ボリューム アクティベーション 計画ガイド

Windows 7 および Windows Server 2008 R2

Microsoft Corporation

公開: 2009 年 6 月

要約

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し管理するのに役立ちます。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、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情報技術 (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、Active Directory、Hyper-V、MSDN、Windows、Windows ロゴ、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

[はじめに 5](#_Toc231723147)

[製品のライセンス認証について 6](#_Toc231723148)

[ライセンス認証のオプション 6](#_Toc231723149)

[小売業 6](#_Toc231723150)

[相手先ブランド供給 7](#_Toc231723151)

[ボリューム ライセンス 7](#_Toc231723152)

[ボリューム アクティベーションのモデル 8](#_Toc231723153)

[キー管理サービス 8](#_Toc231723154)

[マルチ ライセンス認証キー 9](#_Toc231723155)

[システムがライセンス認証されていない場合の対処方法? 9](#_Toc231723156)

[猶予期間 9](#_Toc231723157)

[猶予期間が経過した場合 10](#_Toc231723158)

[プロダクト キー 10](#_Toc231723159)

[利用可能なライセンス認証モデルの確認 11](#_Toc231723160)

[キー管理サービス 11](#_Toc231723161)

[最小コンピューター要件 11](#_Toc231723162)

[KMS の使用法 13](#_Toc231723163)

[KMS 展開の計画 15](#_Toc231723164)

[マルチ ライセンス認証キー 18](#_Toc231723165)

[ボリューム ライセンス認証管理ツール 18](#_Toc231723166)

[MAK アーキテクチャ 19](#_Toc231723167)

[クライアント接続の評価 20](#_Toc231723168)

[コア ネットワーク 23](#_Toc231723169)

[隔離されたネットワーク 23](#_Toc231723170)

[高セキュリティ ゾーン 23](#_Toc231723171)

[支社 25](#_Toc231723172)

[切断された個々のコンピューター 26](#_Toc231723173)

[テストおよび開発ラボ 27](#_Toc231723174)

[コンピューターのライセンス認証方法へのマップ 28](#_Toc231723175)

[プロダクト キーのニーズの判断 29](#_Toc231723176)

[MAK プロダクト キー グループの選択 30](#_Toc231723177)

[KMS キーの選択 31](#_Toc231723178)

[KMS ホストの選択 33](#_Toc231723179)

[監視およびレポートのニーズの判断 35](#_Toc231723180)

[Windows Management Instrumentation 35](#_Toc231723181)

[System Center Configuration Manager 35](#_Toc231723182)

[イベント ログ 35](#_Toc231723183)

[KMS Management Pack 36](#_Toc231723184)

[ボリューム ライセンス認証管理ツール 36](#_Toc231723185)

[付録 A: マイクロソフトに送信される情報 37](#_Toc231723186)

[付録 B: ライセンス状態 38](#_Toc231723187)

[ライセンス認証されています 39](#_Toc231723188)

[猶予期間 39](#_Toc231723189)

[正規 39](#_Toc231723190)

[通知 40](#_Toc231723191)

# はじめに

ボリューム アクティベーションは、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、IT プロフェッショナルが製品ライセンス認証プロセスを自動化し管理するのに役立つ構成可能なソリューションです。このガイドでは、特に Windows 7 および Windows Server 2008 R2 オペレーティング システムのボリューム アクティベーション展開の計画に役立つ計画手順とシナリオを提供します。

**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計画ガイドを提供します。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。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、マイクロソフト Web サイト (<http://go.microsoft.com/fwlink/?LinkID=75674>) で『ボリューム アクティベーション 2.0 テクニカル ガイド』 (英語) を参照してください。

ボリューム アクティベーション展開には、次の手順が含まれます。

1. 製品のライセンス認証について学習します。
2. 利用可能なライセンス認証モデルを確認します。
3. クライアント接続を評価します。
4. 物理コンピューターまたは仮想マシンをライセンス認証方法にマップします。
5. プロダクト キーのニーズを判断します。
6. 監視およびレポートのニーズを判断します。

# 製品のライセンス認証について

プロダクト アクティベーション（製品のライセンス認証）とは、ソフトウェアとその製造元の正当性を検証するプロセスです。ライセンス認証により、製品が正規状態で、プロダクト キーが侵害されていないことを確認します。これは、クレジット カードや新しい携帯電話のライセンス認証に似ています。ライセンス認証によって、ソフトウェアのプロダクト キーとそのソフトウェアのデバイスにおける特定のインストールの間に関係が構築されます。

マイクロソフトによって使用されるすべてのライセンス認証方法は、ユーザーのプライバシーが保護されるように設計されています。ライセンス認証中に送信されるデータをコンピューターまたはユーザーまでたどることはできません。収集されるデータは、ソフトウェアが正規ライセンスのコピーであることを確認するために使用されます。その後、ひとまとめにされて統計解析に使用されます。マイクロソフトがこの情報をユーザーまたは組織の特定や、ユーザーまたは組織への連絡に使用することはありません。

たとえば、オンライン ライセンス認証中、ソフトウェア バージョン、言語、プロダクト キー、インターネット プロトコル (IP) アドレスなどの情報、およびデバイスのハードウェアに関する情報が、マイクロソフトに送信されます。IP アドレスは、要求の場所を確認する目的でのみ使用されます。Windows 7 Starter など Windows の一部のエディションでは、ライセンス認証が、特定のターゲット市場に地理的に限定されているためです。

## ライセンス認証のオプション

Windows 7 および Windows Server 2008 R2 のライセンスは、3 つの基本チャネル (小売業、相手先ブランド供給 (OEM)、ボリューム ライセンス) のいずれかを通じて取得できます。各チャネルには、固有のライセンス認証方法があります。組織は、3 つの利用可能なチャネルのいずれからでもオペレーティング システムを取得できるため、ライセンス認証方法の組み合わせを選択できます。

### 小売業

小売店を通じて取得された Windows 7 およびWindows Server 2008 R2 製品は、個別にライセンスされ、Windows Vista および Windows Server 2008 オペレーティング システムの製品版と同じ方法でライセンス認証されます。購入されたコピーにはそれぞれ、製品インストール中にユーザーが入力する 1 個の一意なプロダクト キーが付属しています (製品パッケージ上に印刷されています)。コンピューターは、オペレーティング システムのインストールが完了した後に、このプロダクト キーを使用してライセンス認証を完了します。この最後のライセンス認証手順は、オンラインまたは電話を使って実行できます。

### 相手先ブランド供給

ほとんどの OEM は、標準ビルドの Windows 7 または Windows Server 2008 R2 オペレーティング システムを含むシステムを販売しています。ハードウェア ベンダーは、コンピューターのオペレーティング システムをファームウェア (基本入出力システム、BIOS) に関連付けることで OEM ライセンス認証を実行します。このプロセスはコンピューターがお客様に送られる前に発生するため、ユーザーによる追加アクションは不要です。このライセンス認証方法は、OEM ライセンス認証と呼ばれています。

OEM ライセンス認証は、システム上で OEM 供給イメージを使用する限り、有効です。カスタマイズされたイメージを作成するには、OEM によって供給されたイメージを、カスタム イメージを作成するための土台として使用できます。それ以外の場合は、別のライセンス認証方法を使用する必要があります。Windows のカスタマイズおよびライセンス認証の影響の詳細については、次の [ホワイトペーパー](http://go.microsoft.com/fwlink/?LinkID=137292&clcid=0x409) (英語) を参照してください。

注OEM ライセンス認証は、OEM チャネルを通じて購入された Windows がインストールされているコンピューターに適用可能です。

### ボリューム ライセンス

Microsoft ボリューム ライセンスは、組織のサイズと購買優先順位に合わせて作成された、カスタマイズされたプログラムを提供します。これらのプログラムにより、組織がライセンスを簡単に管理できる、単純で柔軟性のある、低価格のソリューションが得られます。ボリューム ライセンスを購入するには、組織とマイクロソフトがボリューム ライセンス契約を締結する必要があります。

Windows クライアント オペレーティング システムを搭載した新しいコンピューターに対して新規購入ライセンスを取得する正式な方法は、2 つあります。最初のもっとも経済的な方法は、相手先ブランド供給を通じてプレインストールされているライセンスを入手する方法です。もう 1 つのオプションは、FPP パッケージ小売製品を購入する方法です。

Open License、Select License、Enterprise Agreement などの Microsoft ボリューム ライセンス プログラムは、Windows クライアント オペレーティング システムに対するアップグレードだけをカバーします。ボリューム ライセンスを通じて取得されたアップグレード権をこれらのコンピューター上で行使するには、各コンピューターに条件を満たした OS ライセンスが必要です。

条件を満たした OS のリストを含むボリューム ライセンスの詳細については、<http://go.microsoft.com/fwlink/?LinkId=73076> を参照してください。

注:   Windows 7 Enterprise など、ボリューム ライセンス チャネルを通じてのみ利用可能な Windows のエディションもあります。

##

## ボリューム アクティベーションのモデル

ボリューム アクティベーションを使用すると、ボリューム ライセンスを購入されたお客様は、ユーザーに対して透過的になるようにライセンス認証プロセスを自動化できます。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 プログラムの下で保護されているコンピューターに適用されます。完全にライセンス認証用のツールとして使用され、ライセンスの請求や支払いとは無関係です。

ボリューム アクティベーションは、ボリューム ライセンス認証を完了するためのモデルを 2 つ提供します。キー管理サービス (KMS) とマルチ ライセンス認証キー (MAK) です。KMS を使用すると、組織がそのネットワーク内のシステムをライセンス認証できます。MAK は、マイクロソフトによって提供されたホストされているライセンス認証サービスを使って、1 度に 1 つのシステムをライセンス認証します。顧客は、どちらかまたは両方のキー タイプを使用してその環境内のシステムをライセンス認証できます。

### キー管理サービス

KMS を使用すると、IT プロフェッショナルが、ローカル ネットワーク上でライセンス認証を完了できます。個々のコンピューターが製品のライセンス認証のためにマイクロソフトに接続する必要がなくなります。KMS は、専用システムを必要としない軽量サービスで、他のサービスを提供するシステムで簡単に共同でホストできます。既定で、ボリューム エディションの Windows 7 および Windows Server 2008 R2 は、KMS サービスをホストするシステムに接続してライセンス認証を要求します。ユーザーからのアクションは不要です。

KMS では、ネットワーク環境内に一定の台数を超えるコンピューター (物理または仮想マシン) が存在する必要があります。組織には、Windows Server 2008 R2 をライセンス認証するには 5 台以上のコンピューターが、Windows 7 を実行しているクライアントをライセンス認証するには 25 台以上のコンピューターが必要です。これらの最小値は、ライセンス認証のしきい値と呼ばれます。

Windows 7 で KMS ライセンス認証を使用するには、コンピューターに条件を満たす OS ライセンスがあり (通常 OEM を通じて新規 PC 購入の一部として取得します)、BIOS に Windows マーカーが含まれる必要があります。

### マルチ ライセンス認証キー

MAK は、マイクロソフトがホストしているライセンス認証サービスを使用した 1 回限りのライセンス認証に使用されます。MAK を使用してコンピューターをライセンス認証する方法は、2 つあります。最初の方法は MAK 非依存ライセンス認証です。この方法では、各コンピューターはインターネット経由で、または電話を使ってマイクロソフトに個別に接続し、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。2 番目の方法は、MAK プロキシ ライセンス認証です。この方法を使用すると、MAK プロキシとして動作するコンピューターが、ネットワーク上の複数のコンピューターからライセンス認証情報を収集した後、複数のコンピューターを代表してマイクロソフトとの 1 つの接続だけを使用して、ライセンス認証要求を送信します。MAK プロキシ ライセンス認証は、ボリューム ライセンス認証管理ツール (VAMT) を使って構成されます。

**注**   KMS は、ボリューム アクティベーション クライアントの既定のキーです。MAK ライセンス認証を使用するには、MAK キーをインストールする必要があります。KMS クライアントを MAK に変換する方法の詳細については、『[ボリューム アクティベーション展開ガイド](http://go.microsoft.com/fwlink/?LinkId=150083)』を参照してください。

## システムがライセンス認証されていない場合の対処方法?

ライセンス認証は、ユーザーに対して透過的なライセンス認証エクスペリエンスを提供するように設計されています。オペレーティング システムのインストール直後にライセンス認証が発生しない場合でも、Windows 7 および Windows Server 2008 R2 は、オペレーティング システムのすべての機能を一定期間 (猶予期間) のあいだ提供します。猶予期間の長さは、Windows 7 と Windows Server 2008 R2 の場合、30 日です。猶予期間が経過すると、どちらのオペレーティング システムも、ユーザーにコンピューターのライセンス認証を促す通知を表示します。

### 猶予期間

初期の猶予期間中、コンピューターにライセンス認証が必要であることを知らせる定期的な通知があります。1 日に 1 回、ログオン プロセス中、ユーザーにオペレーティング システムのライセンス認証を促す通知が表示されます。これは、猶予期間の残り日数が 3 日になるまで続きます。猶予期間の残り 3 日間のうち、最初の 2 日間、通知が 4 時間ごとに表示されます。猶予期間の最終日には、通知が毎正時に表示されます。

### 猶予期間が経過した場合

初期の猶予期間が経過した後、またはライセンス認証が失敗した後、Windows 7 および Windows Server 2008 R2 は、オペレーティング システムにライセンス認証が必要であることをユーザーに通知し続けます。オペレーティング システムがライセンス認証されるまで、コンピューターにライセンス認証が必要であることを知らせるアラームが、製品の次に示す複数の場所で表示されます。

* ログオン中、ユーザー資格情報の入力後に [通知] ダイアログ ボックスが表示されます。
* 通知が、画面の一番下の通知領域の上に表示されます。
* 継続的なデスクトップ通知が、デスクトップの背景が黒の状態で表示されたままになります。
* ユーザーが特定の Windows アプリケーションを開いたときに、アラームが表示される場合があります。

## プロダクト キー

ボリューム アクティベーションによって、ボリューム ライセンスのお客様のプロダクト キーの取得方法が変化することはありません。MAK キーおよび KMS キーは、ボリューム ライセンス サービス センター (VLSC) の Web サイト (<http://go.microsoft.com/fwlink/?LinkId=107544>) で、またはライセンス認証コール センターへの電話を通じて取得できます。サービス プロバイダ ライセンス契約 (SPLA) パートナーは、ライセンス認証コール センターへの電話を通じてのみキーを取得できます。アメリカ国内のお客様は、1-888-352-7140 にお問い合わせください。その他の国のお客様は、最寄りのサポート センターに問い合わせる必要があります。世界全域のライセンス認証コール センターの電話番号については、<http://go.microsoft.com/fwlink/?LinkId=107418> を参照してください。サポート センターに電話をかける場合は、お客様にボリューム ライセンス契約が必要となります。

ボリューム ライセンスのお客様は、いつでも VLSC Web サイトにログオンして KMS キー情報を表示できます。VLSC Web サイトには、MAK の要求および使用方法に関する情報も含まれています。許容ライセンス認証数の増加に関する情報を含む、MAK キーおよび KMS キーの詳細については、「**既存の顧客**」 (<http://go.microsoft.com/fwlink/?LinkId=74008>) (英語) を参照してください。

# 利用可能なライセンス認証モデルの確認

ボリューム アクティベーションは、次のライセンス認証モデルを提供します。

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

選択されるモデルは、組織のサイズ、ネットワーク インフラストラクチャ、接続、およびセキュリティの必要条件に依存します。IT プロフェッショナルは、これらのライセンス認証モデルを 1 つだけ使用するか、または組み合わせて使用するかを選択できます。

**注**トークンベースのライセンス認証は、承認済みの Microsoft ボリューム ライセンスのお客様が利用できる特殊なライセンス認証オプションです。末端システムがネットワークまたは電話と完全に切断されている、特定のシナリオで使用するために設計されています。このオプションでは、お客様は、公開キー基盤 (PKI) およびデジタル証明書 (またはトークン、通常スマート カードに格納されます) を使用して、Windows 7 Enterprise および Windows Server 2008 R2 をローカルにライセンス認証できます。お客様がホストしている KMS や MAK を使用したマイクロソフトがホストしているライセンス認証サービスに接続する必要はありません。トークンベースのライセンス認証の詳細については、マイクロソフト アカウント チームまたはサービス担当者にお問い合わせください。

## キー管理サービス

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、ネットワークに一定数 (ライセンス認証のしきい値といいます) 以上の条件を満たしたコンピューターが存在する必要があります。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。

KMS クライアント コンピューターは、ライセンス認証のしきい値に達した後にライセンス認証されます。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動作しているクライアント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 仮想マシンの場合、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 クライアントのレコードを保持します。KMS ホストは、各 KMS クライアントにクライアント 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。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 クライアントだけが KMS ホストに接続している場合、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 日間有効です。これをライセンス認証の検証間隔といいます。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、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 を含むある 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、読み取り専用ドメイン コントローラ (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する任意の 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 クライアントを実行しているコンピューター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。

* x86 ベース コンピューターの場合: 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)
* x64 ベース コンピューターの場合: 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>) (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、IT プロフェッショナルは、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、『[ボリューム アクティベーション展開ガイド](http://go.microsoft.com/fwlink/?LinkId=150083)』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。

## マルチ ライセンス認証キー

MAK は、マイクロソフトがホストしているライセンス認証サービスを使用した 1 回限りのライセンス認証に使用されます。各 MAK の許容ライセンス認証数は、事前に規定されています。この数はボリューム ライセンス契約に基づいており、組織の正確なライセンス数とは異なります。マイクロソフトがホストしているライセンス認証サービスを使って MAK を使用してライセンス認証を実行するたびに、ライセンス認証数が上限に達するまでカウントされます。

MAK を使用してコンピューターをライセンス認証する方法は、2 つあります。

* MAK 非依存ライセンス認証。各コンピューターは、インターネット経由で、または電話を使ってマイクロソフトに個別に接続し、ライセンス認証される必要があります。MAK 非依存ライセンス認証は、企業ネットワークへの接続を保持しない、組織内のコンピューターに最適です。
* MAK プロキシ ライセンス認証。MAK プロキシ ライセンス認証を使用すると、1 台のコンピューターが複数のコンピューターを代表してマイクロソフトとの 1 つの接続だけを使用して、ライセンス認証要求を行えるようになります。MAK プロキシ ライセンス認証は、ボリューム ライセンス認証管理ツール (VAMT) を使用して構成されます。MAK プロキシ ライセンス認証は、セキュリティ上の問題により、インターネットまたは企業ネットワークへの直接アクセスを制限される場合がある環境に適します。この接続が欠けている開発およびテスト ラボにも適します。

MAK は、企業ネットワークにほとんどまたはまったく接続しないコンピューター、およびライセンス認証を必要とするコンピューターの数が KMS ライセンス認証のしきい値に達しない環境に対してお勧めします。MAK は、個々のコンピューターにも、イメージにも使用できます。イメージは Microsoft 展開ソリューションを使って複製またはインストールできます。MAK は、最初は KMS ライセンス認証を使用するために構成されたコンピューター上でも使用できます。これは、コンピューターをコア ネットワークから切断された環境に移動する場合に便利です。

### ボリューム ライセンス認証管理ツール

Windows 自動インストール キット (Windows AIK) に含まれる VAMT は、複数のコンピューターからライセンス認証要求を収集後、それらをマイクロソフトにまとめて送信するスタンドアロン アプリケーションです。VAMT を使用すると、IT プロフェッショナルが、AD DS、ワークグループ名、IP アドレス、またはコンピューター名を使用して、ライセンス認証するコンピューターのグループを指定できます。VAMT は、ライセンス認証確認コードを受け取ると、ライセンス認証を要求したコンピューターに確認コードを配布します。これらの確認コードは VAMT にもローカルに格納されるため、以前にライセンス認証したコンピューターのイメージを再作成した後、マイクロソフトに連絡せずにコンピューターを再びライセンス認証できます。また、VAMT を使用すると、コンピューターのライセンス認証方法を MAK と KMS 間で簡単に移行できます。

Windows Automated Installation Kit (AIK) for Windows 7 RC (<http://go.microsoft.com/fwlink/?LinkId=136976>) (英語) を Microsoft ダウンロード センターからダウンロードしてください。

#### MAK アーキテクチャ

MAK 非依存ライセンス認証では、MAK プロダクト キーがクライアント コンピューターにインストールされます。コンピューターはこのキーの指示により、インターネット経由で Microsoft サーバーを使ってライセンス認証を行います。MAK プロキシ ライセンス認証では、VAMT が、MAK プロダクト キーをクライアント コンピューターにインストールし、インストール ID (IID) をターゲット コンピューターから取得します。VAMT は、その IID をクライアントに代わってマイクロソフトに送信し、確認 ID (CID) を取得します。次に、CID をインストールしてクライアントをライセンス認証します。

# クライアント接続の評価

各ボリューム アクティベーション方法には、その方法に最も適した特定のネットワーク構成があります。その組織に最適なライセンス認証方法を (場合によっては複数) 選択するには、ネットワーク環境を評価して、さまざまなコンピューターのグループがネットワークにどのように接続するかを特定します。企業ネットワークへの接続、インターネット アクセス、および企業ネットワークに定期的に接続するコンピューターの数は、特定する必要がある重要な構成特性です。ほとんどの中規模から大規模な組織では、クライアント コンピューターがネットワークに接続する方法は多様であるため、ライセンス認証方法を組み合わせて使用しています。

KMS は、組織のコア ネットワークに良好に接続されているコンピューターや、オフサイトのコンピューターなど、定期的に接続されるコンピューターに対して推奨されるライセンス認証方法です。MAK は、接続に制限があるオフサイトのコンピューターや、セキュリティ上の制約によりコア ネットワークに接続できないコンピューターに対して推奨されるライセンス認証方法です。これには、コア ネットワークから隔離されたラボおよび開発環境内のコンピューターが含まれます。

表 1 に、一般的なネットワーク構成と各構成に対するベスト プラクティス推奨を示します。各ソリューションでは、コンピューターの数とライセンス認証クライアントのネットワーク接続を考慮に入れています。

表 1   ネットワーク インフラストラクチャ別の計画の考慮事項

| ネットワーク インフラストラクチャ | 推奨 | 考慮事項 |
| --- | --- | --- |
| コア ネットワーク接続状態が良好なローカル エリア ネットワーク (LAN)最も一般的なシナリオ | 総コンピューター数が KMS ライセンス認証のしきい値を超える場合:* 小規模 (100 台未満): KMS ホストが 1 台
* 中規模 (100 台以上): KMS ホストが 1 台以上
* エンタープライズ: KMS ホストが 2 台以上

総コンピューター数が KMS ライセンス認証のしきい値以下の場合:* MAK (電話またはインターネット)
* MAK プロキシ
 | * KMS ホストの数を最小限に抑えます。
* 各 KMS ホストは、総コンピューター数が KMS ライセンス認証のしきい値を常に超えるようにする必要があります。
* KMS ホストは自律しています。
* KMS ホストは電話またはインターネットを使ってライセンス認証されます。
 |
| 隔離されたネットワーク支社、高セキュリティ ネットワーク セグメント、境界ネットワーク接続状態が良好なゾーン化された LAN | KMS クライアントとホスト間でファイアウォール上のポートを開くことが可能な場合:* コア ネットワークで KMS ホストを使用する

ポリシーによってファイアウォールの変更を禁止している場合:* 隔離されたネットワークでローカル KMS ホストを使用する
* MAK (電話またはインターネット)
* MAK プロキシ
 | * ファイアウォール構成
	+ RPC over TCP (TCP ポート 1688)
	+ クライアントによって開始
* ファイアウォール ルール セットの変更管理
 |
| テストまたは開発ラボ隔離されたネットワーク | 総コンピューター数が KMS ライセンス認証のしきい値を超える場合:* KMS ホストが 1 台 (隔離されたネットワークごとに)

総コンピューター数が KMS ライセンス認証のしきい値以下の場合:* ライセンス認証なし (猶予期間をリセット)
* MAK (電話)
* MAK プロキシを手動で実行
 | * 可変構成
* 限られた数のコンピューター
* 電話を使った KMS ホストおよび MAK ライセンス認証、MAK プロキシを手動で実行
 |
| 個々の切断されたコンピューターインターネットまたはコア ネットワークに接続されていない環境コア ネットワークに定期的に接続するか、または仮想プライベート ネットワーク (VPN) を介して接続する、ローミング状態にあるコンピューターインターネットに接続できるが、コア ネットワークに接続できない、ローミング状態にあるコンピューター | コア ネットワークに定期的に接続するクライアントの場合:* コア ネットワークで KMS ホストを使用

コア ネットワークに接続しない、またはインターネットに接続できないクライアントの場合:* MAK (電話)

コア ネットワークに接続できないネットワークの場合:* 総コンピューター数が KMS ライセンス認証のしきい値を超える場合:
	+ 小規模: KMS ホストが 1 台
	+ 中規模: KMS ホストが 1 台以上
	+ エンタープライズ: KMS ホストが 2 台以上
* 総コンピューター数が KMS ライセンス認証のしきい値以下の場合、MAK 非依存または MAK プロキシを手動で実行

コア ネットワークに接続しないが、インターネットに接続できるクライアントの場合:* MAK (インターネット接続)
 | * 他のネットワークに接続できない制限された環境またはネットワーク
* KMS ホストをライセンス認証し、切断されたネットワークに移動可能
* 電話を使った KMS ホストおよび MAK ライセンス認証、MAK プロキシを手動で実行
 |

次のセクションでは、複数のライセンス認証方法が必要な異種企業環境でのボリューム アクティベーション ソリューションの例について説明します。各シナリオには推奨されるライセンス認証ソリューションがありますが、環境のインフラストラクチャまたはポリシー必要条件によっては、別のソリューションが適している場合があります。

## コア ネットワーク

コア ネットワーク上のコンピューターには、集中型の KMS ソリューションをお勧めします。このソリューションは、インターネットにも接続できる複数のネットワーク セグメント上に、接続状態が良好なコンピューターが存在するネットワーク用です。図 2 に、KMS ホストを持つコア ネットワークを示します。

図 2   コア ネットワーク シナリオ

**注**KMS ホストは、仮想マシンにインストールできますが、別のホスト コンピューターに移動される可能性の少ない仮想マシンを選択します。仮想 KMS ホストが別のホスト コンピューターに移動された場合、オペレーティング システムが基礎ハードウェア内の変化を検出します。KMS ホストは、マイクロソフトに連絡して再びライセンス認証する必要があります。KMS ホストは、マイクロソフトにより最大 9 回ライセンス認証できます。

## 隔離されたネットワーク

多くの組織では、ネットワークが複数のセキュリティ ゾーンに分離されています。重要情報が存在するため高セキュリティ ゾーンを隔離しているネットワークもあれば、物理的に離れているために (支社など) コア ネットワークから分離されているネットワークもあります。

### 高セキュリティ ゾーン

高セキュリティ ゾーンは、他のネットワーク セグメントとの通信を制限するファイアウォールによって分離されたネットワーク セグメントです。TCP ポート 1688 の高セキュリティ ゾーンからの送信と RPC 応答の受信が許可されているため、高セキュリティ ゾーン内のコンピューターがコア ネットワークに接続できる場合は、コア ネットワークに存在する KMS ホストを使って高セキュリティ ゾーン内のコンピューターをライセンス認証します。この方法では、高セキュリティ ネットワーク内のクライアント コンピューターの数が KMS ライセンス認証のしきい値に達する必要はありません。

これらのファイアウォールの例外が認定されておらず、高セキュリティ ゾーン内の総コンピューター数が KMS ライセンス認証のしきい値に達している場合は、ローカル KMS ホストを高セキュリティ ゾーンに追加します。次に、電話を使って高セキュリティ ゾーン内の KMS ホストをライセンス認証します。

図 3 に、企業のセキュリティ ポリシーにより、高セキュリティ ゾーン内のコンピューターとコア ネットワーク間のトラフィックが許可されていない環境を示します。高セキュリティ ゾーンのコンピューター数は KMS ライセンス認証のしきい値に達しているため、高セキュリティ ゾーンには固有のローカル KMS ホストが存在します。KMS ホスト自体は、電話を使ってライセンス認証されます。



図 3   高セキュリティ ネットワーク シナリオ

高セキュリティ ゾーンに数台のコンピューターしかないため KMS が適さない場合は、MAK 非依存ライセンス認証をお勧めします。各コンピューターは、電話を使ってマイクロソフトにより個別にライセンス認証できます。

このシナリオでは VAMT を使った MAK プロキシ ライセンス認証も可能です。高セキュリティ ゾーン内のコンピューターはインターネットに接続できないため、VAMT は、AD DS、コンピューター名、IP アドレス、またはワークグループ内のメンバーシップを使ってコンピューターを検出できます。VAMT は Windows Management Instrumentation (WMI) を使用して MAK プロダクト キーと CID をインストールし、MAK クライアントの状態を取得します。このトラフィックはファイアウォールを通過できないため、高セキュリティ ゾーンにローカル VAMT ホストが存在する必要があります。

### 支社

図 4 に、3 つの支社のクライアント コンピューターをサポートするエンタープライズ ネットワークを示します。サイト A では ローカル KMS ホストを使用します。25 台を超えるクライアント コンピューターが存在し、コア ネットワークに対するセキュリティで保護された TCP/IP 接続がないからです。サイト B では MAK ライセンス認証を使用します。KMS が、KMS クライアント コンピューターが 25 台未満のサイトをサポートせず、サイトがセキュリティで保護されたリンクによってコア ネットワークに接続されていないからです。サイト C では KMS を使用します。プライベート ワイド エリア ネットワーク (WAN) 経由でセキュリティで保護された接続によりコア ネットワークに接続されており、コア ネットワークの KMS クライアントによってライセンス認証のしきい値に達しているからです。



図 4   支社シナリオ

## 切断された個々のコンピューター

組織内のユーザーが、遠隔地に勤務している場合や、さまざまな場所に出張する場合があります。このシナリオは、支社以外のオフサイトにいる営業担当者などのユーザーのコンピューターなど、移動するクライアントに該当します。このシナリオは、コア ネットワークに接続できないか、または接続が一時的に切断されているリモートの支店にも適用できます。

切断されたコンピューターは、コンピューターがコア ネットワークに接続する頻度に応じて KMS または MAK を使用できます。コア ネットワークに直接または VPN を通じて 180 日ごとに 1 回以上接続するコンピューターには、コア ネットワークが KMS ライセンス認証を使用している場合、KMS ライセンス認証を使用します。コア ネットワークにほとんどまたはまったく接続しないコンピューターには、電話またはインターネットによる MAK 非依存ライセンス認証を使用します。図 5 に、インターネットおよび電話を通じて MAK 非依存ライセンス認証を使用している切断されたクライアントを示します。



図 5   切断されたコンピューター シナリオ

## テストおよび開発ラボ

ラボ環境には通常、多数の仮想マシンが存在し、ラボのコンピューターは頻繁に再構成されます。テストおよび開発ラボ内のコンピューターにライセンス認証が必要かどうかを判断します。Windows 7 または Windows Server 2008 R2 を実行しているコンピューターの初期の 30 日間の猶予期間は、ライセンス認証を行うことなく 3 回リセットできます。したがって、120 日以内にラボ コンピューターを再ビルドしている場合、これらのコンピューターのライセンス認証は不要です。

ラボ コンピューターがライセンス認証を要求する場合は、KMS または MAK ライセンス認証を使用します。コンピューターが KMS を使用しているコア ネットワークに接続できる場合は、KMS ライセンス認証を使用します。ラボ内のコンピューター数が KMS ライセンス認証のしきい値に達する場合は、ローカル KMS ホストを展開します。

コンピューターの回転率が高く、KMS クライアントの数が少ないラボでは、KMS ホスト上で十分な数のキャッシュ済み CMID が保持されるように KMS ライセンス認証カウントを監視することが重要です。KMS ホストは、コンピューターからのライセンス認証要求を 30 日間キャッシュします (CMID がライセンス認証にどのように影響するかの詳細については、前の「[最小コンピューター要件](#_Minimum_Computer_Requirements)」を参照してください)。ラボ環境でライセンス認証が必要であっても、KMS ライセンス認証の条件を満たしていない場合は、MAK ライセンス認証を使用します。MAK クライアントは、電話またはインターネット (どちらかラボで利用可能なもの) を使ってライセンス認証されます。

このシナリオでは VAMT を使った MAK プロキシ ライセンス認証も使用できます。VAMT を、隔離されたラボ ネットワークおよびインターネットに接続できるネットワークにインストールします。隔離されたラボでは、VAMT が、検出の実行、状態の取得、MAK プロダクト キーのインストール、ラボ内の各コンピューターの IID の取得を行います。この情報を VAMT からエクスポートし、リムーバブル メディアに保存できます。次にそのファイルを、VAMT を実行しており、インターネットに接続できるコンピューターにインポートできます。VAMT は、IID をマイクロソフトに送信し、ライセンス認証を完了するために必要な、対応する CID を取得します。このデータをリムーバブル メディアにエクスポート後、隔離されたラボに運んで CID をインポートすれば、VAMT がライセンス認証を完了できます。

**注**高セキュリティ モードでは、VAMT はエクスポートするファイルから個人の身元を特定する情報 (PII) をすべて削除します。このファイルは、XML またはテキスト エディタで確認できる、読み取り可能な拡張マークアップ言語 (XML) ファイルです。

# コンピューターのライセンス認証方法へのマップ

推奨されるライセンス認証シナリオを評価したら、次のステップではボリューム アクティベーションを使用してコンピューターをライセンス認証方法にマップします。目標は、すべてのコンピューターが 1 つのライセンス認証オプションに関連付けられるようにすることです。表 2 に、すべてのコンピューターが 1 つのライセンス認証方法にマップされていることを確認する単純な演習用参考資料を提供します。この演習用参考資料を完了すると、KMS を使用するすべてのコンピューターが、KMS ライセンス認証のしきい値に達したネットワーク上に存在することを確認できます。

表 2. ライセンス認証方法ワークシート

|  |  |  |
| --- | --- | --- |
| 基準 | ライセンス認証方法 | コンピューター数 |
| ライセンス認証が必要なコンピューターの総数 |  |
| 180 日ごとに 1 回以上、KMS ライセンス認証のしきい値に達しているネットワークに (直接または VPN を使って) 接続するコンピューターの数 | KMS |  |
| ネットワークに 180 日間 1 回も接続しないコンピューターの数 | MAK |  |
| KMS ライセンス認証のしきい値に達している隔離されたネットワーク内のコンピューターの数 | KMS |  |
| KMS ライセンス認証のしきい値に達していない隔離されたネットワーク内のコンピューターの数 | MAK |  |
| ライセンス認証されないテストまたは開発ラボ内のコンピューターの数 | なし |  |
| 残りのコンピューターの数はゼロとなるはずです |  |

# 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および組織が必要なプロダクト キーの数を単純化するため、マイクロソフトはプロダクト キー グループを作成しました。KMS と MAK のプロダクト キーは、個々のエディションではなく製品グループに適用されますが、KMS と MAK では、プロダクト キー グループの使用方法が異なります。

* MAK ライセンス認証は、プロダクト キー グループを個々のグループとして使用します。MAK ライセンス認証のプロダクト キーは、1 つの製品グループに直接関連付けられており、その特定製品グループ内の Windows エディションだけをライセンス認証できます。
* KMS では、プロダクト キーは、製品グループに階層的に機能します。KMS ライセンス認証のプロダクト 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エディションのほか、その製品階層の下位にある他のエディションもライセンス認証できます。

表 3 に、Windows 7 および Windows Server 2008 R2 の製品グループを示します。

表 3. 製品グループ

| ボリューム ライセンス プロダクト キー グループ | Windows オペレーティング システム エディション |
| --- | --- |
| クライアント VL | * Windows 7 Professional
* Windows 7 Enterprise
 |
| サーバー グループ A | * Windows Server 2008 R2 HPC Edition
* Windows Web Server 2008 R2
 |
| サーバー グループ B | * Windows Server 2008 R2 Standard
* Windows Server 2008 R2 Enterprise
 |
| サーバー グループ C | * Windows Server 2008 R2 Datacenter
* Windows Server 2008 R2 for Itanium-Based Systems
 |

## MAK プロダクト キー グループの選択

MAK プロダクト キーは 1 つのグループと関連付けられ、そのグループに対応する OS エディションだけをライセンス認証できるため、インストールする Windows エディションに適合するグループから MAK を選択します。たとえば、Windows 7 Enterprise をインストールしている場合は、クライアント VL MAK キーをそのイメージ内、または直接ターゲット システム上にインストールします。

## 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 4 に、製品グループ間の相関関係を示します。

表 4. 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 5 を参照してください。

表 5   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 v1.2 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 v1.2 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
 |

# 監視およびレポートのニーズの判断

ボリューム アクティベーションを使用する組織では、ライセンス認証されたコンピューターのプロダクト キー使用率とライセンス状態をトラックする必要があります。ボリューム ライセンスを購入した場合、KMS キー情報と MAK キーに残っているライセンス認証の数をボリューム ライセンス サービス センター <http://go.microsoft.com/fwlink/?LinkId=107544> で確認できます。

他にも、ボリューム ライセンスを購入されたお客様がライセンス認証とプロダクト キーの使用率を管理する際に役立つツールが、複数あります。ここでは、利用可能なツールと、各ツールがボリューム ライセンスの使用時にどのように役立つかについて説明します。

## Windows Management Instrumentation

ライセンス認証中に収集されたデータに、WMI を使ってアクセスできます。実際、利用可能な複数のツールが、WMI を使用してボリューム アクティベーションのデータにアクセスします。ボリューム アクティベーションのすべての WMI 方法、プロパティ、レジストリ キー、およびイベント ID のリストについては、『[ボリューム アクティベーション テクニカル リファレンス ガイド](http://go.microsoft.com/fwlink/?LinkId=152550)』(英語) を参照してください。

## System Center Configuration Manager

Microsoft Systems Management Server (SMS) 2003 with SP3 または Microsoft System Center Configuration Manager 2007 を使用して、組織のコンピューターのライセンス状態を監視できます。利用可能なライセンス状態の詳細については、後の「付録 B: [ライセンス状態](#_Appendix_B:_Licensing)」を参照してください。

Systems Management Server with SP3 および System Center Configuration Manager は、ビルトイン資産インテリジェンス レポートと WMI を使用して、Windows 7 または Windows Server 2008 R2 を実行しているコンピューターの詳細なライセンス認証レポートを生成します。この情報は、組織がライセンスの視点からソフトウェア資産管理をトラックおよびレポートする開始点としても利用できます。また、System Center Operations Manager 2007 を使用して、キー管理サービスの健康とハートビートを監視できます。

## イベント ログ

KMS サービスは、すべてのアクションを KMS クライアントおよびホストのライセンス認証ログに記録します。KMS クライアントは、Windows Security Licensing (SLC) イベント ID 12288 および 12289 を使用して、ライセンス認証の要求、更新、および応答を KMS クライアントのローカル アプリケーション ログに記録します。KMS ホストは、KMS クライアントから受け取る各要求に対して別個のエントリを、SLC イベント ID 12290 として記録します。これらのエントリは、[アプリケーションとサービス ログ] フォルダの "Key Management Service" ログに保存されます。各 KMS ホストは、ライセンス認証の個々のログを保持します。KMS ホスト間でのログのレプリケーションはありません。ただし、ログの転送を使用して、監視のため複数の KMS ホストからログを中央の場所にレプリケートできます。KMS イベントの詳細については、『[ボリューム アクティベーション テクニカル リファレンス ガイド](http://go.microsoft.com/fwlink/?LinkId=152550)』(英語) を参照してください。

## KMS Management Pack

KMS イベント ログは、手動でアーカイブおよび確認できます。または Microsoft System Center Operations Manager 2007 により、IT プロフェッショナルが、Windows Key Management Service Management Pack for System Center Operations Manager を使用できます。KMS Management Pack は、KMS サービスの健康とハートビートを監視できます。この Management Pack およびガイドをダウンロードするには、『**System Center Pack カタログ**』(<http://go.microsoft.com/fwlink/?LinkID=110332>) (英語) を参照してください。

## ボリューム ライセンス認証管理ツール

組織は、VAMT を使用してネットワーク上で KMS および MAK ライセンス認証を管理できます。MAK ライセンス認証の残りの数を監視するために使用することもできます。ボリューム アクティベーションを使用しているすべてのコンピューターのライセンス状態をレポートし、MAK ライセンス認証カウントをトラックします。

# 付録 A: マイクロソフトに送信される情報

マイクロソフトは、ライセンス認証中に収集された情報を使用して、ソフトウェアのコピーがライセンスされていることを確認します。その後、情報は、ひとまとめにされて統計解析に使用されます。マイクロソフトがこの情報を組織の特定や、組織への連絡に使用することはありません。ライセンス認証中に取得された情報、およびマイクロソフトによるそのデータの使用の詳細については、<http://go.microsoft.com/fwlink/?LinkID=52526>http://go.microsoft.com/fwlink/?LinkId=52526を参照してください。

MAK ライセンス認証および KMS ホスト ライセンス認証中、次の情報がマイクロソフトに送信されます。

* プロダクト キー
* オペレーティング システム エディションおよびエディションが取得されたチャネル
* 現在の日付
* ライセンスおよびライセンス認証の条件
* ハードウェア ID ハッシュ。これは、リバース エンジニアリングできない一意でない数字です。
* 言語設定
* IP アドレス。要求の場所を確認するためにだけ使用されます。

# 付録 B: ライセンス状態

ソフトウェア ライセンス アーキテクチャは、Windows 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のライセンス状態を管理します。このアーキテクチャには、多数のコア Windows セキュリティ技術からビルドされたポリシー エンジンがあります。これは、コードおよびそれに関連するライセンス状態を改ざんなどの悪意のある行為から保護するために設計されています。

ポリシー エンジンは、一連の暗号署名付きの eXtensible rights Markup Language (XrML) ライセンス ファイルからデータを取得します。XrML は、多数の Windows コンポーネントが使用する業界標準権利記述言語です。ライセンス ファイルは、インストールされているエディションの Windows の権利と状態を定義します。すべてのライセンス ファイルおよびポリシー エンジンが使用する他のデータは、マイクロソフトとの信頼関係を強固なものとするためのキーを使ってデジタル署名または暗号化されます。

Windows 7 および Windows Server 2008 R2 は、4 つのソフトウェア ライセンス状態のいずれかである可能性があります。ライセンス認証されています、猶予期間、正規、または通知です。ここでは、これらの状態について説明します。状態は、コンピューターのライセンス認証の状態と正規状態を反映しており、これによってユーザー エクスペリエンスが決まります。図 6 に、これらの状態を示します。



図 6   ライセンス状態

## ライセンス認証されています

コンピューターがライセンス認証されると、オペレーティング システムのすべての機能にアクセスできます。ライセンス ファイルとライセンス認証プロセスの結果として許可された一連のポリシー (権利) の組み合わせにより、Windows エディションの機能が定義されます。個々の Windows コンポーネントがソフトウェア ライセンス アプリケーション プログラミング インターフェイス (API) を呼び出して、どの権利が許可されているかを判断し、その応答に応じて機能を調整します。

## 猶予期間

Windows 7 または Windows Server 2008 R2 オペレーティング システムをインストール後、オペレーティング システムをライセンス認証するまでのあいだ、オペレーティング システムのすべての機能に期間限定 (猶予期間) でアクセスできます。猶予期間の長さは、クライアント オペレーティング システムもサーバー オペレーティング システムも 30 日です。この猶予期間中、オペレーティング システムは、コンピューターにライセンス認証が必要であることを定期的にユーザーに通知します。また、Windows は、ハードウェアが大幅に変更されたときには、猶予期間の許容範囲外になる場合があります。通知の割り込みは最小限に抑えられており、猶予期間の始めには表示されない場合がありますが、猶予期間が終わりに近づくにつれて通知の回数が増加します。

## 正規

正規状態は、ライセンス認証プロセスに関連付けられていません。これは、オンライン正規検証サービスによって判断される状態です。正規品にしかない機能をダウンロードまたは使用しようとすると、オンライン検証サービスが、要求しているコンピューターのオペレーティング システムを確認します。

オペレーティング システムは、次の 3 つの正規状態のいずれかになります。

* **非正規**。コンピューターは、オンライン検証サービスから正規でないことを示すチケットを取得しています。
* **ローカル正規**。コンピューターは、検証チケットを取得していません。
* **正規**。コンピューターは、正規であることを示す、マイクロソフトによって署名されたチケットをオンライン検証サービスから取得しています。

正規ライセンス状態は、Windows オペレーティング システムのクライアント バージョンにのみ適用されます。最初、猶予期間中、これらの Windows バージョンを実行しているコンピューターは、常にローカル正規状態にあります。コンピューターは、オンライン検証サービスで検証に失敗し、非正規チケットを受け取るまで、非正規とマークされません。同様に、コンピューターが非正規状態になったら、オンライン検証サービスで検証に成功し、正規チケットを受け取る必要があります。

コンピューターが正規であると認められるにはライセンス認証されている必要がありますが、ライセンス認証のプロセスは、前の非正規状態をリセットまたはクリアしません。結果として、コンピューターをすべての機能がライセンス認証された状態に戻すには、オンライン検証サービスに対してライセンス認証および検証される必要があります。詳細については、マイクロソフト Web サイトで「**正規のマイクロソフト® ソフトウェア**」 ([http://www.microsoft.com/genuine/default.aspx?displaylang=ja](http://go.microsoft.com/fwlink/?LinkId=151993)) を参照してください。

## 通知

通知ベースのエクスペリエンスの目的は、ログオン、使い慣れたデスクトップへのアクセスなど、コンピューター機能を維持しながら、ライセンス認証された正規の Windows オペレーティング システムのコピーと、正規でないか、またはライセンス認証されていないコピーを区別することです。Windows 7 と Windows Server 2008 R2 には機能制限モード (RFM) がありません。どちらのオペレーティング システムも通知ベースのエクスペリエンスに代わっています。この新しい通知ユーザー エクスペリエンスでは、猶予期間中にライセンス認証 (初期のライセンス認証およびハードウェア変更により必要となったライセンス認証) が行われなかったコンピューターまたは検証に失敗したコンピューターが、次のユーザー エクスペリエンスを提供する場合があります。

* コンピューターにログオンすると、Windows をライセンス認証する必要があることを通知するダイアログ ボックスが表示されます。今すぐ実行するか、後から実行するかを選択できます。このダイアログ ボックスに 2 分以内に応答しないと、ログオン プロセスが通常どおりに続行されます。
* 通知状態では、デスクトップの壁紙が黒の背景に変わり、ライセンス認証状態を示す通知が通知領域に表示され、ユーザーが実行する必要があるアクションを示したダイアログ ボックスが表示されます。
* 通知状態では、インストール バージョンの Windows のすべての機能にアクセスできますが、次の機能が無効になります。
* KMS ホストとして構成されているコンピューターが、KMS クライアントの要求に対して、KMS がライセンス認証されていないことを知らせるエラー メッセージで応答する。
* Windows Update で、セキュリティ更新プログラムと重要な更新プログラムをダウンロードする (オプションの更新プログラムを除外する)。
* オンライン検証サービスを必要とするオプション ダウンロード (正規ゲート ダウンロードともいいます) を利用不可にする。

コンピューターが通知状態から復帰するには、コンピューターをライセンス認証する必要があります。