

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？

- A. スマートフォンとは？…………… P 4
- B. スマートフォンに入っている大量の情報…………… P 5

2. パスワードを使った安全な管理をしましょう

- A. パスワードの重要性について…………… P 7
- B. パスワードの種類…………… P 9
- C. 安全なパスワードの設定方法…………… P 11
- D. パスワードを忘れた場合…………… P 14

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

- A. 不審なメール・メッセージ・通知の事例…………… P 17
- B. 危険に巻き込まれないために…………… P 21

4. 不安になったときの相談先

- A. 不安に感じることがあったら…………… P 23
- B. 信頼できる相談先の例…………… P 24
- C. スマートフォンの安全な利用についての情報提供…………… P 26

5. 付録 安全なパスワードの作成と保管

1

スマートフォンは 危険なものか？



1-A スマートフォンとは

スマートフォンとは「smart(賢い)+phone(電話)」で
賢い電話を指します。

電話



メール



アプリケーション
(機能)



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。

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情報が
入っており、常にインターネットを介して
外に出て行っている可能性があります。



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

スマートフォン等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。



2-A パスワードの重要性について

パスワードとは、いわば自分の財産を守る
「家の鍵」や「金庫の鍵」です。



家を守る鍵の役割
＝パスワード



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種類があります。

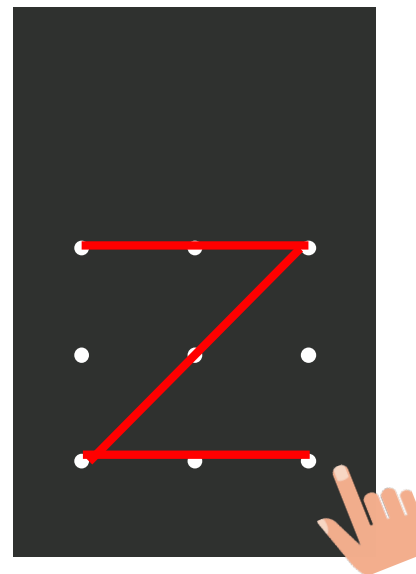
① 画面ロックのパスコード

※機種によって異なります。

暗証番号（数字）



パターン



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。

② アプリやサービス利用時のパスワード

〇〇サービス

ログインページ

ID

パスワード

パスワードを忘れてしまった方は[こちら](#)

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。

利用者が本人であることを証明する為の、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P.11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、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

- 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

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）

英字4文字のパスワードの場合、理論上総当たりで約3秒で見破られます。



上記のパスワード(10文字)の場合、理論上総当たりで約**1000万年**かかります。

内閣官房 内閣サイバーセキュリティセンター『インターネットの安全・安心ハンドブック』より

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ませんか？パスワードを使いまわしていると、1か所からパスワードが流出したら、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ります。

パスワードを使いまわさないためのアイデア

abcネット	abc	+		<u>terebiGAsuki!!!06</u>
いろは銀行	irh	+		
IPA信託	IPA	+		

共通の核となるコアパスワードを決めます

サービスごとに冒頭の文字を変えます

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

2-C 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取り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 : ~~~~~

...

P.29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る場合は再設定ができます。

IDとメールアドレスが分かっている場合は、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。必ず控えておきましょう。

PASSWORD...



ログインページ

ID

パスワード

パスワードを忘れてしまった方は [こちら](#)

IDと登録メールアドレスが分かっている場合は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

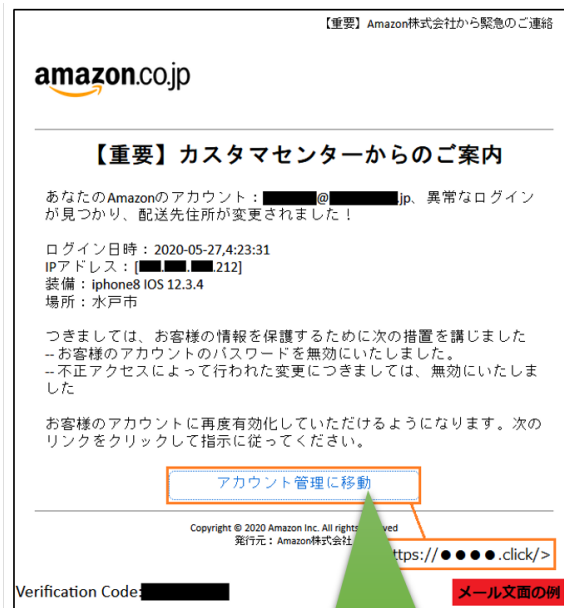


3-A 不審なメール・メッセージ・通知の事例

① フィッシング詐欺

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。

IDやパスワードが盗まれます。



フィッシングメール

URLリンクをクリックしない！！



フィッシングサイト

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

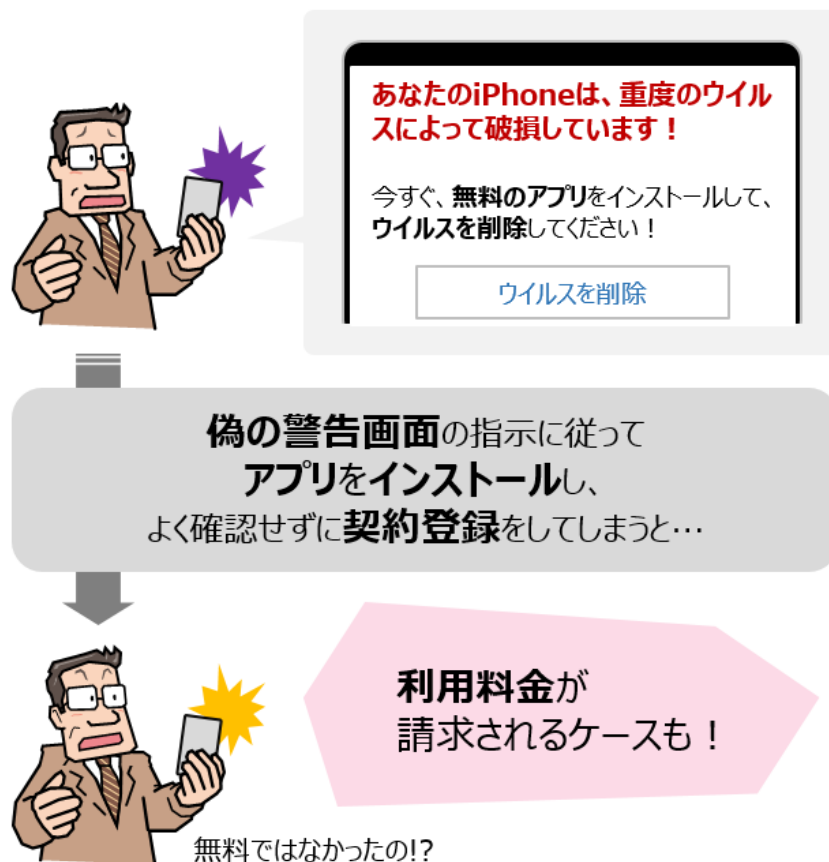
3-A 不審なメール・メッセージ・通知の事例

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。

↓

**利用料が請求され続ける
ことがあります。**



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

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の友人等になりすまし、動画を送りつけてくる手口です。動画を見ようとすると偽のログインページに誘導され、IDとパスワードを入力すると情報が抜き取られます。



**IDやパスワードが盗まれます。
また、さらに不審なサイトに
誘導されることもあります。**



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

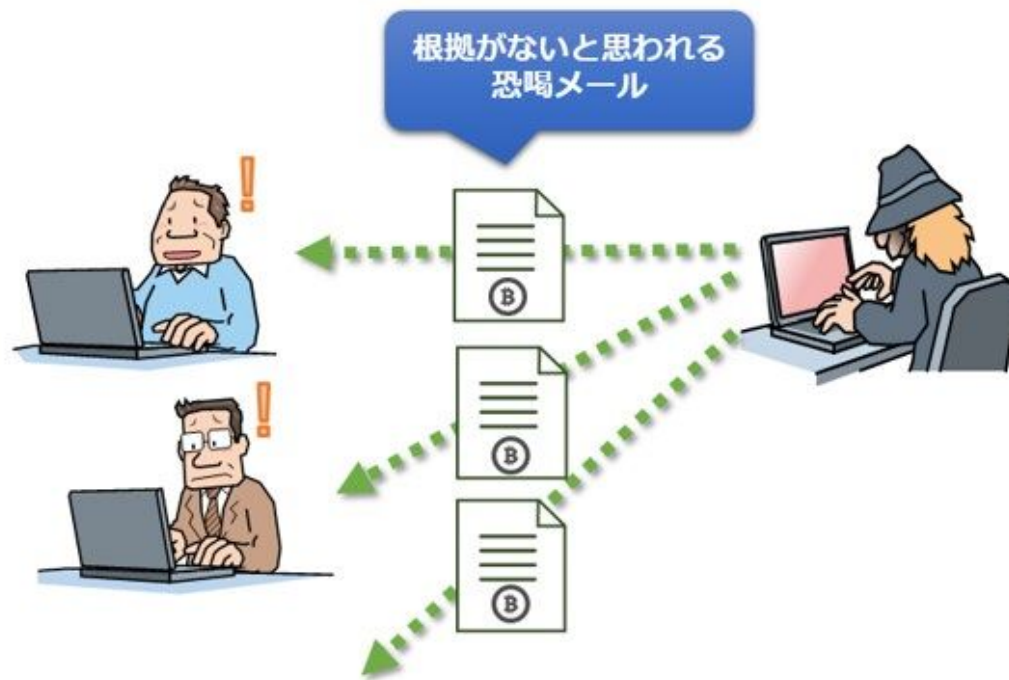
3-A 不審なメール・メッセージ・通知の事例

④ 偽セクストーション被害

「アダルトサイトを閲覧しているあなたの姿をパソコンについているカメラで撮影した。家族や同僚にばらまかれたくなければ仮想通貨で金銭を支払え」といった根拠のない恐喝メールを送りつける手口です。



**金銭を支払ってしまうと
取り戻すことができません。**



3-B 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、見破ることはできません。

時には本物と誤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

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

一人で悩まず
に周囲に相談



聞いてみれば
安心



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「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。

※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。

最近トラブルが多い相談事例

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…



動画でトラブルへの対策が学べます!



1. スマホデビュー時に気を付けないこと (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)



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

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。

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>



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」、又は、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/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](https://security-portal.nisc.go.jp/guidance/handbook.html)



② 情報処理推進機構[IPA] 相談窓口

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



③ 情報処理推進機構[IPA] 窓口だより

[https://www.ipa.go.jp/security/anshin/
attention/index.html](https://www.ipa.go.jp/security/anshin/attention/index.html)



④ 情報処理推進機構[IPA] Twitter

https://twitter.com/IPA_anshin



5

付 録



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

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

①

②

③

最低10文字→

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。

メモ 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
①				
②				
③				
④				
⑤				

※IDとメールアドレスが同じ場合もあります



用語集

用 語	意 味
アプリケーション	特定の用途や目的のために設計されたソフトウェア(機能)のこと。省略してアプリとも呼びます
アカウント	サービスを利用する際に必要な権利や個人認証情報のこと
ID	サービスの登録者や利用者を識別するために使用される文字列のこと
パスワード	サービスを利用する際に利用者本人であることを確認するための秘密の合言葉
ログイン	サービスを利用する際に、IDとパスワードを使って本人情報を確認する仕組みのこと
インストール	スマートフォン等のデジタル機器に、アプリケーション等のソフトウェアを取り込んで使えるようにすること