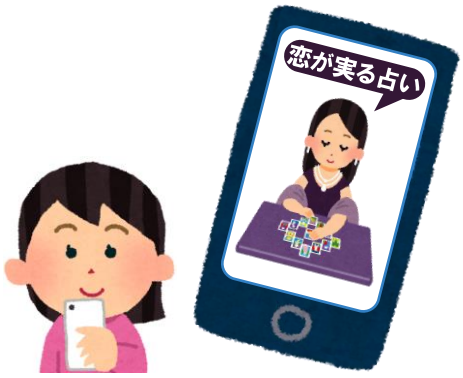
4-1 個人情報漏えい

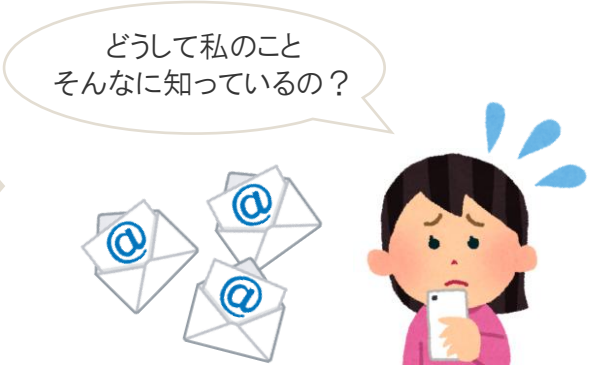
不正アプリやウイルスによる個人情報漏えい

占いアプリで趣味嗜好を入力し



メルマガに掲載されていた無料の占いをしようとアプリをインストールしたIさん。**好きなブランドや音楽など趣味嗜好に答えて、占いをする方法**でした。

大量の迷惑メールが届くようになった



すると、Iさんのスマホに**続々と宣伝のメールが届くようになりました**。その内容は、Iさんが占いの時に入力した趣味嗜好に合うものでした。

解説 個人情報に関するアクセス許可や入力欄には要注意

アプリやWebサービスを利用する際、個人情報の入力を求められることがあります。でも、取得した**氏名や住所、年齢、性別、メールアドレス**などを無断で二次利用したり業者に売ったりするために、**悪意を持って作られたものもある**のです。新しいアプリやサービスを利用する際は、友人に聞く、ネットで調べるなどいくつかの方法で評価をチェックし、安全性を確認してから利用しましょう。また、Web上で配布されているアプリもありますが、ウイルスが潜んでいる可能性もあるため、必ず公式マーケットを利用しましょう。

小・中学生が常に心掛けたいこと

その1 フィルタリングと一緒にウイルス対策を

悪意のある仕掛けがあるサイトにアクセスしないためのフィルタリング。外からの攻撃を防ぐウイルス対策と覚えましょう。

その2 アプリやサービスは保護者に相談して使う

個人情報が必要なときはもちろん、新しく何かを利用したいときも保護者に相談し、許可をもらってから使うようにしましょう。

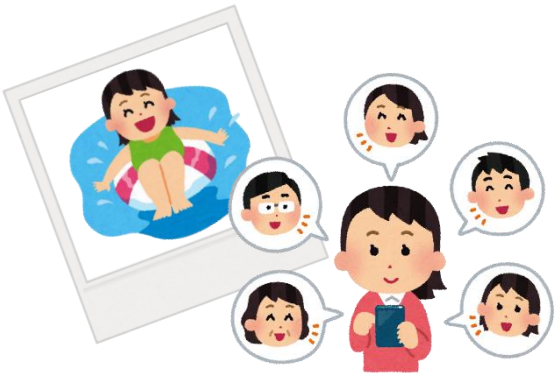
その3 自分がウイルスを広める可能性もあることを知る

1人が感染すると、家族や友人にも広まってしまうウイルス。自分だけでは終わらないことを忘れず、常に注意しましょう。

4-2 個人情報漏えい

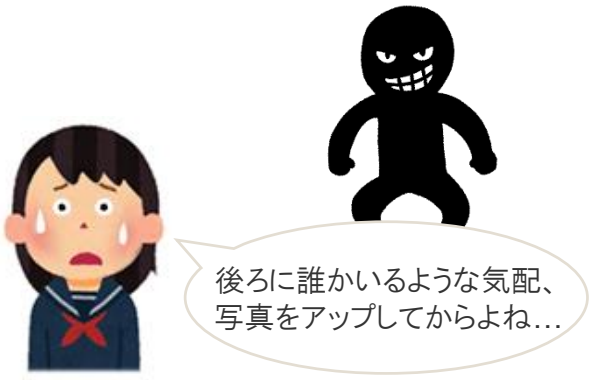
SNSなどへの投稿による個人情報漏えい

友人とシェアするつもりで写真を投稿し



友人と海に行ったJさん。友人にスマホで撮ってもらった写真が気に入り、**親しい人たちとシェアしようと思って、SNSに写真を投稿**しました。

付きまといを受けるようになった



数日後から、Jさんは下校時に後をつけられている気配を感じるようになりました。**投稿した写真で個人が特定されてしまったことが引き金**でした。

解説 写真の中の建物や地域の行事でも生活範囲は憶測できる

未成年者は、SNSなどを利用する際の個人情報の取り扱いにルーズな傾向があります。 基本的に誰でも見ることができるSNS、会話をするのは限られた友人だけだとしても、その**会話の中に名前や住んでいる場所、学校名などがあれば、写真を載せただけで個人が特定できてしまい、非常に危険**です。訪れた店や地域の行事などの話題でも、生活範囲が憶測できるので注意しましょう。また、友人が写っている写真を投稿すれば、(たとえ掲載許可をもらっていたとしても)その友人を同じ危険にさらすことになります。

小・中学生が常に心掛けたいこと

その1

自分がどこの誰かわからないのが安全

ネットに個人情報を書くのは、街中で名前や学校名を掲げているのと同じ。危険な上に悪用されるかも。気をつけましょう。

その2

個人を特定できそうな話はネットでしない

一つだけではわからなくても、複数あれば個人を特定できてしまうことはいっぱい。ネットでは用心しながら会話しましょう。

その3

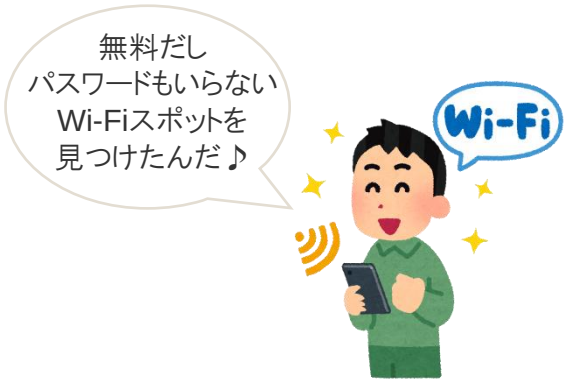
アプリの特性や設定を確認した上で利用する

位置情報入り写真を公開すると、撮影場所がわかります。アプリの特性や設定を確認し、不要な機能はOFFにしましょう。

4-3 個人情報漏えい

悪意あるWi-Fiスポットを利用したことによる情報流出

パスワード不要の無料Wi-Fiスポットで



K君は、**パスワードもいらず無料でネットに接続できる場所**を見つけました。家では電波が不安定なので、頻繁にそこに行ってネットをしていました。

通信内容が盗み見られた

K君の通信内容

- メール内容
- アクセス履歴
- 書き込み内容
- ID/パスワード

ほか

そのWi-Fiスポット（無線LANアクセスポイント）は、**通信内容を盗むために設置されたもの**でした。K君は、気付かないうちに通信内容を見られていました。

解説 ラッキー！が一転、個人情報の流出や悪用の恐れもある

スマホは、携帯電話事業者の回線（3G/4G/LTEなど）だけでなく、Wi-Fiスポットを使ってネットに接続することができます。でも、自宅に無線LAN環境が作れるように、Wi-Fiスポットは誰にでも設置できます。パスワード不要の無料Wi-Fiスポットがあると嬉しいかもしれませんが、**通信傍受やID・パスワードなどの窃取を目的で設置する人もいる**ことを忘れてはいけません。スマホのWi-Fi設定が**自動接続になっていると、悪意あるWi-Fiスポットにつながってしまう危険もある**ので設定を見直すことも大切です。

小・中学生が常に心掛けたいこと

その1 フィルタリングと一緒にウイルス対策を

外でWi-Fiを使うなら、Wi-Fiに有効なフィルタリングと共に、悪意ある攻撃からスマホを守るアプリや設定を活用しましょう。

その2 通信内容が盗み見られる危険性を知る

個人的な情報が多いスマホの通信内容。もし見られれば、悪用される可能性もあります。接続先は慎重に選びましょう。

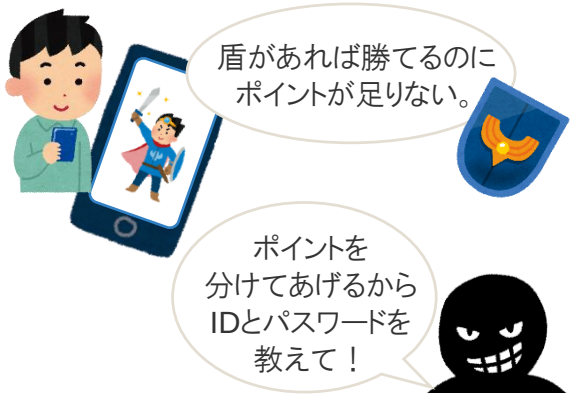
その3 外部から遠隔操作をされる可能性を知る

遠隔操作アプリやウイルスを送り込み、カメラなどを起動させて生活を覗くようなトラブルがあることを知っておきましょう。

4-4 個人情報漏えい

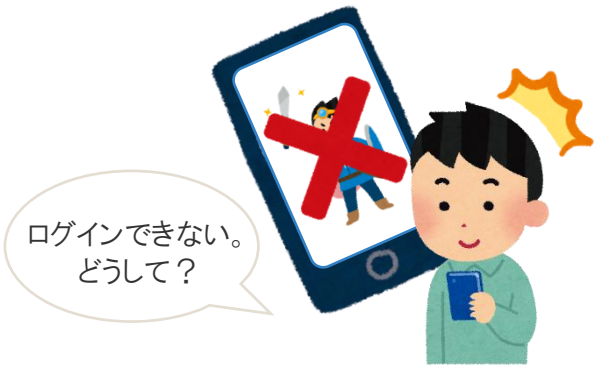
自らIDとパスワードを教えたことによる被害

他人にIDとパスワードを教えてしまい



L君は、ゲームを有利に進めるアイテムが欲しいのですが、ポイント不足で買えません。そのとき、「ポイントあげようか」というメッセージが届きました。

パスワード変更されゲームを乗っ取られた



ポイントをもらえるならとIDとパスワードを教えたら、**パスワードが変更された**らしくログインできません。L君は、**ゲームを乗っ取られてしまった**のです。

解説 IDとパスワードさえ分かれば、誰でもアクセスできるようになる

ゲームのポイントやアイテムを奪われたり、ネット上に保存している写真を盗み見られたり、IDを乗っ取られたり・・。ゲームやSNSなどの**IDやパスワードを他人に利用されて被害にあう**人が増えています。**どんなに親しくなっても、他人に自分のIDやパスワードを教えるのは危険**です。他人のIDとパスワードでログインすることは、不正アクセス禁止法に違反しているのですが、ネット上のサービスでは現物が存在するわけではないため、盗む、無断で立ち入ることへの罪悪感が鈍る傾向があり、注意喚起が必要です。

小・中学生が常に心掛けたいこと

その1 IDやパスワードは大切、しっかり管理する

利用者を特定するIDやパスワードは、親しい友人でも教えてはいけません。パスワードの工夫や定期更新も忘れずに。

その2 困ったら、信頼できる大人に相談する

仲間内で何とかしようとして、取り返しのつかないことになる場合も少なくありません。身近な大人に必ず相談しましょう。

その3 他人のIDでのログインは犯罪だと理解する

誰かのIDを使ってログインすることは、その人になりすましているのと同じ。犯罪行為だということを理解しましょう。