スマートフォン
iPhone基本編

スマートフォンを
安全に使うための
基本的なポイントを知ろう

令和7年4月

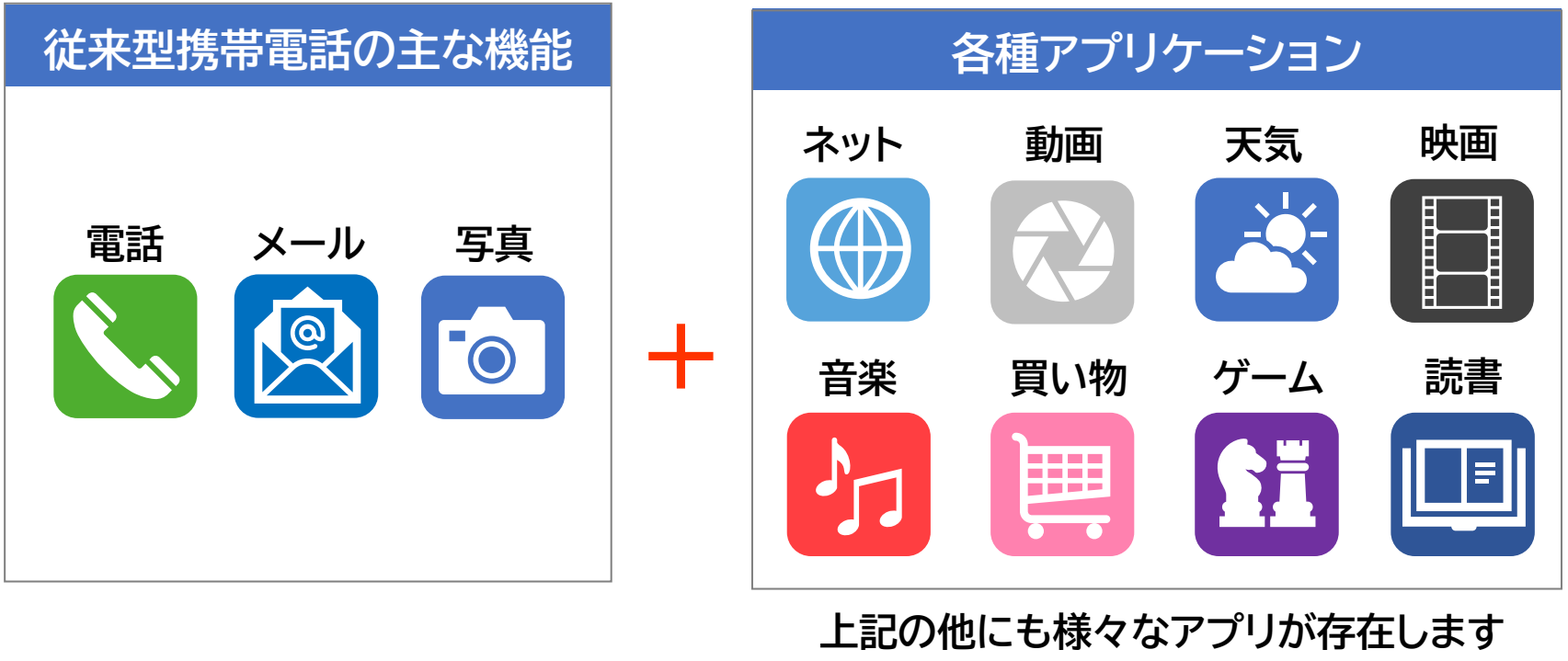
目次

目次

1 スマートフォンは危険なもの？

1-A スマートフォンとは

スマートフォンとはパソコンのような機能を併せ持った携帯電話機の総称です。
従来の電話機よりも多機能かつ高機能なため「smart（賢い）」＋「phone（電話）」を合わせて「スマートフォン」と呼ばれています。従来の携帯電話とは異なり、アプリケーションと呼ばれるソフトを取り込むことでインターネット閲覧、ショッピング、読書、映画視聴等、様々な機能を追加し、利用者の好みに応じで機能を拡張することができます。



1-B スマートフォンに入っている大量の情報

スマートフォンの中には大量の個人情報が格納されますので、適切な方法でインターネットを介した被害から身を守りましょう

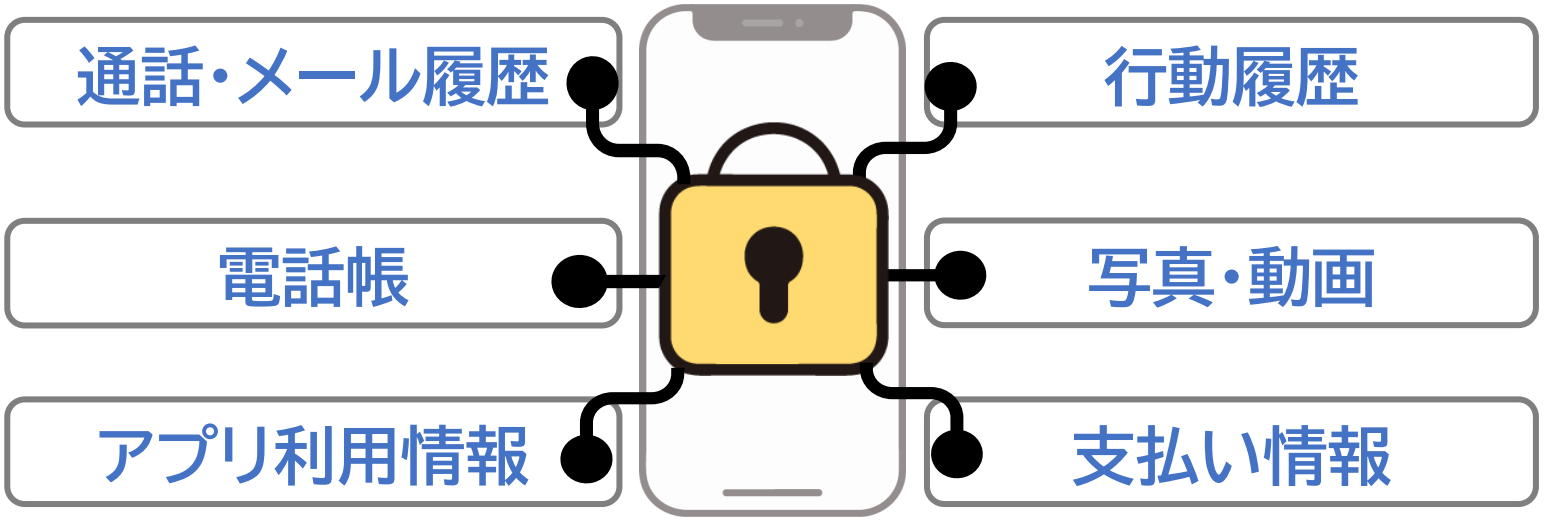
スマートフォンに保存された情報は適切に守ることが必要です。
正しく使うことができればスマートフォンは危険なものではありません。

2 パスワードは安全に管理しましょう

2-A パスワードの重要性について

「パスワード」を適切に設定することでスマートフォンを利用したり、インターネット上の様々なサービスを利用する際、第三者の不正利用を防ぐことができます

以下のものはパスワードを設定しましょう



上記以外にも様々な情報がパスワードによって守られています

2-A パスワードの重要性について

パスワードは自分の財産を守る「鍵」です

家や財産を守る鍵の役割＝パスワード

鍵（＝パスワード）を盗まれてしまうと、第三者が家（＝機器やサービス）に侵入し、情報を盗むことができてしまいます。パスワードは人の目に触れないところで保管し、大切に扱いましょう。

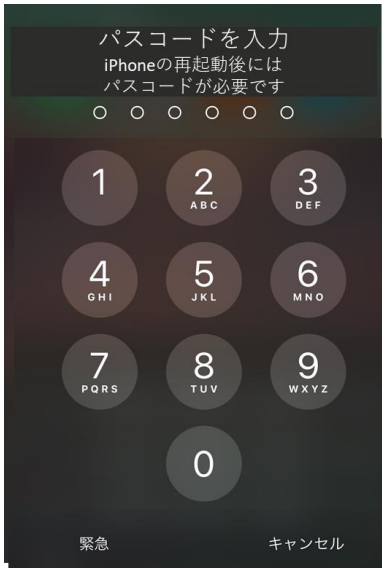
2-B パスワードの種類

※機種によって機能が異なります

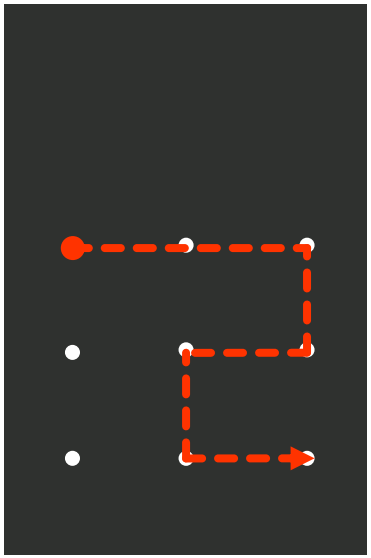
パスワードには様々な種類があります

❶ 画面ロックのパスコード

暗証番号(数字)



パターン認証

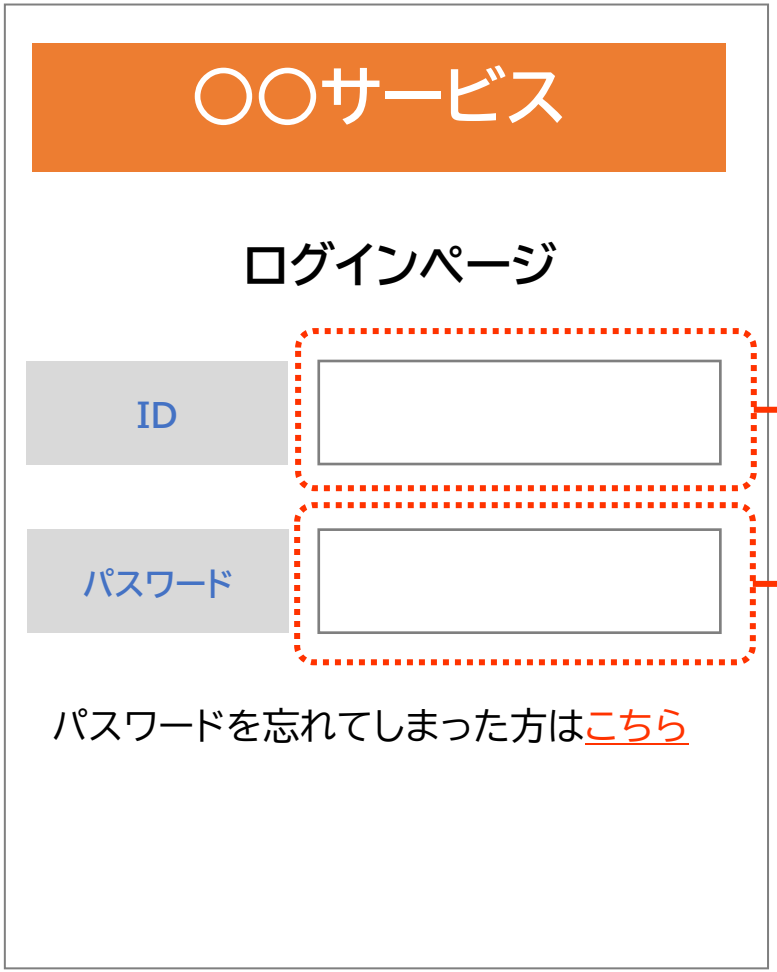


※その他、指紋認証や顔認証なども利用できます。

2-B パスワードの種類

パスワードには様々な種類があります

❷ アプリやサービス利用時のパスワード



IDとは、自身で設定した
メールアドレスやサービスから
個別に付与されるもので、
様々なケースがあります。

パスワードとは、利用者が本人である事を証明する為の他人が推測できない符号です。安全なパスワードの設定方法はp10をご参照ください。

2-C 安全なパスワードの設定方法

パスワードは、なるべく複雑で長いものに設定しましょう

悪いパスワードの例

- 名前や生年月日などを利用したもの
- 「abcd」、「7777」など簡単に類推できるもの
- 文字数が少ないもの

英字4文字のパスワードの場合、理論上総当たりで数秒で見破られます。

良いパスワードの例

- 以下を組み合わせたもの
  - 英大文字(ABC・・・)
  - 英小文字(abc・・・)
  - 数字(123・・・)
  - 記号(!?#・・・)
- 文字数が多いもの(10文字以上)

上記のパスワード(10文字)の場合、理論上総当たりで数百年かかります。

2-C 安全なパスワードの設定方法

パスワードの使いまわしは絶対に避けましょう

複数の機器やサービスで全く同じパスワードを使いまわしたり、似たようなパスワードを使っていないでしょうか。パスワードを使いまわしている場合、1つのサービスからパスワードが流出をきっかけに、同じパスワードを使用している他のサービス等にもログインされる恐れがあるためパスワードの使いまわしは避け、サービスごとのパスワードを必ず作るようにしてください。

パスワードを使いまわさないためのアイディア

サービスごとに冒頭の文字を変えます

＋

共通の核となるパスワードを決めます

terebiGAsuki!!06

独立行政法人情報処理推進機構『安心相談窓口だより』より抜粋

安全なパスワードの設定方法

パスワードをノートやメモ等に書きとめて保管しましょう

パスワードを書き留めたノートやメモ等は他の人に見られない場所で
大切に保管しましょう。なくさない限りにおいては最も安心な方法です。

abcネット
ID:～～～
パスワード:～～～～

いろは銀行
ID:～～～
パスワード:～～～～

※p37の「メモ」もご活用ください

2-D パスワードを忘れた場合

パスワードを忘れた場合には、IDと登録メールアドレスがわかっていれば再設定ができます

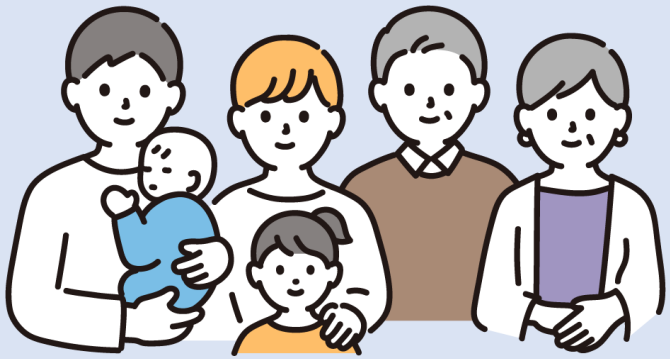
パスワードを忘れてしまうことを懸念して同じパスワードを使いまわす方が多くなっていますが、IDとメールアドレスを忘れなければパスワードを忘れても再設定できますので、**パスワードを忘れないように使いまわすことはやめましょう。**再設定をするためには、IDとメールアドレスが必要ですので、必ず控えておきましょう。

パスワードを忘れてしまっても
IDと登録メールアドレスが
分かっていれば
再設定できるので
安心してください

2-D パスワードを忘れた場合

パスワードを自分で再設定することが難しい場合は、家族やいつも行く携帯ショップのスタッフ等、信頼できる人に相談してみましょう

ご家族・ご友人



携帯ショップ

※相談先ですべてのパスワードを再設定できるわけではありません

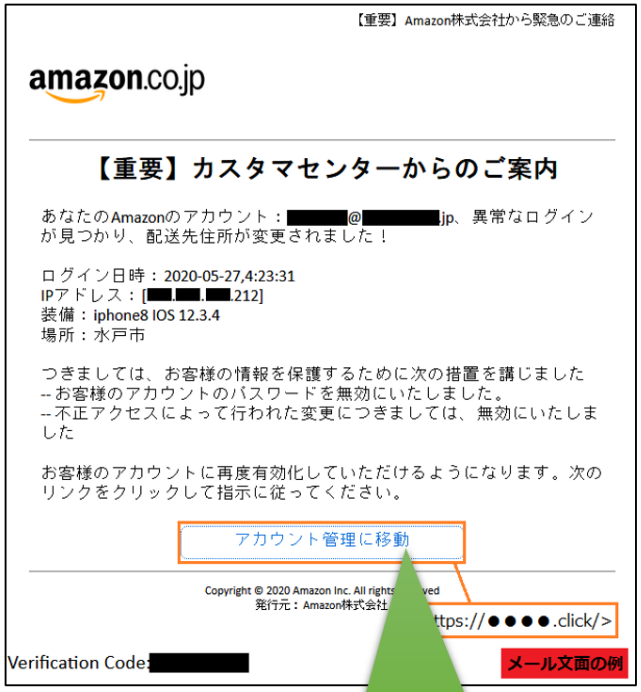
3 不審なメール・メッセージ・通知への対処

3-A 不審なメール・メッセージ・通知の事例

事例1：フィッシング詐欺

通販事業者等をかたる偽のメッセージに書かれているURLにアクセスすると、本物そっくりのサイトに誘導され、IDやパスワード等の重要な情報を抜き取られる手口です

※心当たりのないメール文面のURLリンクはクリックしないようにしましょう



フィッシングメール

フィッシングサイト

URLリンクをクリックしない！！

独立行政法人情報処理推進機構
『安心相談窓口だより』より抜粋

3-A 不審なメール・メッセージ・通知の事例

事例2：偽のセキュリティ警告

スマートフォンでウェブサイトを閲覧中に突然『ウイルスを検出した』などの偽のセキュリティ警告が表示され、指示に従って操作を進めると、アプリのインストールへ誘導する手口です。

※「あなたのiPhoneは、重度のウイルスによって破損しています！」等の偽の警告画面の指示に従ってアプリをインストールし、よく確認せずに契約登録してしまうと、利用料金が請求されるケースもあります。

3-A 不審なメール・メッセージ・通知の事例

事例3：アカウント乗っ取り

アカウントを乗っ取った犯人が、SNSの友人や公式アカウントになりすまし、メッセージを送りつけてくる手口です。 リンクから偽のログインページに誘導され、ログイン情報を要求してきます。ログイン情報を入力すると、自分のアカウントが乗っ取られます。

※実在のアイコンや色使いを
真似ているので、見た目だけで
気付くことは難しいです

乗っ取り被害に遭わないために｜
LINEみんなの使い方ガイド
https://guide.line.me/ja/cyber-bousai/
より抜粋

3-B　SNS型ロマンス詐欺とは

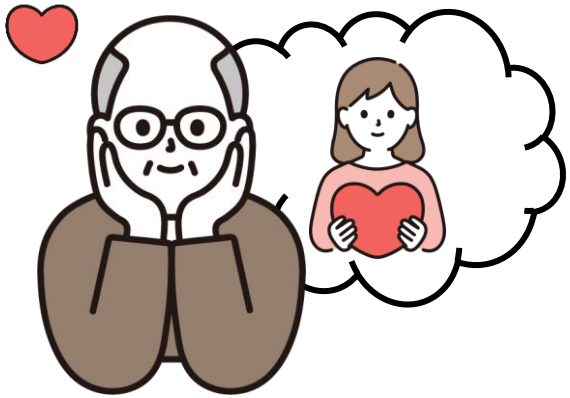
相手の好意や恋愛感情を利用した犯罪行為です

SNSやマッチングアプリなどを通じて出会った面識の無い相手と
やりとりを続けるうちに恋愛感情や親近感を抱かせ、
金銭等をだまし取る詐欺です。

実際に会ったことが無い相手から、**「あなたと結婚するための資金が欲しい」**と
いったような話が出たらすぐに**詐欺**を疑ってください。

SNS型ロマンス詐欺の特徴

その手口は様々ですが、**魅力的な人物を装ってターゲットに近づき、相手の好意に付け込むという点ではどのパターンにも共通点があります。**



3-B SNS型ロマンス詐欺とは

SNS型ロマンス詐欺の注意点

❶実際に会ったことがない人からお金の話をされたら要注意

SNS上に公開された写真や翻訳アプリ、AIなどを利用すれば、誰でも簡単に他人になりすますことができてしまいます。どんなにチャットやメッセージ、電話やビデオ電話で仲良くなっても、本人ではない者がなりすましている可能性があります。

実際に会ったことがなければ、だまされているかもしれません。

❷「投資」に誘導されたら要注意

あの手この手で投資の勧誘などをし、お金をだまし取るという手口が約7割以上です。

投資詐欺のページも確認し、だまされないためのポイントを覚えておきましょう。

https://www.npa.go.jp/bureau/safetylife/sos47/new-topics/investment/（警察庁 特殊詐欺対策ページ）

3-C　SNS型ロマンス詐欺の具体事例

事例1：結婚を約束した相手にお金をだまし取られた

被害者：40代女性
被害額：合計約500万円

英国在住の韓国人と称する男とSNSで知り合い、一度も会わないまま結婚を約束。

「仕事で必要な金を立て替えてほしい」
「立て替えてくれないと契約違反で警察に捕まる」

などと連絡があり、女性は指定された口座に複数回入金してお金をだまし取られた。

恋愛感情や親近感を抱いていると、
相手を疑わずに振り込んでしまうことも。
会ったことのない人からお金の
振り込みを求める連絡には要注意。

出典：警察庁　特殊詐欺対策ページ

3-C　SNS型ロマンス詐欺の具体事例

事例2：投資名目でお金を要求され、だまし取られた

被害者：40代男性
被害額：合計約300万円

SNSで友達申請された女性に恋愛感情を抱き、その者から投資を勧められた。

「2人の将来のために投資でお金を貯めよう」
「必ず儲かる」

などと連絡があり、男性は投資用アプリから口座に振り込みを行い、約300万円をだまし取られた。

SNS型ロマンス詐欺では、2人の将来のための資産形成などと言い、投資や副業を勧めてくる場合があります。
中には偽のアプリで収益が上がっているように見せかけてくることもあります。

出典：警察庁　特殊詐欺対策ページ

3-D　SNS型投資詐欺とは

著名人などの名前を利用して架空投資へ誘導

インターネット上に**著名人の名前・写真を悪用した嘘の投資広告を出し、「必ず儲かる投資方法を教えます」といったメッセージを送るなどして、**SNSに誘導し、投資に関するメッセージのやりとりを重ねて被害者を信用させ、**最終的に「投資金」や「手数料」などという名目で、ネットバンキングなどの手段により金銭等を振り込ませる詐欺です。**

SNS型投資詐欺の特徴

一度だまされると、**詐欺と気付くまで、お金を何度も振り込んでしまうことがあります。**少しでも怪しいと感じたらすぐに警察等へ相談しましょう。

3-D SNS型投資詐欺とは

SNS型投資詐欺の注意点

❶紹介された投資先は実在していますか？

紹介された業者が金融商品取引業者等に登録されているかを確認しましょう。無登録での金融商品取引業や暗号資産交換業は違法です。

https://www.fsa.go.jp/ordinary/chuui/highrisk.html
（金融庁からのお願い・注意喚起HP）に載っていない業者は無登録業者です！

❷「必ず儲かる」「あなただけ」といった誘い文句はありませんか？

犯罪者は、こうした言葉を巧みに操ってあなたの心に付け込んできます。**「必ず儲かる」「確実に利益が出る」といった儲け話や「あなただけ特別に教える」といった誘いは、まず疑いましょう。**

SNS型投資詐欺とは

SNS型投資詐欺の注意点

❸あなたに投資を勧めている「著名人」はなりすましではありませんか？

著名人の名前を騙った広告からの詐欺被害も見られますが、**著名人があなたのために無料で投資教室を開いたりすることは基本的にないものと考えましょう。**このような場合、まずはなりすましを疑い、本人の公式アカウントやホームページからの発信情報を必ず確認しましょう。

❹投資に関係する「暗号資産」や「投資アプリ」等は本当に実在していますか？

実在しない架空の「暗号資産」への投資を勧められたり、偽物の「投資アプリ」をインストールさせられたりするケースが相次いでおり、そういった場合は必ず、**勧められた暗号資産や投資アプリの名前をインターネットで検索しましょう。**詐欺に使用されている架空の暗号資産であることや、偽物の投資アプリであることが口コミ等で分かる場合もあります。

❺振込先の口座に不審な点はありませんか？

投資話が本物の場合、一般的に**「振込先として個人名義の口座を指定されること」または「振込先の口座が振込のたびに変わること」はありません。**どちらか1つでも当てはまる場合は、詐欺を疑い、迷わず警察に相談してください。

3-E　SNS型投資詐欺の具体事例

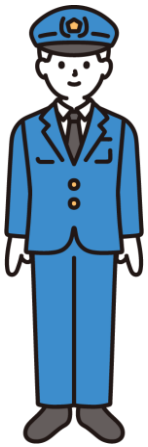
事例1：著名人になりすました相手とその仲間にだまし取られた

被害者：60代男性
被害額：合計約6,300万円

インターネット上で著名人が勧める広告からSNSを通し著名人とそのアシスタントを自称する者と交流。

「金の投資価値が高まっています」
「必ず儲かります」

などと連絡があり、男性は投資専用サイトから指定された口座に入金。最終的に約6,300万円をだまし取られた。



著名人や投資家になりすました偽広告からSNS上でのやり取りに移行し、犯人は言葉巧みに信用を得てお金をだまし取ります。詐欺広告にはご注意ください。

出典：警察庁　特殊詐欺対策ページ

3-E　SNS型投資詐欺の具体事例

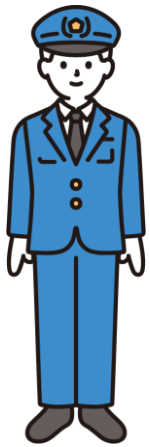
事例2：グループチャットでの偽情報を信用してしまった

被害者：60代女性
被害額：合計約2,000万円

動画配信サイトの新NISAに関する動画のURLからSNSグループチャットへの参加を招待。チャット内で投資や暗号資産の取引を誘われる。

「チャットの参加者はみな利益を得ています」

などと言われ、女性はチャット上で知り合った者から指定された口座への振り込みと暗号資産の送信により合計約2,000万円をだまし取られた。



犯人は投資用アプリやチャットから運用収益が上がっているように見せかけてきます。さらに収益を上げようと複数回振り込みを要求してくることもあります。

出典：警察庁　特殊詐欺対策ページ

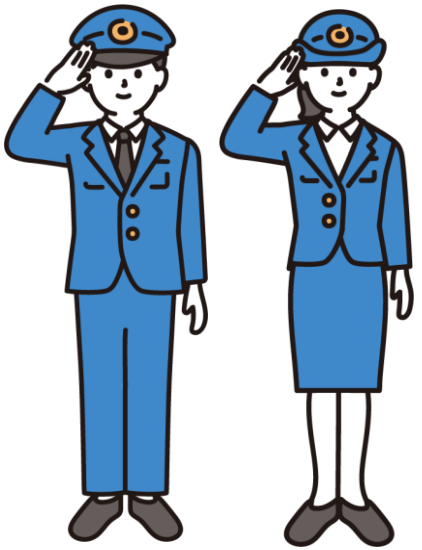
3-F　SNS型詐欺のターゲットになり得る人は？

常に自分自身が被害者になり得ることを自覚する

警察庁によれば、令和6年1月から6月のわずか半年の間にSNS型ロマンス詐欺では1,498件、SNS型投資詐欺では3,570件もの被害が発生しており、いずれも50代以上の世代が60%超を占めています。

他人事ではなく、常に、自分自身が詐欺のターゲットとなり得ることを自覚し、十分に注意しながらSNSを利用しましょう。

また、詐欺の疑いがある場合は、迷わず警察に相談し詐欺被害の拡大を防ぎましょう。



出典：警察庁　特殊詐欺対策ページ

3-G 危険に巻き込まれないために

身に覚えのないメール等が届いたら無視する

詐欺の手口は日々巧妙になっており、簡単に見破ることはほとんど不可能になっています。時には本物と思ってしまうメール等が届くかもしれませんが、不安になったらまずは一度落ち着きましょう。
URLをクリックしないことはもちろん、メール等に記載・表示される電話番号に電話をすることも控えましょう。

重要な情報、人に見られては困る情報は他人に見せない

「パスワードを教える」ことは「家の鍵を貸す」ことと同じです。
また、他人に見られて困るような写真や動画は悪用される可能性がありますので、絶対に第三者に送らないようにしましょう。

不安なときは相談する

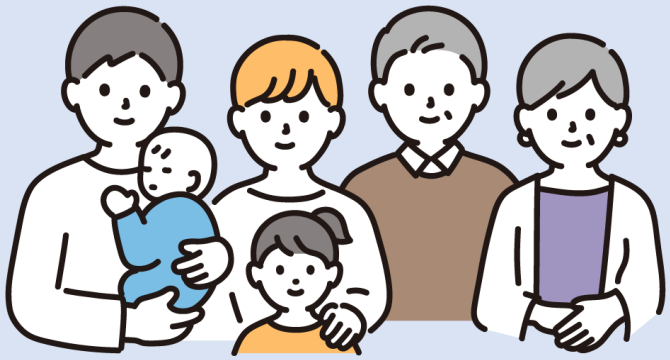
不安な時や判断に迷うときは、信頼できる相談先に相談しましょう。

4 不安を感じた場合の相談先

4-A 不安に感じることがあったら

怪しいメールを受け取ったり、不安なことがある場合は、家族やいつも行く携帯ショップのスタッフ等、信頼できる人に相談しましょう

ご家族・ご友人



携帯ショップ

普段からインターネットの安全・安心な利用や、いざという時に
誰に相談するのかについて周囲と話しあう機会を設けると良いでしょう。

4-B 信頼できる相談先の例

消費者ホットライン188(いやや!)に電話をすると、地方公共団体が設置している身近な消費生活センターや消費生活相談窓口へご案内されます。

実際のトラブル事例

インターネット通信販売を利用したが商品が届かない…

お試し購入のはずだったのに、2回目、3回目が届いた…

消費者庁ウェブサイトより抜粋

※ 相談は無料ですが、通話料はかかります

※ 電話の音声利用が難しい方は、電話リレーサービスを利用し、お住まいの地方公共団体の消費生活相談窓口等にご相談いただくことも可能です

4-B　信頼できる相談先の例

消費者庁では、通信販売や定期購入に関するトラブル対策を学ぶことができる8本の動画を公開しています

■動画ラインナップ

1．スマホデビュー時に気を付けたいこと　(7分37秒)
2．ショートメッセージによる架空請求に気を付けよう　(5分46秒)
3．SNSで、うまい話しにだまされないために　(7分14秒)
4．ネットショッピングを安全に利用するために　(7分19秒)
5．アプリを理解し安全に使おう　(7分07秒)
6．送り付け商法にご用心　(1分53秒)
7．還付金詐欺に気を付けよう　(3分05秒)
8．消費生活センターに相談しよう　(5分28秒)

動画イメージ

消費者庁ウェブサイト

4-B 信頼できる相談先の例

公的な相談先も活用しましょう

情報セキュリティ安心相談窓口	警察相談窓口
IPA（独立行政法人情報処理推進機構）の運営する情報セキュリティに関する相談窓口です。電話かメールでご相談ください。	各都道府県警察本部のサイバー犯罪相談窓口、警察相談専用電話の「＃9110」または最寄の警察署にご相談ください。
■電話：03-5978-7509 ■受付時間：10:00～12:00/13:30～17:00　※土日祝日・年末年始は除く メール:anshin@ipa.go.jp URL:https://www.ipa.go.jp/security/anshin/index.html	都道府県警察本部のサイバー犯罪窓口 サイバー事案に関する相談窓口｜警察庁Webサイト（npa.go.jp） URL:https://www.npa.go.jp/bureau/cyber/soudan.html

4-C スマートフォンの安全な利用についての情報提供

各種ウェブサイトでスマートフォンの安全な利用についての情報提供を行っています

①インターネットの安全・安心ハンドブック
https://security-portal.nisc.go.jp/guidance/handbook.html

②情報セキュリティ安心相談窓口
https://www.ipa.go.jp/security/anshin/index.html

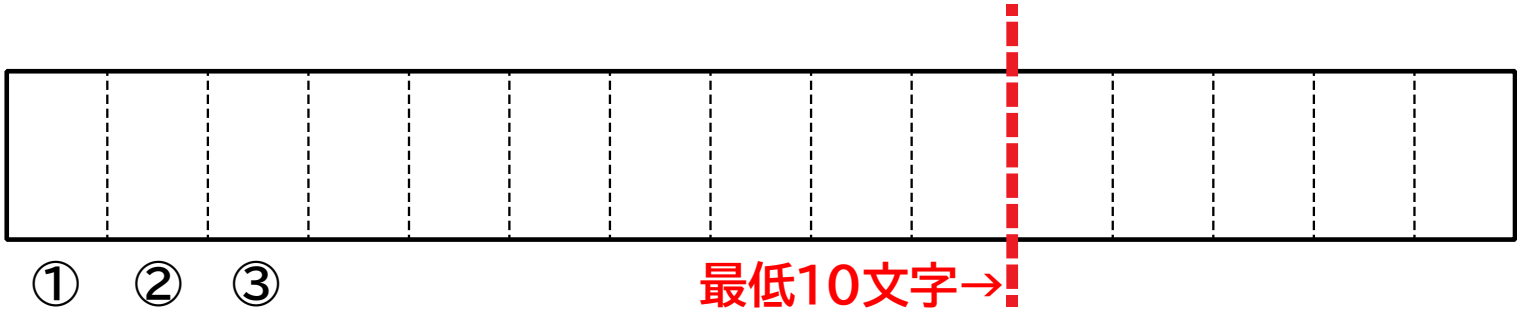
③安心相談窓口だより
https://www.ipa.go.jp/security/anshin/attention/index.html

④情報処理推進機構[IPA]X(旧Twitter)
https://x.com/IPA_anshin

5 付録 安全なパスワードの作成と保管

演習　安全なパスワードを作ってみましょう

安全なパスワードを書き込んでください



チェック項目	チェック
既に使ったことのあるパスワードではありませんか？	□
十分な長さになっていますか？（10文字以上）	□
アルファベットの大文字・小文字・数字・記号が全て含まれていますか？	□
お名前や生年月日等、容易に推測できる情報が含まれていませんか？	□

上記が当てはまれば☑をいれてください。

演習　アカウントの情報をメモしましょう

IDやパスワードの情報についてメモをして、大切に保管しましょう。このメモを信頼できる人以外に渡したり、見せたりすることは絶対にやめましょう。

	サービス名	ID	メールアドレス	パスワード
❶				
❷				
❸				
❹				
❺				

※IDとメールアドレスが同じ場合もあります