先生・保護者の方へ　先生や保護者の方向けの情報です

スマートフォン
スマートフォンのリスクをご存知ですか？

掲載日：2013年3月29日

スマートフォン等を安全・便利に使うために

スマートフォンやタブレット端末の普及に伴い、機器の品質、通信サービス、契約・解約や料金についてなど、様々なトラブル相談が増えています。また、架空請求の被害や、コンピュータウィルス・不正アプリなどによる個人情報の流出など情報セキュリティに関する事件も起きています。

スマートフォンやアプリの機能・性能をよく確かめるとともに、セキュリティ対策を行ってトラブルにあわないようにしましょう。 自分が契約している内容や課金体系などを把握しておくことも重要です。

スマートフォンの盗難・紛失対策 | スマートフォンのウイルス対策 | 無線LANスポットの利用には注意を！ | SNSの利用時の注意点は？ | 無料通話アプリは安全なのかな？ | スマートフォンのフィルタリング | リンク

スマートフォンの盗難・紛失対策

写真や動画データなどたくさんのデータが保存できるスマートフォン！ もし、なくしてしまったら、どうなるだろう？

＊スマートフォンは、便利なだけに盗難・紛失に備えた対策が必要です。

スマートフォンには、自分自身や友達に関するたくさんの情報が保存されています。万一、盗難にあったり、紛失をしてしまった場合でも、重要な情報が流出したり、スマートフォンが不正に使用されないための対策をしておきましょう。

盗難・紛失対策

- パスワード（暗証番号）等でスマートフォンをロックしましょう。盗難や紛失対策として効果的です。
- 他人に盗まれては困るような大切な情報を保存するなら、データの暗号化（注1）が必要です。
  （注1）大事な情報を他人には知られないようにするため、データを見てもその内容がわからないように、定められた規則でデータを変えてしまうこと
- 紛失時には、携帯電話やモバイルパソコンと同じようにリモート（遠隔）からの強制ロックやデータの強制消去サービス、位置情報の確認サービスを利用しましょう。
- 拡張メモリスロットがある場合は、安易にデータを保存するのは避けましょう。SDカードなどにデータを保存する場合は、暗号化やパスワードロックを行っておかないと、盗難・紛失時に簡単に読み取られてしまう危険性があります。
- 万一紛失した場合はサービスを停止してもらうために、携帯電話会社の連絡先の電話番号を確認・記録しておきましょう。

スマートフォンのウイルス対策

自由にアプリをインストールしてパソコンと同じように使えるスマートフォン！パソコンのようなウイルス対策はしなくていいのかな？

＊スマートフォンは、パソコンと同等のウイルス対策が必要です。

スマートフォンは高度に小型化したパソコンです。そのため、パソコンと同様に、コンピュータウイルスによる被害や不正アクセスによる被害、不正なサイトに誘導されて個人情報を入力してしまったり、不当な料金の請求画面が表示されてしまったりするような被害にあう可能性もあります。

被害にあわないために

スマートフォンのOS（オペレーティングシステム）（注2）やアプリ（注3）は、常に最新の状態に更新しましょう。OSやアプリには、情報セキュリティ上の問題となる可能性がある弱点（脆弱性）があるために、ウイルス感染や不正アクセスの原因となります。
（注2）コンピュータを動作させるための基本的な機能を提供するシステム全般のこと
（注3）コンピュータのOS上で動作するソフトウェアのことを「アプリケーション」といい、「アプリ」と略されて使われます。

- アプリの入手方法に気をつけましょう。正規のアプリ・ストア以外では、ウイルスが含まれている可能性が高くなります。アプリをインストールする場合は、必ず正規のアプリ・ストアからインストールするようにしましょう。
- アプリをインストールする際に「アクセス許可」の画面が表示される場合があります。アプリの内容とは無関係な電話帳、位置情報などに対してアクセス許可を求められた場合は、インストールを中断しましょう。
- パソコンと同様に、専用のセキュリティソフト（アプリ）を利用しましょう。

無線LANスポットの利用には注意を！

街中で見つけた無線LANスポット（注4）。誰でも使えて便利そうだけれど、問題はないのかな？
（注4）外出先において、ユーザーが所持する情報機器からのネットワーク接続を可能にする場所や施設

注不特定多数の人が使える無線LANスポットでは、個人情報漏洩（ろうえい）の危険性があります。

スマートフォンで、携帯電話の回線以外の無線LANスポット（Wi-Fi環境）などを利用する場合は、安全な通信が確保できるかどうかわかりません。特に不特定多数の人が使える無線LANスポットでは、個人情報漏洩の危険性もありますので、注意しましょう。

利用上の注意点

- インターネットなどへの接続経路を暗号化していない無線LANスポットでは、その通信内容をすべて簡単に傍受することができます。不特定多数の人が使える無線LANスポットを利用しているときに、ログイン情報やパスワードなどの大切な情報を入力するなどの利用は避けた方が良いでしょう。
- 無線LANスポットは、個人で簡単に設置することができます。街中では、スマートフォンから様々な無線LANスポットを見つけることができますが、通信内容を傍受しようとあなたの接続を待ち構えている悪意のある人が設置した無線LANスポットである可能性もあります。誰が設置したかわからない無線LANスポットに接続してはいけません。

SNSの利用時の注意点は？

いつでも自由に書き込みをして友達とのコミュニケーションが楽しめるSNS（ソーシャル・ネットワーキング・サービス）。どういう点に気をつければいいのかな？

＊SNSで書き込んだ内容は、誰が見ているかわかりません。

SNSでの書き込みにより、自分や友達のプライベートな情報を流出させてしまったり、自分が誹謗（ひぼう）中傷（ちゅうしょう）をうけるトラブルに発展する危険があります。一度書き込んだ内容は、完全に取り消すことができないため、慎重に行いましょう。

″書き込み″の注意点

- 目撃した有名人のプライベートな情報を書き込んでしまい、批難の対象となってインターネット上で誹謗中傷されるトラブルが発生しています。SNSで書き込んだ内容は完全に消すことは難しく、半永久的にインターネット上に残ってしまいます。SNSで書き込みをするときは、写真なども含めて他人のプライベートな情報や個人情報が含まれていないかよく考えましょう。他人の迷惑にならないように気をつけることは、自分が誹謗中傷されることから守ることにつながります。
- スマートフォンで撮影した写真を公開するときは気をつけましょう。GPS機能の付いたスマートフォンで撮影した写真には位置情報が埋め込まれているため、SNSで公開する場合は投稿する際に位置情報を削除する設定をしないと、自宅などの場所が特定されてしまう可能性があります。

″なりすまし″の注意点

- SNSには、有名人などになりまして他人の注目を集めようとしたり、個人情報やクレジットカード情報などを盗み出そうとする悪意のある人もいるのが実態です。実名を公開しているSNSであっても、プロフィールや写真は簡単に偽ることが可能です。簡単に信用しないようにしましょう。
- 知らない相手の書き込みにあるリンクを興味本位で不用意にクリックしないように気をつけましょう。リンク先からウイルスをダウンロードさせられて感染してしまうトラブルも発生しています。

無料通話アプリは安全なのかな？

無料で電話やメッセージのやりとりができる便利な無料通話アプリ。 何に注意すればよいのでしょうか？

＊知らない人からメッセージが！出会い系（注5）のツールとして悪用されてトラブルも。
（注5）異性または同じ趣味趣向の者等との出会いの場を提供するサイトの総称です。

無料通話アプリは、友達とのコミュニケーションツールとして便利ですが、出会い系のツールとして悪用されて無料通話アプリを通じて知り合った人と実際に会ってトラブルに巻き込まれるケースが発生しています。無料通話アプリによるトラブルの危険性を知って、上手に使いましょう。

利用上の注意点

- 知らない人からのメッセージに返信しない。
- 無料通話アプリを通して知り合った人を簡単に信用しない。誘われても実際に会いに行ったりしない。
- 無料通話アプリのIDは、ネット上の掲示板等に公開しない。
- アプリをインストールする際のアクセス許可をしっかり確認しよう。
  住所録（アドレス帳）などの個人情報が、外部に送信されてしまうことがあります。

スマートフォンのフィルタリング

神奈川県では、条例により18歳未満の方が携帯電話のインターネットを使う場合は、フィルタリングサービス（出会い系サイト、アダルトサイト、違法薬物サイトなどに接続できないようにする）の利用が義務付けられています。

スマートフォンは、携帯電話回線のほかに、無線LAN回線により、インターネットに接続することができます。青少年を有害情報から守るために、携帯電話回線、無線LAN回線、それぞれに対応したフィルタリングを設定するか、通信を制限する機能を利用してください。

携帯電話やスマートフォンの必要性、使い方について、親子で話し合い、適切な利用に努めましょう。