

スマートフォン・タブレットを 安心して活用するチカラ 養成 HandBook

だまされた

おかしいな

しまった

困った

と思ったら

一人で悩まずに、
最寄りの消費生活相談窓口
お気軽にご相談ください！

消費生活についての相談や苦情をお聞きして、
その解決をお手伝いします。

秘密厳守

相談は
一切無料
です

消費者ホットライン

守ろうよ

みんなを

0570-064-370

ナビに従って郵便番号を知らせると、近くにある相談窓口につながります。

OS・ウイルス
対策ソフトは最新版に
更新していますか？

パスワードロック
していますか？



余計なつぶやきが
人生を変えてしまうかも？

知らぬ間に個人情報
が漏れいしているかも？



▶ はじめに

近年、急速に普及してきたスマートフォン・タブレット。

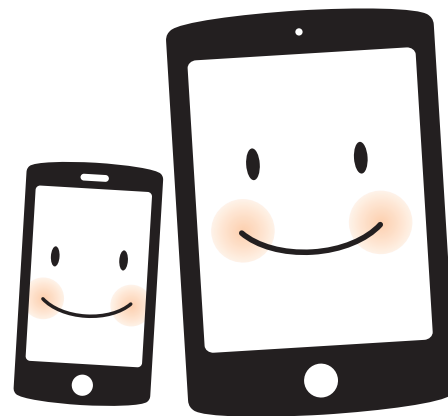
スマートフォンやタブレットを一度使用すると、機能の豊富さや便利さの虜になってしまうことでしょう。使い始めはスムーズに操作できなくても、やがてコツをつかめば便利さが理解でき、もう従来型に戻れなくなります。音楽プレイヤーであったり、カーナビや歩行ナビ、電車の時刻表であったり、駅の構内案内マップに今いる位置までもが表示され、見知らぬ土地でも、問題なく移動できてしまいます。何冊もの本を持ち歩かなくとも、いつでも本が読め、文字の拡大までできてしまいます。一時期のSF映画のような世界が現実の世界で起きているのです。

スマートフォンは大変便利な製品ですが、反面危険性も含まれています。余計なつぶやきが人生を変えてしまうのも事実です。しかし、危険性を恐れてばかりでは、情報化社会で暮らしていくことができません。危険性も、利便性も十分理解して、ブームに左右されないよう自分にふさわしい利用方法を心がけていただくために「スマートフォン・タブレットを安心して活用するチカラ養成ハンドブック」を作成しました。

スマートフォン・タブレット利用の際に、ぜひご一読ください。

兵庫県・大学生協阪神事業連合

スマートフォン・タブレットを 安心して活用するチカラ 養成 HandBook



兵庫県・大学生協阪神事業連合

第1章 スマートフォンとは

1. スマートフォン誕生までの経緯	4
2. スマートフォンと従来型携帯電話の違い	6
3. スマートフォンとタブレットの違い	9
4. スマートフォンの OS の違い	10
5. スマートフォンにできること	12
6. スマートフォンに欠かせないアプリの仕組み	13
7. スマートフォンはなぜ危険なのか	14
8. 携帯電話会社とアプリマーケット	15
9. サイト利用者が行う会員登録の盲点	16
10. 規制の枠外にいる悪意のある会員	17
11. 人気のソーシャルサイト	18
12. 狙われる個人情報	21
13. 割り出される個人の履歴	21
14. 近年減りだしたチラシとDM	22
15. スマートフォンの情報漏えい	22
16. ネットに書き込む個人情報	23
17. アプリから漏れる思わぬ情報	24
18. スマートフォンのウイルス対策	25

第2章 便利に使うスマートフォン

1. スマートフォンには欠かせない Wi-Fi 設定	27
2. 携帯電話から電話帳データを移行する	28
3. バッテリーの消費を抑える	29
4. メール設定でパソコンとリンク	30
5. カメラで撮った写真を自動でウェブ上に保存	31
6. 写真の位置情報設定	31

第3章 安心して使うスマートフォン

1. 紛失から起きるリスク	32
2. スマートフォン紛失から起きる漏れてしまうデータとは	32
3. 必ず行いたいパスワードロック	34
4. スマートフォンの安全対策チェック項目	35

考えてみましょう	37
用語解説	40

執筆者	兵庫県情報セキュリティサポーター	篠原 嘉一
監修	一般社団法人日本スマートフォンセキュリティ協会	

* 兵庫県が実施している「平成24年度 ぐらしの通信講座」のテキストに執筆した内容を大学生向けに一部修正を加えて作成しています。

第1章 スマートフォンとは



①スマートフォン誕生までの経緯

以前から、持ち歩きできる携帯情報端末は各携帯電話会社から販売されていました。基本的にどの機種も、各携帯電話会社の考え方が反映されていました。

そこに、iPhone（アイフォン）がアップル社より発売され、ユーザーにとって使いやすいなどの理由から、爆発的に売上を伸ばすという結果をもたらしました。操作しやすい本体、OS^{*1}（携帯を動かす基本的なソフト）をアップル社が一貫して開発・製造していることが要因の一つです。iPhoneの登場で一気にユーザーの理想に近づいたのです。

アップル社はスマート（携帯自身が利用者に歩み寄りかしこさ）でタッチパネルによる直感的な操作により、仕組みが理解できなくても、指先だけで操作できるように改良した点が、ユーザーを増加することに繋がりました。パソコンの分野でもマウス操作を最初に取り入れ、直感的に使えるようにしたのがアップル社なのです。

このブームのおかげで iPhone の OS（iOS）だけでなく、Android OS 等も市場に受け入れられました。

Android はグーグル社を含めたコミュニティで開発されている OS です。違いは OS を作る会社（グーグル）と、本体を作る会社、回線を提供する会社、アプリケーション（以下 アプリ）を作る会社、それぞれが独自のサービスを提供している点です。（P.10 スマートフォンの OS の違い参照）



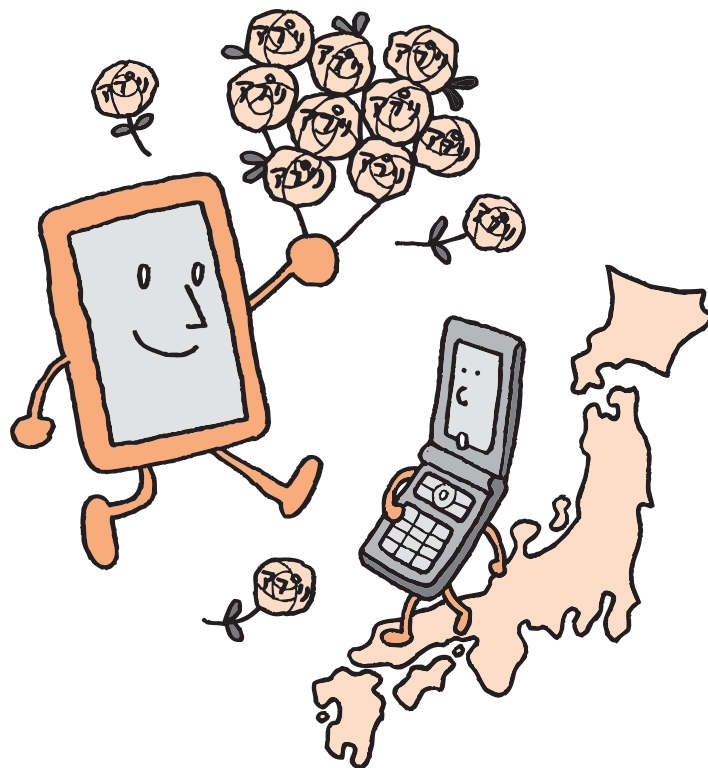
②スマートフォンと従来型携帯電話の違い

従来の携帯電話は、日本固有の特徴を持ち、進化してきました。海外では日本の携帯ほどインターネットへの対応が進んでいません。iモード、EZweb、と言うようなサービスは日本独自のサービスです。独自の進化をとげてきたことが、「ガラパゴスケータイ」*2「ガラケー」と呼ばれる由縁です。各電話会社が競い合い、インターネット機能やお財布ケータイ、カメラにワンセグTV等、次々と便利な機能を搭載しています。これだけ多機能でありながら、今まで情報漏えいなどの危険性やトラブルが表面化してこなかったのは、携帯電話そのものを日本の携帯電話会社が管理してきたからです。携帯電話を一旦購入すると、新たな携帯電話機能をメーカーが開発しても、その機能を搭載した機種に新しく買い換えなければその機能は使えないのです。つまり、購入時の使い方が途中で変わることがないのが従来型の携帯電話です。

かたやスマートフォンは、購入後、アプリをダウンロードする事で自分好みに仕立てられます。年齢、性別、職種、趣味に応じた使い方ができるよう、たくさんのアプリが提供されています。基本OSも随時インターネットを介してバージョンアップ（アップデート）され、常に最新の状態を保ちます。この違いを理解しなければ、ある日突然、昨日までと操作感が違う！と戸惑うことになります。

スマートフォンは携帯電話会社の意向が必ずしも反映されるわけではなく、携帯電話会社が管理できるシステムの範囲は限られています。

この違いが、悪意のある人物につけ込まれる隙を与え、責任の所在をあいまいにしています。



② スマートフォンと従来の携帯電話の違い

	スマートフォン	従来の携帯電話
機 能	● 通話以外の機能が充実。数多くのアプリを自由に追加でき、パソコンのように多機能化が可能。アプリは有料・無料ともある。	● 通話が最優先。他の機能はあらかじめ搭載されたものに限られる場合が多く、拡張性が低い。
インターネット	● パソコン向けサイトの閲覧が可能。従来の携帯電話専用サイトは閲覧できない。パソコン用メールや携帯電話専用メール等の複数のメールを利用可能な機種も多い。 ● 従来の携帯電話の通信(携帯電話回線^{*3})だけでなく、高速な無線LAN通信(Wi-Fi:ワイファイ^{*4})も利用可能なため、サイトの素早い表示やアプリ等の大容量データのダウンロードも可能。	● 携帯電話専用サイトと携帯電話専用メールの利用が中心。 ● 高速な無線LAN通信(Wi-Fi)が利用可能な機種は少ない。
セキュリティ	● アプリ追加後のセキュリティ状態は携帯電話会社でも把握が困難なため、パソコンと同様に、自分でセキュリティアプリの利用等の対策をとる必要がある。 ● 撮影した写真にGPS^{*5}による位置情報を埋め込む機能を持つものが多く、ブログなどでその写真を公開すると自宅等の撮影場所が特定される。プライバシー保護のためなら、GPSによる位置情報を埋め込まない設定にする必要がある。	● 携帯電話会社が定期的なアップデートなどでセキュリティ強化に対応する。自分でセキュリティアプリを準備する必要はない。
そ の 他	● タッチパネルを搭載するものがほとんどで、操作に慣れが必要。 ● 画面が大きく、Wi-FiやGPSなど多様な通信機能を持ち、自動通信機能もあるといった特徴をもつため、電池のもちが悪い。	● 各機能を割り当てたボタンがあるものが多く、ボタンの配置を覚えたら画面をあまり確認することなく素早い操作が可能。 ● 電池のちはスマートフォンより良い。

③ スマートフォンとタブレットの違い

スマートフォンと同様の機能を持ち、画面も数倍大きなモデルをタブレット型と呼んでいます。このタブレット型とスマートフォンの大きな違いは、携帯電話回線を使って通話ができるか否かです。つまり電話をするなら今までの携帯電話を使い、ネットやソフトウェアを使って作業をする時はタブレット型を使うというように使い分けると、お互いの利点が活かれます。

タブレット型には、無線回線(Wi-Fi)^{*4}のみのモデルと、携帯電話回線でもネットが使える携帯電話回線+Wi-Fiモデルがあります。後者はパケット通信料が発生しますので、パケット定額の契約が必要になります。自宅や出先にWi-Fi環境があるのであれば、費用のかからないタイプを選択すれば、料金を気にすることもなく使用できます。



④スマートフォンのOSの違い

スマートフォンを選ぶにあたって、ご自身の契約されている携帯電話会社での利用を選択される方が多いのではないのでしょうか。その電話会社の取り扱うスマートフォン用 OS が何かを知ってから、機種選択に移ります。

電話会社	スマートフォン用 OS	
	Android	iOS
☐ ドコモ＝	○	✕
☐ au ＝	○	○
☐ ソフトバンク＝	○	○

(注意：平成25年春現在で、スマートフォンOSは数種類ありますが、一般的な利用者に限定してiPhoneのOSとAndroidのOSの2種類に限定して表記しています。)

■OSの違いについて

➡ iPhoneのOSはアップル社の管理下にあります。

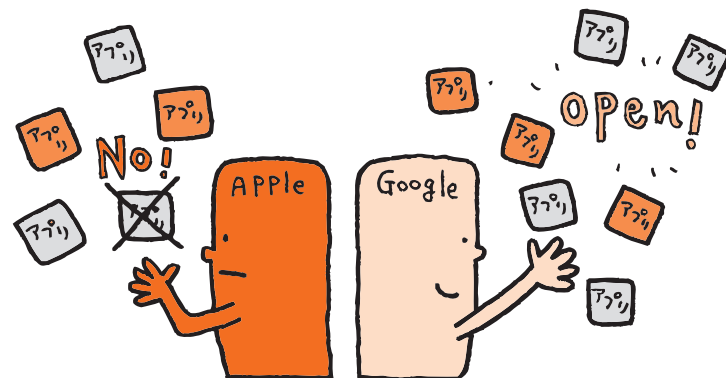
アプリを制作する場合も、登録して審査を受けます。アプリができ上がれば、アップル社が審査を行います。悪意がなく安全と判断されれば、アップル公式ストアにてダウンロード販売されます。無料アプリの制作に関しても同様の手順で行われます。

➡ AndroidのOSは、グーグル社を含めたコミュニティが推進しています。

Google 社は開かれたネットを提唱していますので、アプリの制作

に関してもオープンです。電話機製造会社は、Android OS を使用し、自社の製品向けに修正しています。電話機本体はどの会社でも参入できるのです。

アプリに関しても自由に開発できます。アプリ製作者はフリーマーケットのように自由に販売ができます。審査が無い反面、利用開始から数カ月間の利用者のコメントを見て問題ありと判断されれば、販売・提供されなくなります。(P.13 スマートフォンに欠かせないアプリの仕組み参照) この OS やアプリの管理方法の違いが、現時点では個人情報収集を目的としたアプリの発見が遅れる、ひとつの要因です。



⑤ スマートフォンにできること

従来型の携帯電話と違い、スマートフォンには無数のアプリがあり、日々増え続けています。世界中に製作者がいますので、多種多様なアプリが存在します。なにか不便を感じたら、必ずと言っていいほど、対応するアプリが見つかります。

カメラでの画像の編集や、位置情報を利用したお店案内、絵画、書道、囲碁など、ありとあらゆるアプリが揃っていますが、中でも情報を共有する機能が含まれるアプリが多いのが特徴です。多くのアプリは無料もしくは有料でも数百円程度で購入できます。毎月課金されていた従来の携帯サイトと比べ、一度支払えば長期間利用できるものが大半ですので、いくつものアプリを取り込み、自分好みにアレンジすることができるのです。

ご自身の使い方や知識を広げるために、アプリの提供サイト内を探してみてください。



⑥ スマートフォンに欠かせないアプリの仕組み

スマートフォンの機能が追加できる便利なアプリですが、本体にダウンロードする際に、利用規約が表示されます。利用規約に同意した方がみがアプリを利用しているということになりますから、十分慎重に利用規約を確認してからダウンロードしてください。ただし、ときどき利用規約が表示されないアプリもあります。

無料でアプリが使えるのには、訳があります。例えば無料で提供する代わりにアプリの画面の中に広告を表示して、収入を上げている事例が多く見受けられます。また、最初から悪意のあるアプリであれば、同意事項に「携帯電話内の情報をコピーします」という内容を記載せず、堂々と電話帳の記録や通話履歴、位置情報を収集するアプリがあります。

いずれも悪意のあるアプリは、スマートフォン購入時の標準搭載アプリ以外ですから、自分好みのアプリをダウンロードする際は、アプリ購入時に記載されている利用者の評価欄を読み、十分に気をつけてダウンロードしてください。



⑦スマートフォンはなぜ危険なのか

スマートフォンは従来の携帯電話と比べて危険だと言われています。実際に多くの被害が起きているのです。

これは、スマートフォンが

「多機能であること」「携帯電話会社の管理が限定的なこと」

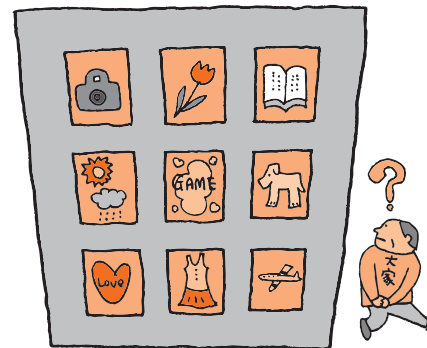
「アプリを追加できること」「常時インターネットに繋がること」

に起因しています。電話帳の個人情報が抜かれ、GPS^{*5}による位置情報が抜かれ、検索結果を見られることにより趣味趣向が、悪意のある者に分かってしまうのです。スマートフォンの設定を意識して扱わなければ、思わぬところでデータ（個人情報）が流出してしまいます。従来の携帯電話は携帯電話会社が全体のシステムを管理していましたが、スマートフォンでは利用者ごとにアプリの種類が違ってもあり、携帯電話会社ではほとんど管理できないのが実情です。スマートフォンで起きるであろうトラブルがどのようなものなのか想定が難しい状況なのです。



⑧携帯電話会社とアプリマーケット

スマートフォンは、たくさんのアプリを使用できる仕組みになっていますが、このアプリに関しては携帯電話会社の管理下にありません。iPhoneであれば、アップル社が管理している「App Store」というマーケットでアプリが提供され、Androidはグーグル社の管理している「Google play」等で提供されます。まずは、そのアプリマーケットが信頼できるかどうかには注意が必要です。従来の携帯電話であれば、サイト上の利用も、携帯電話会社の管理下でした。例えばiモードやezwebと呼ばれているサービスは、携帯電話会社の管理しているサービスです。スマートフォンの場合、携帯電話会社はインターネットに接続するための回線（パケット通信回線）を提供するのであって、アプリそのものは管理していません。いわば場所を提供するビルの大家さんのようなもので、テナントのお店の内容まで口を出さないのです。



⑨サイト利用者が行う会員登録の盲点

アプリの中には、会員登録をして利用するタイプのももあります。ゲームサイトなどは、無料で使用できる代わりに会員登録が必要になります。この会員登録は、利用者のスマートフォンの識別番号をサイト運営会社に登録させることもあります。会員登録により、会員の趣味趣向にあわせた広告を会員ごとに配信することができるのです。(たとえば、無料のゲームサイト運営会社は、ゲームサイトを無償で提供する代わりに、広告を配信することにより広告収入を得ています。)しかし、ゲームサイト運営会社は登録内容を必ずしもチェックするわけではないので、登録した内容が正しいとは限りません。偽った内容で会員登録をすることも可能なのです。

偽った内容で登録をすることで、どのようなことが問題になるのでしょうか。例えば今、女子中学生のAさん、40歳男性のBの2人がソーシャルゲーム※6に参加しようとしています。Bはゲームサイトに登録する際、女子中学生であると偽って登録します。Aさんは、女子中学生を名乗るBとゲームに参加することになりましたが、Aさんには、女子中学生になりましたBが成人男性ということは分かりません。ゲームを進めていく中で、会話が弾み、2人は仲良くなって、様々な個人情報(メールアドレス、名前・住所、写真など)を交換しました。その結果Aさんの多くの情報を得たBが、学校から帰る途中のAさんの前に現れ…ということも起こってしまいます。

現実の世界では、成人男性が未成年に近づき個人情報を集めることは難しいですが、この事例のようにインターネット上では、成人男性が女子中学生になりすまし、情報を集めることができってしまうのです。

⑩規制の枠外にいる悪意のある会員

年齢を偽った会員は未成年になりすまし、相手の情報を集めています。トラブルが起きるとサイト運営会社を規制するようにとの声が出ますが、サイト運営会社の問題ではなく、利用している会員(なんらかの悪意を持ったゲームの利用者)の問題ということがあります。ここに法律でサイト運営会社を規制しても、会員の行動まで規制できない難しさがあります。



事例 1

★悪意のある会員に呼び出された 《女子高生の場合》

彼女はスマートフォンを持つ前から、ポータブルゲーム機で知合った東京に住む同い年の女の子と、チャットをして楽しんでいました。中学生になってから携帯、スマートフォンと機種を変えながら、東京の友だちと写真の交換や、メッセージのやり取りを楽しんでいたようです。

高校生になり、進学校に進んだ彼女に、「恥ずかしい写真をバラまくぞ!」と突然脅迫のメッセージが届きました。添付されていた写真は東京の友達に送ったものでした。また脅迫の内容は、その脅迫者が彼女を全て知っているかのような内容でした。この脅迫者はどのようにして彼女の情報を入手したのでしょうか。脅迫者はメールのやりとりをしていた友人を装った人物から、写真や個人情報を入手したのです。東京の友達(サイト上の友達)は情報収集を目的とした人物でした。

会ったことのないサイト上の友達は、本当の友達ではありません。自分のことを全て話したり、写真を交換したりすることは、このように大変危険なことになってしまいます。自分の身を守るためにも、最低限のルールは自分で決めておきましょう。



アクセス制限をかけていないアカウントは、誰も見ていないと思っつつやういっていても、全てのユーザーに配信されているのと同じです。

SNSの多くは顔の見えない相手との会話なのです。「誰も見ていない」「ただの独り言」のつもりが、不特定多数への配信となると、*個人情報の漏えい*名誉毀損*プライバシーの侵害*守秘義務違反などの問題となり、停学・退学・内定の取り消し・解雇・法的手段による処罰という処分を受ける場合があります。

①人気のソーシャルサイト

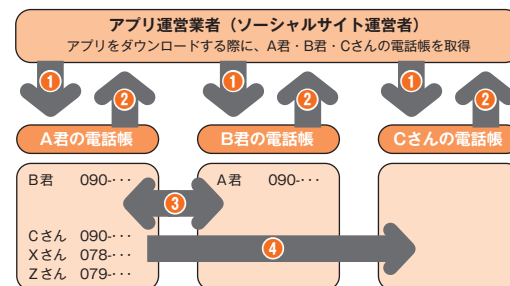
スマートフォンが爆発的に普及した理由のひとつに、ソーシャルサイト（SNS）の存在が大きく影響しています。ソーシャルサイトとは、利用者間を結びつけ、お互いに情報共有しようというものです。例えば自分の同級生や遠くに住む友達などの情報が、いつでも見ることができれば楽しくて便利なサービスです。多くの人達は、このサービスを提供するアプリをダウンロードして利用しています。ではなぜ、この同級生や友達を見つけ出せるのでしょうか。それは、アプリの会員を増やす仕組みにあります。一部のアプリでは、アプリをダウンロードする時点で規約に書いてあるのですが、自分のスマートフォンに登録している電話帳のデータをアプリ運営業者に自動的に送信し、電話帳繋がりで友達、知り合いを結びつける仕組みがあります。相手も同じアプリを持っていると繋がり、承諾すればやり取りが可能となります。自分の電話帳にとどまらず、繋がった相手の電話帳のデータも参照しますから、友達の友達として、電話番号を知らない同級生とも連絡ができるようになり、大学生などは飛びついて利用しています。

しかし、繋がりを持つためには電話帳のデータをアプリ運営会社に提供する必要があり、交友関係が見えてしまうことへの不安を感じる人もいます。自分のスマートフォンから電話帳の記録を削除しても、アプリ運営会社に提供した電話帳の記録は削除されません。別れた恋人の名前をアプリ上から削除できないことが、今後の人間関係にも影響することを理解していないと、個人情報の漏えいというだけでは済まず、将来の生活にまで影響を及ぼし、トラブルにもつながる可能性があります。ソーシャルサイトの設定事項を理解して使用し、必要のないことまで書かない意識が必要です。

友達の友達～として多くのネットワークを築くソーシャルサイトに、何気なくつぶやいたり写真を投稿したりすると、思わぬ人物と繋がりがトラブルになることがあります。

企業人が仕事のことをつぶやくのは、会社に良くも悪くも影響を与えます。友達だけに公開した情報だと思っつつやういっていても、友達の友達の友達をたどることにより、すべての会員は繋がるのです。書き込んだ情報は永遠に消えないのだと意識していないと、大きな落とし穴に落ちることになってしまいます。

●人気のソーシャルサイト



※ソーシャルサイトアプリをダウンロード(①)、電話帳をアプリ提供者に渡すことが条件になります(②)。

A君、B君ともにソーシャルサイトのアプリをつかっている状態で、A君の電話帳にはB君の電話番号が、B君の電話帳にはA君の電話番号が登録されていると「友達かも」というメッセージが自動的にそれぞれのスマートフォンに届きます(③)。

Cさんの電話帳にはA君の電話番号が登録されていませんが、A君の電話帳にはCさんの電話番号が登録されています。この場合、Cさんに「(A君は)知り合いかも」というメッセージが自動的に届きます(④)。

例えば、社会人になったA君とCさんが高校時代は仲よかったクラスメイトであり、ソーシャルサイトを通じて再び親交を深める機会となるのであれば便利なツールといえるでしょう。

しかし、例えばA君とCさんがかつては良好な関係にあったものの、その後関わりを絶ちたい関係にあったとしても、つながってしまう危険性ははらんでいます。

「友達しか見ていないはず」はありません。

最近のSNSはスマートフォンの電話帳とリンクしていますので、想定外の人や、友達の人、就活中の企業担当者など、思いもよらぬ人の目にも触れています。

一度投稿した書き込みや投稿画像は削除が出来ません。削除したつもりでも、それは自分の目に触れないようになっただけで、SNS等には記録として保存されている可能性があります。そのデータは、いつ再現されるかわからない不安があるのです。反社会的な発言や悪意のある書き込みなどは、確実に今後の生活に影響を及ぼすのです。



事例2

★過去の書き込みは消えない 〈大学3回生の男性の場合〉

スマートフォンがまだ発売されていない中学生の頃に携帯電話を手にした彼は、ネットにブログを開設しました。パソコンからも更新していましたが、主に携帯電話で更新をしていました。ブログの他にも掲示板にコメントを書いたり、無料ゲームサイトでコメントを書いたりもしていました。すべてが匿名を前提としたサイトでの利用ですから、身元が分からないとの安心感もあり、勉強で疲れたストレスもネットの中にぶちまけることで解消していました。大学生になり、スマートフォンに機種交換し、電話番号とメールアドレスはそのままに使用を続けていました。スマートフォンの楽しみのひとつであるソーシャルサイトでたくさんの同級生と交流しようと、ダウンロードし利用を開始。電話機に登録していた電話帳に基づき、同じアプリを利用している友達を簡単に見つけることができ、楽しく高校時代の友達ともコメントの交換をしていました。そんな中、就職活動が本格的になり、携帯サイトでも応募するなどし、多くの企業にアタックしたところ、なぜか二次面接にたどり着きません。ある企業で耳にした情報では、企業もサイトで応募者の過去を確認しているらしい…そうです。彼には思い当たることが…

従来の携帯電話の頃は匿名での利用が多く、個人を特定できないモノが多くありました。しかし、スマートフォンの普及と同時にソーシャルサイトの一部で実名サイトが人気を得ました。この実名サイトに登録すると、携帯の電話番号と結びつけ端末の利用者を特定します。つまり、この端末の利用者は実名サイトの〇〇さんだと分かります。データは紐付けされますから、芋づる式に過去の書き込みが誰だか分かってしまいます。

匿名のつもりで、ネットに誹謗中傷や過激な書き込み、良くない行動の記録を書いてしまうと、誰が書いたかが分かってしまうのです。ネットで不適切な発言を書き込むなどすると、就職にも影響してしまうことになってしまうかもしれません。



⑫狙われる個人情報

スマートフォンは携帯電話会社の管理が難しくなる仕組みですから、個人情報も悪意のあるアプリや悪意のある会員によって、のぞき見されることがあります。複数のアプリが入っているスマートフォンですから、利用者本人も、どのアプリをインストールしているか管理が難しいため、個人情報が持ち出されても気づきにくいのです。便利なスマートフォンですが、GPSの位置情報や電話帳への詳細な登録などは情報漏えいにも繋がります。漏えいした個人情報は名簿屋を通じて売買されていますので、あまり詳細な情報はスマートフォン内に記載しないことです。

⑬割り出される個人の履歴

スマートフォンの端末情報がアクセスしたサイト（インターネット閲覧履歴）に残ることがあります。これはサイト側が利用者を把握し、マーケティングに利用しているからです。どのスマートフォンが何回サイトを見に来たかを確認しています。この時集められる端末情報から「何に興味がある利用者か」が見えてきます。端末情報をたどれば、個人情報へも繋がりが、履歴から利用者の趣味趣向が分かってしまうのです。



⑭近年減りだしたチラシとDM

一時期に比べ、家庭へのチラシやダイレクトメールが減ってきたように思いませんか。景気のせいだけではなく、マーケティングの手法が変わってきたためです。必要のない人にまでチラシをばらまかなくなったのです。インターネットサイトへのアクセス履歴が、世間の動向を見る大きな資料となっています。サイト運営会社は沢山の個人情報を収集していますから、サイト運営会社から情報を買えば、チラシを作成せずに、ピンポイントで必要としている方にダイレクトメールが届けられます。ネット上の広告も増えました（ネットに表示される広告は閲覧者によって異なります）。つまり、ネット上も自宅に届くダイレクトメールも、どちらも自分の検索履歴が反映されているのです。

⑮スマートフォンの情報漏えい

スマートフォンの普及が進むにつれて、必ず情報漏えいは問題となるでしょう。不正なアプリやウイルスの攻撃などにより、情報が漏れることもあります。それ以上に利用者の情報リテラシー^{*7}の稚拙さが原因で情報の漏えいが増えていくことでしょう。つぶやきや日記（ブログ）を簡単にネット上に書き込めることが人気なのですから、何気なくつぶやく独り言は、多くの人の目にとまります。芸能人を見つけてつぶやくと、その場に多くの人が押し寄せます。社内のことをつぶやくと企業の内部情報の漏えいに繋るかもしれません。会社のPRのつもりで書いていた社長ブログが、いつの間にか会社の情報を漏らしていたと気づいた

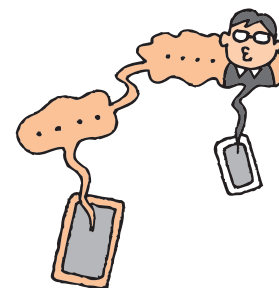
頃には、手遅れなのです。スマートフォン端末には、個人情報が満載です。そのスマートフォンが接続したブログサイトや、会員制交流サイト（SNS）には会員登録情報やプロフィールが多く存在しています。この部分を紐付けすれば、本人だけではなく、家族や仕事仲間、取引先、社内情報などの情報が芋づる式に掘り起こされます。

これまでパソコンで続けてきたブログでさえ、スマートフォンで更新すると見えてしまう情報が増えるのです。

⑯ネットに書き込む個人情報

最近言われるネット上の個人情報とは、氏名、所属、住所、メールアドレス、写真だけでなく、日記やブログ、チャットでの会話、電話帳からの友人関係、行動記録なども含まれます。これらの情報をネット上に書き込むことは、相当覚悟して書き込まなければ、場合によっては大きなトラブルを引き起こすことになります。

今までスマートフォンを持っていない頃に書いてきた、ニックネーム（匿名）でのブログも、スマートフォンを持ち、書き込むことでブログを更新した人物が特定できます。実名サイトに会員登録して、そちらでもつぶやいていると、同じ人物だと分かっています。情報は紐づくのです。今まで書いてきた匿名の日記が誰だったか、発覚してしまうのです。





事例3

★毎日のつぶやきから漏れた 《公務員の場合》

彼はプロフィール欄に役職名と所属する市の名前を記載していました。実名サイトですから、誰でもそのように書くものですが、写真や所属部署名を書くということは、それだけ発言には気を付けなければなりません。彼は毎日のランチの写真をアップして、暇つぶしを兼ねて楽しんでいました。毎日数回の更新は習慣となり、何気なくつぶやくことも増えてきた頃、夜の長い会議に出席した際、「まだ終わらない…」とテーブルの上にある会議資料の画像を添えてアップしました。同僚からは、「お疲れ様」のコメントが届いていましたが、この写真は後日大問題になりました。写真から、市の事業が漏れ、書類に書かれている参加者が分かってしまいました。公務員の守秘義務違反に問われることになりました。ランチのつぶやきが、いつの間にか守秘義務違反になるなんて、おそらく想像しなかったのでしょう。思わぬ画像で人生が変わってしまいます。



⑦アプリから漏れる思わぬ情報

つぶやきなどの SNS の代表的なアプリを多くの方がダウンロードしています。しかし、そのアプリを便利に使えるようにするアプリも同時にダウンロードしている方がいます。この代表的なアプリの名前を盛り込んだ便利に使えるアプリは、非公式のものが多く存在します。公式アプリで非公開に設定していても、非公式アプリをインストールしていれば、シンクロして投稿されるため、非公式アプリ間では公開情報となることもあります。

人気のアプリが許可しているアプリかどうかを見極めてダウンロードしなければ、非公開の情報が出回ることになります。



事例4

★公式、非公式を意識せず使っていた 《会社員の場合》

会社員の彼は、ソーシャルサイトで日々の行動をつぶやいていました。ある日、いつも使っているアプリの機能をアップしたタイプのアプリが出たことをメールで知り、早速ダウンロードして使ってみようとした。つぶやくことのみに特化したアプリで、今まで以上に簡単に書き込めるとあって、そちらを使ってつぶやきをしました。しかし、動きが不安定だったため、次第に元のアプリから書き込むように戻っていたそうです。いつものように社内の同僚に向けたつぶやきをしていたところ、取引先からクレームが来しました。クレームの内容は、彼がつぶやいた内容が契約情報だったため、社内の企画が漏れたとのクレームでした。契約は中止となり、大きな損害が出ました。彼が後からインストールしたアプリは、有名なアプリの名前をもじった非公式サイトでした。その非公式サイトの設定が、社内の同僚宛につぶやいたことを、公開情報として広めてしまっていたのです。設定のミスですが、同じ種類のアプリはリンクしています。片方でつぶやくと、片方のアプリにもデータは書かれます。設定をよく確認しなければ、極秘情報も漏れるということになってしまいます。



⑧スマートフォンのウイルス対策

スマートフォンでもウイルス対策ソフトは必要です。アップル社の製品に関しては、前述のとおり、アプリの審査が行われているためウイルス対策ソフトの必要性はありませんが、Android スマートフォンに関しては必ずウイルス対策は必要です。基本的にウイルス対策ソフトは、侵入を防ぐ為のソフトウェアですので、一度感染して、持ち出されたデー

第2章 便利に使うスマートフォン

タを収集する機能はありません。防波堤のようなもので、崩れると終わりののです。

Android の場合は事前にウイルス対策ソフトをインストールしておきましょう。携帯電話会社ごとにウイルス対策サービスもありますし、社外品のウイルス対策ソフトも出ています。

随時自動更新で最新の状態に更新されますので、新種のウイルスにも対応できます。



SNSでの安易な書き込みトラブルが急増！
書き込みが及ぼす影響を考えておかねば、
将来の生活にも大きな影響が！
損害賠償請求などにも発展…

SNSは、以下を十分に意識した上でご利用ください。

- ① 他者の個人情報を許可なく投稿しない！
- ② 他者を誹謗中傷する投稿をしない！
- ③ 職務上知り得た情報を投稿しない！
- ④ モラルに反する投稿をしない！

①スマートフォンには欠かせないWi-Fi設定

スマートフォンや携帯電話は携帯電話回線と呼ばれる回線で通信を行います。携帯電話の普及で回線が混み合うようになり、基地局や回線数の増設が行われています。通話だけでなく、インターネットの利用も携帯電話回線を使用していますから、データ量の多いスマートフォンの普及は回線の帯域不足に直結します。

スマートフォンは、インターネットを携帯電話回線以外に Wi-Fi で接続することができます（一部の従来型携帯電話でもできます）。Wi-Fi は、携帯電話回線に比べ高速で、データの受け渡しに適しています。特に動画などの閲覧には Wi-Fi 回線が適しています。Wi-Fi を使用してネットを使うと携帯電話回線にも余裕ができ、回線の帯域不足を回避できるため、コンビニや店舗での無料 Wi-Fi の提供が進められています。無料で回線を提供する店舗側にも、集客につながるなどのメリットがありますから、Wi-Fi の使える場所はどんどん増え続けています。

Wi-Fi を利用できるように設定しておきましょう。

ただし、個人情報収集を目的とした悪意をもった接続先（アクセスポイント）もあるので、利用する前に Wi-Fi の運営会社を確認しておきましょう。



②携帯電話から電話帳データを移行する

携帯電話からスマートフォンに乗り換えると、まず電話帳のデータの移行が必要になります。従来型の携帯電話であれば、赤外線通信などで簡単に自分でも行えましたが、スマートフォンの種類によってはうまく移行できないことがあります。これは国内向けの携帯電話と世界標準のスマートフォンの仕様の違いによります。携帯電話購入店で行える場合は、店舗側に任せましょう。自分で行いたい場合はSDカードでの移行、赤外線通信、ネット上にバックアップを取ってからの移行など、いくつかの方法があります。従来の携帯電話とは電話帳の項目名などが違って、全ての項目が移行できないこともありますので、移行後に間違いがないかチェックしておきましょう。



③バッテリーの消費を抑える

スマートフォンと従来型携帯電話の違いのひとつに液晶画面の大きさが挙げられます。液晶画面は大きいほど消費電力も多く必要となりますので、画面設定から明るさと、点灯時間の調整を行いましょう。使用していない時に延々と待受の画像を表示させていると、バッテリーは大量に消費してしまいます。操作後数分で画面が消えるように設定しておきましょう。

また、Wi-Fi、Bluetooth（ブルートゥース）^{*8}等の機能を使用しない場合も、待受中に電力を消費していますので、必要がなければ、設定からOFFにしておきましょう。Wi-Fiは常にONの状態で待ち受けていると、電波が使える場所に入れば自動的にWi-Fi回線に切り替わります。しかし、Wi-Fiが不必要な時も電波を探し続けるとバッテリーを消費することとなりますので、必要な時だけONに手で切り替えるなどすれば、バッテリーの消費を抑えることができます。



④メール設定でパソコンとリンク

スマートフォンの便利な点は、パソコンに届いたメールを出先でも確認できる点にあります。スマートフォンは3種類以上のメールアドレスが使えます。

- ①従来の携帯電話向けメールアドレス。
- ②電話番号でやり取りできる、ショートメッセージサービス（SMS）。
- ③パソコンで使用しているプロバイダの発行するメールアドレス。

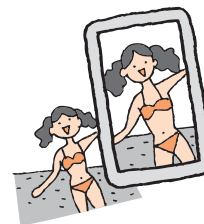
その他に、Yahoo! や Google などのフリーメールもメールアプリで同時に利用できます。

また、パソコン用メールをスマートフォンで読んでも、自身のパソコンでも、後から再度メールを受け取れますので、スマートフォン、パソコン共にデータが残り、紛失も防げます。メール設定から、パソコンメールの設定をしておきましょう。



⑤カメラで撮った写真を自動でウェブ上に保存

スマートフォンを使用していると、カメラを使用する機会が増えると思います。スマートフォンのカメラ機能はコンパクトデジタルカメラ並みに優れています。また、写真を編集するアプリも多く、加工や編集がスマートフォンひとつで行えます。写真共有アプリはスマートフォン本体とは別に、ネット上にも写真データを保存することができます。この共有アプリは撮影と同時に自動的にサイトに保存するものが多いので、非公開設定など、よく公開基準を確認して設定しましょう。



⑥写真の位置情報設定

スマートフォンの写真には位置情報が記録されています。これは、スマートフォンの GPS 情報に基づき、緯度経度が書き込まれます。利用者自身が撮影場所を確認する時には大変便利な機能ですが、そのデータは投稿した画像や、メールに添えた写真にも書き込まれています。不用意にサイト上に投稿した画像から自宅の位置が漏れる場合もありますから、写真に位置情報が必要なければ、設定項目から位置情報サービスを選び、カメラ機能の GPS 項目を使用しない設定にしておきましょう。

また、出会ったことのない相手から写真を要求され、何気なく送ってしまいトラブルに合った事例が多くあります。見知らぬ相手からの写真の要求には応じないようにしましょう。

第3章 安心して使うスマートフォン



①紛失から起きるリスク

スマートフォンなどのモバイル製品に付きまとう問題に、盗難や置き忘れなどの紛失があります。高機能であるが故に多くのデータを保存しているスマートフォンを紛失すると、パスワードやIDなど、仕事関係やプライベートを含め、大変なデータ流出になります。「そんなに重要な内容は登録していない」と思われるでしょうが、電話帳登録でさえ、知人の情報が漏れることになりますし、メモ項目に銀行口座番号を登録していたり、ログインしたままのショッピングサイトでもあれば、通信販売の履歴やカード情報が漏れることもあります。

②スマートフォン紛失から起きる漏れてしまうデータとは

①アドレス帳

スマートフォンのアドレス帳には、機種にもよりますが、約3000件の登録が可能です。データの項目も大変多く、メモ以外に生年月日や学校、勤務先など、自分好みの項目も追加できるため、一人に対し多くの情報を書いている場合があります。

②メールと添付されてきたデータ

パソコンのメールが読める便利な反面、重要なメールでも紛失すると第三者に読まれてしまう恐れがあります。添付データが流出するのは紛失からが多いのです。

③スケジュール管理データ

スケジュール管理はスマートフォンならではの便利な機能ですから、

手帳のように全ての予定を記入している方が多いのです。社内の企画予定、家族の状況などが流出することになります。

④文書やPDFデータ

ワードやエクセルなども使えますから、PCのデータを持ち歩いていると大変重要な内容が漏れることになります。

⑤写真や動画

スマートフォンで保存している写真や動画が漏れてしまいます。会社の写真であれば機密情報の漏れということになるでしょうし、友達の写真であればプライバシー侵害にもなります。

⑥インターネットブラウザ内のブックマークや履歴、ID、パスワード

ネットの検索履歴や表示履歴から、個人の趣味趣向が漏れてしまいます。サイトの会員ログインなどが、自動的に接続できるよう設定している場合は、IDやパスワードが漏れることになります。また、クッキー（一時的にデータを蓄えておく仕組み）内のデータを見られてしまえば、クレジットカード情報などの漏えいにつながり、金銭的なトラブルにもなってしまいます。

⑦ソーシャルサイトの個人情報

SNSなどで登録しているプロフィールやID、パスワードが漏れることになります。第三者が本人になりすまして利用したり、知人に勝手にコメントを送ったりと、深刻な状況になります。

⑧クラウド^{*9}に預けたデータ

便利なクラウドサービスですが、預けたデータは端末があれば見ることができてしまいます。パスワードをその都度要求している場合でも、パスワードが漏れるとデータ流出となってしまいます。

③必ず行いたいパスワードロック

おそらくスマートフォンを使用しだすと、パソコン以上に個人情報を保存することになります。そんな重要な端末を持ち歩くわけですから、必ずパスワードロックの設定をして使用する習慣をつけてください。

スマートフォンには触っても画面が表示できないよう、暗証番号を要求してくるロック機能があります。また、アプリにはそれぞれパスワードを要求するものもありますから、設定できるアプリにはロックをかけておきましょう。

もしもの紛失に備えて、遠隔操作でロックや内部データの削除ができるようなサービスもありますから、事前に設定と手順を確認しておきましょう。車上荒らしなど盗難の場合は、事前にジュラルミンケースを用意して、スマートフォンが遠隔操作できない状況（圏外になるようにする）にして持ち去るケースが増えています。スマートフォンにはパスワードロックを設定し、使用する際にはロック解除をして使う習慣をつけることが、何より重要となってきています。



④スマートフォンの安全対策チェック項目

①パスワードロックをしている。

最初の設定では、起動時のパスワードが4桁の数字であったり、ロック解除パターンがとても簡単なものになっている機種が大半です。安易に想定できない数字やパターンにしましょう。

②英数を混ぜた8桁のパスワードを設定している。

スマートフォンからアクセスする際にパスワードが設定されているサイトが多くあります。スーパーコンピュータでは数字のみで8桁だと解析に数秒です。英数混在で15時間です。最低でも英数混在で8桁のパスワードを設定しましょう。

③遠隔操作ロックなどの予行演習をしたことがある。

パスワードの解析には、時間が必要です。紛失した場合でも、すぐロックできるように遠隔操作の練習をしておきましょう。実際に行わないと、手順が理解できませんし、携帯電話会社のお客サポートセンターなどでは営業時間外では対応してもらえません。

④AndroidのOSやiPhoneのOSを最新に更新している。

OSを最新にすることで、プログラムのバグ（エラー部分）が改善されます。随時新しいOSが提供されていますので、アップデート情報を確認してください。

⑤インストールしているアプリを把握しているか。

無料アプリの中には悪意のあるアプリも紛れ込んでいます。使うことのないアプリがある場合は、削除してください。あまり沢山のアプリがあるとスマートフォンの動きがおかしくなることがあります。ユー

ザーが故障と判断して修理に出しても問題なしとして返却されてしまいます。

⑥ インストールしているSNSアプリは公式版か。

大手の SNS と同じ名前の付くアプリが多く存在しています。非公式アプリは思わぬ情報の漏れにもなりますので、アプリのダウンロードの前に評価欄を確認してください。(P.10 参照)

⑦ 自分の使用しているパソコンと同じ暗証番号を使い回していないか。

インターネットを通じて自分のパソコンとリンクすることのあるスマートフォンですから、同じパスワードを使用していると、パソコンまで狙われることになります。スマートフォンとパソコンでは違うパスワードを設定しておきましょう。

⑧ どのアプリが位置情報を利用するか把握しているか。

設定項目の位置情報欄を見ると、どのアプリが GPS 位置情報を使用するかが分かります。事前に確認しておきましょう。

⑨ ウイルス対策ソフトを最新版に更新しているか。(Androidの場合)

いくらウイルス対策ソフトを入れていても最新に更新していなければ、なんの効果もありません。対策ソフトは新しいウイルスが見つかったら更新されます。常に最新版に更新しておきましょう。

⑩ 盗難にあった場合を想定して、電話会社やプロバイダなどの連絡先を控えているか。

車上荒らしなどで、盗まれる被害も増えています。盗難にあうと動揺して対応が遅れてしまいます。事前に各連絡先一覧を自宅に保存しておきましょう。

● 考えてみましょう

〈回答と解説はP38・P39です〉

次の問 1 から 12 の内容について、正しい(適切な)ものには○、誤っている(不適切な)ものには×を記入してみてください。

問 1 スマートフォンは自分の好きなアプリを取り込める。 ☐

問 2 スマートフォンとタブレットの違いは、大きさだけである。 ☐

問 3 スマートフォンには複数のOSが存在する。 ☐

問 4 時刻表を調べたければ、時刻表アプリを取り込めばいい。 ☐

問 5 無料アプリは収入なしでも使ってもらうために提供されている。 ☐

問 6 スマートフォンの電話帳欄に友達の電話番号と共に誕生日を記載している。 ☐

問 7 携帯電話会社が全てのアプリを管理しているから、発売されているアプリは安全だ。 ☐

問 8 スマートフォンで行う会員登録は、できるだけ詳しく自分のことを書く。 ☐

問 9 ソーシャルサイトで知り合った相手に相談され、一度出会うことになった。 ☐

問 10 ソーシャルサイトのつぶやきは、友達以外は見るできない。 ☐

問 11 スマートフォンの写真にある位置情報から旅行の行動記録を作った。 ☐

問 12 スマートフォンは肌身離さず持っているので、画面ロックの必要はない。 ☐

回答と解説

問① スマートフォンは自分の好きなアプリを取り込める。

☐ スマートフォンは、自分にあったアプリを探して利用することができます。

問② スマートフォンとタブレットの違いは、大きさだけ。

☒ タブレットの多くは電話機能がありません。通話をするならスマートフォンを選ぶ必要があります。

問③ スマートフォンには複数のOSが存在する。

☐ テキスト内に表記しているOS以外にも複数のOSが存在します。OSごとに得意分野が違うため、一般的でないOSはハンドブックでは紹介していません。

問④ 時刻表を調べたければ、時刻表アプリを取り込めばいい。

☐ 使いたいことに応じたアプリが存在しています。便利なアプリを探し出して利用しましょう。ただし、ダウンロードする前に同意事項の確認や利用者の評価欄にも目を通しましょう。

問⑤ 無料アプリは収入なしでも使ってもらうために提供されている。

☒ 無料アプリの収入源は、アプリ利用中に表示される広告収入や、会員登録時の個人情報から広告メールやダイレクトメールを送ることで利益を上げています。無料アプリを使用する場合は、利用者の評価欄を見て、被害が出ていないか確認しましょう。

問⑥ スマートフォンの電話帳欄に友達の電話番号と共に誕生日を記載している。

☒ スマートフォンの電話帳欄は項目が多く、ついついメモ代わりに友達の情報を書き込んでしまいます。電話帳のデータが流出すると、友達に迷惑がかかるだけでなく、人権侵害などの思わぬトラブルにもなります。できるだけシンプルな登録を心がけましょう。

問⑦ 携帯電話会社が全てのアプリを管理しているから、発売されているアプリは安全だ。

☒ アプリは携帯電話会社の管理外です。自己責任での利用となりますので、どんなアプリなのかを確認して利用しましょう。

問⑧ スマートフォンで行う会員登録は、できるだけ詳しく自分のことを書く。

☒ セキュリティ対策のしっかりしたサイトばかりではありません。無料サイトの会員登録などは特に注意して、実名を書かない、住所を書かないなど、必要以上の記入は避けましょう。

問⑨ ソーシャルサイトで知り合った相手に相談され、一度会おうことになった。

☒ インターネット上の相手は出会ったことのない相手です。いくらネット上で親しくなったとしても、相手のプロフィールは偽物かもしれません。サイトの相手が相談してきて、お金を貸した事例や、出会って性犯罪にあった事例は多くあります。出会ったことのない相手との会話だということを忘れずに、慎重に利用しましょう。

問⑩ ソーシャルサイトのつぶやきは、友達だけ見ることができる設定にしているから安心。

☒ 友達の友達にも見ることが出来ます。友達の友達…続けると全ての人となります。ダイレクトメッセージ以外は誰にでも見えると思っていいでしょう。他人に見られてまずいようなことは書かないことです。

問⑪ スマートフォンの写真にある位置情報から旅行の行動記録帳を作った。

☐ ご自分で利用する記録であれば、位置情報をうまく使うと場所が確認でき、行動記録がとりやすくなります。ただし、ネット上のブログに掲載する場合は写真の位置情報を消すため、一度パソコンに写真を転送し、ペイントデータ等として保存し直してから投稿するようにしましょう。

問⑫ スマートフォンは肌身離さず持っているので、画面ロックの必要はない。

☒ いくら肌身離さずといっても、置き忘れや盗難はいつ起きるかわかりません。自分のためだけではなく、電話帳に登録してある知人のためにもロック設定はしておきましょう。

用語解説

※ 1 【OS】 Operating System

オペレーティングシステムとは、コンピュータを制御し、アプリケーションソフトなどがコンピュータ資源を利用可能にするためのソフトウェアのこと。

※ 2 【ガラバゴスケータイ】

ガラバゴス諸島は、大陸、島々の交流が絶たれ、その結果、生物は独自の進化を遂げています。日本の従来の携帯電話は、世界標準とはかけ離れた、ある意味高度な進化を遂げました。ガラバゴス諸島の生物の進化になぞらえ日本の携帯電話は“ガラバゴスケータイ” “ガラケー” と呼ばれることがあります。

※ 3 【携帯電話回線】

携帯電話で一般的に利用されている通信網のこと。現在は、第3世代の携帯電話方式の3Gが主流。LTE等の、4Gと呼ばれる高速通信が普及しつつある。

※ 4 【Wi-Fi (ワイ・ファイ)】

インターネット通信を無線で行う無線LAN通信の標準規格「IEEE802.11a/b/g/n」に対して、業界団体WECA(現:Wi-Fi Alliance)が名付けたブランド名。

※ 5 【GPS】 Global-Positioning-System

人工衛星を利用して位置情報を割り出すシステムのこと。

※ 6 【ソーシャルゲーム】

ソーシャルゲームとは、SNS(ソーシャルネットワーキングサービス)上でソーシャルアプリとして提供されているゲームの総称。ソーシャルゲームには、SNSを通じてコミュニケーションを取っているユーザー同士が共にゲームを楽しめる、あるいはゲームを通じてコミュニケーションが取れるという特色がある。

※ 7 【情報リテラシー】

狭義では、情報機器の操作能力。広義には、情報ネットワークを活用する方法や情報の評価、倫理等を理解し、あらゆる情報を活用する能力を指す。

※ 8 【Bluetooth (ブルートゥース)】

携帯情報機器などで数メートル程度の機器間接続に使われる短距離無線通信技術の一つ。

※ 9 【クラウドサービス】

データを自分のパソコンや携帯電話ではなく、インターネット上に保存するサービスのこと。自宅、勤務先、学校など外出先で、さまざまな環境のパソコンや携帯電話(主にスマートフォン)からでもデータを閲覧、編集、アップロードすることができる。

制 作 兵庫県健康福祉部生活消費局消費生活課

〒650-8567
兵庫県神戸市中央区下山手通5丁目10番1号
TEL.078-362-3157 FAX.078-362-4022

大学生協阪神事業連合 行政連携事業事務局

〒651-0063
兵庫県神戸市中央区宮本通7丁目1番13号
大学生協神戸会館内
TEL.078-262-5670 FAX.078-252-7783

このハンドブックは、兵庫県と大学生協阪神事業連合との「次世代の消費者教育・学習に関する協定」に基づく協働事業の一環として作成しました。