シニアのための デジタル安全ガイド

便利なスマートフォンは、シニア世代の強い味方。
でも、わからないこともたくさんあって、不安になっていませんか。
便利さの裏には、詐欺やトラブルなどの危険があることも事実です。
「スマホとどう安全につき合うか」という心構えで、
消費者被害から身を守る方法を、いっしょに考えましょう。

デジタル被害に遭わないための4カ条

1 簡単に決済をしない!

信用できる相手か、誰と取引しているかを見極めるために、**情報源を確認しましょう**。

2 迷ったら、すぐに操作をやめて!

おかしいなと感じたら、**その場で操作をやめて、インターネットの接続（電源）を切りましょう**。

3 大事な情報は、絶対に人に教えない!

パスワードやクレジットカード番号は、**大切な財産を守るカギ**です。
誰にも教えてはいけません。ノートに書いて、家で大切に保管しましょう。

4 困ったら、ひとりで悩まずに相談を!

少しでも不安になったり、おかしいなと思ったら、すぐに**身近な人や相談窓口に連絡**しましょう。**恥ずかしがることはありません**。

北海道消費者教育
PRキャラクター
「かしこしか」

＼信頼できる相談窓口／

困ったときにはすぐに連絡を!

北海道立消費生活センター

050-7505-0999

消費生活相談専用　平日9:00～16:30 ※土日・祝日・年末年始（12月29日～1月3日）は休館です。

〒060-0003　札幌市中央区北3条西7丁目　北海道庁別館西棟
【アクセス】JR：札幌駅南口から徒歩10分／地下鉄：南北線・東豊線「さっぽろ」駅から徒歩10分

https://www.do-syouhi-c.jp/

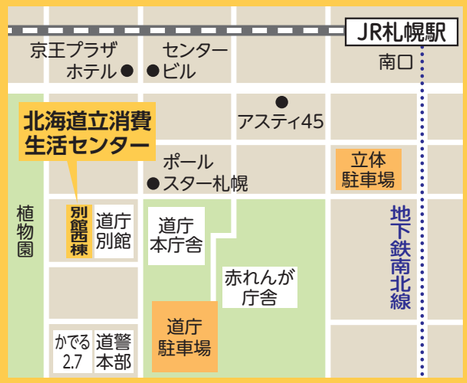
消費者ホットライン

188（いやや）「嫌や!」泣き寝入り

※全国共通の電話番号。お近くの消費生活相談窓口をご案内します。

警察相談電話

#9110（毎日24時間受付）



編集・発行／北海道立消費生活センター（指定管理者：一般社団法人 北海道消費者協会）
〒060-0003 札幌市中央区北3条西7丁目 北海道庁別館西棟　TEL:011-221-0110　FAX:011-221-4210

2025年12月発行

北海道立消費生活センター

スマホとのつきあい方、大丈夫?

スマホは、ご家族や友だちとの連絡、趣味や生活を豊かにする便利な道具です。
でも、その便利さの裏には、思わぬ落とし穴もあります。
「自分は大丈夫」と思わずに、まずは**トラブルの芽がないかチェック**してみましょう。
このガイドは、もしもの場合に備え、**安全にデジタルライフを送るためのお守り**です。

北海道消費者教育
PRキャラクター
「かしこしか」

トラブル予防チェックシート

以下の項目に当てはまるものがいくつありますか。「はい」が多いほど注意が必要です。

- ☑ 知らない人からのメールやメッセージに返信することがある。
- ☑ 「無料」「限定」などの言葉にひかれて、すぐにダウンロードや登録をすることがある。
- ☑ スマホの「設定」は、よくわからないのでほとんど変えていない。
- ☑ パスワードは、誕生日など覚えやすいものを使っている。
- ☑ お店や駅などで、いつの間にかフリーWi-Fiに接続していることがある。
- ☑ 顔写真や自宅周辺の建物、風景などをSNSに投稿することがある。
- ☑ 「すぐに連絡をください」というメッセージや電話に対し、焦って対応することがある。
- ☑ IDやパスワードを他人に入力してもらうことがある。

知っておきたいスマホ用語

用語	意味
アプリ	スマホに入れる「ソフト」や「プログラム」のこと。地図や音楽、SNSなどの機能があります。
Wi-Fi(ワイファイ)	無線でインターネットにつなげる回線のこと。自宅やコンビニ、カフェなどにあります。
SNS(エスエヌエス)	知人や不特定多数の人と情報のやりとりができる交流サイト。Facebook(フェイスブック)など。
アカウント	IDとパスワードをセットにしたもの。あなたを特定する「名札」の役割があります。
ユーザーID(アイディー)	インターネット上のサービスで使う「名前や番号」。IDは登録したら変更できない場合があります。
パスワード	IDとセットで使う、カギの役割をする文字や数字のこと。他人に知られてはいけません。
ダウンロード	インターネット上にあるデータ(アプリや写真など)をスマホに取り込むこと。
バックアップ	大切な写真や連絡先を、スマホとは別の場所にコピーして保存すること。
スクリーンショット	スマホの画面を画像として保存すること。略して「スクショ」ともいう。

外出先で個人情報が漏れないよう注意しましょう

フリーWi-Fi(ワイファイ)には落とし穴も

街中にあるカフェや駅、お店などで使える「**フリーWi-Fi**」。
とても便利ですが、誰でも使える分、注意が必要です。
フリーWi-Fiにつなぐと、あなたのスマホとインターネットのやり取りを盗み見され、**個人情報が漏れてしまう危険**があります。また、中には、悪意のある「なりすましWi-Fi」の可能性もあります。

接続の安全を守るために

1 重要な操作は避ける

外出先でフリーWi-Fiを使うときには、**クレジットカード番号を入力するなどお金に関するやり取り**は避けましょう。

2 接続先をしっかり確認する

Wi-Fiの名前が似ていても、**公式サイトやお店の案内**で正しい名前かどうかを必ず確認しましょう。

3 自動接続設定をオフにする

一度つないだWi-Fiに、**次回から勝手に接続されないよう設定をオフ**にしておきましょう。使わない時はWi-Fiの機能を切っておくのが安心です。

大切な情報を入力するときは、
自宅のWi-Fiなど安全な回線を使いましょう!

2

カメラを安全に使う

位置情報（GPS）など カメラの設定を確認しましょう

写真一枚で「居場所」がバレる!?

スマホで写真を撮ると、その写真に**「どこで撮ったか」という位置情報**が自動で記録されていることがあります。この情報が付いたまま、写真をSNSなどに投稿すると、**自宅やよく行く場所の情報が悪い人に知られてしまう危険**があります。犯罪やトラブルに巻き込まれないためにも、写真の位置情報をうっかり公開しないよう注意しましょう。

写真を撮る&載せるときの注意点

1 位置情報の設定を確認しましょう

写真に位置情報が記録されないよう、スマホの**カメラアプリの設定**で**「位置情報サービス」をオフ**にすることをおすすめします。

2 無断で他者の写真などを載せない

ご家族や友人など身近な人であっても、**本人の許可なく**その人が写った写真をネットに載せてはいけません。これは**肖像権の侵害**にあたります。また、他者の**絵や写真、音楽などの著作物**を勝手に使って載せてはいけません。これは**著作権の侵害**にあたります。

3 居場所や個人が特定できる写真は要注意

家の外観や表札など**居場所が特定されやすい写真**や、**誕生日やパスワードなど大事な個人情報**が含まれる写真は投稿しないようにしましょう。

写真を投稿する前に、
写り込んでいるものや位置情報をチェック!

3

悪質なアプリを避ける

不正なアプリによる 消費者被害が増えています

怪しいアプリでトラブルに!

アプリは便利な一方で、中には**あなたの情報を盗んだり、不正な請求をしたり**する**悪質なアプリ**も紛れ込んでいます。「ウイルスに感染しています!」などと画面に警告を出して不安をあおり、**怪しいアプリ**を入れさせようとしたり、**有名なアプリに名前を似せて**ダウンロードさせようとするニセアプリも存在します。不正アプリの手口を知って、トラブルに巻き込まれないよう注意しましょう。

不要なファイルを削除してスマホの空き容量を増やせる「Cleanup（クリーンアップ）」などのアプリには、個人情報の搾取を目的としているものや「危険」などの警告をして詐欺アプリに誘導するものなどがあるので注意が必要です。

安全なアプリの選び方

1 公式のアプリストアからダウンロードする

App Store（アップ ストア）やGoogle Play（グーグル プレイ）ストアといった公式アプリストアを使って探しましょう。ウェブ検索からのダウンロードは絶対にやめましょう。

2 開発元やレビューを確認する

アプリを作った会社（開発元）が信用できるか、実際に使った人の**レビュー（評価）を読んで**不自然な点がないかチェックしましょう。

3 「許可しますか?」は慎重に

アプリに登録する際、アプリの目的と関係のない情報（連絡先、写真など）へのアクセスは**安易に許可をせず、「スキップ」「次へ」「許可しない」を選択**しましょう。

不正アプリは、個人情報やお金を狙っています。
公式アプリストアを確認してからダウンロード!

4 SNSの被害に遭わないために

SNS広告の落とし穴! パターンを知って防ごう

SNS広告による消費者被害のパターン

Facebook(フェイスブック)やLINEなどのSNSには、あなたの興味に合わせた広告がたくさん出てきます。しかし、そうした**広告を悪用した消費者被害や詐欺**が増えています。

1 必ず儲かる投資話×ディープフェイク

生成AIで作成した本物そっくりの**有名人や専門家などの動画で「投資で大儲けできる」**と誘います。

LINEグループに誘導し、最終的に大金をだまし取ろうとします。

2 ニセ通販サイト

有名ブランドや希少性のある商品から**ニセ通販サイトに誘導**。「クレジット決済ができない」などと言って何度かやりとりを重ね、**個人口座にお金を振り込ませます**。

3 定期購入

「定期縛りなし」という広告を見て「1回限り」と思って注文したところ、**実は定期購入の契約**だったという消費者被害があります。「**定期縛りなし=いつでも解約できる定期購入」として表記している可能性**があるので注意が必要です。

ネット通販で注文する際に、契約条件が記載されている「最終確認画面」で代金等の支払条件や解約条件などを確認しよう!

ダークパターンに注意!

ダークパターンとは、消費者が気づかないうちに不利な判断・意思決定をしてしまうよう誘導するウェブデザインなどを指します。

❶強制
ユーザー登録や個人情報を強制的に要求してくる

❷インターフェース干渉
事業者に都合のよい選択肢を目立たせている

❸執ような繰り返し
事業者に都合の良い設定に変えるように何度も要求してくる

SNS型犯罪はあなたの身近に潜んでいます

SNSを利用した犯罪で被害に遭うケースが増えています。

ロマンス詐欺に注意!

親密な関係を装う
外国の軍人や医師など、魅力的なプロフィールでSNSからメッセージを送ってきます。

▶

お金を無心する
信頼関係を築いた後、「日本に行くための旅費がない」「家族が病気」など、同情を誘う話で送金を求めてきます。送金したら二度と連絡が取れなくなります。

警察官をかたる電話に注意!

警察手帳や逮捕状で信用させる
電話からLINEのビデオ通話に誘導され、警察手帳や逮捕状を見せて警察官だと信用させます。

▶

個人情報や金銭を要求する
信用させて個人情報を聞いたり、捜査の一環として口座を調べると言って、金銭を振り込ませたりする手口がみられます。

被害に遭わないための心得

1 個人情報は絶対に教えない

パスワードやクレジットカード番号、免許証などのコピーは、SNSやメールで**他人に送ってはいけません**。

2 「お金」の話が出たら要注意

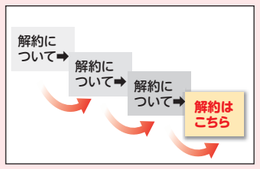
SNSで知り合っただけの人が**電子ギフトカードや送金を求めてきたら**、それは詐欺です。**すぐに家族や警察に相談しましょう**。

3 なりすましに気をつけて

取引のある企業や家族・知人からのメッセージであっても、不自然な内容だったり、**連絡先や引き落とし口座の変更を求められたら、URLをクリックしないこと**。**電話で確認**するか、類似の被害がないかを**ホームページで調べましょう**。

SNSで知り合った相手にお金は送らない!

❹妨害
解約など事業者に都合の悪いことを妨害しようとする



❺こっそり
最後に手数料を追加する、お試し期間後に自動で定期購入に移行する

❻社会的証明
ウソの感想や行動で好評を装い、予約を誘導する

❼緊急性
ウソのカウントダウンなどの表示で「いま買わなければ」と焦らせる