(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4309042号
(P4309042)

(45)発行日　平成21年8月5日(2009.8.5)　(24)登録日　平成21年5月15日(2009.5.15)

(51)Int.Cl.		F I		
G06F 21/22	(2006.01)	G06F	9/06	660A
G06F 21/24	(2006.01)	G06F	12/14	520F
G06F 12/00	(2006.01)	G06F	12/14	540A
G09C 1/00	(2006.01)	G06F	12/00	537H
H04L 9/32	(2006.01)	G09C	1/00	640Z

請求項の数 1　(全 13 頁)　最終頁に続く

(21)出願番号　特願2000-513380 (P2000-513380)
(86)(22)出願日　平成10年9月21日 (1998.9.21)
(65)公表番号　特表2001-517845 (P2001-517845A)
(43)公表日　平成13年10月9日 (2001.10.9)
(86)国際出願番号　PCT/US1998/019618
(87)国際公開番号　WO1999/016205
(87)国際公開日　平成11年4月1日 (1999.4.1)
審査請求日　平成17年9月21日 (2005.9.21)
(31)優先権主張番号　08/935,955
(32)優先日　平成9年9月23日 (1997.9.23)
(33)優先権主張国　米国(US)

前置審査

(73)特許権者　509038902
アールエヌ　アクイジション　コーポレイション
アメリカ合衆国　ワシントン州　９８１２１　シアトル　エリオット　アベニュー　２６０１　スイート　１０００
(74)代理人　100059959
弁理士　中村　稔
(74)代理人　100067013
弁理士　大塚　文昭
(74)代理人　100082005
弁理士　熊倉　禎男
(74)代理人　100084009
弁理士　小川　信夫

最終頁に続く

(54)【発明の名称】暗号化された素材の動的な変換の方法とシステム

(57)【特許請求の範囲】

【請求項１】

ローカルアプリケーション（１０１、１０２）又はネットワークアプリケーション（１０３）と、ファイルシステムマネージャ（１０７）又はネットワークサービスプロバイダ（１０８）と、ファイルシステムドライバ層（１０５）と、入出力デバイス（１０６）とを含むコンピュータのオペレーションシステムによってコンピュータに導入された暗号化された素材の使用を制御する方法において、

オペレーションシステムの仮想デバイスドライバ又はカーネルモードドライバとして構築された変換フィルタ（１０４）を上記ローカルアプリケーション（１０１、１０２）又はネットワークアプリケーショ（１０３）と、ファイルシステムドライバ層（１０５）との間に配置し、上記変換フィルタ（１０４）が、

暗号化された素材に対するローカルアプリケーション（１０１、１０２）又はネットワークアプリケーショ（１０３）からのアクセス要求を監視するステップと、

上記暗号化された素材に対するアクセス要求を受領すると、上記素材を取り出すステップと、

上記素材の使用に使用許諾が存在するかどうかを調べるステップと、

使用許諾が存在する場合には、中間保存媒体に転送することなく上記暗号化された素材を即時に復号化するステップと、

上記復号化された素材の使用期間及び上記復号化された素材に関連するカウンタの少なくとも１つを含む使用計量を監視するステップと、

上記監視された使用計量が上記使用許諾に適合しているかどうかを判断するステップの各ステップを実行することを特徴とする方法。

【発明の詳細な説明】

【０００１】

（技術分野）

本発明は、電子的デジタル形式で存在しているコンピュータ・ソフトウエアおよび他の知的所有物件の、計測されての使用に関する。本発明の最終結果は、ソフトウエア・オン・デマンドやソフトウエア購読などのサービスを可能にする。本発明はまた、コンピュータ・ソフトウエアおよび他の知的所有物件の海賊行為防止に対しても適用することができる。

【０００２】

（背景技術）

現行の消費者市場にあっては、デジタル形式で存在するコンピュータ・ソフトウエアおよび他の知的所有物件は、その他の消費用ハード物品と同様の販売が主としてなされている。しかしビデオ・テープおよび他のハード物品が日常的に賃貸される反面、ソフトウエア製品は、一般的にはまだなお購入を基準にしてしか入手することができない。その結果、少なくとも２つの有用なサービス、即ち、ソフトウエア・オン・デマンドとソフトウエア購読が概して用いられていない。ソフトウエア・オン・デマンドは、使用者が使用回数を基準にしてソフトウエア製品の支払いを行えばよいというサービスである。ソフトウエア購読は、月に１度といったような定期的予約購読を基準にして、１以上のソフトウエア製品を使用者が入手可能であるというサービスである。

【０００３】

これらのサービスが明らかに有用であるにもかかわらず、ソフトウエア製品に内在する性質の故に、技術提供業を可能にすることへの効果的な技術的挑戦が躊躇されてきた。これらのサービスを首尾よく支援するには、その可能にする技術は以下の範疇に合致しなければならない。

I．機密保護。ソフトウエア・オン・デマンドおよび購読形式で入手できるソフトウエア製品は、完全に機密保護対策がとられた方法で保護され、また管理されなければならない。可能にする技術は、もっとも熟練し、また果敢なるハッカ連中からソフトウエアを防衛しなければならない。とりわけ、熟練したシステムレベルでのハッカ連中は簡単にドアを開けてしまうので、ソフトウエアがそのオリジナルの状態で中間保存媒体にそのまま長くは存在し得ない。また可能性としてだが、誰にとってもアクセスが可能であるようなそんな中間保存媒体を利用できるようになるユーティリティがあるかも知れない。

II．非被侵入性。可能にする技術は、保護および計測された使用のためにソース・コードの変更を必要としてはならない。対照的に、侵入技術はそれ自身をソフトウエア製品のソース・コード中に埋設し、そのソフトウエアの再編集を必要とさせる。これに取り組むことは、余分なコーディング実施とリソースの試験実施との点で、保護プロセスにおける大変な費用負担を発生し、また、非常ににエラーを発生しやすい。

III．最小限のシステム費用負担。可能にする技術は、ソフトウエア製品の使用を保護し、起動し、および計測する間に、著しい費用負担を賦課してはならない。可能にする技術によって生じる一般的な費用負担は、追加のＲＡＭとハードディスクの記憶スペースが必要であること、保護されたソフトウエアを復号化する前に保護を行うプロセスを起動すること、および使用を監視する間でのＣＰＵなどの別のシステム・リソースにとっての競合が含まれる。

IV．システム・クロック再設定に対する耐性。コンピュータ・システムのクロック設定を変更することによって、ソフトウエア製品の使用者は、許諾されている使用期間を著しく延長することができ、その結果、ソフトウエア・オン・デマンドおよびソフトウエア購読のサービスの有効性を損なってしまう。可能にする技術は、システム・クロック再設定に対する防衛を可能にし、対策行為をとることが可能であるものでなくてはならない。

V．絶えず保護を行い計測を行うこと。ソフトウエア発行者が、一旦、ソフトウエアを可

能にする技術の保護と管理との下においたならば、それは絶えず保護されまた管理されなければならない。その後、複製をしたり再導入をしたりしても、その保護と管理とを駄目なものにしてはならない。
VI．使用者が使いやすいものであること。可能にする技術は、使用者にとって著しい、システム設定上の変化をもたらすやり方でコンピュータ使用者の環境を変化させてはならない。使用者インターフェイスは完全に直感的なものであり、容易に使用できるものでなくてはならない。
【０００４】
入手することのできる、従来技術での保護技術は、「ラッパー」および「リディレクション」技術とに基づいている。「ラッパー」は、しばしばオペレーティング・システム・シェル・プログラムまたは保護されたソフトウエアの変更された起動コード部の形式をとる。その機能は、保護されたソフトウエアに対する直接のアクセスを遮蔽するものである。保護されたソフトウエアが使用者によってアクセスされた場合、「ラッパー」が最初に実行される。暗号化された状態にある保護されたソフトウエアはその後復号化され、オリジナルの状態で一時保存媒体上に再保存される。「ラッパー」はその後、アクセスを一時保存媒体上の再保存されたソフトウエアに転送する。
【０００５】
カリフォルニャ州サンタ・クララのテストドライブ・コーポレーションによって開発されたシステムは、購入前試行ソフトウエア評価サービスを提供する。このシステムは、ソフトウエアのオリジナル版を、限定された期間もしくは評価期間だけしか使用することができない無効版に変換する。もしソフトウエアの購入を希望するならば、そのソフトウエアをオリジナルの状態に変換する解錠コードを購入することができる。好ましい実施態様にあっては、この従来技術でのシステムは、例えばコンピュータ・プログラムのような、選択された素材に適用され、また、その素材の一部分はオリジナルの素材からは分離される。この方法にあっては、素材の分離された部分と素材の残りの部分とを含むオリジナル素材の変質された版がつくられる。試用期間中、その素材の変質された版は一時保存媒体中におかれるが、分離された部分のみはシステム使用者によってたやすくアクセスされる。さらに、素材の分離された部分は、変形された部分に置き換えられ得る、例えば、素材のアクセスされる回数である数字を限定する目的でカウンタが含まれ得るし、オリジナルの素材に対して、例えば、音声信号における警告音や映像信号における遮蔽物のような妨害素材が加えられ得る。
【０００６】
これら「ラッパー」および「リディレクション」技術を基準にしたシステムにおける幾らかの欠点は明白である。
I．機密保護の欠陥。「ラッパー」および「リディレクション」技術は、再保存されたソフトウエアの全てもしくはオリジナルの状態におけるそのソフトウエアの残りの部分を物理的に受け入れるのに、一時保存媒体を必要とするので、まさしくその、システム使用者によるアクセスが可能である、オリジナル状態での素材の存在が、システムをハッカの攻撃に対して弱いものにしている。オペレーティング・システムの専門家にとって、オリジナルの状態にある素材へのアクセスを入手し、素材の海賊版を再販売することは可能である。ユーティリティ・ソフトウエア・プログラムもまた、この海賊行為を繰り返して成し遂げるために、ことによると開発され得たかも知れないし、可能なサービスの有効性を損なうためにパブリック・ドメインで入手できるようにされているかも知れない。「ラッパー」と「リディレクション」技術は、初心者からの攻撃に対してソフトウエアを保護することができるものの、専門家に対しては、高度に機密保護をするものではない。
II．システムの負担。「ラッパー」プログラムを起動すること、そのオリジナルの状態で再保存されたソフトウエアを物理的に保存すること、および、一時保存媒体を創出し管理すること、これら全ては、使用者が必要とするソフトウエアを起動するに先立っての遅れを負わせる。これらの行為はまた、オペレーティングシステムが走らせる別のプロセスを有する別のシステム・リソースと競合する。

III．スペースの負担。オリジナルの状態でランダム・アクセス・メモリ（ＲＡＭ）中に再保存されたソフトウエアの保存領域は、保護されたソフトウエアが通常必要とするＲＡＭスペースの１００％以上を余分に必要とする。多重の保護されたソフトウエアを同時に実行することのできる多重処理オペレーティングシステムにおいては、この負担は倍化され、またシステムの動作性能に顕著に影響を与える。
IV．好まれざる邪魔物。コンピュータ・システム中に一時保存媒体、例えば仮想的デバイスのような、を創出することは、コンピュータ・システム使用者にとって通常好まれることのない、異質の人工遺物である。したがって、使用者は、ラッパーやリディレクション技術で発生させられた邪魔物や人工遺物を除去するため、結局はオリジナルの素材を完全な姿で購入しようと望むことであろう。従って、これらの技術は、絶え間なく使用を計測し保護を行うサービス提供には向いていない。

【０００７】
現在のところ、復号化された素材を一時媒体上に転送をしたり保存したりすることなく、暗号化されたソフトウエアおよび他の電子的素材のリアルタイムの復合化を提供できる高度に機密保護を行う方法は知られていない。

【０００８】
（発明の開示）
本発明は、ソフトウエア・オン・デマンドおよびソフトウエア購読のサービスを可能にする、ダイナミック変換フィルタ技術に基づいた方法とシステムを提供する。本発明はまた、その他の電子的素材の販売においても有用である。本発明において利用される装置は、本技術の保護下にある復号化された素材にとって如何なる中間保存領域をもつくらない。そのかわりに、本装置は、オペレーティング・システムの仮想的組込部分として構築され、例えばハード・ドライブのような入出力デバイスに出入りする「読み出し」、「書き込み」、および「開く」／「実行する」全てのアクセスを監視し「濾過」する。保護された素材が「読み込み」、「書き出し」、もしくは「開く」／「実行する」アクセスを受けたならば、変換フィルタはそれ自身を、素材を低レベルのファイル・システム層を通って高レベルのアプリケーション層に読み込みをするのに必要とされるクリティカルパスに位置づける。素材は暗号化された状態で、その変換フィルタに入る。変換フィルタは素材が通過するときにそれを復号化し、オリジナルの状態にあるその素材を、アクセス要求を実行するために高位のレベルにあるオペレーティング・システム構成要素に引き渡す。中間保存領域の必要性が除去されたので、そのオリジナルの状態で復号化された素材は、オペレーティング・システム構成要素の組込部分にとってのみ見えるものであり他のシステム使用者は見えない。結果として、従来技術でのシステムを上回って機密保護が格段に改善される。

【０００９】
変換フィルタは、完全に異なった目的用にオペレーティング・システムが提供するプログラム可能なサービスを、「濾過する」機密保護および管理システムへと変換することによって形成される。このプログラム可能なサービスは、ウインドウズ９５™ソフトウエアの場合には、仮想的デバイス・ドライバであり、また、ウインドウズＮＴ™の場合には、カーネル・モードのドライバであることが好ましい。

【００１０】
本発明は、保護された素材の内部に邪魔をしないように埋設された素材と一緒に作動することができる。そのことは、幾ばくかの簡単に追従できるステップを踏むだけで如何なる素材をも復号化するユーティリティを提供する。本発明は、アメリカ合衆国政府および民間企業から入手可能な標準データ暗号化の仕組みを採用する。しかし、本発明にある装置は、復号化された素材の機密保護をさらに保障する目的で、拡張されたキー管理機能を提供する。消費者のパソコン上に導入された全ての素材は、２つの暗号化プロセスを通過する。第２の暗号化プロセスは、そのコンピュータ使用者のユニークＩＤから生成される動的にユニークなキーを必要とする。そのキーの動的生成は、如何なる解読用のキーもハード・ディスク上に保存されたファイルから直接的に得ることができないことを保証する。

【００１１】
本発明は、変換フィルタが、デジタル形式で存在しているソフトウエア製品および他の知的所有物件の使用を絶えず管理し、計測し、課金することを可能にする。そのような素材はオン・デマンドで何回も注文することができるし、また同様に購読を基準にして入手することもできる。導入された素材を別のコンピュータに複製することは、単にその素材の暗号化された版をつくり出すに過ぎない。しかし、復号化された素材の永久的複製は、その発行者の権限でおこなわれる。
【００１２】
本発明は、そのような素材の使用者にとって、モデム経由もしくは現存の民営ネットワークやインターネット接続を介して、交換所のサーバに接続することができるようにするシステムの構成要素を提供する。その交換所のサーバは、注文と課金用のカード番号との受領に基づき、引き換えに、素材の計測されての使用を可能にする許認可コードを生成する。現行の受入可能な課金用カードは通常のクレジット・カードとデビット・カードとを含んでいる。将来の支払方法は、実例的にはスマート・カードとデジタル・キャッシュとを含むことであろう。システムのこれら構成要素はまた、利用者の返還および交換の処理を可能にすることであろう。
【００１３】
本発明は、例えばインターネット上での電子的素材販売や、実際の店先で販売されるＣＤ－ＲＯＭや、ＤＶＤ，ＶＣＤ，ケーブル・モデムおよびその他の放送チャネルのような、あらゆる可能なチャネル経由で販売される素材に適用することが可能である。
【００１４】
本発明はまた、ネットワーク・ファイル・システムにわたって、素材に対するアクセスがシステムによって等しく管理され計測されるネットワーク環境において作動する。
【００１５】
（発明を実施するための最良の形態）
本発明は、マイクロソフトのウインドウズ９５もしくはウインドウNTのようなオペレーティング・システムの内部に組込まれた方法と装置である。この方法と装置は一時保存媒体への転送を行うことなく即時に暗号化された素材の動的な復合化を可能にする。その結果、本発明は電子的形態にあるソフトウエア製品および他の素材が暗号化を通して保護され、また、管理され計測されての使用をするために利用できるようにする。
【００１６】
本発明の好ましい実施態様にあっては、変換フィルタは、多重処理オペレーティング・システム環境で動作しているカーネル・レベルのプログラムとして構築されており、また、暗号化された素材はアプリケーション・ソフトウエアである。しかし、本発明は同様に、べつの状況、例えば暗号化された形式にある音声や映像素材の販売にも適用することができる。
【００１７】
図１は、高レベルの基本設計概念図であり、オペレーティング・システム内部における変換フィルタの位置と機能とを示している。
【００１８】
高レベルのアプリケーション・プログラムは、ローカル・アプリケーションおよびネットワーク・アプリケーション１０１，１０２，１０３を含むが、「読み込み」、「書き込み」および「開く」／「実行する」行為を成就するため、システムの入出力デバイス１０６上に常駐しているソフトウエア素材へのアクセスを要求する。これらの要求は、ＯＳのファイル・システム・マネージャ１０７もしくはネットワーク・サービス・プロバイダ１０８のようなオペレーティング・システム構成要素に対して提出されなければならず、また、ファイル・システム・ドライバ層もしくは同様にカーネル・レベル上にあるネットワーク・ファイル・システム・ドライバ層１０５に中継されなければならない。本発明によると、変換フィルタ１０４は、アプリケーション１０１，１０２，１０３とファイル・システム・ドライバ層１０５との間に位置される。実例として、ウインドウズ９５™ソフトウ

エアの状況にあっては、変換フィルタは仮想的デバイス・ドライバとして構築され、またウインドウズＮＴ™の場合には、カーネル・モードのドライバとして構築される。

【００１９】

もし、ローカルおよび／またはネットワークのアプリケーションから来ている、ファイル・システムに対するアクセス要求が「下流」に進んでいるものであると判断された場合、その後、オペレーティング・システムの上位層に対して入出力デバイスから読み出されている全てのデータは「上流」に進んでいるものであると判断される。下流（アプリケーションからファイル・システムに下る）および上流（ファイル・システムらアプリケーションへ）の両データは、以降本書類ではクリティカルパスと称する特定の経路を通過しなければならない。変換フィルタ１０４は、クリティカルパス中にある。

【００２０】

データが変換フィルタを上流方向に向けて通過するときは常に、変換フィルタは暗号化されたソフトウエアをそのオリジナルの状態に変換するという必要な変換を遂行する。そのオリジナルの状態に転位されてしまっているソフトウエアはその後、オペレーティング・システムの上位層に引き渡される。もしも要求がアプリケーション、例えば画像閲覧ソフトからのものでディスプレイ用にファイルを開くというものであった場合、変換されたソフトウエア素材が、最終的にはそのアプリケーションに引き渡される。要求を出しているアプリケーションの見地からすれば、この暗号化されたソフトウエア素材を開くことは、別のオリジナルのソフトウエア素材を開くことと何も変わることはない。変換プロセスは、要求を出しているソフトウエアに対して完全に透明なものである。もしも要求がファイルを実行することで（例えば、ファイル上でマウスのダブル・クリックがなされる）、オリジナルのソフトウエア素材が実行可能なプログラムである場合、変換されたソフトウエアは、メモリ内部で実行をするようにオペレーティング・システムの読み込み機能に引き渡される。このプロセスは、「濾過をすること」と考えられる。というのは、上流に移動している暗号化されたソフトウエアは、装置に入り、そして、あたかも濾過をするデバイスを通過したかのように、復号化された状態で出てくるからである。全ての「濾過をする」プロセスの間、復号化されたソフトウエアの如何なる中間保存領域もシステム使用者に対して露呈されることがない。すべての引渡と復号化のプロセスとは、高度に機密保護がとられている方法にある内部活動としてオペレーティング・システムの内部で行われる。

【００２１】

変換フィルタ１０４は、あたかもそれがオペレーティング・システムの組込部分であったかのように構築される。追加の機密保護策が変換フィルタ１０４内部に組込まれる。それで上流および下流のデータを「濾過をする」ことが可能であるのみならず、またオペレーティング・システムの中のハッキング行為を監視し、いかなるのであれ機密保護を破壊するものが生じてくるのを防止するための対策をとる。

【００２２】

図２は、ブロック図で、事前導入の暗号化されたステップへとオリジナルのソフトウエア素材を暗号化しているプロセスを示すものである。図２に示されるように、オリジナルのソフトウエア素材M_O２０１は、暗号化プロセスP_E２０３において変換関数f_E２０２のアプリケーションによって暗号化される。暗号化のプロセスは、ＤＥＳもしくはＲＳＡのような標準の暗号化プロセスであることが好ましい。この暗号化プロセスの結果が、暗号化されたソフトウエアM_E２０４であり、ＣＤ－ＲＯＭ、インターネットなどのような種々の販売チャネルを通じて機密保護状態で転送され得るものである。

【００２３】

第２のプロセスP_B２０９の間、ソフトウエア使用の管理と計測とを首尾よく行うことの支援をする４つの別の構成要素がM_E２０４に追加される。これらの構成要素とは、使用許諾マネージャ２０５、利用者アプリケーション２０６、変換フィルタ２０７、および製品独自の署名データ２０８である。使用許諾マネージャ２０５は、ソフトウエア・プログラムであり、暗号化されたソフトウエアの使用に関するデータを含む使用許諾のデータベースを整備すること、暗号化されたソフトウエア素材M_Eの使用者との仲立ちをすること

、および許認可された使用期間の終了に伴い暗号化されたソフトウエア素材の使用打ち切りを行うことに役割を果たす。利用者アプリケーション２０６は、ソフトウエア・プログラムであり、交換所のサーバから、暗号化されたソフトウエア素材M_Eを使用するための許認可を要求するのに、および交換所のサーバからの適切な許認可コードを受領するのに用いられる。この活動はまた電子的支払いの何らかの形式、例えばクレジットもしくはデビット・カードの番号提供のような、を伴うことができる。加えて、利用者アプリケーションはまた、料金徴収、販売促進とアップグレード情報、および追加ソフトウエアのダウンロードを行う能力を含むことができる。変換フィルタ２０７は、当のソフトウエアであり、暗号化されたソフトウエア素材M_Eへのアクセスを管理する。このソフトウエアの更なる詳細が、図１および４との関連で記述される。製品独自の署名データ２０８は、特定の暗号化されたソフトウエア・素材M_Eに対してユニークなコードである。

【００２４】

プロセス２０９の出力は、単一出力ファイルM_I２１０であり、事前導入の暗号化されたソフトウエア素材であって、全ての入力構成要素２０４、２０５、２０６、２０７、２０８から構成される。プロセス２０９は、構成要素２０４、２０５、２０６、２０７、２０８を単一のソフトウエア製品へと単に結合させることが好ましい。他に、プロセス２０９はまた、追加の暗号化プロセスを伴うことができたはずである。

【００２５】

本発明の好ましい実施態様にあっては、出力ファイルM_Iは、オリジナルのソフトウエア素材の名称、アイコンおよびその他のプロパティを見かけ上そのまま引き継ぐ。従って、外部から見た限りでは、このファイルはオリジナルのソフトウエアと全く同じに見える。本実施態様は主として、ソフトウエア製品のパッケージを行うに際しての、ソフトウエア発行者にとっての余分なステップを削除するためのものである。

【００２６】

次に、ソフトウエア発行者は、あたかも図２の暗号化プロセスが決して起きたことがないかのように、自分たちのソフトウエアを正常な導入パッケージに入れ込むのに自分たちが気に入っている導入パッケージング・ユーティリティ、例えばインストール・シールド^{TM}のような、を用いることができる。

【００２７】

図３はブロック図であり、使用者のパソコン上に暗号化されたソフトウエア素材を導入しているプロセスを示している。好ましい実施態様にあっては、出力ファイルM_Iはそれ自身の導入プロセス３０２を、使用者がソフトウエアの導入の通常手順を行った後に、正にあたかもそのソフトウエアは暗号化されたことなどなかったかのように起動する。導入プロセスP_I３０２は、事前導入されたソフトウエア素材M_I２１０／３０１のキーとなる構成要素を生み出す。最初、使用許諾マネージャ３０３、利用者アプリケーション３０４および変換フィルタ３０５が抽出されてシステム中の適当な隠れた場所に導入される。製品独自の署名データ３０６および暗号化されたソフトウエアM_Eが同様に持ってこられる。

【００２８】

同時に、D_P３０７として表されている使用者特性データおよびオペレーティング・システム独自の情報がプロセスP_U３１２中で変換関数f_I３０８によって変換され、利用者にとってのユニークＩＤ３１３を生成する。ユニークＩＤを生成することでは、従来技術のどんな数であってもプロセス３１２で使用することができる。便利なように、ユニークＩＤ３１３の生成にあっては、我々はミリ秒で測定された精度、というのは２人の使用者が同じミリ秒において彼らのソフトウエアを導入する確率は事実上ゼロだから、の時刻印を使用するように設定する。ユニークＩＤ３１３は引き続き、システムのあらゆる局面および構成要素中で使用される。

【００２９】

製品独自の署名データ３０６、ユニークＩＤ３１３および暗号化されたソフトウエアM_Eは、プロセスP_{ES}３０９に供給される。プロセスP_{ES}は、変換関数f_Eの逆関数を用い、ソフトウエア素材を復号化し、それによってオリジナルの素材M_Oを再保存する。ここま

での復合化プロセスは周知である。その後、ユニークＩＤ３１３と製品独自の署名データ３０６とに基づいたユニーク暗号化キーで即座にM_Oを再度暗号化する。再び、例えばＤＥＳもしくはＲＳＡのような標準暗号化プロセスが使用され得る。その結果が、ユニークに暗号化されたソフトウエア・素材M_U３１０である。ソフトウエア・素材M_Uはその後、ドライバ層１０５の上方に導入される（図１を参照のこと）。

【００３０】

好ましい実施態様にあっては、本発明は、M_Uを生成するのに使用されたユニークな暗号化キーを絶対に保存しない。必要な場合には常に、このユニーク・キーは同じ入力（ユニークＩＤおよび製品独自の署名データ）とキー生成プロセスとを用いて動的に再生成することができる。このキー管理方策があるため、暗号化されたソフトウエア素材を損なおうとしても極めて困難なものにしている。キーのユニークさはまた、一旦ソフトウエアが導入されたならば、どんな２人をもってきても、それらの使用者のコンピュータ上に同一である暗号化されたソフトウエア素材は存在することがないということを保証する。

【００３１】

導入の最後に、図４との関連で以下に記述される使用管理や計測のプロセスを首尾よく実行するための、あらゆる使用許諾情報、使用のカウンタおよびその他の重要な情報を保持する使用許諾データベースＤＬ３１１が生成される。使用許諾データベースは暗号化されたソフトウエアを「登録された」状態にあるもの、即ち、本発明のシステムの影響下にあるものとして識別する。このデータベースはまた、コンピュータ・システムに保存される。

【００３２】

図１を参照する。変換フィルタ１０４は、コンピュータ・システムに導入され、入出力デバイス１０６上に常駐しているソフトウエア・ファイルへのあらゆるアクセス要求を途中で捕捉する。ウインドウズ９５™オペレーティング・システムにあっては、このことは当の変換フィルタを仮想的デバイス・ドライバとして導入することで成し遂げられる。ウインドウズＮＴ™オペレーティング・システムにあっては、このことは当の変換フィルタをカーネル・モード・ドライバとして導入することで成し遂げられる。

【００３３】

ソフトウエア素材を読み出したり、書き込んだり、実行したりする、もしくは見るためにソフトウエア素材を開いたりする使用者行為は、オペレーティング・システムによって処理される。より高いレベルのオペレーティング・システム処理（例えば図１のローカルもしくはネットワーク・アプリケーション１０１、１０２、１０３）は、それら行為の要求を下流のドライバ層１０５に向かって変換フィルタ１０４を通過させていく役割を有する。

【００３４】

図４は変換フィルタの内部プロセスのフローが記述されたものを示している。ボックス４１６に示されるように、変換フィルタはあらゆる入出力要求にそなえて、オペレーティング・システムを絶えず監視している。そんな要求が変換フィルタに到着すると、それはソフトウエアと使用許諾情報を得るプロセス４０３を起動する。このプロセスは要求されたソフトウエアにとっての、そのソフトウエアの使用の最新の状態、使用許諾、許認可・コード、失効日、製品独自の署名データ２０８／３０６、を含む使用許諾情報（もしあるならば）をその他の関連する情報と併せて取得する。引き続き、２つの確認テストが適用される。即ち、ソフトウエアが登録されているかどうかのテスト（ステップ４０６）および使用許諾が有効であるかどうかのテスト（ステップ４０７）である。もし、要求されたソフトウエアが登録されていなかった場合、変換フィルタは、それ以上何のアクションもとらずに、単純に管理をオペレーティング・システムのステップ４１３における要求プロセスに移転して戻す。もし、ソフトウエアが登録されている場合、変換フィルタはステップ４０７において、有効である使用許諾が存在するかどうかをチェックする。有効な使用許諾がない場合、利用者アプリケーションがステップ４１４で導入され、使用者に更なる使用を注文するかまたはソフトウエアを購入するように促す。

【００３５】
注文入力プロセスは、システムの利用者アプリケーション構成要素によって取扱われる。利用者アプリケーションは使用者のコンピュータを交換所のサーバにモデム経由もしくは現行のインターネット接続を介して接続する。交換所のサーバは、有効であるクレジット・カードまたはデビット・カードの番号の受領に基づいて、引き換えに許認可コードを生成し、登録されていたソフトウエアの正当な使用ができるようにする。
【００３６】
もし、ソフトウエアにとっての有効な使用許諾が見られ、それを実行することが許認可された使用期間内である場合、変換フィルタは機密保護監視プロセス４０８を起動し、復号化された後変換フィルタを出て行くデータの乗っ取りをしようと試みているものと思われるあらゆる第３者のプロセスの走査を遂行する。オペレーティング・システム中に疑わしい行為が存在する場合、変換フィルタは潜在的脅威を除去するための対策をとる。
【００３７】
次いで、暗号化されたソフトウエアを復号化するのに使用されるべきユニーク・キーは、キー生成プロセス４０９において生成される。このキーは、ユニークID３１３と製品独自の署名データ３０６とから生成される。生成された復合化キーと暗号化プロセス３０９の逆関数とを用いて、変換フィルタはその後、即時に、復号化を行う変換プロセス４１０においてソフトウエアのあらゆる暗号化された部分を復号化する。オリジナルの状態に復号化されたソフトウエアはその後、ステップ４１３で要求プロセスに引き渡される。オペレーティング・システムはいまや、アクセスを要求したアプリケーションに対して復号化されたソフトウエア素材の実行即ち送り込みを首尾よく処理することができる。
【００３８】
復号化されたソフトウエアが要求しているプロセスに一旦引き渡されたならば、変換フィルタは、ステップ４１１で使用計測カウンタを起動する。使用カウンタが走っている間変換フィルタは、ステップ４１２で使用許諾期間違反がないかどうか、即ち使用許諾の満了がないかどうか、絶えず使用の量をテストする。ソフトウエアにとっての使用許諾期間の違反がある、即ち使用許諾が満了してしまっている場合、変換フィルタは、使用許諾マネージャを起動するプロセスをステップ４１５で起動する。使用許諾マネージャは使用許諾データベースを適切に整備し、最新日のものにし、種々の伝言で使用者を案内し、使用者から戻る要望を取り込むことで使用者と対話を行う役割を担う。必要なときは常に、使用許諾マネージャは、使用者に対して警告と応答に必要な妥当な時間を与えた後、登録されたソフトウエア素材の使用打ち切りを行う役割を担う。使用許諾マネージャは、使用許諾が満了したとき、使用者に更なる使用の注文を行うよう案内をするために管理を利用者アプリケーションに移転することができる。
【００３９】
本発明は、ソフトウエア素材の暗号化をすること、登録をすること、注文をすること、使用ができるようにすること、復号化をすること、使用を管理し計測をすること、の全てを可能にする。消費者に益をもたらすことになる業としてのサービスは、それらのみに限定するものではないものの、ソフトウエア・オン・デマンド、ソフトウエア賃貸、ソフトウエア購読、購入前試用を含んで、本発明の方法とシステムによって適切に支援され得る。
【００４０】
ソフトウエア提供における本発明の２つの適用例は、ソフトウエア・オン・デマンドおよびソフトウエア購読サービスである。
【００４１】
ソフトウエア・オン・デマンド・サービスの真髄は、消費者がソフトウエアを使いたいと思ったときにはいつでも自由にそのソフトウエアを入手できるようにすることである。このサービスを通して入手可能となったソフトウエア素材は、例えば会計用ソフトウエア、ゲーム、教育および娯楽用ソフトウエア、CAD用ソフトウエアなどのような、アプリケーション・ソフトウエアであってよい。ソフトウエア素材はまた、例えばオーディオ、ビデオ、類の形式のもしくは、単に平易なバイナリもしくはテキスト・ファイルを呈するマル

チメディア・コンテントのような、どんな電子的に保存された素材であってもよい。このサービスは、本発明によって以下のように支援される。
１．発行者は、図１のステップに沿ってソフトウエア素材を暗号化するのに本発明を使用する。暗号化されたソフトウエア素材は、交換所のサーバが知るところの登録されたソフトウエアとなる。
２．ソフトウエア素材は、どれでもよいが、市販で入手可能な導入パッケージング・ソフトウエア、例えばインストールシールド、を用いてパッケージされる。１人もしくは数人の発行者からの多重プログラムもしくは他のソフトウエア素材が１つのソフトウエア・パッケージに結合され得る。
３．ソフトウエア素材は、例えばインターネット／ＷＷＷ、ＣＤ－ＲＯＭ、ＤＶＤもしくはＶＣＤのような、種々のチャネルを通じて使用者に販売される。
４．使用者は、ソフトウエア・パッケージ内にある入手可能な素材全てをリストしているオンラインに基づいた電子カタログから選択する。彼もしくは彼女は、１つもしくは幾つかのソフトウエア・プログラムもしくは他の素材を、彼もしくは彼女のコンピュータ上に図２のステップに沿って導入しようと判断する。
５．使用者はその後、ソフトウエア・プログラムもしくは他の素材の１つの使用を決心する。
６．使用者は、ソフトウエア・プログラムもしくは他の素材にアクセスするため、実行コマンドを発する即ちアプリケーションを呼び出す。
７．使用者は、利用者アプリケーション経由でそのような使用に対してクレジット・カードもしくはその他の形式のデビット・カード番号で支払いを行うように案内される。
８．使用者は、交換所のサーバ設備に、モデム経由もしくはインターネット接続を介して接続される。もしファイヤ・ウォール（企業使用者用に）がある場合、本発明は、ファイヤ・ウォールの許認可プロセスを通過するための手順を作動する。
９．使用者は、利用者アプリケーションによって交換所のサーバから取り出された料金情報を点検する。
１０．使用者は注文を確認する。
１１．交換所のサーバは、許認可コードを発行する。
１２．許認可コードは、要求されたソフトウエア素材を使用できる状態にする。使用カウンタが、この注文のやりとりを記録するために最新日のものにされる。
１３．使用者は、実行即ちアクセスのコマンドを再度発する。
１４．変換フィルタは、動的に必要な変換を遂行し、ソフトウエア素材の正当な使用を可能にする。
１５．使用は、使用許諾マネージャ・アプリケーションによって計測および管理される。

【００４２】
ソフトウエア購読サービスは、ソフトウエア・オン・デマンド・サービスに類似のステップに従うが、サービスへの支払いが月ベースであるところが異なる。使用者はまた通常多数の製品の使用を毎月自由に選択することができる。

【００４３】
本発明の適用のその他の例は、音声／映像もしくはテキストの素材販売におけるものである。そのような素材は、基本的にアプリケーション・ソフトウエアと同じやり方で暗号化され、準備され、そして販売され得る。使用者は、そこで、見たり聞いたりしたい素材を選択し、ソフトウエアを入手するのと同様のやり方でそれを入手する。但しこの場合、映像素材はディスプレイされるし音声素材はスピーカ・システムを駆動するのに使用される。

【図面の簡単な説明】
本発明のこれらおよび他の目的、特徴および利点は、以下の本発明の詳述からきわめて容易に理解されるであろう。
【図１】　システムの構成要素、それらの相対的位置と相互依存関係およびデータの流れの方向を示している高レベルの基本設計概念図である。

【図２】　オリジナルの素材を、保護された状態に暗号化しパッケージングするプロセスを示す。
【図３】　ユニークIDの生成や使用者ユニーク・キーを用いた第２の暗号化を含んだ、使用者のコンピュータ上に保護された製品を導入するプロセスを示す。
【図４】　変換フィルタの内部プロセスの流れを示すフローチャートである。

【図１】

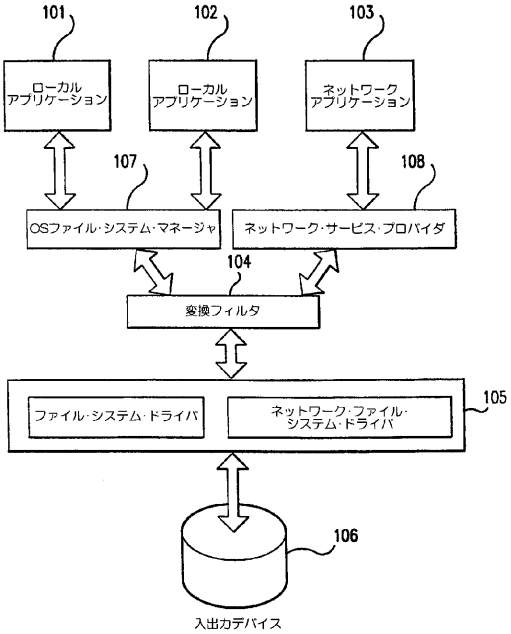

FIG.1

【図２】

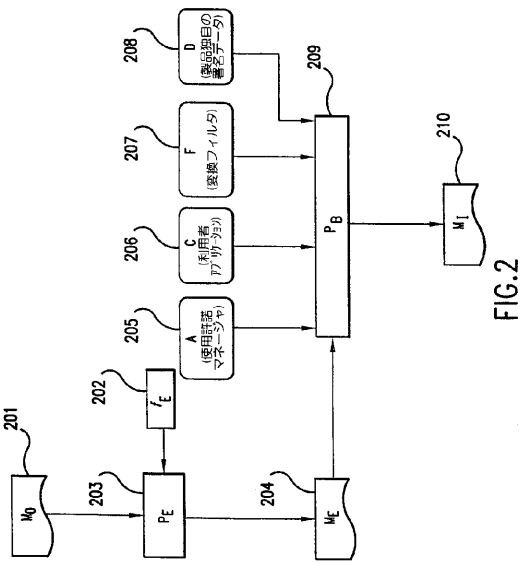

FIG.2

【図３】

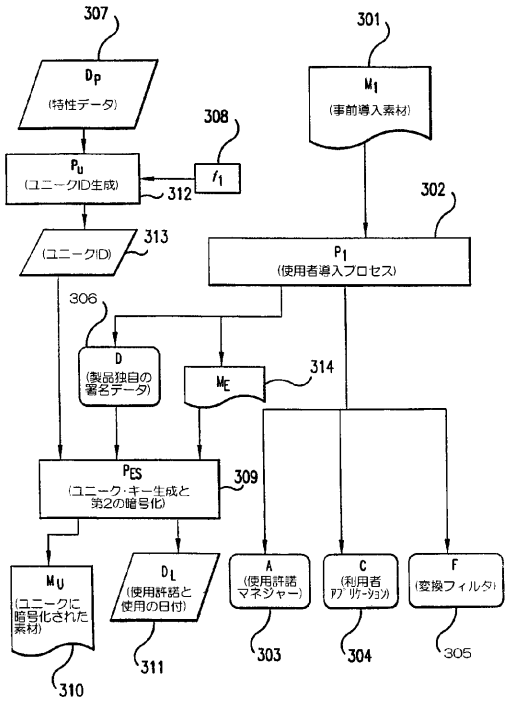

FIG.3

【図４】

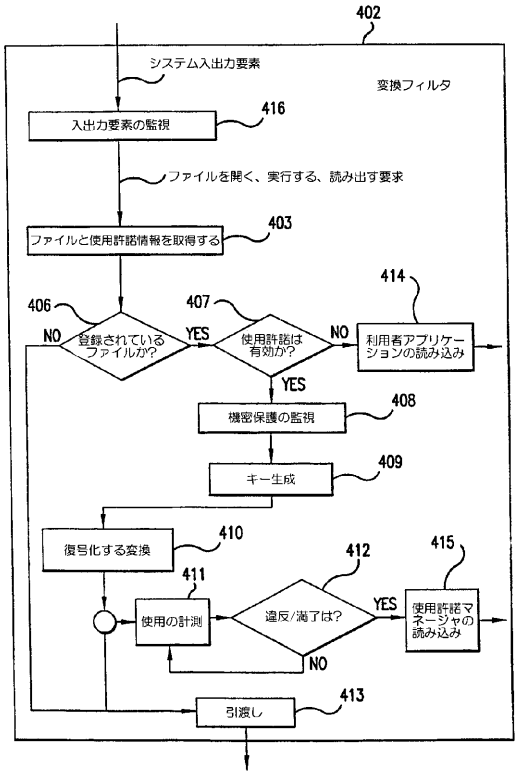

FIG.4

フロントページの続き

(51)Int.Cl. FI
H04L 9/00 671

(74)代理人 100086771
弁理士 西島 孝喜
(74)代理人 100084663
弁理士 箱田 篤
(72)発明者 イア ツェン
アメリカ合衆国 メリーランド州 ２０８７６ ジャーマンタウン ストーニー ポイント プレイス １１４２３
(72)発明者 シェン イー
アメリカ合衆国 メリーランド州 ２０８７８ ゲイザースバーグ トーリー コート ７

審査官 赤穂 州一郎

(56)参考文献 特開平０８－０１６３８４（ＪＰ，Ａ）
特開平０７－２１９７６２（ＪＰ，Ａ）
欧州特許出願公開第０７１５２４６（ＥＰ，Ａ１）
特開平０６－３４８５７６（ＪＰ，Ａ）
特開平０９－２１８８２７（ＪＰ，Ａ）
特開平０８－０４４６３２（ＪＰ，Ａ）
Matt Blaze, "A Cryptographic File System for Unix", 1st ACM Conference on Communication and Computing Security, 米国, ACM, １９９３年１１月, pp.9-16

(58)調査した分野(Int.Cl., ＤＢ名)
G06F 21/22
G06F 12/00
G06F 21/24
G09C 1/00
H04L 9/32
WPI(DIALOG)