特集

乗っ取り&詐欺 新防衛術32

いつものニュースページを見ただけでウイルスに感染――まさかと思うかもしれませんが、本当の話です。最近のネット犯罪者の手口は実に巧妙。あなたも常に狙われているのです。パソコンやスマホが乗っ取られたり、悪質な詐欺の被害に遭ったりしないための最新防御術を紹介しましょう。

文／海岡 史郎、岡村 秀昭、原 如宏、山原 雄海、小野 幸伸
イラスト／朝倉 千夏
扉イメージ写真／渡辺 慎一郎（スタジオキャスパー）

金銭・個人情報・のぞき見・乗っ取り…あの手この手で、あなたも狙われている！

これが2018年情報セキュリティ10大脅威だ!

1位	インターネットバンキングやクレジットカードなどの不正利用
2位	ランサムウエアによる被害
3位	ネットの誹謗（ひぼう）・中傷
4位	スマホやスマホアプリを狙った攻撃
5位	ウェブサービスへの不正ログイン
6位	ウェブサービスからの個人情報の窃取
7位	情報モラル欠如に伴う犯罪の低年齢化
8位	ワンクリック請求などの不当請求
9位	IoT機器の不適切な管理
10位	偽警告によるインターネット詐欺

図1「情報セキュリティ10大脅威」は独立行政法人 情報処理推進機構（IPA）が毎年発表しているランキング。個人向けと法人向けの脅威をそれぞれ発表しているが、上の表は個人向けのもの。専門家で構成される「10大脅威選考会」が、2017年に発生したセキュリティ事故や攻撃の状況などから脅威を選出し、投票により順位付けをしている

上の表は、独立行政法人 情報処理推進機構（IPA）が発表した「情報セキュリティ10大脅威2018」の結果だ（図1）。1位の「インターネットバンキングやクレジットカードなどの不正利用」をはじめ、金銭を狙われる手口が多く入っている。

特に最近被害が拡大しているのは、2位のランサムウエア。いわゆる「身代金ウイルス」と呼ばれるもので、感染するとパソコンやスマホのファイルが暗号化され、金銭を支払えば復旧してやると脅迫してくる（図2）。もちろん金銭を支払ったからといって元に戻る保証はない。恐ろしいのは、普段見ているウェブサイトに不正広告が仕組まれ、そのサイトを表示しただけで感染してしまうケースがあることだ（図3）。10位の偽警告は、ウェブサイトの閲覧中に突然「ウイルスに感染しました」といった警告画面が現われ、不正なソフトをインストールさせたり、不当なサポート契約を結ばせて金銭を要求する手口（図4）。手口としては古典的だが、最近は音声を流したり、マウスポインターが勝手に動くアニメーションを仕組んだりと、あの手この手で不安をあおってくる。

パスワードの使い回しは厳禁 家電製品も狙われる

5位の不正ログインで注意したいのは、パスワードの使い回しだ。一度パスワードが流出してしまうと、ショッピングサイトで勝手に買い物をされたり、ウェブ上の写真を盗み見られたりと、金銭的被害だけでなく個人情報も丸裸になる可能性がある（図5）。

9位のIoT機器では、掃除機ロボットが乗っ取られた事例が報告されている（図6）。勝手に操作されるだけでなく、カメラ付きの製品では室内をのぞき見られてしまう。家電とはいえインターネットにつながっている以上、常に脅威にさらされているのだ。

「自分だけは大丈夫」と思っている人も多いだろう。しかし、手口はますます巧妙化し、誰が被害に遭ってもおかしくない状況となっている。また、自分の知らないうちに、自ら危険に飛び込んでしまっている場合も非常に多く、約10世帯のうち、何と9世帯が不正サイトにアクセスしていたという調査結果もあるほどだ[注]。

こうした危険から身を守る最新の防衛術を次ページ以降で紹介していく。

[注]トレンドマイクロによる「ホームネットワークセキュリティ製品「ウイルスバスター for Home Network」モニターログデータまとめ」より

手口はますます巧妙化している

ここでは、脅威の実例をいくつか紹介しよう。どの場合も、パスワードを使い回さない、OSやソフトを更新して最新にするなど、セキュリティに対する基本的な心構えが大切なのがわかる。

突然の警告画面 慌てて偽サポートに電話

対策
- ブラウザーをすぐに終了
- 警告が表示されても指示に従わない
- 日ごろから事例や手口の情報を収集しておく

図4 サイトを閲覧していたら、突然「ウイルスに感染しました」という警告画面が表示され、不正なサポート契約などを結ばせようとする手口も後を絶たない。最近は、音声を流したり、アニメーションを駆使したりと手の込んだ仕掛けで不安をあおってくる。ウィンドウズやブラウザーがそうした警告画面を出すことはないので、すぐにブラウザーを終了しよう。決してソフトをインストールしたり、電話をかけたりしないこと

パソコンがロック、身代金を要求

対策
- メールやウェブサイトをしっかり確認
- 添付ファイルやリンクを安易にクリックしない
- OSやソフトを更新して最新に
- 大切なデータはバックアップ
- セキュリティ対策ソフトを導入

図2 パソコンやファイルがロックされ、その解除のための身代金を要求してくる。こうしたランサムウエア対策として、大切なデータはクラウドなどにバックアップしておくのも有効だ

勝手に買い物 ウェブ上の写真がのぞき見られる

対策
- パスワードを使い回さない
- できるだけ長く複雑なパスワードにする
- 2段階認証を有効にする
- 利用していないサービスは退会する
- クレジットカードの明細を定期的に確認

図5 パスワードを使い回していると、利用しているサービスに次々と不正にログインされる可能性がある。この特集では、パスワードの管理方法（60ページ）や、複雑なのに覚えやすいパスワード作成法（61ページ）も紹介しているので参考にしてほしい

掃除機ロボットが乗っ取られる

対策
- 初期パスワードを複雑なものに変更
- ファームウエアを更新して最新版に
- 使用していないときは電源を切る
- 廃棄や下取りに出す前に初期化
- 被害を受けたらすぐに電源を切る

図6 家電とはいえインターネットにつながっている以上、常に脅威にさらされている。実際に掃除機ロボットが乗っ取られた例が報告されており、カメラ付きの製品の場合は、室内をのぞき見られる危険もある。ファームウエアを最新版にするなどの対策を怠らないようにしよう

対策
- OSやソフトを更新して最新に
- セキュリティ対策ソフトを導入
- 大切なデータはバックアップ

図3 ランサムウエアなどのウイルスは、不正なメールに添付されたファイルを開いたり、悪質サイトにアクセスしたりすることで感染することが多い。しかし、最近では普段見ているサイトに不正な広告を仕組んで、そのサイトを表示しただけで感染してしまうケースも報告されている。OSやソフトの脆弱性を悪用したものが多いので、常に最新の状態にしておこう

いつものサイトを見ているだけで感染!?

6 アカウントの乗っ取り対策には2段階認証が効果的！

アカウントを乗っ取られ、個人情報を盗まれたり、犯罪の踏み台にされたりする被害が相次いでいる。パスワードの使い回しなど、無防備なサービス利用が原因だ。こうした被害を防ぐ有効な手段が「2段階認証」。自分で設定したパスワードと、サービス会社が発行した“その場限り”の認証コード、2つが合致しないとログインできない仕組みだ（図1）。

コードの受け取り方法は、電話やSMSなど複数。いずれも攻撃者が盗み取ることは困難なため、乗っ取りを防げる。今ではグーグルやアップルなど、多くのサービスが導入済み。これらを安全に使うためにも、2段階認証の利用を勧めたい（図2）。

では、グーグルを例に2段階認証の設定方法を見ていこう。まずパソコンのブラウザーでグーグルを開き、ログイン。ページの右上に自分の名前がログイン名として表示されたら、このボタンを押して「アカウント」の「ログインとセキュリティ」へ進む（図3）。あとは開いたページにある「2段階認証プロセス」から設定していくだけだ。電話番号を指定し、今回はコードの受け取り方法に「音声通話」を選択する（図4）。すぐにグーグルから電話がかかってくるので、音声案内に従ってコードを入力すれば設定完了だ（図5）。

このほかグーグルでは、スマホ上で認証操作ができるプロンプト方式を提供（図6、図7）。コードを入力する手間がないので、ログイン操作が簡単だ。このほか、バックアップコードも用意しておくと、コードの受け取り手段がないときに助かる（図8）。

2つめの認証コードでがっちりガード

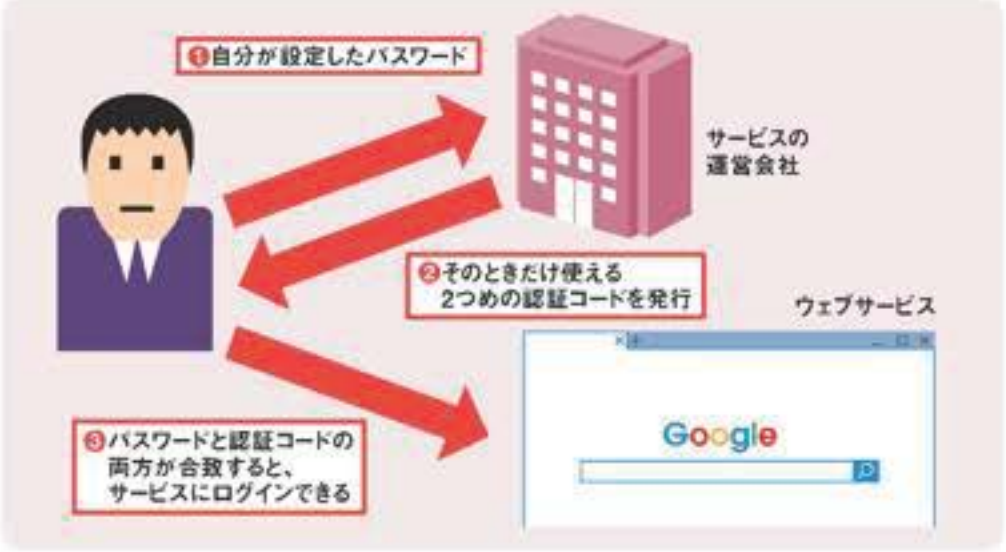

図1 パスワードを使い回していることで、アカウントが乗っ取られる被害が後を絶たない。そんな乗っ取り対策の有効な手段が2段階認証。自分が設定したパスワードと、サービス運営会社が発行した認証コード、この2つが合致しないとログインできなくなる（❶～❸）。認証コードは毎回違うものが通知される

大手サービスの多くは対応済み

サービス名	電話	SMS	メール	アプリ	設定方法
アップル	○	○	–	–	iPhoneの「設定」を開き、「自分のアカウント名」をタップ。「パスワードとセキュリティ」へ進み、「2ファクタ認証」から設定する
アマゾン	○	○	–	○	「アカウントサービス」の「サインインとセキュリティ」を開き、「高度なセキュリティ設定」へ。開いたメニューの「2段階認証」から設定する
インスタグラム	–	○	–	–	スマホアプリの「オプション」を開き、「二段階認証」から設定する
グーグル	○	○	–	○	図3以降を参照
ツイッター	–	○	–	○	「設定とプライバシー」メニューから「アカウント」の「セキュリティ」を開き、「ログイン認証」機能から設定する
ドロップボックス	–	○	–	○	ブラウザーでログイン。「設定」の「セキュリティ」タブを開き、「2段階認証」から設定する
フェイスブック	–	○	–	○	「設定」の「アカウント設定」から「セキュリティとログイン」へ進み、「二段階認証を使用」から設定する
マイクロソフト	○	○	–	○	マイクロソフトの「アカウント」のページを開き、「セキュリティ」から「追加のセキュリティオプション」へ進み、2段階認証を設定
ヤフージャパン	–	–	○	○	「登録情報」から「ログインとセキュリティ」へ進み、「ワンタイムパスワード」から設定する

図2 2段階認証を導入する主なウェブサービス。マイクロソフト、グーグル、アップルをはじめ、フェイスブックやツイッターといったSNSなど、多くのサービスが提供中。認証コードを受け取る手段には、電話、SMSのほか、認証コードを発行する専用のスマホアプリがある

グーグルの2段階認証を有効にする

図3 グーグルで2段階認証を利用するには、ログインした状態で右上の名前をクリックし、現れたメニューから「アカウント」をクリック（❶❷）。次ページで「ログインとセキュリティ」をクリックする（❸）

コードなしで認証するプロンプト方式も

図6 グーグルでは電話やSMS以外に、プロンプト方式という認証方法も用意している。これは、スマホと連携してコードの入力なしにアクセスできるようにする方法だ。このほか、予備のアクセス方法として、認証システムアプリを使ったり、バックアップコードを発行したりする方法がある

図7 プロンプト方式では、まず認証に使うスマホを用意。アンドロイドの場合は、「設定」から利用するグーグルアカウントを登録。iPhoneの場合は「Google」アプリをインストールしておく。続いて図6で「GOOGLE からのメッセージを追加」を実行。設定ウィザードを開始し、認証に使うスマホを一覧から選択する（❶）。すると認証時に、スマホの画面が切り替わるようになる。右の画面で「はい」を選ぶと（❷）、認証コードなしでサービスを利用できる

バックアップコードを発行する

図8 念のためバックアップコードも発行しておこう。図6で「バックアップコード」を実行すると、1回限りで使えるコードが、全部で10個発行される。スマホが手元にない場合などでも、このコードがあれば2段階認証を利用できる。印刷などして手帳や財布などに入れておくと安心だ

図4「Google へのログイン」ページが開いたら、「パスワードとログイン方法」の項目にある「2段階認証プロセス」をクリック（❶）。あとは画面に従って認証コードを受け取る電話番号を入力（❷）。コードの取得方法を選ぶ。ここでは「音声通話」を選択した（❸❹）

図5 指定した電話番号にグーグルから電話がかかってくる（❶）。相手は米国の電話番号だったり、番号非通知なので注意。音声案内の通りにコードを入力し、「次へ」をクリック（❷❸）。「オンにする」をクリックすると2段階認証が有効になる（❹）。次回からは新しい端末でログインする際、通常のパスワードのほかに、毎回、新たな認証コードが電話やSMSで発行され、それを入力しないとサービスを利用できない

7

安易なパスワードの使い回しが被害拡大のもと！

我々は普段、多くのウェブサービスを利用している。その結果、IDやパスワードを覚えきれないからと、同じものや、2～3個のパスワードを使い回す人が多くなった。だが、これが失敗のもと。自分が利用しているサービスの1つが攻撃を受け、IDとパスワードが流出したとしよう。そのサービスでは被害がなかったとしても、別のところで被害に遭う可能性がある。攻撃者は盗み出したIDとパスワードを使って、別のサービスへのログインを試みるからだ。使い回し厳禁といわれる理由がここにある（図1）。

では、どうすれば、パスワードの使い回しをやめられるのか？ すべて記憶するのは困難なため、ソフトに頼ろう。お薦めは「ラストパス」。パソコンではブラウザーの拡張機能、スマホでは専用アプリとして動作するパスワード管理ツールだ。導入すると、覚えるのはマスターパスワードの1つだけで、ほかはソフトまかせにできる。

一連の手続きを見ていこう。まずラストパスの公式サイトから拡張機能を入手して、アカウントを登録する（図2）。次に利用するサービスを開き、現在のIDとパスワードでログイン、同情報をいったんラストパスに追加する（図3）。そして使い回していたパスワードをサービスごとに変更する。その際、ラストパスで安全なパスワードを生成し、新しいパスワードとして割り当てるのがベスト（図4）。最後に変更したパスワードを、図3で登録したログイン情報に上書き保存すれば作業は完了。自分が使う全サービスで、同様の作業をすれば、流出による二次被害を防げる。

流出したIDとパスワードを悪用して不正アクセス

図1 アカウントが乗っ取られる原因として多いのがパスワードの使い回し。どこかのサービスでIDやパスワードが流出すると、攻撃者はそのデータでアクセスできるサービスを手当たり次第に探していく。このためパスワードを使い回していると、ほかのサービスに勝手にログインされ、犯罪などの踏み台などに使われたり、個人情報や金銭を盗まれたりする

パスワード管理ツールを導入する

図2 たくさんのパスワードを頭で覚えるのは大変。そこで利用したいのがパスワード管理ツールだ。お薦めは、パソコンとスマホ、どちらでも使える「ラストパス」。これを使えばラストパス用のマスターパスワードを覚えるだけでよくなり、多くのウェブサービスのパスワードを安全に管理できる。まずは、左の公式サイトでアカウントを登録。ブラウザー上で動作する拡張機能をインストールしよう

図3 ブラウザー（画面はクローム）に拡張機能としてラストパスが組み込まれた。あとは、今まで通りサービスにログイン（❶）。ラストパスがIDとパスワードを検出するので追加する（❷）

安全なパスワードを自動生成

図4 もしパスワードを使い回していた場合は、それぞれのサービスでパスワードの変更手続きをしよう。そのとき役立つのが、ラストパスのメニューにある「安全なパスワードを生成」機能（❶❷）。「パスワードの長さ」（パスワードの文字数）は12以上にし、サービスが対応していれば「高度なオプション」で記号を加えるとなお安全だ

8 複雑でも覚えやすい! 鉄壁パスワード作成法

パスワードを使い回さないことは、セキュリティ対策の基本。しかし、さまざまなサービスで複雑なパスワードを個別に作成・管理するのは面倒だ。前ページで紹介したパスワード管理ソフトを利用する方法もあるが、手間や使い勝手を考えると、どうしても使い回したくなる。

そこでお薦めしたいのが「コアパスワード」を設定する方法。まず、日本語の短いフレーズを考える。ここでは「テレビが好き」とした。これをローマ字に変換し、「terebigasuki」にする。「テレビ」を「TV」ではなく、「terebi」と表記するのもポイント。これだけで、英語圏の人からは推測しにくくなる。この文字列に大文字や記号、数字を混ぜると、安全性が上がる(図1)。「助詞のみを大文字に」「数字は好きな選手の背番号」など、わかりやすいルールを設ければ、複雑なのに覚えやすいコアパスワードが出来上がる。

そして、このコアパスワードにサービスごとの識別子を付けていく。例えば「グーグル」なら「ggl」を識別子にして、「ggl-terebiGAsuki!!06」とするだけでいい(図2)。識別子はコアパスワードの前でも後でも構わない。これで、サービスごとに別々の複雑なパスワードが設定できる。アカウントがたくさんあるときは、識別子のみを紙にメモしておこう(図3)。

コアパスワードを決めておこう

図1 まず、短い日本語のフレーズを決める。ここでは「テレビが好き」とした。ローマ字に変換すると「terebigasuki」となる。助詞に当たる「ga」を大文字の「GA」に変更。さらに末尾に記号を付加する。ここでは「!!」を付けた。さらに末尾に数字を付ければコアパスワードが完成。数字は好きなスポーツ選手の背番号などにすると覚えやすい

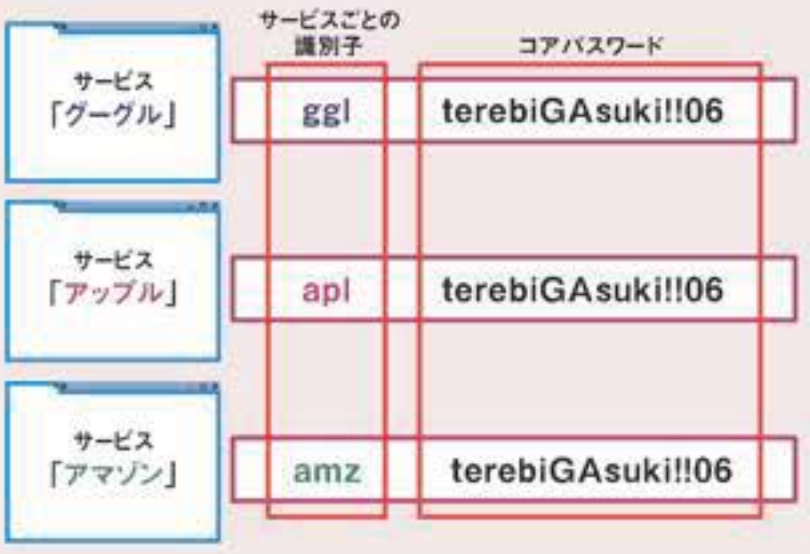

図2 サービスごとの識別子を考える。例えば、「グーグル」なら「ggl」、「アップル」なら「apl」、「アマゾン」なら「amz」という具合だ。これらの識別子を、サービスごとにコアパスワードに付ければ、サービスごとに固有のパスワードが出来上がる。コアパスワードさえ正確に記憶しておけば、管理もラクだ

図3 サービスごとの識別子のみを、紙にメモしておこう。もし、メモを他人に見られてもコアパスワードが知られることはない。今回は覚えやすいように識別子を「ggl」や「apl」などにしているが、ランダムな数字や英文字の組み合わせにすると、さらに強固なパスワードになる

9 秘密の質問には適当な単語1つで答える

アカウントの復旧などに使う「秘密の質問」。これを悪用して、勝手にパスワードをリセットし、不正アクセスをする手口がある。質問の答えは本人しか知らない内容に思えても、出身地やSNSに公開している情報から類推できるケースも多いのだ。そこで、質問とは関係ない単語を1つ用意し、すべての質問にその単語で答えるようにしよう。図1のようにどの質問にも「マンガン電池」と回答すればよい。自分自身も答えを忘れにくくなる。

図1 「初めて覚えた料理は?」「初めて所有した車の名前は?」「初めて遊びにいった海の名前は?」のすべての質問の答えに「マンガン電池」と入力する

●マウスコンピューター
CM01

実売価格:7000円前後

図1 ウィンドウズ10のウィンドウズハローに対応した顔認証カメラ。パソコンとはUSBで接続する

●PQI
マイ ロッキー
My Lockey(DUFPSL)

実売価格:4000円前後(税込み)

図2 厚さはわずか8ミリ。端子を含む全長は20ミリ。ノートパソコンに付けっぱなしにしていても違和感はほとんどない

10 自分のパソコンでも生体認証を使いたい

ウィンドウズ10で利用できる生体認証によるサインイン機能「ウィンドウズハロー」。指紋や顔、虹彩といった生体を鍵とするため、パスワードやPINコードによるサインインよりも破られる危険性が少ない。利便性が高いだけでなく、セキュリティ面でも強固なためウィンドウズ10ユーザーは、ぜひ活用したい。

ところが、生体認証用の指紋センサーや顔認証カメラを搭載しているパソコンは、まだまだ限られている。ウィンドウズハローを使うためだけにパソコンを買い替えるのも現実的ではない。ウィンドウズハロー非対応のパソコンで生体認証によるサインインを使いたいときは、外付けの生体認証センサーを活用するのがお勧めだ。マウスコンピューターの顔認証カメラ「CM01」(図1)やPQIの指紋認証センサー「マイ ロッキー」(図2)といった製品がある。外付けの生体認証センサーは、ほとんどの場合、USBバスパワーで駆動しサイズも小さいので、ノートパソコンでも違和感なく使える。

外付け生体認証センサーをパソコンに接続したら、ウィンドウズの「設定」アプリから「アカウント」→「サインインオプション」と進もう(図3)。生体認証センサー未接続時は「ご利用いただけません」と表示されていたウィンドウズハローの設定項目が有効になる。

ウィンドウズハローを有効にするには

図3 「設定」の「アカウント」をクリック(❶)。左側のメニューにある「サインインオプション」から(❷)、ウィンドウズハローによる生体認証を選ぶことができる

感染レポート ドコモをかたる怪しいメールを検証してみた

ある日、「株式会社NTTドコモから緊急のご連絡」というメールが届いた。内容は「会員登録情報が不正アクセスに遭い、パスワードをリセットしたため、すぐにパスワードを再設定してほしい」というもの(図1)。本物のNTTドコモによるメールのフォーマットを正確に再現しているが、明らかに怪しい。検証のため文中に記載された「パスワード再設定用のURL」を押してみると、スマホからも、パソコンからも開くことができなかった(図2)。同様のメールが届いた事例はSNSでも散見され、IDとパスワードを入力させるフィッシングサイトにつながったケースもあるようだ。万が一こんなメールが届いても絶対に開かないでほしい。

●危険な臭いのするURLにアクセスしてみた

図2 スマホ、パソコンともに開くことはできなかった。スマホでは「サーバーに接続できない」との表示。パソコンのブラウザーでは「個人情報が窃取される可能性があるサイト」として、アクセス自体がブロックされてしまった

図1 パスワードを再設定するように要求し、「http://www.nttdocomo-security.com」という、いかにもそれらしいサイトにアクセスするように誘導している。検証のため、押してみる

11 自宅Wi-Fiの安全を確認する

Wi-Fi機器は、ネットワークの技術内容が難しいこともあって初期設定のまま使うことも多く、リスクがあっても気付きにくい。無償で提供されているツールでチェックしてみるのがお勧めだ（図1）。

ツールを実行すると、同じネットワークに接続している機器を一覧表示し、リスクやアドバイスなどがあれば表示してくれる（図2）。接続機器がすべてわかるので、万一、不正に接続している機器があれば気付ける。対応可能なリスクに対処するだけでも、安全性をアップできるので有意義だ。

オンラインスキャン for Home Network（フォー ホームネットワーク）　無料
●提供：トレンドマイクロ　●対応OS：10／8.1／7
https://www.trendmicro.com/ja_jp/forHome/products/hw_onlinescan.html

図1 上記URLのサイトからインストールファイルをダウンロード。ファイルを実行してインストールする。ウィンドウズに常駐して、新たにWi-Fiに接続した機器のスキャン結果も表示できる

Wi-Fi上の機器の安全性を診断できる

図2 インストールしたソフトを起動して「スキャン」をクリックすると（❶）、Wi-Fiに接続されている機器が一覧で表示される（❷）。リスクがある機器には「！」アイコンが付き、クリックすると詳細を確認できる（❸）

12 Wi-Fiルーターの脆弱性をしっかり塞ぐ

Wi-Fiルーターにも気を配る必要がある。2017年の秋には、通信を暗号化する「WPA2」という規格にセキュリティ上の弱点が見つかり、数多くのルーターが対応を迫られた。悪用されると通信が盗み見られ、個人情報やパスワードが流出するなどの危険がある。

被害を防ぐには「ファームウエア」と呼ばれるルーターの制御ソフトを最新に書き換える。対応状況は各メーカーのホームページに告知されているので確認しよう（図1）。製品型番でネット検索して製品サイトを見て、最新情報を確認してもよい。

脆弱性についての告知と提供ソフトの例

図1 ルーターメーカーが発表する情報に注意しよう。対策済みのファームウエアが公開されたら必ずアップデートする。図はバッファローのサイト

13 カギなしの無料Wi-Fiは要注意

駅やお店などで無料で使える公衆Wi-Fiサービスが増えているが、なかには暗号キーを入力せずにつながるものもある。そうしたオープンWi-Fiは、近くにいる他人に通信内容を傍受される危険を常に意識しながら利用しよう（図1）[注]。

通常は一般的なサイトを見るのにとどめ、パスワードの入力を伴うサイトにアクセスするのは避けたほうが安全だ。もし、オンラインバンキングを利用したり、外部に漏れたら困るメールを送受信したりする場合は、一時的にWi-Fiを切って、スマホのテザリングやモバイルデータ通信を使うといった工夫をするとよい。

オープンWi-Fiの例

図1 iPhoneの「設定」でWi-Fiの一覧を表示させたところ。カギマークがないSSIDは暗号キーなしで誰でも接続でき、通信内容を盗み見られてしまう危険がある

[注]暗号キーがあっても公開されていれば、SSLなどで保護されていないサイトでは技術的には傍受の危険があるので用心したい

14 怪しい広告をブロックする

ウェブサイトを閲覧していると、画面にはさまざまな広告が表示される。なかには危険なサイトへ誘導するような悪質なものもあるので注意したい。怪しい広告をクリックしないように用心することも大事だが、そもそも広告を表示させないという手もある。広告表示をブロックする拡張機能をウェブブラウザーに組み込めば実現できる。

「ユーブロック オリジン」は、エッジやクロームなどに対応する無料の拡張機能（図1）。導入すると、ほとんどの広告が表示されなくなり、画面がスッキリする効果もある（図2）。

広告だけでなく、不適切な画面へのアクセス自体をブロックする機能もある。もし誤認識して、無害な画面なのに開かなくなったり、ポップアップ画面が表示されなくなったりしたら、ブロックの通知画面で「一時的」または「恒久的」にブロックを解除すればよい。拡張機能のメニューから機能全体を一時停止してもよい。

ブロック機能は、各種のサイトを登録したフィルターを基にして実行している。設定画面の「外部フィルター」タブで確認でき、適用するフィルターの選択も可能だ（図3）。国内だけでなく海外サイトの広告にも対応している（図4）。

uBlock Origin
ユーブロック オリジン
無料
●提供：Raymond Hill氏、Nik Rolls氏
●対応ブラウザー：クローム／エッジ／ファイアーフォックス／オペラ／サファリ

図1 エッジの場合はウィンドズ10の「ストア」アプリから、クロームの場合は「Chromeウェブストア」から、それぞれ「uBlock Origin」を検索してインストールする

図3 設定画面の「外部フィルター」タブに表示された日本語対応フィルターの選択リスト。「ウイルス」や「迷惑系」といった項目も用意されている

図4 図2と同様にウェブ画面を表示させた例。海外サイト（上）も含め、広告が見事に消えている

図2 拡張機能をインストールすると、ウェブ画面の広告が表示されなくなる（❶）。メニューを開くと、機能の一時停止などが可能（❷❸）。使用するフィルターを確認するには、設定画面を開く（❹→図3へ）

15 自分に関係する広告をストップする

何かについてネットで検索したら、その分野の商品広告がしつこく表示される――。操作履歴に基づいてユーザーの嗜好に合わせた広告を表示する「行動ターゲティング広告」と呼ぶ仕組みが原因だ。

そんなお節介な機能はいらないという場合は、ネット広告の配信会社に対して「オプトアウト」という操作をすればよい。配信会社が加盟する国内外のグループごとに実行することができる（図1、図2）。実行後は該当の広告スペースには、ユーザーの嗜好とは関係なくランダムな広告が表示されるようになる。

国内サイトのオプトアウトの画面例

図2 DDAI（Data Driven Advertising Initiative）の画面。こちらは説明が日本語なのでわかりやすい。ページの半ばにある「全て選択」→「広告のターゲティング停止（オプトアウト）」で全選択して実行できる（❶❷）

海外サイトのオプトアウトの画面例

図1 「Google Ad」から飛べるDAA（Digital Advertising Alliance）が運営するサイト。右記URLのページを開いてしばらくしたら表示される画面で「CONTINUE」をクリック。この画面になったら「OPT OUT OF ALL」をクリックすると作業が始まり、次に表示される画面で「VIEW UPDATE RESULTS」をクリックすると完了だ。画面下部に表示が出た場合は「キャンセル」でよい

16 フリーソフトの「ひっかけ広告」に注意

気の利いたフリーソフトはとても便利だが、気を付けないと無関係なソフトや姉妹ソフトまでダウンロードして、インストールをしてしまうことがある。フリーソフトのダウンロードサイトでありがちなのが、紛らわしい位置に表示される広告のボタン（図1）。間違えてクリックしないように注意しよう。

インストールするときにも気が抜けない。違うソフトを同時に導入させようとするものがあるからだ。「次へ」で進むインストール画面の途中で、オプションソフトの欄にチェックが入っていることが多い。こうしたチェックを自動で外してくれる無料のソフトもある（図2）。

なかには、ウエブブラウザーに勝手にツールバーを加えたり、検索サイトを変更してしまうものもある。フリーソフトをインストールするときは、注意深く作業を進めよう。

不要なチェックを外すソフトもある

図2 上記URLのサイトでインストールファイルをダウンロード。パソコンにインストールするとソフトがウィンドウズに常駐して、フリーソフトのインストール時に追加ソフトのチェックを自動的に外してくれる

うっかりクリックを誘う広告の例

図1 フリーソフトのダウンロード画面でよくある「ひっかけ広告」。ボタンをよく確かめてクリックしよう

17 検索結果が安全か事前に確認する

有 料のセキュリティ対策ソフトを導入していると、ウェブ検索の結果画面にサイトの安全度を示す評価マークが付く。無償のセキュリティ対策ソフトでも、拡張機能で同様のマークを表示可能だ。

「アヴァスト オンライン セキュリティ」を導入すると（図1）、安全と評価されるサイトには緑色のアイコンが付く。ページを開いた後に詳細画面を開くと、自分の評価を送信でき、行動ターゲティング広告の追跡の有無などもわかる（図2）。

Avast Online Security
アヴァスト オンライン セキュリティ　無料
●提供：Avast Software
●対応ブラウザー：クローム／ファイアーフォックス／オペラ

図1 上記のURLから「Chromeウェブストア」にアクセスし、拡張機能「Avast Online Security」を検索してインストールする

ウェブ検索の結果にアイコンが付く

図2 各ウェブサイトの安全性をチェックして、緑（安全）、グレー（不明）、赤（危険）のアイコンで表示してくれる（❶）。メニューを開くと（❷）、開いている画面の安全性やブロックしている広告などの詳細を確認できる

18 履歴やクッキーを残さずサイト閲覧

欧 州で5月にGDPR（一般データ保護規則）が施行され、クッキーなどユーザーの個人データに関する追跡機能の取り扱いについて同意を求められるケースが増えた。さらに厳しく規制する「eプライバシー規制」の準備も進んでいる。

ユーザー側でも、クッキーなどを一切残さないでサイトを閲覧したいときは、ウェブブラウザーをプライベートモードで開いてアクセスするという方法がある。「エッジ」「クローム」ともメニューから選ぶだけでよい（図1、図2）。プライベートモードなら、サイトの閲覧履歴が残らないため、自分が見たサイトを他人に知られたくない場合にもお薦めだ。

エッジ

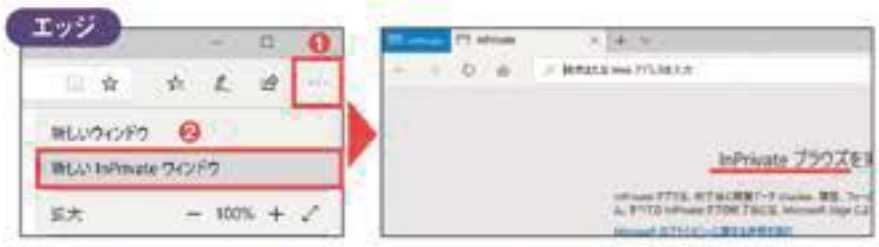

図1 エッジの場合は❶をクリックし、メニューから「新しいInPrivateウィンドウ」を選ぶ（❷）

クローム

図2 クロームの場合は❶をクリックし、メニューから「シークレットウィンドウを開く」を選ぶ（❷）

19 怪しいポップアップはすぐに閉じる

不 正な細工を施されたリンクやサイトを開くと突然、怪しい画面が現れることがある。「システムにエラーが発生した」などとして偽の修復ボタンを押させたり、偽サポートに電話させたりしようとする。マイクロソフトやセキュリティ対策ソフトメーカーの名前やロゴをかたっている場合もあるが、たいがいは悪徳サイトや詐欺サイトと疑ってよい。

そんなときは慌てずにタブやウインドウごと閉じよう（図1、図2）。タスクマネージャーや「Alt」+「F4」キーを使って閉じてもよい。

図1 いつもと異なるウインドウのエラー画面が現れて、ソフトのダウンロードや更新を促されたら、ウインドウ内のボタンは押さずに、すぐにタブやブラウザーを閉じよう

図2 現れたウインドウの「×」ボタンをクリックするのもご法度。本物の「閉じる」ボタンではなく、偽装されたボタンの恐れがある

20 勝手に実行される「マイニング」を防ぐ

ウエブサイトの閲覧中に急にパソコンの動作が遅くなった……。そんなときは、仮想通貨の「マイニング」（採掘）と呼ばれる処理がそのサイトに仕掛けられている可能性がある。閲覧者のパソコンのCPUを勝手に使って処理を開始し、その報酬はツールを仕掛けた者に支払われる仕組みだ。サイトを閉じれば問題ないが、ジャバスクリプトをオフにしても阻止できる（図1）。クロームなら「ノーコイン」という無料の拡張機能でも防止できる（図2）。

拡張機能でマイニングを防ぐ

No Coin
ノーコイン　無料
●提供：Keraf
●対応ブラウザー：クローム／ファイアーフォックス／オペラ

https://chrome.google.com/webstore/

図2 クロームの場合は、上記URLから「Chromeウェブストア」を開き、「No Coin…」を検索して導入する（❶）。マイニングを仕組まれたサイトを開くと、ハンマー形のアイコンに「!」が付く（❷）

Javascriptをオフにする

図1 仮想通貨の不正マイニングが疑われるときは、ジャバスクリプトの実行をオフにするとよい。クロームでは画面右上の「：」から「設定」→「詳細設定」と進み、「コンテンツの設定」→「Javascript」で機能をオフにする（❶～❸）

感染レポート

怪しい無料Wi-Fiにアクセスする人はいるのか？

提供元不明の無料Wi-Fiを、俗に「野良Wi-Fi」と呼ぶ。通信を暗号化しておらず、アクセスする際のパスワードも特にない場合が多い。通信を傍受されるケースもあり、見つけても使わないほうがベター。では、無料で使えるWi-Fiスポットを作ると、アクセスする人はいるのだろうか？ 今回は、アクセスポイント名にパスワードを書き、誰でも接続できる状態にして、実験をした（図1、図2）。

六本木の喫茶店、ファミレス、JR京浜東北線（大宮～有楽町）でそれぞれ1時間開放すると、あるとき一瞬のアクセスがあった（図3）。接続時間は20秒弱で、「試しにつないだがすぐに切った」といったところ。なお、本当に悪意のある無料Wi-Fiは、それとは気付かせない巧妙な名前で待ち伏せしている。注意に越したことはない。

●パスワードを公開して無料Wi-Fiスポットに

図2 続いて、「設定」から「インターネット共有」に進み、「"Wi-Fi"のパスワード」を「12123434」に設定。続いて「インターネット共有」をオンにする。これで、アクセスポイント名にパスワードが書いてある無料Wi-Fiスポットになった

図1 iPhoneの「インターネット共有」（テザリング）機能を使って実験。パスワードなしの設定はできないため、下準備として「設定」から「情報」へと進み、iPhoneの名前を「無料Wi-Fiです。パスワードは12123434。」にする

図3 確認できた限りでは、京浜東北線の浦和駅付近で、一瞬、アクセスポイントが共有状態になった。しかし、時間にして20秒弱で、通信をしているとは思えないほど短い時間だった。面白がってつないだだけだったのかもしれない

21 怪しいショッピングサイトの特徴は？

悪質ショッピングサイトを利用すると、粗悪な模造品が届いたり、商品自体が届かなかったりする。返品や返金が困難なうえに、個人情報を盗み取られてしまうこともある。悪質ショッピングサイトには、いくつか特徴がある（図1）。買い物をする前にサイト内の情報を確認しよう。さらに、サイトのクチコミを調べたり、問い合わせ先を把握することも重要だ。

消費者庁は「悪質な海外ウェブサイト一覧」を公表している。一覧は図2のページからPDFでダウンロードでき、消費者トラブルに関する相談が多数寄せられたサイトなどを400件以上リストアップしている。自分が利用しようとしているサイトが掲載されていないか、しっかり確認しよう。また、悪質サイトかどうかチェックできるサービスもあるので活用するとよい（図3）。

こんなサイトには要注意

- 特定商取引法に基づく表記がない
- 商品の価格が相場に比べて不自然に安い
- サーバーの所在地が海外にある
- 支払い方法が「銀行振り込み」で「前払いのみ」となっている
- 返品・返金が不可となっている
- サイトの公式メールアドレスがフリーメールのアカウントである など

図1 悪質ショッピングサイトの主な特徴をまとめた。特に特定商取引法に基づく表記のないサイトは、その時点で法令違反なので利用するべきではない。ほかの項目に該当する場合も、念のためクチコミなどの評判を調べよう

図2 消費者庁の下記URLのページを開き、「悪質な海外ウェブサイト一覧」からリストのPDFをダウンロードできる。一覧からは悪質サイトの特徴や傾向を知ることもできるので参考にしたい

図3 目的のサイトのURLを貼り付けて「CHECK」ボタンをクリックすると、そのサイトが安全かどうか判定してくれる

22 詐欺商材にだまされないように注意

金もうけの手法やギャンブルの攻略法といった知識を、文書や動画の形で記録してネットで販売する商品を「情報商材」と呼ぶ。なかには効果が薄かったり、実行するのが難しかったりする内容を高額で売りつける、詐欺的な商品も少なくない。

怪しい商材にはありがちな画面パターンがある。改ページのない長大画面に、だらだらと良い話ばかりを並べたものだ（図1）。必ずしも詐欺とは限らないが用心しよう。もし買うなら商材の評判を、検索上位だけでなく下位まで細かく確認しよう。

長文のもうけ話にご用心

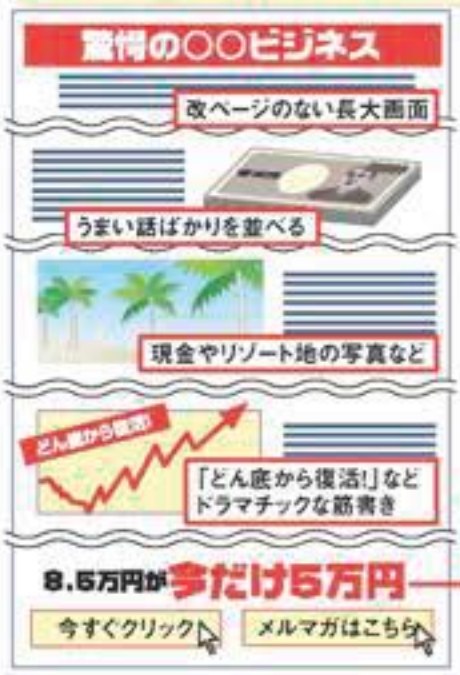

図1 「簡単に稼げる」などと良い話ばかりを書き連ね、最後に「秘密を知りたければクリック」などと購入画面を開かせるパターンが多い。「こんなにもうかりました」といった優雅な生活を装う写真や、「これはすごい!」といったサクラの投書を並べる場合も

23 買う前に出品者・販売者の評価を確認

ネットオークションやフリマアプリで買うなら、出品者の評価を確認するのは不可欠。さらに大手ショッピングサイトのアマゾンでも、「マーケットプレイス」というアマゾン本体以外が販売する商品では、販売者の評価やクチコミをよくチェックしてから購入しよう（図1）。

特に、世間の相場より大幅に安く出品されている商品は要注意。評価やクチコミの中には、販売者自身が購入者のフリをして付けたものもあるので、不自然な点がないかどうかも確認するようにしよう。

アマゾンでも販売元を確認しよう

図1 ヤフオクやメルカリの出品者はもちろん、アマゾン（マーケットプレイス）でも販売者の評価やクチコミを事前に確認しよう。アマゾンの場合は、出品者の名前をクリックすれば評価を確認できる（❶❷）

24 買った商品が家族にバレない方法

インターネット通販で商品を購入するときは、自宅を配送先にしている人がほとんどだろう。梱包を解かなければ中身まではわからないが、伝票の発送元と、箱の大きさ、重さから、受け取った家族は何となく商品を推測できてしまうかもしれない。購入したものを家族に知られたくないときは、店頭受け取りサービスを利用しよう。

例えばアマゾンでは、配送先のコンビニをあらかじめ指定し、店頭の端末から手続きすることで、店頭で受け取れるサービスを用意している。

購入手続きの際の「お届け先住所の選択」画面で「店頭受取先を新しく検索する」を選び、店舗を選択する（図1）。

図1 アマゾンで商品をカートに入れ、「お届け先住所の選択」で、「店頭受取先を新しく検索する」から住所などを指定して検索すると、店頭受け取りができるコンビニが一覧と地図上に表示される。希望のコンビニの「この店舗に送る」をクリック。決済が完了すると指定したコンビニに配達される。受け取り手順は、注文確認メールに記載されているので参照しよう

25 指紋認証を悪用！慌てて閉じたら決済完了!?

iPhoneの指紋認証機能「Touch ID」はロックの解除だけでなく、コンテンツ購入などの決済にも利用でき、非常に便利だ。しかし、Touch IDを悪用した詐欺まがいの課金アプリが発見され、問題になっている。

報告されている例では、SNSの閲覧時に、見慣れない広告がポップアップするという。うっかりタップすると、直ちに決済画面が立ち上がり、認証モードに移行。慌てて閉じようとホームボタンを押すと、指紋認証が働き、決済が完了してしまうというものだ（図1）。6月に問題となったアプリでは毎週5500円、ひと月にして2万2000円もの高額課金が発生したという。

万が一、課金されてしまったら、慌てずに課金登録を解除しよう。iPhoneの「設定」の「iTunes StoreとApp Store」をタップ、自分のアップルIDを選択。続いて、「Apple IDを表示」をタップ。画面をスクロールし、「登録」という項目をタップすると、継続課金サービスが一覧表示されるので、登録を削除したいサービスを選択し、「登録をキャンセルする」をタップする（図2～図5）。ただし、初回分を含め登録が解除されるまでの間の課金は支払わなくてはならない可能性もある[注]。

高額な課金が毎月発生してしまう

図1 6月に問題になった例は、SNSの閲覧時に、見慣れない広告がポップアップするというもの（❶）。うっかりタップすると、決済画面が立ち上がり、指紋認証モードに移行する（❷❸）。慌てて閉じようとホームボタンを押すと（❹）、指紋認証が働きそのまま決済が完了（❺）。課金が発生してしまう（❻）

万が一、課金されてしまったら…

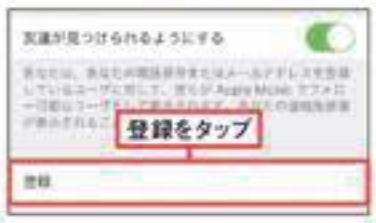

図4 画面をスクロールし、下のほうにある「登録」という項目をタップする

図5 「ご利用中の登録」という項目に、契約中の継続課金サービスが一覧表示されるので、登録を削除したいサービスを選択し、「登録をキャンセルする」をタップする

図3 自分のアップルIDをタップし（❶）、続いて「Apple IDを表示」をタップ（❷）

図2 iPhoneの「設定」から「iTunes StoreとApp Store」をタップする

[注]指紋認証を促す画面で「キャンセル」を選べば、購入を回避できる可能性がある。また、問題があるアプリを購入してしまった場合、90日以内であればアップルに返金を求められる。（アップルのサポート情報：https://support.apple.com/ja-jp/ht204084 ）

26 スマホを紛失した！ 万が一に備えてスマホを設定

スマホを使おうしたら、見当たらない……。さて、どこに置いたのか？ もし紛失していたら一大事だ。連絡手段が断たれるばかりか、大事なデータなどを失う恐れもある。こうしたトラブルに備え、いつでもスマホの現在地をパソコンで調べられるように設定しておこう（図1）。

利用するのは、現在地を検出するGPSなどの機能と、現在地を知らせるスマホの通信機能だ。すぐスマホの紛失に気が付き、まだバッテリーが残っている状況なら、現在地を確認でき、遠隔で画面のロックや、メッセージの表示ができる。ここまでやれば、紛失したスマホが見つかる可能性が高まる。

スマホの紛失に備える機能は、アンドロイドとiPhone、どちらにもある。まずは、利用している端末でGPS機能（位置情報サービス）を有効にしておこう（図2、図3）。

続いてアンドロイドは、グーグル設定の「セキュリティ」にある「端末を探す」機能を有効にする（図4）。スマホでの設定はここまで。スマホが見当たらないときは、パソコンのブラウザーでスマホと同じグーグルアカウントでログインして「端末を探す」ページを開く。すると、地図上にスマホの現在地が表示される（図5）。もし屋外にあるようなら、「端末を保護」機能でロックをかけて拾得者にメッセージを送ろう（図6）。

iPhoneでは、iCloudの「iPhoneを探す」機能を使う。できることは、アンドロイドとほぼ同様。こちらもパソコン上でiPhoneの現在地を確認でき、ロックやメッセージの送付ができる（図7～図9）。

落ち着いてパソコンから操作しよう

図1 スマホを紛失したら落ち着いて現在地を調べよう。スマホの端末を探す機能を使えば、スマホはGPSとデータ通信機能を使って現在地を地図上に示してくれるので、どこで紛失したのかがわかる。遠隔操作でロックしたり、メッセージを表示させたりすることも可能だ

まずはスマホのGPSを有効にする

●アンドロイドの場合

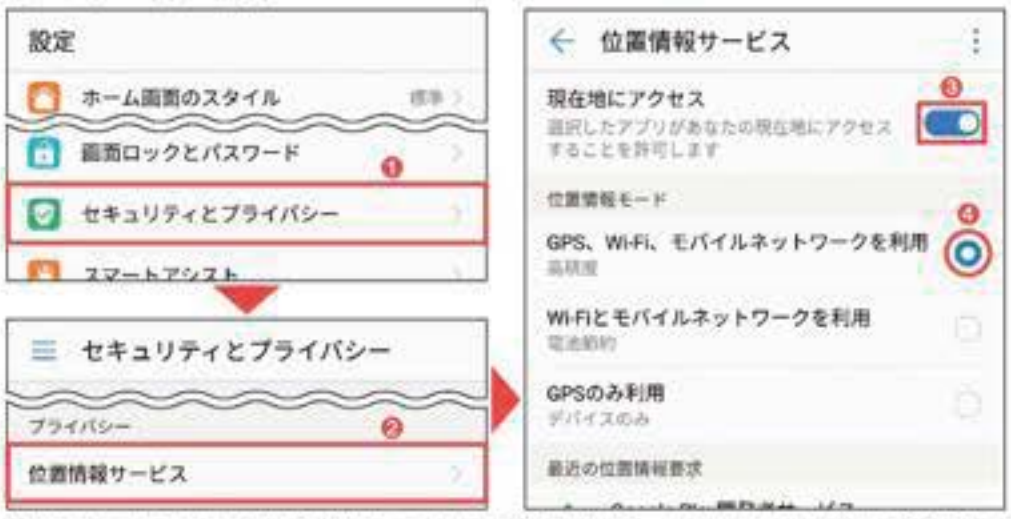

図2 スマホのGPS機能が有効になっていることを確認しよう。アンドロイドの場合は、「設定」から「セキュリティとプライバシー」を開き（❶）、「位置情報サービス」をタップ（❷）。「現在地にアクセス」を有効にし（❸）、「位置情報モード」で「GPS、Wi-Fi…」を選ぶ（❹）

●iPhoneの場合

図3 iPhoneは「設定」から「プライバシー」を開き（❶）、「位置情報サービス」をタップ（❷）。開いた画面で「位置情報サービス」を有効にする（❸）

iPhoneは「iPhoneを探す」を有効に

図7 iPhoneの場合は、「設定」から「アカウントとパスワード」を開き（❶）、アカウント欄にある「iCloud」へ（❷）。開いた画面で「iPhoneを探す」をタップし（❸）、同機能を有効にする（❹）

アンドロイドスマホは「端末を探す」を有効に

図4 続いてスマホを探す機能を有効にする。アンドロイドは、「設定」から「Google」を開いて「セキュリティ」をタップ（❶）。次画面で「端末を探す」へ進み（❷）、同機能を有効にする（❸）

iPhoneを探すには

図8 iPhoneを見つけるには、パソコンのブラウザーで「iCloud」を開き、自身のアップルアカウントでサインイン。メニューにある「iPhoneを探す」をクリックする（右）。開く画面で端末を指定すると、その現在地が示される（下）

図9 外出先に置き忘れたようなら「紛失モード」を実行しよう。図8下のメニューで同モードを実行し、メッセージと連絡が取れる電話番号などを入力する（左）。すると、iPhoneの画面上に拾い主に向けたメッセージと連絡先が表示される（右）

アンドロイドスマホを探すには

図5 アンドロイドスマホを探すには、パソコンのブラウザーで「Google 端末を探す」ページを開けばOK。スマホと同じグーグルアカウントでログインしていると、スマホの現在地が地図上に表示される（上）。「端末を保護」機能を使うと、スマホの画面にメッセージや連絡先の電話番号を表示できる（左）

図6 図5下の「端末を保護」を実行したときのスマホの画面。このようにロック画面に指定したメッセージが表示される。スマホの拾い主が「所有者に発信」というボタンをタップすると、自分宛てに電話がかかる

27 アンドロイドはセキュリティ対策を万全に

スマホにもセキュリティ対策は必要なのか？ 答えはイエスだ。SMSを使った詐欺や、IDやパスワードを盗み取るフィッシング詐欺は、そもそも利用する端末に依存しない。

一方、アプリについてはアンドロイドとiPhoneで状況が違う。アプリの審査が厳しく、入手先も正規ストアだけのiPhoneに対し、アンドロイドは審査が緩く、非正規のストアからでもアプリを入手できてしまう。結果、偽アプリや個人情報を盗み取るようなアプリに出くわす危険がiPhoneに比べて大きい（図1）。新しいアプリを入手する際は、十分に注意しよう。

まず確認すべきは、アプリの評価とダウンロード数。有名なアプリそっくりでも、ダウンロード数が少ないものは偽物の可能性が高い。アプリのアクセス権限にも注目。図2は壁紙アプリなのだが、調べると連絡先や電話機能へのアクセスを求めていた。このようにアプリに関係ない権限を多数要求するものは注意が必要だ。

とはいえ、判断が難しい場合もあるだろう。そんな人は、セキュリティ対策アプリの導入がお勧めだ。「ウイルスバスター モバイル」のように、スマホ版のアプリを提供しているものもある[注]。うとしているアプリや、メッセージアプリで送られてきたリンクの安全性などをチェックできる（図3、図4）。導入すると、インストールしよ

アプリの入手経路と偽物アプリに注意

図1 アンドロイドは、iPhoneと違って非正規のストアがあるため、間違って悪質なアプリを入手する危険がある。また正規ストアでも、人気アプリそっくりの偽アプリが多数配布されている。ちゃんと使えても、裏で情報を盗み取っているかもしれないので用心したほうがよい

必要以上のアクセス権限を主張するアプリは危険

図2 アプリのインストール前には、必ずアプリが使うアクセス権限を確認しよう。「Playストア」のアプリの詳細ページをスクロールし、「このアプリのアクセス権限」をタップすると表示される。左の例は壁紙アプリだが、連絡先や電話など必要以上の権限を求めていることがわかる

セキュリティ対策アプリを導入して安全性をチェック

ウイルスバスター モバイル 無料※
●提供:トレンドマイクロ ●対応OS:アンドロイド／iOS

※30日間の無料体験版終了後は月額300円（税込み）など

図3 セキュリティ対策アプリを使うと、安全性はさらに高まる。左はパソコンでおなじみのウイルスバスターのモバイル版の画面

図4 ウイルスバスターがスマホに常駐していると、インストール前にアプリの安全性を確認でき（左）、危険なウェブサイトへのアクセス、LINEのメッセージ内に含まれる危険なリンクなどもチェックできる（上）

[注]56ページで紹介した「ウイルスバスター クラウド」はウィンドウズとマック、アンドロイド、iPhoneの各OSに対応し、「ウィルスバスター モバイル」の機能も備える。1つのアカウントで最大3台まで使えるため、利用枠の1つをアンドロイドに割り当てれば、追加料金なしでスマホのセキュリティを強化できる

28

ウェブの広告をブロック！ 通信量の節約にも効果的

ウェブページには知りたい情報だけでなく、不要な広告も一緒に表示される。なかには広告が多いページや、操作を邪魔する位置に広告が表示されるページもある。また、広告の内容が不快に思える場合も少なくない。快適にウェブ閲覧したいなら不必要な広告は排除したい（図1）。

またスマホの場合、LTEなどの高速データ通信は毎月利用できる容量が決まっている。広告が多いページだと、それだけ読み込むデータ量も増える。つまり、広告によって無駄に通信量を消費していることになる。

64ページではパソコンで広告をブロックする方法を紹介したが、ここではスマホでの方法を紹介したい。まずはアンドロイド。こちらは広告ブロック機能付きのブラウザーアプリを利用する。定番は「アドブロッカー」こと、「無料の広告ブロック ブラウザ」だ。「クローム」の代わりに起動し、スタートページなどからウェブを検索したり、履歴やお気に入りから目的のページを開いたりする（図2）。ブロックした広告の数やデータ容量もわかるので、効果を実感しやすい。

一方、iPhoneでは、広告の配信元をデータベースとしてまとめたアプリ「アドフィルター」をインストール。「設定」の「Safari」にある「コンテンツブロッカー」で「AdFilter」をオンにすれば、広告が表示されなくなる（図3）。

専用ブラウザーやアプリで広告を非表示に

図1 ウェブ上に表示されるさまざまな広告。数が多いと閲覧の邪魔になって煩わしい。また、無駄に通信量を使うという側面もある。そこで利用したいのが広告をブロックする専用ブラウザーやアプリだ。すべての広告に効果があるわけではないが、ヤフーのトップページでは対策後、図のように大きな広告が消えた

●アンドロイドの場合

無料の広告ブロック ブラウザ 無料
●提供：Adblock - Rocketshield

図2 アンドロイドでは、広告をブロックしてくれるブラウザーアプリを利用する。検索してウェブサイトを閲覧できるなど、使い勝手は通常のブラウザーと変わらない（左）。ブロックした広告の数は、右下のボタンをタップすると確認できる（右）

●iPhoneの場合

AdFilter アドフィルター 無料
●提供：Shinichiro Yamazaki氏

図3 iPhoneの場合は、標準ブラウザーサファリに広告を防ぐ機能を追加できる。まずAppストアから「AdFilter」というアプリをインストール。あとは「設定」の「Safari」を開き、「コンテンツブロッカー」で「AdFilter」を有効にするだけだ（❶❷）。右はAdFilterが対応するブロック先。有名どころは対応済みで、個別に表示するかしないかをオンオフできる（❸）

29

個人情報がダダ漏れ!? SNSの公開範囲を再確認

顔見知りの友人と近況を報告し合う「フェイスブック」。こうしたソーシャルネットワーキングサービス（SNS）には、自分が思っている以上の個人情報が集まっている。住所が特定できそうな写真、生年月日、趣味嗜好、仕事の情報などだ。

どれも抵抗なく公開してしまいがちだが、裏を返せばパスワードの推測に使われる情報や、空き巣に狙われかねない自宅の不在状況などを自ら公表していることになる。そう考えると、SNSに載せる内容は、慎重さが求められる。

特に、気を付けたいのが、投稿した内容を閲覧できる相手だ。通常は「友達」までだが、「友達」の「友達」や、フェイスブックの利用者全員に公開するといった設定もある。もしフェイスブックを利用しているなら、投稿の閲覧範囲を確認しよう。スマホのフェイスブックアプリを使う場合は、図1のように設定メニューの「プライバシー設定」を開くと、重要な設定をまとめて確認できる（図2）。次回からの投稿、自分のプロフィール、フェイスブックのアカウントを連携したアプリなどの中に「友達」以上の公開設定があったら、「自分のみ」や「友達」に修正する。過去の投稿についても、公開範囲の再設定が可能。また、自分のプロフィールページをウェブ検索の対象から外すと、情報の拡散を防げる（図3）。

フェイスブックの公開範囲や内容は慎重に

図1 フェイスブックで注意したいのは、投稿内容の公開範囲。「フェイスブック」アプリでメニューの「設定とプライバシー」をタップし（❶❷）、「アカウント設定」をタップ（❸）。開いたページで「プライバシー設定」をタップする（❹）

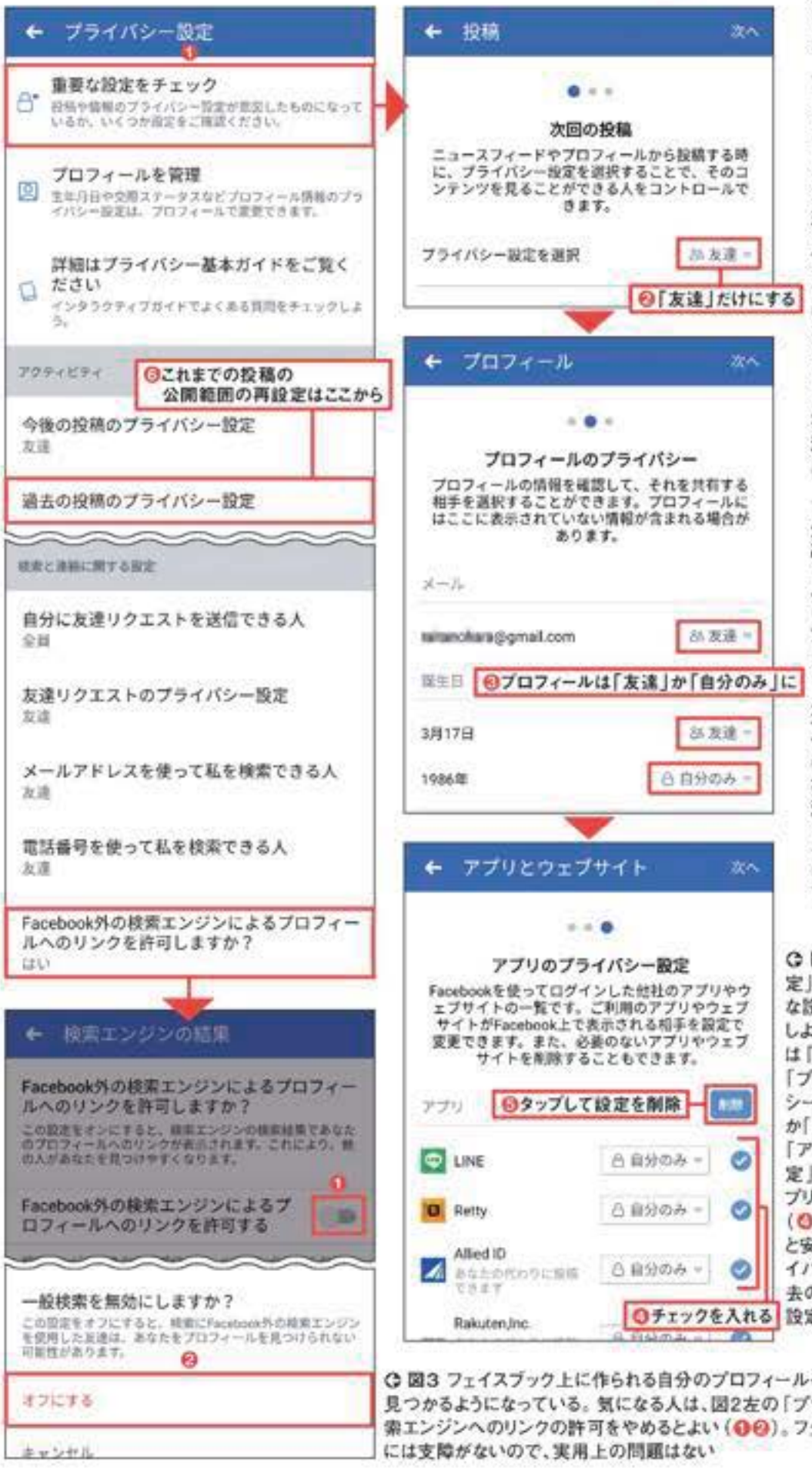

図3 フェイスブック上に作られる自分のプロフィールページは、ウェブ検索で見つかるようになっている。気になる人は、図2左の「プライバシー設定」から検索エンジンへのリンクの許可をやめるとよい（❶❷）。フェイスブック上での検索には支障がないので、実用上の問題はない

図2「プライバシー設定」が開いたら、まず「重要な設定をチェック」をタップしよう（❶）。「次回の投稿」は「友達」だけにし（❷）、「プロフィールのプライバシー」にある項目も「友達」か「自分のみ」にする（❸）。「アプリのプライバシー設定」では、連携しているアプリすべてにチェックを入れ（❹）、設定を削除しておくと安心だ（❺）。また「プライバシー設定」からは、過去の投稿の公開範囲の再設定も可能だ（❻）

30 勧誘や詐欺など不審な電話を撃退する

知らない相手からの電話に出ていいものか？そんなときは「電話帳ナビ」を利用しよう。導入すると、着信時に迷惑電話かどうかを調べてくれる。安全なら水色、危ない前歴がある相手だと黄色や赤色と分類するので、不審な電話に出ることなく、撃退できる（図1、図2）。どんな相手なのか知りたいときは、クチコミ情報を見てみよう（図3）。特定の相手からの電話を着信拒否にも登録できる。

電話帳ナビ 無料
●提供:RIDE AND CONNECT
●対応OS:アンドロイド［注1］

図1 アプリをインストールすると、着信時に相手をチェック。安全もしくは、危険とするデータがない場合ならこのように水色で表示する

図2 勧誘などの前歴がある相手は、このような黄色や赤色で警告。その場合は、電話に出ずに相手が電話を切るのを待とう

クチコミで相手の情報を確認

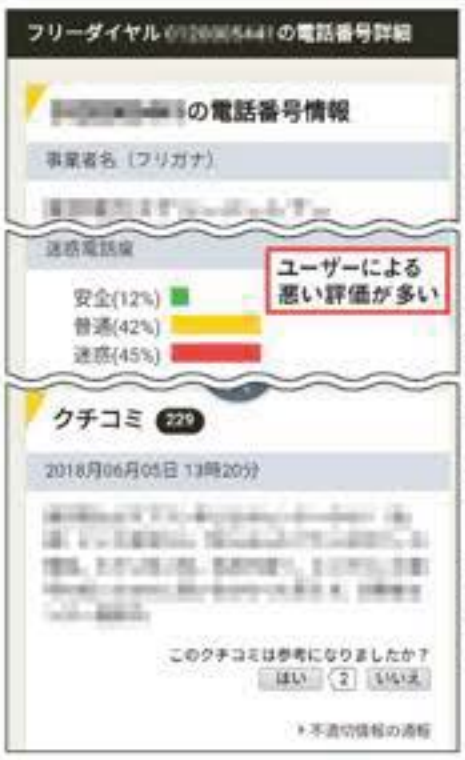

図3 相手が怪しいとされた理由は、利用者による評価やクチコミによる情報を確認できる（上）。危険な場合は、着信拒否相手に設定する（下）［注2］

31 完全無料のセキュリティ対策アプリを導入

アンドロイドの総合的なセキュリティ対策ができるアプリ。「リアルタイムスキャン機能」は、アプリをインストールしたりアップデートしたりした際、不正なものがないか自動でチェックし、通知してくれる（図1）。また、ウェブブラウザーの通信を監視する機能があり、不正請求サイトや個人情報流出サイトなど、悪質なページの閲覧を事前に防いでくれる。こちらの機能は、初期設定では無効のため、アプリの設定でオンにしておこう（図2）。電話帳など個人情報にアクセスしているアプリを一覧で表示してくれる機能もある。

Yahoo! スマホセキュリティ 無料
ヤフー
●提供:Yahoo Japan ●対応OS:アンドロイド

図2「悪質サイト警告機能」はウェブブラウザーの通信を監視し、不正請求サイトなど、悪質サイトの閲覧を事前に防いでくれる

図1 スマホにインストールされたアプリをスキャンし、不正なものがないか自動で調べてくれる。結果は通知パネルに表示される

32 PINコードとパターン、注意すべきことは？

スマホの代表的なロック方法に「パターン」と「PINコード」がある。パターンは他人から予測されにくいが、画面に指の跡が残ってしまうと、ロック解除される危険性が高い（図1）。対策として、画面をこまめに拭き、できるだけ複雑なパターンを設定しよう。

PINコードは、4桁程度で設定すると打ち込む手間も少なく、自身も覚えやすいため、便利だ。しかし、単純なコードは他人から予測される危険があるため、6桁以上のコードを設定しておきたい（図2）。

図1 パターンは、画面に残った指の跡から、他人に予測される危険性がある。日ごろから画面をこまめに拭いて、パターンの跡が残らないように心がけよう

図2 iPhoneはパターンでのロックができないので、6桁以上のPINコードを設定する。「設定」→「Touch IDとパスコード」→「パスコード変更」で変更できる。「パスコードオプション」をタップすると英字入りの複雑なものも設定できる

［注1］iPhoneでは、このアプリが使えない。怪しい電話は出ずに、ウェブ上で電話番号を検索し、安全性を確認しよう
［注2］同様の操作は、電話帳ナビのアプリ上からも実行可能。着信履歴の一覧から相手を選ぶと、検索や着信拒否のメニューが選べる