第3章

SNS・ネットとの付き合い方や情報モラルの重要性を知ろう

現代では、SNSを通じて、世界中の人たちと簡単につながりコミュニケーションできます。しかし、接する人がすべて自分と友好的であるとは限りません。SNSやネットでよくある危険やトラブルについて知り、対策や家族を守る方法を学びましょう。

1 SNSなどのネットとの付き合い方、守り方を知ろう

2 インターネットで守るべき法律やマナーを知ろう

3 便利なサービスや機能を利用して家族を守ろう

1 SNSなどのネットとの付き合い方、守り方を知ろう

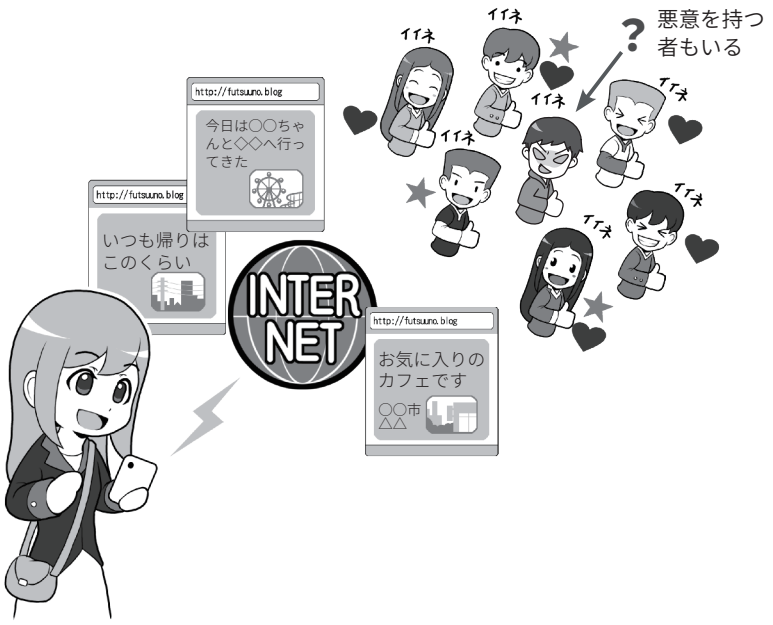
1.1 SNSなどのネットの楽しみ方と気を付けること

インターネットやスマホの普及により、今では、まるで隣に座っているかのようにチャットしたり、SNS▶用語集P.178で写真を送りあったり、映像付きのインターネット電話を使えば無料で顔を見ながらコミュニケーションができます。

一方、あなたがメッセージを発信するとき、それを受け取る人々の中には悪意を持った人や全く考え方が違う人がいることも忘れてはなりません。ネットを使ったコミュニケーションは人と人の意識のつながり合いを容易にしますが、同時に悪意を持った人等との接触も容易になるのです。

私たちは、ネットの世界をよく知って「この時代に合わせた、新しい付き合い方」を作り上げなければならないでしょう。悪意のあるものをしっかりと見分けて、善意のコミュニケーションの世界を作っていくことが必要です。

SNSやネットのコミュニケーションには落とし穴もある



SNSやネットのコミュニケーションは、距離を超えて世界中の人とつながることができます。なに気ない投稿は、多くの人の共感を得るかもしれませんが、その中には、犯罪に使える手がかりを探している悪意を持った人もいます。どうしたら悪意をかわしつつ、SNSやネットを楽しむことができますか？

1.2 SNSやネットの怖さ、こんなことが実際に起こっている

SNSやネットではどのようなトラブルに遭う可能性があるのでしょう。

SNSなどで、実際に会ったことがない同じ年ぐらいの子と友だちになり、どこかで会う約束をしたとします。しかし、待ち合わせ場所に行ってみると来たのは本人ではなくて別人でした。「○○ちゃんが待っているから連れて行ってあげる」といわれ、車に乗せられそうになりました。こんな風に誘拐・略取が行われます。

SNSに家の近くや普段立ち寄る場所、自分の写真などを上げていると、その情報からあなたを特定して、リアルのストーカーがやってくるかもしれません。

闇サイトなどを興味本位に覗いたりしていると、犯罪勧誘といって、顔も知らない人があなたを犯罪に誘ってくることもあります。最近では闇バイトが社会問題ともなっており、明らかな犯罪加担行為でない、一見、割のいい軽作業のような表現で勧誘し、本人情報を取られて脅されるケースもあります。闇バイトについて勧誘された、関わってしまった、不安があるなどの場合には、警

察庁で相談窓口なども開設しているので、適宜相談しましょう。

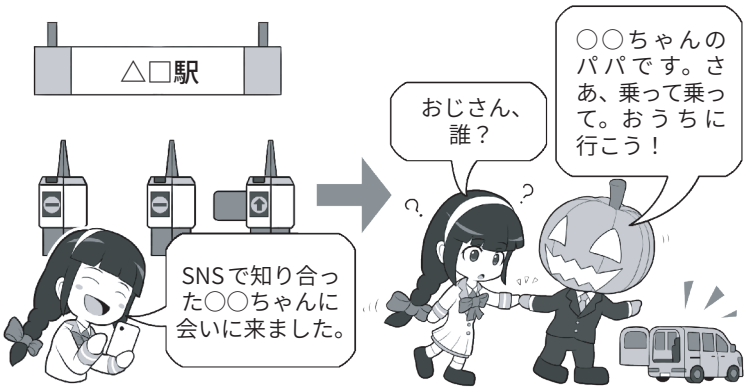
SNSのグループなどで、周りの雰囲気に流され、特定の人物のありもしない書き込みに同調したり、傷つけたり、仲間はずれにしたりする「ネットいじめ」をしたりされたりしてしまうかもしれません。

交際している相手が、「誰にも渡さないから」とあなたの裸の写真を要求してきて、信頼して渡したら、別れた後にその画像がネットに流出してしまうかも。それは、「リベンジポルノ」といって、相手が嫌がらせのために、写真をネットに投稿する行為ですが、その意図がなくても、相手のスマホがマルウェア▶用語集P.188に感染してネットに広く流出してしまうかもしれません。その写真は、消えない「デジタルタトゥー」(デジタルの入れ墨)として、以降あなたの人生に、ずっと影を落とし続けることになるかもしれません。

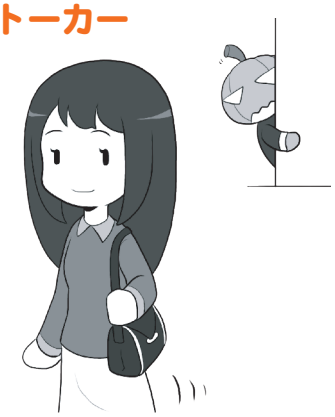
また、SNSを活用した詐欺が増えています。例えば、「SNS投資詐欺▶用語集P.185」は、インターネット上に著名人の名前・写真を悪用した嘘の投資広告を出したり、「必ずもうかる投資方法を教えます」などとメッセージを送ったりして、SNSへ誘導し、投資金などの名目で多額の金額を騙し取るものです。また、「ロマンス詐欺」は、SNSやマッチングアプリ▶用語集P.179などを通じて出会った者と、実際に直接会うことなくやりとりを続けることで恋愛感情や親近感を抱かせ、これを利用して、暗号資産の購入、架空の投資を促したり、必要な資金と称して、お金を振り込ませたりするものです。具体的な手口などは、警察庁が「SNS型投資・ロマンス詐欺」で公表しているので参考にしましょう。

この他にも、SNSやネットでは、さまざまなトラブルが発生することがあります。発信相手や情報の内容をネットだけではない複数のソース▶用語集P.184を確かめ、トラブルに決して巻き込まれないようにしましょう。

誘拐・略取



ストーカー

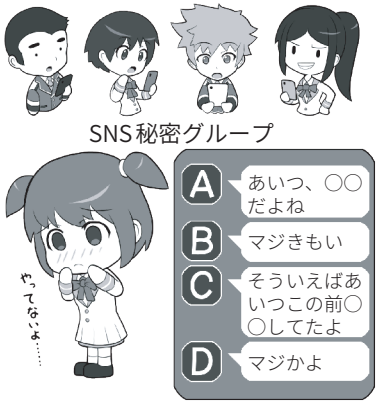


SNSで得た情報をもとに人物を特定し、リアルの世界でストーカーされる場合もあります。

犯罪勧誘

闇サイトなどと呼ばれる怪しいサイトで、面識がない者同士が集まって、犯罪を行うために仲間を探しています。

ネットいじめ



ノリでいじめに加わった結果、悲しい出来事が起きてしまったら、自分はそのときどう思うでしょう。

リベンジポルノ・デジタルタトゥー

元交際相手に、裸の写真をネットに投稿されるかも。ネットに広がった写真は消すことができません。

1.3 SNSやネットとの付き合い方の基本

SNSには、「いいね!」などの他の人からの反応や、コメントをもらうことができる機能があります。「いいね!」をたくさんもらえると嬉しい反面、少ないと気落ちすることもあるでしょう。また、否定的なコメントが来ることもあるかもしれません。人の価値観はそれぞれ違うので、それらに一喜一憂したり、振り回されたりしないようにしましょう。

また、SNSには投稿者に直接ダイレクトメッセージを送れる機能があるものもあります。知らない人からのダイレクトメッセージには注意しましょう。

さらに、多くのSNSでは投稿の公開範囲▶用語集P.181を自由に設定できます。設定範囲によっては友達以外の人が見ることがあるかもしれません。従って、氏名、住所、電話番号、学校や勤務先などの情報をむやみにプロフィールに掲載しないようにしましょう。個人情報▶用語集P.182を悪用されたりする場合やストーカーなどの被害に合うことも考えられます。

自分の投稿を不特定多数の人が見られる設定になっている場合は、自分の顔写真や居場所が特定される場合があるので、投稿には十分注意が必要です。また、知らない人だけでなく、友達の顔写真もむやみに投稿すると個人の特定や肖像権の問題が生じる場合がありますので、慎重に行いましょう。SNS利用に関しては総務省から「安心・安全なインターネット利用ガイド」(https://www.soumu.go.jp/use_the_internet_wisely/)で上手なネットとの付き合い方が示されているので、参考にしましょう。

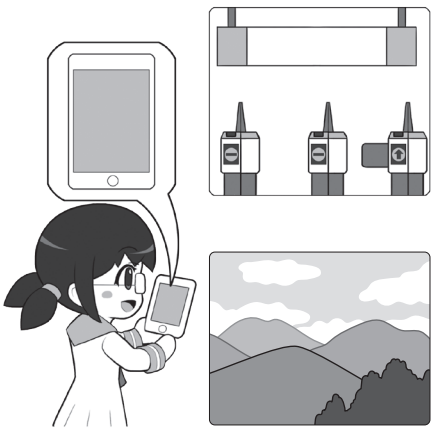
「いいね!」が少なくても気にしない

「いいね!」は、人それぞれの主観です。年齢も学校も大人なら仕事も異なります。多様な価値観があることを理解して、「いいね!」の数を気にしないようにしましょう。

個人情報は基本的に公開しない

一度流出した個人情報は、絶対にネットから消し去ることができませんし、ときに個人の居場所を特定する情報になります。悪意がある人にとって、手がかりになる情報はネットに載せないようにします。

個人が特定される情報はSNSなどに投稿しない



自分自身の写真や、日常的な生活圏がわかる情報を投稿しないようにしましょう。友人のみに公開としていても、その人が共有したら一般に公開されることもあります。また、スマホで「位置情報あり」で撮影していると、見えなくても写真に位置情報が記録されるので注意しましょう。

1.4 モラルを逸脱すると炎上を生む

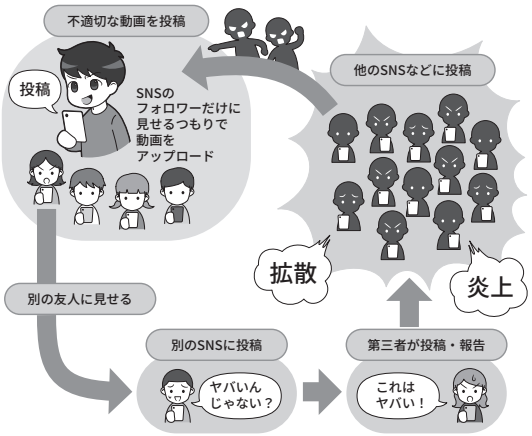
「炎上」▶用語集P.180とは、不適切なSNS投稿が拡散▶用語集P.180され、多数の人から非難を受ける現象を指します。その例には、誹謗中傷の書き込み、プライベート情報の無断投稿、未成年の飲酒投稿などが含まれます。炎上は、世間一般のモラルに反すると判断された場合に発生し、投稿者本人だけでなく、関係する店舗や企業にも多大な影響を与え、店舗の閉店、企業の謝罪、損害賠償請求や名誉毀損での訴訟、解雇や内定取消、さらには悪質な場合には業務妨害などの犯罪として捜査される結果をもたらすこともあります。

炎上を防ぐには、自分の投稿が広く読まれることを意識し、批判を受けない内容かどうかを慎重に考える必要があります。自信がない場合は投稿を控えるのが賢明です。また、ネットでの炎上事例を他人事とせず、自分に置き換えて考えることが重要です。炎上は些細なきっかけで起こり得るため、SNSの拡散力や影響を理解し、その場の勢いなどでの軽率な投稿を避けるべきです。

さらに、「自作自演」や「なりすまし」▶用語集P.185なども状況次第で犯罪や名誉毀損に該当する可能性があるほか、軽い気持ちで行った行為が取り返しのつかない結果を招くことがあります。ネットでの投稿の意味を十分理解し、SNS等の利用を心がけることが大切です。

モラルを逸脱することが炎上を生む

よくある「炎上」の流れ



①発信者が自分のフォロワーなどだけが見るだろうと安易に考え不適切な内容を投稿

②投稿を見たユーザーが問題と感じて元とは違うSNSなどにその内容を投稿

③フォロワーが多いインフルエンサーが該当の投稿を発見して批判的内容を投稿

④インフルエンサーのフォロワーなどがさらに批判的投稿を行い元の不適切な投稿が拡散

⑤マスコミなどに取り上げられることによりさらに拡散

といった流れが考えられます。

③の段階にまで至ると、拡散速度が加速度的に増大し、なかなか沈静化しません。炎上が一旦生じると、発端の問題投稿をした投稿者の個人情報まで特定され、また、元の投稿の拡散も相まって炎上状態が沈静化した後も、ネット上に問題の情報が残り続けます。

1.5 望まない情報流出、流出したら消すことは難しい

個人情報や写真も、スマホなどの中から出さなければ大丈夫ではないかと思われるかもしれませんが、望まない情報流出の罠は、さまざまなところに隠れています。

スマホやパソコンの中に存在しているデータは、写真でもメールでも住所録でも、すべてマルウェアの感染などによって流出する可能性があります。

自分が、セキュリティについて学んでそのような可能性を少なくできても、現状では、サイバー攻撃▶用語集P.182を完璧に防ぐことはできないので油断してはいけません。

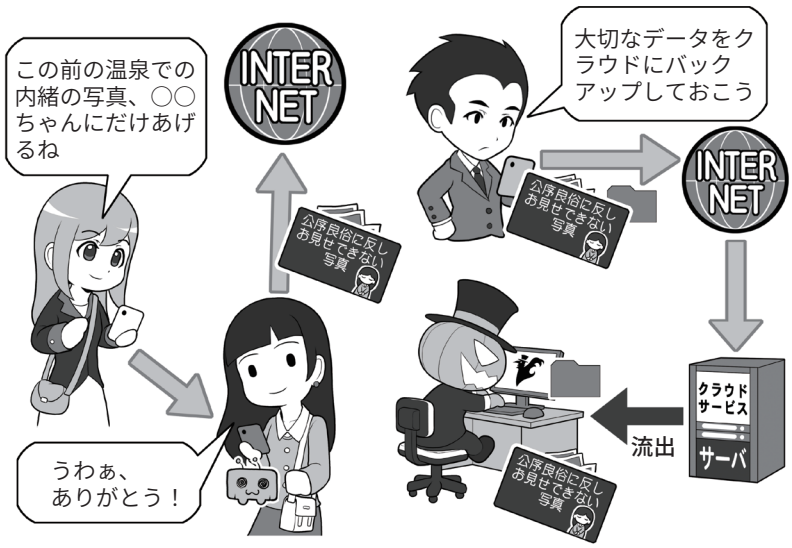
それに、例えば、信頼できる友人であっても、秘密の写真を共有した場合、その友人のスマホなどがマルウェアに感染して流出する可能性もあります。相手が、自分と同じレベルのセキュリティ知識を持ち、実践しているとは限らないですし、また、それを強要もできません。

したがって、流出を確実に阻止したい情報は、ネットワークから切り離して管理し、他人とは共有しないなどの対応が必要です。

さらに、秘密の写真などをクラウドサービスにバックアップ▶用語集P.186のつもりで保管する場合、データが自分の手元と他人の管理下に複数存在するため、流出する可能性のある場所が増えることになります。事実、クラウド▶用語集P.181から有名人の写真が流出する事件も発生しています。

流出したら問題になることは、しない、させない、撮らない、投稿しないようにしましょう。

存在するデータは必ず流出することがあると考える



自分が流出させなくても、渡した相手がマルウェアに感染して流出させてしまうかもしれません。

パスワードの使い回しなどで、クラウドサービスからデータを抜かれて流出してしまうかもしれません。

投稿したデータは一生ついてまわるかも

上記は極端な例ですが、たとえ若気の至りが少年法によって許されて、その後、裁判所などに申し立ててプロバイダに情報の削除の依頼をしても、ネットに拡散した情報のすべてを消し去ることはできず、人生の節目であなたを苛むかもしれません。

まず、問題になることはしないことです。そして、（助長する意味ではなく）ネットに投稿するものはよく考えてから投稿しましょう。

コラム.1 画像情報に含まれるプライバシー情報の管理

普段なにげなく使っているスマホは、10数年前ならば別々の機器だったものが、1つの小さな機器にまとめて収まっています。

例えば、電話、音楽プレイヤー、デジカメ、ビデオカメラ、そして、GPSレシーバーなど。

とくに昔は、GPS衛星からの電波を受信して、緯度経度で構成される位置情報を測るには、大きな専用のGPSレシーバーが必要でした。今はスマホの地図アプリを開いて「現在地」を押せば、即座に自分がいる場所を示してくれます。しかし、便利になった代わりに、意図せず自分の位置情報を公開してしまうこともあります。

例えば、スマホで写真を撮影するときに位置情報を記録する設定にすると、撮影場所情報が「ジオタグ」という形で写真に保存されます。

ジオタグが記録されている写真を、写真アプリなどで見返すと、地図上の撮影したポイントに写真を配置して見ることができ、時系列順に並んだたくさんの写真からわざわざ探さなくても、思い出の場所で撮った写真を即座に見つけることができます。

これは便利ですが、写真にジオタグをつけたままSNSに投稿すると、SNSのサービスによってはジオタグが削除されず位置情報がわかる設定で公開されることもあり得ます。その写真が自宅で撮影したものであると、世界中に自宅の場所が公開されてしまいます。

ジオタグを含め、最近のスマホやデジタルカメラで撮影した画像データには、Exifと呼ばれるデータが併せて保存されています。これにはGPS▶用語集P.176に基づく位置情報のほか、撮影した日時や機種などの情報も含まれています。そのため、Exif情報と合わせて画像データを公開すると、撮影者のプライバシーに関する情報も公開することになってしまいます。

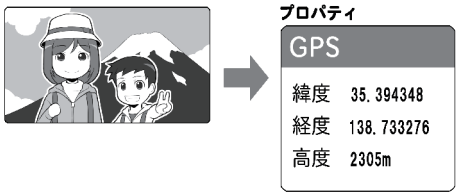
また、普段立ち寄る店の名前を投稿したり、家の周りの風景が映り込んだ写真を投稿するだけで、簡単に撮影場所すなわち生活圏の位置情報に相当する情報を特定される恐れがあります。

Exif情報や「位置情報に相当する情報」は、ストーカーにとっては絶好の手がかりになります。そのため、画像を公開する場合には、プライバシーを守るための対応を行いましょう。スマホでの撮影に際して、「GPSに基づく位置データを保存しない設定」にすることができます。Exif情報は、撮影後に削除することができます。

スマホの場合には、別途アプリ▶用語集P.179を用いることになりますが、これらのアプリを使うことで安全に画像の公開することもできます。また、位置情報に相当する情報については、画像にモザイク加工をするなどして、特定できないようにすることもできます。

画像情報に何が含まれるのかを知り、必要な措置を講じることがネットで公開する際には重要です。

写真には位置情報が含まれることも

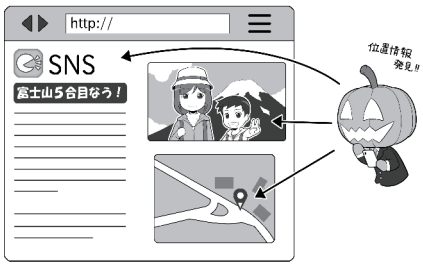


スマホによっては購入時の設定で、写真に位置情報を記録するようになっている場合もあります。必要なければ機能をオフにしましょう。

位置情報は思い出を見返すのに便利

画像アプリによっては地図上に写真が表示され、思い出の場所を拡大すると、そこで撮影した写真を見ることができます。写真を一から探さなくてよいので便利です。

位置情報はストーカーの手がかりになる



写真に付加された位置情報、投稿時の位置情報だけでなく、場所の名前や、場所が特定できる写真からはあなたの居場所が分かります。ストーカーにとっては絶好の手がかりになるので、投稿前に必ずチェックしましょう。

2 インターネットで守るべき法律やマナーを知ろう

2.1 アニメ・マンガ・音楽の違法な共有。パクリなどの著作権侵害

インターネットは、基本的にさまざまなものを共有する場です。しかし、著作権者の許可を得ずに、ネットにアップロードされた、映画、アニメ、テレビ番組、音楽、マンガなどの作品を、そうと知ってダウンロードするのは違法行為です。

また、同様に、上記のような作品を著作権者の許可を得ずにインターネット上にアップロードして配信する行為も違法です。

違法アップロード・ダウンロード▶用語集P.180は作品が生み出される環境を破壊し、結果として新しい作品が生まれなくなります。コンテンツを利用するときは許可を得て公開されているものを利用しましょう。例えば、音楽の場合はエルマーク(https://www.riaj.or.jp/leg/lmark/)、漫画などの書籍はABJマーク(https://aebs.or.jp/ABJ_mark.html)がついているサイトは、適法に許可が得られているサイトです。

ネットでよくいわれる「パクリ」▶用語集P.186も基本的には著作権侵害▶用語集P.184です。

例えば、他人がSNSに投稿した写真や文章を、自分のもののふりをして勝手に投稿することや他人がウェブ▶用語集P.180で発表した小説や写真などの、一部もしくは全部を自分のもののように偽って公開することも著作権侵害であり、SNSによっては利用規約違反としてアカウントを停止される場合もあります。

違法アップロード、ダウンロードは刑罰の対象にも……

＊1：有料の作品が違法にアップロードされているものと知っていた場合

他人の投稿や作品を盗む「パクリ」

パクリで一瞬だけ注目を集めても、いずれ身元が特定されるなどして「パクった人だ」とネットに記録されてしまったらいやですよね。ちなみに、自分のもののように偽らなくても、勝手に転載したら著作権侵害です。

2.2 クラッキングは犯罪になる可能性が高い行為！

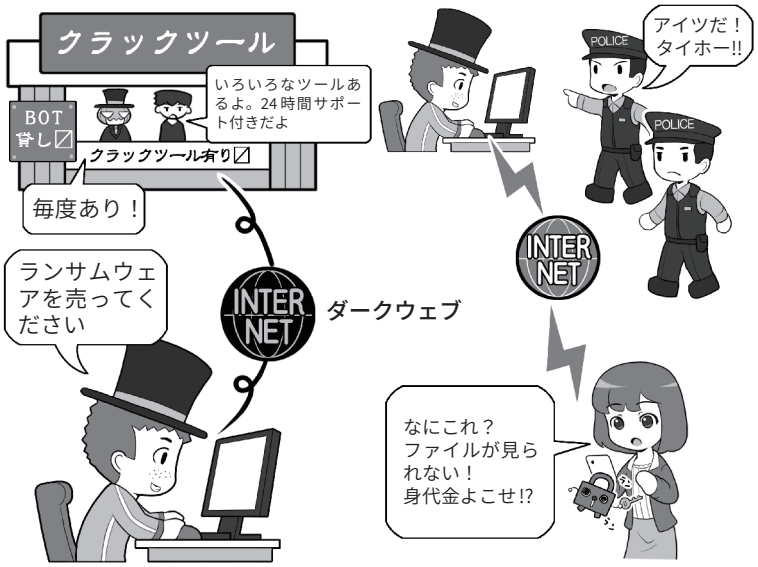
インターネット上には、「ダークウェブ」▶用語集P.184という通常であればアクセスすることがないようなサイトがあります。そこでは、アングラなありとあらゆるものを売るマーケットが存在し、悪意のハッカー▶用語集P.179によるクラッキング▶用語集P.181用ツールの販売や、DDoS攻撃▶用語集P.176のためのゾンビ化した機器群貸出しなどがされたりしています。

近年、若いこどもたちがここに足を踏み入れ「インターネットは匿名だからばれないだろう」とツールを入手して、ランサムウェア▶用語集P.189によるサイバー攻撃や不正送金▶用語集P.187などを行った事例が報告されており、行為者が逮捕された例もあります。そのようなサイトで入手したツールなどを使う行為の多くは、不正アクセス▶用語集P.187禁止法違反、ウィルス作成罪、業務妨害罪などの刑法犯に該当する行為です。でもばれないと思ってやってしまうのでしょう。

果たして、それは本当にばれないのでしょうか。インターネットは、当初悪意が存在することが想定されていない空間でした。しかし、そこに悪意が芽生え、犯罪に利用されるようになった結果、各国の捜査機関も日々こういった犯罪に対応する技術力を向上させています。事件と報道されるのは、日本でも警察等の捜査機関がインターネット上のパトロールをし地道な解析などで犯人を追い詰め特定しているからです。匿名だからばれないということはないのですね。

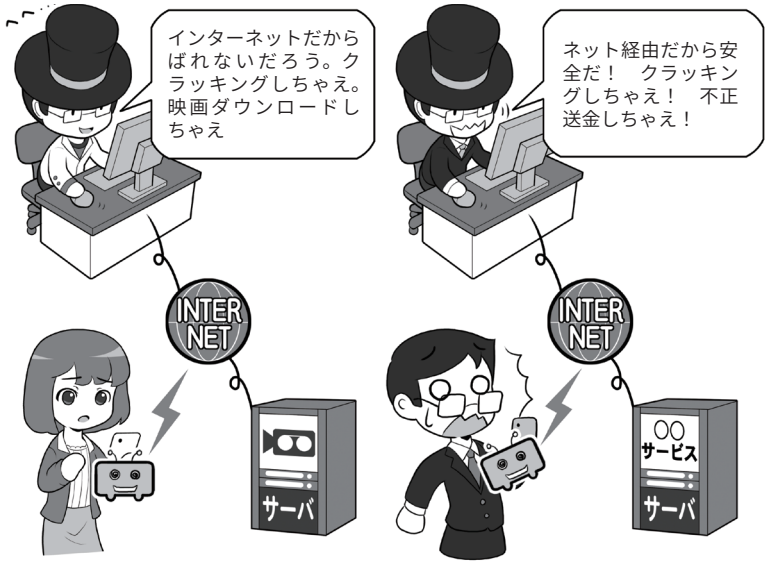
「有名になりたかった」、「腕試しをしたかった」、「小遣い稼ぎで」そういう言い訳をしても、その行為は単なる犯罪です。有名になったところで、その悪名がネットに刻まれるだけで誰も尊敬はしてくれません。実名が流出してその後の人生にずっと影響し続けることだってあるのです。

クラッキングツールに手を出さない



現実世界でもネットでも、広く知られている「安全でない場所」や「怪しい場所」は、当然のことながら捜査する側もよく調べ、必要ならば対策を講じています。「匿名性が高い」はずなのに「捕まったこと」が記事になるということは、なにを意味するでしょう？ネットでも危険場所には近づかないようにしましょう。

インターネットだからばれないと思うのは……



本人は軽い気持ちで始めているつもりでも、クラッキングはさまざまな法律や利用規約に違反します。そして、見つからないと思っていても、現実世界に生きる私たちは、現実世界に生きている痕跡を完璧に消すことはできません。

2.3 災害時のSNSでの情報発信

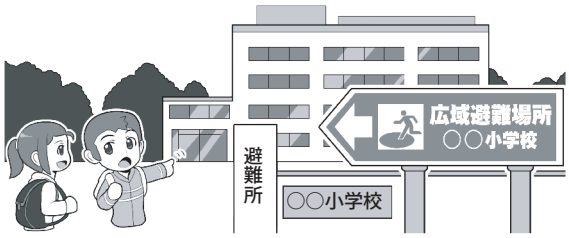
最近では各種の自然災害やテロなどが発生すると、その状況をネットにアップする人がいます。しかし、なんらかの災害・テロの発生や避難勧告が発表されたら、写真を撮ったりSNSに投稿したりせず、速やかに安全な場所に避難しましょう。海や川の近くでの大地震ならば、急いでできるだけ高い場所に避難しましょう。

災害時に現場で写真を撮ったり、実況放送のようにレポートすることは、あなたの仕事ではありません。無事家族や同僚の元に帰ることが使命です。それを最優先に考えて、まずは命を守る行動をしましょう。

さらに、実際には生じていない事象（災害に乗じた犯罪や事故の発生など）や、まったく関係がない被害画像などを、あたかも災害の被害状況のように投稿するケースも見られます。これらは、第２章３（P.60）にも示す偽情報などに当たるものですが、発信内容によっては業務妨害などに該当する可能性があります。また、災害時のSNSによる情報発信は援助要請など緊急性を要するものもありますが、軽率に情報を拡散するとかえって混乱を招くことにもつながります。十分留意して行いましょう。

命を脅かすものから速やかに逃げる

安否の連絡や情報収集は安全な場所に着いてから



自然災害時は避難勧告が出る前でも、自主的な避難が命を守る行動になります。まずは身の安全を確保し、その後、安否の連絡や情報確認を行いましょう。

そして安否連絡や安否確認サービスに登録

安否確認の方法は、複数の候補を事前に家族や同僚などで決めておいて、それらを利用するようにしましょう。災害時には、スマホを含む一般の電話は通話がつながりにくくなります。電話連絡をする場合は、公衆電話か避難所に設けられる災害時用の電話を利用しましょう。なお、インターネットが使えなくなった場合の避難手順や安否確認方法も検討しておきましょう。

コラム.2 デマに踊らされない！

昔から、事件・事故のときに拡散したり、都市伝説のように長く語り継がれたり、出所が不確かなデマはありました。人から人への口伝えで拡がるので、自分が聞いた話を再度確かめようと思っても、すべて遡って大本の発言者までたどるのは至難の業でした。

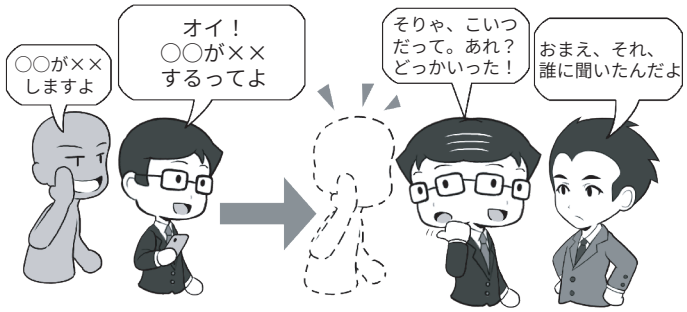
インターネットが普及した現代では、デマは「距離とその移動に必要だった時間が消えた世界」で、恐ろしいスピードで拡散します。しかも、SNSなどの場合「何人の人がその情報を共有したか」ということが数字でついて回るので、それが何万人にもなると、デマであっても妙な信憑性があります。

また、一見正確のように思えるネット上のニュース記事も、情報操作を目的としたフェイクニュース▶用語集P.187である場合もあります。他の情報と比較してみる、発信元を調べてみることも大切です。

また、これらネット上のデマなどはマルウェアへの感染誘導や、フィッシング詐欺を狙った可能性があります。場合によっては、誰かを傷つけ名誉毀損となるものかもしれません。

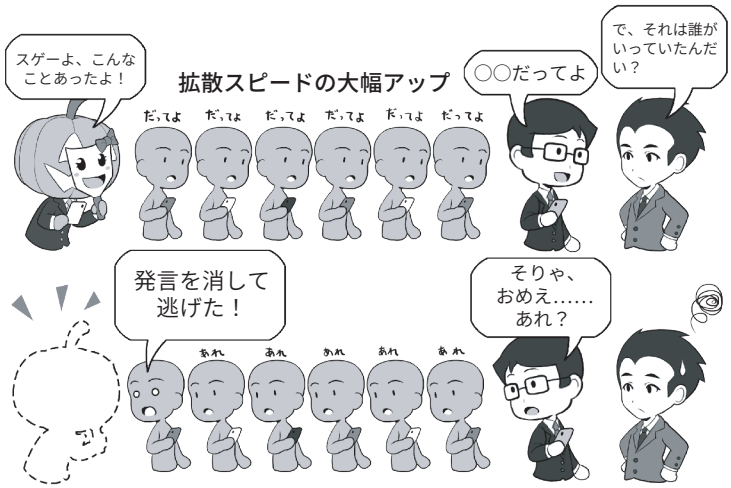
第2章3（P.60）で述べたように、これらは偽・誤情報の一種であり、慎重に確認して対応することが求められます。したがって情報が勢いをつけて手元に飛び込んできても、その勢いに飲まれて拡散に加担せずに、情報の信憑性を確認する余裕を持ちましょう。さらに、災害時には現場の混乱などから本業の人でも間違った発信をしてしまうことも考えられますので、焦らず情報の正確性を確認しましょう。

昔から出所が不確かなデマはあった



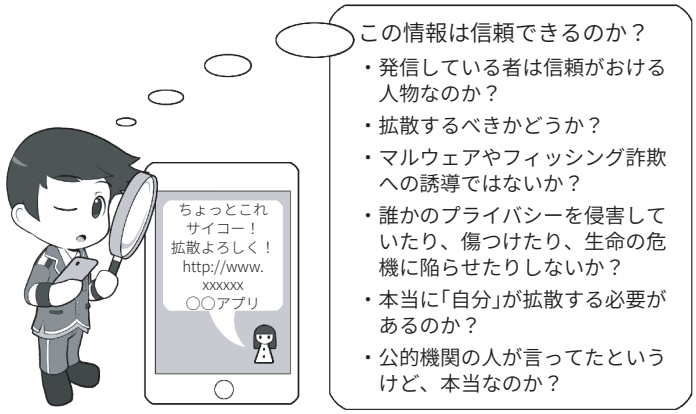
かつてのデマは、人間がしゃべるスピードでしか拡散しませんでしたが……。

ネットではデマが加速して飛び込んでくる



現在は、ネットの特性で「拡散数」を伴ってデマが加速して飛び込んできます。しかし、その数を真実かどうかの尺度にしてはいけません。元ネタが嘘だったり、意図的に流布してから消して逃げたりすることもあるからです。

情報はよく吟味することが必要



参考情報：総務省
「上手にネットと付き合おう！～安心・安全なインターネット利用ガイド～」https://www.soumu.go.jp/use_the_internet_wisely/
「インターネットトラブル事例集」https://www.soumu.go.jp/use_the_internet_wisely/trouble/

コラム.3 法律に違反することをしてはいけません。気軽に考えてはダメ

サイバー犯罪というと、それなりの年齢の悪意のハッカーを想像するかもしれませんが、実は非常に幼いこどもたちが行い、その結果、児童相談所に通告されたり、書類送検されたりしている例もあります。

例えばほんの出来心で、他人がロック▶用語集P.189している情報を、何らかの形で知ったログイン情報を元にのぞく行為も、不正アクセス禁止法違反となる可能性があります。さらにチート行為▶用語集P.184も、規約違反に該当しますし、不正アクセスに当たる場合によっては犯罪として摘発されます。

コンピュータやスマホを使う際には、見てはいけないウェブサイト▶用語集P.180、危険なサイトへのアクセスを防ぐフィルタリングを利用するだけでなく、どういうことをしてはいけないのか、そういう行為は法律に違反する場合もあることを家族で話し合っておきましょう。下記の例などを参考に、これが他人ごとではなく身近に起こる可能性があることとして、家族で話し合ってみてください。

■アカウント乗っ取り

小学4年生の女子児童が、会員制の交流サイトでサービス上の通貨の提供を条件に、別の女子中学生のIDとパスワード▶用語集P.186を聞き出し、本人になりすましてログイン▶用語集P.189し、その女子中学生のアカウントを乗っ取ったとして不正アクセス禁止法違反の容疑で補導され、児童相談所に通告された例があります。

■ウイルス保管と提供

動画サイトなどに掲載されていた動画を参考にコンピュータウイルスを作成、これを保管、提供したなどの理由で、小学3年生の男子児童が不正指令電磁的記録提供などの非行内容で児童相談所に通告されています。また、これをダウンロードした他の小学生も不正指令電磁的記録取得の非行で児童相談所に通告されています。友だちを驚かせたいという軽い気持ちだったようです。

■高校生が少女の裸の画像を拡散

高校生が同級生の少女に裸の画像や動画を撮影させ、これをSNSに投稿することを強要し、そののち拡散した例で、関与した男女の生徒は、児童買春・児童ポルノ禁止法違反(製造、提供など)の疑いで書類送検されています。

他人のアカウントへの不正なログインや乗っ取りをした場合

不正アクセス禁止法
不正アクセス行為の禁止

第3条、第11条
→3年以下の懲役または
100万円以下の罰金

コンピュータウイルスの作成や保管をした場合

刑法
不正指令電磁的記録作成等

(作成、提供、供用)
第第168条の2
→3年以下の懲役または
50万円以下の罰金

(取得、保管)
第168条の3
→2年以下の懲役または
30万円以下の罰金

児童ポルノの所持・提供をした場合

児童買春、児童ポルノ禁止法
児童ポルノ所持、提供等

(所持)
第7条第1項
→1年以下の懲役または
100万円以下の罰金

(特定少数者への提供)
第7条第2項
→3年以下の懲役または
300万円以下の罰金

3 便利なサービスや機能を利用して家族を守ろう

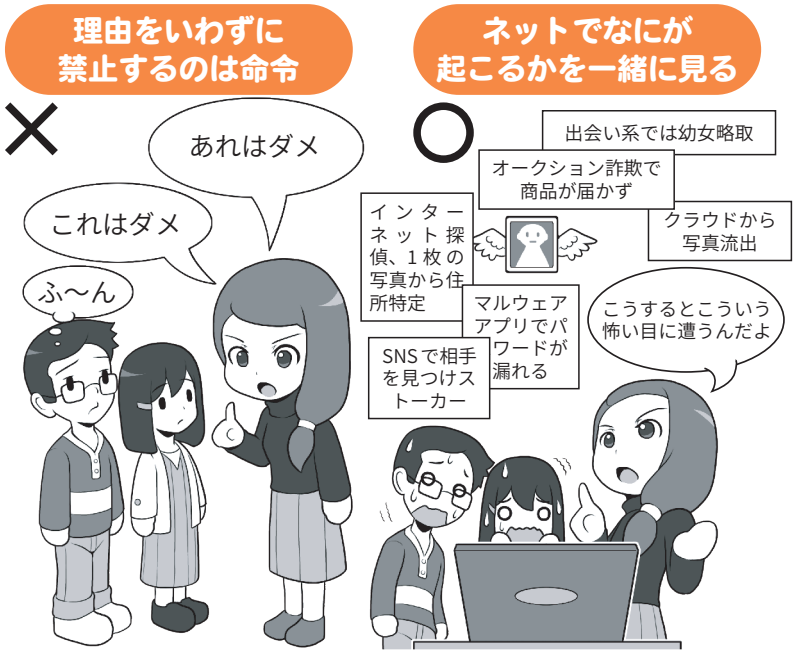
3.1 こどもを守る

こどもをインターネット関連の犯罪から守るには、理由を述べずにあれもダメこれもダメと頭ごなしに禁止せず、まず可能な限りどういった犯罪がどのように行われるのかを知らせましょう。

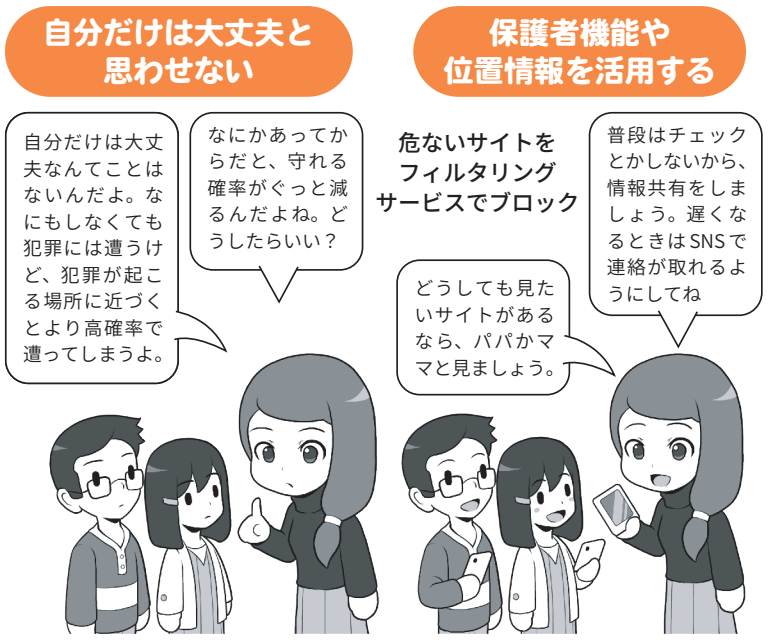
こどもたちが犯罪に当たる行為をするとき、本人たちはそれが「犯罪になると思っていなかった」という例もあります。知ることが抑止することにもつながります。

サイバー犯罪に遭うという視点からも、問題点や危険性、また、それによってどれぐらいの範囲にトラブルが広がるのか、きちんと共有することが必要でしょう。

本当は怖いインターネット



頭ごなしに禁止せず、インターネット関連のトラブルの実例を見ながら、なぜダメなのかを「理解」しあって共通の認識を作ります。こどもだけでは、対処できないトラブルがあることを知ることが重要です。



意識を共有したら、実例を示してこどもたちに答えを出してもらいましょう。自分で出した答えは自らのルールとなるからです。

3.2 こどもに対する情報モラル教育の重要性

SNSやネット上のリスクは、学校に通う児童・生徒に対しては、昨今のGIGAスクール構想による情報モラル教育▶用語集P.182の効果もあり、一定程度は理解が進んでいると思われます。

GIGAスクール構想を推進した文部科学省が告示している小〜中〜高校の学習指導要領によると、「情報モラル」は学習の基盤となる資質・能力の1つである「情報活用能力」にも含まれると定め、SNSやネット上のリスクについての理解などを含め、情報モラル教育の重要性が示されています。

一方で、児童・生徒の保護者には、情報モラル教育の重要性やその教育が求められる背景として存在するSNSやネット上のリスクを十分に理解できていない人も少なくないでしょう。こどもと保護者とのサイバーセキュリティに関する知識格差を埋めるためにも、保護者もSNSやネットのリスクは知っておきましょう。

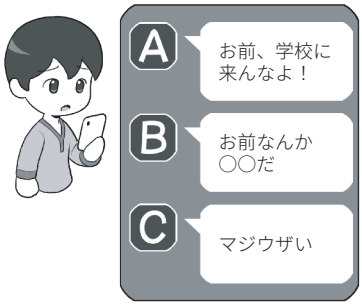
また、ネットの普及により、いじめはSNS上などで表面化しにくく巧妙化しました。悪口の書き込みやSNSグループからの排除といった形で行われ、大人からも発見しにくい場合があります。お子さんがネットいじめに遭った場合は、教師に相談し、画面ショットなどの証拠を保存することが重要です。

GIGAスクール構想により、児童・生徒1人一台の端末が配布され、ICT教育が進む一方で、これらの端末がネットいじめの手段になる可能性もあります。SNSでの誹謗中傷やパスワード流出によるトラブルを防ぐため、アカウントの適切な管理が必要です。このような環境下では、環境整備の本来の目的を踏まえつつ、ネットリテラシー教育の強化と、いじめ防止の仕組みを整えることが求められます。

いじめは閉鎖された場所で起きやすい

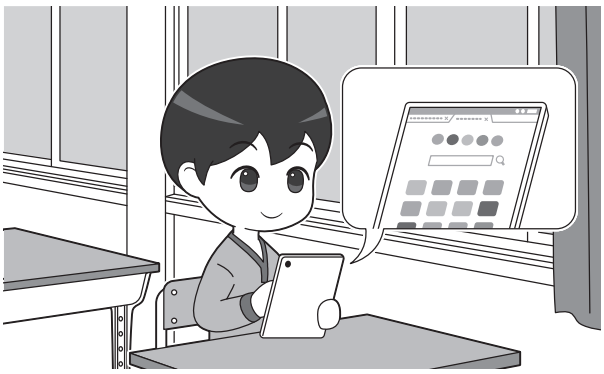
公共の空間では人の目がある

ネットは他人から見えにくい



人の目は、ときに抑止力になりますが、ネットの中は人目が少なく、その分いじめは陰湿でエスカレートしがちです。

GIGAスクールでICT教育環境が充実!!



コロナショックも影響し、2020年から急速に推進されたGIGAスクール構想により、全国の小中学校では児童・生徒1人1台の端末普及が実現しました。

GIGAスクールの端末は、学校のルールを守り、学習など正しい目的で使う

残念ながら、配布された端末を用いてSNSで他人への悪口を書き込むネットいじめが問題になりました。同じパスワードの使い回しにより、勝手に友達のアカウントになりすまし、誰が悪口を書いたかわからない事態になるなど、いじめの早期発見が難しくなってエスカレートする可能性があります。

3.3 こどもにスマホを持たせるとき「スマホ契約書」の提案

こどもがスマホを欲しがる際、利用に関する家庭内ルールを明確に定めることが、トラブル防止に重要です。総務省が実施した「我が国における青少年のインターネット利用に係るペアレンタルコントロールの効果的な啓発に関する調査結果」では、家庭内ルールと保護手段を併用することでトラブルのリスクを軽減できることが示されています。また、こども家庭庁が実施している「青少年のインターネット利用環境実態調査」からは、親とこどもでルールの認識が食い違うケースが多いことが分かり、ルールを確認し合い事前に取り決めておく必要性が浮き彫りになっています。

家庭内ルールを「契約書」という形で明文化することで、親子双方が約束を強く意識できるようになります。契約書はこどもに「一人前」として認められている感覚を与え、ルールを守る意識を高める効果もあります。具体的なルールとしては、「食事中にスマホを見ない」、「夜10時以降は使わない」など家庭ごとの方針のほか、「SNSでは誰に読まれても問題ない内容だけを投稿する」、「恥ずかしい写真を送らない」、「知らない人から、実際に会いたいなどの誘いが来た場合は親に相談する」など、ネットトラブルを防ぐための内容を含めると良いでしょう。

契約書作成の際には、親子で十分に話し合い、こどもが実行可能な具体的なルールを設定することが大切です。また、ルールを破った際の対応策も取り決めておく必要があります。さらに、一度作成した契約書は、こどもの成長や環境の変化に応じて定期的に見直し、更新することが重要です。

家庭内ルール作りの参考として、文部科学省が提供する「話し合っていますか？家庭のルール」教材が役立ちます。このように、ルールの明文化と更新を通じて、親子の信頼関係を深めながら、スマホ利用における健全な習慣を築いていくことが求められます。

口約束は忘れてしまいやすい？

ルールは決めても、口約束だけで見返せないと、あやふやになってしまいがちです。結果的に感情的なやりとりを生みます。

契約書を作り、責任ある人として接する

契約書は固いイメージもありますが、ルールをときどき見返すことができる他、言った言わないにならないというメリットもあります。

なにより相手を責任ある人間としてあつかうことで、ルールを自ら決めたことの自覚と守ることへの自律を促しましょう。

3.4 こどもを守るためのサービス

スマホには、こどもに有害と思われるサイトを閲覧できないようにするフィルタリング機能や、アプリの使用も含めて、こどものスマホ自体を管理するペアレンタルコントロールの機能があります。これらの機能を契約書の内容と合わせて、こどもの年齢に応じて適切に使うことで、こどもに対するスマホやネットの安全性をより高めることができます。

そのため、セキュリティソフト▶用語集P.183やフィルタリングサービス▶用語集P.187、緊急時のための位置情報共有の必要性を一緒に確認しましょう。

いざというとき、こどもを助けに行くためには、位置情報は非常に有効な手段です。一方、こどもたちは過度に位置情報に関することを追求されると、共有を切ってしまうかもしれません。こどもでもセキュリティの設定などはすぐに変更してしまうでしょう。こどもに対しては、セキュリティの必要性をわかりやすく説明しましょう。とくに位置情報の共有は監視のために使わないことを約束し、そして、約束を守りましょう。

また、こどもからルールの変更やどうしても見たいウェブサイトなどを言い出しやすい雰囲気を作り、それについて一緒に話し合って勉強する姿勢を示しましょう。スマホやIT機器は絆を断絶するためのツールではなく、より太く結ぶためのツールなのです。

スマホが使えないほど幼いこどもたちを守るサービスや機器も、いろいろと登場しています。

学校を離れたときや駅を通過したときに、親のスマホにメールが送信される見守りメールサービスや、メッセンジャーアプリ▶用語集P.189、簡単な

安全を守るさまざまな方法

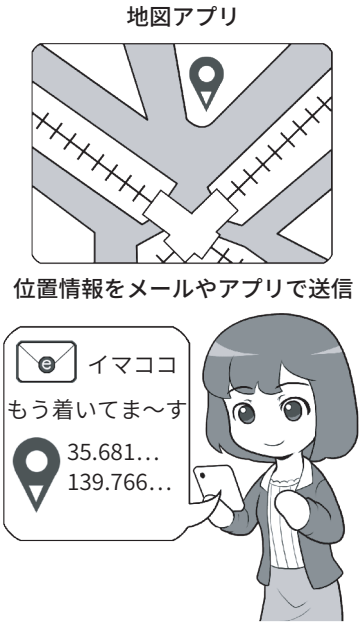
見守りメール

見守りメールは、鉄道会社や一部の学校などが提供しているものがあるので、自分が住んでいるエリアでサービスが行われているかを調べてみるとよいでしょう。

GPS付きキッズケータイ

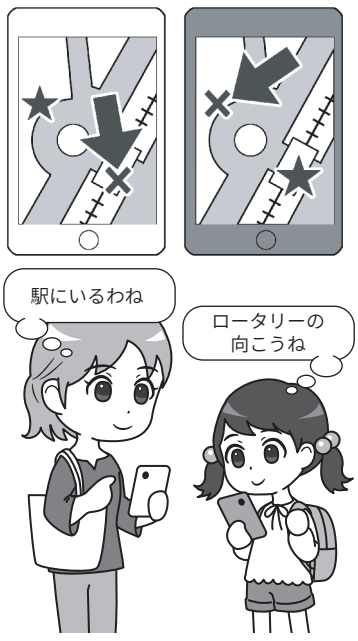
連れ去りや変質者に遭遇したときに使用する、防犯ブザーと簡単な通話機能が一体になったスマホです。簡単な操作で登録された特定の人物への通話なども可能です。

位置情報の送信



地図アプリの位置情報共有機能を利用して、メールやメッセンジャーアプリから現在地を簡単に相手へ送信できます。受信した相手も自分のスマホの地図アプリを起動すれば位置を確認できます。

位置情報共有アプリ



位置情報共有アプリは位置情報を相手へ送信する手間を省いて共有でき便利ですが、不用意に必要以上の人と位置情報の共有をしないことが重要です。

通話機能とGPSと防犯ブザーが合体したキッズケータイは、シンプルな操作方法を理解したら、いざというときの強い味方になります。

また、ある程度スマホの操作ができる年齢になったら、位置情報を送信したり、必要な情報をメールやSNSを通じて共有する方法を、一緒に覚えるのもよいでしょう。

位置情報共有アプリ▶用語集P.180は便利ですが、悪用されストーカーなどの被害に遭う可能性もあり、刺傷事件に至ったケースもあります。位置情報を共有するのは、こどもが幼いうちは親のみにしておくようにするとよいでしょう。また、ある程度の年齢になっても不用意に必要以上の人と位置情報の共有をしないことが重要です。

なお、現在は建物の中で迷子になると位置情報や何階にいるかなどの情報は共有できませんが、今後地下街や建物内などにビーコン(Beacon)と呼ばれる装置が普及することで、屋内でも位置情報の交換が可能となると考えられます。

また、どこかではぐれても、電車やバスの乗り換え案内や徒歩ナビゲーションなどのアプリを利用して、家に帰り着く方法をこどもと一緒に学びましょう。

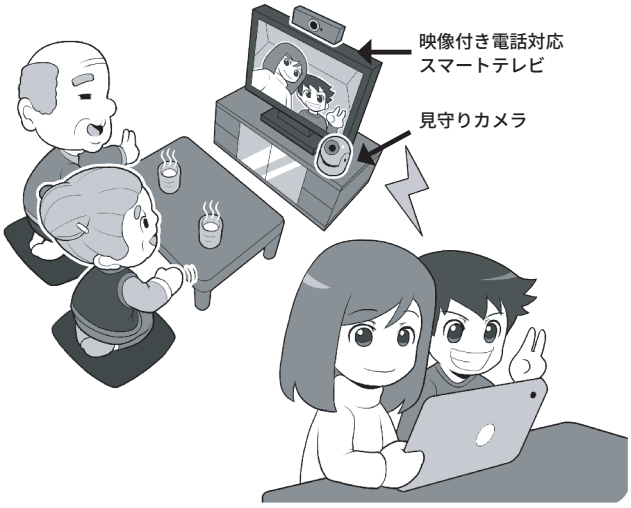
3.5 お年寄りを守る

お年寄りも、最近ではパソコンやスマホなどを使う方が増えています。ただ、これまでに馴染みがなかったことから、操作に不慣れだったり、インターネットの危険性等にうとい方もいます。特にソーシャルエンジニアリング▶用語集P.184(イントロダクション6(P.22)参照)を用いた詐欺は、「振り込め詐欺」のようにネット以外の方法でも被害が増大しています。

振り込め詐欺は電話で顔がみえない状況で、相手を不安に陥れ、さらに即断が必要な状況に追い込むなど、被害者に正常な判断を行わせなくするように仕向けています。これに対抗するために、例えば、ご両親に連絡するときは、通話アプリのTV電話機能を使うと決めておけば、顔が見えない状況で丸め込まれ、騙されることを回避できるかもしれません。

高齢者の方がスマホなどを使い始める際に、操作などを会得するのを支援するため、国では「デジタル活用支援推進事業」(https://www.digi-katsu.go.jp/)を行っており、高齢者等が身近な場所で身近な人からデジタル活用について学べる講習会を設けたり、役立つ学習資料等を提供したりしています。また、いざ操作を勉強する段になって教えてあげやす

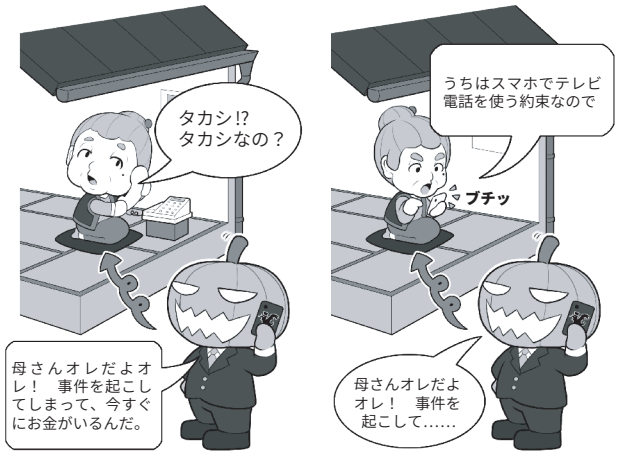
映像付き電話やITサービスの活用



お年寄りにとってこどもや孫たちの顔を見るのは、なによりの楽しみでしょう。会いに行ってあげるのが一番ではありますが、なかなか訪ねて行けないときは、顔を見てコミュニケーションを取れるツールを活用しましょう。

また、1人暮らしのお年寄りに万が一のことがあったときのために、日々生活状況を確かめられるサービスも存在しますので、利用を検討してもよいでしょう。

IT機器を使った振り込め詐欺対策



電子機器の操作に不慣れなお年寄りでも、スマホの電話機能ならよく使うでしょう。こどもや孫から連絡を取るときは必ずテレビ電話を用いるという方法を使えば、顔が見えない状況で不安に陥れる「振り込め詐欺」などの予防にもなります。同じスマホを渡してあげれば、操作を教えることも簡単です。

いように、自分が持っているものと同じ機種を渡しておくのも1つの考え方です。

ご両親の海外旅行時に、きちんと目的地に着けているか、迷ったりしていないか心配な場合は、事前に相談して位置情報共有サービスや移動履歴が残るサービスを設定して旅に出てもらいましょう。

こうすることで、今どこにいるかを確認できるので、予定どおりに旅行しているかもチェックできます。また、仮に旅先で迷子になってしまっても現在地がすぐわかれば、どのようにしたらよいかのアドバイスも的確にできるでしょう。

そのようなことはあまりあってほしくありませんが、もしスマホを紛失したり盗まれたりした場合も、操作するための情報を共有しておけば、スマホをロック▶用語集 P.189 したり所在地を確認したりできます。

認知症を患っているお年寄りは、家族の見ていないときに外で徘徊し、事故に遭ってしまうことがあります。

また、一緒に外出した後で目を離した隙にいなくなってしまい、本人も自分がどこにいるのかわからず、その結果、行方不明になってしまうケースもあります。

そういった場合に備えて、GPS発信器を使った位置情報サービスを契約したり設定したりしておくと、間をおかず探し出すことができます。

もちろん目を離さないことが重要なのですが、ご自身にリカバリ▶用語集 P.189 する能力がない状況では、万が一に備えた方が安心でしょう。

持ち慣れない機器を持つことを嫌がるお年寄りの方も少なくないので、機器を携帯してもらうの際に工夫は必要ですが、事故などを未然に防げる可能性が少しでも高くなるならば、検討してみるとよいでしょう。

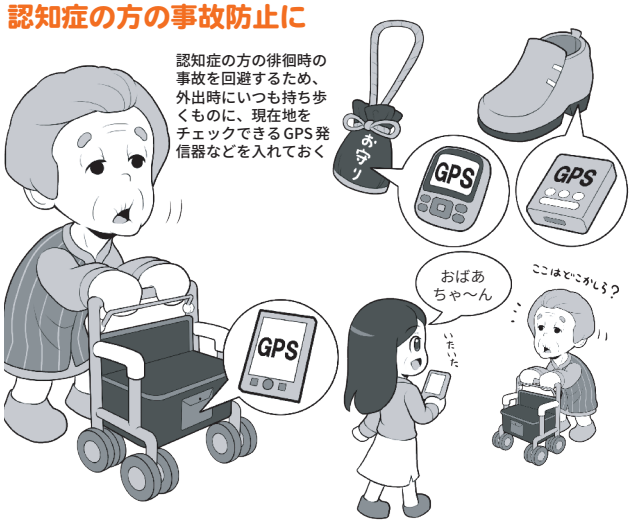
最後に例えばその方が亡くなると、資産や負債を含めて、どういったものが残されたのかわからない場合もあります。残された人が困らないように、万が一のときに備えて管理情報のありかを残したり、PIN コード▶用語集 P.177 をノートや遺言書に残したりするなど、残った家族が分かるようにしてもらいましょう。

位置情報の共有（安否確認）

スマホの位置情報の共有設定をし、現地でもインターネット接続サービスを利用できるようにしておくと、世界中どこにいても現在地を確認することができます。年輩の方自身が位置情報を使いこなせなくても、電話やSNSのメッセージ機能などを使ってサポートすることができます。

※現地でデータ通信できるように、データローミングの利用や海外用のSIMを手配する場合は、渡航前に準備や設定を済ませておきましょう。また、現地に着いたときに確認するべき事項を紙などに書いて、事前に説明しておきましょう。海外で購入したSIMの使用は最初の設定をしないと、インターネット接続もできない場合がありますので注意が必要です。

認知症の方の事故防止に



普段押して歩くカートや、お守りに入れて持たせたり、物を持ちたがらないお年寄りには、靴の中に入れられる機器も存在するのでそのようなものを利用したりします。しかし、これらはなにかあったときのバックアップの手段で、普段から目を離さないことがなにより大切です。