iOS 10.3 + EMM

企業による制御とセキュリティを強化

目次

MobileIron

日本

〒106-0041

東京都港区麻布台1-11-10

日総第22ビル 3階

japan@mobileiron.com

www.mobileiron.com

Tel: +81.03.6426.5301

Fax: +81.03.6426.5302

現代のモバイル企業向け主要機能をiOS 10.3に搭載

Appleは、最近のiOS 10.3リリース時でも、重要なリリースにおいて、従来通り企業を重視した機能の提供を継続していくことを示唆しています。春の更新では、ネイティブメールアプリの使いやすさとセキュリティを高める新しい拡張機能、Wi-Fiネットワークに制限をかけてセキュリティを改善する機能など、影響力の高い企業向け機能を提供しました。デバイスのリモートシャットダウンや再起動など、一部の新機能は、会社所有シングルユース（COSU）デバイスに特に適しています。さらに、AppleはtvOSへの投資を拡大し、第4世代Apple TV向けのEMM構成と制御機能を追加しました。教育にも引き続き力を入れ、Classroomアプリの用途を拡大するとともに、教育におけるShared iPadの進化を継続しています。

企業は、新しい機能の多くが「監視下」のデバイスまたは機関/団体所有のデバイスにのみ対応することに注意する必要があります。これらの新機能を利用したい組織は、デバイス登録プログラム（DEP）とMobileIronなどのエンタープライズモビリティ管理（EMM）プラットフォームを通じてiOSデバイスを管理する必要があります。

新しいファイルシステムが性能を向上

Appleは10.3で、すべてのiOSデバイスのファイルシステムを入れ替えました。前のファイルシステム「HFS+」は1988年からMacに使用され、iOSとtvOSの両方にも発表当初から使用されてきました。後継のApple File System（APFS）は、まずiOSに導入される予定で、現在のソリッドステートドライブ（SSD）に最適化されています。APFSはレイテンシの削減を目的としているため、ユーザーは性能の向上を体感するはずです。APFSでは、保存可能なファイル数が大幅に増えるほか、64ビットファイル名や新しい柔軟な暗号化方式もサポートされます。この方式では、複数の鍵による非常に詳細な暗号化が可能です。ファイルシステムレベルの作業を多用するアプリケーション開発者は、APFSとの意図しない矛盾を防ぐため、iOS 10.3に対してコードを綿密にテストする必要があります。

Wi-Fi制限機能が信頼できないネットワークからデバイスを保護

管理者は、監視下のデバイスに対する新しいWi-Fi制限により、Wi-Fiネットワークのホワイトリストを作成できます。ホワイトリストにないネットワークまたはサービスセット識別子（SSID）は、デバイスのWi-Fi設定メニューに表示されません。

新しいWi-Fi制限機能は、会社所有シングルユースデバイスのiPadなど、許可された店舗ネットワークにしか接続しないCOSUデバイスのセキュリティ確保に特に有用です。Wi-Fiホワイトリストは、空港やカフェなどで、従業員が信頼できないWi-Fiネットワークに接続するのを防止する上でも有効です。このような場所では、ハッカーが既存ネットワークのスプーフィングによってデータを抜き取ろうとすることが増えています。

OAuth 2.0がメールセキュリティを強化

10.3では、Exchange ActiveSync 16.1を併用した場合、Microsoft Office 365に対してOAuth 2.0をサポートするよう、ネイティブのメールクライアントは最適化されています。OAuth 2.0は、ユーザー名とパスワードに依存せず、セキュアトークンを使用してセキュアアクセスを行います。OAuthが導入されていない場合、メールクライアントはデフォルトで以前のドメイン自動発見処理を実行します。すなわちデバイスは、メールアドレスに設定されたドメインに基づいて正しいメールサーバーを見つけようとします。Appleは、署名と暗号化の強化によってS/MIMEも改善しました。S/MIMEは、ActiveSync構成をネイティブのiOSメールに展開する際に何年も前から使用されてきましたが、新しい拡張機能によってユーザーは署名と暗号化に使用する証明書を非常に柔軟に決定できるようになります。

EMM拡張機能がデバイス管理を簡素化

Appleは引き続き、DEPとEMMによるiOSデバイスのセキュリティ確保に注力しています。DEPの新しい機能により、管理者は、新規デバイスのiCloudとホーム設定画面をスキップできます。以下に紹介するように、新しい管理機能のほとんどは、会社所有の監視下のデバイスにのみ対応します。

- **管理者が、監視下のiOSデバイスをリモートでシャットダウンおよび再起動。**この機能は年度末にクラスを終了する学校システムにおいて特に便利です（監視下デバイスのみ）。
- **パスコードでロックされたデバイスを最新のiOSバージョンに更新。**これまでは、デバイスがロックされている場合、ユーザーがパスコードを入力しなければ更新を完了できませんでした。今後はユーザーがデバイスのロックを解除しなくても更新できます。これは、夜間、デバイスのロックを解除する管理者がいないときにOSを更新する際に便利です（監視下デバイスのみ）。
- **iOSデバイスで必要に応じて紛失モードサウンドを再生。**これは、小売店内でキオスクデバイスの置き場所を間違えたり、学生が学校でiPadを紛失した場合など、Apple IDを持たないデバイスの発見に役立ちます（監視下デバイスのみ）。
- **管理者が口述記録に対して新しい制限を実行。**この機能により、機密性の高い医療/法的記録など、慎重に扱うべき口述コンテンツのセキュリティを強化し、紛失や、iCloudや他のクラウドサービスへのコピーを防止できます（監視下デバイスのみ）。

- **ネットワークに接続したiOSデバイスのポスチャーをチェック。**iOSデバイスがネットワークに接続している場合、IT部門は、それが組織にとって信頼できるかどうかを判断できます。
- **モバイル管理者は、デバイスが音声、データ、ローミング接続に、IPv4またはIPv6プロトコルのどちら（または両方）を使用するかを指定可能。**これによりIPv6を標準とする組織が、モバイル環境にコンプライアンスの範囲を拡大できます。

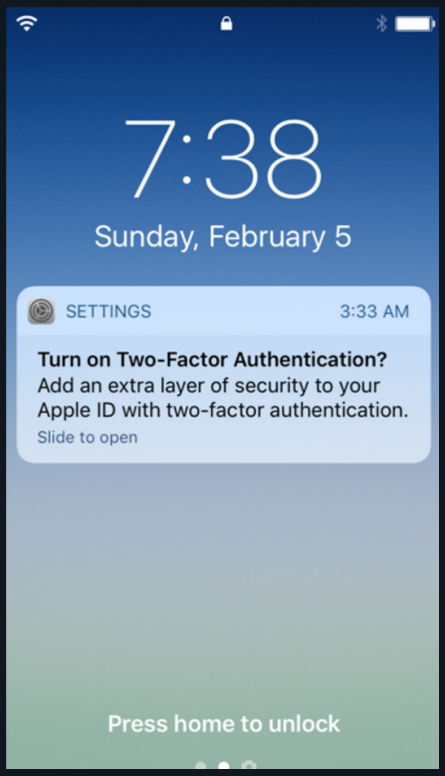
2要素認証がデバイスセキュリティを大幅に向上

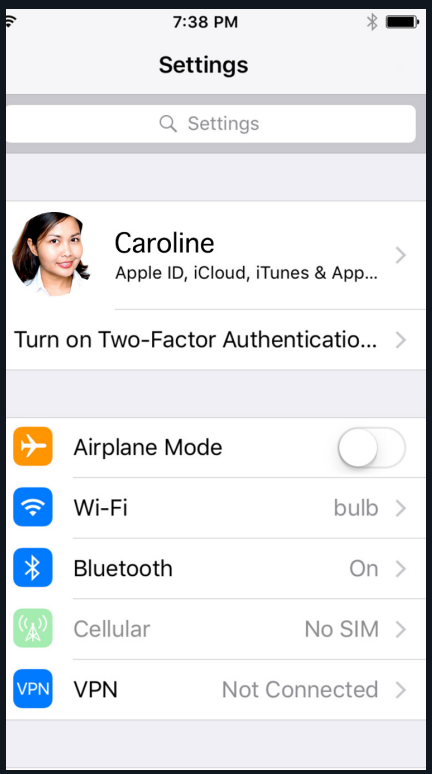
Appleは、しばらく前から2要素認証（2FA）の使用をサポートしていますが、10.3ではさらに前進しています。Apple IDがパスワード認証用にしか設定されていない場合、iOS 10.3デバイスは、2FAを設定するようユーザーに指示を表示します。設定アプリも、ユーザーに2FA設定を開始するよう通知を表示します。最後に、iOS 10.3では設定メニューの一番上に目立つようにApple IDが表示されるため、ユーザーが迷うことなく、すぐにそれを見てApple ID（2FAなど）に変更を加えることができます。

Macによるキャッシングアプリとiosの更新をスピードアップ

Macデバイスを一時キャッシュサーバーとして構成し、iOSの更新やデバイスへのアプリ展開に利用することが可能となりました。たとえば、最近更新されたmacOS Sierraデバイスにiosデバイスを接続すれば、そのMacを通じて展開されたアプリやiOSの更新をダウンロードできます。インターネットでファイルをダウンロードする必要はありません。

この機能は大量のデバイスを運用する企業には特に便利です。病院で100台の新しいiPadに2GBのアプリと最新バージョンのiOSをインストールする場合など、重いファイルは1台目のデバイスにだけダウンロードします。残りのデバイスをUSBまたはUSBハブでMacに接続し、有線でアプリとOSをダウンロ





Appleは、2FAによるApple IDの保護を推奨しています。

ードすれば、デバイスを準備する時間を大幅に短縮できます。テザリング機能は、現在提供されているmacOSサーバー対応のキャッシングサーバー、すなわち企業のローカルネットワークで動作するOTAソリューションを強化するものです。

tvOSが企業向けに対応

Appleは、第4世代のApple TVデバイス向けにtvOS管理を強化しつつあります。tvOS 10.2リリースでは、従来のiOSデバイスでしか使えなかった多くの機能をApple TVデバイスにも対応させました。これには、証明書の構成と展開、セキュアな企業ネットワークの構成、Apple TVのリモート削除などが含まれます。さらに重要なのは、認定DEP代理店から購入すれば、Apple TVをDEPと監視OTAに登録できるようになったことです。これは、tvOSを教育/企業環境で活用するというAppleのビジョンを大きく前進させます。

EMM + iOS 10.3がデジタルクラスルームを強化

教育プログラムにおけるShared iPadには、Apple School Manager（ASM）、教師と学生向けのClassroomアプリ、学生の代わりにマネージドIDを作成する機能が必要です。

iOS 10.3は、従来のマネージドクラス機能を改善し、非マネージドクラスにも対応するよう更新されたClassroom 2.0アプリを含みます。Classroom 2.0アプリをマネージドクラスに導入すれば、教師が学生のデバイスをミュートさせ、学生が文書やURLを教師と共有することも可能です。非マネージドのClassroom 2.0アプリを導入すれば、ユーザーがASMに登録したり、EMM構成プロファイルをデバイスにインストールしたりする必要はありません。教師が4桁のパスコードを入力して非マネージドクラスに学生を招待するだけです。学生はマネージドクラスに登録していない限り、招待に応じることができます。

現代企業を支えるiOSとMobileIron

iOS 10.3は、現代のモバイル企業やモバイルクラスルームに対するAppleの継続的な取り組みを明確に示しています。新しい機能の多くは、監視下の機関/団体所有デバイスにしか対応しませんが、AppleはiOS 10.3により、iOSユーザーの期待する生産性の高いネイティブ体験を犠牲にせず、IT部門による制御/セキュリティを優先することを継続しています。

MobileIronのモバイル/クラウド統一セキュリティプラットフォームの併用により、組織はさらにセキュアにアプリを導入し、デバイスの導入と管理の規模を拡大し、あらゆるネットワーク上でクラウドベースのアプリやデータを保護することができます。MobileIron EMMのiOS運用サポートに関する詳細は、Webサイトをご覧ください。