IBM Security
Thought Leadership White Paper

生産性の変革

出先でのコンテンツ・コラボレーションを保護する

IBM

はじめに

このホワイト・ペーパーでは、従業員がスマートフォンとタブレットを使って手のひらからビジネスを行えるように、エンタープライズ・コンテンツを保護しながら、職場の生産性を迅速に変革する方法について説明します。

モバイル機器を職場で使う人が増える中、モバイル機器でのコンテンツの作成、編集、共有、同期、プッシュを成功させるEnterprise Mobility Management (EMM) ソリューションの主な要素は何でしょうか?このホワイト・ペーパーは、業界固有のシナリオとヒントとともに答えを提供して、IT のセキュリティおよび操作性要件とのバランスを図りながら、C レベルの生産性への要求を満たせるように支援します。

デバイスは小型化する一方で、機能は逆に豊富になっており、大きく向上した生産性をサポートしています。こうした生産性の向上は、最終提供物の機能性またはフォームを損なわずに、デバイスからコンテンツにアクセス可能になったことに派生します。

生産性の変革

シカゴのある医師は、別の専門医と一緒に複雑な事例にあたりたいと考えています。彼はスマートフォンを使って、カルテとレントゲン写真をボルチモアの顧問外科医にメールで送って、添付ファイルを使って知見と評価を交換しています。

ある大株主のプレゼンテーションで、様々な企業のデータ・ソースの最新の財務情報をギリギリになって更新する必要が生じています。CEO は駐機場からタブレット、CFO の時間、コンシューマー・ファイル同期と共有アプリを使います。

これらはよくある実際のシナリオですが、ベスト・プラクティスというわけではありません。事実、セキュアなコンテンツ・コラボレーションの最低プラクティスにすらなりません...これらは非常に危険で、規制違反を犯すという悪夢になる可能性があります。

外出時でもコンテンツにアクセス

ノートパソコンの社内導入に匹敵するモバイル生産性の変革により、従業員は出先で仕事をするときには、重要な機密情報をモバイル機器に入れて持ち運んでいます。

空港から電車の駅、喫茶店から会議室まで、オフィス仕様になっていない場所からドキュメントを作成、オープン、更新、分析、編集、共有します。同僚や顧客との協働で得られる効率性は、固定デバイスからは得られないものです。

ただし、このコンテンツは、Windows File Share、SharePoint、イントラネット、Web アプリのような、セキュアなトランザクションの検証が必要な企業ネットワーク上に保存されています。同僚、パートナー、顧客との協働に不可欠な情報は現在、内部ドライブ、データ・ストア、Wiki、ナレッジベース、ERP、SCM、HRM、CRM、その他の管理システム内に囚われています。

デバイスは小型化する一方で、機能は逆に豊富になっており、大きく向上した生産性をサポートしています。こうした生産性の向上は、最終提供物の機能性またはフォームを損なわずに、デバイスからコンテンツにアクセス可能になったことに派生します。

IT:生産性とセキュリティーの中心点

IT は、モバイル機器を抱えながら移動し続け、増え続ける大勢の従業員のこうした作業形態を実現し、より大きいコンテンツへの高まる期待を満たしています。BYOD がデバイス調達のパラダイムを変えたからといって、データ・セキュリティーと無制限の提供という負担はなくなるものではありません。

Enterprise Mobility Management (EMM) ソリューションは、セキュアなコンテンツ・コラボレーションを可能にし、事業部門からの生産性の要求に応えると同時に C レベルの収益への要求を満たすことができます。このホワイト・ペーパーでは、モバイル機器管理のデバイス・トリアージから、モバイル機器上の企業コンテンツとデータの EMM による先見的保護へのシフトを見ていきます。

適切でセキュアなコンテンツ・プログラムの構築

もちろん、専門医にとっては、患者のカルテを電子メールで共有した方が簡単で便利です。彼らは何年もそうしてきました。しかし、可能だからといってしてもいいとは限りません!

駐機場でコンシューマー向けソリューションを使って同期と共有を行うことは、離陸する CEO にとっては素晴らしいことです。地上にいる IT にとって、これはいつ起こってもおかしくないセキュリティーの悪夢です。

スマートフォン、タブレット、ウェアラブルを使えばいつでも継続的に協働することが叶いますが、適切な EMM ソリューションを使えばこれらのやり取りを安全に保護することができます!ファイルがオフィスや ER を離れたからといって、IT がモバイル・ガイドラインについての話をやめたわけではありません。

電子メールとファイル同期/共有:よくある状況、誤ったプラクティス

今日では、実証済みの本物の電子メールからコンシューマー・クラスのクラウド・コラボレーションまで、データを共有する方法は山とありますが、これらのアプローチは必ずしも、ベスト・プラクティスとしてふさわしいとは限りません。こうしたアプローチは脆弱性に対して無防備なので、従業員の生産性に脅威をもたらし、閲覧方法を知っている知識のある者なら誰にでも機密情報が漏れてしまいます。

電子メールと幅広い共有

ドキュメントを共有するために長年使われてきた主要な手段である電子メールは一般に、効率的、生産的、あるいは安全なコンテンツ・リポジトリではありません。ファイルが誤って転送または共有される可能性に加え、添付ファイルが大きくなりすぎて、メール・サーバーのトラフィック負荷に問題が生じることがあります。また、電子メールは通常、リアルタイムのカテゴリー化、フィルタリング、編集、または同期に対応していません。1 日の終わりには、電子メールは安全でないばかりか、生産性とコラボレーションの妨げになることがあります。

しかし、人々は電子メールを続けています。電子メールでの共有が一般的なプラクティスになり続けるでしょう。最新の Ovum のグローバル調査[1] (5,100 人の従業員が対象) によると、これらの従業員の 44 パーセントが電子メールとメモリー・スティックをドキュメントの共有に使い続けています。

調査対象の IT プロフェッショナルの 46 パーセントが、「ファイル共有製品を管理していないために、会社からデータが漏洩している」ことに同意しています。[2]

コンシューマー向け同期/共有アプリケーション:高いリスクとセキュリティー対策の不在

コンシューマー市場は、ファイル同期/共有アプリであふれています。少し名前を挙げるだけで、Dropbox、Google Drive、Evernote、iCloud などがあります。企業開発型 (社内) アプローチは初期段階にあり、ほとんどのケースで、フラストレ

ーションと生産性の対立が生じています。驚くまでもありませんが、従業員は家族写真用の同じ Dropbox を大型プレゼンテーションの保存にも使って、週末家で作業をする傾向にあります。Ovum の調査によると、従業員の 89 パーセントがコンシューマー・クラスのシステムを使っています。その理由は、会社認可のアプローチに不満があるからです。[3]

従業員にとってアクセスしやすく便利なコンシューマー向けファイル同期/共有アプリケーションは通常、可視化、あるいはコンテンツへの一元的なポリシーの実施といったセキュリティーのニーズを満たしません。保護されないままこれらのソリューションを使うと、企業はデータ漏洩、セキュリティー攻撃、規制遵守違反のリスクにさらされる可能性があります。

しかし、従業員はどうしても使いたいと言います。Interlink の調査によると、[4]調査対象の IT プロフェッショナルの 46 パーセントが、「ファイル共有製品を管理していないために、会社からデータが漏洩している」ことに同意し、84 パーセントが従業員による無料ファイル同期/共有製品の使用のせいで潜在的なセキュリティーの問題が生じていると考えていても、従業員の意思は変わりません。

モバイル機器上で企業コンテンツを適切に保護するための主な要素

生産性を維持し、ビジネスを保護するには、エンタープライズ・モビリティ管理が安全で機能性に優れ、使いやすいと職場の従業員に確信してもらう必要があります。

職場の全員が使えるように設計されたソリューションには、次のものが必要です。

アクセス可能で直感的なツール: ユーザーには、コンテンツをアクセスしやすくして、共通ファイル・タイプ (Excel、Word、PowerPoint、PDF) の作成、編集、同期、共有を行うためのツールが必要です。IT はドキュメントがどのように表示、共有されているのかを把握し、編集に関するより詳細なコントロールにセキュリティー・ポリシーをリモートで適用する必要があります。

クラウドを介したセキュリティーと拡張性: 強固な EMM ソリューションは、セキュアな暗号化済みコンテナーに依存しています。コンテナーは機密データを保護し、時間/ロケーションベースのポリシー、パスワード・コンプライアンス、ベスト・プラクティス・ドキュメント・ワークフローを確立、実現、実施する機能も IT に提供します。クラウドベースのソリューションにより、IT は 1 つのコンソールからロールベースのアクセスやその他の管理を実行できます、また、ユーザーのデバイス上のセキュアなコンテナーでしかドキュメントを開けないので安心です。

グローバルなマネージド・クラウド・ソリューションも、スケーラブルな配布に対応できることがあります。ドキュメントを一度保存し、頻繁に配布するここと で、ストレージの容量や帯域幅の制限などの心配が軽減されます。

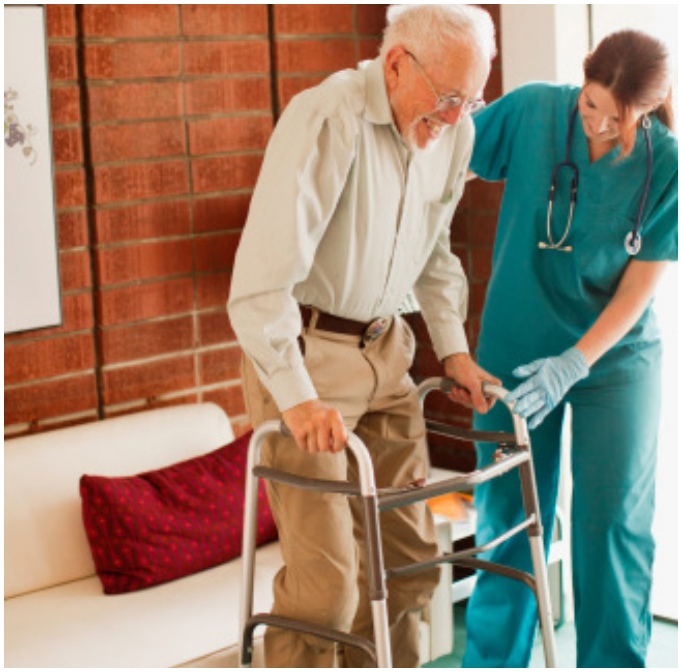
クラウド EMM 実装の費用対効果と使いやすさも、急激に変化するモバイルの世界における投資回収率 (ROI) と共鳴します。導入コストと保守コストを劇的にカットできるため、IT の時間とリソースを別のサーバーの購入や保守ではなく、もっと価値の高い企業イニシアチブに解放することができます。モバイル OS は最新アプリをサポートできるように常に進化しているため、EMM ソフトウェアを同日更新しなくても、モバイル・フリートを無効化できるでしょう。

コンプライアンス: 各種業界はコンプライアンス要件による制約を受けており、EMM ソリューションはこれらの規制に対処する必要があります。

株式会社はサーベンス・オクスリー法 (SOX) の対象となっています。SOX 法により、たとえば、特定の財務報告期間外に財務情報を外部に配布することが制限されています。金融サービスの場合、FINRA (金融取引業規制機構) により、スマートフォンとタブレットを会社の広範な部外秘情報要件に準拠させて消費者情報を保護することが求められます。

医療保険の携行性［相互運用性］と責任に関する法律 (HIPPA) も医療産業に同様の制約を課しており、個人を特定できる暗号化されていない情報と保護医療情報の保存を禁じるルールがあります。小売業の場合、クレジットカード業界のセキュリティ基準 (PCI DSS) によって、どのように使用し、どこに保存していようとも、カード所有者のデータを保護する厳格なガイドラインが定められています。

変革を強化



治癒した患者さんが、「主治医が最高の専門医を呼んで治療にあたってくれる」と安心しながら帰途につきます。彼のカルテは、主治医のデバイスの電子メールの中で機密が守られます。

CEO はプレゼンテーションを大成功させ、株主と重役たちは、最新の数字にわくわくしています。また、情報は会社のセキュアなワークスペースで常に守られています。

あっという間のこれらのモバイルの瞬間が終わり、データが静かに収まっているとき、企業は、モバイル生産性を実現しながら、休止中、移動中、使用中のデータを保護する EMM ソリューションの利点に気付きます。

セキュア・コンテンツのメリット

患者のベッドから空港のラウンジなどに至るまで、IT、事業部門のリーダー、従業員、企業全体にとって、コンテンツのアクセス、作成、編集、管理、共有、同期を実現することのメリットは多数あります。

世界が職場になれば、従業員が出先で作業し、別々の時間帯に居てもコンテンツについて皆と継続的に協働できる場所へと企業が生まれ変わります。

従業員が苦労をしなくても出先で仕事することができ、ドキュメントのアクセス、編集、管理、共有、同期、協働を行うことができれば、生産性とコラボレーションは向上します。IT と C レベルは、休眠中または移動中の機密データとコンテンツが漏洩するリスクがないので安心できます。

従業員が、会社のセキュリティーを侵害することなく、デバイスを個人やプライベートに使用できれば、**従業員の満足度は** 上がり、誰もが円満になります。満足した従業員は生産性が上がります!

セキュア・コンテンツの主な要件

出先でコンテンツを適切に保護するには、次のことが必要です。

- 個人データとは完全に分離した、モバイル・プラットフォーム上で企業ファイルを保存、共有、同期するためのセキュアで直感的なワークスペース
- **IT がドキュメントへのアクセスを完全に把握できるようにするための一元的なコントロールとルールベースの制約**
- **既存の認証システム、認可システムとのスムーズな統合**
- **ドキュメントをリモートでプッシュし、ワークフローを確立、実施して、大勢または一部に配布する機能**
- カスタマイズされたデータ・リポジトリから、IBM Connections、SharePoint、Google などの他のデータ・リポジトリに至るまで、既存の資産と投資にアクセス
- モバイル機器上の特定のファイル共有/同期アプリケーションをブラックリスト化することで、特定のユーザー、グループ、または全ユーザーの使用をブロック
- **電子メールと添付ファイルをコンテナーに入れることで、**電子メールで共有されるドキュメントを保護
- 古い情報、紛失したデバイス、退職した従業員、「脱獄」または「ルート化」されたコンプライアンス違反のデバイスをリモート・ワイプ

IBM® MaaS360®

MaaS360 は、モバイル機器上のコンテンツをより安全、簡単にプッシュ、アクセス、作成、編集、共有、同期できるようにすることで、変革を強化します。その EMM ソリューションにより、従業員はこれらのデバイス上のドキュメントを個別に作業することも、共有することもできるようになります。また、IT は幅広い管理とコントロール機能を保護され、暗号化されたコンテナーで駆使できます。

MaaS360 ソリューションは以下を提供します。

- シンプルに使えるインターフェースでコンテンツを管理できるコンテンツ・ストレージ:
  - クラウド、オンプレミス、またはハイブリッドの複数のデータ・リポジトリ・オプションを提供。オプションには、クラウドベースの Box、 Google Drive、Dropbox と MaaS360、オンプレミス型 (IBM Connections、Windows File Share、SharePoint など) があります。
- iOS、Android、Windows Phone と PC のコンテンツにアクセスでくる On-Device コンテナー:
  - デバイスからのファイル転送を保護
    - 複数のタイプのデータ・リポジトリ (クラウドとオンプレミス型) にアクセス
    - リポジトリからデバイスへのデータ転送を保護
  - モバイル機器のセキュリティ統合:認証、パスコード保護、リモート・ワイプ
  - コンテナー化とデータ損失防止
    - コンテナーで休眠中のデータを暗号化
    - 他のアプリのデータアクセスを制限し、切り取り/コピー/貼り付けをブロックし、画面キャプチャーを防止
    - コンテンツの一部をワイプすることが可能
    - 電子メールなど、他のエンタープライズ・モビリティ・アプリと統合
- 同期と共有:
  - 複数のデバイス・タイプ間でユーザー所有コンテンツを同期し、ノートパソコン上でコンテンツを作成してスマートフォン/タブレットに同期し、電子メールと統合することで、添付ファイルのセキュリティーとコントロールを促進
  - 他のアプリ、社内外のユーザー (同僚、パートナー、顧客) とコンテンツを共有し、認証や共有の期限などの共有ポリシーを適用
- コンテンツ操作
  - よりセキュアな作成、編集、注釈付け

変革を開始する

生産性の変革が起こりつつあります。会社の従業員の生産性を変革する上で、皆さんはどのような役割を果たしていますか?社内全体の変革をサポートするには、まず、いくつかの重要な問いに答えてみてください。

- 事業部門が生産性を上げるために必要なことは何か?
- 現在、どのような業務形態をとっているのか?
- 現在どのような種類のセキュリティーまたはファイル同期、共有ポリシーを提供または実施しているのか?
- 今使っているツールはスケーリング可能か?
- どのような改善計画があるのか?

事例

あるグローバルな保険会社は MaaS360 のおかげで、生産性を強化しながら、コストカットと時間節約を達成できたと言っています。「IBM® MaaS360® Content Suite は使ってみて非常に役に立つことがわかりました。営業担当者は、保険に入る新しいグループに会っているときに、引受部門に電話してコストと加入の詳細を請求し、私たちは営業担当者がお客様とひざを突き合わせている最中に適切な書類を送ることができます。お客様は加入申込書にその場で記入できるので、商談成立がスピードアップします」

– グローバルな保険会社、Network Support Specialist

小売/ホスピタリティの決済を専門とするある企業は、会社所有の BlackBerry Bold デバイスを iPhones と iPad に交換するに際して、BlackBerry Enterprise Server と同じレベルのセキュリティーと管理を提供する必要がありました。彼らは MaaS360 にそれらの機能を見つけました。MaaS360 を使えば、従業員は企業文書に簡単、効率的にアクセスできます。「MaaS360 は、何をするにしてもはるかに使いやすいので、際立っていました。インターフェースは、よりきれいで直感的です。レポート作成はシンプルだし、使用状況の追跡機能もあって費用管理に対応できます。それに、IBM® MaaS360® Secure Mobile Browser とコンテナー機能のおかげで、ネットワークの脆弱性が自動的に軽減されます」

– 小売/ホスピタリティの決済専門会社、テクニカル・システム幹部

IBM MaaS360 について

IBM MaaS360 は、業務のあり方に合わせて生産性とデータ保護を実現するエンタープライズ・モビリティ管理プラットフォームです。モバイル・イニシアチブの基盤として多数の組織から信頼されています。MaaS360 は包括的な管理機能を提供し、ユーザー、デバイス、アプリ、コンテンツへのセキュリティーを強力に制御することで、どのようなモバイル導入もサポートします。IBM MaaS360 の詳細と 30 日間の無料トライアルのご利用については、次の Web サイトをご覧ください。
www.ibm.com/maas360

IBM Security について

IBM のセキュリティー・プラットフォームはセキュリティー・インテリジェンスを提供して、組織が人々、データ、アプリケーション、インフラストラクチャーを包括的に保護できるように支援します。IBM は、ID およびアクセス管理、セキュリティー情報およびイベントの管理、データベース・セキュリティー、アプリケーション開発、リスク管理、エンドポイント管理、次世代侵入保護などのためのソリューションを提供しています。IBM は、世界で最も幅広くセキュリティー研究開発を行い、セキュリティーを提供している組織の一つです。詳細は、以下をご覧ください。www.ibm.com/security

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in Japan
March 2016

リサイクルにご協力ください

1 *Ovum Mobility Survey* 2014 (2014 年 9 月) http://www.ovum.com/research/employee-mobility-survey-2014-results-enterprise-multi-screening-and-application-usage-trends/

2 *Intralinks Survey Report*、*Safe Sharing:「A Survey of Enterprise IT Decision Makers on Best Practices for Adopting File Sync and Share Applications」* (Intralinks、2014 年 6 月) https://www.intralinks.com/sites/default/files/file_attach/via14_65324_email_harrispaper_v1.1.pdf

3 *Ovum Mobility Survey* 2014 (2014 年 9 月) http://www.ovum.com/research/employee-mobility-survey-2014-results-enterprise-multi-screening-and-application-usage-trends/

4 *Intralinks Survey Report*、*Safe Sharing:「A Survey of Enterprise IT Decision Makers on Best Practices for Adopting File Sync and Share Applications」* (Intralinks、2014 年 6 月) https://www.intralinks.com/sites/default/files/file_attach/via14_65324_email_harrispaper_v1.1.pdf

WGW03151-JPJA-00