LINEやTwitter、
ショッピングなど
インターネットを
安全に楽しむ

セキュリティとモラルのガイドブック

2016

CONTENTS

セキュリティとモラルのガイドブック

2016年3月31日　第3版

発行所：株式会社カスペルスキー

〒101-0021
東京都千代田区外神田 3-12-8 住友不動産秋葉原ビル 7F
[制作・編集]株式会社ジャムハウス
[印刷・製本]株式会社厚徳社

定価：680円（税別）

ご挨拶

私たちカスペルスキーは、創業以来「インターネット上の脅威から世界を守る」を使命としているウイルス対策ソフトメーカーです。その実現に向け、最新の脅威に対抗できる製品の開発と安全性能を最高レベルに維持するための調査・研究を日夜続けています。

連日のように「情報漏洩」や「不正侵入」「成り済まし」「フィッシング」「情報や金銭の搾取」といったサイバー犯罪の被害が報道される中、インターネットを安全に利用し、犯罪者にとって活動のしにくい世界にするためには、皆様 一人一人の意識と強固なセキュリティ製品が欠かせません。

攻撃者の標的は大企業や官公庁には留まりません。インターネットユーザーであれば、誰もがサイバー攻撃の標的になり得ます。

個人のパソコンやスマートフォンに保存されるメールアドレスやログイン情報などの情報資産も犯罪者にとっては魅力的なものですが、攻撃者はあなたを介して家族や友人、勤め先といった別のターゲットへの侵入を企んでいるかも知れません。自身が被害者にならないことはもちろん、加害者や時として攻撃者の協力者にならない事が重要です。

このガイドブックは、一般の方々を対象にインターネットを利用する上で最低限気をつけていただきたい事柄について分かりやすくまとめたものです。ガイドブックを通じてご自身やご家族、友人たちがインターネット上のトラブルやサイバー犯罪に巻き込まれることなく、安全にインターネットが利用できるよう心より願っております。

株式会社カスペルスキー
代表取締役社長　**川合林太郎**

あなたは大丈夫？

簡単セキュリティ自己診断チェックシート

ガイドブックを読む前に、まずはあなたの現在のセキュリティ状態をチェックしてみましょう。
チェックが付けられない項目があれば横に記載している該当ページを読んでみてください。

- ☐ 1. 有名ブランド品を極端に安売りしている通販サイトでは偽サイトの可能性を疑い、購入前にサイトの情報を充分に調べている ▶P3
- ☐ 2. 通販サイトでの支払いにクレジットカードを利用している場合、明細書を確認している ▶P3
- ☐ 3. 無料のソフトウェアやスマートフォンのアプリなどは、作成者や配布者が明確なものを利用している ▶P5
- ☐ 4. 自分のパスワードを書いたメモを人目のつきやすいところにおいていない ▶P7
- ☐ 5. パスワードなどの重要情報や個人情報をSNSやメッセンジャーでやりとりしていない ▶P7
- ☐ 6. パスワードに自身の生年月日や電話番号等かんたんに推測される文字を使用していない ▶P7
- ☐ 7. ブラウザにパスワードを保存していない ▶P7
- ☐ 8. 公衆Wi-Fiで、ログインを必要とするサービスを使ったり個人情報をやりとりしていない ▶P9
- ☐ 9. 家庭の無線LANは暗号化され、接続のためのパスワードが設定されている ▶P9
- ☐ 10. パソコンやスマートフォン、タブレットにはログインパスワードや画面ロックの認証機能を設定している ▶P19
- ☐ 11. 迷惑メールに返信したり、本文中のURLリンクをクリックしたりしていない ▶P21
- ☐ 12. OS（WindowsやMacなど）のアップデートは自動更新にしている ▶P26
- ☐ 13. オフィスソフトやPDFビューア、ブラウザ、Java等のソフトは自動更新にしている ▶P27
- ☐ 14. 正式サポートの期限が切れたOSやソフトウェアを使用していない ▶P27
- ☐ 15. USBメモリーなど、外部接続機器のウイルスチェックをしている ▶P29
- ☐ 16. セキュリティソフトのライセンス有効期限は切れていない ▶P31

1

偽のショッピングサイトにだまされない

ショッピングサイトでは、気に入った商品を選んでクリックするだけで、手軽に買い物をすることができます。しかし、偽のショッピングサイトでは、代金を支払っても商品が届かなかったり、破損している物などの粗悪な商品が届いたりすることもあります。

偽ブランドの被害も多発しています。正規の価格よりも極端に値引きされていたりする場合には注意が必要です。ひと目で偽物と分かる品物が届いたり、品物が何も送られて来なかったりします。

信頼できるサイトを見極めよう

日本国内のサイトを装っていても、実際は海外に拠点のある通販サイトも存在します。サイトに記載されている日本語が不自然な場合は注意してください。インターネットで買い物をするときは、信頼できるサイトかどうかを見極めて利用しましょう。信頼できないサイトで買い物をすると、入力した送付先の住所や氏名などの個人の情報を流出してしまうこともあります。

Keyword

フリーメール

必要事項を登録すれば無料でメールアドレスを取得できるサービス。複数のメールアドレスを使い分けたい場合などに便利ですが、匿名性が高く、事実上、誰であってもいくつも作成できるため悪用される可能性もあります。

安心できるショッピングサイトの見分け方

事業者の名称や住所、電話番号が書かれているか

特定商取引法により、事業者名、住所、電話番号の表示が義務づけられています。メールしか連絡先が記載されていない場合は信用できません。また、メールアドレスがYahoo!メールやGmailなどのフリーメールの場合や、電話番号が携帯番号の場合も注意が必要です。

クレジットカードでの支払いができるか

詐欺サイトでは、クレジットカードでの支払いができないことが多くあります。支払い方法が口座振り込みのみ場合は、注意が必要です。また、サイトの名称や運営者と、振り込み口座名称が異なる場合、特に個人名義の口座には注意しましょう。

個人情報の扱い方が記されているか

個人情報保護法によって、入力した個人情報を目的以外の方法で使用しないように義務づけられています。個人情報の扱いに関する記載がないサイトで物品を購入することはやめましょう。

暗号化の仕組みが使用されているか

個人の情報を入力して送信する際、他者から情報を盗まれないように暗号化したり、サイトの正当性を証明したりする「HTTPS」という仕組みがあります。この方法が採用されている場合、URLの先頭に「https」と表示されます。この表示を確認しましょう。

2

オークション詐欺に引っかからない

取引き相手の評価をチェック

インターネットオークションサイトを利用する場合は、サイトと併せて取り引きする相手を見極める必要があります。大手のオークションサイトでは、出品者に対して、これまでの取り引き相手が書き込んだ評価を見ることができます。これを参考に信頼できる相手か確認しましょう。

入札する際は、商品の画像や説明、現在の価格、入札締め切りなどをよく確認しましょう。出品者への質問も見ることができるので、出品者の対応をチェックできます。なお、入札するには、オークションサイトに会員登録する必要があります。

落札できた場合、実際に物品の受け渡しや振り込みを行う前に何度かメールをやり取りして、相手がきちんと対応できる人かどうか確認することも大切です。

仲介・決済サービスでトラブルを回避

また、商品が高額の場合などは、仲介・決済サービスを利用する方法があります。手数料は必要ですが、代金を振り込んだのに物品が届かないなどのトラブルを避けることができます。オークションサイトで有料オプションとして仲介サービスを提供している場合があります。

安心・安全にオークションを利用するには

取り引き評価を参考にする
出品者のこれまでの取り引き内容や、落札者からの評価を見て参考にしましょう。

出品者の情報を確認する
落札後は、出品者の氏名や住所、電話番号などの連絡先を確認します。落札した品物の代金の支払い口座の名義と出品者の氏名が同じかも確認してください。

メールのやり取りを参考にする
出品者への質問の回答や、メールのやり取りなどの対応も参考になります。

仲介・決済サービスを利用する方法も
手数料はかかりますが、高額商品の場合、仲介・決済サービスを利用するのも1つの方法です。

Keyword

仲介・決済サービス
第三者が物品の売買を仲介するサービス。落札者から代金を一時的に預かり、出品者へ入金を連絡します。出品者が落札者に物品を送付し、落札者が受け取ったことを確認したあと、代金を出品者へ支払います。安全・確実にやり取りできる仕組みです。

3

動画サイトで視聴用ツールを入れない

専用のツールに注意

動画サイトで専用の視聴用ツールをインストールするように求められた場合は注意が必要です。特に、アダルトサイトで多く見受けられます。専用ツールをダウンロードした利用者のパソコンの中の情報を盗み見るツールや、ウイルスが含まれていることがあります。高額請求の画面が表示され、架空請求による被害にも繋がっています。動画は、視聴用ツールを利用しなくても視聴できるサイトで楽しむようにしましょう。

安易にダウンロードしない

また、パソコンで使うと便利なアプリや、楽しいゲームなどのデータが公開されていて、自由にダウンロードできるサイトでも注意が必要です。信頼できるサイトからダウンロードすること、プログラムのインストール時には使用許諾を確認することが大切です。とは言え、使用許諾をすべて読んでも、きちんと理解するのは大変です。インターネット上の評判なども参考にすると良いでしょう。

外国語のサイトでは、よく理解できないままダウンロードし、説明を読まずにインストールしてしまうことがありますが、それはとても危険な行為です。無料だからといって安易にダウンロードするのは止めましょう。

偽Flash Playerに注意！

YouTubeなどで動画を再生するために利用するソフトウェアの「Flash Player」（フラッシュ・プレイヤー）の偽物被害が起こりました。Flash Playerの更新が必要なように見せかけた偽サイトに誘導され、最新のバージョンにするように勧められます。本物のサイトに似ていたため、偽物だと気がつかない人も多かったようです。そこで、Flash Playerの最新バージョンだと思ってダウンロードすると、不正なプログラムをダウンロードさせられるというもの。

こういったものを「怪しい」と感じる目を養うことが必要ですが、それは簡単なことではありません。セキュリティ対策ソフトを導入し、ソフトを最新の状態に保つことが、このような被害にあわないようにする最善策です。自分自身も注意してインターネットを利用することが大切です。

Keyword

YouTube

国内でも利用者が多い、動画共有サービスです。専用ツールは不要で、パソコンだけでなく、スマートフォンなどからも視聴できます。登録会員は、自分で用意した動画を投稿することもできます。

4

個人の情報を入力させるサイトに注意

情報を不正に入手するワナに注意

インターネットには、利用者個人の情報を不正に入手するためのワナがさまざまな方法で仕掛けられています。例えば、「お得なプレゼントが当たります」といった呼びかけで、利用者の住所や氏名、年令、電話番号、メールアドレス、家族構成などを入力させるサイトがあります。

「プライバシーポリシー」をチェック

まったく知らないサイトでは、個人の情報を一切入力してはいけません。よく見ている信頼できるサイトでも、必要以上の情報を入力するように求められたら、警戒してください。「プライバシーポリシー」という、個人の情報をどのように取り扱うかの方針が掲載されているかどうかも確認しましょう。プライバシーポリシーの掲載のないサイトは信頼できません。

インターネットには便利で役立つサイトもたくさんありますが、危険なサイトもたくさんあります。インターネットを利用する際は、常に注意するように心がけ、少しでもおかしいと思ったら閲覧や情報の入力を止めましょう。

追いかけてくる広告の不思議

どのウェブサイトを閲覧していても、同じ広告が表示され、不思議に思ったことはありませんか？ まるであなたを追いかけて表示しているようです。これは、リマーケティングと呼ばれるもので、過去に閲覧したページや検索したキーワードなど、インターネット上でのあなたの行動にもとづいて広告を表示するものです。不正に情報を取得されているわけではありませんが、あなたのインターネット上での行動を取得することが可能だということは覚えておきましょう。


KASPERSKY lab　個人のお客様　法人のお客様　購入・更新　サポート

ホーム → プライバシーポリシー

プライバシーポリシー

本プライバシーポリシーは、ここに記載した条項へのリンクを含む、各国の現地法人を含むKaspersky Lab（以下、Kasperskyまたは弊社）が管理運営するWebサイトに適用されます。本プライバシーポリシーまたは本プライバシーポリシーへのリンクが表示されていないか、独自のプライバシーポリシーを有する Web サイトには適用されません。また、本プライバシーポリシーへリンクされている場合を除き、カスペルスキーのサービスおよび製品には適用されません。

本プライバシーポリシーは、お客様が本プライバシーポリシーへのリンクを含む弊社Webサイトをご利用いただく際の、個人情報の取り扱いおよびプライバシー保護についての情報を提供します。セキュリティの専業企業である弊社にとって、データプライバシーとデータセキュリティは非常に重要です。そのため、弊社はお客様のプライバシーを尊重、保護し、個人情報の機密性を保持することに最善を尽しています。弊社は各国の個人情報の保護に関する法令、国が定める指針およびその他の規範を遵守します。法改正や社内手続きの変更により本プライバシーポリシーは更新されることがありますので、このページを定期的に参照いただくことをお勧めします。

最終更新日：2015 年 12 月 17 日

1. 個人情報とは

本プライバシーポリシーにおける「個人情報」とは、識別された個人や識別可能な個人に関するあらゆる情報を指します。（膨大な時間と労力をかけることなく）お客様個人に直接結びつけることのできない情報は、個人情報とはみなされません。

2. 個人情報の収集方法と処理方法

a. 一般原則

通常、弊社Webサイトで提供されるコンテンツの大半は、個人情報を提供いただかずにご覧いただけます。

b. 統計データ

お客様が弊社Webサイトから情報を取得する過程で、弊社のサーバーはサービスの提供や統計あるいはセキュリティ上の用途に必要な特定のデータを、個人を特定しない形式、またはお客様のデータレコードの識別子として、内部的に生成される一意かつランダムな英数字列（以下、代替名）を採用した形式で保存します。ここで記録されるデータは、お客様のドメイン名やブラウザーの種類などの一般的な情報です。このデータは常に代替名を使用して収集されるため、これを利用して弊社がお客様の身元を特定することはありません。また、統計的な評価が完了次第、これらの情報は削除されます。

プライバシーポリシーの例。個人情報をどのように扱うかの方針が書かれているので、信頼できるサイトかどうかの判断になります。

5

パスワードを安全に管理するには?

インターネット上のさまざまなサービスを利用するときには、「ユーザーID」と「パスワード」の入力が必要なことがあります。こうした情報が第三者に漏れると、他人に勝手にログインされたり、勝手に有料のサービスを利用されたりする ともあります。

生年月日や電話番号はキケン

生年月日や電話番号など、単純なパスワードは危険です。また、いちばん避けたいのは、同じIDやパスワードの使い回しです。例えば1つのサービスからユーザーの登録情報が漏れてしまった場合、ほかのサービスで被害が出かねません。また、SNSを他人に乗っ取られると、あなたになりすまして、あなたの友人に迷惑をかける可能性もあります。とは言え、複数のサービスそれぞれに別のIDと複雑なパスワードを用意して管理するのは大変なもの。

自分だけのルールを作ろう

自分だけの「パスワード作成ルール」を決めて、パスワードをつくってみましょう。例えば、好きな歌詞、校歌でもよいでしょう。座右の銘や好きな言葉でもかまいません。忘れない、ベースとなる言葉を決めて、それを、ローマ字に置き換えます。

「**hayabusa**」

そこに、数字を埋め込みます。親や兄弟、結婚相手の誕生日、昔の車のナンバーなど、忘れない数字にします。

「**4h9ay6abu3sa**」

間にはさむアルファベットを、1つ、2つ、3つ…と増やして埋め込んでみました。いかがでしょうか。でも、これでは、1種類のパスワードがつくれたに過ぎません。このパスワードを基本パスワードとして、サービスごとのアルファベットを追加します。例えばYahoo!なら

「**ya4h9ay6abu3sa**」

Amazonなら

「**am4h9ay6abu3sa**」

といった具合に、先頭にアルファベットを入れます。先頭と末尾に入れたり、末尾のみに入れたりしてもよいでしょう。ルールは自分で決めてください。大文字と小文字、さらに記号を組み合わせるとより強固なパスワードになります。

自宅アクセスポイントにもパスワードを設定

自宅でWi-Fiを利用する場合、接続するためのパスワードを必ず設定しておきましょう。誰かが勝手にインターネット接続に利用したり、家庭内 ネットワークから情報を盗んだりするおそれがあります。パスワードの設定方法は各機器のマニュアルを読んでください。

無料ゲームや アプリの追加課金に注意

アイテムが有料の場合も

スマートフォンや携帯電話向けに、無料のゲームを配信するサービスがあります。ただし、「無料」をうたっているゲームでも、すべてが無料で利用できるものばかりではないので、注意が必要です。

ゲーム内でアイテムを購入したり、イベントに参加したりすると、料金がかかる場合があります。このとき、料金はゲーム内で使う通貨の単位で表示されることもあります。子どもは実際にお金がかかるとは思わずに気軽に実行（購入）してしまい、請求書が届いて「コンテンツ使用料」として課金されていて、初めて判明する場合もあります。こうしたアプリをダウンロードする際には、「アプリ内課金あり」などのように記載されているので注意して読むようにしてください。

また、単にゲームだけで遊ぶつもりで登録したのに、出会い系サイトのように使うユーザーが潜んでいる場合もあります。子どもにとって危険だと思ったら、早急に登録を削除してください。

こんなトラブルが発生！ 子どもの被害事例

事例１

無料と思ってゲームサイトを利用したところ高額請求

小学生の息子が無料ゲームをするために、私の携帯電話を貸して遊ばせた。テレビで「無料」とCMをしていたし、息子も友人から無料ゲームだと紹介されたと聞いたので、お金がかからないと安心して利用させていた。しかし実際には、アバター(※)のコンテンツ料として1回5千円かかり、2ヶ月で約6万円もの請求書が届き驚いた。

※アバターとは、自分の分身として画面上に登場するキャラクターのことで、髪型や服装、装飾品、背景などのアイテムを選んで、オリジナルのキャラクターを作成できるようになっている。

（国民生活センターの報道発表資料より）

事例２

ゲーム内のアイテム購入で高額請求

テレビで無料とCMをしているゲームサイトに小学校低学年の娘も興味を示したので、無料なら遊ばせてもいいだろうと思い、母親である私の携帯電話で私の名前で娘のために登録をした。娘は10日ほど遊び、１つ5,000円のアイテムを多数購入していた。娘は本当のお金が必要だとは思わず、アイテムも無料だと思って遊んでいた。しかし、後日携帯電話会社から約10万円もの請求書が届いた。

事例３

無料ゲームにアクセスして高額請求

中学生の息子が携帯電話のコミュニティサイトで知り合った人から無料のゲームサイトを紹介され登録したが、その日のうちに解約したところ、そのサイトから約8万円を今日中に支払えとのメールがきた。最近、息子があまり元気がないので声をかけたところ、その事実が発覚した。

ウェブコンテンツやゲームの年齢制限

インターネットのウェブコンテンツや、ゲームソフトの中には、年齢制限が設定されている場合があります。パソコンやスマートフォンのフィルタリング機能や、フィルタリングソフトを利用することで、設定年齢に満たない子どもによる視聴や利用を制限できます。

7

公衆Wi-Fiは使い方が重要

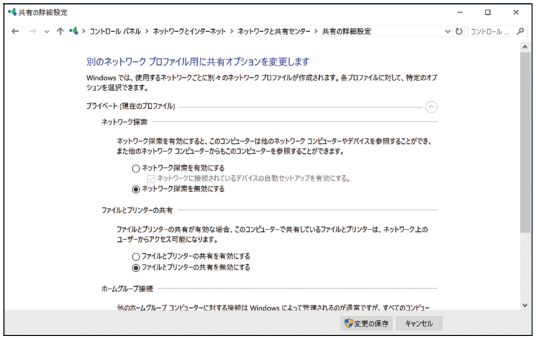
最近では、カフェやファーストフード店、空港や駅など、無料でWi-Fiを利用できるスポットが増えてきました。例えば外出先でパソコンをインターネットに接続したいときも、これらのWi-Fiスポットを利用することで、手軽にインターネットに接続できます。モバイルWi-Fiルーターを持ち歩いていないときなど、いざというときにもとても便利です。

個人情報が盗まれるキケン

便利な反面、気をつけたいこともあります。公衆Wi-Fiではメール、SNS、オンラインショッピング、インターネットバンキング、オークションなど、ログインを必要としたり個人情報の入力を求めるサービスは利用しないようにしましょう。公衆Wi-Fiは誰でも使用できるため、入力情報を盗むことを目的とした人も接続している可能性があるからです。

共有機能はオフにする

なお、Wi-Fiスポットを利用する前には、パソコン側でファイルやプリンターの共有などを無効にしておきましょう。そうすれば、共有している情報を他の人に盗まれる心配がなくなり、共有機能を悪用したウイルス感染も防げます。



無料Wi-Fiに接続する前には、ファイルとプリンターの共有をオフにしておきましょう。

Keyword

Wi-Fi（ワイファイ）

無線LANの規格の1つ。無線の言葉どおり、ケーブルなどで接続する必要はなく、無線通信を利用してインターネットにアクセスできます。

ブラウザにパスワードを保存していない？

ブラウザにパスワードを保存しておくと、すぐにサービスを利用できて便利です。しかし、保存したパスワードは盗まれたり、他人や子どもがパソコンに触れて勝手に買い物などをしてしまうかもしれません。ブラウザにはパスワードを保存しない設定にしましょう。

8

事業者設定のフィルタリングはWi-Fi接続では効かないことも

子どもの利用にフィルタリングは必須

最近では、小学生でもスマートフォンを持つ子どもが増えています。子ども向けのスマートフォンでは、危険なサイトにアクセスできないようにするフィルタリングサービスがあります。違法なサイトや有害なサイトにアクセスできないようにすることで、子どもが個人の情報を漏らしたり、不当な高額請求をされたりするといったトラブルを防ぎます。

携帯電話やスマートフォンを契約する際に、18歳未満の場合は保護者が申し出ない限り、フィルタリングサービスを適用することが通信事業者に義務

Keyword

フィルタリング

一定の条件に基づいて、出会い系サイトやアダルトサイトなど、有害だと思われるサイトにアクセスできないようにする仕組みやサービス。

フィルタリング

ゲーム機からもWi-Fi接続できる

Wi-Fi接続してインターネットにアクセスできるのは、パソコンやスマートフォンだけとは限りません。最近では、ゲーム機や携帯型ゲーム機もWi-Fi接続の機能を持っています。子どもが使用する想定のゲーム機なので、フィルタリング機能を備えています。ゲーム機の解説書などで、設定方法を必ず確認しておきましょう。

安全に楽しく子どもとスマートフォンを使うには？

スマートフォンは便利ですし、学年が上がると子どもたちも持ちたがるようになります。安全に活用するための知識を身につけたいと思ったときに、ぜひ活用していただきたいサイトがあるので、ご紹介します。

電気通信事業者協会
http://www.tca.or.jp/

「青少年の携帯電話利用について」では、フィルタリングサービスや子どもに携帯電話を持たせる際のルールづくりなどについてまとめられています。

ジュニアスマホ検定
https://www.sumaho-kentei.jp/

質問に答えながら、スマートフォンやインターネット利用のスキルをチェックできます。親子で挑戦して、それぞれの家庭でルール作りしましょう。

情報モラル診断サービス
https://www.netmoral.net/

20分程度の診断サービスで、クラスにいる子どもたちのネット利用状況や、トラブルを把握できます。

づけられています。

Wi-Fi利用時に注意

ただし、フィルタリングサービスを適用したからといって、すべて安心というわけではありません。フィルタリングの機能によっては、Wi-Fi（無線LAN）を利用したインターネットの接続では、無効になることがあるため、注意が必要です。契約する際に事業者が提供するプランをよく確認し、Wi-Fi接続時にもフィルタリングが有効かどうかをチェックしましょう。なお、スマートフォン向けのフィルタリングアプリを入れることで、フィルタリングを有効にすることもできます。

また、携帯電話以外にも、iPodやPSP（プレイステーション・ポータブル）、3DSなど、ネット接続できる機器が増えています。携帯電話もゲーム機器も、子どもが安全に利用できるように、お子さまとよく話し合い、フィルタリングやアプリの利用制限を行って使うようにしましょう。

主な通信事業者のフィルタリングサービスの内容

ソフトバンクモバイル
http://www.softbank.jp/

対象年齢に応じた「ウェブ安心サービス」のフィルタリングサービスを提供しています。ただし、Wi-Fi接続では「ウェブ安心サービス」は適用されません（※）。スマートフォンの場合は、使用可能な機能を保護者が制限できる「あんしん設定アプリ」も併せて利用すると良いでしょう。また、3GとWi-Fiのどちらを利用している場合でもフィルタリングが有効な「Yahoo!あんしんねっと for SoftBank」もあります。

（※）「ケータイWi-Fi」利用の場合は、「ウェブ安心サービス」は適用されます。

NTTドコモ
https://www.nttdocomo.co.jp/

子どもの年齢や使い方に応じて、アクセス可能なサイトのレベルを選択できる「アクセス制限サービス」を提供しています。また、保護者が子どものスマートフォンの使用機能を制限できる「あんしんモード」アプリでは、Wi-Fi接続時のインターネットのアクセスやアプリのインストールなどを制限できます。

KDDI
http://www.au.kddi.com/

子どもの年齢に応じて3種類の基本フィルターから選択できる「安心アクセスサービス」（カスタマイズコースは月額100円）を提供しています。ただし、Wi-Fi接続時はフィルタリングが適用されません。スマートフォンの場合は、Wi-Fi接続時も有効な「安心アクセス for Android」「安心アクセス for iOS」アプリを利用しましょう。サイトへのアクセス制限やアプリの利用制限、利用時間制限などができます。

Y!mobile（ワイモバイル）
http://www.ymobile.jp/

利用の機種によって、提供されるフィルタリングのサービス内容が異なります。スマートフォンの場合は「スマホ安心サービス」、3G対応のスマートフォンや携帯電話の場合は「Webアクセス制限」を利用します。なお、「Webアクセス制限」はWi-Fi接続時には適用されません。「Yahoo!あんしんねっと」も利用することが勧められています。

※サービス内容や料金は2016年3月現在のもので、変更になる可能性があります。

世界中の誰でも読めることを知っておこう

ブログやTwitterを友達とのコミュニケーションツールとして利用する方も多いでしょう。その日あった面白い出来事を書いたり、お薦めのお店や料理を紹介したりすれば、すぐに友達みんなに読んでもらえます。写真や動画もアップしてみてもらえます。

書いてしまいがちな“武勇伝”？

いつも読んだり見たりして感想をくれるのは友達ばかりなので、ついつい読者は友達だけだと思いがちです。そのせいか、アルバイト先でしたイタズラや、ちょっとした交通違反などを武勇伝のように書く人がいます。

読んだのが友達だけなら、話はそこで済むかもしれないですが、実はブログやTwitterに書き込んだことは世界中の人に読まれる可能性があります。

勤務先や学校にも迷惑が…

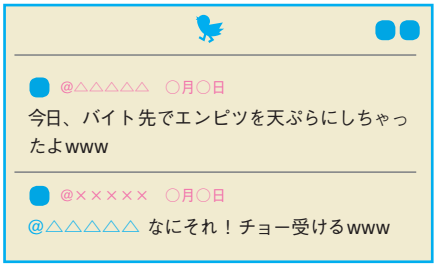
犯罪自慢のような書き込みを誰かが見つけると、すぐに“2ちゃんねる”などの掲示板に書き込まれて、あっという間に拡散してしまいます。中には、書き込んだ人を特定しようとする人もいて、アルバイト先や勤務先、学校などへ電話やメールが殺到することがあります。場合によっては、アルバイト先や勤務先を辞めることになったり、学校に行きづらくなることもあるのです。 アルバイト先が閉店に追い込まれるなど、周囲に影響が及ぶこともあります。

ブログやTwitterに限らず、他のSNSなどネット上に書き込んだことは、友達だけでなく、世界中の誰でも読めるものだと考えてください。親しい友達にしか話せないようなことは、ネット上に書き込んではいけません。

Keyword

SNS（ソーシャル・ネットワーキング・サービス）

インターネット上で情報を交換し合うことができる、コミュニティを作ることができるサービスです。Twitter、Facebook、LINEなども含まれます。



10

SNSの詐欺やトラブルに注意

SNSのサイトを利用すれば、友だちと連絡を取り合ったり、同じ趣味の仲間を見つけられたりして楽しいし、便利です。

悪質な参加者に注意

しかし中には、巧みに有料サイトに誘導したり、個人情報を聞き出そうとしたりする悪質な参加者もいます。そのため、知らないうちに課金されたり、迷惑メールが頻繁に届くようになったりすることもあるので、注意が必要です。

また、SNSで知り合った相手から「直接会いたい」と誘い出され、暴力を振るわれたり、お金を取られたりするなどのトラブルに巻き込まれるケースもあります。SNSを出会い系サイトのように使う参加者もいるので、注意が必要です。

不幸にも万が一、被害に遭った場合、下に紹介するサイトなどで相談することができます。

被害にあう前・あってしまった場合に役立つサイト

国民生活センター
http://www.kokusen.go.jp/

消費・生活のトラブルに関する情報を掲載しています。インターネットでのトラブルについても、具体的な相談内容に対するアドバイスが掲載されています。トラブルを事前に回避するためにも目を通しておきましょう。全国にある消費生活センターの連絡先も載っています。

あぶない！出会い系サイト（警察庁）
http://www.npa.go.jp/cyber/deai/

警察庁が運営しているサイトで、中高生に向けて出会い系サイトの犯罪事例や被害の実態、身を守るためのルールが分かりやすく紹介されています。また、保護者、一般成人、出会い系サイト事業者に向けた情報も掲載されています。インターネットの危険性を確認できます。

警察庁 サイバー犯罪対策
http://www.npa.go.jp/cyber/

コンピューターを使ったサイバー犯罪について、予防策が紹介されています。「インターネット安全・安心相談」では、よくある相談事例や予防のためのアドバイス、実際に被害にあった場合にどうするかなどについて掲載されています。また、「都道府県警察本部のサイバー犯罪相談窓口」で、各県窓口にURLを調べることができます。

JADMA（ジャドマ／日本通信販売協会）
http://www.jadma.org/

通信販売専門の消費者相談窓口、「通販110番」があります。インターネット通販などによるトラブルの相談なども受け付けています。

※本ページに掲載している情報は、本書作成時点の内容です。ホームページアドレス（URL）や内容は変更となる可能性があります。

公開範囲の設定に気をつけて

設定方法を知っておこう

前のページで書いたように、ネット上に書き込んだことは世界中の人に読まれることに、注意が必要です。けれども、サービスによっては、公開の範囲を設定して、友達だけ・特定の人だけ・本人だけなど読める人を限定するよう設定ができます。ここでは、FacebookとTwitterの場合を見てみましょう。

ただし、これだけで安心してはいけません。うっかり設定を変更して公開状態にしてしまったり、気づかないうちに設定の方式や内容が変更になったりすることもあります。また、IDやパスワードがもれてしまうと、他の人に読まれる可能性があります。

Facebookの設定

パソコンの場合

Facebookの画面で右上の▼をクリックし、[設定]を選択します。

[プライバシー]を選択し、[私のコンテンツを見ることができる人]の[編集]をクリックします。

公開の範囲として[友達]を選ぶと、基本の公開範囲が、友達に登録した相手だけに限定されます。

iPhoneの場合

Facebookアプリで[その他]をタップし、[プライバシーショートカット]をタップします。

[私のコンテンツを見ることができる人]をタップします。

[今後の投稿の共有範囲]をタップします。

[友達]を選ぶと、基本の公開範囲が、友達に登録した相手だけに限定されます。

※画面は2016年1月20日時点のものです。

知られて困る事は書かない

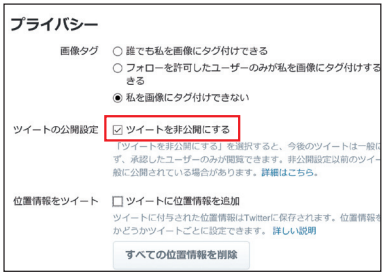
自分のIDはしっかり管理していても、友達がIDを盗まれてしまえば、第三者に投稿を読まれてしまいます。

また、最初は友達だけに読んでもらうつもりで始めたFacebookやTwitterでも、後から仕事で取り引きがある相手を友達登録することもあります。そうなったときに、以前に書いた犯罪自慢や、誰かを誹謗中傷する書き込みが読まれてしまうかもしれません。そのため、たとえ限られた人しか読めない設定にしたとしても、人に知られて困ることを書き込むのはやめましょう。

Twitterの設定

パソコンの場合

ユーザーアイコンをクリックして、[設定]を選択します。



左のメニューから[セキュリティとプライバシー]を選んだら、上の画面で[ツイートを非公開にする]をチェックします。

※非公開にすると、ツイートはフォローしているユーザーだけが読めるようになります。

iPhoneの場合

ホーム画面から「アカウント」を開いて、設定ボタンをタップ。 メニューから[設定]を選択します。

[アカウント]を選択して、設定画面で[ツイートを非公開にする]をオンにします。

12

住所や電話番号など個人の情報を聞かれても答えない

近所の話をしただけでバレることも

ブログや掲示板、Twitterの利用者の中には、個人の情報を聞き出して悪用したり、相手を誘い出したりする目的で、住所や電話番号、名前を聞き出そうとする人がいます。

こうした情報を絶対に教えてはいけません。近所のお店や駅の名前を聞くことで、住所を探ろうとする人もいます。例えば、どこにでもあるスーパーの名前を書いただけのつもりでも、隣にあるお店や、駅からの距離などから場所を特定しようとする人もいます。

ネット上の発言が丁寧で、優しそうな人だと思っても、実際に会いに行くと、暴力を振るわれたり、金品を奪われたりすることがあります。あるいは、ストーカーのように、しつこく付きまとわれたり、家や家族の写真がネット上で公開されたりすることもあります。ネットの振る舞いだけを見て、だまされないようにしてください。

また、Twitterはもちろん、閲覧者を限定していないブログや掲示板に書き込んだ情報は、ふだんコメントをやり取りしている以外の人にも読まれています。まったく知らない相手に個人の情報を知られてしまう危険があることにも、注意が必要です。

まち情報交換　BBS

ID 1234さん
買い物はどこでしてるの？

ID 678910さん
駅前のスーパー○●よ。

ID 1234さん
じゃあ、最寄り駅は△▲駅だね！

ID 678910さん
どうしてわかるの！？

リベンジポルノの恐怖

恋人など親しい相手、あるいはSNSで知り合って親しくなった相手とのやりとりで、つい心を許して、裸の写真を送ったりするSNSの参加者がいます。けれど、こうしたやりとりは絶対にしないでください。万が一、2人の関係がうまくいかなくなったとき、プライベートな写真や動画が公開されてしまうことがあるのです。このことを“リベンジポルノ”と言います。インターネット上で写真や動画が広まってしまうと、削除することはほぼ永遠に不可能となります。

13

LINEのIDを隠す方法を知っておく

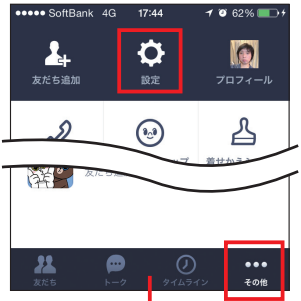
スマートフォンの住所録に登録している相手なら、すぐにLINEで友だち登録できます。それ以外にも、自分の「LINE ID」を教えてあげれば、遠くに住んでいる友だちにもすぐに登録してもらえます。

IDの検索は基本オフに

しかし、このIDが掲示板に書かれたりすると、知らない相手から友だち申請が届くことになります。

また、このIDを専用の掲示板に書き込んで、出会い系サイトのように使おうとする人もいます。しかし、他の出会い系サイトと同じように、IDの交換サイトも犯罪の温床になりがちです。知り合った相手から呼び出されて会いに行くと、トラブルに巻き込まれたり、暴力や殺人の被害にあうこともあります。

IDを使って友だちから探してもらう機能は、基本的にオフにしておきましょう。必要なときだけオンにする使い方なら、安心です。



LINEアプリの「その他」をタップし、「設定」をタップします。

「設定」画面が開いたら、「プロフィール」をタップします。

「IDで友だち追加を許可」をオフにしておくと、IDが知られても、怪しい申請が届くことはありません。

LINEの乗っ取りやなりすまし投稿に注意

2台のスマートフォンが、同じLINEのアカウントを使うことは、基本的にできません。乗っ取りやなりすましは、主にパソコンからログインして行われます。自分がパソコンから利用していないのに、下のようなメッセージが表示されたら、いったんログアウトしてログインし直し、早急にパスワードを変更してください。

また、友達からプリペイドカードの購入依頼など怪しいメッセージが届いたら、なりしましの可能性があります。少しでもおかしいと思ったら、本人に電話したり別のメッセージサービスで確認したりする用心さが必要です。

14 写真をどこで撮ったかバレちゃう!? 位置情報に注意

GPSの位置情報に注意

スマートフォンのカメラ機能や、最近のデジタルカメラの中には、GPSの位置情報を記録できるものが増えています。また、Wi-Fiで位置情報を計測する仕組みもあります。位置情報を記録することで、後からどこで撮影した写真かわかります。撮影した場所ごとに、地図上に写真を整理して配置できるアプリも多くあります。便利な機能ですが、利用には注意が必要です。

例えば、自宅で位置情報付きの写真を撮影し、そのままSNSやブログにアップしたとします。SNSやブログサービス側で、位置情報などの画像固有情報を削除する機能がない場合、誰かがその写真をダウンロードして位置情報を確認すると、自宅がどこにあるのか突き止められてしまうのです。

もし、位置情報付きの写真をうっかり投稿したりメールで送ったりしそうで心配だという方は、あらかじめオフにしておく方法があります。

設定でオフにしておこう

iPhoneやiPad、Androidのスマートフォンやタブレットで、カメラ位置情報の有効／無効を切り替える方法を確認しておきましょう。デジタルカメラの場合には、設定方法がそれぞれ異なるので、製品に付属のマニュアルなどでご確認ください。

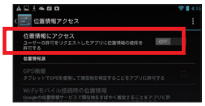
iPhoneの場合

ホーム画面の［設定］をタップして、［プライバシー］をタップ。［位置情報サービス］をタップします。

［位置情報サービス］をオフにすると、すべてのアプリで位置情報が無効になります。カメラだけ設定するには、［カメラ］をタップして［許可しない］を選びます。

Androidの場合

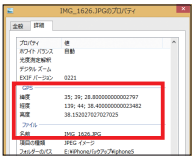
アプリ一覧の［設定］をタップして、［位置情報アクセス］をタップします。



［位置情報にアクセス］で［OFF］を選ぶと、アプリで位置情報が無効になります。カメラアプリの設定画面で個別にオフにする方法もあります。

位置情報の表示

パソコンに保存した写真ファイルを右クリックして［プロパティ］を選択し、［詳細］タブを開きます。緯度、経度を見れば、どこで撮影したのか地図上で確認できます。



Keyword

GPS

地球を周回するGPS衛星に電波を送信し、通信にかかる時間から、距離を計算して、現在地の緯度と経度がわかる仕組みです。

スマートフォンやタブレットは必ずロックしておこう

気軽に持ち歩けるスマートフォンやタブレット。ついついテーブルの上に置いたままそばを離れたり、外出先でうっかり置き忘れたりしたことはないでしょうか？

ロックしなければ情報が盗まれる

もし、ロックを掛けていない状態のスマートフォンを誰かが手にしたら、そこに保存されている様々なあなたの情報が盗み見られます。住所録やメールの内容から、友達の情報まで見られてしまいますし、あなたになりすまして、SNSに投稿されるかもしれません。子どもが勝手に操作して買い物をすることもできますし、危険なサイトを見てしまうこともありえます。

そんなことにならないように、スマートフォンやタブレットには必ずロックをかけておきましょう。パスワードの入力や指紋認証などの方法でロックを解除しなければ、他の誰かが勝手に使うことはできません。

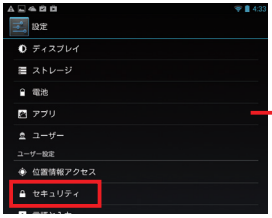
iPhoneの場合

ホーム画面の［設定］をタップして、［Touch IDとパスコード］（5s以下は［パスコード］）をタップします。既に設定済みの場合、このあと現在のパスコードを入力します。

［パスコードをオンにする］をタップして、パスコードを設定します。変更したい場合、［パスコードを変更］をタップして設定します。iPhone 5s、6、6Plusの場合、指紋認証の設定もできます。

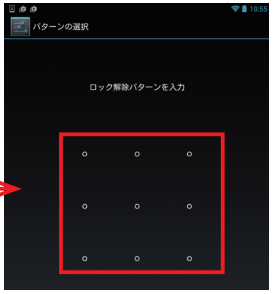
6桁のパスコードを入力します。iOS8以前の場合は4桁です

Androidの場合



アプリ一覧の［設定］をタップして、［セキュリティ］をタップします。

［画面のロック］をタップして、パスワードを設定、あるいは変更します。



画面上の点を決まった順になぞる「パターン」ロック解除も選べます。

16 実はうっかり侵害しているかも!? 著作権や肖像権

お気に入りのマンガや面白かったテレビ番組の映像など、友だちにも見せたくなります。けれども、SNSや動画共有サイトにアップしてしまうと、著作権の侵害にもなってしまいます。

作品には著作権がある

写真や動画、イラストや漫画、文章や音楽、音楽の歌詞にも制作者の著作権があります。家に遊びに来た友だちに見せるぶんには問題ないですが、多くの人が見ることができるSNSやブログなどにアップしてしまうと、著作権を侵害することになります。

芸能人にも一般人にも肖像権がある

また、もう1つ気をつけなければならないのが、肖像権です。芸能人など有名人だけでなく、一般の人にも肖像権があります。

被写体が一般人であっても有名人であっても、あなたが撮影した写真を無断で公開すると肖像権を侵害することになります。もし、友達の写真をSNSで公開したいときには、必ず許可をとるようにしましょう。また、町中など撮った写真に、周囲の人が写っている場合には、顔が見えないように公開するなど配慮が必要です。

なお、ルールを守ることで、他の人の作品を引用することも可能です。以下で紹介するサイトなどをご参照ください。

著作権について学べるサイト

著作権情報センター
http://www.cric.or.jp/index.html

「著作権Q&A」などで、著作権について基本的なことから学ぶことができます。

文化庁
http://www.bunka.go.jp/

著作権について制度を整備する文化庁のサイトです。

マンガでわかる著作物の利用
http://chosakuken.bunka.go.jp/chosakuken/h22_manga/index.html

著作物の利用方法について、マンガで学び、クイズに挑戦できます。文化庁のサイトからリンクされています。

※本ページに掲載している情報は、本書作成時点の内容です。ホームページアドレス（URL）や内容は変更となる可能性があります。

17

知らない人から メールが届いても返信しない

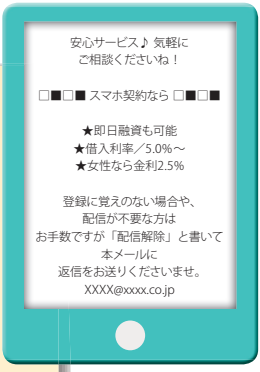
実は不特定多数に送られている

迷惑メールは、特定の相手を狙い打ちするとは限りません。適当なアルファベットを組み合わせてメールアドレスを作成し、不特定多数の人に送信している場合があります。

知らない相手からのメールをうっかり開いたとき、「今後、メールが不要なら返信してください」のように記載されていても、返信してはいけません。相手は適当なメールアドレスに送信しているだけです。返信すると、自分のメールアドレスは実際に人が使用していることを知らせることになります。そして、以降はもっとたくさんの迷惑メールが届くようになります。

リンクのクリックもNG

また、迷惑メールの中には、「お楽しみ」「無料」「もうかる」など、興味をひく言葉がいっぱい書かれています。そして、好奇心をそそる文章に続けて、リンクが用意されています。いくら気になったとしても、こうしたリンクをクリックしてはいけません。



被害にあわないために

- **メールの送信者に心当たりがあるか**
  メールアドレスを教えていないような、知らない人からメールが届いたときは注意が必要です。
- **件名が「緊急」や「重要」など注意をひく単語がないか**
  注意や不安をあおって、添付ファイルを開かせたり、リンクをクリックさせたりさせるのが目的です。
- **自分のメールアドレスが送信元になっていないか**
  迷惑メールによっては、自分のメールアドレスが送信元として表示されるタイプの、なりすましメールもあります。自分が送った覚えのない自分自身からのメールには注意してください。
- **件名や本文が文字化けしていないか**
  海外からの迷惑メールも多くあります。件名や本文、差出人名が文字化けしていたり、変な日本語表現や表記が使われていたりしたときは注意してください。

Keyword

スパムメール

望まないのに届く迷惑なメール全般のことをスパムメールと言います。一方的に送りつけられる広告のメール、サーバーに負担をかけたり、詐欺の内容を含んだりする悪質なメールも含まれます。

18

架空請求に応じない

サービスを利用したり、商品を購入した覚えがなくても、請求のメールが届いたり、請求画面が表示されて驚くことがあります。もし、まちがって過去に怪しいサイトを見てしまった経験があると、こんなときはより焦ってしまうことでしょう。

ページを開いただけでは請求されない

通常、有料サービスの利用時や商品の購入時には何度も確認画面が出るので、開いただけで支払いが発生することはありません。身に覚えのないメールが届いたり、サイト閲覧中に急に請求画面が表示されたりしたら、架空請求だと思ってまちがいないでしょう。無視してください。

例えば、「有料のアダルトサイトに登録されています。退会する場合はこちらをクリックして退会手続きを行ってください」「料金を支払わなければ法的手段に訴えます」といった内容のものがあります。すべて、閲覧者から個人情報やお金を引き出すための罠です。請求画面が表示された場合も、相手に連絡をしてはいけません。

万が一、誤って高額な有料サイトを利用してしまっていたら、消費生活センターに相談してみましょう。13ページで紹介している「国民生活センター」のサイトに連絡先が掲載されています。

請求画面が表示されても慌てない

例えばアダルトサイトなどで、「18歳以上ですか？」という質問に、「はい」をクリックしただけで、「ありがとうございます！　会員登録が完了しました」といった画面が表示されるということがあります。会費を請求する場合や、退会するには費用が発生するなどと書かれています。請求された費用を支払ってはいけません。また、「退会する場合はこちら」のようなボタンやリンクをクリックして画面を進めてはいけません。すみやかに画面を閉じましょう。

ワンクリック詐欺の新手口

ワンクリックしてサイトを開いただけなのにいきなり請求画面が表示されるのが、“ワンクリック詐欺”の手口です。最近ではスマートフォンを対象にしたワンクリック詐欺も増えています。中にはサイトを開くとシャッター音を鳴らして、ユーザーの顔写真を撮影したかのように思わせる新手口も登場しています。実際には撮影されたわけではないですし、他の詐欺と同じように支払いは発生しないので、応じる必要はありません。

19

ネットバンキングで注意する事

銀行の連絡を装う「フィッシング詐偽」

個人の情報を盗み出す「フィッシング詐欺」を行うメールが出回っています。手口の例としては、まず銀行やゲーム会社、ポータルサイト、インターネットプロバイダーなどからの連絡を装ったメールを送りつけます。企業からのメールだと思って安心して開くと、「システムの変更に伴い、カード番号と暗証番号の入力が必要になりました」といった内容です。メール中のリンクをクリックすると、企業ページそっくりの偽サイトが開き、カード番号やログイン情報など個人の情報を入力させます。

盗んだ情報からお金を引き出されたり、勝手にログインされたりするなどの被害が起きています。

Apple IDとパスワードを盗まれて、勝手にiTunes Cardを購入されてしまうという被害も増えています。iTunes Cardはインターネットで利用できる電子マネーで、iTunes Storeなどで音楽やアプリを購入できます。

メールが届いても無視する

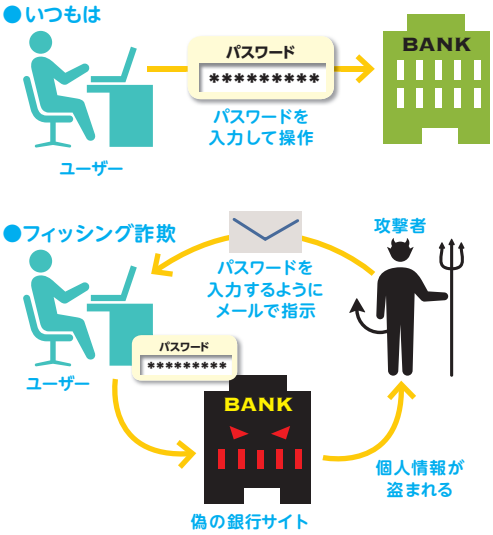
銀行などの金融機関やその他の会社から連絡してきて、個人の情報を入力させることはありません。このようなメールが届いても、リンクをクリックしたり、返信したりしてはいけません。心配なら、発信元になっている会社に問い合わせてみましょう。詐欺メールが発生しているという情報が、各社のサイトに掲載されていることがあります。

フィッシング詐欺について参考になるサイト

フィッシング対策協議会
https://www.antiphishing.jp/

現在報告されているフィッシング詐欺情報や、対策などが紹介されています。怪しいと思うメールが届いたら確認してみましょう。

フィッシング詐欺



20

知っておきたい メールのセキュリティ設定

入力したメールアドレスが悪用される

メールアドレスを知らせた覚えのない相手から届く、広告や勧誘などの迷惑メールがあります。件名や内容が外国語の迷惑メールもあります。ほとんどは、以前インターネットのサービスを利用したときに入力したことのあるメールアドレスが悪用されたものです。また、アルファベットを適当に組み合わせて作成したメールアドレスに、自動送信される場合もあります。

万が一怪しいメールを開いてしまったとしても、こうしたメールに返信したり、リンクをクリックしたりしてはいけません。迷惑メールがより増えたり、不当な請求が届くようになったりします。うっかり開くことでウイルスに感染することもあります。

画像や添付ファイルは開かない

このように、外部とデータをやり取りするメールは、ウイルスの感染源になりがちです。特に、添付ファイルにウイルスが付加されていて、開くと同時に感染することがあります。また、メールに貼り付けられた画像を表示するだけで、ウイルスに感染することもあります。メールソフトの設定で、画像は非表示、添付ファイルはいきなり開かないようにしておくと、感染を防ぐことができます。

また、JavaやAdobe製品がウイルスに

相手によってメールアドレスを使い分ける

迷惑メールの対策の1つとして、複数のメールアドレスを使い分ける方法があります。家族や友人などの親しい相手用、インターネットバンキング用、インターネットショッピング用、SNSなどのコミュニケーション用といった具合です。

フリーメールアドレスを利用すれば複数のアドレスを取得できます。迷惑メールが届くようになったら、そのメールアドレスを破棄して、新たなメールアドレスを取得するようにします。メールを変更の連絡をするのは面倒かもしれませんが、大量に迷惑メールが届くようになったら、変更するとよいでしょう。

また、複数使い分けることによって、どこから情報が漏れたのか、予想することもできるでしょう。

狙われ、感染するケースも多くあります（27ページ参照）。これらのプログラムやアプリがインストールされている場合、常に最新状態に保つようにしましょう。

セキュリティソフトを導入すれば、メール受信の直前に添付ファイルのウイルスチェックを行うことができます。このとき、迷惑メールや詐欺メールを自動的に分類することも可能です。

迷惑メール対策の参考になるサイト

迷惑メール相談センター（日本データ通信協会）
http://www.dekyo.or.jp/soudan/

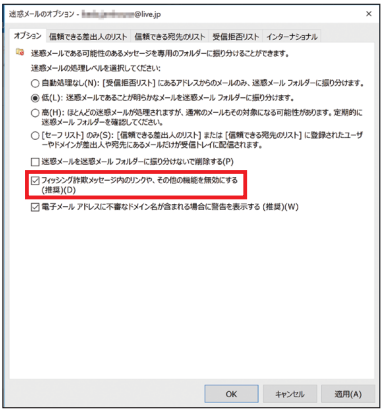
日本データ通信協会が運営するサイト。迷惑メールに関する相談や情報を受け付けています。迷惑メールの種類や迷惑メールを予防する方法、迷惑メールを受け取ったときはどう対応したらよいのかなどが掲載されています。

Keyword

Java

ブラウザーソフトの中で遊べるゲームや、便利に使えるアプリの中には、“Java”（ジャバ）という動作環境を使用するものがあります。最新のJavaを入れておかなければ、アプリを利用できません。最近では、Javaを悪用するウイルスなども登場しているため、常に最新の状態に更新して、対策する必要があります。

メールソフト「Outlook」の「迷惑メール」をクリックし、「迷惑メールのオプション」を選択します。



迷惑メールの処理レベルのほか、フィッシング詐欺メールのリンクを無効にするなどの設定もできます。

セキュリティソフトの「カスペルスキー　2016」。トップ画面にある［設定］をクリックし、［プロテクション］の［迷惑メール対策］をクリック。

右上のスライドボタンをオンにすると、セキュリティレベルを設定できます。

21

Windowsは最新状態にアップデートしておこう

OSにも弱点がある

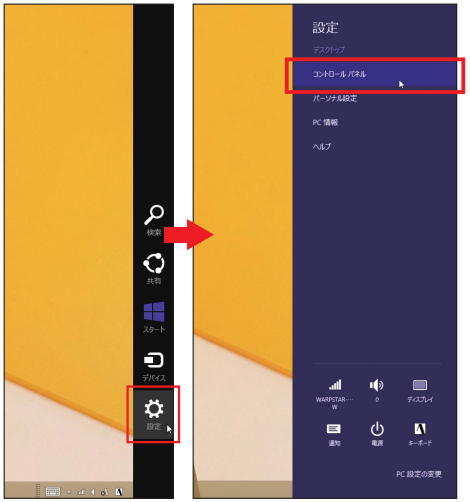
パソコンを使っていて気になるのは、データを壊したり情報を盗んだりする、コンピューターウイルスや、スパイウェアなどの悪質なプログラムの存在です。実は、パソコンの基本ソフト（OS）にも弱点があります。攻撃者は、この弱点からパソコンを攻撃したり、侵入したりしようとするのです。

基本ソフト（OS）のWindowsが入っているパソコンをお使いの方は多いでしょう。ユーザー数の多いWindowsは、攻撃者による標的にされやすいのです。

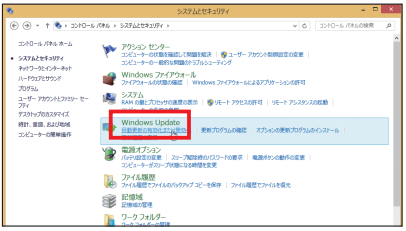
更新プログラムでアップデート

開発元のマイクロソフトは、Windowsに弱点が見つかると、問題を修正するための更新プログラムを配布します。そのため、Windowsを使い続けるには常に更新プログラムを入れてアップデートすることが必要です。もし、アップデートせずに、弱点を放置していると、攻撃を受けやすい危険な状態でパソコンを使うことになります。ここではWindowsのシステムとセキュリティ設定画面で、「自動アップデート」の設定になっていることを確認しておきましょう。

Windows8.1の場合



Windows 8.1の場合、デスクトップでマウスポインターを画面の右上に移動し、チャームが表示したら［設定］をクリック。［設定］メニューの［コントロールパネル］をクリックします。Windows 7の場合、スタートボタンをクリックして、［コントロールパネル］を選択します。



コントロールパネルが表示されたら、［システムとセキュリティ］をクリックします。［Windows Update］の［自動更新の有効化または無効化］をクリックします。

［更新プログラムを自動的にインストールする（推奨）］が選ばれていることを確認します。もし、他の項目になっていたら、ここで選択しましょう。［OK］をクリックします。

コンピューターウイルスやスパイウェアってなに？

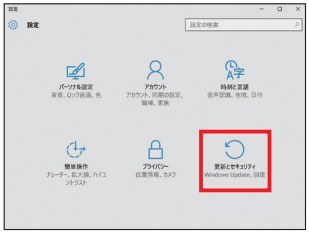
コンピューターウイルスは、パソコンに侵入して動作する悪質なプログラムです。たとえば、パソコンの中のファイルを壊したり、パソコンを起動できなくしたりします。コンピューターウイルスの中には、自分自身を複製して、広めるものもあります。もし感染すると、メールアドレスの連絡先に勝手に送信されて、友達のパソコンにも感染させてしまうことがあるのです。 また、パソコンに侵入用の裏口を作るウイルスもあります。パソコンを遠隔操作して、他のコンピューターなどを攻撃することが目的です。

スパイウェアは、表示したホームページの情報や、入力した文字の情報などを記録し、送信するプログラムです。ソフトメーカーが情報収集のために、他のプログラムと一緒にインストールさせることもあります

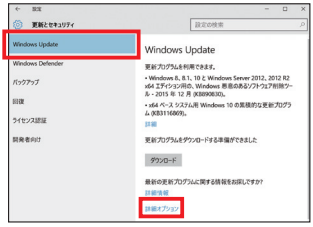
Windowsだけでなくアプリや実行環境のアップデートも大切

危険なコンピューターウイルスに感染しないため、Windowsアップデートは欠かせません。また、ソフトウェアやソフトウェアを実行するための動作環境もアップデートが欠かせません。最近では、利用者の多いAdobe系のソフトウェアが狙われたり、プログラムの実行環境であるJavaがターゲットにされる例もあります。そして、次に解説するセキュリティソフトのインストールも必要です。

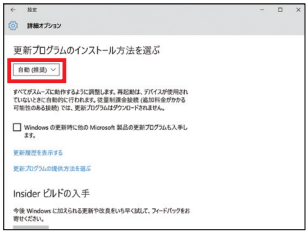
Windows10の場合



スタートメニューから［設定］を選択して、［設定］画面を開いたら、［更新とセキュリティ］をクリックします。



［Windows Update］を選択し、［詳細オプション］をクリックします。



［更新プログラムのインストール方法を選ぶ］で、［自動（推奨）］が選ばれていることを確認します。

22 セキュリティソフトは必ず入れておこう

パソコンにもスマートフォンにも入れておく

パソコンの基本ソフト（OS）も、ある程度のセキュリティ機能を持っています。しかし一方で、インターネットの世界では常に新しいコンピューターウイルスが誕生していますし、これまでにない方法でパソコンを攻撃するプログラムも登場しています。こうした新しい脅威にすばやく対応するには、セキュリティソフトが必要です。

また最近では、Androidスマートフォンをターゲットとしたウイルスも急増しています。パソコンだけでなく、スマートフォンにもセキュリティソフトを入れておく必要があるのです。

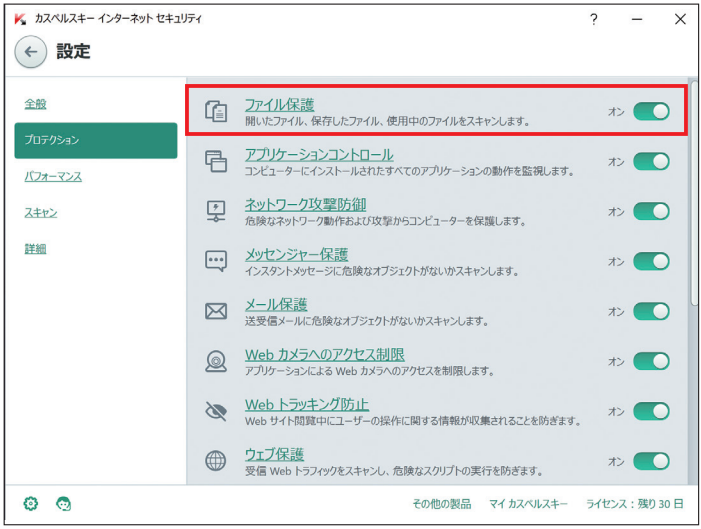
セキュリティソフトは、さまざまな機能でパソコンを守ってくれますが、例えば、カスペルスキーのセキュリティソフトの場合には次のような基本機能があります。

- ウイルススキャン
- ファイアウォール

それぞれ、どのように働いてくれる機能なのか、見てみましょう。

●ウイルススキャン

パソコンの中にコンピューターウイルスが侵入していないかを検査する機能です。



画面は、「カスペルスキー2016」の設定画面。「ファイル保護」がオンになっていれば、ウイルススキャンが実行されて、コンピューターウイルスを検出できます。

※画面は「カスペルスキーインターネットセキュリティ2016」のものです。

大きく分けると、常時監視する機能と定期的に検査する機能の2つがあります。そして、発見した場合には、ファイルを削除したり隔離したりする対策を行います。身体の中に進入したウイルスを退治するワクチンのような役割をする機能です。

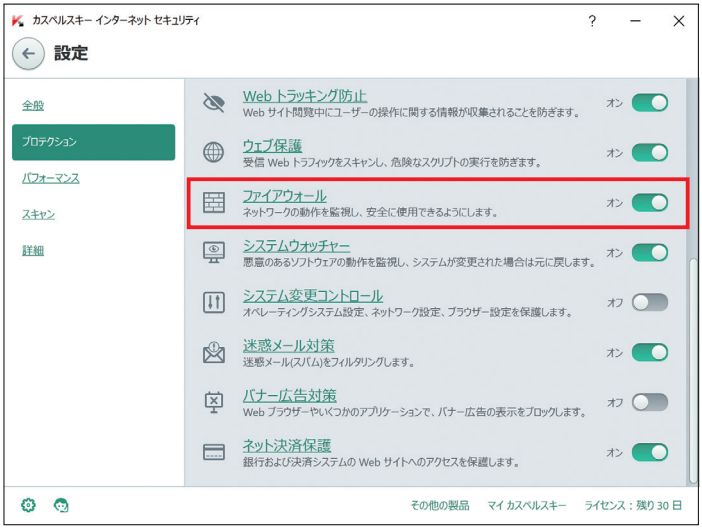
　またそれだけでなく、パソコンの中で怪しい動きをするプログラムがないかいつも監視する機能も搭載しています。例えば、勝手にメールを送ろうとしたり、ファイルを改変しようとしたりするなど、問題ある動きをするプログラムを見つけたら、すぐに停止して、知らせてくれます。また、USBメモリーなどの外部機器を接続したときにも、チェックを実行してくれます。

●ファイアウォール

　インターネットを閲覧したり、メールをやり取りする際には、パソコンとインターネットの間に通信が発生します。ファイアウォールはこの通信とデータを監視してくれます。そして、怪しいデータが出入りしようとしている通信を見つけたらブロックしてくれます。

スマホもウイルスに感染する

ウイルスに感染するのは、パソコンだけとは限りません。最近では、スマートフォンをターゲットにするウイルスも登場しています。特にアプリを自由に配布できるAndroid端末は危険度が高いため、カスペルスキーをはじめとしたソフトウェアメーカーは、Android向けのセキュリティソフトも提供しています。



「ファイアウォール」が有効になっていれば、ネットワークを監視して、怪しいデータの出入りをブロックできます。

※画面は「カスペルスキーインターネットセキュリティ2016」のものです。

23 セキュリティソフトの定義データベースは常に更新する

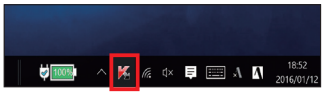
セキュリティソフトを入れておけば、それだけで安全というわけではありません。インターネットには常に新しいコンピューターウイルスが登場しています。そのため、定義データベースも常に更新（アップデート）しておく必要があるのです。

最新のデータベースに更新

セキュリティソフトにとって、コンピューターウイルスを見つけるために必要なものが「定義データベース」です。

もし、古い定義データベースしか持っていなければ、新しいコンピューターウイルスを見つけられません。そのため、常に新しくしておく必要があります。

セキュリティソフトで、定義データベースが最新になっているかどうか、そして常に自動で更新する設定になっているかどうかを確認しておきましょう。



カスペルスキー2016が入っているパソコンの場合、画面右下のタスクトレイのアイコンをクリックします。アイコンの表示がない場合、△をクリックして、選択します。

セキュリティソフトの設定画面が表示されます。[アップデート]をクリックします。

定義データベースが最新であることを確認できます。[設定]をクリックします。

[新しいバージョンのインストール方法]を確認できます。[新しいバージョンを自動的にダウンロードしてインストールする（推奨）]を選んでおくようにしましょう。

※画面は「カスペルスキーインターネットセキュリティ2016」のものです。

Keyword

定義データベース

セキュリティソフトがコンピューターウイルスを見つけるためのデータベースです。プログラムのふるまいなどからウイルスかどうかを判断し、ウイルスに対応した措置を実行します。

すべての保護機能をオンにしておこう

セキュリティソフトには、ウイルススキャンやファイアウォールなど、様々な機能があります。設定内容はソフトによって異なりますが、メール保護やウェブ保護などの機能を持つ場合もあります。設定画面を開けば、個別の機能をオン／オフできます。すべての機能をオンにした状態で使うことで、安全性を高められます。

24 ライセンスを更新して必ず新しいプログラムにバージョンアップしよう

パソコンにセキュリティソフトを入れて、定義データベースも更新しておけば、コンピューターウイルスへの対策が行えます。しかし、攻撃する側も常に進化しているため、これまでにない脅威や攻撃手法が登場する可能性があります。

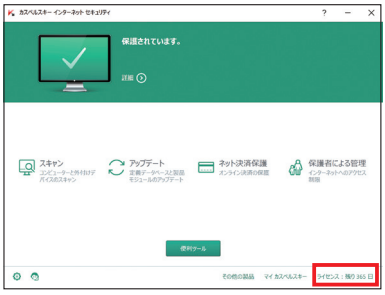
最新バージョンで守ろう

そこで、セキュリティソフトそのものも常に新しくして対抗したり、新しい機能でパソコンやスマートフォンの守りを固めることが必要なのです。

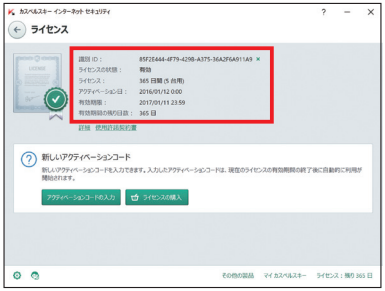
例えば、最新のカスペルスキー2016を入れると、Webカメラを悪用して私生活を盗み見しようとする行為や、勝手にファイルをロックして見られないようにするランサムウェアにも対抗できます。

有効期限に注意

セキュリティソフトには、1年や3年などのライセンス有効期間が設定されています。有効期間が過ぎると定義データベースのアップデートやサポートサービスが受けられなくなり、危険な状態でパソコンを使うことになりますので必ずライセンスを更新してください。また、カスペルスキー製品は毎年新しいバージョンを発表していますので、新しい脅威に対応するためにも必ずバージョンアップするようにしましょう。カスペルスキー製品のバージョンアップは無料で行えます。



現在使っているウイルスソフトがいつまで使えるのかは、「ライセンス」の残り日数で確認できます。



日数の部分をクリックすると、さらに詳しく有効期限やライセンスの状態などがわかります。

※画面は「カスペルスキーインターネットセキュリティ2016」のものです。

Keyword

ライセンス

ソフトウェアを使うための“使用権”です。これにより、不正ユーザーによる使用を防ぐことができます。ライセンスには、1年間、3年間などの期限が設定されている場合があります。継続して使用するには、ライセンスを更新する必要があります。

インターネットを安全に楽しむため

「STOP. THINK. CONNECT.」

インターネットを楽しく利用するためには、安全に使うための知識や、セキュリティ設定について知ることが必要です。インターネットを安全に利用するためのキャンペーン「STOP. THINK. CONNECT.」では、次の3つのステップで確認することを提案しています。

「STOP. THINK. CONNECT.」のサイト
http://stopthinkconnect.jp/

STOP（立ち止まって理解する）

インターネットは便利ですが、一般社会と同様、そこには危険もあります。どのような危険があるかを知り、解決策をどのように見つけるかについて、一旦、立ち止まって調べましょう。

THINK（何が起こるか考える）

様々な警告の見極め方を知る必要があります。警告を確認したら、これから取ろうとする行動がコンピュータやあなた自身の安全を脅かさないか考えましょう。

CONNECT（安心してインターネットを楽しむ）

危険を理解し、十分な対策をとれば、インターネットをより信頼できるようになるでしょう。

米国 APWG（Anti-Phishing Working Group）と NCSA（National Cyber Security Alliance）が共同で、インターネットを安全に使うための消費者向けセキュリティ普及啓発キャンペーン「STOP. THINK. CONNECT.」を行っています。

日本でも、フィッシング対策協議会に参加する、情報セキュリティ対策事業者、銀行、クレジットカード会社、ショッピングサイト事業者など様々なメンバーが、日本国内のサイバー犯罪防止のための対策や啓発活動を行っています。

「STOP. THINK. CONNECT.」のサイトでは、キャンペーンや活動の報告、「安全にモバイル端末を使うためのヒントとアドバイス」「SNSとネットいじめ対策のヒントとアドバイス」といった学習資料の配布などを行っています。インターネットを安全に利用するためのヒントになる情報が数多くあるので、ぜひ活用してください。

30日間無料体験版のご案内

カスペルスキー
マルチプラットフォーム セキュリティ

強くて、軽快。だから、使いやすい。

30日間無料

ご検討中のお客さま

無料ですべての機能を
お試しいただけます。

▼ダウンロードはこちら

http://kmps.jp/1605

最新ウイルスから守る

独自のクラウド技術により、最新のウイルスや脅威にも瞬時に対応します。

ウェブサイトの閲覧を安全に

個人情報を盗んだり、ウイルスに感染させる危険なサイトへのアクセスを防止します。

ネット決済も安心

クレジットカード番号や暗証番号などが盗み取られるのを防止します。

お子様のネット利用を安全に

有害サイトのブロックや、ネットの利用時間を制限することができます。

マルチプラットフォーム対応

Windows、Mac、Androidに対応。パソコン、スマホ、タブレットの各種デバイスでご利用いただけます。

365日無料でサポート

電話とWebで年中無休のサポートをご提供。国内の専門スタッフがご対応します。

「セキュリティとモラルのガイドブック」をダウンロード提供中!

セキュリティとモラルのガイドブック

http://kasperskylabs.jp/activity/csr/book.html

PDF版は無償でダウンロードいただけます。冊子もご用意しております。詳細は上記のページでご確認ください。

ウイルス・スパイウェア倒し

不正アクセス落とし

迷惑メール刈り

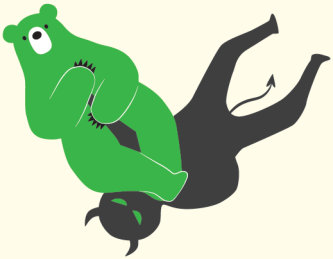
どんな脅威にも死角なし。

カスペルスキーのセキュリティ製品は、
最新の脅威や巧妙化するネット犯罪にもしっかり対応。
その圧倒的な防御力から、国際的に権威のある評価機関により、
2015年の最優秀製品賞※を受賞しました。
年々増加するIT上の脅威からあなたを守ります。

※AV-Comparatives 2015年度 年間最優秀製品賞（Product of the Year）を受賞。
「カスペルスキー インターネット セキュリティ」は、2015年に実施された主要な
8つのテストにおいて、すべて最高位の「Advanced+」を受賞し、テストに参加した
21のWindowsセキュリティ製品の中で最高位にランク付けされました。

ネットワーク攻撃払い

危険・詐欺サイト払い



個人情報保護固め

ネットの守り神
グリーンベア
リアルとバーチャルを行き来し、ウイルスから人々を守っている。世界の勲章を集めるために日々活躍中。本名は、まだ誰も知らない。

4 562302 692728

詳しい情報は
カスペルスキー 検索

カスペルスキー
IT上の脅威から世界を守る

CSR-3001-201602