

スマートフォンの日々

目代純平

4 ケータイ料金・アプリの出費

smart life
with
smartphone

不正アプリに嚴重注意を さまざまに「手口」で襲う

梅雨が明けたら猛暑の到来です。年度始めの予想では今年も冷夏になる、というようなことも聞いていましたが実際には例年通りというか、例年以上の暑さで外に出るのもおっくうでしたが、読者のみなさま体調など崩されていますか。そろそろ夏の疲れが出てくる頃かと思えますのでどうぞあまり無理をなさらないで下さい。

通話は定額時代に 逆に通信が使用量

前回、docomoが始めた「カケホーダイ」という日本国内ならどこにかけても通話料が定額制のサービスをご紹介しましたが、その他のケータイ各社も同様の定額制プランを打ち出してきました。テレビなどでしきりに宣伝をしています。

ソフトバンクは「スマ放題」、docomoは「カケホとデジラ」という名称のようですが、基本的な料金体系

系や仕組みはほとんど一緒で、月額二千円台の定額通話料にプラスして1か月に使うデータ量に合わせその分のデータ通信料を支払う、といったイメージです。

今までの料金体系だと、通話料は時間に応じて計算されていて、データ通信に関しては定額プランに入っていればどれだけ通信をしても定額で収まりましたが、その仕組みがちょうど逆になったような感じでした。使用するデータに関しては、1か月間にどのぐらいの量のデータをやりとりするかによって、最適な容量の契約をします。

例えばデータ定額2GBという契約をした場合、1か月に2GBまでのデータをインターネットでやり取りできます。データ容量はメールなどのいわゆるテキストデータだと小さいですが、写真や動画となると非常に大きくなってきます。

超過で速度ダウン 2GBで十分だが

そのため、「ほとんどメールしか使わないよ!」という方は最小単位の2GBで十分だと思いますが、日々動画を見たり、画像の送受信を頻繁にしたりする方はそれを超

過してしまいます。超過した場合もいきなり通信ができなくなったりはしませんが、超過した日からその月末までの通信速度を128kbpsに制限されてしまいます。

この128kbpsというのはインターネットをかなり昔から使っている私たちにとっては、当時は非常に高速に感じましたが、動画や大容量のデータをやり取りすることが普通になった現代ではあまりにも遅く、メールの送受信や文章がメインのサイトを見るぐらいはできますが、動画を見るのは難しいレベルです。

月内に契約した容量を超過して、速度を制限されてしまった場合は次の月になれば制限は解除されますので、そのまま月末まで我慢して128kbpsのまま使い続けるか、

著者略歴 ● もくだいじゅんぺい

1976年10月28日生まれ、東京都出身。大学4年在学中にチェックフィールド株式会社（現在代表取締役）を興す。中小・中堅規模法人向けのIT運用コンサルティング、運用管理代行を中心に行う傍ら、「安全なケータイ・インターネットの使い方」をメインテーマに講演活動。著書に「子どものための『ケータイ』ルールブック（総合法令出版：2012年）」。
東京都認定eメディアリーダー

耐えられない場合は追加の料金を払ってさらに1GB分を購入、など追加容量を購入するしかありません。

追加で購入した場合、追加した場合は割高になりますから、自分が大体毎月どのぐらいのデータ容量を使用するのかを把握しておき、適切なプランで契約をすることが大事です。各社の契約にはいくつか種類がありますが、超過した場合、自動的に次の上限のプランに切り替わるものもあります。

● Wi-Fiの仕組み 大容量のとき有効

なお、この通信容量はあくまでも電話会社の回線を使ったときだけしか計上されないので、Wi-Fiを使った通信は含まれません。ですから、自宅や会社などの通常のインターネット回線が使える場所でWi-Fiがある場所ではそちらに切り替えて使ったり、容量の大きいファイルや動画をダウンロードする時はWi-Fiに限って使うなど



docomo Wi-Fi ステッカー



ソフトバンク Wi-Fiスポット ステッカー



au Wi-Fiスポット ステッカー

すれば、かなり節約することができます。

ちなみに、私はWi-Fiのつながる場所ではなるべくそちらを使いますし、スマートフォンやタブレットで移動中に大容量の動画を見るときはWi-Fiを使うので、外出先でPCをインターネットにつなぐ際に電話会社の回線を経由してつなぐこと（テザリング）をしても、今のところ毎月3GBを超えたことはありません。

最近ほぼ無料に

各電話会社は近年、通常の電話回線のほかに公衆Wi-Fiといわれる回線を用意しています。これは提供会社によって名称が異なりますが、主に回線の契約者に向けて提供しているものです。元々月額数百円で提供していたようですが、最近ではほとんどの契約プランでは

無料で使えるようです。

Wi-Fiの電波を利用するので、使用できる範囲は数百メートル以内でしかありませんが、そのエリアは主要な駅や空港、喫茶店、ファーストフード店、ファミリーレストラン、コンビニエンスストアなどに広がっています。それらが使える店には下記のようなステッカーが貼ってあることが多いので、自分が契約している電話会社のステッカーがあれば基本的には使用できるはずです。

難しい初期設定

前項に「基本的には使用できるはず」と書いたのには理由があります。まずは初期設定が必要になるのですが、それが少々複雑なのです。下記の各社Wi-Fiサイトを参照して初期設定を行います。その際に機種によって設定が異なる

ることがあるので、自分が使っている機種の設定方法に従って行う必要があります。

また、接続の際に必要なWi-Fiのパスワードを表示するのに契約時に設定した契約IDとパスワードが必要な場合がありますので、あらかじめ用意しておくスムーズです。Wi-FiのIDとパスワードが分かればあとは接続するだけなのですが、スマートフォンの場合には各社共に簡単に接続のできるアプリがありますのでそれを使うとよりスムーズに接続ができて便利です。

電波飛び交う店 繋がらない覚悟

昨今のもう一つの困りごととして、これらの初期設定が問題なくできて、スマートフォンの上部にWi-Fiの無線表示が出ているにもかかわらず、うまくインターネット接続ができないということがあります。これは特に全ての電話会社のWi-Fiに対応している店などでよく起こりますが、各社が同じ周波数帯の電波を使っているため、それらが相互干渉してつながりにくくなるためです。

最近ではほとんどのノートパソコン

コンやスマートフォンにWi-Fiが搭載されていますし、その分ユーザーがとも増えています。同時にWi-Fiの利用者自体も爆発的に増えましたので手元のスマートフォンにWi-Fiをオンにするとおびただしい数のアンテナ表示が見えると思います。電波の強弱はありますが、それだけのアンテナから電波が出ているので、自分の機器と通信していなくても他の機器同士が通信をしている電波が飛び交

っているのです。

各社の公衆Wi-Fiサイト
docomo
https://www.nttdocomo.co.jp/service/data/docomo_wifi/
Softbank
<http://www.softbank.jp/mobile/service/wi-fi/use/>
au
<http://www.au.kddi.com/mobile/service/smartphone/wifi/>

これらのはお店に限ったことではありません。密集した住宅街やマンションなどでも同様なことが起きていますが、お店などの場合は狭い面積の中でたくさんの電波が飛び交っているので余計につながりにくくなってくるのです。この問題に関しては電話会社な

ども把握しているはずですが、公衆無線LANはあくまでも「サービスの一環」として設置している背景があり、かつ世界的な通信規格をすぐに変えるわけにもいかないもので、しばらくはこのままの状態が続くと思われれます。せっかくなWi-Fiが使える！と思ったのにもかかわらず接続ができない場合は、Wi-Fiを切って通常の電話回線を使ってネットに接続するのが無難ですが、これでは従量課金の対象になるのであまり意味がありません。

危ない「PWなし」情報が盗まれる

さて、上記の公衆Wi-Fiも含めた無線LANに接続するには原則としてパスワードが必要です。それらのパスワードで部外者が接続することを防ぐと同時に無線での通信内容を暗号化しているからです。

そのため、家や会社のWi-Fiに接続する際にもパスワードを求められると思います。たまに飲食店や住宅地などでパスワードを入力しなくても接続できるアンテナを発見することがありますが（野良無線、野良Wi-Fiなどと呼ばれま

す）、それらには決して接続しないことです。

外にいるときに高速なネットワークに接続したくなり、ついにつないでしまうと、無線通信が暗号化されないで通信内容が盗聴される危険性があるほか、悪意を持った第三者がそのアンテナを設置していた場合は、その先のネットワークでも通信内容が傍受され、個人情報やパスワードなどが盗まれる可能性があるからです。

前述の電話会社が提供している公衆Wi-Fi以外でもホテルや飲食店などが独自のWi-Fiを提供していることがあります。それらを使用する際もパスワードがかかっているか確認してから使うようにして下さい。パスワードがかかっていれば、概ね安全に使用することができま

複雑な料金プラン ショッピングのり

ここまで携帯電話の料金体系の変化やそれに伴うWi-Fiとの関係などを書いてきましたが、最近ではSkypeやLINE、楽天でんわなどのインターネットを使った無料通話アプリが急増していて、どこに

かけても通話料は無料というのが主流になってきましたので、このように料金体系が逆転したのだと思います。これから契約を変更する際はライフスタイルによってどの契約をすれば一番自分に合ってお得になるのかを考えて行う必要

●アプリのさまざま

前回はパチンコ業界とスマートフォン、というテーマで様々なメーカーが提供しているコンテンツを中心に紹介しました。各社共に特に実機のシミュレーションには力を入れていて、実機と同じ動きをするアプリが次々とリリースされています。今回からはそれらを含めたスマートフォンの「アプリ」について改めてご紹介していきたいと思えます。

タップ一つで簡単に

「アプリ」という言葉が流行りだしたのもつい最近のことです、スマートフォンが台頭と共によく使われるようになってきました。これは「アプリケーションソフト」の略で、これまではよく「ソフト」と略されていたと思いますが、意味は同じです。PCやスマートフォ

があります。ただ、依然として料金プランはいろいろあって複雑なので最適な料金プランの相談は携帯電話会社のショッップでするのが一番いいと思います。時間があるときに立ち寄って見直してみるところをお勧めします。

ンなどの機械（ハード）に対するもので、それらの上に導入（インストール）して様々な応用機能（アプリケーション）を提供するものを指しています。

一昔前、PCのソフトはCD-ROMやそのまた昔はフロッピーディスクなどで提供され、それらをPCにインストールして使っていました。最近では直接インターネットからダウンロードしてインストールするのが主流です。特にスマートフォンは常にインターネットにつながっていますので、好きなアプリを見つけたらタップ一つで簡単にダウンロードできてしまいます。スマートフォンもPCと同様、OSという基本ソフトの上でいろいろなアプリを起動させて様々な機能を使用します。買ってすぐの状態では、あらかじめ導入されている

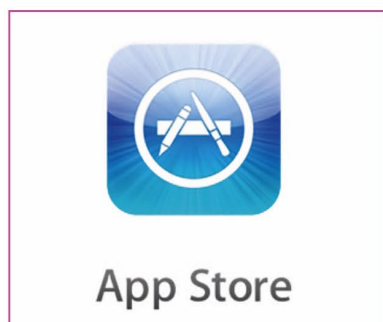
（プリインストール）いくつかのアプリしか入っていませんが、自分で好みのアプリをダウンロードしてインストールすれば自分仕様のスマートフォンを作り上げていくことができます。

公式アプリは安全 確認作業は必要

PCやWindows用、Mac用にそれぞれ別のソフトがあるように、スマートフォンでもAndroid用、iPhone用は基本的に別のアプリを使用します。ただ、アプリはそれぞれ機種で使えるように2種類用意されていることが多いので、自分が使っている機種用のアプリを探してダウンロードします。

原則として「Android」は「Google play」「iPhone」は「App Store」という場所からダウンロードするようになっていて、それらの入口は最初からスマートフォン上のアイコンに用意されています。

これらのダウンロードサイトはそれぞれメーカーの公式なもので



「Google Play」「App Store」それぞれのアイコン

す。ここからダウンロードするアプリに関しては「一応」メーカーの審査を通っていることになっていますので、ウイルスの混入や不正ソフトである可能性は低いとされています。

ただ、過去にはこれらのサイトからダウンロードしたアプリにもウイルスが入っていたり、個人情報報を抜き取る不正ソフトだったことが判明した事例もありますので、ダウンロードする場合はこれらのサイトにあるアプリの「評価」やその他インターネット上の評判を確認した上で行うことをお勧めします。

公式以外は厳禁

たまにこれらの公式サイト以外からスマートフォン用のアプリを配布しているケースがありますが、

これらは完全にノーチェックです
ので基本的にはインストールしな
い方が無難です。

Android・iPhoneともに基本
の設定では上記公式サイト以外か
らのインストールに関しては警告
を発するようになっていたので、
ユーザーが気づかずにインストー
ルしてしまうことはないはずで
すが、最近ではこれらの公式サイト
にデザインを非常に似せた偽ダウ
ンロードサイトもあるようですの
で注意して下さい。警告が出た場
合はそれ以上進まないことが重要
です。

アプリの種類

120万を超えた

Android／iPhoneともに公式
サイトからダウンロードできるア
プリの数は120万を超えたそう
です。公式サイト上でダウンロー
ドができるものでも地図や決済サ
ービス、通話、辞書、スケジュー
ラーなどのビジネスに役立つもの
から、写真の加工や音楽、SNS、
壁紙、アイコン、料理、旅行など
の趣味で使えるもの、そしてゲー
ムまで実にたくさん種類があり
ます。

使用する言語の対応やAndroid

では機種ごとの対応／非対応もあ
るので、実際に使えるアプリの数
はもう少し減ってくると思います
が、それでもとんでもない数です。
この中から自分の使いたいものを
探すのも一苦労ですが、PCと同
様、スマートフォンでも内部の記
憶容量に限りがありますので、イ
ンストールできるアプリの数にも
上限があります。

吟味して選ぶほう

アプリの中には起動しなくても
裏で勝手に起動して動き続けてい
るものもあるので、あまりたくさ
んのアプリをインストールしてい
ると、それらが内部のメモリー
(動作領域)も占領してしまい、
スマートフォン全体の動きが遅く
なるうえ、電池の消耗も激しくな
りますし、通信をするようなアプ
リですと月極の通信容量も使って
しまう可能性があります。

このような理由から、使いたい
アプリ全てではなく、必要なもの
を吟味してインストールすること
が重要です。あるいは、インスト
ールしてみても使わないようならア
ンインストール(消去)すること

も「まめに」行ってみてください。

有料アプリ

買いきすぎの傾向

これらのアプリは大きく分けて
無料のものとう料のものがありま
す。ダウンロードサイトにその金
額が明記されていますので、イン
ストールするかどうかの判断材料
になります。無料のものはそのま
ま「インストール」というボタン
をタッチすればすぐにインストー
ルされます(パスワードの入力を
求められることがあります)。

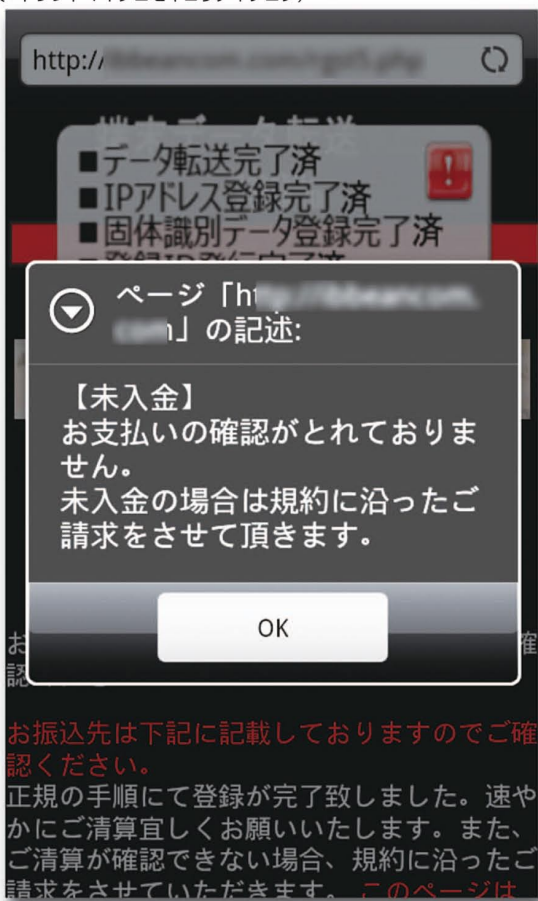
では、有料のものはどのように
支払えばいいのでしょうか。一番
簡単な方法はクレジットカードの
番号をGoogle playやApp Store

にあらかじめ登録しておくこと
です。そうしておけば、有料アプリ
でもタッチ一つで購入・ダウンロ
ードが可能です。ついつい買い
すぎてしまいそうで危ないです。

LINEの詐欺注意

その他の方法としては、ほとん
どのキャリアでは「電話代と一緒
に後で支払う」ことができますが、
これも後払いのため使いすぎの心
配があります。そのような方には
プリペイドカードがおすすです。
これはコンビニ等で販売されてい
るカードをあらかじめ購入してお
き、その裏に書いてあるコード番
号を入力することでその購入した
金額分使用できるというものです。

(出典：トレンドマイクロセキュリティブログ)



最近コンビニに行くとき様々な会社のプリペイドカードがあります。これらは最近流行っている「LINEのアカウント乗っ取り詐欺」でよく使われています。

これはLINEのアカウントが悪意のある者に乗っ取られて、その友人に「コンビニに行ってWebマネーを買ってきて下さい」と依頼し、「買ったら裏の番号を写真に撮って送って下さい」と言ってくるものです。

これらは裏に隠されているコード番号(コインなどで削ると出てきます)を人力すれば実際のお金と同様に使えるため、その金額分を搾取するという手口です。既に同様の手口が広まってきて、LINEの提供会社も対策を始めたため、被害は減っていきと思われませんが、手を変え品を変え次々と詐欺や妨害などが発生するのは近年の「〇〇」とってはとても頭が痛い問題です。

巧妙な仕掛け

iPhoneでも出現

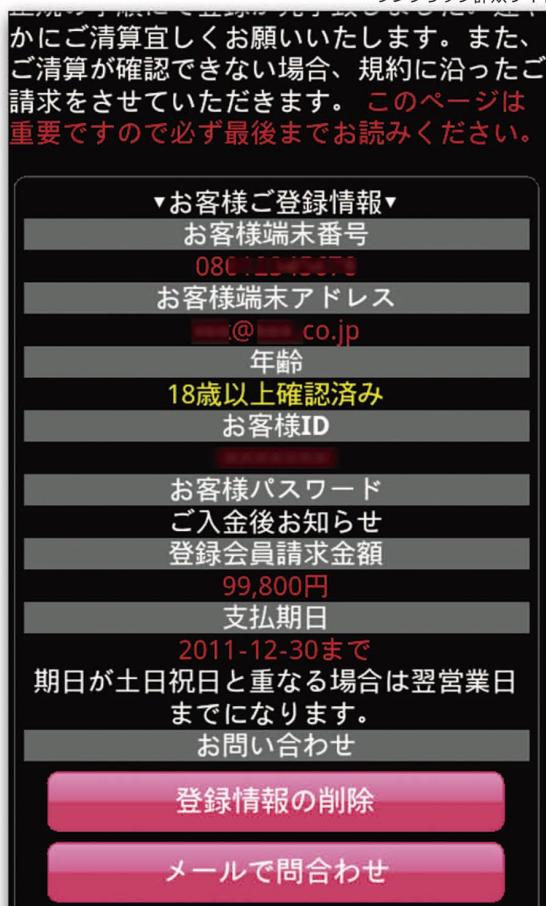
先ほど少し触れた、スマートフォン上の不正なアプリについて詳しくご紹介したいと思います。スマートフォンユーザーが増えるに従って、PCと同様に不正アプリの数も増えてきています。不正アプリの被害はAndroidの方が顕著で、iPhoneではほとんどないと言われてきましたが、ここにきてiPhoneユーザーをターゲットにした不正アプリやサイトも出現し始めているとのことで、同様に注意が必要です。

正規に見せかけ

これらの特徴としては、PCのそれらとほぼ同様で様々な悪事を働きます。ワンクリック詐欺と呼ばれる、実行すると「アダルトサイトの閲覧料金」と称して金銭の振り込みを要求され、その画面が数分に1回自動的に出現して消えないものがあります。

正規のアプリと見せかけて裏で電話帳のデータや画像データ、その他スマートフォン内に保存されているIDやパスワードなどの個人情報勝手に抜き取り、第三者のサーバに送信して盗んだりします。そして「ウイルスに感染した」というような偽のメッセージを出して、有料で偽ウイルス対策ソフトを買わせるもの、さらにもっと悪質なものでは、スマートフォン

ワンクリック詐欺サイト画像



を乗っ取って遠隔で操作することができるよう仕向けるものまであります。

セキュリティ

情報の質を大切に

これらは一度実行されてしまうと、多くの場合スマートフォン内に常駐して様々な悪事を働きますので、決して侵入されることが一番重要です。対策としては

- 何らかのセキュリティソフトを入れておく(電話会社と契約しているスマートフォンなら最初から何かしら入っているはず)。
- アプリを導入する前には必

ず評判を確かめて、怪しいアプリは入れない。

しかありません。PCのウイルス感染も厄介ですが、スマートフォンは電話でもあるため、電話帳やメールのデータ、写真データなどよりプライバシー性の高い情報が入っていて、万一流出や盗難に遭うと非常に大きな被害になることが多く、それらを狙った犯罪者にとっては垂涎的のです。

スマートフォンはいつも携帯しているのが無防備になりがちですが、パスワードの管理や盗難対策と同時にこれらの不正アプリに対する対策も同時に行い、安全に使うことが重要です。