
スマートフォンの利点とリスク

2013年11月

株式会社アイ・シー・アイ



現代社会、iphoneやAndroidといったスマートフォンを持っている人が増えてきています。最近では会社携帯をスマートフォンに変更している企業もあります。



そんなスマートフォンについて
利点とリスクをご紹介したいと思います。

そもそもスマートフォンとはどんな携帯のことを言うのでしょうか。実はスマートフォンに統一した定義というものは現在のところありません。

一般的に言われているのはOS(オペレーティングシステム)を搭載した携帯のことです。

OSの種類としてはiOSとAndroidが主にあげられます。

スマートフォンの利点は、OSを搭載していることと携帯が容易であることがあげられます。

OSを搭載しているということは、PCと同様なアプリケーションを動作することや高描写のWebサイトを閲覧することができることです。ビジネスとしても、職場にいない時でも、社内メールを閲覧/送信することができるということです。

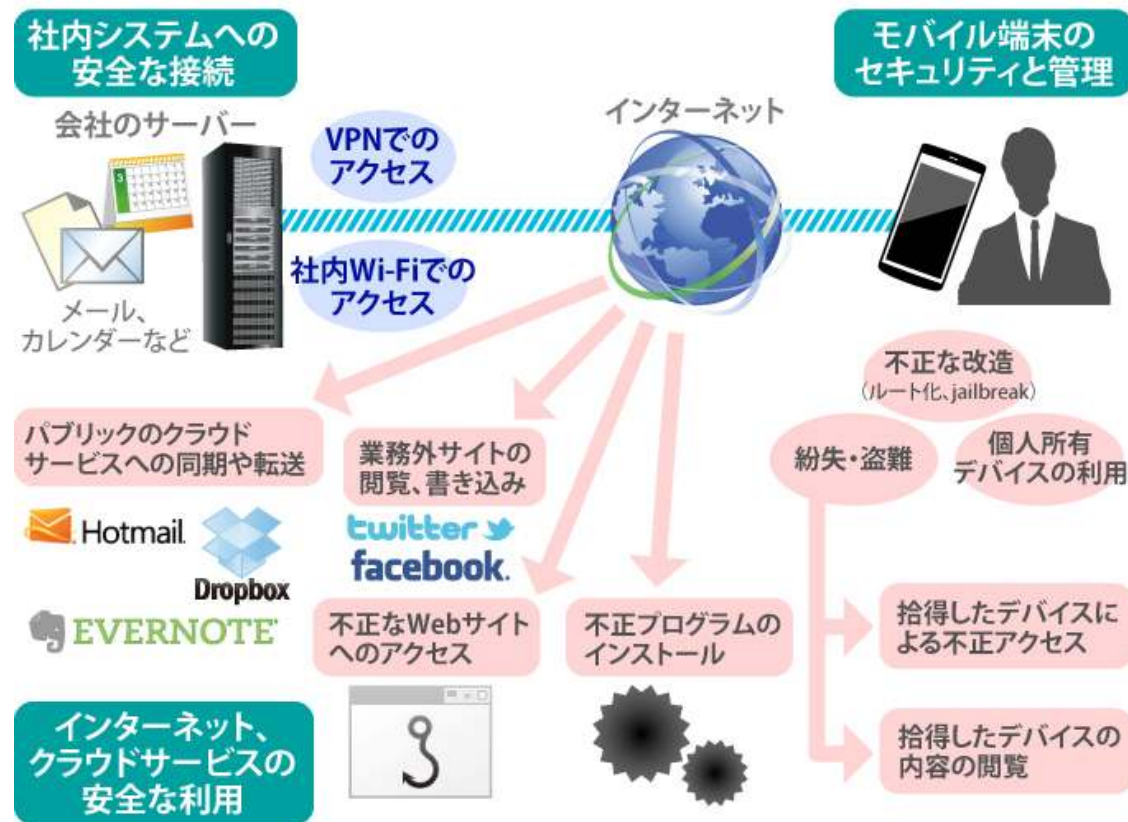
携帯が容易とは、スマートフォンは片手サイズなのでポケットに入れることができ、いつでも簡単に取り出すことができるということです。ふとした時に調べ物や急なメールの返事などがすぐに対応できるという利点もあります。

また、タッチパネル式で直感的な操作ができますので、不便に感じることはないでしょう。

スマートフォンのリスクは主に次の2つが挙げられます

1. 紛失・盗難
2. 不正プログラム・不正ウェブサイト

図1 スマートフォンの業務利用とそのリスク



出典

ソフトバンク

気になる最新セキュリティ事情・第2回「スマートフォンの業務利用に伴うインシデント」より

スマートフォンの利点として携帯が容易であることをあげましたが、それは同時に紛失や盗難の発覚が遅れやすいということです。

発覚に時間がかかると、場所の特定は難しくなり、盗難にあったスマートフォンから機密情報や不法侵入されてしまいます。

これらを防ぐためにはスマートフォンにネックストラップをつけたり、万が一失くしてしまっても、自動的にロックがかかる設定やデータを遠隔で消去できるようにするなどの対策が必要です。



PCと同様なアプリケーションの動作やWebサイトが閲覧できるということは、ウイルスの可能性もPCと同程度存在するといえます。

まず気を付けたいのが、アプリケーションのインストールです。スマートフォンのOSにはiOSとAndroidがあると紹介しましたが、OSの違いによってもセキュリティのリスクが違ってきます。

iOSについてはアプリケーションはApple社の審査がありますので、脅威としてはそれほどではありません。(全く危険がないわけではありません。)一方Androidでは個人サイトでのアプリケーションの配布が可能なので、知らないうちにウイルスに感染している可能性があります。

Webサイトの閲覧にも注意が必要で、フィッシング詐欺などにPCでは注意していても、スマートフォンでは警戒が甘くなると引っかかってしまいます。

考えられる対策としては、スマートフォン用のウイルス対策ソフトはもちろん、まず必要のないアプリケーションはインストールしないといったことが第一です。Webサイトの閲覧も本当に必要な情報だけを得るといったことが必要です。

スマートフォンは使いこなすと大変便利なツールですが、
使い方を一歩間違えてしまうと、脅威になってしまいます。

スマートフォンに限らず、IT技術などありとあらゆるものに共通することだと思えます。

利点とそれに伴うリスクをしっかりと理解し、スマートフォンを使用して頂ければ幸いです。



ソフトバンク「気になる最新セキュリティ事情」 スマートフォンの落とし穴、ウイルスや紛失対策を解説

http://mb.softbank.jp/biz/special/article/security_report/

