

ワークスタイル変革を支援するコミュニケーション&コラボレーションサービスへの取り組み

手束裕司*

Communication & Collaboration Services for Work Style Revolution

Yuji Tetsuka

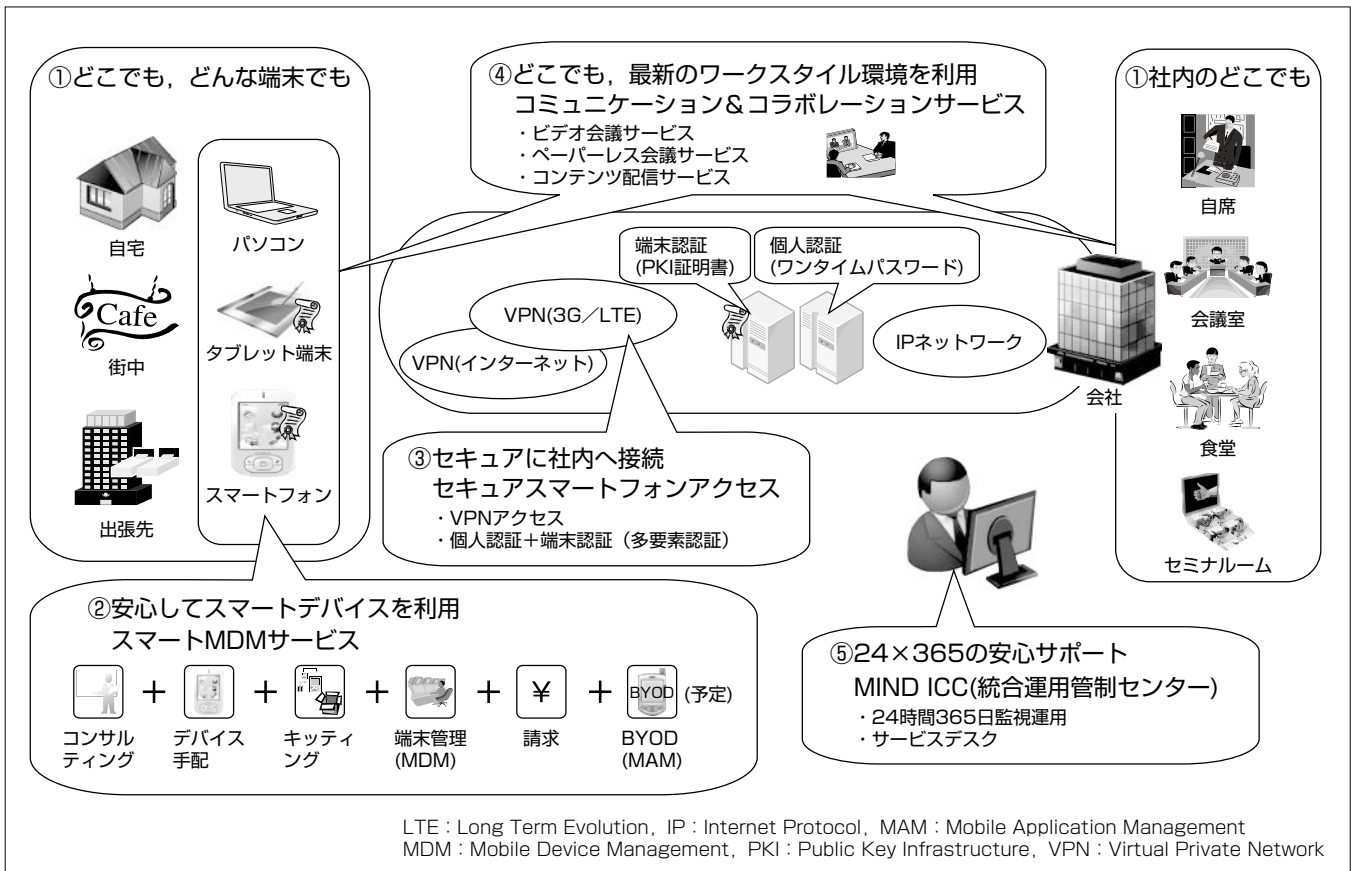
要旨

スマートフォンやタブレット端末の利用が世界中で急速に広まっている。世界市場では2012年携帯電話新規出荷台数のうち約4割は既にスマートフォンになっており⁽¹⁾、日本市場では更に加速して、新規出荷台数の約7割がスマートフォンになっている状況である⁽²⁾。

このような市場におけるスマートデバイスの普及と並行して、ワークライフバランスの実践や従業員の業務効率や生産性の向上を目的とした在宅勤務やサテライトオフィス等、企業における従業員の働き方について変化が起きている。さらに、2011年の東日本大震災以降、事業継続性(Business Continuity Planning: BCP)の観点から、社外でも社内と同様の環境で業務を行えるIT(Information

Technology)環境を求める声が高まっており、企業におけるワークスタイル変革が注目されている。

三菱電機情報ネットワーク株(MIND)では、企業のワークスタイル変革を支援するソリューションとして、スマートデバイスを安全に利用するための“スマートMDMサービス”、業務効率の向上を目的としたコミュニケーション&コラボレーションサービスとして、“スマートデバイス対応ビデオ会議サービス”“ペーパーレス会議サービス”“コンテンツ配信サービス”を提供している。そして、現在、個人所有のデバイスを業務で利用するBYOD(Bring Your Own Device)の提供へ向けたサービス開発に取り組んでいる。



スマートデバイスの管理とコミュニケーション&コラボレーションのトータルサービス

どこからでも, どんな端末でも, セキュリティを確保して社内へ接続し, ビデオ会議, ペーパーレス会議, コンテンツ配信等の最新のワークスタイル環境を利用することによって, 業務効率の向上を実現する。さらに, MINDの運用管制センターであるICC(Integrated Control Center)によって24時間365日のサポートを提供する。

1. ま え が き

スマートフォンやタブレット端末等、スマートデバイスの普及が急速に進んでいる。世界市場では2014年にはスマートフォンの出荷台数が従来の携帯電話の出荷数を超え、タブレット端末については、2015年にノートパソコンの出荷台数を上回ると予測されている⁽¹⁾。さらに、コンシューマライゼーションの流れを受けスマートデバイスを企業の業務で利用しようとする動きが急速に広まっている。

また、ワークライフバランスや事業継続性の観点から、企業における従業員の働き方に革新が起こっており、社外でも社内と同様の環境で業務を遂行できるIT環境の整備が求められている。

スマートデバイスは、ノートパソコンに比べ操作性が良くかつ携帯電話に比べて多くのアプリケーションを利用できることから、このようなワークスタイルの変革に対応するためのツールとしての利用が注目されている。

本稿では、急速に導入が進んでいるスマートデバイスの業務利用における課題と解決策、ワークスタイル変革を支援するスマートデバイスを活用したコミュニケーション&コラボレーションサービスについて述べる。また、次のステップとして注目を浴びている個人所有のデバイスを業務で利用するBYODの動向と実現方式についても述べる。

2. スマートデバイスの業務利用

2.1 スマートデバイスの業務利用の動向

企業がスマートデバイスを業務で利用しようとする動きは急速に広まっており、現在、日本国内の法人契約の携帯電話加入者数におけるスマートフォンの割合は1割強であるが、2016年には法人契約のスマートフォンが5割を超えると予測されている⁽²⁾。特に携帯通信事業者から新規に発売される携帯電話はスマートフォンが主流となっており、従来の携帯電話を入手するにも選択肢が少なくなってきたことも企業におけるスマートフォン導入の促進要因となっている。

2.2 スマートデバイスの業務利用における課題

スマートデバイスは携帯電話の延長線上で開発されたものであるが、機能としてはパソコンの要素を併せ持っている。そのため、スマートデバイスを業務で利用する場合には次の課題を解決する必要がある。

2.2.1 情報及びアプリケーションの適切な管理

スマートデバイスは従来の携帯電話と比べ、多くの情報やアプリケーションをデバイス内部に持っている。スマートデバイスでは、それらの情報とアプリケーションを簡易に利用することができるため、利便性が評価され普及しているが、企業で利用する場合には、デバイス内部に持つこれらの情報やアプリケーションを適切に管理する必要がある。

2.2.2 セキュリティ対策

スマートデバイスは常にネットワークに接続されており、一部のスマートデバイスのOS(Operating System)はオープンソースであるため、その脆弱(ぜいじゃく)性をターゲットとしたマルウェアも出現している。また、悪意のあるアプリケーションがアプリケーションストアから提供され容易にダウンロードができるなど、従来の携帯電話では考慮する必要のなかったセキュリティ対策を講じる必要がある。

2.3 スマートデバイスを安全に利用するための対策

スマートデバイスを安全に利用するためには、スマートデバイス利用におけるセキュリティガイドラインの策定とデバイス管理という大きく2つの対策を講じる必要がある。

2.3.1 セキュリティガイドラインの策定

セキュリティガイドラインでは、スマートデバイスを社員に配布するための基本的な考え方(誰が、どのような目的で、どのように利用するか)、スマートデバイスの機能の制限(カメラ、メモリカードの使用制限など)、利用するアプリケーションの制限(ホワイトリスト管理、ブラックリスト管理)、パスワードの管理(有効期限、文字種類・組合せの設定)等、利用方針及び利用基準を決める必要がある。

2.3.2 デバイスの管理

スマートデバイスの管理は次の3つの対策を講じる必要がある。

(1) 紛失・盗難時の情報漏洩(ろうえい)防止対策

スマートデバイスは外出先で利用することが多いため、万一紛失や盗難にあった場合に企業の機密情報や顧客情報が外部に漏れないように対策を講じる必要がある。対策としては、デバイス内部の情報の暗号化に加え、スマートデバイスがセキュリティガイドラインに準拠するようMDMによる管理が必要となる。MDMによって、デバイスで利用できるアプリケーションの制限やカメラなどの機能制限、万一デバイスを紛失した際に遠隔からデバイスをロックしたり、デバイスの設定を初期化し全てのデータを消去(ワイプ)したりすることが可能になる。

(2) ウイルス対策

スマートデバイスを社内のシステムへ接続する際にウイルスなどを持ち込ませないようにするために、それぞれのスマートデバイスのOSに対応したウイルス対策ソフトを導入する^(注1)。さらに、ウイルス対策ソフトが常に最新の状態になっているかMDMを利用して管理する。

(3) 不正アクセスの防止と通信の保護

社内への不正アクセスや通信経路の盗聴を防ぐ対策として、VPNを用いて暗号化されたネットワークで接続する。社内ネットワークへの接続の際には個人認証と電子証明書による端末認証等の複合的な認証を実施する。

(注1) 一部ウイルス対策ソフトを提供しないOSがある。

2.4 スマートデバイスを安全に利用するためのソリューション
 MINDでは、スマートデバイスを安全に利用するために“スマートMDMサービス”を提供している。このサービスを利用することによって、セキュリティガイドライン策定の支援から、スマートデバイスの手配、スマートデバイスへのセキュリティポリシーの設定、MDMによる24時間365日の遠隔運用管理、利用状況のレポート、請求までをワンストップで行い、顧客のスマートデバイスのライフサイクルを適切に管理することができる(図1)。さらに、MINDでは、“セキュアスマートフォンアクセスサービス”として、外出先から社内へのVPN接続サービス、個人認証及び端末認証の認証サービスを提供している。

3. ワークスタイル変革に合わせたコミュニケーション&コラボレーションサービス

3.1 ワークスタイル変革でのスマートデバイスの有用性
 ワークスタイル変革にはいろいろな考え方があるが、この章では、“時間と場所に制限されない働き方”と定義する。具体的には在宅勤務など社内外を区別せずに業務を行い、かつ社内でも自席を意識せずに社内のどこにいても業務を行える働き方である。

ワークスタイル変革を実践する上で重要となるのは、社外や自席以外で業務を行う際に業務効率や生産性を低下させないことであり、自席と同様の使い勝手で不自由なく業務を遂行できるIT環境を提供することである。そのようなIT環境を実現する上で、スマートデバイスはノートパソコンに比べ、重量が軽く、起動が速い、携帯電話と比べ画面が大きく、業務アプリケーションの利用が可能である等、外出先や自席以外で利用するには利便性が高く適したツールである。また、スマートデバイスは、メール、スケジュール、業務システム等、社内リソースの利用に加えて、営業活動時の迅速な製品カタログの閲覧やプレゼンテーションの実施、外出先でのビデオ会議への迅速な参加等、これまでのパソコンでは準備に時間がかかった業務を短時間で実現することができ、商談の機会損失の削減、業務効率の向上を図ることが可能である。

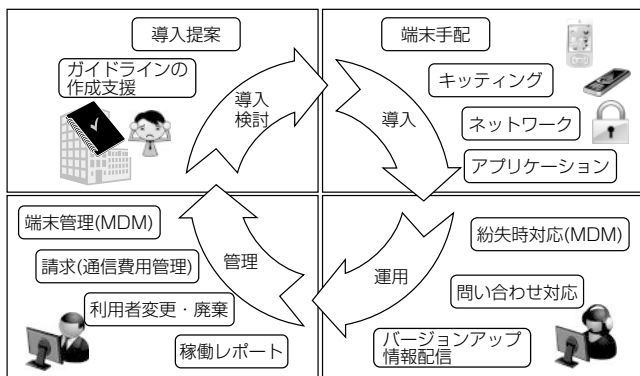


図1. スマートMDMサービス

3.2 スマートデバイスを活用したコミュニケーション&コラボレーションサービス

MINDではワークスタイル変革を支援するコミュニケーション&コラボレーションサービスとして、スマートデバイスを活用したビデオ会議サービス、ペーパーレス会議サービス、コンテンツ配信サービスを提供している。さらに、現在、インスタントメッセージ、プレゼンス、メール、電話、オンライン会議が1つのインターフェースで利用できるUC(Unified Communication)サービスの開発を進めている。

3.2.1 スマートデバイス対応ビデオ会議サービス

従来のビデオ会議システムは、会議室に据置きビデオ会議システム同士で会議を行うか、パソコンにビデオ会議用のアプリケーションをインストールし利用するのが一般的であったが、このサービスではタブレット端末を利用して、出張先や自宅からでも簡単にビデオ会議に参加できる環境を提供している。これによって、いつでも、どこからでも迅速に会議に参加でき、業務効率の向上を図ることができる(図2)。

3.2.2 ペーパーレス会議サービス

会議で配布する資料をPDF(Portable Document File)のファイル形式であらかじめサーバへ保存しておき、会議では出席者がタブレット端末を利用して該当のファイルを開覧し会議に参加できるサービスである。資料にはコメントや下線等の書き込みが可能であり、出席者各自が書き込んだ資料はサーバにそれぞれ保管され、会議終了後に自席のパソコンから閲覧することが可能である(図3)。紙の大幅な削減につながり、グリーンITにも貢献する。

3.2.3 コンテンツ配信サービス

配信する動画や静止画をコンテンツサーバに保存しておき、タブレット端末などのスマートデバイスから閲覧でき

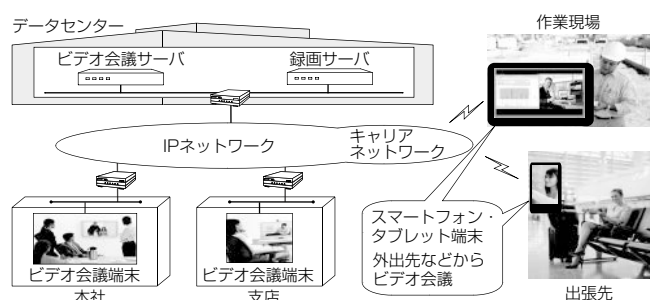


図2. スマートデバイス対応ビデオ会議サービス

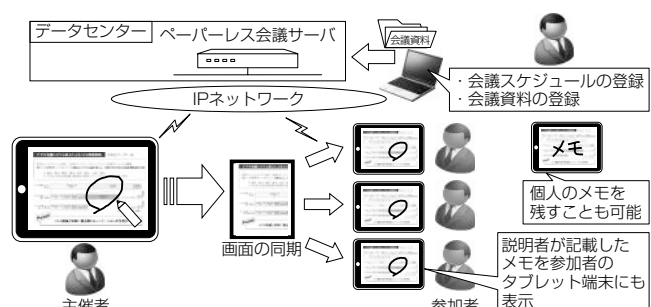


図3. ペーパーレス会議サービス

るサービスである。社員のトレーニング、経営幹部の社内メッセージの動画配信、営業活動における製品カタログ配布等いろいろな場面で利用が可能である。オンラインでの利用に加え、あらかじめダウンロードすることによってオフラインで利用することもできる(図4)。

4. BYODの動向と実現方式

4.1 BYODの概要

BYODとは、個人所有のデバイス(パソコン、スマートフォン、タブレット端末等)を企業内に持ち込み業務用として利用することである。BYODはコンシューマライゼーションの流れを大きく反映したものであり、会社が支給したデバイスでは性能や使い勝手等に満足できないため、個人所有のデバイスを業務用に利用したいという従業員からの要望と、企業側はデバイスを支給し定期的に買い換えるコストを削減できるという利点から欧米を中心に広がっている。日本でもBYODを導入している企業の事例が出始めているが、企業文化の違いやセキュリティ、プライバシーへの懸念もあり導入は欧米の企業に比べまだ慎重であると言える。ただし、企業の情報システム部門が認めていないデバイスを無断で社内を持ち込み利用する事象が現在問題視されており、このような事象を“シャドーIT”と呼んでいる。シャドーITの存在は企業のセキュリティ管理上、極めて重要な課題であり、BYOD対策の導入がその解決策の一つになる。

4.2 BYODを実現するための技術

BYODを実現するには、セキュリティポリシーの設定などMDMによるスマートデバイス自体の管理に加え、デバイスには個人のプライベートな情報と企業の情報が混在するため、企業はプライベートな情報には関与せず企業情報だけを管理する情報管理の仕組みが必要になる。

この仕組みを実現するための技術として現在注目されているのがMAMである。MDMがデバイスのセキュリティや資産管理を主体に実施するのに対し、MAMはデバイスにインストールされているアプリケーションの保護や管理を実現する技術である。MAMの実現方式としては、次の2つの方式がある。

4.2.1 サンドボックス/コンテナ方式

デバイスの内部を業務領域とプライベートな個人領域に分離し、相互の通信を遮断するとともに、万一デバイスを紛失した際にも業務領域だけを一括で削除できる方式である。同方式は自社開発のアプリケーションを業務領域に入れる際にSDK(Software Development Kit)による開発が伴うなどの導入の課題もあるが、業務領域と個人領域をそれぞれ一括で管理できるなど運用管理が容易である。

4.2.2 アプリケーションラッピング方式

個々の業務用アプリケーションをラッピングという技術で保護し、外部からの影響を受けないようにする方式であ

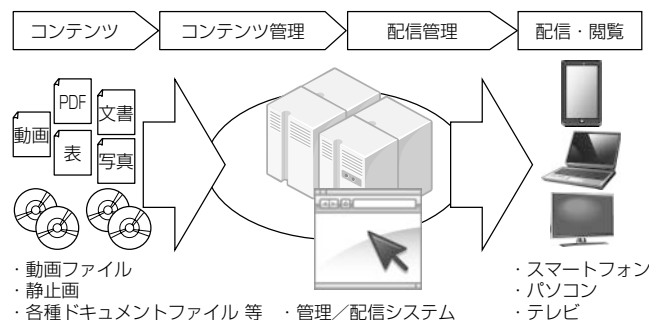


図4. コンテンツ配信サービス

る。アプリケーションを起動する際にパスワードを要求したり自動的にVPNを起動したりセキュリティ機能を付加することも可能である。同方式は自社開発のアプリケーションであっても容易にラッピングすることができ、アプリケーションごとにセキュリティ設定が可能であるなど運用管理の柔軟性が高い。

現在、このサンドボックス/コンテナ方式とアプリケーションラッピング方式の技術を融合させ、セキュリティの強化と運用管理の容易性を併せ持った製品も市場に出てきている。

MINDでは、現在、BYODへの対応として、ニーズ調査、技術調査、製品調査、製品検証を行いサービスの提供へ向け開発を進めている。

5. む す び

今後、ワークスタイルの変革が進むとともに、社内外を問わずに業務を円滑に遂行する環境が求められ、スマートデバイスはワークスタイル変革を実現するための必須のツールとなる。さらに、これまでパソコンでは実現できなかった迅速性や機動性を求められる業務に対して、操作性に優れたスマートデバイスの活用が期待される。

ワークスタイル変革でスマートデバイスを活用するには、スマートデバイスを安全に利用する仕組みと、業務効率を向上させるためのコミュニケーション&コラボレーション環境が必要である。

MINDでは、スマートデバイスを安全に利用するためのスマートMDMサービス、業務効率を向上させる各種コミュニケーション&コラボレーションサービスを提供し、今後、さらにBYODやUC等、新たなサービスの開発にも取り組み、顧客のワークスタイル変革を支援していく所存である。

参 考 文 献

- (1) 株矢野経済研究所 プレスリリース：世界のスマートフォン・タブレットに関する調査結果2012 (2012)
- (2) IDC Japan プレスリリース：2012年第3四半期 国内携帯電話/スマートフォン市場規模を発表 (2012)
- (3) IDC Japan プレスリリース：国内ビジネスモバイル市場予測を発表 (2012)