

13 不正アプリやウイルスによる個人情報流出

占いアプリで趣味嗜好を入力し

大量の迷惑メールが届くようになった



いつも読んでいる情報サイトに掲載されていた無料の占いにアクセスしてみたPさん。生年月日や趣味嗜好を答えると、占いの結果が表示されました。



その後、Pさんのスマホには続々と広告のメールが届くようになりました。その内容は、Pさんが占いの時に入力した好みに合ったものばかりでした。

考えてみよう！

占いの他、ポイントが獲得できるアンケートなどもあります。入力した情報がどう使われるのか、想像してみましょう。

消費者教育

掲載したメルマガや情報サイトの運営会社が信頼できても、広告の内容が信頼できるとは限らない！

A. 興味を示す広告を送る

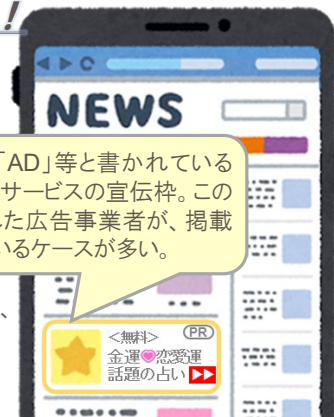
好みの情報が送られてくれば誰でも興味を示します。購入・利用をしてもらえそうな商品や有料サービスの広告メールを送るために、個人の趣味嗜好を集める会社もあるのです。

B. 大量のメールの中には・・・

大量のメール受信は、重要な連絡の読み落としにつながります。また、メール内のURL等をタップさせてパスワード等さらなる個人情報を抜き取るようとする業者もいるのです。

「PR」「広告」「AD」等と書かれている部分は商品やサービスの宣伝枠。このエリアを購入した広告事業者が、掲載内容を選んでいるケースが多い。

名前、生年月日、メールアドレス等を入力する際は気をつけて！



解説

個人に関する情報へのアクセス許可や入力欄には要注意

アプリやサービスを利用登録をするときなどに、個人に関する情報を求められることもありますが、中には必要ない情報を入力させる悪質なものもあるので要注意。氏名や住所、年齢、性別、メールアドレスなどが無断で二次使用されたり、業者に売られたりするリスクもあります。新しいアプリやサービスを利用する際は、評価を確認する、友人に聞く、保護者に見てもらうなど、複数の方法で安全性を確認し、公式ストアを利用しましょう。

また、ダウンロード時に表示される「このアプリにアクセス許可するもの」を確認し、そのアプリに不要な情報へのアクセス許可を求めているなど、少しでも不安があるときはダウンロードを中止するのが賢明です。

ワンポイント
アドバイス

無料のアプリやサービスは、安全なものばかりではありません。個人に関する情報を入力する前にしっかり確認するよう指導しましょう。

14 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



Qくんは、パスワードもいらず無料でネットに接続できる場所を近所に発見。家の電波が不安定なので、よくその場所に行ってネットをしていました。

通信内容が盗み見られてしまった



そのWi-Fiスポットは、他人の情報を盗むために悪意で設置されたものでした。Qくんの通信内容は、ずっと盗み見られていたのです。

考えてみよう！

Wi-Fiが自由に使える場所が増えていますが、ネットを使いたいという人の思いを利用した悪質なWi-Fiスポットもあります。安全に使うために気をつけたいことは？

A. 野良Wi-Fiのワナ

パスワードがいない無料Wi-Fiスポットの中には、悪意で設置されたものもあります。判別が難しいため、個人情報の入力等、悪用されて困る情報のやり取りをしないよう注意しましょう。

B. 接続前に安全性の確認を

安全性の低いWi-Fiスポットがリストの最初に表示されることもあるので、名称や鍵マーク🔒等の確認を習慣にしましょう。普段よく使うWi-Fiサービスを登録しておくと、より安心です。

C. いざ！という時のために

緊急災害時、携帯電話会社の電波が使えなくなることもあります。通学路や自宅近くで安全なWi-Fiを提供している場所をいくつか知っておけば、命をつなぐことに役立ちます。

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。名称、鍵マークやWi-Fiステッカー※等でどのようなWi-Fiスポットであるかを確認しましょう。

スマホやゲームをしたくてパスワード不要の無料Wi-Fiを探す子もありますが、通信傍受やID・パスワードなどを盗むために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接続設定が自動になっていると、悪意の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。

ワンポイントアドバイス

Wi-Fiスポットの中には、悪質なものや安全性の低いものがあることも。外出先で利用するなら、名称や鍵マークの有無等を必ずチェック！

15 ゲーム上でのやり取りから生じたトラブル

他人にIDとパスワードを教えてしまい



Rくんは、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、「ポイントいる？」というメッセージが届きました。

パスワードを変更されゲームを乗っ取られた



ポイントもらえるなら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。ゲームのアカウントを乗っ取られてしまったのです。

考えてみよう！

文字や音声でやり取りしながら楽しむゲームもいっぱい。だからこそ気をつけたいことを、話し合ってみましょう！

A. 甘い誘いはワナの可能性が

IDを乗っ取るため、パスワードを知ろうとする悪い人がいます。聞かれても答えただけでなく、ゲームでのやり取りから推察できるパスワード(例:好きなアイドルやペットの名前)はNG！

B. ボイスチャットはさらに注意

プレイ中、音声で仲間と会話できるゲームがあります。マイクの性能も上がり、周囲の会話が相手に聞こえてしまうことも。個人が判る情報が伝わらないよう、家族で考えてみましょう。

消費者教育

年齢に合ったものを選ぶ

市販のゲームソフトやゲームアプリには、『対象年齢』があるのをご存知ですか？

↓市販のゲームはパッケージに記載



内容や遊び方等を基準に定められたもの。購入・ダウンロードの前に、必ず確認を！

解説 ゲームでのトラブルは高額課金以外にもいろいろ

高額課金を心配する声は多いようですが、ゲーム会社ごとに定めた年齢層に応じた課金の上限設定(例:中学生以下5千円/高校生1万円)や、プリペイドカード等を上手に活用しましょう。また、ゲームやSNSのID・パスワードの悪用による被害への注意喚起も必要です。アカウントを乗っ取られる、ポイントやアイテムを奪われる、クラウド保存した写真を盗み見られるなど、被害はさまざま。親しい人でもID・パスワードを教えるはダメ、他人のID・パスワードでのログイン(不正アクセス禁止法違反)もダメということをしっかり教えましょう。

対象年齢に満たない子のトラブルも増えています。どんなに興味を示しても、対象年齢までガマンが大事です。

ワンポイント
アドバイス

乗っ取ったIDでその人になりすまし、知り合いをだますようなトラブルも増えています。自分のうっかりが、周囲に迷惑をかけることも忘れずに。

16 旅行中の写真投稿や書き込みによる空き巣被害

旅行先から写真をアップしたら



夏休みに、家族旅行に行ったSさん。仲良しへの暑中見舞いを送る代わりに……と思い、**旅先から写真やメッセージを自分のSNSに投稿**しました。

自宅が空き巣に荒らされていた



帰ったら、家の中がグチャグチャ！留守にしている間に空き巣に入られてしまったのです。**投稿内容から不在が知られてしまい狙われた**とのことでした。

考えてみよう！

日常の出来事や楽しい思い出を、仲良しと共有したいと思う人も多くなりました。**投稿内容が予想外のトラブルに発展しないために、どんな工夫ができますか？**

A. 公開範囲に気をつける

非公開のグループトークや、SNSの非公開アカウントを賢く活用すれば、許可した人だけしか読めないのが安心。ただし、「勝手に他所に転載しない！」を全員で守ることが重要です。

B. 内容やタイミングをぼかす

「いいね」が欲しくて公開する子に、とがめるだけでは効果なし。個人が特定される危険も考え、スタンプやボカシをうまく使う、公開は帰った後に、というような工夫をいろいろ考えましょう。

C. 悪い人の目線で想像する

留守だとわかれば空き巣に、ブランド小物を毎日持ち歩くとわかればひったくりに、etc...何が伝わると誰に狙われるか、あれこれと想像してみることもトラブルの予防に役立ちます。

解説

誰でも読めるSNSへの投稿内容は、犯罪に利用されることも

夏休み、お正月、ゴールデンウィーク……旅行にでかけることも多い長期休暇や連休ですが、**リアルタイムでSNSに投稿すれば、「今、自宅は誰もいません！」と留守を公言しているようなもの**。メッセージアプリのタイムラインへの投稿も同様、友だち限定にしていなければ誰でも読むことができますので要注意です。

SNSがきっかけの空き巣被害も深刻ですが、「一人で留守番」が憶測できる投稿も危険。**何気ない投稿が取り返しのつかない事態を招かないよう、送信前に必ず読み返す習慣をつけましょう**。また、非公開設定でも読んだ人のうっかりで人目にさらされることも。誰が読んでもいい内容に留めるのが、一番安全な方法です。

ワンポイント アドバイス

自分の投稿が、悪い事をしようとする人の目に留まることだってある。これを意識できるようになれば、安全確認をする子も増えるはずです。

17 投稿から個人が特定されたことによる被害

おいしい情報をシェアするつもりが

知らない人に付きまといられるようになった



よく行くショッピングタウンでお気に入りのお店を見つけたTさん。親しい人たちに教えてあげようと、**位置情報オフで撮影した写真を投稿**しました。

その後、誰かに後をつけられていることに気づきました。引き金は、Tさんが投稿した**写真の背景**。**場所がわかり生活範囲が特定**されてしまいました。

考えてみよう！

アップした写真から、撮影場所や生活範囲が知られてしまうことも。事件やトラブルに巻き込まれないために、写真投稿の際に注意しなければならないことは？

A. 指紋さえわかる高画質

カメラの性能が高まり、ピースサインで指紋が判別されることもあるとか。電柱や看板の文字が読めたり、瞳に映ったものが見えたりする可能性も。これまで以上の注意が必要です。

B. 読める人を想像して投稿

一番の安全策は、プライベートな情報をネットに載せないこと。とはいえ、情報のシェアは悪いことではありません。投稿前によく見直し、非公開設定にして特定の人とだけ共有する等の危機管理を！

C. もしも不安を感じたら

自分のサイトに気になる投稿があった、知らない人に突然名前呼び止められた、他、不安を感じたときは必ず大人に相談すること。できるだけ、誰かと一緒に行動しましょう。

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

子供・若者は、SNSなどを利用する際の個人情報の取扱いにルーズな傾向があります。メッセージアプリのタイムラインで、定型の質問に答えながら次の人へと回す「バトン」をする等、**公開範囲設定をしていなければ、直接の友だち以外の人まで読めてしまい、トラブルに発展**することも。そもそも、誰でも見ることができるのがSNSの基本。写真に映り込んだものから、**訪れた店や地域など生活範囲が推測できるため注意**が必要です。

①友人同士でも個人情報は安易に答えない・回さない、②ネットで少し話して登録した友だちは、タイムラインを非公開にする、③非公開で得た情報は勝手に再投稿やスクリーンショットをしない、ことに気をつけましょう。

ワンポイント アドバイス

コミュニケーション系アプリの多くは、読んでもいい人の設定ができます。**公開範囲を絞り、共有したい写真を確認することが、何より大切です。**



18 自画撮り写真の交換に端を発した脅迫被害

同性のステキな友達だと信じていたのに



好きなアーティストの話題で意気投合した同じ年のUさんと直接やり取りを始めたVさん。やがて、誰にも言えない秘密も打ち明けられる仲になりました。

写真を送ったら態度が急変、脅迫された



Uさんの写真が届き、嫌われたくなくて自分の写真を返信した途端、写真付きで秘密をネットに拡散されたくなければ裸の写真を送れと脅されました。

考えてみよう！

優しい言葉で相手を油断・信用させ、個人情報や写真入手して「ネットにばら撒く」「学校に知らせる」などと脅す。こんな被害にあわないために、できることは？

A. 善人は違法な要求をしない

好奇心を満たす目的で18歳未満の子の裸や下着姿の写真を持つことはダメ。「裸の写真を撮って送って！大切にすることから」は、違法行為をしようという意味だと判断しましょう。

B. 情報の組み合わせに注意

フォロー相手や友達との会話から名前や学校名が知られてしまうと、顔写真でも脅しのネタになる可能性が！ネットだけの知り合いに、秘密や内緒ごとを打ち明けるのはとても危険です。

C. 深みにはまってしまう前に

SNSのやり取りでは、ウソの書き込みや写真の偽装ができるので、目に見える情報を簡単に信用しないこと。一度送ってしまえば取り戻せないことを忘れずに、困ったら迷わず大人に相談を！

解説

言葉巧みに近づく人、見える情報だけで判別するのは不可能

政府インターネットテレビでは、実際の事件を基にしたドラマ仕立ての動画を公開しています。悪意ある大人の巧妙な手口を、動画で疑似体験できますので、ぜひ参考にしてください。

自画撮り被害児童のほとんどは中高生。仲良くなりたと思わせて個人情報を聞き出し、写真を送らせて脅す手口の一部始終を、じっくり考えながら視聴し、時間をかけて真剣に話し合ってみましょう。

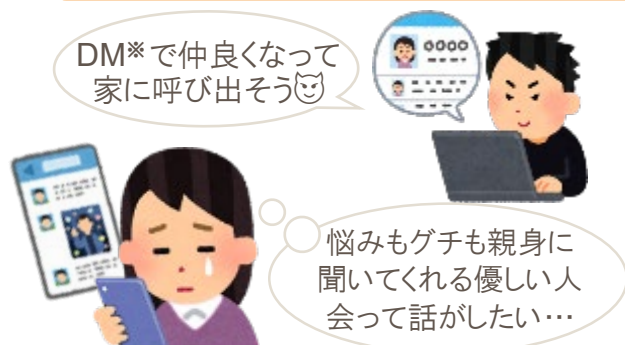


ワンポイントアドバイス

「自分だけは大丈夫」と思って注意を怠ることが一番危険！
”直接”写真をやり取りしない＆秘密を話さない。これが安全の鍵です。

19 心のよりどころだったSNS上の知人による誘い出し

ネットで出会った相談相手に会いに行き



※ DMは「ダイレクトメッセージ」。複数の人たちとやり取りする画面を介さず、個人と直接やり取りできるメッセージのこと。

辛いことが続き、SNSにつぶやいていたWさん。
気持ちが落ち着くメッセージをくれる人に出会い、
DMでやり取りするうちに、会いに行くことになりました。

そのまま連絡がつかなくなってしまった



出かけたきり家に帰ってこなくなり、家族が警察に相談。誰にも言わずに会いに行ったことは、WさんのSNSの記録を確認して初めてわかったのです。

考えてみよう！

ネットだけの交流では、顔、姿、気持ち、メッセージ、どれも本物かどうかわかりません。それなのになぜ、ネットで知り合った人を信じたり頼りにしたりしてしまうのでしょうか？

A. 本当は誰に聞いてほしい？

- 気持ちを察してくれる友人
- じっくり話を聞いてくれる家族
- 何でも相談したいと思える先生がいてもネットで相談しますか？身近にいる誰かに目を向けて、心の内を話してみては？

B. 知らない人のほうが便利？

自分を直接知っている人と、ネットだけでやり取りしている人。優しい言葉をかけられて嬉しいのはどっち？ ネットなら余計な詮索をされずに済み、都合がいいだけではありませんか？

C. どうしてもSNSを使うなら

本当に親身になってくれる人もいますが、上辺だけの人も山ほど。どうしてもSNSに頼りたいのなら、「深入りはしない」「DMを警戒し、個人的なやり取りはしない」を徹底しましょう。

解説

成長過程で生じる不安定な感情につけこまれる危険

多くの子供がSNSを活用し始めるのが、仲間との関係が大事で、悩みもモヤモヤすることも多い思春期の頃。感情の行き違いはしばしば起こり、辛さやイラ立ち、「大人はわかってくれない！」など、リアルな生活で受けたストレスをネットにぶつけることで自分の気持ちをコントロールしようとする子も少なくありません。

でも、そんな心理状態や判断の甘さを知って、近づいてくる危険な大人もいます。ネットの向こうにいたのが悪い人かもしれないことを知りつつ、リスクよりもそのときの感情を優先しがちな時期。ネットで知り合った人に深入りしないよう「ここまで！」の限界を話し合い、意識して使うことが危険回避の第一歩です。

ワンポイントアドバイス

ネットの向こう側に救いを求めたがる時期。子供の言葉に耳を傾け、気持ちに寄り添い、相談できる関係を保つことが最善の予防策です。

20 SNS等での^{ひぼう}誹謗中傷による慰謝料請求

有名人の悪口を匿名で投稿したら

発信者が特定され高額な慰謝料請求へ



テレビやネットでの言動が気に入らない有名人の悪口を匿名投稿したW君。同調する投稿も増え、根拠のない悪口など嫌がらせがネットに広まった。



W君が発信者だと判明したことから、虚偽の投稿内容により名誉を傷つけられたとして、慰謝料などを求める訴訟(裁判)を起こされてしまった。

考えてみよう！

一緒に考えてみよう！ インターネットトラブル事例集2020年版

③メッセージアプリでの悪口・仲間外れ



いら立ちを覚えたり、自分の中の正義感が高じたりして、過激な投稿で個人攻撃をする人がいます。こうした加害行為(再投稿*も含まれる)をしないために注意したいことは？

※再投稿：共感したり気に入ったりした情報をそのまま投稿して他者に広める行為。サービスにより「リツイート」「リグラム」「リポスト」他と称される。

A. ^{ひぼう}誹謗中傷 ≠ 批判意見

多くのSNSサービスには「誹謗中傷禁止」という利用規約があります。相手の人格を否定する言葉や言い回しは批判ではなく誹謗中傷です。正しく見極め、安易に投稿・再投稿をしないで。

B. 匿名性による気のゆるみ

対面や実名では言えないのに、匿名だと言えたり攻撃性が増したりすること。たとえ匿名でも、技術的に投稿の発信者は特定できるため、民事上・刑事上の責任を問われる可能性が...

C. カツとなっても立ち止まって

怒りは人の自然な感情ですが、はけ口にされやすいのがSNS。炎上したり訴えられたりしてから「あんな投稿しなければよかった」と悔やんで時間は戻せません。書いた勢いで送信しない習慣を！

解説 「目立つ存在なんだから仕方がない」という主張は通用しない

SNS上で、悪意を感じる投稿を見かけることがあります。中には「正義感からやったこと」と主張する人もいますが、“立場”や“事実かどうか”を問わず、人格を否定または攻撃するような投稿は正義ではありません。

近年、YouTuber、事件・事故の関係者、感染症の陽性者ほか、『有名な人』と感じる範囲が広がると共に、主体的に投稿する人以外の“安易に再投稿・拡散する人”も増えています。たくさんの悪口が集まれば、集団攻撃となり人を酷く傷つけます。相手がどのような人であっても、単に再投稿しただけであっても、**民事上・刑事上(損害賠償請求、名誉毀損罪による懲役、侮辱罪による拘留等)の責任を問われる可能性があります。**このことを肝に銘じて、法律や利用規約等のルールやモラルを意識した、正しい利用を心がけましょう。

ワンポイント アドバイス

^{ひぼう}誹謗中傷は、再投稿者でも“広めることに加担した”とみなされます。投稿・再投稿する前に必ず「自分が言われたらどう思うか」を考えて！

特集 「ネットで知り合う人」とのやり取りについて

① 真剣に考えてみよう！



SNSなどのコミュニティサイトを介したやり取りには楽しさだけではなく、“危険”もいっぱいです。最近では、SNSのやり取りに端を発した誘拐事件や生命に関わるような凄惨な事件も起きています。

特にDM(ダイレクトメッセージ)*によるやり取りは、本人にしかわからないことから、犯罪に巻き込まれるなどの被害が後を絶ちません。「被害にあう人が特殊なだけ、自分は大丈夫」と油断しないことが重要です。自分を守るために、次のようなことを心がけましょう。

※ DM(ダイレクトメッセージ): 複数の人たちとやり取りする画面を介さず、個人と直接やり取りできるメッセージのこと。

自分を守るためにできることは？

1. 日ごろよく使うSNSの“プライバシー設定”を行いましょう



- アカウントの公開・非公開
- 自分がDMを受け取れる人の範囲設定
- 自分の投稿を読んでいい人の範囲設定
- 自分の画像へのタグ付けに関する許可設定

などのほか、プライバシーやセキュリティに関する設定を確認しましょう。もしもアカウントが複数あるなら、それぞれの用途に合う設定を行い、使い分けの徹底を！（機種変更等の際は設定を再確認しよう）

2. SNS利用の「ここまではOK」「ここからはNG」を決めておく

（DMのやり取りはしない、個人的なことは発信・投稿しない等、以下を参考に）

- いつも発信しているアカウントには、**深刻なこと、プライバシーに関することは、書き込まない**
- SNSで話をした人から急にDMが届いたら「ありがとう、あとはSNSで！」と返すなど、**DMを断ち切る**
- 時間が経つほど断りづらい！イヤなこと、不安なことで「どうしよう…」と**迷ったら、すぐ＆ハッキリ断る**
- しつこく誘われたり脅されたりしても、**決して応じず、独りで抱え込まず、身近な大人に相談する**
- 周囲に相談しづらいとき、相談できる人がいないときは、**勇気をもって警察や専門の窓口*に相談する**

3. ネットだけに頼らずリアルな解決法も大事にしよう

イライラした時は、
スマホを置いて深呼吸
音楽を聴く、好きなことをする等
気分をかえてみるのもオススメ！



溜まっているモヤモヤ・イライラを
ノートにどんどん書いて、
声に出して言って、
吐き出してみることも効果アリ



悩んでしまった時のために
時間を決めておいて、
その時間を過ぎたら
それ以上悩まず寝てしまう Zzz



家族や先生
心を許せるリアルな友人
などに相談してみても？

* 地域や学校の「SNS相談窓口」があれば、それも活用してみよう！



※ 下記URLより『各種相談窓口』（内閣府：ネットの危険から子供を守るために）をご参照ください。

▶ https://www8.cao.go.jp/youth/kankyau/internet_use/soudan.html



消費者トラブルに巻き込まれないために ～消費者としての知識を身につけよう～



成年年齢の引き下げにあたって

2018年6月の民法改正により、2022年4月より成年年齢が18歳に引き下げられます。これに伴い、若者がひとりで取引を行う機会が増えること等により消費者被害に遭う危険性の増大が懸念されています。

このような中で、さまざまな**消費者トラブルに巻き込まれないよう**、「**大人**」になるまでに**消費者としての知識を身につけていくことは一層重要**になっています。

「インターネットトラブル事例集」の活用

消費者トラブルに巻き込まれないようにするためには、サービスの内容や契約の条件をよく確認すること、自分にとって必要な商品を適切に選んで購入すること等が重要です。本事例集では、インターネットに関する消費者トラブルの事例を具体的にいくつか紹介していますので、これらを素材に、消費者として必要な知識や考え方を身に付けることができます。

本事例集にある次の事例の  **消費者教育** マークが付された箇所を中心に確認してみましょう。

- | | |
|---------------------------|-----------------------|
| ⑤ フリマなどネットを介した直接取引によるトラブル | ⑥ SNS経由のチケット転売による詐欺被害 |
| ⑨ 他者の権利を侵害する投稿や視聴 | ⑬ 不正アプリやウイルスによる個人情報流出 |
| ⑮ ゲーム上でのやり取りから生じたトラブル | |

電気通信サービスの契約における注意点

様々なサービスの中でも、**電気通信サービスはその内容が複雑であり、特に注意が必要**です。



インターネット回線(光ファイバーやプロバイダ)などの電話勧誘に注意！

契約は口頭でも成立するので、会話に気をつけないと危険。**勧誘が強引だと感じた場合は、はっきりと断りましょう。**また、大手の通信事業者を名乗る違法な勧誘もあるので、有名な事業者名を聞いただけで安心して契約をしないよう、注意しましょう。



利用状況や目的に合った通信サービスを選びましょう

料金や通信速度等の通信サービスの内容は、多種多様です。一見、月額料金が安いように見える場合であっても、一定の条件下でのみ割引される場合もあります。**料金プラン等をよく確認して、自分に合った通信サービスを選びましょう。**



もし間違えて契約してしまった場合等には ～初期契約解除制度～

いわゆるクーリングオフに似た制度として、携帯電話サービス、光回線サービス等の一定範囲の電気通信サービスには、契約書面の受領日等を初日とする**8日間が経過するまでは、利用者の都合で契約を解除できる『初期契約解除制度』があります。**

消費者教育
ポータルサイト



本事例集のほか、消費者庁が運営する「**消費者教育ポータルサイト**」には、教材や講座などが満載。ぜひ参考にしてみてください。

▶ <https://www.kportal.caa.go.jp/index.php>



「おかしいな」「困った」「だまされた」と思ったら、迷わず、すぐに相談しましょう！

消費者ホットライン **188**

または **最寄りの警察へ**



その情報、ホント？ウソ？

ネット上には、人を混乱させるためにわざと流されたデマ情報も。
身近な医療健康情報、うわさ話やゴシップネタなどにも、間違った情報がある！

どのようなメディアでも、間違った情報が流布されることはあり得ます。

特にSNSの場合、誰もが容易に情報発信できることから、正しくない情報もたくさんあります。中には、騒ぎを起こすことが目的で発信されたデマも。目にした情報をうのみにせず、正確性が判断できない場合には安易に情報を投稿・拡散しないことが大切です。



SNSでは知らず知らずのうちに……

そもそも私たちには、自分が信じたいものを信じる、大勢の人が選ぶものを選ぶ、という特徴があります。また、**SNSや検索エンジンでは、以下のような2つの現象が起きがち**で、情報が偏る可能性もあるのです。

エコー
チェンバー

自分と似た考えの人ばかりが
集まるようになってしまった

フィルター
バブル

自分の好み以外の情報が自動的に
はじかれるようになってしまった

自分と似た意見や、知り合いからの情報はつい信用してしまいがちですが、自分に都合が良くても悪くてもうのみにせず、拡散する前に立ち止まって考えてみましょう。デマやフェイクニュースにだまされないように、普段から多様な情報に接することも重要です。

再投稿・拡散する前に気をつけよう！

☑ 他の情報と比べてみる

ネット検索し、複数の情報を読み比べましょう。本や新聞など、ネット以外で調べるのもお勧めです。

☑ 情報の発信元を確かめる

発信元が明らかであっても、信頼できる人なのか、信頼できるWebサイトなのかを確認しましょう。

☑ その情報はいつ頃書かれたものか確かめる

古い情報だった場合、現在とは状況が異なるかもしれないので、注意しましょう。

☑ 1次情報を確かめる

その情報が引用や伝聞の場合、オリジナルの情報源を確かめてみましょう。

特集 ころ・からだ・いのちを守るために！

④ SNSによる^{ひぼう}誹謗中傷被害への対処方法



**SNS上で言い争ってしまうと、さらに悪化してしまう可能性もあります。
設定を見直す、信頼できる人・窓口相談する等、冷静に対処しましょう！**

炎上投稿に直接参加する人は、ごく限られた一部に過ぎないという研究結果もあります(令和元年版 情報通信白書)。
「**誹謗中傷は多数意見ではない**」「**世の中の人全てが攻撃しているわけではない**」ということ、思い出してください。
それでも、もし、保護者・先生・友人には相談しづらいと思ったときは、専門の窓口を積極的に利用してください。

その①

**ミュートやブロック
等で距離を置く**

とりあえず“見えなくする”設定に

よく使われるSNSには、やり取りをコントロールする機能が備わっています。**相手に知られずに投稿を非表示にする機能(ミュート)**をうまく活用しましょう。**つながり自体を断つ機能(ブロック)**もありますから、深く傷つく前に「見えなくする」ことをお勧めします。

また、**返信やコンタクトができる相手を制限できる機能**もあります。それぞれ、名称や操作方法等はサービスやアプリによって異なります。調べて確認しながら使ってみてください。



**攻撃しているのはごく一部だと
分かっている人も人は傷つきます。まずは
できることからやってみましょう**

その②

**人権侵害情報の
削除を依頼**

削除依頼の流れ



- ① 可能な状況であれば、投稿者に削除してほしいと連絡してみる(無理は禁物)
- ② 該当する投稿のURLやアドレスを控える【画面(=スクリーンショット)や動画の保存も重要】
- ③ 「通報」「報告」「お問い合わせ」など削除依頼等ができるページやメニューを探す
- ④ フォームに従って必要な選択・入力を行い漏れがないか内容を確認して、送信！



発信者の特定も可能 ミュートやブロック、削除依頼だけでは解決しない場合、匿名の発信者を特定して、損害賠償請求などを行うことも可能です。発信者開示請求を行いたい場合は、弁護士にご相談ください。

困ったら、傷ついて辛かったら、1人で悩まず相談を！

その③

**信頼できる機関
に相談する**

電話、メール、各種SNS、Webチャット等を使って、誰にも知られずに相談することができる公的窓口はいろいろあります。**1人で抱え込まず、相談してみましょう。**

- インターネット違法・有害情報相談センター <https://www.ihaho.jp/> (総務省支援事業)

専門の相談員が、誹謗中傷の書き込みを削除する方法などについて丁寧にアドバイスします。ご自身で削除依頼を行っていただくための迅速な対応が可能です。

- 法務省「インターネット人権相談窓口」 <https://www.jinken.go.jp/>

法務省の人権擁護機関(法務局)ではインターネットでも人権相談を受け付けています。削除依頼の方法について相談者に助言を行うほか、内容に応じて、法務局からプロバイダに削除要請を行います。

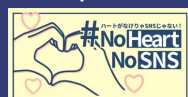
- 厚生労働省「まもろうよ ころ」 <https://www.mhlw.go.jp/mamorouyokokoro/>

もしもあなたが悩みや不安を抱えて困っているときには、気軽に相談できる場所があります。電話、メール、チャット、SNSなど、さまざまな相談窓口をご紹介します。



- 『インターネットトラブル事例集(2020年版)』は、総務省ホームページで公開中。

http://www.soumu.go.jp/main_sosiki/joho_tsusin/kyouiku_joho-ka/jireishu.html



- ハートがなければSNSじゃない! 『#NoHeart NoSNS』特設サイト <https://no-heart-no-sns.smaj.or.jp/> も、併せてご活用ください>>>



スマホの設定、うまく使いこなせていますか？

フィルタリングは青少年を違法・有害情報との不用意な接触から守り、安心・安全にインターネットを利用する手助けをするサービスです。例えるなら、ネットの世界に漂う「見えない危険」から身を守るための“マスク”。冷静さを欠いたアクセスに適度なブレーキをかけるだけでなく、見た目ではわかりづらい悪意の仕掛けがあるサイト等へのアクセスを防いでくれる頼もしいツールです。(SNSに起因する犯罪被害児童の9割以上がフィルタリングを設定していなかったというデータもあります／警察庁調べ)

現在は携帯電話事業者をはじめ各社がフィルタリングサービスを提供しており、**年齢や家庭のルールに応じてカスタマイズすることも可能**です。



18歳未満が使用する端末へのフィルタリング設定は法律上の義務

青少年インターネット環境整備法*では、格安スマホ事業者(MVNO)を含む携帯電話会社とその販売代理店には、新規の携帯電話回線契約時および機種変更・名義変更を伴う携帯電話回線契約の変更・更新時に、次のような義務が課せられています。

青少年確認

契約締結者または携帯電話端末の使用者が18歳未満かどうか確認する

フィルタリングの説明

- ・青少年に有害な情報の閲覧による危険
- ・フィルタリングの必要性和その内容について保護者又は青少年に説明する

フィルタリング有効化措置

契約とセットで販売される携帯電話端末等について、販売時にフィルタリングソフトウェアやOSの設定を行う

* 青少年が安全に安心してインターネットを利用できる環境の整備等に関する法律（平成21年4月施行／平成30年2月改正法施行）

使用する端末に合ったフィルタリングの選択・設定を！

安全な利用環境づくりの基本は、Webとアプリの両方に正しい設定をすること。スマホやタブレットのOS、契約する携帯電話事業者等によって、利用可能なフィルタリングサービスが異なるので、以下の一覧表を参考にしながら、子供が使用するスマホやタブレットに合ったフィルタリングサービスを使いましょう。

スマホのOS 携帯電話事業者	Android		iOS	
	Web	アプリ	Web	アプリ
ドコモ、KDDI(au)、ソフトバンク・ワイモバイル	あんしんフィルター※1		あんしんフィルター	※2 スクリーンタイム 〔iOS11以前では 『機能制限』〕
その他の携帯電話事業者 〔いわゆる“格安スマホ” “格安SIM”の事業者等〕	各事業者が提供するフィルタリングサービス もしくは、各種フィルタリングアプリ等※3			

※1 Android端末の一部の機種では、あんしんフィルターではなく、OSの機能や他のアプリ(例:Googleが提供しているファミリーリンク)等を使用する必要があります。購入もしくは機種変更の際にご確認ください。

※2 iPhoneやiPadは、基本的にあんしんフィルター等のフィルタリングアプリで制御できるのはWeb接続のみとなります。アプリに関するコントロールについては、Appleが提供しているスクリーンタイム等を使用する必要があります。

※3 「iフィルター」等のフィルタリングアプリ、もしくはフィルタリング機能が備わっているセキュリティアプリが利用可能。なお、これらアプリは、あんしんフィルターが使えるスマホや契約の切れている古い機器等にも導入・活用できます。

～フィルタリングや時間管理等で上手にコントロール～

「ペアレンタルコントロール」でできる安全な利用環境づくり

子供の安全のために**保護者がネット利用環境を整えてあげることを「ペアレンタルコントロール」と言い、その代表が「フィルタリング」**です。個別に利用を許可するカスタマイズ機能や、長時間利用を防ぐ時間設定機能など、**本体設定やアプリでできるペアレンタルコントロール機能はいっぱい**。目的に応じて柔軟に活用しましょう。（年齢が高くなれば、自分の力で利用をコントロールするためのツールとしても役立ちます）

有害なサイト等へのアクセスやアプリの利用を制限したい

簡単に設定したい

モード設定を活用しましょう。

（以下のカテゴリ名は一例です）

フィルタリングサービスやアプリには、「小学生モード」「中学生モード」などの学齢等によるわかりやすい推奨モードが設けられています。設定はそれらを選択するだけ。学齢に沿ったある程度のインターネット安全利用環境が整います。

小学生	中学生	高校生	高校生+
ファミリーゲーム	ファミリーゲーム	ファミリーゲーム	ファミリーゲーム
一般ゲームなど	一般ゲームなど	一般ゲームなど	一般ゲームなど
懸賞など	懸賞など	懸賞など	懸賞など
SNSなど	SNSなど	SNSなど	SNSなど
出会いなど	出会いなど	出会いなど	出会いなど

キメ細かく設定したい

カスタマイズ機能を活用しましょう。

アプリ（またはカテゴリ）の単位で閲覧や使用の可否を個別に設定することができます。

サービスA ☒
サービスB ☐

iOSのアプリ制限等では、学齢ではなく年齢区分（4+、9+等）で設定する場合があります。

↑年齢区分の『数字+』は「〇歳以上」を表しています。

うちの子は
小4だから9+ネ!

中学生は12+か!

「長時間利用」を防ぎたい

利用時間設定で、スマホやアプリ等が利用できる時間（長さ）や時間帯を設定することができます。

課金や位置情報ほか

サービスやアプリによって様々な設定があります。目的に合わせて活用しましょう。



組み合わせるとこのような使い方ができます！

スマホを使い始めたばかり。
安全な環境を保ちつつ、家族との
連絡用のSNSだけは使いたい!

まずは、年齢に合った（または
年齢より低い）モードを選択して
多めに制限をかけます。そして
カスタマイズ（個別設定）機能で
保護者が特定のSNSのみ使用
許可をする方法がお勧めです。

基本は自由に利用しつつ
ゲームの利用時間だけは
しっかりコントロールしたい!

高校生モード等、高めの学齢
のモードを選択した上で、利用
時間を設定できる機能を使う
方法がお勧めです。

利用時間や課金等について
家庭のルールを設けて
上手な活用を身につけたい!

話し合ってルールを決めたら、
目につくところに掲げ、各種調整
ツールや設定を上手に使う方法
がお勧めです。レポート機能を
活用することで、
使い方を見直し
などもできます。



保護者に代わり
子供のネット利用
を見守る!!

スマホだけでなく、ゲーム機やタブレット、子供に貸すことがある大人用の
スマホやおさがりの機器等にも、ペアレンタルコントロールを忘れずに!

2019年度総務省調査研究「インターネット利用におけるトラブル事例等に関する調査研究」

発行者 総務省 総合通信基盤局 消費者行政第一課
〒100-8926 東京都千代田区霞が関2-1-2

請負者 株式会社JMC
〒153-0061 東京都目黒区中目黒1-8-8 目黒F2ビル

監修 尾花 紀子 ネット教育アナリスト
西田 光昭 柏市教育委員会 教育研究専門アドバイザー