

(19) 世界知的所有権機関
国際事務局(43) 国際公開日
2008 年 11 月 13 日 (13.11.2008)

PCT

(10) 国際公開番号
WO 2008/136120 A1

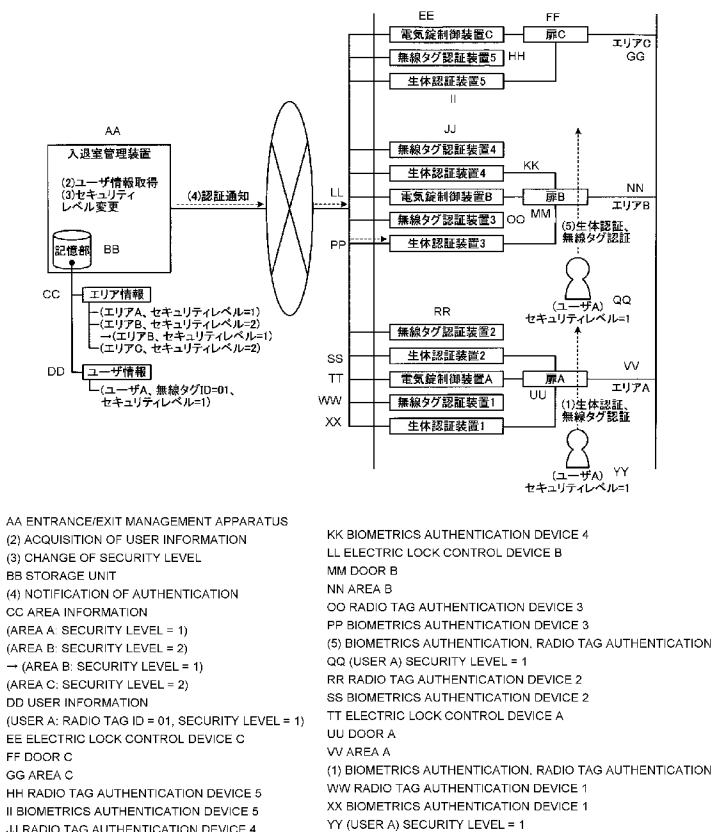
- (51) 国際特許分類:
G07C 9/00 (2006.01)
- (21) 国際出願番号: PCT/JP2007/059097
- (22) 国際出願日: 2007 年 4 月 26 日 (26.04.2007)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (71) 出願人 (米国を除く全ての指定国について): 富士通株式会社 (FUJITSU LIMITED) [JP/JP]; 〒2118588 神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号 Kanagawa (JP).
- (72) 発明者; および
- (75) 発明者/出願人 (米国についてのみ): 川喜田 聖 (KAWAKITA, Hijiri) [JP/JP]; 〒2118588 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 Kanagawa (JP).
- (74) 代理人: 酒井 宏明 (SAKAI, Hiroaki); 〒1006020 東京都千代田区霞が関三丁目 2 番 5 号 霞が関ビルディング 酒井国際特許事務所 Tokyo (JP).
- (81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.
- (84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY,

[続葉有]

(54) Title: ENTRANCE/EXIT MANAGEMENT PROGRAM, ENTRANCE/EXIT MANAGEMENT METHOD, AND ENTRANCE/EXIT MANAGEMENT APPARATUS

(54) 発明の名称: 入退室管理プログラム、入退室管理方法および入退室管理装置

[図 1]



AA ENTRANCE/EXIT MANAGEMENT APPARATUS

(2) ACQUISITION OF USER INFORMATION

(3) CHANGE OF SECURITY LEVEL

BB STORAGE UNIT

(4) NOTIFICATION OF AUTHENTICATION

CC AREA INFORMATION

(AREA A: SECURITY LEVEL = 1)

(AREA B: SECURITY LEVEL = 2)

(AREA C: SECURITY LEVEL = 2)

(AREA D: SECURITY LEVEL = 2)

DD USER INFORMATION

(USER A: RADIO TAG ID = 01, SECURITY LEVEL = 1)

EE ELECTRIC LOCK CONTROL DEVICE C

FF DOOR C

GG AREA C

HH RADIO TAG AUTHENTICATION DEVICE 5

II BIOMETRICS AUTHENTICATION DEVICE 5

JJ RADIO TAG AUTHENTICATION DEVICE 4

KK BIOMETRICS AUTHENTICATION DEVICE 4

LL ELECTRIC LOCK CONTROL DEVICE B

MM DOOR B

NN AREA B

OO RADIO TAG AUTHENTICATION DEVICE 3

PP BIOMETRICS AUTHENTICATION DEVICE 3

(5) BIOMETRICS AUTHENTICATION, RADIO TAG AUTHENTICATION

QQ (USER A) SECURITY LEVEL = 1

RR RADIO TAG AUTHENTICATION DEVICE 2

SS BIOMETRICS AUTHENTICATION DEVICE 2

TT ELECTRIC LOCK CONTROL DEVICE A

UU DOOR A

VV AREA A

(1) BIOMETRICS AUTHENTICATION, RADIO TAG AUTHENTICATION

WW RADIO TAG AUTHENTICATION DEVICE 1

XX BIOMETRICS AUTHENTICATION DEVICE 1

YY (USER A) SECURITY LEVEL = 1

(57) Abstract: An entrance/exit management apparatus includes an area information DB that stores information, such as "area A: security level = 1", "area B: security level = 2", and "area C: security level = 2", and a user information DB that stores information, such as "user A: radio tag ID = 01, security level = 1". The entrance/exit management apparatus changes the security level assigned to the area B from "2" to "1" in accordance with the security level of the user A who currently exists in the area B. When the user A moves to the area C from the area B having the changed security level, the entrance/exit management apparatus authenticates the user A on the basis of the radio tag and biological information as a plurality of authentication processes according to the difference in security level between those areas. When the user A moves from the area B to the area A, the entrance/exit management apparatus authenticates the user A on the basis of the radio tag as an authentication process according to the difference in security level between those areas.

(57) 要約: 入退室管理装置は、「エリア A、セキュリティレベル = 1」「エリア B、セキュリティレベル =

[続葉有]

2」 「エリア C、セキュリティレベル = 2」などと記憶するエ



KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:

— 国際調査報告書

リア情報DBと、「ユーザA、無線タグID=01、セキュリティレベル=1」などを記憶するユーザ情報DBを備える。そして、入退室管理装置は、エリアB内に現に存在するユーザAのセキュリティレベルに応じて、当該エリアBに割り与えられたセキュリティレベルを「2」から「1」に変更し、セキュリティレベルが変更されたエリアBからエリアCにユーザAが移動する際に、当該エリア間のセキュリティレベルの差に応じた複数種の認証として、無線タグによる認証と生体情報による認証をユーザAに対して実施する。また、入退室管理装置は、エリアBからエリアAにユーザAが移動する際には、当該エリア間のセキュリティレベルの差に応じた一種の認証として無線タグによる認証を実施する。

明 細 書

入退室管理プログラム、入退室管理方法および入退室管理装置 技術分野

[0001] この発明は、セキュリティレベルが割り当てられたエリアに対して利用者が入退室する際に、前記利用者の入退室を許可するか否かを複数種の認証によって判定する入退室管理プログラム、入退室管理方法および入退室管理装置に関する。

背景技術

[0002] 従来より、企業および個人の情報資産や財産を盗難から守るためのセキュリティ用途や危険エリアへの立入を制限する防災の目的で入退室管理システムが利用されている。そのため、人や物が通過する場所には、警備室や入退室認証装置、電気錠扉が至るところに用意されている。

[0003] そして、このような高いセキュリティ管理が実現されている入退室管理システムでは、オフィスや部屋を移動する都度、一連の認証手続きやセキュリティチェックを済ませてから入退室することになる。ところが、これらの施策を過剰に実施すると、そこで働く従業員の利便性を損ね、生産性を下げてしまったり、来訪者、来客に対して不快感を与えてしまったりする場合がある。

[0004] 一方で、利便性を重視した入退室管理システムの場合、警備員が目視でチェックするために、入退室で共連れを許可したりするなど、あいまい部分を残し、利用者の良識やモラルで対応することが多く、高いセキュリティ管理が実施されているとは言い難い。そこで、高いセキュリティ管理を保ちつつ、利便性や快適性を重視した様々な入退室管理システムが開示されている。

[0005] 例えば、特許文献1(特開平10-280752号公報)では、エリアのセキュリティレベルに応じてデータ入力を要求することで、高いセキュリティ管理を保ちつつ、利便性を重視した様々な入退室管理システムが開示されている。具体的には、セキュリティレベルの高いエリア(部屋)では、生体認証やIDカードによる認証などの認証手続きに加え、あらかじめ定めたパスワードによる認証を行い、セキュリティレベルの低いエリアでは、上記した認証手続きのみを実施するなど、エリアのセキュリティレベルに応

じてパスワード入力を求めたりすることで、高いセキュリティ管理を保ちつつ、利便性や快適性を重視している。

[0006] 特許文献1:特開平10-280752号公報

発明の開示

発明が解決しようとする課題

[0007] しかしながら、上記した従来の技術は、高いセキュリティ管理を保っているものの、入退室の手続きが煩雑であり、利便性や快適性を重視しているとは言い難いという課題があった。具体的には、セキュリティレベルが低いエリアから高いエリアへ移動したり、セキュリティレベルが高いエリアから低いエリアへ移動したりする場合などセキュリティレベルの高いエリアを介する移動においては、従来どおり、毎回煩雑な認証手続きを実施する必要がある、必ずしも利便性や快適性を重視しているとは言い難い。

[0008] そこで、この発明は、上述した従来技術の課題を解決するためになされたものであり、高いセキュリティ管理を保ちつつ、利便性や快適性を高めることが可能である入退室管理プログラム、入退室管理方法および入退室管理装置を提供することを目的とする。

課題を解決するための手段

[0009] 上述した課題を解決し、目的を達成するため、請求項1に係る発明は、セキュリティレベルが割り当てられたエリアに対して利用者が入退室する際に、前記利用者の入退室を許可するか否かを認証によって判定する入退室管理プログラムであって、予め割り当てられたセキュリティレベルが異なるエリア間を前記利用者が移動する際に、当該エリア間のセキュリティレベルの差に応じた適切な認証を前記利用者に対して実施する認証実施手順、をコンピュータに実行させることを特徴とする。

[0010] また、請求項2に係る発明は、上記の発明において、前記エリア内に現に存在する利用者のセキュリティレベルに応じて、当該エリアに割り与えられたセキュリティレベルを変更するエリアレベル変更手順をさらに備え、前記認証実施手順は、前記エリアレベル変更手順によってセキュリティレベルが変更されたエリア間を前記利用者が移動する際に、当該エリア間のセキュリティレベルの差に応じた複数種の認証を前記利用者に対して実施することをコンピュータに実行させることを特徴とする。

- [0011] また、請求項3に係る発明は、上記の発明において、前記認証実施手順は、前記エリアレベル変更手順によって変更されたセキュリティレベルが低いエリアから高いエリアへ前記利用者が移動する場合には、前記複数種の認証を実施し、セキュリティレベルが高いエリアから低いエリアへ移動する場合には、前記複数種の認証のいずれか一種を実施することを特徴とする。
- [0012] また、請求項4に係る発明は、上記の発明において、前記エリアレベル変更手順は、前記セキュリティレベルが割り与えられたエリア内に存在する利用者のセキュリティレベルが低い場合に、当該エリアに割り与えられたセキュリティレベルを低いセキュリティレベルに変更し、当該エリアから前記セキュリティレベルが低い利用者がいなくなった場合に、当該エリアのセキュリティレベルを元のセキュリティレベルに変更することを特徴とする。
- [0013] また、請求項5に係る発明は、前記認証実施手順は、前記エリアレベル変更手順によって同じセキュリティレベルに変更されたエリア間において、前記利用者が退室したエリアに所定の時間経過前に再度入室する場合に、前記利用者に対して前記一種の認証を実施し、前記利用者が退室したエリアに前記所定の時間経過後に再度入室する場合に、前記利用者に対して前記複数種の認証を実施することを特徴とする。
- [0014] また、請求項6に係る発明は、セキュリティレベルが割り当てられたエリアに対して利用者が入退室する際に、前記利用者の入退室を許可するか否かを認証によって判定することに適した入退室管理方法であって、予め割り当てられたセキュリティレベルが異なるエリア間を前記利用者が移動する際に、当該エリア間のセキュリティレベルの差に応じた適切な認証を前記利用者に対して実施する認証実施工程、を含んだことを特徴とする。
- [0015] また、請求項7に係る発明は、上記の発明において、前記エリア内に現に存在する利用者のセキュリティレベルに応じて、当該エリアに割り与えられたセキュリティレベルを変更するエリアレベル変更工程をさらに備え、前記認証実施工程は、前記エリアレベル変更手順によってセキュリティレベルが変更されたエリア間を前記利用者が移動する際に、当該エリア間のセキュリティレベルの差に応じた複数種の認証を前記利

用者に対して実施することを特徴とする。

[0016] また、請求項8に係る発明は、上記の発明において、前記認証実施工程は、前記エリアレベル変更工程によって変更されたセキュリティレベルが低いエリアから高いエリアへ前記利用者が移動する場合には、前記複数種の認証を実施し、セキュリティレベルが高いエリアから低いエリアへ移動する場合には、前記複数種の認証のいずれか一種を実施することを特徴とする。

[0017] また、請求項9に係る発明は、上記の発明において、前記エリアレベル変更工程は、前記セキュリティレベルが割り与えられたエリア内に存在する利用者のセキュリティレベルが低い場合に、当該エリアに割り与えられたセキュリティレベルを低いセキュリティレベルに変更し、当該エリアから前記セキュリティレベルが低い利用者がいなくなった場合に、当該エリアのセキュリティレベルを元のセキュリティレベルに変更することを特徴とする。

[0018] また、請求項10に係る発明は、上記の発明において、前記認証実施工程は、前記エリアレベル変更工程によって同じセキュリティレベルに変更されたエリア間において、前記利用者が退室したエリアに所定の時間経過前に再度入室する場合には、前記利用者に対して前記一種の認証を実施し、前記利用者が退室したエリアに前記所定の時間経過後に再度入室する場合には、前記利用者に対して前記複数種の認証を実施することを特徴とする。

[0019] また、請求項11に係る発明は、セキュリティレベルが割り当てられたエリアに対して利用者が入退室する際に、前記利用者の入退室を許可するか否かを認証によって判定する入退室管理装置であって、予め割り当てられたセキュリティレベルが異なるエリア間を前記利用者が移動する際に、当該エリア間のセキュリティレベルの差に応じた適切な認証を前記利用者に対して実施する認証実施手順、を備えたことを特徴とする。

発明の効果

[0020] 本発明によれば、予め割り当てられたセキュリティレベルが異なるエリア間を利用者が移動する際に、当該エリア間のセキュリティレベルの差に応じた適切な認証を利用者に対して実施するので、高いセキュリティ管理を保ちつつ、さらに利便性や快適性

を高めることが可能である。

[0021] また、本発明によれば、エリア内に現に存在する利用者のセキュリティレベルに応じて、当該エリアに割り与えられたセキュリティレベルを変更し、セキュリティレベルが変更されたエリア間を利用者が移動する際に、当該エリア間のセキュリティレベルの差に応じた複数種の認証を前記利用者に対して実施するので、さらに利便性や快適性を高めることが可能である。

[0022] さらに、出入り口だけでなくエリア毎にどこにだれがいるのか実態を把握できるので、不正な入退室が発生した場合の追跡や不足の事態が発生した場合の警備員や保安員の最適な配備にも活用することができる。

[0023] また、本発明によれば、変更されたセキュリティレベルが低いエリアから高いエリアへ利用者が移動する場合には、複数種の認証を実施し、セキュリティレベルが高いエリアから低いエリアへ移動する場合には、複数種の認証のいずれか一種を実施するので、より強固なセキュリティを実施することが可能であり、さらに利便性や快適性を高めることが可能である。

[0024] また、本発明によれば、セキュリティレベルが割り与えられたエリア内に存在する利用者のセキュリティレベルが低い場合に、当該エリアに割り与えられたセキュリティレベルを低いセキュリティレベルに変更し、当該エリアから前記セキュリティレベルが低い利用者がいなくなった場合に、当該エリアのセキュリティレベルを元のセキュリティレベルに変更するので、利用者のセキュリティレベルに応じて、エリアのセキュリティレベルを変更することができる結果、さらに利便性や快適性を高めることが可能である。

[0025] また、本発明によれば、同じセキュリティレベルに変更されたエリア間において、利用者が退室したエリアに所定の時間経過前に再度入室する場合に、利用者に対して一種の認証を実施し、利用者が退室したエリアに所定の時間経過後に再度入室する場合に、利用者に対して複数種の認証を実施するので、同じセキュリティレベルのエリア間を移動する利用者に対して、時間的制限を設けることができる結果、利便性や快適性を高めることが可能であるとともに、より強固なセキュリティを実施することが可能である。

図面の簡単な説明

- [0026] [図1]図1は、実施例1に係る入退室管理装置を含むシステムの全体構成を示すシステム構成図である。
- [図2]図2は、実施例1にかかる入退室管理装置の構成を示すブロック図である。
- [図3]図3は、扉情報DBに記憶される情報の例を示す図である。
- [図4]図4は、利用者DBに記憶される情報の例を示す図である。
- [図5]図5は、無線タグDBに記憶される情報の例を示す図である。
- [図6]図6は、利用者プレゼンスDBに記憶される情報の例を示す図である。
- [図7]図7は、利用者証跡DBに記憶される情報の例を示す図である。
- [図8]図8は、エリアプレゼンスDBに記憶される情報の例を示す図である。
- [図9]図9は、エリアレベル遷移DBに記憶される情報の例を示す図である。
- [図10]図10は、実施例1に係る入退室管理装置におけるセキュリティレベル変更処理の流れを示すフローチャートである。
- [図11]図11は、実施例1に係る入退室管理装置における認証処理の流れを示すフローチャートである。
- [図12]図12は、入退室管理プログラムを実行するコンピュータシステムの例を示す図である。

符号の説明

- [0027] 10 入退室管理装置
- 11 通信制御I/F部
- 12 記憶部
- 13 扉情報DB
- 14 利用者DB
- 15 無線タグDB
- 16 利用者プレゼンスDB
- 17 利用者証跡DB
- 18 エリアプレゼンスDB
- 19 エリアレベル遷移DB

- 20 制御部
- 21 無線タグ情報処理部
- 22 利用者情報処理部
- 23 セキュリティレベル変更部
- 24 認証実施部
- 100 コンピュータシステム
- 101 RAM
- 102 HDD
- 102a 扉情報テーブル
- 102b 利用者テーブル
- 102c 無線タグテーブル
- 102d 利用者プレゼンステーブル
- 102e 利用者証跡テーブル
- 102f エリアプレゼンステーブル
- 102g エリアレベル遷移テーブル
- 103 ROM
- 103a 無線タグ情報処理プログラム
- 103b 利用者情報処理プログラム
- 103c セキュリティレベル変更プログラム
- 103d 認証実施プログラム
- 104 CPU
- 104a 無線タグ情報処理プロセス
- 104b 利用者情報処理プロセス
- 104c セキュリティレベル変更プロセス
- 104d 認証実施プロセス

発明を実施するための最良の形態

[0028] 以下に添付図面を参照して、この発明に係る入退室管理装置、入退室管理方法および入退室管理プログラムの実施例を詳細に説明する。なお、以下では、本実施例

で用いる主要な用語、本実施例に係る入退室管理装置の概要および特徴、入退室管理装置の構成および処理の流れを順に説明し、最後に本実施例に対する種々の変形例を説明する。

実施例 1

[0029] [用語の説明]

はじめに、本実施例で用いる用語について説明する。本実施例で用いる「入退室管理装置(特許請求の範囲に記載の「入退室管理プログラム、入退室管理方法、入退室管理装置」に対応する)」とは、セキュリティレベルが割り当てられたエリア(部屋)に対して利用者(ユーザ)が入退室する際に、利用者の入退室を許可するか否かを認証によって判定する装置のことである。

[0030] 一般的に、セキュリティレベルが高いエリアへの入退室には、高度な(複雑な)認証が実施される。そのため、様々なエリアに高いセキュリティレベルを設定すると、全体として高いセキュリティ管理が実現できる。ところが、セキュリティレベルが高いエリアが多ければ、高度な認証手法を頻繁に実施する必要がある、ユーザの利便性が損なわれる。したがって、このような入退室管理装置では、ユーザの利便性を損なうことなく、高いセキュリティを実現することが望まれている。

[0031] なお、本実施例では、エリア間のセキュリティレベルの差に応じた適切な認証として複数種の認証(例えば、「無線タグによる認証」と「生体情報による生体認証」の二種類)を実施する場合について説明するが、本発明はこれに限定されるものではなく、例えば、「パスワードによる認証」を加えた三種類であってもよく、認証の種類や数を限定するものではない。さらに、ユーザを特定することができる身体的特徴(生体的特徴)や行動的特徴(癖)などの情報を用いて認証するようにしてもよい。また、本実施例では、便宜上、エリアをエリアA～エリアCとし、認証装置を生体認証装置1～5、無線タグ認証装置1～5とし、各エリアへの入退室を行う扉(ゲート)を扉A～Cとし、各扉の電気錠を制御する装置を電気錠制御装置A～Cとしているが、これは、数や名称を限定するものではない。

[0032] [入退室管理装置の概要および特徴]

次に、図1を用いて、実施例1に係る入退室管理装置の概要および特徴を説明す

る。図1は、実施例1に係る入退室管理装置を含むシステムの全体構成を示すシステム構成図である。

[0033] 図1に示すように、このシステムは、利用者の入退室に際して、利用者が正当な利用者であるか否かを認証するセキュリティレベルが割り与えられた各エリア間に設置された無線タグ認証装置と生体認証装置と、接続される扉を開錠するタッチパネルなどの表示操作部を備えた電気錠制御装置A～Cと、電気錠制御装置A～Cによって扉を開閉する扉A～Cと、入退室管理装置とがインターネットなどのネットワークを介して接続されている。

[0034] また、各エリア間に存在する扉A～Cには、扉を開錠する電気錠制御装置A～Cが設けられている。この電気錠制御装置A～Cは、生体認証装置1～5から開錠指示を受信すると、扉を開錠してユーザの通過を許可する。

[0035] また、無線タグ認証装置1～5は、ユーザによって所有される無線タグに記憶される無線タグIDを記憶し、無線タグが認識できる距離にある無線タグから自動的に無線タグIDを取得して、取得した無線タグIDを記憶している場合、当該認証を許可して許可した旨を入退室管理装置に通知する。同様に、生体認証装置1～5は、利用者の掌から静脈情報を取得し、取得した静脈情報を記憶している場合または入退室管理装置から「開錠通知」を受信した場合に、当該指示を接続される電気錠制御装置に送信する。

[0036] また、生体認証装置1～5は、入退室管理装置から「認証通知」を受信すると、生体認証を実施する。そして、生体認証装置1～5は、認証許可と判定すると、「開錠通知」を接続される電気錠制御装置に送信し、認証拒否と判定すると、「開錠拒否」を接続される電気錠制御装置に送信する。また、開錠指示を受信した電気錠制御装置は、扉を開錠する。ここでは、無線タグ認証装置1～5は、「無線タグID＝01」と記憶し、生体認証装置1～5は、「生体情報＝静脈情報A」を記憶する。

[0037] そして、この入退室管理装置は、接続される無線タグ装置と生体認証装置とが設置されている「エリア」に対応付けて、それぞれのエリアに割り与えられている「セキュリティレベル」をエリア情報として記憶する。具体的に例を挙げれば、入退室管理装置は、『エリアを示す「エリア名」、割り与えられたセキュリティレベルを示す「セキュリティ

レベル』』として「エリアA、セキュリティレベル＝1」、「エリアB、セキュリティレベル＝2」や「エリアC、セキュリティレベル＝2」などとエリア情報を記憶する。

[0038] また、この入退室管理装置は、セキュリティレベルを記憶する無線タグを所有する「ユーザ名」に対応付けて、所有される無線タグを一意に識別する「無線タグID」と、無線タグに記憶される「セキュリティレベル」とをユーザ情報として記憶する。具体的に例を挙げれば、入退室管理装置は、『無線タグを所有するユーザを示す「ユーザ名」、無線タグを一意に識別する「無線タグID」、無線タグに記憶されるセキュリティレベルを示す「セキュリティレベル』』として「ユーザA、ID＝01、セキュリティレベル＝1」などとユーザ情報に記憶する。

[0039] このような構成において、この入退室管理装置は、上記したように、セキュリティレベルが割り当てられたエリアに対して利用者が入退室する際に、利用者の入退室を許可するか否かを複数種の認証によって判定することを概要とするものであり、特に、高いセキュリティ管理を保ちつつ、利便性や快適性を高めることが可能である点に主たる特徴がある。

[0040] この主たる特徴を具体的に説明すると、この入退室管理装置は、エリアAからエリアBに入室したユーザに関する情報を取得する(図1の(1)と(2)参照)。上記した例で具体的に説明すると、ユーザAがエリアAからエリアBに入室するのに際しては、セキュリティレベルが1のエリアAからセキュリティレベルが2のエリアBへの入室であることより、無線タグ認証と生体認証とが実施される。つまり、無線タグ認証装置1は、ユーザAに所有される無線タグから無線タグID「01」を取得し、取得した無線タグIDを記憶している場合、当該認証を許可して許可した旨を入退室管理装置に通知する。同様に、生体認証装置1は、ユーザAの掌から静脈情報を取得し、取得した静脈情報を記憶している場合、または、入退室管理装置から「開錠通知」を受信した場合に、扉を開錠する指示を電気錠制御装置Aに通知する。そして、電気錠制御装置Aは、生体認証装置1から開錠指示を受信することで開錠し、ユーザAはエリアBに入室する。

[0041] ユーザAがエリアBに入室すると、無線タグ認証装置2は、ユーザAが所有する無線タグから無線タグID「01」を取得して、入退室管理装置に送信する。すると、入退室

管理装置は、無線タグ認証装置1から取得した無線タグID「01」に対応するユーザ名「ユーザA」とセキュリティレベル「1」をユーザ情報から取得するとともに、ユーザAが入室したエリアBのセキュリティレベル「2」をエリア情報から取得する。

[0042] そして、入退室管理装置は、エリア内に現に存在する利用者のセキュリティレベルに応じて、当該エリアに割り与えられたセキュリティレベルを変更する(図1の(3))参照)。上記した例で具体的に説明すると、入退室管理装置は、エリアB内に現に存在するユーザAのセキュリティレベルが「1」であり、エリアBのセキュリティレベルが「2」であることより、エリアBのセキュリティレベルを「1」に変更する。

[0043] そして、入退室管理装置は、セキュリティレベルが変更されたエリア間をユーザが移動する際に、当該エリア間のセキュリティレベルの差に応じた複数種の認証をユーザに対して実施する(図1の(4)と(5)参照)。上記した例で具体的に説明すると、入退室管理装置は、セキュリティレベルが「2」から「1」に変更されたエリアBからセキュリティレベルが「2」のエリアCにユーザAが移動する際に、無線タグによる認証と生体情報による認証の両方が許可である場合にのみ開錠するように、「認証通知」を生体認証装置3に通知する。なお、セキュリティレベルが「2」から「1」に変更されたエリアBからセキュリティレベルが「1」のエリアAにユーザAが移動する場合には、入退室管理装置は、ユーザAが扉Aから入室してきた際に無線タグ認証装置2によって、すでに認証が実施されているため、無線タグによる認証が認証許可である場合に開錠する「開錠通知」を生体認証装置2に対して通知する。

[0044] つまり、はじめは、エリアBとエリアCとは、ともにセキュリティレベルが「2」であることより、無線タグ認証のみで扉Cを通過することができ、同様に、エリアBとエリアAとは、セキュリティレベルが「2」と「1」であることより、無線タグ認証のみで扉Bを通過することができた。ところが、入退室管理装置は、エリアBにセキュリティレベル「1」のユーザAが存在しているため、エリアBのセキュリティレベルを「1」に下げる。すると、エリアBとエリアCとは、セキュリティレベルが「1」と「2」であることより、無線タグ認証と生体認証とが認証許可である場合にのみ扉Cを通過することができ、エリアBとエリアAとは、ともにセキュリティレベルが「1」であることより、無線タグ認証のみで扉Aを通過することができるようになる。

[0045] このように、実施例1に係る入退室管理装置は、エリアに現に存在するユーザのセキュリティレベルに応じて当該エリアのセキュリティレベルを動的に変化させることができる結果、上記した主たる特徴のごとく、高いセキュリティ管理を保ちつつ、利便性や快適性を高めることが可能である。

[0046] [入退室管理装置の構成]

次に、図2を用いて、図1に示した入退室管理装置の構成を説明する。図2は、実施例1にかかる入退室管理装置の構成を示すブロック図である。図2に示すように、この入退室管理装置10は、通信制御I/F部11と、記憶部12と、制御部20とから構成される。

[0047] 通信制御I/F部11は、電気錠制御装置A～C、無線タグ認証装置1～5、生体認証装置1～5との間でそれぞれやり取りする各種情報に関する通信を制御する。具体的に例を挙げれば、通信制御I/F部11は、後述する制御部20から出力される開錠通知や認証通知を生体認証装置1～5に送信したり、無線タグ認証装置1～5から送信される無線タグIDや認証結果を受信して制御部20に出力したりする。

[0048] 記憶部12は、制御部20による各種処理に必要なデータおよびプログラムを格納するとともに、特に本発明に密接に関連するものとしては、扉情報DB13と、利用者DB14と、無線タグDB15と、利用者プレゼンスDB16と、利用者証跡DB17と、エリアプレゼンスDB18と、エリアレベル遷移DB19とを備える。

[0049] 扉情報DB13は、エリア間に設置される扉に関する情報を記憶する。具体的に例を挙げれば、図3に示すように、扉情報DB13は、対象となる扉を示す「扉名」に対応付けて、「生体認証情報」、「エリア情報」、「開閉制御情報」を記憶して、例えば、「扉A、静脈情報、エリアA、エリアB、12:00開、12:01閉」などと記憶する。

[0050] 「生体認証情報」とは、「扉名」に記憶される扉において使用する生体情報の種類を示しており、例えば、静脈情報、指紋、虹彩、声紋などである。また、エリア情報とは、「扉名」に記憶される扉により遮断されている隣接したエリア名を示しており、「開閉制御情報」とは、「扉名」に記憶される扉の開閉状況を記録したログ情報である。なお、図3は、扉情報DBに記憶される情報の例を示す図である。

[0051] 利用者DB14は、無線タグを所有するユーザに関する情報を記憶する。具体的に

例を挙げれば、図4に示すように、利用者DB14は、ユーザに一意に割与えられた「個人ID」に対応付けて、「氏名」、「生体認証データ」、「無線タグID」、「有効期限」、「入退室可能エリア」を記憶して、例えば、「001、特許太郎、静脈情報A、01、2009年3月31日、ALL」や「002、特許花子、静脈情報B、02、2008年12月31日、セキュリティレベル2」などと記憶する。

[0052] 「氏名」とは、ユーザ名の氏名を示しており、「生体認証データ」は、使用される登録された生体情報の種類を示しており、「無線タグID」は、ユーザに所有される無線タグを一意に識別する識別子を示しており、「有効期限」は、当該無線タグの有効期限を示しており、「入退室可能エリア」は、ユーザが入退室できるセキュリティレベルを示している。この「入退室可能エリア」に「ALL」と記憶されていれば、全てのセキュリティレベルのエリアに入退室可能であり、「セキュリティレベル2」と記憶されていれば、セキュリティレベルが「2」以下のエリアに入退室可能であることを示している。なお、図4は、利用者DBに記憶される情報の例を示す図である。

[0053] 無線タグDB15は、無線タグ認証装置により検出されたユーザにより所有される無線タグに関する情報を記憶する。具体的に例を挙げれば、図5に示すように、無線タグDB15は、無線タグ認証装置により検出された「無線タグID」に対応付けて、当該無線タグIDを検出した無線タグ認証装置を示す「無線タグ認証装置情報」と、検出された無線タグが存在する「エリア情報」とを記憶し、例えば、「01、無線タグ認証装置2、エリアB」などと記憶する。この例では、無線タグID「01」がエリアBの無線タグ認証装置2に検出されたことを示している。なお、図5は、無線タグDBに記憶される情報の例を示す図である。

[0054] 利用者プレゼンスDB16は、利用者がどのエリアに存在するかを記憶する。具体的に例を挙げれば、図6に示すように、利用者プレゼンスDB16は、ユーザの氏名を示す「ユーザ情報」に対応付けて、「在室エリア情報」、「継続性」、「利用者のセキュリティレベル」を記憶し、例えば、「特許太郎(001)、エリアA、継続中、セキュリティレベル1」や「特許太郎(001)、エリアB、なし、セキュリティレベル1」などと記憶する。また、「ユーザ情報」には、ユーザの「氏名」と「個人ID」が記憶される。

[0055] 「在室エリア情報」とは、「ユーザ情報」に記憶されるユーザがどのエリアに存在する

かを示し、「継続性」は、「ユーザ情報」に記憶されるユーザの認証が継続中であるか否かを示し、「利用者のセキュリティレベル」は、「ユーザ情報」に記憶されるユーザによって所有される無線タグに記憶されるセキュリティレベルを示している。なお、図6は、利用者プレゼンスDBに記憶される情報の例を示す図である。

[0056] 利用者証跡DB17は、ユーザがエリアに入退室した証跡を記憶する。具体的に例を挙げれば、図7に示すように、利用者証跡DB17は、ユーザの氏名を示す「ユーザ情報」に対応付けて、「日時」、「扉情報」、「認証装置情報」、「エリア情報」、「認証結果」を記憶し、例えば、「特許太郎(001)、2007年4月1日、扉A、生体認証装置1、エリアA、許可」や「特許花子(002)、2006年12月1日、扉B、生体認証装置3、エリアB、拒否」などと記憶する。また、「ユーザ情報」には、ユーザの「氏名」と「個人ID」が記憶される。

[0057] 「日時」は、認証が行われた日時を示しており、「扉情報」は、ユーザが通過を希望した認証対象の扉を示しており、「認証装置情報」は、認証を実施した認証装置を示しており、「エリア情報」は、認証が実施された際にユーザが存在したエリアを示しており、「認証結果」は、当該認証が許可されたか拒否されたかを示している。なお、図7は、利用者証跡DBに記憶される情報の例を示す図である。

[0058] エリアプレゼンスDB18は、エリアにおける利用者のプレゼンス(存在)状況を記憶する。具体的に例を挙げれば、図8に示すように、エリアプレゼンスDB18は、エリアを示す「在室エリア情報」に対応付けて、「継続性」、「利用者のセキュリティレベル」、「エリアのセキュリティレベル」を記憶し、例えば、「エリアA、継続中、セキュリティレベル1、セキュリティレベル1」などと記憶する。

[0059] 「継続性」は、「在室エリア情報」に記憶されるエリアにおいて当該ユーザの認証が継続中であるか否かを示し、「利用者のセキュリティレベル」は、「在室エリア情報」に存在するユーザの中で最も低いセキュリティレベルを示し、「エリアのセキュリティレベル」は、「在室エリア情報」に記憶されるエリアに割り与えられたセキュリティレベルを記憶する。なお、図8は、エリアプレゼンスDBに記憶される情報の例を示す図である。

[0060] エリアレベル遷移DB19は、エリアに割り与えられているセキュリティレベルの遷移

状況(変更状況)を記憶する。具体的に例を挙げれば、図9に示すように、エリアレベル遷移DB19は、セキュリティレベルが遷移した「日時」に対応付けて、「エリア」、「在室者」、「エリアセキュリティレベル」を記憶し、例えば、「2007年4月1日、エリアA、特許太郎(001)、セキュリティレベル1」などと記憶する。

[0061] 「エリア」は、セキュリティレベルが変更された(遷移した)エリアを示しており、「在室者」は、セキュリティレベルが変更された際に当該エリアに在室したユーザを示しており、「エリアセキュリティレベル」は、エリアに割り与えられたセキュリティレベル変更後(遷移後)のセキュリティレベルを示している。なお、図9は、エリアレベル遷移DBに記憶される情報の例を示す図である。

[0062] 制御部20は、OS(Operating System)などの制御プログラム、各種の処理手順などを規定したプログラムおよび所要データを格納するための内部メモリを有するとともに、特に本発明に密接に関連するものとしては、無線タグ情報処理部21と、利用者情報処理部22と、セキュリティレベル変更部23と、認証実施部24とを備え、これらによって種々の処理を実行する。

[0063] 無線タグ情報処理部21は、利用者が所有する無線タグから無線タグIDを取得する。上記した例で具体的に説明すると、無線タグ情報処理部21は、ユーザ(特許太郎)が所有する無線タグから無線タグID(01)を取得した無線タグ認証装置2から無線タグID(01)を取得する。すると、無線タグ情報処理部21は、取得した無線タグID(01)に対応付けて、当該無線タグIDを取得した無線タグ認証装置2と、当該無線タグIDが取得されたエリアBとを、無線タグDB15に格納する。

[0064] 利用者情報処理部22は、生体認証装置により実行された認証結果に応じて、利用者のプレゼンス情報や証跡、エリアプレゼンスを格納する。上記した例で具体的に説明すると、生体認証装置1によって認証が許可(または拒否)された旨の信号を受信すると、利用者情報処理部22は、無線タグ情報処理部21によって取得された無線タグID(01)に対応するユーザ(特許太郎(001))や利用者に所有される無線タグIDに記憶されるセキュリティレベル、無線タグの有効期限などを利用者DB14から特定する。

[0065] そして、利用者情報処理部22は、取得された無線タグID(01)を所有するユーザ

がエリアAからエリアBに入室したため、現地点でユーザが存在するエリア情報として「エリアB」と、取得された無線タグID(01)に記憶される「セキュリティレベル」と、認証の「継続性」とを、取得された「無線タグID=01」に対応付けて利用者プレゼンスDB16に記憶する。ここで、エリアBに入室したユーザ(特許太郎)のセキュリティレベルが「1」であり、入室したエリアBのセキュリティレベルが「2」であることより、「継続性」は「なし」と記憶される。一方、入室したユーザのセキュリティレベルと入室したエリアのセキュリティレベルとが一致する場合やエリアのセキュリティレベルが低い場合、「継続性」は「継続中」と記憶される。

[0066] また、生体認証装置1によって認証が許可されると、ユーザがエリアAからエリアBに入室したことになるため、利用者情報処理部22は、生体認証装置1から認証許可の信号を受信した「日時」に対応付けて、「認証装置情報=生体認証装置1」、「エリア情報=エリアA」、「認証結果=許可」を利用者証跡DB17に格納する。また、利用者情報処理部22は、利用者プレゼンスDB16と利用者証跡DB17とから、「在室エリア情報=エリアB」、「継続性=なし」、「利用者のセキュリティレベル=1」、「エリアのセキュリティレベル=2」を取得してエリアプレゼンスDB18に格納する。

[0067] セキュリティレベル変更部23は、エリア内に現に存在する利用者のセキュリティレベルに応じて、当該エリアに割り与えられたセキュリティレベルを変更する。上記した例で具体的に説明すると、セキュリティレベル変更部23は、エリアプレゼンスDB18が更新されると、エリアプレゼンスDB18に記憶される「利用者のセキュリティレベル=1」、「エリアのセキュリティレベル=2」を取得する。そして、「利用者のセキュリティレベル=1」が「エリアのセキュリティレベル=2」より小さいので、セキュリティレベル変更部23は、「利用者のセキュリティレベル=1」が存在する「エリアBのセキュリティレベル」を「1」に変更する。そして、セキュリティレベル変更部23は、変更した情報をエリアレベル遷移DB19に格納する。なお、セキュリティレベル変更部23は、請求の範囲に記載の「エリアレベル変更手順」に対応する。

[0068] 認証実施部24は、セキュリティレベル変更部23によってセキュリティレベルが変更されたエリア間を利用者が移動する際に、当該エリア間のセキュリティレベルの差に応じた複数種の認証を利用者に対して実施する。上記した例で具体的に説明すると

、認証実施部24は、セキュリティレベルが「2」から「1」に変更されたエリアBからセキュリティレベルが「2」のエリアCにユーザ(特許太郎)が移動する際に、無線タグによる認証と生体情報による認証との両方が許可である場合にのみ開錠するように、「認証通知」を生体認証装置3に送信する。また、認証実施部24は、セキュリティレベルが「2」から「1」に変更されたエリアBからセキュリティレベルが「1」のエリアAにユーザが移動する際には、無線タグによる認証が認証許可である場合に開錠する「開錠通知」を生体認証装置2に通知する。なお、認証実施部24は、請求の範囲に記載の「認証実施手順」に対応する。

[0069] [入退室管理装置による処理]

次に、図10と図11とを用いて、入退室管理装置による処理を説明する。図10は、実施例1に係る入退室管理装置におけるセキュリティレベル変更処理の流れを示すフローチャートであり、図11は、実施例1に係る入退室管理装置における認証処理の流れを示すフローチャートである。

[0070] (セキュリティレベル変更処理の流れ)

図10に示すように、ユーザがエリアに入室すると(ステップS1001肯定)、入退室管理装置10の無線タグ情報処理部21は、ユーザによって所有される無線タグに関する無線タグ情報を格納する(ステップS1002)。

[0071] 具体的には、生体認証装置1により認証が許可されて、ユーザ(特許太郎)がエリアAからエリアBに入室すると、無線タグ認証装置2は、当該ユーザが所有する無線タグから無線タグID「01」を取得して入退室管理装置10に送信する。すると、入退室管理装置10の無線タグ情報処理部21は、無線タグ認証装置2から受信した無線タグID(01)に対応付けて、当該無線タグIDを取得した無線タグ認証装置と、当該無線タグIDが取得されたエリア情報とを無線タグDB15に格納する。

[0072] 続いて、入退室管理装置10は、無線タグ認証装置2から受信した無線タグID(01)に対応する利用者の証跡、利用者プレゼンス情報、エリアプレゼンス情報をそれぞれ利用者証跡DB17、利用者プレゼンスDB16、エリアプレゼンスDB18に格納する(ステップS1003～ステップS1005)。

[0073] 具体的には、入退室管理装置10の利用者情報処理部22は、無線タグ情報処理

部21によって取得された無線タグID(01)に対応するユーザ(特許太郎(001))や利用者に所有される無線タグIDに記憶されるセキュリティレベル、無線タグの有効期限などを利用者DB14から特定する。そして、利用者情報処理部22は、取得された無線タグID(01)に対応付けて、ユーザが入室した「エリアB」と、無線タグID(01)に記憶される「セキュリティレベル=1」と、「認証の継続性=なし」とを利用者プレゼンスDB16に格納する。続いて、利用者情報処理部22は、生体認証装置1から認証許可の信号を受信した「日時」に対応付けて、「認証装置情報=生体認証装置1」、「エリア情報=エリアA」、「認証結果=許可」を利用者証跡DB17に格納するとともに、「入室エリア情報=エリアB」、「継続性=なし」、「利用者のセキュリティレベル=1」、「エリアのセキュリティレベル=2」を取得してエリアプレゼンスDB18に格納する。

[0074] そして、入退室管理装置10は、「エリアのセキュリティレベル」が「利用者のセキュリティレベル」より大きい場合に(ステップS1006肯定)、当該エリアのセキュリティレベルを下げて(ステップS1007)、その結果をエリアレベル遷移DB19に格納する(ステップS1008)。

[0075] 具体的には、入退室管理装置10のセキュリティレベル変更部23は、エリアBの「エリアのセキュリティレベル=2」が「利用者のセキュリティレベル=1」より大きいので、エリアの「セキュリティレベル」を「2」から「1」に変更し、その結果をエリアレベル遷移DB19に格納する。

[0076] (認証処理の流れ)

図11に示すように、無線タグが検出されると(ステップS1101肯定)、入退室管理装置10は、無線タグによる認証が許可されたか否かを無線タグ認証装置から受け付ける(ステップS1002)。

[0077] 具体的には、ユーザがエリアBに入室すると、無線タグ認証装置2は、当該ユーザが所有する無線タグID「01」を取得する。そして、無線タグ認証装置2は、取得した無線タグID「01」を記憶していることより、認証許可の通知を入退室管理装置10に送信する。

[0078] そして、認証が許可された場合に(ステップS1102肯定)、入退室管理装置10の認証実施部24は、無線タグ認証装置から受信した無線タグIDに対応する認証の「継

続性」が「継続中」であるか否かを判定する(ステップS1003)。

[0079] 具体的には、認証実施部24は、無線タグ認証装置2から受信した無線タグID「01」に対応する認証の「継続性」が「継続中」であるか否かを、利用者プレゼンスDB16またはエリアプレゼンスDB18を参照して判定する。

[0080] そして、「継続性」が「継続中」である場合(ステップS1103肯定)、認証実施部24は、扉を開錠するために「開錠通知」を生体認証装置に通知する(ステップS1104)。

[0081] 一方、「継続性」が「なし」である場合(ステップS1103否定)、認証実施部24は、「認証通知」を生体認証装置に送信し、生体認証装置によって生体認証が実施されて許可された場合に、扉が開錠される(ステップS1105とステップS1106)。

[0082] [実施例1による効果]

このように、実施例1によれば、エリアB内に現に存在する利用者のセキュリティレベル「1」に応じて、当該エリアBに割り与えられたセキュリティレベルを「2」から「1」に変更し、セキュリティレベルが変更されたエリアBからエリアCへユーザが移動する際に、当該エリア間のセキュリティレベルの差に応じた生体認証と無線タグ認証とをユーザに対して実施するので、高いセキュリティ管理を保ちつつ、利便性や快適性を高めることが可能である。さらには、セキュリティ管理における堅牢性を向上させることが可能である。

[0083] また、利用者プレゼンスやエリアプレゼンスなどを記憶する結果、出入り口だけでなくエリア毎にどこにだれがいるのか実態を把握できるので、不正な入退室が発生した場合の追跡や不足の事態が発生した場合の警備員や保安員の最適な配備にも活用することができる。

[0084] また、実施例1によれば、変更されたセキュリティレベルが低いエリアBから高いエリアCへユーザが移動する場合には、生体認証と無線タグ認証を実施し、セキュリティレベルが高いエリアCから低いエリアBへ移動する場合には、無線タグ認証のみを実施するので、より強固なセキュリティを実施することが可能であり、さらに利便性や快適性を高めることが可能である。

[0085] また、実施例1によれば、セキュリティレベルが割り与えられたエリアB内に存在するユーザ(特許太郎)のセキュリティレベルが低い場合に、当該エリアBに割り与えられ

たセキュリティレベル「2」を低いセキュリティレベル「1」に変更するので、利用者のセキュリティレベルに応じて、エリアのセキュリティレベルを変更することができる結果、さらに利便性や快適性を高めることが可能である。

実施例 2

[0086] さて、これまで本発明の実施例について説明したが、本発明は上述した実施例以外にも、種々の異なる形態にて実施されてよいものである。そこで、以下に示すように、(1)セキュリティレベルの変更手法、(2)時間的制限、(3)複数サーバによる管理、(4)システム構成等、(5)プログラムにそれぞれ区分けして異なる実施例を説明する。

[0087] (1)セキュリティレベルの変更手法

例えば、本発明では、エリアのセキュリティレベルより当該エリアに現に在室するユーザのセキュリティレベルが小さい場合に、エリアのセキュリティレベルを小さくするだけでなく、当該エリアから当該ユーザがいなくなれば、当該エリアのセキュリティレベルを元のセキュリティレベルに戻すようにしてもよい。そうすることで、利用者のセキュリティレベルに応じて、エリアのセキュリティレベルを動的に変更することができる結果、さらに利便性や快適性を高めることが可能である。

[0088] また、エリアのセキュリティレベルを下げる条件としては、実施例で説明したユーザのセキュリティレベル以外に、なりすましや共連れによる不正な無線タグを検出した場合、顧客や外部の利用者と共有する会議室や食堂などのエリアで、これらの外部の人を検知した場合、火災や地震で認証なしでドア開閉ができる不測の事態が発生した場合などが考えられる。

[0089] また、セキュリティレベルは下げるだけでなく、上げるようにしてもよい。例えば、顧客や外部の利用者と共有する会議室や食堂などのエリアで、就業時間外や休日などでこれらの外部の人の在室(無線タグ)を検出しない場合や、エリアの在室者の全員が当該エリアのセキュリティレベルより高いセキュリティレベルであり、継続性も継続中(保証されている)場合に、エリアのセキュリティレベルを上げるようにしてもよい。

[0090] また、本実施例では、エリア間のセキュリティレベルの差に応じた適切な認証として複数種の認証(例えば、「無線タグによる認証」と「生体情報による生体認証」)の二種

類)を実施する場合について説明するが、本発明はこれに限定されるものではなく、例えば、「パスワードによる認証」を加えた三種類であってもよく、認証の種類や数を限定するものではない。

[0091] (2) 時間的制限

また、本発明では、エリアAからエリアBに移動して、エリアBからエリアAに戻るなど同じセキュリティレベルのエリアに移動して元のエリアに戻る場合は、一定時間経過前(例えば、30分以内など)であれば、簡単な一種の認証で元の部屋に戻ることができ、一定時間経過後であれば、複雑な複数の認証を実施するようにしてもよい。そうすることで、同じセキュリティレベルのエリア間を移動する利用者に対して、時間的制限を設けることができる結果、利便性や快適性を高めることが可能であるとともに、より強固なセキュリティを実施することが可能である。

[0092] 例えば、エリアA(レベル2)からエリアB(レベル2)に移動して、エリアB(レベル2)からエリアA(レベル2)に戻るなど同じセキュリティレベルのエリアに移動して元のエリアに戻る場合は、通常、簡単な一種の認証で移動することができるが、あまりに移動に時間がかかることは不振な行動とみなすことができる。そのため、同じセキュリティレベルのエリアに移動して元のエリアに戻る場合は、一定時間経過前(例えば、30分以内など)であれば、簡単な一種の認証で元の部屋に戻ることができ、一定時間経過後であれば、複雑な複数の認証を実施するようにする。その結果、より強固なセキュリティを実施することが可能である。

[0093] (3) 複数サーバによる管理

また、実施例1では、入退室管理装置は、扉情報、無線タグ情報、利用者情報、利用者プレゼンス情報、利用者証跡、エリアプレゼンス情報、エリアレベル遷移情報など様々な情報を記憶、管理する場合について説明したが、本発明はこれに限定されるものではなく、複数のサーバによって管理するようにしてもよい。

[0094] 例えば、入退室管理システムとして、利用者情報と扉情報とを管理する入退室管理サーバ、無線タグ情報を管理する無線タグ管理サーバ、利用者プレゼンス情報と利用者証跡とエリアプレゼンス情報とエリアレベル遷移情報とを管理するプレゼンス管理サーバなどと管理サーバを分けて構成するようにしてもよい。

[0095] (4)システム構成等

また、本実施例において説明した各処理のうち、自動的におこなわれるものとして説明した処理(例えば、無線タグ検出処理など)の全部または一部を手動的におこなうこともできる。この他、上記文書中や図面中で示した処理手順、制御手順、具体的名称、各種のデータやパラメータを含む情報(例えば、図3～図9など)については、特記する場合を除いて任意に変更することができる。

[0096] また、図示した各装置の各構成要素は機能概念的なものであり、必ずしも物理的に図示の如く構成されていることを要しない。すなわち、各装置の分散・統合の具体的な形態は図示のものに限られず、その全部または一部を、各種の負荷や使用状況などに応じて、任意の単位で機能的または物理的に分散・統合(例えば、無線タグ情報処理部と利用者情報処理部とを統合するなど)して構成することができる。さらに、各装置にて行なわれる各処理機能は、その全部または任意の一部が、CPUおよび当該CPUにて解析実行されるプログラムにて実現され、あるいは、ワイヤードロジックによるハードウェアとして実現され得る。

[0097] (5)プログラム

ところで、上記の実施例で説明した各種の処理は、あらかじめ用意されたプログラムをパーソナルコンピュータやワークステーションなどのコンピュータシステムで実行することによって実現することができる。そこで、以下では、上記の実施例と同様の機能を有するプログラムを実行するコンピュータシステムを他の実施例として説明する。

[0098] 図12は、入退室管理プログラムを実行するコンピュータシステムの例を示す図である。図12に示すように、コンピュータシステム100は、RAM101と、HDD102と、ROM103と、CPU104とから構成される。ここで、ROM103には、上記の実施例と同様の機能を発揮するプログラム、つまり、図12に示すように、無線タグ情報処理プログラム103aと、利用者情報処理プログラム103bと、セキュリティレベル変更プログラム103cと、認証実施プログラム103dとがあらかじめ記憶されている。

[0099] そして、CPU104には、これらのプログラム103a～103dを読み出して実行することで、図12に示すように、無線タグ情報処理プロセス104aと、利用者情報処理プロセス104bと、セキュリティレベル変更プロセス104cと、認証実施プロセス104dとなる

。なお、無線タグ情報処理プロセス104aは、図2に示した、無線タグ情報処理部21に対応し、同様に、利用者情報処理プロセス104bは、利用者情報処理部22に対応し、セキュリティレベル変更プロセス104cは、セキュリティレベル変更部23に対応し、認証実施プロセス104dは、認証実施部24に対応する。

[0100] また、HDD102には、エリア間に設置される扉に関する情報を記憶する扉情報テーブル102aと、無線タグを所有するユーザに関する情報を記憶する利用者テーブル102bと、無線タグ認証装置により検出されたユーザにより所有される無線タグに関する情報を記憶する無線タグテーブル102cと、利用者がどのエリアに存在するかを記憶する利用者プレゼンステーブル102dと、ユーザがエリアに入退室した証跡を記憶する利用者証跡テーブル102eと、エリアにおける利用者のプレゼンス(存在)状況を記憶するエリアプレゼンステーブル102fと、エリアに割り与えられているセキュリティレベルの遷移状況(変更状況)を記憶するエリアレベル遷移テーブル102gと設けられる。

[0101] なお、扉情報テーブル102aは、図2に示した、扉情報DB13に対応し、同様に、利用者テーブル102bは、利用者DB14に対応し、無線タグテーブル102cは、無線タグDB15に対応し、利用者プレゼンステーブル102dは、利用者プレゼンスDB16に対応し、利用者証跡テーブル102eは、利用者証跡DB17に対応し、エリアプレゼンステーブル102fは、エリアプレゼンスDB18に対応し、エリアレベル遷移テーブル102gは、エリアレベル遷移DB19に対応する。

[0102] ところで、上記したプログラム103a～103dは、必ずしもROM103に記憶させておく必要はなく、例えば、コンピュータシステム100に挿入されるフレキシブルディスク(FD)、CD-ROM、MOディスク、DVDディスク、光磁気ディスク、ICカードなどの「可搬用の物理媒体」の他に、コンピュータシステム100の内外に備えられるハードディスクドライブ(HDD)などの「固定用の物理媒体」、さらに、公衆回線、インターネット、LAN、WANなどを介してコンピュータシステム100に接続される「他のコンピュータシステム」に記憶させておき、コンピュータシステム100がこれらからプログラムを読み出して実行するようにしてもよい。

産業上の利用可能性

[0103] 以上のように、本発明に係る入退室管理プログラム、入退室管理方法および入退室管理装置は、セキュリティレベルが割り当てられたエリアに対して利用者が入退室する際に、前記利用者の入退室を許可するか否かを複数種の認証によって判定することに有用であり、特に、高いセキュリティ管理を保ちつつ、利便性や快適性を高めることに適する。

請求の範囲

- [1] セキュリティレベルが割り当てられたエリアに対して利用者が入退室する際に、前記利用者の入退室を許可するか否かを認証によって判定する入退室管理プログラムであって、
- 予め割り当てられたセキュリティレベルが異なるエリア間を前記利用者が移動する際に、当該エリア間のセキュリティレベルの差に応じた適切な認証を前記利用者に対して実施する認証実施手順、
- をコンピュータに実行させることを特徴とする入退室管理プログラム。
- [2] 前記エリア内に現に存在する利用者のセキュリティレベルに応じて、当該エリアに割り与えられたセキュリティレベルを変更するエリアレベル変更手順をさらに備え、
- 前記認証実施手順は、前記エリアレベル変更手順によってセキュリティレベルが変更されたエリア間を前記利用者が移動する際に、当該エリア間のセキュリティレベルの差に応じた複数種の認証を前記利用者に対して実施することをコンピュータに実行させることを特徴とする請求項1に記載の入退室管理プログラム。
- [3] 前記認証実施手順は、前記エリアレベル変更手順によって変更されたセキュリティレベルが低いエリアから高いエリアへ前記利用者が移動する場合には、前記複数種の認証を実施し、セキュリティレベルが高いエリアから低いエリアへ移動する場合には、前記複数種の認証のいずれか一種を実施することをコンピュータに実行させることを特徴とする請求項2に記載の入退室管理プログラム。
- [4] 前記エリアレベル変更手順は、前記セキュリティレベルが割り与えられたエリア内に存在する利用者のセキュリティレベルが低い場合に、当該エリアに割り与えられたセキュリティレベルを低いセキュリティレベルに変更し、当該エリアから前記セキュリティレベルが低い利用者がいなくなった場合に、当該エリアのセキュリティレベルを元のセキュリティレベルに変更することをコンピュータに実行させることを特徴とする請求項2に記載の入退室管理プログラム。
- [5] 前記認証実施手順は、前記エリアレベル変更手順によって同じセキュリティレベルに変更されたエリア間において、前記利用者が退室したエリアに所定の時間経過前に再度入室する場合に、前記利用者に対して前記一種の認証を実施し、前記利用

者が退室したエリアに前記所定の時間経過後に再度入室する場合に、前記利用者に対して前記複数種の認証を実施することをコンピュータに実行させることを特徴とする請求項1～4のいずれか一つに記載の入退室管理プログラム。

- [6] セキュリティレベルが割り当てられたエリアに対して利用者が入退室する際に、前記利用者の入退室を許可するか否かを認証によって判定することに適した入退室管理方法であって、

予め割り当てられたセキュリティレベルが異なるエリア間を前記利用者が移動する際に、当該エリア間のセキュリティレベルの差に応じた適切な認証を前記利用者に対して実施する認証実施工程、

を含んだことを特徴とする入退室管理方法。

- [7] 前記エリア内に現に存在する利用者のセキュリティレベルに応じて、当該エリアに割り与えられたセキュリティレベルを変更するエリアレベル変更工程をさらに備え、

前記認証実施工程は、前記エリアレベル変更手順によってセキュリティレベルが変更されたエリア間を前記利用者が移動する際に、当該エリア間のセキュリティレベルの差に応じた複数種の認証を前記利用者に対して実施することを特徴とする請求項6に記載の入退室管理方法。

- [8] 前記認証実施工程は、前記エリアレベル変更工程によって変更されたセキュリティレベルが低いエリアから高いエリアへ前記利用者が移動する場合には、前記複数種の認証を実施し、セキュリティレベルが高いエリアから低いエリアへ移動する場合には、前記複数種の認証のいずれか一種を実施することを特徴とする請求項7に記載の入退室管理方法。

- [9] 前記エリアレベル変更工程は、前記セキュリティレベルが割り与えられたエリア内に存在する利用者のセキュリティレベルが低い場合に、当該エリアに割り与えられたセキュリティレベルを低いセキュリティレベルに変更し、当該エリアから前記セキュリティレベルが低い利用者がいなくなった場合に、当該エリアのセキュリティレベルを元のセキュリティレベルに変更することを特徴とする請求項6に記載の入退室管理方法。

- [10] 前記認証実施工程は、前記エリアレベル変更工程によって同じセキュリティレベルに変更されたエリア間において、前記利用者が退室したエリアに所定の時間経過前

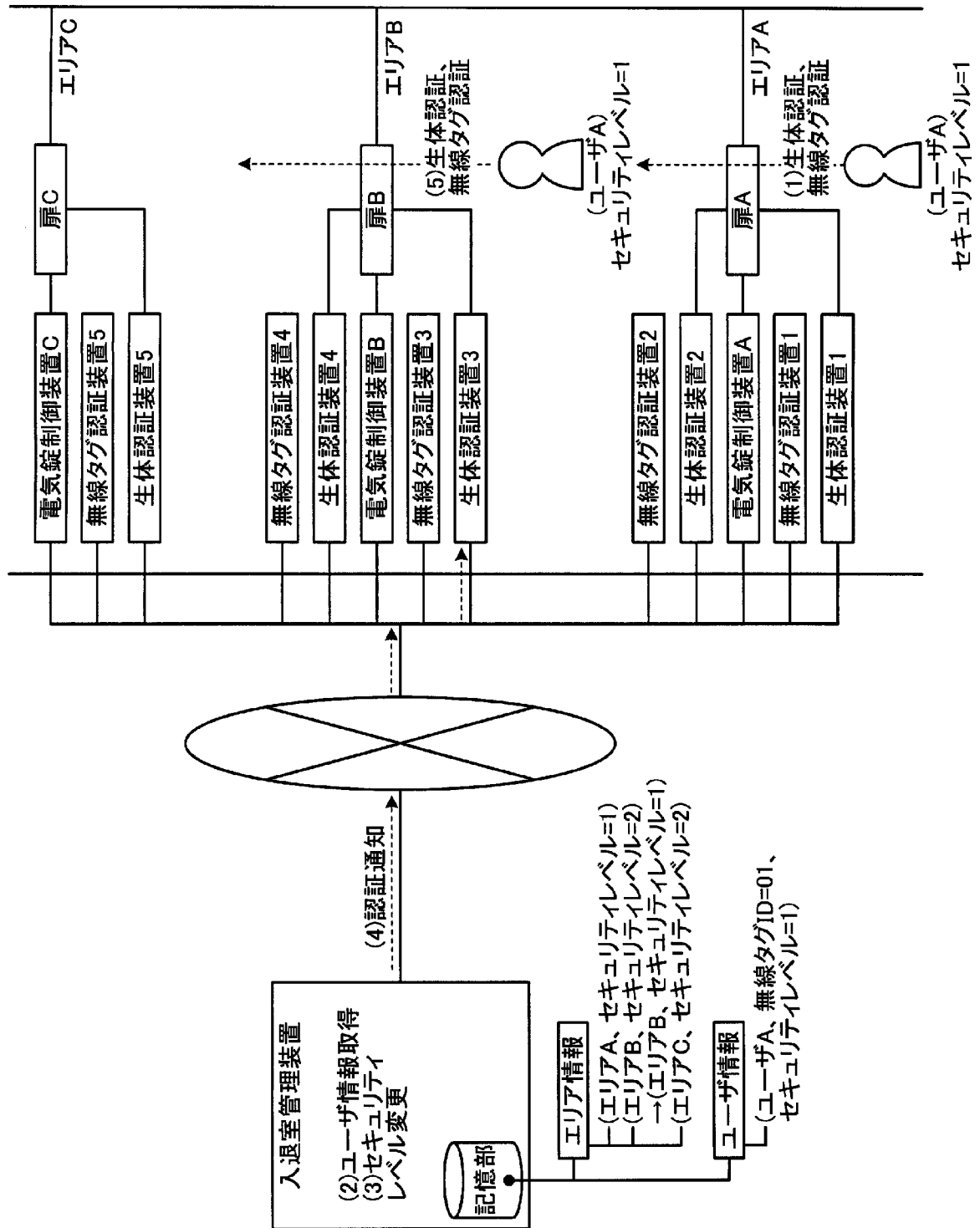
に再度入室する場合に、前記利用者に対して前記一種の認証を実施し、前記利用者が退室したエリアに前記所定の時間経過後に再度入室する場合に、前記利用者に対して前記複数種の認証を実施することを特徴とする請求項6～9のいずれか一つに記載の入退室管理方法。

- [11] セキュリティレベルが割り当てられたエリアに対して利用者が入退室する際に、前記利用者の入退室を許可するか否かを認証によって判定する入退室管理装置であって、

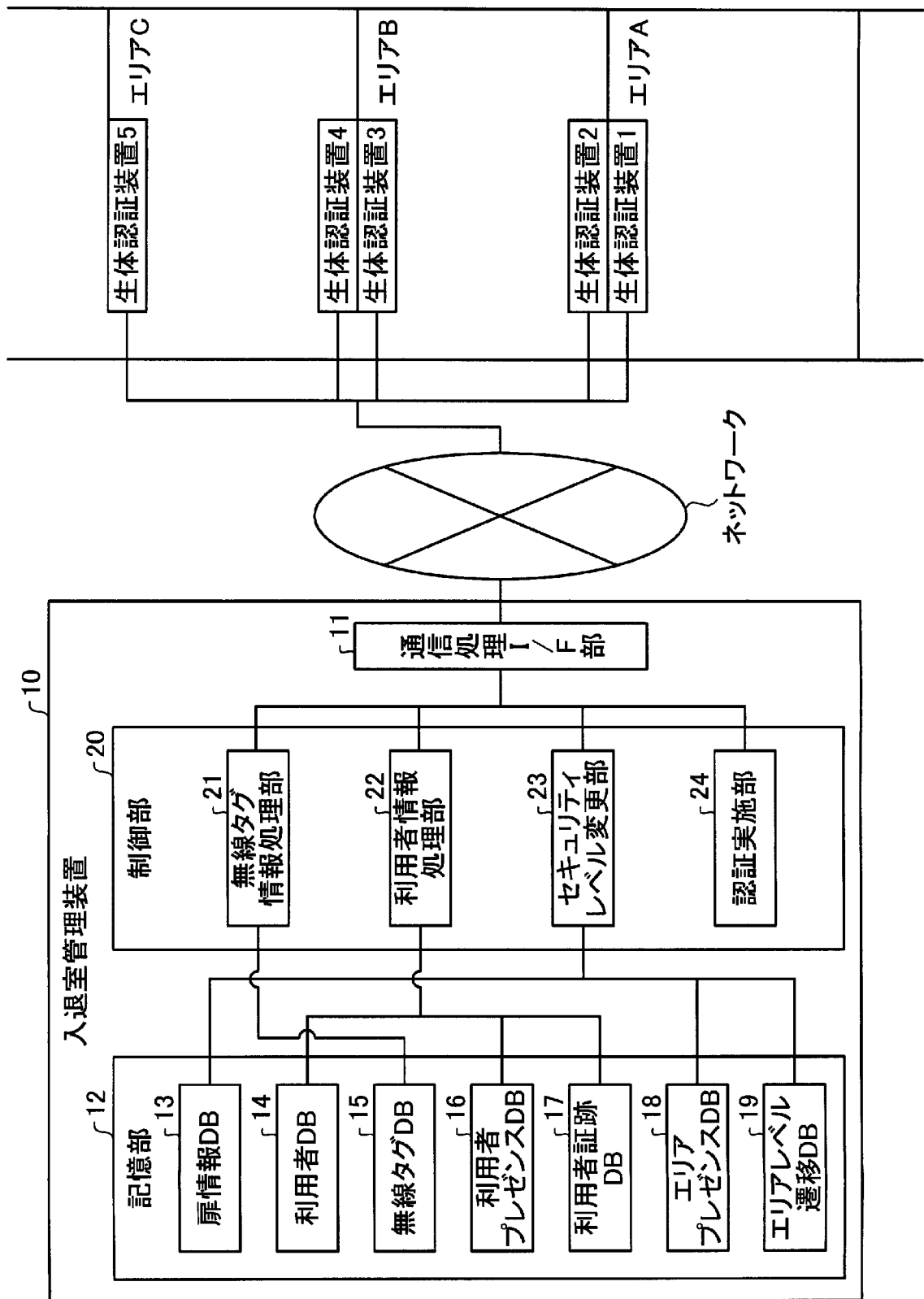
予め割り当てられたセキュリティレベルが異なるエリア間を前記利用者が移動する際に、当該エリア間のセキュリティレベルの差に応じた適切な認証を前記利用者に対して実施する認証実施手順、

を備えたことを特徴とする入退室管理装置。

[図1]



[図2]



[図3]

扉名	生体認証情報	エリア情報	開閉制御情報
扉A	静脈情報	エリアA、エリアB	12:00開 12:01閉
扉B	静脈情報	エリアB、エリアC	12:20開 12:21閉

⋮

⋮

⋮

⋮

[図4]

個人ID	氏名	生体認証データ	無線タグID	有効期限	入退室可能エリア
001	特許太郎	静脈情報A	01	2009年3月31日	ALL
002	特許花子	静脈情報B	02	2008年12月31日	セキュリティレベル2
⋮	⋮	⋮	⋮	⋮	⋮

[図5]

無線タグID	無線タグ認証装置情報	エリア情報
01	無線タグ認証装置2	エリアB
02	無線タグ認証装置1	エリアA
⋮	⋮	⋮

[図6]

ユーザ情報	在室エリア情報	継続性	利用者のセキュリティレベル
特許太郎(001)	エリアA	継続中	セキュリティレベル1
特許太郎(001)	エリアB	なし	セキュリティレベル1
⋮	⋮	⋮	⋮

[図7]

ユーザ情報	日時	扉情報	認証装置情報	エリア情報	認証結果
特許太郎(001)	2007年4月1日	扉A	生体認証装置1	エリアA	許可
特許花子(002)	2006年12月1日	扉B	生体認証装置3	エリアB	拒否
⋮	⋮	⋮	⋮	⋮	⋮

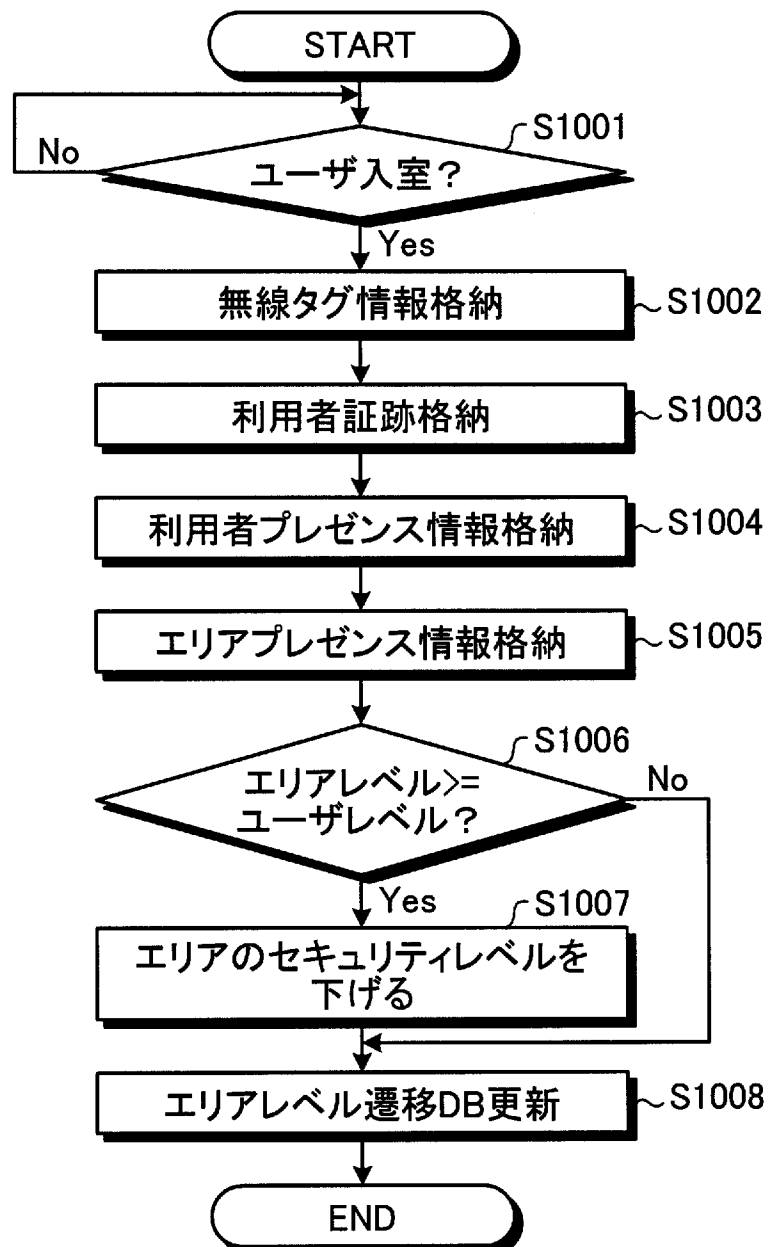
[図8]

在室エリア情報	継続性	利用者セキュリティレベル	エリアセキュリティレベル
エリアA	継続中	セキュリティレベル1	セキュリティレベル1
エリアB	なし	セキュリティレベル1	セキュリティレベル2
⋮	⋮	⋮	⋮

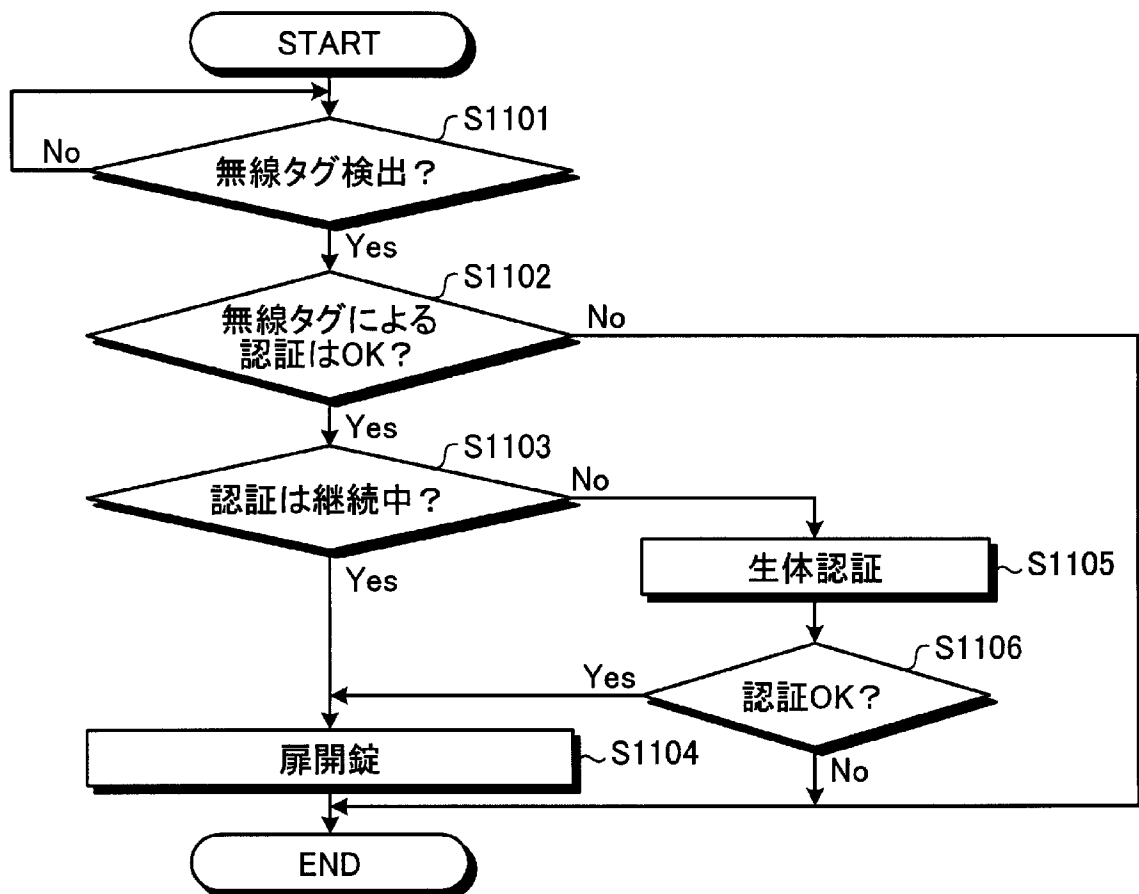
[図9]

日時	エリア	在室者	エリアセキュリティレベル
2007年4月1日	エリアA	特許太郎(001)	セキュリティレベル1

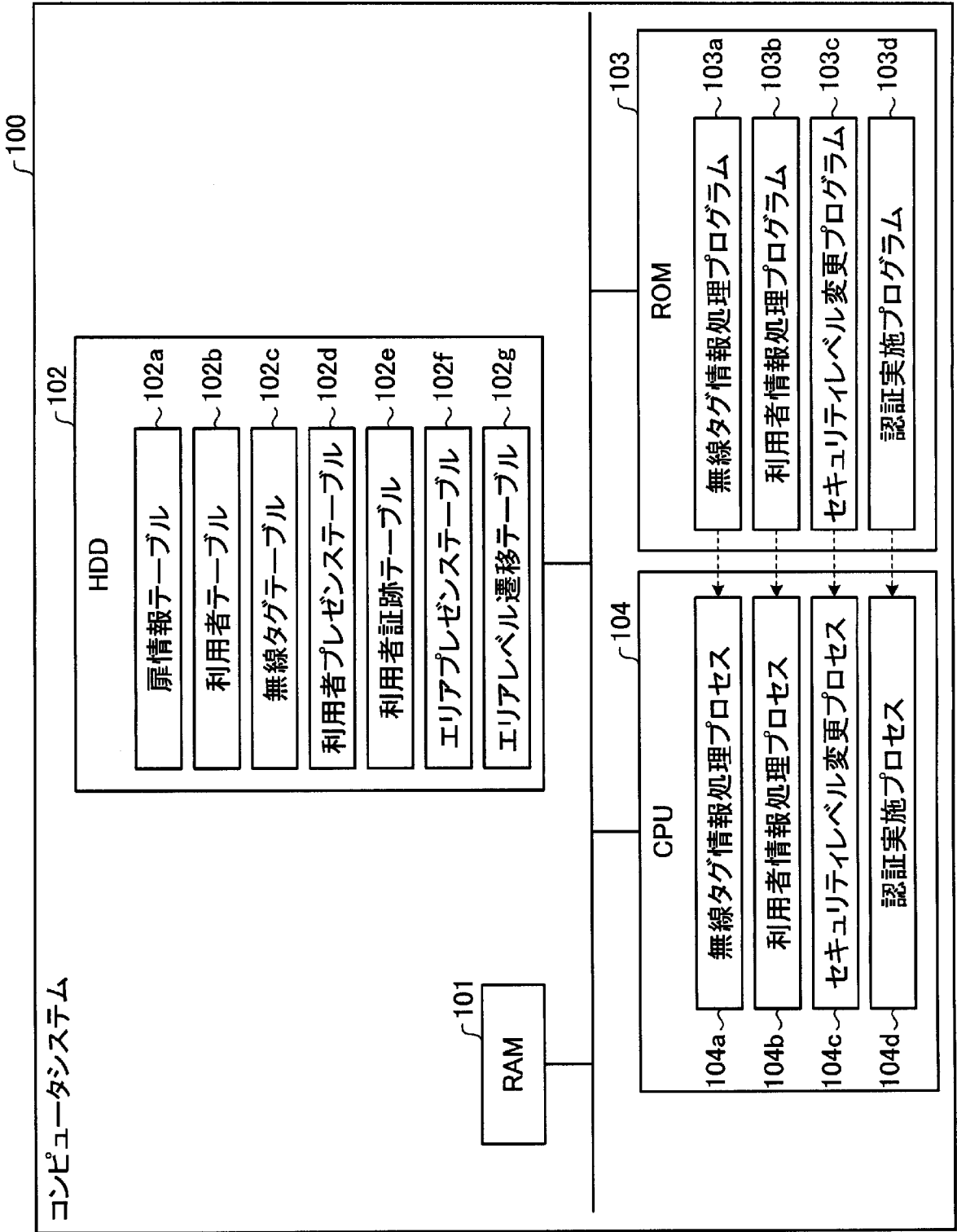
[図10]



[図11]



[図12]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2007/059097

A. CLASSIFICATION OF SUBJECT MATTER

G07C9/00 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G07C9/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2007

Kokai Jitsuyo Shinan Koho 1971-2007 Toroku Jitsuyo Shinan Koho 1994-2007

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X A	JP 62-49490 A (Toshiba Corp.), 04 March, 1987 (04.03.87), Page 3, lower left column, line 7 to page 4, lower right column, line 12; all drawings (Family: none)	1, 6, 11 2-5, 7-10
A	JP 63-300177 A (Yamatate-Honeywell Co., Ltd.), 07 December, 1988 (07.12.88), Full text; all drawings (Family: none)	1-11
A	JP 2006-338451 A (Hitachi Electronics Services Co., Ltd.), 14 December, 2006 (14.12.06), Full text; all drawings (Family: none)	1-11

☐ Further documents are listed in the continuation of Box C.☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
12 July, 2007 (12.07.07)Date of mailing of the international search report
24 July, 2007 (24.07.07)Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

A. 発明の属する分野の分類（国際特許分類（I P C））

Int.Cl. G07C9/00(2006.01)i

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（I P C））

Int.Cl. G07C9/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922-1996年
日本国公開実用新案公報	1971-2007年
日本国実用新案登録公報	1996-2007年
日本国登録実用新案公報	1994-2007年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X A	JP 62-49490 A（株式会社東芝）1987.03.04, 第3頁左下欄第7行－第4頁右下欄第12行、全図（ファミリーなし）	1, 6, 11 2-5, 7-10
A	JP 63-300177 A（山武ハネウエル株式会社）1988.12.07, 全文、全図（ファミリーなし）	1-11
A	JP 2006-338451 A（日立電子サービス株式会社）2006.12.14, 全文、全図（ファミリーなし）	1-11

C欄の続きにも文献が列挙されている。

パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日

12.07.2007

国際調査報告の発送日

24.07.2007

国際調査機関の名称及びあて先

日本国特許庁（I S A / J P）
郵便番号100-8915
東京都千代田区霞が関三丁目4番3号

特許庁審査官（権限のある職員）

門前 浩一

3 R

8723

電話番号 03-3581-1101 内線 3386