(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2008-46723
(P2008-46723A)
(43)公開日　平成20年2月28日(2008.2.28)

(51)Int.Cl.		F I			テーマコード（参考）
G06K 17/00	(2006.01)	G06K	17/00	T	5B058
G06F 21/20	(2006.01)	G06K	17/00	L	5B285
		G06F	15/00	330G	
		G06F	15/00	330D	
		G06K	17/00	F	

審査請求 未請求　請求項の数 13　ＯＬ　（全 23 頁）

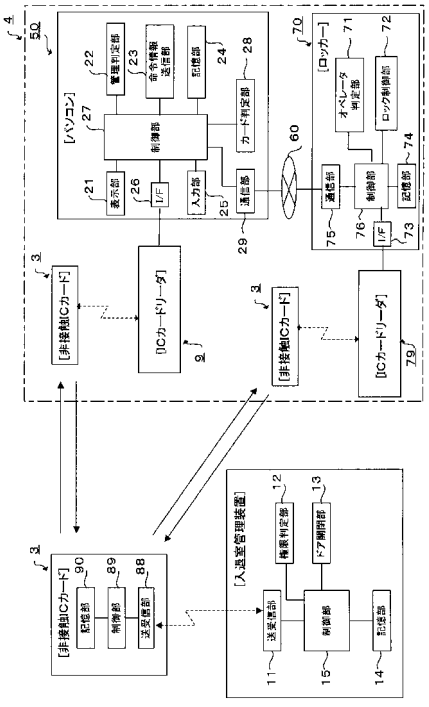
(21)出願番号　特願2006-219568 (P2006-219568)
(22)出願日　平成18年8月11日 (2006.8.11)

(71)出願人　000002897
大日本印刷株式会社
東京都新宿区市谷加賀町一丁目１番１号
(74)代理人　100107331
弁理士　中村　聡延
(74)代理人　100101203
弁理士　山下　昭彦
(74)代理人　100104499
弁理士　岸本　達人
(72)発明者　姉川　武彦
東京都新宿区市谷加賀町一丁目１番１号
大日本印刷株式会社内
(72)発明者　矢野　義博
東京都新宿区市谷加賀町一丁目１番１号
大日本印刷株式会社内

最終頁に続く

(54)【発明の名称】管理者端末、管理対象装置及び管理システム

(57)【要約】
【課題】管理者の手を煩わせることなく、簡易に、管理者が室内にいる間だけ自動的に電子機器や設備の利用が可能な管理システムを提供する。
【解決手段】管理システムにおいて管理者は、部屋４に入場とすると、ＩＣカードリーダ９に非接触ＩＣカード３ａを配置する。ＩＣカード３ａに管理権限情報が含まれている場合、パソコン５０は、ロッカー７０に利用許可情報を送信する。ロック制御部７２は、利用許可情報を受信すると、当該ロッカー７０を利用可能な状態に制御する。これによれば、ロック制御部７２は、管理者が部屋４に入室している場合のみ、当該ロッカー７０を利用可能な状態とするといった制御を、管理者の手を煩わせることなく自動的に行うことができる。
【選択図】図５



【特許請求の範囲】
【請求項１】
利用者が所持する情報記憶媒体を利用して、施設内に設置された管理対象装置の利用を管理する管理者端末であって、
前記管理者端末は、前記情報記憶媒体から情報を読み取る情報読取部を備え、ネットワークを介して前記管理対象装置と通信可能に接続されており、
前記情報記憶媒体は、前記利用者に応じて、前記利用者が管理者であることを示す管理権限情報を有しており、
前記管理者端末は、
前記情報読取部に配置された前記情報記憶媒体から情報を読み取る情報読取手段と、
前記情報読取手段が読み取った情報に前記管理権限情報が含まれているか否かを判定する管理判定手段と、
前記管理判定手段により前記管理権限情報が含まれていると判定された場合に、前記管理対象装置の利用を許可する利用許可情報を前記管理対象装置へ送信する利用許可情報送信手段と、を備えることを特徴とする管理者端末。
【請求項２】
前記情報読取部から前記情報記憶媒体が取り外されたか否かを判定する配置判定手段と、
前記配置判定手段により前記情報記憶媒体が取り外されたと判定された場合に、前記管理対象装置の利用を停止する利用停止情報を前記管理対象装置へ送信する利用停止情報送信手段と、をさらに備えることを特徴とする請求項１に記載の管理者端末。
【請求項３】
前記管理者端末は、情報を表示する表示部を備え、
前記管理対象装置から、前記管理対象装置を識別する種別と、前記管理対象装置を利用している利用者を識別する利用者識別情報とを利用状況情報として取得する利用状況情報取得手段と、
前記表示部により前記利用状況情報を表示する表示手段と、をさらに備えることを特徴とする請求項１又は２に記載の管理者端末。
【請求項４】
前記利用状況情報に基づいて、前記管理対象装置の利用を不許可とする利用者を指定する不許可利用者指定手段と、
前記利用状況情報に基づいて、前記不許可利用者指定手段が指定した利用者による利用を不許可とする管理対象装置を指定する不許可種別指定手段と、
前記不許可利用者指定手段が指定した利用者の識別情報と、前記不許可種別指定手段が指定した管理対象装置の種別とを不許可情報として前記管理対象装置に送信する不許可情報送信手段と、をさらに備えることを特徴とする請求項３に記載の管理者端末。
【請求項５】
施設内に設置され、管理権限を有する管理者が使用する管理者端末によって管理される管理対象装置であって、前記管理対象装置は、ネットワークを介して前記管理者端末と通信可能に接続されており、
前記管理者端末から、前記管理対象装置の利用を許可する利用許可情報を受信する利用許可情報受信手段と、
前記管理者端末から、前記管理対象装置の利用を停止する利用停止情報を受信する利用停止情報受信手段と、
前記利用許可情報受信手段が利用許可情報を受信した場合に前記管理対象装置が利用可能となるように制御し、前記利用停止情報受信手段が利用停止情報を受信した場合に前記管理対象装置が利用不可能となるように制御する制御手段と、を備えることを特徴とする管理対象装置。
【請求項６】
前記利用者は、各利用者を識別する識別情報を有する情報記憶媒体を所持しており、

前記管理対象装置は、前記情報記憶媒体から情報を読み取る情報読取部を備え、
前記情報読取部に配置された前記情報記憶媒体から情報を読み取る情報読取手段と、
情報読取手段が読み取った情報に含まれる識別情報を特定する識別情報特定手段と、
前記識別情報特定手段が特定した識別情報と、前記管理対象装置を識別する種別とを利用状況情報として前記管理者端末へ送信する利用状況情報送信手段と、をさらに備えることを特徴とする請求項５に記載の管理対象装置。
【請求項７】
前記管理者端末から、前記管理対象装置の利用を不許可とする利用者の識別情報と、当該利用者による利用を不許可とする管理対象装置の種別とを不許可情報として受信する不許可情報受信手段と、
前記識別情報特定手段が特定した識別情報と、前記不許可情報受信手段が受信した不許可情報に含まれる識別情報とが一致するか否かを判定する不許可利用者判定手段と、
前記管理対象装置の種別と、前記不許可情報受信手段が受信した不許可情報に含まれる種別とが一致するか否かを判定する不許可種別判定手段と、をさらに備え、
前記制御手段は、前記不許可利用者判定手段及び前記不許可種別判定手段の双方が一致した場合に、前記情報読取部に前記利用者が所持する情報記憶媒体が配置されている間は、前記管理対象装置を利用不可能となるように制御することを特徴とする請求項６に記載の管理対象装置。
【請求項８】
利用者が所持する情報記憶媒体を利用して、管理権限を有する管理者が使用する管理者端末により、施設内に設置された管理対象装置の利用を管理する管理システムであって、
前記管理システムは、前記管理者端末及び前記管理対象装置がネットワークを介して通信可能に接続されており、
前記情報記憶媒体は、前記利用者に応じて、前記利用者が管理者であることを示す管理権限情報を有しており、
前記管理者端末は、
前記情報読取部に配置された前記情報記憶媒体から情報を読み取る情報読取手段と、
前記情報読取手段が読み取った情報に前記管理権限情報が含まれているか否かを判定する管理判定手段と、
前記管理判定手段により前記管理権限情報が含まれていると判定された場合に、前記管理対象装置の利用を許可する利用許可情報を前記管理対象装置へ送信する利用許可情報送信手段と、を備え、
前記管理対象装置は、
前記管理者端末から、前記利用許可情報を受信する利用許可情報受信手段と、
前記利用許可情報受信手段が利用許可情報を受信した場合に前記管理対象装置が利用可能となるように制御する制御手段と、を備えることを特徴とする管理システム。
【請求項９】
前記管理者端末は、
前記情報読取部から前記情報記憶媒体が取り外されたか否かを判定する配置判定手段と、
前記配置判定手段により前記情報記憶媒体が取り外されたと判定された場合に、前記管理対象装置の利用を停止する利用停止情報を前記管理対象装置へ送信する利用停止情報送信手段と、をさらに備え、
前記管理対象装置は、
前記管理者端末から、前記利用停止情報を受信する利用停止情報受信手段をさらに備え、
前記制御手段は、前記利用停止情報受信手段が利用停止情報を受信した場合に前記管理対象装置が利用不可能となるように制御することを特徴とする請求項８に記載の管理システム。
【請求項１０】

前記利用者は、各利用者を識別する識別情報を有する情報記憶媒体を所持しており、
前記管理者端末は、
情報を表示する表示部と、
前記管理対象装置から、前記管理対象装置を識別する種別と、前記管理対象装置を利用している利用者を識別する利用者識別情報とを利用状況情報として取得する利用状況情報取得手段と、
前記表示部により前記利用状況情報を表示する表示手段と、をさらに備え、
前記管理対象装置は、
前記情報記憶媒体から情報を読み取る情報読取部と、
前記情報読取部に配置された前記情報記憶媒体から情報を読み取る情報読取手段と、
情報読取手段が読み取った情報に含まれる識別情報を特定する識別情報特定手段と、
前記識別情報特定手段が特定した識別情報と、前記管理対象装置を識別する種別とを利用状況情報として前記管理者端末へ送信する利用状況情報送信手段と、をさらに備えることを特徴とする請求項８又は９に記載の管理システム。
【請求項１１】
前記管理者端末は、
前記利用状況情報に基づいて、前記管理対象装置の利用を不許可とする利用者を指定する不許可利用者指定手段と、
前記利用状況情報に基づいて、前記不許可利用者指定手段が指定した利用者による利用を不許可とする管理対象装置を指定する不許可種別指定手段と、
前記不許可利用者指定手段が指定した利用者の識別情報と、前記不許可種別指定手段が指定した管理対象装置の種別とを不許可情報として前記管理対象装置に送信する不許可情報送信手段と、をさらに備え、
前記管理対象装置は、
前記管理者端末から、前記不許可情報として受信する不許可情報受信手段と、
前記識別情報特定手段が特定した識別情報と、前記不許可情報受信手段が受信した不許可情報に含まれる識別情報とが一致するか否かを判定する不許可利用者判定手段と、
前記管理対象装置の種別と、前記不許可情報受信手段が受信した不許可情報に含まれる種別とが一致するか否かを判定する不許可種別判定手段と、をさらに備え、
前記制御手段は、前記不許可利用者判定手段及び前記不許可種別判定手段の双方が一致すると判定した場合に、前記情報読取部に前記利用者が所持する情報記憶媒体が配置されている間は、前記管理対象装置を利用不可能となるように制御することを特徴とする請求項１０に記載の管理システム。
【請求項１２】
利用者が所持する情報記憶媒体を利用して、施設内に設置された管理対象装置の利用を管理するコンピュータにより実行されるプログラムであって、
前記コンピュータは、前記情報記憶媒体から情報を読み取る情報読取部を備え、ネットワークを介して前記管理対象装置と通信可能に接続されており、
前記情報記憶媒体は、前記利用者に応じて、前記利用者が管理者であることを示す管理権限情報を有しており、
前記プログラムは、
前記情報読取部に配置された前記情報記憶媒体から情報を読み取る情報読取手段、
前記情報読取手段が読み取った情報に前記管理権限情報が含まれているか否かを判定する管理判定手段、
前記管理判定手段により前記管理権限情報が含まれていると判定された場合に、前記管理対象装置の利用を許可する利用許可情報を前記管理対象装置へ送信する利用許可情報送信手段、として前記コンピュータを機能させることを特徴とするプログラム。
【請求項１３】
施設内に設置され、管理権限を有する管理者が使用する管理者端末によって管理されるコンピュータにより実行されるプログラムであって、

前記コンピュータは、ネットワークを介して前記管理者端末と通信可能に接続されており、
前記管理者端末から、前記コンピュータの利用を許可する利用許可情報を受信する利用許可情報受信手段、
前記管理者端末から、前記コンピュータの利用を停止する利用停止情報を受信する利用停止情報受信手段、
前記利用許可情報受信手段が利用許可情報を受信した場合に前記コンピュータが利用可能となるように制御し、前記利用停止情報受信手段が利用停止情報を受信した場合に前記コンピュータが利用不可能となるように制御する制御手段、として前記コンピュータを機能させることを特徴とするプログラム。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、入室が管理された施設内の部屋などに備えられた電子機器や設備などの管理対象物の利用を管理する管理システムに関する。
【背景技術】
【０００２】
所定の室内にある電子機器や設備をオペレータが利用する際、情報漏洩防止等の観点から、管理者が当該室内にいることが条件となる場合がある。この場合、オペレータが電子機器や設備を利用するためには、「入室した管理者が電子機器や設備を利用可能な状態とする」、「電子機器や設備を利用する際に、オペレータが管理者に申し出て、管理者が当該電子機器等を利用可能な状態とする」、「電子機器や設備を利用する際に、オペレータが管理者から当該電子機器等を利用可能にする媒体を受け取り、オペレータが当該電子機器等を利用可能な状態とする」などの方法がとられている。同様に、電子機器や設備の利用を停止させるためには、「管理者が電子機器や設備を利用停止の状態にする」などの方法がとられている。
【０００３】
しかし、従来の方法では、電子機器や設備を利用可能な状態又は利用停止の状態にするため、管理者自らがその都度対応する必要がある。そのため、電子機器や設備の数が多い場合、管理者に多大な負担がかかるという問題が生じていた。
【０００４】
一方、従来、使用権限を有しない第三者によるコンピュータの不正使用を防止するためのセキュリティ技術として、ＩＣカード等の情報記憶媒体を用いたものが既に知られている。その一例では、コンピュータが使用される際に、予め本人を認証するための識別情報を記憶させたＩＣカード等の情報記憶媒体から識別情報を読み取り、その読み取った識別情報に基づいた照合処理により本人認証を行い、その認証が成立した場合にコンピュータの使用を可能とする（例えば、特許文献１及び２を参照）。
【０００５】
【特許文献１】特開２００３－３０１５５号公報
【特許文献２】特開２００４－７０５４２号公報
【発明の開示】
【発明が解決しようとする課題】
【０００６】
本発明は、以上の点に鑑みてなされたものであり、情報記憶媒体を使用して、管理者の手を煩わせることなく、簡易に、管理者が室内にいる間だけ自動的に電子機器や設備の利用が可能となる管理システムを提供することを課題とする。
【課題を解決するための手段】
【０００７】
本発明の１つの観点では、利用者が所持する情報記憶媒体を利用して、施設内に設置された管理対象装置の利用を管理する管理者端末であって、前記管理者端末は、前記情報記

憶媒体から情報を読み取る情報読取部を備え、ネットワークを介して前記管理対象装置と通信可能に接続されており、前記情報記憶媒体は、前記利用者に応じて、前記利用者が管理者であることを示す管理権限情報を有しており、前記管理者端末は、前記情報読取部に配置された前記情報記憶媒体から情報を読み取る情報読取手段と、前記情報読取手段が読み取った情報に前記管理権限情報が含まれているか否かを判定する管理判定手段と、前記管理判定手段により前記管理権限情報が含まれていると判定された場合に、前記管理対象装置の利用を許可する利用許可情報を前記管理対象装置へ送信する利用許可情報送信手段と、を備える。

【０００８】

上記のように構成された管理者端末は、管理権限を有する者が施設内にいる間だけ自動的に管理対象装置の利用を可能とするものである。施設としては、例えばビルなどの建物、そのフロア、部屋などが挙げられる。また、管理対象装置としては、例えばパソコン、プリンタなどの電子機器、電子制御機能を有するタイムレコーダ、キャビネット、ロッカーなどの設備、及び、建物内部の部屋などが挙げられる。また、管理者端末としては、例えばパソコンなど、管理対象装置の利用状態を制御することが可能な端末などが挙げられる。施設内において、管理対象装置と管理者端末とは、インターネットをはじめとするネットワークを介して通信可能に接続されている。また、便宜上、管理者端末を使用し、管理者権限を有する利用者を「管理者」と呼び、管理対象装置を利用し、管理者権限を有さない利用者を「オペレータ」と呼ぶ。

【０００９】

本システムでは、利用者は情報記憶媒体を所持し、当該情報記憶媒体から読み取った情報に基づいて管理者端末が管理対象装置の利用状態を管理している。情報記憶媒体としては、例えばＩＣカード、携帯電話等に搭載されたＩＣチップやＵＩＭ（User Identity Module）など、情報の読み取りが可能な媒体が使用される。具体的に、本システムでは、施設内に１つ又は複数の管理対象装置及び管理者端末が設けられている。管理者は、施設内に入場とすると、管理者端末の情報読取部に自身が所持する情報記憶媒体を配置する。ここで、情報読取部とは、例えば管理者端末に接続されたＩＣカードリーダ等である。管理者端末は、情報読取部に配置された情報記憶媒体から情報を読み取り、当該情報に管理対象装置を管理することができる管理権限情報が含まれているか否かを判定する。管理権限情報が含まれている場合、管理者端末は、当該管理者端末を起動すると共に、ネットワークを介して管理対象装置に利用許可情報を送信する。利用許可情報とは、管理対象装置をオペレータによって利用可能な状態とすることを求める情報である。管理対象装置は、ネットワークを介して管理者端末から利用許可情報を受信すると、当該管理対象装置をオペレータによって利用可能な状態に制御する。つまり、施設内に設置された管理者端末を管理者が使用している場合、自動的に管理対象装置はオペレータによって利用可能な状態となる。よって、管理対象装置は、管理者が施設に入場している場合のみ、当該管理対象装置を利用可能な状態とするといった制御を、管理者の手を煩わせることなく自動的に行うことができる。

【００１０】

上記管理者端末の一態様では、前記情報読取部から前記情報記憶媒体が取り外されたか否かを判定する配置判定手段と、前記配置判定手段により前記情報記憶媒体が取り外されたと判定された場合に、前記管理対象装置の利用を停止する利用停止情報を前記管理対象装置へ送信する利用停止情報送信手段と、をさらに備える。これによれば、管理者端末に接続されたＩＣカードリーダから情報記憶媒体であるＩＣカードが取り外された場合に、自動的に利用停止情報が管理対象装置に送信される。よって、管理対象装置は、利用停止情報に基づいて、オペレータによる利用を不可能な状態に制御することができる。つまり、管理者が、管理者端末の使用を中止して施設から退場した場合、管理対象装置は、管理者の手を煩わせることなく、自動的に利用不可能な状態に制御することができる。

【００１１】

上記管理者端末の他の一態様では、前記管理者端末は、情報を表示する表示部を備え、

前記管理対象装置から、前記管理対象装置を識別する種別と、前記管理対象装置を利用している利用者を識別する利用者識別情報とを利用状況情報として取得する利用状況情報取得手段と、前記表示部により前記利用状況情報を表示する表示手段と、をさらに備える。この場合、管理対象装置は、予め記憶部等に自身を利用するオペレータの識別情報を記憶している。そして、管理対象装置は、所定のタイミングで、当該管理対象装置を識別する種別と、記憶部に記憶した識別情報とを対応付けて利用状況情報として送信する。管理者端末は、ネットワークを介して管理対象装置から受信した利用状況情報を表示部に表示する。これにより、管理者端末は、どのオペレータがどの管理対象装置を利用しているかといった利用状況を容易に把握することが可能となる。

【００１２】

上記管理者端末のさらに他の一態様では、前記利用状況情報に基づいて、前記管理対象装置の利用を不許可とする利用者を指定する不許可利用者指定手段と、前記利用状況情報に基づいて、前記不許可利用者指定手段が指定した利用者による利用を不許可とする管理対象装置を指定する不許可種別指定手段と、前記不許可利用者指定手段が指定した利用者の識別情報と、前記不許可種別指定手段が指定した管理対象装置の種別とを不許可情報として前記管理対象装置に送信する不許可情報送信手段と、をさらに備える。

【００１３】

上記のように構成された管理者端末は、表示部に表示された利用状況情報に基づいて、管理対象装置を利用できないようにする不許可利用者と、不許可利用者により利用できない管理対象装置の種別である不許可種別とを任意に指定する。そして、管理者端末は、不許可利用者と、不許可種別とに関する情報を不許可情報として、ネットワークを介して管理対象装置へ送信する。管理対象装置は、受信した不許可情報に基づいて、不許可利用者が不許可種別の管理対象装置を利用しようとした場合に、当該管理対象装置を利用不可能な状態に制御する。つまり、管理対象装置は、利用許可情報を予め受信しており、既に利用可能な状態になっていたとしても、不許可利用者が不許可種別の管理対象装置を利用使用とした場合は、当該管理対象装置を利用不可能な状態に制御する。これにより、管理者が任意に指定したオペレータによる管理対象装置の利用を制限することが可能となる。よって、例えば、管理対象装置を長時間利用しているオペレータ等に対して利用を制限することで、間接的に警告を行ったり、不正利用を防止したりすることができる。

【００１４】

本発明の別の観点では、施設内に設置され、管理権限を有する管理者が使用する管理者端末によって管理される管理対象装置であって、前記管理対象装置は、ネットワークを介して前記管理者端末と通信可能に接続されており、前記管理者端末から、前記管理対象装置の利用を許可する利用許可情報を受信する利用許可情報受信手段と、前記管理者端末から、前記管理対象装置の利用を停止する利用停止情報を受信する利用停止情報受信手段と、前記利用許可情報受信手段が利用許可情報を受信した場合に前記管理対象装置が利用可能となるように制御し、前記利用停止情報受信手段が利用停止情報を受信した場合に前記管理対象装置が利用不可能となるように制御する制御手段と、を備える。

【００１５】

上記のように構成された管理対象装置において、管理者は、施設内に入場とすると、管理者端末の情報読取部に自身が所持する情報記憶媒体を配置する。管理者端末は、情報読取部に配置された情報記憶媒体から情報を読み取り、当該情報に管理対象装置を管理することができる管理権限情報が含まれているか否かを判定する。管理権限情報が含まれている場合、管理者端末は、当該管理者端末を起動すると共に、ネットワークを介して管理対象装置に利用許可情報を送信する。管理対象装置は、ネットワークを介して管理者端末から利用許可情報を受信すると、当該管理対象装置をオペレータによって利用可能な状態に制御する。つまり、施設に入場して設置された管理者端末を管理者が使用している場合、自動的に管理対象装置はオペレータによって利用可能な状態となる。

【００１６】

また、管理者端末は、情報読取部から情報記憶媒体が取り外された場合、ネットワーク

を介して管理対象装置に利用停止情報を送信する。管理対象装置は、ネットワークを介して管理者端末から利用停止情報を受信すると、当該管理対象装置をオペレータによって利用不可能な状態に制御する。つまり、管理者が管理者端末から離れて施設から退場した場合、自動的に管理対象装置はオペレータによって利用不可能な状態となる。よって、情報記憶媒体を使用して、管理者の手を煩わせることなく、簡易に、管理者が施設内にいる間だけ自動的に管理対象装置の利用を可能とすることができる。

【００１７】

上記管理対象装置の一態様では、前記利用者は、各利用者を識別する識別情報を有する情報記憶媒体を所持しており、前記管理対象装置は、前記情報記憶媒体から情報を読み取る情報読取部を備え、前記情報読取部に配置された前記情報記憶媒体から情報を読み取る情報読取手段と、情報読取手段が読み取った情報に含まれる識別情報を特定する識別情報特定手段と、前記識別情報特定手段が特定した識別情報と、前記管理対象装置を識別する種別とを利用状況情報として前記管理者端末へ送信する利用状況情報送信手段と、をさらに備える。これによれば、管理対象装置は、オペレータが所持する情報記憶媒体に含まれる情報に基づいて、当該オペレータを識別する識別情報を特定する。そして、管理対象装置は、特定した識別情報と、当該管理対象装置を識別する種別とを利用状況情報として、ネットワークを介し管理者端末へ送信する。管理者端末は、利用状況情報に基づいて、どのオペレータがどの管理対象装置を利用しているかを容易に把握することが可能となる。

【００１８】

上記管理対象装置の他の一態様では、前記管理者端末から、前記管理対象装置の利用を不許可とする利用者の識別情報と、当該利用者による利用を不許可とする管理対象装置の種別とを不許可情報として受信する不許可情報受信手段と、前記識別情報特定手段が特定した識別情報と、前記不許可情報受信手段が受信した不許可情報に含まれる識別情報とが一致するか否かを判定する不許可利用者判定手段と、前記管理対象装置の種別と、前記不許可情報受信手段が受信した不許可情報に含まれる種別とが一致するか否かを判定する不許可種別判定手段と、をさらに備え、前記制御手段は、前記不許可利用者判定手段及び前記不許可種別判定手段の双方が一致した場合に、前記情報読取部に前記利用者が所持する情報記憶媒体が配置されている間は、前記管理対象装置を利用不可能となるように制御する。

【００１９】

上記のように構成された管理対象装置において、管理者端末は、管理対象装置を利用できないようにする不許可利用者と、不許可利用者により利用できない管理対象装置の種別である不許可種別とを任意に指定する。そして、管理者端末は、不許可利用者と、不許可種別とに関する情報を不許可情報として、ネットワークを介して管理対象装置へ送信する。管理対象装置は、受信した不許可情報に基づいて、不許可利用者が不許可種別の管理対象装置を利用しようとした場合に、当該管理対象装置を利用不可能な状態に制御する。つまり、管理対象装置は、利用許可情報を予め受信しており、既に利用可能な状態になっていたとしても、不許可利用者が不許可種別の管理対象装置を利用使用とした場合は、当該管理対象装置を利用不可能な状態に制御する。これにより、管理者が任意に指定したオペレータによる管理対象装置の利用を制限することが可能となる。よって、例えば、管理対象装置を長時間利用しているオペレータ等に対して利用を制限することで、間接的に警告を行ったり、不正利用を防止したりすることができる。

【００２０】

本発明の別の観点では、利用者が所持する情報記憶媒体を利用して、管理権限を有する管理者が使用する管理者端末により、施設内に設置された管理対象装置の利用を管理する管理システムであって、前記管理システムは、前記管理者端末及び前記管理対象装置がネットワークを介して通信可能に接続されており、前記情報記憶媒体は、前記利用者に応じて、前記利用者が管理者であることを示す管理権限情報を有しており、前記管理者端末は、前記情報読取部に配置された前記情報記憶媒体から情報を読み取る情報読取手段と、前記情報読取手段が読み取った情報に前記管理権限情報が含まれているか否かを判定する管

理判定手段と、前記管理判定手段により前記管理権限情報が含まれていると判定された場合に、前記管理対象装置の利用を許可する利用許可情報を前記管理対象装置へ送信する利用許可情報送信手段と、を備え、前記管理対象装置は、前記管理者端末から、前記利用許可情報を受信する利用許可情報受信手段と、前記利用許可情報受信手段が利用許可情報を受信した場合に前記管理対象装置が利用可能となるように制御する制御手段と、を備える。これによれば、情報記憶媒体を使用して、管理者の手を煩わせることなく、簡易に、管理者が施設内にいる間だけ自動的に管理対象装置の利用を可能とすることができる。

【００２１】

上記管理システムの一態様では、前記管理者端末は、前記情報読取部から前記情報記憶媒体が取り外されたか否かを判定する配置判定手段と、前記配置判定手段により前記情報記憶媒体が取り外されたと判定された場合に、前記管理対象装置の利用を停止する利用停止情報を前記管理対象装置へ送信する利用停止情報送信手段と、をさらに備え、前記管理対象装置は、前記管理者端末から、前記利用停止情報を受信する利用停止情報受信手段をさらに備え、前記制御手段は、前記利用停止情報受信手段が利用停止情報を受信した場合に前記管理対象装置が利用不可能となるように制御する。これによれば、管理者が、管理者端末の使用を中止して施設から退場した場合、管理対象装置は、管理者の手を煩わせることなく、自動的に利用不可能な状態に制御することができる。

【００２２】

上記管理システムの他の一態様では、前記利用者は、各利用者を識別する識別情報を有する情報記憶媒体を所持しており、前記管理者端末は、情報を表示する表示部と、前記管理対象装置から、前記管理対象装置を識別する種別と、前記管理対象装置を利用している利用者を識別する利用者識別情報とを利用状況情報として取得する利用状況情報取得手段と、前記表示部により前記利用状況情報を表示する表示手段と、をさらに備え、前記管理対象装置は、前記情報記憶媒体から情報を読み取る情報読取部と、前記情報読取部に配置された前記情報記憶媒体から情報を読み取る情報読取手段と、情報読取手段が読み取った情報に含まれる識別情報を特定する識別情報特定手段と、前記識別情報特定手段が特定した識別情報と、前記管理対象装置を識別する種別とを利用状況情報として前記管理者端末へ送信する利用状況情報送信手段と、をさらに備える。これによれば、管理者は、管理者端末に表示される利用状況情報に基づいて、どのオペレータがどの管理対象装置を利用しているかを容易に把握することが可能となる。

【００２３】

上記管理システムのさらに他の一態様では、前記管理者端末は、前記利用状況情報に基づいて、前記管理対象装置の利用を不許可とする利用者を指定する不許可利用者指定手段と、前記利用状況情報に基づいて、前記不許可利用者指定手段が指定した利用者による利用を不許可とする管理対象装置を指定する不許可種別指定手段と、前記不許可利用者指定手段が指定した利用者の識別情報と、前記不許可種別指定手段が指定した管理対象装置の種別とを不許可情報として前記管理対象装置に送信する不許可情報送信手段と、をさらに備え、前記管理対象装置は、前記管理者端末から、前記不許可情報として受信する不許可情報受信手段と、前記識別情報特定手段が特定した識別情報と、前記不許可情報受信手段が受信した不許可情報に含まれる識別情報とが一致するか否かを判定する不許可利用者判定手段と、前記管理対象装置の種別と、前記不許可情報受信手段が受信した不許可情報に含まれる種別とが一致するか否かを判定する不許可種別判定手段と、をさらに備え、前記制御手段は、前記不許可利用者判定手段及び前記不許可種別判定手段の双方が一致すると判定した場合に、前記情報読取部に前記利用者が所持する情報記憶媒体が配置されている間は、前記管理対象装置を利用不可能となるように制御する。これによれば、管理者が任意に指定したオペレータによる管理対象装置の利用を制限することが可能となる。

【００２４】

本発明の別の観点では、利用者が所持する情報記憶媒体を利用して、施設内に設置された管理対象装置の利用を管理するコンピュータにより実行されるプログラムであって、前記コンピュータは、前記情報記憶媒体から情報を読み取る情報読取部を備え、ネットワー

クを介して前記管理対象装置と通信可能に接続されており、前記情報記憶媒体は、前記利用者に応じて、前記利用者が管理者であることを示す管理権限情報を有しており、前記プログラムは、前記情報読取部に配置された前記情報記憶媒体から情報を読み取る情報読取手段、前記情報読取手段が読み取った情報に前記管理権限情報が含まれているか否かを判定する管理判定手段、前記管理判定手段により前記管理権限情報が含まれていると判定された場合に、前記管理対象装置の利用を許可する利用許可情報を前記管理対象装置へ送信する利用許可情報送信手段、として前記コンピュータを機能させる。

【００２５】

上記プログラムをコンピュータにより実行することにより、上述の管理者端末を実現することができる。また、上述の管理者端末の各態様も同様に実現することができる。

【００２６】

本発明のさらに別の観点では、施設内に設置され、管理権限を有する管理者が使用する管理者端末によって管理されるコンピュータにより実行されるプログラムであって、前記コンピュータは、ネットワークを介して前記管理者端末と通信可能に接続されており、前記管理者端末から、前記コンピュータの利用を許可する利用許可情報を受信する利用許可情報受信手段、前記管理者端末から、前記コンピュータの利用を停止する利用停止情報を受信する利用停止情報受信手段、前記利用許可情報受信手段が利用許可情報を受信した場合に前記コンピュータが利用可能となるように制御し、前記利用停止情報受信手段が利用停止情報を受信した場合に前記コンピュータが利用不可能となるように制御する制御手段、として前記コンピュータを機能させる。

【００２７】

上記プログラムをコンピュータにより実行することにより、上述の管理対象装置を実現することができる。また、上述の管理対象装置の各態様も同様に実現することができる。

【発明の効果】

【００２８】

本発明によれば、情報記憶媒体を使用して、管理者の手を煩わせることなく、簡易に、管理者が室内にいる間だけ自動的に電子機器や設備の利用が可能となる。

【発明を実施するための最良の形態】

【００２９】

以下、図面を参照して本発明の好適な実施の形態について説明する。

【００３０】

本発明は、情報記憶媒体を使用して、管理者の手を煩わせることなく、施設内に備えられた管理対象装置の利用を管理するものである。ここで、情報記憶媒体とは、例えばＩＣカード、携帯電話等に搭載されたＩＣチップやＵＩＭ（User Identity Module）などである。なお、本実施形態では、ＩＣカードを使用するものとする。

【００３１】

本実施形態において電子機器の利用を管理する管理システムの概要を図１に示す。なお、本発明における施設とは、例えば、部屋、ビル、ビル内のフロア、特定場所、特定エリア、特定領域、特定地域、などが含まれるが、本実施形態の説明においては、一例として電子機器が備えられている部屋について説明する。

【００３２】

部屋４の内部に備えられた電子機器であるロッカー７０は、室内に電子機器の管理権限を有する管理者１がいる間のみ、オペレータ２が利用することが可能となる。具体的に、部屋４の内部には、管理者１が使用する管理者端末としてパソコン５０が設置されており、管理者１がパソコン５０を使用している間のみ、オペレータ２がロッカー７０を利用することができる。パソコン５０及びロッカー７０は、インターネットをはじめとするネットワーク６０を介して、通信可能に接続されている。

【００３３】

管理者１は、部屋４への入室権限及びロッカー７０の管理権限を有しており、情報記憶媒体である非接触ＩＣカード３ａを所持している。一方、オペレータ２は、部屋４への入

室権限を有しており、情報記憶媒体である非接触ＩＣカード３ｂを所持している。なお、非接触ＩＣカード３とは、非接触ＩＣカード３ａ及び３ｂの双方を含むものとする。

【００３４】

この部屋４の入口５ａの近傍には、入室管理装置６が備えられ、この入室管理装置６により入口５ａに備えられている自動ドア７の開閉状態がコントロールされている。入室管理装置６は、非接触ＩＣカード３との間で無線により情報の伝送が行えるように構成され、非接触ＩＣカード３に記憶されている情報の読み取りが可能である。さらに、この部屋４の出口５ｂの近傍には、退室管理装置１０が備えられ、この退室管理装置１０により自動ドア７の開閉状態がコントロールされている。また、退室管理装置１０は、非接触ＩＣカード３との間で無線により情報の伝送が行えるように構成され、非接触ＩＣカード３に記憶されている情報の読み取りが可能である。つまり、本実施形態では、入退室のアクセス制御として非接触ＩＣカード３を使用している。

【００３５】

なお、部屋４には、入口５ａと出口５ｂを別々に設ける場合と、入口５ａと出口５ｂを１つにして出入口とする場合とがあるが、図１には、１つの出入口を用いた場合が示されている。また、入室管理装置６と退室管理装置１０を一体型に構成した入退室管理装置とし、部屋の外部と内部を隔てる壁の一部に設けるようにしてもよい。ここで、入退室管理装置とは、例えば、非接触ＩＣカード３からの情報の読取行うことができるＩＣカードリーダやＩＣカードリーダライタ等である。

【００３６】

また、管理者が使用する管理者端末であるパソコン５０と管理者によって管理される管理対象装置であるロッカー７０は、図示のように、それぞれＩＣカードリーダ９及びＩＣカードリーダ７９が備えられている。ＩＣカードリーダ９及びＩＣカードリーダ７９は、入退室管理装置と同様に、非接触ＩＣカード３からの情報の読取を行うことができる。

【００３７】

情報記憶媒体である非接触ＩＣカード３は、例えば、図２乃至図４に示すように、カード基材３０及び３１の内部に非接触ＩＣタグ８が内蔵された構成を有している。非接触ＩＣタグ８は、例えば、非接触データキャリアやＲＦＩＤともいわれ、図４に示すように、プラスチック等の基材８１にコイルパターンからなる送受信部８８が形成されている。非接触ＩＣタグ８は、コイルと容量素子とにより共振回路を形成して一定周波数の電波を受信及び送信する。また、他の方式として、リーダライタからの搬送波の電磁誘導により電力伝送及びデータ伝送を行うようにしてもよい。一般的には、１３５ｋＨｚ（中波）、１３．５６ＭＨｚ、２．４５ＧＨｚ（マイクロ波）の周波数帯が使用される。

【００３８】

図示した例の場合、コイルパターンからなる送受信部８８は、導通部材８４により基材８１の裏面でジャンピング回路を形成し、コイル接続端子８８ＣによりＩＣチップ８２の裏面のバンプに接続している。ＩＣチップ８２には、ＣＰＵである制御部８９と、メモリである記憶部９０とが備えられている。

【００３９】

図示した例では、容量素子はＩＣチップ８２に内蔵されている。このような非接触ＩＣタグ８は、樹脂基材にラミネートしたアルミ箔等の金属箔をフォトエッチングやレジスト印刷後のエッチングすることによりコイルパターンを形成し、ＩＣチップ８２を装着し、保護用の被覆を設けることにより形成される。その大きさも３０ｍｍ×３０ｍｍ程度以下のサイズとすることができる。

【００４０】

非接触ＩＣタグ８に使用する樹脂基材８１としては、ＰＥＴやポリプロピレン、ポリエチレン、ポリスチレン、ナイロン等の各種材料を使用することができ、紙であってもよい。厚みは１５～３００μｍとすることができるが、強度、加工作業性、コスト等の点から２０～１００μｍがより好ましい。金属箔としては銅箔やアルミ箔あるいは鉄箔を使用できるが、コスト、加工性からアルミ箔が好ましく、その厚みは６～５０μｍ程度が好まし

い。
【００４１】
これらの非接触ＩＣタグ８に記録した情報の読み取りや情報の書き込みは、ＩＣカードリーダ９から非接触ＩＣタグ８に対して共振する呼び出し信号を発信し、数ｃｍから数十ｃｍの距離で非接触ＩＣタグ８からの応答信号を読み取る。これにより、非接触ＩＣタグ８のＩＣチップ８２の記憶部であるメモリに記録された情報を読み取ったり、情報を書き込んだりすることができる。また、ＩＣチップ８２の記憶部であるメモリには、本人であることを認証するためのＩＤ情報（識別情報）が予め登録されている。
【００４２】
次に、図５の機能ブロック図を参照し、システム構成を詳細に説明する。図５には、非接触ＩＣカード３、入退室管理装置、ＩＣカードリーダ９、パソコン５０、ＩＣカードリーダ７９及びロッカー７０を含むシステム構成が示されている。
【００４３】
なお、図５のブロック図における、入退室管理装置は、図１における入室管理装置６及び退室管理装置１０を一体型に構成した装置である。
【００４４】
出入口５の近傍に設けられた入退室管理装置は、送受信部１１、権限判定部１２、ドア開閉部１３、記憶部１４及び制御部１５を有している。各部は、制御部１５により制御される。
【００４５】
送受信部１１は、非接触ＩＣカード３の送受信部８８と無線による情報の送受信を行う。
【００４６】
権限判定部１２は、入退室の際に非接触ＩＣカード３から受信した識別情報と、予め記憶部１４に記憶されている権限テーブルとに基づいて、当該非接触ＩＣカードを所持する者が入室権限を有しているか否かを判定する。
【００４７】
ここで、図６を参照して、記憶部１４に記憶されている権限テーブルについて説明する。図６は、権限テーブルのデータ構造を模式的に示す図である。なお、本実施形態において非接触ＩＣカード３には、識別情報として社員ＩＤが含まれているものとする。
【００４８】
権限テーブルは、図示のように、社員ＩＤ、入室権限及び管理権限の項目から構成されている。社員ＩＤは、管理者やオペレータといった各利用者を識別する情報である。入室権限は、部屋４に入室することができる権限であり、権限テーブルでは、入室権限を持つ社員ＩＤに対応する入室権限項目に丸（○）が格納される。管理権限は、部屋４内の管理者端末であるパソコン５０を使用することができると共に、管理対象装置であるロッカー７０を管理することができる権限であり、権限テーブルでは、管理権限を持つ社員ＩＤに対応する管理権限項目に丸（○）が格納される。管理権限を有する管理者が部屋４内に設置されたパソコン５０を使用している間のみ、オペレータはロッカー７０を利用することができる。権限判定部１２は、非接触ＩＣカードから読み取った識別情報、即ち社員ＩＤに基づいて権限テーブルを参照することにより、当該非接触ＩＣカードを所持する者が入室権限を有しているか否かを容易に判定することができる。
【００４９】
権限判定部１２による処理により、入退室の際、非接触ＩＣカード３を所持する者が入室権限を有していると判定された場合、ドア開閉部１３が自動ドア７を開く。
【００５０】
パソコン５０は、表示部２１、管理判定部２２、命令情報送信部２３、記憶部２４、入力部２５、インタフェース（Ｉ／Ｆ）２６、制御部２７、カード判定部２８及び通信部２９を有している。各部は、制御部２７により制御される。
【００５１】

管理判定部２２は、ＩＣカードリーダ９から非接触ＩＣカード３に対して信号を送信する。こうして、非接触ＩＣカード３の記憶部９０に記憶されている情報を読み取り、当該情報に含まれる社員ＩＤを特定する。そして、管理判定部２２は、特定した社員ＩＤに基づいて、記憶部２４に予め記憶された図６に示すような権限テーブルを参照することにより、非接触ＩＣカード３を所持する者が管理権限を有しているか否かを判定する。

【００５２】

また、管理判定部２２は、非接触ＩＣカード３を所持する者が管理権限を有していると判定した場合、パソコン５０のロックを解除し、使用可能な状態に制御する。つまり、パソコン５０を起動できるようにする。一方、管理判定部２２は、非接触ＩＣカード３を所持する者が管理権限を有していないと判定した場合に、パソコン５０のロックを解除しない。よって、管理権限を有していない者、即ち管理者以外の者は、パソコン５０を使用することができない。さらに、管理判定部２２は、後述するカード判定部２８により、ＩＣカードリーダ９から非接触ＩＣカード３が取り外されたと判定された場合に、パソコン５０をロックし、使用不可能な状態に制御する。つまり、パソコン５０を停止させたり、スクリーンロックをかけたりする。

【００５３】

カード判定部２８は、ＩＣカードリーダ９から非接触ＩＣカード３が取り外されたか否かを判定する。

【００５４】

命令情報送信部２３は、管理判定部２２により、ＩＣカードリーダ９に置かれた非接触ＩＣカード３を所持する者が管理権限を有すると判定された場合に、通信部２９を介して、ロッカー７０に利用許可情報を送信する。利用許可情報とは、ロッカー７０を全てのオペレータが利用可能な状態にすることを求める情報である。

【００５５】

また、命令情報送信部２３は、カード判定部２８により、非接触ＩＣカード３がＩＣカードリーダ９から取り外されたと判定された場合に、通信部２９を介して、ロッカー７０に利用停止情報を送信する。利用停止情報とは、ロッカー７０を全てのオペレータが利用不可能な状態にすることを求める情報である。

【００５６】

ロッカー７０は、オペレータ判定部７１、ロック制御部７２、インタフェース（Ｉ／Ｆ）７３、記憶部７４、通信部７５及び制御部７６を有している。各部は、制御部７６により制御される。

【００５７】

オペレータ判定部７１は、ＩＣカードリーダ７９から非接触ＩＣカード３に対して信号を送信する。こうして、非接触ＩＣカード３の記憶部９０に記憶されている情報を読み取り、当該情報に含まれる社員ＩＤを特定する。そして、オペレータ判定部７１は、特定した社員ＩＤに基づいて、記憶部７４に予め記憶された図６に示すような権限テーブルを参照することにより、非接触ＩＣカード３を所持する者が入室権限を有するオペレータであるか否かを改めて判定する。

【００５８】

なお、本実施形態では、オペレータ判定部７１により、非接触ＩＣカード３を所持する者が入室権限を有するオペレータであるか否かを改めて判定しているが、本発明はこれに限定されるものではない。例えば、権限テーブルにロッカー７０の利用権限を有するオペレータに関する情報が含まれており、社員ＩＤに基づいて権限テーブルを参照することにより、非接触ＩＣカード３を所持する者が利用権限を有するか否かを判定することとしてもよい。つまり、オペレータ判定部７１は、ＩＣカードリーダ７９により非接触ＩＣカード３から読み取った情報に基づいて、利用者に関する所定の認証を行うものである。

【００５９】

ロック制御部７２は、通信部７５を介してパソコン５０から利用許可情報を受信している場合に、ロッカー７０のロックを解除し、利用可能な状態に制御する。また、ロック制

御部７２は、通信部７５を介してパソコン５０から利用停止情報を受信している場合に、ロッカー７０をロックし、利用不可能な状態に制御する。

【００６０】

なお、ロック制御部７２は、オペレータ判定部７１による認証に問題がある場合に、利用許可情報を受信していたとしても、ロッカー７０をロックし、利用不可能な状態に制御することとしてもよい。

【００６１】

以上の構成を有する本実施形態においては、部屋４が施設に相当する。また、パソコン５０が管理者端末として機能し、ロッカー７０が管理対象装置として機能する。また、ＩＣカードリーダは、情報読取部に相当する。

【００６２】

次に、上述の管理システムによる利用許可処理について図７を参照して説明する。図７は、利用許可処理のフローチャートである。

【００６３】

入室が管理された施設である部屋４に入室する際、利用者である管理者又はオペレータは、部屋４の入口から入室するために、情報記憶媒体である非接触ＩＣカード３を入退室管理装置に近づける。この際、入退室管理装置は、非接触ＩＣカード３の記憶部９０に記憶されている社員ＩＤを読み取る。入退室管理装置の権限判定部１２は、読み取られた社員ＩＤと、入退室管理装置の記憶部１４に予め登録されている権限テーブルとに基づいて、非接触ＩＣカード３を所持する者が入室権限を有しているか否かを判定する。入室権限を有している場合、ドア開閉部１３により自動ドア７が開かれ、部屋４に入室することができる。一方、入室権限を有していない場合、ドア開閉部１３により自動ドア７が開かれることはなく、部屋４に入室することはできない。

【００６４】

部屋４に入室すると、管理者は、管理者端末であるパソコン５０のＩＣカードリーダ９に自身の非接触ＩＣカード３ａを配置する。この際、パソコン５０は、非接触ＩＣカード３ａの記憶部９０に記憶されている社員ＩＤを読み取る（ステップＳ１）。具体的に、パソコン５０は、記憶部９０に記憶されている情報に基づいて社員ＩＤを特定する。パソコン５０の管理判定部２２は、読み取られた社員ＩＤと、記憶部２４に予め登録されている権限テーブルとに基づいて、非接触ＩＣカード３ａを所持する者が管理権限を有する否かを判定する（ステップＳ２）。

【００６５】

管理権限を有していないと判定した場合（ステップＳ２；Ｎｏ）、管理判定部２２は、パソコン５０のロックを解除せず、使用不可能な状態のままにしておき、利用許可処理を終了する。即ち、管理権限を有していない者は、パソコン５０を使用することはできない。一方、管理権限を有すると判定した場合（ステップＳ２；Ｙｅｓ）、管理判定部２２は、パソコン５０のロックを解除し、使用可能な状態に制御する（ステップＳ３）。また、命令情報送信部２３は、通信部２９を介してロッカー７０に利用許可情報を送信する（ステップＳ４）。

【００６６】

ロッカー７０は、通信部７５を介してパソコン５０から利用許可情報を受信する（ステップＳ５）。すると、ロック制御部７２は、ロッカー７０のロックを解除し、利用可能な状態に制御する（ステップＳ６）。これにより、利用許可処理は完了する。

【００６７】

これによれば、ロッカー７０は、管理者がパソコン５０を使用することにより自動的に利用可能な状態となる。つまり、特別な対応や処置をすることなく、自動的にロッカー７０が利用可能な状態になるため、管理者の負担を軽減することができる。

【００６８】

次に、上述の管理システムによる利用停止処理について図８を参照して説明する。図８は、利用停止処理のフローチャートである。

【００６９】
管理者は、部屋４から退室する際、管理者端末であるパソコン５０を第三者に使用させないために、自身の非接触ＩＣカード３ａをＩＣカードリーダ９から取り外す。そして、管理者は、入退室管理装置に非接触ＩＣカード３ａをかざし、部屋４から退室する。
【００７０】
パソコン５０のカード判定部２８は、ＩＣカードリーダ９から非接触ＩＣカード３が取り外されたか否かを常に判定している（ステップＳ１１）。そして、カード判定部２８により、ＩＣカードリーダ９から非接触ＩＣカード３が取り外されたと判定された場合（ステップＳ１１；Ｙｅｓ）、管理判定部２２は、パソコン５０をロックし、使用不可能な状態に制御する（ステップＳ１２）。これによれば、パソコン５０は、自動的にスクリーンロックがかかった状態となり、第三者による不正使用を防止することができる。さらに、カード判定部２８により、ＩＣカードリーダ９から非接触ＩＣカード３が取り外されたと判定された場合（ステップＳ１１；Ｙｅｓ）、命令情報送信部２３は、通信部２９を介してロッカー７０に利用停止情報を送信する。（ステップＳ１３）。
【００７１】
ロッカー７０は、通信部７５を介してパソコン５０から利用停止情報を受信する（ステップＳ１４）。すると、ロック制御部７２は、ロッカー７０をロックし、利用不可能な状態に制御する（ステップＳ１４）。これにより、利用停止処理は完了する。
【００７２】
これによれば、ロッカー７０は、管理者がパソコン５０から離れた場合、自動的に利用不可能な状態となる。つまり、特別な対応や処置をすることなく、自動的にロッカー７０が利用不可能な状態になるため、管理者の負担を軽減することができる。また、管理者がリーダライタ９から自身の非接触ＩＣカード３ａを取り外すことでパソコン５０が使用不可能な状態となるため、第三者によるパソコン５０の不正使用及びロッカー７０の不正利用を防止することができる。
【００７３】
また、管理者が部屋４へ戻ってきた場合、管理者端末であるパソコン５０のＩＣカードリーダライタ９に非接触ＩＣカード３ａを置くことで、容易にパソコン５０のロックを解除し、使用可能な状態にすることができる。さらに、パソコン５０のロックを解除し使用可能な状態とすることで、ロッカー７０のロックが解除され、自動的且つ容易に、全てのオペレータがロッカー７０を利用可能な状態にすることができる。
【００７４】
なお、本実施形態では、非接触ＩＣカード３を利用することとしているが、本発明はこれに限定されるものではなく、情報記憶媒体を装着した携帯電話を利用することとしてもよい。つまり、本発明では、入退室のアクセス制御や管理者端末及び管理対象装置の認証として利用可能であれば任意の可般記憶媒体を適用することができる。
【００７５】
また、本実施形態では、非接触ＩＣカード３は識別情報のみを有しており、入退室管理装置、パソコン５０及びロッカー７０が、読み取った識別情報に基づいて権限テーブルを参照することで、入室権限及び／又は管理権限の有無を判定することとしている。しかし、本発明はこれに限定されるものではなく、非接触ＩＣカード３が入室権限及び／又は管理権限の有無を示す情報を有していることとしてもよい。具体的には、管理者が有する非接触ＩＣカード３ａには、入室権限及び管理権限があることを示す情報（フラグ等）が含まれており、オペレータが有する非接触ＩＣカード３ｂには、入室権限があることを示す情報が含まれていることになる。この場合、入退室管理装置、パソコン５０及びロッカー７０は予め権限テーブルを登録する必要はなく、非接触ＩＣカードから読み取った情報に基づいて入室権限及び管理権限の有無を判定する。
【００７６】
また、本実施形態では、権限テーブルのデータ構造を図６に示すようにしているが、本発明はこれに限定されるものではなく、非接触ＩＣカード３から読み取った識別情報に基

づいて入室権限及び管理権限の有無が判定できれば、データ構造は任意に設定することができるものとする。さらに、入退室管理装置の記憶部１４及びロッカー７０の記憶部７５に記憶される権限テーブルは、入室権限を有しているか否かを判定することができるテーブルであればよい。

【００７７】

また、本実施形態では、管理者端末としてパソコンを例に使用しているが、本発明はこれに限定されるものではなく、図５に示すような機能を有するものであれば、メインコントローラ装置やロッカー等、管理者が使用する任意の電子機器又は設備に適用することができる。さらに、本実施形態では、管理対象装置としてロッカーを例に説明しているが、本発明はこれに限定されるものではなく、例えばプリンタやパソコン等あらゆる電子機器又は設備に適用することができる。

【００７８】

また、本実施形態では、管理者端末であるパソコン５０が利用許可情報及び／又は利用停止情報といった命令情報を送信し、管理対象装置であるロッカー７０が命令情報に基づいてロック制御を行っている。しかし、本発明はこれに限定されるものではなく、ネットワーク６０を介して、パソコン５０とロッカー７０がサーバと接続されており、当該サーバがパソコン５０の使用状況を判断し、ロッカー７０のロック制御を行うこととしてもよい。即ち、サーバが、管理者端末の使用状況を判断し、管理対象装置のロック制御を行うこととしてもよい。このように、サーバを管理システムの構成要素とすることで、自身ではロック制御を行うことができない種々の電子機器及び設備を管理対象装置として適用することが可能となる。

【００７９】

[第１変形例]

上記の実施形態では記載していないが、管理者が管理者端末により、オペレータによる管理対象装置の利用状況を認識できるようにすることができる。また、利用状況に基づいて、例えば管理対象装置を利用しすぎているオペレータに対して、特定の管理対象装置を利用できないような不許可設定を行うことができる。

【００８０】

なお、第１変形例では、管理対象装置がロッカーだけではなく、コピー機、プリンタ等、複数の電子機器であるものとする。各管理対象装置を識別する情報が「種別」である。

【００８１】

第１変形例において、各管理対象装置は、オペレータ判定部により特定されたオペレータの社員ＩＤと、当該オペレータによる利用回数とを記憶部に記憶している。そして、管理対象装置は、所定のタイミングで通信部を介し、記憶部に記憶された社員ＩＤ及び利用回数を対応付け、利用状況情報として管理者端末へ送信する。このとき、各管理対象装置は、その時点でオペレータが利用中であるか否かを示す情報を利用状況情報に含めることとしてもよい。

【００８２】

ここで、所定のタイミングとは、管理者端末から利用状況情報を要求する信号を管理対象装置が受信した時等である。

【００８３】

管理者端末は、各管理対象装置から受信した利用状況情報を、図９（ａ）に示すように、画面等に表示する。図９は、利用状況情報に基づいて画面等に表示される利用状況テーブルの例である。図示のように、利用状況テーブルは、縦軸が管理対象装置の種別、横軸が社員ＩＤとなっており、交差するボックスに利用中であるか否か及び利用回数が格納されている。利用中ではないが既に利用している場合、ボックスには利用回数のみが格納される。

【００８４】

例えば、社員ＩＤ「Ａ０１」のオペレータは、プリンタを利用中であり、利用回数は２回である。また、社員ＩＤ「Ａ０２」のオペレータは、プリンタを利用中ではないが、既

に利用しており、利用回数は５回である。また、社員ＩＤ「Ａ０３」のオペレータは、１回もプリンタを利用していない。このように、利用状況テーブルに基づいて、管理者は、部屋４内にある管理対象装置をどのオペレータがどのくらい利用しているかを容易に把握することができる。

【００８５】

さらに、管理者は、管理者端末を使用して、利用を不許可とする不許可利用者及び利用を不許可とする管理対象装置を指定することにより、特定のオペレータが特定の種別の管理対象装置を利用できないように設定することができる。このような設定を「不許可設定」と呼ぶ。

【００８６】

具体的に、管理者は、管理者端末を操作して、画面等に表示されている利用状況テーブルのボックスを指定することにより不許可設定をすることができる。図９（ｂ）に示すように、管理者により指定されたボックスには大きくバツ印（×）が表示される。このボックスは、社員ＩＤ「Ａ０２」のオペレータ及び種別「コピー機」に対応している。よって、管理者は、社員ＩＤ「Ａ０２」のオペレータを不許可利用者に指定し、種別「コピー機」を不許可種別に指定したことになる。

【００８７】

管理者端末は、不許可設定が行われると、不許可利用者に指定されたオペレータの社員ＩＤと、不許可種別に指定された管理対象装置の種別とを不許可情報として、通信部を介し管理対象装置へ送信する。管理対象装置は、通信部を介して管理者端末から不許可情報を受信し、記憶部に記憶する。そして、管理対象装置は、不許可情報に基づいて、不許可利用者であるオペレータが不許可種別である管理対象装置を利用しようとした場合に、たとえ利用許可情報を受信していたとしても、利用不可能な状態に制御する。

【００８８】

ここで、第１変形例の管理システムによる不許可実行処理について図１０を参照して説明する。図１０は、不許可実行処理のフローチャートである。

【００８９】

オペレータは、管理対象装置のＩＣカードリーダに自身の非接触ＩＣカード３ｂを置く。この際、管理対象装置は、非接触ＩＣカード３ｂの記憶部９０に記憶されている社員ＩＤを読み取る（ステップＳ３１）。管理対象装置のオペレータ判定部は、記憶部に記憶された不許可情報に基づいて、読み取った社員ＩＤが不許可利用者の社員ＩＤと一致するか否かを判定する（ステップＳ３２）。一致しない場合（ステップＳ３２；Ｎｏ）、不許可実行処理は終了する。一方、一致する場合（ステップＳ３２；Ｙｅｓ）、オペレータ判定部は、オペレータが不許可利用者であると特定する。

【００９０】

オペレータが不許可利用者と特定された場合、オペレータ判定部は、さらに不許可情報に基づいて、当該管理対象装置の種別が、読み取った社員ＩＤの不許可利用者に対応付けされた不許可種別と一致するか否かを判定する（ステップＳ３３）。一致しない場合（ステップＳ３３；Ｎｏ）、不許可実行処理は終了する。一方、一致する場合（ステップＳ３３；Ｙｅｓ）、オペレータ判定部は、不許可利用者であるオペレータが、対応する不許可種別の管理対象装置を利用しようとしていると特定する。よって、ロック制御部は、当該管理対象装置のロックを行い、不許可利用者であるオペレータが当該管理対象装置を利用できないように制御する（ステップＳ３４）。これにより、不許可実行処理は完了する。

【００９１】

なお、ステップＳ３２及びＳ３３において、一致しないと判定された場合、不許可利用者による不許可種別の管理対象装置の実行ではないとして、不許可実行処理は終了する。このとき、管理対象装置が利用許可情報を受信していれば、オペレータは、当該管理対象装置を利用することができる。管理対象装置は、オペレータが利用すると、記憶部に当該オペレータの社員ＩＤと利用回数を記憶する。このように記憶された社員ＩＤ及び利用回数に基づいて、上述の利用状況情報が作成される。

【００９２】
また、第１変形例では、管理対象装置も、実施形態におけるカード判定部２８と同様のカード判定部を有しているものとする。具体的に、利用許可情報を受信している場合、管理対象装置のカード判定部により不許可利用者が所持する非接触ＩＣカード３ｂがＩＣカードリーダから取り外されたと判定されると、ロック制御部は、当該管理対象装置のロックを解除し、再び利用可能な状態に制御する。
【００９３】
また、第１変形例における利用状況テーブルにおいて、長時間利用しているオペレータの社員ＩＤと種別が交差するボックスや、多くの回数利用しているオペレータの社員ＩＤと種別が交差するボックスを警告として赤く表示したり、点滅させたりすることとしてもよい。利用状況テーブルは、図９に示すものに限らず、管理者が利用状況を把握できるものであれば、項目等は任意に設定することができる。さらに、利用状況テーブルの元になる利用状況情報は、ログとして記憶部に記憶しておくこととしてもよい。
【００９４】
このように、第１変形例によれば、管理者は、管理者端末に利用状況テーブルを表示することによって、オペレータによる管理対象装置の利用状況を容易且つ的確に認識することが可能となる。また、利用状況に基づいて、特定のオペレータに対して特定の管理対象装置を利用できなくする不許可設定を容易に行うことができる。これにより、管理対象装置を利用しすぎているオペレータに対して間接的に注意を促したり、不正使用を防止したりといった効果が期待できる。
【００９５】
[第２変形例]
なお、上記の実施形態及び第１変形例では記載していないが、予め各オペレータが所持する非接触ＩＣカード３ｂに利用範囲情報を記憶しておくこともできる。ここで、利用範囲情報について、図１１を参照して説明する。図１１は、利用範囲情報のデータ構造を示す図である。図示のように、利用範囲情報は、種別項目及び利用可能回数項目から構成されている。種別項目とは、管理対象装置の種別を示す情報であり、本変形例では、例えば、ロッカー、スキャナー、プリンタ等とする。利用可能回数項目とは、オペレータが利用可能な回数である。利用範囲情報は、図８（ａ）及び（ｂ）に示すように、オペレータ毎に任意に設定することができる。例えば、図８（ａ）に示す利用者範囲情報Ａが記憶された非接触ＩＣカード３ｂを所持するオペレータの場合、管理者が管理者端末を使用している場合であっても、プリンタを利用することはできない。一方、図８（ｂ）に示す利用者範囲情報Ｂが記憶された非接触ＩＣカード３ｂを所持するオペレータの場合、管理者が管理者端末を使用している場合に、プリンタを１０回まで利用することができる。
【００９６】
この場合、管理対象装置のロック制御部は、利用許可情報を受信している場合であって、且つ、非接触ＩＣカード３ｂに含まれる利用範囲情報の範囲内である場合に限り、利用可能な状態のままにしておく。換言すると、利用許可情報を受信している場合であっても、非接触ＩＣカード３ｂに含まれる利用範囲情報の範囲外であれば、ロック制御部は、管理対象装置をロックし、オペレータが利用不可能な状態に制御する。
【００９７】
具体的に、管理対象装置は、まず、自身の種別が、利用範囲情報において利用できる種別と一致するか否かを判定する。一致しない場合、管理対象装置は、利用範囲情報の範囲外であると判定する。一方、一致する場合、管理対象装置は、利用回数が、利用範囲情報において自身の種別に対応付けられた利用可能回数より少ないか否かを判定する。利用回数が利用可能回数より多い場合、管理対象装置は、利用範囲情報の範囲外であると判定する。一方、利用回数が利用可能回数より少ない場合、管理対象装置は、利用範囲情報の範囲内であると判定する。
【００９８】
なお、オペレータが利用した種別及び利用回数に関する情報は、管理対象装置の記憶部

に記憶されているものとする。

【００９９】

また、上述の第２変形例では、利用範囲情報を図１１に示すようなデータ構造としているが、本発明はこれに限定されるものではなく、任意に設定することができる。例えば、利用範囲情報として有効時間や有効日時を設定し、オペレータが部屋４に入室してからの時間や日付に基づいて管理対象装置の利用を制限するように設定することも可能である。

【０１００】

これによれば、利用範囲情報に基づいて各オペレータに応じた範囲で管理対象装置の利用を制限することができる。

【産業上の利用可能性】

【０１０１】

本発明によれば、情報記憶媒体を使用して、管理者の手を煩わせることなく、簡易に、管理者が室内にいる間だけ自動的に電子機器や設備の利用が可能となる管理システムとして利用することができる。

【図面の簡単な説明】

【０１０２】

【図１】管理システムの概要を説明する図である。

【図２】非接触ＩＣカードの平面図である。

【図３】図２のＡ－Ａ線による断面図である。

【図４】非接触ＩＣカードに内蔵されているＩＣタグの平面図である。

【図５】管理システムの機能ブロック図である。

【図６】権限テーブルのデータ構造を模式的に示す図である。

【図７】管理システムによる利用許可処理を示すフローチャートである。

【図８】管理システムによる利用停止処理を示すフローチャートである。

【図９】利用状況テーブルの例である。

【図１０】第１変形例における不許可実行処理の例である。

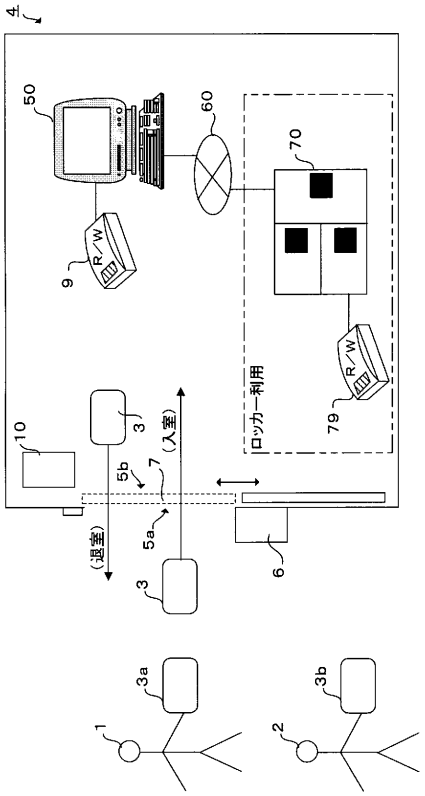
【図１１】第２変形例における利用範囲情報のデータ構造を模式的に示す図である。

【符号の説明】

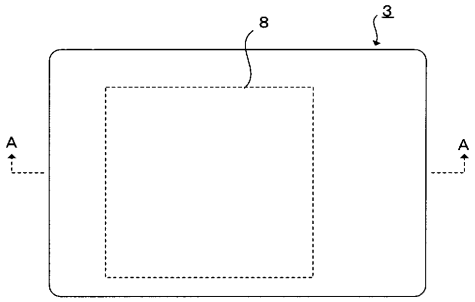
【０１０３】

１…管理者
２…オペレータ
３…非接触ＩＣタグ
４…部屋
６…入室管理装置
１０…退室管理装置
５０…パソコン
６０…ネットワーク
７０…ロッカー

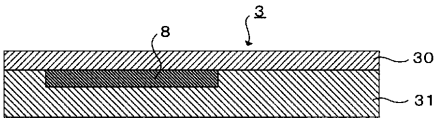
【図１】


4
50
60
70
R/W
9
ロッカー利用
79
10
3
(入室)
5b
7
5a
(退室)
6
3a
3b
1
2

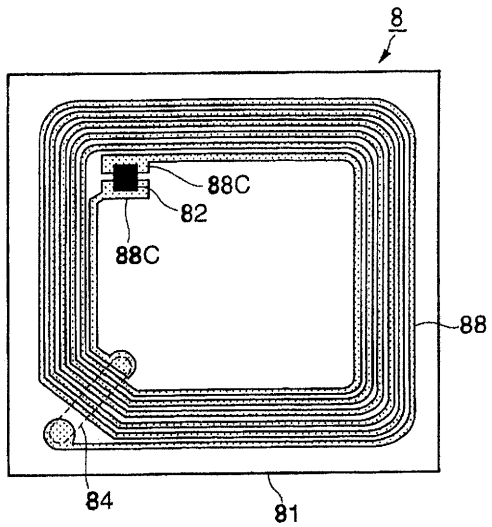
【図２】


8
3
A
A

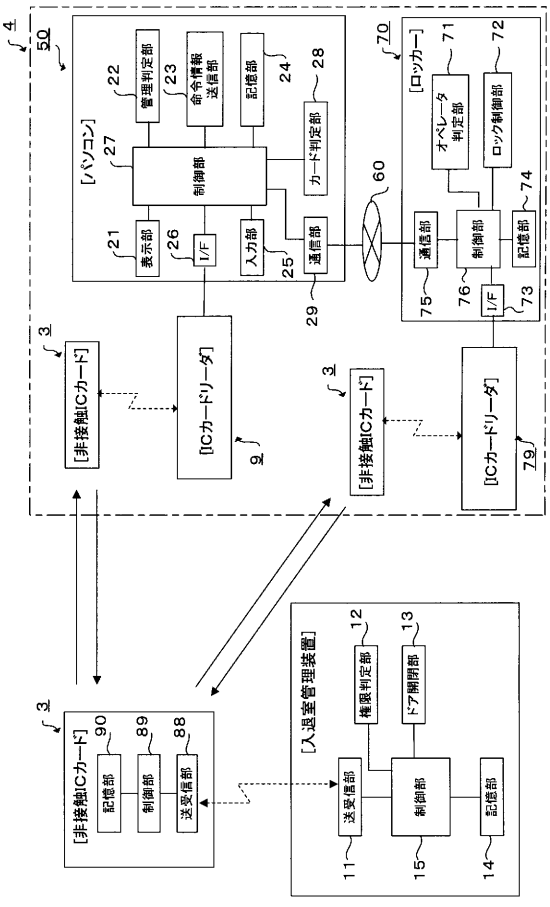
【図３】


8
3
30
31

【図４】


8
88C
82
88C
88
84
81

【図５】

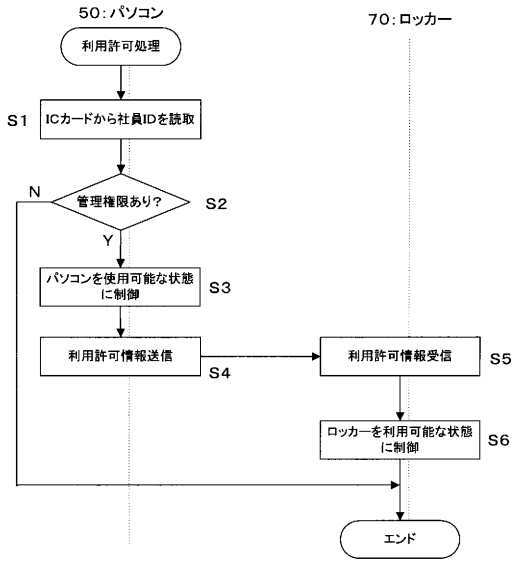

4
50
[パソコン]
27
制御部
22
管理判定部
23
命令情報送信部
24
記憶部
28
カード判定部
21
表示部
26
I/F
入力部
25
通信部
29
60
70
[ロッカー]
71
オペレータ判定部
72
ロック制御部
74
通信部
制御部
記憶部
75
76
I/F
73
3
[非接触ICカード]
[ICカードリーダ]
9
79
[入退室管理装置]
12
権限判定部
13
ドア開閉部
送受信部
制御部
記憶部
11
15
14
90
89
88

【図６】

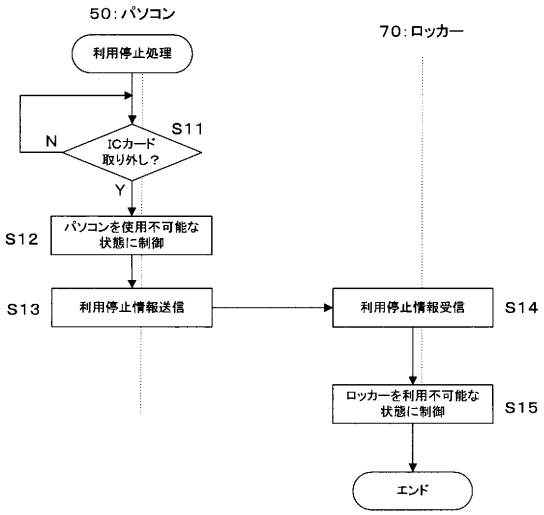
権限テーブル

社員ID	入室権限	管理権限
A01	○	○
A02	○	—
A03	○	—
⋮	⋮	⋮

【図７】



【図８】



【図９】

利用状況テーブル

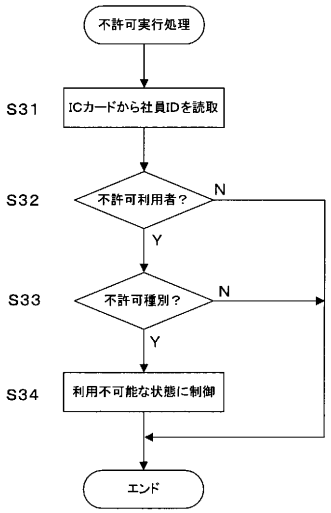
(a)

種別＼社員ID	A01	A02	A03	…
ロッカー	使用中(1)	使用中(1)	使用中(2)	…
コピー機		使用中(20)		…
プリンタ	使用中(2)	(5)		…
⋮	⋮	⋮	⋮	⋮

(b)

種別＼オペレータ	A01	A02	A03	…
ロッカー	使用中(1)	使用中(1)	使用中(2)	…
コピー機		使用中(20)		…
プリンタ	使用中(2)	(5)		…
⋮	⋮	⋮	⋮	⋮

【図１０】



【図１１】

(a)

利用範囲情報A

種別	利用可能回数
ロッカー	3回
スキャナー	5回
プリンタ	—
⋮	⋮

(b)

利用範囲情報B

種別	利用可能回数
ロッカー	3回
スキャナー	10回
プリンタ	10回
⋮	⋮

フロントページの続き

(72)発明者　近田　恭之
東京都新宿区市谷加賀町一丁目１番１号　大日本印刷株式会社内

Ｆターム(参考) 5B058 CA17 KA02 KA31 KA33 YA11 YA13
5B285 AA01 BA01 BA02 BA04 CA02 CA12 CA17 CA18 CA32 CB08
CB63 CB64 CB74 DA10