



総務省 安心してインターネットを使うために

## 国民のためのサイバーセキュリティサイト



### 一般利用者の対策

インターネットを使ったサービスは、私たちの生活のあらゆる場面に浸透しており、私たちは日々、その利便性を享受しています。しかし同時に、インターネットにはさまざまな脅威も潜んでいます。

高度情報社会に生きる私たちは、賢い消費者として、どのような脅威が存在するのかという知識と、その脅威から身を守るための対策を知り、より安全にインターネットを使いこなすことが必要になってきています。

インターネットの利用に際して、適切な情報セキュリティ対策をとらなかった場合、ウイルス感染や、情報漏洩(ろうえい)などの被害に遭う可能性があり、自分が被害を被るだけでなく、他人に迷惑をかける危険性もあります。公共空間であるインターネットを利用する以上は、個人であっても一定の責任が伴います。情報セキュリティ対策を取ることは、必須の約束事であるといえるでしょう。

また、いまやインターネットは、個人の現実世界での生活と密接に結びついています。インターネットを使った個人の情報発信が、現実世界に大きな影響を与える事例も発生しており、インターネット空間での適切な振る舞い方を身につけることも必要になってきています。

ここでは、一般の方向けに【基本的な対策】、さまざまな【インターネット上のサービス利用時の脅威と対策】、【情報発信の際の注意】について解説します。

I. 基本的な対策 .....	3
ソフトウェアを最新に保とう .....	4
ウイルス対策をしよう .....	5
ウイルス対策ソフト .....	6
記憶媒体からのウイルス感染 .....	7
ホームページ閲覧の危険性 .....	8
パスワードの設定と管理 .....	9
フィッシング詐欺に注意 .....	10
ワンクリック詐欺に注意 .....	12
無線LANの安全な利用 .....	14
機器の廃棄 .....	15
個人に関する情報の取扱い .....	16
プライバシー情報の取扱い .....	17
サポート期間が終了するソフトウェアに注意 .....	18
IoTセキュリティ対策として留意すべきルール .....	21
II. インターネット上のサービス利用時の脅威と対策 .....	23
【インターネット】	
ホームページ閲覧における注意点 .....	24
ネットオークションにおける危険性 .....	25
ショッピングサイトの利用 .....	26
インターネットバンキングの注意点 .....	27
SNS利用上の注意点 .....	29
クラウドサービス利用上の注意点 .....	32
動画配信サイトなどの注意点 .....	34
オンラインゲームの注意点 .....	35
【電子メール】	
ウイルス添付メールなどへの対応 .....	37
迷惑メールへの対応 .....	38
チェーンメールの問題点 .....	40
メールの誤送信 .....	41
【情報機器】	
家族共用パソコンの注意点 .....	42
携帯電話・スマートフォン・タブレット端末の注意点 .....	43
ゲーム機の注意点 .....	46
インターネット対応機器(家電、記憶媒体等)の注意点 .....	48
【その他】	
ファイル共有ソフトの利用とその危険性 .....	50
III. 情報発信の際の注意 .....	52
著作権侵害に注意 .....	53
プライバシー公開の危険性 .....	54
ネットを使いたいやがらせや迷惑行為 .....	56
発信内容は慎重に .....	58



## 一般利用者の対策

### I .基本的な対策

---

ここでは、インターネットを使う時に常に行わなければならない基本的な対策について説明します。



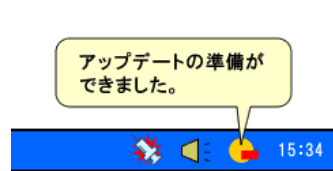
## ソフトウェアを最新に保とう

パソコンやスマートフォン・タブレット端末などのコンピュータは、本体（ハードウェア）を通じて、キーボードなどから入力した情報を、内部のソフトウェアが処理することで動いています。

こうしたソフトウェアには、オペレーティング・システム（OS）と呼ばれる、コンピュータを動かす基本的なソフトウェアや、ホームページを閲覧する際に使うWebブラウザ、メールを送受信するのに使うメールソフトなど、利用目的に合わせたさまざまな種類のものがあります。

今では、パソコンやスマートフォンに限らず、多くの機器にコンピュータが搭載され、ソフトウェアで動いています。その点ではパソコンやスマートフォンと同様です。

しかし、こうしたソフトウェアには、時間の経過とともに、脆弱性（ぜいじゃくせい）と呼ばれる不具合が発見されることがあります。脆弱性は、プログラムの不具合や設計ミスに起因して起こるものですが、それらが発見されるたびに、それを修正するための修正プログラムが、メーカーから配布されています。代表的なソフトウェアでは、最近では、「ソフトウェアの更新が必要です」という形で通知が表示されることが多くなっています。

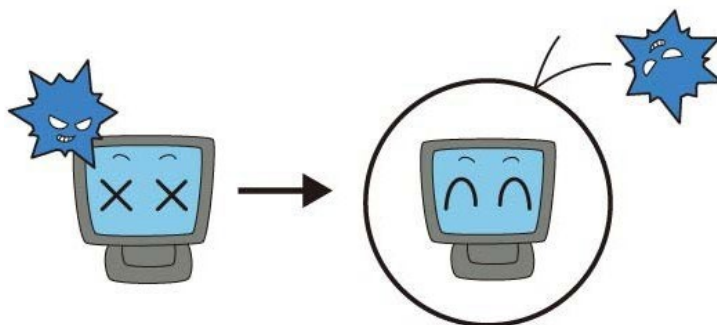


ソフトウェアのアップデートを知らせるアイコンとメッセージ

脆弱性を残しておくことは、さまざまな攻撃のきっかけを与えてしまうこととなりますので、通知が来たら、面倒がらずに毎回更新することが重要です。

パソコンやスマートフォン以外の、インターネットに接続された機器（家電製品やカーナビゲーションなど）も、ソフトウェアの更新が提供されることがあります。多くは自動的に更新されるようになっているので、その機能を無効にしないよう留意しましょう。

なお、古い機器ではメーカーのサポートが終了し、脆弱性が発見されてもソフトウェアの更新が提供されないことがあります。そのような機器をインターネットに接続したまま使い続けるのは危険です。その場合は機器自体の買い替えも考える必要があります。



**参照** 脆弱性（ぜいじゃくせい）とは？（基礎知識）



## ウイルス対策をしよう

インターネット利用時に、ウイルスは、電子メールやホームページ、記憶媒体など、さまざまな経路から侵入し、情報漏洩(ろうえい)などさまざまな被害をもたらします。ウイルスに感染してしまうと、自分のコンピュータが被害を受けるだけでなく、インターネットの別のコンピュータに対する感染活動を行い、加害者となってしまうことがあります。

近年は、PCやスマートフォンのOS自体のセキュリティも向上していますが、安全にコンピュータを利用するためには、ウイルス対策ソフトの導入や、インターネットサービスプロバイダによるウイルス対策サービスの利用が推奨されます。なお、ウイルス対策ソフトを導入した場合には、ウイルス検知用データを常に最新の状態にしておかなければなりません。通常は自動更新されますが、契約期間切れで更新されない場合、かえって脆弱で危険な状態になりかねないので注意が必要です(ウイルス対策ソフトの導入により、OS自身のセキュリティ機能が無効となっている場合があるからです)。

また、ウイルス対策ソフトを装った不正ソフトや、不安を煽る詐欺商法もあるため、信頼できるベンダーの対策ソフトを選ぶようにしましょう。

また、ウイルスに感染しないようにするためには、知らない人からの電子メールやメッセージの添付ファイルを不用意に開かないようにするなどの注意も必要です。

▶ ウイルス対策ソフト

▶ 記憶媒体からのウイルス感染



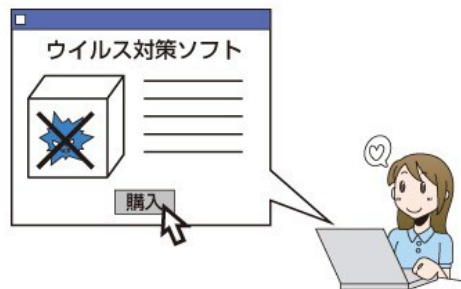
## ウイルス対策ソフト

ウイルス対策ソフトは、主に以下の機能を持っています。

- 受信する電子メールやCD-R、USBメモリなど外部からコンピュータが受け取るデータにウイルスが含まれていないかをチェックし、ウイルスに感染することを防ぎます。
- 送信する電子メールなど、コンピュータの外部に出て行くデータにウイルスが含まれていないかチェックします。
- コンピュータがウイルスに感染している場合には、ウイルスを隔離したり、場合によっては駆除したりすることができます。
- ウイルス対策ソフトの付加機能として、ファイアウォール機能が備わっている場合は、コンピュータに登録している情報が盗まれるのを防いだり、外部からコンピュータを操作されたりすることを防ぎます。

しかし、ウイルス対策ソフトを導入すれば対策が万全ということではありません。ウイルスも日々進化しており、対策ソフトのアップデートが間に合わないことも少なくありません。

対策ソフトは手段のひとつであると考え、ウイルスに感染しないようにするには、ウイルス対策ソフトを導入するだけでなく、ウイルスの侵入経路となりやすい、知らない人からの電子メールやメッセージの添付ファイルを不用意に開かないようにしたり、怪しいホームページは、できるだけ閲覧しないようにしたりなどの注意も必要です。



### 参照 ウィルスとは(基礎知識)

ウィルスの感染経路と主な活動(基礎知識)

事例7: ウィルス対策はしていたはずなのに...

事例8: 送った覚えがないのに...

事例17: 有名サイトからダウンロードしたはずなのに...



## 記憶媒体からのウイルス感染

コンピュータには、USBメモリなどの外部記憶媒体や情報機器をコンピュータに接続しただけで、あらかじめ指定された処理が自動的に実行されるようになっているものがあります。この仕組みを悪用して作られたのが、いわゆるUSB媒介ウイルスです。

USB媒介ウイルスは、この自動実行(Autorun)機能を利用して、コンピュータに、USBメモリなどの外部記憶媒体や情報機器を差し込んだだけでウイルスを実行するようになっています。パソコンに接続して、自動実行がされる可能性がある媒体や機器(携帯電話やスマートフォン、携帯型音楽プレイヤー、デジタルカメラなど)は、全て注意が必要です。USB媒介ウイルスは、感染したコンピュータに差し込んだ別のUSBメモリなどの外部記憶媒体や情報機器に感染する形で被害が拡大していきます。

USB媒介ウイルスへの対策としては、以下のような方法があります。

- USBメモリを差し込んだときには、ファイルを開く前に必ずウイルスチェックを行う。●持ち主の分からないUSBメモリを使用しない。
- コンピュータの設定を変更して、USBメモリの自動再生機能を停止しておく。

たとえ音楽を聞くなどの用途にしか使わない機器であっても、コンピュータに接続するだけでウイルスに感染し、感染を拡大させることがありますので十分注意しましょう。



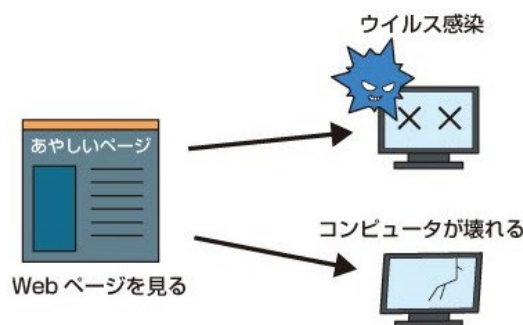
### 参照 ウイルスの感染経路と主な活動(基礎知識)

インターネット対応機器(家電、記憶媒体等)の注意点(一般利用者の対策)



## ホームページ閲覧の危険性

インターネットを利用することで、世界中にある数多くのホームページを閲覧することができますが、残念なことにそれらの中には、情報収集や犯罪への利用を目的としたものもあります。このような悪意のあるホームページを閲覧すると、使用しているコンピュータシステムが壊れてしまったり、ウイルスに感染してしまったりすることがあります。また、特殊なプログラムが埋め込まれたホームページを閲覧すると、あなたのコンピュータに保存されている情報やファイルが盗み出されてしまう可能性もあります。



ホームページによっては、Cookie(クッキー)を利用して、閲覧時に入力した情報をWebブラウザに保管させることがあります。Webブラウザで保管されているCookieの中には、パスワードやクレジットカード番号など、重要な情報が含まれることもあります。使用しているWebブラウザのメーカーのホームページなどを見て、Cookieの適切な取扱い方法や、Webブラウザの設定変更の方法について調べておきましょう。

このような悪意のあるホームページの被害を受けないために、まずは使っているパソコンやスマートフォンのOSやソフト・アプリを最新の状態にしておきましょう。またウイルス対策ソフトを導入するか、インターネットサービスプロバイダによるウイルス対策サービスを利用することも有効です。その上で、怪しいホームページはできる限り閲覧しないことが大切です。特に、不特定多数の利用者がアクセスする電子掲示板やSNSでは、いやがらせや詐欺のために、このような動作をするホームページへのリンクが貼り付けられている場合があるので、むやみにリンクをクリックしないようにしましょう。最近、こうした掲示板から誘導されたホームページでパソコンがウイルスに感染し、悪意のある第三者から遠隔操作されるという事件も発生しています。

また、企業の公式ホームページや個人のホームページであっても、開設者の知らないうちに、悪意の第三者によってWebページが改ざんされ、別の悪意のあるサイトの一部が見えないように埋め込まれていたり、自動的に別の悪意を持ったサイトに誘導されたりする事例が増えています。このような改ざんされたホームページから身を守るためにも、やはりしっかりとしたウイルス対策が必要です。

この他、ホームページには不確かなデマ情報も書き込まれる場合もあります。情報の信憑性を確認することも重要です。

### 参照 ウイルスの感染経路と主な活動(基礎知識)

事例15: 自分の名前で勝手に書き込みが...





## パスワードの設定と管理

パソコンにログインしたり、インターネットのネットオークションやショッピングサイトを利用する際に、なりすましを防ぐための認証には、一般的にパスワードが利用されています。そのため、コンピュータやインターネットを利用する上では、どのようなパスワードを使用するかということが、とても重要なことであると言えます。

オンライン銀行

ユーザーID:

パスワード:

OK

パスワードの適切な管理(安全なパスワードの作成、保管、更新)はパソコンやサーバを安全に利用するためには欠かせません。以下のリンクを参考に、自分のパスワードの管理について再度確認をしてください。

### **参照** IDとパスワード(基礎知識)

事例2: 私の名前で誰かがメールを

事例5: メールが他人に読まれている?



## フィッシング詐欺に注意

フィッシング詐欺とは、送信者を詐称した電子メールを送りつけたり、偽の電子メールから偽のホームページに接続させたりするなどの方法で、クレジットカード番号、アカウント情報（ユーザID、パスワードなど）といった重要な情報を盗み出す行為のことを言います。なお、フィッシングはphishingという綴りで、魚釣り（fishing）と洗練（sophisticated）から作られた造語であると言われています。



最近では、電子メールの送信者名を詐称し、もっともらしい文面や緊急を装う文面にするだけでなく、接続先の偽のWebサイトを本物のWebサイトとほとんど区別がつかないように偽造するなど、どんどん手口が巧妙になってきており、ひと目ではフィッシング詐欺であるとは判別できないケースが増えてきています。

さらに、最近ではパソコンだけでなく、スマートフォンでも同様に電子メールやSMSなどのメッセージ機能からフィッシングサイトに誘導される手口が増えています。

フィッシング詐欺の手口としては以下のようなものが挙げられます。

### ■ 電子メールやメッセージ機能でフィッシングサイトに誘導

典型的な手口としては、クレジットカード会社や銀行からのお知らせと称したメールなどで、巧みにリンクをクリックさせ、あらかじめ用意した本物のサイトにそっくりな偽サイトに利用者を誘導します。

そこでクレジットカード番号や口座番号などを入力するよう促し、入力された情報を盗み取ります。

### ■ SNSなどの情報でフィッシングサイトに誘導

電子メールやメッセージだけではなく、SNSの投稿サイトに、URLを記載してアクセスさせ誘導する手口です。

### ■ 表示されているURLを本物のURLに見せかけてアクセスさせる手口

電子メールやSNSに投稿されたURLを実在するURLに見間違えるような表示にすることで誘導する手口です。

例えば、アルファベットの一文字の(オー) o を数字の0にしたり、アルファベットの大文字の(アイ) I を小文字の(エル) l にしたりして、閲覧者が見間違えたり、信用させたりする手口もあります。

対策としては、以下の点に注意しましょう。

- 金融機関のID・パスワードなどを入力するWebページにアクセスする場合は、金融機関から通知を受けているURLをWebブラウザに直接入力するか、普段利用しているWebブラウザのブックマークに金融機関の正しいURLを記録しておき、毎回そこからアクセスするようにするなど、常に真正のページにアクセスすることを心がけましょう。また、本物のWebサイトのドメイン名やURLを常に意識して、正しいWebサイトにアクセスしているかを確認する、アクセス先のサーバ証明書の内容を確認する、などの対応を心がけましょう。
- 通常、インターネットバンキングへのログインやクレジットカード番号などの重要な情報の入力画面では、SSL/TLSという暗号化技術を利用します。重要な情報を入力するWebページでは、SSL/TLSが採用されているかを毎回確認するようにしましょう。SSL/TLSで通信が行われていることは、WebブラウザのURL表示部分(アドレスバー)や運営組織名が緑色の表示になっているか、鍵マークが表示されているか、などで確認できます。重要な情報の入力を求めるページで、SSL/TLSが使用されていない場合は、まずはフィッシング詐欺を疑いましょう。
- 金融機関などの名前で送信されてきた電子メールやSMSなどのメッセージの中で、通常と異なる手順を要求された場合には、内容を鵜呑みにせず、金融機関に確認することも必要です。フィッシング詐欺であるかどうか判断が難しい場合には、メールの送信元の会社に連絡を試みるのもよいでしょう。ただし、電子メールに記載されている相手の情報は正しいものとは限らないため、電話をかける場合には必ず正規のWebサイトや金融機関からの郵便物などで連絡先の電話番号を調べるようにしてください。

**参照** 事例12: クレジットカード番号が盗まれた

## ワンクリック詐欺に注意

ワンクリック詐欺とは、Webサイトや電子メール、SMSなどのメッセージに記載されたURLを一度クリックしただけで、一方的に、サービスへの入会などの契約成立を宣言され、多額の料金の支払いを求められるという詐欺です。フィッシング詐欺が情報をだまし取るのに対し、不安を煽るなどして直接金銭を支払わせようとするものがワンクリック詐欺です。ワンクリック詐欺の手口には、以下のようなものがあります。



- 利用者の興味を引きそうな電子メールや電子掲示板などを利用して、利用者をおびき寄せる。アダルト系、出会い系などを装った内容であることが多い。
- いかにも正当な契約手続きが完了しているかのように見せかけ、利用料を不正に請求する。多くのWebサイトでは利用者が間違っして契約してしまったように思わせる仕組みや、わざとわかりにくいところに利用規約などを表示して、利用者が気付きにくいような細工をしています。
- 料金請求の際、携帯電話の個人識別番号や、パソコンの固有識別番号、利用しているインターネットサービスプロバイダの情報などを表示させ、利用者の情報が複雑な技術によって特定されたように見せかける。
- 期限内に支払わない場合、延滞料が加算される、法的措置を講ずるといった脅迫的な内容で、利用者に支払いを迫る。

ワンクリック詐欺に対する対処方法としては、以下があげられます。

- 不用意にWebサイトにアクセスせずに、電子メールや電子掲示板の文面をきちんと読んで、利用しましょう。特に、利用規約などが記載されている場合には注意が必要です。場合によってはこの利用規約を非常に長文にしたり、Webブラウザから1～2行しか表示できないように工夫して、利用者が利用規約を読まずにクリックさせるような手口のサイトもあります。
- あたかも個人が特定されたような表現で、「お支払い頂けない場合には、自宅にまで伺います」といった脅し文句が書かれていても、真に受けないようにして、どうしても心配であれば、支払いをする前に、総務省電気通信消費者相談センター、消費生活センター、警察などに相談しましょう。
- 「電子消費者契約及び電子承諾通知に関する民法の特例に関する法律」では、「電子消費者契約に関する民法の特例」として、消費者がコンピュータの操作ミスなどで、契約する意志がなく申し込んだ場合における救済措置がとられています。間違っしてクリックした場合や、意図せずこうしたWebサイトを閲覧して、料金を請求された場合は、解約手続や、連絡などはせずに無視しましょう。
- 利用状況や支払理由などを確認するために業者に連絡を取るといことは、相手に自分の連絡先などの情報を渡すことにつながります。決して連絡をしないようにしましょう。

- ワンクリック詐欺はいわゆる迷惑メールなど知らない人から送信されるメールが発端になる場合が多いので、できるだけ知人以外からの電子メールを受け取らないようにするために、あらかじめ推測しにくいメールアドレスに変更しておくといよいでしょう。
- また、サイト検索結果に詐欺サイトに誘導するものが含まれる場合があります。日常利用しているサービスは、検索せず、過去にアクセスしたことがあるブックマークを利用する方が安全です。
- トラブルになりそうなどときには、表示されているデータを保存したり、画面を印刷したりしておくことも必要です。また、自分の行った手順をメモしておくといよいでしょう。（[いいえ]を選択したが、登録完了画面が表示された時など）。

最近では、ホームページを表示した際に、自動的にウイルスを埋め込む悪質なWebサイトも増えてきているため、知らないWebサイトを訪問する場合には、それらの危険性もきちんと認識しておくようにしましょう。

**参照** 事例14: ワンクリック詐欺に注意  
総務省電気通信消費者相談センター



## 無線LANの安全な利用

無線LANは、ケーブルの代わりに無線を利用するという性質上、通信内容が傍受（盗聴）される危険性があります。そのため、無線LANを使ってユーザIDやパスワードなどのログイン情報、クレジットカード番号のほか、プライバシー性の高い情報をやり取りする場合には、自分と相手先との間でSSL/TLSにより通信が暗号化されていることを確認しましょう。

家庭内や職場のネットワークで複数のパソコンを利用する際には、家族や職場のパソコンとファイルのやり取りを円滑に行うために、ファイル共有機能を有効にしている人もいるかもしれません。しかし、公共の場で無線LANを利用するときに、このファイル共有機能が有効になっていると、他人からパソコンやスマートフォン内のファイルが読み取られたり、ウイルスなどの不正なファイルを送りこまれたりすることがあります。公共の場で無線LANを利用する際には、必ずファイル共有機能を解除しましょう。

一方で、自宅内などに自分で無線LANのアクセスポイントを設置して利用する場合には、アクセスポイントで暗号化の設定を行ってください。現時点では、WPA2方式又はWPA3方式による暗号化を推奨します。WPA3の方が、より強固な暗号化方式を利用できます。旧来からWEPという暗号化方式もありましたが、近年WEPは短時間で解読される方法が発見され、安全な方式とは言えなくなっていますので、注意しましょう。



また、アクセスポイントに設定する管理パスワードや、認証・暗号化のための共有鍵は、単純なものや、無線LANのネットワーク識別子であるSSIDから類推できるものにしないよう、注意が必要です。一般的にSSIDは公開されて使用されるため、SSIDと似たパスワードを設定していると、第三者に類推されてしまう可能性があるからです。共有鍵が知られると、第三者がアクセスポイントに接続できたり、通信内容が容易に解読できたりします。安全なパスワードの設定に関しては、下記のリンクを参照してください。

さらに、現在はセキュリティ機能を強化した無線LAN機器が普及していますので、そのような機器を積極的に利用することをお勧めします。

- 参照** 無線LANの仕組み（基礎知識）ID  
とパスワード（基礎知識）  
SSL/TLSの仕組み（基礎知識）  
一般利用者が安心して無線LANを使用するために



## 機器の廃棄

パソコンや携帯電話・スマートフォン、DVDやUSBメモリなどには、個人に関する情報のほか、さまざまな情報が記録・保管されています。こうした機器を廃棄する際に、そのまま廃棄業者に依頼し、不燃物として廃棄した場合、第三者にこれらの機器から情報を詐取される危険性もあります。

情報漏洩(ろうえい)を防ぐためにも、こうした機器を廃棄する場合は、事前にデータを消去して廃棄しましょう。データの消去方法には以下の方法があります。

### ■ パソコン



専用のデータ消去ソフトなどを使うことで安全に消去が可能です。信頼できるリサイクル業者を選んで廃棄を依頼することもできます。

### ■ 携帯電話・スマートフォン

使用している機種によりますが、初期設定状態にする機能が付いている場合は、購入初期状態にしてから廃棄しましょう。携帯電話・スマートフォンは端末販売店で回収をしていることも多いので、そうした信頼できる事業者に廃棄を依頼するか、安全に廃棄できるリサイクル業者を選んで廃棄を依頼すると良いでしょう。

### ■ DVDやCD-Rなどの外部記録メディア



他のパソコンで読み込めないように、傷を付ける、あるいは、物理的に壊すなどして不燃物として廃棄しましょう。

**参照** 事例11: 中古パソコンによるデータの漏洩





## 個人に関する情報の取扱い

個人に関する情報は、氏名、性別、生年月日、住所といった個人を特定できる情報のほか、電話番号、メールアドレス、職業、家族構成といった、個人のプライバシーなどに関わる情報を含んだ概念です。こうした個人に関する情報が不用意に第三者に知られた場合、その情報が拡散したり、誹謗中傷に使われたり、なりすましなどの被害にあったり、あるいは、犯罪に利用される可能性も否定できません。



インターネットは不特定多数の人が利用しているため、個人に関する情報の取扱いには特に慎重にならなければなりません。例えば、電子掲示板に自分のメールアドレスを公開しただけでも、いたずらの電子メールが送信されてきたり、ネットストーカーにつきまといわれたりなどの被害に遭うこともあります。

まず、電子掲示板やホームページには、氏名や住所、電話番号、メールアドレスなどの情報をできるだけ掲載しないようにすることが大切です。もちろん、自分の情報だけでなく、家族や知人の情報も同様です。

また、訪問したホームページで、サービスなどを利用するために住所氏名などを登録する際には、特に注意が必要です。信頼できないホームページや管理者が不明なホームページでは、できるだけ情報を登録しないように心がけるべきです。悪質なホームページでは、登録された情報は、名簿として売買されるだけでなく、犯罪行為などに利用される可能性もあります。

最近では、登録した人だけが参加できるSNS(ソーシャルネットワーキングサービス)というサービスが増えてきています。多くのSNSでは、あらかじめ自分のプロフィールを登録しておくようになっており、この中には実名での登録と利用が必要なサービスもあります。このような場合は、どのような情報を登録し、どの範囲まで公開するのかをよく検討したうえで、適切に設定するように注意してください。

また、住所氏名などの情報は収集されなくても、サイトアクセスなどの情報が収集されることはよくあります。多くは利用統計の把握や広告のために行われますが、収集された情報を他の情報を突き合わせることで、住所氏名などの個人の特定が可能となるケースがあります。

多くの企業ではプライバシーポリシーを定めて適切に運用されていますが、不安を感じる場合は、ブラウザに保存されている「cookie」を削除することで、情報を収集されなくすることは可能です。ただし、削除すると利用者の特定ができなくなることから、ログイン操作が再び必要になるなどの影響もあります。

**参照** SNS(ソーシャルネットワーキングサービス)の仕組み(基礎知識)

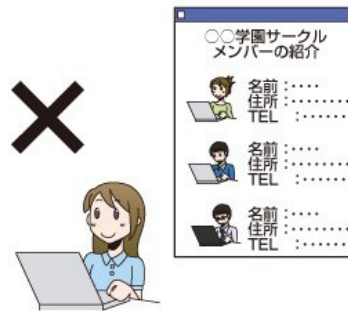
個人情報公開の危険性(一般利用者の対策)

事例1: 資料請求の情報が漏洩した



## プライバシー情報の取扱い

プライバシーとは、一般に、“他人の干渉を許さない、各個人の私生活上の自由”をいうと考えられています。いいかえると自分が他人に知られたくない情報のことで、インターネットにおいても、個人のプライバシーは保護されなければなりません。特にインターネットは不特定多数の人が利用するため、本人に断りなく、個人の氏名や住所、写真、私生活上の事実や秘密など、他人のプライバシーに関わる情報を公開してしまうと、取り返しのつかない事態を引き起こすことがあります。



たとえば、ある電子掲示板に写真を公開しただけであっても、他の利用者によって別の複数の電子掲示板などにどんどん転載されてしまえば、そのデータがどこにあるのか追跡が困難になり、消去することは現実的に不可能になってしまいます。このような行為は、その人に精神的苦痛を与えることがあり、その結果、プライバシーや肖像権の侵害、名誉毀損などによって訴えられる可能性もあります。

また、手紙と同様に、電子メールやメッセージも個人の重要なプライバシーです。そのため、家族であっても、本人の許可なしに、人の電子メールやメッセージを覗き見ることはプライバシーの侵害になります。

**参照** 個人情報の公開の危険性(一般利用者の対策)



## サポート期間が終了するソフトウェアに注意

私たちは、自分のコンピュータでさまざまなソフトウェアを利用しています。Webブラウザやメールソフト、ワープロソフトなどはもちろんのこと、コンピュータの基本動作を担っているOSもソフトウェアです。また、パソコンに限らず、ルータなどの通信機器や、テレビなどの家電製品にもソフトウェアが組み込まれています。

これらのソフトウェアには、実は消費期限ともいべき「安心して利用できる期間」があります。

### ソフトウェアのサポート期間

ソフトウェアを安心して利用できる期間とは、ソフトウェアを開発したメーカーがそのソフトウェアのサポート(保守対応)を行っており、利用者がサポートサービスを受けられる間のことと言い換えられます。

メーカーによるサポートを受けられる間は、仮にそのソフトウェアに不具合や脆弱性(ぜいじゃくせい)が見つかった場合には、メーカーがそれらを修正するための修正プログラム(「更新プログラム」と呼ばれることもあります)を作成し、ホームページ内のソフトウェアサポートページなどで配布するのが一般的です。

メーカーから修正プログラムが発表された場合は、利用者は修正プログラムを自分のコンピュータや機器に適用してソフトウェアを最新の状態に保ち、情報セキュリティのリスクを抑えることができます。

しかし、ソフトウェアのサポート期間が終了してしまった場合、ソフトウェアに不具合や脆弱性が見つかったとしても、修正プログラムがメーカーから提供されなくなります。利用者がそのソフトウェアを使い続けた場合、そのコンピュータや機器は不具合や脆弱性を抱えたままの状態になります。これは、コンピュータが外部から攻撃を受ける危険性のある状態であり、情報セキュリティのリスクが非常に高まります。

### 基本的な対策

ソフトウェアは、サポートされているものを利用することを意識し、常に最新の状態に保つようにすることが、必要最低限の情報セキュリティ対策になります。

具体的には、ソフトウェアの脆弱性が発見された場合には、それを修正するための修正プログラムがメーカーのサポートページなどで配布されますので、修正プログラムのインストールを行ってください。

### サポートが終了したWindows7とOffice2010

これまで、家庭や企業、組織などで一般に広く利用されてきたマイクロソフト社製OSであるWindows7と、ビジネス用アプリケーションであるOffice2010のサポート2020年に終了しています。

サポート期間の終了に伴い、以後、不具合や脆弱性についての修正プログラムが提供されなくなります。そのため、これらのソフトウェアを利用している人は、メーカーのサポートページを参照して、後継となるソフトウェアへ移行したり、サポートが行われている製品を利用したりするなど、コンピュータが外部から攻撃を受けるリスクをなるべく小さくするための対策を行う必要があります。

ソフトウェアは  
サポート期間内のものを利用しましょう



**参照**

Windows7のサポートが終了(Microsoft)

<https://www.microsoft.com/ja-jp/windows/windows-7-end-of-life-support-information>

Office2010のサポートとセキュリティ更新プログラムの提供は終了しました(Microsoft)

<https://www.microsoft.com/ja-jp/microsoft-365/office-2010-end-of-support>

ソフトウェアを最新に保とう(一般利用者の対策)





## IoTセキュリティ対策として留意すべきルール

インターネットに接続するIoT(※1)機器が世の中に普及・増加し、一般利用者の方も日常生活の中でIoT機器を利用するようになってきています。

IoT機器を適切に取り扱わないと、IoT機器の利用に不都合が生じるだけでなく、インターネット経由で機器が操作され、自分(所有者)やその家族等になりすまして不正利用されたり、自分や家族等のプライバシー情報が漏れたり、IoT機器が悪用されて他の利用者に迷惑をかける、あるいは、犯罪に巻き込まれたりする可能性もあります。

そういったリスクの多くは、IoT機器を利用する際に、簡単な注意を払うだけで回避することができます。

ここでは、一般利用者がIoTセキュリティ対策として留意すべき四つのルールをまとめましたので、これらに気を付けながらIoT機器を安全に利用しましょう。

(※1):IoTとは、「Internet of Things」の略で、「モノのインターネット」と呼ばれています。これまでインターネットに接続されてきたパソコンやスマートフォンに加えて、自動車や家電など様々なモノがインターネットにつながるようになってきています。IoT機器とは、そうしたインターネットにつながるモノを指します。



### ルール1) 問合せ窓口やサポートがない機器やサービスの購入・利用を控える

- インターネットに接続する機器やサービスの問合せ窓口やサポートがない(もしくはサポート期限が切れた)場合、何か不都合が生じたとしても、適切に対処することが困難になります。また、インターネットに接続する機器のアップデート(※2)を適切に行うこともできないため、安全な状態で継続して機器やサービスを利用することができなくなります。(問合せ窓口やサポートがある機器やサービスの購入・利用を行って、機器の異常等、何か不都合が生じた場合は、問合せ窓口やサポートの連絡先へ直ちに知らせてください。)
- 問合せ窓口やサポートがない(もしくはサポート期限が切れた)機器やサービスの購入・利用は行わないようにしましょう。

(※2): 機器のアップデートとは、機器の不具合の改善や不正利用の防止を目的として、機器をインターネット経由で最新の状態に更新することです。

## ルール2) 初期設定に気をつける

- インターネットに接続する機器のパスワードが他の人に漏れると、インターネット経由で機器が乗っ取られ、自分(所有者)やその家族等になりすまして不正利用されるおそれがあります。
- 機器を初めて使う際には、ID、パスワードの設定を行きましょう。パスワードの設定では、機器購入時のパスワードのままとしない、他の人とパスワードを共有しない、他のパスワードを使い回さない、生年月日等他の人が推測しやすいものは使わない等の点に気をつけましょう。
- インターネットに接続する機器の取扱説明書等を読んで、取扱説明書等の手順に従って、自分でアップデートを実施してみましょう。

## ルール3) 使用しなくなった機器については電源を切る

- 使用しなくなった機器や不具合が生じた機器をインターネットに接続した状態のまま放置すると、知らず知らずのうちにインターネット経由で機器が乗っ取られ、不正利用されるおそれがあります。
- 使用しなくなった機器や不具合が生じた機器は電源を切りましょう。例えば、使用しなくなったWebカメラ(※3)やルータ(※4)等をそのまま放置せず、電源をコンセントから抜きましょう。  
(※3): Webカメラとは、インターネットに接続することができるカメラです。  
(※4): ルータとは、パソコンやスマート家電等の機器をインターネットへ接続させるための情報通信機器です。

## ルール4) 機器を手放す時はデータを消す

- 機器を捨てる、売る、貸し出すなど、機器を手放す場合は、機器に記憶されている情報の削除を行わないと、自分や家族等の利用者情報が漏洩するおそれがあります。
- 機器を手放す際は、自分や家族等の利用者のプライバシー情報が漏れないよう、情報を確実に削除しましょう。

**参照** 「IoTセキュリティガイドラインVer1.0」(平成28年7月5日総務省、経済産業省、IoT推進コンソーシアム)





## 一般利用者の対策

### Ⅱ. インターネット上のサービス利用時の 脅威と対策

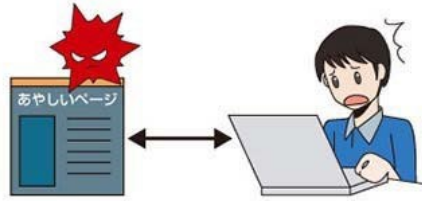
---

ここでは、インターネットを使ったサービスの脅威や対策について説明します。



## ホームページ閲覧における注意点

ホームページを閲覧する場合、ウイルスを配布するなど悪意のあるホームページに遭遇する場合があります。ここではそうした悪意のあるホームページについて説明します。



インターネットには、さまざまなサイトが存在します。その中には、悪意を持って設置された、詐欺やウイルス配布を行うものもあります。ウイルスの置かれたサイト(いわゆる、マルウェア配布サイト)の典型的な手口としては、有名なソフトウェアのダウンロードのリンクなどを悪用して、一見無害なソフトウェアのダウンロードに見せかけて、ウイルスをインストールさせようとしたり、省庁や企業の公式サイトを改ざんして、ウイルスを埋め込んだりすることが行われます。閲覧中に警告メッセージを出し、偽のセキュリティソフト(中身はウイルス)のインストールを促す手口もあります。不審なサイトはできる限り、訪問しないようにしましょう。

基本的なセキュリティ対策として、ウイルス対策ソフトの導入とソフトウェアのアップデートが欠かせません。これらの対策をしていないと、ウイルス感染や詐欺サイトでの被害に遭いやすくなります。パソコンはもちろんのこと、スマートフォンやタブレット端末、ゲーム機など、インターネットに接続する機器でウイルス対策ソフトやウイルス対策サービスがあるものは、できる限り導入するようにしましょう。また、OSやファームウェア、インストールしているアプリも更新するようにしましょう。

この他の悪性サイトの事例として、もし、フィッシング詐欺に遭遇してしまったら、ウイルスなどの不正なプログラムがインストールされてしまっている可能性があるため、ウイルス対策ソフトなどでウイルススキャンをするようにしましょう。騙られた金融機関などのホームページなども確認し、暗証番号やパスワード、秘密の質問の答えなどは、すぐに変更しましょう。



ワンクリック詐欺に遭遇してしまったら、請求が来ても決して支払いはしないようにしましょう。請求のメッセージなどを止めるためには、メールソフトやフィルタリングソフト、フィルタリングサービスなどを利用して、受信を止める設定をしておきましょう。

どうしたら良いかわからない場合は、警察や総務省電気通信消費者相談センターなどに相談するとよいでしょう。

**参照** 事例3: ホームページを見ただけで…  
総務省電気通信消費者相談センター



## ネットオークションにおける危険性

ネットオークションは、出品されている商品に希望者が入札し、指定期間内に最高価格を提示して落札した人が商品を購入できる仕組みです。欲しい商品が安く購入できる、既に市場に出回っていない商品や非売品を手に入れる、自分も商品を出品できるなど、とても魅力的で便利なサービスです。しかし、利用者の急増に伴い、最近はさまざまな手口による詐欺やトラブルが発生しています。数多く発生しているトラブルには、以下のものがあります。

- 入金したけれど、いつまでたっても商品が送られてこない。
- 届けられた商品が出品時の説明と違う。説明にはブランド品と記載されていたが、偽物であった。
- 破損している商品が送られてきた。
- 商品を送ったのに、入金されない。



ネットオークションを安全に利用するためには、まず出品者の過去の取引実績を確認することが大切です。過去の取引実績がないにもかかわらず、同時に大量の商品を出品している場合には注意しなければなりません。

実際に入金したり商品を送付したりする前には、取引相手の氏名とメールアドレス以外の連絡先（住所、電話番号）を確認しておくことが大切です。また、トラブルが発生してしまった場合に備えて、交換した電子メール、銀行振込みの控え、宅配便の伝票などの証拠を保存しておくことも大切です。

さらに、出品者自らが別の参加者になりすまして落札することで、取引実績自体を捏造（ねつぞう）するケースも見受けられます。最近では、例えば宅配便事業者に一定の手数料を支払った上で、落札者が商品の到着や内容の確認を行ってから、代金の決済が行われるサービスも提供されています。ネットオークションを利用する際には、そのようなサービスの利用を検討してみるのもよいかもしれません。

**参照** 事例9: オークションの商品が届かない



## ショッピングサイトの利用

自宅や会社に居ながら買い物ができるインターネットのショッピングサイトは、とても便利なものです。しかし、ショッピングサイトを使って買い物を行う場合、直接その店舗や商品を確認することができないため、それを悪用した詐欺などのトラブルが増加しています。もっとも多いトラブルは、代金を入金しても商品が届かないケースです。このトラブルのほとんどは、詐欺目的で一時的に開設したショッピングサイトを利用したものです。

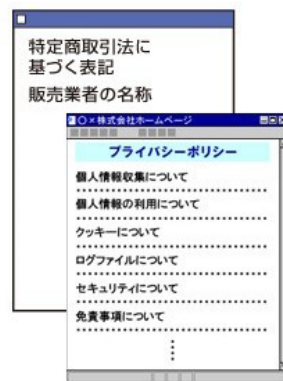
特に、近年は実在するサイトをそっくりコピーして、一見しただけでは区別がつかない偽ショッピングサイトが横行しています。

検索サイトで偽サイトのページが表示されることがあるため、ショッピングサイトはトップページからアクセスするなど、気を付けましょう。

正規に営業しているショッピングサイトでは、特定商取引法に基づいて、販売業者名や運営責任者などの項目を記載しているところが多いため、その会社が安心できるかどうかの判断材料にすることができます。ただし、倒産直前に商品をとんでも安い金額で宣伝して、多くの顧客から現金を集めた上で、商品を発送しないまま一切連絡がつかなくなってしまうという事件も起こっています。販売価格が市価と比べて異常に安い場合には、慎重に取引を行うようにしてください。

もうひとつ注意しなければならないのが氏名、住所、電話番号、クレジットカード番号などのさまざまな情報の入力です。少なくとも、これらの情報を入力する際には、入力用のフォームでSSLという暗号化を利用したデータ送信が可能になっていることを確認するようにしましょう。

多くのショッピングサイトでは、「個人情報保護方針」、「プライバシーポリシー」といったタイトルで、登録された個人情報をどのように取り扱うかということを記載しています。



また、Webサイト内に販売者の連絡先や電話番号、商品の返品や交換の可否、代金の支払い方法などの利用規約が表示されているかを確認して、そのショッピングサイトの信頼性を判断するようにしてください。

**参照** 事例12: クレジットカード番号が盗まれた



## インターネットバンキングの注意点

インターネットバンキングは、インターネットを経由して、さまざまな金融サービスを受けることが可能なサービスです。しかし、フィッシング詐欺やウイルス感染によって、ID・パスワードなどのアカウント情報が流出してしまうと、アカウントが不正利用され、金銭的被害につながるリスクも抱えています。

インターネットバンキングは、以下の点に注意して利用するようにしましょう。

### ■ IDやパスワードなどのアカウント情報を適切に設定し、厳重に管理しましょう

特にパスワードは、生年月日や電話番号などの割り出されやすい情報をそのまま使用したり、第三者の目に付く場所にメモを保管することは推奨できません。メモに残す場合は、施錠できる机の引き出しに保存するなど、盗難にも気を付ける管理をしましょう。また、インターネットバンキングで使用するパスワードは他のWebサービスなどで使い回さないことも大切です。

### ■ フィッシング詐欺に遭わないために、金融機関の本物のWebサイトかどうかを慎重に確認しましょう

フィッシング詐欺は電子メールやメッセージなどでURLをクリックさせることで偽物のサイトに誘導する手口が典型的です。インターネットバンキングを利用する場合には、こうしたリンクを直接クリックするのではなく、金融機関から通知を受けているURLをWebブラウザに直接入力するか、普段利用しているWebブラウザのブックマークに金融機関の正しいURLを記録しておき、毎回そこからアクセスするようにするなど、常に真正のページにアクセスすることを心がけましょう。

また、本物のWebサイトのドメイン名やURLを常に意識して、正しいWebサイトにアクセスしているかを確認することを心がけましょう。

サーバ証明書の確認も有効ですが、そもそも正しくない(偽物や詐欺サイトの)Webサイトにアクセスしていたら、サーバ証明書が正しくても安全ではありません。あくまでドメイン名やURLの確認が重要です。

通常、インターネットバンキングへのログイン画面では、SSL/TLSという暗号化技術を利用します。SSL/TLSで通信が行われていることは、WebブラウザのURL表示部分(アドレスバー)や運営組織名が緑色の表示になっているか、鍵マークが表示されているか、などで確認できます。SSL/TLSが採用されているかを毎回確認するようにしましょう。

### ■ インターネットカフェ・会社・学校・ホテルなど、誰が使ったか分からないパソコンでは、インターネットバンキングなどを利用するのは控えましょう

このような場所のパソコンは、パスワードを収集するための不正なプログラムに感染している可能性や、ウイルス対策ソフトが適切にインストールされていない可能性もあります。インターネットバンキングを利用する際には、不特定多数の人が利用するパソコンは使わないようにしましょう。

## ■ ウイルスによるWebブラウザの乗っ取りに注意しましょう



最近の新たな脅威として、インターネットバンキングを狙ったウイルスによる被害が発生しています。このウイルスに感染すると、Webブラウザがウイルスに乗っ取られ、正規のインターネットバンキングのやり取りに巧妙に割り込まれるという攻撃が報告されています。

ある事例では、利用者が正規の金融機関のWebサイトを見ているときに、ウイルスが偽の画面をポップアップで表示させて、口座情報やパスワードの入力を求め、ログインに必要な情報を窃取するという被害が発生しています。これはフィッシング詐欺に似ていますが異なる手口の犯罪で、利用者は正規のWebサイトにアクセスしているため、URLの確認などの通常のフィッシング詐欺の対策では、攻撃を見分けることができません。対策としては、インターネットバンキングで、通常と異なる手順を求められたり、少しでも不審な点を感じるがあれば、操作を中止し、金融機関の窓口を確認を行うなど、注意しましょう。

さらに、このウイルスでは、やり取りの割り込みに成功した攻撃者が、途中で不正な操作を挿入し、利用者が思いもよらない口座に送金を行う攻撃の存在も確認されています。この場合、利用者が攻撃を見破るのは困難です。

利用者は、こういった攻撃の存在を認識しておき、普段からウイルス対策を万全にする、金融機関などが発表する注意喚起情報に目を通す、異常に気づいたらすぐに金融機関に問い合わせるなどの対策を心がけてください。

### **参照** インターネットバンキングの仕組み(基礎知識)

IDとパスワード(基礎知識)

フィッシング詐欺に注意(一般利用者の対策)

事例12: クレジットカード番号が盗まれた

事例16: インターネットバンキングで情報が盗まれた



近年、短い文章を投稿したり、友人同士がメッセージや写真などを共有してコミュニケーション取ったりする、いわゆるソーシャルネットワーキングサービス(SNS)が普及してきました。しかし、安易な書込みがトラブルに発展したり、知り合い同士の空間であるという安心感を利用して詐欺やウイルスの配布を行う事例も急増しています。

ここではSNS利用時に想定される脅威と対策について紹介します。

### ■ 偽アカウント、架空アカウントの作成

SNSには本人確認が徹底していないサービスもあり、実在の人物・組織の名前を使った偽のアカウントや、架空のアカウントで投稿されているケースもあります。偽のアカウントや架空のアカウントを悪用して、不正リンクの投稿などが行われる事例もありますので、SNSで関わるアカウントの相手が本物であるかどうかは、慎重に確認する必要があります。

SNSサービスによっては、本人確認が行われた上で公式アカウントとして登録されているものもあります。特に公的機関や企業、著名人などの情報を購読する場合には、まず公式アカウントが存在するかを、それぞれの機関のホームページなどで確認してみるとよいでしょう。直接の知人や公式アカウント以外のアカウントで、本人確認ができない場合には、安易にフォロー（購読）したり、友達になったりしないようにしましょう。

### ■ 短縮URLの悪用



短縮URLは、SNSで文字数の制約上URLを短縮して表示する外部のサービスです。本来のURLよりも文字列が短くなり、見た目にも扱いやすくなります。しかし、一見しただけではどのようなサイトにリンクされているかわからないことから、この機能を悪用してフィッシング詐欺やワンクリック詐欺などの悪性ホームページに誘導する手口が確認されていますので、短縮URLをクリックする際には注意が必要です。心配な場合、短縮URLを元のURL表示に戻して確認することのできるWebサービスも提供されています。



## ■ スпамアプリケーションに注意しましょう



SNSのアプリケーションの中には、インストールの際に、連絡先情報へアクセスする許可を求めてくるものがあります。このようなアプリケーションの中には、個人の連絡先情報を収集して、収集したメールアドレスに迷惑メールなどを送りつけることなどを目的としているものもあります。連絡先情報へアクセスするアプリケーションで、作成者の身元やその利用目的がよくわからないものは、使用を避けるようにした方が良いでしょう。

## ■ プライバシー情報の書き込みに注意しましょう

友人間のコミュニケーションを目的としてSNSを利用しているであっても、プライバシー設定が不十分であったり、友人から引用されることなどにより、書き込んだ情報が思わぬ形で拡散する危険性もあります。インターネット上に情報が公開されていることに変わりはないということを念頭に置いて、書き込む内容には十分注意をしながら利用することが大切です。

## ■ SNSへの写真掲載による意図しない情報の流出に注意しましょう。



最近のGPS機能のついたスマートフォンやデジタルカメラで撮影した写真には、設定によっては、目に見えない形で、撮影日時、撮影した場所の位置情報(GPS情報)、カメラの機種名など、さまざまな情報が含まれている場合があります。SNSに、こうした位置情報付きの写真をよく確認せずに掲載してしまうと、自分の自宅や居場所が他人に特定されてしまう危険性があり、迷惑行為やストーカー被害などの犯罪の被害に遭う可能性もあるため、十分注意が必要です。

写真にどのような情報が含まれているか調べる方法はいくつかありますが、これらを表示するための専用のアプリケーションを利用すると、事前に確認ができます。写真に含まれている情報を編集・削除できるアプリケーションもあります。位置情報もプライバシー情報であるということを十分理解して、むやみに位置情報をつけて写真を投稿しないように心がけましょう。

また、写真に写り込む情報にも注意しましょう。特に、バーコードやQRコードには個人を特定する情報が含まれていることが多々あります。特に、郵便物の宛名に付記されているバーコードには番地までの住所情報が含まれ、簡単に読み取れます。住所の部分をマスクしても、バーコードはそのまま掲載されている例が多く、注意が必要です。

## ■ SNSの怪しい投稿のリンクに注意しましょう

SNSは誰でも投稿することができることから、怪しいリンク(ワンクリック詐欺、フィッシング詐欺など)に誘導される危険性があります。投稿した人が実在の信頼できる人であったとしても、他の人が投稿した内容をそのまま再投稿する場合がありますので、元々の情報の発信元の信頼性を意識することが大切です。

- **参照** SNS(ソーシャルネットワーキングサービス)の仕組み(基礎知識)
  - 情報発信の際の注意(一般利用者の対策)
  - 事例6: ネットストーカーに注意

## クラウドサービス利用上の注意点

クラウドサービスは、インターネット経由で情報の保存や処理などのサービスの提供を受けられる点に特徴があります。個人で意識的にクラウドサービスを利用する場合として、例えばオンラインストレージサービスを契約して、クラウドサービス上にデータを預け、自分のさまざまな端末でデータを共有したり、撮影した写真や書類などを他の人と共有したりするといった使い方が代表的です。それ以外にも、現在私たちが利用するWebメールやオンラインショッピングなど、インターネット経由のさまざまなサービスの土台として、実際にはクラウドサービスが活用されることも多くなっています。

クラウドサービス上のデータは、クラウドサービス事業者により安全に管理されることが基本ですが、実際には、障害によるデータの消失や情報漏洩(ろうえい)などの事例も発生しています。クラウドサービスを過度に信頼するのではなく、利用する場合には、想定される脅威に対応した対策を取ることが重要です。

クラウドサービスを利用する際の主な脅威としては、以下のような脅威が考えられます。

### ■ 障害などによりデータが消失する

仮にクラウドサービスに障害が発生した場合、クラウドサービス上のみデータを預けていると、大切なデータの復旧ができなくなる可能性があります。クラウドサービスを利用する場合にも、別のシステムの上に定期的にバックアップを取っておきましょう。

### ■ 預けているデータが外部に漏洩する

クラウドサービス事業者へのサイバー攻撃やその他の要因で、預けているデータが外部に漏洩する可能性があります。万が一を想定し、クラウドサービス上に預けるデータの性質を慎重に判断することが大切です。また、契約するクラウドサービス事業者のセキュリティ対策のレベルや保証の範囲などを、利用規約などであらかじめよく確認することが大切です。

### ■ クラウドサービスのアカウントが第三者に悪用される

ウイルス感染などによって、利用しているクラウドサービスのユーザIDやパスワードが流出した場合、第三者による不正アクセスにより、クラウドサービス上に保管している情報が漏洩する可能性があります。また、流出したものと同一ユーザIDとパスワードを他のサービスでも利用していた場合、そのサービスも不正アクセスを受ける危険性が高まります。ユーザIDやパスワードは、個別のサービスごとに異なるものを設定し、使い回しをしないことが大切です。



**参照** クラウドサービスとは？(基礎知識)  
IDとパスワード(基礎知識)



## 動画配信サイトなどの注意点

インターネットでは、動画を共有するサイト、リアルタイムで動画を配信しながらチャットやメッセージを交換するサイト、音楽配信サイトや、音声番組をポッドキャストで配信するサイトなど、多数のサービスが存在しています。こうしたサービスは利用者にとって大変魅力的ですが、それらのWebサイトの中には、法令違反になりかねない著作権侵害の音楽や動画が掲載されていたり、悪意のあるサイトへ誘導するものもありますので、利用する場合は注意が必要です。

### ■ 著作権法違反のリスクに注意しましょう

違法な動画配信サイトには、権利者に無断でアップロードした動画や、音楽が存在します。こうした著作権法違反の動画や音楽ファイルを、違法性を認識しながらダウンロードする行為も、著作権法違反となります。

### ■ 悪性ホームページへの誘導に注意しましょう



利用者を悪性ホームページに誘導しようとする攻撃者は、利用者にとって魅力的なサイトを構築して、利用者のアクセスを誘おうとします。例えば、主要な検索サイトで音楽を検索する際に、「Free(無料)」という言葉を追加すると、検索結果が上位に表示されるように細工して、多くの利用者の関心を誘い、ウイルスに感染させる手口が報告されています。

こうしたサイトでは、動画の再生画面やクリックボタンを模した偽の画像に、悪性サイトへのリンクを仕込み、巧妙に利用者のクリックを誘って、悪性サイトへ誘導する手口も確認されています。実際、動画配信サイトとそっくりに設計された、マルウェアを配信するWebページは多数報告されています。音楽ばかりでなく、大きな事件や人気スポーツ、映画などのキャッチフレーズで利用者を誘惑し、マルウェア配信サイトに誘導する例もありますので注意が必要です。



## オンラインゲームの注意点

オンラインゲームは、パソコンやスマートフォン・タブレット端末、ゲーム専用機器などから、インターネットを経由して、他のコンピュータとデータを交換しながらゲームを進めるという、コンピュータゲームの一形態です。オンラインゲームにはさまざまなサービス形態のものがありますが、一般的に、パッケージソフトとして購入するゲームと比較すると、オンライン上で複数の人が同時に参加・交流しながらゲームを進めることができる、最初に購入対価を支払うのではなく、月額料金やプレイ内容に応じて課金されることが多い、といった特徴があります。こうしたゲームでは、さまざまなトラブルや危険性も増えています。

例えば、子どもが親のパソコンやスマートフォンを使ってオンラインゲームをし、無料だと勘違いして有料のアイテムを購入してしまい、後になって高額な料金が請求される事例が発生しています。

また、ゲーム内で知らない人にアイテムを売って欲しいと言われ、アイテムのデータを送ったものの、相手から代金の振込がないなどのトラブルもあります。



子どもを持つ保護者の方は、子どもがインターネットの世界でどのような行動をしているのかを理解し、目を配るようにしてください。家庭内で、オンラインゲームを含めたインターネットの利用方法についてのルールを定め、年齢に見合った利用の制約を設けることも必要です。

オンラインゲームを利用する場合は、以下の点に注意しましょう。

### ■ ゲームの課金の仕組みを理解する

ゲームの利用登録は無料でも、ゲームの進行によって、アイテムが有料になるなど、料金が発生する場合がありますので、課金の仕組みをよく理解しましょう。有料課金のゲームを子どもにさせる場合には、携帯電話やクレジットカードの暗証番号、パスワードを子どもに教えず、親が管理するなどの利用方法を検討してください。

### ■ 知らない人との取引をしない

ゲーム内で知り合った人とのアイテムの交換や売買は、特に子どもの場合、その仕組みや代金の徴収方法などを理解しておらず、だまされてアイテムを窃取される場合があります。そもそも多くのゲーム運営会社では、利用規約でゲーム内での通貨やアイテムの取引を禁止しており、禁止行為を行った場合には、ゲーム自体の利用者アカウントが停止するなどの措置を取っています。

## ■ オンラインゲームの詐欺行為に注意しましょう

オンラインゲームではチャット機能を使って、悪性サイトに誘導されたり、オンラインゲームのファンサイトが改ざんされ、同じオンラインゲームをしている人がウイルスに感染したり、オンラインゲームの利用者のアイテムを窃取するなどのウイルスに感染する可能性もあります。アカウントが盗まれてアイテムが窃取されるなどの被害も多く発生していますので、こうした詐欺行為には十分注意しましょう。

## ■ チャット機能に注意する

オンラインゲーム中のチャット機能はリアルタイムに情報を交換したり、ゲームの方法などを教えあったりする場合に非常に便利な機能です。しかし、子どもたちの間でこうしたチャット機能を使って、発言のやりとりや、アイテムの交換などを行っている場合には、友達同士のトラブルになるケースもありますので、注意が必要です。また、やり取りの中で、出会い系サイトに誘導されるなど、犯罪に巻き込まれることもあるので気軽に自分の氏名などのプライバシー情報を教えることはやめましょう。





## ウイルス添付メールなどへの対応

電子メールには、文字のみで記述された「テキスト形式」と、文字の色を変えたり、写真や特殊なプログラムを盛り込める記述をした「HTML形式」という主に2種類の方式があります。これに他のソフトを起動して読むことのできる「添付ファイル」を添えることができます。

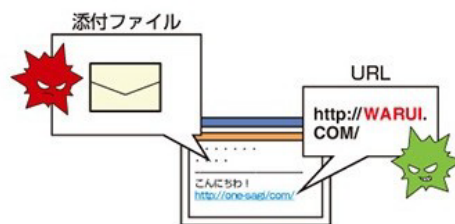
単なる文字だけのテキスト形式のメールでウイルスに感染することはありませんが、HTML形式のメール又は添付ファイルに含まれるウイルスは、パソコンの情報セキュリティ対策が不十分だった場合、これらのメール又はファイルを開くだけで感染してしまいます。

添付ファイルは、ファイル名の拡張子である程度判別でき、例えばWindowsでは、.exe.com.regなど開くことでプログラムが実行されたりシステムの設定が変更されたりとリスクが高いファイルもあります。ただし、拡張子を見るだけでウイルスを防げるものではありません。ソフトウェアを最新にしていれば、リスクの高いファイルを開こうとしたときに警告を表示するものも多いので、安易に続行しないで判断することが大切です。

### ■ 感染してしまうケース

- パソコンのOS、その他ソフトウェアが最新の状態になっていない。● ウイルス対策ソフトがパソコンにインストールされていない。
- ウイルス対策ソフトのパターン定義ファイルが最新の状態に更新されていない。

添付ファイルを開く時には、あらかじめウイルス対策ソフトで添付ファイルがウイルスに感染していないかを確認しましょう。



また、電子メールやSNSなどのメッセージにURLを記載して、あらかじめ用意した悪性ホームページに誘導し、感染させる手口もあります。悪性ホームページは、例えばネットショッピングや、オンラインバンキングなどのホームページを偽装したいわゆるフィッシングサイトの場合もありますし、わざとウイルスを感染させるために、不正なプログラム(ウイルスやボット)を仕込んだホームページもあります。具体的には、ホームページなどで「あなたのコンピュータはウイルスに感染しています」のようなメッセージを表示し、偽のウイルス対策ソフトのダウンロード用Webサイトに誘導して、ウイルスをインストールさせる事例などが発生しています。



## 迷惑メールへの対応

受信者が望んでいないにもかかわらず、一方的に送信されてくる電子メールのことを迷惑メールと呼んでいます。いわゆる「出会い系サイト」やドラッグなどの商品の宣伝などを内容とする電子メールが多く、スパムメールとも呼ばれます。



これらの電子メールは、昼夜を問わずに届けられ、電子メールをダウンロードするために時間がかかるなど、受信者側に大きな負担をかけるため、最近では社会問題のひとつになっています。また、いやがらせのために送りつけられる大量の無意味な電子メールも、迷惑メールの一種といえます。

迷惑メールの対策としては、ホームページのアンケートや電子掲示板などにメールアドレスをむやみに掲載しないことや、使用するメールアドレスは、わかりにくいものにするなどが考えられます。

さらに注意が必要なのは、このような迷惑メールで送信される内容をうかつに信用してはいけないということです。これらの電子メールの中には、無限連鎖防止法に抵触するもの(いわゆるねずみ講)や詐欺行為を目的としているものもあります。

最近では、携帯電話やSNSのメッセージでの迷惑メールの急増が問題化しています。このような迷惑メールを受信しないようにするためには、

- 長く複雑なメールアドレスを使用する。
- 指定したドメインやメールアドレスからの電子メールのみ受信するように設定する。
- 必要以上に自分のアドレスを他人に漏らさない。
- SNSのメッセージでの迷惑メールの場合は、利用しているSNSサービスの機能を使って、メッセージを拒否する、もしくは相手をブロックする。

など、利用者側でできる自衛策も大変有効です。携帯電話による迷惑メール対策の一環として実施してみましょう。

携帯電話番号を使って送られてくるSMS(ショートメッセージサービス)の迷惑メールの場合は、携帯電話会社のサービスを使って、電話番号によるブロック設定をすることが有効です。


また、パソコンの場合には、以下のような対応策が考えられます。

- インターネットサービスプロバイダでメール受け取りの拒否条件設定による受信制限をかける。
- インターネットサービスプロバイダによる迷惑メールフィルタを使用する。
- 統合セキュリティ対策ソフトによる迷惑メールフィルタを使用する。

迷惑メールフィルタを使用すると、電子メールの内容を分析して、迷惑メールと判断された場合には、件名に「SPAM」や「MEIWAKU」などの文字列が追加されます。電子メールソフトで、件名にこれらの文字列が付けられた電子メールを自動的に分類する設定を行うことで、迷惑メールを通常の受信用ボックスから除外することが可能になります。ただし、迷惑メールフィルタは、定められたロジックや蓄積された情報によって迷惑メールであると判定するため、常に正しい判断が行われるわけではないという点に注意しなければなりません。

なお、受信者の望んでいない広告メールを送信する際には、「今後送信を必要としない場合にはこちらのメールアドレスまでご連絡ください」といった内容を記載することが法律で義務付けられていますが、その意思を伝える際には、相手側に氏名・住所などをむやみに開示しないように気を付けましょう。悪意を持って、迷惑メールを送信してくる業者は、このような意思を伝えた際に、その送信元の電子メールアドレスが使われていることを確認できることにもなります。そして、その後も迷惑メールが送信され続けるという被害も起こっています。

**参照** 特定電子メールの送信の適正化等に関する法律(基礎知識)

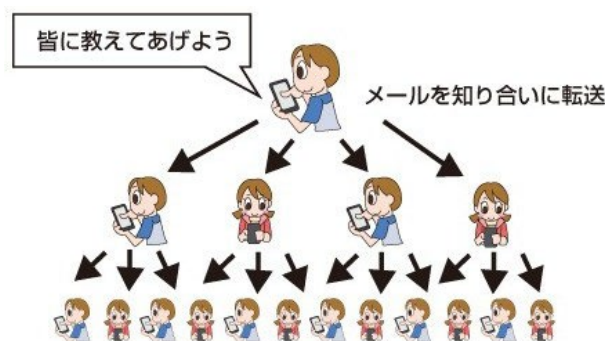
迷惑メール相談センター 



## チェーンメールの問題点

チェーンメールとは、電子メールを受け取った人が次々に知人に電子メールを転送することで、ねずみ算式に広まっていく電子メールのことです。多くの場合、チェーンメールには、「すぐに友達に教えてあげてください」や「できるだけ多くの人に広めてください」「すぐに10名に転送しないと、あなたは不幸になります」などのように、電子メールの転送を促す言葉が付いています。

チェーンメールの内容は、ほとんどがデマ情報やいたずらであったり、「あるテレビ番組の企画です」「すぐにお金儲けができます」など詐欺的な内容のものですが、募金の呼びかけや輸血のお願いなど、本来は善意の電子メールがいつの間にかチェーンメールとして広まってしまうケースもあります。最近では、SNSでも同様に、リツイートやシェアなどの機能で、デマ情報が広まってしまうケースが出ています。



チェーンメールへの対策としては、身に覚えのないメールや不審なメールが送りつけられてきたら、まず次のことはしないように心掛けましょう。

- メールのURLはクリックしない
- メールの添付ファイルは開かない
- メールに返信しない
- メールは転送せず、削除する

こうしたチェーンメール対策は、自分自身が被害にあわないようにするとともに、被害をそれ以上広げないための重要なマナーです。相手にメールの転送を強要する行為は、メールの内容にかかわらず、迷惑行為であるといわざるをえません。人間関係や信用に傷がつくことにもなりかねませんので、勇気を持って転送しないようにしましょう。

**参照** 事例4: 猛威！デマウイルス



## メールの誤送信

電子メールはメッセージやデータを簡単に交換できる利便性の高いサービスですが、送り先を間違えてしまうと、他人にメールが届き、結果的に情報漏洩(ろうえい)につながってしまう危険性もあります。また、複数の相手に同時にメールを送る際に、操作を誤って、本来は秘密にしなければならないそれぞれのメールアドレスが見える状態で送ってしまった場合も、やはり情報漏洩につながります。



電子メールを送る場合、まずはTO:、CC:、BCC:の違いを理解する必要があります。TO:やCC:は、電子メールを受け取った人には、自分以外の誰宛てに送信されたメールかがわかります。このため一度に複数の人宛てに送る場合で、他の人のメールアドレスがわかると困る場合はBCCを使います。この利用方法を間違えると、関係のない第三者にメールアドレスが知られてしまい、情報漏洩事案となってしまう可能性があります。

電子メールの誤送信の対策は、以下のとおりです。

- メールアドレスの宛先(TO:、CC:、BCC:)の設定を間違えないように利用する。
- プライバシー情報が含まれた電子メールを安易に送信しない。
- 誤送信した場合に第三者に電子メールを見られる可能性があるため、添付ファイルなどを送る場合は、ファイルを暗号化したり、添付ファイルにパスワードを設定する。
- メールアドレスの誤入力など、意図しない宛先に電子メールが送信されてしまうことを防ぐため、送信する際に宛先などを確認する画面を開くように、あらかじめ電子メールソフトに設定する。



## 家族共用パソコンの注意点



パソコンを家族で共用して使用している場合、家族の誰かが勝手にファイル共有ソフトをインストールしたために、情報が漏洩(ろうえい)したなどの事故も起こっています。こうした事故を防ぐために、家族共用のパソコンを使う場合は以下の点に注意しましょう。

### ■ アカウントの共有はしない

パソコンを購入したら、家族の一人ずつに一般ユーザ権限のアカウントを作成し、アカウントの共有はしないようにしましょう。これは、万が一、家族の誰かがウイルスに感染したり、ファイル共有ソフトを導入したとしても、別の家族のデータに影響が及ぶ可能性を低くすることができるためです。

### ■ 管理者権限ではなく一般ユーザ権限で利用する

管理者権限は、ソフトウェアのインストールなど、必要な時だけ使用し、通常時には一般ユーザ権限で使うようにしましょう。これにより、危険性の高いソフトウェアを家族が不用意に導入する可能性を低くすることができます。また、最近では、子どもの利用内容を保護者が制限できる機能を備えた機種も登場しています。

**参照** ファイル共有ソフトとは？(基礎知識)





## 携帯電話・スマートフォン・タブレット端末の注意点

最近では携帯電話にかわり、スマートフォンの利用が急増しています。スマートフォンは、従来の携帯電話に比べてパソコンに近い性質を持った情報端末です。大切な仕事上のデータや、位置情報などのプライバシー情報がスマートフォンに保存されるようになったことで、情報漏洩(ろうえい)が発生した場合のリスクがいつそう大きくなっています。また、スマートフォンは、アプリケーションをインストールすることで、さまざまな機能を追加することができます。この便利な性質が、一方でパソコン同様、スマートフォンがウイルスに感染するリスクを生んでいます。

タブレット端末はスマートフォンよりも大きな画面の携帯用端末ですが、性質はスマートフォンとよく似ており、アプリケーションのインストールにより機能の追加が可能である一方、ウイルスに感染する危険性があります。

スマートフォンやタブレット端末はとても便利であるからこそ、安心して利用するためには、常にパソコンと同様に情報セキュリティ対策に気を配りましょう。

### ■ 携帯電話・スマートフォンの盗難や廃棄に注意しましょう

携帯電話・スマートフォンは持ち歩いての利用も多く、紛失したり盗難にあったりする可能性が高くなります。そのような対策として、本人しか使用できないようにパスワードロックをかける機能や、遠隔ロックする機能を利用することが有効です。また、企業や組織などで利用している端末を紛失した際には、管理者にすぐ連絡して、指示を仰ぐなどの対応をしましょう。

なお、携帯電話・スマートフォンに保存された情報を集めることを目的として、廃棄された端末を売買するといった事例も発生しています。携帯電話・スマートフォンを廃棄する際には、必ず登録されているアドレス帳や電子メールなどの情報を、確実に消去してから廃棄するようにしてください。端末販売店で回収をしていることも多いので、そうした信頼できる事業者に廃棄を依頼するか、安全に廃棄できるリサイクル業者を選んで廃棄を依頼すると良いでしょう。

### ■ OSやアプリケーションを最新にしましょう

スマートフォン・タブレット端末のOSやアプリケーションにはパソコンと同様に脆弱性(ぜいじゃくせい)が報告されることがあります。OSやアプリケーションの更新の通知が来たら、忘れずインストールするようにしましょう。

### ■ ウイルス対策ソフトの利用を検討しましょう

スマートフォンを狙ったウイルスが発見されています。ウイルスは通常、アプリケーションの中に紛れ込ませる形で配布されており、これまでに、勝手にSMS(ショートメッセージサービス)の送信を行うものや、ワンクリック詐欺の機能を持つものなどが見つかっています。スマートフォンには機種に応じてウイルス対策ソフトが提供されていますので、ウイルス対策ソフトを入れることを検討してください。



## ■ 信頼できないアプリケーション提供サイトに注意しましょう

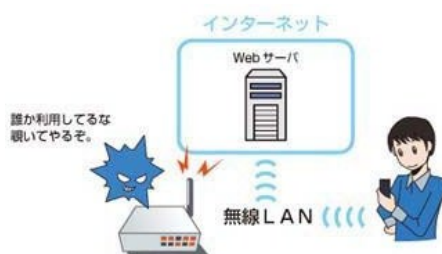


通常、アプリケーションは契約している携帯電話会社やOS・機器メーカー等の公式サイトからダウンロードして利用しますが、スマートフォンの機種によっては、それ以外のサイトから自由にアプリケーションをダウンロード可能なものもあります。最近のアプリケーションには、ウイルスだけでなく、端末情報や電話帳内の情報などを十分な説明なく収集するものもあり、これらのアプリケーションによって電話帳内の情報が流出してしまった場合、自分だけでなく友人などにも被害を及ぼすことになってしまいます。特に、運営者の身元が明らかでないサイトからアプリケーションをダウンロードすることは、こうしたアプリケーションが含まれている可能性があるため、非常に危険です。また、最近では、公式サイトに似せた偽のアプリケーション提供サイトの出現も報告されていますので、ダウンロードの際には注意しましょう。

## ■ アプリケーションの権限、利用条件などを確認しましょう

アプリケーションの中には、利用者の情報を収集するために、スマートフォン内の電話帳情報などを取得するものがあります。インストールする前には、アプリケーションの説明をよく読んで、そのアプリケーションがスマートフォン内のどのような情報や機能にアクセスするのかの表示をよく確認することが必要です。また、インストール時には、本来そのアプリケーションでは使う必要がないと思われる情報（連絡先情報、所有者情報、位置情報など）を収集しようとする確認画面が出てくる場合があります。インストール時に自分の情報の取り扱い方に不安がある場合は、アプリケーションの利用をあきらめることも検討すべきです。

## ■ 無線LANアクセスポイントに注意



携帯電話やスマートフォン・タブレット端末には無線LANの接続機能が付いています。これらのアクセスポイントは無料のものや有料のものもありますが、なかにはわざと無料のアクセスポイントに見せかけて情報を盗み取るような不正なアクセスポイントがある可能性があります。無線LANアクセスポイントに自動的に接続しない設定にするなど、日常的に普段使用している無線LANアクセスポイント以外にはできるだけ接続しないようにしましょう。

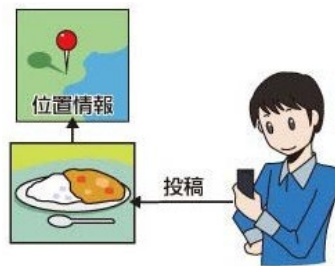
## ■ OSの改造はやめましょう

スマートフォン・タブレット端末はOSやソフトウェアを変更することで、通常ではインストールできないソフトウェアをインストールできる場合もあります。こうしたソフトウェア上の改造を行った端末は、本来のセキュリティレベルを下げ、ウイルス感染の危険性が高まるだけでなく、メーカーのサポート対象外となる可能性があります。また、本来は禁止されているサイトから、不正なアプリケーションをインストールしてしまう危険性も高まります。改造は行わないようにしましょう。

## ■ のぞき見に注意しましょう

携帯電話、スマートフォン・タブレット端末は、電車や、バスの移動中など人目に触れやすいところで操作する場合、後ろからのぞき見されるなどの危険性もあります。人混みの中ではアカウント情報の入力などの機微な操作を行わない、画面操作時に周りの視線に注意する、のぞき見防止シールなどを貼る、などの対策を意識しましょう。

## ■ 写真の位置情報に注意しましょう



スマートフォン・タブレット端末のようなGPS機能を搭載した端末で撮影した写真には、設定によっては、目に見えない形で、撮影日時、撮影した場所の位置情報(GPS情報)、カメラの機種名など、さまざまな情報が含まれている場合があります。SNSなどに、こうした位置情報などが付いた写真をよく確認せずに掲載してしまうと、自分の自宅や居場所が他人に特定されてしまう危険性があり、迷惑行為やストーカー被害などの犯罪の被害に遭う可能性もあるため、十分注意が必要です。事前に使用している端末の設定を確認しておくようにしましょう。

## ■ スマートフォンを使うとき、周囲の状況にも注意しましょう

歩きながらなど、移動しながらスマートフォンを操作していると、周囲の状況に対して不注意になり、トラブルにつながる場合もあります。周囲に迷惑をかけないように、移動しながらの利用は控えましょう。

**参照** ソフトウェアを最新に保とう(一般利用者の対策)

無線LANの安全な利用(一般利用者の対策)

## ゲーム機の注意点

最近のゲーム機の多くは、無線LANなどを通じて、インターネットに接続できる機能を持っています。この機能を使って、インターネット経由で対戦ゲームをしたり、アプリケーションをダウンロードしたりすることができます。専用のWebブラウザを備え、インターネット上のホームページを閲覧できる機能を備えたものも登場しています。



ゲーム機は、パソコンやスマートフォンなどと同様に、次第に子どもたちがインターネットに触れる際の主要な媒体の一つとなってきています。インターネット上にはさまざまな有害サイトが存在しているため、子どもがゲーム機でインターネットを利用する場合、年齢に合わせた閲覧制限（フィルタリング、ペアレンタルコントロール）などの対策を取ることが推奨されます。

また、携帯型ゲーム機の場合、外部へ持ち出して無線LANに接続することができます。ゲームメーカー側でも、このような利用形態を推進しており、ファーストフード店や家電量販店、大型スーパーなどには、ゲームメーカー公式のWi-Fiスポットなどが整備されるようになりました。

他方で、街中には、無料の公衆無線LANや、一般家庭の無線LANアクセスポイントからの漏洩電波、テザリング機能付きのスマートフォンの電波など、さまざまな無線LANの接続機会があります。このような無線LANアクセスポイントの中には、悪意があるもの、セキュリティ設定が不十分なものが含まれている可能性があり、そのような無線LANに接続すると、通信内容を盗聴されるなどの脅威が発生する可能性があります。

インターネット接続できるゲーム機では、パソコンでの利用と同様にリスクがあることを理解し、以下のようなセキュリティ対策をすることが必要になります。

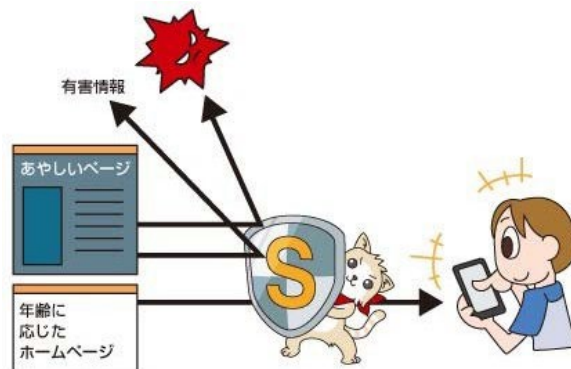
### ■ フィルタリングやペアレンタルコントロール（視聴年齢制限）をゲーム機に設定しましょう

フィルタリングは、子どもがインターネットを利用する際、有害サイトへのアクセスをブロックする機能です。フィルタリングソフトは、パソコン向け、スマートフォン向け、ゲーム機向け、ブロードバンドルータや無線LANアクセスポイント向けなど、利用者の利用環境に合わせて、さまざまな機器向けの製品が開発されています。家庭内でフィルタリングが必要な機器により、サービスの選択を検討してみてください。

ただし、携帯型ゲーム機は、街中で使うことが想定されるため、ゲーム機本体ではなく、家庭内のブロードバンドルータなどでフィルタリングを実施している場合には、外出先ではフィルタリングが機能しない点に留意すべきです。ゲーム機本体へのフィルタリング機能の導入も検討した方がよいでしょう。

ペアレンタルコントロールは、子どもの情報機器の利用を保護者が制限し、管理する考え方です。ゲーム機に備えられているペアレンタルコントロール機能を使用し、子どもに悪影響を及ぼす可能性のあるゲーム利用や、アイテムなどの購入、インターネットの利用を制限することができます。

一度ペアレンタルコントロールを設定すると、子どもが制限された機能を使用したり、制限されたサイトに接続しようとした場合には、事前に設定した、暗証番号やパスワードなどの入力が必要されます。こうした暗証番号やパスワードは保護者がしっかり管理することで、子どもの利用制限をすることが可能です。



#### ■ 家庭内でのルールを明確化しましょう

フィルタリング機能は、子どもの年齢にあわせて、閲覧できるサイトを変更することもできます。子どもの成長やリテラシーの向上に合わせたセキュリティ対策を実施しましょう。

また、ゲーム機の利用や、ゲーム機以外のパソコンや携帯電話・スマートフォンなども含めたインターネットの利用については、子どもと一緒に話し合い、家庭内でルールを決め、それを守らせるようにすると良いでしょう。

#### ■ 怪しいアクセスポイントに接続しない

街中で悪意のある無線LANアクセスポイントなどに接続しないために、あらかじめ家庭内のルールで、外出先ではインターネットに接続しない、または、利用してもよい事業者のアクセスポイントを決めておくなどして、ルールを守らせることが有効だと考えられます。



## インターネット対応機器(家電、記憶媒体等)の注意点

最近のインターネット対応機器(デジタルカメラや携帯音楽プレイヤー)、さらには手の中に隠れるほど小さなサイズのUSBメモリやSDカードなど、自宅や取引先とのデータのやり取りにこうした外部記憶媒体などを利用するケースが増えてきています。特にUSBメモリは、コンピュータのUSB端子に接続するだけで手軽に利用でき、多くの利用者に支持されています。



しかし、小さくて持ち運びが楽であるため、紛失してしまう危険性が高いという点に注意しなければなりません。また、データをそのままメディアに記録していた場合、紛失時にメディア内の情報が漏洩(ろうえい)する危険性が非常に高くなります。もちろん、このことは外付けハードディスク、CD-R、DVD-Rなど、持ち運び可能なメディア全般について言えることです。

これらの持ち運び可能なメディアを外部へ持ち出した際には、以下のような危険性が考えられます。

- メディアを入れたカバンを置き忘れることにより紛失して情報漏洩
- ワイシャツのポケットなどに気軽に入れておいたために紛失して情報漏洩
- USBメモリやSDカードを媒介するウイルスにより、ウイルスに感染
- 自宅のパソコンにデータを移して作業。その後、ウイルスに感染して情報流出

こうした可搬性のあるメディアを利用する際の情報漏洩に対するリスクを軽減するためには、次のような対策が考えられます。

- 盗難、紛失に備えて、持ち運ぶ必要のない機密情報、プライバシー情報は保存しない。
- ファイルは、できるだけ暗号化して保存する。

暗号化の仕組み以外では、パスワード付きの圧縮ファイルや、ドキュメントの保存時にパスワードを付けるなどの対応も有効です。ただし、簡単なパスワードでは意味がありませんから、推測されにくいパスワードにする必要があります。

- USBメモリや外付けハードディスクでは、製品に情報セキュリティ対策機能の仕組みやソフトウェアが装備されているものも多いので、外部に持ち出すために利用する場合にはできるだけそのような製品の購入を検討しましょう。

最近ではスマートフォンやタブレット端末と連携する機能をもった家電製品(テレビ、冷蔵庫、空調など)が発売され、普及しつつあります。こうしたインターネット技術を利用した機器の場合、その操作端末にもなるスマートフォン・タブレット端末も安全に利用する必要があります。万が一スマートフォン・タブレット端末がウイルスなどに感染した場合、家電製品などの誤動作の原因にもなりかねません。スマートフォン・タブレット端末の注意点にもあるように、セキュリティ対策を適切に行って、利用することが必要です。

**参照** ウイルスの感染経路と主な活動(基礎知識)

携帯電話・スマートフォン・タブレット端末の注意点(一般利用者の対策)





## ファイル共有ソフトの利用とその危険性

ファイル共有ソフトとは、インターネットを利用したP2P(Peer to Peerーピア・トゥー・ピア)でファイルをやり取りするソフトウェアのことです。利用者は、インターネットに接続された自分のコンピュータに、ファイル共有ソフトを導入することで、他の利用者とファイルをやり取りすることができるようになります。

ただし、ファイル共有ソフトは、自動的にファイルを送受信する仕組みであるため、違法なファイルのやり取りに利用されたり、ウイルスの感染によって、公開するつもりのないファイルがインターネットに流れてしまったりといったトラブルが数多く発生しています。このような被害を防ぐもっとも確実な対策は、公私ともにファイル共有ソフトを使わないことです。



もっとも重要視しなければならないことは、ウイルスに感染した場合の危険性とその被害の大きさです。ファイル共有ソフトを利用しているということは、インターネットに自分のコンピュータを公開してしまう可能性があるということです。感染したウイルスによって、公開用に設定していたフォルダ以外のフォルダを公開するように変更されてしまうと、コンピュータのハードディスクの中身が全てインターネットに流出してしまう危険性さえもあります。つまり、ファイル共有ソフトを利用しているコンピュータでは、通常のホームページの閲覧や電子メールの利用に比べて、情報漏洩(ろうえい)の危険性が格段に高くなるというわけです。

また、ファイル共有ソフトでは、それぞれのファイルの複製がネットワーク内に大量に作成される可能性があるため、複製された全てのファイルを完全に消去することは事実上不可能です。このことが、情報漏洩の被害を拡大させる大きな要因となっています。

以上のように、ファイル共有ソフトの利用は非常に情報漏洩のリスクが高いということを認識してください。

もうひとつ理解しておかなければならないのは、著作権侵害に対する問題です。多くのファイル共有ソフトは、収集したファイルを再度インターネットに公開する仕組みを持っています。つまり、最初は収集したファイルであっても、後からそれらのファイルを自分のコンピュータから公開することにより、著作権侵害で訴えられる可能性があるということです。

パソコンを家族で共有して使っている場合、家族の誰かが勝手にファイル共有ソフトをインストールしてしまったために、情報漏洩に至った事件も起こっています。ファイル共有ソフト使用については、家族にも徹底が必要です。できれば家族共有のパソコンを使う場合は以下の点に注意しましょう。

- 家族共有のパソコンでも、アカウントは共有しない。  
家族のアカウントは一人一つずつ、別々に作成して利用しましょう。



●管理者権限ではなく、一般ユーザ権限で利用する。

家族や子どもに使用させるアカウントにはユーザ権限を設定し、勝手にソフトウェアをインストールされない設定で利用しましょう。

**参照** ファイル共有ソフトとは？(基礎知識) 著作権法(基礎知識)

事例13: ファイル共有ソフトが原因で・・・



## 一般利用者の対策

### Ⅲ.情報発信の際の注意

---

近年、個人がホームページやブログ、SNSなどを通じて、インターネット上で情報発信をすることが一般的に行われるようになりました。自分の考えや日常生活などを手軽に多くの人と共有できること、また、多くのサービスの場合、自分の投稿に対する読者からの反応をすぐに確認できることなどが、利用者にとっての大きな魅力になっています。

その一方で、これらの情報発信に際して、さまざまなトラブルも起きています。ここでは、インターネットを利用して情報発信をする際の注意点、トラブルと対策について説明します。

ここでは、ブログやSNSなど、インターネット上で既に提供されている専用プラットフォームを利用して情報発信を行う場合を想定しています。自宅に自分自身でWebサーバを設置して、インターネット回線に接続している場合には、さらに多くの情報セキュリティ対策が必要となりますので、情報管理担当者の情報セキュリティ対策などを参考にしてください。

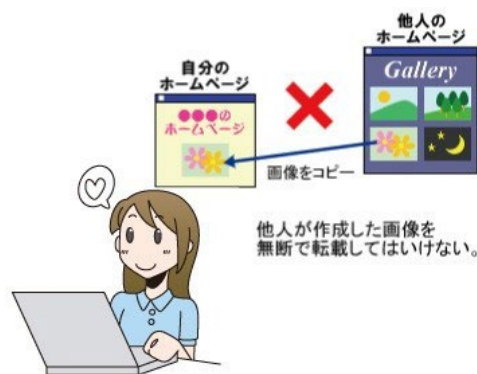


## 著作権侵害に注意

情報を発信する際には、著作権の侵害に注意しなければなりません。写真、イラスト、音楽など、インターネットのホームページや電子掲示板などに掲載されているほとんどのものは誰かが著作権を有しています。これらを、権利者の許諾を得ないで複製することや、インターネット上に掲載して誰でもアクセスできる状態にすることなどは、著作権侵害にあたります。また、新聞や雑誌などの記事にも著作権があり、引用の範囲を越えて掲載すると著作権侵害にあたるため、注意しましょう。

また、人物の写真などの場合は、撮った人などが著作権を有するだけでなく、写っている人に肖像権があるため、ホームページに掲載する場合にはこれら全ての権利者の許諾が必要になる場合があります。

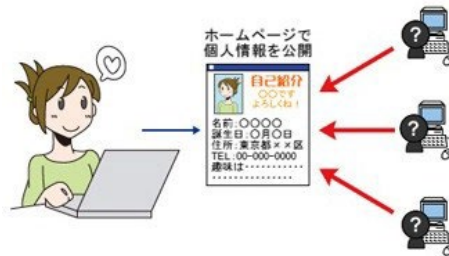
情報を発信する際に、市販の素材集(絵や写真など)やインターネットに素材を提供しているホームページなどでは、これらを利用する場合に権利者による許諾の必要がない旨を記載されていることがあります。しかし、そのような素材であっても、商業利用については制限がかけられていることがあるため、必ず規約をよく読んでから利用するようにしましょう。





## プライバシー公開の危険性

インターネットで公開した情報は、いろいろな人が閲覧する可能性があります。そのため、インターネット上で、氏名、年齢、住所、電話番号、自分の写真といった作成者自身の個人に関する情報を公開することの危険性について、きちんと認識しておかなければなりません。



たとえば、住所や電話番号が公開されていれば、そのホームページを見た人があなたに興味を持って、自宅の周りをうろついたり、電話をかけてきたりといったストーカー行為を行うかもしれません。また、公開している情報を収集され、迷惑メールや振り込め詐欺などの別の犯罪に利用される可能性もあります。

そのような被害から身を守るためには、何よりもインターネット上では、むやみに個人に関する情報を公開しないようにすることが大切です。最近では、検索技術の向上により、たとえあるサイトで公開している情報が断片的なものであっても、インターネット上のさまざまな情報を組み合わせることで、あなた個人を特定する情報を探し出すことができる可能性が高くなっています。また、一度インターネット上に公開された情報が、コピーにより拡散していった場合、それを完全に削除することは困難です。

以上のような観点から、個人に関する情報の公開の判断は、非常に慎重に行うべきです。さらに、自分以外の家族や他人の個人に関する情報を、本人の許可なく掲載することは、厳に慎まなければなりません。

個人に関する情報の公開にあたって、問題となりやすい事例と対策には、以下のようなものがあります。なお、自分の情報が他人に書き込まれた場合の対策については、「ネットを使いたいやがらせや迷惑行為」のページを参照してください。

### ● ネットストーカーによる被害

インターネットの世界においても、実社会と同様にストーカー被害が急増しています。現実世界でのつきまといや、取得されたプライバシー情報が他のWebサイトへの誹謗中傷などに利用される場合があります。こうした被害が深刻な場合には、最寄りの警察に相談しましょう。



SNSのような、基本的には特定の友人だけに公開しているサイトの場合であっても、個人に関する情報の公開には注意が必要です。SNSのプライバシー設定が不十分であったり、友人側の操作などにより、自分の意図しない範囲まで情報が広まってしまう事例が発生しています。SNSとはいっても、インターネット上に個人に関する情報を公開していることにかわりはなく、自分の手の届かないところへ拡散していく危険性があるということを念頭に置いて、投稿内容を判断すべきです。

また、特にSNSの場合、写真などの投稿により、友人のプライバシー情報を公開することになる点にも留意が必要です。どの情報を他人に公開しても良いと考えるかの基準は、人により異なります。友人に関する情報を掲載する場合には、事前に許可を取ることを原則とするべきでしょう。

● メールアドレスの公開

ホームページなどでは、問い合わせ先としてメールアドレスを掲載する場合がありますが、公開しているメールアドレスには、大量の迷惑メールが送られる事例が多く発生しています。Webサイトで公開されているメールアドレスを自動的に検索・収集するプログラムが存在し、悪用されているためです。これへの対策としては、まずは、公開用のメールアドレスには、普段利用しているメールアドレスとは別の専用のアドレスを用意しましょう。そして、上記のプログラムに検知される確率を少なくするため、「@」を「\_atmark\_」などと表記する、メールアドレスを画像ファイルとして表示するなどの対策が有効です。

**参照** SNS利用上の注意点（一般利用者の対策）

事例6: ネットストーカーに注意

## ネットを使いたいやがらせや迷惑行為

ここでは、ホームページやブログ、SNSなどのコメント欄や電子掲示板など、インターネット上の情報発信機能を使いたいやがらせや迷惑行為について取り上げます。

コメント欄や電子掲示板などの場所では、個人を誹謗中傷する内容の書き込みや、無意味な文字の貼り付け、不正な動作を行うHTMLタグの書き込みなどの迷惑行為(いわゆる「荒らし」)を受けることがあります。悪意を持って、特定個人に関する情報が書き込まれる場合もあります。このような迷惑行為への対策としては、以下が考えられます。

### ■ 自分の管理するWebサイト上での迷惑行為への対策

自分の管理するWebサイト上に情報発信機能がある場合には、まず迷惑行為への事前の対策として、Webサイト上に、迷惑行為の禁止や「不相当と思われる発言は削除します」といった旨をはっきりと明記しておくようにしましょう。そして、これらの行為を発見したら、書き込みの削除の対応をとりましょう。

電子掲示板のプログラムによっては、禁止用語の設定、特定のコンピュータからのアクセス制限、連続書き込みの禁止などの対策が可能になっているものもあります。電子掲示板のプログラムの利用方法をよく調べて、これらの対策を検討してみましょう。

悪質な迷惑行為を受けた場合には、電子掲示板のログから、投稿日時、投稿者のコンピュータ名、IPアドレス、投稿内容の情報を抜粋して保管しておくようにしましょう。抜粋したログを調べて、相手が接続しているインターネットサービスプロバイダや企業の管理者に連絡することも対策手段のひとつとなります。

いずれにしても、いやがらせへの対策は、Webサイトの管理者本人が行わなければなりません。管理者であることの責任と権限をよく検討して、対応策を立てるようにしてください。自分のWebサイトに、他人の権利やプライバシーを侵害するような内容の書き込みが行われる場合もあります。その場合に備えて、外部からの問合せを受けられることができる専用のメールアドレスなどをWebサイト上に記載しておきましょう。

### ■ 自分の管理下でないWebサイトにプライバシー情報や誹謗中傷が書き込まれた場合の対策



インターネット上に、自分の個人情報や誹謗中傷の書き込みがされているのを発見した場合には、書き込みに関する証拠(サービス名、URL、書き込み番号など)を保存した上で、サイトの管理者などに削除依頼をしましょう。自分で対応するのが不安な場合は、まずは専門の相談窓口にお問い合わせるのが良いでしょう。

削除依頼の詳しい手順や相談窓口は、以下のサイトなどを参考にしてください。

[インターネットホットライン連絡協議会](#)

[違法・有害情報相談センター](#)

[法務省インターネット人権相談受付窓口](#)



## 発信内容は慎重に

SNSなどのツールは、日常生活の中で、リアルタイムでの個人の思いなどを投稿できる点が大きな魅力です。しかし、その一方で、個人の何気ない発言でも、インターネット上の発言やふるまいは、多くの人の目に触れる可能性があり、場合によっては、現実世界に大きな影響を与えることがあります。

例えば、ある職員が勤務時間中にしたSNSへの投稿が、本来は秘密にするべき職務の内容を外部に漏らしてしまう結果となり、インターネット上で職員自身に非難が集中したり、その組織全体の問題として取り上げられる事例が発生しています。このような場合、しばしば、インターネット上のその問題に関心を持つ人の間で責任追及活動が行われ、その過程で、非難の対象となった個人の特定・暴露や、誹謗中傷などの大量の書き込み(いわゆる「炎上」)などの行為が行われます。そして、インターネット上でこのような現象が発生した場合には、新聞やテレビなどのマスメディアで報道されることも珍しくありません。

こういった危険性を回避するためには、まずは自分のインターネット上での発信内容が、本来秘密にすべき事項を含んでいないか、現実世界でも避難を浴びるような内容でないかなど、毎回立ち止まって考える慎重さが必要です。

さらには、こうした個人の特定が行われるのは、SNS上の情報発信だけではなく、悪ふざけのつもりで投稿された動画から、投稿者の特定が行われ、現実世界での謝罪に至った事例も発生しています。今やインターネットは匿名の空間ではなく、インターネット上の行動は特定されてしまうものだということを自覚することが必要です。



## このテキストに関する問い合わせ先

総務省 サイバーセキュリティ統括官室  
Email:kokumin-security@ml.soumu.go.jp

- 国民のための情報セキュリティサイト  
[https://www.soumu.go.jp/main\\_sosiki/cybersecurity/kokumin/index.html](https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/index.html)
- キッズページ  
[http://www.soumu.go.jp/main\\_sosiki/joho\\_tsusin/security/kids/](http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/kids/)
- このテキストの利用規約  
[https://www.soumu.go.jp/main\\_sosiki/cybersecurity/kokumin/guide.html](https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/guide.html)