iOS 8 ビジネス向け機能強化ポイント解説

主要な機能強化解説と iOS 管理・運用の最新スタイルについて

株式会社アイキューブドシステムズ
2014/10

目次

はじめに

2014年9月にリリースされた iOS 8 は「iCloud Drive」や「他社製キーボードの対応」など、様々に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、3年連続で MDM 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 8 を適切に導入・活用できるように、iOS 8 の主要なビジネス向け機能強化と最新 iOS で実現できる管理・運用スタイルをご紹介します。

1. iOS 8 のビジネス向け機能強化一覧

1. iOS 8 のビジネス向け機能強化一覧

iOS 8 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

- アクティベーションロックの強制解除*
- 「機能制限」の解除を制限*
- 「すべてのコンテンツと設定を消去」の実行を制限*
- iCloud バックアップ最終日時の取得
- iOS デバイスの名前 / 壁紙を設定*
- Spotlight でのインターネット検索を制限
- 「機能制限」のパスコードを解除*

ネットワーク運用機能の強化

- VPN の常時接続設定を追加*
- VPN（IKEv2 形式）に対応
- Wi-Fi 接続時のワンタイムパスワードに対応

iOS デバイスでの構成プロファイル確認手法の強化

- 構成プロファイルの一覧表示画面を改善
- 証明書の詳細情報表示に対応

アプリ 管理 / 運用機能の強化

MDM サービス機能の強化

- Handoff の利用を制限

アプリ起動時の認証強化

- Touch ID を認証要素に追加
- アプリケーション SSO に電子証明書を追加

コンテンツ 管理 / 運用機能の強化

MDM サービス機能の強化

- Enterprise Books の配布 / 削除*
- Managed Books の配布 / 削除*
- Enterprise Books のバックアップを制限
- Enterprise Books のメモとハイライトを制限
- Managed Apps での iCloud Sync 機能を制限

「Safari」運用機能の強化

- Web フィルタリングの外部プラグイン対応*
- 「管理対象の Safari Web ドメイン」設定を追加*

「メール」運用機能の強化

- 「マークされていないメールドメイン」設定を追加*

アプリ間データ連携機能の強化

- App Extension 機能を追加

* 本機能、もしくは本機能の一部を利用するには、Apple Configurator を用いて、iOS デバイスを監視対象に設定する必要があります。

1-1. iOS 8 を徹底活用するための事前準備

iOS デバイスの監視対象設定

概 要

iOS 5 以降、Apple 社が提供するアプリ Apple Configurator を通じて、iOS デバイスを監視対象に設定できるようになりました。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、P4 の機能強化一覧で示した通り、iOS 8 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 を利用して iOS デバイスを監視対象に設定する際には、iOS デバイスを Mac に有線で接続し、デバイスの初期化を実施する必要があります。
- Apple Configurator 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になることを考慮し、予め、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 のダウンロード画面
(引用元：https://itunes.apple.com/jp/app/apple-configurator/id434433123?mt=12)

1-2. デバイス管理 / 運用機能の強化

(1) アクティベーションロックの強制解除

概 要

iOS デバイスの盗難や紛失が発生した場合に、第三者がそのデバイスを使ったり、売却することを難しくするための機能として、アクティベーションロックが提供されています。今まで「iPhone を探す」アプリからアクティベーションロックを設定すると、Apple ID / Password を入力しないかぎり、デバイス上のデータを消去したり、アクティベートし直すことは誰にもできませんでした(図2)。

iOS 8 では、管理者が iOS デバイスに設定されたアクティベーションロックを MDM サービスから強制的に解除できるようになりました。管理者は、本機能を利用することで、デバイス資産の喪失を抑止できます。

効果的な利用シーン

「従業員の入院 / 退職などによって、アクティベーションロックされたデバイスに設定されている Apple ID / Password が分からなくなった場合に、デバイスの再設定を行えなくなった」などのケースに対処できるようになりました。

導入時の注意点

- 本機能を利用するには、Apple Configurator を利用して iOS デバイスを監視対象に設定する必要があります。
- アクティベーションロックそのものは手動で行う必要があります。

図2. アクティベーションロック設定時

(2)「機能制限」の解除を制限

概 要

これまでは、管理者は MDM サービスから配布する構成プロファイルによる機能制限に加えて、デバイスの「機能制限」を利用して設定を行っていました。しかし、「機能制限」のパスワードは４桁の数字以上の設定を行えないため、意図的な解除行為を完全に防ぎきれませんでした (図3)。

iOS 8 では、「機能制限」の解除の可否を構成プロファイルで制限できるようになりました。本機能制限によって、従業員や第三者による意図的な「機能制限」の解除を確実に防止でき (図4)、管理者は、本機能制限を利用することで、統一したデバイス管理を手軽に実現できます。

効果的な利用シーン

「デバイスに設定された機能制限に不満を感じた従業員が、偶然入力したパスワードで認証が通り、位置情報サービスを利用できないように設定変更をした結果、業務に必要なアプリが正常に動作しなくなってしまった。」などのケースに対処できるようになりました。

導入時の注意点

・本機能を利用するには、Apple Configurator を利用して iOS デバイスを監視対象に設定する必要があります。

図3. 解除可能な状態
(～ iOS 7)

図4. 解除不可能な状態
(iOS 8 ～)

(3)「すべてのコンテンツと設定を消去」の実行を制限

概 要

これまでは、ユーザーの操作で「すべてのコンテンツと設定を消去」を実行でき、iOS デバイスの初期化を行えました (図5)。

iOS 8 では、MDM サービスから「すべてのコンテンツと設定を消去」を無効にする設定が可能になったため、ユーザーが勝手に iOS デバイスを初期化できなくなります(図6)。管理者は、本機能制限を利用することで「運用コストの低減」と「デバイス資産の喪失抑止」を実現します。

効果的な利用シーン

・従業員が「すべてのコンテンツと設定を消去」を誤ってタップし、デバイスの初期化を行ってしまった。
・紛失や盗難が発生した際に、第三者がデバイスの初期化を実施し、デバイスの再利用 / 売却が行われた。

など、上記のようなケースでの初期化を防げるようになりました。

導入時の注意点

・本機能を利用するには、Apple Configurator を通じて iOS デバイスを監視対象に設定する必要があります。

図5. 初期化可能な状態
(～ iOS 7)

図6. 初期化不可能な状態
(iOS 8 ～)

(4) VPN の常時接続設定を追加

概 要

今までも、VPN に接続できる「オンデマンド VPN」の設定を行え、社内システムのアクセスを実現する際に活用されてきました。しかし、常時接続設定を行えませんでした。

iOS 8 では、「オンデマンド VPN」の設定で常時接続設定を行えるようになりました。管理者は、本機能強化と MDM サービスを利用することで、ユーザーにとっても負担の無い、安全な社内システム接続環境を構築できます(図8)。

効果的な利用シーン

「VPN 接続をユーザーに徹底することができなかった」などのケースに対処できるようになりました。

導入時の注意点

- 「オンデマンドVPN」の常時接続設定を行うには、VPN（IKEv2形式）の利用が必要です。その他形式の VPN では設定を利用できません。
- 本機能を利用するには、Apple Configurator を通じて iOS デバイスを監視対象に設定する必要があります。

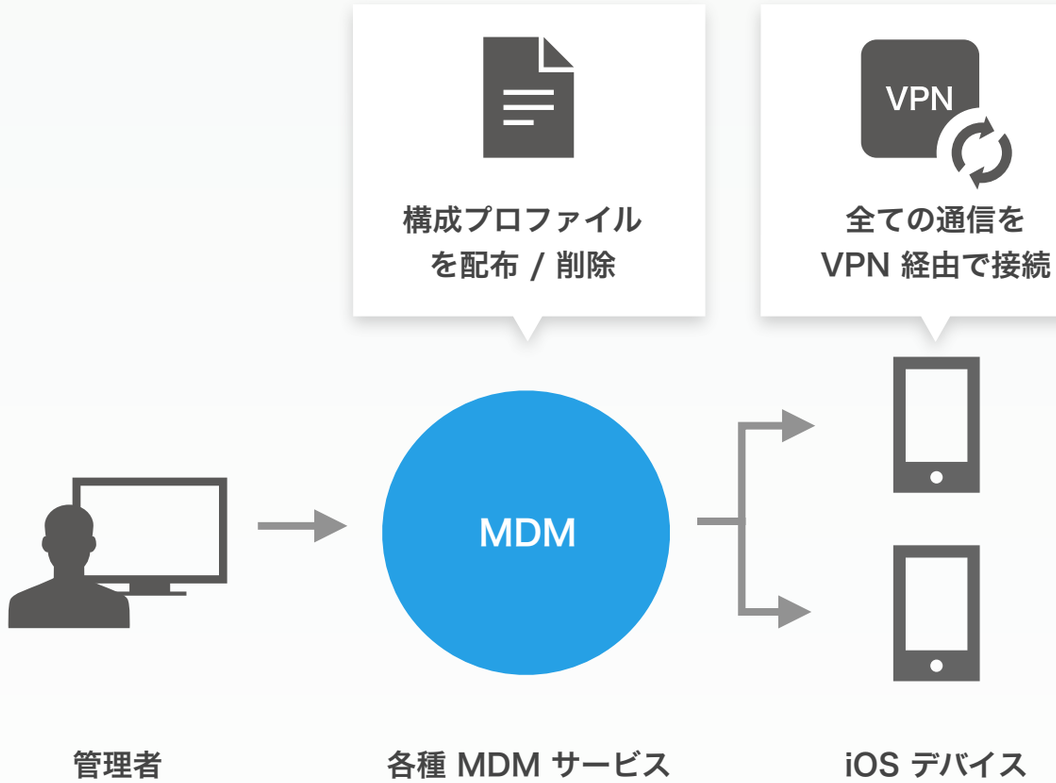


図7. MDM サービスを通じた VPN の常時接続設定の運用イメージ

(5) 構成プロファイルの一覧表示画面を改善

概 要

これまでは、MDM サービスで設定した構成プロファイルを、iOS デバイスの設定画面で一覧表示できました。

iOS 8 では、MDM サービスで設定した構成プロファイル自体の一覧表示画面がモバイルデバイス管理の項目に統合され、MDM サービスで設定した構成プロファイルによる機能制限を、まとめて一覧できる画面に改善されました(図7)。

本機能改善によって、管理者とユーザーの双方がデバイスの設定画面から機能制限を確認しやすくなりました。

効果的な利用シーン

・機能制限を重複反映させた場合に、想定通りの機能制限が反映されているか、動作確認をしないと分からなかった。
・制限されている機能の確認手順が複雑で、デバイスの機能に不満を持つ従業員が管理者に何を伝えて良いか分からなかった。

など、上記のようなケースに以前よりも対処しやすくなりました。

導入時の注意点

・本改善は iOS 8 にアップデートするとすぐに反映されます。機能制限の設定確認画面をデバイス導入 / 運用サポートマニュアルなどに利用されている方はご注意ください。
・プロビジョニングプロファイルの表示 / 期限切れの通知はデバイスから行われないようになりました。プロビジョニングプロファイルを利用されている方は、MDM サービスを通じて取得できる有効期限をご確認ください。

図8. 構成プロファイル表示画面の変更ポイント

1-3. アプリ管理 / 運用機能の強化

(1) Handoff の利用を制限

概 要

iOS 8 では、Handoff 機能を利用できるようになりました。Handoff 機能を利用すると、メールやメッセージの作成、Safari の閲覧など、iOS デバイスで進行中の作業を別のデバイスに引き継いで行えます。iOS 8 を搭載した iPhone / iPad 間をシームレスに移行するだけでなく、Mac OS X Yosemite を搭載した Mac との連携も行えます。

非常に便利な Handoff 機能ですが、運用次第では、この Handoff を制限したい場合もあると思われます。このような場合、管理者は MDM サービスを通じて構成プロファイルを遠隔で配布 / 削除できるようになりました。本機能制限を利用することで、Handoff 機能の利用によって生じる、不測の業務データ漏えいを防止できます (図9)。

効果的な利用シーン

「iPhone で長文のメールを書きづらいと感じた従業員が、Handoff 機能を利用して私物の Mac にメールデータを連携し、私物 Mac の送信済みメールフォルダに重要な業務データを含む添付ファイルを保存した。」などのケースに対処できるようになりました。

導入時の注意点

現在の Handoff 機能の制限設定では「メールアプリのみ制限する」「Safari アプリのみ制限する」など、個別性の高い制限を現段階では行えません。

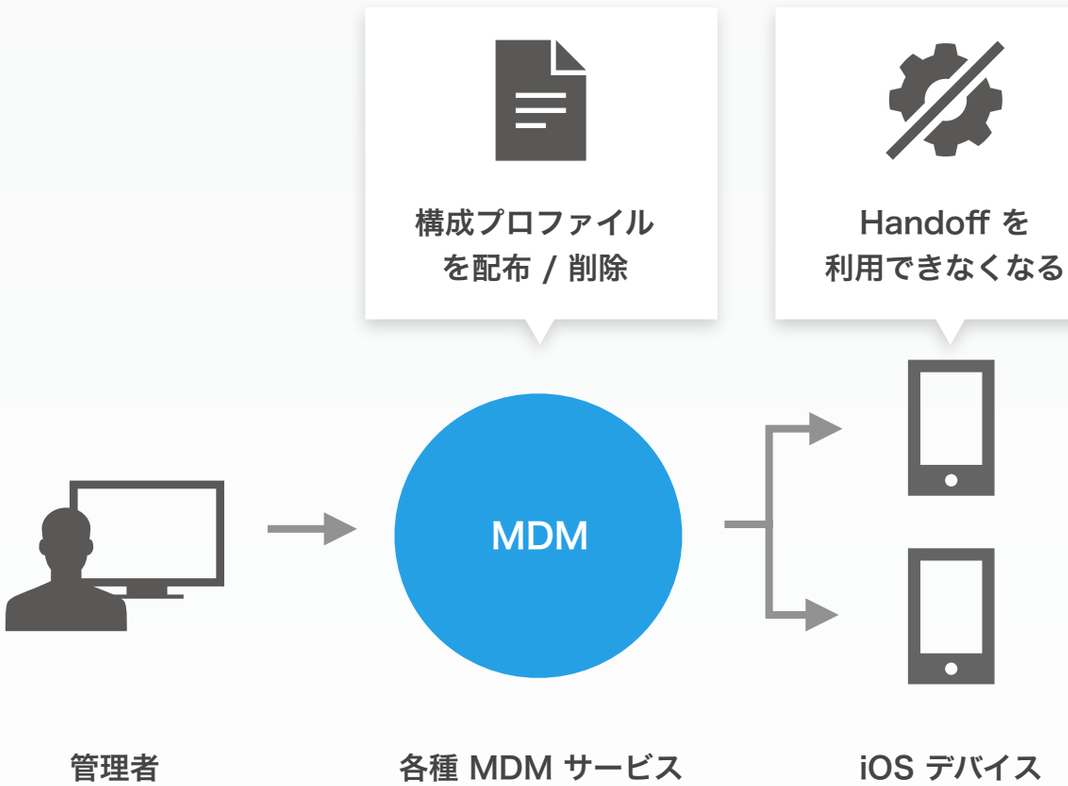


図9. MDM サービスを通じた Handoff 利用制限の運用イメージ

(2) Touch ID を認証要素に追加

概 要

　これまでは、独自アプリを開発する際に、アプリ起動時の認証要素に ID / Password に代表される方式以外の認証機構を開発できませんでした。

　iOS 8 では、独自アプリを開発する際に、アプリの認証機能として Touch ID（指紋情報）を設定できるようになりました。本認証機能の追加によって、管理者は業務データ漏えいのリスクを大きく軽減すると同時に、ユーザーの手間を省くアプリを開発できるようになります (図10)。

効果的な利用シーン

・アプリ起動のための ID / Password を従業員が忘れてしまい、管理者に多数の問い合わせが発生した。
・デバイスの盗難 / 紛失が発生した場合に、第三者が業務用のアプリを起動しようと ID / Password の解除を試みた。

など、上記のようなケースに以前よりも対処しやすくなりました。

導入時の注意点

・全てのアプリが Touch ID 認証に対応したわけではありません。対応状況は各社アプリ開発ベンダーにお問い合わせください。
・独自アプリを開発するには、iOS Developer Program / iOS Developer Enterprise Program に登録する必要があります。
・現在、Touch ID を利用できるデバイスは、iPhone 5s / iPhone 6 / iPhone 6 Plus のみです。

図10. Touch ID とパスワードを
併用した場合に表示される画面イメージ
（引用元：http://support.apple.com/kb/HT5883?viewlocale=ja_JP）

(3) アプリケーション SSO に電子証明書を追加

概 要

iOS 7 から、独自アプリを開発する際に、アプリ起動時の認証をシングルサインオン（以下、SSO）アカウントを利用できるようになりました。

iOS 8 からは、上記 SSO アカウントの認証の際に電子証明書を用いることが可能になりました。なお、電子証明書によるデバイス認証を MDM サービスとともに利用することで、管理者は強固な認証とユーザーの使い勝手を両立するアプリ運用環境を実現できます (図11)。

さらに、電子証明書はデバイスのネットワーク接続状況に関わらず、認証局側で電子証明書の失効を行えるため、もしもの際には、紛失したデバイスによるアプリ起動を確実に無効化できます。

効果的な利用シーン

「アプリケーションSSOは便利だが、認証が心配なので、電子証明書も使いたい」のようなケースに対処できるようになりました。

導入時の注意点

- 全てのアプリが「電子証明書ベースの SSO」に対応したわけではありません。対応状況は各社アプリ開発ベンダーにお問い合わせください。
- 独自アプリを開発するには、iOS Developer Program / iOS Developer Enterprise Program に登録する必要があります。
- 電子証明書の配付 / 失効機能は、MDM サービスごとに実装の方法が異なります。事前にご確認ください。

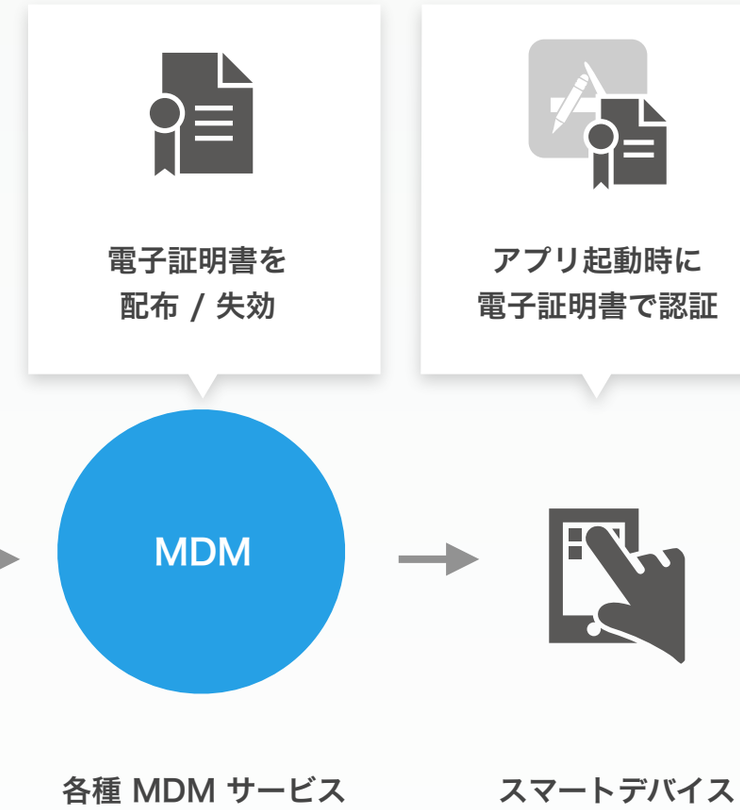


図11. MDM サービスと電子証明書による端末認証環境の運用イメージ

1-4. コンテンツ管理 / 運用機能の強化

(1) Enterprise Books の配布 / 削除

概 要

iOS 8 では、Enterprise Books の配布 / 削除機能が追加されました。本機能を利用すると、企業が独自に作成した電子書籍を MDM サービスを通じて配布 / 削除できるようになりました (図12)。なお、配布した電子書籍は iBooks アプリを通じて閲覧できます。

管理者は、提案資料や設計資料など、企業独自の電子書籍を一般公開せずに従業員のデバイスに配布できるようになりました。最新の電子書籍共有を徹底できると共に、ユーザーも手軽に電子書籍を利用できます。

効果的な利用シーン

「客先で提示した製品資料が最新でなかったため、オフィスに戻り、最新の製品資料を準備してから客先を再訪問したため、二度手間になった。」などのケースに対処できるようになりました。

導入時の注意点

- Enteprise Books の配布 / 削除機能は MDM サービスごとに実装の方法が異なります。事前にご確認ください。
- Enterprise Books の配布 / 削除機能を利用する際には、企業独自の電子書籍はクラスCの暗号化によるデータ保護処理が施されます。
- Enterprise Books のサイレントインストール機能を利用するには、Apple Configurator を用いて、iOS デバイスを監視対象に設定する必要があります。

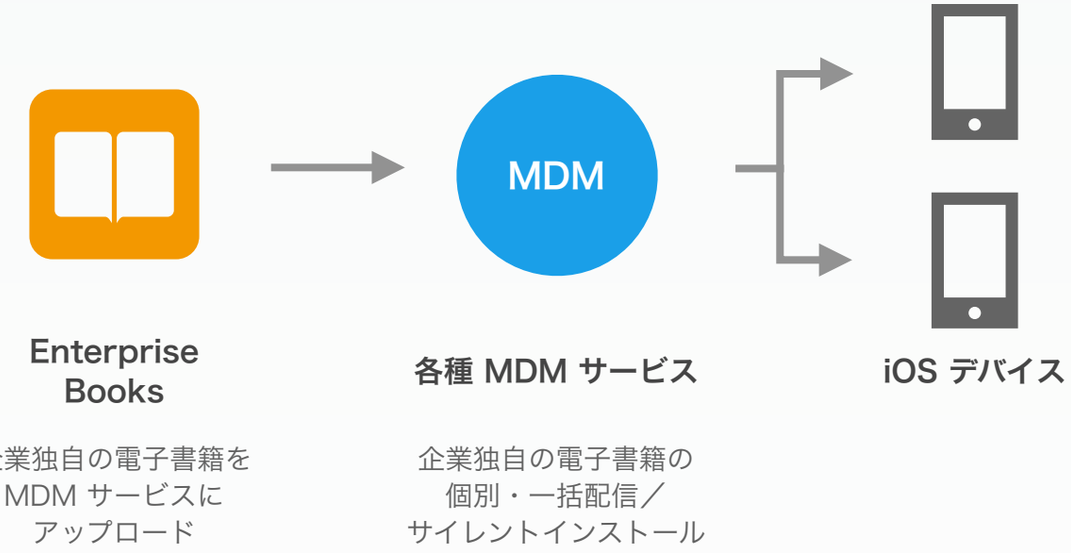


図12. Enterprise Books を配布 / 削除する際の運用イメージ

(2) Managed Books の配布 / 削除

概 要

Apple 社が運営する iBooks Store で販売されている電子書籍（有償・無償を問わない）を、 Managed Books として MDM サービスを通じて配布 / 削除できるようになりました。なお、配布した電子書籍は iBooks アプリを通じて閲覧できます。

本機能強化によって、管理者は効率的に電子書籍の配布を行えるようになると共に、ユーザーも電子書籍を手軽に利用できます。

効果的な利用シーン

「社内研修で利用する電子書籍を購入させるために、電子書籍の購入を従業員自身に行わせたが、購入方法の問い合わせ対応や購入漏れなどが続き、管理者がサポートに追われた。」などのケースに対処できるようになりました。

導入時の注意点

- Managed Books として配信する電子書籍は、有償 / 無償を問わず、Apple 社が提供する Volume Purchase Program（以下、VPP）を通じて購入する必要があります。（VPP について詳しくは、http://www.apple.com/jp/business/vpp/ をご覧ください。）
- 電子書籍をサイレントインストールするには、「VPP 管理配布方式」と「iOS デバイスの監視対象設定」が必要です。

導入時のヒント

- 「VPP 管理配布方式」を利用すると、電子書籍のライセンスを回収・再配布できるため、ライセンス購入数を最適化できます (図13)。

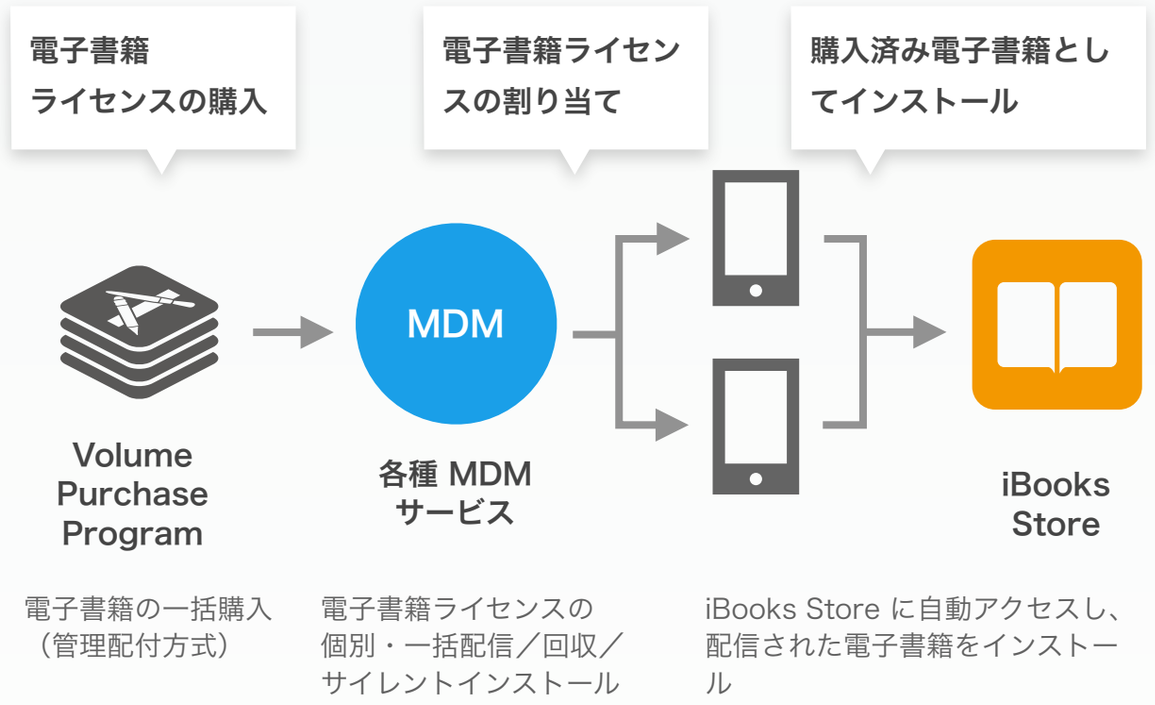


図13. iBooks Store の電子書籍を配布 / 削除する際の運用イメージ

(3) Web フィルタリングの外部プラグイン対応

概 要

これまでも、Safari に Apple 社独自のウェブコンテンツフィルタリング機能を適用できましたが、「詳細なカテゴリ設定を行えない」「フィルタリングの精度が日本に対応しきれていない」など、企業利用の要件に対応しきれない点がありました。

iOS 8 では、サードパーティ製の Web コンテンツフィルタリング機能を Safari で利用できるようになりました (図14)。本機能によって、管理者はユーザーの不適切なウェブサイト閲覧を効率的に防止できます。

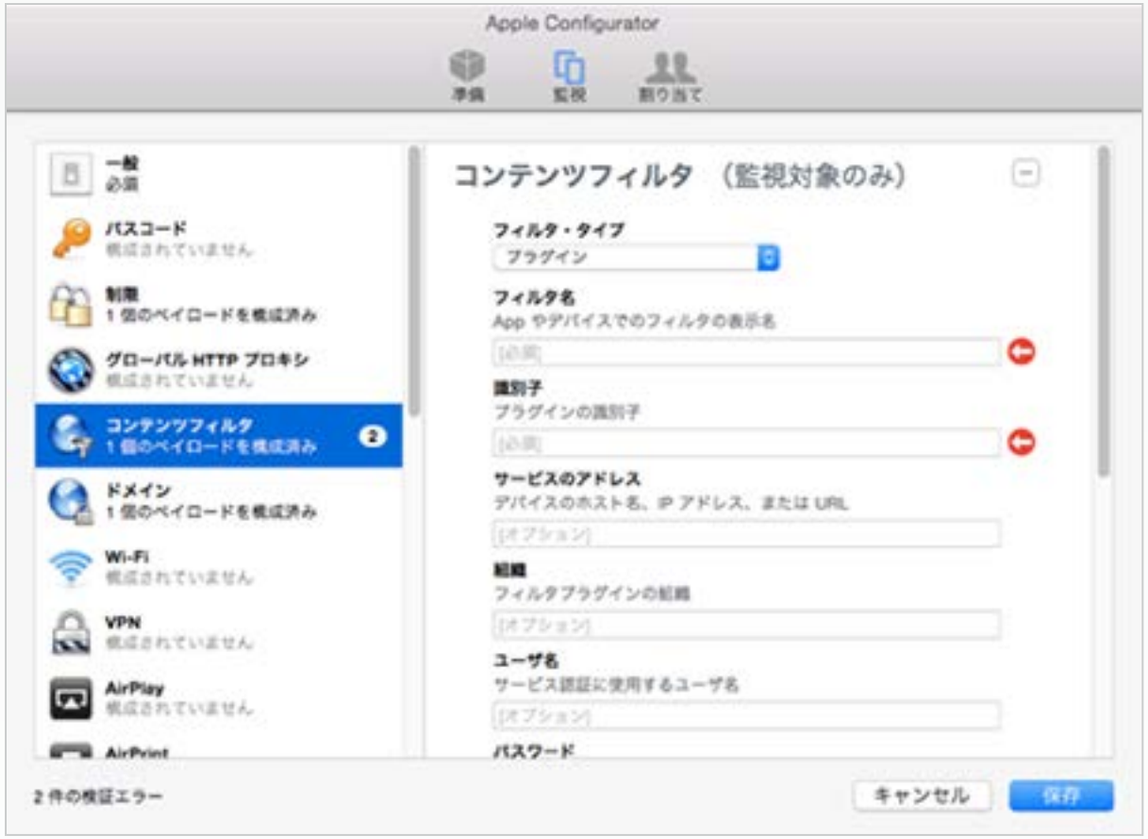


図14. Web コンテンツフィルタリング機能を設定する
Apple Configurator の利用画面イメージ

効果的な利用シーン

・従業員が業務に不必要なウェブサイトを閲覧してしまう。
・学生が授業に不必要なウェブサイトを閲覧してしまう。
など、上記のようなケースに対処できるようになりました。

導入時の注意点

・サードパーティの製品が本プラグインに対応している必要があります。対応状況は事前に確認してください。
・プラグインで提供されるカテゴリフィルタリングの精度がニーズを満たすか、事前に確認してください。
・本機能を利用するには、Apple Configurator を利用して iOS デバイスを監視対象に設定する必要があります。

(4)「管理対象の Safari Web ドメイン」設定を追加

概 要

iOS 8 では、「管理対象の Safari Web ドメイン」を設定できるようになりました。この設定によって、「管理対象の Safari Web ドメイン」から Safari でダウンロードしたファイルについて、認めていないアプリへの連携を制限できるようになりました。本機能強化によって、管理者は業務データの漏えいを防止できます。

効果的な利用シーン

「社内イントラネットから Safari を通じてダウンロードしたファイルを、会社が認めていないファイルストレージサービスに、従業員が勝手に連携 / 保存してしまい、管理できない状態になった。」などのケースに対処できるようになりました。

導入時の注意点

- 会社が認めていないアプリへのファイル連携制限機能（Managed Open In 機能）を利用するには、Managed Apps 機能に対応した MDM サービスを利用する必要があります。
- 認めていないアプリへのファイル連携制限には、仕様的な制限があります。詳細は、 http://businessnetwork.jp/Detail/tabid/65/artid/3228/Default.aspx の Managed Open In 機能についてご覧ください。

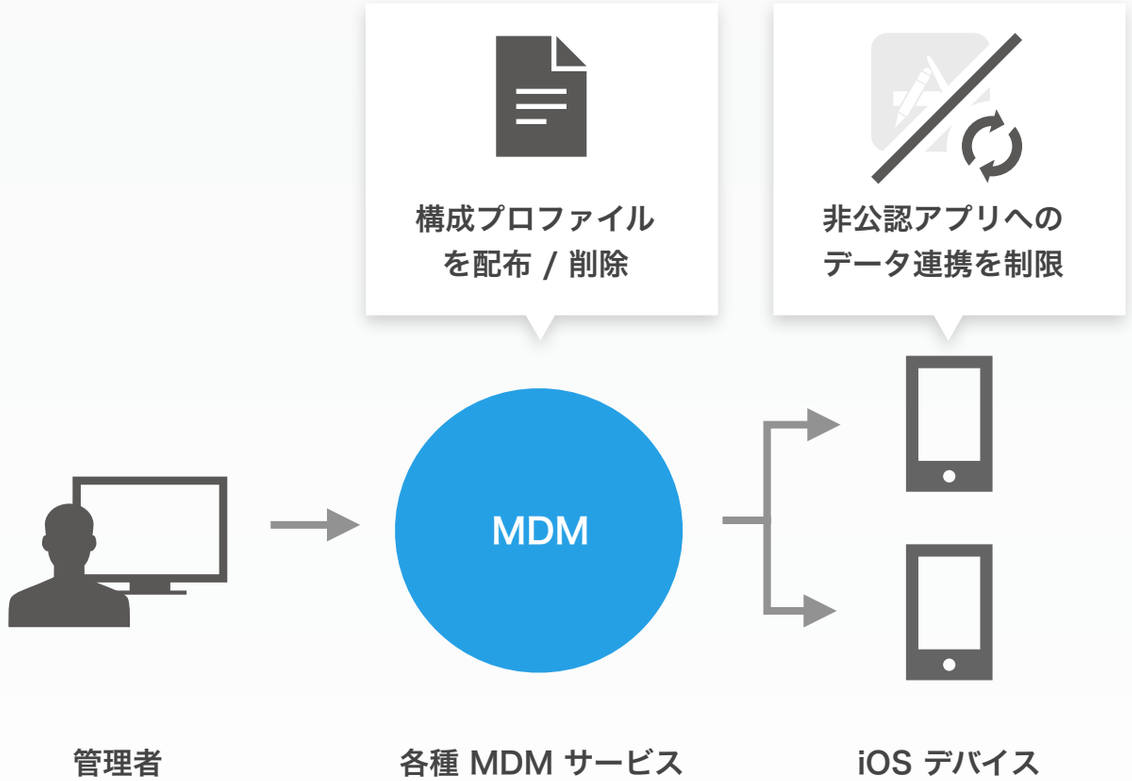


図15. MDM サービスを通じた「管理対象の Safari Web ドメイン」運用イメージ

(5)「マークされていないメールドメイン」設定を追加

概 要

新たに、「マークされていないメールドメイン」を設定できるようになりました。この設定によって、メール作成時に「マークされていないメールドメイン」に設定していないドメインが赤くハイライト表示されるようになります (図16)(図17)。これは例えば、「マークされていないメールドメイン」に所属する企業のドメインを設定すると、所属していない企業のドメインを赤くハイライト表示させる運用を行えます。

本機能強化を利用することで管理者は、メール運用における情報漏えいを抑止する効果が期待できます。また、管理者は MDM サービスと組み合わせて利用することで、本設定の遠隔配布 / 削除も可能となり、効率的なメール運用を行えます。

効果的な利用シーン

「同姓 / 同名の社外連絡先に、機密情報を記入したメールを誤って送信してしまった。」などのケースに以前よりも対処しやすくなりました。

導入時のヒント

・「マークされていないメールドメイン」は複数設定できるため、グループ会社内 / 外を区別する運用も行えます。

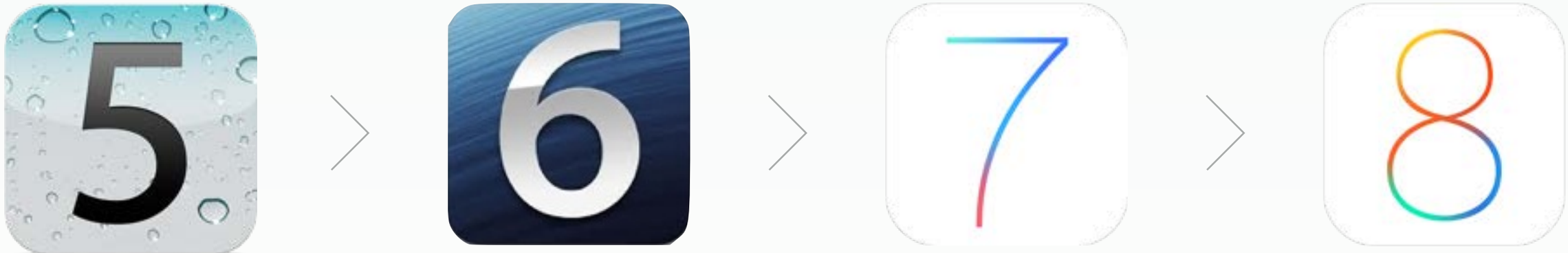
図16.「マークされていないメールドメイン」未設定（ iOS 8 ）

図17.「マークされていないメールドメイン」設定時（ iOS 8 ）

2. iOS 8 による最新の管理・運用スタイル

2. iOS 8 による最新の管理・運用スタイル

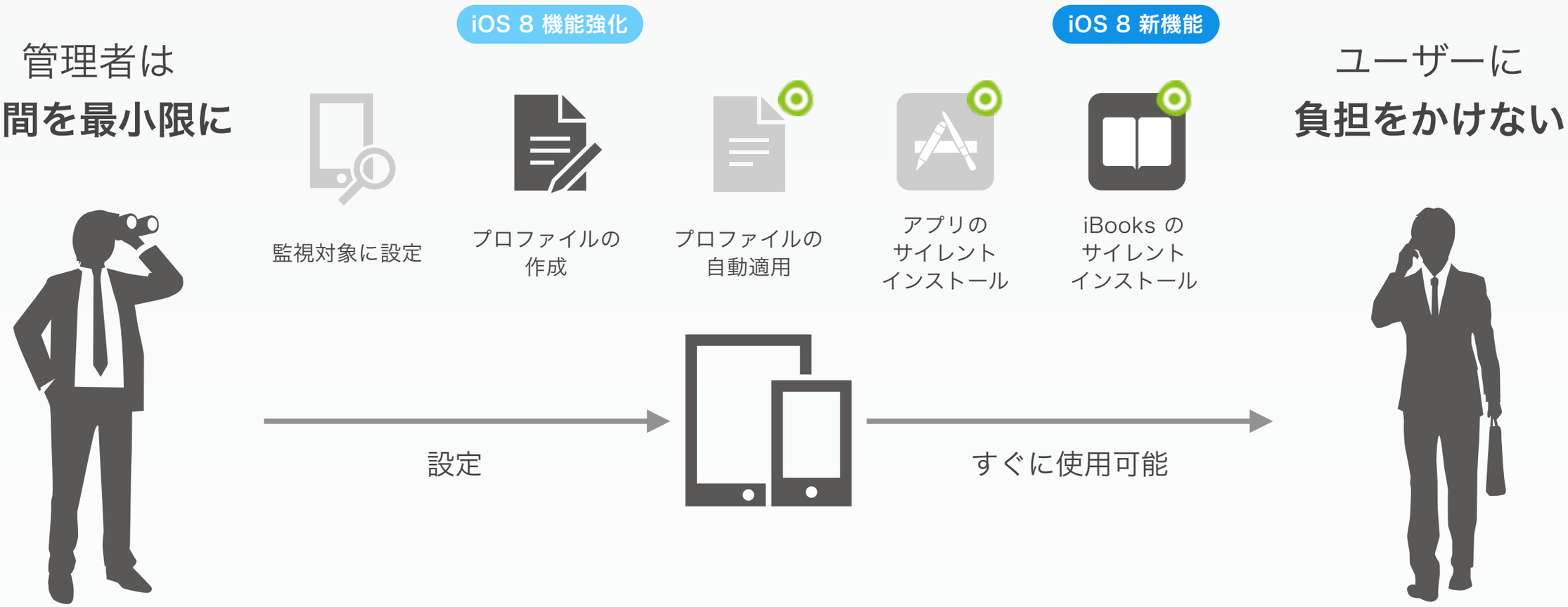
iOS は、Enterprise での利用を見据えて、大幅に進化を続けています (下図)。
次項からは iOS 8 の機能と弊社製品 CLOMO を利用することで実現できる、最新の管理・運用スタイルをご紹介します。



Apple Configurator	Managed Apps	Managed Open In	Managed Books
監視対象デバイス	Global Proxy	Per App VPN	Enterprise Books
	シングルアプリケーションモード	アプリケーション SSO	Handoff
		VPP 管理配布ライセンス	

※次項以降で紹介する機能の一部には、今後対応予定の機能が含まれます。詳細な対応状況については弊社までお問い合わせください。

2-1. 手間を最小限に抑えたデバイス導入



本マークの記載がある機能を利用するには、CLOMO の利用が必要です。

1. デバイス導入の準備

Apple Configurator で iOSデバイスを監視対象に設定します。プロファイルも同時に作成し、全社や部署などに応じて自動的に適用するプロファイルとして予め CLOMO MDM に設定します。

Apple Configurator　CLOMO MDM

2. デバイスを導入

CLOMO MDM の管理下に iOS デバイスを配置すると、「デバイス導入の準備」での設定内容に応じたプロファイルが自動で適用されます。

Apple Configurator　CLOMO MDM

3. アプリ、iBooksの配布

Volume Purchase Program を通じて一括購入したアプリや iBooks を CLOMO MDM を通じてサイレントインストールします。

CLOMO MDM /
CLOMO MOBILE APP PORTAL　Volume Purchase Program

2-2. 利用状況が見えるデバイス運用環境を構築

本マークの記載がある機能を利用するには、CLOMO の利用が必要です。

1. 利用状況を把握

デバイスの通信ログやインストールされているアプリの情報、アプリの起動・設定変更ログ、コンテンツの利用ログなどを、ユーザーに負担をかけずに自動的に収集します。

2. 設定、コンテンツの改善を検討

把握した利用状況から、成果を見出せた点や課題点を見つけ、より活用されると考えた方法を実現するように、デバイス設定やコンテンツなどを改善します。

3. 改善内容の反映

改善内容をユーザーのデバイスに遠隔配布/設定します。反映後には、「想定通りに活用が進んでいるか」「新たな課題は無いか」を定期的に確認し、改善を続けます。

CLOMO MDM

CLOMO SECURED APPs シリーズ

Apple Configurator

コンテンツ / アプリ制作用の各種ツール

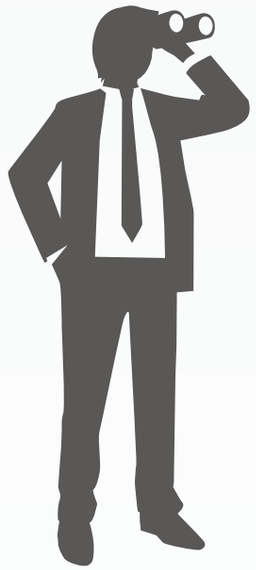
CLOMO MDM / CLOMO MOBILE APP PORTAL

Volume Purchase Program

CLOMO SECURED APPs シリーズ

2-3. 手間を最小限に抑えたデバイス再配置

管理者は
手間を最小限に



プロファイルの
自動適用

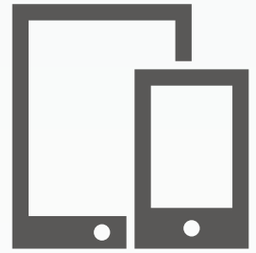
コンテンツの
自動適用

アプリの
回収 / 再配布

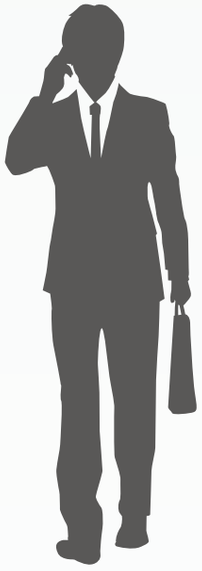
iOS 8 新機能

iBooks の
回収 / 再配布

ユーザーの
業務を止めない



組織に応じた
デバイス設定に
切り替わる



本マークの記載がある機能を利用するには、CLOMO の利用が必要です。

1. デバイス、コンテンツの変更

再配置するデバイスの所属部署を変更することで、予め組織に応じて設定したプロファイルやコンテンツが自動で適用される。

CLOMO MDM

CLOMO SECURED APPs
シリーズ

2. アプリ、iBooks ライセンスの回収 / 再配布

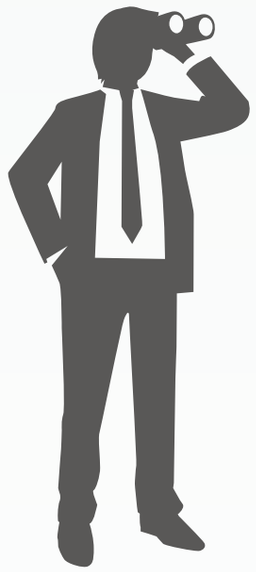
CLOMO MDM を通じて Volume Purchase Program で一括購入したアプリや iBooks のライセンスを回収し、必要なデバイスに再配布する。

CLOMO MDM /
CLOMO MOBILE APP PORTAL

Volume Purchase Program

2-4. 強力なインシデント対策を実現

管理者は
迅速に確実に対応



iOS 8 新機能

リモートロック /
ワイプ

電子証明書の遠隔失効で
サービスの接続を防止

電子証明書の遠隔失効で
アプリの起動を防止

Jailbreak検知

デバイスの利用状況検知

業務データ漏えいの
強力な対策を実現

本マークの記載がある機能を利用するには、CLOMO の利用が必要です。

1. デバイスの緊急事態を検知

ユーザーからの自主的な報告の他にも、「デバイスの通信が一定期間無い」「JailBreak を検知した」際に自動でアラートメールを配信します。その為、インシデント対策を必要とするシーンをすぐに把握できます。

CLOMO MDM

2. 緊急時対策を実施

デバイス、アプリのリモートロックを行っても反映されない場合には、各種アプリ・クラウドサービスの認証要素として設定した電子証明書を失効することで、業務データを閲覧できる環境へのログインを確実に防止します。

CLOMO MDM

CLOMO MDM
証明書連携オプション

CLOMO SECURED APPs
シリーズ

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「No.1 Enterprise Mobile Solution Company」を目指し、これからもスマートデバイスの導入・活用に取り組もうとする企業の課題を解決し、ビジネスの成功の一助となれるよう邁進してまいります。

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/

Innovation^3

※本資料「iOS 8 ビジネス向け機能強化ポイント解説」は、2014年10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。
そのため、内容に誤りの無いよう、出来る限りの注意を払いましたが、正確性・有用性等に関して、当社は一切の責任を負いませんので、あらかじめご了承ください。