



主なメリット

- 単一のコンソールで、デバイスを供給、保護、管理
- 電子メール、カレンダー、連絡先、Wi-Fi や VPN のプロファイルを無線通信経由で設定し、速やかに出発できます
- iOS、Android、Windows Phone、BlackBerry のモバイル・オペレーティングシステムの最新リリースを発売日から利用可能
- デバイスのパスコード要求や、感染デバイスのブロックなどの自動化されたコンプライアンスアクションで、セキュリティポリシーを設定、強制
- 強固なダッシュボードやレポートの活用で、企業デバイスと個人用デバイスの両方を管理

IBM MaaS360 Mobile Device Management

最新のモバイルデバイスを保護、管理

IBM® MaaS360® Mobile Device Management は、エンタープライズアクセスのための設定、スマートフォンやタブレットにある企業データの保護などを単一画面でできる高速で完全な機能を備えたソリューションです。

強固で、統合的なクラウド対応プラットフォームである MaaS360 は、モバイルデバイス、アプリケーション、文書に渡る迅速な展開、可視性、コントロールで、モバイルデバイス管理 (MDM) を簡素化できます。

展開は、極めて迅速です。ほんの数クリックで、IT 管理者はデバイスの登録を開始し、導入から、エンタープライズ統合、設定や管理、監視やセキュリティ、サポート、分析やレポートまでのモバイルデバイスのライフサイクル全体の迅速な管理を実現できます。

MDM の課題を解決

- セキュリティおよびコンプライアンスを強化
- モバイル資産のサポートコストを低減
- アプリケーションおよびパフォーマンスの管理を向上
- より良いビジネス継続性を保証
- 生産性および従業員の満足度を向上

MaaS360 を採用する理由

- 実証済みのエンタープライズ・モバイル管理へのアプローチ
- 強力な管理とセキュリティで、モビリティのライフサイクル全体をカバー
- 既存のインフラストラクチャーと簡単に統合
- 卓越したカスタマー・エクスペリエンスで、簡単かつ迅速





図 1:さまざまなデバイスでの MaaS360 の例

モバイルデバイスを迅速に登録

MaaS360 Mobile Device Management は、プラットフォームのセットアップやデバイスの登録プロセスを効率化し、IT 部門および従業員の活動を簡素化します。

- MDM サービスを選択し、デバイス登録を設定
- SMS、電子メール、カスタム URL を使用して、登録リクエストを over-the-air (OTA) で送信
- ワンタイム・パスコードや SAML を使って、Active Directory/LDAP で認証
- カスタマイズされた使用許可ポリシーや EULA を作成、配布
- 企業および個人が所有する Bring Your Own Device (BYOD) を登録
- 個別または一括のデバイス登録を開始
- デフォルトのデバイスポリシー設定を適用または修正

モバイルデバイスを企業システムと統合

MaaS360 Cloud Extender を使用すれば、オンプレミスのサーバーやネットワークの再設定なしで、企業システムを簡単に統合できます

- 企業システムにアクセスするデバイスを瞬時に検出
- Microsoft Exchange、Lotus Notes、Microsoft Office 365、Gmail と統合可能
- 既存の Active Directory/LDAP や認証機関を利用して構築
- Manage BlackBerry Enterprise Server (BES) ポリシー
- 強固な Web API で、他の業務システムとも接続可能

モバイルデバイスを集中管理

MaaS360 は、複数のプラットフォームに渡るポリシーやコントロールを集中管理し、スマートフォンやタブレットのための統合的デバイス管理コンソールを提供します。

- 電子メール、カレンダー、連絡先、Wi-Fi や VPN のプロファイルを無線通信経由で設定
- 新しいモバイルデバイスを、ネットワークを通じて承認、隔離
- カスタムグループの作成で、きめ細かい管理を実現
- 公開および社内用アプリケーションを配信、管理
- 文書やコンテンツを安全に共有、更新
- MaaS360 Mobile Device Management で、役割に基づく管理ポータルへのアクセス権を定義
- 企業データや MDM コントロールの削除で、デバイスを破棄

予防的にモバイルデバイスを保護

MaaS360 Mobile Device Management は、動的、強固なセキュリティおよびコンプライアンスの管理機能で、デバイスを継続的に監視し、対処します。

- 品質、長さ、期間が設定可能なパスコードポリシーを要求
- 暗号化やパスワード表示設定を強制
- 機能、アプリケーション、iCloud、コンテンツ評価について、デバイス制限を設定
- ジェイルブレイクデバイスやルートデバイスを検出、制限
- 紛失または盗難デバイスをリモートから探し、ロック、ワイプ可能
- 個人用データを残したまま、企業データを選択的にワイプ可能
- 自動化されたアクションで、ほぼリアルタイムのコンプライアンスルールを実装
- ジオフェンシング・ルールを有効にして、場所に基づくコンプライアンスを実施

MDM サポートの効率化

MaaS360 Mobile Device Management は、Web ベースのポータルで、デバイス/ユーザー/アプリケーションの問題を診断、解決する機能を備え、IT に関する詳細な可視性やコントロールを提供し、最適なモバイルユーザーの生産性を推進します。

- デバイスビューへのアクセスで、問題を診断、解決
- 紛失または盗難デバイスを探す
- 忘れたパスコードをリセット
- デバイスへのメッセージ送信
- オンデマンドで構成設定を更新
- セルフサービス・ポータルでユーザー自身によるヘルプを支援

モバイルデバイスを監視、レポート

Mobility Intelligence™ ダッシュボードは、モバイルデバイス管理のオペレーションやコンプライアンスに関するインタラクティブでグラフィカルなサマリーを提供し、IT 部門がオンデマンドで全社的な報告を行えるようにします。

- 詳細なハードウェアおよびソフトウェアのインベントリレポート
- 構成および脆弱性の詳細
- 実質的にすべての属性に対して統合的にスマート検索できる機能
- カスタマイズ可能な監視リストで、アラートを追跡、受信
- BYOD プライバシー設定で、個人を識別できる情報の収集をブロック
- 最適化されたモバイル費用の管理で、継続的にデータ利用を監視、警報

簡便なモバイルデバイス管理

MaaS360 Mobile Device Management は、iPhone、iPad、Android、Kindle Fire、Windows Phone、Windows 10、BlackBerry などのスマートフォンやタブレットを含む、最新のモバイルデバイスをライフサイクル全体に渡って管理できる必須機能を備えた、使いやすい MDM プラットフォームです。

MDM の必須機能

- SMS、電子メール、URL の over-the-air (OTA) 登録
- パスコードおよび暗号化の強制
- 電子メール、VPN および VPN のプロファイル
- デバイス制限の設定
- リモートからの探索、ロック、ワイプ (全面的および選択的)
- ジェイルブレイクおよびルートの検出
- ポリシーの更新および変更
- コンプライアンス・レポート

強固なモビリティ管理

- 電子メールアクセスのコントロール
- 企業ディレクトリの統合
- 証明書管理
- BYOD プライバシー設定
- デバイスではなく、ユーザーに固有のペルソナポリシー
- 自動化されたコンプライアンスエンジンで、ほぼリアルタイムのアクション
- 場所の追跡およびジオフェンシング
- ダッシュボードおよびアラート

IBM Security 詐欺防止ソリューションの詳細については、日本IBM 営業担当員または IBM ビジネス・パートナーにお問い合わせいただくか、次の Web サイトをご覧ください。
ibm.com/security.



© Copyright IBM Corporation 2016

IBM Systems and Technology Group
Route 100
Somers, NY 10589

Produced in Japan
March 2016

IBM、IBM ロゴ、ibm.com、および X-Force は、世界の多くの国で登録された International Business Machines Corporation の商標です。BYOD360™、Cloud Extender™、Control360®、E360®、Fiberlink®、MaaS360®、MaaS360® およびデバイス、MaaS360 PRO™、MCM360™、MDM360™、MI360®、Mobile Context Management™、Mobile NAC®、Mobile360®、Secure Productivity Suite™、Simple. Secure. Mobility.®、Trusted Workplace™、Visibility360®、および We do IT in the Cloud.™ およびデバイスは、IBM 社の一員である Fiberlink Communications Corporation の商標または登録商標です。他の製品名およびサービス名等は、それぞれ IBM または他社の商標である場合があります。現時点での IBM の商標リストについては、次の Web サイトをご覧ください。ibm.com/legal/copytrade.shtml でご覧いただけます。

Apple、iPhone、iPad、iPod touch、および iOS は、米国、その他の国における Apple Inc. の登録商標または商標です。

Microsoft、Windows、Windows NT、および Windows ロゴは、Microsoft Corporation の米国およびその他の国における商標です。

本書の情報は最初の発行日の時点で得られるものであり、IBM によって予告なしに変更される場合があります。掲載されている製品・サービスは IBM がビジネスを行っているすべての国・地域でご提供可能なわけではありません。

性能データとお客様の事例は、説明目的のみのために提示しています。実際の性能結果は、特定の設定や運用条件によって異なる場合があります。他社の製品またはプログラムと IBM の製品またはプログラムを併用した場合の操作の評価および検証は、お客様の責任で行ってください。

本資料の情報は「現状のまま」提供され、商品性、特定目的への適合性に対する保証、および非侵害の保証または条件を含め、いかなる明示的または黙示的な保証も行いません。IBM 製品は、IBM 所定の契約書の条項に基づき保証されます。

適用されるすべての法令と規則の順守は、お客様の責任範囲とします。日本 IBM は、法律上の助言を提供することはいたしません。また日本 IBM のサービスまたは製品が、お客様においていかなる法を順守していることの裏付けとなることを表明し、保証するものでもありません。

IBM の将来の方向性および指針に関する記述は、予告なく変更または撤回する場合があります。

確実なセキュリティ体制への取り組みについて、IT システムのセキュリティでは、社内外の不適切なアクセスの防止策、検出、対応に取り組むことで、システムと情報を保護しています。不適切なアクセスにより、情報が改ざん、破壊、または不正利用される可能性があり、システムへのダメージや他者への攻撃といったシステムの悪用が生じることがあります。IT システムまたは製品によってセキュリティ対策が万全になると考えることは危険であり、1 つの製品またはセキュリティ対策で不正アクセスを完全に有効に防ぐことはできません。IBM のシステムと製品は、包括的なセキュリティ・アプローチの一部として設計されています。そのため、運用手順を追加することがどうしても必要となり、効果を最大限に高めるには、他のシステム、製品、サービスが必要になることがあります。IBM は、システムと製品が他者による悪意のある行為または不正行為から免れることを保証するものではありません。



Please Recycle