BYOD

山口周平，山口浩平
Shuhei YAMAGUCHI，Kohei YAMAGUCHI

1　はじめに

近年, 安価で使い勝手のよいスマートフォンやタブレットといったモバイル端末の普及が進んでいる．また，個人で利用できるクラウドサービスなどの登場により，私的端末で業務を行う環境が整ってきた．これらの背景から，私的端末を業務で利用することを望む執務者が増加している．そこで，時間や場所を問わない働き方ができる新たなワークスタイルとして，BYOD と呼ばれる考え方が注目されている．しかし，BYOD にはセキュリティ面などでの課題も存在するので，本稿では課題の解決手法についても述べる．

2　BYOD について

2.1　BYOD の概要

BYOD とは Bring Your Own Device の略語で「執務者が自分の持っているモバイル端末を職場に持ち込んで業務に利用する」という意味である．かつて一般的であった，企業から支給される端末を用いたワークスタイルとは異なり，BYOD では執務者が持つ個人の端末を業務で利用する．これにより以下のような利点が生じる．

- 執務者が選好する端末で業務を行うことができるため生産性が向上する
- 使い慣れた端末を引き続き利用することができるため，企業や部署の異動に対応しやすい
- オフィス内だけでなく，出先や自宅においても業務を行うことができる
- 業務用端末の配布にかかるコストを削減できる

BYOD の普及率は調査結果によって差があるものの日本では 10〜20% 程度，世界では 40〜50% 程度である [1]．私的端末に対するそれぞれの姿勢をもつ日本企業の割合を Fig. 1 に示す．

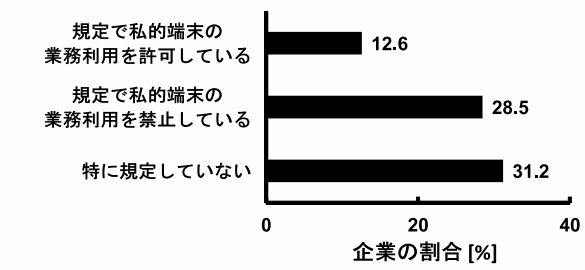

Fig.1　日本企業の BYOD に対する姿勢

Fig. 1 を見ると，私的端末の利用を禁止している企業の割合，規定していない企業の割合が高い．このことから，日本で BYOD が普及していないことが分かる．

また，シャドー IT ユーザと呼ばれる，私的端末を企業に無許可で業務利用する執務者も存在する．実際に，規定を決めていない企業では 62% の執務者，私的端末の利用を禁止している企業では 50% 以上の執務者が私的端末の業務を利用した経験を持つ [2]．シャドー IT ユーザに対しては，紛失・盗難時の対策をとることが容易ではなく，情報管理の面で問題視されている．

今後，端末のさらなる普及と高性能化により，私的端末を業務利用する執務者は，より一層増加すると考えられる．2012 年の調査結果では，私的端末を業務で利用する人は 2016 年までに 1265 万人（2011 年の段階では 192 万人）にまで増えると予想されている [3]．今後は BYOD を前提として，各企業が規定や罰則を作ることが必要である．

2.2　BYOD の課題

BYOD を導入するにあたって主に次に示す 3 つの課題がある．以下の課題を解決するために，私的端末を管理する手法が求められる．

1. 情報管理
   企業の情報を個人の端末で扱うため，端末の盗難・紛失時に社内情報が流出するといった，情報管理に関するリスクが大きい．したがって，情報の流出を防ぐために，企業が執務者の端末に対して，パスワードの設定や位置情報の取得，機能の利用制限などを行う必要がある．
2. 端末環境の違い
   個人で持ち込まれる端末には様々な OS や機種が存在する．機種や OS が統一されていない場合，各執務者が社内で同一のサービスを利用することは容易ではない．よって，企業側がサポート可能な機種を予め執務者に周知しておく必要がある．
3. 労働時間の管理
   私的端末を業務利用する場合，時間や場所を問わず業務が可能である．しかしその反面，公私の区別が曖昧になるという可能性がある．

3　私的端末の管理手法

3.1　MDM

MDM とは Mobile Device Management の略で携帯情報端末のシステム設定などを統合的に管理するシステムである．MDM の概念図を Fig. 2 に示す．MDM を各執務者の端末に導入すると，執務者全体の端末を管理することができるため BYOD の課題であったセキュリ

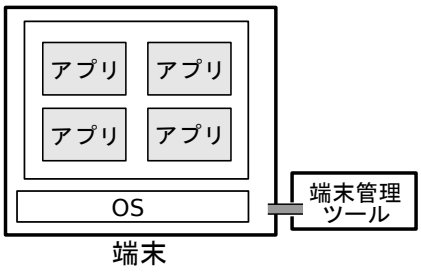

Fig.2　MDM の概念図

ティ面でのリスクが低減される．また，端末の紛失・盗難時には遠隔操作で端末に残っているデータを消去するという方法で対応することが可能である．しかし，MDM は端末全体を管理する手法であるため執務者の私的な端末の利用も管理する．そのため，執務者のプライバシーが侵害されるという問題点が存在する．

3.2　MAM

MDM における執務者のプライバシー保護が困難であるという問題点を改善した新たな解決策が MAM である．MAM は Mobile Application Management の略である．MAM は業務用のアプリケーションとデータを管理するための方法である．MAM の概念図を Fig. 3 に示す．MAM は端末にデータを残すタイプと残さないタイ

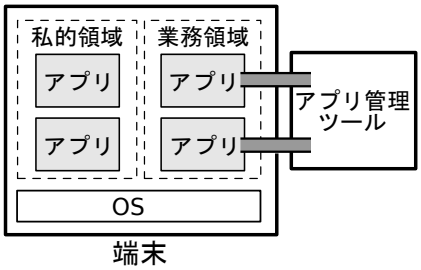

Fig.3　MAM の概念図

プの 2 種類に分けられる．データを残すタイプの MAM は端末内のアプリケーションとデータの部分を Fig. 3 のように私的な領域と業務の領域に分割して管理する．これにより，企業からは個人情報が不可視となり，執務者のプライバシーが守られる．

また，MAM では MDM では不可能だった私的端末内にデータを残さないという利点も存在する．データを残さないタイプの MAM は仮想デスクトップ方式という方法がある．仮想デスクトップ方式とは，サーバ上に仮想的な PC 環境を構築しユーザは自分の端末からそのサーバに接続する．仮想デスクトップ方式では，各執務者の端末環境に依存せず同一のサービスを享受できる，執務者の端末に業務データが残らないという利点が存在する．

さらに，MAM を用いると執務者は会社が配布している業務用アプリケーションを自分の端末にインストールすることができる．業務アプリケーションを使うことによって執務者の業務効率が向上する．

4　導入事例

2011 年に DeNA は BYOD を導入した．導入した目的は，東日本大震災の直後連絡をとることが困難であった経験から，緊急時に社内メールを時間や場所を問わずに確認することだった [3]．しかし，同社は 2012 年のオフィス移転の際に BYOD を原則中止とした．中止へと踏み切った理由は MDM での全執務者の私的端末の管理が現実的に困難であることや，執務者の退職時に私的端末にデータが残ることが挙げられた．DeNA は BYOD を中止した後，企業が端末を配布する方法を採用した．企業支給の端末の場合は予め MDM をインストールでき，端末の利用時にパスワードをことも可能である．さらに，1 分間端末を使用しない場合はパスワードの再入力が必要となり，パスワードを 10 回間違えた場合は端末内のデータを自動消去するように設定することでセキュリティ面のリスクを低減させた．

一方, ヨーロッパのソフトウェア企業の SAP は BYOD に積極的で，日本支社や北米支社などで私的端末の業務利用を認めている [4]．SAP は世界中の 5 万台のモバイル端末をモバイル統合管理ソフトウエアで管理している．このソフトウェアは MAM を用いており，管理用のコンソールから端末データ，アプリケーションの一元的な管理を実現している．

5　BYOD の今後

BYOD のメリットを保ち，課題を解決した考え方として CYOD が注目されている．CYOD とは Choose Your Own Device の略語である．CYOD では，業務利用可能な数種類の端末を企業が提示し，執務者はその中から端末を選択する．執務者はその端末を業務とプライベートの両方で利用出来る．従来の企業が業務専用の端末を配布する方式とは異なり，執務者が私的に利用可能な端末を配布する．CYOD により，企業は BYOD で困難だった各端末の管理が容易になり，セキュリティ面のリスクを減らすことができる．一方，執務者にとっては自分の好みの端末を利用できるので BYOD の利点であった生産性の向上などの利点を維持できる．今後は，BYOD を改善した CYOD が主流になると考えられる．

参考文献

1) ジュニパーネットワークス、モバイル端末ユーザーの世界的な動向調査を実施
https://www.juniper.net/jp/jp/company/press-center/press-releases/2012/pr_2012_05_22-15_00.html
2) －スマホ・タブレット端末の BYOD 実態調査－
http://www.trendmicro.co.jp/jp/about-us/press-releases/articles/20130821051937.html
3) 2016 年に BYOD 利用者は 1,200 万人に-高いシャドー率
http://news.mynavi.jp/news/2013/01/18/088/
4) 【事例】DeNA が BYOD をやめた理由
http://techtarget.itmedia.co.jp/tt/news/1209/20/news05.html
5) SAP ジャパン流の Bring Your Own Device
http://www.itmedia.co.jp/enterprise/articles/1208/02/news005.html