

県民向け情報セキュリティハンドブック

はじめに

インターネットを利用する場合には「セキュリティ対策が必要！」などと言われても、一般のインターネット利用者にとっては、「技術的な難しい話はわからない」「そんなものは、マニアとかオタクとかいう人がやることでしょ？」「私は怪しげなホームページは見ないから大丈夫！」などと思いませんか。

インターネットが普及して、生活に欠かせない情報ツールとなっている現在では、便利なサービスや有意義な情報、また、ブログなど今までとは異なる情報発信方法の発展といったプラス面が強調されています。しかし、ここまで発展し利用されていると、当然マイナスの面も無視できなくなっていることも、また一つの事実です。

自動車保険に例えて考えてみましょう。皆さんが自家用車を購入して運転する場合には、ほとんどの人が任意の自動車保険に加入すると思います。決して安くはない保険に加入するのは何故でしょう。それは、万に一つの事故に備えるためであると思います。インターネットを利用する際のセキュリティ対策も、いってみれば安全に利用するための保険のようなものであり、多少の手間や費用がかかっても必ず行いたいものです。

このハンドブックは、主にパソコンを使用するインターネット初心者の方を対象として、インターネットの利用時に知っておかなければならない最低限の知識を紹介しています。このハンドブックだけですべての危険を避けることは難しいですが、安全で快適なインターネットを利用するための参考となれば幸いです。



CONTENTS

- はじめに 1
- I 情報セキュリティ7か条 3
 - 1 ウイルス対策ソフトを導入し、最新の状態にしておこう！
 - 2 むやみに個人情報を公開しないようにしましょう！
 - 3 不審なホームページにはアクセスしないようにしましょう！
 - 4 ショッピングサイト、ネットオークションを利用するときは、サイトの安全性を確認しよう！
 - 5 ID・パスワードの管理は厳重にしよう！
 - 6 インターネットを使うときのルールを子どもと決めよう！
 - 7 子どもが使うパソコンには、フィルタリングソフトを入れよう！
- II 情報セキュリティ事件簿
 - 1 個人情報の流出 5
 - 2 有料サイトの接続トラブル 7
 - 3 コンピュータウイルスに感染 9
 - 4 ネットショッピングのトラブル (次回追加予定)
- III 情報セキュリティキーワード 11

情報セキュリティ7か条

- 1 ウイルス対策ソフトを導入し、最新の状態にしておこう！
- 2 むやみに個人情報を公開しないようにしましょう！
- 3 不審なホームページにはアクセスしないようにしましょう！
- 4 ネットショッピング、ネットオークションを利用するときは、サイトの安全性を確認しよう！
- 5 ID・パスワードの管理は厳重にしよう！
- 6 インターネットを使うときのルールを子どもと決めよう！
- 7 子どもが使うパソコンには、フィルタリングソフトを入れよう！



I 情報セキュリティか条 ～トラブルを呼び込まないために～

1 ウイルス対策ソフトを購入し、最新の状態にしておこう！

コンピュータウイルスへの対策のため、パソコンの購入時にあわせてウイルス対策ソフトを購入しましょう。さらに、常にパターンファイル等のアップデートを実行し、新種のウイルスに備えましょう。

また、セキュリティホールの悪用を防ぐため、パソコンの基本ソフト（Windows等）や、各種アプリケーション（Office製品等のソフトウェア）は、修正パッチを適用するなど、常に最新の状態にしておきましょう。

万が一ウイルスに感染し、パソコン内のデータが破壊されてしまうと、ワクチンソフトで修復できないため、定期的にバックアップを実行しましょう。

2 むやみに個人情報公開しないようにしましょう！

個人情報の公開は、様々な被害の呼び水になってしまいます。不用意に、掲示板に自分の住所や電話番号、メールアドレスを掲載したり、ネット上で知り合った人に教えないようにしましょう。

また、懸賞サイトや、会員制のサイトに、名前や住所を入力するときは、個人情報の取り扱いや、セキュリティに関する説明を事前に確認しましょう。個人情報の公開によって生じる様々な危険をよく考えて行動してください。

3 不審なホームページにはアクセスしないようにしましょう！

インターネットにある情報は、有意義なものもあれば有害なものもあります。世界中の様々な情報を瞬時に閲覧できることは大変素晴らしい事ですが、全世界の人が利用できるインターネットでは、現実の世界と同様に、詐欺目的や悪意を持った人々が存在し、危険な情報やウイルスを巧妙に隠したホームページも沢山あります。

興味本位で不審なホームページに近づくことは絶対にやめるようにしましょう。

4 ネットショッピング、ネットオークションを利用するときはホームページの安全性を確認しよう！

インターネット上で個人情報を送るときは、SSLという暗号化通信技術を用いて、情報が盗まれても解読できないようにするのが一般的です。個人情報を入力するときは、必ず次の2点を確認してください。

- (1) URLが https://になっていること。
- (2) ブラウザに、黄色い鍵（カギ）のアイコンが表示されていること。

5 ID・パスワードの管理は厳重にしよう！

インターネット上で、様々なサービスを利用するためには、IDとパスワードが必要です。生年月日や電話番号などの推測されやすいパスワードを設定していたことにより、IDとパスワードを不正に使用され、オークションやショッピングサイトなどに登録されたクレジットカード情報を取得されるなどして、被害を被るケースが増えています。

IDとパスワードの設定と管理には、必ず次の3点を守ってください。

- (1) 推測しやすい、簡単なパスワードは厳禁です。15文字以上で英字+数字+記号を組み合わせたパスワードが最も推測しにくいといわれています。
- (2) ネットカフェ等の不特定多数の人間が使用するパソコンでパスワード等を入力しないようにして下さい。スパイウェア（P9参照）や、キーロガー（P10参照）などがパソコンにしかかけられ、パスワードが盗まれる可能性があります。
- (3) 1ヶ月に一度はパスワードを変更しましょう。

6 インターネットを使うときのルールを子どもと決めよう！

インターネットを利用する際、子どもの安全を守るためには、大人のサポートが必要不可欠です。まず、子どもとインターネット上でやっていいことと悪いことをはっきりルール化しましょう。子どもが、様々なトラブルの被害者になる可能性があると同時に、いじめ等の加害者になる可能性があることを認識しましょう。

- (1) 個人を特定できる情報は、どんな些細なことでも掲載しないこと。
- (2) インターネットを通じて、知り合った人とは、保護者が同行しない限り会わないこと。
- (3) 現実の世界と同じく、他の人を傷つける言動を絶対しないこと。
- (4) ゲームなどフリーソフトをむやみにインストールしないこと。

また、パソコンは、リビングなどの家族の共有スペースに置き、両親の目の届くところでインターネットを利用させ、利用時間を決めましょう。

7 子どもが使うパソコンには、フィルタリングソフトを入れよう！

インターネットを利用する際、子どもが「有害サイト」に遭遇する可能性は、高いものです。

子どもが使うパソコンには、フィルタリングソフトを利用しましょう。閲覧できるサイトを制限できるだけではなく、掲示板などへの誹謗中傷や個人情報の書き込み制限機能、インターネットの利用時間を制限する機能などがあります。

ただし、すべての有害情報が制限できるわけではありません。過信せず、両親の目の届くところでインターネットを利用させましょう。

II 情報セキュリティ事件簿

● 事例1：個人情報の流出

①懸賞に応募するため、氏名・住所・メールアドレス等を入力した。
(個人情報の流出)



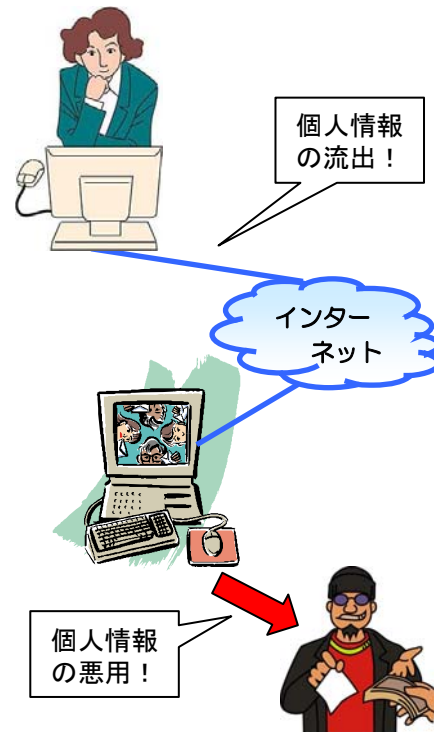
②カード会社を名乗る送信者から、クレジットカード番号などの個人情報を尋ねるメールが届いた。
メールのURLをクリックし、表示されたホームページに、カード番号などを入力した。



③クレジットカードを不正に使われてしまった。
(フィッシング詐欺)



④実家には、家族を名乗る不審な電話が・・・
(振り込め詐欺)



2 とにかく個人情報の流出を防止しよう!

個人情報の流出の主な原因は、フィッシング詐欺や懸賞などで個人情報を収集しているホームページなどでの会員登録など、本人が情報を入力してしまう場合と、コンピューターウイルス等によってパソコンからデータが盗まれてしまう場合が考えられます。

- ・多数の人が閲覧可能なサイトに、自分や家族、友人の情報を公開するのは、やめましょう。

- ・カード会社等、企業を装ったメールにより偽のホームページに誘導し、個人情報を入力させ、その情報が詐欺などに使われてしまうことがあります。個人情報を入力する前に、電話番号案内(104)等を使用して、企業等に真偽を確認するなどし、不審な場合は、回答しないようにしましょう。

- ・懸賞などで個人情報を収集しているサイトも存在することを認識し、会員登録の際には、危険があることを意識して、行動しましょう。個人情報の利用範囲等を記載した「プライバシーポリシー」や社内のセキュリティ管理などを記載した「セキュリティポリシー」が明示されているかどうかなどが、ホームページの安全性に対する目安となります。

- ・信頼のおけないソフトウェアのインストールや、コンピューターウイルス等に感染した場合、個人情報が盗まれてしまう可能性があります。ウイルス対策ソフトを導入し、安易なダウンロードや不審なホームページの閲覧は控えましょう。

■ トラブルに遭ったときには ■

個人情報が不正に使用され、詐欺などの金銭的被害にあったときは、最寄りの警察署または、[茨城県警察サイバー犯罪対策室](#)に相談してください。

※ 茨城県以外の方は、[都道府県警察サイバー犯罪相談窓口一覧](#)から各都道府県警察本部のサイバー犯罪相談担当に相談してください。

■ 予防のためには ■

1 まず個人情報を流出させないことが大切

個人情報の流出は、様々な被害の呼び水になってしまいます。たとえば、メールアドレスを知られてしまうと、迷惑メール、詐欺目的のメール、コンピュータウイルス付のメールが送られてくる可能性が多くなります。

また、住所、電話番号、クレジットカード番号などの流出により、振り込め詐欺、架空請求、クレジットカード詐欺などの被害に遭うおそれが高くなります。

一度流出してしまった個人情報は、取り戻すことができません、日頃から危険があることを意識し、行動することが肝心です。

用語辞典

フリーソフトウェア

フリーソフトウェアとは、無料で利用でき、中にはソフトの完成度が高く、市販されている有料のソフトと比べても、何ら遜色なく使えるものもあるものの、コンピューターウイルスに感染していたり、スパイウェアであるおそれがあります。

必要のないソフトウェアのインストールやダウンロードはしないようにしましょう。また、ダウンロードしたファイルにウイルスの検査を行ってからインストールしましょう。

II 情報セキュリティ事件簿

● 事例2：有料サイトの接続トラブル

①ホームページへのリンクを示した
広告メールが届いた。



②ホームページを開いただけで「〇〇に
御入会ありがとうございます。年会費
〇〇円がかかります」等の表示がされた。



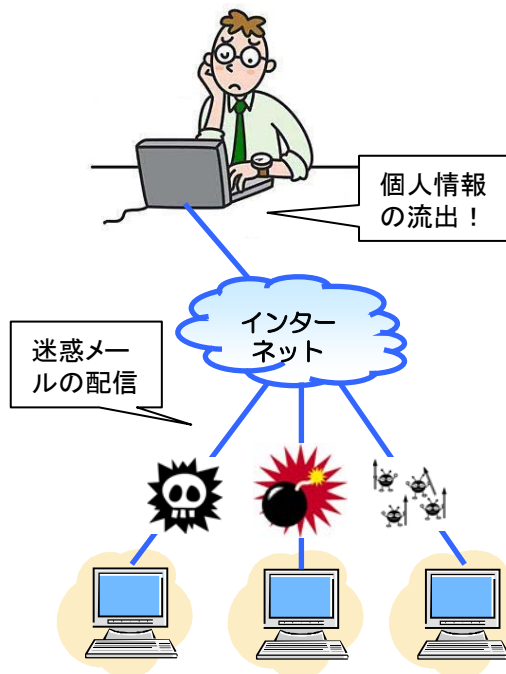
(ワンクリック詐欺)

③あわてて連絡先に問い合わせの
メールをしてしまった。



(個人情報の流出)

④払うように脅すメールや、迷惑メー
ルが大量に来るようになった。



2 ワンクリック詐欺を回避しよう

ワンクリック詐欺は、広告メールに誘導されてのクリックがきっかけであることがほとんどです。

不審なメールについては、コンピュータウイルスの感染のおそれもあるため、開かずに削除しましょう。

利用規約等の記載や確認画面もなく、バナー等をクリックしただけで、突然料金請求の画面が表示されたような場合、契約が有効に成立しているとは考えられません。あわてて相手方に連絡をするのはやめましょう。相手方に新しい情報を与えることとなります。

3 さらにトラブルを呼ばないようにしよう

支払いをする前に支払う義務があるかどうかよく確認しましょう。安易に支払ってしまうと、さらに請求されることがあります。業者間でそういった情報が伝わり、新たな架空請求などを呼んでしまいます。

また、入会した覚えのない有料サイトの退会を促すメールに住所・電話番号を記載するよう指示される事例も起こっています。

そういった業者は、あなたの不安感を煽り、入金させたり、個人情報を得ようとしています。新たなトラブルを呼ばないように、慎重に行動しましょう。

■ トラブルに遭ったときには ■

身に覚えのない請求や、ワンクリック詐欺による請求を受けたときは、[茨城県消費生活センター](#)や、[居住地の消費生活センター](#)に相談してください。

お金を振り込んでしまったなど、金銭的被害が出たときには、最寄りの警察署または、[茨城県警察サイバー犯罪対策室](#)に相談してください。

※ 茨城県以外の方は、[都道府県警察サイバー犯罪相談窓口一覧](#)から各都道府県警察本部のサイバー犯罪相談担当に相談してください。

用語辞典

少額訴訟制度

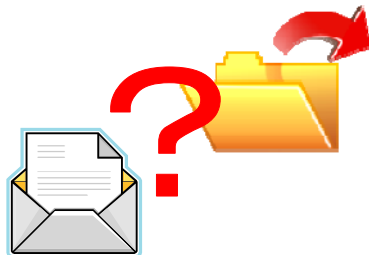
60万円以下の金銭の支払いの請求を目的とする少額の紛争について、その紛争額に見合った費用と時間で紛争を解決するための訴訟制度です。被告には、裁判期日等が記載された「期日呼び出し状」が送付されます。原則として一回の口頭弁論で審理を終え、その日のうちに判決の言渡しがなされ、判決が出ると強制執行ができます。

II 情報セキュリティ事件簿

● 事例3：コンピュータウイルスに感染

①知人から添付ファイル付メールが送られてきたので、開いてしまった。

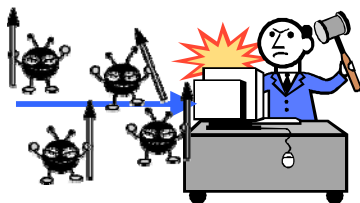
②開いてみると本文がなかった。添付ファイルを見ても、何も起動しない。



③普通に使っていたが・・・その裏で



④知人のメールアドレスに、ウイルス付メールが送りつけられてしまった！



予防のためには

1 ウイルス対策ソフトを導入しよう

最近のウイルスの傾向として、なるべく目立たず、長期に渡りパソコンに潜むようになってきました。そのため、普通にパソコンを使っているだけでも感染に気づかないことがあります。また、ウイルスに感染すると、自分のパソコンだけでなく、他人のパソコンに感染を広げることにもなります。

ウイルス感染を予防するためには、ウイルス対策ソフトを導入し、ウイルス検査を行うことが必要不可欠です。

2 メールには気を配ろう

メールの添付ファイルを開くとウイルス感染する場合があります。見知らぬ相手から送信されたメールは、ウイルス付きのメールであることを疑い、心当たりがない場合は、添付ファイルを開く前に削除しましょう。

また、知人からのメールであっても、悪意の第三者が知人のパソコンを“踏み台”として利用しメールを送信している場合や、ウイルスに感染していることを知らない知人が、知らない間にウイルス付きメールを送信している場合もあります。知人からのメールでも、内容が不自然な場合は、相手に問い合わせて安全を確認することをお勧めいたします。

安全が確認されていても、添付ファイルを開く前には、必ずウイルス対策ソフトによるウイルス検査を行いましょう。

トラブルに遭ったときには

万が一、ウイルスに感染した場合の基本的な対処方法は、以下のとおりです。

※ 対処方法の詳細は、導入しているウイルス対策ソフトのメーカーや、[IPA（独立行政法人情報処理推進機構）](#)に相談してください。

1. インターネットを経由して感染が拡大しないよう、通信ケーブルを抜きます。
2. ウイルスにより対処方法が異なるため、最新のウイルス定義ファイルに更新したウイルス対策ソフトを利用してウイルスを検査し、ウイルス名を特定します。※ ウイルス名が特定できない場合は、ウイルスに感染していないパソコンで、ウイルス対策ソフトのメーカーや、[IPA（独立行政法人情報処理推進機構）](#)のホームページ等からウイルス対処方法の情報収集をします。
3. ウイルス対策ソフトを利用してウイルスを駆除し、パソコンを復旧します。
4. 最新のウイルス定義ファイルに更新したウイルス対策ソフトで、再度ウイルスを検査し、ウイルスに感染していないことを確認します。
5. なお、ウイルスに感染した場合は、ソフトウェアをすべてインストールし直さなければならない場合もありますので、少なくとも重要なファイルや電子メールのデータなどは、バックアップをとっておくことが大切です。

用語辞典

サイバークリーンセンター

近年、インターネット上で感染を拡大しているウイルスの一種「ボット」対策のために、総務省と経済産業省が開設したWebサイト。ボットの特徴を解析し、ボット駆除に必要な情報や駆除ツールをユーザに提供している。

Ⅲ 情報セキュリティキーワード

スパイウェア

スパイウェアとは、利用者が気づかない内に、パソコンにインストールされ、利用者の個人情報などを収集するソフトウェアです。自動的にインターネットに情報を送信してしまう機能を持っています。

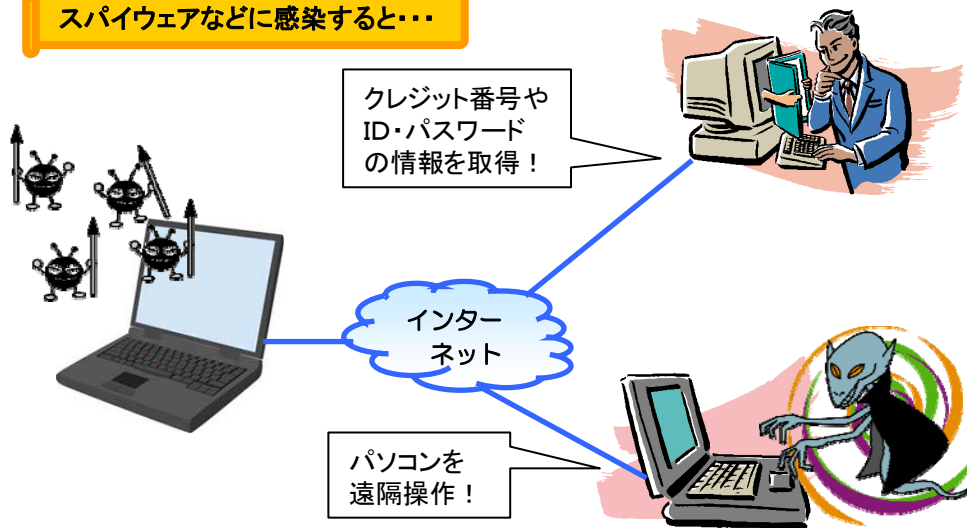
パソコンから情報を取得することを目的としており、直接損害を与えたり、自己増殖をしないことからいわゆるコンピュータウイルスとは区別されます。

悪質なスパイウェアは、個人情報等を盗み取ることを目的としており、IDやパスワード、クレジットカード番号等の情報を送信されてしまう可能性があります。

<被害に遭わないために>

・情報セキュリティ7か条（3ページ）に加えて、ホームページ閲覧時には、安易にソフトウェアのインストールをしないようにしましょう。

スパイウェアなどに感染すると...



ボット

ボットとは、コンピュータウイルスの一種であり、そのパソコンをインターネットを通じて遠隔から操作することを目的として作成された悪質なプログラムです。

「ボット」は、コンピュータウイルスと同様、メールに添付されているファイルの実行や、悪意のあるホームページにアクセスした際、感染します。

ボットには様々な機能があり、キーボードの入力情報を取得する機能や、個人情報や写っているパソコンの画面を画像として取得する機能、また、ウイルス対策ソフトの更新や常時監視機能を無効にすることもできます。

さらに、スパムメールの送信やフィッシングサイトの構築、DoS攻撃の踏み台（経路地）などの用途に悪用され、利用者の気づかぬうちに大規模なコンピュータ犯罪ネットワークの一員になってしまうのです。

<被害に遭わないために>

・情報セキュリティ7か条（3ページ）に加えて、不審なメールの閲覧を行わないようにしましょう。

キーロガー

キーロガーとは、キーボードからの入力を監視し、記録する常駐型のソフトです。

近年、インターネットカフェなど複数の人間が利用するパソコンに仕掛け、パスワードや、クレジットカード番号などを収集するなど、悪用されることが多くなっています。

また、コンピューターウイルスの感染によってインストールされてしまうことも多く注意が必要です。

<被害に遭わないために>

・情報セキュリティ7か条（3ページ）に加えて、ネットカフェなど不特定多数の人が利用するパソコンでは、個人情報を入力しないようにしましょう。