

モバイルファースト行政

MobileIronは、行政機関における職員のモバイル化をサポートします。行政機関は、MobileIronを通じて機関所有/職員所有のモバイルデバイス上で機密データを保護すると同時に、職員の生産性を高め、最終的には市民への対応を迅速化します。また、現場任務の支援と業務の最適化にもモバイル技術の活用が可能となります。

現在の行政機関において、モビリティはますます重要になっています。移動が容易となり、業務が私生活にあふれるに伴い、モバイルデバイスが最前線で活躍するようになりました。もはやEメールだけでは足りません。アプリやファイルへのリアルタイムアクセス、さらにデータ共有機能やコラボレーション機能をいつでもどこでも利用できることが、生産性を最大限に高めるポイントです。

モバイルを活用する職員のために、行政機関はモバイルコンピューティングやテレワークを通じて業務を最適な場所、時間、リソースに業務をシフトする傾向にあります。そして職場でのモビリティが高まるにつれ、多くの機関職員がスマートフォンやタブレットなどのモバイルデバイスを業務に利用しています。

MobileIronは、マルチデバイスのマルチOS環境をサポートする機敏でセキュアなインフラを積極的に構築する行政機関を支援します。どの連邦機関にとってもセキュリティやコンプライアンスは最重要事項であり、MobileIronは機関のモバイルファースト化とクラウドファースト化の両方に対応するセキュアなインフラストラクチャの構築を可能にします。

セキュアな行政機関でのデバイス

政府職員のデバイスがBlackBerryだけだった時代は終わりました。現代の職員は機関所有と個人所有の両方のデバイスで行政/機関のEメールにアクセスしており、モビリティに対する機関の考え方も変化しています。しかし、無料ファイル共有サービスなどの次善策で任務を遂行したり生産性を高めたりすれば、職員は無意識に機関をサイバー攻撃や情報漏洩の危険にさらすことになります。したがって、行政機関のモバイル戦略においては常にデバイスセキュリティを中心に置く必要があります。管理やセキュリティをなおざりにすれば、機関の全モバイルデバイスがネットワークや最重要データへの侵入口となる恐れがあります。

MobileIronは、iOS、Android、Windows PhoneなどOSを搭載したあらゆるデバイスにわたり、行政機関がデータのセキュリティ確保と管理を行う手助けをします。MobileIronの技術は、会社所有とユーザー所有の両方のデバイスに対応する自動デバイス構成、証明書ベースのセキュリティ、企業データのセレクトティブワイプ機能を提供し、企業Eメールとメール添付ファイルのセキュリティを確保します。セキュアなEメール、アプリ、コンテンツの配信により、機関は適切なリソースをユーザーにセキュアに提供しつつ、デバイスのネイティブなユーザー体験を維持できます。

利点

- あらゆるデバイスでネイティブ体験を維持しつつ、機関Eメールにセキュアにアクセス
- 高耐久性デバイスのセキュリティを確保
- 前線任務などの現場作業に有効
- 職員所有デバイスのサポートにより資産コストを削減
- すべての職員のデバイスに行政アプリをセキュアにプッシュ
- チームメンバー間のセキュアなコラボレーションに対応
- CJIS、NSA Commercial Solutions for Classified Program Components List (CSfC)、NIAP MDM-PP、FIPS 140-2 (3PAO認定)、HIPAA、SOC2 Type 2、Government Records Initiativeなどの政府規制に対応

「モビリティビジョン: 従業員のモバイル性を高め、いつでもどこでも情報へのセキュリティアクセスとコンピュータ処理能力を与えることで業務の有効性を高める。」

[DoDモバイルデバイス戦略](#)

機密アプリ/コンテンツのセキュリティ

すべての行政機関は、セキュリティ、モビリティ、高可用性に関する多様な連邦指令に従う必要があります。新しいモバイルワークフローで指令の要件を満たすには、デバイスとアクセスポイントを厳密に管理し、行政データのセキュリティを確保する必要があります。あらゆるセキュリティ侵害は、高い罰金に加え、市民情報や機密データの漏洩につながります。

ネイティブな体験を維持したセキュアクライアントのEメール機能は第一歩ですが、それで十分ではありません。行政機関は、MobileIronにより、デバイス管理とセキュアなEメール配信だけでなく、機密データへのセキュアアクセスも提供できます。また、MobileIronのContent Security Serviceを通じて、複数のビジネス用/個人用クラウドコンテンツリポジトリにわたってドキュメントレベルのセキュリティを提供し、HIPAAなどの規制コンプライアンスを強化できます。内蔵のアクティビティ追跡およびコンプライアンスツールは、すべての監査証跡の記録と保存を要求する行政記録指令 (Government Records Directive) への適合をサポートします。

現場作業のモバイル化

モバイルデバイスは、現地調査員、消防署等の職員職員、前線任務の軍事関係者まで、あらゆる現場作業員によるシームレスなアプリアクセス、生産性の向上、現場からの応答や報告のスピードアップなどを可能にします。しかし、セキュリティの侵害を許さない確実なソリューションがなければモビリティの導入は困難です。

行政機関は、MobileIronにより現場職員に有効に仕事をさせることができます。MobileIronは、包括的なセキュリティソリューションだけでなく、マルチユーザーサポートなどのワークフロー強化機能も提供し、現場での資本コスト削減やビジネスワークフローの革新に貢献します。例えば、アメリカの場合、連邦航空部門がMobileIronで管理されたセキュアタブレットでフライト予約情報へのアクセスを可能にすれば、機体の重量を軽減できるだけでなく、デバイスにリアルタイムで更新情報を配信できます。

個人所有デバイスの業務利用 (BYOD)

行政上の命令や指令に加え、多くの行政機関は、BYODが設備投資とITサポート費用を節約し、同時に職員にモバイルデバイス選択の自由を与える手段と考えています。機関は、BYODにおいてモバイルデバイス上の個人用コンテンツを維持し、職員のプライバシーを保護しつつ、行政データとアプリへのセキュアなアクセスを可能にする必要があります。多くの種類のOSとデバイスにわたって管理を簡素化するには、全モバイルデバイスのセキュリティを確保できる1つのEMMソリューションが必要です。

「MobileIronのセキュアで拡張可能なプラットフォームにより、USDAはモバイルアプリ、データ、およびデバイスがセキュアであるという確信を持ってモビリティイニシアチブを進めていくことができます。」

Jay Sunny Bajaj氏、DMI設立者兼CEO

MobileIronは、企業環境でモバイルデバイスのセレクトティブワイプと管理を可能にするBYODプライバシー技術の特許を取得し、革新性を実証してきました。また、最新のOSおよび関連モバイル機能の更新を即日サポートしています。MobileIronのEMMプラットフォームにより、行政機関は組織内のすべてのデバイスタイプを管理およびサポートし、職員は選択の自由を得、なおかつIT部門は機密データのセキュリティに自信を持つことができます。コンテナ化で複数のモバイルOSベンダーにわたるアプリ/コンテンツ配信に対応することにより、MobileIronは、個人データに触れることなく、機関/行政データを完璧に保護します。

MobileIronについて

モバイルIT分野のリーダーであるMobileIronは、エンタープライズモビリティによってビジネスの変革を図る何千もの組織にご利用いただいています。オンプレミスにもクラウドにも対応するMobileIronのソリューションは、世界企業におけるモバイルアプリ、ドキュメント、デバイスのセキュリティ/管理専用設計され

ました。MobileIronは、マルチOSモバイルデバイス管理 (MDM)、モバイルアプリケーション管理 (MAM)、BYODプライバシーコントロールなどのキーイノベーションを初めて実現しました。

MobileIronの行政向けソリューションは、FIPS 140-2、NIAP-PP、GRI、FISMA、HIPAA、SOC2などの厳しい連邦規制とコンプライアンス要件を満たします。MobileIronは、専任の行政担当チームを駆使し、強力なエコシステムパートナーシップを構築しています。また、新しいOSやOEMリリースの即日サポートでセキュリティを強化し、一切の脆弱性を許しません。

詳細は、<https://www.mobileiron.com/government>をご覧ください。

お問い合わせはglobalsales@mobileiron.comまで。