BYOD（私物端末の業務利用）導入成功のカギ

スマートデバイスによるワークスタイル変革に向けて

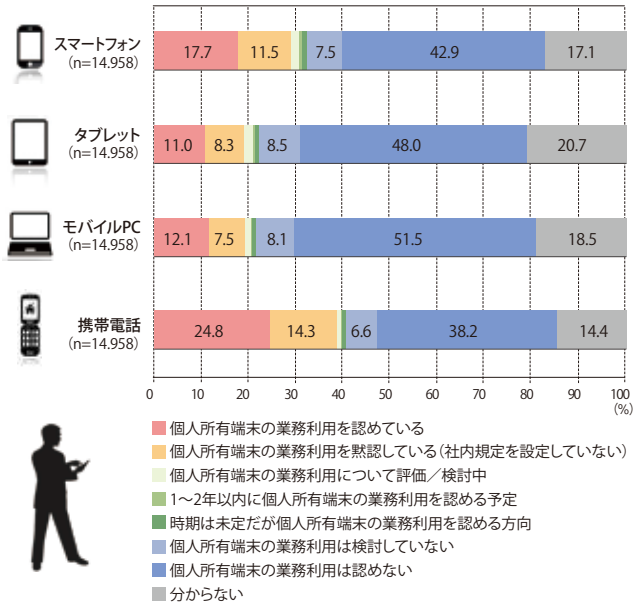
BYOD（ビーワイオーディー）は、「Bring Your Own Device」の頭文字を取ったもので、従業員が私物のスマートフォンやタブレットを企業内に持ち込んで業務に活用することを指す。 従業員は慣れ親しんだ端末で場所を選ばず仕事ができ、会社はコスト削減につながると言われているが、セキュリティに対する懸念から導入を躊躇する企業も多い。日本の BYOD 動向とともに、 先行する米国の実情から、 BYOD 導入成功のカギを探る。

日本におけるBYOD進行状況

●意外に多い？ 私物利用を黙認する「シャドー IT」

日本のBYODの実情を見る前に、スマートデバイス（スマートフォン・タブレット）の導入率について見ていく。「企業IT動向調査2013」によると、スマートフォンを導入済み（一部導入も含む）の企業は28.0%、タブレットは27.0%で、2010年と比較するとスマートフォンは約3倍、タブレットは約4倍に増えている。企業規模別（従業員数別）に見ると、1,000人以上の大企業において、特にタブレットの導入が進んでおり、導入済み企業は34.1%と、1,000人未満の企業より10ポイント以上高い。

では、BYODの導入率はどうだろうか。「2013年 国内BYOD利用実態調査」によると、「個人所有端末の業務利用を認めている（BYOD）」と「個人所有端末の業務利用を黙認している（シャドーIT）」を合わせた導入率は、「スマートフォン:29.2%」「タブレット:19.3%」「モバイルPC:19.6%」「携帯電話（スマートフォンを除く）:39.1%」となっている（図1）。



出典：IDC Japan プレスリリース 2013年1月17日

■図1 モバイルデバイス別 BYOD利用状況

また、同調査の分析によると、BYOD／シャドーIT導入率は、従業員規模が大きくなるに従い低くなっている。さらに、産業分野別では、導入率の高い業種は、流通／小売／卸売、一般サービス、建設／土木、低い業種は、金融、製造、自治体／教育となっている。

2つの調査結果を単純に比較することはできないが、スマートデバイスの導入率とBYOD／シャドーITの導入率は大きく離れてはいない。スマートデバイスの導入によって、事実上はシャドーITも含めた私物端末の業務利用が進んでいる可能性がある。BYOD対シャドーITは6対4程度となっており、シャドーITの存在は大きい。

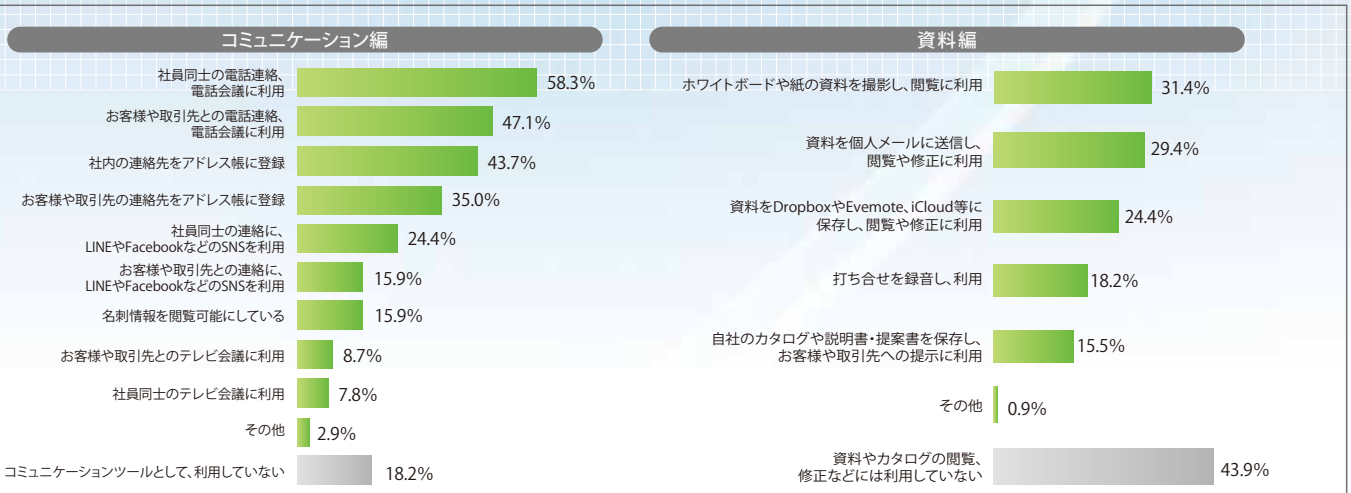
●今後の BYOD の進展は？

米国のBYOD導入率は、調査によっては7割とも8割とも言われ、日本のBYOD導入の遅れが際立っているように見える。しかし、米国では私物PCの業務利用や、企業が購入費用を出して従業員が自由に端末を選択する場合もBYODに含む。一方、日本のBYODは私物PCや企業が費用を負担する支給端末を含まないことが多い。

こうしたBYODの定義そのものの違いによって、米国と日本の差が大きく見えてしまっている可能性はあるものの、アナリストが指摘するのは「企業文化の違い」だ。欧米では成果主義のもと、「従業員はツールの費用を自らが負担し、企業は従業員の働きやすさを支援する」と考え、一方の日本では「就労時間で賃金がもらえ、ツールは企業が支給すべき」と考える。あるいは、欧米よりもさらにBYODの導入が進んでいる新興経済大国「BRICs」では、従業員の入れ替わりが激しく、企業が支給した端末やデータが盗まれることが多いという背景があり、これは欧米とも日本とも事情が違う※。

そしてもう1つ、日本でBYOD導入の大きな阻害要因となっているのは、日本企業のセキュリティに対する意識の高さだ。SSL VPNを使ったPCによるリモートアクセスを含め、何らかのモバイルアクセスを従業員に許可し、既にそのメリットを享受してきた企業は、BYODの利便性を理解しやすいだろう。しかし、あらゆるリモートアクセスを禁じている企業が依然として多いこれまで

※ブラジル、ロシア、インド、中国の企業を対象に行った調査



■図2 私用スマートフォンの業務利用方法

出典：MMD 研究所「職場での私用スマートフォンの利用実態調査」

の日本の実情では、前述の企業文化の違いも手伝って、現時点では海外と比較してもBYOD導入率は低い。

では、今後はどうだろうか。前述の調査で、「BYOD／シャドーITのユーザー数は、2011年の192万人から2016年に1,265万人まで拡大、2011年～2016年の年間平均成長率は45.8%」と、高い成長率を予測している。クラウドの進展や、PCよりもスマートフォンを好む世代の台頭が進む中で、企業におけるスマートデバイス活用は拡大していくと見られ、それに伴ってBYOD導入も、シャドーITを含めて進展することが予想される。このシャドーITの状態を作らず、効果的にBYODを運用することが、これからの企業の課題となってくる。

● BYOD による効果

既に私物端末を業務利用しているビジネスパーソンは、どういう効果を感じているのだろうか。「職場での私用スマートフォンの利用実態調査」によると、「仕事の効率・スピードの向上（43.0%）」「社内コミュニケーションの円滑化（33.4%）」「情報収集力の向上（27.6%）」「顧客とのコミュニケーションの円滑化（25.3%）」といった効果が出ている。

活用例としては、コミュニケーションの分野では「社内連絡（58.3%）」が最も多く、以下「社外連絡（47.1%）」「社内連絡先の登録（43.7%）」と続く。また、資料の分野では「資料を撮影し、閲覧（31.4%）」「個人メールに送信し、閲覧・修正（29.4%）」「クラウドサービスに保存し、閲覧・修正（24.4%）」と続く。一方、資料の閲覧、修正などに私用スマートフォンを利用していないビジネスパーソンは、43.9%にとどまっている（図2）。

BYODによって、個人的に使っているアプリケーションの業務利用（Bring Your Own Application）も広がりつつあり、さらには「あらゆる物」という意味で「X」を使った「BYOX」というコンセプトも登場している。「ITpro会員100万人に聞く！ICT大調査」によると、個人的に使っているクラウドサービスを業務利用している人は22.2%を占める。こうした結果からも、使い慣れた端末とクラウドサービス、アプリケーションを活用することで、自らの仕事の生産性を高めているビジネスパーソンの実態が見えてくる。

BYODに求められるセキュリティ対策

●ユーザー中心の運用アプローチとポリシー策定

組織、業務内容、従業員によって、生産性を向上させる手段は異なる。コミュニケーションを円滑化したい従業員に対しては、BYODで情報系システムのみへのアクセスを許可すればよい場合もあるだろう。あるいは、外出先でも最新データを参照して売上につなげたい従業員に対しては、セキュリティを十分に確保した支給端末の利用規定を理解させたうえで、社外からの業務系システムへのアクセスを許可する場合もあるだろう。最優先すべきは、「私物端末を業務で利用させるか否か」という端末中心の運用アプローチではなく、「どれだけ従業員に自由を与えて生産性を向上させられるか」というユーザー中心の運用アプローチだ。

実際、世界10か国の大規模組織のIT担当責任者を対象に行った調査によると、ユーザー中心でBYODに取り組んでいる組織のほうが、短期間で大きな成果を上げているという。

「BYODの現状と特性 ～あなたの組織はどのパターンですか～」では、私物端末は既に個人によって利用が始まっているものであり、その状態をコントロールすることは困難と捉えるべき、と述べている。そして、許可できる業務範囲を設定し、そのうえで端末や情報、アプリケーション、マーケット（アプリケーションの入手先）、企業（資産）側へのアクセス手段（社内無線LAN、VPN、通信事業者閉域網）のそれぞれについて留意点を検討していくアプローチが必要となる。

同資料では、管理者の心得として、次の4つを記している。

1. 申請は、許可・未許可の端末を区別する機会であり、終了時の業務データ廃棄も含め、規定について互いに合意するための必要なプロセスとなる。業務範囲や労務管理基準、社内ルールなどの規定を明確にしておく。

2. 業務時間外でも従業員が望めば業務利用できるため、労働時間の管理が困難になる。裁量労働制であってもなくても、労務管理と費用負担については、業務内容に合わせて関係部門と協議しておく。
3. 企業が情報資産を管理し保護するように、従業員も自分の情報を管理し保護したいと考える。プライバシーに深く関わるデータを取得する場合は、利用目的と取得範囲、管理方法を伝えておく。
4. BYOD導入を決めた場合は、支給端末とは違う長所を生かし、ワークスタイル変革のために最大限活用する。企業のセキュリティポリシーとの兼ね合いや費用など、さまざまな検討を行ったうえで最適な意思決定をする。

BYODでは、後述するセキュリティ対策ツールだけでなく、社内規定や運用ルールも含めた「BYODポリシー」を従業員が遵守できる仕組み作りが必要となる。米国のBYOD導入で失敗した企業に関する調査では、「ほとんどは、データの削除などの操作をユーザーに任せる方法をとり、BYODポリシーが欠如している」という分析がある。また、「BYODを無制限に許可してきた企業は、自由主義のアプローチの継続は困難であり、より強化された管理や優良な戦略が必要になってくることを認識し始めている」と指摘するアナリストもいる。こうした指摘は、ポリシーのないBYODの危うさを示している。

「スマートフォンの安全な利活用のすすめ ～スマートフォン利用ガイドライン～」は、スマートフォンの導入は事実上のBYOD状態になってしまう可能性があると警鐘。スマートフォンの業務利用開始後のセキュリティチェック項目として、「スマートフォン専用ネットワークのトラフィックのモニタリング」「認証ログの定期的な確認」「汚染されたスマートフォンの接続や、不適切な状態（root化、Jailbreakによりセキュリティが解除された状態など）での利用を検出するための対策」を挙げている。

●スマートデバイスに特化したセキュリティ対策ツールの登場

スマートデバイスのセキュリティ対策として、従来のモバイルPCで慣れ親しんだアクセス制御、ファイアーウォール、VPN、シンクライアント、仮想デスクトップなども応用されているが、スマートデバイスに特化した「MDM（モバイルデバイス管理）」「セキュアブラウザ」「スマートフォン仮想化」といった製品やサービスも、各ベンダーから次々と登場しており、日本企業が最も懸念するスマートデバイスに特有のセキュリティ対策は整いつつある。

・MDM（モバイルデバイス管理）

複数の端末を統合的に管理することが可能。各端末にインストールしたエージェントアプリに対して、端末認証や構成設定の配信、アプリケーション利用制限、さらには紛失・盗難対策となる端末のロック（リモートロック）や、初期化およびデータ削除（リモートワイプ）といった機能を実行できる（表1）。最近ではオンプレミス型に加え、SaaS型の提供も増えている。

資産管理	
端末認証	電話番号、機体番号、MACアドレスなどをキーに、認証された端末のみMDM接続を許可する。
端末情報の取得	OSバージョン、端末識別子、デバイス名などの端末情報を収集し一元管理する。
構成設定の配信	構成プロファイルを遠隔から配信／設定する。
アプリケーション管理	
アプリケーション情報の取得	パッケージ名、バージョンなどのアプリケーション情報を収集し一元管理する。
アプリケーション利用制限	企業ポリシーに沿ってアプリケーションの利用を制限する。
アプリケーション配信	アプリケーションのインストール／アンインストール通知を端末へ配信する。スケジュール実行も可能。
紛失・盗難対策	
リモートロック	遠隔から端末をロックする。
リモートワイプ	遠隔から端末を初期化する。また、挿入されたSDカードのデータを削除する。
位置情報取得	端末の位置情報を取得し一元管理する。
ローカルロック設定	パスワード利用を義務化。文字種、最小文字数、有効期限などを設定する。
ローカルワイプ設定	ローカルロックの解除失敗時に、初期化する。また、挿入されたSDカードのデータを削除する。
不正利用対策	
カメラ制御	カメラ機能の使用可否を制御する。
Jailbreak/root化検知	端末のJailbreak／root化状況を監視する。
エージェント制限	システムのクライアント機能に対するアンインストール操作を制限する。
その他	
管理者機能	運用形態に応じた管理者の登録、および管理者権限をカスタマイズする。
ポリシー機能	セキュリティポリシーを端末や端末グループ、部門単位に設定し配布する。
ログ機能	端末に配布されたセキュリティポリシーの適用状況、コマンド発行履歴などを収集し一元管理する。
アラート機能	管理者ダッシュボードから、システム異常事態を即座に確認する。また、管理者ダッシュボードのアラート情報を定期的にメール送信する。

■表1 MDMの主な機能

・セキュアブラウザ

Webブラウザの基本機能を備えつつ、セキュリティを強化。読み込んだWebページの情報はキャッシュに一時格納され、セキュアブラウザ終了時に消去される。一定時間何も操作しないとセキュアブラウザを終了させる機能や、URLフィルタリング、文字や画像のコピー禁止、画面キャプチャーの制限などの機能をもつ製品もある。

・スマートフォン仮想化

サーバ仮想化の仕組みをスマートフォンで実現したもので、1台の端末で個人用と業務用の2つのプロファイルを切り替えて使用可能。個人用の設定やアプリケーション、データは端末内に保存され、業務用は仮想環境に保存される。

国内BYOD導入事例に見られる共通点

■事例A：職責や業務形態によって私物／支給端末の適用範囲を設定し、労務面もケアしたワークスタイル変革を実現

アパレル販売A社は2010年、「従業員が便利に使っている私物端末の活用で業務効率の向上が期待できるのでは」との考えから、BYOD（スマートフォン・携帯電話）と支給端末（iPad）による社外からのメール・スケジュール管理へのアクセスを許可した。BYODではセキュアブラウザを採用。その製品の選定では、従業員が端末を頻繁に買い換えることを考慮し、多様な端末

に対応している点を重視した。一方、支給iPadでは、Microsoft ActiveSyncによるデータ同期とMDMによるリモートワイプを採用。このように一般職のBYODおよび支給iPadでは「端末にデータを残さない」ことを徹底する一方、幹部には支給iPadまたは私物PC（SSL VPN+仮想リモートデスクトップ）から一部の業務アプリケーション利用を許可している。

BYOD導入にあたっては、セキュリティ面に加え、従業員の労務面も重視。情報システム部門と人事部門が協力してプロジェクトを推進し、モバイル業務時の賃金の取り決めや、通信費などの合意事項を決定していった。現在、会社と従業員が互いにメリットを共有するという考えのもと、時間や場所を問わずに業務を遂行できるワークスタイルの変革を実現している。

■事例B：支給端末と同等のセキュリティ対策をBYODにも適用するために、BYODポリシーをグループ全体で整備

大手グループB社は、2011年6月より、支給PCを低コストかつ迅速にスマートデバイスへ置き換える手段として、当時の大手企業では画期的なBYODを採用。「支給PCと同等のセキュリティ対策を条件に、スマートデバイスによるBYODを禁止しない」とするBYODポリシーを整備した。支給PCにはない、私物スマートデバイス特有のリスクを回避するために、メールと予定表、連絡先の同期機能をもち、かつ基本的なMDM機能を備えるMicrosoft ActiveSyncを選定。パスワードやリモートワイプ、画面ロックを強制適用している。また、新たなスマートデバイスを導入する際には、随時BYODポリシーを更新している。

■事例C：自治体にもBYODの波。私物端末から庁内へのリモートアクセスで業務を効率化

自治体C県は、2012年9月より、一部の部署を対象に、職員の私物スマートフォンから庁内へのリモートアクセスを実験。メールの閲覧、部課長のスケジュール確認、公用車・会議室の予約に利用し、セキュリティ対策は、IDとパスワード、端末識別番号による認証、暗号通信などで行っている。さらに直行直帰が多い職員へも拡大し、業務の効率化を図っている。

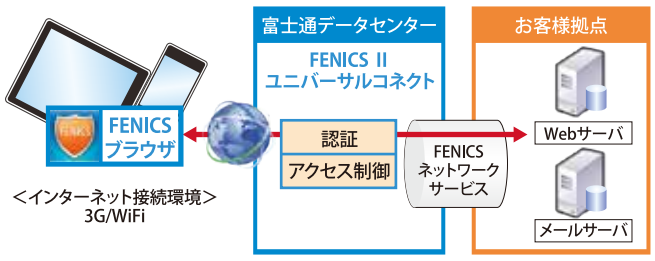
以上の他にも、インスタントメッセージや各種申請の承認をモバイルアプリで行うなど、社外にいる時間を活用することで勤務時間を1日約1時間短縮させ、従業員の満足度を上げている事例もある。いずれの成功事例も、自社の従業員の利便性を考慮し、自社のセキュリティポリシーのもとでBYODを運用している点に注目したい。

富士通の取り組み

スマートデバイスを活用して事業継続、生産性向上を図りたいと考えたり、従業員からBYODを望む声が出ていても、セキュリティに不安を感じて導入に踏み切れない企業は多い。富士通は、多くの企業が懸念しているセキュリティ対策についての考え方とそれに基づくソリューションにより、安心安全に業務を遂行できるよう支援している。例えば、セキュアブラウザ「FENICSブラウザ」、各種仮想デスクトップサービスやシンクライアントソリューション、MDMサービス、持ち込み端末対策「iNetSecシリーズ」などがある。これらの各製品やサービスと、セキュリティポリシー立案のコンサルティングを組み合わせ、お客様のビジネスおよびシステム環境に合わせて最適化して提供している。

●FENICSブラウザ

企業のイントラネットへセキュアに接続するリモートアクセスサービス「FENICSⅡユニバーサルコネクト」では、スマートデバイス向けセキュアブラウザ「FENICSブラウザ」を提供。「FENICSブラウザ」は、終了時のキャッシュや履歴の消去、機体識別番号の取得および認証時チェック、ブックマーク登録や編集の不可、URL／検索フィールドの非表示、といった機能を備える。Android端末およびiOS端末に対応している。



■図3 「FENICSⅡユニバーサルコネクト」のFENICSブラウザ利用時の接続イメージ

富士通では、モバイルワークスタイルの推進力となるお客様のスマートデバイスを、安心安全にご利用いただけるソリューションをこれからも提供していく。

●富士通関連サイト
○スマートデバイスセキュリティ
http://jp.fujitsu.com/solutions/safety/secure/solution/sol35.html
○FENICSブラウザ
http://fenics.fujitsu.com/networkservice/universal-connect/mobile_browser.html

○一般社団法人 日本情報システム・ユーザー協会「企業 IT 動向調査 2013」
http://www.juas.or.jp/servey/it13/index.html
○ IDC Japan プレスリリース
http://www.idcjapan.co.jp/Press/Current/20130117Apr.html
○ MMD 研究所「職場での私用スマートフォンの利用実態調査」
http://mmd.up-date.ne.jp/news/detail.php?news_id=1177
○日経 BP 社「ITpro 会員 100 万人に聞く！ ICT 大調査」
http://itpro.nikkeibp.co.jp/article/COLUMN/20130225/458701/
○一般社団法人 日本スマートフォンセキュリティ協会「BYOD の現状と特性 ～あなたの組織はどのパターンですか～」
http://www.jssec.org/report/20121119_byod.html
○ NPO 日本ネットワークセキュリティ協会「スマートフォンの安全な利活用のすすめ ～スマートフォン利用ガイドライン～」
http://www.jnsa.org/result/2012/surv_smap.html

〈監修〉：編集委員　鈴木 龍明　日邦薬品工業㈱