スマートフォン（アイフォン）活用編

※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。

7　スマートフォンを安全に使うためのポイントを知りましょう

目次

1　スマートフォンは危険なものか？

　基本的に、スマートフォンはとても安全にできています。しかし、使い方によっては、詐欺を誘発する危ないツールになるのも、スマートフォンです。なぜ、危険なツールになるのか、安全に利用することがいかに重要なのかについて、スマートフォンの特徴から見ていきましょう。

1-A　スマートフォンとは

スマートフォンとは「スマート（smart）（賢い）+フォン（phone）（電話）」で賢い電話を指します。電話やメールだけでなく、アプリケーションを入れることで、インターネットや写真、買い物や読書等、様々な機能を追加することができます。

その他、アプリには、たとえば、他者と交流するコミュニケーション系のアプリから、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、交通系のカードや電子マネー

などが使えるお財布系のアプリ、テレビゲーム、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。これらのアプリのほとんどが、インターネットを通して利用する仕組みになっています。

1-B　スマートフォンに入っている大量の情報

　アプリを利用する際には、氏名や住所、年

齢、メールアドレスなどを登録しなければ使えないものもたくさんあります。有料のアプリになると、その上、クレジットカードや銀行の口座情報などの登録も必要になります。これらに加えて、もともと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など、膨大な個人情報が詰まっています。

　インターネットといつも繋がっている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、プライバシーが他人に知られてしまったり、お金がいつの間にか抜き取られてしまうなど、さまざまな被害を受ける可能性があります。ですから、スマートフォンに保存された、これらの個人情報にはしっかりと鍵をかけ、適切に守らなければいけません。それさえ怠らなければ、スマートフォンは、安全、かつ、便利な機能を併せ持つ、その名の通り「賢い電話」として役立つはずです。

2　パスワードを使った安全な管理をしまし

ょう

2-A　パスワードの重要性について

　スマートフォンには非常に多くの重要な情報が保管されています。スマートフォンを利用する際やネットの様々なサービスを利用するときに、自分だけが利用でき、他人が利用できないようにする役割を果たしているのが「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 桁の秘密のパスワードを入力して使います。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様々なサービスを利用するときにも、自分を証明する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」と同じです。今後、スマートフォンがお財布代わりになる電子マネーの本格的な普及や、その他便利なサービスが増えてくると、まさにスマートフォンには「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、「わが家の財産」が勝手に盗み取られる可能性があります。

　これからスマートフォンがさらに便利になれば、パスワードの重要性はますます高まります。パスワードは外に漏れないように、今まで以上にしっかり管理する必要があります。

※大切な鍵（＝パスワード）を盗まれてしまうと、他人が家（＝機器やサービス）に侵入する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する等、大切に扱いましょう。

2-B　パスワードの種類

パスワードには様々な場面で使用する様々な種類のものがあります。①画面ロックのパスワード

　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（パスコードとも言います）ではないでしょうか。4 桁から 6 桁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。これらのパスワードも、他人に知られれば、自分のスマートフォンを人に勝手に使われるきっかけになりますので、十分注意が必要です。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タイプのものもあります。

②アプリやサービス利用時のパスワード

　もうひとつのパスワードのタイプは、様々なアプリを利用する際に必要になるもので

す。その際には、このような画面が出てきて、アイディー（ID）とパスワードを入力する必要があります。

　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です。アイディーには、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、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等があります。次に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、サービスの提供が許可される仕組みです。

このように、インターネット上のサービスを利用する際に、アイディーとパスワードを使って本人を確認することを「ログイン」と言うことがあります。

2-C　安全なパスワードの設定方法

　パスワードは、他人から推測されにくい、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としては、名前や生年月日を含めたものや、文字数が少ないもの、

7777 と同じ数字を並べたり、エイービーシーディーと順番に並んだものなどです。

　良いパスワードの例としては、10文字以上の文字数が多いものや、英語の大文字と小文字、数字や記号を組み合わせたものです。

　英字４文字のパスワードの場合、理論上総当たりすると約3秒で見破られてしまいます。良いパスワードの例で上げた10文字以上かつ、英字の大文字小文字、数字や記号を組み合わせたものだと、理論上総当たりで約

1000 万年かかると言われています。

　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 か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考え出すのも大変です。パスワードを使いまわさないためのアイ

ディアの一例として、共通の核となるパスワードを決めてサービスごとに冒頭の文字を変えるという手法があります。

　今回は「て・れ・び・が・す・き」に、記号や数字を混ぜてコア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コア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って、パスワードの使いまわしを避けながら、簡単に他人から推測されにくいパスワードを設定することができます。

例　コアパスワード　terebiGAsuki!!06

の場合

abc ネット　abc のときは

abcterebiGAsuki!!06

いろは銀行　irh のときは

irhterebiGAsuki!!06

IPA 信託　IPA のときは

IPAterebiGAsuki!!06

　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、保管しておくと良いでしょう。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かないようにしましょう。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。紙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、なくさない限りは最も安全に管理する方法の1つです。

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ります。

2-D　パスワードを忘れた場合

サービスによっても異なりますが、パスワ

ードを忘れた場合、アイディーと登録メールアドレスが判明していれば、パスワードを再設定することができます。パスワードを忘れてしまったときのためにも、アイディーと登録メールアドレスは必ず記録しておくようにしましょう。

　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。多くのサービスは、「パスワードを忘れてしまった方はこちら」のような内容が記載された場所がありますのでそこをタップします。

すると、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。

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などに相談してみましょう。

※新しく設定したパスワードを必ずメモしま

しょう。

3　不審なメール・メッセージ・通知を受け取ったときの対処

3-A　不審なメール・メッセージ・通知の事例

①フィッシング詐欺

　ネット詐欺で代表的なものが、「フィッシング詐欺」と言われるものです。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、最後に問題を解消したいなら、「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」などとおどす、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。

　これら心当たりのないメールでは、絶対にユーアールエルをタップしないようにしてください。

②偽のセキュリティ警告

「偽のセキュリティ警告」も、よく見られる詐欺のひとつです。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。

③アカウント乗っ取り

「アカウント乗っ取り」では、フェイスブック（Facebook）のメッセンジャーのようなエスエヌエス（SNS）に、実際の友達から「このビデオはいつでしたか？」などと書いてある動画を装ったメッセージが届くことがあります。動画を再生しようとメッセージをタップしても、動画は再生されず、アイディーとパ

スワードを入力させる偽サイトに誘導されます。偽サイトには「動画を見るにはアカウント情報を確認する必要がある」というような内容が記載されています。偽サイトに自分のアイディーとパスワードを入力すると、相手にその情報が伝わり、エスエヌエス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、違和感を感じたら、実際に友人に連絡を取ってみても良いでしょう。

④偽セクストーション被害

「偽セクストーション被害」とは、聞きなれない言葉かもしれませんが、このタイプの詐欺も最近増えています。「セクストーション」とは、「セックス（sex）＝性的な」と「エクストーション（extortion）＝脅迫」という英単語を組み合わせた造語です。

本来は、実際に個人のプライベートな動画や写真を交換するようにもちかけ、その後、それらをばらまくと脅迫する犯罪のことですが、実際にはそのような写真や画像は入手していないにもかかわらず、あたかも入手

したかのように振る舞い、それらを家族や同僚等にばらまくなどと脅して、メールで金銭を要求する「偽セクストーション」の手口が増えています。しかし、これはほとんどが相手を不安にさせるための攻撃者のでたらめです。これらに類似したメールが来たら、それは偽セクストーションなのですべて無視してください。何ら被害は発生しませんので、ご安心ください。

3-B　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。

①「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、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掛けましょう。

　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。ユーアールエルをタップしたり、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。

②「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。

③「不安なときは相談する」

　不安になったときや反応した方が良いメ

ール等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。

4　不安になったときの相談先

4-A　不安に感じることがあったら

　不安にかられたときは、ひとりで悩まず、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とき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「消費者ホットライン」188

　「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。局番なしの「188（いち・はち・はち）」という3桁の電話番号で、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。また、必要

に応じてユーアールエルもご参照ください。

・情報セキュリティ安心相談窓口

アイピーエー（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。

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　ansin@ipa.go.jp

ユーアールエル:

https://www.ipa.go.jp/security/anshin/index.html

・警察相談窓口

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。

都道府県警察本部のサイバー犯罪窓口一覧

https://www.npa.go.jp/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

　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なっていますので、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るので、必要に応じてお役立てください。

・インターネットの安全・安心ハンドブック

https://security-portal.nisc.go.jp/handbook/

・情報処理推進機構[アイピーエー]相談窓口

https://www.ipa.go.jp/security/anshin/index.html

・情報処理推進機構[アイピーエー]窓口だより

https://www.ipa.go.jp/security/anshin/mgdayoriindex.html

・情報処理推進機構[アイピーエー]ツイッター(Twitter)

https://twitter.com/IPA_anshin

5　付録　安全なパスワードの作成と保管

A　演習　安全なパスワードを作ってみましょう

　ここでは、演習形式で、実際に安全なパスワードを作ってみます。「2」で学んだルール

を思い出して、安全なパスワードを考えてみてください。パスワードができあがったら、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。

①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。

②十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。

③アルファベットの大文字・小文字・数字・記号がすべ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。

④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。

すべ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。

B　メモ　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」をメモをして、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。