モバイルデバイス管理の基本

101

iPadおよびiPhoneをビジネスでもっと活用しましょう

目次

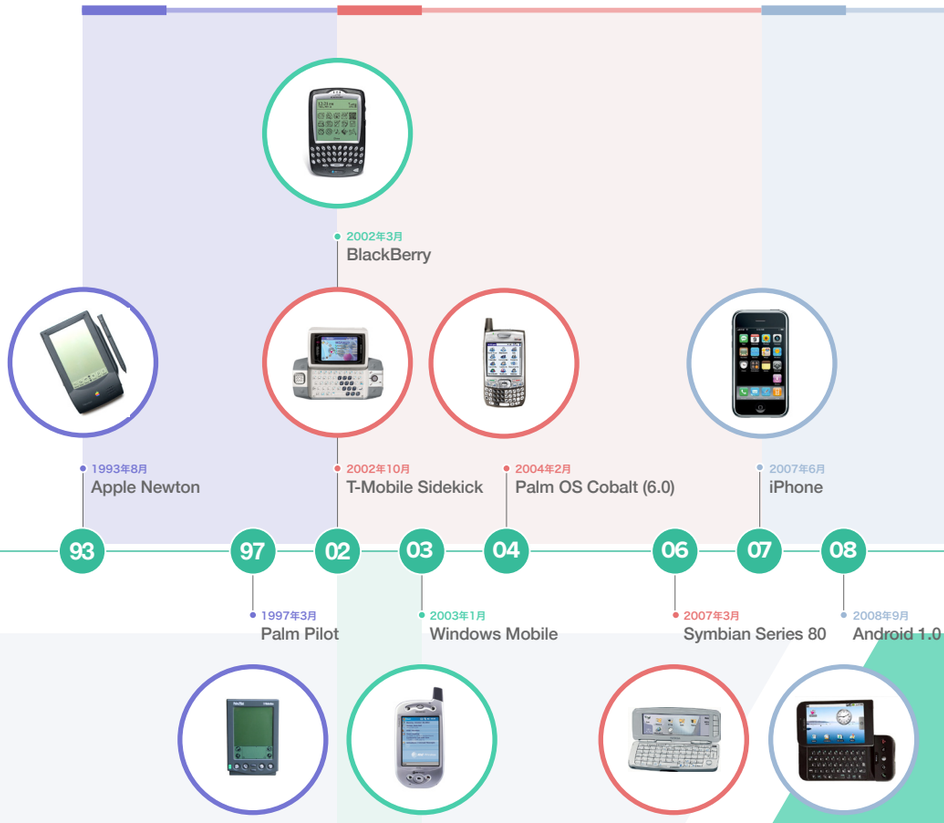
モビリティの概要

モビリティの進化

モビリティは、Apple Newton と Palm Pilot の手書き認識テクノロジーとダイヤルアップモデムへの接続機能を皮切りに1990年代に始まりました。

2000年代の中ごろには、スマートフォン市場に参入する企業が増え、Symbian は欧州で、Palm OS は米国で人気を博しました。市場では5つのモバイル オペレーティング システムの競争が激化していましたが、明確な勝者はいませんでした。

2007年には iPhone が発売され、続く2008年には最初の Android フォンが発売されました。iPhone の発売からほどなくして、Apple の App Store では開発者向けの iOS ネイティブアプリ構築機能が発売され、モバイルの生産性の向上とビジネスプロセスの改革を求めた全く新しい世界の幕開けとなりました。



初期のスマートフォンは、モバイル通信の扉を開いた BlackBerry と Windows Mobile が主流でした。

- iPhone
- Android
- Windows Phone

17

現在、モバイルランドスケープは3つの主要 OS プレーヤーで構成されています。スマートフォンは、モビリティとビジネスの変革のための通信媒体として提供されるアプリにより、単なる通信ツールを超えて発展を遂げています。

iOSを選ぶ理由

3つの一般的なモバイルオペレーティングシステムのうち、iOSは、消費者向けに設計されていながら、企業にも受け入れられている唯一のプラットフォームです。iOSは、直感的なユーザーインターフェイス、ビジネス対応アプリケーションの安全なエコシステム、ユーザーがこれまで以上に生産性を高められる、内蔵ツールを備えています。

最も高速で効率的なモバイルハードウェア

さまざまな画面サイズのiPhoneおよびiPadで実行する

ネイティブのハードウェアベースの暗号化を使用してデータのセキュリティを保つ

App Storeには1,500万件のアプリ、デベロッパーへの支払い額は400億ドル。デベロッ向けの健全なエコシステム

生体認証セキュリティ向けタッチID

ユーザーの70%以上が、1サイクルでリリースされる最新のOSを使用する

Microsoft Office for iOSなどの、ドキュメント制作、スプレッドシート、プレゼンテーションを行うための生産性向上アプリ

iPadで画面を分割してマルチタスクを実施する

VPNやシングルサインオンなど、最新の安全なワイヤレスネットワーキングに内蔵で対応

内蔵Microsoft Exchangeで、メール、カレンダー、連絡先をサポート。

iOSをビジネスで使う理由

Harris Poll*のレポートによると、企業のモビリティは、2016年のIT開発の上位にランクインする見込みです。この調査によると、IT意思決定者の90%以上は、企業モビリティが顧客関与、競争力、および2016年の業務 生産性にとって、重要な機能であると考えています。

企業は、単に従業員の補佐として、モバイルテクノロジーを選んではいません。ユーザーが好み、管理しやす く、安全であるため、企業がiOSを採用する割合が増えています。iPadとiPhoneを従業員に渡すことで、あら ゆる形態、あらゆる規模の組織が、よりすぐれたつながり、強化されたビジネス慣行、創造的で革新的な仕事の成果につながる道を切り開くことができます。

iOSを選んでいる企業の数

2017年度第1回 Jamf 企業内 Apple デバイス管理調査では(1)、企業の IT プロフェッショナルのほぼ全員が、各自の社内チームは職場における iPad と iPhone の使用が前年比で76%増加したと認識している、と答えています。加えて、93%が iPhone と iPad の他のプラットフォームへの導入が簡単になったと感じています。

76%

組織の76%が自社の環境で iPhone と iPad がの使用が増加したことを認識していました。

93%

回答者の93%が、iPhone または iPad の他のプラットフォームへの導入が簡単になったと答えています。

ソース 1-Jamf
https://resources.jamf.com/documents/books/managing-apple-devices-in-the-enterprise.pdf

iOSを活用してビジネスのプロセスを変える

アメリカの心理学者、Abraham Maslowが提示した理論によると、すべての人間は同じ、基本的なニーズを持っています。個人が愛や自尊心などのより高いレベルのニーズに進む動機を得る前に、基本的なニーズ（食糧、衣服、安心できる場所）を満たす必要があります。言い換えれば、特定のニーズが満たされた場合にのみ、一定の改善を達成することができるのです。

Maslowのニーズの階層で、iOSを使ったビジネスでできることを類推できます。デバイスの開発および通信 は、あらゆるビジネスにとって基本的なニーズです。しかし、iOSにはそれを超えるものがあります。業界の変革 の入り口なのです。iOSアプリは、ビジネスが生産性と顧客満足度を最大に高めるために、コミュニケーション を促進し、トランザクションを改善して、ビジネスプロセスを変革するためのメカニズムです。

プロセス

ビジネスで可能なものを超えるために、最も革新的な企業は、ハードウェアに投資するだけでなく、ビジネスプロセスを変革するカスタムアプリケーションにも投資しています。これは、IBMのMobileFirstプログム、B2B（Business-to-Business）アプリ、社内のエンタープライズ・アプリを通じて実施できます。

トランザクション

数百万ものアプリがある豊富なApp Storeエコシステムで、モバイルでのトランザクションをより効果的に行う機会を得られます。たとえば、クレジットカード取引を処理したり、取引を終了するための注文書を提出する、SquareやSalesforce1などがあります。App Storeアプリの導入は、iOSデバイスの可能性を最大限引き出すために欠かせません。

コミュニケーション

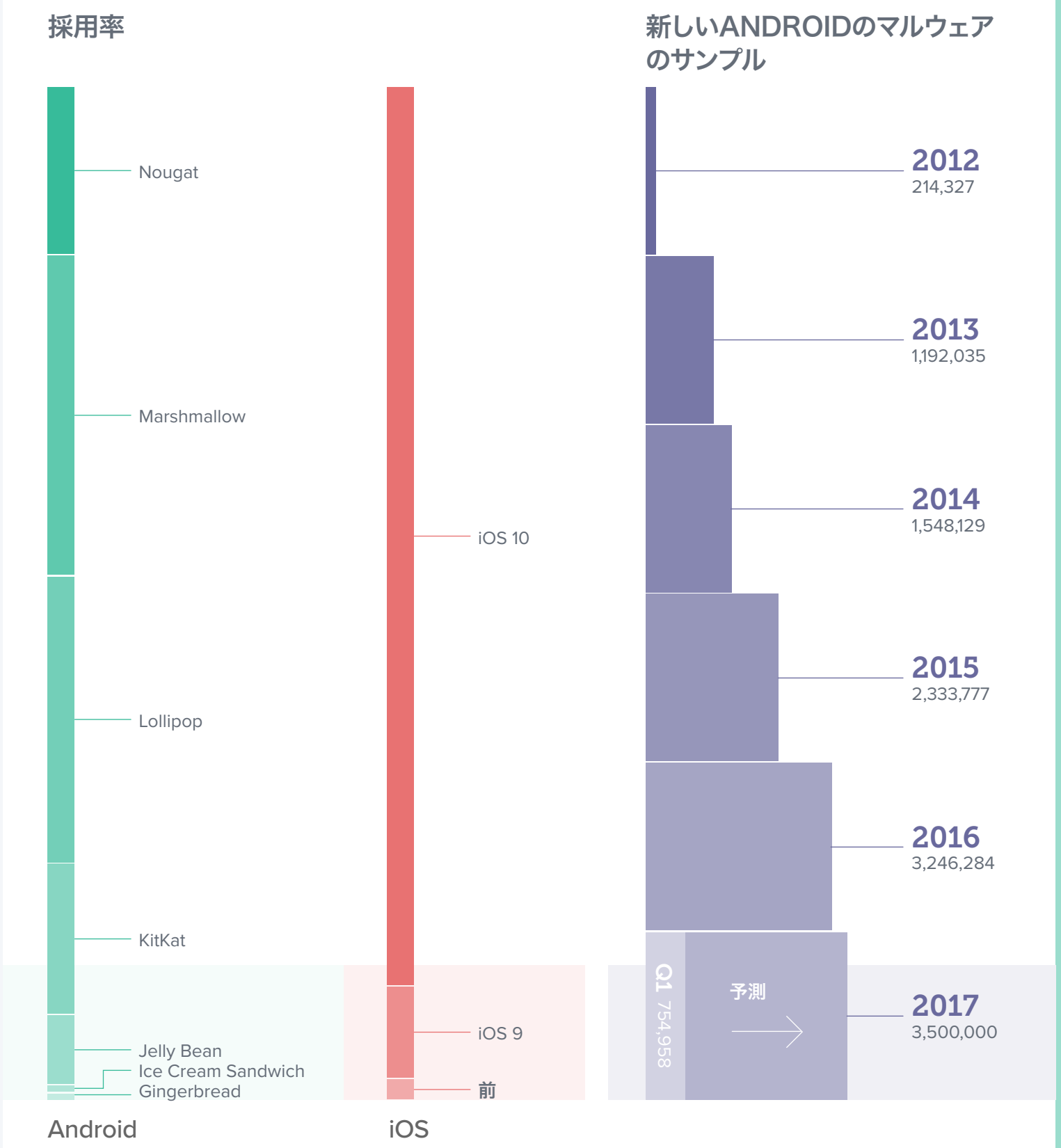
デバイスがユーザーの手に渡ると、IT部門はユーザーの基本的なコミュニケーションを可能にする必要があります。これには、企業の電子メール、Wi-Fi、およびVPN設定へのアクセスが含まれます。

導入

組織は、導入、デバイス構成、在庫に関する、ビジネスの問題に取り組む必要があります。これはピラミッドの最下位層であり、大量のiOSデバイスを見ている組織の基盤です。

Androidとの比較

GoogleのAndroidオペレーティングシステムは、フォームファクターの幅広さ、オペレーティングシステムのカスタマイズ性の高さ、デバイスの価格の低さで、その人気を高めてきました。ユーザーが重宝する機能はそれぞれ異なるため、Androidは、顧客にとって、またBYODプログラムにとって、良い選択肢となりえます。しかし、企業にとっては、フラグメンテーションおよびセキュリティの懸念から、Androidを標準化し、対応するのは困難です。



ソース 2 - Google: http://developer.android.com/about/dashboards/index.html
ソース 1 - Apple: https://developer.apple.com/support/app-store/

ソース 3 - G Data: https://public.gdatasoftware.com/Presse/Publikationen/Malware_Reports/G_DATA_MobileMWR_Q3_2015_EN.pdf

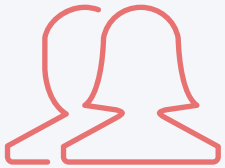
モバイルデバイス管理の概要

MDMとは

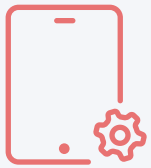
モバイルデバイス管理（MDM）は、iOSの管理のためのAppleのフレームワークです。iOSデ バイスを効果的に管理し、潜在能力を発揮させるためには、組織はデバイスと同等に、強力な MDMソリューションを必要とします。新しいデバイスの導入や在庫の収集、設定の設定、アプ リの管理、データの消去まで、MDMは大規模な導入に対応し、デバイスのセキュリティを確 保するための、完全なツールセットを提供します。

導入

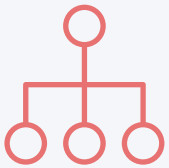
インベントリ



構成プロファイル



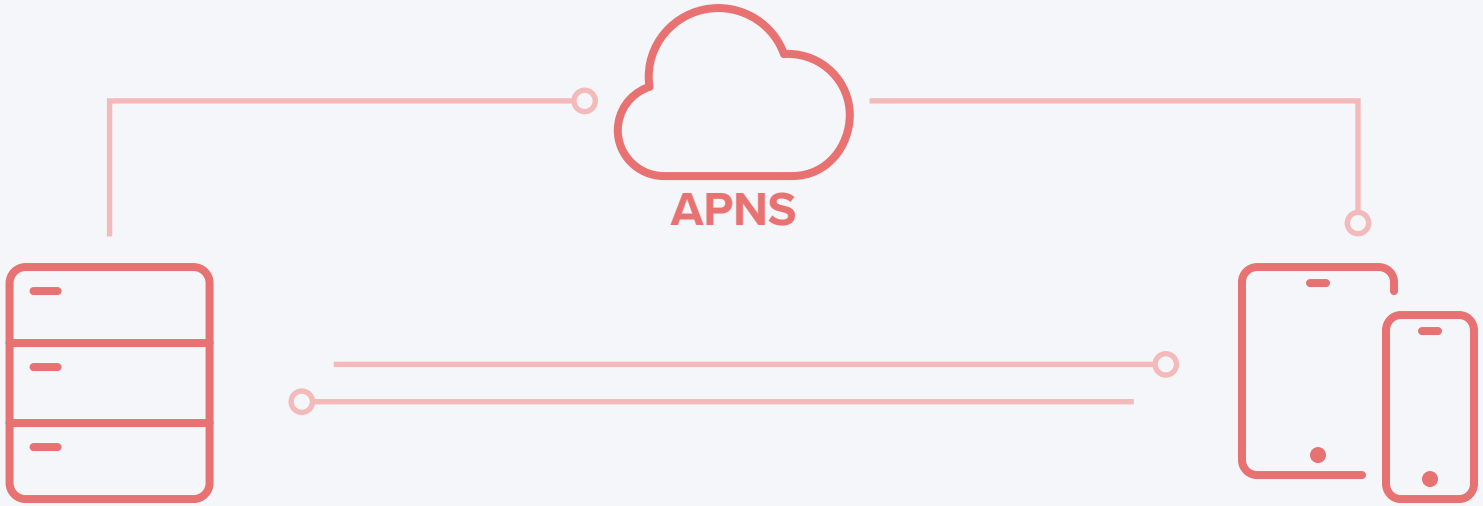
管理コマンド



アプリのデプロイ

セキュリティ

MDMのアーキテクチャ



Apple Push Notification Server

Appleデバイスにコマンドを送信すると、MDMサーバーはAppleのPush Notification Server（APNS）と 通信します。Appleのサーバーは、デバイスと常に接続されているため、接続する必要はありません。デバイス はMDMサーバーと通信し、送信したコマンド、構成プロファイル、アプリケーションを受信します。

導入

MDMを使用してiOSデバイスを管理するには、まずそのデバイスを登録する必要があります。iPadやiPhoneの場合、MDMツールを使用すると、管理者にデバイスを簡単に登録し、アプリとコンテンツを一貫して配布し、セキュリティとアクセスプロファイルを設定することができます。Apple Configuratorによる登録、URL、AppleのDevice EnrollmentProgram（DEP）など、いくつかの方法を使って、Appleのモバイルデバイスを登録できます。

導入

	説明	ユーザーエクスペリエンス	監督	最適
Device Enrollment Program (DEP)	無線での自動登録	ユーザーはパッケージ化されたされたボックスを受け取り、電源を入れると、デバイスは自動的に設定されます。	はい - ワイヤレスで	デバイスをエンドユーザーに送る
Apple Configurator	USBでデバイスに接続するMacアプリを使用した登録	該当なし – IT部門はこのプロセスを管理し、ユーザーにデバイスを手渡す	はい - 有線	共有モデルおよびカート
URLを使用してユーザーが開始	無線での手動登録	ユーザーが特定のURLにアクセスして、自動でデバイスを構成する	いいえ	デバイスは現在、登録が必要な現場にある

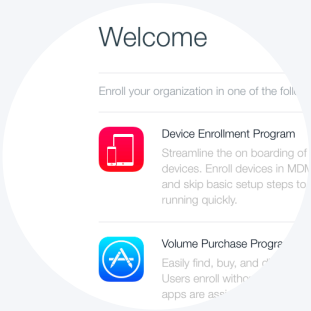
監督

監督は、MDMサーバーを使用したより詳細な管理を可能にする、iOSの特別なモードです。デバイスが監督されている場合にのみ、より多くの構成が使用できます。企業が所有するデバイスを、監督モードにすることを推奨します。

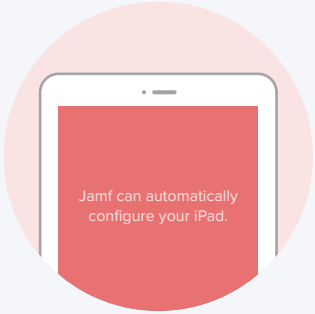
監督モードでのみ使用できるコマンドの例:

- カメラを無効にする
- App Storeを無効にする
- Safariを無効にするi
- 壁紙の変更を無効にする
- メールアカウントの追加を無効に する
- 他多数…

ベストプラクティス: タッチせずにDevice Enrollment Program (DEP)をデプロイ



1 Appleのウェブサイトで DEP に登録し、DEPポータルにご使用のMDMサーバーを追加します。



2 デバイスを購入し、DEPアカウントにリンクさせます。ユーザーにデバイスを直接発送します。

3 ユーザーが最初にiOSデバイスの電源を入れたとき、デバイスが自動的に登録されます。ユーザーが追加で操作をする必要はありません。

4 デバイスはMDMサーバーに登録されます。デバイスに適用する、任意の構成プロファイルとアプリを準備します。

5 デバイスは、対象となる構成とアプリを受信します。ユーザーはホーム画面にリダイレクトされます。これで、デバイスが管理され、構成されました。IT部門が触ることは一切ありません。

インベントリ

大量のインベントリデータを収集するため、MDMは、iOSデバイスにクエリを発行し、常に最新のデバイス情報を保持し、管理上の決定を情報に基づいて下すことができます。さまざまな間隔でデバイスからインベントリを収集でき、シリアル番号、iOSバージョン、インストールされているアプリなどを含めることができます。

MDMを使用したデータの収集

ハードウェアの詳細:
- デバイスタイプ
- デバイスモデル
- デバイス名
- シリアル番号
- UDID
- バッテリーレベル

ソフトウェア詳細:
- iOS のバージョン
- インストール済みアプリのリスト
- ストレージの容量
- 空き容量
- iTunes Storeのステータス

管理詳細:
- 管理ステータス
- 監督ステータス
- IPアドレス
- 登録方法
- セキュリティステータス

その他の詳細:
- インストール済みプロファイル
- インストール済み証明書
- アクティベーションロックステータス
- 購入情報
- 最近のインベントリアップデート

インベントリが重要な理由

測定できないものは、管理できません。MDMが収集するインベントリデータは、幅広いビジネスのニーズに使用し、次のような一般的な質問への回答に使用できます。自社のデバイスがすべて安全か？これまでいくつのアプリをデプロイしたか？デプロイしたiOSのバージョンはいくつか？

構成プロファイル:

プロファイルを使用することで、デバイスの動作方法をデバイスに伝えることができます。以前は手動でデバイスを設定する必要がありましたが、MDMテクノロジでは、パスコード設定、Wi-Fiパスワード、VPN設定などのプロセスを自動化することができます。プロファイルには、カメラ、Safari Webブラウザなどのiosのアイテムを制限する機能や、デバイスの名前を変更する機能もあります。

MDMに利用可能なプロファイルペイロード

基本

- Passcode
- Restrictions
- Wi-Fi
- VPN
- Home Screen Layout
- Single App Mode
- LDAP
- Web Clips

メールアカウント

- Mail
- Exchange ActiveSync
- Google Account
- VPN
- Calendar
- Contacts
- Subscribed Calendars
- macOS Server Account

メールアカウント

- Global HTTP Proxy
- Content Filter
- Domains
- Cellular
- Network Usage Rules
- Certificates

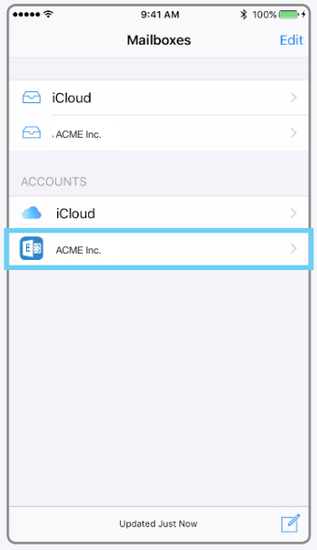
その他の設定

- AirPlay
- AirPlay Security
- Conference Room Display
- AirPrint
- Fonts
- SCEP
- Lock Screen Message
- Notifications
- Single Sign-on
- Access Point Name

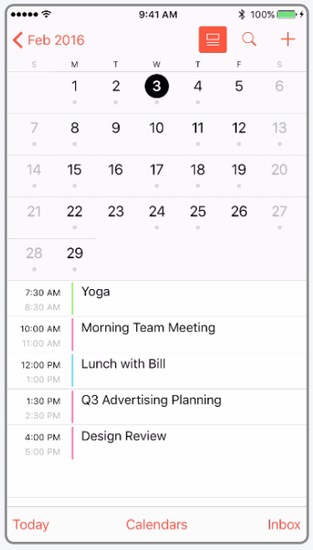
ベストプラクティス：iOS管理用のコンテナを削除する

MDMではコンテナは、電子メール、カレンダー、連絡先、Webブラウジングなど、企業情報の安全な場所として機能するように設計された、追加のアプリケーションを指します。組織はこのコンセプトに基づいていますが、優れたユーザーエクスペリエンスを得る過程で得られます。コンテナは、Androidのセキュリティ上の欠陥を克服するため、一部のMDMソリューションで人気を得るようになりました。

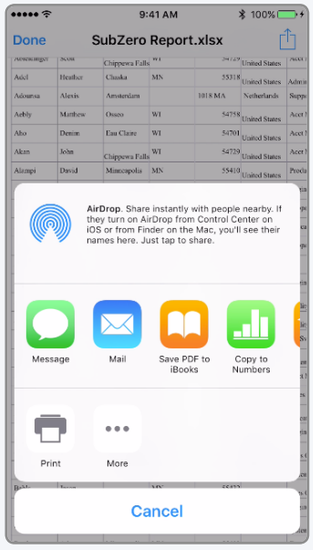
実際、iOSのネイティブアプリ（メール、カレンダー、連絡先、Safari）はすでに安全です。メール コンテナを「安全」にする必要はありません。ユーザーにとって最高のエクスペリエンスを維持 するには、構成プロファイルを使用します。プロファイルにはiOSにExchangeアカウントを追 加する機能があり、そのため、企業アカウントのメールとカレンダーにアクセスできます。



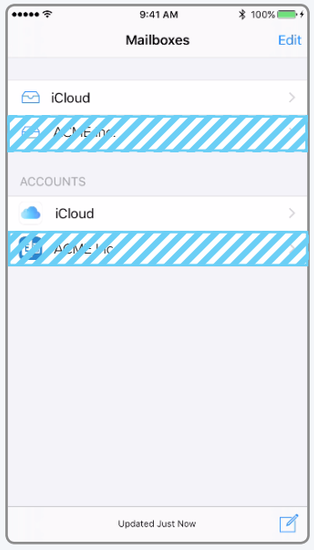
構成プロファイルでは、ネイティブメールアプリの、ユーザーの個人用電子メールアカウントの横にExchangeアカウントが追加されます。



現在、企業のデータは、ネイティブアプリの個人データのすぐそばに存在し、ユーザーエクスペリエンスとセキュリティを維持しています。



IT部門は、企業の電子メールアカウン トの添付ファイルを開けないようにすることで、データの流出を制御することもできます。



最後に、従業員が組織を離れる場合、IT部門は構成プロファイルを削除するだけで、企業の電子メールアカウントとデータを一緒に削除できます。個人アカウントは削除されません。

ベストプラクティス：iPad の標準化

組織所有のデバイスで一貫した体験を提供することで、従業員の生産性の向上に貢献します。Apple デバイスを職場向けに標準化することで、ユーザーがいつでもどこでも必要なアプリにすばやくアクセスできる高効率のセットアッププロセスを構築します。アプリの検索時間を短縮し、ユーザーの生産性を向上させます。

組織内で iPad と iPhone デバイスを標準化する方法を3つご紹介します。

ホーム画面の壁紙の設定

所属組織のロゴを壁紙に表示することでブランドの調和を生み出します。

ホーム画面のレイアウトの事前設計

ホーム画面で、ウェブクリップとともに、アプリとフォルダーの配置を決めておきます。最初のページに必須アプリを配置し、あまり重要ではないアプリは他のページに配置します。

アプリの表示/非表示

従業員が必要とするアプリのみを表示します。業務に不必要なアプリは非表示にします。

管理コマンド

管理コマンドは、企業データのセキュリティを確保するために個々のデバイスに適用できる特定のアクションです。MDM内でこの機能を利用すると、デバイスをロックしたり、完全に消去することで、紛失や盗難にあったデバイスに対処できます。追加のコマンドを使用すると、プッシュ通知を送信したり、iOSを最新バージョンにアップデートしたり、デバイス名を変更したりして、IT部門のデバイス管理を容易にすることができます。

MDMに利用可能なコマンド


インターネット設定


インターネット設定


パスコードの消去


制限の消去


デバイスの管理解除


デバイスの一掃


ブランクのプッシュを送信


壁紙の設定


通知の送信


IOSのアップデート


名前の変更


デバイスのシャットダウン


デバイスの再起動

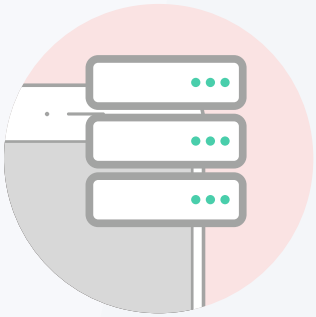

ロストモード&サウンド

ベストプラクティス：MDMを使用してアクティベーションロックを管理する

アクティベーションロックはiPhoneやiPadの盗難を防止する目的で設計されました。所有者のApple IDとパスワードを要求するだけでは、誰でもデバイスを有効にすることはできません。この機能は消費者にとっては優れていますが、デバイスをユーザーに再割り当てする必要があるIT管理者にとっては、問題が発生する可能性があります。MDMソリューションがなければ、アクティベーションロックは管理しなければならない悪夢であり、多くの組織は、ユーザーがApple IDを完全に使用することを禁止するしかなくなります。

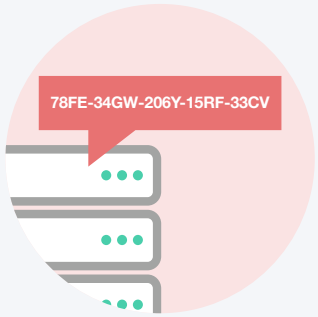
デバイスがMDMサーバーに登録され、監督されている場合に限り、以前のユーザーのApple IDにロックされているデバイスを受け取ったら、アクティベーションロックバイパスコードを生成できます。コードを取得したら、Setup Assistantのパスワードフィールドにコードを入力して、デバイスのロックを解除できます。

1



デバイスはすでにMDMサーバーに登録されており、監視されています。アクティベーションロックバイパスコードが生成され、MDMサーバーに格納されます。

2



ロックされたデバイスはIT部門に返され、MDMサーバーに保存されているバイパスコードが取得されます。

3

IT部門はデバイスをSetupAssistantに再起動します。
最初の画面で前のユーザーのApple IDとパスワードが尋ねられます。アクティベーションロックを避けるするには、IT部門はパスワードフィールドにコードを入力し、Apple IDフィールドを空白のままにします。これで、デバイスのロックが解除されました。

アプリのデプロイ

iOSデバイスはすぐに使える優れたコミュニケーションツールとして機能しますが、iOS AppStoreのパーソナルアプリやビジネスアプリの豊富なライブラリは、ユーザーの生産性を向上させ、従業員のさらなる達成に役立ちます。さらに、iOS App Storeアプリケーションを使用してiPadをキャッシュレジスタに変えたり、外出先で経費レポートを作成して提出したり、営業サイクルの管理や契約書の署名などのビジネスプロセスを変えることさえできます。アプリのデプロイを管理するアプリ戦略とMDMを使用すると、必要なアプリを自社の環境に合わせて設定し、安全に保つことができます。

アプリ管理戦略

マネージドアプリとは

立てられているため、標準アプリとは異なります。具体的には、マネージドアプリはMDMテクノロジーを使用して配布され、アプリのデータのバックアップを防止するように設定し、MDMプロファイルを削除すると削除されます。

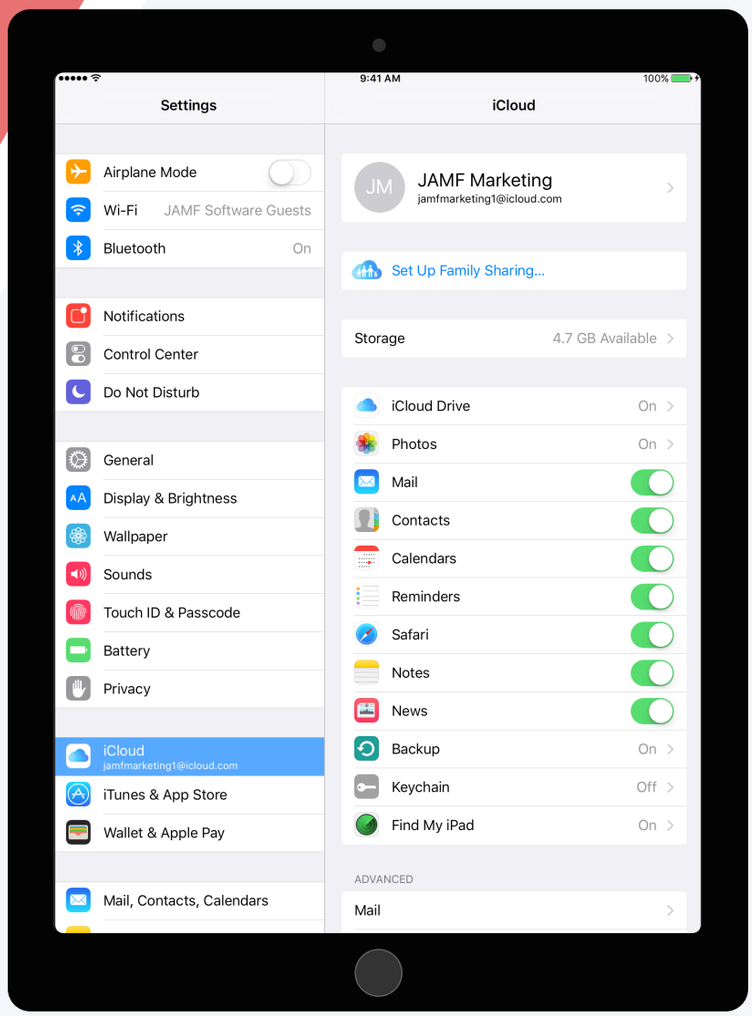
マネージドオープンイン

マネージドオープンインは、あるアプリから別のアプリへのデータの流れを制御することによって、マネージドアプリの概念をさらに進化させます。組織は、iOS共有シートに表示され、ドキュメントを開くアプリを制限できます。たとえば、会社の電子メールアカウント送信されたメールの添付ファイルは、Boxアプリでのみ開くことができ、個人のDropboxアカウントでは開くことができないというルールを定義できます。これにより、コンテナの必要なく、真のネイティブデータ管理が可能になります。

アプリ構成

アプリのデプロイでは不十分で、設定の一部をあらかじめカスタマイズする必要がある場合があります。これはApp Configurationsの前提です。アプリの開発者は、MDMサーバーによってアプリに事前設定できる設定を定義できます。たとえば、サーバーURLがあらかじめ入力された状態でBoxアプリをデプロイすると、ユーザーはアプリケーションを起動して実行するためにユーザー名とパスワードを入力するだけで済みます。

ベストプラクティス：ユーザー用個人Apple ID



個々の個人用Apple IDを使用することで、iOSの導入を促進し、ユーザーがビジネス上の問題に対するユニークなソリューションを見つけるよう促します。

Apple IDとは

Apple IDは、ユーザーがAppStore、iTunes、iCloud、iMessage、FaceTimeなどのAppleサービスにアクセスするための個人アカウントです。Apple IDは、電子メールアドレスとパスワード、連絡先、支払い、セキュリティの詳細で構成されています。

Apple IDがユーザーにとって重要である理由

Apple IDにより、ユーザーはiOSとApp Storeを最大限に活用できます。たとえば、ユーザーがApple IDを持つことを許可することで、ユーザーはFaceTimeやiMessageなどのAppleが提供する無料の通信サービスにアクセスできるほか、Find My iPhoneやiCloudなどの他のサービスも利用できるようになります。

企業所有のアプリについて

VPPストアでは、「Managed Distribution」方法により、アプリにライセンス付与できるようになったため、所有権を恒久的にユーザーに移動することなく、単純にアプリをユーザーのデバイスまたはApple IDに割り当てることができます。このようにして、IT部門はデバイスに特有のApple IDを作成するために何時間も費やさなくてよくなります。

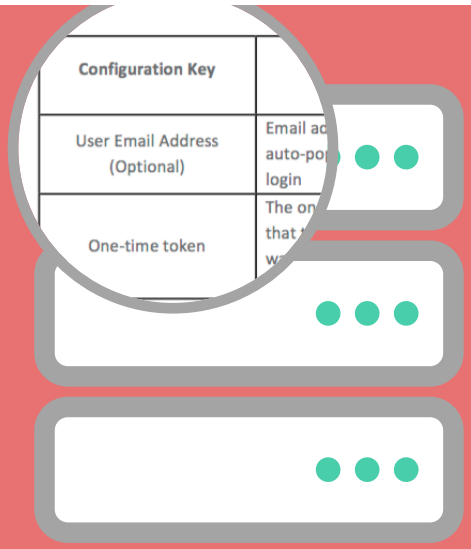
セキュリティリスクについて

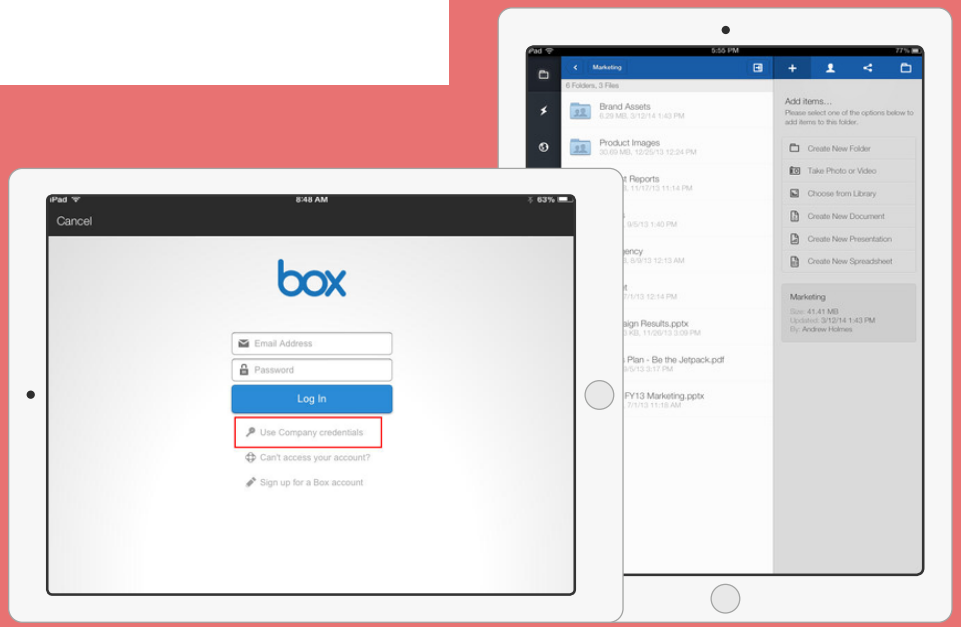
マネージドオープンインなどのMDM機能や設定プロファイル内の制限を利用することで、IT部門はApple IDを完全に禁止せずに、セキュリティリスクをより緩和することができます。Appleのサービスは堅牢なセキュリティで知られており、企業のデバイスに個人用のApple IDを追加しても、全体的なセキュリティは低下しません。場合によっては、Apple IDが2段階認証をサポートしているため、セキュリティを強化することもできます。

ベストプラクティス：マネージドアプリ構成の導入事例

iPhoneおよびiPad用のBoxは、外出先での仕事に役立ちます。すばやく安全で、使いやすいため、どこからでも生産性を高めることができるため、2500万人以上のユーザーと225,000社がBoxを使用しています。

VPPを使用してBoxを展開し、オプションを事前に設定して、確実にユーザー間で採用されるようにします。

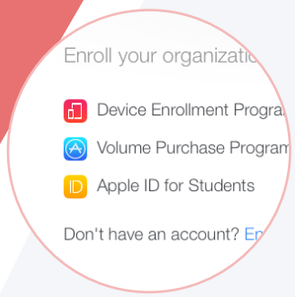




VPPを使用してBoxを展開し、オプションを事前に設定して、確実にユーザー間で採用されるようにします。

MDMサーバー経由でアプリが配備されると、設定キーが実行されます。たとえば、URLをあらかじめ設定しておくと、Boxの初回起動時に、ユーザーは自動的に会社のログイン画面にリダイレクトされ、デフォルトでは表示される、個人アカウントログイン画面は表示されません。

ベストプラクティス：Volume Purchase Program（VPP）を伴うアプリのデプロイ



1

AppleのウェブサイトでVPPに登録し、MDMサーバーにご使用のVPPアカウントをリンクさせます。

3

無料アプリを含め、MDMサーバーにアプリライセンスを追加します。

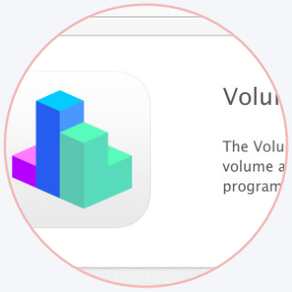
4

アプリが直接デバイスにデプロイされます。介入やApple IDは必要ありません。

?

アプリを、デバイスに直接割り当てるか、ユーザーのApple IDに割り当てるかを選択します

2



Appleのウェブサイトで VPPに登録し、MDMサーバーにご使用のVPPアカウントをリンクさせます。

4

電子メールまたはプッシュ通知を使用して、VPPデプロイに参加するようにユーザーを招待する.

5

アプリはユーザーのApple IDにリンクされており、App Storeの[購入済み]タブにあります。

セキュリティ

セキュリティとプライバシーに関する懸念は、組織にとって深刻な問題です。iOSには、モバイルオペレーティングシステムに組み込まれた多数のセキュリティ機能があります。MDMと組み合わせることで、デバイスが安全であるだけでなく、アプリやネットワークも確実に保護されます。

ネイティブのAppleセキュリティ機能

Pre-App VPN

Virtual Private Networks（VPN）は、インターネット上のトラフィックを暗号化するための手段として、長い間企業内で使用されてきました。従来のデスクトップは、VPN経由ですべてのトラフィックをルーティングすることで動作します。しかし、このモデルはモバイルでは故障する可能性があります。Appleは、組織やアプリケーション開発者がアプリケーションレベルでVPN経由でルーティングされるデータを定義できるようにすることで、この問題を解決しました。こうすることで、帯域幅を節約し、ネットワークの速度が上がります。

Touch ID

Appleの新しいiOSデバイスのほとんどに指紋センサーが搭載され、オペレーティングシステムに生体認証セキュリティが追加されました。Toutch IDを使用して、デバイスのロックを解除して特定のアプリにサインインできます。指紋データはデバイスにローカルに保存され、Appleと共有されることはありません。

暗号化:

iOSには256ビットの暗号化機能が内蔵されており、パスコードが有効な場合は、暗号化も自動的に有効になります。これは、オペレーティングシステムにソフトウェアを追加しなくても、デバイス上のデータが安全であることを意味します。Appleはハードウェアとソフトウェアの両方を作っているため、暗号化は非常に速く、ユーザーは気づかないほどです。

ベストプラクティス：MDM ソリューションを用いたロス予防

監視しているデバイスを MDM を使用してマネージドロストモードにする機能は、iOS 9.3以降で利用できる重要なセキュリティ強化策です。この設定によりデバイスがある場所が分かるため、デバイスの紛失時や盗難時にデバイスを見つけるのに役立ちます。さらに、ロストモードが無効になっている時に限られますが、ユーザーがデバイスのロックを解除できます。ユーザーはロックを解除すると、アクセスした位置情報を共有できます。

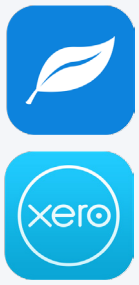
マネージドロストモードの操作は管理者が行います。デバイスが操作性を取り戻す前に管理者がこのモードを無効にする必要があります。Find My iPhone と同様に、管理者はマネージドロストモードになっているデバイスにメッセージを送信できます。

カスタムアプリ

小売業者は、これまで以上に、技術を通して顧客とつながり、購買摩擦を軽減するために力を入れています。小売業者は、販売時点管理（POS）システム、ロイヤルティプログラム、従業員スケジュール、会計などを考慮する必要があります。iPadやiPhoneは、強力なアプリと組み合わせることで、あらゆる小売業者がこれらの問題を迅速かつ手頃な価格で容易に解決することを可能にしました。しかし、App Storeには数千もの小売アプリがあるため、適切なソリューションを見つけるのが難しいかもしれません。以下は、小売業者に採用を検討してもらいたい、選りすぐりの小売アプリです。

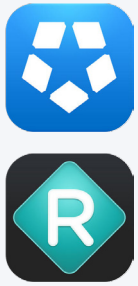
販売時点管理（POS）

POSシステムは、大きくて、場所を取り、ユーザーが使いにくく、持ち運びもできませんでした。iPadおよびiPhoneは、従来のPOSコンピュータと同じくらい強力で、ビジネスを改革すると同時に、持ち運ぶことができます。Square、Vend、Revelといったアプリは、キャッシュドロワー、クレジットカードリーダー、スキャナーなどのハードウェアに接続できる、カスタマイズ可能なPOSアプリです。SquareはApple Payにも対応しています。これは、iPhoneユーザーがレジで支払うときに使用する、最も簡単な方法です。



会計

会計には時間がかかるかもしれませんが、FreshBooksやXeroといった素晴らしいアプリを利用して、少なくとも外出時でも行えるようになりました。これらのソリューションはいずれも、モバイルアプリからアクセスできる、クラウドベースの会計システムをそなえています。これらのシステムは、経費の追跡と収入の合理化に役立つよう設計されています。



時間追跡

スケジュール、タイムカード、従業員コミュニケーションの管理は、一連の作業であり、多くの場合紙とペンで行われます。DeputyとRepliconを使用すると、手動システムをクラウドに移行して、モバイルデバイスを介してそれらと向き合うことができます。これらのソリューションは両方とも、スケジューリング、時間追跡、従業員コミュニケーションのためのプラットフォームを提供します。

リワードプログラム

ロイヤルティプログラムは、顧客に戻ってきてもらうための素晴らしい方法です。しかし、独自のシステムを導入するのはとても難しいものです。この管理をBellyがお手伝いいたします。Bellyは12,000社以上の企業と600万人の顧客と連携している、ロイヤルティリワードプログラムです。このプログラムに登録するだけで、顧客とのロイヤリティを構築できます。

ヘルスケア用iOS

ヘルスケアプロバイダは、医師と看護師のコミュニケーションを改善すると同時に、より迅速でパーソナライズされたケアを患者に提供する新しい方法を模索しています。これを実現するため、医者と看護師がモバイルデバイスから情報にアクセスできる安全な中央ロケーションに、医療記録を格納します。家庭の健康状態を監視するためのサードパーティのアプリケーションとハードウェアが追加されたことにより、Appleと以下の組織は真に医療を変えています。

コミュニケーション

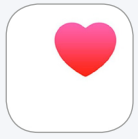
コミュニケーションは、患者の医療を適時提供するための必須コンポーネントであり、iOSは豊富で魅力的なコミュニケーションアプリのプラットフォームを提供します。Voalte、Vocera、Praxifyは、医療機関がAppleの技術を活用しながらコミュニケーションするための強力なツールを提供する、3大企業です。

臨床ケア

現代の電子カルテ（EMR）システムは、自宅にいるか、病院にいるか、外出しているかにかかわらず、また、医療従事者がどこにいても、医療従事者がアクセスできるように設計されるべきです。EmisとEpicはどちらも、iOS用に設計されたEMRソリューションです。両者のモバイルアプリを使用することで、医師や看護師が自分のiPhone、iPad、さらにはApple Watchから、患者の最新情報を得ることができます。

患者ケア

これまでは、臨床ケアのみでした。慢性的な健康状態については、しばしば家庭で観察することが推奨されます。iPadやiPhoneを、サードパーティのハードウェアと組合わせることで、市販レベルの製品を使用して、健康状態を観察することができます。Focus Cura、Physitrack、Withingsは、ユーザーが個人のモバイルデバイスで健康状態を追跡できるようにした、リーディング企業です。

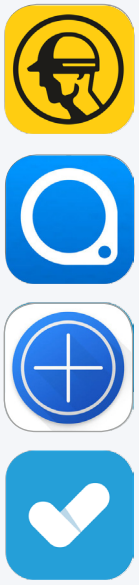


Appleと健康

Appleは、強力な健康の観察と追跡ツールをiPhoneやApple Watchに組み込み、ユーザーに提供しました。ヘルスアプリを使用すると、1つのアプリで自分の健康状態を追跡できます。自分の健康データが安全であるという確信を持っています。

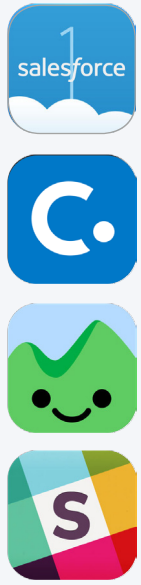
現場サービス用iOS

現場に従業員を配置している組織は、従業員が必要なときにいつでもどこでも、適切なツールや情報にアクセスできるようにする必要があります。外出先の従業員を支援するため、現場チームに力を与えるためのアプリ戦略を作成することは、成功と生産性を追求する上で非常に重要です。以下に、リソースがiOSとペア設定されている場合の一般的な現場営業だけでなく、建設業界で可能になることをいくつか例でご紹介します。



建設

iOSは、青写真プランとCADプラiPadsに搭載した製品により、建設業界道具箱のなかでも重要なツールとす。Fieldwire、PlanGrid、FinalCADのアプリはすべて、建設チームが使用し青写真ファイルにアクセスできます。そのため、大きな印刷物を持ち歩く必要がありません。SafetyCultureとiAuditorアプリで、監査を簡単に行うこともできます。



現場営業

顧客関係管理、プロジェクト管理、チーム管理、費用追跡は、ほとんどすべての営業組織が日常的に従事する、重要なビジネス機能です。Salesforce1、Concur、Basecamp、Slackなどの組織のソリューションを提供して、モバイルアクセスとモバイルエクスペリエンスを最優先事項として、これらの現場作業をサポートすることができます。

カスタムアプリでビジネスのプロセスを変える

iOSを導入している組織であれば、メール、ノート、カレンダーなどの、基本的なコミュニケーションのための内蔵アプリを利用できます。しかし、iOSにはそれを超えるものがあります。カスタムアプリ用の強力なプラットフォームにアクセスすることで、ビジネスプロセスや業界全体を変革する可能性を持つことができます。

たとえば、AppleはIBMと協力して業種別のアプリを作成し、効率性と生産性を、別次元にまで高められるようにしました。AppleとIBMはこれまでに、金融、ハイテク、政府、医療、保険、小売、輸送など、業界特有の機能に特化した、100以上のアプリを開発してきました。

App Storeには150万以上のアプリがあるため、あなたのビジネスに必要なものの90%を実行するアプリを見つけられるかもしれません。これこそが、B2B App Storeが役立つところです。Appleは組織と開発者とを結びつけて、カスタマイズされたバージョンのアプリを提供するサポートをします。企業は簡単なブランディングを行うことも、既存のアプリをビジネスプロセスのニーズに合わせて調整することもできます。

最も革新的な企業は、ハードウェアだけでなくソフトウェアも開発しています。社内のアプリを開発するために開発者リソースに投資することは、モバイルプラットフォームで何が可能かを、企業が再考する役にも立ちます。Appleは、優れたモバイル開発プラットフォームのひとつである、Swiftを提供しています。Swiftは、Appleのすべてのオペレーティングシステムにとって、強力で直感的なプログラミング言語です。Swiftもオープンソースであるため、Appleコミュニティで無料のリソースを見つけて、すぐにビルドを開始できます。

ビジネスの変革

Apple TV によるエンタープライズの推進

職場内でモバイルの需要が高まるにつれて、自分の技術の高さを維持することが必要になります。IT 担当者が Managed Apple TV を使用すれば、最新の tvOS により、家庭用の Apple TV デバイスをマネージドの処理ツールに変身させることができます。

ワイヤレスの会議室

最新式の会議室を作るには、アダプターワイヤレスディスプレイを設置します。次にカンファレンスディスプレイモードを有効にして、各会議室固有の追加指示や情報を含めてカスタマイズした歓迎メッセージを作成します。

デジタル署名

Apple TV を使うと、デジタル署名の入手、アクセス、拡張、管理がさらに簡単になります。さらに MDM ソフトウェアを使えば、企業が、1箇所または複数の拠点で同時に表示する内容を簡単に操作できます。

自発的なコレボレーション

Managed Apple TV と　Airplay を使えば、今までよりもはるかに簡単に、デバイスの画面を共有画面にすぐに表示できます。これにより、職場内の協力体制に最適な設定を構築できます。

jamf | PRO

iOS用MDM

Jamf Proは、iOS向けのAppleモバイルデバイス管理ツールとして、世界をリードしています。Jamf Proは、日々のサポートニーズに対処するツールをユーザに提供するように設計されているため、時間と費用を節約しながら戦略的なタスクに専念することができます。

導入　インベントリ　構成プロファイル　管理コマンド　アプリのデプロイ　セキュリティ　Self Service　Apple School Manager　Classroom Management

無料トライアルで、iOSの管理を始める

付属のチェックリスト：

プロファイルペイロードと管理コマンドリスト

Managed のみ

パスコードのペイロード
- 簡易値を使用できる
- 英数字値が必須
- パスコードが最短(0〜16)
- 複合文字数が最少(0〜4)
- パスコード寿命が最長(0〜730日間)
- 自動ロック時間が最長
- パスコード履歴(0〜50件)
- デバイスロックの猶予期間が最長
- 失敗試行回数が最多

制限のペイロード
- カメラの使用が可能
- スクリーンショットと画面記録が可能
- デバイスのロック時でも音声ダイヤルが可能
- Siri を使用できる
- デバイスのロック時でも Siri を使用できる
- Apple Configulrator と iTunes を使用したアプリのインストールが可能
- アプリ内購入が可能
- 全購入に iTunes Store パスコードが必須
- iCloud バックアップを使用できる
- iCloud キーチェーンを使用できる
- マネージドアプリを使って iCloud にデータを保存できる
- エンタープライズ書籍のバックアップが可能
- エンタープライズ書籍でノートとハイライトの同期が可能
- iCould フォトシェアリングを使用できる
- iCloud フォトライブラリを使用できる
- マイフォトストリームを使用できる
- ローミング中に自動同期が可能
- バックアップを強制暗号化
- 広告トラッキングを強制制限
- ユーザーが信頼性のない TLS 認証を承認できる
- 自動更新により信頼性のある設定を認証できる
- 新しいエンタープライズアプリの開発者を信頼できる
- アンマネージド送信先でマネージドのソースからのドキュメントを使用できる
- マネージド送信先でアンマネージドのソースからのドキュメントを使用できる
- AirDrop をアンマネージドの送信先として扱う
- ハンドオフを使用できる
- 診断データと使用状況データを Apple に送信できる
- タッチ ID を使用してデバイスのロックを解除できる
- Apple Watch の手首検出を強制
- AirPlay ペアリングの初回にパスコードが必要
- ロック画面でウォレット通知を使用できる
- ロック画面に管理センターを表示
- ロック画面に通知センターを表示
- ロック画面に「本日」ビューを表示
- 評価領域を設定
- ムービー、TV、アプリの許容可能なコンテンツ評価を設定
- iBooks Store の明らかな性的コンテンツを許容

その他のペイロード
- Wi-Fi のペイロード
- VPN のペイロード
- メールのペイロード
- Exchange ActiveSync のペイロード
- Google アカウントのペイロード
- LDAP のペイロード
- カレンダーのペイロード
- 連絡先情報のペイロード
- 登録済みカレンダーのペイロード
- ウェブクリップのペイロード
- macOS サーバーアカウントのペイロード
- ドメインのペイロード
- 認証情報のペイロード
- SCEP のペイロード
- APN のペイロード
- 携帯電話のペイロード
- シングルサインオンのペイロード
- フォントのペイロード
- AirPrint のペイロード
- ネットワーク利用ルールのペイロード

管理コマンド
- リモートロック
- リモートワイプ
- パスコードのクリア
- デバイスのアンマネージ
- インベントリーの更新
- ブランクプッシュの送信

Managed + Supervised

登録(DEP のみ)
- デバイスの監視
- MDM プロファイルの必須化
- Mac コンピューターへのペアリングは無効
- ユーザーが MDM プロファイルを削除できない
- 共有 iPad を有効にする
- 登録認証情報が必須
- セットアップアシスタントオプションの省略
- デバイスの命名法の定義

制限のペイロード(Supervised のみ)
- FaceTime を使用できる
- クラスルームアプリによる画面観察が可能
- マネージドクラス向けに AirPlay とビュー画面の許可を変更できる
- AirDrop を使用できる
- iMessage が有効を使用できる
- Siri 優先フィルターを有効化できる
- Siri でユーザー作成コンテンツを使用できる
- iBooks Store を使用できる
- App Store を使ってアプリをインストールできる
- 自動アプリダウンロードが可能
- アプリを削除できる
- Apple Music を使用できる
- ラジオを使用できる
- iCloud のドキュメントとデータを使用できる
- コンテンツと設定をすべて削除できる
- 設定プロファイルをインストールできる
- アカウント設定を変更できる
- Bluetooth 設定を変更できる
- 携帯電話のデータアプリ設定を変更できる
- デバイス名を変更できる
- 友達検索設定を変更できる
- 通知設定を変更できる
- パスコードを変更できる
- タッチ ID の指紋を変更できる
- 制限条件を変更できる
- 壁紙を変更できる
- Configulrator 以外のホストとのペアリングが可能
- 診断設定を変更できる
- Apple Watch とのペアリングが可能
- アンマネージドのWi-Fi ネットワークと接続できる
- 予測キーボードを使用できる
- キーボードショートカットを使用できる
- 自動修正を使用できる
- スペルチェックを使用できる
- 定義を使用できる
- ディクテーションを使用できる
- iTunes Store を使用できる
- ニュースを使用できる
- ポッドキャストを使用できる
- ゲームセンターを使用できる
- Safari を使用できる
- AutoFill を有効にする
- 不正行為警告を強制
- JavaScript を有効にする
- ポップアップをブロック
- Cookies をブロック
- 明示の音楽、ポッドキャスト、iTunes U を再生できる
- 自律シングルアプリモード
- アプリの非表示/表示
- AirPlay の送信先を制限

その他のペイロード(Supervised のみ)
- ホーム画面レイアウトのペイロード
- シングルアプリモード
- グローバル HTTP プロキシのペイロード
- コンテンツフィルターのペイロード
- ロック画面メッセージのペイロード
- 通知のペイロード

管理コマンド(Supervised のみ)
- 壁紙の設定
- アクティベーションロックの回避
- サウンド付きロストモード
- iOS の更新(DEP 登録のみ)
- 制限条件のクリア
- デバイス名の変更
- デバイスの再起動
- デバイスのシャットダウン
- ユーザーの削除(共有 iPad のみ)
- ユーザーのログアウト(共有 iPad のみ)