

明 細 書

発明の名称：

利用管理システム、管理装置、利用制御装置、利用管理方法、およびコンピュータで読み取り可能なプログラム

技術分野

[0001] 本発明は、ホテル、旅館、民泊施設、家屋、倉庫、部屋等の出入口、自動車、自転車等の移動体、および電子カルテ、電子書籍等の電子媒体の閲覧端末を含む、施錠・解錠、アクセス制御、あるいは暗号化・復号化により利用を制限可能な利用対象物の利用管理技術に関する。

背景技術

[0002] 特許文献1には、企業、病院、遊技場、公共施設等の施設内において、ルームキーを携帯するだけで、部屋の解錠および施錠を含む各種サービスを利用することができるシステムが開示されている。このシステムは、ルームナンバー、暗証番号、顧客情報等の情報を記憶し、読み書き可能なRFID(Radio Frequency Identification)無線タグを有するルームキーと、ルームキーのRFID無線タグに対して情報の読み書きをするために施設内の各所に設置されたRFIDリーダと、施設内の各部屋および各設備に関する情報を記憶したデータベースと、ネットワークを介してRFIDリーダおよびデータベースに接続され、施設内の各部屋および各設備の管理を行うサーバと、を備えている。そして、例えば、施設内の各部屋のドア、部屋内等に設置されたRFIDリーダが、ルームキーのRFID無線タグに記憶されている情報を読み取ってサーバに送信し、これを受けてサーバが、RFIDリーダから受信した情報に含まれているルームナンバーとこのRFIDリーダが設置されている部屋のルームナンバーとを照合して、この部屋の解錠および施錠を行う。

先行技術文献

特許文献

[0003] 特許文献1：特開2003-132435号公報

発明の概要

発明が解決しようとする課題

[0004] しかしながら、特許文献1のシステムは、企業、病院、遊技場、公共施設等の施設の受付において、ルームキーの貸与および返却が行われることを前提としている。このため、例えば、インターネット上で施設の予約をした場合でも、この施設を管理する管理部門の受付に立ち寄ってルームキーを借りてから、予約した施設に移動しなければならない。また、施設の利用後には、この管理部門の受付に立ち寄ってルームキーを返却しなければならない。したがって、予約した施設とこの施設を管理する管理部門の受付とが地理的に離れている場合、利便性が悪い。

[0005] また、特許文献1のシステムでは、施設内の各所に設置されたRFIDリーダーが、ルームキーのRFID無線タグに記憶されている情報を読み取って、ネットワーク経由でサーバに送信している。このため、例えばサーバが施設外に設置されており、施設内の各所に設置されたRFIDリーダーと施設外に設置されたサーバとがインターネット経由で接続されている場合、RFIDリーダーがルームキーのRFID無線タグから情報を読み取る都度、この読み取った情報がインターネット上を伝送することとなる。したがって、セキュリティ上のリスクが高くなる。

[0006] 本発明は上記事情に鑑みてなされたものであり、その目的は、ホテル、旅館、民泊施設、家屋、倉庫、部屋等の出入口、自動車、自転車等の移動体、および電子カルテ、電子書籍等の電子媒体の閲覧端末を含む、施錠・解錠、アクセス制御、あるいは暗号化・復号化により利用を制限可能な利用対象物の利用管理技術において、利便性を向上させつつ、セキュリティ上のリスクを低減することを目的とする。

課題を解決するための手段

[0007] 上記課題を解決するために、本発明は、利用許可証に基づいて、施錠・解錠、アクセス制御、あるいは暗号化・復号化により利用対象物の利用を制御

する利用制御装置と、利用対象物を利用制御装置に対応付けて管理する管理装置と、利用制御装置に利用許可証の検証に必要なホールデータを設定する提供者端末と、利用制御装置に利用許可証を通知する利用者端末と、を備えている。

[0008] ここで、利用制御装置は、近距離無線通信でのみ通信可能であり、ネットワークから切り離されている。また、利用制御装置は、自装置に対応付けられて管理装置に記憶されている第1の秘密鍵と対の第1の公開鍵を記憶している。そして、利用制御装置は、近距離無線通信を介して、提供者端末からホールデータを第1の署名とともに受信すると、この第1の署名を第1の公開鍵で検証し、署名検証が成立したならば、このホールデータを自装置に設定する。このホールデータは、自装置に対応付けられて管理装置に記憶されている第2の秘密鍵と対の第2の公開鍵を含んでいる。また、利用制御装置は、近距離無線通信を介して、利用者端末から利用許可証を第2の署名とともに受信すると、この第2の署名を第2の公開鍵で検証し、署名検証が成立したならば、この利用許可証に含まれている取引情報を取得する。そして、取得した取引情報を参照し、この取引情報により特定される条件を満足するならば、利用対象物の利用制限を解除する。

[0009] なお、利用許可証に含める取引情報は、利用制御装置が管理装置と共有する共通鍵で暗号化されていてもよい。そして、利用制御装置が、利用者端末から受信した利用許可証に含まれている暗号化された取引情報をこの共通鍵を用いて復号化する。この場合、共通鍵は、ホールデータに含めて利用制御装置に送信してもよい。

[0010] 例えば、本発明は、
利用対象物の利用を管理する利用管理システムであって、
利用許可証に基づいて、施錠・解錠、アクセス制御、あるいは暗号化・復号化により利用対象物の利用を制御する利用制御装置と、
前記利用対象物を前記利用制御装置に対応付けて管理する管理装置と、
前記利用制御装置に、前記利用許可証の検証に必要なホールデータを設定

する提供者端末と、

前記利用制御装置に前記利用許可証を通知する利用者端末と、を備え、

前記管理装置は、

前記利用対象物の利用に関する条件を含む取引情報を管理する取引管理手段と、

前記利用制御装置に対応付けて、第1の秘密鍵・公開鍵を管理するオブジェクト管理手段と、

前記利用制御装置に対応付けて、第2の秘密鍵・公開鍵を管理するホール管理手段と、

前記オブジェクト管理手段により管理されている前記第1の秘密鍵を用いて、前記ホール管理手段により管理されている前記第2の公開鍵を含む前記ホールデータに対する第1の署名を生成し、前記ホールデータおよび前記第1の署名を前記提供者端末に送信するホールデータ処理手段と、

前記ホール管理手段により管理されている前記第2の秘密鍵を用いて、前記取引管理手段により管理されている前記取引情報を含む前記利用許可証に対する第2の署名を生成し、前記利用許可証および前記第2の署名を前記利用者端末に送信する利用許可証処理手段と、を有し、

前記提供者端末は、

前記管理装置から受信した前記ホールデータおよび前記第1の署名を、近距離無線通信により前記利用制御装置に送信し、

前記利用者端末は、

前記管理装置から受信した前記利用許可証および前記第2の署名を、近距離無線通信により前記利用制御装置に送信し、

前記利用制御装置は、

近距離無線通信でのみ通信可能であり、

前記提供者端末から前記ホールデータとともに受信した前記第1の署名を、予め登録されている前記第1の公開鍵で検証し、検証成立したならば、前記ホールデータを自装置に設定するホール設定手段と、

前記利用者端末から前記利用許可証とともに受信した前記第2の署名を、自装置に設定されている前記ホールデータに含まれている前記第2の公開鍵で検証し、検証成立したならば、前記利用許可証に含まれている前記取引情報を取得する取引情報取得手段と、

前記取引情報取得手段により取得された前記取引情報を参照し、前記取引情報により特定される条件を満足するならば、前記利用対象物の利用制限を解除する解除手段と、を有する。

発明の効果

[0011] 本発明において、利用制御装置は、近距離無線通信でのみ通信可能であり、ネットワークから切り離されている。このため、利用制御装置がインターネット等のネットワークを介して外部から攻撃されることはない。また、利用対象物の利用制限を解除するために用いる利用許可証は、ホールデータに含まれている第2の公開鍵を用いて、この利用許可証に付加されている第2の署名を検証することによりその正当性が証明され、さらに、ホールデータは、第1の公開鍵を用いて、このホールデータに付加されている第1の署名を検証することによりその正当性が証明される。したがって、本発明によれば、セキュリティ上のリスクが低減される。

[0012] また、本発明では、利用許可証に含まれている取引情報により特定される条件を満足する場合にのみ、利用対象物の利用制限が解除され、満足しない場合には、利用対象物の利用制限は解除されない。このため、利用期限、利用回数等の条件を取引情報に含めておくことで、これらの条件に合致しない利用許可証は、たとえその正当性が証明されても無効となるため、利用対象物の利用者（利用者端末の利用者）から利用許可証を返却してもらう必要がない。したがって、本発明によれば、利便性が向上する。

[0013] このように、本発明によれば、施錠・解錠、アクセス制御、あるいは暗号化・復号化により利用を制限可能な利用対象物の利用管理技術において、利便性を向上させつつ、セキュリティ上のリスクを低減することができる。

図面の簡単な説明

[0014] [図1]図 1 は、本発明の一実施の形態に係る利用管理システムの概略構成図である。

[図2]図 2 は、本発明の一実施の形態に係る利用管理システムにおいて、利用制御装置 1 を管理装置 2 に登録するオブジェクト登録動作の一例を示すシーケンス図である。

[図3]図 3 は、本発明の一実施の形態に係る利用管理システムにおいて、利用制御装置 1 にホールデータを設定するホール設定動作の一例を示すシーケンス図である。

[図4]図 4 は、本発明の一実施の形態に係る利用管理システムにおいて、利用対象物の利用に関する条件を含む取引情報を管理装置 2 に登録する取引情報登録動作の一例を示すシーケンス図である。

[図5]図 5 は、本発明の一実施の形態に係る利用管理システムにおいて、管理装置 2 が利用者端末 4 に利用許可証を発行する利用許可証発行動作の一例を示すシーケンス図である。

[図6]図 6 は、本発明の一実施の形態に係る利用管理システムにおいて、利用制御装置 1 が利用対象物の利用制限を解除する利用制限解除動作の一例を示すシーケンス図である。

[図7]図 7 は、利用制御装置 1 の概略機能構成図である。

[図8]図 8 は、利用制御装置 1 の動作を説明するためのフロー図である。

[図9]図 9 は、管理装置 2 の概略機能構成図である。

[図10]図 10 は、利用者情報記憶部 221 の登録内容例を模式的に表した図である。

[図11]図 11 は、提供者情報記憶部 222 の登録内容例を模式的に表した図である。

[図12]図 12 は、オブジェクトデータ記憶部 223 の登録内容例を模式的に表した図である。

[図13]図 13 は、ホールデータ記憶部 224 の登録内容例を模式的に表した図である。

[図14]図14は、取引情報記憶部225の登録内容例を模式的に表した図である。

[図15]図15は、管理装置2の動作を説明するためのフロー図である。

[図16]図16は、図15に示すオブジェクト登録要求処理S305を説明するためのフロー図である。

[図17]図17は、図15に示すホール生成要求処理S306を説明するためのフロー図である。

[図18]図18は、図15に示す取引要求処理S309を説明するためのフロー図である。

[図19]図19は、図15に示す利用許可証要求処理S310を説明するためのフロー図である。

[図20]図20は、図1に示す利用管理システムの変形例の概略構成図である。

[図21]図21は、図20に示す利用管理システムの変形例において、利用制御装置1Aが利用対象物の利用制限を解除する利用制限解除動作の一例を示すシーケンス図である。

発明を実施するための形態

[0015] 以下、本発明の一実施の形態について、図面を参照して説明する。

[0016] 図1は、本実施の形態に係る利用管理システムの概略構成図である。

[0017] 図示するように、本実施の形態に係る利用管理システムは、利用制御装置1と、管理装置2と、提供者端末3と、利用者端末4と、を備えている。

[0018] 利用制御装置1は、利用対象物毎に設けられ、IrDA (Infrared Data Association)、Bluetooth (登録商標) 等の近距離無線通信63でのみ通信可能であり、利用許可証に基づいて、施錠・解錠、アクセス制御、あるいは暗号化・復号化により利用対象物の利用を制御する。ここでは、利用対象物を家屋50とし、出入口51の施錠・解錠により家屋50の利用を制御している。管理装置2は、利用制御装置1を管理する。また、管理装置2は、WAN (Wide Area Netw

ork) 60を介して、利用許可証の検証に用いるホールデータを提供者端末3に送信するとともに、利用許可証を利用者端末4に送信する。提供者端末3は、提供者毎に設けられ、無線ネットワーク62および無線基地局、アクセスポイント等の中継装置61を介してWAN60に接続されて、管理装置2からホールデータを受信する。また、提供者端末3は、近距離無線通信63により管理装置2から受信したホールデータを利用制御装置1に送信する。利用者端末4は、利用者毎に設けられ、無線ネットワーク62および中継装置61を介してWAN60に接続されて、管理装置2から利用許可証を受信する。また、提供者端末3は、近距離無線通信63により管理装置2から受信した利用許可証を利用制御装置1に送信する。

[0019] 図2は、本実施の形態に係る利用管理システムにおいて、利用制御装置1を管理装置2に登録するオブジェクト登録動作の一例を示すシーケンス図である。

[0020] まず、提供者端末3は、利用対象物（家屋50）の利用サービスを提供する提供者からログイン操作を受け付けると（S100）、提供者のユーザID、パスワードを含むログイン要求を管理装置2に送信する（S101）。これを受けて、管理装置2は、ログイン要求に含まれているパスワードと、このログイン要求に含まれているユーザIDに紐付けて管理しているパスワードと、を用いて認証処理を実施する（S102）。そして、認証成立ならば、ログイン要求の送信元である提供者端末3のログインを許可し、ログイン許可通知をこの提供者端末3に送信する（S103）。

[0021] つぎに、提供者端末3は、提供者から利用対象物である家屋50の物件名、住所等を含む施設情報を伴うオブジェクト登録要求操作を受け付けると（S104）、家屋50の施設情報を含むオブジェクト登録要求を管理装置2に送信する（S105）。これを受けて、管理装置2は、家屋50の利用制御（出入口51の施錠・解錠制御）に用いる利用制御装置1に付与するオブジェクトIDを発行する。また、公開鍵暗号方式に従って第1の秘密鍵・公開鍵を生成する。そして、オブジェクトIDおよび第1の秘密鍵・公開鍵と

、オブジェクト登録要求に含まれている施設情報と、を含むオブジェクトデータを生成する（S106）。それから、管理装置2は、生成したオブジェクトデータを提供者のユーザIDに紐付けて登録・管理する（S107）。その後、管理装置2は、オブジェクトIDおよび第1の公開鍵を含むオブジェクト登録通知を提供者端末3に送信する（S108）。

[0022] つぎに、提供者端末3は、利用制御装置1と近距離無線通信63が可能な距離まで利用制御装置1に近づいた状態において、提供者からオブジェクト設定操作を受け付けると（S109）、利用制御装置1に管理装置2から受信したオブジェクト登録通知を近距離無線通信63により送信する（S110）。これを受けて、利用制御装置1は、オブジェクト登録通知に含まれているオブジェクトIDおよび第1の公開鍵を自装置1に設定する（S111）。

[0023] 図3は、本実施の形態に係る利用管理システムにおいて、利用制御装置1にホールデータを設定するホール設定動作の一例を示すシーケンス図である。

[0024] まず、提供者端末3は、利用対象物（家屋50）の利用サービスを提供する提供者からログイン操作を受け付けると（S120）、提供者のユーザID、パスワードを含むログイン要求を管理装置2に送信する（S121）。これを受けて、管理装置2は、ログイン要求に含まれているパスワードと、このログイン要求に含まれているユーザIDに紐付けて管理しているパスワードと、を用いて認証処理を実施する（S122）。そして、認証成立ならば、ログイン要求の送信元である提供者端末3のログインを許可し、ログイン許可通知をこの提供者端末3に送信する（S123）。

[0025] つぎに、提供者端末3は、提供者から利用制御装置1のオブジェクトIDの指定を伴うホール生成要求操作を受け付けると（S124）、オブジェクトIDを含むホール生成要求を管理装置2に送信する（S125）。これを受けて、管理装置2は、共通鍵暗号方式に従って共通鍵を生成するとともに、公開鍵暗号方式に従って第2の秘密鍵・公開鍵を生成する。そして、オブ

ジェクトID、共通鍵、および第2の公開鍵を含むホールデータを生成する（S126）。それから、管理装置2は、ホールデータを第2の秘密鍵とともに登録・管理する（S127）。また、管理装置2は、自身が管理しているオブジェクトデータからホール生成要求操作で指定されているオブジェクトIDを含むオブジェクトデータを特定し、このオブジェクトデータに含まれている第1の秘密鍵を用いて、ホールデータに対する第1の署名を生成する（S128）。その後、管理装置2は、生成したホールデータおよび第1の署名を提供者端末3に送信する（S129）。

[0026] つぎに、提供者端末3は、利用制御装置1と近距離無線通信が可能な距離まで利用制御装置1に近づいた状態において、提供者からホール設定操作を受け付けると（S130）、利用制御装置1に管理装置2から受信したホールデータおよび第1の署名を近距離無線通信63により送信する（S131）。これを受けて、利用制御装置1は、提供者端末3より受信したホールデータと、自身に設定されている第1の公開鍵とを用いて、提供者端末3より受信した第1の署名を検証する（S132）。そして、署名検証に成功したならば、ホールデータを自装置1に設定する（S133）。

[0027] 図4は、本実施の形態に係る利用管理システムにおいて、利用対象物（家屋50）の利用に関する条件を含む取引情報を管理装置2に登録する取引情報登録動作の一例を示すシーケンス図である。

[0028] まず、利用者端末4は、利用対象物（家屋50）の利用サービスを享受する利用者からログイン操作を受け付けると（S140）、利用者のユーザID、パスワードを含むログイン要求を管理装置2に送信する（S141）。これを受けて、管理装置2は、ログイン要求に含まれているパスワードと、このログイン要求に含まれているユーザIDに紐付けて管理しているパスワードと、を用いて認証処理を実施する（S142）。そして、認証成立ならば、ログイン要求の送信元である利用者端末4のログインを許可し、ログイン許可通知をこの利用者端末4に送信する（S143）。

[0029] つぎに、利用者端末4は、希望する利用対象物（家屋50）の利用サービ

スを提供する提供者のユーザID、この利用対象物に設置された利用制御装置1のオブジェクトID、および、利用希望開始・終了時刻、利用回数等の利用対象物の利用に関する希望情報の指定を伴う取引要求操作を、利用者から受け付けると（S144）、これらの指定された提供者のユーザID、オブジェクトID、および利用に関する希望情報を含む取引要求を、管理装置2に送信する（S145）。

[0030] これを受けて、管理装置2は、取引要求に含まれている情報に基づいて取引内容を確認する（S146）。具体的には、取引要求に含まれている提供者のユーザIDに紐付けて管理しているオブジェクトデータのなかに、取引要求に含まれているオブジェクトIDを有するオブジェクトデータがあることを確認することにより、利用者が希望する利用サービスを提供可能であることを確認する。それから、管理装置2は、取引要求に含まれているオブジェクトIDおよび利用に関する希望情報を含む取引認否問合せを生成し、取引要求に含まれている提供者のユーザIDに紐付けて管理しているアドレス情報により特定される提供者端末3に、この取引認否問合せを送信する（S147）。

[0031] つぎに、提供者端末3は、管理装置2から取引認否問合せを受信すると、この取引認否問合せに含まれているオブジェクトIDおよび利用に関する希望情報を表示して、提供者に取引認否を確認する。そして、提供者から取引を許諾する（利用者にオブジェクトIDにより特定される利用制御装置1によって利用が制限される利用対象物の利用サービスを提供する）旨の取引許諾操作を受け付けると（S148）、この取引認否問合せに対する返信として、管理装置2に取引許諾応答を送信する（S149）。

[0032] これを受けて、管理装置2は、取引成立と判断し、取引IDを発行する。そして、この取引IDと、利用者のユーザIDと、取引要求に含まれている提供者のユーザID、オブジェクトID、および利用に関する希望情報と、利用に関する希望情報に含まれている利用希望開始時刻に基づいて定められる利用許可証取得可能時刻（例えば利用希望開始時刻の24時間前）と、を

含む取引情報を生成する（S 1 5 0）。つぎに、管理装置 2 は、生成した取引情報を登録・管理する（S 1 5 1）。それから、管理装置 2 は、取引情報を含む取引成立通知を利用者端末 4 に送信し（S 1 5 2）、利用者端末 4 にこの取引情報を表示させる。

[0033] 図 5 は、本実施の形態に係る利用管理システムにおいて、管理装置 2 が利用者端末 4 に利用許可証を発行する利用許可証発行動作の一例を示すシーケンス図である。

[0034] 利用者端末 4 が管理装置 2 から受信した取引成立通知に含まれている取引情報の利用許可証取得可能時刻を経過したものとする（S 1 6 0）。利用者端末 4 は、この利用許可証取得可能時刻の経過を認識した利用者からログイン操作を受け付けると（S 1 6 1）、利用者のユーザ ID、パスワードを含むログイン要求を管理装置 2 に送信する（S 1 6 2）。これを受けて、管理装置 2 は、ログイン要求に含まれているパスワードと、このログイン要求に含まれているユーザ ID に紐付けて管理しているパスワードと、を用いて認証処理を実施する（S 1 6 3）。そして、認証成立ならば、ログイン要求の送信元である利用者端末 4 のログインを許可し、ログイン許可通知をこの利用者端末 4 に送信する（S 1 6 4）。

[0035] つぎに、利用者端末 4 は、この取引情報に含まれている取引 ID の指定を伴う利用許可証要求操作を、利用者から受け付けると（S 1 6 5）、この取引 ID を含む利用許可証要求を、管理装置 2 に送信する（S 1 6 6）。

[0036] これを受けて、管理装置 2 は、管理している取引情報のなかから利用許可証要求に含まれている取引 ID を有する取引情報を特定し、この取引情報に基づいて利用許可証の発行条件を満足していることを確認する（S 1 6 7）。具体的には、利用者端末 4 の利用者のユーザ ID が取引情報に含まれている利用者のユーザ ID と一致し、かつ取引情報に含まれている利用許可証取得可能時刻を経過していることを確認する。それから、管理装置 2 は、管理しているホールデータのなかから、取引情報に含まれているオブジェクト ID を有するホールデータを特定する。そして、特定したホールデータの共通

鍵を用いて取引情報を暗号化し、この暗号化された取引情報を含む利用許可証を発行する（S 1 6 8）。つぎに、管理装置 2 は、特定したホールデータに対応付けて管理している第 2 の秘密鍵を用いて、利用許可証に対する第 2 の署名を生成する（S 1 6 9）。その後、管理装置 2 は、利用許可証および第 2 の署名を利用者端末 4 に送信する（S 1 7 0）。

[0037] 図 6 は、本実施の形態に係る利用管理システムにおいて、利用制御装置 1 が利用対象物の利用制限を解除する利用制限解除動作の一例を示すシーケンス図である。

[0038] 利用者端末 4 が管理装置 2 から受信した取引成立通知に含まれている取引情報の利用に関する希望情報に含まれている利用可能開始時刻を経過したものとする（S 1 8 0）。利用者端末 4 は、利用者が利用サービスを希望する利用対象物（家屋 5 0）に設置された利用制御装置 1 と近距離無線通信 6 3 が可能な距離まで利用制御装置 1 に近づいた状態において、現在日時が取引情報の利用に関する希望情報に含まれている利用可能開始・終了時刻により特定される期間内であることを認識した利用者から利用操作を受け付けると（S 1 8 1）、利用制御装置 1 に管理装置 2 から受信した利用許可証および第 2 の署名を近距離無線通信 6 3 により送信する（S 1 8 2）。

[0039] これを受けて、利用制御装置 1 は、利用者端末 4 より受信した利用許可証と、自装置 1 に設定されているホールデータに含まれている第 2 の公開鍵とを用いて、利用者端末 4 より受信した第 2 の署名を検証する（S 1 8 3）。そして、署名検証に成功したならば、ホールデータに含まれている共通鍵を用いて利用許可証に含まれている暗号化された取引情報を復号化する（S 1 8 4）。

[0040] つぎに、利用制御装置 1 は、復号化した取引情報に含まれている利用に関する希望情報により特定される条件を満足していることを確認する（S 1 8 5）。具体的には、現在日時が利用に関する希望情報に含まれている利用可能開始・終了時刻により特定される期間内であることを確認する。また、取引情報の取引 I D に紐付けて管理している利用回数が利用に関する希望情報

に含まれている利用回数未満であることを確認する。それから、利用制御装置 1 は、利用に関する希望情報により特定される条件を満足していることを確認できたならば、利用対象物の利用制限を解除する（S 1 8 6）。ここでは、利用対象物である家屋 5 0 の出入口 5 1 のオートロック装置を解錠する。

[0041] その後、利用制御装置 1 は、利用者端末 4 に利用制限解除通知を近距離無線通信 6 3 により送信する（S 1 8 7）。それから、取引情報の取引 ID に紐付けて管理している利用回数を 1 つインクリメントする（S 1 8 8）。ここで、取引情報の取引 ID に紐付けて利用回数が管理されていないならば、利用回数「1」を取引情報の取引 ID に紐付けて管理する。

[0042] つぎに、本実施の形態に係る利用管理システムを構成する利用制御装置 1 および管理装置 2 の詳細を説明する。なお、提供者端末 3 および利用者端末 4 には、スマートホン、タブレット PC（Personal Computer）等の近距離無線通信機能を備えた既存のネットワーク端末を利用することができるので、これらの詳細な説明を省略する。

[0043] まず、利用制御装置 1 の詳細を説明する。

[0044] 図 7 は、利用制御装置 1 の概略機能構成図である。

[0045] 図示するように、利用制御装置 1 は、近距離無線通信部 1 0 と、設定情報等記憶部 1 1 と、オブジェクト設定部 1 2 と、ホール設定部 1 3 と、利用制限解除部 1 4 と、署名検証部 1 5 と、復号化部 1 6 と、を備えている。

[0046] 近距離無線通信部 1 0 は、IrDA デバイス、Bluetooth（登録商標）等の近距離無線通信 6 3 により、提供者端末 3 および利用者端末 4 と通信を行う。

[0047] 設定情報等記憶部 1 1 は、オブジェクト ID、第 1 の公開鍵、ホールデータ等の設定情報を記憶する。また、利用回数等、利用対象物の利用に関する条件を満足しているか否かを判断するために用いられる判断情報を記憶する。

[0048] オブジェクト設定部 1 2 は、提供者端末 3 より取得したオブジェクト ID

および第1の公開鍵を設定情報として設定情報等記憶部11に記憶する。

[0049] ホール設定部13は、提供者端末3よりホールデータとともに取得した第1の署名の検証が成立した場合に、このホールデータを設定情報として設定情報等記憶部11に記憶する。

[0050] 利用制限解除部14は、利用者端末4より利用許可証とともに取得した第2の署名の検証が成立し、かつ利用許可証に含まれている取引情報の利用に関する希望情報により特定される条件を満足している場合に、利用対象物の利用制限を解除する。本実施の形態では、家屋50の出入口51のオートロック装置に解錠命令を出力する。また、利用制限解除部14は、利用回数等の判断情報を設定情報等記憶部11に登録・更新する。

[0051] 署名検証部15は、ホール設定部13の指示に従い、設定情報等記憶部11に記憶されている第1の公開鍵を用いて、ホールデータに対する第1の署名を検証する。また、署名検証部15は、利用制限解除部14の指示に従い、設定情報等記憶部11に記憶されているホールデータに含まれている第2の公開鍵を用いて、利用許可証に対する第2の署名を検証する。

[0052] 復号化部16は、利用制限解除部14の指示に従い、設定情報等記憶部11に記憶されているホールデータに含まれている共通鍵を用いて、利用許可証に含まれている暗号化された取引情報を復号化する。

[0053] なお、図7に示す利用制御装置1の概略機能構成は、ASIC (Application Specific Integrated Circuit)、FPGA (Field Programmable Gate Array) 等の集積ロジックICによりハード的に実現されるものでもよいし、あるいはDSP (Digital Signal Processor) 等の計算機によりソフトウェア的に実現されるものでもよい。または、CPUと、メモリと、フラッシュメモリ、ハードディスクドライブ等の補助記憶装置と、IrDA通信装置、Bluetooth (登録商標) 通信装置等の近距離無線通信装置と、を備えた汎用コンピュータにおいて、CPUが所定のプログラムを補助記憶装置からメモリ上にロードして実行することにより

実現されるものでもよい。

- [0054] 図8は、利用制御装置1の動作を説明するためのフロー図である。
- [0055] オブジェクト設定部12は、近距離無線通信部10を介して提供者端末3よりオブジェクト登録通知を受信すると（S200でYES）、このオブジェクト登録通知に含まれているオブジェクトIDおよび第1の公開鍵を設定情報として設定情報等記憶部11に記憶する（S201）。
- [0056] また、ホール設定部13は、近距離無線通信部10を介して提供者端末3よりホールデータおよび第1の署名を受信すると（S202でYES）、このホールデータおよび第1の署名を署名検証部15に渡して、第1の署名の検証を依頼する。これを受けて、署名検証部15は、設定情報等記憶部11に記憶されている第1の公開鍵を用いて、ホールデータに対する第1の署名を検証する（S203）。具体的には、第1の公開鍵を用いて第1の署名を復号化し、その復号化情報が、ホールデータあるいはそのメッセージダイジェスト（ハッシュ値）と一致するか否かを判断することにより、第1の署名の正当性を検証する。
- [0057] つぎに、署名検証部15は、第1の署名の検証結果をホール設定部13に通知する。これを受けて、ホール設定部13は、第1の署名の検証に成功し、第1の署名の正当性を立証できたならば（S204でYES）、このホールデータを設定情報として設定情報等記憶部11に記憶する（S205）。一方、第1の署名の検証に失敗し、第1の署名の正当性を立証できなかったならば（S204でNO）、近距離無線通信部10を介して提供者端末3にエラーメッセージを送信する等の所定のエラー処理を実施する（S206）。
- [0058] また、利用制限解除部14は、近距離無線通信部10を介して利用者端末4より利用許可証および第2の署名を受信すると（S207でYES）、この利用許可証および第2の署名を署名検証部15に渡して、第2の署名の検証を指示する。これを受けて、署名検証部15は、設定情報等記憶部11に記憶されているホールデータに含まれている第2の公開鍵を用いて、利用許

可証に対する第2の署名を検証する（S208）。具体的には、第2の公開鍵を用いて第2の署名を復号化し、その復号化情報が、利用許可証あるいはそのメッセージダイジェストと一致するか否かを判断することにより、第2の署名の正当性を検証する。

[0059] つぎに、署名検証部15は、第2の署名の検証結果を利用制限解除部14に通知する。これを受けて、利用制限解除部14は、第2の署名の検証に成功し、第2の署名の正当性を立証できたならば（S209でYES）、この利用許可証に含まれている暗号化された取引情報を復号化部16に渡して復号化を指示する。一方、第2の署名の検証に失敗し、第2の署名の正当性を立証できなかったならば（S209でNO）、近距離無線通信部10を介して利用者端末4に、エラーメッセージを送信する等の所定のエラー処理を実施する（S214）。

[0060] つぎに、復号化部16は、利用制限解除部14より復号化の指示とともに暗号化された取引情報を受け取ったならば、設定情報等記憶部11に記憶されているホールデータに含まれている共通鍵を用いて、この暗号化された取引情報を復号化する（S210）。そして、復号化された取引情報を利用制限解除部14に渡す。

[0061] これを受けて、利用制限解除部14は、復号化された取引情報に含まれている利用に関する希望情報により特定される条件を満足しているか否かを判断する（S211）。具体的には、現在日時が利用に関する希望情報に含まれている利用可能開始・終了時刻により特定される期間内であるか否かを判断する。また、取引情報の取引IDに紐付けて設定情報等記憶部11に記憶されている利用回数が利用に関する希望情報に含まれている利用回数未満であるか否かを判断する。なお、取引情報の取引IDに紐付けて設定情報等記憶部11に記憶されている利用回数が存在しない場合は、この利用回数を「0」と判断する。

[0062] つぎに、利用制限解除部14は、取引情報に含まれている利用に関する希望情報により特定される条件を満足していると判断した場合（S211でY

ES)、利用対象物の利用制限を解除する(S212)。本実施の形態では、家屋50の出入口51のオートロック装置に解錠命令を出力する。また、利用制限解除部14は、取引情報の取引IDに紐付けて設定情報等記憶部11に記憶されている利用回数を更新する(S213)。ここで、取引情報の取引IDに紐付けられて設定情報等記憶部11に利用回数が登録されていないならば、利用回数「1」を取引情報の取引IDに紐付けて設定情報等記憶部11に登録する。

[0063] 一方、利用制限解除部14は、取引情報に含まれている利用に関する希望情報により特定される条件を満足していないと判断した場合(S211でNO)、近距離無線通信部10を介して利用者端末4に、エラーメッセージを送信する等の所定のエラー処理を実施する(S214)。

[0064] つぎに、管理装置2の詳細を説明する。

[0065] 図9は、管理装置2の概略機能構成図である。

[0066] 図示するように、管理装置2は、WANインターフェース部200と、記憶部201と、ユーザ管理部202と、オブジェクト管理部203と、ホール管理部204と、取引管理部205と、ログイン処理部206と、オブジェクト登録要求処理部207と、ホール生成要求処理部208と、取引認否問合せ部209と、取引要求処理部210と、利用許可証要求処理部211と、を備えている。

[0067] WANインターフェース部200は、WAN60に接続するためのインターフェースである。

[0068] 記憶部201は、利用者情報記憶部221と、提供者情報記憶部222と、オブジェクトデータ記憶部223と、ホールデータ記憶部224と、取引情報記憶部225と、を有する。

[0069] 利用者情報記憶部221には、利用者毎に利用者情報が記憶される。

[0070] 図10は、利用者情報記憶部221の登録内容例を模式的に表した図である。

[0071] 図示するように、利用者情報記憶部221には、利用者毎に利用者情報の

レコード２２１０が記憶されている。利用者情報のレコード２２１０は、利用者のユーザＩＤを登録するフィールド２２１１と、利用者のパスワードを登録するフィールド２２１２と、利用者端末４のＷＡＮ６０上のアドレス情報を登録するフィールド２２１３と、利用者の氏名、住所、連絡先等の個人情報登録するフィールド２２１４と、を有する。

[0072] 提供者情報記憶部２２２には、提供者毎に提供者情報が記憶される。

[0073] 図１１は、提供者情報記憶部２２２の登録内容例を模式的に表した図である。

[0074] 図示するように、提供者情報記憶部２２２には、提供者毎に提供者情報のレコード２２２０が記憶されている。提供者情報のレコード２２２０は、提供者のユーザＩＤを登録するフィールド２２２１と、提供者のパスワードを登録するフィールド２２２２と、提供者端末３のＷＡＮ６０上のアドレス情報を登録するフィールド２２２３と、提供者の氏名、住所、連絡先等の個人情報登録するフィールド２２２４と、を有する。

[0075] オブジェクトデータ記憶部２２３には、利用制御装置１毎にオブジェクトデータが記憶される。

[0076] 図１２は、オブジェクトデータ記憶部２２３の登録内容例を模式的に表した図である。

[0077] 図示するように、オブジェクトデータ記憶部２２３には、利用制御装置１毎にオブジェクトデータのレコード２２３０が記憶されている。オブジェクトデータのレコード２２３０は、識別子であるオブジェクトＩＤを登録するフィールド２２３１と、第１の公開鍵を登録するフィールド２２３２と、第１の秘密鍵を登録するフィールド２２３３と、利用対象物である家屋５０の物件名、住所等を含む施設情報を登録するフィールド２２３４と、この利用対象物の利用サービスを提供する提供者のユーザＩＤを登録するフィールド２２３５と、を有する。

[0078] ホールデータ記憶部２２４には、利用制御装置１毎にホールデータを含む情報が記憶される。

[0079] 図 1 3 は、ホールデータ記憶部 2 2 4 の登録内容例を模式的に表した図である。

[0080] 図示するように、ホールデータ記憶部 2 2 4 には、利用制御装置 1 毎にホールデータのレコード 2 2 4 0 が記憶されている。ホールデータのレコード 2 2 4 0 は、識別子であるホール ID を登録するフィールド 2 2 4 1 と、第 2 の公開鍵を登録するフィールド 2 2 4 2 と、第 2 の秘密鍵を登録するフィールド 2 2 4 3 と、共通鍵を登録するフィールド 2 2 4 4 と、ホールデータが設定される利用制御装置 1 に付与されたオブジェクト ID を登録するフィールド 2 2 4 5 と、を有する。ここで、フィールド 2 2 4 2、2 2 4 4、2 2 4 5 に登録されている第 2 の公開鍵、共通鍵、オブジェクト ID が利用制御装置 1 に設定されるホールデータを構成している。

[0081] 取引情報記憶部 2 2 5 には、提供者および利用者間で成立した利用対象物の利用サービスの取引毎に取引情報が記憶される。

[0082] 図 1 4 は、取引情報記憶部 2 2 5 の登録内容例を模式的に表した図である。

[0083] 図示するように、取引情報記憶部 2 2 5 には、利用サービスの取引毎に取引情報のレコード 2 2 5 0 が記憶されている。取引情報のレコード 2 2 5 0 は、識別子である取引 ID を登録するフィールド 2 2 5 6 と、利用サービスの取引対象となる利用対象物に設置された利用制御装置 1 に付与されたオブジェクト ID を登録するフィールド 2 2 5 1 と、利用者のユーザ ID を登録するフィールド 2 2 5 2 と、提供者のユーザ ID を登録するフィールド 2 2 5 3 と、利用可能開始・終了時刻、利用回数を含む、利用者の利用に関する希望情報を登録するフィールド 2 2 5 4 と、利用許可証を取得可能となる利用許可証取得可能時刻を登録するフィールド 2 2 5 5 と、を有する。

[0084] ユーザ管理部 2 0 2 は、利用者情報記憶部 2 2 1 を用いて利用者情報を管理するとともに、提供者情報記憶部 2 2 2 を用いて提供者情報を管理する。

[0085] オブジェクト管理部 2 0 3 は、オブジェクトデータ記憶部 2 2 3 を用いてオブジェクトデータを管理する。

- [0086] ホール管理部 204 は、ホールデータ記憶部 224 を用いてホールデータを管理する。
- [0087] 取引管理部 205 は、取引情報記憶部 225 を用いて取引情報を管理する。
- [0088] ログイン処理部 206 は、ユーザ管理部 202 と連携して、提供者端末 3 および利用者端末 4 から受信したログイン要求を処理する。
- [0089] オブジェクト登録要求処理部 207 は、オブジェクト管理部 203 と連携して、提供者端末 3 から受信したオブジェクト登録要求を処理する。
- [0090] ホール生成要求処理部 208 は、オブジェクト管理部 203 およびホール管理部 204 と連携して、提供者端末 3 から受信したホール生成要求を処理する。
- [0091] 取引認否問合せ部 209 は、取引要求処理部 210 の指示に従い、提供者端末 3 に、利用対象物の利用サービスの取引認否を問い合わせる。
- [0092] 取引要求処理部 210 は、取引管理部 205 および取引認否問合せ部 209 と連携して、利用者端末 4 から受信した取引要求を処理する。
- [0093] そして、利用許可証要求処理部 211 は、ホール管理部 204 および取引管理部 205 と連携して、利用者端末 4 から受信した利用許可証要求を処理する。
- [0094] なお、図 9 に示す管理装置 2 の概略機能構成は、ASIC、FPGA 等の集積ロジック IC によりハード的に実現されるものでもよいし、あるいは DSP 等の計算機によりソフトウェア的に実現されるものでもよい。または、CPU と、メモリと、フラッシュメモリ、ハードディスクドライブ等の補助記憶装置と、NIC (Network Interface Card) 等の通信装置と、を備えた汎用コンピュータにおいて、CPU が所定のプログラムを補助記憶装置からメモリ上にロードして実行することにより実現されるものでもよい。また、複数台の汎用コンピュータの連携からなる分散システム上に実現されるものでも構わない。
- [0095] 図 15 は、管理装置 2 の動作を説明するためのフロー図である。

- [0096] このフローは、WANインターフェース部200がWAN60を介して提供者端末3あるいは利用者端末4からログイン要求を受信することにより開始される。
- [0097] まず、WANインターフェース部200は、受信したログイン要求をログイン処理部206に通知する。これを受けて、ログイン処理部206は、ログイン処理を実施する(S300)。
- [0098] 具体的には、提供者端末3からログイン要求を受信した場合、このログイン要求に含まれている提供者のユーザIDの指定を伴うパスワード検索をユーザ管理部202に通知する。これを受けて、ユーザ管理部202は、ログイン処理部206により指定された提供者のユーザIDをキーにして、提供者情報記憶部222からレコード2220を検索する。そして、レコード2220を検出できたならば、このレコード2220に登録されているパスワードをログイン処理部206に通知し、レコード2220を検出できなかったならば、該当レコードが存在しない旨をログイン処理部206に通知する。一方、利用者端末4からログイン要求を受信した場合、このログイン要求に含まれている利用者のユーザIDの指定を伴うパスワード検索をユーザ管理部202に通知する。これを受けて、ユーザ管理部202は、ログイン処理部206により指定された利用者のユーザIDをキーにして、利用者情報記憶部221からレコード2210を検索する。そして、レコード2210を検出できたならば、このレコード2210に登録されているパスワードをログイン処理部206に通知し、レコード2210を検出できなかったならば、該当レコードが存在しない旨をログイン処理部206に通知する。ログイン処理部206は、ユーザ管理部202から受け取ったパスワードと受信したログイン要求に含まれているパスワードとが一致するならば、ログインを許可し(認証成立)、一致しないならば、あるいはユーザ管理部202から該当レコードが存在しない旨を通知されたならば、ログインを拒否する(認証不成立)。
- [0099] つぎに、ログイン処理部206は、ログイン認証が認証不成立である場合

(S301でNO)、WANインターフェース部200を介してログイン要求の送信元にエラーメッセージを送信する等の所定のエラー処理を実施する(S311)。一方、ログイン認証が認証成立である場合(S301でYES)、WANインターフェース部200を介してログイン要求の送信元にログイン許可通知を送信して、ログイン要求の送信元のログイン状態を管理するとともに、ログイン要求の送信元が提供者端末3であるならば(S302で「提供者」)、S303に進み、利用者端末4であるならば(S302で「利用者」)、S307に進む。

[0100] S303において、WANインターフェース部200は、ログインを許可した提供者端末3から要求が送られてくるのを待つ。そして、この提供者端末3から受信した要求がオブジェクト登録要求ならば(S304で「オブジェクト登録要求」)、このオブジェクト登録要求を、この提供者端末3から受信したログイン要求に含まれている提供者のユーザIDとともに、オブジェクト登録要求処理部207に通知して、後述のオブジェクト登録要求処理を実施し(S305)、ホール生成要求ならば(S304で「ホール生成要求」)、このホール生成要求を、この提供者端末3から受信したログイン要求に含まれている提供者のユーザIDとともに、ホール生成要求処理部208に通知して、後述のホール生成要求処理を実施する(S306)。

[0101] また、S307において、WANインターフェース部200は、ログインを許可した利用者端末4から要求が送られてくるのを待つ。そして、この利用者端末4から受信した要求が取引要求ならば(S308で「取引要求」)、この取引要求を、この利用者端末4から受信したログイン要求に含まれている利用者のユーザIDとともに、取引要求処理部210に通知して、後述の取引要求処理を実施し(S309)、利用許可証要求ならば(S308で「利用許可証要求」)、この利用許可証要求を、この利用者端末4から受信したログイン要求に含まれている利用者のユーザIDとともに、利用許可証要求処理部211に通知して後述の利用許可証要求処理を実施する(S310)。

- [0102] 図16は、図15に示すオブジェクト登録要求処理S305を説明するためのフロー図である。
- [0103] まず、オブジェクト登録要求処理部207は、オブジェクトIDを発行するとともに（S3050）、公開鍵暗号方式に従って第1の秘密鍵・公開鍵を生成する（S3051）。そして、オブジェクトIDおよび第1の秘密鍵・公開鍵と、オブジェクト登録要求に含まれている施設情報と、を含むオブジェクトデータを生成し、このオブジェクトデータを、提供者のユーザIDとともに、オブジェクト管理部203に通知して、オブジェクトデータの管理を指示する。
- [0104] これを受けて、オブジェクト管理部203は、オブジェクトデータ記憶部223にオブジェクトデータのレコード2230を追加して、このレコード2230にオブジェクトデータ（オブジェクトID、第1の公開鍵、第1の秘密鍵、施設情報）を提供者のユーザIDに紐付けて登録する（S3052）。それから、オブジェクト管理部203は、オブジェクトIDおよび第1の公開鍵をオブジェクト登録要求処理部207に通知する。
- [0105] つぎに、オブジェクト登録要求処理部207は、オブジェクト管理部203より通知されたオブジェクトIDおよび第1の公開鍵を含むオブジェクト登録通知を生成して、このオブジェクト登録通知をオブジェクト登録要求の送信元である提供者端末3に送信する（S3053）。
- [0106] 図17は、図15に示すホール生成要求処理S306を説明するためのフロー図である。
- [0107] まず、ホール生成要求処理部208は、ホールIDを発行する（S3060）。また、公開鍵暗号方式に従って第2の秘密鍵・公開鍵を生成するとともに（S3061）、共通鍵暗号方式に従って共通鍵を生成する（S3062）。
- [0108] つぎに、ホール管理部208は、ホール生成要求に含まれているオブジェクトID、第1の公開鍵、および共通鍵を含むホールデータを生成し、このホールデータを、ホールIDおよび第2の秘密鍵とともに、ホール管理部2

04に通知して、ホールデータの管理を指示する。これを受けて、ホール管理部204は、ホールデータ記憶部224にホールデータのレコード2240を追加して、このレコード2240にホールデータ（オブジェクトID、第2の公開鍵、共通鍵）をホールIDおよび第2の秘密鍵とともに登録する（S3063）。

[0109] つぎに、ホール生成要求処理部208は、ホール生成要求に含まれているオブジェクトIDをオブジェクト管理部203に通知して、第1の秘密鍵の検索を指示する。これを受けて、オブジェクト管理部203は、オブジェクトIDをキーにして、オブジェクトデータ記憶部223からオブジェクトデータのレコード2230を検索し、このレコード2230に含まれている第1の秘密鍵をホール生成要求処理部208に通知する。そして、ホール生成要求処理部208は、オブジェクト管理部203から通知された第1の秘密鍵を用いて、ホールデータに対する第1の署名を生成する（S3064）。

[0110] それから、ホール生成要求処理部208は、ホールデータを第1の署名とともに、ホール生成要求の送信元である提供者端末3に送信する（S3065）。

[0111] 図18は、図15に示す取引要求処理S309を説明するためのフロー図である。

[0112] まず、取引要求処理部210は、取引要求に含まれている提供者のユーザIDをユーザ管理部202に通知して、取引相手となる提供者の提供者端末3の特定を指示する。これを受けて、ユーザ管理部202は、提供者のユーザIDをキーにして、提供者情報記憶部222から提供者のレコード2220を検索する。そして、検出したレコード2220に含まれている提供者端末3のアドレス情報を取引要求処理部210に通知する（S3090）。

[0113] つぎに、取引要求処理部210は、取引要求に含まれている利用制御装置1のオブジェクトIDおよび利用対象物の利用に関する希望情報を、ユーザ管理部202から通知されたアドレス情報とともに、取引認否問合せ部209に通知して、取引認否の問合せを指示する。これを受けて、取引認否問合せ部209は、

せ部 209 は、利用制御装置 1 のオブジェクト ID および利用対象物の利用に関する希望情報を含む取引認否問合せを生成し、WAN インターフェース部 200 を介して、ユーザ管理部 202 から通知されたアドレス情報により特定される提供者端末 3 に、この取引認否問合せに送信する (S3091)。そして、提供者端末 3 から、この取引認否問合せに対する応答を受信したならば (S3092 で YES)、この受信した応答を取引要求処理部 210 に通知する。

[0114] つぎに、取引要求処理部 210 は、取引認否問合せに対する応答が取引拒否応答である場合 (S3093 で NO)、WAN インターフェース部 200 を介して取引要求の送信元である利用者端末 4 にエラーメッセージを送信する等の所定のエラー処理を実施する (S3097)。

[0115] 一方、取引要求処理部 210 は、取引認否問合せに対する応答が取引許諾応答である場合 (S3093 で YES)、取引成立と判断し、取引 ID を発行するとともに、取引要求に含まれている利用対象物の利用に関する希望情報の利用可能開始時刻に基づいて、利用許可証取得可能時刻を決定する (S3094)。例えば、利用許可証取得可能時刻を利用希望開始時刻の 24 時間前に決定する。

[0116] それから、取引要求処理部 210 は、取引 ID と、利用者のユーザ ID と、取引要求に含まれている提供者のユーザ ID、オブジェクト ID、および利用に関する希望情報と、利用許可証取得可能時刻と、を含む取引情報を生成する。そして、この生成した取引情報の管理を取引管理部 205 に指示する。これを受けて、取引管理部 205 は、取引情報記憶部 225 に取引情報のレコード 2250 を追加して、このレコード 2250 に取引情報 (取引 ID、オブジェクト ID、利用者のユーザ ID、提供者のユーザ ID、利用に関する希望情報、利用許可証取得可能時刻) を登録する (S3095)。

[0117] つぎに、取引要求処理部 210 は、利用許可証取得可能時刻を含む取引成立通知を取引要求の送信元である利用者端末 4 に送信する (S3096)。

[0118] 図 19 は、図 15 に示す利用許可証要求処理 S310 を説明するためのフ

ロー図である。

- [0119] まず、利用許可証要求処理部211は、利用許可証要求に含まれている取引IDを取引管理部205に通知して、取引情報の検索を指示する。これを受けて、取引管理部205は、取引IDをキーにして、取引情報記憶部225から取引情報のレコード2250を検索する。そして、このレコード2250に登録されている取引情報を利用許可証要求処理部211に通知する（S3100）。
- [0120] つぎに、利用許可証要求処理部211は、取引管理部205から通知された取引情報に含まれている利用者のユーザIDがログイン処理部206から通知された利用許可証要求の送信元である利用者端末4の利用者のユーザIDであることを確認するとともに、この取引情報に含まれている利用許可証取得可能時刻を経過していることを確認する（S3101）。
- [0121] 取引情報に含まれている利用者のユーザIDが利用許可証要求の送信元である利用者端末4の利用者のユーザIDでない場合、あるいは、取引情報に含まれている利用許可証取得可能時刻の経過前である場合（S3101でNO）、利用許可証要求処理部211は、WANインターフェース部200を介して利用許可証要求の送信元である利用者端末4にエラーメッセージを送信する等の所定のエラー処理を実施する（S3107）。
- [0122] 一方、取引情報に含まれている利用者のユーザIDが利用許可証要求の送信元である利用者端末4の利用者のユーザIDであり、かつ、取引情報に含まれている利用許可証取得可能時刻を経過している場合（S3101でYES）、利用許可証要求処理部211は、ホール管理部204に、取引情報に含まれているオブジェクトIDを通知して、共通鍵および第2の秘密鍵の検索を指示する。これを受けて、ホール管理部204は、オブジェクトIDをキーにして、ホールデータ記憶部224からホールデータのレコード2240を検索する。そして、検出したレコード2240に含まれている共通鍵および第2の秘密鍵を利用許可証要求処理部211に通知する（S3102）。
- 。

- [0123] つぎに、利用許可証要求処理部 211 は、ホール管理部 204 から通知された共通鍵を用いて取引情報を暗号化し（S3103）、この暗号化された取引情報を含む利用許可証を生成する（S3104）。そして、利用許可証要求処理部 211 は、ホール管理部 204 から通知された第 2 の秘密鍵を用いて、利用許可証に対する第 2 の署名を生成する（S3105）。
- [0124] つぎに、利用許可証要求処理部 211 は、利用許可証および第 2 の署名を利用許可証要求の送信元である利用者端末 4 に送信する（S3106）。
- [0125] 以上、本発明の一実施の形態を説明した。
- [0126] 本実施の形態において、利用制御装置 1 は、近距離無線通信 63 のみ通信可能であり、WAN60 から切り離されている。このため、利用制御装置 1 が WAN60 を介して外部から攻撃されることはない。また、利用対象物である家屋 50 の利用制限を解除するために用いる利用許可証は、ホールデータに含まれている第 2 の公開鍵を用いて、この利用許可証に付加されている第 2 の署名を検証することによりその正当性が証明され、さらに、ホールデータは、第 1 の公開鍵を用いて、このホールデータに付加されている第 1 の署名を検証することによりその正当性が証明される。したがって、本実施の形態によれば、セキュリティ上のリスクが低減される。
- [0127] また、本実施の形態では、利用許可証に含まれている取引情報の利用に関する希望情報を満足する場合にのみ、利用対象物の利用制限が解除され、満足しない場合には、利用対象物の利用制限は解除されない。このため、利用期限、利用回数等の条件を取引情報の利用に関する希望情報に含めておくことで、これらの条件に合致しない利用許可証は、たとえその正当性が証明されても無効となるので、利用対象物の利用者（利用者端末 4 の利用者）から利用許可証を返却してもらう必要がない。したがって、本実施の形態によれば、利便性が向上する。
- [0128] このように、本実施の形態によれば、利用対象物の利用管理において、利便性を向上させつつ、セキュリティ上のリスクを低減することができる。
- [0129] また、本実施の形態において、管理装置 2 は、取引情報に利用許可証取得

可能時刻を含めて管理しており、利用者端末4から利用許可証要求を受信した場合に、この利用許可証要求で指定されている取引IDにより特定される取引情報に含まれている利用許可証取得可能時刻を経過している場合に利用許可証を生成する。このように、利用許可証の取得可能時刻を制限することにより、利用許可証に対する改竄等が可能な機会を減らし、セキュリティをより向上させることができる。

[0130] また、本実施の形態において、管理装置2は、利用者端末4から利用要求を受信した場合に、この利用許可証に含まれている利用に関する希望情報を含む取引認否問合せを提供者端末3に送信する。そして、この取引認否問合せに対する応答として、提供者端末3から取引許諾応答を受信した場合に、取引情報を生成するとともに、この取引情報に含まれている利用許可証取得可能時刻を含む取引成立通知を利用者端末4に送信する。このため、提供者は、利用対象物の利用サービスの取引（提供）毎に、取引の意思を示すことができ、利用者は、取引成立の場合に利用許可証の取得可能時刻を知ることができる。したがって、利用対象物の利用サービスの提供者および利用者双方の利便性がさらに向上する。

[0131] なお、本発明は上記の実施の形態に限定されるものではなく、その要旨の範囲内で数々の変形が可能である。

[0132] 例えば、上記の実施の形態では、管理装置2と利用制御装置1との間で鍵共有した共通鍵を用いて、管理装置2は、利用者端末4に送信する利用許可証に含める取引情報を暗号化し、利用制御装置1は、利用者端末4から受信した利用許可証に含まれている暗号化された取引情報を復号化している。しかし、本発明はこれに限定されない。取引情報は、暗号化せずに、平文のまま、利用者端末4経由で管理装置2から利用制御装置1へ送信されるようにしてもよい。

[0133] また、上記の実施の形態では、取引情報に含める利用に関する希望情報として、利用可能開始・終了時刻および利用回数を用いた場合を例にとり説明した。しかし、本発明はこれに限定されない。利用に関する希望情報は、利

用対象物の利用制限の解除に関する条件を定めるものであればよく、利用可能開始・終了時刻および利用回数的一方のみを含むものでもよい。あるいは、利用可能開始・終了時刻および利用回数に代えて、あるいはそれら的一方に代えて、別の条件を含めてもよい。例えば、利用に関する希望情報に、利用可能開始・終了時刻と利用を許可するユーザのIDのリストとを含めてもよい。

[0134] 図20は、図1に示す利用管理システムの変形例の概略構成図である。

[0135] 図20に示す変形例が図1に示す利用管理システムと異なる点は、IDカード7およびカードリーダ8が追加されていること、および利用制御装置1に代えて利用制御装置1Aを設けたことである。その他の構成は、図1に示す利用管理システムと同様である。

[0136] IDカード7は、利用対象物（家屋50）の利用サービスを享受する利用者の家族、友人等の各関係者に配布され、それぞれに固有の許可IDが記憶されている。カードリーダ8は、利用制御装置1Aに接続され、IDカード7から読み込んだ許可IDを利用制御装置1Aに送信する。利用制御装置1Aは、カードリーダ8に接続するためのカードリーダインタフェース部を有する。その他の構成は、図7に示す利用制御装置1と同様である。

[0137] 図21は、図20に示す利用管理システムの変形例において、利用制御装置1Aが利用対象物の利用制限を解除する利用制限解除動作の一例を示すシーケンス図である。

[0138] なお、図20に示す利用管理システムの変形例において、オブジェクト登録動作およびホール設定動作は、図2および図3に示すオブジェクト登録動作およびホール設定動作と同様である。また、取引情報登録動作および利用許可証発行動作は、利用回数に代えて許可IDのリストが取引情報の利用に関する希望情報に含まれる点を除き、図4および図5に示す取引情報登録動作および利用許可証発行動作と同様である。したがって、これらの動作の詳細を省略する。

[0139] 利用者端末4が管理装置2から受信した取引成立通知に含まれている取引

情報の利用に関する希望情報に含まれている利用可能開始時刻を経過したものとする（S400）。利用者端末4は、利用者が利用サービスを希望する利用対象物（家屋50）に設置された利用制御装置1Aと近距離無線通信63が可能な距離まで利用制御装置1Aに近づいた状態において、現在日時が取引情報の利用に関する希望情報に含まれている利用可能開始・終了時刻により特定される期間内であることを認識した利用者から利用操作を受け付けると（S401）、利用制御装置1Aに管理装置2から受信した利用許可証および第2の署名を近距離無線通信63により送信する（S402）。

[0140] これを受けて、利用制御装置1Aは、自装置1Aに設定されているホールデータに含まれている第2の公開鍵を用いて、利用者端末4より受信した利用許可証に対する第2の署名を検証する（S403）。そして、署名検証に成功したならば、ホールデータに含まれている共通鍵を用いて利用許可証に含まれている暗号化された取引情報を復号化する（S404）。

[0141] つぎに、利用制御装置1Aは、復号化した取引情報に含まれている利用に関する希望情報を特定し、現在日時がこの希望情報に含まれている利用可能開始・終了時刻により特定される期間内であることを確認する（S405）。そして、現在日時がこの希望情報に含まれている利用可能開始・終了時刻により特定される期間内であることを確認したならば、利用対象物の利用制限解除の準備が整ったものと判断し（S406）、利用者端末4に利用制限解除準備通知を近距離無線通信63により送信する（S407）。

[0142] つぎに、カードリーダー8は、利用者の関係者（家族、友人等）からIDカード7に記憶されている許可IDを読み取らせる読取操作を受け付けると（S408）、読み取った許可IDを利用制御装置1Aに送信する（S409）。

[0143] これを受けて、利用制御装置1Aの利用制限解除部14は、現在日時が利用に関する希望情報に含まれている利用可能開始・終了時刻により特定される期間内であることを確認するとともに、カードリーダーインタフェース部を介してカードリーダー8から受信した許可IDが利用に関する希望情報に含ま

れている許可IDのリストに掲載されていることを確認する（S410）。そして、これらの満足していることを確認できたならば、利用対象物の利用制御を解除する（S411）。ここでは、利用対象物である家屋50の出入口51のオートロック装置を解錠する。

[0144] なお、上述の利用管理システムの変形例において、利用に関する希望情報に、利用を許可するユーザのIDのリストに代えて、利用を許可するユーザの指紋、静脈、虹彩等の生体認証情報を含めてもよい。この場合、図20において、IDカード7およびカードリーダ8に代えて、生体認証読取装置を利用制御装置1Aに接続する。また、図21のS408およびS409において、生体認証読取装置は、利用者の関係者（家族、友人等）から生体認証情報を読み取らせる読取操作を受け付けると、読み取った生体認証情報を利用制御装置1Aに送信する。そして、S410において、利用制御装置1Aの利用制限解除部14は、現在日時が利用に関する希望情報に含まれている利用可能開始・終了時刻により特定される期間内であることを確認するとともに、生体認証読取装置から受信した生体認証情報が利用に関する希望情報に含まれている生体認証情報のリストに登録されていることを確認する。

[0145] また、上記の実施の形態では、管理装置2に記憶部201を配置している。しかし、本発明はこれに限定されない。記憶部201は、WAN60に接続されたファイルサーバに保持させてもよい。この場合、利用者情報記憶部221、提供者情報記憶部222、オブジェクトデータ記憶部223、ホールデータ記憶部224、および取引情報記憶部225をそれぞれ別のファイルサーバに保持させてもよい。あるいは、それぞれを複数に分割して複数台のファイルサーバに分散保持させてもよい。また、これらの記憶部221～225に記憶される情報は、ブロックチェーン技術等を利用してその正当性が保証されていることが好ましい。

[0146] また、上記の実施の形態では、利用制御装置1、1Aを利用対象物である家屋50の出入口51に設置されたオートロック装置の解錠に用いる場合を例にとり説明したが、本発明はこれに限定されない。ホテル、旅館、民泊施

設、倉庫、部屋等を利用対象物とし、これらの出入口に設置されたオートロック装置の解錠に利用制御装置 1、1 A を用いてもよい。あるいは、自動車、自転車等の移動体を利用対象物とし、移動体のドアの解除あるいはイグニッションの始動に利用制御装置 1、1 A を用いてもよい。または、電子カルテ、電子書籍等の電子媒体の閲覧端末を利用対象物とし、電子媒体のアクセス制限の解除、あるいは暗号化された電子媒体の復号化に利用制御装置 1、1 A を用いてもよい。

符号の説明

- [0147] 1、1 A : 利用制御装置 2 : 管理装置 3 : 提供者端末
4 : 利用者端末 7 : IDカード 8 : カードリーダー
10 : 近距離無線通信部 11 : 設定情報等記憶部
12 : オブジェクト設定部 13 : ホール設定部
14 : 利用制限解除部 15 : 署名検証部 16 : 復号化部
50 : 家屋 51 : 出入口 60 : WAN 61 : 中継装置
62 : 無線ネットワーク 63 : 近距離無線通信
200 : WAN インターフェース部 201 : 記憶部
202 : ユーザ管理部 203 : オブジェクト管理部
204 : ホール管理部 205 : 取引管理部
206 : ログイン処理部 207 : オブジェクト登録要求処理部
208 : ホール生成要求処理部 209 : 取引認否問合せ部
210 : 取引要求処理部 211 : 利用許可証要求処理部
221 : 利用者情報記憶部 222 : 提供者情報記憶部
223 : オブジェクトデータ記憶部 224 : ホールデータ記憶部
225 : 取引情報記憶部