

(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
2011年6月30日(30.06.2011)



(10) 国際公開番号
WO 2011/077512 A1

- (51) 国際特許分類:
G06F 21/20 (2006.01)
- (21) 国際出願番号: PCT/JP2009/071277
- (22) 国際出願日: 2009年12月22日(22.12.2009)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (71) 出願人(米国を除く全ての指定国について): 安田浩(YASUDA Hiroshi) [JP/JP]; 〒2470008 神奈川県横浜市栄区本郷台2-27-20 Kanagawa (JP).
- (72) 発明者; および
- (71) 出願人: 杉中順子(SUGINAKA Junko) [JP/JP]; 〒1050001 東京都港区虎ノ門3丁目10番4号 虎ノ門ガーデン408号 Tokyo (JP).
- (72) 発明者; および
- (75) 発明者/出願人(米国についてのみ): 古川義久(FURUKAWA Yoshihisa) [JP/JP]; 〒1020094 東京都

千代田区紀尾井町4番3号 株式会社F. t r o n 内 Tokyo (JP).

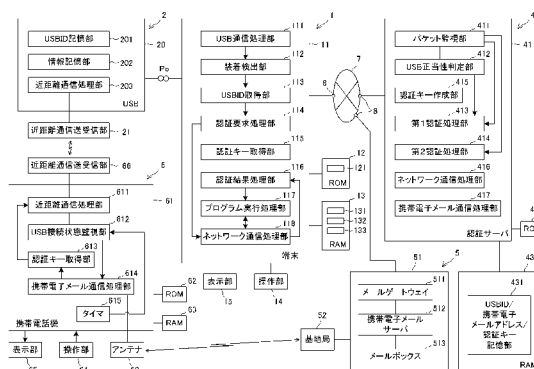
- (74) 代理人: 伊藤孝夫(ITO H Takao); 〒5400011 大阪府大阪市中央区農人橋1丁目4番34号 Osaka (JP).
- (81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.
- (84) 指定国(表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア

[続葉有]

(54) Title: USER AUTHENTICATION METHOD, USER AUTHENTICATION SYSTEM, AND PORTABLE COMMUNICATIONS TERMINAL

(54) 発明の名称: 本人認証方法、本人認証システム及び携帯型通信端末

(図2)



- 1 TERMINAL
4 AUTHENTICATION SERVER
6 CELLULAR PHONE
14, 64 CONSOLE UNIT
15, 65 DISPLAY UNIT
21, 66 SHORT-RANGE COMMUNICATIONS TRANSCIVER UNIT
52 BASE STATION
60 ANTENNA
111 USB MODULE/COMMUNICATIONS PROCESSING UNIT
112 ATTACHMENT DETECTION UNIT
113 USB ID ACQUISITION UNIT
114 AUTHENTICATION REQUEST PROCESSING UNIT
115 AUTHENTICATION KEY ACQUISITION UNIT
116 AUTHENTICATION RESULT PROCESSING UNIT
117 PROGRAM EXECUTION PROCESSING UNIT
118, 416 NETWORK COMMUNICATIONS PROCESSING UNIT
201 USB ID MEMORY UNIT
202 INFORMATION MEMORY UNIT
203, 611 SHORT-RANGE COMMUNICATIONS PROCESSING UNIT
411 PACKET MONITORING UNIT
412 USB MODULE VALIDATION UNIT
413 FIRST AUTHENTICATION PROCESSING UNIT
414 SECOND AUTHENTICATION PROCESSING UNIT
415 AUTHENTICATION KEY GENERATION UNIT
417, 614 CELLULAR PHONE E-MAIL COMMUNICATIONS PROCESSING UNIT
431 USB ID/CELLULAR PHONE E-MAIL ADDRESS/AUTHENTICATION KEY MEMORY UNIT
511 E-MAIL GATEWAY
512 CELLULAR PHONE E-MAIL SERVER
513 MAILBOX
612 USB MODULE CONNECTION STATE MONITORING UNIT
613 AUTHENTICATION KEY ACQUISITION UNIT
615 TIMER

(57) Abstract: A user authentication system comprises a terminal (1) capable of a prescribed type of data processing; a USB memory module (2) capable of short-range communication via Bluetooth with a cellular phone (6), the cellular phone (6) further comprising an e-mail function; and an authentication server (4). When the USB memory module (2) is attached to the terminal (1), the USB ID is read out and transmitted from the terminal (1) to the authentication server (4). The authentication server (4) authenticates the USB ID, and transmits an authentication key corresponding to the USB ID to the cellular phone (6), if the USB ID is valid. The cellular phone (6) transmits the authentication key to the USB memory module (2) via Bluetooth. The authentication key thus received is transmitted from the terminal (1) to the authentication server (4) via the USB memory module (2). The authentication server (4) authenticates the user by comparing the authentication key transmitted thereby with the authentication key received thereby.

(57) 要約:

[続葉有]



(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, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL,
NO, PL, PT, RO, SE, SI, SK, SM, 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 (条約第 21 条(3))

本人認証システムは、所定の情報処理が可能な端末（１）、電子メール機能を備えた携帯電話機（６）とブルーツースによる近距離通信が可能なＵＳＢメモリ（２）、及び認証サーバ（４）を備える。ＵＳＢメモリ（２）が端末（１）に装着されると、ＵＳＢＩＤが読み取られ、端末（１）から認証サーバ（４）に送信される。認証サーバ（４）はＵＳＢＩＤの認証を行い、正当であればＵＳＢＩＤに対応する認証キーを対応する携帯電話機６に送信する。携帯電話機（６）は認証キーをブルーツースでＵＳＢメモリ（２）に送信する。受信された認証キーはＵＳＢメモリ（２）を経て端末（１）から認証サーバ（４）に送信される。認証サーバ（４）は送信した認証キーと受信した認証キーとの異同を比較することで本人認証を行う。

明 細 書

発明の名称：

本人認証方法、本人認証システム及び携行型通信端末

技術分野

[0001] 本発明は、ネットワークに接続された情報処理端末を使用する者の正当性を認証する認証技術に関する。

背景技術

[0002] 近年、インターネットを始めとした通信ネットワークの急激な進展により、種々の商取引等のサービスが、端末から通信ネットワークを介して行われるようになってきている。同様に、行政機関等に対する行政手続等のサービスも通信ネットワークを介して行われるようになってきている。かかるサービスの実行に際し、ネットワークを介して授受される情報には決済情報、取引情報を含む個人情報等が少なくない。一方で、他人になりすましてサーバやデータベース等に侵入し、かかる個人情報等を閲覧、盗用し、また改竄したりする不正行為が増大している。従って、端末を使用する者が本人か否かを判断する本人認証を行うことが重要である。

[0003] ネットワーク上に設けられた認証局で行われる本人認証技術として、生体情報を利用したものが知られている。特許文献 1 には、端末利用者の指紋データの他、クロック回路及びGPS受信機を用いて得られる存在場所や認証日時を併用する認証技術が記載されている。また、特許文献 1 には、指紋の他、虹彩や静脈などの生体を識別できる情報が利用可能であることが記載されている。また、特許文献 2 には、出先のパーソナルコンピュータ（以下、パソコン）からネットワークを介して取引を可能にするネットシステムが記載されている。より詳細には、特許文献 2 には、取引に際して、ユーザの携帯電話機にセンターサーバからパスワードが電子メールで送信されると、ユーザは、受信したパスワードを目視しながら、パソコンのパスワード入力欄にキーを操作してパスワードを入力するものである。そして、入力された情

報がセンターサーバに送信されて、元のパスワードと照合されることで、本人認証が行われることが記載されている（段落番号500～502）。これにより、ユーザが所有するパソコン以外のパソコンにて手続処理やログインや取引処理が安全に行えるようにしている。なお、特許文献2には、携帯電話機で受信したメールをユーザによってセンターサーバに返信するようにしてもよいことが記載されている（段落番号503）。

先行技術文献

特許文献

[0004] 特許文献1：特開2009-104248号公報

特許文献2：特開2008-33571号公報

発明の概要

発明が解決しようとする課題

[0005] 特許文献1に記載の認証技術は、指紋という固体個々の情報を利用する点で優れている一方、指紋などは偽造され易い上に、認証対象となる指紋データが偽造されたものであるか否かを識別することは容易ではない。特許文献2に記載のネットシステムは、ユーザに、携帯電話機の画面を見ながらパソコンへの入力操作という、従来とほぼ同様のパスワード入力操作を強いることになり、キー操作の内容、すなわちパスワードを周囲の他人に知られる虞が高い。また、パスワードが無線傍受によって知得され、不正使用される可能性もある。さらに、特許文献2は、パスワードの入力操作のみクリアすれば、その後は、自由にパソコンを不正使用することも可能となり、万全ではない。一方、特許文献2に記載の、携帯電話機で受信したパスワードをユーザがセンターサーバに返信する態様では、ユーザとパソコンとの物理的な位置の一致が検証できないため、ユーザとパソコンとが同一の場所にいるという保証が取れず、本人認証に一定の限界があることになる。

[0006] 本発明の目的は、情報処理端末に装着して所定の情報処理の実行を許可する携行型記憶媒体に対して、装着状態で前記携行型記憶媒体の認証と、前記

携行型記憶媒体を経由して本人認証を行うようにして、認証処理の不正なすり抜け操作等を効果的に阻止する本人認証方法、本人認証システム及び本システムに使用する携行型通信端末を提供することにある。

課題を解決するための手段

- [0007] 本発明に係る本人認証システムは、ネットワークに接続された情報処理端末に装着することで所定の情報処理の実行を許可する携行型記憶媒体の正当所有者の有無を認証する本人認証システムにおいて、前記ネットワークに接続され、前記正当所有者か否かを認証する認証サーバを備え、前記携行型記憶媒体は、識別情報を記憶する識別情報記憶部と、前記正当所有者の所持する、無線基地局を有する情報伝送系を経由して情報の送受信が可能な携行型通信端末との間で近距離通信を行う第1の近距離通信部とを備え、前記認証サーバは、前記携行型記憶媒体の識別情報に対応付けて、前記携行型記憶媒体の正当所有者の所持する前記携行型通信端末の電子的なアドレス情報、及び固有の認証キー情報が記憶された関連情報記憶部を備え、前記情報処理端末は、前記携行型記憶媒体の装着を検出して前記識別情報を取得し、取得した前記識別情報を含む信号を前記認証サーバに送信する認証要求処理手段と、前記識別情報を含む信号の送信後、前記携行型通信端末及び前記携行型記憶媒体を介して前記認証サーバから認証キー情報を取得すると、取得した前記認証キー情報を前記認証サーバに送信する認証キー中継処理手段とを備え、前記認証サーバは、受信した前記識別情報を含む信号に含まれる前記識別情報に対応する認証キー情報及び電子的なアドレス情報を前記関連情報記憶部から読み出し、読み出した前記認証キー情報を読み出した前記電子的なアドレスに送信する認証キー情報処理手段と、前記認証キー情報の前記電子的なアドレスへの送信後、前記情報処理端末を介して前記認証キー情報を受信すると、前記認証キー情報処理手段によって送信された前記認証キー情報との異同を判定する第1の判定手段とを備えたことを特徴とするものである。
- [0008] また、本発明に係る本人認証方法は、ネットワークに接続された情報処理端末に装着することで所定の情報処理の実行を許可する携行型記憶媒体の正

当所有者の有無を認証する本人認証方法において、前記ネットワークに接続され、前記正当所有者か否かを認証する認証サーバを備え、前記認証サーバの関連情報記憶部には、前記携帯型記憶媒体の識別情報に対応付けて、前記携帯型記憶媒体の正当所有者の所持する前記携帯型通信端末の電子的なアドレス情報、及び固有の認証キー情報が記憶され、前記情報処理端末の認証要求処理手段が、前記携帯型記憶媒体の装着を検出して、前記携帯型記憶媒体に記憶されている識別情報を取得し、取得した前記識別情報を含む信号を前記認証サーバに送信し、前記認証サーバの認証キー情報処理手段が、受信した前記識別情報を含む信号に含まれる前記識別情報に対応する認証キー情報及び電子的なアドレス情報を前記関連情報記憶部から読み出し、読み出した前記認証キー情報を読み出した前記電子的なアドレスに送信し、前記携帯型記憶媒体の近距離通信部が、前記正当所有者の所持する、無線基地局を有する情報伝送系を経由して情報の送受信が可能な携帯型通信端末を介して前記認証キー情報を取得し、前記情報処理端末の認証キー中継処理手段が、前記識別情報を含む信号の送信後、前記携帯型通信端末及び前記携帯型記憶媒体を介して前記認証サーバから認証キー情報を取得すると、取得した前記認証キー情報を前記認証サーバに送信し、前記認証サーバの判定手段が、前記認証キー情報の前記電子的なアドレスへの送信後、前記情報処理端末を介して前記認証キー情報を受信すると、前記認証キー情報処理手段によって送信された前記認証キー情報との異同を判定することを特徴とするものである。

[0009] これらの発明によれば、情報処理端末に装着された携帯型記憶媒体が正当所有者によって所持されていることが認証されると、ネットワークを介して所定の情報処理の実行が可能となる。また、前記ネットワークには、前記正当所有者か否かを認証する認証サーバが接続されている。この認証サーバの関連情報記憶部には、前記携帯型記憶媒体の識別情報に対応付けて、前記携帯型記憶媒体の正当所有者の所持する前記携帯型通信端末の電子的なアドレス情報（例えば電子メールアドレス）、及び固有の認証キー情報が記憶されている。そして、前記情報処理端末の認証要求処理手段によって、前記携帯型

型記憶媒体の装着が検出され、前記携帯型記憶媒体に記憶されている識別情報が取得され、取得された前記識別情報を含む信号が前記認証サーバに送信される。次いで、前記認証サーバの認証キー情報処理手段によって、受信した前記識別情報を含む信号に含まれる前記識別情報に対応する認証キー情報及び電子的なアドレス情報が前記関連情報記憶部から読み出され、読み出された前記認証キー情報が、読み出された前記電子的なアドレスに送信される。次いで、前記携帯型記憶媒体の近距離通信部によって、前記正当所有者の所持する、無線基地局を有する情報伝送系（例えば公衆電話回線）を経由して情報の送受信が可能な携帯型通信端末を介して前記認証キー情報が取得される。次いで、前記情報処理端末の認証キー中継処理手段によって、前記識別情報を含む信号の送信後、前記携帯型通信端末及び前記携帯型記憶媒体を介して前記認証サーバから認証キー情報が取得されると、取得された前記認証キー情報が前記認証サーバに送信される。次いで、前記認証サーバの判定手段によって、前記認証キー情報の前記電子的なアドレスへの送信後、前記情報処理端末を介して前記認証キー情報が受信されると、前記認証キー情報処理手段によって送信された前記認証キー情報との異同が判定される。

[0010] このように、端末使用者に携帯型記憶媒体を付与（貸与を含む）し、この携帯型記憶媒体及び端末使用者の所持する携帯型通信端末を活用して本人認証が可能とされている。すなわち、認証サーバで、端末に装着された携帯型記憶媒体の正当性が判定されたことを条件に、認証キー情報を、認証サーバから携帯型通信端末へ、例えば電子メールで、携帯型通信端末から端末に装着された携帯型記憶媒体へ近距離通信で、そして携帯型記憶媒体を装着している端末から認証サーバへネットワークを経由して送信することで、認証サーバで、送信した認証キーと受信した認証キーとを照合することで、本人認証が可能となる。従って、例えば前記電子メールで送信された認証キーが携帯型通信端末から携帯型記憶媒体に近距離通信によって送信されることで、端末使用者が自己の携帯型記憶媒体と自己の携帯型通信端末の両方を所持していることになり、携帯型記憶媒体の盗用によっても、本人認証処理の不正

なすり抜け操作等がシステムの的に確実に阻止される。

[0011] また、本発明に係る携行型通信端末は、本人認証システムに用いられる前記携帯型通信端末であって、前記第 1 の近距離通信部との間で近距離通信を行う第 2 の近距離通信部と、前記認証サーバから前記認証キー情報を受信すると、該受信した認証キー情報を前記第 2 の近距離通信部から前記第 1 の近距離通信部へ送信する近距離通信制御手段とを備えている。

[0012] 本発明によれば、携行型通信端末に、第 2 の近距離通信部を備え、認証キーを携行型記憶媒体に送信するようにしたので、携行型記憶媒体の盗用によっても、本人認証処理の不正なすり抜け処理が確実に阻止される。

発明の効果

[0013] 本発明によれば、携行型通信端末と携行型記憶媒体との間の近距離通信を介在させることで本人認証処理の不正なすり抜けを効果的に阻止できる。

図面の簡単な説明

[0014] [図1]本発明に係る本人認証システムが適用されるネットワークシステムの概略構成図である。

[図2]端末 1、USBメモリ 2、認証サーバ 4、メールシステム 5 及び携帯電話機 6 の有する機能をそれぞれブロック化した構成図を示すものである。

[図3]USBメモリ 2、端末 1、認証サーバ 4 及び携帯電話機 6 間での本人認証に関する情報の流れの概要を示すシーケンス図である。

[図4]端末 1 の CPU によって実行される USB ポート状態検出の手順の一例を示すフローチャートである。

[図5]認証サーバ 4 の CPU によって実行される認証処理 I の手順の一例を示すフローチャートである。

[図6]認証サーバ 4 の CPU によって実行される認証処理 II の手順の一例を示すフローチャートである。

[図7]認証サーバ 4 の CPU によって実行される認証キー作成処理の手順の一例を示すフローチャートである。

[図8]携帯電話機 6 の CPU によって実行される処理 I の手順の一例を示すフ

ローチャートである。

[図9] 端末1のCPUによって実行されるUSB処理Iの手順の一例を示すフローチャートである。

[図10] 端末1のCPUによって実行されるUSB処理IIの手順の一例を示すフローチャートである。

[図11] 携帯電話機6のCPUによって実行される処理IIの手順の一例を示すフローチャートである。

発明を実施するための形態

[0015] 図1は、本発明に係る本人認証システムが適用されるネットワークシステムの概略構成図である。図1に示すネットワークシステムは、例えば、会員である、消費者や商店乃至は企業等、更には決済を行う1又は複数の金融機関に配置される端末（情報処理端末）1と、これらの各端末1及び端末1間での情報の管理及び保管を統括的に行う管理機関に配設された会員サーバ3とを備える。各端末1及び会員サーバ3はインターネット等のネットワーク7に接続されている。

[0016] 端末1は、一般的にはCPU（Central Processing Unit）を内蔵するパーソナルコンピュータ等で構成されている。端末1内には、例えば、一般的な文書や図形の作成ソフトウェアを利用しての情報の作成、加工、記憶、更に通信用のソフトウェアを利用しての情報の送受信等の一般的な各処理を実行するプログラムファイル（汎用AP（application program）という）と、後述する特定のアプリケーションソフトウェアの実行に関連する処理を行うプログラムファイル（特定APという）とが記憶されている。より具体的には、会員間である消費者、商店及び企業等の端末1には、特定APとして、商品やサービスの売買、見積もり乃至は請求、入出金に関する各書類の作成と通信とを行うソフトウェア、及び後述する認証処理のソフトウェアがインストールされている。すなわち、端末1は、一般的な商取引における決済、例えば業者店舗からの請求書の発行、受領や、購買者側から請求書発行元の契約金融機関の口座への入金（すなわち支払い）指示書、その受領書の発行の

他、電子決済の如何を問わず種々の電子書面での送受信処理を可能とするものである。端末1は、各種書類をテキスト形式の、またバイナリー形式の電子ファイルとして作成可能である。電子ファイルは、例えば会員サーバ3を中継して端末1間で授受される。各金融機関の端末1には、消費者や企業の端末1からの金融的な決済書面に従った決済指示処理（金融機関間での決済処理の指令等）を行う特別アプリケーションソフトウェアもインストールされている。

[0017] また、端末1は、携行可能な記憶媒体（会員用外部記憶媒体）、例えばチップ状のUSB（Universal Serial Bus）メモリ2が装着（接続）可能なUSBポートを有する。記憶媒体としては、IEEE1394ポートを使用したスティック状のハードウェアでもよい。USBメモリ2は、会員に付与されるもので、後述するように所定の情報が記憶可能な記憶部（領域）を有する。また、USBメモリ2は、チップ状の本体の内部等の適所にブルーツース（Blue tooth）等の近距離通信手段を備えている。近距離通信手段は、無線（電波、光）に限定されないが、操作性から無線式が好ましい。近距離通信の方式としては、ブルーツースに限定されず、無線LAN（Local area network）、RFID（Radio Frequency Identification）等でもよい。

[0018] 会員サーバ3は、会員に関する適宜な情報、例えば会員の氏名、名称、メールアドレス、住所等の会員情報等を会員単位で記憶するものである。また、会員サーバ3は、さらに、各会員のファイル送受信履歴やそのファイル類等を管理用に記憶する記憶部を備えている。会員サーバ3は、認証サーバ4としての機能部を備えている。認証サーバ4は、ネットワーク7に接続されており、会員サーバ3と端末1との間で授受されるファイル、すなわちパケットが閲覧可能な状態にある。なお、会員サーバ3と認証サーバ4との関係は、シリアル的な他、パラレル的な接続関係にあってもよく、端末1から会員サーバ3に送信されるパケットが、本発明における認証処理が実現できる範囲において閲覧できる態様であればよい。

[0019] また、本システムは、他の適用例として、秘密情報を作成、保管管理する

、例えば公的機関である団体組織内のＬＡＮに接続された複数の端末１間での情報通信、さらに団体組織外にある端末との間における情報通信・管理体制に適用する例を挙げることができる。団体組織外にある端末との間における情報通信としては、例えば証明書の発行などが想定される。

[0020] 図１において、端末１はプロバイダ（ＩＳＰ）８を介してネットワーク７に接続されている。ＩＳＰ８には、通常、複数の端末１が接続されている。なお、図１には示されていないが、ＩＳＰ８には、各種の情報を提供するＷｅｂサイトを有するサーバも、適宜の数だけ接続されている。また、ＩＳＰ８に接続される端末１には、前述した特定ＡＰがインストールされている会員所有の端末１と、特定ＡＰがインストールされていない通常の端末１’が存在する。特定ＡＰの一部は、認証処理を行うプログラムを有し、認証結果に従って特定ＡＰの実行許可及びその管理を行う。

[0021] また、本ネットワークシステムでは、ＵＳＢメモリ２を使用する会員の正当性、すなわち本人認証を可搬式の携行型通信端末、代表的には電子メールの送受信が可能な携帯電話機６を用いる。電子メールの送受を行うための仕組みとしては、携帯電話会社のメールシステム５が使用される。メールシステム５及び携帯電話機６の構成については、図２を用いて説明する。なお、携行型通信端末６は、携帯電話機６の他、ＰＤＡ（Personal Digital Assistant）でもよい。

[0022] 図２は、端末１、ＵＳＢメモリ２、認証サーバ４、メールシステム５及び携帯電話機６の有する機能をそれぞれブロック化した構成図を示すものである。図２において、端末１は、ＣＰＵから構成される制御部１１を備え、制御部１１にＲＯＭ（Read Only Memory）１２とＲＡＭ（Random Access Memory）１３とが接続されている。制御部１１には、テンキーやマウスなどからなる操作部１４、及びＣＲＴ、液晶又はプラズマディスプレイ等からなり、画像を表示する表示部１５が接続されている。

[0023] ＲＯＭ１２は、端末１の起動（ブート処理）、アプリケーションソフトウェアの読み込みを実行するためのＯＳ（Operating System）やＢＩＯＳ（Bas

ic Input/OutputSystem)等を記憶するOS等記憶部121を少なくとも備えている。

[0024] RAM13は、前述した一般的なアプリケーションソフトウェアがインストールされた汎用AP記憶部131、前述した認証、電子商取引サービス、行政サービス等の処理に関連する特定アプリケーションソフトウェアがインストールされた特定AP記憶部132、汎用APや特定APで作成された、テキストファイルやバイナリーコードで作成されたファイルを格納する作成ファイル記憶部133を少なくとも備えている。作成ファイル記憶部133に記憶されるファイルには、自己が作成したファイルの他、送信、受信したファイルも含まれる。特定APは、予め又は所定の時点で外部記憶媒体を介して取り込まれる。例えば、会員登録する時点で、ネットワーク上の所定のサーバ（会員サーバ3でもよい）から、あるいはハードディスク等の外部記憶媒体からインストールされる。

[0025] 制御部11は、ROM12及びRAM13に記憶されているプログラムがCPUによって実行されることによって、USBメモリ2と通信を行うためのUSB通信処理部111、USBメモリ2が端末1のUSBポートP_oへ装着されているか否かを検出する装着検出部112、USBメモリ2を識別する識別情報（USBID）をUSBメモリ2から取得するUSBID取得部113、認証サーバ4に認証要求信号を送信する認証要求処理部114、USBメモリ2から認証キー情報を取得する認証キー取得部115、認証サーバ4から認証結果の情報を取得し、認証結果に応じた処理を行う認証結果処理部116、指定されたプログラムである汎用AP及び特定APを実行させるプログラム実行処理部117、及びネットワーク7を介して会員サーバ3及び認証サーバ4との間で文書ファイルの送受信、代表的にはTCP/IP（transmission control protocol/internet protocol）規約に沿って形成されたパケットによって文書ファイルの送受信を行うネットワーク通信処理部118として機能する。なお、ネットワーク通信処理部118は、受信パケットを元の文書ファイルに戻したり、送信ファイルをパケットに置換して

送信したりするもので、送信される各パケットのヘッダには、送信元である端末 1 のグローバル I P アドレス、送信先である他の端末及び会員サーバ 3 のグローバル I P アドレスが含まれ、更に端末 1 に装着されている U S B メモリの U S B I D や少なくとも初回における認証キーも含まれるようにしている。

[0026] U S B メモリ 2 は、情報が記憶される構成部 2 0 と、近距離通信を行う構成部である近距離通信送受信部 2 1 とを備えている。情報の記憶を行う構成部 2 0 は、U S B メモリ 2 を識別する U S B I D が記憶された U S B I D 記憶部 2 0 1 と、後述するセッション処理において使用される情報（自己を特定する情報「パスキー：P I N（Personal Identification Number）ともいう」）等が記憶され、また前記セッションで受信した情報が記憶される情報記憶部 2 0 2 とを有する。また、近距離通信送受信部 2 1 は、前述したブルーツース等における電磁波送受用のアンテナを含み、後述するように携帯電話機 6 とブルーツースによる近距離通信を行うものである。近距離通信処理部 2 0 3 は、端末 1 に装着された状態で、端末 1 から所要の信号を受信することで、あるいは所要の制御プログラムを受信することで、近距離通信送受信部 2 1 の動作を制御し、及び前記セッション動作を制御するものである。

[0027] 端末 1 の装着検出部 1 1 2 は、所定のハンドシェイク処理における U S B ポート P o からの応答信号の有無から、U S B メモリ 2 の装着の有無を検出するものである。U S B I D 取得部 1 1 3 は、U S B メモリ 2 が装着されている場合に、U S B I D 記憶部 2 0 1 から U S B I D を読み出して取得するものである。認証要求処理部 1 1 4 は、U S B メモリ 2 が装着された場合に、U S B I D を含む認証要求信号を作成し、所定のパケットに変換してから認証サーバ 4 に送信するものである。

[0028] 認証キー取得部 1 1 5 は、認証要求信号を送信した後、U S B メモリ 2 から認証キーの情報を取得すると、この認証キーを所定のパケットに変換して認証サーバ 4 に送信するものである。認証結果処理部 1 1 6 は、認証サーバ 4 から送信された認証結果を受信し、認証結果が、成功な場合にはプログラ

ム実効処理部 117 による特定 A P のみの実行を許可し、成功でない（失敗の）場合には汎用 A P のみの実行を許可する信号をプログラム実効処理部 117 に出力する。認証サーバ 4 における認証処理は、後述するように、特定 A P の実行によって端末 1 と会員サーバ 3 との間でファイルの送受信（具体的には、会員サーバ 3 を中継して他の端末 1 と文書ファイルの送受信等）が行われている間、継続的に実行される。

[0029] 認証サーバ 4 は、CPU からなる制御部 41、認証処理プログラムが記憶された ROM 42、及び認証用情報が記憶された RAM 43 を備えている。RAM 43 は、各会員に付与された USB メモリ 2 の USB ID と、各会員の所持する携帯電話機 6 の電子メールアドレスと、本人認証のための認証キーが対応付けられて記憶された、USB ID / 携帯電子メールアドレス / 認証キー（以下、関連情報という）記憶部 431 を有する。

[0030] 制御部 41 は、ROM 42 に記憶されているプログラムが CPU によって実行されることによって、端末 1 から送信されてくるパケット内の USB ID や認証キーを読み取るパケット監視部 411、読み取った USB ID の正当性を判定する USB 正当性判定部 412、正当性ありと判定された USB ID に対応する認証キーを、対応する携帯電子メールアドレスに電子メールで送信し、その後、正当性ありと判定された USB ID の送信元である端末 1 から受信した認証キーとの照合（初回認証）を行う第 1 認証処理部 413、初回認証後において端末 1 からパケットを受信する毎に、受信するパケットに含まれる USB ID と初回認証時に取得した USB ID との異同を照合する第 2 認証処理部 414、認証キーを所定のタイミングで変更する認証キー作成部 415、ネットワーク 7 を介して端末 1 との間で文書ファイルの送受信、代表的には TCP / IP プロトコルによって形成されたパケットによって文書ファイルの送受信を行うネットワーク通信処理部 416、及び認証キー情報を電子メールのパケットに変換して所定の携帯電話機 6 に（前記した携帯電話会社のメールシステム 5 を経由して）送信する携帯電子メール通信処理部 417 として機能する。携帯電子メール通信処理部 417 は、いわ

ゆるメールサーバとして機能するもので、送信メールを例えばインターネットメール形式に変換して送信する。

[0031] USB正当性判定部412は、読み取ったUSBIDと関連情報記憶部431に予め記憶されている元情報であるUSBIDのリストとを照合を経て、一致したUSBIDがある場合に、正当性ありと判定するものである。USB正当性判定部412は、一致するUSBIDが発見できなかった場合は、認証キーの認証処理を経るまでもなく、正当なUSBメモリ2ではないとして、正当性なしの情報が、当該USBメモリ2が装着されている端末1に返信されて、以後の通信が遮断等される。

[0032] 本実施形態では、認証処理は、USBメモリ2が端末1に装着されている間、継続して行われる。具体的には、第1認証処理部413は、端末1から送信したUSBIDが正当である場合に、対応する携帯電話機6に送信された認証キーが携帯電話機6、USBメモリ2及び端末1を経由して受信されると両方の認証キーを照合して一致している場合には、当該端末1に認証成功の情報を返信する。一方、両方の認証キーを照合して不一致であった場合には、当該端末1に認証ができない（認証失敗）の情報を返信する。認証失敗の情報は、図略の内蔵カウンタ等で回数をカウントすることで、所定回数まで再トライ（USBメモリ2の装着し直し操作）をガイドする態様として活用し得る。第1認証処理部413による処理は初回の認証処理とされる。

[0033] 第2認証処理部414は、初回の認証処理で認証成功とされると、この初回認証を1回目として例えばRAM43の適所に一旦記憶し、その後において、端末1との間でファイル、すなわちパケットの送受信が行われている間に、当該端末1から受信したパケット内のヘッダに含まれるUSBIDが初回認証処理時に取得したUSBIDと一致しているか否かの照合を行うものである。照合の結果が一致していれば、2回目以降の認証が成立したとして、通信を継続させ、逆に、2回目以降のいずれかの段階での認証処理において、一致しなくなった場合には、USBメモリ2が途中で差し替えられたり、その他の不正行為があったりを見なして、当該端末1との通信を遮断する

等する。

- [0034] 認証キー作成部 4 1 5 は、USBメモリ 2 が端末 1 に装着されて会員による所要の処理が終了してから、次回に装着されるまでの間に、当該USBIDに対応する情報のうち、認証キーのみを変更するものである。認証キーの変更は、USBメモリ 2 が端末 1 に装着され、USBIDが読み取られたことに応答して変更してもよいし、その後であって、少なくとも次回に当該USBメモリ 2 がいずれかの端末 1 に装着されるまでの間に変更されればよい。認証キーの変更は、乱数発生器を利用する等して無作為に変更されるのが好ましい。認証キーの更新は、関連情報記憶部 4 3 1 の対応するUSBIDに対応する現認証キーを書き換えることで行われる。
- [0035] メールシステム 5 は、情報伝送系として機能するもので、ISP 8 を介してネットワーク 7 に接続されており、情報処理部 5 1 と、所要数の無線式の基地局 5 2 を有する。基地局 5 2 は、アンテナを有し、携帯電話機 6 との間で電波の送受信を行う送受信部である。メールシステム 5 は、負荷分散のため所要数台設けてもよい。同様に基地局も通話エリアを拡充する目的で所要数だけ配設されている。
- [0036] 情報処理部 5 1 は、携帯電話機 6 で送受される電子メールのフォーマット及びプロトコルとインターネット上を伝送されて認証サーバ 4 に送受される電子メールのフォーマット及びプロトコルとの間でのそれぞれ変換を行うメールゲートウェイ 5 1 1、電子メールの送受を制御する携帯電子メールサーバ 5 1 2、及び送受する電子メールを一時的に保存するメールボックス 5 1 3 を有する。
- [0037] 携帯電話機 6 は、本体に設けられ、電波の送受信を行うアンテナ 6 0 と、本体内に設けられ、CPUから構成された制御部 6 1 とを有する。制御部 6 1 には、通常の通話処理や電子メール送受信処理の他、本人認証処理のための近距離セッション通信、認証キー受信、セッション結果報告のための各種制御プログラムが記憶されたROM 6 2、処理情報である送信情報及び受信情報、及び認証サーバの電子メールアドレス、対応するUSBメモリ 2 を特

定する情報であるパスキーその他の情報が格納されるRAM 63が接続されている。また、携帯電話機6の本体表面適所には、テンキー等各種機能キーから構成される操作部64と、処理情報や受信情報を表示する液晶パネル等の表示部65とが配設されている。近距離通信送受信部66は、前述したブルーーツース等における電磁波送受用のアンテナを含み、後述するようにUSBメモリ2とブルーーツースによる近距離通信を行うものである。

[0038] 制御部61は、ROM 62に記憶されている制御プログラムがCPUによって実行されることによって、近距離通信送受信部66の動作を制御し、及び前記セッション動作を制御する近距離通信処理部611、USB接続状態監視部612、認証キー取得部613、携帯電子メール通信処理部614、及び計時用のタイマ615を有する。

[0039] 近距離通信処理部611は、認証サーバ4から送信された認証キーを受信すると、USBメモリ2との間で所定のセッションを行うための信号を送信し、送信した信号に対して返答信号が受信されると、セッションを開始して、認証キーを送信すると共に、その後はセッションのための信号を継続的にやり取りするものである。近距離通信処理部611及び近距離通信処理部203によるセッションは、USBメモリ2と携帯電話機6とが、互いの通信範囲である近距離、例えば1m（メートル）以内にある場合、USBメモリ2が端末1から抜かれるまで継続される。なお、光学式の場合は、互いに送受波面が対向し、かつ所定近距離に配置される必要がある。

[0040] USB接続状態監視部612は、USBメモリ2の近距離通信処理部203との間で所定のセッションを行うことで、端末1に装着された状態のUSBメモリ2の近傍に、要するに端末1の近傍に携帯電話機6が存在するか否かを判断するものである。すなわち、USB接続状態監視部612は、近距離通信送受信部21との間のセッションが発生しなければ、端末1の近傍に元々携帯電話機6は存在しないと判断し、またセッションが途中で途切れたら、途中で携帯電話機6が端末1から遠ざかったと判断し、いずれも後述するように異常終了とする。一方、USB接続状態監視部612は、USBメ

メモリ 2 が端末から抜かれてセッションが終了した場合には、携帯電話機 6 が最後まで端末 1 の近傍にあったと判断し、異常終了とはしない。セッションが最初から、あるいは途中で途切れた場合、携帯電話機 6 は、認証処理の失敗を示す信号を認証サーバ 4 に送信する。USB 接続状態監視部 612 によるセッションの継続性の監視（判断）は、例えば十数秒乃至は 1 分程度の内の所要の間隔をタイマ 615 で計時することで実行される。

[0041] 認証キー取得部 613 は、認証サーバ 4 から電子メールシステム 5 を経由して送信される認証キーを受信し、近距離通信処理部 611 に渡すものである。携帯電子メール通信処理部 614 は、認証キーの情報やセッションの失敗を示す情報等を電子メールの形で認証サーバ 4 との間で送受信するものである。

[0042] 図 3 は、USB メモリ 2、端末 1、認証サーバ 4 及び携帯電話機 6 間での本人認証に関する情報の流れの概要を示すシーケンス図である。

[0043] 今、自己の USB メモリ 2 及び自己の携帯電話機 6 を所持する会員が自宅の端末 1 で、あるいは他人、例えば公共設備や店舗に備え付けの端末 1 で、何らかの申請、あるいは商取引を行う場合を想定する。

[0044] 会員は、自己の USB メモリ 2 を対象である端末 1 の USB ポート P o に装着する。この装着によって、端末 1 と USB メモリ 2 との間でハンドシェイク処理が実行される。次いで、USB ID が USB メモリ 2 から端末 1 へ読み取られる。端末 1 は取得した USB ID を含む認証要求信号を生成し、送信用のパケットに変換して認証サーバ 4 に送信する。これにより、初回の認証処理が開始される。認証サーバ 4 は、USB ID の正当性をチェックし、正当であれば、USB ID に対応する認証キーに対応する携帯電話機 6 に電子メールで送信する。携帯電話機 6 は、受信した認証キーを近距離通信で USB メモリ 2 に送信する。そして、USB メモリ 2 で受信された認証キーは端末 1 を介して認証サーバに送信される。ここで、認証サーバ 4 は、携帯電話機 6 に送信した認証キーと、端末 1 から受信した認証キーとの異同を判定し、一致すれば認証成功と判断し、一致しなければ認証失敗と判定する。

認証結果は端末 1 に送信される、認証結果が認証失敗であった場合、その旨は USB メモリ 2 を経て携帯電話機 6 に送信される。これにより、近距離通信が切断される。また、会員には、再トライが可能となる。

[0045] 初回の認証処理が成功すると、その後は、当該端末 1 と認証サーバ 4 との間で（具体的には認証サーバ 4 を介して端末 1 と会員サーバ 3 との間で）所要のファイルがパケットに変換されて送受される。そこで、端末 1 から認証サーバ 4 に送信されるパケットのヘッダ内に書き込まれている USB メモリ 2 の USB ID を含めるようにして、USB メモリ 2 が端末 1 に装着されている間、2 回目以降の認証処理を継続的に行うようにしている。

[0046] すなわち、認証サーバ 4 は、当該端末 1 から送信されるパケットのヘッダ情報を監視し、その中から USB ID を抽出する。そして、初回の認証処理時に端末 1 から取得した USB ID との異同を照合する。ここで、認証が失敗すると、その旨が端末 1 に送信される。なお、初回の認証処理の成功によって稼働される特定 AP の処理には、通信以外にも、単に文書作成などがあるが、パケットの送受以外の処理の間は、2 回目以降の認証は中断していることになる。また、この中断期間であっても、定期的乃至は周期的に USB ID を含む認証用のパケットを作成し、認証サーバ 4 に送信する態様としてもよい。

[0047] 図 4 は、端末 1 の CPU によって実行される USB ポート状態検出の手順の一例を示すフローチャートである。まず、USB ポート P o に対して周期的にハンドシェイク信号の送信が行われて、USB ポート P o の状態が判断される（ステップ S 1）。このとき、USB ポート P o に USB メモリ 2 が装着されていれば、ハンドシェイク信号に応答して、応答信号が返信される一方、USB メモリ 2 が装着されていなければ、応答信号は返信されず、本フローを抜ける。次いで、応答信号が返信されてくると、USB メモリ 2 を含む何らかのチップが装着されているとして、特定 AP 内の、ある専用 AP が起動される。専用 AP は、装着チップが USB メモリ 2 であるか否かの判断と、USB メモリ 2 である場合に、内部の情報を読み出す処理を実行させ

る通信アプリケーションソフトウェアを起動させる。

[0048] ステップS 1において、USBメモリ2から応答があると、USBID記憶部201からUSBIDの読み取りが行われる（ステップS 3）。USBIDが取得されると、USBIDを含む認証要求信号（パケット）が作成される（ステップS 5）。次いで、作成された認証要求信号が認証サーバ4に送信される（ステップS 7）。送信が終了すると、認証サーバ4からのパケットの受信を待つ待機モードに移行する（ステップS 9）。

[0049] なお、USBポート状態検出処理は、特定APに代えて、汎用APで行ってもよい。そして、USBポートP oにチップの装着が検出された後に、特定APへ処理を受け渡すようにしてもよい。

[0050] 図5は、認証サーバ4のCPUによって実行される認証処理Iの手順の一例を示すフローチャートである。認証処理Iとは、初回の認証の処理をいう。

[0051] まず、端末1から認証要求信号が受信されたか否かが判断される（ステップ# 1）。認証要求信号が受信されていなければ、本フローを抜ける。一方、認証要求信号が受信されたのであれば、パケット内からUSBIDが読み取られる（ステップ# 3）。次いで、読み取られたUSBIDと同一の情報があるか否かについて関連情報記憶部431のUSBIDリストが検索され、正当性の有無が判断される（ステップ# 5）。リスト中に同一の情報があれば、正当性ありと判断される（ステップ# 7でY）。一方、同一の情報がないければ、正当性なしと判断されて（ステップ# 7でN）、本フローを抜ける。

[0052] 正当性ありと判断された場合、関連情報記憶部431から、現に正当性ありと判断されたUSBIDに対応した、携帯電話機6の電子メールアドレスが抽出され（ステップ# 9）、さらに当該USBIDに対応した認証キーが抽出される（ステップ# 11）。そして、認証サーバ4の携帯電子メール通信処理部417によって、抽出された電子メールアドレスに、抽出された認証キーが送信される（ステップ# 13）。

- [0053] 次いで、所定時間内に、当該端末 1 からのパケットが受信されたか否かが判断される（ステップ# 15）。所定時間とは、ステップ# 13で認証サーバ4から出力された認証キーの情報が、携帯電話機6、USBメモリ2、端末1を経由して戻って来るに要する時間より多少大きめに設定された時間で、制御部11内の図略のタイマによって計時される。所定時間内に認証キーが（当該認証キーの送信元である端末1から）取得されると（ステップ# 17）、ステップ# 13で送信した認証キーとステップ# 15で受信した認証キーとの異同の照合が行われる（ステップ# 19）。
- [0054] ここで、送信した認証キーと受信した認証キーとが不一致であると（ステップ# 21でN）、認証失敗信号が当該端末1に返信される（ステップ# 23）。この認証失敗信号は、認証の再トライを所要回数だけ促すものとして扱われる。すなわち、会員は、認証失敗信号が当該端末1の表示部15に表示される等によって、正しいUSBメモリ2かを再確認し、かつ端末1のUSBポートP_oに対して差し直し操作を促す。なお、所要回数は、認証失敗信号を図略のカウンタでカウントし、設定回数値と大小比較することで監視可能である。
- [0055] また、ステップ# 21で、送信した認証キーと受信した認証キーとが一致している場合、認証成功信号が当該端末1に送信され（ステップ# 25）、さらに当該端末1との通信の許可を行う（ステップ# 27）。
- [0056] 図6は、認証サーバ4のCPUによって実行される認証処理IIの手順の一例を示すフローチャートである。認証処理IIとは、2回目以降での認証の処理をいう。初回の認証処理が成功すると、そのときのUSBIDが、当該端末1（IPアドレス）と対応付けて認証サーバ4のRAM43の適所に一時的に保存され、さらに特定APが実行されて、当該端末1と認証サーバ4（具体的には会員サーバ3）間で、所要のパケットの授受が可能となる。そして、当該端末1から送信されたパケットが受信されたか否かの判断が、当該端末1のIPアドレスに基づいて行われる（ステップ# 41）。
- [0057] ステップ# 41においてパケットが受信されたのであれば、当該パケット

のヘッダからUSBIDの読み取りが行われる（ステップ#43）。そして、当該端末1における初回の認証時における正当性判断で用いられたUSBID（最初のUSBIDという）と今回のパケットから読み出されたUSBIDとの異同の照合が行われる（ステップ#45）。最初のUSBIDと今回のUSBIDとが一致していると、認証成功として、本フローを抜ける。一方、最初のUSBIDと今回のUSBIDとが不一致である場合、当該端末1との特定APによる通信が遮断され（ステップ#51）、さらに、当該端末1に認証失敗信号が送信される（ステップ#53）。

[0058] なお、ステップ#41で当該端末1からパケットが受信されていない場合、当該端末1に対応する携帯電話機6からセッション失敗の電子メールが受信されたか否かが判断される（ステップ#49）。セッション失敗の電子メールが受信されていない場合は、本フローを抜け、逆にセッション失敗の電子メールが受信されていると、ステップ#51に進む。

[0059] 図7は、認証サーバ4のCPUによって実行される認証キー作成処理の手順の一例を示すフローチャートである。まず、認証キーの作成時点か否かが判断される（ステップ#61）。認証キーの作成時点とは、USBメモリ2が端末1から抜かれてから、次回にUSBメモリ2が端末1（前回装着された端末1との異同は問わない）に装着され、さらに抜かれるまで間の、ある予め設定された時点をいう。例えば、端末1から認証サーバ4に最初のUSBIDが受信された時点とか、USBメモリ2が端末1から抜かれた時点とかでもよい。

[0060] 認証キー作成時点でなければ、本フローを抜ける。一方、認証キー作成時点であれば、無作為に認証キーが作成される（ステップ#63）。次いで、関連情報記憶部431内の対応するUSBID又は携帯電子メールアドレスに対して、作成した認証キーが対応付けされて更新記憶される（ステップ#65）。このように、認証キーをOne time passwordと同様に毎回かつ無作為に変更することで、仮に盗聴されても次回では無用化できる。

[0061] 図8は、携帯電話機6のCPUによって実行される処理Iの手順の一例を

示すフローチャートである。まず、認証サーバ4から認証キーが電子メールで受信されたか否かが判断され（ステップT1）、認証キーが受信されたのでなければ、本フローを抜ける。一方、認証キーが受信されたのであれば、USBメモリ2との間でのセッションに先だって接続コマンドが前記パスキーを有するUSBメモリ2に送信される（ステップT3）。すなわち、携帯電話機6は、認証サーバ4の電子メールアドレスを記憶しておき、当該電子メールアドレスから所定の情報、すなわち、ここでは認証キーの情報が受信されると、自動的にセッションのための接続コマンドの送信処理に移行する。なお、自動的にセッションに移行する態様に代えて、携帯電話機6の所持者に近距離通信によるセッション開始の操作を指示する指示情報を送信するようにしてもよい。

[0062] また、携帯電話機6のRAM63には、対応するUSBメモリ2を特定するためのパスキーがペアリング処理によって予め記憶されている。ペアリング処理とは、セッションの事前処理であって、対応関係にある携帯電話機6とUSBメモリ2とを所定の情報、例えばパスキーで紐付けする処理である。

[0063] 次いで、接続が成功したか否かが判断され（ステップT5）、成功すると、セッションが行われることになる。例えば、機器の接続/認証/暗号化を行うためのプロファイルであるGAP（Generic Access Profile）を使用することで、パスキーの情報を利用して接続を行う。そして、接続されたら、データ転送を行うためのプロファイルであるFTP（File Transfer Profile）を使用してデータ転送を行う。

[0064] 次いで、上記のようにしてセッション処理が開始され、まず認証キーがペアリング先のUSBメモリ2に送信される（ステップT7）。続いて、当該USBメモリ2から応答信号が受信されたか否かが判断され（ステップT9）、受信されたのであれば、予め設定された一定時間（例えば十数秒～1分程度内の所与の時間）が経過したか否かが判断される（ステップT11）。一定時間が経過すると、応答要求信号が送信され（ステップT13）、次い

で当該USBメモリ2から応答信号が受信されたか否かが判断される（ステップT15）。応答信号が受信されたのであれば、当該USBメモリ2が端末1から抜かれたか否かが、例えば抜かれた旨の信号の受信の有無によって判断される（ステップT17）。当該USBメモリ2が端末1から抜かれたのであれば、本フローを終了する。一方、当該USBメモリ2が端末1から抜かれていなければ、ステップT11に戻る。

[0065] また、ステップT5でペアリング相手が発見できず、ステップT9、T15で応答信号が受信されなければ、USBメモリ2を装着する者が対応する携帯電話機6を所有しておらず、あるいは携帯電話機6がUSBメモリ2から所定の近距離以上離れたと見なすなどして、セッション開始での接続失敗又はセッション中での切断を示すセッション失敗信号が電子メールで認証サーバ4に送信される（ステップT19）。

[0066] 図9は、端末1のCPUによって実行されるUSB処理Iの手順の一例を示すフローチャートである。なお、USB処理I及び後述するUSB処理IIは、USBメモリ2内にCPUを内蔵し、USB処理I、IIの処理プログラムを情報記憶部202に記憶した態様で実行されるようにしてもよい。

[0067] まず、携帯電話機6からセッションのための信号、ここでは前記接続コマンドが受信されたかどうか判断される（ステップQ1）。前記コマンドが受信されていないならば、本フローを抜ける。一方、前記信号が受信されていると、パスキーが応答信号として返信される（ステップQ3）。続いて、認証キーの受信の有無が判断され（ステップQ5）、認証キーが受信されていないならば、本フローを抜ける。一方、認証キーが受信されていると、受信した認証キーが端末1に送出される（ステップQ7）。

[0068] 次いで、携帯電話機6から、セッションのための応答要求信号が受信されたか否かが判断される。信号が受信されていないならば、本フローを抜ける。一方、信号が受信されていると、応答信号が送信される（ステップQ11）。次いで、USBメモリ2が端末1から抜かれたか否かが判断され（ステップQ13）、抜かれていなければ、ステップQ9に戻って、応答要求信号の

受信の有無が判断される。このようにして、USBメモリ2が端末1から抜かれるまで、セッションが継続される。

[0069] 図10は、端末1のCPUによって実行されるUSB処理IIの手順の一例を示すフローチャートである。まず、端末1から認証失敗信号が受信されたか否かが判断され（ステップQ21）、端末1から認証失敗信号が受信されていなければ、本フローを抜ける。一方、端末1から認証失敗信号が受信されていると、この信号に対応して認証失敗信号が携帯電話機6に送信される（ステップQ23）。

[0070] 図11は、携帯電話機6のCPUによって実行される処理IIの手順の一例を示すフローチャートである。まず、USBメモリ2から認証失敗信号を受信したか否かが判断される（ステップT31）。認証失敗信号が受信されなければ、本フローを抜ける。一方、認証失敗信号が受信されたのであれば、当該USBメモリ2との近距離通信の切断コマンドが発行される（ステップT33）。この切断コマンドによって、セッション相手である携帯電話機6とUSBメモリ2との近距離通信が遮断される。

[0071] なお、本発明は、以下の態様が採用可能である。

[0072] （1）特定AP記憶部132に記憶される特定アプリケーションソフトウェアは会員サーバ3等に格納されており、会員サーバ3からダウンロードされ、インストールされる態様とすることが好ましい。これにより、端末1にインストールされる特定APを汎用APを分断して実行させることが可能となる。

[0073] （2）USBメモリ2は内部に電源用二次電池を備える構成でもよいし、あるいは端末1に装着（接続）された状態で端末1の電源から電源供給を受けて稼働する態様でもよい。

[0074] （3）認証サーバ4は、認証キーの異同の照合において認証失敗と判定した場合、当該端末に対して認証失敗信号を送信して、当該端末1の特定APの動作自体を禁止する等の態様を採用してもよいし、あるいは認証失敗信号によって認証サーバ4において当該端末1との間のパケットの送受信を禁止す

る態様でもよい。

[0075] (4) 本実施形態では、認証サーバ4は、端末1から受信したUSBIDに対して正当性ありと判断すると(ステップ#7)、認証キーを対応する携帯電話機6に電子メールで送信する(ステップ#13)態様としたが、以下の態様でもよい。すなわち、例えばiモード(登録商標)対応の携帯電話機6にiアプリ(登録商標)のような、ネットワーク(情報伝送系)上の所定のサーバ(認証サーバ4)との間で所要のアプリケーションサービスを行う、アプリケーションプログラムを、認証サーバ4あるいは他の所定のサイトから、予めダウンロードしておき(あるいは必要に応じてその都度ダウンロードして)、所定の情報の授受を行う。また、このアプリケーションサービスを実行するプログラムは、待ち受け機能を利用して、例えば数秒~数十秒での所定周期で認証キー送信要求信号を認証サーバ4に送信すると共に、この認証キー送信要求信号に応答して、(USBIDの受信済み为前提として)認証サーバ4から送信されてきた認証キーを受信するようにする。一方、認証サーバ4は、iアプリ(登録商標)のサービスに対応可能な情報送受信部を備える。この情報送受信部は、携帯電話機6から認証キー送信要求信号を受信すると、それに応答して当該携帯電話機6の電子的なアドレスに認証キーを送信するようにしている。なお、この態様では、記憶部431は、USBID/携帯電話機6の電子的なアドレス/認証キーの各情報を関連付けて記憶しておく。また、認証サーバ4は、前記認証キー送信要求信号の送信元の携帯電話機6の電子的なアドレスの正当性を、前記記憶部431の記憶内容のUSBIDと照合することで判断するようにしてもよい。

[0076] 具体的には、以下の手順で行えばよい。USBメモリ2が端末1に装着されると、USBメモリ2の所持者は携帯電話機6を所定のiアプリ(登録商標)のモードへの起動操作を行う(常時このモード状態にある場合には、起動操作不要)。認証サーバ4は、USBIDを受信済みであることを判断し、次いで、前述の正当性判断のための照合を行った後、正当であれば、認証キー送信要求信号に応答して認証キーを当該携帯電話機6に送信する。認証

サーバ4は、認証キーの送信を（正常受信を条件に）1回行う。携帯電話機6は、認証キーを受信すると、省電のために本モードをスリープするようにしてもよい。このように、認証キーの送受信処理は、電子メールに限らず、携帯電話会社に応じた他のアプリケーションサービスを利用しても可能である。

[0077] 以上のとおり、本発明は、ネットワークに接続された情報処理端末に装着することで所定の情報処理の実行を許可する携行型記憶媒体の正当所有者の有無を認証する本人認証システムにおいて、前記ネットワークに接続され、前記正当所有者か否かを認証する認証サーバを備え、前記携行型記憶媒体は、識別情報を記憶する識別情報記憶部と、前記正当所有者の所持する、無線基地局を有する情報伝送系を経由して情報の送受信が可能な携行型通信端末との間で近距離通信を行う第1の近距離通信部とを備え、前記認証サーバは、前記携行型記憶媒体の識別情報に対応付けて、前記携行型記憶媒体の正当所有者の所持する前記携行型通信端末の電子的なアドレス情報、及び固有の認証キー情報が記憶された関連情報記憶部を備え、前記情報処理端末は、前記携行型記憶媒体の装着を検出して前記識別情報を取得し、取得した前記識別情報を含む信号を前記認証サーバに送信する認証要求処理手段と、前記識別情報を含む信号の送信後、前記携行型通信端末及び前記携行型記憶媒体を介して前記認証サーバから認証キー情報を取得すると、取得した前記認証キー情報を前記認証サーバに送信する認証キー中継処理手段とを備え、前記認証サーバは、受信した前記識別情報を含む信号に含まれる前記識別情報に対応する認証キー情報及び電子的なアドレス情報を前記関連情報記憶部から読み出し、読み出した前記認証キー情報を読み出した前記電子的なアドレスに送信する認証キー情報処理手段と、前記認証キー情報の前記電子的なアドレスへの送信後、前記情報処理端末を介して前記認証キー情報を受信すると、前記認証キー情報処理手段によって送信された前記認証キー情報との異同を判定する第1の判定手段とを備えることが好ましい。

[0078] この構成によれば、認証サーバで、端末に装着された携行型記憶媒体の正

当性が判定されたことを条件に、認証キー情報を、認証サーバから携行型通信端末へ、例えば電子メールで、携行型通信端末から端末に装着された携行型記憶媒体へ近距離通信で、そして携行型記憶媒体を装着している端末から認証サーバへネットワークを経由して送信することで、認証サーバで、送信した認証キーと受信した認証キーとを照合することで、本人認証が可能となる。従って、電子メール等で送信された認証キーが携行型通信端末から携行型記憶媒体に近距離通信によって送信されることで、端末使用者が自己の携行型記憶媒体と自己の携行型通信端末の両方を所持していることになり、携行型記憶媒体の盗用によっても、本人認証処理の不正なすり抜け操作等がシステムの的に確実に阻止される。

[0079] また、前記認証サーバは、受信した前記識別情報を含む信号に含まれる前記識別情報と前記関連情報記憶部に予め記憶されている識別情報との一致を判定する識別情報一致判定手段を備えることが好ましい。この構成によれば、携行型記憶媒体の正当性が判定されるので、携行型記憶媒体に対する認証を確実なものとすることができる。

[0080] また、前記認証サーバは、前記判定の結果を前記認証キー情報の送信元の情報処理端末に送信する判定結果処理手段を備えることが好ましい。この構成によれば、判定の結果、認証が失敗した場合には、その旨が情報処理端末に送信されるので、情報処理端末においても、認証失敗に対する対応処理、例えば認証サーバへの情報の送信処理等を禁止する等の対応が可能となる。

[0081] また、前記情報処理端末は、前記携行型記憶媒体の装着状態を監視し、非装着が検知されると、前記認証サーバとの通信を中止する装着監視手段を備えることが好ましい。この構成によれば、情報処理端末での所定の情報処理を行う間、携行型記憶媒体を情報処理端末に継続して装着して、装着状態の監視をクリアする必要があるため、初回の認証時のみ装着すれば済む場合に比して、不正使用を困難なものとすることができる。

[0082] また、前記情報処理端末は、前記携行型記憶媒体が装着されている間、前記所定の情報処理が実行可能な状態にされるものであり、前記認証サーバは

、前記情報処理端末からの前記識別情報を含む信号の受信が初回か否かを監視し、前記２回目以降の場合、前記識別情報を含む信号に含まれる前記識別情報が１回目に受信された前記識別情報と一致するか否かを判断する第２の判定手段を備えることが好ましい。この構成によれば、初回の本人認証が成功した場合には、２回以降では識別情報のみのチェックで済ますようにしたので、認証キー情報を、認証動作の都度、電子メール、携行型通信端末、携行型記憶媒体を経由させるといった手間を省き、かつ盗聴機会を少なくすることができる。

[0083] また、前記認証キー情報処理手段による前記認証キー情報の送信毎に異なる認証キー情報を作成する認証キー情報作成手段を備えることが好ましい。この構成によれば、仮に認証キー情報を盗聴されたとしても、次の情報処理端末の使用に際しては無益な情報となるので、盗用が阻止できる。

[0084] また、認証キー情報作成手段は、無作為に前記認証キー情報を作成することが好ましい。この構成によれば、盗聴された認証キー情報から変更後の情報を予想できないため、信頼性の高い認証キー情報となる。

[0085] また、前記携行型通信端末は、前記携行型通信端末は、前記無線基地局との間で電磁波を媒介として前記情報の送受信を行う携帯電話機であることが好ましい。この構成によれば、携帯電話機は多数の者が所持しているツールであるため、本発明を汎用性の高いものとすることが可能となる。

[0086] また、前記第１の近距離通信部は、電磁波を媒介とした無線通信装置を備えたものであることが好ましい。この構成によれば、電磁波であれば、例えば光を用いた態様に比して携帯電話機の送受光面を合わせるために向きを調整する等の操作が不要となる。

[0087] また、請求項１～８のいずれかに記載の本人認証システムに用いられる前記携帯型通信端末であって、前記第１の近距離通信部との間で近距離通信を行う第２の近距離通信部と、前記認証サーバから前記認証キー情報を受信すると、該受信した認証キー情報を前記第２の近距離通信部から前記第１の近距離通信部へ送信する近距離通信制御手段とを備えることが好ましい。この

構成によれば、携行型通信端末に、第2の近距離通信部を備え、認証キーを携行型記憶媒体に送信するようにしたので、携行型記憶媒体の盗用によっても、本人認証処理の不正なすり抜け処理が確実に阻止される。

[0088] また、前記近距離通信制御手段は、対応する携行型記憶媒体を特定するパスキーが予め記憶されており、前記パスキーを用いて、前記認証サーバから受信した前記認証キー情報を前記対応する携行型記憶媒体の第1の近距離通信部へ送信することが好ましい。この構成によれば、仮に周囲に複数の携行型記憶媒体が存在していても、特定された1つの携行型記憶媒体にしか認証キーが送信されないため、高い秘匿性が保持できる。

[0089] また、前記認証サーバの電子的なアドレスを記憶するアドレス記憶部と、前記第1の近距離通信部との間での近距離通信の状態を監視し、近距離通信が途絶えた場合、その旨の情報を前記認証サーバの電子的なアドレスに送信する近接通信監視手段とを備えることが好ましい。この構成によれば、携行型通信端末と携行型記憶媒体との距離が相対的に近距離範囲外となった場合に、認証サーバにその旨が連絡されるので、正当者でない可能性の高い場合には所定の情報処理を禁止する等の措置を採ることができる。

符号の説明

- [0090] 1 端末（情報処理端末）
- 1 1 制御部
- 1 1 1 USB通信処理部
- 1 1 2 装着検出部（装着監視手段）
- 1 1 3 USBID取得部
- 1 1 4 認証要求処理部（認証要求処理手段）
- 1 1 5 認証キー取得部（認証キー中継処理手段、回数監視手段）
- 1 1 6 認証結果処理部
- 1 1 7 プログラム実行処理部
- 1 1 8 ネットワーク通信処理部
- 1 3 2 特定AP記憶部

- 2 USBメモリ（携行型記憶媒体）
 - 201 USBID記憶部（識別情報記憶部）
 - 202 情報記憶部
 - 203 近距離通信処理部（第1の近距離通信部）
 - 21 近距離通信送受波部（第1の近距離通信部）
- 3 会員サーバ
- 4 認証サーバ
 - 41 制御部
 - 411 パケット監視部
 - 412 USB正当性判定部（識別情報一致判定手段）
 - 413 第1認証処理部（第1の判定手段、判定結果処理手段）
 - 414 第2認証処理部（第2の判定手段、判定結果処理手段）
 - 415 認証キー作成部（認証キー情報作成手段）
 - 416 ネットワーク通信処理部
 - 417 携帯電子メール通信処理部（認証キー情報処理手段）
 - 431 USBID／携帯電子メールアドレス／認証キー記憶部（関連情報記憶部）
- 5 電子メールシステム（情報伝送系）
- 6 携帯電話機（携行型通信端末）
 - 61 制御部
 - 611 近距離通信処理部（近距離通信制御手段）
 - 612 USB接続状態監視部（近接通信監視手段）
 - 613 認証キー取得部
 - 614 携帯電子メール通信処理部
 - 615 タイマ
 - 63 RAM（アドレス記憶部）
 - 66 近距離通信送受波部（第2の近距離通信部）
- 7 ネットワーク

請求の範囲

[請求項1]

ネットワークに接続された情報処理端末に装着することで所定の情報処理の実行を許可する携帯型記憶媒体の正当所有者の有無を認証する本人認証システムにおいて、

前記ネットワークに接続され、前記正当所有者か否かを認証する認証サーバを備え、

前記携帯型記憶媒体は、

識別情報を記憶する識別情報記憶部と、

前記正当所有者の所持する、無線基地局を有する情報伝送系を経由して情報の送受信が可能な携帯型通信端末との間で近距離通信を行う第1の近距離通信部とを備え、

前記認証サーバは、

前記携帯型記憶媒体の識別情報に対応付けて、前記携帯型記憶媒体の正当所有者の所持する前記携帯型通信端末の電子的なアドレス情報、及び固有の認証キー情報が記憶された関連情報記憶部を備え、

前記情報処理端末は、

前記携帯型記憶媒体の装着を検出して前記識別情報を取得し、取得した前記識別情報を含む信号を前記認証サーバに送信する認証要求処理手段と、

前記識別情報を含む信号の送信後、前記携帯型通信端末及び前記携帯型記憶媒体を介して前記認証サーバから認証キー情報を取得すると、取得した前記認証キー情報を前記認証サーバに送信する認証キー中継処理手段とを備え、

前記認証サーバは、

受信した前記識別情報を含む信号に含まれる前記識別情報に対応する認証キー情報及び電子的なアドレス情報を前記関連情報記憶部から読み出し、読み出した前記認証キー情報を読み出した前記電子的なアドレスに送信する認証キー情報処理手段と、

前記認証キー情報の前記電子的なアドレスへの送信後、前記情報処理端末を介して前記認証キー情報を受信すると、前記認証キー情報処理手段によって送信された前記認証キー情報との異同を判定する第 1 の判定手段とを備えたことを特徴とする本人認証システム。

[請求項2] 前記認証サーバは、受信した前記識別情報を含む信号に含まれる前記識別情報と前記関連情報記憶部に予め記憶されている識別情報との一致を判定する識別情報一致判定手段を備えたことを特徴とする請求項 1 記載の本人認証システム。

[請求項3] 前記認証サーバは、前記判定の結果を前記認証キー情報の送信元の情報処理端末に送信する判定結果処理手段を備えたことを特徴とする請求項 1 又は 2 に記載の本人認証システム。

[請求項4] 前記情報処理端末は、前記携帯型記憶媒体の装着状態を監視し、非装着が検知されると、前記認証サーバとの通信を中止する装着監視手段を備えたことを特徴とする請求項 1 ～ 3 のいずれかに記載の本人認証システム。

[請求項5] 前記情報処理端末は、前記携帯型記憶媒体が装着されている間、前記所定の情報処理が実行可能な状態にされるものであり、

前記認証サーバは、

前記情報処理端末からの前記識別情報を含む信号の受信が初回か否かを監視し、前記 2 回目以降の場合、前記識別情報を含む信号に含まれる前記識別情報が 1 回目に受信された前記識別情報と一致するか否かを判断する第 2 の判定手段を備えたことを特徴とする請求項 1 ～ 4 のいずれかに記載の本人認証システム。

[請求項6] 前記認証キー情報処理手段による前記認証キー情報の送信毎に異なる認証キー情報を作成する認証キー情報作成手段を備えたことを特徴とする請求項 1 ～ 5 のいずれかに記載の本人認証システム。

[請求項7] 認証キー情報作成手段は、無作為に前記認証キー情報を作成することを特徴とする請求項 6 に記載の本人認証システム。

- [請求項8] 前記携帯型通信端末は、前記無線基地局との間で電磁波を媒介として前記情報の送受信を行う携帯電話機であることを特徴とする請求項 1 ～ 7 のいずれかに記載の本人認証システム。
- [請求項9] 前記第 1 の近距離通信部は、電磁波を媒介とした無線通信装置を備えたものであることを特徴とする請求項 8 に記載の本人認証システム。
- [請求項10] 請求項 1 ～ 9 のいずれかに記載の本人認証システムに用いられる前記携帯型通信端末であって、前記第 1 の近距離通信部との間で近距離通信を行う第 2 の近距離通信部と、
前記認証サーバから前記認証キー情報を受信すると、該受信した認証キー情報を前記第 2 の近距離通信部から前記第 1 の近距離通信部へ送信する近距離通信制御手段とを備えることを特徴とする携帯型通信端末。
- [請求項11] 前記近距離通信制御手段は、対応する携帯型記憶媒体を特定するパスキーが予め記憶されており、前記パスキーを用いて、前記認証サーバから受信した前記認証キー情報を前記対応する携帯型記憶媒体の第 1 の近距離通信部へ送信するものであることを特徴とする請求項 10 に記載の携帯型通信端末。
- [請求項12] 前記認証サーバの電子的なアドレスを記憶するアドレス記憶部と、
前記第 1 の近距離通信部との間での近距離通信の状態を監視し、近距離通信が途絶えた場合、その旨の情報を前記認証サーバの電子的なアドレスに送信する近接通信監視手段とを備えたことを特徴とする請求項 10 又は 11 に記載の携帯型通信端末。
- [請求項13] ネットワークに接続された情報処理端末に装着することで所定の情報処理の実行を許可する携帯型記憶媒体の正当所有者の有無を認証する本人認証方法において、
前記ネットワークに接続され、前記正当所有者か否かを認証する認証サーバを備え、
前記認証サーバの関連情報記憶部には、前記携帯型記憶媒体の識別

情報に対応付けて、前記携帯型記憶媒体の正当所有者の所持する前記携帯型通信端末の電子的なアドレス情報、及び固有の認証キー情報が記憶され、

前記情報処理端末の認証要求処理手段が、前記携帯型記憶媒体の装着を検出して、前記携帯型記憶媒体に記憶されている識別情報を取得し、取得した前記識別情報を含む信号を前記認証サーバに送信し、

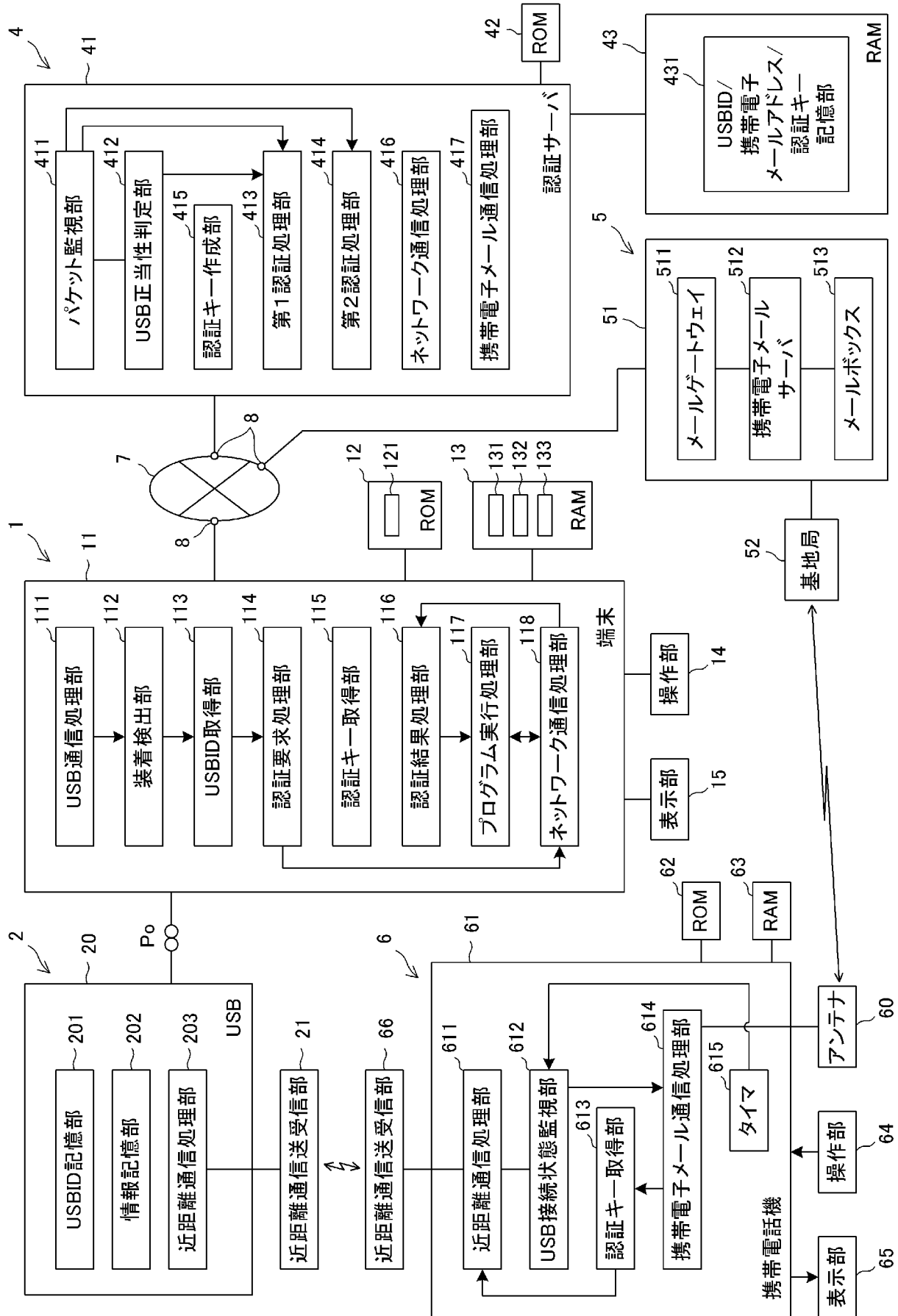
前記認証サーバの認証キー情報処理手段が、受信した前記識別情報を含む信号に含まれる前記識別情報に対応する認証キー情報及び電子的なアドレス情報を前記関連情報記憶部から読み出し、読み出した前記認証キー情報を読み出した前記電子的なアドレスに送信し、

前記携帯型記憶媒体の近距離通信部が、前記正当所有者の所持する、無線基地局を有する情報伝送系を経由して情報の送受信が可能な携帯型通信端末を介して前記認証キー情報を取得し、

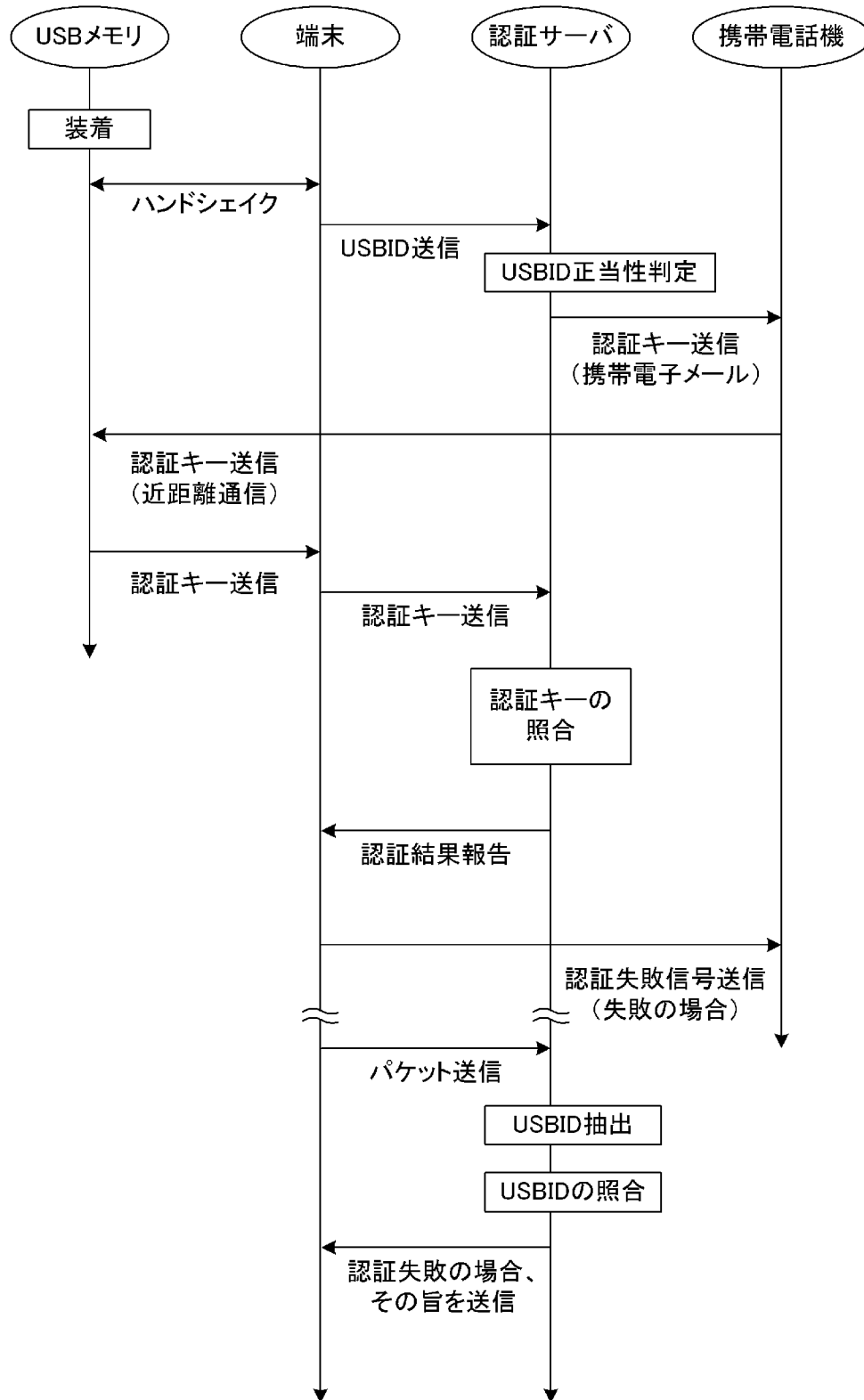
前記情報処理端末の認証キー中継処理手段が、前記識別情報を含む信号の送信後、前記携帯型通信端末及び前記携帯型記憶媒体を介して前記認証サーバから認証キー情報を取得すると、取得した前記認証キー情報を前記認証サーバに送信し、

前記認証サーバの判定手段が、前記認証キー情報の前記電子的なアドレスへの送信後、前記情報処理端末を介して前記認証キー情報を受信すると、前記認証キー情報処理手段によって送信された前記認証キー情報との異同を判定することを特徴とする本人認証方法。

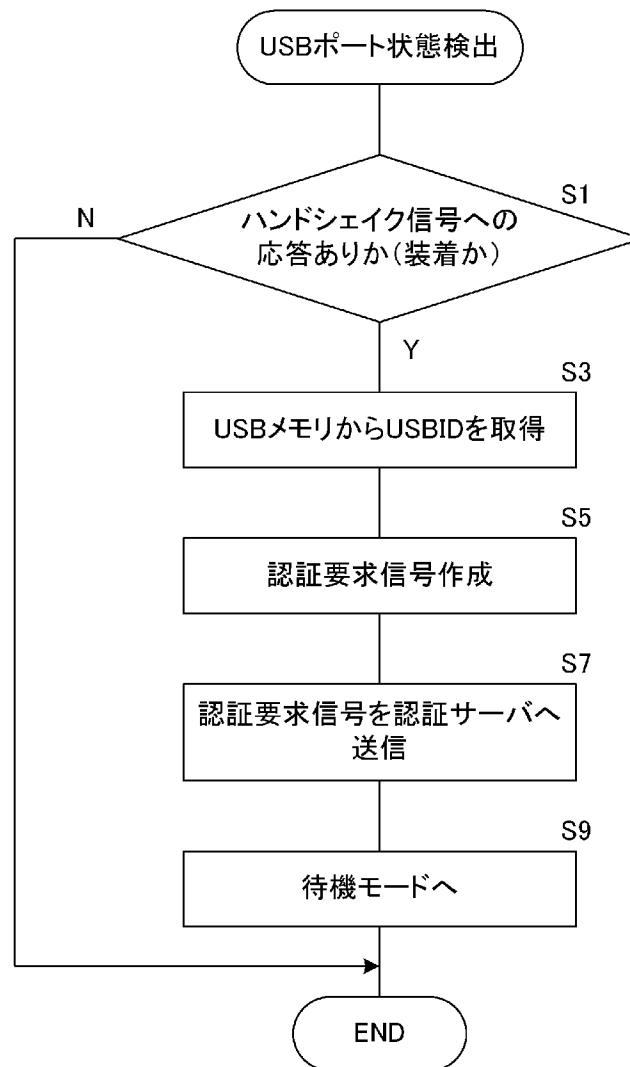
[図2]



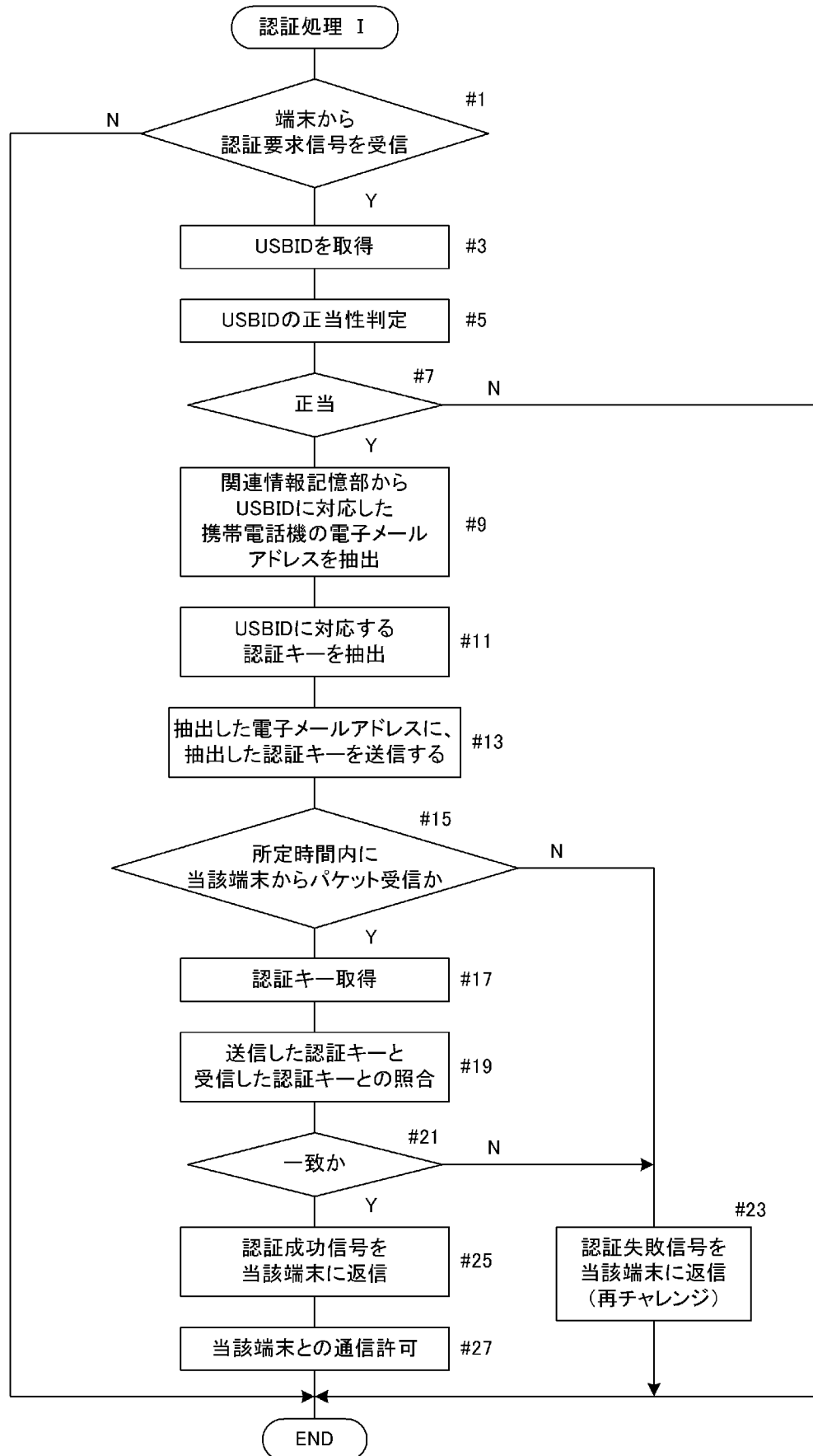
[図3]



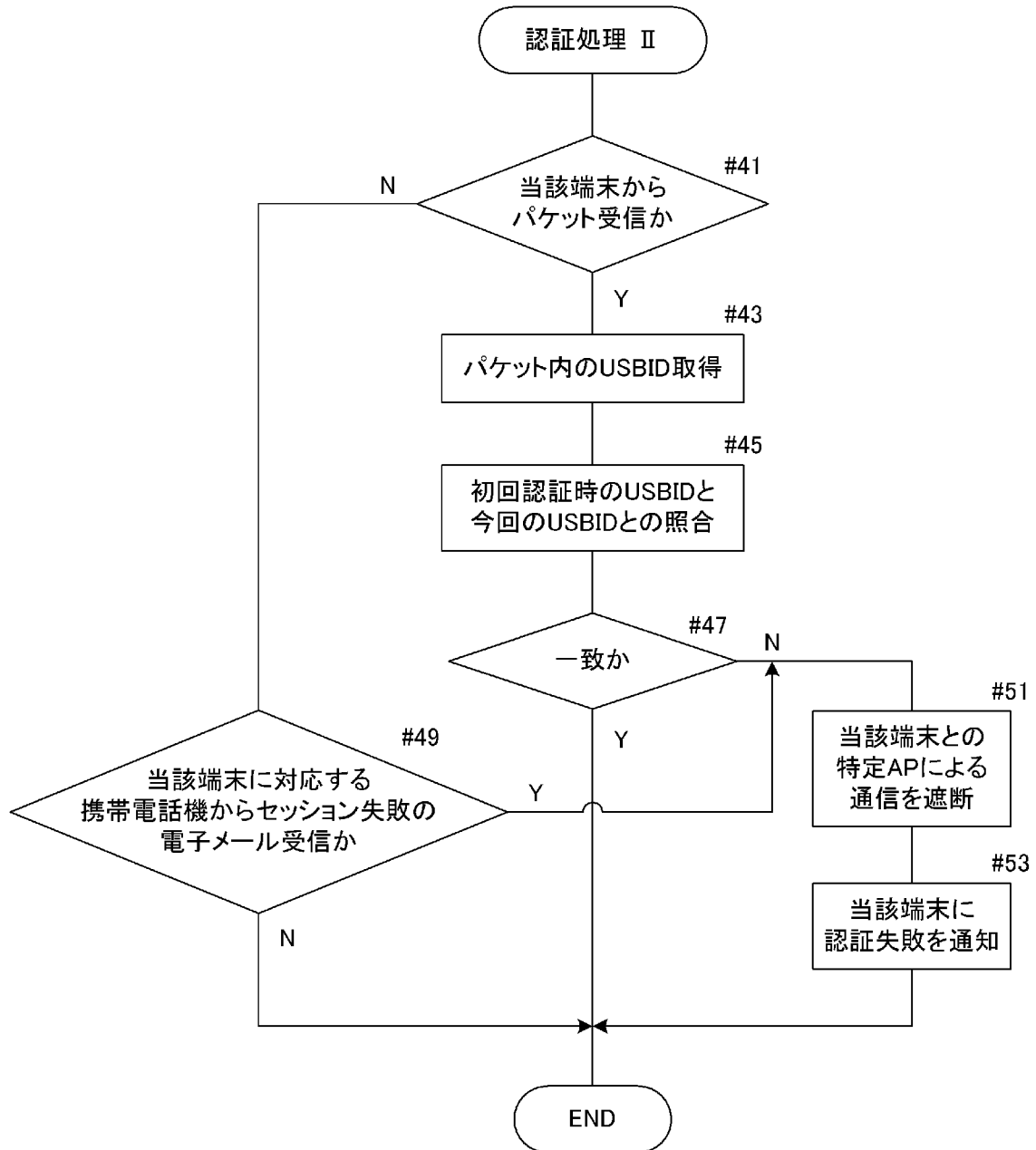
[図4]



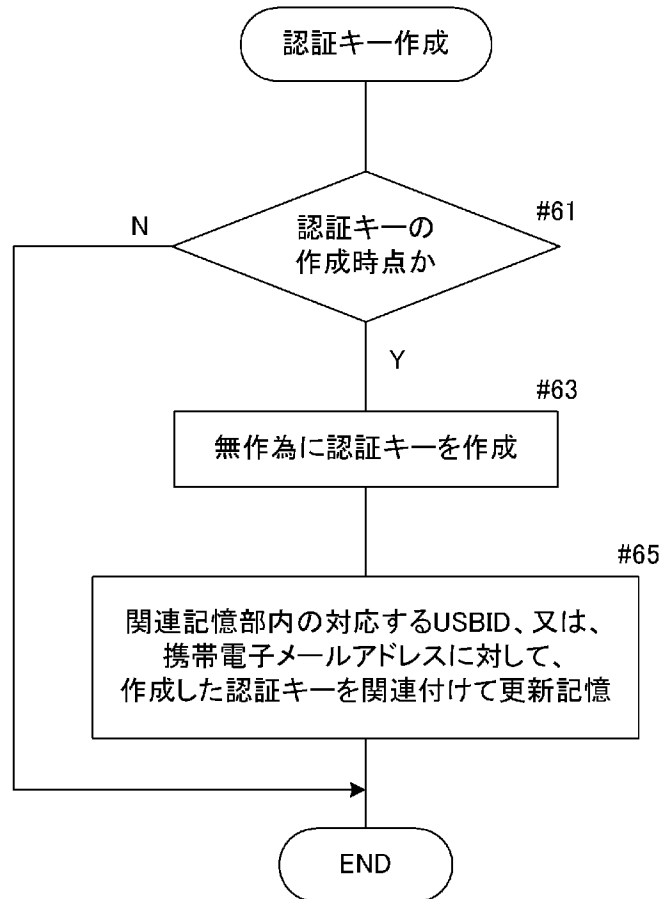
[図5]



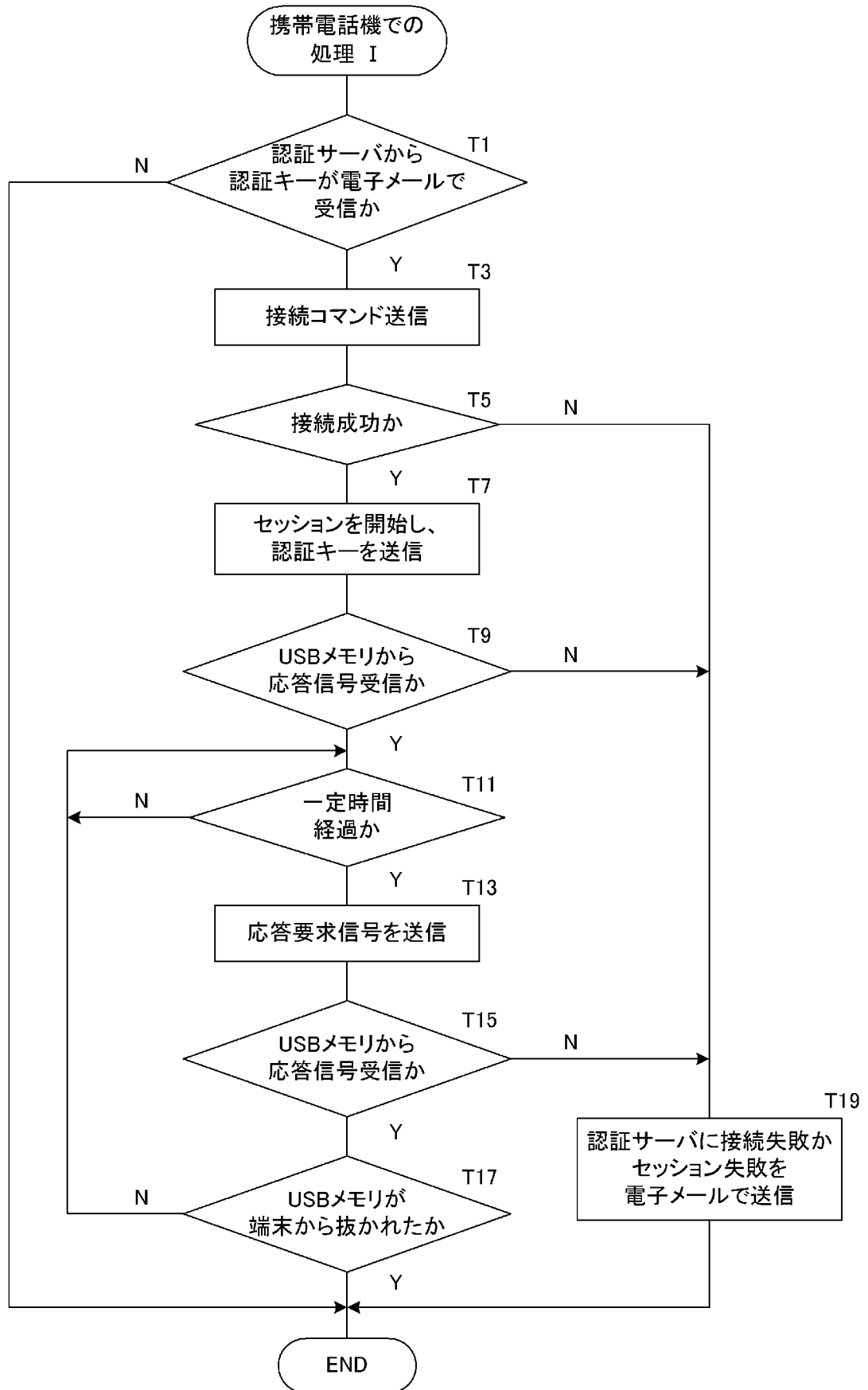
[図6]



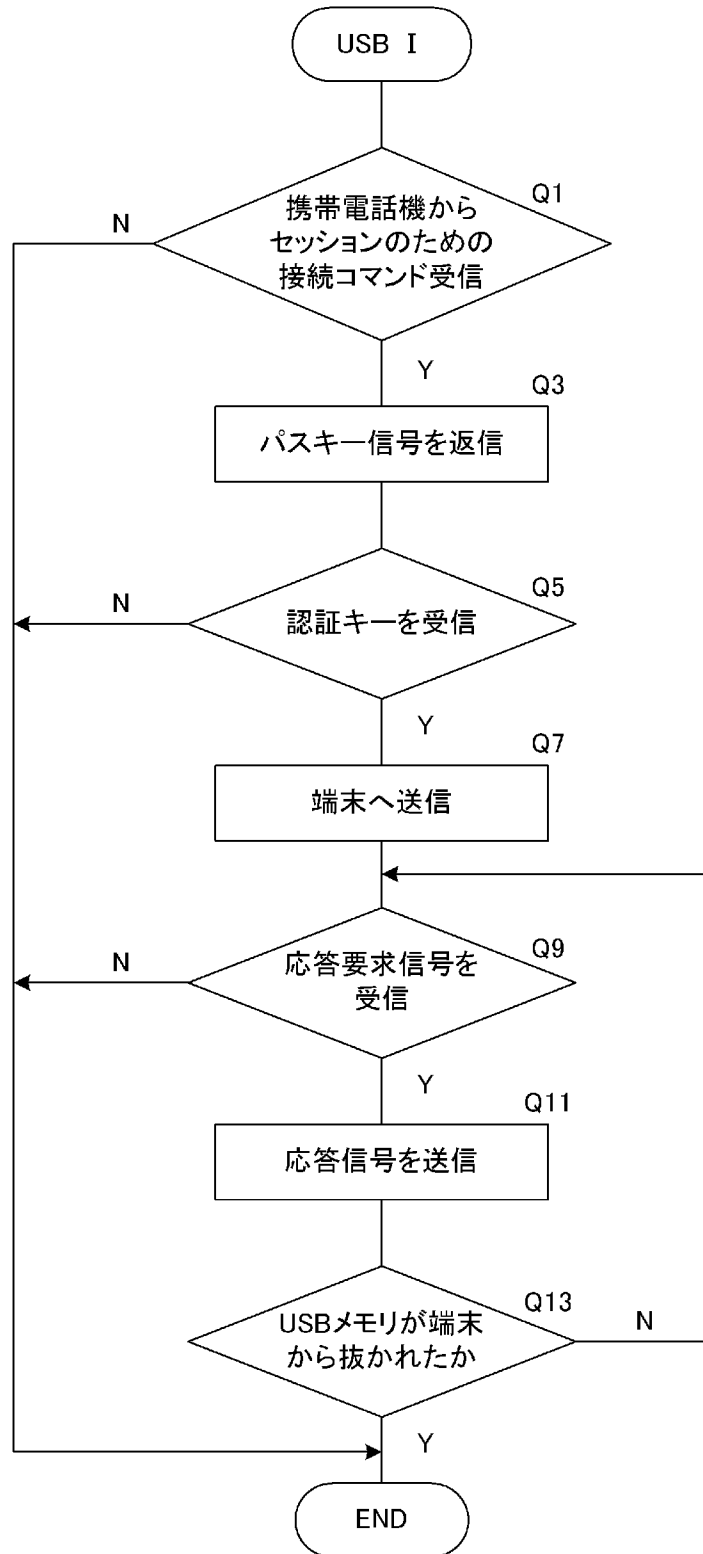
[図7]



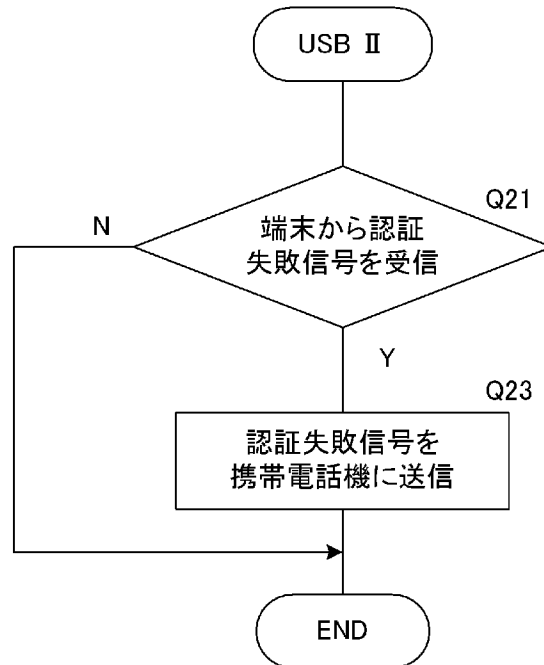
[図8]



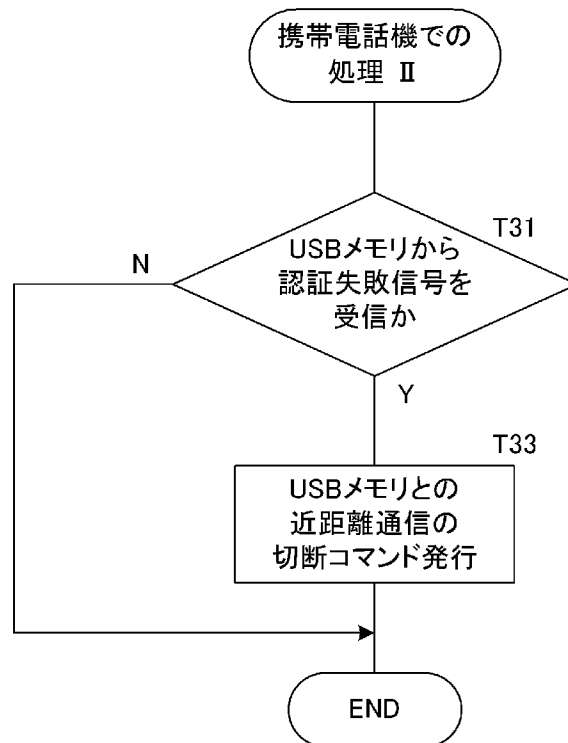
[図9]



[図10]



[図11]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2009/071277

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	1996-2010
Kokai Jitsuyo Shinan Koho	1971-2010	Toroku Jitsuyo Shinan Koho	1994-2010

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.
A	JP 2006-268682 A (Fujitsu Ltd.), 05 October 2006 (05.10.2006), entire text; all drawings & US 2006/0226950 A1 & EP 1705597 A2	1-13
A	JP 2008-250923 A (NTT Docomo Inc.), 16 October 2008 (16.10.2008), entire text; all drawings (Family: none)	1-13
A	JP 2001-306806 A (NEC Corp.), 02 November 2001 (02.11.2001), entire text; all drawings (Family: none)	1-13

☐ 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
16 September, 2010 (16.09.10)

Date of mailing of the international search report
28 September, 2010 (28.09.10)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

A. 発明の属する分野の分類（国際特許分類（I P C））

Int.Cl. 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	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 0 年
日本国実用新案登録公報	1 9 9 6 - 2 0 1 0 年
日本国登録実用新案公報	1 9 9 4 - 2 0 1 0 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
A	JP 2006-268682 A（富士通株式会社）2006. 10. 05, 全文, 全図 & US 2006/0226950 A1 & EP 1705597 A2	1 - 13
A	JP 2008-250923 A（株式会社エヌ・ティ・ティ・ドコモ）2008. 10. 16, 全文, 全図（ファミリーなし）	1 - 13
A	JP 2001-306806 A（日本電気株式会社）2001. 11. 02, 全文, 全図（ファミリーなし）	1 - 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

1 6 . 0 9 . 2 0 1 0

国際調査報告の発送日

2 8 . 0 9 . 2 0 1 0

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 1 0 0 - 8 9 1 5

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）

前 田 浩

5 S

2 9 4 3

電話番号 0 3 - 3 5 8 1 - 1 1 0 1 内線 3 5 4 6