スマートフォンアイフォン（iPhone）基本編

※スマートフォンの操作説明は、アルファベット表記が多いため、音声や点字での確認が効率的に行えるようにカタカナ表記に置き換えています。各単元の最初のみカタカナの後にアルファベット表記をカッコ内に書いています。

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

目次

しょう

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「スマート（smart）（賢い）」＋「フォン（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て機能を拡張することができます。

アプリには、様々な種類のものがあり、例として、他者と交流するコミュニケーション系のアプリ、映画やテレビ、ラジオ、音楽が楽しめる娯

楽系のアプリ、株価や天気予報などがわかる実利系のアプリ、交通機関用の電子マネーや決済に使えるお財布系のアプリ、カードゲームや将棋、囲碁などを楽しめるゲーム系のアプリ、登山やジョギング、ショッピングなどの趣味のためのアプリまで、多種多様なものが揃っています。
これらのアプリをスマートフォンに取り込み、使いこなすことでスマートフォンをより便利に使っていただ

けるようになりますが、アプリの多くが、インターネットを通して利用する仕組みになっていることから利用時には注意が必要です。

1-B スマートフォンに入っている大量の情報

なぜ、インターネットを介して利用するサービスには注意が必要なのでしょうか。

それは、スマートフォンの中には、通話やメールの履歴、電話帳、自分

で撮影した写真や動画、どこを訪れたかという位置情報や支払い履歴など、膨大な個人情報が詰まっているためです。
インターネットに接続されたスマートフォンから、これらの個人情報が漏れてしまうと、プライバシーの侵害を受けたり、身に覚えのない請求を受けたりと、思いもよらない被害を受ける可能性があります。
これらの被害から自分自身を守り、スマートフォンを、安全かつ、便利

な機能を併せ持つ、その名の通り「賢い電話」として役立てるため、スマートフォンに保存される個人情報をしっかりと保護し、適切に守る必要があるのです。

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

スマートフォンを使いこなすほど、非常に多くの重要な情報が蓄積さ

れていくことになります。
そのスマートフォン自体や、インターネット上の様々なサービスを利用する際に、第三者の不正利用を防ぐ役割を果たしているものが「パスワード」です。
例えば、銀行のキャッシュカードやクレジットカードの場合、4ケタの暗証番号を入力して使いますが、同じように、スマートフォンを起動する際や、スマートフォンに入っているアプリでさまざまなサービス

を利用する時にも不正利用でないことを証明するためにパスワードが必要になります。

これらの重要な情報を守るパスワードは、自分の財産を守る「家の鍵」や「金庫の鍵」と同じものと言えます。
今後、スマートフォンがお財布代わりになる電子マネーが本格的に普及したり、その他便利なサービスが増えることで、まさにスマートフォ

ンは「わが家の財産」が詰めこまれた状態になります。
その大切な鍵、すなわち、パスワードが盗まれてしまうと、他人が家（機器やスマートフォン）に侵入して、「財産」とも言える情報が勝手に盗み取られる可能性があります。
そのため、パスワードは外に漏れないように、しっかりと管理する必要があります。

2-B パスワードの種類

次にパスワードの種類についてご説明します。
パスワードには様々な種類がありますが、もっともイメージしやすいのは、スマートフォンの画面ロックを解除する際のパスワード（パスコードともいいます）ではないでしょうか。
4ケタから6ケタの数字を設定して入力するものや、任意の図形パターンを指でなぞるタイプのものがあります。

最近では、パスワードを入力する代わりに、持ち主の顔や指紋を認証して、スマートフォンを起動させる機能を持ったスマートフォンも普及しています。

もうひとつの種類は、アイディー（ID）とパスワードを入力するタイプのものです。
アイディーとは、利用者を識別するユーザー名のことで、名前に近いイメージと考えましょう。

アイディーには、大きく分けて自分で設定できるケースや利用するサービスを提供する事業者から付与されるケースと、自分のメールアドレスをアイディーの代わりにするケースがあります。
そのアイディーと合致する、パスワードを入れることで、本人確認がなされたことになり、サービスの利用が許可される仕組みです。
これらのパスワードがアイディーとセットで盗まれると、他人がご自身

になりすまして、通販サイトで買い物をしたり、さまざまなサービスを自由に受けることが可能になってしまいます。
パスワードは、最初にご説明した通り「家の鍵」と同様に、とても大事なものです。
アイディーとともに、大切に保管しましょう。

2-C 安全なパスワードの設定方法

ここからは、どのようにパスワード

を作れば、より安全かをご説明します。
パスワードは他人から推測されにくく、より複雑なものが、安全です。

自分の名前や生年月日を利用したり、簡単に推測できる文字の羅列を使ったり、または入力するのが面倒だからと、少ない文字数でパスワードを作った場合、簡単に見破られてしまうリスクが高まるため、注意しましょう。

パスワードを見破る手段には「総当たり攻撃」といわれるものがあります。これはすべての文字列の組み合わせを、次から次へとコンピュータで自動で試し、合致するパスワードを発見する手口です。

たとえば、英字4文字だけのパスワードは、この総当たり攻撃に遭うと、数秒で見破られるそうです。

ところが、英大文字、英小文字、数字、記号を組み合わせた、10文字のパスワードになると、理論上、解

明するまでに数百年かかると言われています。
これなら、簡単に見破られることは無くなります。安全なパスワードは、英大文字、英小文字、数字、記号を組み合わせた、10文字以上と、心がけてください。

複雑なパスワードを作ったからといっても、同じものをいろいろなサービスで使いまわしては絶対にいけません。

これが、安全なパスワードを使うために重要なポイントです。
なぜなら、どこか1ヵ所でパスワードが流出したら、同じパスワードを使っている他のサービスにもログインされ、勝手に使われる可能性が高いからです。
とはいっても、毎回毎回、複雑なパスワードをランダムに考え出し、記憶しておくのも難しいことです。
そこで複雑な核となるコアパスワードをまず決めて、サービスごと

に冒頭の文字を変えて管理する方法があります。
ここでは「て・れ・び・が・す・き」に、記号や数字を混ぜて各パスワードにしています。
このように、私的な自分の趣味や嗜好などをヒントに核となるパスワードを考えると、他人からは推測されにくいものにもなり、かつ、楽しくパスワードを作ることができます。
ここでは例として、利用するサービ

スの頭文字を、それぞれ核となるパスワードの冒頭につけています。
これらの冒頭の文字を、末尾につけても構いません。
自分なりの法則性を決めて管理すれば、見破られる可能性は低くなり、より安全にパスワードを管理できるようになります。

利用するアプリが増えると、それぞれのアイディーやパスワードをどう管理するかも大きな問題です。

ノートやメモに、利用するアプリのアイディーやパスワード等を書き記して、保管する方法がおすすめです。このパスワードを管理するノートやメモは、スマートフォンとは一緒に持ち歩いてしまうと紛失した際に悪用される可能性がありますので一緒に持ち歩かないよう気を付けましょう。

また、ノートやメモは他人から見られない場所で大切に保管するよう

にしてください。
最近のスマートフォンには、アプリごとにアイディーやパスワードを自動で記憶してくれる機能があります。
一度アイディーとパスワードを入力すると、次回からはスマートフォンが勝手に入力してくれて、自動的に認証を得る便利な機能です。
しかし、スマートフォンがインターネットと繋がっている限り、個人情報が流出する危険性が常にあると

言えます。
その点で、紙とペンで記録する方法はとても原始的ですが、ネットから遮断されており、パスワードを管理するには一番確実な方法です。

2-D パスワードを忘れた場合

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、アイディー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、アイディー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。
パスワードを忘れた場合は、利用するアプリやサービスのログインページに行きます。
通常、サービスのログインページには「パスワードを忘れてしまった方はこちら」のような記述があります

ので、こちらをダブルタップしてください。
新しくパスワードを設定する方法が案内されているページが表示されたり、登録しているメールアドレスにパスワードを再設定するページを案内するメールが送られてきたりします。
後者の場合は、メールからそのサイトに移動して、新たにパスワードを設定すれば、ログインできるようになります。

その際は新しく設定したパスワードを必ずメモしましょう。

前のページでお伝えしたように、パスワードは自分で再設定することができます。
しかし、どうしても自分で再設定することが難しい場合は、信頼できる家族や友人、または携帯ショップのスタッフなどに相談してみましょう。

但し、相談先ですべてのパスワード

を再設定できるわけではないのでご注意ください。

3　不審なメール・メッセージ・通知への対処

次に、アイディーやパスワードなど、私たちの大事なデータが奪われるリスクがある、不審なメールやメッセージの事例とその対策を見ていきましょう。

ネット詐欺にはいくつかのパターンがありますので、ここで学習する内

容を知っているだけでも、かなりの確率で被害を防ぐことができるようになります。

3-A 不審なメール・メッセージ・通知の事例

ネット詐欺で代表的なものが、「フィッシング詐欺」といわれるものです。ここ数年で急激に増えているネット詐欺の手口です。

これは、通販事業者等をかたる偽の事業者が一方的に送りつけたメ

ールにユーアールエル（URL）が記載してあり、本物そっくりのサイトに誘導し、アイディーやパスワード、場合によってはクレジットカード番号や銀行の口座情報などを、魚釣り、すなわち、フィッシングのように釣り上げ、盗もうとするものです。
「フィッシング詐欺」でよくあるのが、教材で紹介しているような大手通販業者を装ったメールです。
これは「異常なログインが見つかり、配送先住所が変更されました」

というおどすような文面で始まるメールで「問題を解消するには、このユーアールエルをクリックしてください」と、偽のサイトに誘導し、アイディーとパスワードなどの個人情報を入力するように促されるものです。
同じような手口で、宅配便業者を装って、不在通知のメールを送るものや、「あなたのカードが不正に使われた形跡があります」などと不安を煽るクレジットカード会社や銀

行を装った詐欺メールも有名です。
偽のサイトやメールの作り方は
年々巧妙になっており、一見しただけでは見破ることが難しいものも数多くあります。

もっとも効果的な対策は「心当たりのないメールでは、絶対にユーアールエルを開かないこと」です。

「偽のセキュリティ警告」も、よく見られる詐欺の1つです。

スマートフォンでウェブサイトを閲覧中に、突然、「重度のウイルスで破損しています」や、「個人情報が漏えいしています」といった偽のセキュリティ警告画面が出現します。異様な警告音を伴う場合もあります。

例えば、「ウイルスを退治するための無料のアプリをインストールしてください」などと偽り、インストールすると、セキュリティソフト等の購入を迫られ、利用料金を請求され

続けたりします。
困った人をサポートするフリをして、罠にはめる、悪質な詐欺行為です。
不安を感じた場合はそのままにせず、周りの方や携帯ショップの方へ相談するようにしましょう。

「アカウント乗っ取り」では、エスエヌエス（SNS）などで実際の友達や公式アカウントを装ったメッセージが届くことがあります。リンクから

はログイン情報を入力させる偽サイトに誘導されます。
偽サイトは実在のアイコンや色使いを真似ているため、見た目だけで気付くことは難しいです。偽サイトではログイン時に必要な情報の入力を求められ、自分のログイン情報を入力すると、相手にその情報が伝わり、自身のアカウントへ不正ログインされるなどの被害につながる可能性があります。
教材でご紹介しているケースはあ

くまで一例ですが、違和感を覚えたら、実際に友人に連絡を取ってみても良いでしょう。

3-B エスエヌエス型ロマンス詐欺とは

最初にエスエヌエス型ロマンス詐欺についてご説明します。
エスエヌエス型ロマンス詐欺は、エスエヌエス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。

エスエヌエス型ロマンス詐欺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。次のページからは実際の事例をもと

に、エスエヌエス型ロマンス詐欺の手口と具体的な対策を学んでいきます。

エスエヌエス型ロマンス詐欺の注意点をご説明します。
それでは一つ目の注意点です。
実際に会ったことがない人からお金の話をされた場合、警戒するようにしましょう。
エスエヌエス上に公開された写真や翻訳アプリ、エーアイ（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、本人の音声、動画を作る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。

二つ目の注意点です。
「投資」に誘導されたら要注意です。

２人の将来のために、などと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。
警察庁 特殊詐欺対策ページと検索いただき、必要に応じてお役立てください。

3-C エスエヌエス型ロマンス詐欺の具体事例
一つ目の事例です。
被害者は40代女性で、被害額は

合計約500万円です。
海外在住の韓国人と称する男性と結婚を約束し、その後、相手から仕事で必要なお金があり、立て替えてもらえないと刑務所に入るとの連絡があり、そのお金を振り込んでしまいだまし取られたというケースです。
恋愛感情や親近感を抱いていると相手を疑わずお金を振り込んでしまうことがあります。
実際に会ったことが無い相手から

金銭の振り込み要求があった場合は応じずに警察に相談するなどし、対処しましょう。

二つ目の事例です。
被害者は40代男性で、被害額は合計約300万円です。
こちらの事例も一つ前の事例と共通点があり、「二人の将来のため」との言い分で投資を持ちかけられ、お金を振り込んでしまい、だまし取られています。

このケースは投資アプリも利用されており、ここまでご紹介した事例よりもさらに手が込んだ内容になっています。
詐欺犯はあの手この手で相手を騙そうと試みてきます。偽の投資アプリで利益が上がっているように見せかけるケースも発生しており、その手口は年々巧妙化しているため注意が必要です。

3-D エスエヌエス型投資詐欺とは

エスエヌエス型投資詐欺は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、エスエヌエスに誘導し、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。被害者は少額でも一度だまされる

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。

エスエヌエス型投資詐欺の注意点をご説明します。
それでは一つ目の注意点です。
投資先を紹介された場合、その業者が金融商品取引業者等に登録されているか必ず確認しましょう。
業者が掲載されていない場合、

その業者は無登録業者であり、違法な話を持ち掛けられているということになります。
こちらのスライドにホームページのアドレスとキューアール（QR）コードを掲載しておりますので、ぜひ活用してください。
二つ目の注意点です。
「必ず儲かる」「あなただけ」といった誘い文句はなかったでしょうか。
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、まず詐欺を疑ってください。そのような都合の良い儲け話が、あなただけに都合よく舞い込んでくることは無いと考えた方が良いでしょう。

三つ目の注意点です。
エスエヌエス型投資詐欺の特徴として、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ってください。それでもあきらめきれない場合は、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、その情報が確かなものであるか必ず確認しましょう。

四つ目の注意点です。

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。

最後に五つ目の注意点です。

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。
もしエスエヌエスで投資を持ち掛けられた際はこの5つのポイントを思い出し、確認することで詐欺被害を回避しましょう。
次のページからは具体事例をご紹介していきます。

3-E エスエヌエス型投資詐欺の具体事例

一つ目の事例です。

被害者は60代男性で、被害額は合計約6,300万円です。

こちらはエスエヌエス広告経由で著名人を騙る相手とそのアシスタントを名乗る2人組に投資を持ち掛けられ、専用投資サイト上で運用利益が上昇しているように見せかけられ、高額をだまし取られた事例です。

この後にもご紹介しますが、エスエヌエス型投資詐欺の事例には著名人になりすましたケースが多くなっています。
著名人を名乗る相手が現れた場合は詐欺だと認識した方が良いでしょう。

二つ目の事例です。
被害者は60代女性で、被害額は合計約2,000万円です。
こちらは新ニーサ（NISA）に関す

る解説動画に記載されていたユーアールエルから詐欺グループのチャットに繋がってしまいチャットメンバーから「必ず儲かる」との甘い誘いを受け、相手が指定する口座へお金を振り込みだまし取られています。
相手はあらゆる手段で投資を魅力的に見せ、被害者からお金をだまし取ろうとします。
上手い投資話があっても簡単には乗らないように注意しましょう。

3-F エスエヌエス型詐欺のターゲットになり得る人は？

最後に、ここまでご紹介した事例に対して「自分がそんな被害にあうはずがない」と思われている方が大半だと思われますが、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エスエヌエス型ロマンス詐欺では1,498件、エスエヌエス型投資詐欺では3,570件もの被害が発生しています。

また、被害者の年代にも偏りが

あり、いずれも50代以上の世代が60%超を占めています。
エスエヌエスを通じた詐欺が常に身近にあり、なおかつ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エスエヌエスを利用しましょう。

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。

3-G 危険に巻き込まれないために

電話の「オレオレ詐欺」の手口が巧妙化したのと同様に、日々、ネットを使った詐欺も多様化、巧みに進化しています。危険に巻き込まれないために、以下の3点を心掛けてください。

「身に覚えのないメールが届いたら無視する」

最近のメールでは、送信者名を詐称し、もっともらしい文面を装うだ

けでなく、接続先のサイトも本物とほとんど区別がつかないほど、そっくりに偽造するなど、簡単に見破ることはほとんど不可能になっています。
時には不安になってすぐに反応したくなることがあるかもしれませんが、不安になったときこそ、まずは落ち着くことを心がけましょう。
インターネットの詐欺に巻き込まれないための原則は、すべて無視することです。ユーアールエルを開い

たり、窓口に電話をして、真偽を確かめようなどとは、決してしないでください。
また「あなただけに給付金があります」といったような、うまい話の詐欺もよくありますが、これも欲を出さず、すべて無視してください。
つぎに「重要な情報、人に見られては困る情報は他人に見せない」ことを心がけてください。
パスワードは「家の鍵」のようなものであり、パスワードを他人に教え

ることは、「家の鍵を貸す」のと同じです。
決して他人には教えないでください。また他人に見られて困るような写真や動画は、絶対に第三者に送らないようにしましょう。

最後に「不安なときは相談する」という選択肢を忘れないでください。不安になったときや反応した方が良いメールなのか判断に迷う際は、一人で抱え込まずに、信頼できる

相談先に相談しましょう。
デジタルリテラシーに関するご説明は以上です。
相談先については、第4章で詳しくお伝えします。

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

スマートフォンを利用する中で、不安にかられたときは、1人で悩まず、まずは、家族や知人、携帯ショップ

のスタッフなど、信頼できる人に相談してみましょう。
また、第3章のような不審なメール等は、心の準備ができていないときに突然届きます。
慌ててしまわないように、普段から、インターネットの安全・安心な利用について学んだり、何か困ったことが起きた時には誰に相談するかについて、身近な人とも話し合っておくことが大事です。

4-B 信頼できる相談先の例

信頼できる、公的な相談先も活用しましょう。

「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案内されます。

局番なしの「188（いち・はち・はち）」という3ケタの電話番号で、年末年始を除いて原則毎日、ご利用いただけます。

電話の音声利用が難しい方は、手話・文字と音声を通訳する公共インフラサービスである「電話リレーサービス」を利用して、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。

消費生活相談窓口では、「インターネットで注文したが、商品が届かない」「ネット通販でお試し購入のはずだったのに、2回目の商品が届いた」といった、最近多い通信販売

や定期購入のトラブルなども相談できます。

また消費者庁では、「エスエヌエスでうまい話にだまされないために」など、テーマごとにトラブル対策が学べる8本の動画も公開しています。
スマートフォンでも手軽に見ることができるので併せてご活用ください。

経済産業省が所管する「情報処理推進機構」（アイピーエー（IPA））にも、「情報セキュリティ安心相談窓口」があります。
電話とメールで相談を受け付けています。
電話番号は03-5978-7509です。
受付時間は土日祝日・年末年始を除く、10時から12時と13時30分から17時までです。
メールアドレスは

anshin@ipa.go.jpです。
また、警察にも相談窓口が用意されています。
警察相談専用電話「＃9110」か、各都道府県警察本部の「サイバー犯罪相談窓口」へご相談ください。

4-C　スマートフォンの安全な利用についての情報提供

パソコンやスマートフォンで見られるウェブサイトでも、スマートフォンを安全に利用するための情報提供

を行っていますので、参考にしてください。
「内閣官房　内閣サイバーセキュリティセンター」の「インターネットの安全・安心ハンドブック」や前のページでご紹介した、情報処理推進機構（アイピーエー）も多くの情報発信を行っています。
特に新しい詐欺の手口に関しては、いち早くレポートを発表していますので、参考にしてください。
①インターネットの安全・安心ハン

ドブック、②情報セキュリティ安心相談窓口、③安心相談窓口だより、④情報処理推進機構[IPA]X(旧Twitter)と検索いただき、必要に応じてお役立てください。
スマートフォンの安全な利用についての説明は以上です。

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

ここでは、第2章で学んだルールを思い出して、安全なパスワードを教材に書き込んでみてください。教材の中の四角い枠に一文字ずつ記入してください。

パスワードができ上がったら、チェック項目に従って、ご自身でチェックをしてみてください。

・既に使ったことのあるパスワードではありませんか？もし、過去に別のサービス等で使ったパスワードを使いまわしている場合は、別の

パスワードを考えてください。
・十分な長さになっていますか？
10文字以上のパスワードになっているかをご確認ください。
・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？「アルファベットの大文字はここ」「アルファベットの小文字はここ」とパスワードの近くに書き込むとわかりやすいでしょう。
・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？あまりにもわかりやすいパスワードになっていないか、再度確認してみましょう。
全ての項目にチェックが入ったら、このパスワードは安全といえます。
記入を終えたシートは絶対に他人に見せないようにお気をつけください。

演習 アカウントの情報をメモしましょう
ご自宅で、ご自身が利用している

サービスの「サービス名」「アイディー」「登録しているメールアドレス」「パスワード」をメモして、大切に保管しましょう。サービスによっては「アイディー」と「登録しているメールアドレス」が同じ場合もあります。これらは文字で書くだけでなく、点字で保存、録音して保存でも構いません。また、ここに記載する情報は大切な情報ですので、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。