

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

インターネットトラブル事例解説集(平成28年度版)

総務省 総合通信基盤局
消費者行政第一課 青少年担当

目次

はじめに	1
フィルタリング機能を正しく知って上手に活用しましょう	3
子供にスマートフォンを持たせる前に	6
1 ネット依存	7
1-1 スマホ依存などによる日常生活への悪影響	7
1-2 ゲームに夢中になっている最中に生じた高額課金	9
2 ネットいじめ	11
2-1 無料通話アプリなどでの悪口や仲間外れ	11
3 誘い出し・なりすまし	13
3-1 SNS やネットで知り合った人による性犯罪被害	13
3-2 出会い系サイトなどを使った未成年からのアプローチ	15
3-3 なりすまし投稿による誹謗中傷	17
4 個人情報漏えい	19
4-1 不正アプリやウイルスによる個人情報漏えい	19
4-2 SNS などへの投稿による個人情報漏えい	21
4-3 悪意ある Wi-Fi スポットを利用したことによる情報流出	23
4-4 自ら ID とパスワードを教えたことによる被害	25
5 ネット詐欺	27
5-1 オンラインショッピングやフリマアプリでのトラブル	27
5-2 ワンクリック詐欺などによる不当請求	29
6 チェーンメール	31
6-1 友人から回ってきたメッセージで個人情報流出	31
7 著作権・肖像権侵害	33
7-1 動画の違法なアップロードとダウンロード	33
8 その他の不適切な使い方	35
8-1 個人や学校などへの脅迫行為	35
(参考) インターネットやスマホの利用に関するデータ	37
フィルタリングの設定方法	40

はじめに

仕事に、生活に、学びに……今や、私たちの日常になくてはならない存在となっているインターネット。利用端末となるデジタル機器も多種多様になり、パソコンやスマートフォン、ケータイはもちろんのこと、タブレットPCや携帯型音楽プレーヤーでスマートフォン用のアプリを楽しんだり、小型ゲーム機でゲーム仲間とコミュニケーションをとったりする子供が特別ではなくなりました。さらに、そのようなデジタル機器の利用開始年齢は年々下がっています。「ケータイもスマホも持っていないから大丈夫」とは言いきれない時代になっているのです。

インターネットやアプリは、安全に正しく使うことができればとても役立つ便利なものです。しかし、誹謗中傷やいじめの温床になったり、事件や犯罪に巻き込まれるきっかけになったりしているのも事実です。子供たちは被害者だけでなく、加害者になるケースも生じています。

「インターネットトラブル事例集」では、小学校・中学校・高等学校の教員、情報教育に精通する専門家へのヒアリングを通じて、実際に起きたインターネットやアプリを通じた代表的なトラブル事例をご紹介します。子供たちが気を付けるべきポイントについても事例ごとに掲載していますので、トラブル防止にお役立てください。また、この「インターネットトラブル事例解説集」では、事例集のケースについて、関連データを掲載するなどして分かりやすく解説しています。

子供たちの「賢く安全に使うための知識・知恵」や「ルールを守って使える心」を育むには、以下を実践することが大切です。本事例集が、インターネットを安全に賢く使える子供を育てるための一助となれば幸いです。

- デジタル機器の利用に関する現状や子供たちの使い方を正しく知る
- フィルタリングやウイルス対策といった技術(ツール)を使って、子供の発達段階に応じ、安全なインターネット利用環境を整える

トラブル事例の分類

インターネットトラブル事例集では、スマートフォンなどのフィルタリングの有効性や、子供にスマートフォンを持たせる前に保護者が意識すべきことをまとめています。

そして、以下に示すインターネット社会の8つの問題ごとに選定した合計15件のトラブル事例を解説しています。

1. ネット依存
2. ネットいじめ
3. 誘い出し・なりすまし
4. 個人情報漏えい
5. ネット詐欺
6. チェーンメール
7. 著作権・肖像権侵害
8. その他の不適切な使い方

スマートフォンやインターネットは、便利で楽しく、さまざまな魅力が詰まっています。

子供たちが、ルールを守って正しく使える環境を整えていきましょう。

フィルタリング機能を正しく知って上手に活用しましょう

子供のスマートフォンにフィルタリングを設定すると、 どんなメリットがあるのか、よくわからない。

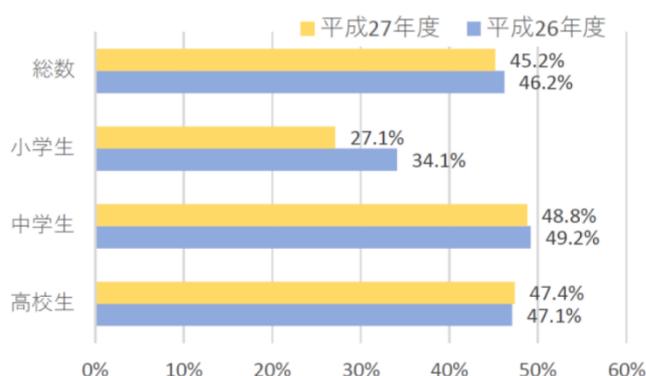
『18歳未満の子供が利用する機器にはフィルタリングを設定しよう！』と言われるけれど、『有害な情報へのアクセスを防止するだけなら自分で気を付ければ大丈夫では？』と思われている方が年齢や立場を問わずいらっしゃいます。しかし、スマートフォンやタブレット PC でのフィルタリングは、有害情報の閲覧制限以外にもさまざまな役割を持っています。また、十分に注意をしても、危険性のある Web サイトなどへのアクセスをしてしまうこともあります。まずは、子供にインターネットを利用させる上での不安について考えてみましょう。

インターネットを利用させる上での不安

① ネット依存	② 対面でのコミュニケーションへの影響	フィルタリングで軽減可能
③ 学習・成績への影響	④ 身体(目、姿勢など)や健康への影響	ウイルス対策で軽減可能
⑤ 個人情報の漏えい	⑥ 課金	そのほかは人の力(工夫)で予防
⑦ ネットいじめ被害・加害	⑧ 誘い出しや性的被害	
⑨ 不適切な情報発信	⑩ 不適切な情報に触れることとその影響	

たとえば、上記の①～⑩のような不安が考えられます。フィルタリングを利用することで、⑥～⑩のトラブルなどの可能性を軽減させることができます。また、ウイルス対策をすることで、⑤～⑥のトラブルなどの可能性を軽減させることができます。

「×見たいものが見られない厄介者」→「○不安を軽減する仕組み」 フィルタリングの利用実態



児童・生徒のスマートフォン利用は増加傾向にあり、低年齢化も加速しています。ところが、フィルタリングの利用率は半数以下という調査結果があります。小学生の利用率が最も低いのは、保護者のスマホやお下がりの機器を使っていることが考えられます

が、これはリスクを考慮すると大きな問題です。インターネットの利用に必要な知識や経験、トラブル回避能力を補うことができるフィルタリング。閲覧できる情報や危険がケータイの比ではないスマホだからこそ、フィルタリングの利用価値が高いことを知っておきましょう。

貸し出しやお下がりも含め、子供が使う機器にはフィルタリングを！

フィルタリングにはいくつかのレベルがあり、年齢や成熟度に応じて自由に選択できます。多少ゆとりのある設定をするなど、うまく活用して安全な利用環境を作りましょう。子供の知識や経験に合わせて、子供と話し合いながら、レベルを変更していくことも重要です。

フィルタリングをすることで防げるトラブル事例

うっかりアクセスによる被害

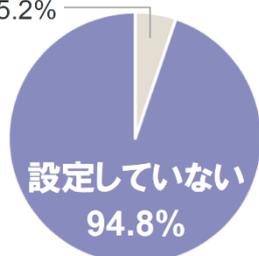
指先で軽く触れるだけで動作するスマホやタブレット PC。うっかりタッチした部分に悪意を持った仕掛けがあり、架空請求やメールアドレスの流出による迷惑メールの急増といったトラブルに巻き込まれることも可能性としてあります。そんな時に「ブラックリストに登録されている危険なサイトです」と、アクセスを止めてくれるフィルタリングはとても便利で心強い存在です。

フィルタリングを外してしまったために

保護者が設定してくれたゲーム機のフィルタリングを自分で外し、ゲーム機のソフトウェアを利用して連絡を取り合った末、児童買春の被害にあってしまったケースもあります。スマホやタブレット PC 同様、ネットにつなげて使うゲーム機にもフィルタリングは必要ですが、いずれの機器でも、設定変更や解除のためのパスワードは慎重に管理することが大切です。

ネットで知り合い被害にあった子供の大半がフィルタリング未設定

設定している 5.2%



フィルタリングを設定していなければ、さまざまなコミュニティサイトや出会い系サイト・アプリなどが自由に使えることから、簡単に大人と知り合うことができ、連絡が取り合えてしまいます。また、フィルタリングを設定していても、Wi-Fi 接続時やア

プリからはアクセスできてしまうこともあるため、どのような使い方の時に、フィルタリングの機能が有効に働いているか確認することが大切です。

(参考)警察庁「平成 27 年における出会い系サイト及び
コミュニティサイトに起因する事犯の現状と対策について」

「青少年インターネット環境整備法」について

平成 21 年 4 月には、「青少年インターネット環境整備法」が施行されています。
この法令の中では、以下の内容が「保護者の責務」として記載されています。

保護者の責務

- ・インターネット利用状況を適切に把握する。
- ・フィルタリング等の利用により、子供のインターネット利用を適切に管理する。
- ・子供がインターネットを適切に活用する能力の習得の促進に努める。
- ・不適切な利用により、売春、犯罪の被害、いじめ等様々な問題が生じることに留意する。

<フィルタリングに関する Web サイト>

関連省庁や団体ではフィルタリングの普及を目的とした、情報提供を行っています。

保護者向け普及啓発用リーフレット(内閣府)

<http://www8.cao.go.jp/youth/youth-harm/koho/keihatsu/260228/index.html>

フィルタリングサービスを利用しましょう！(安心ネットづくり促進協議会)

<http://sp.good-net.jp/filtering/>

フィルタリング(有害サイトアクセス制限サービス)をご存知ですか？(総務省)

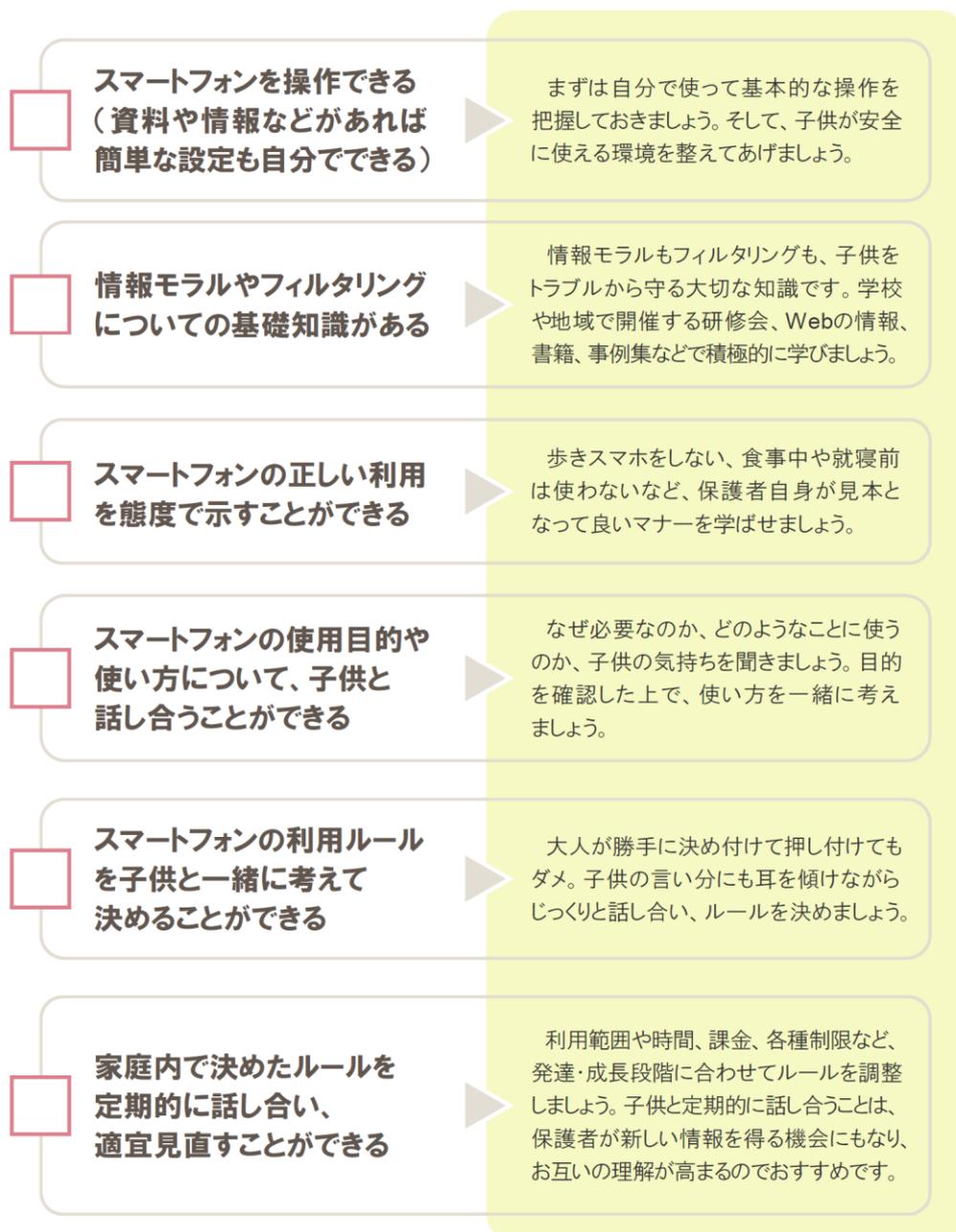
http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/filtering.html

小学生・中学生向け「ちょっと待って！ケータイ&スマホ」リーフレット 2014年版(文部科学省)

http://www.mext.go.jp/a_menu/sports/ikusei/taisaku/1345365.htm

子供にスマートフォンを持たせる前に

スマートフォンを使うようになれば、インターネットを通じて年齢・性別・場所を問わず多くの人とつながる可能性が生じます。そこで、保護者自身が意識して行動したいことを以下にまとめました。高校生は 18 歳に向けて徐々に管理を任せる方法も悪くはありません。しかし、保護者としても、子供の取り扱いを見守っていきましょう。



1 ネット依存

1-1 スマホ依存などによる日常生活への悪影響

友人とのトークが深夜まで連日続き



寝る時間だけど、
あと少しだけ。

無料通話アプリを使った友人とのトークが大好きなAさん。毎回、トークを終わらせるタイミングがわからず、夜遅くまでスマホを使う日々が続きました。

睡眠不足になってしまった



Aさんは、睡眠不足で朝がつらくなり、授業にも集中できなくなりました。体調や成績に悪影響が出ているのに、友人とのトークはやめられません。

【解説1-1】四六時中、気付くとスマホを手にしている

無料通話アプリやSNS、ゲーム、動画など、楽しく魅力的なことがいろいろできるスマホですが、使い過ぎには要注意。勉強や食事をしていてもスマホが気になる、歩行中もスマホから目が離せない、そんな依存傾向のある子供が増えています。自分をコントロールできずスマホを長時間使うようになれば、当然、勉強に充てる時間が減ります。寝不足により授業にも集中できなくなれば、学力への影響は避けられません。意識がスマホに集中するあまり、現実で居合わせている人との会話が疎かになることも。こうした症状は、スマホを使っている本人が気付いておらず、周囲から指摘されて初めて気付くことが多いようです。適切な使い方ができるよう、利用のルールを決め、保護者が利用状況を把握するよう心掛けましょう。利用ルールは、保護者の押し付けではなく、一緒に話し合い、子供に考えさせながら決めることが大切です。また、利用時間を制限するアプリを利用することも一つの方法です。

小・中学生が常に心掛けたいこと

▼家庭でのルールをしっかりと守らせる

- ・ 利用時間について家族で話し合い、決めたルールを守って使うことを習慣にしましょう。ルールが合わなくなったら、家族と一緒に見直しましょう。

▼スマホの利用はメリハリをつけて

- ・ 食事中、歩行中などは使わない。勉強中どうしても気になるなら、保護者に預ける方法も。依存症にならないよう、メリハリを付けて使うようにしましょう。

▼夢中になり過ぎていないか考える

- ・ 人との会話中もスマホをいじっていないか、時間を忘れて使っていないか、自分の利用について振り返ってみましょう。友人と話し合うのもおすすめ。

参考

青少年及び保護者のインターネット利用時間(利用機器の合計)



ネット利用には、「ネットでわからないことをすぐに調べられるので、時間を効率的に使えるようになった」「いろいろな情報を収集できるので知識が増えた」「今まで知らなかったことでも簡単に調べられるので世界が広がった」といったさまざまなメリットがあります。しかし、インターネットを2時間以上利用する青少年の割合の平均は、10歳では21.7%、13歳では44.1%、17歳では71.3%と、年齢が上がるにつれて、インターネット

利用時間は長くなる傾向にあります。子供が食事中や就寝直前まで、携帯電話やスマホが手放せなくなってしまうことがないよう、インターネット利用のルールを作り、日頃から意識させることで、規則正しい生活環境を整えることが大切です。

(参考)内閣府「平成27年度青少年のインターネット利用環境実態調査 調査結果(概要)」

1-2 ゲームに夢中になっている最中に生じた高額課金

アイテム購入は数回だけだったのに



Bくんは、お母さんからスマホを借りて、ゲームをしていました。アイテムが欲しいときはお母さんに相談し、パスワードを入れてもらって購入しました。

請求書は10万円を超えていた



翌月10万円を超える請求が来ました。スマホを確認すると、パスワード入力後の数分間は自由に購入できる設定になっていたことが分かりました。

【解説1-2】クレジットカードやパスワードの管理に要注意

ゲームアプリには、ランキングやレアアイテム、キャンペーン、ガチャのように、競争心や射幸心をあおる演出や仕組みを含むものがあります。一つ一つの金額が低いため、気付いたら思った以上の課金額になっていることも。国民生活センターによると、未成年のオンラインゲームに関する相談では、契約購入金額の平均は約23万円。スマホ利用の低年齢化もあり、判断能力を伴わない9歳以下の相談が増加しています。子供が遊んでいるゲームが完全無料なのか、ゲーム内に課金の仕組みがあるのか、親子で確認しましょう。親子でゲームの内容や課金の仕組みを確認することも大切です。クレジットカードの管理責任は保護者にあります。カードを無断利用させないよう、常に気を配りましょう。クレジットカードの利用明細を毎月確認することで、トラブルの被害を抑えることができます。

(参考)国民生活センター「増え続ける子どものオンラインゲームのトラブル 一家族でゲームの遊び方を話し合うとともに、クレジットカード管理の徹底を!」(平成25年12月)

小・中学生が常に心掛けたいこと

▼購入時は保護者に必ず相談する

- ・ ゲームでアイテムの購入や、課金が必要なときは、保護者に必ず相談しましょう。ネットショッピングやオークションも大人に話して買ってもらいましょう。

▼クレジットカードを勝手に使ってはダメ

- ・ 家族の名義でもクレジットカードを勝手に使ってはいけません。もちろん、ネット上の支払いも普通の買い物と同じ、お金を使っていることを忘れないで。

▼課金し過ぎないためにできることを知る

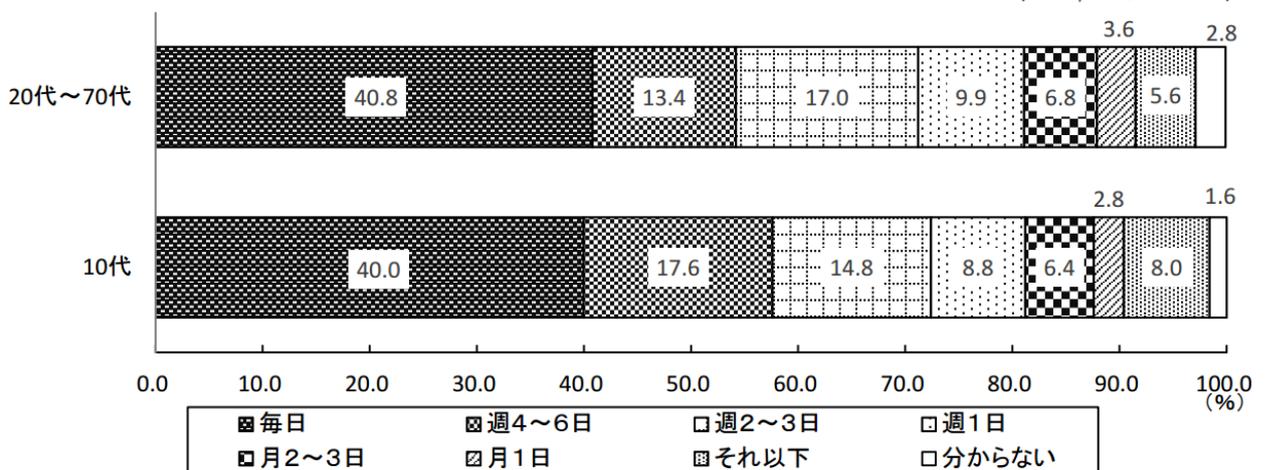
- ・ 中学生までは5千円、高校生は1万円という上限を設けているゲームも。年齢を登録する、パスワードに関する設定を見直す、ということも役立ちます。

参考

消費者庁の調査によると、日頃オンラインゲームを行っている10代の男女のうち、40.0%はオンラインゲームを毎日行っており、2.8%はオンラインゲームの課金トラブルの経験があることがわかりました。トラブルの内容は、「課金されているつもりはなかったのに課金されていた」、「身に覚えのない課金をされた」、「他のユーザーとの間でアイテム等の売買・交換等のトラブルがあった」、など。そのほかにも、「オンラインゲーム内で知り合った人との間の人間関係のトラブルにあった」、「ゲーム依存症になった」といった課金以外のトラブルも発生しています。

図1 オンラインゲームの利用頻度

(N=2,500/N=250)



※各値については、「20代~70代」が20~79歳、「10代」が15~19歳、以下、同様。

(参考)消費者庁「平成25年度消費生活に関する意識調査結果報告書 ―オンラインゲームに関する調査―」

2 ネットいじめ

2-1 無料通話アプリなどでの悪口や仲間外れ

読むだけで書き込まずにいたら



複数の友人とリアルタイムで会話を楽しめるグループトーク機能。Cさんは、ほとんど書き込みをせずに、友人たちの会話を楽しんでいました。

一方的にグループから外されてしまった



友人たちは、Cさんがあまり書き込まないことに腹を立て、Cさんの悪口を書き込むようになり、最後はCさんをグループから外してしまいました。

【解説2-1】グループトーク機能だけでも、トラブルのパターンはさまざま

全国的な課題として、無料通話アプリのグループトーク機能を使ったいじめがあります。特定の子に対し、その子の発言だけ無視する、その子にとって不快な写真や動画をグループで共有する、その子以外とグループを作り悪口を言う、その子をグループから突然外すなどがあり、何気ない出来事からいじめに発展することも少なくありません。メンバーでなければ会話の内容を読むことができないため、トラブルの発見は遅れがちとなります。特に、長期休暇は無料通話アプリの利用が増える傾向にあります。子供たちは、学校で直接会う機会が減るかわりに、時間や場所を問わず、無料通話アプリでコミュニケーションを取るようになります。携帯電話やスマホの使い方に変化があった、友人のことを聞いても話そうとしない、学校へ行くことを嫌がっているなど、日々の様子や会話から子供の変化に気付くこと、これがトラブルの早期発見や解決につながります。

小・中学生が常に心掛きたいこと

▼相手の気持ちになって読み返す、考えて送る

- ・ 何気なく書いたことで友人を傷付けてしまったり、文字だけのやり取りなので意味を取り違えて誤解を受けてしまったり。送る前に内容を確認しましょう。

▼すぐに反応がないときは相手の状況を想像する

- ・ タイミングが悪いときは誰にでもあります。すぐに既読がつかない、メッセージが来ないなどイライラしないように、グループの仲間と話し合っておきましょう。

▼大切なことは電話か直接会って話す

- ・ 急いでいることや大事なことは、相手の顔を見ながら話すのが一番。声の調子が伝わる電話もOK。無料通話アプリだけに頼り過ぎないで。

参考

平成25年9月、「いじめ防止対策推進法」が施行されました。これは、国や地方自治体、学校がいじめ防止に取り組む責務を定めた法律で、インターネットを通じて行われるいじめの防止にも取り組むことが定められています。

第二条

この法律において「いじめ」とは、児童等に対して、当該児童等が在籍する学校に在籍している等当該児童等と一定の人的関係にある他の児童等が行う心理的又は物理的な影響を与える行為（インターネットを通じて行われるものを含む。）であって、当該行為の対象となった児童等が心身の苦痛を感じているものをいう。

第十九条 3

インターネットを通じていじめが行われた場合において、当該いじめを受けた児童等又はその保護者は、当該いじめに係る情報の削除を求め、又は発信者情報（特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律（平成十三年法律第百三十七号）第四条第一項 に規定する発信者情報をいう。）の開示を請求しようとするときは、必要に応じ、法務局又は地方法務局の協力を求めることができる。

「いじめ防止対策推進法(平成二十五年六月二十八日法律第七十一号)」から引用

3 誘い出し・なりすまし

3-1 SNSやネットで知り合った人による性犯罪被害

SNSでは趣味が合う良い人だったのに



Dさんは、同じバンドのファンという男性とSNSでよく話をしていました。ある時「ライブのチケットが余分にあるから一緒に行こう!」と誘われました。

実際に会うと怖い人だった



ライブ当日、待ち合わせ場所に行ってみると、SNSの写真とはまったく違う人で、チケットの話もウソ。無理やり車に乗せられそうになりました。

【解説3-1】 SNSやネットで出会った人は、想像とは全然違うことも

「同じ趣味や話が合う人に、悪い人はいない」と考え、会ってみたいと思う青少年が増えています。しかし、相手が本当のことを言っているとは限らず、実際に会って事件やトラブルに巻き込まれるケースもあります。警察庁によると、平成27年のコミュニティサイトに起因する児童被害は約1,700人、平成20年以降は増加傾向にあるということです。次のページに、被害児童数の推移を掲載しています。平成20年の被害児童数は792人だったのに対し、平成27年の被害児童数は1652人。7年間で2倍以上に増加しています。また、現実の交際相手であっても、あまりにも私的な写真や動画の撮影はやめましょう。万が一、ネット上に流出した場合、あっという間に拡散して、取り返しがつかなくなってしまう。一度流出した情報をネット上から削除することは、ほぼ不可能であることも、子供たちに理解させることが大切です。

(参考)警察庁「平成27年における出会い系サイト及びコミュニティサイトに起因する事犯の現状と対策について」(平成28年4月)

小・中学生が常に心掛けないこと

▼フィルタリングを利用し安全な使い方をしよう

- ・ フィルタリングは、危険がありそうなサイトへの思わぬアクセスを防ぐ役割も担っています。上手に使って、危険な目に遭いづらい環境で使いましょう。

▼話が合う良い人でも誘いには乗らない

- ・ ネットを介してやさしく接してくれていても、それが本当の姿とは限りません。「会おう」、「写真が欲しい」としつこく言ってくるようなら、大人に相談しましょう。

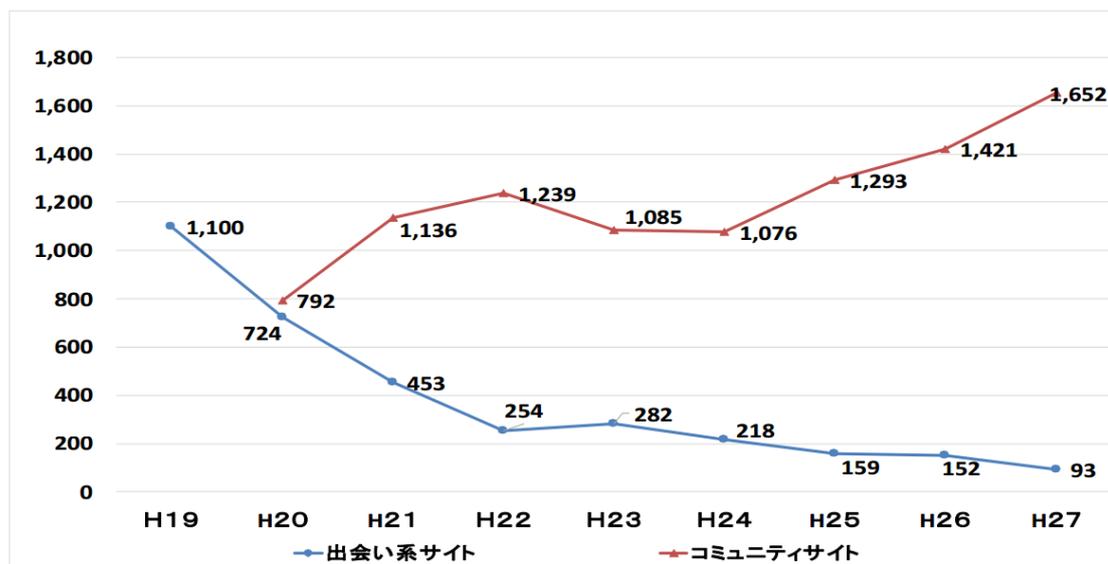
▼私的な写真や動画の撮影や共有は慎重に

- ・ たとえ信頼できる友人でも、不特定多数の人に見られたら困る写真や動画の共有はやめましょう。特に性的な画像は、撮影も所持も禁止です。

参考

警察庁の発表によると、平成27年のコミュニティサイトに起因する事犯の被害児童は1,652人（平成20年以降は増加傾向）。そのうち、フィルタリングを利用していなかった被害児童は724人で、フィルタリングの利用の有無が判明した被害児童の94.8%を占めます。子供のネット利用状況を把握し、適切に管理することが大切です。

図 1 【出会い系サイト及びコミュニティサイトに起因する事犯の被害児童数の推移】
(人)



※ コミュニティサイトの統計は平成20年から取り始めた。

(参考)警察庁「平成27年における出会い系サイト及びコミュニティサイトに起因する事犯の現状と対策について」

3-2 出会い系サイトなどを使った未成年からのアプローチ



【解説3-2】危険な書き込みは、出会い系から非出会い系へと拡大

未成年が出会い系サイトに異性交際(金品目的も含む)を求める書き込みは、出会い系サイト規制法で禁じられています。そのため、「家出中、今晚泊まらせてくれる人募集」といった書き込みも犯罪行為となり得ます。児童がこれらに違反すると、少年法の規定により家庭裁判所に送致されることになっています。そもそも、18歳未満の出会い系サイトの利用は認められていません。ID交換掲示板やチャット型SNSなど、ほかのサービスを使うケースも増えていますが、犯罪に巻き込まれる可能性が高いこと、違法行為であることを認識させ、良識ある行動を促しましょう。フィルタリングなど、出会い系サイトへのアクセス自体を防ぐ対策を取ることも効果的です。保護者は「子供の安全のために」と携帯電話を持たせて安心するのではなく、子供を監督する責任があることを認識しましょう。

小・中学生が常に心掛けないこと

▼フィルタリングを利用し安全な使い方をしよう

- ・ 出会い系やID交換掲示板などへのアクセス予防にもなるフィルタリング。自分の使い方に合った設定で利用しましょう。

▼ネットの向こう側に潜む危険を考える

- ・ 女性を装って誘い出され、被害にあったケースも。不用意な書き込みがどんな危険を招くか、真剣に考えてみましょう。

▼情報発信には、責任が伴うことを理解する

- ・ 年齢を問わず、ネットを使った情報発信には社会的責任が伴います。このことを忘れず、書き込みの際には気を付けましょう。

参考

インターネット異性紹介事業を利用して、児童との異性交際の相手方となるように誘引する行為は禁止されています(出会い系サイト規制法)。出会い系サイトに異性を誘う書き込みをすることは、子供であっても違法です。この違法行為により、100万円以下の罰金が課せられることがあります。警察はインターネット上の違法行為を取り締まるために、サイバーパトロールを行っています。実際に実行するつもりがなくても、書き込みを行っただけで罪に問われることがあることを認識させましょう。

(参考)警察庁「STOP！ ネット犯罪ーネットの世界は危険と隣り合わせ！ー」

3-3 なりすまし投稿による誹謗中傷

他人になりすまして書き込んで



△校のF君は、○校のG君が気に入らなかったため、**F君はG君になりすまし**、ネット上に「○校のH君が万引きしている」と、嘘を書き込みました。

書き込んだ本人が特定された



H君がG君を問い詰めると、G君の書き込みではないことが分かりました。調べると、△校のF君の仕業だと判明。**学校間トラブル**に発展しました。

【解説3-3】迷惑行為や誹謗中傷は、利用規約で禁止されている

多くのSNSは、利用規約の中で迷惑行為や誹謗中傷を禁止しています。登録時に同意したルールですから、守って使うように指導してください。また、他人になりすます行為は発言の責任をなすり付けることになるため、それによって相手が傷付いたり、信用を失ったりした場合、名誉毀損で訴えられる可能性もあります。「ネットなら誰が書いたかわからない」と勘違いしている子供もいますが、警察が動くようなケースだけでなく、ネット上のさまざまな情報により書き込んだ本人が特定できる場合があることを正しく理解しましょう。やってはいけないことはネットでも現実でも同じです。インターネットの特性を理解した上で、自分の言動が周囲にどのような影響を与えるのかについても指導していく必要があります。

小・中学生が常に心掛きたいこと

▼やってはいけないことはネットでも現実でも同じ

- ・ 実際にはやってはいけないことは、ネットでもNG。ネットだから平気、ネットなら見つからない、という考えは改めましょう。

▼困ったら信頼できる大人に相談する

- ・ トラブルや心配事が生じたら、子供だけで解決しようとせず、保護者や先生、スクールカウンセラーなどに相談しましょう。

▼悪質な書き込みは犯罪となる可能性があることを教える

- ・ 悪意があるなしに関わらず、悪質な書き込みは処罰の対象になることがあります。ルールやモラルを守って使いましょう。

参考

インターネット上のなりすましでは、第三者に自分のSNSアカウントが不正にログインされてしまうケースがあります。友人や知人になりすまし悪意のあるサイトのURLを拡散したり、個人情報を聞き出そうとしたりするなどの被害が報告されているため、直接、なりすましの被害にあっていない場合にも注意が必要です。

Twitter、Facebook、LINEなどのSNSでは、公式ホームページ上にヘルプセンターを設置し、不正利用の報告窓口を用意しています。なりすましによる悪質な書き込みを発見した場合には、Webサイトの運営会社(運営者)に直接対応を依頼することが効果的です。

(参考)LINE公式ブログ「【注意喚起】友人や知人になりすまして電話番号やSMS認証番号を聞き出すメッセージにご注意ください」

4 個人情報漏えい

4-1 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1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、1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、1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4-1】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。アプリをインストールする際は、「アクセス許可」を必ず確認し、アプリの動作から考えると不必要なアクセス権限を求められていないか、よく確認する必要があります。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。信頼できるアプリやWebサービスをいかにして見極めていくかが重要となります。

(参考)警視庁「スマートフォンを利用している方へ」(平成28年5月)

<http://www.keishicho.metro.tokyo.jp/kurashi/cyber/security/cyber414.html>

小・中学生が常に心掛けないこと

▼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。

▼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。

▼自分がウイルスを広める可能性もあることを知る

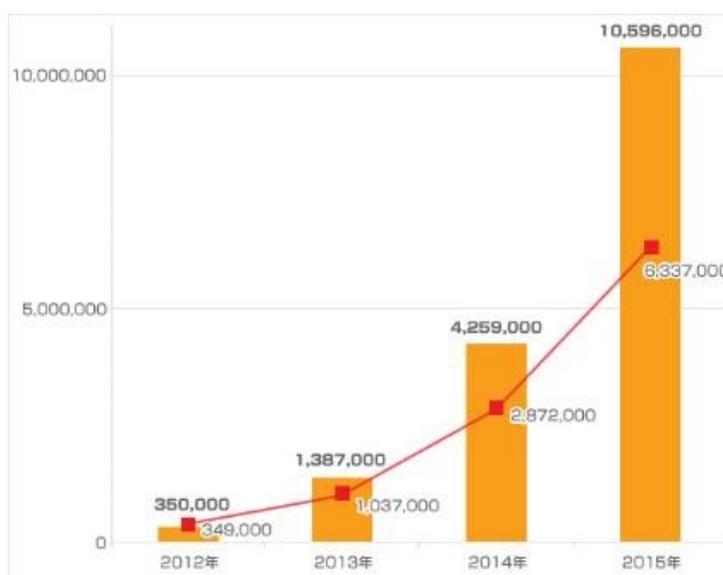
- ・ 1人が感染すると、家族や友人にも広まってしまうウイルス。自分だけでは終わらないことを忘れず、常に注意しましょう。

参考

トレンドマイクロ社の調査によると、Android向けの不正アプリは、2010年に初めて確認されてから5年も経たずに累積1,000万個を突破しています。特に2015年には、それまでの5年間で確認された430万個を大きく上回る630万個の不正アプリが登場しました。これら不正アプリ全体のうち80%が「アドウェア」です。アドウェアは、侵入したスマホ上で表示した広告経由で特定のアプリをインストールさせることにより、アプリ開発者から報酬を受け取ることを目的としています。

Android不正アプリの
累積検体数(棒グラフ)と年間の
増加数(折れ線グラフ)推移

(参考)TREND MICRO is702
「ファイルや端末を人質に脅迫！？
スマホを狙う不正アプリの最新事情」



4-2 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4-2】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。SNSからの個人情報流出をきっかけに、電子掲示板やSNSにいやがらせをされたり、実際のストーカー行為を受けたりするケースもあります。SNSの投稿範囲、コメントやメッセージの受け付け、位置情報の付加などの設定にも、十分に注意しましょう。

(参考)総務省「安心してインターネットを使うために

国民のための情報セキュリティ」事例6: ネットストーカーに注意

http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/enduser/case/06.html

小・中学生が常に心掛けないこと

▼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

▼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。

▼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

参考

デジカメやスマホで撮影した写真データには、カメラの設定や撮影日時、GPS情報(位置情報)などを記録したExif(イグジフ)と呼ばれる情報が記録されています。もし、ExifのGPS情報が付加されたままの写真を投稿すると、そこに写っている内容に関わらず閲覧者は撮影場所がどこであるのかを知ることが可能です。最近では、写真を投稿する際にExif情報が自動で削除されるよう設定されているSNSやブログもありますが、Exif情報の取り扱いには十分な注意が必要です。



(参考)情報処理推進機構「ゴールデンウィーク(GW)の行楽写真を投稿する際はご注意を
～ブログやSNSに投稿した写真からプライバシー漏洩の可能性～」

4-3 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



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4-3】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。また、携帯ゲーム機や音楽プレーヤーにも、Wi-Fiを経由してインターネット通信ができる機能が付いている場合があります。子供たちが利用する機器がどのような設定になっているのか、注意していく必要があります。

小・中学生が常に心掛けたいこと

▼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。

▼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。

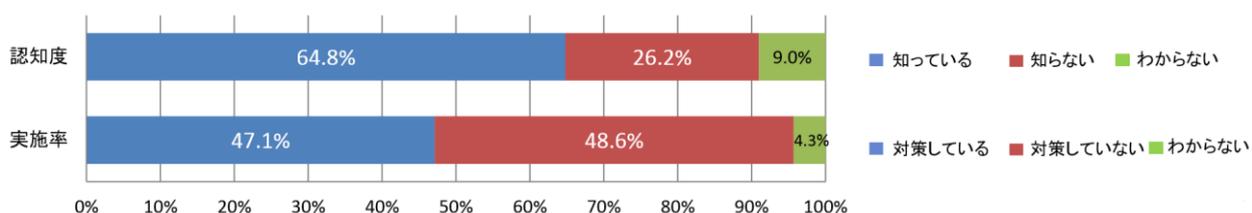
▼外部から遠隔操作をされる可能性を知る

- ・ 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。

参考

2020年オリンピック・パラリンピックの東京開催に向け、総務省では訪日外国人が無料で利用できる公衆無線LANサービスの整備促進を進めています。一方で、総務省が実施した公衆無線LANの利用状況や情報セキュリティ意識等に関する調査によると、公衆無線LAN利用時の脅威について64.8%がその存在を認知しているものの、48.6%が対策を実施していませんでした。

公衆無線LAN利用時の脅威(盗聴／なりすまし／悪意のアクセスポイントやサイトへの接続)
認知度及び実施率



(参考)総務省「公衆無線LAN利用に関する情報セキュリティ意識調査結果」

4-4 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4-4】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。子供がアプリやWebサービスを利用する際には、IDとパスワードの役割や適切な管理方法の指導を忘れずに行いましょう。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、無断で立ち入るといったことへの罪悪感が鈍る傾向があります。些細なことから事件の加害者になってしまう危険性もあるため、注意喚起が必要です。

小・中学生が常に心掛きたいこと

▼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。

▼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。

▼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。

参考

ネットワークを利用したなりすまし行為は、平成12年に施行された「不正アクセス行為の禁止に等に関する法律」により禁止されています。オンラインゲーム上で他人のユーザーIDとパスワードでなりすましてログインし、他人のキャラクターの装備品やアイテムを自分のキャラクターに移し替えたり、他人になりすましてオークションへ出品したり、入札したりするなどの行為も不正アクセス禁止法違反になります。

特にオンラインゲームは若者のユーザーも多く、熱中するあまり犯罪の意識がなくなってしまうケースが見られます。不正アクセス禁止法違反で検挙される未成年者の割合は年々増加傾向にあります。

区分 \ 年次	平成23年	平成24年	平成25年	平成26年	平成27年
14～19歳	51	64	44	49	53
20～29歳	30	34	30	43	43
30～39歳	19	21	37	45	41
40～49歳	10	28	27	25	29
50～59歳	2	6	8	5	5
60歳以上	2	1	1	3	2
計（人）	114	154	147	170	173

図 過去5年の年代別被疑者数の推移

(参考)警視庁「安全な暮らし 情報セキュリティ広場セキュリティ対策 不正アクセス」
警察庁 サイバー犯罪対策「平成27年における不正アクセス行為の発生状況等の公表について」

5 ネット詐欺

5-1 オンラインショッピングやフリマアプリでのトラブル



探していた洋服を扱うサイトを見つけたMさんは、**品質に難あり**といった口コミや、**代金振込後発送のみ**といったことは不安でしたが一着購入しました。

その後、いくら待っても商品は届きませんでした。購入の際にあった連絡先にメールで問い合わせても返信はなく、電話もつながりませんでした。

【解説5-1】購入した商品が届かない、掲載写真と商品や品質が違う

ショッピングサイトの情報を信用して購入したのに、商品が届かない、ニセモノだったなどの被害が多発しています。国民生活センターによると、インターネットショッピングでの商品取引に関する相談件数は、2013年から2015年の3年間では、5万件を超えて推移しています。インターネットショッピングが拡大したことにより、トラブルなどの相談件数も増加傾向にあります。明らかに価格が安い、日本語表現がおかしい、良くない評判がある、といったサイトでの購入は避けましょう。また、最近若い世代に人気のフリマアプリは、未成年者が利用する場合は、保護者の同意が必要なものがほとんどです。もしも、保護者の同意を得て、フリマアプリを利用する場合は、フリマアプリの利用ルールを守って使い、商品説明や詳細写真、出品者の評価などに必ず目を通すなど、安全性の確認を怠らないようにしましょう。

(参考)国民生活センター「インターネット通販(各種相談の件数や傾向)」(平成28年6月)

小・中学生が常に心掛きたいこと

▼欲しい商品があったら必ず保護者に相談する

- ・ 保護者のIDで注文したり、保護者のカードで支払ったりしてはいけません。欲しいモノを見つけたら、必ず保護者に相談を。

▼購入に使った個人情報が悪用されることもある

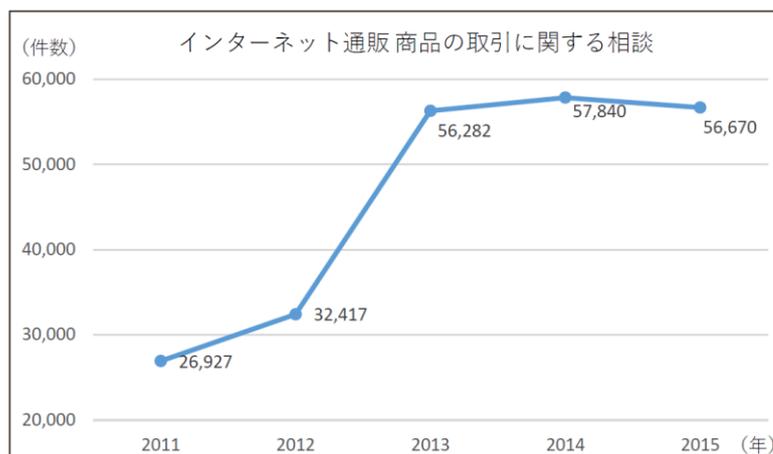
- ・ 悪質なお店を利用してしまうと、連絡先やカード番号などが悪用される危険も。不安を感じたら購入や取引をやめましょう。

▼トラブルは大人に話し急いで窓口で相談を

- ・ 万が一、トラブルにあった場合、すぐに保護者に話して専門の窓口で相談してもらいましょう。一刻でも早い対応が重要です。

参考

インターネットの普及に伴い、インターネット通販の取引に関する相談が急速に増加しています。取引に関する相談件数では、2013年から2015年まで6万件弱を推移しています。近年の事例としては、国民生活センターでは「クーポンサイトでプリペイドカードが当たる抽選



に応募したら、申し込んでもいないサポートマスクを購入したことになる。どうしたらよいか」、「インターネット通販でムートンブーツを注文し代金を振り込んだが、商品が届かなかった。現在、サイトが消えてしまっている。どうすればよいか」などの相談があったということです。

(参考)国民生活センター「インターネット通販(各種相談の件数や傾向)」

5-2 ワンクリック詐欺などによる不当請求

メールの添付データを開いたら



N君がパソコンで写真整理をしていたとき、「この前の写真を送ります」というメールが届いたので、確認しようと、添付ファイルを開いてみました。

パソコンのファイルが暗号化された



すると、N君のパソコン内にあるファイルが暗号化されてしまい、「暗号化を解除して欲しければ、お金を振り込め」という指示が表示されました。

【解説5-2】ファイルを人質に身代金を要求するランサムウェア被害も増加

これまでは、パソコンやスマホなどの操作中いきなり高額な料金を請求されるケースがほとんどでしたが、最近はファイルを暗号化し、使えない状態にして金銭を脅し取ろうとする「ランサム(＝身代金)ウェア」が社会的な問題となっています。こうしたウイルスの主な感染源は、メールの添付ファイルです。情報処理推進機構(IPA)へのランサムウェアに関する相談件数は、増加傾向にあります。誰もが自分宛てだと思うメッセージや、知り合いになりすましたメールが多いため、被害が増えているのです。その他、最近ではスマホでインターネットをしていて、急にシャッター音が鳴って写真を撮ったかのように見せかけて脅すケースもあります。これらは不当請求の一つの手法に過ぎません。不当請求の手法は巧妙化しているので、どのようなやり口がニュースに取り上げられているのかは理解しておきましょう。

(参考)情報処理推進機構(IPA)

「コンピュータウイルス・不正アクセスの届出状況および相談状況」(平成26年4月)

小・中学生が常に心掛けないこと

▼フィルタリングと一緒にウイルス対策を

- ・ 悪意の仕掛けがあるサイトへのアクセスは、フィルタリングで防ぎましょう。ネット詐欺対策にはウイルス対策も不可欠です。

▼少しでも怪しい箇所があるメールは開けない

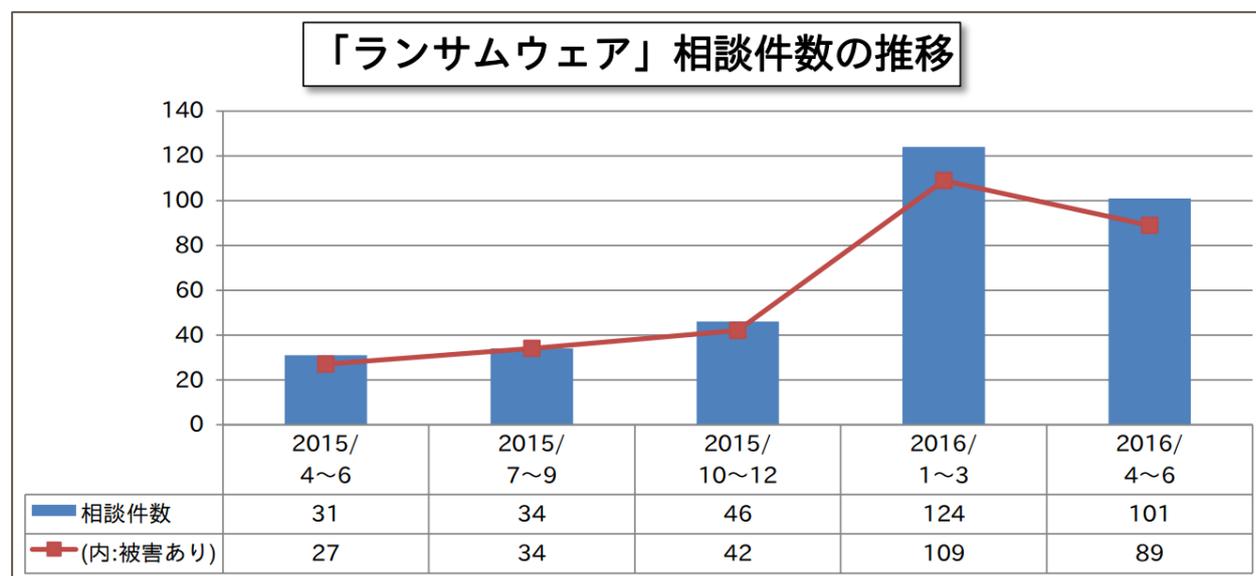
- ・ 誰宛てでもOKな内容は怪しいと考え、用心しましょう。また、添付ファイルの開封には細心の注意を払きましょう。

▼アダルト系や出会い系に潜む危険を知る

- ・ アダルト系や出会い系などのサイトやアプリには、不当請求のワナが潜むものも。興味本位で使わないようにしましょう。

参考

情報処理推進機構(IPA)によると、ランサムウェアに関する相談件数は、2016年4月から6月では101件。これは2015年4月から6月と比較すると、およそ3倍の相談件数と、全体的にみると拡大傾向にあります。



(参考)情報処理推進機構(IPA)「コンピュータウイルス・不正アクセスの届出状況および相談状況[2016年第2四半期(4月~6月)]」(平成28年7月)

6 チェーンメール

6-1 友人から回ってきたメッセージで個人情報流出

友人の間だけで回した内容だったのに



無料通話アプリで、学校の友人からバトンが回ってきました。質問内容を読み、Oさんは、気軽な気持ちで名前や年齢、学校名などを答えました。

ネットで知り合った人に待ち伏せされた



ネットで知り合った男性に待ち伏せされたOさん。以前、その人に無料通話アプリのアカウントを教えたため、Oさんは、情報を見られていたのです。

【解説6-1】バトンの内容、読めるのは本当に親しい友人だけ？

無料通話アプリのタイムラインなど、日常のつぶやきを投稿できるサービスを利用した「バトン」というものがはやっています。バトンとは、定型の質問に答えながら次の人へと回していく遊びのようなもの。一般的なチェーンメールとは違ってもともと悪意はないのですが、公開範囲設定をしていなければ、友人登録しているすべての人が読めるため、トラブルに発展することも少なくありません。個人情報には答えない・回さないように心掛けるとともに、ネットで一言二言話して友人登録した相手は、タイムラインの非公開設定をしましょう。思わぬ個人情報を流してしまうことになります。また、バトンの質問に嫌いな人といった内容を含めてバトンを回して、いじめに発展してしまうようなケースも起きています。バトンは遊びの要素が強いため、気軽に考えてしまいがちですが、大きな危険も生じる可能性があるため、クラスで話し合うなどして理解を深めていきましょう。

小・中学生が常に心掛けないこと

▼SNSでは、名前など書き込まない

- ・ 名前や住所、学校名のほか、個人情報に関することは書き込まないのが原則です。投稿もバトンと同じだと考えましょう。

▼限られた人だけの空間でも、広がる可能性あり

- ・ 学校の友人だけとのやり取りでも安心は禁物。コピーしやすく広がりやすいというネットの特性を理解・意識して使いましょう。

▼親しい友人たちと話し合って考える

- ・ バトンに限らずチェーンメールは「回さない」のが一番。友達関係が悪くならないためにも、クラスや友人で話し合ひましょう。

参考

チェーンメールの主な種類です。今ではSNSを使って広まっています。

デマ系

不安を煽ったり、デマを流布することを求めたりするものがあります。拡散希望と記載された情報であっても、その情報に対して信憑性が担保されている保証はありません。

脅迫系

友人にメールを回さないと不幸になる、回せば幸福になるなども、この種類のチェーンメールにあたります。

バトン系

SNSで定形型の質問を友人に回していくものです。質問の中には、個人情報を回答させるものが含まれていることがあります。

7 著作権・肖像権侵害

7-1 動画の違法なアップロードとダウンロード

映画のデータを無許可で公開し



P君は、話題の映画のデータが手に入ったので学校の友人にもシェアしようと思い、**動画共有サイトに、その映画のデータをアップロード**しました。

著作権法違反で自宅に警察が...

著作権侵害の疑いがあります。動画公開の経緯は？



警察は、**映画の投稿者をP君と特定**。ほかにも、入手した映画や動画をいろいろ公開していたP君は、著作権法違反容疑で書類送検されました。

【解説7-1】身の回りには、著作権や肖像権のあるもので溢れている

年齢を問わず多くの人々が利用している動画共有サイトですが、子供たちがアニメや映画などを無許可でアップロードしてしまい、著作権侵害となるケースが起きています。動画の公開だけでなく、違法だと知りながらダウンロードすることも(個人で楽しむ範囲であっても)2年以下の懲役、または200万円以下の罰金(またはその両方)が科される犯罪行為となります。また、SNSで自分のプロフィール欄に有名人の写真を利用する、友人の写真や動画を許可なく掲載するといったことは肖像権の侵害に当たるので十分に気を付けましょう。

小・中学生が常に心掛きたいこと

▼人の作ったものを大切に持つ心を持つ

- ・ イラストや写真、文章、音楽、どのようなものでも著作権があります。自分以外の人の制作物に対する意識を育みましょう。

▼著作権や肖像権のあるものを無断使用しない

- ・ 映画や漫画、友人や著名人の写真など、著作権や肖像権のあるものは身近に溢れています。ネット掲載には許可が必要です。

▼著作権や肖像権などの知的財産権を知る

- ・ プロフィール欄にキャラクターや有名人の写真を使っていますか。知的財産権を正しく知り、尊重して行動しましょう。

参考

平成22年1月に改正著作権法が施行され、著作権を侵害したサイトと知りながらダウンロードすることは、個人的に楽しむ目的であっても違法(著作権の侵害)となります。

また、平成24年10月「違法ダウンロードの刑事罰化」が施行され、違法にアップロードされたと知りながらダウンロードした場合には、個人的に楽しむ範囲であっても違法(著作権の侵害)となり、2年以下の懲役または200万円以下の罰金(またはその両方)が科されることとなります。

政府広報オンライン <http://www.gov-online.go.jp/useful/article/200908/2.html>

8 その他の不適切な使い方

8-1 個人や学校などへの脅迫行為

嫌がらせを呼び掛ける投稿をして



嫌がらせのつもりで、日時・場所とともに「友人Qを暴行しよう」と、ネットの掲示板に投稿したR君。でも、**実行するつもりはまったくありませんでした。**

投稿者が特定され、地域にも多大な迷惑



その投稿を見た人が警察に通報したことから、警察は指定された日時とその場所をパトロール。R君の行った行為は、大きな問題となりました。

【解説8-1】 ネットやSNSなどへの書き込み、軽く考えないように

単なる脅しや悪ふざけで実行する気はなかったとしても、脅迫めいた書き込みは、犯罪となるおそれがあります。また、学校や駅などで事件を起こすといった、地域社会に大きな不安を与える書き込みも同様に犯罪となります。軽い気持ちで書き込むと、相手を深く傷付けるだけでなく、投稿者自身の傷にもなるのです。安易に考えがちなネットの匿名性ですが、基本的には、いつどこから書き込まれたのか調査でき、投稿した個人を特定できます。その時の感情に任せて書き込むのではなく、投稿前に落ち着いて内容を読み返すように伝えていきましょう。

小・中学生が常に心掛きたいこと

▼やって良いことかどうかきちんと考える

- ・ 誰かを傷付ける投稿がダメなのはもちろん、犯行予告のような書き込みは、冗談ではすみません。善悪の判断を！

▼ネットの特性を正しく理解する

- ・ 書き込んだ途端に多くの人に広まり、投稿者の特定も可能なのがネット。情報の発信には、責任が伴うことを理解しましょう。

▼犯行予告を見つけたら大人に連絡する

- ・ 身近な人・地域に対する危険な書き込みを見つけた場合は、できるだけ急いで保護者や先生などに連絡をしましょう。

参考

ネットや SNS など、脅迫めいたメッセージを送付した場合、次のような罪に問われる可能性があります。

<威力業務妨害罪>

刑法第 234 条には「威力を用いて人の業務を妨害した者は、3 年以下の懲役又は 50 万円以下の罰金に処する」と規定されています(威力業務妨害罪)。

<偽計業務妨害罪>

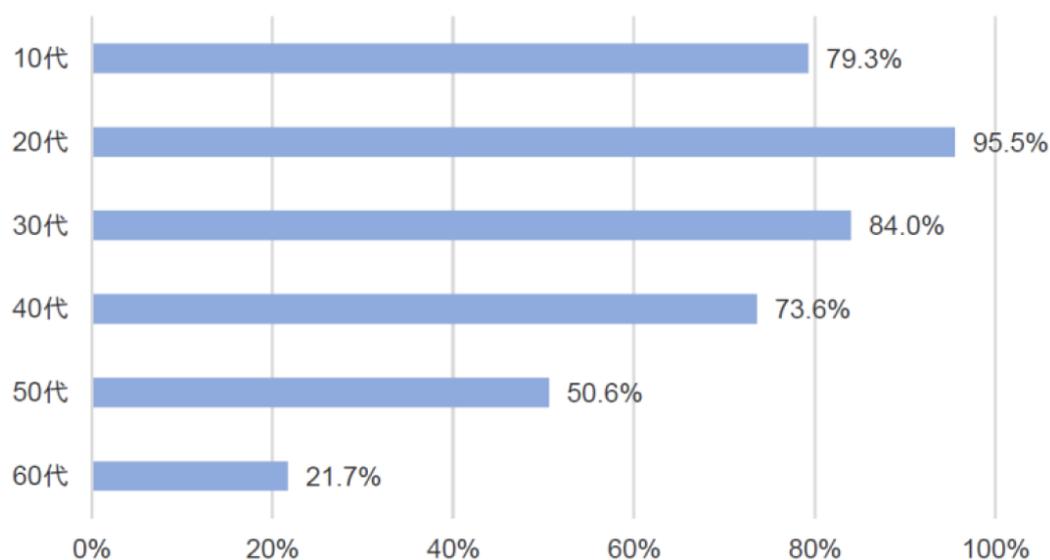
刑法第 233 条には「虚偽の風説を流布し、又は偽計を用いて、人の信用を毀損し、又はその業務を妨害した者は、3 年以下の懲役又は 50 万円以下の罰金に処する」(偽計業務妨害罪)と規定されています。偽計業務妨害罪は、嘘の情報を用いて人の業務を妨害したときに該当する罪で、秋葉原無差別殺傷事件の模倣犯がこれに相当します。

<脅迫罪>

刑法第 222 条には「身体・生命・自由・名誉又は財産に対し害を加える旨を告知して人を脅迫した者は2年以下の懲役又は 30 万円以下の罰金に処する」と規定されています(脅迫罪)。特定の人物を殺傷する予告をした場合は、これにあたります。

(参考) インターネットやスマホの利用に関するデータ

主なソーシャルメディアの利用率

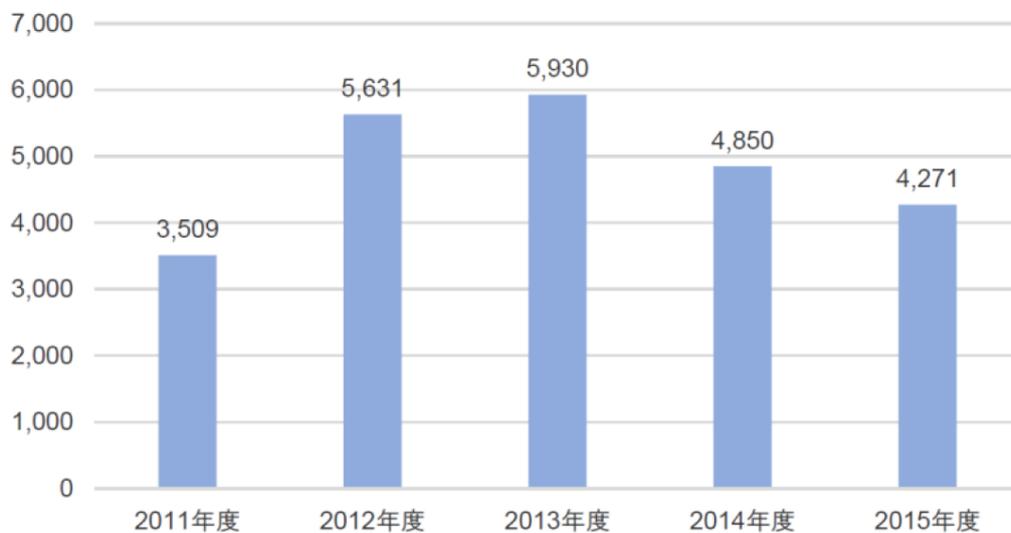


ソーシャルメディアの利用率は、若年層ほど高い傾向があります。主なソーシャルメディアのいずれかを利用している割合は、10代で79.3%にのびます。また、複数のソーシャルメディアを利用している割合も若年層ほど高い傾向があります。子供たちのコミュニケーション手段として定着しているソーシャルメディアですが、保護者としてもどのようなメディアを利用しているのか把握しましょう。

(参考)総務省「平成26年 情報通信メディアの利用時間と情報行動に関する調査」(平成27年5月)

http://www.soumu.go.jp/menu_news/s-news/01iicp01_02000028.html

オンラインゲームに関する相談件数



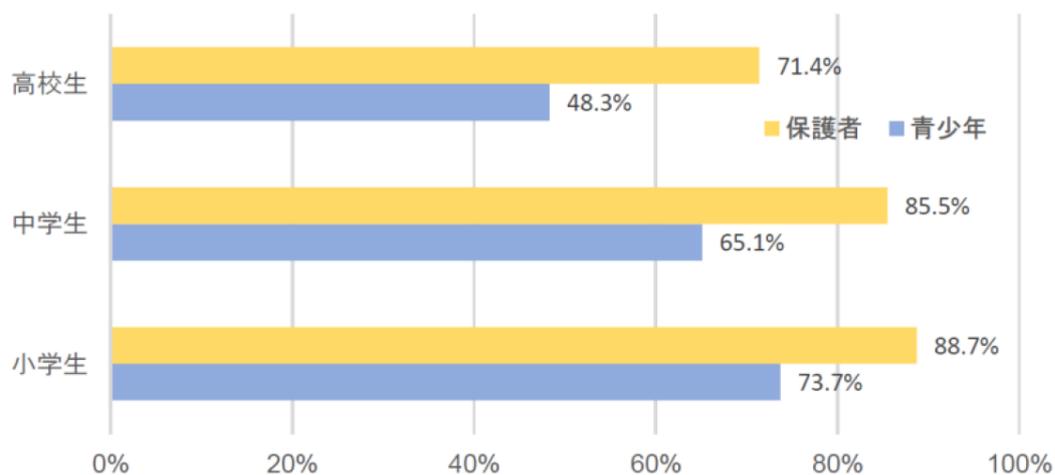
スマホのアプリやパソコンなどで遊べるオンラインゲーム。2015年度は4,271件と、前年度に比べて減少しました。それでも、国民生活センターに対して、年間で4,000件近い相談があります。気が付くと、思っていた以上に課金をしてしまっていたといったことがないように、意識を高めるとともに、子供の取り扱う端末の課金に関する設定を確認するなどして、トラブルを未然に防ぎましょう。

(参考)

独立行政法人国民生活センター「各種相談の件数や傾向・オンラインゲーム」(平成28年6月)

http://www.kokusen.go.jp/soudan_topics/data/game.html

家庭のルールに対する青少年と保護者のギャップ



インターネットの利用に関して家庭でルールを決めていると認識のある青少年と、保護者の間にギャップがあります。学校種が上がるほど、そのギャップは広がっています。上記グラフのように、中学生、高校生では、約20%の開きが、保護者と子供との間にあります。保護者としては、子供に対して家庭でのルールを定期的に話し合い、認識を高めていくことが大切です。また、年齢に応じて、ルールを変更していくことで、子供たちの理解も高まります。

(参考)内閣府「平成27年度青少年のインターネット利用環境
実態調査調査結果」(平成28年3月)

http://www8.cao.go.jp/youth/youth-harm/chousa/net-jittai_list.html

フィルタリングの設定方法

子供たちは、適切にスマホを取り扱えるだけの十分な知識・経験・判断力などを持ち合わせていない場合があります。特に低年齢の子供ほど、情報モラルの知識などが浅く、トラブルに巻き込まれる可能性があります。フィルタリングは、危険性のあるWebサイトへの閲覧制限やアプリの利用制限をするなどの機能があり、子供たちの不十分な知識・経験・判断力などを補うために大変有効です。フィルタリングの設定方法としては、「Webサイト」の利用と、「アプリ」の利用に対してそれぞれ行います。どちらの設定もすることで、抜け漏れがなくなり、子供たちが安全にスマホなどを取り扱える環境を作ることができます。

(1) Webサイトのフィルタリング方法

携帯電話会社には、利用者が18歳未満の場合(保護者が解除を申し出ない限り)フィルタリングの提供が法律で義務付けられています。Wi-Fiでもフィルタリングを有効にするには、スマホなどの契約時に以下サービスを申し込むことになっていますが、利用中の機器がサービスを受けているかどうか、あらためて確認しましょう。

「NTT docomo の場合」

spモードフィルタ、Web制限、キッズiモードフィルタ、iモードフィルタ

Webサイトや、iモードメニューサイトの閲覧制限が行えます。機種によって提供サービスが異なります。また、サービスによって子供の年齢などが考慮され、制限事項が異なります。Wi-Fi通信時の制限には、「ファミリーブラウザ for docomo」があります。

「au(KDDI) の場合」

安心アクセスサービス、安心アクセス for Android™

年齢や用途に合わせたWebサイトのフィルタリングが行えるので、違法サイトやアダルトサイトなどをブロックできます。サービスの申し込みは、EZwebのお客さまサポート/オプションや、auショップで行えます。

「SoftBank の場合」

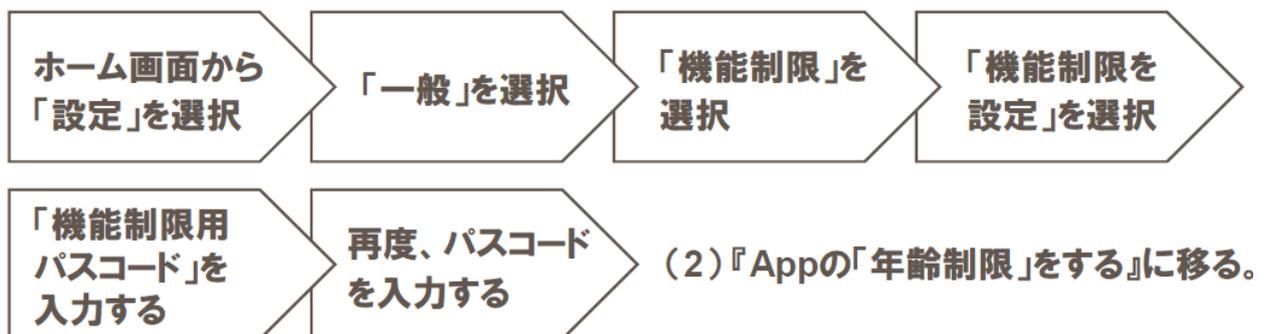
ウェブ安心サービス(フィルタリングサービス)

不適切なWebサイトへの年齢に応じたアクセス制限、有料コンテンツ購入時の暗証番号設定ができます。サービスの申し込みは、My SoftBank、ソフトバンクショップ、ソフトバンク製品取扱店で行えます。Wi-Fi通信時の制限には「Yahoo!あんしんねっと for SoftBank」などがあります。

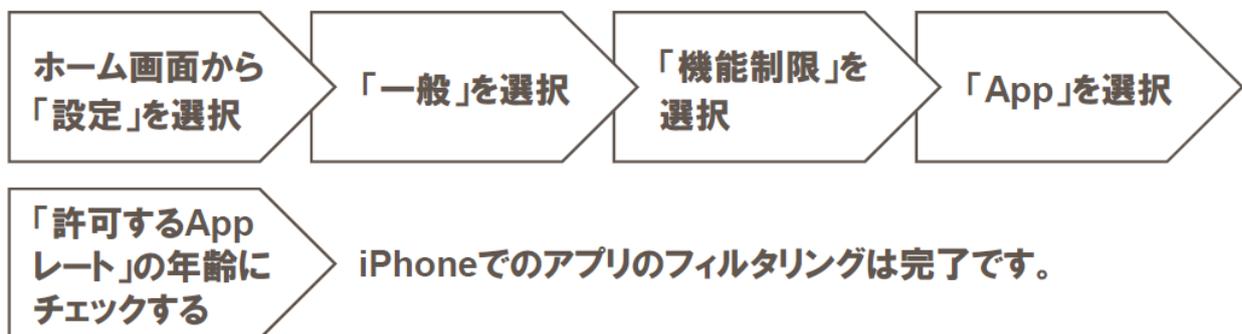
(2) アプリのフィルタリング方法

スマホのアプリは、Webサイトのフィルタリングでのコントロールはほとんどできません。そのため、別途アプリに対する設定が必要です。設定方法はスマホのOS(基本ソフト)で異なるため、ここでは、iPhoneとAndroid端末について、アプリのフィルタリングの方法をご紹介します。

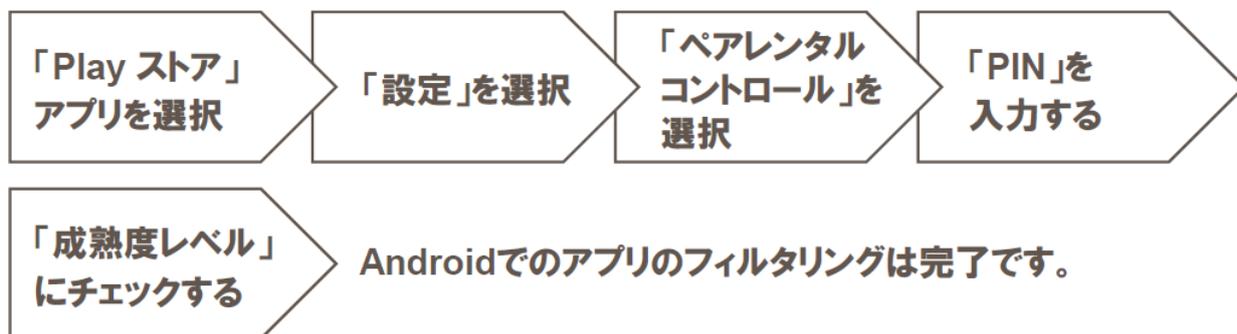
iPhone の場合



(2) Appの「年齢制限」をする ※Appは、iPhoneのアプリのことをいいます。



Android の場合



※設定方法は、OSのバージョンアップなどにより、変更される可能性があります。フィルタリングの方法は、保護者自身が自分の端末でも確認をしながら、進めていきましょう。