カスタマー ホステッド ボリューム アクティベーション ガイド

Windows 7 および Server 2008 R2

Microsoft Corporation

公開: 2009 年 6 月

要約

Microsoft® ボリューム アクティベーションは、ボリューム ライセンスを購入されたお客様が、ボリューム ライセンス メディアのライセンス認証プロセスを自動化および管理するのを支援します。ボリューム ライセンスを購入されたお客様およびマイクロソフト パートナー プログラム、MSDN®、Microsoft TechNet などの特別プログラムのサブスクライバーが、ボリューム ライセンス ソフトウェアおよびメディアを利用できます。このガイドは、キー管理サービスを使用したボリューム アクティベーション バージョンの Windows® 7 および Windows Server® 2008 R2 オペレーティング システムの展開を計画している組織の IT プロフェッショナルを対象としています。

このドキュメントおよびここで参照されているドキュメントに記載された内容は情報提供のみを目的としており、明示または黙示にかかわらず、これらの情報についてマイクロソフトはいかなる責任も負わないものとします。URL などのインターネットの Web サイトの参照先を含め、このドキュメントに記載された内容は、予告なしに変更する可能性があります。このドキュメントの使用または使用した結果から生じたすべてのリスクについては、お客様が責任を負うものとします。特に記載のある場合を除き、ここで使用している会社、組織、製品、ドメイン名、電子メール アドレス、ロゴ、人物、場所、およびイベントの例は、架空のものです。実在する会社、組織、製品、ドメイン名、電子メールアドレス、ロゴ、人物、場所、イベントなどとは一切関係ありません。お客様ご自身の責任において、適用されるすべての著作権関連法規に従ったご使用を願います。このドキュメントのいかなる部分も、マイクロソフトの書面による許諾を受けることなく、その目的を問わず、どのような形態であっても、複製または譲渡することは禁じられています。ここでいう形態とは、複写や記録など、電子的な、または物理的なすべての手段を含みます。ただしこれは、著作権法上のお客様の権利を制限するものではありません。

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

© 2009 Microsoft Corporation.All rights reserved.

Microsoft、Hyper-V、MSDN、Windows、Windows ロゴ、Windows NT、Windows 7、Windows Server、Windows Vista、および Windows Web Server は、Microsoft 企業グループの商標です。

ここに記載されている会社名および製品名には、各所有者の商標のものもあります。

# 目次

[目次 3](#_Toc236539284)

[はじめに 1](#_Toc236539285)

[KMSの理解 2](#_Toc236539286)

[最小コンピューター要件 2](#_Toc236539287)

[KMS ライセンス認証のしきい値 2](#_Toc236539288)

[ライセンス認証カウント キャッシュ 3](#_Toc236539289)

[KMS の使用法 4](#_Toc236539290)

[KMS ライセンス認証の更新 4](#_Toc236539291)

[KMS サービスの発行 5](#_Toc236539292)

[KMS サービスのクライアントの探索 5](#_Toc236539293)

[KMS 展開の計画 6](#_Toc236539294)

[DNS サーバーの構成の計画 7](#_Toc236539295)

[1 台目の KMS ホストのライセンス認証 7](#_Toc236539296)

[後続の KMS ホストのライセンス認証 8](#_Toc236539297)

[既存の KMS ホストのアップグレード 8](#_Toc236539298)

[KMS クライアントの計画 9](#_Toc236539299)

[標準ユーザーとしてのライセンス認証 9](#_Toc236539300)

[プロダクト キーのニーズの判断 10](#_Toc236539301)

[KMS キーの選択 10](#_Toc236539302)

[KMS ホストの選択 11](#_Toc236539303)

[KMS ライセンス認証の展開 13](#_Toc236539304)

[KMS ホストの構成 13](#_Toc236539305)

[リモートでの Slmgr.vbs の実行 15](#_Toc236539306)

[リモートでのソフトウェア ライセンス マネージャー操作のための Windows ファイアウォールの構成 15](#_Toc236539307)

[ワークグループ コンピューターを対象とするリモート操作 16](#_Toc236539308)

[DNS の構成 16](#_Toc236539309)

[SRV レコードに対する既定の DNS アクセス許可の変更 17](#_Toc236539310)

[複数の DNS ドメインへの発行 18](#_Toc236539311)

[DNS に SRV レコードを手動で作成 19](#_Toc236539312)

[BIND 8.2 以降の DNS サーバーの SRV レコードの手動作成 20](#_Toc236539313)

[KMS SRV レコードの DNS への発行の無効化 21](#_Toc236539314)

[KMS ホストのインストール 22](#_Toc236539315)

[KMS クライアントの構成 23](#_Toc236539316)

[KMS ホストの手動での指定 24](#_Toc236539317)

[KMS クライアントの自動探索の有効化 24](#_Toc236539318)

[サフィックス エントリの KMS クライアントへの追加 24](#_Toc236539319)

[KMS クライアントの展開 25](#_Toc236539320)

[KMS クライアントの手動によるライセンス認証 25](#_Toc236539321)

[MAK クライアントの KMS への変換および KMS クライアントの MAK への変換 26](#_Toc236539322)

[製品版のボリューム アクティベーションへの変換 27](#_Toc236539323)

[コンピューターの再ライセンス認証 28](#_Toc236539324)

# はじめに

Microsoft® ボリューム アクティベーションは、IT プロフェッショナルによる製品ライセンス認証手続きの自動化と管理に役立つ構成可能なソリューションで、Microsoft® ボリューム ライセンス プログラムおよびボリューム ライセンス エディションの Windows を提供するその他のプログラムでライセンスされた Windows Vista®、Windows® 7、Windows Server® 2008、および Windows Server 2008 R2 オペレーティング システムを実行しているコンピューター上で使用できます。

このガイドでは、Windows 7 および Windows Server 2008 R2 オペレーティング システムのための計画、展開、および運用について説明します。このガイドは、キー管理サービス (KMS) を使用して自社のボリューム アクティベーション インフラストラクチャをホスティングしている組織を対象としています。

**注** このドキュメントでは、Windows 7 および Windows Server 2008 R2 オペレーティング システム用のボリューム アク  
ティベーションのガイダンスを提供します。Windows Vista および Windows Server 2008 に対するボリューム アクティベーションの計画の詳細については、『**ボリューム アクティベーション 2.0 テクニカル ガイド**』 (<http://go.microsoft.com/fwlink/?LinkID=75674>) を参照してください。ただし、このガイドでは両世代の製品間の相互運用性については説明しません。

# KMSの理解

KMS は、ローカル ネットワーク上のコンピューターをライセンス認証します。個々のコンピューターがマイクロソフトに接続する必要がなくなります。これを行うために、KMS ではクライアント–サーバー トポロジーを使用します。KMS クライアント コンピューターは、ドメイン ネーム システム (DNS) または静的構成を使って KMS ホスト コンピューターを検索できます。KMS クライアントは、リモート プロシージャ コール (RPC) を使って KMS ホストに接続します。KMS は、Windows Vista、Windows 7、Windows Server 2003、Windows Server 2008、または Windows Server 2008 R2 オペレーティング システムを実行しているコンピューターでホストできます。

## 最小コンピューター要件

KMS ライセンス認証を計画している場合、ネットワークにライセンス認証のしきい値 (KMS が必要とする条件を満たしたコンピューターの最小台数) 以上のコンピューターが存在する必要があります。IT プロフェッショナルは、KMS ホストがネットワーク上のコンピューターの数をどのようにトラックするかも理解する必要があります。

### KMS ライセンス認証のしきい値

KMS は、物理コンピューターと仮想マシンをライセンス認証できます。KMS ライセンス認証の資格を得るには、ネットワークがライセンス認証のしきい値を満たす必要があります。KMS ホストは、このしきい値に達した後にのみクライアント コンピューターをライセンス認証します。ライセンス認証のしきい値に達していることを確認するため、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コンピューターの数をカウントします。Windows server 2008 または Windows Server 2008 R2 を実行しているコンピューターの場合、ライセンス認証のしきい値は 5 です。Windows Vista または Windows 7 を実行しているコンピューターの場合、ライセンス認証のしきい値は 25 です。しきい値には、物理コンピューターまたは仮想マシン上で実行しているクライアント コンピューターとサーバーが含まれます。

KMS ホストは、KMS クライアントから有効なライセンス認証要求があると、それぞれにライセンス認証のため KMS ホストに接続しているコンピューターの台数を返します。ライセンス認証のしきい値より低いカウントを受け取ったクライアントは、ライセンス認証されません。たとえば、KMS ホストに接続した最初の 2 台のコンピュー  
ターが Windows 7 を実行している場合、1 番目はライセンス認証カウント 1 を受け取り、2 番目はライセンス認証カウント 2 を受け取ります。次のコンピューターが Windows 7 を実行している場合、そのコンピューターはライセンス認証カウント 3 を受け取ります。以降も同様です。これらのコンピューターは、どれもライセンス認証されません。Windows 7 を実行しているコンピューターがライセンス認証されるためには、25 以上のライセンス認証カウントを受け取る必要があるからです。ライセンス認証カウントが低すぎるためにライセンス認証されていない猶予状態の KMS クライアントは、2 時間ごとに KMS ホストに接続して現在のライセンス認証カウントを取得し、しきい値に達するとライセンス認証されます。

KMS ホストに接続する次のコンピューターが Windows Server 2008 R2 を実行している場合、ライセンス認証カウントは Windows Server 2008 R2 を実行しているコンピューターと Windows 7 を実行しているコンピュー  
ターを合わせた数であるため、そのコンピューターはライセンス認証カウント 4 を受け取ります。Windows Server 2008 または Windows Server 2008 R2 を実行しているコンピューターが 5 以上のライセンス認証カウントを受け取ると、コンピューターはライセンス認証されます。Windows 7 を実行しているコンピューターが 25 以上のライセンス認証カウントを受け取ると、コンピューターはライセンス認証されます。

### ライセンス認証カウント キャッシュ

ライセンス認証のしきい値をトラックするため、KMS ホストは、ライセンス認証を要求する KMS クライアント コンピューターのレコードを保持します。KMS ホストは、各 KMS クライアント コンピューターにクライアント コンピューター ID (CMID) 指定を付与します。KMS ホストは、各 CMID をテーブルに保存します。各ライセンス認証要求は、30 日間テーブルに残ります。クライアント コンピューターがそのライセンス認証を更新するときに、キャッシュ済み CMID がテーブルから削除されます。新しいレコードが作成され、30 日間の保存期間が再び始まります。KMS クライアント コンピューターが 30 日以内にライセンス認証を更新しない場合は、KMS ホストが対応する CMID をテーブルから削除し、ライセンス認証カウントを 1 つ減らします。

KMS ホストは、CMID カウントがライセンス認証のしきい値を下回らないようにするために、KMS クライアントが必要とする CMID の数の 2 倍をキャッシュします。たとえば、Windows 7 を実行しているクライアント コンピューターを持つネットワークでは、KMS ライセンス認証のしきい値は 25 です。したがって、KMS ホストは、最新の 50 個のライセンス認証の CMID をキャッシュします。Windows Server 2008 R2 の KMS ライセンス認証のしきい値は、5 です。Windows Server 2008 R2 を実行している KMS クライアント コンピューターだけが接続している KMS ホストは、10 個の最新 CMID をキャッシュします。Windows 7 を実行しているクライアント コンピュー  
ターが後からその KMS ホストに接続すると、KMS は、より高いしきい値に対応するためにキャッシュ サイズを 50 に増加します。KMS がキャッシュ サイズを減らすことはありません。

## KMS の使用法

KMS ライセンス認証には TCP/IP 接続が必要です。既定で、KMS ホストおよびクライアント コンピューターは、DNS を使用して KMS サービスを発行および検索します。既定の設定を使用できます。これに必要な管理操作はほぼ皆無です。または KMS ホストおよびクライアント コンピューターをネットワーク構成とセキュリティの必要条件に基づいて手動で構成できます。

### KMS ライセンス認証の更新

KMS ライセンス認証は、180 日間有効 (ライセンス認証の検証間隔) です。ライセンス認証された状態であり続けるには、KMS クライアント コンピューターは、ライセンス認証を更新するため 180 日ごとに 1 回以上 KMS ホストに接続する必要があります。既定では、KMS クライアント コンピューターは、7 日ごとにライセンス認証の更新を試行します。KMS ライセンス認証が失敗した場合、クライアントは 2 時間ごとに再試行します。クライアント コンピューターのライセンス認証が更新されると、ライセンス認証の検証間隔が再び始まります。

### KMS サービスの発行

KMS サービスは、DNS 内のサービス (SRV) リソース レコード (RR) を使用して KMS ホストの場所を格納および通信します。KMS ホストは、DNS 動的更新プロトコルを使用して (利用可能な場合) KMS SRV RR を発行します。動的更新が利用できないか、または KMS ホストに RR を発行する権利がない場合は、DNS レコードを手動で発行する必要があります。または IT プロフェッショナルが、特定の KMS ホストに接続するためにクライアント コン  
ピューターを構成する必要があります。

**注** DNS の変更をすべての DNS ホストに伝達するには、ネットワークの複雑さとトポロジーに応じて、時間がかかる場合があります。

### KMS サービスのクライアントの探索

既定で、KMS クライアントが DNS に KMS サービス情報をクエリします。KMS クライアントが DNS に KMS   
サービス情報を初めてクエリするとき、KMS クライアントは、DNS が返す SRV RR のリストから KMS ホストをランダムに選択します。

SRV RR を含む DNS サーバーのアドレスが、KMS クライアントのサフィックスを付加したエントリとしてリストできます。このため、1 つの DNS サーバー内の KMS および他のプライマリ DNS サーバーを持つ KMS クライアントの SRV RR の提供情報によって、それを見つけることができます。

優先度および重みパラメーターを KMS の **DnsDomainPublishList** レジストリ値に追加できます。KMS ホストの優先度グループおよび各グループ内での重み付けの設定により、IT プロフェッショナルはクライアントが最初に試行する KMS ホストを指定でき、複数の KMS ホスト間でトラフィックが分散されます。Windows 7 と Windows Server 2008 R2 だけが、優先度および重みパラメーターを提供します。

クライアントが選択した KMS ホストが応答しない場合は、KMS クライアントが、その KMS ホストを SRV RR のリストから削除し、別の KMS ホストをリストからランダムに選択します。KMS ホストが応答する場合は、KMS クライアントは、KMS ホストの名前をキャッシュし、それを後続のライセンス認証および更新の試行に使用します。  
キャッシュ済みの KMS ホストが後続の更新で応答しない場合は、KMS クライアントが DNS に KMS SRV RR をクエリすることにより、新しい KMS ホストを検出します。

既定で、クライアント コンピューターは、ライセンス認証のため TCP ポート 1688 を通して匿名 RPC を使って KMS ホストに接続します (IT プロフェッショナルは、既定ポートを変更できます)。KMS ホストとの TCP セッションを設定後、クライアントは、1 個の要求パケットを送信します。KMS ホストが、ライセンス認証カウントを返します。カウントがそのオペレーティング システムのライセンス認証のしきい値以上に達している場合は、クライアントがライセンス認証され、セッションが閉じます。KMS クライアントは、更新要求にもこれと同じプロセスを使用します。片道の通信は 250 バイトです。

## KMS 展開の計画

KMS サービスには専用サーバーが不要です。KMS サービスは、Active Directory® Domain Services (AD DS) ドメイン コントローラー、読み取り専用ドメイン コントローラー (RODC) など、他のサービスと共同でホストできます。KMS ホストは、Windows Server 2003 を含め、任意のサポート Windows オペレーティング システムを実行している物理コンピューターまたは仮想マシンでも動作できます。Windows Server 2008 R2 を実行している KMS ホストは、ボリューム アクティベーションをサポートしている任意の Windows オペレーティング システムをライセンス認証できますが、Windows 7 を実行している KMS ホストは、Windows 7 および Windows Vista を実行しているコンピューターでしかライセンス認証できません。1 つの KMS ホストが、無制限の数の KMS クライアントをサポートできますが、マイクロソフトでは、フェールオーバー用に 2 台以上の KMS ホストを展開することをお勧めします。ほとんどの組織では、2 台の KMS ホストで組織のインフラストラクチャ全体に対応できます。

**注** KMS は、Windows Server 2003 に自動的に含まれません。Windows Server 2003 を実行しているコンピューターで KMS をホストするには、次のサイトのいずれかから KMS をダウンロードおよびインストールする必要があります。

* **Windows Server 2003 SP1 以降用キー管理サービス 1.1 (x86)** (<http://go.microsoft.com/fwlink/?LinkID=82964>) (英語)
* **Windows Server 2003 SP1 以降用キー管理サービス 1.1 (x64)** ([http://go.microsoft.com/fwlink/?LinkID=83041](http://go.microsoft.com/fwlink/?LinkId=83041)) (英語)

### DNS サーバーの構成の計画

既定の KMS 自動発行機能には、SRV RR および DNS 動的更新プロトコル サポートが必要です。KMS クライアントの既定の動作および KMS SRV RR 発行が、マイクロソフト ソフトウェアを実行している DNS サーバーまたは (Internet Engineering Task Force [IETF] Request for Comments [RFC] 2782 に準拠している) SRV RR と (RFC 2136 に準拠している) 動的更新をサポートする他の DNS サーバーでサポートされます。たとえば、Berkeley Internet Domain Name (BIND) バージョン 8.x および 9.x は、SRV レコードと動的更新をサポートします。

KMS ホストは、DNS サーバーで SRV、A (Internet Protocol version 4、IPv4)、および AAAA (Internet Protocol version 6、IPv6) RR を作成および更新するために必要な資格情報を持つように構成する必要があります。または、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ための推奨ソリューションは、AD DS にセキュリティ グループを作成した後、すべての KMS ホストをそのグループに追加することです。マイクロソフト ソフトウェアを実行している DNS サーバーで、KMS SRV RR 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。

### 1 台目の KMS ホストのライセンス認証

ネットワーク上の KMS ホストは、KMS キーをインストールした後、マイクロソフトによってライセンス認証される必要があります。KMS キーをインストールすると、KMS ホストでキー管理サービスが有効になります。KMS キーのインストール後、電話またはオンラインを使って KMS ホストのライセンス認証を完了します。この初期のライセンス認証以降、KMS ホストがマイクロソフトに情報を通信することはありません。

KMS キーは、KMS ホスト上にのみインストールされます。個々の KMS クライアントにはインストールされません。Windows 7 および Windows Server 2008 R2 には、KMS キーの KMS クライアント コンピューターへの不注意なインストールを防止できるセーフガードが備わっています。ユーザーが KMS キーをインストールしようとすると、常に図 1 に示す警告が表示されます。

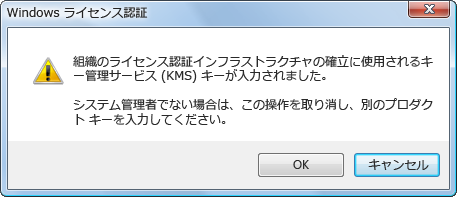


図 1 KMS キーのインストール

### 後続の KMS ホストのライセンス認証

各 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かまいません) 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。

組織に 7 台以上の KMS ホストが必要な場合、ライセンス認証コール センターに連絡して例外を要求することにより、組織の KMS キーに対する追加ライセンス認証を要求できます。詳細については、ボリューム ライセンスの Web サイト <http://go.microsoft.com/fwlink/?LinkID=73076> を参照してください。

### 既存の KMS ホストのアップグレード

Windows Server 2003、Windows Vista、または Windows Server 2008 を実行している KMS ホストを、Windows 7 および Windows Server 2008 R2 を実行している KMS クライアントをサポートするように構成できます。Windows Vista および Windows Server 2008 の場合、拡張 KMS クライアントをサポートするファイルを持つパッケージを使って KMS ホストを更新する必要があります。このパッケージは、Microsoft ダウンロード センター (<http://www.microsoft.com/downloads>) または Windows Update and Windows Server Update Services (WSUS) を通じて利用できます。パッケージが KMS ホストにインストールされたら、Windows 7 と Windows Server 2008 R2 をサポートするように設計された KMS キーを、前の説明に従ってインストールおよびライセンス認証できます。新しいバージョンの Windows オペレーティング システムをサポートする KMS キーは、KMS クライアントとして動作している前のボリューム ライセンス エディションの Windows もサポートします。

Windows Server 2003 KMS ホストを更新する場合、すべての必要なファイルが KMS 1.2 ダウンロード可能  
パッケージに含まれています。パッケージは、Microsoft ダウンロード センター <http://www.microsoft.com/downloads> を通じて利用できます。

### KMS クライアントの計画

既定で、ボリューム ライセンス エディションの Windows Vista、Windows 7、Windows Server 2008、および Windows Server 2008 R2 を実行しているコンピューターは、KMS クライアントです。追加の構成は不要です。KMS クライアントは、DNS に KMS サービスを発行する SRV RR をクエリすることで、KMS ホストを自動的に検索できます。ネットワーク環境が SRV RR を使用しない場合は、特定の KMS ホストを使用するため KMS クライアントを手動で構成できます。

KMS クライアントを手動で構成するには、このガイドで後述する「KMS ホストの手動での指定」の手順に従い  
ます。

### 標準ユーザーとしてのライセンス認証

Windows 7 および Windows Server 2008 R2 では、ライセンス認証に管理者特権は不要です。ただし、この変更では、標準ユーザー アカウントを使って Windows 7 または Windows Server 2008 R2 のライセンス認証された状態を解除することは許可されていません。“rearm” などの他のライセンス認証またはライセンス関連のタスクには、依然として管理者アカウントが必要です。

# プロダクト キーのニーズの判断

Windows 7 および Windows Server 2008 R2 オペレーティング システムには、さまざまなエディションがあります。ボリューム アクティベーションと組織の要件に合ったプロダクト キーの数を合理化するために、マイクロソフトではプロダクト キー グループを作成し、プロダクト キーを個々のエディションではなく製品グループに適用させるようにしました。

## KMS キーの選択

KMS では、プロダクト キーは製品グループに関連付けられており、その特定製品グループ内の Windows エディションのほか、その製品階層の下位にあるエディションもライセンス認証できます。最初の、最も包括的でない階層グループは、クライアント ボリューム ライセンス製品グループで、サーバー グループ C は、KMS 階層で最も包括的なグループです。

この階層には、Windows Vista と Windows Server 2008 のボリューム ライセンス エディションとプロダクト   
キー グループまで含まれます。各プロダクト キー グループに対して別個の KMS キーが発行され、Windows 7 と Windows Vista のどちらの場合も 1 つのクライアント VL 用 KMS キーにアクセスします。より新しい Windows 製品用の KMS キーで 1 つ前の世代もライセンス認証されるため、1 つの KMS キーでエディションや世代の異なる Windows をライセンス認証できます。表 1 に、製品グループ間の相関関係を示します。

表 1. 製品グループの相関関係

| ボリューム ライセンス  プロダクト キー グループ | Windows エディション  (Windows 7 および  Windows Server 2008 R2) | Windows エディション  (Windows Vista および  Windows Server 2008) |
| --- | --- | --- |
| クライアント VL | * Windows 7 Professional * Windows 7 Enterprise | * Windows Vista Business * Windows Vista Enterprise |
| サーバー グループ A | * Windows Web Server® 2008 R2 * Windows Server 2008 R2 HPC Edition * Windows HPC Server 2008 R2 | * Windows Web Server 2008 * Windows Compute Cluster Server 2008 |
| サーバー グループ B | * Windows Server 2008 R2 Standard * Windows Server 2008 R2 Enterprise | * Windows Server 2008 Standard * Windows Server 2008 Enterprise * Hyper-V™ が組み込まれていない エディションを含む |
| サーバー グループ C | * Windows Server 2008 R2 Datacenter * Windows Server 2008 R2 for Itanium-Based Systems | * Windows Server 2008 Datacenter * Windows Server 2008 for Itanium-Based Systems * Hyper-V が組み込まれていない エディションを含む |

## KMS ホストの選択

前に説明したように、KMS は、物理コンピューターまたは仮想マシン上のクライアントまたはサーバー オペレーティング システムにホストできます。KMS ホスト システムを選択するときには、KMS を使ってライセンス認証されるオペレーティング システムのエディションを考慮します。Windows 7 でホストされる KMS は、クライアント オペレーティング システム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 は、クライアント コンピューターとサーバー コンピューターをライセンス認証できます。この階層の説明については、表 2 を参照してください。

表 2 KMS 階層

| プロダクト キー  グループ | KMS をホストできるオペレーティング  システム (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 Server 2003 1.2 用 KMS | * 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 Server 2003 1.2 用 KMS * Windows Web Server 2008 * Windows Web Server 2008 R2 * Windows HPC Server 2008 * Windows HPC Server 2008 R2 | 前の製品エディションと 次の製品エディション:   * 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 | 前の製品エディションと 次の製品エディション:   * Windows Server 2008 R2 Standard * Windows Server 2008 R2 Enterprise * Windows Server 2008 Standard * Windows Server 2008 Enterprise | 前の製品エディションと 次の製品エディション:   * Windows Server 2008 R2 Standard * Windows Server 2008 R2 Enterprise * Windows Server 2008 Standard * Windows Server 2008 Enterprise |
| サーバー グループ C | 前の製品エディションと 次の製品エディション:   * Windows Server 2008 R2 Datacenter * Windows Server 2008 Datacenter * Windows Server 2008 for Itanium-Based Systems | 前の製品エディションと 次の製品エディション:   * Windows Server 2008 R2 Datacenter * Windows Server 2008 Datacenter * Windows Server 2008 for Itanium-Based Systems |

# KMS ライセンス認証の展開

KMS ライセンス認証は、最小限の管理作業で行うことができます。ネットワーク環境に動的ドメイン名システム (DDNS) が実装されており、コンピューターでサービスの自動発行が有効になっている場合は、わずかな作業で KMS ホストを展開できます。組織内に複数の KMS ホストがある場合や、ネットワークで DDNS がサポートされていない場合は、追加の構成作業が必要になることがあります。

警告 このセクションの手順には、レジストリの変更が必要になる場合があります。レジストリ エディターやその他の方法を使用してレジストリを不適切に変更すると、問題が発生する場合があります。発生した問題によってはオペレーティング システムの再インストールが必要になることもあります。マイクロソフトでは、このような問題の解決を保証していません。レジストリの変更は、ご自身の責任において行ってください。

以降のセクションでは、次の主要な作業について説明します。

* KMS ホストの構成
* DNS の構成
* KMS ホストのインストール
* KMS クライアントの構成

## 

## KMS ホストの構成

ソフトウェア ライセンス マネージャーは、別名 SL マネージャー (Slmgr.vbs) とも呼ばれ、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スクリプトです。このスクリプトは、対象のコンピューターでローカルに実行するか、別のリモート コンピューターからリモートで実行することが可能ですが、どちらの場合も管理者特権でのコマンド プロンプトから実行する必要があります。標準ユーザーが Slmgr.vbs を実行すると、一部のライセンス データが見つからなくなったり、不正確なデータになったりすることがあり、多くの操作が抑制されます。

Slmgr.vbs は、Wscript.exe または Cscript.exe を使用できます。IT プロフェッショナルはどちらのスクリプト エンジンを使用するかを指定できます。スクリプト エンジンが指定されていない場合、Slmgr.vbs は、既定のスクリプト エンジンである Wscript.exe を使用して実行されます。

**注** KMS には、KMS ホスト上にファイアウォールの例外が必要です。既定の TCP ポートを使用している場合は、Windows ファイアウォールで **KMS トラフィック**の例外を有効にしてください。別のファイアウォールを使用している場合は、TCP ポート 1688 を開きます。既定以外のポートを使用している場合は、ファイアウォール内で独自の TCP ポートを開きます。

変更を有効にするには、ソフトウェア ライセンス サービスを再起動する必要があります。ソフトウェア ライセンス サービスを再起動するには、Microsoft 管理コンソール (MMC) サービスのスナップインを使用するか、管理者特権でのコマンド プロンプトから次のコマンドを実行します。

net stop sppsvc && net start sppsvc

Slmgr.vbs には少なくとも 1 つのパラメーターを指定する必要があります。パラメーターを指定せずにスクリプトを実行すると、スクリプトに関するヘルプ情報が表示されます。表 3 は、Slmgr.vbs コマンドライン オプションとその説明の一覧です。表 3 のパラメーターの大部分は KMS ホストを構成します。ただし、/sai と /sri パラメーターは、ホストに接続した後に KMS クライアントに渡されます。Slmgr.vbs の一般的な構文は、以下のとおりです。

slmgr.vbs /パラメーター

表 3 Slmgr.vbs パラメーター

| パラメーター | 説明 |
| --- | --- |
| /sprt <ポート番号> | KMS ホストの TCP 通信ポートを設定します。<ポート番号> を、使用する TCP ポート番号に置き換えます。既定の設定は、**1688** です。 |
| /cdns | KMS ホストによる自動 DNS 発行を無効にします。 |
| /sdns | KMS ホストによる自動 DNS 発行を有効にします。 |
| /cpri | KMS ホスト プロセスの優先度を下げます。 |
| /spri | KMS ホスト プロセスの優先度を [**通常**] に設定します。 |
| /sai <ライセンス認証の間隔> | KMS クライアントが KMS ホストが見つからないときに KMS クライアントが自身をライセンス認証することを試行する頻度を変更します。<ライセンス認証の間隔> を時間 (分) に置き換えます。既定の設定は、**120** です。 |
| /sri <更新間隔> | KMS クライアントが KMS ホストにアクセスしてライセンスの更新を試行する頻度を変更します。<更新間隔> を時間 (分) に置き換えます。既定の設定は、**10080** (7 日) です。この設定は、ローカルの KMS クライアント設定より優先されます。 |
| /dli | 現在の KMS ライセンス認証カウントを KMS ホストから取得します。 |

### リモートでの Slmgr.vbs の実行

Slmgr.vbs 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、ターゲットのコンピューターのコンピューター名と、そのターゲット コンピューターのローカル管理者権限が与えられたユーザー アカウントのユーザー名とパスワードです。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は、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。

次の構文は、リモートで Slmgr.vbs を実行する際に追加で指定する必要があるパラメーターを示しています。

slmgr.vbs <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]

### リモートでのソフトウェア ライセンス マネージャー操作のための Windows ファイアウォールの構成

Slmgr.vbs では、Windows Management Instrumentation (WMI) が使用されます。したがって、管理者は WMI トラフィックを許可するように Windows ファイアウォールを構成する必要があります。

* 単一のサブネットでは、Windows ファイアウォール内の **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、**Windows Management Instrumentation (ASync-In)**、**Windows Management Instrumentation (DCOM-In)**、および **Windows Management Instrumentation (WMI-In)** の各接続を有効にします。さらに、その範囲内のリモート 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 ([管理ツール] フォルダー) を使用します。

注 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 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属しているコンピューターに対して Slmgr.vbs をリモートで実行できます。これには、KMS クライアント上のレジストリ サブキー   
**HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System** 内に**DWORD**値 **LocalAccountTokenFilterPolicy** を作成します。この値を **0x01** に設定します。

## DNS の構成

以降のセクションでは、ボリューム アクティベーションで動作するための DNS の構成についての概念を説明し  
ます。

* 複数の KMS ホストを使用する場合は、「SRV レコードに対する既定の DNS アクセス許可の変更」セクションを参照してください。
* 別の DNS サーバーを使用する KMS クライアントで KMS ホストを検索できるようにする場合は、「複数の DNS ドメインへの発行」セクションを参照してください。
* KMS ホストに対して手動で SRV リソース レコードを追加する場合は、「DNS に SRV レコードを手動で作成」、「BIND 8.2 以降の DNS サーバーの SRV レコードの手動作成」、および「KMS SRV レコードの DNS への発行の無効化」の各セクションを参照してください。

注 DNS の変更は、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。

### SRV レコードに対する既定の DNS アクセス許可の変更

KMS ホストを 1 台のみ使用する場合は、DNS 内のアクセス許可を構成する必要はありません。既定の動作では、コンピューターが SRV RR を作成し、それを更新できます。ただし、複数の KMS ホストが存在する場合 (通常の場合)、SRV の既定のアクセス許可を変更しなければ、他のホストでは SRV RR を更新できません。

次に示すハイレベルな手順は、マイクロソフトにおける環境の一例です。詳細な手順は組織ごとに異なる場合があり、目的を達成するための唯一の方法にはならないので、この例では詳細な手順については記載しません。

1. AD DS でグローバル セキュリティ グループを作成します。これは KMS ホストで使用するためのものです。たとえば、「主要な管理サービス グループ」という名前のグループを作成します。
2. 各 KMS ホストをこのグループに追加します。KMS ホストはすべて同じドメインに参加する必要があり  
   ます。
3. 1 台目の KMS ホストを作成すると、オリジナルの SRV レコードが作成されます。1 台目の KMS ホストが SRV リソース レコードを作成できない場合、組織で既定のアクセス許可を変更していることが原因である可能性があります。この場合、「DNS に SRV レコードを手動で作成」セクションの説明に従って、SRV RR を手動で作成します。
4. グローバル セキュリティ グループのメンバーが更新できるように SRV グループのアクセス許可を設定します。

**注** ドメイン管理者は組織内の管理者に上記の手順を実行する権限を委任できます。これには、AD FS 内にセキュリティ グループを作成し、そのグループに SRV レコードを変更する権限を与え、その委任を追加します。

### 複数の DNS ドメインへの発行

既定では、KMS ホストは、その KMS ホストが属している 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。

DNS ドメイン名が複数存在する場合、KMS ホストが SRV RR 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。このレジストリ値を設定すると、プライマリ DNS サフィックスとして指定されたドメイン内のみに発行する KMS ホストの既定の動作が中断します。

必要に応じて、優先度および重みパラメーターを 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を定義できます。

注 DNS の変更は、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。変更をあまり頻繁に行うと ([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。

複数の DNS ドメイン内の KMS を自動発行するには、KMS を発行する各 DNS ドメインのサフィックスを、レジストリ サブキー   
**HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform** の複数文字列値 **DnsDomainPublishList** に追加します。値を変更した後に、SRV RR を作成するためにソフトウェア ライセンス サービスを再起動します。

注 このキーは、Windows Vista® の場所である**HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SL** から変更されました。

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、次にそれを追加の KMS ホスト上のレジストリにインポートします。この手順が正常に実行されたことを確認するには、各 KMS ホスト上のアプリケーション イベント ログを確認します。イベント ID 12294 は、KMS ホストによって SRV RR が正常に作成されたことを示します。イベント ID 12293 は、SRV RR の作成が失敗したことを示します。エラー コードの完全な一覧については、『ボリューム アクティベーション 2.0 運用ガイド』 ([http://technet.microsoft.com/ja-jp/library/cc303695.aspx](http://technet.microsoft.com/en-us/library/cc303695.aspx)) を参照してください。

### DNS に SRV レコードを手動で作成

環境内で DDNS がサポートされていない場合、KMS ホストを発行するために SRV RR を手動で作成する必要があります。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.vbs スクリプトを **/cdns** コマンドライン オプションと共に使用します。Slmgr.vbs スクリプトの詳細については、「KMS ホストの構成」セクションを参照してください。

注 手動で作成した SRV RR を、KMS ホストが他のドメインで自動発行した SRV RR 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。

DNS マネージャーを使用して、適切な前方参照ゾーンでその場所に適した情報を使用して新しい SRV RR 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 4 に SRV RR の設定例を示します。

表 4 SRV リソース レコード

| 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) |

### BIND 8.2 以降の DNS サーバーの SRV レコードの手動作成

組織で Microsoft DNS 以外のサーバーを使用する場合、その DNS サーバーが BIND 8.2 以降に対応している場合は必要な SRV RR を作成できます。レコードを作成する場合、表 5 に示した情報を指定します。表 5 に示す優先度と重みの設定は、Windows 7 および Windows Server 2008 R2 でのみ使用します。

表 5 SRV RR 情報

|  |  |
| --- | --- |
| 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 |

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; };

注 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。

### KMS SRV レコードの DNS への発行の無効化

KMS ホストは、DNS に SRV RR を作成することにより KMS ホスト自身の存在を自動的に発行します。KMS ホストによる DNS の自動発行を無効にするには、Slmgr.vbs スクリプトを **/cdns** コマンドライン オプションと共に使用します。

DNS の自動発行を無効にするには Slmgr.vbs スクリプトを使用することをお勧めしますが、レジストリに **DisableDnsPublishing** という名前の新しい **DWORD** 値を作成して、その値を **1** に設定することでも DNS の自動発行を無効にできます。この値は、レジストリ サブキー   
**HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform** にあります。KMS SRV レコードの DNS への発行のための既定の動作を再度有効にするには、値を **0** に設定します。

## KMS ホストのインストール

KMS 機能を有効にするには、KMS キーを KMS ホストにインストールし、マイクロソフトのライセンス認証サービスを使用してインターネット経由または電話でそのホストに対してライセンス認証を行います。Windows 7 または Windows Server 2008 R2 を実行しているコンピューターは、KMS ホストとして機能させることができます。

また、Windows Vista、Windows Server 2003、および Windows Server 2008 も KMS ホストとして機能させることができます。KMS ホストをライセンス認証できる KMS クライアントは、KMS ホストのライセンス認証に使用するホスト キーによって異なります。KMS ホスト キーの詳細については、『ボリューム アクティベーション 2.0 計画ガイド』 (<http://technet.microsoft.com/ja-jp/library/cc303276.aspx>) を参照してください。

管理者特権でのコマンド プロンプトを使用して Windows 7 または Windows Server 2008 R2 コンピューター上に KMS キーをインストールし、ライセンス認証を行います。

* KMS キーをインストールするには、コマンド プロンプトで「**slmgr.vbs /ipk <KmsKey>**」と入力します。
* オンラインでライセンス認証するには、コマンド プロンプトで「**slmgr.vbs /ato**」と入力します。
* 電話回線を使用してライセンス認証するには、コマンド プロンプトで「**slui.exe 4**」と入力します。

KMS キーをライセンス認証した後に、ソフトウェア ライセンス サービスを再起動します。

Windows 7 および Windows Server 2008 R2 では、管理者がユーザーインタフェース (UI) を使用して KMS ホストをインストールすると常に図 2 に示す警告メッセージが表示されます (Slmgr.vbs スクリプトを使用して KMS ホストをインストールした場合はこの警告は表示されません)。このメッセージは、管理者が KMS ホストに指定しないコンピューター上に間違って KMS キーをインストールすることを防止するためのものです。

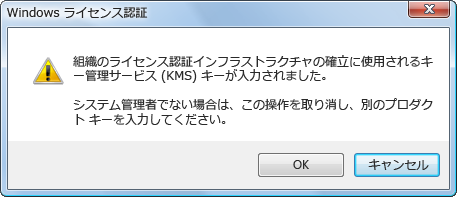


図 2 KMS キー警告

KMS ホストが正しく構成されたかどうかを確認するには、KMS カウントを調べて増加しているかどうかをチェックします。KMS ホストのコマンド プロンプト画面で、「**slmgr.vbs /dli**」と入力して現在の KMS カウントを表示します。また、[アプリケーションとサービス ログ] フォルダーのキー管理サービス ログを調べて、イベント ID 12290 が発生していないかどうかをチェックできます。キー管理サービス ログには、KMS クライアントからのライセンス認証要求が記録されています。各イベントには、コンピューターの名前と、各ライセンス認証要求のタイム スタンプが表示されます。

## KMS クライアントの構成

このセクションでは、コンピューターを KMS クライアントとしてインストールおよび構成するための概念を説明します。既定では、Windows Vista、Windows 7、Windows Server 2008、および Windows Server 2008 R2 のボリューム ライセンス エディションは、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オペレーティング システム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。

DNS を使用して KMS ホストを検索するように KMS クライアントを構成しているが、KMS クライアントが DNS から SRV レコードを受け取らない場合、Windows 7 および Windows Server 2008 R2 ではイベント ログにエラーが記録されます。

### KMS ホストの手動での指定

KMS ホスト キャッシュを使用して KMS ホストを KMS クライアントに手動で割り当てることができます。KMS ホストを手動で割り当てると、KMS クライアント上での KMS の自動探索が無効になります。KMS ホストを KMS クライアントに手動で割り当てるには、次のコマンドを実行します。

slmgr.vbs /skms <値>:<ポート>

この場合、<値> は、KMS ホストの <KMS\_FQDN>、<IPv4 アドレス>、<Netbios 名> のいずれかで、<ポート> は KMS ホスト上の TCP ポートです。

### KMS クライアントの自動探索の有効化

既定では、KMS クライアントは KMS ホストの探索を自動的に試行します。手動で KMS ホストを KMS クライアントに割り当てると、自動探索を無効にすることができます。この操作を行うと、KMS クライアントのキャッシュから KMS ホスト名もクリアされます。自動探索が無効になっている場合、コマンド プロンプトで **slmgr.vbs /ckms** を実行すると、再度有効にすることができます。

### サフィックス エントリの KMS クライアントへの追加

SRV RR を含む DNS サーバーのアドレスを KMS クライアント上のサフィックス エントリとして追加すると、1 台の DNS サーバー上で KMS ホストをアドバタイズして、他のプライマリ DNS サーバーを持つ KMS クライアントがそれを検索できるようになります。KMS クライアント上でのドメイン サフィックス検索一覧の構成の詳細については、Microsoft サポート技術情報「DNS クライアントでのドメイン サフィックス検索一覧の設定方法」(<http://support.microsoft.com/kb/275553>) を参照してください。

### KMS クライアントの展開

このセクションに記述している情報は、Windows オペレーティング システムを展開およびライセンス認証を行うために Windows Automated Installation Kit (Windows AIK) を使用するボリューム ライセンスのお客様を対象にしています。展開のために以下に説明するシステム準備ツール (Sysprep) または Slmgr.vbs スクリプトを使用して KMS を準備します。

* **Sysprep。**イメージをキャプチャする前に、Sysprep を **/generalize** コマンドライン オプションと共に実行して、ライセンス認証タイマー、セキュリティ識別子 (SID)、およびその他の重要な設定をリセットします。ライセンス認証タイマーをリセットすると、イメージの展開前にイメージの猶予期間が切れないようにすることができます。Sysprep.exe を実行しても、インストールされたプロダクト キーは削除されず、ミニセットアップ中に新しいキーの入力を求められることはありません。リセット可能な回数が残っていない場合、Sysprep 操作は終了しますが、ライセンス認証タイマーは変更されず、状況を説明するエラーが返されます。
* **Slmgr.vbs。**社内で使用するためにデモ用の仮想マシンを構築 (たとえば、組織の営業部門用または一時的なトレーニング環境用の仮想マシンの構築) した場合、Slmgr.vbs スクリプトを **/rearm** コマンドライン オプションと共に実行すると、さらに 30 日間猶予期間が延長されます。このとき、ライセンス認証タイマーはリセットされますが、コンピューターに対する他の変更は行われません。Windows 7 または Windows Server 2008 R2 を実行しているコンピューターでは、ライセンス認証タイマーを 3 回までリセットできます。

### 

### KMS クライアントの手動によるライセンス認証

既定では、KMS クライアントは事前に設定された間隔で自動的にライセンス認証を試行します。切断されたクライアントなどの KMS クライアントをユーザーに配布する前に手動でライセンス認証するには、コントロール パネルの [システム] 項目を使用するか、管理者特権でのコマンド プロンプトで **slmgr.vbs /ato** を実行します。Slmgr.vbs スクリプトによって、ライセンス認証の成功/失敗が報告され、結果コードが表示されます。ライセンス認証を行うには、KMS クライアントは組織のネットワーク上の KMS ホストにアクセス可能である必要があります。

### MAK クライアントの KMS への変換および KMS クライアントの MAK への変換

既定では、Windows 7 および Windows Server 2008 R2 オペレーティング システムでは、ライセンス認証を行うために KMS が使用されます。既存の KMS クライアントをマルチ アクセス キー (MAK) クライアントに変更するには、単に MAK をインストールします。同様に、MAK クライアントを KMS クライアントに変更する場合、次のコマンドを実行します。

slmgr.vbs /ipk <KMS セットアップ キー>

この場合、<KMS セットアップ キー> は、表 6 に示すセットアップ キーの 1 つです。KMS セットアップ キーのインストール後に、**cscript slmgr.vbs /ato** を実行して KMS クライアントのライセンス認証を行います。

表 6 KMS クライアントのセットアップ キー

| オペレーティング システム エディション | プロダクト キー |
| --- | --- |
| Windows 7 | |
| Windows 7 Professional | FJ82H-XT6CR-J8D7P-XQJJ2-GPDD4 |
| Windows 7 Professional N | MRPKT-YTG23-K7D7T-X2JMM-QY7MG |
| Windows 7 Enterprise | 33PXH-7Y6KF-2VJC9-XBBR8-HVTHH |
| Windows 7 Enterprise N | YDRBP-3D83W-TY26F-D46B2-XCKRJ |
| Windows Server 2008 R2 | |
| Windows Server 2008 R2 HPC Edition | FKJQ8-TMCVP-FRMR7-4WR42-3JCD7 |
| Windows Server 2008 R2 Datacenter | 74YFP-3QFB3-KQT8W-PMXWJ-7M648 |
| Windows Server 2008 R2 Enterprise | 489J6-VHDMP-X63PK-3K798-CPX3Y |
| Windows Server 2008 R2 for Itanium-Based Systems | GT63C-RJFQ3-4GMB6-BRFB9-CB83V |
| Windows Server 2008 R2 Standard | YC6KT-GKW9T-YTKYR-T4X34-R7VHC |
| Windows Web Server 2008 R2 | 6TPJF-RBVHG-WBW2R-86QPH-6RTM4 |

### 製品版のボリューム アクティベーションへの変換

Windows 7 Professional および Windows Server 2008 R2 の製品版は、KMS クライアントに変換できます。ただし、組織で適切なボリューム ライセンスを取得し、製品使用権説明書に記載されている条項に従っている必要があります。Windows 7 Professional および Windows Server 2008R2 のすべてのエディションを製品版から KMS クライアントに変換するには、オペレーティング システムのインストール時に [**プロダクト キー**] ページをスキップします。インストールが完了したら、管理者特権でのコマンド プロンプト画面で次のコマンドを入力します。

Slmgr.vbs /ipk <セットアップ キー>

この場合、<セットアップ キー> は、表 6 の KMS クライアントのセットアップ キーです。セットアップ キーは、Windows 7 または Windows Server 2008 R2 にそれぞれ対応しています。

# コンピューターの再ライセンス認証

Windows 7 および Windows Server 2008 R2 では、これらのオペレーティング システムがインストールされているコンピューターのハードウェア構成が定期的に確認されます。ハードウェア構成が大幅に変更されていることがオペレーティング システムによって検出されると、再ライセンス認証が要求されます。実際の重み係数としきい値は、発展を続けるコンピューター ハードウェア市場に対応するために変更される場合があります。KMS クライアントでは、ハード ディスクの変更に焦点を当て再ライセンス認証が必要であるかどうかを判断しています。

クライアント ライセンス認証は、180 日間有効 (この期間をライセンス認証の検証間隔といいます) です。ライセンス認証された状態であり続けるには、KMS クライアントは、ライセンス認証を更新するため 180 日ごとに 1 回以上 KMS ホストに接続する必要があります。既定では、KMS クライアント コンピューターは、7 日ごとにライセンス認証の更新を試行します。クライアントのライセンス認証が更新されると、ライセンス認証の検証間隔が再び始まります。