スレートPCの普及とセキュリティ問題

― 教育現場の利用を中心として ―

The Use of Slate PC has Spread and Increased Security issues

― Slate PC for educational use ―

岡田章彦

Akihiko Okada

キーワード：スレートPC　タブレットPC　スマートフォン　コンピュータウイルス　マルウェア　ネットブック　ネット端末　教育利用

Keywords : Slate PC, Tablet PC, Smart Phone, Computer Virus, Malware, Netbook, Network Device, Educational Use

要旨

日本におけるスマートフォン元年は２０１０年秋冬モデルからであると考える。スマートフォンであるiPhone 3Gが日本で２００８年に発売され急速にそのシェアを伸ばしていったが、日本独自の機能を搭載したフィーチャーフォンが主流であった。Apple社が開発し日本ではソフトバンク社が独占販売を開始したが、当初はそれほどシェアを獲得できなかった。しかしながら、２００９年のiPhone3GSの発売とともにスマートフォンの独占的なシェアを拡大していくこととなった。そして、２０１１年、各日本の通信キャリアがグーグル社のAndroid OSを搭載したスマートフォンを開発し、日本独自の機能を付加して販売することとなり、一気に日本のマーケットはスマートフォンに傾くこととなった。

また、スレートPCにおいては２０１０年、iPhoneと同じiOSを搭載したiPadをApple社が販売を開始した。スマートフォンのように急速な伸びを見せていないが２０１１年の世界累積販売数は２８００万台といわれているほどとなっている。グーグル社も同じようにAndroid OSを搭載したスレートPCを各メーカーが開発し販売を始めたことからスレートPCの所有台数は飛躍的な伸びを見せると思われる。

スレートPCはネットブックとスマートフォンの間を埋める端末となるといわれている。重要となるアプリケーションに関しては、Apple iPadはiPhoneアプリケーションと比べ専用アプリケーション数は少ないものの幅広くビジネス、教育、娯楽等で利用できるものが提供されている。ハードウェアとアプリケーションがバランスよくそろうことで普及の速度を高めることとになる。

しかしながら、スマートフォンやスレートPCはフィーチャーフォンとは違いPDA

(Personal Digital Assistants) の発展系であることから、PCに近い存在といえる。このことから、急速にスレートPCとスマートフォンに対するウイルス、マルウェアなどの攻撃が増加している。

この論文では、教育全般で有益に利用できるパーソナルコンピュータに近いスレートPCの導入にあたって、検討するべき事項、セキュリティ問題を検証する。

Ⅰ　はじめに

2010年から急速に普及しているスレートPC（以下タブレット型PC）の歴史は古い。その原点となるタブレット型PCは２０００年１１月に発表され、２００２年にマイクロソフトOSに準拠したものが各PCメーカーから発売された。しかしながら、当時のノートパソコンと同程度の処理性能で3万円程度高いこと、ユーザーインターフェースが成熟していなかったことから普及するには至らなかった。

タブレット型PCの定義はいまだ曖昧な部分がある。機能やアプリケーションの違いからノートPCとははっきりと区別されていたが、iPadが普及することで従来型のパーソナルコンピュータと同等のものと分類されることも多くなってきている。PDAに準ずるデバイスというものから、よりPCにちかい分類になっている。これは、テクノロジーの利用の方法がここ１０年で変容してきていることを示していると考える。

パーソナルコンピュータに限りなく近くなったことから、スマートフォンおよびタブレットPCのセキュリティ問題を避けて通れなくなってきている。この数年で、スマートフォン、タブレットPCに対する攻撃が急速に増加し、法人、個人の区別なく情報の漏洩などの危険度が高まっている。

この論文においては、利用者が急増しているタブレットPCのセキュリティ問題を検証し、特に教育現場への導入が世界的に増加していることも踏まえ、現実的な問題点を考える。

Ⅱ　iPad, Android, Windowsタブレット PCの相違点

タブレットPCの普及の原動力となったiPadは、アップル社が２０１０年１月にアメリカ・サンフランシスコで発表され同年４月より販売された。日本では、５月２８日より（無線LAN（以下、Wi-Fi）モデルとWi-Fi＋携帯電話回線（以下、3G）モデルが販売された。iPadはiPhoneと同じOSであるiOSを搭載し、外部メモリは搭載せず16GB, 32GB, 64GBの３種類で、内部メモリは２５６MBでクローズド環境のモデルである。画面サイズは９.５６インチ、１０２４×７６８ピクセル、解像度１３２ppiでiPhoneの９６０ｘ６４０ピクセル解像度３２６ppi高詳細画面は搭載しなかった。

翌年２０１１年４月２８日にiPad2が販売され、現在に至っている。iPad2においても外

部メモリは搭載されなかったが、内蔵メモリが2倍の５１２MBに増え、初代iPadに搭載予定であったデジタルカメラ機能を搭載し、１GHzデュアルコアApple A5　CPUを搭載した。筐体の大きさはiPadと変わらないが、厚みは８．８ミリに薄型化し、より持ち運びが楽になった。

iOSはもともとiPhoneの基本ソフトウェアとして開発されたものである。OS X iPhoneからiPhone OSとなり、２０１０年６月２１日にリリースのバージョン４．０からはiOSという名称が使われるようになった。

iOSはAndroid OSのオープンソースソフトウェアとは違い、アップル社が管理していて修正を許可していない。そのため、OS自体のセキュリティは１００％ではないが修正を許可しているAndroidよりは安全といわれている。

また、配布アプリケーションにおいても、アップル社が運営するApp Storeからのみ無料もしくは有料のアプリケーションがダウンロードできる。さらに、アップル社の審査を通過しなければApp Storeで配布することができないシステムとなっている。このシステムもセキュリティ向上には貢献していることは確かだが、セキュリティに関して１００％は存在しないことから審査されたアプリケーションにウイルスやマルウェアが潜んでいることがある。加えて、iPadやiPhoneにもOS自体の脆弱性が発見され、細工されたPDFファイルを読み込むだけでウイルスに感染し、外部から遠隔操作が可能になり、個人情報が盗み取られる危険性があった。すでに問題は修正されているが、この修正までに感染していた場合は情報が漏洩した可能性もある。特にiOSはウイルスチェックソフトウェアが提供されていないことか

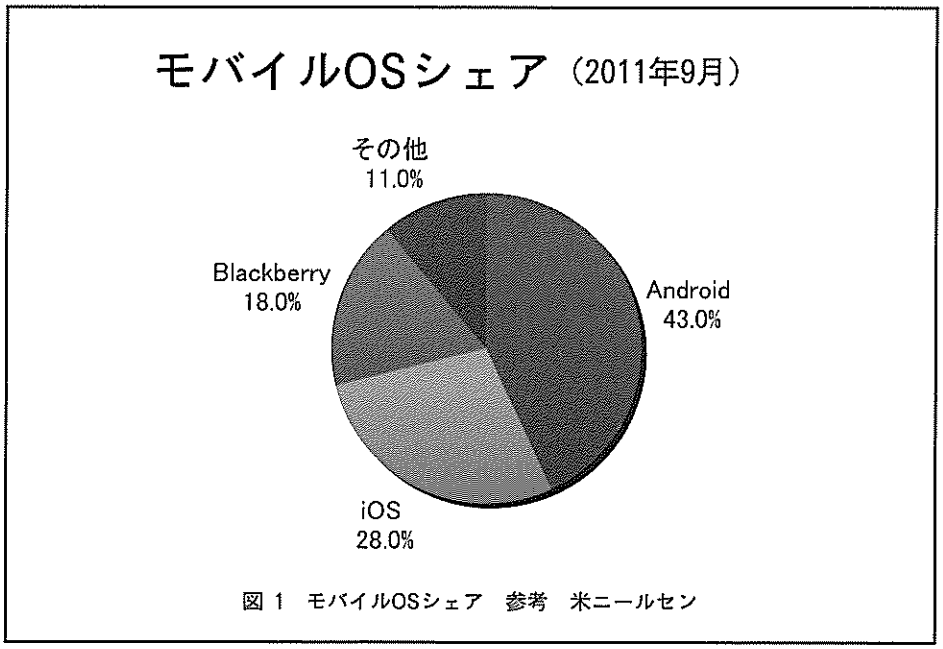

図１　モバイルOSシェア　参考　米ニールセン

ら発見は外部機関であることが多い。

他方、Androidタブレットは、オープンソースソフトウェアであるAndroid OSを搭載し、各メーカーが準拠して販売を行っている。この構図は、過去のIBM互換機戦略とAppleコンピュータ独占の形に似ている。そして、両陣営のシェアは互換機対アップルと同じ傾向を示してきている。

Android OSの比較を難しくしている点は、現時点でタブレット用OSとして３．０を用意し、スマートフォン用として２．０という違うものを用意していることである。このOSの分化は２０１１年に始まったが、次期バージョンである４．０（コードネーム：Ice Cream Sandwich）で統合されることとなっている。

図1の通り、米調査会社ニールセンが2011年9月発表のデータでAndroid OS搭載機種利用者が４３％のシェアを獲得したことがわかった。「週間東洋経済10月8日号」によれば、アンドロイド端末を製造しているメーカーは３９社に上り、世界１２３カ国、２３１の通信キャリアが販売している。やはり、1社独占と互換機との差がでてきていることがうかがえる。Android OSはオープンソースであり、開発者のソフトウェアの修正を認めていること、OSを無償で提供し、設計上の縛りがなく自由度が大きい。これらからiPhoneとは違いハードウェアの独自性を打ち出すことができることがシェア拡大に貢献していると思われる。

先述の通り、設計の自由度が高いということは、各メーカーがOSを修正し独自機能を付加することが可能になるということである。これは機種により独自性を前面に出すことができ、利用者の選択と利便性を高くするが、逆に修正によるセキュリティの脆弱性も生まれてくることとなる。また、メーカーによってOSに変更があるということは、各メーカーの基本部分に違いが生じることから脆弱性を発見できにくくする問題が浮上してくる。

タブレットPCの原点であるWindowsタブレットPCはiPadやAndroidタブレットとは２０００年発売当時から現在まで本質的に違うものと考える。モバイルOSという位置づけではなく、本来のコンピュータのOSであるWindowsにペン認識機能やタッチパネル機能を搭載し、その機能をいかしたものを作り上げた。このため、当初からタブレットPCという認識ではなくノートPCの位置づけとして作られたものである。現時点では同じ視点で比較することは難しいが、今後発売が予定されているWindows8からはタブレットPCとしての機能が組み込まれる可能性が高い。

Ⅲ　タブレットOS，スマートフォンOSのウイルス、マルウェア

スマートフォン、タブレットPCの普及により、新しいウイルス、マルウェアの脅威が非常に高くなってきている。スマートフォンユーザーは携帯電話からの延長線上と考えている場合が多く、常時ネットワークに接続している手のひらに乗るコンピュータであるというこ

との意識が低い。コンピュータと同じようにインターネットに接続して利用できるということから、「フィッシング詐欺」や「ワンクリック詐欺」はごく当然のものとなってきている。特に、比較的自由度の高い「Android Market」などでアプリケーションを配布できるAndroid端末はiOS端末よりもアプリケーションの安全性のリスクが高くなっている。

しかしながら、iOSも安全であるとはいえない。２０１１年１０月にiOS5がリリースされたが、２００以上の新しい機能が追加されたことに加え、セキュリティに関する重大な修正もされている。iOS 5ソフトウェアアップデートは、iOS 3.0～4.3.5を搭載したiPhone 3GSとiPhone 4、iOS 3.1～4.3.5を搭載した第3世代以降のiPod touch、iOS 3.2～4.3.5を搭載したiPadにそれぞれ対応する。細工を施した画像やWebサイトなどを使って悪用される恐れのある脆弱性を多数修正したほか、データセキュリティ関連ではWebトラフィックの通信暗号化に用いられるSSL／TLS関連の脆弱性が指摘されたことに対応してTLS 1.2のサポートを追加した。また、不正な証明書の発行問題が発覚したSSL認証局DigiNotarの証明書を失効させる措置も盛り込んだ。

このように、既知の問題であるものもOS本体のことでありApple社が提供しなければ根本的な解決はできない。今後の課題としては、現在Microsoft社が提供しているように毎月１回定期的にセキュリティパッチソフトの提供が必要になってきていると考える。

一方、表計算ソフトNumbersの更新版となる「Numbers for iOS v1.5」ではExcelファイルの処理に関する2件の問題に、文書作成ソフトPagesの更新版となる「Pages for iOS v1.5」ではMicrosoft Word文書の処理に関するメモリ破損問題にそれぞれ対処した。細工を施したExcelやWordファイルを使ってこれら脆弱性を悪用された場合、任意のコードを実行される恐れがあった。

図２のように２０１１年初めからアンドロイド端末の爆発的な普及が世界で起こり、それにあわせるようにAndroid端末を狙ったウイルスの登録数が急増していきている。怪しいアプリケーションをインストールしなければ安心だと考えるユーザーも多いが、無意識や自動インストールで感染してしまうことが多く、心がけだけで守れるものではない状況になっている。

また、セキュリティソフトウェアプロバイダであるマカフィーの２０１１年８月の調査結果によると、Android端末を標的とするマルウェアは前四半期から７６％も増加し、結果、Android OSは攻撃をもっとも受けるOSになった。２０１１年前半までに前年比２２％増の１２００万種類のマルウェアが発見され、２０１１年末までにサンプル数は７５００万個まで増えると予測している。

加えて、OS自体の脆弱性はある程度の期間放置されることが多く、このシステムのセキュリティホールからウイルスの侵入、不正処理を許してしまうこととなっている。問題は、OS

自体脆弱性の解決は時間がかかることが多いことである。特に、Android OSは各メーカーが修正していることもあるため、iOSと違い各メーカー個々の端末の仕様にあわせて脆弱性を解決するセキュリティパッチや最新版のOSを用意しなければならない。この解決版が提供されない限り、脆弱性は残ったままとなる。

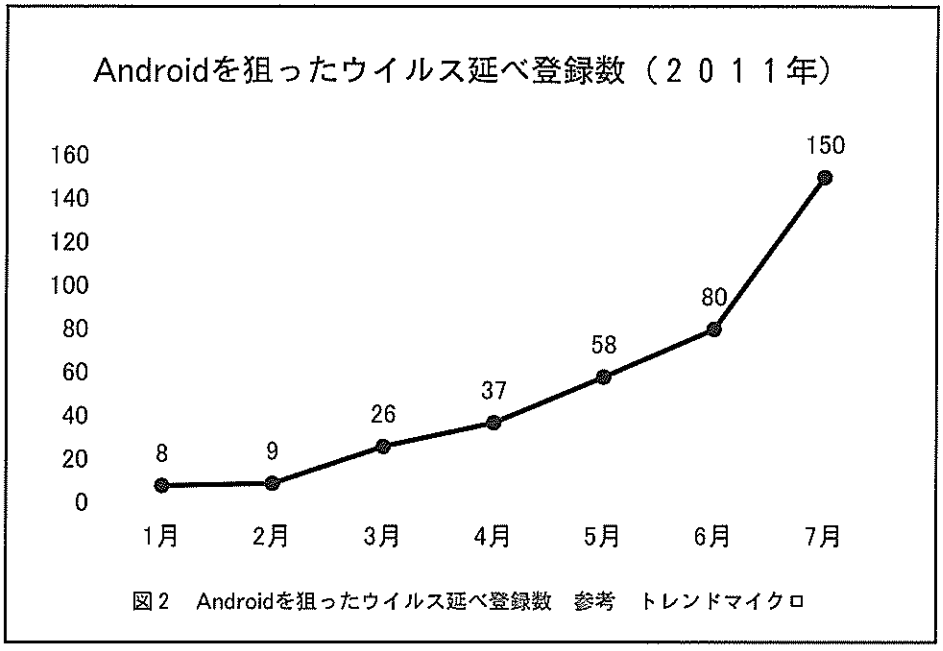

図２　Androidを狙ったウイルス延べ登録数　参考　トレンドマイクロ

Ⅳ　タブレットPCおよびスマートフォンのセキュリティ問題

現時点では、スマートフォンのセキュリティの問題はタブレットPCのセキュリティ問題に直結しているといってよい。ほぼ同じソースコードで書かれているOSを利用するため、iOS, Android OS搭載の携帯端末が普及すれば、同様のセキュリティ問題がタブレットPCでも起こってくると考える。図３のように、２０１０年４－６月期から２０１１年４－６月期の１年間でほぼ１００％近かったスマートフォン以外の携帯端末利用者が７０％以下になり、スマートフォン利用者は一気に３０％以上の比率になった。このような想像以上の普及は、考え方、利用方法が環境について行かない状況を生み出してしまう。

スマートフォンやタブレットPCはネット環境の普及で利用方法は３G回線もしくはWi-Fi接続が前提となっている。常時ネットワークに接続している環境を生み出すことが可能である。すなわち、ほぼ１００％近い状況で端末が常時ネットワークに接続していると考えてよい。総務省は２０１１年１０月１１日に「スマートフォン・クラウドセキュリティ研究会」

を発足させ２０１１年までに一定の取りまとめを行う予定である。総務省はスマートフォンやタブレットPCが私たちの個人生活や企業活動などの様々な場面での利活用の期待をしているが、一方でモバイルパソコンと同等の機能を持つことから情報漏洩などのセキュリティ問題を認識し従来のモバイル端末とは違う対策が必要であると考えている。

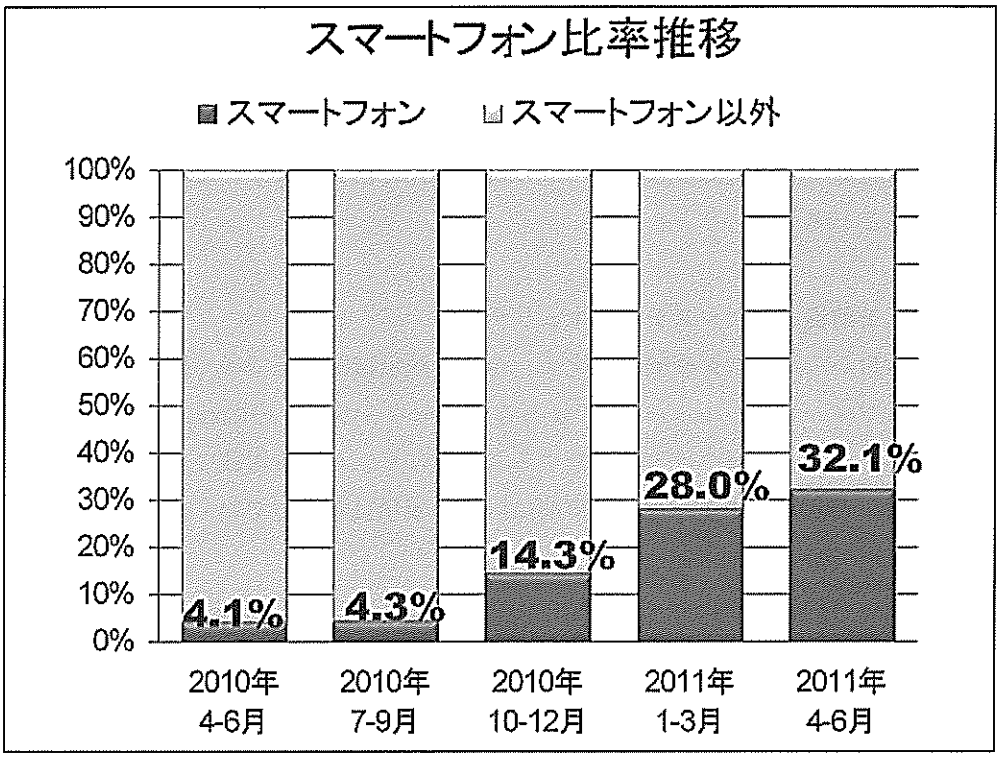

図 3　スマートフォン比率推移　　参考　電子情報技術産業協会（JEITA）

加えて、内蔵メモリが少ない端末であるため、情報をクラウドサービスに同期させ利用する場面も急速に普及してきている。端末内に保存するのではなくインターネット上に分散してデータを残しどこでも利用できるため、基本的には内蔵メモリの残量を気にすることなく利用することができる。しかしながら、ネットワーク上に重要なデータ、画像等を預けるということになることから、セキュリティが万全でなければ情報漏洩に簡単につながってしまう問題をかかえている。

総務省の主な検討事項は

(1) スマートフォン、クラウドサービス等の新たな情報セキュリティ上の課題

(2) サービス提供事業者や端末ベンダにおいて現在取られている対策及び今後導入が検

討されるべき対策

(3) 利用者の情報セキュリティ意識向上策及び取るべき対策

(4) その他

としている。(1) に関してはすでに認知度は高まってきているが、(2)、(3) に関しては情報倫理教育も定着してきてはいるが、いまだパーソナルコンピュータの利用においても意識レベルは低い状態が続いている。このことに加えて、若年層から高齢者まで使いやすいシステムであるとされているスマートフォン、タブレットPCの普及はより早く進むと考えられることから、このモバイル端末の問題を解決するためは早期の法的な整備も必要である。さらに、より基礎の部分である教育の場から自己責任で自分自身を守るための教育を定着させる必要があると考える。

V　学校導入を前提としたシステムセキュリティ

初等中等教育から高等教育機関、研究所、企業、医療機関などで多く採用され利用されているスマートフォンとタブレットPCではあるが、セキュリティの問題は避けて通ることができない。リテラシー教育だけでは完結することはなく、それを実践できる安全な環境構築が必要である。導入するにあたって、事前に以下の事項は確立しておく必要がある。

①セキュリティ教育、継続
②システム側のセキュリティ強化、継続
③端末側のセキュリティ強化、継続

高度なシステムを簡単に使えるがゆえに、より高度なセキュリティの知識を持つこと、そして、それを防御するシステムを構築することが必要である。Android OSに関してはウイルス、マルウェアの急速な増加で、各大手セキュリティソフトウェアプロバイダがソフトウェアを提供し始めている。今後、iOS, Android, Windowsを利用するにあたっては、セキュリティソフトウェアの導入は必須項目であると考えてよい。

また、システム側においては不正アクセスの監視の強化、アプリケーションのインストール規制、紛失時の対応等、個人だけで対応の難しい部分を制御していく必要があると考える。

加えて、導入前に必ず以下のことは最低限保証されなければならない。

①導入効果を検討することが必要になるための母数を決めること
②全体のコンセンサスを得ること
③本体や通信にかかる費用の対応

④安全に利用するためのシステム、アプリケーション、セキュリティ確保のための費用、システム、継続的な教育

上記の事項を満たすためには、予算の確保も必要になってくる。大学教育においては、学部単位、学科単位で最低限配布する必要と考えることから一般的なタブレットPC機種を2年利用、500名という単位で費用を見てみたい。ただし、iPadはOSの性格上、セキュリティソフトの常駐ができないため、本体での検索ができないことからセキュリティソフトは現時点で除外する。

表 1 機種別2年間費用

OS種別	メーカー	機　種	回線種別	本体価格	通信費	セキュリティソフト	2年合計	500台／2年
iOS	Apple	iPad2 wi-fi+3G	無線LAN+3G	64,800	5,125	0	187,800	93,900,000
iOS	Apple	iPad2 wi-fi	無線LAN	52,800	0	0	52,800	26,400,000
Android	Sumsong	GALAXY Tab 10.1 LTE	無線LAN+3G	73,710	5,775	2,980	215,290	107,645,000
Android	Acer	ICONIA TAB A500	無線 LAN	47,000	0	2,980	49,980	24,990,000
Windows	Acer	ICONIATAB-W500	無線 LAN	64,000	0	6,480	70,480	35,240,000

表1は法人購入ではなく個人価格をベースにしている。法人購入の場合は本体価格、利用価格は変動する可能性が高い。しかしながら、どの機種を導入するに当たっても学生に手渡すだけでは費用対効果が望むことができない。

名古屋文理大学はiPadを無償貸与し、2ヶ月間利用した結果を報告した。iPadの教育利用では、「辞書」としては活用できるが「ノート」としては難しいとしている。これは、タッチパネルのソフトキーボードが長文入力には向いていないということであると考える。授業では、資料のデジタル配付、電子辞書、WEB検索、学習用アプリ、eラーニング、SNSでのコミュニケーションを実現している。

大阪大谷大学においてはmoodleを利用している。3G回線もしくはキャンパス全体で無線LANが利用できるようになれば、どの教室にいてもmoodleを活用することができるようになる。Moodle利用は、現時点では情報教室を利用する教員が主であるが、この端末を利

用すれば全教員の活用が可能になる。

また、全学的に行っているe-ラーニングにおいても、情報教室を利用することなく、場所や時間を気にすることなく学生が学習できる環境を構築できる利点がある。教員においても、資料のデジタル配付が簡単に行えることになることから紙主体の資料からの脱却ができる可能性が高い。

これらのことが全学的におこなうことができれば、教育効果は飛躍的に向上すると考える。

Ⅵ　おわりに

タブレットPCの学校教育利用は、過去よく行われたノートPCの配布とよく似た傾向がある。しかしながら、大きな相違点はネットワーク接続である。ノートPCは、当時情報ソケットが必要でネット接続はほとんど考慮されていなかった。タブレットPCはネットワーク接続が前提であるので、Wi-Fiもしくは３G回線を利用し、教育現場のいろいろな場面で活用できることを想定している。すべての利用者が常時ネットワークに接続している環境を提供することは、教育の現場としてセキュリティの確保に努める必要がある。ただ単に効果のみを考え、セキュリティに投資ができない場合は情報漏洩等の大きいな問題に遭遇する可能性が高いと考える。

加えて、費用対効果をきっちりと検証しなければならない。特定の教員が利用するのではなくすべての教員が活用できる環境をシステム側でも用意する必要がある。特に、資料のデジタル化、プレゼンテーションアプリの活用、学習アプリの提供などがあげられる。また、セキュリティの強化策は不可欠であり、情報漏洩、ウイルス感染の可能性を極力低くする努力が必要である。不必要なアプリをインストールすることでメモリが不足しない対策も必要だと考える。

セキュリティ対策に１００％はないといわれているが、すべての問題が解決し教育、研究に導入することができれば、教育の質の向上、学生とのコミュニケーションの幅を広げ、相当な教育効果が見込めると考える。タブレットPC導入は単なる情報教育の一環ではなく、すべての研究分野での常時利用が可能になり、教育の質を向上するツールと今後は考えてよいだろう。

参考文献

1．週刊東洋経済　10月18日号

2．財団法人インターネット協会「インターネット白書　２０１１」インプレスＲ＆Ｄ　２０１１

3．２.財団法人インターネット協会「インターネット白書　２０１０」インプレスＲ＆Ｄ　２０１０

4．ニールセン　http://jp.nielsen.com/site/index.shtml

5．トレンドマイクロ　インターネットセキュリティナレッジ　http://is702.jp/special/992/partner/12_t/

6．マカフィー　http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q2-2011.pdf

7．総務省　「スマートフォン・クラウドセキュリティ研究会」
http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_01000009.html

8．ITmedia エンタープライズ
http://www.itmedia.co.jp/enterprise/articles/1110/13/news017.html

9．「DIME　2011年11号」小学館　2011

10.「日経トレンディ　2011年11月号」日経BP社