シニアのスマホ 安全安心　クイズ （どなたでも必須編）

ネットでeシニア　V1.7 2024.5.13

Q1. スマホの電源ボタンをいれたときのロック解除の方法は　A、Bどちら？

A. 操作が簡単だからスワイプでよい

B. 少なくとも4桁の暗証番号は必要

ヤマオリ

A1. 正解は　B.

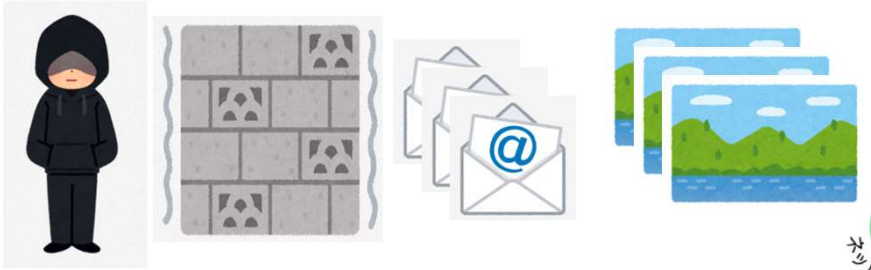
少なくとも4桁の暗証番号は必要です

4桁の数字だけではなく、点を指でなぞるパターン方式、
指紋認証、顔認証などの機能が
あれば、どれかを必ず設定してください

なぜなら：ロックしておかないと、スマホを落とした時や、
ちょっと机に置いておいた時、悪意のある人に勝手に操作
されるかもしれません

落としたら即ショップへ連絡して、スマホを止めてもらう

スマホに入っているあなたと知人の沢山の個人情報
（連絡先、電話履歴、メール、写真など）を、
悪意を持った人から守る必要があります



Q2. ロック解除の４桁の数字はなにがよい？

A. 覚えやすい番号がよい
たとえば
- 誕生日の西暦や月日
- スマホの電話番号下４桁
- １２３４

なら絶対に忘れない

B. 連想できない4桁
たとえば、本を4回適当に開いてページ番号の最下位の数字を並べ４桁にして、設定するメモして記録する

ヤマオリ

A2. 正解は　B.

簡単には連想できない４桁にする

ロック番号やパスワードを誕生日、電話番号、
単純な1234などにはしないでください

なぜなら：悪意のある人に、簡単に見破られてしまうからです

スマホは銀行のキャッシュカードと同じぐらい大切です
ただし、キャッシュカードと同じ番号にしてはいけません

≒

Q3. 複数のアプリやショッピング・サイドのパスワードは A、B どちら？

A. ルールを自分で決めて異なるパスワードにする

B. 違うものを設定しても覚えきれない
複雑なパスワードなら、同じパスワードで良い

自分だけのルールを決める

たとえば
先頭はアプリの先頭、末尾は@
iを１に置き換える
aは大文字Aに置き換えるなど

Amazon なら
（Aミシマダイスキn）
Am1sh1mAdA1suk1@

どのサイトでも
複雑なパスワード
なら同じでOK

たとえば
y32t@59Ng

ヤマオリ

A3. 正解は　A.

ショッピングなどのウェブサイトが中心
スマホのアプリで毎回パスワードを
必要とするものは、あまりありません

アプリやサイトごとに異なるパスワードにする

パスワードを使い回しはしないでください

なぜなら：一度破られると、全てのアプリやサイトを乗っ取られてしまいます

大小英字（A、a）、数字、特殊記号（@、*、#、__など）を混在させた　10桁以上が望ましいといわれています

選択肢A. で紹介したルールはすでに知られています
覚えやすい自分だけのルールを決めてください

- アプリの先頭と末尾のペアを２、３文字目に入れる
- 加えて、真中を”_”で分割する
- 加えて大文字、小文字を繰り返す
  など

Q4. ロック番号やパスワードはどうやって覚えておく？

A. メモに書いて、スマホケースにコッソリしまっておく

これなら、忘れてもすぐに取り出せる

B. いつも使う手帳に書いておくか、
パソコンの表計算ソフト、
パスワード管理ソフト
（有料）で管理する

ヤマオリ

A4. 正解は　B.

紙に書いたロック番号やパスワードをスマホケースに入れたり、貼ったりしないでください

なぜなら：スマホを落とした時や、ちょっと机に置いておいた時、悪意のある人に見つけられて、勝手に操作されるかもしれません

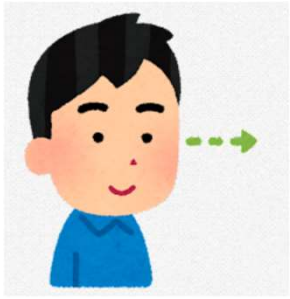
ロック番号やパスワードのメモがスマホケースのポケットに格納されているかもしれないことは、だれでも予想がつき、悪意のある人に簡単に見つけられてしまいます
また、メモを無くしたとき、ご自身も困ります

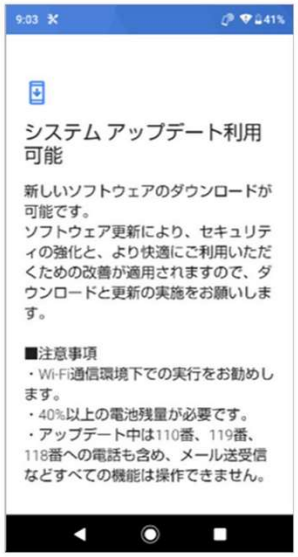
手帳で保管する時、外出では携帯せず、コピーを鍵のかかる机にいれて家人に場所を伝えておくと安心です
パソコンでの管理もお勧めです
スマホでパスワードを自動入力もできます

Q5. システムやアプリの更新（アップデート）のお知らせはどうしますか？

A. 更新する

新機能が使えるようになったり
不具合が修正されるから
できるだけ早く更新する





B. 無視する

手順が分からないし、
時間も手間もかかる
通信料もかかる
今のままでも十分使えている

ヤマオリ

A5. 正解は　A.

更新（アップデート）のお知らせは無視せず、できるだけ早く更新してください

なぜなら：誤動作が修正されたり、新しい機能が追加されるだけではなく、安全・安心を高める機能も追加されるからです

さらには
- バッテリーの消費を抑える機能
- メモリーの消費を抑える機能

なども追加されることがあります

更新は Wi-Fi （無線）環境のあるスマホショップなどで行うと通信量（xxギガ/月）を消費しないですみます

システムの更新は、「設定」から
アプリの更新は
- アイホンなら App Store から
- アンドロイドなら　Playストア　から

Q6. 駅や喫茶店などのフリーWi-Fi（無料）をどのように利用しますか？

A. 家と同じように利用する

美味しいお茶を飲みながらSNSやネットショッピングがゆっくり楽しめる

B. 情報検索だけにする

GoogleやYahoo!の検索、乗換案内、地図検索、ニュースの閲覧程度にする

SNSやネットショッピングのときは、Wi-Fiをオフにする

A6. 正解は　B.

フリーWi-Fiではネット検索だけにして、SNSやネットショッピング等はしないようにしましょう

なぜなら：通信の保護度合が低かった場合、悪意ある者に「ユーザーID」や「パスワード」などが傍受される可能性があります

ドコモ、ソフトバンク、au のショップなど

①公衆Wi-Fi　通信事業者が市中で提供するWi-Fiスポット
安全（各社、利用条件がことなる）

②フリーWi-Fi　駅、喫茶店、ホテル、コンビニなど（PW有/無）
ルーター管理者PWが甘いと乗っ取られる

③野良Wi-Fi　フリーWi-Fiになりすました悪意のあるWi-Fi
危険、ネットワーク名では区別できない
SSL(https://～)通信でも危険

また、後ろにいる人から、操作をのぞき見されるかもしれません

Q7. スマホに発信元名が表示されなかったり、電話番号「非通知」の電話着信が来ました。どうしますか？

A. 出ない

表示されないということは
発信元がスマホの連絡先
リストに無いということだから
無視
「非通知」はあやしいので
無視

B. 出る

宅急便からの連絡かも
しれないので出る

A7. 正解は　A.

スマホに発信元名が表示されない着信や、
「非通知」の着信は「出ない」でください

なぜなら：スマホの連絡先リストに登録のある人からなら、
発信元名が表示されます
「非通知」は、発信元が電話番号を故意に隠しています

番号が表示されても、心当たりのない番号に出たり、
その着信履歴からかけ直すと、あなたが「不審な電話にも
出る人」であることを相手に伝えてしまいます

「非通知」でなければ着信履歴から着信拒否やブロックの
設定ができます

海外からの着信（+から始まる番号）
にはかけ直さないでください
ワン切詐欺で法外な通話料を
請求されることがあります

Q8.メールやSMSで来たインターネットの飛び先（URL）はどうしますか？

A. 好奇心から、即タップ　　B. 絶対にタップしない

インターネットの飛び先（リンク先）　を　URL と呼びます
（Uniform Resource Locator
ユニフォーム　リソース　ロケーター）

- https://www.xxx.yyy/ のような表示形式
  か、または
- ここです　のように下線付きの青字で表示され
  タップすると、飛び先に飛んで表示されます

ヤマオリ

A8. 正解は　B.

ほとんど詐欺サイトへの飛先だと思ってください
正式ホームページからアクセスしてください

なぜなら：本物そっくりの贋のページに
誘導され、そこへ入力したID、パスワード、
クレジットカード番号などを盗まれてしまう
かもしれません。フィッシング詐欺といいます。
添付ファイルはウィルスかもしれません

Fishing ➡
Phishing

怪しい発信元、文章、URLの見分け方

- 発信元として銀行、クレジットカード会社、xxPay、公的機関（eTaxや役所）、スマホ会社、宅配便会社、Amazon、メルカリ、えきねっと　などを名乗ることが多い
- 「ご本人のお取引かを確認したい」、「ご不在で配達できませんでした」、「料金が未納です」、「クレジットカードの再登録が必要です」 などの文言が多い
- 日本語としておかしい、漢字の使い方がおかしい
- 氏名の記載がない（犯人はTEL番号、メルアドしか知らない）

不審な部分をコピペしてネット検索すると、「口コミ」で
詐欺とわかることが多いです

シニアのスマホ 安全安心 クイズ （少し慣れてきた方編）

V1.7 2024.06.10

Q1. SNS（ソーシャルネットワーキングサービス）で友人の顔写真と名前を掲載してよいでしょうか？

LINE, Facebook, X, Instagram・・・

A. 個人情報なので掲載しない　　B. かまわない

A1. 正解は　A.

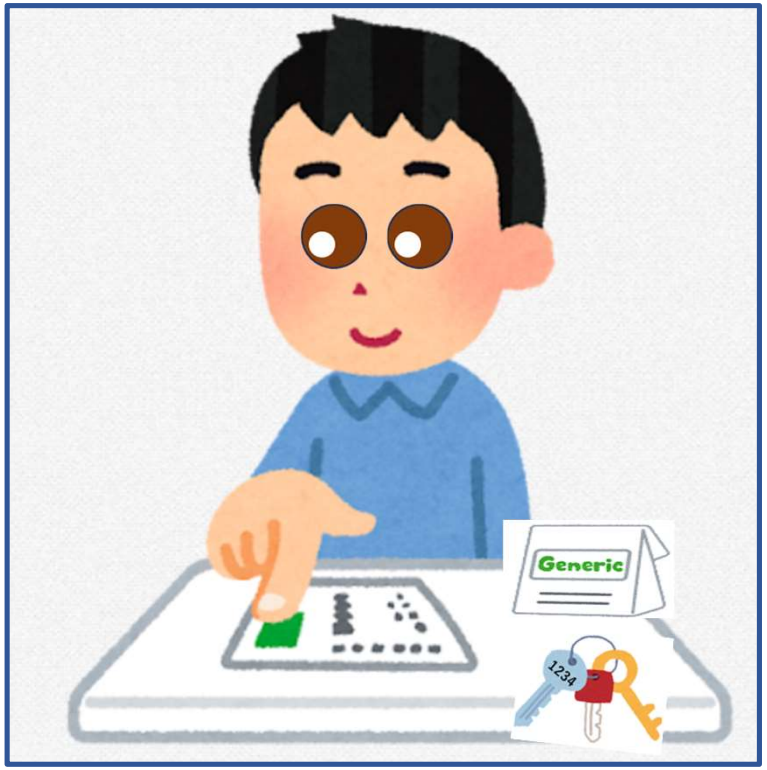
本人の了解を得ていないものは掲載できません

そのほか、SNSでの注意点があります

- 個人情報を掲載しない（了承を得ていない人や孫、通行人、住所や氏名がわかる写真など）
- SNSに近況掲載は要注意！「今、家族旅行中です」と掲載するのは、「家は留守です」と宣伝しているようなもの
- 特定の個人や団体を批判、攻撃、誹謗、中傷しない
- 著作権や肖像権のある物は掲載しない（侵害と知っていながら閲覧したり、ダウンロードすることも違法です）
- 確信が持てない情報は転送、拡散しない（SNSは匿名ではなく発信元のスマホを特定できます）（流言飛語を投稿した者は処罰されることもあります）
- 会ったことのない人とはつながらない（慣れるまでは公開範囲を「友だち」だけにしておきましょう）

なぜなら：個人情報が拡散したり、SNSで炎上したり、被害にあったり、訴えられたりする可能性があります
誹謗、中傷、情報流出は一人で悩まず、スクショを撮ってみんなの人権110番へ相談　☎ 0570-003-110

Q2. スマホで撮ったこの写真を LINE に投稿したり、メールで送付してはいけません なぜでしょうか？



A2.　写真を送ったり、SNSで公開する時は、余計な物（情報）が写っていないかを十分確認してください

なぜなら：写真は拡大でき、葉書で住所が、薬の袋で病気が、瞳に映り込んだ風景で場所が、鍵から鍵番号がわかります

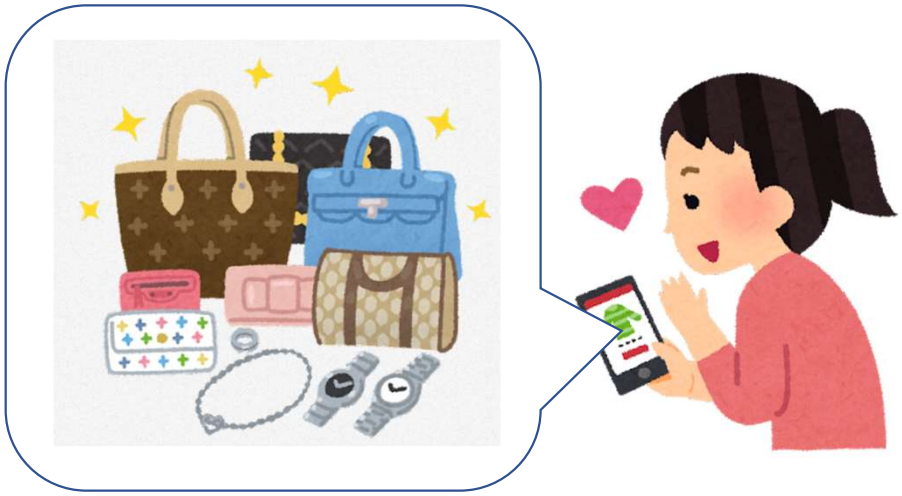
また、写真についている位置情報（GPS）から、自宅の場所、子供や孫の学校や、いつもの遊び場所などがわかってしまうのでメールでの送付は危険です
（ほとんどのSNSアプリでは、写真を投稿すると自動で位置情報が削除されます）

その写真に位置情報がついているかは、アイホンの「写真」アプリ、アンドロイドの「Googleフォト」共に、写真を上にスライドして詳細情報を表示すると分かります
スマホの設定で、写真に位置情報を付けないように設定できます

Q3. 欲しかったブランド物がネットショッピングで激安で売りにだされていた

A. 売り切れになるまえに、即オーダー

B. ブランド物が激安とはなにか怪しい点がありそうなので見合わせる



A3. 正解は　B.

ネットショッピングで「無料」、「激安」、「異常に安いブランド物」は詐欺の可能性が高いです

なぜなら：購買意欲に付けこむ悪意（個人情報搾取、偽物、詐欺）が仕込まれていることが多いです

ネットショッピングは「クーリングオフ」できません
（一定の期間内であれば申し込みや契約が解除できる制度）
PayPalやAmazonでの決済であれば、返品、返金できるケースがあります

一回きりの購入なのか、定期購入（サブスクリプション）なのか、よく確認してから購入してください
「あとxx分で終了」と焦らせたり、「一度お試し」とあっても定期購入になるなどの「ダークパターン」に注意

ネットオークションは物欲からついつい高額入札しがちです
出展者が別のアカウントを使って、せり上げることも
あらかじめ上限を決めてから臨んでください

Q4. ネットショッピングで欲しいものが見つかった初めてのショップだけどクレジット決済していいかな？

A. 是非購入したいので
クレジットカードを登録する

B. 有名なショップではないし
今回しか決済しないので
クレジット登録はやめておく

A4. 正解は　B.

クレジットカード決済は一度きりのネットショッピングでは行わないでください

なぜなら：カード情報の悪用、流出の可能性があります
良く使う有名なショップを十分確認して登録しましょう

海外ショップも含めホームページ記載の住所からGoogleマップやストリートビューで実在を確認してください
ホームページに掲載された電話番号は、赤の他人の番号を勝手に掲載していることもあります

ネットショッピングで被害を最小限にできる決済方法です

- PayPal決済
- ワンタイムクレジットカード
- ネットショッピング用のクレジットカードを
  作成し決済口座に都度入金
- コンビニ決済（コンビニの窓口支払い）➡
- カードの決済上限額を低く設定
- キャリア決済（スマホ通信料と一緒に引き落とし，
  スマホ会社がショップと決済契約していて確かです）

Q5. ネット決済の確認はどうしていますか？

A. アプリで購入履歴を
頻繁に確認
毎月のクレジットカード
利用明細をチェック

B. 特になにも必要はない

購入履歴

クレジットカード
利用明細

A5. 正解は　A.

アプリで頻繁に購入履歴を確認、
毎月のクレジットカード利用明細をしっかりと
確認してください

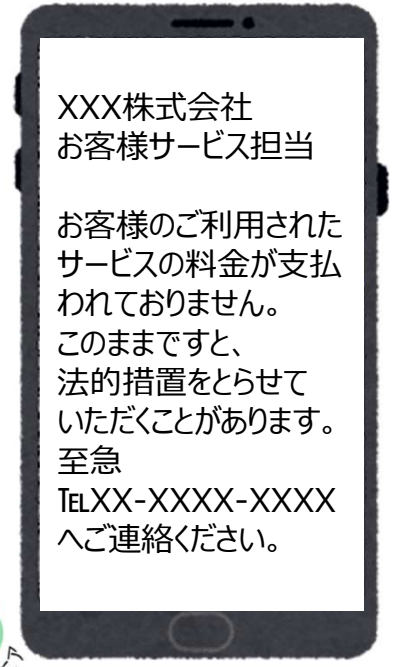
なぜなら：アカウントが乗っ取られると、少額で気が付きにくい
取引が頻繁におこなわれるケースもあります

異常な決済を発見したら、すぐにクレジットカード会社に連絡
してください

Q6. メールやSMSで「まだお支払いがありません。法的手段をとらせていただくことがあります」とメッセージが送られてきた！

A. 急いで返信するか、指定の飛先（リンク）や電話先に連絡をとる

B. 特になにもしない無視する



A6. 正解は　B.

心当たりのない架空請求、不当請求が来たら、
返信しない、支払わない、
メールを受信拒否して削除、
場合によっては消費者ホットライン 188 へ相談

なぜなら：返信すると、「あなたがその請求に関心を持った」ことを相手（加害者）に伝えることになります

また「ウィルス感染を検知しました。
クリーンアップを請け負います。
XXへご連絡ください。」という
高額詐欺も報告されています

それらの文面の特徴的な部分をコピペして、ネット検索すると「架空請求」、「不当請求」とわかることがあります

決して反応せず、
無視しましょう

最近の　スマホ詐欺の話題　２つ

スマホ詐欺の
ニュースに
敏感に！

① お店の決済や、外出先のQRコードを
スマホで読み取る時は、要注意

本物のQRコードの上から偽のQRコードが
張り付けられている場合があります

何がおこる？
- 偽の（犯人の）
決済先に入金される
- 悪意のあるアプリの
導入に誘導される
- 偽のウェブサイトに
誘導され、個人情報
の入力を促される

② 著名人をかたったLINEでの投資詐欺

著名な投資スペシャリストをかたる詐欺師と
SNSで知り合う（インスタグラムの広告クリック
などで）

↓

その人から　LINEの
「投資クラブ」（わな）に
参加を勧められ参加

↓

「投資クラブ」の参加者は
数十人で、全員が利益を得ているよう
なトークやグラフのやり取り（全て偽）で信用

↓

投資を勧められ、送金してしまう
利益が出ているようなトークをもらい、さらに送金
解約しようとすると違約金を請求され送金

シニアのスマホ　安全安心　チェックリスト

どなたでも必須の8つのチェックリスト

- □ 1. スマホの電源をいれたとき、スマホを開く鍵となるロックを必ず設定してください
- □ 2. ロック番号やパスワードを誕生日、電話番号、単純な1234などにはしないでください
- □ 3. 複数のアプリでパスワードを使い回しはしないでください
- □ 4. 紙に書いたロック番号やパスワードをスマホケースに入れたり、貼ったりしないでください
- □ 5. システムやアプリの更新（アップデート）のお知らせは無視せず、実行してください
- □ 6. 駅や喫茶店などのフリーWi-Fiではネット検索だけにして、ネットショッピング等はしないようにしましょう
- □ 7. スマホに発信元の名称が表示されない着信や、非通知からの着信は「出ない」、心当たりのない着信履歴には「かけ直さない」でください
- □ 8. メールやSMS（ショートメッセージサービス）で来たインターネットの飛び先（URL）や添付ファイルは、送信元を十分確認してからタップして下さい

加えて、スマホに少し慣れてきた方の６つのチェックリスト+

- □ 1. LINEやFacebookなどのSNS（ソーシャルネットワークサービス）では、個人情報の流出、誹謗中傷、流言飛語、著作権・肖像権侵害などに注意しましょう
- □ 2. 写真をSNSに公開したり、メールで送る時は、余計な物が写っていないか、位置情報が付いていないか十分確認してください
- □ 3. ネットショッピングで「無料」、「激安」、「異常に安いブランド物」には注意が必要です
- □ 4. クレジットカード決済は一度きりのネットショッピングでは行わないでください
- □ 5. アプリで頻繁に購入履歴を確認し、毎月のクレジットカード利用明細を確認してください
- □ 6. 架空請求、不当請求が来たら、返信しない、支払わない、メールを受信拒否して削除、場合によっては消費者ホットライン 188 へ相談
- □ 最近のスマホ詐欺のニュースに敏感に！

おわり