

(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2016 年 2 月 4 日(04.02.2016)



(10) 国際公開番号
WO 2016/016997 A1

- (51) 国際特許分類:
H04M 1/673 (2006.01) **H04M 11/00** (2006.01)
- (21) 国際出願番号: PCT/JP2014/070216
- (22) 国際出願日: 2014 年 7 月 31 日(31.07.2014)
- (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: 日立マクセル株式会社 (HITACHI MAXELL, LTD.) [JP/JP]; 〒5678567 大阪府茨木市丑寅 1 丁目 1 番 8 8 号 Osaka (JP).
- (72) 発明者: 吉澤 和彦 (YOSHIZAWA, Kazuhiko); 〒5678567 大阪府茨木市丑寅 1 丁目 1 番 8 8 号 Osaka (JP). 益岡 信夫 (MASUOKA, Nobuo); 〒5678567 大阪府茨木市丑寅 1 丁目 1 番 8 8 号

Osaka (JP). 鈴木 基之 (SUZUKI, Motoyuki); 〒5678567 大阪府茨木市丑寅 1 丁目 1 番 8 8 号 Osaka (JP). 橋本 康宣 (HASHIMOTO, Yasunobu); 〒5678567 大阪府茨木市丑寅 1 丁目 1 番 8 8 号 Osaka (JP).

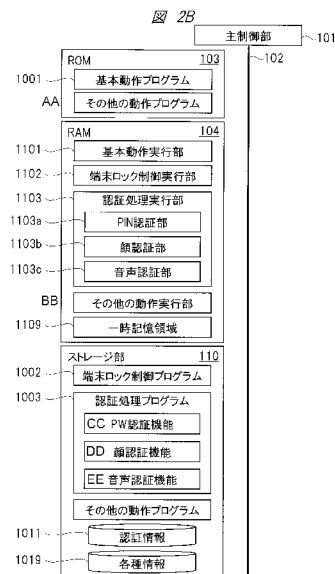
(74) 代理人: 筒井 大和 (TSUTSUI, Yamato); 〒1600022 東京都新宿区新宿 2 丁目 3 番 1 0 号 新宿御苑ビル 3 階 筒井国際特許事務所 Tokyo (JP).

(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, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX,

[続葉有]

(54) Title: MOBILE INFORMATION TERMINAL, METHOD FOR CONTROLLING MOBILE INFORMATION TERMINAL, AND COMMUNICATION SYSTEM

(54) 発明の名称: 携帯情報端末および携帯情報端末の制御方法ならびに通信システム



- 101 Primary control unit
103 ROM
104 RAM
110 Storage unit
1001 Basic operation program
1002 Terminal lock control program
1003 Authentication process program
1011 Authentication information
1019 Various information
1101 Basic operation execution unit
1102 Terminal lock control execution unit
1103 Authentication process execution unit
1103a PIN authentication unit
1103b Face authentication unit
1103c Voice authentication unit
1109 Temporary memory area
AA Miscellaneous operation programs
BB Miscellaneous operation execution units
CC Password authentication function
DD Face authentication function
EE Voice authentication function

(57) Abstract: Provided is a mobile information terminal that can execute a plurality of authentication processes for releasing a function lock state in which the operations of various functions are restricted. This personal information terminal has a primary control unit that selects one authentication process from among the plurality of authentication processes, in accordance with the detected surrounding conditions of the mobile information terminal, and executes the selected authentication process.

(57) 要約: 各種機能の動作が制限される機能ロック状態を解除する認証処理を複数、実行可能な携帯情報端末であって、検出された前記携帯情報端末の周辺の状況に応じて複数の前記認証処理から一つの前記認証処理を選択し、選択した前記認証処理を実行する主制御部を有する。

WO 2016/016997 A1



MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, 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, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ

パ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

添付公開書類:

— 国際調査報告 (条約第 21 条(3))

明 細 書

発明の名称：

携帯情報端末および携帯情報端末の制御方法ならびに通信システム

技術分野

[0001] 本発明は、携帯情報端末および携帯情報端末の制御方法ならびに通信システムに関する。

背景技術

[0002] 近年、スマートフォンやタブレット端末等の携帯情報端末の普及が進み、多数の者が携帯情報端末を保有するようになった。携帯情報端末は、ハードウェアの進化に伴い、多くの個人情報を持続可能となった。さらに、携帯情報端末を用いた金銭取引および各種決済処理等も可能になってきている。このため、携帯情報端末を操作者以外の人物に無断で使用された場合、個人情報の流出や、金銭的被害が発生する可能性がある。

[0003] このような被害が発生することを防止するため、携帯情報端末を使用可能な機能が制限された端末ロック状態にする端末ロック機能を備えることが一般的となってきた。また、正規ユーザの認証により端末ロック状態を解除する認証機能を備えることが一般的となっている。そして、近年の携帯情報端末においては、認証機能に要する認証処理を複数備えるものも多く存在する。

[0004] 特開 2007-49304 号公報（特許文献 1）には、「被写体を撮影するための撮像手段と、顔画像から抽出された特徴情報を登録特徴情報として予め記憶しておく特徴情報記憶手段と、上記撮像手段による撮影画像から特徴情報を抽出し、その特徴情報を上記登録特徴情報と比較することにより認証処理を行う認証処理手段と、上記撮像手段および上記認証処理手段を制御して、上記認証処理において認証に失敗した場合に再度撮影を行い、その撮影画像に基づく認証処理を行うことにより、一連の認証処理を行う連続認証手段とを備え、上記連続認証手段は、上記一連の認証処理中に所定回数の認

証処理において特徴情報の抽出に失敗したことを終了条件として、認証処理を終了する」と記載されている。

[0005] また、特許文献1には、「上記終了条件が成立して認証処理が終了した場合に、暗証番号入力による認証処理を行う」と記載されている。

先行技術文献

特許文献

[0006] 特許文献1：特開2007-49304号公報

発明の概要

発明が解決しようとする課題

[0007] 特許文献1に記載された技術では、撮影画像に基づく認証処理が成功し得ない環境（例えば、光量が不足している環境）においても、撮影画像に基づく認証処理を実行してしまう。そして、特許文献1に記載された技術では、撮影画像に基づく認証処理が失敗した後に、改めて暗証番号入力による認証処理を実行することとなる。そのため、撮像画像に基づく認証処理と暗証番号による認証処理とを実行する手間が発生し、使い勝手が良くないという問題があった。

[0008] 本発明の目的は、携帯情報端末の使い勝手を向上させる技術を提供することである。

課題を解決するための手段

[0009] 前記課題を解決するための手段として、請求の範囲に記載された技術を用いる。

[0010] 一例を挙げるならば、各種機能の動作が制限される機能ロック状態を解除する認証処理を複数、実行可能な携帯情報端末であって、検出された前記携帯情報端末の周辺の状況に応じて複数の前記認証処理から一つの前記認証処理を選択し、選択した前記認証処理を実行する。

発明の効果

[0011] 本願において開示される発明のうち、代表的なものによって得られる効果

を簡単に説明すれば以下のとおりである。

[0012] 本発明の一実施の形態によれば、携帯情報端末の使い勝手を向上させることが可能になる。

図面の簡単な説明

[0013] [図1]実施例1に係る通信システムの構成例の概要を示す図である。

[図2A]実施例1に係る携帯情報端末のハードウェア構成図である。

[図2B]実施例1に係る携帯情報端末のソフトウェア構成図である。

[図2C] (a) および (b) は、実施例1に係る携帯情報端末の外観図であり、(a) は、携帯情報端末の正面図、(b) は、携帯情報端末の背面図である。

[図3]実施例1に係る携帯情報端末の状態遷移図である。

[図4A]実施例1に係る携帯情報端末の認証処理動作の概要を示す図である。

[図4B]実施例1に係る携帯情報端末の認証処理動作の概要を示す図である。

[図4C]実施例1に係る携帯情報端末の認証処理動作の概要を示す図である。

[図5]実施例2に係る携帯情報端末の認証処理動作の概要を示す図である。

[図6A]実施例3に係る携帯情報端末の認証処理動作の概要を示す図である。

[図6B]実施例3に係る携帯情報端末の認証処理動作の概要を示す図である。

[図7]実施例4に係る携帯情報端末の認証処理動作の概要を示す図である。

[図8]実施例5に係る携帯情報端末の認証処理動作の概要を示す図である。

[図9]実施例6に係る通信システムの構成例の概要を示す図である。

[図10]実施例6に係る認証サーバの構成例の概要を示す図である。

[図11]実施例6に係る携帯情報端末のソフトウェア構成図である。

[図12]実施例6に係る携帯情報端末の認証処理動作の概要を示す図である。

発明を実施するための形態

[0014] 以下、本発明の実施の形態を図面に基づいて詳細に説明する。なお、実施の形態を説明するための全図において、同一部には原則として同一の符号を付し、その繰り返しの説明は省略する。

[0015] 実施例1の携帯情報端末は複数の認証処理を実行可能であり、携帯情報端

末の周辺の照度の照度レベルを検出する照度センサを有する。そして、照度センサにより検出された照度レベルが所定値以上である場合に、複数の認証処理から顔認証による認証処理を選択する。一方、センサ部により検出された照度レベルが所定値未満である場合に、複数の認証処理から操作者から入力を受け付けた情報（PIN（Personal Identification Number）コード）を照合する認証処理を選択する。これによって、顔認証が可能な場合は、顔認証による認証処理を実行し、顔認識が困難である場合でも、PINコードを照合する認証処理を選択し、実行することができるようになる。そのため、顔認証による認証処理をすることが困難な状況であっても、顔認証による認証処理とPINコードを照合する認証処理とを実行することなく、PINコードを照合する認証処理だけを実行できるようになり、携帯情報端末の使い勝手を向上させることができるようになる。

[0016] [実施例1]

<システム構成>

図1は、実施例1に係る通信システムの構成例の概要を示す図である。図1に示されるように、通信システムは、携帯情報端末100と、アクセスポイント200aと、移動体電話通信網の基地局300bと、移動体電話通信サーバ300と、アプリケーションサーバ400とを有する。

[0017] アクセスポイント200aと、移動体電話通信サーバ300と、アプリケーションサーバ400とは、インターネット200を介して相互に接続される。なお、インターネット200は、例えば、ブロードバンドネットワークが該当する。

[0018] 携帯情報端末100は、無線通信を介してアクセスポイント200aと接続される。また、アクセスポイント200aは、無線通信または有線通信を介してインターネット200と接続される。これによって、携帯情報端末100は、アクセスポイント200aを介してインターネット200に接続される。

[0019] また、携帯情報端末１００は、無線通信を介して移動体電話通信網の基地局３００ｂと接続される。また、基地局３００ｂは、無線通信を介して移動体電話通信サーバ３００と接続される。また、移動体電話通信サーバ３００は、無線通信または有線通信を介してインターネット２００と接続される。これによって、携帯情報端末１００は、移動体電話通信網の基地局３００ｂおよび移動体電話通信サーバ３００を介してインターネット２００に接続される。これによって、携帯情報端末１００は、電話通信サーバ３００およびアプリケーションサーバ４００との間で、インターネット２００を介してデータを送受信する。

[0020] 移動体電話通信サーバ３００は携帯情報端末１００の移動体電話通信網を介した電話通信（通話）およびデータ送受信を管理する。

[0021] アプリケーションサーバ４００には、一般的なアプリケーションや動作プログラム、コンテンツなどが記憶されている。また、アプリケーションサーバ４００は、記憶されている各種データを配信する。なお、アプリケーションサーバ４００は、複数、存在しても良い。

[0022] 携帯情報端末１００（例えば、携帯電話や、スマートフォンや、タブレット端末）は、各種機能の使用が制限された端末ロック状態へと切り替える、端末ロック機能を備える。また、携帯情報端末１００は、正規ユーザを認証することにより、端末ロック機能による端末ロック状態を解除する認証機能を備える。

[0023] なお、携帯情報端末１００は、ＰＤＡ（Personal Digital Assistants）やノート型ＰＣ（Personal Computer）、電子ブックリーダ等であっても良い。また、デジタルスチルカメラや動画撮影可能なビデオカメラ、携帯型ゲーム機等、またはその他の携帯用デジタル機器であっても良い。

[0024] ＜携帯情報端末のハードウェア構成＞

図２Ａは、実施例１に係る携帯情報端末１００のハードウェア構成図である。図２Ａに示されるように、携帯情報端末１００は、主制御部１０１と、

システムバス１０２と、ROM１０３と、RAM１０４と、ストレージ部１１０と、通信処理部１２０と、拡張インタフェース部（図中、拡張Ｉ／Ｆ部）１２４と、操作部１３０と、画像処理部１４０と、音声処理部１５０と、センサ部１６０とから構成される。

[0025] 主制御部１０１は、所定の動作プログラムに従って携帯情報端末１００全体を制御するマイクロプロセッサユニットである。

[0026] システムバス１０２は、主制御部１０１と携帯情報端末１００内の各動作ブロック（ROM１０３、RAM１０４、ストレージ部１１０、通信処理部１２０、拡張インタフェース部１２４、操作部１３０、画像処理部１４０、音声処理部１５０、センサ部１６０）との間でデータ送受信を行うためのデータ通信路である。

[0027] ROM（Read Only Memory）１０３は、オペレーティングシステム等の基本動作プログラムやその他の動作プログラムが記憶されているメモリであり、例えばEEPROM（Electrically Erasable Programmable ROM）やフラッシュROMのような書き換え可能なROMが用いられる。

[0028] RAM（Random Access Memory）１０４は、基本動作プログラムやその他の動作プログラム実行時のワークエリアとなる。

[0029] なお、ROM１０３およびRAM１０４を主制御部１０１と一体で構成するようにしても良い。また、ROM１０３は、図２Ａに示されるような独立した構成とはせず、ストレージ部１１０の一部の記憶領域を使用するようにしても良い。

[0030] ストレージ部１１０には、携帯情報端末１００の動作設定値や動作プログラムが記憶されている。また、ストレージ部１１０には、携帯情報端末１００のユーザの個人情報や、携帯情報端末１００の操作者が正規のユーザであるか否かを確認するための認証情報等が記憶されている。

[0031] また、ストレージ部１１０には、インターネット２００を介してダウンロードした動作プログラムや動作プログラムで作成した各種データ等が記憶さ

れている。さらに、ストレージ部１１０には、インターネット２００を介してダウンロードされる、動画や、静止画や、音声等のコンテンツが記憶される。

[0032] なお、ストレージ部１１０の一部領域をもって、ROM１０３の機能の全部または一部を代替しても良い。ここで、ストレージ部１１０は、携帯情報端末１００に外部から電源が供給されていない状態であっても記憶されている情報を保持する必要がある。したがって、ストレージ部１１０には、例えば、フラッシュROMやSSD (Solid State Drive) 等の半導体素子メモリや、HDD (Hard Disc Drive) 等の磁気ディスクドライブが用いられる。

[0033] また、インターネット２００を介して接続される各サーバ装置からダウンロードすることにより、ROM１０３やストレージ部１１０に記憶されている各動作プログラムを更新および機能拡張することが可能である。

[0034] 通信処理部１２０は、LAN (Local Area Network) 通信部１２１と、電話網通信部１２２と、NFC (Near Field Communication) 通信部１２３とから構成される。

[0035] LAN通信部１２１は、アクセスポイント２００aを介してインターネット２００と接続される。そして、LAN通信部１２１は、インターネット２００上の各サーバ装置とデータを送受信する。なお、LAN通信部１２１とアクセスポイント２００aとは、Wi-Fi (登録商標) 等の無線接続を介して接続される。

[0036] 電話網通信部１２２は、移動体電話通信網の基地局３００bとの無線通信により、電話通信 (通話) およびデータの送受信を行う。

[0037] NFC通信部１２３は、対応するリーダ／ライタとの近接時に無線通信を行う。

[0038] LAN通信部１２１、電話網通信部１２２、NFC通信部１２３は、それぞれ符号回路や復号回路、アンテナ等を備える。なお、通信処理部１２０が、Bluetooth (登録商標) 通信部や赤外線通信部等、他の通信部を

さらに備えていても良い。

[0039] 拡張インタフェース部124は、携帯情報端末100の機能を拡張するためのインタフェース群であり、本実施例では、映像／音声インタフェース、USB(Universal Serial Bus)インタフェース、メモリインタフェース等で構成される。映像／音声インタフェースは、外部映像／音声出力機器からの映像信号／音声信号の入力、外部映像／音声入力機器への映像信号／音声信号の出力等を行う。USBインタフェースは、PC等と接続してデータの送受信を行う。なお、USBインタフェースは、キーボードやその他のUSB機器と接続してデータの送受信を行うようにしても良い。メモリインタフェースは、メモリカードやその他のメモリ媒体を接続してデータの送受信を行う。

[0040] 操作部130は、携帯情報端末100に対する操作指示の入力を受け付ける指示入力部である。本実施例では、操作部130は、表示部141に重ねて配置されるタッチパネルおよびボタンスイッチを並べた操作キーで構成される。なお、操作部130は、タッチパネルまたは操作キーの何れか一方のみで構成されるようにしても良い。また、拡張インタフェース部124に接続されたキーボード等を用いて携帯情報端末100に対する操作指示の入力を受け付けるようにしても良い。さらに、有線通信または無線通信を介して接続された別体の携帯情報端末機器を用いて携帯情報端末100に対する操作指示の入力を受け付けるようにしても良い。また、タッチパネル機能を、表示部141が備えるようにしても良い。

[0041] 画像処理部140は、表示部141と、画像信号処理部142と、第一画像入力部143と、第二画像入力部144とから構成される。

[0042] 表示部141は、例えば液晶パネル等の表示デバイスであり、画像信号処理部142で処理した画像データを携帯情報端末100のユーザに提供する。

[0043] 画像信号処理部142は、図示を省略したビデオRAMを備える。そして、表示部141は、ビデオRAMに入力された画像データに基づいて駆動さ

れる。また、画像信号処理部 142 は、必要に応じてフォーマット変換を行う。また、画像信号処理部 142 は、メニューやその他の OSD (On Screen Display) 信号の重畳処理等を行う。

[0044] 第一画像入力部 143 および第二画像入力部 144 は、例えば、カメラが該当する。そして、第一画像入力部 143 および第二画像入力部 144 は、CCD (Charge Coupled Device) や CMOS (Complementary Metal Oxide Semiconductor) センサ等の電子デバイスを用いてレンズから入力された光を電気信号に変換することにより、周辺や対象物の画像データを入力する。

[0045] 音声処理部 150 は、音声出力部 151 と、音声信号処理部 152 と、音声入力部 153 とから構成される。

[0046] 音声出力部 151 はスピーカであり、音声信号処理部 152 で処理した音声信号を携帯情報端末 100 のユーザに提供する。音声入力部 153 はマイクであり、ユーザの声等を音声データに変換して入力する。

[0047] センサ部 160 は、携帯情報端末 100 の状態を検出するためのセンサ群であり、本実施例では、GPS (Global Positioning System) 受信部 161 と、ジャイロセンサ 162 と、地磁気センサ 163 と、加速度センサ 164 と、照度センサ 165 と、近接センサ 166 とから構成される。これらのセンサ群により、携帯情報端末 100 の位置、傾き、方角、動き、周囲の照度等を検出することが可能となる。なお、携帯情報端末 100 が、気圧センサ等の他のセンサをさらに備えていても良い。

[0048] 主制御部 101 は、センサ部 160 から送信されるデータに基づき、携帯情報端末 100 の状態を検出する。主制御部 101 は、検出した携帯情報端末 100 の状態に応じて複数の認証処理から一つの認証処理を選択する。そして、主制御部 101 は、選択した認証処理を実行する。

[0049] なお、図 2 A に示した携帯情報端末 100 の構成例は、本実施例に必須ではない構成も多数含んでいるが、これらが備えられていない構成であっても本実施例の効果を損なうことはない。また、デジタル放送受信機能や電子マ

ネー決済機能等、図示していない構成がさらに加えられていても良い。

[0050] <携帯情報端末のソフトウェア構成>

図2Bは、実施例1に係る携帯情報端末100のソフトウェア構成図である。図2Bに示されるように、ROM103には、基本動作プログラム1001と、その他の動作プログラムが記憶されている。また、ストレージ部110には、端末ロック制御プログラム1002と、認証処理プログラム1003と、その他の動作プログラムが記憶されている。

[0051] さらに、ストレージ部110は、認証情報記憶領域（図中、認証情報）1011と、各種情報記憶領域（図中、各種情報）1019とを有する。認証情報記憶領域1011には、携帯情報端末100の操作者が正規のユーザであるか否かを確認するための認証情報が記憶される。また、各種情報記憶領域1019には、その他の情報が記憶される。

[0052] 主制御部101は、ROM103に記憶されている基本動作プログラム1001を、RAM104に展開する。そして、主制御部101は、RAM104に展開した基本動作プログラム1001を実行する。これによって、基本動作実行部1101が構成される。なお、以下では、説明を簡単にするために、主制御部101がROM103に記憶されている基本動作プログラム1001をRAM104に展開して実行することにより各動作ブロックの制御することを、基本動作実行部1101が、各動作ブロックの制御を行うと記述する場合がある。

[0053] また、主制御部101は、ストレージ部110に記憶されている端末ロック制御プログラム1002をRAM104に展開する。そして、主制御部101は、RAM104に展開した端末ロック制御プログラム1002を実行する。これによって、端末ロック制御実行部1102が構成される。なお、以下では、主制御部101が、ストレージ部110に記憶されている端末ロック制御プログラム1002をRAM104に展開して実行することにより各動作ブロックの制御を行う処理を、端末ロック制御実行部1102が、各動作ブロックの制御を行うと記述する場合がある。

- [0054] また、主制御部１０１は、ストレージ部１１０に記憶されている認証処理プログラム１００３をＲＡＭ１０４に展開する。そして、主制御部１０１は、ＲＡＭ１０４に展開した認証処理プログラム１００３を実行する。これによって、認証処理実行部１１０３が構成される。なお、以下では、主制御部１０１が、ストレージ部１１０に記憶されている認証処理プログラム１００３をＲＡＭ１０４に展開して実行することにより各動作ブロックの制御することを、認証処理実行部１１０３が、各動作ブロックの制御を行うと記述する場合がある。
- [0055] ＲＡＭ１０４は、各動作プログラム実行時に作成したデータを、必要に応じて一時的に保持する一時記憶領域１１０９を備える。
- [0056] 端末ロック制御実行部１１０２は、携帯情報端末１００の動作状態を、携帯情報端末１００の各種機能の動作が制限される機能ロック状態とするか、或いは、携帯情報端末１００の各種機能の動作が許容されるアンロック状態とするかの制御をする。
- [0057] ここで、機能ロック状態とは、携帯情報端末１００の電源のオンおよびオフと、スリープモードの設定および解除と、機能ロック状態を解除するための操作以外の操作指示を受け付けない状態である。或いは、機能ロック状態は、操作部１３０がユーザから操作指示を受け付けても、操作指示を無効なものとすることで、操作指示に従った処理を主制御部１０１等に行わせないような状態であっても良い。なお、機能ロック状態は、電源オン状態におけるアクセスポイントや基地局のサーチや、メールチェックや、自動実行される各種機能については適宜許容されるようにしても良い。また、端末ロック制御実行部１１０２は、機能ロック状態において、必ずしも携帯情報端末１００の全ての機能の動作を制限せず、その一部の機能のみを制限するようにしても良い。
- [0058] 認証処理実行部１１０３は、携帯情報端末１００の操作者が正規のユーザであるか否かを確認するための認証処理動作（後述、図４Ａ～図４Ｃ）を実行する。携帯情報端末１００においては、認証処理実行部１１０３は、ＰＩ

N照合による認証処理、顔認識による認証処理、音声認識による認証処理、を実行可能である。すなわち、携帯情報端末100は、認証処理実行部1103の制御に基づいて、PIN照合による認証処理、顔認識による認証処理、音声認識による認証処理から、いずれかの認証処理を状況に応じて適宜選択して認証処理を行う。

[0059] なお、各動作プログラムは、製品出荷の時点で、予めROM103および／またはストレージ部110に記憶されている状態であっても良い。また、製品出荷後に、インターネット200上のその他のアプリケーションサーバ400等からLAN通信部121または電話網通信部122を介して取得されるようにしても良い。また、メモリカードや光ディスク等に記憶されている各動作プログラムを、拡張インタフェース部124等を介して取得するようにしても良い。

[0060] <携帯情報端末の概観>

図2C(a)および図2C(b)は、実施例1に係る携帯情報端末100の外観図であり、図2C(a)は、携帯情報端末100の正面図、図2C(b)は、携帯情報端末100の背面図である。なお、同図は、携帯情報端末100がスマートフォン等である場合の例を図示し、左側面と右側面および天面と底面に関しては図示を省略する。

[0061] 図2C(a)および図2C(b)に示されるように、携帯情報端末100は、電源キー130k1と、ホームキー130k2と、表示部141と、第一画像入力部143（例えば、カメラ）と、第二画像入力部144（例えば、カメラ）と、音声出力部151（例えば、スピーカ）と、音声入力部153（例えば、マイク）とを有する。

[0062] また、図2C(a)に示されるように、第一画像入力部143は、表示部141と同一面（表面）上に位置する。

[0063] また、図2C(b)に示されるように、第二画像入力部144は、表示部141の反対側の面（背面）上に位置する。

[0064] なお、第二画像入力部144は、第一画像入力部143と同一面でなけれ

ば背面以外に位置されるようにしても良い。たとえば、第二画像入力部 144 が、左側面、右側面、点面、底面のいずれかに位置されるようにしても良い。

[0065] また、第二画像入力部 144 を別個の端末が備えるようにしても良い。例えば、有線通信または無線通信を介して、第二画像入力部 144 と携帯情報端末 100 とがと接続されるものであっても良い。また、携帯情報端末 100 は、第一画像入力部 143 または第二画像入力部 144 の何れか一方のみを有するようにしても良い。また、携帯情報端末 100 が、デジタルスチルカメラである場合等、図 2C と異なる外観であっても良い。

[0066] 以下では、表示部 141 と同一面に位置する第一画像入力部 143 を「インカメラ」と呼び、表示部 141 と反対面に位置する第二画像入力部 144 を「アウトカメラ」と呼ぶ場合がある。

[0067] 電源キー 130k1 は、携帯情報端末 100 の主電源のオン／オフおよびスリープモードの設定／解除の入力を受け付ける操作キーである。

[0068] ホームキー 130k2 は、任意のアプリケーションプログラムの実行中に、表示部 141 に基本画面を表示させる入力を受け付けるための操作キーである。

[0069] <携帯情報端末の動作状態遷移>

図 3 は、本実施例の携帯情報端末 100 における動作状態の遷移状況の一例を説明する状態遷移図である。

[0070] 図 3 に示されるように、端末ロック機能が無効化されている携帯情報端末 100 の動作状態としては、端末ロック機能が無効化されている状態における通常動作状態 T100 と、端末ロック機能が無効化されている状態におけるスリープ状態 T101 と、端末ロック機能が無効化されている状態における電源オフ状態 T102 とがある。また、端末ロック機能が有効化されている携帯情報端末 100 の動作状態としては、端末ロック機能が有効化されている状態における通常動作状態 T110 と、端末ロック機能が有効化されている状態におけるスリープ状態 T111 と、端末ロック機能が有効化されて

いる状態における電源オフ状態 T 1 1 2 とがある。さらに、携帯情報端末 1 0 0 の動作状態としては、認証処理が実行されている認証処理動作状態 T 1 1 3 がある。

[0071] 端末ロック機能が無効化されている状態では、携帯情報端末 1 0 0 の動作状態は、スリープ状態 T 1 0 1 または電源オフ状態 T 1 0 2 から認証処理動作状態 T 1 1 3 を経ることなく通常動作状態 T 1 0 0 へと遷移する。

[0072] 一方、端末ロック機能が有効化されている状態では、携帯情報端末 1 0 0 の動作状態は、認証処理動作状態 T 1 1 3 を経て、スリープ状態 T 1 0 1 または電源オフ状態 T 1 0 2 から通常動作状態 T 1 0 0 へと遷移する。

[0073] 携帯情報端末 1 0 0 は、例えば、機能設定メニューが操作されることで、端末ロック機能の有効化または無効化を選択する入力を受け付ける。

[0074] すなわち、端末ロック機能が無効化されている状態における通常動作状態 T 1 0 0 にて、端末ロック機能の設定操作がされることで、携帯情報端末 1 0 0 の動作状態は、端末ロック機能を有効化した状態における通常動作状態 T 1 1 0 へと遷移する。

[0075] 一方、端末ロック機能を有効化した状態における通常動作状態 T 1 1 0 にて、端末ロック機能の解除操作がされることで、携帯情報端末 1 0 0 の動作状態は、端末ロック機能が無効化されている状態における通常動作状態 T 1 0 0 へと遷移する。

[0076] 端末ロック機能が無効化されている状態における通常動作状態 T 1 0 0 にて、携帯情報端末 1 0 0 が操作されないまま所定時間以上経過した場合、携帯情報端末 1 0 0 の動作状態は、端末ロック機能が無効化されている状態におけるスリープ状態 T 1 0 1 へと遷移する。

[0077] また、端末ロック機能が無効化されている状態における通常動作状態 T 1 0 0 にて、操作者からスリープ状態 T 1 0 1 へ遷移させるための入力を受け付けた場合、携帯情報端末 1 0 0 の動作状態は、端末ロック機能が無効化されている状態におけるスリープ状態 T 1 0 1 へと遷移する。

[0078] また、端末ロック機能が無効化されている状態における通常動作状態 T 1

００にて、操作者から電源をオフする入力を受け付けた場合、携帯情報端末１００の動作状態は、端末ロック機能が無効化されている状態における電源オフ状態Ｔ１０２へと遷移する。

[0079] 端末ロック機能が無効化されている状態におけるスリープ状態Ｔ１０１にて、操作者からスリープ状態を解除する入力を受け付けた場合、携帯情報端末１００の動作状態は、端末ロック機能が無効化されている状態における通常動作状態Ｔ１００へと遷移する。

[0080] 端末ロック機能が無効化されている状態における電源オフ状態Ｔ１０２にて、操作者から電源オンする入力を受け付けた場合、携帯情報端末１００の動作状態は、端末ロック機能が無効化されている状態における通常動作状態Ｔ１００へと遷移する。

[0081] 端末ロック機能が有効化されている状態における通常動作状態Ｔ１１０にて、携帯情報端末１００が操作されないまま所定時間以上経過した場合、携帯情報端末１００の動作状態は、端末ロック機能が有効化されている状態におけるスリープ状態Ｔ１１１へと遷移する。

[0082] また、端末ロック機能が有効化されている状態における通常動作状態Ｔ１１０にて、操作者からスリープ状態Ｔ１１１へ遷移させるための入力を受け付けた場合、携帯情報端末１００の動作状態は、端末ロック機能が有効化されている状態におけるスリープ状態Ｔ１１１へと遷移する。

[0083] また、端末ロック機能が有効化されている状態における通常動作状態Ｔ１１０にて、操作者から電源をオフする入力を受け付けた場合、携帯情報端末１００の動作状態は、端末ロック機能が有効化されている状態における電源オフ状態Ｔ１１２へと遷移する。

[0084] 端末ロック機能が有効化されている状態におけるスリープ状態Ｔ１１１にて、操作者からスリープ状態を解除する入力を受け付けた場合、携帯情報端末１００の動作状態は、認証処理動作状態Ｔ１１３へと遷移し、認証処理動作が実行される。

[0085] 端末ロック機能が有効化されている状態における電源オフ状態Ｔ１１２に

て、操作者から電源オンする入力を受け付けた場合、携帯情報端末１００の動作状態は、認証処理動作状態Ｔ１１３へと遷移し、認証処理動作が実行される。

[0086] 認証処理動作状態Ｔ１１３での認証処理動作にて、操作者の認証に成功した場合には、携帯情報端末１００の動作状態は、端末ロック機能が有効化されている状態における通常動作状態Ｔ１１０へ遷移する。一方、操作者の認証に失敗した場合には、携帯情報端末１００の動作状態は、端末ロック機能が有効化されている状態におけるスリープ状態Ｔ１１１へ遷移する。

[0087] <認証処理動作>

本実施例の携帯情報端末１００は複数の認証処理を実行可能であり、センサ等により確認した携帯情報端末１００の周辺の状況や操作者の状態や動作設定等に応じて、複数の認証処理からいずれか一つの認証処理を選択し、選択した認証処理を実行する。

[0088] 実施例１に係る携帯情報端末１００における認証処理動作は、認証処理実行部１１０３と端末ロック制御実行部１１０２、および基本動作実行部１１０１によって制御される。

[0089] なお、携帯情報端末１００が、認証処理実行部１１０３および端末ロック制御実行部１１０２と同等の動作をハードウェアで実現する各ハードウェアブロックをさらに備えるようにしても良い。その場合、各ハードウェアブロックが、認証処理実行部１１０３および端末ロック制御実行部１１０２に代替して携帯情報端末１００の動作を実行する。

[0090] 以下、図４Ａ～図４Ｃを用いて、実施例１に係る携帯情報端末１００の認証処理動作を説明する。

[0091] まず、図４Ａを用いて、携帯情報端末１００の周辺の照度レベルに応じて実行する認証処理を選択する認証処理動作について説明する。

[0092] まず、Ｓ１０１にて、基本動作実行部１１０１は、要求された機能ロック解除要求を認識する。Ｓ１０１にて、基本動作実行部１１０１が、基本ロック解除要求を認識しない場合（Ｓ１０１－Ｎｏ）、Ｓ１０１へ進む。一方、

S 1 0 1 にて、基本動作実行部 1 1 0 1 が、機能ロック解除要求を認識した場合（S 1 0 1 − Y e s）、S 1 0 2 へ進む。

[0093] なお、端末ロック機能が有効化されている状態におけるスリープ状態 T 1 1 1（前述、図 3）にて、操作者からスリープ状態を解除する入力を受け付けると、基本動作実行部 1 1 0 1 は、スリープ状態解除の指示を検出する。そして、基本動作実行部 1 1 0 1 は、検出したスリープ状態解除の指示を機能ロック状態の解除要求として認識する。

[0094] また、端末ロック機能が有効化されている状態における電源オフ状態 T 1 1 2（前述、図 3）にて、操作者から電源オンする入力を受け付けると、基本動作実行部 1 1 0 1 は、電源オンの指示を検出する。そして、基本動作実行部 1 1 0 1 は、検出した電源オンの指示を機能ロック状態の解除要求として認識する。

[0095] 次に、S 1 0 2 にて、基本動作実行部 1 1 0 1 は、照度センサ 1 6 5 を有効化する。

[0096] 次に、S 1 0 3 にて、照度センサ 1 6 5 は、携帯情報端末 1 0 0 の周辺の照度を検出する。

[0097] 次に、S 1 0 4 にて、基本動作実行部 1 1 0 1 は、S 1 0 3 にて検出された照度の照度レベルが所定値以上かを判定する。S 1 0 4 にて、基本動作実行部 1 1 0 1 が、照度レベルが所定値以上であると判定する場合（S 1 0 4 − Y e s）、S 1 0 7 へ進む。一方、S 1 0 4 にて、基本動作実行部 1 1 0 1 が、照度レベルが所定値未満であると判定する場合（S 1 0 4 − N o）、S 1 0 5 へ進む。

[0098] 次に、S 1 0 5 にて、基本動作実行部 1 1 0 1 は、表示部 1 4 1 に P I N 入力画面を表示させる。そして、携帯情報端末 1 0 0 の操作部 1 3 0 は、操作者から数字列（P I N コード）の入力を受け付ける。

[0099] 次に、S 1 0 6 にて、認証処理実行部 1 1 0 3 の P I N 認証部 1 1 0 3 a は、S 1 0 5 にて入力を受け付けた数字列を照合する認証処理（P I N 照合による認証処理）を実行する。そして、P I N 認証部 1 1 0 3 a は、携帯情

報端末 100 の操作者が正規のユーザかを判定する。これによって、照度レベルが所定値未満であり、顔認識が困難である場合でも、PINコードを照合する認証処理を実行し、携帯情報端末 100 の操作者が正規のユーザかを判定できるようになる。S106 の次は、S109 へ進む。

[0100] なお、数字列を照合する認証処理は公知の技術を用いれば良いため詳細な説明を省略する。例えば、PIN認証部 1103a は、携帯情報端末 100 の操作部 130 が入力を受け付けた数字列が、認証情報記憶領域 1011 に正規ユーザにより指定されることで登録される数字列と一致するか否かを判定する。

[0101] 一方、S104 にて Yes だった場合（周辺の照度レベルが所定値以上で、顔認証が可能な場合）、S107 にて、基本動作実行部 1101 は、第一画像入力部 143（インカメラ）を有効化する。

[0102] 次に、S108 にて、認証処理実行部 1103 の顔認証部 1103b は、顔認証による認証処理を実行する。そして、顔認証部 1103b は、携帯情報端末 100 の操作者が正規のユーザかを判定する。なお、顔認識による認証処理は公知の技術を用いれば良いため詳細な説明を省略する。例えば、顔認証部 1103b は、第一画像入力部 143 で撮像された携帯情報端末 100 の操作者の顔画像データから特徴点を抽出し、認証情報記憶領域 1011 に予め登録されている正規ユーザの顔画像データの特徴点と比較して一致度を確認することで、顔認証による認証処理を実行する。

[0103] 次に、S109 にて、携帯情報端末 100 の操作者が正規のユーザであり、認証が成功したか否かが判定される。S106 の PIN 照合による認証処理または S108 の顔認証による認証処理の結果、携帯情報端末 100 の操作者が正規のユーザでないと判定される場合（S109-No）、携帯情報端末 100 の機能ロック状態が解除されずに S101 へ戻る。一方、S106 の PIN 照合による認証処理または S108 の顔認証による認証処理の結果、携帯情報端末 100 の操作者が正規のユーザであると判定される場合（S109-Yes）、S110 へ進む。

- [0104] 次に、S 1 1 0にて、携帯ロック制御実行部 1 1 0 2は、携帯情報端末 1 0 0の機能ロック状態を解除する。そして、携帯情報端末 1 0 0の動作状態は、スリープ状態 T 1 1 1または電源オフ状態 T 1 1 2から通常動作状態 T 1 1 0へと遷移する。
- [0105] 以上の処理により、本実施例の携帯情報端末 1 0 0は、周辺の照度レベルに応じて実行する認証処理を選択することが可能になり、携帯情報端末 1 0 0の使い勝手を向上させることができるようになる。
- [0106] なお、S 1 0 6にて実行される認証処理は、画像に基づいて実行される認証処理でなければ、P I N照合による認証処理に限られるものではない。例えば、操作部 1 3 0が、操作者からパスワードの入力を受け付け、入力を受け付けたパスワードと予め記憶されているパスワードとが一致するかを照合するようにしても良い。また、操作部 1 3 0が、操作キーへの入力を複数回受け付け、入力を受け付けた操作キーと操作順との組み合わせが、予め記憶されている操作キーと操作順との組み合わせと一致するかを照合するようにしても良い。
- [0107] また、S 1 0 8にて実行される認証処理は、顔認証による認証処理に限られるものではない。例えば、カメラで撮像される画像に基づいて認証処理を行う場合、虹彩パターンに基づいた認証処理や掌紋認証等を適用しても良い。
- [0108] 次に、図 4 Bを用いて、携帯情報端末 1 0 0の周辺の照度レベルに応じて実行する認証処理を選択する認証処理動作の変形例について説明する。図 4 Aにて説明した認証処理動作では、携帯情報端末の周辺の照度レベルが不足している場合に、P I Nコードを照合する認証処理を実行する。一方、図 4 Bにおける認証処理動作では、携帯情報端末 1 0 0の周辺の照度レベルが不足している場合に、表示部 1 4 1を補助光源として使用する点で異なる。また、補助光源を使用した後の照度レベルが不足している場合に、P I Nコードを照合する認証処理を実行する。
- [0109] なお、図 4 BのS 2 0 1～S 2 0 4は、図 4 AのS 1 0 1～S 1 0 4に相

当する。また、図４ＢのＳ２０８～Ｓ２１３は、図４ＡのＳ１０５～Ｓ１１０に相当する。すなわち、図４Ａの認証処理動作に対して、図４Ｂの認証処理動作は、Ｓ２０５～Ｓ２０７の処理を有する点で異なる。

[0110] まず、Ｓ２０１にて、基本動作実行部１１０１は、要求された機能ロック解除要求を認識する。Ｓ２０１にて、基本動作実行部１１０１が、基本ロック解除要求を認識しない場合（Ｓ２０１－Ｎｏ）、Ｓ２０１へ進む。一方、Ｓ２０１にて、基本動作実行部１１０１が、機能ロック解除要求を認識した場合（Ｓ２０１－Ｙｅｓ）、Ｓ２０２へ進む。

[0111] なお、端末ロック機能が有効化されている状態におけるスリープ状態Ｔ１１１（前述、図３）にて、操作者からスリープ状態を解除する入力を受け付けると、基本動作実行部１１０１は、スリープ状態解除の指示を検出する。そして、基本動作実行部１１０１は、検出したスリープ状態解除の指示を機能ロック状態の解除要求として認識する。

[0112] また、端末ロック機能が有効化されている状態における電源オフ状態Ｔ１１２（前述、図３）にて、操作者から電源オンする入力を受け付けると、基本動作実行部１１０１は、電源オンの指示を検出する。そして、基本動作実行部１１０１は、検出した電源オンの指示を機能ロック状態の解除要求として認識する。

[0113] 次に、Ｓ２０２にて、基本動作実行部１１０１は、照度センサ１６５を有効化する。

[0114] 次に、Ｓ２０３にて、照度センサ１６５は、携帯情報端末１００の周辺の照度を検出する。

[0115] 次に、Ｓ２０４にて、基本動作実行部１１０１は、Ｓ２０３にて検出された照度の照度レベルが所定値以上かを判定する。Ｓ２０４にて、基本動作実行部１１０１が、照度レベルが所定値以上であると判定する場合（Ｓ２０４－Ｙｅｓ）、Ｓ２０８へ進む。一方、Ｓ２０４にて、基本動作実行部１１０１が、照度レベルが所定値未満であると判定する場合（Ｓ２０４－Ｎｏ）、Ｓ２０５へ進む。

- [0116] 次に、S 2 0 5 にて、基本動作実行部 1 1 0 1 は、表示部 1 4 1 を制御することで、表示部 1 4 1 を補助光源として使用可能にする。例えば、基本動作実行部 1 1 0 1 は、表示部 1 4 1 のバックライトから発光される光の色を白色に変化させる。なお、基本動作実行部 1 1 0 1 は、表示部 1 4 1 のバックライトから発光される光の輝度を最高輝度としても良いし、S 2 0 4 にて検出された周辺の照度レベルに応じた輝度としても良い。また、基本動作実行部 1 1 0 1 は、表示部 1 4 1 のバックライトから発光される光の強度の増加させるようにしても良い。
- [0117] 次に、S 2 0 6 にて、照度センサ 1 6 5 は、表示部 1 4 1 が補助光源として使用可能になった後の、携帯情報端末 1 0 0 の周辺の照度を検出する。
- [0118] 次に、S 2 0 7 にて、基本動作実行部 1 1 0 1 は、S 2 0 6 にて検出された照度の照度レベルが所定値以上かを判定する。S 2 0 7 にて、基本動作実行部 1 1 0 1 が、照度レベルが所定値以上であると判定する場合（S 2 0 7 - Y e s ）、S 2 0 8 へ進む。一方、S 2 0 7 にて、基本動作実行部 1 1 0 1 が、照度レベルが所定値未満であると判定する場合（S 2 0 7 - N o ）、S 2 1 0 へ進む。
- [0119] 次に、S 2 1 0 にて、基本動作実行部 1 1 0 1 は、表示部 1 4 1 に P I N 入力画面を表示させる。そして、携帯情報端末 1 0 0 の操作部 1 3 0 は、操作者から数字列（P I N コード）の入力を受け付ける。
- [0120] 次に、S 2 1 1 にて、認証処理実行部 1 1 0 3 の P I N 認証部 1 1 0 3 a は、S 2 1 0 にて入力を受け付けた数字列を照合する認証処理（P I N 照合による認証処理）を実行する。そして、P I N 認証部 1 1 0 3 a は、携帯情報端末 1 0 0 の操作者が正規のユーザかを判定する。これによって、照度レベルが所定値未満であり、顔認識が困難である場合でも、P I N コードを照合する認証処理を実行し、携帯情報端末 1 0 0 の操作者が正規のユーザかを判定できるようになる。S 2 1 1 の次は、S 2 1 2 へ進む。
- [0121] 一方、S 2 0 4 にて Y e s だった場合、または、S 2 0 7 にて Y e s だった場合（周辺の照度レベルが所定値以上で、顔認証が可能な場合）、S 2 0

8にて、基本動作実行部1101は、第一画像入力部143（インカメラ）を有効化する。

[0122] 次に、S209にて、認証処理実行部1103の顔認証部1103bは、顔認証による認証処理を実行する。そして、顔認証部1103bは、携帯情報端末100の操作者が正規のユーザかを判定する。S209の次は、S212へ進む。

[0123] 次に、S212にて、携帯情報端末100の操作者が正規のユーザであり、認証が成功したか否かが判定される。S209のPIN照合による認証処理またはS211の顔認証による認証処理の結果、携帯情報端末100の操作者が正規のユーザでないと判定される場合（S212-No）、携帯情報端末100の機能ロック状態は、解除されずにS201へ戻る。一方、S209のPIN照合による認証処理またはS211の顔認証による認証処理の結果、携帯情報端末100の操作者が正規のユーザであると判定される場合（S212-Yes）、S213へ進む。

[0124] 次に、S213にて、携帯ロック制御実行部1102は、携帯情報端末100の機能ロック状態を解除する。そして、携帯情報端末100の動作状態は、スリープ状態T111または電源オフ状態T112から通常動作状態T110へと遷移する。

[0125] なお、機能設定メニュー等に「認証時に液晶モニタを補助光源として使用する」等の項目を用意し、この項目が設定オフの場合には図4Aにて説明した認証処理動作を実行し、項目が設定オンの場合には図4Bにて説明した認証処理動作を実行するように携帯情報端末100を制御しても良い。

[0126] 次に、図4Cを用いて、携帯情報端末100の周辺の照度レベルに応じて実行する認証処理を選択する認証処理動作の変形例について説明する。図4Aにて説明した認証処理動作では、携帯情報端末100の周辺の照度を照度センサ165にて検出する。一方、図4Cにおける認証処理動作では、携帯情報端末100の周辺の照度を第一画像入力部143（インカメラ）を用いて検出する点で異なる。

- [0127] なお、図4CのS301、S303～S306は、図4AのS101、S103～S106に相当する。また、図4CのS307～S309は、図4AのS108～S110に相当する。
- [0128] まず、S301にて、基本動作実行部1101は、要求された機能ロック解除要求を認識する。S301にて、基本動作実行部1101が、基本ロック解除要求を認識しない場合（S301-No）、S301へ進む。一方、S301にて、基本動作実行部1101が、機能ロック解除要求を認識した場合（S301-Yes）、S302へ進む。
- [0129] なお、端末ロック機能が有効化されている状態におけるスリープ状態T111（前述、図3）にて、操作者からスリープ状態を解除する入力を受け付けると、基本動作実行部1101は、スリープ状態解除の指示を検出する。そして、基本動作実行部1101は、検出したスリープ状態解除の指示を機能ロック状態の解除要求として認識する。
- [0130] また、端末ロック機能が有効化されている状態における電源オフ状態T112（前述、図3）にて、操作者から電源オンする入力を受け付けると、基本動作実行部1101は、電源オンの指示を検出する。そして、基本動作実行部1101は、検出した電源オンの指示を機能ロック状態の解除要求として認識する。
- [0131] 次に、S302にて、基本動作実行部1101は、第一画像入力部143（インカメラ）を有効化する。
- [0132] 次に、S303にて、第一画像入力部143は、携帯情報端末100の周辺の画像を撮像することで、携帯情報端末100の周辺の照度を検出する。詳細には、第一画像入力部143は、撮像した画像に含まれる各画素の平均輝度を算出し、算出した平均輝度を携帯情報端末100の周辺の照度レベルとして検出する。
- [0133] 次に、S304にて、基本動作実行部1101は、S303にて検出された照度の照度レベルが所定値以上かを判定する。S304にて、基本動作実行部1101が、照度レベルが所定値以上であると判定する場合（S304

－Ｙｅｓ）、Ｓ３０７へ進む。一方、Ｓ３０４にて、基本動作実行部１１０１が、照度レベルが所定値未満であると判定する場合（Ｓ３０４－Ｎｏ）、Ｓ３０５へ進む。

[0134] 次に、Ｓ３０５にて、基本動作実行部１１０１は、表示部１４１にＰＩＮ入力画面を表示させる。そして、携帯情報端末１００の操作部１３０は、操作者から数字列（ＰＩＮコード）の入力を受け付ける。

[0135] 次に、Ｓ３０６にて、認証処理実行部１１０３のＰＩＮ認証部１１０３ａは、Ｓ３０５にて入力を受け付けた数字列を照合する認証処理（ＰＩＮ照合による認証処理）を実行する。そして、ＰＩＮ認証部１１０３ａは、携帯情報端末１００の操作者が正規のユーザかを判定する。これによって、照度レベルが所定値未満であり、顔認識が困難である場合でも、ＰＩＮコードを照合する認証処理を実行し、携帯情報端末１００の操作者が正規のユーザかを判定できるようになる。Ｓ３０６の次は、Ｓ３０８へ進む。

[0136] 一方、Ｓ３０４にてＹｅｓだった場合（周辺の照度レベルが所定値以上で、顔認証が可能な場合）、Ｓ３０７にて、認証処理実行部１１０３の顔認証部１１０３ｂは、顔認証による認証処理を実行する。そして、顔認証部１１０３ｂは、携帯情報端末１００の操作者が正規のユーザかを判定する。

[0137] 次に、Ｓ３０８にて、携帯情報端末１００の操作者が正規のユーザであり、認証が成功したか否かが判定される。Ｓ３０６のＰＩＮ照合による認証処理またはＳ３０７の顔認証による認証処理の結果、携帯情報端末１００の操作者が正規のユーザでないと判定される場合（Ｓ３０８－Ｎｏ）、携帯情報端末１００の機能ロック状態は、解除されずにＳ３０１へ戻る。一方、Ｓ３０６のＰＩＮ照合による認証処理またはＳ３０７の顔認証による認証処理の結果、携帯情報端末１００の操作者が正規のユーザであると判定される場合（Ｓ３０８－Ｙｅｓ）、Ｓ３０９へ進む。

[0138] 次に、Ｓ３０９にて、携帯ロック制御実行部１１０２は、携帯情報端末１００の機能ロック状態を解除する。そして、携帯情報端末１００の動作状態は、スリープ状態Ｔ１１１または電源オフ状態Ｔ１１２から通常動作状態Ｔ

110へと遷移する。

[0139] 以上の処理により、本実施例の携帯情報端末100は、周辺の照度レベルに応じて実行する認証処理を選択することが可能になり、携帯情報端末100の使い勝手を向上させることができるようになる。

[0140] なお、本実施例の端末ロック機能は、携帯情報端末100の電源のオン／オフ、スリープモードの設定／解除および機能ロック状態を解除するための操作指示のみを受け付けるように制御する。しかしながら、これはあくまでも一例であり、所定のアプリケーションに関する操作指示のみを受け付けないように制御しても良い。例えば、携帯情報端末100が電子マネー決済機能をさらに備えており、機能ロック状態においては、電子マネー決済機能以外の各種機能に関しては通常通りに操作指示を受け付け、電子マネー決済機能に関する操作指示は受け付けないように制御しても良い。さらに、携帯情報端末100の操作者が電子マネー決済機能のアプリケーションを起動しようとした場合、電子マネー決済機能のアプリケーションの起動指示を機能ロック状態の解除要求として認識し、その後、前述した図4A～図4Cの認証処理動作を行うようにしても良い。この場合も、本実施例の携帯情報端末100は、周辺の照度レベルに応じて実行する認証処理を選択することが可能な、より使い勝手の良い制御方法を実現することができる。

[0141] <実施例1の効果>

以上説明した実施例1によれば、検出された携帯情報端末100の周辺の状態に応じて複数の認証処理から一つの認証処理を選択し、選択した認証処理を実行することで、携帯情報端末100の使い勝手を向上させることができるようになる。

[0142] また、センサ部160により検出された照度レベルが所定値以上である場合に、複数の認証処理から顔認証による認証処理を選択し、選択した認証処理を実行することで、正確に顔認証が可能な状況にて、顔認証による認証処理を実行できるようになる。

[0143] また、センサ部160により検出された照度レベルが所定値未満である場

合に、複数の認証処理から操作者から入力を受け付けた情報を照合する認証処理を選択し、選択した前証処理を実行することで、顔認識が困難である場合でも、PINコードを照合する認証処理を実行することができるようになる。

[0144] 【実施例2】

実施例2におけるシステム構成、携帯情報端末100のハードウェア構成、ソフトウェア構成等は実施例1と同様である。このため、以下では、実施例2と実施例1とで異なる認証処理動作について主に説明し、それ以外の共通する点については極力説明を省略する。

[0145] 実施例2が実施例1と異なる点は、実施例2では、操作者周辺の操作者以外の人物の存在の有無に応じて実行する認証処理を選択する点である。つまり、実施例2では、携帯情報端末100の周辺に操作者以外の人物が存在する場合に、操作者から操作部130が入力を受け付ける認証処理以外の認証処理（例えば、携帯情報端末100の周辺に存在する操作者以外の人物に携帯情報端末100が覗かれることによって不利益を生じない認証処理）を選択する。一方、携帯情報端末100に周辺に操作者以外の人物が存在しない場合には、操作者から操作部130が入力を受け付ける認証処理を選択する。

[0146] これによって、携帯情報端末100に周辺に操作者以外の人物が存在せず、携帯情報端末100に入力される数字列が操作者以外の人物に覗かれる可能性がない場合に限り、操作者から操作部130が入力を受け付ける認証処理を実行できるようになる。以下、図5を用いて、実施例2に係る携帯情報端末100の認証処理動作を説明する。

[0147] ＜認証処理動作＞

まず、S401にて、基本動作実行部1101は、要求された機能ロック解除要求を認識する。S401にて、基本動作実行部1101が、基本ロック解除要求を認識しない場合（S401-N）、S401へ進む。一方、S401にて、基本動作実行部1101が、機能ロック解除要求を認識した

場合（S 4 0 1－Y e s）、S 4 0 2へ進む。

[0148] なお、端末ロック機能が有効化されている状態におけるスリープ状態 T 1 1 1（前述、図 3）にて、操作者からスリープ状態を解除する入力を受け付けると、基本動作実行部 1 1 0 1 は、スリープ状態解除の指示を検出する。そして、基本動作実行部 1 1 0 1 は、検出したスリープ状態解除の指示を機能ロック状態の解除要求として認識する。

[0149] また、端末ロック機能が有効化されている状態における電源オフ状態 T 1 1 2（前述、図 3）にて、操作者から電源オンする入力を受け付けると、基本動作実行部 1 1 0 1 は、電源オンの指示を検出する。そして、基本動作実行部 1 1 0 1 は、検出した電源オンの指示を機能ロック状態の解除要求として認識する。

[0150] 次に、S 4 0 2にて、基本動作実行部 1 1 0 1 は、第一画像入力部 1 4 3（インカメラ）を有効化する。

[0151] 次に、S 4 0 3にて、第一画像入力部 1 4 3は、携帯情報端末 1 0 0の周辺の画像を撮像する。そして、基本動作実行部 1 1 0 1 は、第一画像入力部 1 4 3により撮像された画像を解析することで、携帯情報端末 1 0 0の周辺に操作者以外の人物が存在するかを検出する。画像を解析することで、携帯情報端末 1 0 0の周辺に操作者以外の人物が存在するかを検出するには、例えば、公知の顔抽出技術を用いれば良い。例を挙げるならば、第一画像入力部 1 4 3により撮像された周辺画像から顔画像が一つだけ抽出された場合は、操作者以外の人物は検出されない。一方、第一画像入力部 1 4 3により撮像された周辺画像から顔画像が二つ以上抽出された場合は、基本動作実行部 1 1 0 1 は、携帯情報端末 1 0 0の周辺に操作者以外の人物が存在することを検出する。

[0152] 次に、S 4 0 4にて、基本動作実行部 1 1 0 1 は、S 4 0 3にて携帯情報端末 1 0 0の周辺に操作者以外の人物が存在することを検出されたかを判定する。S 4 0 4にて、基本動作事項部 1 1 0 1 が、S 4 0 3にて操作者以外の人物が存在することが検出されたと判定する場合（S 4 0 4－Y e s）、

S 4 0 7 へ進む。一方、S 4 0 4 にて、基本動作実行部 1 1 0 1 が、S 4 0 3 にて操作者以外の人物が存在することが検出していないと判定する場合（S 4 0 4 - N o）、S 4 0 5 へ進む。

[0153] 次に、S 4 0 5 にて、基本動作実行部 1 1 0 1 は、表示部 1 4 1 に P I N 入力画面を表示させる。そして、携帯情報端末 1 0 0 の操作部 1 3 0 は、操作者から数字列（P I N コード）の入力を受け付ける。

[0154] 次に、S 4 0 6 にて、認証処理実行部 1 1 0 3 の P I N 認証部 1 1 0 3 a は、S 4 0 5 にて入力を受け付けた数字列を照合する認証処理（P I N 照合による認証処理）を実行する。そして、P I N 認証部 1 1 0 3 a は、携帯端末 1 0 0 の操作者が正規のユーザかを判定する。これによって、携帯情報端末 1 0 0 に周辺に操作者以外の人物が存在せず、携帯情報端末 1 0 0 に入力される数字列が操作者以外の人物に覗かれる可能性がない場合に限り、P I N コードを照合する認証処理を実行できるようになる。S 4 0 6 の次は、S 4 0 8 へ進む。

[0155] 一方、S 4 0 4 にて Y e s だった場合（携帯情報端末 1 0 0 の周辺に存在する操作者以外の人物に携帯情報端末 1 0 0 に入力される数字列が除かれる可能性がある場合）、S 4 0 7 にて、認証処理実行部 1 1 0 3 の顔認証部 1 1 0 3 b は、顔認証による認証処理を実行する。

[0156] 次に、S 4 0 8 にて、携帯情報端末 1 0 0 の操作者が正規のユーザであり、認証が成功したか否かが判定される。S 4 0 6 の P I N 照合による認証処理または S 4 0 7 の顔認証による認証処理の結果、携帯情報端末 1 0 0 の操作者が正規のユーザでないと判定される場合（S 4 0 8 - N o）、携帯情報端末 1 0 0 の機能ロック状態は、解除されずに S 4 0 1 へ戻る。一方、S 4 0 6 の P I N 照合による認証処理または S 4 0 7 の顔認証による認証処理の結果、携帯情報端末 1 0 0 の操作者が正規のユーザであると判定される場合（S 4 0 8 - Y e s）、S 4 0 9 へ進む。

[0157] 次に、S 4 0 9 にて、携帯ロック制御実行部 1 1 0 2 は、携帯情報端末 1 0 0 の機能ロック状態を解除する。そして、携帯情報端末 1 0 0 の動作状態

は、スリープ状態 T 1 1 1 または電源オフ状態 T 1 1 2 から通常動作状態 T 1 1 0 へと遷移する。

[0158] 以上の処理により、本実施例の携帯情報端末 1 0 0 は、周辺に操作者以外の人物が存在するか否かに応じて認証処理を選択することが可能になり、携帯情報端末 1 0 0 の使い勝手を向上させることができるようになる。

[0159] なお、S 4 0 7 で実行される認証処理は顔認識による認証処理に限らない。つまり、周辺に存在する操作者以外の人物に携帯情報端末 1 0 0 が覗かれることによって不利益を生じない認証処理であれば良い。顔認証による認証処理に替えて、例えば、S 4 0 7 にて、虹彩パターンに基づいた認証処理を実行するようにしても良い。また、S 4 0 7 にて、生体認証による認証処理（例えば、指紋認証による認証処理や、静脈認証による認証処理等）を実行するようにしても良い。

[0160] また、S 4 0 6 で実行される認証処理は、P I N 照合による認証処理に限らない。P I N 照合による認証処理に替えて、例えば、パスワードの入力を受け付けることによる認証処理や、操作キーが所定の順番で操作されたかを認証する認証処理等を実行するようにしても良い。

[0161] また、S 4 0 2 にて、本動作実行部 1 1 0 1 が、第一画像入力部 1 4 3（インカメラ）および第二画像入力部 1 4 4（アウトカメラ）を有効化するようにしても良い。この場合、S 4 0 3 にて、第一画像入力部 1 4 3（インカメラ）および第二画像入力部 1 4 4（アウトカメラ）が、携帯情報端末 1 0 0 の周辺の画像を撮像し、基本動作実行部 1 1 0 1 が撮像された画像を解析することで、携帯情報端末 1 0 0 の周辺に操作者以外の人物が存在するかを検出する。

[0162] <実施例 2 の効果>

以上説明した実施例 2 によれば、センサ部 1 6 0 により操作者以外の人物が検出された場合に、複数の認証処理から操作者から入力を受け付けた情報を照合する認証処理以外の認証処理を選択する。これによって、携帯情報端末 1 0 0 の周辺に操作者以外の人物が存在する場合に、携帯情報端末 1 0 0

が覗かれることによって不利益を生じない認証処理を実行できるようになる。

[0163] [実施例 3]

実施例 3 におけるシステム構成、携帯情報端末 100 のハードウェア構成、ソフトウェア構成等は実施例 1 と同様である。このため、以下では、実施例 3 と実施例 1 とで異なる認証処理動作について主に説明し、それ以外の共通する点については極力説明を省略する。

[0164] 実施例 3 が実施例 1 と異なる点は、実施例 3 では、周辺の音声の音量レベルに応じて実行する認証処理を選択する点である。つまり、実施例 3 では、周辺の音声の音量レベルが所定値以上の場合に、音声認識による認証処理以外の認証処理を選択する。一方、周辺の音声の音量レベルが所定値未満の場合に、音声認識による認証処理を選択する。これによって、音声認識に適した静かな環境で音声認識による認証処理を実行できるようになる。以下、図 6 A および図 6 B を用いて、実施例 3 に係る携帯情報端末 100 の認証処理動作を説明する。

[0165] <認証処理動作>

まず、図 6 A を用いて、携帯情報端末 100 の周辺の音量レベルに応じて認証処理を選択する認証処理動作について説明する。

[0166] まず、S 501 にて、基本動作実行部 1101 は、要求された機能ロック解除要求を認識する。S 501 にて、基本動作実行部 1101 が、基本ロック解除要求を認識しない場合 (S 501 - N o)、S 501 へ進む。一方、S 501 にて、基本動作実行部 1101 が、機能ロック解除要求を認識した場合 (S 501 - Y e s)、S 502 へ進む。

[0167] なお、端末ロック機能が有効化されている状態におけるスリープ状態 T 111 (前述、図 3) にて、操作者からスリープ状態を解除する入力を受け付けると、基本動作実行部 1101 は、スリープ状態解除の指示を検出する。そして、基本動作実行部 1101 は、検出したスリープ状態解除の指示を機能ロック状態の解除要求として認識する。

- [0168] また、端末ロック機能が有効化されている状態における電源オフ状態 T 1 1 2（前述、図 3）にて、操作者から電源オンする入力を受け付けると、基本動作実行部 1 1 0 1 は、電源オンの指示を検出する。そして、基本動作実行部 1 1 0 1 は、検出した電源オンの指示を機能ロック状態の解除要求として認識する。
- [0169] 次に、S 5 0 2 にて、基本動作実行部 1 1 0 1 は、音声入力部 1 5 3（マイク）を有効化する。
- [0170] 次に、S 5 0 3 にて、音声入力部 1 5 3 は、携帯情報端末 1 0 0 の周辺の音声を集音する。そして、音声入力部は、集音された音声の音声レベルを検出する。
- [0171] 次に、S 5 0 4 にて、基本動作実行部 1 1 0 1 は、S 5 0 3 にて集音された音声の音声レベルが所定値未満かを判定する。S 5 0 4 にて、基本動作実行部 1 1 0 1 が、音声レベルが所定値未満であると判定する場合（S 5 0 4－Y e s）、S 5 0 7 へ進む。一方、S 5 0 4 にて、基本動作実行部 1 1 0 1 が、音声レベルが所定値以上であると判定する場合（S 5 0 4－N o）、S 5 0 5 へ進む。
- [0172] 次に、S 5 0 5 にて、基本動作実行部 1 1 0 1 は、表示部 1 4 1 に P I N 入力画面を表示させる。そして、携帯情報端末 1 0 0 の操作部 1 3 0 は、操作者から数字列（P I N コード）の入力を受け付ける。
- [0173] 次に、S 5 0 6 にて、認証処理実行部 1 1 0 3 の P I N 認証部 1 1 0 3 a は、S 5 0 5 にて入力を受け付けた数字列を照合する認証処理（P I N 照合による認証処理）を実行する。そして、P I N 認証部 1 1 0 3 a は、携帯端末 1 0 0 の操作者が正規のユーザかを判定する。これによって、携帯情報端末 1 0 0 の周辺の音量が大きく、音声認識が困難である場合であっても、音声認識による認証処理を実行することなく、P I N コードを照合する認証処理を実行できるようになる。
- [0174] 一方、S 5 0 4 にて Y e s だった場合（携帯情報端末 1 0 0 の周辺の音声の音量レベルが所定値未満であり、音声認識による認証処理が可能な場合）

、S 5 0 7 にて、認証処理実行部 1 1 0 3 の音声認証部 1 1 0 3 c は、音声認識による認証処理を実行する。なお、音声認識による認証処理は公知の技術を用いれば良い。例を挙げるならば、音声入力部 1 5 3（マイク）から入力された携帯情報端末 1 0 0 の操作者の音声をデジタルデータに変換し、変換後のデジタルデータと、認証情報記憶領域 1 0 1 1 に予め記憶される正規ユーザの声のデジタルデータとを比較し、パターンの一致度を確認することで音声認識による認証処理を実行する。

[0175] 次に、S 5 0 8 にて、携帯情報端末 1 0 0 の操作者が正規のユーザであり、認証が成功したか否かが判定される。S 5 0 6 の P I N 照合による認証処理または S 5 0 7 の音声認識による認証処理の結果、携帯情報端末 1 0 0 の操作者が正規のユーザでないと判定される場合（S 5 0 8－N o）、携帯情報端末 1 0 0 の機能ロック状態は、解除されずに S 5 0 1 へ戻る。一方、S 5 0 6 の P I N 照合による認証処理または S 5 0 7 の音声認識による認証処理の結果、携帯情報端末 1 0 0 の操作者が正規のユーザであると判定される場合（S 5 0 8－Y e s）、S 5 0 9 へ進む。

[0176] 次に、S 5 0 9 にて、携帯ロック制御実行部 1 1 0 2 は、携帯情報端末 1 0 0 の機能ロック状態を解除する。そして、携帯情報端末 1 0 0 の動作状態は、スリープ状態 T 1 1 1 または電源オフ状態 T 1 1 2 から通常動作状態 T 1 1 0 へと遷移する。

[0177] 以上の処理により、本実施例の携帯情報端末 1 0 0 は、周辺の音声の音量レベルに応じて認証処理を選択することが可能になり、携帯情報端末 1 0 0 の使い勝手を向上させることができるようになる。

[0178] なお、S 5 0 6 で実行される認証処理は音声認識による認証処理に限られるものではない。つまり、マイクにより集音された音声の音声データに基づいて認証処理を行うものであれば良い。例えば、S 5 0 6 にて、声紋認証や所定の楽曲をキーサウンドとしてその一致度を比較する認証処理を実行するようにしても良い。

[0179] また、S 5 0 6 で実行される認証処理も音声認証による認証処理でなけれ

ば良い。例えば、PIN照合による認証処理に替えて、S506にて、パスワードの入力を受け付けることによる認証処理や、操作キーが所定の順番で操作されたかを認証する認証処理を実行するようにしても良い。

[0180] 次に、図6Bを用いて、携帯情報端末100の周辺の音量レベルに応じて実行する認証処理を選択する認証処理動作の変形例について説明する。図6Aにて説明した認証処理動作に対して、図6Bにおける認証処理動作では、携帯情報端末100の動作設定状態がマナーモード（サイレントモード）が設定されているマナーモード設定状態でない場合にのみ、音声入力部153（マイク）を有効化し、携帯情報端末100の周辺の音声を集音する点で異なる。

[0181] なお、マナーモードとは、通話やメールの着信があった場合に、着信音を出力せず、バイブレータ等を動作させることで着信があったことを操作者に報知するモードを意味する。マナーモードは、主に、音声を出力するのに相応しくない場所で設定される。

[0182] また、図6BのS601、S603～S610は、図6AのS501～S509に相当する。すなわち、図6Aの認証処理動作に対して、図6Bの認証処理動作は、S602の処理を有する点で異なる。

[0183] まず、S601にて、基本動作実行部1101は、要求された機能ロック解除要求を認識する。S601にて、基本動作実行部1101が、基本ロック解除要求を認識しない場合（S601-No）、S601へ進む。一方、S601にて、基本動作実行部1101が、機能ロック解除要求を認識した場合（S601-Yes）、S602へ進む。

[0184] なお、端末ロック機能が有効化されている状態におけるスリープ状態T111（前述、図3）にて、操作者からスリープ状態を解除する入力を受け付けると、基本動作実行部1101は、スリープ状態解除の指示を検出する。そして、基本動作実行部1101は、検出したスリープ状態解除の指示を機能ロック状態の解除要求として認識する。

[0185] また、端末ロック機能が有効化されている状態における電源オフ状態T1

12（前述、図3）にて、操作者から電源オンする入力を受け付けると、基本動作実行部1101は、電源オンの指示を検出する。そして、基本動作実行部1101は、検出した電源オンの指示を機能ロック状態の解除要求として認識する。

[0186] 次に、S602にて、基本動作実行部1101は、機能設定メニューの設定値を参照することで、携帯情報端末100の動作設定状態が、マナーモード設定状態であるかを判定する。S602にて、基本動作実行部1101が、携帯情報端末100の動作設定状態が、マナーモード設定状態であると判定する場合（S602-On）、S606へ進む。一方、S602にて、基本動作実行部1101が、携帯情報端末100の動作設定状態が、マナーモード設定状態でないと判定する場合（S602-Off）、S603へ進む。

[0187] 次に、S603にて、基本動作実行部1101は、音声入力部153（マイク）を有効化する。

[0188] 次に、S604にて、音声入力部153は、携帯情報端末100の周辺の音声を集音する。そして、音声入力部は、集音された音声の音声レベルを検出する。

[0189] 次に、S605にて、基本動作実行部1101は、S604にて集音された音声の音声レベルが所定値未満かを判定する。S605にて、基本動作実行部1101が、音声レベルが所定値未満であると判定する場合（S605-Yes）、S608へ進む。一方、S605にて、基本動作実行部1101が、音声レベルが所定値以上であると判定する場合（S605-No）、S606へ進む。

[0190] 次に、S606にて、基本動作実行部1101は、表示部141にPIN入力画面を表示させる。そして、携帯情報端末100の操作部130は、操作者から数字列（PINコード）の入力を受け付ける。

[0191] 次に、S607にて、認証処理実行部1103のPIN認証部1103aは、S606にて入力を受け付けた数字列を照合する認証処理（PIN照合

による認証処理)を実行する。そして、PIN認証部1103aは、携帯端末100の操作者が正規のユーザかを判定する。

[0192] 一方、S605にてYesだった場合(携帯情報端末100の周辺の音声の音量レベルが所定値未満であり、音声認識による認証処理が可能な場合)、S608にて、認証処理実行部1103の音声認証部1103cは、音声認識による認証処理を実行する。

[0193] 次に、S609にて、携帯情報端末100の操作者が正規のユーザであり、認証が成功したか否かが判定される。S607のPIN照合による認証処理またはS608の音声認識による認証処理の結果、携帯情報端末100の操作者が正規のユーザでないと判定される場合(S609-No)、携帯情報端末100の機能ロック状態は、解除されずにS601へ戻る。一方、S607のPIN照合による認証処理またはS608の音声認識による認証処理の結果、携帯情報端末100の操作者が正規のユーザであると判定される場合(S609-Yes)、S610へ進む。

[0194] 次に、S610にて、携帯ロック制御実行部1102は、携帯情報端末100の機能ロック状態を解除する。そして、携帯情報端末100の動作状態は、スリープ状態T111または電源オフ状態T112から通常動作状態T110へと遷移する。

[0195] 上述したように、S602にて携帯情報端末100の動作設定状態が、マナーモード設定状態であると判定する場合、S603～S605の処理がされることなく、S606～S608の処理がされる。すなわち、携帯情報端末100の動作設定状態が、マナーモードに設定されている場合に、携帯情報端末100が音声を発するに相応しくない場所に存在するものと判定され、携帯情報端末100の周辺の音量レベルに関わらず、PIN照合による認証処理が選択される。

[0196] すなわち、本実施例の携帯情報端末100は、周辺の音量レベルおよび携帯情報端末100のマナーモード設定状態(動作設定状態)に応じて実行する認証処理を選択する。これによって、音声を発するに相応しくない場所に

て、音声認識による認証処理以外の認証処理を選択することが可能になり、携帯情報端末 100 の使い勝手を向上させることができるようになる。

[0197] <実施例 3 の効果>

以上説明した実施例 3 によれば、センサ部 160 により検出された音量レベルが所定値未満の場合に、複数の認証処理から音声による認証処理を選択し、選択した認証処理を実行することで、音声認識に適した静かな環境で音声認識による認証処理を実行できるようになる。

[0198] また、センサ部 160 により検出された音量レベルが所定値以上である場合に、複数の認証処理から操作者から入力を受け付けた情報を照合する認証処理を選択し、選択した認証処理を実行することで、音声認識に適さない騒がしい環境では、音声認識による認証処理を実行することなく PIN 照合による認証処理を実行できるようになる。

[0199] また、携帯情報端末 100 の動作設定状態がマナーモードである場合に、複数の認証処理から音声による認証処理以外の認証処理を選択し、選択した認証処理を実行することで、音声を発するに相応しくない環境では、音声認識による認証処理を実行することなく、音声認識による認証処理以外の認証処理を選択することが可能になる。

[0200] [実施例 4]

実施例 4 におけるシステム構成、携帯情報端末 100 のハードウェア構成、ソフトウェア構成等は実施例 1 と同様である。このため、以下では、実施例 4 と実施例 1 とで異なる認証処理動作について主に説明し、それ以外の共通する点については極力説明を省略する。

[0201] 実施例 4 が実施例 1 と異なる点は、実施例 4 では、携帯情報端末 100 を保持する操作者が自身で移動中（例えば、歩行中）であるか否かに応じて実行する認証処理を選択する点である。ここで、携帯情報端末 100 を保持する操作者が移動中の場合、操作者が携帯情報端末 100 の操作部 130 等を注視しながら操作を行うことは好ましくない。このため、実施例 4 では、操作者が移動中である場合に、音声認識による認証処理を選択する。一方、操

作者が移動中ではない場合に、PINコードを照合する認証処理を選択する。

[0202] これによって、移動中の操作者は、進行方向を確認しつつ認証情報を入力できるようになる。また、移動中の操作者が、携帯情報端末100の操作部130等を注視しながら歩行することを抑制させることができるようになる。以下、図7を用いて、実施例4に係る携帯情報端末100の認証処理動作を説明する。

[0203] <認証処理動作>

まず、S701にて、基本動作実行部1101は、要求された機能ロック解除要求を認識する。S701にて、基本動作実行部1101が、基本ロック解除要求を認識しない場合(S701-No)、S701へ進む。一方、S701にて、基本動作実行部1101が、機能ロック解除要求を認識した場合(S701-Yes)、S702へ進む。

[0204] なお、端末ロック機能が有効化されている状態におけるスリープ状態T111(前述、図3)にて、操作者からスリープ状態を解除する入力を受け付けると、基本動作実行部1101は、スリープ状態解除の指示を検出する。そして、基本動作実行部1101は、検出したスリープ状態解除の指示を機能ロック状態の解除要求として認識する。

[0205] また、端末ロック機能が有効化されている状態における電源オフ状態T112(前述、図3)にて、操作者から電源オンする入力を受け付けると、基本動作実行部1101は、電源オンの指示を検出する。そして、基本動作実行部1101は、検出した電源オンの指示を機能ロック状態の解除要求として認識する。

[0206] 次に、S702にて、基本動作実行部1101は、ジャイロセンサ162および加速度センサ164を有効化する。

[0207] 次に、S703にて、ジャイロセンサ162は、携帯情報端末100の姿勢を検出する。また、加速度センサ164は、携帯電話端末100の加速度を検出する。

- [0208] 次に、S704にて、基本動作実行部1101は、S703にて検出される携帯情報端末100の姿勢（傾き）と、加速度とに基づき、携帯情報端末100を保持する操作者が移動中（例えば、歩行中）であるかを判定する。S704にて、基本動作実行部1101が、操作者が移動中であると判定する場合（S704－Yes）、S707へ進む。一方、S704にて、基本動作実行部1101が、操作者が移動中でないと判定する場合（S704－No）、S705へ進む。なお、操作者が移動中であるかを判定するのには、公知の技術を用いる。例を挙げるならば、所定時間ごとにジャイロセンサ162および加速度センサ164から検出される携帯情報端末100の傾きや加速度と、予め記憶されている歩行時の傾きおよび加速度のパターンと比較することで、操作者が移動中であるかを判定する。
- [0209] 次に、S705にて、基本動作実行部1101は、表示部141にPIN入力画面を表示させる。そして、携帯情報端末100の操作部130は、操作者から数字列（PINコード）の入力を受け付ける。
- [0210] 次に、S706にて、認証処理実行部1103のPIN認証部1103aは、S705にて入力を受け付けた数字列を照合する認証処理（PIN照合による認証処理）を実行する。そして、PIN認証部1103aは、携帯端末100の操作者が正規のユーザかを判定する。
- [0211] 一方、S704にてYesだった場合（操作者が移動中であり、音声認識による認証処理が適している場合）、S707にて、認証処理実行部1103の音声認証部1103cは、音声認識による認証処理を実行する。
- [0212] 次に、S708にて、携帯情報端末100の操作者が正規のユーザであり、認証が成功したか否かが判定される。S706のPIN照合による認証処理またはS707の音声認識による認証処理の結果、携帯情報端末100の操作者が正規のユーザでないと判定される場合（S708－No）、携帯情報端末100の機能ロック状態は、解除されずにS701へ戻る。一方、S706のPIN照合による認証処理またはS707の音声認識による認証処理の結果、携帯情報端末100の操作者が正規のユーザであると判定される

場合（S 7 0 8－Y e s）、S 7 0 9へ進む。

[0213] 次に、S 7 0 9にて、携帯ロック制御実行部 1 1 0 2は、携帯情報端末 1 0 0の機能ロック状態を解除する。そして、携帯情報端末 1 0 0の動作状態は、スリープ状態 T 1 1 1または電源オフ状態 T 1 1 2から通常動作状態 T 1 1 0へと遷移する。

[0214] 以上の処理により、本実施例の携帯情報端末 1 0 0は、操作者が移動中か否かに応じて実行する認証処理を選択することが可能になり、携帯情報端末 1 0 0の使い勝手を向上させることができるようになる。

[0215] なお、S 7 0 6で実行される認証処理は音声認識による認証処理に限られるものではない。つまり、マイクにより集音された音声の音声データに基づいて認証処理を行うものであれば良い。例えば、S 7 0 6にて、声紋認証や所定の楽曲をキーサウンドとしてその一致度を比較する認証処理を実行するようにしても良い。

[0216] また、S 7 0 6で実行される認証処理も音声認証による認証処理でなければ良い。P I N照合による認証処理に替えて、例えば、パスワードの入力を受け付けることによる認証処理や、操作キーが所定の順番で操作されたかを認証する認証処理等を実行するようにしても良い。

[0217] これによって、操作者が移動中か否かに応じて、実行する認証処理を選択することが可能になり、携帯情報端末 1 0 0の使い勝手を向上させることができるようになる。

[0218] <実施例 4 の効果>

以上説明した実施例 4 によれば、操作者が移動中である場合に、複数の認証処理から音声による認証処理を選択し、選択した認証処理を実行することで、移動中の操作者が、携帯情報端末 1 0 0の操作部 1 3 0等を注視しながら操作することを抑制させることができるようになる。

[0219] [実施例 5]

実施例 5 におけるシステム構成、携帯情報端末 1 0 0のハードウェア構成、ソフトウェア構成等は実施例 1 と同様である。このため、以下では、実施

例５と実施例１とで異なる認証処理動作について主に説明し、それ以外の共通する点については極力説明を省略する。

[0220] 実施例５が実施例１と異なる点は、実施例５では、携帯情報端末１００の周辺の照度レベルが不足し、かつ、周辺の音声の音量レベルが所定値以上の場合に、ＰＩＮコードを照合する認証処理を選択する点である。これによって、周辺の照度レベルおよび周辺の音量レベルに応じて実行する認証処理を選択できるようになる。

[0221] <認証処理動作>

まず、Ｓ８０１にて、基本動作実行部１１０１は、要求された機能ロック解除要求を認識する。Ｓ８０１にて、基本動作実行部１１０１が、基本ロック解除要求を認識しない場合（Ｓ８０１－Ｎｏ）、Ｓ８０１へ進む。一方、Ｓ８０１にて、基本動作実行部１１０１が、機能ロック解除要求を認識した場合（Ｓ８０１－Ｙｅｓ）、Ｓ８０２へ進む。

[0222] なお、端末ロック機能が有効化されている状態におけるスリープ状態Ｔ１１１（前述、図３）にて、操作者からスリープ状態を解除する入力を受け付けると、基本動作実行部１１０１は、スリープ状態解除の指示を検出する。そして、基本動作実行部１１０１は、検出したスリープ状態解除の指示を機能ロック状態の解除要求として認識する。

[0223] また、端末ロック機能が有効化されている状態における電源オフ状態Ｔ１１２（前述、図３）にて、操作者から電源オンする入力を受け付けると、基本動作実行部１１０１は、電源オンの指示を検出する。そして、基本動作実行部１１０１は、検出した電源オンの指示を機能ロック状態の解除要求として認識する。

[0224] 次に、Ｓ８０２にて、基本動作実行部１１０１は、照度センサ１６５を有効化する。

[0225] 次に、Ｓ８０３にて、照度センサ１６５は、携帯情報端末１００の周辺の照度を検出する。

[0226] 次に、Ｓ８０４にて、基本動作実行部１１０１は、Ｓ８０３にて検出され

た照度の照度レベルが所定値以上かを判定する。S 8 0 4 にて、基本動作実行部 1 1 0 1 が、照度レベルが所定値以上であると判定する場合（S 8 0 4 - Y e s）、S 8 1 0 へ進む。一方、S 8 0 4 にて、基本動作実行部 1 1 0 1 が、照度レベルが所定値未満であると判定する場合（S 8 0 4 - N o）、S 8 0 5 へ進む。

[0227] 次に、S 8 0 5 にて、基本動作実行部 1 1 0 1 は、音声入力部 1 5 3（マイク）を有効化する。

[0228] 次に、S 8 0 6 にて、音声入力部 1 5 3 は、携帯情報端末 1 0 0 の周辺の音声を集音する。そして、音声入力部は、集音された音声の音声レベルを検出する。

[0229] 次に、S 8 0 7 にて、基本動作実行部 1 1 0 1 は、S 8 0 6 にて集音された音声の音声レベルが所定値未満かを判定する。S 8 0 7 にて、基本動作実行部 1 1 0 1 が、音声レベルが所定値未満であると判定する場合（S 8 0 7 - Y e s）、S 8 1 2 へ進む。一方、S 8 0 7 にて、基本動作実行部 1 1 0 1 が、音声レベルが所定値以上であると判定する場合（S 8 0 7 - N o）、S 8 0 8 へ進む。

[0230] 次に、S 8 0 8 にて、基本動作実行部 1 1 0 1 は、表示部 1 4 1 に P I N 入力画面を表示させる。そして、携帯情報端末 1 0 0 の操作部 1 3 0 は、操作者から数字列（P I N コード）の入力を受け付ける。

[0231] 次に、S 8 0 9 にて、認証処理実行部 1 1 0 3 の P I N 認証部 1 1 0 3 a は、S 8 0 5 にて入力を受け付けた数字列を照合する認証処理（P I N 照合による認証処理）を実行する。そして、P I N 認証部 1 1 0 3 a は、携帯端末 1 0 0 の操作者が正規のユーザかを判定する。S 8 0 9 の次には、S 8 1 3 へ進む。

[0232] S 8 0 4 にて Y e s だった場合（周辺の照度レベルが所定値以上で、顔認証が可能な場合）、S 8 1 0 にて、基本動作実行部 1 1 0 1 は、第一画像入力部 1 4 3（インカメラ）を有効化する。

[0233] 次に、S 8 1 1 にて、認証処理実行部 1 1 0 3 の顔認証部 1 1 0 3 b は、

顔認証による認証処理を実行する。そして、顔認証部 1103b は、携帯情報端末 100 の操作者が正規のユーザかを判定する。S811 の次は、S813 へ進む。

[0234] S807 にて Yes だった場合（携帯情報端末 100 の周辺の音声の音量レベルが所定値未満であり、音声認識による認証処理が可能な場合）、S812 にて、認証処理実行部 1103 の音声認証部 1103c は、音声認識による認証処理を実行する。

[0235] 次に、S813 にて、携帯情報端末 100 の操作者が正規のユーザであり、認証が成功したか否かが判定される。S808 の PIN 照合による認証処理または S811 の顔認証による認証処理または S812 の音声認識による認証処理の結果、携帯情報端末 100 の操作者が正規のユーザでないと判定される場合（S813-No）、携帯情報端末 100 の機能ロック状態は、解除されずに S801 へ戻る。一方、S808 の PIN 照合による認証処理または S811 の顔認証による認証処理または S812 の音声認識による認証処理の結果、携帯情報端末 100 の操作者が正規のユーザであると判定される場合（S813-Yes）、S814 へ進む。

[0236] 次に、S814 にて、携帯ロック制御実行部 1102 は、携帯情報端末 100 の機能ロック状態を解除する。そして、携帯情報端末 100 の動作状態は、スリープ状態 T111 または電源オフ状態 T112 から通常動作状態 T110 へと遷移する。

[0237] 以上の処理により、本実施例の携帯情報端末 100 は、周辺の照度レベルおよび周辺の音量レベルに応じた認証処理を選択することが可能になり、携帯情報端末 100 の使い勝手を向上させることができるようになる。

[0238] なお、実施例 5 は、実施例 1 の認証処理動作（前述、図 4A）と、実施例 3 の認証処理動作（前述、図 6A）とを組み合わせたものであるが、これ以外に、前述した実施例 1～実施例 5 の各認証処理動作処理を適宜組み合わせるようにしても良い。

[0239] また、実施例 5 は認証処理動作では、各認証処理の選択の優先順位として

、まず、顔認識による認証処理の選択を検討し、次に音声認識による認証処理の選択を検討し、最後にPIN照合による認証処理を検討している。しかしながら、選択の優先順位はあくまでも一例であり、異なる優先順位にて各認証処理の選択を検討するようにしても良い。

[0240] また、携帯情報端末100が備えるセンサ等の検出結果に応じて優先順位の低い認証処理が選択された場合に、優先順位の高い認証処理が選択されなかった理由を表示部141等に表示するようにしても良い。或いは、携帯情報端末100が備えるセンサ等の検出結果に応じて所定の認証処理が選択された場合に、選択された認証処理が選択された理由を表示部141等に表示するようにしても良い。このようにすれば、携帯情報端末100の使い勝手をさらに向上させることができる。

[0241] また、実施例1～実施例5に例示しなかった認証処理が適宜選択されるように携帯情報端末100を制御するようにしても良い。例えば、携帯情報端末100が備えるセンサ等の検出結果に応じて、携帯情報端末100の周辺の状態や操作者の状態に応じた好適な認証処理が適宜選択されるように携帯情報端末100を制御するようにしても良い。

[0242] <実施例5の効果>

以上説明した実施例5によれば、携帯情報端末100の周辺の照度レベルが不足し、かつ、周辺の音声の音量レベルが所定値以上の場合に、PINコードを照合する認証処理を選択し、選択した認証処理を実行することで、周辺の照度レベルおよび周辺の音量レベルに応じた認証処理を実行できるようになる。

[0243] [実施例6]

実施例6におけるシステム構成、携帯情報端末100のハードウェア構成、ソフトウェア構成等は特に説明がない限り、実施例1と同様である。このため、以下では、実施例6と実施例1とで異なる認証処理動作について主に説明し、それ以外の共通する点については極力説明を省略する。

[0244] 実施例6が実施例1と異なる点は、実施例6では、携帯情報端末100が

ら送信された認証情報を受信し、受信した認証情報に基づいて、認証処理を行う認証サーバ500を有する点である。これによって、認証サーバ500に蓄積された膨大な情報に基づく認証処理が可能になり、認証処理の精度を向上させることが可能になる。

[0245] <システム構成>

図9は、実施例6に係る通信システムの構成例の概要を示す図である。図9に示されるように、通信システムは、携帯情報端末100と、アクセスポイント200aと、移動体電話通信網の基地局300bと、移動体電話通信サーバ300と、アプリケーションサーバ400と、認証サーバ500とを有する。

[0246] 認証サーバ500は、無線通信または有線通信を介してインターネット200と接続される。そして、認証サーバ500は、携帯情報端末100との間で、インターネット200を介してデータを送受信する。

[0247] 携帯情報端末100は、インターネット200を介して認証サーバ500へ認証処理動作に必要な認証情報を送信する。認証サーバ500は、携帯情報端末100から送信された認証情報を受信し、受信した認証情報に基づいて、認証処理を行う。

[0248] 具体的には、認証サーバ500は、携帯情報端末100から送信されたPIN照合による認証処理のための認証情報、顔認識による認証処理のための認証情報、音声認識による認証処理のための認証情報を受信し、受信した認証情報を照合する。

[0249] <認証サーバの構成>

図10は、実施例6に係る認証サーバの構成例の概要を示す図である。図10に示されるように、認証サーバ500は、主制御部501と、RAM504と、ストレージ部510と、LAN通信部521とを有する。

[0250] 主制御部501と、RAM504と、ストレージ部510と、LAN通信部521とは、システムバス502を介して相互に接続される。

[0251] 主制御部501は、所定の動作プログラムに従って認証サーバ500全体

を制御するマイクロプロセッサユニットである。

[0252] システムバス502は、主制御部501と認証サーバ500内の各動作ブロック（RAM504、ストレージ部510、LAN通信部521）との間でデータ送受信を行うためのデータ通信路である。

[0253] LAN通信部521は符号回路や復号回路等を備えるものとする。そして、LAN通信部521は、インターネット200と接続され、携帯情報端末100からの認証情報の受信処理や携帯情報端末100への認証結果の送信処理を実行する。

[0254] RAM504は、基本動作プログラムやその他の動作プログラム実行時のワークエリアとなる。なお、RAM504を主制御部101と一体で構成するようにしても良い。

[0255] ストレージ部510には、基本動作プログラム5001と認証処理プログラム5002が記憶されている。また、ストレージ部510の認証情報記憶領域5011には、携帯情報端末100の操作者が正規のユーザであるか否かを確認するための認証情報等が記憶されている。主制御部501は、ストレージ部510に記憶されている基本動作プログラム5001をおよび認証処理プログラム5002をRAM504に展開する。そして、主制御部101は、RAM504に展開した基本動作プログラム5001を実行する。これによって、基本動作実行部5101が構成される。

[0256] また、主制御部501は、ストレージ部510に記憶されている認証処理プログラム5002をRAM504に展開する。そして、主制御部101は、RAM504に展開した認証処理プログラム5002を実行する。これによって、認証処理実行部5102が構成される。なお、以下では、主制御部501が、ストレージ部510に記憶されている認証処理プログラム5002をRAM504に展開して実行することにより各動作ブロックの制御を行う処理を、認証処理実行部5102が、各動作ブロックの制御を行うと記述する場合がある。

[0257] 認証処理実行部5102は、携帯情報端末100から受信した認証情報に

基づいて携帯情報端末１００の操作者が正規のユーザであるか否かを確認するための認証処理動作（後述、図１２）を実行する。

[0258] 携帯情報端末１００から送信されたＰＩＮ照合による認証処理のための認証情報、顔認識による認証処理のための認証情報、音声認識による認証処理のための認証情報と、認証情報記憶領域５０１１に記憶されている認証情報とを照合する。すなわち、認証サーバ５００は、携帯情報端末１００から送信された認証情報の種類に応じて認証情報記憶領域５０１１を参照することにより、認証処理を行う。

[0259] なお、ストレージ部５１０に記憶されている各動作プログラムは更新および機能を拡張することが可能である。

[0260] また、各動作プログラムは、予めストレージ部５１０に記憶されている状態であっても良い。また、インターネット２００上のその他のアプリケーションサーバ４００等からＬＡＮ通信部５２１を介して取得されるようにしても良い。また、メモリカードや光ディスク等に記憶されている各動作プログラムを、拡張インタフェース部（不図示）を介して取得するようにしても良い。

[0261] ＜携帯情報端末のソフトウェア構成＞

図１１は、実施例６に係る携帯情報端末１００のソフトウェア構成図である。図１１に示されるように、ＲＯＭ１０３には、基本動作プログラム１００１と、その他の動作プログラムが記憶されている。また、ストレージ部１１０には、端末ロック制御プログラム１００２と、認証データ送受信プログラム１００４と、その他の動作プログラムが記憶されている。また、ストレージ部１１０には、その他の情報が記憶される各種情報記憶領域（図中、各種情報）１０１９を有する。

[0262] 主制御部１０１は、ＲＯＭ１０３に記憶されている基本動作プログラム１００１を、ＲＡＭ１０４に展開する。そして、主制御部１０１は、ＲＡＭ１０４に展開した基本動作プログラム１００１を実行する。これによって、基本動作実行部１１０１が構成される。

[0263] また、主制御部１０１は、ストレージ部１１０に記憶されている端末ロック制御プログラム１００２をＲＡＭ１０４に展開する。そして、主制御部１０１は、ＲＡＭ１０４に展開した端末ロック制御プログラム１００２を実行する。これによって、端末ロック制御実行部１１０２が構成される。

[0264] また、主制御部１０１は、ストレージ部１１０に記憶されている認証データ送受信プログラム１００４をＲＡＭ１０４に展開する。そして、主制御部１０１は、ＲＡＭ１０４に展開した認証データ送受信プログラム１００４を実行する。これによって認証データ送受信実行部１１０４が構成される。なお、以下では、主制御部１０１が、ストレージ部１１０に記憶されている認証データ送受信プログラム１００４をＲＡＭ１０４に展開して実行することにより各動作ブロックの制御を行う処理を、認証データ送受信実行部１１０４が、各動作ブロックの制御を行うと記述する場合がある。

[0265] 認証データ送受信実行部１１０４は、携帯情報端末１００の操作者が正規のユーザであるか否かを認証サーバ５００に確認させるために必要な認証情報を認証サーバ５００に送信する処理を実行する。また、認証データ送受信実行部１１０４は、認証サーバ５００から送信される認証結果を受信する処理を実行する。

[0266] なお、各動作プログラムは、製品出荷の時点で、予めＲＯＭ１０３および／またはストレージ部１１０に記憶されている状態であっても良い。また、製品出荷後に、インターネット２００上のその他のアプリケーションサーバ４００等からＬＡＮ通信部１２１または電話網通信部１２２を介して取得されるようにしても良い。また、メモリカードや光ディスク等に記憶されている各動作プログラムを、拡張インタフェース部１２４等を介して取得するようにしても良い。

[0267] <認証処理動作>

実施例６の通信システムは複数の認証処理を備え、センサ等により確認した携帯情報端末１００の周辺の状況や操作者の状態や動作設定等に応じて、複数の認証処理からいずれか一つの認証処理を選択し、選択した認証処理と

対応する認証情報を取得する。そして、携帯情報端末１００は、取得した認証情報を認証サーバ５００に送信し、認証サーバ５００に認証処理を行わせる。

[0268] また、実施例６に係る認証処理動作は、前述した図１１に示される、携帯情報端末１００の認証データ送受信実行部１１０４と、端末ロック制御実行部１１０２と、基本動作実行部１１０１と、前述した図１０に示される認証サーバ５００の認証処理実行部５１０２と、基本動作実行部５１５１とによって制御される。

[0269] なお、携帯情報端末１００が、認証データ送受信実行部１１０４および端末ロック制御実行部１１０２と同等の動作をハードウェアで実現する各ハードウェアブロックをさらに備えるようにしても良い。その場合、各ハードウェアブロックが、認証データ送受信実行部１１０４および端末ロック制御実行部１１０２に代替して携帯情報端末１００の動作を実行する。

[0270] 以下、図１２を用いて、実施例６に係る認証処理動作について説明する。図１２に示される認証処理動作では、携帯情報端末１００の周辺の照度レベルに応じて実行する認証処理を選択する。

[0271] まず、Ｓ９０１にて、基本動作実行部１１０１は、要求された機能ロック解除要求を認識する。Ｓ９０１にて、基本動作実行部１１０１が、基本ロック解除要求を認識しない場合（Ｓ９０１－Ｎｏ）、Ｓ９０１へ進む。一方、Ｓ９０１にて、基本動作実行部１１０１が、機能ロック解除要求を認識した場合（Ｓ９０１－Ｙｅｓ）、Ｓ９０２へ進む。

[0272] なお、端末ロック機能が有効化されている状態におけるスリープ状態Ｔ１１１（前述、図３）にて、操作者からスリープ状態を解除する入力を受け付けると、基本動作実行部１１０１は、スリープ状態解除の指示を検出する。そして、基本動作実行部１１０１は、検出したスリープ状態解除の指示を機能ロック状態の解除要求として認識する。

[0273] また、端末ロック機能が有効化されている状態における電源オフ状態Ｔ１１２（前述、図３）にて、操作者から電源オンする入力を受け付けると、基

本動作実行部 1101 は、電源オンの指示を検出する。そして、基本動作実行部 1101 は、検出した電源オンの指示を機能ロック状態の解除要求として認識する。

[0274] 次に、S902 にて、基本動作実行部 1101 は、照度センサ 165 を有効化する。

[0275] 次に、S903 にて、照度センサ 165 は、携帯情報端末 100 の周辺の照度を検出する。

[0276] 次に、S904 にて、基本動作実行部 1101 は、S903 にて検出された照度の照度レベルが所定値以上かを判定する。S904 にて、基本動作実行部 1101 が、照度レベルが所定値以上であると判定する場合（S904－Yes）、S907 へ進む。一方、S904 にて、基本動作実行部 1101 が、照度レベルが所定値未満であると判定する場合（S904－No）、S905 へ進む。

[0277] 次に、S905 にて、基本動作実行部 1101 は、表示部 141 に PIN 入力画面を表示させる。

[0278] 次に、S906 にて、携帯情報端末 100 の操作部 130 は、操作者から数字列（PINコード）の入力を受け付ける。

[0279] 一方、S904 にて Yes だった場合（周辺の照度レベルが所定値以上で、顔認証が可能な場合）、S907 にて、基本動作実行部 1101 は、第一画像入力部 143（インカメラ）を有効化する。

[0280] 次に、S908 にて、第一画像入力部 143 は、操作者の顔画像を撮像する。

[0281] 次に、S909 にて、認証データ送受信実行部 1104 は、認証情報を認証サーバ 500 へ送信する。具体的には、認証データ送受信実行部 1104 は、S906 にて入力を受け付けた数字列または、S908 にて撮像された顔画像データを認証サーバ 500 へ送信する。

[0282] 次に、S910 にて、認証サーバ 500 の LAN 通信部 521 は、S909 にて送信された認証情報を受信する。そして、認証サーバ 500 へ認証処

理実行部5102は、受信した認証情報に基づく認証処理を実行する。

[0283] ここで、S909にて送信された認証情報がS906にて入力を受け付けた文字列である場合、認証処理実行部5102は、数字列を照合する認証処理（PIN照合による認証処理）を実行する。そして、認証処理実行部5102は、携帯情報端末100の操作者が正規のユーザかを判定する。

[0284] 一方、S909にて送信された認証情報がS908にて撮像された顔画像データである場合、認証処理実行部5102は、顔認証による認証処理を実行する。そして、認証処理実行部5102は、携帯情報端末100の操作者が正規のユーザかを判定する。

[0285] 次に、S911にて、認証処理実行部5102のLAN通信部521は、S910にて実行した認証処理の結果を携帯情報端末100へ送信する。

[0286] 次に、S912にて、基本動作実行部1101は、S911にて送信された認証結果に基づき、認証が成功したか否かを判定する。S912にて、基本動作実行部1101が、認証が成功せず、携帯情報端末100の操作者が正規のユーザでないと判定する場合（S912-No）、携帯情報端末100の機能ロック状態は、解除されずにS901へ戻る。一方、S912にて、基本動作実行部1101が、携帯情報端末100の操作者が正規のユーザであると判定する場合（S912-Yes）、S913へ進む。

[0287] 次に、S913にて、携帯ロック制御実行部1102は、携帯情報端末100の機能ロック状態を解除する。そして、携帯情報端末100の動作状態は、スリープ状態T111または電源オフ状態T112から通常動作状態T110へと遷移する。

[0288] 以上の処理により、本実施例の携帯情報端末100は、周辺の照度レベルに応じて実行する認証処理を選択することが可能になり、携帯情報端末100の使い勝手を向上させることができるようになる。

[0289] なお、図12に示される認証処理動作は、前述した図4Aに示される認証処理動作と同等の処理を、通信システムを構成する携帯情報端末100および認証サーバ500により実現したものである。そして、実施例1～実施例

5にて説明した他の認証処理動作と同等の処理を、実施例6の通信システムを構成する携帯情報端末100および認証サーバ500により実現するようにしても良い。

[0290] また、S906にて実行される認証処理は、画像に基づいて実行される認証処理でなければ、PIN照合による認証処理に限られるものではない。例えば、操作部130が、操作者からパスワードの入力を受け付け、入力を受け付けたパスワードと予め記憶されているパスワードとが一致するかを照合するようにしても良い。また、操作部130が、操作キーへの入力を複数回受け付け、入力を受け付けた操作キーと操作順との組み合わせが、予め記憶されている操作キーと操作順との組み合わせと一致するかを照合するようにしても良い。

[0291] また、S908にて実行される認証処理は、顔認証による認証処理に限られるものではない。例えば、カメラで撮像される画像に基づいて認証処理を行う場合、虹彩パターンに基づいた認証処理や掌紋認証等を適用しても良い。

[0292] なお、前述したソフトウェアは、製品出荷の時点で、予め携帯情報端末100のROM103またはストレージ部110に記憶されている状態であっても良い。また、製品出荷後に、インターネット200上のその他のアプリケーションサーバ400等からLAN通信部121または電話網通信部122を介して取得されるようにしても良い。また、メモリカードや光ディスク等に記憶されている各動作プログラムを、拡張インタフェース部124等を介して取得するようにしても良い。

[0293] <実施例6の効果>

以上説明した実施例6によれば認証サーバ500が、送信された認証情報を受信し、受信した認証情報を照合することで、認証サーバ500に蓄積された膨大な情報に基づく認証処理が可能になり、認証処理の精度を向上させることが可能になる。

[0294] 以上、本発明の実施形態の例を実施例1～実施例6を用いて具体的に説明

したが、本発明は前記実施の形態に限定されるものではなく、その要旨を逸脱しない範囲で種々変更可能であることはいうまでもない。例えば、ある実施例の構成の一部を他の実施例の構成と置き換えるようにしても良い。また、ある実施例の構成に他の実施例の構成を追加するようにしても良い。そして、これらは全て本発明の範疇に属するものである。

[0295] また、文中や図中に現れる数値やメッセージ等もあくまでも一例であり、異なるものを適用するようにしても良い。

[0296] また、携帯情報端末は、タブレット端末以外にも、スマートフォン等の様々な形態の携帯情報端末を全て含むものである。

[0297] また、前述した本発明の機能等は、それらの一部または全部を、例えば集積回路で設計する等によりハードウェアで実現しても良い。また、マイクロプロセッサユニット等がそれぞれの機能等を実現するプログラムを解釈して実行することによりソフトウェアで実現しても良い。また、ハードウェアとソフトウェアを併用しても良い。

[0298] また、図中に示した制御線や情報線は説明上必要と考えられるものを示しており、必ずしも製品上の全ての制御線や情報線を示しているとは限らない。そして、全ての構成が相互に接続されるように構成しても良い。

符号の説明

[0299] 100…携帯情報端末、101…主制御部、102…システムバス、103…ROM、104…RAM、110…ストレージ部、120…通信処理部、121…LAN通信部、122…移動体電話網通信部、123…NFC通信部、124…拡張インタフェース部、130…操作部、140…画像処理部、141…表示部、142…画像信号処理部、143…第一画像入力部、144…第二画像入力部、150…音声処理部、151…音声出力部、152…音声信号処理部、153…音声入力部、160…センサ部、161…GPS受信部、162…ジャイロセンサ、163…地磁気センサ、164…加速度センサ、165…照度センサ、166…近接センサ。

請求の範囲

- [請求項1] 各種機能の動作が制限される機能ロック状態を解除する認証処理を複数、実行可能な携帯情報端末であって、
- 検出された前記携帯情報端末の周辺の状況に応じて複数の前記認証処理から一つの前記認証処理を選択し、選択した前記認証処理を実行する主制御部を有する、携帯情報端末。
- [請求項2] 各種機能の動作が制限される機能ロック状態を解除する認証処理を複数、実行可能な携帯情報端末であって、
- 検出された前記携帯情報端末の周辺の状況と、前記携帯情報端末を操作する操作者の状態と、前記携帯情報端末の動作設定状態の少なくともいずれか一つに応じて複数の前記認証処理から一つの前記認証処理を選択し、選択した前記認証処理を実行する主制御部を有する、携帯情報端末。
- [請求項3] 請求項2に記載の携帯情報端末において、
- 前記携帯情報端末の周辺の照度の照度レベルを検出するセンサ部を有し、
- 前記携帯情報端末は、顔認証による認証処理を実行可能であり、
- 前記主制御部は、前記センサ部により検出された前記照度レベルが所定値以上である場合に、複数の前記認証処理から前記顔認証による認証処理を選択し、選択した前記認証処理を実行する、
- 携帯情報端末。
- [請求項4] 請求項2に記載の携帯情報端末において、
- 前記携帯情報端末の周辺の照度の照度レベルを検出するセンサ部を有し、
- 前記携帯情報端末は、操作者から入力を受け付けた情報を照合する認証処理を実行可能であり、
- 前記主制御部は、前記センサ部により検出された前記照度レベルが所定値未満である場合に、複数の前記認証処理から前記操作者から入

力を受け付けた情報を照合する認証処理を選択し、選択した前記認証処理を実行する、

携帯情報端末。

[請求項5]

請求項2に記載の携帯情報端末において、

前記携帯情報端末の周辺の前記操作者以外の人物を検出するセンサ部を有し、

前記携帯情報端末は、操作者から入力を受け付けた情報を照合する認証処理を実行可能であり、

前記主制御部は、前記センサ部により前記操作者以外の人物が検出された場合に、複数の前記認証処理から前記操作者から入力を受け付けた情報を照合する認証処理以外の前記認証処理を選択し、選択した前記認証処理を実行する、

携帯情報端末。

[請求項6]

請求項2に記載の携帯情報端末において、

前記携帯情報端末の周辺の音声の音量レベルを検出するセンサ部を有し、

前記携帯情報端末は、音声による認証処理を実行可能であり、

前記主制御部は、前記センサ部により検出された前記音量レベルが所定値未満の場合に、複数の前記認証処理から前記音声による認証処理を選択し、選択した前記認証処理を実行する、

携帯情報端末。

[請求項7]

請求項2に記載の携帯情報端末において、

前記携帯情報端末の周辺の音声の音量レベルを検出するセンサ部を有し、

前記携帯情報端末は、操作者から入力を受け付けた情報を照合する認証処理を実行可能であり、

前記主制御部は、前記センサ部により検出された前記音量レベルが所定値以上である場合に、複数の前記認証処理から前記操作者から入

力を受け付けた情報を照合する認証処理を選択し、選択した前記認証処理を実行する、

携帯情報端末。

[請求項8]

請求項2に記載の携帯情報端末において、

前記携帯情報端末は、音声による認証処理を実行可能であり、

前記主制御部は、前記携帯情報端末の動作設定状態がマナーモードである場合に、複数の前記認証処理から前記音声による認証処理以外の認証処理を選択し、選択した前記認証処理を実行する、

携帯情報端末。

[請求項9]

請求項2に記載の携帯情報端末において、

携帯情報端末の姿勢と加速度の少なくともいずれか一つを検出するセンサ部を有し、

前記携帯情報端末は、音声による認証処理を実行可能であり、

前記主制御部は、前記センサ部により検出された前記姿勢と前記加速度の少なくともいずれか一つに基づき、前記携帯情報端末の操作者が移動中であるか否かを判定し、前記操作者が移動中であると判定する場合に、複数の前記認証処理から前記音声による認証処理を選択し、選択した前記認証処理を実行する、

携帯情報端末。

[請求項10]

各種機能の動作が制限される機能ロック状態を解除する認証処理を複数、実行可能な携帯情報端末の制御方法であって、

主制御部が、出した前記携帯情報端末の周辺の状況に応じて複数の前記認証処理から一つの前記認証処理を選択する認証処理選択ステップと、

主制御部が、選択した前記認証処理を実行する認証処理実行ステップと、

を有する、携帯情報端末の制御方法。

[請求項11]

各種機能の動作が制限される機能ロック状態を解除する認証処理を

複数、実行可能な携帯情報端末の制御方法であって、

主制御部が、検出された前記携帯情報端末の周辺の状況と、前記携帯情報端末を操作する操作者の状態と、前記携帯情報端末の動作設定状態の少なくともいずれか一つに応じて複数の前記認証処理から一つの前記認証処理を選択する認証処理選択ステップと、

主制御部が、選択した前記認証処理を実行する認証処理実行ステップと、

を有する、携帯情報端末の制御方法。

[請求項12]

請求項 1 1 に記載の携帯情報端末の制御方法において、

センサ部が、前記携帯情報端末の周辺の照度の照度レベルを検出する検出ステップをさらに有し、

前記認証処理選択ステップは、前記主制御部が、前記検出ステップにて検出された前記照度レベルが所定値以上である場合に、複数の前記認証処理から顔認証による認証処理を選択する、

携帯情報端末の制御方法。

[請求項13]

請求項 1 1 に記載の携帯情報端末の制御方法において、

センサ部が、前記携帯情報端末の周辺の照度の照度レベルを検出する検出ステップをさらに有し、

前記認証処理選択ステップは、前記主制御部が、前記検出ステップにて検出された前記照度レベルが所定値未満である場合に、複数の前記認証処理から操作者から入力を受け付けた情報を照合する認証処理を選択する、

携帯情報端末の制御方法。

[請求項14]

請求項 1 1 に記載の携帯情報端末の制御方法において、

センサ部が、前記携帯情報端末の周辺の前記操作者以外の人物を検出する検出ステップをさらに有し、

前記認証処理選択ステップは、前記主制御部が、前記検出ステップにて前記操作者以外の人物が検出された場合に、複数の前記認証処理

から操作者から入力を受け付けた情報を照合する認証処理以外の認証処理を選択する、

携帯情報端末の制御方法。

[請求項15]

請求項 1 1 に記載の携帯情報端末の制御方法において、

センサ部が、前記携帯情報端末の周辺の音声の音量レベルを検出する検出ステップをさらに有し、

前記認証処理選択ステップは、前記主制御部が、前記検出ステップにて検出された前記音量レベルが所定値未満の場合に、複数の前記認証処理から音声による認証処理を選択する、

携帯情報端末の制御方法。

[請求項16]

請求項 1 1 に記載の携帯情報端末の制御方法において、

センサ部が、前記携帯情報端末の周辺の音声の音量レベルを検出する検出ステップをさらに有し、

前記認証処理選択ステップは、前記主制御部が、前記検出ステップにて検出された前記音量レベルが所定値以上の場合に、複数の前記認証処理から操作者から入力を受け付けた情報を照合する認証処理を選択する、

携帯情報端末の制御方法。

[請求項17]

請求項 1 1 に記載の携帯情報端末の制御方法において、

前記認証処理選択ステップは、前記主制御部が、前記携帯情報端末の動作設定状態がマナーモードである場合に、複数の前記認証処理から音声による認証処理以外の認証処理を選択し、選択した前記認証処理を実行する、

携帯情報端末。

[請求項18]

請求項 1 1 に記載の携帯情報端末の制御方法において、

センサ部が、前記携帯情報端末の姿勢と加速度の少なくともいずれか一つを検出する検出ステップと、

前記主制御部が、前記検出ステップにて検出された情報に基づき、

前記携帯情報端末の操作者が移動中であるか否かを判定する判定ステップと、

をさらに有し、

前記認証処理選択ステップは、前記主制御部が、前記操作者が移動中であると判定する場合に、複数の前記認証処理から前記音声による認証処理を選択する、

携帯情報端末の制御方法。

[請求項19]

各種機能の動作が制限される機能ロック状態を解除する認証処理を複数、実行可能な認証サーバと、前記認証サーバとネットワークを介して接続される携帯情報端末と、を有する通信システムであって、

前記携帯情報端末は、

検出された前記携帯情報端末の周辺の状況に応じて複数の前記認証処理から一つの前記認証処理を選択する主制御部と、

前記主制御部により選択された前記認証処理と対応する認証情報を前記認証サーバに送信する通信処理部と、

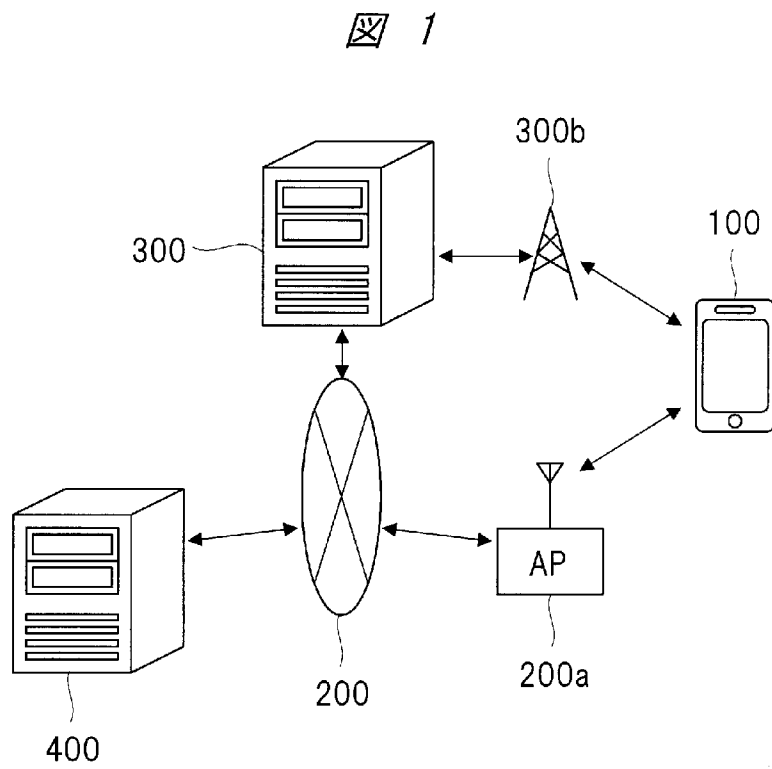
を有し、

前記認証サーバは、

送信された前記認証情報を受信し、受信した前記認証情報を照合する、

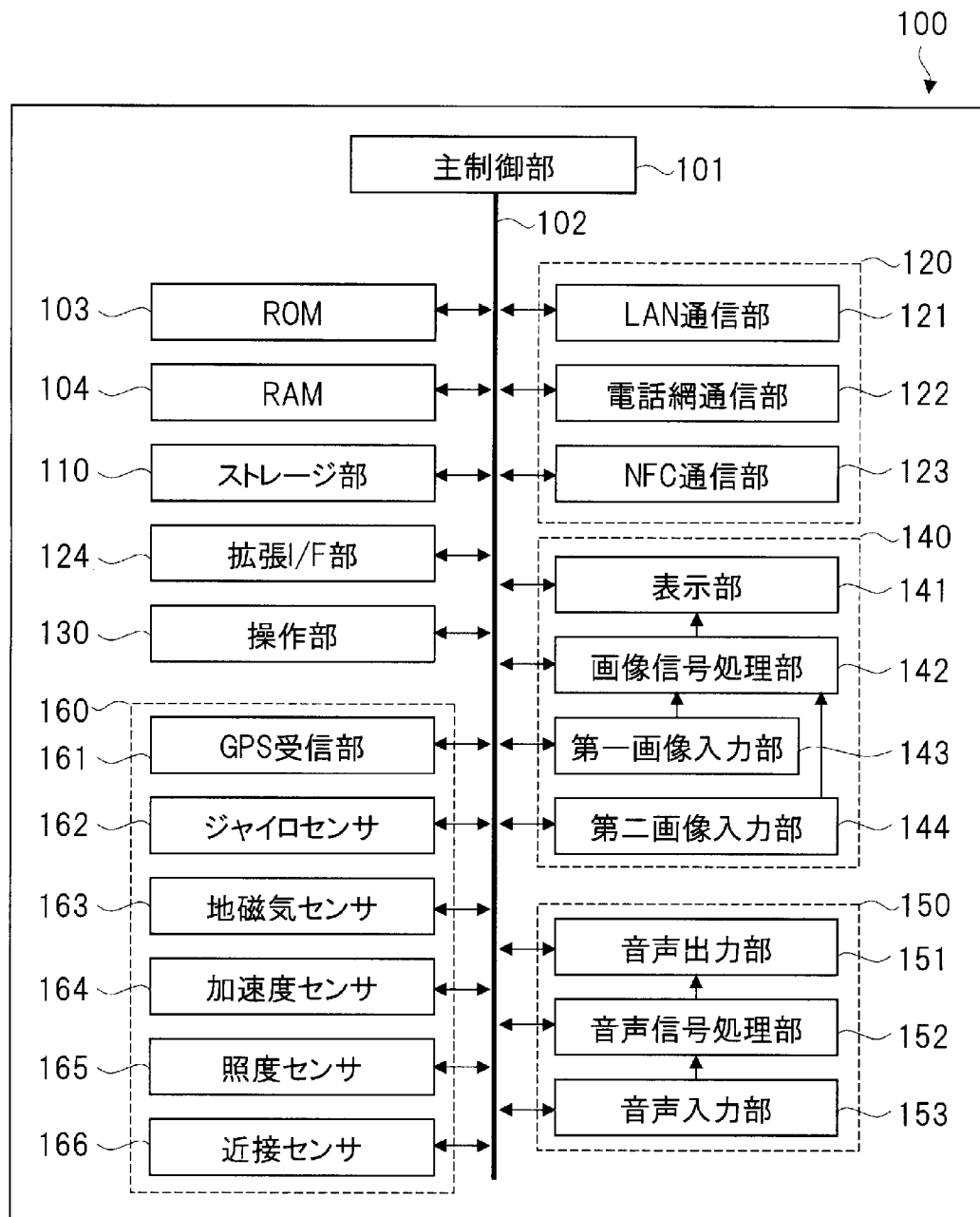
通信システム。

[図1]

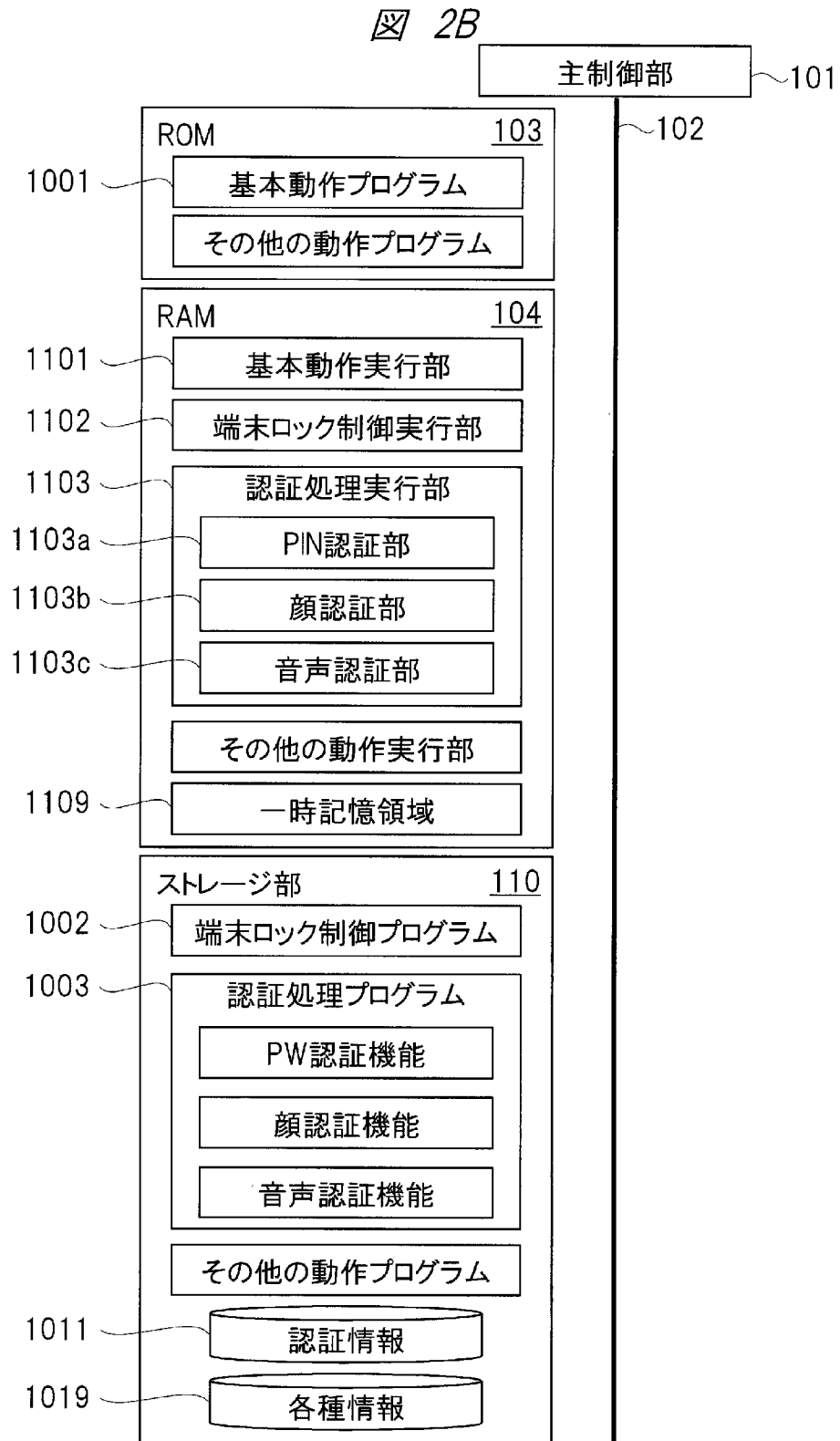


[図2A]

図 2A

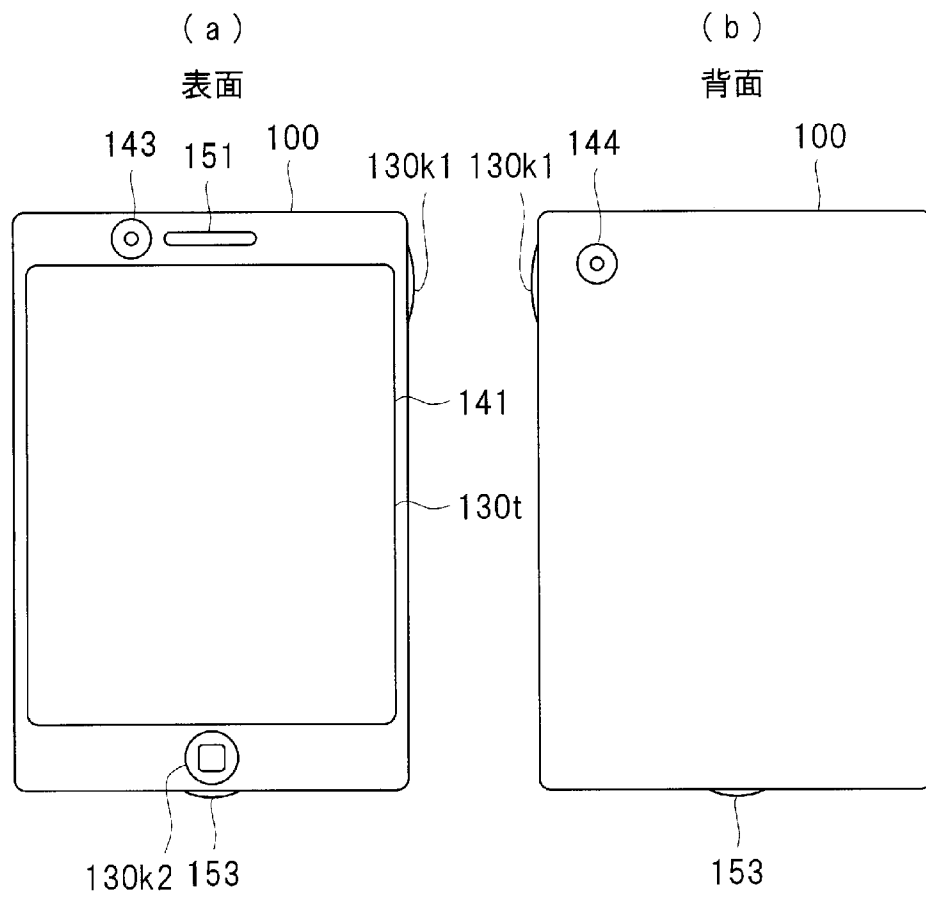


[図2B]



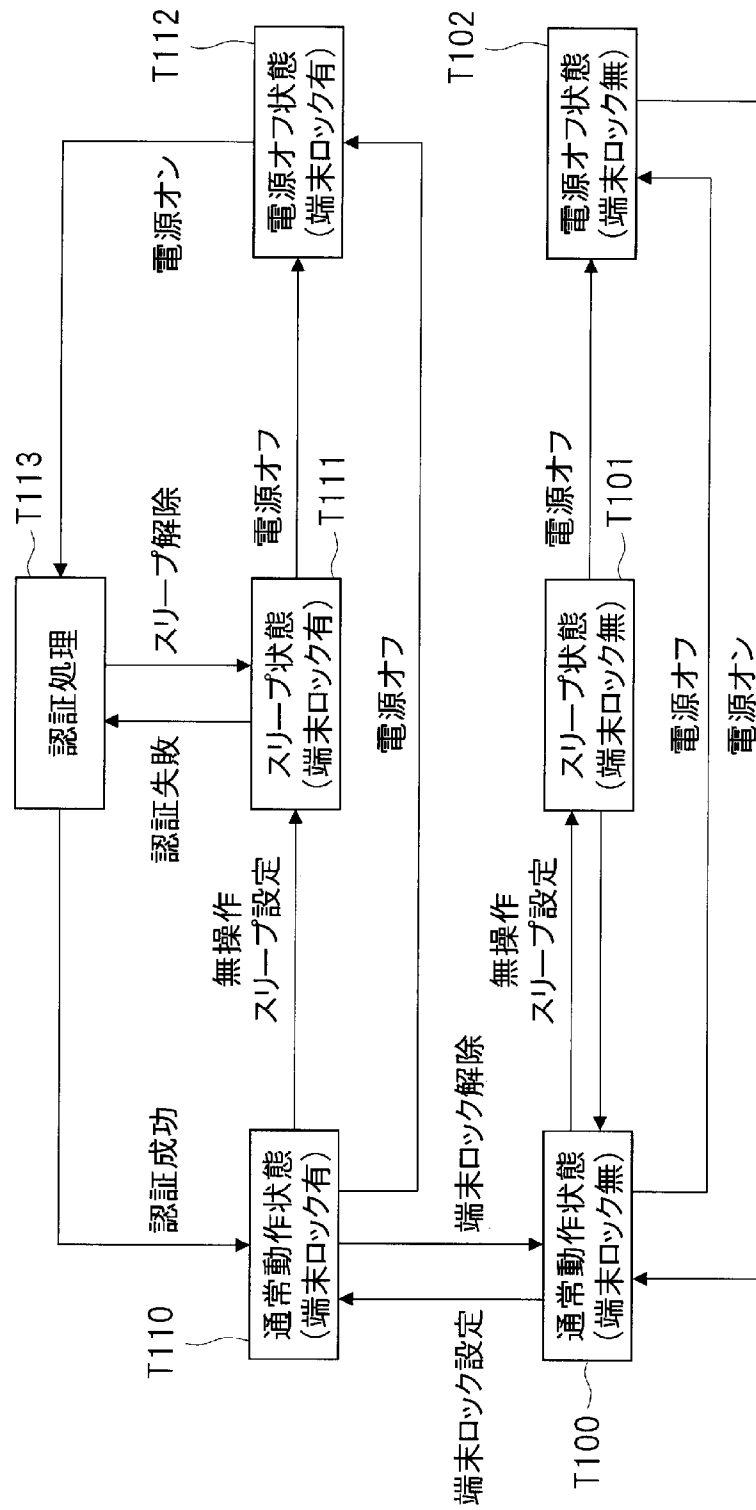
[図2C]

図 2C



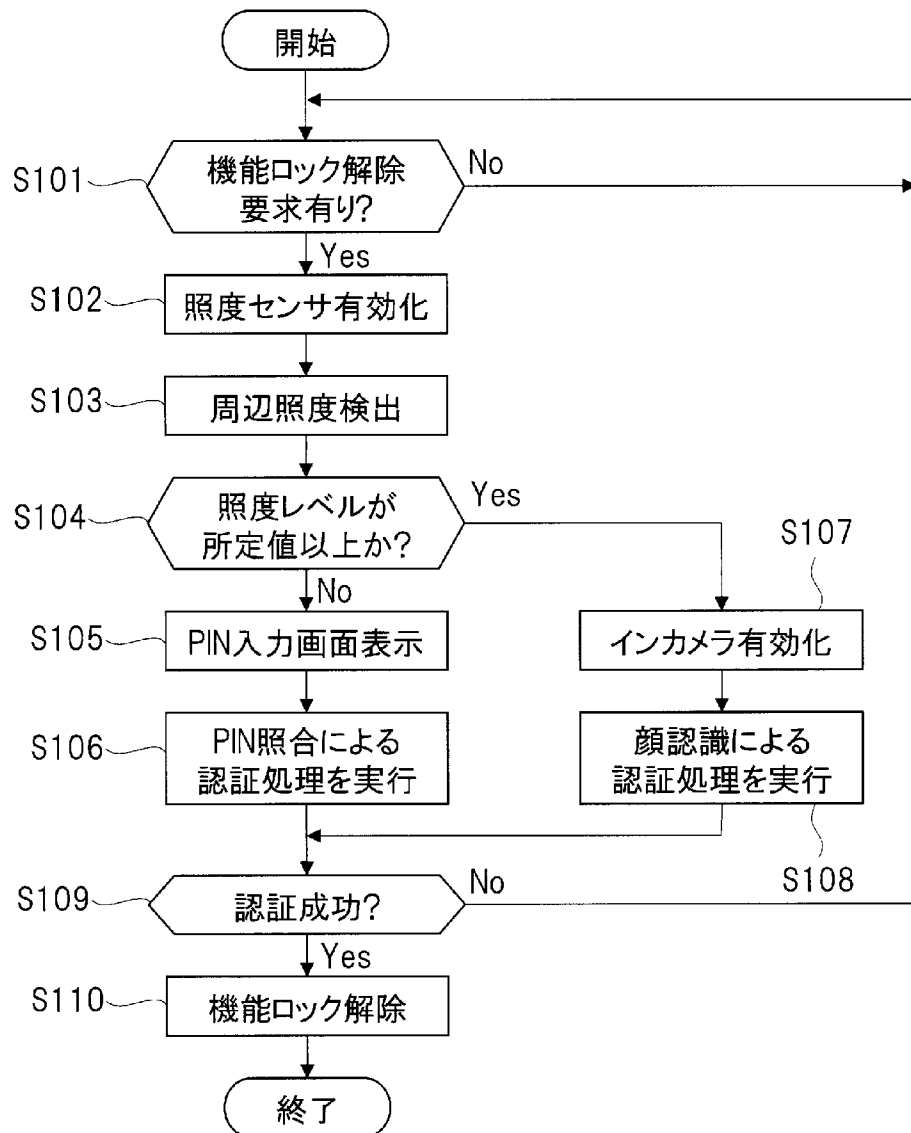
[図3]

図 3



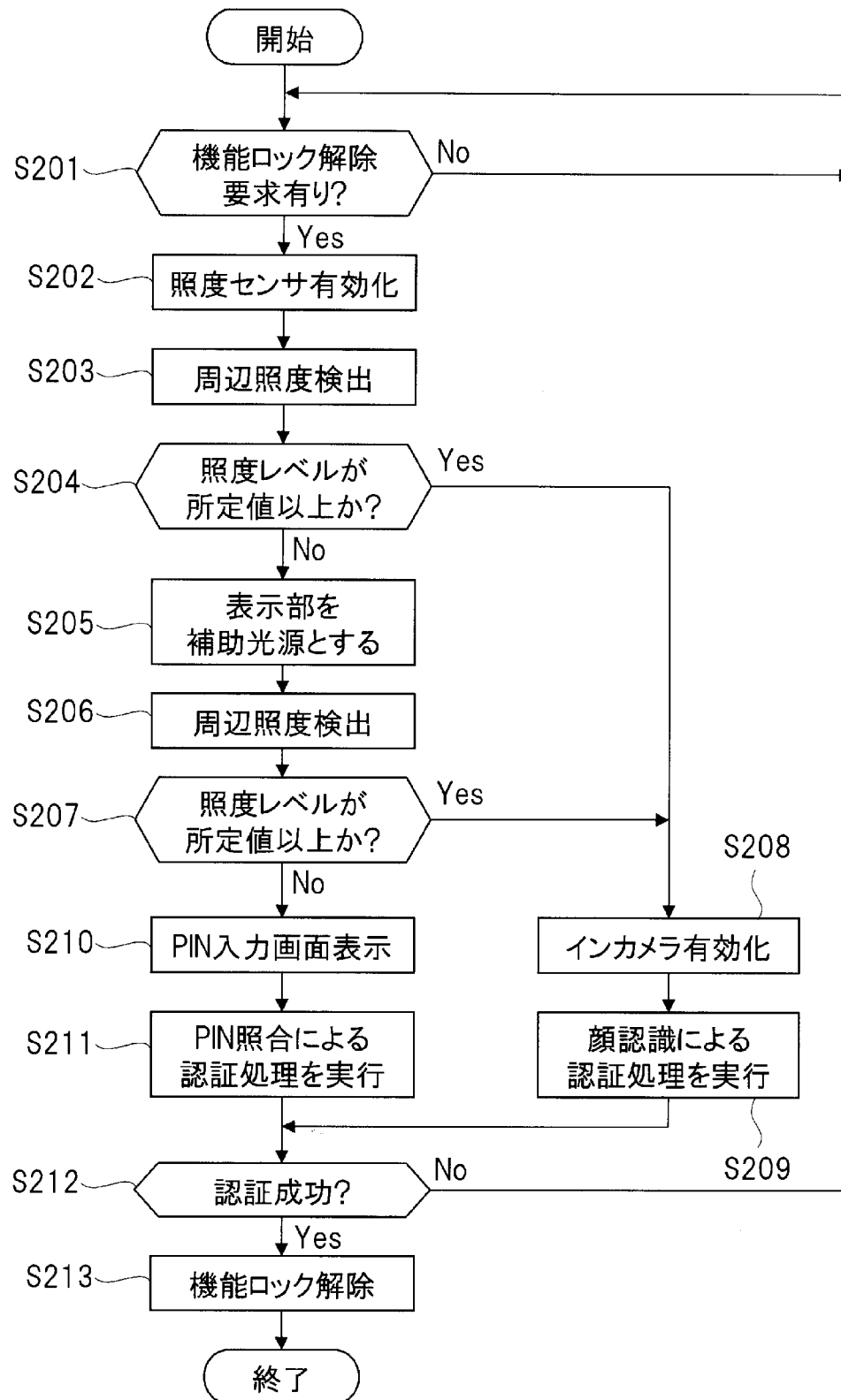
[図4A]

図 4A



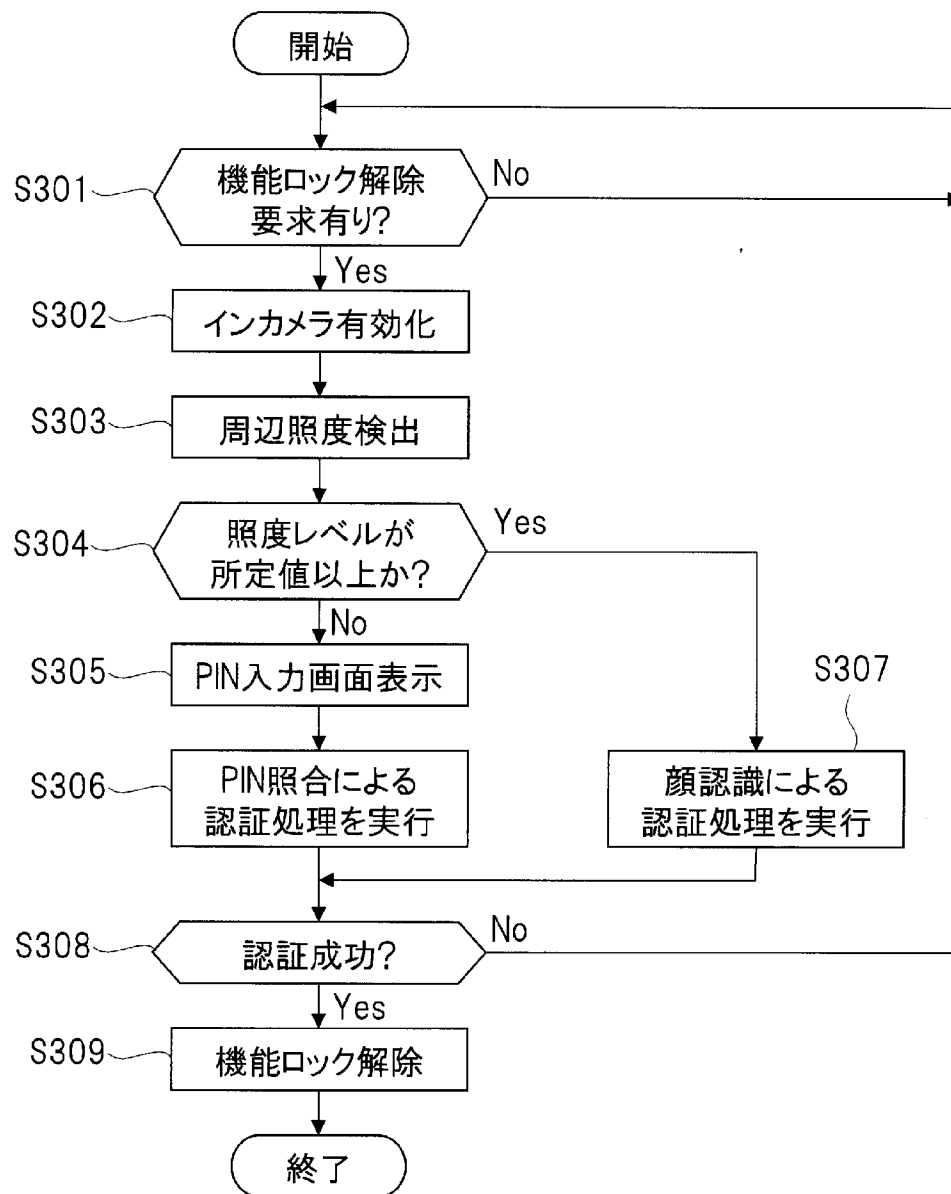
[図4B]

図 4B



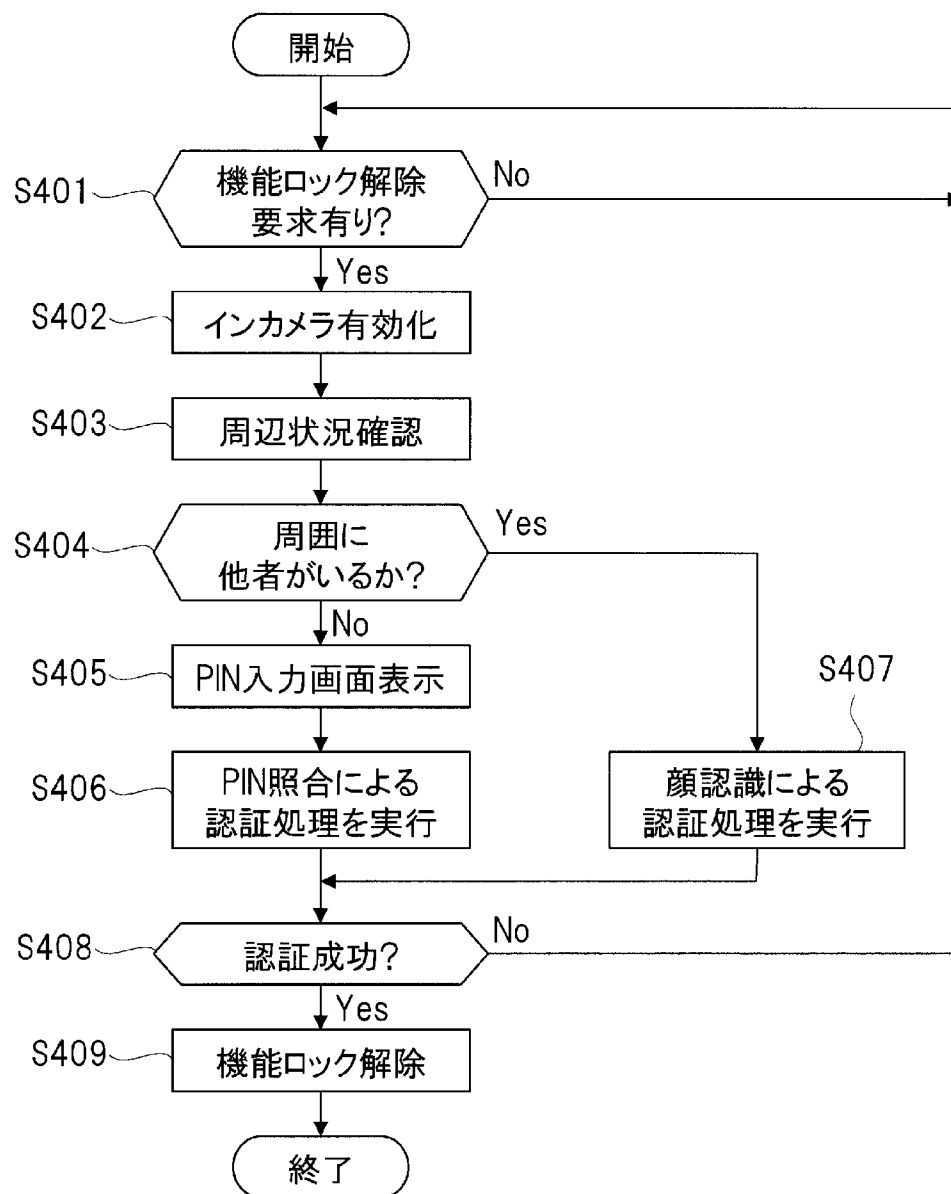
[図4C]

図 4C



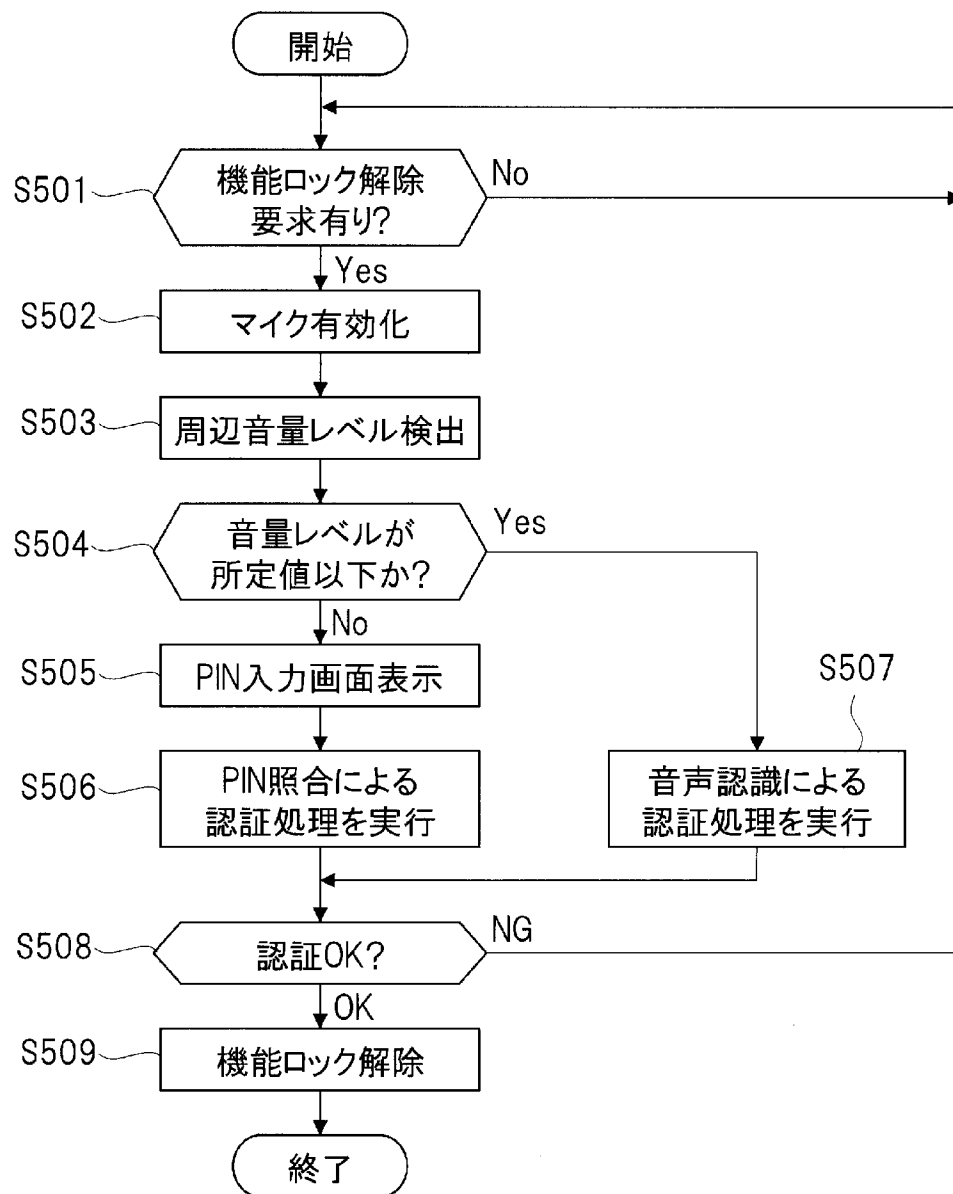
[図5]

図 5



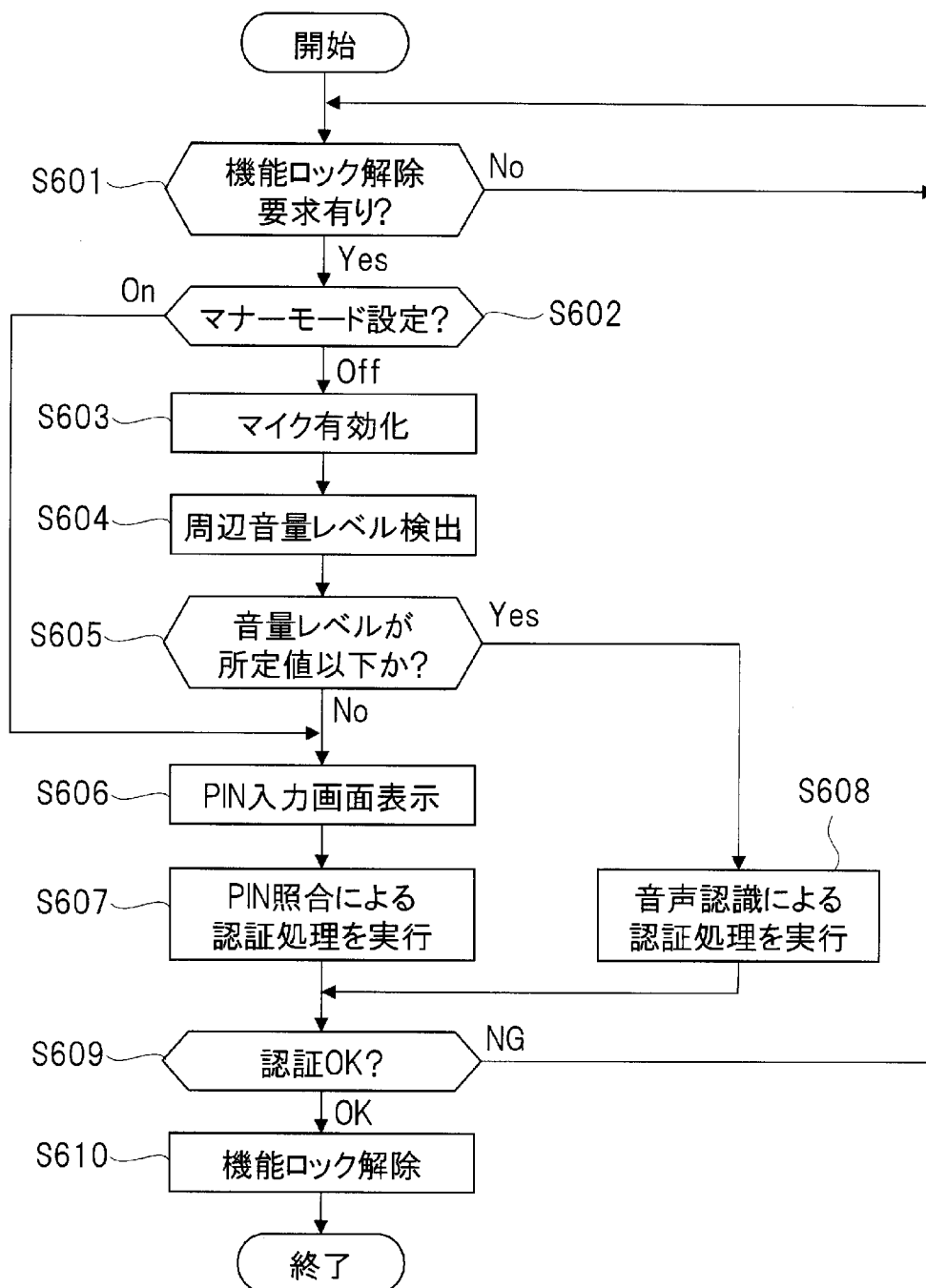
[図6A]

図 6A



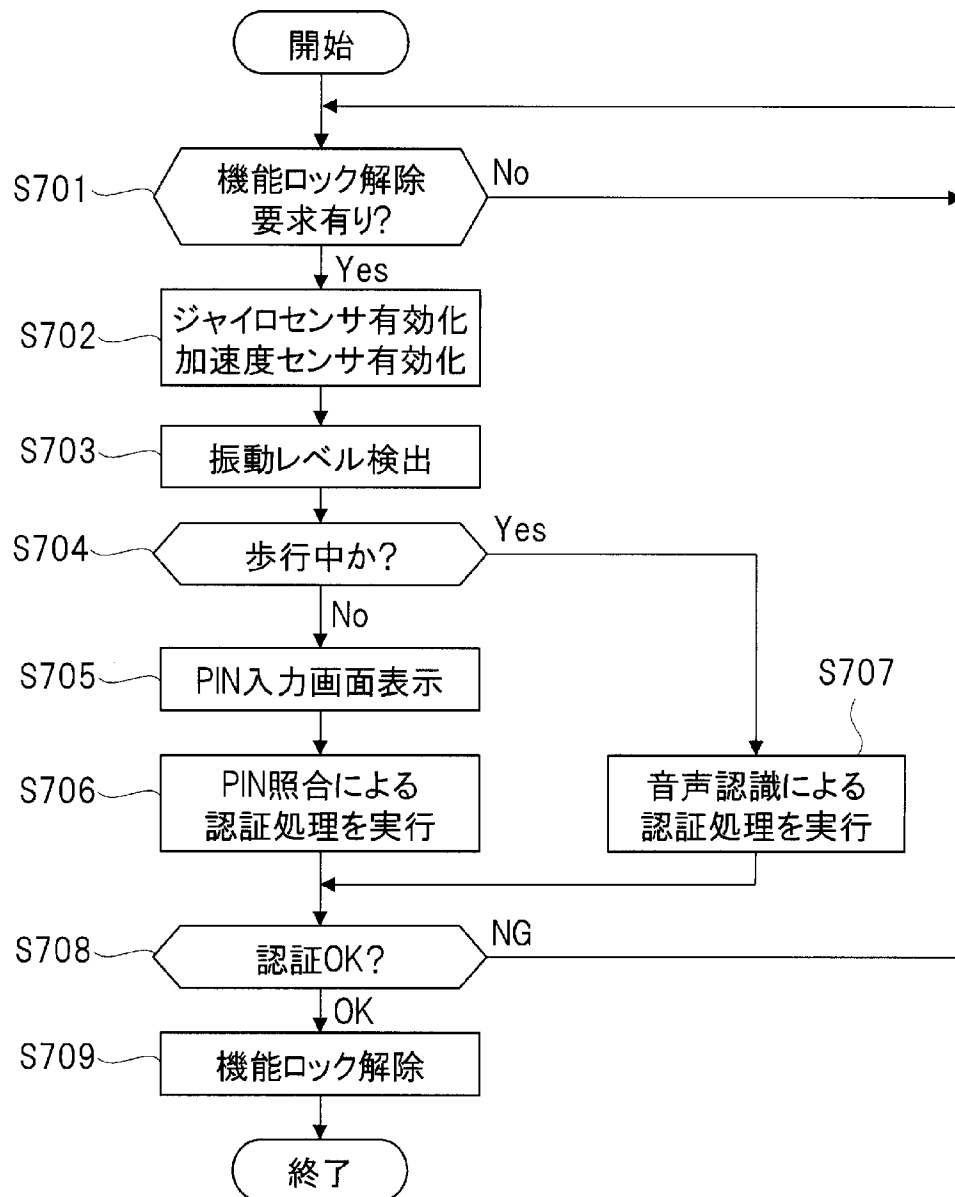
[図6B]

図 6B



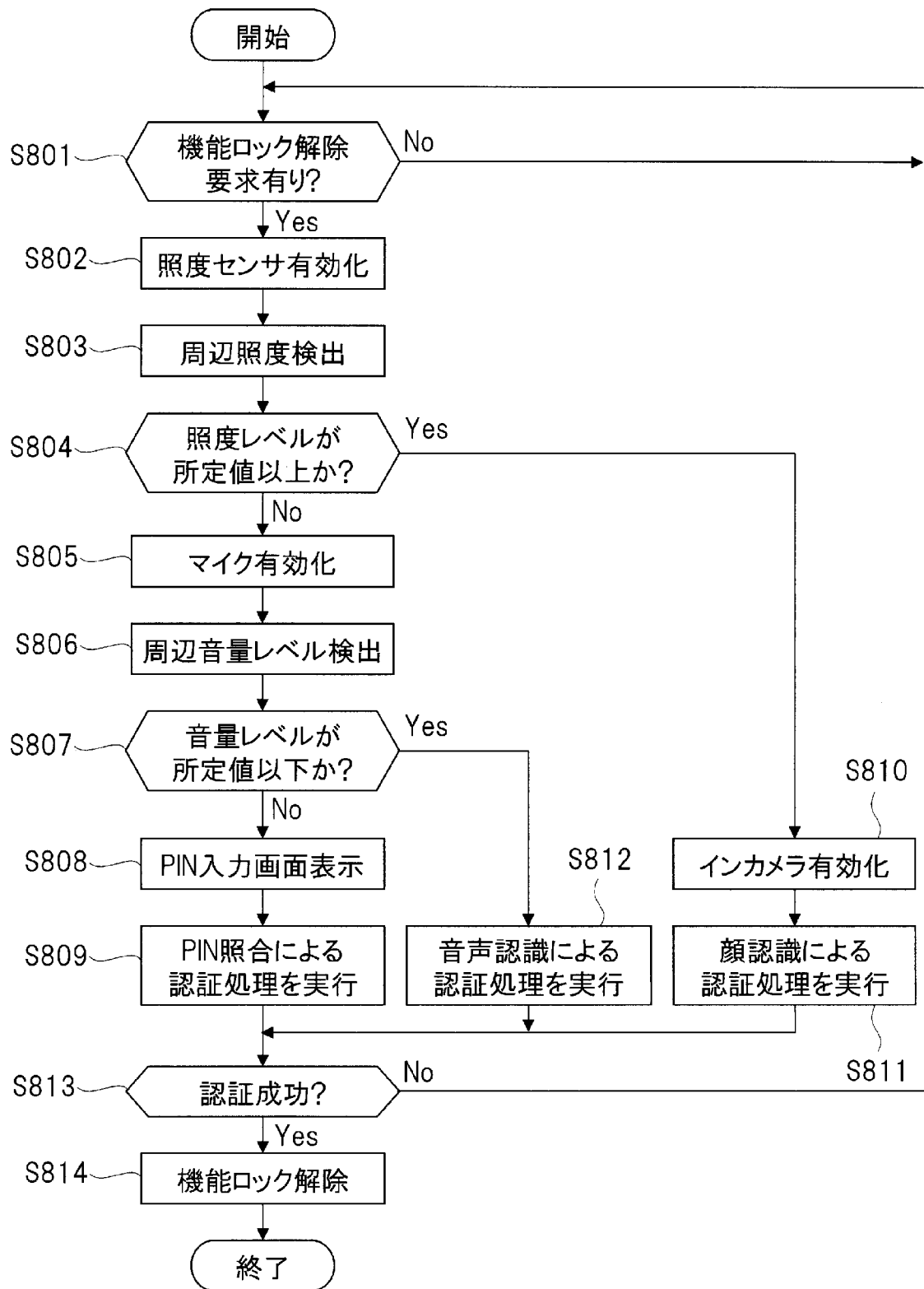
[図7]

図 7



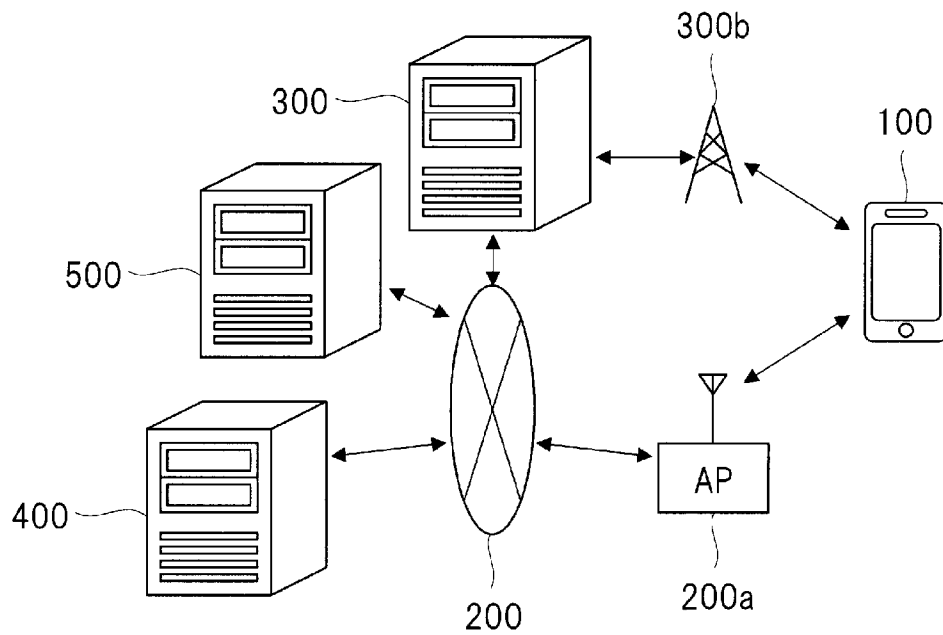
[図8]

図 8



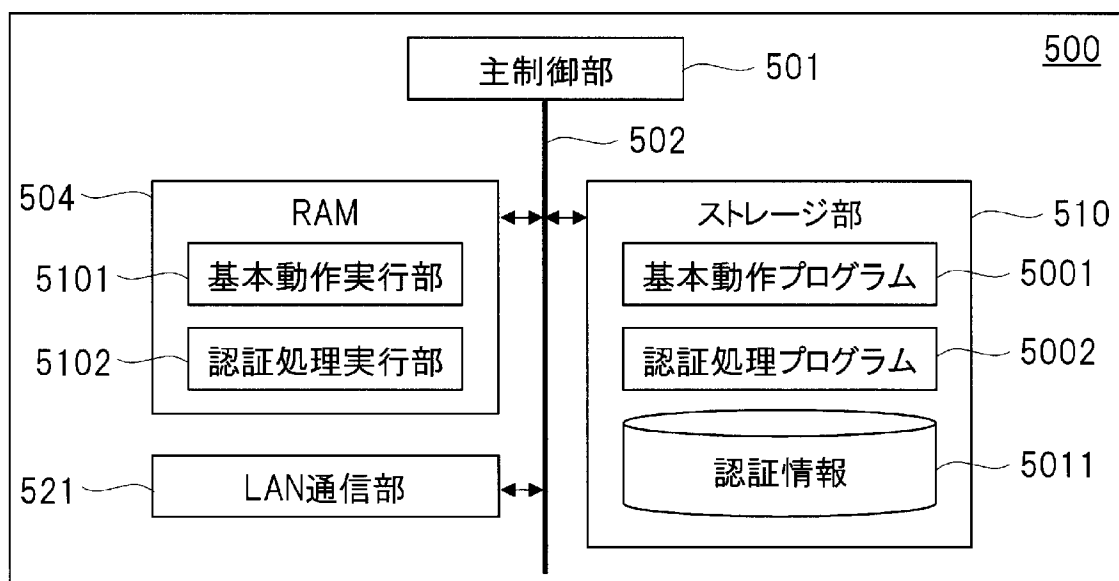
[図9]

図 9



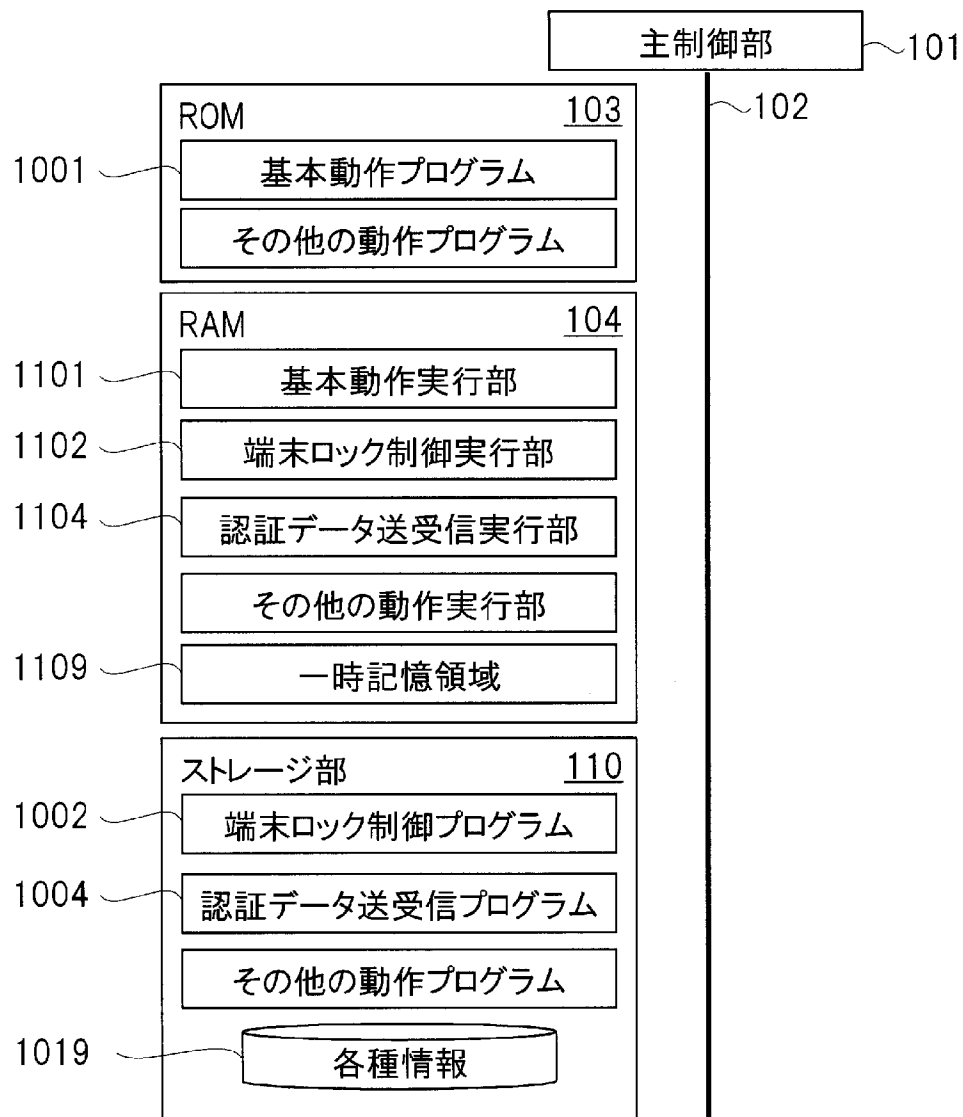
[図10]

図 10



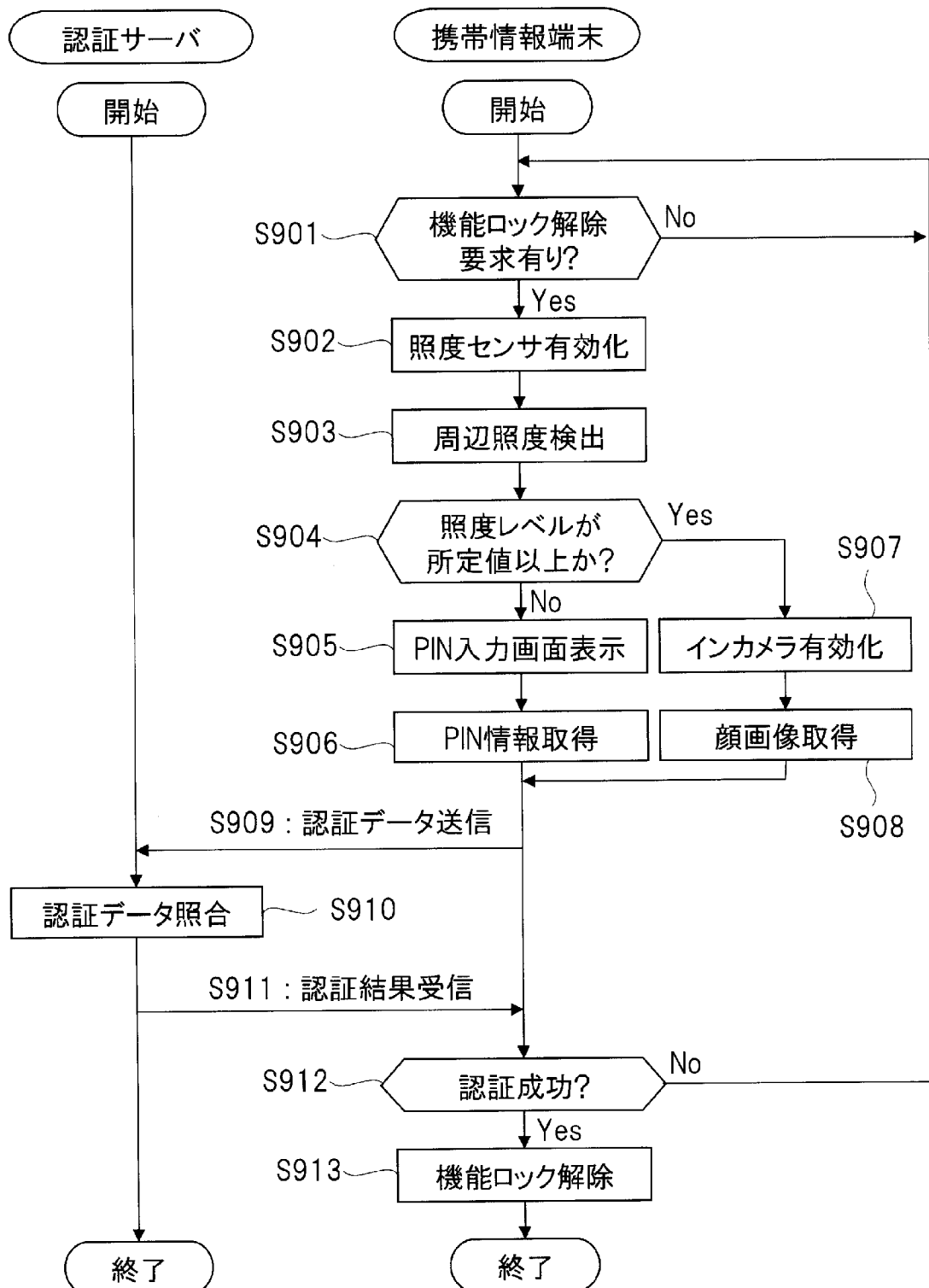
[図11]

図 11



[図12]

図 12



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2014/070216

A. CLASSIFICATION OF SUBJECT MATTER

H04M1/673(2006.01)i, H04M11/00(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)

G06F3/01-3/0482, 3/0485, 3/0487-3/0489, 12/14, 21/00, 21/10, 21/30-21/46, 21/60-21/88, H03M11/04, 11/08-11/14, 11/20-11/24, H04M1/00, 1/24-3/00, 3/16-3/20, 3/38-3/58, 7/00-7/16, 11/00-11/10, 99/00, H04N5/222-5/257

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 1996-2014
Kokai Jitsuyo Shinan Koho 1971-2014 Toroku Jitsuyo Shinan Koho 1994-2014

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.
Y	JP 2002-008034 A (Cyber Sign Japan Inc.), 11 January 2002 (11.01.2002), paragraphs [0068] to [0124]; fig. 1 to 6 (Family: none)	1-19
Y	JP 2012-238141 A (Sony Corp.), 06 December 2012 (06.12.2012), paragraph [0055] & US 2012/0291093 A1 & CN 102780560 A	1-19
Y	JP 2007-049304 A (Sharp Corp.), 22 February 2007 (22.02.2007), paragraphs [0070], [0071] (Family: none)	3, 4, 12, 13

☒ 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
02 October, 2014 (02.10.14)

Date of mailing of the international search report
14 October, 2014 (14.10.14)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2014/070216

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2009-081657 A (Kyocera Corp.), 16 April 2009 (16.04.2009), paragraphs [0023], [0038], [0039] (Family: none)	3, 4, 12, 13
Y	JP 2002-318885 A (Toshiba Tec Corp.), 31 October 2002 (31.10.2002), paragraphs [0071], [0072] (Family: none)	5, 14
Y	JP 2012-129701 A (NEC CASIO Mobile Communications, Ltd.), 05 July 2012 (05.07.2012), paragraphs [0021], [0028] (Family: none)	5, 14
Y	JP 2007-235810 A (NEC Corp.), 13 September 2007 (13.09.2007), paragraph [0043] (Family: none)	8, 17
Y	JP 2012-063921 A (NTT Docomo Inc.), 29 March 2012 (29.03.2012), paragraphs [0006], [0024], [0032] (Family: none)	9, 18

A. 発明の属する分野の分類（国際特許分類（I P C））

Int.Cl. H04M1/673(2006.01)i, H04M11/00(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. G06F3/01-3/0482, 3/0485, 3/0487-3/0489, 12/14, 21/00, 21/10, 21/30-21/46, 21/60-21/88
 H03M11/04, 11/08-11/14, 11/20-11/24,
 H04M1/00, 1/24-3/00, 3/16-3/20, 3/38-3/58, 7/00-7/16, 11/00-11/10, 99/00, H04N5/222-5/257

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	1 9 2 2 - 1 9 9 6 年
日本国公開実用新案公報	1 9 7 1 - 2 0 1 4 年
日本国実用新案登録公報	1 9 9 6 - 2 0 1 4 年
日本国登録実用新案公報	1 9 9 4 - 2 0 1 4 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 請求項の番号
Y	JP 2002-008034 A（日本サイバーサイン株式会社）2002.01.11, 段落【0068】-【0124】、図1-6（ファミリーなし）	1-19
Y	JP 2012-238141 A（ソニー株式会社）2012.12.06, 段落【0055】 & US 2012/0291093 A1 & CN 102780560 A	1-19
Y	JP 2007-049304 A（シャープ株式会社）2007.02.22, 段落【0070】、【0071】（ファミリーなし）	3, 4, 12, 13

☒ 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

0 2 . 1 0 . 2 0 1 4

国際調査報告の発送日

1 4 . 1 0 . 2 0 1 4

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）

松原 徳久

5 G

4 8 7 8

電話番号 0 3 - 3 5 8 1 - 1 1 0 1 内線 3 5 2 6

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 請求項の番号
Y	JP 2009-081657 A (京セラ株式会社) 2009. 04. 16, 段落【0023】 , 【0038】 , 【0039】 (ファミリーなし)	3, 4, 12, 13
Y	JP 2002-318885 A (東芝テック株式会社) 2002. 10. 31, 段落【0071】 , 【0072】 (ファミリーなし)	5, 14
Y	JP 2012-129701 A (NECカシオモバイルコミュニケーションズ株 式会社) 2012. 07. 05, 段落【0021】 , 【0028】 (ファミリーなし)	5, 14
Y	JP 2007-235810 A (日本電気株式会社) 2007. 09. 13, 段落【0043】 (ファミリーなし)	8, 17
Y	JP 2012-063921 A (株式会社エヌ・ティ・ティ・ドコモ) 2012. 03. 29, 段落【0006】 , 【0024】 , 【0032】 (ファミリーなし)	9, 18