



iOS 9 ビジネス向け機能強化ポイント解説

主要な機能強化の活用メリットと導入時の注意点を解説

株式会社アイキューブドシステムズ
2015/11

目次

はじめに	3
1. iOS 9 のビジネス向け機能強化一覧	4
2. iOS 9 を徹底活用するための事前準備	6
3. デバイス管理 / 運用機能の強化	10
4. アプリ管理 / 運用機能の強化	15
5. コンテンツ管理 / 運用機能の強化	20
最後に	22

はじめに



2015年9月にリリースされた iOS 9 は「メモアプリケーションなどアプリの機能向上」「iCloud Driveの強化」「バッテリーパフォーマンスの向上」など、様々な利便性が向上されて注目を集めていますが、ビジネス向けにも様々な機能強化が実施されました。

弊社は、スマートフォン、タブレットのビジネス利用に取り組む企業を支援する独立系ベンダーとして、法人スマートデバイスの管理・運用・活用基盤を提供するプラットフォームサービス「CLOMO」を提供しており、2010年に国内初の iOS 向け MDM サービスを提供開始した後、4年連続でモバイル管理市場シェアNo.1を達成し、iOS 製品に精通する企業として Apple Consultants Network のメンバーに Apple 社から認定されています。これらの活動を通じて得た知見をもとに、本資料では、iOS デバイスの法人活用を検討・実施されている方が iOS 9 を適切に導入・活用できるように、iOS 9 の主要なビジネス向け機能強化の活用メリットや、導入時の注意点などをご紹介します。

1. iOS 9 のビジネス向け機能強化一覧

1. iOS 9 のビジネス向け機能強化一覧

iOS 9 では、以下一覧のように、ビジネス向けに多種多様な機能強化が行われました。
次項からは、特に注目すべき機能（青色で記載している機能）についてご紹介します。



デバイス 管理 / 運用機能の強化

MDM サービス機能の強化

「DEP エンロールメント」の最適化(*2)

「iOS」の強制アップデート(*1)(*2)

「スクリーンショットと画面収録」を制限

「キーボードショートカット」を制限(*1)

「Apple Watch ペアリング」を制限(*1)

「パスコード変更」を制限(*1)

「デバイス名の変更」を制限(*1)

「デバイス壁紙の変更」を制限(*1)

「ロック中の音声ダイヤル」を制限

デバイス準備機能の強化

「DEP エンロールメント」の自動化(*2)(*4)



アプリ 管理 / 運用機能の強化

MDM サービス機能の強化

「Apple ID を利用しない App Store アプリ
の遠隔インストール」を実現(*3)

「App Store を経由しない App Store アプ
リの遠隔インストール」を実現

「インストール済みアプリのManaged Apps
移行」を実現(*1)

「Apple Configurator 2 / iTunes 経由の App
Store アプリインストール」を制限

「Newsアプリ」を制限(*1)

「新しい独自アプリ作成元の信頼」を制限

「アプリの自動ダウンロード」を制限(*1)



コンテンツ 管理 / 運用機能の強化

MDM サービス機能の強化

「Managed AppsでのAirdrop機能」を制限

*1：本機能、または本機能の一部を利用するには、iOS デバイスを監視対象に設定する必要があります。

*2：本機能、または本機能の一部を利用するには、Device Enrollment Program を利用する必要があります。

*3：本機能、または本機能の一部を利用するには、Volume Purchase Program を利用する必要があります。

*4：本機能、または本機能の一部を利用するには、Apple Configurator 2 を利用する必要があります。

2. iOS 9 を徹底活用するための事前準備

(1) iOS デバイスの監視対象設定

概要

Apple 社が提供するアプリ「Apple Configurator 2」または、法人向けサービス「Device Enrollment Program」のいずれかを通じて、iOS デバイスを監視対象に設定できます。本設定を行うことで、管理者は、高度な管理 / 運用機能を MDM サービスを通じて利用できるようになり、管理の強化や柔軟なアプリ配布を遠隔で行える環境を実現できます。

なお、P.4の機能強化一覧で示した通り、iOS 9 の機能強化にも、iOS デバイスの監視対象設定を必要とするものが多く含まれています。

導入時の注意点

- Apple Configurator 2 / Device Enrollment Program を利用して iOS デバイスを監視対象に設定する際には、デバイスの初期化を実施する必要があります。
- Apple Configurator 2 は、Mac App Store から無償でダウンロードできる Mac OS 専用のアプリです (図1)。

導入時のヒント

- iOS デバイスを新規 / 追加導入する際には、高度な管理 / 運用機能が将来的に必要なことを考慮し、あらかじめ、監視対象の設定を実施した上で社内に展開することを推奨します。
- 既に iOS デバイスを導入 / 運用しており、監視対象に設定していない場合には、デバイスの故障や再配置など、業務に支障の生じないタイミングに順次、監視対象の設定を行うことを推奨します。



図1. Apple Configurator 2 のダウンロード画面

(引用元 : <https://itunes.apple.com/jp/app/apple-configurator-2/id1037126344?mt=12>)

(2) Device Enrollment Program

概要

Apple 社が2014年11月に日本国内での提供を開始した法人・教育機関向けサービス「Device Enrollment Program」は、iOS デバイスを自動的に MDM サービス管理下に配置できるプログラムです。本プログラムに対応した MDM サービスを利用することで、MDM サービスに個別デバイスを登録するための各種作業を大幅に省力化し、iPhone / iPad の法人・教育機関利用におけるデバイス導入・運用コストを飛躍的に低減します。

「Device Enrollment Program」を利用すると「監視対象設定」や「MDM サービスへのデバイス登録強制（図3）」を行えるなど、多様な活用メリットがあります。当社ホームページにて、具体的な活用メリットやデモ動画などをご紹介します（図2）。是非、ご参照ください。

導入時の注意点

- 「Device Enrollment Program」を利用できる iOS デバイスは「Apple Japan」「Apple Store」「Apple 正規販売店」「携帯電話会社」を通じて法人販売契約で購入する必要があります。ただし、各社の提供準備状況には差があるため、必ず事前に「Device Enrollment Program」対応状況をお問い合わせの上ご購入ください。
- 「Device Enrollment Program」を通じて iOS デバイスを監視対象設定に変更する際にも、デバイスの初期化を実施する必要があります。

導入時のヒント

「Device Enrollment Program」と MDM サービスが提供するプロファイル自動適用機能を一緒に活用することで、キッティングの手間を大幅に削減できます。



図2. 「Device Enrollment Program」活用メリット解説
(引用元：<http://www.i3-systems.com/hint-device-enrollment-program.html>)

新機能：MDM サービスへのデバイス登録を強制



図3. MDM サービスへのデバイス登録強制の利用イメージ

(3) Volume Purchase Program

概要

Apple 社が2012年9月に日本国内での提供を開始した法人・教育機関向けサービス「Volume Purchase Program」は、「App Store アプリの一括購入」や、「効率的なアプリケーション配信・管理」を実施するために必要なサービスです (図4)。

「Volume Purchase Program」と MDM サービスを組み合わせることで、「アプリライセンスの回収 / 再配布」や「App Store アプリのサイレントインストール (図5)」を行えます。本サービスを利用することで、iPhone / iPad の法人活用におけるアプリ導入・運用コストを飛躍的に低減できます。

導入時の注意点

- アプリライセンスの回収/再配布機能を利用するには「Volume Purchase Program 管理配布方式」を利用する必要があります。
- App Store アプリのサイレントインストール機能を利用するには「Volume Purchase Program 管理配布方式」と「監視対象設定」を利用する必要があります。また、上記機能を利用する場合にも、利用規約の変更などに応じてApple IDなどの情報入力を求められることがあります。

導入時のヒント

- App Store アプリを新規 / 追加導入する際には、高度なアプリ管理 / 運用機能が将来的に必要なことを考慮し、予め、「Volume Purchase Program」を利用した上で社内に展開することを推奨します。
- 教育機関では「Volume Purchase Program」を通じてアプリの大量購入を行うことで、一部アプリではアカデミック価格が適用されます。



図4. Apple 社 Volume Purchase Program 紹介ページ
(引用元：<http://www.apple.com/jp/education/it/vpp/>)

アプリのサイレントインストール



図5. 「サイレントインストール」の利用イメージ

3. デバイス管理 / 運用機能の強化

(1) 「DEP エンロールメント」の最適化

概要

これまでは「Device Enrollment Program」を利用した場合、管理者は、初期設定のプロセス（図6）において、設定途中でプロファイルの適用を行うなど細かなプロセス制御を行うことはできませんでした。

iOS 9 では、「Device Enrollment Program」を通じた初期設定画面のプロセスの段階でそのステップを一時停止できるようになりました（図7）。初期設定を一時停止した状態で、MDM サービスを通じてプロファイルなどをインストールすることで、より望ましい状態のデバイスをユーザーに配布することができるようになります。

効果的な利用シーン

購入した iOS デバイスを社員に直接配布し、ユーザー自身に初期設定を行わせる場合にも、MDM サービスを通じて、より望ましい状態のデバイス設定を行った後に利用開始させられます。

導入時の注意点

- 本機能を利用するには「Device Enrollment Program」を利用する必要があります。
- MDM サービスが提供する「構成プロファイルの自動適用機能」などを同時に活用すると、図7における「現在の手順」を実施した際にも「デバイス利用開始」と「MDM 経由で機能制限・アプリを反映」のプロセスを自動化できるため、ユーザー自身が初期設定を行う際にも安心です。



図6.Device Enrollment Program を通じた初期設定の様子
(引用元：<http://www.i3-systems.com/hint-device-enrollment-program.html>)

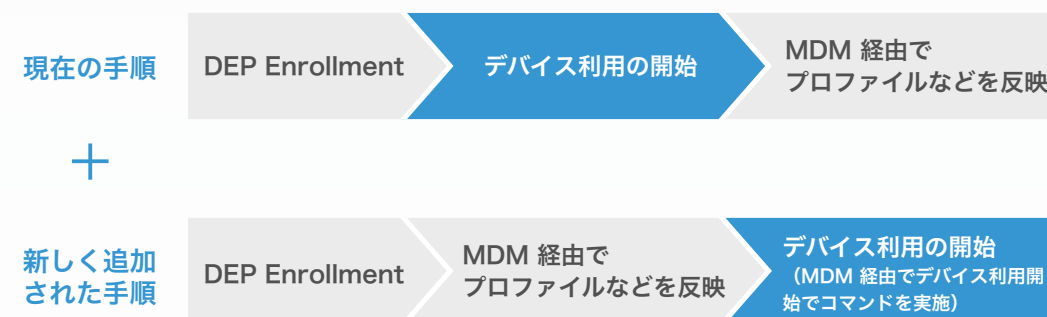


図7. 「DEP エンロールメント」の最適化で追加されたデバイス配備手順

(2) 「iOS」の強制アップデート

概要

これまでは、iOS のアップデートを遠隔では制御できず、MDM サービスが取得した iOS デバイスの OS バージョン情報を閲覧しながらユーザーにアップデートを促す必要がありました。

iOS 9 では、MDM サービスを通じて iOS のアップデートを強制実行できるようになりました（図8）。本機能によって、管理者はセキュリティ対策が強化されたより安全な OS へのアップデートをユーザーに強制できるようになりました。

効果的な利用シーン

従業員の手を煩わせることなく、計画的に iOS のアップデートを徹底できるため、セキュリティ対策が強化された状態を保てます。

導入時の注意点

- 本機能を利用するには、iOSデバイスを監視対象に設定する必要があります。
- 本機能を利用するには「Device Enrollment Program」を利用する必要があります。
- 本機能では、iOSの「バージョンダウン」「アップデート制限」は行えません。

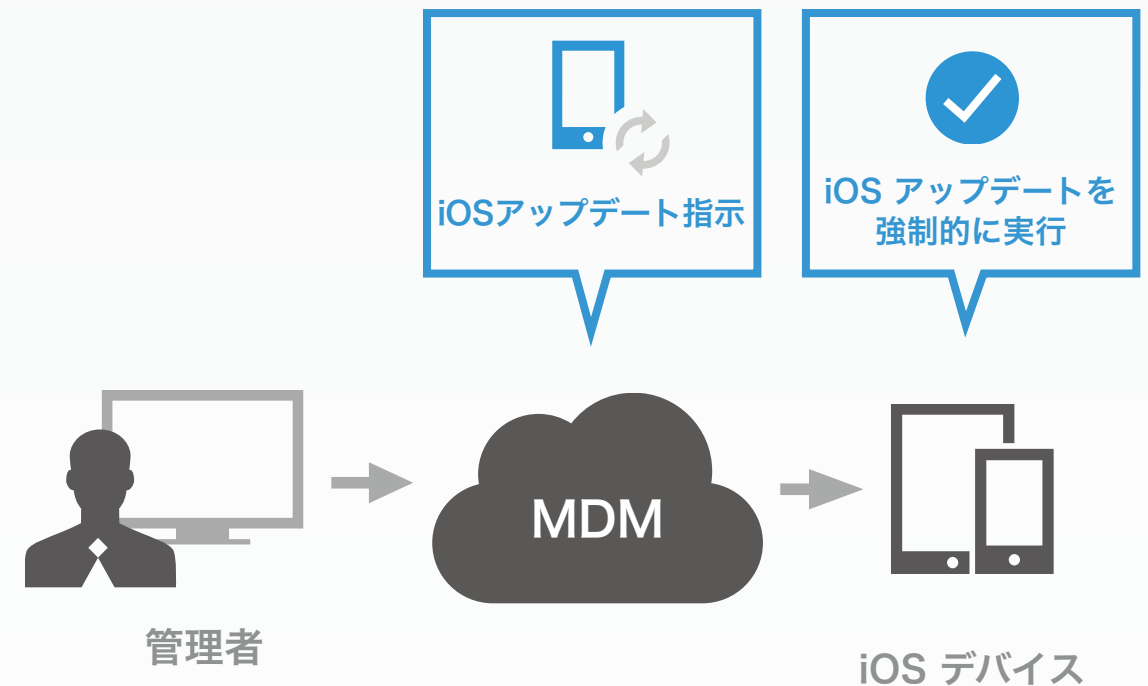


図8.MDM サービスを通じた「iOS アップデート強制」の運用イメージ

(3) 「パスコード変更」を制限

概要

これまでは、ユーザーの操作でパスコードや Touch ID の変更を行えました（図9）。

iOS 9 では、MDM サービスから iOS デバイスのパスコード変更機能制限を行えるようになったため、ユーザーが勝手にパスコードを変更できなくなりました（図10）。本機能制限によって、従業員や第三者による意図的な「パスコード変更」を確実に防止でき、管理者は、自社のセキュリティポリシーに準じたパスコード利用の徹底を手軽に実現できます。

効果的な利用シーン

従業員による勝手なパスコード変更を確実に制限します。

導入時の注意点

- 本機能を利用するには、iOSデバイスを監視対象に設定する必要があります。
- パスコード制限を行う場合には、同時に Touch ID（指紋認証）の変更も制限されます。

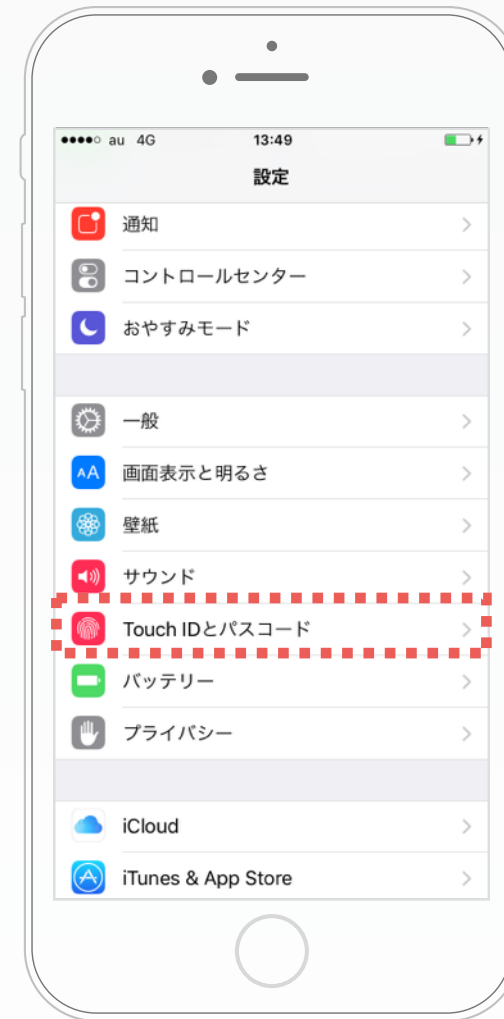


図9. 変更可能な状態

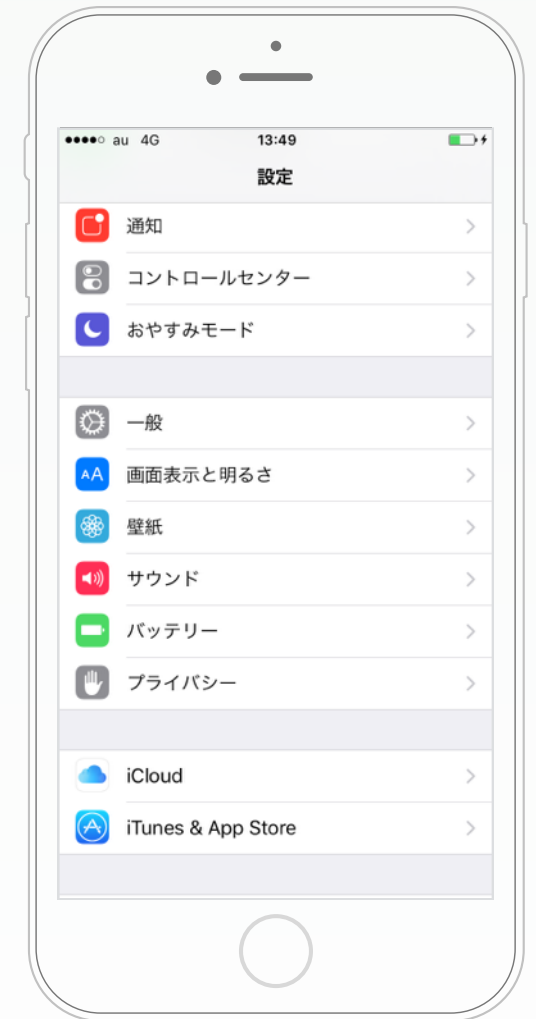


図10. 変更不可能な状態

(4) 「DEP エンロールメント」の自動化

概要

これまでは、「Device Enrollment Program」を利用する際にも多くの設定アシスタントを操作する必要があり、特に、パスワード入力が必要なWi-Fiネットワークへの接続などは、デバイスから手動で行う必要があったため、大量デバイスを同時にキッティングする際に手間となっていました。

iOS 9 では、「Apple Configurator 2」を通じて、デバイス準備時点の初期設定作業をさらに省略できるようになりました（図11）。

効果的な利用シーン

- デバイス導入 / 運用時点でのキッティング作業を単純化でき、アウトソーシングなども含めて効率的に実施できるようになります。
- 接続時にパスワード認証を求められる Wi-Fi 環境下のキッティング環境において、パスワード入力を省略できるため、作業の手間を削減できます。

導入時の注意点

- 本機能を利用するには「Device Enrollment Program」を利用する必要があります。
- 本機能を利用するには「Apple Configurator 2」を利用する必要があります。
- 「Apple Configurator 2」からインストールした「プロファイル」「アプリ」には、MDM サービスの高度な管理機能を利用できません。「Apple Configurator 2」を利用した初期設定の完了後に、MDM サービスから「プロファイル」「アプリ」をインストールすることを推奨します。
- 本機能利用時に設定したWi-Fiプロファイルは、DEPエンロールメントの初期設定時にのみ有効です。初期設定後には別途設定する必要があります。

初期設定時の表示画面	Apple Configurator 2	
言語	○ (スキップ可能)	※
国または地域を選択	○ (スキップ可能)	※
キーボード	× (スキップ不可)	
Wi-Fi ネットワークを選択	○ (スキップ可能)	※
位置情報サービス	○ (スキップ可能)	
Apple ID	○ (スキップ可能)	
Siri	○ (スキップ可能)	
Apple Pay	○ (スキップ可能)	
利用規約	○ (スキップ可能)	
復元	○ (スキップ可能)	
パスコード	○ (スキップ可能)	
Touch ID	○ (スキップ可能)	
診断	○ (スキップ可能)	
画面表示の拡大	○ (スキップ可能)	

図11. DEP エンロールメントの自動化によって省略可能な初期設定項目
※ Apple Configurator 2 を使用した時のみスキップ可能となる項目です。

4. アプリ管理 / 運用機能の強化

(1) Apple ID を利用しない App Store アプリの遠隔インストール

概要

これまでは、MDM サービスを通じて Apple ID を登録していない iOS デバイスに対して App Store アプリはインストールできませんでした。

iOS 9 では、MDM サービスを通じて、Apple ID を登録していない iOS デバイスにも App Store アプリのインストールを行えるようになりました(図12)。「Volume Purchase Program」とデバイスの Apple ID を紐付ける招待プロセスも不要になるため、管理者の iOS アプリ導入 / 運用時の手間を大きく削減できます。

効果的な利用シーン

- 「Volume Purchase Program」管理配布方式への参加招待のプロセスを省略でき、アプリ管理を行う際の初期設定コストを削減できます。
- 本機能を利用することで、会社が購入したアプリライセンスを業務用として認めたデバイス以外で利用できないように運用できます。

導入時の注意点

- デバイスの識別はシリアルナンバーによって行われます。
- 本機能を利用するには、Apple 社 Volume Purchase Program の「管理配布方式」で入手したアプリケーションライセンスを利用する必要があります。
- Apple ID を利用しない遠隔インストールを行う場合には、デバイスごとにアプリのライセンスが付与され、アプリのライセンス数がデバイス数分必要になります。

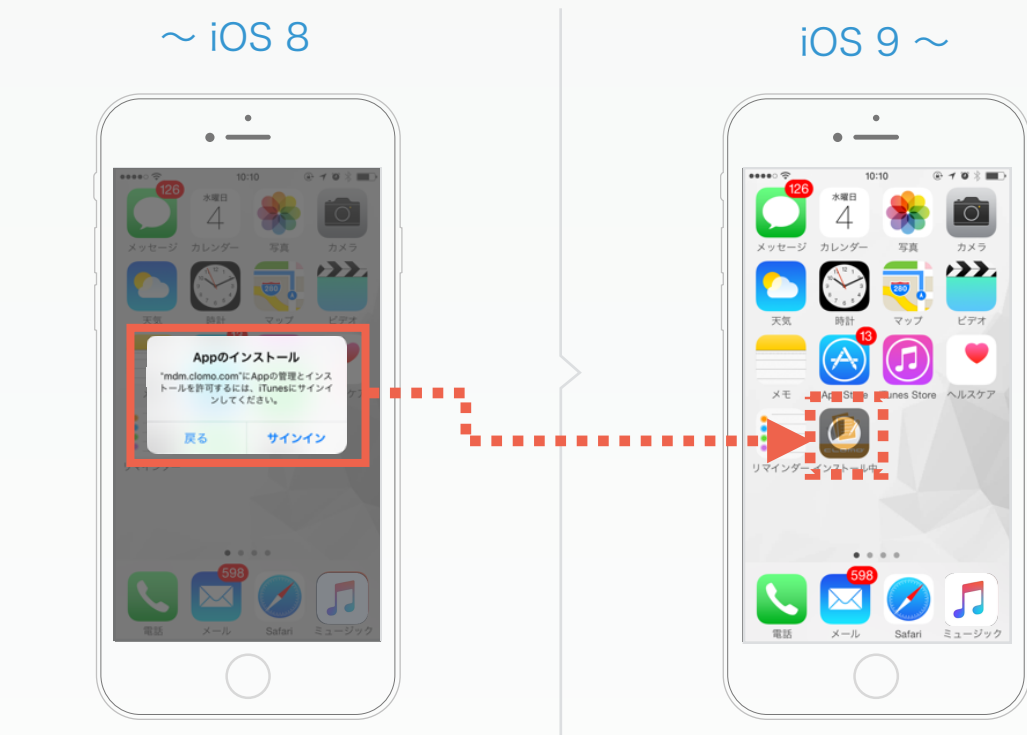


図12.Apple ID を利用しない App Store アプリ遠隔インストール利用イメージ

	Apple ID	
	利用する	利用しない
VPP 管理配布方式	自由	必須
VPP 招待プロセス	必要	不要
アプリ購入履歴の表示 (デバイス側)	表示される	表示されない
アプリのインストール・アップデート	App Store 経由で実施 (ユーザーも可能)	MDM 経由で実施 (管理者のみ可能)
購入ライセンス数	Apple ID 数量分	デバイス数量分

図13.Apple ID の利用状況によって生じるアプリ運用の違い

(2) App Store を経由しない App Store アプリの遠隔インストール

概要

これまでは、App Store の利用制限を実施した状態で App Store アプリのインストールやアップデートを行えないため、App Store アプリのために、App Store の利用制限を一時解除する必要がありました。そのため、インストールやアップデート作業の途中に、制限解除された App Store を通じてデバイスユーザーが禁止アプリをインストールする可能性が生じ、これらの対策を講じることに大きな手間が生じていました。

iOS 9 では、App Store の利用制限を実施したまま、MDM サービスを通じて App Store アプリの遠隔インストールやアップデートを行えます（図 14）。管理者は本機能を利用することで、MDM サービスを通じて、App Store アプリのインストールやアップデートを確実に、手間なく制御できるようになりました。

効果的な利用シーン

- 業務外のアプリインストールを制限したまま、業務用アプリをインストールでき、アプリ管理の手間を削減します。
- App Store の利用制限を継続して実施することにより、App Store アプリの自動アップデートも制限できます。

導入時の注意点

今後、App Store の機能制限に監視対象設定が必要になる見込みです。監視対象設定の導入を前向きにご検討ください。

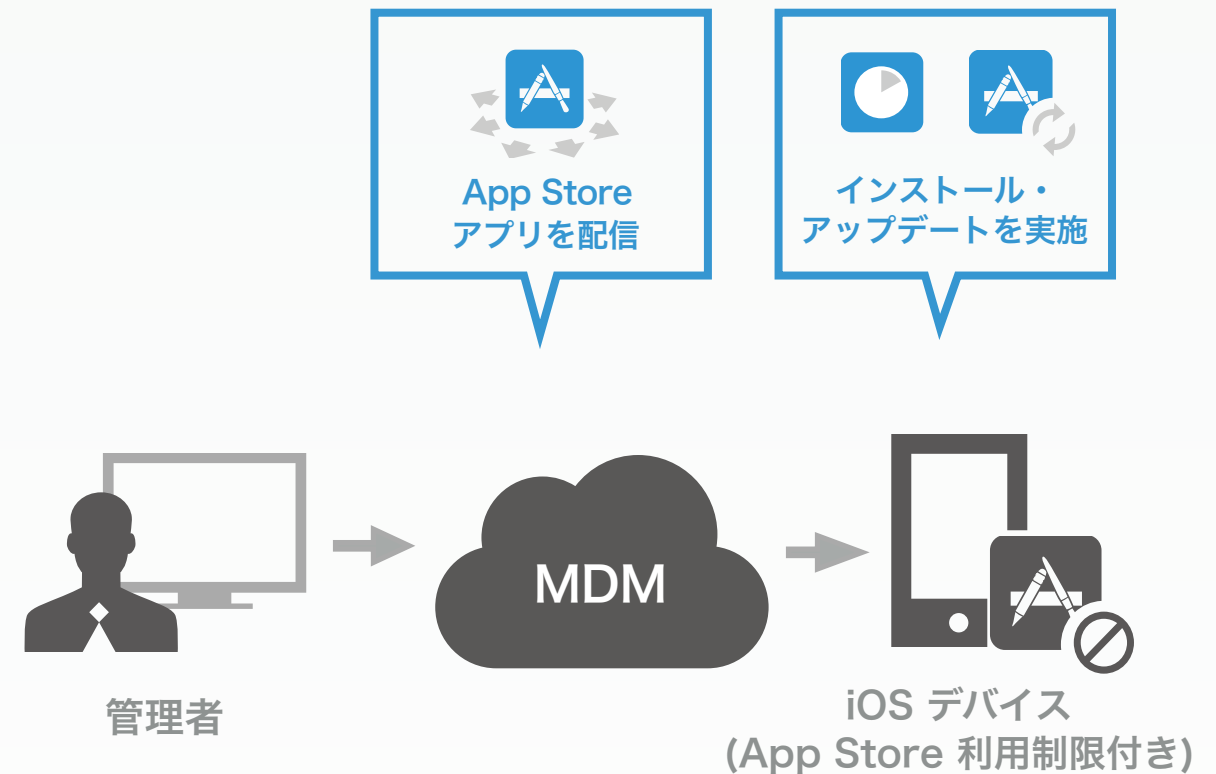


図14. MDMサービス を通じてアプリの遠隔インストールする運用イメージ

(3) インストール済みアプリの Managed Apps 移行

概要

これまでは、iOS デバイスにインストール済みのアプリを Managed Apps に移行できず、Managed Apps として利用するには、すでにインストールされているアプリをデバイス側で一旦削除した後に、MDM サービス経由で Managed Apps アプリとして、再インストールする必要がありました。

iOS 9 では、iOS デバイスにインストール済みのアプリを MDM サービスを通じて再インストールすることなく、Managed Apps に移行できるようになりました（図15）。本機能を利用することで管理者は、従業員が勝手にインストールしたアプリに対して、高度なアプリ管理機能を利用したい場合に手間なく導入できるようになります。

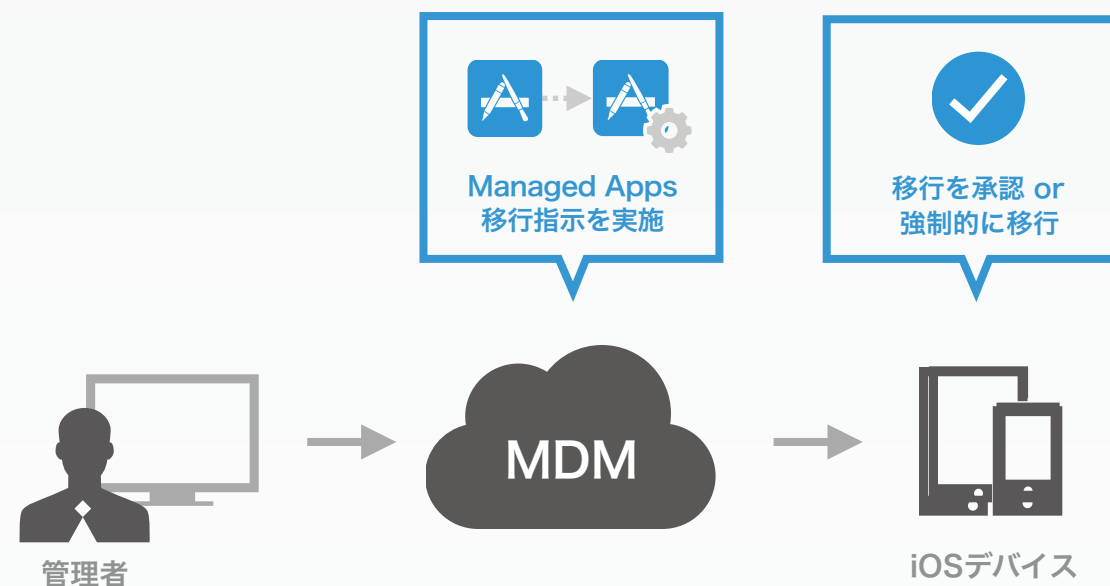


図15.MDM サービスを通じた Managed Apps 以降の運用イメージ

効果的な利用シーン

デバイスユーザーが勝手にインストールした利用禁止アプリを強制的に削除などの運用を行えるようになります（図16）。

導入時の注意点

- 本機能を用いて、Managed Apps を 非 Managed Apps に移行することは行えません。
- 監視対象に設定された iOS デバイスでは、Managed Apps 移行時にユーザーの承認を必要としませんが、監視対象に設定されていない iOS デバイスではユーザーの承認が必要です。
- アプリの Managed Apps 設定を有効にするには、MDM サービスの利用が必要です。

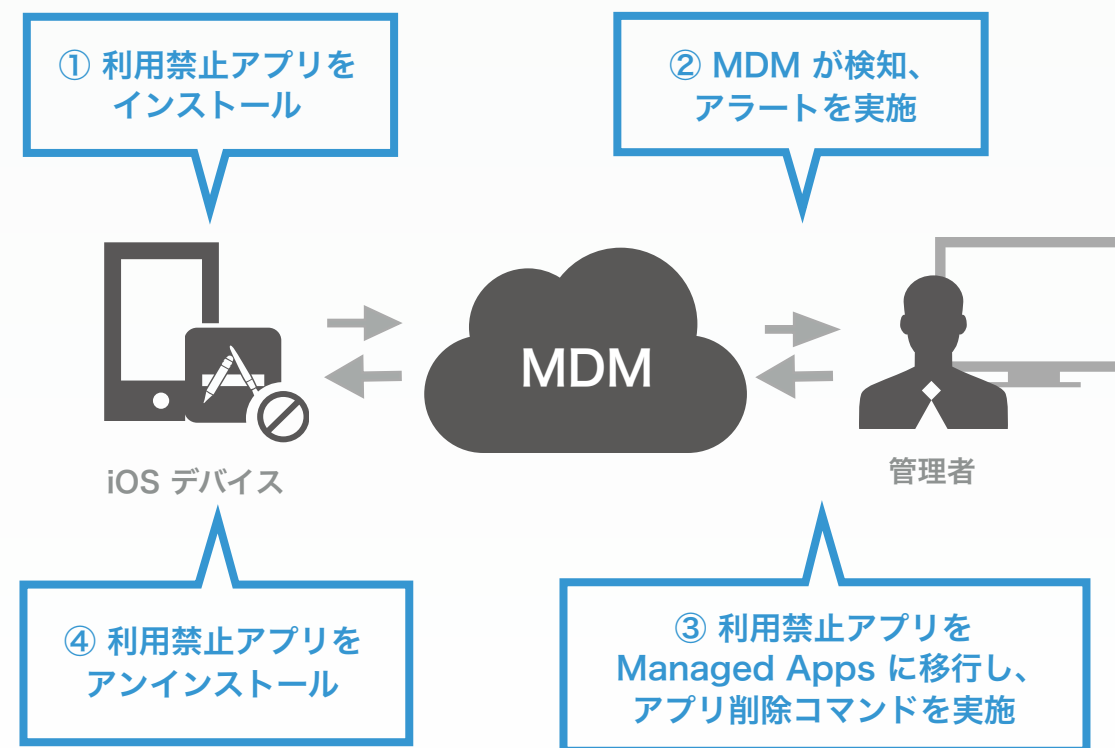


図16. インストールしたアプリを Managed Apps に移行する運用イメージ

(4) 「新しい独自アプリ作成元の信頼」を制限

概要

iOS 9 では、独自アプリを利用する際に、信頼できる作成元かどうかをデバイスのユーザーが承認する機能が追加されました。承認されない場合には、独自アプリを全く利用できません。

上記機能の追加と共に、MDM サービスを通じて「独自アプリ配布元の信頼」をデバイスユーザーが勝手に行えないように制限できるようになりました（図17）。

効果的な利用シーン

従業員がインターネットなどで入手し、インストールした独自アプリの勝手利用を禁止できます。

導入時の注意点

特にありません。

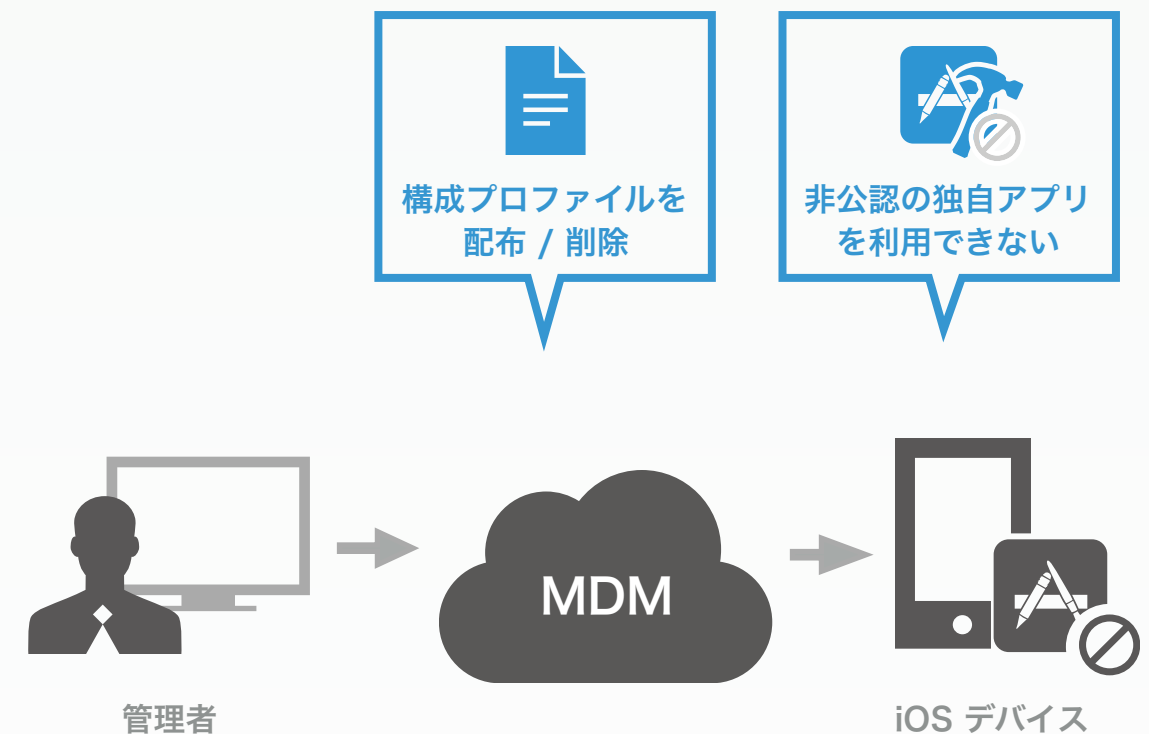


図17.MDM サービスを通じた「新しい独自アプリ作成元の信頼」制限の運用イメージ

5. コンテンツ管理 / 運用機能の強化

(1) 「Managed Apps での AirDrop 機能」を制限

概要

これまで、AirDrop 機能を通じてアプリ内の各種データを他の iOS / Mac デバイスに送付でき、本機能を通じた業務データの漏えい対策を実施するには、AirDrop 機能の利用を完全に制限する必要がありました。

iOS 9 では、Managed Apps に限り、AirDrop 機能を使わせないように制限できるようになりました (図18)。

効果的な利用シーン

業務用アプリに関しては、機密データ漏えいに配慮しながら、業務アプリ以外のアプリでの利便性を損なわない運用を行えます。

導入時の注意点

アプリの Managed Apps 設定を有効にするには、MDM サービスを利用する必要があります。

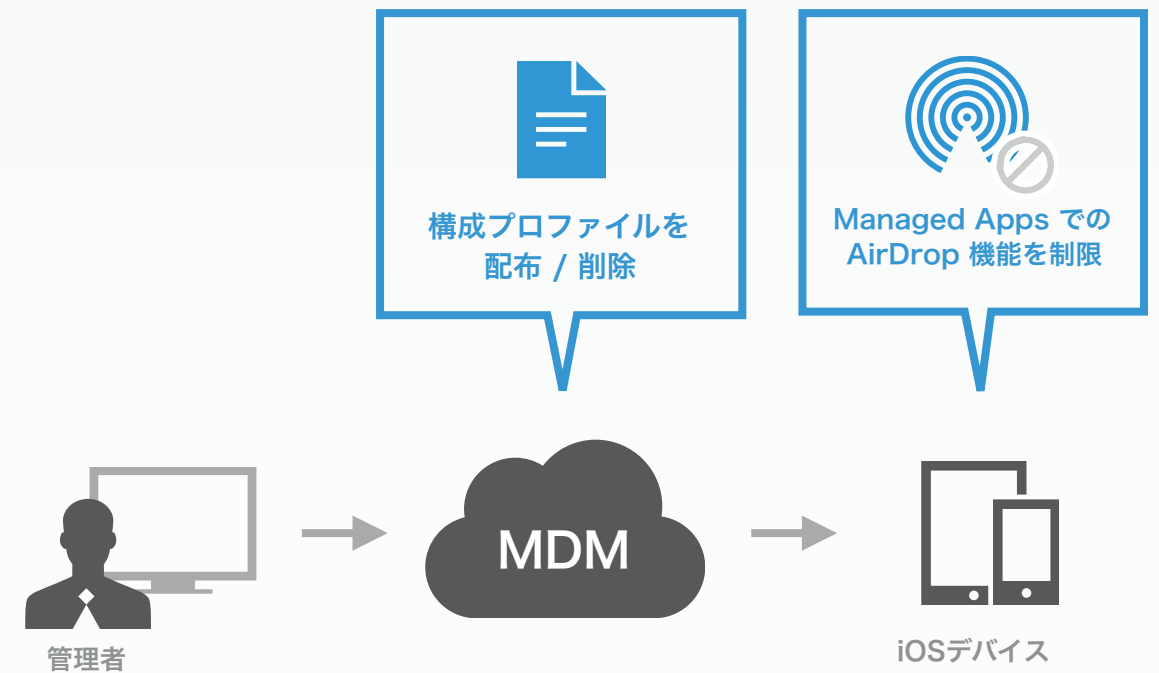


図18.MDM サービスを通じた Managed Apps 設定後の運用イメージ

最後に

弊社は、2010年10月に国内初の iOS 向け MDM サービス「CLOMO MDM」を提供開始して以来、iOS の進化にあわせて対応を進めて来ました。特に、iOS 5 以降の進化は目覚ましく、企業利用に望ましい理想へと近づいています。

弊社は CLOMO の提供を中軸に、CLOMO の導入検討やトライアル、導入後の活用拡大のご提案や、CLOMO 製品のサポート、スマートデバイスの効率的な運用・管理、高度な活用に向けてのアドバイスを行うサービスを提供しています。皆様が iOS デバイスのビジネス向け機能を適切に体感頂けるように、しっかりとサポート致します。iOS デバイスの運用や活用でお悩みの方は是非、弊社へのお問い合わせや、CLOMO のトライアルプログラムをご検討ください。

本資料を末尾までご覧頂きまして、誠にありがとうございました。

今後も、弊社は法人スマートデバイス市場のフロントランナーとして、最新で最良の技術をご利用ユーザーの皆様へ、いち早く提供できるよう努力していく所存です。何卒よろしく願いいたします。

CLOMO トライアルプログラムお申込み先：<http://www.i3-systems.com/trial-order/>

本資料についての問い合わせ先：<http://www.i3-systems.com/>



Innovation³

- ※ 本資料「iOS 9 ビジネス向け機能強化ポイント解説」は、2015年11月20日現在におけるアイキューブドシステムズが独自に調査した結果に基づいたものです。
- ※ 「CLOMO」「i3Systems」は、株式会社アイキューブドシステムズの登録商標です。
- ※ iPhone、iPad は、米国ならび他の国々で登録された Apple Inc. の商標です。
- ※ App Store は Apple Inc. のサービスマークです。
- ※ iPhone 商標は、アイホン株式会社のライセンスに基づき使用されています。
- ※ 文中の社名、商品名等は各社の商標または登録商標である場合があります。