ボリューム アクティベーション

ステップ バイ ステップ  
（Windows 10 および Windows Server 2012 R2対応）

日本マイクロソフト株式会社

発行 : 2015 年 10月 (改版 : 2020 年 8 月)

内容

[ボリューム アクティベーション 1](#_Toc433993004)

[ボリューム アクティベーションの概要 1](#_Toc433993005)

[ボリューム アクティベーション （VA）とは 1](#_Toc433993006)

[Active Directory によるライセンス認証 2](#_Toc433993007)

[キー管理サービス (KMS) ライセンス認証 4](#_Toc433993008)

[ KMS ホスト自動検出に必要な DNS サーバー設定 5](#_Toc433993009)

[ KMS ライセンス認証の仕組み 6](#_Toc433993010)

[ KMSホストの構築手順 7](#_Toc433993011)

[ KMS クライアントの認証手順 8](#_Toc433993012)

[マルチ ライセンス認証キー (MAK) ライセンス認証 8](#_Toc433993013)

[ マルチ ライセンス認証キーによるライセンス認証の手順 9](#_Toc433993014)

[ボリューム ライセンス認証の計画と考慮事項 10](#_Toc433993015)

[KMS ボリューム ライセンス キー タイプ 10](#_Toc433993016)

[Active Directory によるライセンス認証を計画する場合の考慮事項 12](#_Toc433993017)

[キー管理サービス (KMS) ライセンス認証の計画 13](#_Toc433993018)

[ KMS ホスト 13](#_Toc433993019)

[ 複数のKMSホストが存在する場合 13](#_Toc433993020)

[ KMS クライアント 13](#_Toc433993021)

[ KMS ホストの動的検出を可能にする DNS サーバーの基本的な前提条件 14](#_Toc433993022)

[ クライアント コンピューターの DNS 関連の設定について 15](#_Toc433993023)

[ボリューム ライセンス認証の事前準備 16](#_Toc433993024)

[ボリューム ライセンス キーの認証 16](#_Toc433993025)

[Active Directoryによる認証を構成するための事前準備 16](#_Toc433993026)

[ アカウントの準備とアクセス許可の付与 16](#_Toc433993027)

[ Active Directory スキーマの更新 16](#_Toc433993028)

[KMS による認証を構成するための事前準備 17](#_Toc433993029)

[ アカウントの準備とアクセス許可の付与 17](#_Toc433993030)

[ Windows 10 を認証するための、KMS ホストの事前準備 17](#_Toc433993031)

[Active Directory によるライセンス認証の構成手順 18](#_Toc433993032)

[[ボリューム ライセンス認証サービス] 役割のインストール 18](#_Toc433993033)

[参考：コマンドを利用した[ボリューム ライセンス認証サービス] 役割のインストール 21](#_Toc433993034)

[[ボリューム ライセンス認証ツール] の構成 21](#_Toc433993035)

[Windows Server 2012 R2 を使用した KMS ホストの構成手順 (サーバー VL) 25](#_Toc433993036)

[ボリューム ライセンス認証サービスのサーバーの役割のインストール 25](#_Toc433993037)

[参考：コマンドを利用した[ボリューム ライセンス認証サービス] 役割のインストール 28](#_Toc433993038)

[[ボリューム ライセンス認証ツール] を使用したKMS ホストの設定 29](#_Toc433993039)

[KMSホストファイアウォールの設定 34](#_Toc433993040)

[Windows 10 を使用した KMS ホストの構成手順（クライアント VL） 35](#_Toc433993041)

[必要とする環境 35](#_Toc433993042)

[KMS ホストの初期設定 35](#_Toc433993043)

[KMS ホストのライセンス認証 38](#_Toc433993044)

[KMSホストのファイア ウォール設定 41](#_Toc433993045)

[DNS サーバーで SRV レコードの確認 (ドメインに参加する KMS ホストの場合) 43](#_Toc433993046)

[参考：SRV レコードの手動作成 44](#_Toc433993047)

[ Windows Server を実行する DNSサーバーを使用した SRV レコードの手動作成 44](#_Toc433993048)

[ BIND 8.2 以降の DNS サーバーを使用した SRV レコードの手動作成 45](#_Toc433993049)

[ 追加のドメインに、KMS ホストの SRV レコードを自動的に発行する 46](#_Toc433993050)

[Windows 10 のライセンス認証 47](#_Toc433993051)

[ライセンス認証が行われていない状態を確認する 47](#_Toc433993052)

[ライセンス認証の実行 49](#_Toc433993053)

[ MAK による認証 49](#_Toc433993054)

[ KMS ホストに認証されない 51](#_Toc433993055)

[ ライセンス認証後の確認 52](#_Toc433993056)

[ボリューム アクティベーションの管理 54](#_Toc433993057)

[ボリューム ライセンス認証サービスによる管理 55](#_Toc433993058)

[イベント ビューアーによる確認 57](#_Toc433993059)

[KMS ホストから DNS サーバーに対して、SRV レコードの発行要求の確認 58](#_Toc433993060)

[MAK / KMS キーが認証上限数を超えてしまった際の対処方法 59](#_Toc433993061)

[ 電話での問い合わせ 60](#_Toc433993062)

[ Web ページでの申請 61](#_Toc433993063)

[スクリプトによる管理 62](#_Toc433993064)

[ リモートでの Slmgr の実行 62](#_Toc433993065)

[ リモート管理 に必要な Windows ファイアウォールの構成 63](#_Toc433993066)

[ ワーク グループのコンピューターを対象とするリモート操作 64](#_Toc433993067)

[ グローバル管理および設定 65](#_Toc433993068)

[ Active Directory による認証の設定 67](#_Toc433993069)

[ KMS ホスト設定 68](#_Toc433993070)

[ KMS クライアント設定 70](#_Toc433993071)

[仮想マシンの自動ライセンス認証 71](#_Toc433993072)

[自動ライセンス認証要件 71](#_Toc433993073)

[自動ライセンス認証方法 71](#_Toc433993074)

[自動ライセンス認証の運用 72](#_Toc433993075)

[まとめ 75](#_Toc433993076)

[Appendix 76](#_Toc433993077)

[FAQ 76](#_Toc433993078)

[ ボリューム アクティベーション FAQ 76](#_Toc433993079)

[ KMS ライセンス認証 FAQ 78](#_Toc433993080)

[ ボリューム ライセンス認証サービス FAQ 81](#_Toc433993081)

[以前の KMS キー タイプ 83](#_Toc433993082)

[KMS クライアントセットアップキー（GVLK） 85](#_Toc433993083)

[出典 87](#_Toc433993084)

# ボリューム アクティベーション

## ボリューム アクティベーションの概要

マイクロソフトのさまざまな製品は、ライセンス認証を行う必要があります。

製品のライセンス認証とは、ソフトウェアが正規品であり、プロダクト キーが悪用されていないことを確認するために、マイクロソフトが行う検証のプロセスです。ライセンス認証により、ソフトウェアの  
プロダクト キーと、デバイス上の該当するソフトウェア インストールが関連付けられます。

Windows Server 2012 R2 および Windows 10 では、ライセンス認証と検証が同時に  
行われます。ライセンス認証の対象となるのは、次のライセンスです。

* パッケージ製品のライセンス
* ボリューム ライセンス
* OEMライセンス

ライセンス認証を行うには、プロダクト キーの入力、ネットワーク サーバーへの接続、またはサービス   
センターへの問い合わせなどの手順が必要ですが、ライセンスの種類によって方法は異なります。

この文章に記載されているライセンス認証方法は、ボリューム ライセンスを対象としています。

## ボリューム アクティベーション （VA）とは

ボリューム アクティベーション (VA) とは、Windows Vista および Windows Server 2008 で、初めて導入された、法人ユーザー様向けの製品のライセンス認証方法です。  
ボリューム ライセンスを利用している企業のエンド ユーザー様にとって、透過的な方法でライセンス認証プロセスを自動化できるように設計されています。

組織内の複雑なネットワーク環境やサービス環境に柔軟に対応できるように、ボリューム アクティベーションでは、次の3種類のライセンス認証方法を用意しています。

* **Active Directory によるライセンス認証**
* **キー管理サービス (KMS) ライセンス認証**
* **マルチ ライセンス認証キー (MAK) ライセンス認証**

## Active Directory によるライセンス認証

Active Directory によるライセンス認証は、Active Directory ドメイン サービス (AD DS) を使用してライセンス認証オブジェクトを格納することができます。  
Active Directoryによるライセンス認証を実装するには、Windows Server 2012 以降のWindows Serverを実行するドメインコントローラーで、[ボリュームライセンス認証サービス]役割を構成します。これにより、ボリューム ライセンス認証サービスを構成するタスクを大幅に簡略化できます。

Active Directory によるライセンス認証の場合、KMS クライアント セットアップ キー (GVLK) を使用して、Windows 8以降およびWindows Server 2012 以降のドメインに参加しているすべてのコンピューターで、コンピューターの起動時に自動的かつ透過的にライセンス認証が行われます。Active Directory によるライセンス認証は、180 日間有効です。これを、"**ライセンス認証の有効期間**" といいます。これらのクライアントは、ドメインのメンバーである限りライセンス認証を維持し、ドメイン コントローラーと定期的に通信を行います。

ボリュームライセンス版の OS をインストールすると、既定で Generic Volume License Key (GVLK)が入力されて  
います。GVLK はKMS クライアントのライセンスキーになります。

ライセンス認証は、Software Protection サービスの開始後に実行されます。  
Software Protection サービスが開始されると、Windows 8 以降または Windows Server 2012 以降を実行しているコンピューターは、自動的に AD DS に接続し、ライセンス認証オブジェクトを受信し、ユーザーによる操作なしでライセンス認証が完了します。

Active Directory によるライセンス認証は、Windows 8 以降、または Windows Server 2012 以降を実行しているコンピューターのみライセンス認証ができます。したがって、Windows 8 以降、または Windows Server 2012 以降の Windows を実行するドメイン環境では、Active Directory によるライセンス認証はすべてのクライアントおよびサーバーをライセンス認証するための最適なオプションとなり、KMS ホストが不要になります。

ボリューム アクティベーションが適用されている、以前のバージョンの Windows を今後も使用し続ける場合、次の2種類の認証方法が環境内に混在することになります。

* Windows 8 以降、および Windows Server 2012 以降のクライアントの認証  
  **Active Directory によるライセンス認証**
* Windows 7以前、および Windows Server 2008 R2以前のクライアントの認証  
  **KMS ホストによる認証**

Active Directory によるライセンス認証を使用してライセンス認証された、コンピューターの  
ライセンス認証状態は、180 日間維持されます。

ライセンスの再認証は、次の手順で行われます。

クライアントが以前にライセンス認証されていた場合、ライセンス認証イベントが成功すると、ライセンス認証期間が 180 日に再設定されます。ライセンス認証試行が失敗した場合、ライセンスの  
再認証が成功するまで、既定で 7 日ごとにライセンス認証が試行されます。180 日のライセンス認証期間が経過した場合、ライセンス認証は失敗し、ユーザーに通知が表示されます。さらに、 Application ログにイベントが記録されます。

Active Directory によるライセンス認証を使用できない場合、最初に Active Directory によるライセンス認証を使用してライセンス認証されたコンピューターは、KMS ライセンス認証を試行します。この試行は、ライセンス認証が成功するまで続行されます。コンピューターが、次回ライセンスの再認証を試行するとき、クライアントは最初に Active Directory によるライセンス認証を試行します。この試行が成功すると、クライアントでは再度 Active Directory によるライセンス認証が使用されます。

ボリューム ライセンス情報が AD DS で見つからない場合、Windows Server 2012 以降、または Windows 8   
以降を実行しているクライアントは、KMS ホストを探し、KMS ライセンス認証プロセスに従ってライセンス認証を試行します。

ドメインのメンバーでなくなったコンピューターでは、コンピューターまたはSoftware Protection   
サービスが再起動したときにライセンス認証が失敗します。

Active Directory によるライセンス認証は、ドメインのメンバーではないコンピューターのライセンス認証に、使用することはできません。

## キー管理サービス (KMS) ライセンス認証

KMS ライセンス認証は、Active Directory によるライセンス認証と同様、企業内に存在する  
クライアント コンピューターが、インターネットや電話によるライセンス認証を個別に行わなくてもいいように考慮された認証方式です。これにより、ライセンス認証を行うためのトラフィックがインターネットに流れないというメリットがあります。Windows がインストールされた状態であれば、KMS クライアント セットアップ キー (GVLK) が登録されますので、ライセンスキーの入力は必要ありません。

KMS ライセンス認証を行うには、KMS ホストと呼ばれる役割を持つコンピューターを構築し、  
マイクロソフト ライセンス認証サービスに接続して、KMS ホストのライセンス認証を1回だけ行います。KMS クライアントは、ライセンス認証を行うために、ローカル ネットワークに配置されているKMS ホストに接続します（KMS ホストは、ローカル ネットワーク上に存在する必要があります）。KMS ホストが、クライアントのライセンス認証を行います。

KMS ホストは、ほかのサービスと共存させることができるため、専用サーバーである必要はありません。Windows 10を認証するための KMS ホストは、次のWindowsが実行されている任意の物理システム、または仮想システムで構成することができます。

* Windows Server 2012 R2
* Windows Server 2012
* Windows 10
* Windows 8.1
* Windows 8

KMS ホストは、上記のWindowsが実行されているコンピューターに、「KMS キー」をインストールすることによって構築することができます。

KMS ライセンス認証を行うには、ネットワークに最小限の数 ("**ライセンス認証のしきい値**" といいます) の物理コンピューターもしくは仮想コンピューターが存在している必要があります。

このしきい値を満たすと、KMS クライアントのライセンス認証を行うことができます。ライセンス認証のしきい値が満たされていることを確認するために、KMS ホストは、ネットワーク上でライセンス認証を要求している物理コンピューターおよび仮想コンピューターの数をカウントします。

KMS ライセンス認証のしきい値は、次のようになっています。

* Windows Server **5** 台以上
* Windowsクライアント **25** 台以上

Windows Server を実行している物理コンピューターまたは仮想コンピューターが、5 以上の  
ライセンス認証カウントを受け取ると、ライセンス認証が行われます。Windows クライアントを実行している物理コンピューターまたは仮想コンピューターが 25 以上のライセンス認証カウントを受け取ると、ライセンス認証が行われます。

KMS ライセンス認証は、180 日間有効です。これを、"**ライセンス認証の有効期間**" といいます。KMS クライアントは、認証状態を維持するために、少なくとも 180 日ごとに 1 回 KMS ホストに接続してライセンス認証を更新する必要があります。KMS クライアント コンピューターは、既定で 7 日ごとにライセンス認証を更新します。クライアントのライセンス認証が更新された後、再びライセンス認証の有効期間が開始されて有効期限が自動延長されるため、各コンピューターは有効期間を気にせず使い続けることができます。

### KMS ホスト自動検出に必要な DNS サーバー設定

KMS クライアントが KMS ホストを見つけ出す際、通常では、DNSサーバーを使用します。KMS ホストの構築時に、DNS サーバーに対して、自動的に KMS ホストの IP アドレスとライセンス認証に使用するポート番号などの情報を発行します。

KMS クライアントが KMS ホストを自動検出する際、DNS サーバーに対して、KMS ホストの IP アドレスとライセンス認証に使用するポート番号を問い合わせます。これらの情報を取得することで KMS クライアントは KMS ホストを検出することができ、ライセンス認証を完了することができます。

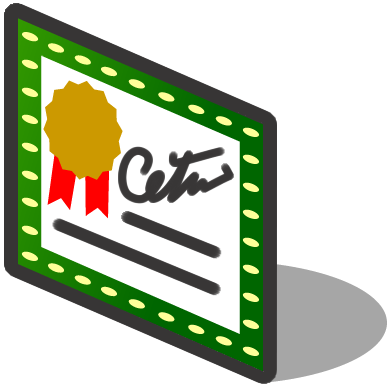
DNS サーバーが企業環境に構築されていない場合、KMS クライアントが KMS ホストを自動検出することができないため、スクリプトにより手動で設定する必要があります。

### KMS ライセンス認証の仕組み

KMS ホストを使用している環境では、ボリューム ライセンス認証プロセスは、次のように実行されます。

1. KMS キーを、KMS ホストとなるコンピューターにインストールします。
2. KMS ホストが、マイクロソフト のホストされているライセンス認証サービスに接続することで、  
   ライセンス認証が行われます。
3. KMS が有効になった後は、KMS が開始されるたび、または 1 日に 1 回、KMS によって SRV レコードがドメイン ネーム システム (DNS) に登録されます。
4. KMS クライアント コンピューターは、構成済みのレジストリ エントリから、または DNS 内の KMS SRV レコードを介して、KMS ホストを検出します。
5. クライアントは、1688/TCP を使って KMS ホストに RPC 要求を送信します (既定の設定)。この要求には、暗号化されたクライアント コンピューター ID が含まれています。このコンピューターでまだライセンス認証が行われたことがなく、KMS ホストから応答がない場合、  
   クライアントは 2 時間後に新しい要求を送信します。コンピューターでライセンス認証が行われている場合、クライアントは 7 日後に新しいライセンス認証要求を送信します。
6. KMS ホストはクライアント コンピューター ID をテーブルに追加し、クライアントにライセンス認証カウントを返します。
7. クライアントはライセンス認証カウントをしきい値に照らして評価し、ライセンス認証しきい値が満足されている場合は、ライセンス認証を行います。

ライセンス契約



1



マイクロソフト  
ライセンス認証サービス

3

2



4



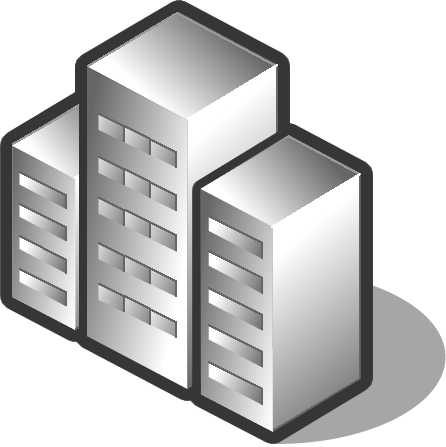
DNSサーバー

KMSホスト

2

3

1



KMSクライアント

組織内

図 1： キー管理サービスによるライセンス認証

### KMSホストの構築手順

KMS キーをマイクロソフトから入手します。

1

KMS ホストを作成し、KMSキーを入力します。

2

KMS ホストを、マイクロソフトライセンス認証サーバーに接続して認証します。

3

DNS サーバーに、KMS ホストの SRV レコードを登録します。

4

### KMS クライアントの認証手順

KMS クライアントが、DNS サーバーに対して、KMS ホストの問い合わせ（SRV レコード）を行います。

1

KMS ホストに認証要求を行います。

2

KMS ホストが認証情報を入手し、ライセンス認証のしきい値を満たしていた場合、ライセンス認証が行われ、有効期間（180日間）が設定されます。

3

## マルチ ライセンス認証キー (MAK) ライセンス認証

MAK は、ライセンス認証サービスに対して、1 回だけライセンス認証を行う認証方法です。

コンピューターは、1 回マイクロソフトとのライセンス認証を行えば、ハードディスク交換や大幅な  
ハードウェア変更がない限り、以降のライセンス認証は不要となります。

それぞれの MAK キーには、許可されるライセンス認証の回数があらかじめ設定されています。

この回数は、ボリューム ライセンス認証契約に基づいており、組織のライセンス カウントと厳密には一致しません。マイクロソフトによってホストされるライセンス認証サービスと、MAK キーを使用して  
ライセンス認証を行うごとに、ライセンス認証制限まで回数がカウントされます。

MAK ライセンス認証は、KMS ホストを構築されていない環境や、必要とするコンピューターの台数が足りないために KMS ライセンス認証のしきい値が満たされない環境に推奨されます。

さらに、180日以上 KMS ホストにアクセスできない環境においても推奨されます。

MAKライセンス認証では、各コンピューターが、インターネットまたは電話を使って、それぞれ個別に マイクロソフトに接続してライセンス認証を行う必要があります。

セキュリティ上の理由からインターネットまたは社内ネットワークへの直接アクセスが制限される環境においては、複数のコンピューターのライセンス認証要求をまとめて、ボリューム ライセンス認証管理ツール (VAMT) を使ってマイクロソフトに送信することができます。

VAMT は、ライセンス認証要求を複数のシステムから収集して マイクロソフトに一括送信することができるスタンドアロン アプリです。



ライセンス契約







C:\Users\BBM100041\AppData\Local\Microsoft\Windows\INetCache\Content.Word\mini key_s.png



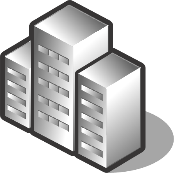
1

マイクロソフト  
ライセンス認証サービス

2

C:\Users\BBM100041\AppData\Local\Microsoft\Windows\INetCache\Content.Word\mini key_s.png





クライアント

組織内

図 2： マルチライセンス認証キー (MAK) によるライセンス認証

### マルチ ライセンス認証キーによるライセンス認証の手順

MAK キーを、認証を行いたいコンピューターに入力します。

1

マイクロソフト ライセンス認証サーバーに接続し、認証を行います。

2

# ボリューム ライセンス認証の計画と考慮事項

## KMS ボリューム ライセンス キー タイプ

下表は、KMS キー製品グループと認証できるWindowsのエディションを記載したものです。

|  |  |  |
| --- | --- | --- |
| KMSキー製品 グループ | KMSホストとして構成できる Windows のバージョン | 認証できる Windows エディション |
| クライアント | Windows 8\*  Windows 8.1\*  Windows 10 | Windows Vista Business  Windows Vista Enterprise  Windows 7 Professional  Windows 7 Enterprise  Windows 8 Pro  Windows 8 Enterprise  Windows 8.1 Pro  Windows 8.1 Enterprise  Windows 10 Pro  Windows 10 Enterprise  Windows 10 Enterprise LTSB  Windows 10 Education |
| サーバー | Windows Server 2012 Standard\*  Windows Server 2012 Datacenter\*  Windows Server 2012 R2 Standard\*  Windows Server 2012 R2 Datacenter\* | Windows Vista Business  Windows Vista Enterprise  Windows 7 Professional  Windows 7 Enterprise  Windows 8 Pro  Windows 8 Enterprise  Windows 8.1 Pro  Windows 8.1 Enterprise  Windows 10 Pro  Windows 10 Enterprise  Windows 10 Enterprise LTSB  Windows 10 Education  Windows Server 2008 (全てのエディション)  Windows Server 2008 R2 (全てのエディション)  Windows Server 2012 (全てのエディション)  Windows Server 2012 R2 (全てのエディション) |

表 1 Windows 10 および Windows Server 2012 R2 で提供される KMS キー

＊これらの OS を使用して KMS ホストを構成する場合は更新プログラムを適用する必要があります

Windows 10、および Windows Server 2012 R2 で提供される KMS キーはクライアントと  
サーバーの 2 種類が提供されています。

KMS キー製品グループがクライアントの場合は、すべてのエディションのクライアント OS の認証をサポートしています。このクライアント KMS キーを使用して、KMS ホストを構築し、Windows 10を認証できる Windows のバージョンは、次の通りです。

* Windows 8
* Windows 8.1
* Windows 10

KMS キー製品グループがサーバーの場合は、すべてのエディションのクライアント OS およびサーバー OS の認証をサポートしています。つまり、サーバー KMS キーはクライアント KMS キーを  
包括していることになります。

サーバー KMS キーを使用して、KMS ホストが構築でき、Windows 10を認証できる  
Windows Serverのバージョンは、次の通りです。

* Windows Server 2012
* Windows Server 2012 R2

以前の KMS キーとの違いに関しては Appendix を参照してください。

## Active Directory によるライセンス認証を計画する場合の考慮事項

Active Directory によるライセンス認証では、追加のホスト サーバーは必要ありません。

既存のドメイン コントローラーで、ライセンス認証クライアントをサポートできますが、次の制限および注意事項があります。

* 読み取り専用ドメイン コントローラー上では、Active Directory によるライセンス認証を  
  構成できません。
* Active Directory によるライセンス認証は、マイクロソフト以外のディレクトリ サービスと共に使用できません。
* ライセンス認証オブジェクトを格納するためには、**AD DS が、Windows Server 2012 以上のスキーマ レベルである必要があります**（操作方法は後述します）。以前のバージョンの Windows Server を実行しているドメイン コントローラーでは、Windows Server 2012 /2012 R2バージョンの Adprep.exe を使用してスキーマを更新した後でクライアントのライセンス認証を行うことができます(ドメイン機能レベルやフォレスト機能レベルが Windows Server 2012 以上である必要はありません)。
* 必要なライセンス認証オブジェクトは、フォレスト内で1 つだけです。
* KMS を使用する場合と異なり、クライアントまたはサーバーをライセンス認証する際のしきい値制限はなく1台から認証されます。

## キー管理サービス (KMS) ライセンス認証の計画

KMSによるライセンス認証を行う場合、KMSホストの認証方法やバックアップKMS配置などに  
ついて事前に計画しておく必要があります。

### KMS ホスト

KMS ホストは1 回ライセンス認証を実行すると、ハードディスク交換や大幅なハードウェア変更がない限り、再ライセンス認証は不要です。KMS ホストのライセンス認証はインター  
ネット経由の他に、電話窓口でも行えるので、インターネットに接続していないローカル ネットワーク環境でも運用することが可能です。１つの KMS ホストで、数十万単位の KMS   
クライアントをサポートできます。マイクロソフトは、ほとんどの企業組織においてインフラストラクチャ全体を2つの KMS ホストのみで運用できると想定しています（メインの KMS ホストと、冗長性のためのバックアップ KMS ホスト）。

KMS キーは、最大 6 台の KMS ホスト (物理コンピューターでも仮想マシンでも  
構いません) にインストールできます。KMS ホストのライセンス認証後、同じホストを同じキーでさらに最大 9 回再ライセンス認証できます（同じ KMS ホストの認証は10回まで  
可能）。

### 複数のKMSホストが存在する場合

１つの KMS ホストで、数十万単位の KMS クライアントをサポートできますが、KMS ホストに障害が発生した場合のために、バックアップ KMS ホストを用意することもできます。

ただし、障害発生時は、KMS クライアントからバックアップ KMS ホストも認識できるように、バックアップ KMS ホストの SRV レコードを追加もしくは編集する必要があることに注意しなければなりません。

### KMS クライアント

ボリュームライセンスメディアによって提供される Windows Vista 以降のクライアント OS および、Windows Server 2008 以降のサーバーOSの既定の状態は KMS クライアントです。KMS を使用してライセンス認証を行う組織内のコンピューターでこれらの OS の  
いずれかを使用し、ネットワークで DNS自動探索が許可されている場合、これ以上の  
構成は必要ありません。

### KMS ホストの動的検出を可能にする DNS サーバーの基本的な前提条件

KMSホストが自身の存在を発行し、KMS クライアントが KMS ホストを検出できるようにするためには、環境内の DNS サーバーで、以下の機能をサポートしている必要があります。

* SRV リソースレコード
* 動的更新

上記の機能は、Windows 2000 Server 以降の DNS サーバーでサポートされているため、Windows Server で構築した DNSサーバーであれば考慮する必要はありません。

また、Berkeley Internet Domain Name (BIND) バージョン 8.2.2 patch 7 以降の  
バージョンで、SRV レコードと動的更新をサポートします。

また、KMS ホストは、DNS サーバー内の、次のレコードに対する作成、更新を行うための資格情報が必要です。

* SRV レコード
* A(Internet Protocol version 4、IPv4) レコード
* AAAA(Internet Protocol version 6、IPv6) レコード

KMSホストによる作成を行わない場合、レコードを手動で作成する必要があります。

KMS ホストに必要な資格情報を付与する場合の推奨されるソリューションは、AD DS にセキュリティ グループを作成した後、すべての KMS ホストを、作成したグループに追加することです。Windows DNS サーバーで、KMS SRV リソースレコード が含まれる、各 DNS ドメインの \_VLMCS.\_TCP レコードを完全に制御する権限がこのセキュリティ グループに  
与えられるようにします。

また、KMS ホストは運用中に、コンピューター名または TCP ポートがサービスの起動時に変化したことをソフトウェアライセンスサービス（slsvc.exe）が検出した場合、自動的に SRVエントリを更新します。また、DNS サーバーが必要なレコードを自動的に削除しない  
ように、１日に１回 SRV エントリを更新します。

ただし、これらの動作は、DNS サーバーがレコードの動的更新をサポートしている場合のみ有効に動作します。使用している DNS サーバーが動的更新をサポートしていない場合、  
これらの機能を無効化することが推奨されます。

### クライアント コンピューターの DNS 関連の設定について

KMS クライアントは、自身のコンピューターに設定されている DNS サーバーに対して、KMS ホストの情報を問い合わせます。そのため、KMS ホストの IP アドレスを解決できる DNS サーバーの IP アドレスを、KMS クライアントで設定しなければなりません。

また、ワーク グループ環境でコンピューターを運用している場合、KMSクライアントの設定で、DNS サフィックスに、KMS ホストの SRV レコードが格納されている DNS ゾーンの FQDN が設定されていることを確認する必要があります。

DHCP サーバーが導入されている環境では、オプション（015 DNS ドメイン名）を使用して DNS ゾーンの FQDN を配布することもできます。

# ボリューム ライセンス認証の事前準備

ボリュームライセンス認証を構成するには、事前に次の準備を行っておく必要があります。

## ボリューム ライセンス キーの認証

ボリューム ライセンス キーは、事前に認証する必要があります。ボリューム ライセンス キーは  
インターネットまたは電話を使って認証できます。インターネットを使って認証を行う場合、ボリューム ライセンス キーの認証後はライセンス認証サーバーをインターネットから切断できます。

## Active Directoryによる認証を構成するための事前準備

Active Directoryによる認証を構成するためには、次の準備を行う必要があります。

### アカウントの準備とアクセス許可の付与

選択したボリューム ライセンス認証オプションに応じて、[ボリューム ライセンス認証サービス]のインストールに使用するアカウントに、次のアクセス許可が必要です。

1. [ボリューム ライセンス認証サービス]を実行するコンピューターに対する、ローカル管理者のアクセス許可が必要です。
2. [ライセンス認証オブジェクト] コンテナーに、データをコピーするためのアクセス許可が  
   必要です。これらのアクセス許可は、既定では Enterprise Administrators グループのメンバーに割り当てられていますが、委任することができます。

### Active Directory スキーマの更新

Active Directory によるライセンス認証を使用するには、スキーマ レベルが Windows Server 2012 以上である必要があります。環境内に、Windows Server 2012 / 2012 R2 のドメイン コントローラーが既に存在する場合は、スキーマの更新は不要です。

一方、環境内に Windows Server 2012 以降のドメイン コントローラーが存在しない  
場合、スキーマを更新しなければなりません。スキーマの更新にあたって、以下の点を確認します。

* 既存環境の、フォレスト機能レベルと、ドメイン機能レベルは、Windows Server 2003   
  以上である必要があります。

スキーマの更新を行うには、適切なドメイン コントローラーで、次のコマンドを実行します。

adprep /forestprep

adprep /domainprep

## KMS による認証を構成するための事前準備

KMS による認証を構成するためには、次の準備を行う必要があります。

### アカウントの準備とアクセス許可の付与

選択したボリューム ライセンス認証オプションに応じて、ボリューム ライセンス認証ツールの  
インストールに使用するアカウントに、次のアクセス許可が必要です。

1. ボリューム ライセンス認証ツールを実行するコンピューターに対する、ローカル管理者の  
   アクセス許可が必要です。

### Windows 10 を認証するための、KMS ホストの事前準備

Windows 8/8.1、Windows Server 2012、Windows Server 2012 R2を実行する  
コンピューターで、KMS ホストを構築し、Windows 10を 認証できるようにするには、KMS キーのインストール前に、次の更新プログラムが適用されている必要があります。

更新: Windows 8 または Windows 8.1 では、Windows Server 2012 または Windows Server 2012 R2 の KMS ホストと Windows の 10 をアクティブにします。  
<https://support.microsoft.com/ja-jp/kb/3058168>

OSのバージョンごとに、更新プログラムが提供されているため、適切な更新プログラムを  
ダウンロードし、インストールしてください。

更新プログラムの適用後、次のコマンドを実行します。

slmgr /ipk < KMS キー>

Windows Server 2008 R2以前、Windows 7以前のバージョンを実行する KMS ホストが存在する場合、Windows 10の認証を行うことはできないため、新規に KMS ホストを構築する必要があります。

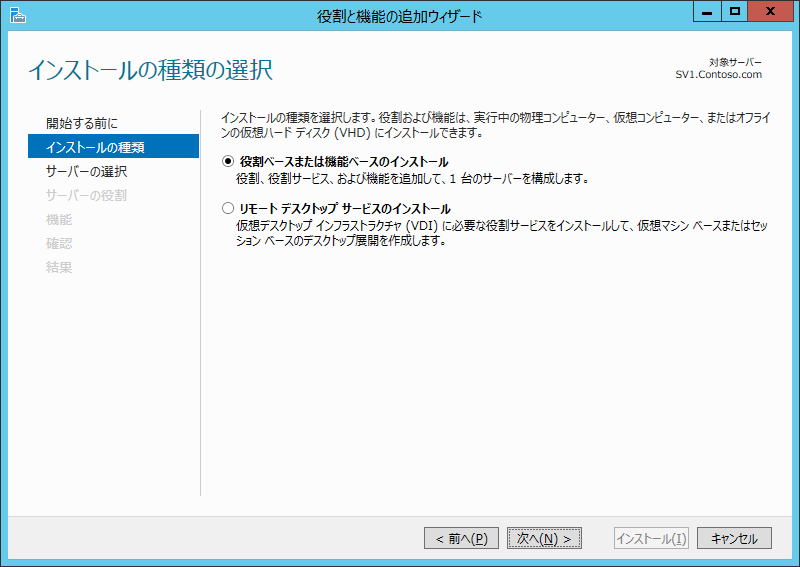
# Active Directory によるライセンス認証の構成手順

Windows Server 2012 から、[ボリュームライセンス認証サービス]役割が追加されました。

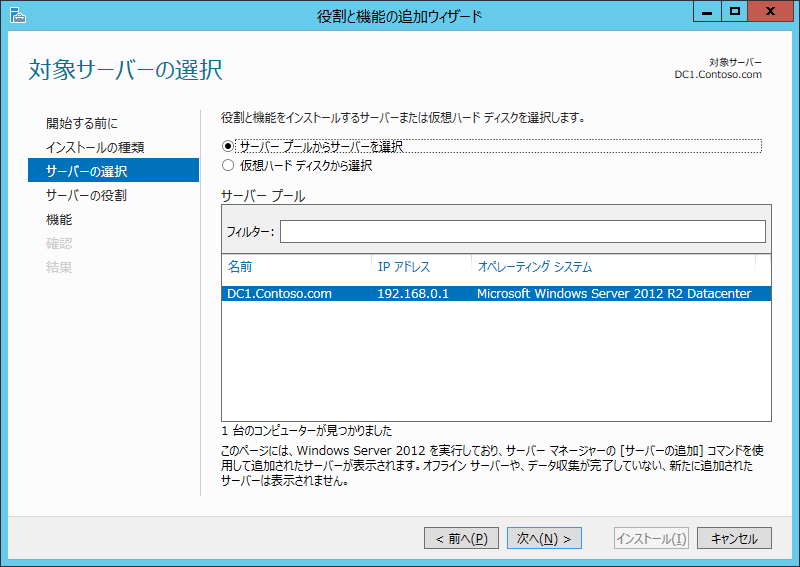
これをインストールすることで、簡単に構成を行うことができます。

## [ボリューム ライセンス認証サービス] 役割のインストール

1. Windows Server 2012/2012 R2 を実行しているドメインコントローラーで、[**サーバー   
   マネージャー**] を起動します。
2. [管理] メニューをクリックし、[役割と機能の追加] をクリックします。
3. [役割と機能の追加ウィザード] が起動したことを確認し、[次へ] ボタンをクリックします。
4. **[インストールの種類の選択]** ページで **[役割ベースまたは機能ベースのインストール]** を  
   選択し、**[次へ]** ボタンをクリックします。

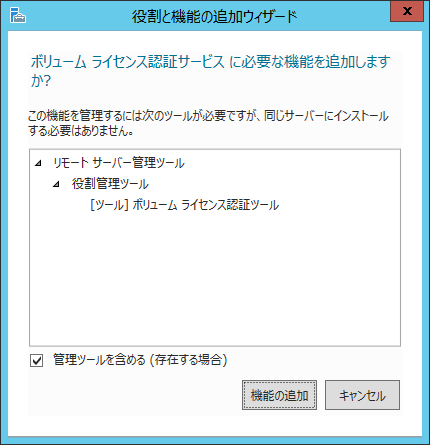


1. **[対象サーバーの選択]** ページで、**[サーバー プール]** から、インストール先のサーバーを  
   選択し、**[次へ]** ボタンをクリックします。

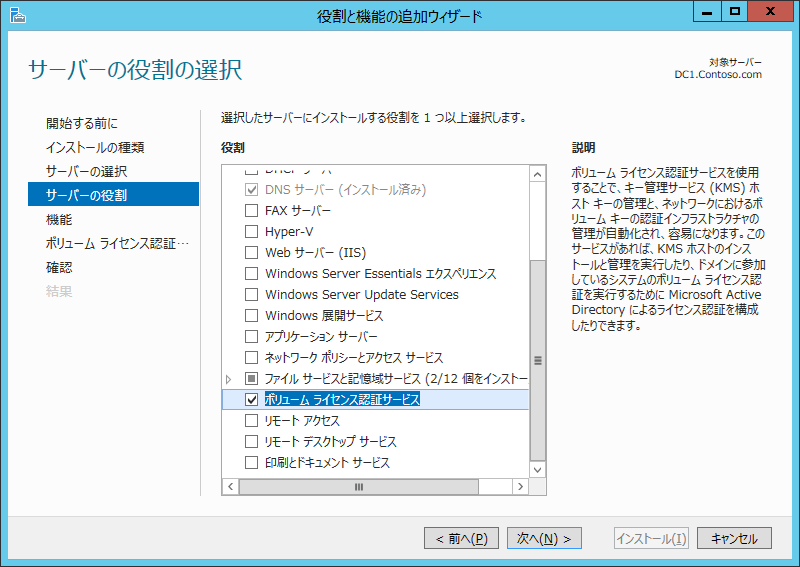


Windows Server 2012 以降では、[サーバー マネージャー] を使用して、リモート サーバーに対して役割や  
機能をインストールできます。既定では、[サーバー プール] の一覧には、ローカルサーバーのみが表示されます。  
リモートサーバーを指定する場合は、[サーバー マネージャー] の [管理] メニューをクリックし、[サーバーの追加]を選択して、リモートサーバーを追加しておく必要があります。

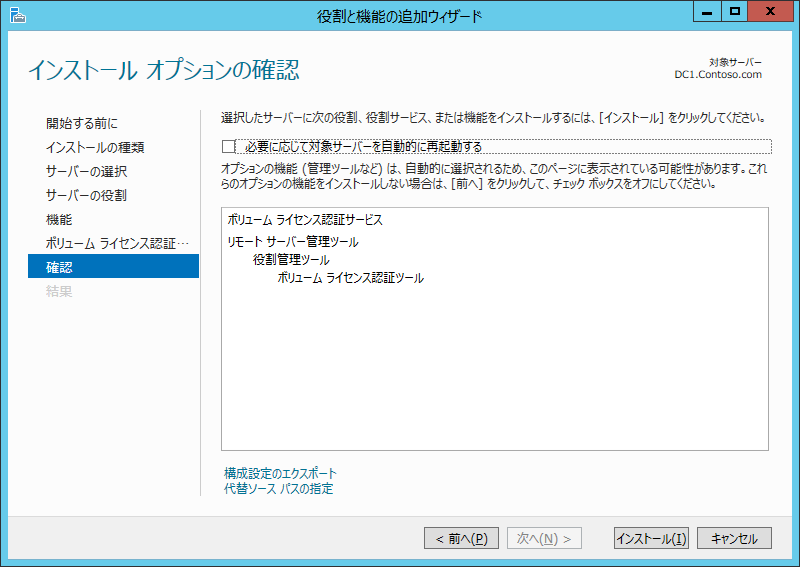
1. [サーバーの役割の選択] ページで、[ボリューム ライセンス認証サービス] チェック ボックスを  
   オンにします。
2. [役割と機能の追加ウィザード] ダイアログボックスが表示されたことを確認し、[機能の追加] ボタンをクリックします。



1. [サーバーの役割の選択] ページで、[ボリューム ライセンス認証サービス] チェックボックスが  
   オンになったことを確認し、[次へ] ボタンをクリックします。



1. [機能の選択] ページで、[次へ] ボタンをクリックします。
2. [ボリューム ライセンス認証サービス] ページで、[次へ] ボタンをクリックします。
3. [インストール オプションの確認] ページで、情報が正しいことを確認し、[インストール] ボタンをクリックします。

****

1. インストールが完了したことを確認し、[インストールの進行状況] ページで、[閉じる] ボタンをクリックします。

## 参考：コマンドを利用した[ボリューム ライセンス認証サービス] 役割のインストール

**[ボリューム ライセンス認証サービス]は、Dism コマンドおよび、PowerShell コマンド レットを  
使用してインストールすることもできます。**

* **Dism コマンドによるインストール**

**Import-Module Dism**

**Enable-WindowsOptionalFeature -Online -FeatureName VolumeActivation-Full-Role**

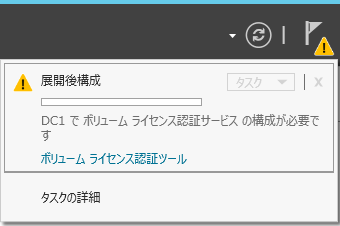
* **PowerShell コマンド レットによるインストール**

**Import-Module ServerManager**

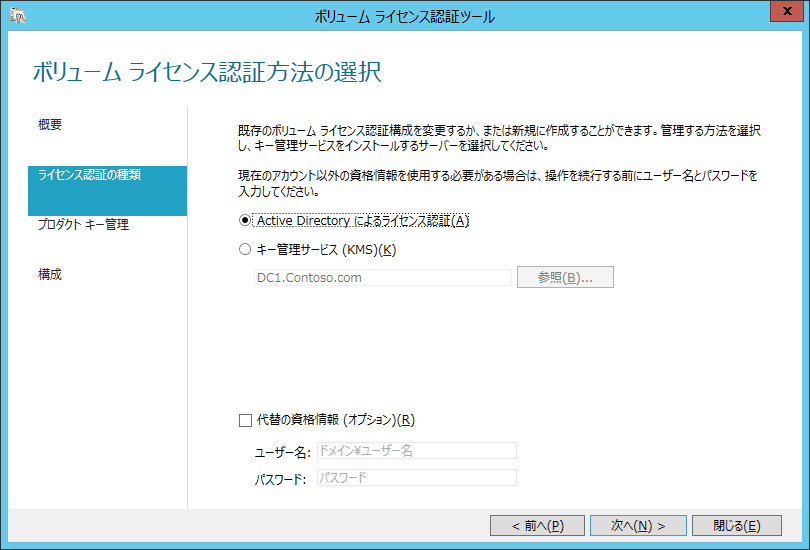
**Install-WindowsFeature VolumeActivation**

## [ボリューム ライセンス認証ツール] の構成

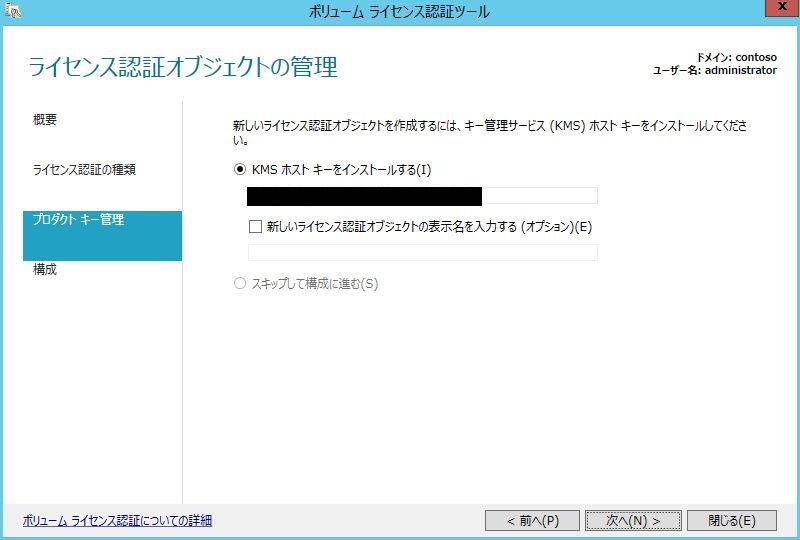
1. **[サーバー マネージャー] の、[通知] アイコンをクリックし、[ボリューム ライセンス認証ツール]をクリックします。**

****

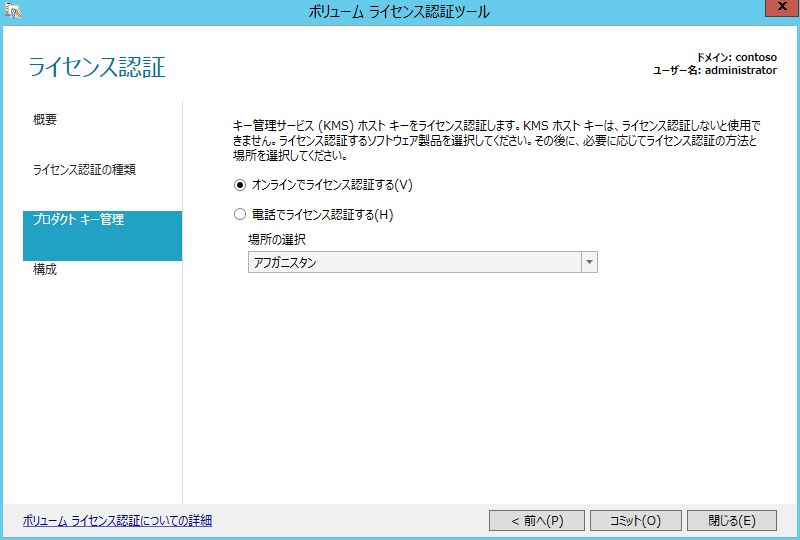
1. **[ボリューム ライセンス認証ツール]が起動したことを確認し、[次へ] ボタンをクリックします。**
2. **[ボリューム ライセンス認証方法の選択] ページで、[Active Directory によるライセンス  
   認証] を選択して、[次へ] ボタンをクリックします。**

****

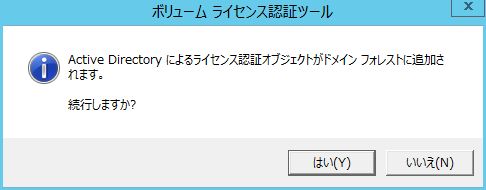
1. **[ライセンス認証オブジェクトの管理] ページで、[KMS ホスト キーをインストールする] が  
   選択されていることを確認し、KMS キーを入力して、[次へ] ボタンをクリックします。**



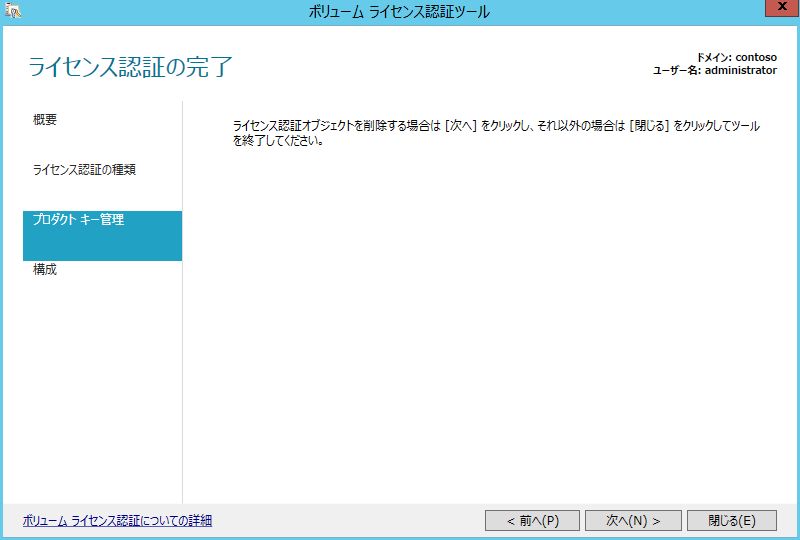
1. **[ライセンス認証] ページで、[オンラインでライセンス認証する] が選択されていることを  
   確認し、[コミット] ボタンをクリックします。**



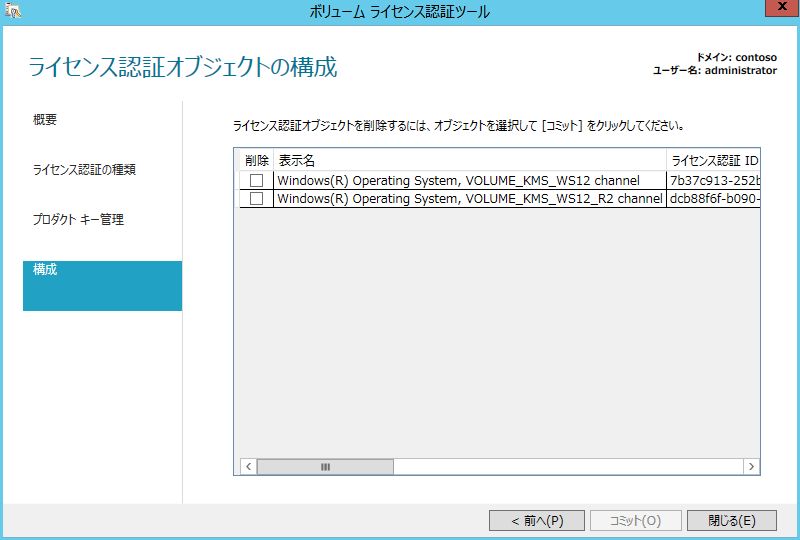
1. **次のような、確認のメッセージが表示されたことを確認し、[はい] ボタンをクリックします。**



1. **[ライセンス認証の完了] ページで、[次へ] ボタンをクリックします。**



1. **[ライセンス認証オブジェクトの構成] ページで、[閉じる] ボタンをクリックします。**



1. **メッセージボックスが表示されたことを確認し、[はい] ボタンをクリックします。**

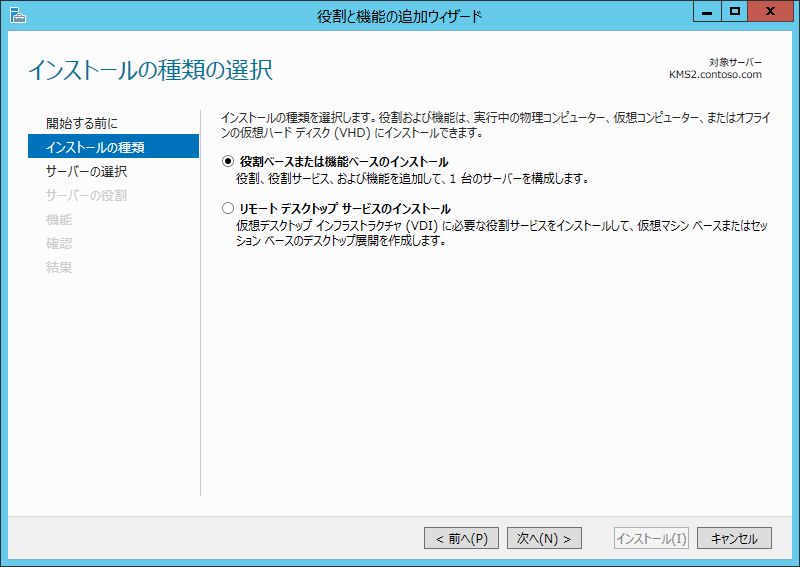
# Windows Server 2012 R2 を使用した KMS ホストの構成手順 (サーバー VL)

Windows Server 2012 R2 では、[ボリュームライセンス認証サービス] 役割が追加されました。これにり、対話的に KMS ホストをインストールすることができるようになりました。

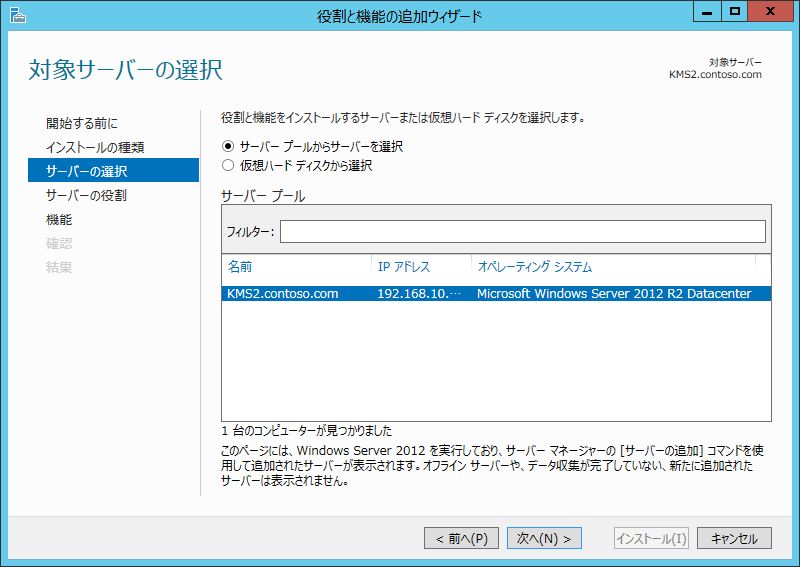
ここでは、ドメインに参加する Windows Server 2012 R2 を使用してKMS ホストの  
構成手順を確認します。

## ボリューム ライセンス認証サービスのサーバーの役割のインストール

1. KMS ホストとして構成を行うコンピューターで、[サーバー マネージャー] を起動します。
2. [管理] メニューの [役割と機能の追加] をクリックします。
3. [役割と機能の追加ウィザード] が起動したことを確認し、[次へ] ボタンをクリックします。
4. [インストールの種類の選択] ページで [役割ベースまたは機能ベースのインストール] が  
   選択されていることを確認し、[次へ] ボタンをクリックします。

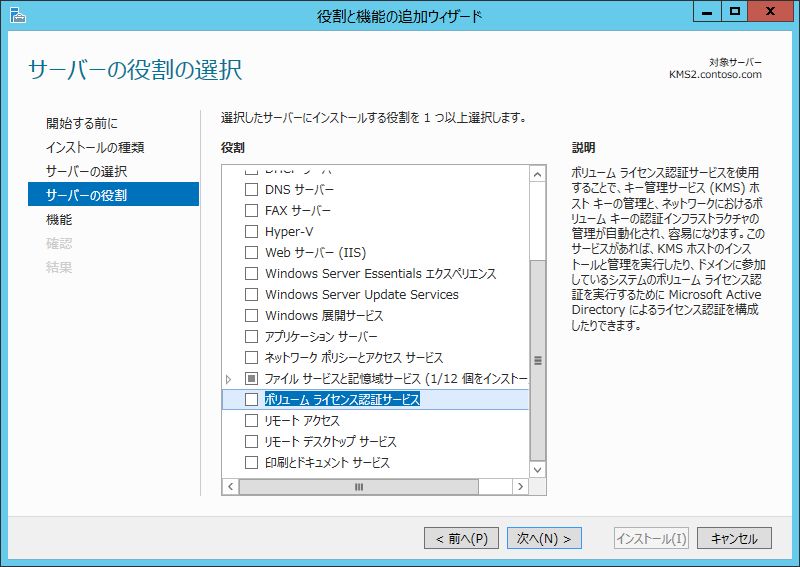


1. [対象サーバーの選択] ページで、[サーバー プール] から対象サーバーを選択し、[次へ]   
   ボタンをクリックします。

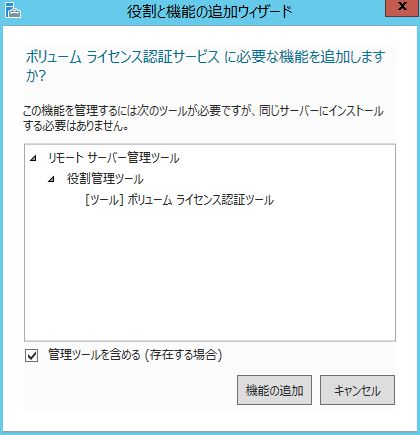


Windows Server 2012 以降では、[サーバー マネージャー] を使用して、リモート サーバーに対して役割や  
機能をインストールできます。既定では、[サーバー プール] の一覧には、ローカルサーバーのみが表示されます。  
リモートサーバーを指定する場合は、[サーバー マネージャー] の [管理] メニューをクリックし、[サーバーの追加]を選択して、リモートサーバーを追加しておく必要があります。

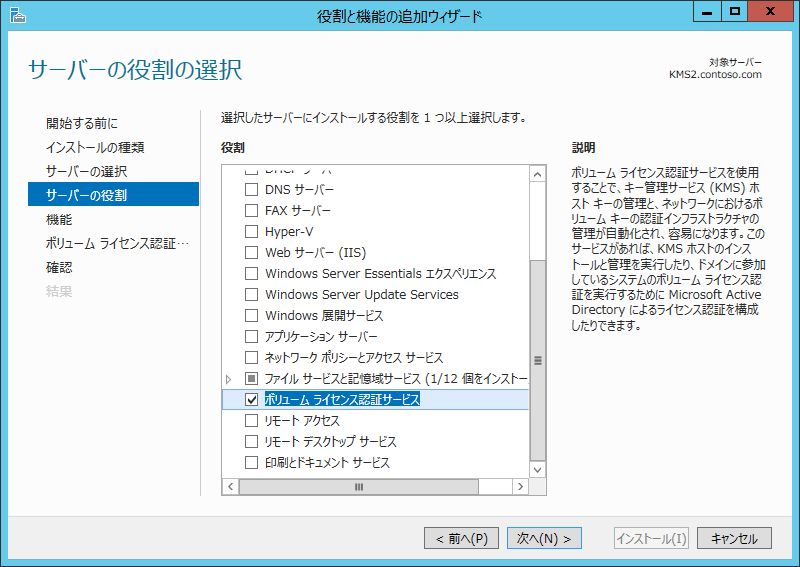
1. [サーバーの役割の選択] ページで、[ボリューム ライセンス認証サービス] チェックボックスを  
   オンにします。



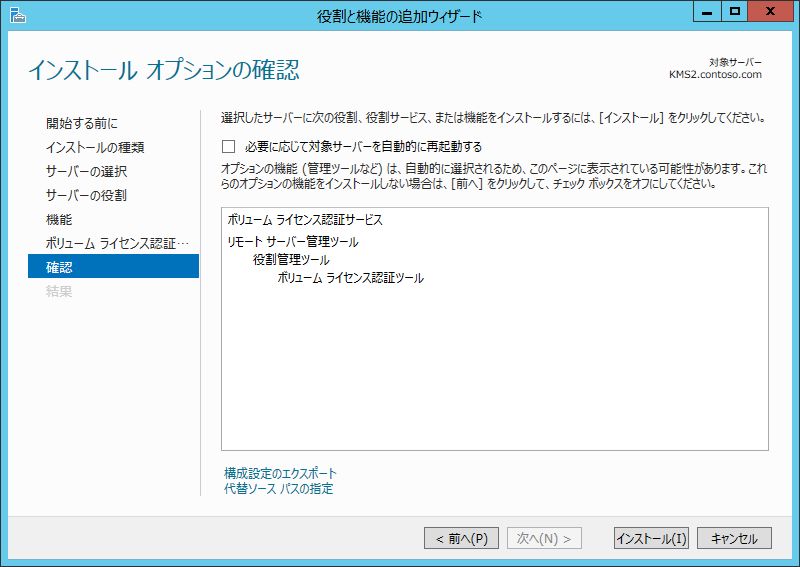
1. [役割と機能の追加ウィザード] ダイアログ ボックスが表示されたことを確認し、[機能の追加] ボタンをクリックします。



1. [サーバーの役割の選択] ページで、[ボリューム ライセンス認証サービス] チェックボックスが  
   オンになったことを確認し、[次へ] ボタンをクリックします。



1. [機能の選択] ページで、[次へ] ボタンをクリックします。
2. [ボリューム ライセンス認証サービス] ページで、[次へ] ボタンをクリックします。
3. [インストール オプションの確認] ページで、情報が正しいことを確認し、[インストール] ボタンをクリックします。



1. インストールが完了したことを確認し、[インストールの進行状況] ページで、[閉じる] ボタンをクリックします。

## 参考：コマンドを利用した[ボリューム ライセンス認証サービス] 役割のインストール

**[ボリューム ライセンス認証サービス] は、Dism コマンドおよび、PowerShell コマンド レットを  
使用してインストールすることもできます。**

* **Dism コマンドによるインストール**

**Import-Module Dism**

**Enable-WindowsOptionalFeature -Online -FeatureName VolumeActivation-Full-Role**

* **PowerShell コマンド レットによるインストール**

**Import-Module ServerManager**

**Install-WindowsFeature VolumeActivation**

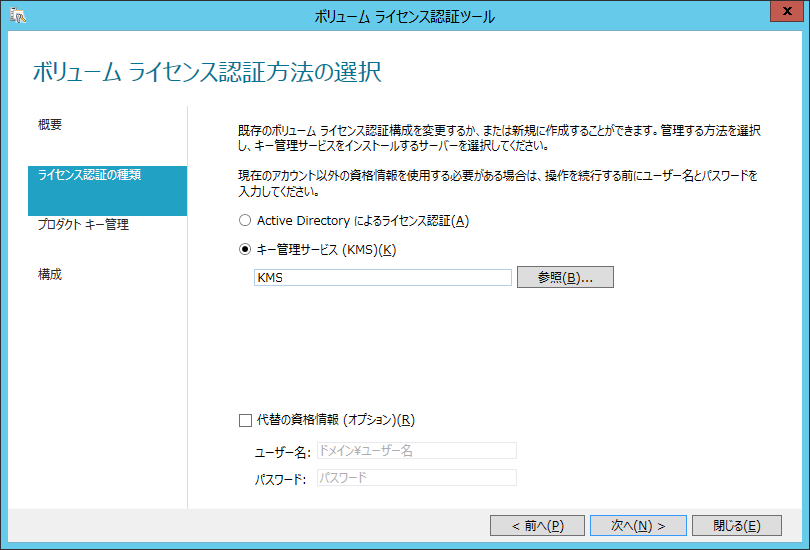
## ****[ボリューム ライセンス認証ツール] を使用したKMS ホストの****設定

[ボリューム ライセンス認証ツール] を使用してKMSホストの構成を行います。

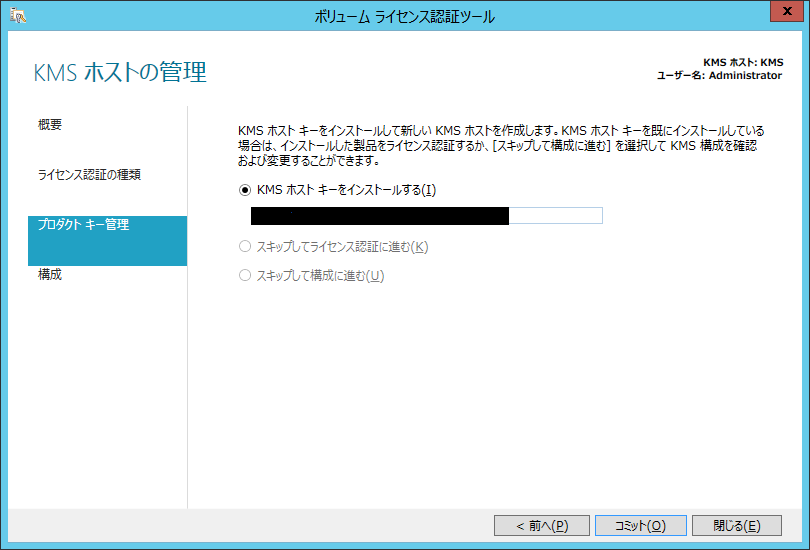
1. **[ボリューム ライセンス認証サービス] 役割をインストールしたコンピューターで、[サーバー   
   マネージャー] を起動します。**
2. **[ツール] メニューの [ボリュームライセンス認証ツール] をクリックします。**
3. **[ボリューム ライセンス認証ツール] が起動したことを確認し、[次へ] ボタンをクリックします。**



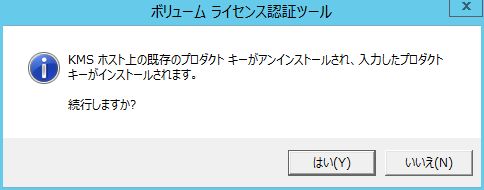
1. **[ボリュームライセンス認証方法の選択] ページで、[キー管理サービス（KMS）] を選択し、KMS ホストとして構成するコンピューターの名前を入力して、[次へ] ボタンをクリックします。**

****

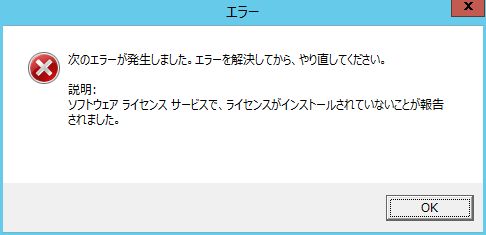
1. **[KMS ホストの管理] 画面で、[KMS キーをインストールする] が選択されていることを  
   確認し、KMS キーを入力して [コミット] ボタンをクリックします。**



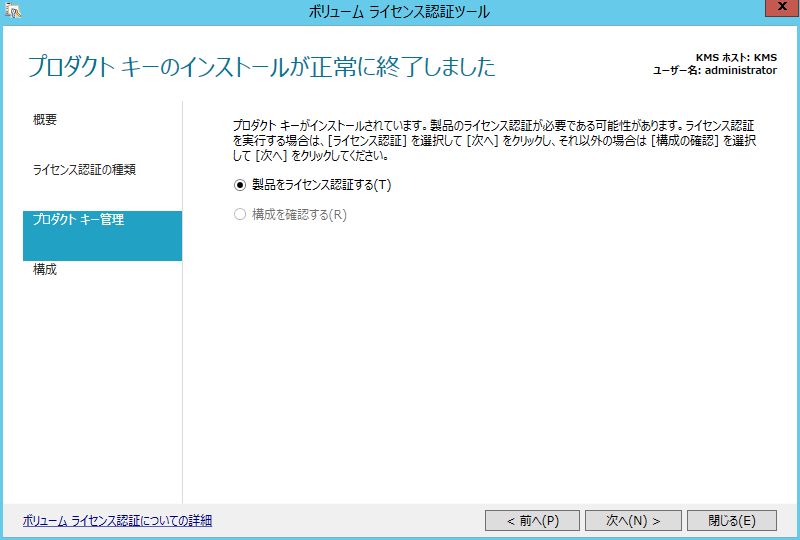
1. **[ボリューム ライセンス認証ツール] メッセージ ボックスが表示されたことを確認し、  
   [はい] ボタンをクリックします。**



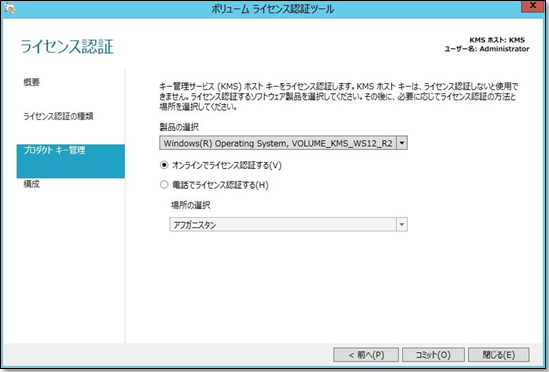
無効なキーを入力した場合は次のようなメッセージ ボックスが表示されます。



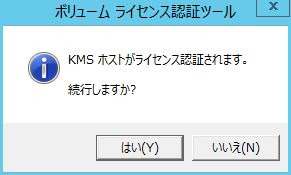
1. **[プロダクト キーのインストールが正常に終了しました] ページで、[製品をライセンス認証する] が選択されていることを確認して、[次へ] ボタンをクリックします。**



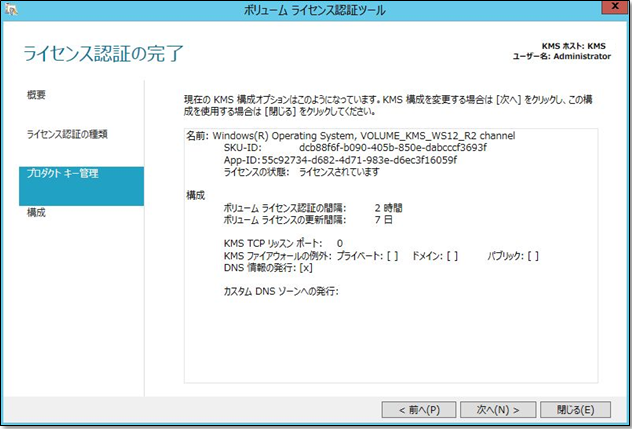
1. **[ライセンス認証] ページで、[オンラインでライセンス認証する] が選択されていることを  
   確認し、[コミット] ボタンをクリックします。**



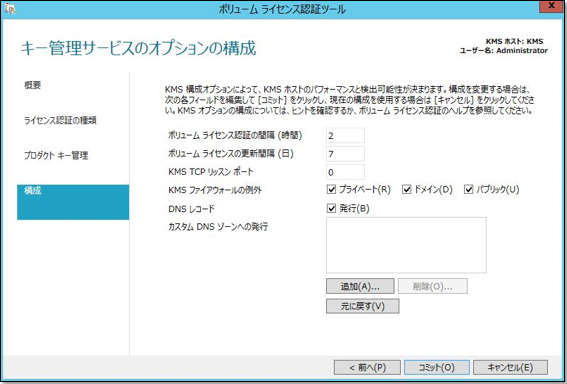
1. **続行を確認するメッセージ ボックスが表示されたことを確認し、[はい] ボタンをクリックします。**



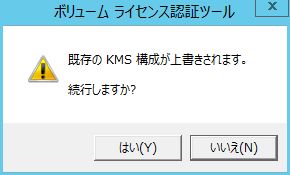
1. **[ライセンス認証の完了] ページで、[次へ] ボタンをクリックします。**

****

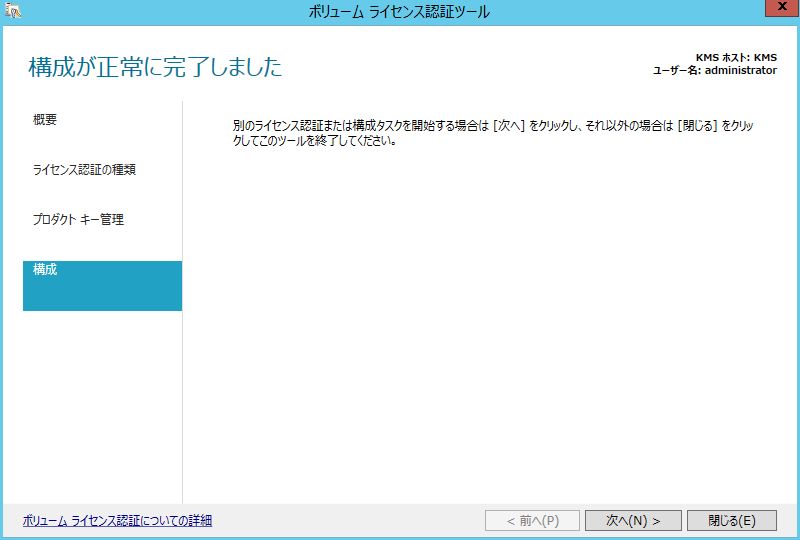
1. **[キー管理サービスのオプションの構成] ページで、KMS のオプション構成を行います。  
   既定では、[KMS ファイアウォールの例外] がすべてオフになっています。  
   [プライベート]、[ドメイン]、[パブリック] の 3 つのチェック ボックスをオンにし、[コミット] ボタンをクリックします。**

****

1. 既存の構成を上書きすることを確認するメッセージ ボックスが表示されたことを確認し、[はい] ボタンをクリックします。



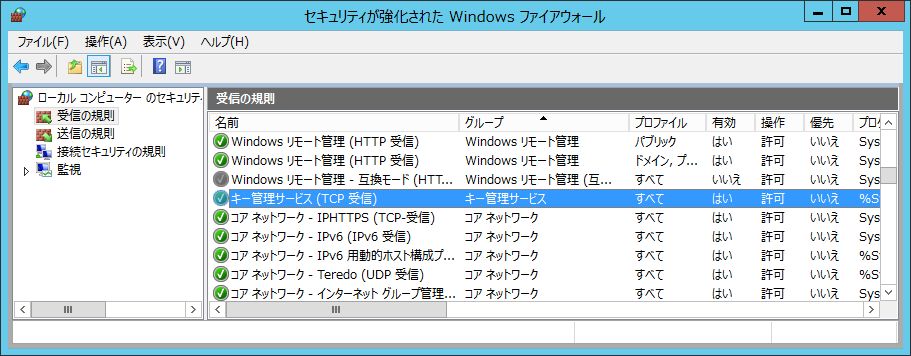
1. [構成が正常に完了しました] ページで、[閉じる] ボタンをクリックします。



## KMSホストファイアウォールの設定

KMS ホストと KMS クライアントで、ライセンス認証が正常に行えるように、KMS ホストで TCP 1688ポートの受信が許可されているかを確認します。

1. **[サーバー マネージャー] を起動し、[ツール] メニューの [セキュリティが強化された indows   
   ファイアウォール] をクリックします。**
2. **[受信の規則] の [キー管理サービス] が許可されていることを確認します。**

****

# Windows 10 を使用した KMS ホストの構成手順（クライアント VL）

ここでは、Windows 10 を実行するコンピューターを、KMS ホストとして構成する方法について、ステップ バイ ステップで確認します。

## 必要とする環境

構成に必要な環境は、次の通りです。

この手順はWindows Server 2012 R2 でも同様です。

* KMS ホストに Windows 10 を使用する。
* 組織内に Active Directory ドメインが構築され、[Active Directory 統合] ゾーンで、DNS サーバーが構築されている。
* KMS による認証を行うクライアントコンピューターのネットワーク設定で、KMS ホストの解決が可能な DNS サーバーの IP アドレスが指定されている。
* KMS ホストは、インターネット接続が可能である。

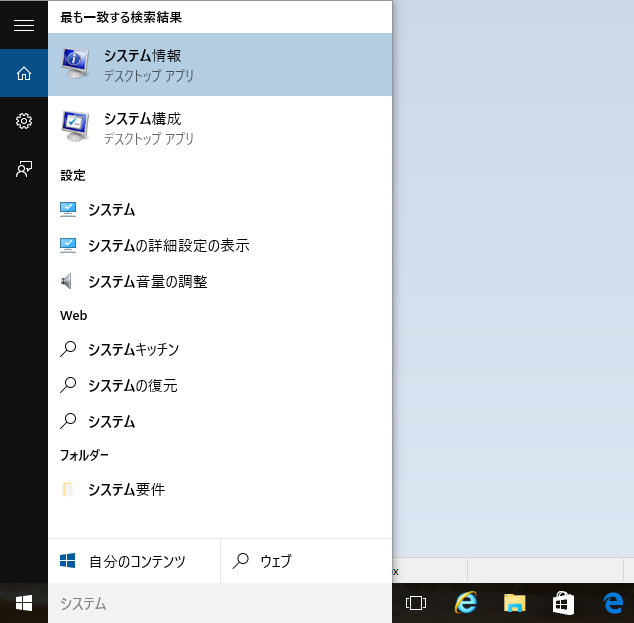
## KMS ホストの初期設定

KMS ホストとして構成するコンピューターに、Windows 10 を新規インストールし、次の設定を  
行います。

Windows 10 では、Administrator アカウントが既定で無効になっています。

Administrator アカウントを使用してサインインするには、管理者権限のあるユーザー アカウントでサインインし、Administrator アカウントを有効化する必要があります。

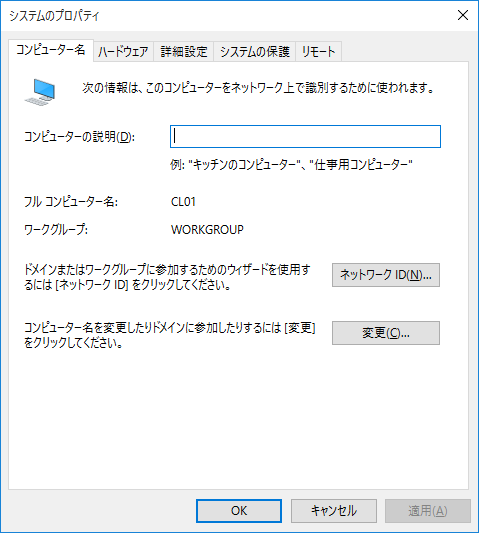
1. ボリュームライセンス メディアを使用して、Windows 10 をインストールします。
2. 管理権限を持つユーザー アカウントでサインインし、コンピューター名や IP アドレスなど、  
   必要な初期設定を行います。
3. ドメインに参加していない場合や、DHCP サーバーから DNS サフィックスを取得していない  
   場合は、DNS サフィックスを登録しますので、次の手順を実行します。  
   タスクバーの、[Web と Windows を検索]ボックスに、「システム」と入力し、[最も一致する検索結果] の一覧から、[システム] をクリックします。



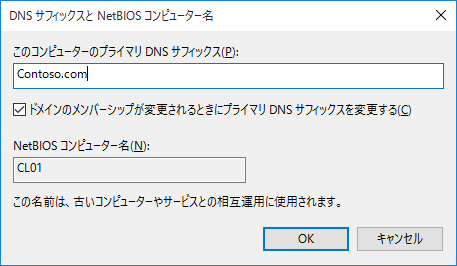
1. [システム] ウィンドウが表示されたことを確認し、[コンピューター名、ドメインおよびワーク   
   グループの設定] の、[設定の変更] をクリックします。



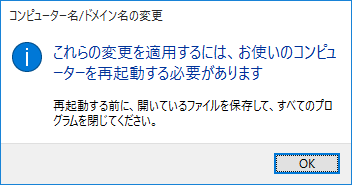
1. [システムのプロパティ] ダイアログ ボックスの [コンピューター名] タブが表示されたことを  
   確認し、[変更] ボタンをクリックします。



1. [コンピューター名/ドメイン名の変更] ダイアログ ボックスが表示されたことを確認し、[詳細] ボタンをクリックします。
2. [DNS サフィックスと NetBIOS コンピューター名] ダイアログ ボックスが表示されたことを  
   確認し、[このコンピューターのプライマリ DNS サフィックス] ボックスにドメイン名を入力して、[OK] ボタンをクリックします。



1. [コンピューター名/ドメイン名の変更] ダイアログ ボックスで、[OK] ボタンをクリックします。
2. 再起動をする必要があるという内容のメッセージボックスが表示されたことを確認し、  
   [OK] ボタンをクリックします。



1. [システムのプロパティ] ダイアログ ボックスで、[閉じる] ボタンをクリックします。
2. コンピューターの再起動を促すメッセージボックスが表示されたことを確認し、[今すぐ再起動  
   する] ボタンをクリックします。

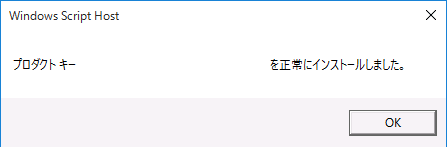
## KMS ホストのライセンス認証

KMS ホストに、KMS キーをインストールしてライセンス認証を実行します。ライセンス認証を実行することで、KMS ホストとして稼働します。

1. KMS ホストとなるコンピューターに KMS ホストの管理者となるユーザー アカウントで  
   サインインオンします。
2. コマンドプロンプトを管理者として実行します。
3. 次のコマンドを実行して、KMS キーをインストールします。

slmgr -ipk < KMS キー>

1. キーが正常にインストールされたことを示す、メッセージ ボックスが表示されたことを確認し、[OK] ボタンをクリックします。

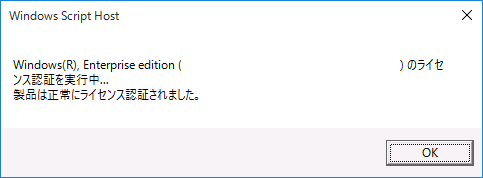


1. オンライン、もしくは電話を使用して、KMSホストのライセンス認証を行います。

* オンラインでライセンス認証を行うには、以下のコマンドを実行します。

slmgr /ato

正常にライセンス認証が行われたという内容のメッセージが表示されたことを確認し、[OK]ボタンをクリックします。



* 電話でライセンス認証を行うには、以下の手順を実行します。
  1. 以下のコマンドを実行し、OS のインストール ID を確認します。

slmgr /dti



( )

※ この後の手順でインストール ID を使用します。

メモ帳などのテキスト エディターにコピーし、以下のように 6 桁毎もしくは 7 桁毎に区切っておいていただくことをお勧めいたします。

(例)

xxxxxx-xxxxxx-xxxxxx-xxxxxx-xxxxxx-xxxxxx-xxxxxx-xxxxxx-xxxxxx

② ライセンス認証窓口 (0120-801-734) に電話します。

電話の音声ガイダンスに従って、手順 ① で確認したインストール ID を電話機で入力します。

③ 電話の音声ガイダンスに従って操作し、応答のあった OS 認証用の確認 ID (48 桁)を書き留めま

す。

※ この後の手順で確認 ID (48 桁) を使用します。いったん、メモ帳などのテキスト エディターに入力しておいていただくことをお勧めいたします。6 桁毎の区切り文字は不要です。

(例)

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

④ 以下のコマンドを実行し、指定した確認 ID を使用してライセンス認証を行います。

 slmgr /atp <確認 ID>

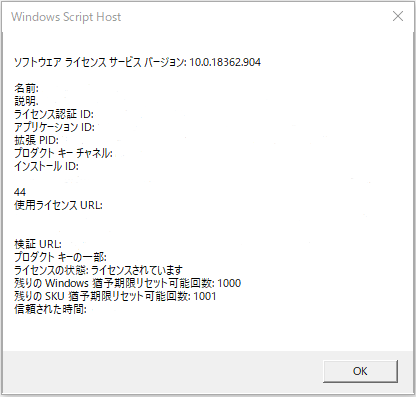
(例)

　　　　 slmgr.vbs /atp xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

⑤ 以下のコマンドを実行し、「ライセンスの状態」が "ライセンスされています" と記

載されていることを確認します。

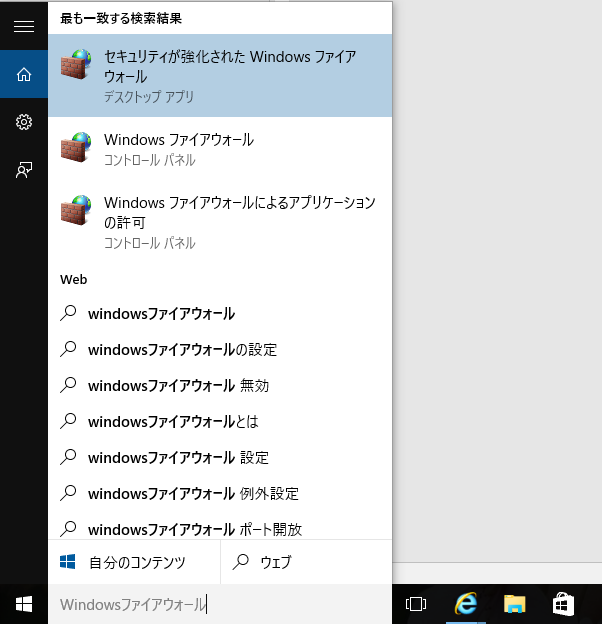
slmgr /dlv



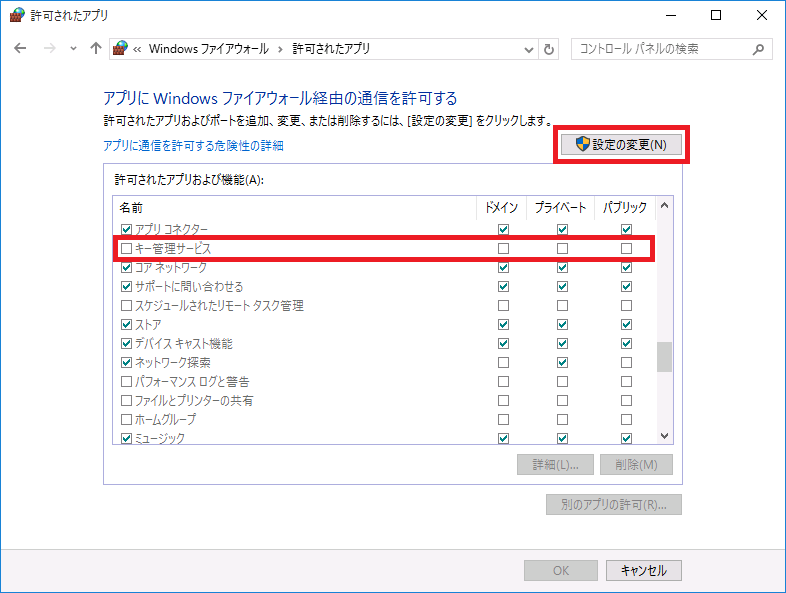
## KMSホストのファイア ウォール設定

KMS ホストと KMS クライアントでライセンス認証が正常に行えるように、TCP 1688 ポートで  
通信が行える状態かを確認します。

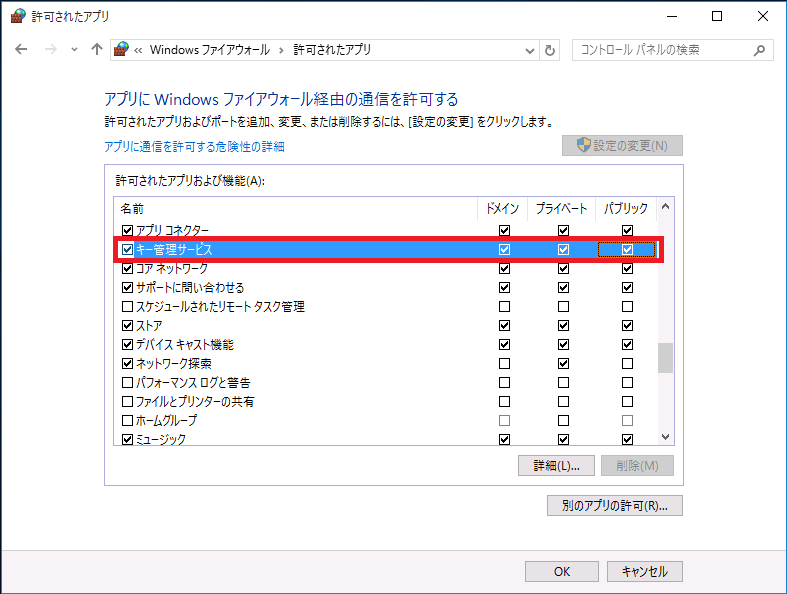
1. タスクバーの、[Web と Windows を検索]ボックスに、「Windowsファイアウォール」と  
   入力し、[最も一致する検索結果] の一覧から、[Windows ファイアウォール] を  
   クリックします。



1. [Windows ファイア ウォール] ウィンドウが表示されたことを確認し、[Windows ファイア  
   ウォールを介したアプリまたは機能を許可] をクリックします。
2. 許可されたアプリに [キー管理サービス] という項目が追加されていることを確認し、[設定の変更] をクリックします。



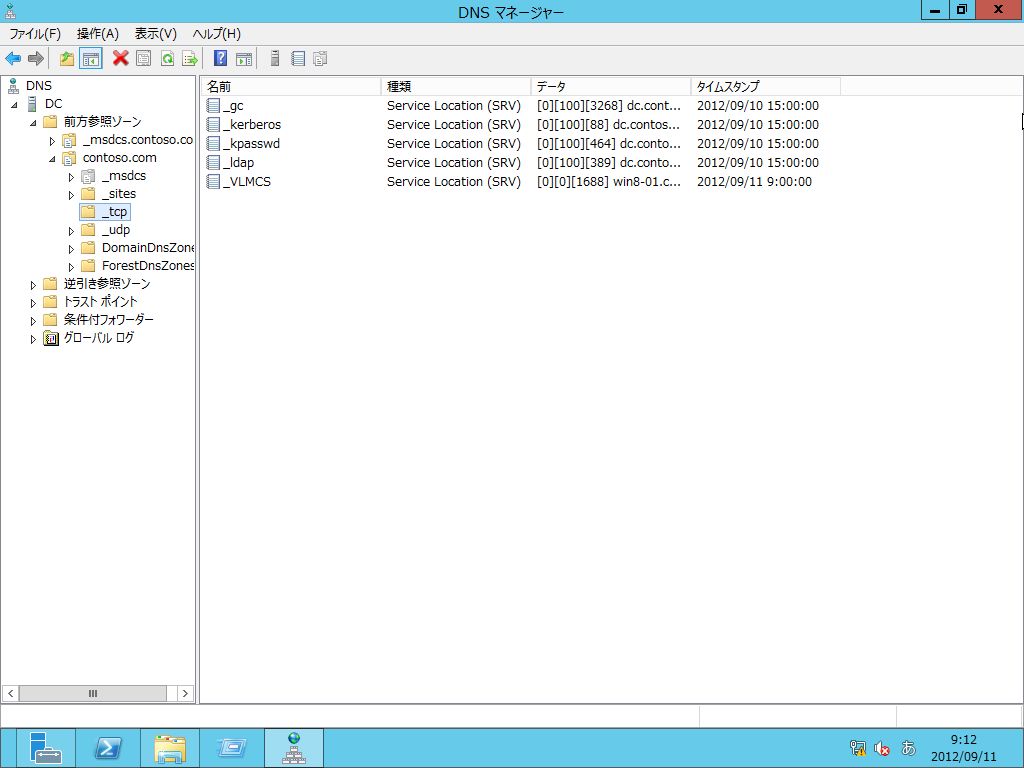
1. [キー管理サービス] のドメイン、プライベート、パブリックのすべてのチェックボックスをオンにし、 [OK] ボタンをクリックします。



## DNS サーバーで SRV レコードの確認 (ドメインに参加する KMS ホストの場合)

ドメインに参加する KMS ホストの場合、自動発行された SRV レコードが、DNS サーバーに  
登録されているかを確認します（Active Directory によるライセンス認証の場合は、  
必要ありません）。

1. DNS サーバーを実行するコンピューターに、管理者アカウントを使用してサインインします。
2. [サーバーマネージャー] の、[ツール] - [DNS] をクリックします。
3. [DNS マネージャー] が起動したことを確認し、KMS ホストがドメイン参加しているゾーンを  
   展開して、[\_tcp] をクリックします。  
   [\_VLMCS] というSRVレコードが存在することを確認します。



## 参考：SRV レコードの手動作成

次の場合KMS ホストを発行するために SRV レコードを手動で作成する必要があります。

* ワークグループで KMS ホストを構築した場合
* DDNS(動的更新) がサポートされていない場合
* SRV レコードの動的登録に失敗した場合

注意

DDNS をサポートしていない環境では、すべての KMS ホストでの発行を無効にして、DNS の発行に失敗した  
イベントがイベント ログに記録されないようにします。自動発行を無効にするには、Slmgr スクリプトを /cdns オプションと共に使用します。

手動で作成した SRV レコード を、KMS ホストが他のドメインで自動発行した SRV レコードと共存させることができますが、その場合、すべてのレコードを管理して競合を回避する必要があります。

### Windows Server を実行する DNSサーバーを使用した SRV レコードの手動作成

[DNS マネージャー] を使用して、適切な前方参照ゾーンで新しい SRV レコード を作成します。既定では、KMS は TCP ポート 1688 をリッスンし、サービスは \_VLMCS です。

表 2 に SRV レコードの設定例を示します。

|  |  |
| --- | --- |
| 名前 | 設定 |
| サービス | \_VLMCS |
| プロトコル | \_TCP |
| ポート番号 | 1688 |
| サービスを提供しているホスト | KMS ホストの完全修飾ドメイン名 (FQDN) |

表 2 SRV レコード

### BIND 8.2 以降の DNS サーバーを使用した SRV レコードの手動作成

組織で BIND 8.2 以降の DNS サーバーを実行している場合、必要な SRV レコードを作成できます。レコードを作成する場合、表 3 に示した情報を指定します。

|  |  |
| --- | --- |
| 名前 | 設定 |
| 名前 | \_vlmcs.\_tcp |
| 種類 | SRV |
| 優先度 | 0 |
| 重み | 0 |
| ポート | 1688 |
| ホスト名 | KMS ホストの FQDN |

表 3 SRV レコード情報

KMS の自動発行をサポートするように BIND 8.2 以降の DNS サーバーを構成するには、KMS ホストからの RR 更新を有効にするように BIND サーバーを構成します。

たとえば、named.conf 内のゾーン定義に次の行を追加します。

allow-update { any; };

allow-update ステートメントを named.conf.options に追加して、このサーバー上でホストされるすべてのゾーンで DDNS を有効にすることができます。

### 追加のドメインに、KMS ホストの SRV レコードを自動的に発行する

既定では、KMS ホストは、所属している DNS ドメインにのみ登録されます。

ネットワーク環境内に DNS ドメインが 1 つのみである場合、これ以上の操作は必要ありません。

一方、DNS ドメインが複数存在する場合、SRV レコードを発行する際に使用する   
DNS ドメインの一覧を作成できます。この設定を行うと、プライマリ DNS サフィックスとして指定されたドメインにのみ発行する KMS ホストの既定の動作が中断します。

必要に応じて、優先度および重みなどを KMS の **DnsDomainPublishList** レジストリ値に追加します。この機能を使用すると、各グループ内に KMS ホスト優先度グループと  
重みを設定し、1 台目の KMS ホストを定義し、複数の KMS ホストで負荷分散を行うことができます。

DNS に対する変更は、すべての DNS サーバーの複製が完了するまで反映されない場合があります。

変更を頻繁に行うと ([時間] < [レプリケーション時間])、複製が完了していないサーバー上で変更を行った場合に古いレコードが残る可能性があります。

KMS ホストの SRV レコードを発行する各 DNS ドメインのサフィックスの登録は、  
次のレジストリキーを使用します。

**HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion  
\SoftwareProtectionPlatform**   
値の名前 : DnsDomainPublishList  
種類 : REG\_MULTI\_SZ （複数行文字列値）  
値のデータ : KMS が発行する各 DNS ドメインを別の行に入力します。

複数のドメインに発行するように KMS ホストを構成したら、レジストリ サブキーをエクスポートし、追加の KMS ホスト上のレジストリにインポートします。

Software Licensing サービスを再起動すると、レコードが直ちに作成されます。

アプリケーション ログには、発行が成功したドメインごとに 1 つの 12294 イベント、  
また発行が失敗したドメインごとに 1 つの 12293 イベントが記録されます。

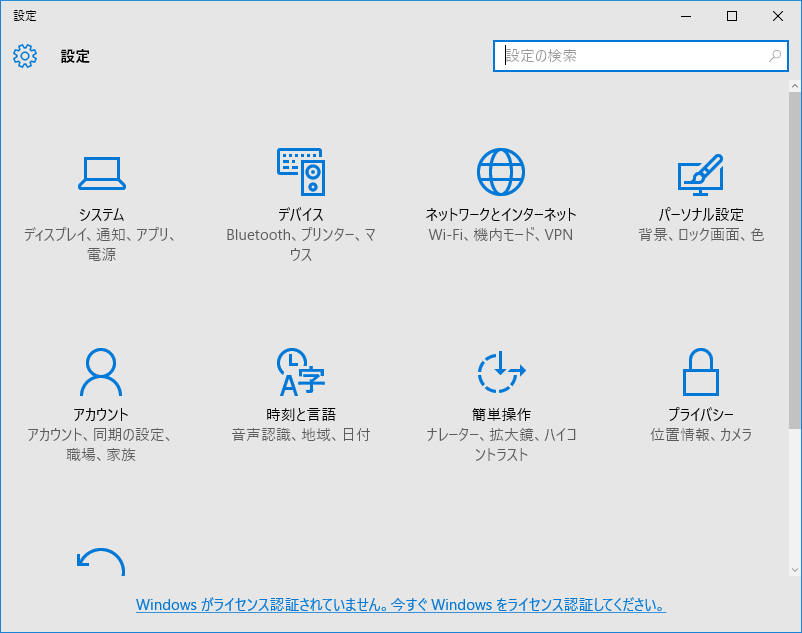
# Windows 10 のライセンス認証

ボリュームライセンス版の Windows 10 をインストールした後、ライセンス認証を行う必要が  
あります。ただし、Active Directory によるライセンス認証や KMS ライセンス認証を導入している場合は自動的に認証が行われるため、1 台ずつライセンス認証を行う必要はありません。

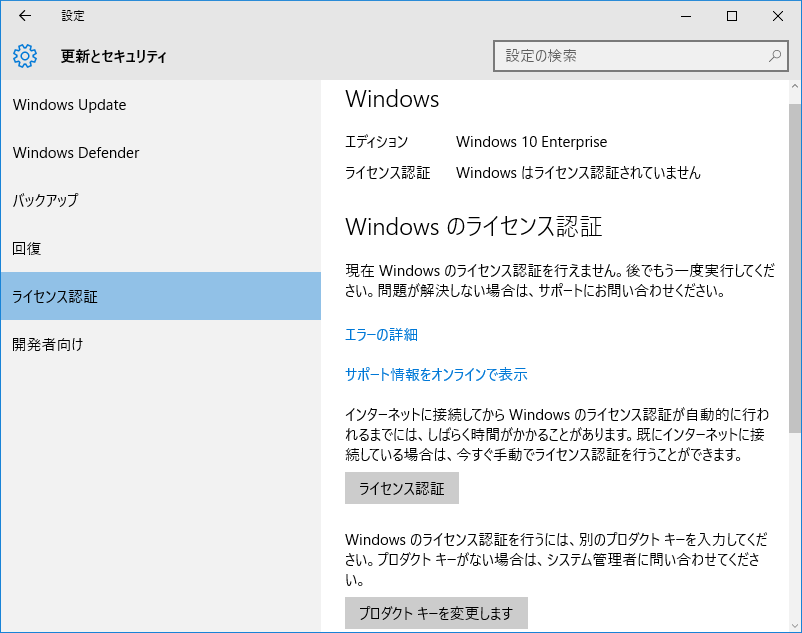
## ライセンス認証が行われていない状態を確認する

Windows 10 を実行しているコンピューターでライセンス認証が行われているかを確認します。

1. [スタート]-[設定] をクリックします。
2. [設定] ウィンドウの下部に、ライセンス認証が行われていないことを示すメッセージが表示されていることを確認します。



1. [更新とセキュリティ] をクリックします。
2. [更新とセキュリティ] ウィンドウで、[ライセンス認証]をクリックします。  
   ライセンス認証を行うための画面が表示されます。



ライセンス認証を行わないと、ユーザーの画像を登録するなどのパーソナル設定を行うことができません。

ライセンス認証を行わない状態で、しばらくするとデスクトップ画面右下にライセンス認証を促すウォーター  
マークが表示されます。これにより、ライセンス認証が行われていないことを、ユーザーが認識します。

## ライセンス認証の実行

ここでは、MAKによるライセンス認証の実行方法を確認します。

### MAK による認証

既定では、KMS クライアントセットアップキー（GVLK）が登録されているため、MAK によるライセンス認証を行うためには、MAK キーを Windows 10 に入力しなくてはいけません。

MAK キーを入力せずに、ライセンス認証を行うと、KMS による認証を試行します。

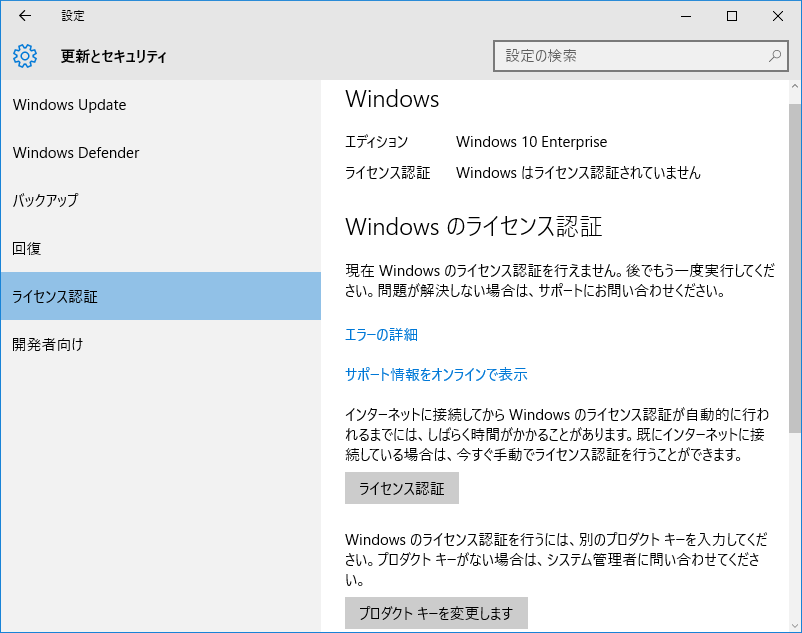
KMS ホストが存在しない場合、ライセンス認証は失敗します。

MAK キーを入力するためには、次の手順を実行します。

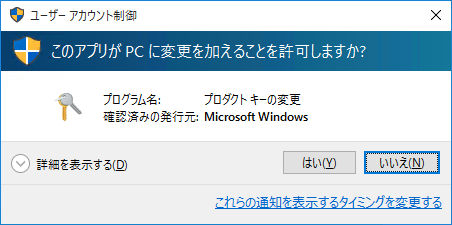
1. 管理者権限のあるユーザーでサインインし、コマンドプロンプトを起動します。
2. 次のコマンドを実行します。

slui 3

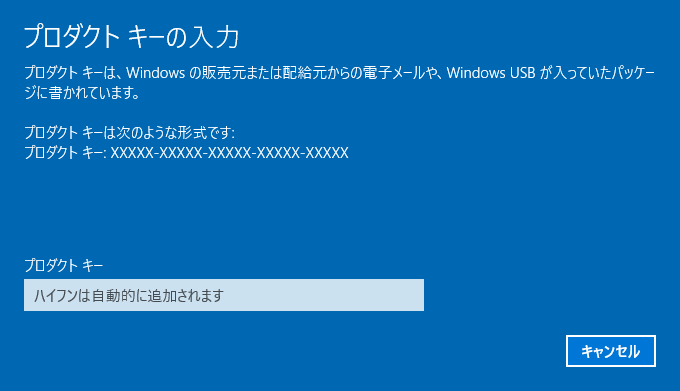
[更新とセキュリティ] ウィンドウで、[ライセンス認証]をクリックし、[プロダクト キーを変更します] ボタンを  
クリックしても、プロダクト キーの入力を行うことができます。



1. [ユーザー アカウント制御] ダイアログ ボックスが表示された場合は、[はい] ボタンを  
   クリックします。



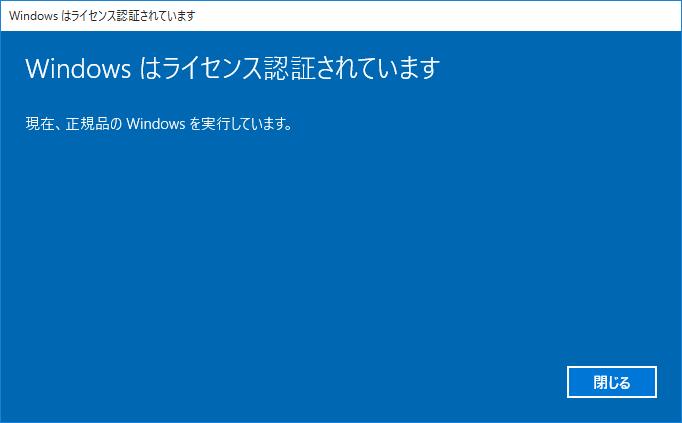
1. [プロダクト キーの入力] 画面が表示されたことを確認し、MAK キーを入力します。



1. [Windowsのライセンス認証] 画面で、[次へ] ボタンをクリックします。



1. ライセンス認証が行われたことを確認し、[閉じる] ボタンをクリックします。



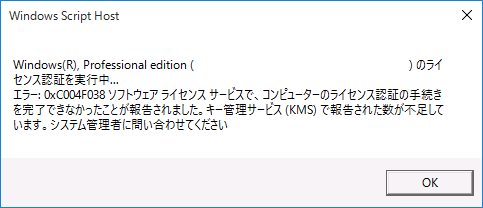
次のスクリプトを実行することにより、プロダクトキーの入力とライセンス認証を行うこともできます。

slmgr /ipk <ライセンスキー>

slmgr /ato

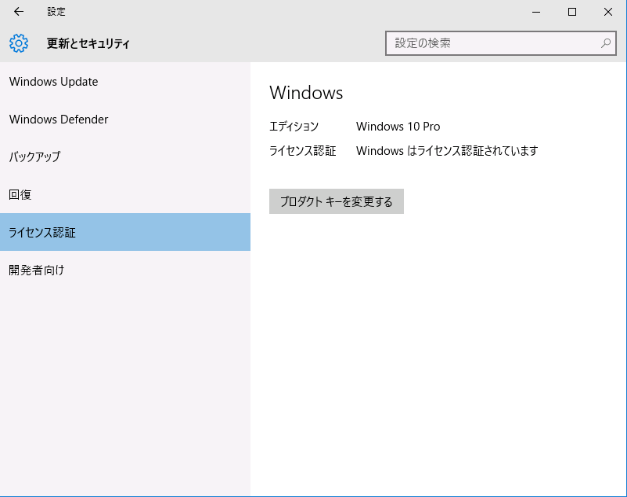
### KMS ホストに認証されない

KMS ホストのライセンス認証のしきい値の要件を満たしていない状態で、ライセンス認証を行うことはできません。KMS の規定台数を満たしていない状態で、「slmgr /ato」 スクリプトを実行して、ライセンス認証を行うと、下図のようなメッセージ ボックスが表示されます。



### ライセンス認証後の確認

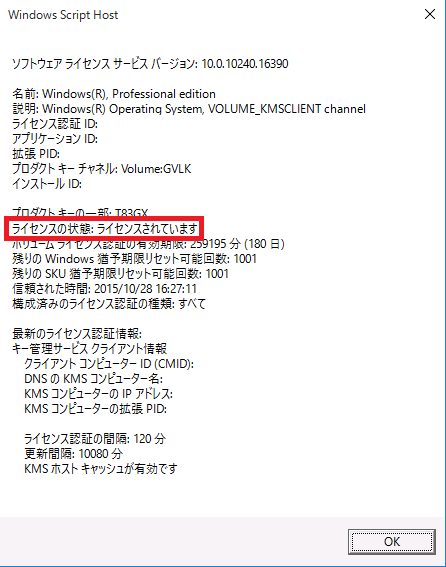
KMS ホストのライセンス認証のしきい値の要件を満たした状態でライセンス認証を行うと  
次のようになります。



また、スクリプトを使用してライセンス認証の状態を確認するには、次のコマンドを実行  
します。

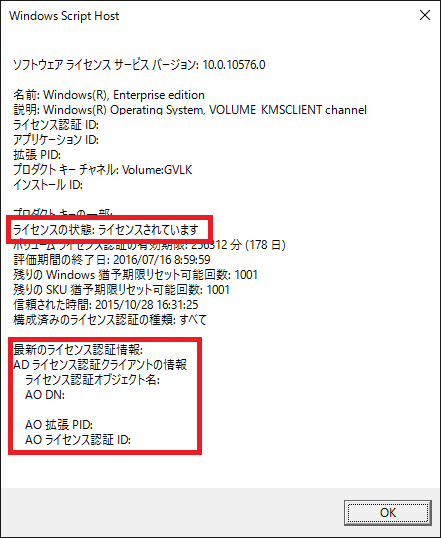
slmgr /dli

下図のような、ダイアログボックスが表示され、ライセンス認証の状態が確認できます。



Active Directory によるライセンス認証の状態を確認するには、次のコマンドを実行  
します。

slmgr /dlv



# ボリューム アクティベーションの管理

ボリューム アクティベーションにおいて、Active Directory によるライセンス認証サービスや KMS ホストが正常に動作しているかを監視、確認する必要があります。

管理、運用を行う主なツールとして、イベント ビューアー、ボリューム ライセンス認証サービスおよびスクリプトがあります。イベント ビューアーを使用して、SRV レコードの発行要求の確認、ライセンス認証要求、更新、および応答などを確認することができます。

ボリュームライセンス認証サービスでは、認証の種類ごとに、次のことを行うことができます。

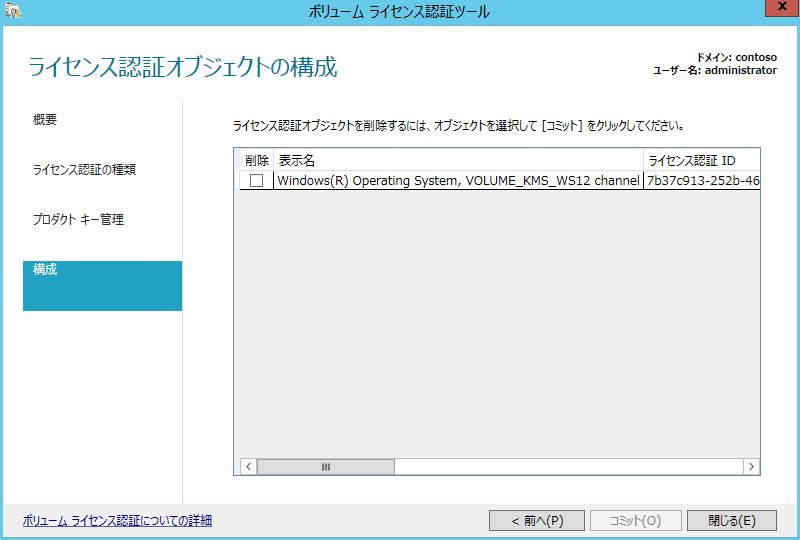
* Active Directory によるライセンス認証
* ライセンス認証オブジェクトの削除
* KMS ホストによるライセンス認証
* ボリューム ライセンス認証の間隔を設定
* ボリューム ライセンスの更新間隔を設定
* KMS TCP リッスン ポートの設定
* KMS ファイアウォールの例外設定
* DNS レコードの発行
* カスタム DNS ゾーンへの発行

また、スクリプトを使用することによって、KMS ホスト、KMS クライアント、Active Directory   
によるライセンス認証の管理ができます。

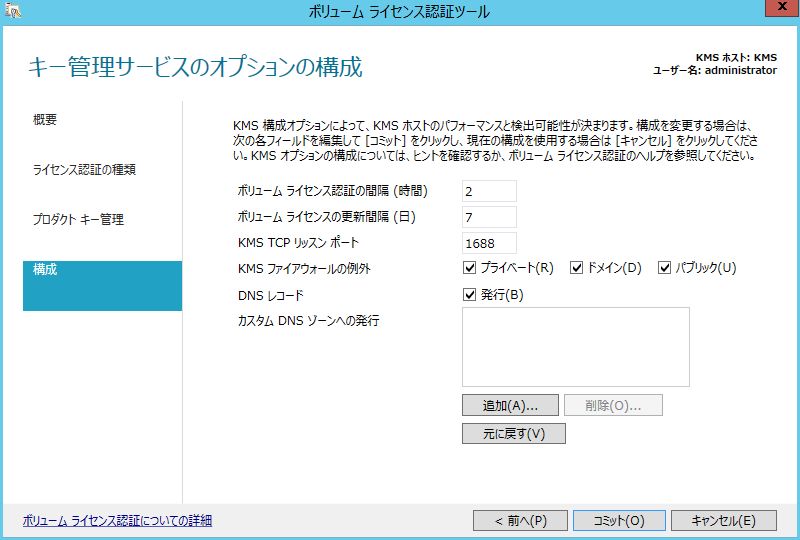
例えば、KMS ホストの動的検出を可能にする DNS サーバーが存在しない場合、KMS クライアントが利用する KMS ホストの完全修飾ドメイン名（FQDN）の登録などを行います。

## ボリューム ライセンス認証サービスによる管理

[ボリューム ライセンス認証ツール] を使用すると、Active Directory によるライセンス認証では、ライセンス認証オブジェクトの削除を行うことができます。



また、KMS ホストの構成を [ボリューム ライセンス認証ツール] を使用して行うことができます。



[ボリューム ライセンス認証ツール] を使用して行うことができる KMS ホストの構成に関する  
詳細は、下表のとおりです。

|  |  |
| --- | --- |
| メニュー項目 または操作 | 構成 |
| キー管理サービス オプションの構成 | * **[ボリューム ライセンス認証の間隔 (時間)]** 期限が近いまたは有効期限が切れたライセンスの再認証を試行するために クライアントが使用する間隔です。既定値は 2 時間です。 （この値はレジストリに直接設定する場合、分単位で指定します。） * **[ボリューム ライセンスの更新間隔 (日)]** 初めてのボリューム ライセンスの認証後、ライセンスを更新するためにクライアントが 使用する間隔です。 （この値はレジストリに直接設定する場合、分単位で指定します。）   これらの値は、ライセンス認証が成功したときに KMS ホスト内の値によって上書きされます。   * **[KMS TCP リッスン ポート]** パブリック アドレス、プライベート アドレス、ドメイン アドレスに関するオプションが含まれます。既定では、クライアントは RPC 要求を 1688/TCP を使って KMS ホスト サーバーに送信します。 * **[KMS ファイアウォールの例外]** 例外は、パブリック ネットワークまたはプライベート ネットワークに追加できます。既定では、すべての例外が無効になっています。必要に応じて、このオプションを使って代替 TCP リッスン ポートを構成できます。 * **[DNS レコード]** KMS が開始されるたび、および 1 日に 1 回、KMS によってサービス (SRV) リソース レコードがドメイン ネーム システム (DNS) に登録されます。KMS クライアント コンピューターは、構成済みのレジストリ エントリから、または DNS 内の KMS SRV レコードを介して、KMS ホスト サーバーを検出します。 * **[カスタム DNS ゾーンへの発行]** 必要に応じて、この設定を使ってカスタムの DNS ゾーンを追加します。既定では、プライマリ DNS サフィックスにのみ公開します。カスタムの DNS 値が設定されている場合、クライアントはこのリストで定義されているゾーンにのみ転送されます。 |
| KMS の構成変更 の確認 | 選択した構成オプションを検証し、変更を受け入れて直前の画面に戻ってさらに変更を 加えるか、[元に戻す] をクリックして以前の設定を復元します。 |

表 4 KMS ホストの構成

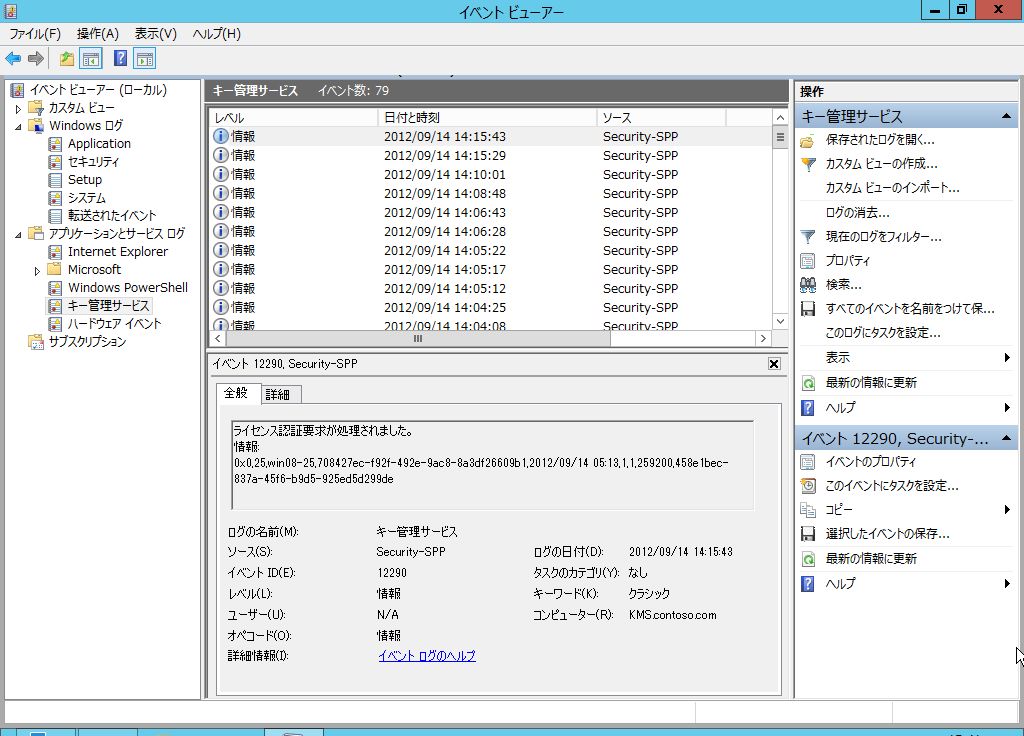
## イベント ビューアーによる確認

ボリューム ライセンス認証サービスおよび KMS サービスは、認証にかかわるすべてのアクションを  
クライアント コンピューターとホスト コンピューターにイベント ログとして記録します。

クライアントは、Microsoft Windows Security Licensing (SLC) イベント ID 12288 ～ 12289 を使用して、ライセンス認証要求、更新、応答をApplication ログに記録します。

また、KMS クライアントからのライセンス認証要求を KMS ホストで処理したかを確認するには、KMS ホストのイベント ログを確認します。これらのログは、[アプリケーションとサービスログ]-[キー管理サービス] に記録されます。

KMS ホストおよびドメイン コントローラーは、クライアントから受信した要求ごとに、別個のエントリを SLC イベント ID 12290 として記録します。



複数の KMS ホストが配置されている場合、個別にライセンス認証のログが保持されます。

KMS ホスト間でのログの複製は行われません。

## KMS ホストから DNS サーバーに対して、SRV レコードの発行要求の確認

[イベントビューアー] を起動し、[Windows ログ]-[Application] を選択します。

イベントIDが、「12294」 のイベントを確認します。



正常に発行した場合は、イベント ID 12294が発行されますが、発行できなかった場合は 12293が発行されます。  
その際は手動でDNS サーバーに SRV レコードの登録をする必要があります。

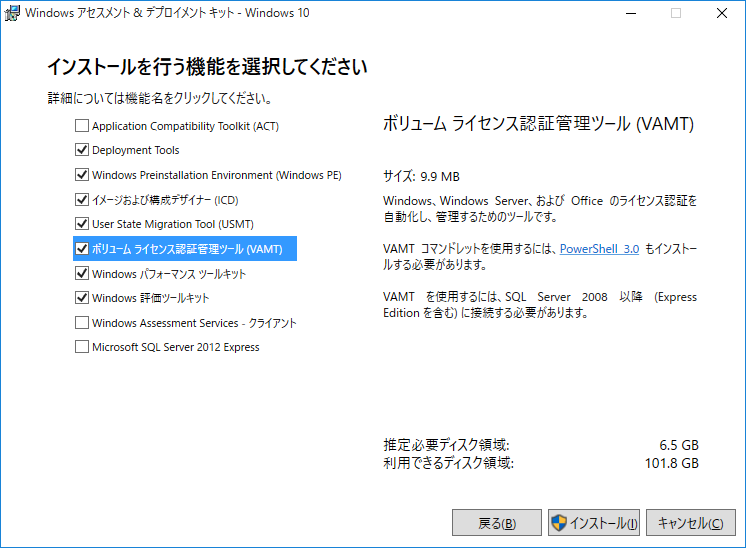
## MAK / KMS キーが認証上限数を超えてしまった際の対処方法

MAK / KMS キーには認証の上限値が設定されており、上限に達するとライセンス認証ができなくなります。

KMS キーが上限に達してしまった場合、KMS ホストのライセンス認証ができなくなります。

それにより、KMS ホストが、KMS クライアントの認証を行えなくなりますので注意が必要です。

それぞれのキーの上限はプロダクト キー ページ、またはWindows 10 用 Windows アセスメントデプロイメントキット (Windows ADK) に付属のボリューム ライセンス認証管理ツール (VAMT) で確認できます（KMSホストキーの認証回数は除く）。



Windows 10 用 Windows アセスメントデプロイメントキット (Windows ADK)   
http://go.microsoft.com/fwlink/p/?LinkId=526740

ライセンス キーの上限に達する場合、次のようなシナリオが考えられます。

* MAK キーを使用していたが、企業で使用しているコンピューターが故障したため、Windows を再インストールし、再度ライセンス認証しようとしたが、MAK キーの上限に達してしまい認証ができない。
* 検証環境など、一時的に使用するコンピューターを、MAK キーが入力されたマスターイメージから必要に応じて展開して使用しているが、展開と同時にライセンス認証されるため MAK キーの上限に達してしまった。
* KMS キーをMAK キーと間違えて、KMS ホストではなく、一般のサーバーに使用してしまい KMS キーの上限に達してしまった。
* KMS ホストを KMS キーの上限以上に構築してしまった。

ライセンス認証の上限に達してしまった際の対処方法は、ライセンス認証専用窓口に電話で  
問い合わせる、もしくは Web サイトから申請を行います。

### 電話での問い合わせ

国や地域ごとにライセンス認証専用窓口が異なるため、以下のWeb ページで電話番号を確認し、問い合わせを行います。

ライセンス認証専用窓口  
<http://www.microsoft.com/ja-jp/licensing/existing-customers/activation-centers.aspx>

### Web ページでの申請

マイクロソフトでは、ライセンス認証の上限に達してしまった際、上限数の変更を行うための申請ページを用意しています。申請フォームの入力項目は次の通りです。

* 会社名
* 名前
* 電子メールアドレス
* 該当のライセンスプログラム名
* 契約番号
* Open License  
  ライセンス番号(数字 8 桁)
* Select Plus  
  パブリックカスタマーナンバー(PCN)(英数字 8 桁)
* School Agreement または Campus Agreement  
  加入契約番号(数字 7 桁あるいは 8 桁)または購入申込番号
* その他  
  加入契約番号または契約番号(数字 7 桁または英数字 8 桁)
* 製品名およびエディション、バージョン
* MAK または KMS キー
* MAK または KMS キーの下 5 桁
* 現在の認証上限数
* 変更後の認証上限数
* 申請理由

MAK / KMS 認証上限数変更申請フォーム  
<https://support.microsoft.com/contactus/emailcontact.aspx?scid=sw;ja;1997>

## スクリプトによる管理

ソフトウェア ライセンス マネージャー (Slmgr) は、ボリューム アクティベーション情報を構成および取得するために使用するツールです。ここでは、Slmgr を使用したボリューム アクティベーションの管理について紹介します。

### リモートでの Slmgr の実行

Slmgr をリモートで実行するには、管理者が追加のパラメーターを指定する必要があります。必要なパラメーターは、次の通りです。

* ターゲット コンピューターの名前
* ターゲット コンピューターのローカル管理者のユーザー名とパスワード

ユーザー名とパスワードを指定せずにリモートで実行した場合、スクリプトを実行したユーザーの資格情報が使用されます。

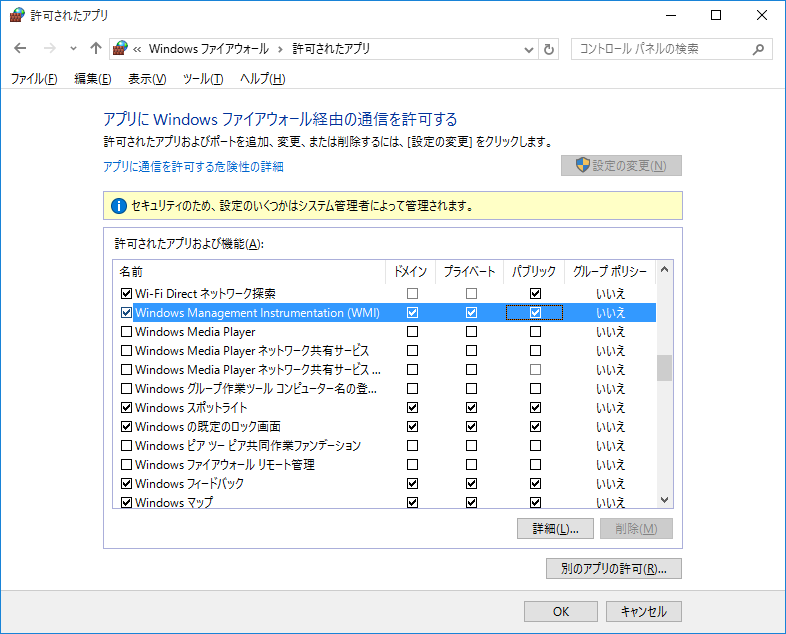
リモートで Slmgr を実行する際、指定する必要があるパラメーターは次の通りです。

slmgr <ターゲット コンピューター名> [ユーザー名] [パスワード] /パラメーター [オプション]

### リモート管理 に必要な Windows ファイアウォールの構成

Slmgr では、Windows Management Instrumentation (WMI) が使用されます。

そのため、管理者は WMI トラフィックを許可するように、管理される側のコンピューターでWindows ファイアウォールの設定を行う必要があります。

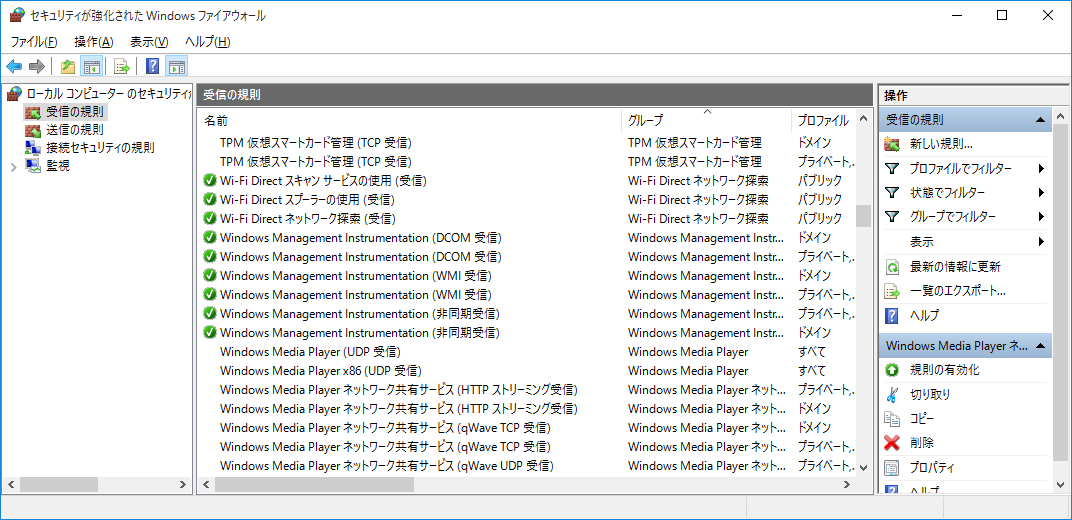


単一のサブネットでは、Windows ファイアウォールで、Windows Management Instrumentation (WMI) 例外を許可します。

複数のサブネット内で WMI トラフィックを許可するには次のWMIを許可する必要が  
あります。

* Windows Management Instrumentation (非同期受信)
* Windows Management Instrumentation (DCOM受信)
* Windows Management Instrumentation (WMI受信)

さらに、複数のサブネット内のリモート アクセスを有効にします。これらの設定を行うには、  
セキュリティが強化された Windows ファイアウォールを使用します。



既定では、プライベートおよびパブリック プロファイルの Windows ファイアウォールの例外は、ローカル   
サブネットからのトラフィックにのみに例外を適用します。例外が複数のサブネットに適用されるように適用範囲を拡張するには、セキュリティが強化された Windows ファイアウォールの例外の設定を変更するか、  
AD DS ドメインに参加している場合は、ドメイン プロファイルを選択します。

### ワーク グループのコンピューターを対象とするリモート操作

管理者は、ワーク グループに所属しているコンピューターに対して、Slmgr をリモートで実行できます。これを行うには、次のレジストリ設定を変更する必要があります。

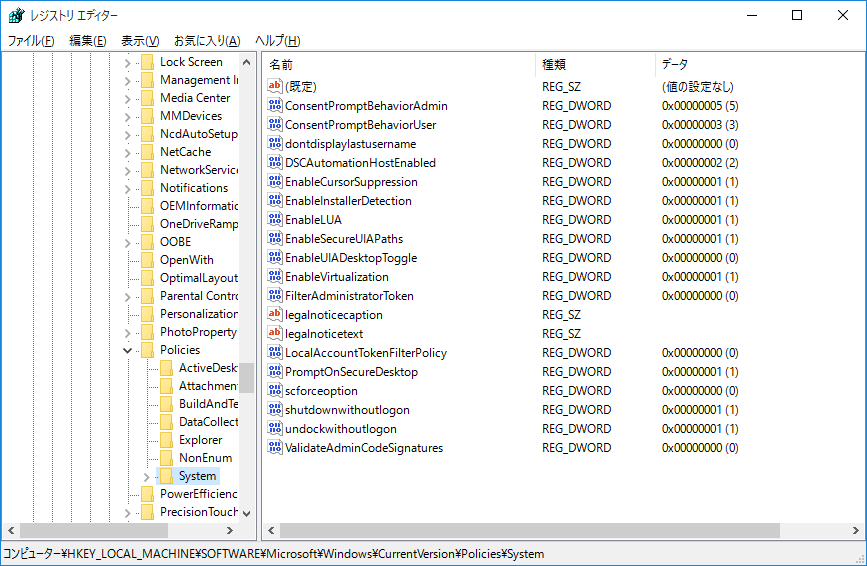
HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

種類：REG\_DWORD

名前：LocalAccountTokenFilterPolicy

データ：0x01

既定では、LocalAccountTokenFilterPolicy は存在しないので作成する必要が  
あります。



### グローバル管理および設定

ここでは、Slmgr のオプションと意味について解説します。

* ライセンスキーのインストール

slmgr /ipk <ライセンスキー>

* Windows のライセンス認証を行う

slmgr /ato

* ライセンス情報を表示する

slmgr /dli

* ライセンスの詳細情報を表示する

slmgr /dlv

* 現在のライセンスの有効期限日を表示する

slmgr /xpr

* レジストリからプロダクトキーを削除する（無断での公開を防ぎます）

slmgr /cpky

* ライセンス認証の種類を変更する

slmgr /act-type <ライセンス認証の種類>

|  |  |
| --- | --- |
| 値 | 種類 |
| 0 | すべてに対応 |
| 1 | Active Directory 認証 |
| 2 | KMS 認証 |
| 3 | Token ベース認証 |

* コンピューターのライセンス状態をリセットする

slmgr /rearm

* オフライン状態でライセンス認証のインストール ID を表示する

slmgr /dti

### Active Directory による認証の設定

ここでは、Slmgr を使用したActive Directoryによる認証の設定について解説します。

* Active Directory フォレストをライセンス認証する

slmgr /ad-activtion-online <プロダクトキー> [ライセンス認証オブジェクト名]

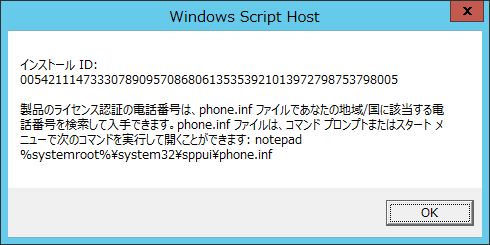
* Active Directory フォレストをライセンス認証する（プロダクトキー＋確認 ID）

slmgr /ad-activtion-apply-cid <プロダクトキー> <確認 ID> [ライセンス認証オブジェクト名]

* Active Directory フォレストのインストール ID を表示する

slmgr /ad-activtion-get-iid <プロダクトキー>

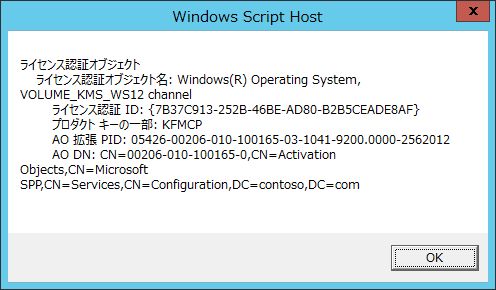
このコマンドを実行すると、下図のようなメッセージボックスが表示され、インストールIDを  
確認することができます。



* Active Directory のライセンス認証オブジェクトを表示する

slmgr /ao-list

このコマンドを実行すると、下図のようなメッセージボックスが表示され、ライセンス認証  
オブジェクトの情報を確認することができます。



* Active Directory のライセンス認証オブジェクトを削除する

slmgr /del-ao <ライセンス認証オブジェクト DN | ライセンス認証オブジェクト RDN>

### KMS ホスト設定

KMSホスト上の使用するTCPポートの設定やDNS発行の有効化/無効化などの設定を行います。

変更を有効にするためにKMS サービス (またはコンピューター) を再起動する必要があります。  
KMS サービス(slsvc.exe) を再起動するには、サービス スナップ インを使用するか、管理者権限で起動したコマンド プロンプトで次のコマンドを実行する必要があります。  
net stop slsvc  
net start slsvc

* TCP通信ポートの設定  
  KMSホストが使用するTCP通信ポートを設定します。

slmgr /sprt <ポート番号>

既定では1688ポートを使用していますが、そのポート番号を変更したい場合に  
使用します。変更をすぐに反映したい場合は、slsvc.exeサービスを再起動するか  
コンピューターを再起動します。

* DNS 発行の無効化/有効化  
  自動的なDNS発行を無効にします。

slmgr /cdns

自動的なDNS発行を有効にします。

slmgr /sdns

KMS ホストの情報を記載している SRV レコードを DNS サーバーに発行する機能の無効化と有効化を行います。

* プロセスの優先度の設定  
  プロセスの優先度を下げます。

slmgr /cpri

プロセスの優先度を通常に戻します。

slmgr /spri

* クライアントがライセンス認証されないときの再試行設定  
  クライアントがライセンス認証されないときにクライアントが使用するライセンス認証間隔(分) を設定します ( 既定では 120 分に設定されています )。

slmgr /sai <ライセンス認証間隔>

* クライアントの定期ライセンス認証の有効期限の変更  
  クライアントが定期的に KMS ホストとライセンス認証を行う更新間隔を設定します (分単位、既定では 10080{7 日間} です )。

slmgr /sri <更新間隔>

### KMS クライアント設定

ここで解説する設定が必要なのは、組織内の KMS ホストを KMS クライアントが自動  
検出できない場合のみです。これらの設定を行うと、KMS クライアントによる KMS ホストの自動検出が無効になります。

* KMS ホストを FQDN で指定する  
  KMS クライアントが利用する KMS ホストの完全修飾ドメイン名（FQDN）を  
  登録します。例えば、kms.comtoso.comなどです。オプションで、KMS との通信に使用する TCP ポートも登録することができます。

slmgr /skms <KMS\_FQDN> [:<ポート>]

* KMS ホストを IP で指定  
  KMSホストをFQDNで指定するのではなく、IPアドレスやコンピューター名で  
  直接指定する方法です。

slmgr /skms <IPv4アドレス> <:ポート>

slmgr /skms <IPv6アドレス> <:ポート>

slmgr /skms <コンピューター名> <:ポート>

* 登録情報の解除  
  登録されているクライアントコンピューターの自動検出を改めて有効にし、特定のKMSを使用するには、次のスクリプトを実行します。

slmgr /ckms

# 仮想マシンの自動ライセンス認証

Windows Server 2012 R2 では、自動ライセンス認証 （AVMA: Automatic Virtual Machine Activation） 機能が新たに追加されています。自動ライセンス認証である AVMA は Hyper-V 上で動作する仮想マシンに対する認証プロセスであり、物理マシンでは機能しません。この認証プロセスは AVMA キーを仮想マシンに設定することによって、KMS ホストや  
インターネット経由のライセンス認証を行うことなく、自動的にライセンス認証が行われます。

## 自動ライセンス認証要件

自動ライセンス認証は以下の条件を満たした環境で使用できます。

* ホスト OS が Windows Server 2012 R2 Datacenter を実行している
* ホスト OS がライセンス認証済みである
* ゲスト OS(仮想マシン) が、以下の OS を実行している
* Windows Server 2012 R2 Standard
* Windows Server 2012 R2 Datacenter
* Windows Server 2012 R2 Essentials

## 自動ライセンス認証方法

仮想マシンに 次のコマンドを使用して AVMA ライセンスキーを入力します。

slmgr /ipk <AVMA キー>

AVMA ライセンス キーはエディションごとに異なります。

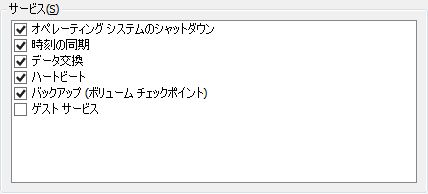
|  |  |
| --- | --- |
| OS のエディション | AVMA キー |
| Datacenter | Y4TGP-NPTV9-HTC2H-7MGQ3-DV4TW |
| Standard | DBGBW-NPF86-BJVTX-K3WKJ-MTB6V |
| Essentials | K2XGM-NMBT3-2R6Q8-WF2FK-P36R2 |

表 5 AVMA ライセンス キー

## 自動ライセンス認証の運用

自動ライセンス認証を行うと、対象となる仮想マシンは自動的にライセンス認証されます。

AVMA によるライセンス認証では、仮想マシンとの通信に、ネットワークは一切使用せず、  
Hyper-V ホストおよびゲスト間の統合サービスで提供されているデータ交換サービスを使用します。よって、Hyper-V ホストおよびゲスト間でデータ交換サービスが動作していることを確認する  
必要があります (既定ではオンになっています)。

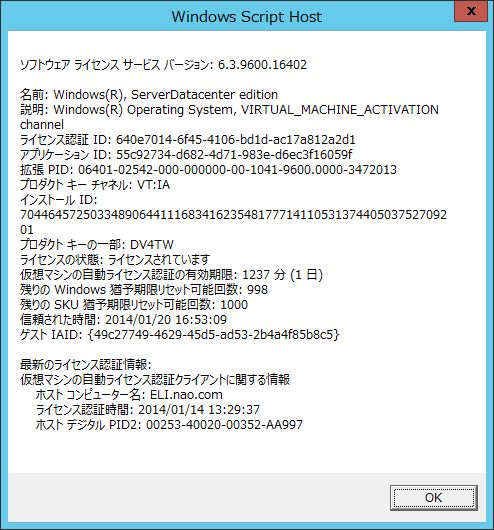


AVMA のライセンス認証の有効期間は 7 日ですが、Hyper-V ホストである Windows Server 2012 R2 Datacenter を実行するコンピューターがライセンス認証されていれば、  
AVMA の認証期限が切れても、認証プロセスが起動し再認証されます。

また、ライブマイグレーションやエクスポート/インポートによるホストの移動も同様です。

次のコマンドをゲスト OS で実行することにより、AVMA ライセンス認証における残りの有効期限を確認することができます。

Slmgr /dlv



ホスト OS のイベント ログでは、AVMA 認証が行われると、Application ログに  
「イベント ID:12310」 が記録されます。



ゲスト OS のイベント ログでは、AVMA 認証が行われると、Application ログに  
「イベント ID:12309」 が記録されます。



# まとめ

新しいボリューム アクティベーションでは、Windows 10 およびWindows Server 2012/R2 に対応し、さまざまな認証方法を提供しています。

Windows Server 2012 R2 では、ボリューム ライセンス認証サービスを利用することよって、  
ウィザード形式で KMS ホストを構築することが可能です。これまでは、スクリプトを使用して構築を行っていましたが、容易に KMS 認証を行う環境が構築できますので是非ご活用ください。

仮想マシン環境においては、自動ライセンス認証 (AVMA: Automatic Virtual Machine Activation) 機能が新たに追加されました。これにより、仮想マシンの展開と同時にライセンス  
認証を行うことができるようになりました。

Active Directory によるライセンス認証もサポートされ、ドメインに参加したメンバーは自動的に  
ライセンス認証が行われる環境が構築できます。

このように、Windows OS のライセンス認証はあらゆる環境にも対応できるように柔軟な方法を提供しています。よって、それぞれの企業に適した認証方法を選択していただき、適切な運用をしていただければ幸いです。

# Appendix

## FAQ

### ボリューム アクティベーション FAQ

|  |  |
| --- | --- |
| Q1 | KMS か MAKかの選択は、インストール時にインストール作業をする担当者が選択可能 なのですか。 |
| A | インストール時に、キーの入力はありません。そのため、エンド ユーザーがインストール後、 何も作業を行わない場合は KMS クライアントとして運用がされます。MAK 端末にする場合は、管理者権限でサイン インし、プロダクト キーを変更する作業が必要です。（インストールする OS イメージに、あらかじめキーを入力しておくことも可能です。） |

|  |  |
| --- | --- |
| Q2 | MAKからKMSへ変更することは可能ですか？ |
| A | KMS クライアント セットアップ キーに変更することによって可能です。 |

|  |  |
| --- | --- |
| Q3 | ボリューム ライセンス キーの入手はどのように行うことができますか。 |
| A | ほとんどの製品で、VLK は次の 2 種類の方法で入手できます。  ボリューム ライセンス サービス センター <https://www.microsoft.com/Licensing/servicecenter/default.aspx>  マイクロソフト ライセンス認証専用窓口 <http://www.microsoft.com/ja-jp/licensing/existing-customers/activation-centers.aspx> |

|  |  |
| --- | --- |
| Q4 | n カウントとは何ですか。 |
| A | n カウントとは、KMS クライアントがライセンス認証を実行するまでに、KMS ホストに接続する 必要のあるコンピューターの最小数を意味します。この値はクライアントコンピューターのライセンス ポリシーに保存されており、KMS が返すカウントに基づいて、コンピューターがライセンス認証を 実行するかを決定します。KMS クライアント の n カウントは 25 です。この値は変更できません。KMS クライアント は、KMS ホストが返す n カウントが 25 以上である場合にライセンス認証を実行します。 |

|  |  |
| --- | --- |
| Q5 | MAK ライセンス認証を実行した場合にも KMS の n カウントは増えますか。 |
| A | いいえ。MAK ライセンス認証の実行によって KMS の n カウントが増えることはありません。 |

|  |  |
| --- | --- |
| Q6 | 仮想マシンでの認証でも KMS の n カウントは増えますか。 |
| A | はい、増えます。初期のバージョンのボリューム アクティベーションでは、仮想マシンはカウントされませんでしたが、現在は仮想マシンでの KMS ライセンス認証の実行によって KMS の n カウントが増えます。 |

|  |  |
| --- | --- |
| Q7 | n カウントの値 -1 は何を意味するのですか。 |
| A | n カウントが -1 である場合は、KMS ホストにアクセスしたクライアントがまったく存在しないことを意味します。 |

|  |  |
| --- | --- |
| Q8 | "通知" とは、どのようなライセンス状態をいうのですか。 |
| A | OS をインストールした初期状態ではライセンス認証がされていません。この状態のコンピューターは通知モードで動作します。通知モードでは、OS のライセンス認証を行う必要があることをウォーターマークの表示を行いユーザーに通知します。 |

|  |  |
| --- | --- |
| Q9 | イベント ログの定期クリーン アップを行った場合、イベント ログに保存されているライセンス認証の履歴は失われるのですか。 |
| A | はい。クリーンアップ ツールを使用する場合は、[Windows ログ] および [アプリケーションとサービス ログ] のイベント ログをエクスポートすることをお勧めします。 |

|  |  |
| --- | --- |
| Q10 | slmgr を実行するときに一部のオプションしか表示されません。これはなぜですか。 |
| A | slmgr で使用できるオプションはインストールされているプロダクト キーによって異なります。たとえば、MAK ライセンス認証を使用しているコンピューターでは KMS に関連するオプションは表示されません。 |

|  |  |
| --- | --- |
| Q11 | クライアント OS のMAK認証をしてからイメージ展開をした場合、展開後の認証は不要となりますか。 |
| A | いいえ、展開後の認証手続が必要になります。 |

|  |  |
| --- | --- |
| Q12 | クライアントOSで25台を超えてイメージ展開する場合、MAK認証は利用できますか？ |
| A | 利用可能です。キーが足りない場合はライセンス認証窓口にご相談ください。ライセンス認証窓口では、MAK キーの再補充および多少の上限値変更に対応しています。 |

|  |  |
| --- | --- |
| Q13 | slmgr スクリプトをセーフ モードで実行することはできますか。 |
| A | いいえ。セーフ モードではライセンス認証の情報にアクセスできません。 |

|  |  |
| --- | --- |
| Q14 | 仮想化された Windows 10 について留意しなければならない点はありますか。 |
| A | 仮想コンピューターを作成する場合は、sysprep /generalize を実行して製品のライセンス認証タイマーをリセットすることをお勧めします。 |

|  |  |
| --- | --- |
| Q15 | 複数の会社で、異なる社員グループに、KMS と MAK の両方を使用することはできますか。 |
| A | はい、複数の会社で、KMS と MAK の両方を使用することを想定しています (例えば、ネットワーク上のユーザーには KMS、外出中のユーザーには MAK)。 |

|  |  |
| --- | --- |
| Q16 | KMS ライセンス認証に対して発行されたキーを、MAK ライセンス認証で使用することはできますか。 |
| A | いいえ、できません。 |

|  |  |
| --- | --- |
| Q17 | アクティベーションの猶予期間はなくなったのですか。 |
| A | Windows 8 で、猶予期間が廃止されました。 |

|  |  |
| --- | --- |
| Q18 | ライセンス キーを入力して、アクティベーションを行ったらデスクトップの背景が黒くなりましたが、なぜしてですか。 |
| A | ライセンス キーが偽造されたもの、あるいは盗まれたものと判定すると、デスクトップの背景が黒くなります。更に OS が正規品ではないことをユーザーに知らせるメッセージが画面に表示され、PC が 1 時間ごとにシャットダウンされます。 |

### KMS ライセンス認証 FAQ

|  |  |
| --- | --- |
| Q1 | KMS ホストとして利用するために用意したサーバーに、サーバー ライセンスは必要ですか。 |
| A | はい、必要です。 |

|  |  |
| --- | --- |
| Q2 | サーバーを KMS ホストとして利用する場合、CAL は必要ですか。 |
| A | はい、必要です。 |

|  |  |
| --- | --- |
| Q3 | KMS ホストでのライセンス認証は、契約ライセンス数までしかできないのですか。 |
| A | いいえ、KMS ホストは契約ライセンス以上のライセンス認証に対応しています。 |

|  |  |
| --- | --- |
| Q4 | KMS キーは、どこで入手できますか。 |
| A | ボリューム ライセンス サービス センター（VLSC）のポータルサイト、またはマイクロソフト ライセンス認証専用窓口で入手が可能です。 |

|  |  |
| --- | --- |
| Q5 | KMS の機能でアクティベーションできるクライアントの台数を制限ができますか。 |
| A | いいえ、できません。 |

|  |  |
| --- | --- |
| Q6 | MAK 認証した PC を、KMS ホストで管理することはできるのですか。 |
| A | いいえ、できません。 |

|  |  |
| --- | --- |
| Q7 | 1 つの KMS キーを複数の KMS ホストで使用することはできますか。 |
| A | KMS キーは、1つにつき最大 6 台のコンピューターで 10 回まで使用できます。6 台を超える KMS ホストが必要な場合は、組織の KMS キーに対して追加のライセンス認証を申請する 必要があります。 |

|  |  |
| --- | --- |
| Q8 | 複数の KMS ホストを構築する場合、KMS の情報は KMS ホスト間で複製されるのですか。 |
| A | KMS ホストはそれぞれ独立しているため、ホスト間の通信や情報共有はできません。 |

|  |  |
| --- | --- |
| Q9 | KMS ホストが正しくセットアップされているかどうかを確認することはできますか。 |
| A | KMS が正しくセットアップされているかどうかを確認するには、KMS カウントと KMS イベント  ログ エントリを調べます。KMS ホストで slmgr -dli を実行すると、KMS カウントの現在値が表示されます。  KMS イベント ログでは、コンピューター名と各要求のタイムスタンプを確認できます。 |

|  |  |
| --- | --- |
| Q10 | ライセンス認証の情報は KMS ホストから マイクロソフトに送信されますか。 |
| A | いいえ。KMS ホストの最初のライセンス認証を除き、ライセンス認証の情報が マイクロソフトに送信されることはありません。 |

|  |  |
| --- | --- |
| Q11 | KMS クライアントのライセンス認証を実行するためには先に KMS ホストのライセンス認証を 実行することが必要ですか。 |
| A | はい。KMS クライアントのライセンス認証を実行する前に KMS ホストのライセンス認証を完了する必要があります。ライセンス認証はインターネットと電話のどちらでも実行できます。  ハードウェアに大幅な変更があった場合は、KMS ホストのライセンス認証の再実行が必要となることがあります。 |

|  |  |
| --- | --- |
| Q12 | クライアント コンピューターはどのように KMS サービスを検出するのですか。 |
| A | クライアント コンピューターは次のいずれかの方法で KMS サービスを検出します。   * 自動検出 クライアント コンピューターがドメイン ネーム システム (DNS) サービスの SRV リソース レコード (既定) を使用して自動的にローカル KMS  ホストを検出します。 * 直接登録 システム管理者が KMS ホストと通信ポートをレジストリに指定します。 |

|  |  |
| --- | --- |
| Q13 | KMS クライアントで、特定の KMS ホストへの接続を設定するためには、管理者権限が必要ですか。 |
| A | はい。システムの安定性と機能の継続性を保証するためには直接登録の設定が重要な意味を持ちます。したがって、クライアント コンピューターで特定の KMS ホストへの接続設定を行うために管理者権限が必要となります。 |

|  |  |
| --- | --- |
| Q14 | KMS クライアントは、どのような方法で KMS サービスに接続するのですか。 |
| A | KMS クライアントは、既知のポートでの短時間の RPC over TCP/IP セッションによって KMS サービスに接続します。既定のポートは 1688 ですが、別のポートに変更することもできます。KMS ホストと KMS クライアントとの接続を可能にするためにファイアウォール規則の変更が必要となる場合があります。 |

|  |  |
| --- | --- |
| Q15 | KMS クライアントが、通常は仮想プライベート ネットワーク (VPN) 経由で接続する場合、 ライセンス認証の更新を要求されることはありますか。 |
| A | はい。ライセンス認証期間またはライセンス認証の更新期間 (いずれも変更可能ですが、既定値はそれぞれ 2 時間、7 日間です) が経過すると、KMS クライアントは VPN 接続の確立後 5 分ごとに KMS ホストに接続します。 |

|  |  |
| --- | --- |
| Q16 | KMS ライセンス認証のエージングはどのように管理されるのですか。 |
| A | KMS によるライセンス認証が完了すると、クライアント コンピューター ID (CMID) が n キャッシュに格納されます。同じKMS クライアントがライセンス認証を更新すると、キャッシュ内の CMID と日付が削除され、新たなキャッシュ エントリが作成されます。KMS クライアントのライセンス認証は、既定では 7 日ごとに更新されます。ただし、30 日後に KMSクライアントのライセンス認証が更新されなかった場合、そのKMS クライアントの CMID が n キャッシュから削除され、n カウントの値が 1 つ小さくなります。KMS ライセンス認証のエージングによって n カウントが 25 未満とならないように、KMS は最近実行された 50 のライセンス認証の CMID をキャッシュに格納します。 |

|  |  |
| --- | --- |
| Q17 | KMS ではどのような種類の暗号化を使用するのですか。 |
| A | KMS では、署名メカニズムとして Cipher Block Chaining Message Authentication Code (CBC-MAC) を使用し、基礎となる暗号化機能として AES (Advanced Encryption Standard) を使用しています。 |

|  |  |
| --- | --- |
| Q18 | 既定の KMS プロセスは BIND などの マイクロソフト以外の DNS システムと互換性がありますか。 |
| A | はい。KMS システムでは SRV リソース レコード (RR) を使用して DNS 経由で KMS の場所および構成の情報を保存、送信します。SRV レコード (RFC 2782 準拠) と動的更新 (RFC 2136 準拠) をサポートする DNS サーバーは、いずれも KMS クライアントでの自動検出と KMS クライアントの検出に対応しています。  Berkeley Internet Domain Name (BIND) のバージョン 8.x および 9.x は SRV レコードと DDNS のどちらもサポートしています。  注：SRV および A リソース レコードを必要な DNS ゾーンに書き込むためには、DNSSEC、ACL、その他の セキュリティ メカニズムを構成する必要があります。 |

|  |  |
| --- | --- |
| Q19 | BIND 9.x DNS サーバーでは、KMS の自動公開をサポートするためにどのような設定が 必要ですか。 |
| A | BIND サーバーでは、KMS ホストによるリソース レコードの更新を有効に設定する必要が あります。たとえば、named.conf (または named.conf.local) のゾーン定義に次の行を追加します。  allow-update { any; };  allow-update ステートメントを named.conf.options に追加することによって、そのサーバーが権限を持つ サーバー上のすべてのゾーンで DDNS を有効にすることもできます。 |

### ボリューム ライセンス認証サービス FAQ

|  |  |
| --- | --- |
| Q1 | Windows PowerShell を使ってボリューム ライセンス認証サービスをインストールおよび構成することができますか。 |
| A | Windows PowerShell ではボリューム ライセンス認証サービスの構成はサポートされていません。ただし、ボリューム ライセンス認証サーバーの役割は、Windows PowerShell スクリプトを使ってインストールできます。  従来どおり、スクリプトを使用してボリューム ライセンス認証をインストールおよび管理することもできます。 |

|  |  |
| --- | --- |
| Q2 | ボリューム ライセンス認証サービスを仮想マシンで実行できますか? |
| A | はい。ボリューム ライセンス認証サービスは仮想マシンから実行できます。ただし、その仮想マシンが使用できない期間は、KMS と Active Directory によるボリューム ライセンス認証でクライアントからのボリューム ライセンス認証更新要求をサポートすることはできません。 |

|  |  |
| --- | --- |
| Q3 | ボリューム ライセンス認証サービスをマルチサーバー環境で展開して構成できますか? |
| A | ボリューム ライセンス認証サービスは、マルチサーバー構成をサポートするように設計されて います。 |

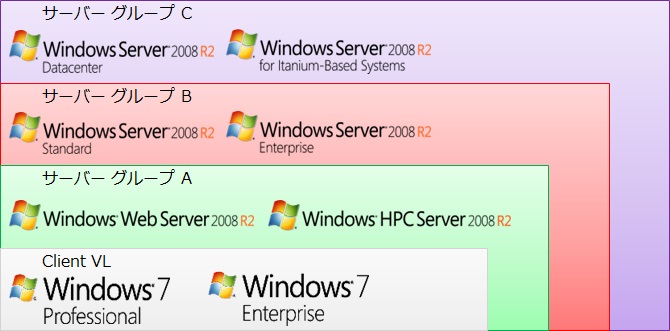
|  |  |
| --- | --- |
| Q4 | ボリューム ライセンス認証サービスをクラスター環境で実行できますか? |
| A | ボリューム ライセンス認証サービスを実行しているサーバーへのライセンス認証要求は比較的小さく断続的なデータ要求であるため、クラスター サーバー間にまたがるインストールはサポートされていません。  ただし、ボリューム ライセンス認証サービスは、クラスター内で構成されたサーバーをライセンス認証して管理するのに使用できます。特別に構成を変更する必要はありません。 |

|  |  |
| --- | --- |
| Q5 | ボリューム ライセンス認証サービスはリモート コンピューターから管理できますか? |
| A | ボリューム ライセンス認証サービスはリモート コンピューターから管理できます。 |

|  |  |
| --- | --- |
| Q6 | ボリューム ライセンス認証サービスは、Windows Server の Server Core インストールにインストールできますか? |
| A | サーバー マネージャーに用意されているグラフィカル ユーザー インターフェイス ツールを使って、Windows Server 2012 の Server Core インストールを実行しているコンピューターを含むリモート コンピューターにボリューム ライセンス認証サービスをインストールできます。ただし、Server Core インストールを実行しているコンピューターで KMS や Active Directory によるライセンス認証を直接管理する場合、グラフィカル ユーザー インターフェイスは使用できないため、コマンド ラインから管理する必要があります。 |

## 以前の KMS キー タイプ

Windows 7 およびWindows Server 2008 R2で提供される KMS キー タイプは  
下図 のようになっていました。



このように、クライアント VL からサーバーグループ A、B、C まで存在し、利用する最上位の製品グループの KMS キーが付与されていました。それぞれの製品グループの KMS キーで構成された KMS ホストは、対応する製品グループと下位の製品グループをライセンス認証できます。

また、Windows 7 および Windows Server 2008 R2で提供される KMS キーは、下表の  
通りです。

|  |  |  |
| --- | --- | --- |
| プロダクト キー  グループ | KMS をホストできる OS (KMS キーが KMS ホストをライセンス認証) | この KMS ホストによってライセンス認証 される Windows 製品エディション |
| Windows 7 用 クライアント VL | Windows Vista  Windows 7 | Windows 7 Professional  Windows 7 Enterprise  Windows Vista Business  Windows Vista Enterprise |
| Windows Server 2008 R2 用 サーバー グループ A | Windows Web Server 2008  Windows Web Server 2008 R2  Windows HPC Server 2008  Windows HPC Server 2008 R2 | 上記の製品エディションと  Windows Web Server 2008 R2  Windows Web Server 2008  Windows HPC Server 2008 R2  Windows HPC Server 2008 |
| Windows Server 2008 R2 用 サーバー グループ B | 上記の製品エディションと  Windows Server 2008 R2 Standard  Windows Server 2008 R2 Enterprise  Windows Server 2008 Standard  Windows Server 2008 Enterprise | 上記の製品エディションと  Windows Server 2008 R2 Standard  Windows Server 2008 R2 Enterprise  Windows Server 2008 Standard  Windows Server 2008 Enterprise |
| Windows Server 2008 R2  用サーバーサーバー グループ C | 上記の製品エディションと  Windows Server 2008 R2 Datacenter  Windows Server 2008 Datacenter  Windows Server 2008 for Itanium-Based Systems | 上記の製品エディションと  Windows Server 2008 R2 Datacenter  Windows Server 2008 Datacenter  Windows Server 2008 for Itanium-Based Systems |

表 7 Windows 7 および Windows Server 2008 R2 で提供される KMS キー

Windows 7 でホストされる KMS ホストは、クライアント OS だけをライセンス認証できますが、Windows Server 2008 R2 でホストされる KMS ホストは、クライアント OS とサーバー OS をライセンス認証できます。この際、サーバーグループA、B、Cが存在し、企業のライセンス体系にあったライセンスグループのキーを使用する必要がありました。

このようにサーバーグループが設定されていましたが、Windows 8 以降とWindows Server 2012 以降の KMS キー タイプではクライアントとサーバーの2種類のみ提供されています。

そしてサーバーライセンスキーがクライアントライセンスキーを包括しています。

サーバーライセンスキーは、すべての Windows エディションをライセンス認証することが可能なキーであるため、よりわかり易いライセンス認証体系となっています。

## KMS クライアントセットアップキー（GVLK）

MAK 認証から KMS 認証に変更する際は、使用している Windows エディションの KMS クライアントライセンスキーである GVLK を入力する必要があります。

その際は、次のコマンドを実行します。

slmgr /ipk < ライセンスキー >

slmgr /ato

|  |  |
| --- | --- |
| オペレーティング システム エディション | GVLK |
| Windows 10 Professional | W269N-WFGWX-YVC9B-4J6C9-T83GX |
| Windows 10 Enterprise | NPPR9-FWDCX-D2C8J-H872K-2YT43 |
| Windows 10 Education | NW6C2-QMPVW-D7KKK-3GKT6-VCFB2 |
| Windows 10 Enterprise 2015 LTSB | WNMTR-4C88C-JK8YV-HQ7T2-76DF9 |

表 8 Windows 10

|  |  |
| --- | --- |
| オペレーティング システム エディション | GVLK |
| Windows 8.1 Professional | GCRJD-8NW9H-F2CDX-CCM8D-9D6T9 |
| Windows 8.1 Enterprise | MHF9N-XY6XB-WVXMC-BTDCT-MKKG7 |
| Windows Server 2012 R2 Server Standard | D2N9P-3P6X9-2R39C-7RTCD-MDVJX |
| Windows Server 2012 R2 Datacenter | W3GGN-FT8W3-Y4M27-J84CP-Q3VJ9 |
| Windows Server 2012 R2 Essentials | KNC87-3J2TX-XB4WP-VCPJV-M4FWM |

表 9 Windows Server 2012 R2 および Windows 8.1

|  |  |
| --- | --- |
| オペレーティング システム エディション | GVLK |
| Windows 8 Professional | NG4HW-VH26C-733KW-K6F98-J8CK4 |
| Windows 8 Enterprise | 32JNW-9KQ84-P47T8-D8GGY-CWCK7 |
| Windows Server 2012 Core | BN3D2-R7TKB-3YPBD-8DRP2-27GG4 |
| Windows Server 2012 Core Single Language | 2WN2H-YGCQR-KFX6K-CD6TF-84YXQ |
| Windows Server 2012 Core Country Specific | 4K36P-JN4VD-GDC6V-KDT89-DYFKP |
| Windows Server 2012 Server Standard | XC9B7-NBPP2-83J2H-RHMBY-92BT4 |
| Windows Server 2012 Standard Core | XC9B7-NBPP2-83J2H-RHMBY-92BT4 |
| Windows Server 2012 MultiPoint Standard | HM7DN-YVMH3-46JC3-XYTG7-CYQJJ |
| Windows Server 2012 MultiPoint Premium | XNH6W-2V9GX-RGJ4K-Y8X6F-QGJ2G |
| Windows Server 2012 Datacenter | 48HP8-DN98B-MYWDG-T2DCC-8W83P |
| Windows Server 2012 Datacenter Core | 48HP8-DN98B-MYWDG-T2DCC-8W83P |

表 10 Windows Server 2012 および Windows 8

|  |  |
| --- | --- |
| オペレーティング システム エディション | GVLK |
| Windows 7 Professional | FJ82H-XT6CR-J8D7P-XQJJ2-GPDD4 |
| Windows 7 Professional E | W82YF-2Q76Y-63HXB-FGJG9-GF7QX |
| Windows 7 Enterprise | 33PXH-7Y6KF-2VJC9-XBBR8-HVTHH |
| Windows 7 Enterprise E | C29WB-22CC8-VJ326-GHFJW-H9DH4 |
| Windows Server 2008 R2 Web | 6TPJF-RBVHG-WBW2R-86QPH-6RTM4 |
| Windows Server 2008 R2 HPC edition | TT8MH-CG224-D3D7Q-498W2-9QCTX |
| Windows Server 2008 R2 Standard | YC6KT-GKW9T-YTKYR-T4X34-R7VHC |
| Windows Server 2008 R2 Enterprise | 489J6-VHDMP-X63PK-3K798-CPX3Y |
| Windows Server 2008 R2 Datacenter | 74YFP-3QFB3-KQT8W-PMXWJ-7M648 |
| Windows Server 2008 R2 for Itanium-based Systems | GT63C-RJFQ3-4GMB6-BRFB9-CB83V |

表 11 Windows 7 および Windows Server 2008 R2

|  |  |
| --- | --- |
| オペレーティング システム エディション | GVLK |
| Windows Vista Business | YFKBB-PQJJV-G996G-VWGXY-2V3X8 |
| Windows Vista Enterprise | VKK3X-68KWM-X2YGT-QR4M6-4BWMV |
| Windows Web Server 2008 | WYR28-R7TFJ-3X2YQ-YCY4H-M249D |
| Windows Server 2008 Standard | TM24T-X9RMF-VWXK6-X8JC9-BFGM2 |
| Windows Server 2008 Standard without Hyper-V | W7VD6-7JFBR-RX26B-YKQ3Y-6FFFJ |
| Windows Server 2008 Enterprise | YQGMW-MPWTJ-34KDK-48M3W-X4Q6V |
| Windows Server 2008 Enterprise without Hyper-V | 39BXF-X8Q23-P2WWT-38T2F-G3FPG |
| Windows Server 2008 HPC | RCTX3-KWVHP-BR6TB-RB6DM-6X7HP |
| Windows Server 2008 Datacenter | 7M67G-PC374-GR742-YH8V4-TCBY3 |
| Windows Server 2008 Datacenter without Hyper-V | 22XQ2-VRXRG-P8D42-K34TD-G3QQC |
| Windows Server 2008 for Itanium-Based Systems | 4DWFP-JF3DJ-B7DTH-78FJB-PDRHK |

表 12 Windows Vistaおよび Windows Server 2008

## 出典

* Windows 8.1 および Windows RT 8.1 ボリューム ライセンス ガイド

<http://download.microsoft.com/download/4/C/B/4CB42B2E-B4EC-43A2-BFA0-1FE7E30A39E2/Windows_8_1_Licensing_Guide-JP.pdf>

* ボリューム アクティベーション 運用ガイド

<http://download.microsoft.com/download/4/1/3/413E9302-B6C7-46B8-82F1-8D5D2399BDC6/Volume_Activation_Operations_Guide_Windows7.docx>

* ボリューム アクティベーション 2.0 KMS 編 ステップ バイ ステップ

<http://www.microsoft.com/downloads/details.aspx?familyid=302BE39D-E217-4313-A7A7-FD9FCCE5BE3A&displaylang=ja>

* マイクロソフト ボリュームライセンス ホームページ

<http://www.microsoft.com/ja-jp/licensing/default.aspx>

* ボリューム ライセンス認証の概要 ホームページ

<http://technet.microsoft.com/ja-jp/library/hh831612.aspx>

* Appendix A: KMS Client Setup Keys

<http://technet.microsoft.com/en-us/library/jj612867.aspx>

* Deploying Metro style apps to businesses

<http://blogs.msdn.com/b/windowsstore/archive/2012/04/25/deploying-metro-style-apps-to-businesses.aspx>

* DISM によるアプリの追加と削除

<http://technet.microsoft.com/ja-jp/library/hh852635.aspx>

* ボリュームライセンス認証の計画

<https://technet.microsoft.com/ja-jp/library/jj134042.aspx>