

## 参考・引用

- インターネット上の各種情報、特にQ&Aサイト
- 国民生活センターHP <<http://www.kokusen.go.jp/topics/internet.html>>
- 消費者庁HP <<https://www.caa.go.jp>>
- 総務省HP <<https://www.soumu.go.jp>>
- 経済産業省HP <<https://www.meti.go.jp>>
- 警察庁HP <<https://www.npa.go.jp/cybersafety/>>
- 警視庁HP <<https://www.keishicho.metro.tokyo.jp>>
- 文部科学省HP <<https://www.mext.go.jp>>
- 文化庁HP <<https://www.bunka.go.jp>>
- 内閣府HP <<https://www.cao.go.jp>>
- 東京都HP <<https://www.tokyohelpdesk.metro.tokyo.lg.jp/consult/jirei/>>
- 各自治体
- 独立行政法人情報処理推進機構HP <<https://www.ipa.go.jp>>

企画・発行 株式会社NTTドコモ モバイル社会研究所  
eメール : [msri-inq-ml@nttdocomo.com](mailto:msri-inq-ml@nttdocomo.com)  
Webサイト : <https://www.moba-ken.jp/>



# 安心して使っていただくための スマートフォンガイドブック

## 上手に使おうみんなのスマホ

～コンパクト版～



### スマートフォンを 安全に楽しく使うために

中高生の間でさかんに使われているスマートフォン。今や、中高生のコミュニケーションの中心を占めるとまで言われています。パソコンと携帯電話の特徴をあわせもつと言われているスマートフォンは、いろいろなアプリをダウンロードすることで、ゲームができたり、チャットや通話ができたり、動画を見たり、写真や動画を加工して、カンタンにSNSなどにアップできたりと、その活用範囲が広がっています。

生活に溶け込み、一日中手放せない人も多いスマートフォンですが、使い方を一歩誤ると、その便利で楽しい機能が大きなトラブルを招くこともあります。近ごろは情報が広がるスピードが速くなっており、一度ネット上で広まってしまったものを削除するのは非常に困難です。また、新しいサービスも次々と登場し、それを悪用した事件も多発しています。中高生が、被害にあうだけでなく、加害者になるケースも増えています。さらに、使いすぎによるさまざまな悪影響も指摘されています。

スマートフォンによるトラブルにはどんなものがあるのかを知ること、トラブルを招かない安全な使い方やトラブルが起こってしまったときに被害を最小限にする方法を身につけていきましょう。

本冊子は【トラブル事例に学ぶスマートフォン安心ガイド】より大切な事例をいくつか抜粋し掲載しています。ぜひ【トラブル事例に学ぶスマートフォン安心ガイド】をあわせてご覧ください。

### スマートフォンのさまざまな用途と 注意する点

#### 学ぶ

辞書ですぐ調べる、語学のアプリでいろいろな言葉を学習、電子書籍で世界の名作を手軽に、いつでもニュースにふれる、動画で分かりやすく学ぶ



ネットの情報は、常に正しい情報とは限りません。簡単・便利だからといって、すべてをそのまま信じないようにしましょう。

#### 暮らす

外出時の地図や時刻表、天気予報、ショッピング、料理の作り方、スケジュール管理



特にショッピング時には、詐欺サイト、不正アクセスによる乗っ取りに注意。ウイルスによる個人情報流出や詐欺の被害も……。

#### 遊ぶ

ゲーム、同じ趣味の仲間探し、写真の加工や動画編集、音楽や動画の視聴、音楽演奏や作曲



有料サービスでの使い過ぎ、熱中して他のことが手に付かない、ゲーム課金による高額請求に注意

#### コミュニケーション

メッセージ、メール、写真/動画共有、SNS



ネットいじめが起こったり、情報/写真/動画が想像以上に大きく広がったり、出会い系サイトでの被害、違法ダウンロードなどの犯罪の可能性も



## スマートフォンの利用、これだけは気をつけよう！



スマートフォンを利用する際は、利便性だけでなくリスクの可能性もよく知り、家庭や学校などで「気をつける面」を話し合しましょう。トラブルにあわないために、基本的な仕組みを知り、家庭などで使用のルールを決め、スマートフォンを安全に使うための機能やサービスも活用してください。



### ルールやマナーを守る

歩きながらのスマホ、自転車を運転しながらのスマホ、どちらもルール違反だけでなく、大きな事故につながります。他にも、公共機関や交通機関が定めたルールや、社会が求めるマナーを守ることが大切。ルールやマナーを守るのは、他人のためだけでなく、スマートフォンを使う人自身を守ることになるのです。

### 気軽なコミュニケーションだけに十分注意

いつでも、どこでも、だれとでもコミュニケーションが可能。だからこそ危険や罠もいっぱい。被害者だけではなく、加害者にもなることをいつも意識しましょう。

### 時間とお金を使い過ぎない

いつでもどこでも、ゲーム、SNS、動画などを楽しめます。同時に「いつまでも」熱中できてしまうので、時間とお金の使い過ぎには十分注意。自分に許された時間と金額の中で楽しみましょう。

### トラブルにあったらすぐに相談

いくら注意していても、トラブルにあう可能性があります。お金を払って無理に解決しようとしたり、ひとりで悩み続けるようなことをやめ、すぐに家族や学校に相談しましょう。

### セキュリティを常に意識する

スマートフォンやインターネットの世界で、いつも話題になる「セキュリティ＝安全性」。広く世界に開かれ、誰でもが気軽に使えるスマートフォンは、その分悪事や犯罪などに利用されやすい面もあります。悪意のある人々が、スマートフォンを通じて、利用者の弱みを狙っていることをいつも意識しておきましょう。

### 怪しいサイトにはアクセスしない

人気サイトに似せたサイトや、詐欺を目的にしたサービスも多くあります。そんなサイトへアクセスすると、ウイルスに感染したり、個人情報盗まれたり、金銭的な被害にあってしまいます。怪しいサイトにはアクセスしないようにし、商品やサービスの購入も避けましょう。

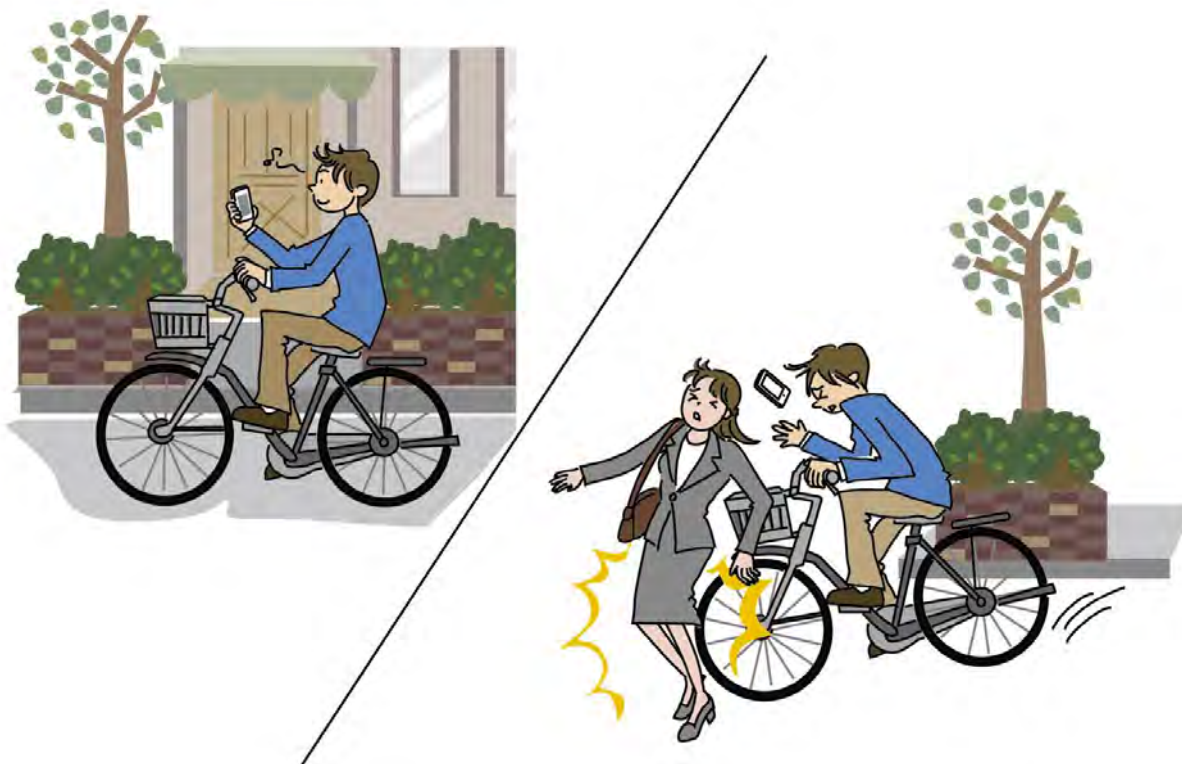
### スマートフォンを安全に使うための機能とサービス例

- 出会い系サイトなどへのアクセスを制限する「フィルタリング機能」
- 迷惑電話・迷惑メールから守るための「電話・メール制限」
- アプリの起動・インストールやWi-Fi通信を制限する「機能制限モード」
- ウイルスアプリ・メールや危険サイトを検出する「スキャン機能」

### 事例 1 「トラブル事例に学ぶスマートフォン安心ガイド」事例33より

## 自転車の乗りながらスマホ操作。 歩行者に気がつかず、衝突事故に。

自転車に乗りながら、スマートフォンでSNSをチェックしたり、動画を見たりしていた男子高校生のAくん。ふと目を上げると女の人の後ろ姿が見えたが、ブレーキが間に合わず思いっきり衝突。相手に大ケガを負わせてしまい、多額の賠償金を支払うことになってしまった。



### 解説

#### 自転車に乗りながらのスマートフォン操作は危険。

自転車乗車中にスマートフォンを手に持って通話したり、画面を注視することは、非常に危険です。自分だけでなく、他人にも大けがをさせる危険性があります。

自転車の危険運転による事故では、未成年でも多額の賠償金を請求されることもあります。

みんながやっているから……という言い訳は通じません。一人ひとりが危険性を認識して、絶対にやらないという意識が必要です。

スマートフォンの操作や通話は必ず自転車から降りて、止まってから安全な場所で行いましょう。自転車に乗りながらの携帯電話（スマートフォンを含む）利用は、多くの地方自治体が道路交通法施行細則/道路交通規則で禁止しており、これに違反した場合は道路交通法上の罰則の適用対象となります。



### ここがポイント

- ✓ 自転車に乗りながらのスマートフォンは、大きな事故につながる可能性がある。
- ✓ 自転車の危険運転による事故では、多額の賠償金を請求されることもある。
- ✓ 自転車に乗りながらの携帯電話（スマートフォンを含む）の使用は、多くの地方自治体が道路交通法施行細則/道路交通規則で禁止しており、これに違反した場合は道路交通法上の罰則の適用対象となります。

スマートフォンは自転車を降りてから閲覧・操作しましょう。



### 事例 2 「トラブル事例に学ぶスマートフォン安心ガイド」事例6より

## ふざけた画像をつぶやきサイトに投稿。大迷惑行為として、嚴重注意に。

つぶやきサイトにふざけたネタ画像をアップして楽しんでいた男子中学生のAくんたち。ウケを狙うために内容はだんだんエスカレートし、危険なことや人に迷惑をかけるいたずらをするようになった。ついには駅のホームから線路に降り、記念撮影した写真をつぶやきサイトにアップ。写真はすぐにネット上に広がり、Aくんたちの身元も特定された。鉄道会社にも通報され、後日、危険行為をして迷惑をかけたと嚴重に注意を受けた。



### 解説

#### ウケ狙いのつもりでも、一歩間違えば命の危険も。

線路に立ち入るという行為は、電車の遅延や人身事故など重大な事態に陥ることもあります。ウケを狙うために、危ないことをしたりいたずらをしているところなどを撮影する行為は、とても危険で迷惑です。軽いいたずらのつもりでも、一歩間違えば大ケガや命に関わるような事故も起こりかねません。また、場合によっては犯罪行為と見なされたり、損害賠償を請求されたりすることもあります。

危険行為や迷惑行為をしないことはもちろんですが、そのシーンを写真や動画に撮ってネットにアップすることもやめましょう。ネット上に写真や動画が拡散すると、写っている内容や利用しているサービスのアカウントから名前などのプライベートな情報まで公開される危険性があります。

一度ネット上に広まった写真などを完全に消すことは困難です。ネットに写真などをアップする際は、人に迷惑をかけないか、個人情報が含まれていないかということを確認しましょう。

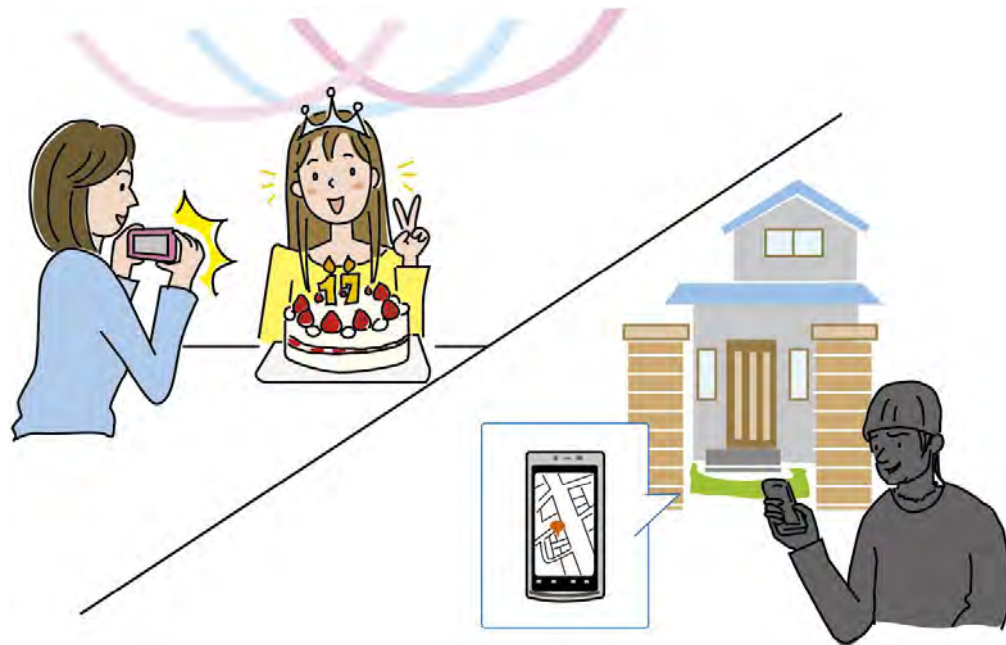
### ここがポイント

- ✓ 自分たちは悪ふざけのつもりでも、自分たち自身が危険だけでなく、社会に重大な影響を及ぼす迷惑となる場合がある。
- ✓ ネット上にアップした写真や情報は、不特定多数の人の目にふれ、自分の意図に反して広がってしまう可能性がある。
- ✓ 一度流出した写真や個人情報などは、半永久的にネット上に残ることを十分認識する。

### 事例 3 「トラブル事例に学ぶスマートフォン安心ガイド」事例19より

## 写真アップで、ストーカーが居場所を特定。家の前までやってきた。

女子高生Aさんは、元彼がストーカーになり付きまといなどの被害を受けたので、引っ越すなどして関わり合いを断つようにしていた。あるときAさんは自宅で行われたバースデーパーティの写真撮影し、スマートフォンでSNSにアップした。するとSNSを見たAさんの元彼が、写真の位置情報を確認して自宅を特定。自宅前から「いま家の前にいる」というメールを送信し、それを見たAさんの背筋は凍りついた。



### 解説

#### スマートフォン撮影の写真に「位置情報」が含まれることも。

スマートフォンで撮影した写真のデータには、端末のGPS機能により、撮影した場所の緯度経度情報が含まれる場合があります。位置情報が含まれたまま不用意にSNSなどにアップすると、第三者がその情報を確認して撮影場所が特定されてしまう危険性もあります。

SNSの初期設定では、「すべての情報を公開する」となっていることが多いので、登録の際に必ず「何の情報をどこまで公開するか」ということを検討し、不用意に情報を公開しないようにしましょう。

また、自分がアップしなくても、他の人が「あなたが写っている位置情報付の写真」をアップしてしまう可能性もあります。さらにリンクやタグ付けにより、自分が想定している以上の範囲に写真や位置情報が公開されてしまう場合もあります。ネット上のサービスへ写真をアップする場合は、様々なリスクがあることを自覚しておきましょう。



### ここがポイント

- ✓ 写真データに位置情報(GPS情報)を記録する設定は普段利用時はOFFにする。必要な時だけONにする。
- ✓ SNSでは、写真以外にも住所、電話番号、家族構成、不在情報等の公開には注意する。
- ✓ 住所などの情報が流出すると、ストーカー行為や脅迫行為などに悪用される危険性がある。

### 事例4 「トラブル事例に学ぶスマートフォン安心ガイド」事例22より

## IDとパスワードの使い回しが原因でプリペイドカードの残高がゼロに。

男子中学生のA君、保護者の許可を得て、スマホのゲームサイトで、有料アイテムを購入していた。使っていたのはコンビニで購入したプリペイドカード。お年玉でまとめて1年分を買っておいた。ある日、追加アイテムを購入しようとする、使った覚えがないのに、残高がゼロになっていた。

原因は、ゲームサイトと同じIDとパスワードでアクセスしていたSNSから、IDとパスワードの情報が流出。A君のIDとパスワードを入手した犯人が、ゲームサイトへ不正ログインして、プリペイドカードの残額をすべて使ってしまったのだ。

ゲームサイトとSNSのパスワードを違うものにしていれば、防ぐことができたかも……。



### 解説

#### IDとパスワードの使い回しは絶対にしない。

サイバー犯罪者が、個人情報を盗み取る方法はさまざまです。

- ・ SNSなどのサービスに不正アクセスし、大量のデータを盗み出す
- ・ ウイルス等を使い、個人のパソコンやスマホから不正入手
- ・ 偽ショッピングサイト等から不正入手
- ・ Wi-Fiフリースポットで

こうして、不正入手した個人情報を使って、別サイト(ショッピングサイト等)に不正ログインします。本人を装い、買い物をしたり、ポイントを利用したりします。最近では、ショッピングサイト側にクレジットカード情報が保存されているので、ログインさえできれば、簡単に決済されてしまいます。

その他、他人に気軽に教えてしまったものや、WEBサービス提供企業からの内部流出したものも、サイバー犯罪者によって使われる可能性があります。

パスワードが流出していないからといって、安心はできません。簡単な類推しやすいパスワードを使っていると、ID(多くの場合はメールアドレス)だけ分かれば、サイトに不正ログインできるのです。また、さまざまなサイトで同じID/パスワードを使っていると、ひとつのサイトから漏えいしたID/パスワードで、他のサイトにも不正ログインされてしまいます。



### ここがポイント

- ✓ 類推しやすいパスワードを使わない  
例：12345 09876 password qwerty asdfgh 誕生日
- ✓ 同じパスワードを使い回ししない
- ✓ 定期的にパスワードを変える
- ✓ 使っているWEBサービスへの不正アクセスが発覚したら、パスワードをすぐに変更する
- ✓ 怪しいサイトにはアクセスしない



### 事例5 「トラブル事例に学ぶスマートフォン安心ガイド」事例27より

## 不正アプリをインストールしたら、アドレス帳のデータが流出。

男子高校生のAくんは、SNSで紹介されていた「電池長持ち」などと利便性をうたうアプリを、インストール前にアプリの権限をよく確認せずにインストールボタンを押した。  
アプリを起動すると、「お使いの端末は未対応のためご利用いただけません」というエラーメッセージが表示された。  
Aくんがインストールしたのは、アドレス帳の個人情報を盗み取る不正アプリだった。



### 解説

## 必ずアプリの権限を確認してからインストールしよう。

マルウェア（悪意のある不正なアプリ）は、スマートフォンに登録されているアドレス帳の情報や位置情報などを外部に送信してしまうものや高額請求画面が表示されるものなどさまざまです。

そのアプリを削除すれば不正な動作はなくなりますが、流出してしまった個人情報などのデータは回収できません。

また、アプリ名も「電池改善アプリ」「電話改善！」など気を引くような名前をつけています。

マルウェア（悪意のある不正なアプリ）による被害にあわないためにも、必ずアプリの権限を確認し、不審なアプリのインストールはやめましょう。

### ここがポイント

- ✓ アプリをインストールする前にアクセス許可（個人情報、電話発信、位置情報、ネットワーク通信、SNSメッセージ送信）を求めるアプリは必ず慎重に確認する。
- ✓ 疑問に思う項目の許可を求められた場合には、そのアプリのインストールを中止する。
- ✓ 各携帯電話会社が運営するマーケットなど信頼できる公式アプリマーケットからアプリをインストールする。
- ✓ 信頼できるセキュリティ対策アプリを導入して、パターンファイルを最新の状態に保っておく。
- ✓ マルウェア（悪意のある不正なアプリ）が見つかったらすみやかにアンインストールする。