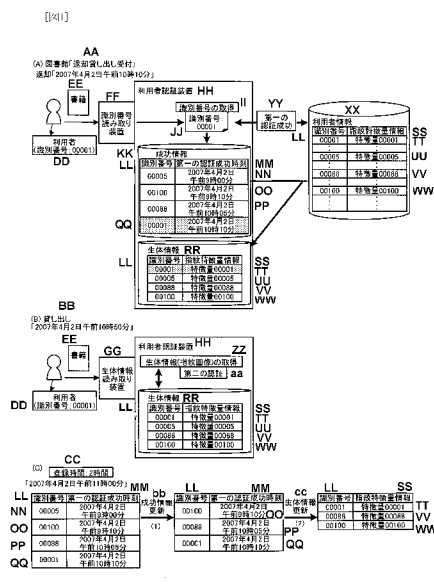


(10) 国際公開番号
WO 2009/008074 A1

- [続葉有]

(54) 発明の名称: 利用者認証装置、利用者認証方法および利用者認証プログラム

AA (A) "RETURN, LEND, ACCEPT" AT LIBRARY
BB (B) LEND
 "AM 10:50, APRIL 2, 2007"
CC (C) [REGISTRATION TIME PERIOD: 2 HOURS]
 "AM 11:00, APRIL 2, 2007"
DD USER (ID NO.: 00001)
EE BOOK
FF ID NUMBER READING DEVICE
GG LIVING BODY INFORMATION READING DEVICE
HH USER AUTHENTICATION DEVICE
II ACQUIRE ID NUMBER
JJ ID NO.: 00001
KK SUCCESS INFORMATION
LL ID NUMBER
MM FIRST AUTHENTICATION SUCCESS TIME
NN AM 9:00, APRIL 2, 2007
OO AM 9:10, APRIL 2, 2007
PP PM 10:05, APRIL 2, 2007
QQ AM 10:10, APRIL 2, 2007
RR LIVING BODY INFORMATION
SS FINGERPRINT CHARACTERIZING
 INFORMATION
TT CHARACTERISTICS 00001
UU CHARACTERISTICS 00005
VV CHARACTERISTICS 00088
WW CHARACTERISTICS 00100
XX USER INFORMATION
YY FIRST AUTHENTICATION SUCCESS
ZZ ACQUIRE LIVING BODY INFORMATION
 (FINGERPRINT IMAGE)
aa SECOND AUTHENTICATION
bb UPDATE SUCCESS INFORMATION
cc UPDATE LIVING BODY INFORMATION

[続葉有]



SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, 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

(57) 要約: 複数の利用者ごとに、各利用者を一意に識別するための識別情報と当該利用者の生体情報とを対応付けた利用者情報を記憶し、利用者が所定の対象に対する利用を開始する場合に、当該利用者の識別情報を取得し、第一の認証として、取得された識別情報と、記憶された利用者情報とを用いて利用者を認証し、第一の認証が成功した利用者の識別情報を成功情報として記憶し、利用者の生体情報を取得し、第二の認証として、取得された生体情報と、記憶された生体情報のうちで成功情報として記憶された利用者の識別情報に対応した生体情報とを用いて利用者を認証する。

明 細 書

利用者認証装置、利用者認証方法および利用者認証プログラム

技術分野

[0001] この発明は、利用者認証装置、利用者認証方法および利用者認証プログラムに関する。

背景技術

[0002] 従来より、同一人物に対して、異なる局面ごとに、繰り返して認証処理を実行することで、例えば、特定の領域内の安全性を保証することが行なわれている。

[0003] 認証処理の方法としては、個人に固有の情報であるとともに、偽造することが困難である生体情報（例えば、指紋や、手のひらの静脈パターンや、眼球の虹彩など）を用いて個人を認証する生体認証方法が、高い安全性を保証する方法として、広く用いられている。

[0004] ここで、生体認証方法は、「1:1認証」と「1:N認証」との2種類に大別される。「1:1認証」とは、認証を要求する人物から、生体情報とともに、IDなどの識別情報を受け付け、当該識別情報に対応する生体情報を特定し、特定された生体情報と、受け付けた生体情報とを照合することで、正当な利用者か否かを認証するものである。また、「1:N認証」とは、認証を要求する人物から、生体情報のみを受け付け、予め登録されている複数の生体情報すべて（あるいは照合対象とした生体情報すべて）と、受け付けた生体情報とを照合することで、正当な利用者か否かを認証するものである。

[0005] ここで、特許文献1では、認証されて施設内に入場した利用者を入場者リストに加え、当該施設内にある情報端末装置にログオンする際に、ログオン要求者が入場者リストにあることを確認した上で、ログオンを許可することで、施設内に設置される情報端末装置における安全性を保証する技術が開示されている。

[0006] また、特許文献2および特許文献3では、施設内への入場あるいは情報端末装置にログオンする際に、生体認証方法を適用することで、施設内の安全性を確保する技術が開示されている。

[0007] また、特許文献4では、生体認証方法において、利用者が認証のために入力した

生体情報と、予め登録されている利用者の生体情報と粗照合を行なうことで、「1:N認証」の照合対象となる生体情報を選別する技術が開示されている。

[0008] また、特許文献5では、利用者の行動パターンに基づいて、照合対象となる生体情報に優先順位を付加することで、「1:N認証」の照合対象となる生体情報を選別する技術が開示されている。

[0009] また、特許文献6および特許文献8では、予め登録されている利用者の生体情報に有効期限を設定しておくことで、「1:N認証」の照合対象となる生体情報を選別する技術が開示されている。

[0010] また、特許文献7では、要注意者の生体情報を記録したブラックリストを参照し、ブラックリストに記録された生体情報を、予め登録されている利用者の生体情報から除外することで、「1:N認証」の照合対象となる生体情報を選別する技術が開示されている。

[0011] 特許文献1:特開2006-155138号公報

特許文献2:特開2004-246553号公報

特許文献3:特開2004-355318号公報

特許文献4:特開2004-258963号公報

特許文献5:特開2002-140707号公報

特許文献6:特開2006-277028号公報

特許文献7:特開2006-260482号公報

特許文献8:特開2003-193723号公報

発明の開示

発明が解決しようとする課題

[0012] ところで、上記した従来の入場者リストを参照して安全性を確保する技術は、2回目の認証は入場者リストを参照するのみであり、必ずしも情報端末装置における安全性が確保されていないので、認証性能が悪いという問題点があった。

[0013] また、上記した従来の生体認証方法を適用することで安全性を確保する技術は、照合対象の数が増大するとともに、照合処理に要する時間が増大することに対応することはできないので、認証性能が悪いという問題点があった。

[0014] また、上記した従来の「1:N認証」の照合対象となる生体情報を選別する技術は、固定情報に基づいて照合対象を選別しているので、状況に応じて柔軟に照合対象を選別することができず、選別の精度が悪化する危険性があるので、認証性能が悪いという問題点があった。

[0015] 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、認証性能を向上することが可能になる利用者認証装置、利用者認証方法および利用者認証プログラム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

[0016] 上述した課題を解決し、目的を達成するため、本発明は、利用者を認証する利用者認証装置であって、複数の利用者ごとに、各利用者を一意に識別するための識別情報と当該利用者の生体情報とを対応付けた利用者情報を記憶する利用者情報記憶手段と、前記利用者が所定の対象に対する利用を開始する場合に、当該利用者の識別情報を取得する識別情報取得手段と、前記識別情報取得手段により取得された識別情報と、前記利用者情報記憶手段に記憶された利用者情報とを用いて利用者を認証する第一の認証手段と、前記第一の認証手段による認証が成功した利用者の識別情報を成功情報として記憶する成功情報記憶手段と、前記利用者の生体情報を取得する生体情報取得手段と、前記生体情報取得手段により取得された生体情報と、前記利用者情報記憶手段に記憶された生体情報のうちで前記成功情報記憶手段に成功情報として記憶された利用者の識別情報に対応した生体情報とを用いて利用者を認証する第二の認証手段と、を備えたことを特徴とする。

[0017] また、本発明は、上記の発明において、所定の成功情報が前記成功情報記憶手段に記憶されてから所定の登録時間が経過したか否かを判定し、当該登録時間が経過した場合に、当該所定の成功情報を前記成功情報記憶手段から削除する成功情報削除手段をさらに備えたことを特徴とする。

[0018] また、本発明は、上記の発明において、前記成功情報削除手段は、前記利用者ごとに定められた登録時間が経過したか否かを判定することを特徴とする。

[0019] また、本発明は、上記の発明において、前記成功情報削除手段は、前記成功情報記憶手段に記憶された成功情報の個数が所定値以上になった場合に、当該所定値

未満に際して判定に用いられる登録時間よりも短い登録時間を用いて、当該登録時間が経過したか否かを判定することを特徴とする。

[0020] また、本発明は、上記の発明において、前記利用者の利用頻度を記憶する利用頻度記憶手段をさらに備え、前記成功情報削除手段は、前記成功情報記憶手段に記憶された成功情報の個数が所定値以上になった場合に、前記利用頻度記憶手段に記憶された各利用者の利用頻度に基づいて、当該利用頻度が所定値よりも低い利用者の成功情報を前記成功情報記憶手段からさらに削除することを特徴とする。

[0021] また、本発明は、上記の発明において、前記利用者情報記憶手段は、各利用者が属するグループを一意に識別するグループ識別情報を、前記利用者の識別情報に対応付けてさらに記憶し、前記成功情報記憶手段は、前記第一の認証手段による認証が成功した利用者の識別情報の他に、当該利用者のグループ識別情報に対応する他の利用者の識別情報も成功情報として記憶することを特徴とする。

[0022] また、本発明は、上記の発明において、前記利用者情報記憶手段は、前記利用者が利用している物品または情報を、前記利用者の識別情報に対応付けてさらに記憶し、前記識別情報取得手段は、前記利用者が利用する物品または情報から当該利用者の識別情報を取得することを特徴とする。

[0023] また、本発明は、上記の発明において、前記識別情報取得手段は、前記利用者が所定の対象に対する利用を終了する場合に、当該利用者の識別情報をさらに取得し、前記成功情報削除手段は、前記識別情報取得手段による利用の終了に際して取得された識別情報を前記成功情報記憶手段からさらに削除することを特徴とする。

[0024] また、本発明は、上記の発明において、前記識別情報取得手段は、所定の物品または情報を返却する利用者の識別情報を取得し、前記生体情報取得手段は、所定の物品または情報を貸し出そうとする利用者の生体情報を取得することを特徴とする。

[0025] また、本発明は、上記の発明において、前記成功情報記憶手段に成功情報として記憶されている利用者の識別情報に対応した生体情報を前記利用者情報記憶手段から取得して記憶する生体情報記憶手段をさらに備え、前記第二の認証手段は、前記生体情報記憶手段に記憶された生体情報を用いて前記利用者を認証することを

特徴とする。

- [0026] また、本発明は、上記の発明において、所定の物品または情報を返却した利用者が、同日に所定の物品または情報を貸し出す頻度を記憶する貸し出し頻度記憶手段をさらに備え、前記成功情報削除手段は、前記成功情報記憶手段に記憶された成功情報の個数が所定値以上になった場合に、前記貸し出し頻度記憶手段に記憶された各利用者の貸し出し頻度に基づいて、当該貸し出し頻度が所定値よりも低い利用者の成功情報を前記成功情報記憶手段からさらに削除することを特徴とする。
- [0027] また、本発明は、上記の発明において、前記識別情報取得手段は、所定の領域に入域する利用者の識別情報を取得するとともに、当該所定の領域から出域する利用者の識別情報を取得し、前記成功情報記憶手段は、前記所定の領域に入域している利用者の識別情報を成功情報として当該所定の領域から出域するまで記憶することを特徴とする。
- [0028] また、本発明は、上記の発明において、前記識別情報取得手段により入域として取得された識別情報を、前記成功情報記憶手段に追加して格納するとともに、前記識別情報取得手段により出域として取得された識別情報を、前記成功情報記憶手段から削除する成功情報追加削除手段をさらに備えたことを特徴とする。
- [0029] また、本発明は、上記の発明において、前記成功情報追加削除手段は、前記識別情報取得手段により取得された複数の識別情報を入手し、各識別情報が入域であるか出域であるかに応じて、各識別情報を前記成功情報記憶手段に追加または削除することを特徴とする。
- [0030] また、本発明は、上記の発明において、前記成功情報追加削除手段は、前記識別情報取得手段により取得された複数の識別情報を所定の時間毎に入手し、各識別情報が入域であるか出域であるかに応じて、各識別情報を前記成功情報記憶手段に追加または削除することを特徴とする。
- [0031] また、本発明は、上記の発明において、前記成功情報記憶手段は、前記所定の領域に入域しているか出域しているかにかかわらず、所定の利用者の識別情報を成功情報として常に記憶することを特徴とする。
- [0032] また、本発明は、上記の発明において、前記成功情報記憶手段は、前記所定の領

域に入域しているか出域しているかにかかわらず、所定の利用者の識別情報を非成功情報として常に記憶し、前記第二の認証手段は、前記成功情報記憶手段に非成功情報として記憶された利用者の識別情報に対応した生体情報を用いることなく前記利用者を認証することを特徴とする。

[0033] また、本発明は、上記の発明において、前記第二の認証手段は、いずれの領域において前記生体情報取得手段により生体情報が取得されたかに応じて、前記生体情報が取得された領域に入域している利用者であり、かつ、前記成功情報記憶手段に成功情報として記憶された利用者の識別情報を用いて利用者を認証することを特徴とする。

[0034] また、本発明は、利用者を認証する利用者認証方法であって、複数の利用者ごとに、各利用者を一意に識別するための識別情報と当該利用者の生体情報とを対応付けた利用者情報を記憶する利用者情報記憶ステップと、前記利用者が所定の対象に対する利用を開始する場合に、当該利用者の識別情報を取得する識別情報取得ステップと、前記識別情報取得ステップにより取得された識別情報と、前記利用者情報記憶手段に記憶された利用者情報とを用いて利用者を認証する第一の認証ステップと、前記第一の認証ステップによる認証が成功した利用者の識別情報を成功情報として記憶する成功情報記憶ステップと、前記利用者の生体情報を取得する生体情報取得ステップと、前記生体情報取得ステップにより取得された生体情報と、前記利用者情報記憶ステップに記憶された生体情報のうちで前記成功情報記憶ステップに成功情報として記憶された利用者の識別情報に対応した生体情報とを用いて利用者を認証する第二の認証ステップと、を備えたことを特徴とする。

[0035] また、本発明は、利用者を認証する利用者認証方法をコンピュータに実行させる利用者認証プログラムであって、複数の利用者ごとに、各利用者を一意に識別するための識別情報と当該利用者の生体情報とを対応付けた利用者情報を記憶する利用者情報記憶手順と、前記利用者が所定の対象に対する利用を開始する場合に、当該利用者の識別情報を取得する識別情報取得手順と、前記識別情報取得手順により取得された識別情報と、前記利用者情報記憶手順に記憶された利用者情報とを用いて利用者を認証する第一の認証手順と、前記第一の認証手順による認証が成功

した利用者の識別情報を成功情報として記憶する成功情報記憶手順と、前記利用者の生体情報を取得する生体情報取得手順と、前記生体情報取得手順により取得された生体情報と、前記利用者情報記憶手順に記憶された生体情報のうちで前記成功情報記憶手順に成功情報として記憶された利用者の識別情報に対応した生体情報とを用いて利用者を認証する第二の認証手順と、をコンピュータに実行させることを特徴とする。

発明の効果

- [0036] 本発明によれば、利用開始を認証された利用者のみを「1:N認証」の照合対象として絞り込むことができ、認証性能を向上することが可能になる。
- [0037] また、本発明によれば、例えば、図書館における利用開始が認証された利用者の中で、書籍などの貸し出し要求を行なう可能性が低くなった利用者を「1:N認証」の照合対象から除外することができ、認証性能を向上することが可能になる。
- [0038] また、本発明によれば、例えば、図書館における利用者ごとの行動履歴に基づいて利用者それぞれに登録時間を設定することで、「1:N認証」の照合対象を利用者それぞれの特性に基づいて柔軟に絞り込むことができ、認証性能を向上することが可能になる。
- [0039] また、本発明によれば、成功情報の個数が膨大になった場合でも、登録時間を短縮することで「1:N認証」の照合対象を減少させて照合処理にかかる時間を速くすることができ、認証性能を向上することが可能になる。
- [0040] また、本発明によれば、成功情報の個数が膨大になった場合でも、認証要求を行なう可能性が低い利用者の成功情報を削除することで「1:N認証」の照合対象を減少させて照合処理にかかる時間を速くすることができ、認証性能を向上することが可能になる。
- [0041] また、本発明によれば、利用開始が認証された利用者と同様に認証要求を行なう可能性の高い利用者を「1:N認証」の照合対象に加えることができ、認証性能を向上することが可能になる。
- [0042] また、本発明によれば、利用者自身ではなく、利用者を特定することが可能な物品または情報によって第一の認証を速やかに処理することができ、認証性能を向上す

ることが可能になる。

[0043] また、本発明によれば、認証要求を行なう可能性がない利用者を、「1:N認証」の照合対象から除外することができ、認証性能を向上することが可能になる。

[0044] また、本発明によれば、例えば、書籍を返却することで図書館の利用開始を認証された利用者を、書籍貸し出し時における「1:N認証」の照合対象として絞り込むことができ、認証性能を向上することが可能になる。

[0045] また、本発明によれば、第一の認証が成功した利用者の生体情報を予め取得して記憶しておくことで、第二の認証における「1:N認証」の際の処理速度を速くすることができ、認証性能を向上することが可能になる。

[0046] また、本発明によれば、成功情報の個数が膨大になった場合でも、例えば、図書館において書籍の貸し出し要求のための認証要求を行なう可能性が低い利用者の成功情報を削除することで「1:N認証」の照合対象を減少させて照合処理にかかる時間を速くすることができ、認証性能を向上することが可能になる。

[0047] また、本発明によれば、認証要求を行なう可能性がある利用者のみを、「1:N認証」の照合対象とすることができ、認証性能を向上することが可能になる。

[0048] また、本発明によれば、認証要求を行なう可能性がない利用者を、「1:N認証」の照合対象から速やかに除外することができ、認証性能を向上することが可能になる。

[0049] また、本発明によれば、成功情報の追加および削除を一括して実行して「1:N認証」の照合対象を絞り込むことができ、認証性能を向上することが可能になる。

[0050] また、本発明によれば、成功情報が更新されるごとに処理を行なうのではなく、一定間隔で成功情報の更新処理を行なって、更新処理に要する装置の負荷を軽減でき、認証性能を向上することが可能になる。

[0051] また、本発明によれば、例えば、取締役などの役職にある利用者を「1:N認証」の照合対象として常に設定するなど、利用者のニーズに柔軟に対応することができ、認証性能を向上することが可能になる。

[0052] また、本発明によれば、例えば、所定の領域内で問題を起こした利用者を「1:N認証」の照合対象として常に除外するなど、利用者のニーズに柔軟に対応することができ、さらに認証性能を向上することが可能になる。

[0053] また、本発明によれば、生体情報読み取り装置が設置される場所に入域することが許可されている利用者を「1:N認証」の照合対象における母集団として絞り込むことができ、認証性能を向上することが可能になる。

図面の簡単な説明

[0054] [図1]図1は、実施例1における利用者認証装置の概要および特徴を説明するための図である。

[図2]図2は、実施例1における利用者認証装置の構成を示すブロック図である。

[図3]図3は、実施例1における利用者情報記憶部を説明するための図である。

[図4]図4は、実施例1における成功情報記憶部を説明するための図である。

[図5]図5は、実施例1における生体情報記憶部を説明するための図である。

[図6]図6は、実施例1における利用者認証装置の第一の認証処理を説明するための図である。

[図7]図7は、実施例1における利用者認証装置の成功情報および生体情報の削除処理を説明するための図である。

[図8]図8は、実施例1における利用者認証装置の第二の認証処理を説明するための図である。

[図9]図9は、実施例2における利用者認証装置を説明するための図である。

[図10]図10は、実施例3における利用者認証装置を説明するための図である。

[図11]図11は、実施例4における利用者認証装置を説明するための図である。

[図12]図12は、実施例5における利用者認証装置を説明するための図である。

[図13]図13は、実施例6における利用者認証システムの概要および特徴を説明するための図である。

[図14]図14は、実施例6における利用者認証システムの概要および特徴を説明するための図である。

[図15]図15は、実施例6における利用者認証システムの概要および特徴を説明するための図である。

[図16]図16は、実施例6における入退室管理装置の構成を示すブロック図である。

[図17]図17は、実施例6における領域入出権限記憶部を説明するための図である。

[図18]図18は、実施例6における利用者認証装置の構成を示すブロック図である。

[図19]図19は、実施例6における生体情報記憶部を説明するための図である。

[図20]図20は、実施例6における利用者認証対象者記憶部を説明するための図である。

[図21]図21は、実施例6における端末センサ記憶部を説明するための図である。

[図22]図22は、実施例6における端末装置利用権限記憶部を説明するための図である。

[図23]図23は、実施例6における入退室管理装置の入室時処理を説明するための図である。

[図24]図24は、実施例6における利用者認証装置の入室時処理を説明するための図である。

[図25]図25は、実施例6における利用者認証装置の認証処理を説明するための図である。

[図26]図26は、実施例7における利用者認証システムを説明するための図である。

[図27]図27は、実施例8における利用者認証システムを説明するための図である。

[図28]図28は、実施例9における利用者認証システムを説明するための図である。

[図29]図29は、実施例1の利用者認証プログラムを実行するコンピュータを示す図である。

符号の説明

- [0055]
- 1 識別番号読み取り装置
 - 2 生体情報読み取り装置
 - 3 利用者情報記憶部
 - 10 利用者認証装置
 - 11 通信制御I/F部
 - 12 記憶部
 - 12a 成功情報記憶部
 - 12b 生体情報記憶部
 - 13 処理部

13a 第一認証部

13b 生体情報格納部

13c 第二認証部

13d 成功情報削除部

発明を実施するための最良の形態

[0056] 以下に添付図面を参照して、この発明に係る利用者認証装置、利用者認証方法および利用者認証プログラムの実施例を詳細に説明する。

実施例 1

[0057] [実施例1における利用者認証装置の概要および特徴]

まず最初に、図1を用いて、実施例1における利用者認証装置の主たる特徴を具体的に説明する。図1は、実施例1における利用者認証装置の概要および特徴を説明するための図である。

[0058] 実施例1における利用者認証装置は、利用者を認証することを概要とする。例えば、実施例1における利用者認証装置は、図書館の「返却貸し出し受付」に設置され、書籍の貸し出しを要求する利用者から「指紋画像」などの生体情報を取得して「1:N認証」を行ない、取得した生体情報が、予め利用者として登録されている生体情報と一致した場合にのみ、取得した生体情報を入力した利用者に書籍を貸し出すことを認める。なお、「1:N」認証とは、認証を要求する人物から、生体情報のみを受け付け、予め登録されている複数の生体情報すべてと(あるいは、照合対象とされた生体情報すべてと)、取得した生体情報とを照合することで、正当な利用者か否かを認証するものである。

[0059] ここで、本発明は、認証性能を向上することが可能になることに主たる特徴がある。この主たる特徴について簡単に説明すると、実施例1における利用者認証装置は、複数の利用者ごとに、各利用者を一意に識別するための識別情報と当該利用者の生体情報とを対応付けた利用者情報を記憶する。

[0060] 具体的には、図1の(A)に示すように、実施例1における利用者認証装置は、図書館に登録される複数の利用者ごとに、各利用者を一意に識別するための識別情報と、当該利用者の生体情報である「指紋画像」から抽出した「指紋特徴量情報」とを対

応付けた利用者情報を記憶する。例えば、図1の(A)に示すように、利用者情報として、「識別番号:00001」と、「指紋特徴量情報:特徴量00001」とを対応付けて記憶する。

[0061] そして、実施例1における利用者認証装置は、利用者が図書館の利用を開始する場合として、所定の物品を返却する利用者の識別情報を取得する。具体的には、貸し出していた書籍を返却するために図書館に来館した利用者が、自身に割り振られた識別番号を記憶するICカードを識別情報読み取り装置に提示することで、実施例1における利用者認証装置は、識別情報読み取り装置がICカードから読み取った識別番号を所得する。

[0062] より具体的には、実施例1における利用者認証装置は、図1の(A)に示すように、貸し出していた書籍を返却するために図書館に来館した「識別番号:00001」の利用者が「2007年4月2日午前10時10分」に提示したICカードから、識別番号読み取り装置を介して、「識別番号:00001」を取得する。また、識別番号を取得した時間である「2007年4月2日午前10時10分」も併せて取得する。

[0063] そして、実施例1における利用者認証装置は、第一の認証として、取得された識別情報と、記憶された利用者情報とを用いて利用者を認証する。すなわち、取得された識別番号が利用者情報として登録されている識別番号に存在するか否かを検索し、利用者情報に該当する識別番号が存在する場合には、「第一の認証成功」と判定し、利用者情報に該当する識別番号が存在しない場合には、「第一の認証不成功」と判定する。すなわち、「第一の認証成功」と判定された利用者の図書館利用開始を許可とし、「第一の認証不成功」と判定された利用者の図書館利用開始を不許可とする。

[0064] そして、実施例1における利用者認証装置は、第一の認証が成功した利用者の識別情報を成功情報として記憶する。具体的には、第一の認証が成功した利用者の識別情報とともに、当該識別情報を取得した時間を「第一の認証成功時刻」として記憶する。例えば、図1の(A)に示すように、「第一の認証成功」と判定された「識別番号:00001」を「第一の認証成功時刻:2007年4月2日午前10時10分」とともに、成功情報として記憶する。

- [0065] そして、実施例1における利用者認証装置は、成功情報として記憶されている利用者の識別情報に対応した生体情報を利用者情報から取得して記憶する。例えば、図1の(A)に示すように、成功情報として新たに記憶された「識別番号:00001」に対応する「特徴量00001」を利用者情報から取得して記憶する。
- [0066] なお、図1の(A)に示すように、「識別番号:00001」に対応する「特徴量00001」を取得して記憶される以前に、「識別番号:00005」に対応する「特徴量00005」と、「識別番号:00100」に対応する「特徴量00100」と、「識別番号:00088」に対応する「特徴量00088」とを、既に取得して記憶している。
- [0067] そして、実施例1における利用者認証装置は、所定の物品を貸し出そうとする利用者の生体情報を取得する。具体的には、実施例1における利用者認証装置は、図1の(B)に示すように、書籍を貸し出そうとする利用者(識別番号:00001)の生体情報としての「指紋画像」を、生体情報読み取り装置を介して、取得する。
- [0068] そして、実施例1における利用者認証装置は、第二の認証として、取得された生体情報と、予め利用者情報から取得して記憶した生体情報とを用いて利用者を認証する。具体的には、実施例1における利用者認証装置は、取得した「指紋画像」から「指紋特徴量情報」を抽出し、生体情報として記憶した「指紋特徴量情報」に、抽出した「指紋特徴量情報」と一致する「指紋特徴量情報」が存在する場合は、利用者として認証する。すなわち、当該利用者が書籍を貸し出すことを認めると判定する。また、生体情報として記憶した「指紋特徴量情報」に、抽出した「指紋特徴量情報」と一致する「指紋特徴量情報」が存在しない場合は、利用者が書籍を貸し出すことを認めないと判定する。
- [0069] 例えば、図1の(B)に示すように、利用者(識別番号:00001)の「指紋画像」から抽出した「指紋特徴量情報」と一致する「指紋特徴量情報:特徴量00001」が、生体情報として記憶した「指紋特徴量情報」に存在するので、利用者(識別番号:00001)が書籍を貸し出すことを認めると判定する。
- [0070] 一方、実施例1における利用者認証装置は、所定の成功情報が記憶されてから所定の登録時間が経過したか否かを判定し、当該登録時間が経過した場合に、当該所定の成功情報を削除する。すなわち、実施例1における利用者認証装置は、例え

ば、「登録時間:2時間」とする設定を記憶し、成功情報ごとに、識別番号とともに記憶されている「第一の認証成功時刻」から「2時間」が経過したか否かを判定し、「第一の認証成功時刻」から「2時間」経過した成功情報がある場合は、当該成功情報を削除する。

[0071] より具体的には、図1の(C)に示すように、「2007年4月2日午前11時00分」の時点で、「第一の認証成功時刻」から「2時間」経過した「識別番号:00005、第一の認証成功時刻:2007年4月2日午前9時00分」の成功情報は削除され、成功情報は更新される(図1の(C)の(1)参照)。また、これにより、「識別番号:00005、特徴量00005」の生体情報も削除され、生体情報も更新される(図1の(C)の(2)参照)。

[0072] このようなことから、実施例1における利用者認証装置は、書籍を返却することで図書館の利用開始を認証された利用者を、書籍貸し出し時における「1:N認証」の照合対象として絞り込むことができ、上記した主たる特徴のごとく、認証性能を向上することが可能になる。

[0073] [実施例1における利用者認証装置の構成]

次に、図2などを用いて、実施例1における利用者認証装置を説明する。図2は、実施例1における利用者認証装置の構成を示すブロック図である。

[0074] 図2に示すように、実施例1における利用者認証装置10は、通信制御I/F部11と、記憶部12と、処理部13とから構成され、さらに、識別番号読み取り装置1と、生体情報読み取り装置2と、利用者情報記憶部3とに接続される。

[0075] 利用者情報記憶部3は、図書館に登録される複数の利用者ごとに、各利用者を一意に識別するための識別情報と、当該利用者の生体情報である「指紋画像」から抽出した「指紋特徴量情報」とを対応付けた利用者情報を記憶する。また、利用者情報記憶部3は、例えば、図書館の管理センターに設置され、利用者認証装置10とネットワークにて接続される。ここで、利用者情報記憶部3は、請求の範囲に記載の「利用者情報記憶手段」に対応する。

[0076] 例えば、利用者情報記憶部3は、図3に示すように、利用者情報として、「識別番号:00001」と、「指紋特徴量情報:特徴量00001」とを対応付けて記憶する。ここで、「指紋特徴量情報」とは、「指紋画像」から指紋を構成する曲線の切れ目や分かれ目な

どの特徴的な部分を特徴量として抽出した情報のことである。なお、図3は、実施例1における利用者情報記憶部を説明するための図である。

[0077] 識別番号読み取り装置1は、利用者が図書館の利用を開始する場合として、所定の物品を返却する利用者の識別情報を取得し、取得した識別番号を利用者認証装置10に送信する。ここで、識別番号読み取り装置1は、請求の範囲に記載の「識別情報取得手段」に対応する。

[0078] 具体的には、識別番号読み取り装置1は、貸し出していた書籍を返却するために図書館に来館した利用者が提示したICカードから識別番号を読み取り、当該識別番号を利用者認証装置10に送信する。

[0079] より具体的には、識別番号読み取り装置1は、図1の(A)に示すように、貸し出していた書籍を返却するために図書館に来館した「識別番号:00001」の利用者が「2007年4月2日午前10時10分」に提示したICカードから、「識別番号:00001」を読み取り、「識別番号:00001」と、当該識別番号を取得した時間である「2007年4月2日午前10時10分」とを利用者認証装置10に送信する。

[0080] 生体情報読み取り装置2は、所定の物品を貸し出そうとする利用者の生体情報を取得し、取得した生体情報を利用者認証装置10に送信する。ここで、生体情報読み取り装置2は、請求の範囲に記載の「生体情報取得手段」に対応する。

[0081] 例えば、生体情報読み取り装置2は、図1の(B)に示すように、書籍を貸し出そうとする利用者(識別番号:00001)の生体情報としての「指紋画像」を取得し、取得した生体情報を利用者認証装置10に送信する。

[0082] 通信制御I/F部11は、識別番号読み取り装置1、生体情報読み取り装置2および利用者情報記憶部3と、記憶部12および処理部13との間でやり取りする各種情報に関する通信を制御する。例えば、識別番号読み取り装置1が送信した識別番号や、生体情報読み取り装置が送信した生体情報を、処理部13に転送したり、後述する生体情報格納部13bが利用者情報記憶部3から取得した生体情報を、記憶部12に転送したりする。

[0083] 記憶部12は、後述する処理部13による各種処理結果などを記憶し、特に本発明に密接に関連するものとしては、図2に示すように、成功情報記憶部12aと、生体情

報記憶部12bとを備える。成功情報記憶部12aは、後述する第一認証部13aが、上記した識別番号読み取り装置1から受信した識別番号の中で、成功情報として判定した識別番号を記憶し、生体情報記憶部12bは、後述する生体情報格納部13bが、上記した利用者情報記憶部3から取得した生体情報を記憶する。ここで、成功情報記憶部12aは、請求の範囲に記載の「成功情報記憶手段」に対応し、生体情報記憶部12bは、同じく「生体情報記憶手段」に対応する。なお、各部については、後に詳述する。

[0084] 処理部13は、各種処理を実行し、特に本発明に密接に関連するものとしては、図2に示すように、第一認証部13aと、生体情報格納部13bと、第二認証部13cと、成功情報削除部13dとを備える。ここで、第一認証部13aは、請求の範囲に記載の「第一の認証手段」に対応し、第二認証部13cは、同じく「第二の認証手段」に対応し、成功情報削除部13dは、同じく「成功情報削除手段」に対応する。

[0085] 第一認証部13aは、識別番号読み取り装置1から受信した識別情報と、利用者情報記憶部3が記憶する利用者情報とを用いて利用者を認証する。すなわち、識別番号読み取り装置1から受信した識別番号が、利用者情報記憶部3において利用者情報として登録されている識別番号に存在するか否かを検索し、利用者情報に該当する識別番号が存在する場合には、「第一の認証成功」と判定し、利用者情報に該当する識別番号が存在しない場合には、「第一の認証不成功」と判定する。そして、「第一の認証成功」と判定された利用者の図書館利用開始を許可とし、「第一の認証不成功」と判定された利用者の図書館利用開始を不許可とする。

[0086] 例えば、第一認証部13aは、受信した「識別番号:00001」が、図3に示すように、利用者情報記憶部3において利用者情報として登録されている識別番号に存在しているので、「第一の認証成功」と判定し、「識別番号:00001」の利用者の図書館利用開始を許可する。

[0087] また、第一認証部13aは、「第一の認証成功」と判定した利用者の「識別情報」と、当該「識別番号」を識別番号読み取り装置1から受信した時刻である「第一の認証成功時刻」とを成功情報として成功情報記憶部12aに格納する。

[0088] 具体的には、第一認証部13aは、図4に示すように、「第一の認証成功」と判定する

ごとに、「識別番号」と「第一の認証成功時刻」とを成功情報として成功情報記憶部12aに格納する。つまり、「識別番号:00005、第一の認証成功時刻:2007年4月2日午前9時00分」と、「識別番号:00100、第一の認証成功時刻:2007年4月2日午前9時10分」と、「識別番号:00088、第一の認証成功時刻:2007年4月2日午前10時05分」とを成功情報として、成功情報記憶部12aに格納する(図4の(A)参照)。

[0089] そして、第一認証部13aは、新たに「第一の認証成功」として判定した「識別番号:00001」および「第一の認証成功時刻:2007年4月2日午前10時10分」を成功情報として成功情報記憶部12aに追加して格納する(図4の(B)参照)。なお、図4は、実施例1における成功情報記憶部を説明するための図である。

[0090] 生体情報格納部13bは、成功情報記憶部12aが成功情報として記憶する利用者の識別情報に対応した生体情報を、利用者情報記憶部3が記憶する利用者情報から取得して、生体情報記憶部12bに格納する。

[0091] 具体的には、生体情報格納部13bは、図5に示すように、成功情報における識別番号に対応した生体情報である「指紋特徴量情報」を、利用者情報記憶部3が記憶する利用者情報から取得して、生体情報記憶部12bに格納する。

[0092] つまり、生体情報格納部13bは、「識別番号:00005」に対応する「特徴量00005」と、「識別番号:00100」に対応する「特徴量00100」と、「識別番号:00088」に対応する「特徴量00088」とを利用者情報記憶部3から取得し、生体情報記憶部12bにこれらを格納する(図5の(A)参照)。なお、図5は、実施例1における生体情報記憶部を説明するための図である。

[0093] ここで、生体情報格納部13bは、成功情報記憶部12aが記憶する成功情報が追加された場合、追加された成功情報における識別番号に対応した生体情報を利用者情報記憶部3が記憶する利用者情報から取得して、生体情報記憶部12bに追加して格納する。

[0094] すなわち、生体情報格納部13bは、図4の(B)に示すように、成功情報として新たに「識別番号:00001」が追加されると、「識別番号:00001」に対応する「指紋特徴量情報:特徴量00001」を利用者情報記憶部3から取得し、図5の(B)に示すように、生体情報記憶部12bに追加して格納する。

[0095] 第二認証部13cは、生体情報読み取り装置2から受信した生体情報と、生体情報記憶部12bが記憶している生体情報とを用いて利用者を認証する。具体的には、第二認証部13cは、受信した「指紋画像」から「指紋特徴量情報」を抽出し、生体情報記憶部12bが記憶している「指紋特徴量情報」に、抽出した「指紋特徴量情報」と一致する「指紋特徴量情報」が存在する場合は、利用者として認証する。すなわち、当該利用者に書籍を貸し出すことを認めると判定する。また、生体情報記憶部12bが記憶している「指紋特徴量情報」に、抽出した「指紋特徴量情報」と一致する「指紋特徴量情報」が存在しない場合は、利用者に書籍を貸し出すことを認めないと判定する。

[0096] 例えば、利用者(識別番号:00001)の「指紋画像」から抽出した「指紋特徴量情報」と一致する「指紋特徴量情報:特徴量00001」を、図5の(B)に示すように、生体情報記憶部12bが記憶しているので、利用者(識別番号:00001)に書籍を貸し出すことを認めると判定する。

[0097] 成功情報削除部13dは、所定の成功情報が記憶されてから所定の登録時間が経過したか否かを判定し、当該登録時間が経過した場合に、当該所定の成功情報を削除する。すなわち、成功情報削除部13dは、例えば、記憶部に記憶されている「登録時間:2時間」とする設定を参照し、成功情報ごとに、識別番号とともに記憶されている「第一の認証成功時刻」から「2時間」が経過したか否かを判定し、「第一の認証成功時刻」から「2時間」経過した成功情報がある場合は、当該成功情報を削除する。

[0098] より具体的には、「2007年4月2日午前11時00分」の時点で、図4の(C)に示すように、「第一の認証成功時刻」から「2時間」経過した「識別番号:00005」の成功情報を削除し、成功情報記憶部12aが記憶する成功情報を更新する。

[0099] ここで、生体情報格納部13bは、成功情報記憶部12aが記憶する成功情報が削除された場合、削除された成功情報における識別番号に対応した生体情報を削除する。すなわち、図5の(C)に示すように、「識別番号:00005」に対応した「特徴量00005」を削除し、生体情報記憶部12bが記憶する生体情報を更新する。

[0100] [実施例1における利用者認証装置による処理の手順]

次に、図6～8を用いて、実施例1における利用者認証装置10による処理を説明する。図6は、実施例1における利用者認証装置の第一の認証処理を説明するための

図であり、図7は、実施例1における利用者認証装置の成功情報および生体情報の削除処理を説明するための図であり、図8は、実施例1における利用者認証装置の第二の認証処理を説明するための図である。

[0101] [実施例1における利用者認証装置の第一の認証処理の手順]

図6に示すように、まず、実施例1における利用者認証装置10は、識別番号読み取り装置1から識別番号を受信すると(ステップS601肯定)、第一認証部13aは、識別番号読み取り装置1から受信した識別番号と、利用者情報記憶部3が記憶する利用者情報とを照合する(ステップS602)。すなわち、実施例1における利用者認証装置10は、識別番号読み取り装置1から書籍を返却する利用者の識別番号を受信すると、第一認証部13aは、受信した識別番号が、利用者情報記憶部3において利用者情報として登録されている識別番号に存在するか否か照合を行なう(ステップS603)。

[0102] そして、第一認証部13aは、利用者情報記憶部3において利用者情報として登録されている識別番号に、受信した識別番号と一致する識別番号が存在しない場合は(ステップS603否定)、「第一の認証不成功」と判定して利用者の図書館利用開始を不許可とし(ステップS604)、処理を終了する。

[0103] これに反して、第一認証部13aは、利用者情報記憶部3において利用者情報として登録されている識別番号に、受信した識別番号と一致する識別番号が存在する場合は(ステップS603肯定)、「第一の認証成功」と判定して利用者の図書館利用開始を許可する(ステップS605)。

[0104] そして、第一認証部13aは、新たに「第一の認証成功」と判定した利用者の「識別情報」と、当該「識別番号」を識別番号読み取り装置1から受信した時刻である「第一の認証成功時間」とを成功情報として成功情報記憶部12aに追加して格納する(ステップS606)。

[0105] 続いて、生体情報格納部13bは、追加された成功情報における識別番号に対応した生体情報を利用者情報記憶部3が記憶する利用者情報から取得して、生体情報記憶部12bに追加して格納し(ステップS607)、処理を終了する。すなわち、生体情報格納部13bは、図4の(B)に示すように、成功情報として新たに「識別番号:00001」が追加されると、「識別番号:00001」に対応する「指紋特徴量情報:特徴量0000

1」を利用者情報記憶部3から取得し、図5の(B)に示すように、生体情報記憶部12bに追加して格納する。

[0106] [実施例1における利用者認証装置の成功情報および生体情報の削除処理手順]

図7に示すように、実施例1における利用者認証装置10は、登録時間が経過した成功情報があるか否かを、常に判定する(ステップS701)。すなわち、成功情報削除部13dは、例えば、記憶部に記憶されている「登録時間:2時間」とする設定を参照し、成功情報ごとに、識別番号とともに記憶されている「第一の認証成功時刻」から「2時間」が経過したか否かを、常に判定する。

[0107] ここで、成功情報削除部13dは、登録時間が経過した成功情報があると判定した場合に(ステップS701肯定)、成功情報削除部13dは、当該成功情報を成功情報記憶部12aから削除する(ステップS702)。具体的には、成功情報削除部13dは、「2007年4月2日午前11時00分」の時点で、図4の(C)に示すように、「第一の認証成功時間」から「2時間」経過した「識別番号:00005」の成功情報を削除し、成功情報記憶部12aが記憶する成功情報を更新する。

[0108] そして、生体情報格納部13bは、削除された成功情報における識別番号に対応した生体情報を生体情報記憶部12bから削除して(ステップS703)、処理を終了する。具体的には、図5の(C)に示すように、「識別番号:00005」に対応した「特徴量00005」を削除し、生体情報記憶部12bが記憶する生体情報を更新する。

[0109] なお、本実施例では、成功情報削除部13dが、成功情報が記憶されてからの経過時間を、常に監視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、所定の時間ごと(例えば、5分ごと)に、成功情報が記憶されてからの経過時間を監視する場合であってもよい。

[0110] [実施例1における利用者認証装置の第二の認証処理の手順]

図8に示すように、まず、実施例1における利用者認証装置10は、生体情報読み取り装置2から生体情報を受信すると(ステップS801肯定)、第二認証部13cは、受信した生体情報と、生体情報記憶部12bに格納されている生体情報との照合を行なう(ステップS802)。具体的には、第二認証部13cは、受信した「指紋画像」から「指紋特徴量情報」を抽出し、生体情報記憶部12bが記憶している「指紋特徴量情報」に、

抽出した「指紋特徴量情報」と一致する「指紋特徴量情報」が存在するか否かを判定する。

[0111] そして、第二認証部13cは、生体情報記憶部12bが記憶している「指紋特徴量情報」に、抽出した「指紋特徴量情報」と一致する「指紋特徴量情報」が存在しない場合には(ステップS803否定)、利用者に書籍を貸し出すことを認めないとする「貸し出し不許可」を生体情報読み取り装置2に通知して(ステップS805)、処理を終了する。

[0112] これに反して、第二認証部13cは、生体情報記憶部12bが記憶している「指紋特徴量情報」に、抽出した「指紋特徴量情報」と一致する「指紋特徴量情報」が存在する場合には(ステップS803肯定)、利用者が書籍を貸し出すことを認めるとする「貸し出し許可」を生体情報読み取り装置2に通知して(ステップS804)、処理を終了する。

[0113] 例えば、利用者(識別番号:00001)の「指紋画像」から抽出した「指紋特徴量情報」と一致する「指紋特徴量情報:特徴量00001」を、図5の(B)に示すように、生体情報記憶部12bが記憶しているので、利用者(識別番号:00001)が書籍を貸し出すことを認めると判定する。

[0114] [実施例1の効果]

上記したように、実施例1によれば、図書館に登録される複数の利用者ごとに、各利用者を一意に識別するための識別情報と当該利用者の生体情報としての「指紋特徴量情報」とを対応付けた利用者情報を記憶し、書籍を返却する利用者から、当該利用者の識別情報を取得し、第一の認証として、取得された識別情報と、記憶された利用者情報とを用いて利用者の図書館利用開始を認証し、第一の認証が成功した利用者の識別情報を成功情報として記憶し、書籍を貸し出そうとする利用者の「指紋画像」を取得し、第二の認証として、取得された「指紋画像」から抽出した「指紋特徴量情報」と、記憶された「指紋特徴量情報」のうちで成功情報として記憶された利用者の識別情報に対応した「指紋特徴量情報」とを用いて利用者が書籍を貸し出すことを認証するので、書籍を返却することで図書館の利用開始を認証された利用者を、書籍貸し出し時における「1:N認証」の照合対象として絞り込むことができ、認証性能を向上することが可能になる

[0115] また、実施例1によれば、所定の成功情報が成功情報記憶部12aに記憶されてか

ら所定の登録時間が経過したか否かを判定し、当該登録時間が経過した場合に、当該所定の成功情報を成功情報記憶部12aから削除するので、例えば、図書館における利用開始が認証された利用者の中で、書籍などの貸し出し要求を行なう可能性が低くなった利用者を「1:N認証」の照合対象から除外することができ、認証性能を向上することが可能になる。

- [0116] また、実施例1によれば、成功情報として記憶されている利用者の識別情報に対応した「指紋特徴量情報」を利用者情報記憶部3から取得して生体情報記憶部12bに記憶し、第二の認証は、生体情報記憶部12bに記憶された「指紋特徴量情報」を用いて利用者を認証するので、「1:N認証」の際の処理速度を速くすることができ、認証性能を向上することが可能になる。

実施例 2

- [0117] 上述した実施例1では、成功情報の登録時間が利用者すべてにおいて同様に設定される場合について説明したが、実施例2では、成功情報の登録時間が利用者ごとに設定される場合について、図9を用いて説明する。なお、図9は、実施例2における利用者認証装置を説明するための図である。

- [0118] 実施例2における利用者認証装置は、図9の(A)に示すように、利用者ごとに割り振られた識別番号と、利用者ごとに設定される成功情報の登録時間とを対応付けてさらに記憶する。例えば、実施例2における利用者認証装置は、図9の(A)に示すように、「識別番号:00001」の「登録時間」を「2時間」として記憶し、「識別番号:00005」の「登録時間」を「3時間」として記憶し、「識別番号:00088」の「登録時間」を「1時間30分」として記憶し、「識別番号:00100」の「登録時間」を「4時間」として記憶する。

- [0119] そして、実施例2における成功情報削除部13dは、所定の成功情報が成功情報記憶部12aに記憶されてから、利用者ごとに設定された登録時間が経過したか否かを判定して、設定された登録時間が経過した場合に、当該所定の成功情報を成功情報記憶部12aから削除する。

- [0120] 例えば、実施例2における成功情報削除部13dは、図9の(B)に示すように、「2007年4月2日午前11時35分」の時点で、「識別番号:00088、第一の認証成功時刻:

2007年4月2日午前10時05分」の成功情報は、「識別番号:00088」の「登録時間」である「1時間30分」が経過していると判定する。そして、実施例2における成功情報削除部13dは、当該成功情報を削除して、成功情報記憶部12aの成功情報を更新する(図9の(B)の(1)参照)。

[0121] そして、実施例2における生体情報格納部13bは、実施例1と同様に、成功情報記憶部12aの成功情報が削除されて更新されると、削除された成功情報の識別番号に対応する生体情報(指紋特徴量情報)を削除して、生体情報記憶部12bの生体情報を更新する(図9の(B)の(2)参照)。

[0122] このようなことから、実施例2における利用者認証装置は、図書館における利用者ごとの行動履歴に基づいて利用者それぞれに登録時間を設定することで、「1:N認証」の照合対象を利用者それぞれの特性に基づいて柔軟に絞り込むことができ、認証性能を向上することが可能になる。

実施例 3

[0123] 上述した実施例1では、第一の認証が成功した利用者の生体情報を第二の認証の照合対象に追加する場合について説明したが、実施例3では、第一の認証が成功した利用者の生体情報とともに、当該利用者が所属するグループの利用者の生体情報も第二の認証の照合対象に追加する場合について、図10を用いて説明する。なお、図10は、実施例3における利用者認証装置を説明するための図である。

[0124] 実施例3における利用者認証装置は、各利用者が属するグループを一意に識別する「グループ情報」を、利用者の「識別情報」に対応付けてさらに記憶する。具体的には、図10に示すように、実施例3における利用者情報記憶部3は、「グループ情報」を、「識別番号」と「指紋特徴量情報」とに対応付けて記憶する。例えば、図書館の利用者として登録されている「識別情報:00001」の利用者と、「識別情報:00002」の利用者および「識別情報:00003」の利用者とは、同じ家族であることから、「グループ情報:1」が与えられている。なお、「識別情報:00005」の利用者、「識別情報:00088」の利用者および「識別情報:00100」の利用者には、「グループ情報:なし」が与えられているとする。

[0125] そして、実施例3における成功情報記憶部12aは、第一認証部13aによる認証が成

功した利用者の識別情報の他に、当該利用者のグループ情報に対応する他の利用者の識別情報も成功情報として記憶する。

[0126] すなわち、実施例3における第一認証部13aは、実施例1と同様に、図10に示すように、貸し出していた書籍を返却するために家族とともに図書館に来館した「識別番号:00001」の利用者が「2007年4月2日午前10時10分」に提示したICカードから、識別番号読み取り装置1を介して、「識別番号:00001」を取得し、取得された「識別番号:00001」が利用者情報として登録されている識別番号に存在しているので、「第一の認証成功」と判定し、利用者(識別番号:00001)の図書館利用開始を許可する。

[0127] そして、実施例3における第一認証部13aは、「第一の認証成功」と判定された「識別番号:00001」の他に、「識別番号:00001」に与えられた「グループ情報:1」に対応する「識別情報:00002」および「識別情報:00003」を「第一の認証成功時刻:2007年4月2日午前10時10分」とともに、成功情報として追加して成功情報記憶部12aに格納する。これにより、生体情報格納部13bは、「識別番号:00001」に対応する「指紋特徴量情報:特徴量00001」と、「識別番号:00002」に対応する「指紋特徴量情報:特徴量00002」と、「識別番号:00003」に対応する「指紋特徴量情報:特徴量00003」とを、生体情報記憶部12bに追加して格納する。

[0128] このようなことから、実施例3における利用者認証装置は、図書館の利用開始が認証された利用者と同様に、貸し出し時において認証要求を行なう可能性の高い利用者を「1:N認証」の照合対象に加えることができ、認証性能を向上することが可能になる。

実施例 4

[0129] 上述した実施例1および2では、設定された成功情報の登録時間が一定である場合について説明したが、実施例4では、設定された成功情報の登録時間を、状況に応じて短縮して再設定する場合について、図11を用いて説明する。なお、図11は、実施例4における利用者認証装置を説明するための図である。

[0130] 実施例4における利用者認証装置は、成功情報記憶部12aに記憶された成功情報の個数が所定値以上になった場合に、当該所定値未満に際して判定に用いられる

登録時間よりも短い登録時間を用いて、当該登録時間が経過したか否かを判定する。

[0131] 例えば、実施例1において、図11の(A)に示すように、第一認証部13aによって、100個目の成功情報として「識別番号:00105、第一の認証成功時刻:2007年4月2日午前10時30分」が成功情報記憶部12aに格納された場合、実施例4における成功情報削除部13dは、成功情報記憶部12aに記憶された成功情報の個数が「閾値個数」として設定された「100個」以上となったので、記憶部に「2時間」として記憶されていた「登録時間」を、「1時間」に短縮して再設定する。

[0132] そして、実施例4における成功情報削除部13dは、「2007年4月2日午前10時30分」の時点で、再設定された「登録時間:1時間」を経過している「識別番号:00005」の成功情報および「識別番号:00100」の成功情報を削除する。

[0133] ところで、この場合には、利用者認証装置は、図11の(A)に示す状況が、実施例2において発生した場合に対応するために、図11の(B)に示すように、利用者ごとの「識別情報」に対応付けて、「登録時間」を設定して記憶するとともに、「短縮登録時間」をさらに設定して記憶するようにしてもよい。例えば、実施例4における利用者認証装置は、図11の(B)に示すように、「識別番号:00001」の「短縮登録時間」を「1時間」として記憶し、「識別番号:00005」の「短縮登録時間」を「1時間30分」として記憶し、「識別番号:00088」の「短縮登録時間」を「1時間」として記憶し、「識別番号:00100」の「短縮登録時間」を「1時間」として記憶する。

[0134] そして、実施例4における成功情報削除部13dは、成功情報記憶部12aに記憶された成功情報の個数が「閾値個数」として設定された「100個」以上になると、成功情報が成功情報記憶部12aに格納されてからの時間が、「短縮登録時間」を経過したしたか否かを判定し、「短縮登録時間」を経過した成功情報を削除する。例えば、実施例4における成功情報削除部13dは、「2007年4月2日午前10時30分」の時点で、「短縮登録時間」を経過している「識別番号:00001」の成功情報を削除する。

[0135] なお、実施例4における生体情報格納部13bは、実施例1および2と同様に、成功情報記憶部12aの成功情報が削除されて更新されると、削除された成功情報の識別番号に対応する生体情報(指紋特徴量情報)を削除して、生体情報記憶部12bの生

体情報を更新する。

- [0136] このようなことから、実施例4における利用者認証装置は、成功情報の個数が膨大になった場合でも、登録時間を短縮することで「1:N認証」の照合対象を減少させて照合処理にかかる時間を速くすることができ、認証性能を向上することが可能になる。

実施例 5

- [0137] 上述した実施例4では、成功情報の個数が所定の個数以上となると、設定された成功情報の登録時間を短縮して照合対象を減少する場合について説明したが、実施例5では、成功情報の個数が所定の個数以上となると、利用者の利用頻度を参照して照合対象を減少する場合について、図12を用いて説明する。なお、図12は、実施例5における利用者認証装置を説明するための図である。

- [0138] 実施例5における利用者認証装置は、利用者の利用頻度として、所定の物品を返却した利用者が、同日に所定の物品を貸し出す頻度である「同日貸し出し頻度」を記憶する。すなわち、図書館において、書籍を返却した利用者が、同日に新たに書籍を別途貸し出す頻度である「同日貸し出し頻度」を、利用者ごとに割り振られた「識別番号」に対応付けて記憶する。例えば、図12に示すように、「同日貸し出し頻度:90%」を「識別情報:00001」に対応付けて記憶し、「同日貸し出し頻度:70%」を「識別情報:00005」に対応付けて記憶し、「同日貸し出し頻度:20%」を「識別情報:00088」に対応付けて記憶し、「同日貸し出し頻度:95%」を「識別情報:00100」に対応付けて記憶し、「同日貸し出し頻度:98%」を「識別情報:00105」に対応付けて記憶する。

- [0139] そして、実施例5における成功情報削除部13dは、成功情報記憶部12aに記憶された成功情報の個数が所定値以上になった場合に、各利用者の利用頻度としての「同日貸し出し頻度」に基づいて、当該「同日貸し出し頻度」が所定値よりも低い利用者の成功情報を成功情報記憶部12aからさらに削除する。例えば、図12に示すように、第一認証部13aによって、100個目の成功情報として「識別番号:00105、第一の認証成功時刻:2007年4月2日午前10時30分」が成功情報記憶部12aに格納された場合、実施例4における成功情報削除部13dは、成功情報記憶部12aに記憶さ

れた成功情報の個数が「閾値個数」として設定された「100個」以上になったので、「同日貸し出し頻度:30%」以下である「識別番号:00088」に対応する成功情報を削除する。

[0140] そして、実施例5における生体情報格納部13bは、実施例1、2および4と同様に、成功情報記憶部12aの成功情報が削除されて更新されると、削除された成功情報の識別番号に対応する生体情報(指紋特徴量情報)を削除して、生体情報記憶部12bの生体情報を更新する。

[0141] このようなことから、実施例5における利用者認証装置は、成功情報の個数が膨大になった場合でも、図書館において書籍の貸し出し要求のための認証要求を行なう可能性が低い利用者の成功情報を削除することで「1:N認証」の照合対象を減少させて照合処理にかかる時間を速くすることができ、認証性能を向上することが可能になる。

実施例 6

[0142] 上述した実施例1～5では、利用者認証としての第一の認証および第二の認証を、一つの装置で行なう場合について説明したが、実施例6では、利用者認証としての第一の認証および第二の認証を、別々に設置される装置にて行なう利用者認証システムについて説明する。

[0143] [実施例6における利用者認証システムの概要および特徴]

まず最初に、図13～15を用いて、実施例6における利用者認証システムの主たる特徴を具体的に説明する。図13～15は、実施例6における利用者認証システムの概要および特徴を説明するための図である。

[0144] 実施例6における利用者認証システムは、図13に示すように、施設に設けられた領域内における利用者の入退室管理を、第一の認証によって管理する入退室管理装置と、領域内に設置される情報端末の利用者による利用開始管理を、第二の認証によって管理する利用者認証装置とから構成される。

[0145] 実施例6における利用者認証システムを構成する入退室管理装置は、利用者が領域内に入室する場合に、当該利用者の識別情報を取得する。すなわち、領域外に設置される領域外読み取り装置を介して、領域内への入室を要求する利用者の本人

証拠として、「識別番号」を取得する。例えば、図13に示すように、領域外読み取り装置(識別番号:out001)を介して、領域内への入室を要求する利用者の「識別番号:00001」を取得する。ここで、実施例6における利用者認証システムを構成する入退室管理装置は、「識別番号:00001」とともに、利用者の識別番号を読み取った領域外読み取り装置の「識別番号:out001」も同時に取得する。

[0146] そして、実施例6における利用者認証システムを構成する入退室管理装置は、第一の認証として、取得した「利用者の識別番号」と、領域入出権限管理データベースが記憶する「領域内への入出権限が与えられている利用者の識別情報」とを用いて、利用者を認証する。また、「利用者の識別番号」と同時に取得した「領域外読み取り装置の識別番号」と、領域入出権限管理データベースが記憶する「領域内への入室管理をするために設置された領域外読み取り装置の識別情報」とをさらに用いて、利用者を認証する。

[0147] すなわち、領域入出権限管理データベースが記憶する利用者の「識別番号」の中に、領域内への入室を要求する利用者の「識別番号:00001」と一致するものがあり、かつ、領域入出権限管理データベースが記憶する領域外読み取り装置の「識別情報」の中に、領域外読み取り装置の「識別番号:out001」と一致するものがある場合に、「第一の認証成功」と判定して、「識別番号:00001」の利用者が領域内へ入室することを許可し、例えば、図13に示すように、領域内と領域外の境界に設置された扉に制御信号を送信して、当該扉を開錠する。一方、取得した利用者の「識別番号:00001」または領域外読み取り装置の「識別番号:out001」のうち、どちらか一方でも領域入出権限管理データベースに該当するものがない場合は、「第一の認証不成功」と判定して、「識別番号:00001」の利用者が領域内へ入室することを許可しないと、扉に制御信号を送信して、当該扉を施錠したままにする。

[0148] そして、実施例6における利用者認証システムを構成する入退室管理装置は、第一の認証によって、領域内への入室が成功した利用者の識別情報を成功情報として領域内利用者データベースに格納する。例えば、図13に示すように、新たに領域内への入室が許可された利用者の「識別番号:00001」を、領域内利用者データベースに追加して格納する。

- [0149] そして、実施例6における利用者認証システムを構成する入退室管理装置は、領域内利用者データベースにおいて追加更新された成功情報としての識別番号を、データベース連携ポリシーを参照して、該当する利用者認証装置に通知する。ここで、データベース連携ポリシーは、入退室管理装置と連携して第二の認証を行なう利用者認証装置を特定する情報を記憶している。また、実施例6における利用者認証システムを構成する入退室管理装置は、追加更新された識別番号とともに、自身を一意に特定するための情報である識別番号を、該当する利用者認証装置に伝達する。例えば、図13に示すように、追加更新された「識別番号:00001」と、入退室管理装置の識別番号である「A001」とを、データベース連携ポリシーを参照して、該当する利用者認証装置に通知する。
- [0150] そして、実施例6における利用者認証システムを構成する利用者認証装置は、入退室管理装置から受信した利用者の「識別番号」を、利用者認証対象者データベースに格納する。その際、実施例6における利用者認証システムを構成する利用者認証装置は、データベース連携ポリシーを参照して、利用者の「識別番号」とともに受信した入退室管理装置の識別番号が、自身と連携して第一の認証を行なう入退室管理装置の識別番号であり、かつ、認証対象者選別ポリシーを参照して、受信した利用者の「識別番号」が、当該領域内において情報端末を利用することを認証要求する許可された利用者の「識別番号」に含まれている場合のみ、受信した利用者の「識別番号」を、利用者認証対象者データベースに格納する。
- [0151] 例えば、実施例6における利用者認証システムを構成する利用者認証装置は、図13に示すように、入退室管理装置の識別番号である「A001」がデータベース連携ポリシーを満たし、かつ、追加更新された「識別番号:00001」が認証対象者選別ポリシーを満たすので、利用者認証対象者データベースに「識別番号:00001」を追加して格納する。
- [0152] ところで、実施例6における利用者認証システムを構成する利用者認証装置は、複数の利用者ごとに、各利用者を一意に識別するための識別情報と当該利用者の生体情報とを対応付けた利用者情報を予め記憶する。具体的には、実施例6における利用者認証システムを構成する利用者認証装置は、領域内の利用者として予め登

録された複数の利用者ごとに、各利用者を一意に識別するための識別情報と、当該利用者の生体情報である「指紋画像」から抽出した「指紋特徴量情報」とを対応付けた生体情報データベースを記憶する。例えば、図14に示すように、生体情報データベースとして、「識別番号:00001」と、「指紋特徴量情報:特徴量00001」とを対応付けて記憶する。

[0153] そして、実施例6における利用者認証システムを構成する利用者認証装置は、領域内に設置される情報端末へログインするための認証要求を行なう利用者から、当該情報端末に接続される生体情報読み取り装置を介して、生体情報としての「指紋画像」を取得する。ここで、実施例6における利用者認証システムを構成する利用者認証装置は、生体情報としての「指紋画像」とともに、当該生体情報を読み取った生体情報読み取り装置の識別番号と、当該生体情報読み取り装置に接続される情報端末の識別番号とを取得する。

[0154] 例えば、実施例6における利用者認証システムを構成する利用者認証装置は、図14に示すように、「識別番号:00001」の利用者から生体情報としての「指紋画像」とともに、当該生体情報を読み取った生体情報読み取り装置の「識別番号:S001」と、当該生体情報読み取り装置に接続される情報端末の「識別番号:C001」とを取得する。ここで、実施例6における利用者認証システムを構成する利用者認証装置は、端末センサデータベースを参照して、受信した情報端末の識別番号と生体情報読み取り装置の識別番号との組み合わせが正当なものであることを確認した場合のみ、利用者からの情報端末へログインするための認証要求に対応して、第二の認証を行なう。例えば、図14に示すように、情報端末の「識別番号:C001」と生体情報読み取り装置の「識別番号:S001」との組み合わせが正当なので、「識別番号:00001」の利用者から情報端末へログインするための認証要求に対応して、第二の認証を行なう。

[0155] そして、実施例6における利用者認証システムを構成する利用者認証装置は、第二の認証として、取得された生体情報と、記憶された生体情報のうちで成功情報として利用者認証対象者データベースに記憶された利用者の識別情報に対応した生体情報とを用いて利用者を認証する。具体的には、実施例6における利用者認証システムを構成する利用者認証装置は、図14に示すように、端末利用権限データベース

をさらに参照して、「ログイン要求を行なっている情報端末(識別番号:C001)」において利用権限を与えられている利用者」であり、かつ、「利用者認証対象者データベースに登録されている利用者」である利用者の識別番号を選別し、選別した識別番号に対応した生体情報のみを生体情報データベースから読み出し、取得された生体情報と、読み出された生体情報とを用いて利用者を認証する。

[0156] すなわち、取得された生体情報である「指紋画像」から「指紋特徴量情報」を抽出し、選別された生体情報としての「指紋特徴量情報」の中に、抽出された「指紋特徴量情報」と一致する「指紋特徴量情報」が存在する場合は、利用者として認証する。すなわち、当該利用者が、情報端末(識別番号:C001)にログインすることを認めると判定する。一方、選別された生体情報としての「指紋特徴量情報」の中に、抽出された「指紋特徴量情報」と一致する「指紋特徴量情報」が存在しない場合は、利用者が、情報端末(識別番号:C001)にログインすることを認めないと判定する。

[0157] 例えば、図14に示すように、利用者(識別番号:00001)の「指紋画像」から抽出した「指紋特徴量情報」と一致する「指紋特徴量情報:特徴量00001」が、選別された「指紋特徴量情報」に存在する場合は、利用者(識別番号:00001)が情報端末(識別番号:C001)にログインすることを認めると判定する。

[0158] 一方、実施例6における利用者認証システムを構成する入退室管理装置は、利用者が領域内に設置される情報端末の利用を終了して領域内から退室する場合においても、当該利用者の識別情報を取得する。すなわち、領域内に設置される領域内読み取り装置を介して、領域内からの退室を要求する利用者の本人証拠として、「識別番号」を取得する。例えば、図15に示すように、領域内読み取り装置(識別番号:in001)を介して、領域内からの退室を要求する利用者の「識別番号:00001」を取得する。ここで、実施例6における利用者認証システムを構成する入退室管理装置は、「識別番号:00001」とともに、利用者の識別番号を読み取った領域内読み取り装置の「識別番号:in001」も同時に取得する。

[0159] そして、実施例6における利用者認証システムを構成する入退室管理装置は、第一の認証として、取得した「利用者の識別番号」と、領域入出権限管理データベースが記憶する「領域内への入出権限が与えられている利用者の識別情報」とを用いて、

利用者を認証する。また、「利用者の識別番号」と同時に取得した「領域内読み取り装置の識別番号」と、領域入出権限管理データベースが記憶する「領域内からの退室管理をするために設置された領域内読み取り装置の識別情報」とをさらに用いて、利用者を認証する。

[0160] すなわち、領域入出権限管理データベースが記憶する利用者の「識別番号」の中に、領域内からの退室を要求する利用者の「識別番号:00001」と一致するものがあり、かつ、領域入出権限管理データベースが記憶する領域内読み取り装置の「識別情報」の中に、領域内読み取り装置の「識別番号:in001」と一致するものがある場合に、「第一の認証成功」と判定して、「識別番号:00001」の利用者が領域内から退室することを許可し、例えば、領域内と領域外の境界に設置された扉を開錠する。

[0161] そして、実施例6における利用者認証システムを構成する入退室管理装置は、第一の認証によって、領域内からの退室が成功した利用者の識別情報を領域内利用者データベースが記憶する成功情報から削除して更新する。例えば、図15に示すように、新たに領域内からの退室が許可された利用者の「識別番号:00001」を、領域内利用者データベースから削除して更新する。

[0162] そして、実施例6における利用者認証システムを構成する入退室管理装置は、領域内利用者データベースにおいて削除更新された成功情報としての識別番号を、データベース連携ポリシーを参照して、該当する利用者認証装置に通知する。また、実施例6における利用者認証システムを構成する入退室管理装置は、追加更新された識別番号とともに、自身を一意に特定するための情報である識別番号を、該当する利用者認証装置に伝達する。例えば、図15に示すように、削除更新された「識別番号:00001」と、入退室管理装置の識別番号である「A001」とを、データベース連携ポリシーを参照して、該当する利用者認証装置に通知する。

[0163] そして、実施例6における利用者認証システムを構成する利用者認証装置は、入退室管理装置から受信した利用者の「識別番号」を、利用者認証対象者データベースから削除して更新する。その際、実施例6における利用者認証システムを構成する利用者認証装置は、データベース連携ポリシーを参照して、利用者の「識別番号」とともに受信した入退室管理装置の識別番号が、自身と連携して第一の認証を行なう

入退室管理装置の識別番号であり、かつ、認証対象者選別ポリシーを参照して、受信した利用者の「識別番号」が、当該領域内において情報端末を利用することを認証要求する許可された利用者の「識別番号」に含まれている場合のみ、受信した利用者の「識別番号」を、利用者認証対象者データベースから削除する。

[0164] 例えば、実施例6における利用者認証システムを構成する利用者認証装置は、図15に示すように、入退室管理装置の識別番号である「A001」がデータベース連携ポリシーを満たし、かつ、追加更新された「識別番号:00001」が認証対象者選別ポリシーを満たすので、利用者認証対象者データベースから「識別番号:00001」を削除して更新する。

[0165] このようなことから、実施例1における利用者認証装置は、領域内への入室が認証された利用者のみを、領域内に設置される情報端末のログイン時における「1:N認証」の照合対象として絞り込むことができ、認証性能を向上することが可能になる。

[0166] [実施例6における入退室管理装置の構成]

次に、図16などを用いて、実施例6における入退室管理装置を説明する。図16は、実施例6における入退室管理装置の構成を示すブロック図である。

[0167] 図16に示すように、実施例6における入退室管理装置20は、通信制御I/F部21と、記憶部22と、処理部23とから構成され、さらに、領域外読み取り装置4と、領域内読み取り装置5と、扉6と、利用者認証装置30とに接続される。

[0168] 領域外読み取り装置4は、利用者が領域内に入室する場合に、当該利用者の識別情報を取得し、取得した識別番号を入退室管理装置20に送信する。すなわち、領域外読み取り装置4は、領域外に設置され、領域内への入室を要求する利用者から本人証拠として、「識別番号」を取得する。例えば、図13に示すように、領域外読み取り装置4(識別番号:out001)は、領域内への入室を要求する利用者の「識別番号:00001」を取得し、取得した「識別番号:00001」と、自身の「識別番号:out001」とを入退室管理装置20に送信する。

[0169] 領域内読み取り装置5は、利用者が領域内から退室する場合に、当該利用者の識別情報を取得し、取得した識別番号を入退室管理装置20に送信する。すなわち、領域内読み取り装置5は、領域内に設置され、領域内からの退室を要求する利用者か

ら本人証拠として、「識別番号」を取得する。例えば、図15に示すように、領域内読み取り装置5(識別番号:in001)は、領域内からの退室を要求する利用者の「識別番号:00001」を取得し、取得した「識別番号:00001」と、自身の「識別番号:in001」とを入退室管理装置20に送信する。

[0170] 扉6は、領域内と領域外の境界に設置される。領域外読み取り装置4や領域内読み取り装置5から送信された利用者の「識別番号」を用いて、後述する第一認証部23aが「第一の認証」を行なった結果が「第一の認証成功」の場合、扉6は施錠から開錠の状態となり、「第一の認証不成功」の場合、扉6は施錠状態のままとなる。

[0171] 利用者認証装置30は、領域内に設置される情報端末の利用者による利用を、第二の認証によって管理する。なお、これについては後に詳述する。

[0172] 通信制御I/F部21は、領域外読み取り装置4、領域内読み取り装置5、扉6および利用者認証装置30と、記憶部22および処理部23との間でやり取りする各種情報に関する通信を制御する。例えば、領域外読み取り装置4や領域内読み取り装置5が送信した識別番号を、処理部23に転送したり、後述するデータベース連携部23bによる利用者の識別番号の更新内容の通知を、利用者認証装置30に転送したりする。

[0173] 記憶部22は、後述する処理部23による各種処理結果などを記憶し、特に本発明に密接に関連するものとしては、図16に示すように、領域入出権限管理記憶部22aと、領域内利用者記憶部22bと、データベース連携ポリシー記憶部22cとを備える。

[0174] 領域入出権限管理記憶部22aは、「領域内への入出権限が与えられている利用者の識別情報」を、領域の内外に設置される領域外読み取り装置4および領域内読み取り装置5の識別番号と対応付けて記憶する。例えば、図17に示すように、領域外読み取り装置4の識別番号である「out001」および領域内読み取り装置5の識別番号である「in001」と、「領域内への入出権限が与えられている利用者の識別情報」である「00001、00002、00003」などを対応付けて記憶する。なお、図17は、実施例6における領域入出権限記憶部を説明するための図である。

[0175] 領域内利用者記憶部22bは、後述する第一認証部23aが、領域外読み取り装置4や領域内読み取り装置5から受信した利用者の識別番号を認証した結果を記憶する。なお、領域内利用者記憶部22bについては、後に詳述する。

- [0176] データベース連携ポリシー記憶部22cは、入退室管理装置20と連携して第二の認証を行なう利用者認証装置を特定する情報を記憶する。例えば、入退室管理装置20と連携して第二の認証を行なう利用者認証装置は、利用者認証装置30であると記憶する。
- [0177] 処理部23は、各種処理を実行し、特に本発明に密接に関連するものとしては、図16に示すように、第一認証部23aと、データベース連携部23bとを備える。
- [0178] 第一認証部23aは、領域外読み取り装置4もしくは領域内読み取り装置5から受信した「利用者の識別番号」と、当該「利用者の識別番号」を取得した領域外読み取り装置4もしくは領域内読み取り装置5の識別番号と、領域入出権限管理記憶部22aが記憶する「領域内への入出権限が与えられている利用者の識別情報」とを用いて、利用者を認証する。例えば、第一認証部23aは、利用者の「識別番号:00001」と、領域外読み取り装置4の「識別番号:out001」とを受信すると、図17に示す領域入出権限管理記憶部22aが記憶する組み合わせを参照して、これらの識別番号が正しい組み合わせであると判定して、「識別番号:00001」の利用者が領域内へ入室することを許可し、扉6に制御信号を送信して、扉6を施錠から開錠の状態にする。
- [0179] また、第一認証部23aは、利用者の「識別番号:00001」と、領域内読み取り装置5の「識別番号:in001」とを受信すると、図17に示す領域入出権限管理記憶部22aが記憶する組み合わせを参照して、これらの識別番号が正しい組み合わせであると判定して、「識別番号:00001」の利用者が領域内から退室することを許可し、扉6に制御信号を送信して、扉6を施錠から開錠の状態にする。
- [0180] また、第一認証部23aは、受信した「利用者の識別番号」と、当該「利用者の識別番号」を取得した領域外読み取り装置4もしくは領域内読み取り装置5の識別番号との組み合わせが正しい組み合わせではない場合は、「識別番号:00001」の利用者が領域内へ入室することや、領域内から退室することを許可せず、扉6に制御信号を送信して、扉6を施錠状態のままにする。
- [0181] さらに、第一認証部23aは、領域内への入室が成功した利用者の識別情報を成功情報として領域内利用者記憶部22bに追加して格納する。例えば、図13に示すように、新たに領域内への入室が許可された利用者の「識別番号:00001」を、領域内

利用者記憶部22bに追加して格納する。また、領域内からの退室が成功した利用者の識別情報を成功情報として領域内利用者データベースが記憶する成功情報から削除して更新する。例えば、図15に示すように、新たに領域内からの退室が許可された利用者の「識別番号:00001」を、領域内利用者データベースから削除して更新する。

[0182] データベース連携部23bは、領域内利用者記憶部22bが記憶する成功情報が更新されると、データベース連携ポリシー記憶部22cを参照して、成功情報の更新内容および入退室管理装置20の識別番号を、該当する利用者認証装置に通知する。例えば、図13に示すように、追加更新された「識別番号:00001」と、入退室管理装置の識別番号である「A001」とを、データベース連携ポリシーを参照して、該当する利用者認証装置30に通知する。また、図15に示すように、削除更新された「識別番号:00001」と、入退室管理装置の識別番号である「A001」とを、データベース連携ポリシーを参照して、該当する利用者認証装置30に通知する。

[0183] なお、ここでは、領域内利用者記憶部22bが更新されるたびに、データベース連携部23bが利用者認証装置に通知する場合について説明したが、成功情報が複数たまと、それを、まとめて送るようにしてもよい。これにより、成功情報の追加および削除を一括して実行して「1:N認証」の照合対象を絞り込むことができ、認証性能を向上することが可能になる。

[0184] また、成功情報を複数まとめる際には、所定の時間毎に、当該所定時間内にたまつた成功情報を、まとめて送るようにしてもよい。これにより、一定間隔で成功情報の更新処理を行なつて、更新処理に要する装置の負荷を軽減でき、認証性能を向上することが可能になる。

[0185] [実施例6における利用者認証装置の構成]

次に、図18などを用いて、実施例6における利用者認証装置を説明する。図18は、実施例6における利用者認証装置の構成を示すブロック図である。

[0186] 図18に示すように、実施例6における利用者認証装置30は、通信制御I/F部31と、記憶部32と、処理部33とから構成され、さらに、生体情報読み取り装置8と、生体情報記憶部9と、入退室管理装置20とに接続される。また、生体情報読み取り装置8

は、さらに情報端末7に接続される。

[0187] 情報端末7は、領域内に設置されるコンピュータなどの情報端末である。また、生体情報読み取り装置8は、情報端末7と対応付けて接続される生体情報読み取り装置である。生体情報読み取り装置8は、領域内に設置される情報端末7へログインするための認証要求を行なう利用者から、生体情報としての「指紋画像」を取得し、取得した「指紋画像」を利用者認証装置30に送信する。なお、図18では、情報端末7と生体情報読み取り装置8の組み合わせを一つのみ示しているが、本実施例では、さらに情報端末と生体情報読み取り装置の組み合わせが複数存在し、生体情報読み取り装置それぞれが、利用者認証装置と接続されているものとする。

[0188] 生体情報記憶部9は、複数の利用者ごとに、各利用者を一意に識別するための識別情報と当該利用者の生体情報とを対応付けた利用者情報を記憶する。具体的には、領域内の利用者として登録された複数の利用者ごとに、各利用者を一意に識別するための識別情報と、当該利用者の生体情報である「指紋画像」から抽出した「指紋特徴量情報」とを対応付けた利用者情報を記憶する。例えば、図19に示すように、利用者情報として、「識別番号:00001」と、「指紋特徴量情報:特徴量00001」とを対応付けて記憶する。なお、図19は、実施例6における生体情報記憶部を説明するための図である。

[0189] 通信制御I/F部31は、情報端末7、生体情報読み取り装置8、入退室管理装置20および生体情報記憶部9と、記憶部32および処理部33との間でやり取りする各種情報に関する通信を制御する。例えば、情報端末7の識別番号や、生体情報読み取り装置8の識別番号や、生体情報読み取り装置8が取得した「指紋画像」や、入退室管理装置20が送信した成功情報の更新内容を処理部33に転送したり、後述する第二認証部33fが生体情報記憶部9から取得した生体情報を、記憶部32に転送したりする。

[0190] 記憶部32は、後述する処理部33による各種処理に用いるデータや、後述する処理部33による各種処理結果などを記憶し、特に本発明に密接に関連するものとしては、図18に示すように、データベース連携ポリシー記憶部32aと、認証対象者選別ポリシー記憶部32bと、利用者認証対象者記憶部32cと、端末センサ記憶部32dと、端

末装置利用権限記憶部32eと、照合対象者選別結果記憶部32fと、照合対象者生体情報記憶部32gとを備える。

[0191] データベース連携ポリシー記憶部32aは、利用者認証装置30と連携して第一の認証を行なう入退室管理装置を特定する情報を記憶する。例えば、データベース連携ポリシー記憶部32aは、利用者認証装置30と連携して第一の認証を行なう入退室管理装置の識別番号は「A001」とであると記憶する。

[0192] 認証対象者選別ポリシー記憶部32bは、領域内において情報端末7を含む情報端末を利用することを許可された利用者の「識別番号」を記憶する。例えば、利用者の「識別番号:00001」を、領域内において情報端末7を含む情報端末を利用することを許可された利用者の「識別番号」として記憶する。

[0193] 端末センサ記憶部32dは、情報端末および当該情報端末に接続される生体情報読み取り装置それぞれの識別番号の組み合わせを記憶する。すなわち、図21に示すように、情報端末7の識別番号は「C001」であり、情報端末7に接続される生体情報読み取り装置8の識別番号は「S001」とであると記憶する。なお、図21は、実施例6における端末センサ記憶部を説明するための図である。

[0194] 端末装置利用権限記憶部32eは、領域内に設置される情報端末の識別番号ごとに、当該情報端末の利用権限が与えられている利用者の識別番号を対応付けて記憶する。例えば、図22に示すように、「識別番号:C001」の情報端末7を利用する権限が与えられている利用者の識別番号は、「00001」や、「00005」や、「00088」や、「00100」などであると記憶する。なお、図22は、実施例6における端末装置利用権限記憶部を説明するための図である。

[0195] 利用者認証対象者記憶部32cは、入退室管理装置20から受信した成功情報の更新内容のうち、後述するデータベース連携部33aが正当と判定した成功情報の更新内容を記憶し、照合対象者選別結果記憶部32fは、後述する照合対象者選別部33dが照合対象として選別した利用者の識別情報を記憶し、照合対象者生体情報記憶部32gは、後述する照合対象者生体情報選別部33eが、照合対象者選別結果記憶部32fが記憶する利用者の識別番号に対応する生体情報を生体情報記憶部9から取得して記憶する。なお、これら各記憶部に関しては、後に詳述する。

- [0196] 処理部33は、各種処理を実行し、特に本発明に密接に関連するものとしては、図18に示すように、データベース連携部33aと、認証要求処理部33bと、照合用データ作成部33cと、照合対象者選別部33dと、照合対象者生体情報選別部33eと、第二認証部33fとを備える。
- [0197] データベース連携部33aは、入退室管理装置20から受信した成功情報(利用者の識別番号)の追加更新内容を、利用者認証対象者記憶部32cに格納する。例えば、データベース連携部33aは、図13に示すように、データベース連携ポリシー記憶部32aを参照して、成功情報(利用者の識別番号)の更新内容とともに受信した入退室管理装置20の識別番号(A001)が、利用者認証装置30と連携して第一の認証を行なう入退室管理装置20の識別番号であると判定し、さらに認証対象者選別ポリシー記憶部32bを参照して、追加更新内容である利用者の識別番号「00001」に問題なしと判定すると、図20に示すように、利用者の「識別番号:00001」を、利用者認証対象者記憶部32cに追加して格納する。なお、図20は、実施例6における利用者認証対象者記憶部を説明するための図である。
- [0198] また、データベース連携部33aは、図15に示すように、データベース連携ポリシー記憶部32aを参照して、成功情報(利用者の識別番号)の削除更新内容とともに受信した入退室管理装置20の識別番号(A001)が、利用者認証装置30と連携して第一の認証を行なう入退室管理装置20の識別番号であると判定し、さらに認証対象者選別ポリシー記憶部32bを参照して、削除更新内容である利用者の識別番号「00001」に問題なしと判定すると、利用者の「識別番号:00001」を、利用者認証対象者記憶部32cから削除する。
- [0199] なお、ここでは、データベース連携部33aが入退室管理装置20から受信した更新内容に基づいてデータベース連携ポリシー記憶部32aを更新する場合について説明したが、データベース連携ポリシー記憶部32aが、所定の利用者の識別情報を成功情報として常に記憶しておいてもよい。これにより、例えば、取締役などの役職にある利用者を「1:N認証」の照合対象として常に設定するなど、利用者のニーズに柔軟に対応することができ、認証性能を向上することが可能になる。
- [0200] また、これとは逆に、データベース連携ポリシー記憶部32aが、所定の利用者の識

別情報を非成功情報として常に記憶しておいてもよい。これにより、例えば、所定の領域内で問題を起こした利用者を「1:N認証」の照合対象として常に除外するなど、利用者のニーズに柔軟に対応することができ、認証性能を向上することが可能になる。

- [0201] 認証要求処理部33bは、生体情報読み取り装置8が送信した生体情報としての「指紋画像」を、生体情報読み取り装置8の識別番号および生体情報読み取り装置8に接続される情報端末7の識別番号とともに受信する。例えば、「識別番号:00001」の利用者の「指紋画像」とともに、当該生体情報を読み取った生体情報読み取り装置8の「識別番号:S001」と、生体情報読み取り装置8に接続される情報端末7の「識別番号:C001」とを取得する。
- [0202] そして、認証要求処理部33bは、端末センサ記憶部32dを参照して、受信した生体情報読み取り装置8の「識別番号:S001」および情報端末7の「識別番号:C001」組み合わせに問題がないと判定すると、受信した「識別番号:00001」の利用者の「指紋画像」から、照合用データとしての「指紋特徴量情報」を作成するように、照合用データ作成部33cに指示を行い、さらに、照合対象者選別部33dに対し、「1:N認証」を行なう照合対象者の識別番号を選別する指示を行なう。
- [0203] 照合用データ作成部33cは、認証要求処理部33bの指示に基づいて、「識別番号:00001」の利用者の「指紋画像」から「指紋特徴量情報」を作成する。
- [0204] 照合対象者選別部33dは、認証要求処理部33bの指示に基づいて、「1:N認証」を行なう照合対象者の識別番号を選別し、その選別結果を照合対象者選別結果記憶部32fに格納する。すなわち、照合対象者選別部33dは、端末装置利用権限記憶部32eおよび利用者認証対象者記憶部32bを参照し、「ログイン要求を行なっている情報端末(識別番号:C001)において利用権限を与えられている利用者」であり、かつ、「利用者認証対象者記憶部32bに登録されている利用者」である利用者の識別番号を選別する。
- [0205] 照合対象者生体情報選別部33eは、照合対象者選別結果記憶部32fが記憶する選別された利用者の識別番号に対応する生体情報としての「指紋特徴量情報」を、生体情報記憶部9から取得し、取得した「指紋特徴量情報」を照合対象者生体情報

記憶部32gに格納する。

[0206] 第二認証部33fは、照合用データ作成部33cが作成した「指紋特徴量情報」と、照合対象者生体情報記憶部32gが記憶する「指紋特徴量情報」とを用いて利用者を認証する。すなわち、照合用データ作成部33cが作成した「識別番号:00001」の利用者の「指紋特徴量情報」と一致する「指紋特徴量情報」が照合対象者生体情報記憶部32gに存在する場合は、「識別番号:00001」の利用者が、情報端末(識別番号:C001)にログインすることを認めると判定する(図14参照)。また、一致する「指紋特徴量情報」が照合対象者生体情報記憶部32gに存在しない場合は、「識別番号:00001」の利用者が、情報端末(識別番号:C001)にログインすることを認めないと判定する。

[0207] なお、上記では、領域内に入室した利用者であり、かつ、情報端末7の利用権限が与えられている利用者を照合対象として選別する場合について説明したが、さらに、認証要求が発生した領域に現に入域した利用者であって、かつ、領域内に入室した利用者であり、かつ、情報端末7の利用権限が与えられている利用者を照合対象として選別する場合であってもよい。これにより、生体情報読み取り装置が設置される場所への入域が許可された利用者を「1:N認証」の照合対象における母集団として絞り込みことができ、さらに認証性能を向上することが可能になる。

[0208] [実施例6における利用者認証システムの処理の手順]

次に、図23～図25を用いて、実施例6における利用者認証システムの処理を説明する。図23は、実施例6における入退室管理装置の入室時処理を説明するための図であり、図24は、実施例6における利用者認証装置の入室時処理を説明するための図であり、図25は、実施例6における利用者認証装置の認証処理を説明するための図である。

[0209] [実施例6における入退室管理装置の入室時処理の手順]

図23に示すように、まず、実施例6における入退室管理装置20は、領域外読み取り装置4から、利用者の識別番号および領域外読み取り装置4の識別番号を受信すると(ステップS2301肯定)、第一認証部23aは、受信した利用者の識別番号と領域外読み取り装置4の識別番号とが、領域入出権限管理記憶部22aに登録されている

識別番号の組み合わせであるか否かを判定する(ステップS2302)。

[0210] そして、第一認証部23aは、受信した利用者の識別番号と領域外読み取り装置4の識別番号とが、領域入出権限管理記憶部22aに登録されている識別番号の組み合わせでないと判定すると(ステップS2302否定)、領域内に入室することを認証しないとする結果を扉6に通知し(ステップS2306)、処理を終了する。すなわち、受信した「利用者の識別番号」と、領域外読み取り装置4の識別番号との組み合わせが正しい組み合わせではない場合は、「識別番号:00001」の利用者が領域内へ入室することを許可せず、扉6に制御信号を送信して、扉6を施錠状態のままにする。

[0211] これに反して、第一認証部23aは、受信した利用者の識別番号と領域外読み取り装置4の識別番号とが、領域入出権限管理記憶部22aに登録されている識別番号の組み合わせであると判定すると(ステップS2302肯定)、領域内利用者記憶部22bに利用者の識別番号を追加して格納することで領域内利用者記憶部22bを更新する(ステップS2303)。例えば、「識別番号:00001」を領域内利用者記憶部22bに追加して格納する。

[0212] そして、データベース連携部23bは、追加更新された内容を利用者認証装置30に通知する(ステップS2304)。すなわち、新たに「識別番号:00001」が追加更新されたことを、データベース連携ポリシー記憶部22cを参照して、利用者認証装置30に通知する。

[0213] そして、第一認証部23aは、領域内に入室することを認証したとする結果を扉6に通知し(ステップS2305)、処理を終了する。すなわち、受信した「利用者の識別番号」と、領域外読み取り装置4の識別番号との組み合わせが正しい組み合わせの場合は、「識別番号:00001」の利用者が領域内へ入室することを許可し、扉6に制御信号を送信して、扉6を施錠から開錠の状態にする。

[0214] なお、実施例6における入退室管理装置の退室時処理の手順は、図23と同様であるので、以下に説明する。

[0215] まず、実施例6における入退室管理装置20は、領域内読み取り装置5から、利用者の識別番号および領域内読み取り装置5の識別番号を受信すると(ステップS2301肯定)、第一認証部23aは、受信した利用者の識別番号と領域内読み取り装置5の

識別番号とが、領域入出権限管理記憶部22aに登録されている識別番号の組み合わせであるか否かを判定する(ステップS2302)。

[0216] そして、第一認証部23aは、受信した利用者の識別番号と領域内読み取り装置5の識別番号とが、領域入出権限管理記憶部22aに登録されている識別番号の組み合わせでないと判定すると(ステップS2302否定)、領域内から退室することを認証しないとする結果を扉6に通知し(ステップS2306)、処理を終了する。

[0217] これに反して、第一認証部23aは、受信した利用者の識別番号と領域内読み取り装置5の識別番号とが、領域入出権限管理記憶部22aに登録されている識別番号の組み合わせであると判定すると(ステップS2302肯定)、領域内利用者記憶部23bから当該利用者の識別番号を削除することで領域内利用者記憶部22bを更新する(ステップS2303)。

[0218] そして、データベース連携部23bは、削除更新された内容を、データベース連携ポリシー記憶部22cを参照して、利用者認証装置30に通知する(ステップS2304)。

[0219] そして、第一認証部23aは、領域内から退室することを認証したとする結果を扉6に通知し(ステップS2305)、処理を終了する。すなわち、受信した「利用者の識別番号」と、領域内読み取り装置5の識別番号との組み合わせが正しい組み合わせの場合は、「識別番号:00001」の利用者が領域内から退室することを許可し、扉6に制御信号を送信して、扉6を施錠から開錠の状態にする。

[0220] [実施例6における利用者認証装置の入室時処理の手順]

図24に示すように、まず、実施例6における利用者認証装置30は、入退室管理装置20から当該入退室管理装置20の識別番号とともに、追加更新の内容(利用者の識別番号)を受信すると(ステップS2401肯定)、データベース連携部33aは、受信した入退室管理装置20の識別番号が、データベース連携ポリシー記憶部32aに登録されている入退室管理装置の識別番号に含まれるか否かを判定する(ステップS2402)。

[0221] そして、データベース連携部33aは、受信した入退室管理装置20の識別番号が、データベース連携ポリシー記憶部32aに登録されている入退室管理装置の識別番号に含まれなかった場合は(ステップS2402否定)、処理を終了する。

- [0222] これに反して、データベース連携部33aは、受信した入退室管理装置20の識別番号が、データベース連携ポリシー記憶部32aに登録されている入退室管理装置の識別番号に含まれる場合は(ステップS2402肯定)、受信した追加更新の内容(利用者の識別番号)が、認証対象者選別ポリシー記憶部32bに登録されている領域内における利用者認証の対象者に含まれるか否かを判定する(ステップS2403)。
- [0223] そして、データベース連携部33aは、受信した追加更新の内容(利用者の識別番号)が、認証対象者選別ポリシー記憶部32bに登録されている領域内における利用者認証の対象者に含まれない場合は(ステップS2403否定)、処理を終了する。
- [0224] これに反して、データベース連携部33aは、受信した追加更新の内容(利用者の識別番号)が、認証対象者選別ポリシー記憶部32bに登録されている領域内における利用者認証の対象者に含まれる場合は(ステップS2403肯定)、受信した追加更新の内容を利用者認証対象者記憶部32cに追加して更新し(ステップS2404)、処理を終了する。
- [0225] なお、実施例6における利用者認証装置の退室時処理の手順は、図24と同様であるので、以下に説明する。
- [0226] 図24に示すように、まず、実施例6における利用者認証装置30は、入退室管理装置20から当該入退室管理装置20の識別番号とともに、削除更新の内容(利用者の識別番号)を受信すると(ステップS2401肯定)、データベース連携部33aは、受信した入退室管理装置20の識別番号が、データベース連携ポリシー記憶部32aに登録されている入退室管理装置の識別番号に含まれるか否かを判定する(ステップS2402)。
- [0227] そして、データベース連携部33aは、受信した入退室管理装置20の識別番号が、データベース連携ポリシー記憶部32aに登録されている入退室管理装置の識別番号に含まれなかった場合は(ステップS2402否定)、処理を終了する。
- [0228] これに反して、データベース連携部33aは、受信した入室管理装置20の識別番号が、データベース連携ポリシー記憶部32aに登録されている入室管理装置の識別番号に含まれる場合は(ステップS2402肯定)、受信した削除更新の内容(利用者の識別番号)が、認証対象者選別ポリシー記憶部32bに登録されている領域内における

利用者認証の対象者に含まれるか否かを判定する(ステップS2403)。

[0229] そして、データベース連携部33aは、受信した削除更新の内容(利用者の識別番号)が、認証対象者選別ポリシー記憶部32bに登録されている領域内における利用者認証の対象者に含まれない場合は(ステップS2403否定)、処理を終了する。

[0230] これに反して、データベース連携部33aは、受信した削除更新の内容(利用者の識別番号)が、認証対象者選別ポリシー記憶部32bに登録されている領域内における利用者認証の対象者に含まれる場合は(ステップS2403肯定)、受信した削除更新の内容を利用者認証対象者記憶部32cから削除して更新し(ステップS2404)、処理を終了する。

[0231] [実施例6における利用者認証装置の認証処理の手順]

図25に示すように、まず、実施例6における利用者認証装置30は、生体情報読み取り装置8が送信した生体情報としての「指紋画像」を、生体情報読み取り装置8の識別番号および生体情報読み取り装置8に接続される情報端末7の識別番号とともに受信すると(ステップS2501肯定)、認証要求処理部33bは、端末センサ記憶部32dにおいて受信した生体情報読み取り装置8の識別番号および情報端末7の識別番号組み合わせが登録されているか否かを判定する(ステップS2502)。

[0232] そして、認証要求処理部33bは、端末センサ記憶部32dにおいて受信した生体情報読み取り装置8の識別番号および情報端末7の識別番号組み合わせが登録されていないと判定した場合は(ステップS2502否定)、ログインを認証しないとする結果を情報端末7に通知し(ステップS2508)、処理を修了する。

[0233] これに反して、認証要求処理部33bは、端末センサ記憶部32dにおいて受信した生体情報読み取り装置8の識別番号および情報端末7の識別番号組み合わせが登録されていると判定した場合は(ステップS2502肯定)、照合用データ作成部33cは、認証要求処理部33bの指示に基づいて、受信した「指紋画像」から「指紋特徴量情報」を作成する(ステップS2503)。

[0234] そして、照合対象者選別部33dは、認証要求処理部33bの指示に基づいて、「1:N認証」を行なう照合対象者の識別番号を選別する(ステップS2504)。すなわち照合対象者選別部33dは、端末装置利用権限記憶部32eおよび利用者認証対象者

記憶部32cを参照し、「ログイン要求を行なっている情報端末(識別番号:C001)」において利用権限を与えられている利用者」であり、かつ、「利用者認証対象者記憶部32cに登録されている利用者」である利用者の識別番号を選別する。

[0235] 続いて、照合対象者生体情報選別部33eは、照合対象者選別部33dによって選別された利用者の識別番号に対応する生体情報としての「指紋特徴量情報」を、生体情報記憶部9から取得し、取得した「指紋特徴量情報」を照合対象者生体情報記憶部32gに格納する(ステップS2505)。

[0236] そののち、第二認証部33fは、照合用データ作成部33cが作成した「指紋特徴量情報」と一致する「指紋特徴量情報」が照合対象者生体情報記憶部32gに存在するか否かを判定する(ステップS2506)。

[0237] そして、第二認証部33fは、照合用データ作成部33cが作成した「指紋特徴量情報」と一致する「指紋特徴量情報」が照合対象者生体情報記憶部32gに存在しない場合は(ステップS2506否定)、ログインを認証しないとする結果を情報端末7に通知し(ステップS2508)、処理を修了する。

[0238] これに反して、第二認証部33fは、照合用データ作成部33cが作成した「指紋特徴量情報」と一致する「指紋特徴量情報」が照合対象者生体情報記憶部32gに存在する場合は(ステップS2506肯定)、ログインの認証を情報端末7に通知し(ステップS2507)、処理を修了する。

[0239] [実施例6の効果]

上記したように、実施例6によれば、領域内に入退室することが予め許可されている複数の利用者ごとに、各利用者を一意に識別するための識別情報と当該利用者の生体情報としての「指紋特徴量情報」とを対応付けて記憶する。また、領域内への入室要求を行なう利用者から、当該利用者の識別情報を取得し、第一の認証として、取得された識別情報と、記憶された識別情報とを用いて利用者の領域内への入室を認証し、第一の認証が成功した利用者の識別情報を成功情報として記憶する。そして、領域内に設置される情報端末へログイン要求を行なう利用者から「指紋画像」を取得し、第二の認証として、取得された「指紋画像」から抽出した「指紋特徴量情報」と、記憶された「指紋特徴量情報」のうちで成功情報として記憶された利用者の識別

情報に対応した「指紋特徴量情報」とを用いて利用者が情報端末へログインすることを認証するので、領域内に入室が許可された利用者のみを「1:N認証」の照合対象として絞り込むことができ、認証性能を向上することが可能になる。

[0240] また、実施例6によれば、利用者が領域内から退室する場合に、当該利用者の識別情報をさらに取得し、領域内から退室するに際して取得された識別情報を成功情報からさらに削除するので、認証要求を行なう可能性がない利用者を、「1:N認証」の照合対象から除外することができ、認証性能を向上することが可能になる。

[0241] また、実施例6によれば、領域内へ入室する利用者の識別情報を取得するとともに、当該領域内から退室する利用者の識別情報を取得し、領域内に入室している利用者の識別情報を成功情報として当該領域内から退室するまで記憶するので、認証要求を行なう可能性がある利用者のみを、「1:N認証」の照合対象とすることができ、認証性能を向上することが可能になる。

[0242] また、実施例6によれば、領域内へ入室として取得された識別情報を、成功情報として追加して格納するとともに、領域内から退室として取得された識別情報識別情報を、成功情報から削除するので、認証要求を行なう可能性がない利用者を、「1:N認証」の照合対象から速やかに除外することができ、認証性能を向上することが可能になる。

[0243] ところで、実施例6では、入退室管理装置20が、物理的な空間への出入りを管理し、利用者認証装置30が、論理的な空間への出入りを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、入退室管理装置20および利用者認証装置30が物理的な空間への出入りを管理する場合であってもよい。例えば、利用者が建物へ入出館することを入退室管理装置20が管理し、利用者が当該建物の内部にある部屋への入室管理を、利用者認証装置30が、入退室管理装置20から受信した成功情報を参照して「1:N認証」により行なう場合であってもよい。

[0244] さらに、入退室管理装置20が、論理的な空間への出入りを管理し、利用者認証装置30が、物理的な空間への出入りを管理する場合であってもよい。例えば、空港内の搭乗手続きカウンタに設置される入退室管理装置20が、利用者の搭乗手続きの管理を行なうことで、利用者が「搭乗手続き済み」とする論理的グループに入ることを

管理し、飛行機の搭乗口に設置される利用者認証装置30が、利用者が飛行機内へ搭乗することを、入退室管理装置20から受信した成功情報を参照して「1:N認証」により行なう場合であってもよい。

- [0245] さらに、入退室管理装置20が、論理的な空間への出入りを管理し、利用者認証装置30が、論理的な空間への出入りを管理する場合であってもよい。例えば、入退室管理装置20が、電話会議の予約管理を行い、利用者が「電話会議予約済み」とする論理的グループに入ることを管理し、利用者認証装置30が、利用者が「予約時間内における電話会議への参加」とする論理的グループに入ることを、入退室管理装置20から受信した成功情報を参照して「1:N認証」により行なう場合であってもよい。

実施例 7

- [0246] 上述した実施例6では、第一の認証が成功した利用者の生体情報を第二の認証の照合対象に追加する場合について説明したが、実施例7では、第一の認証が成功した利用者の生体情報とともに、当該利用者が所属するグループの利用者の生体情報も第二の認証の照合対象に追加する場合について、図26を用いて説明する。なお、図26は、実施例7における利用者認証システムを説明するための図である。
- [0247] 実施例7における利用者認証システムを構成する電話会議予約装置は、各利用者が属するグループを一意に識別する「グループ情報」を、利用者の「識別情報」に対応付けてさらに記憶する。具体的には、図26に示すように、実施例7における利用者認証システムを構成する電話会議予約装置は、「グループ情報」を「識別番号」に対応付けて記憶する。例えば、「識別情報:00001」の利用者と、「識別情報:00005」の利用者、「識別情報:00088」の利用者および「識別情報:00100」の利用者は、電話会議を使用することが予め認められている利用者として登録されており、また、これらの利用者には、同じグループ情報である「第一営業部」が与えられている。
- [0248] そして、実施例7における利用者認証システムを構成する電話会議予約装置は、第一の認証が成功した利用者の識別情報の他に、当該利用者のグループ情報に対応する他の利用者の識別情報も成功情報として記憶する。すなわち、実施例7における利用者認証システムを構成する電話会議予約装置は、図26に示すように、「識別番号:00001」の利用者が提示したICカードから、「識別番号:00001」を取得して

、「予約時間:2007年4月2日午後1時から2時間」とする電話会議の予約を受け付けて認証した場合、「予約受け付け完了」と判定された「識別番号:00001」の他に、「識別番号:00001」に与えられた「グループ情報:第一営業部」に対応する「識別情報:00005」、「識別情報:00088」および「識別情報:00100」を予約利用者データベースに追加更新する。

[0249] そして、実施例7における利用者認証システムを構成する利用者認証装置は、図26に示すように、追加更新した「識別番号」を受信すると、これらの「識別番号」を利用者認証対象者データベースに追加更新する。

[0250] このようなことから、実施例7における利用者認証システムは、電話会議システムに接続される生体情報読み取り装置から、例えば、「予約時間:2007年4月2日午後1時」に「識別情報:00005」の利用者から生体情報を受信した場合でも、「識別情報:00005」に対応する生体情報を照合対象として速やかに読み出せるので、認証性能を向上することが可能になる。

実施例 8

[0251] 上述した実施例6では、「利用者自身の出入り」を第一の認証によって管理する場合について説明したが、実施例8では、「物の出入り」を第一の認証によって管理する場合について、図27を用いて説明する。なお、図27は、実施例8における利用者認証システムを説明するための図である。

[0252] 実施例8における利用者認証システムを構成する情報端末管理装置は、利用者が利用を開始しようとする情報端末の情報を、利用者の識別情報に対応付けてさらに記憶する。例えば、実施例8における利用者認証システムを構成する情報端末管理装置は、図27に示すように、「IPアドレス:10. 10. 30. 1」の情報端末を利用することが許可されている利用者の識別番号は、「識別情報:00001」、「識別情報:00005」、「識別情報:00088」および「識別情報:00100」であることを、情報端末利用権限データベースに保持する。

[0253] そして、実施例8における利用者認証システムを構成する情報端末管理装置は、利用者が利用を開始しようとする情報端末の情報から当該利用者の識別情報を取得する。例えば、「識別情報:00001」の利用者が、「IPアドレス:10. 10. 30. 1」の情

報端末の電源を「ON」にした場合、当該情報端末の電源が「ON」になったことを、ネットワークを介して受信する。「IPアドレス:10. 10. 30. 1」の情報端末の電源を「ON」になったことを受信した実施例8における利用者認証システムを構成する情報端末管理装置は、図27に示すように、情報端末利用権限データベースを参照して、「識別番号:00001」、「識別情報:00005」、「識別情報:00088」および「識別情報:00100」を、情報端末利用者データベースに追加更新して格納する。

[0254] そして、実施例8における利用者認証システムを構成する利用者認証装置は、図27に示すように、追加更新した「識別番号」を受信すると、これらの「識別番号」を利用者認証対象者データベースに追加更新する。

[0255] このようなことから、実施例8における利用者認証システムは、「IPアドレス:10. 10. 30. 1」の情報端末にログインをするために、当該情報端末に接続される生体情報読み取り装置から、「識別情報:00001」の利用者から生体情報を受信した場合でも、「識別情報:00001」に対応する生体情報を照合対象として速やかに読み出せるので、認証性能を向上することが可能になる。また、利用者自身ではなく、利用者を特定することが可能な情報端末のIPアドレスを活用して第一の認証を速やかに処理することができるので、認証性能を向上することが可能になる。

実施例 9

[0256] 上述した実施例6～8では、2段階で利用者認証を処理する場合について説明したが、実施例9では、多段階で利用者認証を処理する場合について、図28を用いて説明する。なお、図28は、実施例9における利用者認証システムを説明するための図である。

[0257] 実施例9における利用者認証システムは、ビル入退室管理装置と、勤怠管理装置と、所属管理装置と、利用者認証装置とから構成される。ビル入退室管理装置は、本社ビルの1Fからの利用者の入退室を、ビル入出権限管理データベースを用いて管理する。ビル入出権限管理データベースは、本社ビルの1Fからの入退室を許可される利用者の識別番号を予め記憶しており、ビル入退室管理装置は、利用者から受信した識別番号と一致する識別番号を、ビル入出権限管理データベースが記憶している場合に、当該利用者の本社ビルの1Fからの利用者の入退室を許可する。例えば、

実施例9におけるビル入退室管理装置は、図28に示すように、「2007年4月2日午前9時00分」において、「識別番号:00001」である利用者(Eさん)の本社ビルの1Fからの入室を、ビル入出権限管理データベースを参照して許可する。

[0258] 勤怠管理装置は、ビル入退室管理装置と連動して、利用者ごとの勤怠管理を行い、その記録を勤怠管理データベースに記憶する。例えば、図28に示すように、「識別番号:00001」の利用者(Eさん)が、「2007年4月2日午前9時00分」に出社したとする記録を記憶する。

[0259] 所属管理装置は、利用者ごとの役職を、社員所属情報データベースに記憶している。例えば、「識別番号:00001」の利用者(Eさん)の役職が「取締役」とであると記憶する。

[0260] ここで、実施例9における利用者認証システムを構成する利用者認証装置は、ビル入退室管理装置と、勤怠管理装置と、所属管理装置との情報を統合して、「2007年4月2日午前9時00分」に出社した利用者(Eさん)の「識別番号:00001」を、「役職」を参照した場合、「取締役」と高い地位が与えられた利用者であることから、直ちに認証対象者として、利用者認証対象者データベースに登録しておく。

[0261] これにより、例えば、「役職:取締役」の利用者(Eさん)が、本社ビル5Fにある共有情報端末室に設置される情報端末にログオン要求する際に、当該情報端末に接続される生体情報読み取り装置に自身の生体情報を読み取らせた場合でも、実施例9における利用者認証システムを構成する利用者認証装置は、利用者認証対象者データベースを参照することで、生体情報読み取り装置から受信した利用者(Eさん)の生体情報を速やかに認証することができ、認証性能を向上することが可能になる。

[0262] ところで、上記の実施例1～9では、ハードウェアロジックによって各種の処理を実現する場合を説明したが、本発明はこれに限定されるものではなく、あらかじめ用意されたプログラムをコンピュータで実行するようにしてもよい。そこで以下では、図29を用いて、上記の実施例1に示した利用者認証装置10と同様の機能を有する利用者認証プログラムを実行するコンピュータの一例を説明する。図29は、実施例1における利用者認証プログラムを実行するコンピュータを示す図である。

[0263] 図29に示すように、情報処理装置としてのコンピュータ290は、キーボード291、デ

ディスプレイ292、CPU293、ROM294、HDD295およびRAM296をバス297などで接続して構成され、さらに、識別番号読み取り装置1と、生体情報読み取り装置2と、利用者情報記憶部3と接続される。

[0264] ROM294には、上記の実施例1に示した利用者認証装置10と同様の機能を発揮する利用者認証プログラム、つまり、図29に示すように、第一認証プログラム294a、生体情報格納プログラム294b、第二認証プログラム294c、成功情報削除プログラム294dが予め記憶されている。なお、これらのプログラム294a～294dについては、図2に示した利用者認証装置10の各構成要素と同様、適宜統合または分散してもよい。

[0265] そして、CPU293が、これらのプログラム294a～294dをROM294から読みだして実行することで、図29に示すように、各プログラム294a～294dは、第一認証プロセス293a、生体情報格納プロセス293b、第二認証プロセス293c、成功情報削除プロセス293dとして機能するようになる。なお、各プロセス293a～293dは、図2に示した、第一認証部13a、生体情報格納部13b、第二認証部13c、成功情報削除部13dにそれぞれ対応する。

[0266] また、HDD295には、図29に示すように、成功情報データ295aと、生体情報データ295bとが設けられる。この成功情報データ295aは、図2に用いた成功情報記憶部12aに対応し、生体情報データ295bは生体情報記憶部12bに対応する。そしてCPU293は、成功情報データ296aを成功情報データ295aに対して登録し、生体情報データ296bを生体情報データ295bに対して登録し、この成功情報データ296aと、生体情報データ296bとを読み出してRAM296に格納し、RAM296に格納された成功情報データ296aと、生体情報データ296bとに基づいて利用者認証処理を実行する。

[0267] なお、上記した各プログラム294a～294dについては、必ずしも最初からROM294に記憶させておく必要はなく、例えば、コンピュータ290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」、または、コンピュータ290の内外に備えられるHDDなどの「固定用物理媒体」、さらには、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290に接続される「他のコンピュータ(またはサーバ)」などに各プログラムを記憶させておき、コンピュータ290がこれらから各プログラムを読み出して実行するようにしてもよい。

[0268] また、上記の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の全部または一部を手動でおこなうこともでき(例えば、成功情報の更新を自動的に行なうのではなく、利用者認証装置10の管理者から受け付けるなど)、あるいは、手動的におこなうものとして説明した処理の全部または一部を公知の方法で自動的におこなうこともできる。例えば、この他、上記文章中や図面中で示した処理手順、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、成功情報の登録時間など)については、特記する場合を除いて任意に更新することができる。

[0269] 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、各処理部および各記憶部の分散・統合の具体的形態(例えば、図2の形態など)は図示のものに限られず、例えば、第一認証部13aと生体情報格納部13bとを統合するなど、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。

産業上の利用可能性

[0270] 以上のように、本発明に係る利用者認証装置、利用者認証方法および利用者認証プログラムは、利用者の認証を行う場合に有用であり、特に、認証性能を向上することが可能になることに適する。

請求の範囲

- [1] 利用者を認証する利用者認証装置であつて、
 複数の利用者ごとに、各利用者を一意に識別するための識別情報と当該利用者の
 生体情報とを対応付けた利用者情報を記憶する利用者情報記憶手段と、
 前記利用者が所定の対象に対する利用を開始する場合に、当該利用者の識別情
 報を取得する識別情報取得手段と、
 前記識別情報取得手段により取得された識別情報と、前記利用者情報記憶手段
 に記憶された利用者情報とを用いて利用者を認証する第一の認証手段と、
 前記第一の認証手段による認証が成功した利用者の識別情報を成功情報として記
 憶する成功情報記憶手段と、
 前記利用者の生体情報を取得する生体情報取得手段と、
 前記生体情報取得手段により取得された生体情報と、前記利用者情報記憶手段
 に記憶された生体情報のうちで前記成功情報記憶手段に成功情報として記憶され
 た利用者の識別情報に対応した生体情報とを用いて利用者を認証する第二の認証
 手段と、
 を備えたことを特徴とする利用者認証装置。
- [2] 所定の成功情報が前記成功情報記憶手段に記憶されてから所定の登録時間が経
 過したか否かを判定し、当該登録時間が経過した場合に、当該所定の成功情報を前
 記成功情報記憶手段から削除する成功情報削除手段をさらに備えたことを特徴とす
 る請求項1に記載の利用者認証装置。
- [3] 前記成功情報削除手段は、前記利用者ごとに定められた登録時間が経過したか
 否かを判定することを特徴とする請求項2に記載の利用者認証装置。
- [4] 前記成功情報削除手段は、前記成功情報記憶手段に記憶された成功情報の個数
 が所定値以上になった場合に、当該所定値未満に際して判定に用いられる登録時
 間よりも短い登録時間を用いて、当該登録時間が経過したか否かを判定すること
 を特徴とする請求項2に記載の利用者認証装置。
- [5] 前記利用者の利用頻度を記憶する利用頻度記憶手段をさらに備え、
 前記成功情報削除手段は、前記成功情報記憶手段に記憶された成功情報の個数

が所定値以上になった場合に、前記利用頻度記憶手段に記憶された各利用者の利用頻度に基づいて、当該利用頻度が所定値よりも低い利用者の成功情報を前記成功情報記憶手段からさらに削除することを特徴とする請求項2に記載の利用者認証装置。

- [6] 前記利用者情報記憶手段は、各利用者が属するグループを一意に識別するグループ識別情報を、前記利用者の識別情報に対応付けてさらに記憶し、

前記成功情報記憶手段は、前記第一の認証手段による認証が成功した利用者の識別情報の他に、当該利用者のグループ識別情報に対応する他の利用者の識別情報も成功情報として記憶することを特徴とする請求項1に記載の利用者認証装置。

- [7] 前記利用者情報記憶手段は、前記利用者が利用している物品または情報を、前記利用者の識別情報に対応付けてさらに記憶し、

前記識別情報取得手段は、前記利用者が利用する物品または情報から当該利用者の識別情報を取得することを特徴とする請求項1に記載の利用者認証装置。

- [8] 前記識別情報取得手段は、前記利用者が所定の対象に対する利用を終了する場合に、当該利用者の識別情報をさらに取得し、

前記成功情報削除手段は、前記識別情報取得手段による利用の終了に際して取得された識別情報を前記成功情報記憶手段からさらに削除することを特徴とする請求項2に記載の利用者認証装置。

- [9] 前記識別情報取得手段は、所定の物品または情報を返却する利用者の識別情報を取得し、

前記生体情報取得手段は、所定の物品または情報を貸し出そうとする利用者の生体情報を取得することを特徴とする請求項1に記載の利用者認証装置。

- [10] 前記成功情報記憶手段に成功情報として記憶されている利用者の識別情報に対応した生体情報を前記利用者情報記憶手段から取得して記憶する生体情報記憶手段をさらに備え、

前記第二の認証手段は、前記生体情報記憶手段に記憶された生体情報を用いて前記利用者を認証することを特徴とする請求項1に記載の利用者認証装置。

- [11] 所定の物品または情報を返却した利用者が、同日に所定の物品または情報を貸し

出す頻度を記憶する貸し出し頻度記憶手段をさらに備え、

前記成功情報削除手段は、前記成功情報記憶手段に記憶された成功情報の個数が所定値以上になった場合に、前記貸し出し頻度記憶手段に記憶された各利用者の貸し出し頻度に基づいて、当該貸し出し頻度が所定値よりも低い利用者の成功情報を前記成功情報記憶手段からさらに削除することを特徴とする請求項2に記載の利用者認証装置。

- [12] 前記識別情報取得手段は、所定の領域に入域する利用者の識別情報を取得するとともに、当該所定の領域から出域する利用者の識別情報を取得し、

前記成功情報記憶手段は、前記所定の領域に入域している利用者の識別情報を成功情報として当該所定の領域から出域するまで記憶することを特徴とする請求項1に記載の利用者認証装置。

- [13] 前記識別情報取得手段により入域として取得された識別情報を、前記成功情報記憶手段に追加して格納するとともに、前記識別情報取得手段により出域として取得された識別情報を、前記成功情報記憶手段から削除する成功情報追加削除手段をさらに備えたことを特徴とする請求項12に記載の利用者認証装置。

- [14] 前記成功情報追加削除手段は、前記識別情報取得手段により取得された複数の識別情報を入手し、各識別情報が入域であるか出域であるかに応じて、各識別情報を前記成功情報記憶手段に追加または削除することを特徴とする請求項13に記載の利用者認証装置。

- [15] 前記成功情報追加削除手段は、前記識別情報取得手段により取得された複数の識別情報を所定の時間毎に入手し、各識別情報が入域であるか出域であるかに応じて、各識別情報を前記成功情報記憶手段に追加または削除することを特徴とする請求項13に記載の利用者認証装置。

- [16] 前記成功情報記憶手段は、前記所定の領域に入域しているか出域しているかにかかわらず、所定の利用者の識別情報を成功情報として常に記憶することを特徴とする請求項12に記載の利用者認証装置。

- [17] 前記成功情報記憶手段は、前記所定の領域に入域しているか出域しているかにかかわらず、所定の利用者の識別情報を非成功情報として常に記憶し、

前記第二の認証手段は、前記成功情報記憶手段に非成功情報として記憶された利用者の識別情報に対応した生体情報を用いることなく前記利用者を認証することを特徴とする請求項12に記載の利用者認証装置。

[18] 前記第二の認証手段は、いずれの領域において前記生体情報取得手段により生体情報が取得されたかに応じて、前記生体情報が取得された領域に入域している利用者であり、かつ、前記成功情報記憶手段に成功情報として記憶された利用者の識別情報を用いて利用者を認証することを特徴とする請求項12に記載の利用者認証装置。

[19] 利用者を認証する利用者認証方法であって、
複数の利用者ごとに、各利用者を一意に識別するための識別情報と当該利用者の生体情報とを対応付けた利用者情報を記憶する利用者情報記憶ステップと、
前記利用者が所定の対象に対する利用を開始する場合に、当該利用者の識別情報を取得する識別情報取得ステップと、
前記識別情報取得ステップにより取得された識別情報と、前記利用者情報記憶手段に記憶された利用者情報とを用いて利用者を認証する第一の認証ステップと、
前記第一の認証ステップによる認証が成功した利用者の識別情報を成功情報として記憶する成功情報記憶ステップと、
前記利用者の生体情報を取得する生体情報取得ステップと、
前記生体情報取得ステップにより取得された生体情報と、前記利用者情報記憶ステップに記憶された生体情報のうちで前記成功情報記憶ステップに成功情報として記憶された利用者の識別情報に対応した生体情報とを用いて利用者を認証する第二の認証ステップと、
を備えたことを特徴とする利用者認証方法。

[20] 利用者を認証する利用者認証方法をコンピュータに実行させる利用者認証プログラムであって、
複数の利用者ごとに、各利用者を一意に識別するための識別情報と当該利用者の生体情報とを対応付けた利用者情報を記憶する利用者情報記憶手順と、
前記利用者が所定の対象に対する利用を開始する場合に、当該利用者の識別情

報を取得する識別情報取得手順と、

前記識別情報取得手順により取得された識別情報と、前記利用者情報記憶手順に記憶された利用者情報とを用いて利用者を認証する第一の認証手順と、

前記第一の認証手順による認証が成功した利用者の識別情報を成功情報として記憶する成功情報記憶手順と、

前記利用者の生体情報を取得する生体情報取得手順と、

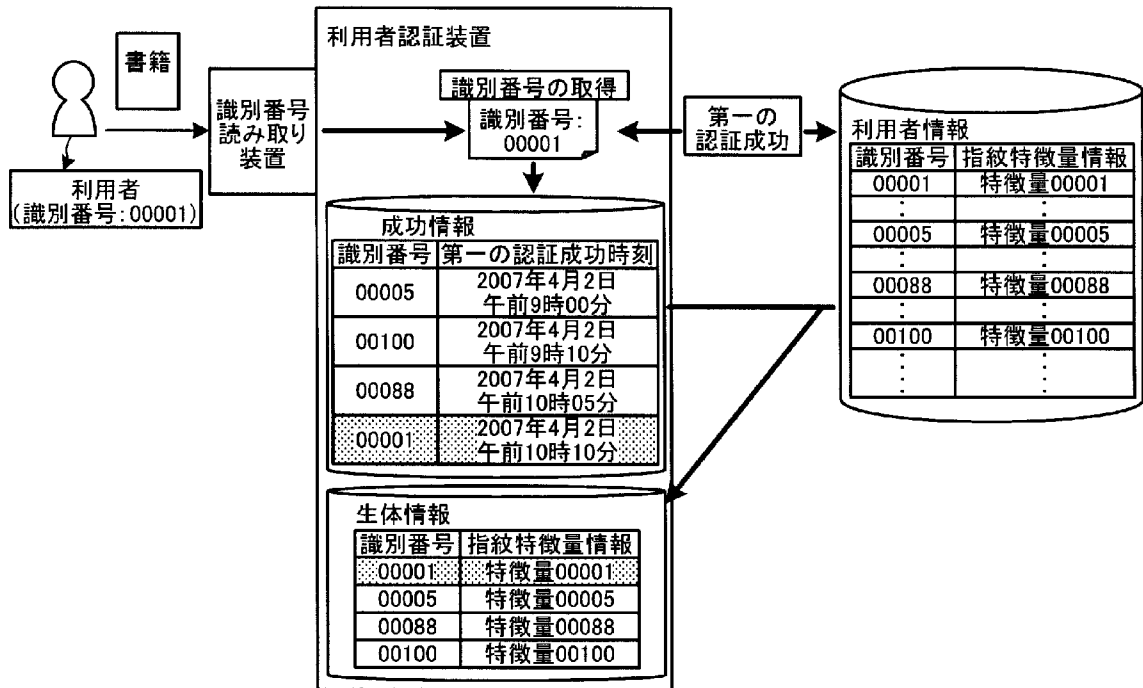
前記生体情報取得手順により取得された生体情報と、前記利用者情報記憶手順に記憶された生体情報のうちで前記成功情報記憶手順に成功情報として記憶された利用者の識別情報に対応した生体情報とを用いて利用者を認証する第二の認証手順と、

をコンピュータに実行させることを特徴とする利用者認証プログラム。

[図1]

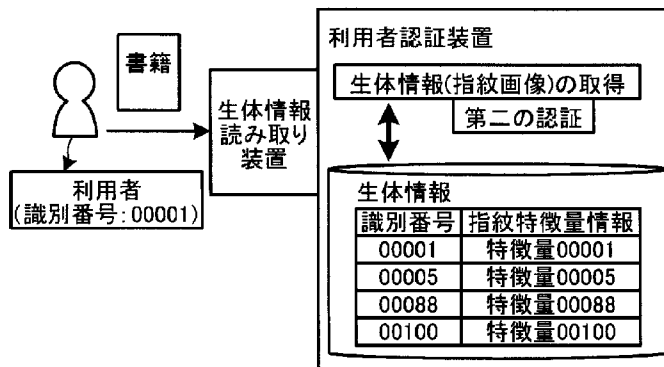
(A) 図書館「返却貸し出し受付」

返却「2007年4月2日午前10時10分」



(B) 貸し出し

「2007年4月2日午前10時50分」



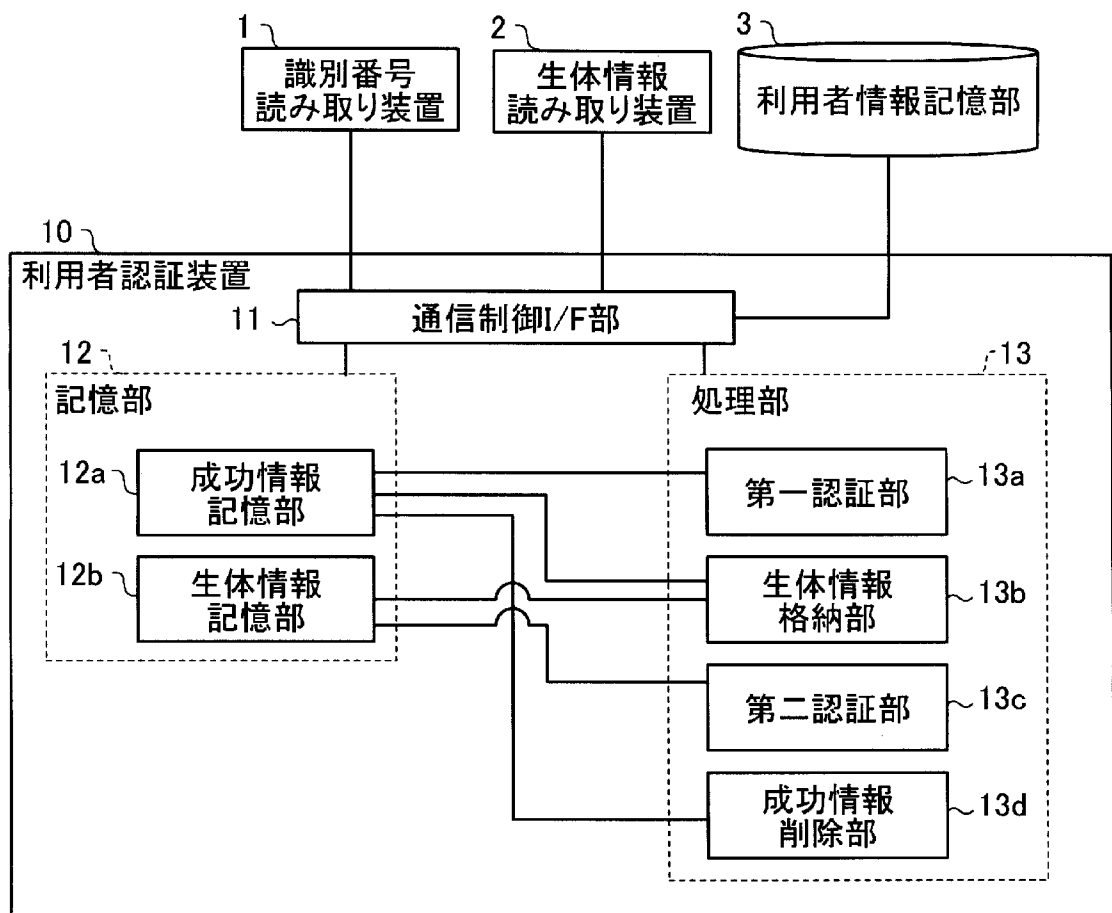
(C)

登録時間: 2時間

「2007年4月2日午前11時00分」



[図2]



[図3]

識別番号	指紋特徴量情報
00001	特徴量00001
⋮	⋮
00005	特徴量00005
⋮	⋮
00088	特徴量00088
⋮	⋮
00100	特徴量00100
⋮	⋮
⋮	⋮

[図4]

(A)

識別番号	第一の認証成功時刻
00005	2007年4月2日 午前9時00分
00100	2007年4月2日 午前9時10分
00088	2007年4月2日 午前10時05分

(B)

識別番号	第一の認証成功時刻
00005	2007年4月2日 午前9時00分
00100	2007年4月2日 午前9時10分
00088	2007年4月2日 午前10時05分
00001	2007年4月2日 午前10時10分

(C)

識別番号	第一の認証成功時刻
00100	2007年4月2日 午前9時10分
00088	2007年4月2日 午前10時05分
00001	2007年4月2日 午前10時10分

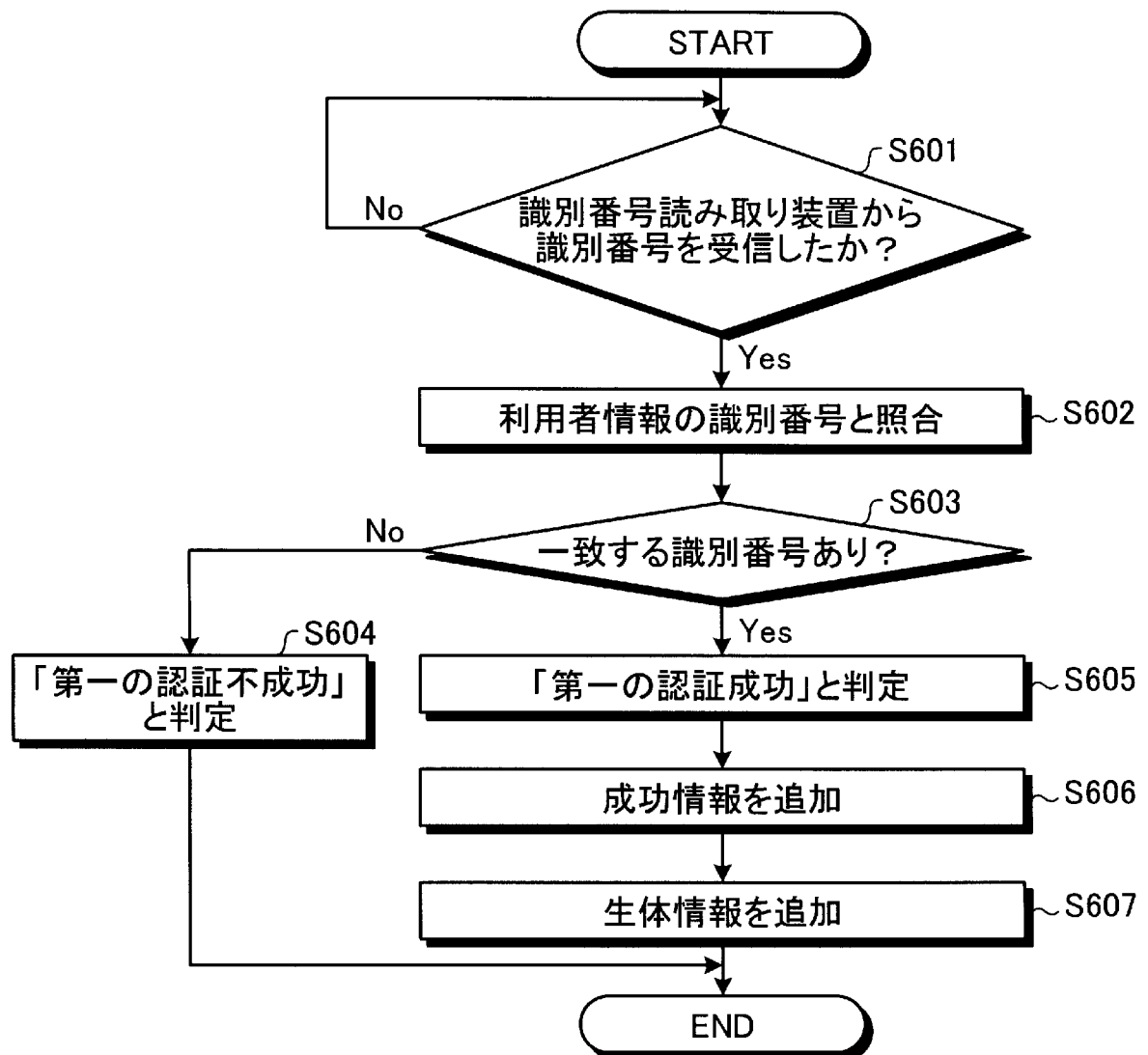
[図5]

(A)	識別番号	指紋特徴量情報
	00005	特徴量00005
	00088	特徴量00088
	00100	特徴量00100

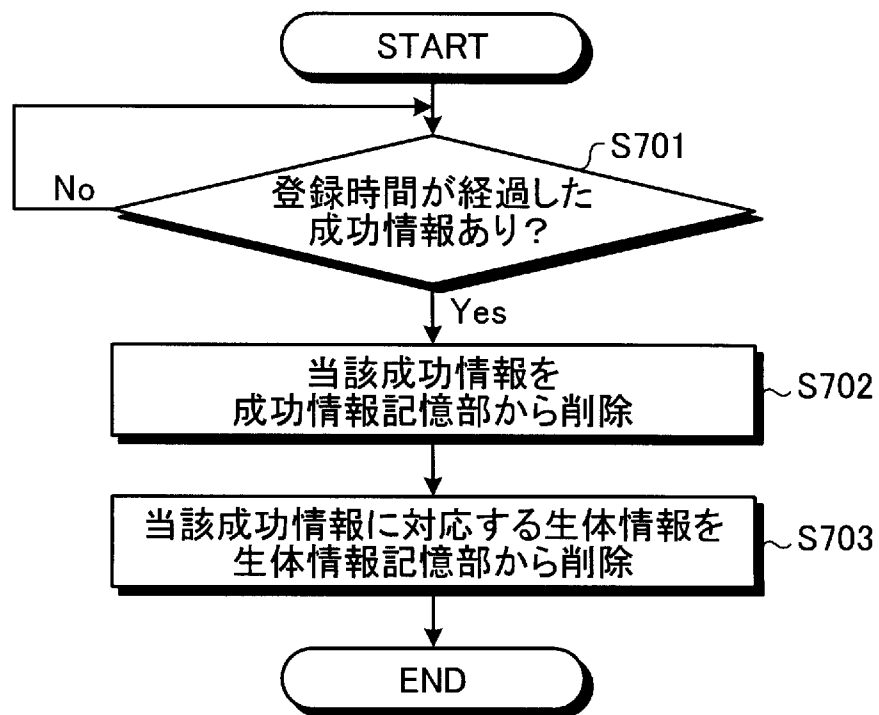
(B)	識別番号	指紋特徴量情報
	00001	特徴量00001
	00005	特徴量00005
	00088	特徴量00088
	00100	特徴量00100

(C)	識別番号	指紋特徴量情報
	00001	特徴量00001
	00088	特徴量00088
	00100	特徴量00100

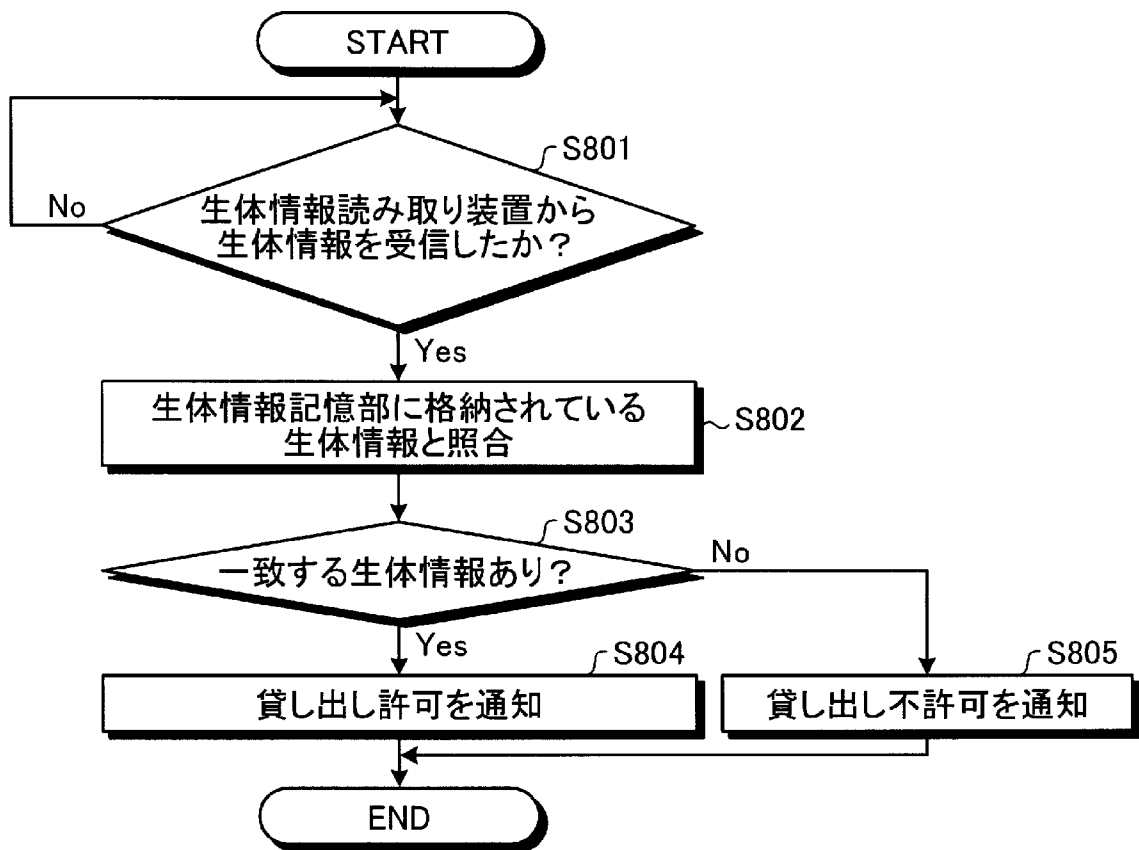
[図6]



[図7]



[図8]



[図9]

(A)

識別番号	登録時間
00001	2時間
⋮	⋮
00005	3時間
⋮	⋮
00088	1時間30分
⋮	⋮
00100	4時間
⋮	⋮
⋮	⋮

利用者ごとに登録時間を設定

(B)「2007年4月2日午前11時35分」

識別番号	第一の認証成功時刻
00005	2007年4月2日 午前9時00分
00100	2007年4月2日 午前9時10分
00088	2007年4月2日 午前10時05分
00001	2007年4月2日 午前10時10分

成功情報
更新

(1)

識別番号	第一の認証成功時刻
00005	2007年4月2日 午前9時00分
00100	2007年4月2日 午前9時10分
00001	2007年4月2日 午前10時10分

生体情報
更新

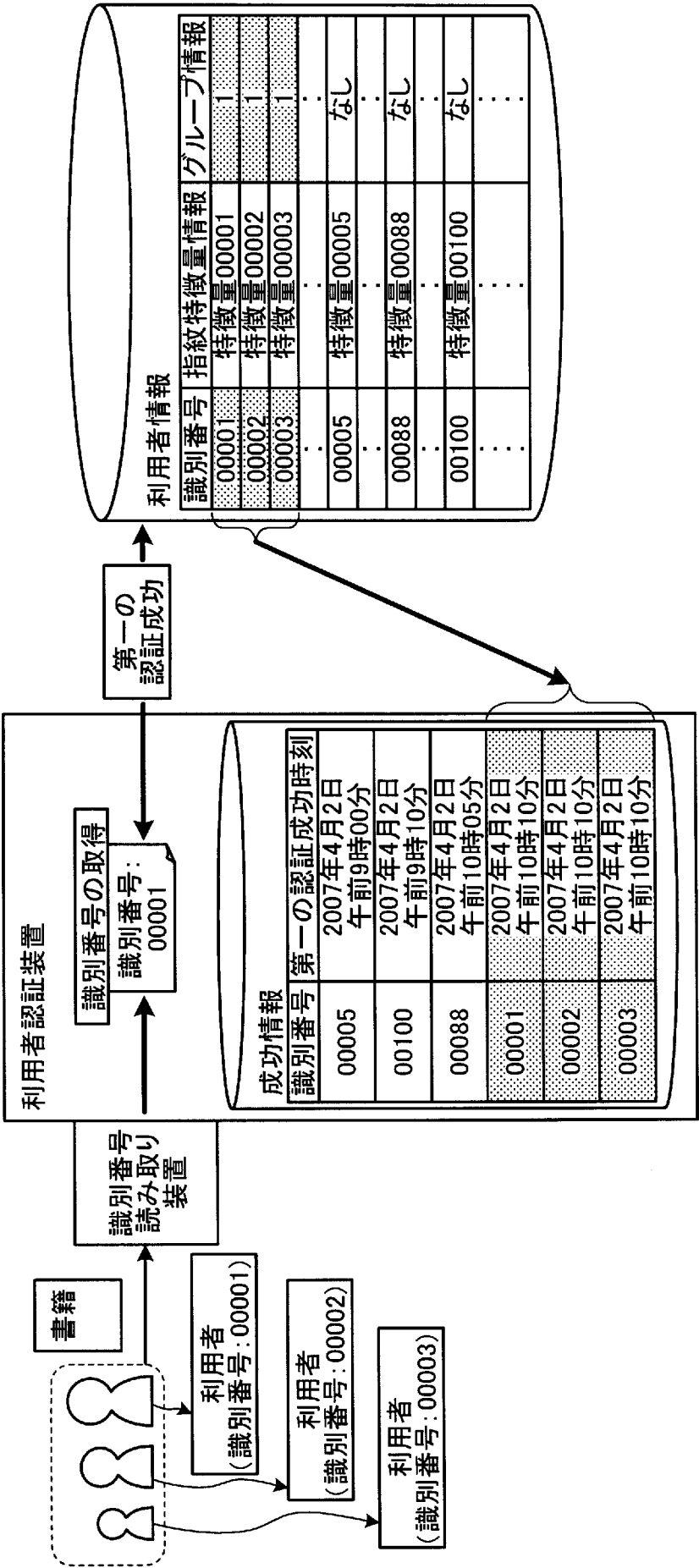
(2)

識別番号	指紋特徴量情報
00001	特徴量00001
00005	特徴量00005
00100	特徴量00100

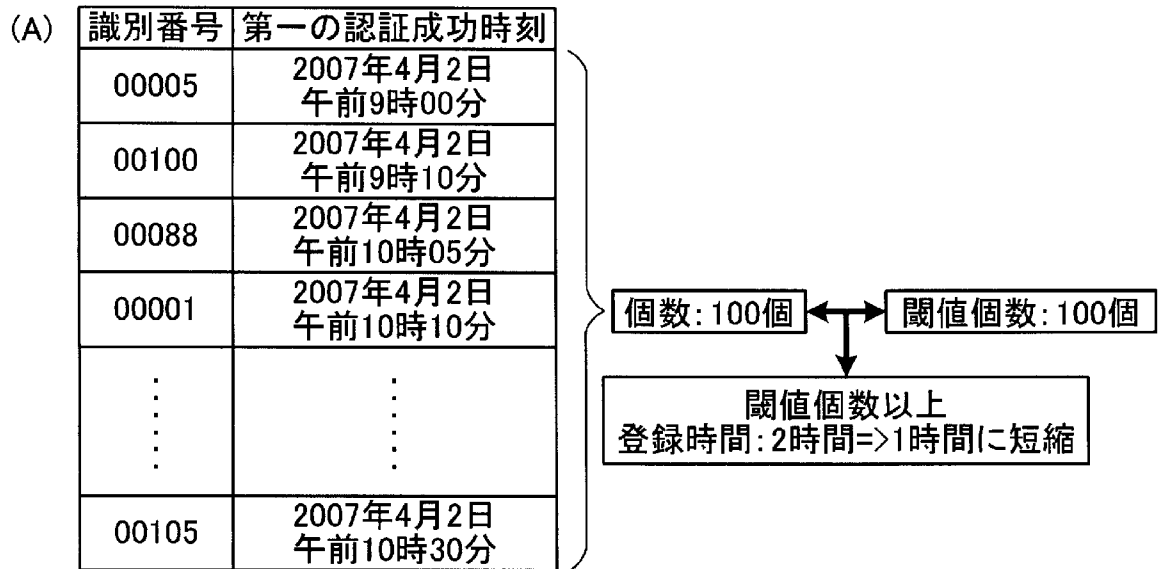
[図10]

図書館「返却貸し出し受付」

返却「2007年4月2日午前10時10分」



[図11]

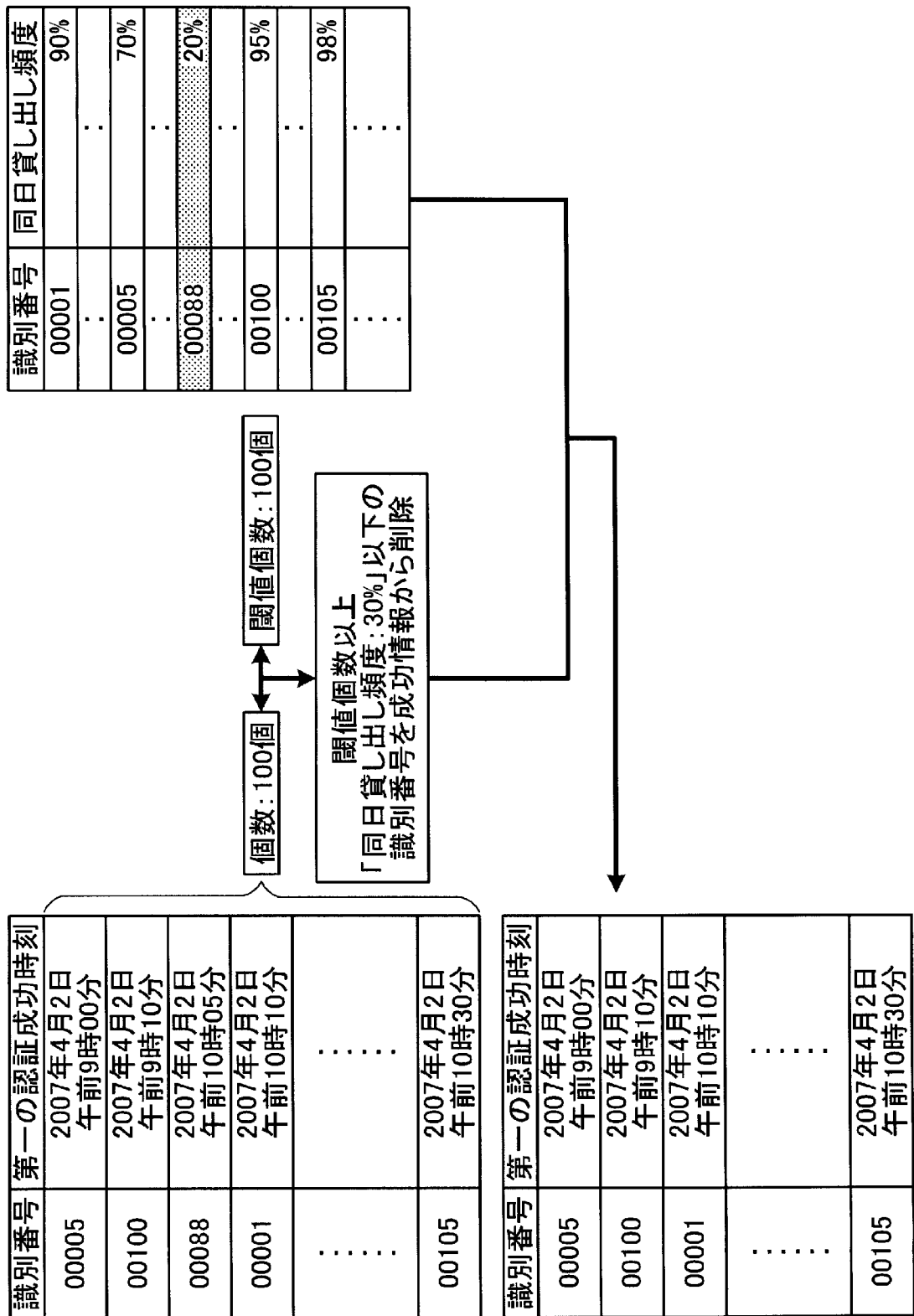


(B)

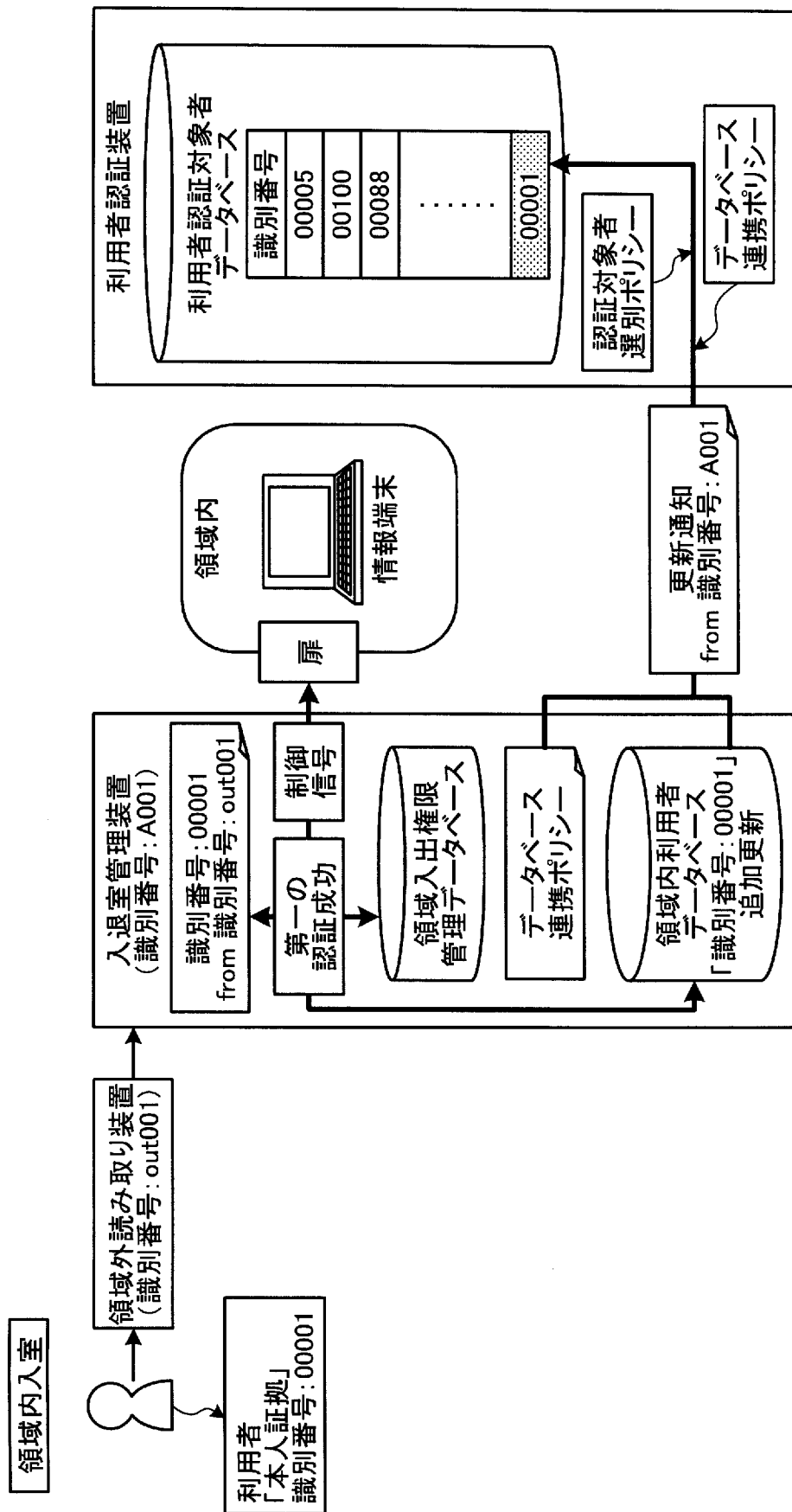
識別番号	登録時間	短縮登録時間
00001	2時間	1時間
⋮	⋮	⋮
00005	3時間	1時間30分
⋮	⋮	⋮
00088	1時間30分	1時間
⋮	⋮	⋮
00100	4時間	1時間
⋮	⋮	⋮
00105	5時間	3時間
⋮	⋮	⋮

利用者ごとに
短縮登録時間も設定

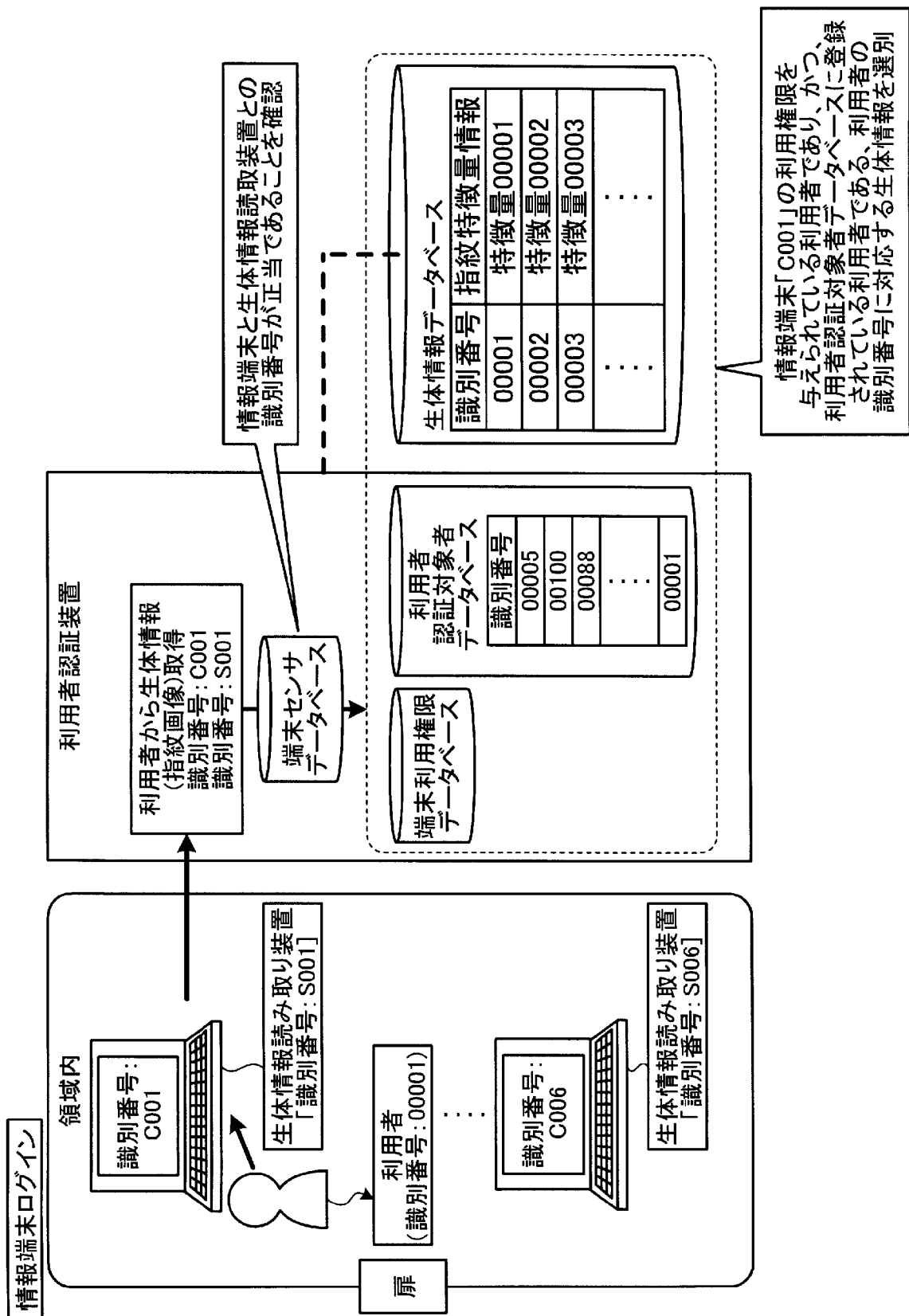
[図12]



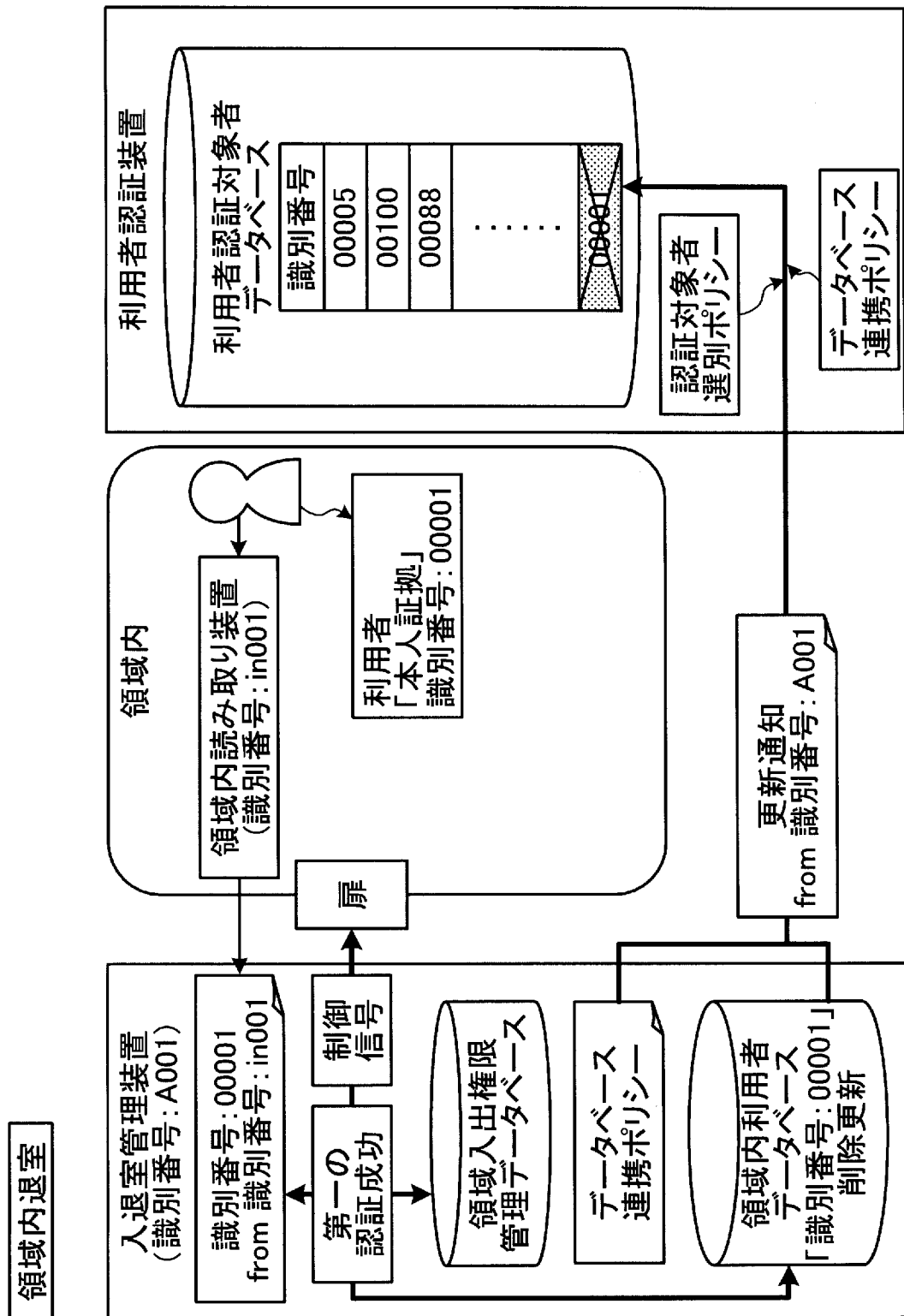
[図13]



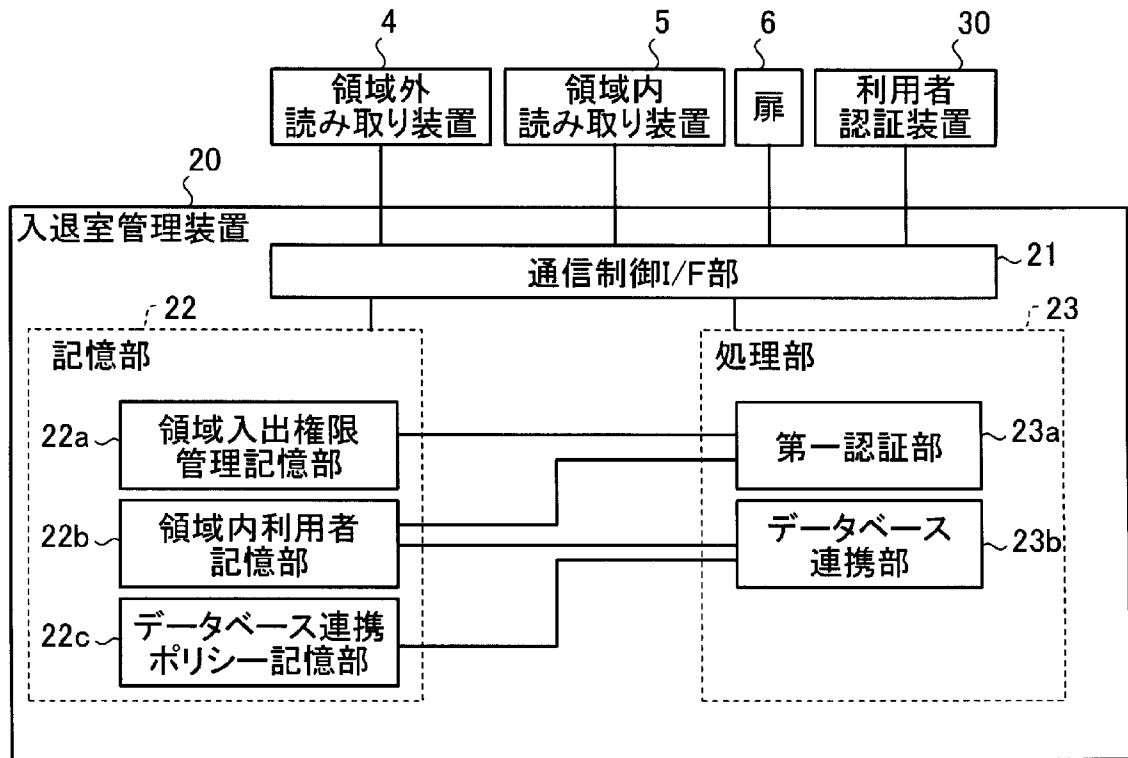
[図14]



[図15]



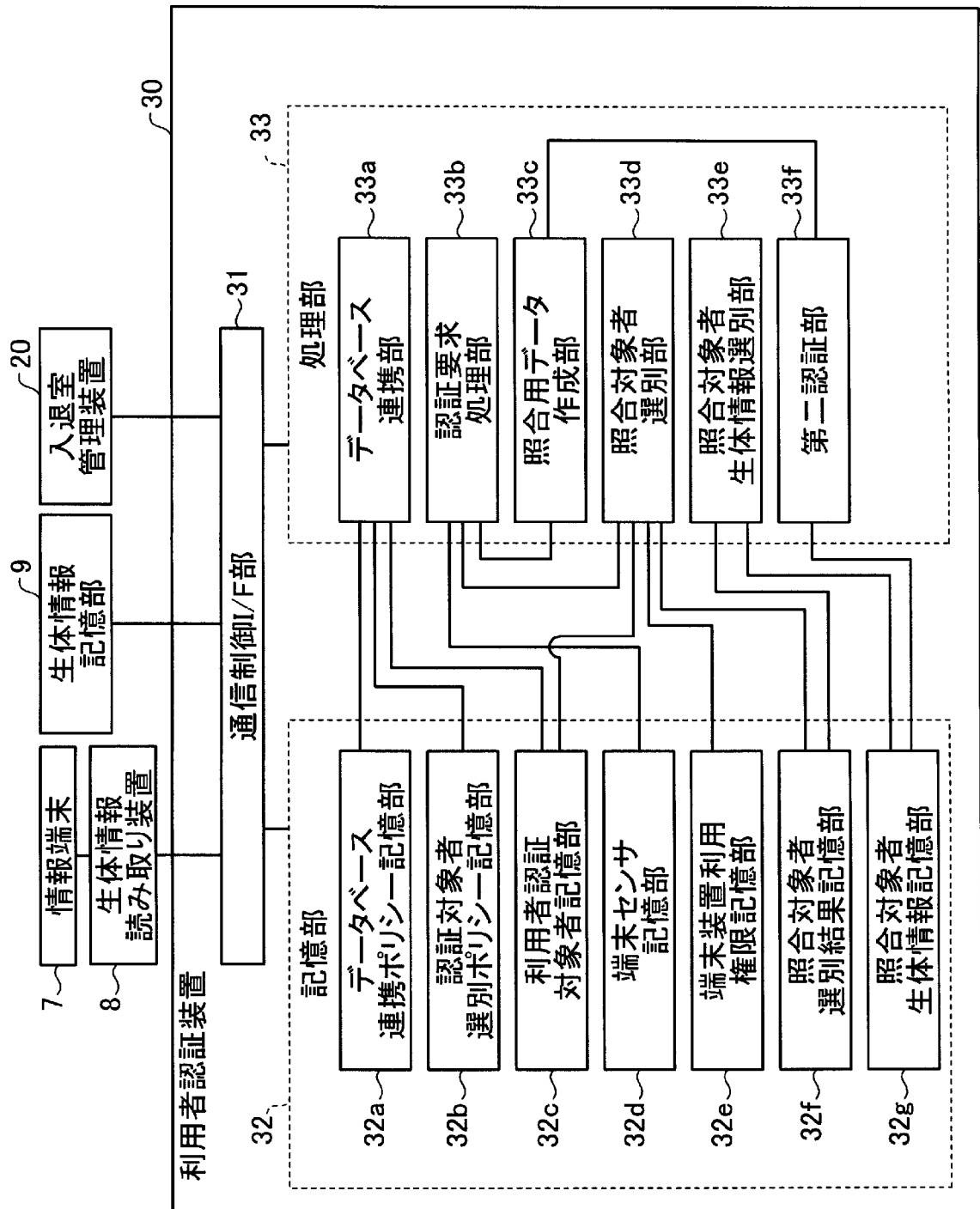
[図16]



[図17]

領域外読み取り装置	領域内読み取り装置	識別番号
out001	in001	00001
		00002
		00003
		・
		・
⋮	⋮	・
		⋮
		⋮
		⋮
		⋮

[図18]



[図19]

識別番号	指紋特徴量情報
00001	特徴量00001
00002	特徴量00002
00003	特徴量00003
⋮	⋮
⋮	⋮
⋮	⋮

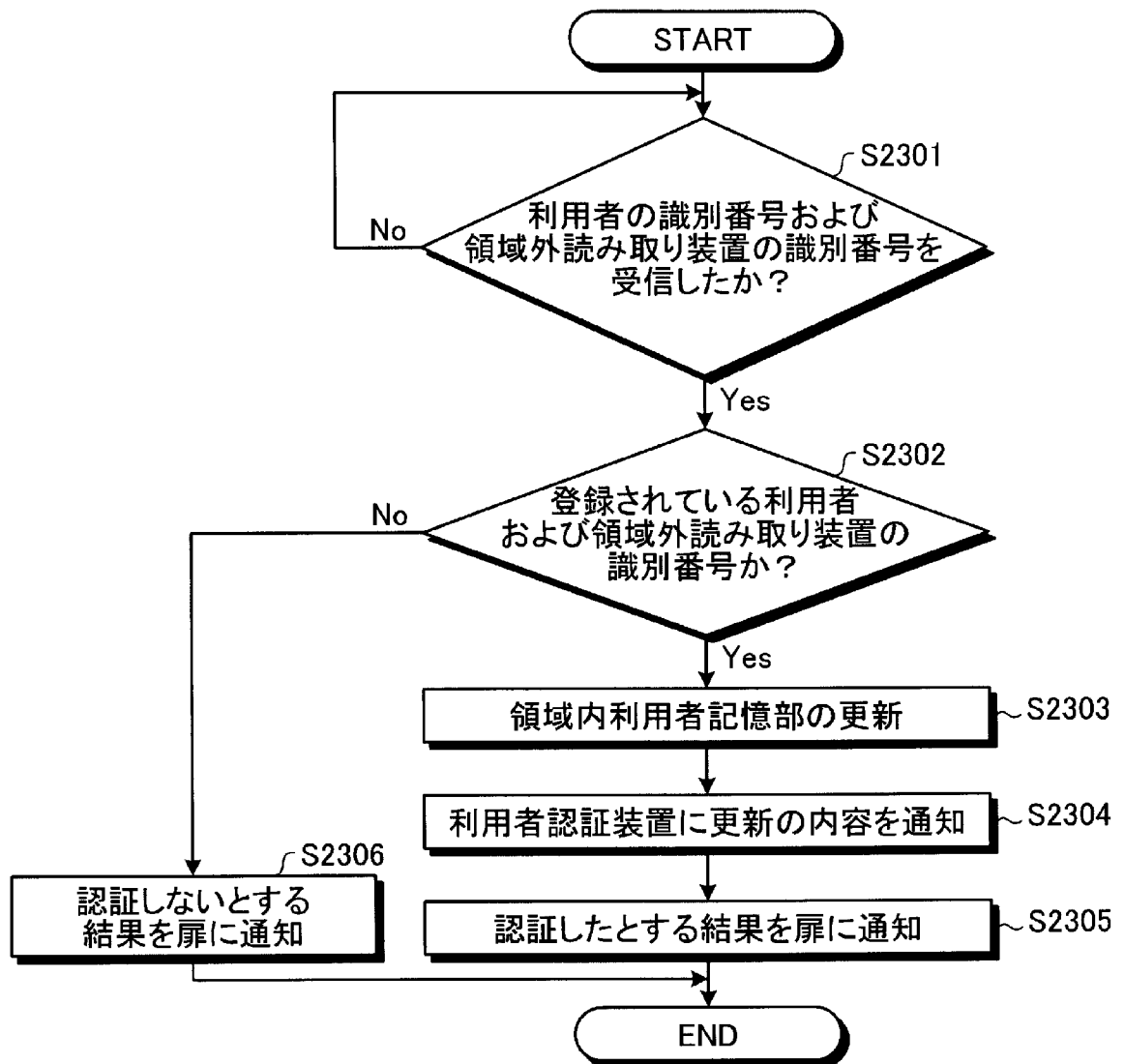
[図20]

識別番号
00005
00100
00088
⋮
00001

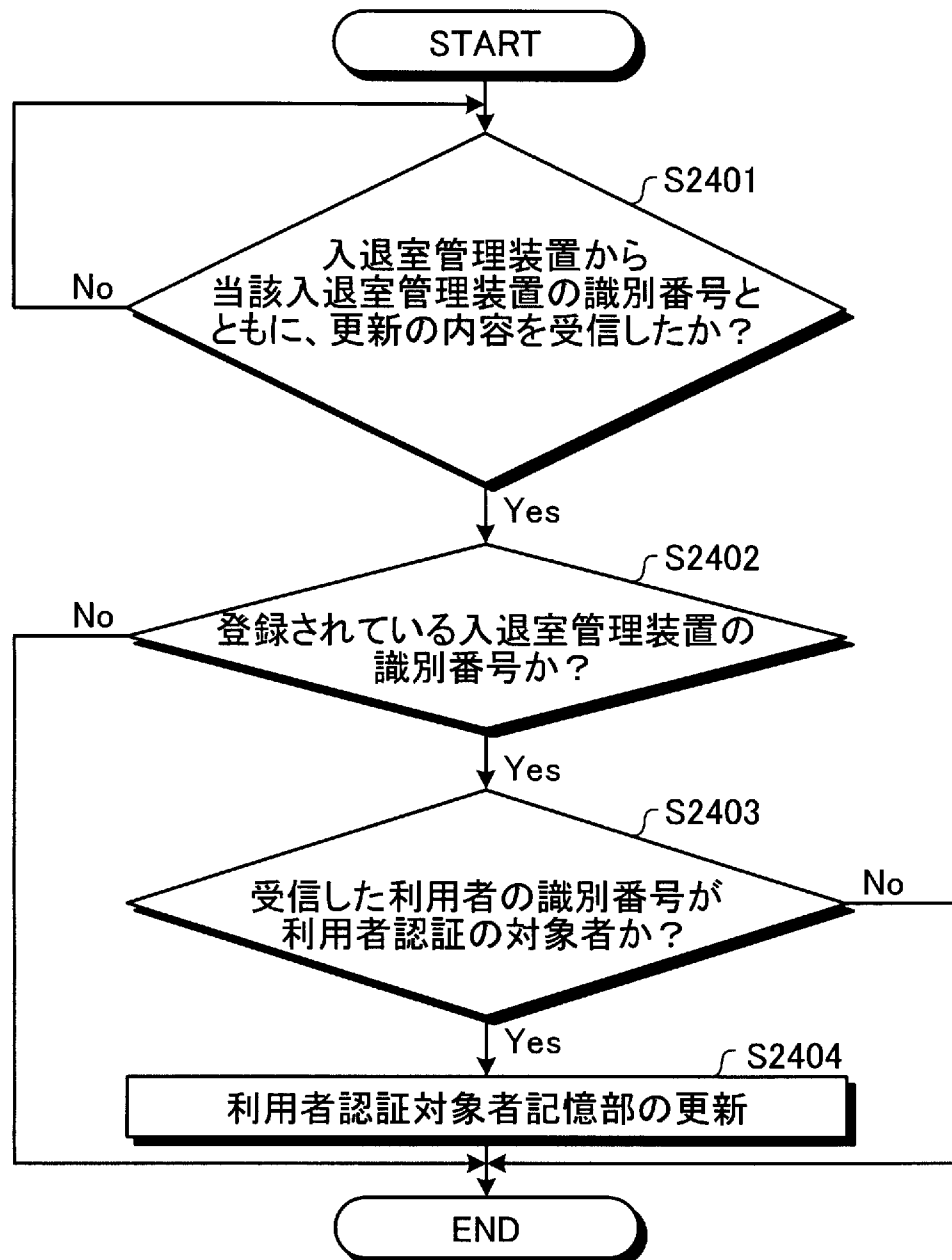
情報端末 識別番号	生体情報読み取り装置 識別番号
C001	S001
C002	S002
C003	S003
C004	S004
C005	S005
C006	S006
▪	▪
▪	▪
▪	▪

[illegible]

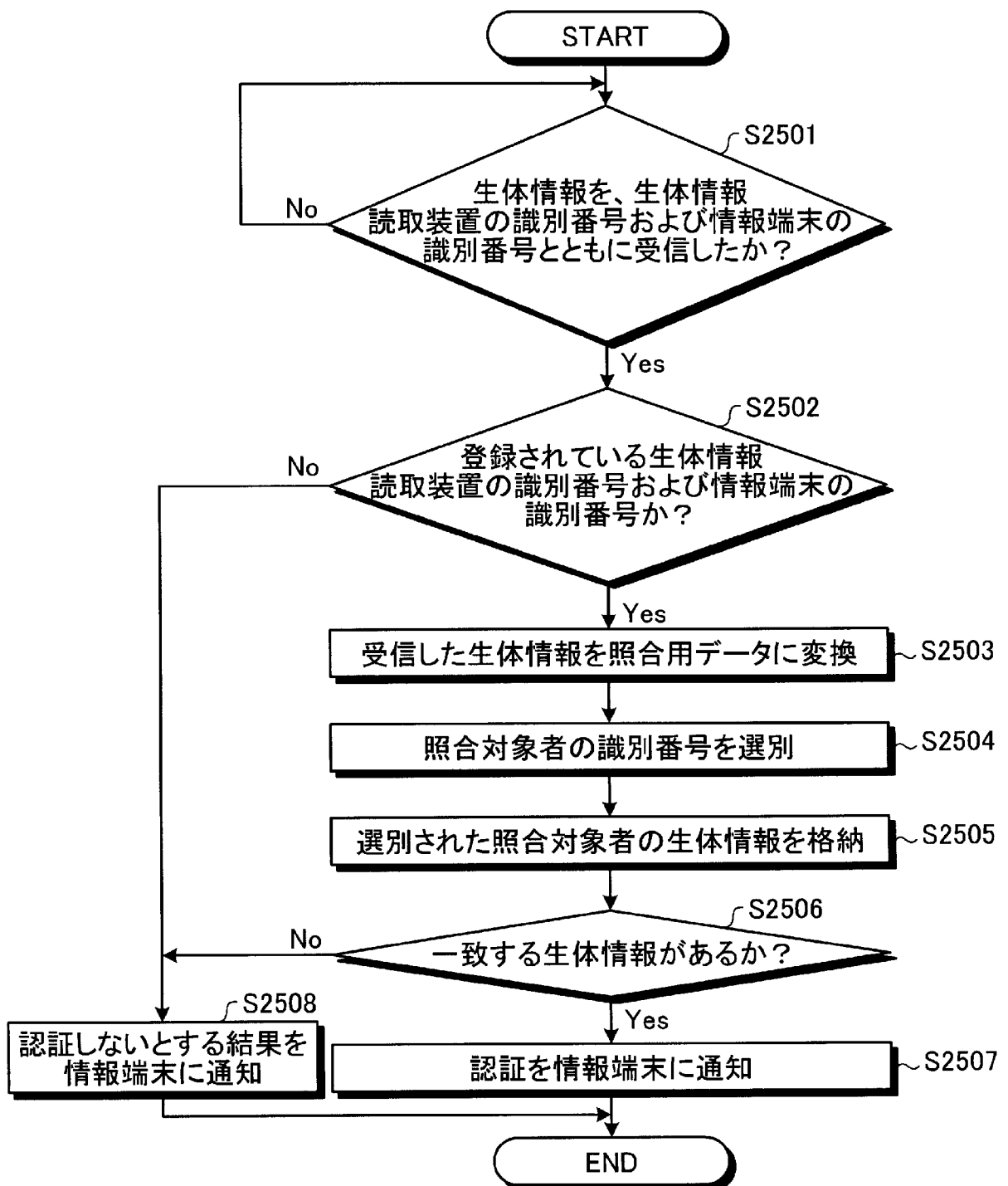
[図23]



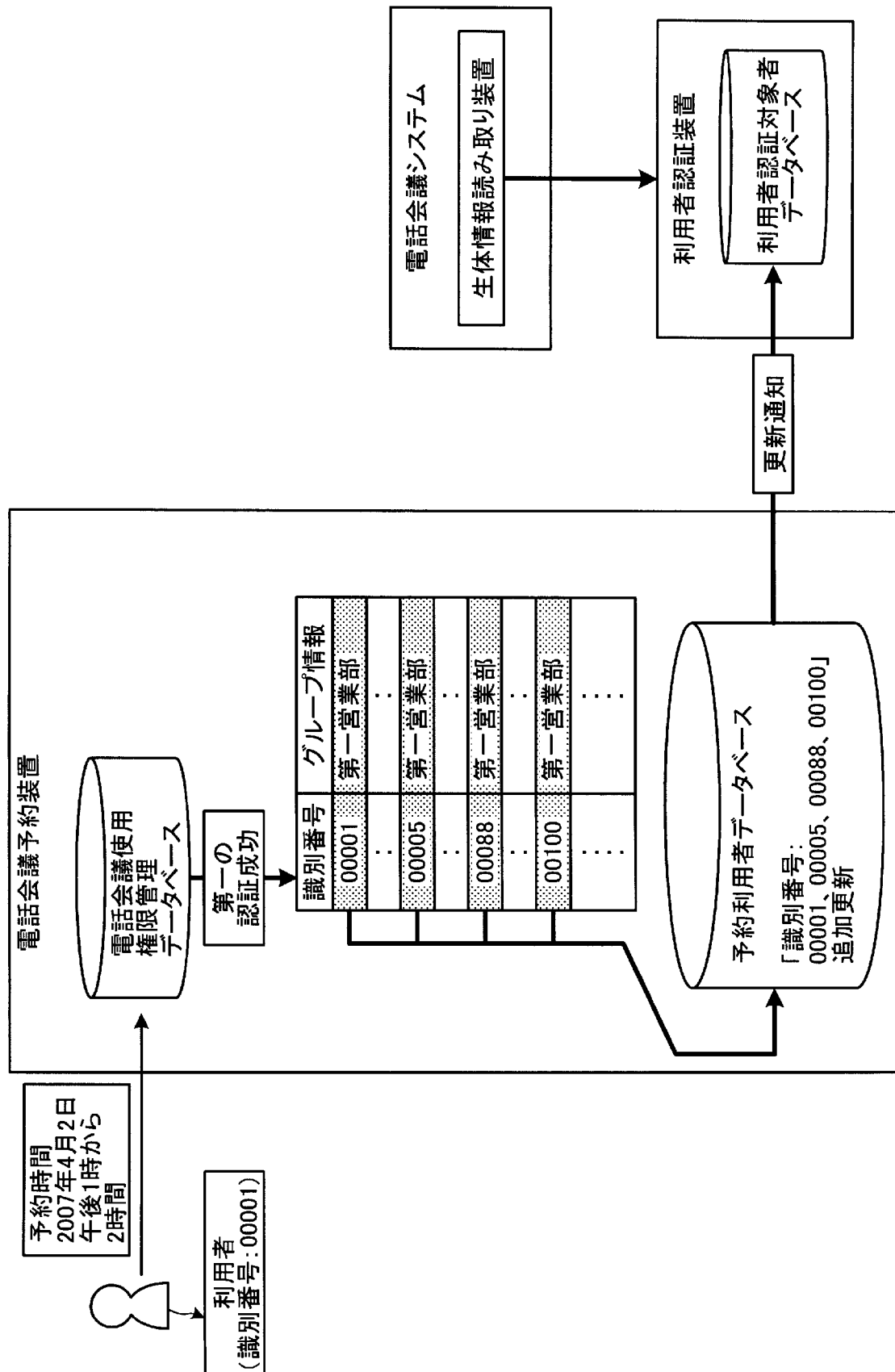
[図24]



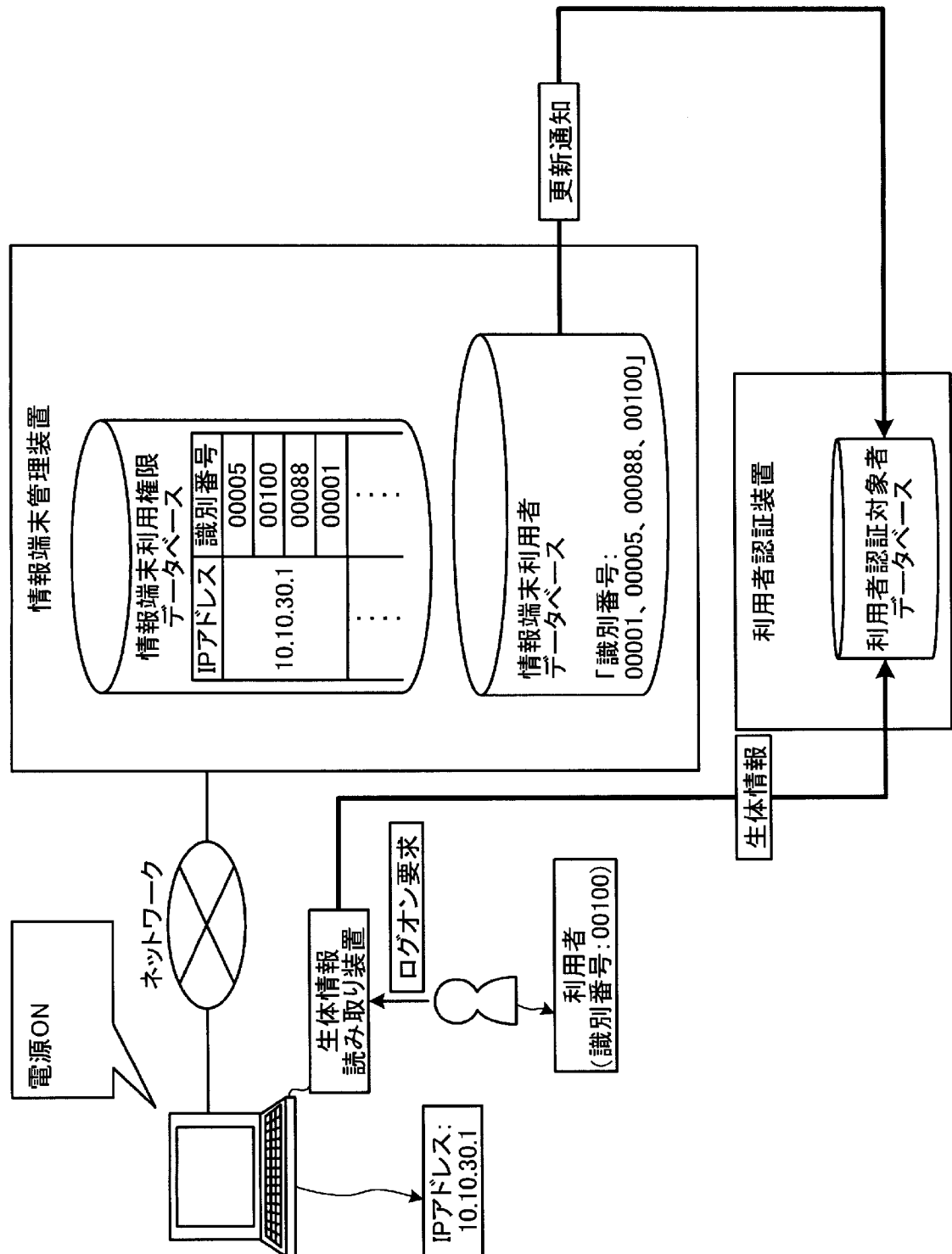
[図25]



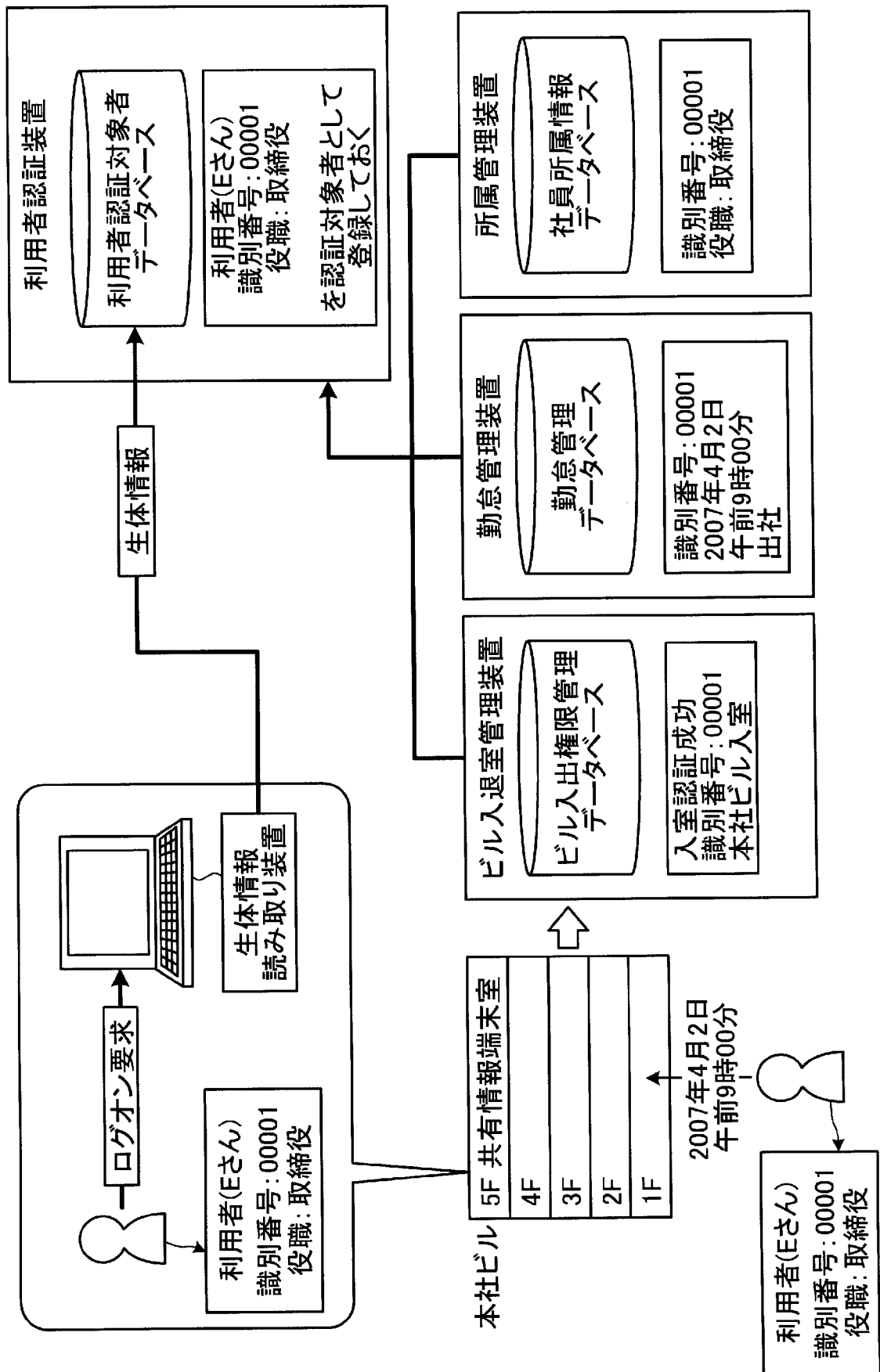
[図26]



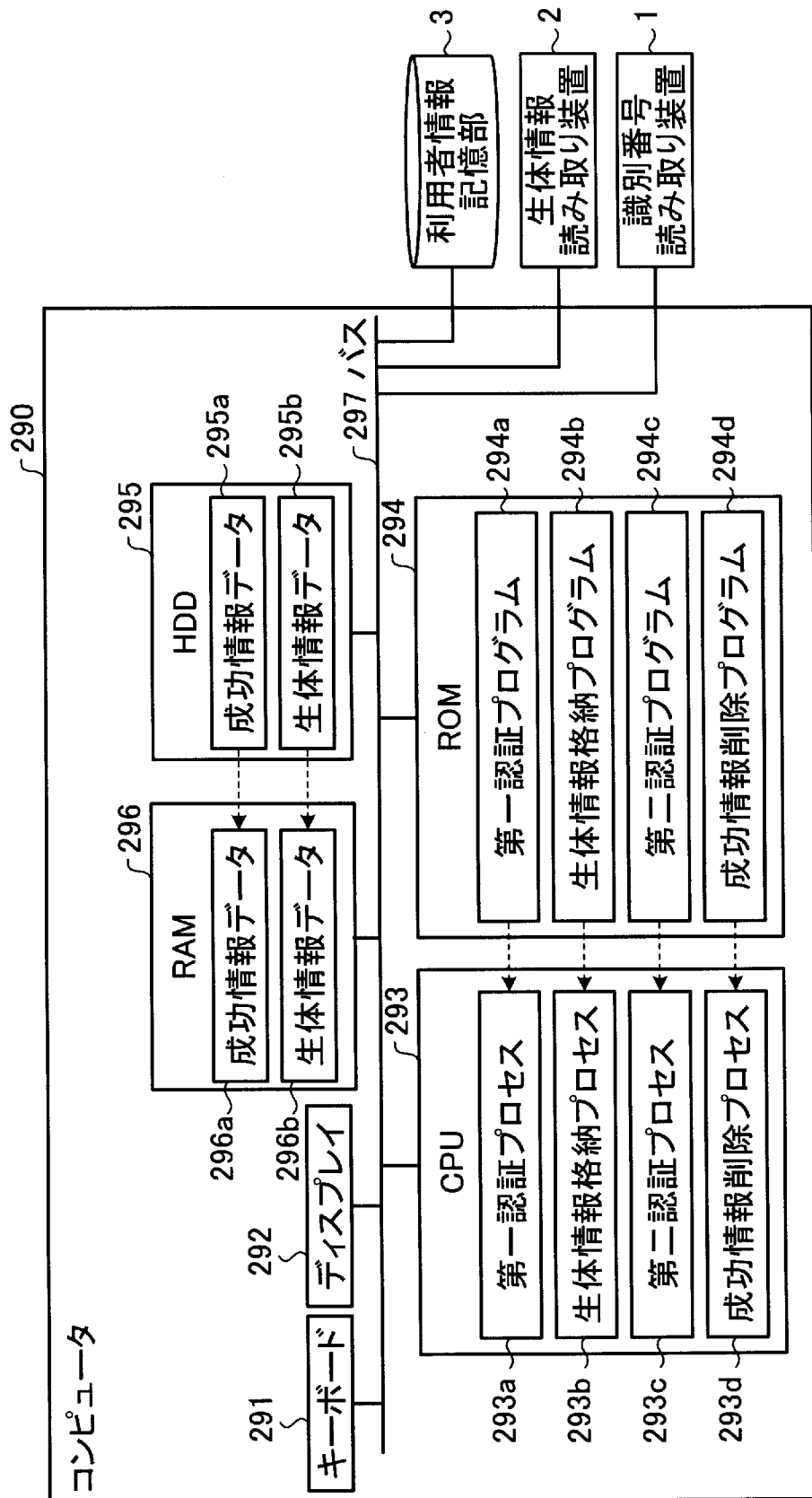
[図27]



[図28]



[図29]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2007/063850

A. CLASSIFICATION OF SUBJECT MATTER

G06F21/20 (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)

G06F21/20

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	JP 2003-196686 A (Omron Corp.), 11 July, 2003 (11.07.03), Par. Nos. [0088] to [0108]; Fig. 14 (Family: none)	1, 7, 9-10, 12, 16-20
Y	JP 2007-66107 A (Fujitsu Ltd.), 15 March, 2007 (15.03.07), Par. Nos. [0037], [0046] & US 2007/0050637 A1	2-5, 8, 11, 13-15
Y	JP 2002-194911 A (Ishikawajima Transport Machinery Co., Ltd.), 10 July, 2002 (10.07.02), Abstract; Par. No. [0014] (Family: none)	6

☒ 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
27 July, 2007 (27.07.07)

Date of mailing of the international search report
07 August, 2007 (07.08.07)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2007/063850

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2006-106827 A (Toshiba Corp.), 20 April, 2006 (20.04.06), Full text; all drawings (Family: none)	1-20

A. 発明の属する分野の分類（国際特許分類（I P C））

Int.Cl. G06F21/20(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. G06F21/20

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	JP 2003-196686 A（オムロン株式会社）2003.07.11, [0088]-[0108], 図14（ファミリーなし）	1, 7, 9-10, 12, 16-20
Y	JP 2007-66107 A（富士通株式会社）2007.03.15, [0037], [0046] & US 2007/0050637 A1	2-5, 8, 11, 13- 15
Y	JP 2002-194911 A（石川島運搬機械株式会社）2002.07.10, 要約, [0014]（ファミリーなし）	6

☒ 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

27.07.2007

国際調査報告の発送日

07.08.2007

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）

平井 誠

5 S

9 0 7 1

電話番号 03-3581-1101 内線 3546

C (続き) . 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
A	JP 2006-106827 A (株式会社東芝) 2006. 04. 20, 全文, 全図 (ファミリーなし)	1-20