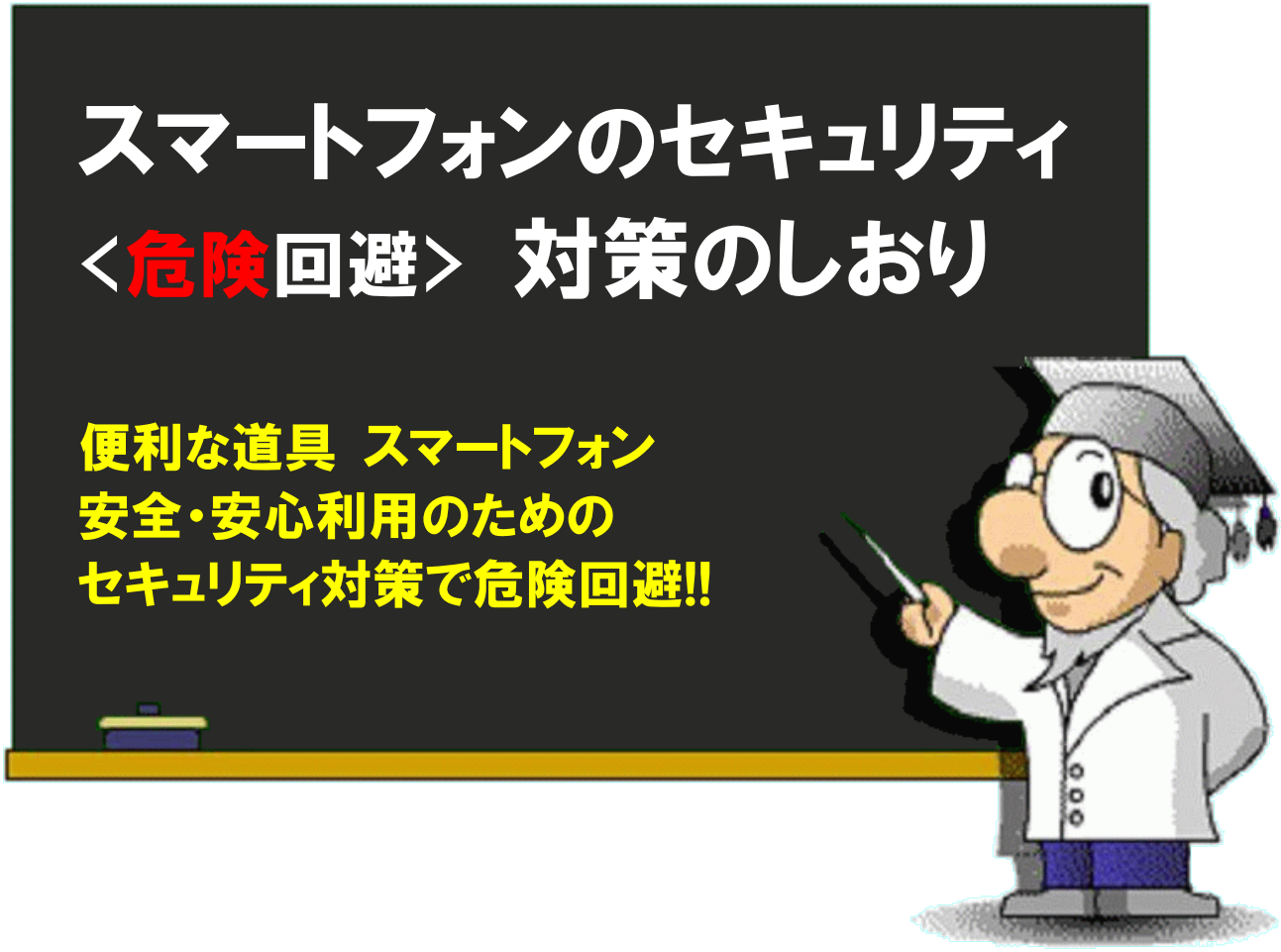
IPA 対策のしおり シリーズ (8)

スマートフォンのセキュリティ
<危険回避> 対策のしおり

便利な道具 スマートフォン
安全・安心利用のための
セキュリティ対策で危険回避!!

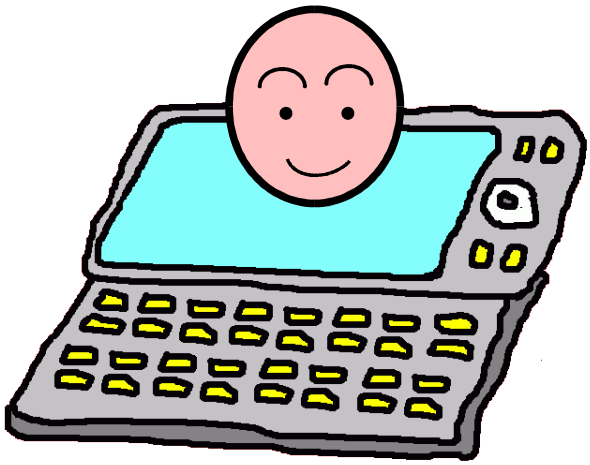


IPA 独立行政法人情報処理推進機構
セキュリティセンター

http://www.ipa.go.jp/security/

2012年6月8日 第2版

目次



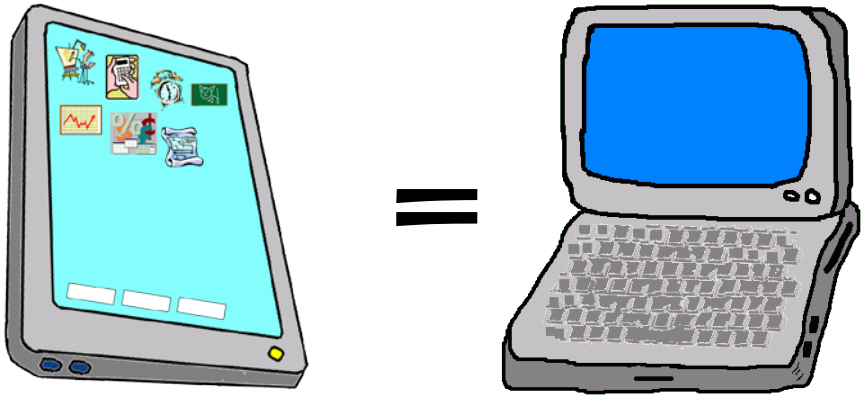
はじめに

まわりを見渡してみて下さい。スマートフォンと呼ばれる携帯型端末が流行しています。電車の中、駅のホーム、コーヒーショップ、公園のベンチあらゆるところで気軽に利用されています。

インターネット上の動画も見られるし、小説を読むことも出来ます。買い物も出来るし、小遣い帳を付けることも出来ます。

高機能な携帯電話といえるスマートフォン、携帯電話専用の制限のあるWebサイトではなく、パソコンと同じWebサイトがそのまま参照できたり、自分専用のあるいはみんなでオンライン利用できるアプリケーション（各種機能を実現するプログラム）が自由に使えたりします。

つまり、その実体はパソコン（パーソナルコンピュータ）であるといえます。



皆さんの良く知っているパソコンと同じとは思えないでしょうけれど、ネットブックとかタブレットPC（スレートPC）と呼ばれるモバイルパソコンと同じですよね？

インターネットを介していろいろなネットワークに繋がる機能と機動性が、クラウド・コンピューティング*1の拡大とあいまって、企業活動にも効果的であることが着目されてきています。実際に、タブレット系の大型ディスプレイを搭載したスマートフォンが、営業活動を行う上での新しい武器（ツール）になりつつあるようです。

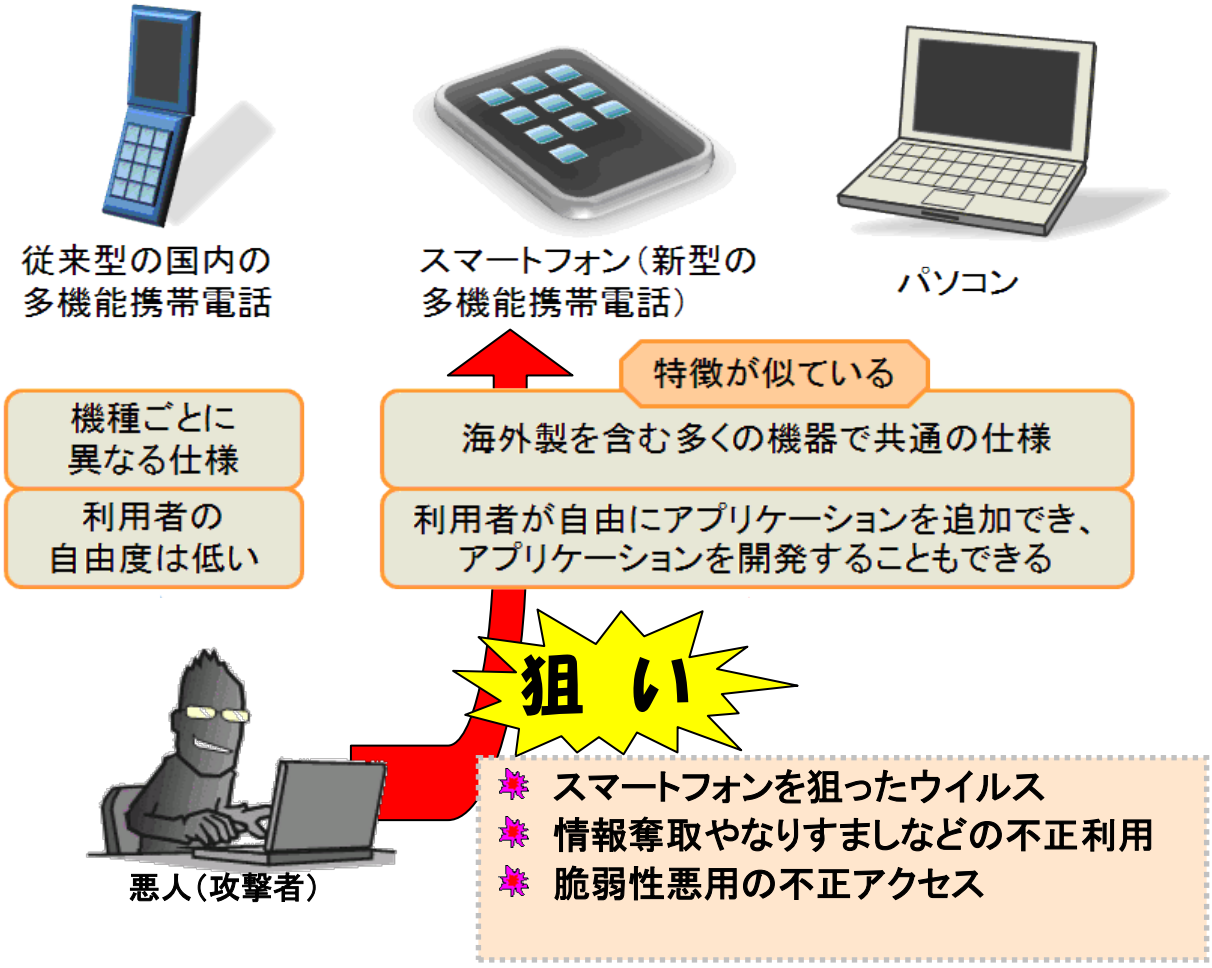
何といっても見た目や表示できる映像・画像にインパクトありますから、効果抜群といった具合です。さらに、教育現場でも教科書の代わりに利用されたり、医療現

場で持ち歩き可能な情報端末として利用されたり、今後のさらなる利用者の増加も予測できます。

しかし、利用者の増加は別の問題も発生させます。利用者が多い環境は、悪人たち（攻撃者たち）にとっては格好のターゲットとなります。

携帯電話はその利用環境がある意味閉鎖的（必ずキャリアを経由する利用環境、機種毎に仕様も違う）であったために、あまり攻撃の対象にはなりませんでしたが、パソコンと同じ利用環境でも動作するスマートフォンは、パソコンやネットワークを攻撃ターゲットとしていた悪人たちの次なる狙い目となってきているようです。

つまり、「利用者が多い」「攻撃対象の特徴が似ている（同じ）」「攻撃のための資産(資源)が使える」等の理由から、悪人たちから目を付けられたということです。



ところで、スマートフォンの利用者が一番気になる問題（脅威）は何でしょう。いろいろな調査機関での報告にもありますが、それは**盗難・紛失**です。

携帯電話もそうでしたが、スマートフォンは便利な代物だけに**紛失する**ことは利用者にとって厄介な問題です。自分自身の情報、おサイフ機能のプリペイドマネーやカメラ機能で蓄積された映像や画像データ、自分自身で購入した動画や音楽

やアプリケーションのデータ、アドレス帳のような友達情報、さらには企業活動で得た情報（顧客情報や営業情報）も蓄積された電子記憶媒体（まるで機能をたくさん持った USB メモリ）であるといえます。当然のことですが、無くなれば、情報漏えいの恐れがあるわけです。

さらに、盗難･紛失により発生する不正使用も考えられます。自分が使っていないのに使用料や有償アプリの購入代金が請求されるなんて、利用者にとっては許しがたいことです。こういった金銭トラブルも利用者にとっての脅威と言えるでしょう。

近年、情報セキュリティと言えば情報漏えい問題が大きく取り沙汰されますが、盗難･紛失対策だけでなく、前述したような、**悪人の攻撃から身を守る**ことも重要なセキュリティ対策となります。

こういった状況の中では、スマートフォンでは、パソコンや各種の電子記憶媒体と同様のセキュリティ対策が必要となります。

それらのセキュリティ対策は、利用者自らがスマートフォンのセキュリティを意識し、実施する必要があるわけです。

というわけで、スマートフォンのセキュリティ対策として大きく 3 つに分けて考えてみましょう。

スマートフォンの盗難・紛失対策
スマートフォンの感染対策
スマートフォンの情報漏えい対策

*1) クラウド・コンピューティング

クラウド（コンピューティング）とは、自前でIT（の動作環境：ハードウェア）を持たないで、ITのサービス（ハードウェアやソフトウェアの機能）だけを利用するひとつの方法です。

例えば、インターネットを検索するような簡単な操作で、会社内の事務作業だけでなく、営業活動や業務活動を効率よくこなすためのサービスを受けることができます。さらに、既存のパソコンだけでなく、高機能な携帯電話ともいえる最新のスマートフォンや携帯電話、あるいはタブレット型コンピュータからの利用でも十分威力を発揮します。営業の出先や自宅など、会社外からの業務処理もできるようになってきており、営業活動などの効率化や業務改善も簡単に実現できるようになってきています。

1.スマートフォンの盗難・紛失対策

携帯電話や電子記憶媒体、モバイルパソコンと同様に、スマートフォンも盗難・紛失に備えたセキュリティ対策が必要です。

まず、携帯電話や電子記憶媒体、パソコンでのセキュリティ対策を思い出してください。

■ 携帯電話の場合

携帯電話の場合は、暗証番号(パスワード)による機能ロックや、盗難・紛失時にリモートから強制ロックするキャリアのサービスを利用したセキュリティ対策が効果的です。さらには、SIM(UIM/USIM)カード*2が悪用(なりすまし利用等)されることを防ぐためのPINコード*3によるロックが効果的です。さらに、拡張メモリ(SDメモリ等)には重要なデータを安易に格納しない*4などの対策も重要です。

■ 電子記憶媒体の場合

電子記憶媒体の盗難・紛失対策は、やはり暗号化です。さらに、利用時の認証(パスワード入力)を数回失敗するとデータを強制消去する機能もあるようです。まぁ、鈴を付けたり、大きなタグを付けたり、常時首から提げるためのストラップを付けたり、他人に貸さないとか、利用者自らが実践するセキュリティ対策もあります。

■ モバイルパソコンの場合

モバイルパソコンの場合は、利用するにあたって、BIOSのパスワードロック*5や安易に推測されないパスワードを使ったログイン機能、HDD(ハードディスクドライブが抜き取られ別のパソコンに接続されても情報漏えいさせないためのHDDの暗号化など、いろいろなセキュリティ対策があります。また、インターネット経由でのリモート接続によるHDD内のデータの強制消去や接続環境から利用者位置を特定する機能やサービス*6を利用したセキュリティ対策が実施される場合もあります。

さて、スマートフォンではどうでしょう。

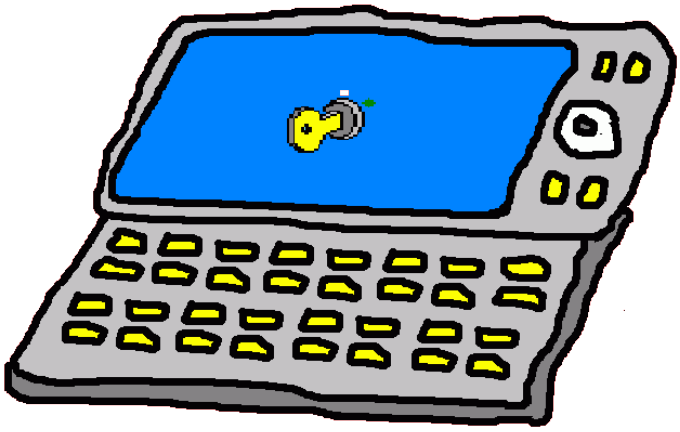
スマートフォンの盗難･紛失対策も、携帯電話や電子記憶媒体、モバイルパソコンと同じです。

- **パスワードによるデバイスのロック（利用者認証）が効果的**
- **携帯電話と同じように、SIM（UIM/USIM）カードの PIN コードによるロックも必要（SIM カードの不正利用対策）**
- **重要な情報を格納（保存）するならば、データの暗号化対策（アプリ）が必要**
- **携帯電話やモバイルパソコンと同じようにリモート（遠隔）からの強制ロックやデータの強制消去サービス、位置情報の確認サービス（置き忘れ/盗難の確認）あるいはそれらの機能を持つ専用のアプリケーションの利用も効果的**
- **拡張メモリスロットがある場合は、安易なデータ格納は避けましょう（SD カードなどのフラッシュメモリはデータの完全消去が難しい電子記憶媒体で、消したつもりのデータが復元できる可能性があります）**
- **大事なデータはスマートフォンとは別の場所（例えば、オンラインストレージや PC を通じて外部記憶媒体等）にバックアップを取っておきましょう。ただし、バックアップ媒体もセキュリティ対策（盗難･紛失対策）が必要です**

といったところでしょうか!!

最初の二つについては、設定方法など機種ごとで異なるので、機種毎の取扱説明書をよく読んでご利用ください。

意外と「パスワード（利用者認証）によるデバイスのロック」が利用されていないといった報告*7もあるようですが、面倒くさがらずに、パスワードロックは利用しましょう。また、ロックしていない状態で紛失した場合は、キャリア等が提供するリモートロックサービスを思い出してください。



*2) SIM(UIM/USIM)カード

携帯電話や携帯端末で使われている電話番号を特定するための固有番号が記録されたICカードです。この番号を元に電話料金などが課金されます。

*3) PIN(Personal Identification Number)コード

携帯電話や携帯端末の機能を利用する場合に、利用者本人を特定(認証)するために使われる暗証番号です。前述のSIM(UIM/USIM)カードに登録されます。

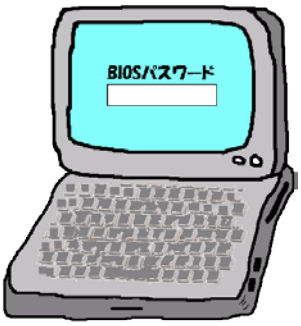
*4) 拡張メモリ(SDカード等)には重要なデータを安易に格納しない

SDカードなどのフラッシュメモリは、格納されたデータを削除したりフォーマットしたりしても、消したはずのデータが復元される可能性が高いようです。これは、フラッシュメモリ等の寿命問題と密接な関係があります。フラッシュメモリは小さな物理的なスイッチがたくさんで組み立てられたメモリですが、それらのスイッチが開け閉めされる回数が寿命となります。そのため、寿命を延ばすためには、一度使ったスイッチをなるべく使わないようにします。結果、一度データが書き込まれた場合は、そのあたりはなかなか使わないようになります。つまり、消したはずのデータなかなか別のデータで上書きされないため、復元しやくなっているといえます。

このような仕様なので、重要なデータを安易に格納すると、それらのメモリから情報漏えいする可能性があるわけです。同じ理由で、それらのメモリの貸し借りは避けたほうが無難ということになります。他人には見せられない大事な写真、削除したはずなのに、復元されたら嫌ですよね…

*5) BIOSのパスワードロック

コンピュータを起動するときに最初に動作するプログラムであるBIOS(Basic I/O System)にパスワードによる認証機能が適用されている場合があります。このパスワードによる認証機能により、コンピュータの不正利用を防ぐことができます。ただし、コンピュータに接続している各種のデバイスを取り外した場合、それらのデバイスは別のコンピュータで利用できるので、コンピュータ本体の不正利用を抑止することしかできません。さらに、このパスワードを忘れると非常に厄介なことに(コンピュータの基板(マザーボード)を交換しないと何もできなくなる)なるので、パスワードを忘れないように注意してください。



*6) 利用者位置を特定する機能やサービス

GPS(Global Positioning System:カーナビなどに利用される全地球測位システム)を利用しなくても、インターネットに接続する方法によっては、利用するコンピュータの利用場所をアクセスポイントなどからある程度特定することができます。これを利用して、コンピュータの利用場所を特定する機能やサービスがいろいろ提供されています。一般的には、利用者に利用環境にあわせた情報の提供などに利用(いわゆるマーケティング利用)されますが、使い方によっては盗難コンピュータを探索する場合に利用することもあります。

*7) 報告

2011年8月にこんな記事がありました。

67% のユーザーが携帯電話をパスワードで保護していない(ソフォス)

http://www.sophos.co.jp/pressoffice/news/articles/2011/08/67-percent-not-password.html

2. スマートフォンの感染対策

前述の盗難･紛失に備えたセキュリティ対策以外にも、スマートフォンで考慮すべきセキュリティ対策があります。

「はじめに」にも書いたように、利用者が自由にアプリケーション（以下アプリと呼ぶ）をインストールし、様々な用途に利用できます。そのため、スマートフォンの利用者は、パソコンの利用者と同様に、コンピュータウイルス（以下ウイルスと呼ぶ）による被害や不正アクセスによる被害に遭う可能性があります。さらに、不正なサイトに誘導されフィッシング被害やワンクリック詐欺の被害に遭う可能性もあります。

2011 年 1 月 21 日、IPAはスマートフォンのウイルスに関する注意喚起*8を公開しました。これは、Android（アンドロイド）というOS*9を採用している、一部のスマートフォンやタブレット型端末（Android端末）に感染する可能性のある危険性の高いウイルスが発見され、国内の利用者でもその被害に遭う可能性が高まったためです。

その後も、Android 端末を狙ったウイルスは増加傾向にあり、徐々に機能も高度化しつつあるようです。そういった意味では、スマートフォンの第一の自己防衛対策は、スマートフォンを狙ったコンピュータウイルス対策ということになります。

*8) 注意喚起

「Android OS を標的としたウイルスに関する注意喚起」（IPA）
http://www.ipa.go.jp/security/topics/alert20110121.html

*9) Android（アンドロイド）という OS

Android は米 Google 社が発表した、Linux ベースのモバイル用 OS です。OS とは、Operating System の略で、「基本ソフトウェア」とも呼ばれています。スマートフォンを含む、コンピュータなどの機器（ハードウェア）の基本的な制御をつかさどり、様々なアプリケーションソフトウェアを動作させる基盤部分のことです。

■ コンピュータウイルス対策

スマートフォンを不正な処理を行うマルウェア（マリシャスウェア：有害なソフトウェア、コンピュータウイルス全般のこと。以下ウイルスと呼ぶ）や不正アクセスの脅威から自己防衛するためには、スマートフォンが利用者の意図に関わらず、ウイルスに感染しないようにしなければなりません。ウイルスに感染すると、そのウイルスを介してあるいはウイルスが盗み出した個人情報を介して、不正アクセスが行われる危険性が高まります。

ウイルスに感染するのは、大きく分けて以下の場合です。

- **スマートフォンの動作環境（OS やブラウザ）にウイルスに悪用される脆弱性が存在する場合**
- **利用者が意図せずに自分でウイルスをインストールする場合**

前者の対策は、動作環境（OS）の脆弱性を解消することです。

スマートフォンの OS は常に最新の状態にアップデートする

スマートフォンの場合は、基本的に販売元（キャリアまたはメーカー）主導で OS のバージョンアップやアップデートが行われます。Android 端末の場合は、機種毎に使用される OS のバージョンが違っていたり、販売元毎に独自機能を組み込んだりしてある場合が多いので、一律にバージョンアップやアップデートが行われるわけではありません。

Android 端末の OS は、Linux ベースのモバイル用 OS で常に進化しているため、機種によってはサポート対応が遅れる場合もあるようです。販売元の機種毎の情報を常に意識し、必要に応じて対応してください。

後者の対策は、ウイルスに感染しないようにすることです。

アプリは信頼できる場所からインストールする

一般的に、スマートフォンがウイルスに感染するのは、利用者が意図的にインストールするアプリにウイルス（不正な処理）が仕込まれている場合が多いようです。

利用者がアプリをインストールする経路には、いわゆるアプリケーション・ストア（App Store は Apple 社での呼称、Android 系では Android Market）と呼ばれるアプリの配信チャネルからインストールする場合や、SNS（ソーシャル・ネットワーク・サービス）や SMS（ショート・メッセージ・サービス）を通じて、アプリのインストール勧誘から行われる場合があるようです。

正規でないアプリ・ストアからインストールしたアプリの場合、正規のアプリと見た目が同じアプリ（海賊版）があったとしても、場合によってはウイルスが仕掛けられている場合もあるようです。

そのため、アプリをインストールする場合は、必ず信頼できる場所からインストールすることをお勧めします。

一般的に、信頼できる場所とは、メーカーやキャリアが用意する正規のアプリケーション・ストアであるといわれています。しかしながら、正規のアプリケーション・ストアでもストア側の監視の目をかいくぐってウイルス付きのアプリが提供される場合も、ごく稀にあるようなので、Android 系のスマートフォン（Android 端末）の場合は、次の対策も併用してください。

Android 端末では、「提供元不明のアプリ」はインストールしない設定にしておく

Android 端末の設定画面に「提供元不明のアプリ」という項目があります。この項目のチェックを外しておくと、正規のアプリ・ストア（Android Market）以外で入手したアプリケーションのインストールが阻止されます（初期状態ではチェックは外れた状態になっています）。「提供元不明のアプリ」の設定の確認・変更手順は、図1を参照してください。

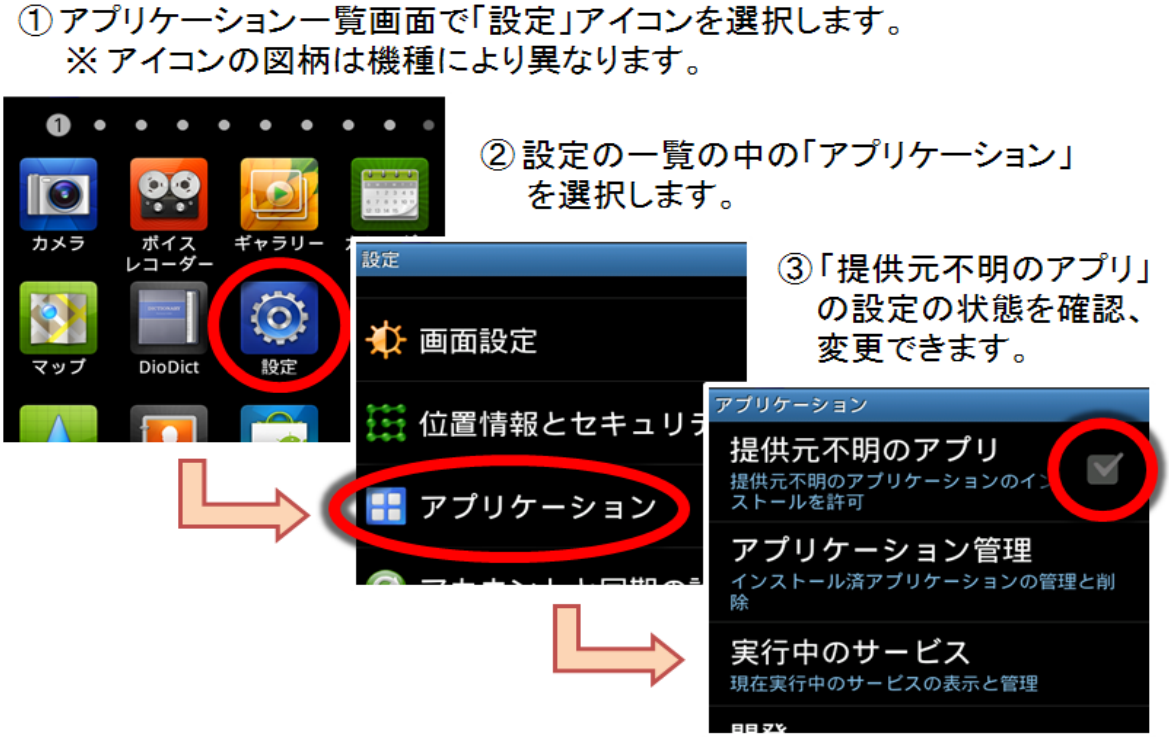


図1 「提供元不明のアプリ」設定の確認、変更方法(例)

操作を誤るなどして不正なアプリケーションをインストールしてしまわないよう、普段はこの項目のチェックを外した状態にしておくことをお勧めします。

なお、信頼できる第三者のアプリ・ストアであっても、正規の Android Market 以外で入手したアプリケーションをインストールする際は、一時的にこの設定を変更する

（チェックを入れる）必要があります。どうしてもインストールする必要がある場合は、インストール終了後、再度チェックを外すことを忘れないでください。

Android 端末では、アプリをインストールする際にアクセス許可を確認する

Android 端末の場合、アプリをインストールする際に表示される「アクセス許可」（アプリが Android 端末のどの情報／機能にアクセスするか定義したもの）の一覧には必ず目を通してください（図2参照）。

過去発見された Android 端末を狙ったウイルスには、個人情報などを不正に盗み取るため、アプリの種類から考えると不自然なアクセス許可をユーザーに求めるものがありました。例としては、壁紙アプリにも関わらず、アドレス帳の内容や通話履歴の記録へアクセスするための「連絡先データを読み取り」の許可を求めるなどといったものがあります。

Android 端末にアプリをインストールする際に、不自然なアクセス許可や疑問に思うアクセス許可を求められた場合には、そのアプリのインストールを中止してください。

図2「アクセス許可」の表示画面（例）

なお、アプリケーションの中には、広告の表示などのために、本来のアプリケーションの機能とは関係がなさそうな「アクセス許可」を求めるものがあります。「アク

セス許可」について代表的なものや、意味が分かりにくいものを、表 1 に示します。

表 1「アクセス許可」の説明（一部）

	「アクセス許可」の表示	説明
①	電話発信 →電話の状態を読み取る	電話の着信状況に応じて再生中の音楽を停止するといった用途に使われていると考えられます。 この許可が与えられたアプリケーションは、スマートフォンの**電話番号、機器ごとに付けられている端末識別番号**といった情報を読み取ることもできます。
②	あなたの場所 →粗い（ネットワークベース）場所	「粗い場所」というのは、携帯電話の基地局や、周囲にある無線 LAN の設備から推測できる位置情報を意味しており、およそ数十 m から数 km 程度の誤差の範囲で**スマートフォンの位置情報**を得られます。 この位置情報は、アプリケーションの画面に表示する広告の内容を決めるために使われることがあります。
③	ネットワーク通信 →完全インターネットアクセス	文字通り、インターネットへのアクセスにより情報を送受信するという機能です。広告に関するデータのやりとりにも使われます。

※「アクセス許可」の表示内容（表現）は機種により若干異なる場合があります

スマートフォンのアプリは、インターネットとの通信ができてはじめて役に立つものが多いのですが、例えば上記の表の①や②、あるいは「あなたの個人情報」といった項目と合わせて表の③の許可を求められた場合は、インターネットを通じて、電話番号やスマートフォンの位置の情報が何処かへ送信されてしまう可能性があるということになります。

「アクセス許可」の一覧だけでは、それが正当な目的のみに使用されるのか、不正なアプリなのかを判断するのが難しい場合があります。**アプリの入手元や開発元の信頼性、他の利用者の評判などを参考にしつつ、万が一を考慮し、妥当と思われる範囲で「アクセス許可」を確認してください。**

アプリは常に最新の状態で利用する(自動アップデートする)

アプリ・ストアなどからインストールしたアプリの場合は、一般的にアプリの自動更新ができる仕様になっています。

アプリに脆弱性がある場合は、前述の OS の脆弱性と同様に、それらの脆弱性が悪用され、ウイルスに感染したり、情報が盗み出されたりするなどの不正アクセスを受ける危険性があります。

対策としては、アプリに脆弱性が見つかった場合などに、**アプリを自動更新する許可**を与えておけば、アプリを常に最新の状態で利用することができます。この設定をお勧めします。

何らかの事情で、自動更新できない場合は、アプリに脆弱性が見つかっているか(更新情報が公開されているか)を常に意識し、必要に応じて自ら更新を実施するようにしてください。

もうひとつ、ウイルスに感染しないようにする大事な対策があります。

セキュリティソフト(アプリ)を利用する

パソコンの場合もそうですが、ウイルス対策は専用の対策ソフト(アプリ)を利用するのがお勧めです。

スマートフォンが国内で流行し出した当時は、まだセキュリティ対策ソフトのベンダーからは、スマートフォン用の対策アプリは提供されていませんでした。ウイルスもそれほど見つかっていなかったこともありますが・・・

しかしながら、昨今ではスマートフォンに対応したウイルスが増加傾向にあるため、ベンダー各社も挙(こぞ)って、スマートフォン用のセキュリティ対策ソフトを発表しています(詳細はベンダー各社の製品紹介を参照してください)。

これらのセキュリティソフトは、パソコンで培った技術を利用して、スマートフォンでも高度な対策ができるようです。それゆえ、これらのセキュリティソフトは、ウイルス対策だけでなく、それ以外のセキュリティ機能を持っている場合が多いので、スマートフォンの機種毎に対応状況を確認の上、利用することをお勧めします。

3. スマートフォンの情報漏えい対策

前述の盗難･紛失に備えたセキュリティ対策やスマートフォンの自己防衛対策以外にも、スマートフォンで考慮すべきセキュリティ対策があります。それは、スマートフォンを利用する上での情報漏えい対策です。

複数の人で共同利用しない

（個人利用ではあまりないと思いますが…）スマートフォンに重要な個人情報などが格納されている場合は、デバイスの共同利用は避けたほうが無難です。利用者ごとに管理･運用できない以上、他の人がどんなアプリを利用するかもわかりませんので、場合によっては情報漏えいする危険性があります。これは、外部記憶媒体の貸し借りが危険であることと同じ理由となります。削除したつもりの情報が復元されたり、記録したことを忘れた情報が残っていたりする場合は、情報漏えいが起きる危険性が存在するといえます。

重要な情報を通信する場合は、安全な回線を利用する

スマートフォンは、インターネットなどの外部に接続するためにいろいろな接続方法を持っています。携帯電話の回線を利用する方法、街中などの無線 LAN スポット（Wi-Fi 環境）を利用する方法などがありますが、携帯電話の回線以外では、安全な通信が確保できるかどうかは不明です。重要な情報を受け渡すような通信を行う場合は、安全な回線を利用するようにしてください。不特定多数の利用者がいる(無償の)Wi-Fi 環境では、盗聴の危険性があるようです。

企業での業務活動に利用する場合は企業で定めたセキュリティ･ポリシーにあわせて利用する(無断使用は厳禁)

スマートフォンを企業の業務活動に利用する場合は、業務に利用する以外のアプリケーションに注意が必要です。ウイルスはともかくとして、SNSサービスや SMS サービスを利用する際に、誤って企業の重要情報を漏えいさせる危険もあります。

業務活動で利用するのであれば、こういった過失による情報漏えいを防止する

ためには、業務活動で利用する以外のアプリを制限する必要があるでしょう。

さらに、紛失や盗難対策となりますが、スマートフォン上にどんな情報が格納されているのかを常に把握できる管理・運用体制が必要になります。

こういった事情から、現状では*10、私用のスマートフォンなどは、勝手に業務活動に利用しないことをお勧めします。

*10) 現状では…

最近、米国において「高度な仮想化技術を使えば、私物の PC を持ち込んで業務システムに接続し利用しても、セキュリティを確保できる」といった、Bring-Your-Own-PC と呼ばれるビジネスモデルが出現しているようです。近い将来、こういった技術背景から、私物のデバイスを利用してもセキュリティが維持できる環境になる可能性もありそうです。しかし、現状ではマネジメント(管理・運用)の面から、前述の通り、危険といえます。

4. その他の対策

ウイルス対策とは違いますが…

携帯電話が盛んに使われ始めたころのトラブルに未成年のダイヤル Q2 による高額請求問題、パソコンやオンライン端末でのオンラインゲームでのアイテム購入などにまつわる高額請求問題、さらにはワンクリック請求問題やフィッシングによる個人情報漏えい問題など、事前の対策ではいかんともしがたい問題がスマートフォンでも発生する可能性があります。こういった問題の対策は、利用者の意識付け(説明はよく読む、理解できないなら興味本位で先に進まない、自分ひとりで解決しようとしない等)しかありません。特に未成年の利用者には、そういった意識付けの教育が必要となるでしょう。また、携帯電話で実施されるような Web フィルタリングなどの必要性も出てくるかもしれません。

世間で発生したいろいろなトラブルに耳を傾け、利用者それぞれがトラブルから身を守る術を身につけなければならないと思います。

＜参考情報＞

くらしの豆知識（国民生活センター）

http://www.kokusen.go.jp/book/data/mame.html

5. まとめ

現在、広く普及したパソコンを標的にして作成されるウイルスは、何年もかけて巧妙化・悪質化が進んできました。そこで発生した様々な手口は、そのままスマートフォンへ応用される可能性が高く、場合によっては急激に危険な状態となりえます。

スマートフォンの利用者は、パソコンと同様、まず利用している機種にどのようなOS が搭載されているのかを認識してください。そして、必要なウイルスなどへの予防策を実施し、セキュリティ関連のニュース等にも注意を払いながら、安全に使用するよう心掛けてください。

- ☑ **盗難・紛失対策として、パスワード等によるデバイスロックが効果的、できない場合はリモートからロックする方法を覚えておこう**
- ☑ **重要な情報を保存するならば、データの暗号化が必要**
- ☑ **重要な情報はバックアップする**
  ただし、バックアップ媒体のセキュリティ対策も忘れずに…
- ☑ **スマートフォンの OS は常に最新の状態にアップデートする**
- ☑ **アプリは信頼できる場所からインストールする**
- ☑ **Android 端末では、「提供元不明のアプリ」はインストールしない設定にしておく**
- ☑ **Android 端末では、アプリをインストールする際にアクセス許可を確認する**
- ☑ **アプリは常に最新の状態で利用する(アップデートする)**
- ☑ **セキュリティソフトを利用する**
- ☑ **重要な情報を通信する場合は、安全な回線を利用する**
- ☑ **企業での業務活動に利用する場合は企業で定めた**
  セキュリティ・ポリシーにあわせて利用する(無断使用は厳禁)

6. 参考情報

＜セキュリティ・ベンダーの情報＞

- スマートフォンセキュリティ 脅威の増加と利用時の留意事項 10 カ条（アンラボ）
  http://www.ahnlab.co.jp/securityinfo/blog.asp?blog_view=view&board_gu=%20&top_gu=&sub_gu=&movePage=&searchWord=&seq=24
- スマートフォンにもセキュリティを［AKB48 カスペルスキー研究所スマートフォン対策室］（Kaspersky Labs Japan）
  http://www.androidsecurity.jp/
- モバイルデバイスのセキュリティに関する現状（シマンテック）
  http://www.symantec.com/connect/blogs-201
- Android 用マルウェア、日本語版アプリにも混入（シマンテック）
  http://communityjp.norton.com/t5/blogs/blogarticlepage/blog-id/npbj/article-id/68
- あなたのケイタイは大丈夫？携帯電話、スマートフォンのセキュリティ対策（トレンドマイクロ）
  http://is702.jp/special/888/
- 最新版 スマートフォンのセキュリティ対策（トレンドマイクロ）
  http://is702.jp/special/991/
- スマートフォンを守るための 5 つのヒント（マカフィー）
  http://www.mcafee.com/japan/security/mcafee_labs/blog/content.asp?id=1211
- 通話内容を記録する最新の Android マルウェア：1 年間の進化の軌跡（マカフィー）
  http://www.mcafee.com/japan/security/mcafee_labs/blog/content.asp?id=1278

本しおりを作成発行するにあたり以下の企業の協力を得ています。
（社名五十音順）

●株式会社アンラボ
http://www.ahnlab.co.jp/
●株式会社 Kaspersky Labs Japan
http://www.kaspersky.co.jp/
●株式会社シマンテック
http://www.symantec.com/ja/jp/
●株式会社ソースネクスト
http://www.sourcenext.com/
●トレンドマイクロ株式会社
http://jp.trendmicro.com/jp/home/
●マイクロソフト株式会社
http://www.microsoft.com/ja/jp/
●マカフィー株式会社
http://www.mcafee.com/japan/

＜IPA テクニカルウォッチ＞

- 『スマートフォンへの脅威と対策』に関するレポート
  ～IPA 自らの検査に基づくアンドロイド端末における
  脆弱（ぜいじゃく）性対策の実情と課題の考察～（2011 年 6 月）
  http://www.ipa.go.jp/about/technicalwatch/20110622.html

＜今月の呼びかけ：コンピュータウイルス・不正アクセスの届出状況＞

- スマートフォンを安全に使おう！（2011 年 8 月）
  http://www.ipa.go.jp/security/txt/2011/08outline.html
- スマートフォンのウイルスに注意！（2011 年 2 月）
  http://www.ipa.go.jp/security/txt/2011/02outline.html

＜楽天ブログ：IPA 情報セキュリティブログ＞

- また登場、Android に感染するウイルス（2011 年 2 月）
  http://plaza.rakuten.co.jp/ipablog/diary/201102220000/
- Android に感染するウイルスに注意！（2011 年 2 月）
  http://plaza.rakuten.co.jp/ipablog/diary/201102220000/

＜IPA Channel（YouTube）＞

- 情報セキュリティ通信 #1 Android に感染するウイルスに注意！
  http://www.youtube.com/watch?v=A-xIqfbZ_N0

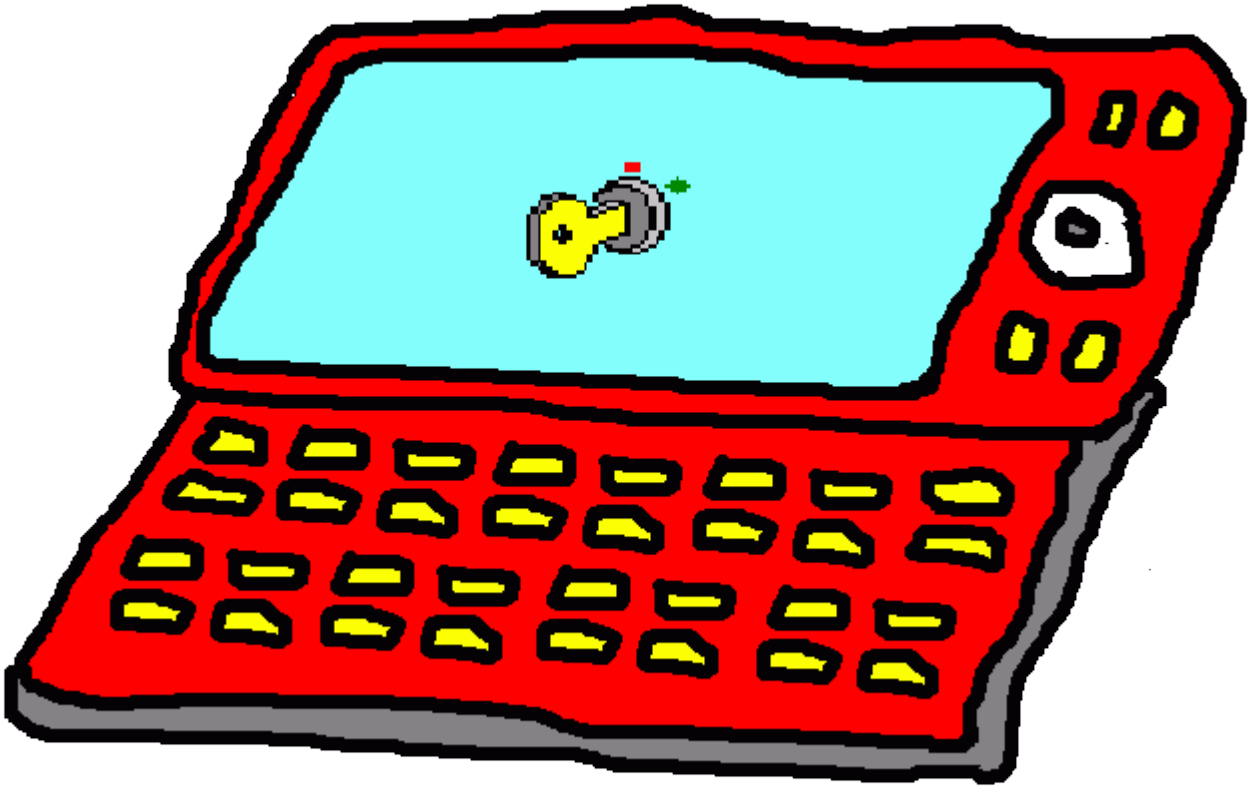
＜IPA 注意喚起＞

- Android OS を標的としたウイルスに関する注意喚起（2011 年 1 月）
  http://www.ipa.go.jp/security/topics/alert20110121.html

IPA 対策のしおり シリーズ

http://www.ipa.go.jp/security/antivirus/shiori.html

- IPA 対策のしおり シリーズ(1) ウイルス対策のしおり
- IPA 対策のしおり シリーズ(2) スパイウェア対策のしおり
- IPA 対策のしおり シリーズ(3) ボット対策のしおり
- IPA 対策のしおり シリーズ(4) 不正アクセス対策のしおり
- IPA 対策のしおり シリーズ(5) 情報漏えい対策のしおり
- IPA 対策のしおり シリーズ(6) インターネット利用時の危険対策のしおり
- IPA 対策のしおり シリーズ(7) 電子メール利用時の危険対策のしおり
- IPA 対策のしおり シリーズ(8) スマートフォンのセキュリティ 対策のしおり
- IPA 対策のしおり シリーズ(9) 初めての情報セキュリティ 対策のしおり
- IPA 対策のしおり シリーズ(10) 標的型攻撃メール対策のしおり



IPA 独立行政法人情報処理推進機構
セキュリティセンター

〒113-6591 東京都文京区本駒込2丁目28番8号
（文京グリーンコートセンターオフィス16階）
URL http://www.ipa.go.jp/security/

【情報セキュリティ安心相談窓口】
URL http://www.ipa.go.jp/security/anshin/
E-mail anshin@ipa.go.jp