IBM MaaS360 Mobile Device Management for iOS

最新の iOS デバイス、アプリ、コンテンツを供給、管理、保護

主なメリット

- 単一のコンソールで、デバイス、アプリ、コンテンツを供給、保護、管理
- 電子メール、カレンダー、連絡先、Wi-Fi や VPN のプロファイルを無線通信経由で設定し、速やかに出発できます
- iOS デバイスのモバイル・オペレーティングシステムの最新リリースを発売日から利用可能
- デバイスのパスコード要求や、感染デバイスのブロックなどの自動化されたコンプライアンスアクションで、セキュリティポリシーを設定、強制
- 強固なダッシュボードやレポートの活用で、企業デバイスと個人用デバイスの両方を管理

Apple + IBM® MaaS360® = より良い協調

Apple は、エンタープライズ・グレードの技術の革新を続け、iOS 9 をより生産的なプラットフォームに作り上げています。そして、MaaS360 は、より高速、かつより強固に iOS 9 およびそれ以前のバージョンをサポートしています。協調している、Apple + IBM は、社員、顧客、パートナーにおいてまだ実現されていないモビリティの可能性の具現化を目指す企業を支援しています。

ユーザーの混乱や IT 部門にとっての頭痛なしで、Apple の発売日に、すぐに、そして、シームレスにデバイスを iOSの最新版に更新できます。他のモバイル・デバイス管理 (MDM) プロバイダーに遅れをとってはなりません。MaaS360 で、すぐに新しい iOS 9 の機能を体験してください!

手軽な Apple iOS 管理

IBM MaaS360 for iOS は、広範な可視性を提供し、企業での iPhones および iPads のサポートをコントロールします。iOS バージョン 4.3 以上をサポートしています。現在は iOS 9 をサポートしており、見識を獲得したり、アクションを実行したり、ポリシーの設定や配布、アプリや文書の管理を行うためのツールを提供します。

このソリューションは、こうしたデバイスや、そこに含まれている企業データ v を保護する迅速で簡単な方法です。over-the-air (OTA) での展開、セキュリティ・ポリシーやコンプライアンス・ルールの使用によるパスコードや暗号化の強制、ジェイルブレイク・デバイスの検出および制限、アプリのホワイトリストまたはブラックリストへの登録、ファイルのバックアップのコントロールなど、さらに多くのことができます。

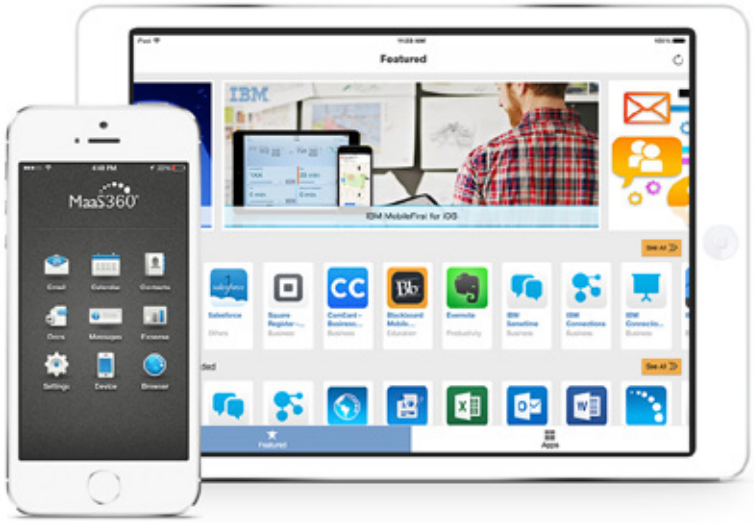

図 1: アプリやコンテンツを簡単に組織の iOS デバイスに展開

見識の獲得

- モデル、シリアル番号、オペレーティング・システム
- ホーム・ネットワーク/現在のネットワーク
  - ローミングのステータス、MAC アドレス
- フリーストレージ容量
- アプリ、バージョンおよびサイズ
- デバイス ID (電話番号、IMEI、電子メールアドレス)
  - 暗号化レベル、ジェイルブレイク検出、パスコードのステータス、デバイスの 制限、インストールされているプロファイル、セキュリティ・ポリシー、その他
- DEP を使用して、構成やポリシーによるアクティベーション中に、企業所有のデバイスを自動的に展開
- 「Find My iPhone」でのアクティベーションのロックを有効化し、デバイスをユーザーの Apple ID にロック
- デバイスに iTunes アカウントが存在する場合、報告する
- 文書、ユーザー、アプリ、その他に関する掘り下げたレポートの表示

アクションの実行

- Wi-Fi、VPN や電子メールの設定およびプロファイルの構成
- デバイスを探し、バズ、ロックする、あるいは忘れたパスコードをリセットする
- 社員が所有するデバイスで、個人的データは維持しながら、企業データを選択的にワイプする
- 紛失または盗難にあったデバイスの全面的ワイプを実行する
- iOS ポリシーを変更する
- 音声やデータのローミング・コントロールを有効化/無効化

エンタープライズ・アプリケーション・カタログ

- エンタープライズ・アプリの管理可能性：MaaS360 によって iOS デバイスに配布されたモバイル・アプリは、完全に管理可能であり、セキュリティを高めながら、アプリの導入を簡素化することができます。
  - iTunes アプリの社員への推奨
  - 「自社製」アプリを配布し、更新を公開
  - リモートからアプリをデバイスへプッシュ、デバイスが監視されている場合は、サイレントでインストール
  - Open In コントロールを管理し、企業アプリで個人用アプリのファイルを開く場合や、逆の場合を制限
  - ネットワークへのアクセスを保護するために、管理されているアプリを VPN へ接続
  - 認証のため、アプリでシングル・サインオンを有効化
  - 自動的に、サードパーティのアプリのデータの暗号化を適用
- Apple VPP をサポート
  - Apple の App Store にアクセスすることなく、前払いアプリを配布、インストール
  - ユーザーが必要としなくなった場合、アプリやブックの VPP ライセンスの完全な所有やコントロールを維持することで費用を節約

ポリシーの設定および配布

- パスコード要求を強制
- デバイスの制限を設定
  - 暗号化されたバックアップを強制
  - カメラ、FaceTime、Touch ID などの利用を制限
  - アプリのインストール、Photo Stream の共有などを制限
  - グローバル HTTP プロキシ・サーバーを通じたインターネット・トラフィックを強制
  - Exchange ActiveSync 設定などの Wi-Fi、VPN、電子メール・プロファイルを配布
- iCloud コントロールを管理
  - 文書、アプリのデータ、デバイスのバックアップ、iCloud とのフォトの同期などをユーザー、グループ、すべてのデバイスで管理
- 電子メールのセキュリティを強化
  - ユーザーによるアカウント間での電子メールの移動を制限し、企業データの漏洩を防止
  - サードパーティのアプリが電子メールを送信することを防止
- 高度な Wi-Fi 設定
  - プロキシの設定や SSID 自動ジョインを管理、プッシュ
- iTunes パスワードの強制
  - コンテンツ、アプリ、iTunes に保存されているデータに アクセスする際に、ユーザーに iTunes パスワードの入力を要求
- デバイスが紛失した際に、ロック画面にメッセージや番号を送信
- 継続性、管理されているアプリについて Spotlight や iCloud の同期の Web の結果を有効にする Handoff 機能を許可する

発売日からサポート

同時に、iOS 9 および MaaS360 は、まったく新しいレベルのセキュリティ、生産性、デバイスやデータの管理機能を提供する準備ができており、組織がモビリティの次の段階へ進むことをサポートします。

新しい iOS 9 エンタープライズ・セキュリティ機能

- 管理されているアプリや iCloud Photo ライブラリに対する AirDrop の制限
- App Store の使用、キーボードのショートカット、Apple Watch、パスコードの変更、自動 app ダウンロードなど、新しい監視された制限の設定
- 監視されているデバイスでの企業アプリのオン/オフ

新しい iOS 9 アプリの配布機能

- デバイスに基づく app の配布で、Volume Purchase Program (VPP) および MaaS360 を使用しているデバイスへアプリを直接展開することで、Apple ID を必要とせずに、シリアル番号によってデバイスへ、アプリを直接割り当てます。
- ユーザーが App Store にアクセスする必要なしで、公開アプリをプルまたはプッシュ
- MaaS360 にインストールされている企業アプリは、明示的に信頼され、ユーザーには信頼の確認はプロンプトされなくなります。
- 監視前に、デバイスにアプリがある場合、そのアプリは監視になった段階でサイレントで管理されます。
- VPP を通じて購入、配布されたアプリは、そのアプリが利用できるすべての国で、デバイスやユーザーに割り当てることができます。

新しい iOS 9 のデバイスおよびデータの管理

- MaaS360 は、デバイス登録プログラム (DEP) にあるデバイスに対して、新しい iOS バージョンの更新を起動します。
- Apple Configurator では、DEP を通じて MaaS360 により、アプリやストリームデバイスの登録を事前展開できます。
- App VPN サポートにより、UDP や TCP でオーディオやビデオをストリーミング

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 Systems and Technology Group
Route 100
Somers, NY 10589

Produced in the United States of America
April 2016

本書の情報は最初の発行日の時点で得られるものであり、IBM によって予告なしに変更される場合があります。掲載されている製品・サービスは IBM がビジネスを行っているすべての国・地域でご提供可能なわけではありません。

性能データとお客様の事例は、説明目的のみのために提示しています。実際の性能結果は、特定の設定や運用条件によって異なる場合があります。他社の製品またはプログラムと IBM の製品またはプログラムを併用した場合の操作の評価および検証は、お客様の責任で行ってください。

本資料の情報は「現状のまま」提供され、商品性、特定目的への適合性に対する保証、および非侵害の保証または条件を含め、いかなる明示的または黙示的な保証も行いません。IBM 製品は、IBM 所定の契約書の条項に基づき保証されます。

適用されるすべての法令と規則の順守は、お客様の責任範囲とします。日本 IBM は、法律上の助言を提供することはいたしません。また 日本 IBM のサービスまたは製品が、お客様においていかなる法を順守していることの裏付けとなることを表明し、保証するものでもありません。

IBM の将来の方向性および指針に関する記述は、予告なく変更または撤回する場合があります。

確実なセキュリティー体制への取り組みについて:IT システムのセキュリティーでは、社内外の不適切なアクセスの防止策、検出、対応に取り組むことで、システムと情報を保護しています。不適切なアクセスにより、情報が改ざん、破壊、または不正流用される可能性があり、システムへのダメージや他者への攻撃といったシステムの悪用が生じることがあります。IT システムまたは製品によってセキュリティー対策が万全になると考えることは危険であり、1 つの製品またはセキュリティー対策で不正アクセスを完全に有効に防ぐことはできません。IBM のシステムと製品は、包括的なセキュリティー・アプローチの一部として設計されています。そのため、運用手順を追加することがどうしても必要となり、効果を最大限に高めるには、他のシステム、製品、サービスが必要になることがあります。IBM は、システムと製品が他者による悪意のある行為または不正行為から免れることを保証するものではありません。


Please Recycle

WGD03066-JPJA-00