

## 請求の範囲

### [請求項1]

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

ことを特徴とする利用管理システム。

[請求項2]

請求項 1 に記載の利用管理システムであって、

前記管理装置において、

前記取引管理手段は、前記取引情報に利用許可証取得可能時刻を含めて管理し、

前記利用許可証処理手段は、前記利用者端末から前記取引情報の指定を伴う利用許可証要求を受信した場合に、前記取引管理手段により管理されている前記利用許可証要求で指定された前記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ならば、前記取引情報を含む前記利用許可証を生成するとともに、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

ことを特徴とする利用管理システム。

[請求項3]

請求項2に記載の利用管理システムであって、

前記管理装置は、

前記利用者端末から前記利用対象物の利用に関する条件を含む利用要求を受信した場合に、当該条件を含み、前記利用対象物の利用サービスの取引認否を問い合わせる取引認否問合せを前記提供者端末に送信する取引認否問合せ手段と、

前記取引認否問合せ手段により前記提供者端末に送信された前記取引認否問合せに対する応答として、前記提供者端末から取引許諾応答を受信した場合に、前記取引認否問合せに含まれている前記利用対象物の利用に関する条件および前記利用許可証取得可能時刻を含む前記取引情報を生成するとともに、当該利用許可証取得可能時刻を含む取引成立通知を前記利用者端末に送信する取引情報処理手段と、をさらに有する

ことを特徴とする利用管理システム。

[請求項4]

請求項1ないし3のいずれか一項に記載の利用管理システムであって、

前記管理装置において、

前記ホールデータ処理手段は、前記提供者端末から前記利用制御装置の指定を伴うホール生成要求を受信した場合に、前記第2の秘密鍵・公開鍵を生成するとともに、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、前記ホール生成要求に従い前記第2の公開鍵を含む前記ホールデータに対する前記第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

ことを特徴とする利用管理システム。

- [請求項5]           請求項 1 ないし 4 のいずれか一項に記載の利用管理システムであって、
- 前記管理装置において、
- 前記提供者端末から前記利用制御装置の指定を伴うオブジェクト登録要求を受信した場合に、前記第 1 の秘密鍵・公開鍵を生成するとともに、当該第 1 の公開鍵を含むオブジェクト登録通知を前記提供者端末に送信するオブジェクト登録要求処理手段をさらに有し、
- 前記提供者端末は、
- 前記管理装置から受信した前記オブジェクト登録通知を、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、
- 前記提供者端末から受信した前記オブジェクト登録通知に含まれている前記第 1 の公開鍵を登録する
- ことを特徴とする利用管理システム。
- [請求項6]           請求項 1 ないし 5 のいずれか一項に記載の利用管理システムであって、
- 前記管理装置において、
- 前記ホール管理手段は、前記利用制御装置に対応付けて共通鍵も管理しており、
- 前記ホールデータ処理手段は、前記ホールデータに前記共通鍵を含めて送信し、
- 前記利用許可証処理手段は、前記共通鍵を用いて、前記利用許可証に含める前記取引情報を暗号化し、
- 前記利用制御装置において、
- 前記取引情報取得手段は、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共通鍵を用いて、前記利用許可証に含まれている暗号化された前記取引情報を復号化する
- ことを特徴とする利用管理システム。

- [請求項7]           請求項1ないし6のいずれか一項に記載の利用管理システムであって、
- 前記利用制御装置に接続されたＩＤリーダーをさらに備え、
- 前記管理装置において、
- 前記取引管理手段は、前記利用対象物の利用に関する条件の一つとして、前記利用対象物の利用に必要な許可ＩＤのリストを含む前記取引情報を管理しており、
- 前記利用制御装置において、
- 前記解除手段は、前記ＩＤリーダーによってＩＤ記憶媒体から前記許可ＩＤが読み取られた場合に、当該許可ＩＤが前記取引情報取得手段により取得された前記取引情報により特定される条件に含まれている前記リストに掲載されており、かつ前記リスト以外の前記取引情報により特定される条件を満足しているならば、前記利用対象物の利用制限を解除すること
- ことを特徴とする利用管理システム。
- [請求項8]           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を管理する管理装置であって、
- 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、前記利用許可証の検証に必要な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、前記利

用制御装置に前記ホールデータを設定する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、前記利用制御装置に前記利用許可証を通知する利用者端末に送信する利用許可証処理手段と、を有する

ことを特徴とする管理装置。

[請求項9]

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であって、

近距離無線通信でのみ通信可能であり、

提供者端末から前記利用許可証の検証に必要なホールデータとともに受信した第1の署名を、予め登録されている第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、

利用者端末から前記利用許可証とともに受信した第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利用制限解除手段と、を有する

ことを特徴とする利用制御装置。

[請求項10]

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、を用いて、前記利用対象物の利用を管理する利用管理方法であって、

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とともに、前記利用制御装置に対応付けて、第１の秘密鍵・公開鍵および第２の秘密鍵・公開鍵を管理し、

前記第１の秘密鍵を用いて、前記第２の公開鍵を含む前記ホルダーデータに対する第１の署名を生成し、前記ホルダーデータおよび前記第１の署名を前記提供者端末に送信し、

前記第２の秘密鍵を用いて、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し、

前記提供者端末は、

前記管理装置から受信した前記ホルダー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ルダー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、前記ホルダーデータを自装置に設定し、

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ルダー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

ことを特徴とする利用管理方法。

[請求項11]

コンピュータで読み取り可能なプログラムであって、

前記プログラムは、前記コンピュータを、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を管理する管理装置として機能させ、

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、前記利用許可証の検証に必要な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、前記利用制御装置に前記ホールデータを設定する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、前記利用制御装置に前記利用許可証を通知する利用者端末に送信する利用許可証処理手段と、を有する

ことを特徴とするコンピュータで読み取り可能なプログラム。

[請求項12]

コンピュータで読み取り可能なプログラムであって、

前記プログラムは、前記コンピュータを、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して機能させ、

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、

提供者端末から前記利用許可証の検証に必要なホールデータとともに受信した第１の署名を、予め登録されている第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、

利用者端末から前記利用許可証とともに受信した第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

ことを特徴とするコンピュータで読み取り可能なプログラム。