子どもと学ぶネット社会　資料２

安心して使うスマートフォンとタブレット
～情報漏えいから身を守ろう～

滋賀県イメージキャラクター
キャッフィー

執筆者
ＮＩＴ情報技術推進ネットワーク代表
篠原　嘉一

滋賀県

目　次

はじめに

近年、スマートフォンが急速に普及してきています。そこで、スマートフォンと従来型の携帯電話との違いを知り、スマートフォンの使用上の注意点を理解していきましょう。

なお、スマートフォンと同様の機能を持つタブレット型端末（ひと周り大きなスマートフォン）についても、同様のトラブルが考えられますので紹介していきます。

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

以前は、持ち歩きできる携帯情報端末が各社から販売されていましたが、どの機種も各メーカーの思いが強く、ユーザーが何にでも便利に使えるというモノではありませんでした。スケジュール管理に特化したモデルが多くありましたが、いざその端末で全てのスケジュールを管理しようとすると、まず、使いこなすための知識が必要でした。また高機能ゆえ、多くの情報を入れてしまうと、故障でもした時には、すべてのデータが消えてなくなる不安を持っていました。メーカーそれぞれが競い合って開発していましたので、メーカごとの互換性がなく、一度購入した機種を使い続けなければならない環境でした。

そこに、iPhone（アイフォン）がアップル社より発売され、この問題がほぼ解消されることとなり、爆発的に売上を伸ばすという結果をもたらしました。本体、OS※1（携帯を動かす基本的なソフト）、アプリ※2（さまざまなソフトウエア）をアップル社が一貫して開発・製造しているからです。今までは携帯電話会社の意向が大きく影響し、開発者の思うように作ることができず、中途半端な形で市場に出回り、使いづらいと評判を落としてきた多機能端末が、iPhone の登場で一気にユーザーの理想に近づいたのです。iPhone は、携帯電話会社に合わせた回線を組み込むだけで、スムーズに導入にこぎつける事ができました。

高機能携帯電話からスマートな（かしこい）携帯電話へと進化したのです。高機能携帯電話は、利用者がその機能を理解して使う必要がありましたが、iPhone は、それ自体が利用者に歩み寄るかしこさを持つタッチパネルを使用することにより利用者の直感的な操作を可能にしました。

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その点が、利用者の増加につながりました。

このブームのおかげで iPhone の OS とは異なる AndroidOS も市場に受け入れられました。アップル社と契約できなかった携帯電話会社は、AndroidOS を選び、スマートフォンを提供しています。

Android はグーグル社の 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。（Ｐ４　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電話ほどインターネットへの対応が進んでいません。（海外の国の携帯電話は基本的に電話をする機能以外はありません。）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様子から「ガラパゴスケータイ」※3「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１００％把握、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、多く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。

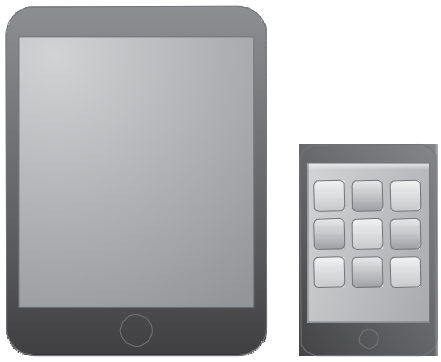
スマートフォンには携帯電話会社の意向が必ずしも反映されず、携帯電話会社は回線を提供する程度にとどまっています。携帯電話会社がシステム全体をすべて管理できていた頃とは違い、携帯電話会社はスマートフォンをほとんど把握できない場合もあります。この違いが、悪意のある人物につけ込まれる隙を与え、責任の所在を曖昧にしています。

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※2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定される場合が多く、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(３G※5等)だけでなく、高速な無線 LAN 通信（Wi-Fi※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※7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。 ●電池のも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

いくら便利なスマートフォンでも、年齢によって文字の小ささが気になる方もおられると思います。指の操作で画面拡大できるので、従来の携帯電話より大きくはなりますが、すべてが拡大できるわけではなく、今ひとつ購入に踏み切れない方もおられるでしょう。



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

やソフトウエ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せます。

タブレット型には、無線回線（Wi-Fi）※4のみのモデルと、電話回線でもネットが使える３G※5＋Wi-Fi モデルがあります。後者はパケット通信料※6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、まず電話会社を決めなければなりません。これは既に携帯電話をお持ちの場合、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	
	AndroidOS	iPhoneOS
□ドコモ　＝	○	×
□ au　＝	○	○
□ソフトバンク　＝	○	○
□イーアクセス　＝	○	×

（注意：平成 25 年現在で、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 iPhoneOS と AndroidOS の 2 種類に限定して表記しています。）

次に OS の違いを理解して選択します。

iPhoneOS はすべてアップル社の管理下にあります。基本 OS に関わる技術者は登録制です。アプリを制作する場合でも、登録して審査を受けます。開発ツールも購入します。アプリができ上がれば、アップル社が 2 ヶ月かけて審査を行ないます。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。そのため、Android と比べ、扱える携帯電話会社が制限されます。

AndroidOS は、グーグル社の管理下にあります。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、グーグル社から OS を購入し、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出来るのです。

アプリに関しても自由に開発できます。製作者はフリーマーケットのように自由に販売が出来ます。審査が無い反面、利用開始から数ヶ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。（Ｐ５　６．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、個人情報回収を目的としたアプリの発見が遅れることのひとつの要因です。

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や、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出来る便利なアプリですが、本体にダウンロードする際には必ず規約が表示されます。規約に同意した場合のみアプリを利用しているという事ですから、十分に規約を確認してからダウンロードして下さい。

無料でアプリが使えるのには、理由があります。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、収入を得ているもの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」という内容を記載して堂々と電話帳の記録や通話履歴、位置情報を回収する場合もあります。

悪意のあるアプリは、購入時に標準搭載されているアプリ以外のものですから、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下さい。

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」

「携帯電話会社が管理不可能なこと」

「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き取られ、GPS※7により位置情報が特定され、検索結果を見られることにより、個人の趣味趣向が悪意のある者に知られてしまうのです。スマートフォンの設定を意識しなければ、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１００％と言えるほど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うこともあり、ほとんど携帯電話会社では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かすら想定できない状況なのです。

８．携帯電話会社とアプリ管理会社

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ます。Android はグーグル社の管理です。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

アプリのなかには会員登録をして利用するタイプのものもあります。ゲームサイトなどは、無料で使用できるか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作業になります。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。（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かわりに、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※8に参加しようとしているとします。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たとします。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、女子中学生になりすました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を名乗るなど別人になりすまし、情報を集めることができてしまうのです。

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者になりすまし、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り合った東京に住む同い年の女の子とチャット※12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、彼女をのことすべて知っている

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）は情報回収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。

11．人気のソーシャルサイト

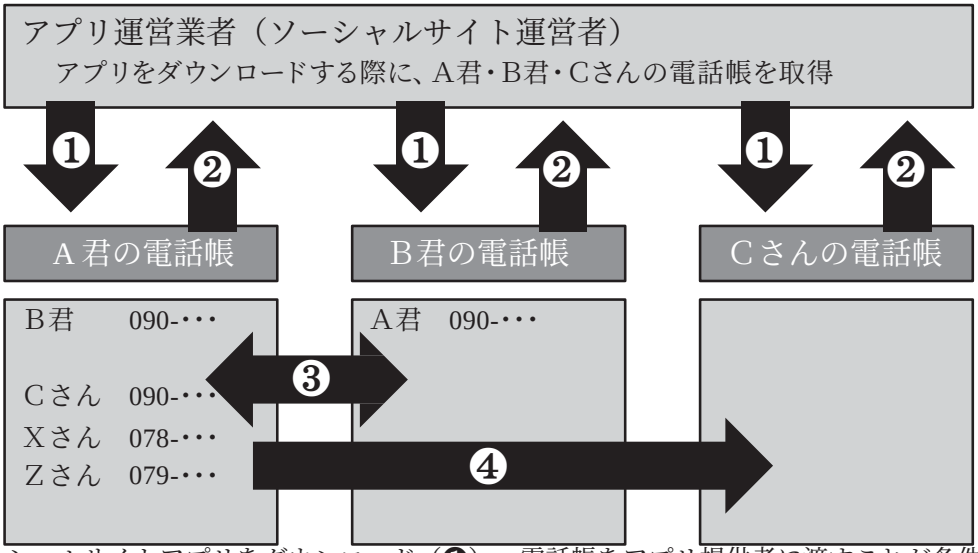
スマートフォンが爆発的に普及した理由のひとつに、ソーシャルサイト（SNS）※9の存在が大きく影響しています。ソーシャルサイトとは、利用者間を結びつけ、お互いに情報共有しようというものです。例えば自分の同級生や遠くに住む友達などの情報がいつも見ることができれば、楽しいだろうと結びつけるサービスです。多くの人達はこのサービスを提供するアプリをダウンロードして利用しています。ではなぜ、この同級生や友達を見つけ出せるのでしょうか。それは、アプリの会員を増やす仕組みにあります。アプリをダウンロードする際に規約に書いてあるのですが、自分のスマートフォンに登録している電話帳のデータをアプリ運営業者に提供させ、電話帳つながりで友達、知人を結びつける仕組みです。自分の電話帳の中にある友達の電話番号が相手のスマートフォンにコメントを送ります。相手も同じアプリを持っているとつながり、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、つな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、つな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、思わぬ人物とつながりトラブルになることがあります。

例えば、企業で働く人が仕事上のことをつぶやく行為は、良くも悪くもその企業に影響を与えます。友達だけに公開した情報だと思っていても友達の友達をたどることにより、すべての会員はつながるのです。書き込んだ情報は永遠に消えないものだと意識していないと、大きな落とし穴に落ちることとなってしまいます。

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（❶）、電話帳をアプリ提供者に渡すことが条件になります（❷）。

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況で、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（❸）。

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（❹）。

例えば、社会人になったA君とCさんが高校時代は仲の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をはらんでいます。

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、身元がわ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、アプリを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○○さんだと解ります。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わかってしまいます。

匿名のつもりでネットで誹謗中傷や、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、就職にも影響するかもかもしれません。

12．狙われる個人情報

前述したとおり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、のぞき見ら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付きにくいのです。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つながります。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、個人情報へもつながり、履歴から利用者の趣味趣向がわ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。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きたため、必要のない人にまでチラシをばらまかなくなってきたのです。サイト運営会社は多くの個人情報を回収していますから、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、ネット上の広告にも自宅に届くダイレクトメールにも、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。不正プログラム、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が、そ

れ以上に利用者の情報リテラシー※10の稚拙さが原因の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）※11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漏れにつながるかもしれません。「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）※9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。この部分を紐づけすれば、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※12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お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しまいます。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守秘義務違反に問われた公務員の場合

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つ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たようです。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、おそらく想像されたことが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。

17．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となります。

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たそうです。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アプリでした。その非公式アプリの設定が、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、極秘情報がもれるということになってしまいます。

18．スマートフォンのウイルス対策

スマートフォンでもコンピュータ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、前述の通り、すべてが管理されているためウイルス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エアですので、一度感染して、持ち出されたデータを回収する機能はありません。防波堤のようなもので、崩れると終わりなのです。

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。携帯電話会社毎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。

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

スマートフォンや携帯電話は３G 回線と呼ばれる電話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３G 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不足に直結します。

スマートフォンは、インターネットを３G 回線以外に Wi-Fi 回線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 の無線回線は、３G 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３G 回線にも余裕ができ、回線不足を回避できるため、コンビニや店舗での無料 Wi-Fi 回線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、ネットの使える場所はどんどん増え続けています。

Wi-Fi の利用は設定項目にあります。利用できるように設定しておきましょう。

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、いくつもの方法があります。携帯電話とは電話帳の項目名などが違っていて、すべ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※13 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 に手動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出来る、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。

パソコン用メールアドレスと携帯電話用メールアドレスでは使用するアプリが違っていますので、間違えて操作することもありません。また、パソコン用メールをスマートフォンで読んでも、後からパソコンでも、再度メールを受け取れますので、スマートフォン、パソコンともにデータが残り、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エブ上に保存

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ことと思います。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、加工や編集も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くありますので、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。利用者自身で、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．スマートフォンの紛失で漏れてしまうデータとは

①アドレス帳

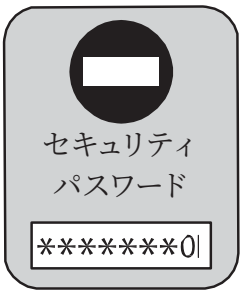
スマートフォンのアドレス帳には機種にもよりますが、約 3,000 件の登録が可能です。データの項目も大変多く、メモ以外に生年月日や勤務先など、自分好みの項目も追加出来るため、一人に対し多くの情報を登録している場合があります。

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３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。社内の企画予定などが流出することとなります。

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これらの内容が流出することになります。

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。仕事上の写真であれば機密情報の漏れということも考えられるでしょうし、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、自動的に接続出来るよう設定してある場合は、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なるおそれもあります。

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３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、深刻な状況になることも考えられます。

⑧クラウド※14 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出来てしまいます。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出来ないよう、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、設定出来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出来るようになっていますから、事前に設定と手順を確認しておきましょう。事前に登録した自宅電話番号や家族の携帯電話から発信することで、遠隔操作が可能になります。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。
起動時のパスワードは４桁の数字の機種が大半です。安易に想定できない数字にしましょう。

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様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。

④AndroidOS や iPhoneOS 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。あまり多く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。（Ｐ３参照）

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となります。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ると更新されます。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。

終わりに

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、手放せなくなる人も多いようです。カメラにも音楽プレイヤーにもカーナビにもなり、電車の時刻表や駅の構内案内マップもすぐ調べることができます。歩行ナビでは、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、文字の拡大もできます。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、今日の情報社会では危険性を恐れているばかりというわけにはいきません。

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【アプリ】
　スマートフォン用アプリケーションソフト（様々な用途のソフト）のこと。ゲームやニュース、乗換案内など、多数のアプリがある。アプリのマーケットサイトにアクセスしてダウンロードする。

※３【ガラパゴスケータイ】
　ガラパゴス諸島は、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。日本の携帯電話は、世界標準とはかけ離れた進化を遂げました。ガラパゴス諸島の生物の進化になぞらえ日本の携帯電話は“ガラパゴスケータイ”“ガラケー”と呼ばれています。

※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【３Ｇ（スリージー）】
　現在の携帯電話で一般的に利用されている通信網のこと。第３世代の携帯電話方式の総称。（次期モデルでは４Ｇと呼ばれる高速通信）

※６【パケット通信料】
　携帯電話でｗｅｂサイトやメールなどを利用した時のデータ通信にかかる料金。

※７【ＧＰＳ】
　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。

※８【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

※９【ソーシャル・ネットワーキング・サービス（ＳＮＳ）・会員制交流サイト】
　「人同士のつながり」を電子化するサービス。自己情報のコントロールや人との出会といった目的を掲げ、各社がサービス行っている。「コミュニティー」を通じた「友達の輪」のネットワーク型組織。mixi、Facebook、Line など。

※１０【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。

※11【ブログ】
　日記的なウエブサイト。

※12【チャット】
インターネットを介して２人以上で行われる会話。

※13【Bluetooth】
携帯情報機器などで数 m 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。

※14【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。