White Paper



CodeMeter® in Virtual Environments

Rüdiger Kügler
Professional Services | Security Expert
WIBU-SYSTEMS AG
www.wibu.com

WIBU SYSTEMS

目次

はじめに 3
仮想マシンの脅威と課題 4
ターミナルサーバーの脅威と課題 5
過去のソリューション 6
最新のソリューション：CodeMeter 6
ライセンス数のカウント 7
ネットワークライセンスサーバー上のライセンス 8
CmDongle：1つのドングル、1人のユーザー 8
ホストシステム上のCmDongle 10
USB-over-Ethernet のCmDongle 10
ホストシステム上のCmActLicense 11
ゲストシステム上のCmActLicense 12
ユーザーのライセンス管理 13
ターミナルサーバークライアント 14
高可用性とセキュリティ 14
結論 15

著者



リュディガー・キューゲラー（Rüdiger Kügler）は、1988年にソフトウェア開発に初めて携わり、物理学の学位コースの一部としてFORTRAN、C、およびAssemblerを学びました。 1995年に研究を終えた後、ソフトウェア保護、ソフトウェア配布、インターネットバンキング、およびマルチメディアプロジェクトのプロジェクトマネージャーおよびプロジェクト管理責任者を務めました。

2003年以来、ウイブシステムズにてセキュリティ専門家およびプロフェッショナルサービスチームのリーダーとして取り組んできました。 彼のコアコンピタンスには、リバースエンジニアリングに対するソフトウェアの保護、ソフトウェアベンダーの内部プロセスにおけるライセンスの統合、およびソフトウェアとライセンスの配布と管理プロセスの最適化が含まれます。 彼の役割の一部には、ホルストゲルツ財団から授与された第5回ドイツITセキュリティ賞で第1位を獲得したBlurryBox®テクノロジーの開発への多大な貢献があります。

はじめに

世界中のITプロフェッショナルは、仮想マシンとターミナルサーバーによって少ないハードウェアリソースで多くの利点を享受し、問題が発生した場合でも簡単に回復できるようにしています。ソフトウェアの発行元や開発会社としては、仮想マシンについて少し複雑な感情を抱くかもしれません。仮想マシンは、自由に定義可能な環境でソフトウェアをテストする簡単な手段を提供します。一方、仮想マシンとターミナルサーバーは、ソフトウェアの収益化、ライセンスと著作権侵害に対する不可欠になったときに、製品のライセンス形態に大きく新たな課題をもたらします。

CodeMeterは、仮想マシンとターミナルサーバーの両方で安全で信頼性の高いライセンスを発行するための強力なツールを提供します。このホワイトペーパーでは、CodeMeterの機能における様々な使用例を紹介します。

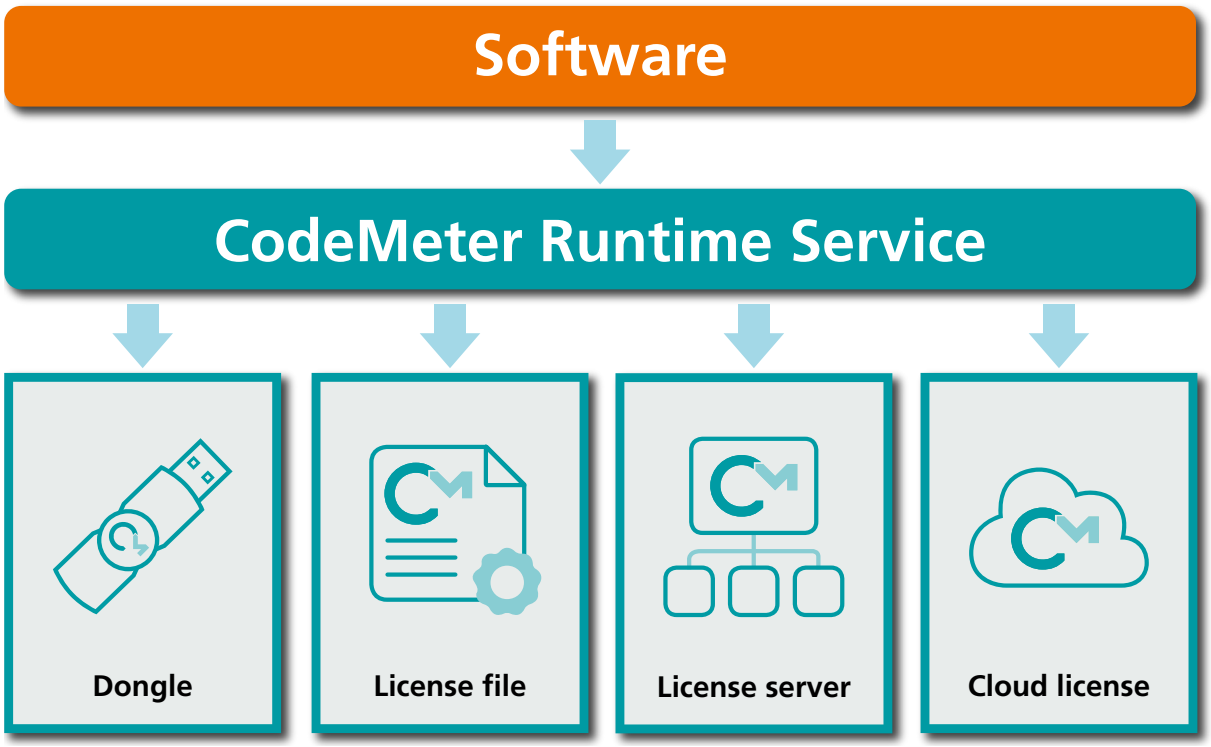


図1:
CodeMeterの概要

CodeMeterでは、個々のクライアントごとに次のライセンスコンテナを選択できます。

- ドングル（CmDongle：すべてのライセンスを安全な外部ハードウェアに保存）
- ソフトライセンス（CmActLicense：ハードウエアにバインドした暗号化されたライセンスファイル）
- ライセンスサーバー（LANまたはWAN）
- クラウドライセンス（CmCloud：すべてのライセンスをクラウド内のサーバーに保存）

仮想マシンの脅威と課題

仮想マシンは、コンピューター上（ホストまたはマスター）でシミュレートされたハードウェアです。この仮想ハードウェアは、完全な（ゲストまたはチャイルド）オペレーティングシステムを実行しますが、周囲の実際の環境と対話する機能を大幅に制限します。すべてのゲストシステムとホストは同じ実際のハードウェアを共有しますが、ゲストシステムへの即時アクセスは与えられません。シミュレートされた仮想マシンが表示されます。

図2：
仮想マシンの
アーキテクチャ



仮想マシンは、簡単に保存および復元（以前の状態に戻す）できます。

ライセンスの観点から、仮想マシンはいくつかの新しい脅威を生み出します：

ドングルユーザーの場合：
- 複数のゲストシステムに1つのドングルを使用することにより、不正に1つのライセンスを複数使用 する可能性。

純粋なソフトライセンスの場合：
- コピーまたはスナップショットを使用して、期間限定または従量制のライセンスをリセット。
- 割り当てられたマシン全体を複製して、マシンにバインドされたライセンスを複製。

ソフトウェアの正当なユーザーには、次のような固有の課題もあります。
- ドングルと仮想マシンを接続する機能。
- 仮想マシンで実行されている高可用性ライセンスサーバー。

ターミナルサーバーの脅威と課題

ターミナルサーバーは、インストールされているソフトウェアをホストします。アプリケーションはサーバーで実行され、ユーザーはサーバーのディスプレイ出力をユーザーのハードウェアに反映するクライアントシステムにのみアクセスできます。多くのユーザーは同じターミナルサーバーを同時に使用でき、それぞれに他のユーザーのセッションとは独立して動作する個別のセッションが与えられます。クライアントは、マウス、キーボード、またはその他の周辺機器のみを提供します。

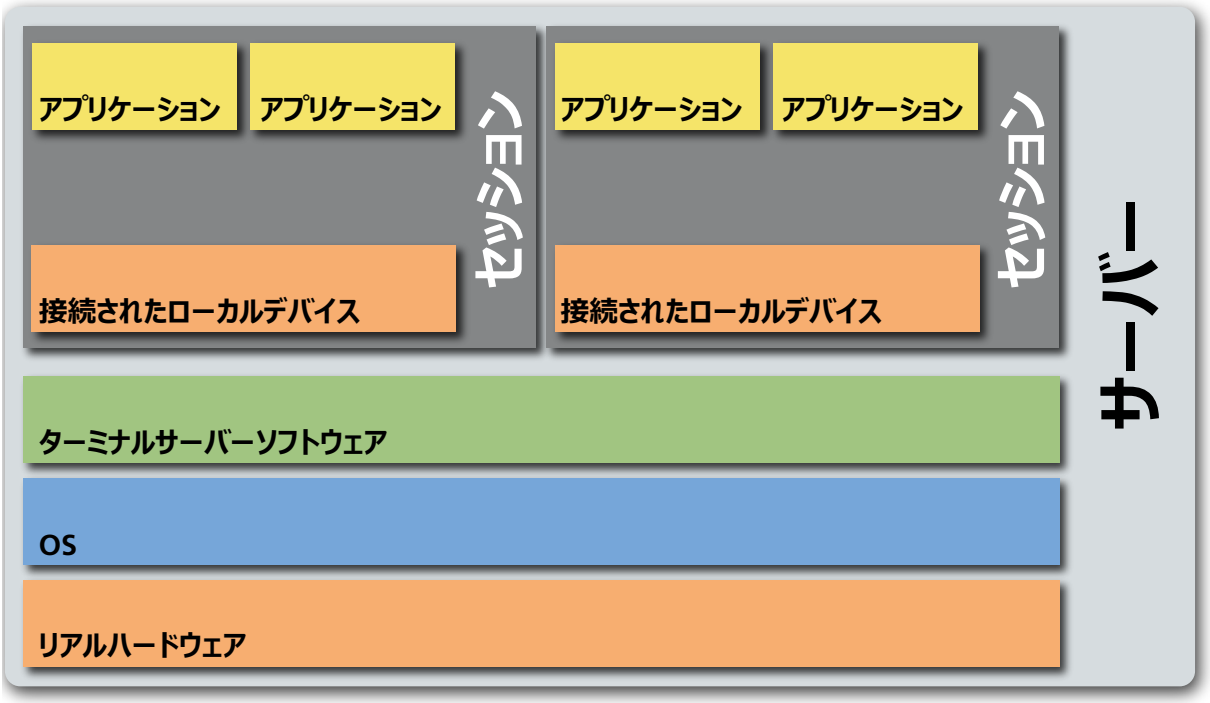


図3：
ターミナルサーバーの
アーキテクチャ

次の脅威を考慮する必要があります。

- ターミナルサーバー上の複数の同時セッションでの単一ライセンスの不正使用。
- フローティングネットワークライセンスとしてのシングルユーザーライセンスの使用。

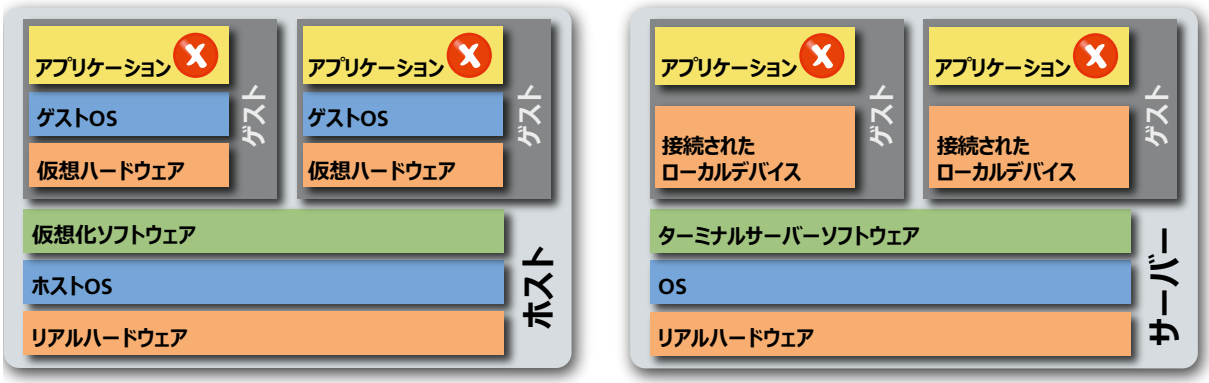
次のシナリオは、ターミナルサーバーの特定の課題を表しています。

- ターミナルサーバーで定義されたユーザーがライセンスを利用できるようにするにはどうすればよいか？
- クライアントシステムに保持されているライセンスをターミナルサーバーでどのように使用するか？

過去のソリューション

これらの課題に対する1つの対応策は、仮想マシンとターミナルサーバーを識別する手段をソフトウェアに装備することでした。そのような望ましくない環境が特定された場合、ソフトウェアはエラーメッセージを表示し動作を止めます。

図4：
時代遅れのアプローチ



このソリューションは、今日には適していないと見なすことができます。仮想世界全体からビジネスを切り離してしまうため、重要な収益源が枯渇してしまいます。リモートデスクトップアクセスを持つすべてのコンピューターは、その性質上ターミナルサーバーであるため、ソフトウェアを操作できません。これは、識別機能を統合および維持するために必要な労力によってさらに悪化します。

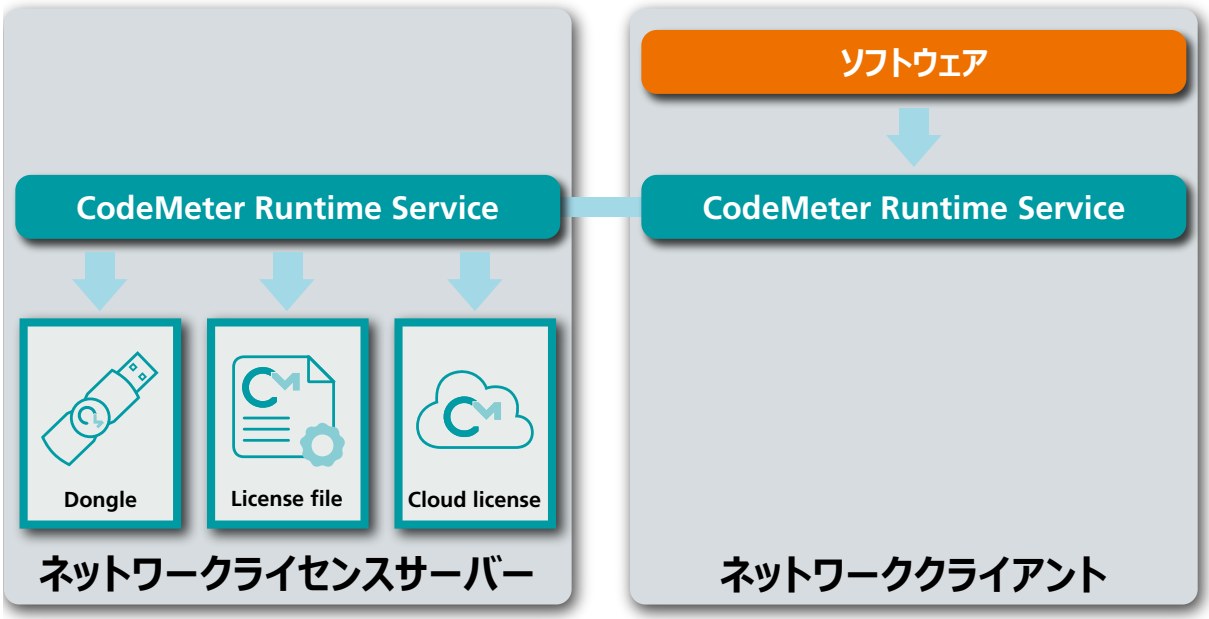
ソリューションは、「ソフトウェアはどこで実行されているのか」という問題を中心に展開されました。しかし問題は、「ライセンスはどこにあるのか」です。これは、汎用的で用途が広く、自動的に使用できるソリューションを提供するCodeMeterの原則です。

最新のソリューション：CodeMeter

CodeMeterアーキテクチャのコア要素は、CodeMeter Runtime Service（CodeMeter.exe）です。CodeMeter Runtime Serviceは、ソフトウェアとともにユーザーのマシンにインストールするサービス（Windows）またはデーモン（LinuxおよびOS X）です。CodeMeter Runtime Serviceのインストールは、エンドユーザーにはソフトウェアインストールプロセスを目に見えない形で行われる可能性があります。CodeMeter Runtime Service は、Windows、Linux、OS Xで利用できます。

CodeMeter Runtime Serviceは、接続されているすべてのCmDongleと利用可能なすべてのCmActLicenseを整理し、ソフトウェアのライセンスを提供します。

図5：
ネットワーク環境での
CodeMeter



CodeMeter Runtime Serviceは、ネットワーク内のライセンスサーバーとしても機能します。ユーザーは、ネットワークのライセンスサーバーとして構成されたネットワーク内のサーバーにCodeMeter Runtime Serviceのみをインストールします。次に、ソフトウェアは、CodeMeter Runtime Serviceのローカルインストールと通信し、次に、使用可能なライセンスを管理および割り当てるネットワークサーバーのCodeMeter Runtime Serviceと通信します。

ライセンス数のカウント

CodeMeterのすべてのライセンスには、ライセンスが作成されたときにソフトウェアベンダーによって定義された規定のライセンス数量があります。標準数量は1個です。

CodeMeterを統合すると、ソフトウェアでのカウント方法が決まります。「アクセスごと」、「マシンごと」、「カウントなし」から選択できます。すべてのライセンスは、CmDongle、ローカルのCmActLicense、またはライセンスサーバーのいずれであっても、まったく同じように扱われます。

アクセスごと ーユーザー制限

「アクセスごと」のカウントを使用すると、アクセスの始まり（APIコマンドCmAccess2）から解放（APIコマンドCmRelease）を 1アクセスとし、1つのライセンスフラグが付けられます。 各ライセンスは、ライセンス数の値で許可されている回数だけ使用できます。

マシンごとーステーションシェア

「マシンごと」のカウントを使用して、CodeMeterはソフトウェア環境に関する特定の詳細（セッション、IPアドレス、プロセスIDなど）を自動的に記録し、CodeMeter Runtime Serviceに送信します。この情報は、各マシン、ターミナルサーバー上の各セッション、または各仮想マシンを個別のエンティティとして自動的に識別するために使用されます。たとえば、ライセンス数が『 3 』のライセンスは、2つのターミナルサーバーと1つの仮想マシンで同時に使用できますが、これらの各セッションまたは仮想マシンで必要な分だけ使用できます。

自動解放

CodeMeter Runtime Serviceは、プロセスIDを使用して、ソフトウェアがまだアクティブかどうかを検出します。ソフトウェアで使用した後にライセンスを解放する機能を含めるのを忘れた場合や、ソフトウェアがクラッシュするという稀な場合でも、CodeMeter Runtime Serviceはこれを検出して自動的にライセンスを解放します。

ローカルライセンス

ライセンス数がゼロの場合、特別な意味があり、ローカルのシングルユーザーライセンスを表します。これは、ライセンス数『1』としてカウントされますが、ライセンス（例：CmDongleまたはCmActLicense）は、同じ実マシンまたは仮想マシンで使用する必要があります。CodeMeterは、実際のターミナルサーバーとリモートデスクトップを自動的に区別できます。ライセンス数がゼロのライセンスを実際のターミナルサーバーのセッションで使用することはできませんが、リモートデスクトップを備えたローカルマシンでは可能です。

ネットワークライセンスサーバー上のライセンス

CodeMeter Runtime Serviceはネットワーク内のサーバーにインストールされ、ネットワークライセンスサーバーとして機能するように構成されます。CmDongleがこのマシンに接続されているか、CmActLicenseがアクティブ化され、サーバーの特定の特性によってサーバーにリンクされています。

ライセンスサーバーで使用可能なすべてのライセンスは、仮想マシンまたはターミナルサーバーですぐに使用できます。ライセンス数により、ネットワークライセンスサーバーは、ターミナルサーバー上の物理または仮想マシンまたはセッションの許容数をカウントできます。

ソフトウェア発行元は、ユーザーに適切なライセンス数のライセンスを提供するだけで済みます。

CmDongle：1つのドングル、1人のユーザー

CmDongleは、大容量記憶装置（MSD）またはヒューマンインターフェイスデバイス（HID）として構成できます。 このプロセスは標準ドライバーに依存しているため、ユニットは現在のすべてのオペレーティングシステムの仮想マシンに接続できます。暗号化された通信により、HIDまたはMSDのいずれかの標準ドライバーを使用するときに完全なセキュリティが確保されます。

CmDongleは排他モードに制限

ユーザーが複数のゲストシステムを持つホストでUSBデバイス（CmDongleなど）を使用する場合、通常の仮想化ソフトウェアでは、排他モードまたは共有モードのいずれかを使用できます。 排他モードでは、USBデバイスは単一のゲストまたはホストシステム自体でのみ使用できますが、共有モードでは、複数のシステムが同じUSBデバイスにアクセスできます。

ゲストシステムのCodeMeter Runtime Serviceは、そのゲストシステムに排他的に接続されているCmDongleのみを検出して使用します。共有されているCmDongleは自動的にロックアウトされます。これにより、複数のゲストシステムでCmDongleを同時に使用できなくなります。

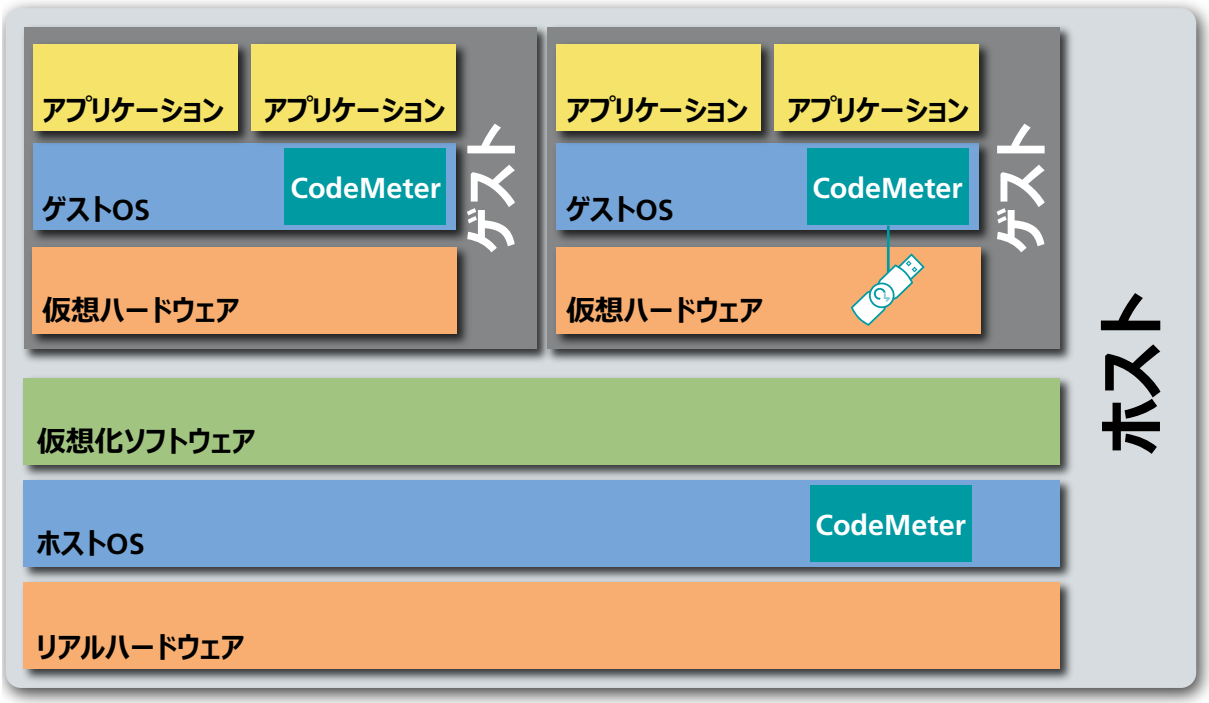


図6：
CmDongleは単一のゲストでのみ実行–ライセンスの使用が許可

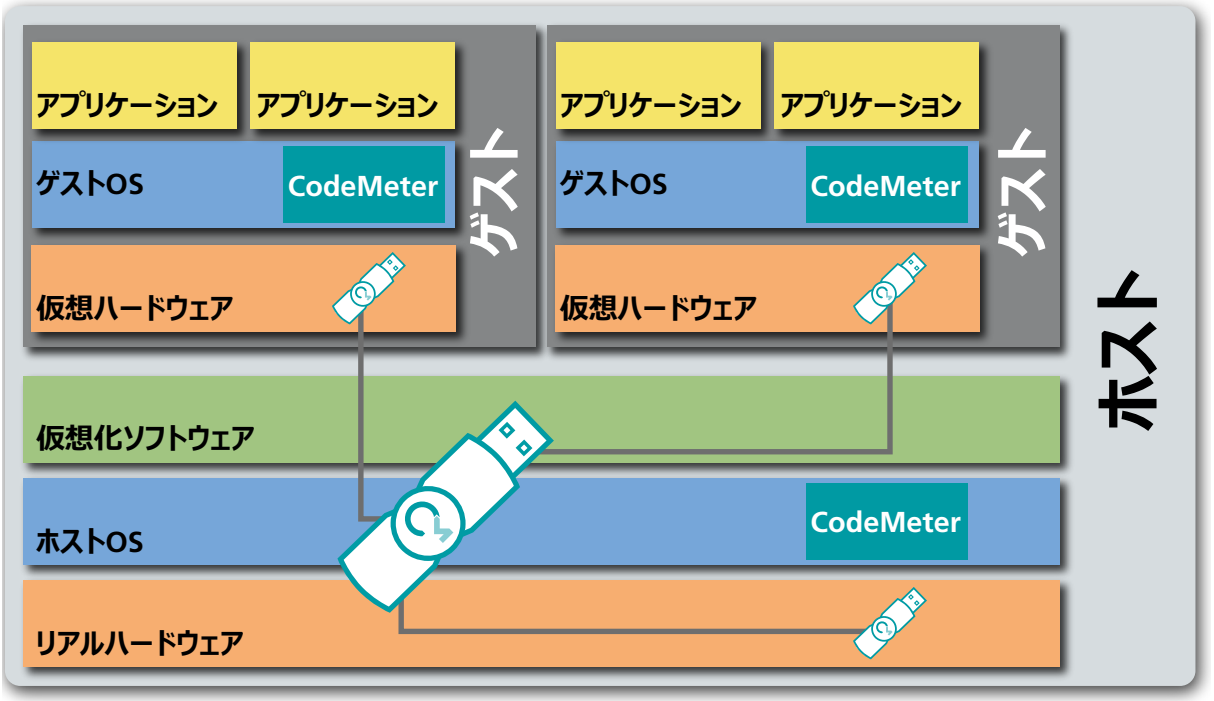


図7：
共有環境での
CmDongle
–ライセンスの使用は
許可されていない

CmDongleの重複使用の禁止

CmDongleがゲストシステムからゲストシステムに渡されるとどうなるか？繰り返しになりますが、CodeMeter Runtime Serviceとすべてのに、それに対する自動防御機能が備わっています。CodeMeter Runtime Serviceは複数のCmDongleとCmActLicenseを処理できますが、すべてのCmDongleは単一のCodeMeter Runtime Serviceによって排他的に使用されます。 これは、CodeMeter Runtime ServiceとCmDongleが暗号化された通信を確立するときに特定のパラメーターを設定することによって実現されます。CmDongleが別のCodeMeter Runtime Serviceに接続されている場合、このパラメーターは機能しません。元のCodeMeter Runtime Serviceによって管理されているライセンスは自動的に解放され、ソフトウェアはそれに応じて応答できます。

別のメカニズムは、CmDongleの高速または自動再接続（仮想マシンの切り替えまたはリバースUSBハブのいずれかによる）を通常の操作と区別し、攻撃として検出できるようにします。そのような場合、CmDongleは5分間自動的にロックアウトされます。

ソフトウェアの発行元として、CodeMeterがすべてを自動的に実行するので安心できます。

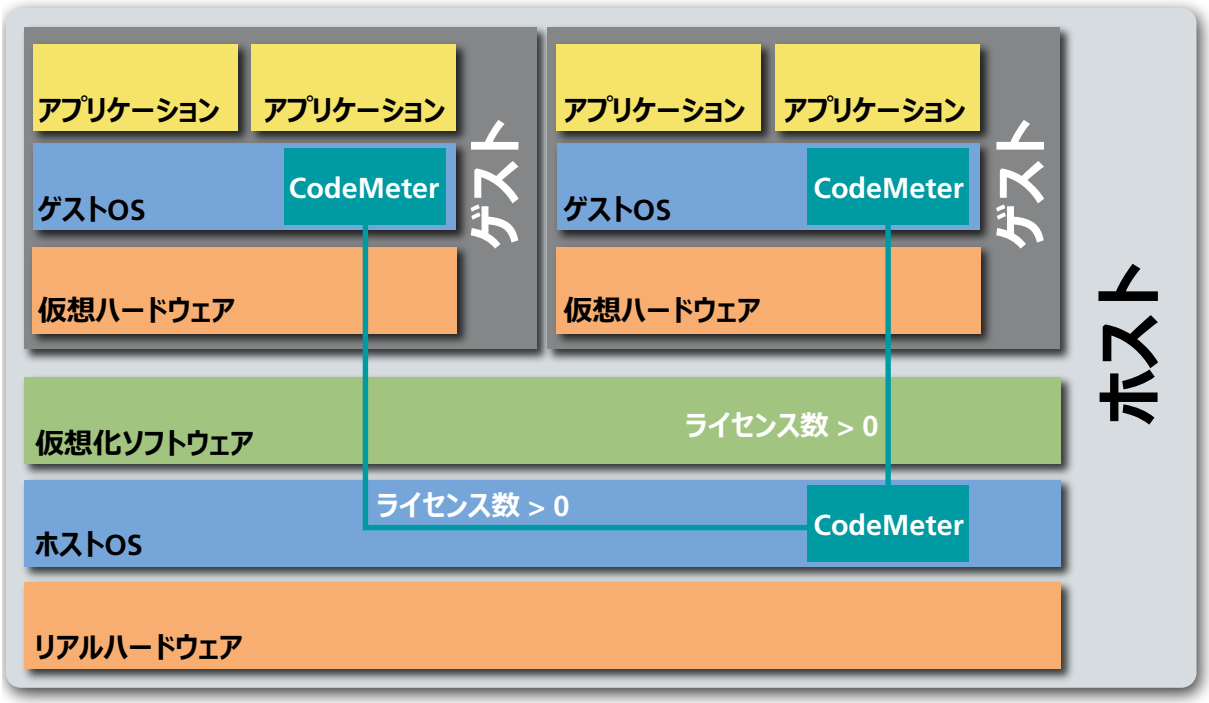
ホストシステム上のCmDongle

Windows、Linux、OS Xなどの標準オペレーティングシステムを使用するホストシステムでは、ネットワークライセンスサーバーとして構成されたホストシステム自体にCodeMeter Runtime Serviceをインストールできます。この目的のために、CmDongleはホストシステムに直接接続されたままです。

ゲストシステムにホストとのTCP/IP接続があり、ライセンスに1つ以上のライセンス数がある場合、ゲストシステムのソフトウェアはネットワーク内のクライアントのソフトウェアのように動作し、ホストのネットワークライセンスサーバーで1つのライセンスを使用できます。そのネットワークライセンスサーバーは、同じライセンスが、定義されたライセンス数で許可されている回数を超えて使用されないことを自動的に確認します。ライセンス数が1の場合、ライセンスは一度に1つのゲストシステムでのみ使用できます。

ソフトウェア発行元は、ユーザーに選択したライセンス数（通常は1つ）のライセンスを提供します。

図8：
ホストシステム上の
ライセンスサーバー



USB-over-Ethernet上のCmDongle

CmDongleは、仮想マシンでUSB接続の直接フィードスルーが許可されていない場合でも、USB-over-Ethernetデバイスを使用して仮想環境で使用できます。

USB接続を介して仮想マシンに直接フィードする場合と同じルールが適用されます。CodeMeter Runtime Serviceを使用すると、CmDongleを一度に1台のマシンでのみ使用できます。CmDongleが切断されたことを検出し、ソフトウェアが応答するためのライセンスを自動的に解放します。多くのデバイスに連続して接続されたCmDongleは攻撃と見なされ、ユニットの5分間のロックアウトにつながります。

繰り返しになりますが、CodeMeterがすべてを自動的に処理するという知識があれば、ソフトウェア発行元は安全です。



ホストシステム上のCmActLicense

ホストシステム上のCmActLicenseは、CmDongleと同様に動作します。ユーザーは、CodeMeter Runtime Serviceをインストールし、それをホストシステム上のネットワークライセンスサーバーとして構成します。

この場合、CmActLicenseのそのシステムへのバインディングのフィンガープリントは、ホストシステムの実際のハードウェア機能を参照することによって作成されます。CodeMeter SmartBind®は、ハードウェアのさまざまな特性と機能を決定し、それらの有効性によって優先順位を付け、フィンガープリントを作成します。作成したCmActLicenseはホストシステムにバインドされ、そのシステムでのみ使用したり、ホストシステム上のネットワークライセンスサーバーによって他のマシンまたはゲストシステムに提供したりできます。ライセンス数を決定することにより、ライセンスをホストでローカルにのみ使用できるか、ゲストシステムのネットワーククライアントとしても使用できるかを決定します。

ソフトウェアパブリッシャーとして、「loose（ゆるい）」、「Medium（標準）」、「Strict（厳しい）」のいずれかの設定を選択することにより、ホストシステムハードウェアの変更に関して、CmActLicenseの許容度も決定します。

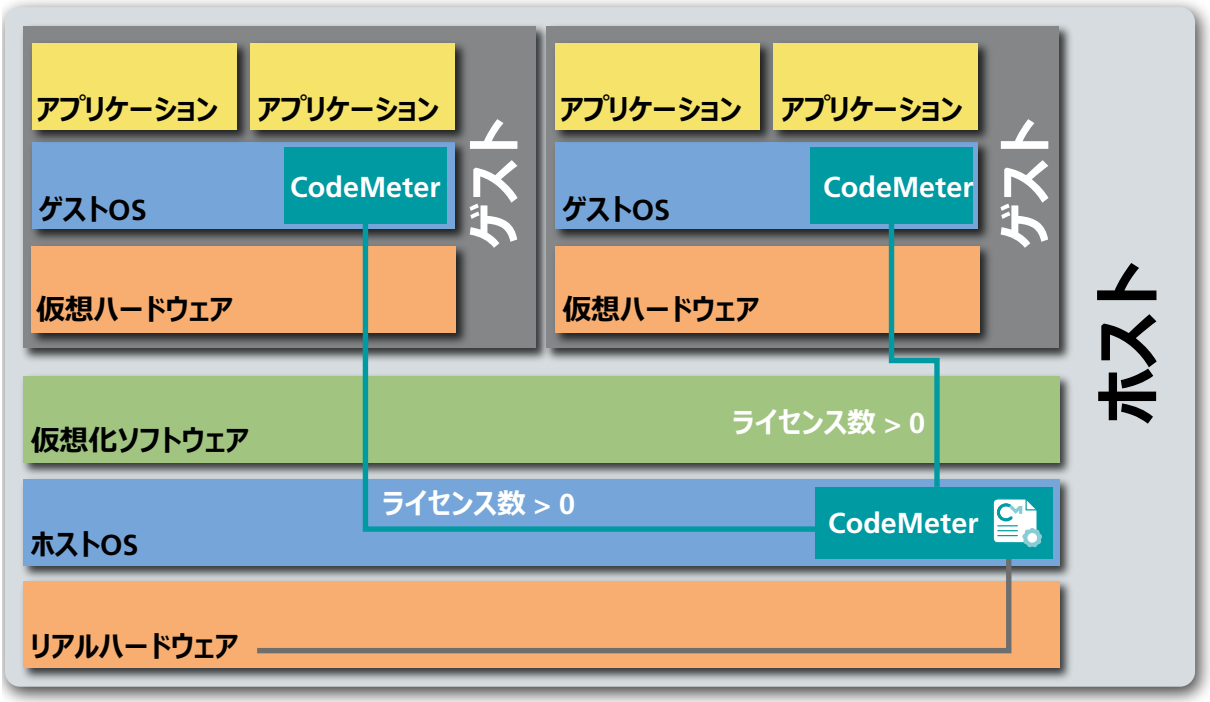


図9：
ホストシステム
にバインドされた
CmActLicense

ユーザーは、同じハードウェアを共有していても、各ゲストシステムで同じCmActLicenseをホストとして使用することはできません。CodeMeterは、同じホスト上のゲストシステムで同じCmActLicenseを使用しようとするユーザーによるライセンスの急増を自動的に防止します。

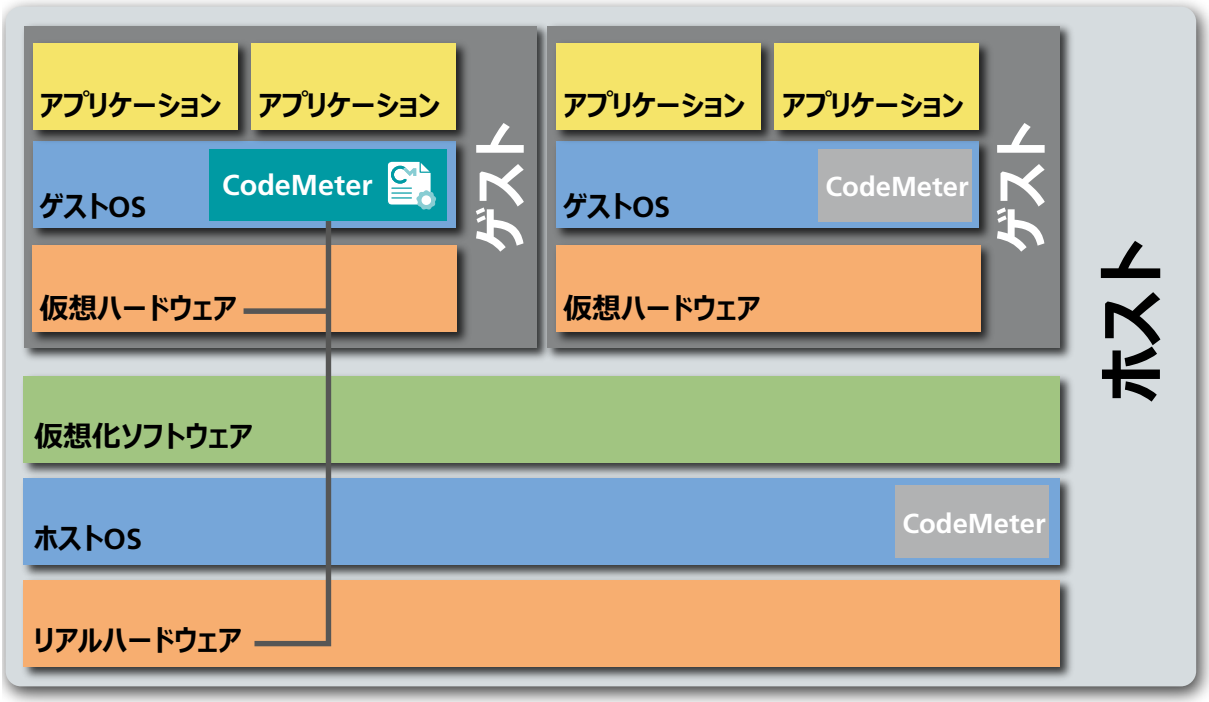
ゲストシステム上のCmActLicense

CmActLicenseは、ゲストシステムでもアクティベーションできます。ソフトウェア発行者は、これを許可するか禁止するかを決定します。

SmartBind –カスタムレシピ

CodeMeter Runtime Serviceは、ゲストシステム上にあるかどうかを自動的に検出します。さまざまなハードウェア機能を識別して優先順位を付ける場合、CodeMeter SmartBindは、仮想環境専用に選択されたカスタム式を使用します。これにより、仮想のみの機能よりも、基盤となる実際のハードウェアに関連する機能の優先度が高くなります。別のマシンに移動したときに変更される機能にも、このような高い重みが与えられます。

図10：
ゲストシステムの
CmActLicense



クローンされたゲストシステムからの保護

CodeMeter SmartBindは、ゲストシステム全体のクローン作成に対するCmActLicenseの最大限の保護を提供します。許容範囲設定「Medium（標準）」または「Strict（厳しい）」を使用する場合、SmartBindはゲストシステムが別のハードウェアにコピーされたことを自動的に検出し、CmActLicenseに破損していて使用不可のフラグを付けます。フィンガープリントはCodeMeter保護の暗号化キーとして含まれているため、CmActLicenseは、適切なハードウェア機能がなければ、クエリにパッチを適用するだけでは「修復」できず CmActLicenseは使用できなくなります。

ゲストシステムの移動

ゲストシステムが同じホストシステム内で移動された場合、CmActLicenseは有効なままです。つまり、ユーザーが導入した構成の変更は、ソフトウェアベンダーとしてのサポートインシデントを自動的に意味するものではありません。移動したゲストシステムは通常、同じホストシステム上で複数回使用できないため、これはビジネスにとって脅威ではありません。

ゲストシステムを別のホストシステムに移動するには、考慮すべき2つの異なる側面があります。同じゲストシステムと、暗黙的に同じライセンスが重複して存在するため、これは潜在的な脅威です。同時に、それは高可用性ソリューションの本質を構成します。

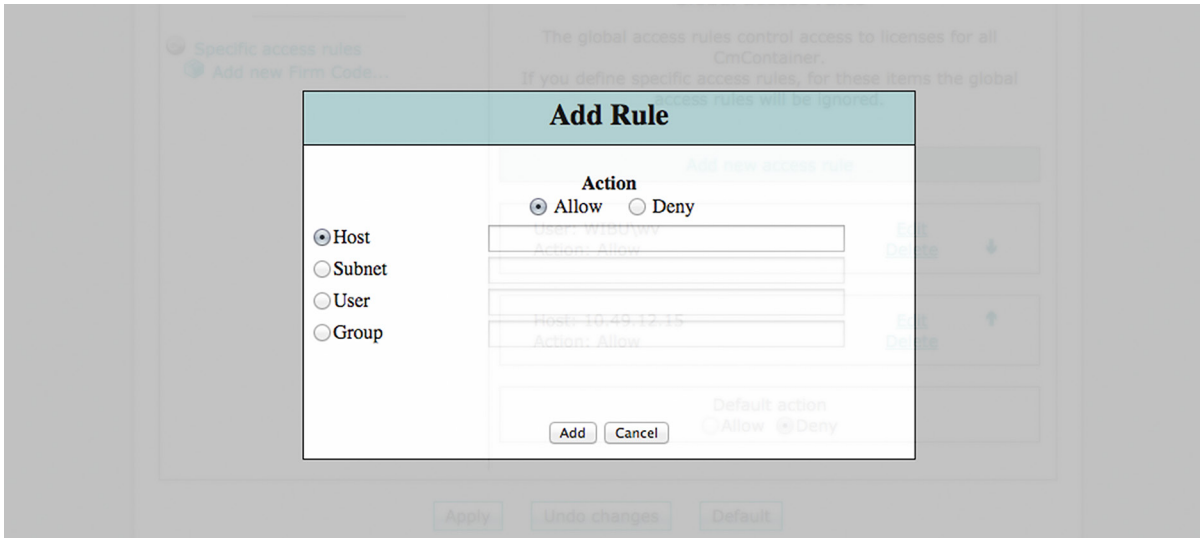
CodeMeterの構成を決めるのはソフトウェアベンダー次第です。CodeMeter SmartBindを「Medium（標準）」または「Strict（厳しい）」に設定すると、98%を超える信頼性で別のホストシステムへの移動が検出されます。これは、現在のテクノロジーで許可されている最高の検出率です。

SmartBindを「loose（ゆるい）」に設定するか、「乱数」や「IPアドレス」などの弱いバインドを使用することで、ゲストシステムのライセンスを別のホストシステムに取得できると判断できます。 これにより、クライアントはシンプルな高可用性ソリューションを確立できます。

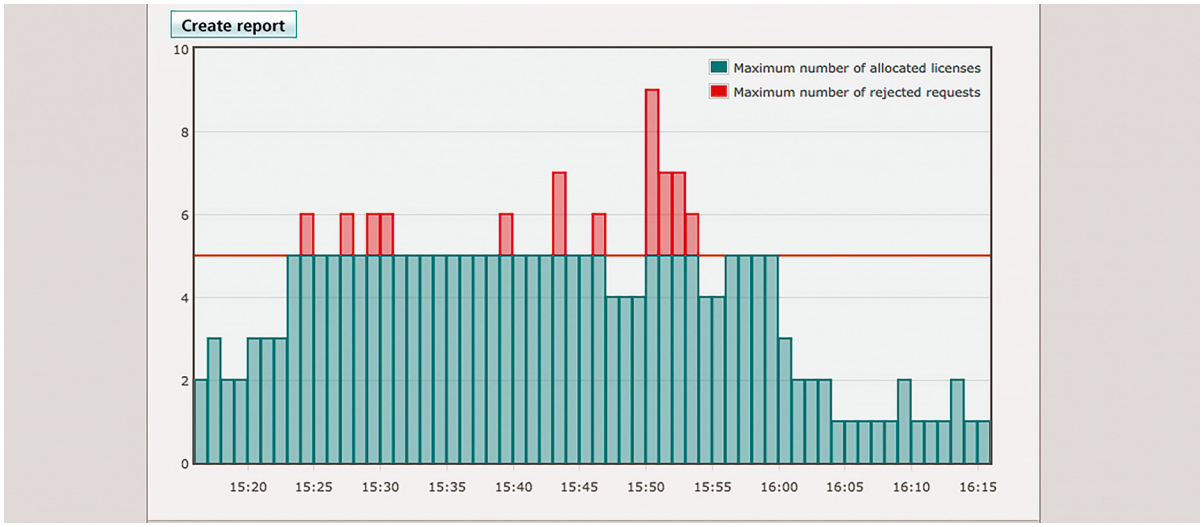
ユーザーのライセンス管理

CodeMeterを使用すると、ソフトウェアのユーザーは、Active Directory内の特定のマシン、ユーザー、またはユーザーグループのライセンスを予約できます。 そうすることで、ユーザーは許可された担当者のみが使用可能なライセンスにアクセスできることを確認できます。 これにより、特に保護されたソフトウェアとCodeMeter Runtime Serviceの両方がターミナルサーバーに保持されている場合に、権限のないユーザーがライセンスを「占有」するのを防ぐことができます。

ユーザーは、フローティングネットワークライセンスを柔軟かつ直接、指定されたスタッフメンバーに割り当てることができます。たとえば、10個の使用可能なライセンスには、サポートチーム用の3つのライセンス、開発チーム用の4つのライセンス、さらに無料で使用できる3つのライセンスが含まれます。アクセスを特定のマシン、ユーザー、またはグループに制限することもできます。 定義された最大数は、ライセンスを使用できるこれらのマシンまたはユーザーの数を示します。



使用時間に関する詳細情報により、ユーザーはライセンスの使用方法を監視し、利用可能なリソースのボトルネックや未使用の予約を検出できます。

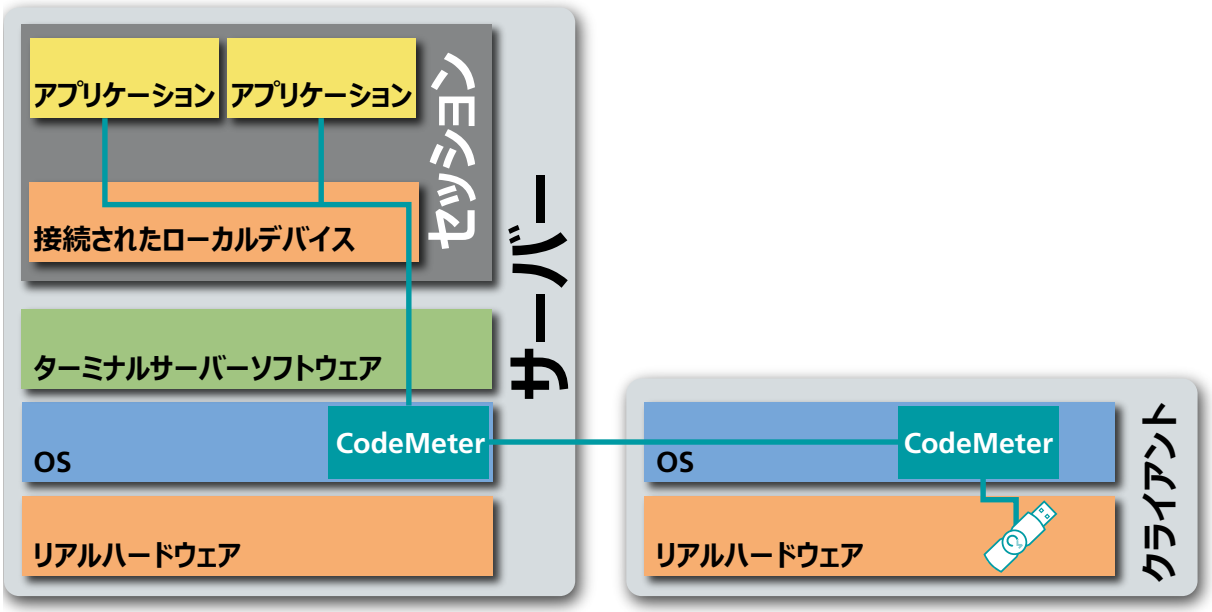


ターミナルサーバークライアント

個々の使用例では、ターミナルサーバークライアントにライセンスを保存する必要があります。このような場合、CodeMeter Runtime Serviceはクライアントにインストールされ、ネットワークサーバーとして構成されます。

ターミナルサーバー上の保護されたソフトウェアには、クライアントのIPアドレスと名前が与えられ、そこに格納されているライセンスサーバーとのリンクを確立します。クライアントへのアクセスを制御することにより、ユーザーはライセンスが実際に自分だけで使用されていることを確認できます。 ターミナルサーバー側では、このセットアップに必要なのは、ポート22350を介したクライアントへの直接TCP/IP接続のみです。

図11：
高可用性とセキュリティを備えたクライアント上のCmDongle



高可用性とセキュリティ

非信頼環境での高可用性には、2対3の冗長性を備えたネットワークライセンスサーバーが必要です。

ユーザーは、3つの同一の関連するネットワークライセンスサーバーを受け取ります。ソフトウェアが3つのサーバーすべてとリンクします。 使用可能なすべてのサーバーに適切なライセンスを割り当て、同時に2つのサーバーを使用できるようにする必要があります。これにより、1台のサーバーが失われた場合でも、ソフトウェアを引き続き利用できます。

3つのネットワークライセンスサーバーに、CmDongleまたはCmActLicense、あるいは両方の組み合わせを装備できます。CmActLicenseを使用する場合、ネットワークライセンスサーバーが実際のシステムまたは仮想マシンで実行できるかどうか、および変更または移動したときにCmActLicenseが許容する許容量を定義できます。

結論

CodeMeterは、仮想環境およびターミナルサーバーで使用できるように完全に装備されており、現実的なユースケースにすぐに使用できるソリューションを提供します。



- CodeMeterは、実際のシステムと仮想システムのための単一のソリューションです。
- CodeMeterは、ライセンスの悪用に対する最高の保護を提供します。
- CodeMeterは、ソフトウェアに簡単に統合できます。
- CodeMeterは、必要に応じてライセンスの使用をカウントします。
- CodeMeterは、独自のニーズに合わせて柔軟にカスタマイズできます。

CodeMeterを使うことによりビジネスを完全にコントロールし、仮想環境のライセンスモデルを、実際のハードウェアのライセンスと同じように多用途かつ安全にします。

ドイツ本社



WIBU-SYSTEMS AG
Rueppurrer Str. 52-54
76137 Karlsruhe, Germany
Telephone: +49 721 93172-0
Fax: +49 721 93172-22
sales@wibu.com | www.wibu.com

ウイブシステムズは、グローバルなソフトウェアライセンス市場における革新的なセキュリティテクノロジーリーダーです。1989年に2人のテクノロジー起業家Oliver WinzenriedとMarcellus Buchheitによって設立された同社は、拡大する『繋がった世界』でデジタル資産と知的財産の最高レベルでの保護、ライセンス管理、セキュリティの提供を唯一の使命として注力しています。

最も安全で、ユニークで、汎用性の高いものを提供するという使命を持ち、ウイブシステムズはソフトウェアパブリッシャーとインテリジェントデバイスメーカーに技術を提供し、デジタル資産、技術的ノウハウ、知的財産の完全性の保護に特化した国際特許プロセスを組み込んだ、受賞歴のある包括的なハードウェアおよびソフトウェアベースのソリューションスイートを開発しました。

ウイブシステムズは、モットーである「保護、ライセンス、セキュリティの完全性」を通じて、倫理的に作成されたソフトウェアに立ち向かい、ERPやCRM、eコマースプラットフォームと完全に統合された新しいデジタルビジネスモデルを生成する一方で、ソフトウェアの偽造、リバースエンジニアリング、コード改ざんを撲滅する取り組みを強化します。

WIBU-SYSTEMS オフィス

WIBU-SYSTEMS USA, Inc.
USA: +1 800 6 Go Wibu
+1 425 775 6900
sales@wibu.us

WIBU-SYSTEMS BV
The Netherlands
+31 74 750 14 95
sales@wibu-systems.nl

WIBU-SYSTEMS sarl
France
+33 1 86 26 61 29
sales@wibu.fr

WIBU-SYSTEMS (Shanghai) Co., Ltd.
Shanghai: +86 21 556 617 90
Beijing: +86 10 829 615 60
info@wibu.com.cn

WIBU-SYSTEMS NV/SA
Belgium | Luxembourg
+32 3 808 0381
sales@wibu.be

WIBU-SYSTEMS LTD
United Kingdom | Ireland
+44 20 314 747 27
sales@wibu.co.uk

WIBU-SYSTEMS K.K.
Japan
+81-3-4360-8205
info-jp@wibu.com

WIBU-SYSTEMS IBERIA
Spain | Portugal
+ 34 91 123 0762
sales@wibu.es

Wibu-Systemsは、プログラムまたはこのドキュメントを事前の通知なしに変更する権利を明示的に留保します。

© 2020 Wibu-Systems. WIBU®, CodeMeter®, SmartShelter®, SmartBind® and Blurry Box® は、WIBU-SYSTEMS AGの登録票商標です。このドキュメントで使用されているその他すべてのブランド名および製品名は、それぞれの所有者の商号、サービスマーク、商標、または登録商標です。

5062-005-07/20200615