(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4827392号
(P4827392)
(45)発行日　平成23年11月30日(2011.11.30)　(24)登録日　平成23年9月22日(2011.9.22)

(51)Int.Cl.　　F I
G06F 1/00 (2006.01)　　G06F 1/00 370E
G06K 17/00 (2006.01)　　G06K 17/00 S

請求項の数 5　(全 19 頁)

(21)出願番号　特願2004-227451 (P2004-227451)
(22)出願日　平成16年8月4日 (2004.8.4)
(65)公開番号　特開2005-100359 (P2005-100359A)
(43)公開日　平成17年4月14日 (2005.4.14)
審査請求日　平成19年6月8日 (2007.6.8)
審判番号　不服2010-11707 (P2010-11707/J1)
審判請求日　平成22年6月1日 (2010.6.1)
(31)優先権主張番号　特願2003-208341 (P2003-208341)
(32)優先日　平成15年8月22日 (2003.8.22)
(33)優先権主張国　日本国 (JP)

(73)特許権者　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　100091476
弁理士　志村　浩
(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】コンピュータの不正使用防止システム及びその方法

(57)【特許請求の範囲】
【請求項１】
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コンピュータの不正使用防止システムであって、
前記コンピュータの使用権限を有する使用者が所持し、少なくともフラグ記憶領域を有するメモリを備えた情報記憶媒体と、
前記コンピュータが備えられている部屋の出入口付近に備えられ、前記情報記憶媒体のフラグ記憶領域に入室を示すフラグを書き込む手段を有する第１の装置と、
前記コンピュータと情報伝送可能に備えられ、前記情報記憶媒体のフラグ記憶領域におけるフラグの有無を読み取る読取手段と前記フラグを消去する消去手段とを有する第２の装置と、
前記第２の装置の前記読取手段からの情報に基づいて、前記情報記憶媒体のフラグ記憶領域にフラグが書き込まれているか否かを確認するフラグ確認手段と、前記フラグ確認手段でフラグが書き込まれていることが確認された場合に、前記コンピュータの処理実行を可能とする状態に制御するパソコンロック制御手段と、前記コンピュータの使用が終了された場合に、前記第２の装置の前記消去手段を用いて前記フラグを消去するフラグ消去手段と、を有する前記コンピュータと、
を具備することを特徴とするコンピュータの不正使用防止システム。
【請求項２】
前記情報記憶媒体のメモリは、個人を特定可能な固有情報が記憶された固有情報記憶領

域を有し、前記第１の装置は、前記固有情報を読み取る読取手段と、前記固有情報と照合する情報が記憶された記憶手段と、前記読取手段で読み取った前記固有情報を前記記憶手段に記憶された情報と照合する照合手段と、前記照合手段による照合処理で照合一致した場合に、前記情報記憶媒体のフラグ記憶領域に入室を示すフラグを書き込む手段と、を有することを特徴とする請求項１に記載のコンピュータの不正使用防止システム。

【請求項３】

前記情報記憶媒体が、接触ＩＣカード、非接触ＩＣカード、もしくは携帯電話機であることを特徴とする請求項１または２に記載のコンピュータの不正使用防止システム。

【請求項４】

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コンピュータの不正使用防止方法であって、

前記コンピュータが備えられている部屋の入口から入室する際に、コンピュータの使用権限を有する使用者が所持している情報記憶媒体のフラグ記憶領域に対して、第１の装置でフラグを書き込むステップと、

前記コンピュータによる処理を行なう際に、第２の装置で前記情報記憶媒体にフラグが書き込まれているか否かを識別するステップと、

前記情報記憶媒体にフラグが書き込まれていることを条件に、前記コンピュータによる処理を可能とするステップと、

前記コンピュータの使用が終了された場合に、前記第２の装置で前記フラグを消去するステップと、

を有することを特徴とするコンピュータの不正使用防止方法。

【請求項５】

前記コンピュータが備えられている部屋の入口から入室する際に、コンピュータの使用権限を有する使用者が所持している情報記憶媒体に記憶されている固有情報を読み取るステップと、

前記固有情報を照合処理するステップと、

を有し、前記照合処理で照合一致することを条件として、フラグ記憶領域に対して、第１の装置でフラグを書き込むことを特徴とする請求項４に記載のコンピュータの不正使用防止方法。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、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コンピュータの不正使用防止システム及びその方法に関する。

【背景技術】

【０００２】

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技術として、コンピュータを使用する際に、予め本人を認証するためのＩＤ情報を記憶させたＩＣカード等の情報記憶媒体による照合処理による認証を行ない、本人認証が成立したことを条件に、コンピュータの使用を可能とするセキュリティ技術が既に知られている。（例えば、特許文献１参照）

【０００３】

これらのセキュリティ技術においては、ＩＣカード等の情報記憶媒体に記憶されたＩＤ情報に基いて、本人の認証処理が行なわれる。

また、これらの情報記憶媒体は、必ずしも本人が常に所持しているとは限らず、会社などのコンピュータ等が備えられている部屋に置かれている机の引出しの中などに保管していることもあり、不正行為を働こうとする第三者が部屋に侵入して、これらの情報記憶媒体を探し出して、コンピュータを使用して様々な不正行為が行なわれる危険性があるという問題がある。

【特許文献１】特開２００３－３０１５５号公報

【発明の開示】
【発明が解決しようとする課題】
【０００４】
本発明は、使用権限を有しない第三者が、他人のＩＣカード等の情報記憶媒体を不正に入手して、コンピュータを使用するために認証処理を行なった場合でも、コンピュータの使用ができないようにして、コンピュータのセキュリティを確保したコンピュータの不正使用防止システム及びその方法を提供する。
【課題を解決するための手段】
【０００５】
本発明のコンピュータの不正使用防止システムは、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コンピュータの不正使用防止システムであって、
前記コンピュータの使用権限を有する使用者が所持し、少なくともフラグ記憶領域を有するメモリを備えた情報記憶媒体と、前記コンピュータが備えられている部屋の出入口付近に備えられ、前記情報記憶媒体のフラグ記憶領域に入室を示すフラグを書き込む手段を有する第１の装置と、前記コンピュータと情報伝送可能に備えられ、前記情報記憶媒体のフラグ記憶領域におけるフラグの有無を読み取る読取手段を有する第２の装置と、前記第２の装置から前記情報記憶媒体のフラグ記憶領域にフラグが書き込まれているか否かを確認するフラグ確認手段と、前記フラグ確認手段でフラグが書き込まれていることが確認された場合に、前記コンピュータの処理実行を可能とする状態に制御する手段とを有する前記コンピュータと、を具備することを特徴とする。
【０００６】
また、本発明のコンピュータの不正使用防止システムは、前記情報記憶媒体のメモリには、個人を特定可能な固有情報が記憶された固有情報記憶領域を有し、前記第１の装置には、前記固有情報を読み取る読取手段と、前記固有情報と照合する情報が記憶された記憶手段と、前記読取手段で読み取った前記固有情報を前記記憶手段に記憶された情報と照合する照合手段と、前記照合手段による照合処理で照合一致した場合に、前記情報記憶媒体のフラグ記憶領域に入室を示すフラグを書き込む手段を有することを特徴とする。
【０００７】
更に、本発明のコンピュータの不正使用防止システムは、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コンピュータの不正使用防止システムであって、前記コンピュータの使用権限を有する使用者が所持し、少なくともフラグが記憶されたフラグ記憶領域を有するメモリを備えた情報記憶媒体と、前記コンピュータが備えられている部屋の出入口付近に備えられ、前記情報記憶媒体のフラグ記憶領域に記憶されているフラグを消し込む手段を有する第１の装置と、前記コンピュータと情報伝送可能に備えられ、前記情報記憶媒体のフラグ記憶領域におけるフラグの有無を読み取る読取手段を有する第２の装置と、前記コンピュータには、前記第２の装置から前記情報記憶媒体のフラグ記憶領域にフラグが書き込まれているか否かを確認するフラグ確認手段と、前記フラグ確認手段でフラグが書き込まれていないことが確認された場合に、前記コンピュータの処理実行を可能とする状態に制御する手段と、を具備することを特徴とする。
【０００８】
また、本発明のコンピュータの不正使用防止システムは、前記情報記憶媒体のメモリには、個人を特定可能な固有情報が記憶された固有情報記憶領域を有し、前記第１の装置には、前記固有情報を読み取る読取手段と、前記固有情報と照合する情報が記憶された記憶手段と、前記読取手段で読み取った前記固有情報を前記記憶手段に記憶された情報と照合する照合手段と、前記照合手段による照合処理で照合一致した場合に、前記情報記憶媒体のフラグ記憶領域に入室を示すフラグを消し込む手段を有することを特徴とする。
【０００９】
更に、本発明のコンピュータの不正使用防止システムは、前記情報記憶媒体が、接触ＩＣカードであることを特徴とする。
【００１０】

また、本発明のコンピュータの不正使用防止システムは、前記情報記憶媒体が、非接触ＩＣカードであることを特徴とする。

【００１１】

更に、本発明のコンピュータの不正使用防止システムは、前記情報記憶媒体が、携帯電話機であることを特徴とする。

【００１２】

また、本発明のコンピュータの不正使用防止方法は、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コンピュータの不正使用防止方法であって、前記コンピュータが備えられている部屋の入口から入室する際に、コンピュータの使用権限を有する使用者が所持している情報記憶媒体のフラグ記憶領域に対して、第１の装置でフラグを書き込むステップと、前記コンピュータによる処理を行なう際に、前記情報記憶媒体にフラグが書き込まれているか否かを識別するステップと、前記情報記憶媒体にフラグが書き込まれていることを条件に、前記コンピュータによる処理を可能とするステップと、からなることを特徴とする。

【００１３】

更に、本発明のコンピュータの不正使用防止方法は、前記コンピュータが備えられている部屋の入口から入室する際に、コンピュータの使用権限を有する使用者が所持している情報記憶媒体に記憶されている固有情報を読み取るステップと、前記固有情報を照合処理するステップと、前記照合処理で照合一致した場合にフラグ記憶領域に対して、第１の装置でフラグを書き込むステップと、を有していることを特徴とする。

【００１４】

また、本発明のコンピュータの不正使用防止方法は、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コンピュータの不正使用防止方法であって、前記コンピュータが備えられている部屋の入口から入室する際に、コンピュータの使用権限を有する使用者が所持している情報記憶媒体のフラグ記憶領域に書き込まれているフラグを、第１の装置で消去するステップと、前記コンピュータによる処理を行なう際に、前記情報記憶媒体にフラグが書き込まれているか否かを識別するステップと、前記情報記憶媒体にフラグが書き込まれていないことを条件に、前記コンピュータによる処理を可能とするステップと、からなることを特徴とする。

【００１５】

更に、前記コンピュータが備えられている部屋の入口から入室する際に、コンピュータの使用権限を有する使用者が所持している情報記憶媒体に記憶されている固有情報を読み取るステップと、前記固有情報を照合処理するステップと、前記照合処理で照合一致した場合にフラグ記憶領域に対して、第１の装置でフラグを書き込むステップと、を有していることを特徴とする。

【００１６】

また、本発明のコンピュータの不正使用防止方法は、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コンピュータの不正使用防止システムであって、前記コンピュータの使用権限を有する使用者が所持する情報記憶媒体と、前記コンピュータが備えられている場所の出入口付近に備えられ、前記情報記憶媒体に前記使用者が入る場所の場所特定情報を書き込む手段を有する第１の装置と、前記コンピュータと情報伝送可能に備えられ、前記情報記憶媒体に記憶された場所特定情報を読み取る読取手段を有する第２の装置と、前記コンピュータが備えられている場所の場所特定情報が記憶された記憶手段と、前記第２の装置で読み取った場所特定情報と、前記記憶手段に記憶されている場所特定情報とを照合する場所特定情報照合手段と、前記場所特定情報照合手段での照合結果が一致した場合に、前記コンピュータを起動可能な状態に制御する手段とを有するコンピュータと、を具備することを特徴とする。

【００１７】

更に、本発明のコンピュータの不正使用防止方法は、前記コンピュータには、前記コンピュータが正常に起動した際に、前記情報記憶媒体に記憶されている場所特定情報を消去

させる消去手段を具備することを特徴とする。

【００１８】

また、本発明のコンピュータの不正使用防止方法は、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コンピュータの不正使用防止システムであって、前記コンピュータの使用権限を有する使用者が所持する情報記憶媒体と、前記コンピュータが備えられている部屋の出入口付近に備えられ、前記情報記憶媒体に前記使用者の入室時刻情報を書き込む手段を有する第１の装置と、前記コンピュータと情報伝送可能に備えられ、前記情報記憶媒体に記憶された入室時刻情報を読み取る手段を有する第２の装置と、前記コンピュータを起動可能な時間帯情報が記憶された記憶手段と、前記第２の装置で読み取った入室時刻情報の入室時刻が、前記記憶手段に記憶されている時間帯情報の時間帯内にあるか否かを検証する時刻検証手段と、前記時刻検証手段での検証結果が時間帯内であると判定された場合に、前記コンピュータを起動可能な状態に制御する手段とを有するコンピュータと、を具備することを特徴とする。

【００１９】

更に、本発明のコンピュータの不正使用防止方法は、前記コンピュータには、前記コンピュータが正常に起動した際に、前記情報記憶媒体に記憶されている入室時刻情報を消去させる消去手段を具備することを特徴とする。

【発明の効果】

【００２０】

本発明のコンピュータの不正使用防止システム及びその方法は、コンピュータの使用者が、コンピュータが備えられている部屋の入口から正規に入室した場合にだけ、コンピュータを使用することができるようにしてあるので、たとえ使用権限を有しない第三者が、他人の非接触ＩＣカード等の情報記憶媒体を不正に入手して、不正にコンピュータが備えられている部屋に侵入して、コンピュータの使用をしようとしても、コンピュータのロック状態を解除することができず、コンピュータのセキュリティを保つことができる。

また、一旦、コンピュータの使用を終了させた場合には、再度、入室時の照合処理を受けなければコンピュータの使用ができないようにしてあるので、コンピュータが備えられている部屋で、他人の非接触ＩＣカード等の情報記憶媒体を無断で使用してもコンピュータが機能されないので、コンピュータのセキュリティを確保することができるという効果がある。

【００２１】

また、本発明は、コンピュータが備えられている部屋の入口から入室した際に、情報記憶媒体に書き込まれた部屋情報と、コンピュータに記憶されている部屋情報とが照合一致しない場合には、コンピュータが起動できないので、コンピュータが備えられた部屋毎にコンピュータ使用者の管理を行なうことができるので、使用者毎のコンピュータの使用権限に応じてコンピュータの使用制限を行なうことができ、使用権限を有しない者のコンピュータの不正使用を防止することができるという効果がある。

更に、コンピュータが正常に起動した際に、情報記憶媒体に記憶されている部屋情報を消去させるので、既に部屋情報が記憶された情報記憶媒体を再度使用して不正にコンピュータを起動することができないので不正使用を防止できるという効果がある。

【００２２】

更に、本発明は、コンピュータが備えられている部屋の入口から入室した際に、情報記憶媒体に書き込まれた入室時刻情報に基づいて、コンピュータに記憶されている起動可能な時間帯情報の時間内であるのかを検証するので、深夜などに不正に入室してコンピュータを使用しようとしてもコンピュータの起動ができないので、使用権限を有しない者のコンピュータの不正使用を防止することができるという効果がある。

更に、コンピュータが正常に起動した際に、情報記憶媒体に記憶されている入室時刻情報を消去させるので、既に部屋情報が記憶された入室時刻情報を再度使用して不正にコンピュータを起動することができないので不正使用を防止できるという効果がある。

【発明を実施するための最良の形態】

【００２３】
以下、本発明の実施形態に係るコンピュータの不正使用防止システム及びその方法を図面に基づいて詳細に説明する。
図１は、本発明の第１実施形態に係るコンピュータの不正使用防止システムの概要を説明する図、図２は、非接触ＩＣカードの平面図、図３は、図２のＡ－Ａ線断面図、図４は、非接触ＩＣカードに内蔵されているＩＣタグの平面図、図５は、本発明の第１実施形態に係るコンピュータの不正使用防止システムのシステムブロック図、図６は、本発明の第１実施形態に係るコンピュータの不正使用防止システムにおける処理手順及びコンピュータの不正使用防止方法を説明するフローチャート、図７は、本発明の第２実施形態に係るコンピュータの不正使用防止システムの概要を説明する図、図８は、本発明の第２実施形態に係るコンピュータの不正使用防止システムのシステムブロック図、図９は、本発明の第２実施形態に係るコンピュータの不正使用防止システムにおける処理手順を説明するフローチャート、図１０は、本発明の第３実施形態に係るコンピュータの不正使用防止システムの概要を説明する図、図１１は、本発明の第３実施形態に係るコンピュータの不正使用防止システムのシステムブロック図、図１２は、本発明の第３実施形態に係るコンピュータの不正使用防止システムにおける処理手順を説明するフローチャートである。
【００２４】
まず、本発明の第１実施形態に係るコンピュータの不正使用防止システムの概要を図１に基づいて説明する。
本発明による不正使用の防止を行なうコンピュータ１は、使用者２が入室する際に、情報記憶媒体である非接触ＩＣカード３を用いたＩＤ照合処理による本人確認が行なわれる部屋４の内部に置かれている。
この部屋４の出入口５には、第１の装置である入室管理装置６が備えられ、入室管理装置６により出入口５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、入室する権限を有していない第三者の不正な入室ができないように管理されている。
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な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や、非接触ＩＣカード３への情報の書き込みを可能としている。
【００２５】
また、コンピュータ１には、第２の装置であるＩＣカードリーダライタ９がコンピュータ１と情報伝送可能に備えられている。
ＩＣカードリーダライタ９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な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や、非接触ＩＣカード３への情報の書き込みを可能としており、コンピュータ１からの制御信号により情報の読み取り処理や書き込み処理などをコントロール可能にしてある。
【００２６】
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３ａ，３ｂ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。
この非接触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手段８８が形成され、当該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し送信することができるように構成されている。
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。
【００２７】
図示した例の場合、コイルパターンからなる送受信手段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てコイル接続端子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、制御手段であるＣＰＵと、記憶手段であるメモリが備えられている。

【００２８】

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することができる。

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。

【００２９】

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が使用できるが、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。

【００３０】

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カードリーダライタ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タグからの応答信号を読み、且つ非接触ＩＣタグ８のＩＣチップ８２の記憶手段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の記憶手段であるメモリには、本人であることを認証するためのＩＤ情報が予め登録されている。

【００３１】

次に、本発明の第１実施形態に係るコンピュータの不正使用防止システムのシステム構成を図５に基いて説明する。

コンピュータが備えられている部屋４の出入口５付近に設けられた第１の装置である入室管理装置６には、送受信手段１０、照合手段１１、ドア開閉手段１２、フラグ書込手段１３、記憶手段１４、制御手段１５などを有している。

送受信手段１０は、非接触ＩＣカード３の送受信手段８８と無線による情報の送受信を行なうアンテナである。

また、照合手段１１は、非接触ＩＣカード３から受信したＩＤ情報を、記憶手段１４に予め記憶されている照合用のＩＤ情報を照合処理する機能を有していて、この照合手段１１による照合処理で一致した場合に、ドア開閉手段１２により自動ドア７が開かれるように機能する。

【００３２】

また、フラグ書込手段１３は、照合手段１１による照合処理で一致した場合に、送受信手段１０が非接触ＩＣカード３の送受信手段に対して、非接触ＩＣカード３の記憶手段９０に設けられているフラグ記憶領域に対して、入室を示すフラグが書き込まれるようにフラグ書込情報を送信させる機能を有している。

記憶手段１４には、非接触ＩＣカード３から受信したＩＤ情報と照合するための照合用のＩＤ情報が記憶されている。

【００３３】

次に、コンピュータ１には、表示手段１６、フラグ確認手段１７、コンピュータロック制御手段１８、フラグ消去手段１９、記憶手段２０、入力手段２１、制御手段２２などが備えられている。

フラグ確認手段１７は、ＩＣカードリーダライタ９から非接触ＩＣカード３に対して信号を送信して、非接触ＩＣカード３の記憶手段９０に設けられているフラグ記憶領域にフラグが書き込まれているか否かを確認する機能を有する。

【００３４】
コンピュータロック制御手段１８は、フラグ確認手段１７でのフラグの書込み状態によって、コンピュータ１を使用可能な状態と、使用できないロック状態とに制御する機能を有し、フラグ確認手段１７において、フラグが非接触ＩＣカード３の記憶手段９０に設けられているフラグ記憶領域に書込まれていることが確認された場合にだけ、コンピュータ１を使用可能な状態に制御する。
また、コンピュータ１の使用が終了された場合に、再度、コンピュータ１を使用できないロック状態に制御する機能を有している。
【００３５】
フラグ消去手段１９は、コンピュータ１の使用が終了された場合に、ＩＣカードリーダライタ９から非接触ＩＣカード３に対して信号を送信して、非接触ＩＣカード３の記憶手段９０に設けられているフラグ記憶領域に書き込まれているフラグを消去する機能を有する。
フラグ記憶領域のフラグが消去された場合には、コンピュータ１の利用者は、コンピュータ１が設置されている部屋４の出入口５から一旦出てから、再度、部屋４の出入口５付近に設けられた第１の装置である入室管理装置６により、照合手段１１による非接触ＩＣカード３のＩＤ情報による照合処理を行なう必要があり、部屋４の出入口５での非接触ＩＣカード３を用いた照合処理で、照合一致をしない場合には、コンピュータ１が使用できないようにシステム化されている。
【００３６】
また、コンピュータ１の使用が終了された場合に、再度、コンピュータ１を使用できないロック状態にすることで、部屋４の出入口５から退出する際に、非接触ＩＣカード３に記憶されているＩＤ情報をＩＣカードリーダライタ９や入室管理装置６などで読み取る手間が省けるようにしてある。
【００３７】
また、本発明の他の実施形態に係るコンピュータの不正使用防止システムでは、情報記憶媒体のフラグ記憶領域に予めフラグを書き込んだ状態にしておいてもよい。
このシステムの場合には、前記照合手段による照合処理で照合一致した場合に、情報記憶媒体のフラグ記憶領域に記憶されているフラグを消し込む手段を第１の装置である入室管理装置に設ける。
更に、コンピュータに、情報記憶媒体のフラグ記憶領域にフラグが書き込まれているか否かを確認するフラグ確認手段と、前記フラグ確認手段でフラグが書き込まれていることが確認された場合に、前記コンピュータの処理実行を可能とする状態に制御する手段とを設ける。
【００３８】
次に、本発明の第１実施形態の処理手順を図６のフローチャートに基いて説明する。
まず、コンピュータ１を使用しようとする使用者は、コンピュータが備えられている部屋の入口から入室する際に、所持している情報記憶媒体である非接触ＩＣカード３を入室管理装置６に近づけることで、入室管理装置６が非接触ＩＣカード３の記憶手段９０に記憶されているＩＤ情報を読み取る。（ステップＳ１）
入室管理装置６の照合手段１１により、この読み取られたＩＤ情報と、入室管理装置６の記憶手段１４に予め登録されているＩＤ情報との照合処理が行なわれる。（ステップＳ２）
【００３９】
この照合処理で照合一致した場合には、入室管理装置６のフラグ書込手段１３により送受信手段１０から非接触ＩＣカード３に対して、フラグを書き込むための信号が送信され、非接触ＩＣカード３のフラグ記憶領域に対してフラグが書き込まれる。（ステップＳ３）
これと略同時に、ドア開閉手段１２により自動ドア７が開いて、入室可能な状態になる。（ステップＳ４）

【００４０】
そして、入口から入室した使用者は、次にコンピュータ１に備えられているＩＣカードリーダライタ９に非接触ＩＣカード３を近づけて、非接触ＩＣカード３のフラグ記憶領域の書き込み状態からフラグが書き込まれているか否かが識別される。（ステップＳ５）
ここで、フラグ記憶領域にフラグが書き込まれていると判定された場合には、コンピュータロック制御手段１８によりコンピュータのロックが解除されて、コンピュータが使用可能な状態となる。（ステップＳ６）
【００４１】
また、フラグ記憶領域にフラグが書き込まれていないと判定された場合には、コンピュータロック制御手段１８によるコンピュータのロックが解除されることがなく、コンピュータの使用ができない状態のままで、その使用者によるコンピュータの使用ができない状態のまま終了するようにしてある。
【００４２】
また、前記ステップＳ２のＩＤ情報との照合処理において、照合不一致の場合には、入室管理装置６のフラグ書込手段１３により送受信手段１０から非接触ＩＣカード３に対して、フラグを書き込むための信号が送信されないで、自動ドア７が閉じた状態のままとなり、入室できないで処理も終了される。
【００４３】
次に、コンピュータ１の使用者がコンピュータ１の使用を終了する際に、フラグ消去手段１９により、ＩＣカードリーダライタ９から非接触ＩＣカード３に対して、非接触ＩＣカード３のフラグ記憶領域に書き込まれているフラグを消去する信号が送信されて、フラグ記憶領域にフラグが消去された状態にすることで、コンピュータ１の使用ができない状態にする。（ステップＳ７）
この処理により、その使用者がコンピュータ１を再度使用する場合には、もう一度、入口におけるＩＤ情報による照合処理を行なう必要があり、これによりコンピュータ１の使用が正規の入室者でなければできないように管理されている。
更に、コンピュータ１における時刻情報の検証処理で、検証が認められなかった場合には、警報音を発生させたり、メールを送信して不正を知らせるようにしてもよい。
【００４４】
また、情報記憶媒体のフラグ記憶領域に予めフラグを書き込んだ状態にしておいた場合には、前記照合手段による照合処理を行ない、照合一致した際に、情報記憶媒体のフラグ記憶領域に記憶されているフラグを消し込むステップとする。
そして、コンピュータで、情報記憶媒体のフラグ記憶領域にフラグが書き込まれているか否かを確認し、フラグ確認手段でフラグが書き込まれていることが確認された場合に、コンピュータの処理実行を可能とする状態に制御する。
【００４５】
また、情報記憶媒体は、非接触ＩＣカードに限らず、接触ＩＣカードや携帯電話機であってもよい。
【００４６】
次に、本発明の第２実施形態に係るコンピュータの不正使用防止システムの概要を図７に基づいて説明する。
本発明の第２実施形態に係るによる不正使用の防止を行なうコンピュータ１は、例えば、部屋、店舗、フロアー、建物、などの所定の場所に備えられている。
例えば、所定の部屋の備えられているコンピュータ１の不正防止をする場合において、使用者２が入室する際に、情報記憶媒体である非接触ＩＣカード３を用いたＩＤ照合処理による本人確認が行なわれる部屋４の内部に置かれている。
この部屋４の出入口５には、第１の装置である入室管理装置６が備えられ、入室管理装置６により出入口５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、入室する権限を有していない第三者の不正な入室ができないように管理されている。
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なえるよう

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や、非接触ＩＣカード３への情報の書き込みを可能としている。

【００４７】

また、コンピュータ１には、第２の装置であるＩＣカードリーダライタ９がコンピュータ１と情報伝送可能に備えられている。

ＩＣカードリーダライタ９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な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や、非接触ＩＣカード３への情報の書き込みを可能としており、コンピュータ１からの制御信号により情報の読み取り処理や書き込み処理などをコントロール可能にしてある。

また、非接触ＩＣカード３の記憶手段であるメモリには、本人であることを認証するためのＩＤ情報が予め登録されている。

【００４８】

次に、本発明の第２実施形態に係るコンピュータの不正使用防止システムのシステム構成を図５に基いて説明する。

コンピュータが備えられている部屋４の出入口５付近に設けられた第１の装置である入室管理装置６には、送受信手段１０、照合手段１１、ドア開閉手段１２、部屋特定情報書込手段２３、記憶手段１４、制御手段１５などを有している。

送受信手段１０は、非接触ＩＣカード３の送受信手段８８と無線による情報の送受信を行なうアンテナである。

また、照合手段１１は、非接触ＩＣカード３から受信したＩＤ情報を、記憶手段１４に予め記憶されている照合用のＩＤ情報を照合処理する機能を有していて、この照合手段１１による照合処理で一致した場合に、ドア開閉手段１２により自動ドア７が開かれるように機能する。

【００４９】

また、部屋特定情報書込手段２３は、照合手段１１による照合処理で一致した場合に、送受信手段１０が非接触ＩＣカード３の送受信手段に対して、入室する部屋を特定することができる部屋番号などの部屋特定情報を送信することで、非接触ＩＣカード３の記憶手段９０に対して部屋特定情報を書き込む機能を有している。

記憶手段１４には、非接触ＩＣカード３から受信したＩＤ情報と照合するための照合用のＩＤ情報が記憶されている。

【００５０】

次に、コンピュータ１には、表示手段１６、コンピュータロック制御手段１８、記憶手段２０、入力手段２１、制御手段２２、部屋特定情報照合手段２４、部屋特定情報消去手段２５などが備えられている。

そして、記憶手段２０には、予めコンピュータ１が設置されている部屋を特定することができる部屋番号などの部屋特定情報が予め登録されている。

部屋特定情報照合手段２４は、ＩＣカードリーダライタ９により非接触ＩＣカード３から読み取った部屋特定情報と、記憶手段２０に予め登録されている部屋特定情報との照合処理を行う機能を有している。

【００５１】

コンピュータロック制御手段１８は、部屋特定情報照合手段２４による照合処理の結果によって、コンピュータ１を使用可能な状態と、使用できないロック状態とに制御する機能を有し、部屋特定情報照合手段２４による照合処理において、照合一致した場合にだけ、コンピュータ１を使用可能な状態に制御する。

また、コンピュータ１の使用が終了された場合に、再度、コンピュータ１を使用できないロック状態に制御する機能を有している。

【００５２】

部屋特定情報消去手段２５は、コンピュータ１の使用が終了された場合に、ＩＣカードリーダライタ９から非接触ＩＣカード３に対して信号を送信して、非接触ＩＣカード３の記憶手段９０に書き込まれている部屋特定情報を消去する機能を有する。

この部屋特定情報が消去された場合には、コンピュータ１の利用者は、コンピュータ１が設置されている部屋４の出入口５から一旦出てから、再度、部屋４の出入口５付近に設けられた第１の装置である入室管理装置６により、照合手段１１による非接触ＩＣカード３のＩＤ情報による照合処理を行なう必要があり、部屋４の出入口５での非接触ＩＣカード３を用いた照合処理で、照合一致をしない場合には、コンピュータ１が使用できないようにシステム化されている。

【００５３】

また、コンピュータ１の使用が終了された場合に、再度、コンピュータ１を使用できないロック状態にすることで、部屋４の出入口５から退出する際に、非接触ＩＣカード３に記憶されているＩＤ情報をＩＣカードリーダライタ９や入室管理装置６などで読み取る手間が省けるようにしてある。

【００５４】

次に、本発明の第２実施形態の処理手順を図９のフローチャートに基いて説明する。

まず、コンピュータ１を使用しようとする使用者は、コンピュータが備えられている部屋の入口から入室する際に、所持している情報記憶媒体である非接触ＩＣカード３を入室管理装置６に近づけることで、入室管理装置６が非接触ＩＣカード３の記憶手段９０に記憶されているＩＤ情報を読み取る。（ステップＳ８）

入室管理装置６の照合手段１１により、この読み取られたＩＤ情報と、入室管理装置６の記憶手段１４に予め登録されているＩＤ情報との照合処理が行なわれる。（ステップＳ９）

【００５５】

この照合処理で照合一致した場合には、入室管理装置６の部屋特定情報書込手段２３により送受信手段１０から非接触ＩＣカード３に対して、部屋特定情報を書き込むための信号が送信され、非接触ＩＣカード３に対して部屋特定情報が書き込まれる。（ステップＳ１０）

これと略同時に、ドア開閉手段１２により自動ドア７が開いて、入室可能な状態になる。（ステップＳ１１）

【００５６】

そして、入口から入室した使用者は、ＩＣカードリーダライタ９に非接触ＩＣカード３を近づけて、非接触ＩＣカード３の記憶手段に記憶されている部屋特定情報を読み取り、部屋特定情報をコンピュータ１に送る。（ステップＳ１２）

次に、コンピュータ１において、ＩＣカードリーダライタ９で読み取られた部屋特定情報と、記憶手段２０に登録されている部屋特定情報を照合処理する。（ステップＳ１３）

【００５７】

この照合処理の結果、照合一致した場合には、コンピュータロック制御手段１８によるコンピュータのロックが解除されて、コンピュータの使用が行なえる状態に制御される。（ステップＳ１４）

また、照合処理の結果、照合不一致の場合には、コンピュータの使用ができない状態のままで、その使用者によるコンピュータの使用ができない状態のまま終了するようにしてある。

【００５８】

また、前記ステップＳ９のＩＤ情報との照合処理において、照合不一致の場合には、入室管理装置６の部屋特定情報書込手段２３により送受信手段１０から非接触ＩＣカード３に対して、部屋特定情報を書き込むための信号が送信されないで、自動ドア７が閉じた状態のままとなり、入室できないで処理も終了される。

【００５９】

次に、コンピュータ１の使用者がコンピュータ１の使用を終了する際に、部屋特定情報消去手段２５により、ＩＣカードリーダライタ９から非接触ＩＣカード３に対して、非接触ＩＣカード３の記憶手段９０に書き込まれている部屋特定情報を消去する信号が送信されて、コンピュータ１の使用ができない状態にする。（ステップＳ１５）

この処理により、その使用者がコンピュータ１を再度使用する場合には、もう一度、入口におけるＩＤ情報による照合処理を行なう必要があり、これによりコンピュータ１の使用が正規の入室者でなければできないように管理されている。

【００６０】

また、非接触ＩＣカード３の記憶手段９０に書き込まれた部屋特定情報を消去する場合に、コンピュータ１を用いて消去するのではなく、部屋４の出口にＩＣカードリーダライタを設けて、使用者が部屋から出る際に、非接触ＩＣカード３の記憶手段９０に書き込まれた部屋特定情報を消去するようにしてもよい。

更に、コンピュータ１における部屋特定情報の照合処理で、照合不一致の場合には、警報音を発生させたり、メールを送信して不正を知らせるようにしてもよい。

尚、上記の第２実施形態の説明では、場所の一例として部屋について説明したが、場所として、例えば、店舗、フロアー、建物、などであっても同様なシステムを利用することができる。。

【００６１】

次に、本発明の第３実施形態に係るコンピュータの不正使用防止システムの概要を図１０に基づいて説明する。

本発明による不正使用の防止を行なうコンピュータ１は、使用者２が入室する際に、情報記憶媒体である非接触ＩＣカード３を用いたＩＤ照合処理による本人確認が行なわれる部屋４の内部に置かれている。

この部屋４の出入口５には、第１の装置である入室管理装置６が備えられ、入室管理装置６により出入口５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、入室する権限を有していない第三者の不正な入室ができないように管理されている。

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な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や、非接触ＩＣカード３への情報の書き込みを可能としている。

【００６２】

また、コンピュータ１には、第２の装置であるＩＣカードリーダライタ９がコンピュータ１と情報伝送可能に備えられている。

ＩＣカードリーダライタ９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な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や、非接触ＩＣカード３への情報の書き込みを可能としており、コンピュータ１からの制御信号により情報の読み取り処理や書き込み処理などをコントロール可能にしてある。

また、非接触ＩＣカード３の記憶手段であるメモリには、本人であることを認証するためのＩＤ情報が予め登録されている。

【００６３】

次に、本発明の第３実施形態に係るコンピュータの不正使用防止システムのシステム構成を図１１に基いて説明する。

コンピュータが備えられている部屋４の出入口５付近に設けられた第１の装置である入室管理装置６には、送受信手段１０、照合手段１１、ドア開閉手段１２、入室時刻情報書込手段２６、記憶手段１４、制御手段１５などを有している。

送受信手段１０は、非接触ＩＣカード３の送受信手段８８と無線による情報の送受信を行なうアンテナである。

また、照合手段１１は、非接触ＩＣカード３から受信したＩＤ情報を、記憶手段１４に予め記憶されている照合用のＩＤ情報を照合処理する機能を有していて、この照合手段１１による照合処理で一致した場合に、ドア開閉手段１２により自動ドア７が開かれるように機能する。

【００６４】

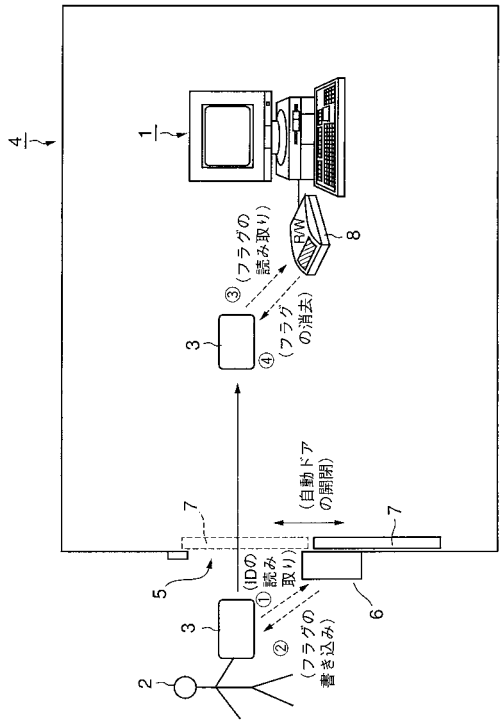
また、入室時刻情報書込手段２６は、照合手段１１による照合処理で一致した場合に、送受信手段１０が非接触ＩＣカード３の送受信手段に対して、入室した時刻情報を送信して、非接触ＩＣカード３の記憶手段９０に対して入室時刻情報を書き込む機能を有してい

る。
記憶手段１４には、非接触ＩＣカード３から受信したＩＤ情報と照合するための照合用のＩＤ情報が記憶されている。
【００６５】
次に、コンピュータ１には、表示手段１６、コンピュータロック制御手段１８、記憶手段２０、入力手段２１、制御手段２２、時刻検証手段２７、入室時刻情報消去手段２８などが備えられている。
そして、記憶手段２０には、予めコンピュータ１を起動可能な時間帯情報が登録されている。
時刻検証手段２７は、ＩＣカードリーダライタ９により非接触ＩＣカード３から読み取った入室した入室時刻情報と、記憶手段２０に予め登録されている時間帯情報との照合処理を行ない、入室時刻情報の入室時刻が、記憶手段２０に予め登録されている時間帯情報の時間帯内であるか否かを検証する機能を有している。
【００６６】
コンピュータロック制御手段１８は、時刻検証手段２７による検証の結果によって、コンピュータ１を使用可能な状態と、使用できないロック状態とに制御する機能を有し、検証の結果において、入室時刻が、記憶手段２０に予め登録されている時間帯情報の時間帯内である場合にだけ、コンピュータ１を使用可能な状態に制御し、更に、コンピュータ１の使用が終了された場合に、再度、コンピュータ１を使用できないロック状態に制御する機能を有している。
【００６７】
入室時刻情報消去手段２８は、コンピュータ１の使用が終了された場合に、ＩＣカードリーダライタ９から非接触ＩＣカード３に対して信号を送信して、非接触ＩＣカード３の記憶手段９０に書き込まれている入室時刻情報を消去する機能を有する。
この入室時刻情報が消去された場合には、コンピュータ１の利用者は、コンピュータ１が設置されている部屋４の出入口５から一旦出てから、再度、部屋４の出入口５付近に設けられた第１の装置である入室管理装置６により、照合手段１１による非接触ＩＣカード３のＩＤ情報による照合処理を行なう必要があり、部屋４の出入口５での非接触ＩＣカード３を用いた照合処理で、照合一致をしない場合には、コンピュータ１が使用できないようにシステム化されている。
【００６８】
また、コンピュータ１の使用が終了された場合に、再度、コンピュータ１を使用できないロック状態にすることで、部屋４の出入口５から退出する際に、非接触ＩＣカード３に記憶されているＩＤ情報をＩＣカードリーダライタ９や入室管理装置６などで読み取る手間が省けるようにしてある。
【００６９】
次に、本発明の第３実施形態の処理手順を図１２のフローチャートに基いて説明する。
まず、コンピュータ１を使用しようとする使用者は、コンピュータが備えられている部屋の入口から入室する際に、所持している情報記憶媒体である非接触ＩＣカード３を入室管理装置６に近づけることで、入室管理装置６が非接触ＩＣカード３の記憶手段９０に記憶されているＩＤ情報を読み取る。（ステップＳ１６）
入室管理装置６の照合手段１１により、この読み取られたＩＤ情報と、入室管理装置６の記憶手段１４に予め登録されているＩＤ情報との照合処理が行なわれる。（ステップＳ１７）
【００７０】
この照合処理で照合一致した場合には、入室管理装置６の入室時刻情報書込手段２６により送受信手段１０から非接触ＩＣカード３に対して、入室時刻情報を書き込むための信号が送信され、非接触ＩＣカード３に対して入室時刻が書き込まれる。（ステップＳ１８）
これと略同時に、ドア開閉手段１２により自動ドア７が開いて、入室可能な状態になる

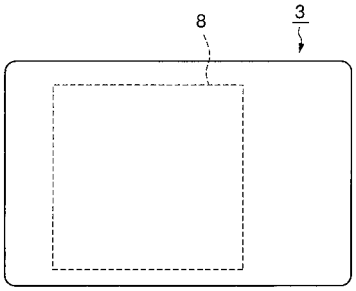
。（ステップＳ１９）
【００７１】
そして、入口から入室した使用者は、ＩＣカードリーダライタ９に非接触ＩＣカード３を近づけて、非接触ＩＣカード３の記憶手段に記憶されている入室時刻情報を読み取り、入室時刻情報をコンピュータ１に送る。（ステップＳ２０）
次に、コンピュータ１において、ＩＣカードリーダライタ９で読み取られた入室時刻情報と、記憶手段２０に登録されている時間帯情報とを照合して、その入室時刻がその時間帯内に入っている時刻であるか否かを検証する。（ステップＳ２１）
【００７２】
この検証処理の結果、入室時刻がその時間帯内に入っている時刻であると認証された場合には、コンピュータロック制御手段１８によるコンピュータのロックが解除されて、コンピュータの使用が行なえる状態に制御される。（ステップＳ２２）
また、検証処理の結果、入室時刻がその時間帯外の時刻であると判定された場合には、コンピュータの使用ができない状態のままで、その使用者によるコンピュータの使用ができない状態のまま終了するようにしてある。
【００７３】
また、前記ステップＳ１７のＩＤ情報との照合処理において、照合不一致の場合には、入室管理装置６の入室時刻情報書込手段２６により送受信手段１０から非接触ＩＣカード３に対して、入室時刻情報を書き込むための信号が送信されないで、自動ドア７が閉じた状態のままとなり、入室できないで処理も終了される。
【００７４】
次に、コンピュータ１の使用者がコンピュータ１の使用を終了する際に、入室時刻情報消去手段２８により、ＩＣカードリーダライタ９から非接触ＩＣカード３に対して、非接触ＩＣカード３の記憶手段９０に書き込まれている入室時刻情報を消去する信号が送信されて、コンピュータ１の使用ができない状態にする。（ステップＳ２３）
この処理により、その使用者がコンピュータ１を再度使用する場合には、もう一度、入口におけるＩＤ情報による照合処理を行なう必要があり、これによりコンピュータ１の使用が正規の入室者でなければできないように管理されている。
【００７５】
また、非接触ＩＣカード３の記憶手段９０に書き込まれた時刻情報を消去する場合に、コンピュータ１を用いて消去するのではなく、部屋４の出口にＩＣカードリーダライタを設けて、使用者が部屋から出る際に、非接触ＩＣカード３の記憶手段９０に書き込まれた時刻情報を消去するようにしてもよい。
更に、コンピュータ１における時刻情報の検証処理で、検証が認められなかった場合には、警報音を発生させたり、メールを送信して不正を知らせるようにしてもよい。
【図面の簡単な説明】
【００７６】
【図１】本発明の第１実施形態に係るコンピュータの不正使用防止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】本発明の第１実施形態に係るコンピュータの不正使用防止システムのシステムブロック図である。
【図６】本発明の第１実施形態に係るコンピュータの不正使用防止システムにおける処理手順及びコンピュータの不正使用防止方法を説明するフローチャートである。
【図７】本発明の第２実施形態に係るコンピュータの不正使用防止システムの概要を説明する図である。
【図８】本発明の第２実施形態に係るコンピュータの不正使用防止システムのシステムブロック図である。

【図９】本発明の第２実施形態に係るコンピュータの不正使用防止システムにおける処理手順を説明するフローチャートである。
【図１０】本発明の第３実施形態に係るコンピュータの不正使用防止システムの概要を説明する図である。
【図１１】本発明の第３実施形態に係るコンピュータの不正使用防止システムのシステムブロック図である。
【図１２】本発明の第３実施形態に係るコンピュータの不正使用防止システムにおける処理手順を説明するフローチャートである。
【符号の説明】
【００７７】
１　コンピュータ
２　使用者
３　非接触ＩＣカード
３ａ，３ｂ　カード基材
４　部屋
５　出入口
６　入室管理装置
７　自動ドア
８　非接触ＩＣタグ
９　ＩＣカードリーダライタ
１０，８８　送受信手段
１１　照合手段
１２　ドア開閉手段
１３　フラグ書込手段
１４，２０，９０　記憶手段
１５，２２，８９　制御手段
１６　表示手段
１７　フラグ確認手段
１８　コンピュータロック制御手段
１９　フラグ消去手段
２１　入力手段
２３　部屋特定情報書込手段
２４　部屋特定情報照合手段
２５　部屋特定情報消去手段
２６　入室時刻情報書込手段
２７　時刻検証手段
２８　入室時刻情報消去手段
８１　基材
８２　ＩＣチップ
８４　導通部材
８８Ｃ　コイル接続端子

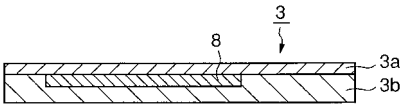
【図１】


4
1
8
RW
③（フラグの読み取り）
④（フラグの消去）
3
（自動ドアの開閉）
7
7
5
6
①（IDの読み取り）
②（フラグの書き込み）
3
2

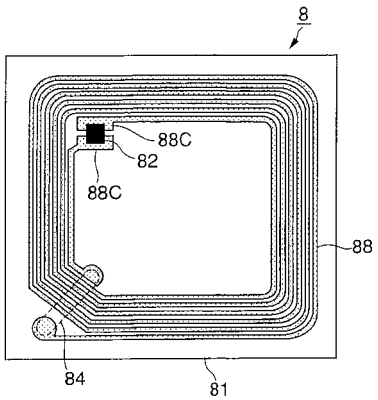
【図２】


8
3

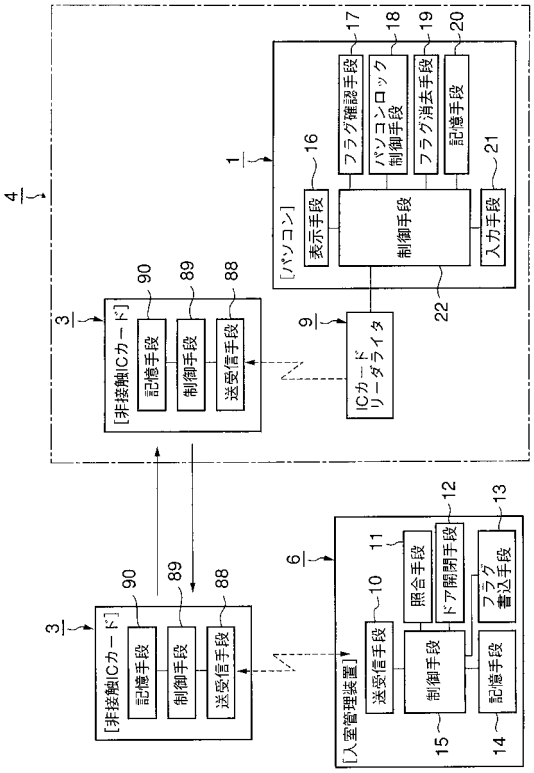
【図３】


3
8
3a
3b

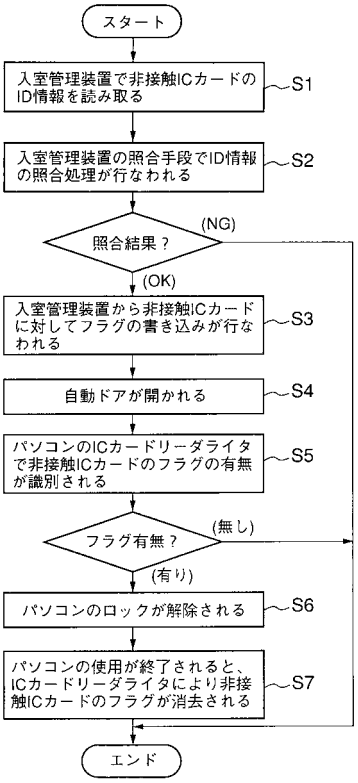
【図４】


8
88C
82
88C
88
84
81

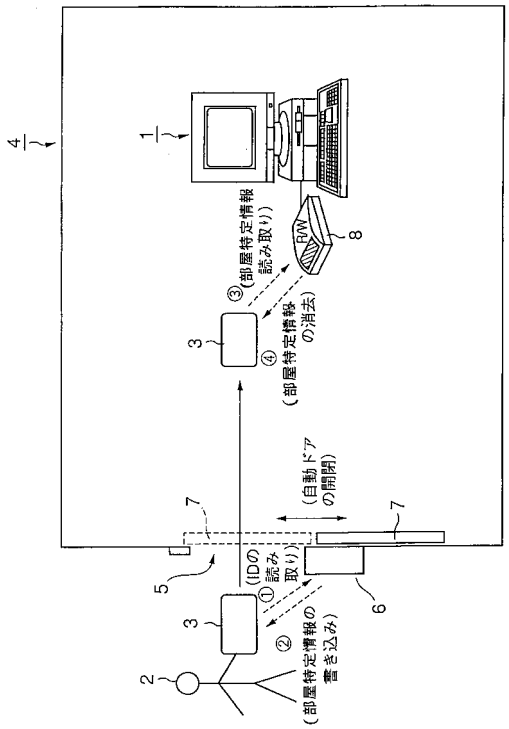
【図５】


4
1
[パソコン]
表示手段
16
制御手段
入力手段
21
フラグ確認手段
17
パソコンロック制御手段
18
フラグ消去手段
19
記憶手段
20
22
3
[非接触ICカード]
記憶手段
90
制御手段
89
送受信手段
88
9
ICカードリーダライタ
6
[入室管理装置]
送受信手段
10
制御手段
15
照合手段
11
ドア開閉手段
12
フラグ書込手段
13
記憶手段
14

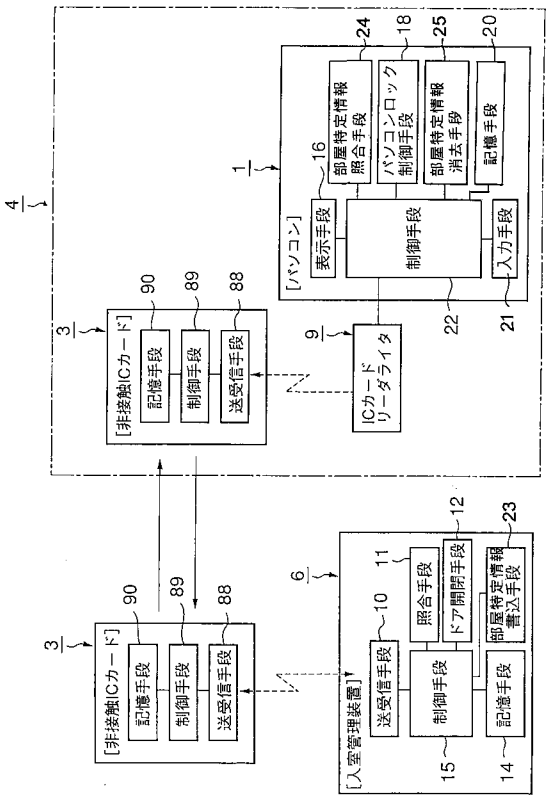
【図６】


スタート
入室管理装置で非接触ICカードのID情報を読み取る
S1
入室管理装置の照合手段でID情報の照合処理が行なわれる
S2
照合結果？
(NG)
(OK)
入室管理装置から非接触ICカードに対してフラグの書き込みが行なわれる
S3
自動ドアが開かれる
S4
パソコンのICカードリーダライタで非接触ICカードのフラグの有無が識別される
S5
フラグ有無？
(無し)
(有り)
パソコンのロックが解除される
S6
パソコンの使用が終了されると、ICカードリーダライタにより非接触ICカードのフラグが消去される
S7
エンド

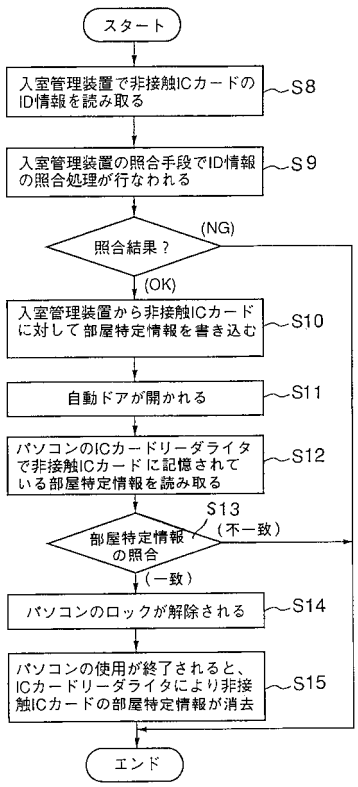
【図７】


4
1
8
P/W
③(部屋特定情報読み取り)
④(部屋特定情報の消去)
3
(自動ドアの開閉)
7
7
5
(IDの読み取り)①
6
3
②(部屋特定情報の書き込み)
2

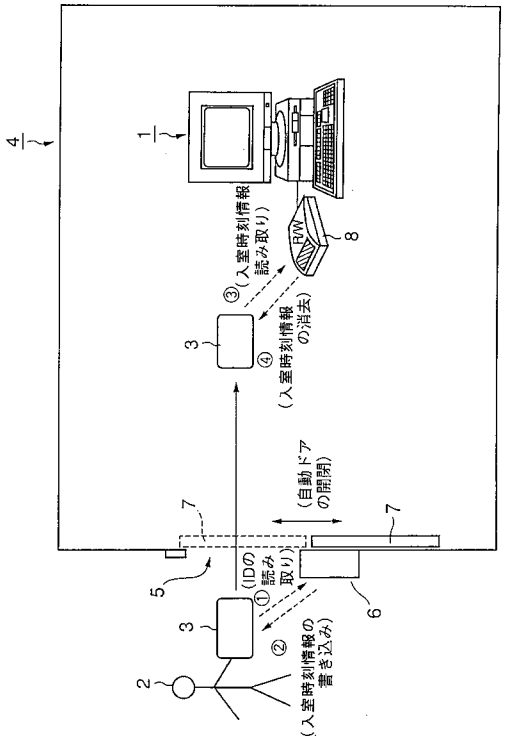
【図８】


4
1
[パソコン]
16 部屋特定情報照合手段
24
18 パソコンロック制御手段
25 部屋特定情報消去手段
20 記憶手段
表示手段
制御手段
入力手段
22
21
3
[非接触ICカード]
90 記憶手段
89 制御手段
88 送受信手段
9
ICカードリータライタ
6
[入室管理装置]
10 送受信手段
11 照合手段
12 ドア開閉手段
23 部屋特定情報書込手段
制御手段
15
14 記憶手段

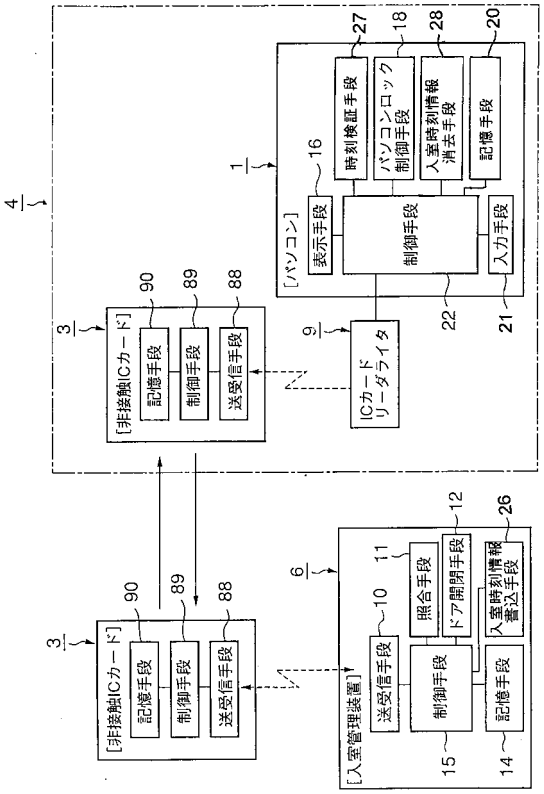
【図９】


スタート
入室管理装置で非接触ICカードのID情報を読み取る
S8
入室管理装置の照合手段でID情報の照合処理が行なわれる
S9
照合結果？
(NG)
(OK)
入室管理装置から非接触ICカードに対して部屋特定情報を書き込む
S10
自動ドアが開かれる
S11
パソコンのICカードリーダライタで非接触ICカードに記憶されている部屋特定情報を読み取る
S12
S13
部屋特定情報の照合
(不一致)
(一致)
パソコンのロックが解除される
S14
パソコンの使用が終了されると、ICカードリーダライタにより非接触ICカードの部屋特定情報が消去
S15
エンド

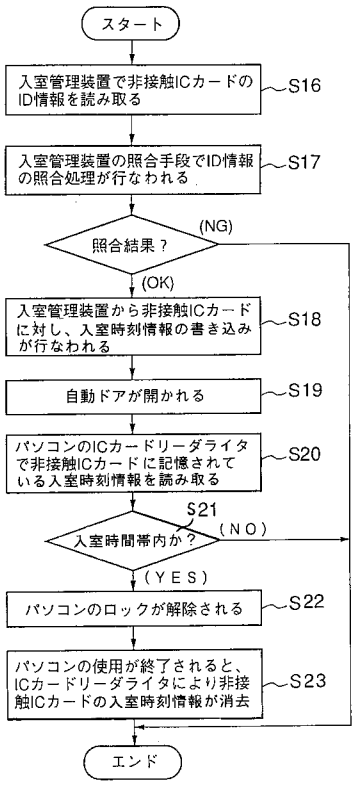
【図１０】


4
1
8
R/W
③（入室時刻情報読み取り）
④（入室時刻情報の消去）
3
（自動ドアの開閉）
7
7
5
①（IDの読み取り）
6
3
②（入室時刻情報の書き込み）
2

【図１１】


4
1
[パソコン]
16
表示手段
制御手段
入力手段
22
21
27
時刻検証手段
18
パソコンロック制御手段
28
入室時刻情報消去手段
20
記憶手段
3
[非接触ICカード]
90
記憶手段
89
制御手段
88
送受信手段
9
ICカードリーダライタ
6
[入室管理装置]
10
送受信手段
15
制御手段
14
記憶手段
11
照合手段
ドア開閉手段
12
26
入室時刻情報書込手段

【図１２】


スタート
入室管理装置で非接触ICカードのID情報を読み取る
S16
入室管理装置の照合手段でID情報の照合処理が行なわれる
S17
照合結果？
(NG)
(OK)
入室管理装置から非接触ICカードに対し、入室時刻情報の書き込みが行なわれる
S18
自動ドアが開かれる
S19
パソコンのICカードリーダライタで非接触ICカードに記憶されている入室時刻情報を読み取る
S20
S21
入室時間帯内か？
(NO)
(YES)
パソコンのロックが解除される
S22
パソコンの使用が終了されると、ICカードリーダライタにより非接触ICカードの入室時刻情報が消去
S23
エンド

フロントページの続き

合議体
審判長　小松　正
審判官　月野　洋一郎
審判官　関谷　隆一

(56)参考文献　特開２０００－２５９８７８（ＪＰ，Ａ）
特開２００２－１９７５００（ＪＰ，Ａ）
特開２００１－５１９５０（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F 1/00