困った時に開く

スマホ安全手帳

ネット被害を防ぐための知識

※詐欺メール、詐欺警告、LINE のっとりなど

2024 年7月13日(7/10 版)　YO_Takatsuki

目次

目次（続き）

1．はじめに

シニアの方のスマホ利用が広がる中、ネット被害が急増しています。不安をあおるメッセージがスマホに表示され、怖い、対処方法がわからないなどの相談をよく受けます。
そこで、シニアの方向けに、被害や不安に対処できるよう、必要な知識をまとめました。

本書は、パソコン・スマホの相談会や教室にて、希望者の方に、実費（印刷代のみ）にて、配布させていただいております。
シニアの方々のスマホライフを支援するための一助になることを願っています。

2. 用語集

	用語	内容
あ	**アイコン**	例.  例のようにアプリを表す小さな画像で、タップでアプリが起動する
	アカウント	お店の会員権に相当し、ID とパスワードによりログイン（入店）し、お店のサービスを受けることができる
	IDと パスワード	お店に例えると、ID は会員名、パスワードは暗証番号に相当。会員が入店する際の本人確認のために使われる。
	アップデート	OS やアプリを新しくすること。 セキュリティ強化、不具合の改善、機能強化が目的。
	アプリ	メール閲覧、地図、カメラなど、特定の目的をもって作られたソフトウェア
	アプリストア	アプリを入手する為のお店。Android は、  Google プレイ、iPhone は、「  App ストアのアプリを使う。
	インストール	ダウンロードしたアプリをスマホで、使えるように登録すること
	ウェブサイト （ウェブページ）	インターネット上のお店 （別名 Web サイト））
	OS （オーエス）	スマホの基本ソフト。アンドロイドと、iOS（iPhone）の 2 種類があり、操作方法が異なる
か	**画面ロック**	電源オン時に他人に不正利用されないようスマホの画面に鍵をかける機能。暗証番号や指紋認証などで解除する

さ	ショートメッセージ	電話番号で送信・受信するメール 略称は SMS
	スクショ（スクリーンショット）	画面を写真として、スマホに保存する
た	ダウンロード	ネットから、写真やアプリなどを入手し、スマホに保存すること
	タップ	アイコンやメニューを指で軽く叩いて、すぐ離す動作。アプリの起動やメニューの選択に使用。
な	２段階認証	パスワードに対し、第２の本人確認を追加し、パスワードをより強固にする
は	バックアップ	データを失っても、復元できるように複製すること
	ブラウザ	インターネットの閲覧や検索をするためのアプリ　　例．Chrome、Safari
	ホーム画面	スマホを起動すると初めに表示される画面。操作の起点になる
	ホームボタン	ホーム画面に戻すボタン
ら	リンク	「http～」やボタンで表示され、タップすると、ウエブページに進む。
	ログイン	ネット上のお店への入店に相当します。ログインにはＩＤとパスワードの入力が必要になる。
	履歴ボタン	開いたアプリの一覧を表示 別名：タスクボタン、アプリ履歴ボタン
わ	WiFi（ワイファイ）	無線で提供されるインターネット回線。スマホを WiFi に接続することで、無制限にインターネットが利用できる

3．スマホの安全対策８か条

安全対策は8つに集約されます

1 詐欺メールや偽ウェブサイトに騙されない！

2 メール内のリンクや電話番号に注意！

「4. 詐欺メール・詐欺広告 P7-10

3 パスワードは長く、複雑に使いまわしはしない！

「6. 安全なパスワード」P13-16

4 パスワードだけでは不十分 2 段階認証で 2 重に防御

「7.画面ロック」P17

5 紛失時に備え画面ロックを設定

「8. OS とアプリを最新にする」P18-20

6 OS やアプリは常に最新状態に

「11. データをバックアップ」P26

7 大切なデータをバックアップ(複製)

8 信頼できる窓口に相談しよう

「12. ネット被害相談窓口」P27 参照

4.詐欺メール・詐欺広告

不安あおる詐欺メール

大半が詐欺で、実存の機関名を騙ります

・××電力
【重要】未払い料金のお知らせ

・YY 銀行
【至急】カード不正利用の連絡

XXX 運輸です
ご不在の為、荷物を持ち持ち帰りました。
ご確認ください https:xx.yy.zzx

開くと、電話番号やリンクがあります

例）・**感染しました！**至急、連絡ください
TEL○○○○

・**不正利用**があり、至急、確認ください
https:XXXXX

電話やリンクをタップすると

本物そっくりの企業の画面や偽担当者が、パスワード、クレジットカード番号を入力させる、または高額請求へ誘導します

4.詐欺メール・詐欺広告

詐欺メールの対策

対策

・企業、公共機関であっても、不安をあおるメールは開かない

・電話やリンクのタップはせずに閉じる

・パスワード、クレジットカード番号は不用意に入力しない

さらに

・スクリーンショットを撮って、身近な詳しい人や公共の相談窓口に相談

☛P11,P27 参照

・検索アプリで調べる

相手の連絡先を調べ、問い合わせる
同様のメールの情報がないか検索

☛P25 参照

さらにさらに

メール内リンクは避け、検索アプリや専用アプリから、ウェブページを開くようにする

☛P25 参照

4.詐欺メール・詐欺広告

突然、現る不安あおる警告

大半が悪質な広告

アプリのインストールや動画視聴をさせ、
高額請求、または個人情報を盗もうとします

例

対策

- 警告を閉じる　☛方法は次頁参照
- ボタンやリンクは無視

さらに

ボタンやリンクをタップしてしまったら、
アプリの削除やパスワード変更などが必要な場合があります
身近な詳しい人や、公共機関に相談
☛P27 参照

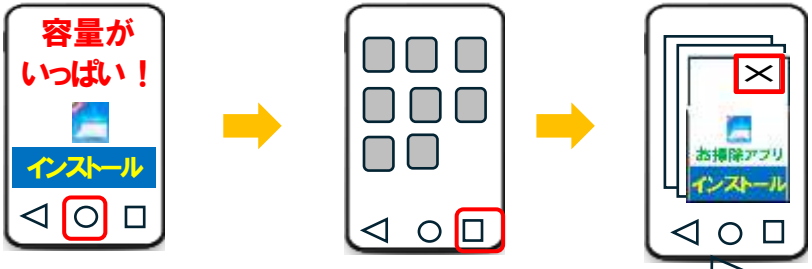
警告を閉じる方法

方法 警告を閉じる方法

①ホームボタンで、ホーム画面に戻す

②履歴（タスク）ボタンでアプリの履歴を表示

③閉じるボタンで全てのアプリを閉じる



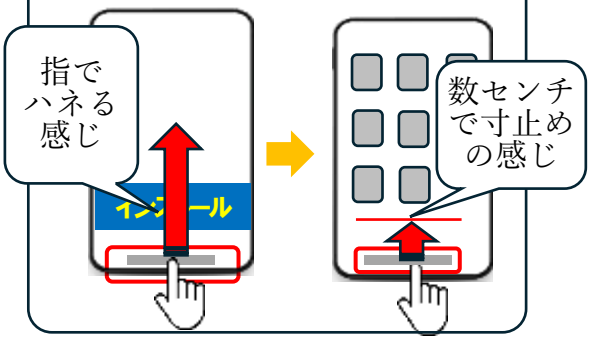
「すべてのアプリを閉じる」ボタンがあれば、それを使うとよい

※③機種によっては、アプリに指を置き上側へハネて閉じる機種もあります

※①②のボタンについて
ボタンがない機種もあり、その場合は下記を参照

①画面の下から上に指でハネる（途中で指を離す）

②画面の下から上に指でなぞり止めて離す



補足

どうしても消せない場合は、スマホを再起動してから②、③を行います

5.スクリーンショット

トラブル時は画面をスクショ

画面を写真として記録※します

※スクショ(スクリーンショットの略)と呼びます

相談する時に、より適切な回答がえられます

スクショを撮る画面の例

警告画面

メールの内容

XXX 運輸です
ご不在の為、荷物を
持ち持ち帰りました。
ご確認ください
https:xx.yy.zzx

誇大広告

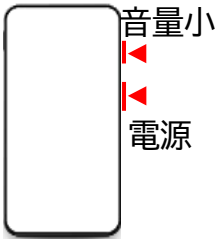
方法 電源ボタンと音量ボタンを同時に押す
（機種によって違います）

約 2 秒、画面に反応または、シャッター音があれば成功

iPhone

ホームボタン
がある場合

アンドロイド



5.スクリーンショット

スクショ（スクリーンショット）の方法

スクショがうまくいかない場合は？

チェックポイント

・音量キーと電源キーを同時に押していますか？
・キーを間違えていませんか？
・機種によっては、設定が必要、未対応の場合もあり、スマホの取説を確認してください

機種によっては、より簡単な方法があり、
取説を確認してみてください

保存場所

撮った画面は、写真アプリに入ります

例

フォト

補足

写真アプリの共有（または送る）機能を使って、相談者にメールや LINE でスクショを送れます

例 共有アイコン

6.安全なパスワード

基本知識：アカウントとは？

アカウントは、お店の会員権に相当し、IDとパスワードにより入店し、買い物できる状態（ログイン）になります。

アカウント関連用語

・**アカウント**：お店の会員権に相当
・**ID**：会員名に相当（メールアドレスが使われる）
・**パスワード**：暗証番号に相当
・**ログイン**：入店し買物できる状態に相当

よく使うアカウントの例

●Google アカウント

※サービスの例　メール　写真　地図　You Tube　Play ストア

●携帯電話会社のアカウント

例　d アカウント、auID、Softbank ID

●Apple ID（iPhone の場合のみ）

※サービスの例　メール　写真　App ストア

●LINE

パスワードの管理

●各アカウントごとに
ID、パスワードを１セットにし、専用の手帳に記録し、大切に保管

●2 段階認証（後述）の電話番号、
パスワード再設定用の電話番号も記録

●各パスワードは違うものにする
（使いまわしはしない）

Google アカウントの記録例

※1.誤読しやすい字には、フリガナや大文字表記入れる
※2. P30 付録「セキュリティ設定の確認方法」参照

【Google アカウント】	
ID	sample1@xxxxx.yy
パスワード※1	ｎｉＮｊｉｎ－４ｒｏ９ｍＡ＃ 大　　大 エヌアイエヌジェイアイエヌ- アールオーエムエー
2 段階認証用 電話番号※2	090-1234-5678
パスワード再設定 用電話番号※2	090-1234-5678
メモ	

安全なパスワードの作り方

推測しにくいことが大事です

・１０ 桁以上
・大文字／小文字／数字／記号を混ぜる
※記号の例 ！＃ ＄ ％ ＆ ( ) ^ ＠ -

作り方 2つの言葉から作る

例　野菜と動物

→ ninjin-sirokuma　ニンジン-白クマ
→ ninjin-4ro9ma　一部、数字におきかえ
→ninjin-4ro9mA#　一部を大文字、記号を追加

パスワードを作成後、パスワード専用の手帳に記録し、大切に保管しよう

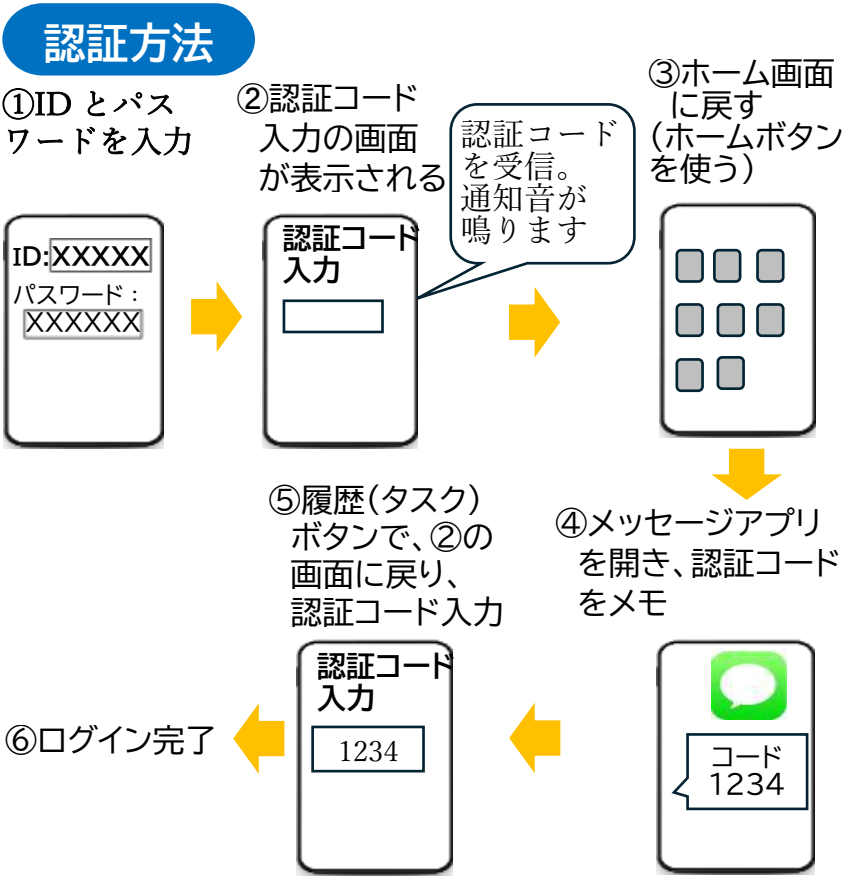
パスワードは、暗記の必要はありません。
１回目の手入力以降は、アプリやスマホが記憶し、以降、手入力は必要ないからです

２段階認証で防御を高める

パスワードに加え、電話番号やメールで本人確認をします。パスワードが漏洩しても、アカウントのっとりを防止できます

P13のよく使うアカウントも、２段階認証が推奨または、設定済みになっています。

認証方法



7.画面ロック

紛失に備え画面ロックは有効に！

スマホの紛失時に、他人の不正利用を防ぐことができます

解除方法は、機種により異なり、暗証番号、パターン、指紋認証、顔認証などがあります

無効の場合は、有効に設定しましょう

◆アンドロイド（機種によって異なります）

①「設定」

②「セキュリティと現在地情報」（または「ロック画面とセキュリティ」、「セキュリティ」など）

③画面ロックの方法を選択します

◆iPhone

①「設定」

②「Touch ID とパスコード」
または「FaceID とパスワード」

③パスコードを入力する

④「指紋を追加」
または「Face ID をセットアップ」

OS とアプリを最新にする

アップデートがあれば最新にします

最新のウイルスへの対応など、セキュリティを強化します。約２か月に１回は確認をお薦め

★アップデートする際の注意点
- **WiFi に接続をしましょう**
- **バッテリー残量が十分あること**
- **ストレージの空き容量が十分あること**

OS のアップデート確認方法

機種により異なります

iPhone

①「設定」 
②「一般」
③「ソフトウェアアップデート」

アンドロイド

①「設定」 
②「システム」
③「システムアップデート」

OS のアップデート通知

OSのアップデートは、画面上に通知で表示されます。
設定アイコンに赤い点が付くこともあります。

例

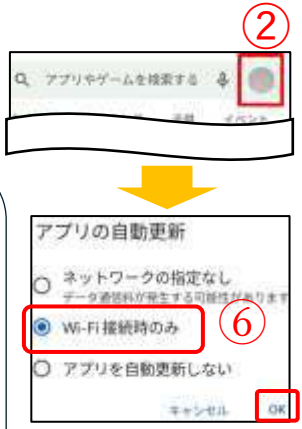
システム
アップデート
今すぐインストール
あとで

8.OSとアプリを最新にする

アプリの自動アップデート

アプリは自動アップデートに設定可
WiFi 環境ある方は有効がお薦め

アプリの自動アップデート設定



アンドロイド

①「Play ストア」をタップ
②画面右上の自分のアイコンをタップ
③「設定」→④「ネットワーク設定」
⑤「アプリの自動更新」
⑥「WiFi 接続時のみ」を選択し
「ＯＫ」

ｉPhone

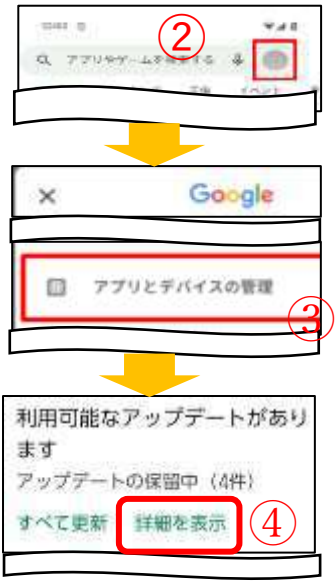
①「設定」
②下側にスクロールし、
App Store をタップ
③「アプリのアップデート」
を有効（緑色）にします
④モバイルデータ通信の
「自動ダウンロード」は無効

8.OSとアプリは最新にする

アプリの手動アップデート

自動アップデートは働かないこともあり、時々、手動でも確認しましょう

アプリの手動アップデート



アンドロイド

①「Play ストア」をタップ
②画面右上の自分のアイコンをタップ
③「アプリとデバイスの管理」をタップ
④「詳細を表示」をタップ

iPhone

①「App ストア」をタップ
②画面右上の自分のアイコンをタップ
③下側にスクロールし、「アップデート」の表示があればタップ

LINEの安全な設定

知らない人の友達追加や、LINE の乗っ取りを防止する設定です

設定方法

❶ LINE 画面の左下のホームをタップ

❷ 画面の右上の ⚙ をタップ

❸

パソコンや iPad で LINE をしない場合は以下のようにオフ

アカウント → ログイン許可

プライバシー管理 →
- IDによる友だち追加を許可
- メッセージ受信拒否
- Letter Sealing

友だち →
- 友だち自動追加
- 友だちへの追加を許可

※補足 オフ / オン

LINEのっとりの防止

ＬＩＮＥで、友達から、認証番号(4桁)を、求められた場合は、要注意！

※右のように求められた場合、認証番号を知らせてはいけません

ＬＩＮＥアカウントを盗まれた偽の友達が、あなたのＬＩＮＥアカウントを乗っ取ろうとしている可能性が高いです

対策

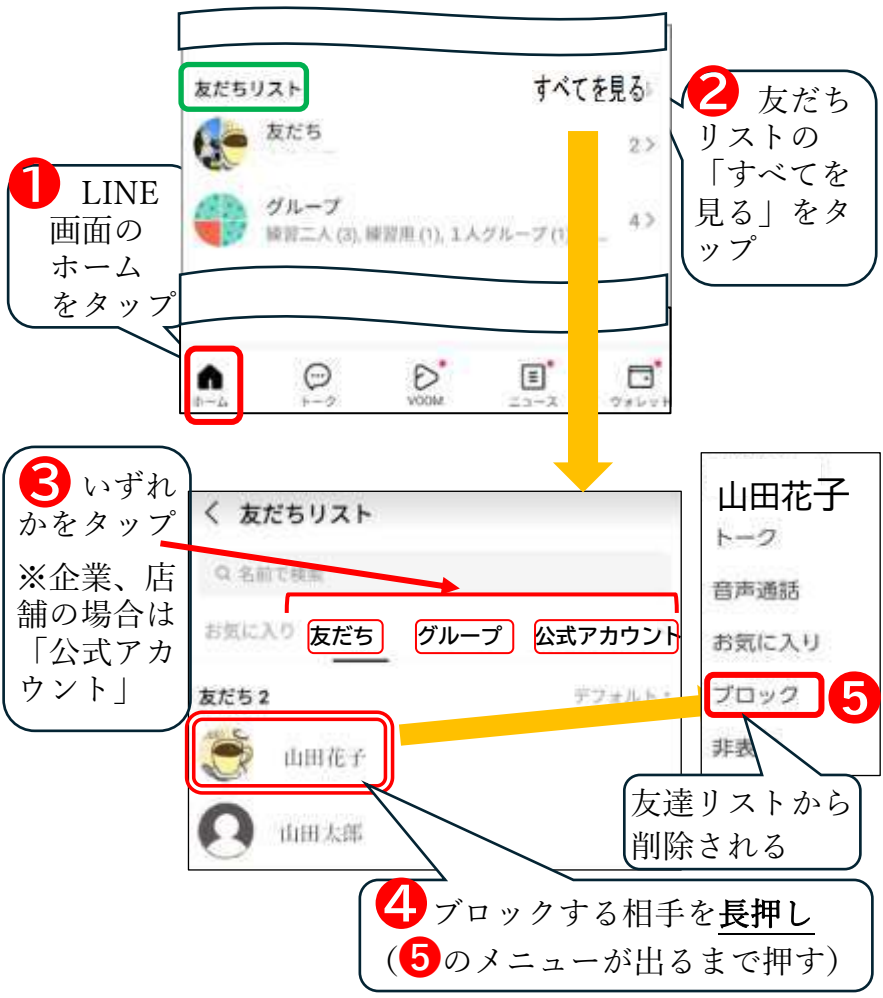
認証番号（４桁）を知らせてはいけません
友だちに電話またはメールで、問い合わせ
偽の友達と判明すればブロック（次ページ参）

知らない友達の削除

知らない人や、不要な企業・店舗からのメッセージは、ブロックしよう

※新たなメッセージは受け付けなくなります

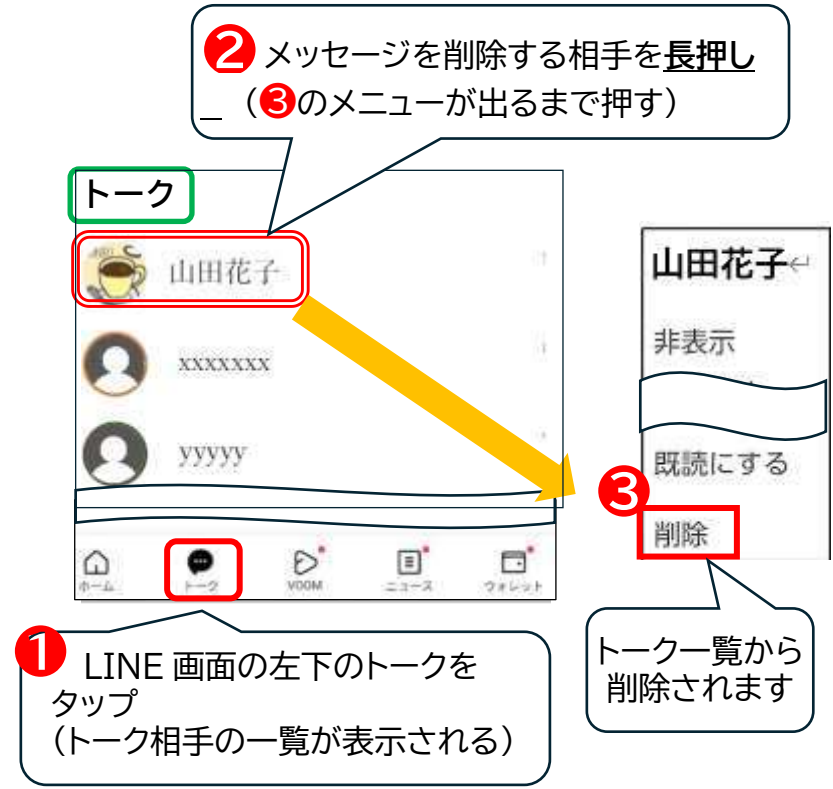
ブロックの方法



知らない友達の削除（続き）

ブロックしても、旧メッセージは残ります。旧メッセージを削除しましょう

旧メッセージ削除



検索アプリで被害を防ぐ

詐欺メールを一目で見分けるのは困難
検索アプリを活用しましょう

●その1:
リンクは、メール内からは開かずに、
検索アプリで、事前登録したリンクや、検索結果から得たリンクから開く　※またはアプリから開く

●その2:
怪しいメールは、検索で真偽を調べる

検索アプリ※の例
※ブラウザとも呼びます


Google


Chrome


Safari

補足

◆検索アプリには、リンクを事前登録するブックマーク※1という機能があります

※1 コレクションや、お気に入りと呼ぶアプリもあり

◆メール内容そのままを、検索アプリの検索欄に入力し検索すれば、ほぼ真偽がわかります

※詳細は、身近な人や、スマホ支援団体に相談ください

データをバックアップ(複製)

大切なデータを失う前にバックアップ

バックアップ設定方法

電話帳、メール、写真などをバックアップします

注)・LINE のメッセージのバックアップは、対象外です。
「LINE　バックアップ」で検索し、LINE が提供しているバックアップ方法を参照ください
・WiFi 接続が必要です
・機種により操作は異なり、必要に応じスマホ取説を参照

アンドロイド

①「設定」
②「Google」
③「バックアップ」をオン
④「今すぐバックアップ」

iPhone

①「設定」
②最上段の「ユーザ名」
③「iCloud」
④「iCloud バックアップ」
⑤上段をオン(緑色)
⑥下段をオフ
⑦ココをタップ

12.ネット被害相談窓口

ネット被害の公共の相談窓口

被害にあったら、相談しましょう

●消費者ホットライン１８８

（電話で１８８にかける）

自宅の郵便番号を入力すると地域の消費生活センター等につなげてくれます。

消費生活センターでは、解決の助言をしてくれます

相談内容例

（例）・断っても強引な勧誘が続く

・無料と聞いたのに、高額な請求をされ

詳細は右のQRコード
から参照ください

全国共通の電話番号
「消費者ホットライン」188
のリーフレットです

付録

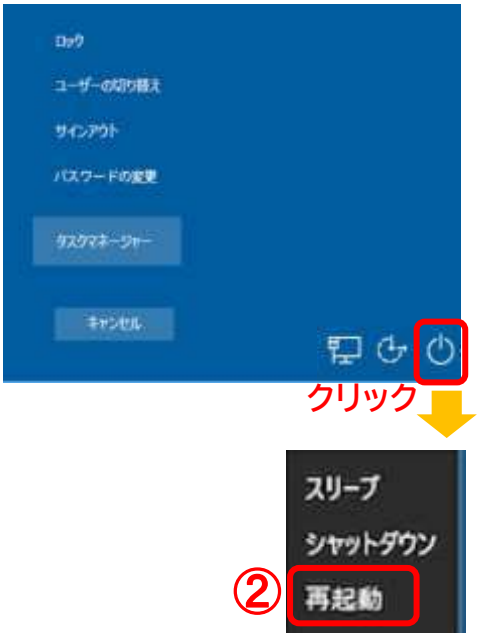
パソコン版

詐欺警告が表示された時の対処方法

操作中に突然、表示される警告は大半が詐欺

対策 以下の方法で警告を閉じます

①左手で Ctrl キーと
Alt キーをおしながら、
右手で DEL キーを押す
②右の画面に移行した
ら、右下の電源ボタン
をクリックし、
「再起動」を選択し
PC を再起動



付録

パソコン版

詐欺警告が表示された時の対処方法(続き)

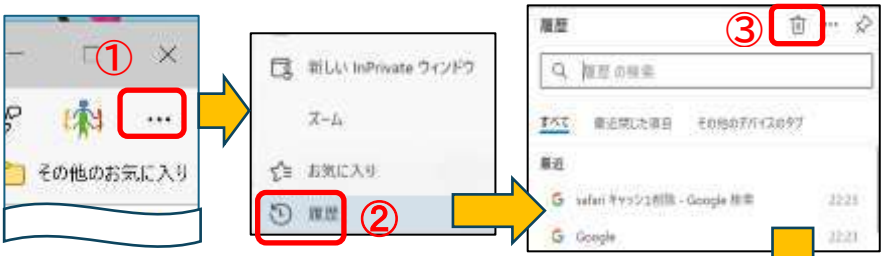
③再起動後、利用しているブラウザ(Edge, Chrome)の閲覧履歴データを全期間消去（下図参照）
④セキュリティソフトのウイルススキャン（フル）で、感染有無を確認

閲覧履歴データのクリアの方法

①Edge を起動し、「…」をクリック

②「履歴」をクリック

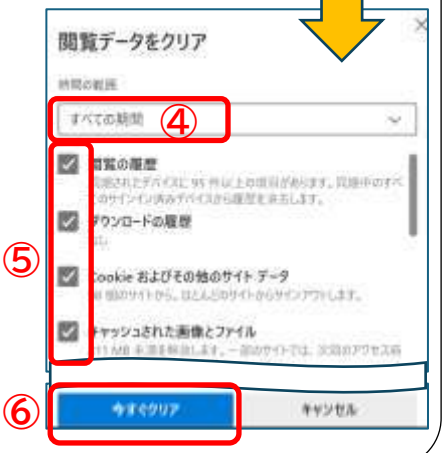
③（閲覧データをクリア）をクリック



④「すべての期間」を選択

⑤赤枠のみチェックが入っていることを確認

⑥「今すぐクリア」を選択
しばらく待つと終了し、
完了です



付録

セキュリティ設定の確認方法

※P14「パスワードの管理」の参考資料

Google アカウントと、iPhone の Apple ID アカウントを例にあげます。以下の確認や変更ができます。

- 2 段階認証の有効／無効
- パスワードの変更
- 2 段階認証のための電話番号の設定
- パスワード再設定用の電話番号の設定※1
- パスワード再設定用のメールアドレスの設定※1

※1．パスワードを忘れた時の再設定に使用

確認方法

●Ｇｏｏｇｌｅアカウント

①検索アプリで Google 検索ページを開く
②右上の自分のアイコン
③「～アカウントを管理」
④「セキュリティ」をタップ

●ＡｐｐｌｅＩＤアカウント

①「設定」
②「サインインとセキュリティ」

ネットでクレジットカード、銀行利用する方に向けて

付録

スマホ乗っ取り（SIM スワップ）の被害(1/3)

●スマホのっとり(SIM スワップ)とは

電話番号をのっとる犯罪行為

※SIM＝電話番号を使う為の IC カード

犯人は、携帯店で、スマホ紛失を理由に、偽身分証明書で SIM 再発行を依頼し、電話番号をのっとります

●犯人の目的

盗んだ電話番号と、詐欺メールなどで盗んだ ID、パスワードとをあわせ、あなたの銀行や、ショッピングサイトに侵入(ログイン)し、**クレジットカードで買い物や不正送金をしようとします**

●見分け方

どの場所でも、以下の症状がずっと続きます

- **電波マークが消え圏外表示となる**
- **電話、LINE、メールが使用不能となる**

スマホ乗っ取り（SIM スワップ）の被害(2/3)

●対策

・**「安全対策 8 か条」を守り**、パスワード漏洩を防ぐ

・**個人情報**（住所、氏名、生年月日、電話番号）**を、ネットに出すのは必要最小限にし**、偽造身分証明書を防止する

・電波マーク  **の圏外表示を定期的に確認**

・利用しているサービスの以下メールはチェック

　・**覚えのない送金や注文の通知**※1、※2、※4

　・**覚えのない SIM 再発行の通知**※1、※3、※4

　※1通知が来るよう設定しておく

　※2もしあれば、アプリまたはブラウザで確認

　※3もしあれば携帯電話会社に電話で確認

　※4メールのリンクは開かないこと

・**スマホ上の決済やネット銀行の送金に上限金額を設定**

クレジットカード口座には必要最低の金額

（・できれば、2 段階認証に電話番号認証を止め、固定電話、PC 専用メール、認証アプリや生体認証に変更）

スマホ乗っ取られた時の対応(3/3)

SIM スワップの症状なら、即、携帯電話会社に確認し、乗っ取りなら、即、電話番号の停止

電話番号停止の後すぐに行うこと

●電話番号を紐づけているサービスに対し
・ID とパスワードとメールアドレスを変更
・不正利用あれば、サービス会社に一時利用停止

●ネットバンキングを利用している場合
銀行に不正送金確認と口座利用停止を相談

●クレジットカード会社に
不正使用確認と即停止要請

●専門の相談窓口に相談！
「12. ネット被害相談窓口」P27参照
または最寄りの警察