働き方改革の理想的なサイクルを生み出す「人中心」のテレワークプラットフォーム

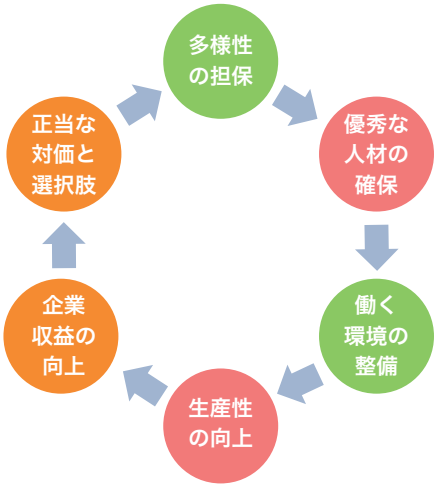
「セキュアMAM」でリモートアクセスとビジネスコミュニケーションを融合

「働き方改革」に取り組む目的は、多様な働き方を実現する環境を整備することで人材の確保と生産性の向上を図り、従業員にも自由や対価を還元することだ。そのために不可欠なのはテレワークの実現だが、その環境構築は時間もコストも負担が大きい。そこで注目したいのがセキュア MAM だ。スマートデバイスを使ったメールやチャット、音声通話、オフィスドキュメントなどによるビジネスコミュニケーションを迅速かつセキュアに実現できる。

「働き方改革関連法」が施行 企業の対応は急務

2019 年 4 月から働き方改革関連法が施行され、企業は働き方改革への対応が喫緊の課題となっている。企業は有給休暇の取得や労働時間の把握が義務化され勤怠管理の厳格化が要求されている。時間外労働の上限規制を始め、さまざまな項目に罰則が設けられ、労働環境改善はいよいよ無視できなくなった。また労働者のワークライフが多様化し、さらに労働人口の減少が加速する今日の環境に対しても、企業は手をこまねいていられない。今までと同じようなワークスタイルや勤務体系のままでは、子育てや介護などの時間、プライベートの時間を確保しながら働くことができず、人材採用は一層困難になってくる。

しかし、現状では、まだ働き方改革をどのように進めてよいかわからず、場当たり的な施策にとどまっている企業が多いのも現実だ。ただ働き方に自由を与える施策では決して機能しない。目指すべきは、企業が優秀な人材を確保して企業を成長させ、その結果として従業員が正しい評価と対価を得て、さらなる働き方の自由と多様性が生まれる環境である。これがさらなる人材確保にもつながり、企業成長のサイクルを生み出す。働き方改革はそのための手段であり、あくまで企業の成長と表裏一体となった「自由」や「多様性」の創造を追求しなければならない。



働き方改革の理想的なサイクル

何から着手すべきか迷う改革 テレワーク環境の整備から始めるアプローチ

では多様性のある働き方を実現するためにどうすればよいのか。そのアプローチは「制度・プロセス」「文化・風土」「働く場所」「ICT 環境」の大きく 4 つの観点があるが、制度・プロセスは決定までに膨大な労力と時間を要し、文化・風土についても、トップの強い意志と実行力や現場の意識改革がないと簡単には変わらない。「働く場所」についても、制度の問題にも絡んでくるうえ場合によってはオフィスなどへ多額の設備投資が必要になる。

そこで現実的な方法が ICT 環境の整備から着手するアプローチであり、まず整備すべきなのがテレワーク環境である。ICT によって働く場所が自由になり、時間や場所にとらわれずに業務を行うことで高い生産性を実現できることが浸透すれば、それに合わせて必要な制度や設備も自ずと整備されていくはずである。

そしてテレワークで極めて重要な役割を担うのが、「モバイル端末」である。しかし、企業の中には、過度なセキュ

リティポリシーのために、テレワークが逆に非効率になってしまうケースも多い。そこで次に現れる論点が、このモバイル端末を、いかに利便性を失わずにセキュアに利用できるようにするかである。

悩ましい BYOD のセキュリティ リモートワイプでは限界も

まず、テレワークで使用するモバイル端末の配布形態を見てみると、大きく 2 つのケースがある。企業が端末を所有して従業員に配布する方法と従業員個人が所有している端末を使用する方法（BYOD:Bring Your Own Device）だ。これまで営業担当者などの一部の従業員だけが利用していたモバイル端末は、テレワークの時代では全従業員に展開することが望ましい。そこで、調達や通信コストを大幅に削減でき、また 2 台持ちによる煩わしさを解消できる点からも BYOD への注目が集まっている。

だが、セキュリティ面ではどちらもリスクがあることに変わりはない。企業配布端末では、電話番号など利用者のプライバシーに関わる個人情報の漏えい対策が必要であるし、BYOD では、退職者がアプリにデータを残したままになるなど企業の情報資産の漏えい対策が必要になる。

そこで多くの企業は、デバイスを遠隔で管理し、紛失や盗難の際にデータを消去する、いわゆる「リモートワイプ」機能を持つ MDM（Mobile Device Management）製品を導入し、強固なセキュリティのネットワークと認証基盤も用意するのが常だ。

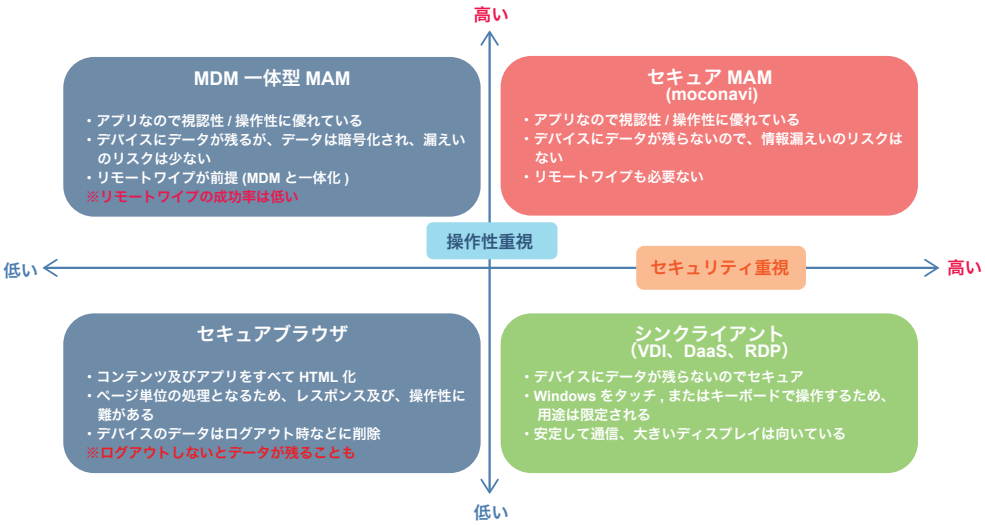
しかしどんなに周りを固めてもモバイル端末に標準で用意されているアプリを使用している限り情報漏えいを防ぐことは難しい。他のアプリへとデータを引き継ぐことができるため、流出経路は無数に存在するからだ。またリモートワイプについても、その実際の成功率は 4% ～ 16% 程度ともいわれ、決して万能な対策ではない。

端末にデータを残さず モバイル環境を利用する最適な方法とは?

モバイル端末から情報漏えいを防ぐもっともシンプルかつ確実な方法はそもそも端末にデータを残さないことだ。これについては、端末の利用用途や利用シーン、操作性をどれだけ優先するかにもよるが、さまざまな実現手段がある。以下に主要なものを見ていこう。

まず 1 つ目の方法が、通常のアプリを使用し、セキュリティについては MDM と一体となってリモートワイプを実現するタイプのモバイルアプリ管理（MAM：Mobile Application Management）製品を採用する方法だ。この場合、操作性は高いもののデータ漏えい対策は、先述の通り成功率が低いリモートワイプに依存することになる。

2つ目が、セキュアブラウザを使うことで、アプリをすべて Web アプリとして使用するという方法だ。これならば端末にデータは残らず高いセキュリティを実現する。ただし、使用後にログアウトしないとデータが残存している場合もあり、またページ単位で読み込みを行うために操作性やレスポンスが相対的に低くなってしまうのが弱点だ。



リモートアクセスの分類

3 つ目の方法が、VDI などによるシンクライアント化である。これならば端末にデータを残さないが、モバイル端末を前提とした使い方が難しい。PC からの利用には適するものの、スマートフォンのような小さな画面から Windows OS の操作をするには利便性に難がある。

これらに対して、モバイル端末で

moconavi は多様な業務アプリ（グループウェア、クラウドストレージ、CRM、電話・UC など）と連携できるため利便性高く使える

の操作性とセキュリティを両立する方法が「セキュア MAM」を利用する方法である。利用イメージとしては、データを保持しない仕組みを持つ専用アプリ内に、もう 1 つ別のアプリケーションランチャーが広がり、多彩なアプリを利用できるというものである。それぞれは標準アプリと同様の機能と操作性を実現するが、データを残さないため、データの消去にリモートワイプを行う必要がない。

テレワークに必要なアプリを 1つのプラットフォームから安全に実行

テレワークの ICT 環境と一概にいっても、スマートフォン、タブレット、ノート PC のどのデバイスをどの程度利用するか、どんなシーンで利用するかによって理想の環境は変わってくる。キーボード操作かタッチ操作かという軸と、モバイル回線網か固定網や Wi-Fi なのかという 2 軸に、オフィスや在宅、現場などの利用シーンを掛け合わせ、自社にあった最適なソリューションを導入するのが賢明だ。

そうした中、レコモットが提供するセキュア MAM ソリューション「moconavi」は、シーンを問わずにモバイル端末で安全にテレワークを行ううえで最適なソリューションとなる。あらゆるビジネスツールと連携することでテレワークプラットフォームとして機能する。

ユーザーの moconavi の利用開始イメージは次のとおりだ。まず自身のモバイル端末に moconavi アプリをインストールし、普段社内の PC で使用しているシングルサインオン対応の ID とパスワードなどを入力してログインするだけで利用を開始できる。iOS の Touch ID、Android の指紋認証などにも対応。マルチデバイス対応の幅も広く、Windows 10 や、Android 搭載の「ガラホ」版のアプリも用意されているため、さまざまなユーザーや利用場面に対応する。

あとは先述の通り、moconavi アプリ上から管理者が設定した多彩なアプリを利用するだけだ。メール、チャット、電話、アドレス帳、カレンダー、ストレージ、ドキュメントビューワー、ブラウザなど、moconavi が用意する標準のアプリだけでも十分に使用できるが、グループウェアやクラウドストレージ、CRM など多彩なサードパーティの製品と連携して利用できるため、普段使い慣れているアプリ環境から使い勝手が変わってしまう心配はない。

管理者の立場でも、容易にサービス提供を開始できる。moconavi をクラウド型で導入する場合、主だったクラウドサービスと簡単な設定で接続でき、無償トライアルの 30 日間で設定したものは、そのまま継続して本番環境として展開できる。オンプレミスでの導入も可能だ。

労務管理に役立つ機能も備えており、管理者がユーザーに対して設定するアプリ制御のポリシーは、権限などセキュリティの観点だけでなく利用可能曜日や利用可能時間の設定も可能だ。時間外労働になりやすい環境を生み出さないよう、労務規定に沿った設定を行うなどして、ワークライフバランスを実現する仕組みがある。

moconavi では、連携サービスは順次拡大して行く予定であり、新たな要望はロードマップに取り入れて対応してい

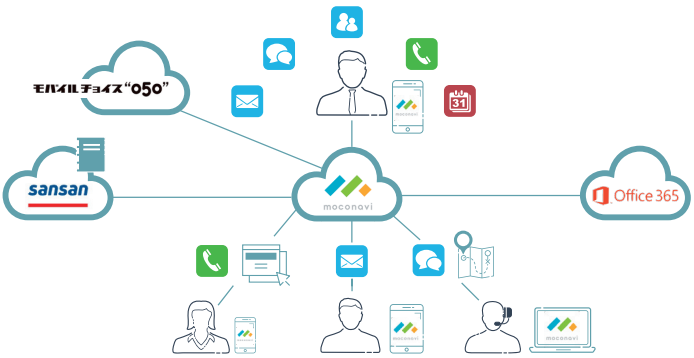
るが、別途カスタムにも対応する。また、シングルサインオンの認証基盤やグループウェアを社内で独自に運用しているケースは多いが、それらをクラウドに移行する必要はなく、中間サーバーを経由して接続する仕組みも用意している。すべて moconavi アプリ 1 つだけをポータルとしてユーザーに提供することが可能な仕組みだ。ライセンス形態もシンプルで、クラウド型の場合はユーザー 1 人ごとにワンコイン程度の料金で、追加にも柔軟に対応できる。

働き方改革とテレワークを加速させる「ビジネスコミュニケーションの融合」

テレワークではセキュアな環境下で業務アプリを利用できるようにする必要があるが、それだけでは不十分だ。チャットや Web 会議、IP 電話、SNS など、コミュニケーションの手段が多彩になる今日、利用者を中心にあらゆるコミュニケーション手段とシステムがつながり、高いユーザビリティを実現する環境を構築しなければいけない。言い換えれば「ビジネスコミュニケーションが融合」した環境である

moconavi は、さまざまなツールとの連携で、こうした環境構築を支援するプラットフォームとなる。中でも評価が高いのが、プライベートと業務で料金を自動的に使い分けできる IP 通話サービス「モバイルチョイス “050”」や名刺管理サービスの「Sansan」との連携だ。BYOD で料金を分計するために、業務用として IP 通話サービスを導入する企業は少なくないが、セキュリティ上、標準の電話帳に名刺情報を登録することができないルールや仕組みになっていると発着信で著しく利便性を欠いてしまう。moconavi の場合はリアルタイムに Sansan の名刺データを参照して発信に利用できるほか、モバイルチョイス “050” からの着信時に名刺データを検索して発信者情報として通知することが可能である。

また、リモートデスクトップのクラウドサービス「Splashtop Business」を moconavi の認証を利用して起動できるため、不正なログインを防ぎつつ社内の PC にアクセス可能だ。



これからのテレワーク環境で重要となる「ビジネスコミュニケーションの融合」

セキュリティを維持しつつスピーディなビジネス環境へ追随

一般的にセキュリティ対策を行えば行うほど、利便性や自由が損なわれてしまいがちだ。それが顕著であれば、テレワークの普及も阻害されてしまい、結果として、せっかく導入したツールも活用されなくなり悪循環に陥ってしまう。そこで、moconavi を活用することで、普段と変わらない業務を安全に実行することができれば、場所を問わずにスピーディに業務を実行でき、高い生産性を生み出すことにもつながる。そしてそれらを加速するのが、先に触れたコミュニケーションの融合という同製品のコンセプトだ。

moconavi は国内のクラウド型 MAM 製品市場で高いシェアを誇り、これまで 420 社以上、23 万 ID を超える利用実績がある。多くの企業でリモートアクセスの課題となるモバイル端末の情報保護を実現しながら、快適な業務を支援するソリューションとして、“ テレワーク時代 ” の多くの企業のニーズに応えている。

株式会社レコモット

〒102-0083 東京都千代田区麹町 3 丁目 3－8 丸増麹町ビル8F
お問い合わせ 03-4446-5007 sales@recomot.co.jp
https://moconavi.jp/