2011.8.10

情報セキュリティニュース ＜2011 No.2＞

スマートフォンのセキュリティ

2011 年のスマートフォンの世界出荷数は 4 億 2,000 万台でパソコンを超える見通しとなっている。また、日本においても、2015 年にはスマートフォンの契約台数がフィーチャーフォン（注 1）を逆転し、6,000 万人を越える日本人がスマートフォンを所持すると言われている。一方、その最中で、スマートフォンを狙うコンピューターウイルス（悪質なプログラム）も次々と出現している。ウイルスの主な標的となっているのは、グーグルの OS「Android（アンドロイド)」を搭載したスマートフォンである。ウイルスが埋め込まれたアプリケーションを実行すると、個人情報を盗まれたり、スマートフォンを遠隔から勝手に操作されたりするウイルス感染の報告が 2010 年 8 月以降から徐々に増え始めた。このようなスマートフォンにおけるウイルスは、パソコン向けウイルスと比べると現時点での確認例は少ないが、今後増えていく可能性は高い。本稿ではその危険性を認識するために、スマートフォンとそのセキュリティについて詳述する。

注 1：通話とショートメッセージサービスなど限定された機能を持つベーシック・フォンやシンプルフォンから進化し、インターネットに接続でき、アプリケーションが動作するほか、GPS、ワンセグ、デジタル・カメラでの静止画・動画の撮影、音楽再生機能などが追加された端末のこと。

1. スマートフォン市場規模の拡大

2011 年 3 月末の日本におけるスマートフォン契約数は 955 万件で、端末総契約数 1 億 912 万件に対するスマートフォン契約比率は 8.8%となった。さらに、2012 年 3 月末には 2,598 万件（23.1%）となり、その後 1 年ごとに平均 10%程度の成長率を見せ、2015 年 3 月末には 6,137 万件（50.9%）に達し、スマートフォン契約数がフィーチャーフォンを抜いて過半数を超えると予測されている（図 1)。特にアンドロイド OS を搭載したスマートフォンの市場普及成長率が高く、2011 年 3 月末の時点では、既に市場の 50%程度の普及率を見せる iOS（i-phone の OS）に迫るシェアの割合となり（図 2)、2011 年度以降のスマートフォン出荷台数に占める OS 別シェアにおいてはアンドロイドが 70%以上で推移すると予測されている。

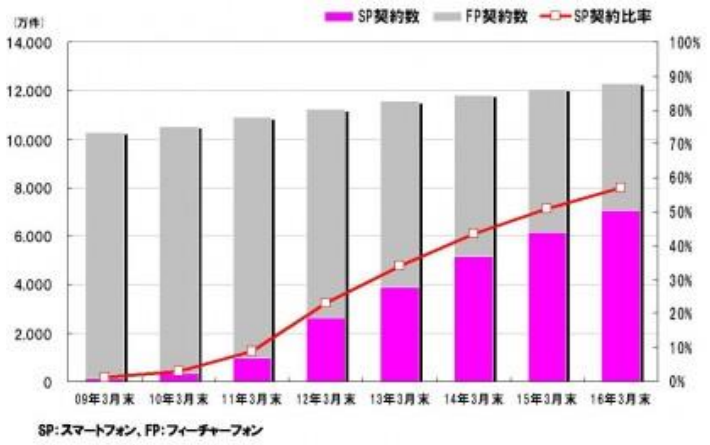

図 1. スマートフォン契約数・比率の推移・予測
（出典：MM総研）

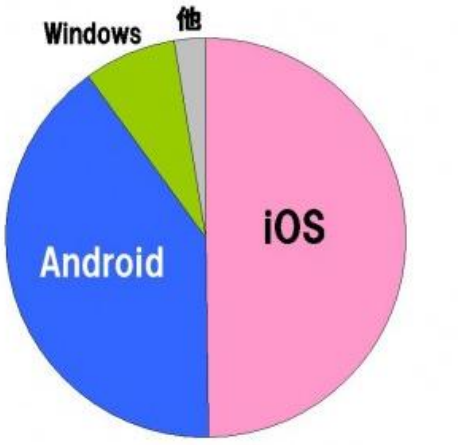

図 2. スマートフォンの OS 別契約数シェア
（11 年 3 月末）（出典：MM総研）

2. アンドロイド OS 搭載スマートフォンの危険性

アンドロイド OS を搭載したスマートフォンを狙ったウイルスは 2010 年 8 月に初めて見つかり、それ以降、次々と種類の異なるウイルスが発生したことが大手セキュリティソフト会社によって確認されている。2010 年 8 月から近年までに発見されたアンドロイド OS 用ウイルスの一覧を表 1 に示す。

表 1. アンドロイド OS を狙ったウイルスの種類

出現時期	名称	特徴	配布場所
2010年8月	FakePlayer	動画再生アプリに見せかける。有料のメッセージサービスを勝手に利用される。	非公式の配布サイト
2010年8月	Tap Snake	ゲームアプリに潜伏。機器の位置情報を取得し、特定のサーバーへ送信する。	Androidマーケット（現在は公開中止）
2010年12月	Geinimi	複数のゲームアプリに潜伏。機器を乗っ取り、攻撃者が操作できるようにする。	非公式の配布サイト
2011年3月	DroidDream	50種類以上のアプリに潜伏。機器を乗っ取り、攻撃者が操作できるようにする。	Androidマーケット（現在は公開中止）

（出典：日本経済新聞）

発見されたウイルスは、いずれもアンドロイド OS 搭載のスマートフォン上で起動するゲームや動画のアプリケーション内に潜入し、ユーザーが気づかないうちにプログラムを実行するよう、巧妙に仕組まれているものばかりである。また、その感染ルートは非公式の配布サイトからのアプリケーションのダウンロードによるウイルス感染だけではなく、公式のアンドロイドマーケットからダウンロードしたアプリケーションからもウイルスが検出されていることが特徴と言える。ユーザーから見ると、「公式サイト」からのダウンロードという認識が安心感を生むと考えられるが、アンドロイドマーケットは開発者が自由にアプリケーションを開発し、google による必要最低限の審査（アダルトや暴力、差別的な内容等を含まないこと）さえクリアすれば登録できてしまうため、アプリケーションのプログラムに対しての検閲が無いに等しいことに注意が必要である。

一方、同じスマートフォンでもアプリケーションを公式サイトに登録する際に米 Apple 社の審査が必要な i-phone においては、ある程度安全性が高いと言える。ただし、サイバー犯罪者はここにも既に抜け道を見つけつつあり、アンドロイド OS で最初のウイルスの見つかった時期と同じ、2010 年 8 月に、ウェブページを開いただけで勝手に i-phone のアプリケーションがインストールされるウイルスが発見されている。これは、i-phone の OS を狙った攻撃の準備段階として捉えることができ、今後大きなセキュリティ問題が発生する前に、ウイルスに対する対策を講じておくことが肝要であると考えられる。

3. ウイルスに感染しないための個人の留意点

近年増加してきたスマートフォンのウイルス攻撃に対して、個々人が日々の使用の中で気をつけるべき留意点は次のようなことである。

現在までのところ、スマートフォンに対するウイルスの攻撃は、ユーザーがダウンロードするアプリケーションに対してウイルスを潜ませ、不正に個人情報やクレジットカード情報を入手したり、端末を操作する方法に留まっている（図 3）。従って、ユーザー自身でアプリケーションについての信頼性を確認したり、ダウンロードやインストール時の挙動に注意を払うことで概ねウイルス感染を予防できると考えられる。

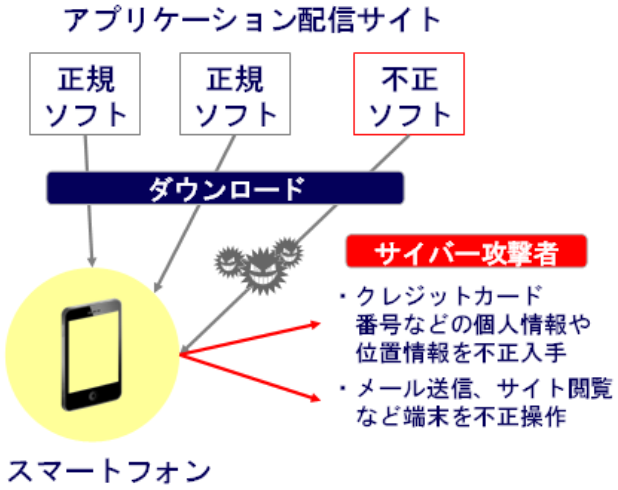

図 3. スマートフォンへのウイルス攻撃イメージ

① アプリケーションの配布元を確認する

表 1 より、2010 年に確認されたスマートフォンを狙った 2 種類のウイルス（FakePlayer, Jeinimi）はいずれも非公式のアプリケーション配布サイトからダウンロードされたアプリケーションより検出されている。公式サイト以外からのアプリケーションのダウンロードについては、google や Apple 等によるセキュリティ審査が全く行われていないため、公式サイトと比較してウイルス感染の危険性が高く、推奨できない。

② アプリケーションの開発元を確認する

アプリケーションの配布元が公式サイトだからと言って油断もできない。表 1 に示したウイルスの内､2010 年 8 月に確認された Tap Snake と 2011 年 3 月に確認された DroidDream については、Android 携帯のアプリケーション配布公式サイトである Android マーケットからダウンロードされたアプリケーションより確認されたものである。特に、DroidDream が仕込まれた違法コピーアプリケーションは 50 種類以上も確認されており、その中には、誰もが聞いたことのある有名なアプリケーションの違法コピーもあったことから、アプリケーションの名前のみで判断せず、開発元までしっかりと確認することが重要である。

※アプリケーションをダウンロードする際に、デベロッパー情報を必ず確認し、HP 等が公開されている場合はアクセスしてその信頼性を確認する。

③ アプリケーションのインストール時の「アクセス許可」を確認する

単純なゲームを楽しむためのアプリケーションにも関わらず、インストール時に個人情報を取得することの許可を求めてきたり、有料の通話やメールを送信する許可を求めてくるようなアプリケーションの場合、ウイルスの存在を疑うべきである。スマートフォンでは、アプリケーションのインストール時に、そのアプリケーションが行う動作項目を列挙する表示が必ずあるため、その時点で不審な項目があればインストールを中止した方が良い。

【アプリケーションのインストール時に求められる許可項目で注意すべき項目】

- (無料のゲームの場合) 料金の発生の許可を求める表示
- E メールや SMS（ショートメールサービス）の送受信許可を求める表示
- ユーザーの現在地情報を求める表示
- インターネットへのアクセス許可を求める表示
- ストレージ（SD カード内の情報）データの削除や修正を求める表示

4. スマートフォンのセキュリティソフト

パソコンと同じくスマートフォンにもウイルス対策（ウイルスを検出・駆除）ソフトが続々開発されてきている。スマートフォンを従業員に情報端末として配布している企業においては、このようなウイルス対策ソフトのインストールを、徹底させる必要がある。

以下、ウイルス対策ソフトメーカー大手各社が開発しているソフトの特徴を紹介する。

4-1. Android 端末用セキュリティソフト

- 『ALYac Android』

悪意のあるプログラム・コードやアプリケーションの精密スキャンと駆除・除去、そしてリアルタイム監視による危険なアプリの確認・通知、さらには定期的なウィルス・マルウェアのパターン・定義ファイルデータベースの更新もある。特徴は、**インターフェイスが日本語のアプリであることで操作・設定もわかりやすく、日本人スマートフォン・ユーザーに優しい**ウィルス対策アプリケーションであると言える。

- 『Norton Mobile Security』

平時に悪意ある脅威をもったアプリケーションからの防御を行ってくれることはもちろん、**リモートロック機能による個人情報のロック、GPS リモート検索機能、個人情報などの遠隔消去機能、SIM カードロックによる端末自動強制ロック機能等の機能も付いており、スマートフォン端末を紛失した場合の、遠隔操作によるセキュリティ防御機能も充実している。**

- 『Dr.Web for Android』

海外では「Dr.Web Mobile Security Suite」の名称で 100 万ダウンロードを超える実績があるスマートフォン用アンチウイルスソフトである。**直感的でわかりやすい操作法・インターフェース**と高度な防御機能により、個人・法人を問わず多くのユーザーが利用している。Android 携帯を使用するユーザーのもう一つの悩みである**バッテリー消費に関しても、パフォーマンスへの影響を最小限に抑えることで省エネを果たしている。ノンストップアンチウイルスと呼ばれる主要機能が付いており、メモリに保存してある全てのファイルをリアルタイムにスキャンし、悪意のあるプログラムからシステムを保護することが可能である。**

4-2. i-phone 用セキュリティソフト

- 『VirusBarrier X6』

パソコンに i-phone を接続した状態で、i-phone 内のマルウェアや悪意のあるファイルのスキャンが可能である。尚、常駐タイプのセキュリティソフトは i-phone では開発されていない。

Android 端末では、近年、ウイルスの確認事例が多発していることもあり、開発されているウイルス対策ソフトも多機能化されている。悪意のあるプログラムから端末を保護する機能はどのソフトも充実しているため、企業においては、それ以外の機能で自社におけるスマートフォンの使用目的と照らし合わせ、必要と思われる機能が付与されているソフトを選定することが肝要である。

一方、i-phone においては、i-phone の機種によってマルチタスク（注 2）を行えない機種があるという機能的な問題、i-phone でアプリケーションをダウンロードする公式サイトである Mac App Store では、厳正なアプリケーションのプログラム審査を行っており、不正なソフトに対する安全性は高いという観点から、現状、常駐型のウイルス対策ソフトはどのメーカーからも公開されていない。しかし、いつ何時、それらの審査を巧妙に潜り抜ける不正ソフトが現れないとも限らないので、i-phone を業務に利用している企業においては、そのセキュリティ

動向に注意を傾けておく必要がある。

注 2:同時に二つ以上のプログラムを実行すること。常駐型のウイルス対策ソフトを実行すると、その他のプログラムが実行できなくなる。

5. おわりに

2011 年 5 月 25 日に、「日本スマートフォンセキュリティフォーラム」が設立された。このフォーラムには、パソコン向けセキュリティソフトを手掛ける米シマンテックやトレンドマイクロ、通信機器のシスコシステムズなど内外 40 社を含む企業が参加している。さらには、スマートフォン向け OS を開発した google や Apple も参加を表明し、企業が安全にスマートフォンを利用するための方策を 2011 年 10 月までにまとめる方針となっている。しかし、サイバー犯罪者によるウイルス攻撃は年々巧妙化しており、これら団体が打ち出した方針や対策も絶対的に安全な策では無いと言うことを企業においては認識する必要がある。

パソコンよりも簡単に自社の重要なデータを持ち運びできるスマートフォンでは、むしろパソコンよりも高いレベルのセキュリティ対策を敷き、自社データを守ることが肝要である。

インターリスク総研 コンサルティング第二部　BCM 第二グループ
主任コンサルタント 橘田　生基 (キッタ　セイキ)