Microsoft

Windows Embedded 8.1 Industry Enterprise 評価ガイド

Microsoft Corporation

発行日 ：2014 年 12 月

■ 企画/執筆/監修

執筆 ：株式会社ソフィアネットワーク
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	2014 年 12 月 16 日	株式会社ソフィアネットワーク	作成

内容

1 はじめに

このドキュメントは Windows Embedded 8.1 Industry Enterprise の各種機能について解説し、Windows Embedded 8.1 Industry Enterprise の評価を行う上で必要な環境の構築手順と、Windows Embedded 8.1 Industry Enterprise を利用した業務端末を構築する上での一連の手順を記述したものです。

本書の構成

章段		説明
1	はじめに	このドキュメントの概要について説明します。
2	Windows Embedded 8.1 Industry Enterprise の概要	Windows Embedded 8.1 Industry Enterprise で利用可能な機能や製品の位置づけなどについて説明します。
3	評価環境と前提条件	本評価ガイドにそって評価を行っていただくために必要な前提条件について説明します。
4	導入と初期設定	Windows Embedded 8.1 Industry Enterprise のインストールと初期設定について説明します。
5	シナリオの概要	Windows Embedded 8.1 Industry Enterprise の利用シナリオについて説明します。
6	シンクライアントとしての利用	シンクライアントとして Windows Embedded 8.1 Industry Enterprise を利用するために必要な設定について説明します。
7	読み取り専用リッチクライアントとしての利用	読み取り専用リッチクライアントとして Windows Embedded 8.1 Industry Enterprise を利用するために必要な設定について説明します。
8	業務アプリ専用端末への転用	Windows Embedded 8.1 Industry Enterprise を業務アプリ専用端末へ転用するために必要な設定について説明します。
9	SCCM による管理	SCCM から Windows Embedded 8.1 Industry Enterprise を管理する方法について説明します。
10	まとめ	

2 Windows Embedded 8.1 Industry Enterprise の概要

本章では、Windows Embedded 8.1 Industry Enterprise の特徴について解説します。

2.1 Windows Embedded 8.1 Industry Enterprise とは

Windows Embedded 8.1 Industry Enterprise は Windows 8.1 をベースに組織での利用シーンに合わせて利用可能な機能を絞り込むことで、利用者に対する利便性を提供します。具体的には、Windows 8.1 機能に対する制限 (ロックダウン) を行うことで、端末による業務外の作業を禁止します。その結果、業務に必要な作業に集中でき、誤動作によるサポートおよび問い合わせの削減や、情報漏えいの防止などにつながります。

2.2 Windows Embedded 8.1 Industry Enterprise の用途

Windows Embedded 8.1 Industry Enterprise はロックダウンを主な機能として実装しているため、次のような用途での利用が想定されています。

- シンクライアントとしての利用
  シンクライアントとして利用する端末はリモート デスクトップ接続だけを必要としており、ロックダウンによってローカルにデータが保存されないような構成が求められます。

- 業務端末への転用
  Windows Embedded 8.1 Industry Enterprise は汎用的な PC に OS をインストールして利用することができます。そのため、POS レジのような専用端末で行うような作業も汎用的な PC を業務端末へ転用して、簡単に使い始めることができます。

- 読み取り専用リッチクライアント
  業務の中には組織で扱うデータを参照する目的のみで活用される端末があります。こうした端末を読み取り専用で利用させることで、データの持ち出しや不適切な場所への保存を制限し、安全にデータを扱うことができます。

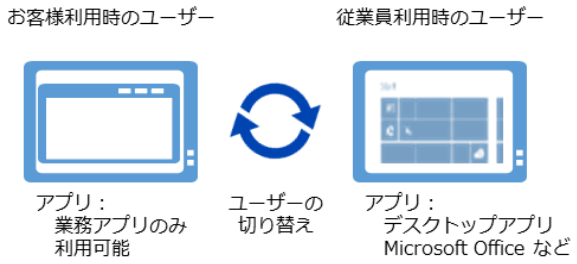
- 電子広告 (デジタル サイネージ)
  大型ディスプレイによる広告を配信する場合、特定アプリケーションだけを利用します。そのため、ほかのアプリケーションの実行を制限し、広告配信中に意図せずアプリケーションやダイアログが起動し、画面に入り込むことを制限します。

2.3 Windows Embedded のライセンスとアクティベーション

Windows Embedded 8.1 Industry Enterprise のライセンスは、これまでのハードウェアと一体で提供される OEM の提供形態とは異なり、ボリューム ライセンスの形態で提供されます。そのため、Microsoft Surface を含む一般の PC にインストールして利用できるメリットがあります。

また、Windows Embedded 8.1 Industry Enterprise の利用権は Windows SA (Software Assurance) の権利に含まれています。SA を保有する組織では Windows 8.1 Enterprise の代わりとして Windows Embedded 8.1 Industry Enterprise を利用することも可能なため、1 台の物理 PC で、汎用的な PC と特定業務端末を切り替えて利用するようなシナリオも実現できます。

図 2.3-1 1 台を、組み込み端末として利用、Windows 8.1 として通常利用の切り替えが可能



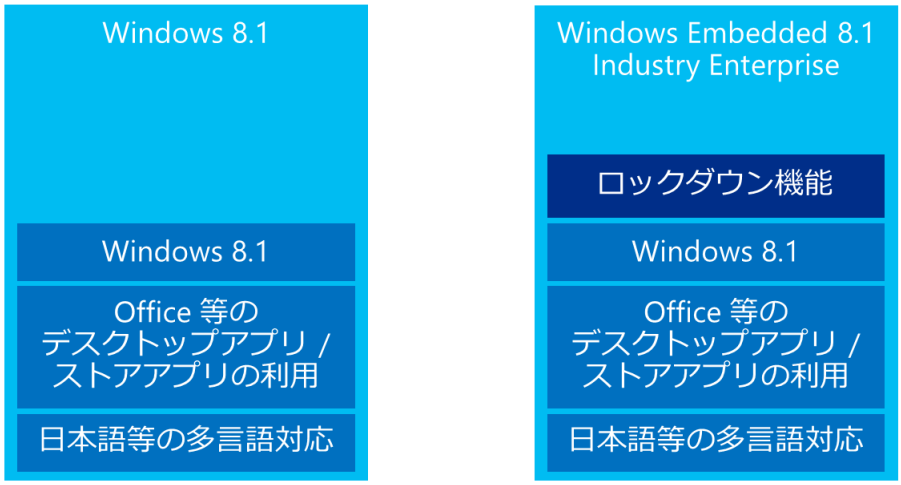
Windows Embedded 8.1 Industry Enterprise のライセンス認証は、ボリューム ライセンスのライセンス認証方式に基づいた方法が採用されており、マルチライセンス認証キー (MAK) またはキー管理サービス (KMS) による認証を行うことができます。

なお、ライセンス認証は、端末への書き込みを制限する書き込みフィルターが設定されていない状態のときに行ってください。書き込みフィルターが有効な状態でライセンス認証を行うと再起動後にライセンス情報が消去されますので注意してください。

2.4 Embedded Lockdown Manager の概要

Windows Embedded 8.1 Industry Enterprise が通常の Windows 8.1 と大きく異なる点は Windows 8.1 の機能に加えて組み込み向け専用機能である Embedded Lockdown Manager を実装している点です。

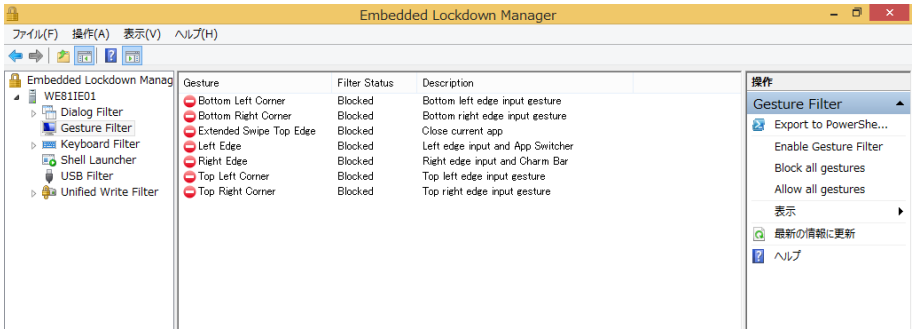
図 2.4-1 Windows 8.1 と Windows Embedded 8.1 の違い



Embedded Lockdown Manager は各種ロックダウンを行う機能で、設定内容は該当するユーザーでサインインすることで反映されます。
Embedded Lockdown Manager による設定には大きく分けて以下の項目があります。(各項目については次節より解説します)

・書き込みフィルター
・Application Launcher / Shell Launcher
・ジェスチャー フィルター
・キーボード フィルター
・ダイアログ フィルター
・USB フィルター

画面 2.4-1 Embedded Lockdown Manager 画面

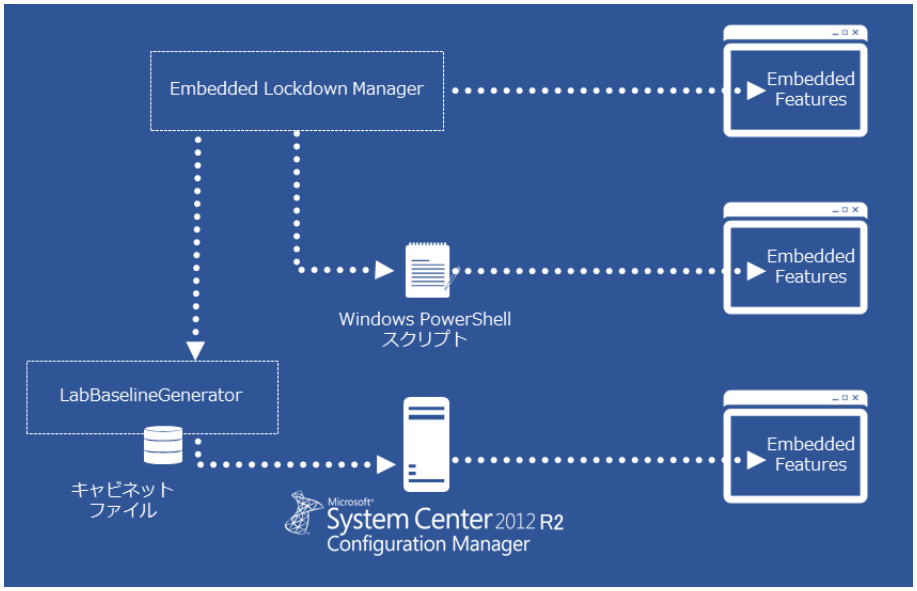


最新の Embedded Lockdown Manager はマイクロソフト ダウンロードセンターからダウンロードすることができ、上記のようなロックダウンを行うことができます。一方、Windows Embedded 8.1 Industry Enterprise でロックダウンを実現するにはロックダウン設定を処理するためのコンポーネントである、Embedded Features と呼ばれるコンポーネントを事前に実装している必要があります。Embedded Features は Windows Embedded 8.1 Industry Enterprise のコントロール パネルから追加可能です。最新の Embedded Features についても、マイクロソフト ダウンロード センターで提供されています。

このように Embedded Lockdown Manager を利用したロックダウンの設定は、ロックダウン設定を行うためのユーザー インターフェイスである Embedded Lockdown Manager と、それを処理する Embedded Features から構成されます。

また、Embedded Lockdown Manager の設定内容は Windows PowerShell スクリプトにエクスポートし、Embedded Features が実装された別のコンピューターでスクリプトを実行して設定を適用する事や、LabBaselineGenerator ツールを利用してロックダウン設定をキャビネット ファイル形式でエクスポートし、System Center 2012 R2 Configuration Manager 経由で設定を配布することも可能です。複数のコンピューターに対してロックダウンを設定する場合、管理者 PC にのみ Embedded Lockdown Manager をインストールし、ロックダウン対象の PC には Embedded Features のみを実装する方法が採れます。

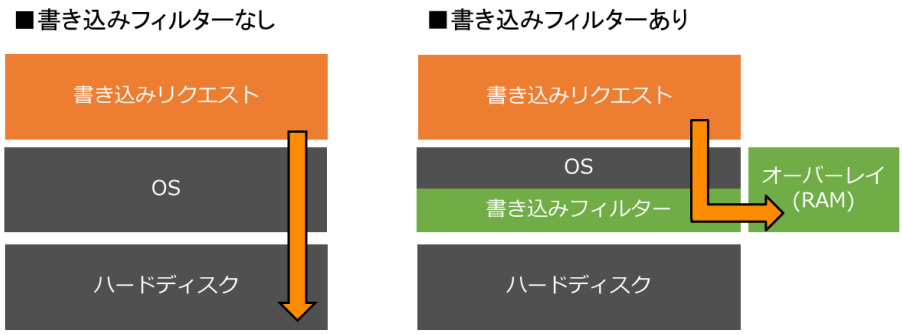
図 2.4-2 ロックダウン設定の適用パターン



2.5 書き込みフィルター

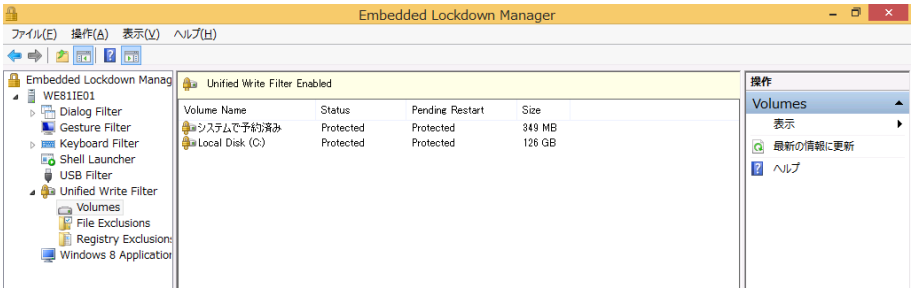
書き込みフィルター（ユーザー インターフェイス上では Unified Write Filter と表示）は PC の内臓ディスクに対する書き込みを制限する設定です。書き込みフィルターによる書き込み制限はリアルタイムで書き込みを禁止するものではなく、OS 内に組み込まれた書き込みフィルターにより、オーバーレイと呼ばれるメモリ領域に一時的に書き込みを行います。そしてシャットダウン/再起動時にオーバーレイに書き込まれた内容を消去するため、一時的な書き込みを必要とするアプリケーションもこれまでどおりに利用することが可能です。
書き込みフィルターは、不適切なファイル保存をさせたくない、シンクライアントや不特定多数のユーザーが利用するような端末での活用が想定されます。

図 2.5-1 書き込みフィルターによるオーバーレイ書き込み



書き込みフィルターはボリューム単位で書き込みを制限するフィルターが適用されます。設定は再起動後に適用され、管理者アカウントを含む、すべてのユーザーにフィルターが適用されます。

画面 2.5-1 Unified Write Filter によってローカルのすべてのボリュームへの書き込みを制限



ボリューム単位での書き込みフィルター設定はファイル、フォルダー、レジストリ キー単位での例外を設定することができます。例外設定を行うことによって、たとえば C ドライブの中でも Document フォルダーだけ書き込みを許可するような運用が可能になります。

書き込みフィルター設定はオーバーレイに書き込まれた内容を再起動によって消去しますが、その内容は更新プログラムのインストールでも例外ではありません。しかし、それでは更新プログラムがいつまでもインストールされない状態で Windows Embedded 8.1 Industry Enterprise を利用しなければなりません。そこで、書き込みフィルターでは Windows Update や System Center Endpoint Protection (SCEP) の定義ファイルなどによるボリュームへの書き込みを許可するように例外を設定することができます。

2.6 Application Laucher / Shell Launcher

Application Launcher と Shell Launcher は特定のアプリケーションの実行だけを許可する制限機能で、キオスク端末など特定業務向け端末としての用途での利用が想定されています。

Application Launcher は Windows 8.1 のモダン UI から実行可能な特定の Windows ストア アプリのみを実行できるように制限し、Shell Launcher は特定のデスクトップ アプリケーションのみを実行できるように制限します。

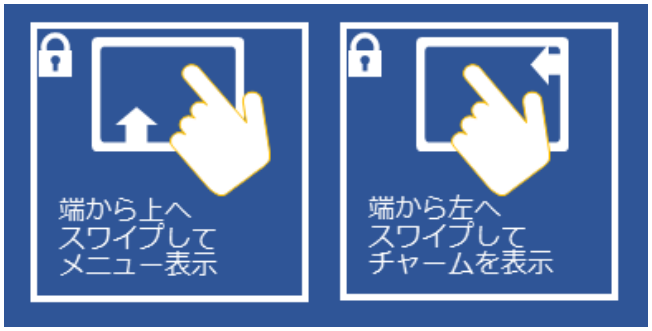
Application Launcher と Shell Launcher はユーザーまたはグループごとに実行するアプリを指定できます。そのため、ユーザーごとに異なるアプリを割り当てておき、業務内容に合わせて異なるユーザーでサインインするような利用方法や、管理者でサインインしたときには制限のない汎用 PC として利用するなどの活用が可能です。

Application Launcher と Shell Launcher は同時に利用することができません。そのため、利用するアプリケーションに合わせて使い分けてください。

2.7 ジェスチャー フィルター

ジェスチャー フィルターはタッチパネルで行うタッチ操作を制限する設定です。ジェスチャー フィルターを制限して、チャームの表示による PC 設定の変更や、スワイプによる起動アプリに対する設定変更などを防ぐことで、不特定多数のユーザーに利用されることが考えられる受付端末や電子広告に対する不適切な操作 (いたずら) を防げる効果があります。
一方、ジェスチャー フィルターの制限が設定されていてもキーボード操作は引き続き利用可能なので、メンテナンス等の目的で端末 (タブレット) を利用するときだけキーボードを設置して通常の PC と変わらない操作を行うことができます。
ジェスチャー フィルターによって行うことができる、主な制限設定には図 2.7-1 のような操作があります。

図 2.7-1 ジェスチャー フィルターで制限可能な操作



2.8 キーボード フィルター

キーボード フィルターはキーボード操作に対する制限を行う設定で、特定のキー操作だけを無効にすることができます。キーボード フィルターで制限可能なキー操作カテゴリーには次のようなものがあります。

カテゴリー	説明
Accessibility Keys	アクセシビリティに関連するキー操作
Application Keys	Alt+F4 などのアプリに対して行うキー操作
Browser Keys	ブラウザー起動時に利用するキー操作
Extended Shell Keys	ブラウザー起動など、キーボードに割り当てられている特殊キーの操作
Media Keys	Windows Media Player に対して行うキー操作
Modifier Keys	Alt, Ctrl, Shift, Windows キーの操作
Security Keys	Ctrl+Alt+Del などのセキュリティ関連のキー操作
Shell Keys	Windows デスクトップ上で行う各種ショートカットキーの操作
All Keys	キーボード フィルターで設定可能なすべてのキー操作
Custom Keys	管理者自身が定義したキー操作
Custom Scan Codes	管理者が利用するキーボードと異なるキー配列*のキーボードで行うキー操作

* 管理者が 101 キーボードを利用しており、利用者が 106/109 キーボードを利用しているケースを指します。

また、キーボード フィルターは設定すると、タブレット使用時に利用可能なスクリーンキーボードにも適用されます。

2.9 ダイアログ フィルター

ダイアログ フィルターはダイアログボックスの表示を制限する設定です。電子広告や受付端末では、起動しているアプリの内容だけが表示されるべきであるにも関わらず、他のバックグラウンドで実行しているアプリからのメッセージによってダイアログが表示されてしまう場合があります。このようなときにダイアログの表示を制限し、余計な画面が表示されないように構成することができます。
ダイアログ フィルターでは既定のダイアログ表示を許可/拒否のいずれかに設定することができ、またアプリごとに例外を設けることができます。

2.10 USB フィルター

USB フィルターは USB デバイスの利用を制限するための設定です。USB フィルターを設定すると、すべての USB デバイスの利用を制限しますが、例外として次のレベルでの許可設定を行うことができます。

・ポート レベル
PC に搭載されている USB ポートの単位で許可するように構成できます。

・クラス レベル
ストレージやヒューマン インターフェイス デバイスなど、USB 接続デバイスの種類に合わせて、USB デバイス利用の許可/拒否を構成できます。接続デバイスの種類の識別にはデバイス クラス ID を利用します。

・デバイス レベル
特定のデバイスのみ利用を許可するように構成できます。利用するデバイスは、プロダクト ID (Device Product ID) やベンダー ID (Device Vendor ID) を指定することができます。

【Note:】
USB フィルターで指定する ID 情報はコントロール パネルのデバイス マネージャーから確認することができます。デバイス マネージャーの [表示] メニューから [デバイス (接続別)] を選択すると、現在接続しているデバイス名とデバイス種類の関係を簡単に確認できます。デバイス種類のプロパティを開いて、[全般] タブでポートレベルの番号、[詳細] タブの [互換性 ID] プロパティからデバイスのクラスレベル (Class_ 以降の番号部分)、[ハードウェア ID] プロパティからデバイス レベルで使用するプロダクト ID (PID_ 以降の番号部分) とベンダーID (VID_ 以降の番号部分) が

それぞれ確認できます。(プロダクト ID とベンダー ID はそれぞれ 16 進数で表示されます。設定は 10 進数で行うため、16 進数から 10 進数へ変換した上で行ってください)

図 2.10-1 ポート レベルで使用する番号の確認画面

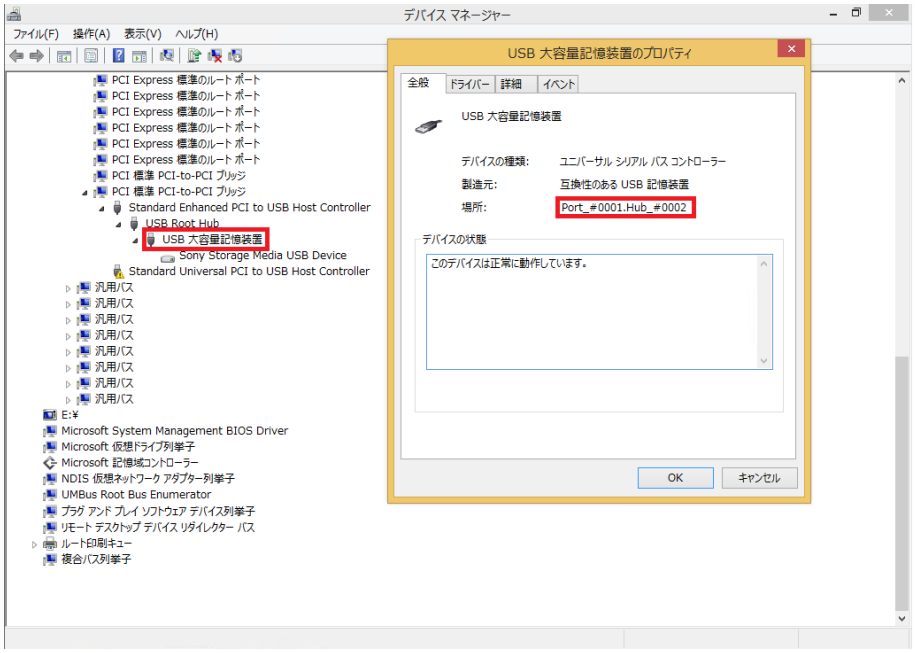


図 2-10-2 デバイス クラス ID の確認画面

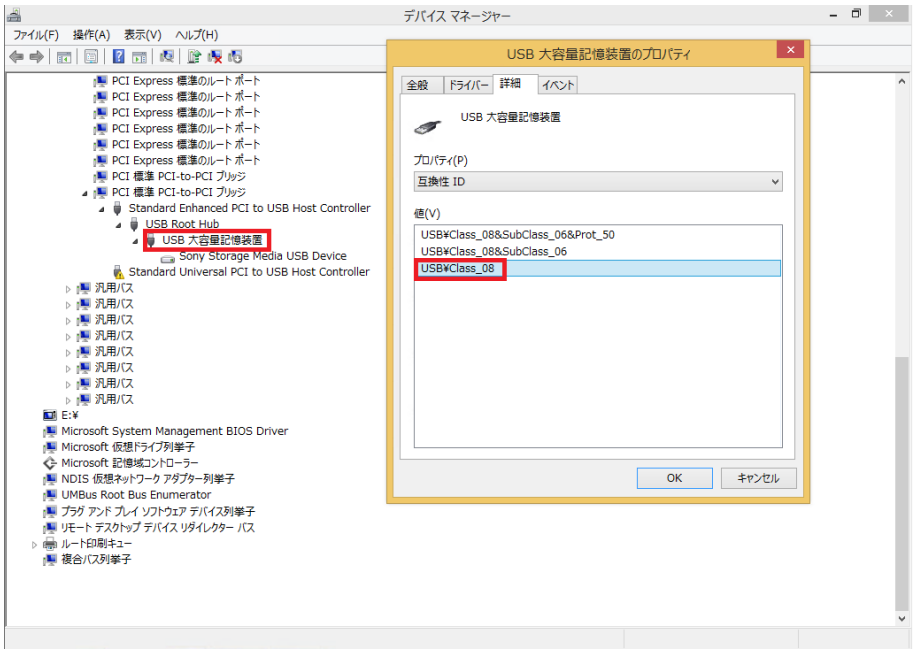
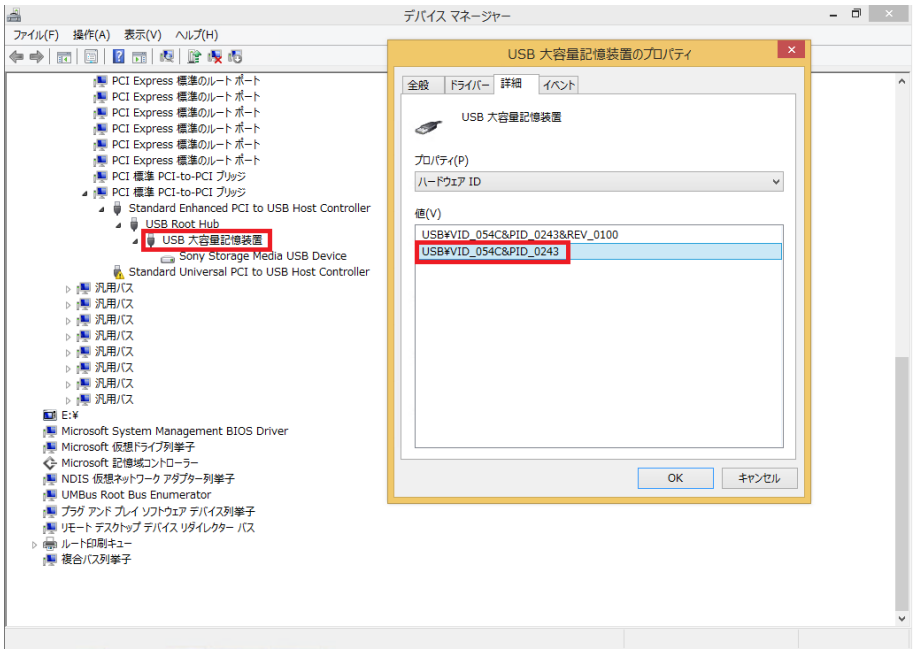


図 2.10-3 プロダクト ID と ベンダー ID の確認画面



3 評価環境と前提条件

本書では、Windows Embedded 8.1 Industry Enterprise のインストールから始まり、Embedded Lockdown Manager を利用した様々なロックダウンまでを行うことで、Windows Embedded 8.1 Industry Enterprise の全体的な評価を行って頂けます。
また、第 9 章では System Center 2012 R2, Configuration Manager (以降、SCCM 2012 R2) との組み合わせによる Windows Embedded 8.1 Industry Enterprise の管理方法についても評価を行います。SCCM 2012 R2 そのものの環境構築については、「System Center 2012 R2 Configuration Manager 評価ガイド - 基本環境構築編」をご覧ください。

System Center 2012 R2 Configuration Manager 評価ガイド - 基本環境構築編
http://www.microsoft.com/ja-jp/download/details.aspx?id=41686

本書で利用する、各コンピューターの情報は以下の通りです。

表 3-1 評価環境 コンピューター情報

コンピューター名	説明
WE81IE01	・ Windows Embedded 8.1 Industry Enterprise をインストールし、管理を行うコンピューター ・ ワークグループに参加 (第 9 章の評価を行うときは contoso.com ドメインに参加し、SCCM クライアントになるように構成してください) ・ Windows ストア アプリとして MSN 天気をインストール
WE81IE02	・ Windows Embedded 8.1 Industry Enterprise をインストールし、管理されるコンピューター (4.4 節のみで使用*) ・ ワークグループに参加 ・ リモート デスクトップ接続の許可 (6.5 節のみで使用)
ws2012-dc01.contoso.com	・ contoso.com ドメインの AD ドメイン コントローラー ・ DNS サーバー ・ DHCP サーバー ・ Windows Server 2012 R2 (GUI)
ws2012-cm01.contoso.com	・ SCCM 2012 R2 を実行するサーバー。 ・ contoso.com ドメインに参加 ・ Windows Server 2012 R2 (GUI) ・ SCCM 2012 R2 + SQL Server 2012

* 4.4 節はオプションです。4.4 節の評価を行う場合のみ、WE81IE02 コンピューターをご用意ください。

評価環境における各コンピューターのアカウント情報は以下の通りです。

表 2.10-2 評価環境アカウント情報

アカウント名	パスワード	説明
Admin	P@ssw0rd	WE81IE01/ WE81IE02 コンピューター用ローカル管理者アカウント
administrator@contoso.com	Pass@w0rd1	Active Directory ドメイン(contoso.com)の Administrator アカウント。

コンピューターのネットワーク情報は以下の通りです。第 8 章までのネットワーク情報は以下のとおりですが、第 9 章の評価を行うときは「System Center 2012 R2 Configuration Manager 評価ガイド - 基本環境構築編」に基づいて構成されるため、ネットワーク情報が変わります。適宜、IP アドレス等を変更してご利用ください。

表 2.10-3 評価環境 ネットワーク情報 (第 4 章～第 8 章)

コンピューター名	IP アドレス	サブネットマスク	デフォルトゲートウェイ	DNS
WE81IE01	192.168.1.100	255.255.255.0	192.168.1.1	192.168.1.1
WE81IE02	192.168.1.101	255.255.255.0	192.168.1.1	192.168.1.1

実際に評価環境を構築する際は、適宜、お手元のネットワーク環境に置き換えてください。

(*1) デフォルトゲートウェイおよび DNS サーバーの IP アドレスは、インターネットへの接続ができるように構成しておいてください。

表 2.10-4 評価環境 ネットワーク情報 (第 9 章)

コンピューター名	IP アドレス	サブネットマスク	デフォルトゲートウェイ	DNS
ws2012-dc01.contoso.com	192.168.0.10	255.255.255.0	192.168.0.254	127.0.0.1 (*1)
ws2012-cm01.contoso.com	192.168.0.11	255.255.255.0	192.168.0.254	192.168.0.10
WE81IE01.cotnoso.com	(DHCP)			

実際に評価環境を構築する際は、適宜、お手元のネットワーク環境に置き換えてください。

*1 ドメイン コントローラーに昇格後、WORKGROUP 環境で構成していた DNS サーバーアドレスが DNS サーバーのフォワーダー先として自動的に構成され、ループバック アドレス (127.0.0.1) がドメイン コントローラーの DNS サーバーアドレスに構成されます。

■ 必要なソフトウェアとソフトウェアライセンス

本書で構築する環境の画面ショット内では、MSDN サブスクリプションライセンスを用いた製品を使用しています。

MSDN サブスクリプション及びボリュームライセンスをお持ちでない場合は、以下のサイトの評価版ライセンスを利用してください。

Windows Embedded 製品をダウンロードする

http://www.microsoft.com/windowsembedded/ja-jp/downloads.aspx

4 導入と初期設定

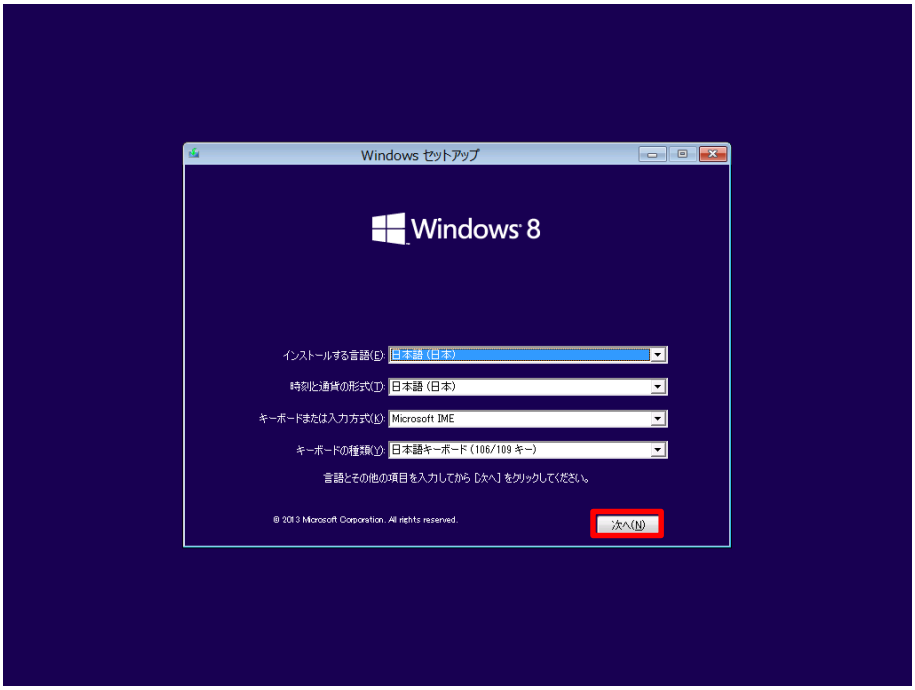
本章では、Windows Embedded 8.1 Industry Enterprise をインストールし、利用開始するために必要な設定について確認します。

4.1 Windows Embedded 8.1 Industry Enterprise のインストール

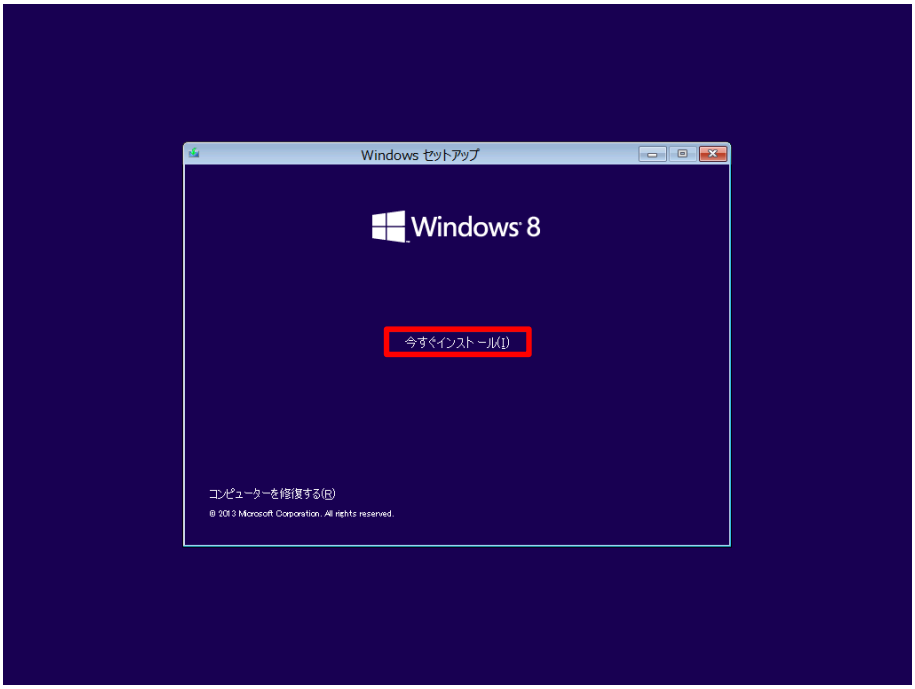
本手順では、Windows Embedded 8.1 Industry Enterprise のインストール手順について確認します。この手順は、 WE81IE01、 WE81IE02 コンピューターで実施します。

1) DVD ドライブに Windows Embedded 8.1 Industry Enterprise のセットアップ DVD (もしくは ISO ファイル) をセットし、コンピューターを起動します。

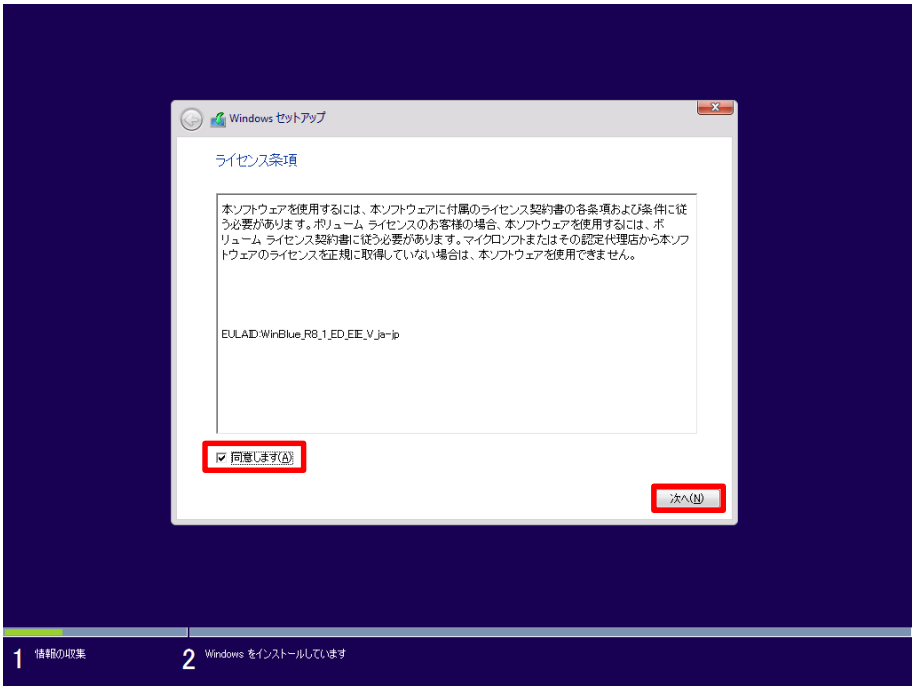
2) [Windows セットアップ] 画面で、[次へ] をクリックします。



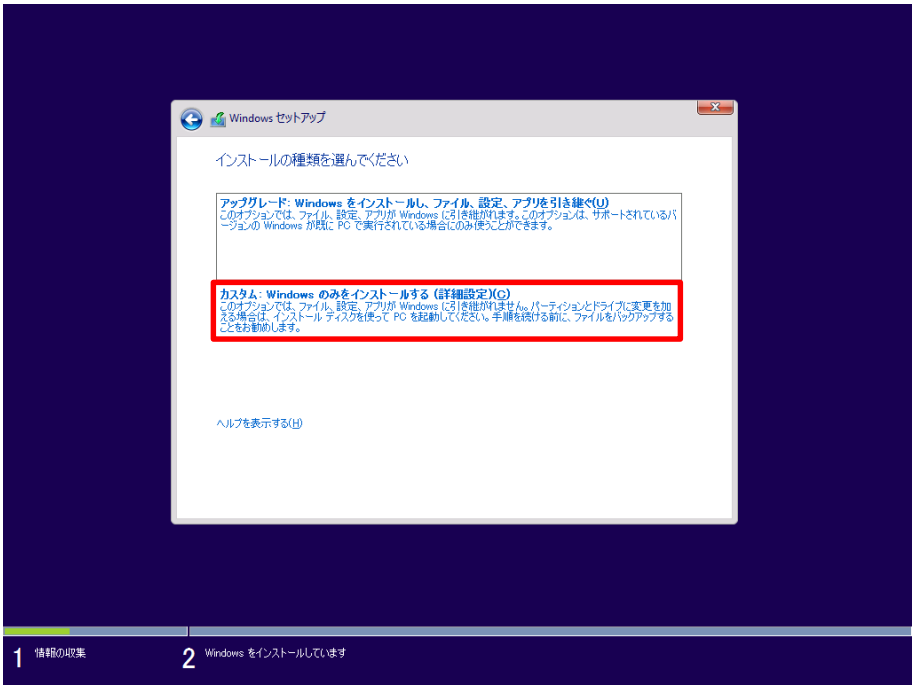
3) [Widnows セットアップ] 画面で、[今すぐインストール] をクリックします。



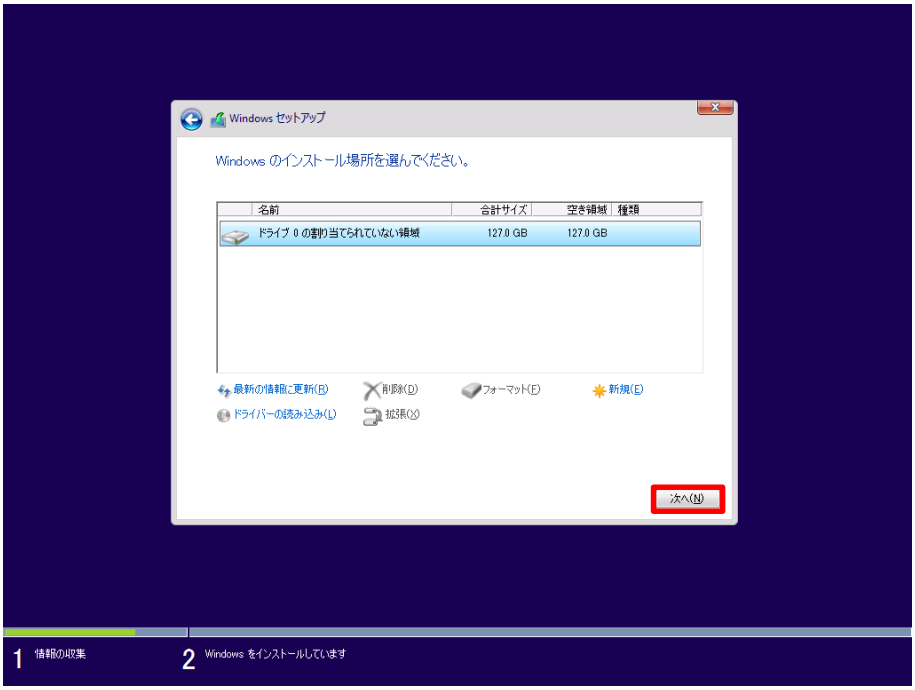
4) [Widnows セットアップ] 画面で、[同意します] にチェックをつけ、[次へ] をクリックします。



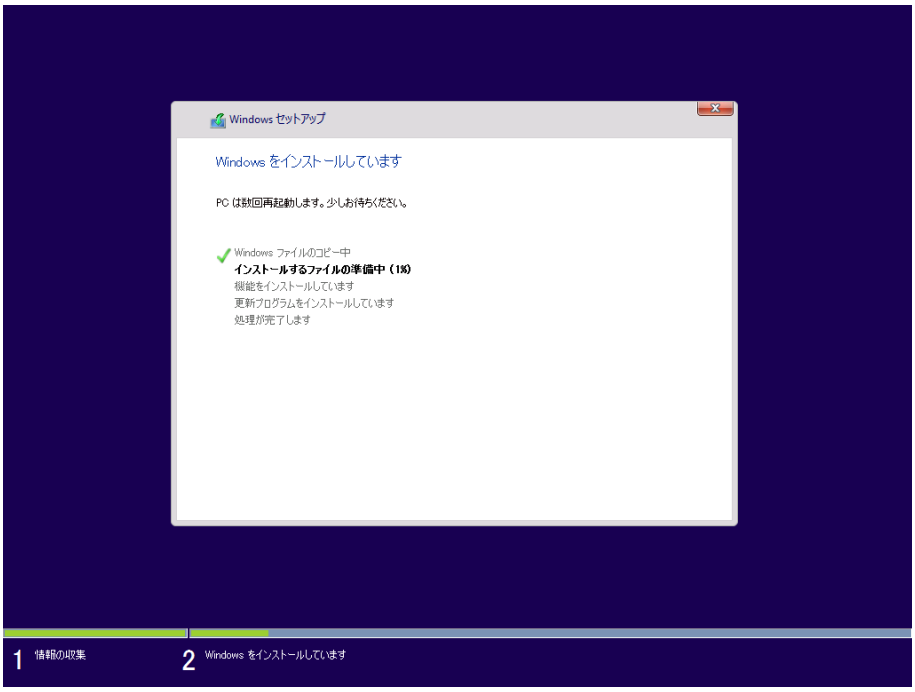
5) [Windows セットアップ] 画面で、[カスタム] をクリックします。



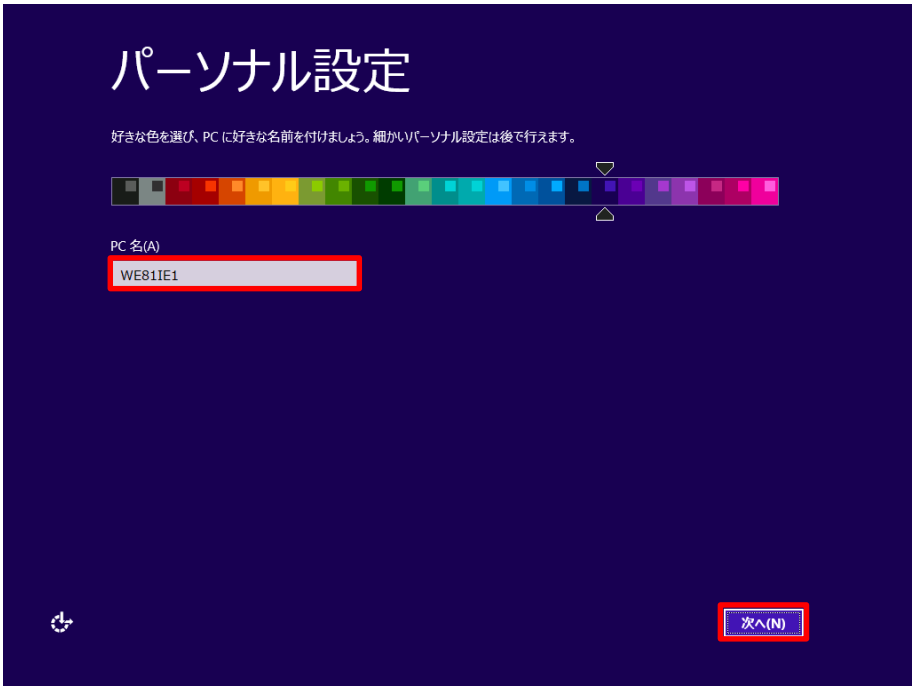
6) [Windows セットアップ] 画面で、インストールする領域を選択し、[次へ] をクリックします。



7) ここまでの手順で、Windows Embedded 8.1 Industry Enterprise のインストールが始まり、しばらくするとインストールが完了します。

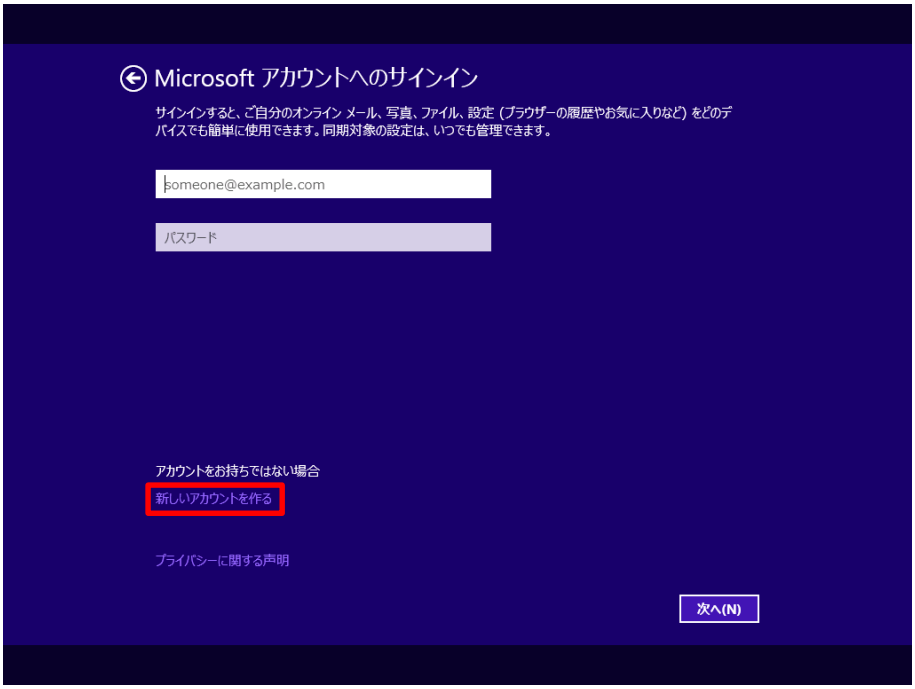


8) [パーソナル設定] 画面で、[PC 名] 欄に「WE81IE01」(もしくは「WE81IE02」) と入力し、[次へ] をクリックします。

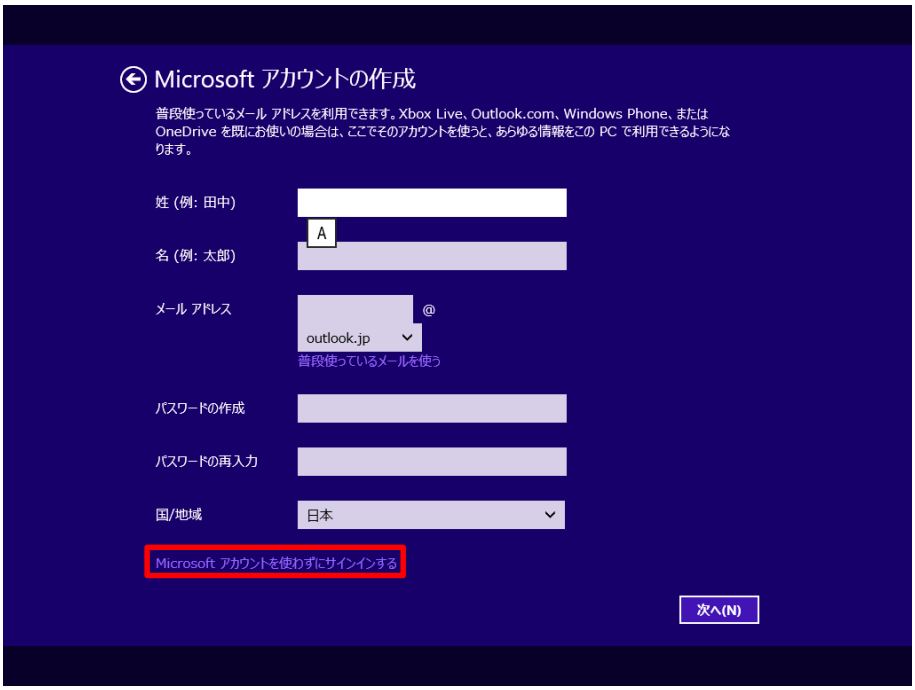


9) [設定] 画面で、[簡単設定を使う] をクリックします。

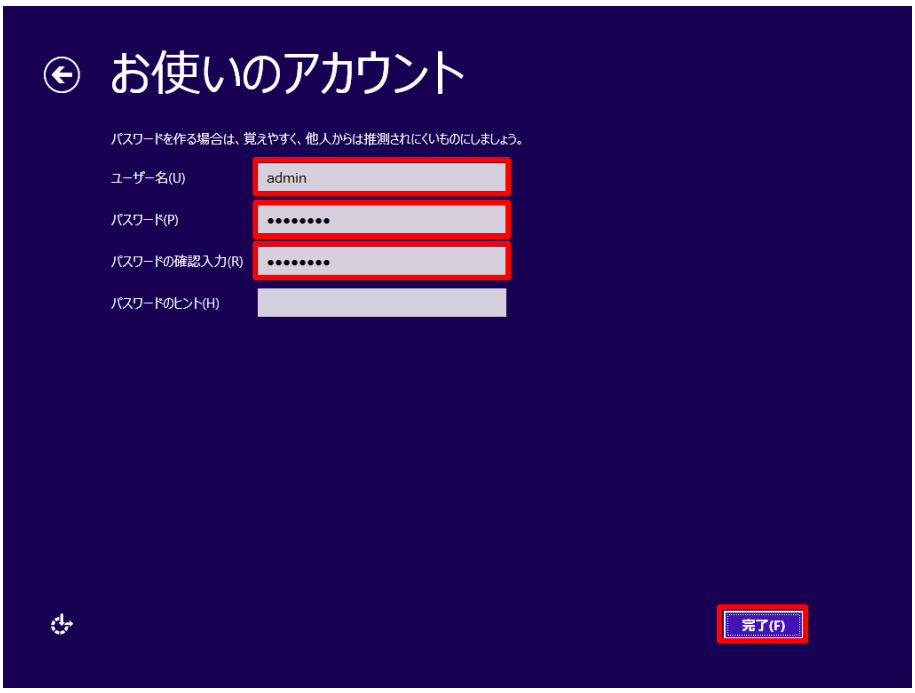
10) [Microsoft アカウントへのサインイン] 画面で、[新しいアカウントを作る] をクリックします。尚、ネットワークに接続していない場合、このステップは表示されません。その際は、次の [お使いのアカウント] ステップに進んでください。



11) [Microsoft アカウントの作成] 画面で、[Microsoft アカウントを使わずにサインインする] をクリックします。



12) [お使いのアカウント] 画面で、[ユーザー名] 欄に「admin」、[パスワード] と [パスワードの確認入力] 欄に「P@ssw0rd」、[パスワードのヒント] 欄に任意の文字を入力して、[完了] をクリックします。



4.2 Embedded Features の実装

Windows Embedded 8.1 Industry Enterprise による機能制限を行う場合、Embedded Features と Embedded Lockdown Manager の実装を最初に行います。コントロール パネルにて Embedded Features を追加し、マイクロソフト ダウンロード センターより最新のアップデート (KB2932074, KB2932354) をダウンロードして適用します。アップデートファイルは、以下のサイトよりダウンロードできます。

■ マイクロソフト ダウンロード センター
Update for Windows Embedded 8.1 Industry : KB2932074
http://www.microsoft.com/en-us/download/details.aspx?id=42025
Embedded Lockdown Manager : KB2932354
http://www.microsoft.com/en-us/download/details.aspx?id=37020

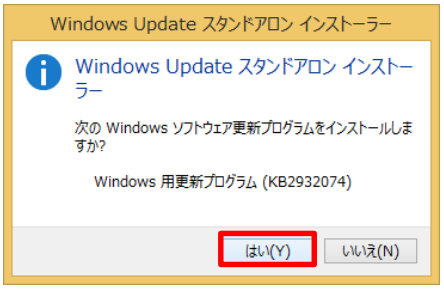
4.2.1 Embedded Features の追加

Embedded Features のアップデート (KB2932074) を適用して、コントロール パネルから Embedded Features を追加する手順について確認します。
この手順は、 WE81IE01、 WE81IE02 コンピューターで実施します。

1) Windows Embedded 8.1 コンピューターに、 Admin ユーザーでサインインします。
※サインイン後、3 節の前提条件で記載のネットワーク情報を構成してください。

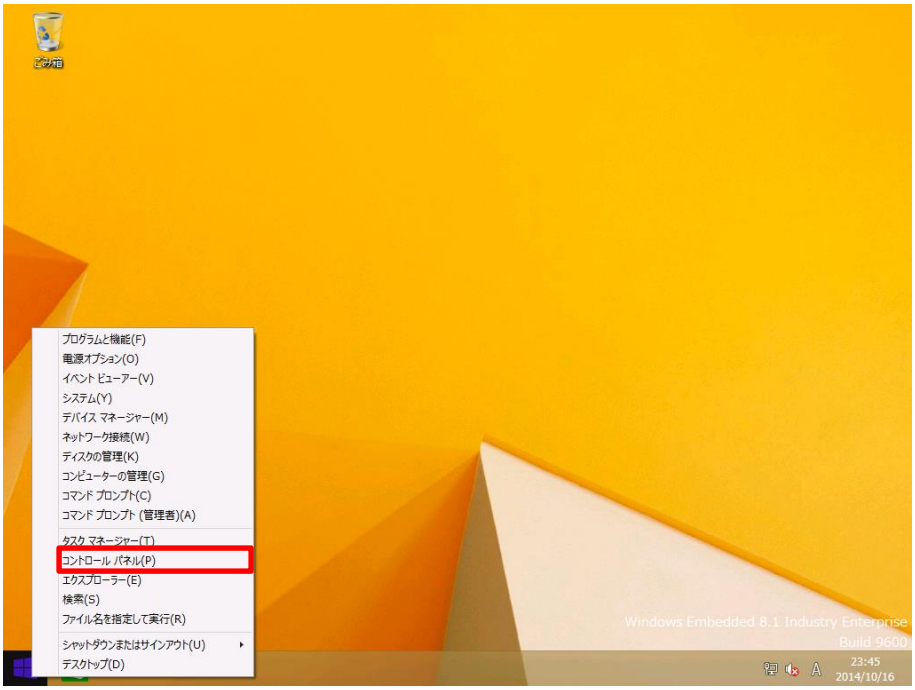
2) ダウンロード センターからダウンロードした [Windows8.1-KB2932074-x**.msu] ファイルを実行します。

3) [Windows Update スタンドアロン インストーラー] 画面で、[はい] をクリックします。



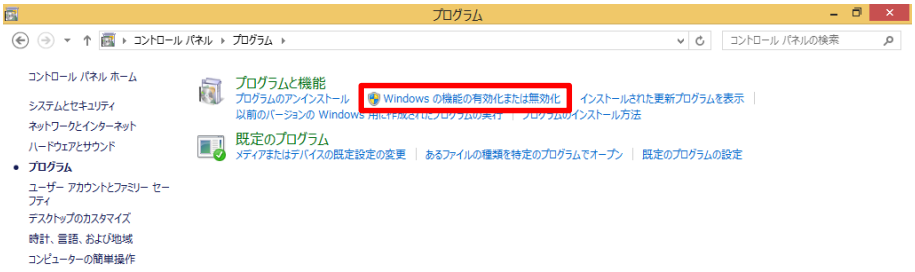
4) [更新プログラムのダウンロードとインストール] 画面で、[閉じる] をクリックします。

5) Windows ボタンを右クリックし、[コントロール パネル] をクリックします。

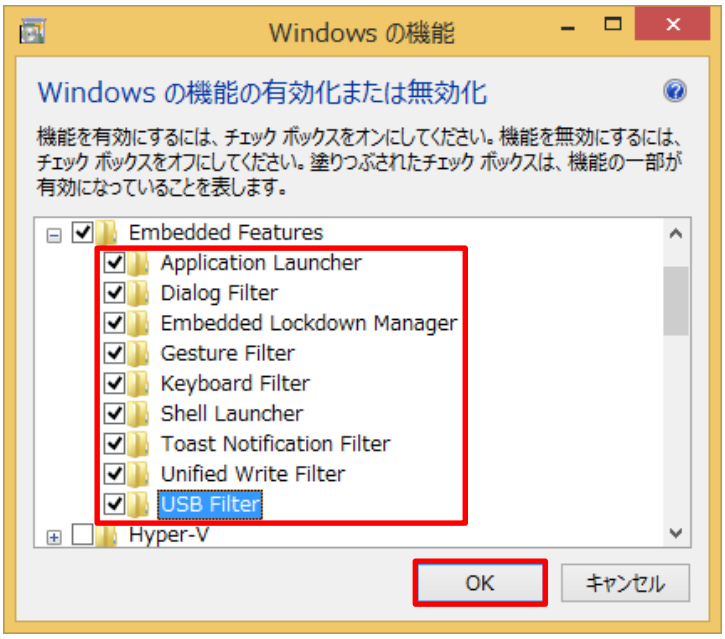


6) [コントロール パネル] 画面で、[プログラム] をクリックします。

7) [プログラム] 画面で、[Windows の機能の有効化または無効化] をクリックします。



8) [Windows の機能] 画面で [Embedded Features] 以下にある、[Application Launcher]、[Dialog Filter]、[Embedded Lockdown Manager]、[Gesture Filter]、[Keyboard Filter]、[Shell Launcher]、[Toast Notification Filter]、[Unified Write Filter]、[USB Filter] をそれぞれ選択し、[OK] をクリックします。
尚、WE81IE02 コンピューターの場合は、 [Embedded Lockdown Manager] にチェックを入れる必要はありません。

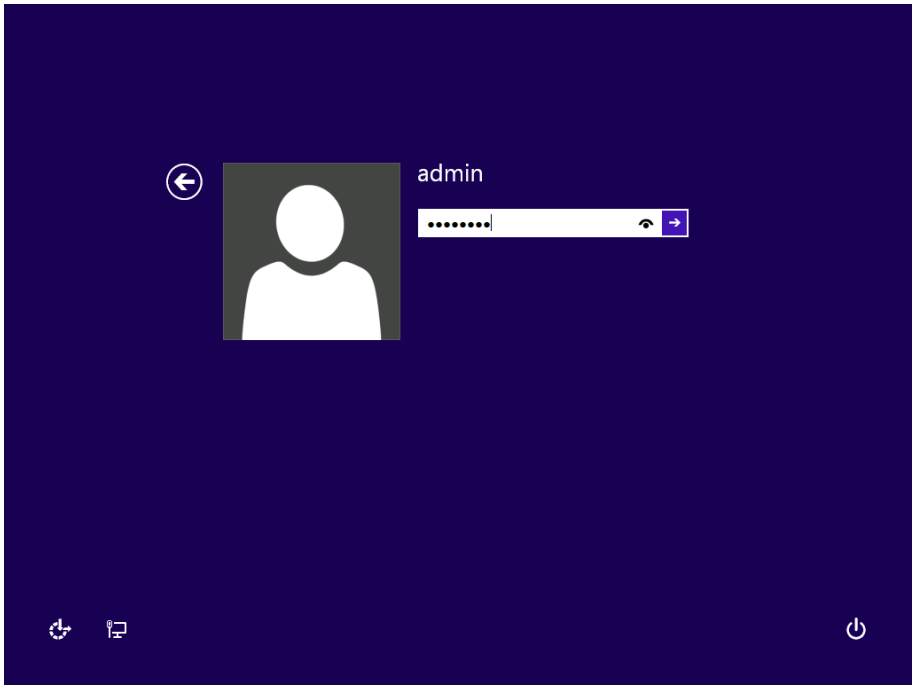


9) [Windows の機能] 画面で、[今すぐ再起動] をクリックします。

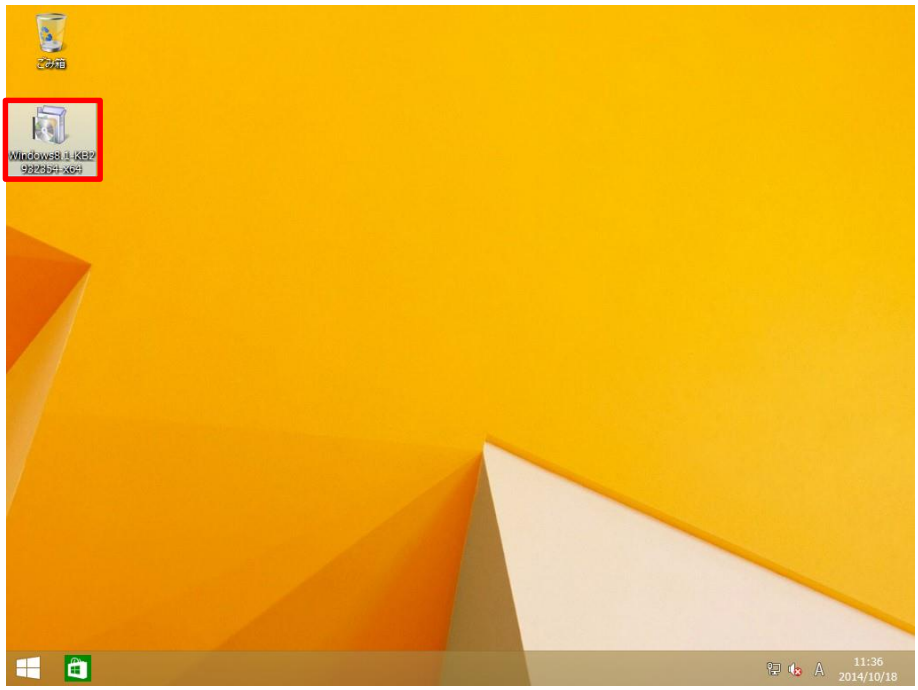
4.2.2 Embedded Lockdown Manager のインストール

本手順では、ダウンロード センターからダウンロードした Embedded Lockdown Manager のアップデート (KB 2932354) をインストールする手順について確認します。Embedded Lockdown Manager のアップデートをインストールする事で一部の機能が追加されます。

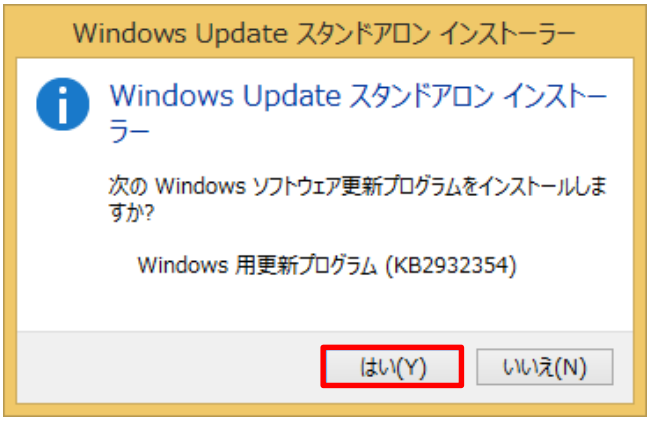
1) WE81IE01 に、 Admin ユーザーでサインインします。



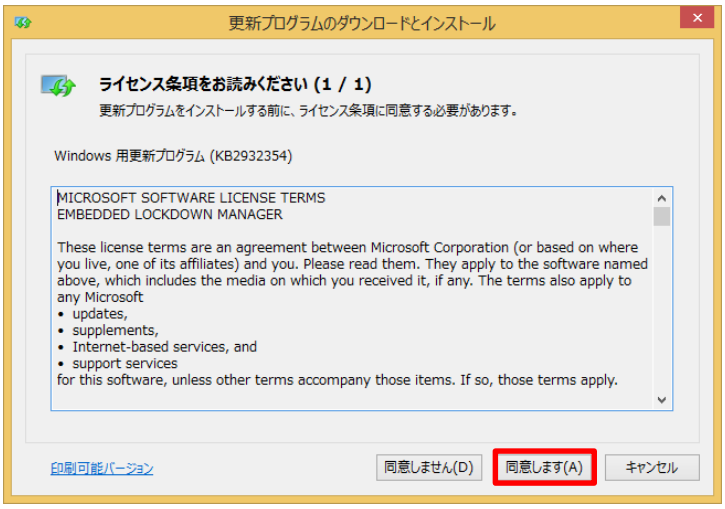
2) ダウンロード センターからダウンロードした [Windows8.1-KB293254-x**.msu] ファイルを実行します。



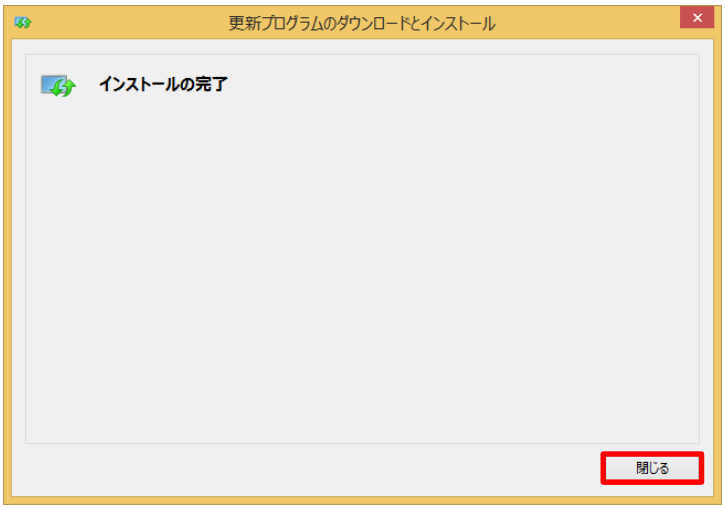
3) [Windows Update スタンドアロン インストーラー] 画面で、[はい] をクリックします。



4) [更新プログラムのダウンロードとインストール] 画面で、[同意します] をクリックします。



5) [更新プログラムのダウンロードとインストール] 画面で、[閉じる] をクリックします。



6) マシンを再起動します。

4.3 Embedded Lockdown Manager でのロックダウン設定

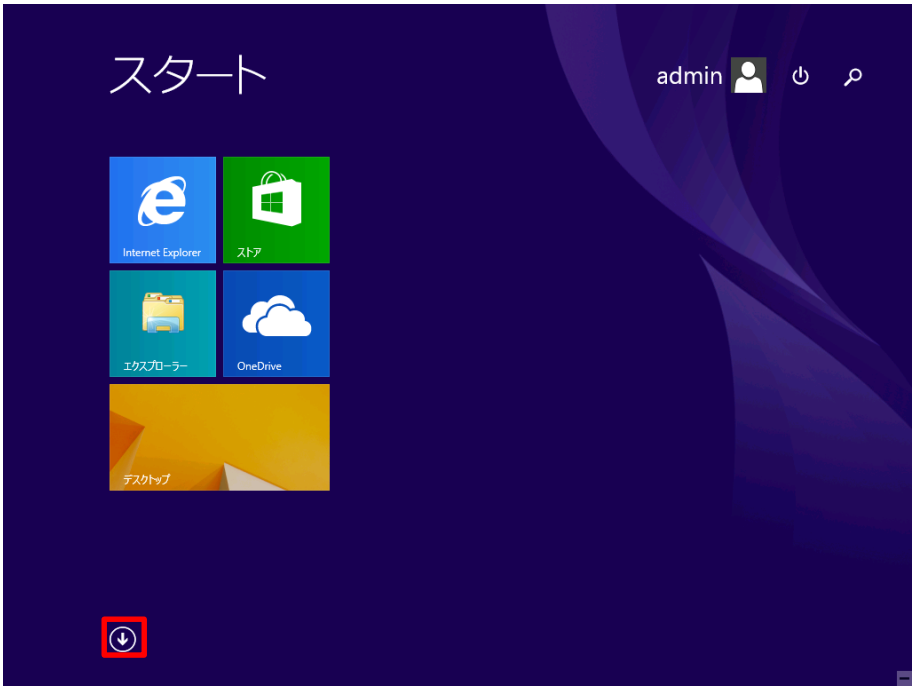
本節では、Embedded Lockdown Manager を利用して、ロックダウンが設定できることを確認します。設定例として、書き込みフィルターを利用して Windows Embedded 8.1 Industry Enterprise コンピューターへのファイルの書き込みを制限する手順と、設定した制限を解除する手順について確認します。

4.3.1 書き込みフィルターによるロックダウン設定

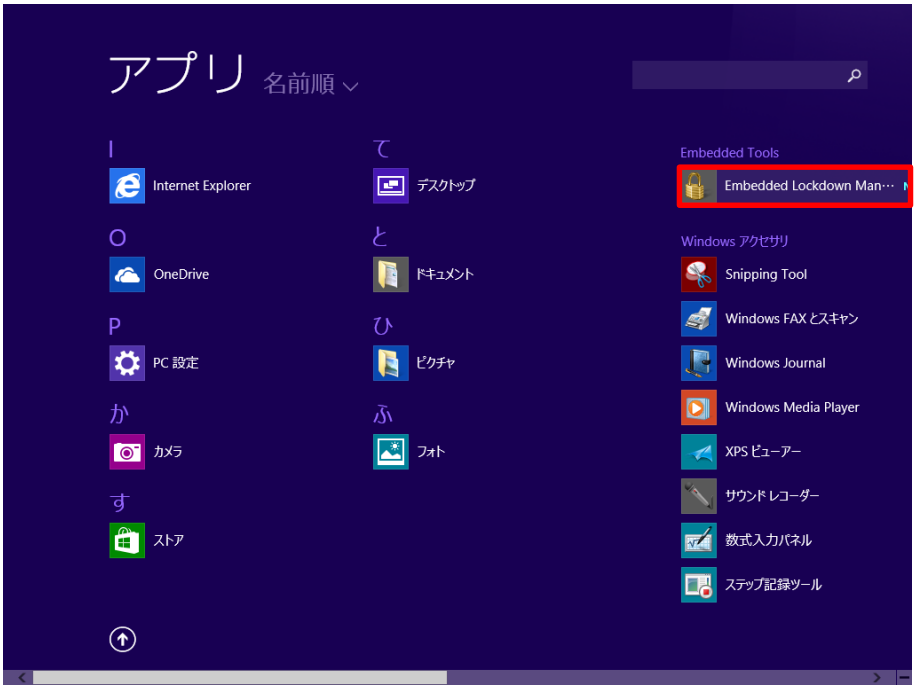
本手順では、Embedded Lockdown Manager を起動し、書き込みフィルターを有効にします。

1) WE81IE01 に、Admin ユーザーでサインインします。

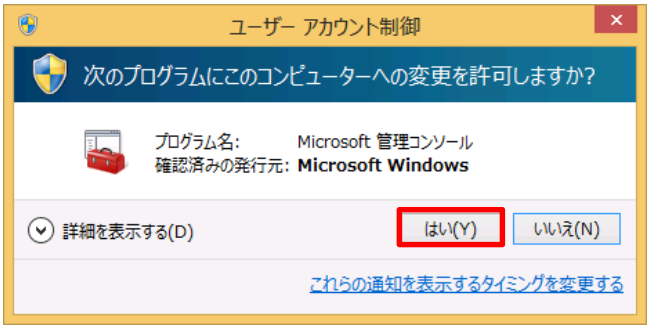
2) スタート画面の ↓ をクリックします。



3) スタート画面で、[Embedded Lockdown Manager] をクリックします。

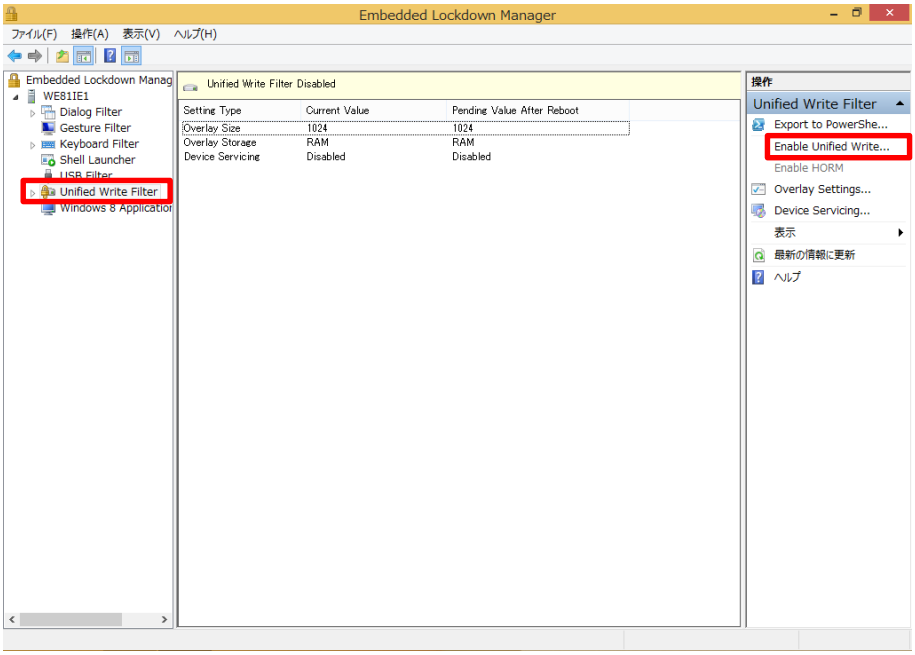


4) [ユーザー アカウント制御] 画面で、[はい] をクリックします。

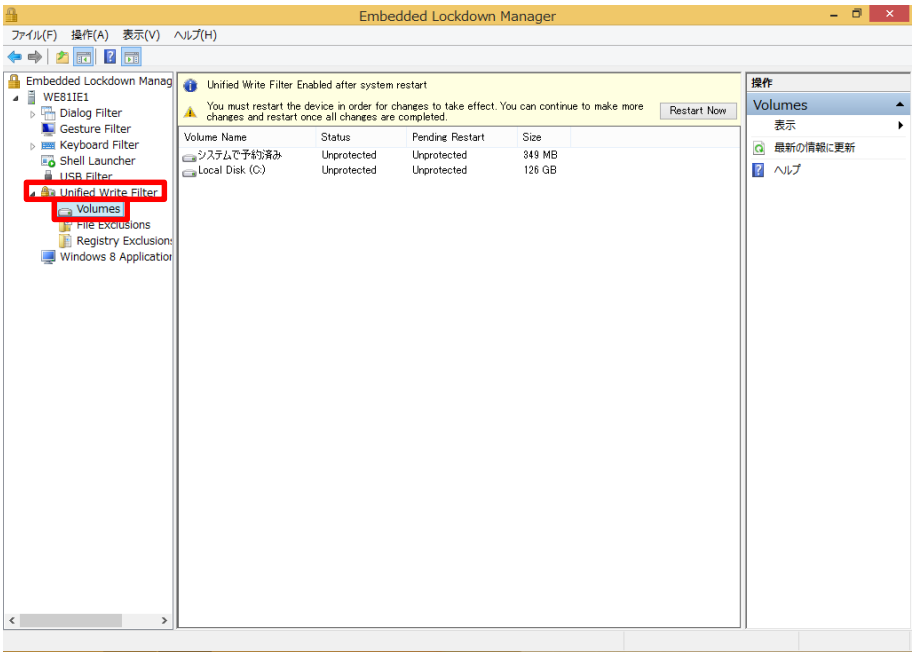


5) [Customer Experience Improvement Program] 画面で、[No, thanks] をクリックし、[OK] をクリックします。

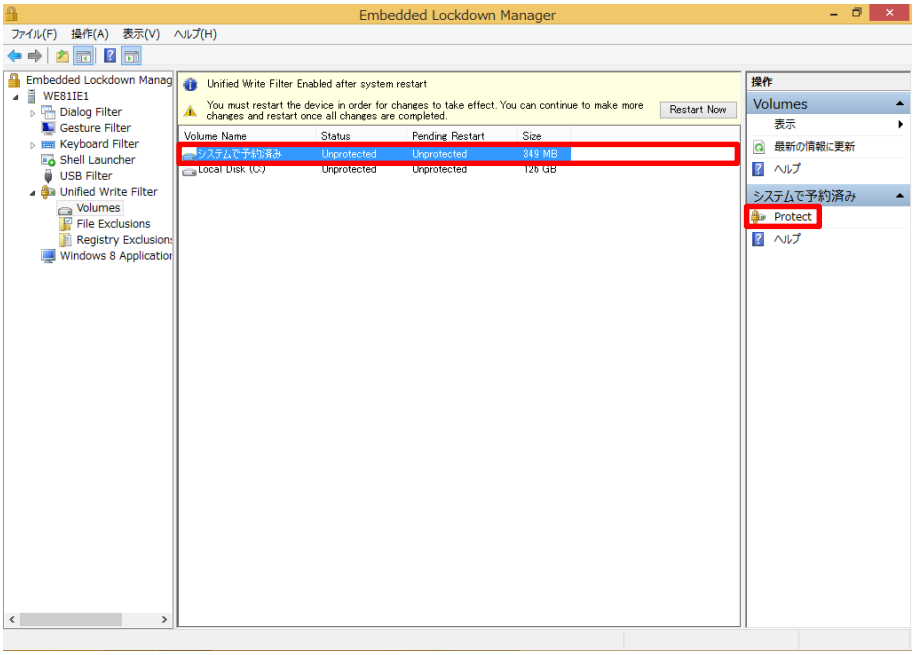
6) [Embedded Lockdown Manager] 画面で、左ペインの [Unified Write Filter] をクリックし、右ペインの [Enable Unified Write Filter] をクリックします。



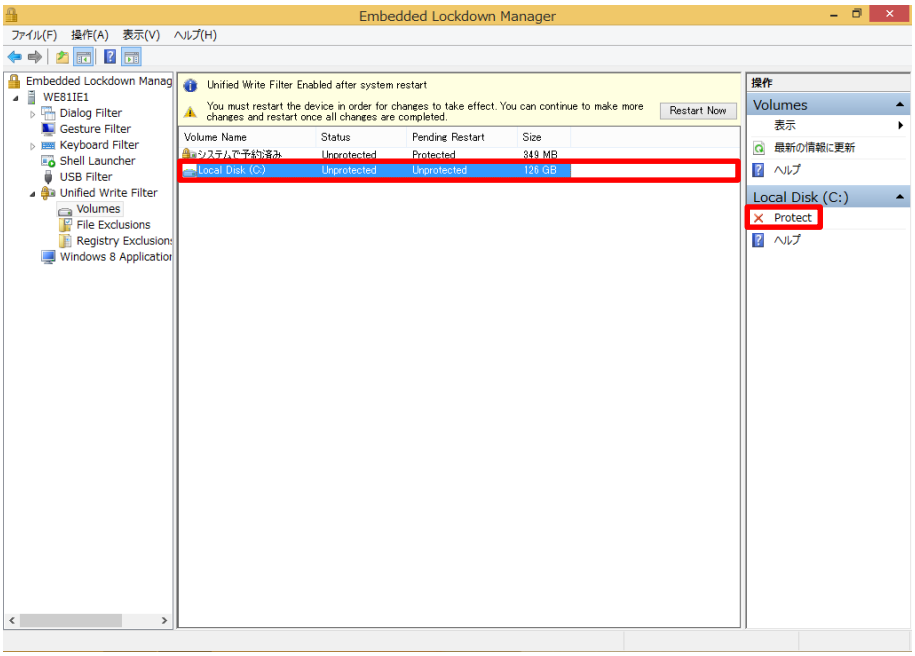
7) [Embedded Lockdown Manager] 画面で、左ペインの [Unified Write Filter] - [Volumes] をクリックします。



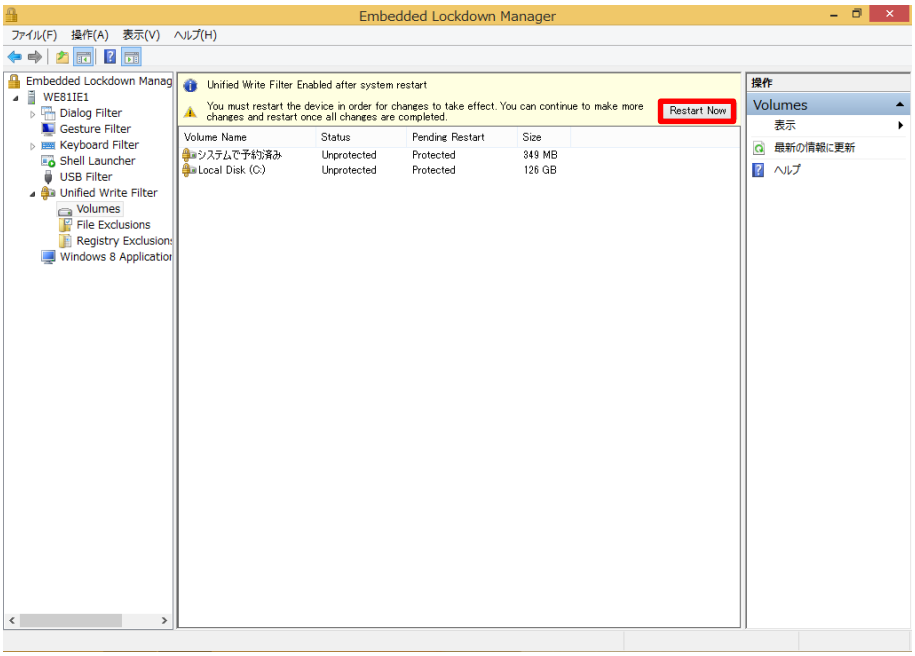
8) [Embedded Lockdown Manager] 画面で、中央ペインの [システムで予約済み] をクリックし、右ペインの [Protect] をクリックします。



9) [Embedded Lockdown Manager] 画面で、中央ペインの [Local Disk (C:)] をクリックし、右ペインの [Protect] をクリックします。



10) [Embedded Lockdown Manager] 画面で、中央ペインの [Restart Now] をクリックします。

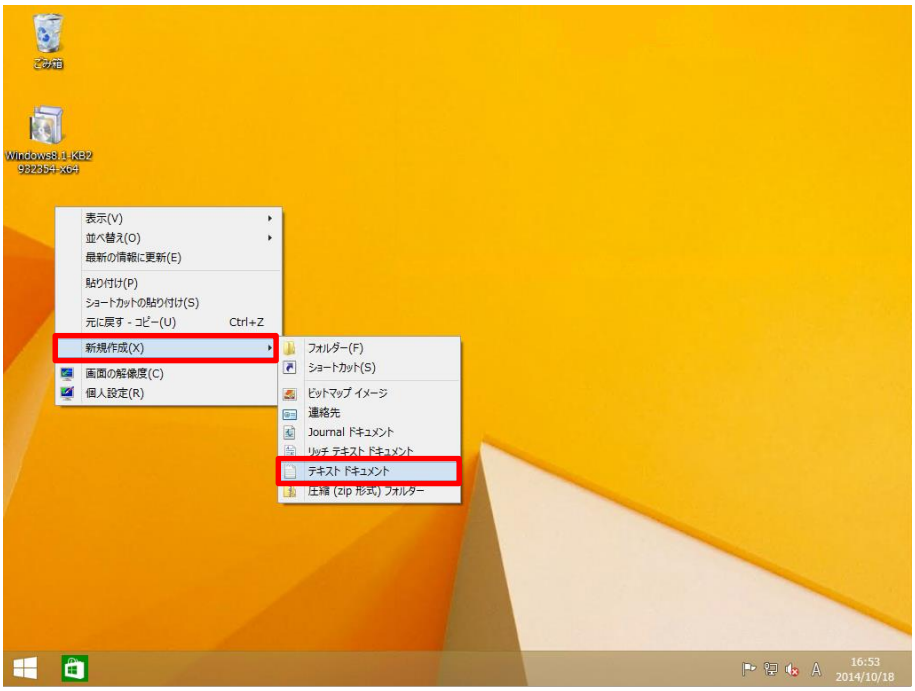


4.3.2 ロックダウン設定の確認

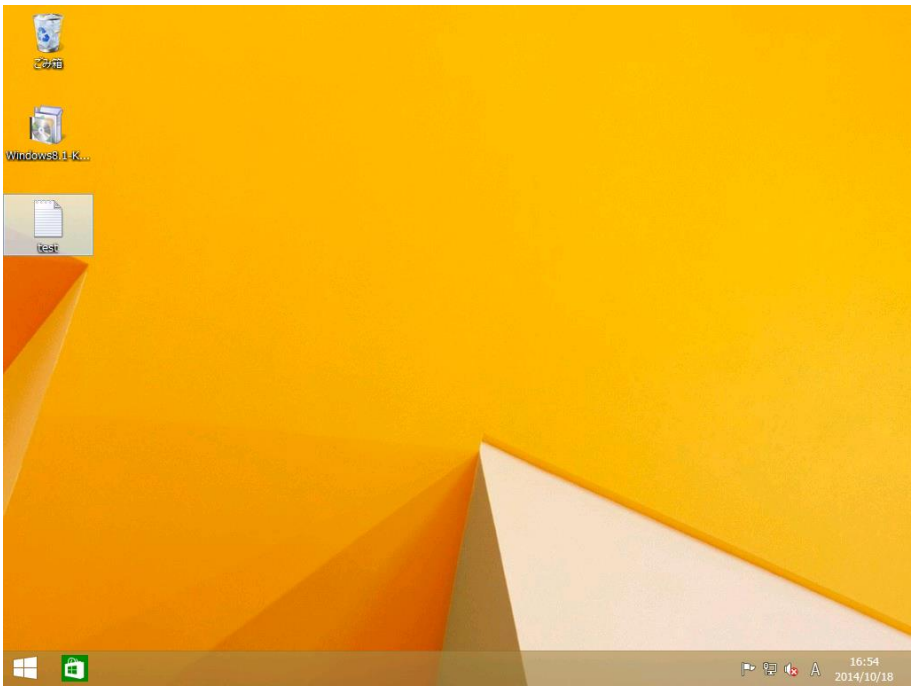
本手順では、前の手順で行った Embedded Lockdown Manager によるロックダウン設定が適用されていることを確認します。

1) WE81IE01 に、Admin ユーザーでサインインします。

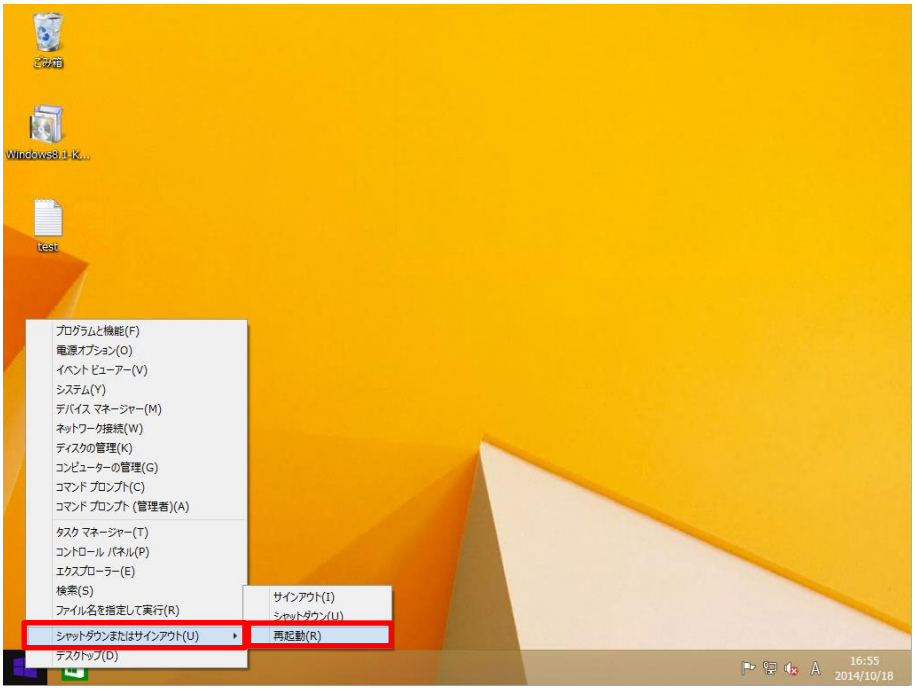
2) デスクトップ画面で、デスクトップを右クリックし、[新規作成] - [テキスト ドキュメント] をクリックして、ファイルを作成します。



3) 作成したファイルに対して、必要に応じてファイルの名前を変更します。また、ファイルをダブルクリックしてメモ帳を開き、適当に文字を入力し、上書き保存します。

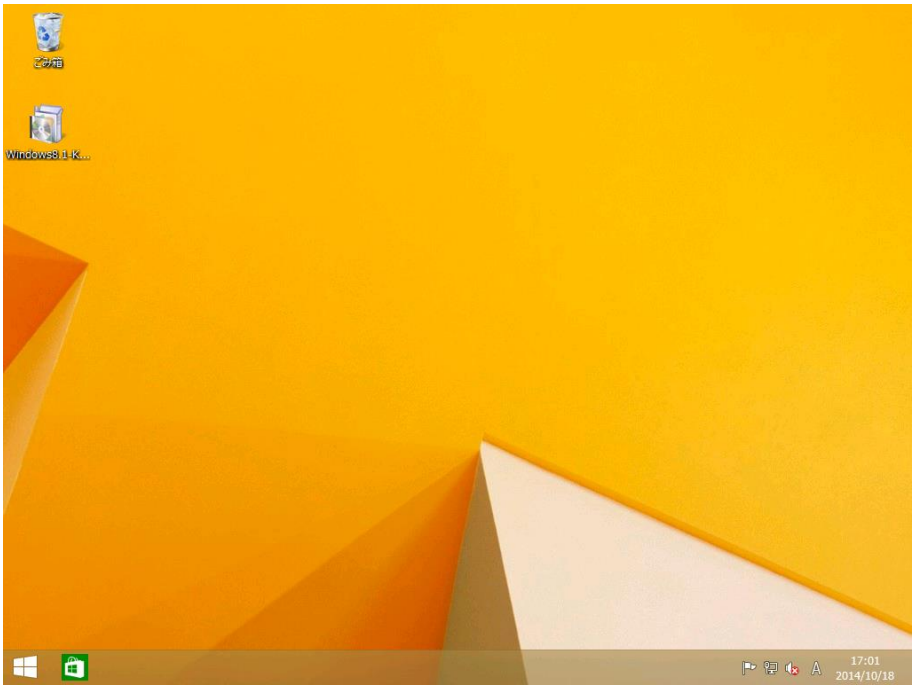


4) スタートボタンを右クリックし、[シャットダウンまたはサインアウト] - [再起動] をクリックします。



5) 再起動後、 Admin ユーザーでサインインします。

6) デスクトップ画面に前の手順で作成したファイルが保存されていないことを確認します。

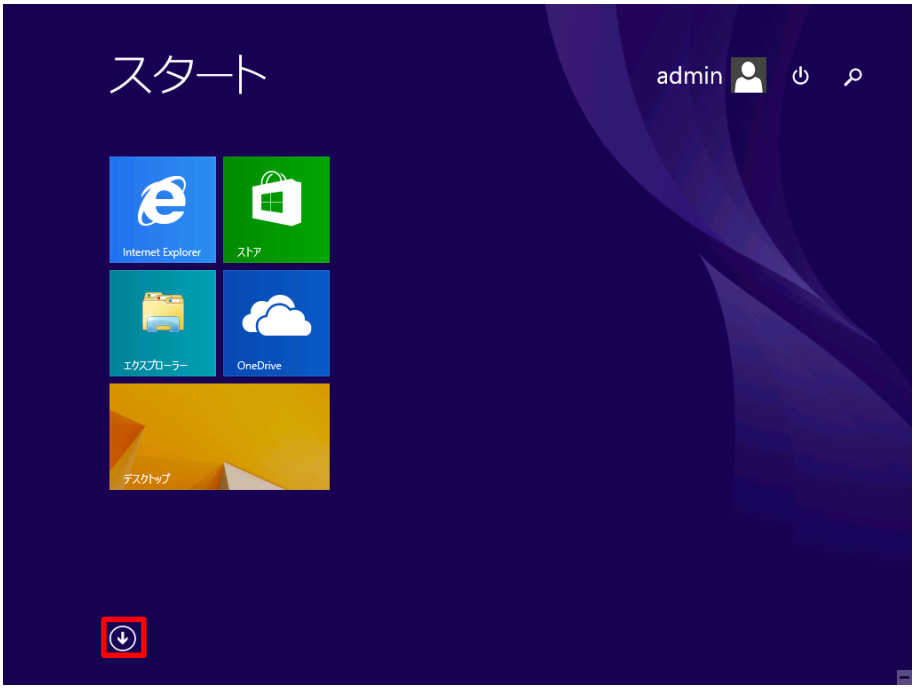


4.3.3 ロックダウン設定の無効化

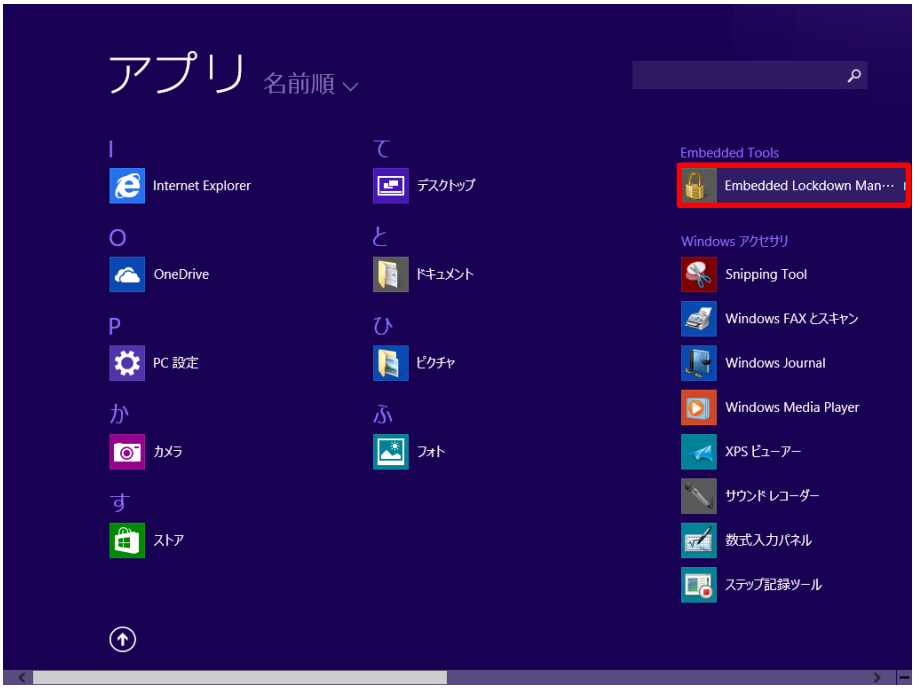
本手順では、以降の手順のために書き込みフィルターを無効にします。

【Note:】
本手順では、書き込みフィルターの無効化を Embedded Lockdown Manager から行いますが、uwfmgr.exe コマンドから無効化することも可能です。無効化する場合、「uwfmgr.exe filter disable」と入力して実行します。また、有効化する場合は「uwfmgr.exe filter enable」、有効化/無効化後の再起動は「uwfmgr.exe restart」コマンドを実行します。

1) WE81IE01 のスタート画面を開き、 ↓ をクリックします。

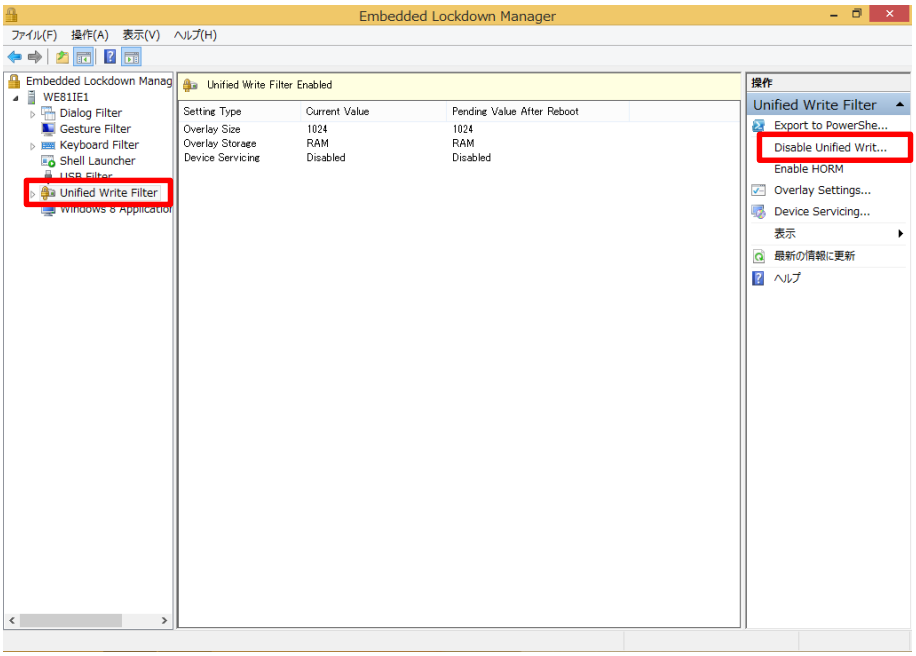


2) スタート画面で、[Embedded Lockdown Manager] をクリックします。

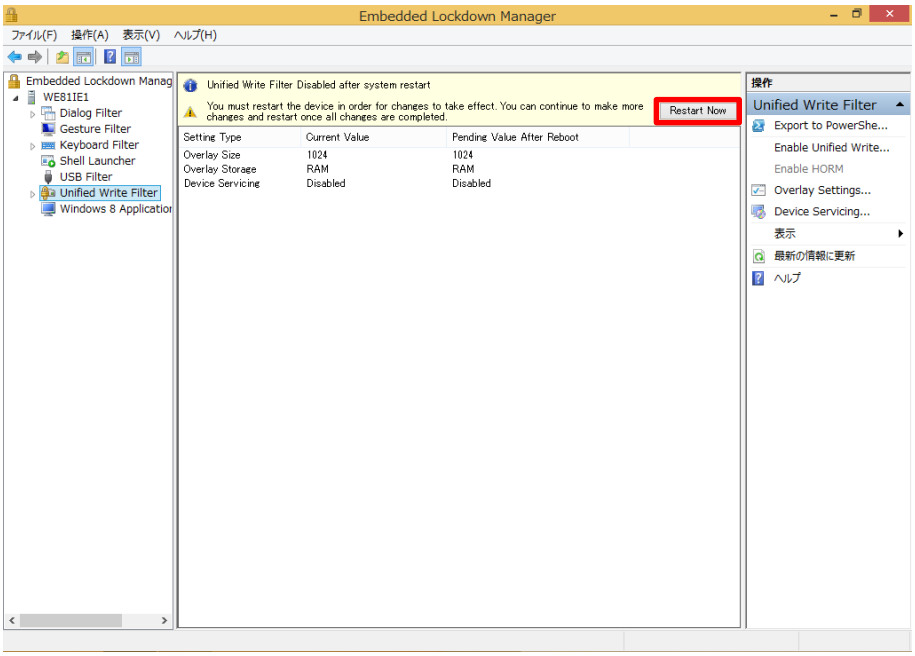


3) [ユーザー アカウント制御] 画面で、[はい] をクリックします。

4) [Embedded Lockdown Manager] 画面で、左ペインの [Unified Write Filter] をクリックし、右ペインの [Disable Unified Write Filter] をクリックします。



5) [Embedded Lockdown Manager] 画面で、中央ペインの [Restart Now] をクリックします。



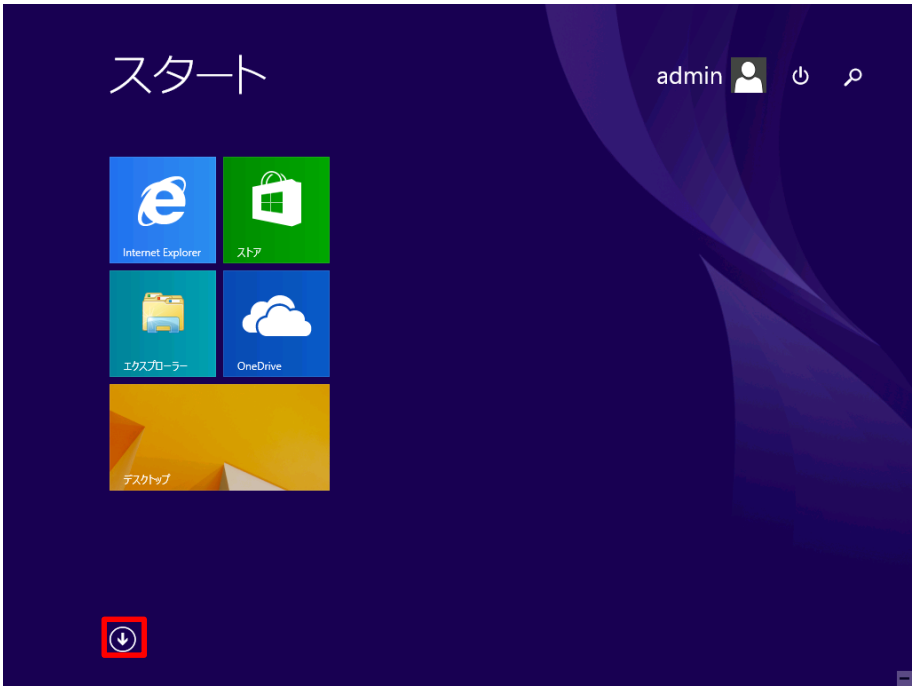
4.4 Windows PowerShell によるロックダウン設定 (オプション)

本節では、Embedded Lockdown Manager を利用せず、Windows PowerShell を利用して、ロックダウンが設定できることを確認します。本節の手順では、WE81IE01 と WE81IE02 の 2 台のコンピューターを利用します。評価を行うときは WE81IE02 コンピューターにも事前に 4.1 節と 4.2.1 節の手順に沿って Windows Embedded 8.1 Industry Enterprise と Embedded Features コンポーネント (Embedded Lockdown Manager は不要) をそれぞれインストールしてください。

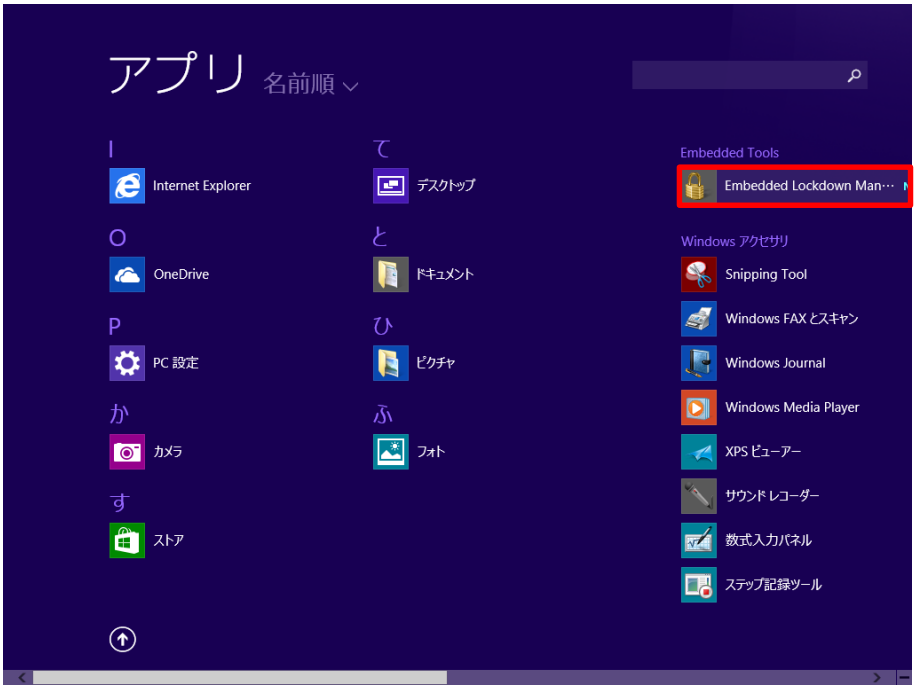
本手順では、WE81IE01 コンピューターの Embedded Lockdown Manager で キーボードフィルターを有効にして、その設定内容を Windows PowerShell スクリプトにエクスポートします。その後、WE81IE02 コンピューターでエクスポートしたスクリプトを実行して設定を反映させます。

1) WE81IE01 に、Admin ユーザーでサインインします。

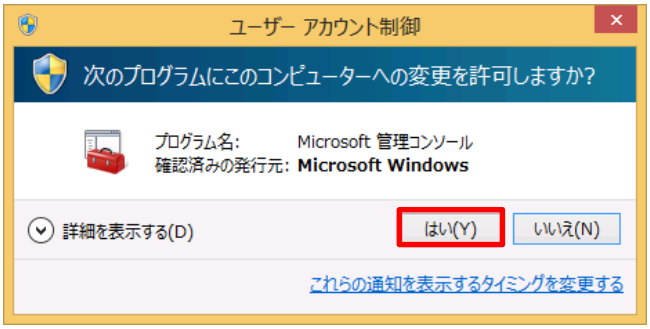
2) スタート画面の ↓ をクリックします。



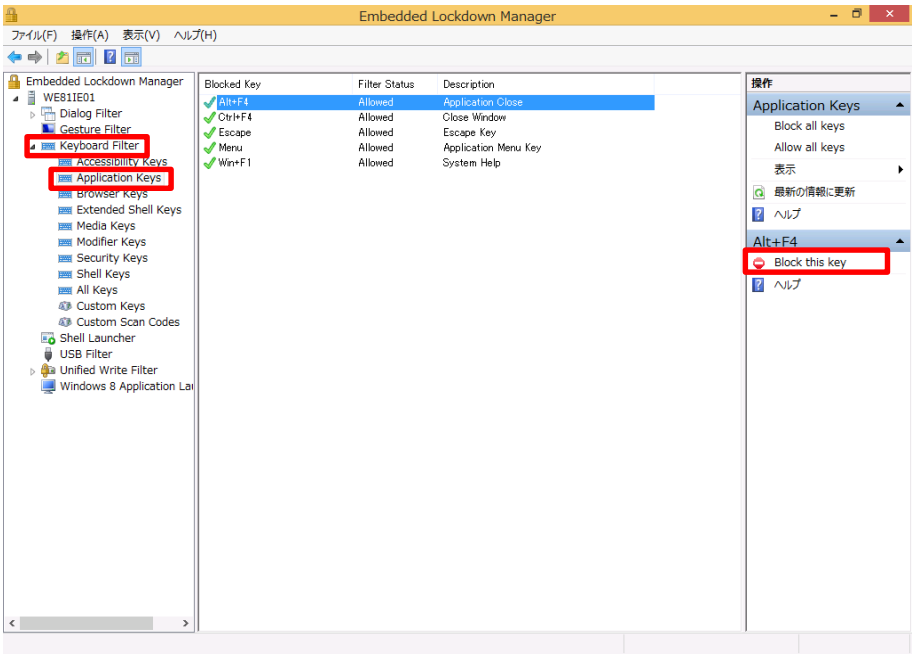
3) スタート画面で、[Embedded Lockdown Manager] をクリックします。



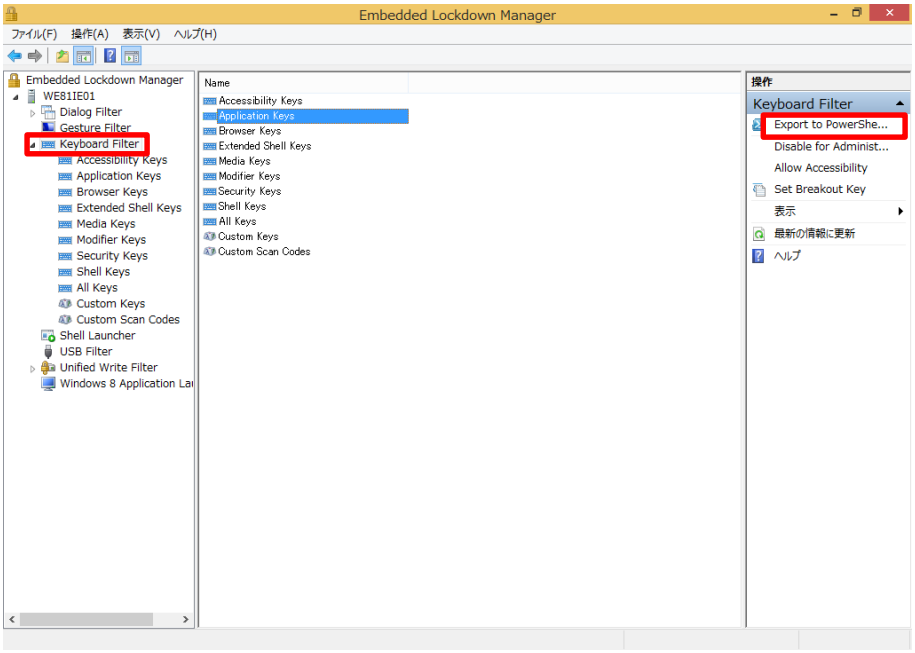
4) [ユーザー アカウント制御] 画面で、[はい] をクリックします。



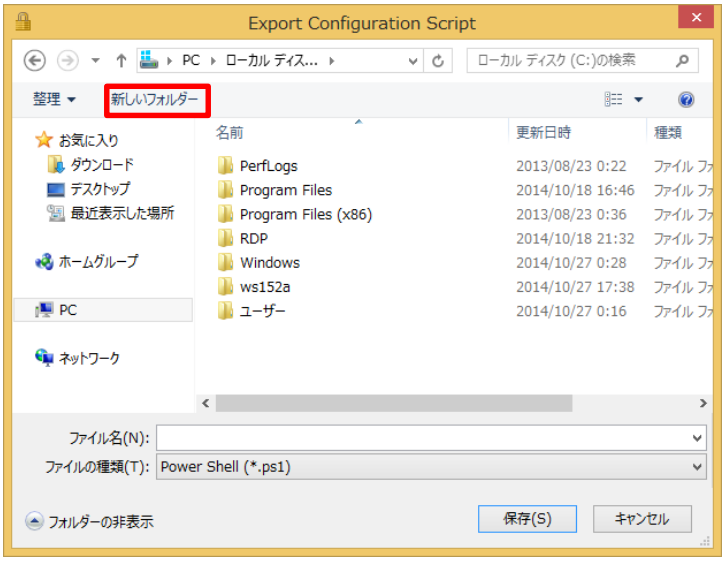
5) [Embedded Lockdown Manager] 画面で、左ペインの [Keyboard Filter] - [Application Filter] をクリックし、中央ペインの [Alt + F4] をクリックし、右ペインの [Block this key] をクリックします。



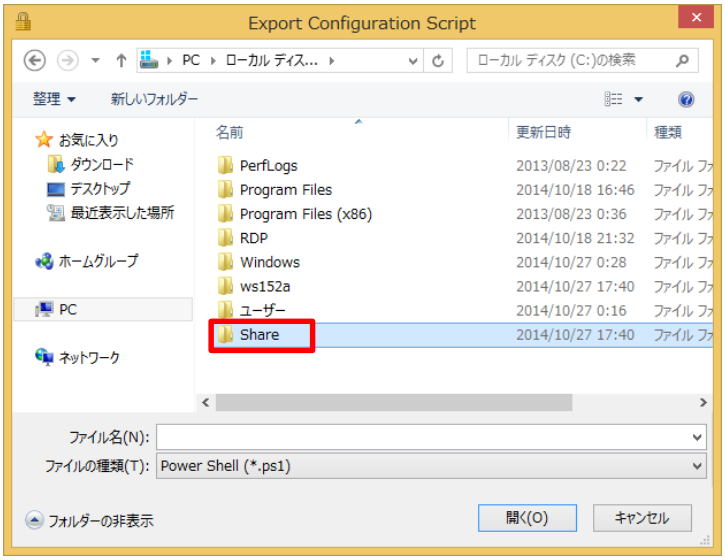
6) [Embedded Lockdown Manager] 画面で、左ペインの [Keyboard Filter] をクリックし、右ペインの [Export to PowerShell] をクリックします。



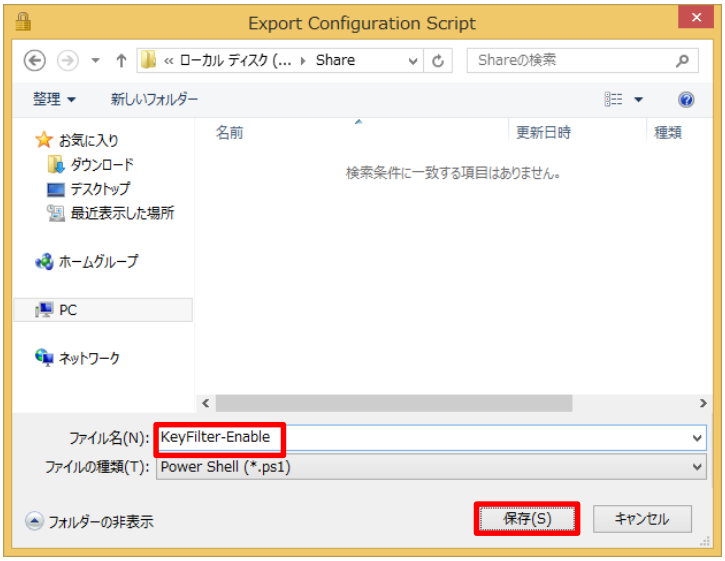
7) [Export Configuration Script] 画面で、C ドライブ直下 (C:¥) に移動して [新しいフォルダー] をクリックします。新しいフォルダーの名前には「Share」を指定します。



8) [Export Configuration Script] 画面で、Share フォルダーを開きます。

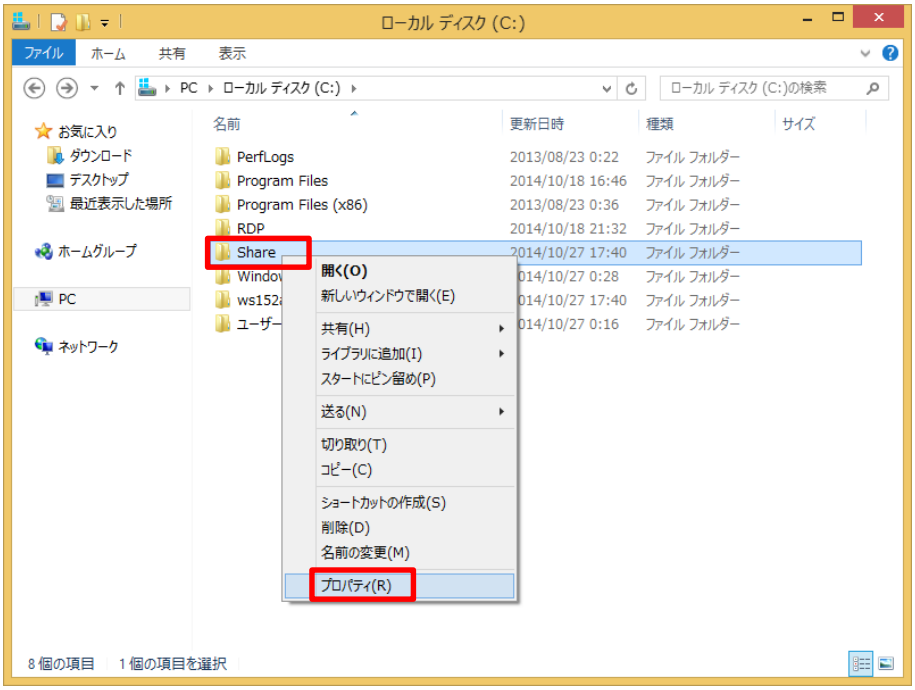


9) [Export Configuration Script] 画面で、[ファイル名] 欄に「KeyFilter-Enable」と入力し、[保存] をクリックします。

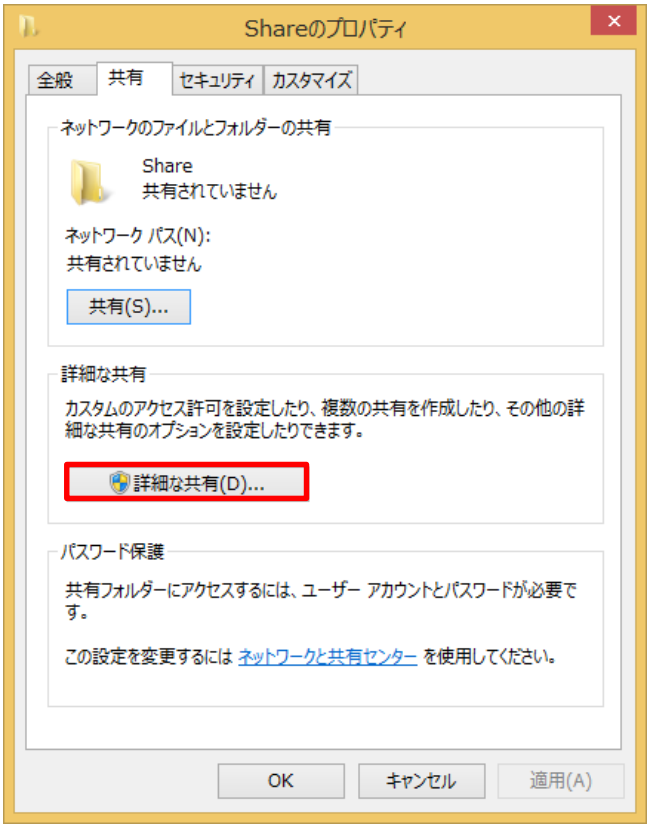


10) [Embedded Lockdown Manager] 画面を閉じます。

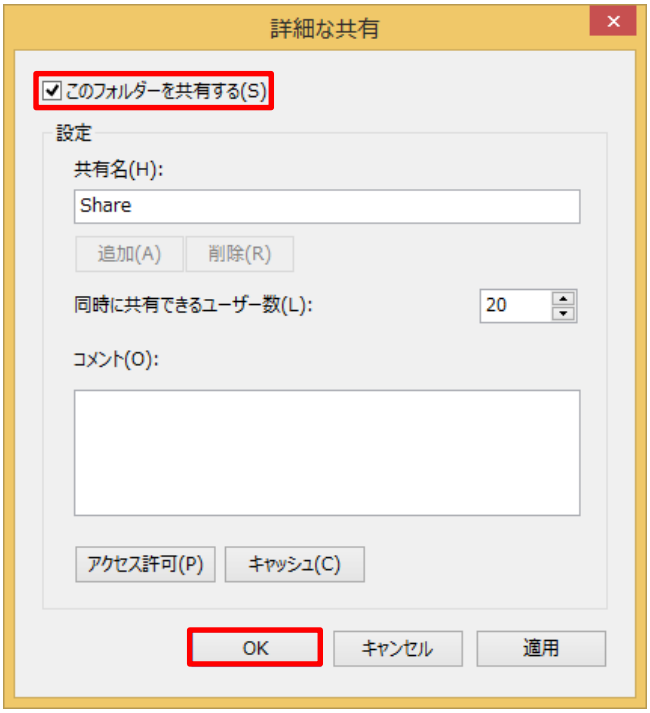
11) Windows エクスプローラーを起動し、C:¥Share を右クリックし、[プロパティ] をクリックします。



12) [Share のプロパティ] 画面で、[詳細な共有] をクリックします。

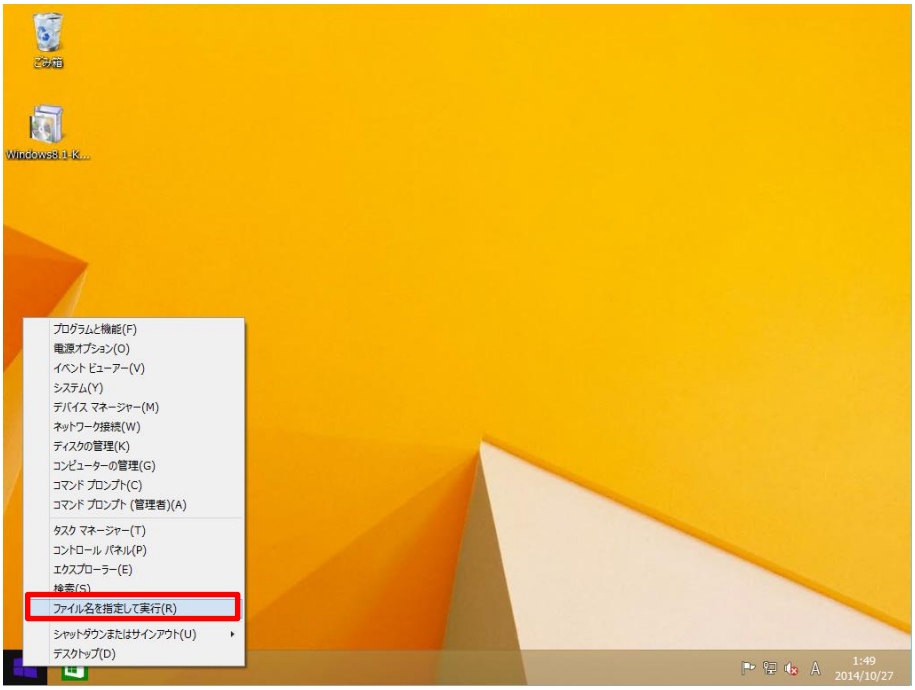


13) [詳細な共有] 画面で、[このフォルダーを共有する] にチェックをつけ、表示されている、すべてのダイアログで [OK] をクリックします。

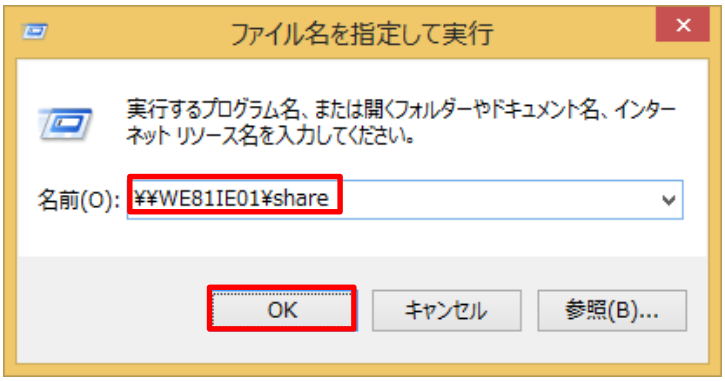


14) WE81IE02 コンピューターに、 Admin ユーザーでサインインします。

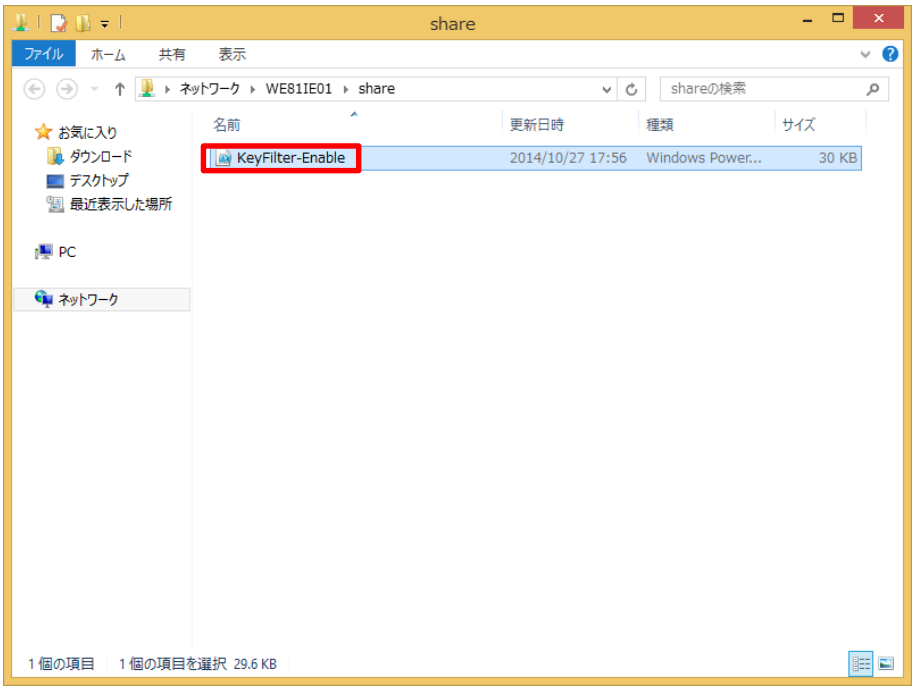
15) スタートボタンを右クリックし、[ファイル名を指定して実行] をクリックします。



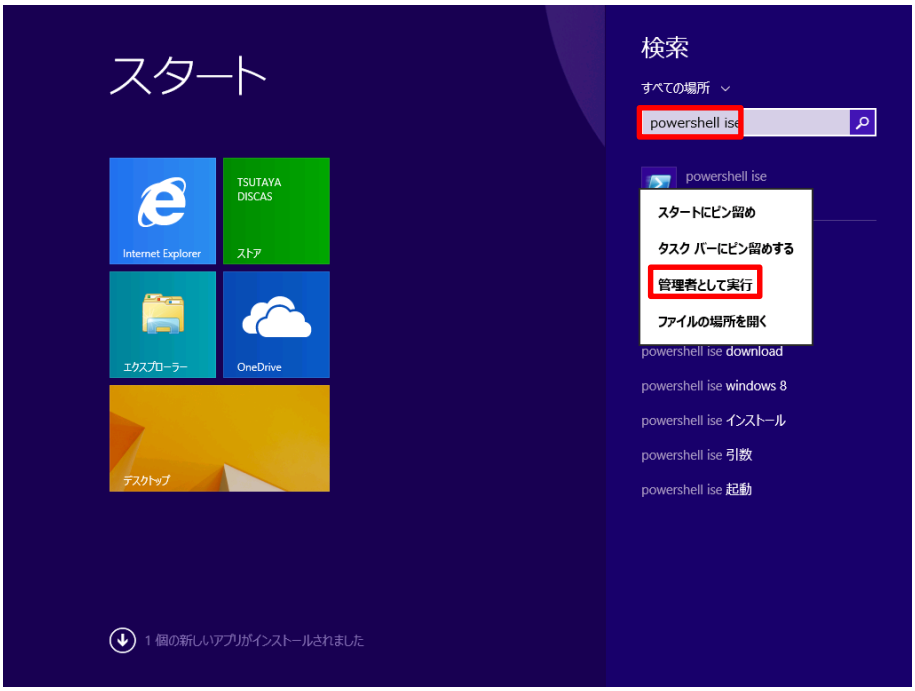
16) [ファイル名を指定して実行] 画面で、「¥¥WE81IE01¥Share」と入力し、[OK] をクリックします。



17) Windows エクスプローラー画面で、共有先の KeyFilter-Enable.ps1 ファイルをローカルのデスクトップにコピーします。

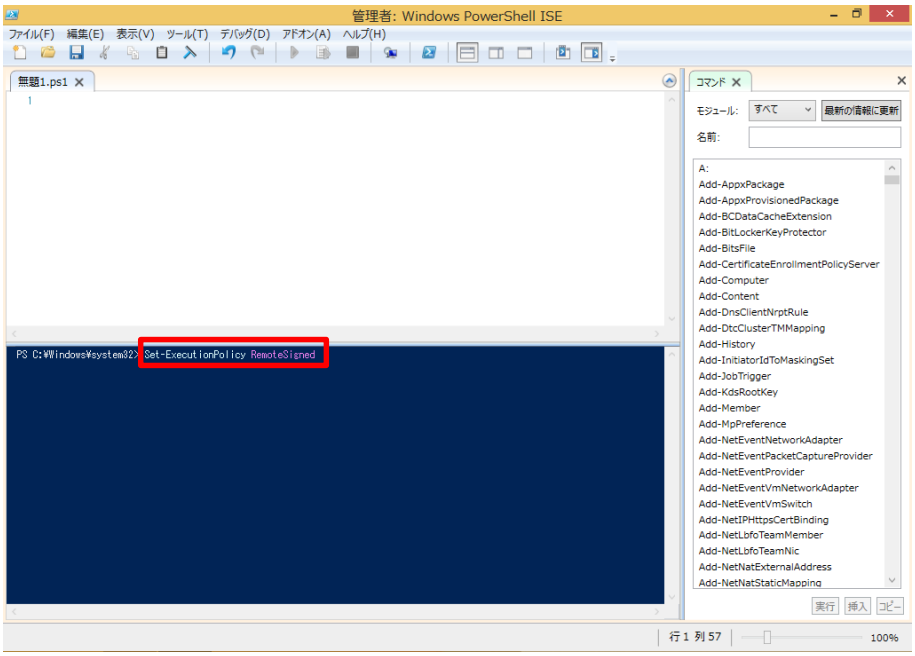


18) スタート画面を開き、「PowerShell ISE」と入力し、表示された [PowerShell ISE] を右クリックして、[管理者として実行] をクリックします。

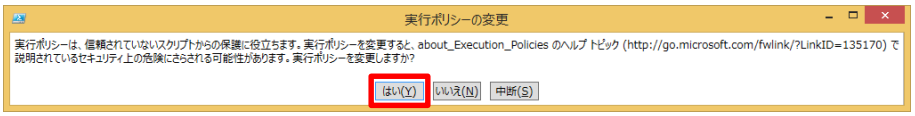


19) [ユーザー アカウント制御] 画面で、[はい] をクリックします。

20) [管理者：Windows PowerShell ISE] 画面で、下ペインに「Set-ExecutionPolicy RemoteSigned」と入力し、Enter キーを押します。



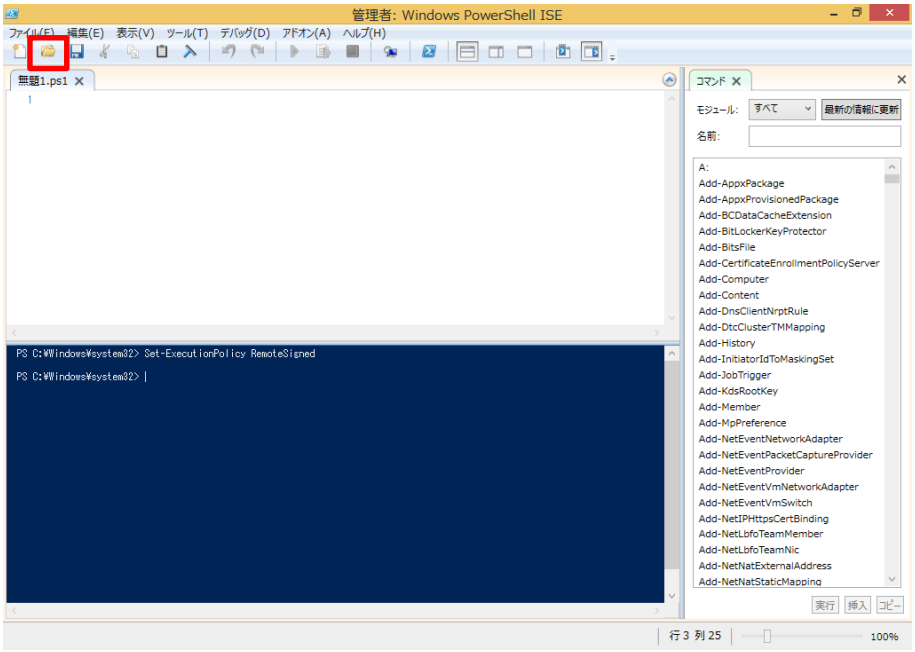
21) [実行ポリシーの変更] 画面で、[はい] をクリックします。



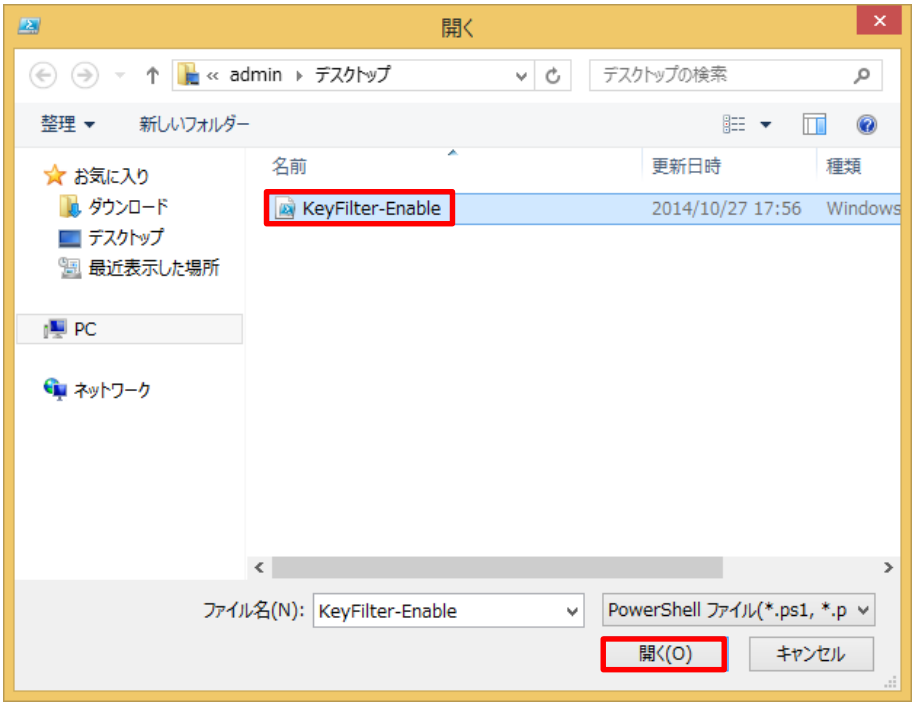
【Note:】

Set-ExecutionPolicy コマンドレットは ps1 拡張子のスクリプトの実行を許可するための設定です。コンピューターで 1 度実行すれば、以降の実行は不要です。

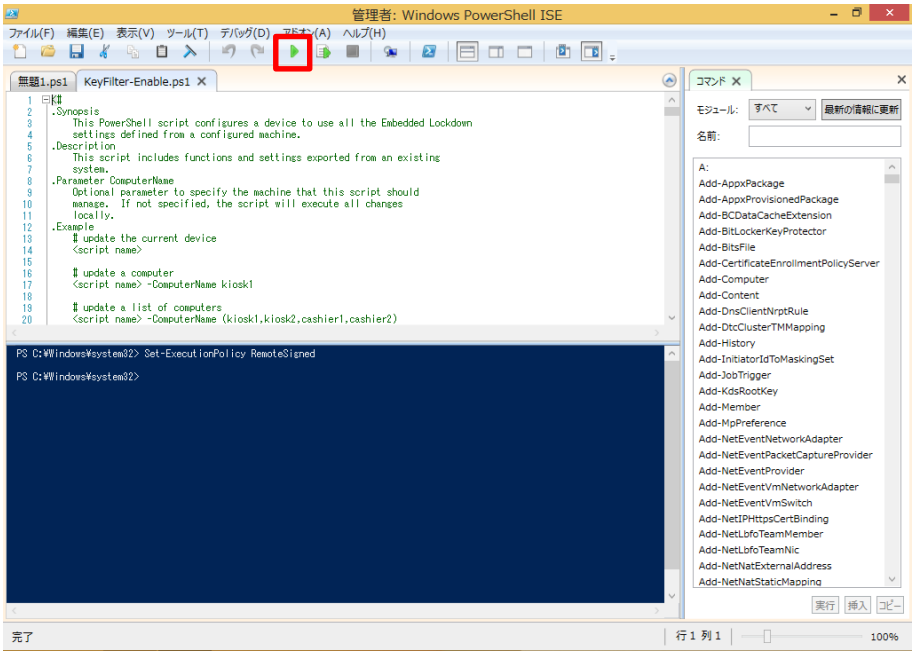
22) [管理者：Windows PowerShell ISE] 画面で、[開く] ボタンをクリックします。



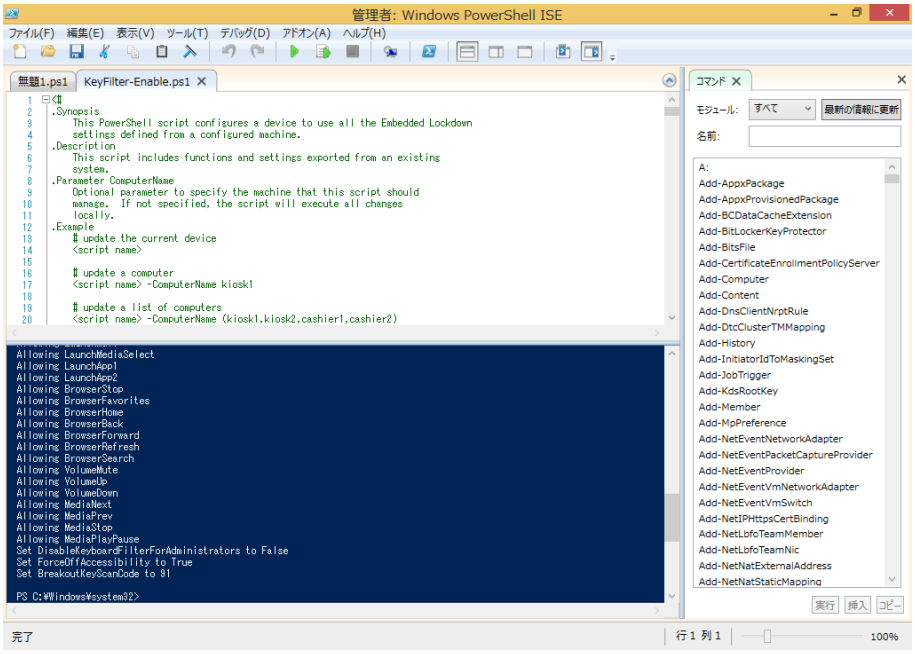
23) [開く] 画面で、デスクトップに保存されている KeyFilter-Enable.ps1 ファイルを選択し、[開く] をクリックします。



24) [管理者：Windows PowerShell ISE] 画面で、実行ボタンをクリックします。



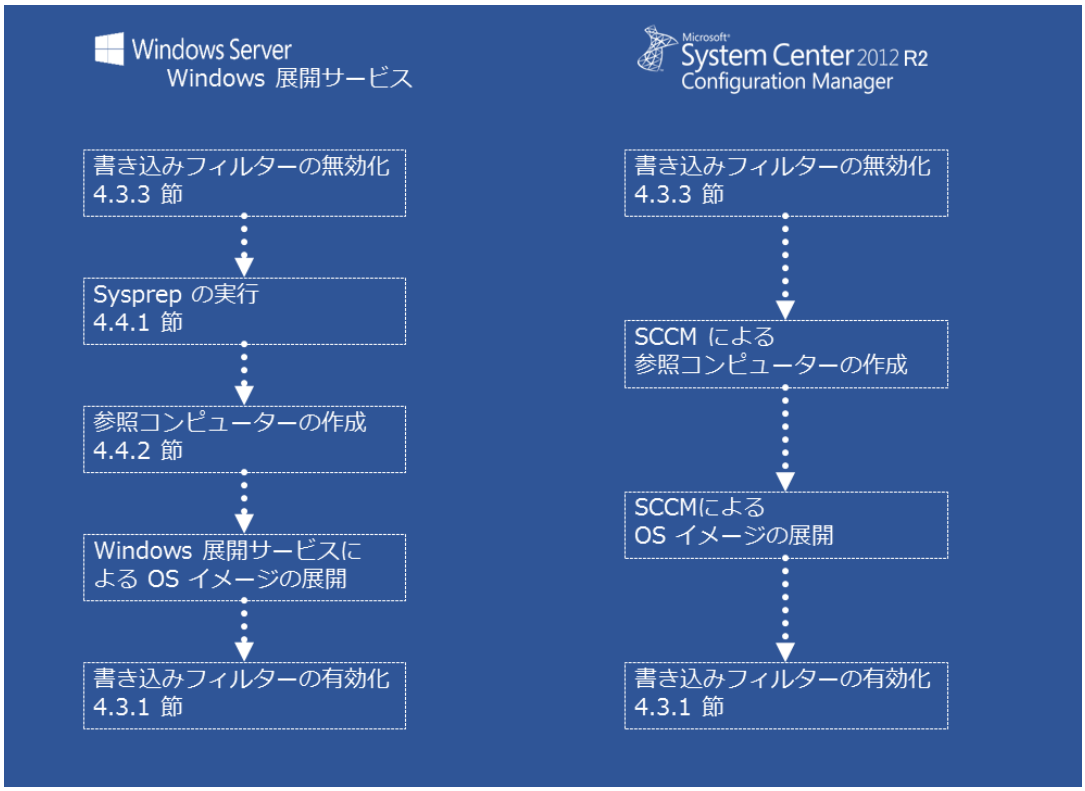
25) [管理者：Windows PowerShell ISE] 画面で、実行が完了すると、Alt+F4 キーが利用できなくなっていることが確認できます。



4.5 キッティング

複数台のコンピューターに対して、Embedded Lockdown Manager によるロックダウン設定を施した OS イメージを展開する場合、通常のコンピューターの OS イメージと同じ展開方法でロックダウン設定済み Windows Embedded 8.1 Industry Enterprise のイメージを展開できます。
ただし、ロックダウン設定に書き込みフィルターが含まれている場合、書き込みフィルターが有効なために OS イメージを作成することができません。そのため、OS イメージ作成時には書き込みフィルターを無効にした上で OS イメージを作成し、イメージ展開後に改めて書き込みフィルターを有効にします。

画面 4.4-1 Windows 展開サービス/SCCM によるキッティング手順



本節では、キッティングを行うために必要な参照コンピューターの作成方法について説明します。参照コンピューターの作成手順と OS イメージの展開方法は Windows 展開サービスを利用して行う方法と、SCCM を利用して行う方法があります。それぞれの方法による展開については、以下のドキュメントまたは Web サイトを参照してください。

【Note:】
OS イメージ展開後のコンピューターに対して書き込みフィルターを有効化する方法については 9 章で説明します。

System Center 2012 R2 Configuration Manager 評価ガイド - OS 展開編
http://www.microsoft.com/ja-jp/download/details.aspx?id=41687

Windows 展開サービスの概要
http://technet.microsoft.com/ja-jp/library/hh831764.aspx

Windows ADK による標準イメージの作成手順 評価ガイド
http://technet.microsoft.com/ja-jp/library/hh831764.aspx

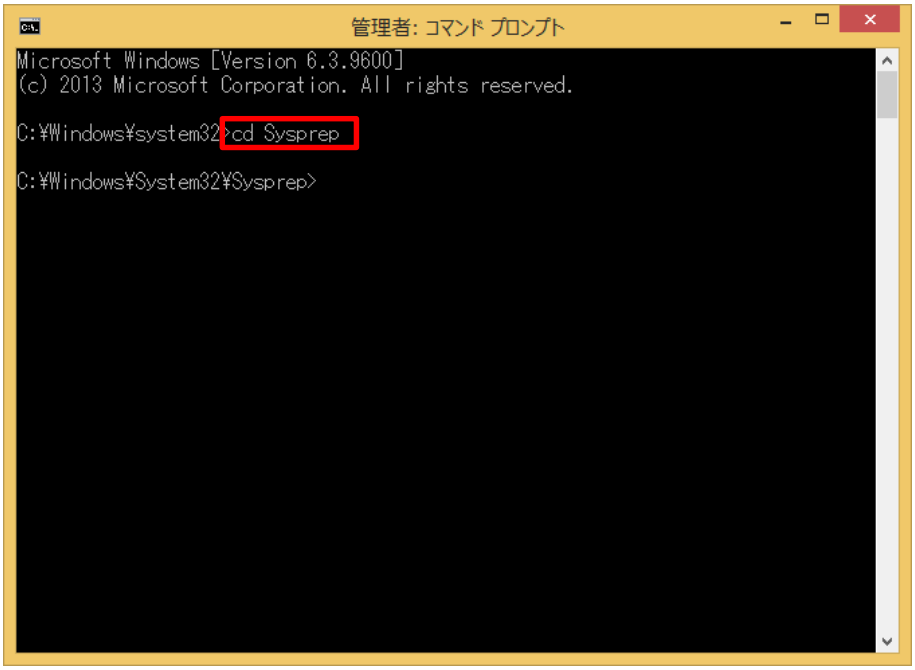
4.5.1 Sysprep の実行

参照コンピューターを作成するための最初のステップとして、書き込みフィルターを無効にしたコンピューターを対象に、Sysprep コマンドを実行し、参照コンピューターの一般化を行います。

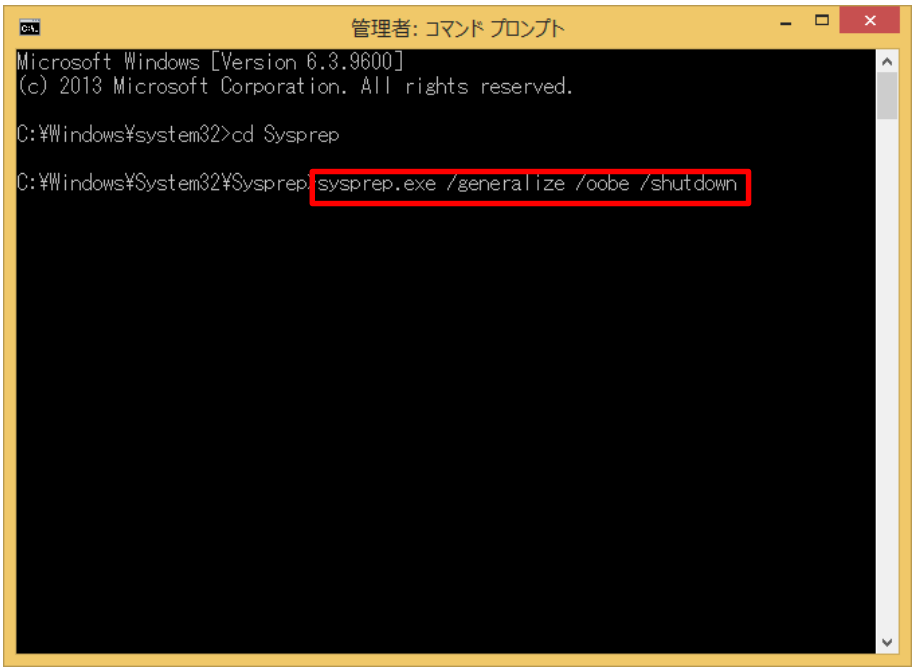
1) Widnows Embedded 8.1 Industry Enterprise コンピューターで、スタートボタンを右クリックし、[コマンド プロンプト (管理者)] をクリックします。

2) [ユーザー アカウント制御] 画面で、[はい] をクリックします。

3) [管理者:コマンドプロンプト] 画面で、「cd sysprep」と入力し、Enter キーを押します。



4) ［管理者：コマンドプロンプト］ 画面で、「Sysprep /generalize /oobe /shutdown」と入力し、Enter キーを押します。



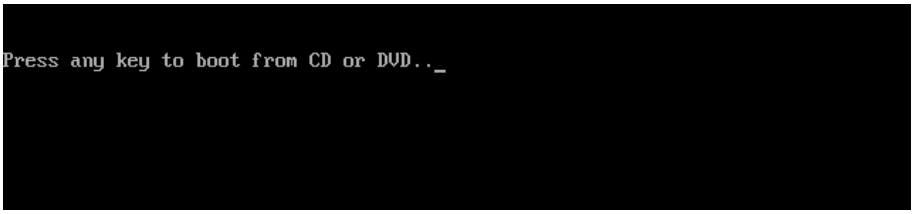
4.5.2 参照コンピューターの作成

Sysprep で一般化した参照コンピューターを OS イメージとしてキャプチャする手順を確認します。本手順を実行するにあたり、起動可能な Windows PE 4.0 ディスクを事前に用意する必要があります。Windows PE ディスクの作成に当たっては Windows アセスメント & デプロイメント キット (Windows ADK) をマイクロソフト ダウンロードセンターから入手し、作成する必要があります。具体的な Windows PE ディスクを作成する方法については、以下の Web サイトを参照してください。

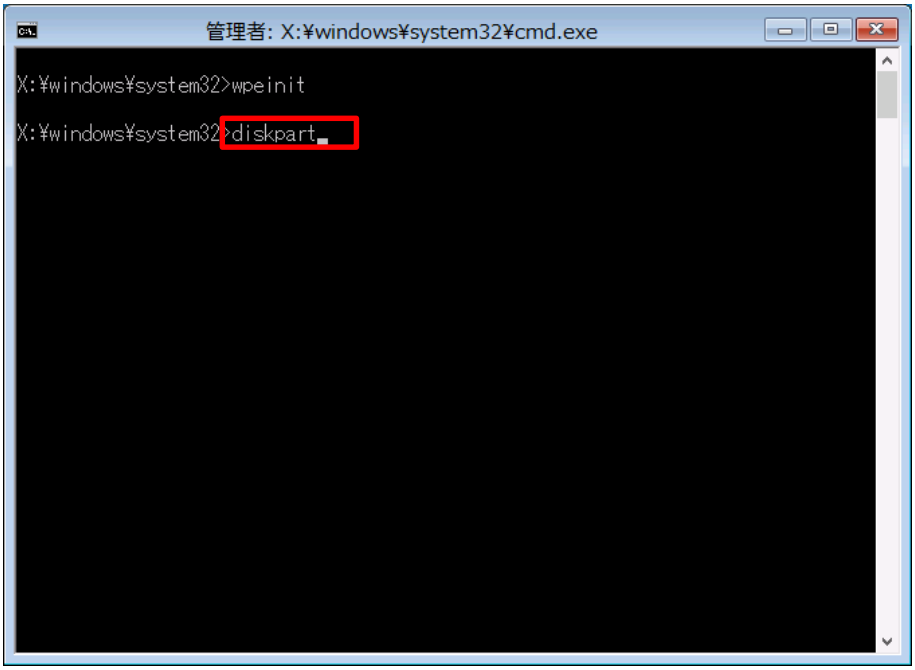
Windows ADK による標準イメージの作成手順 評価ガイド
http://technet.microsoft.com/ja-jp/library/hh831764.aspx

1) 参照コンピューターに Windows PE ディスクを差し込み、コンピューターを起動します。

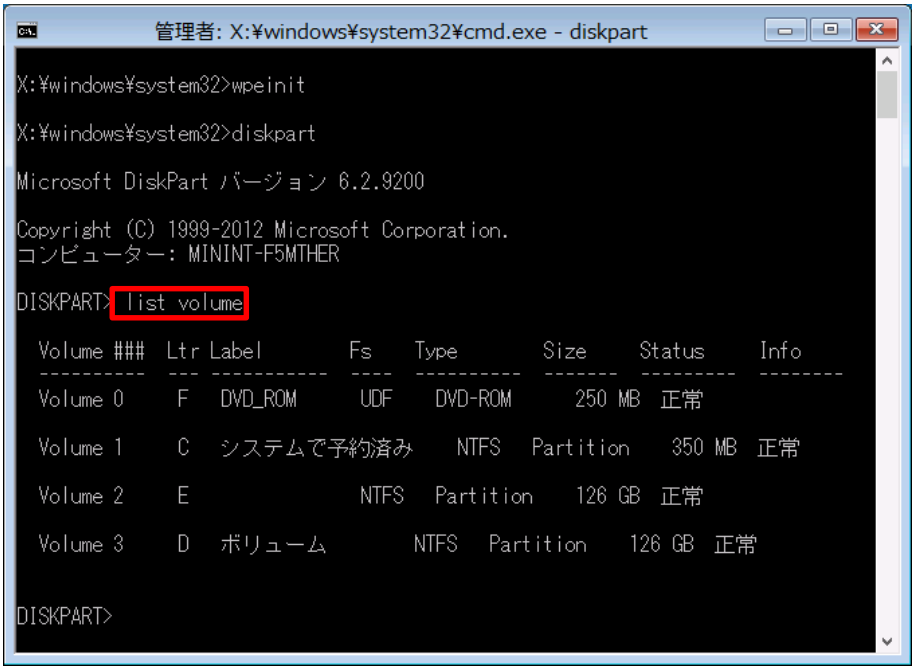
2) コンピューターの起動画面で、[Press any key to boot from CD or DVD] の文字が表示されているタイミングで Enter キーを押します。



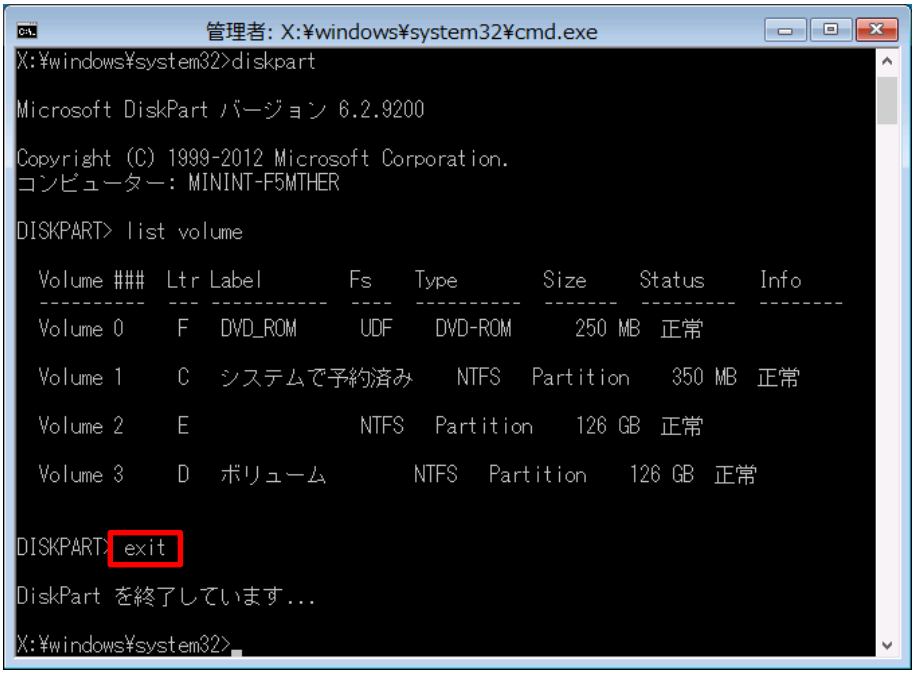
3) コマンドプロンプト画面で、「diskpart」と入力し、Enter キーを押します。



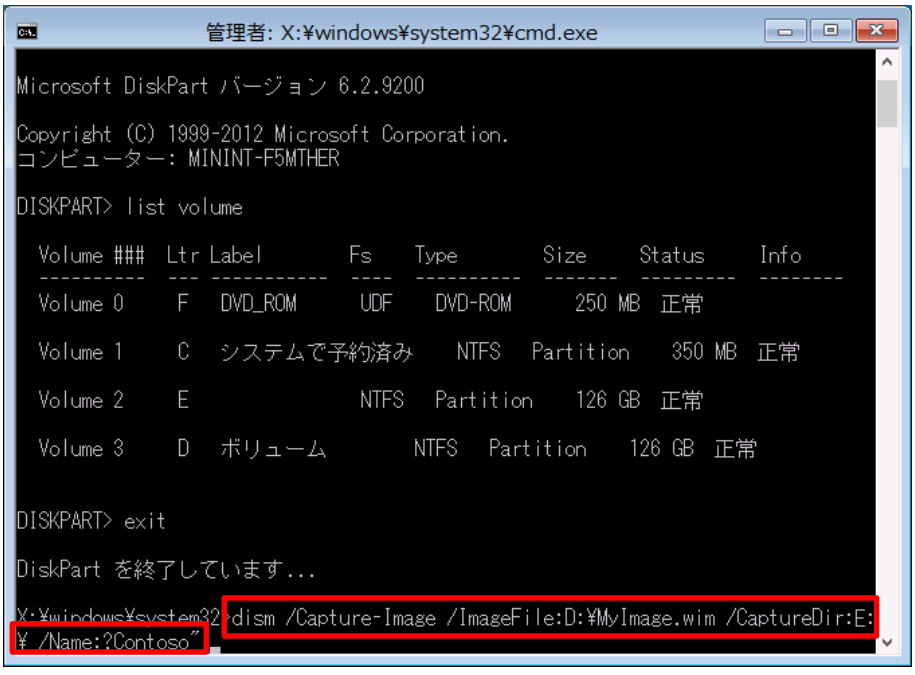
4) コマンドプロンプト画面で、「disk volume」と入力し、OS がインストールされているドライブと OS イメージを保存するドライブを確認します。(本手順では、E ドライブを OS がインストールされているドライブ、D ドライブを OS イメージを保存するドライブとします。)



5) コマンドプロンプト画面で、「exit」と入力し、Enter キーを押します。



6) コマンドプロンプト画面で、「dism /Capture-Image /ImageFile:D:¥MyImage.wim /CaptureDir:E:¥ /Name:"Contoso"」と入力し、Enter キーを押します。



7) イメージ作成が完了したら、コンピューターをシャットダウンします。
ここまでの手順により、MyImage.wim という名前の OS イメージが D ドライブに保存されました。

5 シナリオの概要

Windows Embedded 8.1 Industry Enterprise は組み込みの端末として利用することを想定した Windows 8.1 ベースの OS です。そのため、従来の組み込み端末で活用されているような次の用途をシナリオとして用意し、それぞれのシナリオにおける具体的な設定方法を紹介します。

■シンクライアント
シンクライアントとして従来の PC を活用する場合、リモート デスクトップ (mstsc.exe) だけの利用を許可し、ローカルでは他のプログラムを起動できないような制限が求められます。また、リモート接続先のデスクトップで作成したファイルをシンクライアントのローカルに保存するようなことがあると、情報漏えいの温床となります。そこで、ローカルのディスクに対する書き込みを禁止するような設定も同時に求められます。
以上のことを踏まえると、シンクライアントとして Windows Embedded 8.1 Industry Enterprise を利用するには次の設定が必要になります。

・RDP ファイルの作成
リモート デスクトップの接続方法は、シンクライアント環境に適合するようにカスタマイズすることが可能です。たとえば、ローカルとリモート接続先のデスクトップ環境間でのクリップボードの共有やローカル ディスクの共有などの機能に対して制限を行うことが可能です。これらの機能の利用を制限した リモート デスクトップ プログラム ファイル (RDP ファイル) をあらかじめ作成し、ユーザーの操作を制限します。

・Shell Launcher
RDP ファイルの作成が完了したら、Windows Embedded 8.1 Industry Enterprise の Shell Launcher を使用して、ユーザーがマシンにサインインした際は、シンクライアント向けに機能制限した RDP ファイルのみにアクセスできるように構成します。これにより、ローカルでの他のプログラムの実行を制限します。

・キーボード フィルター
ユーザーに使用されたくないキー操作（ショートカットキーなど）を無効します。具体的には Ctrl + Shift + Esc ショートカットキーや Ctrl + Alt + Del ショートカットキー操作によるタスク マネージャー プログラムの起動などを制限します。

・書き込みフィルター
シンクライアントとして利用するローカル端末にファイルを保存させないようにするため、書き込みフィルターを有効にします。書き込みフィルターによって、ローカルのすべてのドライブへの書き込みを制限します。

■読み取り専用リッチクライアント
読み取り専用リッチクライアントとして利用する PC の場合、通常の PC に近い操作性と機能性を提供する必要がありますが、一方で堅牢な情報保護が求められます。そのため、読み取り専用リッチクライアントとして Windows Embedded 8.1 Industry Enterprise を活用する場合、業務で扱うデータを読み取り専用にし、任意の場所にデータを保存させず、そしてデータを持ち出せないような制限が求められます。
以上のことを踏まえると、読み取り専用リッチクライアントとして Windows Embedded 8.1 Industry Enterprise を利用するには次の設定が必要になります。

・USB フィルター
USB 接続のデバイスに対するアクセスを制限することで、USB メモリや USB ハードディスクなどの外部メディアへの書き込みを制限します。

・書き込みフィルター
読み取り専用リッチクライアントとして利用するローカル端末にファイルを保存させないようにするため、書き込みフィルターを有効にします。書き込みフィルターによって、ローカルのすべてのドライブへの書き込みを制限します。

■業務アプリ専用端末への転用
業務アプリ専用端末や受付端末 / 電子広告端末として利用する PC の場合、サインインユーザーを切り替えることによって、すぐに業務アプリ専用端末と通常の機能制限のない PC 環境に切り替えられるような操作性を提供する必要があります。そのため、業務アプリ専用端末として利用しているときには業務アプリだけが実行できるように制限を行います。
以上のことを踏まえると、業務アプリ専用端末として Windows Embedded 8.1 Industry Enterprise を利用するには次の設定が必要になります。

・Application Launcher
Windows ストア アプリ形式の業務アプリを提供する場合は、他のストア アプリの利用を制限するために Application Launcher を構成します。(もし、業務アプリがデスクトップ アプリケーションとして開発されたものであれば、代わりに Shell Launcher を利用します)

・ジェスチャー フィルター
Windows 8.1 のタッチパネル操作を使用すると、チャーム機能などを利用して業務アプリ以外のプログラムを実行できます。そのため、業務アプリだけが実行されるようにするために、ジェスチャー フィルターを有効にしてタッチパネル特有の操作を制限します。

・ダイアログ フィルター
業務アプリの起動中に意図しないダイアログやウィンドウの表示は見栄えが悪いだけでなく、操作上のトラブルに発展する可能性があります。そのため、ダイアログフィルターを利用してダイアログとウィンドウの表示を制限します。[A1]

それぞれのシナリオにおけるロックダウン設定について、第 6 章から第 8 章で具体的な手順と共に説明します。
なお、第 6 章からの手順はワークグループの環境で利用することを前提としています。そのため、別のユーザーに切り替えたときの操作を確認できるよう、事前にローカルにユーザーとグループを作成しておきます。具体的な手順は 5.1 節を確認してください。

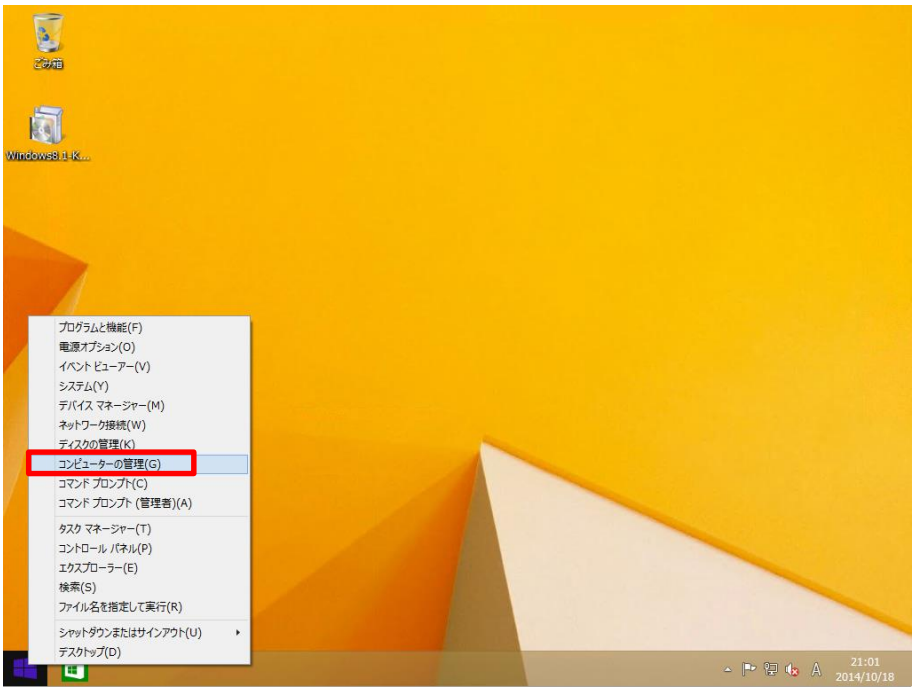
5.1 シナリオ検証用ユーザーとグループの作成

以降の手順で設定するシナリオの内容を検証するために使用する、ワークグループのユーザー (user1) とグループ (RestrictedGroup) をそれぞれ作成します。

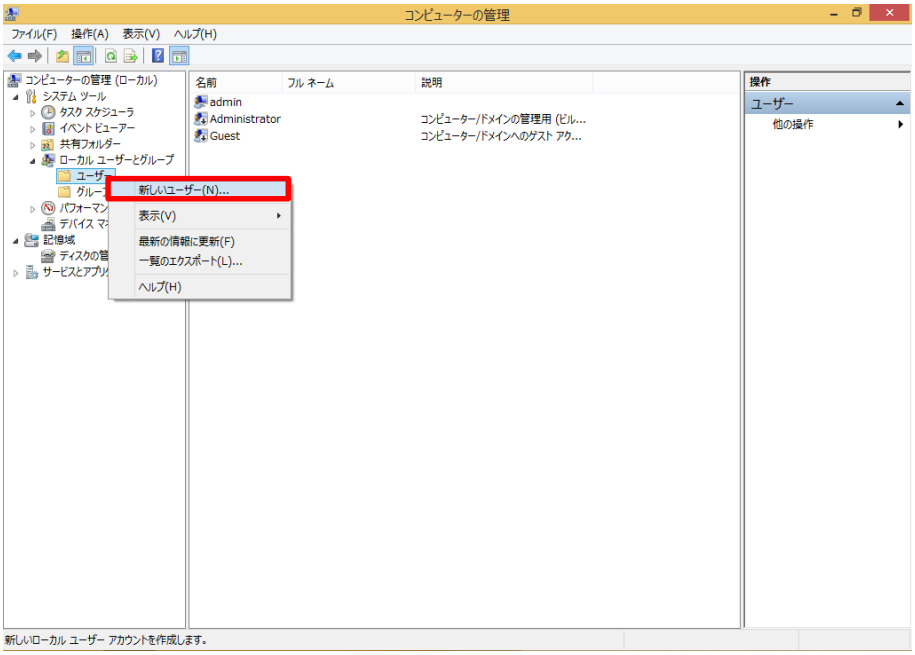
【Note:】
同様の作業をドメインの環境で行う場合、Active Directory ドメインに評価用のユーザー (ユーザー名：User1) とグループ (グループ名：RestrictedGroup) を事前に作成してください。

1) WE81IE01 に、 Admin でサインインします。

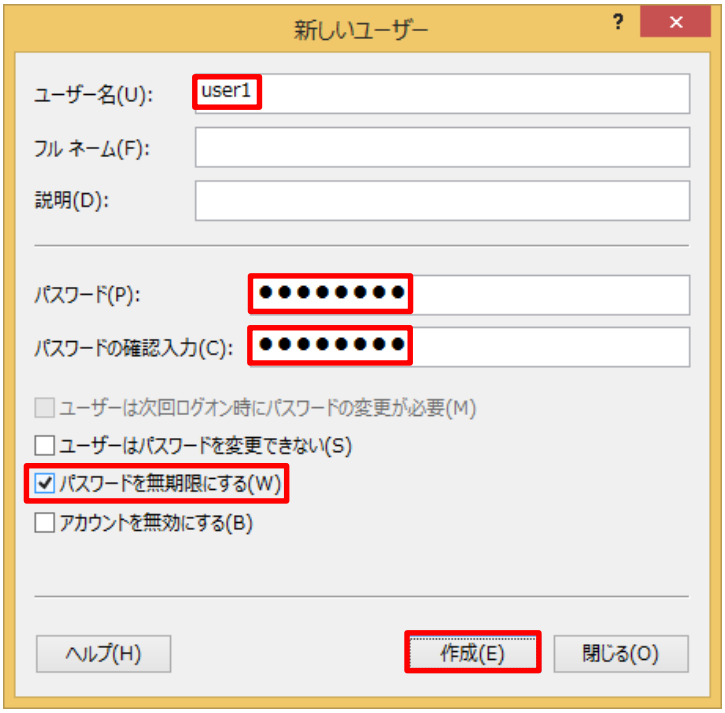
2) スタートボタンを右クリックし、[コンピューターの管理] をクリックします。



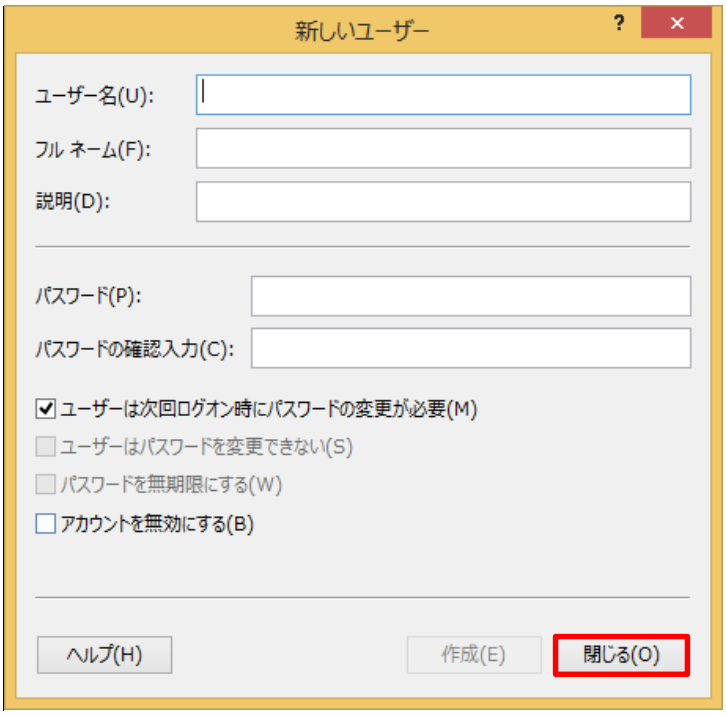
3) [コンピューターの管理] 画面で、[コンピューターの管理] - [システムツール] - [ローカル ユーザーとグループ] - [ユーザー] の順に展開し、[ユーザー] を右クリックして、[新しいユーザー] をクリックします。



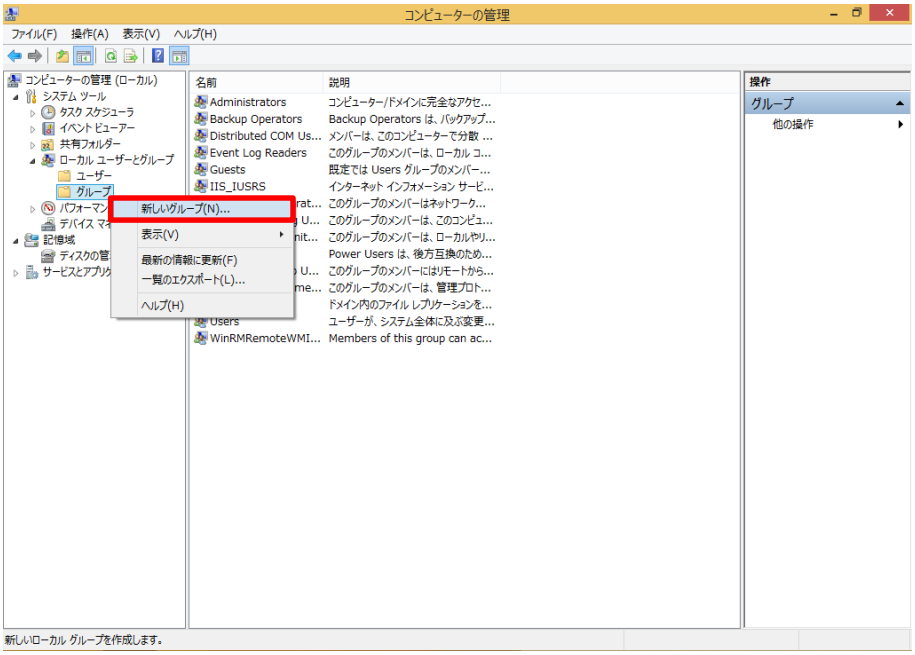
4) [新しいユーザー] 画面で、[ユーザー] 欄に「user1」、[パスワード] と [パスワードの確認入力] 欄に「P@ssw0rd」と入力します。さらに、[ユーザーは次回ログオン時にパスワードの変更が必要] のチェックを外し、[パスワードを無期限にする] のチェックをつけて [作成] をクリックします。



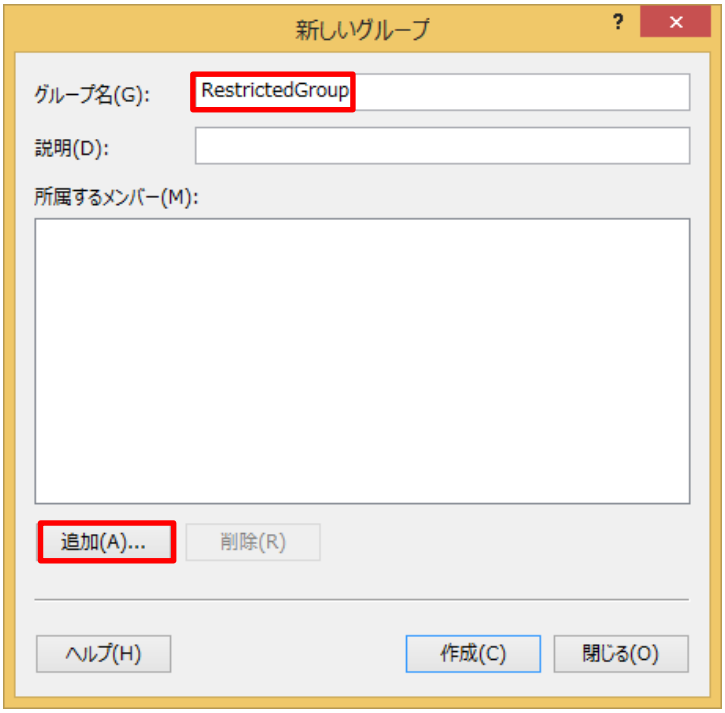
5) [新しいユーザー] 画面で [閉じる] をクリックします。



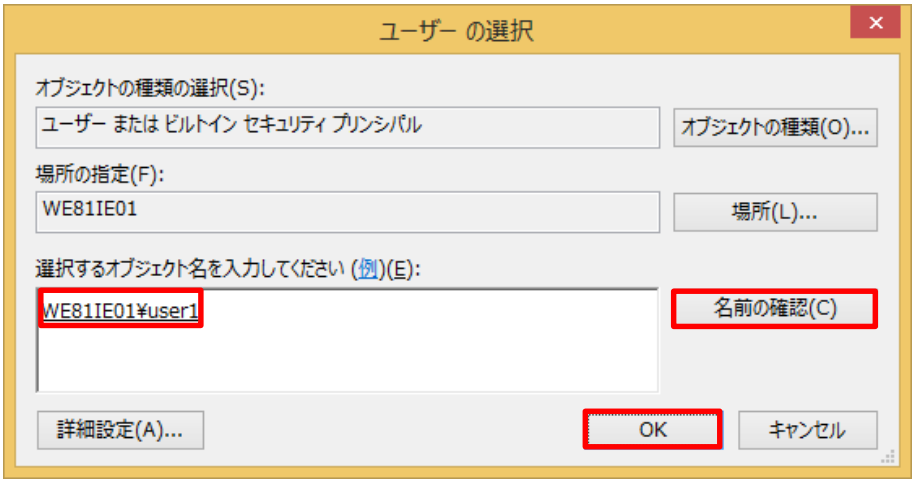
6) [コンピューターの管理] 画面で、[グループ] を右クリックし、[新しいグループ] をクリックします。



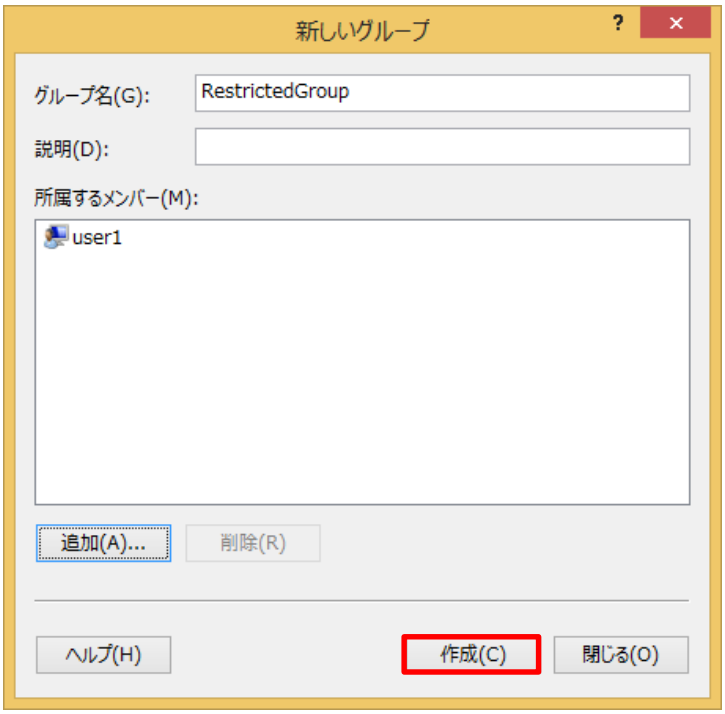
7) [新しいグループ] 画面で、[グループ名] 欄に「RestrictedGroup」と入力し、[追加] をクリックします。



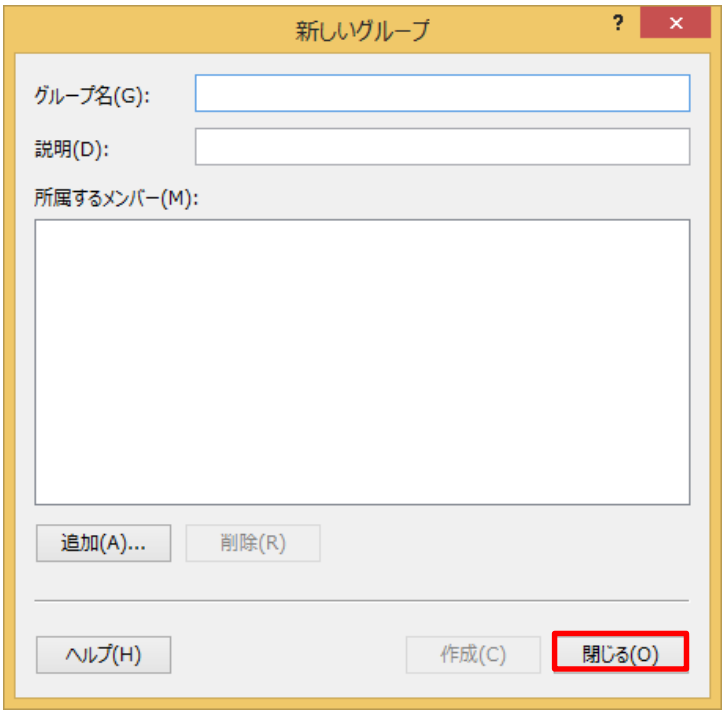
8) [ユーザーの選択] 画面で、[選択するオブジェクト名を入力してください] 欄に「user1」と入力し、[名前の確認] をクリックして、[OK] をクリックします。



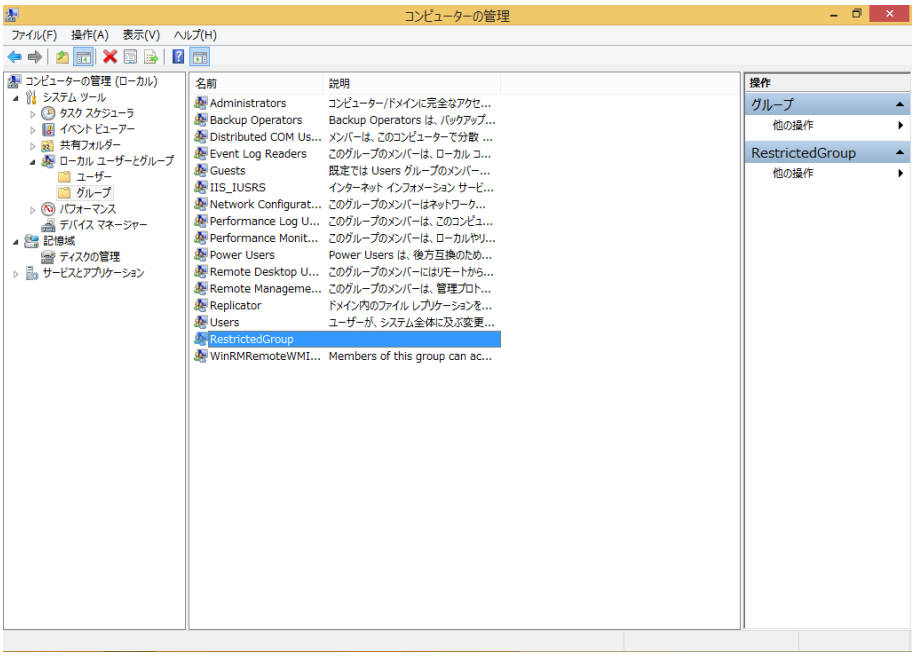
9) [新しいグループ] 画面で、[作成] をクリックします。



10) [新しいグループ] 画面で、[閉じる] をクリックします。



11) [コンピューターの管理] 画面を閉じます。



6 シンクライアントとしての利用

本章では、シンクライアントとして Windows Embedded 8.1 Industry Enterprise を利用するために必要な設定について手順を解説します。第 5 章でも解説したように、シンクライアントとして利用するために、シンクライアント利用を想定した機能制限付きの RDP ファイルの作成と、Embedded Lockdown Manager を利用して Shell Launcher、キーボード フィルター、書き込みフィルターをそれぞれ設定します。

6.1 RDP ファイルの作成

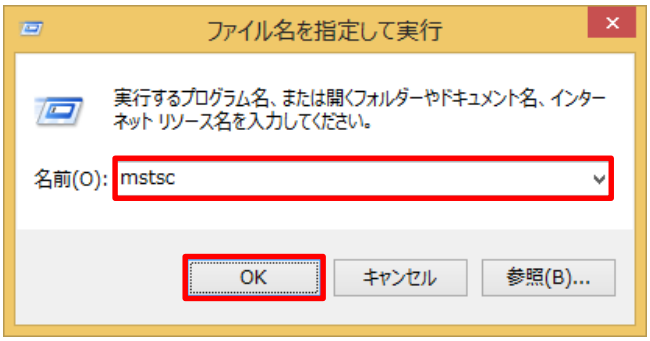
Windows Embedded 8.1 Industry Enterprise をシンクライアントとして利用する際にリモート接続先となるコンピューターを設定した RDP ファイルを作成します。実際に RDP ファイルを実行して接続確認を行えるように、本手順では WE81IE02 コンピューターをリモート接続先として指定します。

1) WE81IE01 に、Admin ユーザーでサインインします。

※ 端末にロックダウン設定が施されている場合は、すべての設定を解除してください。

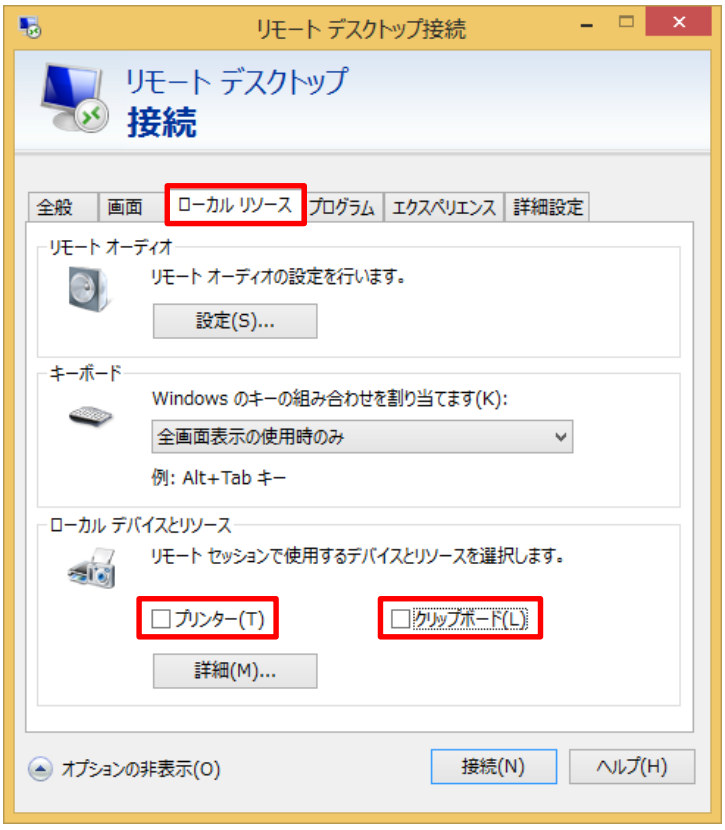
2) スタートボタンを右クリックし、[ファイル名を指定して実行] をクリックします。

3) [ファイル名を指定して実行] 画面で、「mstsc」と入力し、[OK] をクリックします。

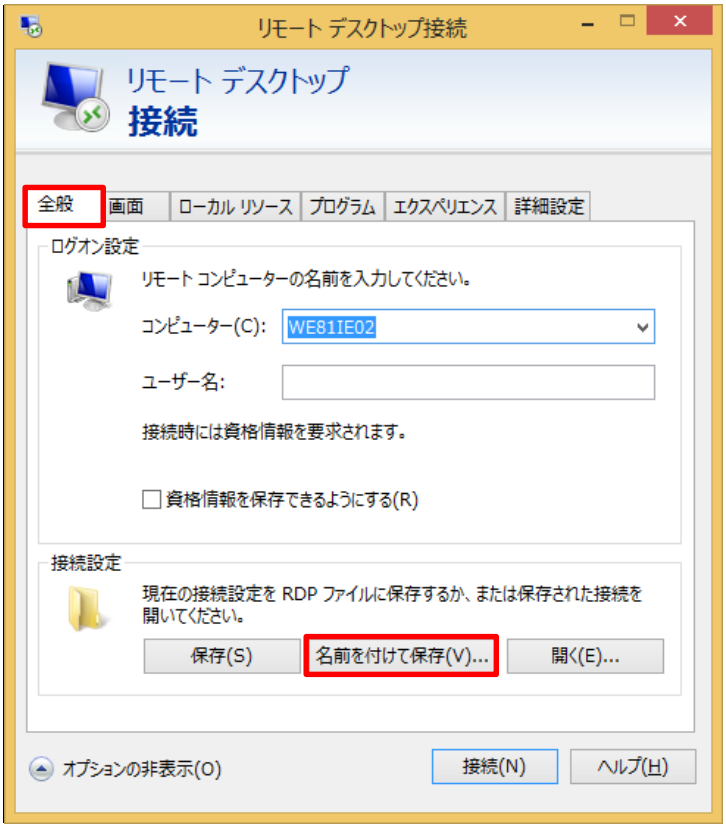


4) [リモート デスクトップ接続] 画面で、[コンピューター] に接続先となるコンピューター名として、「WE81IE02」と入力し、[オプションの表示] をクリックします。

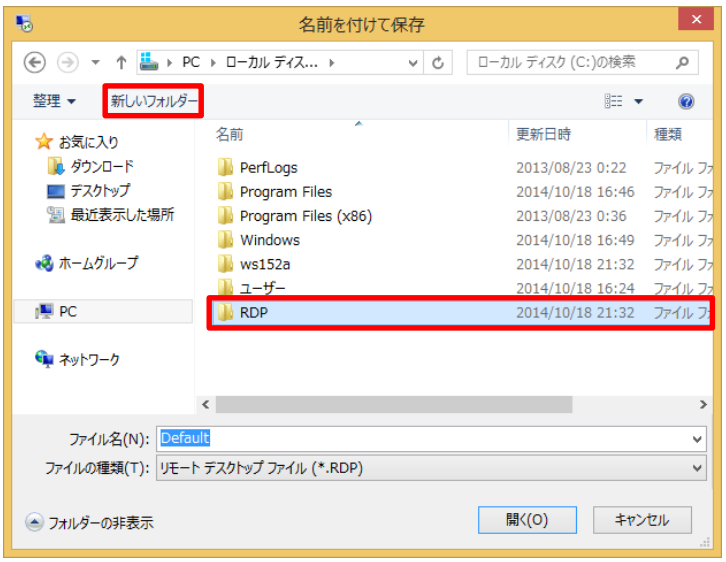
5) [リモート デスクトップ] 画面で、[ローカル リソース] タブをクリックし、[プリンター] および [クリップボード] のチェックを外します。



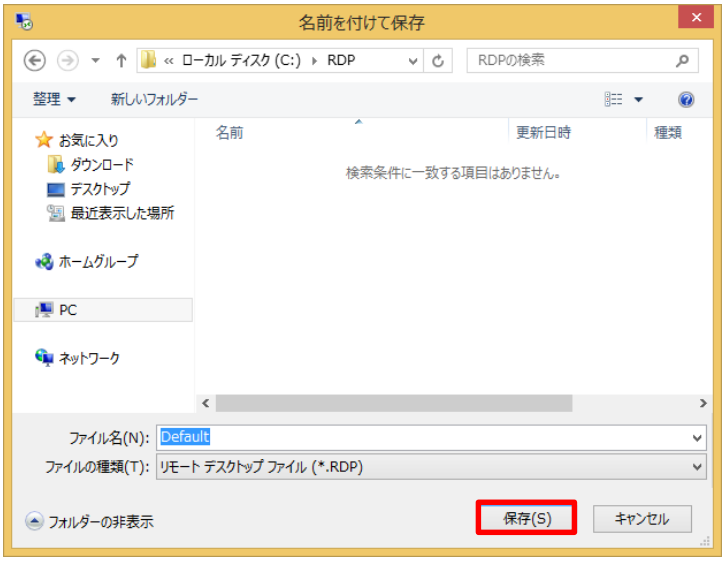
6) [リモート デスクトップ] 画面で、[全般] タブをクリックし、[名前を付けて保存] をクリックします。



7) [名前を付けて保存] 画面で、C ドライブ直下 (C:¥) を開きます。[新しいフォルダー] から「RDP」というフォルダーを新規作成します。作成した [RDP] フォルダーをダブルクリックします。



8) [名前を付けて保存] 画面で、ファイル名が [Default] であることを確認し、[保存] をクリックします。

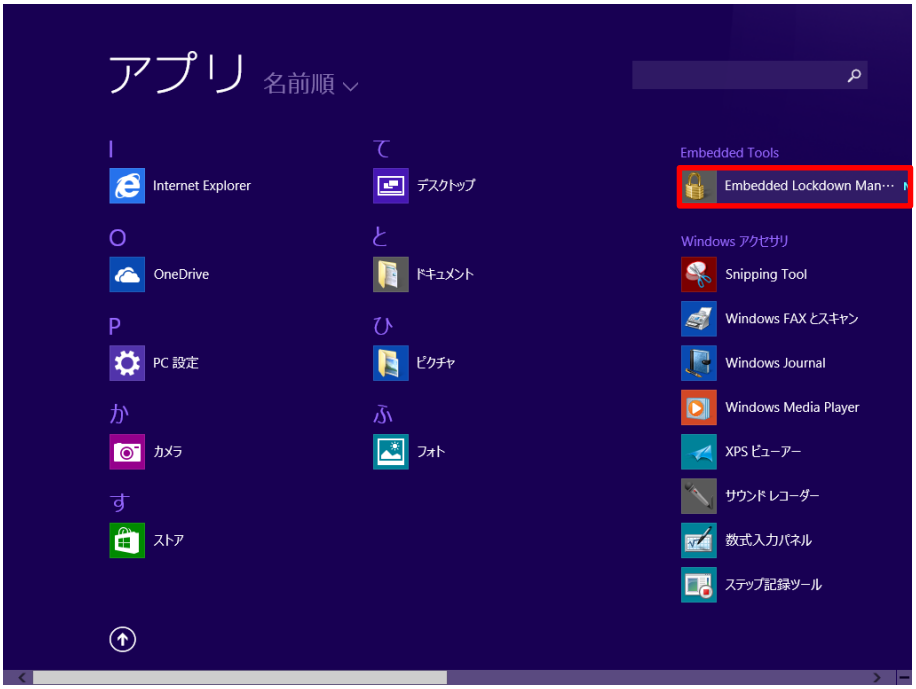


6.2 Shell Launcher による RDP の有効化

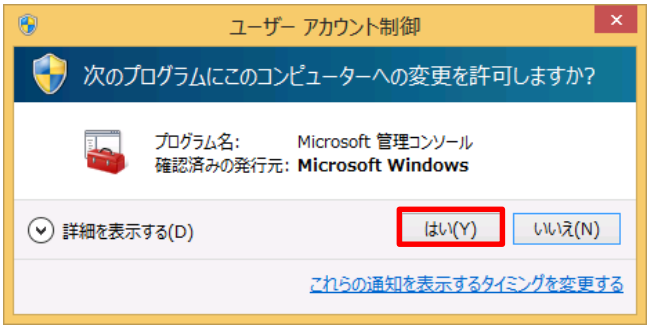
Embedded Lockdown Manager の Shell Launcher 設定を利用して、前の手順で作成した Default.rdp ファイルだけが実行されるように構成します。本手順では、RestrictedGroup グループのメンバーでサインインしたときに Default.rdp ファイルだけが実行されるように構成します。

1) スタート画面を開き、 ↓ をクリックします。

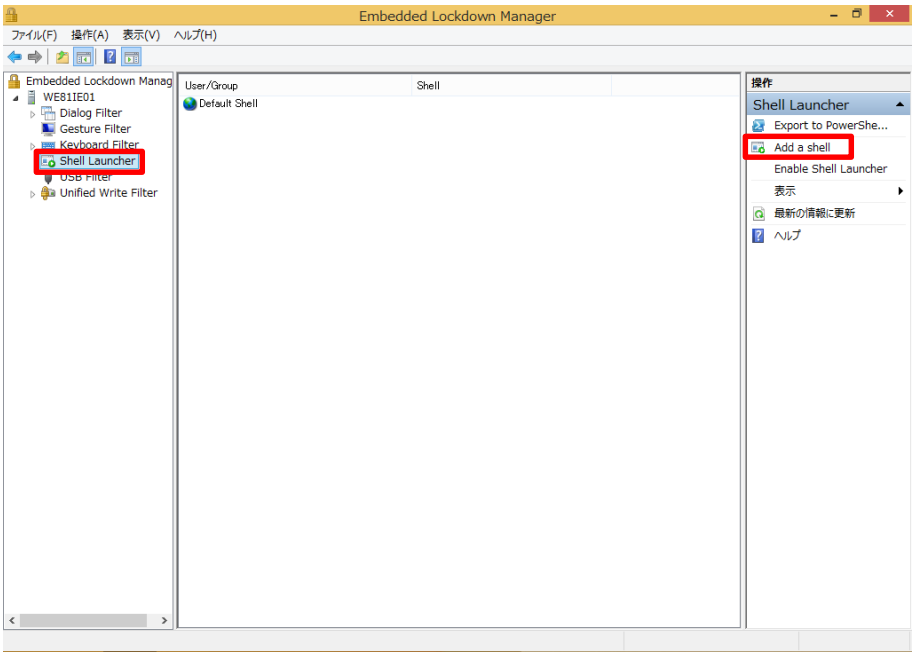
2) スタート画面で、[Embedded Lockdown Manager] をクリックします。



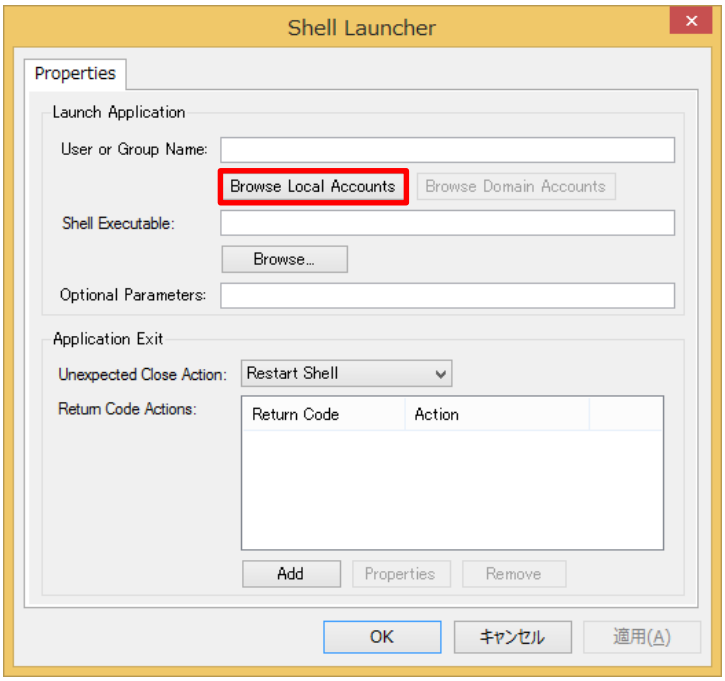
3) [ユーザー アカウント制御] 画面で、[はい] をクリックします。



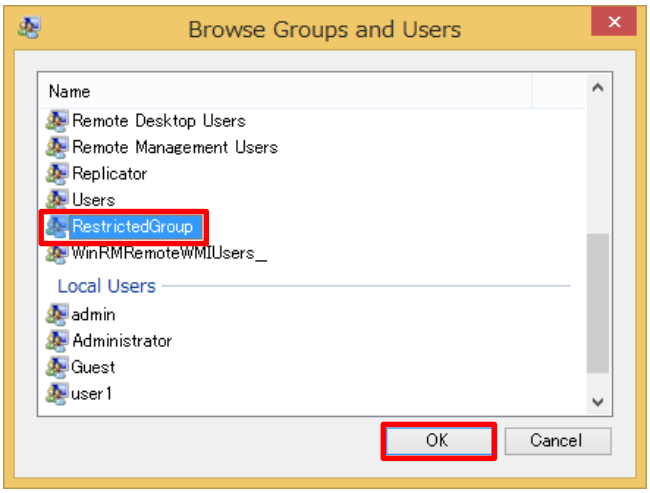
4) [Embedded Lockdown Maneger] 画面で、左ペインの [Shell Launcher] をクリックし、右ペインの [Add a shell] をクリックします



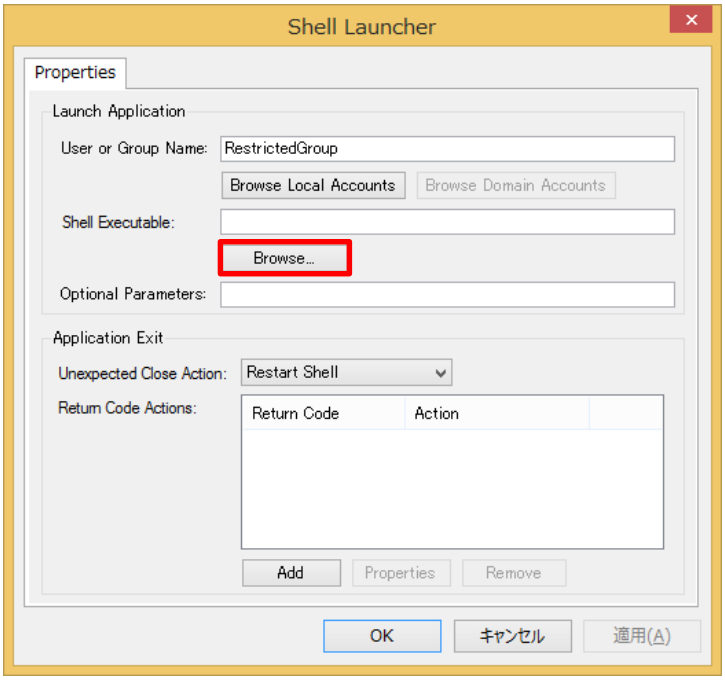
5) [Shell Launcher] 画面で、[User or Group Name] の [Browse Local Accounts] をクリックします。



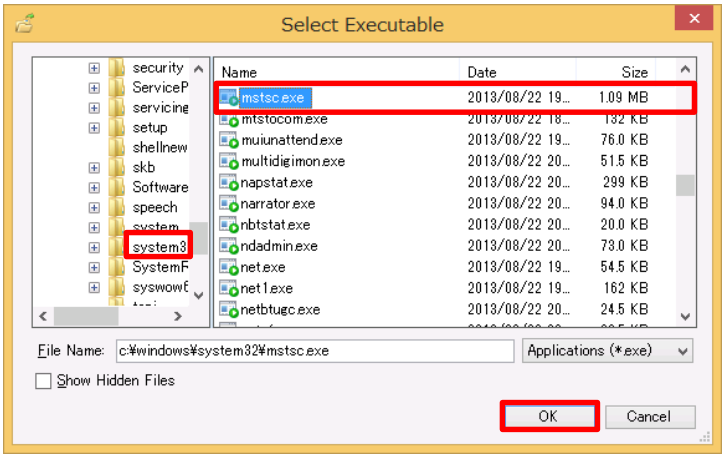
6) [Browse Groups and Users] 画面で、[RestrictedGroup] を選択し、[OK] をクリックします。



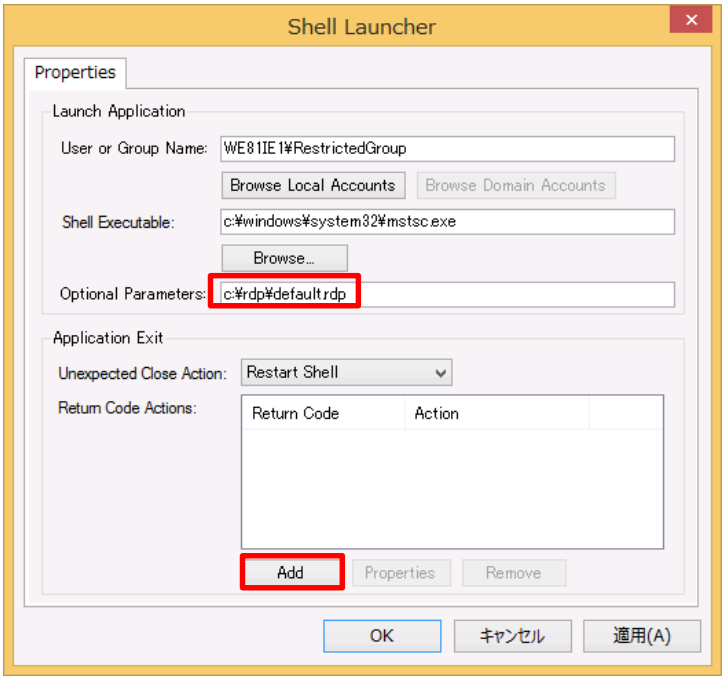
7) [Shell Launcher] 画面で、[Shell Executable] の [Browse...] をクリックします。



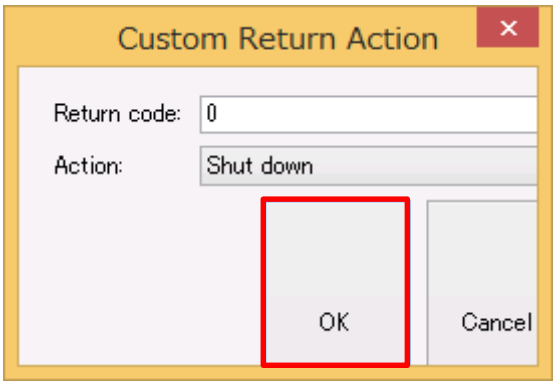
8) [Select Executable] 画面で、左ペインから c:¥windows¥system32 フォルダーをクリックし、右ペインから [mstsc.exe] をクリックし、[OK] をクリックします。



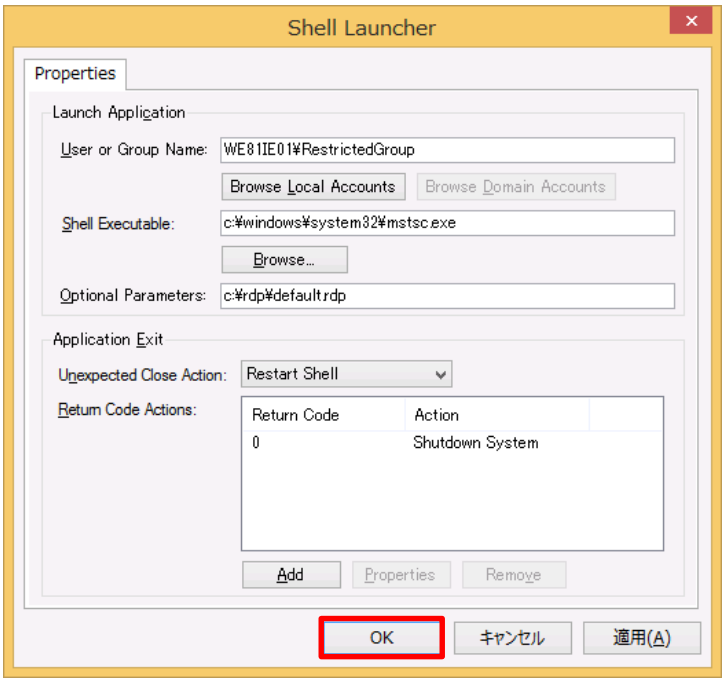
9) [Shell Launcher] 画面で、[Optional Parameters] 欄に「c:¥rdp¥default.rdp」と入力し、[Add] をクリックします。



10) [Custom Return Action] 画面で、[Action] 欄から [Shutdown] を選択し、[OK]をクリックします。



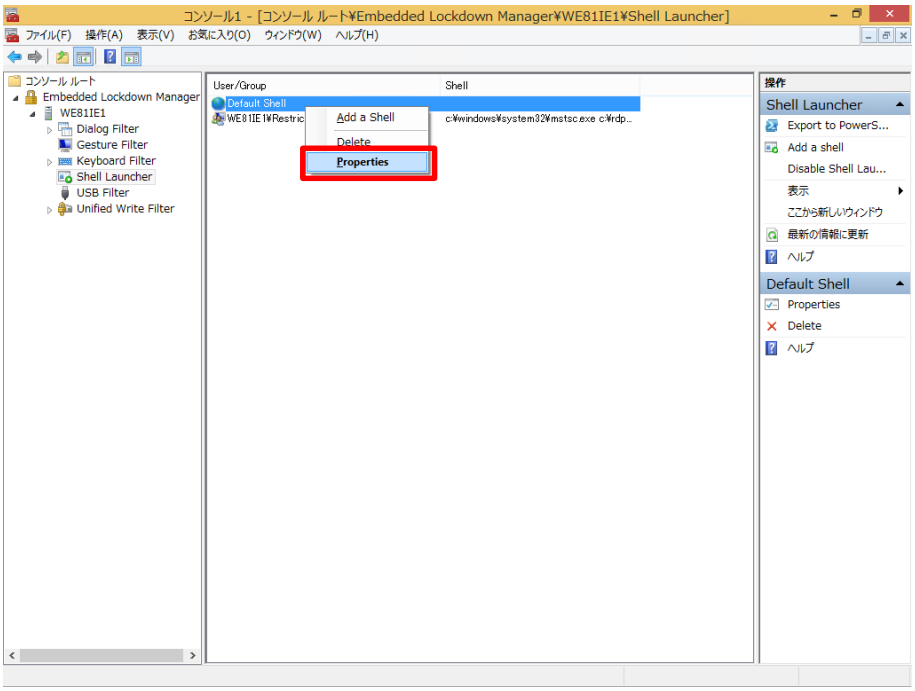
11) [Shell Launcher] 画面で、[OK] をクリックします。



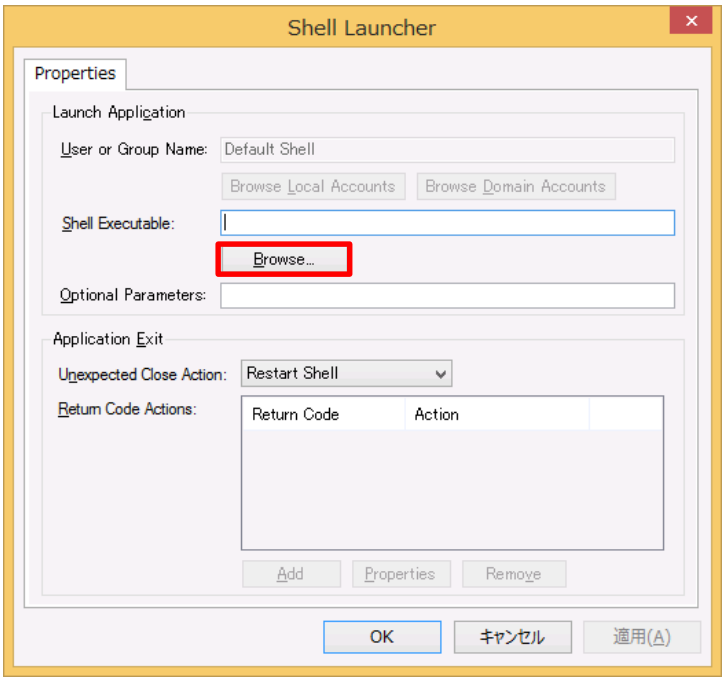
【Note:】

[Application Exit] 欄で設定する内容は Shell Launcher で実行したアプリケーションが終了したときの動作について定義します。本手順では [Restart Shell] を指定しているため、アプリケーションが終了すると、アプリケーションが改めて起動します。

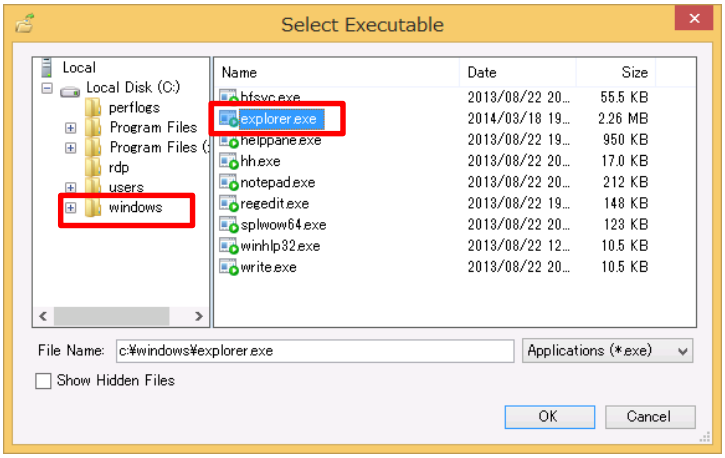
12) [Embedded Lockdown Maneger] 画面で、中央ペインの [Default Shell] を右クリックし、[Properties] をクリックします。



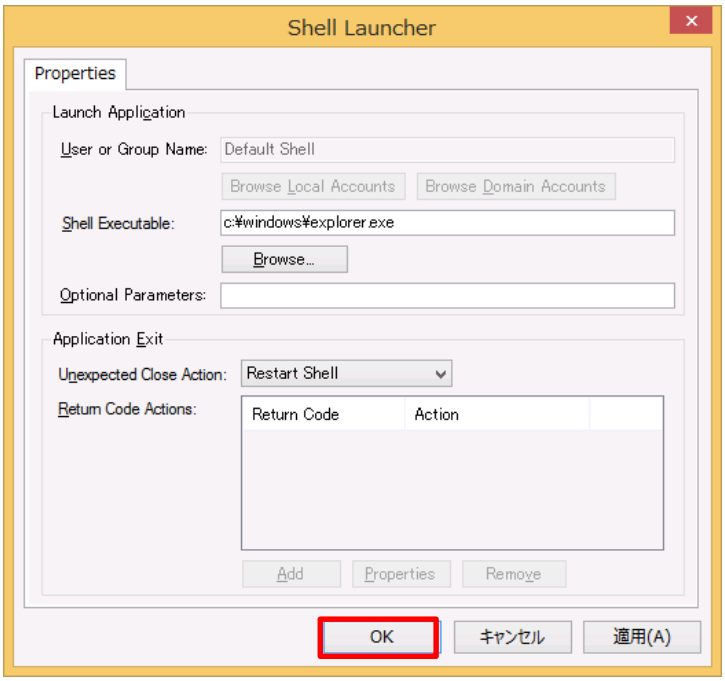
13) [Shell Launcher] 画面で、[Browse] をクリックします。



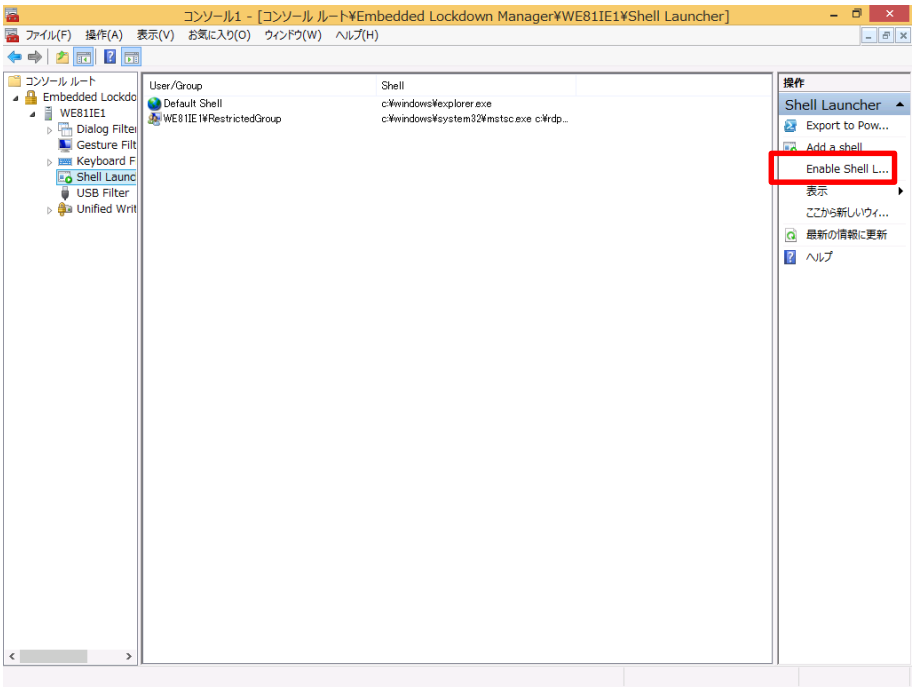
14) [Select Executable] 画面で、左ペインから c:¥windows フォルダーを展開し、右ペインから [explorer.exe] をクリックし、[OK] をクリックします。



15) [Shell Launcher] 画面で、[OK] をクリックします。



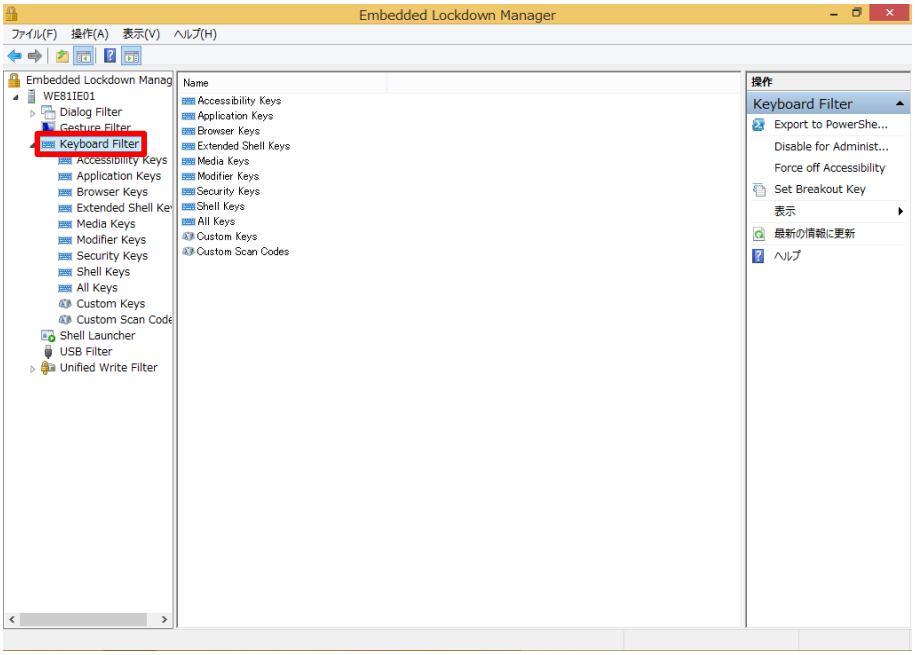
16) [Embedded Lockdown Maneger] 画面で、設定内容を有効にするため右ペインの [Enable Shell Launcher] をクリックします。



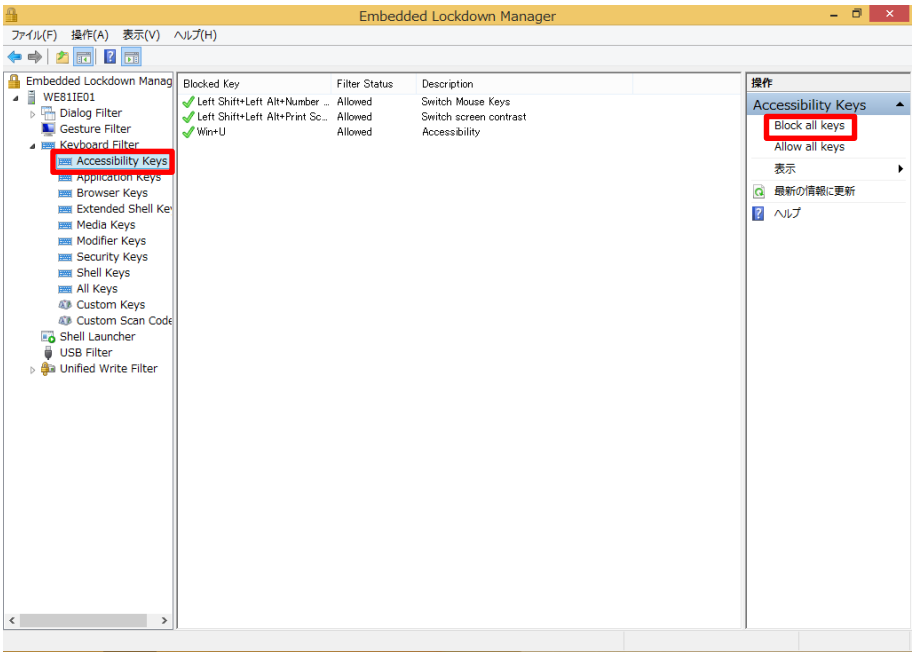
6.3 キーボード フィルターによる特定操作の制限

Embedded Lockdown Manager の キーボード フィルターを設定し、特定のキー操作ができないように構成します。本手順で制限するキー操作は、アクセシビリティ ([コントロール パネル] - [コンピューターの簡単操作センター]) 関連のキー、キーボードの特殊キーに割り当てられたメールや Windows Media Play 等アプリケーションの起動、タスク マネージャーの実行に使われる Ctrl + Shift + Esc キーおよび Ctrl + Alt + Del キーです。

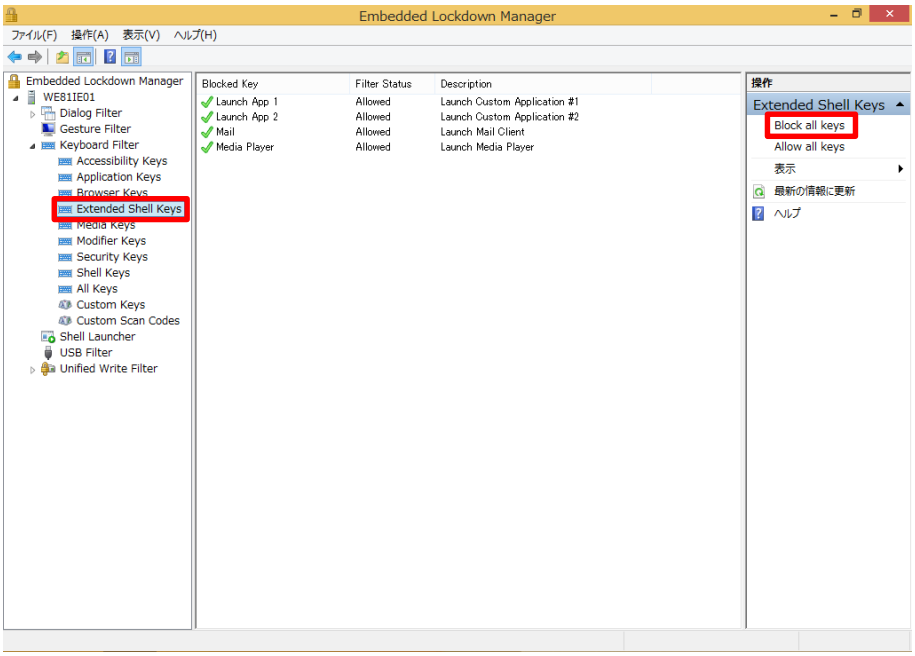
1) [Embedded Lockdown Maneger] 画面で、左ペインの [Keybord Filter] をクリックして展開します。



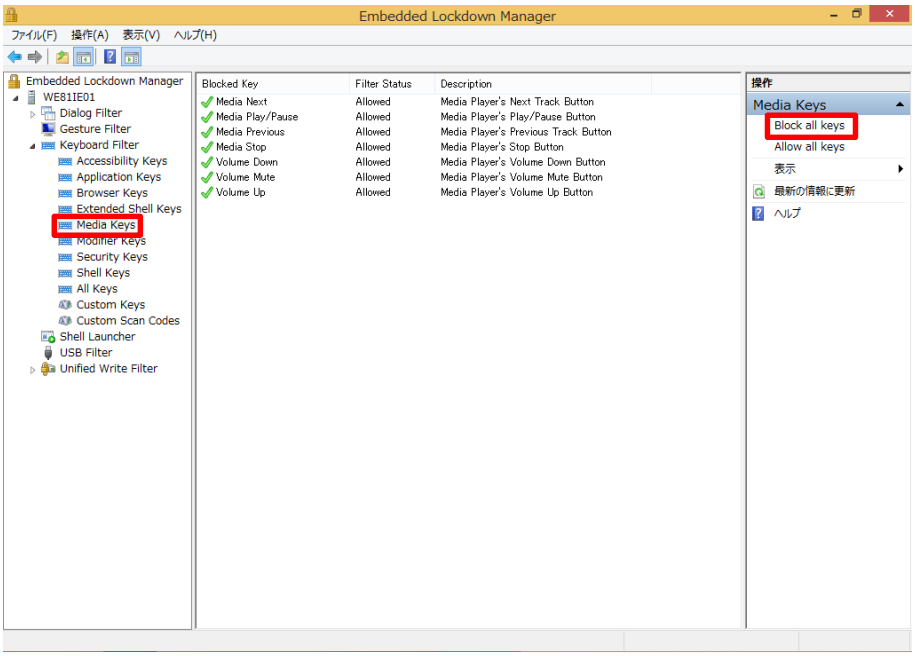
2) [Embedded Lockdown Maneger] 画面で、左ペインの [Accessibility Keys] をクリックし、右ペインの [Block all keys] をクリックします。



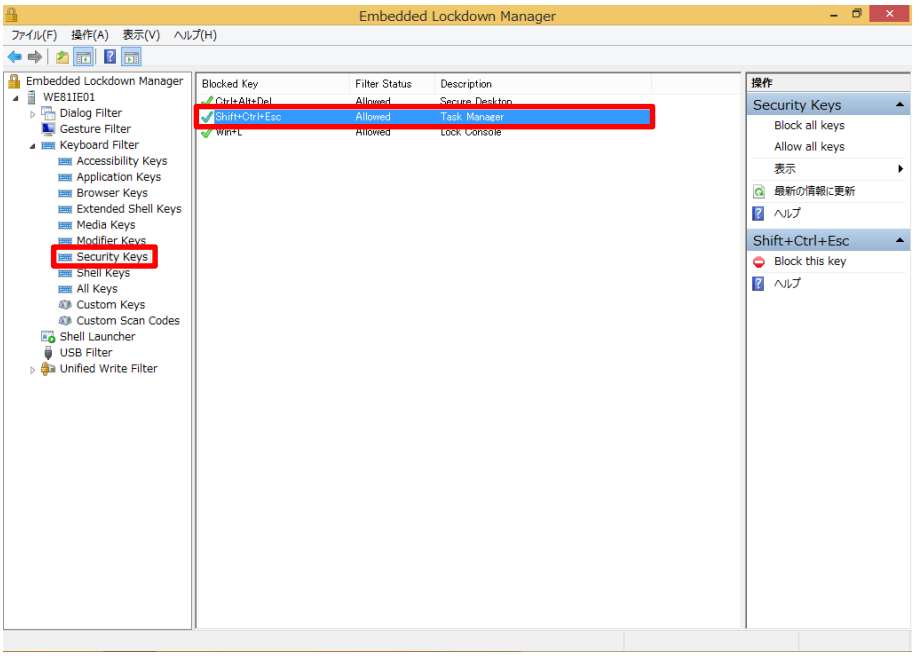
3) [Embedded Lockdown Maneger] 画面で、左ペインの [Extended Shell Keys] をクリックし、右ペインの [Block all keys] をクリックします。



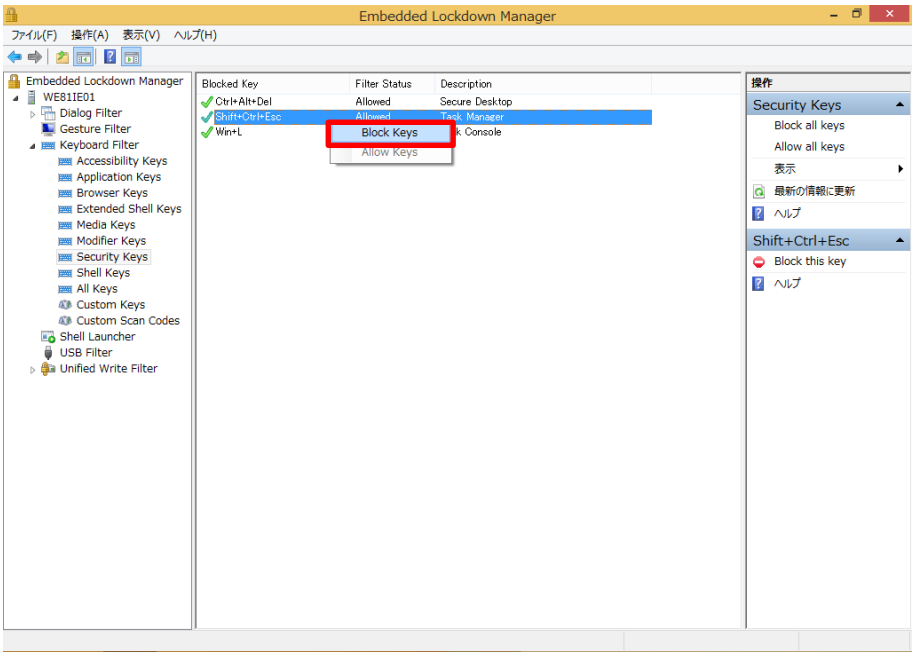
4) [Embedded Lockdown Maneger] 画面で、左ペインの [Media Keys] をクリックし、右ペインの [Block all keys] をクリックします。



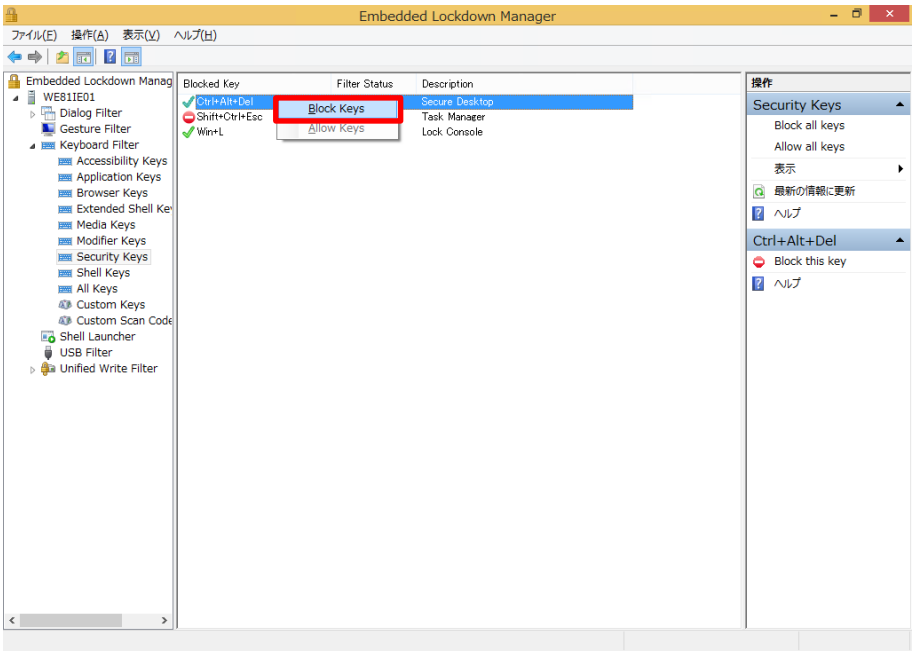
5) [Embedded Lockdown Maneger] 画面で、左ペインの [Security Keys] をクリックし、中央ペインの [Task Maneger] を選択します。



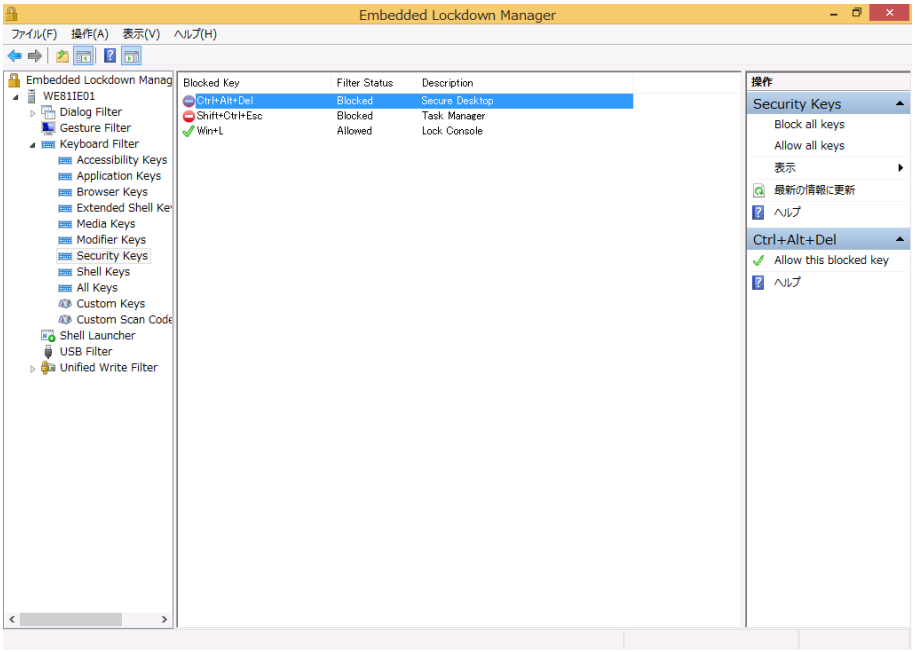
6) [Embedded Lockdown Maneger] 画面で、中央ペインの [Task Maneger] を右クリックし、[Block keys] をクリックします。



7) [Embedded Lockdown Maneger] 画面で、中央ペインの [Secure Desktop] を右クリックし、[Block keys] をクリックします。



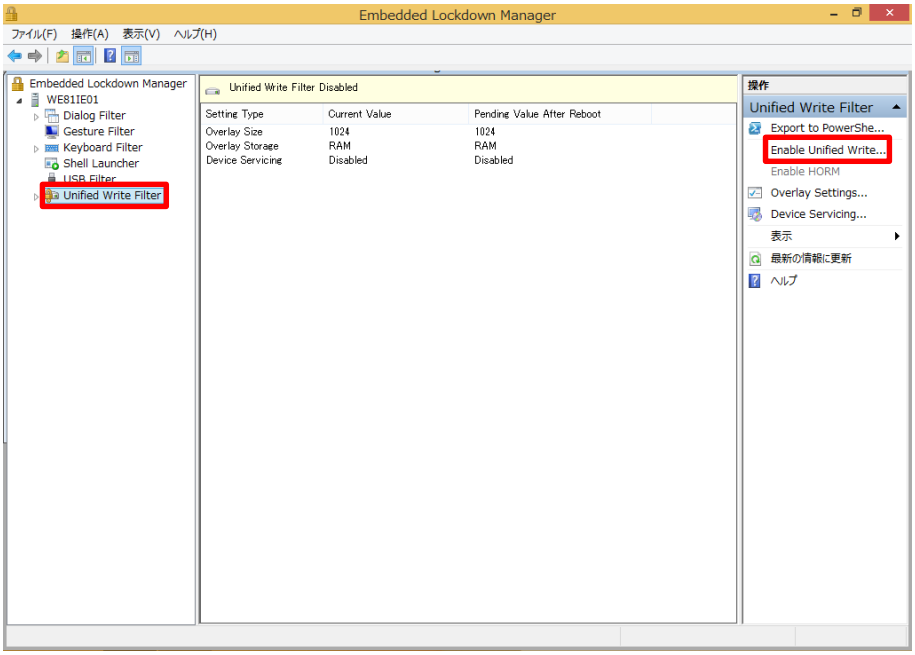
8) [Embedded Lockdown Maneger] 画面で、中央ペインの [Task Maneger] と [Secure Desktop] がそれぞれブロック設定になっていることを確認します。



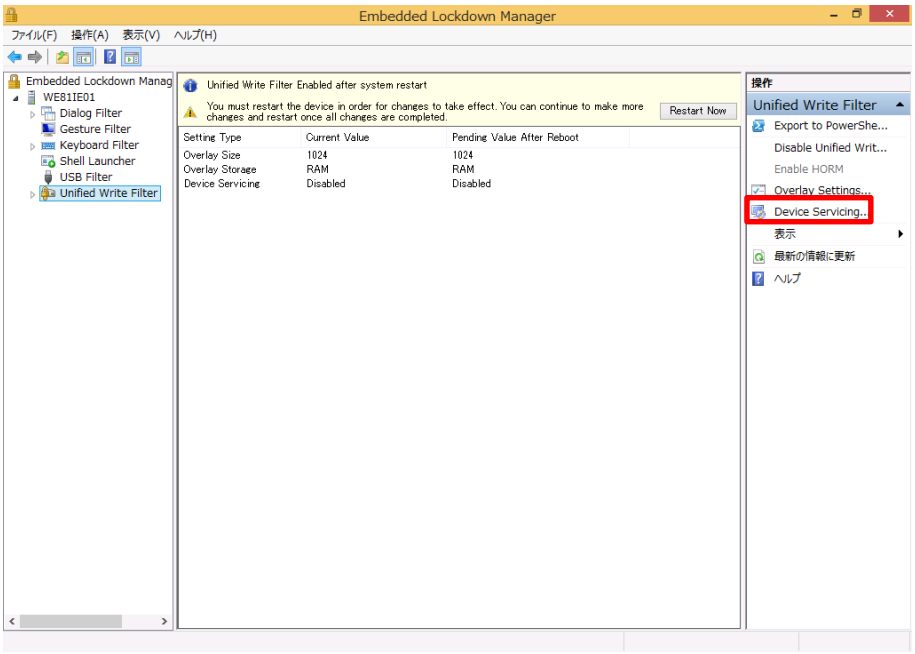
6.4 書き込みフィルターによる書き込み制限設定

Embedded Lockdown Manager の 書き込みフィルターを設定し、ハードディスクにファイルを永続的に保存できないように構成します。また、書き込みフィルターの例外設定として、Windows Update による更新プログラムのインストール内容が書き込まれるように構成します。

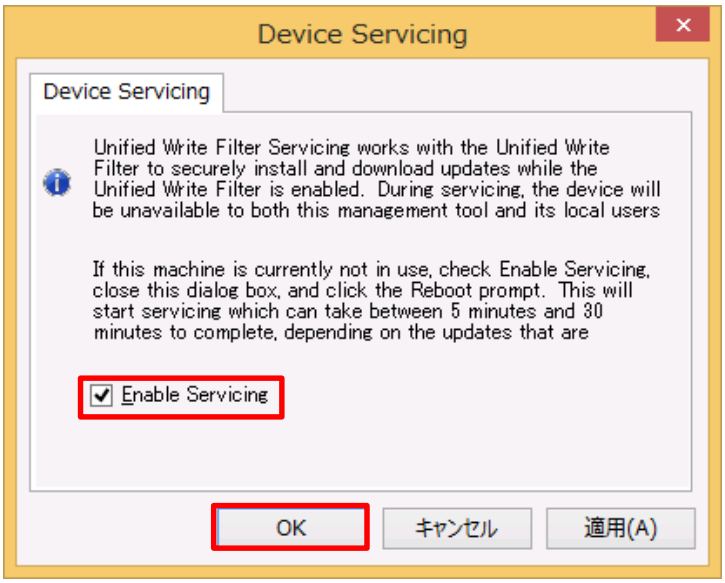
1) [Embedded Lockdown Maneger] 画面で、左ペインの [Unified Write Filter] をクリックし、右ペインの [Enable Unifide Write Filter] をクリックします。



2) [Embedded Lockdown Maneger] 画面で、右ペインの [Device Servicing] をクリックします。



3) [Device Servicing] 画面で、[Enable Servicing] にチェックをつけ、[OK] をクリックします。



【Note:】
Device Servicing を有効にすることで、書き込みフィルターが適用された状況での Windows Update 等の更新プログラムの適用が可能になります。

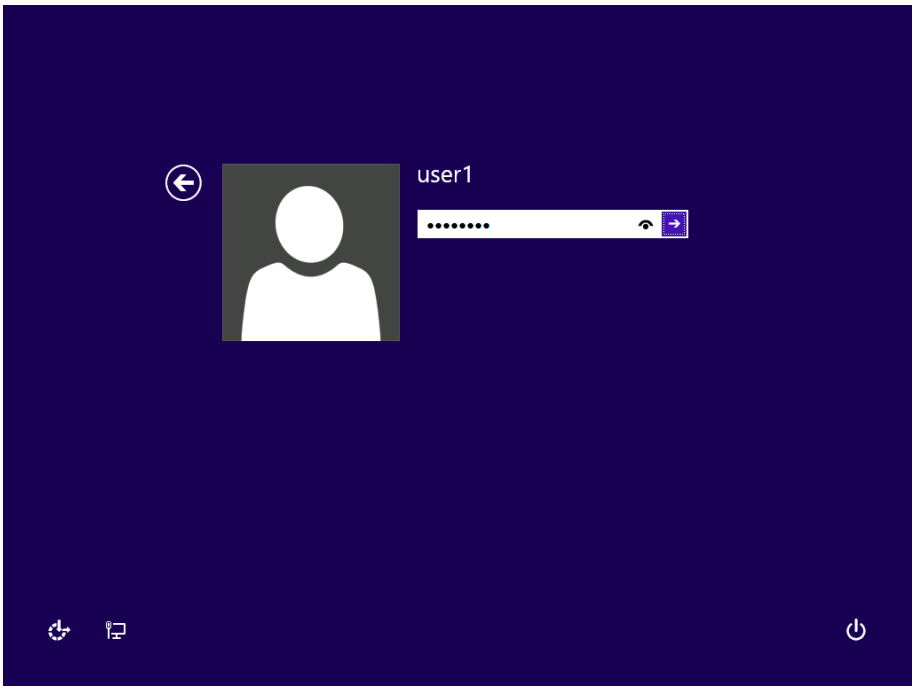
【Note:】[A2]
Windows Update 以外にも、ファイル、フォルダーおよびレジストリの例外設定により、System Center Endopoint Protection 定義ファイルの適用や、Windows Defender 定義ファイルが適用されるよう構成できます。設定に関する詳細は下記サイトを参考にしてください。

■ Antimalware support on UWF-protected devices
http://msdn.microsoft.com/en-us/library/dn449271(v=winembedded.82).aspx

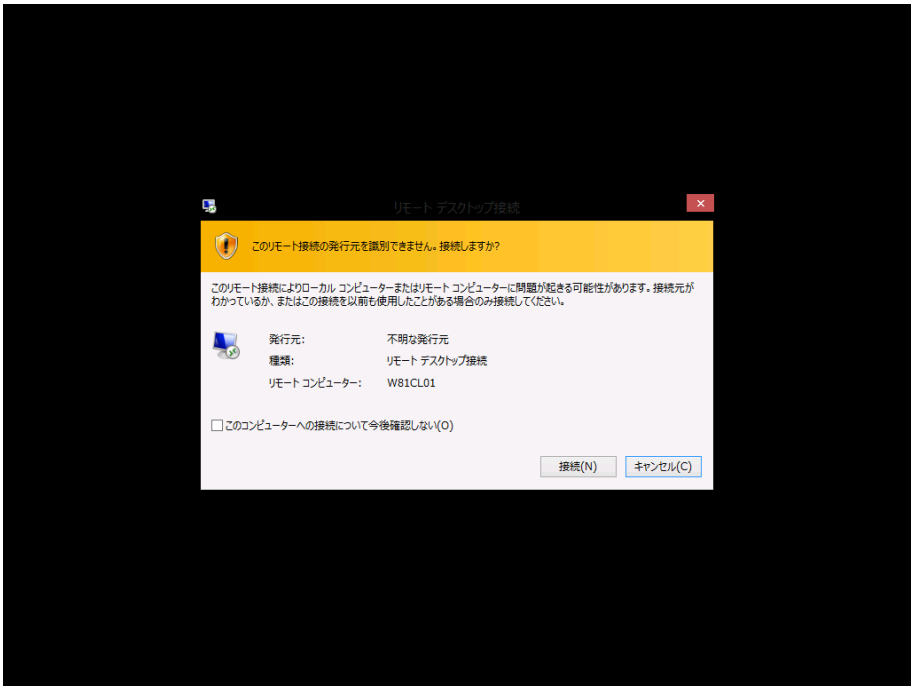
6.5 設定の確認

6.1 ～ 6.4 節で設定した内容を確認します。

1) WE81IE01 に、User1 としてサインインします。



2) [リモート デスクトップ接続] 画面が表示され、その他のプログラムが一切起動できないことが確認できます。また、リモート デスクトップ接続を終了すると、コンピューターがシャットダウンすることも確認できます。[A3][A4]



3) [リモート デスクトップ接続] 画面を終了し、シャットダウンします。

7 読み取り専用リッチクライアントとしての利用

本章では、読み取り専用リッチクライアントとして Windows Embedded 8.1 Industry Enterprise を利用するために必要な設定について手順を解説します。第 5 章でも解説したように、読み取り専用リッチクライアントとして利用するために、USB フィルターと書き込みフィルターをそれぞれ設定します。尚、本章ではエンドユーザーに提供するアプリケーションなどについては既に構成済みであると仮定し、最後のロックダウン設定についてのみ解説します。

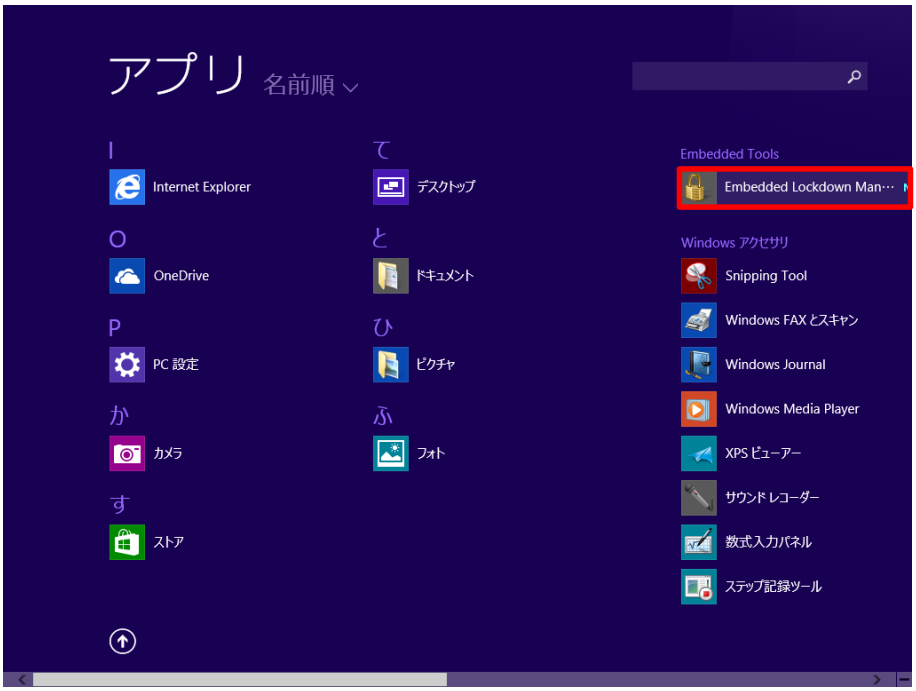
7.1 USB フィルターによるデータアクセスの制限設定

Embedded Lockdown Manager の USB フィルターを設定し、USB 接続のデバイスを利用できないように構成します。

1) WE81IE01 に、Admin ユーザーでサインインします。
   ※ 端末にロックダウン設定が施されている場合は、すべての設定を解除してください。

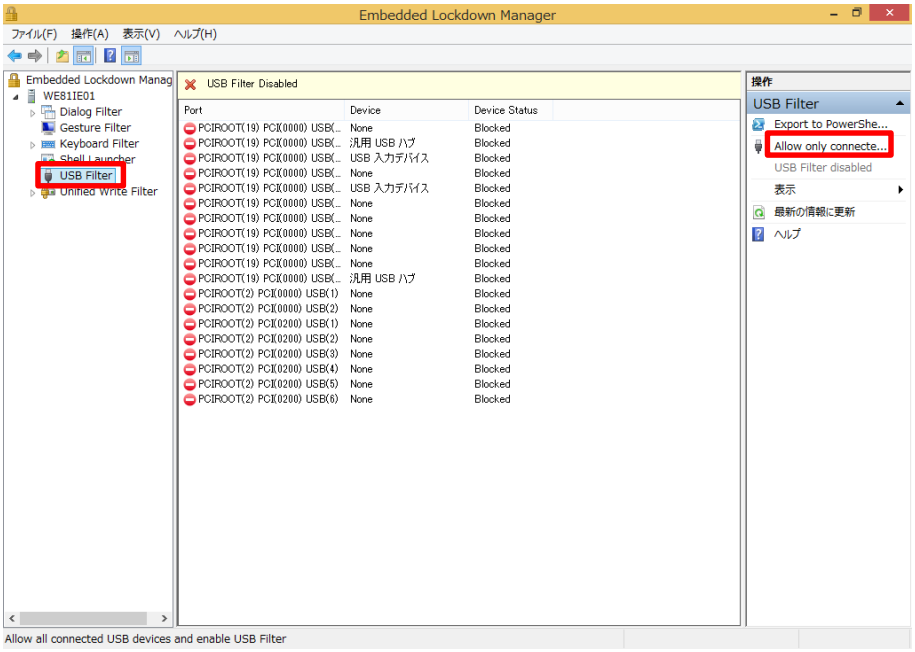
2) スタート画面を開き、↓ をクリックします。

3) スタート画面で、[Embedded Lockdown Manager] をクリックします。

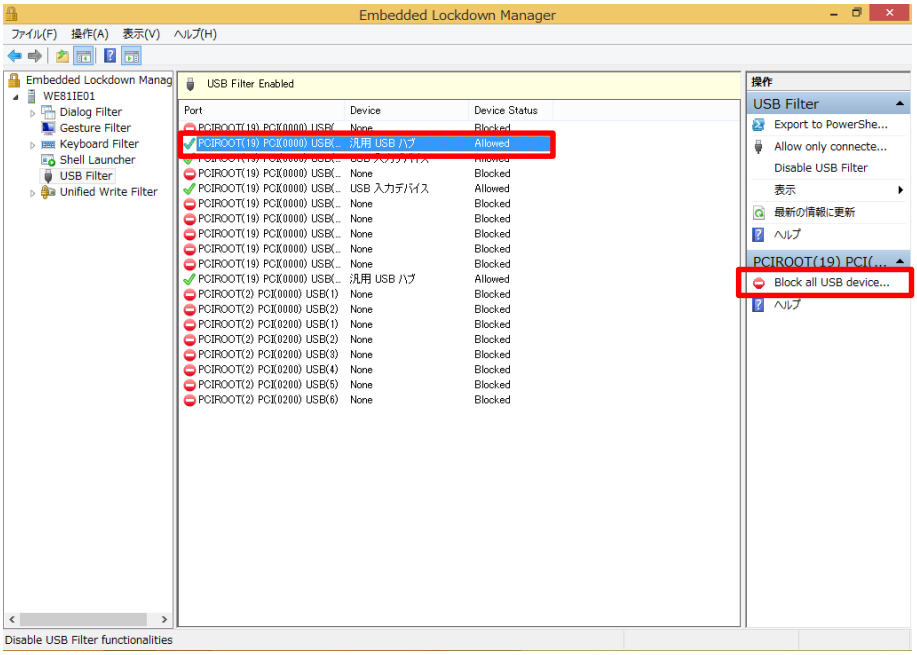


4) [ユーザー アカウント制御] 画面で、[はい] をクリックします。

5) [Embedded Lockdown Maneger] 画面で、左ペインの [USB Filter] をクリックし、右ペインの [Allow only connected devices] をクリックします。



6) [Embedded Lockdown Maneger] 画面で、中央ペインの [Device Status] 欄が Allowed になっているポートをクリックし、右ペインの [Block all USB devices on this port] をクリックします。



7) 手順 5 を繰り返し、すべてのポートが Blocked になるまで繰り返します。

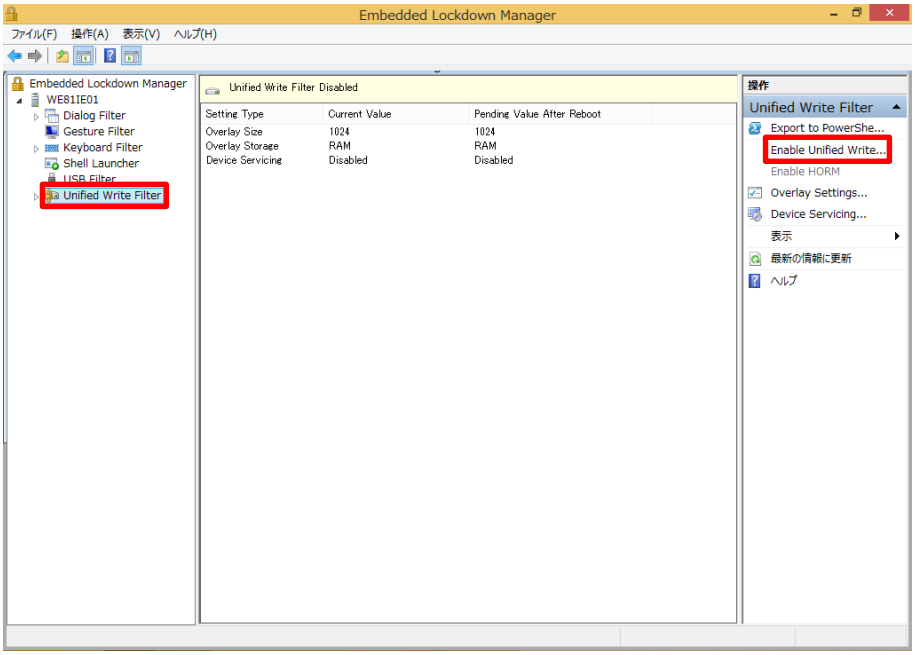
【Note:】
本手順では、すべての USB デバイスを無効にする設定を行いましたが、第 2 章でも解説したように特定のポート、デバイス、またはデバイスクラスに対してのみを有効/無効にすることが可能です。しかし、Embedded Lockdown Manager ではポート単位での設定しかできないため、デバイスまたはデバイス クラスを単位とする設定を行う場合、Windows PowerShell より以下のコマンドレットを順に実行します。(下記のコマンドレットをまとめて PowerShell スクリプトとして実行することも可能です)

```
$wmiNS = "root¥standardcimv2¥embedded"

#アクセス許可リストの取得と表示
$permissions = Get-WmiObject -namespace $wmiNS -class USBF_PermissionEntry
Echo "Total " $permissions.Count "USB Permission Entries"
$permissions | format-table Port*, Device*, Permission*

#新しいアクセス許可の設定
$PermissionEntryClass = [WMIClass]
"root¥standardcimv2¥embedded:USBF_PermissionEntry"
$PermissionEntry = $PermissionEntryClass.CreateInstance();
$PermissionEntry.PortLocationPath = "PCIROOT(0)#PCI(1D07)#USB(2)"    # ポート
$PermissionEntry.PermissionLevel   = 2          # デバイス レベル
$PermissionEntry.DeviceClassID      = 3          # デバイス クラス
$PermissionEntry.DeviceProductID   = 12345          # プロダクト ID (10 進数で入力)
$PermissionEntry.DeviceVendorID    = 123          # ベンダー ID (10 進数で入力)
$PermissionEntry.Put()

#アクセス許可リストの取得と表示
$permissions = Get-WmiObject -namespace $wmiNS -class USBF_PermissionEntry
Echo "Total " $permissions.Count "USB Permission Entries"
$permissions | format-table Port*, Device*, Permission*
```

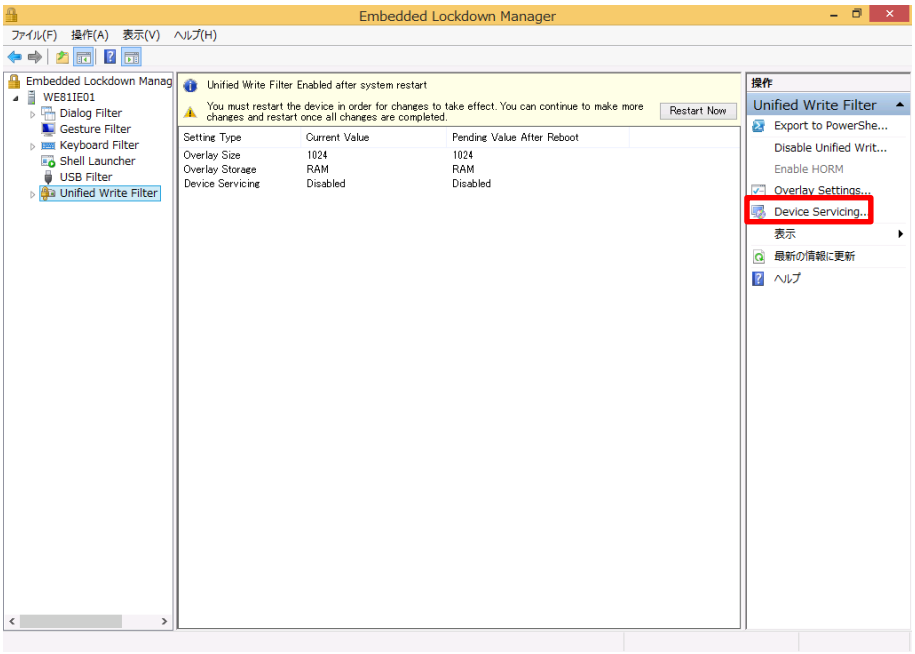
7.2 書き込みフィルターによる書き込み制限設定

Embedded Lockdown Manager の 書き込みフィルターを設定し、ハードディスクにファイルを永続的に保存できないように構成します。また、書き込みフィルターの例外設定として、Windows Update による更新プログラムのインストール内容が書き込まれるように構成します。

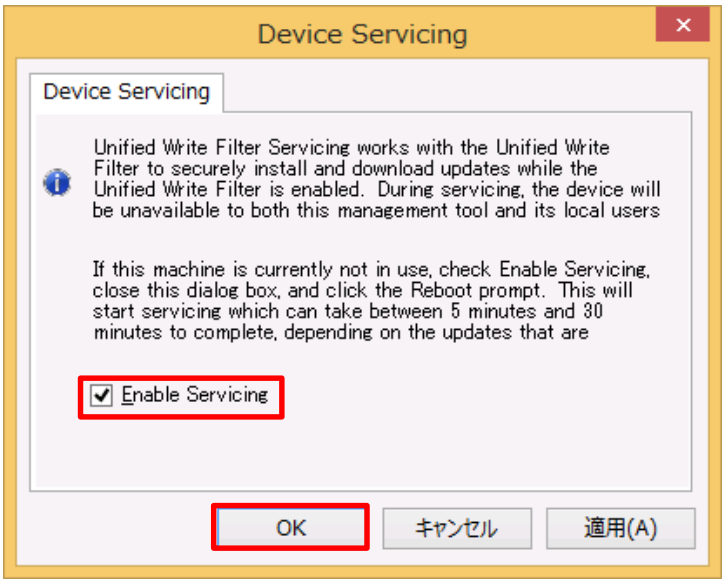
1) [Embedded Lockdown Maneger] 画面で、左ペインの [Unified Write Filter] をクリックし、右ペインの [Enable Unifide Write Filter] をクリックします。



2) [Embedded Lockdown Maneger] 画面で、右ペインの [Device Servicing] をクリックします。



3) [Device Servicing] 画面で、[Enable Servicing] にチェックをつけ、[OK] をクリックします。



【Note:】[A5]

Windows Update 以外にも、ファイル、フォルダーおよびレジストリの例外設定により、System Center Endopoint Protection 定義ファイルの適用や、Windows Defender 定義ファイルが適用されるよう構成できます。設定に関する詳細は下記サイトを参考にしてください。

■ Antimalware support on UWF-protected devices

http://msdn.microsoft.com/en-us/library/dn449271(v=winembedded.82).aspx

7.3 設定の確認

読み取り専用リッチクライアントとしての設定を行ったコンピューターは 4.3.2 節で行った確認作業と同じように、キャッシュを使用した一時的なファイルの保存自体は可能ですが、再起動を行うと保存データは消去されます。

8 業務アプリ専用端末への転用

本章では、汎用的な業務で使用していた PC を業務アプリ専用の端末に転用することを目的として Windows Embedded 8.1 Industry Enterprise を利用するために必要な設定について手順を解説します。第 5 章でも解説したように、業務アプリ専用端末へ転用する場合、Windows 8 Application Launcher（もしくは Shell Launcher）、ジェスチャー フィルター、ダイアログフィルターをそれぞれ設定します。[A6][A7]

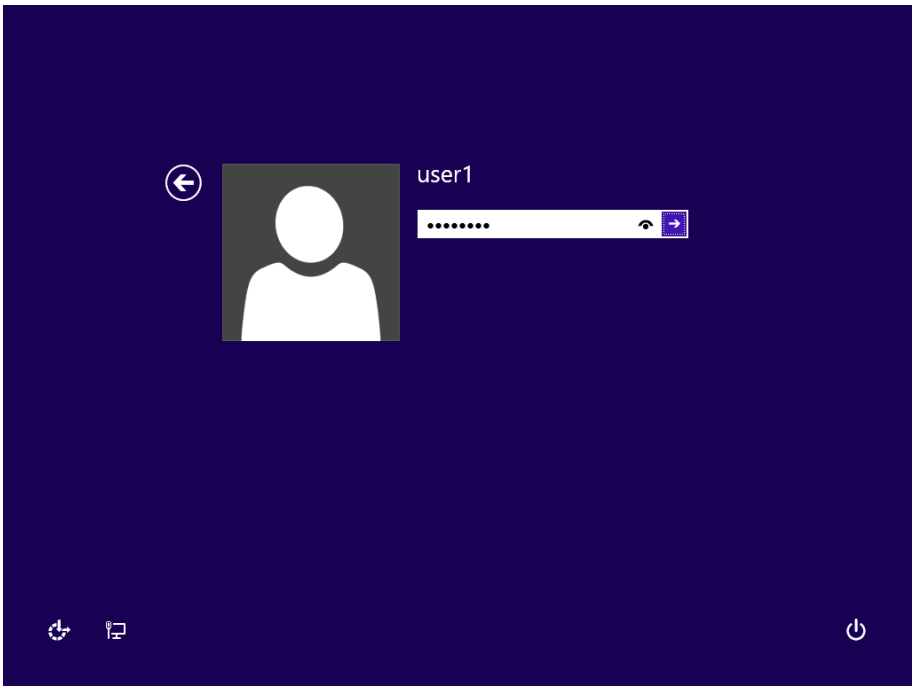
8.1 Application Launcher による実行アプリの指定

Embedded Lockdown Manager の Windows 8 Application Launcher を設定し、特定のユーザーでサインインしたときに、特定のアプリ (本手順では、MSN 天気を業務アプリ専用端末で実行する唯一のアプリと想定します) だけが実行されるように構成します。

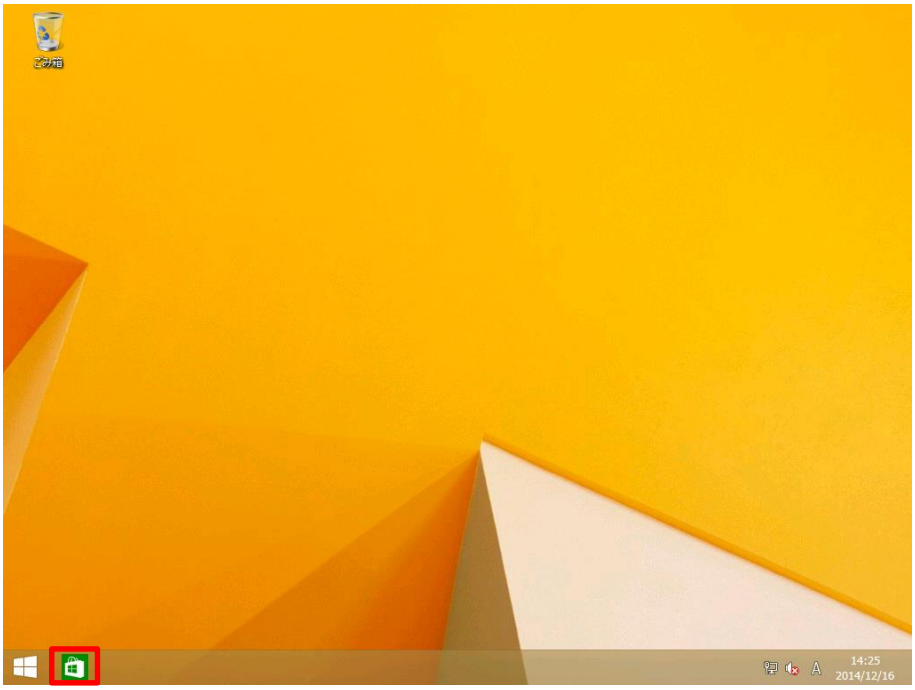
8.1.1 MSN 天気アプリのインストール[A8]

MSN 天気アプリは Windows Embedded 8.1 Industry Enterprise に既定でインストールされていません。そのため、最初の手順として Windows ストアから MSN 天気アプリをインストールします。

1) WE81IE01 に、User1 ユーザーでサインインします。



2) デスクトップ画面で、ストア アイコンをクリックします。

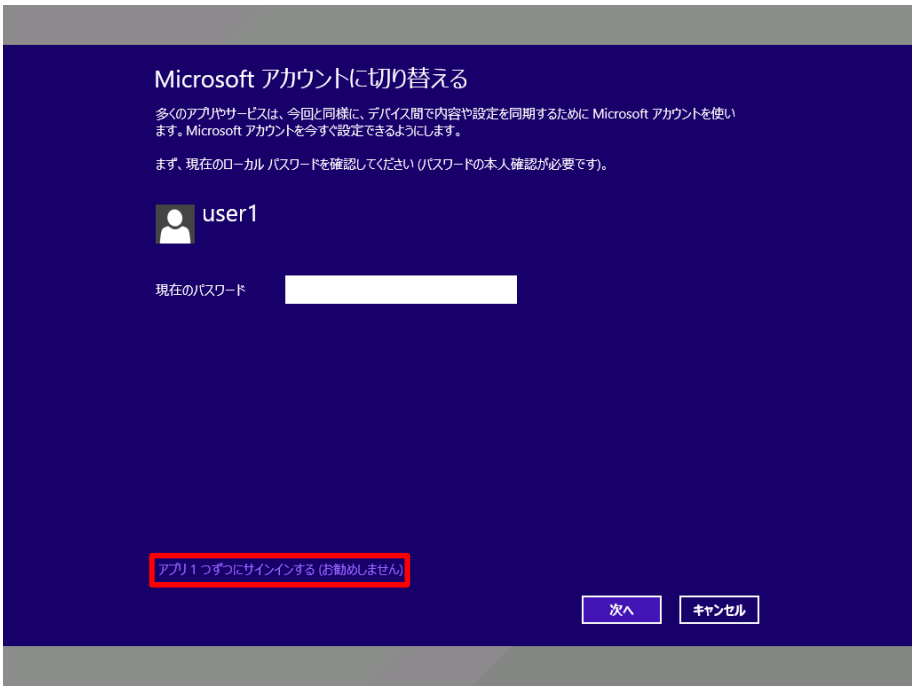


3) [ストア] 画面で、検索画面に「MSN 天気」と入力し、Enter キーを押します。

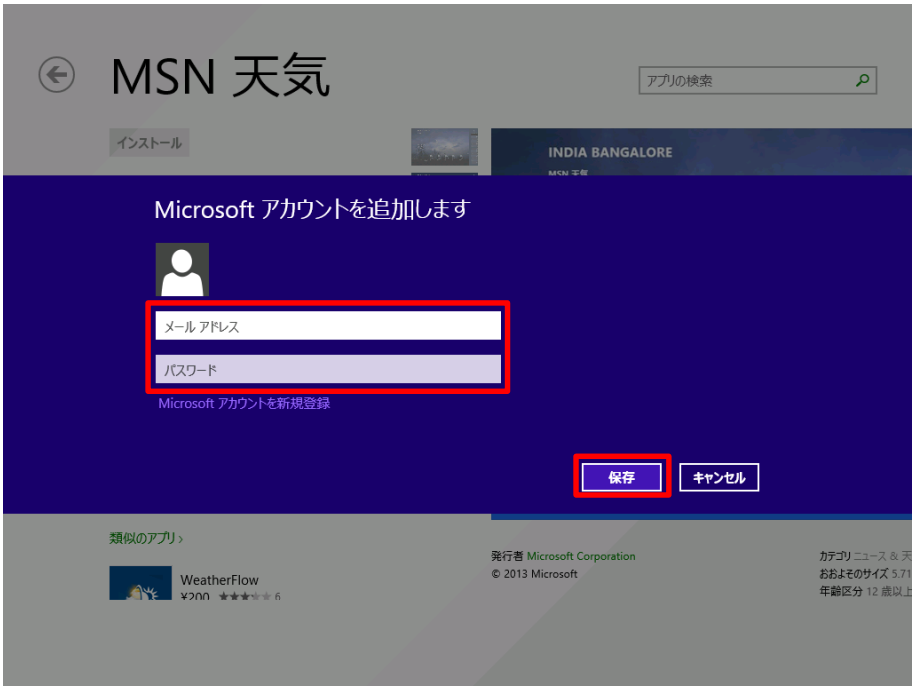
4) [MSN 天気の検索結果] 画面で、[MSN 天気] をクリックします。

5) [MSN 天気] 画面で、[インストール] をクリックします。

6) [Microsoft アカウントに切り替える] 画面で、[アプリ 1 つずつにサインインする] をクリックします。

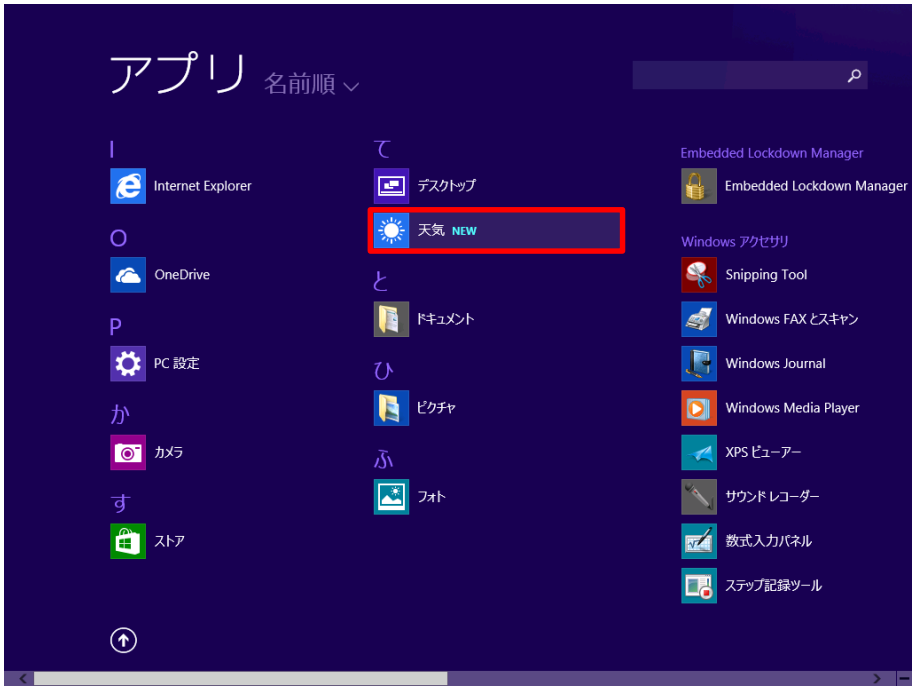


7) [Microsoft アカウントを追加します] 画面で、切り替える Microsoft アカウントのメールアドレスとパスワードをそれぞれ入力し、[保存] をクリックします。

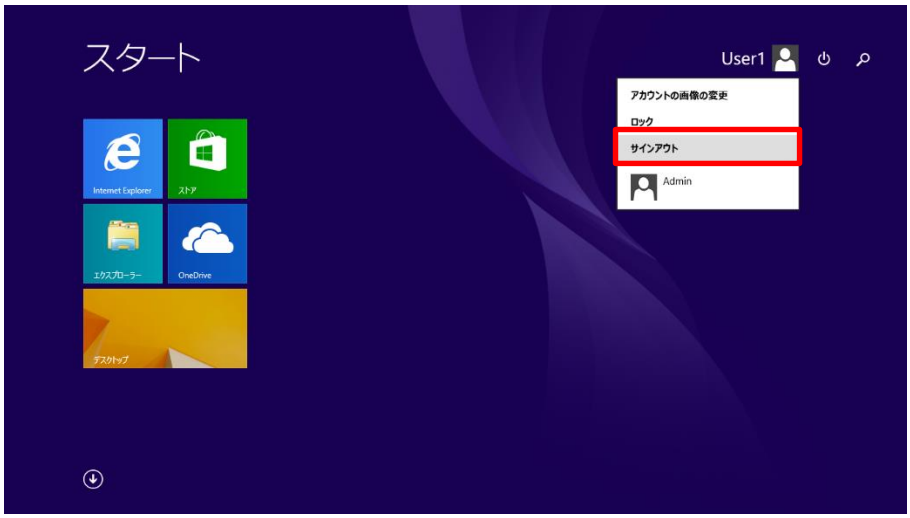


8) [無料アプリをインストールしています] 画面で、[後で確認する] をクリックします。
以上の操作により、MSN 天気アプリのインストールが開始します。

9) MSN 天気アプリのインストールが完了したことは、スタートメニューに [天気] が追加されたことで確認できます。



10) User1 ユーザーからサインアウトします。[A9]

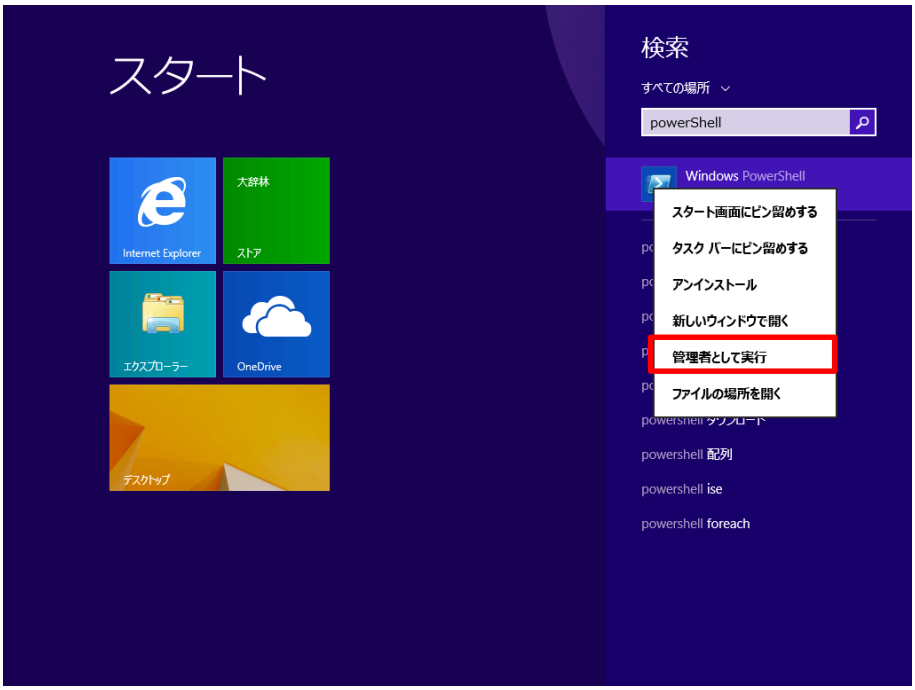


8.1.2 Application Launcher の有効化

Embedded Lockdown Manager の Windows 8 Application Launcher は既定で無効になっています。そのため、Windows PowerShell から Application Launcher を有効にします。

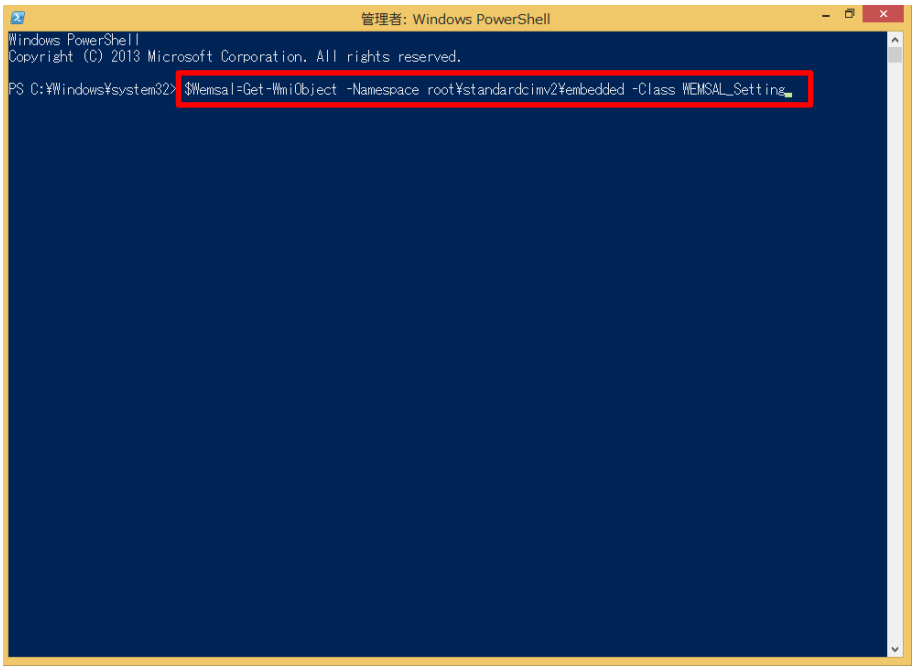
1) WE81IE01 コンピューターに、、Admin ユーザーでサインインします。

2) スタート画面を開き、「PowerShell」と入力し、[管理者として実行] をクリックします。

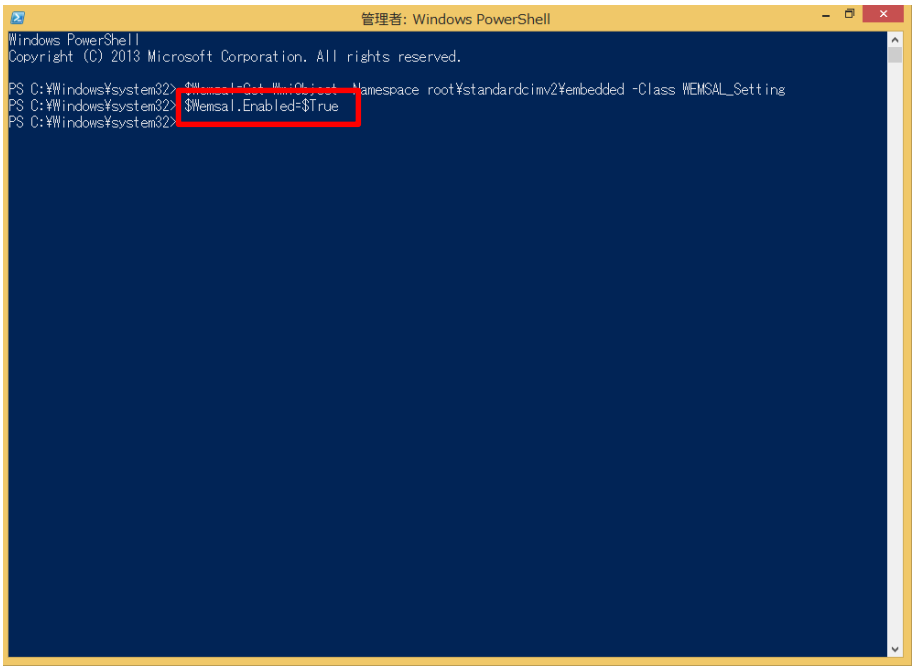


3) [ユーザー アカウント制御] 画面で、[はい] をクリックします。

4) [管理者 : Windows PowerShell] 画面で、「$Wemsal=Get-WmiObject -Namespace root¥standardcimv2¥embedded -Class WEMSAL_Setting」と入力し、Enter キーを押します。



5) [管理者：Windows PowerShell] 画面で、「$Wemsal.Enabled=$True」と入力し、Enter キーを押します。



6) Ctrl+Alt+Del キーを押し、再起動します。

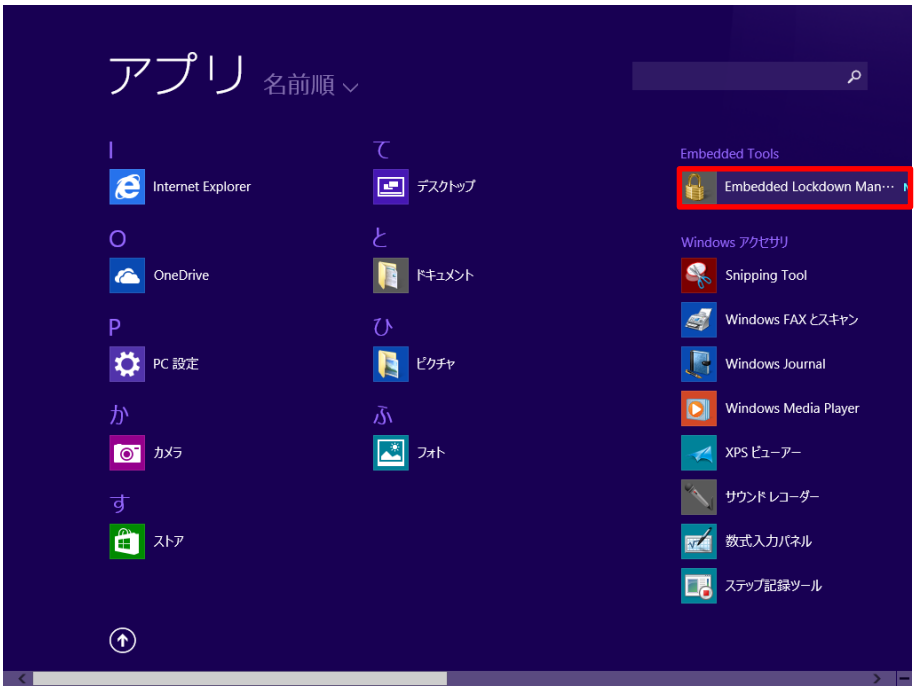
8.1.3 Application Launcher の設定

Embedded Lockdown Manager の Application Launcher で MSN 天気だけがを実行できるように構成します。今回は、MSN 天気を業務アプリに見立てて設定しています。
尚、業務アプリが、デスクトップ アプリケーションの場合は、 Shell Launcher を使用します。
Shell Launcher の設定方法については、 6.2 節を参照してください。

1) WE81IE01 に、 Admin ユーザーでサインインします。

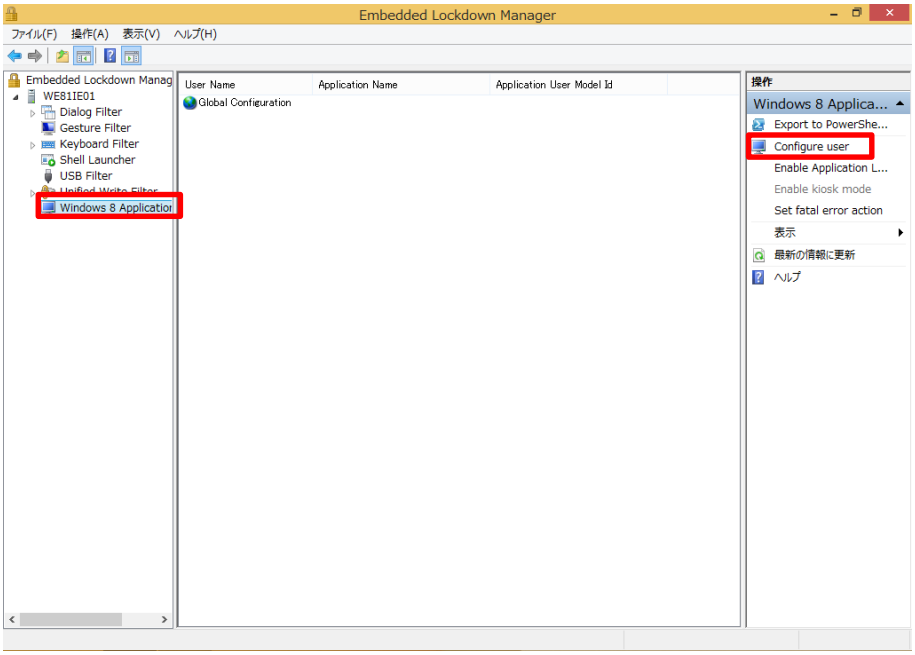
2) スタート画面を開き、 ↓をクリックします。

3) スタート画面で、[Embedded Lockdown Manager] をクリックします。



4) [ユーザー アカウント制御] 画面で、[はい] をクリックします。

5) [Embedded Lockdown Maneger] 画面で、左ペインの [Windows 8 Application Launcher] をクリックし、右ペインの [Configure user] をクリックします。

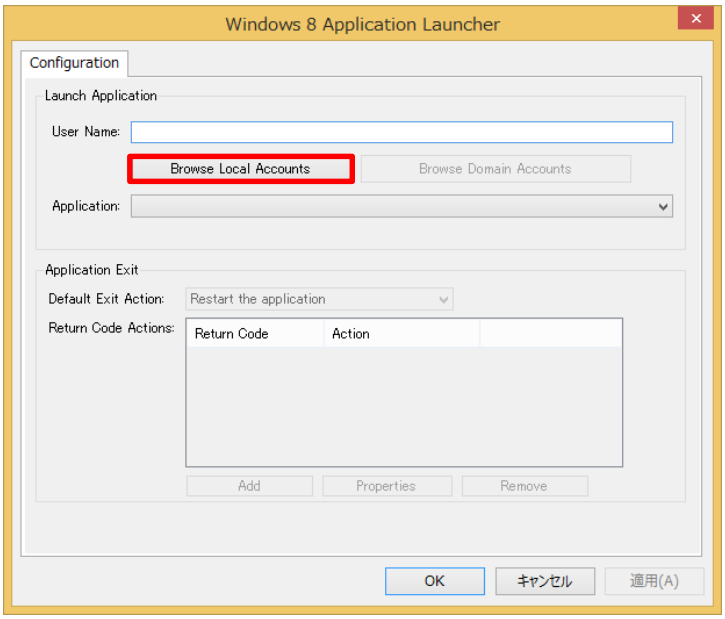


【Note:】

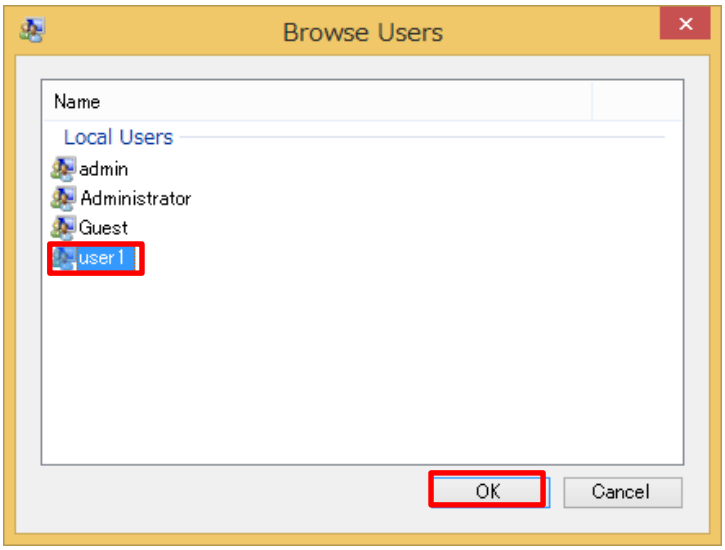
Windows 8 Application Launcher が表示されない場合について、4.2 節で説明したアップデート (KB2932074) が適用されていない可能性があります。この場合は、下記サイトよりアップデートをダウンロードして適用してください。

http://www.microsoft.com/en-us/download/details.aspx?id=42025

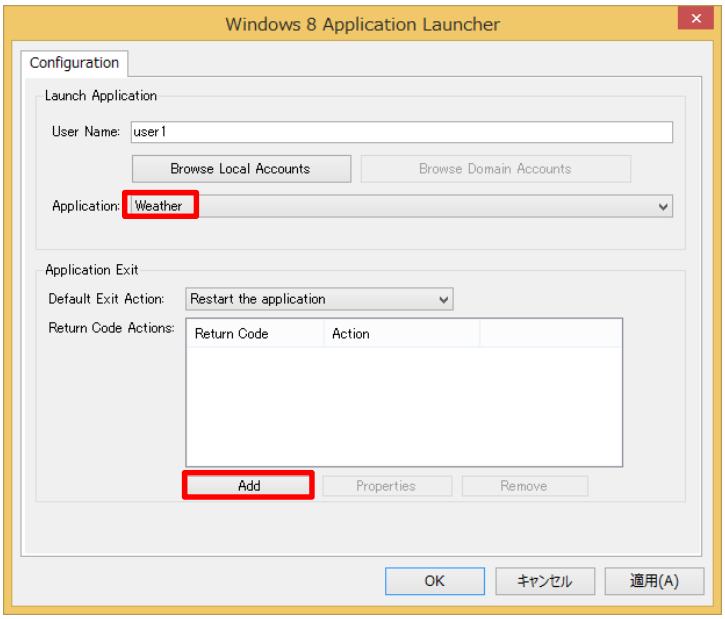
6) [Windows 8 Application Launcher] 画面で、[Browse Local Accounts] をクリックします。



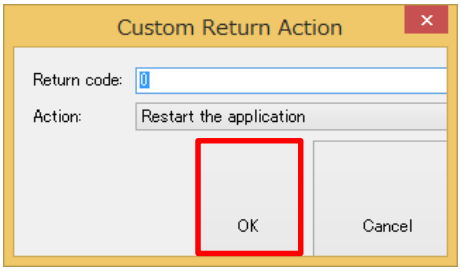
7) [Browse Users] 画面で、[User1] をクリックし、[OK] をクリックします。



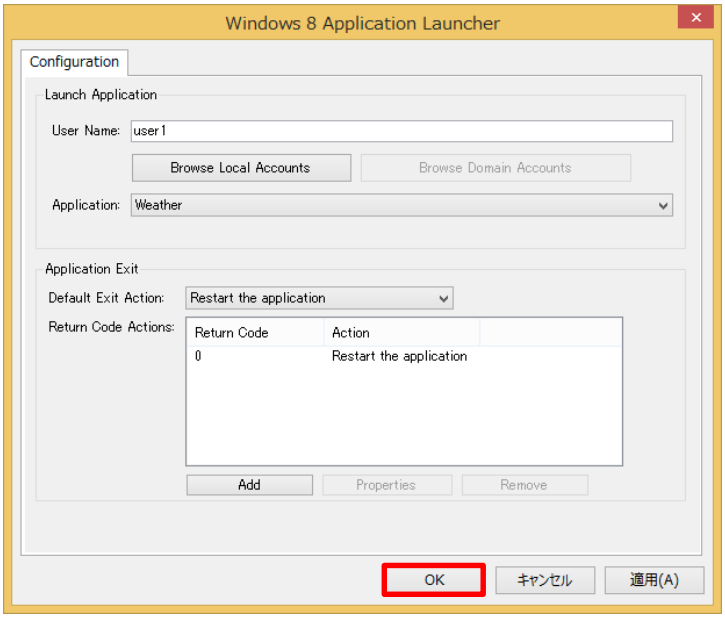
8) [Windows 8 Application Launcher] 画面で、[Application] 欄で [Weather] をクリックし、[Add] をクリックします。



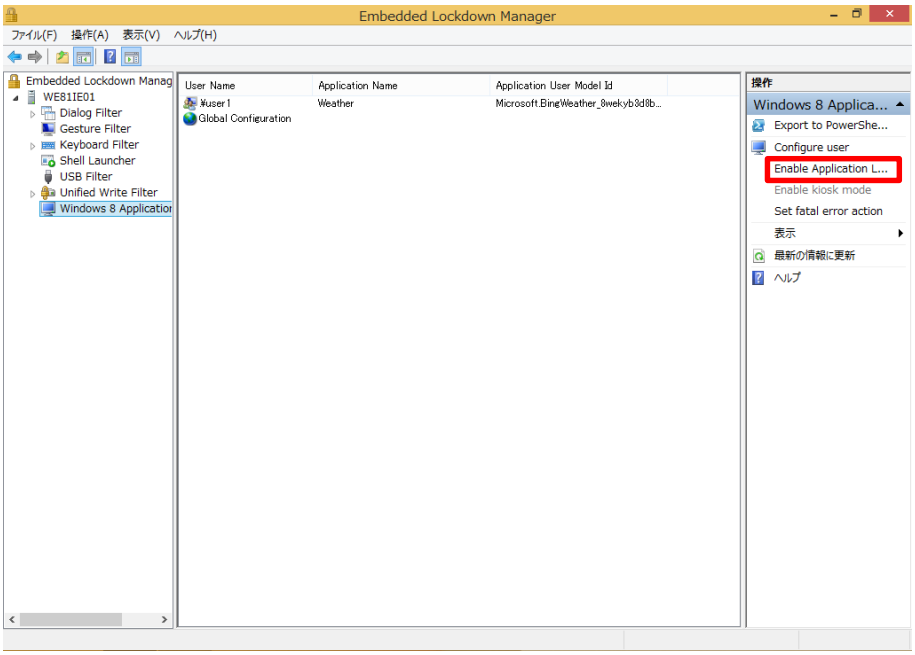
9) [Custom Return Action] 画面で、[OK] をクリックします。



10) [Windows 8 Application Launcher] 画面で、[OK] をクリックします。



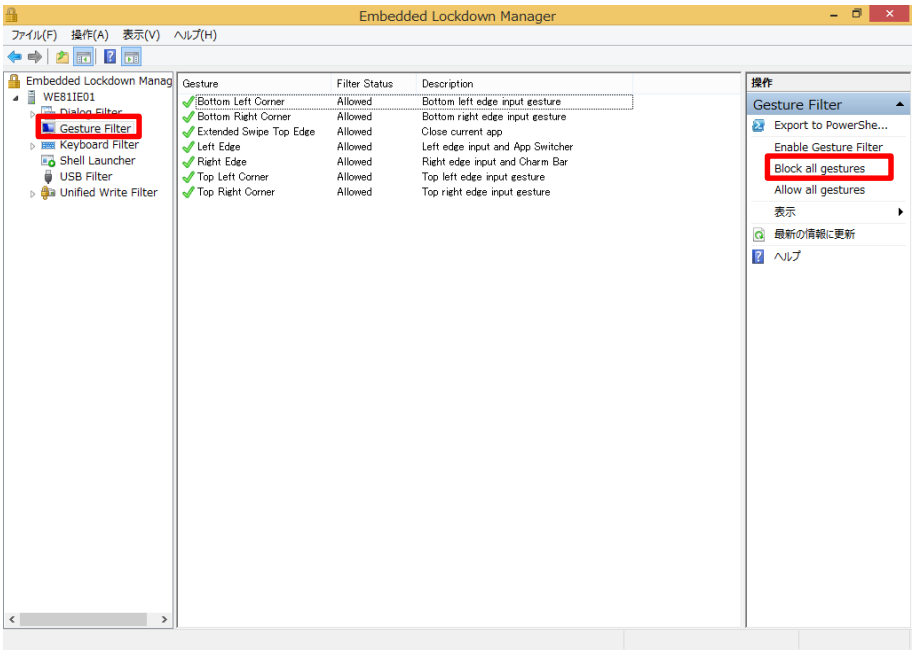
11) [Windows 8 Application Launcher] 画面で、右ペインの [Enable Application Launcher] をクリックします。



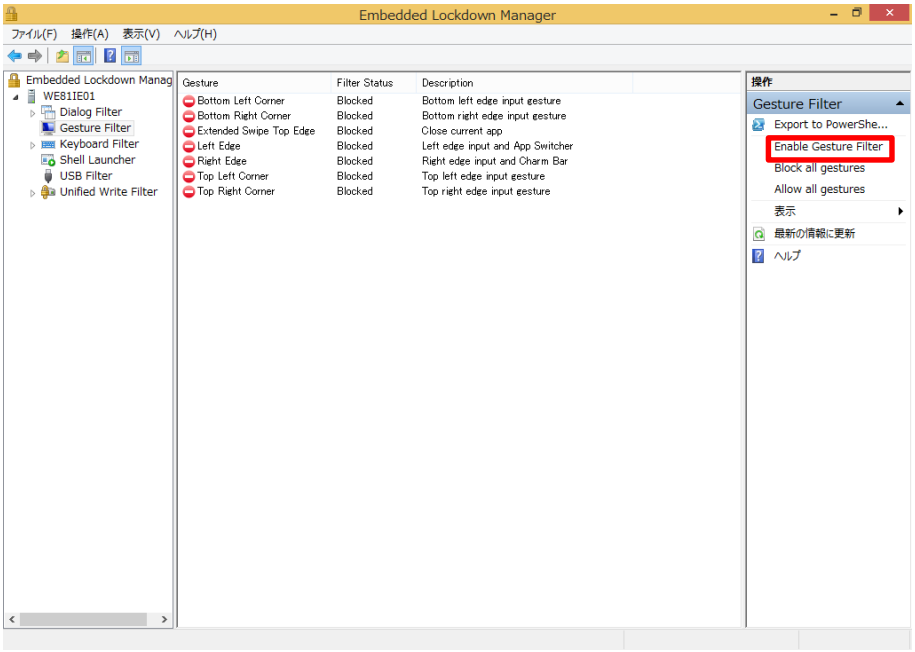
8.2 ジェスチャー フィルターによる Windows 操作の制限設定

Embedded Lockdown Manager のジェスチャー フィルターを設定し、タッチによる各種 Windows 操作の制限を行います。

1) [Embedded Lockdown Maneger] 画面で、左ペインの [Gesture Filter] をクリックし、右ペインの [Block all gestures] をクリックします。



2) [Embedded Lockdown Maneger] 画面で、右ペインの [Enable Gesture Filter] をクリックします。



8.3 ダイアログ フィルターによる Windows 操作の制限設定

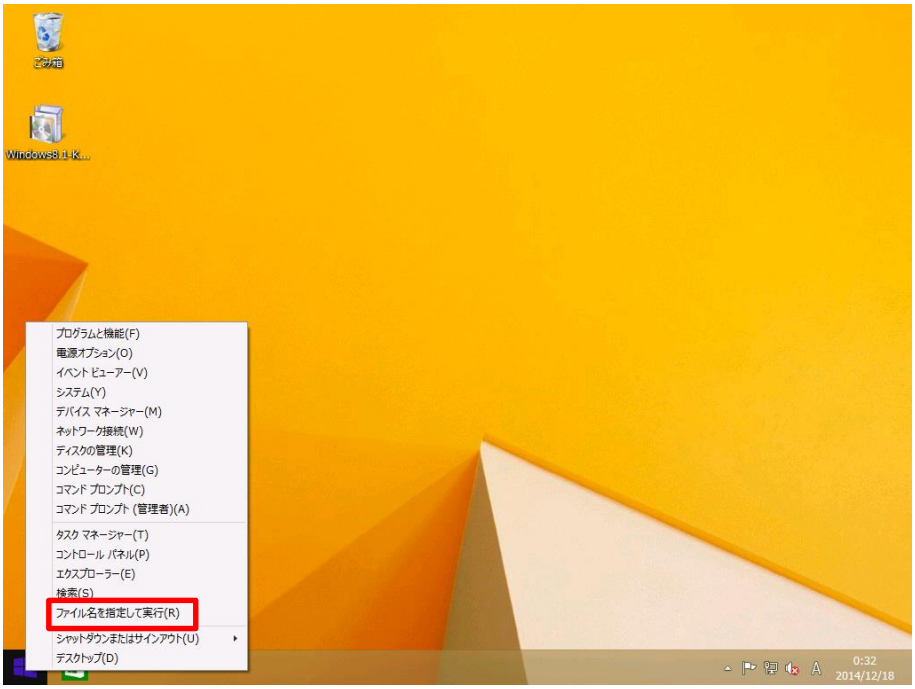
[A10]

Embedded Lockdown Manager のダイアログ フィルターを設定し、意図しないダイアログやウィンドウの表示を制限します。ダイアログ フィルターでは既定でダイアログが表示されないように設定すると、管理者ユーザーでサインインしてもスタート画面が表示されなくなり、Embedded Lockdown Manager 自体も起動できなくなります。そのため、ダイアログ フィルターを設定するときは事前に Embedded Lockdown Manager のショートカットを管理者ユーザーのデスクトップ画面に保存し、スタート画面にアクセスせずに Embedded Lockdown Manager を起動できるようにあらかじめ構成しておく必要があります。

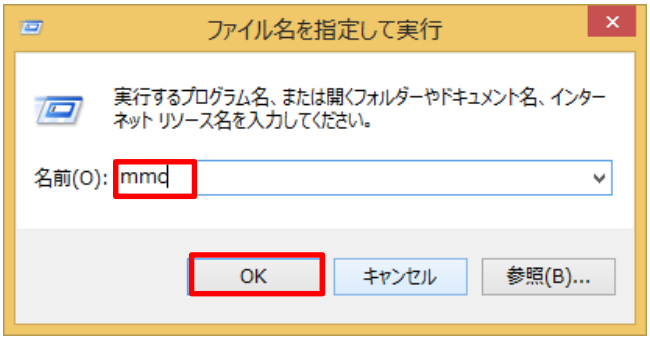
8.3.1 Embedded Lockdown Manager のショートカット作成

Embedded Lockdown Manager のショートカットを管理者ユーザーのデスクトップ画面に作成します。

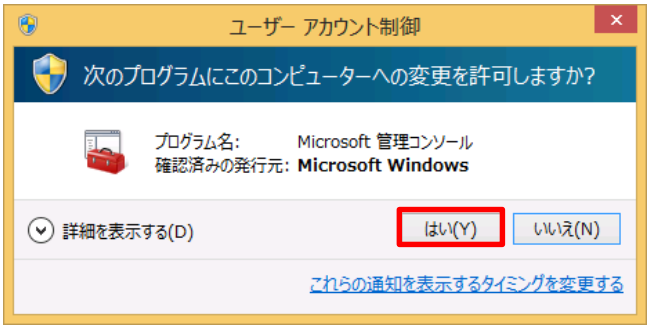
1) スタートボタンを右クリックし、[ファイル名を指定して実行] をクリックします。



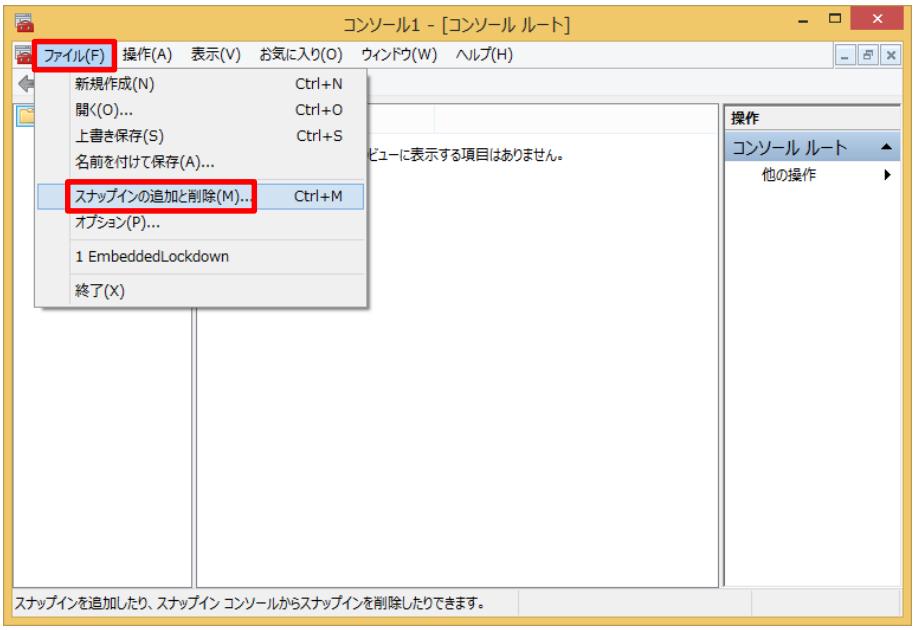
2) [ファイル名を指定して実行] 画面で、「mmc」と入力し、[OK] をクリックします。



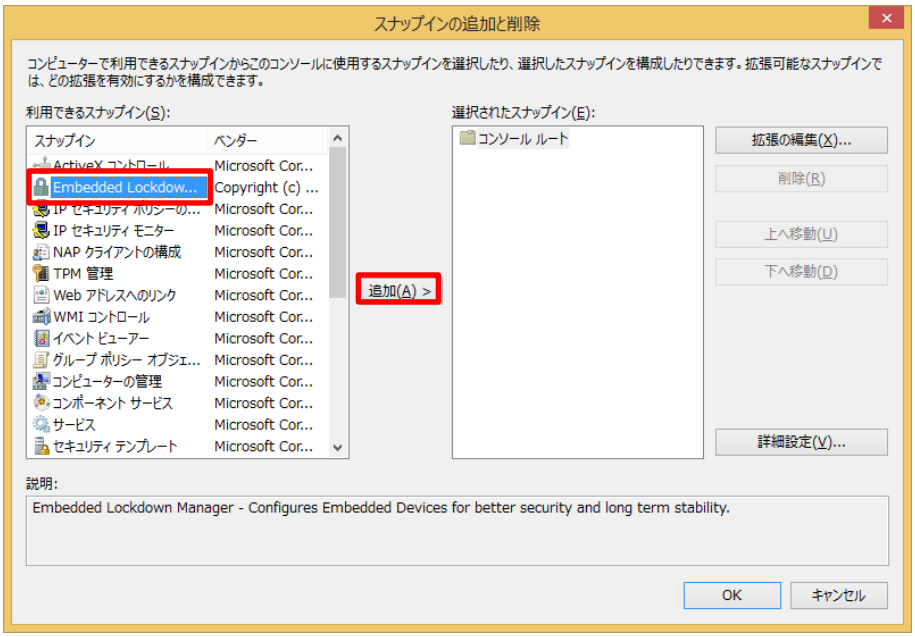
3) [ユーザー アカウント制御] 画面で、[OK] をクリックします。



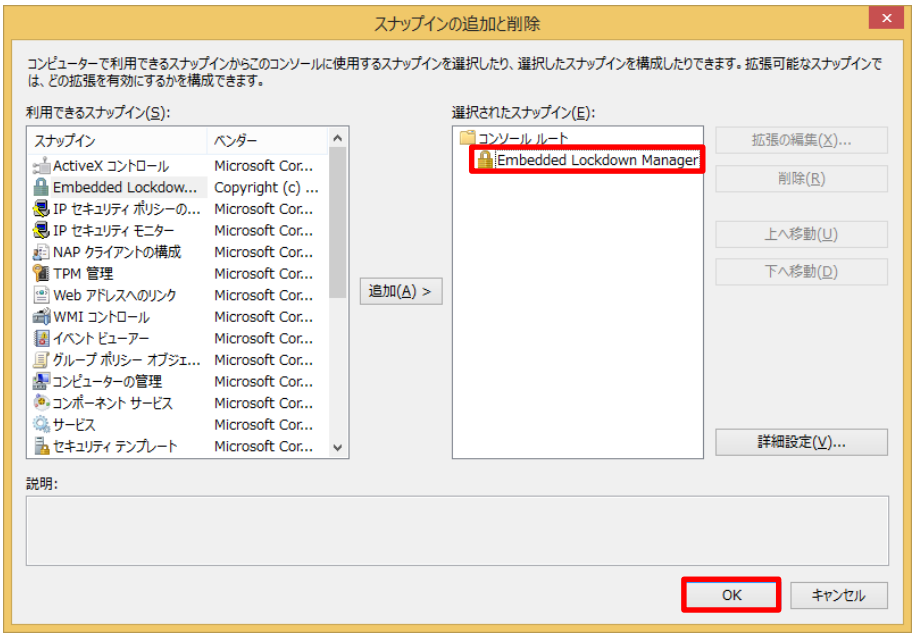
4) [コンソール 1] 画面で、[ファイル] メニューの [スナップインの追加と削除] をクリックします。



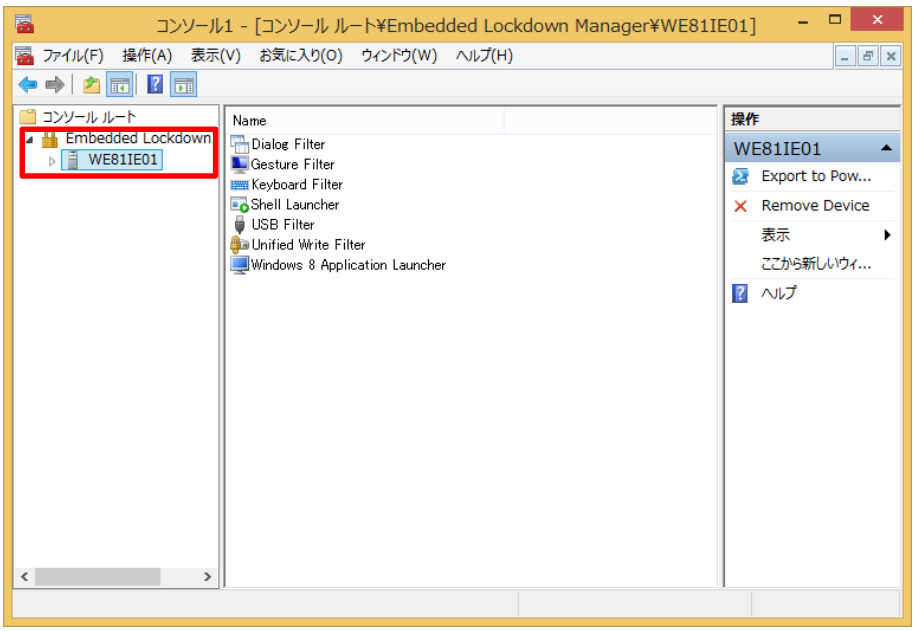
5) [スナップインの追加と削除] 画面で、[利用できるスナップイン] 一覧から [Embedded Lockdown Manager] をクリックし、[追加] をクリックします。



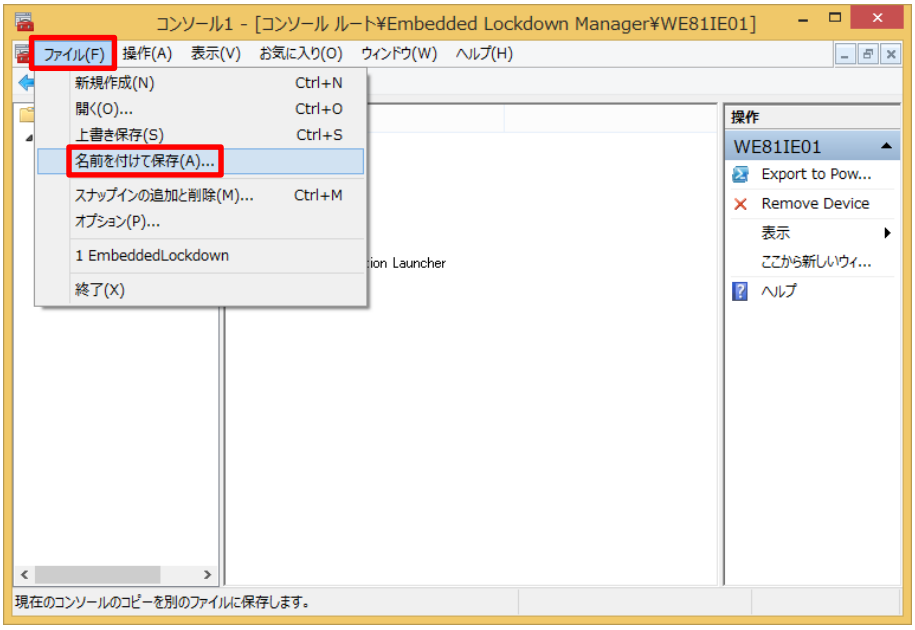
6) [スナップインの追加と削除] 画面で、[選択されたスナップイン] 一覧に [Embedded Lockdown Manager] が追加されたことを確認し、[OK] をクリックします。



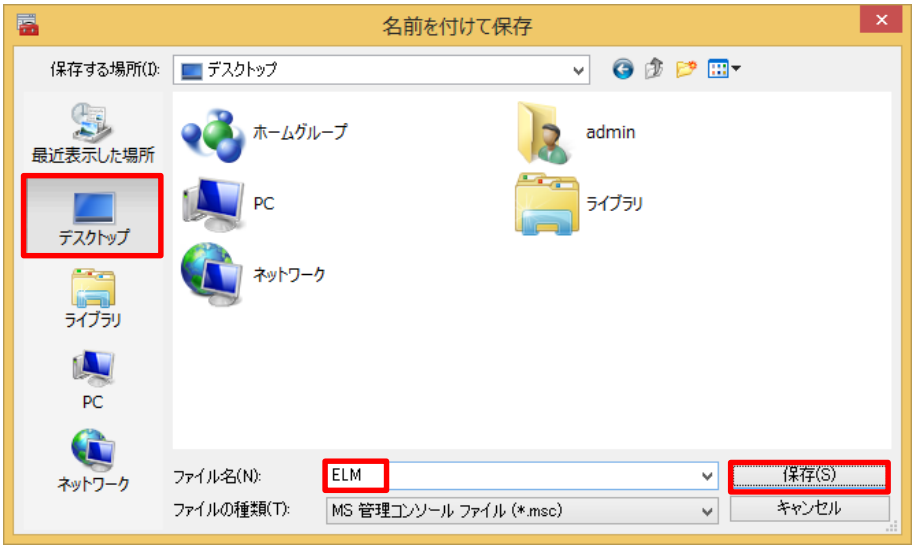
7) [コンソール 1] 画面で、左ペインに [Embedded Lockdown Manager] が追加されたことを確認します。



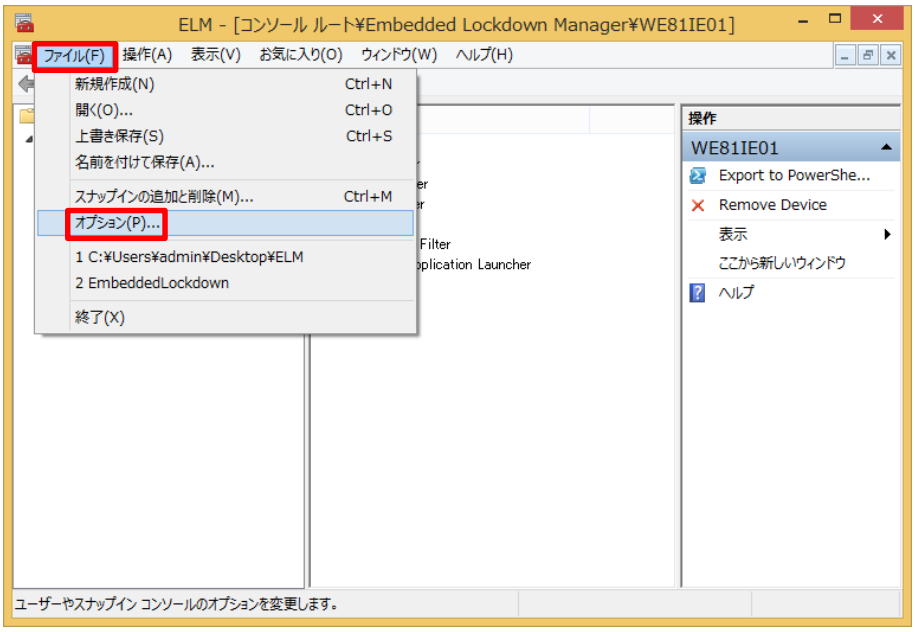
8) [コンソール 1] 画面で、[ファイル] メニューの [名前を付けて保存] をクリックします。



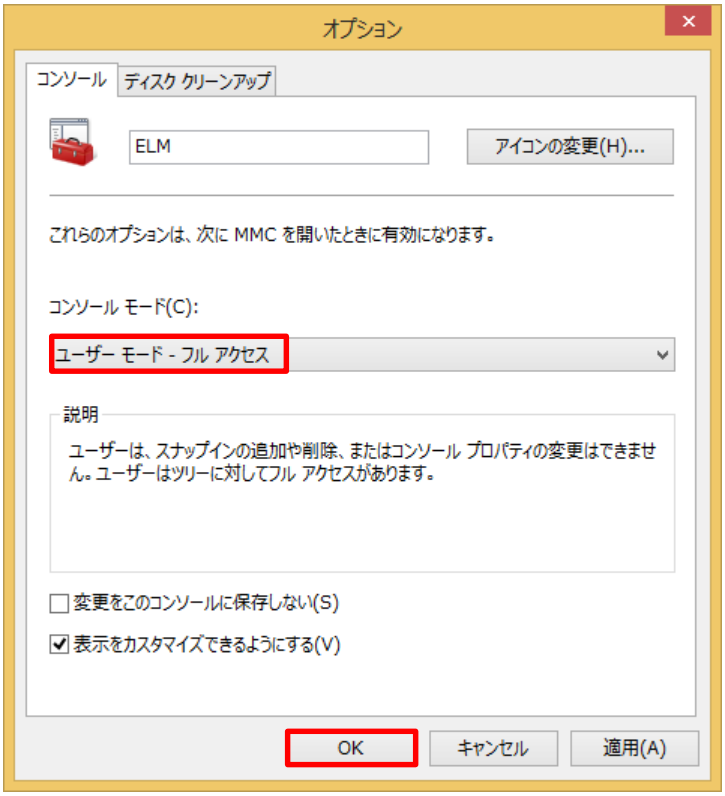
9) [名前を付けて保存] 画面で、デスクトップに「ELM」というファイル名で保存します。



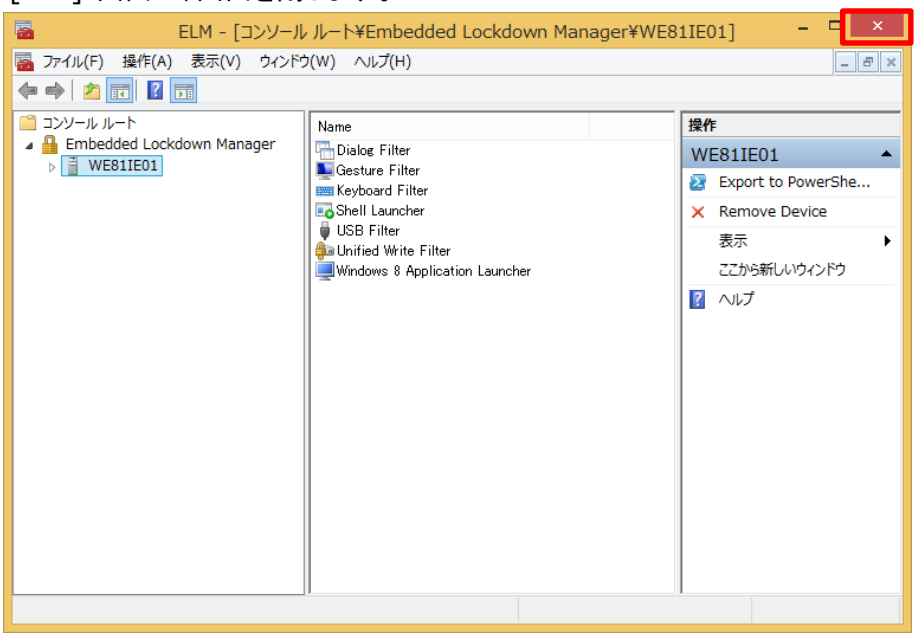
10) [ELM] 画面で、[ファイル] メニューの [オプション] をクリックします。



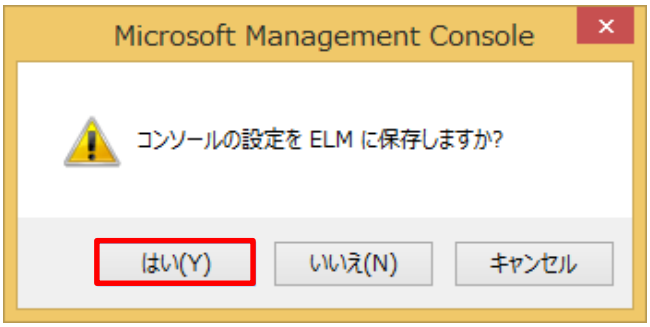
11) [オプション] 画面で、[コンソール モード] 欄から [ユーザー モード - フルアクセス] を選択し、[OK] をクリックします。



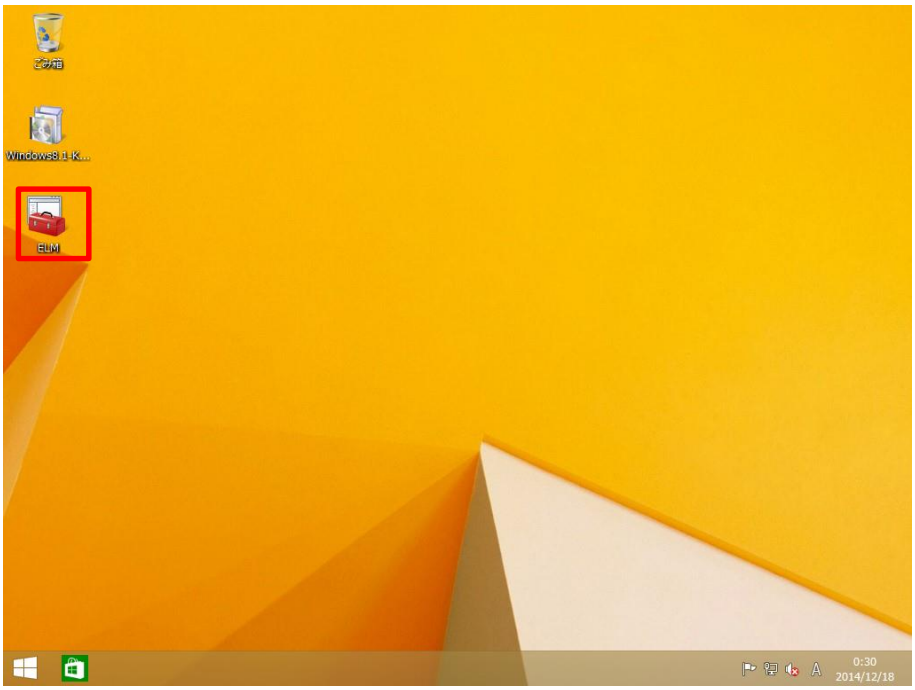
12) [ELM] 画面で、画面を閉じます。



13) [Microsoft Management Console] 画面で、[はい] をクリックします。

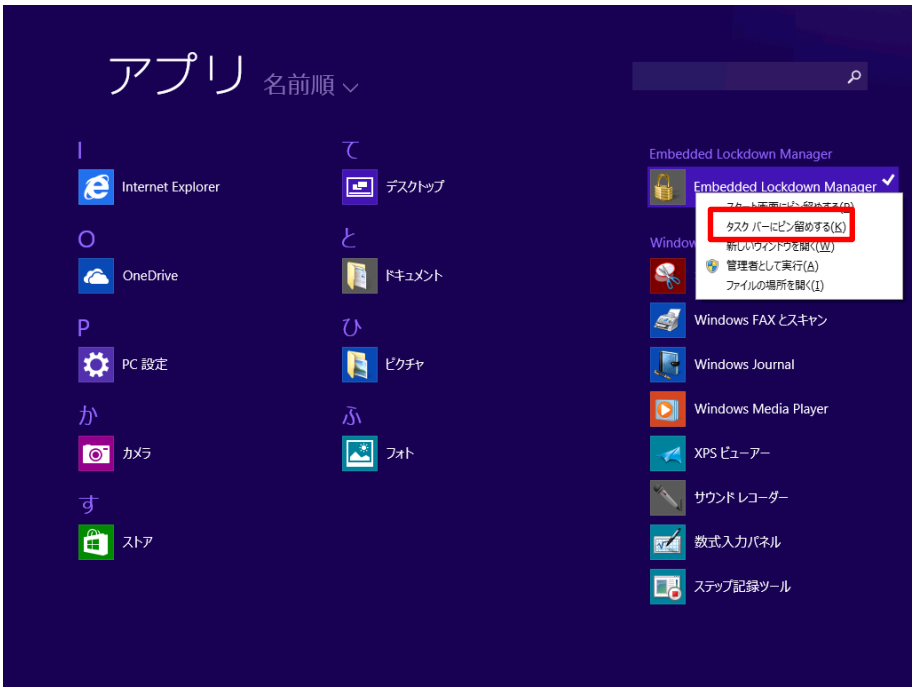


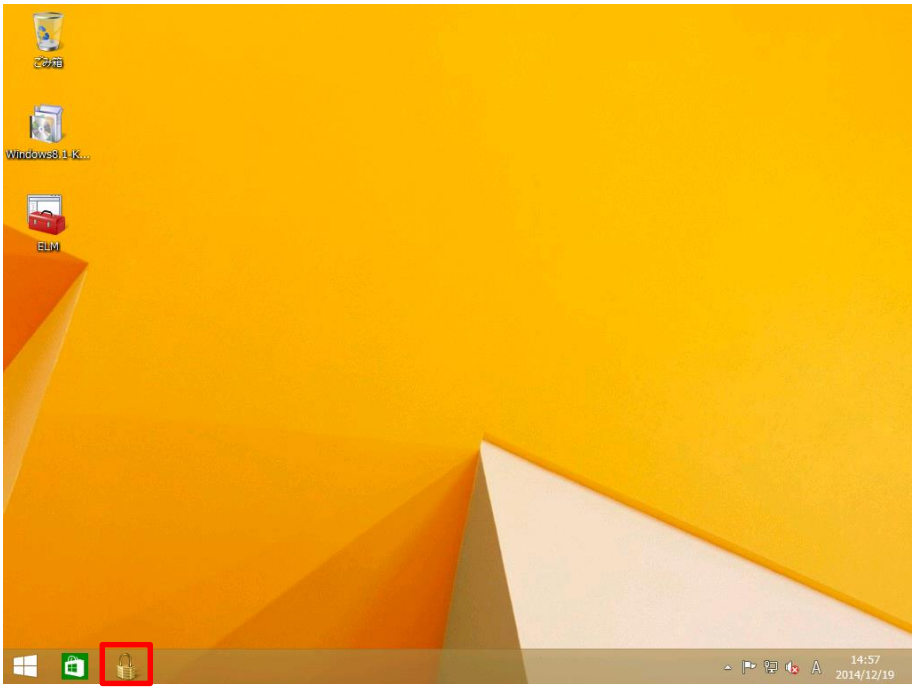
14) デスクトップに ELM という名前の Embedded Lockdown Manager アイコンが保存されたことを確認します。



【Note:】[A11]

Embedded Lockdown Manager を実行するためのアイコンはスタート画面から Embedded Lockdown Manager アイコンを右クリックし、[タスク バーにピン留めする] をクリックすることでも登録することが可能です。

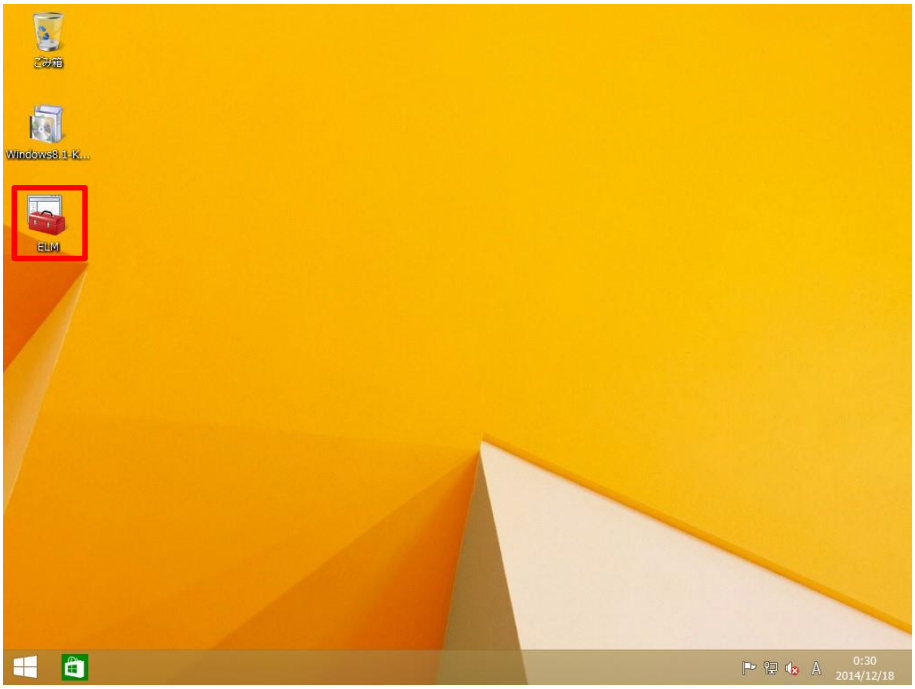




8.3.2 ダイアログ フィルターの設定

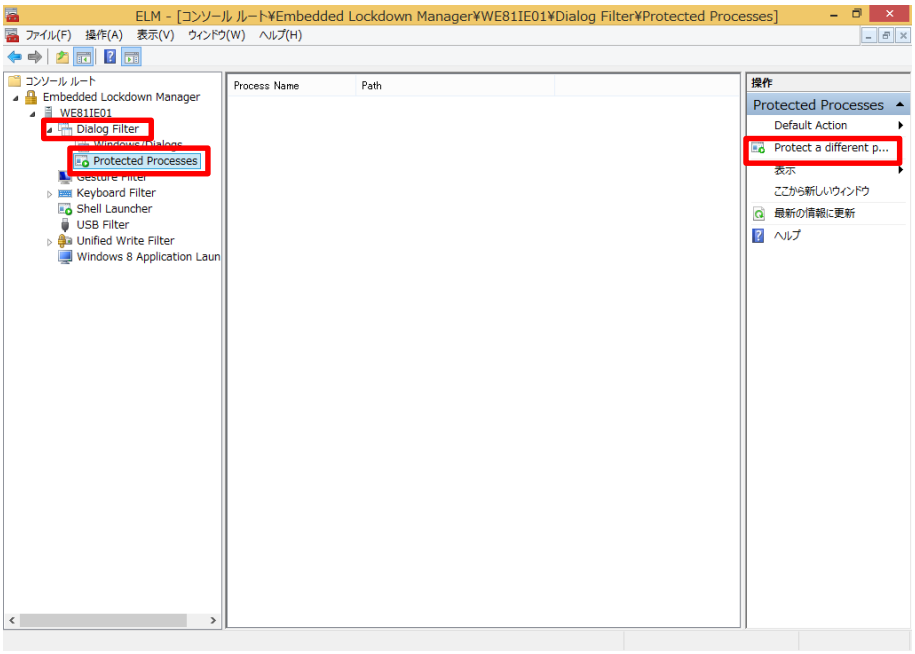
Embedded Lockdown Manager のダイアログ フィルターを設定し、意図しないダイアログやウィンドウの表示を制限します。

1) デスクトップ画面で、[ELM] をダブルクリックします。

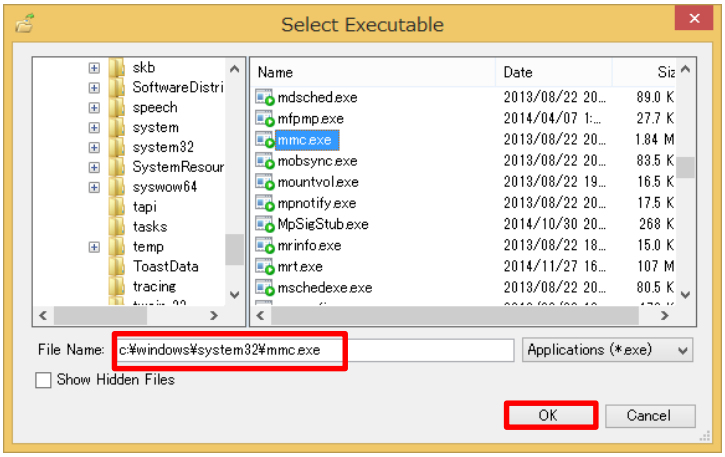


2) [ユーザー アカウント制御] 画面で、[はい] をクリックします。

3) [Embedded Lockdown Maneger] 画面で、左ペインの [Dialog Filter] - [Protected Processes] をクリックし、右ペインの [Protect a different process] をクリックします。



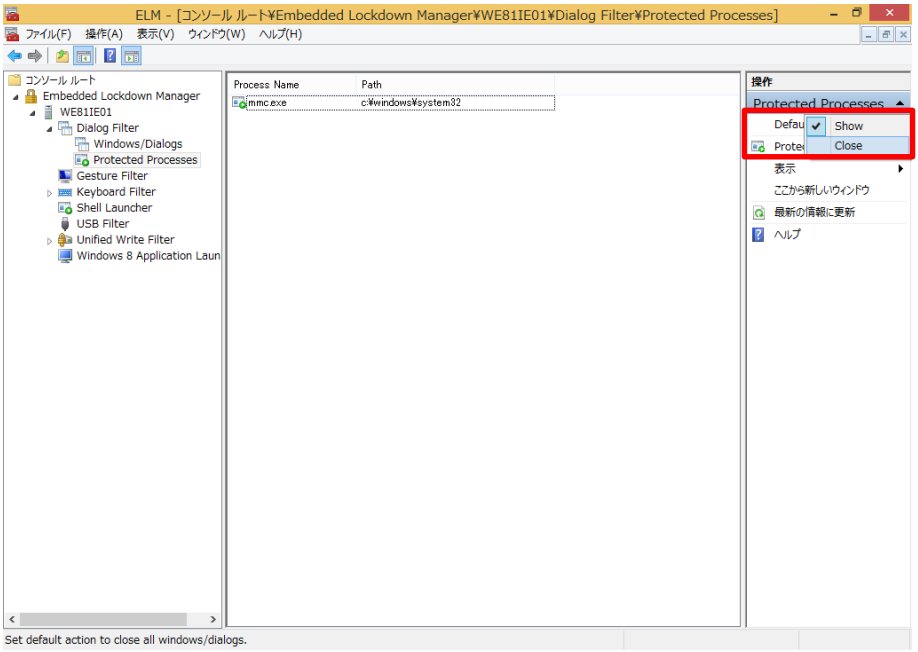
4) [Select Executable] 画面で、c:¥windows¥system32¥mmc.exe[A12] を指定して [OK] をクリックします。



【Note:】

[Dialog Filter] - [Protected Processes] では [Default Action] による既定のダイアログの表示／非表示設定にあわせて、個別のプログラムごとに表示／非表示のを指定することで既定の設定に対する例外を登録できます。

5) [Embedded Lockdown Maneger] 画面で、右ペインの [Default Action] - [Close[A13]] をクリックします。

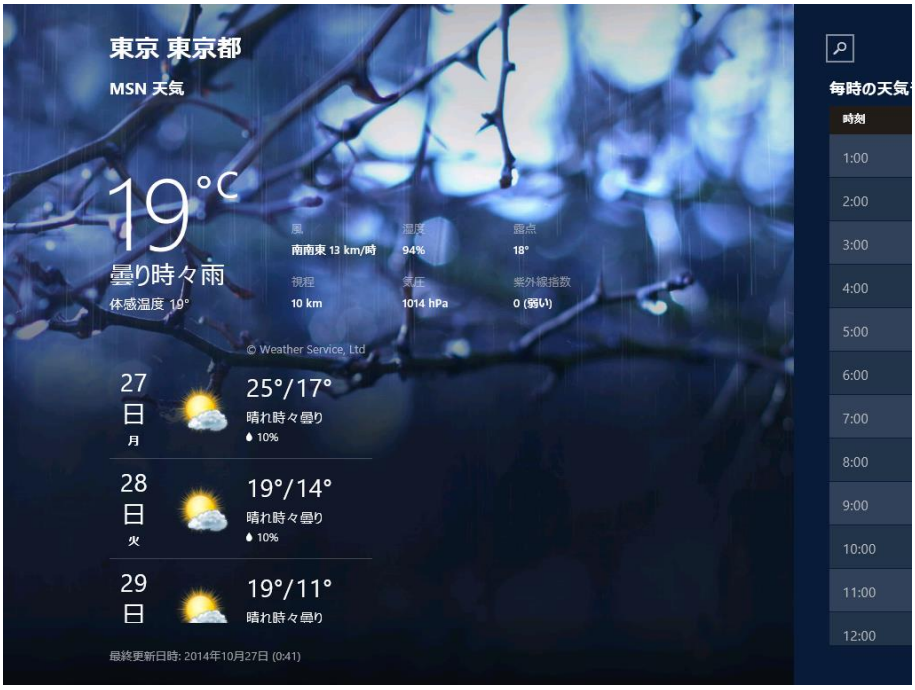


8.4 設定の確認

8.1 ～ 8.3 節で設定した内容を確認します。

1) WE81IE01 に、User1 としてサインインします。

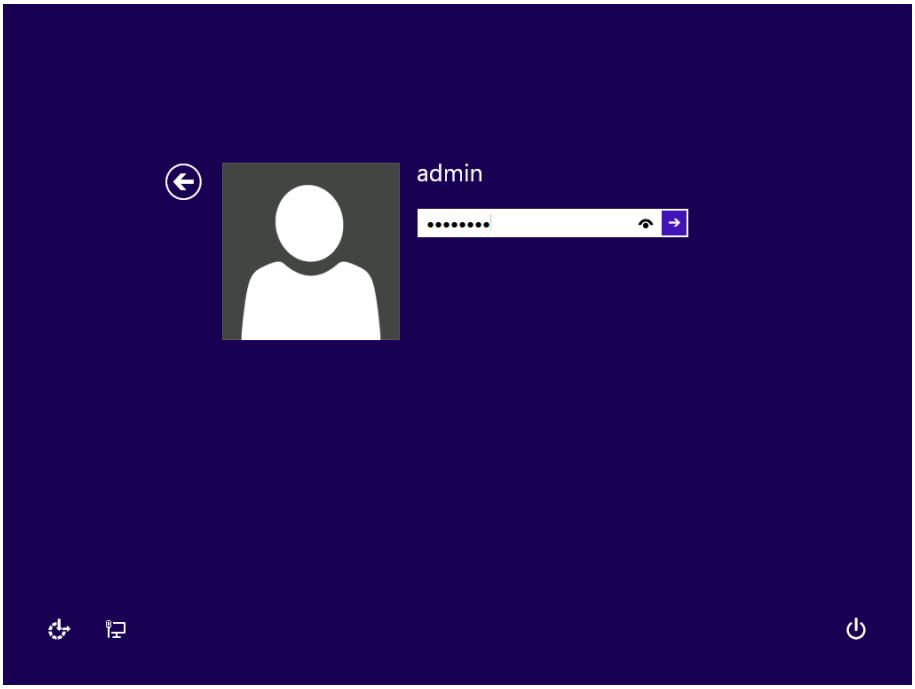
2) MSN 天気アプリが表示され、その他のプログラムが一切起動できないことが確認できます。また、ジェスチャー フィルターによって、タッチ操作も制限されていることも確認できます。



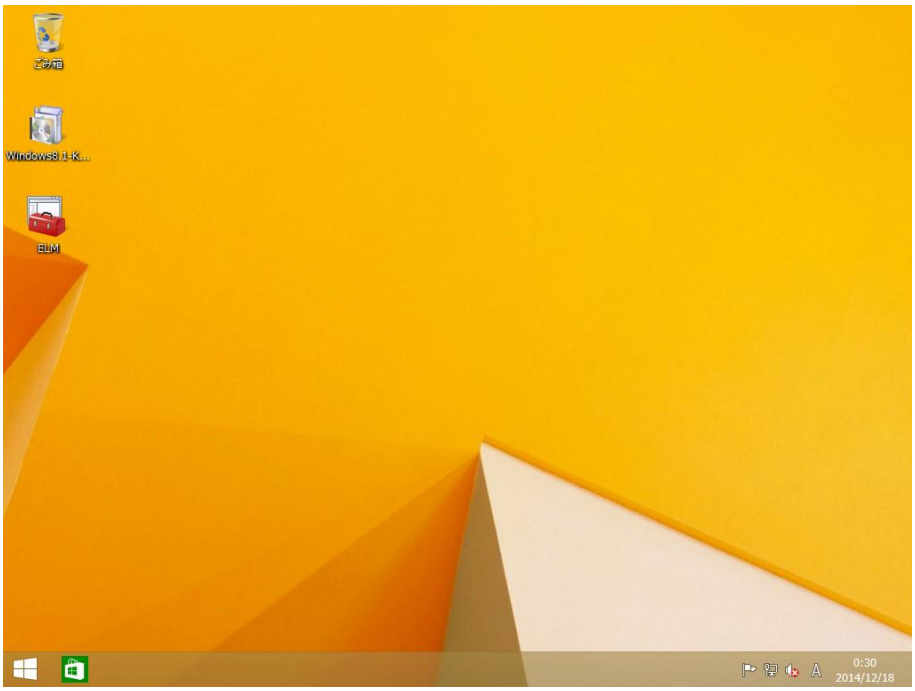
3) Ctrl + Alt + Del キーを押し、サインアウトします。

【Note:】
Windows 8 Application Launcher で特定のアプリだけ実行するように構成した場合、マウス操作によってサインアウトやシャットダウンを含む、一切の操作を行えなくなります。そのため、サインアウト操作を行うときはキーボードによる Ctrl + Alt + Del キー操作を利用してください。

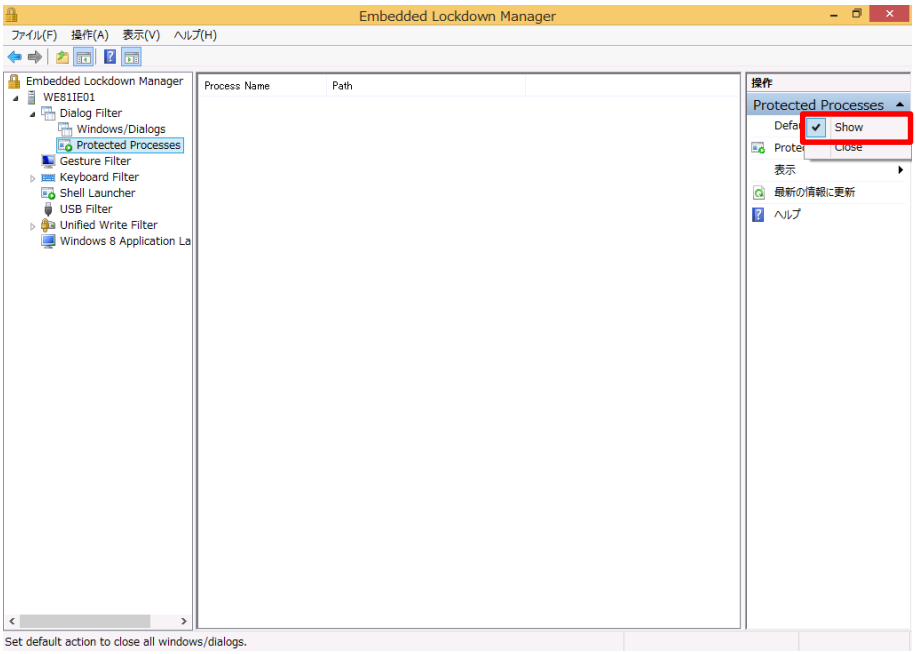
4) Admin ユーザーで、サインインします。



5) 通常のデスクトップ画面が表示されることを確認します。[A14][A15][A16][A17]



【Note:】
ダイアログ フィルターを有効にしている場合、スタート ボタンをクリックして、スタート画面を表示させることはできません。スタート画面を表示して任意のアプリケーションを実行できるようにするには、ダイアログ フィルターの [Default Action] - [Show] になるように再設定してください。尚、[Default Action] - [Show] の設定は次回サインインした際に有効になります。



9 SCCM による管理

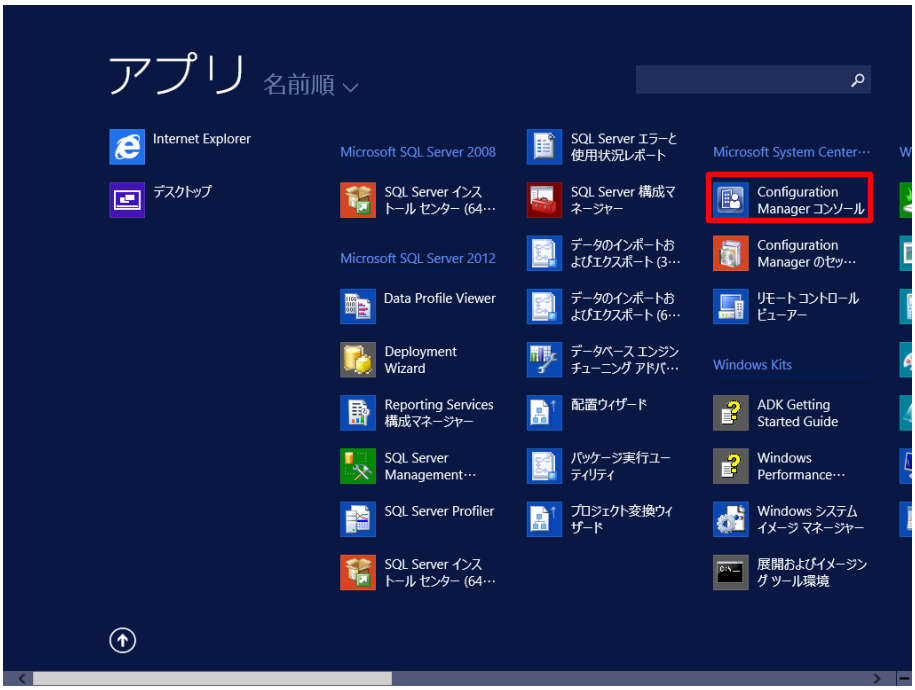
本章では、SCCM クライアントとして管理されている Windows Embedded 8.1 Industry Enterprise コンピューターを、SCCM からロックダウン管理する方法について説明します。
SCCM による管理機能のひとつには、インベントリによる書き込みフィルターの実装状況を確認する項目があります。SCCM のインベントリには、各クライアントのフィルター適用状況を一括で確認できるメリットがあります。
もうひとつの SCCM の管理機能は、ロックダウン設定をキャビネットファイル (.cab) に集約し、SCCM のコンプライアンス設定 (構成項目/構成基準) として配布できることが挙げられます。ロックダウン設定はあらかじめ Lockdown Baseline Tool (LabBaselineGenerator.exe) を利用して現在の設定をキャビネットファイルにエクスポートしてから、SCCM にインポートして利用します。

9.1 インベントリによるロックダウン状況の取得

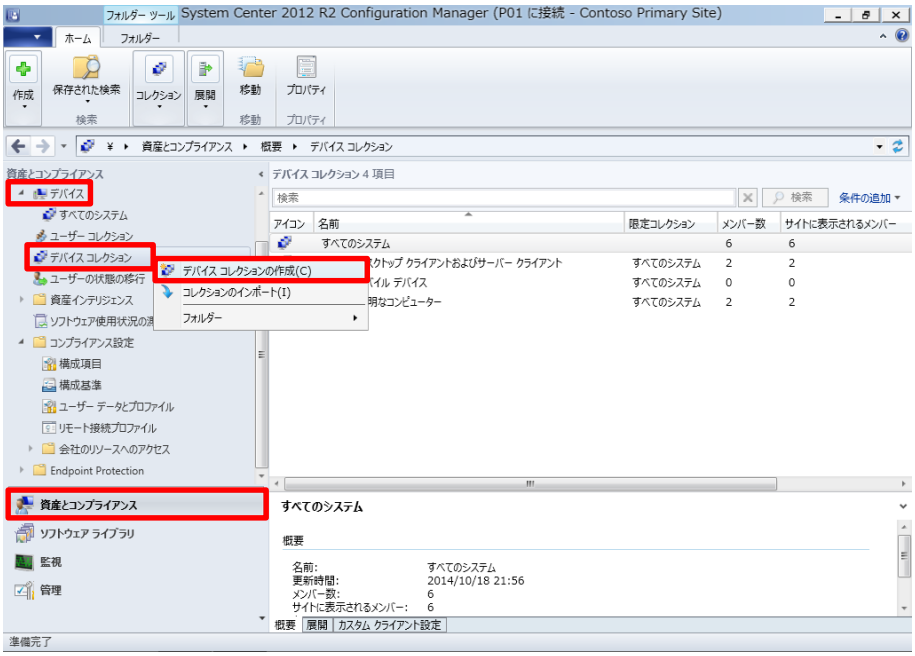
SCCM が収集したインベントリから、Windows Embedded 8.1 Industry Enterprise コンピューターの書き込みフィルターが実装されているか確認することができます。本節では、書き込みフィルターが実装されているデバイスを含むデバイス コレクションの作成方法を通じて、具体的な確認方法を解説します。

1) SCCM サイト サーバー (ws2012-cm01 コンピューター)
に、"CONTOSO¥Administrator" でサインインします。

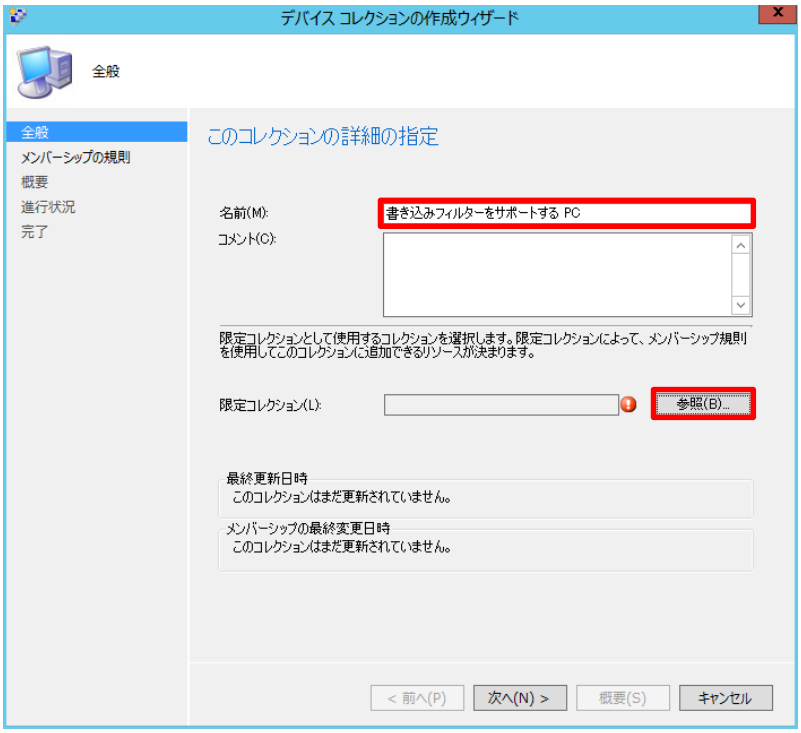
2) スタートメニューから下矢印をクリックし、[Configuration Manager コンソール] を起動します。



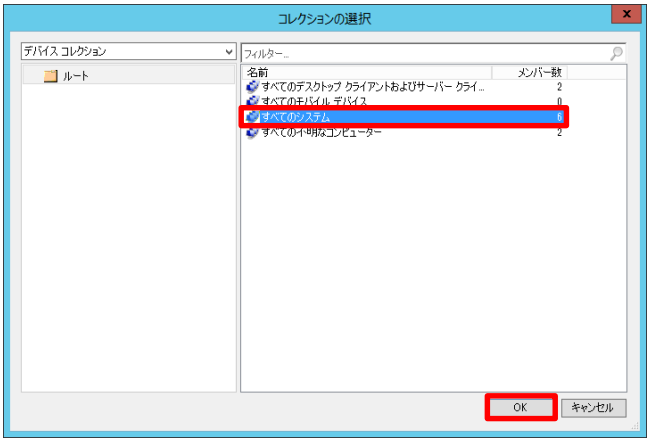
3) [Configuration Manager コンソール] 画面で [資産とコンプライアンス] をクリックし、[デバイス] - [デバイス コレクション] を右クリックして、[デバイス コレクションの作成] をクリックします。



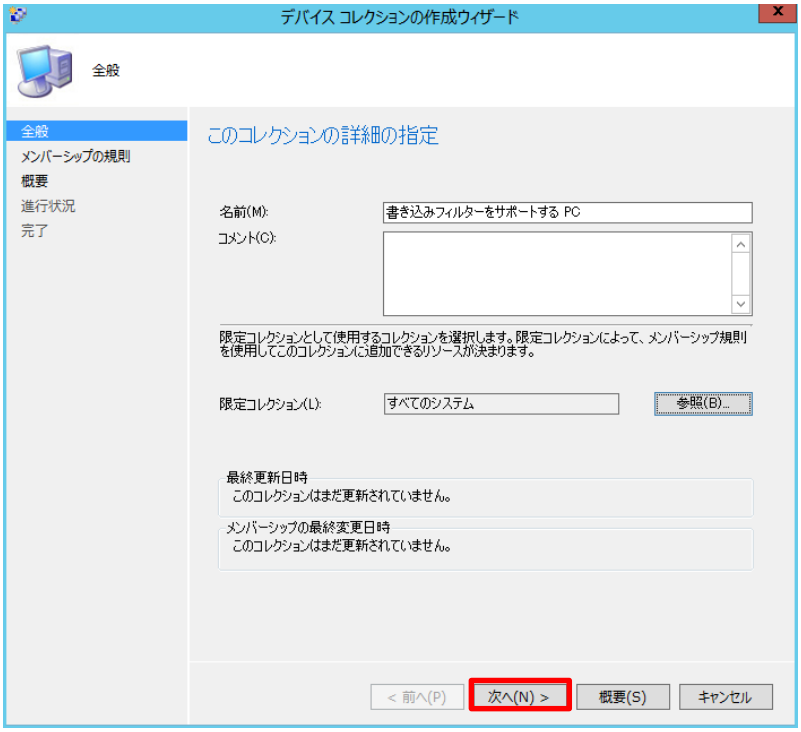
4) [デバイス コレクションの作成ウィザード] の [全般] 画面で、[名前] に「書き込みフィルターをサポートするPC」と入力します。[限定コレクション] の [参照] をクリックします。



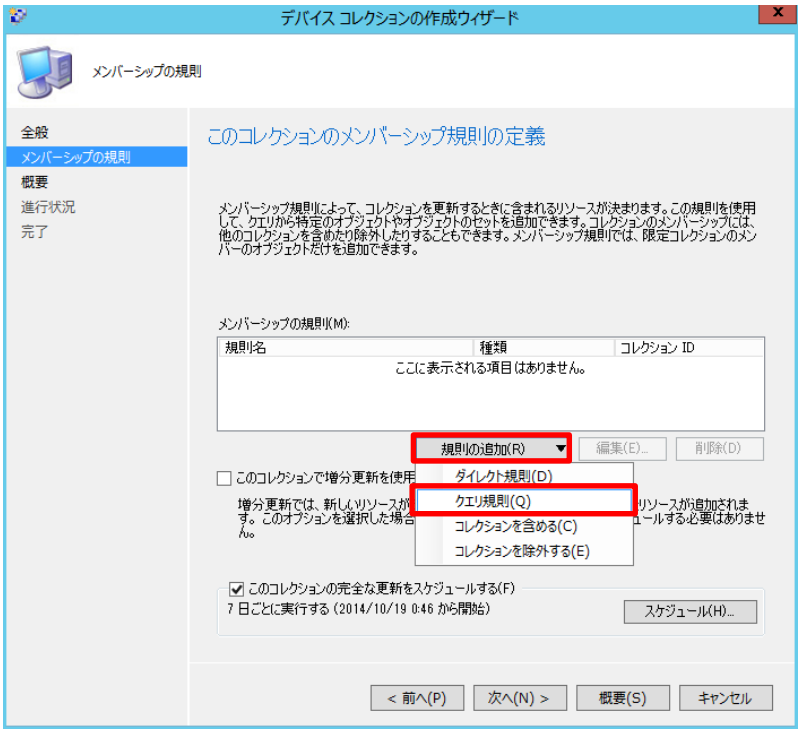
5) [コレクションの選択] 画面で、[すべてのシステム] を選択し、[OK] をクリックします。



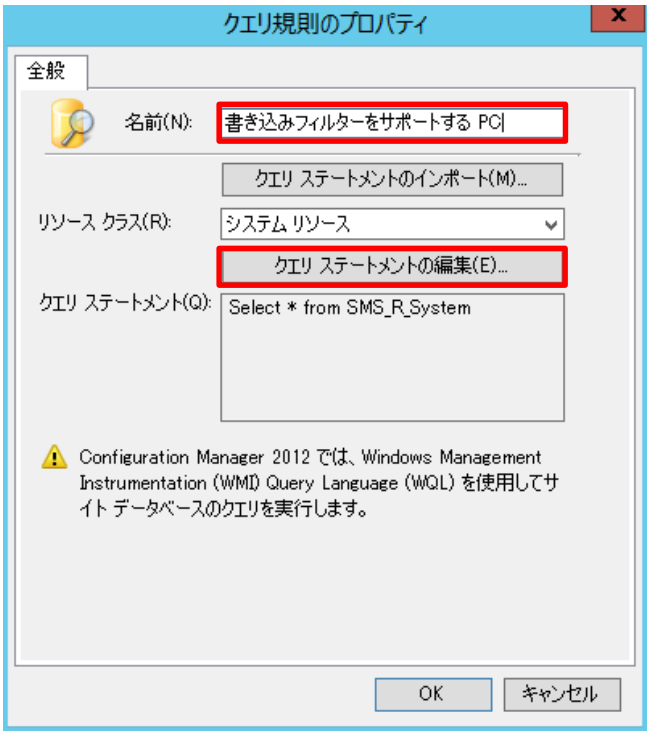
6) [デバイス コレクションの作成ウィザード] の [全般] 画面で、[次へ] をクリックします。



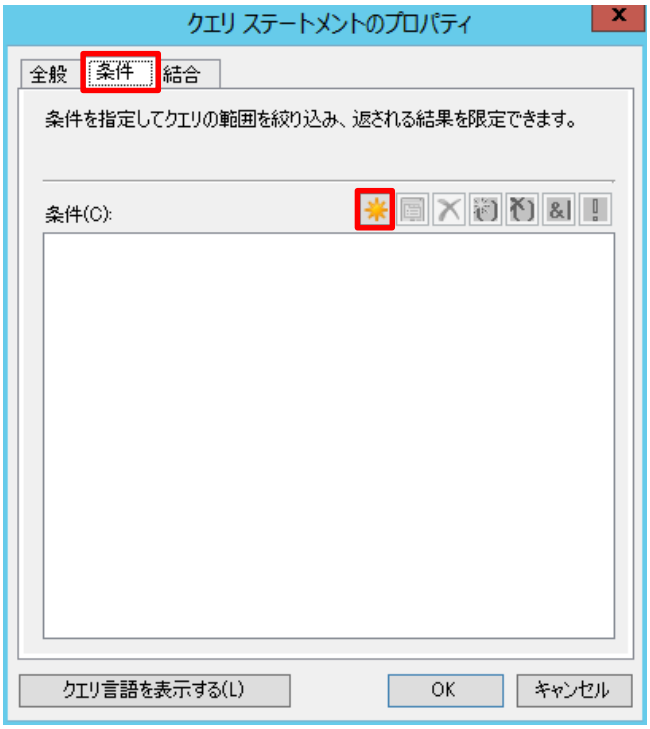
7) [デバイス コレクションの作成ウィザード] の [メンバーシップの規則] 画面で、[規則の追加] プルダウンメニューより [クエリ規則] を選択します。



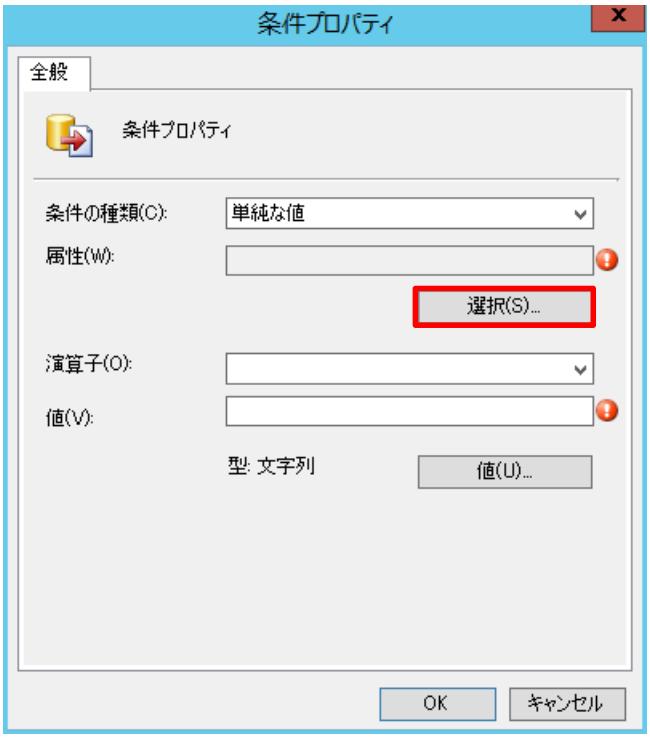
8) [クエリ規則のプロパティ] 画面で、[名前] に「書き込みフィルターをサポートする PC」と入力し、[クエリ ステートメントの編集] をクリックします。



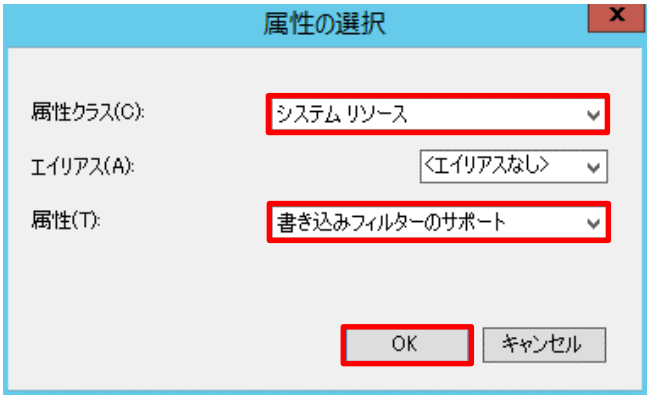
9) [クエリ ステートメントのプロパティ] 画面で、[条件] タブをクリックし、[新規] ボタンをクリックします。



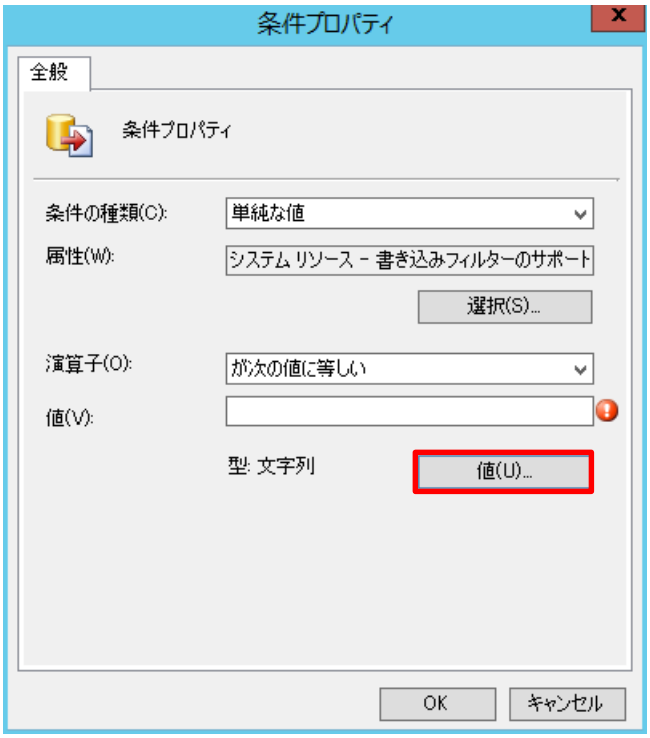
10) [条件プロパティ] 画面で、[選択] をクリックします。



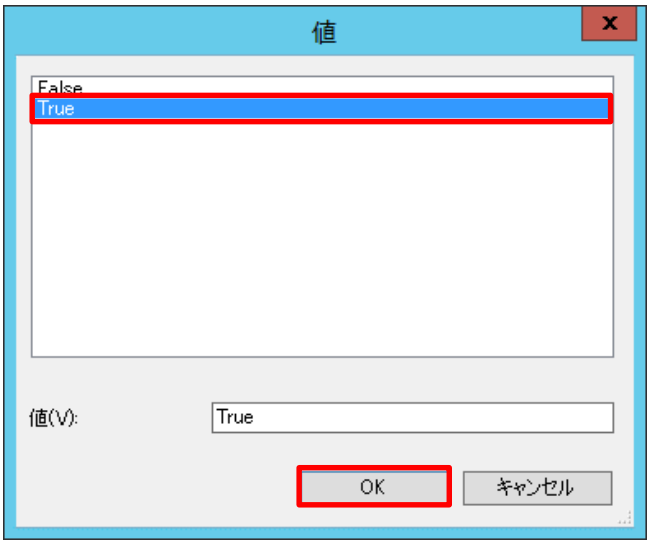
11) [属性の選択] 画面で、[属性クラス] に [システムリソース]、[属性] に [書き込みフィルターのサポート] をそれぞれプルダウンメニューから選択し、[OK] をクリックします。



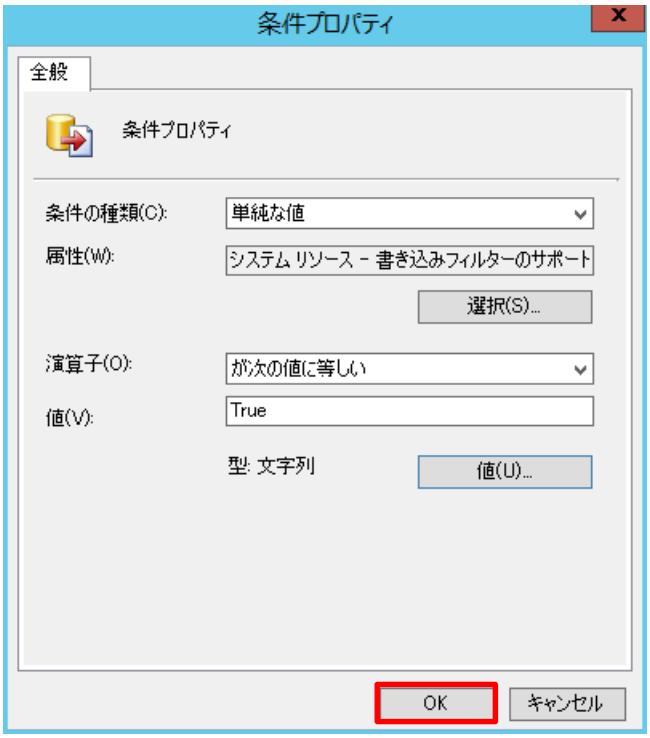
12) [条件プロパティ] 画面で、[値] をクリックします。



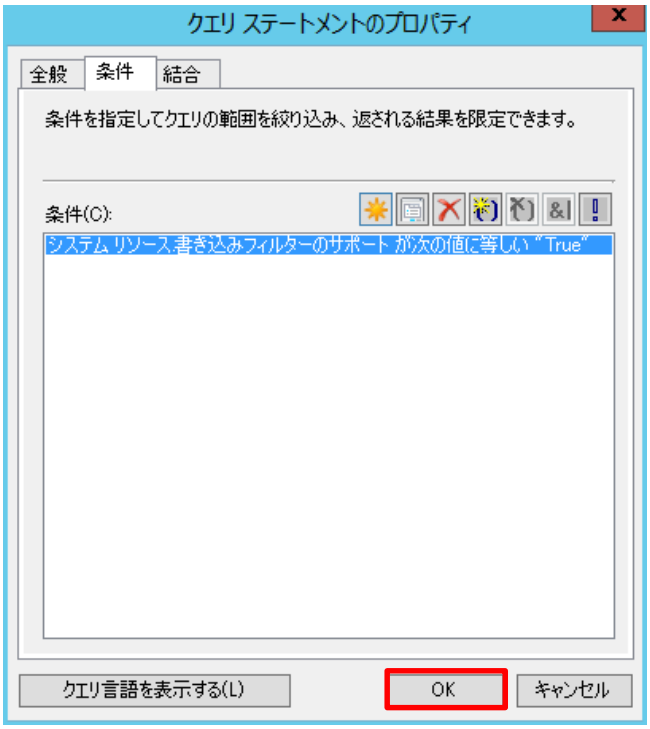
13) [値] 画面で、[True] を選択し [OK] をクリックします。



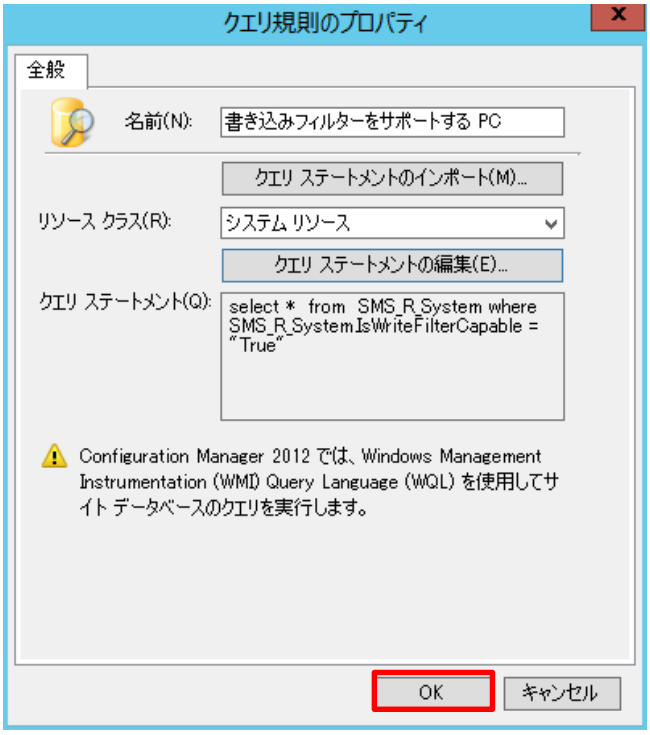
14) [条件プロパティ] 画面で、[OK] をクリックします。



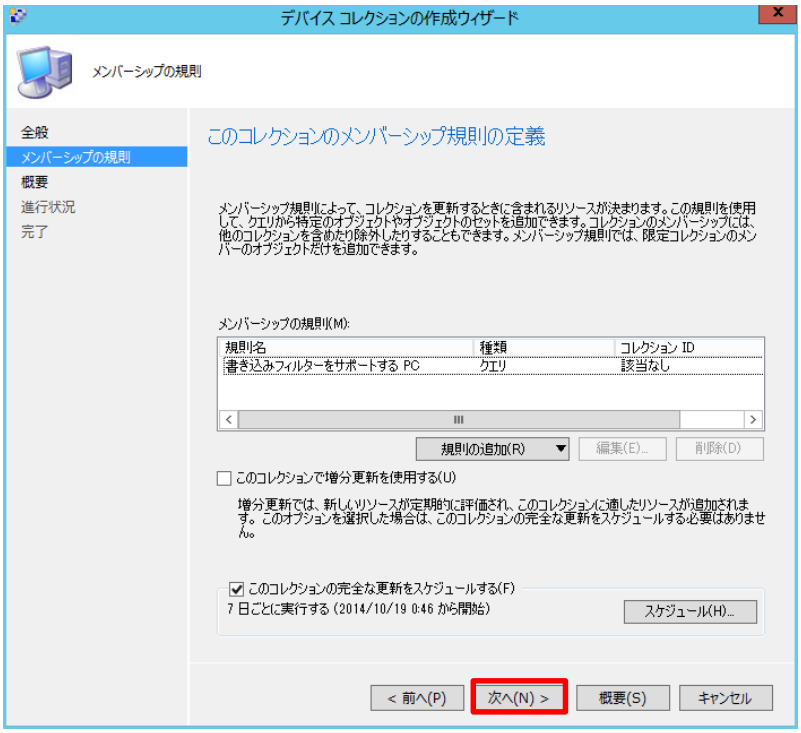
15) [クエリ ステートメントのプロパティ] 画面で、[OK] をクリックします。



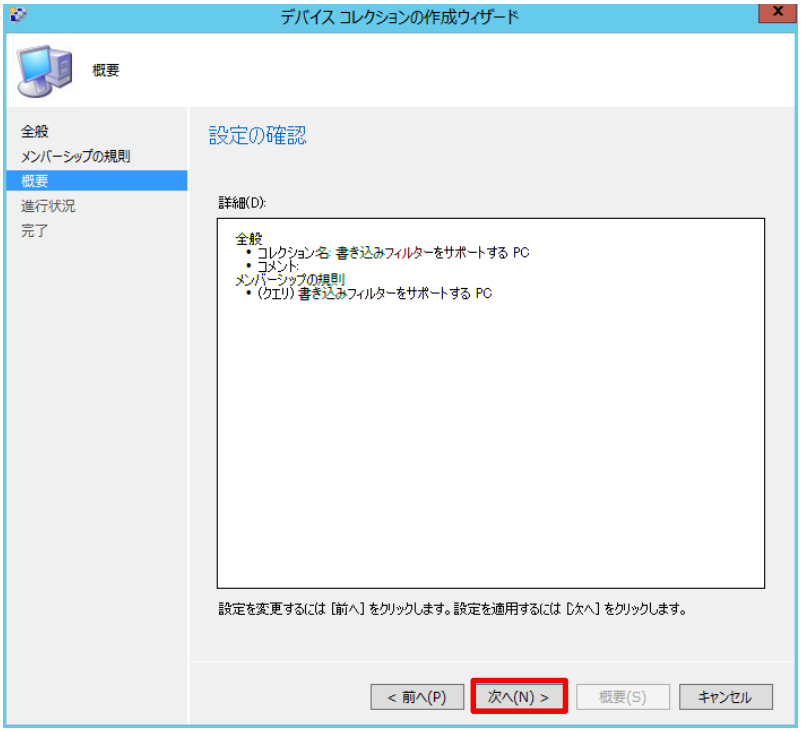
16) [クエリ規則のプロパティ] 画面で、[OK] をクリックします。



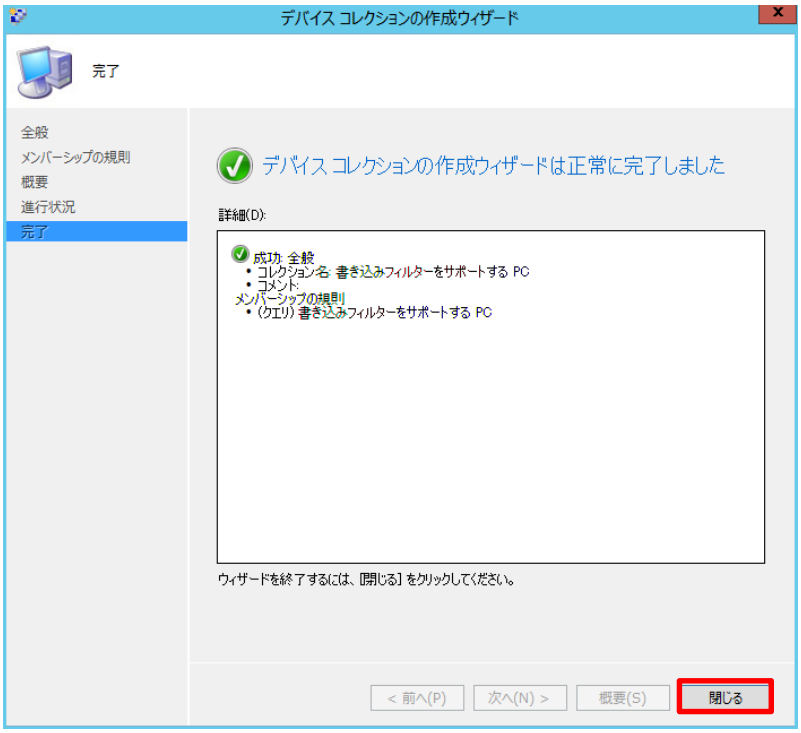
17) [デバイス コレクションの作成ウィザード] の [メンバーシップの規則] 画面で、[次へ] をクリックします。



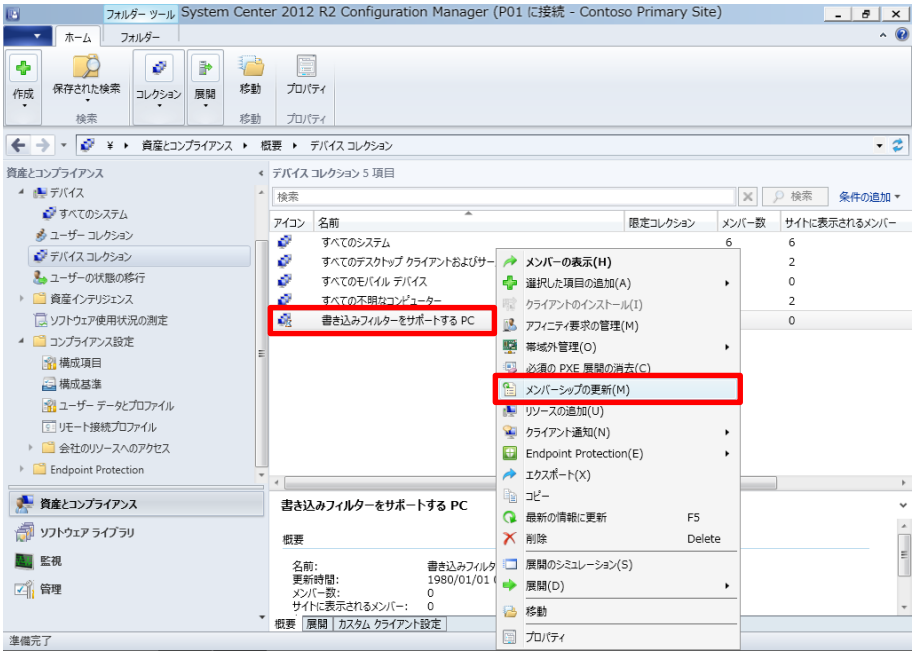
18) [デバイス コレクションの作成ウィザード] の [概要] 画面で、[次へ] をクリックします。



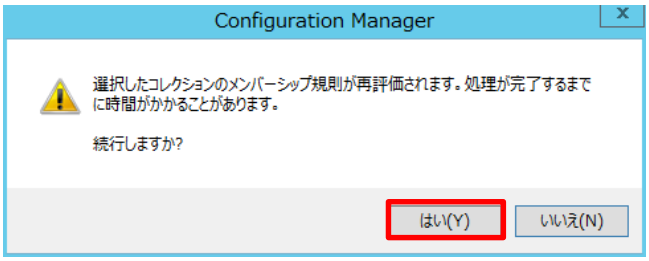
19) [デバイス コレクションの作成ウィザード] の [完了] 画面で、[閉じる] をクリックします。



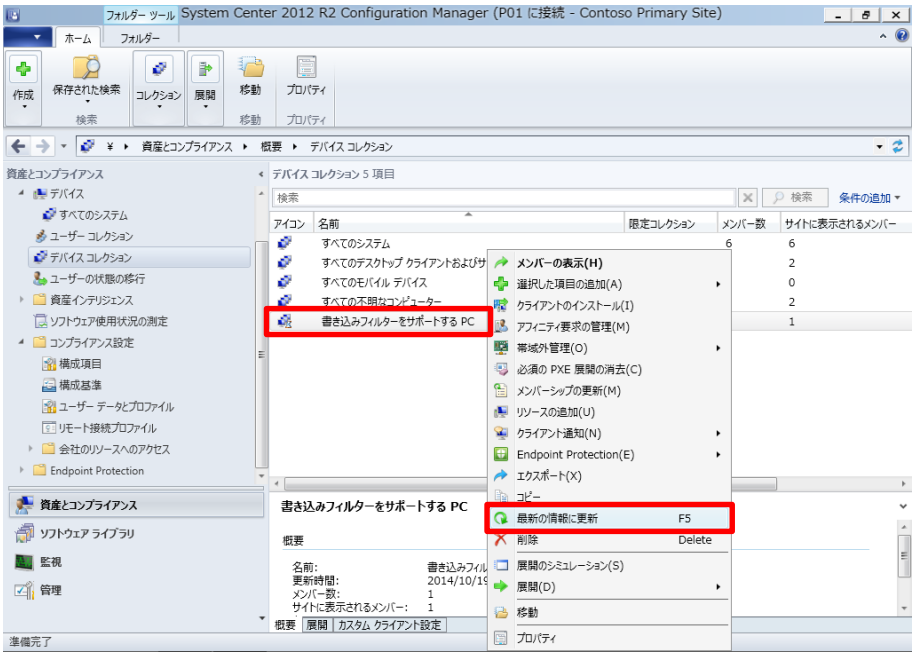
20) [Configuration Maneger] 画面で、中央ペインに作成したデバイス コレクション [書き込みフィルターをサポートする PC] が表示されます。[書き込みフィルターをサポートする PC] を右クリックし、[メンバーシップの更新] をクリックします。



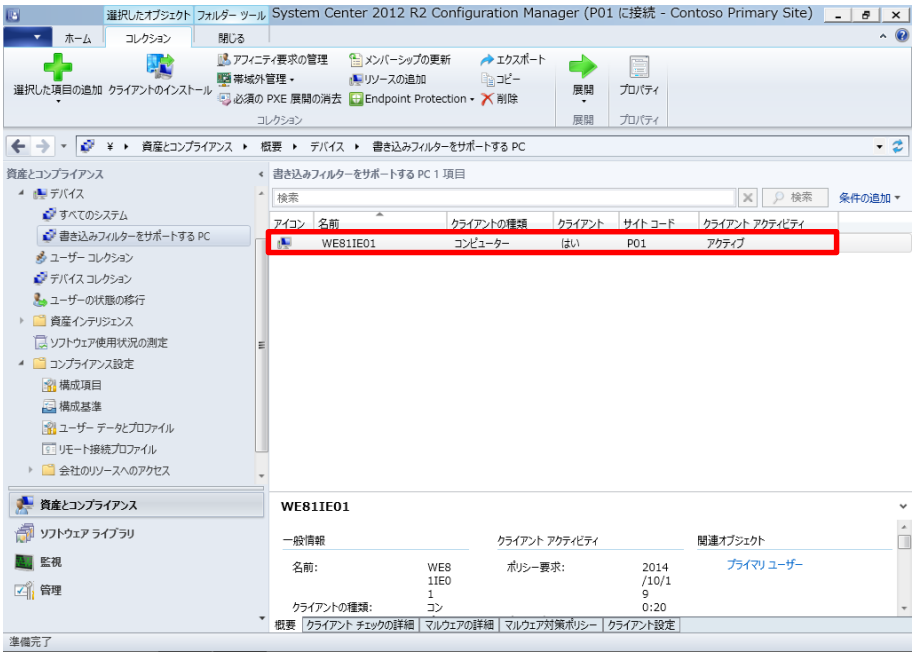
21) [Configuration Maneger] 画面で、[はい] をクリックします。



22) [Configuration Maneger] 画面で、中央ペインの [書き込みフィルターをサポートする PC] を右クリックし、[最新の情報に更新] をクリックします。



23) [Configuration Maneger] 画面で、中央ペインの [書き込みフィルターをサポートする PC] をダブルクリックします。書き込みフィルターをサポートする PC の一覧を確認することができます。



9.2 コンプライアンス設定によるフィルター設定の同時配布

Embedded Lockdown Manager で行ったフィルター設定は、構成データとしてエクスポートすることで、SCCM のコンプライアンス設定として SCCM クライアントである Widnows Embedded 8.1 Industry Enterprise コンピューターに配布することができます。本節では、フィルター設定のエクスポート手順とインポート手順、SCCM クライアントへの展開手順について、それぞれ確認します。

9.2.1 書き込みフィルターの例外設定

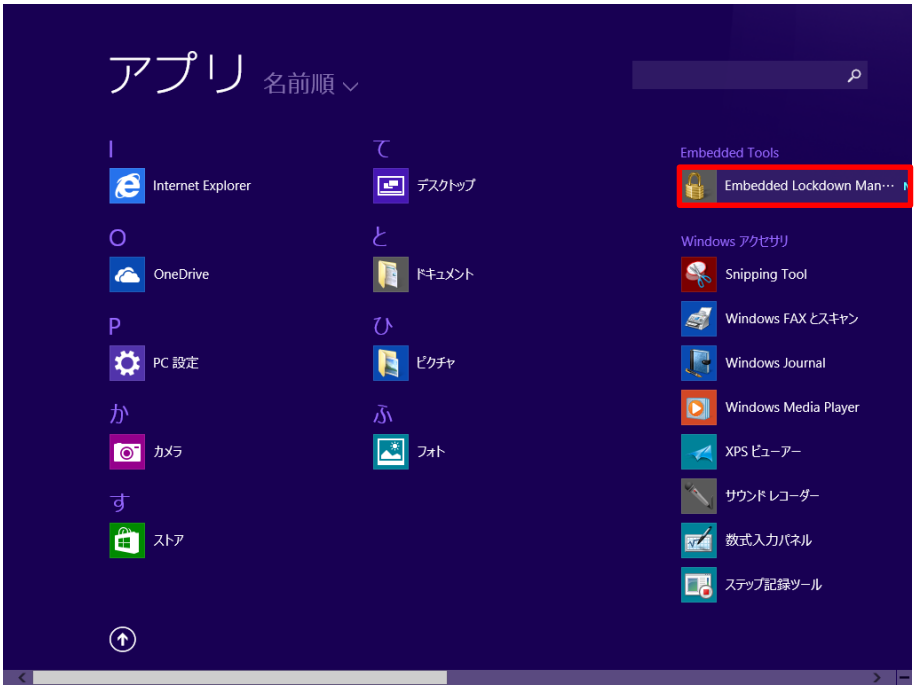
SCCM クライアントに対して書き込みフィルターを設定する場合、Embedded Lockdown Manager で SCCM クライアントに対する書き込みフィルターの例外を設定します。これにより、書き込みフィルターを適用した PC 上で SCCM クライアントが共存できるようになります。

【Note:】
この書き込みフィルターの例外設定を行う場合、設定を行うコンピューターで書き込みフィルターが既に有効になっている必要があります。書き込みフィルターの有効化手順については、4.3 節を参照してください。

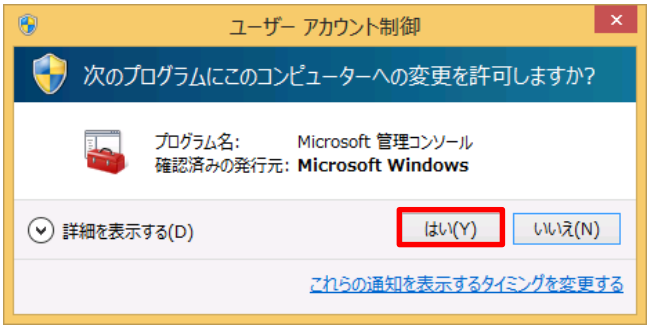
1) WE81IE01 に、"CONTOSO¥Administrator" でサインインします。

2) スタート画面を開き、 ↓ をクリックします。

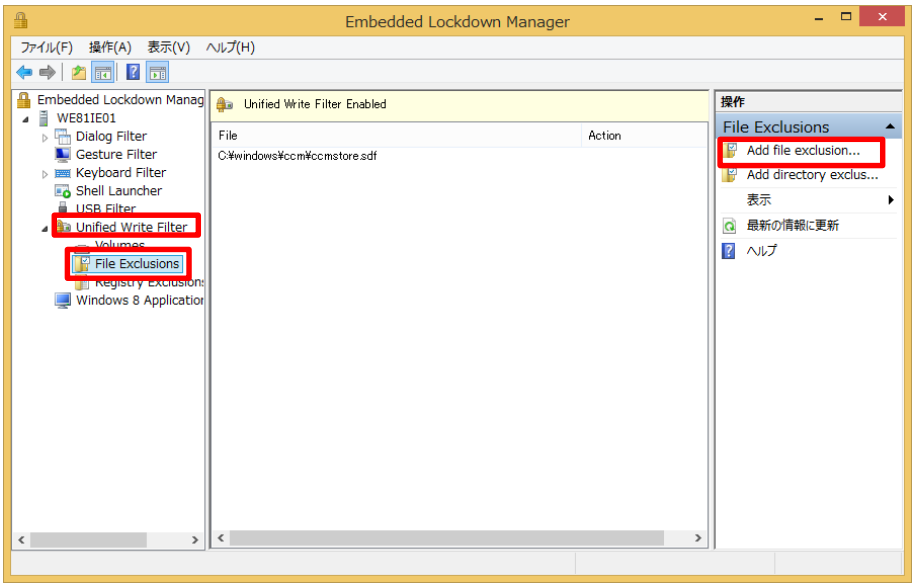
3) スタート画面で、[Embedded Lockdown Manager] をクリックします。



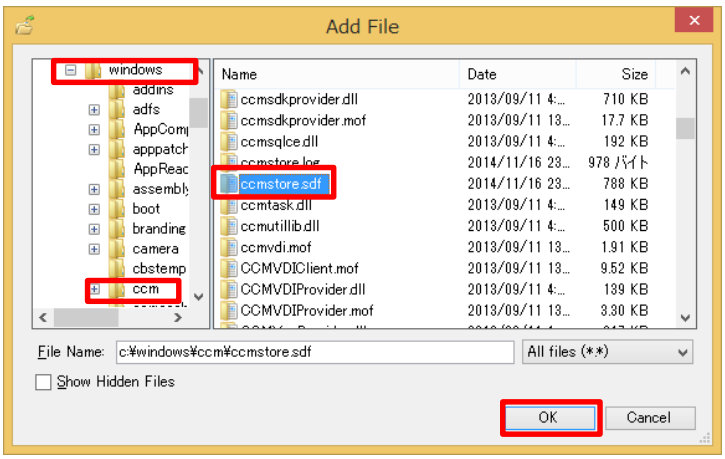
4) [ユーザー アカウント制御] 画面で、[はい] をクリックします。



5) [Embedded Lockdown Maneger] 画面で、左ペインの [Unified Write Filter] - [File Exclusions] の順に展開し、右ペインの [Add file exclusions] をクリックします。



6) [Add File] 画面で、左ペインの [Local Disk (C:)] - [windows] - [ccm] をクリックして展開し、右ペインの [ccmstore.sdf] をクリックして、[OK] をクリックします。



7) 手順 5～6 を繰り返し、次のファイルを追加します。[A18][A19]

【SCCM クライアントのための例外設定】

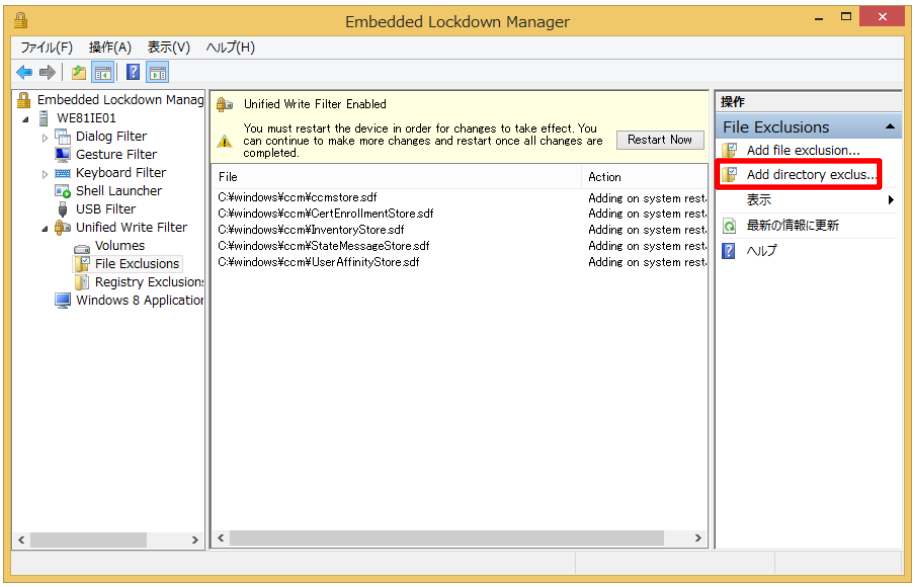
・C:¥windows¥ccm¥certenrollmentstore.sdf

・C:¥windows¥ccm¥inventorystore.sdf

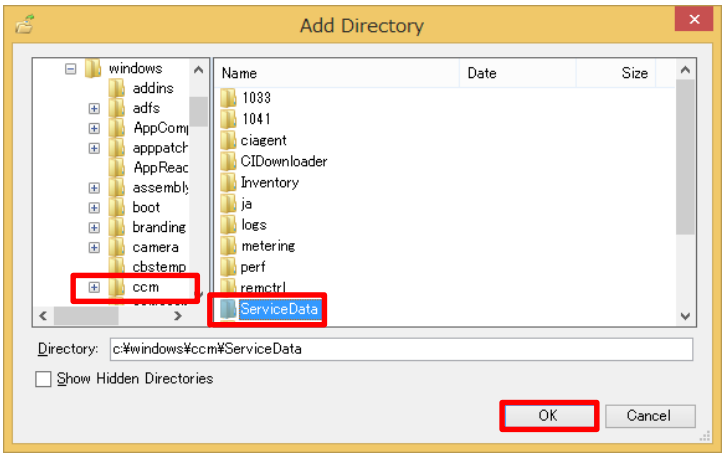
・C:¥windows¥ccm¥statemessagestore.sdf

・C:¥windows¥ccm¥useraffinitystore.sdf

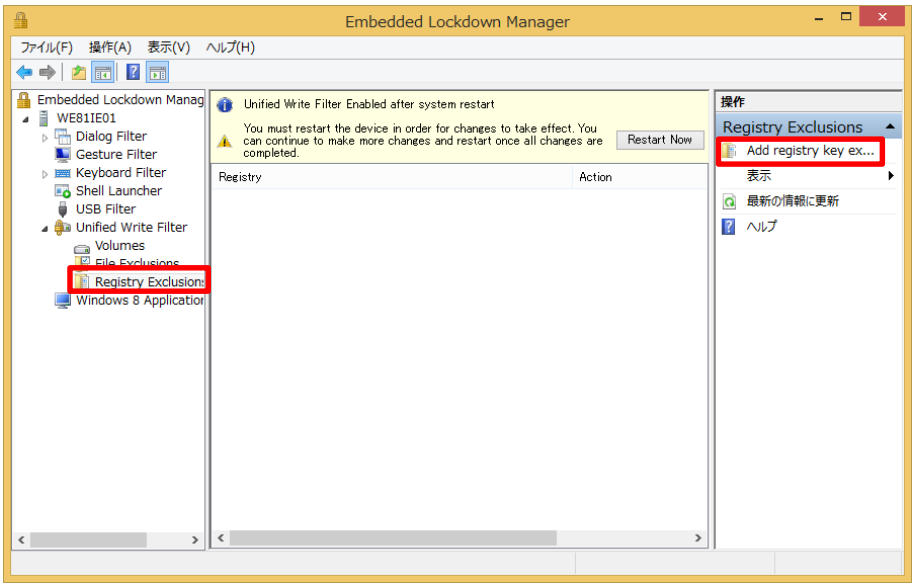
8) [Embedded Lockdown Maneger] 画面で、右ペインの [Add directory exclusions] をクリックします。



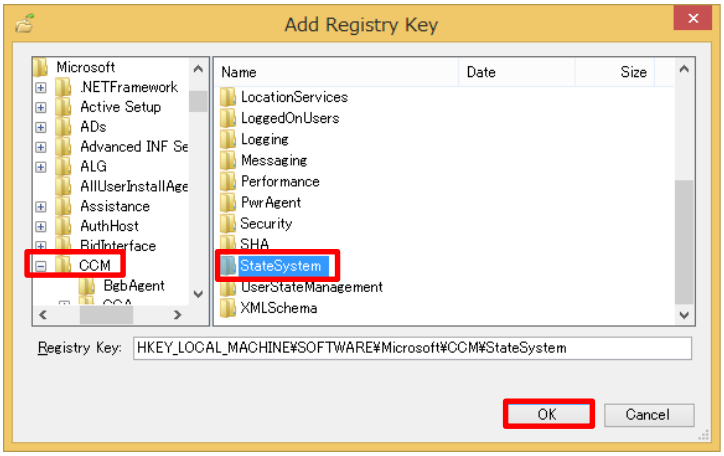
9) [Add Directory] 画面で、左ペインの [Local Disk (C:)] - [windows] - [ccm] をクリックして展開し、右ペインの [ServiceData] をクリックして、[OK] をクリックします。



10) [Embedded Lockdown Maneger] 画面で、左ペインの [Registry Exclusions] をクリックし、右ペインの [Add registry key exclusions] をクリックします。



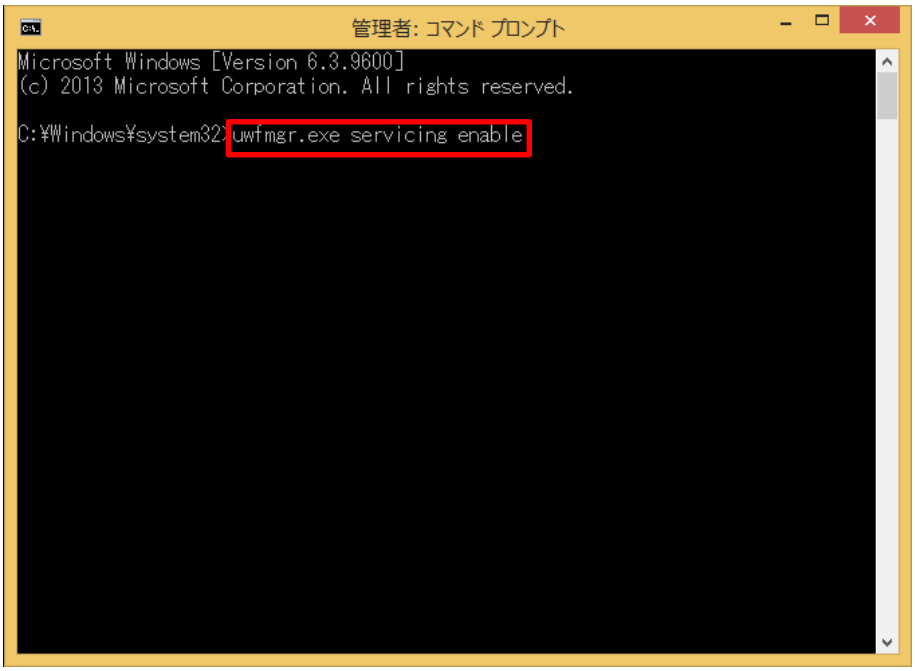
11) [Add Registry Key] 画面で、左ペインの [LOCAL] – [HKEY_LOCAL_MACHINE] - [SOFTWARE] - [Microsoft] - [CCM] をクリックして展開し、右ペインの [StateSystem] をクリックして、[OK] をクリックします。



12) デスクトップで、スタートボタンを右クリックし、[コマンド プロンプト (管理者)] をクリックします。

13) [ユーザー アカウント制御] 画面で、[はい] をクリックします。

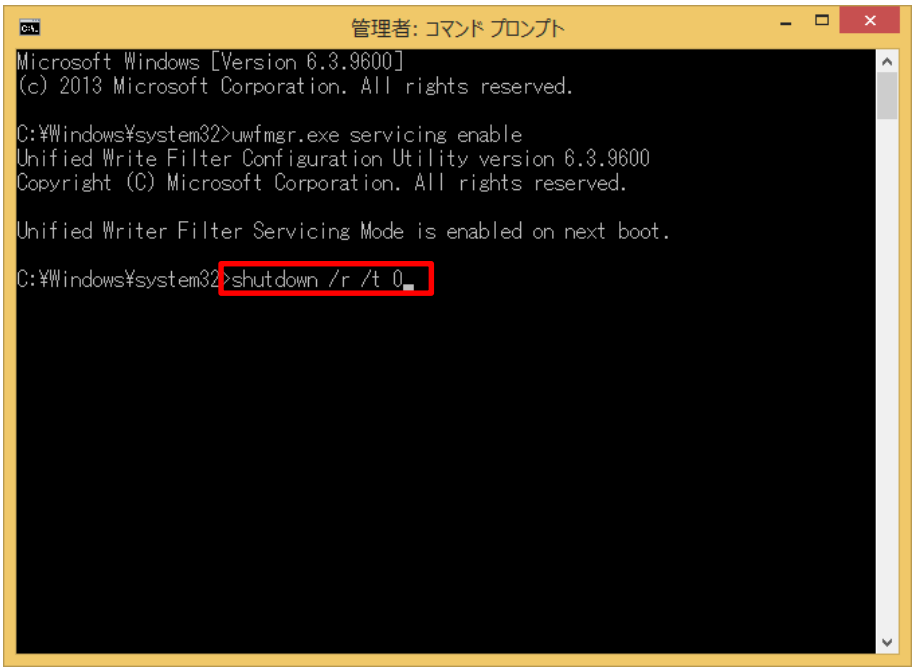
14) [管理者：コマンドプロンプト] 画面で、「uwfmgr.exe servicing enable」と入力し、Enter キーを押します。



【Note:】

「uwfmgr.exe servicing enable」コマンドの実行によって Device Servicing 設定が有効になり、書き込みフィルターが設定されたコンピューターで Windows Update が利用できるようになります。

15) [管理者:コマンドプロンプト] 画面で、「shutdown /r /t 0」と入力し、Enter キーを押して、コンピューターを再起動します。



【Note:】[A20]

Windows Update 以外にも、ファイル、フォルダーおよびレジストリの例外設定により、System Center Endopoint Protection 定義ファイルの適用や、Windows Defender 定義ファイルが適用されるよう構成できます。設定に関する詳細は下記サイトを参考にしてください。

■ Antimalware support on UWF-protected devices

http://msdn.microsoft.com/en-us/library/dn449271(v=winembedded.82).aspx

9.2.2 フィルター設定のエクスポート

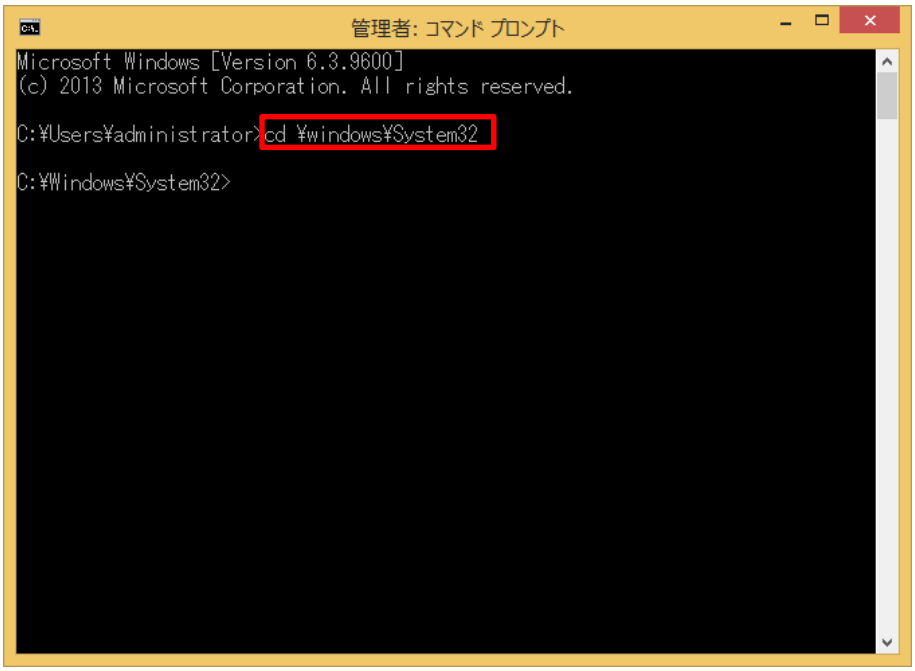
Embedded Lockdown Manager で行ったフィルター設定をエクスポートする手順について確認します。

1) WE81IE01 に、"CONTOSO¥Administrator" でサインインします。

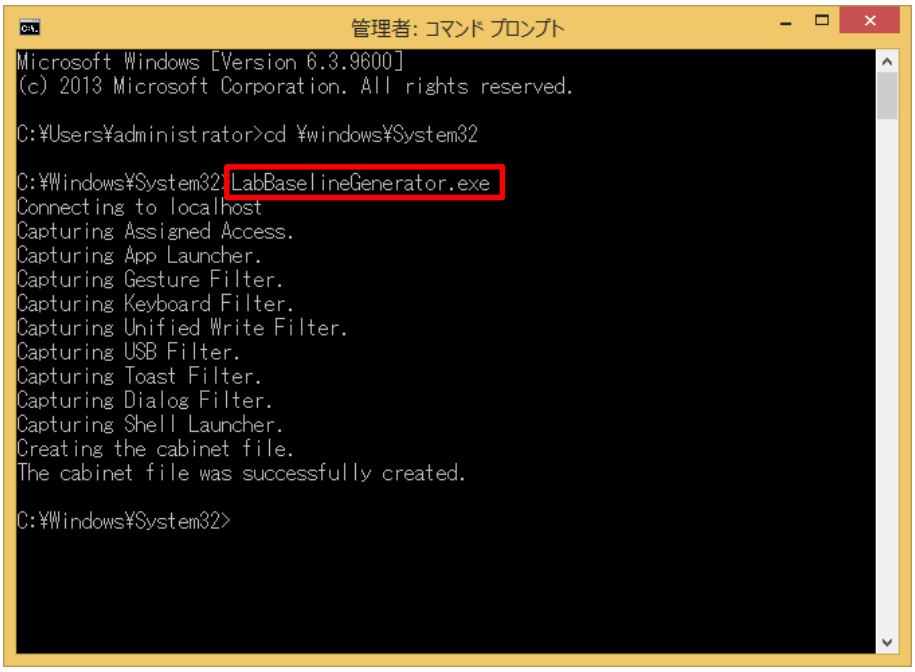
2) デスクトップで、スタートボタンを右クリックし、[コマンド プロンプト (管理者)] をクリックします。

3) [ユーザー アカウント制御] 画面で、[はい] をクリックします。

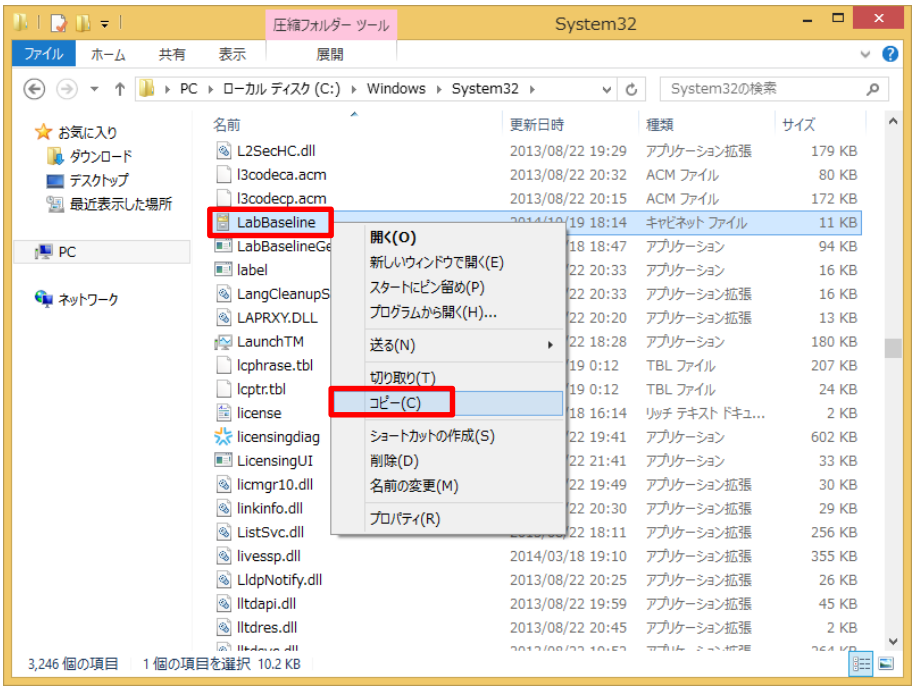
4) [管理者:コマンドプロンプト] 画面で、「cd ¥windows¥system32」と入力し、Enter キーを押します。



5) [管理者:コマンドプロンプト] 画面で、「LabBaselineGenerator.exe」と入力し、Enter キーを押します。

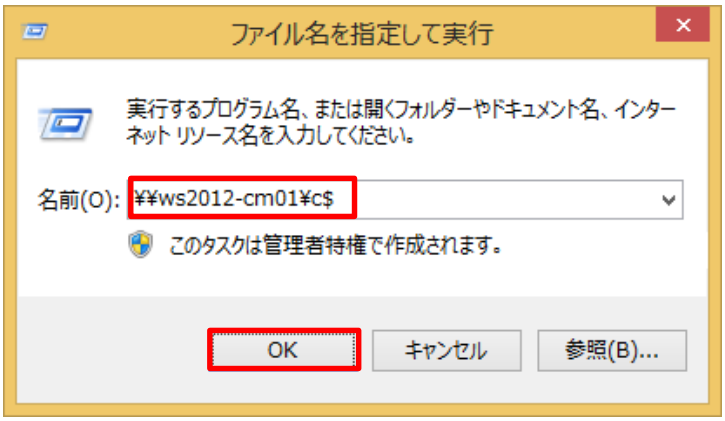


6) Windows エクスプローラーを起動し、c:¥windows¥system32 フォルダーにある LabBaseline.cab ファイルを右クリックして、[コピー] をクリックします。

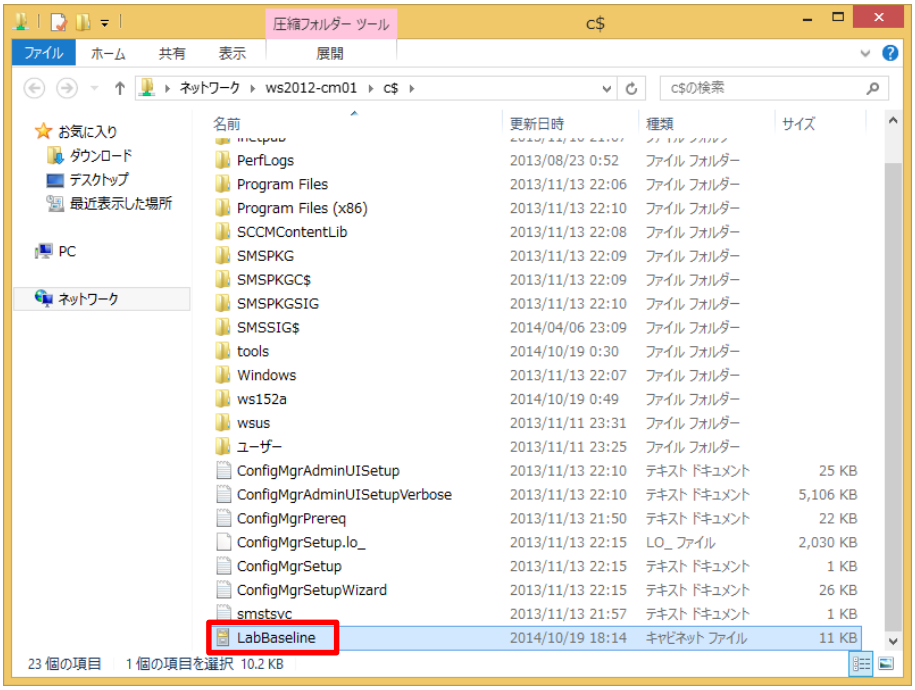


7) スタートボタンを右クリックし、[ファイル名を指定して実行] をクリックします。

8) [ファイル名を指定して実行] 画面で、SCCM サーバーにファイルをコピーするため、「¥¥ws2012-cm01¥c$」と入力し、[OK] ボタンを押します。



9) Windows エクスプローラー画面 (¥¥ws2012-cm01¥c$) が開きます。Ctrl+V キーを押して、LabBaseline.cab ファイルを貼り付けます。これにより、SCCM サーバーの C ドライブ直下にキャビネットファイルがコピーされました。

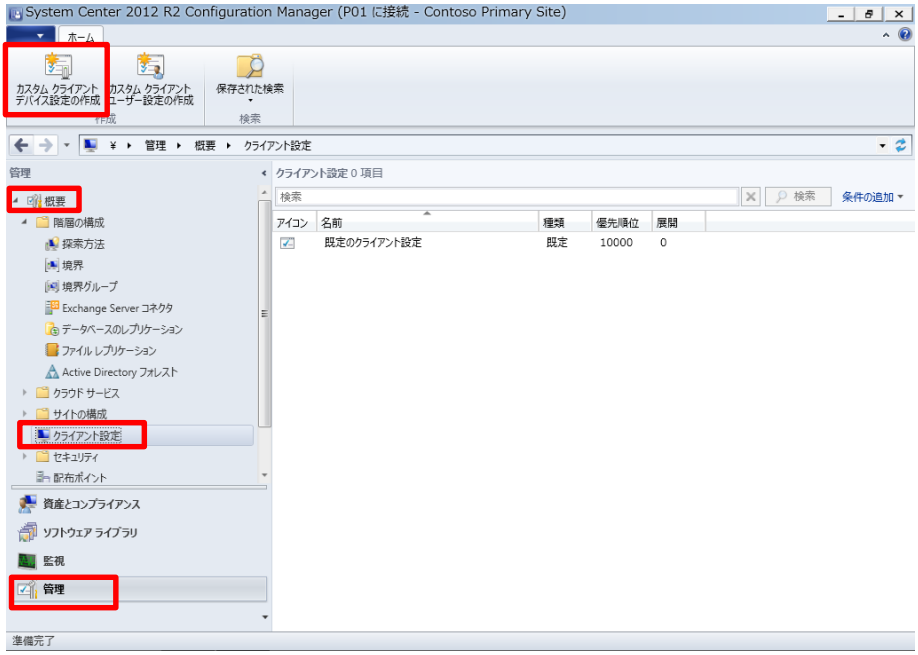


9.2.3 フィルター設定適用のための事前設定

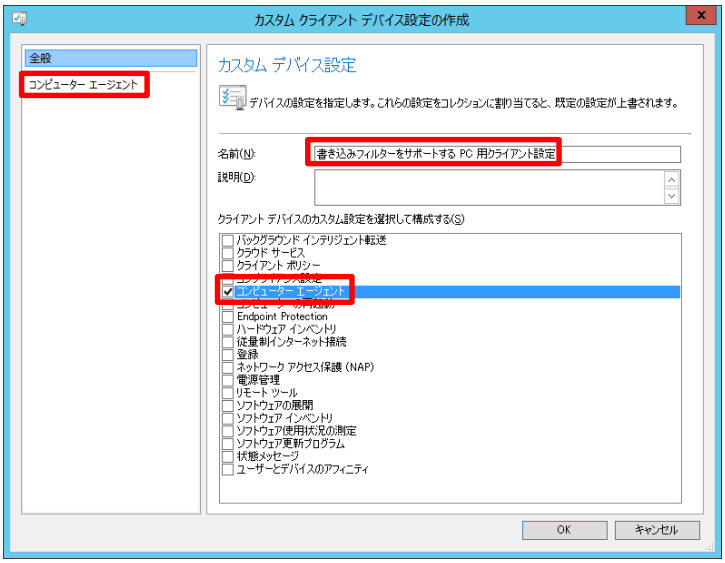
SCCM のコンプライアンス設定を使用して先ほどエクスポートしたフィルター設定を配布する場合、SCCM クライアント側でフィルター設定のスクリプトを実行できるよう、SCCM のクライアント設定を変更する必要があります。本手順では、クライアントで PowerShell スクリプトを実行できるようにクライアント設定を構成し、Windows Embedded 8.1 Industry Enterprise コンピューターを含むコレクションに適用します。

1) WS2012-CM01 に、"CONTOSO¥Administrator" でサインインします。

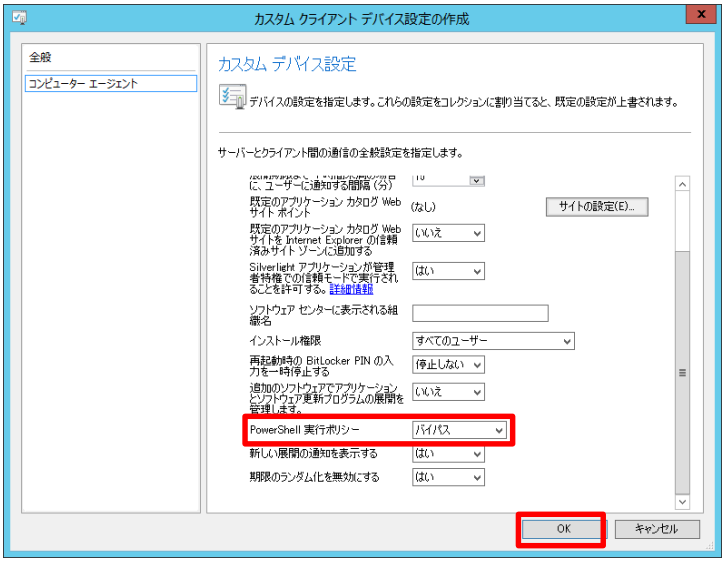
2) [Configuration Maneger] 画面で、左ペインの [管理] をクリックし、[概要] - [クライアント設定] の順に展開し、[カスタム クライアント デバイス設定の作成] をクリックします。



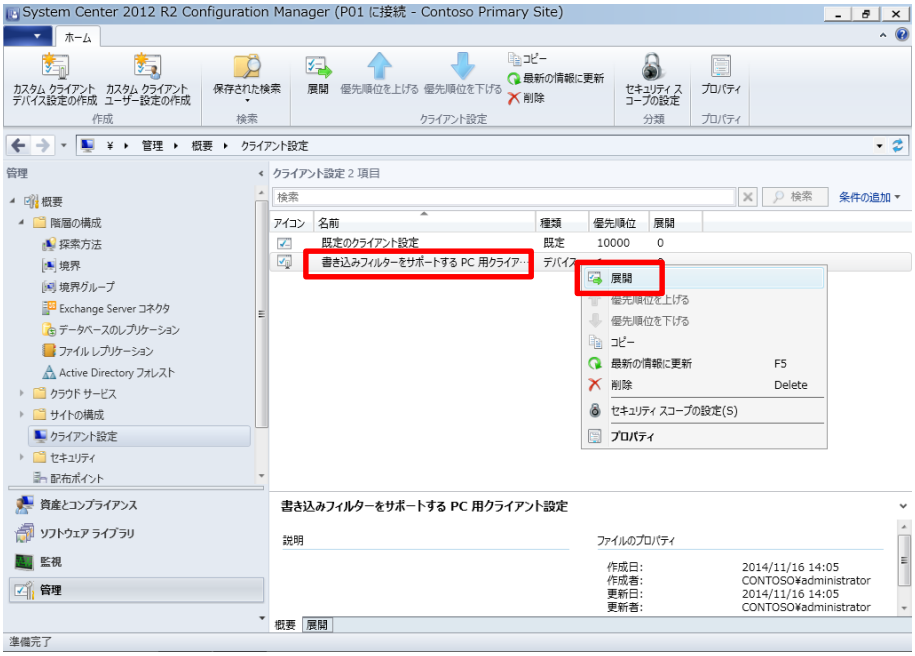
3) [カスタム クライアント デバイス設定の作成] 画面で、[名前] 欄に「書き込みフィルターをサポートする PC 用クライアント設定」と入力し、[コンピューター エージェント] にチェックをつけ[A21][A22]、左ペインの [コンピューター エージェント] をクリックします。



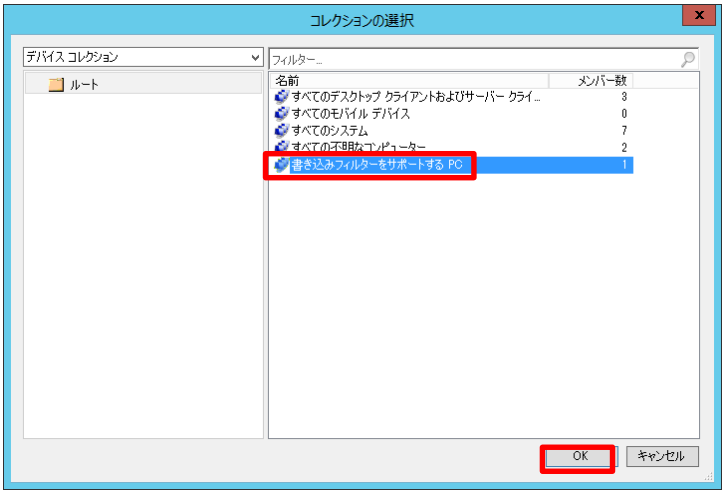
4) [カスタム クライアント デバイス設定の作成] 画面で、[PowerShell 実行ポリシー] 欄で [バイパス] を選択し、[OK] をクリックします。



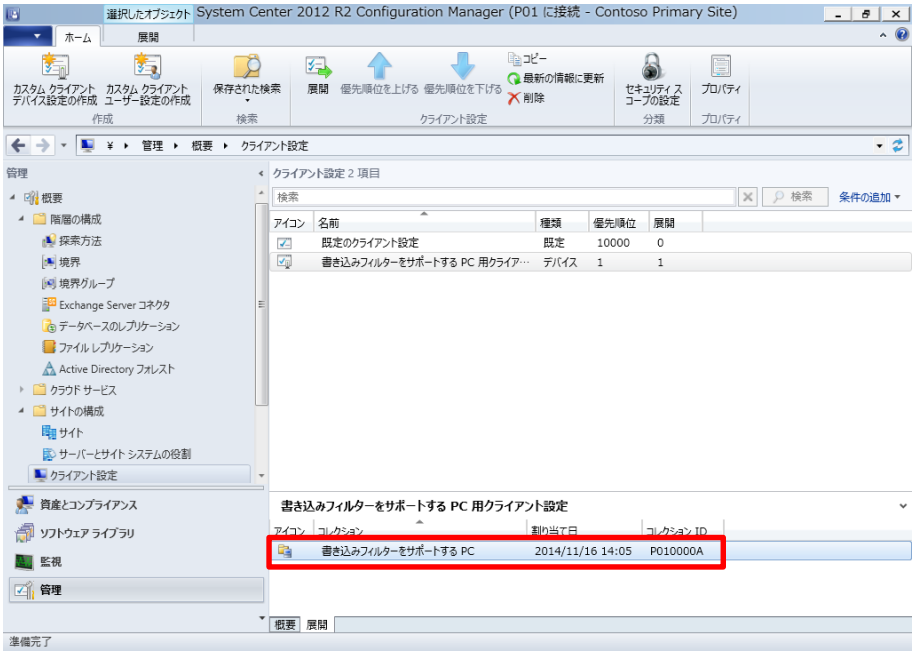
5) [Configuration Maneger] 画面で、中央ペインにある作成した [書き込みフィルターをサポートする PC 用クライアント設定] を右クリックし、[展開] をクリックします。



6) [コレクションの選択] 画面で、[書き込みフィルターをサポートする PC] を選択し、[OK] をクリックします。



7) [Configuration Maneger] 画面で、右下ペインから展開結果が確認できます。

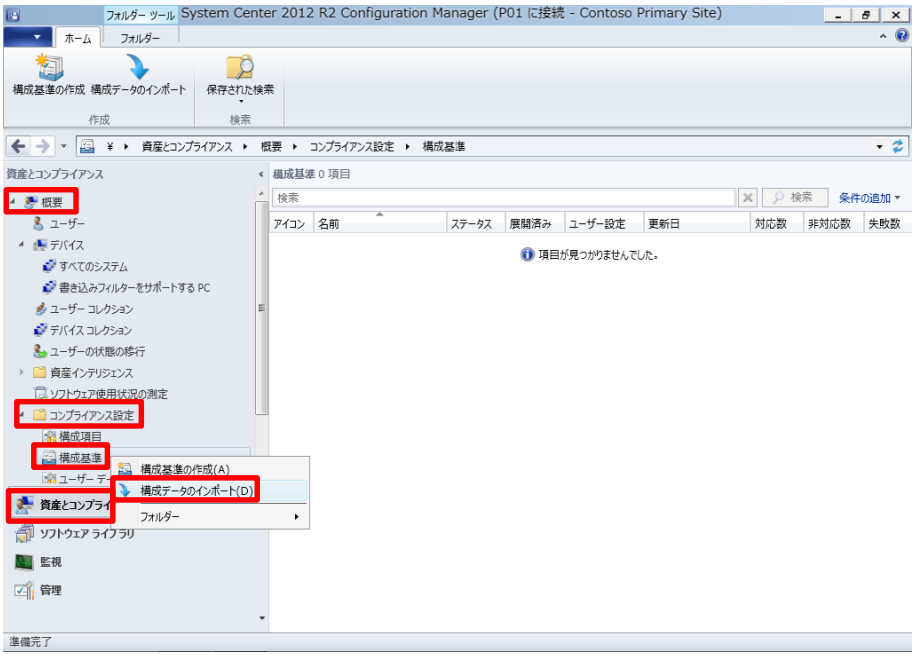


9.2.4 フィルター設定のインポートと適用

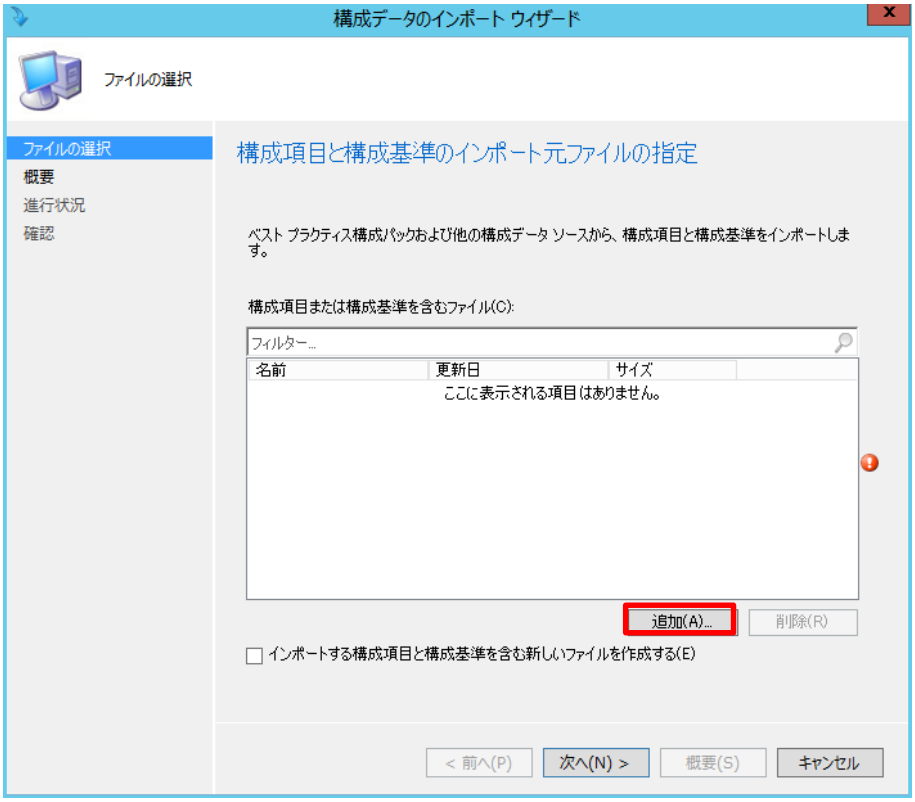
前の手順でエクスポートしたフィルター設定を SCCM の[構成基準] 設定にインポートし、SCCM クライアントに適用する手順を確認します。

1) WS2012-CM01 に、”CONTOSO¥Administrator” でサインインします。

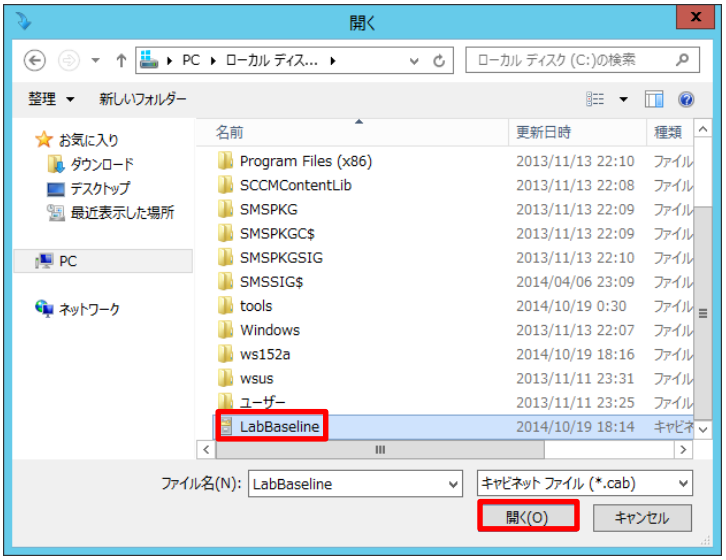
2) [Configuration Maneger] 画面で、左ペインの [資産とコンプライアンス] をクリックし、[概要] - [コンプライアンス設定] - [構成基準] の順に展開し、[構成基準] を右クリックして、[構成データのインポート] をクリックします。



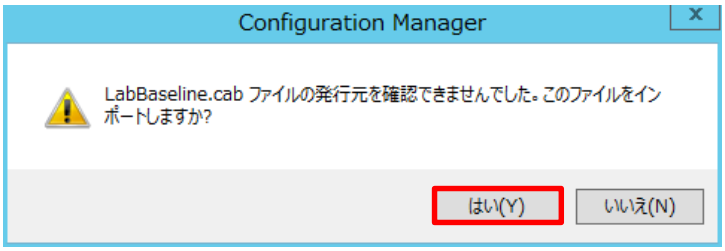
3) [構成データのインポート ウィザード] の [ファイルの選択] 画面で、[追加] をクリックします。



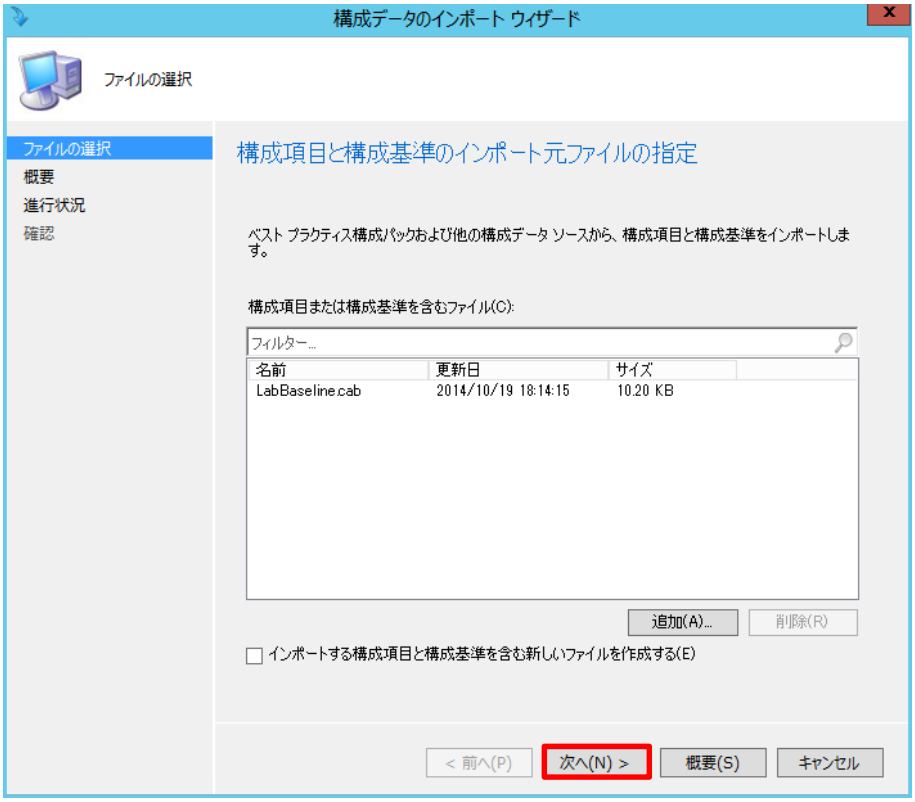
4) [開く] 画面で、c:¥LabBaseline.cab ファイルを選択し、[開く] をクリックします。



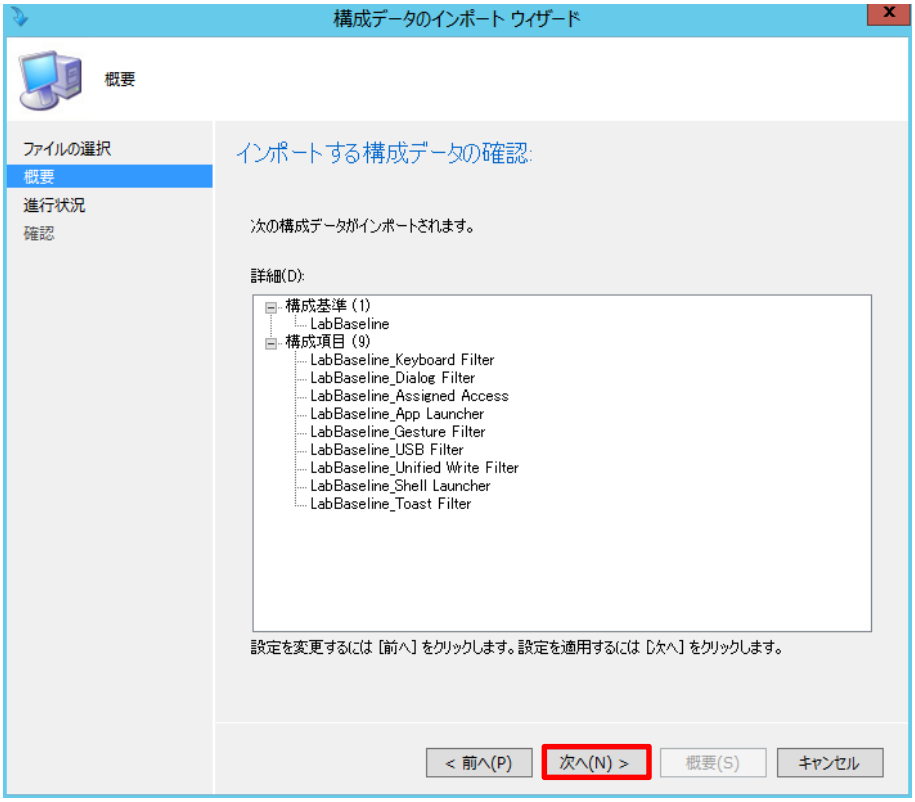
5) 警告メッセージが表示されます。[はい] をクリックします。



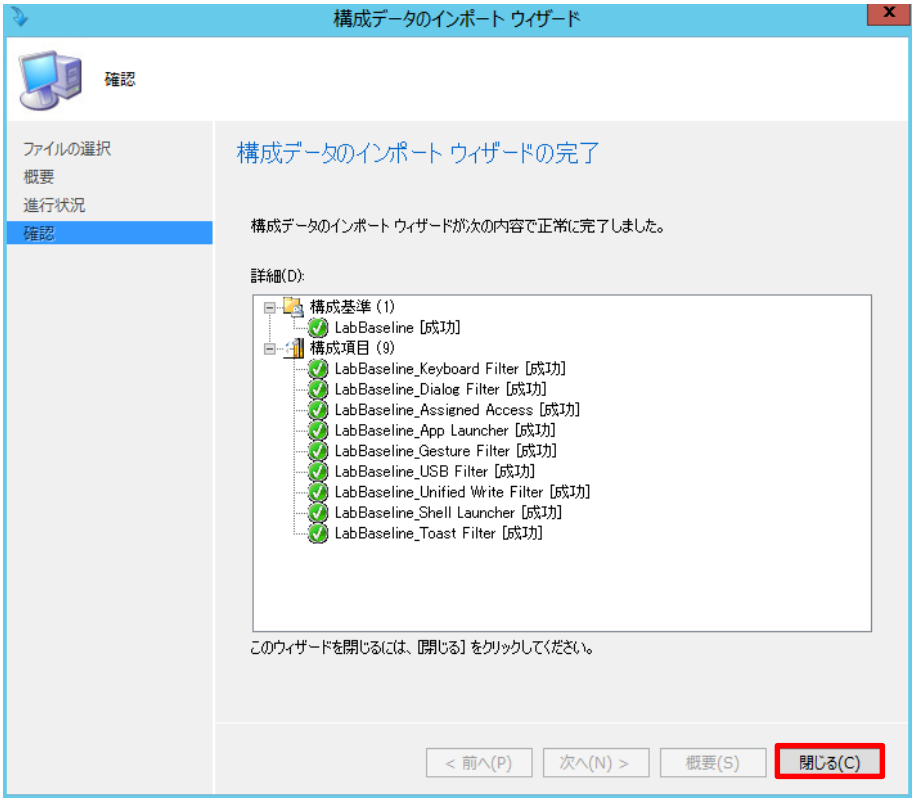
6) [構成データのインポート ウィザード] の [ファイルの選択] 画面で、[次へ] をクリックします。



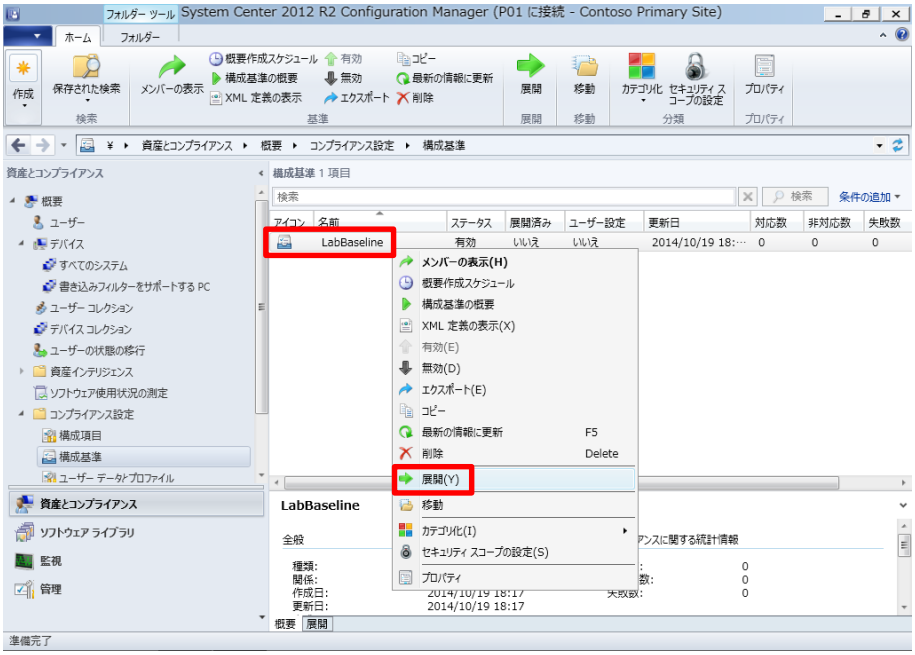
7) [構成データのインポート ウィザード] の [概要] 画面で、[次へ] をクリックします。



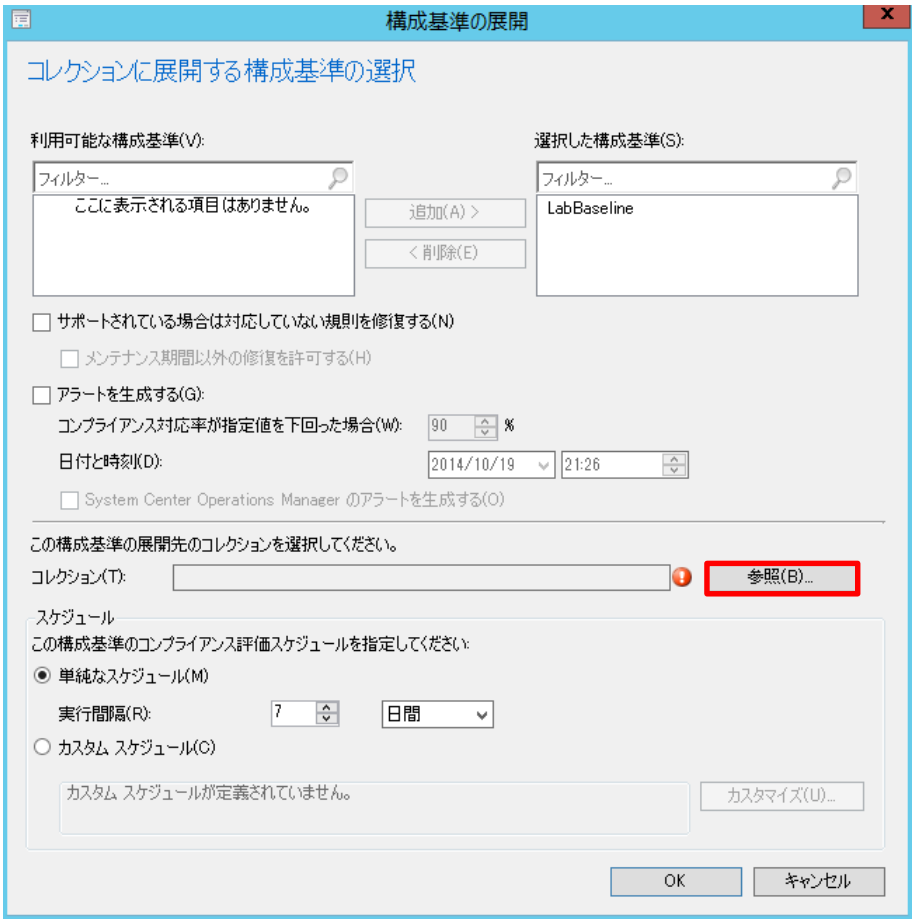
8) [構成データのインポート ウィザード] の [確認] 画面で、[閉じる] をクリックします。



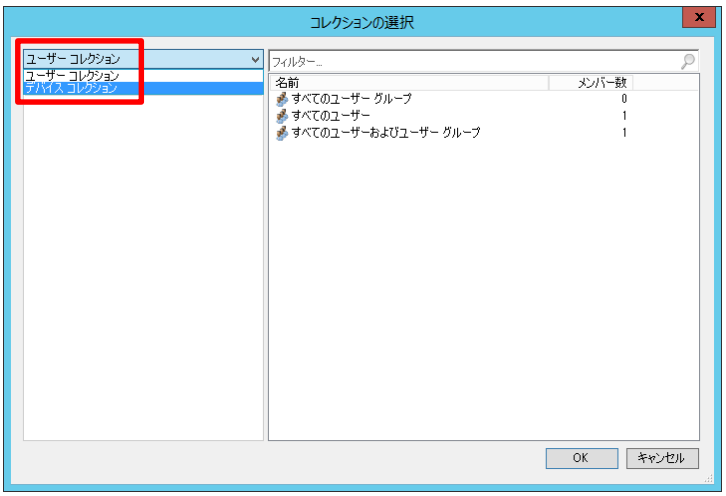
9) [Configuration Maneger] 画面で、中央ペインのインポートした [LabBaseline] を右クリックし、[展開] をクリックします。



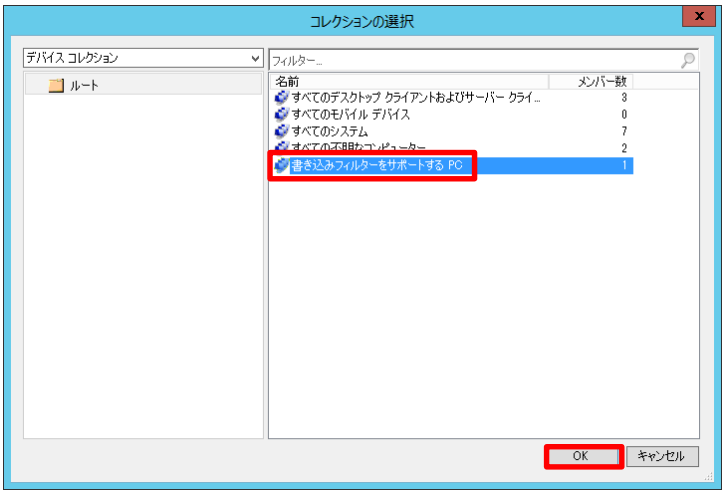
10) [構成基準の展開] 画面で、[参照] をクリックします。



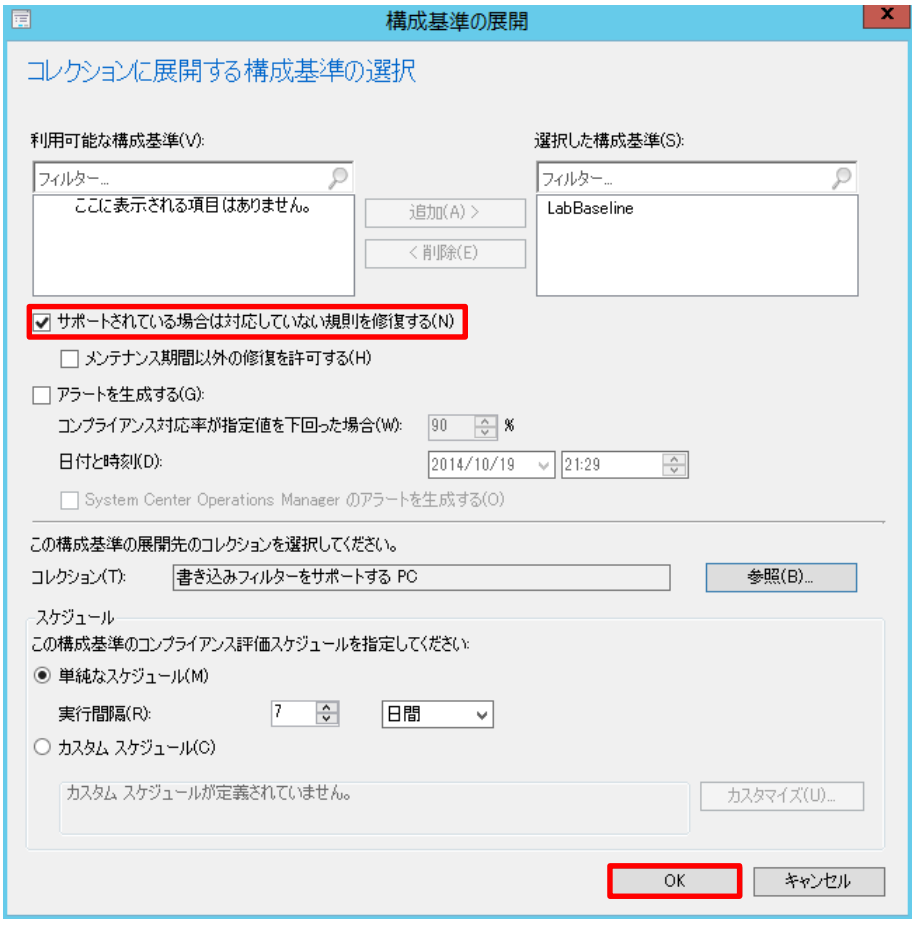
11) [コレクションの選択] 画面で、[デバイスコレクション] を選択します。



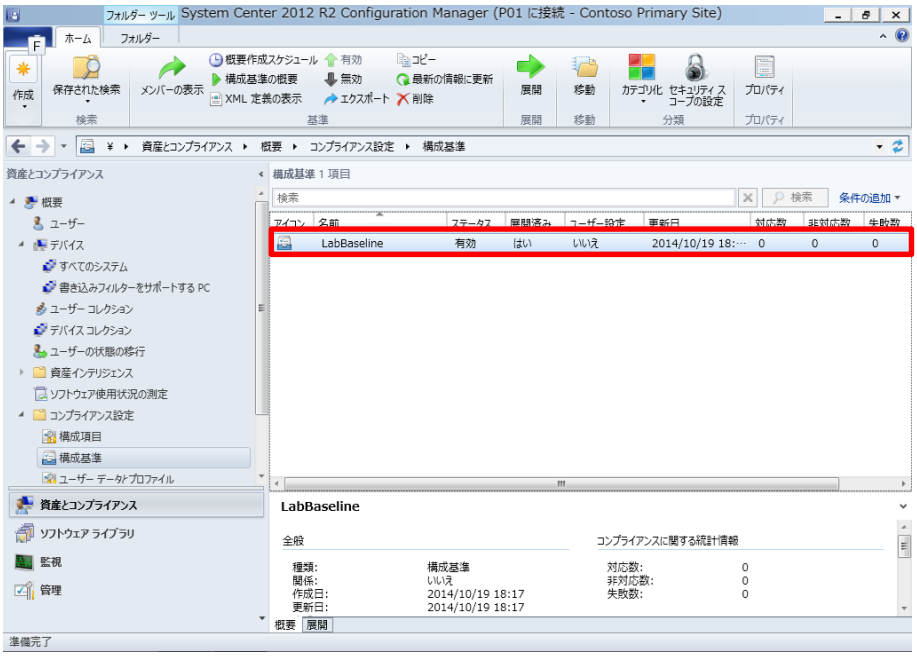
12) [コレクションの選択] 画面で、[書き込みフィルターをサポートする PC] をクリックし、[OK] をクリックします。



13) [構成基準の展開] 画面で、[サポートされている場合は対応していない規則を修復する] にチェックをつけ、[OK] をクリックします。



14) [Configuration Maneger] 画面で、[LabBaseline] 欄の [展開済み] が [はい] に変わり、SCCM クライアントに対して配布が開始されたことが確認できます。

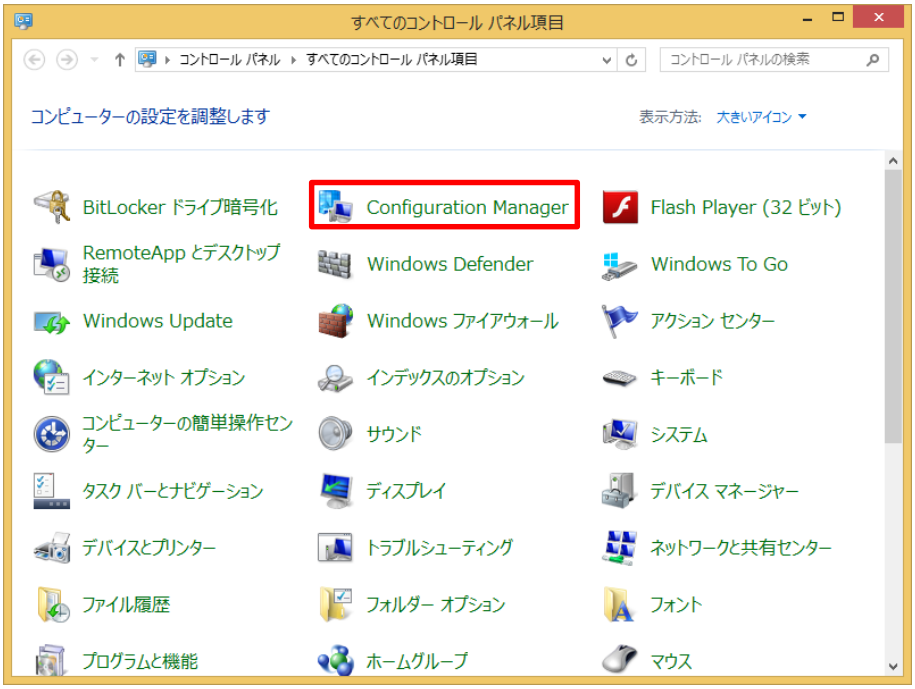


9.2.5 フィルター設定の適用状況の確認

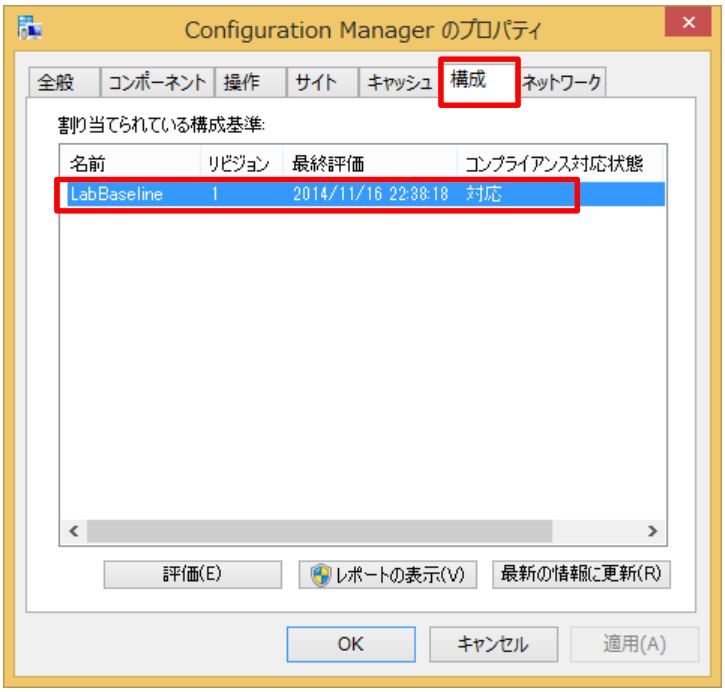
SCCM のコンプライアンス設定によって展開されたフィルター設定の適用状況をクライアント PC から確認します。

1) SCCM クライアントで管理されている Widnows Embedded 8.1 Industry Enterprise コンピューター (WE81IE01 コンピューター) で、スタートボタンを右クリックし、[コントロール パネル] をクリックします。

2) [すべてのコントロール パネル項目] 画面で、[Configuration Manager] をクリックします。



3) [Configuration Manager のプロパティ] 画面で、[構成] タブをクリックすると、前の手順で作成した LabBaseline フィルター設定の適用状況が確認できます。[コンプライアンス対応状態] 欄が [対応] と表示されていれば、フィルター設定が適用されていることが確認できます。



【Note:】
SCCM からクライアント側にフィルター設定が展開されるまでには時間がかかります。

10 まとめ

Windows Embedded 8.1 Industry Enterprise は、Windows 8.1 をベースに組み込み端末として必要なロックダウンを行うことができます。
本書では Windows Embedded 8.1 Industry Enterprise のインストールから、Embedded Lockdown Manager によるロックダウン設定、そしてシナリオ別に必要となるロックダウン設定について実際の手順の説明を行いました。
本書が Windows Embedded 8.1 Industry Enterprise の検証、環境構築を行う際の参考になれば幸いです。