(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2010-92172
(P2010-92172A)
(43)公開日　平成22年4月22日(2010.4.22)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/20	(2006.01)	G06F	15/00	330D	3E038
G07C 9/00	(2006.01)	G07C	9/00	Z	5B285

審査請求 未請求　請求項の数 9　ＯＬ　（全 38 頁）

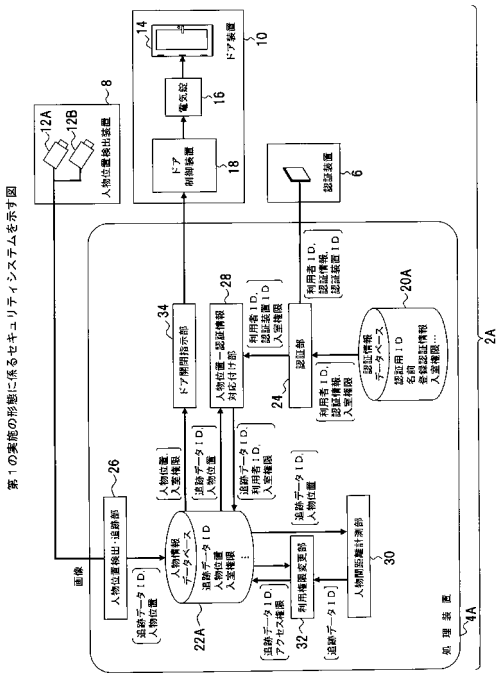
(21)出願番号　特願2008-259955 (P2008-259955)
(22)出願日　平成20年10月6日 (2008.10.6)

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(74)代理人　100083725
弁理士　畝本　正一
(72)発明者　辻　健太郎
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　瀬川　英吾
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　塩原　守人
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

最終頁に続く

(54)【発明の名称】セキュリティシステム、セキュリティプログラム及びセキュリティ方法

(57)【要約】
【課題】施設利用等のセキュリティに関し、認証要求の回数を低減して利便性を高めるとともに、認証により付与された利用権限の他人利用を防止し、又は、施設利用等のセキュリティに関し、一度認証したら毎回認証を行わなくても利用権限を維持し、利用権限のない他人利用を防止する。
【解決手段】利用者に認証により利用権限を付与し、一旦利用権限が付与された利用者は認証の省略を可能にして利便性を高めるとともに、利用者が他の利用者との距離に応じ（他人との接触等）、利用権限を変更することにより、利用権限のない他人の権限利用を防止する。認証回数の低減による利便性の向上に対し、利用者間の距離（接近）により利用権限を変更し、利用権限がない部屋やＰＣログイン等の利用を防止することにより、セキュリティの低下防止と利便性向上とを図っている。
【選択図】図１



【特許請求の範囲】
【請求項１】
特定エリアの利用者に認証に基づく利用権限を付与し、その利用権限により前記特定エリアの利用を許可するセキュリティシステムであって、
利用者を認証する認証手段と、
利用者の位置及び／又はその移動を検出する位置検出手段と、
前記認証手段の認証に基づき、利用権限が付与された利用者の位置及び／又はその移動を前記位置検出手段の検出出力によって監視し、利用者間の距離が所定値以下になった場合、各利用者に付与されている利用権限を変更する利用権限制御手段と、
を備えることを特徴とするセキュリティシステム。
【請求項２】
請求項１のセキュリティシステムにおいて、
前記利用権限制御手段は、前記認証に基づき、利用者に同一又は異なるレベルの利用権限を設定し、利用者間の距離が所定値以下になった場合に、各利用者に設定されている利用権限をレベルの低い利用権限に変更する構成としたことを特徴とするセキュリティシステム。
【請求項３】
請求項１のセキュリティシステムにおいて、
認証した利用者を追跡する利用者追跡手段を備え、前記利用権限制御手段は、前記利用者追跡手段の追跡に基づき、前記利用者の利用権限又は変更された利用権限を維持する構成としたことを特徴とするセキュリティシステム。
【請求項４】
請求項１のセキュリティシステムにおいて、
前記利用権限制御手段は、前記利用権限をサービス毎に設定し、利用者間の距離が所定値以下になった場合に、各利用者に設定されている利用権限を、サービスとの論理積により求められた利用権限に変更する構成としたことを特徴とするセキュリティシステム。
【請求項５】
請求項１のセキュリティシステムにおいて、
前記利用権限制御手段は、利用者間の距離が所定値以下になった場合に、各利用者の利用権限の低減又は解除をする構成としたことを特徴とするセキュリティシステム。
【請求項６】
請求項１、２、３、４又は５のセキュリティシステムにおいて、
前記利用権限制御手段は、利用権限が変更された利用者が再認証を受けることにより、新たな利用権限を受け得る構成としたことを特徴とするセキュリティシステム。
【請求項７】
請求項１のセキュリティシステムにおいて、
前記利用権限制御手段は、認証を受けた利用者と、他の利用者との距離が所定値内であることを検出した場合、認証を受けた利用者に利用権限を与えない構成としたことを特徴とするセキュリティシステム。
【請求項８】
特定エリアの利用者に認証に基づく利用権限を付与し、その利用権限により前記特定エリアの利用を許可する機能を備え、斯かる機能をコンピュータに実行させるセキュリティプログラムであって、
利用者を認証する認証機能と、
利用者の位置及び／又はその移動を表す検出情報を取り込む検出情報取込み機能と、
前記認証に基づき、利用権限が付与された利用者の位置及び／又はその移動を前記検出情報によって監視し、利用者間の距離が所定値以下になった場合、各利用者に付与されている利用権限を変更する利用権限制御機能と、
をコンピュータに実行させることを特徴とするセキュリティプログラム。
【請求項９】

特定エリアの利用者に認証に基づく利用権限を付与し、その利用権限により前記特定エリアの利用を許可するセキュリティ方法であって、
利用者を認証する認証ステップと、
利用者の位置及び／又はその移動を検出する位置検出ステップと、
前記認証に基づき、利用権限が付与された利用者の位置及び／又はその移動を監視し、利用者間の距離が所定値以下になった場合、各利用者に付与されている利用権限を変更するステップと、
を含むことを特徴とするセキュリティ方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、複数の人が利用する複数の施設等のセキュリティに関し、特に、施設等のエリアの利用権限を制御し、利用権限のない人に対するサービス提供等を防止するセキュリティシステム、セキュリティプログラム及びセキュリティ方法に関する。
【背景技術】
【０００２】
個人認証にＩＤ（IDentification）カードやパスワードを用いてドアの開錠やＰＣ（パーソナルコンピュータ）のログイン等を行うセキュリティシステムが普及している。このようなシステムでは、部屋等のと施設や装置毎に認証作業が要求され、施設の出入等、移動を伴う場合には進入毎に要求される認証が煩雑であり、非常に手間がかかる。このため、利便性を高めるため、カメラやレーザセンサ等の機器を組み合わせ、認証を受けた人の位置を把握し、認証を受けた人であれば、再認証を受けることなく、ドアの開錠やＰＣのログインが行えるシステムがある。
【０００３】
このようなセキュリティシステムに関し、特許文献１には、カメラによって人を追跡し、認証が行われた際には、その人の移動軌跡と認証情報とを対応付けることで、ドアの前にいる人が認証を受けなくてもその人の移動軌跡の属性（認証していること）を調べて開錠の判断を行うことが開示されている。
【０００４】
特許文献２では、操作内容の重要性に応じて異なる認証を要求し、その認証によって権限を得た場合でも一定時間経過すると権限を元に戻すことにより、権限のない人が重要な操作を行うことを防止することが開示されている。
【０００５】
特許文献３には、利用者がサービスを受けているときに、非利用者がサービス利用圏内に入るとサービスを中断し、非利用者がサービスを受けることを防止することが開示されている。
【０００６】
また、特許文献４には、利用者の他にアクセス権限を持つ人（高利用者）がいるときのみ操作可能とし、利用者の操作を他者が監視することによって、誤った操作や不正な操作が行われることを防止することが開示されている。
【特許文献１】特開２００４－１８５４８４号公報
【特許文献２】特開平９－１６５２３号公報
【特許文献３】特開平９－２９７７３５号公報
【特許文献４】特開２００３－２２３４２１号公報
【発明の開示】
【発明が解決しようとする課題】
【０００７】
ところで、人の移動軌跡と認証情報とを関係付けるシテスム（特許文献１）では、認証の後に、ある人が別人と入れ違えて誤追跡すると、本人以外の他人に認証結果が対応付けられる。この場合には認証を受けていない人を受入れ、サービスが受けられるというセキ

ュリティの低下を引き起こすおそれがある。認証を受けた人のみが利用権限を保持し、他の人がその人にすり代わってサービスを受けることを防止する必要がある。

【０００８】

操作内容の重要性に応じて異なる認証をする場合（特許文献２）では、一定時間経過すると権限を元に戻すので、認証を受けても一定時間内は別の人とすり代わることが可能であり、それを防止するために一定時間を短く設定すると、利便性が失われる。

【０００９】

利用者がサービスを受けているときに、非利用者がサービス利用圏内に入るとサービスを中断するシステム（特許文献３）では、機器の動作を制御するのみで、非利用者が近づいても利用者のアクセス権を変更するわけではないため、非利用者と利用者が近づいて入れ換わると不正利用が可能となるという問題がある。

【００１０】

利用者の他にアクセス権限を持つ人（高利用者）がいるときのみ操作可能とし、利用者の操作を他者が監視するシテスム（特許文献４）では、人の位置の検出を行っていないため、利用者認証を行い、利用者が操作権利を一旦得ると、高権利者の状態に拘らずアクセスが可能であるという問題がある。

【００１１】

斯かる要求や課題について、特許文献１ないし４にはその開示や示唆はなく、それを解決する構成等についての開示や示唆はない。

【００１２】

そこで、本発明の目的は、施設利用等のセキュリティに関し、認証要求の回数を低減して利便性を高めるとともに、認証により付与された利用権限の他人利用を防止することを目的とする。

【００１３】

また、本発明の他の目的は、施設利用等のセキュリティに関し、一度認証したら毎回認証を行わなくても利用権限を維持し、利用権限のない他人利用を防止することにある。

【課題を解決するための手段】

【００１４】

上記目的を達成するため、本発明は、利用者に認証により利用権限を付与し、一旦利用権限が付与された利用者は認証の省略を可能にして利便性を高めるとともに、利用者が他の利用者との距離に応じ（他人との接触等）、利用権限を変更することにより、利用権限のない他人の権限利用を防止する。即ち、利用者が認証後、その利用者より権限の低い他の利用者と接近した場合には、利用権限のレベルを低下させる。認証回数の低減による利便性の向上に対し、利用者間の距離（接近）により利用権限を変更し、利用権限がない部屋やＰＣログイン等の利用を防止することにより、セキュリティの低下防止と利便性向上とを図っている。

【００１５】

上記目的を達成するため、本発明は、特定エリアの利用者に認証に基づく利用権限を付与し、その利用権限により前記特定エリアの利用を許可するセキュリティシステムであって、利用者を認証する認証手段と、利用者の位置及び／又はその移動を検出する位置検出手段と、前記認証手段の認証に基づき、利用権限が付与された利用者の位置及び／又はその移動を前記位置検出手段の検出出力によって監視し、利用者間の距離が所定値以下になった場合、各利用者に付与されている利用権限を変更する利用権限制御手段とを備えることである。

【００１６】

上記構成では、認証手段で認証された利用者の位置及び／又はその移動が位置検出手段により検出されるので、利用権限制御手段は、認証手段の認証に基づき、利用権限が付与された利用者の位置及び／又はその移動を位置検出手段の検出出力によって監視し、利用者間の距離が所定値以下になった場合、各利用者に付与されている利用権限を変更し、利用者が他の利用者と接触した場合即ち、利用者間の距離が所定値以下になった場合には利

用権限を変更することにより、セキュリティレベルを向上させ、また、他の利用者との接触がなければ、認証した利用者はその利用権限を維持させることができ、利便性の向上とともに高度なセキュリティを維持することができる。

【００１７】

上記目的を達成するためには、上記セキュリティシステムにおいて、好ましくは、前記利用権限制御手段は、前記認証に基づき、利用者に同一又は異なるレベルの利用権限を設定し、利用者間の距離が所定値以下になった場合に、各利用者に設定されている利用権限をレベルの低い利用権限に変更する構成としてもよい。斯かる構成によっても上記目的を達成できる。

【００１８】

上記目的を達成するためには、上記セキュリティシステムにおいて、好ましくは、認証した利用者を追跡する利用者追跡手段を備え、前記利用権限制御手段は、前記利用者追跡手段の追跡に基づき、前記利用者の利用権限又は変更された利用権限を維持する構成としてもよい。斯かる構成によれば、認証を受けた利用者は、利用者追跡手段の追跡情報に基づき、利用権限が維持され、その利用権限は当初の利用権限又は既述の他人との接触による低下した利用権限であるから、繰り返しの認証を受けることなく利用権限を維持でき、セキュリティレベルの低下を来すことなく、利便性を高めることができる。

【００１９】

上記目的を達成するためには、上記セキュリティシステムにおいて、好ましくは、前記利用権限制御手段は、前記利用権限をサービス毎に設定し、利用者間の距離が所定値以下になった場合に、各利用者に設定されている利用権限を、サービスとの論理積により求められた利用権限に変更する構成としてもよいし、また、前記利用権限制御手段は、利用者間の距離が所定値以下になった場合に、各利用者の利用権限の低減又は解除をする構成としてもよい。斯かる構成によっても上記目的を達成できる。

【００２０】

上記目的を達成するためには、上記セキュリティシステムにおいて、好ましくは、前記利用権限制御手段は、利用権限が変更された利用者が再認証を受けることにより、新たな利用権限を受け得る構成としてもよいし、また、前記利用権限制御手段は、認証を受けた利用者と、他の利用者との距離が所定値内であることを検出した場合、認証を受けた利用者に利用権限を与えない構成としてもよい。斯かる構成によっても上記目的を達成できる。

【００２１】

上記目的を達成するため、本発明は、特定エリアの利用者に認証に基づく利用権限を付与し、その利用権限により前記特定エリアの利用を許可する機能を備え、斯かる機能をコンピュータに実行させるセキュリティプログラムであって、利用者を認証する認証機能と、利用者の位置及び／又はその移動を表す検出情報を取り込む検出情報取込み機能と、前記認証に基づき、利用権限が付与された利用者の位置及び／又はその移動を前記検出情報によって監視し、利用者間の距離が所定値以下になった場合、各利用者に付与されている利用権限を変更する利用権限制御機能とをコンピュータに実行させることである。斯かる構成によっても、上記目的を達成することができる。

【００２２】

上記目的を達成するため、本発明は、特定エリアの利用者に認証に基づく利用権限を付与し、その利用権限により前記特定エリアの利用を許可するセキュリティ方法であって、利用者を認証する認証ステップと、利用者の位置及び／又はその移動を検出する位置検出ステップと、前記認証に基づき、利用権限が付与された利用者の位置及び／又はその移動を監視し、利用者間の距離が所定値以下になった場合、各利用者に付与されている利用権限を変更するステップとを含むことである。斯かる構成によっても、上記目的を達成することができる。

【発明の効果】

【００２３】

本発明によれば、次のような効果が得られる。

【００２４】

(1) 利用者は認証を受けることによって付与される利用権限に基づき、特定エリア内のサービス提供等の利用が可能であり、一度認証したら繰り返しの認証を求めることなく利用権限を維持する等、利便性を高めることができるとともに、利用権限を持たない他人利用を防止できる。

【００２５】

(2) 認証を受けた利用者は、特定エリア内で位置及び／又はその移動が監視され、他の利用者との距離が所定値以下になった場合には、利用者の利用権限を変更し、例えば、各利用者の持つ共通の利用権限以下に低下し、利用権限を持たない他人の利用を防止でき、セキュリティ低下を防止できる。

【００２６】

(3) 利用権限を持たない人の利用を防止でき、利用者の位置や移動を追跡し、移動軌跡に認証結果を対応付けるので、一度の認証の後、繰り返しの認証を避け、セキュリティ低下を防止するとともに、利便性を高めることができる。

【００２７】

そして、本発明の他の目的、特徴及び利点は、添付図面及び各実施の形態を参照することにより、一層明確になるであろう。

【発明を実施するための最良の形態】

【００２８】

〔第１の実施の形態〕

【００２９】

第１の実施の形態について、図１を参照する。図１は、第１の実施の形態に斯かるセキュリティシステムを示す図である。図１に示す構成は一例であって、斯かる構成に本発明が限定されるものではない。

【００３０】

このセキュリティシステム２Ａは、特定エリアとして設定された監視範囲に対し、進入者に認証を求め、認証の成立によって利用権限を付与し、利用権限が付与された利用者を追跡して繰返しの認証を要求することなく利用権限を維持するとともに、監視範囲内の全ての人の位置をカメラやレーダ等の位置検出手段により検出し、利用権限を有する人が利用権限のない人に接近したときに、接近者が持っている利用権限に応じて利用権限を制御し、人（接近した人同士）を入れ換えて誤追跡した場合でも、利用権限がないか制限された人に対するサービスの提供を阻止するように構成されている。

【００３１】

このセキュリティシステム２Ａでは、図１に示すように、処理装置４Ａと、認証装置６と、人物位置検出装置８と、ドア装置１０とを備えている。処理装置４Ａは、認証及び人物の検出及び追跡に基づく利用権限を制御する制御手段であって、具体的には、認証装置６による認証と、利用者追跡手段としての人物位置検出装置８による人物位置の検出及び追跡と、これら認証及び人物の追跡に基づくドア装置１０の施錠又は開錠等を行う。利用権限の制御には、利用権限の変更、低減又は解除が含まれる。

【００３２】

認証装置６は、指紋、静脈、虹彩等の生体情報等の認証情報、利用者ＩＤ、認証装置ＩＤ等、認証に用いる情報を処理装置４Ａに入力する入力手段である。

【００３３】

人物位置検出装置８は例えば、単一又は複数の撮像手段として例えば、撮像装置１２Ａ、１２Ｂで構成され、検出した人物及びその追跡を表す映像を処理装置４Ａに提供する。撮像装置１２Ａ、１２Ｂは、例えばレーザセンサやＲＦＩＤリーダ等、人物の位置を知る手段であって、斯かる機能を備えた手段であれば撮像装置１２Ａ、１２Ｂに代えることができる。即ち、人物位置検出装置８は、処理装置４Ａとともに利用者追跡手段を構成している。

【００３４】
ドア装置１０は、ドア１４と、電気錠１６と、ドア制御装置１８とを備えている。ドア１４は、監視範囲である室の出入部に設置された開閉ドアである。電気錠１６は、ドア１４の出入りを許可又は禁止する手段として施錠又はその開錠を行う。ドア制御装置１８は、処理装置４Ａによって制御され、電気錠１６の施錠又は開錠をする制御手段である。
【００３５】
そして、処理装置４Ａは、認証及び人物の検出及び追跡に基づく利用権限を制御する手段として、認証情報データベース２０Ａと、人物情報データベース２２Ａと、認証部２４と、人物位置検出・追跡部２６と、人物位置－認証情報対応付け部２８と、人物間距離計測部３０と、利用権限変更部３２と、ドア開閉指示部３４とを備える。
【００３６】
認証情報データベース２０Ａは、利用者の認証情報を管理する利用者１Ｄ、登録してある人物の名前、認証情報と比較して本人か否かを判断する登録認証情報、その人が入室できるドアを示す入室権限等、利用者認証処理を行うための情報が登録されたデータベースである。この認証情報データベース２０Ａには、認証用ＩＤ、名前、登録認証情報、入室権限等を表す情報が格納されている。
【００３７】
人物情報データベース２２Ａは、それぞれの人物毎に、追跡データを管理する追跡データＩＤ、追跡データが誰であるかを示す利用者ＩＤ、現在開錠可能なドアを示す入室権限、人物の現在位置、移動軌跡等、人物の現在の状況を表す情報が登録されたデータベースである。人物情報データベース２２Ａには、追跡データＩＤ、人物位置、入室権限等の人物情報が格納されている。
【００３８】
認証部２４は、認証装置６に入力される生体情報等の入力認証情報と、認証情報データベース２０Ａにある登録認証情報とに基づいて利用者の認証を行う認証手段である。認証部２４は、認証装置６から入力された利用者ＩＤ、認証情報、認証装置ＩＤ等の入力認証情報と、認証情報データベース２０Ａにある利用者ＩＤ、認証情報、入室権限等の登録情報とを照合し、その認証結果として利用者ＩＤ、認証装置ＩＤ、入室権限等を出力し、人物位置－認証情報対応付け部２８に提供する。
【００３９】
人物位置検出・追跡部２６は、利用者の位置及び／又はその移動を検出する位置検出手段の一例であって、撮像装置１２Ａ、１２Ｂで取得された画像から人物の検出、その位置の検出及び又はその移動を追跡する人物位置検出及び／又は追跡を行い、追跡データＩＤ、人物位置等の人物情報（利用者情報）を生成する。この人物情報は、人物情報データベース２２Ａに格納される。
【００４０】
人物位置－認証情報対応付け部２８は、認証情報と人物位置を対応付けて利用権限としてアクセス権限を利用者に付与する手段である。この人物位置－認証情報対応付け部２８では、追跡データＩＤ、利用者ＩＤ、入室権限と、人物情報データベース２２Ａにある追跡データＩＤ、人物位置とが対応付けられる。
【００４１】
人物間距離計測部３０は、人物情報データベース２２Ａから人物の位置情報を読み出し、利用者の距離を計測する手段である。即ち、人物間距離計測部３０では、追跡データＩＤから人物間の距離を計測し、その距離が所定値以下か否か、即ち、利用者が他の利用者と所定距離内に入ったか否かを検出する。
【００４２】
利用権限変更部３２は、人物間距離計測部３０で計測された距離に応じて利用者に付与されているアクセス権限を変更する手段である。利用権限変更部３２では、追跡データＩＤに応じて利用者に対してアクセス権限の変更を行う。
【００４３】

ドア開閉指示部３４は、利用者の位置とそのアクセス権限からドア１４の開閉を指示する手段であって、その指示信号はドア装置１０のドア制御装置１８に出力される。この場合、ドア開閉指示部３４は、人物位置に応じて入室権限を付与する。ドア制御装置１８は、ドア開閉指示部３４からの指示に基づき、ドア１４の電気錠１６の開錠又は施錠を行う。

【００４４】

次に、処理装置４Ａのハードウェア構成について、図２を参照する。図２は、処理装置のハードウェア構成を示す図である。図２に示す構成は一例であって、斯かる構成に本発明が限定されるものではない。

【００４５】

この処理装置４Ａは、既述の機能を実現するためのハードウェアを備えており、図２に示すように、中央処理装置３６と、主記憶装置３８と、補助記憶装置４０とを備えたパーソナルコンピュータ等で構成され、この処理装置４Ａには、入力装置４２と、出力手段として出力装置４４と、表示装置４５とが接続されている。

【００４６】

中央処理装置３６は、制御装置４６と、演算装置４８とを備えている。中央処理装置３６は、ＣＰＵ（Central Processing Unit ）で構成され、主記憶装置３８にあるＯＳ（Operating System）やアプリケーションを実行し、ＲＡＭ（Random-Access Memory）とともに既述の認証部２４、人物位置検出・追跡部２６、人物位置－認証情報対応付け部２８、人物間距離計測部３０、利用権限変更部３２、ドア開閉指示部３４等の機能部を構成する。制御装置４６は、主記憶装置３８、補助記憶装置４０及び演算装置４８を制御し、データの書込み、その読出し及び演算等の制御を行う。演算装置４８は、認証情報の照合、人物間距離の計測演算、利用者の権限付与等の各種の演算を行う。

【００４７】

主記憶装置３８は、プログラム等の記憶手段であって、既述のＯＳやセキュリティプログラム等の各種のアプリケーションプログラムを格納する記録媒体で構成される。補助記憶装置４０は、データ記憶手段やＲＡＭ等の記録媒体で構成され、既述の認証情報データベース２０Ａ、人物情報データベース２２Ａ等、各種のデータベースを構成する。

【００４８】

入力装置４２は、各種データの入力手段であって、この入力装置４２には、認証を行うための認証装置６や、監視範囲内にいる人物位置を把握するため、一つ又は複数の撮像装置１２Ａ、１２Ｂ等が含まれる。

【００４９】

出力装置４４は、処理装置４Ａから演算出力や制御出力を受け、それに応じた動作を行う手段であって、この出力装置４４には、既述のドア装置１０等が含まれる。ドア制御装置１８は処理装置４Ａから出力される制御信号により、ドア１４の電気錠１６の開錠、施錠を制御する。

【００５０】

表示装置４５は、結果情報や告知情報の表示手段であって、例えば、ＬＣＤ（Liquid Crystal Display）やＣＲＴで構成されている。この表示装置４５は、再認証の呼びかけ等に用いられる。

【００５１】

次に、認証情報データベース２０Ａについて、図３を参照する。図３は、認証情報データテーブルを示す図である。図３に示す構成は一例であって、斯かる構成に本発明が限定されるものではない。

【００５２】

認証情報データベース２０Ａ（図１）には認証情報データテーブル５０（図３）が設定されている。この場合、監視領域として部屋Ａ、部屋Ｂ・・・役員室及び会議室が設定されている。そこで、この認証情報データテーブル５０には、図３に示すように、利用者ＩＤ５２、名前５４、登録認証情報５６、入室権限５８が設定され、利用者ＩＤ５２は、利

用者の名前５４及び登録認証情報５６として例えば、パスワードが設定され、入室権限５８は各利用者及び各部屋Ａ、部屋Ｂ・・・役員室について付与されている。図中○は、利用権限あり、×は利用権限なしを表す。例えば、利用者ＩＤが「０００００１」の「鈴木太郎」はパスワードがｘｘｘｘｘで、部屋Ａ、Ｂ及び会議室に利用権限があるが、役員室には利用権限がないという如きである。

【００５３】

次に、人物情報データベース２２Ａについて、図４を参照する。図４は、人物情報データテーブルを示す図である。図４に示す構成は一例であって、斯かる構成に本発明が限定されるものではない。

【００５４】

人物情報データベース２２Ａ（図１）には人物情報データテーブル６０（図４）が設定されている。この場合の監視領域として部屋Ａ、部屋Ｂ・・・役員室及び会議室が設定されている。そこで、この人物情報データテーブル６０には、図４に示すように、追跡データＩＤ６２、利用者ＩＤ６４、人物位置（ｘ，ｙ）６６、移動軌跡（ｘ，ｙ）６８及び現在の入室権限７０が設定されている。追跡データＩＤ６２は、追跡データの識別情報であり、利用者ＩＤ毎に設定されている。人物位置６６は、監視領域に設定されたｘ，ｙ座標の位置情報を表している。移動軌跡６８は、所定の時間毎の利用者の移動軌跡を表す情報であって、人物位置（ｘ，ｙ）６６と同様に、監視領域に設定されたｘ，ｙ座標の位置情報から移動軌跡を表している。また、その移動軌跡は、時間毎の位置の変化を表していることから、この実施の形態では、移動軌跡６８には、１時刻前位置欄７２１、２時刻前位置欄７２２・・Ｎ時刻前位置欄７２Ｎが設定されている。また、現在の入室権限７０は、監視領域毎即ち、既述の部屋Ａ、部屋Ｂ・・・役員室及び会議室毎に設定されている。

【００５５】

この人物情報データテーブル６０によれば、例えば、追跡データＩＤ「００１」、利用者ＩＤ「０００００１」の人物位置は移動軌跡の座標位置に移動し、現在の入室権限は、部屋Ａ、Ｂ及び会議室に利用権限があるが、役員室には利用権限がないという如きである。

【００５６】

次に、利用者の状態管理及び状態管理処理について、図５及び図６を参照する。図５は、第１の実施の形態に係る利用者の状態管理処理の処理手順を示すフローチャート、図６は、ドアの開閉制御処理の処理手順を示すフローチャートである。図５及び図６に示す構成は一例であって、斯かる構成に本発明が限定されるものではない。

【００５７】

このセキュリティシステム２Ａ（図１）では、利用者の状態管理をする処理と、ドアの開閉制御を行う処理の双方を並行して行っている。これらの処理手順は、セキュリティ方法及びセキュリティプログラムの一例であって、利用者の状態管理とともにドアの施錠、開錠の制御を行う処理を含んでいる。

【００５８】

利用者の状態管理処理の処理手順では、図５に示すように、人物の位置を検出し（ステップＳ１０１）、人物が認証されたか否かを判定し（ステップＳ１０２）、人物の位置と認証情報の対応付けを行い（ステップＳ１０３）、人物間の距離の計測を行い（ステップＳ１０４）、人物の距離が近いか否かを判定し（ステップＳ１０５）、人物の距離が近い場合には近い人物のアクセス権限の変更を行い（ステップＳ１０６）、ステップＳ１０１に戻る。また、人物の距離が近くない場合にはステップＳ１０１に戻り、人物を監視し、ステップＳ１０２～Ｓ１０６の処理を実行する。

【００５９】

ステップＳ１０１では、撮像装置１２Ａ、１２Ｂ（図１）から得られた画像を基に人物位置検出・追跡部２６で常に監視範囲にいる人物の位置を把握する。この実施の形態では、各部屋や廊下等、全ての場所に、それぞれ撮像装置１２Ａ、１２Ｂを設置し、人物がどの場所にいても連続して追跡が行われる。人物の追跡方法は例えば、複数の撮像装置１２

Ａ、１２Ｂを用いて人物の位置を認識し、逆投影法とカルマンフィルタを用いればよい（例えば、文献１：早坂光晴，富永英義，小宮一三:"逆投影法とカルマンフィルタを用いた複数移動物体位置認識とその追跡",PRMU2001-132,pp.133-138,Nov,2001.）。また、レーザ光を使う方法としてはマルチレーザスキャナを用いて人物の足を計測してもよい（例えば、文献２：中村克行,"マルチレーザスキャナを用いた歩行者トラッキング,"電子情報通信学会論文誌 D-II，vol.J88-D-II，no.7，pp.1143-1152，Jul,2005.）。文献２に開示されているように、得られた追跡データＩＤ毎に人物位置を随時に人物情報データベース２２Ａに保存する。初めて検出された人物については、誰であるか分からないため利用者ＩＤはなし、入室権限も全てなしとして初期化を行えばよい。

【００６０】

ステップＳ１０２では、利用者が部屋へ入室する際、認証装置６によって認証を実行する。具体的には、ディスプレイ上に利用者認証用のダイアログを表示し、ユーザとパスワードを用いて認証する方法や、静脈や指紋を用いた認証装置を利用した認証方法により、認証部２４では、認証装置６から入力された入力認証情報と、認証情報データベース２０Ａにある登録情報との照合を行い、個人を特定する。認証情報データベース２０Ａに予め登録されていない等、認証されない場合はステップＳ１０４に遷移する。

【００６１】

ステップＳ１０３では、認証が行われた際（ステップＳ１０２）、人物情報データベース２２Ａに格納されている人物位置と認証が行われた場所との位置関係から、人物認証情報と人物との対応付けを行う。具体的には、認証装置６の位置とその認証装置６が持つ認証装置ＩＤを予め対応付けておき、認証が行われた認証装置６の場所に最も近い位置にいる追跡データＩＤの利用者に認証で判定された利用者ＩＤを登録する。また、同時に、利用者に合わせた入室権限も分かるので、その入室権限に基づき、人物情報データベース２２Ａにある入室権限も更新する。

【００６２】

ステップＳ１０４では、各人物の位置を用いてそれぞれの位置関係を求める。人物間の距離が所定距離以下にある状態を検出すれば（ステップＳ１０５）、ステップＳ１０６に遷移する。

【００６３】

ステップＳ１０６では、人物間距離が一定距離以内にいる各利用者の入室権限を人物情報データベース２２Ａから読み出す。そして、その読み出した入室権限を利用して、各利用者の入室権限を変更する。具体的には、それぞれの利用者の現在持っている入室権限の論理積を取って、その入室権限を各利用者の入室権限とする。

【００６４】

そして、ステップＳ１０５又はステップＳ１０６を経てステップＳ１０１に戻り、既述の処理を繰り返す。

【００６５】

また、ドアの開閉制御処理の処理手順では、図６に示すように、人物情報データベース２２Ａから情報の読込みを行い（ステップＳ１１１）、ドアの前に人がいるか否かを判定し（ステップＳ１１２）、ドアの前に人がいれば、その人が入室権限を持っているか否かを判定し（ステップＳ１１３）、入室権限を持っていれば、ドア開錠とする（ステップＳ１１４）。

【００６６】

この場合、ステップＳ１１１では人物情報データベース２２Ａにアクセスし、人物位置、利用者ＩＤ、入室権限等を読み出し、ステップＳ１１２では各ドア周辺に人物がいるか否かを人物位置を用いて確認する。ドア周辺に人物がいる場合にはステップＳ１１３に遷移し、ステップＳ１１３ではドア周辺にいる人物がそのドアの入室権限を持っている場合、ドアを開錠する。そして、ドア開錠の後、既述の処理を繰り返す。

【００６７】

次に、第１の実施の形態に係るセキュリティシステム２Ａの具体的な実施例について、

図７、図８、図９、図１０、図１１、図１２、図１３、図１４及び図１５を参照する。図７は、セキュリティシステムの実施例を示す図、図８は、利用者の権限例を示す図、図９は、利用者の移動経路の一例を示す図、図１０は、利用者の入室権限の変化例を示す図、図１１は、権限レベル－入室可能部屋変換テーブルを示す図、図１２は、権限レベルを利用した認証情報データテーブルを示す図、図１３は、権限レベルを利用した人物情報データテーブルを示す図、図１４は、権限レベルを利用した利用者権限例を示す図、図１５は、権限レベルを利用した権限変化例を示す図である。図７～図１５は一例であって、斯かる構成に本発明が限定されるものではない。図７、図９において、図１と同一部分には同一符号を付してある。

【００６８】

この実施例では、既述のセキュリティシステム２Ａが、複数の利用者が利用する複数の部屋等の環境に使用された場合であって、利用者の距離に応じて変化する入室権限の変化例を示している。

【００６９】

セキュリティシステム２Ａが設置される環境として建造物９０には、図７に示すように、監視領域として、部屋Ａ、部屋Ｂ、部屋Ｃ及び部屋Ｄが設置されているとともに、各部屋の出入りが可能な通路として廊下９２が設置されている。部屋Ａの入口部にはドア１４Ａ及び認証装置６Ａ、部屋Ｂの入口部にはドア１４Ｂ及び認証装置６Ｂ、部屋Ｃの入口部にはドア１４Ｃ及び認証装置６Ｃ、部屋Ｄの入口部にはドア１４Ｄ及び認証装置６Ｄが設置されている。各ドア１４Ａ、１４Ｂ、１４Ｃ、１４Ｄを開錠するには、利用者は入室しようとする部屋の認証装置６Ａ、６Ｂ、６Ｃ、６Ｄでの認証を行い、入室権限を獲得することが必要となる。この場合、ドア１４Ａを開錠する際に認証を行った場合は、ドア１４Ｂで再度認証を行わなくても開錠できるシステムである。

【００７０】

そこで、利用者１、利用者２、利用者３、利用者４を想定すれば、これら利用者は、各部屋Ａ、Ｂ、Ｃ、Ｄの利用権限（図８）を持っていると仮定する。この場合、利用者の利用権限は、図８に示すように、利用者１は部屋Ａ、部屋Ｂ、部屋Ｄの入室権限を持っており、利用者２は部屋Ｂ、部屋Ｃ、部屋Ｄの入室権限、利用者３は部屋Ａ、部屋Ｂの入室権限、利用者４は部屋Ｄの入室権限のみを有する。

【００７１】

これら利用者１、利用者２、利用者３及び利用者４が図９に示すように、移動したとする。図９において、利用者１は、移動経路９６、９８、１００、１０２、１０４により移動している。

【００７２】

利用者１の移動と利用権限は図１０に示すように変化する。即ち、利用者１が廊下９２に入ってきた時点では認証を行っていないので、利用者が誰であるか分からない。即ち、人物情報データベース２２Ａには新しい人物の到来（発見）により追跡データＩＤと現在位置が新しく加えられるが、それに対応する利用者ＩＤは「なし」、入室権限も「全てなし」となる（図１０のｆ１１）。ここでは、簡単にするために、利用者２、利用者３、利用者４については既に認証が行われているものとする。

【００７３】

利用者１が認証を行い、利用者１であると判断された時点で、人物情報データベース２２Ａには利用者ＩＤを「利用者１」に設定し、利用者１の持つ入室権限である部屋Ａ、部屋Ｂ、部屋Ｄの入室権限あり、即ち、入室権限が「○」とされ、この人物に部屋Ａ、部屋Ｂ、部屋Ｄの入室権限が与えられる（図１０のｆ１２）。

【００７４】

利用者１は、部屋Ａでの作業後、部屋Ａから廊下９２に出て部屋Ｂへの移動途中に利用者２と接近すると、利用者２を利用者１として認識する可能性がある。そこで、利用者１は接近した人物（利用者２）が持っていない部屋Ａの入室権限を失い、即ち、利用権限の変更が行われ、また、利用者２は接近した人物（利用者１）が持っていない部屋Ｃの入室

権限を失う。即ち、利用者２についても利用権限の変更が行われる。つまり、両者共に両者の入室権限の論理積を取った部屋Ｂ、部屋Ｄのみの入室権限に変更される（図１０のｆ１３）。この場合、人物情報データベース２２Ａでは、利用者１の部屋Ａの利用権限と利用者２の部屋Ｃの利用権限を「×」と書き換える。利用者２は部屋Ｂの入室権限は持っているため、認証せずに部屋Ｂに入ることができる。その後、利用者３と接近した場合も同様に、現在それぞれの利用者が持っている入室権限を比較し、利用者１は利用者３が入室できない部屋Ｄの入室権限を失い、また、利用者３は利用者１が入室できない部屋Ａの利用権限を失う。人物情報データベース２２Ａには、前回と同様に利用者１の部屋Ｄの入室権限と利用者３の部屋Ａの入室権限が「×」とされる（図１０のｆ１４）。入室権限を失った場合でも、再度の認証（再認証）を行い、誰であるか確認された時点で、元来利用者１が与えられていた入室権限が再度与えられる（図１０のｆ１５）。また、部屋の中でも同様であり、利用者１が、部屋の中で利用者４と接近した場合も、両者の論理積を取った部屋Ｄの入室権限のみしか持たなくなる（図１０のｆ１６）。

【００７５】

次に、部屋毎に入室権限の有無を決めずに、権限レベルと部屋への入室権限の関係を予め定めた権限レベル－入室可能部屋変換テーブル１０８（図１１）を利用すれば、利用権限レベルを各利用者に設定しても同様である。この権限レベル－入室可能部屋変換テーブル１０８には、図１１に示すように、権限レベル１１０に対して各部屋の入室権限１１２が設定され、権限レベル１１０には５段階の権限レベル「０」～「４」が設定され、権限レベル「０」では部屋Ａ～部屋Ｄの全ての入室権限がなく、権限レベル「１」では部屋Ｄのみの入室権限があり、権限レベル「２」では部屋Ｃ及び部屋Ｄの入室権限があり、権限レベル「３」では部屋Ｂ、部屋Ｃ及び部屋Ｄの入室権限があり、権限レベル「４」では部屋Ａ、部屋Ｂ、部屋Ｃ及び部屋Ｄの全ての入室権限がある。

【００７６】

この場合、認証情報データテーブル１１４（図１２）及び人物情報データテーブル１１６（図１３）を用いる。この認証情報データテーブル１１４は、図１２に示すように、利用者の認証情報を管理する利用者ＩＤ１１８、登録してある人物の名前１２０、認証情報と比較して本人か否かを判断する登録認証情報１２２、その人が持つ入室権限レベル１２４等の情報が登録される。人物情報データテーブル１１６は、図１３に示すように、それぞれの人物毎に、追跡データを管理する追跡データＩＤ１２６、追跡データが誰であるかを示す利用者ＩＤ１２８、人物位置１３０、移動軌跡１３２、現在の入室権限レベル１３４等が登録される。

【００７７】

そこで、このような権限レベルを、既述の環境（図９）で使用した場合の入室権限の変化例を説明する。各利用者は例えば、図１４に示すように、異なる権限レベルを持っていることを想定する。

【００７８】

利用者１の移動と利用権限は図１５に示すように変化する。即ち、利用者１が廊下９２に入ってきた時点では認証を行っていないため、誰であるか分からない。よって、人物情報データベース２２Ａには新しい人物の到来（発見）により追跡データＩＤと現在位置が新しく加えられるが、それに対応する利用者ＩＤは「なし」、入室権限レベルも「０」となる（ｆ２１）。ここでは、簡単にするために、利用者２、３、４については既に認証が行われているものとする。

【００７９】

図１５に示すように、利用者１が認証を行い利用者１であると判断された時点で、人物情報データベース２２Ａには利用者ＩＤを「利用者１」に設定し、利用者１の持つ入室権限レベル「４」が与えられる（ｆ２２）。部屋Ａに入室可能かどうかは、権限レベル－入室可能部屋変換テーブル１０８（図１１）を参照して判断する。

【００８０】

利用者１が部屋Ａでの作業後、部屋Ｂへの移動途中で利用者２と接近すると、利用者２を利用者１として認識する可能性があるため、利用者１と利用者２は両者のうち低い方のレベルに設定される（ｆ２３）。利用者２の方が低いレベルのため、人物情報データベース２２Ａの利用者１の入室権限レベルが「３」に書き換えられる。しかし、利用者１は入室権限レベル「３」であり、部屋Ｂの入室権限は持っているため、認証せずに部屋Ｂには入れる。その後、利用者３と接近した場合も同様に、現在それぞれの利用者が持っている入室権限を比較し、低い方のレベルに設定される。この場合、人物情報データベース２２Ａには、前回と同様に利用者１の入室権限レベルが「１」とされる（ｆ２４）。入室権限を失った場合でも、再度認証を行い、誰であるか確認された時点で、もともと利用者１が与えられていた入室権限を再度与えられるため、この場合は再度、入室権限レベル「４」を得ることができる（ｆ２５）。また、部屋の中でも同様であり、利用者１が、部屋の中で利用者４と接近した場合も、両者の低い方のレベルに設定される（ｆ２６）。

【００８１】

第１の実施の形態によれば、利用者が認証した後であっても、自分より権限の低い人物と接近し、どちらが権限を持った人であるかが判別できない場合には利用権限を低下させるので、セキュリティシステム２Ａが誤って利用権限がない他人の入室を許可することがなく、セキュリティの低下を防止することができる。その他、第１の実施の形態の特徴事項や利点を以下に列挙する。

【００８２】

(1) アクセス権限を持たない者に対して、誤ってサービスを提供することを防止でき、アクセス権限のコントロールが可能である。

【００８３】

(2) 利用者に利用権限を付加して毎回認証をせずにサービスを受けられるシステムを構成でき、利用者間の距離に応じて利用者の利用権限を変化させることで、利用権限がない人がサービスを受ける不正利用を防止できる。

【００８４】

(3) 利用者の追跡に基づき、人物の位置と利用権限を対応付けることで、一度認証したら毎回認証を行わなくてもサービスを受けられるシステムを構成でき、利用権限を持たない人がサービスを受ける不正利用を防止できる。

【００８５】

(4) 人物の位置を検出、追跡するシステム、人物を認証するシステムを備え、認証行為によってサービスを受けるための権限（利用権限）が与えられるシステムを構成でき、人物間の距離が所定値以下になった場合に、両者の利用権限の状態に応じて、それぞれの人物の利用権限を変更することができる。

【００８６】

(5) 人物の利用権限を段階的に設定し、人物間の距離が所定値以下になった場合に、それぞれの利用権限を低いレベルの人に合わせる機能により、認証の繰り返しを求めることなく、セキュリティレベルを維持することができる。

【００８７】

(6) 認証した利用者を追跡する利用者追跡手段を備え、利用権限制御手段は、利用者追跡手段の追跡に基づき、利用者の利用権限又は変更された利用権限を維持する構成としたので、繰り返しの認証を求めることなく、利便性を高めることができる。

【００８８】

(7) 人物の利用権限をサービス毎に設定し、人物間の距離が所定値以下になった場合に、それぞれの人物の利用権限を、サービス毎に論理積を取った利用権限に変更する機能を備えているので、サービス毎にセキュリティレベルを設定することができ、利便性を高めることができる。

【００８９】

(8) 人物間の距離が所定値以下になった場合に、それぞれの人物の利用権限をなくす機能を備えれば、セキュリティレベルを高度に維持することができる。

【００９０】
(9) 利用権限が変更された場合に、再度認証システムで認証を行うことで、その人が持っていた利用権限に復帰させることができ、セキュリティレベルを維持しながら、利便性が高められる。
【００９１】
(10) 現在利用者が持っている利用権限を表示装置４５に表示すれば、利用者は自己の利用権限を確認でき、また、施設管理者もその利用権限と利用者との関係を表示情報を通じて容易に知ることができる。
【００９２】
(11) 人物の位置を検出、人物を認証するシステム、認証行為によって利用権限が与えられるシステムでは、認証が行われたときに認証を行った人物とその周辺の人物との距離が所定値以内である状態を検出した場合、認証した人に利用権限を与えない構成とすることもでき、斯かる構成では、セキュリティレベルをより高くすることができる。
【００９３】
(12) 認証時に認証を行った人物とその周辺の人物との距離が所定値以内である状態を検出した際に、利用権限が与えられない構成とすれば、他人受入れによるセキュリティレベルの低下を未然に防止できる。
【００９４】
〔第２の実施の形態〕
【００９５】
第２の実施の形態について、図１６を参照する。図１６は、第２の実施の形態に係るセキュリティシステムを示す図である。図１６に示す構成は一例であって、斯かる構成に本発明が限定されるものではない。図１６において、図１と同一部分には同一符号を付してある。
【００９６】
このセキュリティシステム２Ｂ（図１６）は、第１の実施の形態のセキュリティシステム２Ａにパーソナルコンピュータ（ＰＣ）へのログイン制御を付加したシステムを構成している。
【００９７】
このセキュリティシステム２Ｂでは、図１６に示すように、処理装置４Ｂと、認証装置６と、人物位置検出装置８と、ドア装置１０と、ＰＣ１４０とを備えている。処理装置４Ｂは、認証及び人物の検出及び追跡に基づく利用権限を制御する制御手段であって、具体的には、認証装置６による認証と、人物位置検出装置８による人物位置の検出及び追跡と、これら認証及び人物の追跡に基づくドア装置１０の施錠又は開錠、ＰＣ１４０へのログイン制御等を行う。認証装置６、人物位置検出装置８、ドア装置１０は第１の実施の形態と同様であるので、同一符号を付し、その説明を省略する。
【００９８】
処理装置４Ｂは、認証及び人物の検出、追跡に基づく利用権限及びＰＣ１４０の画面制御等を行う制御手段として、認証情報データベース２０Ｂと、人物情報データベース２２Ｂと、認証部２４と、人物位置検出・追跡部２６と、人物位置－認証情報対応付け部２８と、人物間距離計測部３０と、利用権限変更部３２と、ドア開閉指示部３４と、ＰＣ画面制御部１４２とを備えている。
【００９９】
認証情報データベース２０Ｂは、第１の実施の形態と同様に、利用者の認証情報を管理する利用者１Ｄ、登録してある人物の名前、認証情報と比較して本人かを判断する登録認証情報、その人が入室できるドアを示す入室権限等、利用者認証処理を行うための情報が登録されたデータベースである。この認証情報データベース２０Ｂには、認証用ＩＤ、名前、登録認証情報、入室権限等を表す情報が格納されている。
【０１００】
人物情報データベース２２Ｂは、それぞれの人物毎に、追跡データを管理する追跡デー

タＩＤ、追跡データが誰であるかを示す利用者ＩＤ、現在開錠可能なドアを示す入室権限、ＰＣ利用権限等の情報を格納するデータベースである。

【０１０１】

認証部２４は、認証装置６に入力される生体情報等の入力認証情報と、認証情報データベース２０Ｂにある登録認証情報とに基づいて利用者の認証を行う認証手段である。認証部２４は、認証装置６から入力された利用者ＩＤ、認証情報、認証装置ＩＤ等の入力認証情報と、認証情報データベース２０Ｂにある利用者ＩＤ、認証情報、入室権限等の登録情報とを照合し、その認証結果として利用者ＩＤ、認証情報、入室権限、ＰＣ利用権限等を出力し、人物位置－認証情報対応付け部２８に提供する。

【０１０２】

人物位置検出・追跡部２６は、第１の実施の形態と同様に、利用者の位置及び／又はその移動を検出する位置検出手段の一例であって、撮像装置１２Ａ、１２Ｂで取得された画像から人物の検出、その位置の検出及び又はその移動を追跡する人物位置検出及び／又は追跡を行い、追跡データＩＤ、人物位置等の人物情報（利用者情報）を生成する。この人物情報は、人物情報データベース２２Ｂに格納される。

【０１０３】

人物位置－認証情報対応付け部２８は、第１の実施の形態と同様に、認証情報と人物位置を対応付けて利用権限としてアクセス権限を利用者に付与する手段である。この人物位置－認証情報対応付け部２８では追跡データＩＤ、人物ＩＤ、入室権限、ＰＣ利用権限と、人物情報データベース２２Ｂにある追跡データＩＤ、人物位置とが対応付けられる。

【０１０４】

人物間距離計測部３０、利用権限変更部３２及びドア開閉指示部３４は第１の実施の形態と同様である。

【０１０５】

また、ＰＣ画面制御１４２は、人物情報データベース２２Ｂから人物位置に応じ、利用者に設定されたＰＣ利用権限に関する情報が付与され、それに基づく制御信号を出力する。この制御信号は、ＰＣ１４０に対するログインの許可又は禁止の制御信号である。

【０１０６】

処理装置４Ｂのハードウェア構成は、図２に示すハードウェア構成と同様であって、中央処理装置３６やＲＡＭによるセキュリティプログラムの実行によりＰＣ画面制御部１４２が構成される以外は、処理装置４Ａと同様である。処理装置４Ｂには、認証を行うための認証装置６、監視範囲内にいる人物位置を把握するため一つ又は複数の撮像装置１２Ａ、１２Ｂ、制御信号によってドアの開錠・施錠を制御するドア制御装置１８、制御信号によってログイン状態を変更することができるＰＣ１４０が接続されている。なお、この撮像装置１２Ａ、１２Ｂは、例えばレーザセンサやＲＦＩＤリーダ等、人物の位置を知ることができるもので代用可能である。

【０１０７】

そして、この実施の形態においても、撮像装置１２Ａ、１２Ｂによって得られた画像から人物を検出して追跡を行う人物位置検出・追跡部２６、認証情報データベース２０Ｂに基づいて認証を行う認証部２４、認証情報と人物位置を対応付けてアクセス権限を付与する人物位置－認証情報対応付け部２８、人物情報データベース２２Ｂから人物の位置を読み出してそれぞれの人物の距離を計測する人物間距離計測部３０、その距離に応じて各人の利用権限を変更する利用権限変更部３２、人の位置とそのアクセス権限からドアの開閉を指示するドア開閉指示部３４、人の位置とそのアクセス権限からＰＣ画面の起動を行うＰＣ画面制御部１４２により、入室権限やＰＣ１４０のログインの制御が実行される。

【０１０８】

次に、認証情報データベース２０Ｂについて、図１７を参照する。図１７は、認証情報データテーブルを示す図である。図１７に示す構成は一例であって、斯かる構成に本発明が限定されるものではない。

【０１０９】

認証情報データベース２０Ｂ（図１６）は、利用者の認証情報を管理する利用者ＩＤ、登録してある人物の名前、認証情報と比較して本人かを判断する登録認証情報、その人が入室できるドアを示す入室権限、ログイン可能なＰＣ利用権限等、利用者認証処理を行うためのデータベースであり、この認証情報データベース２０Ｂには認証情報データテーブル１４４（図１７）が設定されている。この場合、監視領域として部屋Ａ、部屋Ｂ・・・役員室及び会議室が設定されている。

【０１１０】

この認証情報データテーブル１４４には、図１７に示すように、利用者ＩＤ１４６、名前１４８、登録認証情報１５０、ＰＣの利用権限１５２、入室権限１５４が設定され、利用者ＩＤ１４６は、利用者の名前１４８及び登録認証情報１５０として例えば、パスワードが設定され、ＰＣの利用権限１５２及び入室権限１５４は各利用者及び各部屋Ａ、部屋Ｂ・・・役員室について付与されている。この場合、ＰＣ１４０として複数のＰＣα、ＰＣβ・・・ＰＣζが設定されている。図中○は、利用権限あり、×は利用権限なしを表す。例えば、利用者ＩＤが「０００００１」の「鈴木太郎」はパスワードがｘｘｘｘｘで、ＰＣα、ＰＣβ、部屋Ａ、Ｂ及び会議室には利用権限があるが、ＰＣζ、役員室には利用権限がないという如きである。

【０１１１】

また、人物情報データベース２２Ｂ（図１６）は、それぞれの人物毎に、追跡データを管理する追跡データＩＤ、追跡データが誰であるかを示す利用者ＩＤ、現在開錠可能なドアを示す入室権限、現在ログイン可能なＰＣの利用権限、人物の現在位置、移動軌跡等、人物の現在の状況を表すデータベースである。この人物情報データベース２２Ｂ（図１６）には人物情報データテーブル１５６（図１８）が設定されている。

【０１１２】

この人物情報データテーブル１５６には、図１８に示すように、追跡データＩＤ１５８、利用者ＩＤ１６０、人物位置（ｘ，ｙ）１６２、移動軌跡（ｘ，ｙ）１６４、現在のＰＣの利用権限１６６、現在の入室権限１６８が設定されている。追跡データＩＤ１５８は、追跡データの識別情報であり、利用者ＩＤ毎に設定されている。人物位置１６２は、監視領域に設定されたｘ、ｙ座標の位置情報を表している。移動軌跡１６４は、所定の時間毎の利用者の移動軌跡を表す情報であって、人物位置１６２と同様に、監視領域に設定されたｘ、ｙ座標の位置情報から移動軌跡を表している。また、その移動軌跡は、時間毎の位置の変化を表していることから、移動軌跡１６４には、１時刻前位置欄、２時刻前位置欄・・・Ｎ時刻前位置欄が設定されている。現在のＰＣの利用権限１６６は、ログイン可能な利用権限が設定され、また、現在の入室権限１６８は、監視領域毎即ち、既述の部屋Ａ、部屋Ｂ・・・役員室及び会議室毎に設定されている。

【０１１３】

この人物情報データテーブル１５６によれば、例えば、追跡データＩＤ「００１」、利用者ＩＤ「０００００１」の人物位置は移動軌跡（ｘ，ｙ）の座標位置に移動し、現在のＰＣの利用権限はＰＣαに設定され、また、現在の入室権限は、部屋Ａ、Ｂ及び会議室に利用権限があるが、役員室には利用権限がないという如きである。

【０１１４】

次に、利用者の状態管理処理、ドアの開閉・ＰＣログイン制御処理について、図１９及び図２０を参照する。図１９は、第２の実施の形態に係る利用者の状態管理処理の処理手順を示すフローチャート、図２０は、ドアの開閉制御処理及びＰＣログイン制御処理の処理手順を示すフローチャートである。図１９及び図２０に示す構成は一例であって、斯かる構成に本発明が限定されるものではない。

【０１１５】

このセキュリティシステム２Ｂ（図１６）では、利用者の状態管理の処理と、ドア制御の処理、ＰＣの利用権限の処理を行っている。これらの処理手順は、セキュリティ方法及びセキュリティプログラムの一例であって、利用者の状態管理、ドアの施錠、開錠の管理及びＰＣのログイン制御の処理を含んでいる。

【０１１６】
利用者の状態管理処理の処理手順では、図１９に示すように、人物の位置を検出し（ステップＳ２０１）、人物が認証されたか否かを判定し（ステップＳ２０２）、認証された場合には、人物の位置と認証情報の対応付けを行い（ステップＳ２０３）、人物間の距離の計測を行い（ステップＳ２０４）、人物の距離が近いか否かを判定し（ステップＳ２０５）、人物の距離が近い場合には近い人物のアクセス権限の変更を行い（ステップＳ２０６）、ステップＳ２０１に戻る。また、人物の距離が近くない場合にはステップＳ２０１に戻り、人物を監視し、ステップＳ２０２～Ｓ２０６の処理を実行する。
【０１１７】
この状態管理処理の処理手順において、ステップＳ２０１では、撮像装置１２Ａ、１２Ｂから得られた画像を基に人物位置検出・追跡部２６では常に監視範囲にいる人物の位置を把握する。この実施の形態では、各部屋や廊下等の監視範囲の全ての場所に、それぞれ撮像装置１２Ａ、１２Ｂ等が置かれており、人物がどの場所にいても連続して追跡が行われる。人物の追跡方法は例えば、複数のカメラを用いて人物の位置を認識する方法としては逆投影法とカルマンフィルタを用いる方法がある（例えば、文献１：早坂光晴，富永英義，小宮一三:"逆投影法とカルマンフィルタを用いた複数移動物体位置認識とその追跡", PRMU2001-132,pp.133-138,Nov,2001．）。また、レーザ光を使う方法としてはマルチレーザスキャナを用いて人物の足を計測するものがある（例えば、文献２：中村克行,"マルチレーザスキャナを用いた歩行者トラッキング,"電子情報通信学会論文誌 D-II，vol.J88-D-II，no.7，pp.1143-1152，Jul,2005.）。
【０１１８】
得られた追跡データＩＤ毎に、人物位置は人物情報データベース２２Ｂに随時保存される。初めて検出された人物については誰であるか分からないため利用者ＩＤはなし、入室権限も全てなしとして初期化を行う。
【０１１９】
また、ステップＳ２０２では、利用者が部屋へ入室する際、又はＰＣ１４０にログインする際に認証を行う。具体的には、ＰＣ１４０のディスプレイ１４３上に利用者認証用のダイアログを表示し、ユーザとパスワードを用いて認証する方法や、静脈や指紋を用いた認証装置を利用した認証方法によって認証情報データベース２０Ｂとの照合を行い、個人を特定する。予め、認証情報データベース２０Ｂに登録されていない等、認証されない場合にはステップＳ２０４に遷移する。
【０１２０】
ステップＳ２０３では、ステップＳ２０２の認証が行われた際には、人物情報データベース２２Ｂに格納されている人物位置と認証が行われた場所との位置関係から、人物認証情報と人物との対応付けを行う。具体的には、認証装置位置と認証装置ＩＤを予め対応付けておき、認証が行われた認証装置の場所に最も近い位置にいる追跡データＩＤの利用者に認証で判定された利用者ＩＤを登録する。また、同時に、利用者に合わせた入室権限とＰＣ１４０の利用権限も分かるため、人物情報データベース２２Ｂの利用権限も更新する。
【０１２１】
ステップＳ２０４では各人物の位置を用いてそれぞれの位置関係を求める。仮に、人物間の距離が所定距離以下にある状態を検出したら（ステップＳ２０５のＹＥＳ）、ステップＳ２０６に遷移する。
【０１２２】
ステップＳ２０６では、人物間距離が一定距離以内にいる各利用者の入室権限、ＰＣ１４０の利用権限を人物情報データベース２２Ｂから読み出す。そして、その読み出した入室権限、ＰＣ１４０の利用権限を利用して、各利用者のそれぞれの利用権限を変更する。具体的には、それぞれの利用者の現在持っている利用権限の論理積を取って、その利用権限を各利用者の利用権限とする。
【０１２３】

そして、ステップＳ２０５又はステップＳ２０６を経てステップＳ２０１に戻り、既述の処理を繰り返す。

【０１２４】

また、ドアの開閉制御処理及びＰＣログイン制御処理の処理手順では、図２０に示すように、人物情報データベース２２Ｂにアクセスし、人物位置、利用者ＩＤ、入室権限、ＰＣ利用権限等を読み出し（ステップＳ２１１）、各ドア周辺に人物がいるか否かを人物位置を用いて確認する（ステップＳ２１２）。ドア周辺に人物がいる場合には（ステップＳ２１２のＹＥＳ）、ドア周辺にいる人物がそのドアの入室権限を持っているか否かを判断し（ステップＳ２１３）、入室権限を持っている場合には（ステップＳ２１３のＹＥＳ）、ドアを開錠し（ステップＳ２１４）、ステップＳ２１５に移行する。ドア周辺に人物がいない場合（ステップＳ２１２のＮＯ）、入室権限を持っていない場合（ステップＳ２１３のＮＯ）にも、ステップＳ２１５に移行する。

【０１２５】

ステップＳ２１５では、ＰＣ周辺に人物がいるか否かを人物位置を用いて確認し、ＰＣ周辺に人物がいる場合は（ステップＳ２１５のＹＥＳ）、ドア周辺にいる人物がそのＰＣ利用権限を持っているか否かを判断し（ステップＳ２１６）、ドア周辺にいる人物がそのＰＣ利用権限を持っている場合には（ステップＳ２１６のＹＥＳ）、ＰＣ画面をログイン状態に変更し（ステップＳ２１７）、ログインを自動で行う。また、ドア周辺にいる人物がそのＰＣ利用権限を持っていない場合には（ステップＳ２１６のＮＯ）、ＰＣ画面を認証待ち状態に変更する（ステップＳ２１８）。

【０１２６】

そして、ステップＳ２１７又はステップＳ２１８の処理の後、ステップＳ２０１に戻り、既述の処理を繰り返す。

【０１２７】

次に、第２の実施の形態に係るセキュリティシステム２Ｂの具体的な実施例について、図２１、図２２、図２３、図２４、図２５、図２６及び図２７を参照する。図２１は、セキュリティシステムの実施例を示す図、図２２は、利用者の権限例を示す図、図２３は利用者の移動経路の一例を示す図、図２４は、利用者の権限の変化例を示す図、図２５は、権限レベル－利用可能情報変換テーブルを示す図、図２６は、権限レベルを利用した利用者権限例を示す図、図２７は、権限レベルを利用した権限変化例を示す図である。図２１～図２７は一例であって、斯かる構成に本発明が限定されるものではない。図２１、図２３において、図１６と同一部分には同一符号を付してある。

【０１２８】

この実施例では、既述のセキュリティシステム２Ｂが複数の利用者が利用する複数の部屋等の環境に使用された場合であって、利用者の距離に応じて変化する入室権限、ＰＣ利用権限の変化例を示している。

【０１２９】

セキュリティシステム２Ｂが設置される環境として建造物９０には、図２１に示すように、監視領域として、部屋Ａ、部屋Ｂが設置されているとともに、各部屋の出入りが可能な通路として廊下９２が設置され、部屋Ａには複数のＰＣとしてＰＣα、ＰＣβ、ＰＣγが設置されている。部屋Ａの入口部にはドア１４Ａ及び認証装置６Ａ、部屋Ｂの入口部にはドア１４Ｂ及び認証装置６Ｂが設置されている。この場合、ドアＡを開錠するためにはその認証装置での認証が必要となる。また、ＰＣα、ＰＣβ、ＰＣγはログインするために認証を必要とするシステムである。

【０１３０】

この場合、利用者１、利用者２（図２３）を想定し、それぞれは異なる入室権限やＰＣ利用権限（図２２）を有する。入室権限及びＰＣ利用権限について、図２２に示すように、利用者１は部屋Ａ、Ｂの入室権限とＰＣα、ＰＣβの利用権限を持っており、利用者２は部屋Ａの入室権限とＰＣα、ＰＣγの利用権限を持っている。

【０１３１】

この場合、利用者１は、図２３に示すように、移動経路２１４、２１６で移動し、利用者２は部屋Ａにいる。利用者１の移動に伴う権限の変化は図２４に示すように変化する。利用者１が廊下９２に入ってきた時点では認証を行っていないため、誰であるか分からない。よって、人物情報データベース２２Ｂには新しい人物の発見により追跡データＩＤと現在位置が新しく加えられるが、それに対応する利用者ＩＤは「なし」、入室権限も全て「×」、ＰＣ利用権限も全て「×」となる（ｆ３１）。利用者１が認証を行い、利用者１であると判断された時点で、人物情報データベース２２Ｂには利用者ＩＤを「利用者１」に設定し、利用者１の持つ入室権限として部屋Ａ、部屋Ｂの入室権限が「○」、ＰＣ利用権限としてＰＣα、ＰＣβの利用権限が「○」と書き換えられ、部屋Ａ、部屋Ｂの入室権限とＰＣα、ＰＣβの利用権限が与えられる（ｆ３２）。一度認証するだけで、ＰＣ利用権限も得られるため、再認証をせずにＰＣの利用が可能である。しかし、部屋Ａへの入室後、利用者２と接近すると、利用者２と利用者１を誤認識する可能性があるため、利用者１は接近した人物（利用者２）が持っていないＰＣ利用権限及び入室権限を失い、また、利用者２は接近した人物（利用者１）が持っていないＰＣ利用権限及び入室権限を失う。つまり、今回の場合では、両者共に両者の権限の論理積を取ったＰＣαの利用権限及び部屋Ａの入室権限しか持たなくなる（ｆ３３）。このとき、人物情報データベース２２Ｂでは、利用者１のＰＣβの利用権限、部屋Ｂの入室権限、利用者２のＰＣγの利用権限を「×」と書き換える。利用者１は再度ＰＣやドアの認証装置６Ａによって認証を行うことで、人物情報データベース２２ＢのＰＣβの利用権限と部屋Ｂの入室権限が「○」と書き換えられ、ＰＣβにログインすることが可能となる（ｆ３４）。

【０１３２】

次に、部屋毎に入室権限の有無を決めずに、権限レベルと部屋への入室権限、ＰＣ利用権限の関係を予め定めた権限レベル－利用可能情報変換テーブル２１８（図２５）を利用すれば、利用権限レベルを各利用者に設定しても同様である。この権限レベル－利用可能情報変換テーブル２１８は図２５に示すように、権限レベル２２０に対して各部屋の入室権限２２２が設定され、権限レベル２２０には５段階の権限レベル「０」～「４」が設定され、権限レベル「０」では部屋Ａ～部屋Ｄの全ての入室権限、ＰＣα、ＰＣβ及びＰＣγの利用権限がなく、権限レベル「１」では部屋Ａのみに入室権限、ＰＣαのみに利用権限があり、権限レベル「２」では部屋Ａのみに入室権限、ＰＣα及びＰＣβに利用権限があり、権限レベル「３」では部屋Ａのみに入室権限、ＰＣα、ＰＣβ及びＰＣγに利用権限があり、権限レベル「４」では部屋Ａ及び部屋Ｂに室権限があり、ＰＣα、ＰＣβ及びＰＣγに利用権限がある。

【０１３３】

利用者の認証情報を管理する利用者ＩＤ、登録してある人物の名前、認証情報と比較して本人かを判断する登録認証情報、その人が持つ権限レベル等の情報が登録され、人物情報データベース２２Ｂには、図１２、図１３に示すように、それぞれの人物毎に、追跡データを管理する追跡データＩＤ、追跡データが誰であるかを示す利用者ＩＤ、現在の権限レベル、人物の現在位置、移動軌跡等が登録される。

【０１３４】

このような権限レベル（図２６）において、その権限レベルの変化は図２７に示すように変化する。利用者１が廊下９２に入ってきた時点では認証を行っていないため、誰であるか分からない。よって、人物情報データベース２２Ｂには新しい人物の発見により追跡データＩＤと現在位置が新しく加えられるが、それに対応する利用者ＩＤは「なし」、権限レベルは全ての権限が「×」である「０」となる（ｆ４１）。

【０１３５】

利用者１が認証を行い利用者１であると判断された時点で、人物情報データベース２２Ｂには利用者ＩＤを「利用者１」に設定し、利用者１の持つ権限レベルが「４」となり、この権限レベルに応じた、部屋Ａ、部屋Ｂへの入室、ＰＣα、ＰＣβの利用が可能となる（ｆ４２）。

【０１３６】

一度認証するだけで、ＰＣの利用権限も得られるため、再認証をせずにＰＣの利用が可能である。しかし、部屋Ａへの入室後、利用者２と接近すると、利用者２と利用者１を誤認識する可能性があるため、利用者１と利用者２の権限レベルを比較し、両者の権限レベルを低い方のレベルに設定する。つまり、今回の場合では両者の低い方に合わせるため、利用者２の権限レベルである「２」が利用者１に与えられることになり、人物情報データベース２２Ｂでは利用者１の権限レベルを「２」と書き換える（ｆ４３）。

【０１３７】

利用者１は再度ＰＣやドアの認証装置によって認証を行うことで、人物情報データベース２２Ｂの権限レベルがもともと持っていたレベルである「４」と書き換えられ、ＰＣβへのログインと部屋Ｂへの入室が可能となる（ｆ４４）。

【０１３８】

以上説明したように、第２の実施の形態においても、利用者が認証した後であっても、自分より権限の低い人物と接近し、どちらが権限を持った人であるかが不明であるとき、利用権限が低下するので、誤って利用権限がない人の入室やＰＣログインを許可することがなく、セキュリティの低下を防止することができる。

【０１３９】

〔第３の実施の形態〕

【０１４０】

第３の実施の形態について、図２８、図２９、図３０及び図３１を参照する。図２８は、第３の実施の形態に係る利用者の状態管理処理の処理手順を示すフローチャート、図２９は、第３の実施の形態に係るドアの開閉制御処理の処理手順を示すフローチャート、図３０は、認証動作例を示す図、図３１は、他の認証動作例を示す図である。図２８～図３１に示す構成は一例であって、斯かる構成に本発明が限定されるものではない。図３０及び図３１において、図１、図７及び図９と同一部分には同一符号を付してある。

【０１４１】

第３の実施の形態に係るセキュリティシステムは、第１の実施の形態のセキュリティシステム２Ａと同一の構成であるので、装置構成の説明は図１を参照し、その説明を省略する。

【０１４２】

この第３の実施の形態に係るセキュリティシステムでは、利用者の状態管理処理の処理手順（図２８）と、ドアの開閉制御処理の処理手順（図２９）の双方の処理を並行して行っている。

【０１４３】

利用者の状態管理処理の処理手順では、図２８に示すように、人物の位置を検出し（ステップＳ３０１）、認証作業が行われたか否かを判定し（ステップＳ３０２）、認証作業が行われた場合には（ステップＳ３０２のＹＥＳ）、人物間の距離の計測を行い（ステップＳ３０３）、人物の距離が近いか否かを判定し（ステップＳ３０４）、人物の距離が近い場合には（ステップＳ３０４のＹＥＳ）、再認証の呼びかけを行い（ステップＳ３０５）、ステップＳ３０１に戻る。また、人物の距離が近くない場合には（ステップＳ３０４のＮＯ）、人物の位置と認証情報の対応付けを行い（ステップＳ３０６）、ステップＳ３１０に戻り、人物を監視し、ステップＳ３０２～Ｓ３０６の処理を実行する。

【０１４４】

この処理手順において、ステップＳ３０１では、撮像装置１２Ａ、１２Ｂから得られた画像を基に人物位置検出・追跡部２６で常に監視範囲にいる人物の位置を把握する。この実施の形態においても図７に示すように、各部屋Ａ、Ｂ、Ｃ、Ｄや廊下９２等、全ての場所に、それぞれ撮像装置１２Ａ、１２Ｂ、１２Ｃ、１２Ｄ、１２Ｅが置かれており、人物がどの場所にいても連続して追跡が行われる。得られた人物ＩＤ毎の人物位置は人物情報データベース２２Ａに随時に保存される。初めて検出された人物については誰であるか分からないため、利用者ＩＤはなし、入室権限も全てなしとして初期化を行う。

【０１４５】

また、ステップＳ３０２では、利用者が部屋へ入室する際には、認証装置によって認証を実行する。その場合、表示装置４５（図２）のディスプレイ上に利用者認証用のダイアログを表示し、利用者とパスワードを用いて認証する方法や、静脈や指紋を用いた認証装置を利用した認証方法によって認証情報データベース２０Ａとの照合を行い、個人を特定する。予め、認証情報データベース２０Ａに登録されていない等、認証されない場合にはステップＳ３０１に遷移する。

【０１４６】

ステップＳ３０３では、ステップＳ３０２で認証が行われた際には、認証が行われた認証装置６の周囲の人の位置関係を、人物情報データベース２２Ａに格納されている人物位置によって調べる（ステップＳ３０４）。このとき、認証を行ったと思われる人物と周辺の人物との距離が所定距離以下の情況を検出した場合（ステップＳ３０４のＹＥＳ）は、認証結果を人物に対応付けず、入室権限が与えられなかったことを利用者に伝え、再認証の呼びかけを行う（ステップＳ３０５）。この呼びかけは、表示装置４５を通して行えばよい。

【０１４７】

また、その状態が検出されなかった場合には（ステップＳ３０４のＮＯ）、認証者と認証が行われた場所との位置関係から、認証情報と人物の位置との対応付けを行う（ステップＳ３０６）。具体的には、認証装置６の位置と認証装置ＩＤを予め対応付け、認証が行われた認証装置６の場所に最も近い位置にいる追跡データＩＤの利用者に認証で判定された利用者ＩＤを登録する。また、同時に、利用者に合わせた入室権限とＰＣ利用権限（第２の実施の形態）も分かるため、人物情報データベース２２Ａ（図１）又は人物情報データベース２２Ｂ（図１６）の利用権限も更新する。

【０１４８】

そして、ステップＳ３０５又はステップＳ３０６を経てステップＳ３０１に戻り、既述の処理を繰り返す。

【０１４９】

ドアの開閉制御処理の処理手順では、図２９に示すように、人物情報データベース２２Ａにアクセスし、人物位置、利用者ＩＤ、入室権限等を読み出す（ステップＳ３１１）。この処理の後、各ドア周辺に人物がいるか否かを人物位置を用いて確認し（ステップＳ３１２）、ドアの前に人がいなければ、ステップＳ３１１に戻る。

【０１５０】

ドア周辺に人物がいる場合には（ステップＳ３１２のＹＥＳ）、ドア周辺にいる人物がそのドアの入室権限を持っているか否かを判断し（ステップＳ３１３）、ドア周辺にいる人物がそのドアの入室権限を持っている場合には（ステップＳ３１３のＹＥＳ）、ドアを開錠する（ステップＳ３１４）。

【０１５１】

ステップＳ３１３又はステップＳ３１４を経た後、ステップＳ３１１に戻り、既述の処理を繰り返す。

【０１５２】

このような環境で稼動した場合について、一人で認証を行った場合の認証動作（図３０）では、図３０Ａに示すように、利用者Ｐ１が認証装置６で認証をすることにより、認証装置６を設置した部屋２３０の入室権限を得る。この入室権限を持つ利用者Ｐ１が部屋２３０のドア１４の前に行くと、図３０Ｂに示すように、ドア１４が開錠し、利用者Ｐ１は部屋２３０に入室することができる。

【０１５３】

このような一人認証に対し、その認証時、図３１Ａに示すように、利用者Ｐ１の認証動作を行う際、周辺に他人又は複数の他人として利用者Ｐ２、Ｐ３がいる場合には、利用者Ｐ１の認証が正しく行われた場合でも、その認証結果を認証した本人に正しく対応付けられない可能性がある。そこで、このような場合は入室権限を与えず、入室権限が与えられなかった旨を伝えるとともに、周辺の人物に離れるような指示を送る等をして、再認証を

促す指示を出力する。

【０１５４】

このような動作はＰＣのログインについても利用権限を持たない他人のログインを防止することができる。

【０１５５】

以上のように、認証を行った時点で、誰に権限を持たせるか怪しくなったときには権限を与えないため、システムが誤って利用権限がない人の入室やＰＣログインを許可することがなくなり、セキュリティの低下を防止することができる。

【０１５６】

次に、以上述べた本発明の実施の形態から抽出される技術的思想を請求項の記載形式に準じて付記として列挙する。本発明に係る技術的思想は上位概念から下位概念まで、様々なレベルやバリエーションにより把握できるものであり、以下の付記に本発明が限定されるものではない。

【０１５７】

（付記１）　特定エリアの利用者に認証に基づく利用権限を付与し、その利用権限により前記特定エリアの利用を許可するセキュリティシステムであって、

利用者を認証する認証手段と、

利用者の位置及び／又はその移動を検出する位置検出手段と、

前記認証手段の認証に基づき、利用権限が付与された利用者の位置及び／又はその移動を前記位置検出手段の検出出力によって監視し、利用者間の距離が所定値以下になった場合、各利用者に付与されている利用権限を変更する利用権限制御手段と、

を備えることを特徴とするセキュリティシステム。

【０１５８】

（付記２）　付記１のセキュリティシステムにおいて、

前記利用権限制御手段は、前記認証に基づき、利用者に同一又は異なるレベルの利用権限を設定し、利用者間の距離が所定値以下になった場合に、各利用者に設定されている利用権限をレベルの低い利用権限に変更する構成としたことを特徴とするセキュリティシステム。

【０１５９】

（付記３）　付記１のセキュリティシステムにおいて、

認証した利用者を追跡する利用者追跡手段を備え、前記利用権限制御手段は、前記利用者追跡手段の追跡に基づき、前記利用者の利用権限又は変更された利用権限を維持する構成としたことを特徴とするセキュリティシステム。

【０１６０】

（付記４）　付記１のセキュリティシステムにおいて、

前記利用権限制御手段は、前記利用権限をサービス毎に設定し、利用者間の距離が所定値以下になった場合に、各利用者に設定されている利用権限を、サービスとの論理積により求められた利用権限に変更する構成としたことを特徴とするセキュリティシステム。

【０１６１】

（付記５）　付記１のセキュリティシステムにおいて、

前記利用権限制御手段は、利用者間の距離が所定値以下になった場合に、各利用者の利用権限の低減又は解除をする構成としたことを特徴とするセキュリティシステム。

【０１６２】

（付記６）　付記１、２、３、４又は５のセキュリティシステムにおいて、

前記利用権限制御手段は、利用権限が変更された利用者が再認証を受けることにより、新たな利用権限を受け得る構成としたことを特徴とするセキュリティシステム。

【０１６３】

（付記７）　付記１のセキュリティシステムにおいて、

前記利用権限制御手段は、認証を受けた利用者と、他の利用者との距離が所定値内であることを検出した場合、認証を受けた利用者に利用権限を与えない構成としたことを特徴

とするセキュリティシステム。
【０１６４】
（付記８）　付記４のセキュリティシステムにおいて、
　前記利用権限制御手段は、認証を受けた利用者と、他の利用者との距離がある所定値以内であることを検出した際に、認証時に利用権限が与えられないことを通知する通知手段を備えることを特徴とするセキュリティシステム。
【０１６５】
（付記９）　特定エリアの利用者に認証に基づく利用権限を付与し、その利用権限により前記特定エリアの利用を許可するセキュリティ方法であって、
　利用者を認証する認証ステップと、
　利用者の位置及び／又はその移動を検出する位置検出ステップと、
　前記認証に基づき、利用権限が付与された利用者の位置及び／又はその移動を監視し、利用者間の距離が所定値以下になった場合、各利用者に付与されている利用権限を変更するステップと、
　を含むことを特徴とするセキュリティ方法。
【０１６６】
（付記１０）　付記９のセキュリティ方法において、
　前記認証に基づき、利用者に同一又は異なるレベルの利用権限を設定し、利用者間の距離が所定値以下になった場合に、各利用者に設定されている利用権限をレベルの低い利用権限に変更するステップを含むことを特徴とするセキュリティ方法。
【０１６７】
（付記１１）　付記９のセキュリティ方法において、
　認証した利用者の追跡情報に基づき、前記利用者の利用権限又は変更された利用権限を維持するステップを含むことを特徴とするセキュリティ方法。
【０１６８】
（付記１２）　付記９のセキュリティ方法において、
　前記利用権限をサービス毎に設定し、利用者間の距離が所定値以下になった場合に、各利用者に設定されている利用権限を、サービスとの論理積により求められた利用権限に変更するステップを含むことを特徴とするセキュリティ方法。
【０１６９】
（付記１３）　付記９のセキュリティ方法において、
　利用者間の距離が所定値以下になった場合に、各利用者の利用権限の低減又は解除をするステップを含むことを特徴とするセキュリティ方法。
【０１７０】
（付記１４）　付記９、１０、１１、１２又は１３のセキュリティ方法において、
　利用権限が変更された利用者は、再認証を受けることにより、新たな利用権限を受けるステップを含むことを特徴とするセキュリティ方法。
【０１７１】
（付記１５）　付記９のセキュリティ方法において、
　認証を受けた利用者と、他の利用者との距離が所定値内であることを検出した場合、認証を受けた利用者に利用権限を与えないステップを含むことを特徴とするセキュリティ方法。
【０１７２】
（付記１６）　付記９のセキュリティ方法において、
　認証を受けた利用者と、他の利用者との距離が所定値以内であることを検出した際に、認証時に利用権限が与えられないことを通知するステップを含むことを特徴とするセキュリティ方法。
【０１７３】
（付記１７）　特定エリアの利用者に認証に基づく利用権限を付与し、その利用権限により前記特定エリアの利用を許可する機能を備え、斯かる機能をコンピュータに実行させる

セキュリティプログラムを格納したコンピュータ読取り可能な記録媒体であって、
利用者を認証する認証機能と、
利用者の位置及び／又はその移動を表す検出情報を取り込む検出情報取込み機能と、
前記認証に基づき、利用権限が付与された利用者の位置及び／又はその移動を前記検出情報によって監視し、利用者間の距離が所定値以下になった場合、各利用者に付与されている利用権限を変更する利用権限制御機能と、
を含むセキュリティプログラムを格納したコンピュータ読取り可能な記録媒体。

【０１７４】

（付記１８）　付記１７の記録媒体において、
前記認証に基づき、利用者に同一又は異なるレベルの利用権限を設定し、利用者間の距離が所定値以下になった場合に、各利用者に設定されている利用権限をレベルの低い利用権限に変更する機能を含むセキュリティプログラムを格納したコンピュータ読取り可能な記録媒体。

【０１７５】

（付記１９）　付記１７の記録媒体において、
認証した利用者の追跡情報に基づき、前記利用者の利用権限又は変更された利用権限を維持する機能を含むセキュリティプログラムを格納したコンピュータ読取り可能な記録媒体。

【０１７６】

（付記２０）　付記１７の記録媒体において、
前記利用権限をサービス毎に設定し、利用者間の距離が所定値以下になった場合に、各利用者に設定されている利用権限を、サービスとの論理積により求められた利用権限に変更する機能を含むセキュリティプログラムを格納したコンピュータ読取り可能な記録媒体。

【０１７７】

（付記２１）　付記１７の記録媒体において、
利用者間の距離が所定値以下になった場合に、各利用者の利用権限の低減又は解除をする機能を含むセキュリティプログラムを格納したコンピュータ読取り可能な記録媒体。

【０１７８】

（付記２２）　付記１７、１８、１９、２０又は２１の記録媒体において、
利用権限が変更された利用者は、再認証を受けることにより、新たな利用権限を受ける機能を含むセキュリティプログラムを格納したコンピュータ読取り可能な記録媒体。

【０１７９】

（付記２３）　付記１７の記録媒体において、
認証を受けた利用者と、他の利用者との距離が所定値内であることを検出した場合、認証を受けた利用者に利用権限を与えない機能を含むセキュリティプログラムを格納したコンピュータ読取り可能な記録媒体。

【０１８０】

（付記２４）　付記１７の記録媒体において、
認証を受けた利用者と、他の利用者との距離がある所定値以内であることを検出した際に、認証時に利用権限が与えられないことを通知する通知機能を含むセキュリティプログラム格納したコンピュータ読取り可能な記録媒体。

【０１８１】

以上説明したように、本発明の最も好ましい実施の形態等について説明したが、本発明は、上記記載に限定されるものではなく、特許請求の範囲に記載され、又は発明を実施するための最良の形態に開示された発明の要旨に基づき、当業者において様々な変形や変更が可能であることは勿論であり、斯かる変形や変更が、本発明の範囲に含まれることは言うまでもない。

【産業上の利用可能性】

【０１８２】

本発明は、施設利用等のセキュリティに関し、認証要求の回数を低減して利便性を高めるとともに、認証により付与された利用権限の他人利用を防止し、利用者は認証を受けることによって付与される利用権限に基づき、特定エリア内のサービス提供等の利用が可能であり、一度認証したら繰り返しの認証を求めることなく利用権限を維持する等、利便性を高めることができるとともに、利用権限を持たない他人利用を防止でき、利用者の位置や移動を追跡し、移動軌跡に認証結果を対応付けるので、一度の認証の後、繰り返しの認証を避け、セキュリティ低下を防止するとともに、利便性を高めることができ、研究施設等の高度なセキュリティが必要なエリアで利用でき、有用である。

【図面の簡単な説明】

【０１８３】

【図１】第１の実施の形態に係るセキュリティシステムを示す図である。
【図２】処理装置のハードウェア構成を示す図である。
【図３】認証情報データテーブルを示す図である。
【図４】人物情報データテーブルを示す図である。
【図５】第１の実施の形態に係る利用者の状態管理処理の処理手順を示すフローチャートである。
【図６】第１の実施の形態に係るドアの開閉制御処理の処理手順を示すフローチャートである。
【図７】セキュリティシステムの使用例を示す図である。
【図８】利用者の権限例を示す図である。
【図９】利用者の移動経路の一例を示す図である。
【図１０】利用者の入室権限の変化例を示す図である。
【図１１】権限レベル－入室可能変換テーブルを示す図である。
【図１２】権限レベルを利用した認証情報データテーブルを示す図である。
【図１３】権限レベルを利用した人物情報データテーブルを示す図である。
【図１４】権限レベルを利用した利用者権限例を示す図である。
【図１５】権限レベルを利用した権限変化例を示す図である。
【図１６】第２の実施の形態に係るセキュリティシステムを示す図である。
【図１７】認証情報データテーブルを示す図である。
【図１８】人物情報データテーブルを示す図である。
【図１９】第２の実施の形態に係る利用者の状態管理処理の処理手順を示すフローチャートである。
【図２０】ドアの開閉制御処理及びＰＣログイン制御処理の処理手順を示すフローチャートである。
【図２１】第２の実施の形態に係るセキュリティシステムの実施例を示す図である。
【図２２】利用者の権限例を示す図である。
【図２３】利用者の移動経路の一例を示す図である。
【図２４】利用者の権限の変化例を示す図である。
【図２５】権限レベル－利用可能情報変換テーブルを示す図である。
【図２６】権限レベルを利用した利用者権限例を示す図である。
【図２７】権限レベルを利用した権限変化例を示す図である。
【図２８】第３の実施の形態に係る利用者の状態管理処理の処理手順を示すフローチャートである。
【図２９】第３の実施の形態に係るドアの開閉制御処理の処理手順を示すフローチャートである。
【図３０】認証動作例を示す図である。
【図３１】他の認証動作例を示す図である。

【符号の説明】

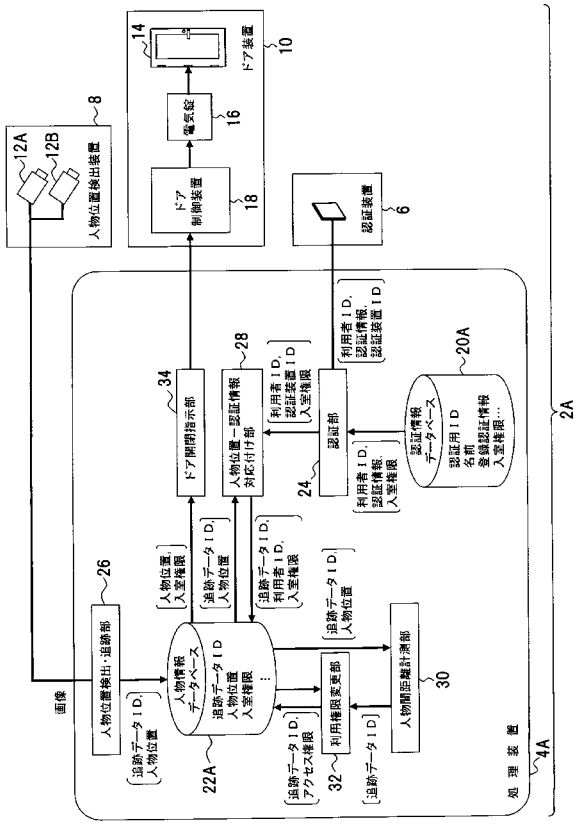
【０１８４】

２Ａ、２Ｂ　セキュリティシステム

４Ａ、４Ｂ　処理装置
６　認証装置
８　人物位置検出装置
１０　ドア装置
１２Ａ、１２Ｂ、１２Ｃ、１２Ｄ、１２Ｅ　撮像装置
１４　ドア
１６　電気錠
１８　ドア制御装置
２０Ａ、２０Ｂ　認証情報データベース
２２Ａ、２２Ｂ　人物情報データベース
２４　認証部
２６　人物位置検出・追跡部
２８　人物位置－認証情報対応付け部
３０　人物間距離計測部
３２　利用権限変更部
３４　ドア開閉指示部
３６　中央処理装置
３８　主記憶装置
４０　補助記憶装置
４２　入力装置
４４　出力装置
４６　制御装置
４８　演算装置
５０　認証情報データテーブル
５２　利用者ＩＤ
５４　名前
５６　登録認証情報
５８　入室権限
６０　人物情報データテーブル
６２　追跡データＩＤ
６４　利用者ＩＤ
６６　人物位置
６８　移動軌跡
７４　現在の入室権限
９０　建造物
９２　廊下
９６、９８、１００、１０２、１０４　移動経路
１０８　権限レベル－入室可能部屋変換テーブル
１１４　認証情報データテーブル
１１６　人物情報データテーブル
１４０　ＰＣ
１４１　ディスプレィ
１４２　ＰＣ画像制御部
１４４　認証情報データテーブル
１５６　人物情報データテーブル
２１４、２１６　移動経路
２３０　部屋
Ｐ１、Ｐ２、Ｐ３　利用者

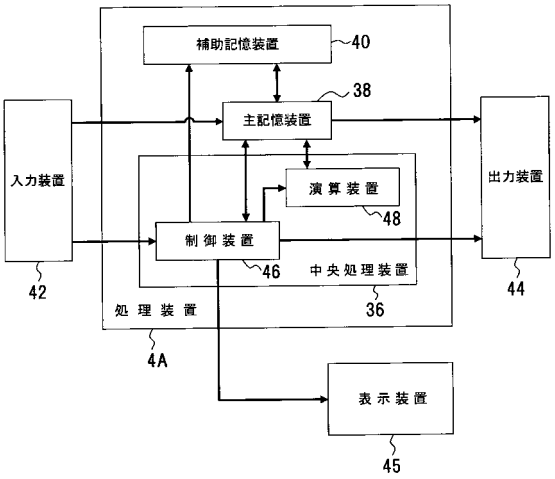
【図１】

第１の実施の形態に係るセキュリティシステムを示す図



【図２】

処理装置のハードウェア構成を示す図



【図３】

認証情報データテーブルを示す図

認証情報データテーブル 50（20A）

利用者ＩＤ	名前	登録認証情報（パスワード）	入室権限				
			部屋Ａ	部屋Ｂ	…	役員室	会議室
000001	鈴木 太郎	××××××	○	○		×	○
000002	田中 次郎	△△△△△△	○	×		×	×
000003	山田 三郎	□□□□□□	○	○		○	○
…	…	…	…	…		…	…

52　54　56　58

【図４】

人物情報データテーブルを示す図

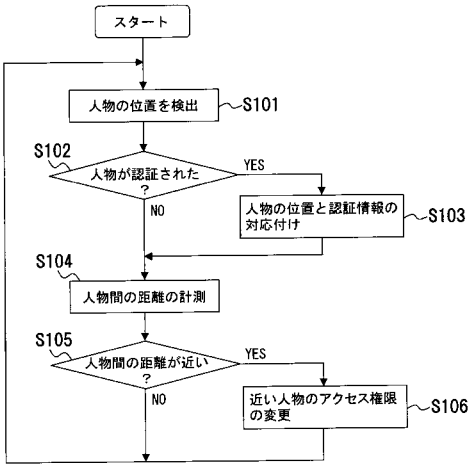
人物情報データテーブル 60（22A）

追跡データID	利用者ＩＤ	人物位置 (x, y)	移動軌跡 (x, y)				現在の入室権限				
			1時刻前位置	2時刻前位置	…	N時刻前位置	部屋Ａ	部屋Ｂ	…	役員室	会議室
001	000001	(100, 200)	(110, 210)	(120, 200)	…	(50, 0)	○	○	…	×	○
002	なし	(500, 100)	(500, 100)	(450, 150)	…	(0, 200)	×	×	…	×	×
003	000003	(0, 0)	(20, 20)	(20, 20)	…	(20, 20)	○	○	…	○	×
…	…	…	…	…	…	…	…	…	…	…	…

62　64　66　721　722　68　72N　70

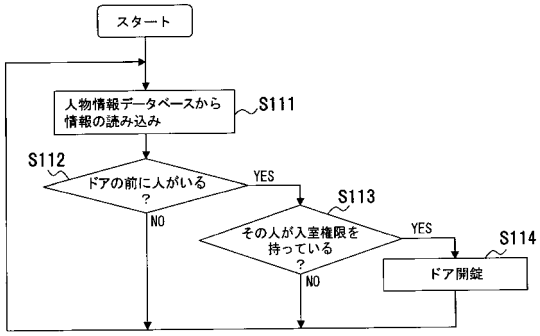
【図５】

第１の実施の形態に係る利用者の状態管理処理の処理手順を示すフローチャート



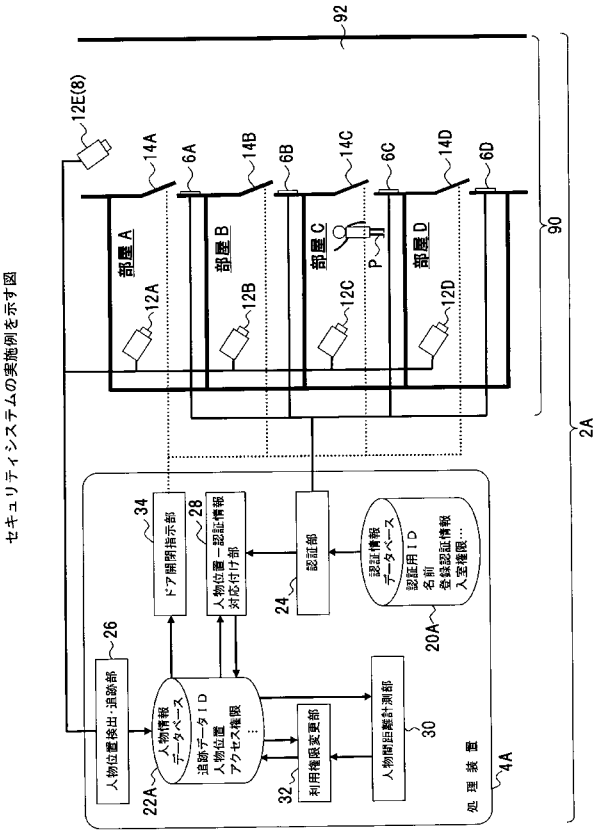
【図６】

第１の実施の形態に係るドアの開閉制御処理の処理手順を示すフローチャート



【図７】

セキュリティシステムの実施例を示す図



【図８】

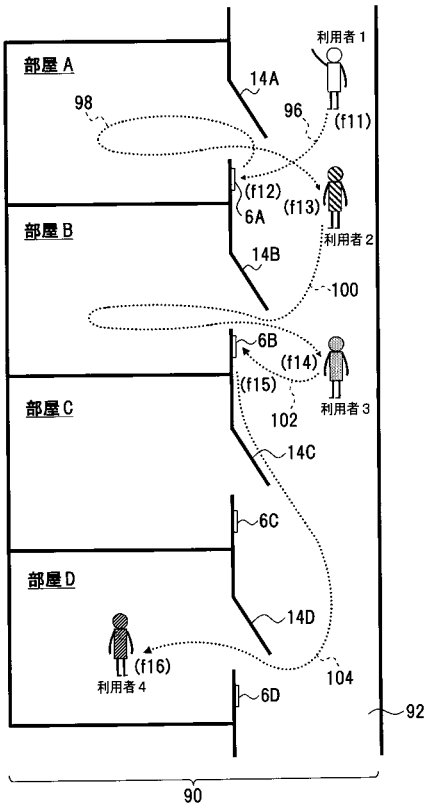
利用者の権限例を示す図

利用者の権限例

	部屋Ａ	部屋Ｂ	部屋Ｃ	部屋Ｄ
利用者１	○	○	×	○
利用者２	×	○	○	○
利用者３	○	○	×	×
利用者４	×	×	×	○

【図９】

利用者の移動経路の一例を示す図



【図１０】

利用者の入室権限の変化例を示す図

利用者の入室権限の変化例

行動内容	各部屋の入室権限															
	利用者1				利用者2				利用者3				利用者4			
	A	B	C	D	A	B	C	D	A	B	C	D	A	B	C	D
f11：認証前	×	×	×	×	×	○	○	○	○	○	×	×	×	×	×	○
f12：認証して利用者１であると判定	○	○	×	○	×	○	○	○	○	○	×	×	×	×	×	○
f13：廊下で利用者２と接近	×	○	×	○	×	○	×	○	○	○	×	×	×	×	×	○
f14：廊下で利用者３と接近	×	○	×	×	×	○	×	○	×	○	×	×	×	×	×	○
f15：認証装置Ｂで再認証	○	○	×	○	×	○	×	○	×	○	×	×	×	×	×	○
f16：部屋Ｄで利用者４と接近	×	×	×	○	×	○	×	○	×	○	×	×	×	×	×	○

【図１１】

権限レベル―入室可能部屋変換テーブルを示す図

権限レベル―入室可能部屋変換テーブル 108（20A）

	部屋A	部屋B	部屋C	部屋D
権限レベル０	×	×	×	×
権限レベル１	×	×	×	○
権限レベル２	×	×	○	○
権限レベル３	×	○	○	○
権限レベル４	○	○	○	○

110 112

【図１２】

権限レベルを利用した認証情報データテーブルを示す図

権限レベルを利用した認証情報データテーブル 114（22A）

利用者ＩＤ	名前	登録認証情報（パスワード）	入室権限レベル
000001	鈴木 太郎	××××××	4
000002	田中 次郎	△△△△△△	2
000003	上田 三郎	□□□□□□	1
…	…	…	…

118 120 122 124

【図１３】

権限レベルを利用した人物情報データテーブルを示す図

権限レベルを利用した人物情報データテーブル116（20A）

追跡データＩＤ	利用者ＩＤ	人物位置 (x, y)	移動軌跡 (x, y)			現在の入室権限レベル
			1時刻前位置	2時刻前位置	…… N時刻前位置	
001	000001	(100, 200)	(110, 210)	(120, 200)	…… (50, 0)	3
002	なし	(500, 100)	(500, 100)	(450, 150)	…… (0, 200)	0
003	000003	(0, 0)	(20, 20)	(20, 20)	…… (20, 20)	1
…	…	…	…	…	… …	…

126　128　130　132　134

【図１４】

権限レベルを利用した利用者権限例を示す図

権限レベルを利用した利用者権限例

	権限レベル
利用者１	4
利用者２	3
利用者３	1
利用者４	2

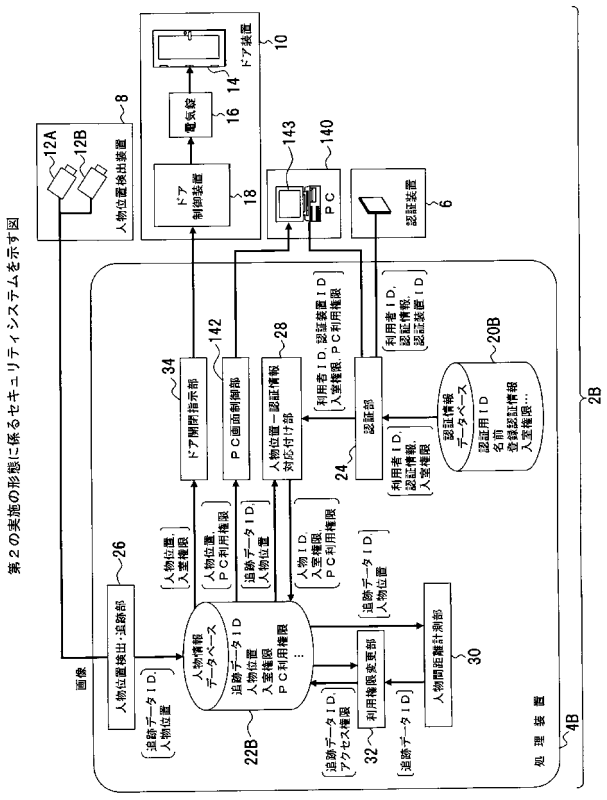
【図１５】

権限レベルを利用した権限変化例を示す図

権限レベルを利用した権限変化例

行動内容	各利用者の入室権限レベル			
	利用者１	利用者２	利用者３	利用者４
f21：認証前	0	3	1	2
f22：認証して利用者１であると判定	4	3	1	2
f23：廊下で利用者２と接近	3	3	1	2
f24：廊下で利用者３と接近	1	3	1	2
f25：認証装置Ｂで再認証	4	3	1	2
f26：部屋Ｄで利用者４と接近	2	3	1	2

【図１６】



【図１７】

認証情報データテーブルを示す図

認証情報データテーブル 144（20B）

利用者ＩＤ	名前	登録認証情報（パスワード）	ＰＣの利用権限			入室権限			
			ＰＣα	ＰＣβ	ＰＣζ	部屋Ａ	部屋Ｂ	役員室	会議室
000001	鈴木 太郎	×××××××	○	○	×	○	○	×	○
000002	田中 次郎	△△△△△△△	×	×	○	○	×	×	×
000003	山田 三郎	□□□□□□□	○	○	○	○	○	○	○
…	…	…	…	…	…	…	…	…	…

146 148 150 152 154

【図１８】

人物情報データベースを示す図

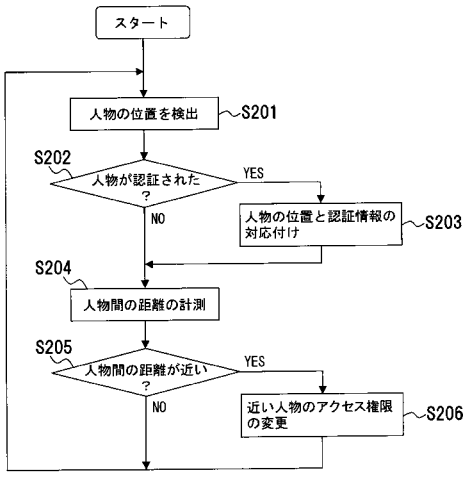
人物情報データテーブル 156（22B）

追跡データＩＤ	利用者ＩＤ	人物位置（x, y）	移動軌跡（x, y）			現在のＰＣの利用権限			現在の入室権限			
			1時刻前位置	2時刻前位置	N時刻前位置	ＰＣα	ＰＣβ	ＰＣζ	部屋Ａ	部屋Ｂ	役員室	会議室
001	000001	(100, 200)	(110, 210)	(120, 200)	(50, 0)	○	×	×	○	○	×	○
002	なし	(500, 100)	(500, 100)	(450, 150)	(0, 200)	×	×	×	×	×	×	×
003	000003	(0, 0)	(20, 20)	(20, 20)	(20, 20)	○	×	○	○	○	○	×
…	…	…	…	…	…	…	…	…	…	…	…	…

158 160 162 164 166 168

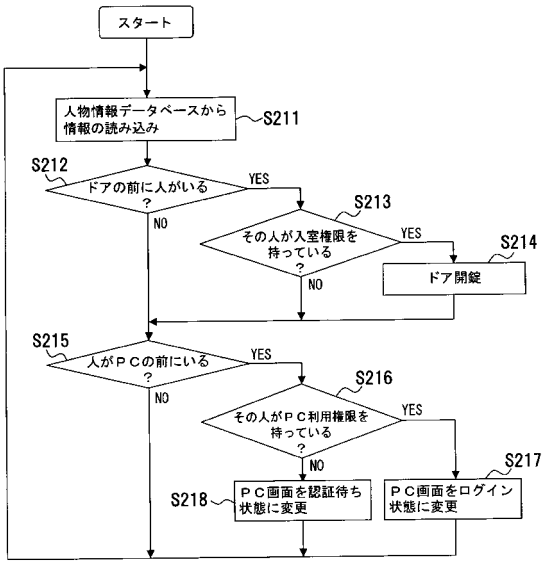
【図１９】

第２の実施の形態に係る利用者の状態管理処理の処理手順を示すフローチャート



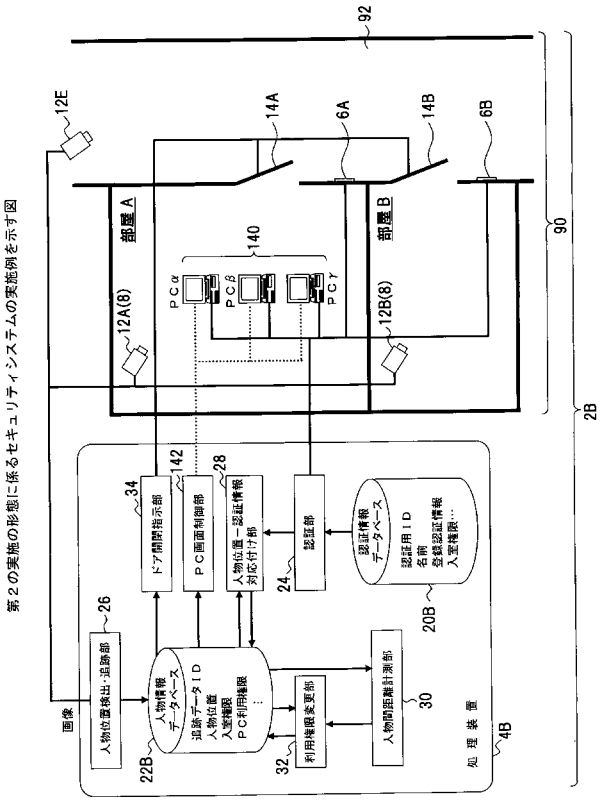
【図２０】

ドアの開閉制御処理及びＰＣログイン制御処理の処理手順を示すフローチャート



【図２１】

第２の実施の形態に係るセキュリティシステムの実施例を示す図



【図２２】

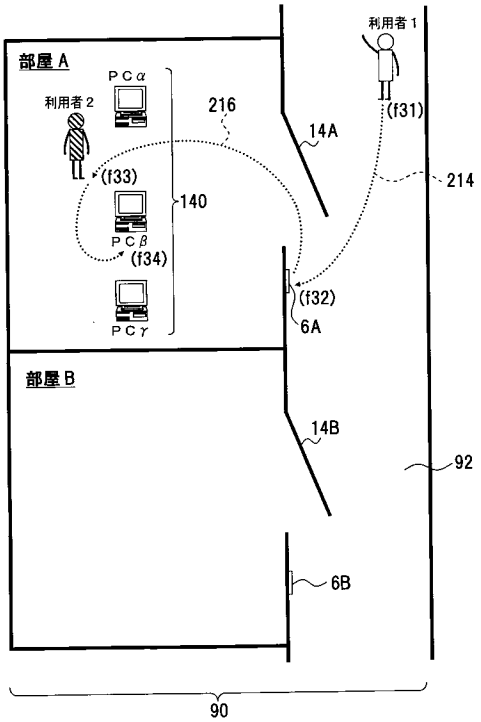
利用者の権限例を示す図

利用者の権限例

利用者	入室権限		PC利用権限		
	A	B	PCα	PCβ	PCγ
利用者１	○	○	○	○	×
利用者２	○	×	○	×	○

【図２３】

利用者の移動経路の一例を示す図



【図２４】

利用者の権限の変化例を示す図

利用者の権限の変化例

行動内容	利用者１					利用者２				
	入室権限		PC利用権限			入室権限		PC利用権限		
	A	B	α	β	γ	A	B	α	β	γ
f31：認証前	×	×	×	×	×	○	×	○	×	○
f32:認証により利用者１であると判定	○	○	○	○	×	○	×	○	×	○
f33:室内で利用者２と接近	○	×	○	×	×	○	×	○	×	×
f34:PCβで再認証	○	○	○	○	×	○	×	○	×	×

【図２５】

権限レベル－利用可能情報変換テーブルを示す図

権限レベル－利用可能情報変換テーブル 218（22B）

	入室権限		PC利用権限		
	部屋A	部屋B	PCα	PCβ	PCγ
権限レベル０	×	×	×	×	×
権限レベル１	○	×	○	×	×
権限レベル２	○	×	○	○	×
権限レベル３	○	×	○	○	○
権限レベル４	○	○	○	○	○

220　222　224

【図２６】

権限レベルを利用した利用者権限例を示す図

権限レベルを利用した利用者権限例

	権限レベル
利用者１	4
利用者２	2

【図２７】

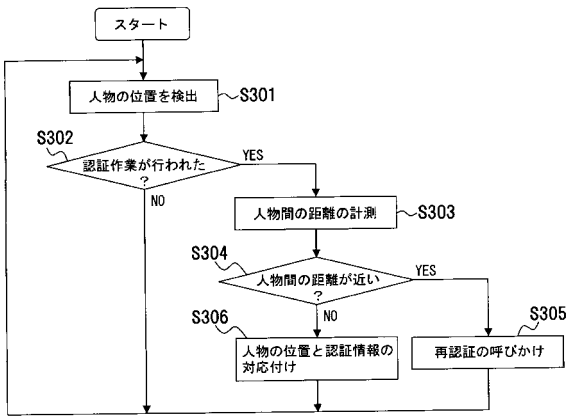
権限レベルを利用した権限変化例を示す図

権限レベルを利用した権限変化例

行動内容	権限レベル	
	利用者１	利用者２
f41：認証前	0	2
f42：認証により利用者１であると判定	4	2
f43：室内で利用者２と接近	2	2
f44：PCβで再認証	4	2

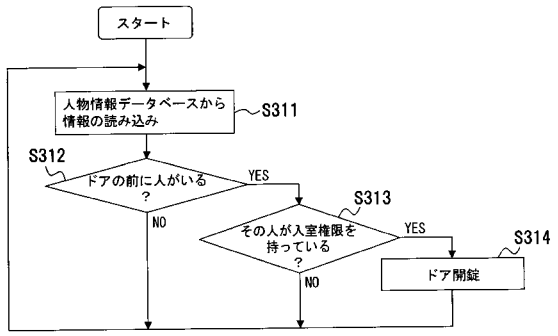
【図２８】

第３の実施の形態に係る利用者の状態管理処理の処理手順を示すフローチャート



【図２９】

第３の実施の形態に係るドアの開閉制御処理の処理手順を示すフローチャート



【図３０】

認証動作例を示す図

図30A

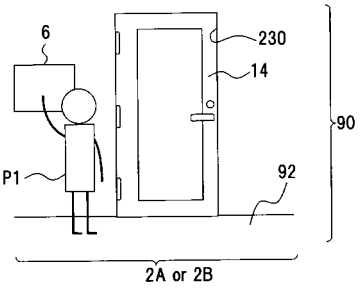
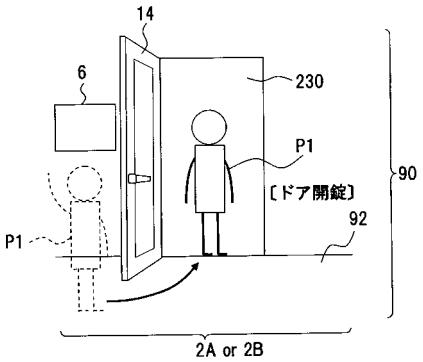


図30B



【図３１】

他の認証動作例を示す図

図31A

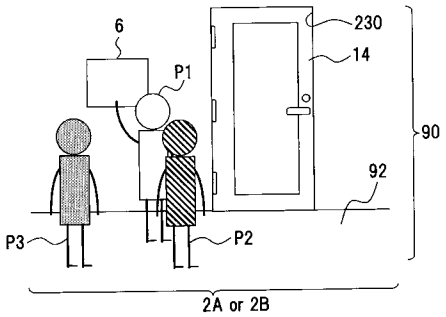
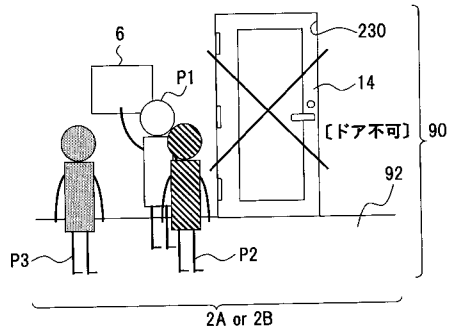


図31B



【手続補正書】
【提出日】平成21年7月30日(2009.7.30)
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】００３６
【補正方法】変更
【補正の内容】
【００３６】
認証情報データベース２０Ａは、利用者の認証情報を管理する利用者ＩＤ、登録してある人物の名前、認証情報と比較して本人か否かを判断する登録認証情報、その人が入室できるドアを示す入室権限等、利用者認証処理を行うための情報が登録されたデータベースである。この認証情報データベース２０Ａには、認証用ＩＤ、名前、登録認証情報、入室権限等を表す情報が格納されている。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】００９９
【補正方法】変更
【補正の内容】
【００９９】
認証情報データベース２０Ｂは、第１の実施の形態と同様に、利用者の認証情報を管理する利用者ＩＤ、登録してある人物の名前、認証情報と比較して本人かを判断する登録認証情報、その人が入室できるドアを示す入室権限等、利用者認証処理を行うための情報が登録されたデータベースである。この認証情報データベース２０Ｂには、認証用ＩＤ、名前、登録認証情報、入室権限等を表す情報が格納されている。
【手続補正３】
【補正対象書類名】明細書
【補正対象項目名】０１０５
【補正方法】変更
【補正の内容】
【０１０５】
また、ＰＣ画面制御部１４２は、人物情報データベース２２Ｂから人物位置に応じ、利用者に設定されたＰＣ利用権限に関する情報が付与され、それに基づく制御信号を出力する。この制御信号は、ＰＣ１４０に対するログインの許可又は禁止の制御信号である。
【手続補正４】
【補正対象書類名】明細書
【補正対象項目名】０１２９
【補正方法】変更
【補正の内容】
【０１２９】
セキュリティシステム２Ｂが設置される環境として建造物９０には、図２１に示すように、監視領域として、部屋Ａ、部屋Ｂが設置されているとともに、各部屋の出入りが可能な通路として廊下９２が設置され、部屋Ａには複数のＰＣとしてＰＣα、ＰＣβ、ＰＣγが設置されている。部屋Ａの入口部にはドア１４Ａ及び認証装置６Ａ、部屋Ｂの入口部にはドア１４Ｂ及び認証装置６Ｂが設置されている。この場合、ドア１４Ａを開錠するためにはその認証装置での認証が必要となる。また、ＰＣα、ＰＣβ、ＰＣγはログインするために認証を必要とするシステムである。
【手続補正５】
【補正対象書類名】明細書
【補正対象項目名】０１３２
【補正方法】変更

【補正の内容】
【０１３２】
次に、部屋毎に入室権限の有無を決めずに、権限レベルと部屋への入室権限、ＰＣ利用権限の関係を予め定めた権限レベル－利用可能情報変換テーブル２１８（図２５）を利用すれば、利用権限レベルを各利用者に設定しても同様である。この権限レベル－利用可能情報変換テーブル２１８は図２５に示すように、権限レベル２２０に対して各部屋の入室権限２２２が設定され、権限レベル２２０には５段階の権限レベル「０」～「４」が設定され、権限レベル「０」では部屋Ａ～部屋Ｄの全ての入室権限、ＰＣα、ＰＣβ及びＰＣγの利用権限がなく、権限レベル「１」では部屋Ａのみに入室権限、ＰＣαのみに利用権限があり、権限レベル「２」では部屋Ａのみに入室権限、ＰＣα及びＰＣβに利用権限があり、権限レベル「３」では部屋Ａのみに入室権限、ＰＣα、ＰＣβ及びＰＣγに利用権限があり、権限レベル「４」では部屋Ａ及び部屋Ｂに入室権限があり、ＰＣα、ＰＣβ及びＰＣγに利用権限がある。
【手続補正６】
【補正対象書類名】明細書
【補正対象項目名】０１４３
【補正方法】変更
【補正の内容】
【０１４３】
利用者の状態管理処理の処理手順では、図２８に示すように、人物の位置を検出し（ステップＳ３０１）、認証作業が行われたか否かを判定し（ステップＳ３０２）、認証作業が行われた場合には（ステップＳ３０２のＹＥＳ）、人物間の距離の計測を行い（ステップＳ３０３）、人物の距離が近いか否かを判定し（ステップＳ３０４）、人物の距離が近い場合には（ステップＳ３０４のＹＥＳ）、再認証の呼びかけを行い（ステップＳ３０５）、ステップＳ３０１に戻る。また、人物の距離が近くない場合には（ステップＳ３０４のＮＯ）、人物の位置と認証情報の対応付けを行い（ステップＳ３０６）、ステップＳ３０１に戻り、人物を監視し、ステップＳ３０２～Ｓ３０６の処理を実行する。
【手続補正７】
【補正対象書類名】明細書
【補正対象項目名】０１８３
【補正方法】変更
【補正の内容】
【０１８３】
【図１】第１の実施の形態に係るセキュリティシステムを示す図である。
【図２】処理装置のハードウェア構成を示す図である。
【図３】認証情報データテーブルを示す図である。
【図４】人物情報データテーブルを示す図である。
【図５】第１の実施の形態に係る利用者の状態管理処理の処理手順を示すフローチャートである。
【図６】第１の実施の形態に係るドアの開閉制御処理の処理手順を示すフローチャートである。
【図７】セキュリティシステムの使用例を示す図である。
【図８】利用者の権限例を示す図である。
【図９】利用者の移動経路の一例を示す図である。
【図１０】利用者の入室権限の変化例を示す図である。
【図１１】権限レベル－入室可能部屋変換テーブルを示す図である。
【図１２】権限レベルを利用した認証情報データテーブルを示す図である。
【図１３】権限レベルを利用した人物情報データテーブルを示す図である。
【図１４】権限レベルを利用した利用者権限例を示す図である。
【図１５】権限レベルを利用した権限変化例を示す図である。

【図１６】第２の実施の形態に係るセキュリティシステムを示す図である。
【図１７】認証情報データテーブルを示す図である。
【図１８】人物情報データテーブルを示す図である。
【図１９】第２の実施の形態に係る利用者の状態管理処理の処理手順を示すフローチャートである。
【図２０】ドアの開閉制御処理及びＰＣログイン制御処理の処理手順を示すフローチャートである。
【図２１】第２の実施の形態に係るセキュリティシステムの実施例を示す図である。
【図２２】利用者の権限例を示す図である。
【図２３】利用者の移動経路の一例を示す図である。
【図２４】利用者の権限の変化例を示す図である。
【図２５】権限レベル－利用可能情報変換テーブルを示す図である。
【図２６】権限レベルを利用した利用者権限例を示す図である。
【図２７】権限レベルを利用した権限変化例を示す図である。
【図２８】第３の実施の形態に係る利用者の状態管理処理の処理手順を示すフローチャートである。
【図２９】第３の実施の形態に係るドアの開閉制御処理の処理手順を示すフローチャートである。
【図３０】認証動作例を示す図である。
【図３１】他の認証動作例を示す図である。

フロントページの続き

Ｆターム(参考) 3E038 AA01 CA02 CA06 CA07 CC03 GA02 HA05 HA07 JA01
5B285 AA01 BA00 CA02 CA33 CB02 CB15 CB16 CB17 CB49