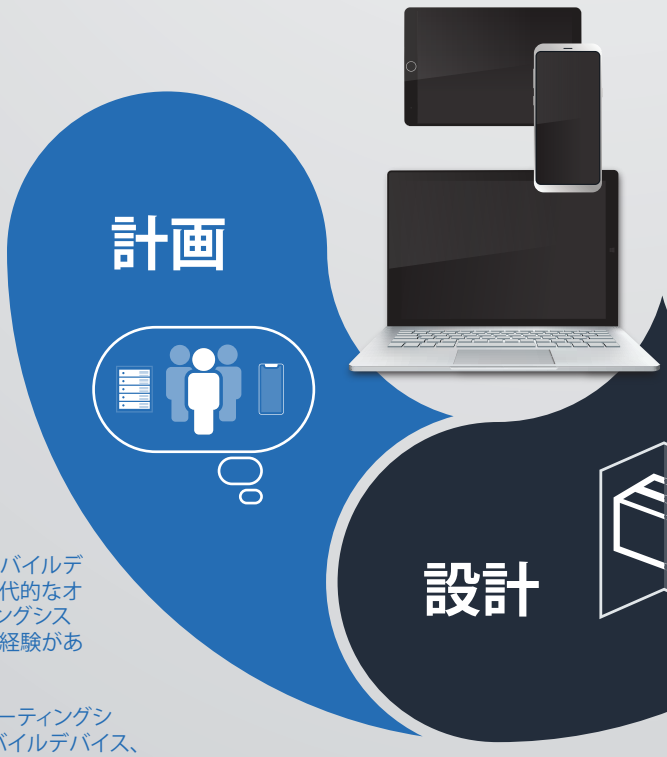
UEM導入のベストプラクティス

職場の改革は大きな冒険に思えるかもしれませんが、適切な統合エンドポイント管理（UEM）ソリューションを選べば、現代のモバイル企業への道も遠くありません。UEMソリューションの導入は、以下で説明する4つの手順で行うのが最適です。



計画

従業員にモバイルデバイスや現代的なオペレーティングシステムの使用経験があるか？

どのオペレーティングシステム、モバイルデバイス、デスクトップを社内でサポートするか？

ネットワークインフラはどれくらい複雑か？

ITガバナンスフレームワーク、ポリシー、プロセスはどれくらい成熟しているか？

ITチームが企業向けモバイルアプリを開発、導入できるか？

従業員の教育やトレーニングリソースはどの程度効果があるか？

ITチームに証明書認証の経験があるか？

会社にどのようなセキュリティ要件があるか？

設計

役割の定義
- この体制を支えるために必要な管理者の人数は？
- それぞれの職責は？

可視性の定義
- 各管理者が可視化し、レポートを作成するユーザーとデバイスは？

アクションの割り当て
- 各管理者が実行できるアクションは？

配布の管理
- 各管理者がユーザー/デバイスに配布できるアプリ、ポリシー、構成は？

導入

導入形態はオンプレ？

クラウドベース？

運用開始

ヘルプデスクのスタッフがマルチOS管理の問題を理解しているか？

ヘルプデスクのスタッフが必要に応じてデバイスの専門家と協力できるか？

期待されるレベルのサポートを提供するためにヘルプデスクのスタッフが必要なリソースにアクセスできるか？

ヘルプデスクのスタッフが最新の情報を把握できるよう継続的な研修が提供されているか？

MobileIron

MobileIronの統合エンドポイント管理（UEM）により、従業員は、セキュアなモバイルデバイス、デスクトップ、クラウドサービスを通じてビジネスアプリ/データにシームレスにアクセスし、なおかつ自分のプライバシーを完全に維持することができます。

MobileIron UEMバンドル	Silver	Gold	Platinum
オンプレおよびクラウドベースのUEM導入形態オプション	✓	✓	✓
Sentryは、モバイルデバイスとバックエンドの企業システム間のトラフィックを管理、暗号化し、セキュリティを確保するインラインのゲートウェイです。	✓	✓	✓
Apps@Workは、ユーザーに配布可能な社内開発のアプリとサードパーティのビジネスアプリを管理する企業向けアプリストアです。	✓	✓	✓
AppConnectは、AppConnect対応アプリ用のセキュアなビジネスアプリコンテナで、特定アプリ向けVPNを備えています。		✓	✓
Email+は、メール、連絡先、カレンダー、iOS/Androidデバイス用のタスクを含むセキュアなモバイル生産性向上アプリパッケージです。		✓	✓
Docs@Workは、さまざまなEメールシステムやオンプレ/クラウドコンテンツ管理システムで文書へのアクセス、注釈付け、共有、表示を可能にします。		✓	✓
Web@Workは、エンドユーザーが社内のWebリソースに短時間で簡単にアクセスするためのセキュアな企業向けモバイルブラウザです。		✓	✓
macOSデスクトップ管理機能は、プロビジョニング、構成、セキュリティ/制御、アプリ展開、監視、コンプライアンスなど、ライフサイクル全般にわたります。		✓	✓
Help@Workは、ユーザーとヘルプデスク担当者の画面共有を可能にし、トラブルシューティングの効率化と問題解決の時間短縮に貢献します。			✓
Tunnelは、Per-App VPN機能によって特定のアプリを認証し、エンドユーザーの操作なしでファイアウォール内の企業リソースにアクセスさせることができます。			✓
MobileIron Monitorは、重要なMobileIron UEMコンポーネントすべての正常性を維持する包括的なダッシュボードベースのソリューションです。			✓
ServiceConnect Integrationsは、MobileIron App for Splunk EnterpriseServiceNowとの統合により、ITのワークフローを簡素化します。			✓
MobileIron Bridgeは、既存のグループポリシーオブジェクト（GPO）スクリプトを利用し、Windows 10 PCの詳細なセキュリティと管理を可能にします。	オプショナルライセンス。MobileIron UEMバンドルが必要。		
MobileIron Accessは、Microsoft Office 365、Salesforce、G Suite、Boxなどのクラウドサービスに対応するセキュアな条件付きアクセス制御機能を提供します。	オプショナルライセンス。MobileIron UEMバンドルが必要。		
MobileIron Threat Defenseは、モバイルデバイス上で既知の脅威やゼロデイ脅威を検出し、対処することにより、企業データを保護します。インターネット接続やユーザーの介入は不要です。	オプショナルライセンス。MobileIron UEMバンドルが必要。		

MobileIronが現代的なモバイル企業を実現

MobileIron UEM

現代のセキュアなデバイス、アプリ、クラウドサービスを活用し、ビジネスの革新を実現します。
https://www.mobileiron.com/ja/solutions/enterprise-mobile-management-emm

MobileIron ACCESS

Microsoft Office 365、Salesforce、G Suite、Boxなどのクラウドサービスに対応するセキュアな条件付きアクセス制御機能です。
www.mobileiron.com/ja/products/mobileiron-access

MobileIron THREAT DEFENSE

モバイルデバイス上で既知の脅威やゼロデイ脅威を検出し、対処することにより、1つのアプリで企業データを保護。インターネット接続やユーザーの介入は不要です。
https://www.mobileiron.com/ja/threat-defense

MobileIron BRIDGE

既存のグループポリシーオブジェクト（GPO）スクリプトを利用し、Windows 10 PCの詳細なセキュリティと管理を実行します。
https://www.mobileiron.com/ja/products/mobileiron-bridge-ja

MobileIron

〒106-0041 • 東京都港区麻布台1-11-10 • 日総第22ビル3階
www.mobileiron.com • japan@mobileiron.com

Tel: +81.3.6426.5301
Fax: +81.3.6426.5302