(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5572112号
(P5572112)
(45)発行日　平成26年8月13日(2014.8.13)　(24)登録日　平成26年7月4日(2014.7.4)

(51)Int.Cl.　F I
G06F 21/10 (2013.01)　G06F 21/22 110J
G06F 21/22 110F

請求項の数 9　(全 15 頁)

(21)出願番号　特願2011-38388(P2011-38388)
(22)出願日　平成23年2月24日(2011.2.24)
(65)公開番号　特開2012-174189(P2012-174189A)
(43)公開日　平成24年9月10日(2012.9.10)
審査請求日　平成25年8月22日(2013.8.22)

(73)特許権者　000208891
ＫＤＤＩ株式会社
東京都新宿区西新宿二丁目３番２号
(74)代理人　100106002
弁理士　正林　真之
(74)代理人　100120891
弁理士　林　一好
(72)発明者　稲村　勝樹
埼玉県ふじみ野市大原二丁目１番１５号
株式会社ＫＤＤＩ研究所内
(72)発明者　田中　俊昭
埼玉県ふじみ野市大原二丁目１番１５号
株式会社ＫＤＤＩ研究所内

審査官　中里　裕正

最終頁に続く

(54)【発明の名称】ライセンス移譲装置、ライセンス移譲システム及びライセンス移譲方法

(57)【特許請求の範囲】
【請求項１】
サービスを利用するためのライセンス情報を移譲するライセンス移譲装置であって、
所定のライセンス管理装置に対して、自装置の識別子を含む暗号データを伴って、移譲ライセンスの発行許可要求を行う要求部と、
前記発行許可要求に応じて前記ライセンス管理装置により発行された署名情報を受信する受信部と、
前記発行された署名情報を検証し、少なくとも当該署名情報及び前記サービスの利用可能な有効回数を含む前記移譲ライセンスを生成する生成部と、
前記生成部により生成された前記移譲ライセンスを、外部端末へ送信する第１の送信部と、を備えるライセンス移譲装置。
【請求項２】
前記生成部は、前記移譲ライセンスに含める情報を保証するための鍵付きメッセージ認証コードをさらに連接して当該移譲ライセンスを生成する請求項１に記載のライセンス移譲装置。
【請求項３】
前記要求部は、前記発行許可要求の度に新たにシリアル番号を生成し、前記暗号データに当該シリアル番号を含め、
前記署名情報は、前記シリアル番号を含んで発行される請求項１又は請求項２に記載のライセンス移譲装置。

【請求項４】
前記生成部は、前記シリアル番号に対応して前記サービスを利用した支払総回数をさらに含んで前記移譲ライセンスを生成する請求項３に記載のライセンス移譲装置。
【請求項５】
請求項４に記載のライセンス移譲装置と、前記ライセンス管理装置と、前記外部端末と、を有するライセンス移譲システムであって、
前記外部端末は、前記ライセンス移譲装置から受信した前記移譲ライセンスを記憶する第１の記憶部と、
前記サービスを利用する際には、前記第１の記憶部に記憶されている前記移譲ライセンスに含まれる前記有効回数を減じて更新する更新部と、
前記シリアル番号と当該シリアル番号に対応する前記支払総回数との組を記憶する第２の記憶部と、を備えるライセンス移譲システム。
【請求項６】
請求項４に記載のライセンス移譲装置と、前記ライセンス管理装置と、前記外部端末と、前記サービスの利用機器と、を有するライセンス移譲システムであって、
前記外部端末は、
前記ライセンス移譲装置から移譲された前記移譲ライセンスを記憶する第１の記憶部と、
前記利用機器からの要求に応じて、前記第１の記憶部に記憶されている前記移譲ライセンスを前記利用機器へ送信する第２の送信部と、
前記利用機器により支払処理された移譲ライセンスを受信し、前記第１の記憶部に記憶されている前記移譲ライセンスを更新する更新部と、を備え、
前記利用機器は、
前記サービスを利用する際に、前記ライセンス移譲装置から受信した前記移譲ライセンスに含まれる前記有効回数を減じて支払処理し、当該支払処理後の移譲ライセンスを前記外部端末へ送信する支払部と、
前記シリアル番号と当該シリアル番号に対応する前記支払総回数との組を記憶する第２の記憶部と、を備えるライセンス移譲システム。
【請求項７】
前記ライセンス管理装置は、
前記第２の記憶部に記憶されている前記シリアル番号と前記支払総回数との組を回収する回収部と、
前記回収部により回収された組データの正当性を確認する確認部と、を備える請求項５又は請求項６に記載のライセンス移譲システム。
【請求項８】
前記第２の記憶部は、前記サービスの識別データと、当該サービスの利用回数との組をさらに記憶し、
前記回収部は、前記第２の記憶部に記憶されている前記識別データと前記利用回数との組をさらに回収する請求項７に記載のライセンス移譲システム。
【請求項９】
ライセンス移譲装置がサービスを利用するためのライセンス情報を移譲するライセンス移譲方法であって、
所定のライセンス管理装置に対して、自装置の識別子を含む暗号データを伴って、移譲ライセンスの発行許可要求を行う要求ステップと、
前記発行許可要求に応じて前記ライセンス管理装置により発行された署名情報を受信する受信ステップと、
前記発行された署名情報を検証し、少なくとも当該署名情報及び前記サービスの利用可能な有効回数を含む前記移譲ライセンスを生成する生成ステップと、
前記生成ステップにおいて生成された前記移譲ライセンスを、外部端末へ送信する送信ステップと、を含むライセンス移譲方法。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、サービスを利用するためのライセンス情報を移譲する装置、システム及び方法に関する。
【背景技術】
【０００２】
従来、コンピュータの利用形態として、サーバ又はサーバ群（クラウド）によりサービスの提供を行い、ユーザは、自分のコンピュータに専用のソフトウェアをインストールしなくても、ライセンス認証によりそのサービスを受けることができる方式が運用されている。また、コンテンツ提供サービスにおいては、テレビ放送等のメディアがデジタル化されたことに伴い、ユーザにライセンスを発行し、コンテンツ利用時にライセンス認証を行うことで安全にコンテンツを提供するシステムが運用されている。
【０００３】
ユーザがこれらのサービスを受ける際には、例えば、ＣＡＳ（Ｃｏｎｄｉｔｉｏｎａｌ Ａｃｃｅｓｓ Ｓｙｓｔｅｍ）等のように、特定のハードウェア情報による認証、又はパスワード認証（例えば、特許文献１及び特許文献２を参照）によりサービスを受ける。
【先行技術文献】
【特許文献】
【０００４】
【特許文献１】特開２００２－３６６５１９号公報
【特許文献２】特開２０００－８２０４４号公報
【発明の概要】
【発明が解決しようとする課題】
【０００５】
しかしながら、特定のハードウェア情報による認証の場合、この特定のハードウェアがない所では、サービスを利用できない。したがって、例えば、ユーザが移動端末を所有し、移動中や移動先でサービスを利用することは困難となる。
【０００６】
また、パスワード認証であれば、移動端末からでも容易に認証を行えるが、このためには、移動端末が認証先とネットワークで繋がっている必要があるため、ダウンロード済みのコンテンツを視聴するとき等に、利用可能な条件に制限が生じる。さらに、パスワードが漏洩すると第三者によりサービスが利用される可能性がある。
【０００７】
本発明は、ライセンス情報に基づいて提供されるサービスを、外部端末においても利用できるように、このライセンス情報を移譲できるライセンス移譲装置、ライセンス移譲システム及びライセンス移譲方法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】
【０００８】
本発明では、以下のような解決手段を提供する。
【０００９】
（１）サービスを利用するためのライセンス情報を移譲するライセンス移譲装置であって、所定のライセンス管理装置に対して、自装置の識別子を含む暗号データを伴って、移譲ライセンスの発行許可要求を行う要求部と、前記発行許可要求に応じて前記ライセンス管理装置により発行された署名情報を受信する受信部と、前記発行された署名情報を検証し、少なくとも当該署名情報及び前記サービスの利用可能な有効回数を含む前記移譲ライセンスを生成する生成部と、前記生成部により生成された前記移譲ライセンスを、外部端末へ送信する第１の送信部と、を備えるライセンス移譲装置。
【００１０】
このような構成によれば、ライセンス移譲装置は、自装置が有するライセンス情報に基

づいて提供されるサービスを、外部端末においても利用できるように、このライセンス情報を移譲できる。さらに、サービス利用時に認証先とネットワークで繋がっている必要がないため、コンテンツの視聴等において、より広範囲なサービスが提供可能である。

【００１１】

また、移譲ライセンスには、残り有効回数が設定されるため、仮にこの移譲ライセンスが漏洩した場合であっても、第三者による有効回数を超えるサービスの利用はできない。したがって、サービスの不正利用の被害が限定されるので、パスワード認証に比べて、より安全なサービス提供が可能となる。

【００１２】

（２）前記生成部は、前記移譲ライセンスに含める情報を保証するための鍵付きメッセージ認証コードをさらに連接して当該移譲ライセンスを生成する（１）に記載のライセンス移譲装置。

【００１３】

このような構成によれば、ライセンス移譲装置は、鍵付きメッセージ認証コードが連接された移譲ライセンスを生成できるので、ライセンス情報の正当性が保証され、安全にサービス提供が行われる。

【００１４】

（３）前記要求部は、前記発行許可要求の度に新たにシリアル番号を生成し、前記暗号データに当該シリアル番号を含め、前記署名情報は、前記シリアル番号を含んで発行される（１）又は（２）に記載のライセンス移譲装置。

【００１５】

このような構成によれば、ライセンス移譲装置は、移譲ライセンス毎にシリアル番号を生成する。したがって、ライセンス管理装置において、このシリアル番号に対応付けてライセンスの残り有効回数を管理でき、移譲ライセンスの複製や不正な作成を検出できる。したがって、パスワード認証に比べて、より安全なサービス提供が可能となる。

【００１６】

（４）前記生成部は、前記シリアル番号に対応して前記サービスを利用した支払総回数をさらに含んで前記移譲ライセンスを生成する（３）に記載のライセンス移譲装置。

【００１７】

このような構成によれば、ライセンス移譲装置は、移譲ライセンスに支払総回数を含めることにより、有効回数との組合せで、より厳密なライセンス情報を外部端末へ移譲できる。

【００１８】

（５）（４）に記載のライセンス移譲装置と、前記ライセンス管理装置と、前記外部端末と、を有するライセンス移譲システムであって、前記外部端末は、前記ライセンス移譲装置から受信した前記移譲ライセンスを記憶する第１の記憶部と、前記サービスを利用する際には、前記第１の記憶部に記憶されている前記移譲ライセンスに含まれる前記有効回数を減じて更新する更新部と、前記シリアル番号と当該シリアル番号に対応する前記支払総回数との組を記憶する第２の記憶部と、を備えるライセンス移譲システム。

【００１９】

このような構成によれば、ライセンス移譲システムの外部端末において、移譲されたライセンス情報を用いて、有効回数に従ってサービスを利用できると共に、移譲ライセンスのシリアル番号毎に支払総回数等の使用状況を保持できる。

【００２０】

（６）（４）に記載のライセンス移譲装置と、前記ライセンス管理装置と、前記外部端末と、前記サービスの利用機器と、を有するライセンス移譲システムであって、前記外部端末は、前記ライセンス移譲装置から移譲された前記移譲ライセンスを記憶する第１の記憶部と、前記利用機器からの要求に応じて、前記第１の記憶部に記憶されている前記移譲ライセンスを前記利用機器へ送信する第２の送信部と、前記利用機器により支払処理された移譲ライセンスを受信し、前記第１の記憶部に記憶されている前記移譲ライセンスを更

新する更新部と、を備え、前記利用機器は、前記サービスを利用する際に、前記ライセンス移譲装置から受信した前記移譲ライセンスに含まれる前記有効回数を減じて支払処理し、当該支払処理後の移譲ライセンスを前記外部端末へ送信する支払部と、前記シリアル番号と当該シリアル番号に対応する前記支払総回数との組を記憶する第２の記憶部と、を備えるライセンス移譲システム。

【００２１】

このような構成によれば、ライセンス移譲システムのサービス利用機器において、移譲されたライセンス情報を用いて、有効回数に従ってサービスを利用できると共に、移譲ライセンスのシリアル番号毎に支払総回数等の使用状況を保持できる。

【００２２】

（７）前記ライセンス管理装置は、前記第２の記憶部に記憶されている前記シリアル番号と前記支払総回数との組を回収する回収部と、前記回収部により回収された組データの正当性を確認する確認部と、を備える（５）又は（６）に記載のライセンス移譲システム。

【００２３】

このような構成によれば、ライセンス移譲システムのライセンス管理装置において、移譲ライセンスの使用状況を示す組データを回収し、これらの正当性を確認することにより、サービスの不正利用を検出できる。

【００２４】

（８）前記第２の記憶部は、前記サービスの識別データと、当該サービスの利用回数との組をさらに記憶し、前記回収部は、前記第２の記憶部に記憶されている前記識別データと前記利用回数との組をさらに回収する（７）に記載のライセンス移譲システム。

【００２５】

このような構成によれば、ライセンス移譲システムのライセンス管理装置において、移譲ライセンスにより提供されたサービスの識別データと、このサービスの利用回数とを把握できる。さらに、これらのデータに基づいて、不正利用の追跡が可能となる。

【００２６】

（９）ライセンス移譲装置がサービスを利用するためのライセンス情報を移譲するライセンス移譲方法であって、所定のライセンス管理装置に対して、自装置の識別子を含む暗号データを伴って、移譲ライセンスの発行許可要求を行う要求ステップと、前記発行許可要求に応じて前記ライセンス管理装置により発行された署名情報を受信する受信ステップと、前記発行された署名情報を検証し、少なくとも当該署名情報及び前記サービスの利用可能な有効回数を含む前記移譲ライセンスを生成する生成ステップと、前記生成ステップにおいて生成された前記移譲ライセンスを、外部端末へ送信する送信ステップと、を含むライセンス移譲方法。

【発明の効果】

【００２７】

本発明によれば、ライセンス移譲装置においてライセンス情報に基づいて提供されるサービスが、外部端末においても利用できる。

【図面の簡単な説明】

【００２８】

【図１】第１実施形態に係るライセンス移譲システムの全体構成を示す概要図である。

【図２】第１実施形態に係るライセンス移譲システムの機能構成を示すブロック図である。

【図３】第１実施形態に係るライセンス移譲システムにおける処理の流れを示すシーケンス図である。

【図４】第２実施形態に係るライセンス移譲システムの全体構成を示す概要図である。

【図５】第２実施形態に係るライセンス移譲システムの機能構成を示すブロック図である。

【図６】第２実施形態に係るライセンス移譲システムにおける処理の流れを示すシーケン

ス図である。
【発明を実施するための形態】
【００２９】
＜第１実施形態＞
以下、本発明の第１実施形態について説明する。
【００３０】
図１は、本実施形態に係るライセンス移譲システム１の全体構成を示す概要図である。
ライセンス移譲システムは、ライセンス管理機関１０（ライセンス管理装置）と、ＰＣ（Ｐｅｒｓｏｎａｌ　Ｃｏｍｐｕｔｅｒ）やセットトップボックス等の自宅機器２０（ライセンス移譲装置）と、携帯電話機等の移動端末３０（外部端末）とを含んで構成されている。
【００３１】
ライセンス管理機関１０は、サービス提供に関するライセンス情報を管理する装置又は装置群であり、自宅機器２０から移譲されたライセンスの移譲先での使用状況を管理する。
【００３２】
自宅機器２０は、サービスを利用するためのライセンス情報を移譲する装置である。自宅機器２０は、ライセンス管理機関１０から移譲ライセンスを許可する署名情報の発行を受け、自宅機器２０が有しているライセンスの一部又は新たなライセンスを移譲ライセンスとして、移動端末へ提供する。
【００３３】
移動端末３０は、サービス提供者４０からのサービス提供に応じて、移譲ライセンスの有効回数を更新し、更新された移譲ライセンスを保存する。また、移動端末３０は、ライセンス管理機関１０からの要求に応じて、移譲ライセンスの使用状況を示す回収データを送信し、ライセンス管理機関１０において正当性が確認される。
【００３４】
図２は、本実施形態に係るライセンス移譲システム１の機能構成を示すブロック図である。
ライセンス管理機関１０の制御部は、発行部１１と、回収部１２と、確認部１３とを備え、ライセンス管理機関１０の記憶部は、履歴ＤＢ１４を備える。
自宅機器２０の制御部は、要求部２１と、受信部２２と、生成部２３と、送信部２４（第１の送信部）とを備える。
移動端末３０の制御部は、受信部３１と、更新部３２と、抽出部３３とを備え、移動端末３０の記憶部は、ライセンスＤＢ３４（第１の記憶部）と、使用状況ＤＢ３５（第２の記憶部）とを備える。
【００３５】
発行部１１は、要求部２１からの要求に応じて、移譲ライセンスの一部を構成する署名情報を発行し、自宅機器２０へ送信する。
【００３６】
回収部１２は、移動端末３０における移譲ライセンスの使用状況として、使用状況ＤＢ３５に記憶されている回収データを回収する。回収データには、移譲ライセンスを識別するためのシリアル番号と、各移譲ライセンスによるサービスの利用回数を示す支払総回数との組が、さらには、利用されたサービスの識別データとその利用回数との組が含まれる。
【００３７】
確認部１３は、回収部１２により回収された回収データの正当性を確認し、移譲ライセンスの重複利用や不正利用を検出する。
【００３８】
履歴ＤＢ１４は、回収部１２により回収され、確認部１３により正当性が確認された回収データに基づいて、シリアル番号毎の支払総回数の履歴データを記憶する。すなわち、

確認部１３は、回収データと、この履歴データとの整合性（重複しないこと）を確認することにより、正当性を確認する。

【００３９】

要求部２１は、移譲ライセンスを識別するためのシリアル番号を生成し、ライセンス管理機関１０に対して、自宅機器２０の識別子と生成したシリアル番号とを含む暗号データを伴って、移譲ライセンスの発行許可要求を行う。なお、要求部２１は、移譲ライセンスを識別するため、発行許可要求の度に新たにシリアル番号を生成する。

これにより、発行部１１は、シリアル番号を含んで署名情報を発行するので、各移譲ライセンスそれぞれの正当性が保証される。

【００４０】

受信部２２は、発行許可要求に応じてライセンス管理機関１０の発行部１１により発行された署名情報を受信する。

【００４１】

生成部２３は、ライセンス管理機関１０の発行部１１により発行された署名情報を検証し、少なくともこの署名情報及びサービスの利用可能な有効回数を含む移譲ライセンスを生成する。具体的には、生成部２３は、署名情報及び有効回数の他、データの正確性を高めるために、要求部２１により生成されたシリアル番号に対応してサービスを利用した回数を示す支払総回数をさらに含んで移譲ライセンスを生成する。また、このとき、生成部２３は、これら移譲ライセンスに含める情報を保証するための鍵付きメッセージ認証コードをさらに連接して移譲ライセンスを生成する。

【００４２】

送信部２４は、生成部２３により生成された移譲ライセンスを、移譲先であり、かつ、サービスを利用するための端末である移動端末３０へ送信する。

【００４３】

受信部３１は、自宅機器２０の送信部２４から送信された移譲ライセンスを受信し、ライセンスＤＢ３４に記憶させる。

【００４４】

更新部３２は、移動端末３０がサービスを利用する際には、ライセンスＤＢ３４に記憶されている移譲ライセンスに含まれる有効回数を１減少させると共に、支払総回数を１増加させて更新する。また、このとき、更新部３２は、移譲ライセンスに含まれるシリアル番号と支払総回数との組を使用状況ＤＢ３５に記憶させる。

【００４５】

抽出部３３は、ライセンス管理機関１０からの要求に応じて、使用状況ＤＢ３５に記憶されている回収データのうち、未送信の回収データを抽出してライセンス管理機関１０へ送信する。

【００４６】

ライセンスＤＢ３４は、ライセンス移譲装置から受信部３１により受信した移譲ライセンスを記憶する。また、記憶されている移譲ライセンスは、更新部３２により更新される。

【００４７】

使用状況ＤＢ３５は、移動端末３０がサービスを利用する際に、更新部３２の制御によって、シリアル番号と支払総回数との組、さらには、利用したサービスの識別データとこのサービスの利用回数との組を記憶する。

【００４８】

図３は、本実施形態に係るライセンス移譲システム１における処理の流れを示すシーケンス図である。図３に沿って、各部によって生成又は送受信されるデータを具体的に説明する。

【００４９】

以下で使用される記号は、次の通り定義される。なお、各記号の添字ｎａ，ｎｂ，ｎｃ，ｎｄ，ｐ，ｓ，ｚは、それぞれ独立した０以上の整数を表す。

・‖：前後の値の連接。
・PUB_a，PUB_{at}：移動端末３０の公開鍵。ａは認証局により発行された正規のものであり、ａｔは一時的な暗号化通信用のものである。
・ＰＥＮＣ（ｍ，ｋ）：メッセージ（ｍ）を、公開鍵（ｋ）を使用して公開鍵暗号方式により暗号化したデータ。
・ＳＥＮＣ（ｍ，ｋ）：メッセージ（ｍ）を、共有鍵（ｋ）を使用して共通鍵暗号方式により暗号化したデータ。
・ＭＡＣ（ｍ，ｋ）：メッセージ（ｍ）の共有鍵（ｋ）による鍵付きメッセージ認証コード。ｍ＝ＡＬＬの場合、自身（鍵付きメッセージ認証コード）を除く全てのメッセージを対象とする。
・ＬＩＤ：自宅機器２０の識別子であり、機器内に記憶されている。
・S_S，$Z_{(s,z)}$，$T_{(s,z)}$，$rc_{(s,z)}$：移譲ライセンスのシリアル番号（S_S）、残り有効回数（$Z_{(s,z)}$）、支払総回数（$T_{(s,z)}$）、データスクランブル用の乱数（$rc_{(s,z)}$）。
・K_M：ライセンス管理機関１０と各機器（例えば、自宅機器２０）とで共有するマスター鍵であり、ユーザが知り得ない形態により、各機器に記憶されている。
・SIG_L（ｍ）：ライセンス管理機関１０によるメッセージ（ｍ）の電子署名。
・SS_{nb}，ST_{nb}：移譲ライセンスに関する回収データとして移動端末３０に記録される、移譲ライセンスのシリアル番号（SS_{nb}）と、支払総回数（ST_{nb}）。
・ＮＳ，ＮＰ：移動端末３０に保存されている、利用された移譲ライセンスのシリアル番号と支払総回数との組の個数（ＮＳ）と、利用されたサービスの識別データと利用回数との組の個数（ＮＰ）。
・RS_{nc}，$RT_{(nc,nd)}$：ライセンス管理機関１０において履歴管理している、移譲ライセンスのシリアル番号（RS_{nc}）と支払総回数（$RT_{(nc,nd)}$）。

【００５０】
ステップＳ１において、自宅機器２０の要求部２１は、まず、移譲ライセンスを識別するためのシリアル番号S_Sを生成する。続いて、要求部２１は、自宅機器２０の識別子（ＬＩＤ）及びマスター鍵（K_M）を用いて、

$$SENC(LID, K_M) \| S_S \| MAC(ALL, K_M) \quad \cdots (1)$$

を生成し、移譲ライセンスの発行許可要求として、ライセンス管理機関１０へ送信する。

【００５１】
ステップＳ２において、ライセンス管理機関１０の発行部１１は、（１）の「$MAC(ALL, K_M)$」を検証した後、シリアル番号（S_S）に署名し、

$$SENC(SIG_L(S_S), K_M) \quad \cdots (2)$$

を、移譲ライセンスの一部として生成し、自宅機器２０へ送信する。

【００５２】
ステップＳ３において、自宅機器２０の生成部２３は、（２）の署名情報「$SIG_L(S_S)$」を検証する。生成部２３は、この署名情報が正当であれば、残り有効回数（$Z_{(s,0)}$）と支払総回数（$T_{(s,0)}$）とを設定し、さらに、乱数（$rc_{(s,0)}$）を生成した後、移譲ライセンスを共通鍵（K_W）で暗号化し、その鍵付きメッセージ認証コードを連接して、

$$SENC(rc_{(s,0)} \| T_{(s,0)} \| Z_{(s,0)} \| S_S \| SIG_L(S_S) \| MAC(rc_{(s,0)} \| T_{(s,0)} \| Z_{(s,0)} \| S_S \| SIG_L(S_S), K_M), K_W) \| MAC(ALL, K_W) \quad \cdots (3)$$

を、移動端末３０へ送信する。

【００５３】
ステップＳ４において、移動端末３０の受信部３１は、受信したデータの正当性を検証した後、復号化した移譲ライセンスとして、

$$rc_{(s,z)} \| T_{(s,z)} \| Z_{(s,z)} \| S_S \| SIG_L(S_S) \| MAC(ALL, K_M) \quad \cdots (4)$$

を、ライセンスＤＢ３４に保存する。なお、「ｚ」の初期値は０である。

【００５４】

ステップＳ５において、移動端末３０の更新部３２は、サービスの利用に応じた支払処理として、（４）の移譲ライセンスに含まれている残り有効回数を１減少（$Z_{(s,z+1)}$）させると共に、支払総回数を１増加（$T_{(s,z+1)}$）させ、さらに、新たに乱数（$rc_{(s,z+1)}$）を生成して、

$$rc_{(s,z+1)} \| T_{(s,z+1)} \| Z_{(s,z+1)} \| S_S \| SIG_L(S_S) \| MAC(ALL, K_M) \quad \cdots (5)$$

を、新たな移譲ライセンスとしてライセンスＤＢ３４に保存する。

また、更新部３２は、サービスの識別データ（Pro_p）の総利用回数（Pay_p）に１を加算して、使用状況ＤＢ３５に回収データとして保存する。さらに、更新部３２は、移譲ライセンスのシリアル番号（S_S）及び支払総回数（$Z_{(s,z)}$）を、それぞれ回収データの「SS_{nb}」及び「ST_{nb}」の組に記録する。

【００５５】

ステップＳ６において、ライセンス管理機関１０の回収部１２は、所定のスケジュールに従って、移動端末３０に移譲ライセンスの使用状況に関する回収データの回収要求を送信する。

【００５６】

ステップＳ７において、移動端末３０は、前回の回収要求に対する応答より後に保存されている回収データを抽出し、

$$SENC((SS_0 \| ST_0) \| \cdots \| (SS_{NS-1} \| ST_{NS-1}) \| (Pro_0 \| Pay_0) \| \cdots \| (Pro_{NP-1} \| Pay_{NP-1}), K_M) \| MAC(ALL, K_M) \quad \cdots (6)$$

を生成して、ライセンス管理機関１０へ送信する。

【００５７】

ステップＳ８において、ライセンス管理機関１０の確認部１３は、（６）の「$SS_i \| ST_i$」（$0 \leqq i \leqq NS-1$）の組より、「SS_i」が履歴ＤＢ１４に登録されていない場合、「SS_i」と「ST_i」とを、この履歴ＤＢ１４に追加する。

一方、「SS_i」が履歴ＤＢ１４に登録されている場合、「ST_i」が重複しないこと、及び順序の正当性（例えば、昇順であること）を確認する。正当である場合、確認部１３は、「SS_i」と同番号である管理シリアル番号（RS_{nc}）と組で管理されている支払総回数（$RT_{(nc,nd)}$）に「ST_i」を追加する。そして、回収データの全ての組について正当性が確認されると、確認部１３は、移動端末３０へ確認応答（Ａｃｋ）を送信する。

【００５８】

以上のように、本実施形態によれば、自宅機器２０は、自機器が有するライセンス情報に基づいて提供されるサービスを、移動端末３０においても利用できるように、このライセンス情報を移譲できる。さらに、移動端末３０は、サービス利用時に認証先とネットワークで繋がっている必要がないため、コンテンツの視聴等において、より広範囲なサービスが提供可能である。

【００５９】

さらに、自宅機器２０は、鍵付きメッセージ認証コードが連接された移譲ライセンスを生成できるので、ライセンス情報の正当性が保証され、安全にサービス提供が行われる。

【００６０】

また、移譲ライセンスには、残り有効回数が設定されるため、仮にこの移譲ライセンスが漏洩した場合であっても、第三者による有効回数を超えるサービスの利用はできない。したがって、サービスの不正利用の被害が限定されるので、パスワード認証に比べて、より安全なサービス提供が可能となる。

さらに、移譲ライセンスには支払総回数も含まれるので、有効回数との組合せで、より厳密なライセンス情報が外部端末へ移譲される。

【００６１】
　また、移譲ライセンス毎にシリアル番号が生成され、ライセンス管理機関１０において、このシリアル番号に対応付けて移譲ライセンスの使用状況を示す回収データを履歴管理できる。これにより、ライセンス管理機関１０は、移譲ライセンスの複製や不正な作成を検出できると共に、不正利用の追跡が可能となる。したがって、パスワード認証に比べて、より安全なサービス提供が可能となる。
【００６２】
　＜第２実施形態＞
　以下、本発明の第２実施形態について説明する。なお、第１実施形態と同様の構成については、同一の符号を付し、説明を省略又は簡略化する。
【００６３】
　図４は、本実施形態に係るライセンス移譲システム１ａの全体構成を示す概要図である。
　ライセンス移譲システムは、ライセンス管理機関１０（ライセンス管理装置）と、自宅機器２０（ライセンス移譲装置）と、移動端末３０ａ（外部端末）と、外出先機器３０ｂ（サービス利用機器）とを含んで構成されている。つまり、本実施形態では、ライセンス情報の移譲を受けた移動端末３０ａとは別の外出先機器３０ｂにおいてサービスが利用される。なお、本実施形態では、移動端末３０ａ及び外出先機器３０ｂの構成が第１実施形態と異なっている。
【００６４】
　移動端末３０ａは、自宅機器２０から移譲された移譲ライセンスを保存しつつ、この移譲ライセンスを外出先機器３０ｂへ提出し、サービスの利用に伴って更新された移譲ライセンスを受け取って上書き保存する。
【００６５】
　外出先機器３０ｂは、サービス提供者４０からのサービス提供に応じて、移譲ライセンスの有効回数を更新し、更新された移譲ライセンスを移動端末３０ａへ送信する。また、外出先機器３０ｂは、ライセンス管理機関１０からの要求に応じて、移譲ライセンスの使用状況を示す回収データを送信し、ライセンス管理機関１０において正当性が確認される。
【００６６】
　図５は、本実施形態に係るライセンス移譲システム１ａの機能構成を示すブロック図である。
　移動端末３０ａの制御部は、受信部３１と、送信部３６（第２の送信部）と、更新部３８とを備え、移動端末３０ａの記憶部は、ライセンスＤＢ３４（第１の記憶部）を備える。
　また、外出先機器３０ｂの制御部は、抽出部３３と、支払部３７とを備え、外出先機器３０ｂの記憶部は、使用状況ＤＢ３５（第２の記憶部）を備える。
【００６７】
　ここで、受信部３１、抽出部３３、ライセンスＤＢ３４及び使用状況ＤＢ３５は、第１実施形態と同様の構成である。そして、送信部３６、支払部３７及び更新部３８の機能は、第１実施形態の更新部３２の機能に相当する。
【００６８】
　移動端末３０ａの送信部３６は、外出先機器３０ｂからの要求に応じて、ライセンスＤＢ３４に記憶されている移譲ライセンスを外出先機器３０ｂへ送信する。
【００６９】
　外出先機器３０ｂの支払部３７は、移動端末３０ａから移譲ライセンスを受信し、署名情報及び鍵付きメッセージ認証コードの正当性を検証する。そして、支払部３７は、サービスを利用する際に、移譲ライセンスの支払処理として、移譲ライセンスに含まれる残り有効回数を１減少させると共に、支払総回数を１増加させると、処理後の移譲ライセンスを移動端末３０ａへ送信する。

【００７０】
移動端末３０の更新部３８は、外出先機器３０ｂにより支払処理された移譲ライセンスを受信し、ライセンスＤＢ３４に記憶されている移譲ライセンスを更新する。
【００７１】
図６は、本実施形態に係るライセンス移譲システム１ａにおける処理の流れを示すシーケンス図である。図６に沿って、各部によって生成又は送受信されるデータを具体的に説明する。
【００７２】
ステップＳ１～Ｓ４は、第１実施形態と同様であり、移動端末３０ａは、移譲ライセンスとして、

$rc_{(s,z)} \| T_{(s,z)} \| Z_{(s,z)} \| S_S \| SIG_L(S_S) \| MAC(ALL, K_M)$ ・・・（７）

を、ライセンスＤＢ３４に保存する。
【００７３】
ステップＳ１１において、移動端末３０ａ及び外出先機器３０ｂは、鍵交換と利用サービスの選択とを行う。具体的には、まず、移動端末３０ａの制御部は、一時的な公開鍵（PUB_{at}）を生成し、サービス要求として外出先機器３０ｂへ送信する。外出先機器３０ｂの制御部は、一時的なワーク鍵（K_{wt}）を生成し、公開鍵（PUB_{at}）で暗号化した、

$PENC(K_{wt}, PUB_{at})$ ・・・（８）

を、移動端末３０ａへ送信する。
続いて、移動端末３０ａの制御部は、ユーザが選択したサービスの識別データ（Pro_p）を外出先機器３０ｂへ送信する。そして、外出先機器３０ｂの制御部は、移譲ライセンスの有効回数を１減ずることを移動端末３０ａへ通知する。
【００７４】
ステップＳ１２において、ユーザが有効回数の減少に合意した場合、移動端末３０ａの送信部３６は、移譲ライセンスの有効回数（$Z_{(s,z)}$）が残っている（＞０）ことを確認する。そして、送信部３６は、ライセンスＤＢ３４に保存されている移譲ライセンスを、鍵交換されたワーク鍵（K_{wt}）で暗号化し、

$SENC(rc_{(s,z)} \| T_{(s,z)} \| Z_{(s,z)} \| S_S \| SIG_L(S_S) \| MAC(rc_{(s,z)} \| T_{(s,z)} \| Z_{(s,z)} \| S_S \| SIG_L(S_S), K_M), K_{Wt}) \| MAC(ALL, K_{Wt})$ ・・・（９）

を、外出先機器３０ｂへ送信することにより、移譲ライセンスを提出する。
【００７５】
ステップＳ１３において、外出先機器３０ｂの支払部３７は、（９）に含まれている署名情報と鍵付きメッセージ認証コードとを検証する。そして、支払部３７は、サービスの利用に応じた支払処理として、残り有効回数を１減少（$Z_{(s,z+1)}$）させると共に、支払総回数を１増加（$T_{(s,z+1)}$）させ、さらに、新たに乱数（$rc_{(s,z+1)}$）を生成して、

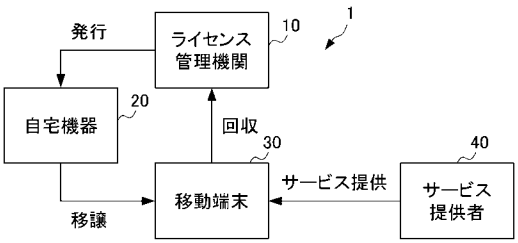
$SENC(rc_{(s,z+1)} \| T_{(s,z+1)} \| Z_{(s,z+1)} \| S_S \| SIG_L(S_S) \| MAC(rc_{(s,z+1)} \| T_{(s,z+1)} \| Z_{(s,z+1)} \| S_S \| SIG_L(S_S), K_M), K_{Wt}) \| MAC(ALL, K_{Wt})$ ・・・（１０）

を、移動端末３０ａへ送信する。
また、支払部３７は、サービスの識別データ（Pro_p）の総利用回数（Pay_p）に１を加算して、使用状況ＤＢ３５に回収データとして保存する。さらに、支払部３７は、移譲ライセンスのシリアル番号（S_S）及び支払総回数（$Z_{(s,z)}$）を、それぞれ回収データの「SS_{nb}」及び「ST_{nb}」の組に記録する。
【００７６】
ステップＳ１４において、移動端末３０ａの更新部３８は、外出先機器３０ｂから受信したデータを検証した後、復号化し、

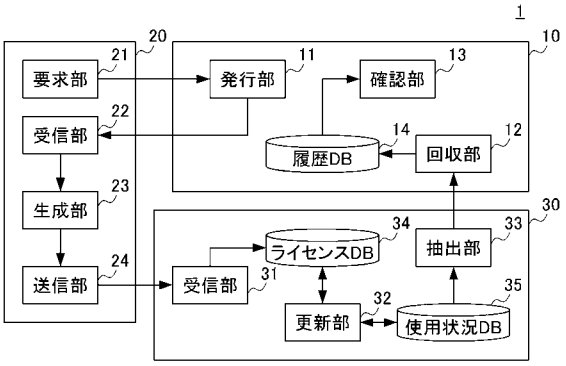
$rc_{(s,z+1)} \| T_{(s,z+1)} \| Z_{(s,z+1)} \| S_S \| SIG_L(S_S) \| MAC(ALL, K_M)$ ・・・（１１）
を、新たな移譲ライセンスとしてライセンスＤＢ３４を更新する。
【００７７】
ステップＳ１５～Ｓ１７は、第１実施形態のステップＳ６～Ｓ８に相当する。ただし、ライセンス管理機関１０は、サービスを利用した外出先機器３０ｂから回収データを回収し、正当性を確認する。
【００７８】
なお、本実施形態において、移動端末３０ａは、第１実施形態と同様に更新部３２、抽出部３３及び使用状況ＤＢ３５を備えていてもよく、この場合、移動端末３０ａ及び外出先機器３０ｂの双方において、移譲ライセンスに基づいてサービスを利用できる。
【００７９】
以上のように、本実施形態によれば、ユーザは、ライセンス情報が移譲された移動端末３０ａのみならず、外出先機器３０ｂにおいて、移動端末３０ａに移譲されたライセンス情報を用いて、有効回数に従ってサービスを利用できる。
【００８０】
以上、本発明の実施形態について説明したが、本発明は上述した実施形態に限るものではない。また、本発明の実施形態に記載された効果は、本発明から生じる最も好適な効果を列挙したに過ぎず、本発明による効果は、本発明の実施形態に記載されたものに限定されるものではない。
【００８１】
上述の実施形態では、回収要求（ステップＳ６又はステップＳ１５）に基づいて回収データが回収されたが、これには限られない。例えば、サービスを利用した機器（第１実施形態の移動端末３０、又は第２実施形態の外出先機器３０ｂ）がライセンス管理機関１０とネットワークで繋がったときや、処理負荷の低いアイドル中等に、自発的に回収データを送信してもよい。
【００８２】
また、ライセンス移譲システム１（又は１ａ）が有する各装置は、上述の機能を備える専用の装置であってもよいし、ＰＣ、サーバ、携帯電話機又はＰＤＡ（Ｐｅｒｓｏｎａｌ Ｄｉｇｉｔａｌ Ａｓｓｉｓｔａｎｔ）等、様々な情報処理装置（コンピュータ）であってよい。
【００８３】
そして、ライセンス移譲システム１（又は１ａ）における各機能は、ソフトウェアにより実現される。ソフトウェアによって実現される場合には、このソフトウェアを構成するプログラムが、上記情報処理装置（コンピュータ）にインストールされる。また、これらのプログラムは、ＣＤ－ＲＯＭのようなリムーバブルメディアに記録されてユーザに配布されてもよいし、ネットワークを介してユーザのコンピュータにダウンロードされることにより配布されてもよい。
【符号の説明】
【００８４】
１、１ａ　ライセンス移譲システム
１０　ライセンス管理機関（ライセンス管理装置）
１１　発行部
１２　回収部
１３　確認部
１４　履歴ＤＢ
２０　自宅機器（ライセンス移譲装置）
２１　要求部
２２　受信部
２３　生成部

２４　送信部（第１の送信部）
３０、３０ａ　移動端末（外部端末）
３０ｂ　外出先機器（サービス利用機器）
３１　受信部
３２　更新部
３３　抽出部
３４　ライセンスＤＢ（第１の記憶部）
３５　使用状況ＤＢ（第２の記憶部）
３６　送信部（第２の送信部）
３７　支払部
３８　更新部
４０　サービス提供者

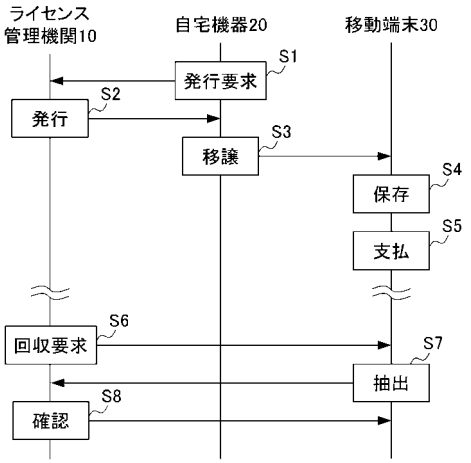
【図１】



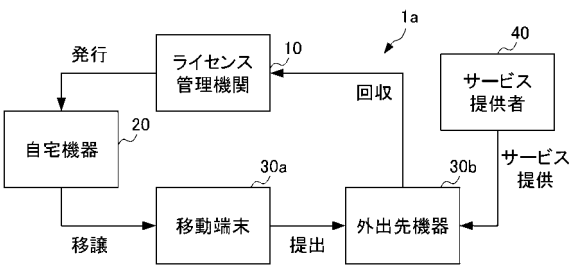
【図２】



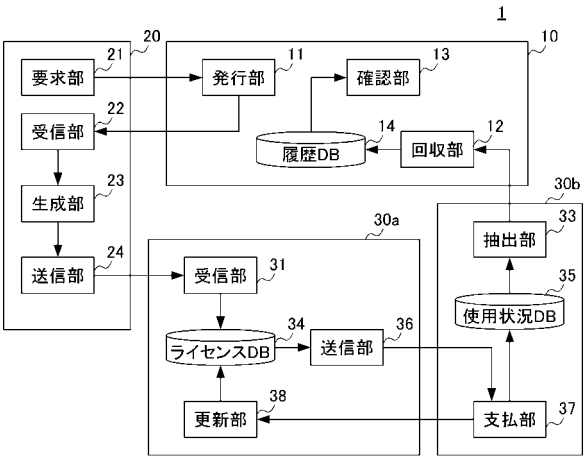
【図３】



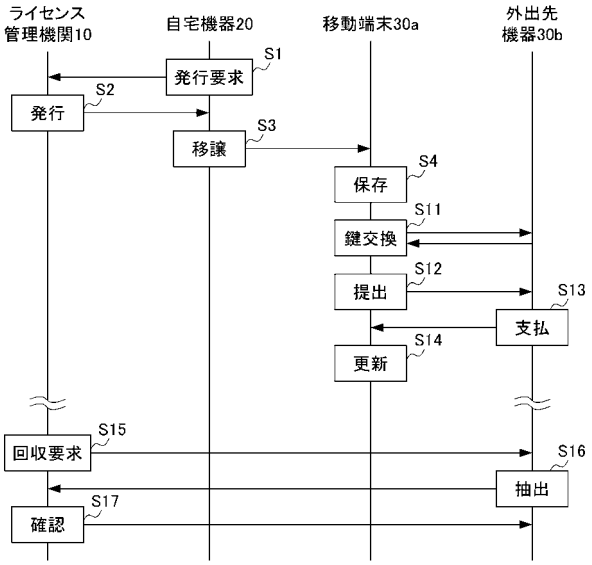
【図４】



【図５】


1
20
21
要求部
22
受信部
23
生成部
24
送信部
10
発行部
11
確認部
13
履歴DB
14
回収部
12
30b
33
抽出部
35
使用状況DB
30a
31
受信部
34
ライセンスDB
36
送信部
38
更新部
37
支払部

【図６】


ライセンス
管理機関10
自宅機器20
移動端末30a
外出先
機器30b
S1
発行要求
S2
発行
S3
移譲
S4
保存
S11
鍵交換
S12
提出
S13
支払
S14
更新
S15
回収要求
S16
抽出
S17
確認

フロントページの続き

(56)参考文献 特開２００３－１０１５２６（ＪＰ，Ａ）
特開２００３－１６２６００（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ ２１／１０
Ｈ０４Ｎ ７／１６
Ｈ０４Ｌ ９／００