



総務省

国民のための情報セキュリティサイト



「エンドユーザー」の情報セキュリティ対策：一般利用者

一般利用者のための情報セキュリティ対策

現在のインターネットの一般的な使い方は、電子メールの利用、ホームページからの情報収集、ショッピングサイトの利用などです。これらの一般的な利用方法において、どのような情報セキュリティ対策が必要なのでしょうか。

💡 インターネットの匿名性	2
個人情報の取り扱い	3
プライバシーの保護	4
ウイルスに注意	5
悪意のあるホームページ	7
ソフトウェアを最新に保とう	9
ネットオークションにおける危険性	10
ショッピングサイトの利用	11
チェーンメールの問題点	12
迷惑メールへの対応	13
常時接続の危険性	15
スパイウェアに注意	16
フィッシング詐欺に注意	17
携帯電話におけるセキュリティ確保の重要性と対策	18
ファイル共有ソフトの利用とその危険性	19
ワンクリック詐欺の概要	21
USB メモリからのウイルス感染	23
ボットの危険性と対策	24
💡 インターネットにおける安全性の確保	25

※特に重要な項目には 💡 マークがついています。



総務省

国民のための情報セキュリティサイト



「エンドユーザー」の情報セキュリティ対策：一般利用者

インターネットの匿名性



重要!

インターネットに接続するときには、あなたのコンピュータに識別番号としてIPアドレスという全世界で固有の番号が割り当てられます。このIPアドレスはデータの送受信の際に必ず利用されるため、たとえば電子掲示板に書き込みを行った場合には、その電子掲示板を管理しているWebサーバーにあなたの使用しているコンピュータのIPアドレスが記録されます。

なお、ホームページを閲覧した場合には、IPアドレス以外にも、以下の情報が接続先のサーバーに記録されます。

- 使用しているWebブラウザの種類
- 使用しているOSの種類
- 使用しているリモートホスト名（プロバイダとのアクセスポイント）
- 直前に閲覧していたホームページのURLアドレス



Webサーバーの管理者は、これらの情報を利用することで、電子掲示板に書き込みを行ったユーザーを特定することが可能になります。インターネットには匿名性は存在しないことをよく理解した上で、良識を持って利用するようにしてください。



総務省

国民のための情報セキュリティサイト



「エンドユーザー」の情報セキュリティ対策：一般利用者

個人情報の取り扱い

インターネットは不特定多数の人が利用しているため、個人情報の取り扱いには特に慎重にならなければなりません。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るなどの被害にあうこともあります。

まず第一に、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個人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、自分の個人情報だけでなく、家族や知人の個人情報も同様です。

また、訪問したホームページで個人情報を登録する際には、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、できるだけ個人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、登録された個人情報は、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（ソーシャルネットワーキングサービス）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いますが、このような場合であっても、できるだけ住所や電話番号といった個人情報は不用意に登録しないように注意してください。





総務省

国民のための情報セキュリティサイト



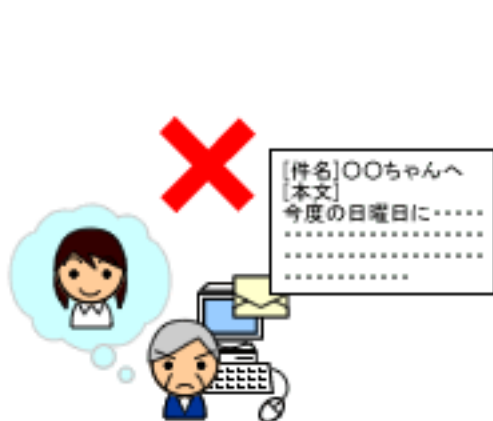
「エンドユーザー」の情報セキュリティ対策：一般利用者

プライバシーの保護

当然のことですが、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環境であるため、たとえちょっとしたいたずらのつもりでも、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、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、他のユーザーによって別の電子掲示板に転載されてしまえば、そのデータを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、名誉毀損等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、人の電子メールを覗き見ることはプライバシーの侵害になります。



他人のメールを無断で読む



他人の個人情報を公開する



総務省

国民のための情報セキュリティサイト



「エンドユーザー」の情報セキュリティ対策：一般利用者

ウイルスに注意

ウイルスは、電子メールやホームページ、CD-ROM、ネットワークの共有フォルダ、USB メモリなど、さまざまな経路からコンピュータに侵入してきます。

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、LAN や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うことがあります。

つまり、インターネットを利用する場合にウイルス対策を怠るということは、被害を受けるだけでなく、他人のセキュリティを脅かす可能性があるということをしっかりと理解しておかなければなりません。インターネットを利用する上では、たとえホームページを閲覧するだけであっても、ウイルス対策ソフトを導入することと、常に最新のウイルス検知用データに更新することは最低限のマナーと言えます。

ウイルス対策ソフトは、主に以下のことを行ってくれます。

- 受信する電子メールやフロッピーディスク、CD-ROM、USB メモリなど外部からコンピュータが受け取るデータから、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てくれます。
- 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。





総務省

国民のための情報セキュリティサイト



「エンドユーザー」の情報セキュリティ対策：一般利用者

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、知らない人からの電子メール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にはできるだけ近づかないなどの注意も必要です。

また、ウイルス対策ソフトを導入する以外にも、プロバイダが自社の接続サービスの利用者向けに提供しているウイルス対策サービスを利用する方法もあります。ウイルス対策サービスの提供の有無や提供内容などについては、プロバイダのホームページで確認するか、加入しているプロバイダに問い合わせてください。なお、プロバイダのウイルス対策サービスを利用する場合には、プロバイダがウイルス検知用データを自動的に更新するため、ユーザーによる更新作業は不要になります。

注意

最近、無料のウイルス対策ソフトのように見せかけて、ウイルスをインストールさせる手口による被害が増えているため、注意してください。その代表的な手口は、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方法です。

ホームページを見ているだけでウイルス対策ソフトのインストールを促された場合には、不用意にリンク先のホームページに接続したり、ソフトウェアをダウンロード / インストールしたりしないようにしてください。



総務省

国民のための情報セキュリティサイト



「エンドユーザー」の情報セキュリティ対策：一般利用者

悪意のあるホームページ

インターネットを利用すると、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いたずらや情報収集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では、あなたのコンピュータに格納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 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、重要な個人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 の適切な取り扱い方法や、Web ブラウザの設定変更の方法について調べてみましょう。

このようなホームページの被害を受けないために、まずはウイルス対策ソフトを導入するか、プロバイダによるウイルス対策サービスを利用するようにしてください。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、不特定多数のユーザーが利用する電子掲示板では、いやがらせ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を貼り付ける場合があるので、むやみにリンクをクリックせずに慎重に利用するようにしましょう。



総務省

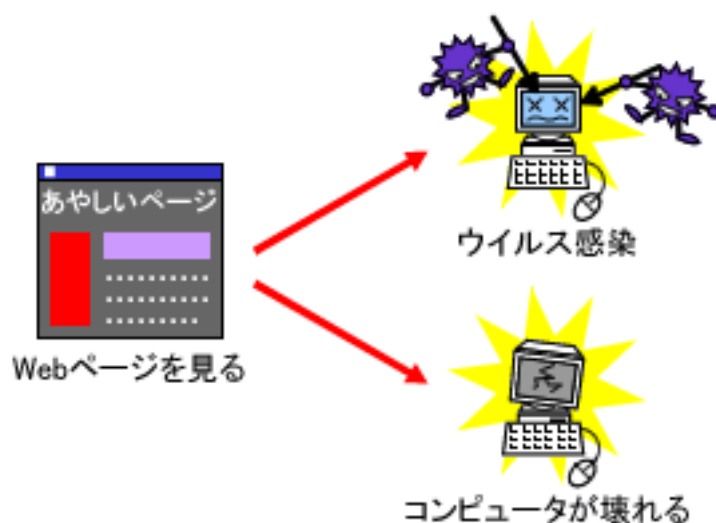
国民のための情報セキュリティサイト



「エンドユーザー」の情報セキュリティ対策：一般利用者

最近では悪意を持たないホームページであっても、ホームページ開設者の知らないうちに Web ページが改ざんされてしまい、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、自動的に別のサイトに誘導されたりすることが増えています。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。また、パッチ等の修正プログラムを確実に適用し、Web ブラウザは常に最新の状態を保つようにしてください。

悪意のあるスクリプトが自動的に実行されないようにするには、Web ブラウザの設定を変更して、JavaScript の実行時に警告を出すようにする、もしくは信頼できる Web サイト（信頼済みサイト）以外では JavaScript を実行させないといったことを実施してください。





総務省

国民のための情報セキュリティサイト



「エンドユーザー」の情報セキュリティ対策：一般利用者

ソフトウェアを最新に保とう

OS、Web ブラウザ、電子メールソフト、Office アプリケーションなどのソフトウェアには、時間の経過とともに、セキュリティホールと呼ばれる不具合が発見されることがあります。セキュリティホールは、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、それらを修正するためのパッチなどの修正プログラムが、メーカーから配布されています。

セキュリティホールを放置していると、たとえウイルス対策ソフトを入れて、最新版のウイルス検知用データに更新していたとしても、ウイルスに感染してしまったり、ウイルス付きの電子メールを知人に自動的に送ってしまったり、悪意のあるホームページを見ただけでコンピュータシステムが破壊されてしまったりすることがあります。

セキュリティホールを修正するために、修正プログラムがメーカーやソフトウェアのホームページ等で配布されています。攻撃者は、パッチが適用されるまでのわずかな時間を狙って攻撃をかけてきますので、自分が使っているソフトウェアの製品名やメーカー名を調べ、直ちに修正プログラムを適用する必要があります。

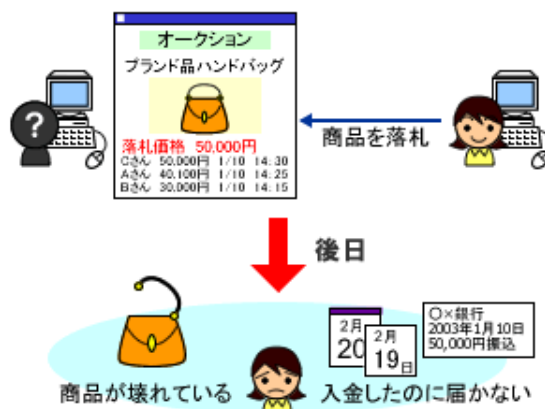




ネットオークションにおける危険性

ネットオークションは、出品されている商品を希望者が入札して、指定期間内に最高価格で入札した人がその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入手できる、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関わらず、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。電話番号は、携帯電話ではなく、自宅の電話番号を覚えてもらうようにしましょう。もちろん、実際にその電話番号で相手に連絡がつくことを確認しておく必要があります。

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、銀行振り込みの控え、宅配便の伝票などの証拠を残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するケースも見受けられます。最近では、宅配便事業者の様な第三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るので、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。



ショッピングサイトの利用

家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、普通の買い物と違い、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。



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とて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、慎重に取り引き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個人情報の入力です。少なくとも、個人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、「プライバシーについて」や「個人情報について」、「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。



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」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。

チェーンメールのほとんどが「新しいウイルスに注意！！」や「あるテレビ番組の企画です」、「すぐにお金儲けができます」などのいたずら目的のものです。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いうケースもあります。

電子メールは転送が楽でコストが安いので、手紙と比べて広まる速度が速いことも、問題を大きくする一因となっています。チェーンメールが広まると、ネットワークに不要な負荷をかけるだけでなく、デマの情報が広まってしまう可能性があるため、他の人に転送する際には、注意してください。





総務省

国民のための情報セキュリティサイト



「エンドユーザー」の情報セキュリティ対策：一般利用者

迷惑メールへの対応

受信者が望んでいないにも関わらず、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（いわゆるねずみ講）に抵触するものや詐欺行為を目的としているものもあります。

最近では、携帯電話へ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、

- ① 長く複雑なメールアドレスを使用する。
- ② 指定したドメインや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。
- ③ 必要以上に自分のアドレスを他人に漏らさない。

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。





総務省

国民のための情報セキュリティサイト



「エンドユーザー」の情報セキュリティ対策：一般利用者

また、コンピュータ（パーソナルコンピュータ）の場合には、以下のような対応策が考えられます。

- 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。
- 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なうことで、迷惑メールを通常を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な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・住所等の個人情報をむやみに開示しないように気を付けましょう。



常時接続の危険性

ブロードバンドネットワーク時代の到来とともに、家庭内においても、常時接続回線の利用が一般的になっています。常時接続回線の場合には、固定化されたグローバルIPアドレスが付与されることが多いため、ネットワーク機器やコンピュータに対する危険性が高くなるという点に注意しなければなりません。

これらの対策としては、きちんとしたウイルス対策を実施することと、定期的にOSのメーカーのホームページなどでセキュリティ情報をチェックして、パッチなどの修正用プログラムを適用することが大切です。また、パーソナルファイアウォールやブロードバンドルーターを導入すると、さらに安全性を高めることができます。

特に、コンピュータに直接グローバルIPアドレスが割り当てられている場合には、インターネット上からそのコンピュータを直接参照できるということになり、コンピュータに不正アクセスされたり、ウイルスが送り込まれたりという危険性が高くなります。また、同一のIPアドレスを長時間使い続けているということは、それだけハッカーが時間をかけて攻撃の手法を試せることを意味します。

これらに対する対策としては、まずは「ソフトウェアの更新」、「ウイルス対策サービスの利用、ウイルス対策ソフトの導入」、「パーソナルファイアウォール・ブロードバンドルーターの利用」の3つを情報セキュリティ三原則として心がけるようにしてください。



総務省

国民のための情報セキュリティサイト



「エンドユーザー」の情報セキュリティ対策：一般利用者

スパイウェアに注意

スパイウェアとは、ユーザーの知らないうちに勝手にインターネットに情報を送信するソフトウェアのことです。スパイウェアには、コンピュータにインストールしたアプリケーションソフトに、機能として組み込まれているものや、インターネットでダウンロードしたソフトウェアに付属しているものなどがあります。

スパイウェアには、アプリケーションソフトに登録されたユーザー名やシリアル番号といった情報を収集して自動的に送信するものもあれば、ソフトウェアやインターネットなどの利用履歴を随時送信するものもあり、送信する内容はスパイウェアによって大きく異なります。

これらのスパイウェアによる情報の漏洩を防ぐためには、スパイウェア自体を削除する方法と、スパイウェアによるデータの送信を停止する方法があります。スパイウェアの削除は、専用のスパイウェアの駆除ツールで実行することができます。また、個人用の統合セキュリティ対策ソフトには、ウイルス対策機能、パーソナルファイアウォールに加えて、スパイウェアによる情報の送信をブロックする機能を持つものもあります。必要に応じて、これらのソフトウェアの導入を検討してください。





総務省

国民のための情報セキュリティサイト



「エンドユーザー」の情報セキュリティ対策：一般利用者

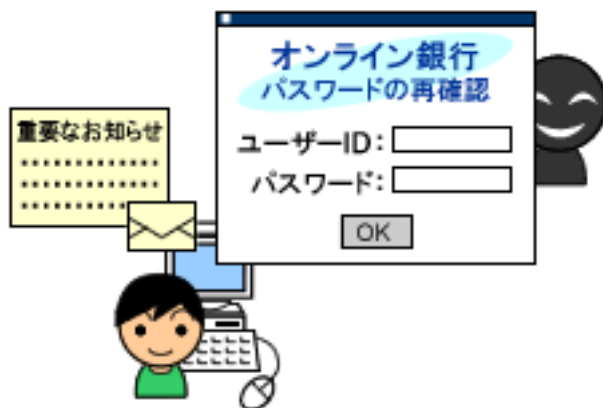
フィッシング詐欺に注意

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、ユーザー名、パスワードといった重要な個人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、接続先の偽のホームページを本物のWebサイトとほとんど区別がつかないようにするなど、少しずつ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断できないケースが増えてきています。

フィッシング詐欺に対しては、明確な対策が取りにくいものですが、電子メールで送信されてきた案内に対して、送信者名や電子メールの内容を鵜呑みにしないこと、ホームページでの登録にSSLという暗号化技術が採用されているかということを確認すること（通常、クレジットカード番号などの重要な個人情報の登録では、SSLを利用します）などの対策を取るようによしてください。

何よりも、むやみにホームページで個人情報や重要な情報を登録することを避けることが大切です。フィッシング詐欺であると判断できない場合には、送信元の会社に連絡をして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、電話を掛ける場合には必ずホームページや電話帳などで連絡先の電話番号を調べるようにしてください。





総務省

国民のための情報セキュリティサイト



「エンドユーザー」の情報セキュリティ対策：一般利用者

携帯電話におけるセキュリティ確保の重要性と対策

携帯電話の中には、アドレス帳、スケジュール、他人とやり取りした電子メールなど、とても重要な情報が格納されています。また、最近では、買い物ができたり、乗り物の切符やイベントの入場券代わりに使用できたりする携帯電話も登場してきており、ますます便利になってきています。

しかし、携帯電話に多くの個人情報が格納され、お金の代わりに使用できるようになると、情報セキュリティ対策が重要になってきます。実際に、携帯電話に格納された個人情報を目的として、廃棄された携帯電話を売買するといった事例も発生しています。

携帯電話を毎日持ち歩いて使用するのであれば、紛失したり盗難されたりする可能性が高くなります。そのような対策として、本人しか携帯電話を使用できないようにするロック機能を装備した携帯電話の利用を検討するのもひとつの方法です。ただし、パスワード（暗証番号）の設定にあたっては、ランダム番号など容易に推測されないものとしておくことが不可欠という認識が大切です。なお、携帯電話を廃棄する際には、必ず登録されているアドレス帳や電子メールなどの個人情報を消去してから廃棄するようにしてください。

さらに、最近ではワンクリック詐欺と呼ばれる行為が増えています。ワンクリック詐欺は電子メールを送信して、Web サイトにおびき寄せ、半ば脅迫のような手口で支払いを強要する行為のことです。その対策として、メールアドレスを他人には推測しにくい複雑なアドレスに変更することも大切です。

便利な携帯電話であるからこそ、安心して利用するためには、常に情報セキュリティ対策に気を配ることを忘れないようにしなければなりませんと言えます。

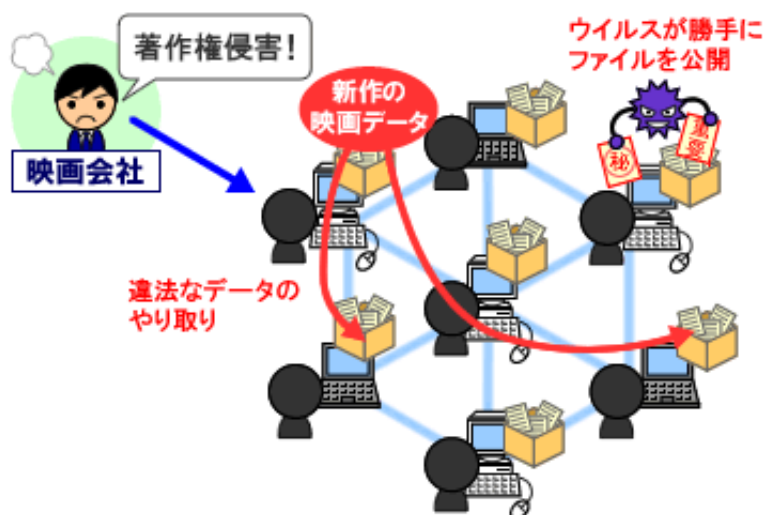




ファイル共有ソフトの利用とその危険性

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－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。ユーザーは、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、他のユーザー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、原則として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いるということなので、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すべ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、公開されていた期間がたった1日であったとしても、複製されたすべ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。



総務省

国民のための情報セキュリティサイト



「エンドユーザー」の情報セキュリティ対策：一般利用者

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、元のファイルの著作権保有者から著作権侵害で訴えられる可能性があるということです。

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。リスクを理解した上で、それでも職場でファイル共有ソフトを利用する必要が生じた場合は、必ずシステム管理者やネットワーク管理者に相談してください。また、自分では使っていないつもりでも、いつの間にか家族の誰かが勝手にインストールし、情報漏洩している事件も起こっています。ファイル共有ソフト使用の方針については、家族にも徹底が必要です。

なお、ファイル共有ソフトを利用する上でも、ウイルス対策ソフトの導入は必須です。しかし、これまでに発生したウイルスでは、ウイルス検知用データの対応が数日遅れたケースもあったため、ウイルス対策ソフトが導入されているからといって決して安心はできないということを認識しておいてください。



総務省

国民のための情報セキュリティサイト

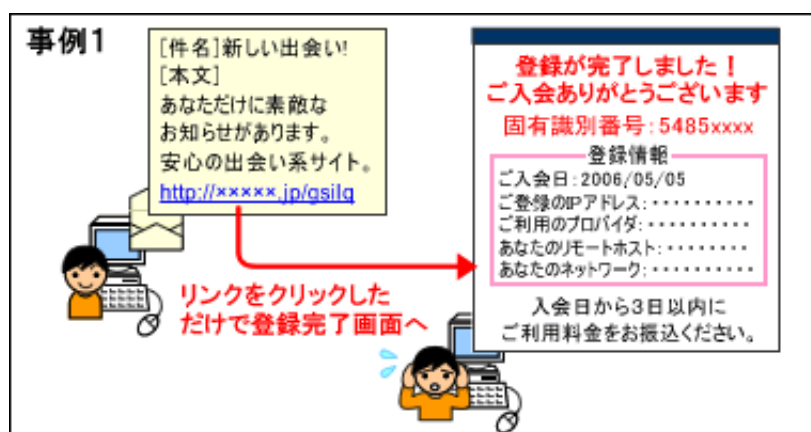


「エンドユーザー」の情報セキュリティ対策：一般利用者

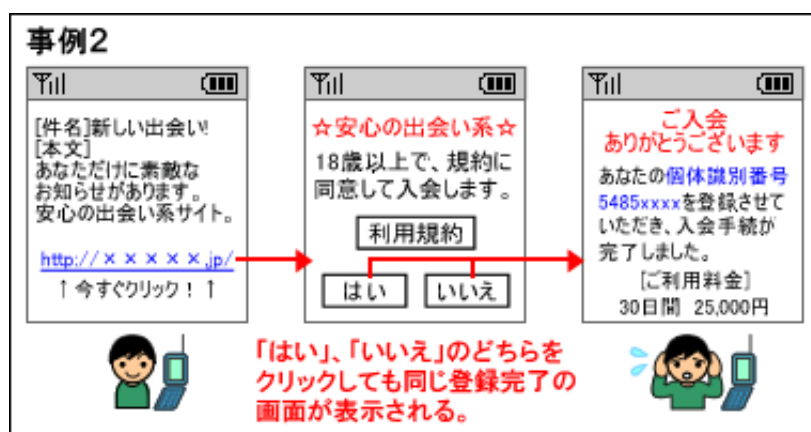
ワンクリック詐欺の概要

ワンクリック詐欺とは、パソコンや携帯電話などによる Web サイトを利用した犯罪行為です。ワンクリック詐欺には、以下のようなものがあります。

事例1：リンクをクリックしただけで登録完了画面が表示されるもの



事例2：「はい」と「いいえ」のどちらを選択しても、規約に同意したと見なしてしまうもの





総務省

国民のための情報セキュリティサイト



「エンドユーザー」の情報セキュリティ対策：一般利用者

これらの図からもわかるように、ワンクリック詐欺にはいくつかのポイントがあります。

- 電子メールや電子掲示板などを利用して、ターゲットをおびき寄せる。
- いかに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て、利用料を請求する（多くのWeb サイトではユーザー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契約書を表示しておく手口を使っている）。
- 携帯電話の個体識別番号や、パソコンの固有識別番号といった表示を行うことで、利用者の個人が“複雑な技術によって”特定されたように見せかけることが多い。また、個人情報として、インターネット上の接続情報（接続元ホストのプロバイダ情報など）によって、地域名や会社名、組織名が表示される場合もある（Web サイトに渡される情報からは個人の特定はできないが、会社や組織のインターネットを使用した場合には、接続情報から会社名や組織名がわかることもある）。

ワンクリック詐欺に対する対処方法としては、以下のことがらがあげられます。

- 不用意にWeb サイトにアクセスせずに、電子メールの文面をきちんと読んでから利用すること。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ある。
- 個体識別番号や固有識別番号と称して、プロバイダのIP アドレスやホスト名が表示されることもあるが、そこからは個人は特定することはできないため、「お支払い頂けない場合には、自宅にまで伺います」といった脅し文句を真に受けないようにする（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、警察などに相談する）。
- 「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る（法律の全文）。
- 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うことは、相手に自分の個人情報を渡すことにつながるため、決して連絡をしないこと（電子メールでの連絡も行わないこと）。
- 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ようにする。
- トラブルになりそうときには、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検討する。また、自分の行った手順をメモしておくとい（「いいえ」を選択したが、登録完了画面が表示されたなど）。

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。



総務省

国民のための情報セキュリティサイト



「エンドユーザー」の情報セキュリティ対策：一般利用者

USBメモリからのウイルス感染

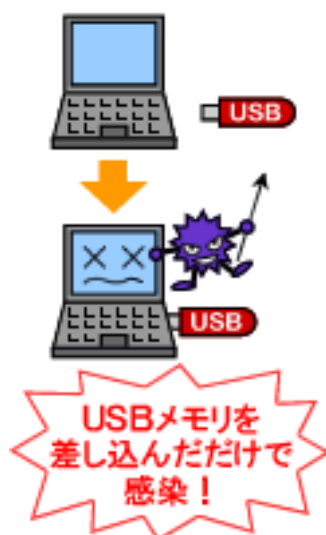
最近のコンピュータでは、USB メモリをコンピュータに接続しただけで、あらかじめ指定された処理が自動的に実行されるようになっているものがあります。この仕組みを悪用して作られたのがUSB 媒介ウイルスです。

USB 媒介ウイルスは、この自動実行機能を利用して、コンピュータにUSB メモリを差し込んだだけでウイルスに感染するようになっています。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。

なお、USB 媒介ウイルスは、記憶領域を持つUSB デバイスであれば感染する危険性があるため、USB メモリだけでなく、外付けハードディスクやデジタルオーディオプレーヤーなどにも感染するという点に注意してください。たとえ音楽用途にしか使わなくても、コンピュータにつなぐだけでウイルスに感染し広めることがありますので十分注意しましょう。





総務省

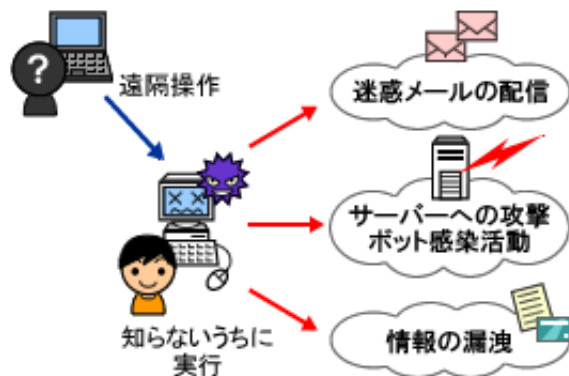
国民のための情報セキュリティサイト



「エンドユーザー」の情報セキュリティ対策：一般利用者

ボットの危険性と対策

ボット（BOT）とは、コンピュータを外部から遠隔操作するためのコンピュータウイルスで、ボットに感染したコンピュータはボットネットワークの一部に組み込まれてしまいます。悪意のあるハッカーは、ボットネットワーク上のコンピュータをインターネットから遠隔操作することで、持ち主の知らないうちに「迷惑メールの配信」、「インターネット上のサーバーへの攻撃」、「感染活動」などの迷惑行為や犯罪行為を行ないます。また、感染したコンピュータに含まれる個人情報やコンピュータを操作した情報を盗み出す「スパイ活動」も行なうことがあります。



ボットは、旧来のウイルスのように愉快犯的な行為で作られたものではなく、迷惑メールの送信者や個人情報を不正に利用しようとする犯罪者と取引するために作られているという点が手口の巧妙化の要因のひとつとなっています。そのため、旧来のウイルスと比べると、感染しているということに気付きにくくしているというのも特徴のひとつです。なお、ボット対策プロジェクト「Cyber Clean Center（サイバークリーンセンター）」が2008年6月に国内のボット感染者数を調査したところ、ブロードバンドユーザー約3000万人のうち約30万人（感染率約1%）と推計されています。

ボットに感染したコンピュータは大量に迷惑メールを送信したり、別のサイトを攻撃したりするため、被害を受けたコンピュータから見ると、ボットに操られたコンピュータが加害者に見えます。あなた自身が加害者にならないようにするためにも、ボットへの対策はとても大切なことと言えます。

ボットへの対策としては、以下を心がけるようにしてください。

- ウイルス対策ソフト・サービスの導入とウイルス検知用データの更新
- セキュリティホールを塞ぐためのOSやソフトウェアのパッチの適用
- パーソナルファイアウォール・ブロードバンドルーターの導入

特に、コンピュータにグローバルIPアドレスが直接割り当てられている場合には、ブロードバンドルーターを設置するとインターネットから直接コンピュータを操作しにくくなり、ファイアウォール機能によってある程度の攻撃から防御することができるようになります。常時接続回線を使用している場合にブロードバンドルーターを利用していない場合には、できる限りブロードバンドルーターの設置を検討してください。



総務省

国民のための情報セキュリティサイト



「エンドユーザー」の情報セキュリティ対策：一般利用者

インターネットにおける安全性の確保



重要!

インターネットを安全に利用するためには、ユーザー自身が危険性をきちんと理解した上で、正しい情報セキュリティ対策を講じなければなりません。主な情報セキュリティ対策には、以下の様なものがあります。これらを参考にして、安全にインターネットを利用してください。

インターネットではネットストーカーなどの危険性があるので、むやみに個人情報をホームページや電子掲示板に掲載してはいけません。また、信頼できないホームページへの個人情報の登録はできるだけ避けましょう。



参照

P.3 個人情報の取り扱い

本人に断りなく、他人のプライバシーに関わる情報をインターネットで公開してはいけません。場合によっては、プライバシー侵害や名誉毀損に抵触することがあります。また、他人の電子メールを無断で読むことも、プライバシーの侵害です。



参照

P.4 プライバシーの保護

ウイルスは、電子メールやホームページ、CD-ROM、ネットワークの共有フォルダなど、さまざまな経路から侵入してきます。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、プロバイダによるウイルス対策サービスの利用が必須です。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。

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。



参照

P.5 ウイルスに注意



総務省

国民のための情報セキュリティサイト



「エンドユーザー」の情報セキュリティ対策：一般利用者

悪意のあるホームページでは、閲覧するだけでコンピュータシステムを破壊したり、ウイルスに感染させたり、情報を盗み出したりすることがあります。これらのホームページはできるだけ閲覧しないようにすることと、ウイルス対策ソフトの導入やプロバイダによるウイルス対策サービスの利用が必要です。

参照 P.7 悪意のあるホームページ

ウイルス対策ソフトを入れたり、プロバイダによるウイルス対策サービスを利用するだけでなく、Web ブラウザや電子メールソフト、OS、Office アプリケーションなどのソフトウェアにパッチを継続的に導入することが必要です。

参照 P.9 ソフトウェアを最新に保とう

ネットオークションやショッピングサイトの利用には、相手が信頼できるかどうかをきちんと見極めることが大切です。

参照 P.10 ネットオークションの危険性

参照 P.11 ショッピングサイトの利用

不特定多数の人々の間で、連鎖しながら広まっていく電子メールをチェーンメールと言います。このようなチェーンメールを受け取ったとしても、むやみに人に転送してはいけません。

参照 P.12 チェーンメールの問題点

信頼できないホームページで安易にアンケートに答えたり、電子掲示板に自分のメールアドレスを投稿することは避けましょう。

参照 P.13 迷惑メールへの対応



総務省

国民のための情報セキュリティサイト



「エンドユーザー」の情報セキュリティ対策：一般利用者

常時接続回線を利用したり、無線 LAN を使用したりする場合には、外部からの不正アクセスによる危険があります。安全な利用のためには、不正侵入への対策が必要です。

参照 P.15 常時接続の危険性

コンピュータにインストールされて、ユーザーの知らないうちにインターネットに対して個人情報やコンピュータの情報などを送信するソフトウェアをスパイウェアと言います。スパイウェアは、プライバシーや個人情報を守る上で、大きな問題になることもあるため、注意しなければなりません。

参照 P.16 スパイウェアに注意

銀行やクレジットカード会社などから、指定されたホームページで個人情報やカード番号などの登録を要求する内容の電子メールが送られてくることがあります。このような場合には、自分が利用している会社の名義であっても、その内容を鵜呑みにせずに、必ず送信元の会社に確認するようにしてください。

参照 P.17 フィッシング詐欺に注意

携帯電話には、アドレス帳（電話帳や住所録）、スケジュール、他人とやり取りした電子メールなど、とても重要な情報が格納されています。日頃、携帯電話を持ち歩く場合には、紛失や盗難によって、これらの情報が盗み出されないように注意しなければなりません。

参照 P.18 携帯電話におけるセキュリティ確保の重要性と対策

ファイル共有ソフトとは、インターネット上でファイルをやり取りするソフトウェアのことです。しかし、ウイルスに感染して、自分のコンピュータの中身が公開されてしまうといったトラブルが続出しています。

参照 P.19 ファイル共有ソフトの利用とその危険性



総務省

国民のための情報セキュリティサイト



「エンドユーザー」の情報セキュリティ対策：一般利用者

ワンクリック詐欺とは、電子メールでWebサイトに誘い出して、そのWebサイトを訪問した人に対して、脅迫めいた手口で料金の振り込みを迫るという詐欺行為のことです。

参照 P.21 ワンクリック詐欺の概要

USB 媒介ウイルスは、コンピュータにUSB メモリを差し込んだだけでウイルスに感染します。その後、感染したコンピュータに差し込まれたUSB メモリが次々に感染していきます。USB メモリを利用する場合には、USB 媒介ウイルスに注意しなければなりません。

参照 P.23 USB メモリからのウイルス感染

ボットはコンピュータを外部から遠隔操作するためのウイルスで、コンピュータを悪用することを目的に作られたものです。ボットに感染すると、あなたのコンピュータは遠隔操作によって、「迷惑メールの配信」、「インターネット上のサーバーへの攻撃」、「感染活動」などの迷惑行為や犯罪行為を行ないます。

参照 P.24 ボットの危険性と対策