Windows 10 Mobile 評価ガイド

評価ガイド (運用編)

日本マイクロソフト株式会社

発行日 : 2017 年 2 月

■ **企画/執筆/監修**

執筆：富士ソフト 株式会社

秋元 剛

池田 健

黒澤 健二

企画/監修/改訂：日本マイクロソフト株式会社

■ 改訂履歴

バージョン	年月日	改訂者	内容
1.0	2017 年 2 月 10 日	富士ソフト 株式会社	初版を作成

目次

1. はじめに 4

2. シナリオ 1 「Continuum」 5

2.1. 概要 6
2.1.1. Continuum 6
2.1.2. リモート デスクトップ 6
2.2. 準備 7
2.2.1. Continuum の要件 7
2.2.2. リモート デスクトップ セッション ホスト 8
2.2.3. リモート デスクトップ クライアント 13
2.3. 実践 15
2.3.1. Continuum 接続 15
2.3.2. リモート デスクトップ アクセス 18

3. シナリオ 2 「Office 365 との連携」 20

3.1. 概要 20
3.1.1. シングル サインオン 20
3.1.2. OneDrive for Business 20
3.1.3. WIP 21
3.1.4. Conditional Access 21
3.2. 準備 22
3.2.1. DRA 証明書 22
3.2.2. アプリの発行元・製品名の取得 23
3.2.3. WIP の作成および展開 26
3.2.4. Azure AD Premium 31
3.3. 実践 35
3.3.1. シングル サインオン 35
3.3.2. OneDrive for Business でのファイル共有 36
3.3.3. WIP 39
3.3.4. Conditional Access 42

4. シナリオ 3 「ポリシーによる機能制限」 44

4.1. 概要 44
4.1.1. ポリシーの作成と展開 44
4.1.2. 確認 44
4.2. 準備 45
4.2.1. 全般構成 45
4.2.2. カスタム構成 47
4.2.3. ポリシーの即時反映 50
4.3. 実践 51
4.3.1. アプリケーション ストアを許可しない 51
4.3.2. カメラを許可しない 54
4.3.3. リムーバブル記憶域を許可しない 56
4.3.4. メッセージング アプリを禁止する 58

5. おわりに 62

6. 用語集 63

1. はじめに

本書は、[Windows 10 mobile 評価ガイド Windows 10 mobile 導入手順] の続編です。前書では、現在すでに Microsoft Office 365 (以下、Office 365) と Microsoft Intune を利用している組織を対象に、IT 管理者が Windows 10 Mobile デバイスを組織内で配布して利用できるよう導入する手順を紹介しました。

本書では、組織の IT 管理者が Windows 10 Mobile デバイスを評価するにあたり、想定される作業を 3 つのシナリオに分け、ステップ バイ ステップで作業を進めることにより、評価環境を構築し、Windows 10 Mobile デバイスの機能を評価できるよう構成されております。

1 つ目のシナリオでは、Windows 10 Mobile の特徴的な機能である Continuum を評価します。Continuum は、Windows 10 Mobile デバイスにテレビや PC ディスプレイ等の外部モニターを接続することにより Windows 10 PC のデスクトップと同等の環境を表示する機能です。このシナリオでは、Continuum とリモート デスクトップ アプリを組み合わせて、職場の PC やリモート デスクトップ サーバーへ接続しての作業を想定しています。職場で行っていた作業を中断し、自宅や出張先で外部ディスプレイに Windows 10 Mobile デバイスに接続すると、職場で行っていた作業をそのままの状態で続行することができます。この場合、すべての作業は職場の PC やリモート デスクトップ サーバー上で行われ、一切のデータを外部のデバイスに持ち出すことも保存することもありません。

2 つ目のシナリオでは、Office 365 を例に、クラウドサービスと連携することにより、より利便性を高めつつもセキュアな状態で使用できることを評価します。Azure Active Directory に登録された組織のユーザーを Windows 10 Mobile デバイスに登録することにより、シングル サインオン機能によってユーザーは Office 365 を使用するために ID やパスワードを入力する必要はありません。また OneDrive for Business を用いることにより、他のデバイスで使用していたファイルをあたかもローカル ドライブに保存していたかのように閲覧、編集を行うことができます。

しかしながら、セキュリティの観点から、会社で配布したデバイスからのみ Office 365 環境にアクセスしたいという場合があります。そのため、Conditional Access や組織のファイルを選択的に自動で暗号化する Windows Information Protection を設定し、組織のアプリやデータをセキュアに使用できることを評価します。

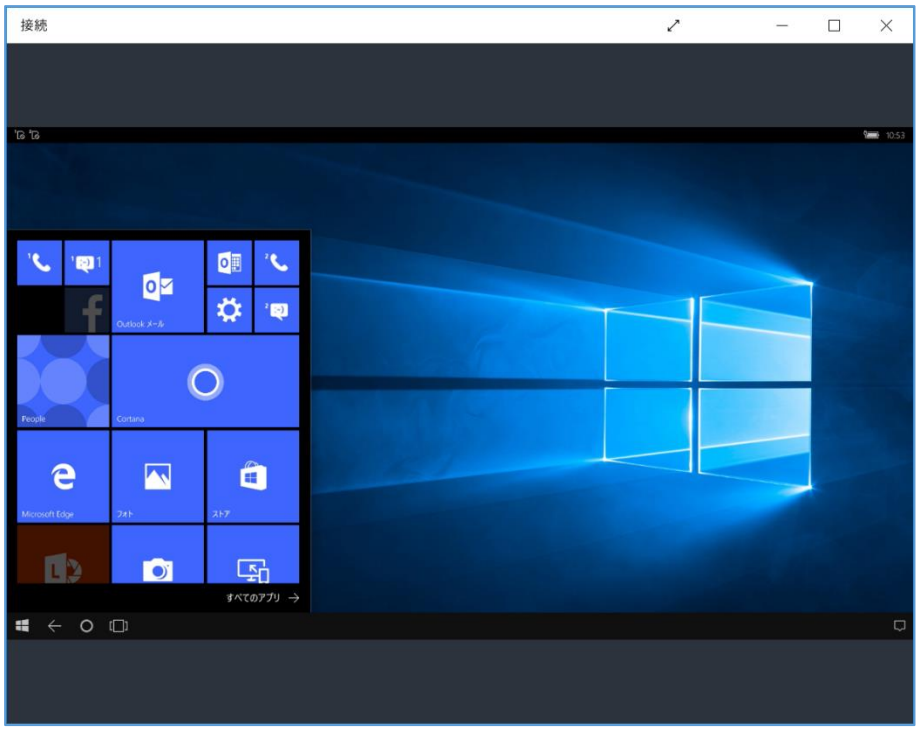
3 つ目のシナリオでは、クラウドサービスとして提供されている Mobile Device Management である Microsoft Intune を用いてポリシーを適用することにより、Windows 10 Mobile デバイスに対し組織で求められる様々な制限をかけられることを評価します。カメラや SD カードの使用を禁止したり、Store アプリの使用を禁止したりすることにより、ユーザーによる勝手なアプリのインストールを制限できることを評価します。

本書では、無料試用版や評価版を活用することにより、組織の既存環境に影響を与えることなく、Windows 10 Mobile の評価が行えるよう構成されております。そのため、実際に無料の評価環境を取得し、後述する手順を検証していただくことをお勧め致します。

なお、本書では混乱を避けるため、Windows 10 Mobile または PC の手順表内に、下記のいずれかのアイコンを表記しています。

2. シナリオ 1 「Continuum」

Continuum は、Windows 10 Mobile デバイスを外部ディスプレイに接続したときに、自動的にレイアウトを変更して、Windows 10 PC のような画面を表示させることができます。さらに、マウス、キーボードを接続することで、Windows 10 PC と同等の操作感で作業することが可能になります。これは、セカンド ディスプレイとしての役割だけではありません。例えば、1 つの Windows 10 Mobile デバイスで、通話をしながら Excel ファイルを編集したり、外出先で PowerPoint からプレゼンしたりといった、新しいワークスタイルを実現することができます。



Continuum は、リモート デスクトップと組み合わせることで、より便利に機能します。例えば、自宅で仕事がしたいとき、Windows 10 Mobile デバイスからリモート デスクトップで職場環境に接続し、Continuum 接続で外部ディスプレイに画面を表示させて、Windows 10 PC のように作業することができます。また、Windows 10 Mobile では、Device Guard が標準で搭載されています。そのため、その他のマルウェア対策ソフトを導入する必要がありません。さらに、自宅からリモート デスクトップで職場環境に接続することで、一切データを持ち出すことなく、セキュアに運用することが可能となります。

2.1. 概要

Continuum を評価するための準備および実践についての概要を下記に説明します。

2.1.1. Continuum

Continuum を利用するには、デバイス、ディスプレイ、アダプターなどのハードウェア要件を満たしている必要があります。本章では、これらのハードウェア要件を満たしていることを前提に、外部ディスプレイに接続し作業するまでの手順について説明します。

2.1.2. リモート デスクトップ

Windows 10 Mobile から Continuum で外部ディスプレイに接続し、PC にリモート デスクトップ アクセスするには、リモート デスクトップ クライアントをインストールする必要があります。また、Windows 10 Mobile のリモート デスクトップ アクセスを評価するにあたって、Microsoft Azure (以下、Azure) にリモート デスクトップ セッション ホストの役割を追加した Windows Server 2016 の仮想マシンを構築しています。そのため、Windows 10 Mobile のリモート デスクトップ アクセスを評価するには、下記 URL から Azure の評価版に登録する必要があります。

https://azure.microsoft.com/ja-jp/free/

また、下記の URL を参考に、Azure で Windows Server 2016 の仮想マシンを構築していることを前提とします。

https://docs.microsoft.com/ja-jp/azure/virtual-machines/windows/

本章では、Windows 10 Mobile にリモート デスクトップ クライアントをインストールし、Continuum 接続で外部ディスプレイにリモート デスクトップの画面を表示させ、PC のように操作するまでの手順について説明します。

2.2. 準備

Windows 10 Mobile から職場環境にリモート デスクトップ アクセスし、Continuum で外部ディスプレイに画面を表示させ、PC のように作業するためには、専用のデバイスやアプリの準備が必要になります。ここでは、Windows 10 Mobile から 職場の PC にリモート デスクトップ アクセスし、Continuum で外部ディスプレイに表示させるために準備について説明します。

2.2.1. Continuum の要件

Continuum を利用するためには、下記の要件を満たしている必要があります。

<Windows 10 Mobile デバイスの要件>

Continuum を利用するために必要な Windows 10 Mobile デバイスの要件について、下記に説明します。

ハードウェア	要件
プロセッサー	Snapdragon 617 (無線のみ対応) Snapdragon 808 Snapdragon 810
メモリ	2GB 以上
内蔵ストレージ	16GB 以上
Bluetooth	Ver 4.0 以上
Wi-Fi	IEEE802.11n デュアルバンド以上
Miracast	Windows 10 Miracast 拡張のサポート
USB	USB 2.0 以上

<無線接続の要件>

Continuum から無線接続するために必要なデバイスの要件について、下記に説明します。

ハード ウェア	要件
ディスプレイ	HDMI 対応ディスプレイ
キーボード / マウス	Bluetooth 対応
アダプター	Miracast アダプター

Note
ディスプレイが Miracast に対応している場合、HDMI 対応および、Miracast アダプターは必要ありません。

<有線接続の要件>

Continuum から有線接続するために必要なデバイスの要件について、下記に説明します。

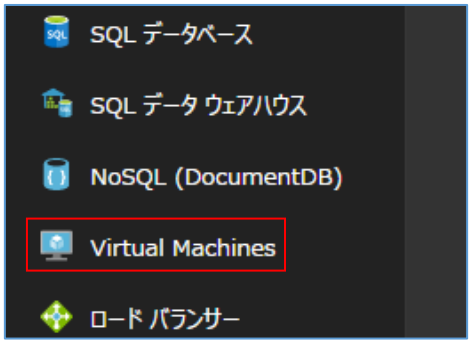
ハード ウェア	要件
ディスプレイ	HDMI 対応ディスプレイ
キーボード / マウス	Bluetooth または、USB 2.0 以上
ドッキングステーション	Acer / Liquid Jade Primo ドッキング ステーション HP / HP Elite x3 デスク ドック / ノート ドック

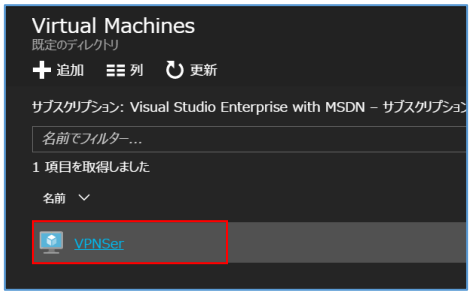
2.2.2. リモート デスクトップ セッション ホスト

ここでは、Windows 10 Mobile のリモート デスクトップ アクセスを評価するにあたって、Azure 上に Windows Server 2016 を展開していることを前提とします。Azure の仮想マシン機能を利用するためには、下記の URL から Azure の評価版に登録する必要があります。

https://azure.microsoft.com/ja-jp/free/

また、ユーザーから職場の Windows Server 2016 にリモート デスクトップ アクセスするには、リモート デスクトップ セッション ホストを構築する必要があります。ここでは Windows Server 2016 の仮想マシンを作成していることを前提に、Windows Server 2016 にリモート デスクトップ セッション ホストの役割を追加するための手順について下記に説明します。

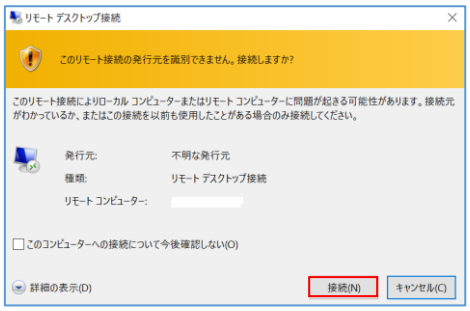
図	手順 PC
	1. https://portal.azure.com/ から、Azure ポータルに管理者アカウントでサインインします。
	2. 左メニューから、[Virtual Machines] をクリックします。



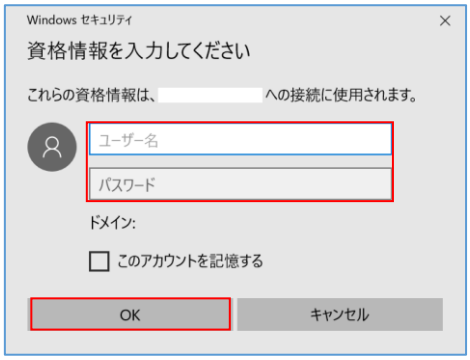
3. [Virtual Machines] から、作成した仮想マシンを選択します。

4. [接続] をタップします。
5. 「servername.rdp を開くか、または保存しますか？」と表示されたら、[ファイルを開く] をクリックし、リモート デスクトップを起動します。

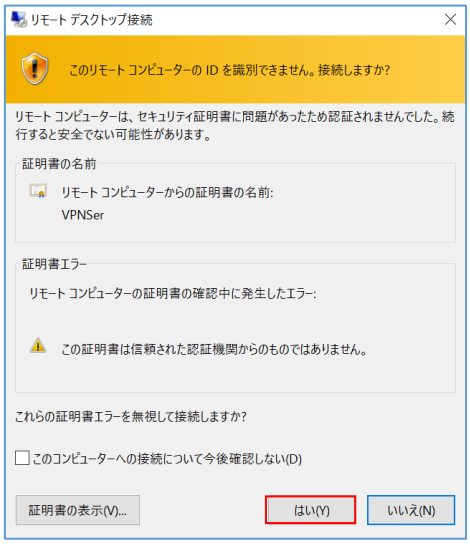
アプリ遷移



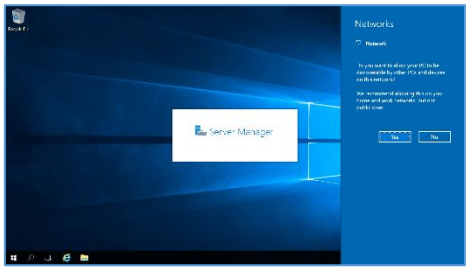
6. 「このリモート接続の発行元を識別できません。接続しますか？」と表示されたら、[接続] をクリックします。



7. 仮想マシンの作成時に入力した資格情報を入力し、[OK] をクリックします。

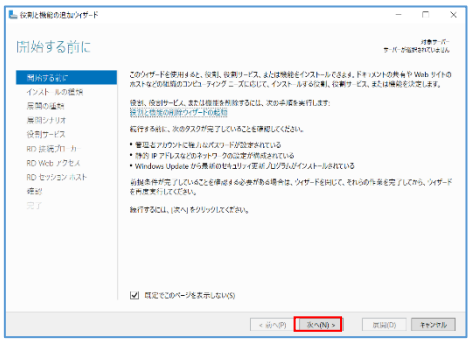


8. 「このリモート コンピューターの ID を識別できません。接続しますか？」と表示されたら、[はい] をクリックします。

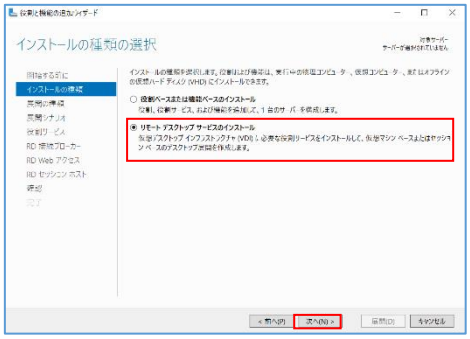


9. Windows Server 2016 が正常に起動することを確認します。

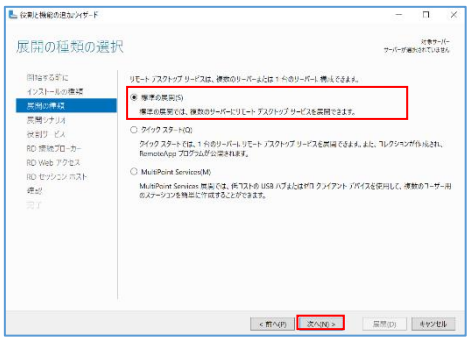
10. [サーバーマネージャー] の [ダッシュボード] > [管理] > [役割と機能の追加] をクリックします。



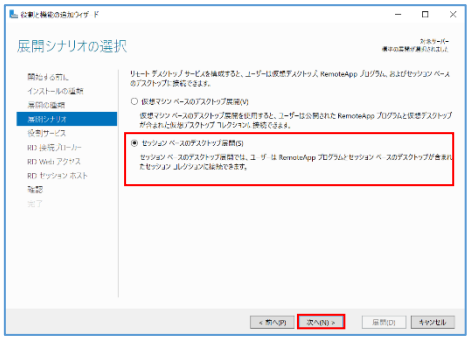
11. [役割と機能の追加ウィザード] 画面で、[次へ] をクリックします。



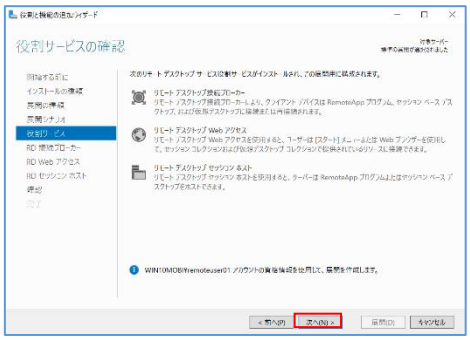
12. [インストール種類の選択] 画面で、[リモート デスクトップ サービスのインストール] を選択し、[次へ] をクリックします。



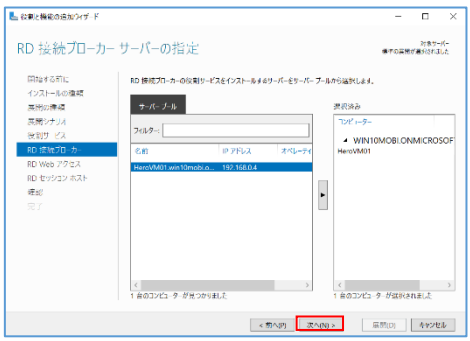
13. [展開の種類の選択] 画面で、[標準の展開] を選択し、[次へ] をクリックします。



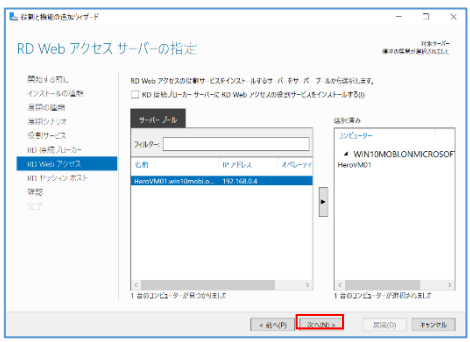
14. [展開シナリオの選択] 画面で、[セッションベースのデスクトップ展開] を選択し、[次へ] をクリックします。



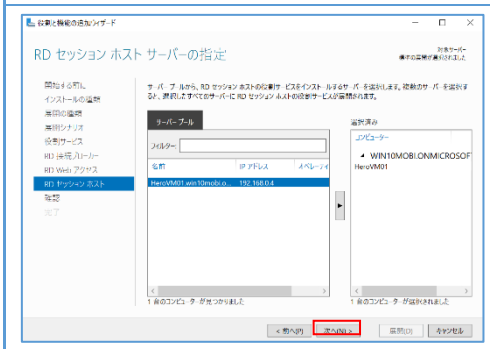
15. [役割サービスの確認] 画面で、[次へ] をクリックします。



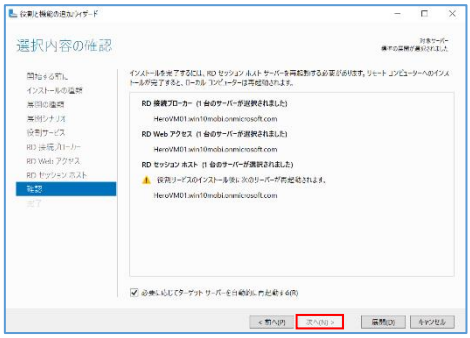
16. [RD 接続ブローカーサーバー] 画面で、接続先サーバーを選択し、[次へ] をクリックします。



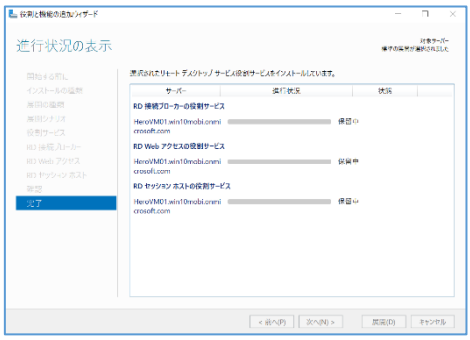
17. [RD Web アクセスサーバー] 画面で、接続先サーバーを選択し、[次へ] をクリックします。



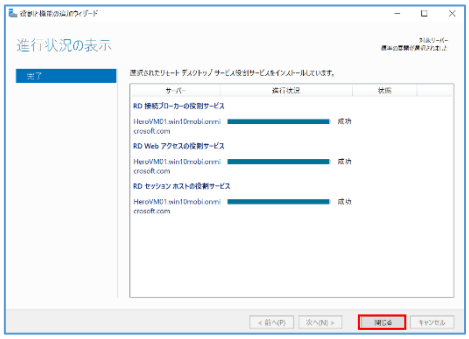
18. [RD セッションホストサーバー] 画面で、接続先サーバーを選択し、[次へ] をクリックします。



19. [選択内容の確認] 画面で内容を確認し、[次へ] をクリックします。



20. [進行状況の表示] 画面でインストールが完了するのを待ちます。

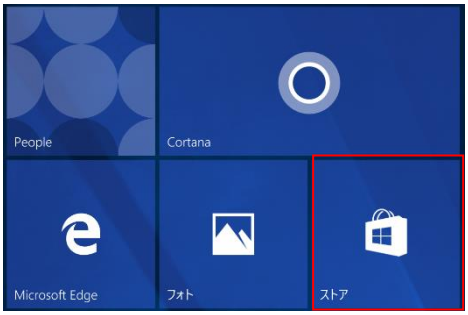
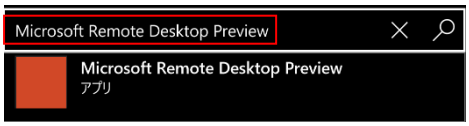
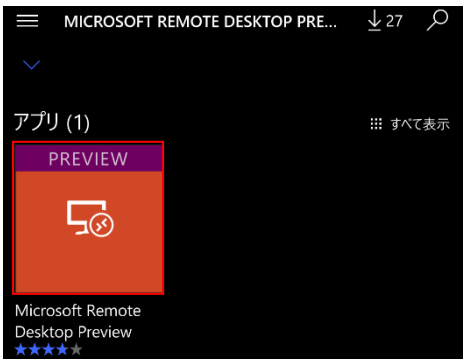


21. 完了したことを確認し、[閉じる] をクリックします。

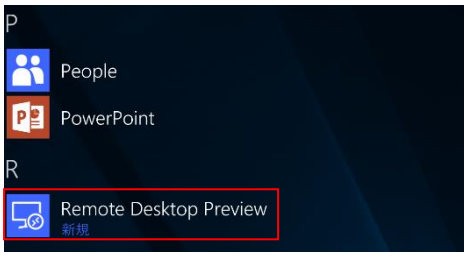
2.2.3. リモート デスクトップ クライアント

Windows 10 Mobile からリモート デスクトップ アクセスをするにはリモート デスクトップ クライアントが必要です。リモート デスクトップ クライアントを使うと、どこからでもリモート ホストに接続することができます。これにより、職場でしていた作業を引き継いで、外出先から続きをするといった利用が可能になります。また、アプリを起動した状態のリモート ホストに接続して、そのまま操作することもできます。ここではリモート デスクトップ クライアントを Windows ストアからインストールする手順について、下記に説明します。

> **Note**
> 2017 / 2 現在、RD クライアントは Preview 版のみ Continuum に対応します。

図	手順 Mobile
	1. Windows 10 Mobile デバイスから、[ストア] を起動します。
	2. 検索窓に「Microsoft Remote Desktop Preview」と入力し、検索します。
	3. [Microsoft Remote Desktop Preview] をタップします。
	4. [インストール] をタップし、アプリをインストールします。

5. インストールが完了するまで待ちます。



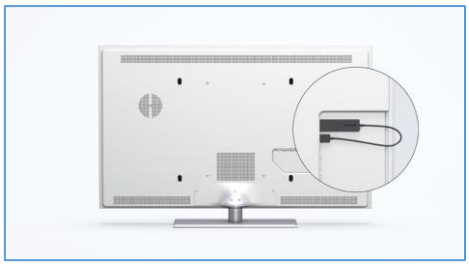
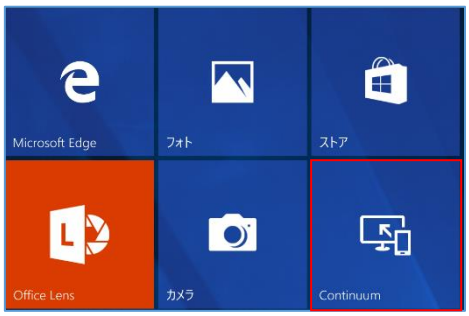
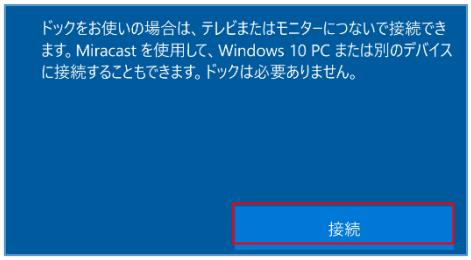
6. [すべてのアプリ] に Microsoft Remote Desktop Preview が追加されていることを確認します。

2.3. 実践

Continuum で Windows 10 Mobile を PC のように操作し、リモート デスクトップで Windows Server 2016 にアクセスする実践の手順について説明します。

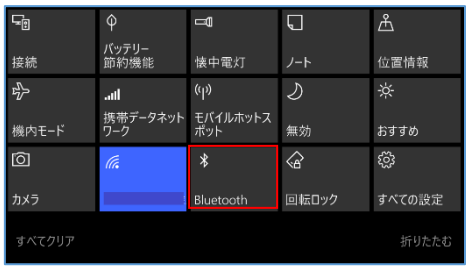
2.3.1. Continuum 接続

Continuum で外部ディスプレイに無線接続し、Windows 10 Mobile を PC のように操作する手順について、下記に説明します。

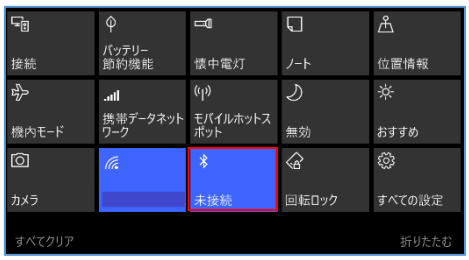
図	手順 Mobile
	1. 接続する外部ディスプレイに Miracast アダプターを接続し、電源を入れます。 **Note** Continuum 対応のアダプターであれば、Microsoft 製品でなくても動作します。
	2. Windows 10 Mobile デバイスから、Continuum を起動します。
	3. [ワイヤレス アダプター] を選択します。
	4. [接続] をタップします。

5. 接続の一覧から、外部ディスプレイに表示されている受信機名を探し、タップします。

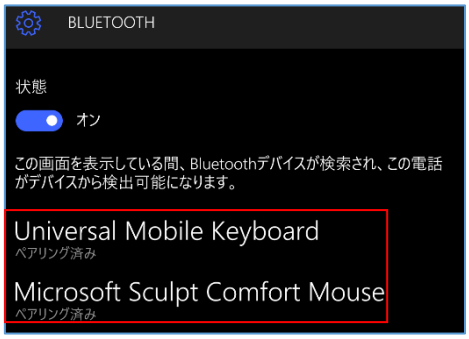
6. 外部ディスプレイに Windows 10 のスタート画面が表示されていることを確認します。



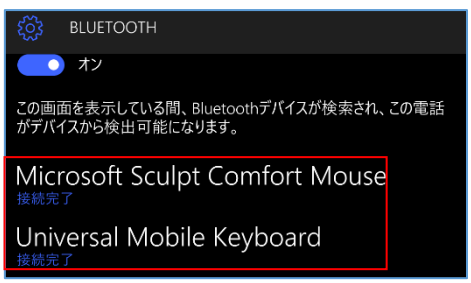
7. さらに Bluetooth でマウス、キーボードを接続するため、Windows 10 Mobile デバイスから、アクション センターを開き、Bluetooth をオンにします。



8. Bluetooth のパネルを数秒間タップし、Bluetooth の設定画面を開きます。



9. 使用するマウス、キーボードをタップして、ペアリングします。

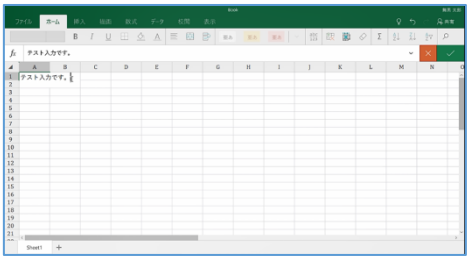


10. [接続完了] と表示されていることを確認します。

外部ディスプレイ

11. 外部ディスプレイから、マウス、キーボードを使って操作ができることを確認します。

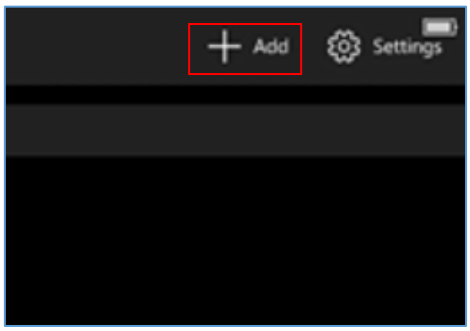
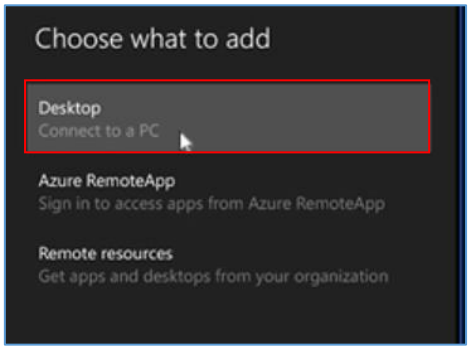
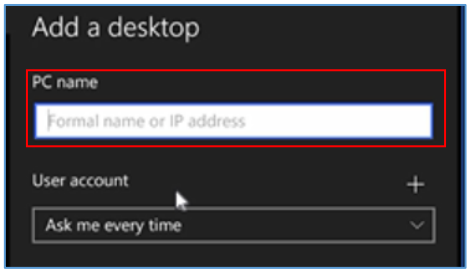
12. [Excel] をクリックします。

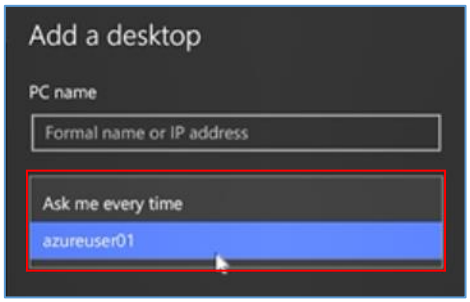


13. [Excel] が起動し、PC のように操作できることを確認します。

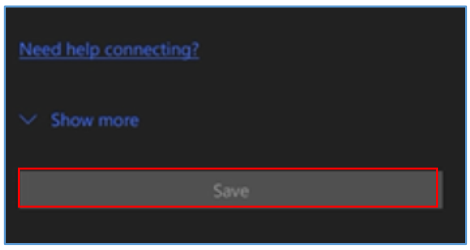
2.3.2. リモート デスクトップ アクセス

Windows 10 Mobile から職場のリモート デスクトップ ホストにリモート デスクトップ アクセスするための手順について下記に説明します。

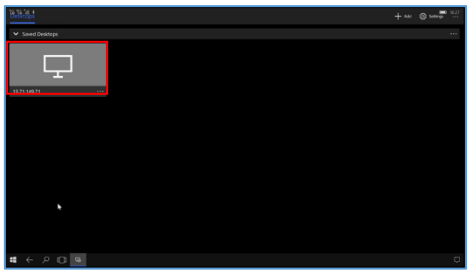
図	手順 外部ディスプレイ
	1. Windows 10 Mobile から Continuum で外部ディスプレイに接続します。 2. スタート画面から、[すべてのアプリ] をクリックします。
	3. 「2.2.2. リモート デスクトップ クライアント」でインストールした [Remote Desktop Preview] を起動します。
	4. [Add] をクリックします。
	5. [Desktop] をクリックします。
	6. [PC name] を入力します。



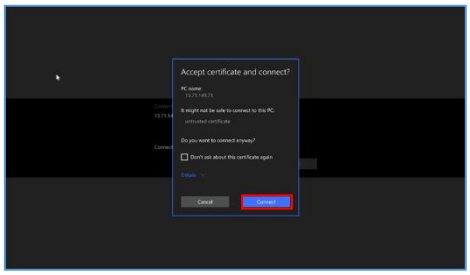
7. [User account] を追加または選択します。



8. [Save] をクリックします。



9. 画面に追加された リモート デスクトップをダブルクリックします。



10. [Connect] をクリックします。

11. 接続に成功したことを確認します。

3. シナリオ 2 「Office 365 との連携」

Windows 10 Mobile では、Windows 10 PC と同じように Word、Excel、PowerPoint などの Office アプリを利用することができます。これらは、Windows 10 Mobile デバイスの小さな画面に最適化されるため、モバイル環境でも快適な操作が実現します。また、本書のシナリオ 1「Continuum for Phone」で記載した Continuum を利用することで、Windows 10 PC と同等の操作感で作業することもできます。

さらに、Office 365 と連携することで、便利なクラウド サービスを利用することができます。例えば、OneDrive for Business を導入すれば、職場で作業途中だった Excel ファイルを、クラウド ストレージ上に保存して、通勤や移動の時間に作業するといった、時間や場所に縛られないワークスタイルを実現します。さらに、シングル サインオンによって、デバイスを認証するだけで ID やパスワードを入力することなく Office 365 にサインインすることができます。これは、手打ち入力に弱いモバイル デバイスとも相性が良く、生産性の向上に繋がります。

また、Windows Information Protection (以下、WIP) や Conditional Access を設定すれば、よりセキュアな運用が可能です。

Note
Office 365 を商用利用するには、法人向けまたは一般向けの Office 365 ライセンスの契約が必要となります。

3.1. 概要

本章では、Windows 10 Mobile の利便性およびセキュリティを評価するため、下記の準備および実践を行います。

3.1.1. シングル サインオン

Windows 10 Mobile では、Azure Active Directory(以下、Azure AD) アカウントをデバイスに登録することにより、Office 365 などの、さまざまなアプリケーションおよびリソースにシングル サインオンすることが可能です。そのため、ユーザーはアカウント認証を意識することなく、業務に必要なアプリケーションを利用することができます。

3.1.2. OneDrive for Business

OneDrive for Business は、Office 365 のクラウドストレージとして機能します。これにより、ユーザーは作業途中のファイルを OneDrive for Business に保存して、別のデバイスから編集したり、他のユーザーと共有したりすることができます。

本章では、Windows PC から OneDrive for Business に保存したファイルを、Windows 10 Mobile で開いて編集する手順について説明します。

3.1.3. WIP

WIP は、組織のデータにアクセスできるアプリを制御したり、ファイルを暗号化したりすることで、強固な情報保護を実現します。これは、Microsoft Intune などの MDM (以下、MDM) にデバイスを登録し、WIP ポリシーを適用することで機能します。これにより、WIP を設定するアプリで作成された、すべてのデータに WIP ポリシーが適用されます。

例えば、WIP ポリシーが適用した Word では、組織のファイルの内容をコピーして SNS に貼り付けようとしたり、メールに添付して送信したりしても、暗号化され他のデバイスからは開くことができないので、情報漏洩を防止することができます。これは、WIP が自動的に組織のデータと個人のデータを切り分け、ファイルを暗号化しているためです。

本章では、Microsoft Intune で WIP ポリシーを作成、展開し、Windows 10 Mobile でポリシーが適用されていることを確認する手順について説明します。

3.1.4. Conditional Access

Conditional Access は、Azure AD の条件付きアクセス制御機能です。利用には Azure AD Premium のライセンスが必要であるため、評価には下記 URL から、Azure AD Premium の無料試用版を有効化します。

https://azure.microsoft.com/ja-jp/trial/get-started-active-directory/

Office 365 は通常、アカウントの ID とパスワードがあれば、どのデバイスからでもサインインすることができます。しかし、組織で管理されていないデバイスから Office 365 にサインインできると、情報漏洩の危険性があります。このような場合には、Conditional Access を設定して、組織によって管理されたデバイスでしか Office 365 にサインインできないようにします。これにより、アカウントの ID とパスワードが流出してしまったとしても、組織に管理されないデバイスから Office 365 にサインインすることができないため、情報は保護されます。そのため、組織はセキュアにモバイル デバイスを運用することが可能になります。

本章では、Azure AD で Conditional Access を設定、展開し、Windows 10 Mobile で設定が適用されていることを確認する手順について説明します。

3.2. 準備

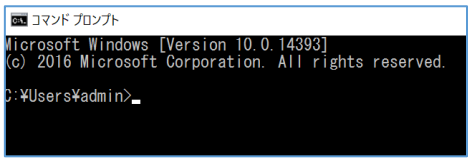
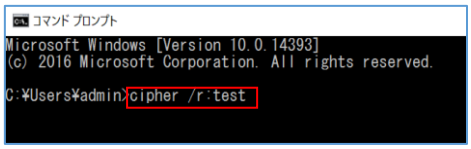
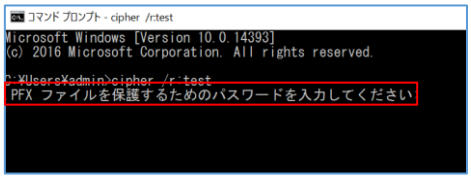
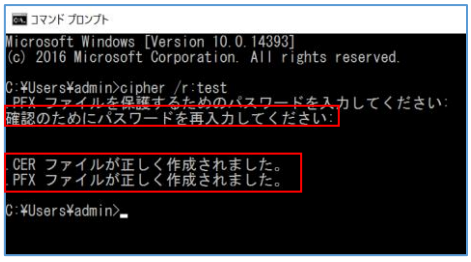
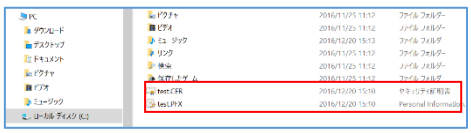
WIP ポリシーを作成するには、DRA 証明書が必要です。DRA 証明書は、Windows 10 PC にログオンし、コマンド プロンプトから作成します。また、WIP ポリシーは Microsoft Intune で作成し、各デバイスに展開します。

Conditional Access は、Azure AD premium から有効化します。

ここでは、WIP と Conditional Access を評価するための準備として、これらの手順について説明します。

3.2.1. DRA 証明書

WIP ポリシーを作成するために必要な DRA 証明書を作成する手順について下記に説明します。すでに DRA 証明書を持っている場合は、この手順をスキップします。

図	手順 PC
	1. コマンド プロンプトを起動します。
	2. 「cipher /r:<EFSRA>」と入力します。 ※<EFSRA> の部分は、作成する .cer および .pfx ファイルの名前になります。
	3. 「.PFX ファイルを保護するためのパスワードを入力してください」と表示されたら、したがってパスワードを入力します。
	4. 「確認のためにパスワードを再入力してください」と表示されたら、したがってパスワードを入力し、エンター キーを押します。 5. 「.CER ファイルが正しく作成されました。」、「.PFX ファイルが正しく作成されました。」と表示されていることを確認します。
	6. 手順 2 のディレクトリに移動し、ファイルが作成されていることを確認します。

3.2.2. アプリの発行元・製品名の取得

<WIP 対応アプリ>

WIP ポリシーを作成するには、WIP に対応するアプリの [発行元]、[製品名]、[アプリの種類] の情報が必要になります。ここでは、WIP に対応する代表的なアプリの情報について、下記に説明します。

製品名	アプリの情報
Microsoft Edge	発行元:CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US 製品名: Microsoft.MicrosoftEdge アプリの種類: ユニバーサル アプリ
Microsoft People	発行元:CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US 製品名: Microsoft.People アプリの種類: ユニバーサル アプリ
Word Mobile	発行元:CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US 製品名: Microsoft.Office.Word アプリの種類: ユニバーサル アプリ
Excel Mobile	発行元:CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US 製品名: Microsoft.Office.Excel アプリの種類: ユニバーサル アプリ
PowerPoint Mobile	発行元:CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US 製品名: Microsoft.Office.PowerPoint アプリの種類: ユニバーサル アプリ
OneNote	発行元:CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US 製品名: Microsoft.Office.OneNote アプリの種類: ユニバーサル アプリ
Outlook メール/カレンダー	発行元:CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US 製品名: microsoft.windowscommunicationsapps アプリの種類: ユニバーサル アプリ

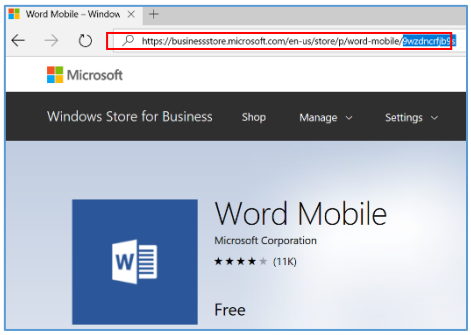
Microsoft フォト	発行元:CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US 製品名: Microsoft.Windows.Photos アプリの種類: ユニバーサル アプリ
Groove ミュージック	発行元:CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US 製品名: Microsoft.ZuneMusic アプリの種類: ユニバーサル アプリ
Microsoft 映画 & テレビ	発行元:CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US 製品名: Microsoft.ZuneVideo アプリの種類: ユニバーサル アプリ
Microsoft メッセージング	発行元:CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US 製品名: Microsoft.Messaging アプリの種類: ユニバーサル アプリ

参考 URL : https://technet.microsoft.com/ja-jp/itpro/windows/keep-secure/enlightened-microsoft-apps-and-wip

<アプリの情報を調べる>

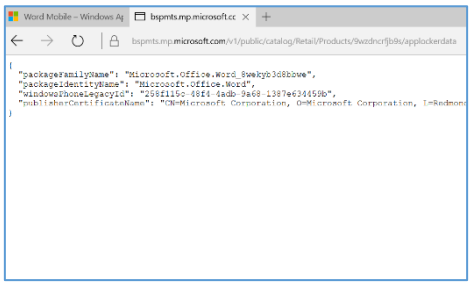
<WIP 対応アプリ>に記載したアプリ以外の情報を調べる手順について、下記に説明します。

図	手順 PC
	1. 追加するアプリ発行元名と製品名を調べため、https://businessstore.microsoft.com/en-us/store/apps から、ビジネス向け Windows ストアに管理者アカウントでサインインします。
	2. 追加するアプリを検索し、クリックします。ここでは例として、「Word Mobile」を選択します。

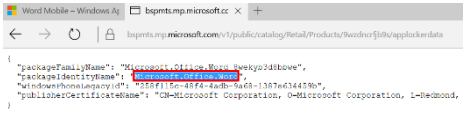


3. アプリの URL から ID 値をコピーします。
https://businessstore.microsoft.com/en-us/store/p/word-mobile/9wzdncrfjb9s
の「9wzdncrfjb9s」をコピーします。

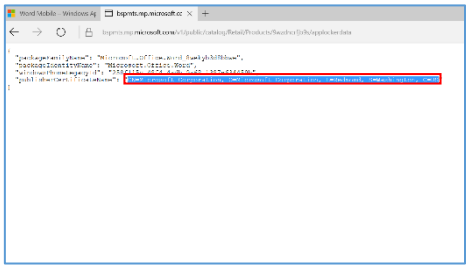
サイト遷移



4. ビジネス向けストアポータルの WebAPI を実行し、発行元と製品名を調べるため、
https://bspmts.mp.microsoft.com/v1/public/catalog/Retail/Products/9wzdncrfjb9s/applockerdata にアクセスします。URL の「9wzdncrfjb9s」の部分は、手順 10 でコピーした ID を指定します。



5. 製品名を取得するため、packageIdentityName の値をメモします。ここでは、
「Microsoft.Office.Word」をメモします。



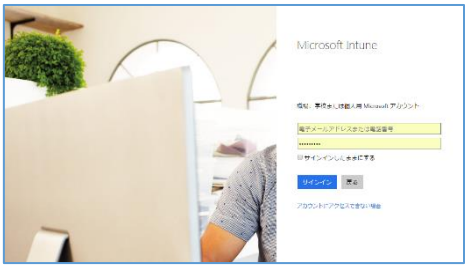
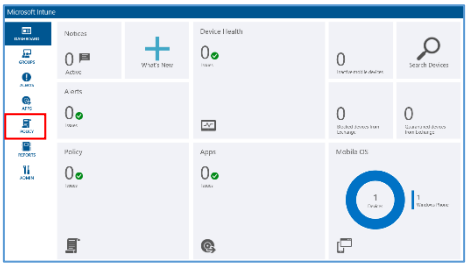
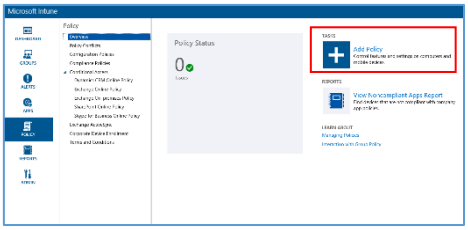
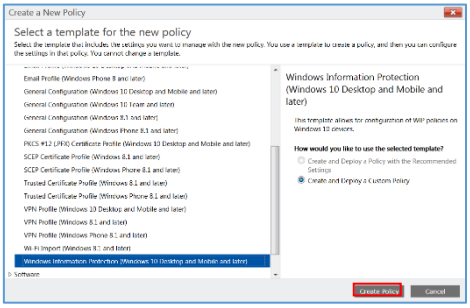
6. 発行元名を取得するため、publisherCertificateName の値をメモします。ここでは、「CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US」をメモします。

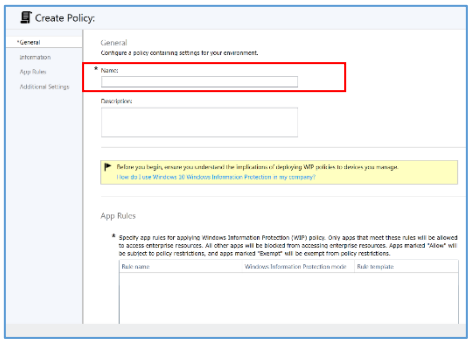
3.2.3. WIP の作成および展開

> **Note**
> 2017 / 2 現在、Microsoft Intune では、WIP ポリシーが日本語 UI 環境でサポートされていません。そのため、WIP ポリシーを作成するには、PC の言語設定を英語にする必要があります。

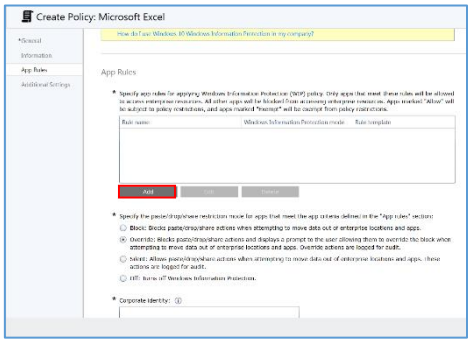
<WIP ポリシーの作成および展開>

ここでは、「3.2.1. DRA 証明書」、「3.2.2. アプリの発行元・製品名の取得」で取得した証明書、アプリの情報を基に、Intune から WIP ポリシーを作成および展開するまでの手順について説明します。

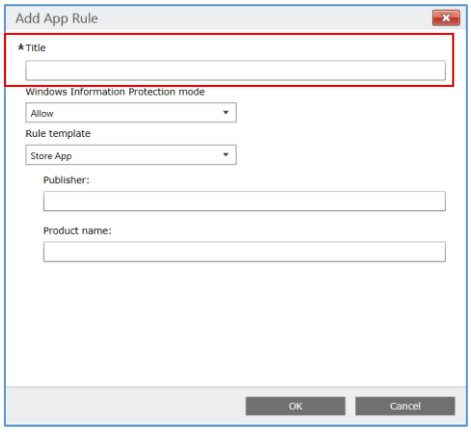
図	手順 PC
	1. http://admin.manage.microsoft.com/ から、Microsoft Intune に管理者アカウントでサインインします。
	2. 左メニューから [POLICY] をクリックします。
	3. [Add Policy] をクリックします。
	4. [Windows] > [Windows Information Protection (Windows 10 Desktop and Mobile and later)] の順に展開し、[Create Policy] をクリックします。



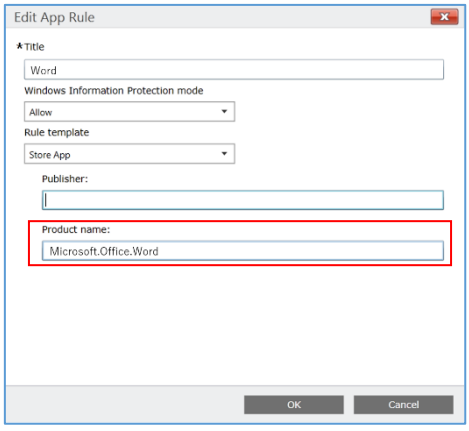
5. [General] > [Name] に、作成するポリシーの名前を入力します。



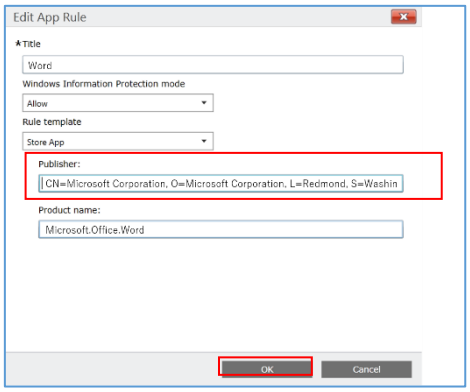
6. [App Rules] から、[Add] をクリックします。



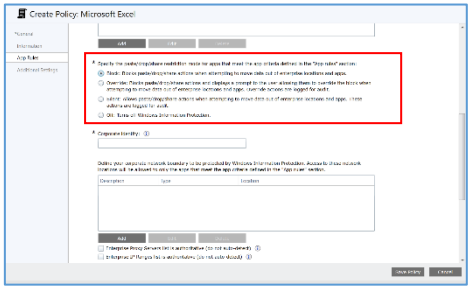
7. [Add App Rule] > [Title] に、追加するアプリのタイトルを入力します。



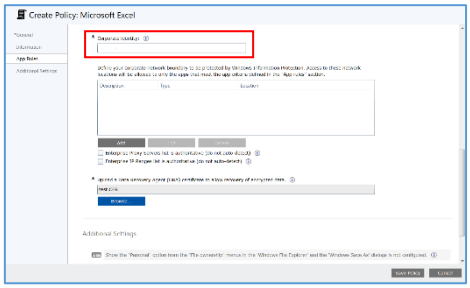
8. [Add App Rule] > [product name] に、製品名を入力します。ここでは、「Microsoft.Office.Word」と入力します。



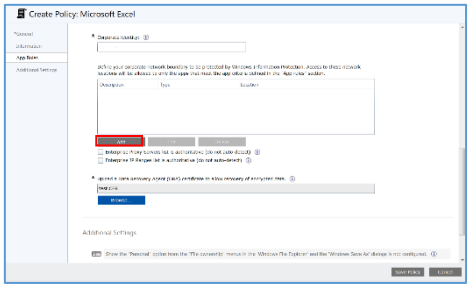
9. [Add App Rule] > [publisher] に、発行元を入力します。ここでは、「CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US」と入力します。
10. 入力した値を確認し、[OK] をクリックします。



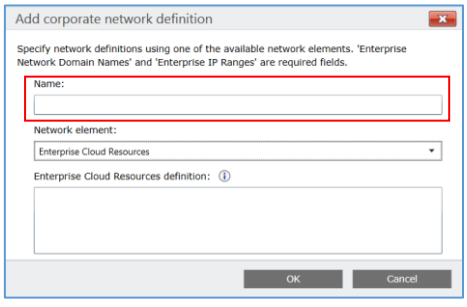
11. [App Rules] のラジオ ボタンで、[Block]、[Override]、[Silent]、[Off] から、アプリに対する貼り付け / ドロップ / 共有の制限モードを指定します。



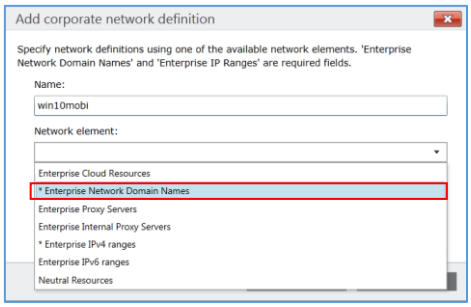
12. [Corporate Identity] に、会社の ID (推奨地 : ドメイン) を入力します。



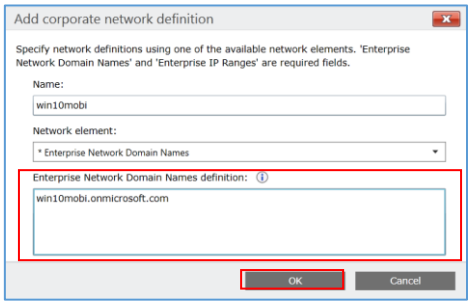
13. [Add] をクリックします。



14. [Name] に分かりやすい名前を入力します。



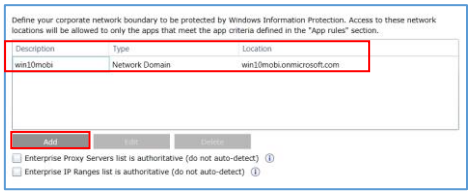
15. [Network element] から [Enterprise Network Domain Names] を選択します。



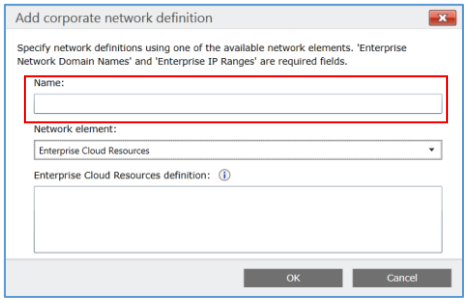
16. [Enterprise Network Domain Names definition] に組織の FQDN を入力します。

> **Note**
> 複数指定する場合は、”,” (カンマ) を区切り文字として指定します。

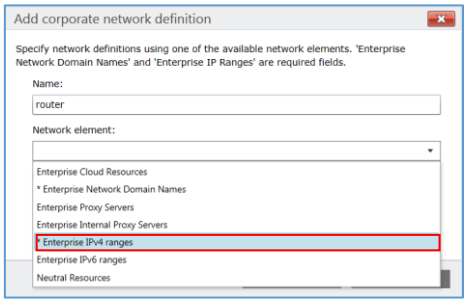
17. [OK] をクリックします。



18. 追加されたリストが表示されていることを確認したら、再度 [Add] をクリックします。

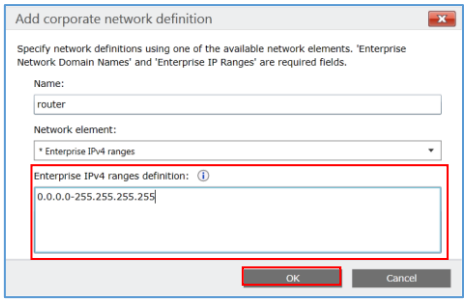


19. [Name] に分かりやすい名前を入力します。

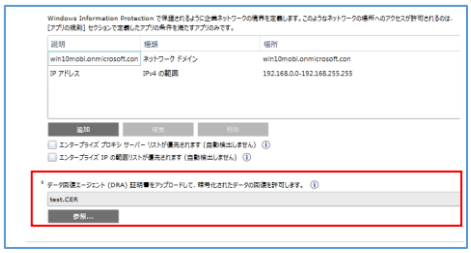


20. [Network element] から [Enterprise IPv4 ranges] を選択します。

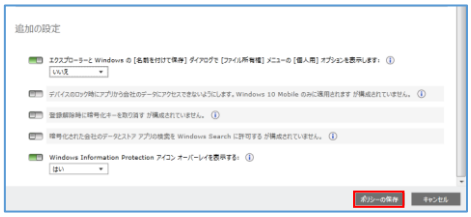
> **Note**
> IPv4 を使用しない場合は、[Enterprise IPv6 ranges] を選択します。



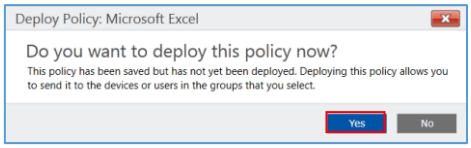
21. [Enterprise IPv4 ranges definition] に、イントラネット内で有効な IPv4 値の範囲のアドレスを入力します。
22. [OK] をクリックします。



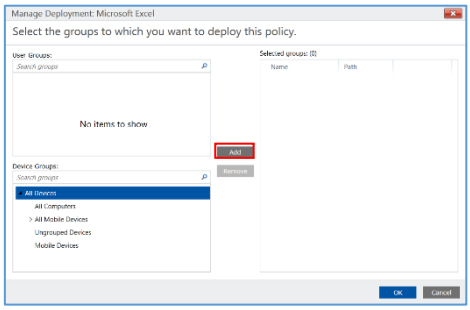
23. DRA 証明書をアップロードします。



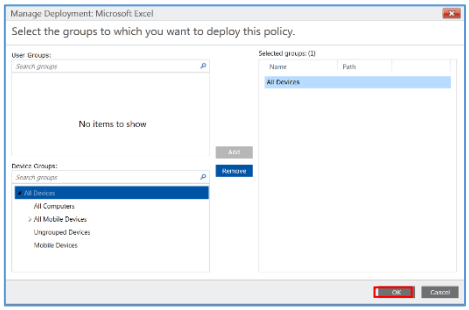
24. [additional settings] で、任意の構成をします。
25. [save policy] をクリックします。



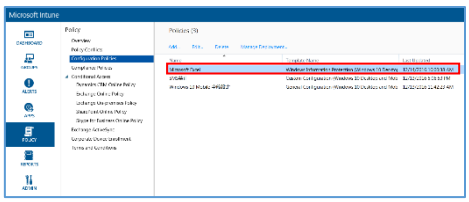
26. [Yes] をクリックします。



27. [All Devices] を選択し、[Add] をクリックします。



28. [OK] をクリックします。



29. [Configuration Policies] に、作成したポリシーが追加されていることを確認します。

Note

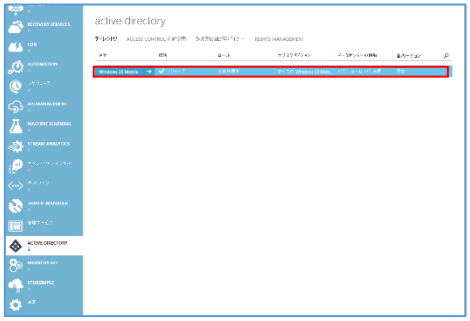
手順 24 の [additional settings] では、「Show the “Personal” option from the “File ownership” menus in the ‘Windows File Explorer’ and the ‘Windows Save As’ dialogs」を [No] に構成することで、組織のアプリで作成したドキュメントを作業用でのみ保存させることができます。[Yes] を設定した場合、ユーザーは個人用としてファイルを保存することができるようになります。個人用として保存したファイルには、WIP ポリシーが適用されません。

3.2.4. Azure AD Premium

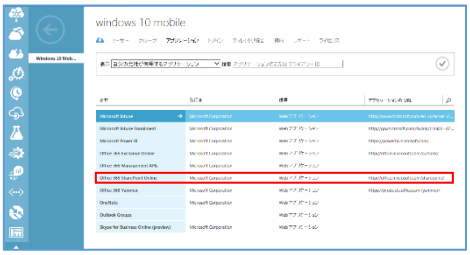
Conditional Access を設定するには、Azure クラシック ポータルから制御するデバイスを指定する必要があります。

<Conditional Access の設定>

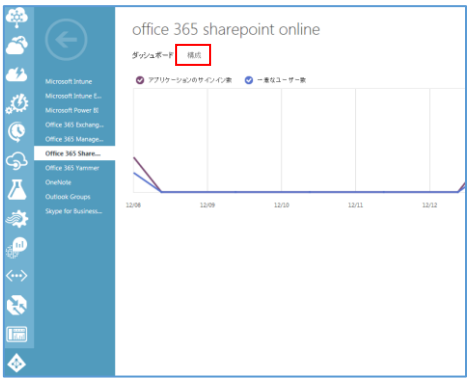
Azure クラシックポータル から Conditional Access を設定する手順について下記に説明します。ここでは、組織のアカウントが流出してしまった場合にも情報が保護されることを評価するため、Windows 10 Mobile デバイスに登録されている Azure AD アカウントに対し、そのデバイスでのみ Office 365 にアクセスできるよう、Office 365 SharePoint Online に条件付きアクセス制限を設定します。

図	手順 PC
	1. https://manage.windowsazure.com/ から、Azure クラシックポータルに管理者アカウントでサインインします。
	2. 左メニューから [ACTIVE DIRECTORY] をクリックします。
	3. ディレクトリを選択します。

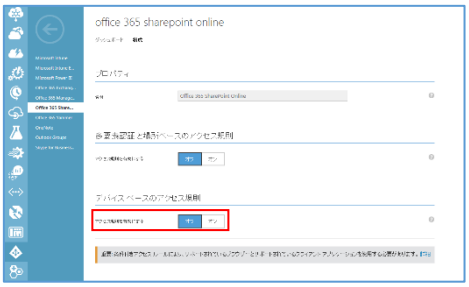
4. [アプリケーション] タブをクリックします。



5. [Office 365 SharePoint Online] を選択します。



6. [構成] タブをクリックします。



7. [デバイス ベースのアクセス規制] をオンにします。

8. [適用対象] の項目から、[グループ] を選択します。

9. [グループの追加] をクリックします。

10. 適用するデバイス グループを選択します。

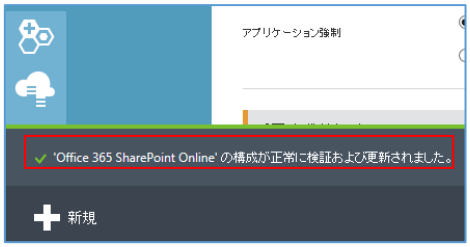
11. 画面右下のチェックマークをクリックして、グループの追加を完了します。

12. [適用対象] の項目に、追加したグループ名が表示されていることを確認します。

13. [デバイス ルール] の項目から、準拠するデバイスを定義します。ここでは、[すべてのデバイスに準拠している必要があります] を選択し、[Windows デバイス準拠の条件] 下のドロップダウン リストから [ドメイン参加済みまたはポリシーに準拠] を選択します。

14. [アプリケーション強制] から、適用する環境を選択します。ここでは、[ブラウザーとネイティブ アプリケーション用] を選択します。

15. [保存] をクリックします。



16. 「'Office 365 SharePoint Online' の構成が正常に検証および更新されました。」と表示されていることを確認します。

Note

各設定項目の詳細は、下記の URL を参考にしてください。

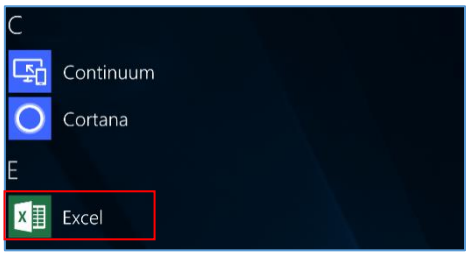
https://docs.microsoft.com/ja-jp/azure/active-directory/active-directory-conditional-access

3.3. 実践

ここでは、OneDrive for Business を利用したファイル共有と、3.2. 準備で設定したポリシーが正常に適用されているかを確認するための実践手順について説明します。

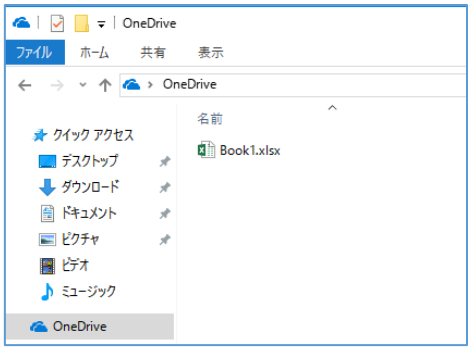
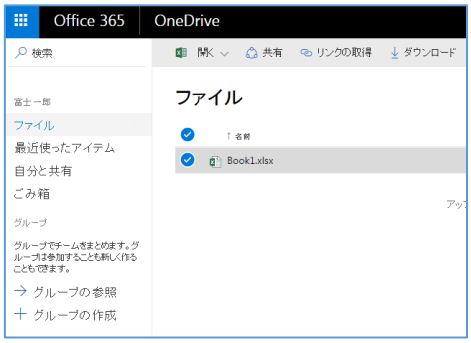
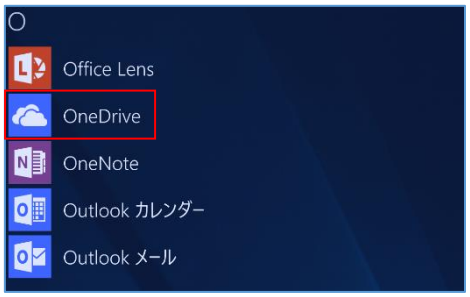
3.3.1. シングル サインオン

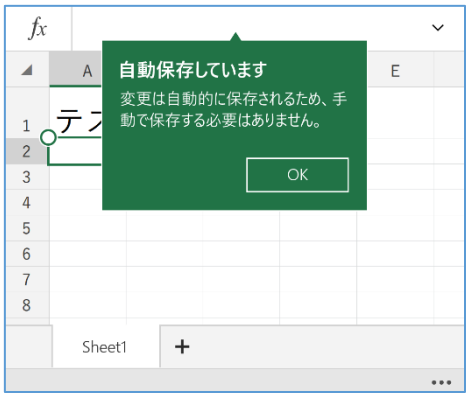
Windows 10 Mobile で、シングル サインオンを確認する手順について下記に説明します。

図	手順 Mobile
	1. Windows 10 Mobile デバイスを起動し、セットアップ時に設定した PIN を入力します。
	2. Office アプリを起動します。ここでは例として、Microsoft Excel を起動します。
	3. アカウント情報を入力することなくサインインできることを確認します。

3.3.2. OneDrive for Business でのファイル共有

職場で保存したファイルを Windows 10 Mobile から起動して編集する手順について、下記に説明します。

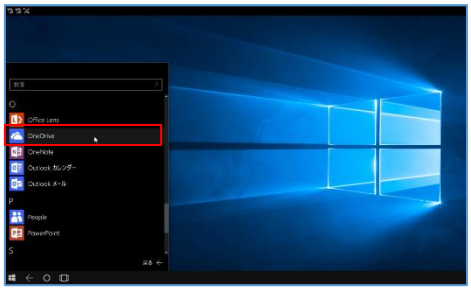
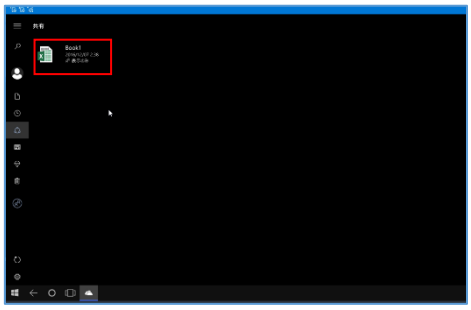
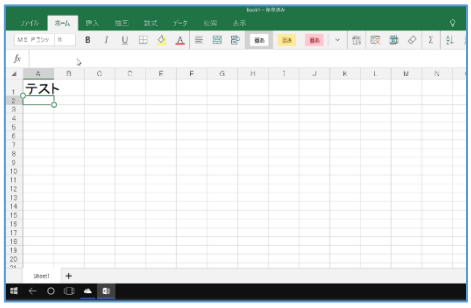
図	手順 PC
	1. Wndows 10 PC で作成した Excel ファイルを、OneDrive に保存します。
	2. クラウド上の OneDrive と同期されていることを確認します。
Mobile	
	3. Windows 10 Mobile デバイス から OneDrive を起動します。
	4. PC で保存した Excel ファイルがあることを確認し、ファイルを開きます。



5. 正常に起動することを確認します。変更を加えると、自動保存されます。

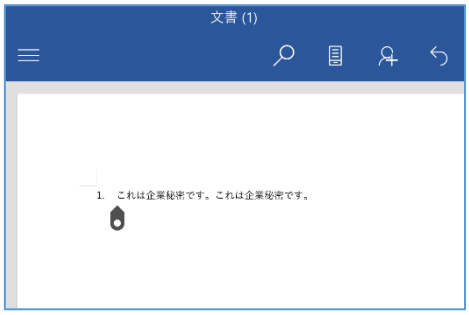
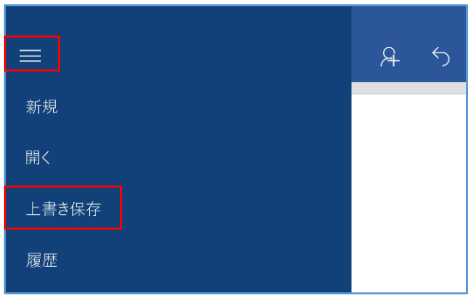
<Continuum で起動する場合>

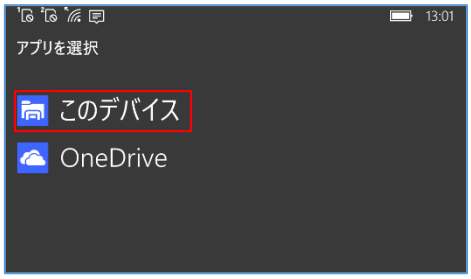
Continuum 接続で外部ディスプレイに表示させながら OneDrive のファイルを編集する手順について、下記に説明します。

図	手順 Mobile
	1. Windows 10 Mobile を Continuum で外部ディスプレイに接続し、スタート メニューから [すべてのアプリ] をクリックします。
	2. [OneDrive] をクリックします。
	3. 共有したファイルをクリックします。
	4. 正常に起動することを確認します。

3.3.3. WIP

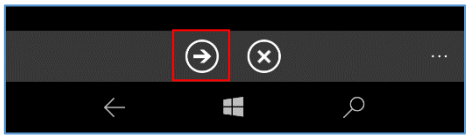
3.2.2. Microsoft Intune で作成した WIP ポリシーが正常に機能しているか確認する手順について、下記に説明します。ここでは、ユーザーが Word の内容を Twitter にコピーしようとした場合を想定します。

図	手順 Mobile
	1. Windows 10 Mobile デバイスから、[Word] を起動します。
	2. [新規作成] から、テスト用のファイルを作成します。
	3. [メニュー] から、[上書き保存] をタップします。
	4. [このファイルのコピーの保存] をタップします。 **Note** 規定の保存先への自動保存の場合、ファイルの所有権は [個人] になるため、WIP は適用されません。



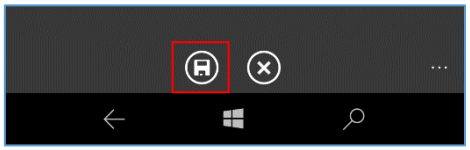
5. [このデバイス] をタップします。

6. 保存先のフォルダーを選択します。

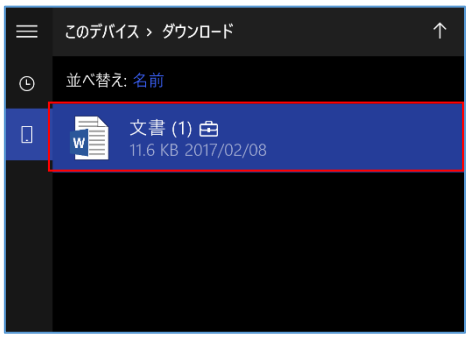


7. ボタンをタップします。

8. [ファイルの所有権] が、組織の FQDN になっていることを確認します。



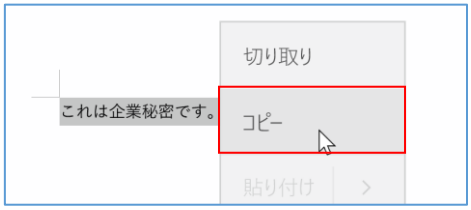
9. ボタンをタップします。



10. [エクスプローラー] から、保存したファイルを開きます。

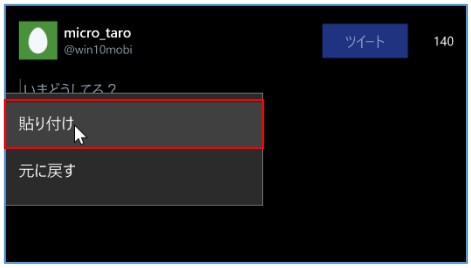
Note

3.2.2. WIP の手順 24 で、「Show the Windows Information Protection icon overlay」を [Yes] で構成した場合、WIP が適用されたファイル名の右に、 が表示されます。

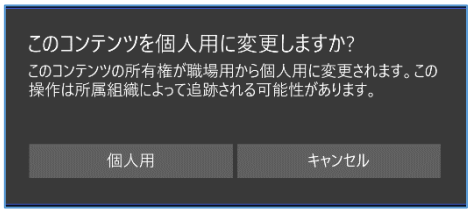


11. テキストをコピーします。

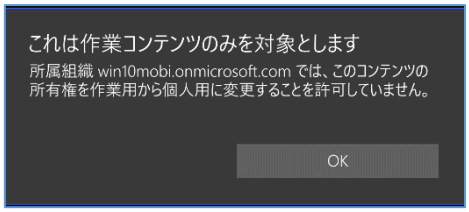
12. 別のアプリを開きます。ここでは、例として [Twitter] を起動します。



13. [ツイート] に手順 4 でコピーしたテキストを貼り付けます。



14. 3.2.2. Microsoft Intune の手順 17 で [Override] を選択した場合は、[このコンテンツを個人用に変更しますか?] と警告が表示されることを確認します。[個人用] をタップすると、貼り付けが完了します。



15. 3.2.2. Microsoft Intune の手順 17 で [Block] を選択した場合は、[これは作業コンテンツのみを対象とします] と警告が表示されることを確認します。この場合、[OK] をタップしても貼り付けは完了しません。

Note

組織のデータを個人のアプリにコピーペーストすることは制限できますが、組織のファイルを開いた状態でスクリーンショットを取得すると、その画像ファイルは暗号化されないため、添付ファイルとして送信することができます。そのため、4.2.2. カスタム構成にならって、下記の「AllowScreenCapture」ポリシーを設定し、スクリーンショット機能を制限することをお勧めします。

参考 URL : https://msdn.microsoft.com/windows/hardware/commercialize/customize/mdm/policy-configuration-service-provider#experience-allowscreencapture

設定名： AllowScreenCapture

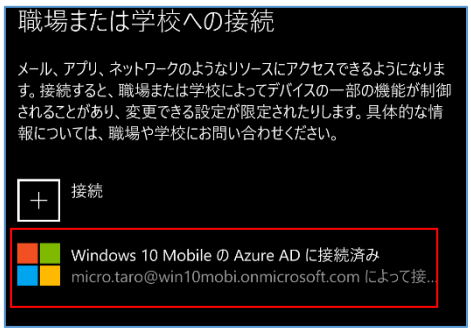
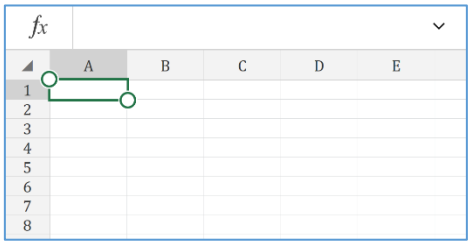
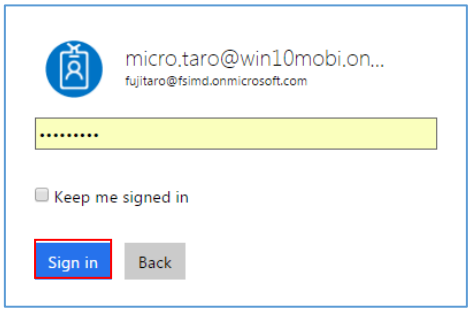
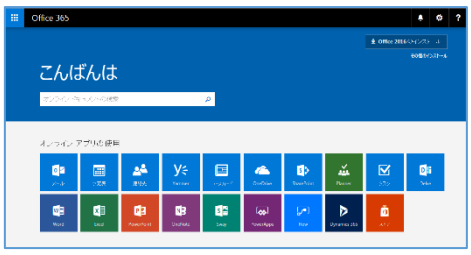
データ型：整数

OMA-URI：./Vendor/MSFT/Policy/Config/Experience/AllowScreenCapture

値：0

3.3.4. Conditional Access

Conditional Access が正常に機能しているか確認する手順について、下記に説明します。

図	手順 Mobile
	1. Windows 10 Mobile デバイスから、[設定] > [アカウント] > [職場または学校にアクセスする] の順にタップし、デバイスが準拠していることを確認します。
	2. Office アプリをタップし、正常に起動することを確認します。
PC	
	3. 準拠しない他のデバイスから、手順 1 と同じアカウントで、Office 365 にサインインします。ここでは、例として Windows 10 PC からサインインします。
	4. Office アプリをクリックします。

5. [ここからアクセスすることはできません] と表示され、アプリが起動しないことを確認します。

4. シナリオ 3 「ポリシーによる機能制限」

組織で Windows 10 Mobile を運用するにあたって、情報漏洩のリスクがあるデバイスの機能やアプリを制限したい場合があります。例えば、ユーザーの判断で、Windows ストアから業務と関係のないアプリをインストールしたり、SD カードにデータをコピーして外へ持ち出したりすることが可能な状態だと、組織で利用するのは危険です。このような場合、Microsoft Intune などの MDM にデバイスを登録して、機能を制限するためのポリシーを適用することでセキュアな運用を実現します。

4.1. 概要

4.1.1. ポリシーの作成と展開

Microsoft Intune から、モバイル デバイスの機能およびアプリを制限するには、ポリシー用のテンプレートから [全般構成] または [カスタム構成] を選択し、ポリシーを作成、展開します。[全般構成] は、GUI ベースの簡単な操作で、あらかじめ用意された項目に対して [はい]、[いいえ] の選択をするだけで設定が完了します。[カスタム構成] は、OMA-URI でポリシーを定義することで、[全般構成] よりもより細かな構成をすることができます。[カスタム構成] に必要な [OMA-URI] や [値] については、下記の URL などを参考に入力します。

- AppLocker CSP

https://msdn.microsoft.com/windows/hardware/commercialize/customize/mdm/applocker-csp

- Policy CSP (ApplicationManagement/ApplicationRestrictions)

https://msdn.microsoft.com/windows/hardware/commercialize/customize/mdm/policy-configuration-service-provider

- Microsoft Intune での Windows 10 デバイス向けの Intune ポリシー設定

https://docs.microsoft.com/ja-jp/intune/deploy-use/windows-10-policy-settings-in-microsoft-intune

本章では、全般構成およびカスタム構成のポリシーを作成、展開する手順について説明します。

4.1.2. 確認

Microsoft Intune から展開したポリシーで Windows 10 Mobile で機能およびアプリが制限されることを評価するためには、実際にポリシーが適用され機能およびアプリが制限されていることを確認する必要があります。

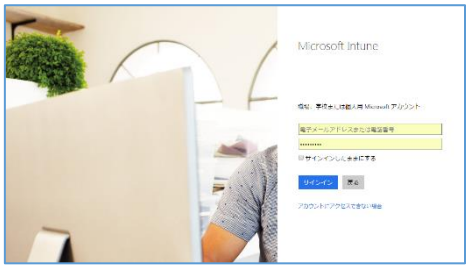
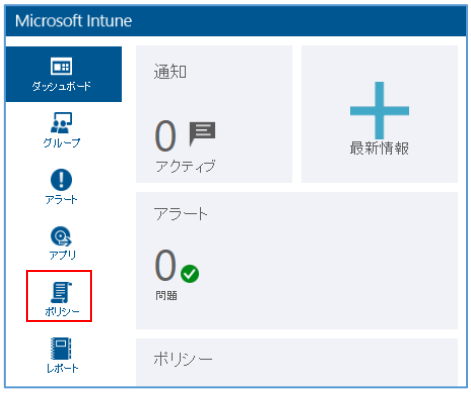
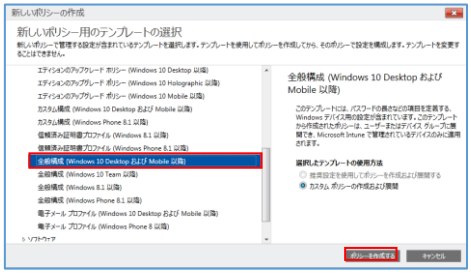
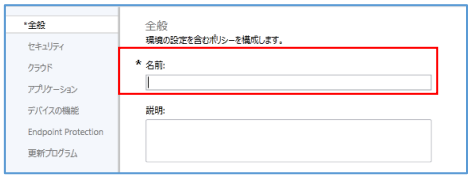
本章では、Microsoft Intune から展開したポリシーが Windows 10 Mobile 適用されていることを確認する手順について説明します。

4.2. 準備

ここでは、Microsoft Intune のポリシーによる機能制限を評価するため、全般構成とカスタム構成のポリシー作成手順について説明します。

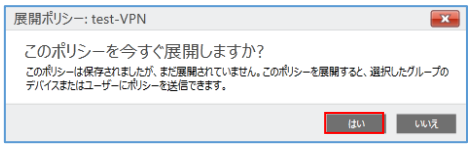
4.2.1. 全般構成

Microsoft Intune から、全般構成のポリシーを作成する手順について、下記に説明します。

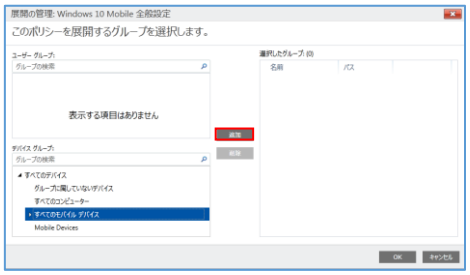
図	手順 PC
	1. http://admin.manage.microsoft.com/ から、Microsoft Intune に管理者アカウントでサインインします。
	2. 左メニューから [ポリシー] をクリックします。
	3. [ポリシーの追加] をクリックします。
	4. [Windows] > [全般構成 (Windows 10 Desktop および Mobile 以降)] を選択し、 [ポリシーを作成する] をクリックします。
	5. [ポリシーの作成] から [名前] を入力します。

6. 制限したい機能を探し、構成します。

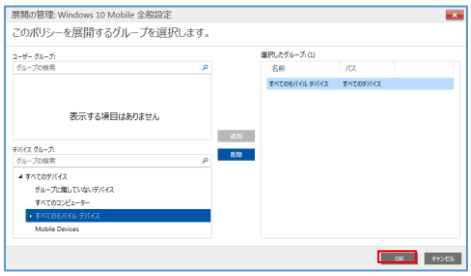
7. 画面右下から、[ポリシーの保存] をクリックします。



8. [はい] をクリックします。



9. デバイス グループから、ポリシーを展開するデバイス グループを選択し、[追加] をクリックします。

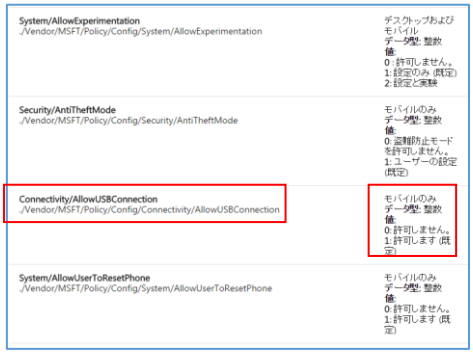
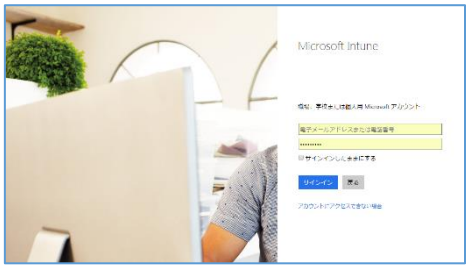
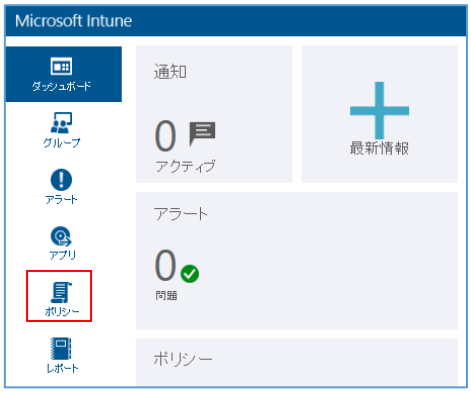


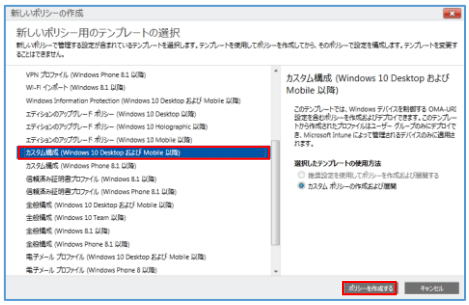
10. [OK] をクリックします。

4.2.2. カスタム構成

[全般構成] から設定できない機能は、カスタム構成から設定する必要があります。

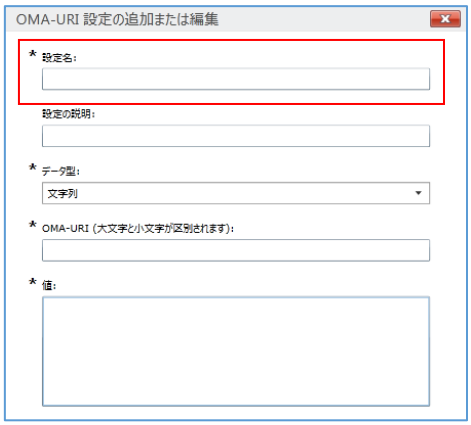
ここでは、例として、USB 接続を許可しないポリシーを作成する手順について、下記に説明します。

図	手順 PC
	1. https://docs.microsoft.com/ja-jp/intune/deploy-use/windows-10-policy-settings-in-microsoft-intune から、設定したい項目を探し、[OMA-URI] 、[データ型] 、[値] をメモします。
	サイト遷移
	2. http://admin.manage.microsoft.com/ から、Microsoft Intune に管理者アカウントでサインインします。
	3. 左メニューから [ポリシー] をクリックします。
	4. [ポリシーの追加] をクリックします。



5. [Windows] > [カスタム構成 (Windows 10 Desktop 及び mobile 以降)] を選択し[ポリシーを作成する] をクリックします。

6. [名前] を入力します。
7. [OMA-URI 設定] > [追加] をクリックします。

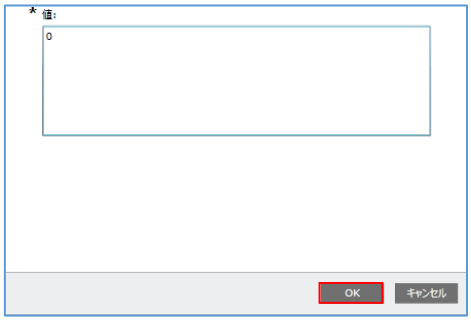


8. [設定名] を入力します。

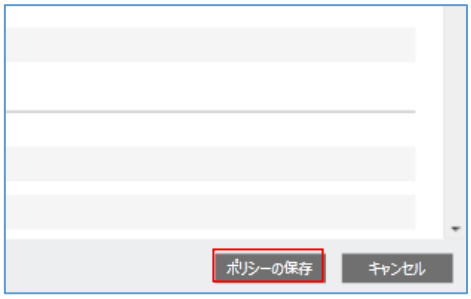
9. OMA-URI 設定から [データ型] を選択します。ここでは、[整数] を選択します。

10. [OMA-URI] を入力します。ここでは、「./Vendor/MSFT/Policy/Config/Connectivity/AllowUSBConnection」と入力します。

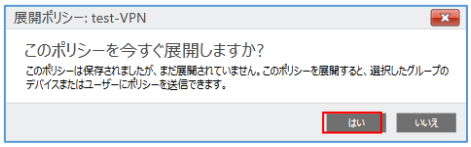
11. [値] を入力します。ここでは、「0」と入力します。



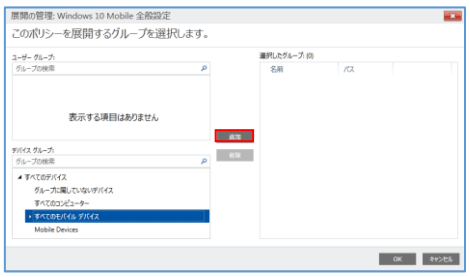
12. [OK] をクリックします。



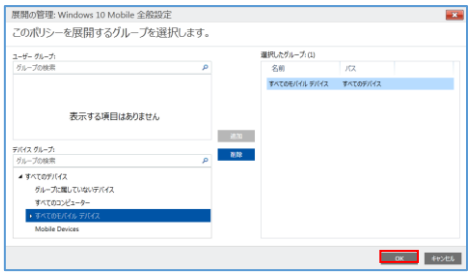
13. 画面右下から、[ポリシーの保存] をクリックします。



14. [はい] をクリックします。



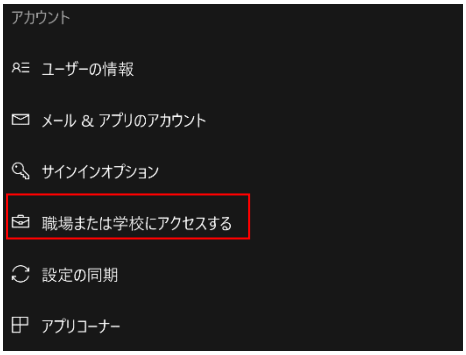
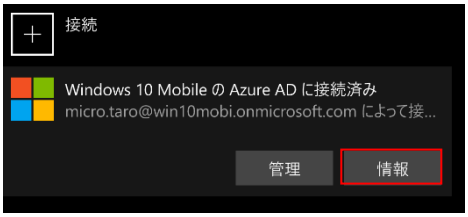
15. デバイスグループからポリシーを展開するデバイスグループを選択し、[追加] をクリックします。



16. [OK] をクリックします。

4.2.3. ポリシーの即時反映

Microsoft Intune から Windows 10 Mobile に展開したポリシーは、すぐには適用されません。いますぐに適用したい場合は、下記の手順を実行します。

図	手順 Mobile
	1. [設定] をタップします。
	2. [アカウント] をタップします。
	3. [職場または学校にアクセスする] をタップします。
	4. 接続している Azure AD > [情報] の順にタップします。
	5. [同期] をタップします。

4.3. 実践

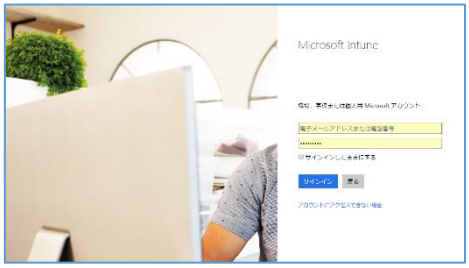
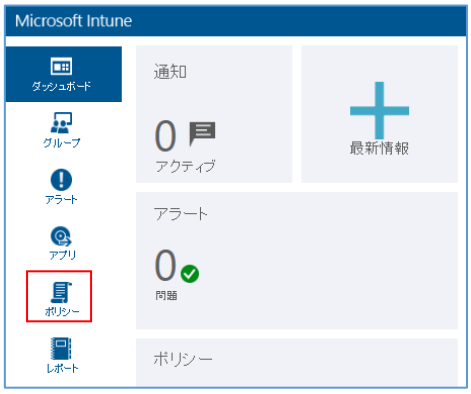
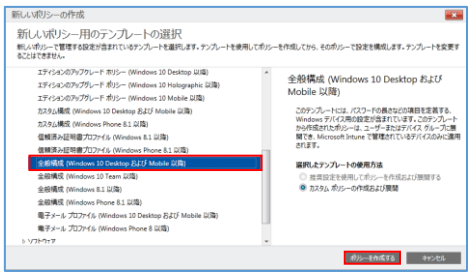
組織向けのポリシーの設定と確認について、Microsoft Intune を使った例をいくつか紹介します。

4.3.1. アプリケーション ストアを許可しない

ユーザーが個人の判断によってアプリをインストールできないよう、Windows ストアへのアクセスを制限することができます。

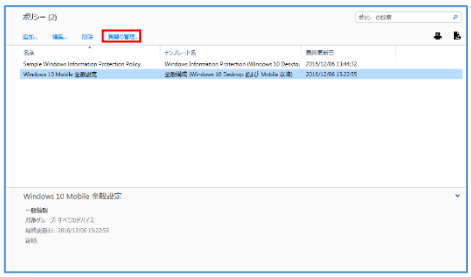
<設定手順>

Windows ストアを禁止するポリシーを適用する手順について、下記に説明します。

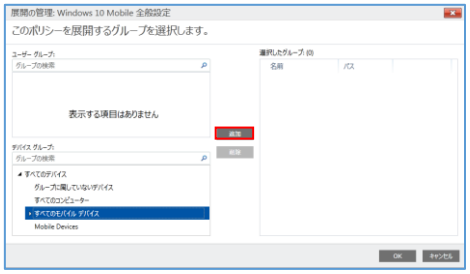
図	手順 PC
	1. http://admin.manage.microsoft.com/ から、Microsoft Intune に管理者アカウントでサインインします。
	2. 左メニューから [ポリシー] をクリックします。
	3. [ポリシーの追加] をクリックします。
	4. [Windows] > [全般設定 (Windows 10 Desktop および Mobile 以降)] を選択し、 [ポリシーを作成する] をクリックします。

5. [ポリシーの作成] から [名前] を入入力します。

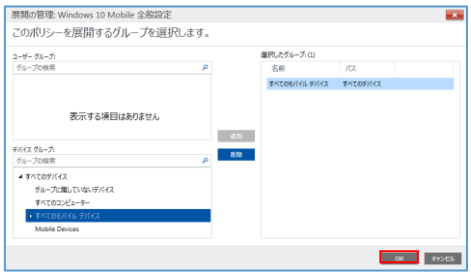
6. [アプリケーション] > [アプリ] > アプリケーションストアを許可する (Windows 10 モバイル限定) :] を、 [いいえ] に設定し、 [ポリシーの保存] をクリックします。



7. ポリシーが追加されます。追加されたポリシーを選択し、 [展開の管理] をクリックします。



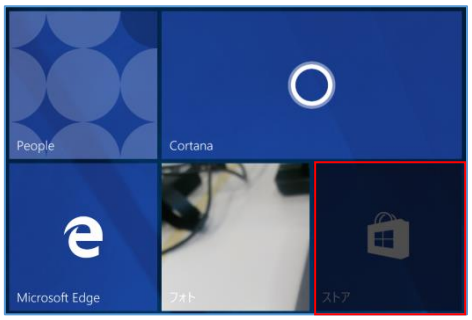
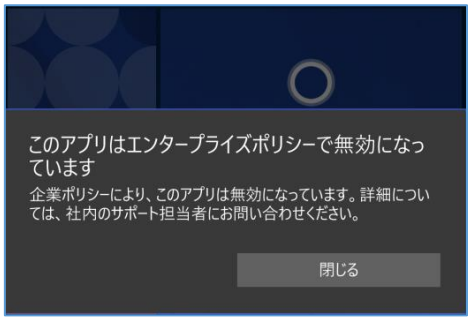
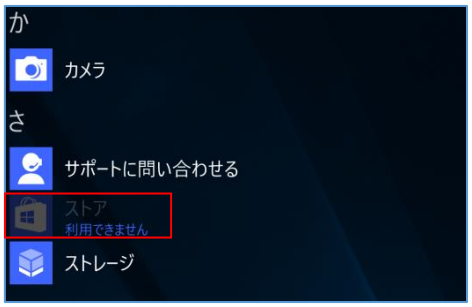
8. デバイスグループから [全てのモバイル デバイス] を選択し、[追加] をクリックします。



9. [OK] をクリックします。

<確認手順>

適用したポリシーが正常に機能しているか確認する手順について、下記に説明します。

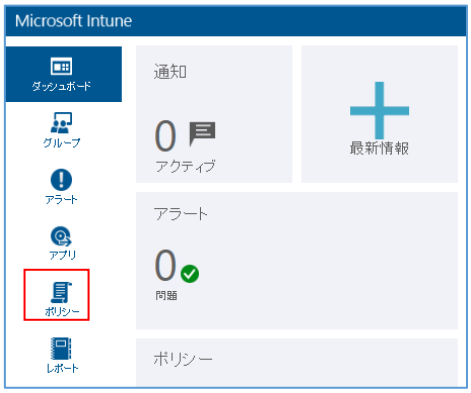
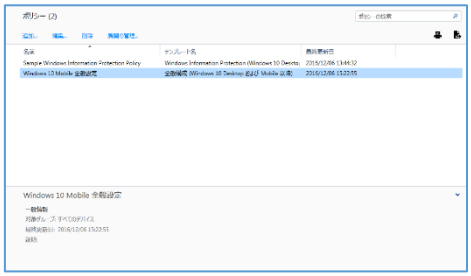
図	手順 Mobile
	1. ポリシーを適用したモバイル デバイスを起動し、スタート画面の [ストア] が無効になっていることを確認します。
	2. [ストア] をタップしても、アプリが起動しないことを確認します。
	3. [全てのアプリ] から、[ストア] が無効になっていることを確認します。

4.3.2. カメラを許可しない

重要なデータの写真が流出することがないよう、カメラ機能を制限することができます。

<設定手順>

カメラを制限するポリシーを適用する手順について、下記に説明します。

図	手順 PC
	1. 左メニューから [ポリシー] をクリックします。
	2. [構成ポリシー] から、4.2.1 で作成した全般構成のポリシーを選択し、ダブルクリックします。
	3. [デバイスの機能] > [ハードウェア-カメラを許可する:] を、[いいえ] に設定し、[ポリシーの保存] をクリックします。

<確認手順>

適用したポリシーが正常に機能しているか確認する手順について、下記に説明します。

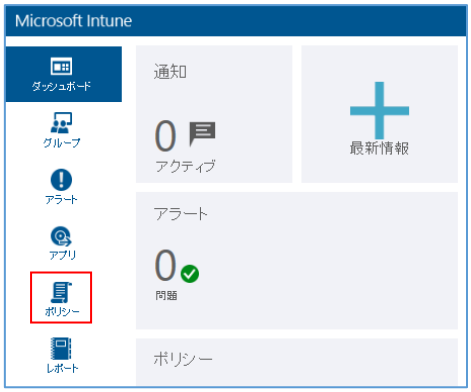
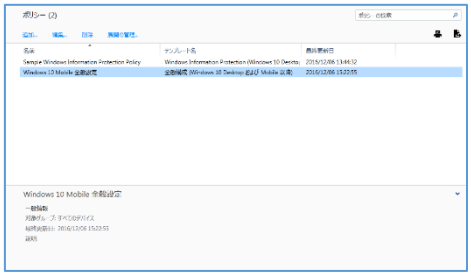
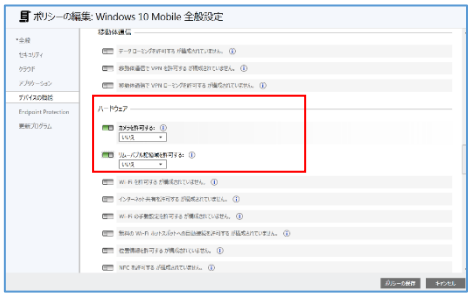
図	手順 Mobile
	1. ポリシーを適用したモバイル デバイスを起動します。
	2. [カメラ] をタップしても、アプリが起動しないことを確認します。

4.3.3. リムーバブル記憶域を許可しない

SD カードなどに重要なデータをコピーして、外に持ち出せないよう、リムーバブル記憶域を制限することができます。

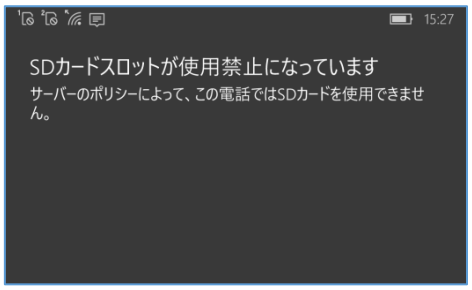
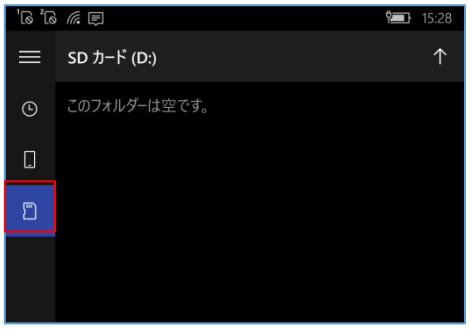
<設定手順>

カメラを制限するポリシーを適用する手順について、下記に説明します。

図	手順 PC
	1. 左メニューから [ポリシー] をクリックします。
	2. [構成ポリシー] から、4.2.1 で作成した全般構成のポリシーを選択し、ダブルクリックします。
	3. [デバイスの機能] > [ハードウェア] > [リムーバブル記憶域を許可する:] を、[いいえ] に設定し、[ポリシーの保存] をクリックします。

<確認手順>

適用したポリシーが正常に機能しているか確認する手順について、下記に説明します。

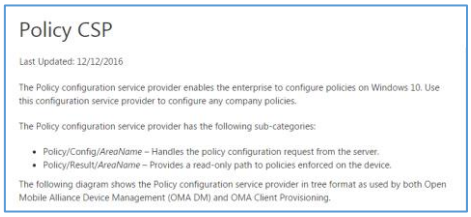
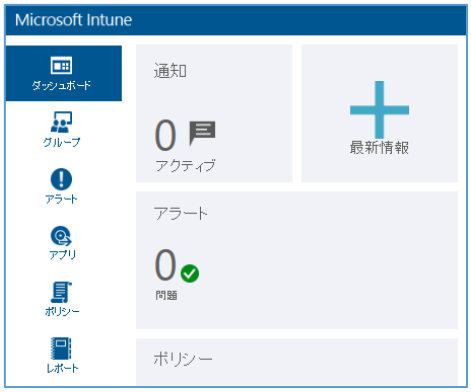
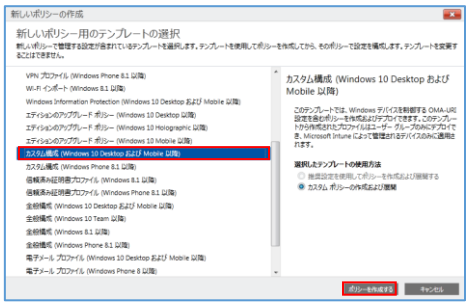
図	手順 Mobile
	1. ポリシーを適用したモバイル デバイスを起動します。[SD カードスロットが使用禁止になっています] と表示されていることを確認します。
	2. [エクスプローラー] > [SD カード] をタップし、フォルダーが空になっていることを確認します。

4.3.4. メッセージング アプリを禁止する

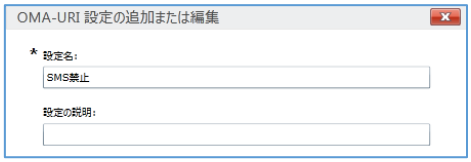
SMS 機能を制限するため、メッセージング アプリを禁止することができます。

<設定手順>

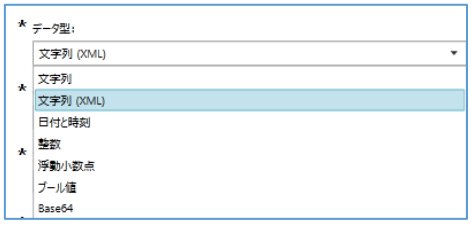
メッセージング アプリを禁止させるため、カスタム構成でポリシーを作成する手順について、下記に説明します。ここでは、Policy CSP の ApplicationRestrictions を利用します。

図	手順 PC
	1. https://msdn.microsoft.com/windows/hardware/commercialize/customize/mdm/policy-configuration-service-provider にアクセスし、[OMA URI]、[データ型]、[値] を確認します。
	サイト遷移
	2. Microsoft Intune に移動し、左メニューから [ポリシー] をクリックします。
	3. [ポリシーの追加] をクリックします。
	4. [Windows] > [カスタム構成 (Windows 10 Desktop 及び mobile 以降)] を選択し[ポリシーを作成する] をクリックします。

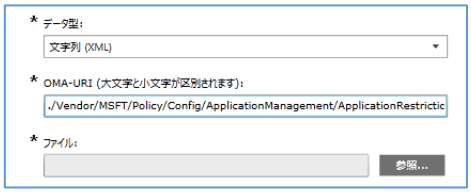
5. [名前] を入力します。
6. [OMA-URI 設定] > [追加] をクリックします。



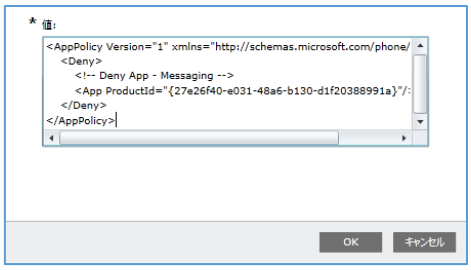
7. [設定名] を入力します。



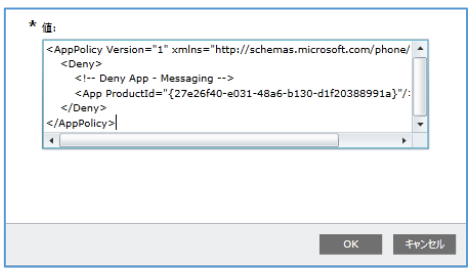
8. Microsoft Intune に戻り、[データ型] から [文字列 (XML)] を選択します。



9. [OMA-URI (大文字と小文字が区別されます)] に、値を入力します。

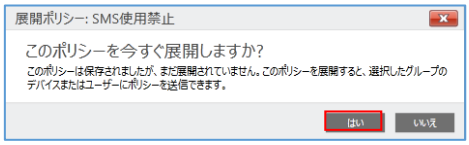


10. [値] を入力します。ここでは、メッセージング アプリを禁止するため、下記のように入力します。
11. <AppPolicy Version="1" xmlns="http://schemas.microsoft.com/phone/2013/policy"><Deny><!-- Deny App - Messaging --><App ProductId="{27e26f40-e031-48a6-b130-d1f20388991a}"/></Deny></AppPolicy>

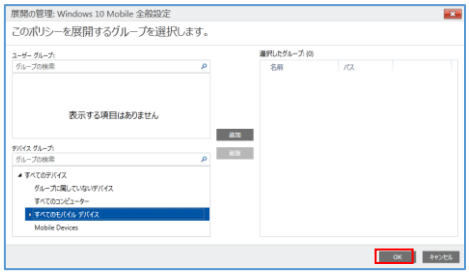


12. [OK] をクリックします。

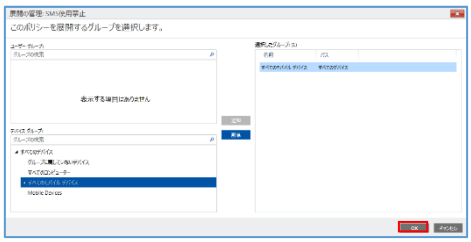
13. 画面右下の [ポリシーの保存] をクリックします。



14. [はい] をクリックします。



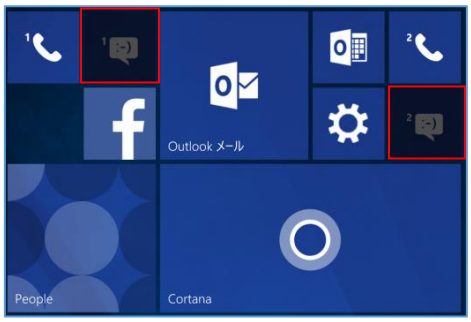
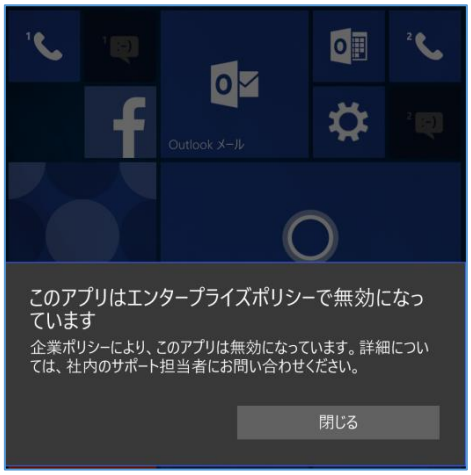
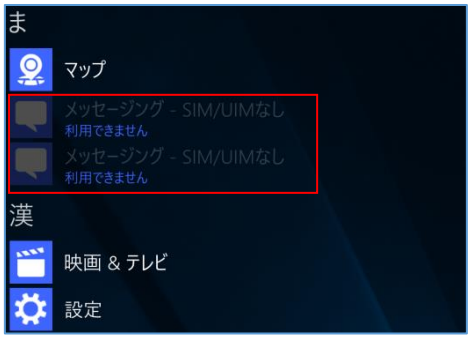
15. デバイスグループから [全てのモバイル デバイス] を選択し、[追加] をクリックします。



16. [OK] をクリックします。

<確認手順>

適用したポリシーが正常に機能しているか確認する手順について、下記に説明します。

図	手順 Mobile
	1. ポリシーを適用したモバイル デバイスを開き、スタート画面の [メッセージング] が無効になっていることを確認します。
	2. [メッセージング] をタップしても、アプリが起動しないことを確認します。
	3. [全てのアプリ] から、[メッセージング] が無効になっていることを確認します。

Note

プレインストールされているスカイプ プレビューにも SMS 機能があるため、AppLocker にて無効化するか、アンインストールするポリシーを設定する必要があります。

5. おわりに

本書では、組織の IT 管理者が Windows 10 Mobile を導入するにあたり想定される作業を 3 つのシナリオに分け、ステップ バイ ステップで作業を進めることにより、評価環境を構築し、機能を評価する手順を説明しました。

Windows 10 Mobile デバイスは、通話やメール、ウェブサイトの閲覧といったスマートフォンとしての基本機能に加え、デストップやタブレットの Windows 10 PC との一貫した、使い慣れたエクスペリエンスを有しています。さらに、Office 365 と組み合わせることにより、いつでもどこでも仕事ができる環境を実現できたのではないかと思います。

また、Windows 10 Mobile デバイス自体の持つ強固なセキュリティ機能と多様な設定を施すことのできるモバイル デバイス管理機能により、組織での利用に適したデバイスであることもご確認頂けたことでしょう。

普段使い慣れた Windows 10 PC と、Windows 10 Mobile を組み合わせることにより、高いセキュリティに守られつつも、時間にも、場所にも、デバイスにも縛られず仕事ができることにより新たなワークスタイルを創造することが可能となります。

本書が、組織内のモバイル デバイスの導入をご検討されている IT 管理者の皆様の一助になりましたら幸いです。

6. 用語集

本書内の用語集になります。

用語	解説
Microsoft Azure	マイクロソフトのクラウド プラットフォームです。アプリケーションとデータをホストしており、アプリケーションの動作環境 (Microsoft Azure) と、Windows Azure AppFabric (クラウドのミドルウェア サービス)、SQL Database (クラウドの RDB) を提供しています。
Bluetooth	デジタル機器用近距離無線通信の規格のひとつです。パソコンや携帯電話、周辺機器などのケーブルを使わずにワイヤレスで接続し、機器間で音声やデータをやりとりすることができます。
Device Guard	Windows 10 Mobile に標準で搭載されるセキュリティ機能です。日々増え続け、多様化したウィルスへの対策として導入されています。Device Guard は、信頼されていないアプリを起動できないようにロックダウンすることで、デバイスを保護することができます。
DRA 証明書	データ回復エージェント (Data Recovery Agent) の略称です。暗号化ファイル・システム (EFS) で暗号化されているユーザーのデータを復号化するための公開鍵の証明書を DRA 証明書といい、与えられている管理者のことを DRA といいます。
Miracast	Wi-Fi Alliance によって策定された、無線通信によるディスプレイ伝送技術です。
OMA-URI	Open Mobile Alliance Uniform Resource Identifier の略称です。Microsoft Intune のテンプレートでは設定できないポリシーは、OMA-URI で記述します。
シングル サインオン	1 度の認証で複数のアプリケーションやサービスにアクセスできる機能です。これにより、ユーザーは認証を意識せずに仕事をすることができます。