

# Functions and Problems of Mobile Device Management: Necessity and Form of MDM Systems

|       |                                                                                             |
|-------|---------------------------------------------------------------------------------------------|
| メタデータ | 言語: jpn<br>出版者:<br>公開日: 2017-10-03<br>キーワード (Ja):<br>キーワード (En):<br>作成者:<br>メールアドレス:<br>所属: |
| URL   | <a href="http://hdl.handle.net/2297/34380">http://hdl.handle.net/2297/34380</a>             |

# モバイル・デバイス・マネジメントの機能と課題

## —— MDMシステムの必要性とあり方 ——

白 石 弘 幸

### 目 次

- I 問題の所在
- II スマートフォンと高速通信
  - 1. スマートフォンの開発経緯と競争動向
  - 2. 高速通信とスマートフォンの利用形態
- III スマートフォンが内包する情報流出リスク
- IV モバイル・デバイス・マネジメントの必要性
- V モバイル・デバイス・マネジメントの機能
- VI BYOにおけるセキュリティ対策の課題
- VII 結 び

### I 問題の所在

高速通信サービスが普及しこれに対応したモバイル端末の機種が増大すると、社外たとえば移動中に大量データの送受信を行うことが容易になり、業務用ツールとしてのモバイル端末の利便性が向上する。それにともない、ビジネスパーソンはますますスマートフォンやタブレット端末を社外に持ち出し、これらの端末を業務用ツールとして利用するようになる。

しかし一方では、記憶媒体がフロッピーディスクやCDからUSBフラッシュメモリーに小型化するにつれて紛失事故が増えたのと同様に、モバイル環境で利用される端末が小型・薄型・軽量化するのにもない紛失や置忘れのトラブルが増えるだろう。ノートパソコンをファーストフード店のテーブルや電車のソファに置き忘れるということは少ないが、スマートフォンならば

これが十分起こりうる。そもそもノートパソコンといっても、現行製品よりも分厚く重たかった時代にはこれをかばんの中に入れて携行し、飲食店や電車の中で広げるという気持ちにもなりにくかった。

パソコンに比べて安価である一方、業務用ツールとしての機能・性能がパソコンとさほど差がなくなると、自分のスマートフォンやタブレット端末を仕事に使う、たとえばこういったスマート端末で自社のサーバーにアクセスするという“Bring Your Own (Device)”, いわゆるBYO (BYOD) も増大する。モバイルで大量のデータを送受信され、場合によってはどのようなセキュリティが施されているかわからない私物の端末でサーバーにアクセスされる以上、企業側もこれに対応したセキュリティ体制を構築する必要がある。そのための取組が本研究で取り上げるモバイル・デバイス・マネジメント (MDM) である。

業務にスマートフォン、タブレット端末をどのように活用するかの方法論や具体的ノウハウの紹介はコンピュータやビジネスの専門誌で盛んに行われており、多少過熱気味の感さえあるので、本研究では取り上げない。むしろ本研究の目的はそのようなモバイル端末のビジネス利用に潜むセキュリティ・リスクとこれへの対応策について検討することにある。特に無料アプリによる情報流出リスクの高いスマートフォンを業務に利用する場合の当該リスク・マネジメントについて論ずる。

## II スマートフォンと高速通信

### 1. スマートフォンの開発経緯と競争動向

スマートフォン、タブレット端末は前者が主要機能の一つに音声通話(電話)があることからしても、また端末の大きさから言っても携帯電話の発展型であると見なせ、後者はサイズの的にパーム系デバイス(PDA)もしくはパソコンの延長線上にあると見ることもできる。しかし両者には携帯性に優れ、インターネットの閲覧等パソコンと同等の多機能性を備え、タッチパネル方式のインターフェイスを持つという共通の特徴がある。後に述べるようにこうした技術的特性、デザインの独自性をめぐる米国Apple社と韓国サムス

ン(三星電子)社の間で法廷論争が行われているが<sup>3</sup>, その起源はと言うと必ずしも定かではないし, これを両者のどちらか一方に断定ないし限定することも難しい。むしろ多くの他社製品たとえば1996年にフィンランドのNokia社より発売されたNokia 9000 Communicator, 1999年にサービスが開始されたNTTドコモのiモード対応端末, その他に萌芽的形態を見て取ることができ, 技術的な原点を一つの特定制品に求めることは極めて困難であると言える。異種技術を組み合わせた典型的なマルチテクノロジー型商品, 多機能端末という製品特性上, これは当然なのかもしれない。

スマートフォンが世界的に普及し始めたのは2007年から2008年で, まず2007年に米国のApple社が同社のパソコンMacをベースに開発したスマートフォンiPhoneを市場投入した。翌2008年には第三世代携帯電話に対応したiPhone 3 Gが日本を含む世界各国で発売された。これと並行して, Google社のOSであるAndroidを搭載したスマートフォンが韓国のサムスン社や台湾のHTC社によって商品化されている。

AndroidはもともとはGoogle社が買収したソフトウェアのメーカー Android社により開発されたOSである。この他にスマートフォン向けOSとしてフィンランドのNokia社がSymbian, カナダのResearch In Motion (RIM) 社がBlack Berry, 米国Microsoft社がWindows MobileやWindows Phoneを実用化した。ハード(端末)のデザインについてはApple社等現行製品メーカーのオリジナルであるという見方以外に, 現行製品はソニー社の新商品コンセプトをモデル(原型)としてそれから派生したものであるという見解もある。より具体的には, 「iPhoneのデザインが生まれたきっかけは, ソニーのデザイナーが着想した『ボタンを極力無くした携帯端末』を紹介した記事」であり, Apple社に当時勤務していた日本人デザイナーに「『ソニーが(iPhoneを)作るとしたら, どんなデザインにするか作ってくれ』と依頼。その“ソニースタイル”の試作品デザインが<sup>4</sup>, 「iPhoneに影響を及ぼした」という主張が韓国サムスン社によりなされている。これに対しApple社は, 「“ソニースタイル”の試作品ができる前にiPhoneデザインの原型は生まれていたと反論」している(日本経済新聞, 2012年8月1日)。

米国の調査会社ガートナーによれば, 2012年4～6月期におけるスマート

フォンの世界販売台数は前年同期比43%増の1億5368万台になった。従来型の携帯電話は減少傾向が続き、携帯電話全体に占めるスマートフォンの割合は前年同期の25%から37%に上昇した。各社の具体的なマーケット・シェアはサムスン32.6%、Apple16.9%、Nokia6.6%等となっている(図表1)。すなわち「スマホ普及の追い風を十分に受けているのはサムスンとアップルの『2強』」で、特に「サムスは主力の『ギャラクシーS』シリーズが好調で4～6月期の携帯部門の営業利益が前年同期の2.5倍に拡大した(日本経済新聞、2012年8月16日)。一方、3位以下のメーカーについては次のように報じられている。「従来型携帯電話で長年世界一だったノキアなど3位以下のメーカーは軒並み苦戦している。ノキア、台湾の宏達国際電子(HTC)、カナダのリサーチ・イン・モーション(RIM)は4～6月期に2～4割減収になり、営業減益または赤字だった。各社は立て直しに向けて大規模な人員削減など事業見直しに動いている。ノキアは6月、2013年末までに全社員の約1割に当たる1万人程度を削減する方針を示した。RIMも13年2月までに全社員の3割に相当する5000人を減らす。HTCは競争が厳しい韓国やブラジル市場からの撤退や、米ノースカロライナ州の研究開発拠点を閉鎖することを決めている」(日本経済新聞、前掲同所)<sup>1)</sup>。このように、スマートフォンのシェア争いにおける優劣がそのままIT機器大手の業績、さらには投資やリストラに影響を及ぼす格好となっている。

|                 |             |
|-----------------|-------------|
| 1. サムスン電子 (韓国)  | 32.6 (15.6) |
| 2. アップル (米国)    | 16.9 (▲1.9) |
| 3. ノキア (フィンランド) | 6.6 (▲8.8)  |
| 4. 宏達国際電子 (台湾)  | 5.7 (▲5.0)  |
| 5. 中興通迅 (中国)    | 5.2 (3.4)   |
| その他             | 32.9 (▲3.3) |

備考. 2012年4～6月期・出荷台数、IDC調べ  
 ( ) 内は前年同期比  
 四捨五入の関係で合計は100とならない。

図表1 スマートフォンの世界シェア

もっともデファクト・スタンダードが定まらず規格争いが続いている情報機器等の場合、シェアは短期間に変動しうる。図表1に示されているスマートフォン市場のシェア増減(前年同期比)を見ても、その傾向は顕著である。したがって、後に述べるLTE(Long Term Evolution)など高速通信サービスにどう対応するかによって、スマートフォン市場における競争動向は大きく変わる可能性もある。

また日米欧等の各国で行われているスマートフォン関連訴訟の行方、すなわちApple社とサムスン社間で行われている技術やデザインをめぐる紛争の動向も今後、マーケット・シェアに影響を与えるという見方も一部にある。しかしながら少なくともサムスン社の方はその影響を回避する製品戦略を取るものと見られている。実際、2012年8月に米国連邦地裁はサムスン社の一部特許侵害を認める判決を出したが、その直後、同社はAndroidではなくWindows Phone 8搭載の新機種を同2012年内に発売することを発表している。

## 2. 高速通信とスマートフォンの利用形態

スマートフォンを含む携帯電話の使い勝手を左右する一つのファクターは、その通信速度にある。従来、携帯電話向けの通信サービスで比較的高速だったのはKDDIグループのWiMAXであるが、その速度は37.5~40Mbpsが主流であった。LTEすなわちLong Term Evolutionは100Mbps超で、固定回線のADSLに迫る広帯域通信サービスである。欧米では既にサービスが始まっているが、日本ではNTTドコモが先行し、これに対応したスマートフォンも同社が2012年、他社に先駆けて発売した。「KDDI、ソフトバンクもLTEスマホ市場に参入する構えで、通信速度をめぐる競争は一段と激化する」一方、「スマホは通信速度がパソコンに迫る高速携帯が主流となり、ネット接続の主力端末になる」(日本経済新聞、2012年8月20日)という見通しもある。

このLTEの普及によって、業務支援ツールとしてのスマートフォンの利用形態も大きく変わる可能性がある。スマートフォンやタブレット端末の業務用ツールとしての利点は「パソコンのように立ち上げに時間がかからず、使いたい時にすぐ起動できる」「パソコンや専用端末より初期投資は安く、多くの社員が働く店頭や製造、物流現場などにも導入しやすい」「直感的なインターフェイスで操作できる」「画像や映像の扱いが容易」といったことである。実際

の利用形態としても、端的に言えばフィンガータッチの入力用端末、映像付きのマニュアル・カタログ・会議用資料が一般的だった(小林・山端, 2011, 28-30)<sup>2)</sup>。つまりユーザー・フレンドリーなインターフェイスに重点を置いて開発されたため、実際フィンガータッチ方式の操作パネルは親近性が高く、操作性の優れた端末とはなったが、その反面、通信速度に関しては比較的軽視されている感があった。通信速度が遅く大量データの送受信には不向きという短所がビジネスツール、特に社外における業務用端末としてのスマートフォンの利用にとって障害となり、ビジネスユースの普及に歯止めをかけていたと言える。国内販売台数で見て、2011年度にスマートフォンはパソコンを初めて上回ったが、「ネット接続では通信速度がネックになっていた」(日本経済新聞, 2012年8月20日)。

ところがLTE等高速通信サービスと対応端末の普及はこの限界を解消することになる。すなわち自社サーバーとの大量データのやり取りがスムーズに行えるようになり、モバイル環境ないしテレワーク環境での送受信端末としての利用が増大することになる。

### Ⅲ スマートフォンが内包する情報流出リスク

スマートフォンには本人のメールアドレスや電話番号、アドレス帳に登録された取引先や顧客あるいは親族や友人等のアドレス、サイトの閲覧履歴等が蓄積されている。精細な位置情報もリアルタイムで入手されうる。端的に言えば、スマートフォンは個人情報の固まりである。このため、前章で述べたようにスマートフォンは業務用ツールとしての携帯電話の可能性と重要性を大幅に増大させつつあるが、その一方で業務情報の流出リスクを高めることとなった。たとえばスマートフォン用アプリをダウンロードすると、そのスマートフォンに蓄積されている取引先や顧客のメールアドレスが知らず知らずのうちに外部の第三者に伝送され、利用されるという危険性が増大している。これは無料アプリの中には、スマートフォン保存情報を自動的に、定期的に吸い上げ外部のサーバーに送信する機能を有するものが少なくないからである。極端な場合この機能を利用し、「振り込め詐欺など犯罪目的で収集す

る事業者もいる」(日本経済新聞, 2012年5月14日)。

ただし「日本では、アプリによる情報収集は個人情報保護法の規制対象となりうる。本人を特定できる情報の取得・利用には、目的を明示しなければならない」(日本経済新聞, 前掲同所)。このため、アプリをダウンロードする際の同意事項に、このような送信を行う旨が記載されている場合も多いものの、大多数の個人はそれを意識せずに、あるいはそもそもきちんとは読まずに、「同意する」をクリックしていると言われる。「手軽なスマホだからこそ、利用者は何気なくボタンを押してしまう」という傾向もあると指摘されている(日本経済新聞, 2012年8月11日)。

なかには、このような個人情報保護法による規制があるにもかかわらず、ユーザー本人に無断で、電話帳に登録されている氏名や電話番号などの情報を送出する無料アプリもある。2012年5月にはこのようなアプリがインターネットで大規模配信されるという問題も起き、これを受けて警視庁は東京都内のIT関連会社など関係先数箇所を不正指令電磁的記録供用容疑で家宅搜索した(日本経済新聞, 2012年5月19日)。非接触ICタグ、いわゆるRFIDを装備したカードの情報を盗み取る機能を備えたアプリも出回っている。このアプリをインストールしたスマートフォンを財布と重ねて置くと、中にあるカードや社員証の番号や有効日、有効期限などが抜き取られ、外部に発信されてしまう危険性がある。

現状では、スマートフォン向けアプリは汎用性の低いものが各OS別にいわゆるネイティブ・アプリケーションとしてつくられ、流通している。iPhoneについて言えば、アプリ開発に際してApple Developer Connectionへの加入と公式サイトApp Storeにおける配信が求められ、Apple社により不正な機能が備わっていないかの審査が行われる。このプロセスを経していないアプリはいわば非公認アプリという位置付けになる。

これに対し、Google社は最低限のネガティブチェックを自動で行っているものの、個々のアプリを細部まで検査するということはしていない。元来、同社のビジネスモデルは製品の規格情報やアーキテクチャーを秘匿し、これをベースに収益をあげるという形にはなっていない。たとえばデファクト・スタンダード化したOS等の規格をクローズし、アプリケーション等の周辺ビ

ビジネスをも自ら手がけるというスタイルは取られてこなかった。むしろ「場」やプラットフォームの提供を事業ミッションとし、これらのアーキテクチャーを公開する傾向にあった。またAndroid向けアプリは、利用しているエンジニアの多いJavaで開発されるのが一般的で、「インストールした不正アプリのプログラムの内容は端末上でわかるため、ある程度の知識があれば同じような不正アプリを簡単につくってしまう」(日本経済新聞, 2012年8月11日)。

このようなことから、現在のところ情報の吸い上げを行う無料アプリのほとんどは、OSとしてGoogle社のAndroidを搭載するスマートフォン向けに開発されている。Androidが標的にされている一因は前述したオープン性にあり、この点についてはGoogle社のオープン・ポリシーが裏目に出たと言えなくもない。

#### IV モバイル・デバイス・マネジメントの必要性

スマートフォンは、「その利便性ゆえに従来の機器以上に使用状況の把握が難しく、管理は困難」(小島, 2012a, 122)である。しかもII章で触れたLTE等の高速通信サービスが整備され、これに対応した端末の比率が増し、モバイル環境やテレワーク環境での利用が増えれば、この困難性は一層高まる。一方ではこのような高速通信サービスの整備と対応端末の普及によって、社外における情報端末としての使用が増し、送受信され処理されるデータ量も従来より格段に大きくなる。それとともに外部の悪意あるスパイウェア等から狙われる危険性、情報流出リスクも大幅に高まる。そのような危険性やリスクは端末の廃棄処分後までともなうから、結局、「ビジネス用途では、スマートデバイスの一台一台に対して導入から廃棄までライフサイクル全般にわたって管理が求められ、その管理負荷は相当のものとなる」(前掲同所)と考えなければならない。

II章でも言及したように、業務用ツールとしてのモバイル端末の一つの長所は安さで、「iPadのようなタブレットは5万円程度、スマホは1万円前後で購入できる機種もある。(中略)パソコンや専用端末より初期投資は安く、多くの社員が働く店頭や製造、物流現場などにも導入しやすい」(小林・山端, 2011, 28)というのがその強みであると企業側には見られている。

しかしながら企業が業務への私物利用解禁, BYO (BYOD) と一般的に略される“Bring Your Own (Device)” (社員本人にとってはTake My Own) を端末購入コスト削減につながるという理由で歓迎するのは短絡的, 安易である。というのも管理コストを考えるとBYOは企業にとって負担増となりうるからである。つまり私物解禁によるITコスト節減というのは, 企業にとって「幻想」に終わる可能性が高い。

また卑見ではコスト削減でBYOを実施すると, 社員の反感を買い, 失敗に終わる可能性が高い。むしろ「私物解禁の大きな目的は, 個人の働き方を変えたり, 仕事の効率を高めたり, 従業員のモチベーションを高めること」と認識した方がよからう (吉田, 2011, 36)。

もっとも, コスト節減に関しては私物解禁が幻想に終わる可能性が大きい一方で, これが現実のトレンドとして顕著になっていることは否定できない。すなわち, いずれにせよ業務支援ツールとしてのモバイル端末普及とBYOはビジネスの世界では現在「流れ」になっており, これは今後も加速するだろう。もともとこうした小型の端末は, 「私的利用環境と業務利用環境が混在した状態」となる傾向が強く, そのような状態での使用では「故意か過失かは別としてデータ漏洩のリスクが高まる」(山科, 2011, 73)。加えて, 「機器そのもののセキュリティもPCに比べ脆弱である」(前掲同所)。したがって負荷は大きくとも, 企業全体としての情報の流出防止策とセキュリティ対策にはこのようなモバイル環境で利用される端末に対する管理, モバイル・デバイス・マネジメント (MDM) が必要不可欠であり, 今後企業はこれに積極的に取り組まなければならない。

しかもスマートフォン, タブレット端末のモバイル環境やテレワーク環境での使用増大を考えると, 企業はこのような管理を遠隔かつ常時的に行う必要がある。ウィルス対策ソフトをインストールするなど初期設定時, あるいは適宜, セキュリティ対策を各端末に対して講じるというのでは不十分である。

先にも触れたように, 業務支援ツールとしてのスマートフォン, タブレット端末の利用では, モバイル環境やテレワーク環境での利用, 業務への私物利用の解禁 (BYO, BYOD) という流れが顕著になりつつある。そのようなことから企業はモバイル・デバイス・マネジメントの本質的重要性を認識し,

これに本格的に取り組む必要があるのだが<sup>3</sup>、「MDMサービス事業者やMDM製品において若干の機能追加はあるものの、業務利用を想定した場合の端末管理としては、不十分」(遠藤, 2011, 95)というのが現状である。

それでは、今後、モバイル・デバイス・マネジメントはどのような機能を担わなければならないのであろうか。ビジネスパーソンが安心してスマートフォンやタブレット端末を業務に使えるようになるために、これは広汎なセキュリティ機能を担わなければならない。次章では、その具体的あり方について検討したい。

## V モバイル・デバイス・マネジメントの機能

モバイル・デバイス・マネジメントが担うべき機能について論ずる際には、当該議論の前にスマートフォンやタブレット端末のビジネス利用に付随する潜在的な危険性について検討する必要がある。特に重要となるのは他の情報機器には見られない、こういったスマート端末特有のリスクとしてどのようなものがあるかということである。たとえば電子メール組込型のウィルス対策は、モバイル・デバイス・マネジメントでも重要であることはもちろんであるが、そういうスパムメールはデスクトップ・パソコンにも送られてくるのでモバイル・デバイス・マネジメントでことさら強調すべき問題、研究すべき新しいテーマとは言い難い。

スマートフォンやタブレット端末のビジネス利用に潜む特有のリスクとしてまずあげられるのは、社外での紛失・盗難の危険性である。デスクトップ・パソコンを社外で使い、電車のシートや飲食店のテーブルに置き忘れるということは通常ありえないが、スマートフォンや小型のタブレット端末ならばこういう事態の発生も考えられる。すなわち、「スマートデバイスは、社内外問わずに持ち運ばれ、それほど大きくなく目立たないため、紛失／盗難は避けられない」(小島, 2012b, 102)。このようなことから遠隔で端末を使用不可能にするリモートロック、遠隔で端末に保存されたデータを消去するリモートワイプの機能がモバイル・デバイス・マネジメントには不可欠である。有効でないパスワードを一定回数入力した場合に端末を操作不可能にしたり、

端末内のデータを削除し初期状態に戻すといった機能も、紛失・盗難リスクの高いスマート端末に関しては他の情報機器よりも強固にする必要がある。

スマートフォンやタブレット端末の場合、「無線LANでの通信が前提となる上、PCとは異なる認証やアクセス制御の仕組みが必要となる」(福田, 2012, 58)。より具体的には、MACアドレスや電子証明書によって登録済みの端末か否かを判別し、登録済みでない場合には新規登録や一時利用申請を受け、審査した上で電子証明書やパスワードの発行を行う仕組みを組み入れることになる。「デバイスの種類やユーザー権限に応じて、アクセス先を制限する」(前掲記事, 62)といった制御を行うことも考えられる<sup>3)</sup>。

スマートフォンについては、アプリに関する制御も重要となる。すなわちスマートフォンはアプリのダウンロードによって機能が強化され、使い勝手がよくなる一方、Ⅲ章で述べたようにスマホからの情報流出は悪意をもって開発されたアプリ経由で起こりやすい。会社全体としてのセキュリティ対策、ファイアウォールで守られているオフィス内の端末と異なり、「スマートデバイスがマルウェア／ウイルスに侵された際の被害は、ユーザーID／パスワードといったアカウント情報の流出やデバイス内データの流出など、深刻なものになり得る」(小島, 2012b, 103)。このようなことから、モバイル・デバイス・マネジメントはアプリの配信を行うことも必要となる。アプリによる情報流出の危険性があるのに、その配信機能をセキュリティ対策に持たせるというのは、一見矛盾する。しかしモバイル・デバイス・マネジメントの一環として厳しくアプリの有害性チェックを行ったり、ホワイトリストもしくはブラックリストを整備した上で、ダウンロードを当該MDMシステムの管理下で運営されるサイト経由に制限すれば、社員が問題のあるアプリをインストールする危険性は著しく低下することになる。こうしたアプリの配信に加え、アンチウィルスソフトの配信とインストール、一定レベルの危険性ありと判定されたインストール済みアプリの削除といった機能も必要となろう。

モバイル環境やテレワーク環境での利用が増えることを考えるとリモートによる端末本体のモニターと設定、利用可能な機能やサービスの管理、データ保存時の暗号化やログアウト時の消去を行える必要がある。これらは自社全体のセキュリティ対策と情報管理に不可欠であるとはいえ、おそらく社員

個人の感覚としてはかなり「シビア」となりうる。会社貸与の機器ではなく、特に私物を業務に用いるBYO (BYOD) の場合「そこまでやる必要があるのか」という反発や抵抗もありえ、次章で述べる社員側の理解を得ることがここでは大きな課題となる。

より具体的に述べると、遠隔での端末に対するモニターと設定についてはハードウェア構成の把握やOSのバージョン管理、OSに関する修正いわゆる脱獄 (Jail Break) 有無の検知、自社のセキュリティポリシーに端末のスペックや設定等が合致しているかの判別、メールの送受信に関する設定、インストールされているアプリの種類と何をどれ位の頻度で使用しているかの追跡、自社サーバーその他へのアクセスログの取得が行えなければならない。どのようなアンチウィルス・ソフトがインストールされているかなどセキュリティ対策の実施状況を確認し、ウィルスの感染有無と感染している場合はその種類を感知する機能も求められる。加えてウィルス検出時にアラート表示 (警告) したり、さらには除去できることが望ましい。

機能やサービスの管理に関して言えば、利用可能な機能やサービスを制限するといったことができればならない。制限についてはカメラ等組み込みデバイス、音楽再生やインターネット閲覧、その他が対象になりうるが、企業ごと所有者ごとに業務の内容・特性を考慮したうえで制限を設けるようにするのが適当であろう。

データの暗号化については、基本的にはデータを端末に残さないのが情報管理上、無難である。したがって盗難・紛失時のリモートワイプとは別に、システムからログアウトした際に自動的にデータを消去するような仕組みを採用することも考えられる<sup>4)</sup>。しかし業務遂行上どうしても保存したいという場合も考えられるので、その際にデータを暗号化する機能、さらには暗号化したデータに対する利用者認証の導入などアクセス管理機能が必要となろう。

ここで述べた一部の機能を遂行するモバイル・デバイス・マネジメント用のシステムやソフトは既に販売されている。しかし以上の領域を総合的、包括的にカバーするツールは寡聞ながら無いに等しい。具体的なソフト名を出すことは差し控えるものの、「パッケージソフト」を謳いながら部分的な機能領域しか扱っていないものが現状ではほとんどである。

敢えて誤解を恐れずに言うならば、端末の普及に比してセキュリティ用ツールの開発が大幅に遅れているのは明白であり、両者のアンバランスが顕著となっている<sup>5)</sup>。ビジネスパーソンがスマートフォンやタブレット端末を安心して業務に使えるようになるためには、後者の開発は急務であると言える。当事者のモラルとコンプライアンス精神、高いセキュリティ意識、継続的な修正とアップデートはもちろん必要であるが、それを導入すればモバイル・デバイス・マネジメントについては安心というようなオールインワン型のソフトやサービス、それを整備すればBYO (BYOD) を大規模に実践できるというようなシステムの開発が待たれる。

## VI BYOにおけるセキュリティ対策の課題

業務への私有機器利用 (BYO, BYOD) は往々にして社員側、会社側のある種の「幻想」から出発すると考えられる。すなわち「使いなれた私有機器を業務に使わせてほしい」という社員側からの申し出、あるいは「情報化投資を抑えるために業務への私物利用を解禁したい」という会社側の思惑で、これがスタートする。しかし実際には、その企業の業務用端末としてカスタマイズされていないデバイスは当該企業のオフィスにある機器類を利用する際とは勝手が違うことも多く、「自分のスマートフォンを使えたら楽」と思って使い出したら、かえってストレスが大きかったということもある。またスマート端末の管理には多大なコストがかかるため、会社側から見ればBYOはかえって「高くつく」ことも多い。

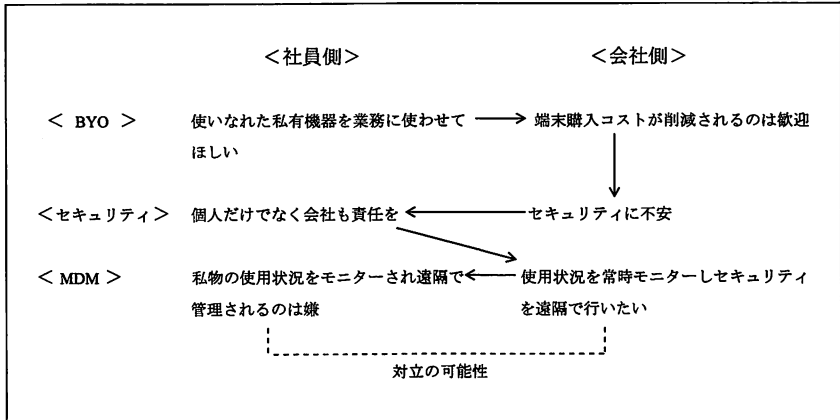
BYOに対する申し出が社員側からなされた場合、前述したようにコストについては結局は期待はずれに終わることが少なくないものの、会社側は通常少なくとも当初は「端末購入コストが削減されるのは歓迎」という立場を取るであろう。しかしすぐに次の段階で「セキュリティが不安」という認識を持つに違いない(図表2)。いずれにせよ現実問題として、BYOの開始にあたり会社側は新たなセキュリティ対策の実施に迫られる。個々の社員としては、ある程度のセキュリティ対策は自分で行えるものの、業務利用を前提にした厳重な対策には専門知識が必要であることもあり、「会社も責任を」あるいは「会

社に任せたい」と一般に考える。つまり個人、特にコンピュータに詳しくないごく普通の社員にできることには限界があるので、セキュリティについては会社へ依存し、難しいことは依頼、ないしは完全な委任すなわちすべて「丸投げ」という態度を示すと考えられる。ここまでは社員側と会社側の利害が基本的に一致しており、対立は生じにくい。

しかし具体的なモバイル・デバイス・マネジメントの方法を検討する段階になると、両者に対立が生じうる。すなわち今日、情報流出は会社の存続を脅かしかねない重大 이슈 となるため、会社側はセキュリティに万全を期すべく「使用状況を常時モニターし、セキュリティを遠隔で行いたい」という意向を持つはずである。またそういう問題意識やセキュリティ・ポリシーは合理的でもある。

ところが社員にとっては私物利用といっても、常にこれを業務に使うわけではない。すなわち本来、会社から支給されるべき業務用ツールを自己負担で購入しているという状態には抵抗感があるはずで、常に自分のスマートフォンやタブレット端末を仕事に使うというスタイルを取る社員は少数派であろう。私物利用といっても、必要に応じて、つまりそうすることが便利なときにだけそうするのであって、普段はオフィスでもモバイル環境でも会社から与えられた機器を使う。そうであるのに自分のスマートフォンの使用状況が常にモニターされ遠隔で端末を管理されるのはプライバシーの侵害と思う社員もいるに違いない。

会社側としては、「だったら私物を使いたいなどと言い出すな」ということになりかねず、ここに両者の間で気持ちの折り合いをつける必要が生ずる。本当に社員側がその必要性を理解し、意義を認識し、気持ちのうえで十分に納得しないと、モバイル・デバイス・マネジメントは失敗する可能性が大きい。機能もさることながら、事前の教育研修、意識のすりあわせが重要なのである<sup>6)</sup>。取えて誤解を恐れずに言うならば、企業の情報システム部門および教育研修部門、コンサルティング会社はこの問題に十分に対応しているようには思われない。



図表2 BYOやMDMに対する社員側と会社側の論理(言い分)

## VII 結 び

スマートフォンやタブレット端末などモバイル環境での利用がしやすい端末が普及し、BYO(BYOD)すなわち業務への私物利用解禁が行われつつある今日、セキュリティもモバイルすなわち遠隔で行われる必要がある。すなわちモバイル環境で端末が利用される場合には、どのような情報がサーバからダウンロードされ、それがどのように処理されているのか、またどういった潜在的リスクに狙われているのか、これに対していかなる対策を講じているのかがわかりにくい。したがってモバイル・デバイス・マネジメントは単に「モバイル・デバイスのマネジメント」を行うだけでなく、それをリモートで臨機応変に行うデバイス・マネジメントでもなければならない。そういう意味で、「モバイルによるデバイス・マネジメント」的な発想がそこでは求められると言える。

また悪意を持った脅威から自社の情報システムを守り、情報管理に万全を期すためには、モバイル・デバイス・マネジメントは総合的、包括的でなければならない。すなわちこれはV章で述べた機能領域のすべてを担うものでなければならない。欠如している機能、脱落しているセキュリティ対策があれば、そこからハッカーやマルウェアが侵入し、情報システム全体を危機にさらすことになるからである。

一方では、VI章で述べたようにモバイル・デバイス・マネジメントは会社貸与の機器ではなく、特に私物を利用するBYO(BYOD)の場合、社員側の理解を得ないと先に進まない。実際には、これにはかなりの困難をとまなう。しかしこの困難を克服し、徹底したモバイル・デバイス・マネジメントを行う覚悟が無いと、ごく小規模の「水漏れ」的な漏洩が大規模な情報流出に拡大し、一部分のほころびや小さなセキュリティ・ホールが情報システム全体の危機をもたらすことになりかねない。当該困難を克服し、万全なモバイル・デバイス・マネジメントを行った企業だけが、スマートフォンやタブレット端末のビジネス利用で大きな成果を得ることになるだろう。

#### 脚 注

- 1) 米国の大手携帯電話会社Motorolaについては次のように記されている。「インターネット検索最大手の米グーグルの傘下に入った米モトローラ・モビリティも社員の約2割に当たる4000人の削減や、拠点の統廃合、製品点数の削減などを進める。同社は世界初の商業用携帯電話を開発するなど無線通信業界の老舗に当たるが、競争激化の影響で直近の16四半期のうち14四半期が赤字だった」(日本経済新聞、2012年8月16日)。尚、この記事中では「中国勢も台頭の兆しをみせており先行きは不透明」という見通しが示されているが、単見では中国メーカーの動向もさることながら、後に述べるようにLTE等高速通信サービスへの対応がスマートフォン市場における今後のシェア争いを大きく左右すると思われる。
- 2) タブレット端末について述べると、「相対あるいは数人の打ち合わせのシーンでは、携帯性と視認性を有効活用することで、プロジェクタやディスプレイ装置を常設していない会議室やセッションあるいは執務席での打ち合わせに、紙の代替として画面上の資料を見ながら手軽に会話できる」(山科、2011、77)という利点がある。また「映像を共有した協調作業が可能となる」という特長もあり、「例えば被災地に赴いたメンバーと現場の状況を共有しながら対策を検討したり、作業指示をすることも可能となる」(前掲同所)。
- 3) 引用した記事では、「『スマホのウイルス対策やMDM(モバイルデバイス管理)を実施しているから安全だ』という考えも早計だ」という立場から、モバイル・デバイス・マネジメントとは別に「スマホやタブレット端末を想定した、新たな認証・制御のシステム」(福田、2012、59)の必要性が説かれている。本研究では、ビジネスパーソンが安心してスマートフォンやタブレット端末を業務に使えるようになるために、モバイル・デバイス・マネジメントは広汎なセキュリティ機能を担うべきという立場から、認証・制御もこの範疇に含めることとした。

- 4) たとえば顧客の個人情報等は端末側に残さない方が安全であり、「端末に取り込むと、セキュリティを強化するための様々な作り込みが発生し、開発に時間がかかる」(小林・山端, 2011, 41)という立場から、データを端末にセーブしないようにしている企業も実際のところ少なくない。
- 5) 一部のMDMソフトはiPhone/iPadとAndroid端末の両方に対応しているが、ほとんどのソフトがどちらか片方を対象として開発されている。「企業にとっては同一機種のスマートフォンを導入するのが、管理の面で効率はよい」が、「iPhone/iPadとAndroid端末を同時に管理することになる可能性も考えられる」(福田, 2011, 47)。特にBYO(BYOD)においては、この同時管理が当然となる。しかしながら現状では、前述したように一方だけを前提にソフト開発が行われており、こうした状況を考えると、端的に言えば「MDMソフト／サービスはまだ発展途上である」(前掲同所)。
- 6) 私物利用解禁においては、情報管理に対する従業員のモラルを高めることも重要となる。すなわち「私物PCの業務利用を検討する場合、『データをコピーされないか。印刷して持ち出されないか』といったことを心配する声が少ない」が、「本気で会社の情報を盗もうとしたら、カメラで画面を撮影したりノートに書き写したりするなど、いくらでも抜け道はある」(吉田, 2011, 37)。したがって内部的起因による情報流出を防ぐ最も基本的な対策は従業員の間に情報倫理を確立することであり、そのための教育研修も本質的に重要となる。

#### 参考文献

- 遠藤英幸(2011)「スマートフォンの業務利用における留意点」,『UNISYS TECHNOLOGY REVIEW』第110号, 93-101.
- 福田崇男(2011)「MDMで安心度を高める」,『日経コンピュータ』3月3日号, 40-47.
- 福田崇男(2012)「社内ネットのスマホ対応を急げーPCと異なる認証・制御が必須ー」,『日経コンピュータ』3月3日号, 58-63.
- 小林暢子・山端宏実(2011)「スマホ&タブレット端末で組織力上げよ」,『日経情報ストラテジー』11月号, 26-52.
- 小島一仁(2012a)「MDMの導入は欠かせない, 社内システム連携も視野に」,『日経コンピュータ』2月2日号, 122-125.
- 小島一仁(2012b)「4ステップでセキュリティ対策ーBYODで難易度があがるー」,『日経コンピュータ』2月16日号, 100-103.
- 山科順一(2011)「テレワークの推進と今後のオフィス環境」,『UNISYS TECHNOLOGY REVIEW』第109号, 73-81.
- 吉田洋平(2011)「私物解禁ー今夏を乗り切る一石五鳥の情報化ー」,『日経コンピュータ』6月23日号, 28-45.