Windows 10

Windows 10 Mobile

展開および管理ガイド

2016 年 7 月

このドキュメントに記載されている情報は、このドキュメントの発行時点におけるマイクロソフトの見解を反映したものです。マイクロソフトは市場の変化に対応する必要があるため、このドキュメントの内容に関する責任を問われないものとします。また、マイクロソフトは発行日以降に発表される情報の正確性を保証できません。

このホワイト ペーパーは情報提供のみを目的としています。明示または黙示にかかわらず、この内容に関してマイクロソフトはいかなる責任も負わないものとします。

お客様ご自身の責任において、適用されるすべての著作権関連法規に従ったご使用を願います。著作権法による制限に関係なく、マイクロソフトの書面による許可なしに、このドキュメントの一部または全部を複製したり、検索システムに保存または登録したり、別の形式に変換したりすることは、手段、目的を問わず禁じられています。ここでいう手段とは、複写や記録など、電子的、または物理的なすべての手段を含みます。

マイクロソフトは、このドキュメントに記載されている内容に関し、特許、特許申請、商標、著作権、またはその他の知的財産権を有する場合があります。別途マイクロソフトのライセンス契約上に明示の規定のない限り、このドキュメントはこれらの特許、商標、著作権、またはその他の知的財産権に関する権利をお客様に許諾するものではありません。

このドキュメントで例として使用されている会社、組織、製品、ドメイン、電子メール アドレス、ロゴ、人物、場所、出来事などの名称は架空のものです。実在する会社名、団体名、商品名、ドメイン名、電子メール アドレス、ロゴ、人物、場所、出来事などとは一切関係ありません。

このプレゼンテーションで使用されている画面はハメコミ合成です。一部のアプリは別売りです。提供状況とエクスペリエンスはアプリによって異なります。アプリは Windows ストアで提供されているものです。提供状況は変動する場合があります。一部の機能とサービスでは、Microsoft アカウント、Wi-Fi アクセス、およびデータ接続が必要です。別途、通信事業者の料金がかかります。アプリとコンテンツの提供状況は変動する場合があります。Office ライセンスは別売です。すべての機能を利用するには別途購入する必要があります。

Windows Information Protection (WIP) は、2016 年半ばに一般提供される予定です。

Windows Hello で生体認証を使用するには、指紋リーダー、照明付き赤外線センサー、その他の生体認証センサーを含む、専用のハードウェアが必要です。Windows Hello の資格情報またはキーをハードウェア ベースで保護するには、TPM 1.2 以上が必要です。TPM が存在しない、または構成されていない場合、資格情報およびキーの保護はソフトウェア ベースで行われます。Windows Hello のコンパニオン デバイスは、Bluetooth で Windows 10 PC とペアリングする必要があります。Windows Hello の資格情報のローミングに対応した Windows Hello コンパニオン デバイスを使用するには、Windows 10 PC の Pro または Enterprise エディションにサインインする必要があります。

Windows デバイス正常性構成証明サービスは、モバイル デバイス管理ソリューション (Microsoft Intune など) やその他の種類の管理システム (SCCM など) で実現される条件付きアクセスのシナリオで使用できます。

別途記載されている場合を除き、Windows 10 Mobile が提供されている国においては、すべての機能をご利用いただけます。アジアの一部の国では画面レイアウトが異なる場合があります。

改訂履歴

本ガイドの PDF 版をお読みの場合は、http://aka.ms/W10Mobile-MDMGuide から本ガイドの最新版をご確認ください。

2015 年 11 月	Windows 10 Mobile (バージョン 1511) に関する更新
2016 年 7 月	Windows 10 Mobile Anniversary Update (バージョン 1607) に関する更新

日常的な業務にスマートフォンを活用する従業員はますます増加しています。しかしそれに伴って、管理とセキュリティの面でこれまでにはなかった問題が発生しているのも事実です。企業側でデバイスを用意して支給する場合でも、従業員自身のデバイスの使用を許可する場合でも、ビジネス目標を達成できるように、IT 部門はモバイル デバイスとアプリをすばやく展開し、管理する必要があります。同時に、モバイル デバイス上のアプリとデータをサイバー犯罪や消失から確実に保護しなければなりません。企業がこのような課題に正面から取り組めるよう、Windows 10 Mobile には、モバイル デバイスとアプリを管理するための堅牢かつ柔軟なテクノロジが組み込まれています。

Windows 10 は、企業が自社のデバイス、データ、アプリを管理できるエンドツーエンドのデバイス ライフサイクル管理に対応しています。包括的なモバイル デバイス管理ソリューションを使用することで、デバイスの登録、構成、アプリケーション管理から、メンテナンス、モニタリング、使用中止まで、標準的な実際のライフサイクルにデバイスを簡単に組み入れることができます。

この記事の内容は次のとおりです。

- 展開
- 構成
- アプリ
- 管理
- 使用中止

展開

Windows 10 Mobile には、スマートフォンを展開、構成、メンテナンス、サポートするためのデバイス管理クライアントが組み込まれています。デスクトップ、モバイル、モノのインターネット (IoT) デバイスを含め、Windows 10 オペレーティング システムの全エディションに共通する 1 つのインターフェイスから、モバイル デバイス管理 (MDM) ソリューションを使用して、Windows 10 を搭載したデバイスを管理できます。MDM クライアントには ID 管理が統合されているため、ライフサイクル全体を通してデバイスを管理する手間が大幅に軽減されます。

Windows 10 には、包括的な MDM 機能が搭載されています。この機能は、マイクロソフトの管理ソリューションである Microsoft Intune や System Center Configuration Manager だけでなく、多くのサード パーティ製 MDM ソリューションでも管理できます。デバイスを登録して MDM の管理下に置くために、カスタムの MDM アプリを追加インストールする必要はありません。どの MDM システム ベンダーも、Windows 10 Mobile デバイス管理アプリケーション プログラミング インターフェイス (API) にアクセスできるため、企業の IT 部門は、Microsoft Intune でもサード パーティ製 MDM でも、自社の管理要件に最適なシステムを自由に選択することができます。Windows 10 Mobile デバイス管理 API の詳細については、「モバイル デバイスの管理 (英語)」を参照してください。

展開シナリオ

対象: 企業所有デバイスおよび個人所有デバイス

企業がデバイスを展開する際、一般的には、個人所有デバイスの業務利用 (BYO: Bring Your Own) と、企業所有デバイスの選択 (CYO: Choose Your Own) の 2 つのシナリオを検討します。どちらを採用する場合も、デバイスを MDM システムに登録する必要があります。MDM システムは、組織と従業員に適した設定を使用してデバイスを構成します。

Windows 10 Mobile のデバイス管理機能は、BYO シナリオで使用する個人所有デバイスと、CYO シナリオで使用する企業所有デバイスの両方に対応しています。このオペレーティング システムでは、柔軟な方法でデバイスをディレクトリ サービスや MDM システムに登録することができます。IT 部門は、モバイル ビジネス データの管理と保護に関する自社のビジネス ニーズに基づき、包括的なデバイス構成プロファイルをプロビジョニングできます。個人所有デバイスや企業所有デバイスに対するアプリのプロビジョニングは、ビジネス向け Windows ストアから、または MDM システムを使用して、簡単に行うことができます。MDM システムとビジネス向け Windows ストアを連携させて、一般公開されているストアのアプリをプロビジョニングすることもできます。

デバイスの所有者と用途を把握することは、管理戦略や、組織に必要な制御項目を決定するうえで重要な要素です。個人所有デバイス、企業所有デバイス、その組み合わせのいずれを使用するかによって、展開プロセスと構成ポリシーは異なるものになります。

個人所有デバイスの場合は、デバイス上の企業のアプリとデータを管理できるようにしつつ、従業員個人のニーズを満たすためのカスタマイズを妨げないようにする必要があります。デバイスの所有者は従業員であるため、企業のポリシーでは、業務目的と個人的な用途の両方での使用を許可し、各自が自由に個人のアプリを追加できるようにします。個人所有デバイスに関する主な懸念事項は、個人データのプライバシーを保護して従業員本人だけが管理できる状態を維持しながら、どのようにして企業データをセキュリティ侵害から保護するかという点です。これには、アプリとデータの分離に対応し、ビジネス データと個人データのトラフィックを厳格に制御できるデバイスが必要です。

企業所有デバイスの場合は、企業が制御できる範囲が広がります。IT 部門は、サポート対象のデバイス モデルのリストを従業員に提供するか、デバイスを直接購入して事前に構成することができます。デバイスの所有者は企業である

ため、従業員がデバイスをパーソナライズできる範囲は限られています。デバイスは現在の企業ポリシーに完全に準拠し、セキュリティとプライバシー上の懸念事項に対処しやすくなります。

デバイスの登録

対象: 企業所有デバイスおよび個人所有デバイス

個人所有デバイスと企業所有デバイスを MDM システムに登録するには複数の方法が存在します。どのアプローチが自社のモバイル ワーカーに最適かを判断する際は、次のような違いについて運用チームで検討する必要があります。

デバイスの初期化と登録に関する考慮事項		
	個人所有デバイス	**企業所有デバイス**
所有権	従業員 (一部例外あり)	企業
デバイスの初期化 Out-of-the-Box エクスペリエンス (OOBE)、つまりデバイスの初回起動時に、従業員はデバイスにクラウド ID を追加することを求められます。	デバイス上での主な ID は、個人 ID です。個人所有デバイスの起動プロセスは、Microsoft アカウント (MSA) で行います。これには電子メール アドレスを使用します。	デバイス上での主な ID は、組織 ID です。企業所有デバイスの初期化は、組織アカウント (account@corporatedomain.ext) で行います。 企業アカウントを使用したデバイスの初期化は、Windows 10 独自の機能です。現在、この機能を提供しているモバイル プラットフォームは他にはありません。既定のオプションでは、Azure Active Directory の組織 ID を使用します。 OOBE 中にアカウントの設定をスキップすると、ローカル アカウントが作成されます。後からクラウド アカウントを追加するには、MSA を追加する必要があります。その場合、このデバイスは個人所有デバイスの展開シナリオに移行することになります。最初からやり直すには、デバイスをリセットする必要があります。

デバイスの初期化と登録に関する考慮事項		
	個人所有デバイス	**企業所有デバイス**
デバイスの登録 MDM システムにデバイスを登録することで、従業員の生産性を維持したまま、企業データの制御と保護を行うことができます。	デバイスの登録は従業員が開始できます。Azure アカウントをサブ アカウントとして Windows 10 Mobile デバイスに追加することも可能です。MDM システムが Azure AD に登録されている場合、ユーザーが Azure AD のアカウントをサブ アカウントとして追加すると、デバイスが自動的に MDM システムに登録されます (MSA + AAD + MDM)。組織で Azure AD を使用していない場合は、従業員のデバイスは自動的に組織の MDM システムに登録されます (MSA + MDM)。 MDM への登録は、プロビジョニング パッケージを使用して開始する方法もあります。この方式を選択すると、個人所有デバイスを従業員がセルフサービスで簡単に登録できます。現時点では、プロビジョニングで利用できるのは、MDM だけを使用した登録方式 (MSA + MDM) のみです。	MDM に登録するには、まずデバイスを組織の Azure AD インスタンスに参加させます。Azure AD に登録されると、デバイスは自動的に MDM システムに登録されます。これを行うには、MDM システムが Azure AD に登録されている必要があります (AAD + MDM)。

推奨事項

マイクロソフトでは、企業所有デバイスのシナリオ (AAD + MDM) でも、個人所有デバイスのシナリオ (MSA + AAD + MDM) でも、Azure AD への登録と MDM への自動登録を推奨しています。

ID 管理

対象: 企業所有デバイスおよび個人所有デバイス

従業員がデバイスの初期化に使用できるアカウントは 1 つだけです。そのため、最初に有効化するアカウントを組織で管理する必要があります。選択したアカウントによってデバイスの管理者が決まるため、企業の管理機能にも影響が生じます。

メモ

OOBE 中に、デバイスにアカウントを追加する必要があるのはなぜでしょうか。Windows 10 Mobile を搭載したデバイス上でユーザー アカウントを使用すれば、さまざまな既定のクラウド サービスにアクセスできるため、1 台のスマートフォンできわめて高い生産性とエンターテイメント性が発揮されます。また、アプリをダウンロードできるストア、音楽とエンターテイメントを提供する Groove、ゲームを配信する Xbox などのサービスが提供されており、MSA と Azure AD のどちらのアカウントでも、これらのサービスにアクセスすることができます。

次の表では、個人所有デバイスと企業所有デバイスの各シナリオに関して、ID の選択がデバイス管理の特性に及ぼす影響を示しています。

ID を選択する際にデバイス管理に関して考慮すべき点		
	個人 ID	**組織 ID**
デバイス上の最初のアカウント	Microsoft アカウント	Azure AD アカウント
登録のしやすさ	従業員が Microsoft アカウントを使用してデバイスをアクティブ化した場合、次に Azure AD アカウント (組織の ID) を使用して Azure AD にデバイスを登録すると共に、組織の MDM ソリューションにデバイスを登録します (MSA + AAD + MDM)。	従業員が Azure AD アカウントを使用して Azure AD にデバイスを登録した場合、デバイスは自動的に組織の MDM ソリューションに登録されます (AAD + MDM: Azure AD Premium が必要)。
資格情報の管理	従業員は Microsoft アカウントの資格情報でデバイスにサインインします。 Azure AD の資格情報ではデバイスにサインインできません。Microsoft アカウントにより最初のアクティブ化を行った後に資格情報を追加した場合でも不可能です。	従業員は Azure AD の資格情報を使用してデバイスにサインインします。 IT 担当者は、MSA や Google アカウントなど、個人 ID の追加をブロックすることができます。IT 担当者はすべてのデバイスのアクセス ポリシーを自由に制御できます。
デバイスでの個人 ID の使用をブロック	×	○
複数の Windows デバイス間でのユーザー設定とデータのローミング	ユーザーとアプリの設定は、同一の個人 ID を使用してアクティブ化したすべてのデバイス間で OneDrive を介してローミングすることができます。	デバイスを MSA でアクティブ化した場合は、Azure AD アカウントを追加すれば、ユーザーとアプリの設定をローミングできます。Azure AD に参加済みのデバイスに MSA を追加した場合は、これに該当しません。マイクロソフトでは現在、今後のリリースの参考とするべく、エンタープライズ向けのローミングについて調査を進めています。

ID を選択する際にデバイス管理に関して考慮すべき点		
	個人 ID	**組織 ID**
制御レベル	組織は、利用可能なほとんどの制限ポリシーをデバイスに適用できます。また Microsoft アカウントを無効化することも可能です。組織の MDM ソリューションへの登録を解除するかデバイスをリセットすることで、デバイスのフル コントロールをユーザーに渡さないようにできます。法的制限が適用される場合があります。詳細については、自社の法務部門にお問い合わせください。	組織は、企業の基準と法令遵守規定に従って、制御ポリシーをデバイスに自由に適用することができます。また、ユーザーによるデバイスの登録解除を禁止することもできます。
情報保護	企業のアプリとデータの保護および保存に関するポリシーをデバイスに適用して、知的財産の漏えいを防止しつつ、アプリやゲームのダウンロードとインストールなどのプライベートな操作については、従業員にフル コントロールを許可することができます。	企業は、デバイスの個人利用をブロックできます。組織 ID を使用してデバイスを初期化することで、デバイスを完全に制御し、カスタマイズを防止できます。
アプリの購入	従業員は個人のクレジット カードを使用してストアからアプリを購入してインストールすることができます。	従業員はビジネス向けストアからアプリをインストールできます。ただし、MSA を追加しないと、ストアからのアプリのインストールや購入はできません。

メモ

Windows as a Service (英語) に関連して、MDM 機能の差別化方針は今後変更される予定です。

インフラストラクチャの選択

対象: 企業所有デバイスおよび個人所有デバイス

MDM システムは、個人向けと企業向けの両方の展開シナリオで、Windows 10 Mobile デバイスの展開と管理に欠かせないインフラストラクチャです。ID プロバイダーとして Azure AD Premium のサブスクリプションを利用することをお勧めします。一部の機能ではこのサブスクリプションの利用が必須となっています。Windows 10 Mobile では、完全にクラウド ベースのインフラストラクチャを構築することも、Azure AD の ID 管理機能とオンプレミスの管理システムを組み合わせてデバイスを管理するハイブリッド インフラストラクチャを実現することも可能です。また、

マイクロソフトでは現在、Configuration Manager を使用して Windows 10 Mobile デバイスを管理する完全なオンプレミス ソリューションもサポートしています。

Azure Active Directory

Azure AD は、ID とアクセスの管理機能を提供するクラウド ベースのディレクトリ サービスです。既存のオンプレミス ディレクトリに統合して、ハイブリッドの ID 管理ソリューションを構築できます。Microsoft Office 365 や Intune を利用している組織では、既に Azure AD を使用しています。Azure AD には、Free、Basic、Premium の 3 つのエディションがあります (「Azure Active Directory のエディション」を参照)。どのエディションも Azure AD へのデバイス登録をサポートしていますが、MDM 自動登録と、デバイスの状態に基づく条件付きアクセスを有効にするには、Premium エディションが必要です。

モバイル デバイス管理

Microsoft Intune は、社外のデバイスを管理するクラウド ベースの MDM システムで、Enterprise Mobility Suite の一部として提供されます。Office 365 と同様に、Intune は ID 管理に Azure AD を使用しているため、従業員は Office 365 へのサインインに使用する資格情報で Intune にデバイスを登録することができます。包括的な MDM ソリューションを実現するために、Intune は iOS や Android などといった他のオペレーティング システムを搭載したデバイスもサポートしています。

Intune を Configuration Manager と統合すると、単一のコンソールから、クラウドとオンプレミスのすべてのデバイス (モバイルおよび PC) を一元管理できます。詳細については、「Configuration Manager と Microsoft Intune を使用してモバイル デバイスを管理する」を参照してください。スタンドアロンの Intune をインストールするか Intune と System Center Configuration Manager を統合するのかを判断する方法については、「Intune をスタンドアロンで使用するか、Intune を System Center Configuration Manager と統合するかを選択する」を参照してください。

多くの MDM システムが Windows 10 をサポートしています。また、ほとんどのシステムが個人所有デバイスと企業所有デバイスの両方のシナリオをサポートしています。現在、Windows 10 Mobile をサポートしている MDM は、AirWatch、Citrix、Silverback (Matrix42) (英語)、MobileIron、SAP、SOTI (英語)、MAAS360 (IBM)、Sophos、Symantec、Good Technologies (BlackBerry) などのベンダーから提供されています。業界をリードするほとんどの MDM ベンダーは、既に Azure AD との統合もサポートしています。Azure AD をサポートしている MDM ベンダーは、Azure Marketplace で確認できます。Azure AD を使用していない場合、ユーザーが企業のアカウントを使用してデバイスを MDM に登録するには、OOBE で MSA を使用する必要があります。

メモ

本ガイドでは扱いませんが、全機能を備えた MDM システムを使用する代わりに、Exchange ActiveSync (EAS) を使用してモバイル デバイスを管理することもできます。EAS は、Microsoft Exchange Server 2010 以降および Office 365 で使用できます。

また、マイクロソフトではこのほど、Intune を利用した MDM 機能を Office 365 に追加しました。Office 365 の MDM では、Windows 10 Mobile デバイス、iOS デバイス、Android デバイスなど、モバイル デバイスのみがサポートされます。Office 365 の MDM では、デバイスをリモートでワイプする機能、デバイスから Exchange Server の電子メールへのアクセスをブロックする機能、デバイス ポリシー (パスコードの要件など) を構成する機能といった、Intune の管理機能の一部を提供しています。Office 365 の MDM 機能の詳細については、「Mobile Device Management (MDM) for Office 365 の概要」を参照してください。

クラウド サービス

Windows 10 Mobile を搭載したモバイル デバイスでは、ユーザー通知の提供と利用統計情報 (使用状況に関するデータ) の収集を行うクラウド サービスに簡単に接続できます。組織は、Windows 10 Mobile を通じてデバイスによるクラウド サービスの使用方法を管理できます。

Windows プッシュ通知サービス

サード パーティのソフトウェア開発者は、Windows プッシュ通知サービスを使用して、トースト更新、タイル更新、バッジ更新、直接更新を自社のクラウド サービスから送信できます。このしくみにより、更新情報を効率的かつ確実にユーザーへと配信することができます。

ただし、プッシュ通知はバッテリー残量に影響することがあるため、Windows 10 Mobile ではバッテリー節約機能により、持続時間を延長できるようにバックグラウンド アクティビティが制限されます。ユーザーは、バッテリー残量が指定のしきい値を下回ったときに機能が自動的にオンになるように、バッテリー節約機能を設定することができます。Windows 10 Mobile では、バッテリー節約機能がオンに設定されていると、プッシュ通知の受信が無効になります。

また、この動作には例外があります。Windows 10 Mobile では、バッテリー節約機能の設定 (設定アプリ内) の **[常に許可]** リストにアプリを追加すると、バッテリー節約機能がオンになっている場合でも、そのアプリのプッシュ通知を受信することができます。

ユーザーはこのリストを手動で設定できます。また、IT 担当者が MDM システムを使用して、Windows 10 Mobile のバッテリー節約機能の URI スキーム (**ms-settings:batterysaver-settings**) を設定することもできます。

> **メモ**
>
> Windows 10 Mobile の正常性構成証明の詳細については、「Windows 10 Mobile セキュリティ ガイド」を参照してください。

Windows Update for Business

Windows Update for Business は、IT 管理者に Windows Update を中心とした管理機能を追加で提供することを目的としたものです。デバイスのグループに更新プログラムを展開する機能、更新プログラムをインストールするメンテナンス期間を定義する機能などが含まれます。詳細については、「管理」を参照してください。

ビジネス向け Windows ストア

IT 管理者は、ビジネス向け Windows ストアから Windows 10 デバイス用のアプリを検索、入手、管理、および配布することができます。社内用の基幹業務 (LOB) アプリだけでなく、市販のサード パーティ製のアプリも利用できます。詳細については、「アプリ」を参照してください。

構成

MDM 管理者は、MDM システムに登録された個人所有デバイスと企業所有デバイスに対して、ポリシー設定を定義して実装することができます。使用する構成設定は展開シナリオにより異なります。企業所有デバイスのシナリオでは、IT 担当者が制御できる範囲を最大限に拡大することができます。

メモ

本ガイドでは、IT プロフェッショナル向けに、Windows 10 Mobile OS で利用できる管理オプションを紹介しています。これらのポリシーを有効にする方法については、MDM ベンダーの MDM システムに関するドキュメントをご確認ください。

MDM システムによっては、本ガイドで説明した設定の一部をサポートしていない場合があります。OMA-URI の XML ファイルを使用したカスタム ポリシーをサポートしているものもあります。Microsoft Intune のカスタム ポリシーのサポート状況を参照してください。命名規則についても MDM ベンダー間で異なる場合があります。

アカウント プロファイル

対象: 企業所有デバイス

企業所有デバイスで使用可能なアカウントを従業員に必ず使用させることは、データの漏えいを防止してプライバシーを保護するうえで重要です。デバイスで使用可能なアカウントを組織側が 1 つに制限することで、データ漏えいのリスクが低減されます。ただしその場合も、個人の Microsoft アカウントやその他のコンシューマー向けの電子メール アカウントの追加を従業員に許可することは可能です。

設定	説明
Microsoft アカウントを許可する	Microsoft アカウントをデバイスに追加して、Windows ストア、Xbox、Groove でのアプリ購入時など、クラウド サービスで認証を行う際にこのアカウントを使用することをユーザーに許可するかどうかを指定します。
Allow Adding Non-Microsoft Accounts (Microsoft アカウント以外の追加を許可する)	Microsoft アカウント以外の電子メール アカウントの追加をユーザーに許可するかどうかを指定します。

電子メール アカウント

対象: 企業所有デバイスおよび個人所有デバイス

電子メールとそれに関連付けられている予定表および連絡先は、ユーザーがスマートフォンでアクセスする主要なアプリです。これらのアプリを適切に構成することが、モバイル プログラムを成功に導く鍵です。企業所有デバイスと個人所有デバイスの展開シナリオのどちらでも、これらのアプリの電子メール アカウント設定は登録直後に展開されます。自社の MDM システムを使用して、企業電子メール アカウント プロファイルの定義、デバイスへの展開、受信トレイ ポリシーの管理を行うことができます。

ほとんどの企業の電子メール システムで、Exchange ActiveSync (EAS) が利用されています。次の表で、定義可能な EAS の電子メール プロファイルの属性とポリシーについて説明します。

設定	説明
電子メール アドレス	EAS アカウントに関連付けられている電子メール アドレス。
ドメイン (オプション)	Exchange Server インスタンスのドメイン名。
アカウント名	デバイスで使用する電子メール アカウントの名前。デバイスの電子メール タイルに表示されます。
パスワード	電子メール アカウントのパスワード。
サーバー名	電子メール アカウントが使用するサーバーの名前。
ユーザー名	電子メール アカウントを使用するユーザーの名前。
予定表の最大範囲のフィルター	デバイスと同期する予定表アイテムの最大範囲 (過去 7 日間以内の予定表アイテムを同期するなど)。
Logging (ログ)	診断ログの記録のレベル。
Mail Body Type (電子メール本文の種類)	電子メール本文の形式の種類 (テキスト、HTML、または Multipurpose Internet Mail Extensions)。
Mail HTML Truncation (電子メール HTML の切り捨て)	デバイスに同期される HTML 形式の電子メール メッセージの最大サイズ (このサイズを超える HTML 形式の電子メール メッセージを自動的に切り捨て)。
Mail Plain Text Truncation (電子メールのプレーン テキストの切り捨て)	デバイスに同期されるテキスト形式の電子メール メッセージの最大サイズ (このサイズを超えるテキスト形式の電子メール メッセージを自動的に切り捨て)。
Schedule (スケジュール)	Exchange Server とデバイスの間で電子メールを同期するスケジュール。
Use SSL (SSL を使用する)	同期するときに Secure Sockets Layer (SSL) が必要かどうかを指定します。
電子メールの最大範囲フィルター	デバイスと同期するメッセージの最大範囲 (過去 7 日間以内のメッセージを同期するなど)。
Content Types (コンテンツの種類)	同期するコンテンツの種類 (電子メール、連絡先、予定表、タスク アイテムなど)。現時点で Outlook はデバイス上でのタスク ビューをサポートしていません。

メモ

EAS の電子メール プロファイルの設定の詳細については、「ActiveSync CSP (英語)」を参照してください。

簡易メール転送プロトコル (SMTP) の電子メール アカウントについても、MDM システムで設定できます。次の表に、定義可能な設定をまとめます。

設定	説明
ユーザー ログオン名	電子メール アカウントのユーザー ログオン名。
Outgoing authentication required (送信認証が必要)	送信サーバーでの認証を必須にするかどうかを指定します。
パスワード	**[ユーザー ログオン名]** フィールドのアカウントのパスワード。
ドメイン	**[ユーザー ログオン名]** フィールドのアカウントのドメイン名。
Days to download (ダウンロード対象範囲の日数)	サーバーからダウンロードする電子メールの量 (日数単位)。
受信サーバー	受信サーバー名とポート名。値の形式は *server_name:port_number* (ポート番号はオプション)。
Send and receive schedule (送受信スケジュール)	電子メールの送受信を更新する期間 (分単位)。
IMAP4 maximum attachment size (IMAP4 添付ファイル最大サイズ)	インターネット メッセージ アクセス プロトコル バージョン 4 (IMAP4) アカウントのメール添付ファイルの最大サイズ。
Send mail display name (送信メール表示名)	送信する電子メールに表示される送信者の名前。
送信サーバー	送信サーバー名とポート名。値の形式は *server_name:port_number* (ポート番号はオプション)。
返信アドレス	ユーザーの返信用電子メール アドレス。
Email service name (電子メール サービス名)	電子メール サービスの名前。
Email service type (電子メール サービスの種類)	電子メール サービスの種類 (POP3、IMAP4 など)。
受信メッセージの最大サイズ	受信メール サーバーから受信するメッセージの最大サイズ (バイト単位。このサイズを超えるメッセージを最大サイズで切り捨て)。
メッセージの削除アクション	サーバー上でメッセージを削除する方法 (完全に削除するか、またはごみ箱フォルダーに送るか)。
Use cellular only (携帯ネットワークのみを使用)	アカウントで、Wi-Fi 接続を使用せずに、携帯ネットワーク接続だけを使用するかどうかを指定します。

設定	説明
Content types to synchronize (同期するコンテンツの種類)	同期対象のコンテンツの種類 (メール メッセージ、連絡先、予定表アイテムなど)。
Content synchronization server (コンテンツ同期サーバー)	コンテンツ同期サーバーの名前 (メール サーバーと異なる場合)。
Calendar synchronization server (予定表同期サーバー)	予定表同期サーバーの名前 (メール サーバーと異なる場合)。
Contact server requires SSL (連絡先サーバーで SSL を必須にする)	連絡先サーバーで SSL 接続を必須にするかどうかを指定します。
Calendar server requires SSL (カレンダー サーバーで SSL を必須にする)	カレンダー サーバーで SSL 接続を必須にするかどうかを指定します。
Contact items synchronization schedule (連絡先アイテム同期スケジュール)	連絡先アイテムの同期スケジュール。
Calendar items synchronization schedule (予定表アイテム同期スケジュール)	予定表アイテムの同期スケジュール。
Alternative SMTP email account (代替 SMTP 電子メール アカウント)	ユーザーの代替簡易メール転送プロトコル (SMTP) 電子メール アカウントと関連付けられている表示名。
Alternate SMTP domain name (代替 SMTP ドメイン名)	ユーザーの代替 SMTP 電子メール アカウントのドメイン名。
Alternate SMTP account enabled (代替 SMTP アカウントを有効化)	ユーザーの代替 SMTP アカウントを有効にするかどうかを指定します。
Alternate SMTP password (代替 SMTP パスワード)	ユーザーの代替 SMTP アカウントのパスワード。
Incoming and outgoing servers require SSL (受信サーバーと送信サーバーで SSL を必須にする)	受信サーバーと送信サーバーで SSL を使用するかどうかを指定するプロパティのグループ。

メモ

SMTP の電子メール プロファイルの設定の詳細については、「EMAIL2 CSP (英語)」を参照してください。現時点で Microsoft Intune は SMTP の電子メール プロファイルの作成をサポートしていません。

デバイス ロック制限

対象: 企業所有デバイスおよび個人所有デバイス

一般的に、企業情報が格納されているデバイスは、使用していないときにはパスコードで保護します。マイクロソフトではベスト プラクティスとして、Windows 10 Mobile のデバイス ロック ポリシーを実装してアプリとデータの安全性を確保することをお勧めしています。デバイスのロックには、複雑なパスワードや数字 PIN を使用できます。Windows 10 で導入された Windows Hello では、PIN、コンパニオン デバイス (Microsoft Band など)、または生体認証を使用して ID を検証し、Windows 10 Mobile デバイスのロックを解除することができます。

メモ

初回リリース時の Windows 10 には、Microsoft Passport と Windows Hello が搭載され、これらが連携することで多要素認証を提供していました。マイクロソフトでは、展開方法を簡素化してサポート性を高めるために、2 つのテクノロジを Windows Hello の名称で 1 つのソリューションに統合しました。既にこれらのテクノロジを展開している場合、機能面での変更はありません。Windows Hello をまだ試したことがないお客様にとっては、ポリシー、ドキュメント、セマンティクスがシンプルになったことで、より展開しやすくなっています。

Windows Hello で生体認証を使用するには、指紋リーダー、照明付き赤外線センサー、その他の生体認証センサーを含む、専用のハードウェアが必要です。Windows Hello の資格情報をハードウェア ベースで保護するには、TPM 1.2 以上が必要です。TPM が存在しない、または構成されていない場合、資格情報およびキーの保護はソフトウェア ベースで行われます。

コンパニオン デバイスは、Bluetooth で Windows 10 PC とペアリングする必要があります。Windows Hello の資格情報のローミングに対応した Windows Hello コンパニオン デバイスを使用するには、Windows 10 PC の Pro または Enterprise エディションにサインインする必要があります。

次の表に、デバイス ロック制限の設定で使用可能な Windows 10 Mobile の MDM の設定を示します。これらのポリシーの大部分は、Windows Phone 7 以降の ActiveSync および MDM でも提供されていたものであり、Windows 10 Mobile にも継承されています。個人所有デバイスの展開シナリオで Windows 10 デバイスを展開する場合は、次の設定が適用されます。

設定	説明
Device Password Enabled (デバイス パスワードを有効にする)	ユーザーにデバイス ロック パスワードの使用を義務付けるかどうかを指定します。
Allow Simple Device Password (単純なデバイス パスワードを許可する)	ユーザーが単純なパスワード (*1111* や *1234* など) を使用できるようにするかどうかを指定します。

設定	説明
Alphanumeric Device Password Required (英数字のデバイス パスワードを必須にする)	ユーザーに英数字のパスワードの使用を義務付けるかどうかを指定します。 設定した場合、複雑なパスワードの入力に使用するフル キーボードがデバイスに表示されます。設定されていない場合、ユーザーはキーボードで数字 PIN を入力できます。
Min Device Password Complex Characters (デバイス パスワード内の複雑な文字の最小数)	強固なパスワードの作成に必要な、パスワード内の要素の種類 (大文字、小文字、数字、または句読点文字) の数。
デバイス パスワードの有効期限	パスワードの有効期限が切れるまでの日数 (生体認証データは期限切れにはなりません)。
Device Password History (デバイス パスワードの履歴)	Windows 10 Mobile のパスワード履歴に保存するパスワードの数 (履歴に保存されているパスワードを再利用して新しいパスワードを作成することはできません)。
Min Device Password Length (デバイス パスワードの最小の長さ)	新しいパスワードの作成に必要な最小文字数。
Max Inactivity Time Device Lock (デバイス ロックまでの無操作時間)	デバイスがロックされてロック解除のためにパスワードの入力が必要になるまでの無操作時間 (分単位)。
Allow Idle Return Without Password (パスワードなしでアイドル状態から復帰することを許可する)	無操作時間が経過する前にデバイスがスリープ状態から復帰したときに、ユーザーに再認証することを求めるかどうかを指定します。
Max Device Password Failed Attempts (許容されるデバイス パスワード入力失敗回数)	デバイスがワイプされるまでに許容される認証の失敗回数 (値を 0 にするとデバイスのワイプ機能が無効化されます)。
Screen Timeout While Locked (ロック中のスクリーン タイムアウト)	ロック画面のタイムアウトまでの時間 (分単位。このポリシーはデバイスの電源管理に影響します)。
Allow Screen Timeout While Locked User Configuration (ロック中のスクリーン タイムアウトのユーザー構成を許可する)	デバイスのロック画面表示中のスクリーン タイムアウトをユーザーが手動で構成できるようにするかどうかを指定します (この設定を無効にすると、Windows 10 Mobile は **[Screen Timeout While Locked (ロック中のスクリーン タイムアウト)]** の設定を無視します)。

Windows Hello に関連する設定は、企業所有デバイスのシナリオでデバイスを展開する場合に重要性の高いデバイス ロック設定です。

マイクロソフトでは、すべてのユーザーに対して、Azure AD への参加時に数字のパスコードを作成することを要件としています。このポリシーは、既定ではユーザーに 4 桁のパスコードを選択することを求めていますが、AAD に登録された MDM システムを使用すれば、組織で求められるレベルの複雑なパスコードを要件とするようにこの設定を構成できます。Azure AD と MDM への自動登録機能を使用している場合、これらのポリシー設定はデバイス登録中に自動的に適用されます。

次の表で、Windows Hello を使用している企業所有デバイスに定義可能な設定について説明します。

設定	説明
Windows Hello を使用	Windows にサインインする方法として Windows Hello を使用することを許可または禁止します。
Require a security device (セキュリティ デバイスを必須にする)	Passport for Work でトラステッド プラットフォーム モジュール (TPM) を必須にします。設定した場合、使用可能な TPM 搭載のデバイスだけが Windows Hello の ID をプロビジョニングできます。Windows Phone 8.0 以降のすべてのデバイスで TPM の搭載が必須になります。
PIN の最小文字数	PIN に必要な最小文字数を設定します。規定値は 4 です (設定可能な最小の値)。
PIN の最大文字数	PIN に許可する最大文字数を設定します。規定値は 127 です (設定可能な最大の値)。
PIN requirements for uppercase letters (大文字に関する PIN の要件)	PIN に大文字を使用することを許可、要求、または禁止するかどうかを設定します。
PIN requirements for lowercase letters (小文字に関する PIN の要件)	PIN に小文字を使用することを許可、要求、または禁止するかどうかを設定します。
PIN requirements for special characters (特殊文字に関する PIN の要件)	PIN に特殊文字を使用することを許可、要求、または禁止するかどうかを設定します。
PIN requirements for digits (数字に関する PIN の要件)	PIN に数字を使用することを許可、要求、または禁止するかどうかを設定します。
PIN 履歴	PIN を再利用できないようにするためにユーザー アカウントに関連付ける過去の PIN の数 (0 ～ 50) を指定します。このポリシーを 0 に設定すると、以前の PIN の記憶が必須でなくなります。
PIN の有効期限	PIN を使用できる期間 (0 ～ 730 日間) を指定します。この期間を過ぎると、システムがユーザーに変更するよう求めます。
Using Remote Passport (リモート パスワードを使用)	Windows Hello コンパニオン デバイスとしてデスクトップ認証に利用する、登録済みのポータブル デバイスの使用を有効または無効にします。Azure AD に参加しているデスクトップ PC と、PIN が設定されているコンパニオン デバイスが必要です。

設定	説明
Using biometrics (生体認証を使用)	PIN の代わりとして生体認証ジェスチャ (顔や指紋など) を使用することを有効または無効にします。ユーザーは、生体認証ジェスチャを構成した場合も、認証が失敗する事態に備え、PIN を構成する必要があります。
Anti-spoofing for facial recognition (顔認識のスプーフィング対策)	顔認識の拡張スプーフィング対策を有効または無効にします (サポートしているデバイスの場合)。

メモ

一部の設定、特にパスコードの長さ、履歴、有効期間、複雑さなどの設定は、お互いに非常によく似ています。複数の場所でポリシーを設定した場合、両方のポリシーが適用され、最も強力なポリシーが保持されます。詳細については、「PassportForWork CSP (英語)」、「DeviceLock CSP (英語)」(Windows Phone 8.1 向け)、および「Policy CSP (英語)」を参照してください。

設定変更の防止

対象: 企業所有デバイス

従業員には通常、企業所有デバイスで一部の個人用設定を変更することが許可されますが、ロックダウンが必要になる場合もあります。従業員は、設定アプレットからスマートフォンの一部の設定をインタラクティブに調整できます。MDM を使用すれば、ユーザーが変更できる項目を制限できます。

設定	説明
Allow Your Account (アカウントの変更を許可する)	**[設定]** の **[メールとアカウント]** パネルで、ユーザーがアカウント構成を変更できるようにするかどうかを指定します。
Allow VPN (VPN の変更を許可する)	ユーザーによる VPN 設定の変更を許可します。
Allow Data Sense (データセンサーの変更を許可する)	ユーザーによるデータセンサーの設定の変更を許可します。
Allow Date Time (日付/時刻の変更を許可する)	ユーザーによる日付と時刻の設定の変更を許可します。
Allow Edit Device Name (デバイス名の編集を許可する)	ユーザーによるデバイス名の変更を許可します。
Allow Speech Model Update (音声モデルの更新を許可する)	デバイスで音声認識と音声合成モデルの更新を (正確性とパフォーマンスの向上のために) 受信するかどうかを指定します。

ハードウェアの制限

対象: 企業所有デバイス

Windows 10 Mobile には、カメラ、グローバル ポジショニング システム (GPS)、センサー、マイク、スピーカー、近距離無線通信 (NFC)、メモリ カード スロット、USB インターフェイス、Bluetooth インターフェイス、セル方式無線電話、Wi-Fi など、広く普及しているハードウェア機能をはじめとする最先端のテクノロジが搭載されています。ハードウェア制限機能を使用すれば、これらの機能を使用できるかどうかを制御することができます。次の表に、Windows 10 Mobile でサポートされる、ハードウェア制限の構成に関する MDM の設定を示します。

メモ

これらのハードウェア制限の中には、接続を提供し、データ保護を支援するものもあります。

設定	説明
NFC を使用する	NFC 無線通信を有効にするかどうかを指定します。
USB 接続を許可する	USB 接続を有効にするかどうかを指定します (USB 充電には影響しません)。
Bluetooth を許可する	ユーザーがデバイス上で Bluetooth 無線通信を有効にして使用できるようにするかどうかを指定します。
Bluetooth 広告を許可する	デバイスを Bluetooth 広告の配信元として動作させて、他のデバイスから検出可能にするかどうかを指定します。
Bluetooth 検出可能モードを許可する	デバイスから他のデバイス (ヘッドセットなど) を検出できるようにするかどうかを指定します。
Allow Bluetooth pre-pairing (Bluetooth の事前ペアリングを許可する)	バンドルされた特定の Bluetooth 周辺機器をホスト デバイスに自動的にペアリングすることを許可するかどうかを指定します。
Bluetooth Services Allowed List (Bluetooth サービス許可リスト)	デバイスから接続できる Bluetooth サービスとプロファイルのリスト。
Set Bluetooth Local Device Name (Bluetooth ローカル デバイス名を設定する)	Bluetooth ローカル デバイス名。
カメラを使用する	カメラを有効にするかどうかを指定します。
Allow Storage Card (メモリ カードを使用する)	メモリ カード スロットを有効にするかどうかを指定します。
音声録音を許可する	マイクを使用して音声録音を作成できるようにするかどうかを指定します。

設定	説明
Allow Location (位置情報を使用する)	デバイスの GPS センサーやその他の位置を特定するテクノロジを使用可能にして、アプリケーションで位置情報を使用できるようにするかどうかを指定します。

証明書

対象: 個人所有デバイスと企業所有デバイス

証明書を使用することで、アカウント認証、Wi-Fi 認証、VPN 暗号化、および Web コンテンツの SSL 暗号化を実施し、セキュリティを高めることができます。ユーザーがデバイス上で証明書を手動で管理することもできますが、MDM システムを使用して、登録から更新、失効まで、ライフサイクル全体にわたって証明書を管理することをお勧めします。

証明書を手動でインストールするには、Microsoft Edge の Web サイトに登録します。また、電子メールで直接送信することもでき、特にテストを行うときに便利です。

SCEP と MDM システムを使用すると、証明書の管理が完全に透過的に処理され、ユーザーの操作も不要になるため、ユーザーの生産性を高めつつ、電話によるサポートの件数を減らすことができます。MDM システムでは、デバイスの登録後、これらの証明書をデバイスの証明書ストアに自動的に展開することができます (ただし、MDM システムが Simple Certificate Enrollment Protocol (SCEP) または Personal Information Exchange (PFX) をサポートしている場合に限ります)。また MDM サーバーでは、SCEP で登録したクライアント証明書 (ユーザーがインストールした証明書を含む) の照会と削除が可能です。または、現在の証明書が期限切れになる前に、新規登録リクエストをトリガーすることもできます。

次の表に、Windows 10 Mobile の MDM クライアントで利用できる SCEP 関連の設定を示します。

メモ

MDM による証明書管理の詳細については、「ClientCertificateInstall CSP (英語)」と「Windows 10 Mobile へのデジタル証明書のインストール」を参照してください。

SCEP による証明書の登録に関する設定

設定	説明
Certificate enrollment server URLs (証明書登録サーバーの URL)	証明書登録サーバーを指定します (複数のサーバー URL を指定する場合は、セミコロン (;) で URL を区切ります)。
SCEP enrollment challenge (SCEP 登録チャレンジ)	Base64 でエンコードされた SCEP 登録チャレンジ。
Extended key use object identifiers (拡張キー使用法のオブジェクト識別子)	拡張キー使用法のオブジェクト識別子 (OID)。
キー使用法	証明書のキー使用法のビット (10 進数形式)。

設定	説明
サブジェクト名	証明書のサブジェクト名。
Private key storage (秘密キーの格納場所)	秘密キーの格納場所 (トラステッド プラットフォーム モジュール (TPM)、ソフトウェア キー格納プロバイダー (KSP)、または Microsoft Passport の KSP)。
Pending retry delay (保留中の再試行の待ち時間)	SCEP サーバーが保留中ステータスを送信したときに再試行するまでに待機する時間の長さ。
Pending retry count (保留中の再試行の回数)	SCEP サーバーが保留中ステータスを送信したときにデバイスが再試行する回数。
テンプレート名	証明書のテンプレート名の OID。
Private key length (秘密キーの長さ)	秘密キーの長さ (1,024 ビット、2,048 ビット、または 4,096 ビット。Microsoft Passport でサポートされるキーの長さは 2,048 ビットのみ)。
Certificate hash algorithm (証明書のハッシュ アルゴリズム)	ハッシュ アルゴリズム ファミリ (SHA-1、SHA-2、SHA-3。複数のアルゴリズム ファミリを指定する場合はプラス記号 (+) で区切ります)。
Root CA thumbprint (ルート CA の拇印)	ルート CA の拇印。
サブジェクトの別名	証明書のサブジェクトの別名 (複数のサブジェクトの別名を指定する場合は、セミコロンを使用して区切ります)。
Valid period (有効期間)	証明書が有効と見なされる期間の単位 (日、月、または年)。
Valid period units (有効期間の単位)	証明書が有効と見なされる期間の単位 (この設定は **[Valid period (有効期間)]** の設定と共に使用します。たとえば、この設定が **3**、**[Valid period (有効期間)]** が **年**に指定されている場合、証明書は 3 年間有効です)。
Custom text to show in Microsoft Passport PIN prompt (Microsoft Passport の PIN プロンプトに表示するカスタム テキスト)	証明書の登録中に Microsoft Passport の PIN プロンプトに表示するカスタム テキスト。
拇印	現在の証明書の拇印 (証明書の登録が成功した場合)。

SCEP による証明書の管理に加え、Windows 10 Mobile では PFX 証明書の展開もサポートしています。次の表で、Windows 10 Mobile における PFX 証明書の展開に関する設定を示します。

設定	説明
Private key storage (秘密キーの格納場所)	秘密キーの格納場所 (TPM、ソフトウェア KSP、または Microsoft Passport の KSP)。

設定	説明
Microsoft Passport container name (Microsoft Passport のコンテナー名)	Microsoft Passport が基にしている Azure AD テナントのテナント ID。**[Private key storage (秘密キーの格納場所)]** に **Microsoft Passport KSP** を選択した場合にのみ必要です。
PFX packet (PFX パケット)	エクスポート済みの暗号化された証明書と Binary64 形式のキーを備えた PFX パケット。
PFX packet password (PFX パケットのパスワード)	**[PFX packet (PFX パケット)]** で指定した PFX BLOB を保護するパスワード。
PFX packet password encryption (PFX パケットのパスワードの暗号化)	MDM システムで、PFX 証明書のパスワードを MDM の証明書を使用して暗号化するかどうかを指定します。
PFX private key export (PFX 秘密キーのエクスポート)	PFX 秘密キーをエクスポートできるようにするかどうかを指定します。
拇印	インストールされている PFX 証明書の拇印。

ルート CA 証明書と中間 CA 証明書をユーザーが故意にまたは誤って手動でインストールすることを防ぐには、**[ルート証明書の手動インストールを許可する]** の設定を使用します。

メモ

Windows 10 Mobile デバイスの証明書関連の問題を診断するには、Windows ストアにある無料の証明書アプリを使用してください。この Windows 10 Mobile アプリでは、次の操作を実行できます。

- すべての個人証明書の概要を表示する
- 各証明書の詳細を表示する
- VPN、Wi-Fi、および電子メールの認証に使用されている証明書を表示する
- 有効期限が切れている可能性のある証明書を特定する
- 証明書のパスを検証して、正しい中間証明書とルート CA 証明書を保有していることを確認する
- デバイスの TPM に格納されている証明書キーを表示する

Wi-Fi プロファイル

対象: 企業所有デバイスおよび個人所有デバイス

Wi-Fi は、モバイル デバイスにおいて、携帯データ ネットワーク接続と同じくらい、またはそれ以上に使用されています。ほとんどの企業の Wi-Fi ネットワークでは、ユーザーのアクセスを制限して安全性を確保するために、証明書をはじめとする複雑な情報が必要です。このような高度な Wi-Fi 情報は、一般的なユーザーが構成するのは困難ですが、MDM システムを使用すれば、ユーザーが操作しなくても、このような Wi-Fi プロファイルを完全に構成することができます。

MDM システムでは複数の Wi-Fi プロファイルを作成できます。次の表に、管理者が構成できる Windows 10 Mobile の Wi-Fi 接続プロファイルに関する設定を示します。

設定	説明
SSID	Wi-Fi ネットワークのサービス セット識別子。大文字と小文字を区別します。
セキュリティの種類	Wi-Fi ネットワークで使用するセキュリティの種類。次の認証の種類のうち、いずれか 1 つを使用できます。 • Open 802.11 • Shared 802.11 • WPA-Enterprise 802.11 • WPA-Personal 802.11 • WPA2-Enterprise 802.11 • WPA2-Personal 802.11
認証の暗号化	認証で使用する暗号化の種類。次の認証の種類のうち、いずれか 1 つを使用できます。 • なし (暗号化なし) • Wired Equivalent Privacy (WEP) • Temporal Key Integrity Protocol (TKIP) • Advanced Encryption Standard (AES)
Extensible Authentication Protocol Transport Layer Security (EAP-TLS)	セキュリティの種類のうち WPA-Enterprise 802.11 と WPA2-Enterprise 802.11 で、EAP-TLS を使用できます。認証には証明書を使用します。
Protected Extensible Authentication Protocol with Microsoft Challenge Handshake Authentication Protocol version 2 (PEAP-MSCHAPv2)	WPA-Enterprise 802.11 と WPA2-Enterprise 802.11 で、PEAP-MSCHAPv2 を使用できます。認証にはユーザー名とパスワードを使用します。
共有キー	WPA-Personal 802.11 と WPA2-Personal 802.11 で、認証に共有キーを使用できます。
プロキシ	Wi-Fi 接続が要求するネットワーク プロキシの構成 (プロキシ サーバーの指定には、完全修飾ドメイン名 (FQDN)、インターネット プロトコル バージョン 4 (IPv4) アドレス、インターネット プロトコル バージョン 6 (IPv6) アドレス、または IPvFuture アドレスを使用)。
Disable Internet connectivity checks (インターネット接続チェックを無効にする)	Wi-Fi 接続でインターネット接続を確認するかどうかを指定します。

設定	説明
Proxy auto-configuration URL (プロキシの自動構成 URL)	プロキシの自動構成ファイルを指定する URL。
Enable Web Proxy Auto-Discovery Protocol (WPAD) (Web Proxy Auto-Discovery Protocol (WPAD) を有効にする)	WPAD を有効にするかどうかを指定します。

また、デバイス全体の Wi-Fi 設定の一部も設定できます。

設定	説明
Allow Auto Connect to Wi-Fi Sense Hotspots (Wi-Fi センサー ホットスポットへの自動接続を許可する)	デバイスで Wi-Fi ネットワークを自動的に検出して接続するかどうかを指定します。
Allow Manual Wi-Fi Configuration (Wi-Fi の手動構成を許可する)	Wi-Fi 設定の手動構成をユーザーに許可するかどうかを指定します。
Wi-Fi を許可	Wi-Fi ハードウェアを有効にするかどうかを指定します。
インターネット共有を許可する	インターネット共有を許可するか禁止するかを指定します。
WLAN Scan Mode (WLAN スキャン モード)	デバイスで Wi-Fi ネットワークをアクティブにスキャンする程度。

メモ

Wi-Fi 接続プロファイルの設定の詳細については、「WiFi CSP (英語)」と「Policy CSP (英語)」を参照してください。

APN プロファイル

対象: 企業所有デバイス

アクセス ポイント名 (APN) は、携帯ネットワーク接続のネットワーク パスを定義するものです。通常は通信事業者と提携し、1 台のデバイスに 1 つの APN のみを定義しますが、企業が複数の通信事業者を利用している場合は、複数の APN を定義できます。

APN で提供される企業ネットワークへのプライベート接続は、同じ通信事業者のネットワークを利用する他の企業が使用することはできません。

MDM システムで APN プロファイルを定義して展開することで、Windows 10 Mobile の携帯ネットワーク接続を構成できます。Windows 10 Mobile を搭載したデバイスに展開できる APN プロファイルは 1 つのみです。次の表に、Windows 10 Mobile でサポートされる APN プロファイルに関する MDM の設定を示します。

設定	説明
APN name (APN 名)	APN の名前。
IP connection type (IP 接続の種類)	IP 接続の種類。次のいずれかの値に設定します。 • IPv4 のみ • IPv6 のみ • IPv4 と IPv6 の併用 • 464XLAT による IPv6 と IPv4 の共存
LTE attached (LTE にアタッチ)	LTE アタッチの一部として APN をアタッチするかどうかを指定します。
APN class ID (APN クラス ID)	APN クラスをモデムに対して定義するグローバル一意識別子。
APN authentication type (APN の認証タイプ)	APN の認証タイプ。次のいずれかの値に設定します。 • なし • 自動 • PAP • CHAP • MSCHAPv2
ユーザー名	**[APN authentication type (APN の認証タイプ)]** でパスワード認証プロトコル (PAP)、CHAP、または MSCHAPv2 を選択した場合のユーザー アカウント。
パスワード	**[ユーザー名]** で指定したユーザー アカウントのパスワード。
Integrated circuit card ID (IC カードの ID)	携帯ネットワーク接続プロファイルに関連付けられている IC カードの ID。
Always on (常時アクセス)	APN が利用できる場合、接続マネージャーが自動的に APN に接続を試みるどうかを指定します。
Connection enabled (接続を有効にする)	APN 接続を有効にするかどうかを指定します。
Allow user control (ユーザーによる制御を許可する)	企業の APN 以外の APN に接続することをユーザーに許可するかどうかを指定します。

設定	説明
ビューを隠す	モバイル デバイス上で企業の APN を確認できるようにするかどうかを指定します。

メモ

APN の設定の詳細については、「EnterpriseAPN CSP (英語)」を参照してください。

プロキシ

対象: 企業所有デバイス

次の表に、Windows 10 Mobile デバイスの接続に関する APN プロキシ設定の管理に使用する設定を示します。

設定	説明
接続名	プロキシが関連付けられている接続名 (構成した接続の APN 名)。
Bypass Local (ローカルのバイパス)	デバイスでローカル ホストにアクセスした場合にプロキシをバイパスするかどうかを指定します。
有効にする	プロキシを有効にするかどうかを指定します。
例外	アクセス時にプロキシをバイパスする外部ホストのリスト (セミコロンで区切ります)。
ユーザー名	プロキシに接続する際に使用するユーザー名。
パスワード	プロキシに接続する際に使用するパスワード。
サーバー	プロキシ サーバーの名前。
Proxy connection type (プロキシ接続の種類)	プロキシ接続の種類。サポートされる種類は Null proxy、HTTP、WAP、SOCKS4 です。
ポート	プロキシ接続のポート番号。

メモ

プロキシ設定の詳細については、「CM_ProxyEntries CSP (英語)」を参照してください。

VPN

対象: 企業所有デバイスおよび個人所有デバイス

多くの企業が、自社のイントラネット上のアプリとリソースへのアクセスを制御するために、VPN を使用しています。Windows 10 Mobile では、ネイティブのプロトコルである Microsoft Point-to-Point トンネリング プロトコル (PPTP)、レイヤー 2 トンネリング プロトコル (L2TP)、およびインターネット キー交換プロトコル バージョン 2 (IKEv2) による VPN だけでなく、SSL VPN 接続もサポートしています。SSL VPN 接続を利用するには、Windows ストアからプラグインをダウンロードする必要があります。また、接続サービスの内容は、利用する VPN ベンダーにより異なります。このプラグインはアプリのように動作し、MDM システムを使用して Windows ストアから直接インストールできます (「アプリの管理」を参照)。

複数の VPN 接続プロファイルを作成し、プロビジョニングを行ってから、Windows 10 Mobile を搭載した管理対象デバイスにそのプロファイルを展開できます。

Windows 10 Mobile のネイティブの VPN プロトコル (IKEv2、PPTP、L2TP など) を使用した VPN プロファイルを作成する場合、次の設定を使用できます。

設定	説明
VPN Servers (VPN サーバー)	VPN プロファイルの VPN サーバー。
Routing policy type (ルーティング ポリシーの種類)	VPN プロファイルで使用するルーティング ポリシーの種類。次のいずれかに設定します。 **分割トンネル。**イントラネット宛てのネットワーク トラフィックのみが VPN 接続を経由します。 **強制トンネル。**すべてのトラフィックが VPN 接続を経由します。
Tunneling protocol type (トンネリング プロトコルの種類)	Windows 10 Mobile ネイティブの VPN プロトコルを使用する VPN プロファイルで使用するトンネリング プロトコル。PPTP、L2TP、IKEv2、または Automatic を指定できます。
ユーザーの認証方法	VPN 接続の認証方法に設定できる値は、**EAP** または **MSChapv2** (IKEv2 ベースの VPN 接続の場合、Windows 10 Mobile では **MSChapv2** はサポートされません)。
コンピューター証明書	IKEv2 ベースの VPN 接続に使用するコンピューター証明書。
EAP configuration (EAP 構成)	証明書認証を使用して VPN ユーザーにシングル サインオン機能を提供するには、拡張認証プロトコル (EAP) の構成 XML ファイルを作成して VPN プロファイルに含める必要があります。
L2tpPsk	L2TP 接続に使用する事前共有キー。
Cryptography Suite (暗号スイート)	IPsec トンネリングに使用する暗号スイート属性の選択を有効にします。

メモ

EAP 構成 XML ファイルを使用してシングル サインオン機能用のプロファイルを作成する場合、Windows 10 PC の rasphone ツールを使用するのが最も簡単です。rasphone.exe を実行すると、構成ウィザードが表示され、必要な手順を行うことができます。EAP 構成 XML BLOB の作成に関する詳しい手順については、「EAP 構成 (英語)」を参照してください。作成される XML BLOB を MDM システムで使用することで、Windows 10 Mobile スマートフォンの VPN プロファイルを作成できます。複数の証明書がデバイス上にある場合、自動的に証明書が選択されるようにフィルター条件を構成することをお勧めします。そうすることで、従業員は VPN を有効にするたびに認証証明書を選択する必要がなくなります。詳細については、こちらの記事 (英語) をご覧ください。PC 用の Windows 10 と Windows 10 Mobile の VPN クライアントは同じです。

VPN 接続に使用する Windows ストア ベースの VPN プラグインでは、次の属性を持つ VPN プラグイン プロファイルを作成できます。

設定	説明
VPN サーバー	VPN サーバーのコンマ区切りリスト。サーバーは、URL、完全修飾ホスト名、または IP アドレスで指定できます。
カスタム構成	プラグイン プロバイダーで要求される SSL-VPN プラグイン用構成情報 (認証情報など) の HTML エンコードされた XML BLOB。
Windows Store VPN plugin family name (Windows ストアの VPN プラグイン ファミリ名)	Windows ストア ベースのプラグインの Windows ストア パッケージ ファミリ名を指定します。

また、各 VPN プロファイルに次の設定を指定することもできます。

設定	説明
アプリ トリガーの一覧	それぞれの VPN プロファイルにアプリ トリガーの一覧を追加できます。この一覧に指定されているアプリは、イントラネット接続の VPN プロファイルを自動的にトリガーします。各種アプリに対応した複数の VPN プロファイルが必要な場合は、ユーザーがアプリを切り替えると、オペレーティング システムによって VPN 接続が自動的に確立されます。同時にアクティブにできる VPN 接続は 1 つだけです。デバイスの VPN 接続が解除された場合は、ユーザー操作不要で自動的に VPN に再接続されます。
Route List (ルートの一覧)	VPN インターフェイスのルーティング テーブルに追加するルートの一覧。分割トンネリングにおいて、VPN サーバー サイトのサブネットの数が、インターフェイスに割り当てられた IP に基づく既定のサブネットよりも多い場合に必要です。
ドメイン名情報の一覧	VPN プロファイル用の名前解決ポリシー テーブル (NRPT) のルール。
Traffic Filter List (トラフィック フィルターの一覧)	ルールのリストを指定します。これらのルールに一致するトラフィックのみが、VPN インターフェイス経由で送信されます。

設定	説明
DNS サフィックス	VPN 接続用の DNS サフィックスのコンマ区切りリスト。このリスト内の DNS サフィックスは、**サフィックス検索一覧**に自動的に追加されます。
プロキシ	**プロキシ サーバー名や自動プロキシ構成 URL** など、VPN 接続に必要な接続後のプロキシのサポート。プロキシ サーバーの設定を自動的に取得するための URL を指定します。
Always on connection (常時接続)	Windows 10 Mobile は VPN 常時接続機能を搭載しています。これにより、ユーザーがサインインしたときに、VPN 接続を自動的に開始することができます。VPN 接続は、ユーザーが手動で切断するまで維持されます。
Remember credentials (資格情報を記憶する)	VPN 接続で資格情報をキャッシュするかどうかを指定します。
Trusted network detection (信頼されたネットワークの検出)	信頼されたネットワークのコンマ区切りリスト。これにより、イントラネットに直接アクセスできる場合 (Wi-Fi) は、VPN 接続が行われなくなります。
Enterprise Data Protection Mode ID (エンタープライズ データ保護モードの ID)	エンタープライズ ID。このフィールド (オプション) を使用すると、Windows Information Protection ポリシーで定義されているアプリで、VPN を自動的にトリガーすることができます。
デバイスのポリシー準拠	デバイスのポリシーに準拠するために、Azure AD ベースの条件付き VPN アクセスを設定して、Kerberos 認証用の VPN 認証証明書とは異なる証明書で SSO を許可するために使用します。
Lock Down VPN profile (ロックダウン VPN プロファイル)	ロックダウン VPN プロファイルの特徴を次に示します。 • 常時接続の VPN プロファイルです。 • 接続が切断されることはありません。 • VPN プロファイルが接続されていない場合、ユーザーはネットワーク接続を利用できません。 • 別の VPN プロファイルを使用したり、修正したりすることはできません。
ProfileXML	お使いの MDM システムでサポートされていない VPN 設定を構成する必要がある場合は、必要なフィールドすべてに適用する VPN プロファイルを定義した XML ファイルを作成できます。

メモ

VPN プロファイルの詳細については、「VPNv2 CSP (英語)」を参照してください。

VPN 接続の管理に関するデバイス全体の設定には、携帯データ ネットワーク経由の VPN 接続を管理できるものがあります。これを使用すると、ローミング関連のコストやデータ プランの料金を削減できます。

設定	説明
Allow VPN (VPN の変更を許可)	ユーザーが VPN の設定を変更できるようにするかどうかを指定します。
携帯データ ネットワーク経由での VPN 接続を許可	ユーザーが携帯データ ネットワーク経由で VPN 接続を確立できるようにするかどうかを指定します。
Allow VPN Over Cellular when Roaming (ローミング中に携帯データ ネットワーク経由での VPN 接続を許可)	ユーザーがローミング中に携帯データ ネットワーク経由で VPN 接続を確立できるようにするかどうかを指定します。

ストレージ管理

対象: 企業所有デバイスおよび個人所有デバイス

デバイスに格納されているアプリとデータを保護することは、デバイスのセキュリティを確保するうえできわめて重要です。アプリとデータを保護する効果的な方法として、内部のデバイス ストレージを暗号化する方法が挙げられます。Windows 10 Mobile のデバイス暗号化は、承認されていないユーザーがデバイスを物理的に所持している場合でも、企業データを不正アクセスから保護するのに役立ちます。

Windows 10 Mobile では、セキュア デジタル (SD) カードにアプリをインストールすることができます。アプリは専用のパーティションにインストールされます。この機能は常に有効であるため、ポリシーを設定して明示的に有効化する必要はありません。

SD カードはデバイスと 1 対 1 でペアリングされます。他のデバイスでは、暗号化されたパーティション内のアプリやデータが表示されません。ただし、SD カード内の暗号化されていないパーティションに格納されているデータ (音楽や写真など) にはアクセスできます。これにより、ユーザーは SD カードを柔軟に使用しながら、その中の機密アプリと機密データを保護することができます。

SD カードの使用を完全に禁止する場合は、**[Allow Storage Card (メモリ カードを使用する)]** の設定を無効にすることも可能です。ストレージを暗号化しない場合、[Restrict app data to the system volume (アプリ データの保存先をシステム ボリュームに制限する)] と [Restrict apps to the system volume (アプリの保存先をシステム ボリュームに制限する)] の設定を使用して、企業のアプリとデータを保護できます。この設定を使用すると、ユーザーはアプリとデータを SD カードにコピーできなくなります。

以下の表に、Windows 10 Mobile で提供される、MDM のストレージ管理に関連する設定を示します。

設定	説明
Allow Storage Card (メモリ カードを使用する)	データの保存にメモリ カードの使用を許可するかどうかを指定します。
Require Device Encryption (デバイスの暗号化を必須にする)	内部のストレージを暗号化するかどうかを指定します (デバイスが暗号化されている場合は、暗号化をオフにするポリシーを使用できません)。

設定	説明
暗号化方法	BitLocker ドライブの暗号化方法と暗号強度を指定します。次のいずれかの値に設定します。 • AES-Cipher Block Chaining (CBC) 128 ビット • AES-CBC 256 ビット • XEX-based tweaked-codebook mode with cipher text stealing (XTS)–AES (XTS-AES) 128 ビット (既定) • XTS-AES 256 ビット
Allow Federal Information Processing Standard (FIPS) algorithm policy (連邦情報処理標準 (FIPS) アルゴリズム ポリシーを許可する)	デバイスで FIPS アルゴリズム ポリシーを許可するか禁止するかを指定します。
SSL 暗号	SSL 接続で許可する暗号化アルゴリズムのリストを指定します。
Restrict app data to the system volume (アプリ データの保存先をシステム ボリュームに制限する)	アプリ データの保存先をシステム ドライブに制限するかどうかを指定します。
Restrict apps to the system volume (アプリの保存先をシステム ボリュームに制限する)	アプリの保存先をシステム ドライブに制限するかどうかを指定します。

アプリ

対象: 企業所有デバイスおよび個人所有デバイス

アプリを活用すると、多くの場合、モバイル デバイスの生産性が高まります。

Windows 10 では、Windows アプリ用向けのユニバーサル Windows プラットフォーム (UWP) を使用して、複数のデバイスでシームレスに動作するアプリを開発することができます。UWP は、Windows 10 を搭載したすべてのデバイス向けにアプリケーション プラットフォームを統合したものであるため、開発したアプリは修正を加えることなく Windows 10 の全エディションで実行できます。開発者の時間とリソースを節約できるため、よりいっそう迅速かつ効率的にモバイル ユーザーにアプリを提供できます。また、このような「一度プログラムを書けばどこでも動く」モデルにより、どのデバイス タイプでも一貫性のある使い慣れたアプリのエクスペリエンスが提供されるため、ユーザーの生産性も高まります。

既存のアプリとの互換性の点では、Windows Phone 8.1 のアプリが Windows 10 Mobile デバイスでも実行できるため、最新プラットフォームに簡単に移行できます。マイクロソフトでは、Windows 10 Mobile の改善点を最大限にご活用いただけるように、アプリを UWP に移行することをお勧めしています。また、既存の Windows Phone 8.1 (Silverlight) と iOS アプリを UWP にすばやく簡単に更新するためのブリッジも既に開発済みです。

さらに、ビジネス向け Windows ストアから UWP アプリの購入とライセンス取得を簡単に行い、Windows ストアやビジネス向け Windows ストアと統合可能な MDM システムを使用して、アプリを従業員のデバイスに展開できるようになりました。アプリをモバイル ワーカーに届けることは非常に重要ですが、その一方で、効率的な方法を使用してアプリを企業のデータ セキュリティ ポリシーに確実に準拠させる必要もあります。

> ユニバーサル Windows アプリの詳細については、「ユニバーサル Windows プラットフォーム (UWP) アプリのガイド」または「クイック スタート チャレンジ: Visual Studio を使用したユニバーサル Windows アプリ (英語)」を参照してください。また、「Windows 10 にアプリを移植する」も併せて参照してください。

ビジネス向け Windows ストア: 適切なアプリの調達

アプリ管理の最初のステップは、ユーザーが必要とするアプリを用意することです。独自のアプリを開発する方法も、Windows ストアからアプリを調達する方法もあります。Windows Phone 8.1 では、Windows ストアからアプリを入手してインストールするために、MSA が必要でした。ビジネス向け Windows ストアでは、企業が Windows ストアを使用して非公開ストアから従業員用のアプリを取得することができます。そのため、Windows 10 デバイスでは MSA が不要になりました。

ビジネス向け Windows ストアは、IT 管理者が Windows 10 デバイス用のアプリを検索、入手、管理、および配布することができる Web ポータルです。

Azure AD の認証済み管理者は、ビジネス向け Windows ストアの機能と設定にアクセスできます。また、ストア マネージャーは、自社専用の非公開のアプリ カテゴリを作成することができます (ビジネス向け Windows ストアに対する Azure AD アカウントのアクセス権の詳細については、こちらのページで確認できます)。企業はビジネス向け Windows ストアから自社で使用するアプリのライセンスを購入して、そのアプリを従業員に提供できます。市販のアプリを利用できるだけでなく、依頼に応じて開発者が**基幹業務** (LOB) アプリをビジネス向け Windows ストアに公開することも可能です。また、ビジネス向け Windows ストアのサブスクリプションを MDM システムと統合できるため、MDM システムでビジネス向け Windows ストアのアプリの配布と管理を実行できます。

ビジネス向け Windows ストアは、オンラインとオフラインの 2 つのライセンス モデルによるアプリ配布に対応しています。

お勧めの方法はオンライン モデル (ストア管理) です。このモデルは個人所有デバイスと企業所有デバイスの両方の展開シナリオに対応しています。オンライン アプリをデバイスにインストールするには、インストール時にインターネット アクセスが必要になります。企業所有デバイスの場合は、従業員が Azure AD アカウントで認証を受けてオンライン アプリをインストールします。個人所有デバイスの場合は、企業がライセンスを保有しているオンライン アプリをインストールできるように、従業員のデバイスを Azure AD に登録する必要があります。

企業所有デバイスのユーザーは、スマートフォンのストア アプリの非公開カタログで、企業がライセンスを保有しているオンライン アプリを確認できます。MDM システムがビジネス向けストアと関連付けられている場合、IT 管理者はユーザーが必要なアプリを見つけてインストールできるように、ストア アプリを MDM システム内のアプリ カタログに表示することができます。また IT 管理者は、従業員に操作させることなく、必要なアプリを従業員のデバイスに直接配信することも可能です。

個人所有デバイスを使用している従業員は、デバイスのストア アプリを使用して、企業がライセンスを保有するアプリをインストールすることができます。ストア アプリで個人用のアプリを購入する場合、Azure AD アカウントか Microsoft アカウントのどちらかを使用します。企業所有デバイスを使用する従業員に 2 つ目の Microsoft アカウント (MSA) の追加を許可することで、デバイス上のストア アプリから個人用のアプリと企業のアプリを 1 つの方法でインストールできるようになります。

ライセンスを保有しているオンライン上のアプリを配布および管理する際に、Windows ストアから MDM システムに転送またはダウンロードする必要がなくなります。企業が保有するアプリを従業員が選択すると、自動的にクラウドからインストールされます。さらに、アプリは新しいバージョンが利用可能になると自動的に更新され、必要に応じて削除することもできます。アプリが MDM システムまたはユーザーによってデバイスから削除されると、ビジネス向け Windows ストアがライセンスを回収するため、別のユーザーや別のデバイスがそのライセンスを利用できます。

アプリをオフラインで配布 (社内で管理) するには、アプリをビジネス向け Windows ストアからダウンロードする必要があります。ダウンロードは、承認された管理者がビジネス向け Windows ストア ポータルから行うことができます。オフライン ライセンス モデルの場合は、Windows ストアによるライセンスの追跡ができないため、アプリの開発者がこのライセンス モデルを許可する必要があります。アプリ開発者が Windows ストアからアプリをダウンロードすることを許可しなかった場合、ユーザーは開発者からファイルを直接入手するか、オンライン ライセンス モデルを使用する必要があります。

オフラインで入手した Windows ストア アプリや LOB アプリを Windows 10 デバイスにインストールする際、IT 管理者は MDM システムを使用できます。MDM システムを使用すると、Windows ストアからダウンロードしたアプリ パッケージを Windows 10 Mobile デバイスに配布できます (**サイドローディング**とも呼ばれます)。オフラインでのアプリ配布に対するサポートは、お使いの MDM システムごとに異なります。詳細については MDM ベンダーのドキュメントを参照してください。アプリの展開プロセスは完全に自動化できるため、ユーザーの操作は不要です。

ビジネス向け Windows ストアにアップロードした Windows ストア アプリや LOB アプリは、Windows ストアの証明書を使用して暗号署名されているため、Windows デバイスに自動的に信頼されます。ビジネス向け Windows ストアにアップロードした LOB アプリは、自社にのみ公開され、他の企業や消費者に表示されることはありません。LOB アプリをアップロードしない場合は、デバイス上でアプリの信頼を確立する必要があります。信頼を確立するには、公開キー基盤で署名証明書を生成して、デバイス上の信頼された証明書に信頼チェーンを追加する必要があります (証明書に関するセクションを参照してください)。自己署名 LOB アプリは、Windows 10 Mobile デバイス 1 台に 20 個までインストールできます。20 個を超えるアプリをデバイスにインストールするには、信頼された公的認証機関から署名証明書を購入する、またはデバイスを Windows 10 Mobile Enterprise エディションにアップグレードする必要があります。

詳細については「ビジネス向け Windows ストア」を参照してください。

アプリの管理

対象: 企業所有デバイス

IT 管理者は、Windows 10 Mobile デバイスへのインストールを許可するアプリと、アプリを最新の状態に維持する方法を制御できます。

Windows 10 Mobile に搭載されている AppLocker を使用することで、管理者は許可または禁止する Windows ストア アプリのリスト (ホワイトリスト、ブラックリストとも呼ばれます) を作成できます。この機能は、Xbox、Groove、テキスト メッセージ、電子メール、予定表など、組み込みアプリも対象になります。アプリを許可または拒否する機能を活用すれば、意図した目的以外にモバイル デバイスが使用されることを回避できます。しかし、従業員のニーズや要求とセキュリティ上の懸念事項にバランス良く対処することは、必ずしも簡単ではありません。許可リストや禁止リストを作成する場合は、Windows ストアのアプリの提供状況の変更に対応する必要もあります。

詳細については、「AppLocker CSP (英語)」を参照してください。

MDM を使用することで、IT 担当者は、許可するアプリの制御に加えて、追加のアプリ管理設定を Windows 10 Mobile に実装することができます。

設定	説明
信頼されたアプリをすべて許可する	デバイスにサイドローディングしたアプリをユーザーが使用できるようにするどうかを指定します。
Allow App Store Auto Update (アプリ ストアの自動更新を許可する)	Windows ストアのアプリの自動更新を許可するかどうかを指定します。
Allow Developer Unlock (開発者によるロック解除を許可する)	開発者によるロック解除を許可するかどうかを指定します。
Allow Shared User App Data (ユーザー アプリ データの共有を許可する)	同じアプリのユーザー間でデータを共有できるようにするどうかを指定します。
Allow Store (ストアを許可する)	Windows ストア アプリの実行を許可するかどうかを指定します。この設定を使用すると、ユーザーがストアからアプリをインストールすることは完全にブロックされますが、MDM システムを使用したアプリの配布は許可されます。
アプリケーションの制限	デバイスのアプリ制限を定義する XML BLOB。XML BLOB にはアプリの許可リストまたは拒否リストを含めることができます。アプリの許可や拒否は、アプリの ID または発行元に基づいて設定します。前述の AppLocker のページ (英語) を参照してください。

設定	説明
Disable Store Originated Apps (ストアから取得されたアプリを無効にする)	プレインストールされたアプリや、ポリシーが適用される前にダウンロードされたすべての Windows ストア アプリの起動を無効にします。
Require Private Store Only (非公開ストアのみを利用可能にする)	デバイス上のストア アプリから利用できるストアを非公開ストアに限定するかどうかを指定します。有効にすると、利用できるストアが非公開ストアのみに限定されます。無効にすると、市販のカタログと非公開ストアの両方が利用可能になります。
Restrict App Data to System Volume (アプリ データの保存先をシステム ボリュームに制限する)	アプリ データの保存先をシステム ドライブに限定するか、SD カードにも保存できるようにするかを指定します。
Restrict App to System Volume (アプリの保存先をシステム ボリュームに制限する)	アプリのインストール先をシステム ドライブに限定するか、SD カードにもインストールできるようにするかを指定します。
Start screen layout (スタート画面のレイアウト)	スタート画面の構成に使用する XML BLOB (詳細については「Windows 10 モバイル エディションのスタート画面のレイアウト」を参照してください)。

アプリケーション管理の詳細については、「Policy CSP (英語)」を参照してください。

ユーザーが自分を Windows 10 Mobile のアプリ開発者として登録し、デバイスの開発者向け機能を有効にできてしまうと、セキュリティ上の問題が発生する可能性があります。こうした場合には、提供元が不明のアプリがユーザーによってインストールされたり、デバイスがマルウェアの脅威にさらされたりするおそれがあります。ユーザーによる開発者向け機能の有効化を防止するには、**[Disable development unlock (side loading) (開発用ロック解除 (サイドローディング) を無効にする)]** ポリシーを設定します。この設定は、お使いの MDM システムで構成できます。

データ漏えい防止

Windows Information Protection

対象: 企業所有デバイスおよび個人所有デバイス

モバイル デバイス上の企業データを保護するうえで特に難しい問題となるのは、企業データを個人データから分離することです。一般に入手できるほとんどのソリューションでは、このようなデータの分離を実現するために、ユーザーが別のユーザー名とパスワードを使用して、企業アプリとデータがすべて格納されている場所にログインする必要がありますが、この方法ではユーザーの生産性が低下してしまいます。

Windows 10 Mobile に搭載された Windows Information Protection では、企業データと個人データのプライバシーを透過的に保護できます。この機能を使用すると、個人データと企業データに自動的にタグが付けられ、企業データとして分類されたデータにはポリシーによって定義された一部のアプリからのみアクセスできます。このポリシーは、データがローカルのストレージやリムーバブル ストレージに保存されている場合にも適用されます。企業データは常

に保護された状態にあるため、ユーザーはデータをソーシャル メディアや個人の電子メールなどの公共の場所にコピーすることはできません。

Windows Information Protection はあらゆるアプリで動作し、対応アプリと非対応アプリの 2 つのカテゴリにアプリを分類します。対応アプリでは企業データと個人データが区別され、どちらを保護対象とすべきかが内部ポリシーに基づいて正確に決定されます。企業データは常に暗号化され、コピーや貼り付けをしようとしたり、企業アプリ以外のアプリや社外のユーザーと共有したりしようとしても、実行することができません。非対応アプリでは、すべてのデータが企業データと見なされ、既定ではすべてのデータが暗号化されます。

UWA プラットフォーム上で開発したアプリは、対応アプリにすることが可能です。マイクロソフトでは、広く普及している当社アプリのいくつかを対応させることに重点的に取り組みました。そのアプリを次に示します。

- Microsoft Edge
- Microsoft People
- モバイル Office アプリ (Word、Excel、PowerPoint、および OneNote)
- Outlook メール/カレンダー
- Microsoft フォト
- Microsoft OneDrive
- Groove ミュージック
- メモ帳
- Microsoft 映画 & テレビ
- Microsoft メッセージング

次の表に、Windows Information Protection に関して構成可能な設定を示します。

設定	説明
実施レベル	情報保護の実施レベルを次の中から設定します。 **オフ** (保護なし) **サイレント モード** (暗号化と監査のみ) **上書きモード** (暗号化、ダイアログの表示、および監査) **ブロック モード** (暗号化、ブロック、および監査)
エンタープライズ保護ドメイン名	企業が自社のユーザー ID 用に使用するドメインのリスト。リスト内のドメインのいずれかに属するユーザー ID は、いずれも企業が管理するアカウントと見なされ、この ID と関連付けられているデータは保護されます。
ユーザーの解読を許可する	ユーザーにファイルの暗号化解除を許可します。許可されていない場合、ユーザーは OS やアプリのユーザー機能を使用して企業のコンテンツの保護を解除することはできません。
Require protection under lock configuration (ロックによる保護の構成を必須にする)	ロック機能による保護 (PIN による暗号化とも呼ばれます) の構成を必須にするかどうかを指定します。

設定	説明
データ回復証明書	暗号化されたファイルのデータの回復に使用できる回復証明書を指定します。これは、暗号化ファイル システム (EFS) 用のデータ回復エージェント (DRA) 証明書と同じものです。提供にはグループ ポリシーではなく MDM を使用する必要があります。
Revoke on unenroll (登録解除時に取り消し)	デバイスを管理サービスから登録解除するときに、情報保護キーを取り消すかどうかを指定します。
RMS template ID for information protection (情報保護のための RMS テンプレート ID)	IT 管理者は RMS 保護ファイルへのアクセスを許可するユーザーと期間に関する詳細を構成することができます。
Allow Azure RMS for information protection (情報保護のための Azure RMS を許可する)	情報保護のための Azure RMS 暗号化を許可するかどうかを指定します。
Show information protection icons (情報保護アイコンを表示する)	Web ブラウザーとスタート メニュー内の企業専用アプリのタイルで、情報が安全に保護されているファイルのアイコンにオーバーレイを追加するかどうかを指定します。
状態	デバイスの情報保護に関する現在の状態を示す、読み取り専用のビット マスク。MDM サービスはこの値を使用して、情報保護に関する現在の全体的な状態を判定することができます。

Windows Information Protection の詳細については、「EnterpriseDataProtection CSP (英語)」または「Windows 10 Mobile セキュリティ ガイド」を参照してください。

メモ

Windows Information Protection の機能を使用するには、AppLocker とネットワークの分離の設定 (特に、[エンタープライズ IP の範囲] と [エンタープライズ ネットワーク ドメイン名]) も構成する必要があります。これにより、保護が必要なすべての企業データのソースを定義して、これらのソースに書き込まれるデータが、ユーザーの暗号化キーで暗号化されないように (企業内の他のユーザーがアクセスできるように) します。詳細については、「AppLocker CSP (英語)」(英語) と、「Policy CSP (英語)」のネットワークの分離ポリシーに関する説明を参照してください。

ユーザーの活動の管理

対象: 企業所有デバイス

企業所有デバイスでは、ユーザーの活動によって企業データが不要なリスクにさらされることがあります。たとえば、社内の LOB アプリの企業情報が含まれた画面キャプチャが作成されるケースなどが挙げられます。Windows 10 Mobile のユーザー エクスペリエンスを制限し、企業データを保護してデータの漏えいを防止することで、こうしたリスクを軽減できます。次の表では、データ漏えいの防止に役立つ機能を説明します。

設定	説明
コピー/貼り付けを使用する	ユーザーがコンテンツをコピー/貼り付けできるようにするかどうかを指定します。
Cortana を許可する	ユーザーがデバイスで Cortana を使用できるようにするかどうかを指定します (対応デバイスの場合)。
Allow device discovery (デバイスの検出を許可する)	ロック画面でデバイスの検出機能を使用できるようにするかどうかを指定します (たとえば、ロック画面表示中に、デバイスでプロジェクターやその他のデバイスを検出可能にするかどうかなど)。
入力の個人設定を許可する	個人を特定できる情報をデバイスに残したり、ローカルに保存したりできるかどうかを指定します (Cortana の学習内容、手書き入力、音声入力など)。
Allow manual MDM unenrollment (手動での MDM 登録解除を許可する)	ユーザーによる企業アカウントの削除 (MDM システムからのデバイスの登録解除) を許可するかどうかを指定します。
画面キャプチャを使用する	デバイス上でのスクリーンショットのキャプチャをユーザーに許可するかどうかを指定します。
Allow SIM error dialog prompt (SIM エラー ダイアログの表示を許可する)	SIM カードがインストールされていない場合に、ダイアログを表示するかどうかを指定します。
Allow sync my settings (設定の同期を許可する)	ユーザー エクスペリエンス設定をデバイス間で同期するかどうかを指定します (Microsoft アカウントでのみ使用可能)。
Allow toasts notifications above lock screen (ロック画面へのトースト通知を許可する)	ユーザーがデバイスのロック画面でトースト通知を確認できるようにするかどうかを指定します。
音声録音を許可する	音声録音の実行をユーザーに許可するかどうかを指定します。
フィードバックの通知を表示しない	デバイスにマイクロソフトからのフィードバックの質問を表示させないようにします。
Allow Task Switcher (タスク スイッチャーを許可する)	デバイス上でのタスクの切り替えを許可するか、切り替えを禁止してタスク スイッチャーに廃棄状態のアプリ画面を表示させないようにします。

設定	説明
Enable Offline Maps Auto Update (オフライン マップの自動更新を有効にする)	マップ データの自動ダウンロードと更新を無効にします。
Allow Offline Maps Download Over Metered Connection (従量制課金接続時のオフライン マップのダウンロードを許可する)	従量制課金接続時のマップ データのダウンロードと更新を許可します。

ユーザー エクスペリエンス設定の詳細については、「Policy CSP (英語)」を参照してください。

Microsoft Edge

対象: 企業所有デバイスおよび個人所有デバイス

MDM システムは、モバイル デバイス上の Microsoft Edge を管理する機能も備えています。Microsoft Edge は Windows 10 Mobile デバイスで唯一利用できるブラウザーです。Microsoft Edge のモバイル バージョンは、Flash や拡張機能がサポートされないという点でデスクトップ バージョンとわずかに異なります。Edge は管理性が高く、Windows Information Protection と統合されているため、PDF ビューアーとしても優れています。

次の表に、Windows 10 Mobile の Microsoft Edge の設定を示します。

設定	説明
ブラウザーを許可する	ユーザーがデバイスで Microsoft Edge を実行できるようにするかどうかを指定します。
Allow Do Not Track headers (トラッキング拒否ヘッダーを許可する)	トラッキング拒否ヘッダーを許可するかどうかを指定します。
InPrivate を許可	ユーザーが InPrivate ブラウジングを使用できるようにするかどうかを指定します。
Password Manager を許可する	ユーザーが Password Manager を使用してローカルでパスワードを保存および管理できるようにするかどうかを指定します。
アドレス バーで検索候補を許可する	アドレス バーに検索候補を表示するかどうかを指定します。
Allow SmartScreen (SmartScreen を許可する)	SmartScreen フィルター機能を有効にするかどうかを指定します。
クッキー	クッキーを許可するかどうかを指定します。
お気に入り	お気に入りの URL を構成します。

設定	説明
最初の実行時の URL	ユーザーが Microsoft Edge を最初に起動したときに開く URL。
Prevent SmartScreen Prompt Override (SmartScreen のダイアログの無視を防止する)	URL に関する SmartScreen の警告をユーザーが無視できるようにするかどうかを指定します。
Prevent SmartScreen Prompt Override for Files (ファイルに関する SmartScreen のダイアログの無視を防止する)	ファイルに関する SmartScreen の警告をユーザーが無視できるようにするかどうかを指定します。

管理

企業の IT 環境では、セキュリティのニーズとコスト管理とのバランスを考えながら、最新のテクノロジをユーザーに提供する必要があります。サイバー攻撃が日常茶飯事となっている今、Windows 10 Mobile デバイスの状態を適切にメンテナンスすることが欠かせません。IT 担当者は構成設定を制御して、設定が各種ポリシーに違反しないように努めると共に、社内アプリケーションへのアクセスが認められているデバイスの使用を徹底させる必要があります。Windows 10 Mobile には、デバイスを企業ポリシーに準拠させるために必要な、モバイル操作に関する管理機能が備わっています。

サービス オプション

更新プロセスの合理化

対象: 企業所有デバイスおよび個人所有デバイス

マイクロソフトでは、Windows 製品のエンジニアリング サイクルとリリース サイクルの合理化に努めてきました。その結果、市場から求められている最新の機能やエクスペリエンスを、これまで以上に速いペースで提供することが可能になりました。マイクロソフトでは、年 (12 か月間) に 2 回の**機能更新プログラム**の提供を予定しています。機能更新プログラムは **Current Branch (CB)** として提供され、バージョン番号が付与されます。

ブランチ	バージョン番号	リリース時期
Current Branch	1511	2015 年 11 月
Current Branch for Business	1511	2016 年 3 月
Current Branch	1607	2016 年 7 月

また、マイクロソフトは、セキュリティと安定性に関する月 1 回の更新を実施し、Windows 10 Mobile デバイスに更新プログラムを直接提供してインストールします。この**品質更新プログラム**は、マイクロソフトが Windows Update を通じてリリースを管理しており、Windows 10 Mobile を搭載しているすべてのデバイスに提供されます。Windows 10 Mobile デバイスは、機能更新プログラムと品質更新プログラムを同一の標準的な更新プロセスの一環として実行します。

品質更新プログラムは通常、機能更新プログラムよりも小規模ですが、インストールのプロセスと操作は非常に似ています。ただし、大規模な更新であればインストール時間は長くなります。企業のお客様は、Enterprise エディションにデバイスをアップグレードすると、MDM システムを使用して Windows 10 Mobile デバイスの更新の操作とプロセスを管理することができます。ほとんどの場合、更新プロセスを管理するポリシーは、機能更新プログラムと品質更新プログラムの両方に適用されます。

マイクロソフトでは、Windows 10 Mobile デバイスの**最新**の更新プログラムを、**自動的**かつ業務に**支障**をきたすことのない形で、すべてのお客様に提供することを目指しています。Windows 10 Mobile デバイスでは初期セットアップ時に、利用可能な更新プログラムを確認するために**自動スキャン**が実行されます。ただし、デバイスのネットワーク接続状況と電源状態に応じて、更新の方法とタイミングは変わります。

ネットワーク接続	説明	自動スキャン	自動ダウンロード	自動インストール	自動再起動
Wi-Fi	デバイスが個人または企業の Wi-Fi ネットワークに接続されている (データ料金が発生しない状態)	○	○	○	○ - アクティブな時間帯以外 (ユーザーが再起動を延期した場合、7 日間経過すると強制的に再起動)
携帯ネットワーク	デバイスが携帯ネットワークにのみ接続されている (通常のデータ料金が適用される状態)	過去 5 日間にスキャンが正しく実行されている場合、日次のスキャンをスキップ	更新パッケージのサイズが小さく、モバイル通信事業者のデータ制限を超えていない場合、またはユーザーが [今すぐダウンロード] をクリックした場合にのみ実行	ユーザーが [今すぐダウンロード] をクリックした場合にのみ実行	
携帯ネットワーク - ローミング	デバイスが携帯ネットワークに接続されていて、ローミング料金が適用されている	×	×	×	

更新リリースの履歴

対象: 企業所有デバイスおよび個人所有デバイス

マイクロソフトでは、Windows 10 と Windows 10 Mobile の新しい機能更新プログラムを定期的に公開しています。「Windows 10 のリリース情報」では、お使いのデバイスに Windows 10 の最新の機能更新プログラムと品質更新プログラムが適用されているかどうかを確認することができます。このページでは、PC 用の Windows 10 と Windows 10 Mobile の両方のリリース情報を公開しています。また、「Windows 10 の更新履歴」では、更新内容の詳細を参照できます。

メモ

マイクロソフトでは、IT 担当者の方に Windows Insider Program へのご参加をお勧めしています。このプログラムは、正式リリース前に更新内容をテストして Windows 10 Mobile をさらに改善することを目的としたものです。疑問や質問、困ったことがございましたら、**Feedback Hub** からご意見をお寄せください。

Windows as a Service

対象: 企業所有デバイスおよび個人所有デバイス

マイクロソフトは、モバイル通信事業者の承認を経ずに、Windows 10 Mobile の更新プログラムを直接デバイスに提供してインストールする方法を新たに開発しました。この機能により、更新プログラムの展開と継続的な管理を簡略化して、より広範な従業員が常に最新の Windows 機能とエクスペリエンスを利用できるようになります。さらに、デバイスのセキュリティを保つための更新管理が不要になるため、組織の総保有コストを抑えることができます。

更新プログラムの提供状況は、そのデバイスで選択したサービス オプションによって異なります。次の表で、サービス オプションの概要を説明します。

サービス オプション	新機能がインストール可能になる時期	サービス提供の最短期間	主なメリット	サポート対象のエディション
Windows Insider ビルド	開発サイクル期間中の適切な時期。 Windows Insider 参加者のみにリリース。	場合による。次の Insider ビルドが Windows Insider 参加者にリリースされるまで。	機能更新プログラムがリリースされるまで、参加者は新機能とアプリケーション互換性をテストすることが可能。	Mobile。
Current Branch (CB)	マイクロソフトが Windows Update に機能更新プログラムを公開した直後。	通常、マイクロソフトは機能更新プログラムを 12 か月間に 2 回リリース (約 4 か月おき。ただしこれより長くなる場合もある)。	新機能をできるだけ早くユーザーに提供することが可能。	Mobile と Mobile Enterprise。
Current Branch for Business (CBB)	対応する機能更新プログラムをマイクロソフトが Windows Update に初めて公開してから少なくとも 4 か月後。	少なくとも 4 か月間 (ただしこれより長くなる場合もある)。	展開前に新機能をテストする時間的猶予が得られる。	Mobile Enterprise のみ。

メモ

Windows as a Service の詳細については、こちらのページ (英語) を参照してください。

Enterprise エディション

対象: 企業所有デバイス

Windows 10 Mobile では Windows Update から直接ユーザーのデバイスに更新プログラムが提供されますが、企業所有デバイスに対する更新について追跡やテストを行い、計画を立てたいと多くの組織が考えています。このような要望にお応えするために、マイクロソフトは **Windows 10 Mobile Enterprise** エディションを開発しました。

Windows 10 Mobile Enterprise エディションにアップグレードすると、企業が必要とするデバイスとアプリの管理機能が追加で利用できます。具体的には、次のことが可能になります。

- **機能更新プログラムと品質更新プログラムの保留、承認、および展開:** Windows 10 Mobile デバイスは、Windows Update から直接更新プログラムを取得します。展開する前に更新プログラムを選定したい場合は、Windows 10 Mobile Enterprise エディションにアップグレードする必要があります。Enterprise エディションを有効にすると、スマートフォンのサービス オプションを Current Branch for Business に設定できるようになり、IT 管理者は更新リリース前にテストするための時間を確保できます。

- **1 台のデバイスに自己署名 LOB アプリを無制限に展開:** MDM システムを使用して LOB アプリを直接デバイスに展開するには、自社の証明機関 (CA) で生成したコード署名証明書を使用して、ソフトウェア パッケージに暗号署名する必要があります。自己署名 LOB アプリは Windows 10 Mobile デバイスに 20 個まで展開できます。20 個を超える自己署名 LOB アプリを展開するには、Windows 10 Mobile Enterprise が必要です。

- **利用統計情報レベルを設定:** マイクロソフトでは、Windows デバイスのセキュリティを維持し、Windows とマイクロソフトのサービスの品質を高めるために、利用統計情報のデータを収集しています。利用統計情報レベルを設定して、デバイスのセキュリティを保つために必要な利用統計情報だけが収集されるようにするには、Windows 10 Mobile Enterprise エディションにアップグレードする必要があります。

利用統計情報の詳細については、こちらのページを参照してください。

Windows 10 Mobile Enterprise をアクティブ化するには、お使いの MDM システムまたはプロビジョニング パッケージを使用して、Windows 10 Mobile デバイスに Windows 10 Enterprise ライセンスを追加します。ライセンスはボリューム ライセンス ポータルから入手できます。テストを目的として使用する場合は、MSDN ダウンロード サーバーからライセンス ファイルを入手することができます。なお、有効な MSDN サブスクリプションが必要です。

Enterprise エディションへのデバイスの更新の詳細は「WindowsLicensing CSP (英語)」を参照してください。

推奨事項

Enterprise エディションは企業所有デバイスでのみ使用することをお勧めします。一度アップグレードすると、ダウングレードすることはできません。デバイスをワイプまたはリセットしても、Enterprise ライセンスは個人所有デバイスから削除されません。

MDM を使用した更新の保留と承認

対象: Enterprise エディション搭載の企業所有デバイス

デバイスを Windows 10 Mobile Enterprise エディションにアップグレードすると、更新ポリシーのセットを使用して、Windows Update (または Windows Update for Business) から更新プログラムを受信するデバイスを管理できるようになります。

機能更新プログラムを制御するには、デバイスのサービス オプションを Current Branch for Business (CBB) に移行する必要があります。CBB をサブスクライブしているデバイスでは、次の CBB が Microsoft Update に公開されるまで更新が保留されます。デバイスが次の CBB まで機能更新プログラムを保留している間も、デバイスは品質更新プログラムを受信します。

毎月提供される品質更新プログラムを制御するには、保留に関するポリシーを追加して、必要な保留期間を設定する必要があります。保留期間を設定すると、Windows 10 Mobile デバイスで品質更新プログラムが Windows Update から利用可能になっても、その期間が経過するまでインストールされなくなり、IT 担当者はデバイスとアプリに対する更新の影響をテストする時間を確保することができます。

更新プログラムを配布してインストールする前に、アプリケーションの互換性の問題がないかテストする必要がある場合もあります。その場合、IT 担当者は更新前の承認を必須にすることができます。これにより MDM 管理者は、デバイスにインストールする更新プログラムを個別に選択して承認し、ユーザーの代わりに更新に関連する EULA を承諾できるようになります。Windows 10 Mobile では、更新プログラムはすべて「OS の更新」としてパッケージ化されており、個別の修正プログラムとして提供されることはない点にご注意ください。

次の CBB がデバイスにリリースされるまで待機せず、品質更新プログラムと機能更新プログラムを同じ方法で管理することが求められる場合もあります。承認とリリースが同じプロセスで行われるようになり、更新プログラムのリリースが合理化されるためです。その場合、更新プログラムの種類ごとに異なる保留期間を適用できます。バージョン 1607 では、更新をきめ細かく制御できるように、ポリシー設定がさらに追加されています。

更新プログラムをデバイスに展開した後で、企業所有デバイスへの更新のロールアウトを一時停止する必要があるケースもあります。

たとえば、品質更新プログラムのロールアウトを開始した後に、一部のスマートフォン モデルに悪影響が生じたり、一部の LOB アプリでデータベースへの接続と更新が実行できないという報告があったりする場合です。最初のテストでは見つからなかった問題が生じることもあります。

そのような場合、IT 担当者は更新を一時停止して、予期しなかった問題を調査して修復することができます。

次の表に、Windows 10 Mobile の各バージョンで適用可能な更新ポリシー設定の概要を示します。ポリシー設定はいずれも下位互換性があり、今後の機能更新プログラムでも維持されます。これらの設定がお使いの MDM システムでサポートされているかどうかを確認するには、お使いの MDM システムのドキュメントを参照してください。

アクティビティ (ポリシー)	バージョン 1511 の設定	バージョン 1607 の設定
機能更新プログラムを保留するために、デバイスで CBB をサブスクライブする	**RequireDeferUpgrade** 次の CBB のリリースまで機能更新プログラムを保留します。デバイスは品質更新プログラムを Current Branch for Business (CBB) から受信します。 Current Branch のリリース後、最低 4 か月間にわたり機能更新プログラムを保留します。	**BranchReadinessLevel** 次の CBB のリリースまで機能更新プログラムを保留します。デバイスは品質更新プログラムを Current Branch for Business (CBB) から受信します。 Current Branch のリリース後、最低 4 か月間にわたり機能更新プログラムを保留します。
更新を保留する	**DeferUpdatePeriod** 品質更新プログラムを 4 週間 (28 日間) 保留します。	**DeferQualityUpdatePeriodInDays** 機能更新プログラムと品質更新プログラムを最大 30 日間保留します。
更新を承認する	**RequireUpdateApproval**	**RequireUpdateApproval**
承認した更新プログラムを展開した後に、更新プログラムのロールアウトを一時停止する	**PauseDeferrals** 機能更新プログラムを最大 35 日間一時停止します。	**PauseQualityUpdates** 品質更新プログラムを最大 35 日間一時停止します。

更新操作の管理

対象: Enterprise エディション搭載の企業所有デバイス

更新クライアントの操作については、AllowAutoUpdate ポリシー (英語) で設定します。IT 担当者はこのポリシーを設定することで、更新プログラムをスキャン、ダウンロード、インストールする際の、デバイスの更新クライアントの動作を調整できます。

設定できる内容は次のとおりです。

- 更新プログラムをダウンロードする前にユーザーに通知する。
- 更新プログラムを自動的にダウンロードした後、再起動のスケジュールを決めるようユーザーに通知する (ポリシーを構成していない場合は、これが既定の動作となります)。
- 自動的にダウンロードしてデバイスを再起動する (ユーザーへの通知が表示されます)。
- 指定された時刻に自動的にダウンロードしてデバイスを再起動する。
- 自動的にダウンロードしてデバイスを再起動する。ユーザーの操作は不要です。
- 自動更新をオフにする。このオプションは規制を遵守しているシステムでのみ使用する必要があります。デバイスが更新プログラムを受信することはありません。

また、バージョン 1607 では、更新プログラムのインストールや再起動が業務や従業員の生産性の妨げにならないように、従業員のデバイスに更新プログラムを適用するタイミングを構成することができます。アクティブな時間帯以外 (英語) に更新プログラムのインストールと再起動を行うようにスケジュールを設定することができます (サポートされる値は 0 ～ 23。0 は午前 0 時、1 は午前 1 時を表します)。また、特定の曜日 (英語) を設定することも可能です (サポートされる値は 0 ～ 7。0 は毎日、1 は日曜、2 は月曜を表します)。

MDM を使用した更新プログラム提供元の管理

対象: Enterprise エディション搭載の企業所有デバイス

Windows 10 Enterprise では、IT 管理者は Windows Update からの更新プログラムのインストールを延期できますが、企業によっては更新プロセスをさらに細かく制御する必要がある場合もあります。このような状況に配慮し、マイクロソフトでは Windows Update for Business を開発しました。Windows Update for Business は、IT 管理者に Windows Update を中心とした管理機能を追加で提供することを目的としたものです。これには、デバイスのグループに更新プログラムを展開する機能、更新プログラムをインストールするメンテナンス期間を定義する機能などが含まれます。MDM システムを使用している場合、Windows Update for Business の使用は必須ではありませんが、これらの機能を MDM システムから管理することができます。

> Windows Update for Business の詳細については、こちらのページ (英語) を参照してください。

IT 管理者は、デバイスが更新プログラムを取得する場所を AllowUpdateService (英語) で指定することができます。指定できる場所は、Microsoft Update、Windows Update for Business、Windows Server Update Services (WSUS) です。

Windows Update サーバーを使用した更新プログラムの管理

対象: Enterprise エディション搭載の企業所有デバイス

WSUS を使用する場合は、UpdateServiceUrl (英語) を設定して、Windows Update の代わりに WSUS サーバーに更新を確認することをデバイスに許可します。これは、インターネットに接続できないデバイス (通常、業務の遂行に使

用するハンドヘルド デバイスやその他の Windows IoT デバイス) を更新する必要があるオンプレミスの MDM に便利です。

> Windows Server Update Services (WSUS) を使用した更新プログラムの管理の詳細については、こちらのページを参照してください。

デバイスの更新状態の照会

対象: 個人所有デバイスと企業所有デバイス

Windows 10 Mobile Enterprise では更新プログラムの取得方法を構成できるだけでなく、MDM 管理者は Windows 10 Mobile の更新情報についてデバイスに照会し、承認した更新プログラムの一覧と照らし合わせて更新状態を確認することができます。

デバイスの更新状態を照会すると、次の内容を参照できます。

- インストールされた更新プログラム: デバイスにインストールされた更新プログラムの一覧。
- インストール可能な更新プログラム: インストール可能な更新プログラムの一覧。
- 失敗した更新: インストール中に失敗した更新プログラムの一覧 (失敗した理由を含む)。
- 保留中の再起動: インストールを完了するために再起動する必要がある更新プログラムの一覧。
- 最後にスキャンを正常に完了した時刻: 最後に更新プログラム スキャンを正常に完了した時刻。
- アップグレードの保留: アップグレードが次の更新サイクルまで延期されているかどうか。

デバイスの正常性

対象: 個人所有デバイスと企業所有デバイス

デバイス正常性構成証明 (DHA) は、Windows 10 Mobile に新しく追加された防御機能の 1 つです。この機能を使用すると、セキュリティ構成が不足しているデバイスや、高度な攻撃に簡単に悪用されるおそれのある脆弱性を持ったデバイスをリモートで検出できます。

Windows 10 Mobile は、Microsoft Intune やサード パーティ製の MDM ソリューションと簡単に統合できると共に、デバイスの正常性とコンプライアンス状態を総合的に把握できます。これらのソリューションを組み合わせて使用することで、ジェイルブレイク (脱獄) されたデバイスの検出、デバイスのコンプライアンス状態の監視、コンプライアンス レポートの作成、ユーザーや管理者に対する問題の警告、修正操作の実施、および Office 365 や VPN などのリソースへの条件付きアクセスの管理を実行することができます。

デバイス正常性構成証明 (DHA) の最初のバージョンは、企業のクラウド ベースのトポロジで運用されている TPM 2.0 対応の Windows 10 デバイス向けに、2015 年 6 月にリリースされました。Windows 10 Anniversary Update では、デバイス正常性構成証明機能が、インターネットにアクセスするかエアギャップ ネットワークで運用されているかを問わず、TPM 1.2 対応のレガシ デバイス、ハイブリッド環境、オンプレミス環境にまで拡張されました。

正常性構成証明機能は、Open Mobile Alliance (OMA) 標準に準拠しています。DHA を使用して検証できるデバイスの条件を次に示します。

- Windows 10 オペレーティング システムを搭載している (携帯電話または PC)
- ディスクリート形式かファームウェア形式の Trusted Module Platform (TPM 1.2 または 2.0) に対応している
- DHA 対応のデバイス管理ソリューション (Intune またはサード パーティ製の MDM) で管理されている

- クラウド、ハイブリッド環境、オンプレミス環境、または BYOD シナリオで運用されている

DHA 対応のデバイス管理ソリューションを利用することで、IT 管理者は管理対象のすべての Windows 10 Mobile デバイスに適用する一元的なセキュリティ基準を作成できます。このようなソリューションでは、IT 管理者は次の操作を実行できます。

- ハードウェアの構成証明データ (確実性の高いデータ) をリモートで収集する
- デバイスの正常性コンプライアンスを監視して、脆弱性のあるデバイスまたは高度な攻撃により悪用されるおそれのあるデバイスを検出する
- 危害を受けるおそれのあるデバイスに対して、次のような対策を講じる
- 修正操作をリモートから実行して、攻撃元デバイスからのアクセスを不可能にする (デバイスのロック、ワイプ、ブロックなど)
- デバイスから価値の高い資産へのアクセスを防止する (条件付きアクセス)
- 詳しい調査と監視を実施する (詳しい監視のために、デバイスをハニーポットとして運用する)
- ユーザーに警告するか、管理者が問題を修正する

メモ

Windows デバイス正常性構成証明サービスは、モバイル デバイス管理ソリューション (Microsoft Intune など) や、別途購入したその他の種類の管理システム (SCCM など) によって実現される条件付きアクセスのシナリオで使用できます。

Windows 10 Mobile の正常性構成証明の詳細については、「Windows 10 Mobile セキュリティ ガイド」を参照してください。

次の表に、DHA によってサポートされる属性と、前述した修正操作を実行できる属性について示します。

データ ポイント	説明
Attestation Identity Key (AIK) present (構成証明識別キー (AIK) が存在)	AIK が存在することを示します (AIK がないデバイスよりも信頼性が高くなります)。
Data Execution Prevention (DEP) enabled (データ実行防止 (DEP) が有効)	デバイスで DEP ポリシーが有効にされているかどうかを示します。DEP ポリシーが有効なデバイスは、DEP ポリシーがないデバイスよりも信頼できます。
BitLocker の状態	BitLocker はデバイスのストレージの保護に役立ちます。BitLocker を使用しているデバイスは、使用していないデバイスよりも信頼できます。
セキュア ブートが有効	デバイスでセキュア ブートが有効にされているかどうかを示します。セキュア ブートが有効にされているデバイスは、有効にされていないデバイスよりも信頼できます。Windows 10 Mobile デバイスでは、セキュア ブートは常に有効にされています。
コードの整合性が有効	ドライブまたはシステム ファイルのコードの整合性が、メモリにロードされるたびに検証されているかどうかを示します。コードの整合性が有効にされているデバイスは、有効にされていないデバイスよりも信頼できます。

データ ポイント	説明
セーフ モード	Windows がセーフ モードで実行されているかどうかを示します。Windows をセーフ モードで実行しているデバイスは、標準のモードで実行しているデバイスよりも信頼性に劣ります。
Boot debug enabled (ブート デバッグが有効)	デバイスでブート デバッグが有効にされているかどうかを示します。ブート デバッグが有効にされているデバイスは、ブート デバッグを有効にしていないデバイスよりも安全性 (信頼性) に劣ります。
OS kernel debugging enabled (OS カーネル デバッグが有効)	デバイスでオペレーティング システムのカーネル デバッグが有効にされているかどうかを示します。オペレーティング システムのカーネル デバッグが有効にされているデバイスは、オペレーティング システムのカーネル デバッグを無効にしているデバイスよりも安全性 (信頼性) に劣ります。
Test signing enabled (テスト署名が有効)	テスト署名が有効にされているかどうかを示します。テスト署名が有効にされているデバイスは、テスト署名が無効にされているデバイスよりも信頼性に劣ります。
ブート マネージャーのバージョン	デバイスで実行しているブート マネージャーのバージョンを示します。HAS はこのバージョンを調べることで、より安全性 (信頼性) が高い最新のブート マネージャーが実行されているかどうかを確認します。
Code integrity version (コードの整合性のバージョン)	ブート シーケンス中に整合性チェックを実行しているコード整合性のバージョンを示します。HAS はこのバージョンを調べることで、より安全性 (信頼性) が高い最新のコードのバージョンが実行されているかどうかを確認します。
Secure Boot Configuration Policy (SBCP) present (セキュア ブート構成ポリシー (SBCP) が存在)	カスタム SBCP のハッシュが存在するかどうかを示します。SBCP ハッシュが存在するデバイスは、SBCP ハッシュがないデバイスよりも信頼できます。
Boot cycle whitelist (ブート サイクルのホワイトリスト)	発行済みのホワイトリストとの比較に使用する、ブート サイクル中のホスト プラットフォーム (製造元が定めるもの) を表示できます。ホワイトリストに準拠しているデバイスは、準拠していないデバイスよりも信頼性 (安全性) が高くなります。

シナリオ例

Windows 10 Mobile は、Microsoft Intune やサード パーティ製のモバイル デバイス管理 (MDM) ソリューションと連携および統合できる保護機能を備えています。IT 管理者は、コンプライアンス状態の監視と検証を行い、デバイスの物理ハードウェアを基盤とした安全性と信頼性によって、企業のリソースをエンドツーエンドで確実に保護することができます。

スマートフォンを起動したときに実行される処理を次に示します。

1. Windows 10 のセキュア ブート機能がブート シーケンスを保護し、定義済みの信頼された構成でデバイスを起動させ、工場出荷時の信頼されたブート ローダーを読み込みます。

2. Windows 10 のトラスト ブート機能に制御が渡り、Windows カーネルのデジタル署名を検証します。Windows ブート プロセス中にコンポーネントが読み込まれ、実行されます。
3. ステップ 1 と 2 に並行して、ハードウェアで保護されたセキュリティ ゾーン (ブート アクティビティを監視するブート実行パスから分離されたゾーン) で、Windows 10 Mobile の TPM (トラステッド プラットフォーム モジュール - メジャー ブート) が独立して実行されます。これにより、整合性が保護され、改ざん時にその証明が残る監査証跡 (TPM のみがアクセスできるシークレットによる署名付き) が作成されます。
4. DHA 対応の MDM ソリューションで管理されているデバイスが、保護、改ざん防止、改ざん証明を備えた通信チャネルを通じて、この監査証跡のコピーをマイクロソフトの正常性構成証明サービス (HAS) に送信します。
5. HAS がこの監査証跡を確認し、署名付きの暗号化されたレポートを発行して、デバイスに転送します。
6. IT 管理者は DHA 対応の MDM ソリューションを使用して、保護、改ざん防止、改ざん証明を備えた通信チャネルを通じて、レポートを確認することで、デバイスがポリシーに準拠した (正常な) 状態で実行されているかどうかを評価し、企業のセキュリティ要件とポリシーに基づいてアクセスを許可したり修正操作を実行したりすることができます。

資産レポート

対象: Enterprise エディション搭載の企業所有デバイス

デバイスのインベントリを使用すると、デバイスについて詳細な情報が得られるため、組織のデバイスをより効果的に管理することができます。MDM システムは、インベントリ情報をリモートから収集します。また、デバイスのリソースと情報を分析するためのレポート機能を備えています。これらのデータに基づいて、IT 担当者は現在のハードウェアとソフトウェアのリソースに関する情報を把握することができます (インストールされた更新プログラムなど)。

次の表に、デバイスのインベントリから得られる Windows 10 Mobile のソフトウェアとハードウェアに関する情報の例を示します。こうした情報が得られることに加え、MDM システムでは、本ガイドで説明している構成設定を読み込むこともできます。

設定	説明
インストールされているエンタープライズ アプリ	デバイスにインストールされているエンタープライズ アプリの一覧。
デバイス名	デバイスに構成されているデバイス名。
ファームウェア バージョン	デバイスにインストールされているファームウェアのバージョン。
オペレーティング システムのバージョン	デバイスにインストールされているオペレーティング システムのバージョン。
デバイスの現地時刻	デバイスに設定されている現地時刻。
プロセッサの種類	デバイスに使用されているプロセッサの種類。
デバイス モデル	製造元が定めるデバイスのモデル。
デバイスの製造元	デバイスを製造したメーカー。

設定	説明
デバイスのプロセッサ アーキテクチャ	デバイスに使用されているプロセッサ アーキテクチャ。
デバイスの言語	デバイスで使用されている言語。
電話番号	デバイスに割り当てられている電話番号。
ローミング状態	デバイスが携帯ネットワークにローミングで接続しているかどうかを示します。
国際移動体装置識別番号 (IMEI) と国際携帯電話加入者識別子 (IMSI)	携帯電話が利用する携帯ネットワーク接続の一意の識別子。グローバル移動体通信システム (GSM) ネットワークでは、IMEI を使用して有効なデバイスを識別します。また、どの携帯ネットワークでも、デバイスとユーザーを識別するために IMSI が使用されています。
Wi-Fi の IP アドレス	デバイスの Wi-Fi アダプターに現在割り当てられている IPv4 と IPv6 のアドレス。
Wi-Fi のメディア アクセス制御 (MAC) アドレス	デバイスの Wi-Fi アダプターに割り当てられている MAC アドレス。
Wi-Fi の DNS サフィックスとサブネット マスク	デバイスの Wi-Fi アダプターに割り当てられている DNS サフィックスと IP サブネット マスク。
セキュア ブートの状態	セキュア ブートが有効であるかどうかを示します。
企業の暗号化ポリシーの準拠状況	デバイスが暗号化されているかどうかを表示します。

利用統計情報の管理

対象: Windows 10 Mobile Enterprise エディション搭載の企業所有デバイス

マイクロソフトでは、Windows デバイスから収集した利用統計情報 (診断、パフォーマンス、および使用状況に関するデータ) を使用して、情報に基づく意思決定と重点的な取り組みに役立てると共に、最も堅牢で価値のあるプラットフォームを提供することで、Windows を信頼いただいている企業とユーザーの生産性を最大限に高めることを目指しています。利用統計情報は、常に Windows デバイスを正常に保ち、オペレーティング システムを改善して、機能とサービスをパーソナライズすることに活用されています。

利用統計情報システムが収集するデータのレベルは制御できます。デバイスの設定を変更するには、お使いの MDM システムの **[利用統計情報の許可]** の設定で、利用統計情報のレベルを指定します。

詳細については、「組織内の Windows 利用統計情報の構成」を参照してください。

メモ

利用統計情報の管理は、デバイスを Windows 10 Mobile Enterprise エディションにアップグレードした場合にのみ実行できます。

リモート アシスタンス

対象: 個人所有デバイスと企業所有デバイス

Windows 10 Mobile リモート アシスタンス機能を使用すれば、デバイスに物理的にアクセスできないときでも、ヘルプ デスクはユーザーに発生している問題を解決することができます。この機能の詳細を次に示します。

- **リモート ロック:** サポート担当者はリモートからデバイスをロックできます。この機能は、ユーザーがモバイル デバイスを紛失し、すぐには回収できない場合 (顧客訪問時にデバイスを忘れた場合など) に役立ちます。
- **リモート PIN リセット:** サポート担当者はリモートからデバイスの PIN をリセットできます。この機能は、ユーザーが PIN を忘れ、デバイスにアクセスできないときに役立ちます。企業データやユーザー データは消去されないため、デバイスをすぐに利用することができます。
- **リモート着信音再生:** サポート担当者はリモートからデバイスの着信音を再生することができます。この機能は、置き忘れたデバイスの位置を突き止めるのに役立ちます。また、リモート ロック機能と併せて使用すれば、承認されていないユーザーがデバイスを発見した場合に、デバイスへのアクセスを防止できます。
- **リモート検索:** サポート担当者はリモートからデバイスの位置を地図上で突き止めることができます。この機能は、デバイスの地理的位置を割り出すのに役立ちます。リモート検索のパラメーターは、電話の設定 (以下を参照) で構成することができます。リモート検索機能では、デバイスの現在の緯度、経度、高度に関する情報が返されます。

これらのリモート管理機能を活用することで、デバイスの管理に必要な IT 部門の負担が軽減されます。また、ユーザーがデバイスを置き忘れた場合やパスワードを忘れた場合も、すばやく使用を再開することができます。

設定	説明
Desired location accuracy (必要な位置精度)	必要とする精度。半径の値 (メートル単位) で表され、値の範囲は 1 ～ 1,000 m です。
Maximum remote find (リモート検索の最大時間)	サーバーが正常なリモート検索を受け付ける最大時間 (分単位)。値の範囲は 0 ～ 1,000 分です。
Remote find timeout (リモート検索のタイムアウト)	デバイスがリモート検索を終了するまでの時間 (秒単位)。値の範囲は 0 ～ 1,800 秒です。

使用中止

対象: 企業所有デバイスおよび個人所有デバイス

デバイスの使用中止は、デバイスのライフサイクルの最終段階です。今日のビジネス環境におけるライフサイクルの長さは、平均で約 18 か月です。その期間が経過するころには、さらに高い生産性とパフォーマンスを兼ね備えた最新のハードウェアを従業員が必要とするようになります。新しいモデルの導入に伴い、古くなったデバイスは廃棄されますが、廃棄するデバイスに企業データを残すと、データの機密性が損なわれるおそれがあるため、デバイスの使用を安全に中止することが重要です。この作業は通常、企業所有デバイスでは問題になりませんが、個人所有デバイスのシナリオでは困難な場合があります。デバイス上の個人のアプリやデータに影響を及ぼすことなく、すべての企業データを選択的にワイプできることが求められます。また、IT 担当者には、紛失したデバイスや盗難に遭ったデバイスに対してワイプを実行する際にユーザーを十分にサポートするための手段が欠かせません。

Windows 10 Mobile は、個人所有デバイスと企業所有デバイスの両方の使用中止シナリオに対応しているため、IT 担当者は安心して企業データの機密性とユーザーのプライバシーを保護することができます。

> **メモ**
>
> これらの MDM の機能は、デバイスのソフトウェアやハードウェアに備わっている出荷時の設定へのリセット機能とは別のものです。リセット機能を使用すると、デバイスを出荷時の構成に復元することができます。

個人所有デバイス: Windows 10 Mobile は、米国の規制要件である、電話の紛失や盗難に備えた「データ抹消 (kill switch)」機能をサポートしています。リセット防止機能は、account.microsoft.com の無料サービスです。この機能を使用すると、電話を簡単にリセットして再利用を防止することができます。リセット防止機能を有効にする手順は、Microsoft アカウントでサインインし、推奨設定をそのまま使用するだけです。手動で有効にするには、[設定]、[更新とセキュリティ]、[電話を探す] の順に選択し、表示された設定を使用します。現時点でリセット防止機能は MSA でのみ使用できます。Azure AD アカウントでは使用できません。また、米国内でのみ提供されます。その他の地域では利用できません。

Windows 10 Mobile には、リセット防止機能に加え、紛失したデバイスの発見に役立つ機能が他にも備わっています。[電話を探す] 機能では、電話を本当に紛失したのか、単なる置き忘れなのかを確かめることができます。この機能を使用すると、電話の地理的位置が地図上に表示されます。着信音が聞こえる距離であれば、電話の着信音を再生する方法も有効です。位置を突き止めたら、回収するまでの間、リモートから電話をロックできます。電話を取り戻せない場合は、リモートでデバイスのデータを消去できます。

紛失時や従業員の退職時にデバイスを完全にワイプする場合、ユーザーの同意を得たことと、ユーザーの個人データの保護に関する地域の法令を遵守していることを確認してください。

デバイスの完全なワイプよりも望ましい方法として、Windows Information Protection を使用し、個人所有デバイスから企業データだけを消去する方法があります。「アプリ」の章で説明されているとおり、企業データにはすべてタグが付けられており、お使いの MDM システムからデバイスの登録を解除するときに、暗号化されたすべての企業データ、アプリ、設定、およびプロファイルは、デバイスから直ちに削除され、従業員の既存の個人データに影響が及ぶことはありません。登録解除は、ユーザーが設定画面から開始できます。また、IT 担当者が MDM の管理コンソールから実行することも可能です。なお、登録解除は管理イベントであるため、MDM システムに報告されます。

企業所有デバイス: デバイスの盗難時に、ユーザーの暗号化キーをリモートから失効させることができます。ただし、この操作を実行すると、そのユーザーは他の Windows デバイス上の暗号化されたデータも読み取れなくなるので、

ご注意ください。廃棄するデバイスや紛失したデバイスの使用を中止する場合は、デバイスを完全にワイプする方法が最適です。デバイスの完全なワイプは、ヘルプ デスクまたはデバイスのユーザーが開始できます。ワイプが完了すると、Windows 10 Mobile はデバイスをクリーンな状態に戻し、OOBE プロセスを再起動します。

個人所有デバイスと企業所有デバイスの使用中止に関する設定	
設定	**説明**
Allow manual MDM unenrollment (手動での MDM 登録解除を許可する)	ユーザーによる企業アカウントの削除 (MDM システムからのデバイスの登録解除) を許可するかどうかを指定します。
Allow user to reset phone (ユーザーによる電話のリセットを許可する)	[設定] またはハードウェアのキーの組み合わせを使用してデバイスを出荷時の状態に戻すことを許可するかどうかを指定します。