(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2007-183696
(P2007-183696A)
(43)公開日　平成19年7月19日(2007.7.19)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/22	(2006.01)	G06F	9/06	660F	5B076
G06Q 50/00	(2006.01)	G06F	17/60	142	5B276
H04L 9/32	(2006.01)	H04L	9/00	675A	5J104

審査請求 未請求　請求項の数 9　ＯＬ　（全 14 頁）

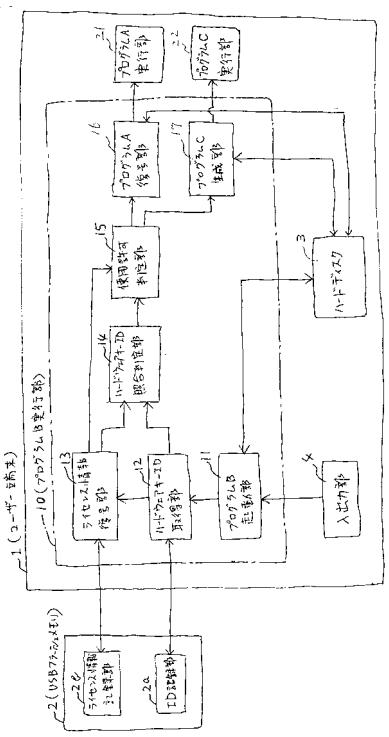
(21)出願番号　特願2005-380681 (P2005-380681)
(22)出願日　平成17年12月29日 (2005.12.29)

(71)出願人　506005097
押川　定邦
大分県別府市南立石１区５－５　第３山口コーポ４０３号　オスカークリエイション内
(71)出願人　500422528
ジュール有限会社
福岡県北九州市小倉北区金鶏町１０番２４－２０１号
(74)代理人　100094581
弁理士　鯨田　雅信
(72)発明者　押川　定邦
大分県別府市南立石１区５－５　第３山口コーポ４０３号　オスカークリエイション内

最終頁に続く

(54)【発明の名称】アプリケーションプログラム又はコンテンツのライセンスを管理するためのプログラム、方法、及び装置

(57)【要約】　（修正有）
【課題】アプリケーションプログラム又はコンテンツのライセンス管理において、低コストで、ユーザーが気楽に使用でき、市販パッケージなどのソースコードが入手できないプログラムにも適用することができ、さらに、プログラムではない音楽や映像などのコンテンツにも適用することができるようにする。
【解決手段】ユーザー端末１に内蔵又は接続されているハードウェアキーの識別情報を取得する手段１２と、前記取得したハードウェアキーの識別情報に基づいて前記暗号化されたライセンス情報を復号化する手段１３と、前記復号化されたライセンス情報の中に含まれるハードウェアキーの識別情報と前記取得したハードウェアキーの識別情報とが一致するとき、前記暗号化されたアプリケーションプログラム又はコンテンツを動的に復号化する手段１６とを備える。
【選択図】図１



【特許請求の範囲】
【請求項１】
ユーザー端末に内蔵又は接続された記録手段に、暗号化されたアプリケーションプログラム又はコンテンツを含むプログラムがインストール又は記録されており、且つ、ユーザー端末に内蔵又は接続された記録手段に、前記アプリケーションプログラム又はコンテンツの使用有効期限などの使用許可条件とユーザー端末に内蔵又は接続されるハードウェアキーの識別情報とを含むライセンス情報であって前記ハードウェアキーの識別情報により暗号化されたライセンス情報が記録されている環境下で、前記アプリケーションプログラム又はコンテンツのライセンスを管理するためのプログラムであって、
ユーザーが前記アプリケーションプログラム又はコンテンツの使用を希望するとき、ユーザー端末に内蔵又は接続されている一つ又は複数のハードウェアキーの識別情報を取得する機能と、
前記ハードウェアキーの識別情報が取得されたとき、前記取得したハードウェアキーの識別情報に基づいて前記暗号化されたライセンス情報を復号化する機能と、
前記復号化されたライセンス情報の中に含まれるハードウェアキーの識別情報と前記取得したハードウェアキーの識別情報とが一致するとき、前記暗号化されたアプリケーションプログラム又はコンテンツの中のこれから実行又は再生する部分を動的に復号化する機能と、
前記復号化されたライセンス情報の中に含まれるハードウェアキーの識別情報と前記取得したハードウェアキーの識別情報とが一致するとき、前記アプリケーションプログラム又はコンテンツのライセンス監視を行うためのライセンス監視プログラムを動的に生成する機能と、
前記ライセンス監視プログラムにより実現される機能であって、前記アプリケーションプログラム又はコンテンツが部分的に動的に実行又は再生されている場合において、前記ハードウェアキーがユーザー端末に内蔵又は接続されなくなったとき又は前記ライセンス情報中の使用許可条件が充足されなくなったとき、前記アプリケーションプログラム又はコンテンツの復号化を終了させる機能と、
を備えたことを特徴とするアプリケーションプログラム又はコンテンツのライセンスを管理するためのプログラム。
【請求項２】
請求項１において、前記ハードウェアキーは、「前記ユーザー端末に内蔵又は接続され、その識別情報が電子的に読み取り可能な複数のハードウェア」の中からユーザーが任意に選択した一つ又は複数のハードウェアである、ことを特徴とするアプリケーションプログラム又はコンテンツのライセンスを管理するためのプログラム。
【請求項３】
請求項１又は２において、前記ハードウェアキーは、固有の識別ＩＤを取得可能なＵＳＢフラッシュメモリなどのＵＳＢ機器、ハードディスク装置、ネットワークカード、又はＵＳＩＭ（ｕｎｉｖｅｒｓａｌ ｓｕｂｓｃｒｉｂｅｒ ｉｄｅｎｔｉｔｙ ｍｏｄｕｌｅ）カードであり、前記暗号化されたライセンス情報はこのハードウェアキー又はこれとは別の電子的に記録可能な記録媒体に記録されている、ことを特徴とするアプリケーションプログラム又はコンテンツのライセンスを管理するためのプログラム。
【請求項４】
ユーザー端末に内蔵又は接続された記録手段に、暗号化されたアプリケーションプログラム又はコンテンツを含むプログラムがインストール又は記録されており、且つ、ユーザー端末に内蔵又は接続された記録手段に、前記アプリケーションプログラム又はコンテンツの使用有効期限などの使用許可条件とユーザー端末に内蔵又は接続されるハードウェアキーの識別情報とを含むライセンス情報であって前記ハードウェアキーの識別情報により暗号化されたライセンス情報が記録されている環境下で、前記アプリケーションプログラム又はコンテンツのライセンスを管理するための方法であって、
ユーザーが前記アプリケーションプログラム又はコンテンツの使用を希望するとき、ユ

ーザー端末に内蔵又は接続されている一つ又は複数のハードウェアキーの識別情報を取得する第１ステップと、
前記ハードウェアキーの識別情報が取得されたとき、前記取得したハードウェアキーの識別情報に基づいて前記暗号化されたライセンス情報を復号化する第２ステップと、
前記復号化されたライセンス情報の中に含まれるハードウェアキーの識別情報と前記取得したハードウェアキーの識別情報とが一致するとき、前記暗号化されたアプリケーションプログラム又はコンテンツの中のこれから実行又は再生する部分を動的に復号化する第３ステップと、
前記第３ステップと同時に又は相前後して、前記復号化されたライセンス情報の中に含まれるハードウェアキーの識別情報と前記取得したハードウェアキーの識別情報とが一致するとき、前記アプリケーションプログラム又はコンテンツのライセンス監視を行うためのライセンス監視プログラムを動的に生成する第４ステップと、
前記アプリケーションプログラム又はコンテンツが部分的に動的に実行又は再生されている場合において、前記ハードウェアキーがユーザー端末に内蔵又は接続されなくなったとき又は前記ライセンス情報中の使用許可条件が充足されなくなったとき、前記ライセンス監視プログラムにより、前記アプリケーションプログラム又はコンテンツの復号化を終了させる第５ステップと、
を備えたことを特徴とするアプリケーションプログラム又はコンテンツのライセンスを管理するための方法。
【請求項５】
請求項４において、前記ハードウェアキーは、「前記ユーザー端末に内蔵又は接続され、その識別情報が電子的に読み取り可能な複数のハードウェア」の中からユーザーが任意に選択した一つ又は複数のハードウェアである、ことを特徴とするアプリケーションプログラム又はコンテンツのライセンスを管理するための方法。
【請求項６】
請求項４又は５において、前記ハードウェアキーは、固有の識別ＩＤを取得可能なＵＳＢフラッシュメモリなどのＵＳＢ機器、ハードディスク装置、ネットワークカード、又はＵＳＩＭ（ｕｎｉｖｅｒｓａｌ ｓｕｂｓｃｒｉｂｅｒ ｉｄｅｎｔｉｔｙ ｍｏｄｕｌｅ）カードであり、前記暗号化されたライセンス情報はこのハードウェアキー又はこれとは別の電子的に記録可能な記録媒体に記録されている、ことを特徴とするアプリケーションプログラム又はコンテンツのライセンスを管理するための方法。
【請求項７】
ユーザー端末に内蔵又は接続された記録手段に、暗号化されたアプリケーションプログラム又はコンテンツを含むプログラムがインストール又は記録されており、且つ、ユーザー端末に内蔵又は接続された記録手段に、前記アプリケーションプログラム又はコンテンツの使用有効期限などの使用許可条件とユーザー端末に内蔵又は接続されるハードウェアキーの識別情報とを含むライセンス情報であって前記ハードウェアキーの識別情報により暗号化されたライセンス情報が記録されている環境下で、前記アプリケーションプログラム又はコンテンツのライセンスを管理するためのライセンス管理装置であって、
ユーザーが前記アプリケーションプログラム又はコンテンツの使用を希望するとき、ユーザー端末に内蔵又は接続されている一つ又は複数のハードウェアキーの識別情報を取得するためのハードウェアキーＩＤ取得手段と、
前記ハードウェアキーの識別情報が取得されたとき、前記取得したハードウェアキーの識別情報に基づいて前記暗号化されたライセンス情報を復号化するためのライセンス情報復号化手段と、
前記復号化されたライセンス情報の中に含まれるハードウェアキーの識別情報と前記取得したハードウェアキーの識別情報とが一致するとき、前記暗号化されたアプリケーションプログラム又はコンテンツの中のこれから実行又は再生する部分を動的に復号化するためのハードウェアキーＩＤ一致判定手段と、
前記復号化されたライセンス情報の中に含まれるハードウェアキーの識別情報と前記取

得したハードウェアキーの識別情報とが一致するとき、前記アプリケーションプログラム又はコンテンツのライセンス監視を行うためのライセンス監視プログラムを動的に生成するためのライセンス監視プログラム生成手段と、
前記ライセンス監視プログラムにより実現されるライセンス監視手段であって、前記アプリケーションプログラム又はコンテンツが部分的に動的に実行又は再生されている場合において、前記ハードウェアキーがユーザー端末に内蔵又は接続されなくなったとき又は前記ライセンス情報中の使用許可条件が充足されなくなったとき、前記アプリケーションプログラム又はコンテンツの復号化を終了させるためのライセンス監視手段と、
を備えたことを特徴とするアプリケーションプログラム又はコンテンツのライセンスを管理するためのライセンス管理装置。
【請求項８】
請求項７において、前記ハードウェアキーは、「前記ユーザー端末に内蔵又は接続され、その識別情報が電子的に読み取り可能な複数のハードウェア」の中からユーザーが任意に選択した一つ又は複数のハードウェアである、ことを特徴とするアプリケーションプログラム又はコンテンツのライセンスを管理するためのライセンス管理装置。
【請求項９】
請求項７又は８において、前記ハードウェアキーは、固有の識別ＩＤを取得可能なＵＳＢフラッシュメモリなどのＵＳＢ機器、ハードディスク装置、ネットワークカード、又はＵＳＩＭ（ｕｎｉｖｅｒｓａｌ ｓｕｂｓｃｒｉｂｅｒ ｉｄｅｎｔｉｔｙ ｍｏｄｕｌｅ）カードであり、前記暗号化されたライセンス情報はこのハードウェアキー又はこれとは別の電子的に記録可能な記録媒体に記録されている、ことを特徴とするアプリケーションプログラム又はコンテンツのライセンスを管理するためのライセンス管理装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、アプリケーションプログラム又はコンテンツのライセンスを管理するためのプログラム、方法、及び装置に関する。
【背景技術】
【０００２】
従来より、アプリケーションプログラム又はコンテンツのライセンス範囲外の不正使用を防止するために様々な方策が提案されている。例えば、特許文献１は、所定のキー情報を記録した特殊なハードウェアキーをアプリケーションプログラムと共にユーザー側に配布しておき、ユーザーがアプリケーションプログラムの使用を希望するときは、ユーザー側から前記ハードウェアキーのキー情報をホストコンピュータ側にネットワーク経由で送信し、前記ホストコンピュータ側で必要な照合・判定を行った後に起動許可情報をユーザー側に送信するという方式を提案している。
【０００３】
また、ライセンスチェック（暗号解除）用のＡＰＩ（アプリケーション・プログラム・インターフェース）をプログラムのソースコードに埋め込む（ハードウェアキーも使用する）ことにより、ライセンス管理を可能にしたＦｌｅｘＬＭという方式も一部で実用化されている。
【特許文献１】特開２００２－３１２０５１号公報
【発明の開示】
【発明が解決しようとする課題】
【０００４】
前記特許文献１の方式は、いちいち専用の特殊なハードウェアキーを配布する必要があるのでコスト高になってしまう、専用のデバイスドライバをインストールする必要がありまた使用時にはホストコンピュータにキー情報を送信する必要があるのでユーザーにとって極めて煩雑である、専用のハードウェアキーは記憶容量が比較的小さいため柔軟なライセンス管理が難しい、などの問題がある。

【０００５】
また、前記ＦｌｅｘＬＭは、プログラムのソースコードにライセンスチェック（暗号解除）用のＡＰＩ（アプリケーション・プログラム・インターフェース）を直接埋め込む必要があるため、ソースコードの設計段階からプロテクトを意識した設計が必要になる、市販パッケージなどのソースコードが入手できないプログラムには適用できない、プログラムではない音楽や映像などのコンテンツには（ＡＰＩを埋め込むことができないので）適用できない、などの問題がある。
【０００６】
本発明はこのような従来技術の問題点に着目してなされたものであって、ライセンス管理のためのコストを最小にすることができ、ユーザーに煩雑な作業を要求する必要がなく、記憶容量が比較的大きいハードウェアキーを使用できるため柔軟なライセンスモデルの構築を可能にし、ソースコードの設計段階からプロテクトを意識した設計を不要にでき、市販パッケージなどのソースコードが入手できないプログラムにも適用することができ、さらに、プログラムではない音楽や映像などのコンテンツにも適用することができる、アプリケーションプログラム又はコンテンツのライセンスを管理するためのプログラム、方法、又は装置を提供することを目的とする。
【課題を解決するための手段】
【０００７】
以上のような課題を解決するための本発明は、ユーザー端末に内蔵又は接続された記録手段に、暗号化されたアプリケーションプログラム又はコンテンツを含む（カプセル化・エンベロープ化した）プログラムがインストール又は記録されており、且つ、ユーザー端末に内蔵又は接続された記録手段（後述のハードウェアキーでもよい）に、前記アプリケーションプログラム又はコンテンツの使用有効期限などの使用許可条件とハードウェアキー（ユーザー端末に内蔵又は接続され、その識別情報が電子的に読み取り可能な一つ又は複数のハードウェアから成る）の識別情報とを含むライセンス情報であって前記ハードウェアキーの識別情報により暗号化されたライセンス情報が記録されている環境下で、前記アプリケーションプログラム又はコンテンツのライセンスを管理するためのプログラム、方法、又は装置であって、ユーザー端末に内蔵又は接続されている一つ又は複数のハードウェアキーの識別情報を取得する機能（ステップ、又は手段）と、前記取得したハードウェアキーの識別情報に基づいて前記暗号化されたライセンス情報を復号化する機能（ステップ、又は手段）と、前記復号化されたライセンス情報の中に含まれるハードウェアキーの識別情報と前記取得したハードウェアキーの識別情報とが一致するとき、前記暗号化されたアプリケーションプログラム又はコンテンツの中のこれから実行又は再生する部分を動的に復号化する機能（ステップ、又は手段）と、前記復号化されたライセンス情報の中に含まれるハードウェアキーの識別情報と前記取得したハードウェアキーの識別情報とが一致するとき、前記アプリケーションプログラム又はコンテンツのライセンス監視を行うためのライセンス監視プログラムを動的に生成する機能（ステップ、又は手段）と、前記ライセンス監視プログラムにより実現される機能（ステップ、又は手段）であって、前記ハードウェアキーがユーザー端末に内蔵又は接続されなくなったとき又は前記ライセンス情報中の使用許可条件が充足されなくなったとき前記アプリケーションプログラム又はコンテンツの復号化を終了させる機能（ステップ、又は手段）と、を備えたことを特徴とするものである。
【０００８】
また、本発明によるアプリケーションプログラム又はコンテンツのライセンスを管理するためのプログラム、方法、又は装置においては、前記ハードウェアキーは、「前記ユーザー端末に内蔵又は接続され、その識別情報が電子的に読み取り可能な複数のハードウェア」の中からユーザーが任意に選択した一つ又は複数のハードウェアである、ことが望ましい。
【０００９】
また、本発明によるアプリケーションプログラム又はコンテンツのライセンスを管理す

るためのプログラム、方法、又は装置においては、前記ハードウェアキーは、固有の識別ＩＤを取得可能なＵＳＢフラッシュメモリなどのＵＳＢ機器、ハードディスク装置、ネットワークカード、又はＵＳＩＭ（ｕｎｉｖｅｒｓａｌ ｓｕｂｓｃｒｉｂｅｒ ｉｄｅｎｔｉｔｙ ｍｏｄｕｌｅ）カードであり、前記暗号化されたライセンス情報はこのハードウェアキーとしてのＵＳＢフラッシュメモリ又はこれとは別の電子的に記録可能な記録媒体の中に記録されている、ことが望ましい。

【発明の効果】

【００１０】

本発明によるアプリケーションプログラム又はコンテンツのライセンスを管理するためのプログラム、方法、又は装置においては、ユーザー端末に内蔵されているハードディスクやユーザー端末に接続されているＵＳＢフラッシュメモリ、ネットワークカード、ＵＳＢのＩＤが取得可能なマウスやプリンタなどのように、ユーザー端末に日常的に内蔵又は接続されている市販の機器をハードウェアキーとしている。よって、本発明によれば、従来のように専用の特殊なハードウェアをハードウェアキーとする場合と異なって、ライセンス管理のために特別なコストや専用のデバイスドライバをインストールする手間などは必要なく、低コストで手軽なライセンス管理が可能である。また、本発明では、前述のようにハードディスクやＵＳＢフラッシュメモリなどの記憶容量が比較的大きい機器をハードウェアキーとして使用できるので柔軟なライセンスモデルを構築できるようになる。

【００１１】

また、本発明によるアプリケーションプログラム又はコンテンツのライセンスを管理するためのプログラム、方法、又は装置においては、ユーザーが前記アプリケーションプログラム又はコンテンツの使用を希望するとき（例えばユーザーが前記アプリケーションプログラム又はコンテンツを含む（カプセル化・エンベロープ化した）プログラムをマウスでダブルクリックしたとき）、前記ハードウェアキーの識別情報を自動的に取得するようにして、この識別情報から前記アプリケーションプログラム又はコンテンツのライセンスチェック（暗号解除）やライセンス監視を自動的に行うようにしている。よって、本発明によれば、ソフトウェアベンダーは、ユーザーに煩雑さを感じさせることなく手軽なライセンス管理を行うことができる。

【００１２】

また、本発明によるアプリケーションプログラム又はコンテンツのライセンスを管理するためのプログラム、方法、又は装置においては、アプリケーションプログラム又はコンテンツそのものを暗号化しておき、前記アプリケーションプログラム又はコンテンツとは別のプログラムでライセンスチェック（暗号解除）やライセンス監視を行うようにしているので、前記アプリケーションプログラム又はコンテンツそれ自体の中にライセンスチェック（暗号解除）用のＡＰＩを埋め込む必要がない。よって、本発明によれば、前記アプリケーションプログラムのソースコードの設計段階ではプロテクトを意識して設計する必要がない。また、本発明によるライセンス管理は、ソースコードが入手できない市販のアプリケーションプログラムやプログラムではないコンテンツに対しても、プロテクトのために適用することができる。

【発明を実施するための最良の形態】

【００１３】

本発明を実施するための最良の形態は、以下の実施例１について述べるような形態である。

【実施例１】

【００１４】

以下、本発明の実施例１によるアプリケーションプログラム又はコンテンツのライセンスを管理するためのプログラム、方法、及び装置を説明する。なお、以下では、可逆暗号変換前のアプリケーションプログラム又はコンテンツを「プログラムＡ」、前記アプリケーションプログラム又はコンテンツを可逆暗号変換したものをカプセル化・エンベロープ化したプログラム（ベンダーがユーザーに提供するもの）を「プログラムＢ」、プログラ

ムＢの中に含まれているプログラムＡのライセンス監視をするプログラムを「プログラムＣ」と呼ぶ。また、「コンテンツ」とは、映像や音楽などから構成される映画、番組、ゲーム、その他の映像ソフト、音楽ソフトなどの情報の内容をいう。

【００１５】

また、本実施例１において、前記のプログラムＡは、プログラムＢを生成するときに使用するオリジナル（暗号化前のプログラム）である。本実施例１では、後述するように、プログラムＢを実行すると、プログラムＡとプログラムＣが復号化・生成される。プログラムＡとプログラムＣは、プログラムＢ内に暗号化されて格納（エンベロープ化・カプセル化）され、全体が１つのソフトウェアとしてパッケージングされている。

【００１６】

図１は本実施例１によるアプリケーションプログラム又はコンテンツのライセンス管理装置を示す概念ブロック図、図２は暗号化されたアプリケーションプログラム又はコンテンツをライセンス付きでユーザー側に配布するベンダー側のサーバー（ライセンス発行サーバー及びソフトウェア提供サーバー）の動作を示すフローチャート、図３はユーザー端末側で暗号化されたアプリケーションプログラム又はコンテンツを復号して利用するときの動作を示すフローチャート、である。

【００１７】

図１において、１はユーザーが保有するパソコン、ＰＤＡ（携帯型情報端末）、携帯電話などのユーザー端末、２はこのユーザー端末１に接続されるＵＳＢフラッシュメモリ（本実施例１ではこれがハードウェアキーとなっている）、３は前記ユーザー端末１に内蔵されるハードディスク、４は前記ユーザー端末に備えられているキーボードやディスプレイなどから成る入出力部、である。

【００１８】

また、図１において、１１はユーザーからの所定の入力操作に基づいてプログラムＢを起動するためのプログラムＢ起動部、１２は前記プログラムＢ起動部１１からの信号に基づいて前記ＵＳＢフラッシュメモリ（ハードウェアキー）２のＩＤを前記ＵＳＢフラッシュメモリ２のＩＤ記録部２ａから読み取るためのハードウェアキーＩＤ取得部、１３は前記ハードウェアキーＩＤ取得部１２からのハードウェアキーＩＤに基づいて前記ＵＳＢフラッシュメモリ（ハードウェアキー）２のライセンス情報記録部２ｂに記録されている暗号化されたライセンス情報を復号化するためのライセンス情報復号部、である。

【００１９】

また、図１において、１４は、前記ライセンス情報復号部１３からの前記復号化されたライセンス情報の中に含まれているハードウェアキーＩＤと、前記ハードウェアキーＩＤ取得部１２からのユーザー端末１に現在内蔵又は接続されているハードウェアキーのＩＤとを照合して両者が一致するかどうかを判定するためのハードウェアキーＩＤ照合判定部、である。前記ハードウェアキーＩＤ照合判定部１４は、前記照合の結果、前記両ＩＤが一致しないときは、そのことを警告表示して、プログラムＢに含まれるプログラムＡの復号化を不可とする。また、前記ハードウェアキーＩＤ照合判定部１４は、前記照合の結果、前記両ＩＤが一致するときは、そのことを示す信号を次の使用許可判定部１５に出力する。

【００２０】

また、図１において、１５は、前記ハードウェアキーＩＤ照合判定部１４から前記両ＩＤが一致することを示す信号を受信したとき、前記ライセンス情報復号部１３からの復号化されたライセンス情報中の使用有効期限などの使用許可条件の情報を受信し、プログラムＢがこの使用有効期限などの使用許可条件（逆変換の条件）を満たしているかどうかを判定するための使用許可判定部である。

【００２１】

また、図１において、１６は前記使用許可判定部１５によりプログラムＢが使用許可条件を満たしていると判定されたときにそれを示す信号を受けてプログラムＡの実行に必要な部分（プログラムＡがコンテンツの場合はその再生に必要な部分）を部分的に復号化す

るためのプログラムＡ復号部、１７は前記使用許可判定部１５によりプログラムＢが使用許可条件を満たしていると判定されたときにそれを示す信号を受けてプログラムＣを動的に生成するためのプログラムＣ生成部、である。

【００２２】

以上に説明した符号１１～１７で示す部分により、プログラムＢ実行部１０が構成されている。このプログラムＢ実行部１０は、実際には、プログラムＢとこれを実行するためのＣＰＵやメモリなどにより実現されている。

【００２３】

また、図１において、２１は前記プログラムＡ復号部１６により部分的に復号化されたプログラムＡを実行するためのプログラムＡ実行部で、復号化されたプログラムＡとこれを実行するためのＣＰＵやメモリなどにより実現されている。

【００２４】

また、図１において、２２は前記プログラムＣ生成部１７により動的に生成されたプログラムＣを実行するためのプログラムＣ実行部で、動的に生成されたプログラムＣとこれを実行するためのＣＰＵやメモリなどにより実現されている。前記プログラムＣは、前記プログラムＡ実行部２１により実行されるプログラムＡのライセンス監視を行うためのもので、ユーザー端末１からハードウェアキー（ＵＳＢフラッシュメモリ）２が取り外されたり、ライセンスの使用有効期限が終了した場合は、そのことを検知して直ちにプログラムＡを終了させ、その後プログラムＣも直ちに終了する。

【００２５】

次に、図２を参照してベンダー側のライセンス発行サーバー（ソフトウェア提供サーバーを兼ねる）及びユーザー端末の動作を説明する。

【００２６】

ユーザー側からプログラムＡの送信要求が送信されると（ステップＳ１）、ベンダー側は、ハードウェアキーは指定せずにプログラムＢのみをインターネット経由でユーザー側にダウンロードさせる（プログラムＢの出荷段階。ステップＳ２、Ｓ３）。

【００２７】

その後、ユーザー端末側で前記ダウンロードしたプログラムＢをインストールするときは（ステップＳ４）、前記プログラムＢのインストーラが、ユーザー端末に内蔵又は接続されており固有の製品番号やＭＡＣアドレスなどのＩＤが電子的に読み取り可能なハードウェア機器、例えば内蔵のハードディスク３、外付けのＵＳＢフラッシュメモリ２（図１参照）、ネットワークカード、ＵＳＢのＩＤを有しているプリンタやマウスなどのハードウェア機器を、検出する（ステップＳ５）。例えば、図１において、ＵＳＢフラッシュメモリ２やハードディスク３などは、固有の製品番号などのＩＤが電子的に読み取り可能であるから、前記プログラムＢのインストーラにより検出される。

【００２８】

次に、前記プログラムＢのインストーラは、前述のように各ＩＤが電子的に読み取り可能な複数の機器を画面に一覧表示し、ユーザーに対して、この一覧表示された複数の機器の中からプログラムＢの復号のためのハードウェアキーとすべきもの（一つ又は複数）を任意に選択するように促す（ステップＳ６）。この画面上で、ユーザーが例えばＵＳＢフラッシュメモリ２をハードウェアキーとして選択すると、前記プログラムＢのインストーラは、この選択されたＵＳＢフラッシュメモリのＩＤを読み取り、これをハードウェアキーＩＤとしてベンダー側に送信する（ステップＳ７）。

【００２９】

ベンダー側では、この送信されてきたハードウェアキーＩＤ（ＵＳＢフラッシュメモリ２のＩＤ）を使用して、このハードウェアキーＩＤとプログラムＡの使用許可条件などを含むライセンス情報を生成し、これを暗号化する（ステップＳ８）。ベンダー側は、この暗号化したライセンス情報をユーザー端末１に送信する（ステップＳ９）。

【００３０】

ユーザー端末１では、前記プログラムＢのインストーラが、このベンダー側から送信さ

れてきた暗号化されたライセンス情報をＵＳＢフラッシュメモリ２（ハードウェアキー）の中のライセンス情報記録部２ｂに記録して、前記プログラムＢのインストールを終了する（ステップＳ１０）。

【００３１】

次に、図３を参照して、ユーザー側で、前記プログラムＢを起動して、ライセンスチェックを行って、暗号化されたプログラムＡを復号化し、この復号化したプログラムＡを実行又は再生するときの動作を説明する。

【００３２】

まず、ユーザーがプログラムＢを起動すると（ステップＳ２１）、プログラムＢ起動部１１（図１参照）からの信号に基づいて、ハードウェアキーＩＤ取得部１２が、ユーザー端末１に接続又は内蔵されているハードウェアキー（本実施例１ではＵＳＢフラッシュメモリ２）のＩＤを取得する（ステップＳ２２）。その後、前記ライセンス情報復号部１３が、前記ハードウェアキーＩＤ取得部１２が取得したハードウェアキーＩＤに基づいて、前記ＵＳＢフラッシュメモリ２に記録されたライセンス情報を復号化する（ステップＳ２３）。

【００３３】

次に、前記ハードウェアキーＩＤ照合判定部１４が、前記ハードウェアキーＩＤ取得部１２により取得されたハードウェアキーＩＤと、前記ライセンス情報復号部１３により復号化されたライセンス情報に含まれるハードウェアキーＩＤとが、互いに一致するかどうかを照合・判定する（ステップＳ２４）。

【００３４】

前記ステップＳ２４で前記両ＩＤが一致していないと判定されたときは、プログラムＡの復号化を不可とし、処理を終了する（ステップＳ２５）。他方、前記ステップＳ２４で前記両ＩＤが一致していると判定されたときは、ステップＳ２６に進み、前記使用許可判定部１５が、前記復号化されたライセンス情報に含まれる使用許可条件をプログラムＢ（この中に含まれるプログラムＡ）が満たしているかどうかを判定する。

【００３５】

前記ステップＳ２６で前記使用許可条件を満たしていないと判定されたときは、プログラムＡの復号化を不可とし、処理を終了する（ステップＳ２５）。他方、前記ステップＳ２６で前記使用許可条件を満たしていると判定されたときは、ステップＳ２７に進み、前記プログラムＡ復号部１６によりプログラムＡの実行（又は再生）に必要な部分を動的に復号化し、前記プログラムＡ実行部２１により実行（又は再生）する。さらに、ステップＳ２８に進み、前記プログラムＣ生成部１７によりプログラムＣを動的に生成し、前記プログラムＣ実行部２２により実行する。

【００３６】

前記プログラムＣは、プログラムＡが動的に実行されているとき、そのライセンス監視をするプログラムである。前記プログラムＣは、ユーザー端末１からハードウェアキーの接続又は内蔵が無くなったとき又はプログラムＡのライセンスの使用有効期限が終了したとき、プログラムＡを直ちに終了させ、プログラムＣも直ちに終了する。

【００３７】

以上、本発明の各実施例について説明したが、本発明及び本発明を構成する各構成要件は、それぞれ、前記の各実施例及び前記の各実施例を構成する各要素として述べたものに限定されるものではなく、様々な修正及び変更が可能である。例えば、前記の実施例１においては、ユーザー端末１に外付けされたＵＳＢフラッシュメモリ２をハードウェアキーとしているが、本発明ではこれに限られるものではなく、様々な機器をハードウェアキーとして使用することができる。例えば、マウスやプリンタなどでも、ＵＳＢフラッシュメモリなどと同様にＵＳＢのＩＤを取得可能な機器であれば、ハードウェアキーとして使用できる。また、ハードディスクなどの固有の製品番号を電子的に保有している機器、ネットワークカードなどのＭＡＣアドレスを電子的に保有している機器も、ハードウェアキーとして使用できる。また、例えば株式会社ＮＴＴドコモが３Ｇ携帯電話用に提供している

「ＦＯＭＡカード」（商品名）を初めとする「ＵＳＩＭ（ｕｎｉｖｅｒｓａｌ ｓｕｂｓｃｒｉｂｅｒ ｉｄｅｎｔｉｔｙ ｍｏｄｕｌｅ）カード」のような、契約者・加入者情報を電子的に記録して契約者・加入者を電子的に特定できる機器も、ハードウェアキーとして使用できる。

【００３８】

また、前記の実施例１では、ハードウェアキーＩＤと使用許可条件とを含む暗号化されたライセンス情報を、ハードウェアキーの中に記録するようにしているが、本発明では、前記暗号化されたライセンス情報はハードウェアキー以外の他の記録手段（ユーザー端末１に内蔵又は接続されている他の記録手段）の中に記録するようにしてもよい。例えば、上記のＵＳＢのＩＤを取得可能なマウスやプリンタの場合は、他の記録可能な媒体（ハードディスク、ＵＳＢフラッシュメリ、ＣＤ－Ｒなど）に、前記暗号化されたライセンス情報を記録する。

【００３９】

また、前記の実施例１においては、ユーザー側にライセンスを発行する方法として、ユーザー側からオンラインでハードウェアキーＩＤをサーバー側に送信させてそれを基にライセンス情報を生成・暗号化してユーザー側に送信するという方式（ユーザーによるオンライン・アクティベーション方式）を説明したが、本発明ではこの方式に限定されるものではなく、他の方式も可能である。例えば、ベンダー側からのソフトウェアの出荷段階で使用可能なハードウェアキーに対してライセンスを発行してソフトウェアに添付するという従来のセキュリティ製品におけると同様の方式（ベンダーによるハードウェアキーのアクティベーション方式）、ユーザーが指定したハードウェアキーの情報をベンダー側にメールやＦＡＸで送信してもらい、ベンダー側でその情報に基づいてライセンスの自動設定プログラムを生成し、これをユーザー側にメールや郵送などの方法で送付する方式（センドバックによるアクティベーション方式）などの様々な方式を採用することができる。

【図面の簡単な説明】

【００４０】

【図１】本発明の実施例１によるアプリケーションプログラム又はコンテンツのライセンス管理装置の動作原理を示す概念ブロック図。

【図２】本実施例１におけるユーザー側に暗号化されたアプリケーションプログラム又はコンテンツをライセンス付きで配布するためのベンダー側（ライセンス発行サーバー及びソフトウェア提供サーバー）の動作を示すフローチャート。

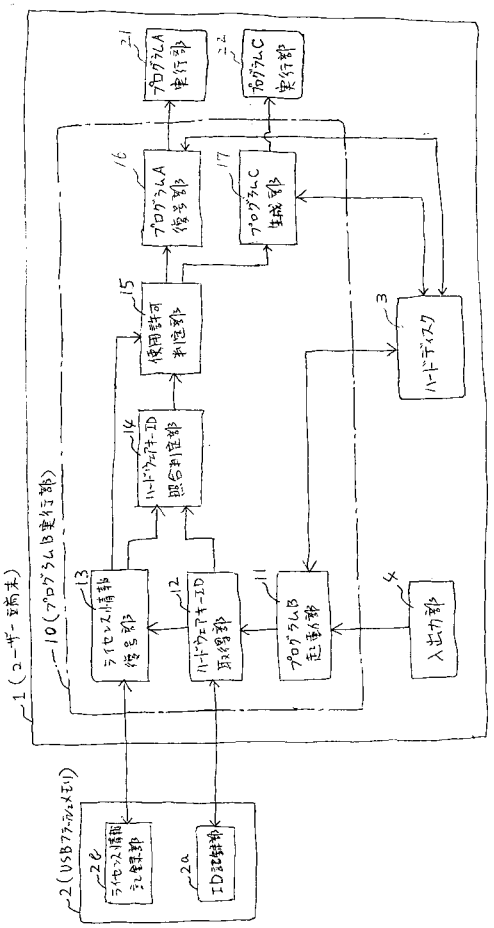
【図３】本実施例１におけるユーザー端末側で暗号化されたアプリケーションプログラム又はコンテンツを復号して利用するときの動作を示すフローチャート。

【符号の説明】

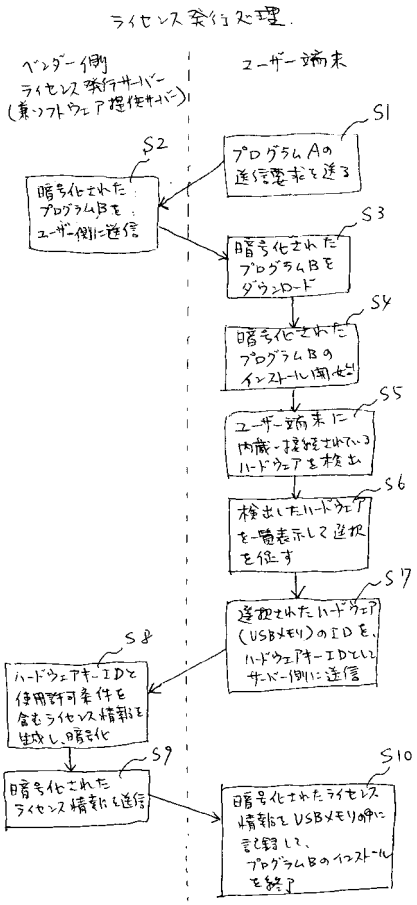
【００４１】

１　ユーザー端末
２　ＵＳＢフラッシュメモリ
２ａ　ハードウェアキーＩＤ記録部
２ｂ　ライセンス情報記録部
３　ハードディスク
１０　プログラムＢ実行部
１１　プログラムＢ起動部
１２　ハードウェアキーＩＤ取得部
１３　ライセンス情報復号部
１４　ハードウェアキーＩＤ照合判定部
１５　使用許可判定部
１６　プログラムＡ復号部
１７　プログラムＣ生成部
２１　プログラムＡ実行部
２２　プログラムＣ実行部

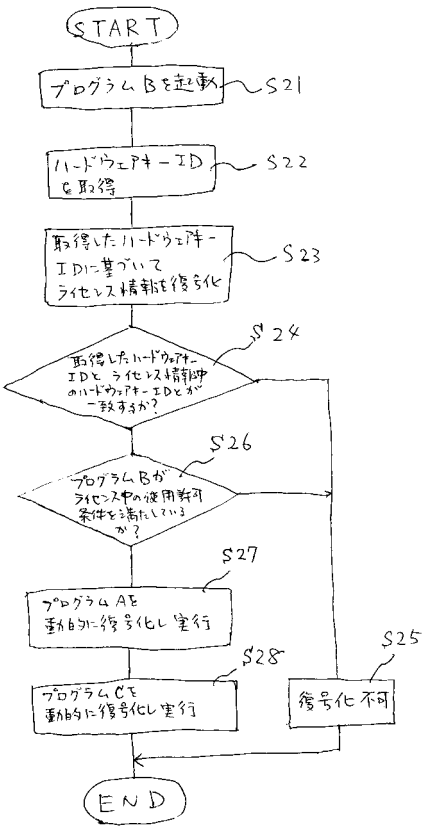
【図１】


プログラムA実行部
プログラムC実行部
プログラムA復号部
プログラムC生成部
使用許可判定部
ハードディスク
ハードウェアキーID照合判定部
ライセンス情報復号部
ハードウェアキーID取得部
プログラムB起動部
入出力部
1（ユーザー端末）
10（プログラムB実行部）
2（USBフラッシュメモリ）
ライセンス情報記録部
IDE録部

【図２】

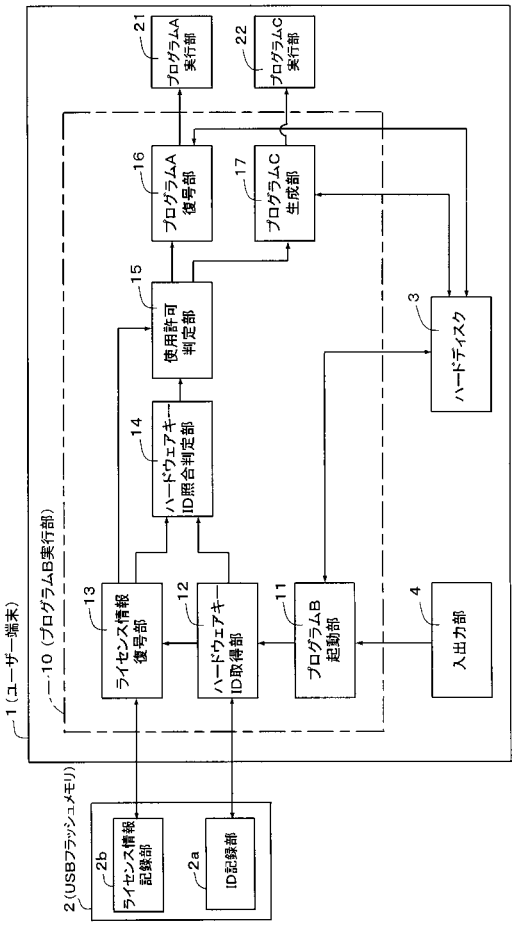

ライセンス発行処理
ベンダー側
ライセンス発行サーバー
（兼ソフトウェア提供サーバー）
ユーザー端末
S1
プログラムAの送信要求を送る
S2
暗号化されたプログラムBをユーザー側に送信
S3
暗号化されたプログラムBをダウンロード
S4
暗号化されたプログラムBのインストール開始
S5
ユーザー端末に内蔵・接続されているハードウェアを検出
S6
検出したハードウェアを一覧表示して選択を促す
S7
選択されたハードウェア（USBメモリ）のIDを、ハードウェアキーIDとしてサーバー側に送信
S8
ハードウェアキーIDと使用許可条件を含むライセンス情報を生成し暗号化
S9
暗号化されたライセンス情報を送信
S10
暗号化されたライセンス情報をUSBメモリの中に記録して、プログラムBのインストールを終了

【図３】

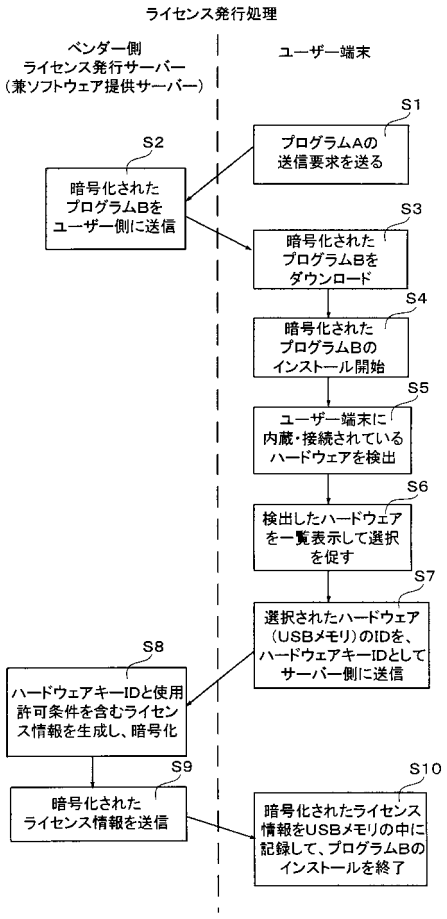

START
プログラムBを起動
S21
ハードウェアキーIDを取得
S22
取得したハードウェアキーIDに基づいてライセンス情報を復号化
S23
取得したハードウェアキーIDとライセンス情報中のハードウェアキーIDとが一致するか？
S24
プログラムBがライセンス中の使用許可条件を満たしているか？
S26
プログラムAを動的に復号化し実行
S27
プログラムCを動的に復号化し実行
S28
復号化不可
S25
END

【手続補正書】
【提出日】平成18年1月10日(2006.1.10)
【手続補正１】
【補正対象書類名】図面
【補正対象項目名】全図
【補正方法】変更
【補正の内容】

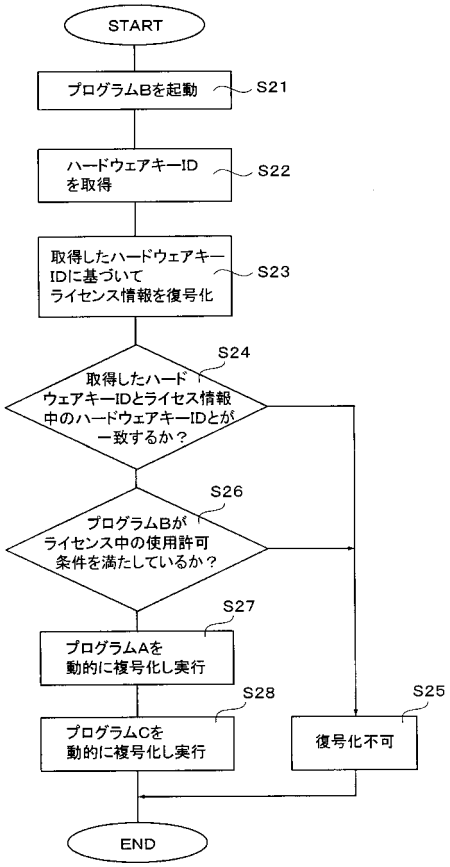
【図１】



【図２】



【図３】


START
プログラムBを起動
S21
ハードウェアキーID
を取得
S22
取得したハードウェアキー
IDに基づいて
ライセンス情報を復号化
S23
S24
取得したハード
ウェアキーIDとライセス情報
中のハードウェアキーIDとが
一致するか？
S26
プログラムBが
ライセンス中の使用許可
条件を満たしているか？
S27
プログラムAを
動的に複号化し実行
S28
プログラムCを
動的に複号化し実行
S25
復号化不可
END

フロントページの続き

(72)発明者　興梠　卓也
福岡県北九州市小倉北区金鶏町１０－２４－２０１　ジュール有限会社内

Ｆターム(参考) 5B076 FB09
5B276 FB09
5J104 KA02 PA07 PA14