第5章

SNSやインターネット関連の犯罪やトラブルから、自分や家族を守ろう。災害に備えよう

SNSやインターネットを使う上で、どんなふうにしたら自分や家族を守れるの？
具体的にどんなことが起こり、そのときどのようにしたら自分や家族を守ることができるのか、
一緒に考えてみましょう。
海外での利用の注意点や、災害時に情報を生かしてどうやって身を守るかを知りましょう。

1 SNSやネットとのつきあい方、守り方

1 SNSやネットの楽しみと気をつけること

私たちは、インターネットの普及により、「距離とその移動に必要だった時間が消えた世界」を手に入れることができました。

昔は、遠い国の人と連絡を取り合うには、手紙を書いて何週間も返事を待ったり、電話をかけるにしても料金が高く気軽にかけられなかったり、あるいは顔を見るために旅行するにしても、大変な手間とお金がかかったものです。

しかし今では、まるで隣に座っているかのようにチャットしたり、SNSで写真を送りあったり、映像つ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。

そして、IT技術の進歩は言葉の壁すらも崩しつつあります。まるで世界が一つになったような時代が訪れ、人の意識そのものが変わっていくかもしれません。

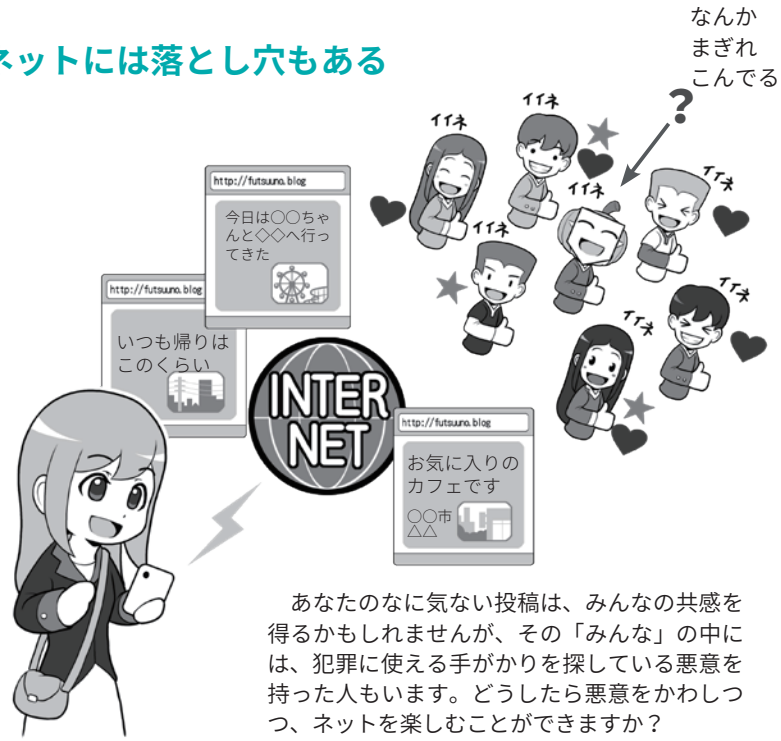
一方、あなたが世界中の人にメッセージを発信するとき、それを受け取る人々の中には悪意を持った人がいることも忘れてはなりません。ネットを使ったコミュニケーションは人と人の意識のつながり合いを容易にしますが、同時に自分の意識の壁の中に、そういった悪意をもった人間がするりと入ってきやすくなるのです。

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、新しいつきあい方」を作り上げなければならないでしょう。悪意のあるものを鋭く見分けて、善意のコミュニケーションの世界を作っていくことができるように。

ネットやSNSによるコミュニケーション

ネットやSNSで、距離を超えて世界とつながることができます。そして、時間を越えて様々なことを知ることもできるのです。

ネットには落とし穴もある



あなたのなに気ない投稿は、みんなの共感を得るかもしれませんが、その「みんな」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、ネットを楽しむことができますか？

2 SNSやネットの怖さ、こんなことが実際に起こっている

では、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の人でした。「○○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。こんな風に誘拐や略取が行われます。

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。

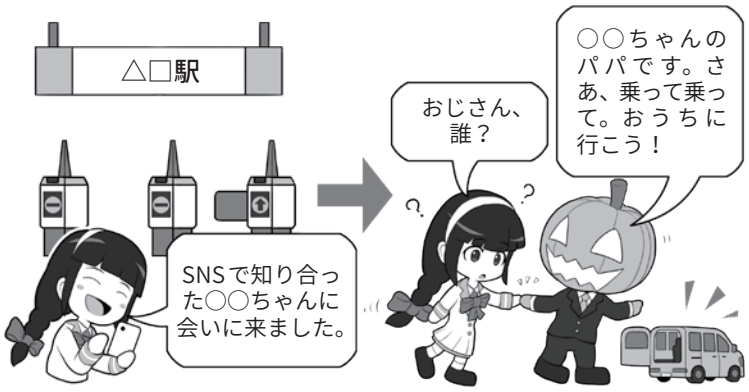
闇サイトなどを興味本位に覗いたりしていると、犯罪勧誘といって、顔も知らない人があなたを犯罪に誘ってくることもあります。

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。

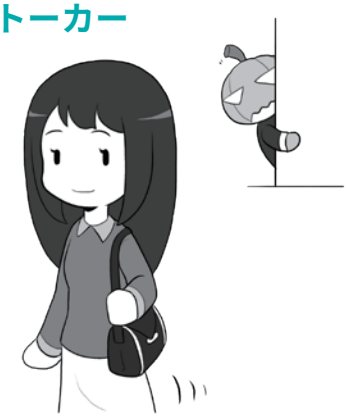
交際している相手が、「誰にも渡さないから」とあなたの裸の写真を要求してきて、信頼して渡したら、別れた後にその画像がネットに流出してしまうかも。それは、「リベンジポルノ」といって、相手が嫌がらせのために、写真をネットに投稿する行為ですが、その意図がなくても、相手のスマホがマルウェアに感染して流出してしまうかもしれません。その写真は、消えない「デジタルタトゥー」(デジタルの入れ墨)として、以降あなたの人生に、ずっと影を落とし続けることになるかもしれません。

このほかにも、SNSやネットでは、様々なトラブルが発生することがあります。トラブルのことをよく知って、決して巻き込まれないようにしましょう。

誘拐や略取



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。

3 SNSやネットとのつきあい方の基本

自分からネットの怪しげな場所に近づかないなら、あとは日常的に注意しなければならないのは、システムなどを最新の状態に保ちサイバー攻撃を受けないようにすることと、SNSやネットで悪意がある人に個人情報や画像が渡り、あなた自身が狙われたり、攻撃の対象にならないよう、投稿する内容には気をつけることです。

例えば、SNSを利用する場合、個人情報はサービスの規約などで必須のもの以上は記入しないようにしましょう。その上で、投稿の公開範囲の設定は、友だち限定にしましょう。そのほか個人情報を守る仕組みが提供されている場合は、それらを有効活用しましょう。

実際に会ったことがない人が、突然お友だちになりたいといってきても、即座にOKせず家族などに相談しましょう。誰かの友だちなら、実際に会ったときの印象や、どういった人かを教えてもらい検討の材料にしましょう。また、その人の過去の発言などを良く見て、二面性などを含め判断しましょう。

そして、一度も会ったことがないのに、本名や連絡先をたずねたり、いきなり実際に会おうなどと誘ってきたりしたときは、基本的にお断りしましょう。文化活動や物の売買など、なんらかのきちんとした理由で会う必要があるときは、大人や保護者同伴で行き、その際でも本名や住所などは極力教えないようにしましょう。

SNSやネットへ投稿をする場合は、普段の立ち回り先や生活のパターンの情報などは避けるようにしましょう。些細なことですが、一枚の写真に写っている背景だけで、自宅を特定される場合もあるので注意しましょう。

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。

会ったことがない人とむやみに友だちにならない

会ったことない人が友だちになろうと近づいてくるときは、その中に悪意をもったものがいることを知りましょう。基本的には友だちにならず、必要ならよく吟味したり、相手について調べたりしてから判断しましょう。

現実世界で会おうとする人を警戒する。出会い系に近づかない

実際に会ったことがない人は、プロフィールの年齢や性別が本当なのかわかりませんし、これを偽って近づいてきた人と会い、被害に遭った例もあります。また、よく事件が起こる出会い系サイトなどには、絶対に近づかないようにしましょう。

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、デジカメで「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。

4 存在するデータは流出することがある。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じゃ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、様々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ういった可能性を少なくできても、現状では、サイバー攻撃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、信頼できる友人に秘密の写真をシェアしたあと、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。

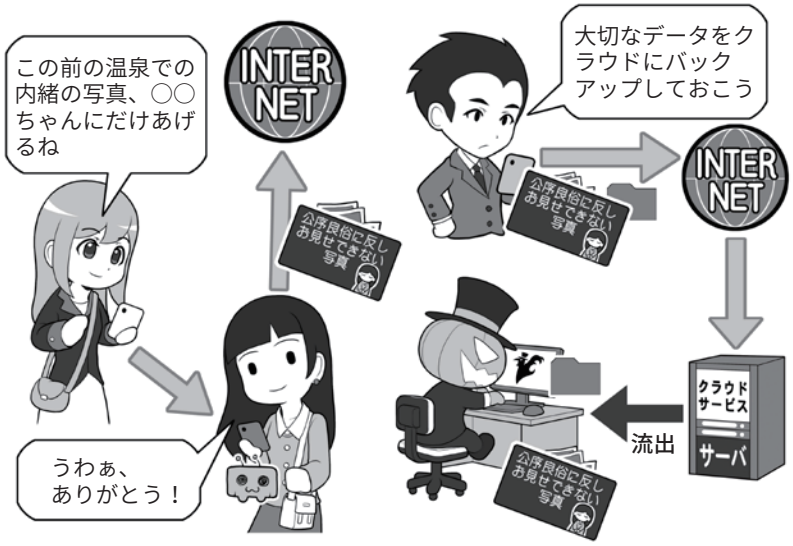
相手が、自分と同じレベルのセキュリティ知識を持ち、実践しているとは限らないですし、また、それを強要もできません。

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した場合、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、少なくとも2カ所から流出する可能性が存在するようになります。事実、クラウドからセレブの写真が流出する事件も発生しています。

問題がある画像は、なにかということに関する意識の差でも問題は起こります。例えば、若気の至りで公序良俗に反することをして、これを、その場ののりでSNSに投稿したとします。その写真が大炎上を起こしたとしたら、もしかしたらあなたの人生のあらゆる局面での歩みを妨げるものとなってしまうかもしれません。

流出したら問題になることは、しない、させない、(助長する意味ではなく)撮らない、投稿しないようにしましょう。

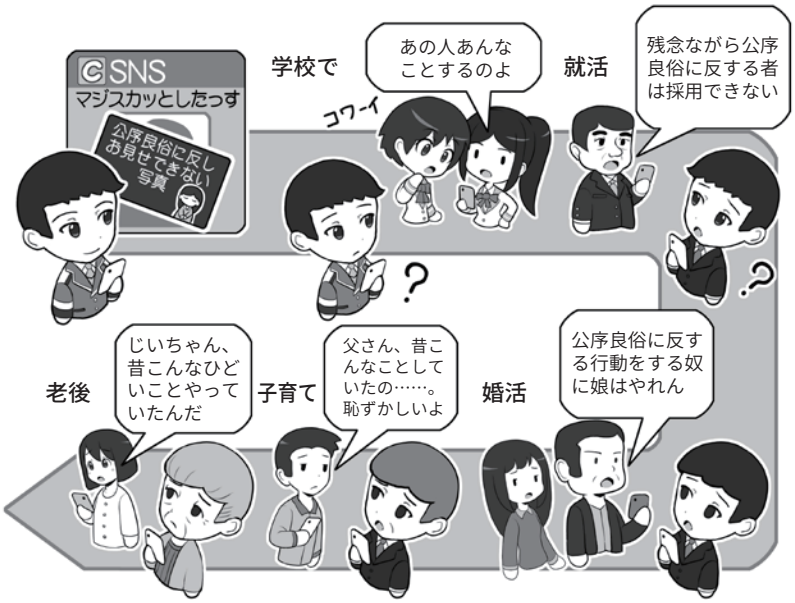
存在するデータは必ず流出すると考える



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：子どもにスマホを持たせるとき、「スマホ契約書」という提案

子どもがスマホを使いたいと要望してきたので、人生の課題を設定してそれをクリアしたら契約書付きで提供するようにした、というニュースがありました。

契約書というと物々しいですが、スマホ利用のルールを口頭ではなくきちんと明文化し、それをお互いが確認し合うことで、利用する子どもも「それをないがしろにしてはいけないことだ」ということを強く認識するというわけです。厳しいという意見もあると同時に、一歩階段を上り大人として扱われたことを喜ぶ子ども自身の意見もあるようです。

契約書の内容は、「家族からの連絡にきちんと返信すること」や、「朝受け取って夜親に返すこと」、「実際に会ったことがない人はアプリで友だちにならないこと」などがあります。

また、SNSを使ったトラブルになりそうな「面と向かっていわないことはSNSでもいわないこと」とか、海外の例では、「恥ずかしい写真を交換したいといわれてもやってはいけない」といった項目もありました。これは、SNS上での炎上の芽を摘んだり、未成年が同年代になりすました人間に裸の写真を要求された上で脅されたり、あるいは同級生同士で交換したものが流出したりする、セクスティングなどを未然に防ぐ意味で重要です。

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、ルールを時々見返したり、いったいわないにならない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と自律を促しましょう。

それと同時に、インターネット上の情報は必ずしも正しいとはいえず、フェイクニュースやデマが存在すること、情報は裏を取って初めて本当の情報となること、ときにスマホを置いて現実の世界へと飛び出し、自然や様々な動物に興味を持つことなどを書いた項目もありました。

些細なことですが、夜になったら親に返し、朝になったら渡してもらうといった項目は、友だちとメッセージをやり取りして眠れない、勝手に眠ると仲間はずれにされるといったことにして、「うちは夜になると親に返さないといけないからごめんね」とスパッといえ、一つのいい対処方法でもあるといえるでしょう。

「スマホ　契約書」で検索して、実際の契約書や記事を見てください。スマホのルール作りの一助になるかもしれません。

コラム：GPS、位置情報、ジオタグの管理

私たちが普段なにげなく使っているスマホは、実は相当に高機能で、10数年前ならばすべて別々の機器だったものが、まとまって小さなボディに収まっています。

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衛星からの電波をキャッチして、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」と押せば、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、油断すると意図せずこういった情報を公開してしまっていることもあります。

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ようにしておくと、撮影場所の情報が「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によっては撮影場所が公開されてしまうことがあります。その写真が自宅で撮影したものだったりすると、世界中に自宅の場所が公開されてしまうのです。

また、位置情報はSNSの投稿時に位置情報を公開する設定にしておくと、文字だけの投稿をしたつもりでも、写真を撮った場所まで文字で公開されてしまいます。

生活圏の位置情報を公開してしまうトラブルは、GPSにまつわるものだけではなく、普段立ち寄る店の名前を投稿したり、周りの風景が映り込んだ写真を投稿したりするだけで、いともたやすく「撮影場所が特定される」ことがあります。

そして、これらの「位置情報」もしくは「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。

ネットは知らない人と「距離とその移動に必要な時間」を超えて知り合える場所ですが、トラブルが発生すれば、それは距離を越えて現実世界の我が身に即座に襲いかかってきます。

位置情報を含む個人情報の管理は、しっかり行いましょう。

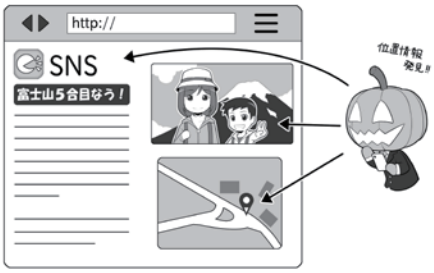
写真には位置情報が含まれることも

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OFF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ドロップされ、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いいので便利です。

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、投稿前後に必ずチェックしましょう。

コラム：SNSやSNSのグループを使ったいじめに備える（いじめ経験者からのアドバイス）

いじめは公共の目がある場よりも、人々の目が届きにくい比較的閉鎖された空間で起こりやすく、学校はときにその条件に当てはまります。

ネットが普及する以前であれば、コミュニケーションは言葉や暴力など、実際の行動となって現れていたので、それでもまだ目につく可能性がありました。

しかし、ネットの普及によって、そのいじめの一部がSNS上で匿名で、あるいはSNSの外から見えないグループ内で行われるようになると、いじめの実状を目にする方法が少なくなりました。

また、昔であれば学校から離れた別のコミュニティをもつことで、自分が自分らしくいられる場所を確保し、バランスを保つことができました。今はスマホを始終持ち歩くので、学校から離れ別のコミュニティに行き、スイッチを切り替えることも難しくなります。スマホを持っているとそれを通じて四六時中、学校のコミュニティにつながり続け、その中でのいじめは生活すべてにおいて、その影を落とし続けてしまうからです。

物理的ないじめはもちろん、SNSやネットを使ったいじめを受けているときは親に相談し、画面キャプチャーやコピー、録音などで証拠を集め、それを添えて恐れずに、専門の窓口に相談しましょう。

また、学校以外の自分の居場所やコミュニティをもつことで、「学校の中の自分ではない自分」という時間をもち、その中でのアイデンティティを確立しましょう。

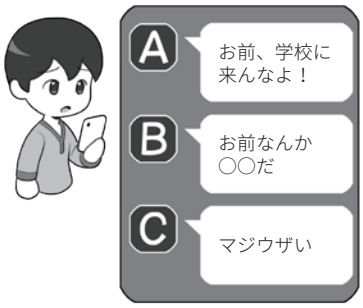
いじめに遭うのは辛いことですが、自分が否定されない別の空間をもつことができれば、心を休める場所と時間をもてます。その場所にいるときは、いっそスマホの電源をOFFにして、目の前に集中して過ごしてみましょう。

（空手道場で生き延びられたNISCのおじさんより）

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

ネットも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。

証拠を集めて相談しよう

いじめの告発をするときは、きちんと証拠がある方がトラブルの説明がしやすくなります。

自分らしくいられる別の場所をもとう

ネットに関係がない場所を探して、学校以外に自分の居場所を作りましょう。

コラム：モラルを逸脱すると炎上を生む

ネットのニュースなどを見ていると、「炎上」という言葉を良く目にします。

炎上とは、特定の人物がSNSなどに投稿した内容が不適切であるとして拡散され、多くの人から集中的に非難を受けることを指します。

例えば、特定のお店に関していいがかりのような投稿や嘘の書き込みをしたり、飲食店などで働いている人が芸能人のプライベートでの来店を投稿したり、引っ越し業者が業務上知り得た情報で引っ越した女性にアプローチをしたり、あるいは未成年が飲酒ありの大宴会をした投稿をするなどなど。

多くの場合は、世間一般の「モラル」に照らし合わせて、おかしいと思われるものに対して炎上は発生します。

問題は、その炎上の結果、炎上させた本人が非難されるだけでなく、嫌がらせをされたお店が閉店してしまったり、雇っていた会社が謝罪したりと、周辺に多大なる影響を及ぼしたり、また、本人にも損害賠償責任が発生したり、名誉棄損で訴えられたり、内定が取り消しになったりということが起こる点です。

この「炎上」をおこさないためには、投稿する人が「世間とのモラルと自分の意識のギャップを埋める」か、「投稿をしないか」しか解決策はありません。

ネットで炎上を見たら、その顛末を見て、どのような書き込みがどのような経緯で炎上を生み、どのような結果を招くか、どこに意識のずれがあったのか調べてみましょう。

また、ネットの掲示板などを利用して、自分の投稿を多人数のふりをしてはやす「自作自演」や、焚きつけるアオリ行為、誰かのふりをするなりすましの書き込みなども、状況によっては犯罪や名誉棄損の対象となる場合があります。

「こんなことになると思わなかった」という言い訳は昔からよく聞きますが、そういったところでもとには戻りません。現実世界とネットでのコミュニケーションの差、SNSの情報拡散の特徴などを、興味を持って調べて、騒がしくない穏やかな生活を送って下さい。

モラルを逸脱することが炎上を生む

自作自演やアオリ行為、嘘の書き込み

コラム：屋外でのゲームを安全に楽しむ。ながらスマホは×！

ここ数年のスマホのパワーアップにより、昔ならば専用ゲーム機が必要だった複雑なゲームでも、スマホで軽く動かせるようになりました。

それに伴い、従来から存在していた「位置情報ゲーム」と呼ばれるジャンルに、リアルタイムの地図情報や動く3Dキャラクター、カメラ映像にAR（拡張現実）を重ねたものも登場してきました。

スマホを持って現実世界に飛び出して、モンスターを捕獲したり、様々な場所に行ってご当地でアニメキャラクターと写真を撮ったり、あるいは全国の駅を巡るといったゲームが登場しています。

そういったゲームでは、みんなが安全に楽しく遊び、幸せになるために守らなければならないルールがあります。

まず、屋外でゲームをするとき「ながらスマホ」をするのは危険です。場所やものを探すゲームでは、ついついスマホの画面を見ながら歩いてしまいますが、わずかの時間スマホを見ているだけで誰かにぶつかったり、線路に落ちそうになったり、車にはねられそうになったりすることはありえます。また、わざとぶつかってくる「スマホ当たり屋」によって怪我をしたり、難癖をつけられ金銭を要求されるということも起こっています。

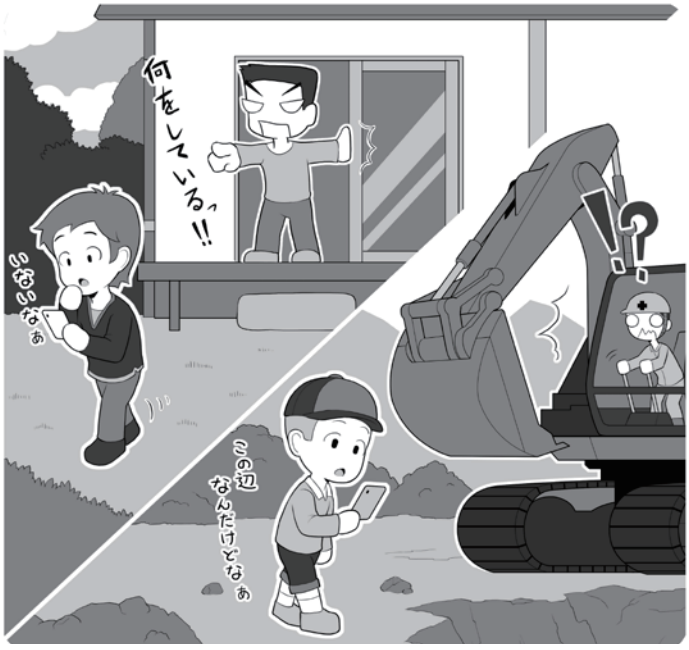
移動中は、画面を見ずに遊べる方法が提供されているこ

歩きスマホは自分も周りの人も危険

自分は大丈夫と思っていても、歩きスマホは大変危険な行為です。歩いているうちに車道に出て事故に遭ったり、駅のホームから転落することもあります。

また、歩きスマホをしている人を避けようとして、自転車や車に乗っている人が事故を起こしてしまう可能性もあります。歩きスマホはやめましょう。

私有地や危険な場所には入らない



スマホを使ったゲームをしていると、それに集中するばかりに、危険な場所に立ち入ったり、他人の家の敷地の中に入ってしまうこともあります。

危険な場所での事故や、海外では発砲トラブルも起きています。ゲームはゲーム、命をかけるものではなく、楽しむものです。モラルを持って楽しみましょう。

ともあるので、よく調べてみましょう。

また、自転車を運転しながらの操作や、当然のことながら自動車を運転中のスマホ操作は論外です。周りを見ないで運転する乗り物は、周りからすると命を奪いかねない大変な脅威ですし、条例や法律に違反する場合もあります。

また、ゲームに熱中していて誰かの家の敷地や私有地に入り込んでしまうと、これは「不法侵入」に当たります。

ただ、そういった不法行為の問題としてではなく、単純に「自分の家の庭に、知らない人が入ってきたらびっくりするよね」というように、相手の立場に立って考えましょう。そういった考え方ができるようになれば、ほかのシチュエーションでも生かせるはずです。

自分の街に、たくさん人が来て賑わうのはウェルカムですが、迷惑行為があると「もう来なくてよい」となり、誰もハッピーになりません。

また、危険な場所に入り込んでケガをすれば、救助する人員や救急車、場合によってはヘリコプターが必要になります。常識的に考えて、その場所が危険であると思われるなら、例えゲームのプレイエリアが設定されていても、近づかないようにしましょう。

こういったモラルや安全を守りながら楽しめるなら、現実世界でプレイするゲームは様々な場所にたくさんの人を呼び、ときには災害に遭った地域の復興支援にも役立つことがあります。

それが成功するかどうかは、みなさんに心持ちひとつにかかっていますよ。

運転中のスマホはダメ。車は凶器になります

運転中のながらスマホは違反です。運転している車はルールを守って使わないと一瞬で人の命を奪う凶器になるということを考えましょう。

位置ゲームを活用すれば、いいこともあるよ

スマホを使った位置ゲームは、上手く使えば地域活性化や復興支援に使える素晴らしいアイテムです。安全に使い、安全に楽しみ、そして、ゲームとともに様々な場所を巡って、旅を楽しみましょう。

2 サイバー関連でやってはいけないこと

1 アニメ・マンガ・音楽の違法なシェア。パクリなどの著作権侵害

インターネットは、基本的に様々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サーバ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、ダウンロードは作品が生み出される環境を破壊し、結果として作品が生まれなくなります。許可を得て公開されているものを利用しましょう。

こういった違法行為以外にも、ネットでは「パクリ」といわれるカジュアルな著作権侵害がよく行われています。

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のは著作権侵害ですし、SNSによっては利用規約違反になりアカウントを停止される場合もあります。

また、他人がウェブ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す。

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うでしょう。

ネットには距離が存在しない分、今まで会うことができなかった人に作品を届ける世界です。誰かの作品ではなく自ら作品を生み出して世界に届けましょう。

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」

2 ゲームの不正行為。恋人や家族でもプライバシーは守る

ゲームの不正コピーやチート行為もやってはいけないことです。

それ自身、規約違反で場合によっては犯罪として摘発されますし、「自分ひとりぐらいやっていても大丈夫」という人たちが増えていけば、楽しんでいるゲームそのものが生まれてくる環境を破壊してしまうことになります。

ゲームを作る人はゲームを売ることで利益を上げ、生活をし、また、新しいゲームを世の中に生み出してくれます。この利益の循環があるからこそ、ゲームを遊ぶ側は楽しい時間を過ごせるのです。

しかし、誰かが不正行為でこの「利益の循環」を回らなくしてしまうと、やがてゲームを作る人々は生活できなくなり、結果としてゲームがこの世に生み出されなくなってしまいます。

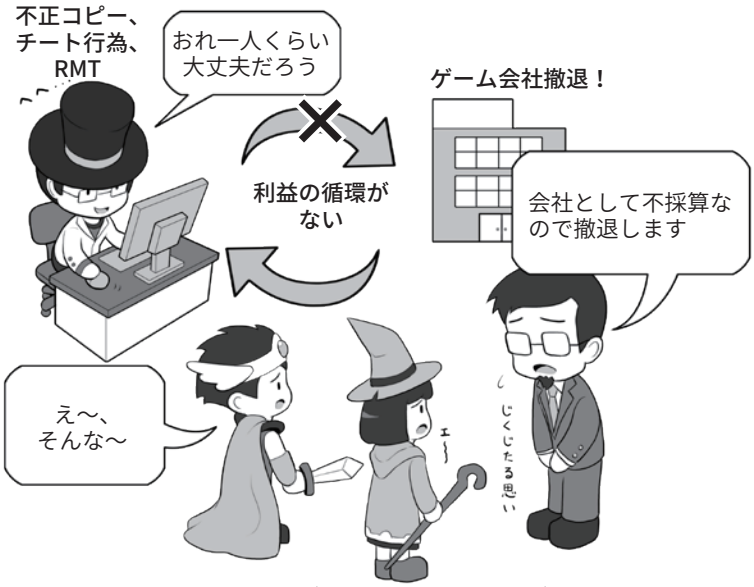
楽しみのある世界がいいですか？ない世界がいいですか？

私たちは信頼関係をもって楽しい世界を盛り上げていく人たちが大好きです。

信頼関係は普段の生活でも大切です。例えば、プライバシー。あなたが席を立っている間に勝手にスマホの中身を見られてしまったり、あるいは親があなたの部屋に勝手に入り込んで、パソコンに保存している日記を見ていたらどうでしょう。特に、「信頼している」人の行為は人を深く傷付けます。

また、「信頼関係」の名のもとに自分のプライバシーを守ってほしかったら、自分も誰かにとって、信頼を裏切らない人物にならなければいけません。

ゲームの不正行為は犯罪になることも…



不正コピー、チート行為、RMT（リアルマネートレード）など、ゲームの販売や運営を妨げたりする行為は、場合によっては犯罪として摘発されますが、それよりも積もり積もってゲームを生み出す会社やシステムの崩壊を引き起こしてしまうことが問題です。

その結果、みんなが楽しめる世界が奪われてしまうのです。利用者を信頼している制作者の人たちを裏切ってはいけません。

恋人や家族の間でも信頼関係は大事、でしょ

例えば、あなたの恋人や親がスマホの中を勝手に見たり、内緒でパソコンを開いて勝手に日記を見ていたりしたら、信頼関係はなくなってギスギスしてしまうでしょう。それにスマホやパソコンに対する安心感を失ってしまうかもしれません。

自分が「信頼」を守ってほしいと考えるなら、相手に対しても守らないとフェアではありません。信頼を守って笑顔の関係を作りましょう。

というようなことを真顔でいちいちいわれるよりも、お互いのことを思い合って、信頼し合い、笑顔で生活できる社会になった方がいいですよね。「いい笑顔」を守りましょう。

3 クラッキングはクールじゃない！

インターネット上には、「ダークウェブ」という、通常は見ることがないネットの陰の部分が確かにあります。そこには、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、悪意のハッカーがクラッキング用のツールを売っていたり、DDoS攻撃のためのゾンビ化した機器群を時間あたりいくらで貸し出したりもしています。

近年、若い子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」とツールを購入したり入手したりして、ランサムウェアによるサイバー攻撃や不正送金などを行い逮捕された例もあります。

では、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を想定し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り、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。

事実、「そういう事件があった」と報道されるのは、匿名でばれないと思った者たちを、捜査機関が地道な解析などで追い詰め、犯人を特定しているからです。

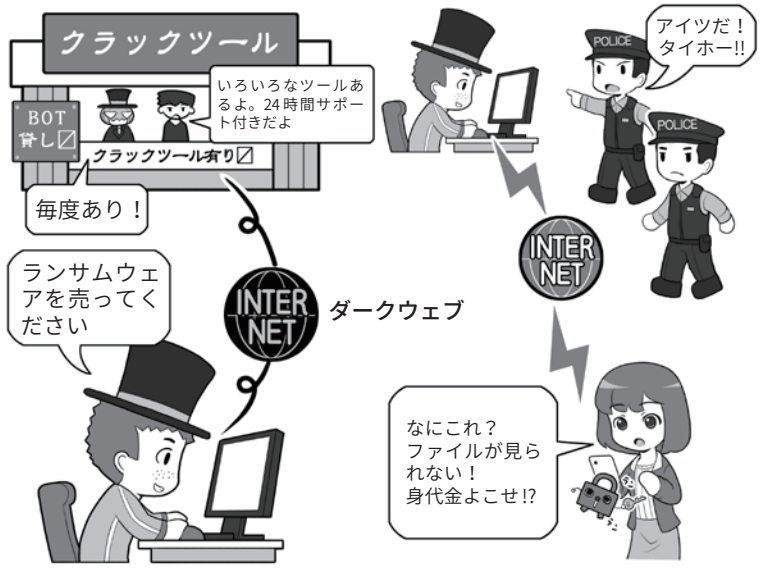
「有名になりたかった」「腕試しをしたかった」「小遣い稼ぎで」

そういう言い訳をしつつクラッキングを行っても、しょせんは自己満足であって、その行為は誰もハッピーにしません。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つづけることだってあるのです。

それよりも、腕と技術力で多くの人々をハッピーにし、ネットの偉人として名前を刻む方が「かっこいい」でしょう？

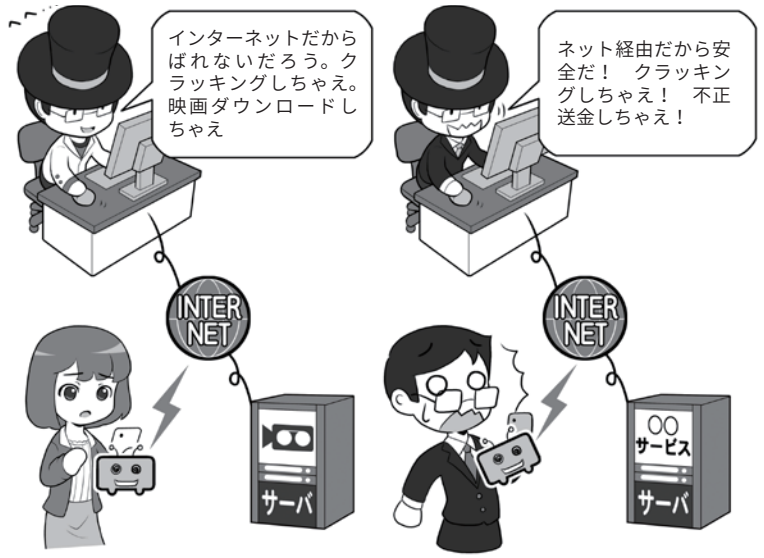
ネットでは、現実よりも名前が長く残るかもしれませんよ。

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、クラッキングは様々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。

コラム：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、非常に幼い子ども達が行い児童相談所に通告されたり、未成年が書類送検されたりしている事件もあります。

見てはいけないウェブサイト、危険なサイトをフィルタリングするだけでなく、コンピュータやスマホを使う際、どういうことをしてはいけないのか、きちんと家族で話し合っておく必要があります。下記の例などを参考に事例を調べて、共有してみてください。

他人のアカウントへの不正なログインや乗っとりをした場合

不正アクセス禁止法
不正アクセス行為の禁止

第三条、第十一条
→三年以下の懲役または
百万円以下の罰金

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）
第百六十八条の二
→三年以下の懲役または
五十万円以下の罰金

（取得、保管）
第百六十八条の三
→二年以下の懲役または
三十万円以下の罰金

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）
第七条第一項
→一年以下の懲役または
百万円以下の罰金

（特定少数者への提供）
第七条第二項
→三年以下の懲役または
三百万円以下の罰金

● アカウント乗っ取り

2011年　奈良県の小学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とパスワードを聞き出し、本人になりすましてログイン、その女子中学生のアカウントを乗っ取ったもの。小学生の女子児童は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。

● ウイルス保管と提供

2017年12月、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、大阪に住む小学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た。またこれをダウンロードした京都、山梨などに住む児童も不正指令電磁的記録取得の非行内容で児童相談所に通告された。児童は「友だちを驚かせたかった」などと述べた。

● 同級生の少女の裸の画像を拡散

2018年4月、同級生が高校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。16歳から17歳の男女4人の児童は、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た。

コラム：成人年齢18歳引き下げに伴って注意が必要なこと

2018年6月に民法が改正され、約140年ぶりに成人年齢が20歳から18歳に変更されることとなりました。この改正により、2022年4月1日以降は、18歳になると成人になり、また、すでに18歳、19歳になっている人は、この日をもって成人となります。

さて、成人すると、なにが変わるのでしょう。すぐに思いつくのは、飲酒や喫煙、ギャンブルなどがありますが、これらは、成人年齢が変更されても20歳以上のままで変更はありません。最も大きな変化は、「親権者の親権に服さなくなる」ことです。

未成年者は、親権者の同意なく契約行為ができませんが、今回の改正で、18歳になれば成人になりますから、自らの意思で契約行為をすることができます。

例えば、携帯電話の購入では、回線の利用契約が必要ですが、保護者が契約した上で、利用者を未成年者としたり、保護者の同意のもと未成年者が契約したりすることになっています。これも施行後は、18歳以上ならば自身で契約できるようになります。また、青少年インターネット環境整備法で携帯電話会社に提供が義務付けられているフィルタリングも、その提供が契約事項に含まれているため、これまでは未成年者は親権者の同意がなければ自分の意思で解除をできませんでしたが、施行後は18歳ならばそれも可能になります。

ソーシャルゲーム、オンラインゲームでの課金やオンライン通販などでの購入も契約行為です。親権者の同意のない課金は、未成年者による契約を理由に取り消しを申し出ることが可能でしたが、施行後は18歳になれば成人ですので、未成年であることを理由に取り消しはできません。日頃から課金などをしている場合には、自身で課金額などを確認し、支払える範囲内に収めておくよう心掛けましょう。

さらに、高齢者だけでなく成人したばかりの若者をターゲットに、SNSなどで甘い言葉や人間関係を作って勧誘するような手口が国民生活センターからも報告されています。18歳成人化を控えて、従来よりもより低年齢層にターゲットが広がるおそれもありますので、日頃からこうした甘い言葉や見知らぬ人からの誘いには注意しておきましょう。

18歳成人化の対象者

対象者	成人になる日	成人年齢
2002年4月1日以前の生まれ	20歳の誕生日	20歳
2002年4月2日～2003年4月1日生まれ	2022年4月1日	19歳
2003年4月2日～2004年4月1日生まれ	2022年4月1日	18歳
2004年4月2日以降の生まれ	18歳の誕生日	18歳

変わるもの・変わらないもの

変わるもの	変わらないもの
・携帯電話の契約 ・ローンを組む ・クレジットカードをつくる ・賃貸契約を結ぶ ・10年有効のパスポート取得 ・結婚　など	・お酒を飲む ・タバコを吸う ・競馬、競輪、オートレース、競艇の投票券（馬券等）を買う ・大型・中型自動車運転免許の取得　など

コラム：デジタル遺産相続

近年、生活の中にIT機器やウェブサービスが深く入り込むにつれ、それぞれで必要となるIDとパスワードの数は増加する一方です。

また、例えば家族の中でITに詳しい人が一人だったり、あるいは互いになにを利用しているか話していなかったりした場合、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。

特に、問題になりやすいのは負の遺産で、FX(外国為替証拠金取引)で取引をしたまま亡くなった場合、取引が継続されていて、その後相場が大きく変動して、知らないうちに莫大な負債(不足)を抱え込んだという例もあります。

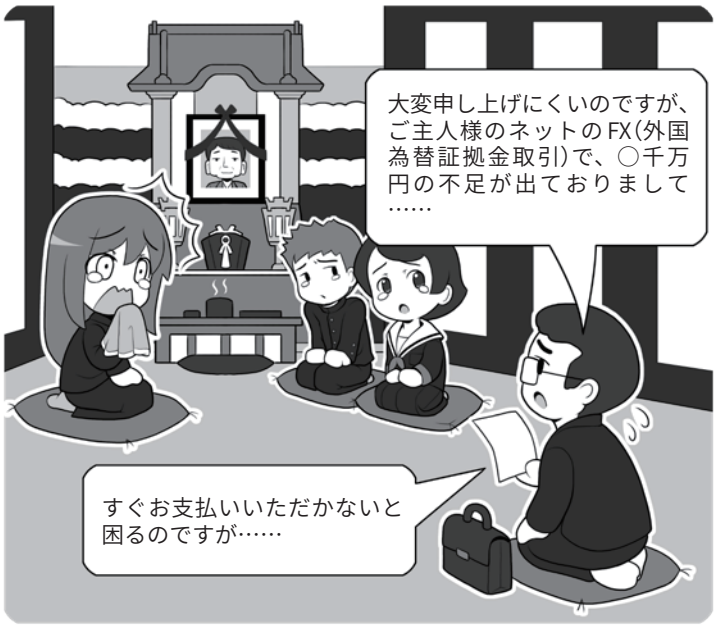
イラストのように、極端な話しになるかどうかはさておき、「立つ鳥跡を濁さず」にするためには、残された人が迷わないように、万が一のときに備えて管理情報のありかを残しておきましょう。

どういったサービスを利用していたかの一覧や、もし亡くなったらどのような処理をしたらいいか。IDやパスワードなどをパスワード帳に書き残すか、スマホのパスワード管理アプリを利用している場合は、その解除のためのPINコードなどを、ノートや遺言書に残すか、家族と共有しておきましょう。

SNSのウェブサービスなどは、本人が亡くなった場合、特定の人を管理者に指定できる機能が提供されている場合もあります。調べてみましょう。

残された家族が美しい思い出に浸りながらあなたを偲ぶことができるように、きちんと整理をしておきましょう。

きちんと伝えておかないと、突然負の遺産が現れることも



これは極端なたとえですが、お金のやりとりが発生するサービスをそのままにしておくと、支払いや負債が残された家族にかかってくる場合があります。

なにをやっていたかをパスワードを含めて書き残す

お金のやりとりが発生するものは支払いや負債が発生する可能性があり、ブログや電子メールアカウント、デジタル写真サービスは乗っ取られる可能性があります。誰かが相続し管理をするか、きちんと終了させる必要があります。パスワード帳などに書き残すのも一つの方法です。

3 デジタルテクノロジーで家族を守る

1 子ども達を守る

子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。

子どもたちが犯罪に当たる行為をするとき、本人達はそれが「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。

その上で、セキュリティソフトやフィルタリングサービス、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、子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、子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。セキュリティ設定の変更などはあっという間にクリアしてしまうでしょう。

ですから、叱ったり、とがめたり、あるいは取引のようにするのではなく、その必要性を共有し、特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、子どもからルールの変更

本当は怖いインターネット

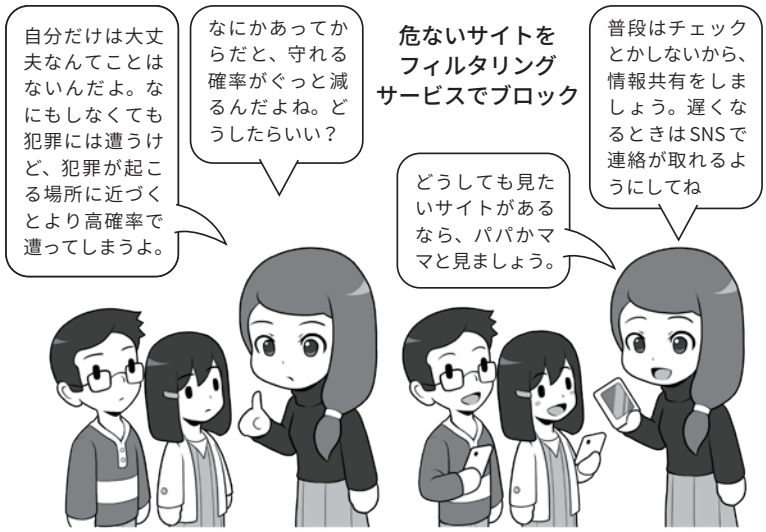
理由をいわずに禁止するのは命令

ネットでなにが起こるかを一緒に見る

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。子どもだけでは、対処できないトラブルがあることを知ることは重要です。

自分だけは大丈夫と思わせない

保護者機能や位置情報を活用する



意識を共有したら、実例を示して子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。

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お子さん達を守るサービスや機器も、いろいろと登場しています。

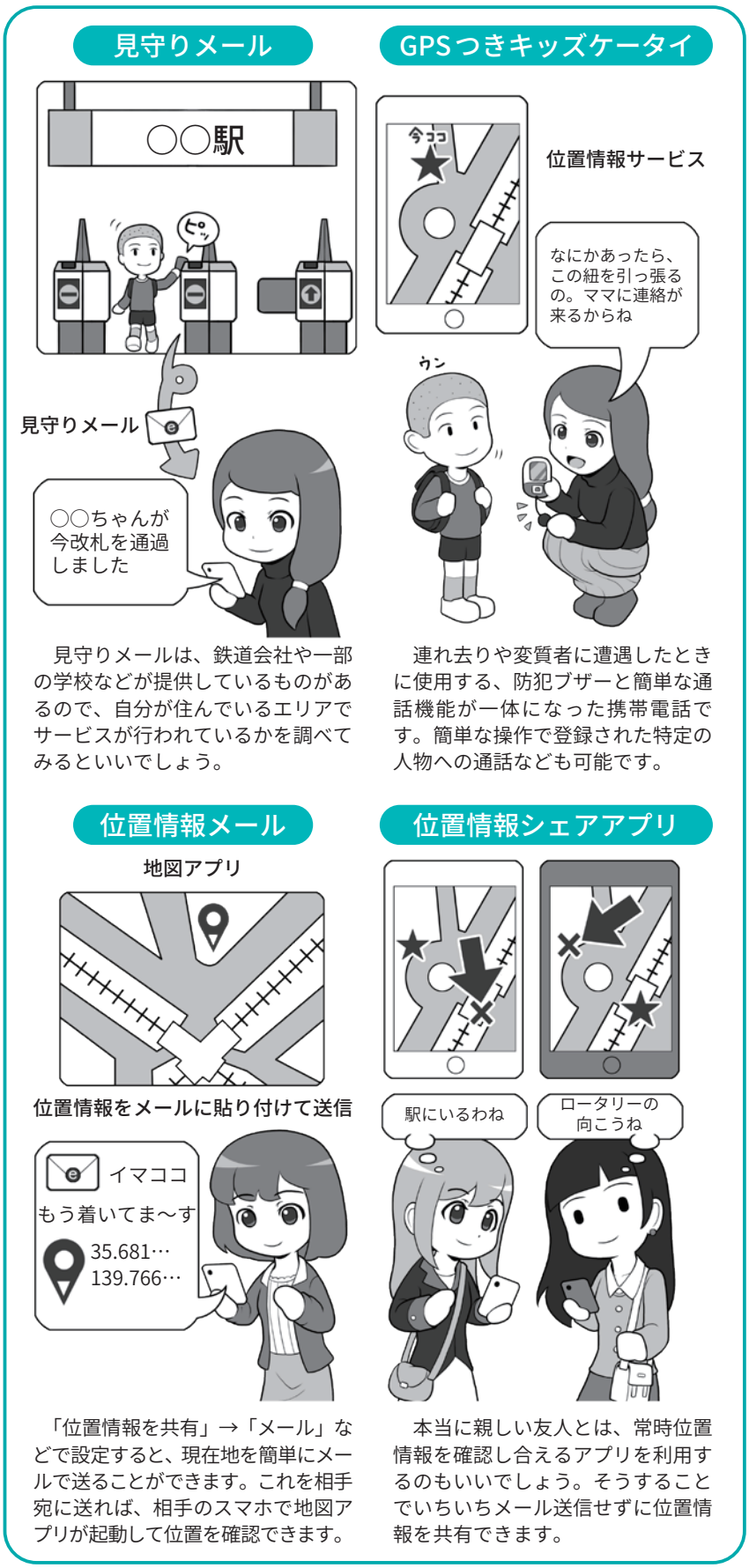
学校を離れたときや駅を通過したときに、親のスマホにメールが送信される見守りメールサービスや、簡単な携帯電話とGPSと防犯ブザーが合体したキッズケータイは、子どもたちが意識しないで使え、あるいはシンプルな操作方法を理解したら、いざというときの強い味方になります。

また、ある程度スマホの操作をすることができる年代になったら、位置情報を送信したり、必要な情報をメールやSNSを通じてシェアする方法を、一緒に覚えるのもいいでしょう。

幼いお子さんの姿が見えなくなって、一番困るのは迷子になってしまうことです。また、親とでもお友だちとでも、待ち合わせ場所などで誰かを探すようなそぶりをしていると、知らない人物から「一緒に探してあげる」というような声をかけられる隙になります。目的の場所に迷わずたどり着け、必要であれば待ち合わせをし、迷わず会うことができるスキルを身につけると役に立つでしょう。

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、今後地下街や屋内などにビーコンと呼ばれる機械の設置により、屋内でも位置情報の交換が可能となると考えられます。

そのほかにも、電車やバスの乗り換え案内アプリ、徒歩ナビゲーションの活用などを覚えることで、どこかではぐれても、家に帰り着くスキルを一緒に学びましょう。



2 お年寄りを守る

離れて暮らしているお年寄りと連絡を取り合うのに、テレビ電話機能に対応したスマートテレビや大きなタブレット、液晶付きスマートスピーカーをプレゼントして、ときどき映像つき電話をして声だけでなく顔を見せるのもいいでしょう。

また、一人暮らしのお年寄りの見守りのために、よく相談をした上でウェブカメラの設置をしたり、毎日部屋の中を動いて電化製品やガスを使用しているかをメールで連絡してくれるサービスも存在するので、こちらも相談し、納得してもらった上で利用したりするのも一つの手でしょう。

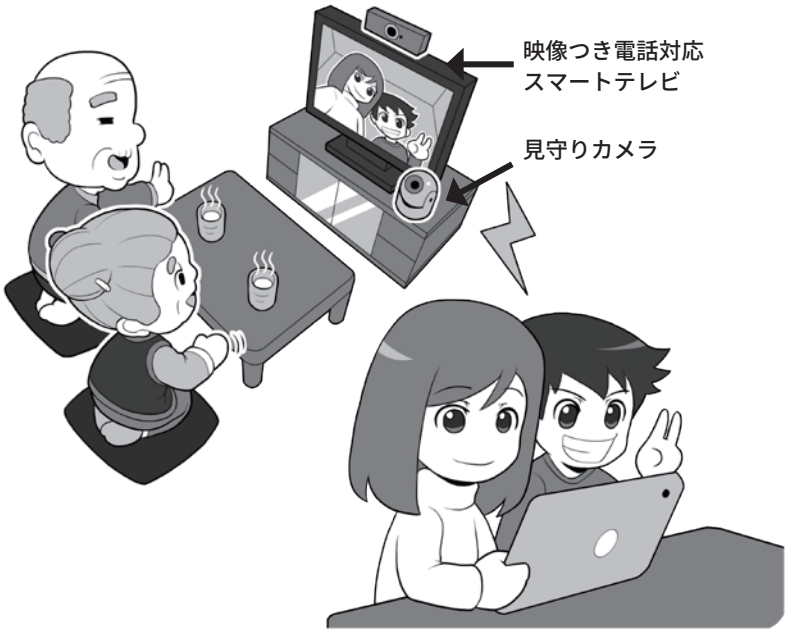
一番いいのは会いに行くことですが、離れて住んでいて頻繁に会えないならば、そういうときこそインターネットの「距離とその移動に必要だった時間が消えた世界」という能力を生かしましょう。

また、「自分は大丈夫」と思っているお年寄りほど、あっさりと振り込め詐欺などに引っかかってしまうものです。振り込め詐欺は電話で顔が見えない状況で、相手を不安に陥れ正常な判断ができなくなることを利用しています。

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、だまされることを回避できるかもしれません。

そのテレビ電話機能のためではありませんが、お年寄りには使いやすい簡単操作のスマホを渡すのも一つのアイデアです。または、いざ操作を勉強する段になって教えてあげやすいように、自分が持っているものと同じ機種を渡しておくのも一つの考え方です。

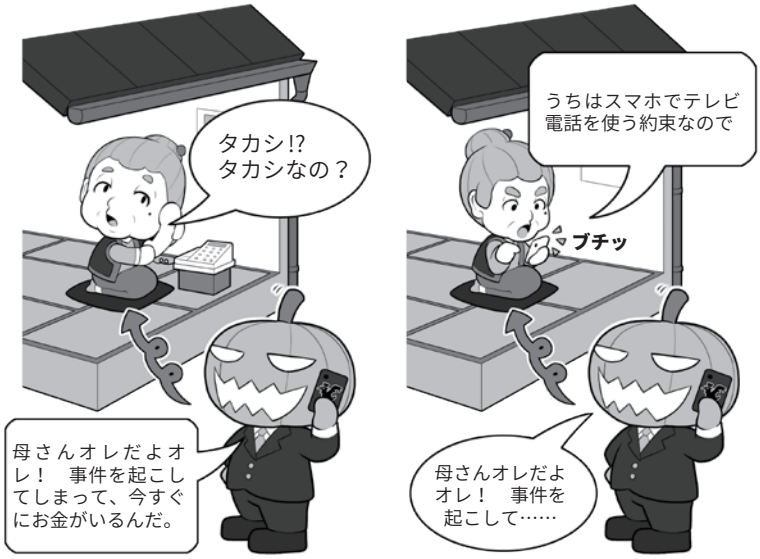
映像つき電話やITサービスの活用



お年寄りにとって子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、一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、利用を検討してもいいでしょう。

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、かかってきた電話を受けることはできるものです。子どもや孫から連絡を取るときは必ずTV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。

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することができるので、予定どおりに旅行しているかもチェックすることができます。

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、どのようにしたらいいかのアドバイスも的確にできるでしょう。

そん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られたりした場合も、操作するための情報を共有しておけば、スマホをロックしたり所在地を確認することもできます。

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に出て徘徊し、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。

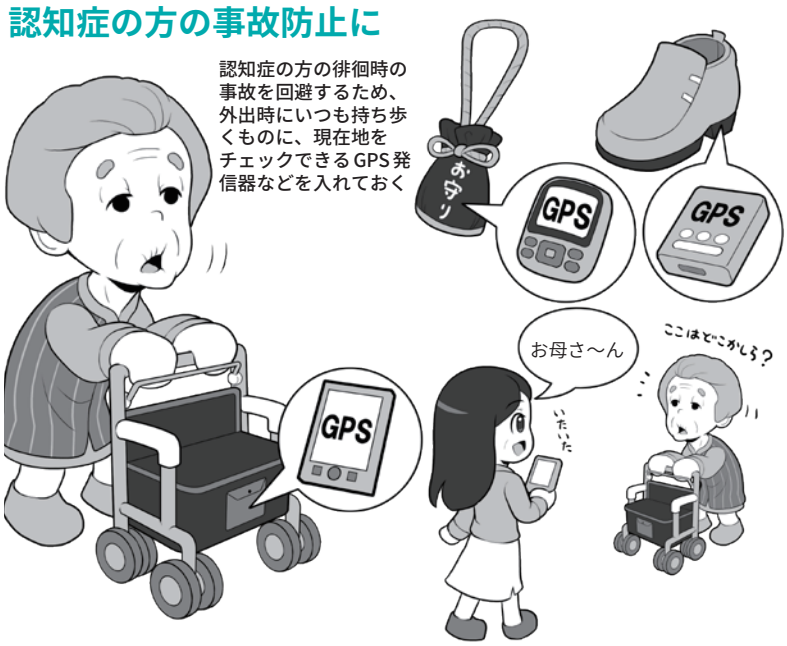
お年寄りによっては、持ち慣れない機器を持つことを嫌がる場合もありますので、機器を入れる場所の工夫は必要ですが、事故などを未然に防げる可能性が少しでも高くなるならば、検討してみるといいでしょう。

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、そもそも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ういった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。

4 屋外・海外でのネットワーク利用

1 一見なにもないように見えて、危険がいっぱい

例えば、国内でも国外でも、あなたが屋外のカフェでパソコンを開いてウェブを見たりメールをやりとりしたりするとします。カフェには無料の無線LANアクセスポイントがあって快適にネットに接続することができます。うららかな日差し、さえずる鳥の声、実に平和そのものだし、ちょっとお店に入ってケーキでも選んでこようかな？

さぁこのカフェには、どんなサイバーセキュリティ上の危険があると思いますか？

まず日本では、よくスマホで席取りをしてレジに行くのを見かけますが、海外では、貴重品は肌身離さず持つことをおすすめします。日本と同じ治安レベルとは限らないので盗難される可能性があります。日本でも油断はなりません。

また、席に置きっぱなしにしたパソコンへ目を離した一瞬に、USBメモリを差し込んでマルウェアに感染させることもできます。

所持品が盗まれなくても、肩越しや場合によっては双眼鏡や望遠レンズを使って、スマホやパソコンのロック解除用PINコードを盗み見されるかもしれません。

お店の無線LANアクセスポイントの暗号化は、本当に安全な方式ですか？パスワード（暗号キー）を店内に貼り出していませんか？通信を盗聴されたり、ウェブサービスにログインするIDやパスワードを盗まれたり、不正なサイトへ誘導されたりするかも知れません。そのために攻撃者が店のアクセスポイントと全く同じ名前の偽のアクセスポイントを設置して、あなたを待ち構えているかもしれませんよ。

気をつけてくださいね。

2 インターネットカフェの利用

海外旅行に出かけるときになるべく荷物を減らそうとすると、仕事での渡航でないなら、パソコンはお留守番になるでしょう。

最近では、スマホもありますし、長いメールを書く必要があるなら、インターネットカフェに行って、ウェブメールを利用すれば、ホテルでもなんでも予約できるし…、なんて思ってはいませんか？

インターネットカフェは、国内外を問わず便利ではありますが、これを使ってメールやなんらかのウェブサービスのIDとパスワードの入力、あるいはクレジットカード情報の入力は、絶対に避けることをおすすめします。

海外のインターネットカフェのパソコンは、管理が充分ではないことがあるほか、攻撃者にとっても狙いやすいターゲットでもあります。キーロガーというマルウェアを仕込んで、利用者が入力したIDやパスワードなどの個人情報を抜き取って攻撃者に送信してしまうことがあるのです。

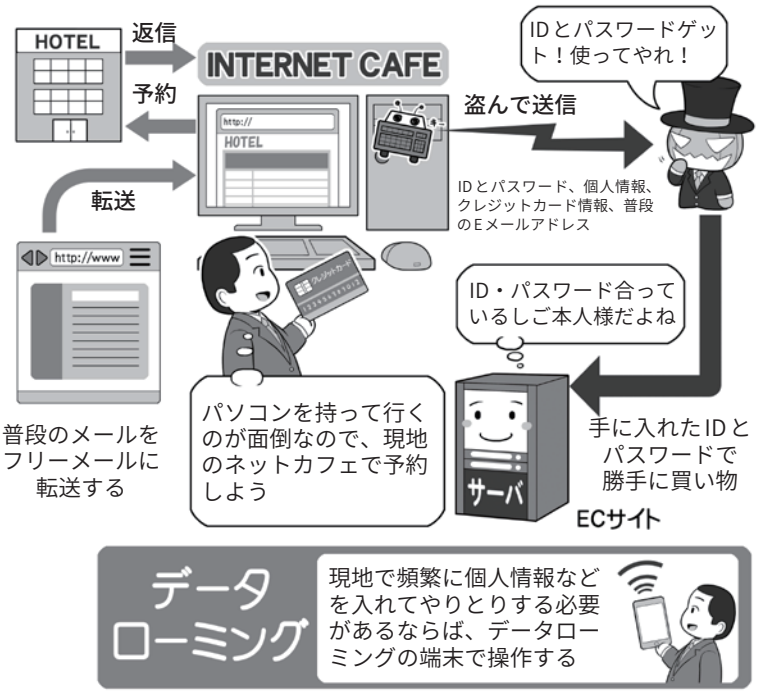
お店の人がシステムを最新に保ち、セキュリティソフトも入れ管理しているから、そんなソフト仕込めないよ、と思ったら甘いのです。キーロガーにはハードウェア版もあり、数秒あればパソコンの本体の後ろ、キーボードのUSB端子と本体の間に装着でき、あとは無線LAN経由でデータを送信できるものもあります。今まで利用したパソコンの後ろをいちいち確認したことはないでしょう？

また、自分のパソコンやタブレットを持ち込んで店のWi-Fiを使用する場合は、自前の暗号化ができないなら利用はおすすめしません。もし現地で頻繁にデータ通信を利用するならば、データローミングや現地の定額SIM（次頁参照）の使用をおすすめします。

インターネットカフェのマシンには、キーロガーなどが仕込んである前提で利用する

インターネットカフェは、基本的に情報を検索するだけに利用します。IDとパスワード、個人情報、クレジットカード情報は絶対に入力しないように。自分の持ち込みパソコンなどを利用する場合は、自前の通信の暗号化ができるならOKです。

共用のパソコンで重要な情報をやりとりしたら攻撃者に漏れる可能性あり



インターネットカフェで普段利用しているウェブメールを使うのは危ないと考え、フリーメールアドレスを作成しそこにメールを転送しても、結局予約のやりとりなどを現地で行うことになるのなら、情報流出の危険性はかわりません。

現地でそういった情報を入力することが多いのならば、タブレットなどでデータローミングを行うか、自前の暗号化＋公衆無線LANを使うようにしましょう。

3 海外でスマホやタブレットを活用するために

スマホやタブレットを海外旅行にもっていって現地で使う場合、日本で契約している携帯電話会社が提供するローミングサービスを使って、現地の携帯電話回線提供会社と契約せず、データ通信を利用する方法があります。

ローミングサービスは国内よりは割高で、また、音声とデータ通信は別々に料金設定されていることもあるので、利用した場合いくらかかるのかをよく確かめてから使いましょう。さもないと途轍もない料金請求が届く場合があります。最近は手頃な1日あたり料金定額などのプランも存在します。

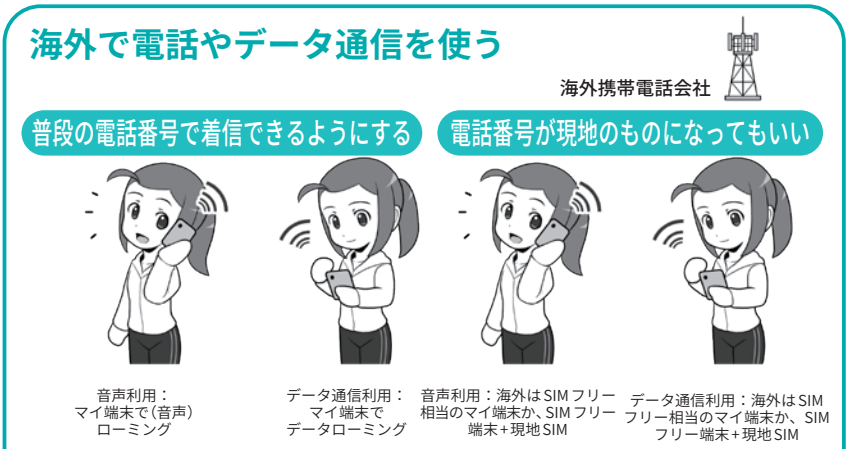
また海外では、電話を受けただけでも電話料金がかかる会社もあります。着信が無料ではない場合、電話を受けたらいくらかかるのかもチェックしておきましょう。さもないと、不意の長話で高額な請求が来てしまうかもしれません(くどい?)。

データ通信が使えなくも、短い文章のやりとりをする方法にショートメッセージ(SMS)がありますが、これも利用可能かどうかと、利用できる場合の料金を調べておきましょう。電波整備状況がよくなくデータ通信が使えない場合の文字通信手段になります。

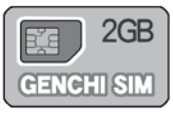
ローミングサービスを電話で利用するメリットは、海外にいても自分の電話番号にかかってきた通話を受けられることです。

もし、長期で滞在する場合などで、その間電話番号が変わってもいいならば、現地携帯電話会社のSIMを購入して利用する方法もあります。SIMには目的別に音声のみ、音声＋データ通信、タブレット用にデータ通信のみなどのSIM

海外で電話やデータ通信を使う



現地SIMは現地空港などでも買えるが……



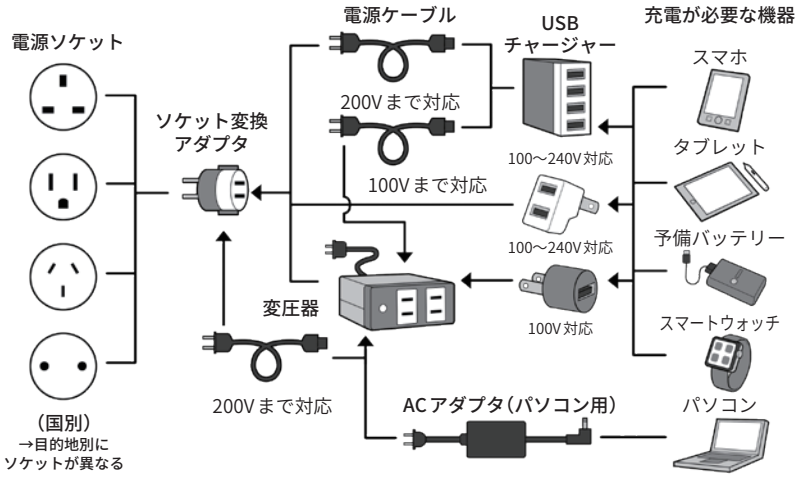
- 日本で買えることも(SIMのサイズに注意)
- 事前使用設定を済ませておく
- 音声の料金、データ通信の上限容量をチェック
- 月額料金が発生せず、チャージすれば保存可能なものもある。何回も訪れるなら選択肢に
- 料金は従量制か、上限のある定額制か確かめる

外国語が苦手だからメールでやりとりしようと思ったら

海外では意外とデータ通信できず、音声のみのエリアも多いのです。データ通信できても遅い場合もあります。データ通信速度を確保できないことを想定して、地図アプリの地図データなどは日本で事前にダウンロードしておきましょう。

電源・充電方法の確保

ソケットと電源のボルト数はまちまち。理想的にはすべて100〜240V対応であること



USBチャージャーのUSB端子は、充電する機器の数だけ差し込み口はあるか、全体の電源容量は足りているか、タブレット用には充電能力は足りているかチェック。200V系の国へ訪問するときは、ACアダプターだけでなくケーブルまでもが200V対応かをチェックします。

が存在します。

普段の端末は日本からの着信専用にして、別途SIMフリーの端末を用意し、これに現地のSIMを入れて使用する方法もあります。

海外のSIMを使う場合の注意点は、利用する端末が「SIMフリー」か同様の状態であることを確かめることです。日本の携帯電話会社で販売されてる端末は、その会社のSIMしか使えない設定になっていることがあるからです。ただ、多くの端末では、国内では制限があっても海外ではどのSIMでも使える「SIMフリー」相当になっているものもあり、また、条件を満たせば携帯電話会社が有料でSIMフリーに改修する「SIMロック解除」を行ってくれます。

また、忘れがちなのが充電に関することです。充電器の対応電圧と、充電器にケーブルがある場合はこのケーブルの対応電圧が訪問国の電気事情にあっているか確認して、必要に応じ変圧器を用意、また、現地の様々なタイプの電源ソケットの形状に対応できるソケット変換アダプターも用意しておきましょう。

次に、せっかくスマホなどを海外に持っていくのなら、海外で使える機能や役立つ機能を準備していきましょう。

まずは翻訳系です。文字を入力するのではなく、音声で入力、翻訳結果も音読してくれるアプリなどもあります。また、逆に相手にしゃべってもらってそれを翻訳することもできるので、音声を使って現地の人と理解を深め合うことができるでしょう。

次は翻訳カメラ。海外で街並みやメニューなどを撮影すると、文字部分を認識し翻訳して表示するものです。こちらもいちいち辞書アプリなどに文字を入力する手間が省けますので、海外の旅をより楽しむことができるでしょう。

地図系のアプリのインストールと、現地の地図のダウンロードも重要です。前述のコラムでも書きましたが、海外では場所によっては日本のように通信網が充実しておらず、データ通信があっても遅いか、場所によっては全く使えないこともしばしばです。そんな中で、現在地を確認しなければならない状態になったとき、オフラインでも使えるように、地図をスマホにダウンロードできるものを準備しておきましょう。

海外でITを活用する

翻訳アプリ

翻訳カメラ

地図ソフト、GPSナビ

(音声)ローミングの注意点

- 海外では通話を受けても料金がかかる場合もある
- ローミング時の料金はいくらかかるのかチェックしておく
- SMS(ショートメッセージ)が利用できるかどうかと、その料金

データローミングの注意点

- 必要がないなら、データローミングの設定を必ず切る
- つながるからと放置しておくと、莫大な請求金額がくる場合がある

海外利用におけるSIMフリーとは

手持ちのスマホなどが海外でも使えるか

- 目的の国でのローミングに対応しているか、実際使用されているか。現地の会社の周波数帯(バンド)に合っているか
- 海外のSIMが使用可能か(≒SIMフリー)

日常使っているスマホなどを、SIMを入れ替えて使う

○ 現地SIMなら料金も手頃なものがあり、電話料金も安い

× 日本から普段の番号につなげない。滞在期間中の電話番号を教えておく必要あり

SIMフリー端末の入手とは

- 日本では、特定の会社のSIMのみ利用可能だが、海外では、どれでもOK(海外では「SIMフリー」相当)
- お金を払うと携帯電話会社がSIMフリー状態に改修してくれる(SIMフリー)
- そもそも電気店やメーカーから直接SIMフリーのスマホを買う(SIMフリー)

普段使っていないSIMフリー機を使う

○ 手頃なSIMフリー機を入手するか、使わなくなったものをSIMフリー化しておく

現地SIM使用、料金も手頃

○ 普段使用の機種は電話を受けるだけのローミング。日本の電話番号でかけられる

× 2台持ちは面倒

5 大災害やテロに備える

1 まずは自分の身の安全を確保する

大地震・各種の自然災害・テロなどが発生したり、なんらかの避難勧告が発表されたら、決してその場に留まって写真を撮ったり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。昨今の豪雨・水害などの自然災害の例を見ると、避難勧告前に自主的に避難場所に移動することが安全です。

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。

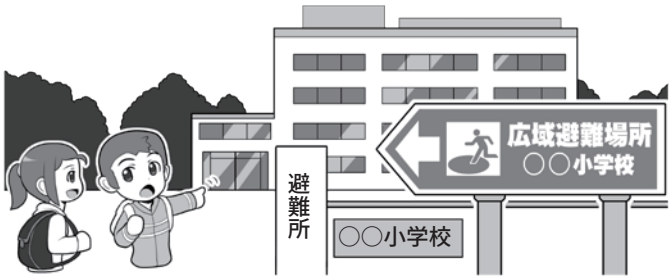
避難場所に到着し、そこが安全であると確認できたら、安否確認の連絡や情報収集をしましょう。

安否確認サービスは様々なものがあるので、家族や友だちと事前にどのサービスを利用するかを決めておきましょう。また、災害時はスマホの電話やウェブの閲覧などは混み合ってつながりにくくなります。災害時に通話が優先される公衆電話や、データ通信量の少なくてすむ、メールやSNSなどのサービスを使いましょう。

なお、スマホアプリの通話機能もメールなどより通信容量を多く使います。譲り合い、少ないデータ通信ですむ手段を利用しましょう。

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。

2 電池をもたす、情報収集をする

災害時などに街中なのにスマホが圏外になったら、それは通信会社の基地局が機能しなくなった印です。そのまま電源をONにしておくと、スマホはつながらない基地局に接続しようとして貴重な電池を消耗してしまいます。

そういったときはスパッとスマホの電源を切るか、スマホの中身を見る場合でもフライトモード（機内モード）にして少しでも電池の消費を抑えましょう。

電波が回復しても、電話よりはデータ通信であるメールやSNSを利用しましょう。災害時はその方がつながりやすく、電池の消費も少なくてすみます。次に、いつ充電できるかわからない状況では、とにかく電池の節約を心がけましょう。モバイルバッテリーを日常的に持ち歩くのもいいでしょう。

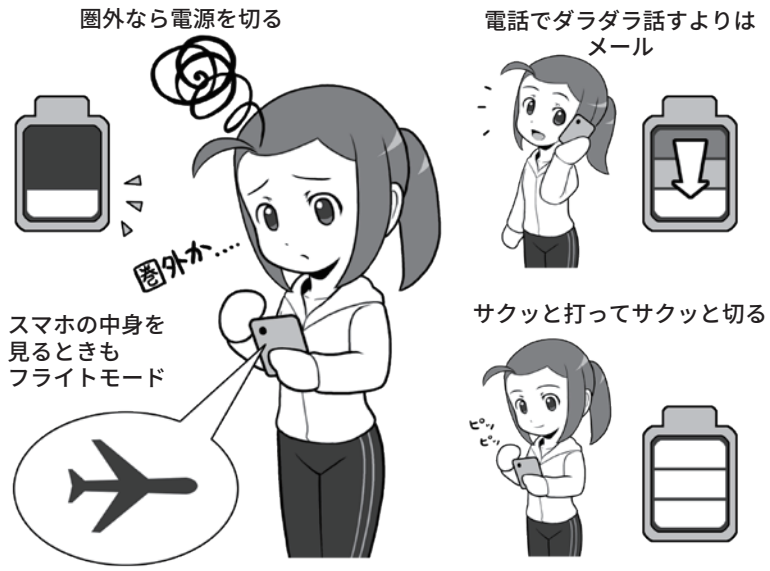
災害直後は情報が錯綜しますが、一定時間が経過すると救援物資や脱出ルートなどの情報がネットに発信され、やがて整然とした情報発信が行われるようになります。

しかし、だらだらとウェブを見て回って情報を収集しても電池を消費するだけなので、メールやSNSで、情報の収集と整理に長けた家族や親しい友人に助けを求め、信憑性や関連性の高い情報、必要としている情報だけを整理して送ってもらうのもいいでしょう。

東日本大震災では、旅行で被災地に訪れているときに震災に遭い、帰ることができなくなった方たちが、SNSを通じて被災地から地元に帰るためのルートの確認や車両手配、バスの予約などをしてもらった例もあります。

ぜひ、そういった事例をみんなで話し合って、いざというときにどうするか、ということを相談しておいてみてください。

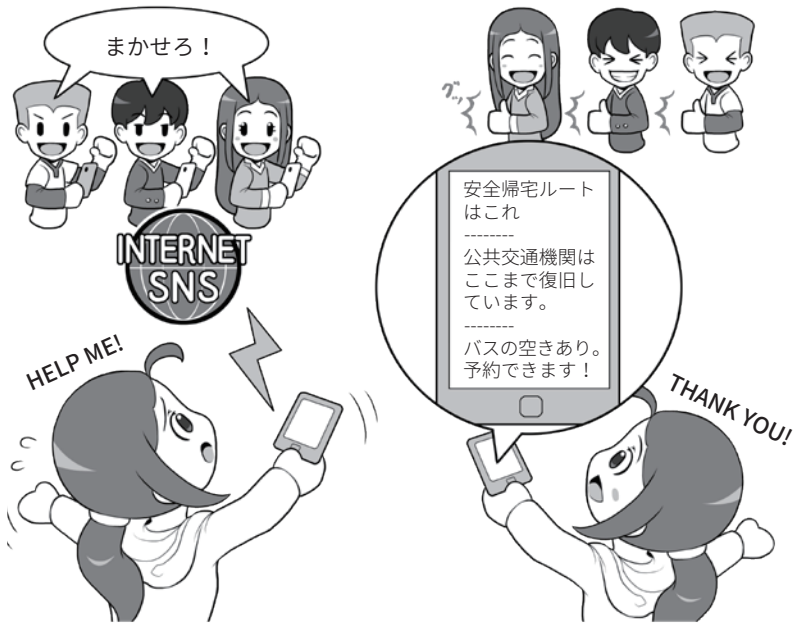
電池をもたすテクニック



圏外ならば電源を切るか、スマホの内容の閲覧時もフライトモードを利用します。電波が回復したら災害用の超省電力モードがあれば活用してもいいでしょう。

電話で長く話すよりも、メールをさくっと打って電源を切った方が電池を消費しません。充電器にもなるモバイルバッテリーを持ち歩くのも役立ちます。

情報収集に協力してもらう



情報収集に長けた家族や友人に相談して、いざというときは情報収集や必要なものの手配をお願いできるようにしておきましょう。自分一人では、気づかない情報も外から見ていると気づく場合もあります。

3 ラジオ、車載テレビを使った情報収集

大災害時に電波がきちんと飛んでいる状態でも、目的のサーバに接続しようとすると、反応がない場合があります。

それは、サイバー攻撃のDDoS攻撃のように、多くの人が特定のサーバに集中して接続することで、サーバの反応が間に合わなくなり、ギブアップの状況になっているためと思われます。

この問題は災害時には避けがたく、双方向通信のメディア、つまり私たちがサーバに接続してサーバが返信するというプロセスを前提としているインターネットでは、どうすることもできません。

こういったときに力を発揮するのが、「片方向通信メディア」である、ラジオやテレビです。これらのメディアは送信局が一方的に情報を発信して私たちが受信するだけなので、アクセスが集中し反応できなくなるということはありえません。

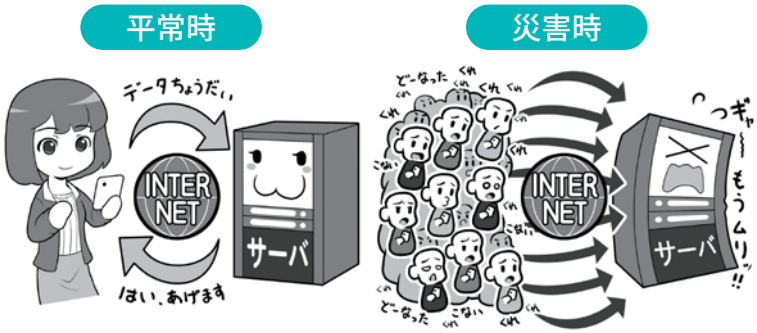
比較的近距離の範囲の放送をするテレビやFMラジオなどは、大震災時などに送信局や送信施設が自分の被災地域に含まれる可能性があります。しかし、一局で広範囲に電波を送信できるAMラジオや短波放送ならば、災害時に放送が中断する可能性がテレビやFMと比較して少なくなります。

これが災害用の持ち出し袋にAM放送を受信できるラジオを入れる理由でもあります。

トラブルに対しては、複数の手段で備えるのが基本ですから、普段は聴くことがなくても、災害用持ち出し袋にはAMラジオを入れることを検討しましょう。

また、車の中ならAM/FMのラジオ、一部は車載テレビでテレビ放送が受信できます。

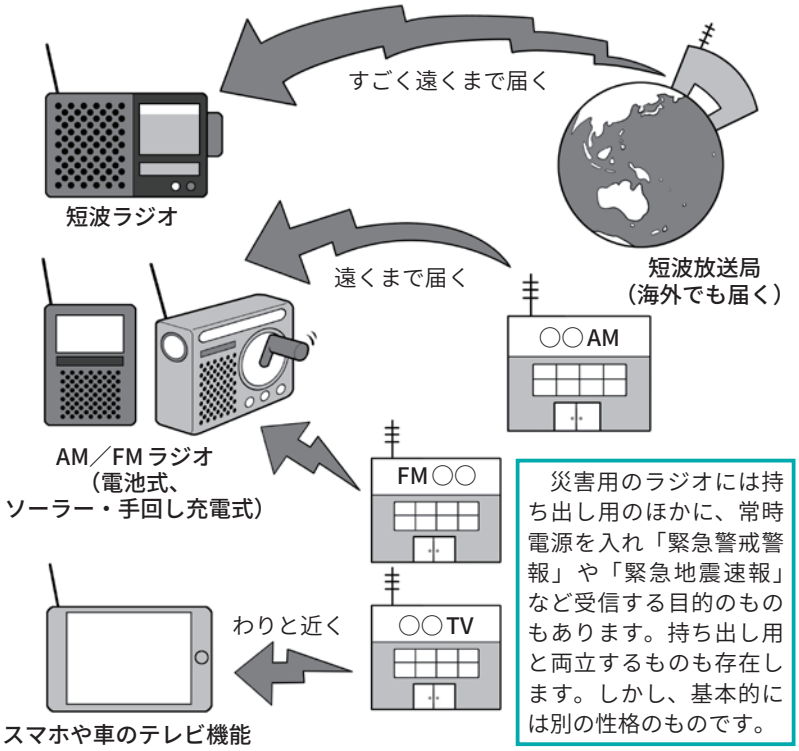
災害時のアクセス集中によるサーバの沈黙(双方向通信)



インターネットでは、私たちのリクエストにサーバが答えることで情報が表示可能になります。しかし、一気にリクエストが集中するとサーバの処理能力を超えるため、反応が返ってこなくなります。これがアクセス集中です。

災害時でも沈黙しないラジオやテレビ(片方向通信)

ラジオ・TVは一方的に送信できるので大丈夫



災害用のラジオには持ち出し用のほかに、常時電源を入れ「緊急警戒警報」や「緊急地震速報」など受信する目的のものもあります。持ち出し用と両立するものも存在します。しかし、基本的には別の性格のものです。

片方向通信の機器は、対応する受信機を持っているすべての人が受信可能です。FMやテレビは、放送局も被災して発信できなくなる可能性もありますが、AMはかなり遠くまで届くので、別の地域の放送を拾うこともできる場合もあります。短波に至っては海外まで届きますが、逆に地域別情報発信には不向きです。ラジオは消費電力が少なく、ソーラー充電や手回し式充電型も実用的です。なお、ワンセグTV搭載のスマホは少なくなりましたが、カーナビはフルセグテレビ受信可能なものもあることをお忘れなく。

4 徒歩帰宅、海外での災害やテロに備えて

災害時は、原則としては政府や各自治体・消防などの指示に従うべきですが、ときに徒歩帰宅をするという選択肢を取らざるを得ない場合もあります。スマホには、学校や仕事場から自宅までの道中、災害時に役立つ情報を掲載した帰宅支援マップやアプリを入れておくと役立つでしょう。日没時や降雨時の避難場所などもわかります。

また、その場合に備え、家族と落ち合う集合場所や、帰宅手順を話し合っておきましょう。長期大規模停電で通信できない状況まで想定して、プランを立てましょう。

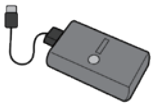
災害時には、スマホの電池が命綱になる場合もあるので、普段からACアダプター一体型のモバイルバッテリーや、車の電源を活用できるようにカーチャージャー、ケーブルなどを持ち歩きましょう。

海外での災害やテロに備える場合は、事前に外務省の「海外安全ホームページ」で渡航先の情報を確認し、渡航が推奨されない場所には行かないようにしましょう。

また、渡航前に外務省の海外安全情報配信サービス「たびレジ」に登録し、リアルタイムで渡航先の安全状況が把握できるようにしましょう。万が一災害が起こった場合に、緊急時の安否確認などがすみやかに行えるように、SMSでメッセージを受け取れるようにしましょう。「海外ではどういう風にデータ通信をするか」を前提に考えつつ、特にデータ通信しない場合でも、いざというとき、最低限上記のSMSメッセージは必要なんだと覚えておきましょう[*1]。

災害時に徒歩帰宅をする場合は

帰宅マップ


予備電池

ACアダプタ

USB
カーチャージャー

タブレット対応か
チェックする
（2Aなど）

災害時は政府方針で、最大3日（72時間）程度現地に待機を求められる場合もあるので、スマホなどの情報機器を使う場合、電池を持たす準備が重要です。ACアダプター機能付きのモバイルバッテリーの携帯や、車で充電できるようにUSB端子のついたカーチャージャーを必要に応じて携帯しましょう。また、自分の機器の充電に対応しているかもチェックしておきましょう。条件に合わないと充電できないこともあります（おもに2Aや2.1A対応と書かれている給電能力）。

海外での災害やテロに備える場合は

渡航前後に現地の情報を確認する

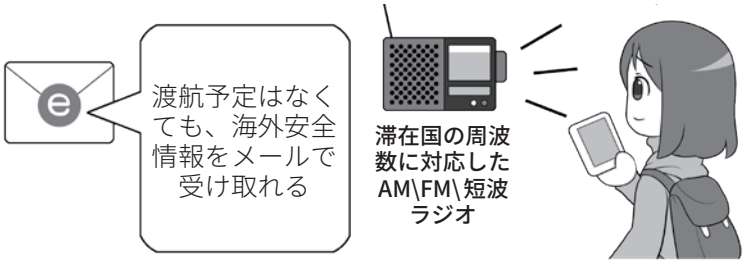
外務省海外安全ホームページもしくは外務省海外安全アプリをダウンロード

外務省たびレジに登録する

渡航時は外務省の「たびレジ」ウェブサイトで登録

緊急時はSMSで連絡

たびレジ簡易登録にメールアドレスを登録する



＊1：SMSは基本的には通常の携帯電話回線（インターネット電話ではない）を利用していれば、データ通信を利用していなくてもメッセージを受け取ることができます。

注）「外務省海外安全アプリ」では、約120ページの「海外安全虎の巻」が同梱されていたり、海外安全にかかわる外務省のウェブサイトなどを簡単に分類し、手早くアクセスできるようになっていたりするので、ぜひダウンロードしておきましょう。

コラム：情報の取り扱いは国によって異なる。要らぬトラブルに巻き込まれないように

インターネットは国境を越えて世界の人々を繋ぎ、理想的には皆同じ基準で、平等にその恩恵を享受できるべきです。しかし、現実的にそれぞれの国の中ではローカルルールによって、様々な制約を受ける場合があります。

訪問国のルールを理解せず、自国の常識でネットを利用などすると、思わぬトラブルに遭遇することもあるので注意が必要です。

ここでは、あなたが他国を旅行やビジネスで訪れると想定して、遭遇するトラブルを、あくまでフィクションとしてですが考察してみましょう。

1．入国まで

あなたがA国に訪れたいと考えました。ビザは免除されていますが、テロ対策の点から、事前に入国登録することが求められました。項目には「利用しているSNSアカウントを全て記入せよ」というものがありました。

これはSNSアカウントの書き込みから、テロを起こす過激思想を持っていないかを判断するために利用するようですが、日本ではちょっとした冗談の書き込みでも、A国ではそう受け取られず、入国を拒否されそうになりました。

入国したら、今度は入国審査で、利用しているスマホやパソコンのパスワードを開示せよと言われました。様々なウェブサービスのアカウントの分もです。書き出したものの一覧を見ると、係官は鼻で笑い、ロックを外された機器は別室に持って行かれ、コピーを取られました。あなたは長い間待たされたあげく、今度は取調室に呼ばれます。

そして、スマホに保存していた特殊な嗜好のマンガや写真の所持を指摘され、法律違反で逮捕され、起訴され、懲役判決を受けるかもしれないと言われました。私たちの国では問題無くても、そういったものが法律的あるいは宗教的に許されない国も、世界にはあります。

2．入国してから

やっとの事で入国することはできましたが、パソコンは没収されてしまいました。

スマホは戻ってきたものの初期化され、ローミングでの通信も著しく遅く通信に支障が出るので、値段も手頃だった、現地で販売しているその国の携帯電話会社のSIMカードを購入しました。代金はクレジットカードで支払います。

ところが、スマホを元の状態にリカバリーしようとアプリストアを見ると、普段使い慣れているエンドツーエンド暗号化のSNSのアプリがありません。そうやらその国では、使い慣れたSNSアプリが禁止されているようです。かわりにVPNを使おうとしたら、度々VPN機能がOFFになります。やっとの事で見つけた通信暗号化するメッセージアプリをインストールしたら、今度は通信ができなくなりました。

3．撮影していると…

携帯電話会社のお店に駆け込んで、通信ができなくなったといったら、別のSIMを買うことをすすめられました。仕方が無いので、再度購入します。

回線が復活したので観光に戻って、現地での様子でも写真で撮って送ろうと、車での移動中や観光地で撮影をして、日が暮れたのでホテルに戻りました。

夕食を終えて部屋でくつろいでいると、突然部屋に警察官が入ってきて連行されます。軍事施設を撮影した容疑で逮捕されたのです。そんな場所を撮影した記憶は全くないのですが、確かに撮影したと言われ、またしてもスマホを取り上げられました。

同行者が速やかに大使館に連絡をしてくれたので、数日後やっとのことで釈放されました。

4．日本の常識は通じない

取り調べの過程で所持品も色々と没収されてしまったので、足りないものを翌日配達のオンラインショップで買おうと、アカウントを取得しクレジットカードを設定し、不正利用が怖いので、SMS経由

でワンタイムパスワードを利用する二要素認証を設定しました。

翌日、家族に帰国の日程を報告するべくスマートフォンで電話しようとすると、また通じなくなっていました。

仕方ないのでホテルの電話で連絡し、準備を整えてチェックアウトしようとしたら、クレジットカードも使えなくなっていました。

クレジットカード会社に問い合わせすると、昨日利用したオンラインショップで、一度に多量の購入があったので、利用を停止したとのことでした。

二要素認証を設定していたのに、なんで使われてしまったか調べたところ、電話番号を乗っ取るSIMハイジャックと言う攻撃に遭っていたことが判明しました。

5．帰国してからも

なんとか帰国してからしばらくすると、クラウドサーバに上げていた、子どもの成長記録のうち、いくつかが勝手に削除されていることに気付きました。

写真の内容によっては、サーバが置かれた国のルールに従って、「児童ポルノ」と判断され、国際的に手配される可能性があるかもしれないという話もありました。

また、サーバに保管していた書類が流出した形跡もありました。その国では情報は検閲され、その過程で機密情報が流出することもあるようでした。

インターネットは世界を繋ぎますが、実状として、訪問した国のルールや物理的なサーバの所在国のルールが適用されます。

自国の慣習をそのまま持ち込んだり、よく考えずに利用したりせず、必ず調べてから利用しましょう。またクラウドサーバの所在地は必ず確認し、重要な情報は自国にサーバのあるサービスを利用しましょう。

要らぬトラブル

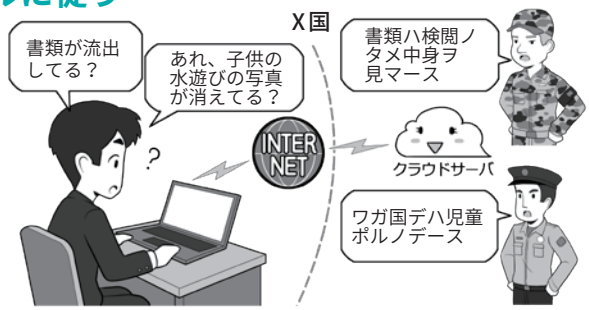
①自国で問題ない写真がアウトなことも

我が国の常識がそのまま外国の常識や法、宗教的規範に合致するとは限りません。そのルールに反すると、最悪の場合実刑を受けることもありえるのです。

②他国ではどこでも撮影していいとは限らない

また、軍事的にセンシティブな国では、関連施設にカメラを向けるだけで、スパイ容疑をかけられて拘束されることもあります。ルールを調べてから渡航しましょう。

③クラウドサーバのデータは所在地の国のルールに従う



クラウドサーバにあるデータは、サーバの実際の所在地や提供する企業のルールに従って、その内容が検閲され、その結果情報が流出する可能性もあります。要注意です。

コラム：デマに踊らされない！　ソースを探せ！　確かめよう！

昔からデマというものはありました。事件のときに拡散するものや、都市伝説のように長く語り継がれるものなど。

当時は、人から人への口伝えですから、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すが、その分「うわさ」ということを前提とした「不確かさ」「あやしさ」がありました。

ところが、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。その代わり、ネットではソースをたどることができますので、怪しいと思って調べると、元の発言をした人間が、発言を消して逃亡してたなんてこともあります。

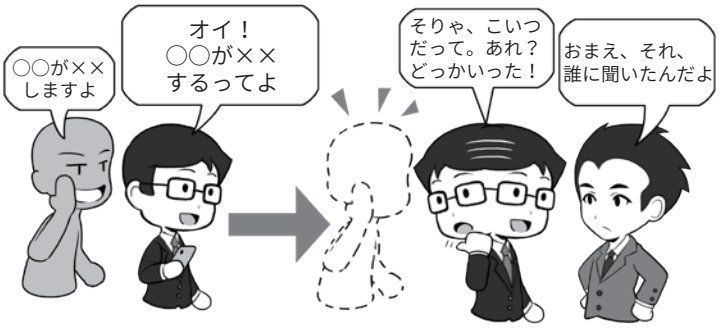
この構造は、「意図的なデマの拡散」にも使われます。デマになりそうな話題を使ったマルウェアへの感染誘導や、フィッシング詐欺を狙った釣りかもしれません。場合によっては、誰かを傷つけ名誉棄損となるものかもしれません。

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ってください。

そして、ほとんどの場合、後で冷静になって考えると、それはあなたが拡散する必要が、特にないものなのです。

それに災害時には本業の人ですら間違った発信をしてしまうミスもあるのでご注意を！

昔から出所が不確かなデマはあった

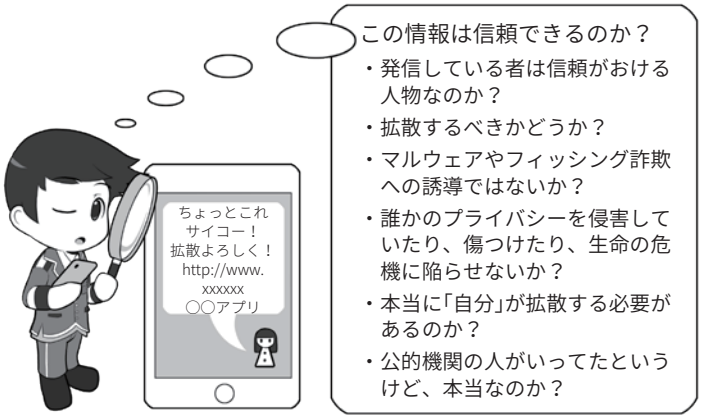


かつてのデマは、人間がしゃべるスピードでしか拡散しませんでしたが……。

ネットでは加速して飛び込んでくるが……

現在は、ネットの特性で「拡散数」を伴って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



コラム：災害時の情報収集について（本年の振り返り）

近年は、様々な自然災害が発生し、その中で様々なデマが飛び交い、正確な情報収集の難しさを浮き彫りにしました。悪意のデマではないとしても、不正確な情報の拡散も多く見受けられました。拡散する方々は善意で行っているのですが、情報源（ソース）がはっきりしないものの拡散は状況を混乱させます。物事の正確さ担保するためには、「現場」を知る責任がある方の「公式な情報発信」以外は、むやみに拡散するべきではありません。特に、「誰かに聞いた」という伝聞は、たとえそれが「通信会社の人に聞いた」「役所がの人が言っていた」というものでも、公式発表ではないかぎり、「不正確」である可能性が高くなります。「伝聞情報」には気をつけて、「本当に拡散するべきか」良く考えてください。

また、災害時の救助要請をSNSで行う方法が、広く一般に認識されたことが確認されました。これも本人、もしくや直接依頼された家族などの代理人が行うことは大変有効な手段ともいえますが、上記と同様に伝聞の情報を拡散したり、あるいは本人が救助された後も救助要請が残されたままだったりすると、それが一人でも多く助けようとする方の妨げにもなります。それ以外にもSNSの情報を見て、直接関係がない人が善意で電話での救助要請を行うなどのケースがあったようです。

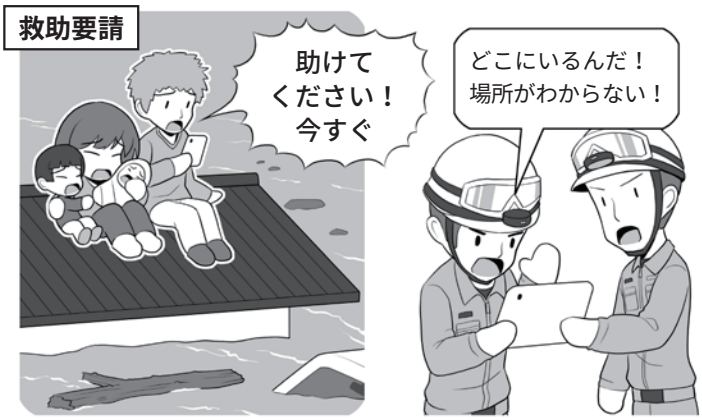
こういった情報は、本当に必要な情報収集への「雑音（ノイズ）」となる可能性があるので控えましょう。

また、最近は様々な災害時用のアプリが登場し、安否確認の方法も増えてきていますが、これらは連絡を取り合う人と、事前になにを使うか決めておかなければ意味を成しません。きちんと利用するサービスの確認をしておきましょう。

なお、2018年に北海道を襲った地震では、全道が長期間にわたって停電する事態が発生しました。携帯電話網もスマホも使えなくなる可能性が垣間見えた災害でした。そういった場合どういう手段で連絡を取り合うかも確認しておきましょう。

災害時の避難所などでは、自治体や電気通信事業者の取組により、無料で使えるWi-Fi「00000JAPAN」などが立ち上がることがありますが、このWi-Fiは接続しやすさを優先するため、暗号化されていないことを覚えておき、利用時はIDとパスワードの入力を避け、もし利用したい場合はVPNなど自前で通信を暗号化する知識を得ておきましょう。

災害時の救助関係発信はわかりやすく確実に



公的機関の災害時の窓口は、あくまでも110番119番の電話ですが、SNSで救助関係の発信をするときは、住所やGPS情報を付けましょう。

災害時は必要がない情報の拡散はひかえる

平成30年7月（西日本）豪雨時の不要不急拡散TOP3

…災害時に拡散しなくてもよいのでは？

5 ネットを使わない移動トレーニング（現代版オリエンテーリング）

災害時に、スマホの電池が切れてしまったり、あるいは旅行先でスマホを落としてしまったり、誰かに盗られてしまったりしたシチュエーションを想定して、スマホを使わずに自力で自宅に帰り着くためのトレーニングを、遠足のような遊びの一環としてチャレンジしてみましょう。

例えば、地図とコンパスやGPS受信機を持って、地図を読んで現在の場所を特定し、ハイキングルートを抜けて駅の場所を目指したり、駅に到着したら鉄道路線図から自宅までの経路を割り出したり、駅に設置されている時刻表をめくって自宅までの電車の時刻を書き出してみたりしましょう。

こういったことは、実はオリエンテーリングという野外スポーツのアレンジで、慣れると面白いゲームとして取り組むことができます。目的地を自宅ではなく、遠くの親戚の家へ訪問する機会にトライしてみるのもいいかもしれません。

地図が読めるようになると、コンパスがあるだけでも結構なんとかなるものですよ。

さて、最近はスマホになんでも記録できてしまうため、自宅の電話番号や家族の電話番号を覚えていないケースもあります。緊急に連絡を取る必要のある大切な番号は暗記して、公衆電話を見つけてコインやテレホンカードで電話をかける訓練をしてみましょう。公衆電話が見つからない場合は、お店などで聞いて探すところから始めるなど、いろいろなサバイバルを試してみてもいいでしょう。

ゲームとして帰宅サバイバルを楽しむ

地図の地形や記号などを読んで、現在地の特定にチャレンジしてみよう

ゲームとしていろいろなことにチャレンジしよう

GPS 情報からの現在地の地図の落とし込みや経路探索をしよう

電車の路線図を見て、自宅までの経路を決め、切符を買ってみよう

こういったことを経験しておくと、災害に遭ったときにスムーズに行動にすることができます。

大災害でもそんなことは起こらない？　いえ、こういったことは、どこまで「まさか」と思うことを想定できるかが、サバイバルの鍵になるのです。