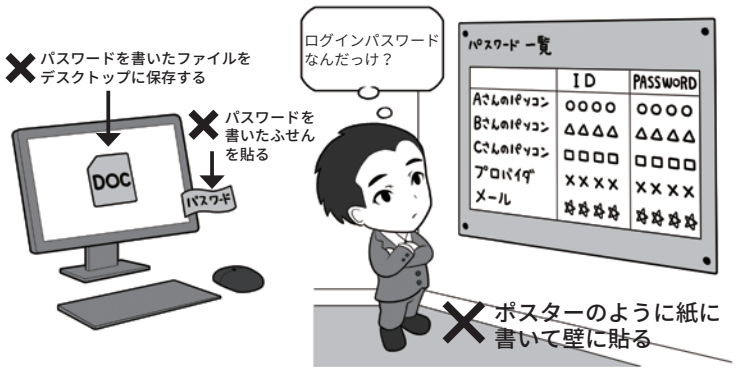
パソコンで、ウェブブラウザに覚えさせる「自動入力」機能も要注意です。あなたが席を離れた隙に、誰かがパソコンを勝手に操作するかもしれません。それに、ノートパソコンなら本体ごと盗まれてしまいます。パスワードは、基本的に利用する場所で保管してはいけないのです。しかし、個別に複雑なパスワードをそれぞれ設定していては、とても覚えきれません。では、どうしたらいいでしょう。

一つは、紙のパスワード管理ノートに書いて、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があります。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、過去にセキュリティ上のトラブルがあったアプリは避けましょう。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、スマホでもパスワードを使う場合も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。

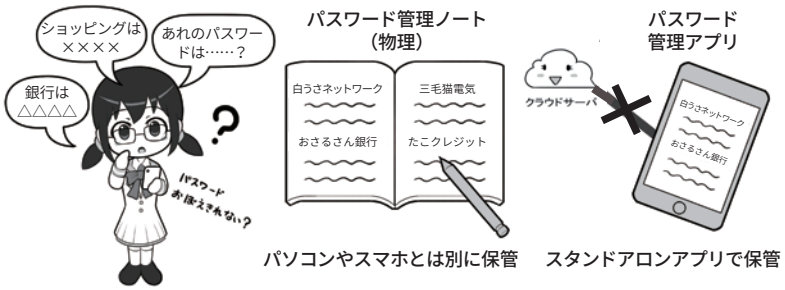
ただ、管理しているパスワードは、必ずバックアップを忘れないようにしましょう。落としたスマホが戻るとは限りませんから。

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。

パスワードは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。アプリの機能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、各種ウェブ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の本人確認、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、こういった個人情報はSNSが普及した現在、ネットで簡単に見つけられることもあり、セキュリティ上、安全とはいえなくなっています。

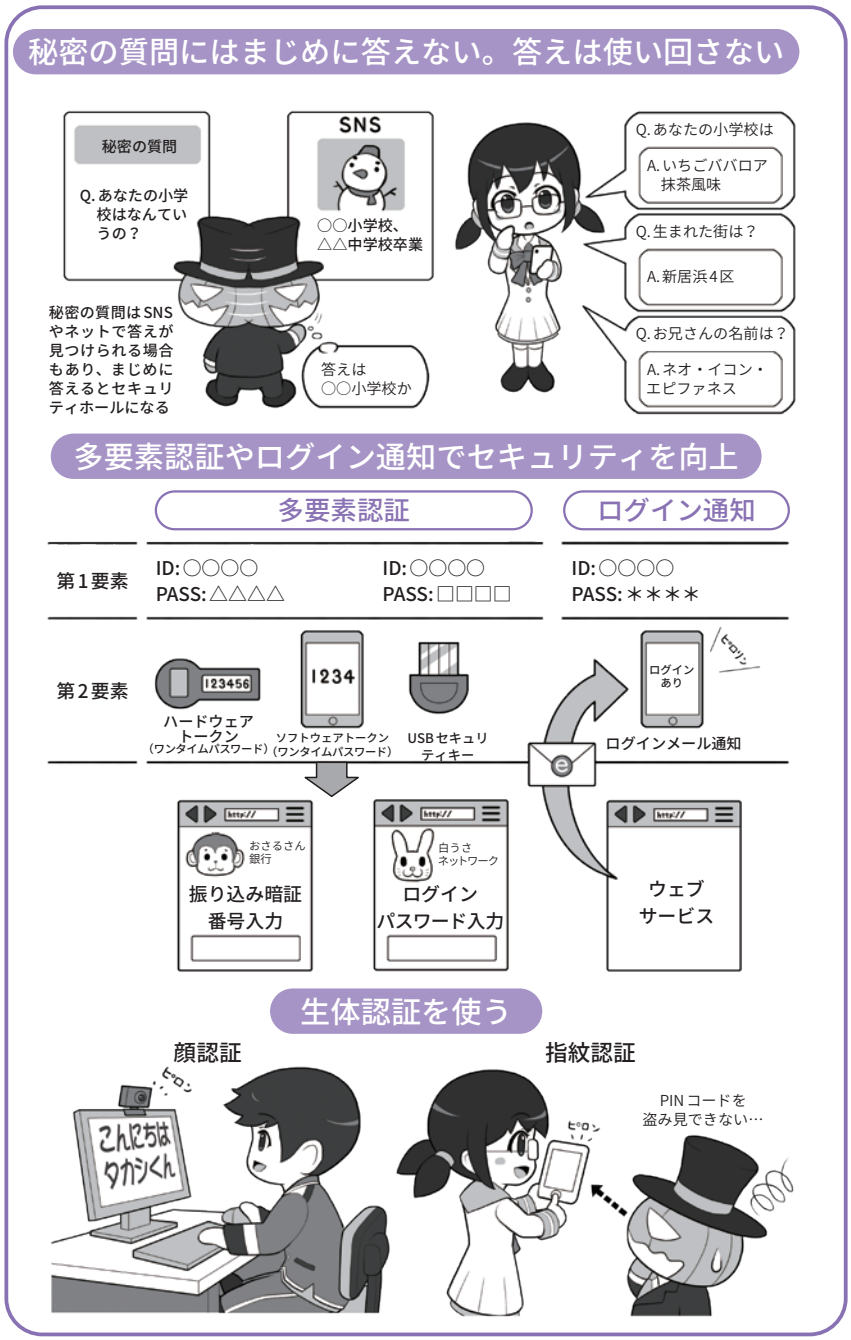
ですから、秘密の質問に答えを設定する場合、まじめに答えず、あえて全く関係ない答えを使い、SNSなどから推測できないようにし、その上で忘れないように管理アプリなどに保存しましょう。

また、ウェブサービスに安全にログインするために、二要素以上を使う多要素認証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ほかに、そのときに一度きり使用する使い捨て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。（SMSやメールで送信する方式もありますが、安全面で非推奨です）

そのほかにも、USBセキュリティキーなどで物理的に確認する方法や、不審なログインがあったときに、メールで利用者に通知するサービスがあれば活用しましょう。

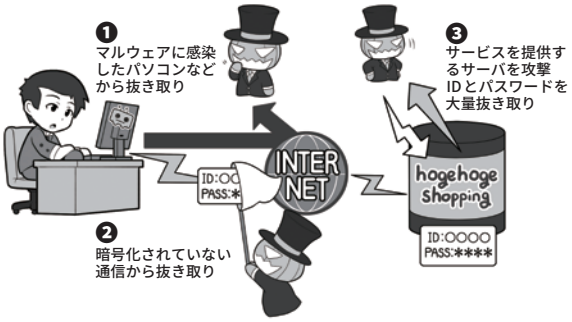
また、最近の機器では3次元の立体的な顔形状や、虹彩や指紋で本人確認をして機器のロック状態を解く生体認証機能もあります。

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、PINコードには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？

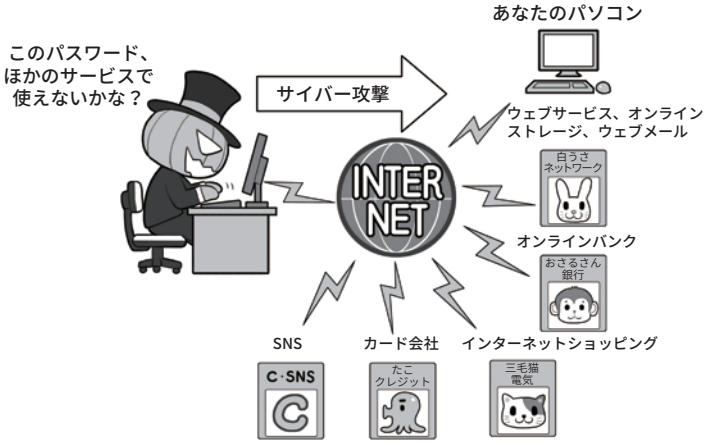
様々なIDとパスワードの抜き取り方法



攻撃者にIDとパスワードが抜き取られる方法は、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。

攻撃者は盗んだIDとパスワードを使い、様々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様々な方法で試します。

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、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るケースなどがあります。

ここで知っ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。IDやパスワードを普段入力してしないから安心、とはいい切れません。

IDとパスワードを盗み取った攻撃者は、それで別のウェブサービスなどが乗っ取れないか、様々な場所で試します。

あなたが、複数のサービスで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が一気に乗っ取られます。あとは、オンラインショッピングで勝手に物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してしまうわけです。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 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

サイバー攻撃を行う攻撃者は、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、なんらかの利益が目的の行動が多いということができるでしょう。

彼等にとってのサイバー攻撃はビジネスであり、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。

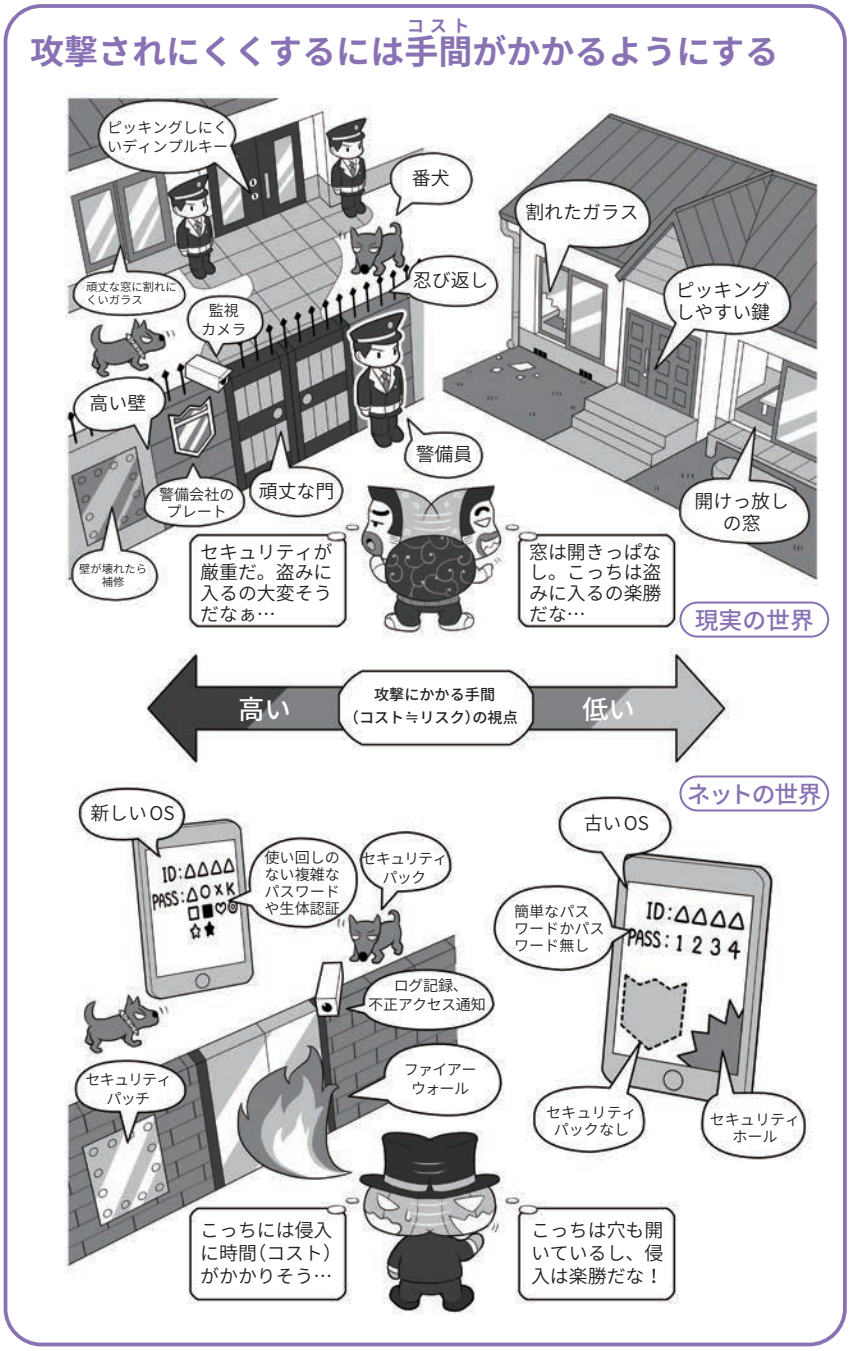
例えば、現実世界では、泥棒は防犯がしっかりしていて警戒が厳重な家よりも、鍵をかけなかったり窓を開けっ放しで外出したりするような家の方に侵入します。その方が、彼等にとって安全、つまり手間(コスト)がかからないからです。

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、ファイルそのものも暗号化されておらず、パスワードを使っていても、たくさんのウェブサービスで全部同じものを使い回している。

これならば、どっちに行くのがビジネスとしてコストパフォーマンスがいいか明らかですよね。

こういった攻撃者の視点を持ち、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。一方、単純な利益目的でない場合、すこし対策が変わってきます。



金銭などの利益目的ではない攻撃の例としては、相手そのもの、つまり未成年者略取や、いかがわしい写真の入手などを目的とするものがあります。

現実の世界で、面と向かって「いかがわしい写真を撮らせてください」といったら、たいていの人は拒否して逃げ出すでしょう。それが、ネットの世界だと許容してしまう理由は、攻撃者がネットを利用して、警戒心をもたれないような人間になりすまし、相手をうまくだましてしまうからです。

ですから、SNSや掲示板などのウェブサービスで知らない人物が近づいてきたら、注意して絶対に個人情報は教えないようにしましょう。現実の知り合いでもないのに会おうと誘われた場合は、基本的に会わないか、会う必要がある場合は必ず保護者同伴で行きましょう。

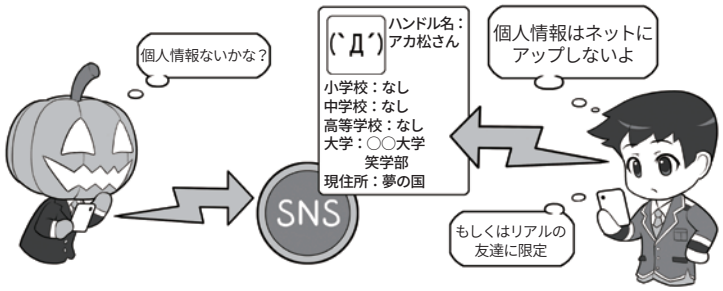
そして、少しでも変だなと思ったり、最初と話が違ったりした場合、それは人をだます「心理的な」テクニックかもしれません。警戒し、その場から立ち去りましょう。

あまり聞いたことがないかもしれませんが、そういった「人をだます心理的なテクニック(≒ソーシャルエンジニアリング)」は体系化されマニュアルのようになって存在するのです。

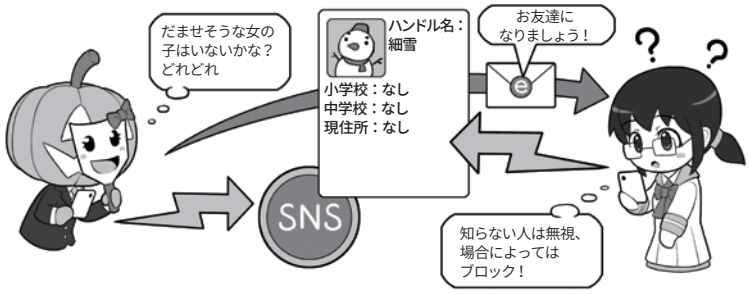
この人をだますテクニックは、なにも上記のような例だけでなく、私たちも日常生活の様々なシーンで直面しているのです。

例えば、「振り込め詐欺」や「標的型メール」。どんなにセキュリティを固めても、本人がだまされ結果として犯罪者に操られてしまうと、すべては無意味になってしまいます。厳重に注意しましょう。

金銭目的ではない攻撃にも備えよう



個人情報はネットに上げない！



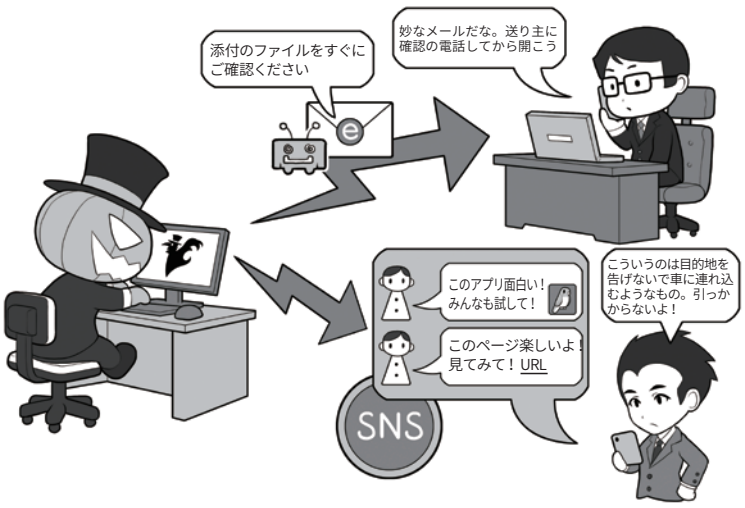
リアルで知り合いじゃない人とはネットで友達にならない！

未成年がSNSを利用する場合、写真や自分の個人情報を記載しないようにしましょう。また、投稿内容も原則的に一般に公開せず、SNSで友達になった人のみが見られる設定にしましょう。

SNSで、知らない人が友達になろうとリクエストを送ってきても、会ったことがない人はスルーするか基本的にお断り(ブロック)しましょう。

それは、現実の世界で自分の個人情報を書いた名札をつけて歩いたり、名前もわからない初めて会った人に、ついていったりするのと同じぐらい、たいへん危ないことなのです。

攻撃者に操られて、内側から鍵を開けてしまわないように、心がまえを持とう



不審なメールに気をつけ、怪しいときは開かず送信者に確認する癖をつけましょう。ネットやSNSの引っかけは、セキュリティ関係のニュースをこまめに見ていると、次第に傾向がわかるようになります。訓練しましょう。

5 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）

心の隙を突く攻撃、ソーシャルエンジニアリングには、「トラッシング（ゴミ箱あさり）」など相手に直接接触せずにやるものや、「ネームドロップ（権威があるように見せて聞き出す）」「ハリーアップ（急がせて聞き出す）」など、相手が正常に判断できない状況に追い込んで必要な情報を聞き出したり、相手に自分が求める行動を行わせたりするものがあります。

振り込め詐欺をはじめ詐欺全般には、こういった「人間の心の隙を突くソーシャルエンジニアリングの手法がよく用いられている」といわれています。

そして、デジタル世代のソーシャルエンジニアリングも、また、人間の心の隙を突くものなのです。

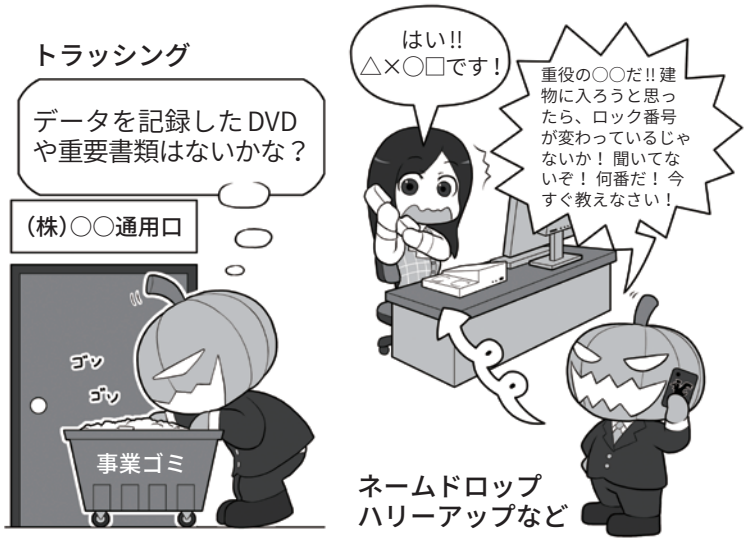
例えば、相手に直接接触せず情報を入手するものとしては、電車で座席に座っている人のスマホ操作を見て「PINコード」やパターンロック形状を盗む「ショルダーハッキング」、カフェなどのテーブルに放置されているスマホの画面に残る指の脂跡からパターンロックを見破る方法などがあります。事前に、ロック解除の手段を特定してから機会を見てスマホを盗めば、個人情報が丸ごと手に入ります。

また、メールで相手の心理的な隙を攻撃するのが「標的型メール」です。詐欺師が詐欺にかける相手をよく調べてから行動するように、標的型メールでは攻撃者が相手の名前、所属、身分、同じような会社でやりとりするメールのパターンなどを入手して、通常の仕事のメールと見分けがつかないほど精緻なものを送ってきます。そうして、会社のネットワークに侵入されたり経営層のふりをして送金を迫るビジネスメール詐欺（BEC）が行われたりするのです。

精緻な「標的型メール」がライフルによる狙撃のように狙った獲物だけを撃つものだとすると、「スパムメール」は広範囲を攻撃する手法として今でもよく使われます。

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

公共の場でロック解除をするときは、背後などから見られていないか気をつけましょう。

スマホを席に残しておいたり、席取りのためにテーブルに置いて離れたりしてはいけません。

スパムメールでの攻撃は、引っかかる率が少なくとも、その攻撃の母数を大きく取ることで攻撃者にとっての利益回収のパフォーマンスを上げています。

例えば、「フィッシングメールの例」の画面は、実際にSMSに送りつけられた、銀行を名乗るフィッシングメールを模したものです。

これには、フィッシング(=詐欺)メールを疑う手がかりがたくさんあります。まず、口座を持っていない人はそこで気づけるでしょう。表示しているリンクも、よく見ると、URLの末尾が日本を示すjpではなくgqになっています。しかし、こういったものでも一定の割合で引っかかる人がいます。その先が詐欺サイトではなく、ゼロデイ攻撃のマルウェアが埋め込まれたウェブサイトならば、開いただけで感染してしまうでしょう。

また、もっとやっかいなのが、攻撃者ではなく、善意でマルウェアを拡散させてしまう人々です。「悪意はないが拡散してしまう例」の画面を見てください。このSNSアカウントが友達のアカウントだった場合、きっと本当に「このアプリが面白いと思って薦めているかも」と、あまり不審に思わないでしょう。

しかし、友達は知らなくても、実はこのアプリがマルウェア入りだったり、あるいは拡散する間は無害でも、後に権限を拡大して個人情報を抜き取るかもしれません。

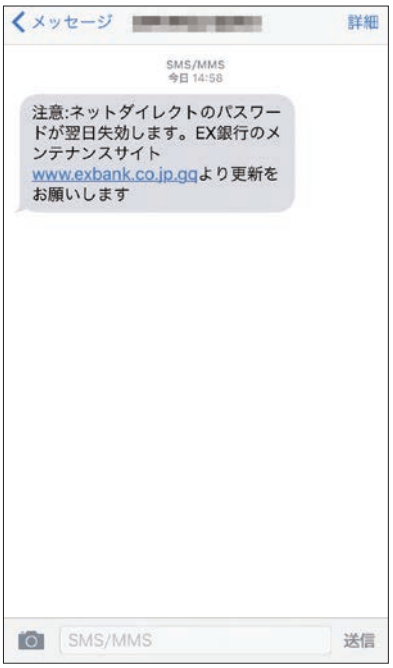
これが、他人の発信ならば警戒できますが、親しい友達や家族だった場合、警戒するでしょうか？

対抗策としては、こういったお薦め系のものは一つの線引きを持って接するようにしましょう。

標的型メールとスパムメールの例

標的型メールの例

スパムメールの例
SMS(ショートメッセージ)を使った例



悪意はないが拡散してしまう例

メールの文面など、目の前に見ている情報で完結しないものは一律に警戒するのです。動画が面白いとかお金が儲かる方法があるとかだけでなく、リンクでジャンプするとか、添付ファイルを開かせるものは一律に避ける。

それは、現実世界で「ちょっと向こうまでつきあってよ」とか「ちょっとこの車に乗ってよ」といって連れて行かれるのに等しいと思いましょう。

さらに、「リンクでジャンプしないけど検索エンジンで調べて見る分にはいいよね」、と思っても、攻撃者はそうやって検索エンジンからやってくる人向けに、二段構えでマルウェアを仕込んだウェブサイトを用意していることもある、と覚えておいてください。

コラム：クリックしてはいけない！フィッシング詐欺の傾向

近年、フィッシング詐欺の攻撃でもっとも目を引いたのは、宅配業者の不在通知詐欺です。宅配業者を名乗って「配達に行ったが不在だった。下記のリンクから確認して欲しい」というようなSMS（ショートメッセージ）を送りつけて、利用者をリンク先の偽サイトに誘導し、そこでIDとパスワードなどを詐取するというものです。

実は、この業者は「SMSで不在通知を行なわない」のですが、それを知らない人たちはまんまとだまされてしまったわけです。関係機関で日々、「不審なメールに気をつけてください」というアナウンスをしているのですが、SMSとメールは違うものと思われてしまったのかもしれません。

その考え方からいえば、こういったメッセージを使った詐欺には、SMSやメールだけでなく、SNSのメッセージ機能、あるいはゲーム内のメッセージ機能を使った攻撃も考えられるので、同様に注意してください。

ほかにも、地震が発生したときに、気象庁を名乗って津波に関する迷惑メールが送られた例もありました。いずれも私たちが「だまされないぞ」と身構えているのとは違う方向や、災害時で正常な判断が行えない状況を狙っています。

こういった詐欺メールは、送信元アドレスを確認したり、メッセージ中のリンクのアドレスをよく見ることなどで詐欺を見抜くこともできますが、それらは偽装することも可能なので、確認するだけで安全とはいい切れません。基本は「見るだけで完結しない情報はすべて疑え」です。情報を確認する場合は、正規のウェブサイトのURLを直接入力して見るか正規のアプリから行いましょう。

また、日々巧妙になる手口を少しでも知るにはフィッシング対策協議会（https://www.antiphishing.jp/）のウェブサイトや内閣サイバーセキュリティセンターのTwitter（@nisc_forecast）をフォローするとよいでしょう。最新の事例をすぐに確認できます。

フィッシング詐欺はいろんな方法がある

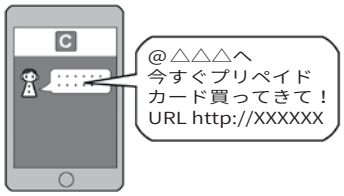
SMS（ショートメッセージ）

電話番号宛てに送る

電子メール（eメール）

メールアドレス宛に送る

メッセージ（アプリなど）



アプリのアカウント宛に送る

ゲーム内のメッセージ機能

ゲームのユーザー宛に送る

「怪しいメール」といわれたら「メール」だけでなく似たような機能全般に気をつけましょう。

驚くと人間は警戒心を忘れる

災害時などに驚いて人間の警戒心が弱くなった瞬間を狙った攻撃もあります。注意しましょう。

コラム：映画「ザ・ハッカー」にみるソーシャルエンジニアリング

ケビン・ミトニック（左）

ケビン・ミトニックは車で走りながら電話一本で人をだまし、情報を手に入れる段取りをします。

シモムラ・ツトム（右）

シモムラは、当初、後手に回りますが、そこから巻き返してミトニックを追い込んでいきます。

「ザ・ハッカー」は1999年に公開された、ハッカー対ハッカーの戦いを描いた、実話ベースの映画です。

原作はその登場人物のうちの一人「シモムラ・ツトム」が共著した『Takedown』という小説です。

相手のハッカー「ケビン・ミトニック」にも『欺術（ぎじゅつ）』などの著書があります。

原作では、シモムラがホワイトハット的に、ミトニックがクラッカー的に描かれていますが、映画では、その勧善懲悪的な雰囲気よりも、ハッカーとハッカーの意地とテクニックのぶつかり合いに重点を置いて描かれています。

この映画の注目するべきポイントは、「ハッカーの技術」とはなにかという部分です。特に、「凄腕ハッカーは目的のためならデジタルの世界に留まらない」ということに驚愕します。みなさんの中の「ハッカー像」が変わると思います。

ミトニックは劇中で、「ソーシャルエンジニアリング」を駆使し、人をだまして情報を手に入れたり、コンピューターセンターに堂々と入り込んで暗号解析をしたりします。

私たちの日常で、「要人のメールや個人情報が、電話が原因で盗まれた」といったニュースを目にすると、情報管理が緩いんだなと思ったりしますが、この映画を観れば、人間というものがどれぐらいあっけなくだまされ、どれぐらいあっけなく情報を流出させるのかを実感することができます。

見たほとんどの人は、「あんなことやられたら、絶対に逃げられない」といいます。

残念ながら、現在日本では、この作品を販売している会社がありません。中古のDVDを手に入れるか、有料のネット配信サービスで見つけたらぜひご覧になってください。

心の隙への攻撃にポイントを置いた、セキュリティの教材にもおすすめです。

ミトニックさんは現在では、ホワイトハットとして社会に貢献されています。罪を償って守る側に回ったミトニックさんはかなりクールですよ。

コラム：スパムメールとその由来

スパムおにぎり、スパムの味噌汁、スパムのソテー、スパムのポークオムレツは単品で存在しますが、スパムの姿煮はないだろ！　ドヤッ！（スパムの姿煮は執筆担当の夢です）

かつて、メールソフトを開くと、うんざりするほど広告や勧誘、フィッシングなどをする「スパムメール（spam mail）」が送信されてきていて、メールを見るのに滅入る（おっと失礼）時代がありました。

この、うんざりする多量のメールを「スパム（spam）」と呼ぶ由来はなにか。諸説ありますが、有力なのはソーセージの中身を缶詰にしたスパム（SPAM）と、これをネタにした英国のコメディ集団「モンティパイソン」のコントでしょう。

実際のコントの内容は、文字では表現できないナンセンス系なので、動画サイト検索で探し「考えるより感じろ」で味わってみて下さい。

そして、このコントの劇中での「スパム推しのウザさ」が当時のスパムメールの「ウザさ」とつながり、「spam mail」と呼ばれるに至ったのでしょう。

なお、SPAMを生産しているホーメルフーズ社は商品を大文字、スパムメールを小文字と表記することで、迷惑メールがスパムメールと呼ばれることを容認しています。

さて、とはいえ日本人にこのうんざり感を説明するのは難しいので、某グルメマンガをリスペクトしつつ、日本風にアレンジしたイラストを描いてもらいました。

「めいる百軒」と書かれた定食屋ののれんをくぐって、「おやじ！おまかせ定食！」と注文したら、これが出てきたと思って下さい。滅入るでしょ。

ところで、SPAMはすごくおいしいですよ！　姿煮以外は沖縄でお目にかかれます。ただ、さすがの沖縄でも、この完全スパム定食には出くわしたことはありませんけど(^o^)