スマートモバイル BYOD 実現の現実解
―― MDM やシンクライアントに頼らない新たな BYOD 実現方法

丸　尾　和　弘

要　約　スマートフォンやタブレット端末などのスマートモバイル端末を BYOD（Bring Your Own Device：私物端末を業務の中で利用するスタイル）で活用する場合に、会社支給端末での運用とは異なり特に意識して検討しなければならない要点がある。それらの要点を考慮すると、私物端末については「MDM（Mobile Device Management）で端末を管理する」という手段はそぐわない。また、BYOD で利用される端末は、タブレット端末よりもスマートフォンが主流であるため、スマートフォンでの利用を意識したユーザビリティが重要である。

これらのことから、BYOD の実現には「セキュリティの確保」「端末運用管理の簡便性」「利便性・ユーザビリティの確保」という、相反する要望を叶える手段が求められる。

これらの要望を叶える BYOD 実現の現実解として、現時点ではモバイルアクセスゲートウェイ方式が最も現実的な解決策の一つであると言える。

1. は　じ　め　に

スマートフォンやタブレット端末などのスマートモバイル端末[*1] が登場し、コンシューマ市場への普及が進んでいる。また、これらのスマートモバイルの利便性の高さがビジネスの現場にも広く認知され、業務の中でのスマートモバイルの活用を検討している企業も多い。そして今、多くの企業が直面しているキーワードとして、BYOD（Bring Your Own Device：私物端末を業務の中で利用するスタイル）が挙げられる。BYOD は、従業員にとっては普段使い慣れた使いやすい端末を業務の中でも使える、というメリットがある。また企業側にとっても、端末や通信のコスト負担軽減や、従業員のワークスタイルを変革し企業としての競争力を強化するという目的を果たす手段として期待されている。従業員と企業経営者の双方にメリットがあるため、大きな注目を集めている。しかし、いざ実際に BYOD を実現しようとすると、様々な検討すべき課題に直面する。実現手段、利用制度、勤務制度、企業風土、など様々な課題があるが、本稿ではそれらのうち、実現手段の課題について考察し、一つの現実的な実現手段を提唱する。

2.　スマートモバイル BYOD を実現する三つのポイント

スマートモバイル端末を会社支給して活用する場合と比べて、BYOD で活用する場合に意識して検討しなければならないポイントは大きく三つ挙げられる。

ポイント 1：セキュリティ対策が万全であること

スマートモバイル端末は、PC とは OS の構造や実際の使われ方が違うため、さらされるリスクも異なる。そうなると、従来の PC とは異なるセキュリティ対策が必要となってくる。万

全なセキュリティ対策が必要なのはもちろんだが、セキュリティを強固にすればするほど、スマートモバイル端末が本来備えている利便性が損なわれてしまう。

会社支給端末であれば、特定の利用目的が果たせさえすれば、その他の利便性などのベネフィットは必要ない、という考え方もあるが、BYOD の場合、特にこのセキュリティと利便性のバランスを取ることが非常に重要かつ難しい問題となってくる。そこには、会社支給端末とは異なる、BYOD ならではのセキュリティの守り方というものが求められる。

ポイント 2：個人の私的利用に制限をかけないこと

私物端末に対して会社が個人の私的利用にまで利用制限をかけることは現実的ではない。例えば、インストールしてもよいアプリケーション（以下、アプリ）/インストールしてはいけないアプリというものを会社が規定し、規定違反をしていないかどうか私物端末を監視する、というわけにもいかないであろうし、本来個人の所有物である端末のカメラ機能や外部メディア書き込みの機能自体をロックしたりすることも端末所有者からは許容されないだろう。

端末の設定情報を管理する MDM（Mobile Device Management）ツールを入れることでこれらの制限をかけることは可能だが、MDM による制限を実施するということはすなわち個人の私物端末を企業が管理するということになってしまう。BYOD を実現するためには、MDM に頼らないセキュリティ制御の仕組みが必要となる。

ポイント 3：端末運用が簡便・シンプルであること

私物のスマートフォンは、個々人が好きな端末を自由に選択するものだが、端末の機種や OS のバージョンごとに設定方法や設定確認方法が異なると、もはや企業の情報システム管理者は対応しきれない。そのため、機種依存性は極力排除した設定で済むような仕組みである必要がある。

また、私物端末は 2 年に 1 回程度の頻度で機種変更をすることが一般的だが、低頻度であるため、新端末に替えた時に社内にアクセスするための設定方法が分からなくなり、情報システム管理者に問い合わせることになるのは容易に想像がつく。一人ひとりは 2 年に 1 回程度の頻度かもしれないが、情報システム管理者の方は毎日のように問い合わせを受け、対応に追われることになってしまう。

このような事態を避けるために、BYOD の実現には、端末運用が簡便・シンプルである必要がある。

3.　BYOD の実現手法

本章では、現在一般的とされている三つの BYOD 実現手法を挙げ、それぞれの特徴と課題を述べる。

3. 1　BYOD の実現手法　その 1：MDM 方式

最近の MDM ソリューション市場では、業務の中で使ってもよいアプリケーションを管理する MAM（Mobile Application Management）機能や、端末内に持つ情報コンテンツのセキュリティを管理する MCM（Mobile Contents Management）機能も包括した、業務利用における総合的なスマートモバイル端末管理ソリューションとして Enterprise Mobility Manage-

ment（EMM）と称する製品が市場を先導している。EMM 製品の中には、私的利用と業務利用でデータやアプリケーションの領域を分離して管理することができる製品がいくつかある。確かにこの機能を適用することにより、BYOD を実現することはできるかもしれないが、EMM 製品による BYOD の場合、いくつかの矛盾や運用上の限界が見え始めている。そのうち二つを本節で説明する。

3. 1. 1　リモートワイプは万全ではない

リモートワイプ機能が欲しい理由は、ずばり「端末紛失時などに端末内から削除したい情報（業務に関わる情報）があるから」である。そして、端末内に業務に関わる情報を保持させる理由は、「ネットワークが繋がらない状況でも業務に関わる情報にアクセスしたいから」であろう。

しかし、ネットワークが繋がらない状況では、企業の情報システム管理者がネットワーク越しに端末内の情報や設定を削除するリモートワイプを実行しても、その処理は端末には届かず、リモートワイプは実行されない。例えば、交通機関などの遺失物預り所で電波が届かない状況にあったり、充電切れで電源がオフになってしまったり、端末を拾った人が意図的に通信機能をオフにしたり通信用 SIM カードを抜いたりするなど、ネットワークが繋がらない状況は意外と多い。米国のジュニパーネットワークス　モバイル脅威センターによると、スマートモバイル端末の紛失時にリモートワイプが成功しデータをロック・消去できたケースはわずか 7% という調査結果[1]もある。

3. 1. 2　私的利用への制限やプライバシーの侵害

スマートモバイル端末を MDM の管理下に置くことで、情報セキュリティを確保するために端末にさまざまな制限をかけることができる。例えば、

- お客様の名刺や会議のホワイトボード、社内資料などをカメラで撮影されることを防ぐために、カメラ機能を禁止する
- オンラインストレージと同期するようなアプリのインストールを制限する
- 怪しいアプリが端末にインストールされていないかどうかを情報システム管理者が把握する
- 端末紛失時に端末の所在を探すために、業務時間外でも GPS 位置情報を情報システム管理者が把握できる

しかし、いくら業務上の情報セキュリティを確保するためとは言え、私物端末に対して端末機能の制限をかけたり、私的な利用に関する情報まで会社に把握されたりしてまで、私物端末を業務に使わせて欲しいとは思わないのではないだろうか。また、情報システム管理者としても、企業の所有物ではない私物端末の管理・把握までしたいとは思わないだろう。

すなわち、MDM 製品を活用した BYOD の実現は、日本企業では受け容れられにくいのが実情である。

3. 2　BYOD 実現手法　その 2：シンクライアント方式

クライアント端末側に情報コンテンツを残さない手段として、シンクライアントや仮想デス

クトップ（VDI）/リモートデスクトップという手法が挙げられる。これらのいわゆるシンクライアント方式であれば、業務端末であっても私物端末であっても同等に情報セキュリティを確保することができるが、本節で挙げるような課題もある。

3. 2. 1　デスクトップユーザーインターフェースの操作性

シンクライアント方式の場合、クライアント端末には従来の Windows PC のデスクトップ画面が画像イメージとして表示され、その画面をシンクライアント端末側で操作することになるが、物理的なマウスとキーボードがないスマートモバイル端末でこの画面を操作しようとするとなかなか難しい。

私物のスマートモバイル端末での利用を目的とした場合、いつでも常に持ち歩いていてちょっとした合間時間にさっと取り出して使う、という使い方がメインになるが、そのようなケースで使用する端末は大半の場合、タブレット端末ではなくスマートフォンであることが想像される。タブレット端末程度の画面サイズがあればシンクライアント方式でも慣れてくればある程度は使いこなせるようになるかもしれないが、スマートフォンの画面サイズではシンクライアント方式で使いたいとは思わない人が多い。

3. 2. 2　社内ネットワーク・デスクトップ環境の整備

シンクライアント方式の懸念事項のもう一つは、社内のデスクトップ環境に安全にアクセスさせる環境を用意するには意外とコストと手間がかかるという点である。

普段社内で各自の物理的な PC で執務を行っている場合、その社内 PC のローカルディスク内にファイルやデータが保管されていると、その社内 PC に対してリモートデスクトップアクセスしないといけないことになる。通常、社内のデスクトップ環境にアクセスするためには、VPN で社内 LAN に入り込む必要があるが、その場合、実はリモートデスクトップ以外にもさまざまな社内システムにアクセスできるようになってしまうため、セキュリティを維持するということが難しい。

この課題を解決する手段としては、物理的な PC ではなく仮想デスクトップ環境（VDI）を用意し、普段から社内の自席においてもこの VDI 環境を使用するようにするという案があるが、これを実現するには大がかりなネットワーク構成やサーバ構成を組むことになり、コストもかかる。

つまり、スマートモバイルのために手間とお金をかけてシンクライアントやリモートデスクトップ環境を整えた割には、私物端末のメインであるスマートフォンでは使いにくい仕組みができあがる、という結果になってしまう。

3. 3　BYOD 実現手法　その 3：セキュアブラウザ方式

BYOD を実現する第三の手段として、セキュアブラウザ方式という手段が普及しつつある。

社内システムにアクセスさせる際には、スマートモバイル端末が標準で備えているブラウザ（Safari や Chrome など）ではなく、セキュリティが確保された専用ブラウザ（＝セキュアブラウザ）のみが社内システムにアクセスできるようにモバイルアクセス環境を構築する、という手法である。この方式にも、本節で挙げるような懸念事項がある。

3. 3. 1　Web システムのみという利用制限

セキュアブラウザ方式は、スマートモバイル端末側で使用するアプリケーションはあくまで Web ブラウザであるため、利用できるのは Web システムのみ、という制約がある。また、端末側では Web 画面を操作することになるため、何か操作するたびに Web 通信が発生し画面を更新する、という動きになり、端末ネイティブアプリのような操作性を実現することは難しい。

3. 3. 2　ネットワーク設定・構成の変更や認証環境の整備

端末自体の認証や暗号化通信の確保、複数のアクセス先システムへのアクセス制御までを実現しようとすると、セキュアブラウザ単体では実現が難しく、さまざまなネットワーク装置の構築や設定が必要になってくるため、より複雑なシステム構成になりがちである。

4.　BYOD 実現手法　その 4：モバイルアクセスゲートウェイ方式

前章で紹介した三つの BYOD 実現手法には、それぞれ一長一短があり、自社の置かれている状況によって向き不向きがある。しかしいずれの手段にも共通しているのは、“セキュリティ確保を重視するあまり、実利用上の不便さやシステム環境の構築/管理の手間が見落とされたまま手段の選択を迫られがち”ということである。これらの手段は、利用者にとってもシステム管理者にとっても望ましい姿が実現できているとは言い難い。

そこで新たに着目されているのが、モバイルアクセスゲートウェイ方式である。

モバイルアクセスゲートウェイ方式とは、標準的な Web アクセス技術を活用しつつも、端末側ではブラウザではなくネイティブアプリとして動作する専用アプリを使用する方式である。最大の特長は、端末には業務に関わる情報を一切残さないため、MDM に頼らずにセキュリティを確保できることである。

このモバイルアクセスゲートウェイ方式のソリューションの一つとして、日本ユニシスが提供するクラウドサービス「mobiGate」が挙げられる。本章では mobiGate について解説する。

4. 1　mobiGate のしくみ

mobiGate は大きく以下の三つのコンポーネントで構成されている（図 1）。

① スマートモバイル端末にインストールする mobiGate ネイティブアプリ
② 日本ユニシスのクラウド基盤上に構築された mobiGate ゲートウェイサーバ
③ ユーザ企業内に設置する mobiGate アダプタサーバ

本節では、実際の利用の流れに沿って mobiGate の仕組みを解説する。

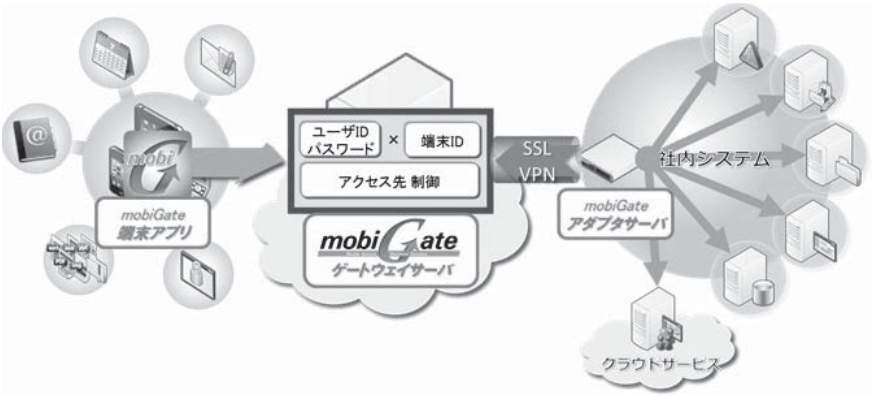

図 1　mobiGate 概念図

4. 1. 1　mobiGate における認証

端末には予め mobiGate アプリをアプリストアからインストールしておく。この mobiGate アプリを起動すると、mobiGate ゲートウェイサーバにアクセスし、そこで認証をする。初回ログイン時に mobiGate アプリが、その時に使っている端末の個体識別番号（端末 ID）を生成し、ユーザ ID との紐付け登録を行う。それ以降は、ユーザ ID/パスワードと端末 ID を認証情報として用いるため、仮にユーザ ID/パスワードが漏洩し、他の端末からそのユーザ ID/パスワードを使ってアクセスされても、認証が通らない仕組みになっている。

4. 1. 2　ユーザごとのアクセス先システムの制御

ゲートウェイサーバで認証が通ると、そのユーザがアクセスを許可された業務システムだけが一覧メニューとして表示される（図 2）。例えば一般社員はメールと社内掲示板だけ、営業担当者は SFA/CRM も、役職者はワークフローの承認システムも使える、という具合にユーザごとにアクセスできるシステムを制御することができる。

図 2　ユーザごとのアクセス先システム一覧メニュー画面

4. 1. 3　mobiGate ネイティブアプリの利用

メニュー画面から、各接続先システムを mobiGate アプリで利用する。メーラーやスケジューラー、アドレス帳検索、ドキュメントビューワーなどがスマートモバイル端末のネイティブアプリとして用意されており、スマートフォンの画面サイズでも視認性が高く、コンテンツを半

同期型で取得しながら親指一本で軽快に操作する操作性を実現している。この辺りの操作性や視認性がシンクライアント方式とは異なるため、ユーザにとって使いやすい仕組みとなっている（図 3）。

図 3　mobiGate クライアントアプリ画面イメージ

そして mobiGate アプリをログオフすると、閲覧してきたメールやファイル、アドレス帳などのデータや、Web アクセスの Cookie、キャッシュなどは強制的に削除されるため、業務に関わる情報は端末には一切残らない。

4. 2　mobiGate の特長

4. 2. 1　スマートモバイル端末ならではの操作性

モバイルアクセスゲートウェイ方式は、端末側ではネイティブアプリを使用するためセキュアブラウザ方式やシンクライアント方式とは一線を画したスマートモバイル端末ならではの操作性を体験できる、という点が大きな特長である。

特に、BYOD を念頭に置いた場合、私物端末として常に肌身離さず持ち歩いているデバイスは PC やタブレット端末ではなくスマートフォンであろう。スマートフォンを業務の中で利用する場合、その操作性や情報へのアクセシビリティというのは非常に重要になってくる。

4. 2. 2　スマートモバイル活用用途の拡張性

セキュアブラウザ方式ではアクセスできるシステムが Web システムや Web サイトに限定されてしまうが、mobiGate の場合、Web システムはもちろん、Web 化されていないシステムに対してもスマートモバイル端末からアクセスできるという活用用途の拡張性の高さがある。スマートモバイル端末を業務の中で活用することを検討した場合に、単にメールや自分のスケジュールだけ見られればよい、というレベルではもはや利用者（従業員）の業務環境としては十分とはいえない状況になりつつある。

4. 2. 3　複数のポイントを押さえた万全のセキュリティ

スマートモバイルならではの操作性や拡張性、利便性を実現しつつも、業務に関わるセキュリティを確保する、ということがスマートモバイル活用における至上命題である。その点において、mobiGate では、以下の四つの点で万全のセキュリティを確保している。

1．電子証明書に頼らない mobiGate アプリ独自の端末個体識別番号による認証を標準装備

2．業務に関わる情報は端末の中には一切保存させない、ゆえにリモートワイプなども一切不要
3．業務に関わる情報は mobiGate アプリ内でのみ閲覧可能とし、他のアプリへの情報の受け渡しを許可しない
4．通信経路上も SSL 暗号化通信を確保し、mobiGate アプリだけが社内システム/社内サイトにアクセス可能

4. 2. 4　シンプルなシステム構成

mobiGate の特長の一つとして、シンプルなシステム構成であるためシステムの導入や運用が非常に簡便であることが挙げられる。

mobiGate を構成する要素として、①スマートモバイル端末用の『クライアントアプリ』 ②クラウド側の『ゲートウェイサーバ』 ③各利用企業社内に設置する『アダプタサーバ』 の三つに分解されるが、これらのうち、ポイントとなるのは、ゲートウェイサーバとアダプタサーバの接続形態である（図 4）。アダプタサーバは、DMZ で外部ネットワークに公開するのではなく、社内 LAN 内に設置する。そして、この社内のアダプタサーバからインターネット上のクラウドゲートウェイサーバにアウトバウンド方向に port:443 を使って SSL-VPN セッションを張る。そのため、Firewall やネットワーク機器において、外部から社内に通信が入ってくるようなインバウンド方向の設定変更やポリシー変更をする必要はない。また、DMZ に VPN ルータを設置したり、認証局を立てたりする必要もない。さらに、クライアント端末の認証は mobiGate アプリが実装しているため、端末認証のための電子証明書を発行・配布する必要もない。

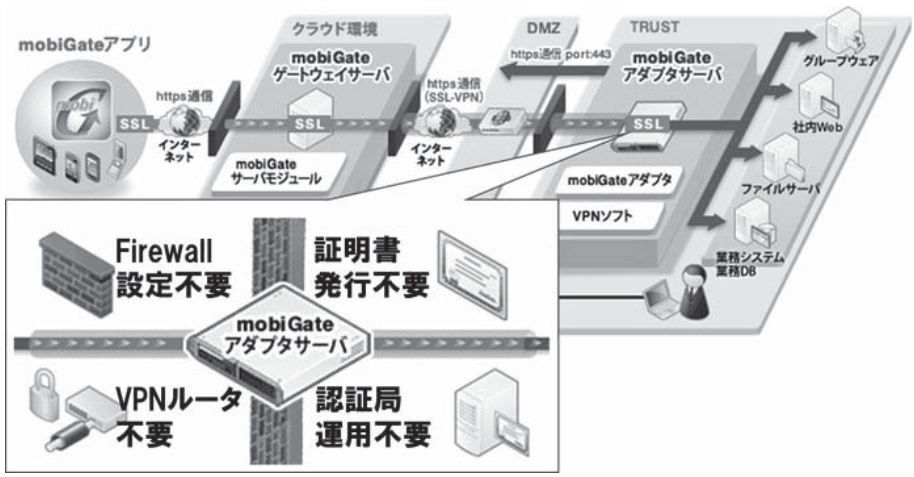

図 4　mobiGate アダプタサーバによるシンプルな構成

以上の特長により、利用者は mobiGate アプリをインストールするだけで、端末に様々な設定や制約を施さなくても簡単に利用できるため、利用者にとって非常に分かり易い仕組みになっている。また、企業のシステム管理者にとっても、利用者の私物端末の設定を管理したりリモートワイプしたりするなどの管理の手間がかからずに業務システムを安全に利用させることができる。

5. スマートモバイル BYOD 実現の現実解

ここでもう一度、スマートモバイルの BYOD を実現するために必要なポイントを振り返ってみる。

ポイント 1：セキュリティ対策が万全であること
ポイント 2：個人の私的利用に制限をかけないこと
ポイント 3：端末運用が簡便・シンプルであること

セキュリティを保つためには、社内へのアクセスの入り口における認証強度、端末の中の情報コンテンツ、不正な操作による情報漏えいなど、さまざまなポイントを考慮し、それぞれに適切な対策を採らなければ、万全なセキュリティを確保することができない。そして、さまざまなセキュリティポイントを守るためには、さまざまなセキュリティ対策ソリューションを組み合わせて適用しなければならないが、そうなると複雑な仕組みができあがってしまい、コストもかさみ、その環境を維持・改善していくための運用も煩雑・複雑になってしまう。

また、セキュリティ確保のために端末そのものに対して機能制限をかけてしまうと、個人の私的利用に制限をかけることになってしまったり、自社のシステム管理者が各個人の私物端末を管理することになってしまう。

そのような観点において、モバイルアクセスゲートウェイ方式である mobiGate の場合、mobiGate アプリを一つインストールするだけで、これらの懸念事項は解決される。様々なセキュリティポイントをワンストップで包括しているということが、上記三つのポイントを押さえるためのキーポイントとなっているのである。

6. お わ り に

スマートモバイルの市場は、機種や OS バージョンなど、変化の早い領域であるため、このスピードに追随できる仕組みである必要がある。そういった観点では、自社で独自のシステム基盤やアプリケーションを開発していくよりも、クラウドサービスを利用する方が現実的であると言える。また、実現手段としても、今後も様々な新しい方式や技術が世の中に出てくるであろう。絶対的な正解手段というものを待っていると、その間に周りの企業と比べて、企業競争力の面で取り残されていってしまう。そのため、今あるものをいち早く活用し、よりよい仕組みが出てくればそれに切替えていく、という柔軟性も必要である。

本稿では様々な BYOD の実現手段について考察してきた。現時点では、モバイルアクセスゲートウェイ方式はスマートモバイル BYOD 実現のための最も現実的な解決策の一つであると言えるが、現状の形式に拘らず今後も新しい技術や方式を取り込み、よりよいサービスとして進化させていきたい。

関連情報：
日本ユニシスのモバイルアクセスゲートウェイソリューション『mobiGate』
http://www.unisys.co.jp/services/mobile/mobigate/
日本ユニシスのエンタープライズ・モバイルソリューション
http://www.unisys.co.jp/services/mobile/
本件に関するお問い合わせ先：smartmobile-box@ml.unisys.co.jp

＊1　本稿では、スマートフォンやタブレット端末をスマートモバイル端末と呼び、それらを用いて業務を行うことを単にスマートモバイルと呼ぶ。

参考文献　［1］「2011 Mobile Threats Report」，ジュニパーネットワークス，2012年2月，https://www.juniper.net/us/en/local/pdf/additional-resources/jnpr-2011-mobile-threats-report.pdf（2015年4月30日確認）

執筆者紹介　丸　尾　和　弘（Kazuhiro Maruo）
2001年日本ユニシス(株)入社。業種横断型のソリューション企画・ビジネス企画部門に従事。現在は、スマートモバイルを企業の業務の中で活用するエンタープライズ・モバイル領域における、ソリューションの企画、マーケティング、提案支援活動を担当。