

(19) 世界知的所有権機関
国際事務局



(43) 国際公開日
2005 年 2 月 17 日 (17.02.2005)

PCT

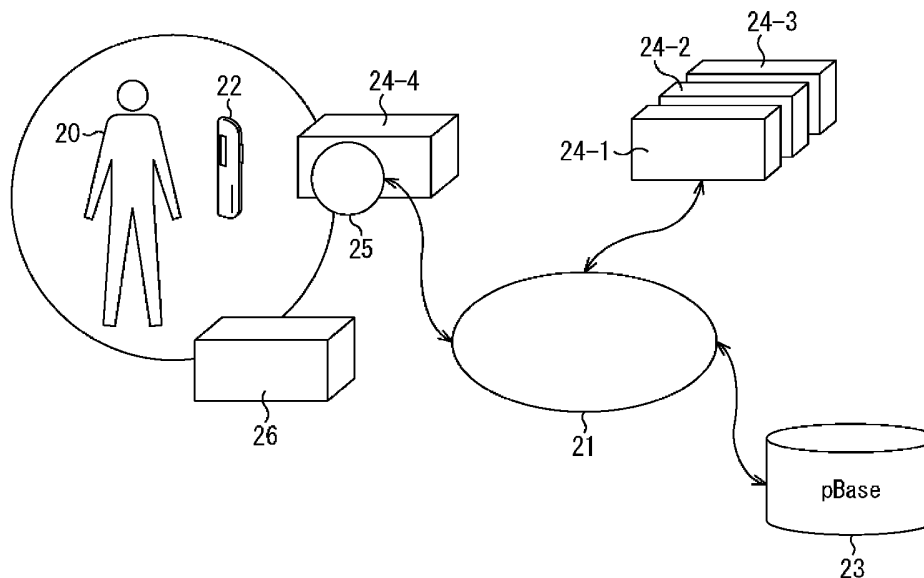
(10) 国際公開番号
WO 2005/015417 A1

- (51) 国際特許分類: G06F 15/00 (72) 発明者; および
(21) 国際出願番号: PCT/JP2004/011160 (75) 発明者/出願人 (米国についてのみ): 大森 睦弘 (OHMORI, Mutsuhiro) [JP/JP]; 〒1410001 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社内 Tokyo (JP). 角田 智弘 (TSUNODA, Tomohiro) [JP/JP]; 〒1410001 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社内 Tokyo (JP). 嶋田 繁広 (SHIMADA, Shigehiro) [JP/JP]; 〒1410001 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社内 Tokyo (JP).
(22) 国際出願日: 2004 年 8 月 4 日 (04.08.2004)
(25) 国際出願の言語: 日本語
(26) 国際公開の言語: 日本語
(30) 優先権データ: 特願2003-290053 2003 年 8 月 8 日 (08.08.2003) JP (74) 代理人: 稲本 義雄 (INAMOTO, Yoshio); 〒1600023 東京都新宿区西新宿 7 丁目 1 1 番 1 8 号 7 1 1 ビルディング 4 階 Tokyo (JP).
(71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒1410001 東京都品川区北品川 6 丁目 7 番 3 5 号 Tokyo (JP). (81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM,

/ 続葉有 /

(54) Title: INFORMATION PROCESSING DEVICE AND METHOD, PROGRAM, AND RECORDING MEDIUM

(54) 発明の名称: 情報処理装置および方法、プログラム、並びに記録媒体



(57) Abstract: It is possible to provide a pleasant user-friendly service not worrying a user. When a PK (22) storing PMD as personal information on a user (20) communicates with a service system (24) and uses the service system (24) for the first time, it stores the service ID of the service system (24) and the spoofing prevention method. When the PK (22) communicates with the service system (24) for the second time and after, the spoofing prevention processing is performed by each other before providing the PMD to the service system (24). The read out or modification processing of the PMD by the service system (24) is performed according to the preset access permission information by the user (20). The present invention may be applied to the PDA.

(57) 要約: ユーザの利便性を向上させ、さらにユーザにとって快適で安心なサービスを提供できるようにする。ユーザ 20 の個人関連情報である PMD を記憶する PK 22 が、サービスシステム 24 と通信し、サービスシステム 24 を初めて利用す

/ 続葉有 /



WO 2005/015417 A1



DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:

- 国際調査報告書
- 補正書

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE,

2 文字コード及び他の略語については、定期発行される各 *PCT* ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

るとき、サービスシステム 24 のサービス ID となりすまし防止方法を記憶する。PK 22 がサービスシステム 24 と、2 回目以降に通信するときは、互いになりすまし防止処理を行った後、サービスシステム 24 に PMD を提供する。サービスシステム 24 による PMD の読み出しまたは変更の処理は、ユーザ 20 により、予め設定されたアクセス許可情報に基づいて行われる。本発明は、PDA に適用できる。

明 細 書

情報処理装置および方法、プログラム、並びに記録媒体 技術分野

[0001] 本発明は、ユーザの利便性を向上させ、さらにユーザにとって快適で安心なサービスを提供できるようにする情報処理装置および方法、プログラム、並びに記録媒体に関する。

背景技術

[0002] 近年、個人情報提示することで、様々なサービスを受けられるようになった。個人情報としては、名前、住所、嗜好情報、サービスへの認証情報、点数情報、他の人からもらった情報等さまざまな情報があげられる。

[0003] このような個人情報をカードに保存して持ち運び、ユーザが店に入ったとき、ショッピングカートに搭載されたカードリーダーによりカードの情報が読み取られ、カードの情報に基づいて、広告を表示したり、場所案内、好みの商品のディスカウント情報などを表示する技術が提案されている(例えば、非特許文献1参照)。

[0004] また、個人情報を利用して、個人認証を行い、商品の購入、支払いなどの処理を便利にしようとする試みも行われている(例えば、特許文献1乃至3参照)。

[0005] 特許文献1によれば、ユーザの端末で、商品コードを入力し(または、商品のバーコードを読み込み)、それをページャー等での遠隔通信によりパブリックなネットワークに接続を行い、自宅のPCまたはPCS NCC(Personal Communication Service Network Control Center)に転送し、PCS NCCでは商品コードから商品の値段等の情報をユーザの端末へ転送する。商品情報はユーザの端末にのみ表示され、購入の申し込みを行うと、実際の支払いが電子マネー等で処理される。

[0006] また、特許文献2は、離れたところから、財務情報を制御するプラットフォームを提供しようとするもので、財務情報の提供は銀行により行われる。また、銀行とノンバンクの間で銀行業務とは関係のないサービスも提供する。

[0007] 特許文献3は、携帯電話を使って、電子財布、ワイヤレスPIN(personal identification number)パッド、および非接触型のスマートカードの機能を実現しようというものであ

る。携帯電話会社等でのサービスプロバイダーにおいて、アカウントと認証情報を保持し、携帯電話から予め決められた機能コードを入力すると、機能コードがサービスプロバイダーへ転送され要求された処理が行われる。サービスプロバイダーの中央処理装置により、認証が必要か否かの判断を行い、必用であれば個人認証番号を中央処理装置に転送し、中央処理装置にて認証処理を行い取引が行われる。

特許文献1:US5,991,601(Personal intercommunication purchase and fulfillment system)

特許文献2:US5,787,403 (Bank-centric service platform, network and system)

特許文献3:US5,991,749 (Wireless telephony for collecting tolls, conducting financial transactions, and authorizing other activities)

非特許文献1:US2002-174025-A1 Method and System for providing targeted Advertising and personalized customer services (IBM)

発明の開示

発明が解決しようとする課題

- [0008] しかしながら、非特許文献1の技術では、他の店で受けたサービスとの情報交換ができない。また、カードを使っているのがユーザ本人か否かを確認する、なりすまし防止機構がないという課題があった。
- [0009] また、特許文献1の技術では、PCS NCCにおいてデータベースの管理を行うにあたり、商品コードから商品情報を検索するためのデータベース作成等が必要になり、迅速な処理ができないという課題があった。
- [0010] 特許文献2の技術では、サービスの流れを規定しているが、ユーザの端末においてどのような認証処理がなされるかが考慮されていないという課題があった。
- [0011] 特許文献3の技術では、固定的な機能コードが必要となるため、認証システムおよび商品情報に依存した携帯電話等を作成しなければならず、柔軟なシステムの運用が行えず、その結果、ユーザの利便性が損なわれる恐れがあるという課題があった。
- [0012] 本発明はこのような状況に鑑みてなされたものであり、ユーザの利便性を向上させ、さらにユーザにとって快適で安心なサービスを提供できるようにするものである。

課題を解決するための手段

- [0013] 本発明の第1の情報処理装置は、ユーザに関連するユーザ情報を記憶し、複数の他の情報処理装置と通信を行う情報処理装置であって、他の情報処理装置により読み出したりは変更が行われるユーザ情報を提示する提示手段と、提示手段により提示されたユーザ情報の読み出したりは変更の許可を指定する指定手段と、他の情報処理装置を特定する特定手段と、特定手段により特定された他の情報処理装置と他の情報処理装置により読み出したりは変更が行われるユーザ情報を関連付けて記憶する記憶手段とを備えることを特徴とする。
- [0014] 準静電界通信、電磁波通信、光通信、または電氣的通信を行う通信手段をさらに備えるようにすることができる。
- [0015] 前記情報処理装置の外部の機器を、入力または出力のインタフェースとして利用するようにすることができる。
- [0016] 前記他の情報処理装置と初回の通信を行うとき、他の情報処理装置に情報処理装置を特定する情報を送信するようにすることができる。
- [0017] 前記他の情報処理装置と初回の通信を行うとき、情報処理装置が情報を暗号化するために用いる第1のコードと、第1のコードに対応して生成される第2のコードを生成し、第1のコードを他の情報処理装置に送信し、他の情報処理装置が情報を暗号化するために用いる第3のコードを前記通信手段を介して取得するようにすることができる。
- [0018] 前記ユーザ情報を前記他の情報処理装置から提供されたコンテンツの利用履歴にもとづいて更新するようにすることができる。
- [0019] 前記ユーザ情報を管理する情報管理装置とネットワークを介して通信し、情報処理装置に記憶されたユーザ情報の内容が情報管理装置に記憶されたユーザ情報の内容と同じになるようにユーザ情報を更新するようにすることができる。
- [0020] 前記情報管理装置は、ユーザ情報の読み出したりは変更が許可された他の情報処理装置を特定し、ユーザ情報をユーザ情報の読み出したりは変更が許可された他の情報処理装置に、ネットワークを介して提供するようにすることができる。
- [0021] 前記ユーザの体に発生する準静電界または静電界の変化パターンに基づいて、前記ユーザを認証するようにすることができる。

- [0022] 前記ユーザ情報は、ユーザの嗜好を表す嗜好情報を有し、ユーザが指定する情報機器に嗜好情報を送信し、情報機器を嗜好情報に対応して動作させるようにすることができる。
- [0023] 複数の他の情報処理装置に関連付けられた複数のユーザ情報に基づいて、あらたなユーザ情報を生成するようにすることができる。
- [0024] 本発明の第1の情報処理方法は、ユーザに関連するユーザ情報を記憶し、複数の他の情報処理装置と通信を行う情報処理装置の情報処理方法であって、他の情報処理装置により読み出しまたは変更が行われるユーザ情報を提示する提示ステップと、提示ステップの処理により提示されたユーザ情報の読み出しまたは変更の許可を指定する指定ステップと、他の情報処理装置を特定する特定ステップと、特定ステップの処理により特定された他の情報処理装置と他の情報処理装置により読み出しまたは変更が行われるユーザ情報を関連付けて記憶する記憶ステップとを含むことを特徴とする。
- [0025] 本発明の第1のプログラムは、ユーザに関連するユーザ情報を記憶し、複数の他の情報処理装置と通信を行う情報処理装置のプログラムであって、他の情報処理装置により読み出しまたは変更が行われるユーザ情報の提示を制御する提示制御ステップと、提示制御ステップの処理により提示されたユーザ情報の読み出しまたは変更の許可の指定を制御する指定制御ステップと、他の情報処理装置の特定を制御する特定制御ステップと、特定制御ステップの処理により特定された他の情報処理装置と他の情報処理装置により読み出しまたは変更が行われるユーザ情報を関連付けて記憶するように制御する記憶制御ステップとをコンピュータに実行させることを特徴とする。
- [0026] 本発明の第1の記録媒体は、ユーザに関連するユーザ情報を記憶し、複数の他の情報処理装置と通信を行う情報処理装置のプログラムが記録される記録媒体であって、他の情報処理装置により読み出しまたは変更が行われるユーザ情報の提示を制御する提示制御ステップと、提示制御ステップの処理により提示されたユーザ情報の読み出しまたは変更の許可の指定を制御する指定制御ステップと、他の情報処理装置の特定を制御する特定制御ステップと、特定制御ステップの処理により特定された

他の情報処理装置と他の情報処理装置により読み出したりまたは変更が行われるユーザ情報を関連付けて記憶するように制御する記憶制御ステップとをコンピュータに実行させるプログラムが記録されることを特徴とする。

[0027] 本発明の第1の情報処理装置および方法、並びに第1のプログラムにおいては、他の情報処理装置により読み出したりまたは変更が行われるユーザ情報が提示され、提示されたユーザ情報の読み出したりまたは変更の許可が指定され、他の情報処理装置が特定され、特定された他の情報処理装置と他の情報処理装置により読み出したりまたは変更が行われるユーザ情報が関連付けられて記憶される。

[0028] 本発明の第2の情報処理装置は、ネットワークを介して複数の他の情報処理装置と通信を行い、ユーザに関連するユーザ情報を記憶する情報処理装置であって、ユーザが所持する携帯端末とネットワークを介して通信する通信手段と、携帯端末に記憶され、ユーザに関連するユーザ情報を取得する取得手段と、取得手段により取得されたユーザ情報に基づいて、情報処理装置に記憶されるユーザ情報の更新を行う更新手段と、携帯端末に記憶されるユーザ情報を更新するデータを作成する作成手段とを備えることを特徴とする。

[0029] 前記携帯端末が前記ネットワークに接続されていない場合、前記通信手段は、前記携帯端末に代わって前記他の情報処理装置と通信を行うようにすることができる。

[0030] 前記ユーザ情報として、携帯端末を特定する情報と、携帯端末が、他の情報処理装置を認証する合言葉と、携帯端末が、情報を暗号化するとき用いる第1のコードおよび第1のコードに対応して生成される第2のコードと、他の情報処理装置を特定する情報と、他の情報処理装置が、携帯端末を認証する合言葉と、他の情報処理装置が、情報を暗号化するとき用いる第3のコードとをさらに記憶するようにすることができる。

[0031] 前記ユーザ情報を前記他の情報処理装置から提供されたコンテンツの利用履歴にもとづいて更新する更新手段をさらに備えるようにすることができる。

[0032] 前記携帯端末と前記ネットワークを接続するアクセスポイントを特定し、特定されたアクセスポイントの位置に基づいて、ユーザの現在値を特定し、ユーザの現在地の情報をユーザ情報として記憶するようにすることができる。

- [0033] 前記アクセスポイントに対応する機器を特定するIDと、機器と通信するために必要なアクセスキーをユーザ情報としてさらに記憶するようにすることができる。
- [0034] 前記通信手段は、携帯端末と所定の時間間隔で通信し、ユーザの現在地の情報、並びにアクセスポイントに対応する機器のIDおよびアクセスキーを更新するようにすることができる。
- [0035] 前記他の情報処理装置からユーザとの会話の要求を表す要求信号をネットワークを介して受信した場合、ユーザ情報を他の情報処理装置に送信するようにすることができる。
- [0036] 前記携帯端末の記憶容量を超えて存在する前記ユーザ情報をさらに記憶するようにすることができる。
- [0037] 本発明の第2の情報処理方法は、ネットワークを介して複数の他の情報処理装置と通信を行い、ユーザに関連するユーザ情報を記憶する情報処理装置の情報処理方法であって、ユーザが所持する携帯端末とネットワークを介して通信する通信ステップと、携帯端末に記憶され、ユーザに関連するユーザ情報を取得する取得ステップと、取得ステップの処理により取得されたユーザ情報に基づいて、情報処理装置に記憶されるユーザ情報の更新を行う更新ステップと、携帯端末に記憶されるユーザ情報を更新するデータを作成する作成ステップとを含む。
- [0038] 本発明の第2のプログラムは、ネットワークを介して複数の他の情報処理装置と通信を行い、ユーザに関連するユーザ情報を記憶する情報処理装置のプログラムであって、ユーザが所持する携帯端末と前記ネットワークを介して通信するように制御する通信制御ステップと、前記携帯端末に記憶され、ユーザに関連するユーザ情報の取得を制御する取得制御ステップと、取得制御ステップの処理により取得されたユーザ情報に基づいて、情報処理装置に記憶されるユーザ情報の更新を行うように制御する更新制御ステップと、携帯端末に記憶されるユーザ情報を更新するデータの作成を制御する作成制御ステップとをコンピュータに実行させることを特徴とする。
- [0039] 本発明の第2の記録媒体は、ネットワークを介して複数の他の情報処理装置と通信を行い、ユーザに関連するユーザ情報を記憶する情報処理装置のプログラムが記録される記録媒体であって、ユーザが所持する携帯端末と前記ネットワークを介して通

信するように制御する通信制御ステップと、前記携帯端末に記憶され、前記ユーザに関連するユーザ情報の取得を制御する取得制御ステップと、前記取得制御ステップの処理により取得されたユーザ情報に基づいて、前記情報処理装置に記憶される前記ユーザ情報の更新を行うように制御する更新制御ステップと、前記携帯端末に記憶される前記ユーザ情報を更新するデータの作成を制御する作成制御ステップとをコンピュータに実行させるプログラムが記録されることを特徴とする。

- [0040] 本発明の第2の情報処理装置および方法、並びに第2のプログラムにおいては、ユーザが所持する携帯端末とネットワークを介して通信が行われ、携帯端末に記憶されるユーザに関連するユーザ情報が取得され、取得されたユーザ情報に基づいて、情報処理装置に記憶されるユーザ情報の更新が行われ、携帯端末に記憶されるユーザ情報を更新するデータが作成される。

発明の効果

- [0041] 本発明によれば、ユーザに利便性の高いサービスを提供することができる。特に、ユーザにとって快適で安心なサービスを提供できる。

図面の簡単な説明

- [0042] [図1]本発明のサービス提供システムの構成例を示す図である。
[図2]図1のPKの構成例を示すブロック図である。
[図3]図1のpBaseの構成例を示すブロック図である。
[図4]図1のPKのソフトウェアの構成例を示すブロック図である。
[図5]サービスIDの初期登録を行う処理の流れを示すフローチャートである。
[図6]PKとサービスシステムにおいて、なりすまし防止を行う処理の流れを示すフローチャートである。
[図7]PKとサービスシステムにおいて、なりすまし防止を行う処理の流れを示すフローチャートである。
[図8]鍵管理処理を説明するフローチャートである。
[図9]サービスID登録処理を説明するフローチャートである。
[図10]サービスIDマッチング処理を説明するフローチャートである。
[図11A]PKによりユーザの認証が行われる例を示す図である。

[図11B]PKによりユーザの認証が行われる例を示す図である。

[図12]ユーザ認証処理1を説明するフローチャートである。

[図13]ユーザ認証処理2を説明するフローチャートである。

[図14]PMD管理処理を説明するフローチャートである。

[図15]PKの外部の機器を利用して、入出力インタフェースを構成する例を示す図である。

[図16]PKにより、周辺機器へのアクセスキーが隠蔽される様子を示す図である。

[図17A]PK、pBase、およびサービスシステム間の通信のパターンを示す図である。

[図17B]PK、pBase、およびサービスシステム間の通信のパターンを示す図である。

[図17C]PK、pBase、およびサービスシステム間の通信のパターンを示す図である。

[図18]pBaseとサービスシステムにおいて、なりすまし防止を行う処理の流れを示すフローチャートである。

[図19]pBaseとサービスシステムにおいて、なりすまし防止を行う処理の流れを示すフローチャートである。

[図20A]PMDの構成例を示す図である。

[図20B]PMDの構成例を示す図である。

[図20C]PMDの構成例を示す図である。

[図21]PMD更新処理を説明するフローチャートである。

[図22]複数のPMDに基づいて生成される新しいPMDを示す図である。

[図23]複数のPMDに基づいて生成される新しいPMDを示す図である。

[図24]コンテンツアクセスパッケージの構成例を示す図である。

[図25]PKにより、各種の機器をパーソナライズする例を示す図である。

[図26]音楽再生処理を説明するフローチャートである。

[図27]Web情報提供処理を説明するフローチャートである。

[図28]PKにより、各種の機器をパーソナライズする例を示す図である。

[図29]ファイヤーウォール機能をもつルータを挟んで通信を行う例を示す図である。

[図30]PMDの同期の処理の流れを示すフローチャートである。

[図31]PMD同期処理を説明するフローチャートである。

- [図32]PKに各種カード情報を保持させて利用する例を示す図である。
- [図33]コンソール端末に制御コードをインストールする例を示す図である。
- [図34]制御コードを取得する処理の流れを示すアローチャートである。
- [図35]PKによりドアを開放する例を示す図である。
- [図36]PKの顔特徴情報が端末に表示される例を示す図である。
- [図37]会話接続サービスの例を示す図である。
- [図38]会話接続が行われる処理の流れを示すアローチャートである。
- [図39]PKを利用して、ユーザの位置を特定する例をしめす図である。
- [図40]ユーザの位置を特定する処理の流れを示すアローチャートである。
- [図41]地図情報サービスを提供する例を示す図である。
- [図42]カメラを用いて、ユーザの位置を特定する例を示す図である。
- [図43]アクセスポイント検出処理1を説明するフローチャートである。
- [図44]アクセスポイントが検出される仕組みを示す図である。
- [図45]アクセスポイント検出処理2を説明するフローチャートである。
- [図46]アクセスポイントが検出される仕組みを示す図である。
- [図47]PKの複数の通信ルートを示す図である。
- [図48]PMDの構成例を示す図である。
- [図49]PKがプログラムを実行する処理を説明するフローチャートである。
- [図50]pBaseをサービスシステムとして、処理が行われる流れを示すアローチャートである。
- [図51]通信スタンバイ処理を説明するフローチャートである。
- [図52]待ち受け時の通信の例を示す図である。
- [図53]RF通信が行われる例を示す図である。
- [図54A]PKにより、ユーザにメッセージを通知する例を示す図である。
- [図54B]PKにより、ユーザにメッセージを通知する例を示す図である。
- [図55]コミュニケーションリストの例を示す図である。
- [図56]会議室内の機器を示す図である。
- [図57]会議室内の着席位置を示す図である。

[図58]IP電話機の消費電力を抑制する例を示す図である。

[図59]PKのソフトウェアとサービスシステムのソフトウェアを1つの機器に実装する例を示す図である。

[図60]協調フィルタリングサーバと、PMDを用いてパーソナライズを行う例を示す図である。

符号の説明

[0043] 22 PK, 23 pBase, 24 サービスシステム, 62 ユーザ制御許可入力モジュール, 64 なりすまし防止モジュール, 66 DBアクセスモジュール, 67PMD B, 101 CPU, 106 入力部, 107 出力部, 121 CPU, 126 入力部, 127 出力部

発明を実施するための最良の形態

[0044] 以下、図面を参照して、本発明の実施の形態について説明する。図1は、本発明を適用したサービス提供システム1の構成例を表すブロック図である。この例においては、ユーザ20が、そのユーザの個人関連情報を記憶する携帯可能な小型のコンピュータなどで構成されるPK (Personal Key) 22を携帯している。ここで、個人関連情報とは、単に、名前、住所などそのユーザを特定するための情報だけでなく、嗜好情報、認証情報、点数情報、他の人からもらった情報などを含む、そのユーザに関連する様々な情報の集合を意味する。

[0045] PK22は、アクセスポイント25の周囲のエリア41において、RF (Radio Frequency) 通信、準静電界通信、光通信などの無線通信により、インターネット21に接続されたアクセスポイント25と通信する。また、PK22は、無線通信などにより近傍の情報機器との通信も行う。PK22は、暗号鍵に基づいて情報を暗号化する暗号化機能を有しており、暗号鍵の鍵データは必要に応じてSB (Secure Button) 26に記憶される。SB26は通信機能を有するコンピュータであり、PK22と通信し、鍵データの送受信を行う。

[0046] インターネット21には、PK22から、ユーザ20の個人関連情報であるPMD (Personal Meta Data) を、インターネット21を介して取得し、取得したPMDをデータベースとして記憶するpBase (Personal Information Base) 23が接続されている。

pBase23は、コンピュータで構成され、インターネット21に接続される他の情報処理装置と通信する。なお、pBase23には、PK22(ユーザ20)以外のPK(ユーザ)のPMDも複数記憶されている。

[0047] また、インターネット21には、コンピュータなどにより構成され、それぞれ所定の処理を実行するサービスシステム24-1乃至24-3が接続されている。サービスシステム24-1乃至24-3は、インターネット21を介して、PK22またはpBase23からPMDを取得し、取得したPMDに基づいて、所定のプログラムを実行することにより、情報提供、買い物代金の決済などのサービスをユーザに提供する。

[0048] 例えば、サービスシステム24-1は、パーソナルコンピュータにWebページ、音楽情報など提供するコンテンツサーバとされ、サービスシステム24-2は、クレジットカードによる決済などを行うクレジットカード処理サーバとされ、サービスシステム24-3は、ユーザ20に対して行われるコミュニケーションを制御するコミュニケーションサーバとされる。また、アクセスポイント25も、PK22との通信を行うサービスシステム24-4に包含される。なお、これらを個々に区別する必要がない場合、まとめてサービスシステム24と称する。

[0049] この例では、サービスシステム24-1乃至24-4が表示されているが、実際には、多数のサービスシステムが存在する。また、サービスシステム24は、パーソナルコンピュータ、サーバなどに限られるものではなく、コンソール端末、または各種のコンシューマエレクトロニクス機器(CE機器)などにより構成されるようにしてもよい。さらに、サービスシステム24は、インターネット21に接続されるものに限られることなく、通信機能を有するものであれば、どこに設置されていてもよい。なお、PK22とサービスシステム24は、インターネット21を介さずに、直接通信することも可能である。

[0050] 図2は、PK22の構成例を示すブロック図である。CPU(Central Processing Unit)101は、ROM(Read Only Memory)102に記憶されているプログラム、または記憶部108からRAM(Random Access Memory)103にロードされたプログラムに従って各種の処理を実行する。RAM103にはまた、CPU101が各種の処理を実行する上において必要なデータなども適宜記憶される。

[0051] CPU101、ROM102、およびRAM103は、バス104を介して相互に接続されている

。このバス104にはまた、入出力インタフェース105も接続されている。

[0052] 入出力インタフェース105には、スイッチまたはボタンなどよりなる入力部106、およびドットマトリックスディスプレイ、スピーカ、振動モータなどにより構成され、画像、音声、点字または振動などによりユーザに提示する情報を出力する出力部107が接続されている。さらに、入出力インタフェース105には、ハードディスク、またはEEPROM (Electrically Erasable and Programmable Read Only Memory) などにより構成される記憶部108、無線送受信装置などにより構成される通信部109が接続されている。なお、通信部109は、RF通信(電磁波通信)、準静電界通信、光通信など通信方法に応じて、複数設けられるようにしてもよい。

[0053] RF (Radio Frequency) 通信は、IEEE802. 11bに代表される無線LANなどの通信であり、この通信により、所定のアクセスポイント(ハブ)の周囲およそ数十メートルで通信することができる。準静電界通信は、人体近傍に、遠隔伝播せず閉域のみに成立する物理的性質(エバネッセント性)をもつ閉じた静電的な情報空間を形成する通信方式であり、この通信により、人体が微弱な静電気のアンテナとなり人体の周囲およそ数センチメートル、または数メートルの限られた空間で通信することが可能となる。これにより、例えば、PK22を携帯したユーザが、歩行しながら、PK22に通信させることができる。

[0054] 勿論、通信部109は、イーサネット(登録商標)などに代表される有線の電氣的通信または赤外線などの光通信を行うものとすることも可能である。

[0055] 入出力インタフェース105には、必要に応じてドライブ110が接続され、ドライブ110には、本発明のプログラムが記録された記録媒体として、例えば、リムーバブルメディア111が装着され、それらから読み出されたコンピュータプログラムが、必要に応じて記憶部108にインストールされる。

[0056] 図3は、pBase23の構成例を示すブロック図である。その構成は、図2に示したPK22の構成と同様であり、図3のCPU121乃至リムーバブルメディア131は、図2のCPU101乃至リムーバブルメディア111に対応している。各部の機能は、図2の場合と同様であり、詳細な説明は省略するが、通信部129は、無線送受信装置の他、LANカード、モデムなどの有線による通信装置により構成される。

- [0057] また、サービスシステム24も図3と同様の構成であり、同図を適用する。
- [0058] 図4は、PK22の記憶部108に記憶されるソフトウェア60の構成例を示すブロック図である。ソフトウェア60には、PK22に保存される個人情報であるPMDをデータベースとして記憶するPMDB67、および通信部109を制御して通信を行う通信モジュール61が含まれている。
- [0059] また、ユーザによる、PMDに対するアクセスの許可の指定を受け付けるユーザ制御許可入力モジュール62、サービスシステム24からアクセス要求があったPMDについて、ユーザにアクセス可否を判断させるために、そのPMDを提示する許可項目確認モジュールが含まれている。さらに、サービスシステム24のなりすましを防止するなりすまし防止モジュール63、必要に応じてPMDの変更を行うPMD変更モジュール65が含まれている。DBアクセスモジュール66は、ユーザ制御許可入力モジュール62乃至PMD変更モジュール65の指令(要求)に基づいて、PMDB67にアクセスし、PMDの読み出しまたは変更を行う。
- [0060] PMDB67は、複数のPMDにより構成されるデータベースであり、各PMDは、各サービスシステム24に対応した固有のIDであるサービスIDをキーとして、各情報がディレクトリ状に関連付けられている。サービスID1のディレクトリ(PMD)には、アクセス許可情報、メタデータA-1、メタデータA-2、メタデータA-3、...が関連付けられている。
- [0061] アクセス許可情報は、そのディレクトリに関連付けられた情報に対する、サービスシステム24からのアクセスの可否を表す情報であり、ユーザにより設定される。メタデータA-1、メタデータA-2、およびメタデータA-3、...は、サービスID1に対応するサービスシステム24において、利用される個人関連情報であり、例えば、サービスID1に対応するサービスシステムが、映画やテレビ番組などのコンテンツを提供するコンテンツサーバである場合、メタデータA-1、メタデータA-2、およびメタデータA-3、...には、それぞれ視聴された番組のメタデータが記憶される。その他、PMDには、PK22(ユーザ20)を特定するユーザID、なりすまし防止処理において必要となる合言葉または暗号鍵などの認証情報、視聴された番組に基づくユーザの嗜好情報、およびテレビジョン受像機などを制御する制御情報などが記憶される。

- [0062] 同様に、サービスID2のディレクトリにもアクセス許可情報、メタデータB-1、メタデータB-2、メタデータB-3、・・・が関連付けられている。そして、PKが新たに、サービスシステム24を利用する場合、新たなサービスIDが登録され、そのサービスIDに対応するディレクトリが生成される。そして、それぞれのディレクトリがPMDとされ、PMDB67が構成される。なお、PMDの詳細な構成例については、図20を参照して後述する。
- [0063] 図5は、PK22にサービスシステム24に対応するサービスIDを、最初に登録(初期登録)するときの処理の流れを示すフローチャートである。ステップS1において、サービスシステム24は、PK22に対して、登録要求、サービスIDおよび、そのサービスシステムの読み出し変更対象となるメタデータを表す情報を送信し、ステップS21において、PKの通信モジュール61により、これが受信される。
- [0064] ステップS22において、通信モジュール61は、許可項目確認モジュール63に受信内容を転送する。許可項目確認モジュール63は、ステップS42において、読み出し変更対象となるメタデータをユーザに提示する。このとき、例えば、メタデータの内容が、ドットマトリックスディスプレイ等に文字または図形等が表示されるか、スピーカを通じて音声により内容を読み上げられる。あるいはまた、メタデータの内容が、機械的機構により点字として生成され、提示されるか、振動によりモールス信号等の信号が生成され、提示されるようにしてもよい。
- [0065] ステップS43において、許可項目確認モジュール63は、ユーザ制御許可入力モジュール62に対して、確認要求を出力し、ステップS61においてこれが取得される。ステップS62において、ユーザ制御許可入力モジュール62は、ステップS42で提示された読み出し変更対象メタデータに対するアクセスを、ユーザが拒否したか否かを判定し、拒否したと判定された場合、拒否信号を出力し、ステップS23において、通信モジュール61によりこれが受信される。ステップS24において、通信モジュール61は、拒否信号をサービスシステム24に送信し、ステップS2でこれが受信される。
- [0066] 一方、ステップS62において、ステップS42で提示された読み出し変更対象メタデータに対するアクセスを、ユーザが拒否していないと判定された場合、ユーザ制御許可入力モジュール62は、ステップS63において、ユーザの指定に基づいて、読み出

し変更対象となるメタデータのそれぞれについて、例えば、「読み出しと変更を許可」、「読み出しのみ許可」などの情報を設定し、これらの情報がアクセス許可情報(図4)としてPMDB67に記憶される。ステップS64において、ユーザ制御許可入力モジュール62は、アクセス制御情報が設定されたことを、許可項目確認モジュール63に対して通知し、ステップS44において、これが取得される。ステップS45において、許可項目確認モジュール63は、なりすまし防止モジュール64に対して、確認コードの生成要求を行い、ステップS81において、なりすまし防止モジュール64により、これが取得される。

[0067] ステップS82において、なりすまし防止モジュール64は、確認コードを生成する。確認コードは、PK22とサービスシステム24が、次回通信を行うときのなりすまし防止方法を表すコードである。すなわち、不正なユーザ、または通信を盗聴した第三者などが、自身のアドレス、またはIDなどを詐称するなどして、PK22、またはサービスシステム24になりすましていないかを、互いに確認するための方法を表すコードである。

[0068] ここで、なりすまし防止方法としては、例えば、合言葉による認証、公開鍵により暗号化された情報による認証、共通鍵により暗号化された情報による認証などが採用されるが、サービスシステム24との通信において、どれだけの安全性が要求されるのか、どの程度、頻繁になりすまし防止のためのチェックをおこなうか、暗号鍵の管理方法の安全性と平易さ、暗号化と復号化における演算量、などを考慮して、そのサービスシステム24との通信において、最適なりすまし防止方法が選択され、そのなりすまし防止方法に対応する確認コードが生成される。なお、なりすまし防止の処理については、図6と図7を参照して後述する。

[0069] ステップS82において、なりすまし防止モジュール64は、確認コードを、通信モジュール61に対して出力し、ステップS25において、通信モジュール61によりこれが取得される。ステップS26において、通信モジュール61は、ステップS25で取得された確認コードをサービスシステム24に送信し、ステップS3においてこれが受信される。

[0070] なお、このとき、PK22(のユーザ)を特定するユーザIDも合わせてサービスシステム24により受信され、サービスシステム24は、ユーザIDと、そのユーザIDに対応す

る確認コードを記憶する。ユーザIDは、サービスシステム24がPK22(のユーザ)を特定できるものであれば、どのような形式でもよい。例えば、ユーザIDが所定の数字の組み合わせにより構成されるようにしてもよいし、所定の文字列で構成されるようにしてもよい。また、複数のサービスシステム24に対応して、それぞれ別のユーザIDが生成されるようにしてもよい。

[0071] ステップS46において、許可項目確認モジュール63は、DBアクセスモジュール66に対して、サービスID登録要求を出力し、ステップS101において、DBアクセスモジュール66により、これが受信される。ステップS102において、DBアクセスモジュール66は、図9を参照して後述するサービスID登録処理を実行し、これによりサービスIDが登録され、サービスIDに対応するPMDが生成される。

[0072] このようにして、PK22において、サービスシステム24に対応するサービスIDが登録される。サービスIDが登録されるとき、そのサービスシステム24により、読み出される、または変更されるPMDのメタデータがユーザに提示されるようにしたので、ユーザは、より安心してサービスを受けることができる。また、PK22が、そのサービスIDが登録されたサービスシステム24と次回に通信するときは、確認コードに基づいて、なりすまし防止処理を行うことができる。同様に、サービスシステム24が、そのユーザIDが登録されたPK22と次回に通信するときは、確認コードに基づいて、なりすまし防止処理を行うことができる。

[0073] 次に、図6と図7を参照して、PK22が、既にサービスIDが登録されているサービスシステム24との通信を行うときのなりすまし防止の処理について説明する。

[0074] 図6は、PK22とサービスシステム24の間のなりすまし防止方法として、合言葉による認証が採用されている場合のなりすまし防止の処理の流れを説明するアローチャートである。この例では、PK22において、サービスシステム24がなりすましではないことを確認し、その後サービスシステム24において、PK22がなりすましではないことを確認する。そして、PK22とサービスシステム24において、それぞれがなりすましではないことが確認できた後、PMDの読み出し、または変更の処理を行う。

[0075] 合言葉は、所定の文字列またはコードなどであり、PK22において、サービスIDの登録時に、サービスIDに対応する合言葉として、サービスシステム24を認証するた

めの合言葉(サービス合言葉)とPKを認証するための合言葉(PK合言葉)が生成され、PMDB67に記憶されている。また、サービスID登録時にサービス合言葉とPK合言葉が、サービスシステム24にも送信され、サービスシステム24の記憶部128の中のデータベースに、サービス合言葉とPK合言葉が、PK22のユーザIDと関連付けられて記憶されている。

[0076] ステップS201において、サービスシステム24は、接続要求、サービスID、合言葉をPK22に送信し、ステップS221において、PK22の通信モジュールによりこれが受信される。なお、ステップS201においては、上述したサービス合言葉が送信される。ステップS222において、通信モジュール61は、ステップS221で受信した内容をなりすまし防止モジュール64に転送し、ステップS281においてこれが受信される。

[0077] ステップS282において、なりすまし防止モジュール64は、図9を参照して後述するサービスIDマッチング処理を実行し、サービスIDの認識を行い、ステップS283において、DBアクセスモジュール66に対して、サービスIDに対応するユーザIDと合言葉の要求を通知し、ステップS301において、DBアクセスモジュール66によりこれが取得される。なお、ステップS282のサービスマッチング処理はDBアクセスモジュール66で行われるようにしてもよい。

[0078] ステップS302においてDBアクセスモジュール66は、PMDB67からサービスIDに対応するサービス合言葉、PK合言葉、およびユーザIDを読み出し、なりすまし防止モジュール64に出力する。なりすまし防止モジュール64は、ステップS284で取得されたサービス合言葉と、ステップS281で取得された合言葉を比較し、合言葉が一致しないと判定された場合、サービスシステム24が、なりすましである可能性があると判定し、通信モジュール61に対して、通信の拒否を表す拒否信号を通知し、ステップS223において、通信モジュール61により、これが取得される。ステップS224において、通信モジュール61は、拒否信号をサービスシステム24に送信し、ステップS202において、サービスシステム24により、これが受信される。

[0079] このように、通信を開始するとき、サービスシステム24からサービスIDに対応する合言葉が送信されなかった場合、PK22により、その通信は拒否される。

[0080] 一方、ステップS285において、サービス合言葉が一致すると判定された場合、なり

すまし防止モジュール64は、ステップS286において、サービスシステム24が、なりすましでないことが確認できたことを表すコード(OK)と、ユーザID、ステップS284で取得されたPK合言葉を、通信モジュール61に出力し、ステップS225において、通信モジュール61により、これが取得される。ステップS226において、通信モジュール61は、ステップS225で取得された情報を、サービスシステム24に送信し、ステップS203において、サービスシステム24によりこれが受信される。

[0081] ステップS204において、サービスシステム24は、ステップS203で受信されたユーザIDに対応するPK合言葉を、自身のデータベースから読み出し、ステップS203で受信された合言葉と比較し、合言葉が一致しているか否かを判定する。ステップS204において、合言葉が一致しないと判定された場合、PK22が、なりすましである可能性があるかと判定し、サービスシステム24は、通信の拒否を表す拒否信号をPK22に送信する。PK22では、通信モジュール61を介して、なりすまし防止モジュール64によりステップS287で、これが受信される。

[0082] このように、通信を開始するとき、PK22からユーザIDに対応する合言葉が送信されなかった場合、サービスシステム24により、その通信は拒否される。

[0083] 一方、ステップS204において、合言葉が一致すると判定された場合、サービスシステム24は、PK22がなりすましでないことが確認できたと判定し、ステップS205において、PK22に対してPMDの読み出し要求を送信し、ステップS227において、PK22の通信モジュール61により、これが受信される。ステップS228において、通信モジュール61は、ステップS227で受信された内容を、DBアクセスモジュール66に対して出力し、ステップS303において、DBアクセスモジュール66により、これが取得される。

[0084] ステップS304において、DBアクセスモジュール66は、サービスシステム24から読み出し要求のあったPMD(のメタデータ)が、サービスシステム24に対応するサービスIDに対して、読み出しが許可されているPMDであるか否かを確認し、読み出しが許可されているPMDである場合、そのPMDをPMDB67から読み出す。そして、ステップS305において、DBアクセスモジュール66は、読み出したPMDを通信モジュール61に対して出力し、ステップS229において、通信モジュール61により、これが

取得される。

- [0085] ステップS230において、通信モジュール61は、ステップS229で取得された情報を、サービスシステム24に対して送信し、ステップS206において、サービスシステム24により、これが受信される。
- [0086] ステップS207において、サービスシステム24は、ステップS206で取得されたPMDに基づいて、各種の処理(サービス対応処理)を実行する。ステップS207の処理の結果、PMDの変更が必要となる場合、サービスシステム24は、ステップS208において、PMDの内容を変更し、PK22に対して送信し、ステップS231において、PK22の通信モジュール61により、これが受信される。
- [0087] ステップS232において、通信モジュール61は、ステップS231で受信された情報をDBアクセスモジュール66に対して出力し、ステップS306においてDBアクセスモジュール66によりこれが取得される。そして、ステップS307において、DBアクセスモジュール66は、ステップS306で取得されたPMDが、サービスシステム24に対応するサービスIDに対して変更許可のあるPMDであるか否かを確認し、変更許可のあるPMDである場合、PMDB67の中の対応するPMDの変更を行う(変更内容に対応して更新する)。
- [0088] このようにすることで、PMDの読み出し、または変更を行う前に、なりすましの確認することができるので、安全なサービスを提供することができる。さらに、PK22によるサービスシステム24のなりすましの確認と、サービスシステム24によるPK22のなりすましの確認が行われるようにしたので、より安全なサービスを提供することができる。
- [0089] 次に図7を参照して、PK22が、既にサービスIDが登録されているサービスシステム24との通信を行うときのなりすまし防止の処理の別の例について説明する。図7は、PK22とサービスシステム24の間のなりすまし防止方法として、公開鍵により暗号化された情報による認証が採用されている場合のなりすまし防止の処理の流れを説明するアローチャートである。
- [0090] この例においても、PK22において、サービスシステム24がなりすましではないことを確認し、その後サービスシステム24において、PK22がなりすましではないことを確認する。そして、PK22とサービスシステム24において、それぞれがなりすましではな

いことが確認できた後、PMDの読み出し、または変更の処理を行う。

- [0091] また、この例においては、PK22とサービスシステム24は、RSAなどの公開鍵方式の暗号アルゴリズムによる情報の暗号化または複合化の処理を実行する機能を有しており、サービスIDを登録するとき、PK22により、サービスシステム24の公開鍵が、サービスシステム24のサービスIDに関連付けられてPMDB67に記憶されており、サービスシステム24により、PK22の公開鍵が、PK22のユーザIDに関連づけられて記憶部128の中のデータベースに記憶されている。PK22とサービスシステム24の秘密鍵は、それぞれの記憶部108または128に記憶されている。
- [0092] ステップS401において、サービスシステム24は、接続要求とサービスIDをPK22に送信し、ステップS421において、PK22の通信モジュールによりこれが受信される。ステップS422において、通信モジュール61は、ステップS421で受信した情報をなりすまし防止モジュール64に転送し、ステップS481においてこれが受信される。
- [0093] ステップS482において、なりすまし防止モジュール64は、図10を参照して後述するサービスIDマッチング処理を実行し、サービスIDの認識を行い、ステップS483において、DBアクセスモジュール66に対して、サービスIDに対応するユーザID、PKの秘密鍵、およびサービスシステム24の公開鍵の要求を通知し、ステップS501において、DBアクセスモジュール66によりこれが取得される。なお、ステップS482のサービスマッチング処理は、DBアクセスモジュール66において実行されるようにしてもよい。
- [0094] ステップS502において、DBアクセスモジュール66は、サービスIDに対応するサービスシステム24の公開鍵と、PKの秘密鍵をPMDB67から読み出し、なりすまし防止モジュール64に対して出力し、ステップS484において、なりすまし防止モジュール64により、これが取得される。
- [0095] ステップS485において、なりすまし防止モジュール64は、サービスシステム24を認証するため、所定のコードで構成されるチャレンジコードを生成し、チャレンジコードをサービスIDに対応する公開鍵(サービスシステム24の公開鍵)で暗号化し、暗号化されたチャレンジコードとユーザIDを通信モジュール61に対して出力し、ステップS423において、通信モジュール61により、これが取得される。ステップS424におい

て、通信モジュール61は、ステップS423で取得された情報をサービスシステム24に送信し、ステップS402において、サービスシステム24により、これが受信される。

[0096] ステップS403において、サービスシステム24は、ステップS402で受信された、暗号化されたチャレンジコードをサービスシステム24の秘密鍵により復号し、復号されたチャレンジコードをレスポンスコードとし、レスポンスコードをユーザIDに対応する公開鍵(PK22の公開鍵)で暗号化してPK22に対して送信し、ステップS425において、PK22の通信モジュール61により、これが受信される。

[0097] ステップS426において、通信モジュール61は、ステップS425で受信された、暗号化されたレスポンスコードを、なりすまし防止モジュール64に対して出力し、ステップS486において、なりすまし防止モジュール64により、これが取得される。

[0098] ステップS487において、なりすまし防止モジュール64は、ステップS486で取得された、暗号化されたレスポンスコードをPK22の秘密鍵で複合化し、ステップS485で生成したチャレンジコードと比較して、チャレンジコードとレスポンスコードが一致しているか否かを判定し、チャレンジコードとレスポンスコードが一致しないと判定された場合、サービスシステム24が、なりすましである可能性があると判定し、通信モジュール61に対して、通信の拒否を表す拒否信号を通知し、ステップS426において、通信モジュール61により、これが取得される。ステップS427において、通信モジュール61は、拒否信号をサービスシステム24に送信し、ステップS404において、サービスシステム24により、これが受信される。

[0099] このように、通信を開始するとき、PK22からチャレンジコードが送信され、サービスシステム24からチャレンジコードと一致するレスポンスコードが返信されなかった場合、PK22により、その通信は拒否される。

[0100] 一方、ステップS487において、チャレンジコードとレスポンスコードが一致すると判定された場合、なりすまし防止モジュール64は、ステップS488において、サービスシステム24がなりすましでないことが確認できたことを表すコード(OK)を、通信モジュール61を介して、サービスシステム24に送信し、ステップS405において、サービスシステム24によりこれが受信される。

[0101] ステップS406において、サービスシステム24は、PK22を認証するため、所定のコ

ードにより構成されるチャレンジコードを生成し、チャレンジコードをユーザIDに対応する公開鍵(PK22の公開鍵)で暗号化し、暗号化されたチャレンジコードをPK22に対して送信し、ステップS429において、PK22の通信モジュール61によりこれが受信される。ステップS430において、通信モジュール61は、ステップS429で受信された情報をなりすまし防止モジュール64に対して出力し、ステップS489において、なりすまし防止モジュール64により、これが取得される。

[0102] ステップS490において、なりすまし防止モジュール64は、ステップS489で受信された、暗号化されたチャレンジコードをPK22の秘密鍵で復号し、復号されたチャレンジコードをレスポンスコードとし、レスポンスコードをサービスIDに対応する公開鍵(サービスシステム24の公開鍵)で暗号化し、通信モジュール61に対して出力し、ステップS431において、通信モジュール61により、これが取得される。ステップS432において、通信モジュール61は、ステップS431で取得された情報をサービスシステム24に対して送信し、ステップS407において、サービスシステム24によりこれが受信される。

[0103] ステップS408において、サービスシステム24は、ステップS407で受信された、暗号化されたレスポンスコードを、サービスシステム24の秘密鍵で復号し、復号されたレスポンスコードが、ステップS406で生成されたチャレンジコードと一致するか否かを判定し、チャレンジコードとレスポンスコードが一致しないと判定された場合、PK22が、なりすましである可能性があるかと判定し、PK22に対して、通信の拒否を表す拒否信号を送信し、ステップS433で、PK22の通信モジュール61により、これが受信される。ステップS434において、通信モジュール61は、ステップS433で受信された情報を、なりすまし防止モジュール64に対して送信し、ステップS491において、なりすまし防止モジュール64により、これが取得される。

[0104] このように、通信を開始するとき、サービスシステム24からチャレンジコードが送信され、PK22からチャレンジコードと一致するレスポンスコードが返信されなかった場合、サービスシステム24により、その通信は拒否される。

[0105] 一方、ステップS408において、チャレンジコードとレスポンスコードが一致すると判定された場合、サービスシステム24は、PK22がなりすましでないことが確認できたと

判定し、ステップS409において、PK22に対してPMDの読み出し要求を送信し、ステップS435において、PK22の通信モジュール61により、これが受信される。ステップS436において、通信モジュール61は、ステップS435で受信された情報を、DBアクセスモジュール66に対して出力し、ステップS503において、DBアクセスモジュール66により、これが取得される。

[0106] ステップS504において、DBアクセスモジュール66は、サービスシステム24から読み出し要求のあったPMD(のメタデータ)が、サービスシステム24に対応するサービスIDに対して、読み出しが許可されているPMDであるか否かを確認し、読み出しが許可されているPMDである場合、そのPMDをPMDB67から読み出す。そして、ステップS505において、DBアクセスモジュール66は、読み出したPMDを通信モジュール61に対して出力し、ステップS437において、通信モジュール61により、これが取得される。

[0107] ステップS438において、通信モジュール61は、ステップS437で取得された情報を、サービスシステム24に対して送信し、ステップS410において、サービスシステム24により、これが受信される。

[0108] ステップS411において、サービスシステム24は、ステップS410で取得されたPMDに基づいて、各種の処理(サービス対応処理)を実行する。ステップS411の処理の結果、PMDの変更が必要となる場合、サービスシステム24は、ステップS412において、PMDの内容を変更し、PK22に対して送信し、ステップS439において、PK22の通信モジュール61により、これが受信される。

[0109] ステップS440において、通信モジュール61は、ステップS439で受信された情報をDBアクセスモジュール66に対して出力し、ステップS506においてDBアクセスモジュール66によりこれが取得される。そして、ステップS507において、DBアクセスモジュール66は、ステップS506において取得されたPMDが、サービスシステム24に対応するサービスIDに対して変更許可のあるPMDであるか否かを確認し、変更許可のあるPMDである場合、PMDB67の中の対応するPMDの変更を行う(変更内容に更新する)。

[0110] このようにすることで、PMDの読み出し、または変更を行う前に、PK22とサービス

システム24が、互いになりすましでないことを確認することができるので、安全なサービスを提供することができる。また、PK22またはサービスシステム24を認証するためのチャレンジコードとレスポンスコードは、それぞれPK22とサービスシステム24の公開鍵と秘密鍵により、暗号化または復号化されるので、仮に、第三者に通信が傍受されても、チャレンジコードとレスポンスコードの内容は、秘匿されるので、より確実になりすましを防止することができる。

[0111] なお、図7においては、公開鍵方式の暗号アルゴリズムにより、チャレンジコードとレスポンスコードを暗号化する例について説明したが、PK22とサービスシステム24が、公開鍵方式の暗号アルゴリズムではなく、共通鍵方式の暗号アルゴリズムで、情報の暗号化または複合化の処理を実行する機能を有し、PK22とサービスシステム24において、互いに共通の暗号鍵が保持され、チャレンジコードとレスポンスコードが、その鍵で暗号されることにより通信が行われるようにしてもよい。

[0112] この場合、サービスIDの登録を行うとき、PK22により、そのサービスIDに対応する暗号鍵が生成され、サービスIDに関連付けられてPMDB67に記憶されると同時に、同じ暗号鍵が、サービスシステム24に送信され、PK22のユーザIDに対応付けられてサービスシステム24のデータベースに記憶される。

[0113] 暗号鍵が漏洩した場合、PK22とサービスシステム24は、暗号鍵を変更する必要がある。例えば、あるサービスシステムの公開鍵方式の暗号アルゴリズムで用いられる秘密鍵が漏洩した場合、そのサービスシステムを利用する多数のPKにおいて、サービスIDに対応する公開鍵を変更する必要がある。しかし、PK22とサービスシステム24において、互いに共通の暗号鍵が保持されるようにすれば、暗号鍵が漏洩した場合でも、その鍵を使うPK22とサービスシステム24の暗号鍵のみ変更するだけで、対処することができる。

[0114] なお、図7においては、チャレンジコードとレスポンスコードが暗号化される例について説明したが、通信内容の全てが暗号化されるようにしてもよい。

[0115] また、図7の例では、秘密鍵(または共通鍵)がPK22の中(PMDB67)に保管される例について説明したが、PK22とは異なる機器、例えば、図1のSB26に保管されるようにしてもよい。この場合、サービスシステム24と通信を行うに先立って、PK22とS

B26が通信を行い、SB26からPK22に秘密鍵が送信される(このとき、SBはPKに対して、1つのサービスシステムとして通信する)。PKは、一定時間経過すると秘密鍵を消去する処理を行い、必要なときには、都度、SB26と通信して秘密鍵を取得する。

[0116] この場合のPK22の鍵管理処理について、図8を参照して説明する。この処理は、PK22が、サービスシステム24との通信を行うとき、図7に示されるようななりすまし防止の処理が行われるのに先立って実行される。

[0117] ステップS681において、PK22のCPU101は、SB26から鍵を取得し、記憶部108に記憶する。ステップS682において、CPU101は、所定の時間(例えば、1時間)が経過したか否かを判定し、所定の時間が経過したと判定されるまで待機する。ステップS682において、所定の時間が経過したと判定された場合、ステップS683において、記憶部108に記憶されている鍵を消去する。

[0118] このようにして、鍵の管理が行われる。このようにすることで、例えば、PK22が盗まれた場合でも、秘密鍵が漏洩することを防止することができる。

[0119] 次に、図9を参照して、図5のステップS102のサービスID登録処理の詳細について説明する。多くの場合、サービスシステム24は、インターネット21に接続されたサーバである。この処理は、図5のステップS102において、サービスシステム24を特定する情報として、サービスシステム24を構成するサーバのURI(Uniform Resource Identifiers)が取得された場合、実行される。

[0120] ステップS801において、DBアクセスモジュール66は、URIを取得する。ステップS802において、DBアクセスモジュール66は、マスクがあるか否かを判定する。マスクは、URIの中の所定のセグメントを示す情報であり、例えば、ユーザにより、予め設定されている。

[0121] URIは、インターネット21でのユニークなアドレスとして管理されており、全世界でのさまざまなサーバに、例えば、「http://aaa.bbb.ccc」のようなネーミングが行われている。ここで、「http://aaa.bbb.」(または「http://aaa.」)の部分は、通常そのサーバが提供するサービスに対応する会社名などを示し、cccの部分は、そのサービスの内容に応じて変化する。例えば、ユーザが、特定の会社が行うさまざまなサービスすべてに

対して、PMDの読み出しまたは変更を許可する場合、「http://aaa.bbb.」の部分のみを参照してサービスシステム24を特定すればよい。このような場合、マスクとして、下位1セグメント(「ccc」の部分)が設定される。

[0122] ステップS802において、マスクがあると判定された場合、ステップS804に進み、DBアクセスモジュール66は、サービスIDとして、マスクされた部分を取り除いたURI(「http://aaa.bbb.」の部分)を登録する。ステップS802において、マスクがないと判定された場合、ステップS803に進み、DBアクセスモジュール66は、サービスIDとしてURIをそのまま(「http://aaa.bbb.ccc」)登録する。

[0123] ステップS803またはS804の処理の後、ステップS805に進み、DBアクセスモジュール66は、サービスIDと、そのサービスIDに対応するサービスシステム24において、利用される個人関連情報を関連づけて、そのサービスIDに対応するPMDを生成する。

[0124] このようにして、サービスIDが登録される。

[0125] 次に、図10を参照して、図6のステップS282、または図7のステップS482のサービスIDマッチング処理の詳細について説明する。なお、この例では、サービスIDマッチング処理が、DBアクセスモジュール66により実行されるものとする。

[0126] ステップS841において、DBアクセスモジュール66は、URIを取得する。ステップS842において、DBアクセスモジュール66は、URIをサービスIDと同じ長さに切り出す。このとき、例えば、URIとして「http://aaa.bbb.ccc」が取得された場合、「http://aaa.bbb.」の部分が切り出される。ステップS843において、DBアクセスモジュール66は、ステップS842で切り出されたURIを登録されたサービスIDと比較する。

[0127] ステップS844において、DBアクセスモジュール66は、ステップS843における比較の結果、サービスIDと一致したか否かを判定し、一致しないと判定された場合、ステップS846に進み、登録されたサービスIDを全てチェックしたか否かを判定し、まだ、全てチェックしていないと判定された場合、ステップS847に進み、ステップS842で切り出されたURIを次のサービスIDと比較し、ステップS844に戻る。

[0128] ステップS844において、ステップS843における比較の結果、サービスIDと一致したと判定された場合、ステップS845に進み、一致したサービスIDを、サービスシステ

ム24を特定するサービスIDとして認識する。

[0129] ステップS846において、登録されたサービスIDを全てチェックしたと判定された場合、ステップS848に進みDBアクセスモジュール66は、このサービスの拒否を通知する。

[0130] このようにして、サービスIDの認識が行われる。

[0131] ところで、上述したようにPK22には、PMDとして個人関連情報が記憶されており、仮にPK22を盗まれても、悪用されないように、PK22の内部に保存されたPMDが暗号化されて秘匿されることが好ましい。

[0132] 例えば、PMDをPK22の公開鍵で暗号化しておいて、必要に応じて秘密鍵を用いて復号するようにしてもよい。秘密鍵は、SBに保管されているので、PK22とSBの通信が途絶えた場合には、PKの中に秘密鍵がないことになり、PMDを読み出したり変更したりすることができない。

[0133] あるいはまた、PK22が、ユーザ20を認証し、正当なユーザ20であると確認された場合だけ、PMDが利用可能とされるようにしてもよい。

[0134] 例えば、一定の時間内に、ワンタイムパスワード(固定パスワードでもよい)または後述する生体認証により、そのユーザが正当なユーザであることが確認できない場合、PMDの読み出しまたは変更の制御が禁止されるようにしてもよいし、PMDが自動的に消去されるようにしてもよい。PMDが消去された場合、ワンタイムパスワードまたは生体認証により、正当なユーザであることが確認されたとき、pBase23に保存されているPMDを利用して、PK22のPMDが回復される。

[0135] 図11は、PK22によるユーザ20の認証方法の例を示す図である。図11Aは、PK22は、ユーザ20が常に携帯するチップ201を検知してユーザの認証を行う例を示す図である。チップ201は、例えば、特定の周波数の電波を常に発信する十分に小さい発信機であり、ユーザ20により常に携帯されている。この場合、PK22には、チップ201が発信する電波を検知するセンサが設けられており、センサは、PK22の入力部106に接続されているものとする。PK22は、予め登録されたチップ201が発信する周波数の電波を検知することによりユーザ20を認証する。

[0136] この場合、PK22がユーザ20を認証するユーザ認証処理1について、図12を参照

して説明する。この処理は、例えば、PK22の電源がONの状態である間、常に継続して実行される。

- [0137] ステップS901において、PK22のCPU101は、センサにより検知された信号を登録されているチップ201の信号と比較する。ステップS902において、CPU101は、ステップS901の比較の結果、信号が一致したか否かを判定し、一致しないと判定された場合、ステップS901に戻る。
- [0138] ステップS902において、信号が一致したと判定された場合、ステップS903に進み、ユーザ認証情報を記憶する。このとき、ユーザ20を認証したことを表す情報が、現在時刻(日時)とともに、ユーザ認証情報として、記憶部108に記憶される。
- [0139] ステップS904において、CPU101は、所定の時間(例えば、1時間)が経過したか否かを判定し、所定の時間が経過したと判定されるまで待機する。ステップS904において、所定の時間が経過したと判定された場合、ステップS905に進み、CPU101は、ユーザ認証情報を削除する。その後、処理は、ステップS901に戻り、それ以降の処理が繰り返し実行される。
- [0140] あるいはまた、ユーザの生体的特徴(指紋、声紋、虹彩、歩紋等)を用いた認証、すなわち生体認証が行われるようにしてもよい。図11Bは、ユーザ20の生体的特徴としての歩紋202を検知することで、ユーザ20を認証する例を示す図である。この場合、PK22には、準静電界の変化を検知するセンサが設けられており、センサは、PK22の入力部106に接続されているものとする。PK22は、予め登録されたユーザ20の歩紋を検知することによりユーザ20を認証する。なお、歩紋とは、人が歩行するとき、人体に発生する準静電界の変化パターンであり、このパターンを用いて人を認識することができる(例えば、特開2003-58857 歩行検出方法、歩行検出装置 参照)。
- [0141] この場合、PK22がユーザ20を認証するユーザ認証処理2について、図13を参照して説明する。この処理は、例えば、PK22の電源がONの状態である間、常に継続して実行される。
- [0142] ステップS921において、PK22のCPU101は、センサにより検知された準静電界の変化パターン(歩紋)を登録されているユーザ20の歩紋と比較する。ステップS902において、CPU101は、ステップS921の比較の結果、歩紋が一致したか否かを判

定し、一致しないと判定された場合、ステップS921に戻る。

- [0143] ステップS922において、歩紋が一致したと判定された場合、ステップS923に進み、ユーザ認証情報を記憶する。このとき、ユーザ20を認証したことを表す情報が、現在時刻(日時)とともに、ユーザ認証情報として、記憶部108に記憶される。
- [0144] ステップS924において、CPU101は、所定の時間(例えば、1時間)が経過したか否かを判定し、所定の時間が経過したと判定されるまで待機する。ステップS924において、所定の時間が経過したと判定された場合、ステップS925に進み、CPU101は、ユーザ認証情報を削除する。その後、処理は、ステップS921に戻り、それ以降の処理が繰り返し実行される。
- [0145] このようにして、所定の時間毎に、PK22によりユーザ20が認証される。以上においては、チップ201または歩紋202によりユーザ20が認証される例について説明したが、ユーザの認証方法は、これに限られるものではない。例えば、PK22を、近傍のパーソナルコンピュータと通信させ、パーソナルコンピュータから入力されるパスワードに基づいて、ユーザが認証されるようにしてもよい。
- [0146] また、上述したように、PK22においては、ユーザが正当なユーザであることが確認(認証)できない場合、PMDが自動的に消去されるようにすることができる。この場合のPMD管理処理について、図14を参照して説明する。この処理は、PK22において、PMDが必要となる都度、実行される。なお、実行に先立って、PK22のCPU101により、図12のステップS903、または図13のステップS923で記憶されたユーザ認証情報が、記憶部108の中に存在する(ユーザが認証されている)ことが確認される。
- [0147] ステップS941において、CPU101は、pBase23と通信し、pBase23からPMDを取得し、記憶部108に記憶する。ステップS942においてCPU101は、ステップS941で、PMDを取得してから所定の時間(例えば、3時間)が経過したか否かを判定し、所定の時間が経過したと判定されるまで待機する。
- [0148] ステップS942において、所定の時間が経過したと判定された場合、ステップS943に進み、CPU101は、ユーザが認証されたか否かを判定する。このとき、図12のステップS903、または図13のステップS923で記憶されたユーザ認証情報が、記憶部1

08の中に存在するか否かが判定され、ユーザ認証情報が存在する場合、ユーザが認証されたと判定され、ユーザ認証情報が存在しない場合、ユーザが認証されなかったと判定される。ステップS943において、ユーザが認証されたと判定された場合、処理はステップS942に戻り、それ以降の処理が繰り返し実行される。

[0149] ステップS943において、ユーザが認証されなかったと判定された場合、CPU101は、ステップS944に進み、ステップS941で取得したPMDを記憶部108から消去する。

[0150] このようにして、PK22において、ユーザが正当なユーザであることが確認(認証)できない場合、PMDが自動的に消去される

[0151] ところで、上述したように、PK22は、ユーザが簡単に持ち運べる小型のコンピュータであり、PK22に、いろいろなインタフェース(例えば、ディスプレイ、タッチパッドなど)を直接配置すると、PK22の大きさが大きくなり、重量も重くなるので、ユーザが簡単に持ち運ぶことができなくなる恐れがある。

[0152] このために、PK22に直接配置されるインタフェースは、できるだけ小さくし、例えば、複雑な情報の入力または出力に用いられるインタフェースとして、PK22の外部にある機器などを利用できることが望ましい。

[0153] 図15は、PK22が外部コンソール221と、外部コンソール222を入力または出力に用いられるインタフェースとして利用する例を示す図である。この場合、PK22は、外部コンソール221および222と、RF通信などの無線通信を行う。外部コンソール221には、項目リスト画面242とプッシュスイッチ241が設けられており、例えば、項目リスト画面242にPMDのリストが表示され、プッシュスイッチ241をユーザが操作することにより、項目リスト画面242に表示されたPMDに対するアクセス許可が指定される。

[0154] 外部コンソール222には、タッチパッド付ディスプレイ261が設けられており、タッチパッド付ディスプレイ261に表示される操作卓を変化させることができ、例えば、サービスIDに対応して異なるインタフェースが提供される。

[0155] なお、外部コンソール221または222は、PK22に対して、インタフェースサービスを提供する、サービスシステムの一つとみなすこともできる。この場合、PK22は、外部コンソール221または222の制御コードを記憶するサーバをサービスシステムとし

て通信を行い、外部コンソール221または222の制御コードを取得する。その後、外部コンソール221または222をサービスシステムとして通信を行い、外部コンソール221または222に制御コードを実装させる。

- [0156] このように、サービスシステム24から、PK22を介して、外部コンソール221などの周辺機器を制御させることにより、図16に示されるように、サービスシステム24に対して、周辺機器(外部コンソール221など)のアドレスなどのアクセスキー280を隠蔽して、サービスの提供を受けることができる。
- [0157] 次に、図17を参照して、PK22、pBase23、およびサービスシステム24によりPMDが利用される様子を説明する。PK22は、上述したように、RF通信、準静電界通信、光通信などの無線通信により、インターネット21に接続されたアクセスポイント25と通信し、インターネット21に接続される。このとき、図17Aに示されるように、インターネット21を介してPK22とpBase23が接続され、両者のPMDの内容が比較され、PMDの同期が行われる。例えば、PK22のPMDの内容が更新されている場合、pBase23のPMDも同様に更新され、PMDの同期が行われる。なお、PMDの同期の詳細については後述する。
- [0158] また、例えば、PK22に記憶しきれないPMDをpBase23に記憶させ、図17Bに示されるように、サービスシステム24は、pBase23のPMDを参照し、PK22のユーザに対するサービスを行うようにすることもできる。
- [0159] あるいはまた、PK22をインターネット21に接続できない場合、pBase23には、PK22のPMDが記憶されているので、図17Cに示されるように、pBase23を、PK22に代わってサービスシステム24と通信させることにより(PK22の代用としてpBase23を利用して)、ユーザはサービスの提供を受けることができる。
- このような場合、PK22に代わったpBase23とサービスシステム24の間でなりすまし防止の処理が行われ、PMDの送受信が行われる。
- [0160] 図18と図19を参照して、図17Cの場合の、pBase23とサービスシステム24との間の処理の流れを説明する。図18の例では、PK22(のユーザ)に対応するPMDが、pBase23の記憶部128の中のデータベースに記憶されているものとし、サービスシステム24との間で、なりすまし防止方法として、図6の場合と同様に合言葉による認証

が採用されているものとする。

- [0161] 同図においては、pBase23において、サービスシステム24がなりすましではないことを確認し、その後サービスシステム24において、pBase23がなりすましではないことを確認する。そして、pBase23とサービスシステム24において、それぞれがなりすましではないことが確認できた後、PMDの読み出し、または変更の処理を行う。また、この例においては、PK合言葉、サービスシステム合言葉、PK22のユーザID、およびサービスシステム24のサービスIDは、やはりPK22のPMDとして、pBase23の記憶部128の中のデータベースに記憶されているものとする。
- [0162] ステップS1101において、サービスシステム24は、接続要求、サービスID、合言葉をpBase23に送信し、ステップS1121において、これが受信される。ステップS1122において、pBase23は、図10を参照して上述したサービスIDマッチング処理を実行し、サービスIDの認識を行い、サービスIDに対応するサービス合言葉、PK合言葉、およびユーザIDを記憶部128のデータベースから読み出す。ステップS1123において、pBase23は、ステップS1121で取得されたサービス合言葉と、記憶部128のデータベースから読み出されたサービス合言葉を比較し、サービス合言葉が一致しないと判定された場合、サービスシステム24が、なりすましである可能性があると判定し、サービスシステム24に対して、通信の拒否を表す拒否信号を送信し、ステップS1102において、これが受信される。
- [0163] このように、通信を開始するとき、サービスシステム24からサービスIDに対応する合言葉が送信されなかった場合、pBase23により、その通信は拒否される。
- [0164] 一方、ステップS1123において、サービス合言葉が一致すると判定された場合、pBase23は、ステップS1124において、サービスシステム24がなりすましでないことが確認できたことを表すコード(OK)と、ユーザID、およびユーザIDに対応するPK合言葉を、サービスシステム24に送信し、ステップS1103において、これが受信される。
- [0165] ステップS1104において、サービスシステム24は、ステップS1103で受信されたユーザIDに対応するPK合言葉を、自身のデータベースから読み出し、ステップS1103で受信されたPK合言葉と比較し、PK合言葉が一致しているか否かを判定する。ス

テップS1104において、PK合言葉が一致しないと判定された場合、pBase23が、なりすましである可能性があると判定し、サービスシステム24は、通信の拒否を表す拒否信号をpBase23に送信し、ステップS1125で、これが受信される。

[0166] このように、通信を開始するとき、pBase23からユーザIDに対応する合言葉が送信されなかった場合、サービスシステム24により、その通信は拒否される。

[0167] 一方、ステップS1104において、PK合言葉が一致すると判定された場合、サービスシステム24は、pBase23がなりすましでないことが確認できたと判定し、ステップS1105において、pBase23に対してPMDの読み出し要求を送信し、ステップS1126において、これが受信される。ステップS1127において、pBase23は、サービスシステム24から読み出し要求のあったPMDが、サービスシステム24に対応するサービスIDに対して、読み出しが許可されているPMDであるか否かを確認し、読み出しが許可されているPMDである場合、そのPMDを記憶部128のデータベースから読み出す。そして、ステップS1128において、pBase23は、読み出したPMDをサービスシステム24に対して送信し、ステップS1106において、これが受信される。

[0168] ステップS1107において、サービスシステム24は、ステップS1106で取得されたPMDに基づいて、各種の処理(サービス対応処理)を実行する。ステップS1107の処理の結果、PMDの変更が必要となる場合、サービスシステム24は、ステップS1108において、PMDの内容を変更し、pBase23に対して送信し、ステップS1129において、これが受信される。そして、ステップS1130において、pBase23は、ステップS1129において受信されたPMDが、サービスシステム24に対応するサービスIDに対して変更許可のあるPMDであるか否かを確認し、変更許可のあるPMDである場合、記憶部128のデータベースの中の対応するPMDの変更を行う(変更内容に更新する)。

[0169] このようにして、PMDの読み出し、または変更を行う前に、PK22に代わって、pBase23が、図6の場合と同様に、サービスシステム24との間でなりすましの確認を行うので、安全なサービスを提供することができる。

[0170] 次に図19を参照して、図17Cの場合の、pBase23とサービスシステム24との間の処理の流れの別の例を説明する。この例では、PK22(のユーザ)に対応するPMD

が、pBase23の記憶部128に記憶されているものとし、サービスシステム24との間で、なりすまし防止方法として、図7の場合と同様に公開鍵により暗号化された情報による認証が採用されているものとする。

[0171] 同図においては、pBase23において、サービスシステム24がなりすましではないことを確認し、その後サービスシステム24において、pBase23がなりすましではないことを確認する。そして、pBase23とサービスシステム24において、それぞれがなりすましではないことが確認できた後、PMDの読み出し、または変更の処理を行う。また、この例においては、pBase23とサービスシステム24は、RSAなどの公開鍵方式の暗号アルゴリズムによる情報の暗号化または複合化の処理を実行する機能を有しているものとする。なお、PK22の秘密鍵、サービスシステム24の公開鍵、PK22のユーザID、およびサービスシステム24のサービスIDは、PK22のPMDとしてpBase23の記憶部128の中のデータベースに記憶されているものとする。

[0172] ステップS1861において、サービスシステム24は、接続要求とサービスIDをpBase23に送信し、ステップS1881において、これが受信される。ステップS1882において、pBase23は、図10を参照して上述した場合と同様に、サービスIDマッチング処理を実行し、サービスIDの認識を行い、サービスIDに対応するユーザID、サービスシステム24の公開鍵、PK22の秘密鍵を取得する。

[0173] ステップS1883において、pBase23は、サービスシステム24を認証するため、所定のコードで構成されるチャレンジコードを生成し、チャレンジコードをサービスIDに対応する公開鍵(サービスシステム24の公開鍵)で暗号化し、暗号化されたチャレンジコードとユーザIDをサービスシステム24に送信し、ステップS1862において、これが受信される。

[0174] ステップS1863において、サービスシステム24は、ステップS1862で受信された、暗号化されたチャレンジコードをサービスシステム24の秘密鍵により復号し、復号されたチャレンジコードをレスポンスコードとし、レスポンスコードをユーザIDに対応する公開鍵で暗号化してpBase23に対して送信し、ステップS1884において、これが受信される。

[0175] ステップS1885において、pBase23は、ステップS1884で取得された、暗号化さ

れたレスポンスコードをPK22の秘密鍵で複合化し、ステップS1883で生成したチャレンジコードと比較して、チャレンジコードとレスポンスコードが一致しているか否かを判定し、チャレンジコードとレスポンスコードが一致しないと判定された場合、サービスシステム24が、なりすましである可能性があると判定し、通信の拒否を表す拒否信号をサービスシステム24に送信し、ステップS1864において、これが受信される。

[0176] このように、通信を開始するとき、pBase23からチャレンジコードが送信され、サービスシステム24からチャレンジコードと一致するレスポンスコードが返信されなかった場合、pBase23により、その通信は拒否される。

[0177] 一方、ステップS1885において、チャレンジコードとレスポンスコードが一致すると判定された場合、pBase23は、ステップS1886において、サービスシステム24がなりすましでないことが確認できたことを表すコード(OK)を、サービスシステム24に送信し、ステップS1865において、これが受信される。

[0178] ステップS1866において、サービスシステム24は、pBase23(PK22)を認証するため、所定のコードにより構成されるチャレンジコードを生成し、チャレンジコードをユーザIDに対応する公開鍵(PK22の公開鍵)で暗号化し、暗号化されたチャレンジコードをpBase23に対して送信し、ステップS1887において、これが受信される。

[0179] ステップS1888において、pBase23は、ステップS1887で受信された、暗号化されたチャレンジコードをPKの秘密鍵で復号し、復号されたチャレンジコードをレスポンスコードとし、レスポンスコードをサービスIDに対応する公開鍵で暗号化し、サービスシステム24に対して送信し、ステップS1867において、サービスシステム24によりこれが受信される。

[0180] ステップS1868において、サービスシステム24は、ステップS1867で受信された、暗号化されたレスポンスコードを、サービスシステム24の秘密鍵で復号し、復号されたレスポンスコードが、ステップS1866で生成されたチャレンジコードと一致するか否かを判定し、チャレンジコードとレスポンスコードが一致しないと判定された場合、pBase23が、なりすましである可能性があると判定し、pBase23に対して、通信の拒否を表す拒否信号を送信し、ステップS1889で、これが受信される。

[0181] このように、通信を開始するとき、サービスシステム24からチャレンジコードが送信さ

れ、pBase23からチャレンジコードと一致するレスポンスコードが返信されなかった場合、サービスシステム24により、その通信は拒否される。

[0182] 一方、ステップS1868において、チャレンジコードとレスポンスコードが一致すると判定された場合、サービスシステム24は、pBase23がなりすましでないことが確認できたと判定し、ステップS1869において、pBase23に対してPMDの読み出し要求を送信し、ステップS1890において、これが受信される。ステップS1891において、pBase23は、サービスシステム24から読み出し要求のあったPMDが、サービスシステム24に対応するサービスIDに対して、読み出しが許可されているPMDであるか否かを確認し、読み出しが許可されているPMDである場合、そのPMDを記憶部128のデータベースから読み出す。そして、ステップS1892において、pBase23は、読み出したPMDをサービスシステム24に対して送信し、ステップS1870において、サービスシステム24により、これが受信される。

[0183] ステップS1871において、サービスシステム24は、ステップS1870で取得されたPMDに基づいて、各種の処理(サービス対応処理)を実行する。ステップS1871の処理の結果、PMDの変更が必要となる場合、サービスシステム24は、ステップS1872において、PMDの内容を変更し、pBase23に対して送信し、ステップS1893において、これが受信される。そして、ステップS1894において、pBase23は、ステップS1893において受信されたPMDが、サービスシステム24に対応するサービスIDに対して変更許可のあるPMDであるか否かを確認し、変更許可のあるPMDである場合、記憶部128のデータベースの中の対応するPMDの変更を行う(変更内容に更新する)。

[0184] このようにして、PMDの読み出し、または変更を行う前に、PK22に代わって、pBase23が、図7の場合と同様に、サービスシステム24との間でなりすましの確認を行うので、安全なサービスを提供することができる。なお、図19においては、公開鍵方式の暗号アルゴリズムにより、チャレンジコードとレスポンスコードを暗号化する例について説明したが、共通鍵方式の暗号アルゴリズムで、チャレンジコードとレスポンスコードが、暗号化されるようにしてもよい。

[0185] 図20A乃至Cは、PMDの詳細な構成例を示す図である。同図に示されるPMDは

、上述したように、あるサービスID(例えば、サービスID1)に関連付けられたメタデータの集合であり、そのメタデータの識別情報であるプロパティと、そのプロパティの内容が記述されている。プロパティ「name」は、サービスID1に対応するサービスシステム24に対して提供されたユーザIDを示すものであり、その内容は「foo」と記述されている。

- [0186] 図20Aにおいて、プロパティ「なりすまし防止方法」は、サービスID1に対応するサービスシステム24との間で行われるなりすまし防止の処理の方法を示すものであり、その内容は、「公開鍵方式」と記述されており、図5のステップS82で生成される確認コードに対応する。プロパティ「サービス公開鍵」は、サービスID1に対応するサービスシステム24の公開鍵を示すものであり、その内容として鍵のデータが記述されている。

プロパティ「PK秘密鍵」は、PK22の秘密鍵を示すものであり、その内容として鍵のデータが記述されている。

- [0187] なお、図20Bに示されるように、プロパティ「なりすまし防止方法」の内容が「共通鍵方式」と記述されている場合、プロパティ「サービス公開鍵」とプロパティ「PK秘密鍵」に代わってプロパティ「共通鍵」がPMDの中に生成され、その内容として鍵データが記述される。さらに、図20Cに示されるように、プロパティ「なりすまし防止方法」の内容が「合言葉方式」と記述されている場合、プロパティ「サービス公開鍵」とプロパティ「PK秘密鍵」に代わってプロパティ「サービス合言葉」とプロパティ「PK合言葉」がPMDの中に生成され、その内容としてそれぞれ、サービス合言葉とPK合言葉が記述される。

- [0188] プロパティ「action」は、サービスID1に対応するサービスで実行される処理プログラムを示すものであり、その内容としてプログラムが記述されている。プロパティ「番組嗜好情報」は、サービスID1に対応するサービスで利用されるユーザの嗜好情報を示すものであり、その内容として、「スポーツ10、バラエティ7、音楽5、その他3」が記述されている。

- [0189] アクセス制御は、そのプロパティの内容に対するアクセス制御情報を記述したものであり、各プロパティに対して、制御情報が設定される。制御情報は、所定のビット数

で構成されるコードであり、例えば、次のように設定される。

- [0190] 第1番目のビットにより、サービスID1に対応するサービスにおける当該プロパティの内容の読み出し可否が設定される。第2番目のビットにより、サービスID1に対応するサービスにおける当該プロパティの内容の変更可否が設定される。第3番目のビットにより、サービスID1以外のサービスIDに対応するサービスにおける当該プロパティの内容の読み出し可否が設定され、第4番目のビットにより、サービスID1以外のサービスIDに対応するサービスにおける当該プロパティの内容の変更可否が設定される。
- [0191] このほか、プログラムの実行可否を設定するビット、自由にアクセスすることが可能である(アクセス制限を設けない)ように設定するビットなどが設けられるようにしてもよい。なお、アクセス制御に設定される制御情報は、アクセス許可情報(図4)としてまとめて記憶されるようにしてもよい。
- [0192] 次に、図21を参照して、PMD更新処理について説明する。この処理は、例えば、サービスシステム24により、コンテンツの視聴サービスが提供された場合、図6のステップS207または図7のステップS411のサービス対応処理の1つとして、この処理がサービスシステム24により実行される。
- [0193] ステップS1901において、CPU121は、視聴された番組(コンテンツ)のメタデータを取得する。ステップS1902において、CPU121は、メタデータのジャンルを分析する。ステップS1903において、CPU121は、ステップS1902で分析されたジャンルがスポーツであるか否かを判定し、ジャンルがスポーツであると判定された場合、ステップS1904に進み、PMDの中のプロパティ「番組嗜好情報」の内容におけるスポーツのポイントをアップさせる。例えば、図20において、「スポーツ10、バラエティ7、音楽5、その他3」とされていたものが、「スポーツ11、バラエティ7、音楽5、その他3」とされる。
- [0194] ステップS1903において、ステップS1902で分析されたジャンルがスポーツではないと判定された場合、CPU121は、ステップS1905において、ジャンルがバラエティであるか否かを判定し、ジャンルがバラエティであると判定された場合、ステップS1906に進み、PMDの中のプロパティ「番組嗜好情報」の内容におけるバラエティのポ

イントをアップさせる。例えば、図20において、「スポーツ10、バラエティ7、音楽5、その他3」とされていたものが、「スポーツ10、バラエティ8、音楽5、その他3」とされる。

[0195] ステップS1905において、ステップS1902で分析されたジャンルがバラエティではないと判定された場合、CPU121は、ステップS1907において、ジャンルが音楽であるか否かを判定し、ジャンルが音楽であると判定された場合、ステップS1908に進み、PMDの中のプロパティ「番組嗜好情報」の内容における音楽のポイントをアップさせる。例えば、図20において、「スポーツ10、バラエティ7、音楽5、その他3」とされていたものが、「スポーツ10、バラエティ7、音楽6、その他3」とされる。

[0196] ステップS1907において、ステップS1902で分析されたジャンルが音楽ではないと判定された場合、CPU121は、ステップS1909に進み、PMDの中のプロパティ「番組嗜好情報」の内容におけるその他のポイントをアップさせる。例えば、図20において、「スポーツ10、バラエティ7、音楽5、その他3」とされていたものが、「スポーツ10、バラエティ7、音楽5、その他4」とされる。

[0197] このようにして、サービスシステム24においてPMDが更新される。更新されたPMDは、PK22に送信され、PK22のPMDが更新される。

[0198] 以上においては、サービスシステム24により、PMD更新処理が実行され、その更新に対応してPK22のPMDが更新される例について説明したが、PK22においてPMD更新処理が実行されるようにしてもよい。あるいはまた、pBase23において、PMD更新処理が実行され、PK22のPMDがpBase23のPMDと同期されるようにしてもよい。

[0199] また、異なるサービスにおいて利用されるPMDの内容を組み合わせることで新たにPMDを生成することも可能である。例えば、サービスID1に対応するサービスと、サービスID2に対応するサービスが、ともに音楽に関するコンテンツを提供するサービスであり、図22に示められるようにサービスID1に対応するPMD301とサービスID2に対応するPMD302の中に、プロパティ「R&B」、プロパティ「jazz」、およびプロパティ「POP」が存在しているものとする。

[0200] この場合、PMD301とPMD302が組み合わせられ、新しいPMD303が生成される。このとき、PMD301のプロパティ「R&B」の内容(15)と、PMD302のプロパティ

「R&B」の内容(17)が足し合わされ、新しいPMD303のプロパティ「R&B」の内容が、「 $32(=17+15)$ 」に設定される。同様に、新しいPMD303のプロパティ「jazz」の内容は、「 $10(=5+5)$ 」に設定され、新しいPMD303のプロパティ「POP」の内容が「 $15=(15+0)$ 」に設定される。

[0201] このようにして、生成された新しいPMD303は、例えば、複数の音楽提供サービスのサービスIDに対応するPMDとして生成され、PK22のユーザの音楽に関する嗜好情報として利用される。

[0202] また、サービスシステム24(または、pBase23)が、複数のPK22のPMDの内容を組み合わせることで新たにPMDを生成することも可能である。図23に、この場合の例を示す。1つのサービスシステム24(または、pBase23)を利用するPKとして、PK22-1とPK22-2が存在し、PK22-1のPMD321と、PK22-2のPMD322の中に、プロパティ「R&B」、プロパティ「jazz」、およびプロパティ「POP」が存在している。このとき、サービスシステム24(または、pBase23)は、PMD321とPMD322を組み合わせることで、新しいPMD323を生成する。

[0203] このとき、PMD321のプロパティ「R&B」の内容(15)と、PMD322のプロパティ「R&B」の内容(17)が足し合わされ、新しいPMD323のプロパティ「R&B」の内容が、「 $32(=17+15)$ 」に設定される。同様に、新しいPMD323のプロパティ「jazz」の内容は、「 $10(=5+5)$ 」に設定され、新しいPMD323のプロパティ「POP」の内容が「 $15=(15+0)$ 」に設定される。

[0204] このようにして、生成された新しいPMD303は、例えば、複数のユーザの共通するPMDとして生成され、まだ嗜好情報が蓄積されていないPK22のユーザに対して、そのユーザの嗜好情報として提供される。

[0205] また、PK22に代えて別の機器から、サービスシステム24を利用することも可能である。このような場合、図24に示されるように、ユーザ20は、PK22を、ユーザ20が指定する端末362と通信させ、コンテンツアクセスパッケージ361を、端末26に送信される。そして、端末362がサービスシステム24と通信を行う。コンテンツアクセスパッケージ361は、サービスシステム24との通信を行うために必要な情報をまとめたパッケージであり、例えば、コンテンツのURI等のコンテンツを特定するユニークなID、コンテ

ンツに関連する簡易な映像または文字列などにより構成されるアイコン、並びにサービスシステム24との間でおこなわれるなりすまし防止の処理に用いられるPK認証情報(例えば、PK22の秘密鍵、ユーザIDなど)、およびサービス認証情報(例えば、サービスシステム24の公開鍵、サービスIDなど)により構成される。

[0206] このようにすることで、ユーザは、端末362を、あたかもPK22であるかのように(仮想のPKとして)利用することができる。

[0207] 次に、図25乃至図27を参照して、PMDを利用して、情報機器に自分の嗜好情報を反映させる(以下、パーソナライズと称する)例について説明する。図25において、PK22のユーザ20が、所定の音楽データに基づいて、音楽の再生を行う音楽再生機器381と、インターネット21に接続され、Webの閲覧などを行うパーソナルコンピュータ382を利用する。

[0208] ユーザ20は、PK22のPMDを利用して、音楽再生装置に、自分の好みの音楽を再生させることができる。この場合、PK22は、音楽再生装置381を1つのサービスシステムとして、インターネット21を介さずに無線通信などにより、音楽再生装置381と通信する。このとき、図6または図7に示されるような処理が、PK22と音楽再生装置381の間で行われる。このとき、例えば、図7のステップS409において、音楽再生装置381から音楽の嗜好情報のPMDの読み出し要求が、PK22に対して送信され、ステップS504で、PK22から音楽の嗜好情報のPMDが音楽再生装置381に対して送信される。そして、ステップS410で、音楽再生装置381が、PK22からPMDを取得すると、ステップS411のサービス対応処理として、ユーザの好みの音楽を再生する処理を実行する。この場合の音楽再生装置381の音楽再生処理について、図26を参照して説明する。

[0209] ステップS1921において、音楽再生装置381は、PK22からPMDを取得する。ステップS1922において、音楽再生装置381は、ステップS1921で取得されたPMDの中の嗜好情報を分析する。ステップS1923において、音楽再生装置381は、嗜好情報に対応する音楽を再生する。

[0210] このように、嗜好情報が含まれるPMDを、音楽再生装置381に送信することで、好みの音楽を再生することができる。PMDは、PK22に記憶されており、いろいろな場

所に持ち運ぶことができるので、その場にある音楽再生装置を自分の好みの音楽を再生する音楽再生装置にパーソナライズすることが可能となる。

- [0211] また、図25において、ユーザ20は、pBase23のPMDを利用して、パーソナルコンピュータ382に、自分の好みのWebページを表示させることができる。この場合、PK22は、サービスシステム24-10と、インターネット21を介して通信する。このとき、図6または図7に示されるような処理が、PK22とサービスシステム24-10の間で行われる。そして、サービスシステム24-10は、PK22のユーザIDに基づいて、ユーザ20のPMDが記憶されているpBase23を特定し、pBase23からユーザ20のPMDを取得する。このとき、図18または図19に示されるような処理が、サービスシステム24-10とpBase23の間で行われ、例えば、図19のステップS1869において、サービスシステム24-10からWebの嗜好情報のPMDの読み出し要求が、pBase23に対して送信され、ステップS1891で、pBase23からWebの嗜好情報のPMDがサービスシステム24-10に対して送信される。
- [0212] ステップS1870で、サービスシステム24-10が、pBase23からPMDを取得すると、ステップS1871のサービス対応処理として、パーソナルコンピュータ382に対して、ユーザの好みに合ったWebサービスを提供する処理を実行する。この場合のサービスシステム24-10のWeb情報提供処理について、図27を参照して説明する。
- [0213] ステップS1941において、サービスシステム24-10は、PK22のユーザIDを取得する。ステップS1942において、サービスシステム24-10は、ステップS1941で取得されたユーザIDに対応するPMDをpBase23から取得する。ステップS1943において、サービスシステム24-10は、ステップS1942で取得されたPMDの嗜好情報を分析する。ステップS1944において、サービスシステム24-10は、嗜好情報に対応するWebサービスを提供する。
- [0214] あるいはまた、サービスシステム24-10がユーザのパーソナルコンピュータ382に作成するテキストファイルであるクッキーが、PMDとしてPK22またはpBase23に保存され、Webの閲覧を行う都度、パーソナルコンピュータ382にクッキーが送信されるようにしてもよい。
- [0215] このようにして、Webサービスが提供される。例えば、容量が大きいためPK22に記

憶することができないPMDをpBase23に記憶しておき、pBse23のPMDに基づいて、パーソナルコンピュータなどの情報機器をパーソナライズすることができる。その結果、ユーザの嗜好をより適確に反映したパーソナライズを行うことができる。

- [0216] 次に、図28を参照して、PMDを利用して、情報機器をパーソナライズする別の例について説明する。同図において、家400には、ユーザ20-1乃至20-3の3人のユーザが住んでおり、それぞれPK22-1乃至22-3を所有している。家400には、リビング400-1、キッチン400-2、および子供部屋400-3の3つの部屋があり、それぞれの部屋には、各種の映像または音楽などのデータ(コンテンツ)を取得し、コンテンツを記憶または再生するコンテンツボックス421-1乃至421-3が設置されている。
- [0217] コンテンツボックス421-1乃至421-3は、LAN402を介してルータ403と接続されており、ルータ403を介してインターネット21に接続された各種のサーバと通信を行い、各種のコンテンツを取得する。
- [0218] また、コンテンツボックス421-1乃至421-3は、歩紋を検知するセンサが設けられており、ユーザがその近傍を通過すると歩紋検知してユーザを特定する。ルータ403は、インターネット21からの不正なアクセスを防御するファイヤーウォール機能と、所定の容量のデータを記憶する記憶部を有している。LAN402には、PKを載置して充電を行うクレドール401が接続されており、クレドール401は、載置されたPKの情報をルータ403に送信する。
- [0219] ユーザ20-1乃至20-3は、外出時はPK22-1乃至22-3を携帯し、家400に帰宅するとクレドール401に自分が所有するPKを載置する。クレドール401は、PK22-1乃至22-3が載置されると、PK22-1乃至22-3のPMDをルータ403に送信し、ルータ403は、インターネット21を介してPbse23と通信し、Pbse23からユーザ20-1乃至20-3のPMDを取得し、記憶部に記憶する。
- なお、ユーザ20-1乃至20-3のPMDには、ユーザ20-1乃至20-3の嗜好情報および歩紋情報が記憶されているものとする。
- [0220] コンテンツボックス421-1乃至421-3は、ルータ403からユーザ20-1乃至20-3の歩紋情報を取得し、近傍のユーザの好みにあったコンテンツの再生をおこなう。例えば、ユーザ20-2がキッチンにいるとき、ユーザ20-2の歩紋202-2を検知したコ

ンテンツボックス421-2は、ルータ403からユーザ20-2のPMDを取得し、嗜好情報を分析し、自身が蓄積したコンテンツの中から嗜好情報に対応した音楽などを再生する。

[0221] また、ユーザ20-1と20-3がリビング400-1にいるとき、コンテンツボックス421-1は、ユーザ20-1と20-3の歩紋202-1と202-3を検知して、ルータ403から、ユーザ20-1のPMDと、ユーザ20-3のPMDを取得し、それぞれの嗜好情報を分析し、自身が蓄積したコンテンツの中から、例えば、ユーザ20-1の好みにあった音楽を再生し、ユーザ20-3の好みにあった映像を再生する。このように、家400の中のコンテンツボックス421-1乃至421-3を、近傍のユーザに対応してパーソナライズすることができる。

[0222] この例では、コンテンツボックス421-1乃至421-3をパーソナライズする例について説明したが、同様の方法で、各種のCE機器などをパーソナライズすることも可能であり、ユーザはPKを用いて所望の機器をパーソナライズすることができる。

[0223] ところで、上述したようにルータ403は、ファイヤーウォール機能を有しているので、例えば、LAN402に接続される機器とインターネット21に接続される機器との通信が制約されている(例えば、コンテンツボックスとpBaseの通信に利用できるプロトコル(ポート番号)が限られる)。このため、LAN402に接続される機器とインターネット21との通信は、図29に示されるようにして行われる。最初に、コンテンツボックス421-1からpBase23に対して、矢印441に示されるようにhttps(SSL)プロトコルを使って、セッションを開始する。セッションが確立された後、コンテンツボックス421-1とpBase23は、点線442に示されるようにhttpsプロトコルでの通信を行う。

[0224] また、図17Aを参照して上述したように、PK22-1乃至22-3とpBase23の間では、PMDの同期が行われる。図28の例の場合、PMDの同期は、クレドール402およびコンテンツボックス421-1乃至421-3を介して行われる。PK22-1、クレドール401、pBase23、およびコンテンツボックス421-1の間でPMDの同期が行われる場合の処理の流れについて、図30を参照して説明する。

[0225] ステップS2001において、PK22-1は、クレドール401に載置されると、自身のPMDの内容をクレドール401に送信し、ステップS2021においてこれが受信される。ス

ステップS2022において、クレドール401は、ステップS2021で受信された情報をpBase23に送信し、ステップS2041でこれが受信される。ステップS2042において、pBase23は、図31を参照して後述するPMD同期処理を実行する。これにより、pBase23に記憶されているPMDが更新され、PK22-1のPMDを更新する同期データが生成される。

[0226] ステップS2043において、pBase23は、同期データをクレドール401に送信し、ステップS2023で、これが受信される。ステップS2044において、クレドール401は、ステップS2023で受信された情報をPK22-1に送信し、ステップS2002で、これが受信される。そして、ステップS2003において、PK22-1は、ステップS2002で受信した同期データに基づいて、PK22-1のPMDを更新し、PK22-1のPMDとpBase23のPMDの同期が行われる。

[0227] コンテンツボックス421-1において、コンテンツが再生されると、ステップS2061において、コンテンツボックス421-1は、コンテンツの視聴履歴などの履歴情報をpBase23に送信し、ステップS2044で、これが受信され、pBase23は、履歴情報に基づいてPMDの嗜好情報を更新する。ステップS2045において、pBase23は、PMDの更新結果を同期データとして、クレドール401に送信し、ステップS2025でこれが受信される。ステップS2026において、クレドール401は、ステップS2025で受信された情報をPK22-1に送信し、ステップS2003で、これが受信され、ステップS2005において、PK22-1のPMDが更新される。

[0228] このようにしてPMDの同期が行われる。

[0229] 次に、図31を参照して、図30のステップS2042のPMD同期処理の詳細について説明する。

[0230] ステップS2081において、CPU121は、図30のステップS2041で受信したPMDと、pBase23に記憶されているPMDの内容を比較する。このとき、pBase23に記憶されているPMDの中から、受信したPMDに対応するPMDが1つずつ抽出されて比較され、そのPMDが最後に更新された日時を表す更新日時の情報が比較される。

[0231] ステップS2082において、CPU121は、ステップS2041で受信したPMDの更新日時が、pBase23に記憶されているPMDの更新日時より新しいか否かを判定し、受

信したPMDの更新日時が、pBase23に記憶されているPMDの更新日時より新しいと判定された場合、ステップS2083に進み、pBase23に記憶されているPMDの内容を受信したPMDの内容に更新する。

[0232] 一方、ステップS2082において、CPU121は、ステップS2041で受信したPMDの更新日時が、pBase23に記憶されているPMDの更新日時より新しくないと判定された場合、ステップS2084に進み、pBase23に記憶されているPMDの内容を同期データとする。この同期データは、PMD同期処理の終了後、ステップS2043(図30)で、PK22-1に送信され、PK22-1において、同期データに基づくPMDの更新が行われる。

[0233] ステップS2083またはS2084の処理の後、CPU121は、ステップS2085において、全てのPMDをチェックしたか否かを判定し、まだ全てのPMDをチェックしていないと判定された場合、ステップS2086に進み、次のPMDをチェックする。
その後処理は、ステップS2081に戻り、それ以降の処理が繰り返し実行される。

[0234] ステップS2085において、全てのPMDをチェックしたと判定された場合、処理は終了される。

[0235] このようにして、pBase23において、PMDの同期が行われる。

[0236] 次に、PKに各種のカードの情報を保存して利用する例について図32を参照して説明する。この例では、カード情報を有するPMD461がPK22に保存されているものとする。例えば、ユーザ20が買い物をするとき、PK22は、レジ481と無線通信などにより通信を行い、PMD461の情報がレジ481に取得される。PMD461は、ユーザ20が保有するクレジットカードなどのカード1乃至カードNのカード番号が記述されたカード情報を含むPMDである。このとき、レジ481をサービスシステムとして、PK22とレジ481の間で図6または図7に示されるような処理が行われる。そして、レジ481は、買い物代金の決済などを行うカード処理サーバ483とインターネット21を介して通信し、代金を決済する。

[0237] 例えば、プリペイドカードの残高、カードの利用履歴などの情報は、インターネット21を介して接続される、別のサーバのデータベース482-1乃至482-Nに記憶されており、カード処理サーバ483は、代金の決済を行った後、データベース482-1乃至4

82-Nの内容を更新する。

- [0238] このようにすることで、PK22を仮想のカードケースとし、各種カードをカードケースにまとめて入れて、必要なときにそのカードを取り出して利用することができる。また、PK22にカードリーダ機能を設けて、カードの情報を読み込ませ、その内容がPK22の近傍のレジ481に送信されるようにしてもよい。
- [0239] 次に、図33を参照して、PKを利用して、ユーザの周辺の機器の制御を行う例について説明する。同図において、ユーザ20は、PK22を携帯すると同時に、タッチパッド付ディスプレイ521を有するコンソール端末521を携帯し、プロジェクター503が設置された会議室に入る。会議室には、アクセスポイント25が設置されており、アクセスポイント25は、インターネット21に接続される。インターネット21には、プロジェクター503など、アクセスポイント25の周辺に存在する機器の制御情報を保有する環境サーバ501が接続されている。ユーザ20は、PK22を利用して、プロジェクター503の制御コードを取得し、コンソール端末521を操作して、プロジェクター503を制御する。
- [0240] このとき、環境サーバからプロジェクター503の制御コードを取得する処理の流れについて、図34を参照して説明する。ステップS2121において、PK22は、無線通信などによりコンソール端末502と通信を行い、コンソール端末502に対して機器情報の要求を送信し、ステップS2101においてこれが受信される。ステップS2102において、コンソール端末502は、自身の機器情報をPK22に送信し、ステップS2122でこれが取得される。
- [0241] また、ユーザが会議室に入るとPK22は、アクセスポイント25と無線通信などにより通信を行い、アクセスポイント25を経由して、環境サーバ501と通信を行う。このとき、環境サーバ501をサービスシステムとして図6または図7に示されるような処理が、PK22と環境サーバ501の間で行われる。そして、ステップS2123において、PK22は、コンソール端末502の機器情報を1つのPMDとして、環境サーバ501に対して、制御コードの取得要求を送信し、ステップS2141でこれが受信される。
- ステップS2142において、環境サーバ501は、コンソール端末502にインストールするプロジェクター503の制御コードを、PMDに追加してPK22に送信し、ステップS2

124でこれが受信される。

- [0242] その後、コンソール端末502をサービスシステムとして図6または図7に示されるような処理が、PK22とコンソール端末502の間で行われる。そして、ステップS2125において、PK22は、ステップS2124で受信したPMDをコンソール端末502に対して送信し、ステップS2103でこれが受信され、プロジェクター503の制御コードがコンソール端末502にインストールされる。ユーザ20は、タッチパッド付ディスプレイ521を操作して、プロジェクター503の制御を行う。
- [0243] このようにして、PKを利用して、ユーザの周辺の機器の制御が行われる。このように、周辺の機器に対応して、適切な制御コードやデータなどを選択して送信することで、各種の機器を適正に制御することができる。
- [0244] また、PKを利用した、ユーザの周辺の機器の制御の別の例として、図35に示されるようなドアの開閉をおこなうこともできる。この例では、アクセスポイント25の周辺にドア543と、ドア543のロックなどを解除してドア543の開放処理を行うドア開放制御機542が存在する。ドア開放制御機542は、インターネット21を介して、ドア開放制御機542の制御コードを記憶しているサーバ541と接続されている。
- [0245] ユーザ20が、サービスポイント25と通信可能な範囲41の中に入ると、サーバ541をサービスシステムとして、図6または図7に示されるような処理が行われ、ユーザ20が携帯するPK22が、アクセスポイント25を介して、インターネット21に接続されているサーバ541と通信し、サーバ541は、ドア開放制御機542に対して、ドア543の開放処理を実行させるように制御する。
- [0246] この場合、例えば、ユーザ20(PK22)の近傍のドア543を特定するIDなどの情報が、PMDとして、サーバ541に送信され、サーバ541は、受信したPMDに基づいて、ドア543を特定し、ドア開放制御機542に対して、ドア543の開放処理を実行させる制御する制御コードを送信する。
- [0247] このように、ユーザ20がドア543の近くのアクセスポイント25の近傍に行くと、自動的にドア543が開放されるようにすることができる。また、PK22とサーバ541の間で、図6または図7に示されるようななりすまし防止の処理が行われるので、不正な侵入者などに対してドア543が開放されないようにすることができる。

- [0248] また、例えば、ドア543付近に守衛室などがあり、ドア543から不正な侵入者が入らないように守衛が監視している場合、例えば、図36に示されるように、PK22から、守衛室のパーソナルコンピュータ562に対して、ID番号と顔写真のデータが含まれるPMDを送信し、パーソナルコンピュータ562に、PMDに対応する顔写真が表示されるようにすることで、さらにセキュリティを強化することができる。このようにすることで、PK22(ユーザ20)のPMDに対応した顔写真が、パーソナルコンピュータ562に表示されるので、例えば、不正な侵入者が、盗んだPK22を使ってドア543から侵入しようとしても、顔写真と違う人物である(ユーザ20ではない)ことが守衛に分かってしまうため、ドア543から侵入することができない。
- [0249] 次に、図37を参照して、PKを利用して、周辺の機器を使った会話を行う例について説明する。この例においては、ユーザ20-2が、PK22-1を所有するユーザ20-1との会話を希望しているものとする。そして、PK22-1は、pBase23と所定の時間間隔で通信を行い、図31を参照して上述したようにPMDの同期処理が行われているものとする。
- [0250] ユーザ20-1の周囲には、アクセスポイント25、電話機581、ならびにテレビ会議を行うとき利用するカメラ582とディスプレイ583が存在し、電話機581乃至ディスプレイ583の制御コードを記憶する環境サーバ584が、インターネット21に接続されている。さらに、インターネット21には、pBase23と、会話の接続サービスを提供する会話接続サーバ601が接続されている。会話接続サーバ601は、ユーザ(例えば、ユーザ20-2)から、特定の相手(例えば、ユーザ20-1)に対する会話接続要求を受け付けて、相手の周辺の機器を使った会話を提供する。
- [0251] この場合、会話接続を行う処理の流れについて、図38を参照して説明する。PK22-1は、カメラ582乃至ディスプレイ583などの周辺機器をサービスシステムとし、図6または図7に示されるような処理を行い、周辺機器と通信する。そして、ステップS2221において、PK22-1は、周辺機器に対して機器情報の要求を送信し、ステップS2201で、これが受信される。ステップS2202において、カメラ582乃至ディスプレイ583など周辺機器は、自身のIDまたはアドレスなどの機器情報をPK22-1にPMDとして送信し、ステップS2222で、これが受信される。受信されたPMDは、ステップS2223

において、ユーザ20-1が利用可能な機器を表すPMDとしてpBase23に送信され、ステップS2241でこれが受信される(PK22-1とpBase23で、PMDの同期が行われる)。

[0252] 一方、ユーザ20-2から、ユーザ20-1に対する会話の接続要求を受け付けた会話接続サーバ601は、ステップS2261において、ユーザ20-1に対応するPMDを保持するpBase23に対して、会話要求を送信し、ステップS2242で、これが受信される。このとき、会話接続サーバ601をサービスシステムとし、pBase23が、PK22-1の代わりとなって(代行して)、会話接続サーバ601とpBase23の間で、図6または図7に示されるような処理を行い通信が行われる。そして、pBase23は、ステップS2243において、ユーザ20-1が利用可能な機器を表すPMDを会話接続サーバ601に対して送信する。

[0253] ステップS2263において、会話接続サーバ601は、環境サーバ584を介して、周辺機器を制御し、ユーザ20-1と20-2の間で、電話機581による会話、またはカメラ582とディスプレイ583によるテレビ会議が行われる。このように、PKを利用して、周辺の機器を使った会話が行われる。このようにすることで、ユーザ20-1が、別の場所に行っても、ユーザ20-1が利用可能な機器を表すPMDに基づいて、会話を行うことができる。また、PK22-1とpBase23の間で、所定の時間間隔(例えば、30分間毎)にPMDの同期が行われるので、ユーザは、いつでも、どこでも周辺機器を利用して会話を行うことができる。

[0254] 次に、PKを利用してユーザの現在地を特定する例について、図39を参照して説明する。この例では、ユーザ20は、PK22を携帯しており、PK22は、近傍のアクセスポイント25-1と通信する。アクセスポイント25-1乃至25-nは、スペースサーバ641と接続されており、スペースサーバ641は、PK22が通信しているアクセスポイントのIDなどの情報を記憶する。また、スペースサーバ641は、インターネット21と接続されており、インターネット21には、pBase23と、ユーザの現在地を特定するロケーションサーバ642が接続されている。

[0255] この場合、インターネットに接続された機器643を用いて、ユーザの現在地を特定する処理の流れについて、図40を参照して説明する。

- [0256] PK22は、スペースサーバ641をサービスシステムとし、図6または図7に示されるような処理を行い、スペースサーバ641と通信する。そして、ステップS2321において、PK22は、スペースサーバ641に対して、今、PK22が通信しているアクセスポイントのIDの取得を要求し、ステップS2301において、これが受信される。
- ステップS2302において、スペースサーバ641は、アクセスポイント25-1のIDをPMDとして、PK22に送信し、ステップS2322で、これが受信される。受信されたPMDは、ステップS2323において、ユーザ20の近傍のアクセスポイントを表すPMDとしてpBase23に送信され、ステップS2341でこれが受信される(PK22-1とpBase23で、PMDの同期が行われる)。
- [0257] 一方、機器643は、ステップS2381において、ユーザ20の現在地の取得要求をロケーションサーバ642に対して送信し、ステップS2361で、これが受信される。
- ステップS2362において、ロケーションサーバ642は、ユーザ20のPMDを保持するpBase23に対して、ユーザ20の現在地の取得要求を送信し、ステップS2342で、これが受信される。このとき、ロケーションサーバ642をサービスシステムとし、pBase23が、PK22の代わりとなって(代行して)、ロケーションサーバ642とpBase23の間で、図18または図19に示されるような処理が行われ、通信が行われる。そして、ステップS2343において、pBase23は、ユーザ20の近傍のアクセスポイントを表すPMDをロケーションサーバ642に対して送信し、ステップS2363で、これが受信される。
- [0258] ロケーションサーバ642は、ステップS2363で受信されたPMDに基づいて、ユーザ20の近傍のアクセスポイント(今の場合、アクセスポイント25-1)の情報を取得し、そのアクセスポイントの位置を特定する。そして、ロケーションサーバ642は、アクセスポイント25-1の近傍を、ユーザ20の現在地とし、その現在地の情報を、ステップS2382において、機器643に送信し、ステップS2382で、これが受信される。
- [0259] このように、PKを利用して、ユーザ20の現在地が特定される。このようにすることで、ユーザ20が、別の場所(例えば、アクセスポイント25-2の近傍)に行っても、ユーザ20の近傍のアクセスポイントを表すPMDに基づいて、現在地を正確に特定することができる。
- [0260] また、ユーザ20の近傍のアクセスポイントを表すPMDが、PK22に記憶されるよう

にしてもよい。例えば、図41に示されるように、ユーザ20が旅行などで移動するとき、PK22を携帯し、PK22は、ユーザの現在地(近傍のアクセスポイントの情報)と、行き先のアドレスを含むPMD660を生成する。ユーザ20は移動中に、地図情報を提供する端末661と、PK22を通信させ、PMD660を端末661に送信させる。これにより、例えば、端末661に、現在地から目的地までの道を案内する地図が表示される。

[0261] また、PMD660を方向表示機662に送信させ、進むべき方向が表示されるようにしてもよい。このようにPMD660を利用することで、ユーザにとって利便性の高い、道案内をすることができる。

[0262] あるいはまた、このようにして特定されたユーザの現在地に基づいて、ユーザへのメッセージが伝達されるようにすることも可能である。例えば、インターネットに接続されたメールサーバが、スペースサーバ641からユーザの現在地の情報を取得し、図37に示されるような方法で、ユーザが利用可能な機器に関する情報を取得して電子メールを送信することもできる。このようにすることで、例えば、ユーザが本社にいるときは、本社のパーソナルコンピュータに電子メールが送信され、ユーザが、支社に出張しているときは、支社のパーソナルコンピュータに電子メールが送信される。その結果、ユーザは、どこにいても確実に自分宛のメッセージを受け取ることができる。

[0263] 以上においては、ユーザの近傍のアクセスポイントの情報からユーザの現在地を特定する例について説明したが、より詳細に現在地を特定することもできる。例えば、図42に示されるように、アクセスポイント25の近傍にPK22-1を携帯するユーザ20-1と、PK22-2を携帯するユーザ20-2がいる場合、PK22-1または22-2は、スペースサーバ641と通信し、ユーザ20-1または20-2の顔特徴情報を含むPMDをスペースサーバ641に送信する。なお、PK22-1または22-2は、範囲41の中において、アクセスポイント25と通信することができるものとする。

[0264] カメラ681は、アクセスポイント25に近接して設置され、範囲42の中にあるオブジェクトを撮影し、画像データを出力する。スペースサーバ641は、カメラ681と接続されており、カメラ681から出力される画像データを、ユーザ20-1または20-2の顔特徴情報と比較する。そして、顔特徴情報が一致する画像が検出された場合、スペースサーバ641は、ユーザ20-1または20-2は、アクセスポイント25の近傍にいるものと

判定し、アクセスポイント25のIDをPK22-1または22-2に送信する。

- [0265] このようにすることで、ユーザ20-1または20-2の現在地を、アクセスポイントの近傍(範囲41の中)から、さらに詳細に、カメラ681の近傍(範囲42の中)として特定することができる。
- [0266] あるいはまた、カメラ681から出力される画像データが、PMDとしてpBase23に記憶され、ユーザの現在地の周辺の情報として、必要に応じてサービスシステムに提供されるようにしてもよい。このようにすることで、ユーザの正確な現在地を隠蔽しつつ、ユーザの周辺の映像を提供することができる。
- [0267] ところで、複数のアクセスポイントが、比較的近傍に設置されている場合、PK22は、通信すべきアクセスポイントを選択(検出)する必要がある。
- [0268] 図43を参照して、PK22によるアクセスポイントの検出の例であるアクセスポイント検出処理1について説明する。ステップS2501において、PK22は、通信出力のパワーを最小にする。上述したように、PK22は、RF(Radio Frequency)通信、準静電界通信、光通信などの無線通信によりアクセスポイントと通信を行う。ステップS2501においては、例えば、PK22の電波出力を最小に設定する。
- [0269] ステップS2502において、PK22は、アクセスポイントが検出されたか否かを判定し、アクセスポイントが検出されなかったと判定された場合、ステップS2506に進み、通信出力のパワーが最大か否かを判定し、まだ最大ではないと判定された場合、ステップS2507に進み、通信出力のパワーを1段階上げる。そして、処理は、ステップS2502に戻り、それ以降の処理が繰り返し実行される。
- [0270] 図44を参照して、さらに詳しく説明する。PK22は、通信パワーが最小出力の場合、範囲701に電波を出力することができる。アクセスポイント25-1乃至25-nは、PK22からの電波を検知すると、応答を発信し、PK22において、これが受信されることにより、PK22がアクセスポイントを検出する。範囲701には、アクセスポイントがないため、PK22は、アクセスポイントを検出できない。そこで、PK22は、通信出力のパワーを1段階上げて、範囲702に電波を出力する。範囲702の中には、アクセスポイント25-1が存在し、PK22は、アクセスポイント25-1を検出する。
- [0271] 図43に戻って、ステップS2502において、アクセスポイントが検出されたと判定され

た場合、PK22は、ステップS2503に進み、検出されたアクセスポイント25-1と通信する。

[0272] 一方、ステップS2506において、通信出力のパワーが最大であると判定された場合、PK22の近傍にアクセスポイントはないものと判定され、ステップ2508において、エラー処理が実行され、アクセスポイント検出処理は終了される。

[0273] このように、PK22は、その通信出力を序所に上げていき、最初に見つかったアクセスポイントと通信する。このようにすることで、例えば、図44において、PK22は、アクセスポイント25-2と通信しないようにできるので、通信による消費電力を抑制することができる。

[0274] 図43においては、PK22が、通信出力を変化させ、アクセスポイントを検出する例について説明したが、PKの通信出力が同じでも、複数のアクセスポイントが検出される場合もある。そのような場合、アクセスポイントから発せられる通信出力(例えば、電界強度)に基づいて、アクセスポイントが検出されるようにしてもよい。図45を参照して、PK22によるアクセスポイントの検出の別の例であるアクセスポイント検出処理2について説明する。

[0275] ステップS2521において、PK22は、検出されたアクセスポイントの電界強度を取得する。ステップS2522において、PK22は、電界強度が最も大きいアクセスポイントを検索する。ステップS2523において、PK22は検索されたアクセスポイントと通信する。

[0276] 図46を参照して、さらに詳しく説明する。範囲711-1において、アクセスポイント25-1から出力される電波は電界強度1で、PK22に受信される。範囲712-1において、アクセスポイント25-1から出力される電波は電界強度2で、PK22に受信される。同様に、範囲711-2において、アクセスポイント25-2から出力される電波は電界強度1で、PK22に受信され、範囲712-2において、アクセスポイント25-2から出力される電波は電界強度2で、PK22に受信される。

[0277] いま、PK22は、アクセスポイント25-1から出力される電波を電界強度1で受信しており、同時に、アクセスポイント25-2から出力される電波を電界強度2で受信している。このような場合、複数のアクセスポイント(アクセスポイント25-1と25-2)の中から

、電界強度が最も大きいアクセスポイントが検索される。いまの場合、アクセスポイント25-1が検索され、PK22は、アクセスポイント25-1と通信する。

[0278] このようにして、アクセスポイントが検出される。このようにすることで、例えば、ユーザがいる部屋とその部屋に隣接する部屋の両方にアクセスポイントが設置されている場合であっても、PK22は、確実に、ユーザがいる部屋のアクセスポイントを利用した通信を行うことができる。

[0279] なお、PKの通信経路は1つに限られるものではなく、複数あってもよい。また、複数の通信経路において、それぞれ異なる方法で通信が行われるようにしてもよい。図47は、PK22の複数の通信経路を示す図である。

[0280] 同図において、PK22は、範囲41に電波を出力し、アクセスポイント25とRF通信を行う。そして、アクセスポイント25を経由して、インターネット21に接続され、サービスシステム24-2と通信が行われる。一方、PK22は、光通信用のインタフェース762を有する近傍のパーソナルコンピュータ761と光通信を行う。この場合、例えば、赤外線のような指向性のある光が、矢印781に沿ってPK22とパーソナルコンピュータ761から照射される。

[0281] また、ユーザ20が、準静電界通信用のインタフェース762の上にいるとき、PK22は、矢印782に示されるように、インタフェース762と準静電界通信を行う。インタフェース762は、サービスシステム24-1と接続されており、PK22は、インタフェース762を経由して、サービスシステム24-1と通信を行う。

[0282] 例えば、図39に示されるように、ユーザの現在地を特定する場合、ユーザ(PK22)の現在地が、RF通信のアクセスポイント25の位置情報ではなく、準静電界通信用のインタフェース762の位置情報に基づいて、特定されるようにすれば、ユーザの現在地をより詳細に特定することができる。また、指向性の高い光通信用のインタフェース762の位置情報に基づいて、ユーザの現在地が特定されるようにすれば、さらに正確にユーザの現在地を特定することができる。例えば、会議室の机に、光通信用のインタフェース762を複数設けておき、着座したユーザが、それぞれが所持するPKを光通信用のインタフェース762と光通信させるようにすれば、どの席にどのユーザが着座したのかを正確に把握することができる。

- [0283] あるいはまた、図5に示されるようなサービスシステム24の初期登録を行う場合の通信と、その後の通信で、異なる通信経路が設定されるようにしてもよい。例えば、サービスシステム24の初期登録を行う場合、PK22とサービスシステム24の間で、まだなりすまし防止方法が定められていないので、PK22が光通信などの通信が傍受され難い通信により、サービスシステム24と直接通信して初期登録を行い、その後の通信は、RF通信により、インターネット21を介してサービスシステム24と通信するようにしてもよい。このようにすることで、より安全なサービスを提供することができる。
- [0284] 上述したようにPKは小型のコンピュータであり、PK自身にプログラムを実行させ、所定の処理(例えば、受信した電子メールを表示させる処理)を行うようにすることも可能である。図48と図49を参照して、PKにプログラムを実行させ、所定の処理を行う例について説明する。
- [0285] 図48において、PKがPMD801を有しているものとする。PMD801のプロパティ「プログラム」は、PK22が実行するプログラムを表すものであり、その内容として、プログラムコードの実体が記憶されている。プロパティ「name」は、PKのユーザIDを表すものであり、その内容は、「foo」とされている。プロパティ「push」は、処理すべきデータ(例えば受信した電子メール)を表すものであり、その内容として、「緊急の連絡あり・・・」が記述されている。
- [0286] 次に、図49を参照して、PK22がプログラムを実行する処理について説明する。この処理は、所定の周期(例えば、1時間毎)に行われるようにしてもよいし、ユーザの指令に基づいて、実行されるようにしてもよい。ユーザの指令は、例えば、PK22の入力部106を構成するスイッチが、所定の回数押下されることにより行われる。ステップS2541において、CPU101は、PMD801のプロパティ「push」にデータがあるか否かを判定し、データがあると判定された場合、ステップS2542に進み、プロパティ「push」の内容をディスプレイに表示させる。いまの場合、「緊急の連絡あり・・・」が表示される。ステップS2543において、CPU101は、プロパティ「push」の内容を消去する。
- [0287] ステップS2541において、データがないと判定された場合、処理は終了される。
- [0288] このようにして、PK自身にプログラムを実行させ、例えば、受信した電子メールを表

示させる処理が実行される。例えば、PKを1つのサービスシステムとして、別のPKとの間で、図6または図7に示されるような処理が行われ、電子メールの送受信を行うようにすれば、なりすまし防止処理により、ユーザを正確に認証することができるので、電子メールのセキュリティをより向上させることができる。

- [0289] また、pBase23を1つのサービスシステムとして、PK22と通信させ、pBase23からの要求に基づいて、PK22がプログラムを実行することも可能である。この場合の処理の流れについて、図50を参照して説明する。同図は、図7に対応しており、図7のサービスシステム24に代わってpBase23とされている。
- [0290] 図50のステップS2801乃至S2808の処理は、図7のステップS401乃至S408の処理と同様の処理なので、その説明は省略する。図50のステップS2821乃至S2836の処理は、図7のステップS421乃至S436と同様の処理なので、その説明は省略する。図50のステップS2881乃至S2891は、図7のステップS481乃至S491と同様であり、図50のステップS2901とS2902は、図7のステップS501とS502と同様なのでその説明は省略する。
- [0291] ステップS2809において、pBase23は、PK22に対して、プログラムの実行要求を送信し、ステップS2835において、PK22の通信モジュール61によりこれが受信される。ステップS2836において、通信モジュール61は、ステップS2835で受信された内容を、DBアクセスモジュール66を経由してプログラムに対して出力し、ステップS2921において、これが受信されプログラムが実行される。
- [0292] このようにして、pBase23からの要求に基づいて、PK22のプログラムが実行される。
- [0293] なお、図50においては、pBase23を1つのサービスシステムとして、PK22と通信させる例について説明したが、PK22-1が、別のPKであるPK22-2を1つのサービスシステムとし、PK22-2と通信を行うことも可能である。
- [0294] ところで、PK22は、ユーザが携帯するものなので、バッテリーなどにより電力が供給される。このため、通信に用いられる電力は最小限にすることが望ましい。図51を参照して、PK22の通信スタンバイ処理について説明する。
- [0295] ステップS3101において、CPU101は、待ち受けモードで通信する。このとき、PK2

2においては、例えば、図47に示した複数の通信経路のうち、最も消費電力が少ない準静電界通信のみが行われる。ステップS3102において、CPU101は、通信があったか否かを判定し、通信があったと判定された場合、ステップS3103において、802. 11bによるRF通信を起動する。ステップS3104において、CPU101は、所定の時間が経過したか否かを判定し、所定の時間が経過したと判定されるまで待機する。

[0296] ステップS3104において、所定の時間が経過したと判定された場合、CPU101は、ステップS3105に進み、802. 11bによるRF通信を終了する。その後、処理は、ステップS3101に戻り、それ以降の処理が繰り返し実行される。

[0297] 図52と図53を参照してさらに詳しく説明する。図52において、ユーザ20が、準静電界通信用のインタフェース821-1乃至821-3の上にいるとき、PK22は、インタフェース762と準静電界通信を行う。サービスシステム822は、インタフェース821-1乃至821-3と接続されており、常に、サービスIDとサービス情報により構成されるパケット823をインタフェース821-1乃至821-3に送信している。いま、ユーザ20が、インタフェース821-1の上にいるので、PK22は、パケット823を受信し、通信があったと判定する(図51のステップS3102)。

[0298] そして、PK22は、RF通信を起動し(図51のステップS3103)、図53に示されるように、範囲41の中にあるアクセスポイント25と通信を行い、アクセスポイント25を経由して、サービスシステム822との通信を行う。

[0299] このようにすることで、通常(待ち受けモード時)は、RF通信と比較して消費電力の少ない準静電界通信を行い、サービスシステム822と通信する必要があるときだけ、準静電界通信と比較して通信速度が高いRF通信を用いて高速通信を行うようにすることができ、消費電力を抑制し、効率よく通信することができる。

[0300] 次に、PKまたはpBaseにより、実現されるサービスを複数組み合わせ例について、図54乃至図58を参照して説明する。図54Aにおいて、PK22を携帯したユーザが、アクセスポイントが設置された部屋にはいると、pBase23からユーザ20に対する連絡内容が送信される。これにより、例えば、PK22のディスプレイに「Aさんから連絡あり」のメッセージが表示される。あるいはまた、図54Bに示されるように、部屋881の中の床に設置された表示装置882が点灯することにより、ユーザ20に対してメッセー

ジがあることが通知されるようにしてもよい。

- [0301] 自分に対する連絡があることを知ったユーザ20は、PK22をパーソナルコンピュータ901と通信させ、図55に示されるように、パーソナルコンピュータ901に、pBase23からコミュニケーションリストを含むPMDを取得させ、コミュニケーションリストを表示させる。コミュニケーションリストは、ユーザ20に対して、連絡があった人の一覧を記述したリストであり、例えば、人物A乃至Dの4人からの連絡があったことが記述されている。
- [0302] 人物A乃至DもそれぞれPKを所持しており、図39に示されるような方法で、それぞれの現在地が特定され、コミュニケーションリストには、たとえば、人物Aは移動中であり、人物Bは自席にあり、人物Cは会議室Cにあり、人物Dは伝言を残している旨が表示される。
- [0303] 例えば、会議室にいる人物Cと連絡をとりたいとき、ユーザ20は、近傍の会議室Aに入り、会議室Cとテレビ会議を行う。図56に示されるように、会議室Aには、電子ドキュメントなどを表示するモニタ921、相手の顔を表示するモニタ922、会議室Cの全体の様子を表示するモニタ923、およびタッチパッド付ディスプレイを備えたコンソール端末924が設置されている。
- [0304] このとき、ユーザ20は、図33に示されるような方法で、コンソール端末924にモニタ921乃至923の制御コードをインストールし、コンソール端末924を操作して、モニタ921乃至923を制御する。
- [0305] ここで、図57に示されるように、会議室Cに、人物C、および人物F乃至Iの6人がいる場合、各人物が、それぞれ自分のPKを所有しているものとし、各自のPKを会議室Cの机に設置された光通信装置と通信させる。光通信は、指向性が強いので、PKの存在する場所を正確に特定することができる。これにより、例えば、会議室Aのコンソール端末924に人物C、および人物F乃至Iの名前、所属、および着席位置などが表示される。
- [0306] このように、PKとpBaseにより、ユーザにとって利便性の高いコミュニケーションの仕組を提供することができる。
- [0307] 図58は、PK22とpBase23の組み合わせによるIP電話機961の待ち受け電力を抑

制する例を説明する図である。PK22を携帯したユーザ20の近傍に、アクセスポイント25と、IP電話機961があり、IP電話機961は、インターネット21に接続され、所定の相手と通話を行う。なお、消費電力抑制のために、IP電話機961は、通常電源がOFFの状態にされている。

[0308] この場合、PK22は、アクセスポイント25を介して、pBase23と通信を行い、図37に示されるような方法で、ユーザ20が利用可能な機器を表すPMDをpBase23に送信する(図58の矢印1001)。ユーザ20との会話を希望する機器981は、インターネット21の会話接続サーバに対して会話接続要求を行い、会話接続要求が、pBase23に送信される(図58の矢印1002)。pBase23は、PK22と通信し、会話接続要求を通知する(図58の矢印1003)。この結果、図49を参照して上述したように、PK22のディスプレイに接続要求が表示される。

[0309] ユーザ20が、会話接続要求があることを知り、IP電話機961の電源をONにすると、IP電話機961が利用可能となったことがpBase23に送信される(図58の矢印1004)。さらに、pBase23から機器981に対してIP電話機961が利用可能となったことが通知される(図58の矢印1005)これにより、機器981とIP電話機961による通話が開始される。

[0310] このようにして、ユーザ20は、消費電力を抑制しながらIP電話機961を利用することができる。

[0311] 以上においては、PK22を、ユーザが携帯可能な小型のコンピュータとして説明したが、図4のソフトウェア60を、例えば、汎用のパーソナルコンピュータなどに実装することにより、汎用のパーソナルコンピュータがPKとして利用されるようにすることも可能である。

[0312] 図59は、PK22のソフトウェア60を、ユーザが持ち歩く携帯機器1101と1102に実装する例を示す図である。同図において、携帯機器1101と1102は、ユーザが所望する音楽データを再生する、例えばウォークマン(商標)のような小型の音楽再生装置である。携帯機器1101と1102には、PK22のソフトウェア60が実装されているとともに、ユーザの嗜好情報に適合する音楽データの取得または送信を行うサービスシステムであるサービスシステム24-20のソフトウェアが実装されている。

- [0313] すなわち、携帯機器1101と1102は、PK22とサービスシステム24-20を1つの情報処理装置として実現したものであり、ユーザは、通信によるデータの授受を行うことなく、サービスの提供を受けることができる。この結果、ユーザは、どこに行っても、携帯機器1101または1102に蓄積されたPMDの嗜好情報に基づいて、自分の好みに合う音楽を聴くことができる。
- [0314] また、携帯機器1101と1102に通信機能を設けるようにしてもよい。このようにすることで、例えば、携帯機器1101のユーザ22-11と、携帯機器1102のユーザ22-12が道で会ったとき、自分の好みに合う音楽の音楽データを交換し合うことができる。
- [0315] なお、図25においては、ユーザのPMDの中の嗜好情報に基づいて、パーソナライズが行われる例について説明したが、例えば、ネットワークに接続される他のサーバにおいて、ユーザの嗜好が既に分析されている場合、その分析結果と合わせて、より詳細なパーソナライズを行うことも可能である。図60において、インターネット21に接続されるサービスシステム24-21は、PK22のユーザの嗜好情報に基づいて、テレビ番組を推薦する。一方、インターネット21には、協調フィルタリングによりユーザの嗜好を分析する協調フィルタリングサーバ1201が接続されている。
- [0316] 協調フィルタリングサーバ1201は、pBase23からユーザのPMDを取得し、PMDに含まれる視聴(操作)履歴を分析する。そして、あるユーザの視聴履歴に対して、他のユーザの視聴履歴との間でマッチングを取り、当該ユーザと視聴履歴の類似する他のユーザの視聴履歴を取得する。そして、視聴履歴が類似する(好み似ている)他のユーザが視聴した番組で、当該ユーザが未だ視聴していない番組名を取得し、推薦する。
- [0317] このようにして協調フィルタリングサーバ1201により推薦される番組を、サービスシステム24-21が、PK22のPMDに基づいて、さらに選択し、ユーザに推薦する。このようにすることで、ユーザに対して、より嗜好に適合する番組を推薦することができる。
- [0318] 勿論、協調フィルタリングサーバ1201により推薦される番組が直接ユーザに推薦されるようにしてもよい。上述したように、PK22またはpBase23により、ユーザのPMDの中に嗜好情報が既に蓄積されているので、PK22またはpBase23を用いずに、ユーザが使用する機器(例えば、テレビジョン受像機など)の視聴履歴などから直接嗜

好情報を収集して、番組の推薦を行う場合と比較して、協調フィルタリングサーバ1201の処理負荷を軽減することができる。

- [0319] なお、本明細書において上述した一連の処理を実行するステップは、記載された順序に沿って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

請求の範囲

- [1] ユーザに関連するユーザ情報を記憶し、複数の他の情報処理装置と通信を行う情報処理装置であって、
前記他の情報処理装置により読み出しまたは変更が行われるユーザ情報を提示する提示手段と、
前記提示手段により提示されたユーザ情報の読み出しまたは変更の許可を指定する指定手段と、
前記他の情報処理装置を特定する特定手段と、
前記特定手段により特定された前記他の情報処理装置と前記他の情報処理装置により読み出しまたは変更が行われるユーザ情報を関連付けて記憶する記憶手段とを備えることを特徴とする情報処理装置。
- [2] 準静電界通信、電磁波通信、光通信、または電氣的通信を行う通信手段をさらに備えることを特徴とする請求項1に記載の情報処理装置。
- [3] 前記情報処理装置の外部の機器を、入力または出力のインタフェースとして利用する
ことを特徴とする請求項1に記載の情報処理装置。
- [4] 前記他の情報処理装置と初回の通信を行うとき、前記他の情報処理装置に前記情報処理装置を特定する情報を送信する
ことを特徴とする請求項1に記載の情報処理装置。
- [5] 前記他の情報処理装置と初回の通信を行うとき、前記情報処理装置が情報を暗号化するために用いる第1のコードと、前記第1のコードに対応して生成される第2のコードを生成し、前記第1のコードを前記他の情報処理装置に送信し、
前記他の情報処理装置が情報を暗号化するために用いる第3のコードを前記通信手段を介して取得する
ことを特徴とする請求項1に記載の情報処理装置。
- [6] 前記ユーザ情報を前記他の情報処理装置から提供されたコンテンツの利用履歴にもとづいて更新する
ことを特徴とする請求項1に記載の情報処理装置。

- [7] 前記ユーザ情報を管理する情報管理装置とネットワークを介して通信し、前記情報処理装置に記憶されたユーザ情報の内容が前記情報管理装置に記憶されたユーザ情報の内容と同じになるように前記ユーザ情報を更新することを特徴とする請求項1に記載の情報処理装置。
- [8] 前記情報管理装置は、前記ユーザ情報の読み出しまたは変更が許可された前記他の情報処理装置を特定し、前記ユーザ情報を前記ユーザ情報の読み出しまたは変更が許可された他の情報処理装置に、前記ネットワークを介して提供することを特徴とする請求項7に記載の情報処理装置。
- [9] 前記ユーザの体に発生する準静電界または静電界の変化パターンに基づいて、前記ユーザを認証することを特徴とする請求項1に記載の情報処理装置。
- [10] 前記ユーザ情報は、前記ユーザの嗜好を表す嗜好情報を有し、前記ユーザが指定する情報機器に前記嗜好情報を送信し、前記情報機器を前記嗜好情報に対応して動作させることを特徴とする請求項1に記載の情報処理装置。
- [11] 複数の他の情報処理装置に関連付けられた複数のユーザ情報に基づいて、あらたなユーザ情報を生成することを特徴とする請求項1に記載の情報処理装置。
- [12] ユーザに関連するユーザ情報を記憶し、複数の他の情報処理装置と通信を行う情報処理装置の情報処理方法であって、
前記他の情報処理装置により読み出しまたは変更が行われるユーザ情報を提示する提示ステップと、
前記提示ステップの処理により提示されたユーザ情報の読み出しまたは変更の許可を指定する指定ステップと、
前記他の情報処理装置を特定する特定ステップと、
前記特定ステップの処理により特定された前記他の情報処理装置と前記他の情報処理装置により読み出しまたは変更が行われるユーザ情報を関連付けて記憶する記憶ステップと を含むことを特徴とする情報処理方法。

- [13] ユーザに関連するユーザ情報を記憶し、複数の他の情報処理装置と通信を行う情報処理装置のプログラムであって、
- 前記他の情報処理装置により読み出したりは変更が行われるユーザ情報の提示を制御する提示制御ステップと、
- 前記提示制御ステップの処理により提示されたユーザ情報の読み出したりは変更の許可の指定を制御する指定制御ステップと、
- 前記他の情報処理装置の特定を制御する特定制御ステップと、
- 前記特定制御ステップの処理により特定された前記他の情報処理装置と前記他の情報処理装置により読み出したりは変更が行われるユーザ情報を関連付けて記憶するように制御する記憶制御ステップと
- をコンピュータに実行させることを特徴とするプログラム。
- [14] ユーザに関連するユーザ情報を記憶し、複数の他の情報処理装置と通信を行う情報処理装置のプログラムが記録される記録媒体であって、
- 前記他の情報処理装置により読み出したりは変更が行われるユーザ情報の提示を制御する提示制御ステップと、
- 前記提示制御ステップの処理により提示されたユーザ情報の読み出したりは変更の許可の指定を制御する指定制御ステップと、
- 前記他の情報処理装置の特定を制御する特定制御ステップと、
- 前記特定制御ステップの処理により特定された前記他の情報処理装置と前記他の情報処理装置により読み出したりは変更が行われるユーザ情報を関連付けて記憶するように制御する記憶制御ステップと
- をコンピュータに実行させるプログラムが記録されることを特徴とする記録媒体。
- [15] ネットワークを介して複数の他の情報処理装置と通信を行い、ユーザに関連するユーザ情報を記憶する情報処理装置であって、
- ユーザが所持する携帯端末と前記ネットワークを介して通信する通信手段と、
- 前記携帯端末に記憶され、前記ユーザに関連するユーザ情報を取得する取得手段と、
- 前記取得手段により取得されたユーザ情報に基づいて、前記情報処理装置に記

憶される前記ユーザ情報の更新を行う更新手段と、

前記携帯端末に記憶される前記ユーザ情報を更新するデータを作成する作成手段と

を備えることを特徴とする情報処理装置。

- [16] 前記携帯端末が前記ネットワークに接続されていない場合、前記通信手段は、前記携帯端末に代わって前記他の情報処理装置と通信を行うことを特徴とする請求項15に記載の情報処理装置。

- [17] 前記ユーザ情報として、
前記携帯端末を特定する情報と、
前記携帯端末が、前記他の情報処理装置を認証する合言葉と、
前記携帯端末が、情報を暗号化するとき用いる第1のコードおよび第1のコードに対応して生成される第2のコードと、
前記他の情報処理装置を特定する情報と、
前記他の情報処理装置が、前記携帯端末を認証する合言葉と、
前記他の情報処理装置が、情報を暗号化するとき用いる第3のコードと
をさらに記憶することを特徴とする請求項16に記載の情報処理装置。

- [18] 前記ユーザ情報を前記他の情報処理装置から提供されたコンテンツの利用履歴にもとづいて更新する更新手段をさらに備えることを特徴とする請求項15に記載の情報処理装置。

- [19] 前記携帯端末と前記ネットワークを接続するアクセスポイントを特定し、特定された前記アクセスポイントの位置に基づいて、前記ユーザの現在値を特定し、前記ユーザの現在地の情報を前記ユーザ情報として記憶することを特徴とする請求項15に記載の情報処理装置。

- [20] 前記アクセスポイントに対応する機器を特定するIDと、前記機器と通信するために必要なアクセスキーを前記ユーザ情報としてさらに記憶することを特徴とする請求項19に記載の情報処理装置。

- [21] 前記通信手段は、前記携帯端末と所定の時間間隔で通信し、前記ユーザの現在地の情報、並びに前記アクセスポイントに対応する機器のIDおよびアクセスキーを更

新する

ことを特徴とする請求項20に記載の情報処理装置。

- [22] 前記他の情報処理装置から前記ユーザとの会話の要求を表す要求信号を前記ネットワークを介して受信した場合、前記ユーザ情報を前記他の情報処理装置に送信する

ことを特徴とする請求項21に記載の情報処理装置。

- [23] 前記携帯端末の記憶容量を超えて存在する前記ユーザ情報をさらに記憶することを特徴とする請求項15に記載の情報処理装置。

- [24] ネットワークを介して複数の他の情報処理装置と通信を行い、ユーザに関連するユーザ情報を記憶する情報処理装置の情報処理方法であって、
ユーザが所持する携帯端末と前記ネットワークを介して通信する通信ステップと、
前記携帯端末に記憶され、前記ユーザに関連するユーザ情報を取得する取得ステップと、

前記取得ステップの処理により取得されたユーザ情報に基づいて、前記情報処理装置に記憶される前記ユーザ情報の更新を行う更新ステップと、

前記携帯端末に記憶される前記ユーザ情報を更新するデータを作成する作成ステップと を含むことを特徴とする情報処理方法。

- [25] ネットワークを介して複数の他の情報処理装置と通信を行い、ユーザに関連するユーザ情報を記憶する情報処理装置のプログラムであって、

ユーザが所持する携帯端末と前記ネットワークを介して通信するように制御する通信制御ステップと、

前記携帯端末に記憶され、前記ユーザに関連するユーザ情報の取得を制御する取得制御ステップと、

前記取得制御ステップの処理により取得されたユーザ情報に基づいて、前記情報処理装置に記憶される前記ユーザ情報の更新を行うように制御する更新制御ステップと、

前記携帯端末に記憶される前記ユーザ情報を更新するデータの作成を制御する作成制御ステップと

をコンピュータに実行させることを特徴とするプログラム。

- [26] ネットワークを介して複数の他の情報処理装置と通信を行い、ユーザに関連するユーザ情報を記憶する情報処理装置のプログラムが記録される記録媒体であって、ユーザが所持する携帯端末と前記ネットワークを介して通信するように制御する通信制御ステップと、
- 前記携帯端末に記憶され、前記ユーザに関連するユーザ情報の取得を制御する取得制御ステップと、
- 前記取得制御ステップの処理により取得されたユーザ情報に基づいて、前記情報処理装置に記憶される前記ユーザ情報の更新を行うように制御する更新制御ステップと、
- 前記携帯端末に記憶される前記ユーザ情報を更新するデータの作成を制御する作成制御ステップと
- をコンピュータに実行させるプログラムが記録されることを特徴とする記録媒体。

補正書の請求の範囲

[2004年12月8日 (08.12.04) 国際事務局受理：出願当初の請求の範囲 5 は補正された；
他の請求の範囲は変更なし。]

[1] ユーザに関連するユーザ情報を記憶し、複数の他の情報処理装置と通信を行う情報処理装置であって、

前記他の情報処理装置により読み出しまたは変更が行われるユーザ情報を提示する提示手段と、

前記提示手段により提示されたユーザ情報の読み出しまたは変更の許可を指定する指定手段と、

前記他の情報処理装置を特定する特定手段と、

前記特定手段により特定された前記他の情報処理装置と前記他の情報処理装置により読み出しまたは変更が行われるユーザ情報を関連付けて記憶する記憶手段とを備えることを特徴とする情報処理装置。

[2] 準静電界通信、電磁波通信、光通信、または電氣的通信を行う通信手段をさらに備えることを特徴とする請求項 1 に記載の情報処理装置。

[3] 前記情報処理装置の外部の機器を、入力または出力のインタフェースとして利用する

ことを特徴とする請求項 1 に記載の情報処理装置。

[4] 前記他の情報処理装置と初回の通信を行うとき、前記他の情報処理装置に前記情報処理装置を特定する情報を送信する

ことを特徴とする請求項 1 に記載の情報処理装置。

[5] (補正後) 前記他の情報処理装置と初回の通信を行うとき、前記情報処理装置が情報を暗号化するために用いる第 1 のコードと、前記第 1 のコードに対応して生成される第 2 のコードを生成し、前記第 1 のコードを前記他の情報処理装置に送信し、

前記他の情報処理装置が情報を暗号化するために用いる第 3 のコードを前記通信手段を介して取得する

ことを特徴とする請求項 2 に記載の情報処理装置。

[6] 前記ユーザ情報を前記他の情報処理装置から提供されたコンテンツの利用履歴にもとづいて更新する

ことを特徴とする請求項 1 に記載の情報処理装置。

図1
[図1]

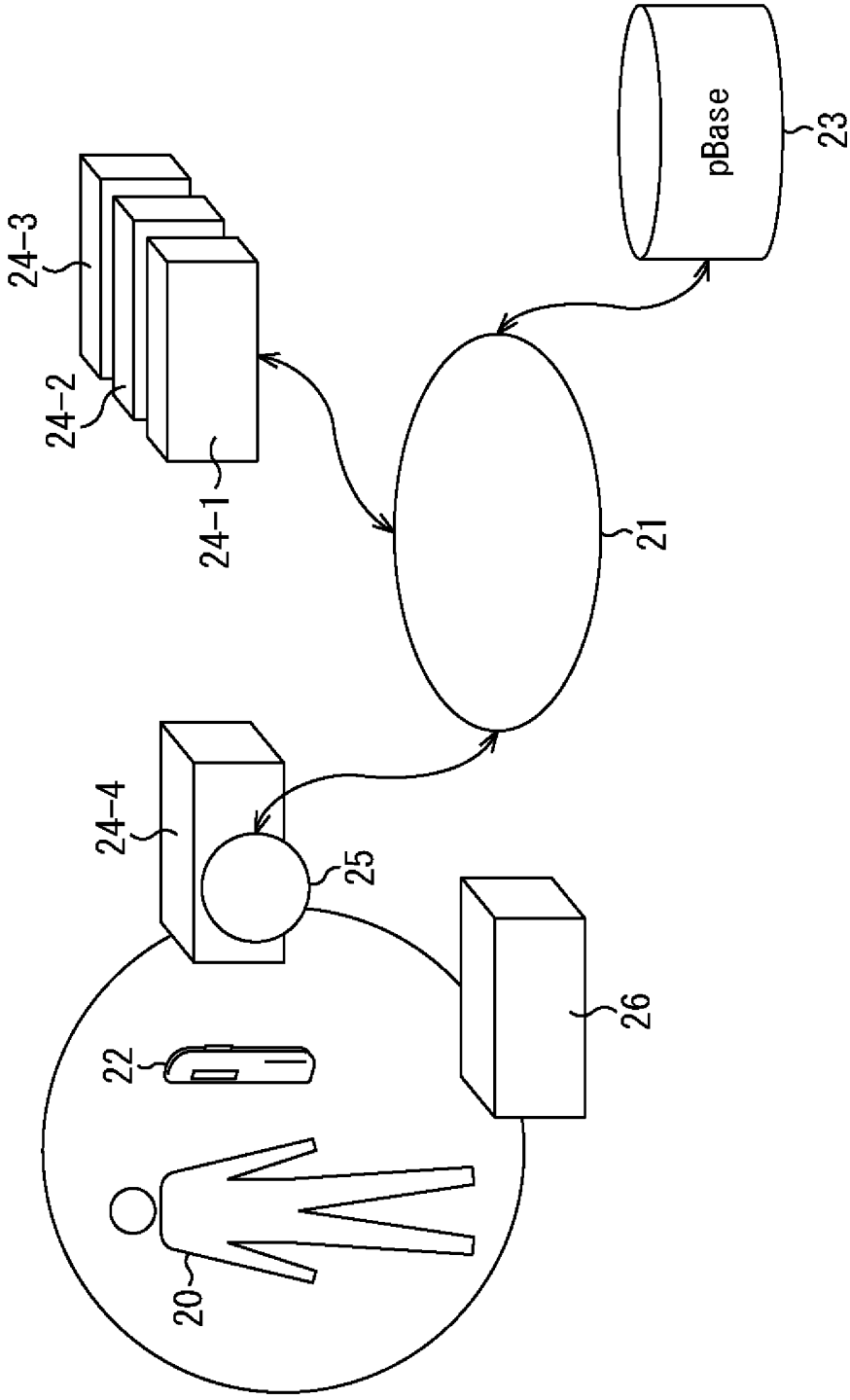


図2

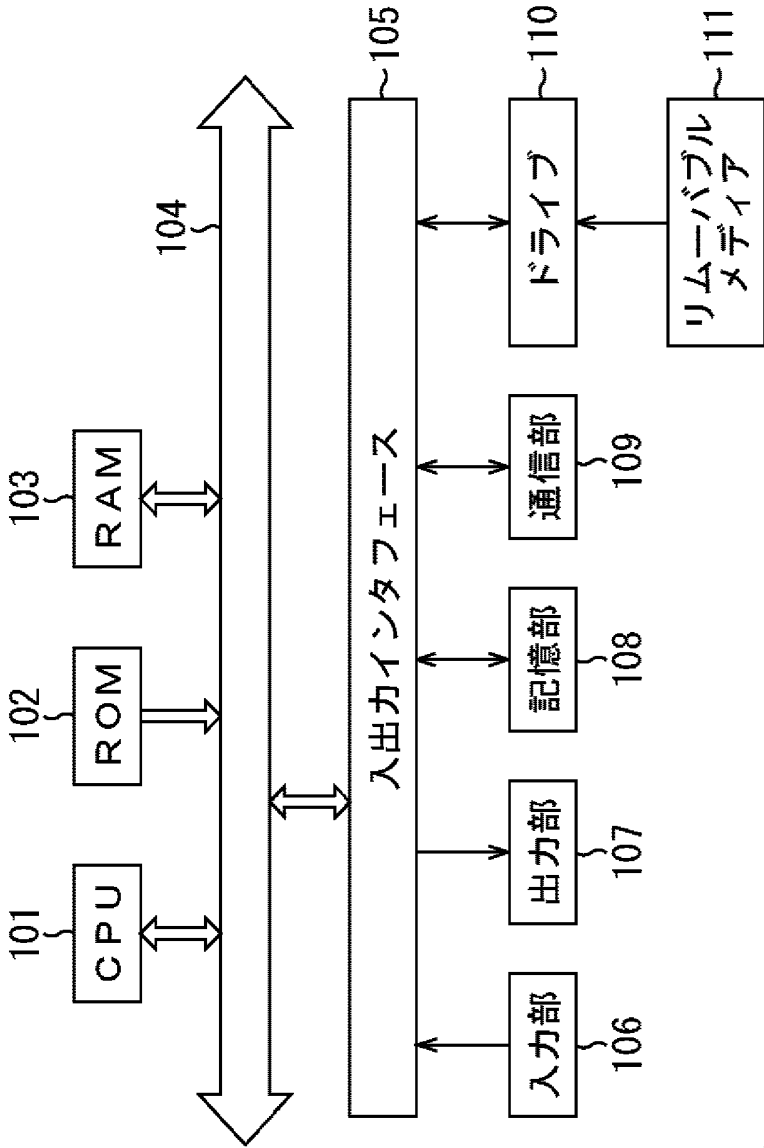


図3 [図3]

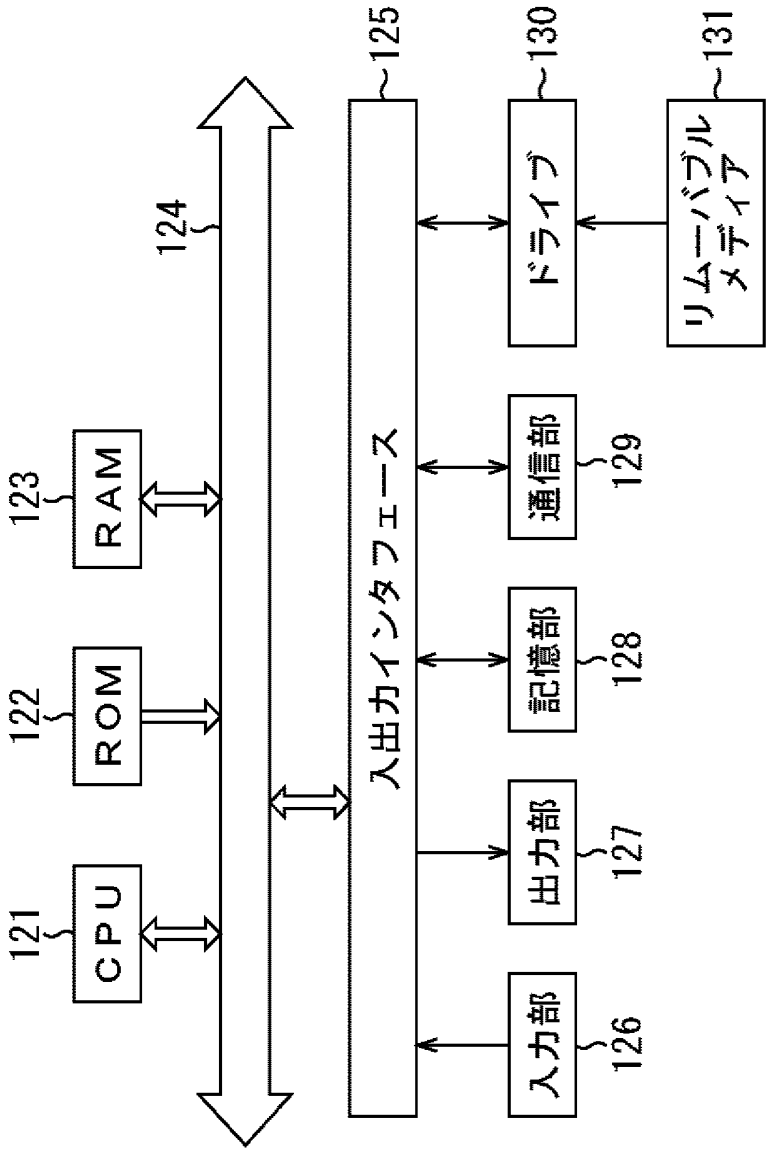


図4

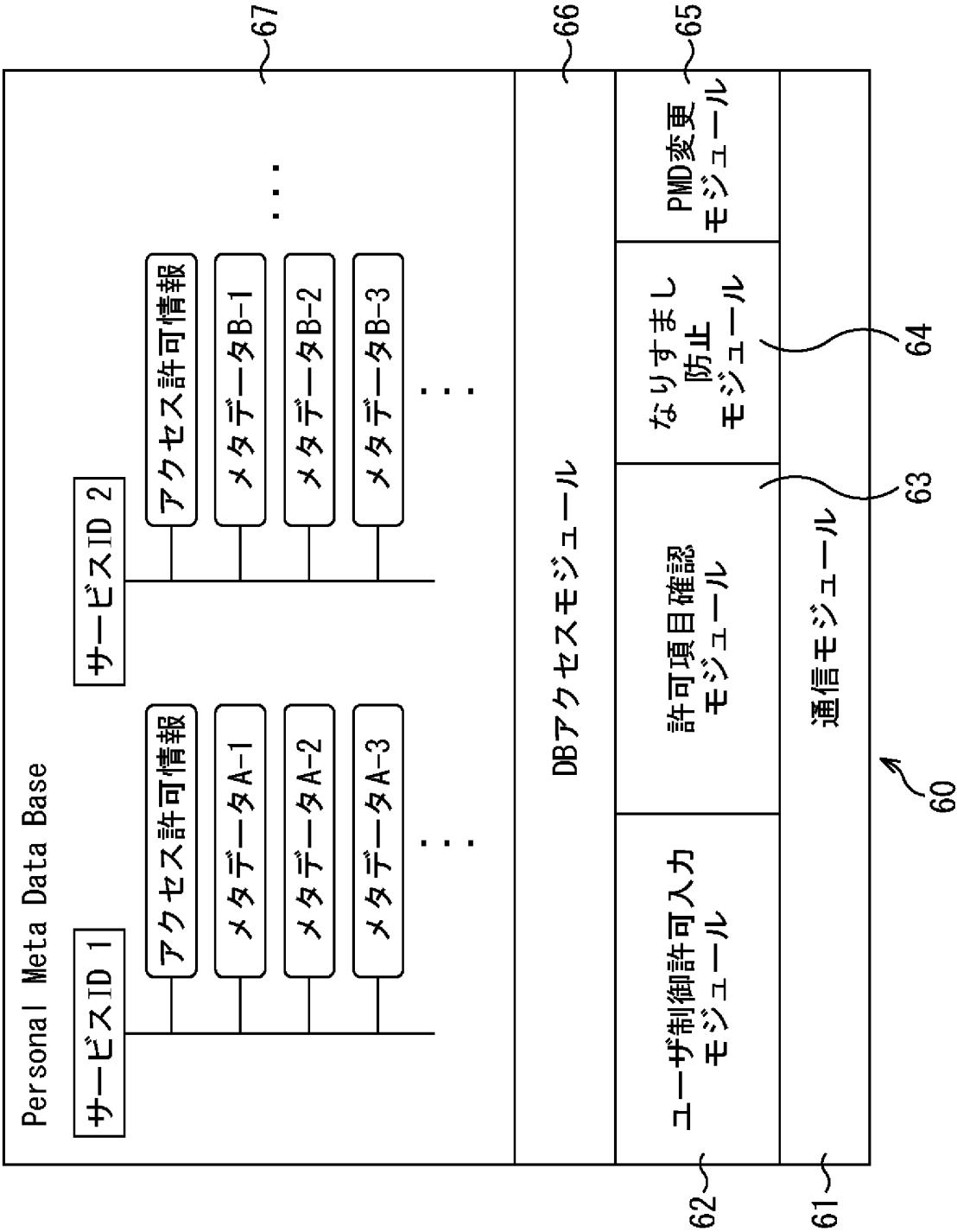
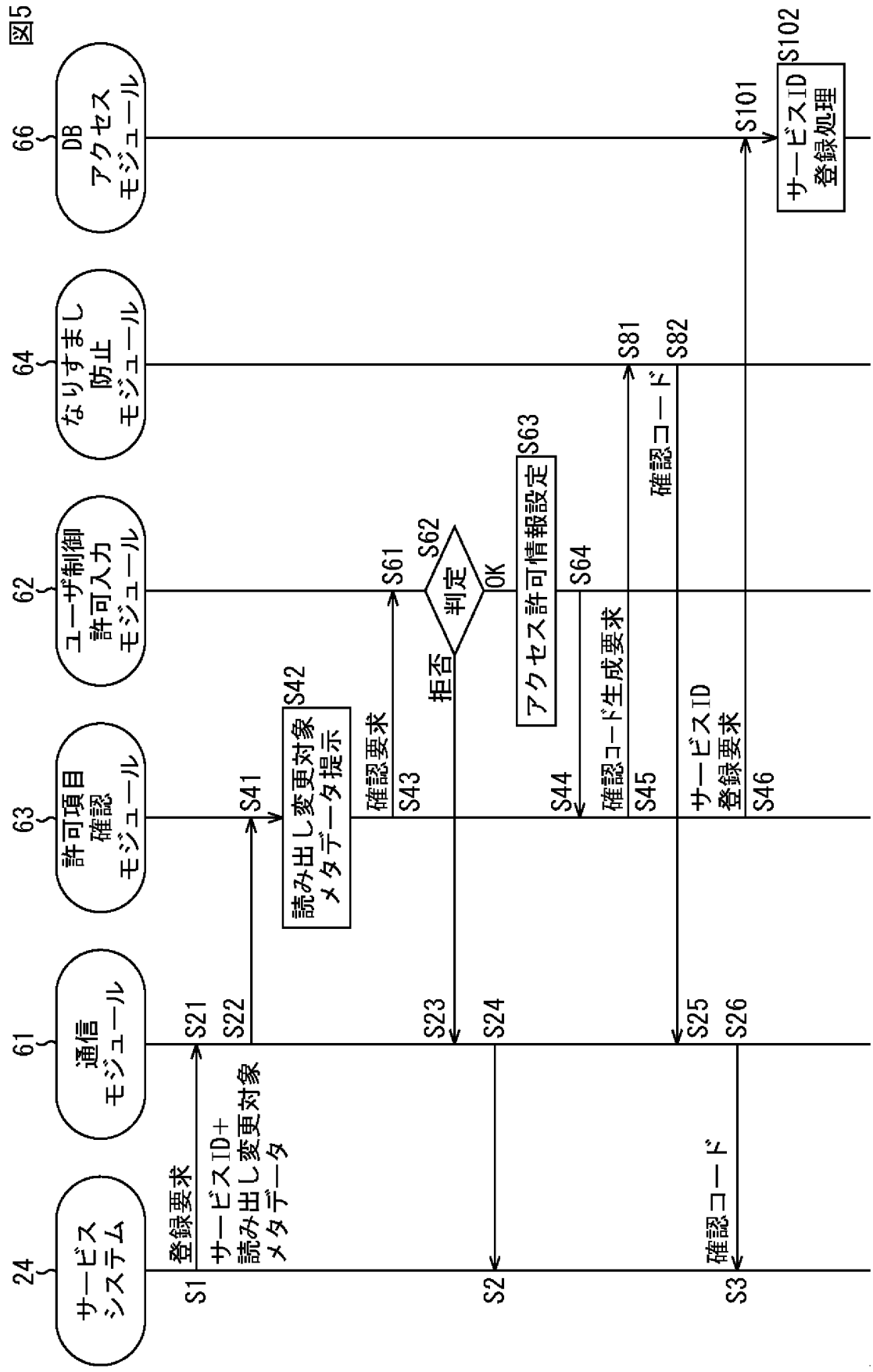
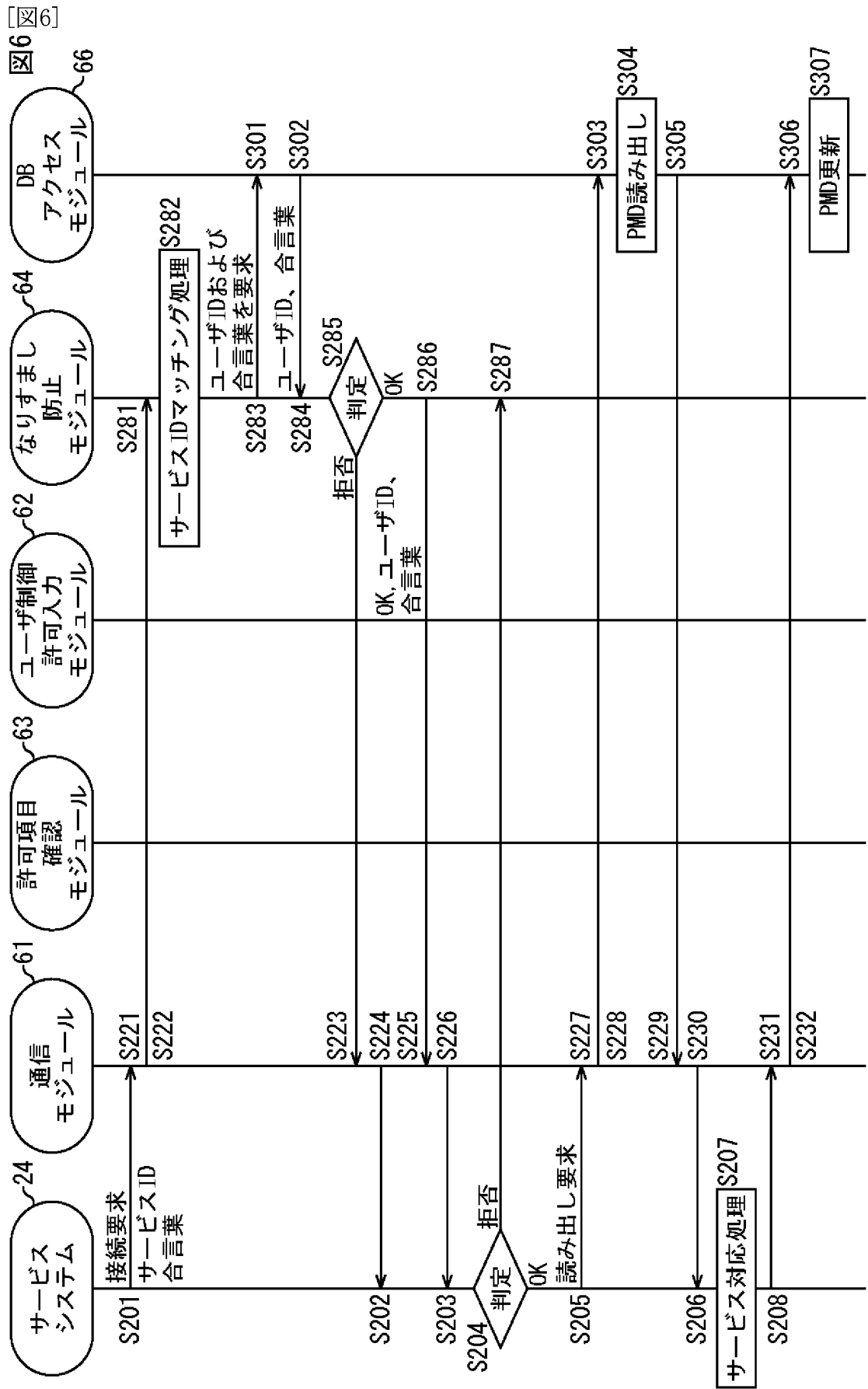
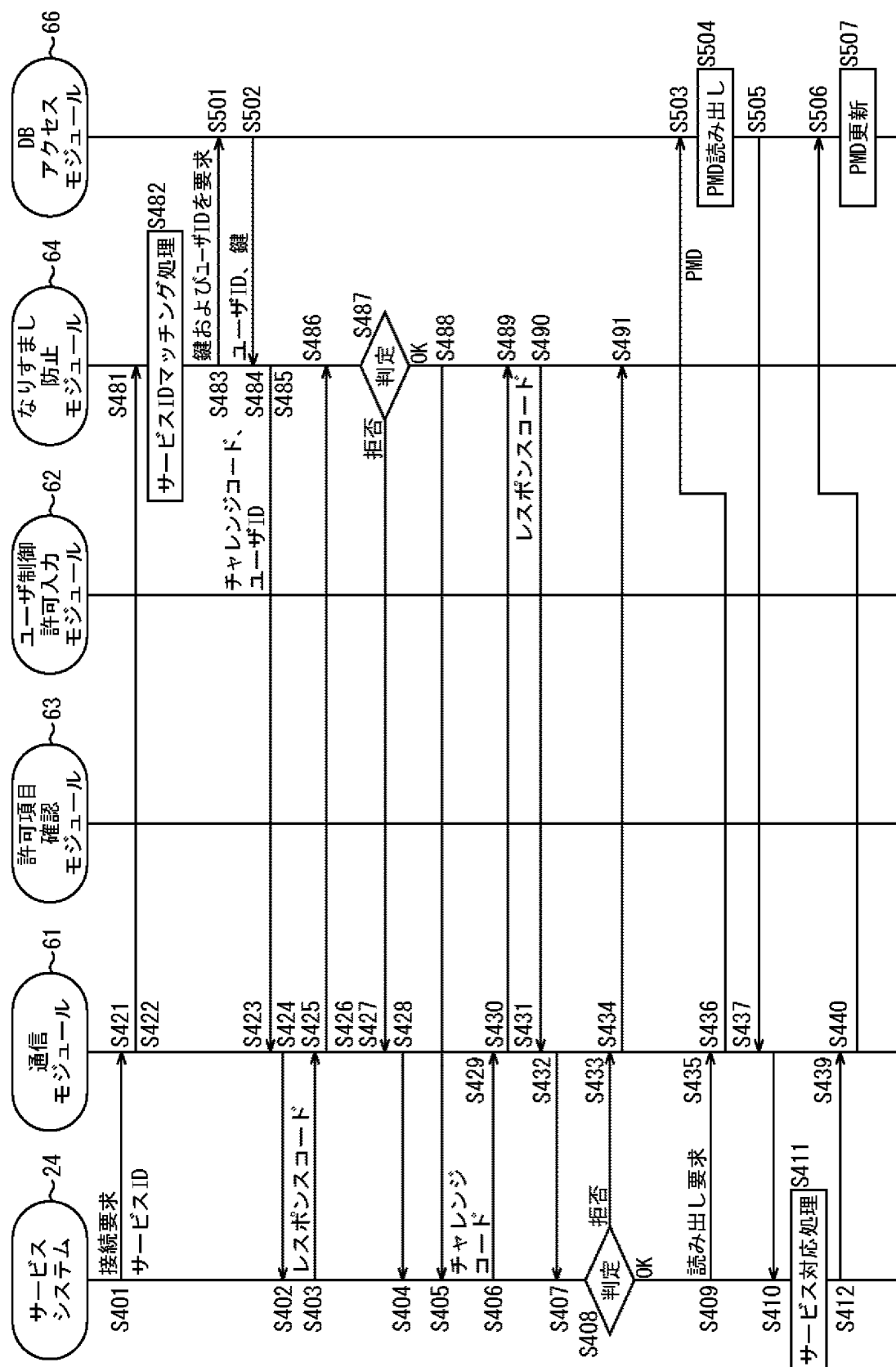


図5



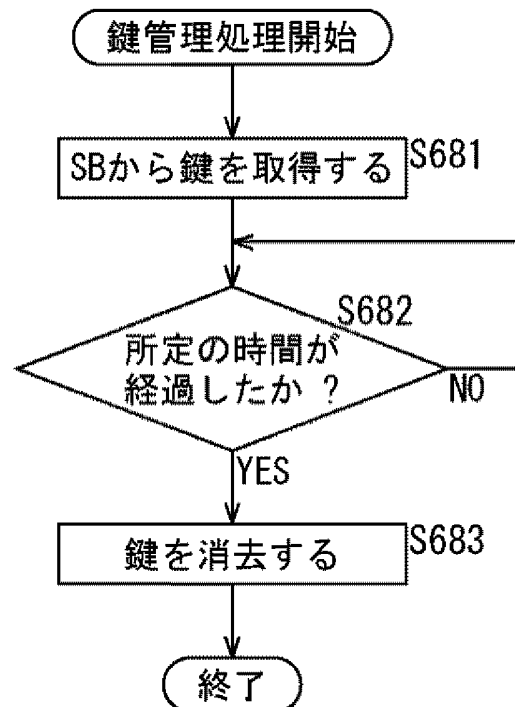


7
図



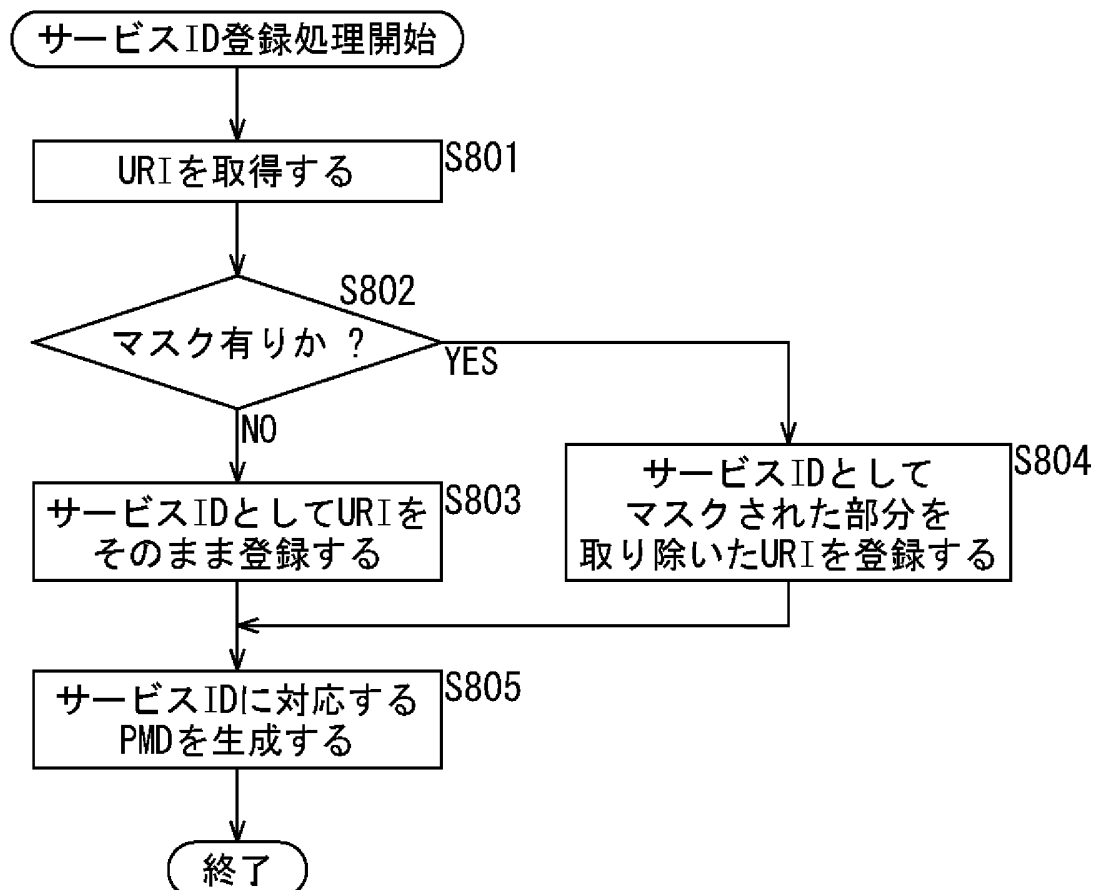
[図8]

図8



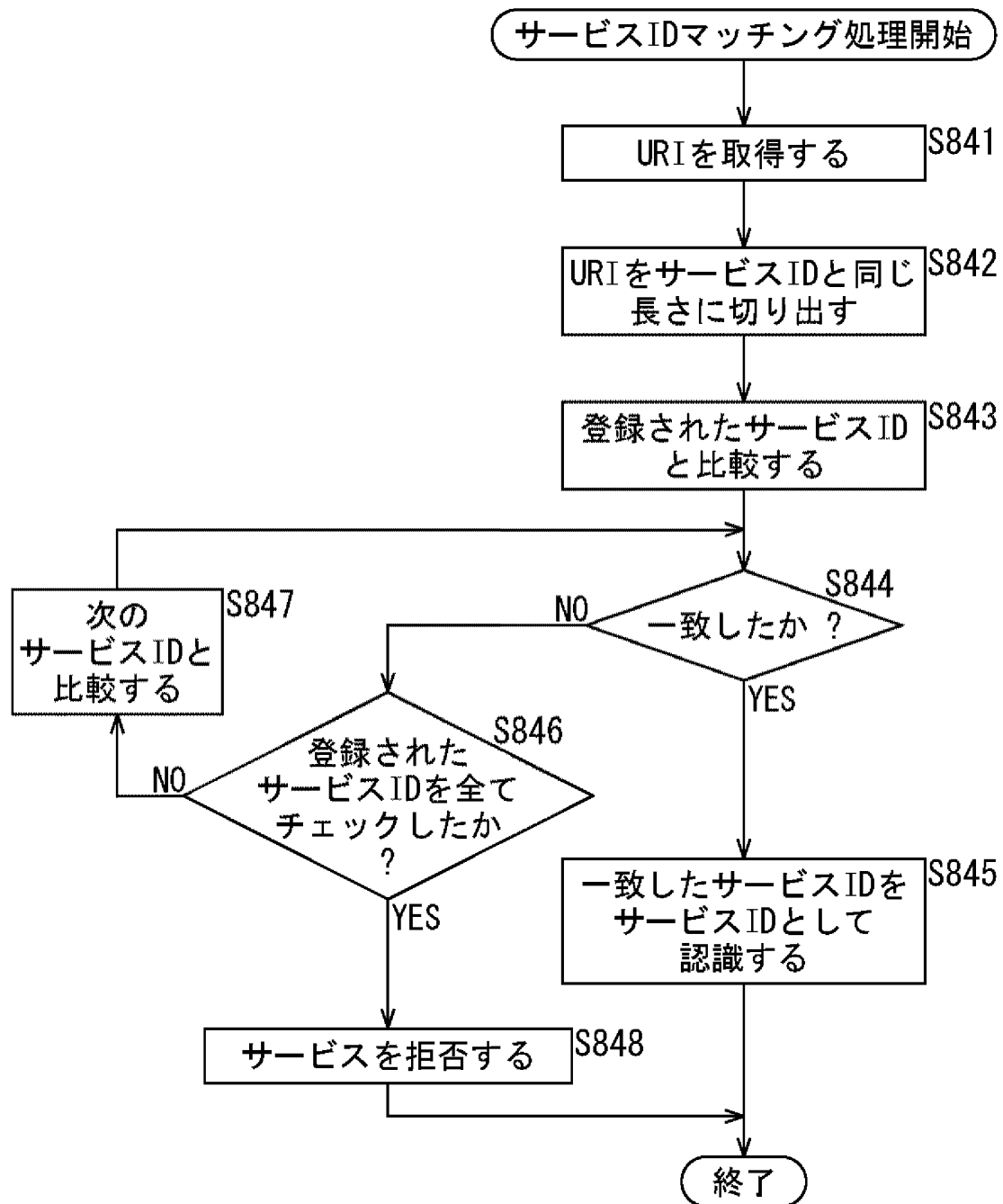
[図9]

図9



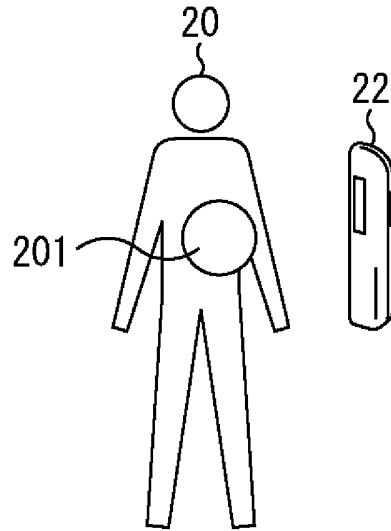
[図10]

図10



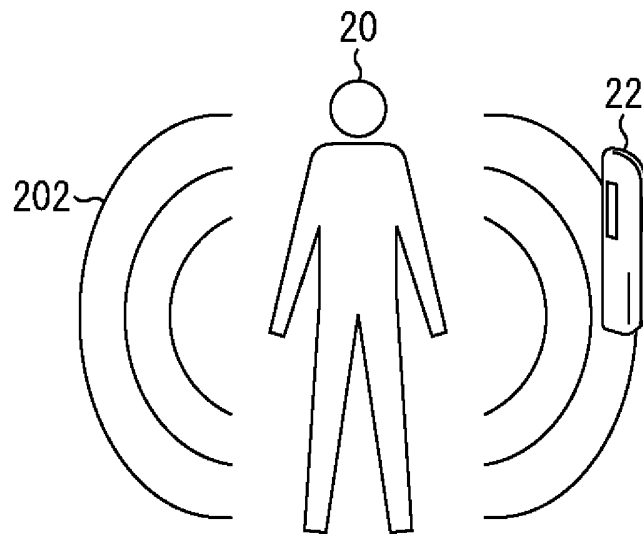
[図11A]

図11A



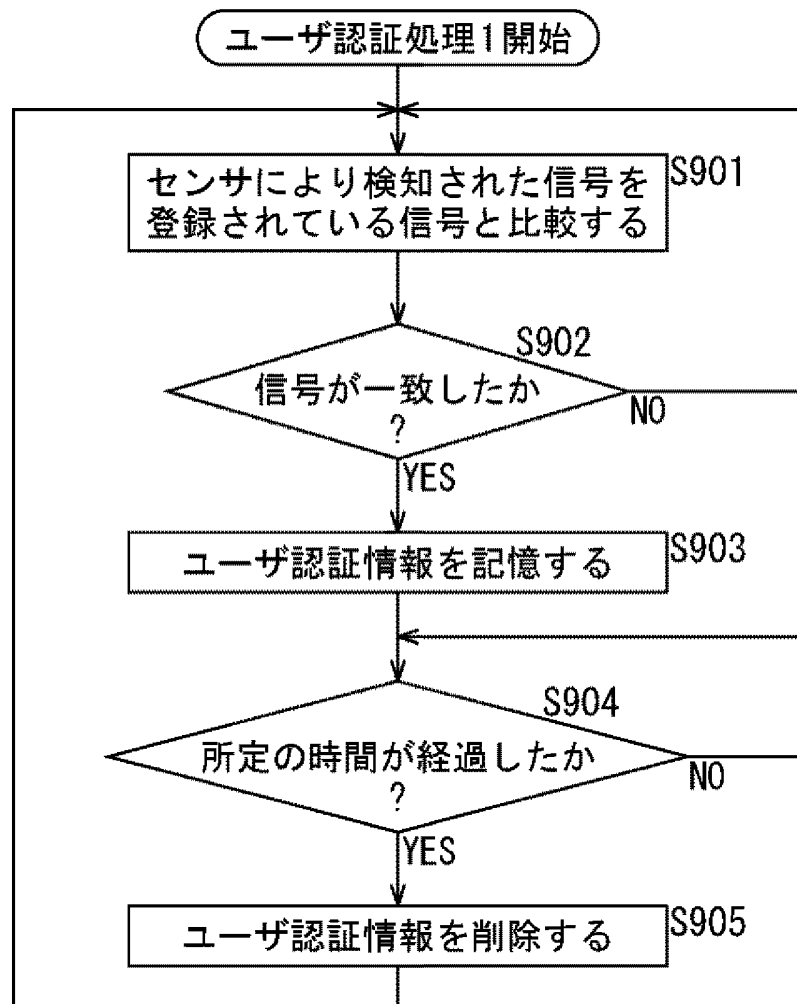
[図11B]

図11B



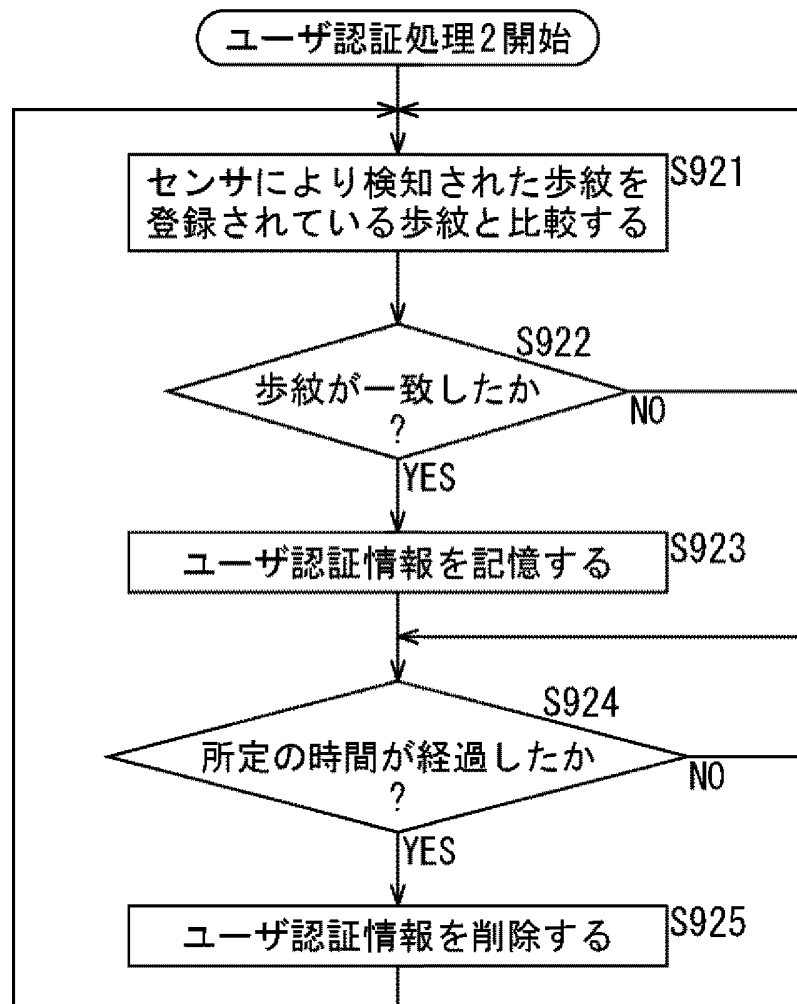
[図12]

図12



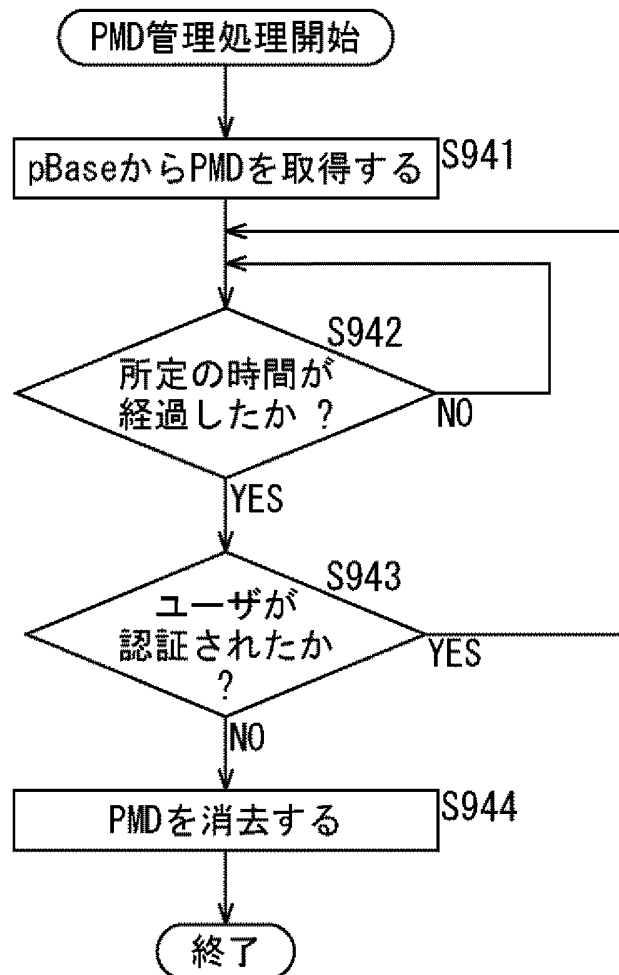
[図13]

図13



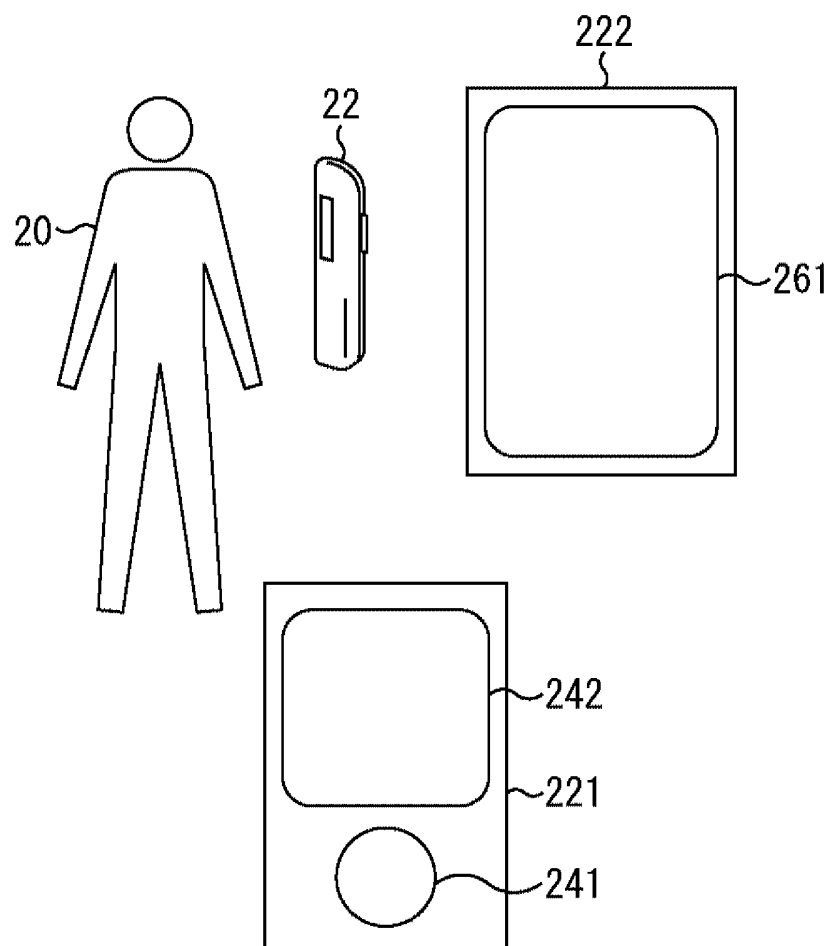
[図14]

図14



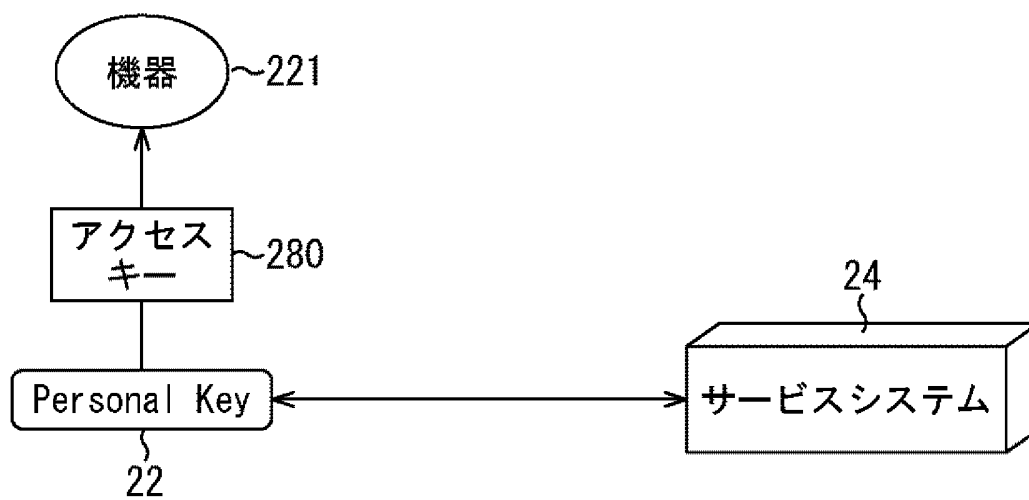
[図15]

図15



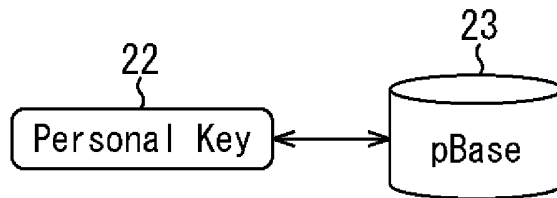
[図16]

図16



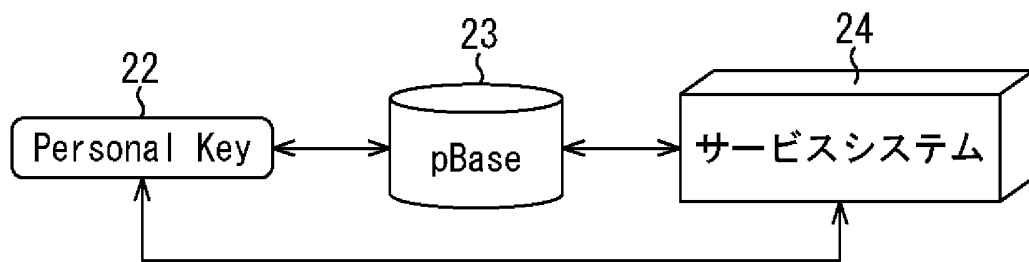
[図17A]

図17A



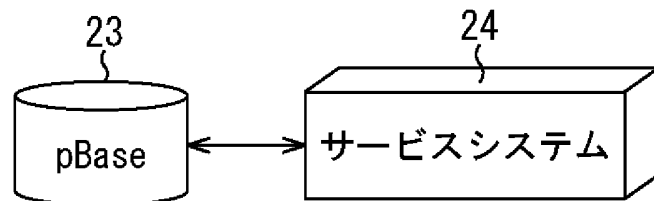
[図17B]

図17B



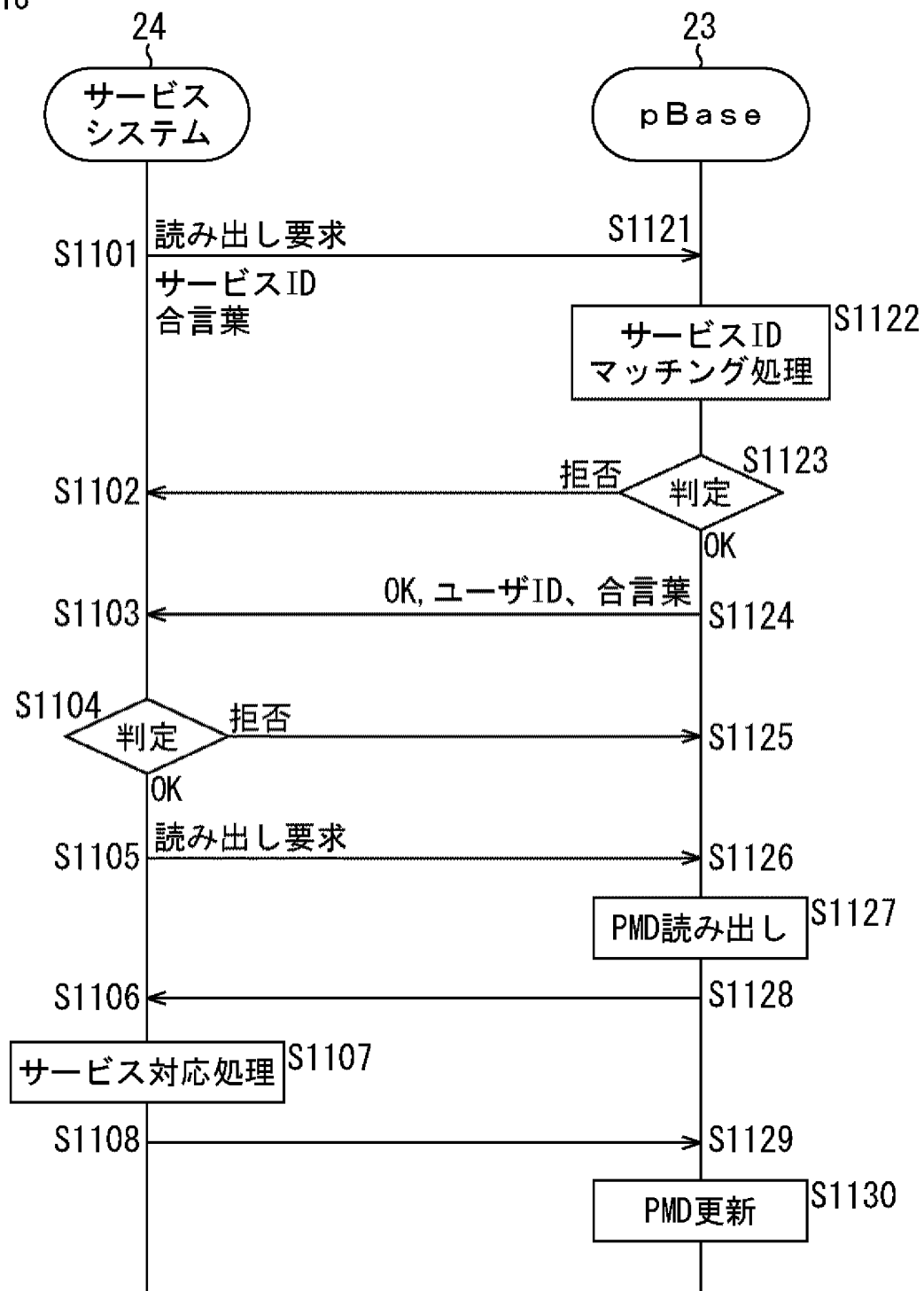
[図17C]

図17C



[図18]

図18



[図19]

図19

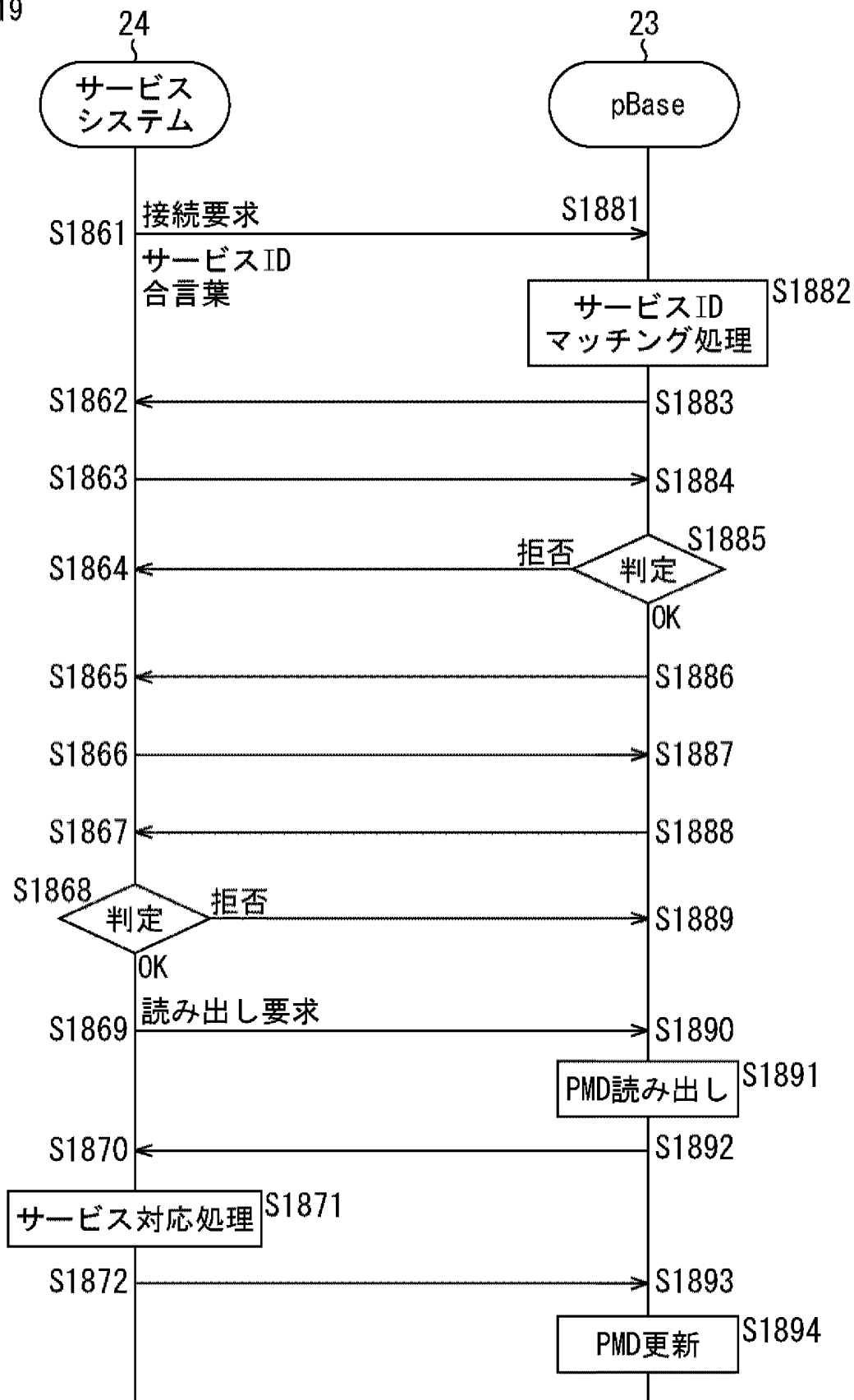


図20A [図20A]

プロパティ	内容	アクセス制御
name	foo	制御情報
なりすまし防止方法	公開鍵方式	制御情報
サービス公開鍵	鍵データ	制御情報
PK秘密鍵	鍵データ	制御情報
action	プログラム	制御情報
番組嗜好情報	スポーツ10 バラエティ7 音楽5 その他3	制御情報

・
・
・

図20B [図20B]

プロパティ	内容	アクセス制御
name	foo	制御情報
なりすまし防止方法	共通鍵方式	制御情報
共通鍵	鍵データ	制御情報
action	プログラム	制御情報
番組嗜好情報	スポーツ10 バラエティ7 音楽5 その他3	制御情報

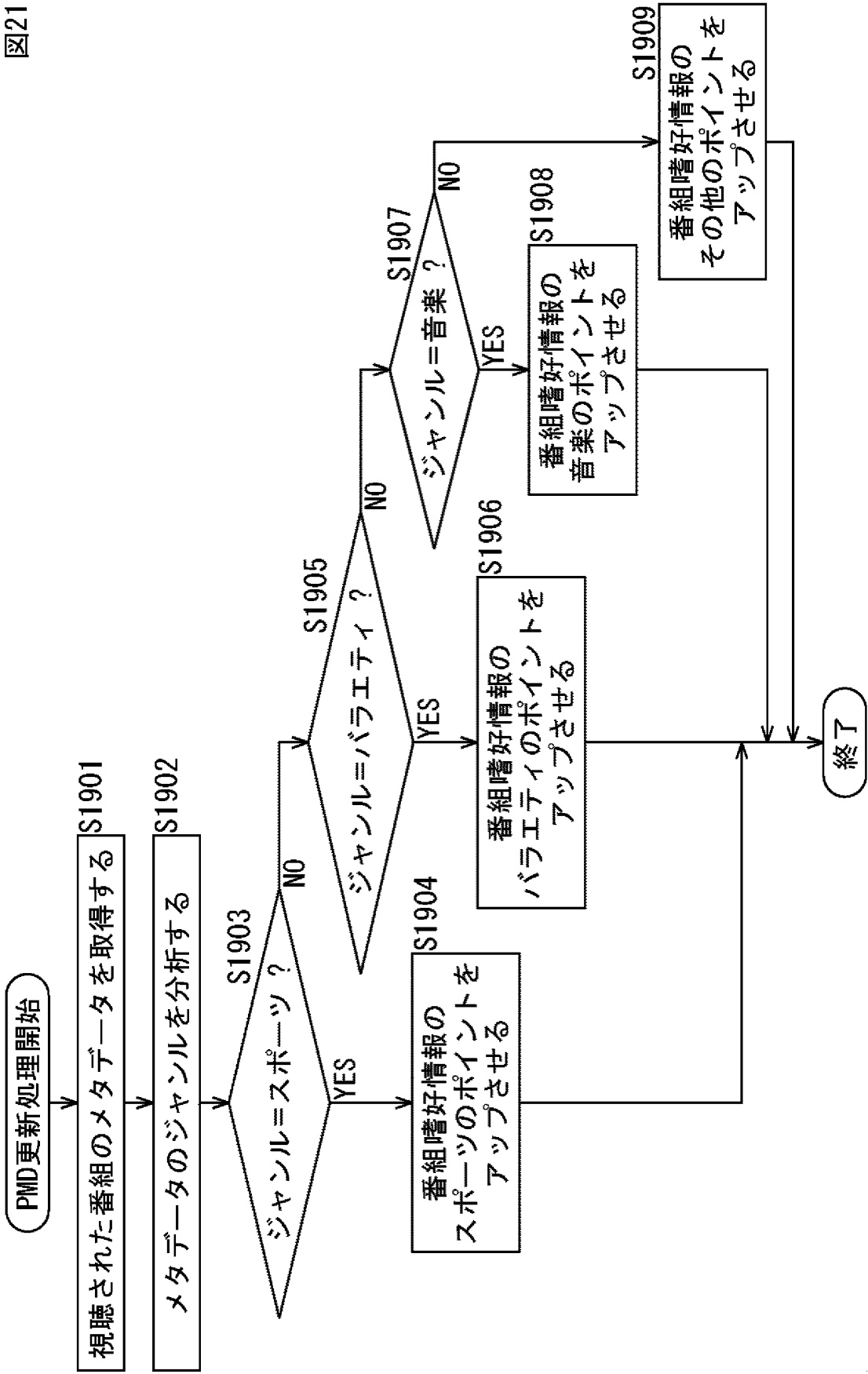
.
. .
.

図20C

プロパティ	内容	アクセス制御
name	foo	制御情報
なりすまし防止方法	合言葉方式	制御情報
サービス合言葉	合言葉データ	制御情報
PK合言葉	合言葉データ	制御情報
action	プログラム	制御情報
番組嗜好情報	スポーツ10 バラエティ7 音楽5 その他3	制御情報

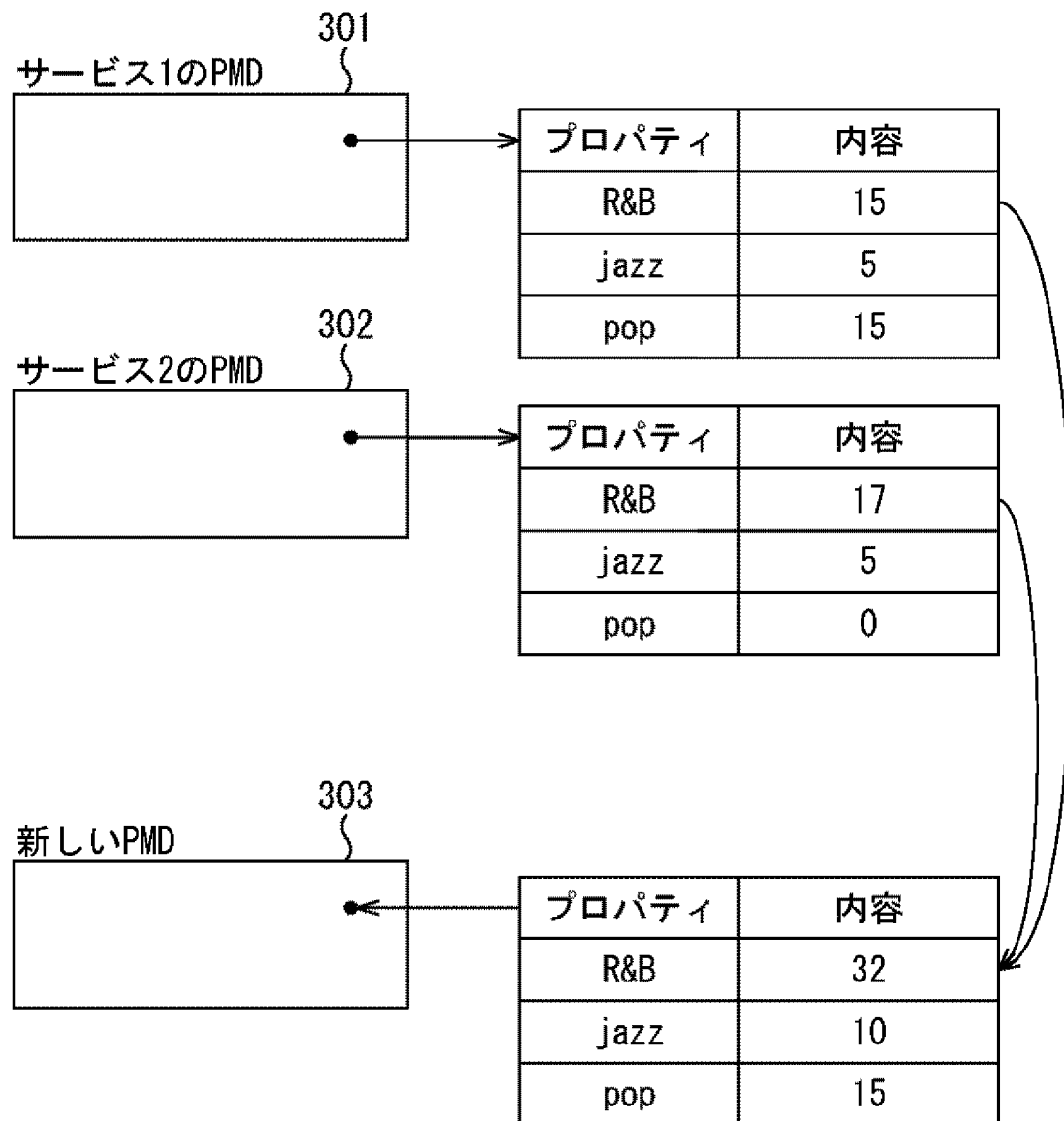
・
・
・

図21



[図22]

図22



[図23]

図23

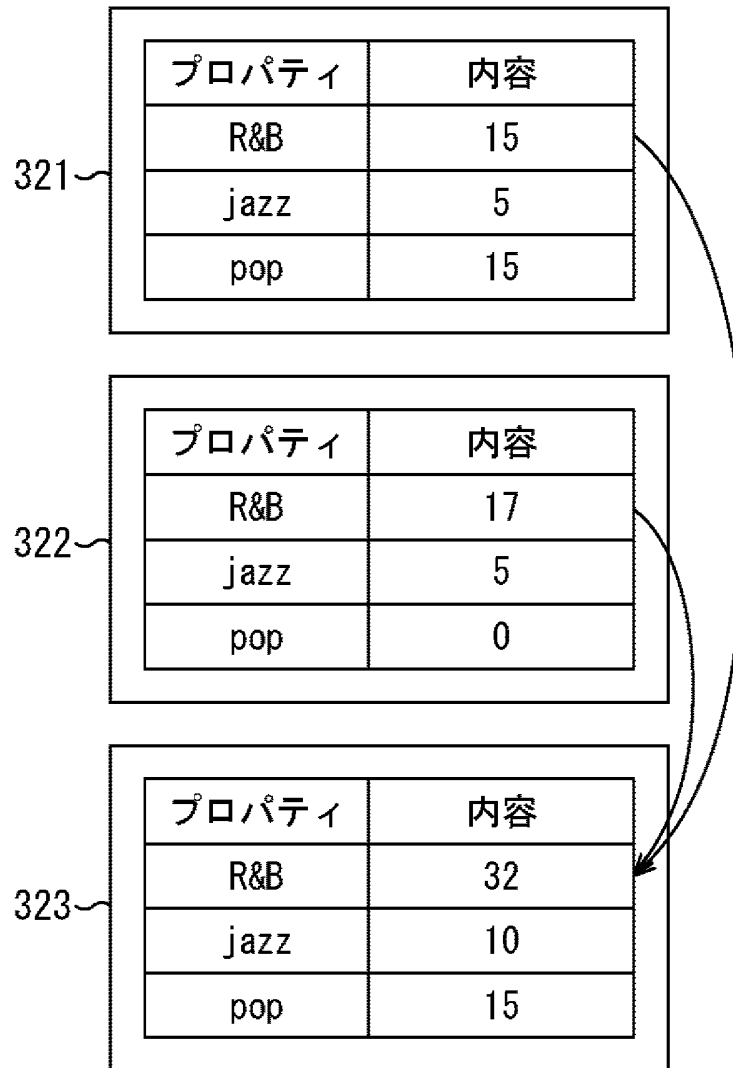


図24

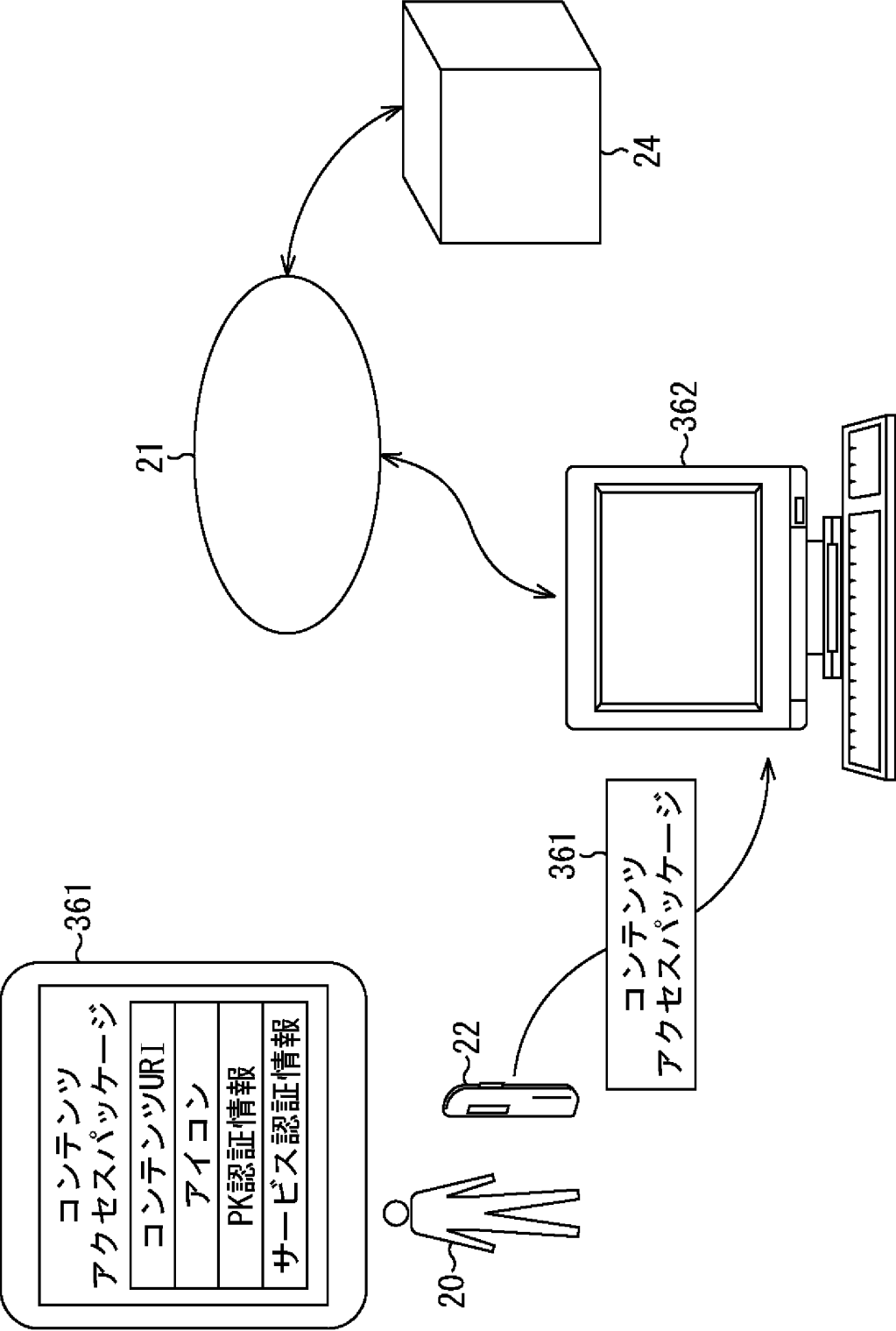
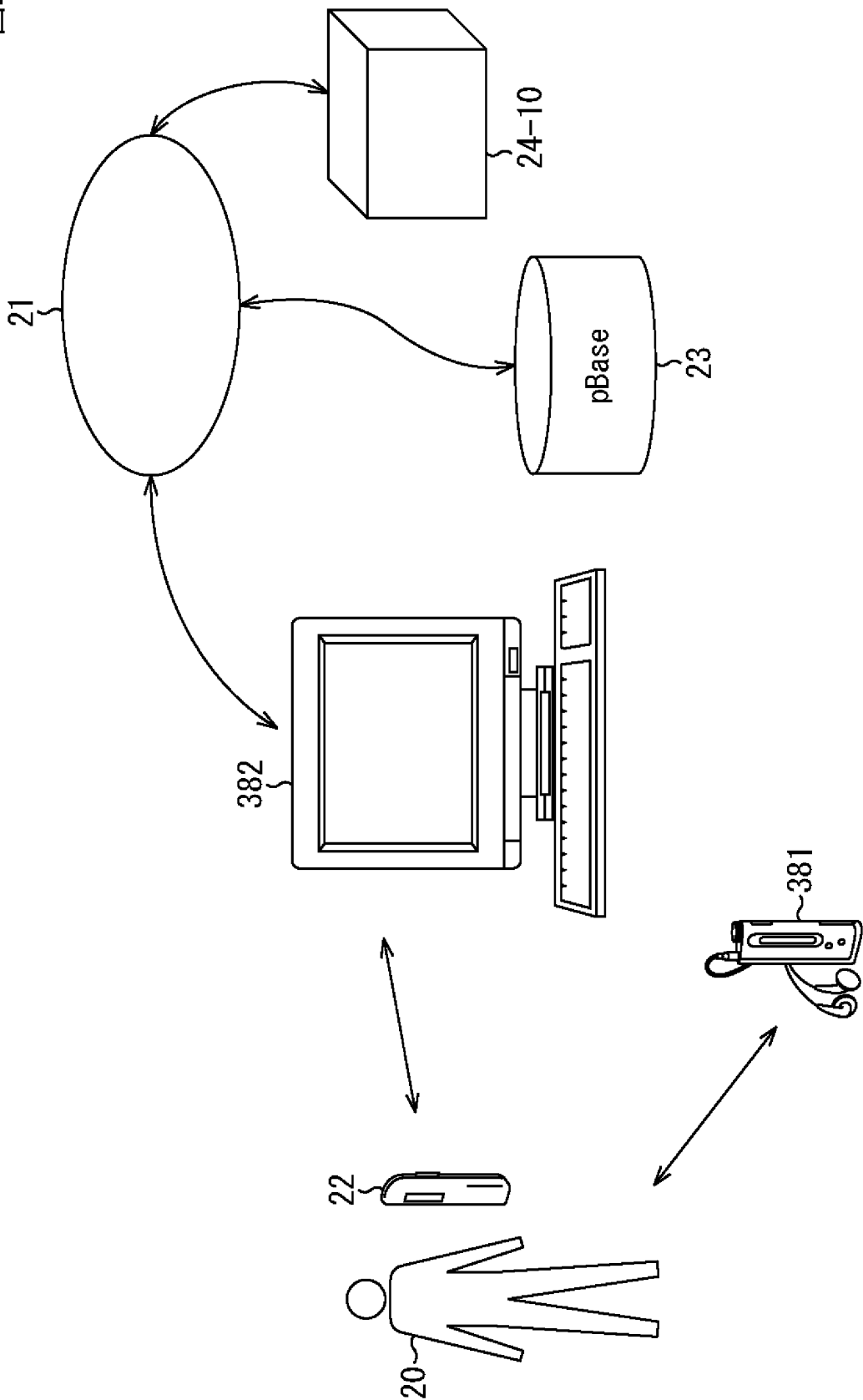
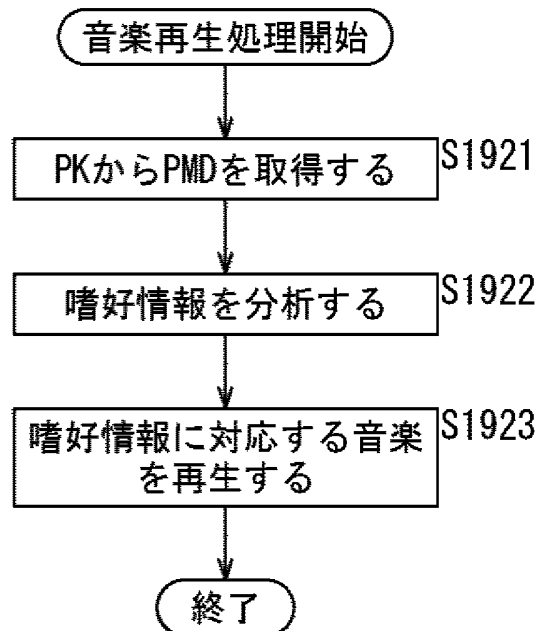


図25



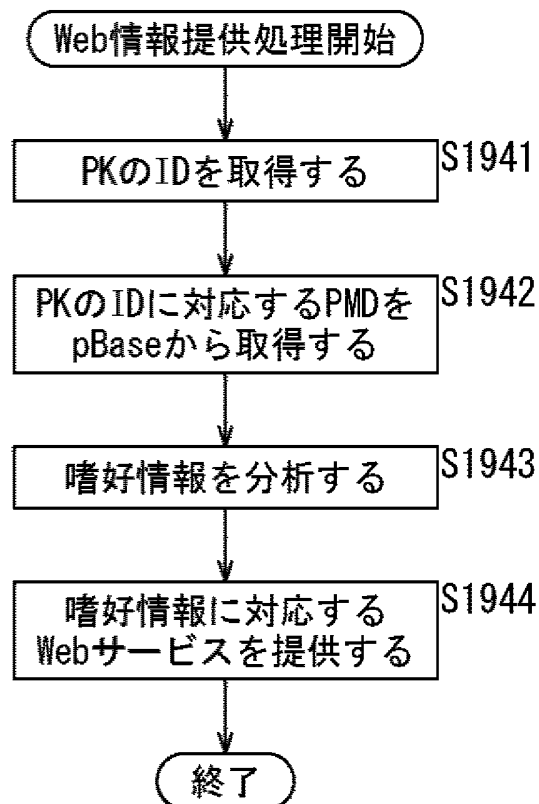
[図26]

図26



[図27]

図27



[図28]

図28

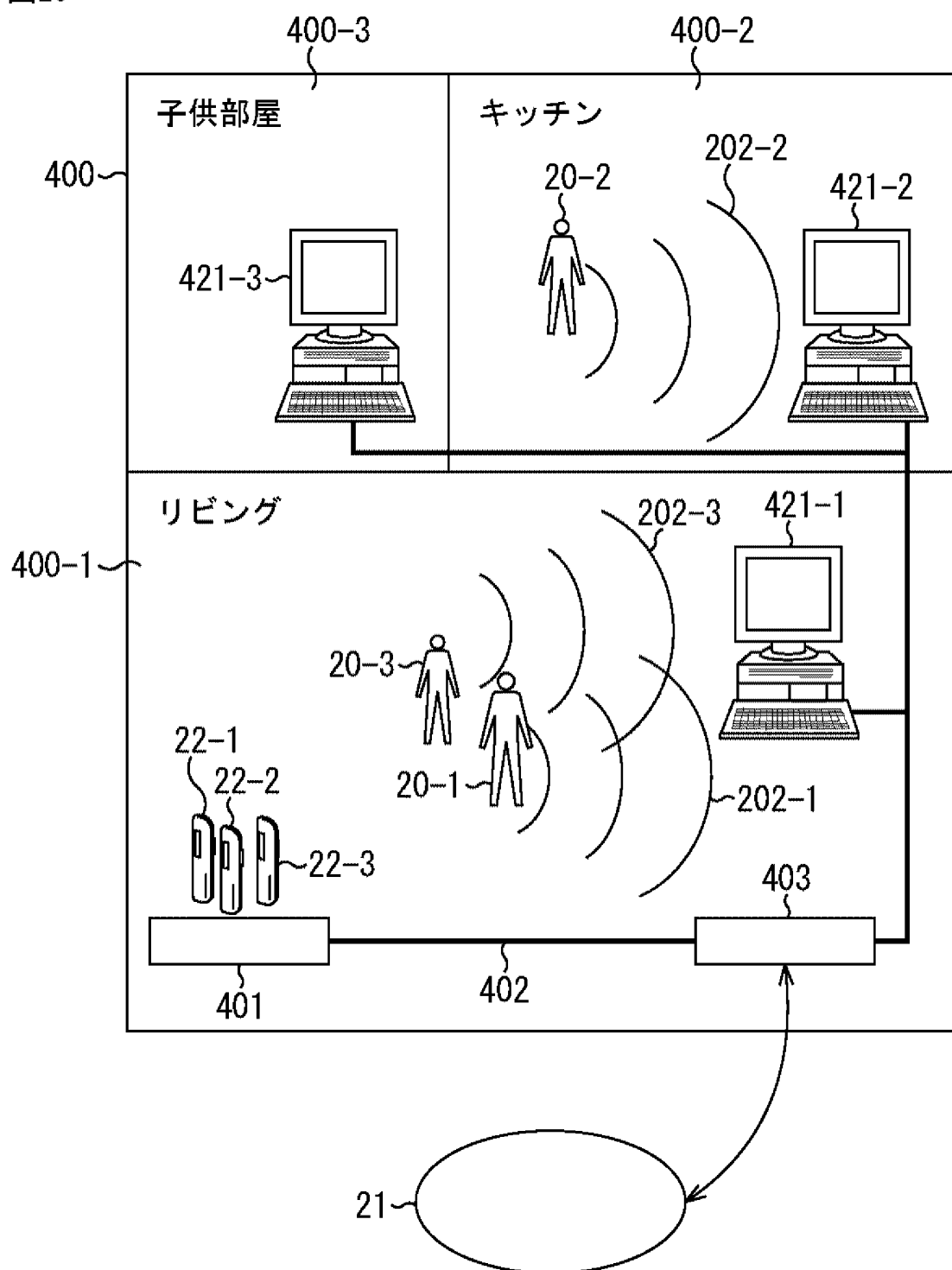


図29

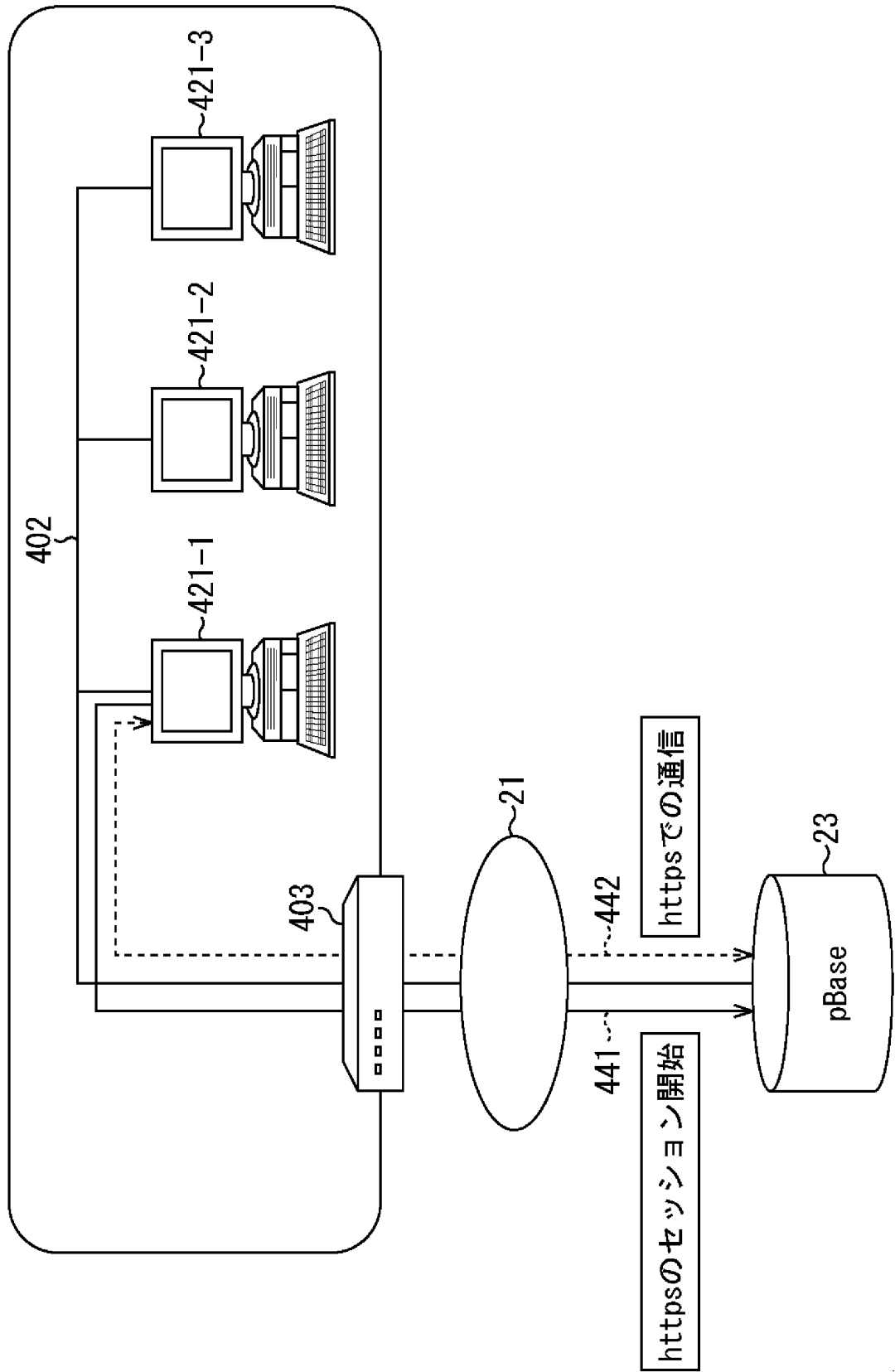
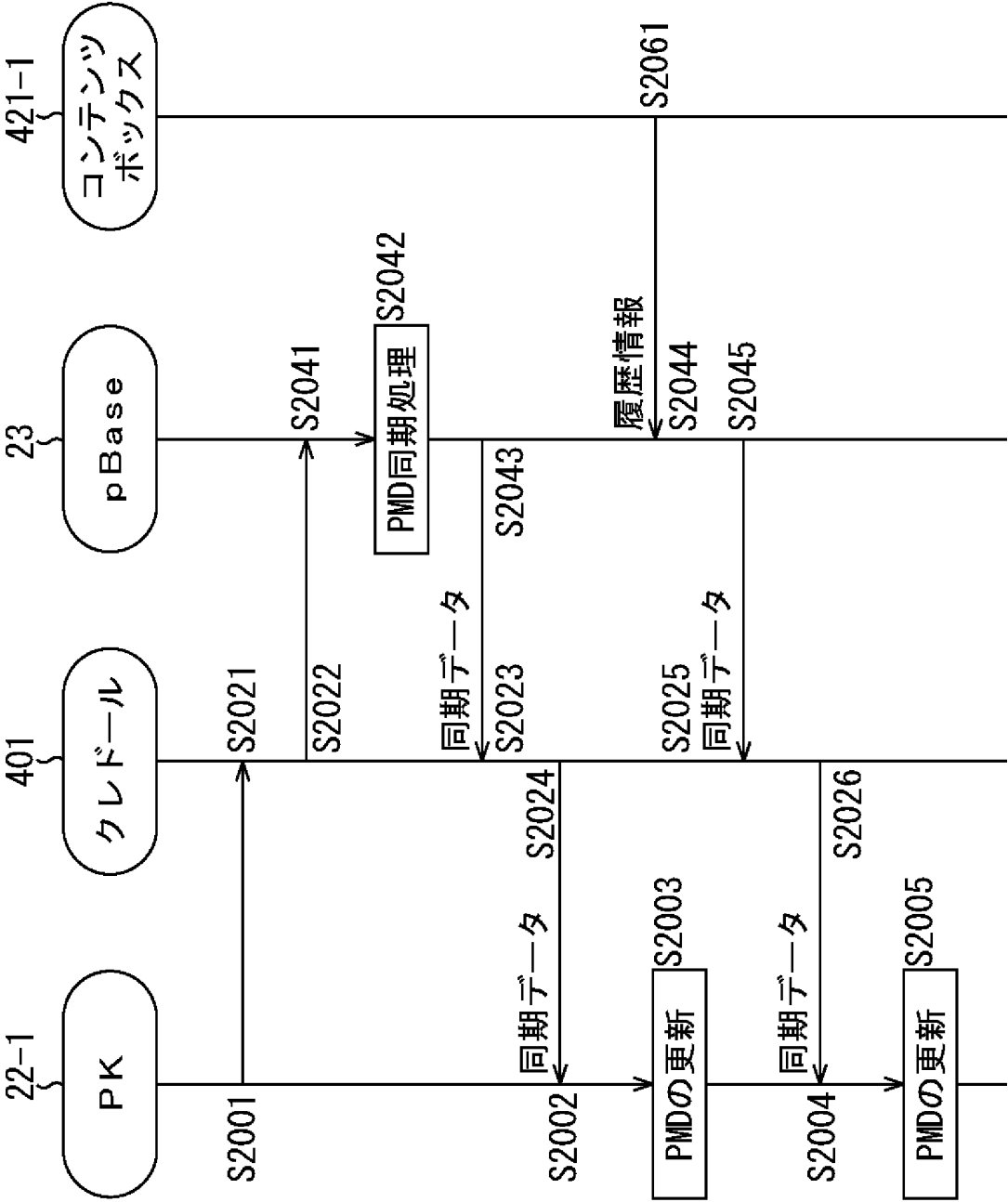


図30



[図31]

図31

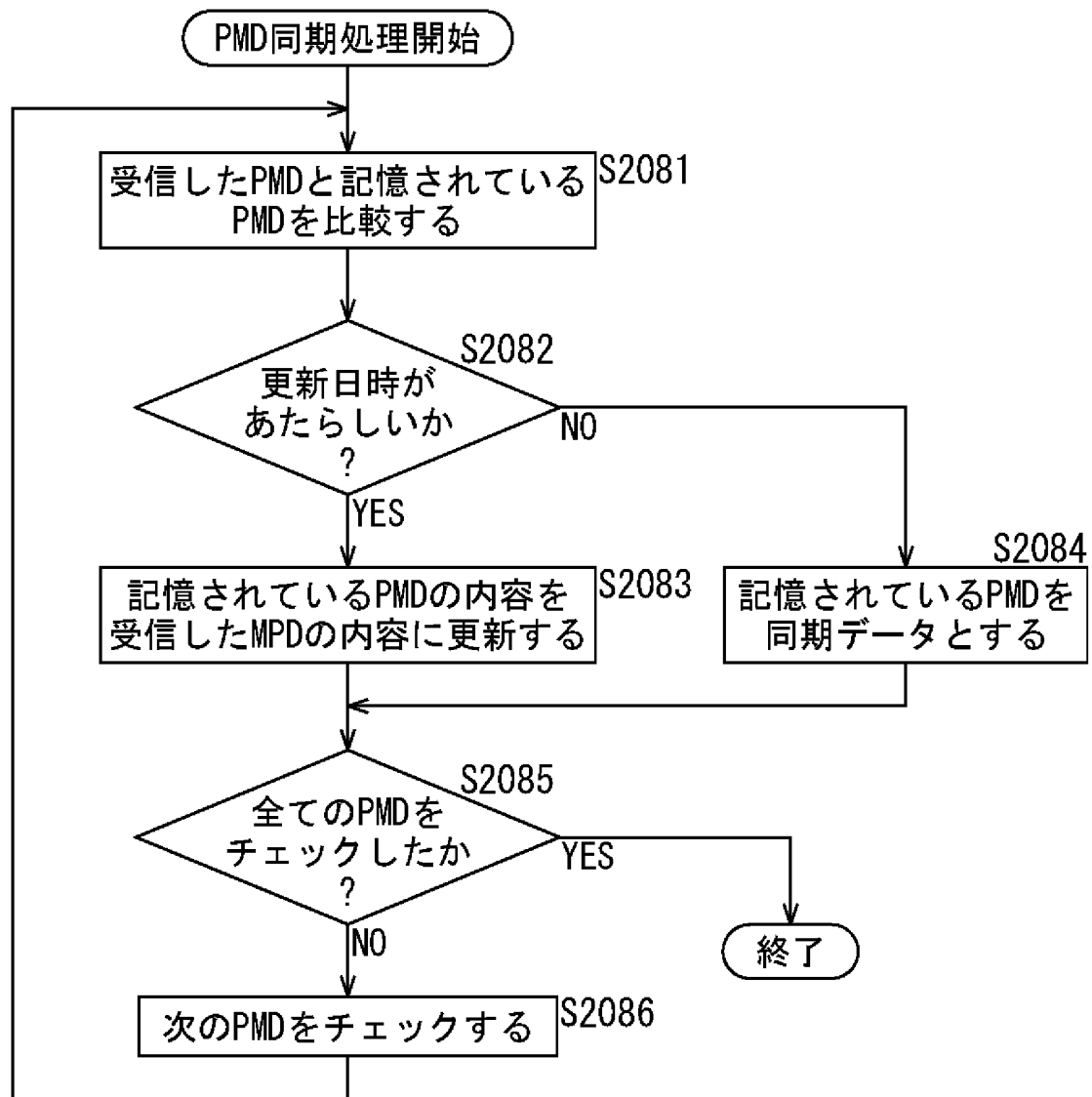


図32

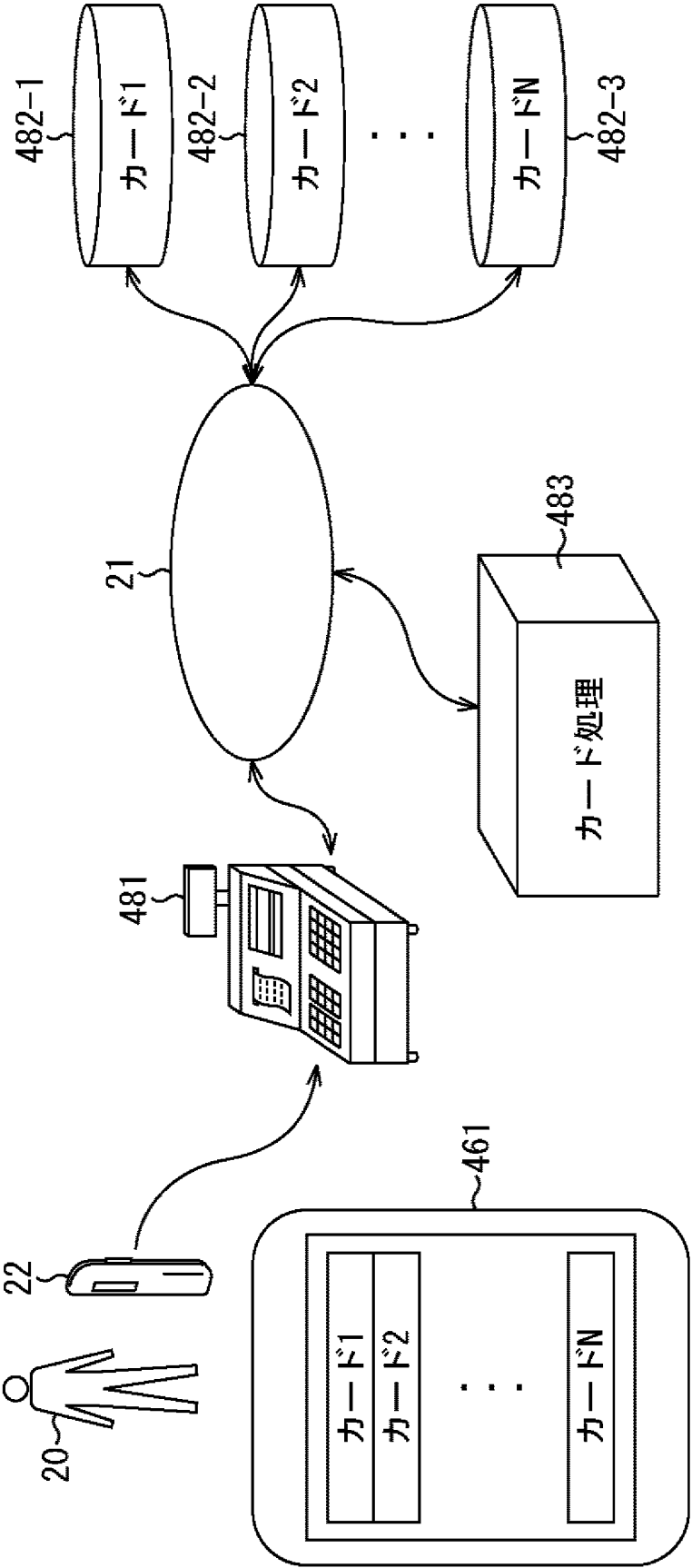


図33

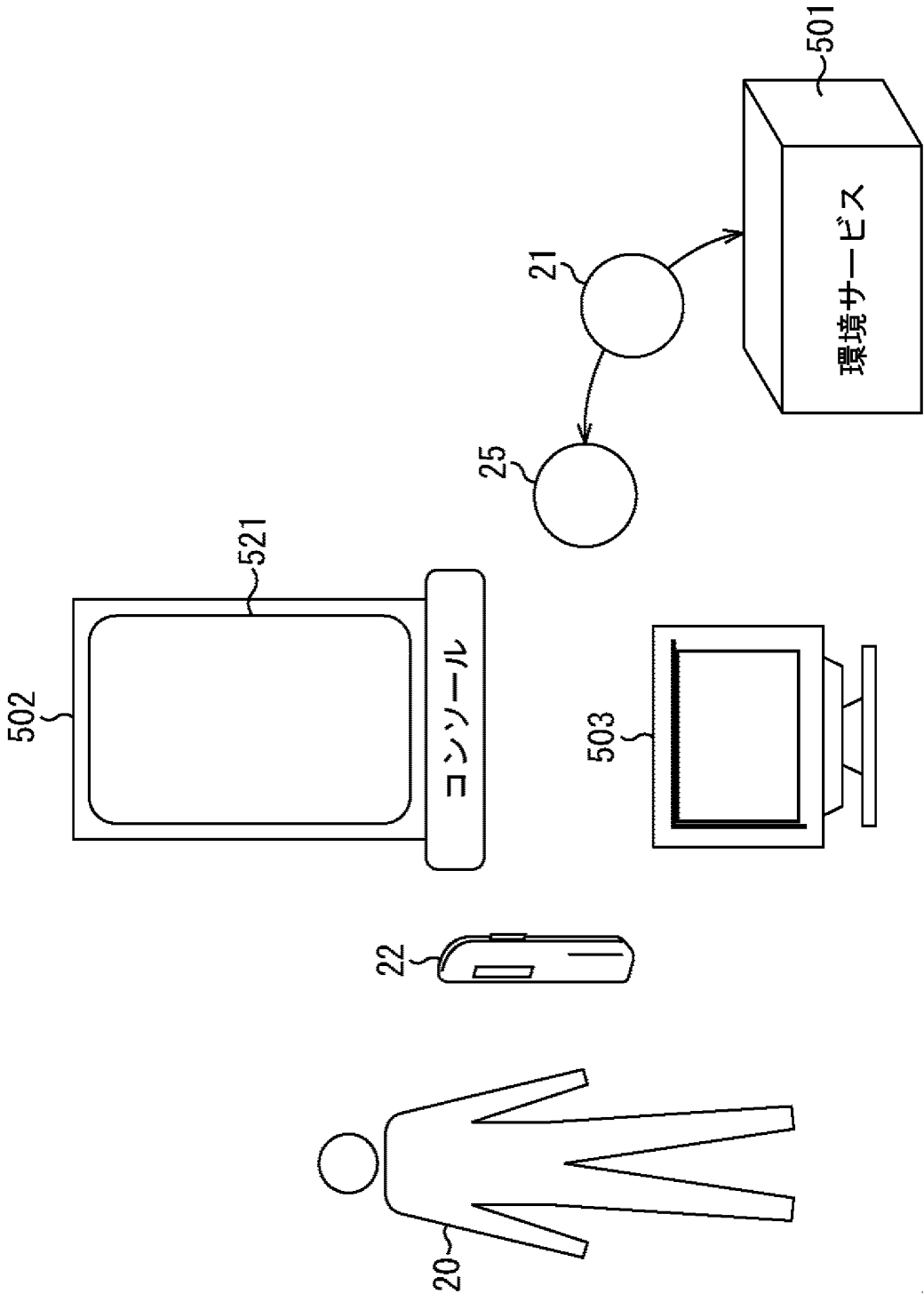


図34

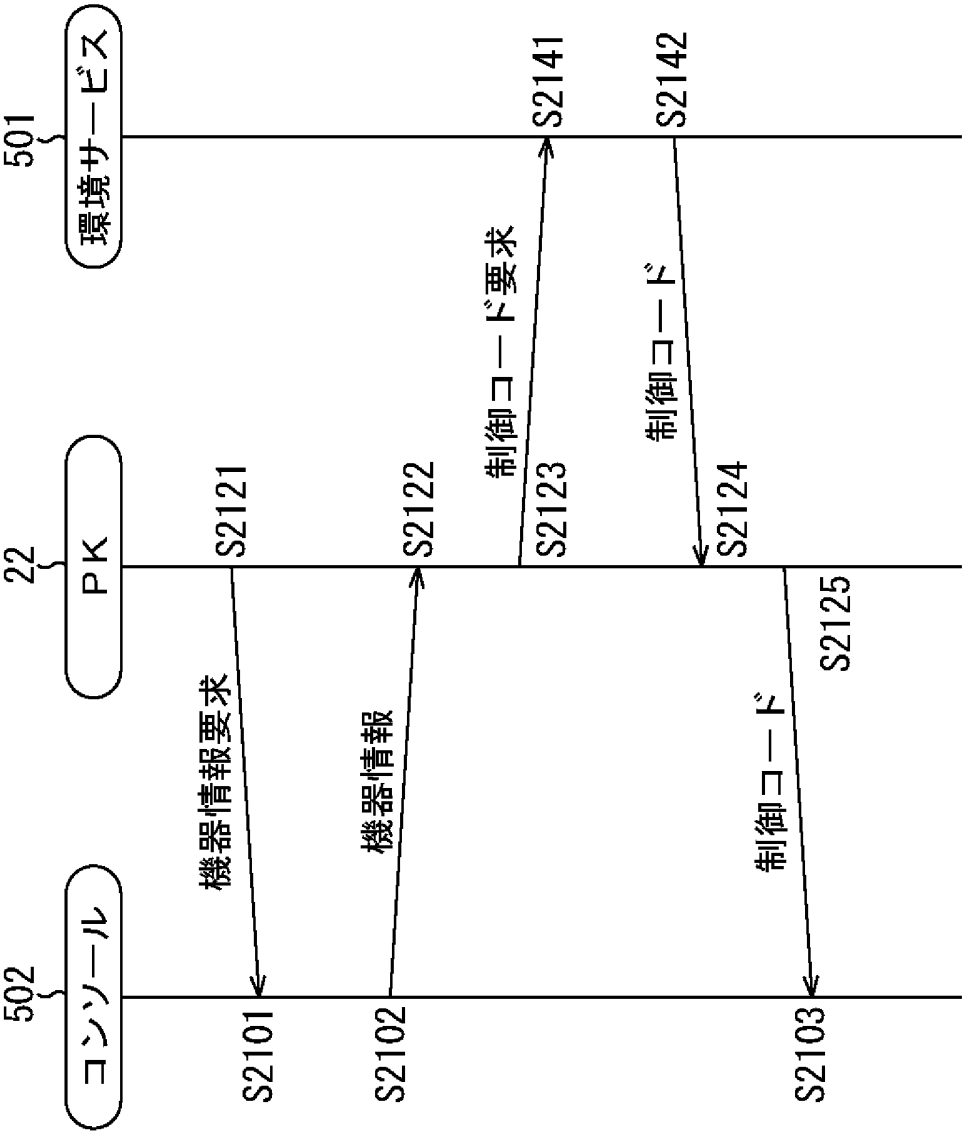
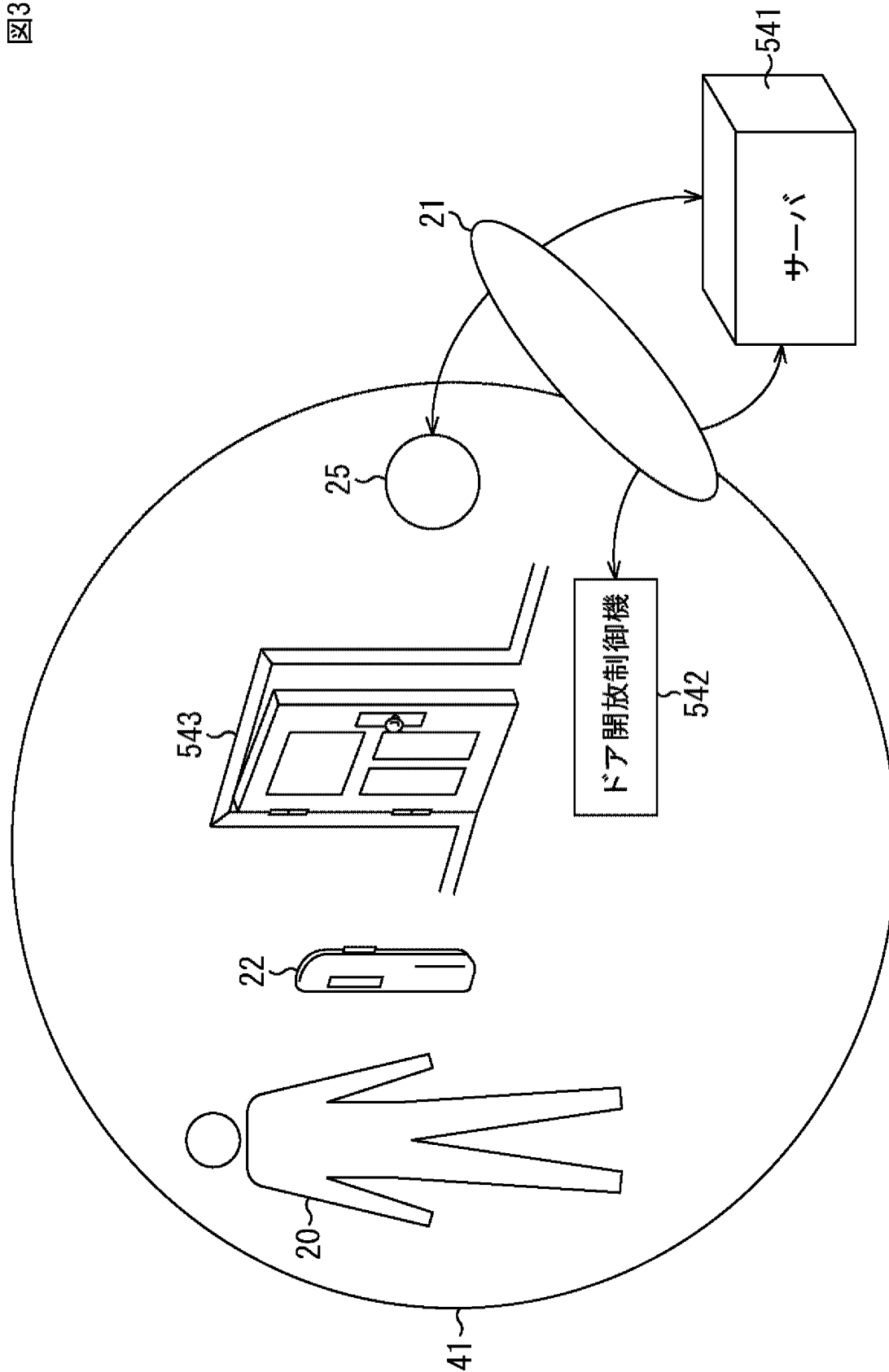


図35 [図35]



[図36]

図36

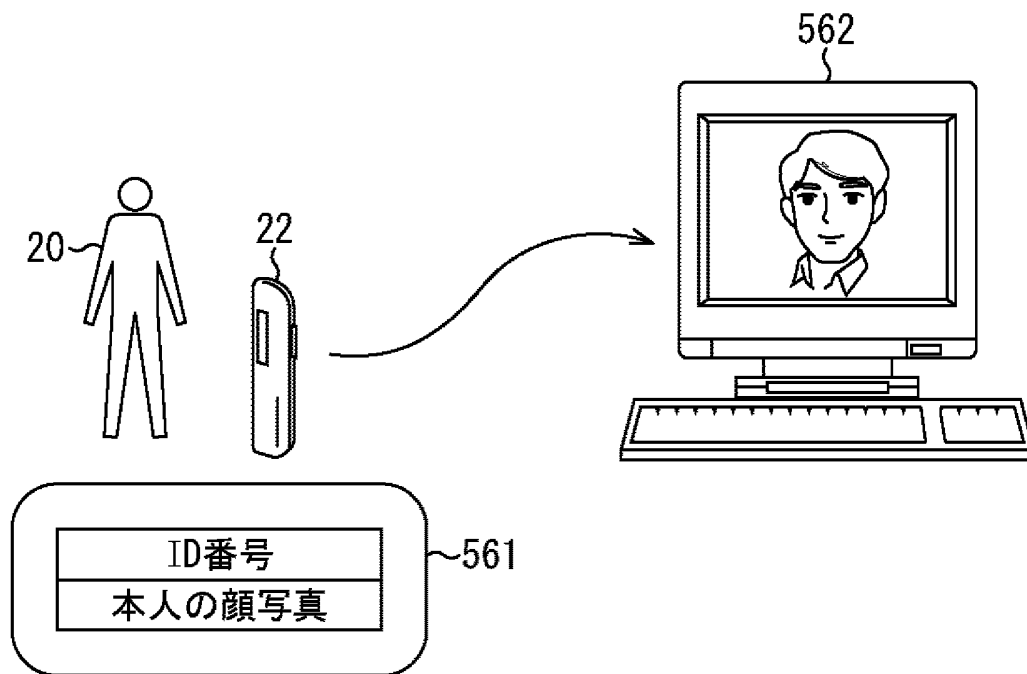


図37 [図37]

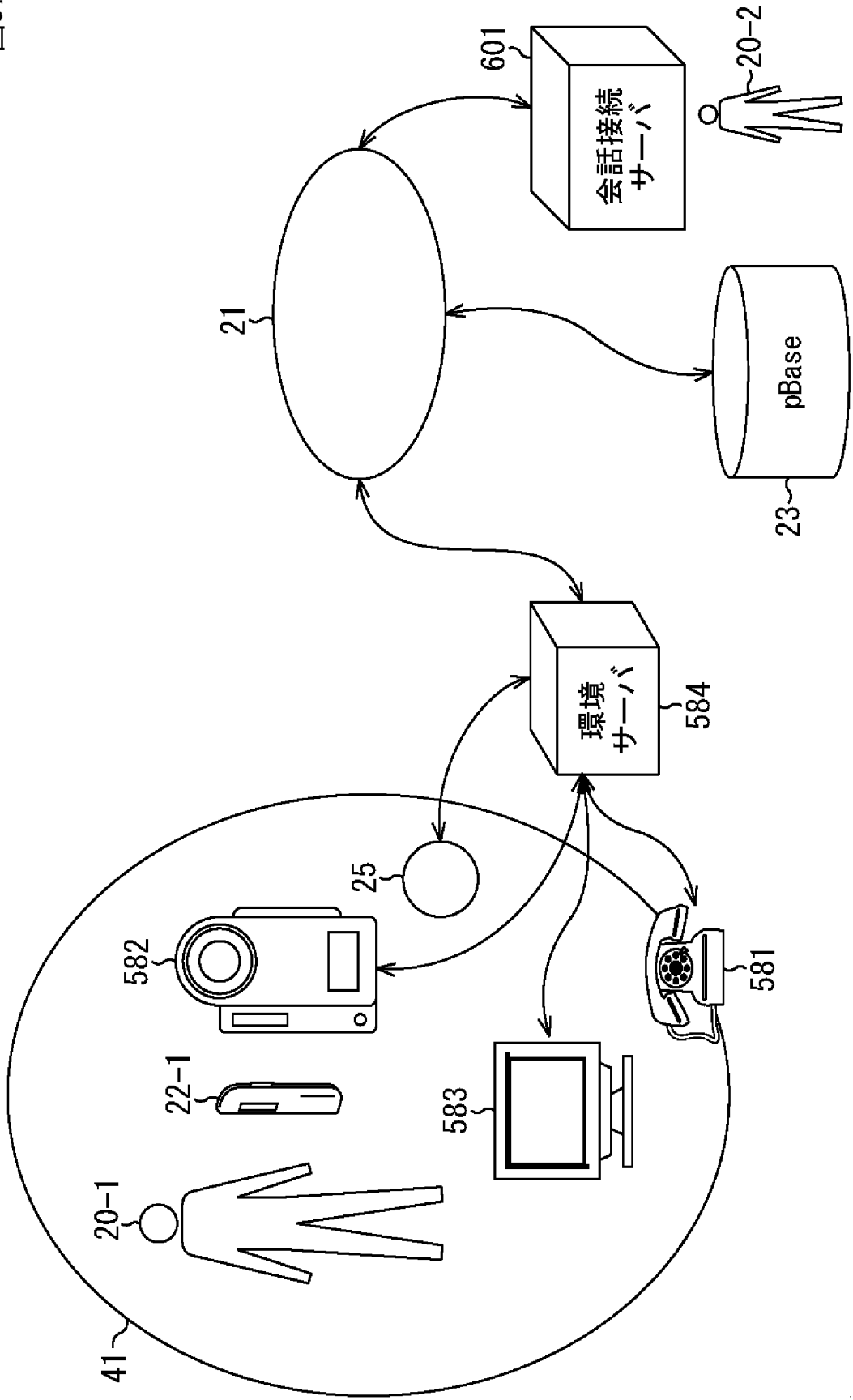


図38

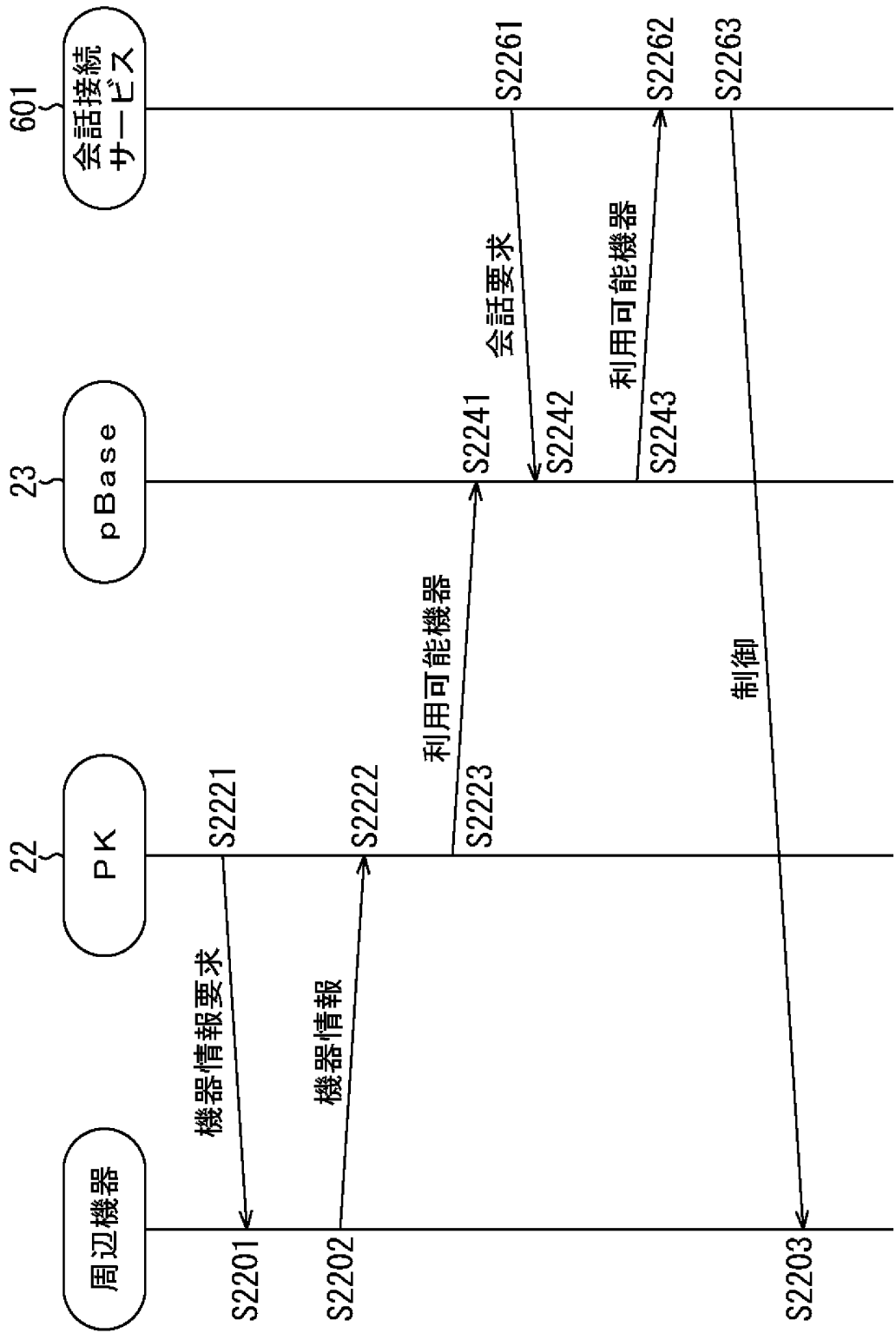


図39

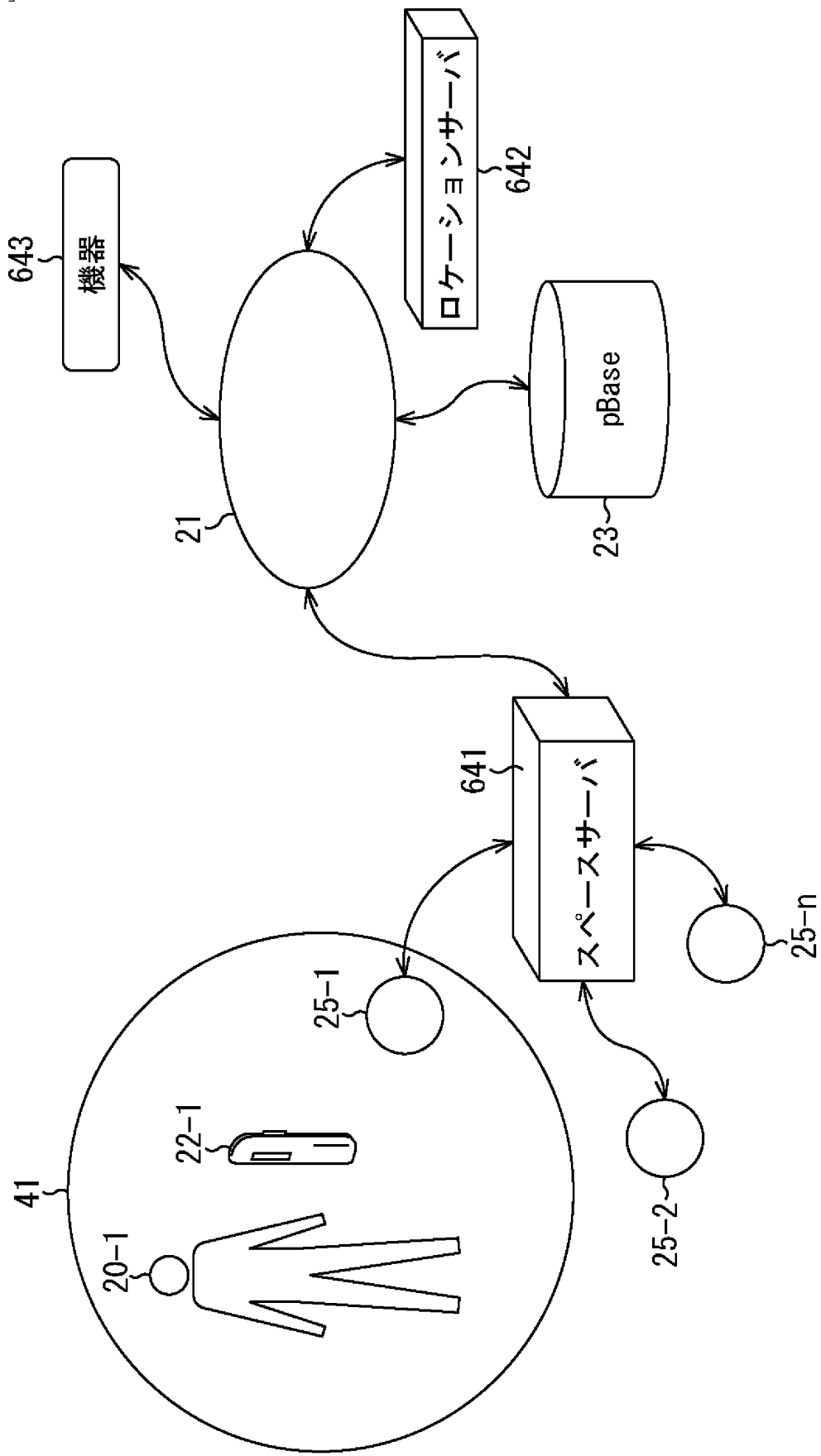
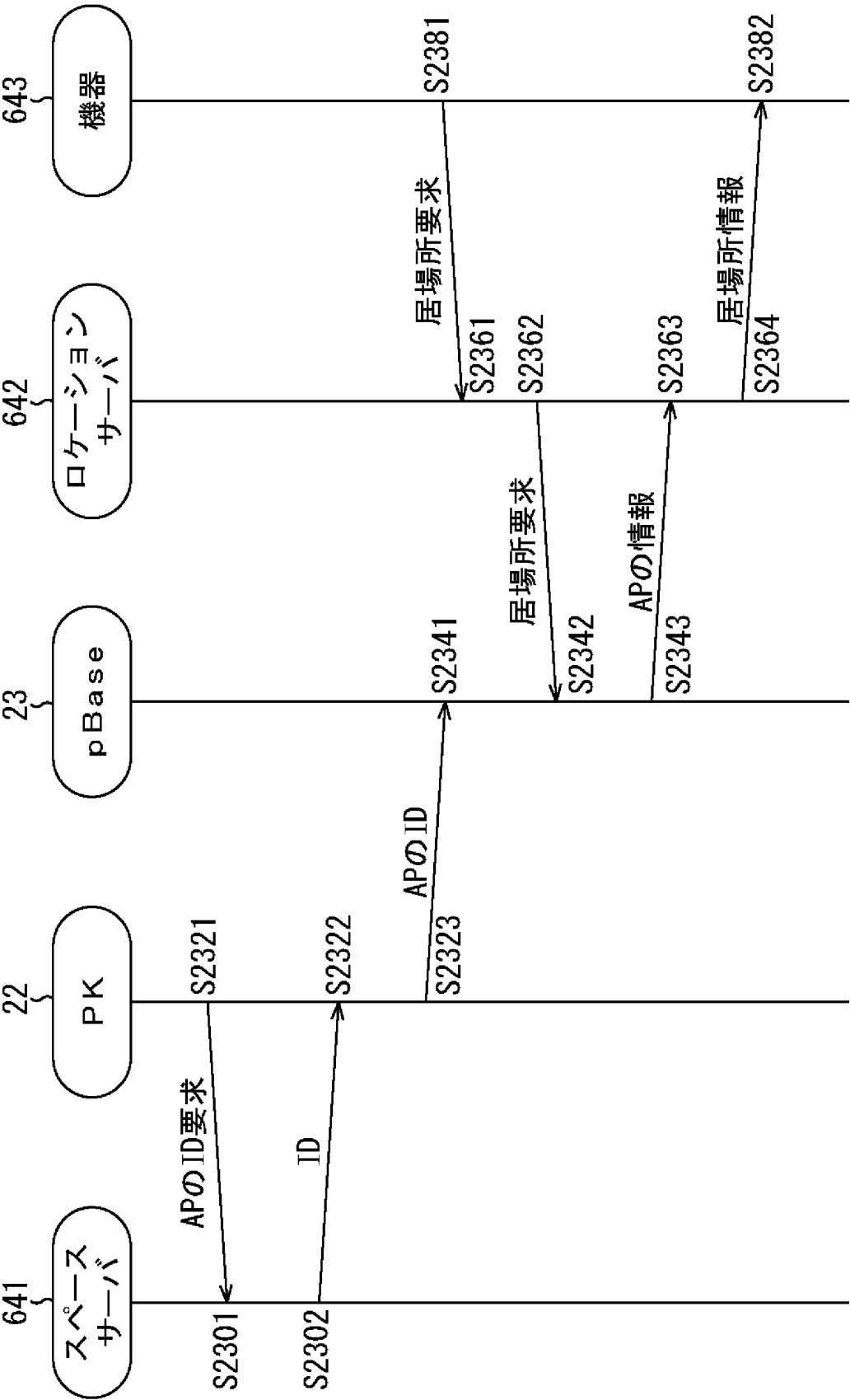


図40



[図41]

図41

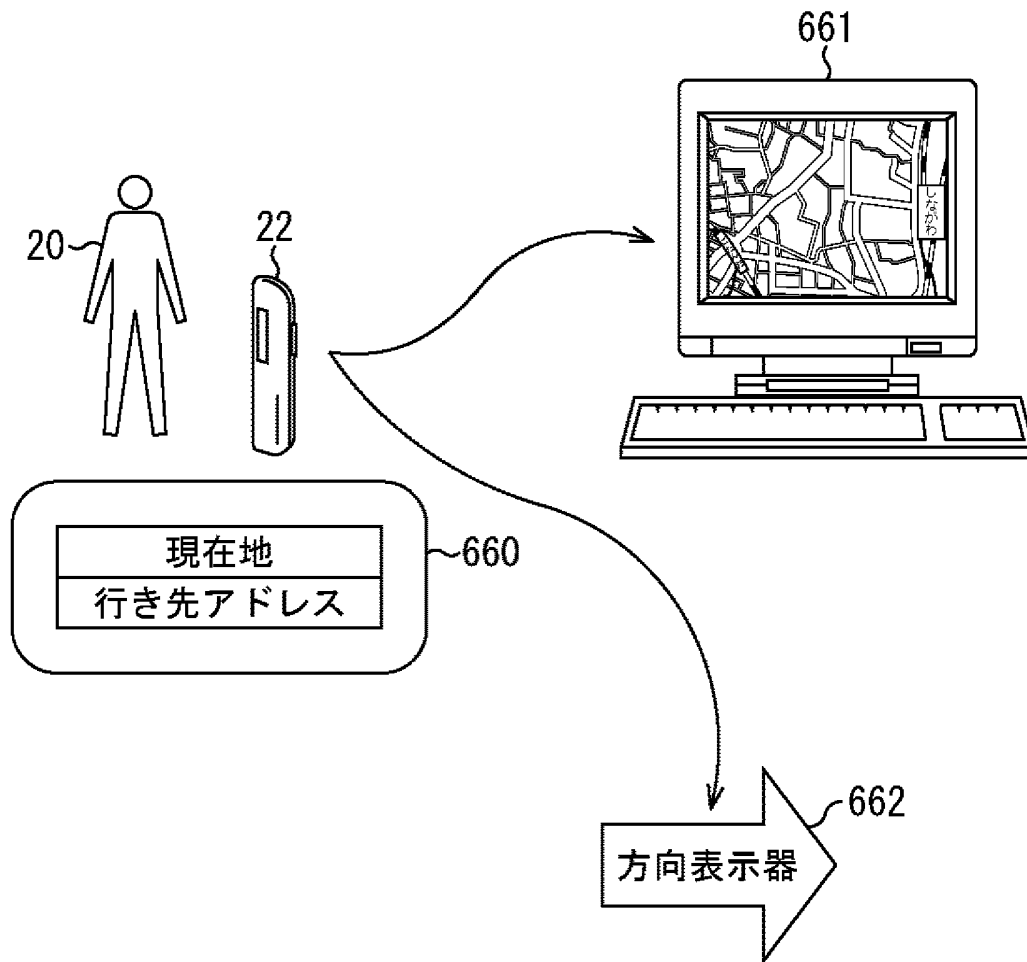
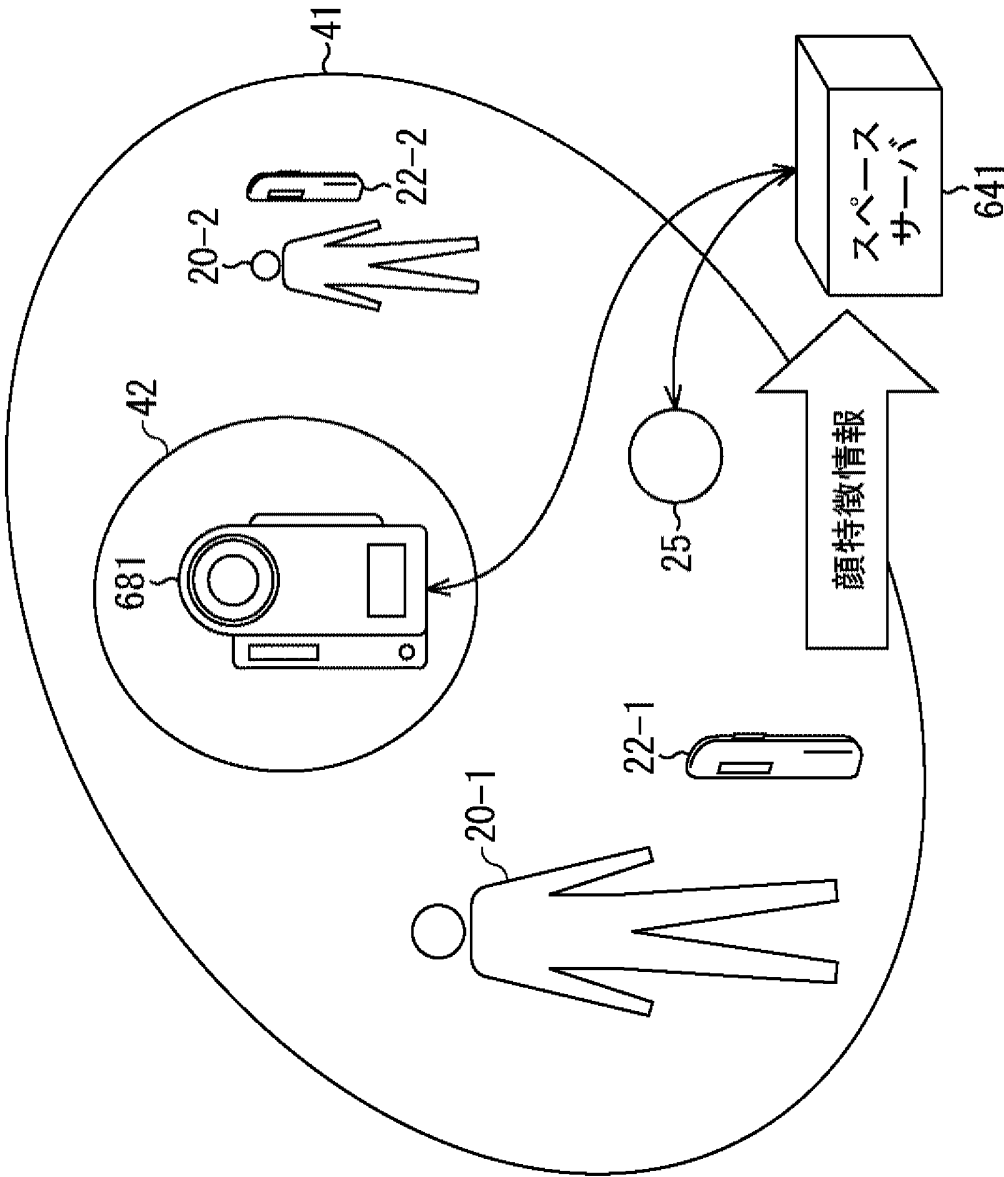


図42



[図43]

図43

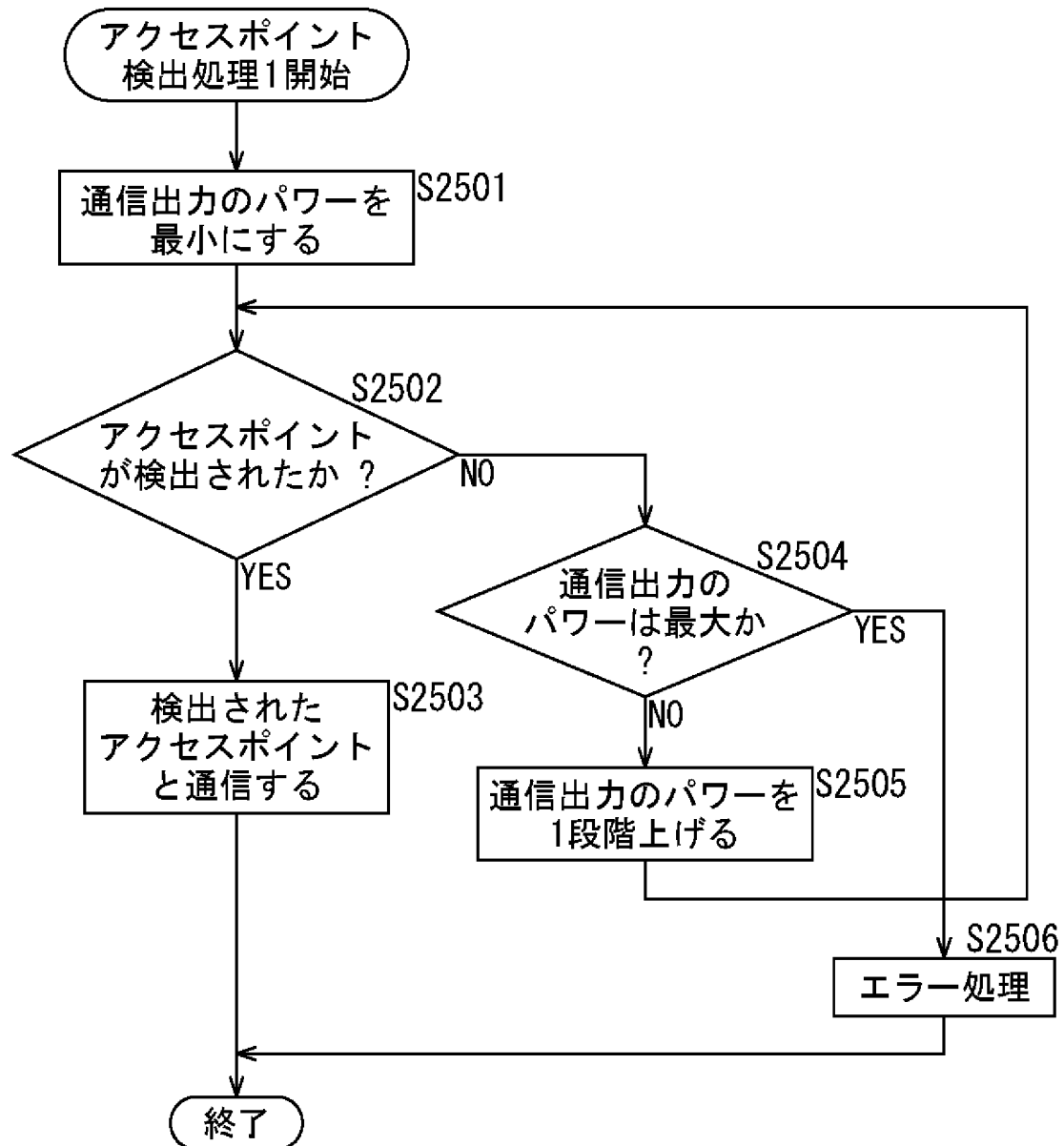
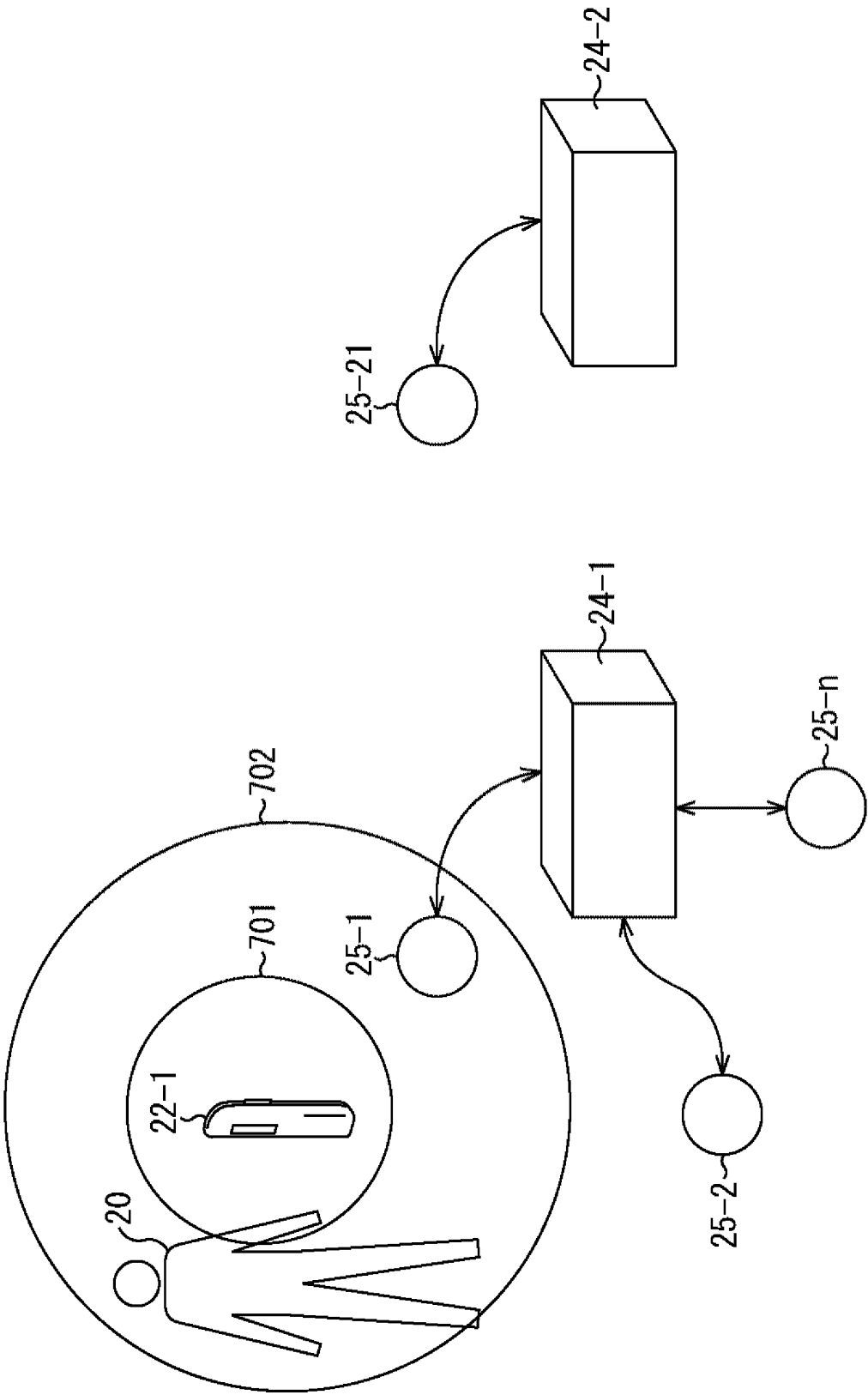
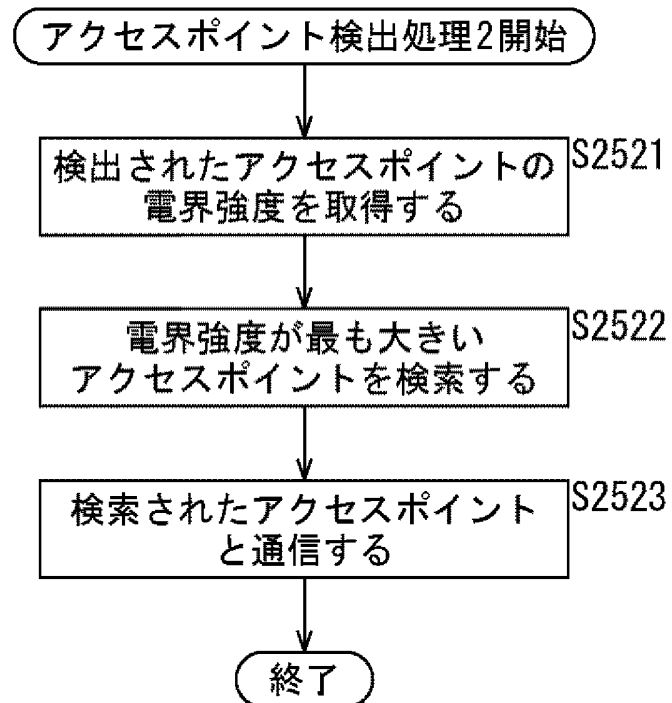


図44



[図45]

図45



[図46]

図46

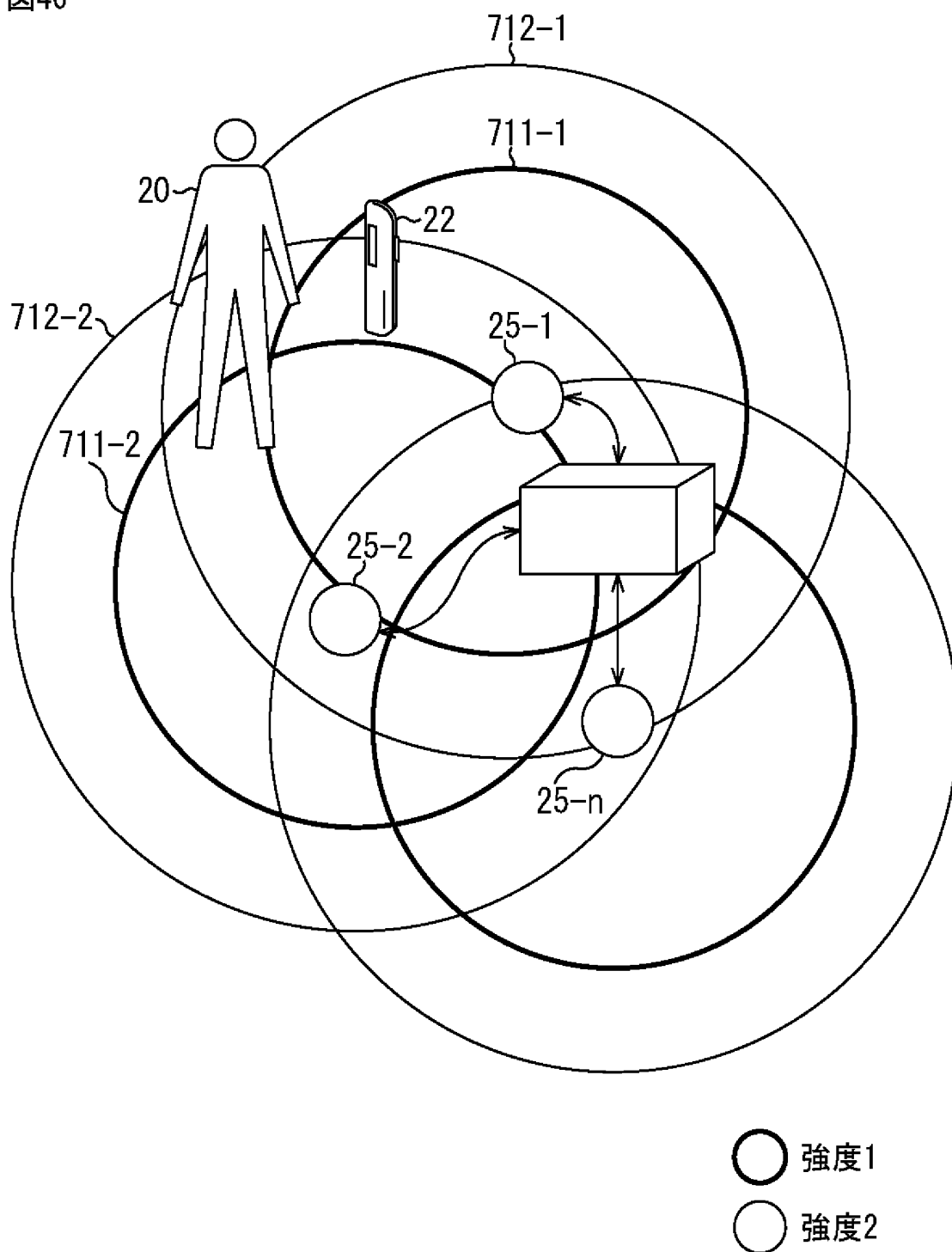
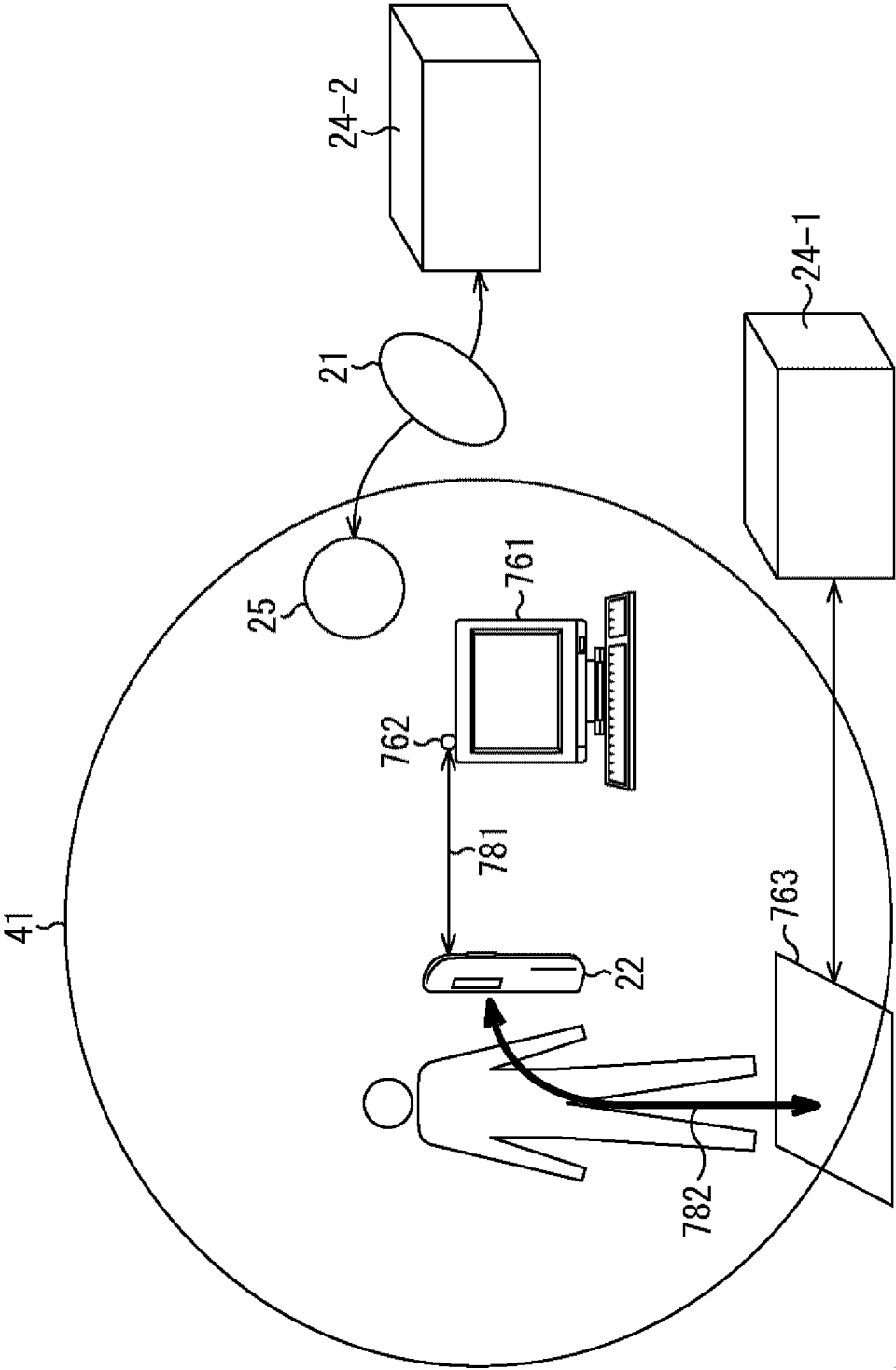


図47



[図48]

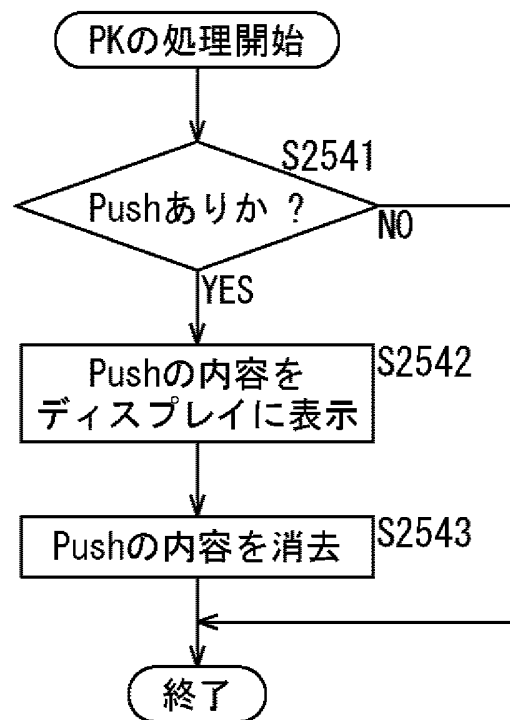
図48

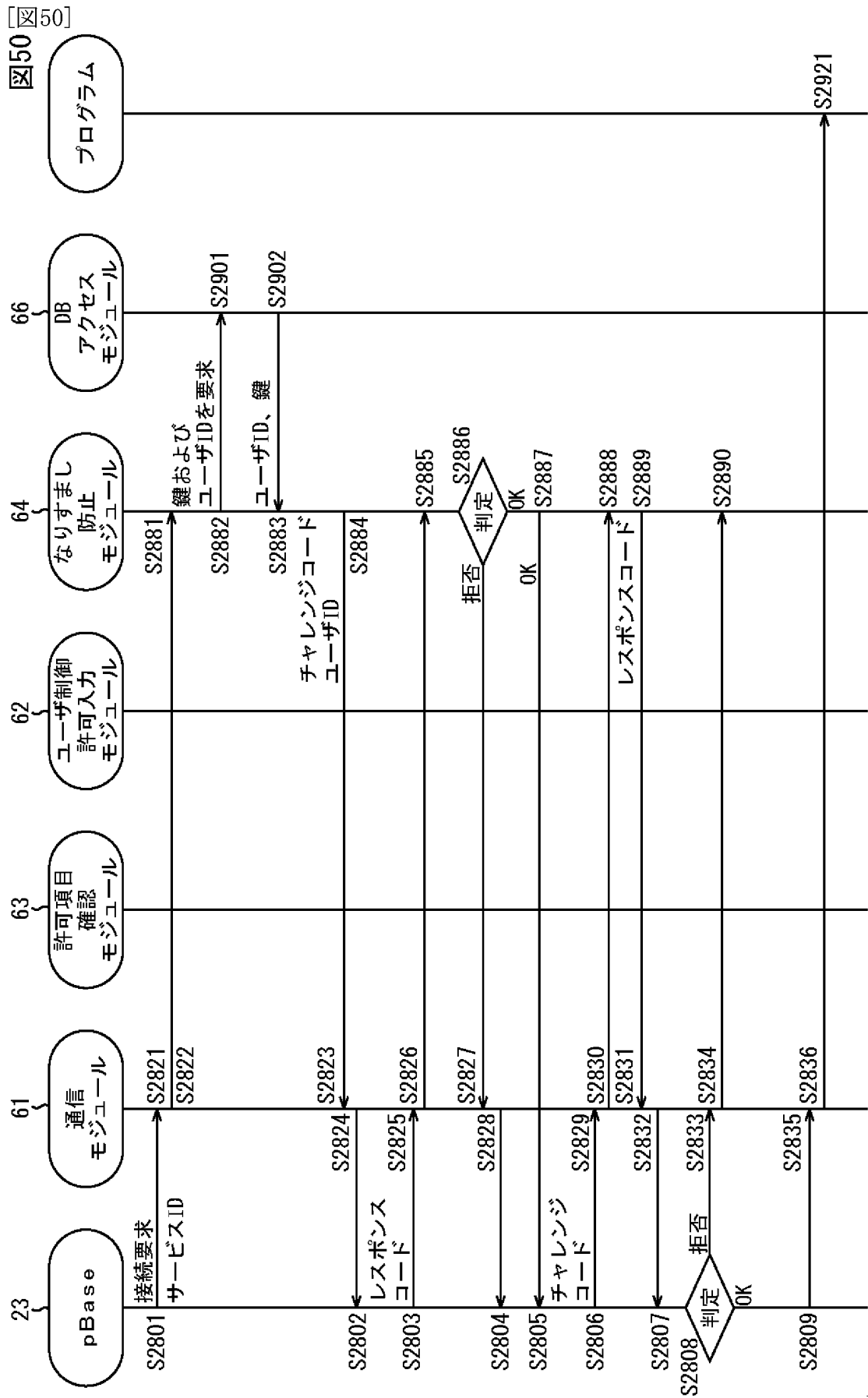
801~

プロパティ	内容
プログラム	プログラムコード実体
name	foo
push	「緊急の連絡あり…」

[図49]

図49





[図51]

図51

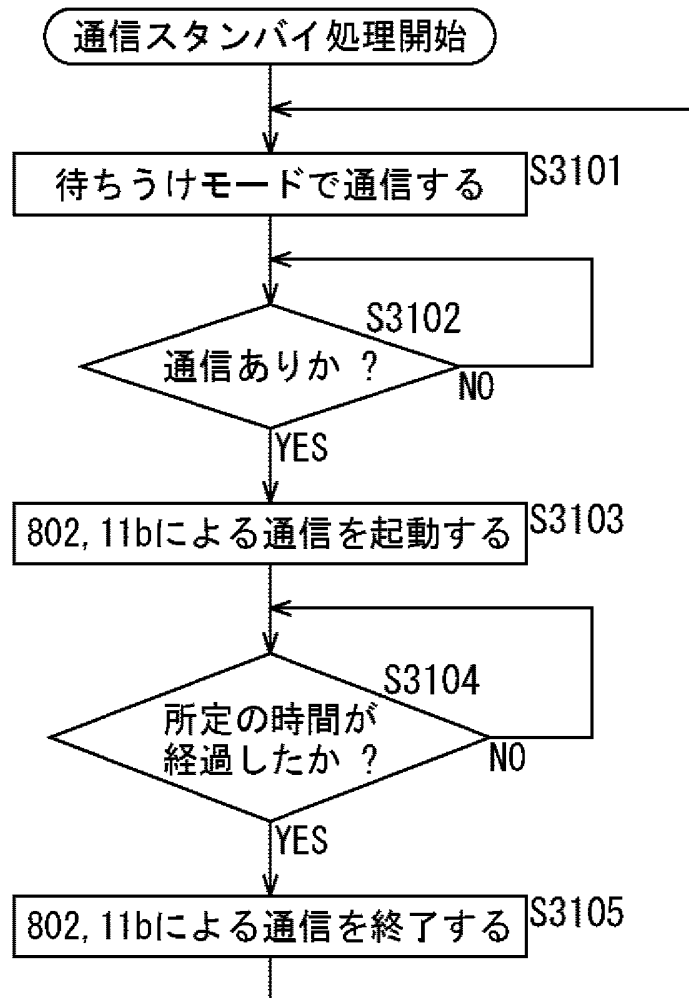
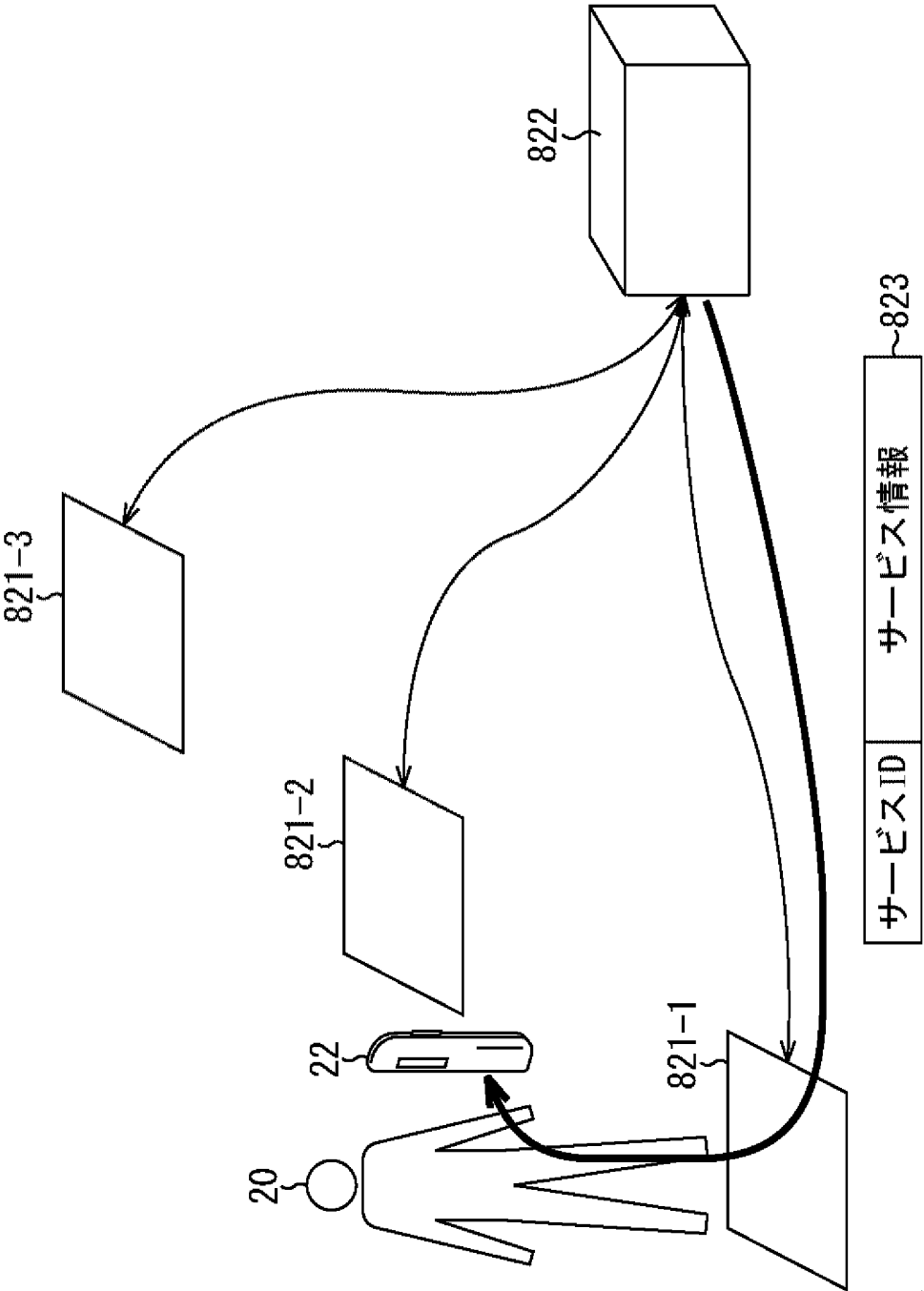
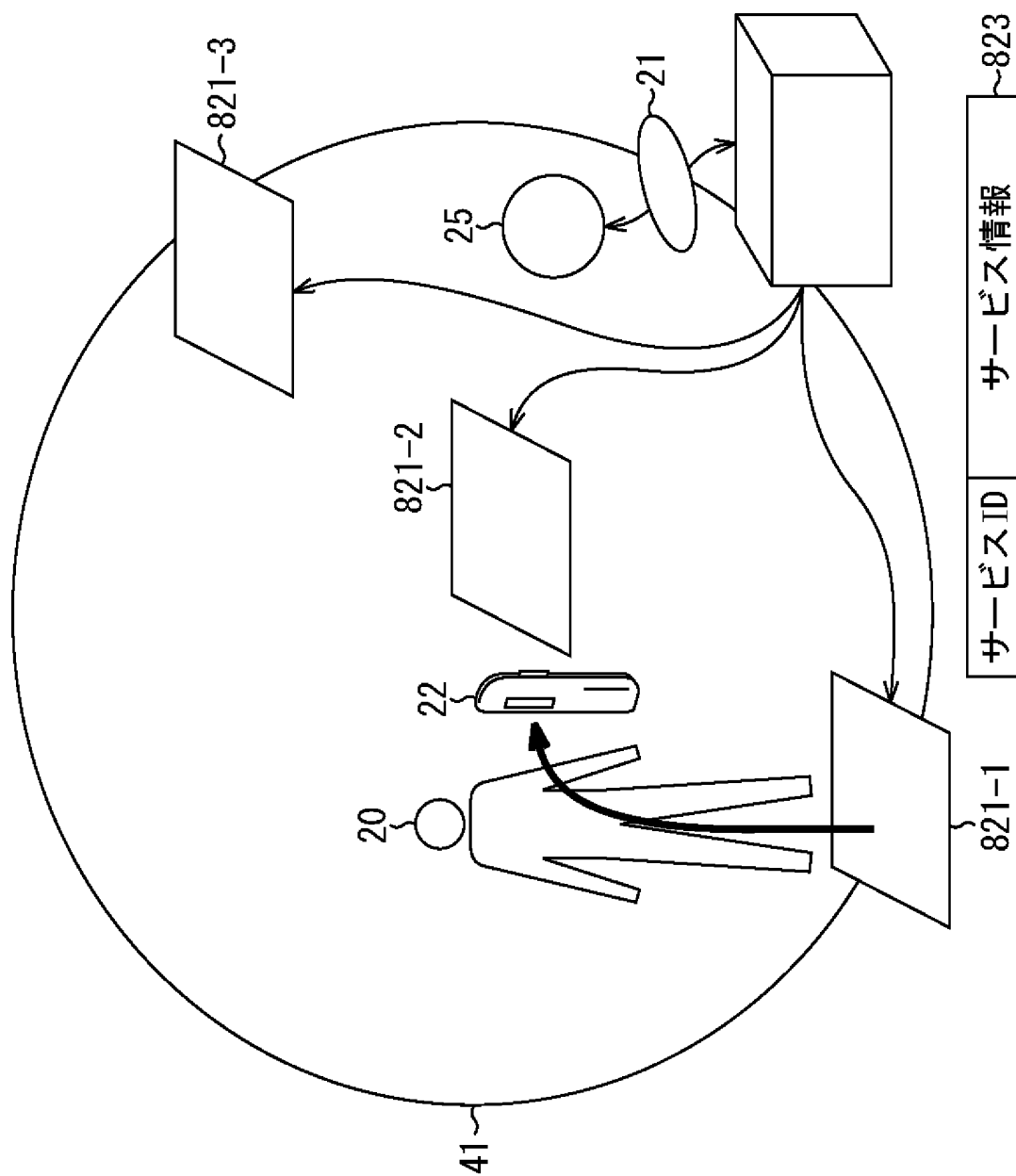


図52

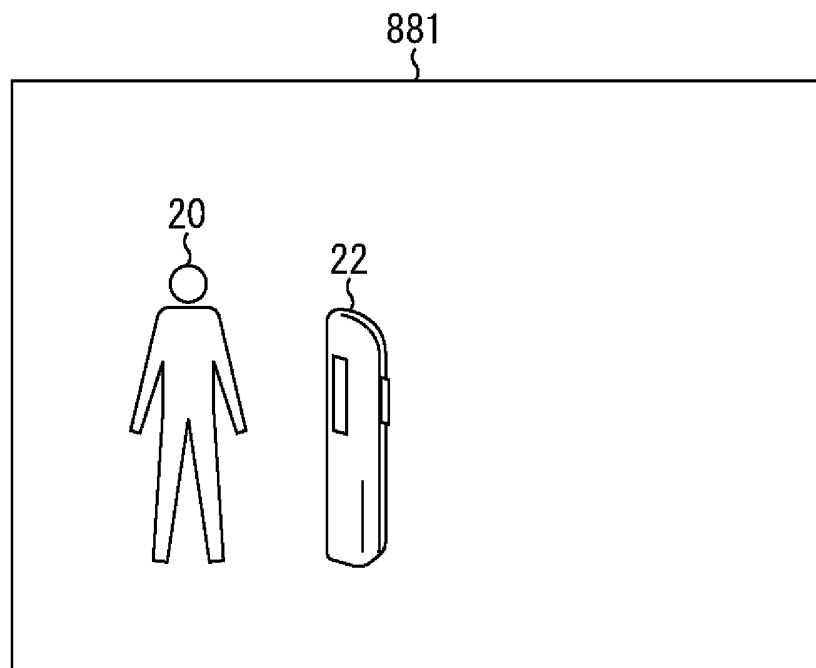


53



[図54A]

図54A



[図54B]

図54B

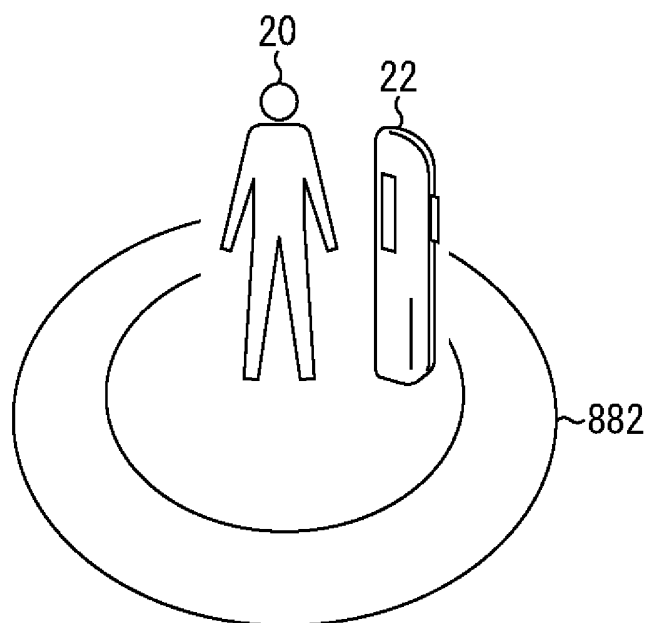


図55

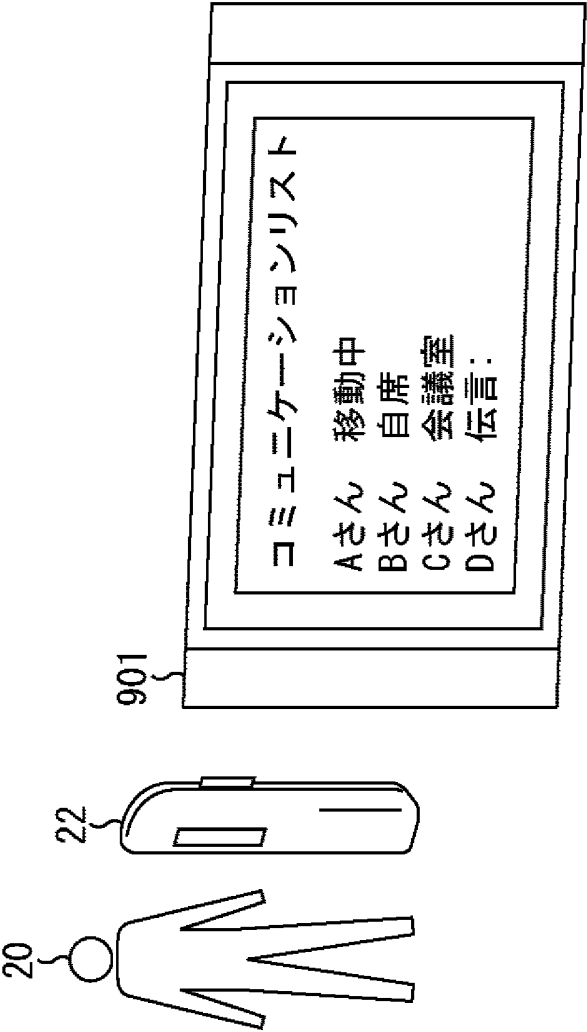
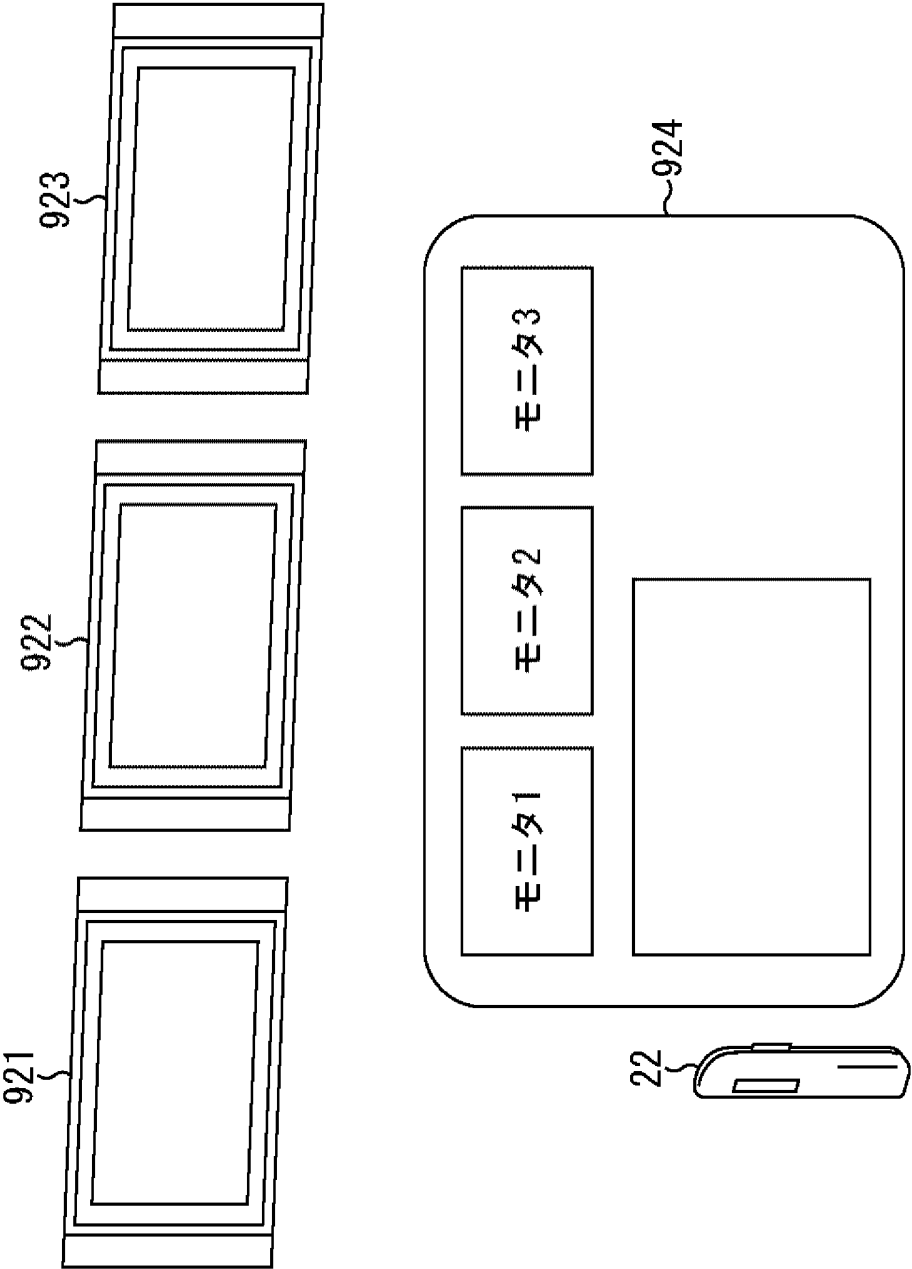
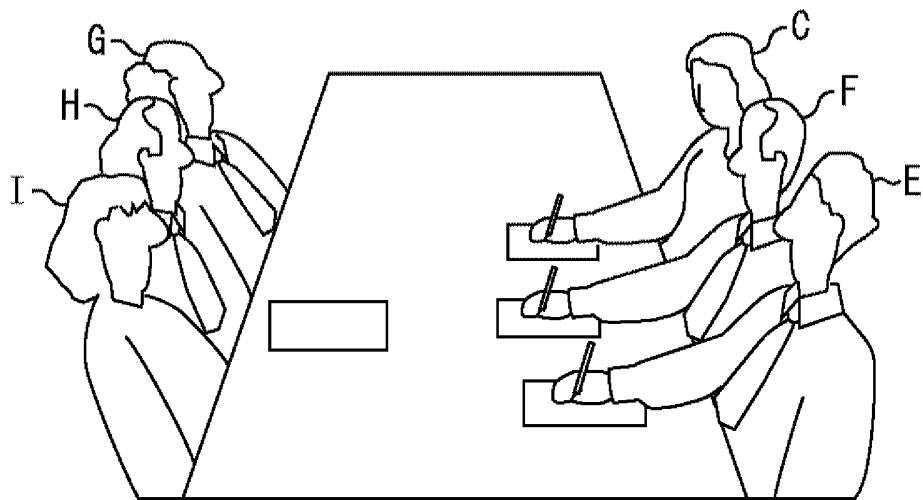


図56



[図57]

図57



58

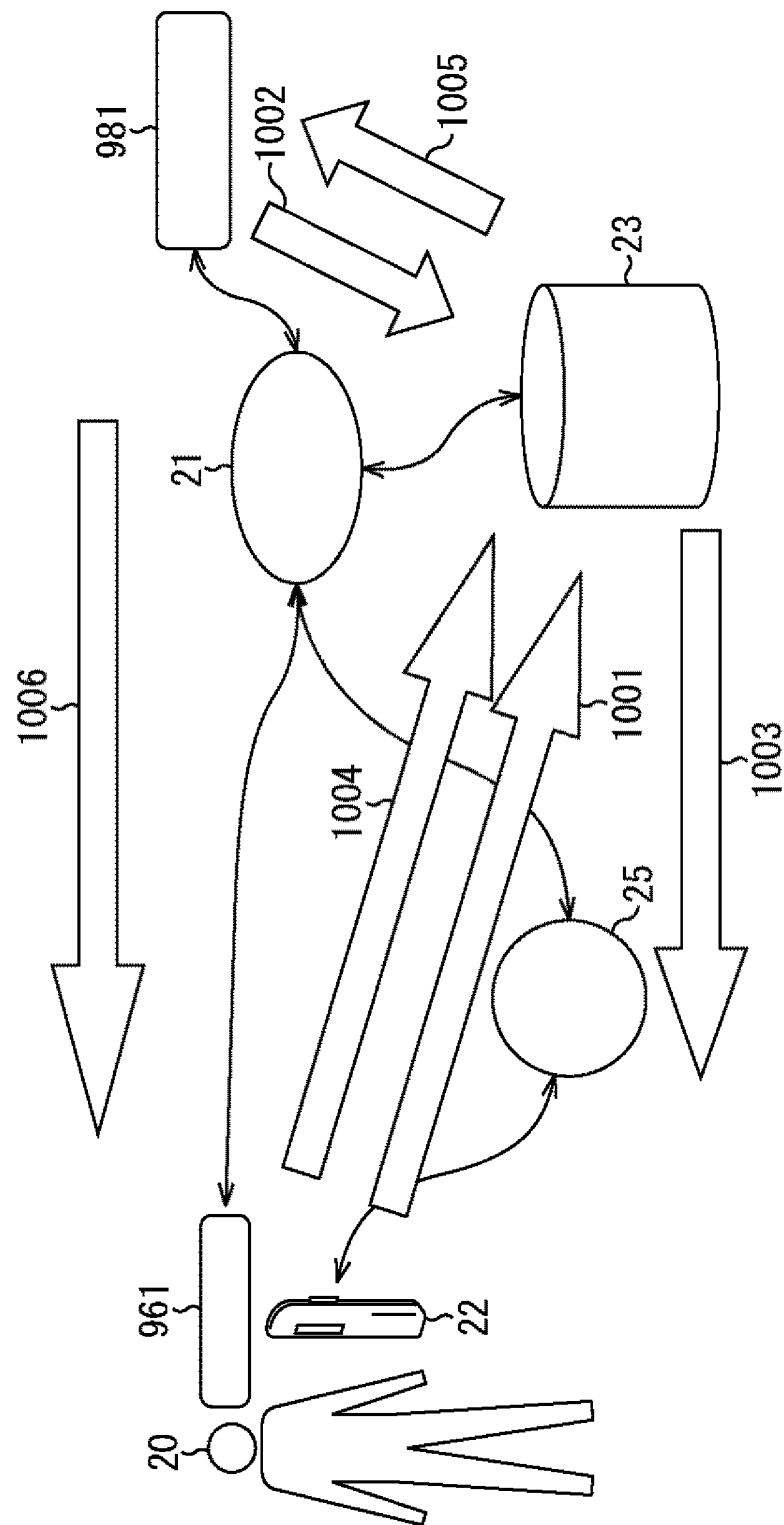


図59

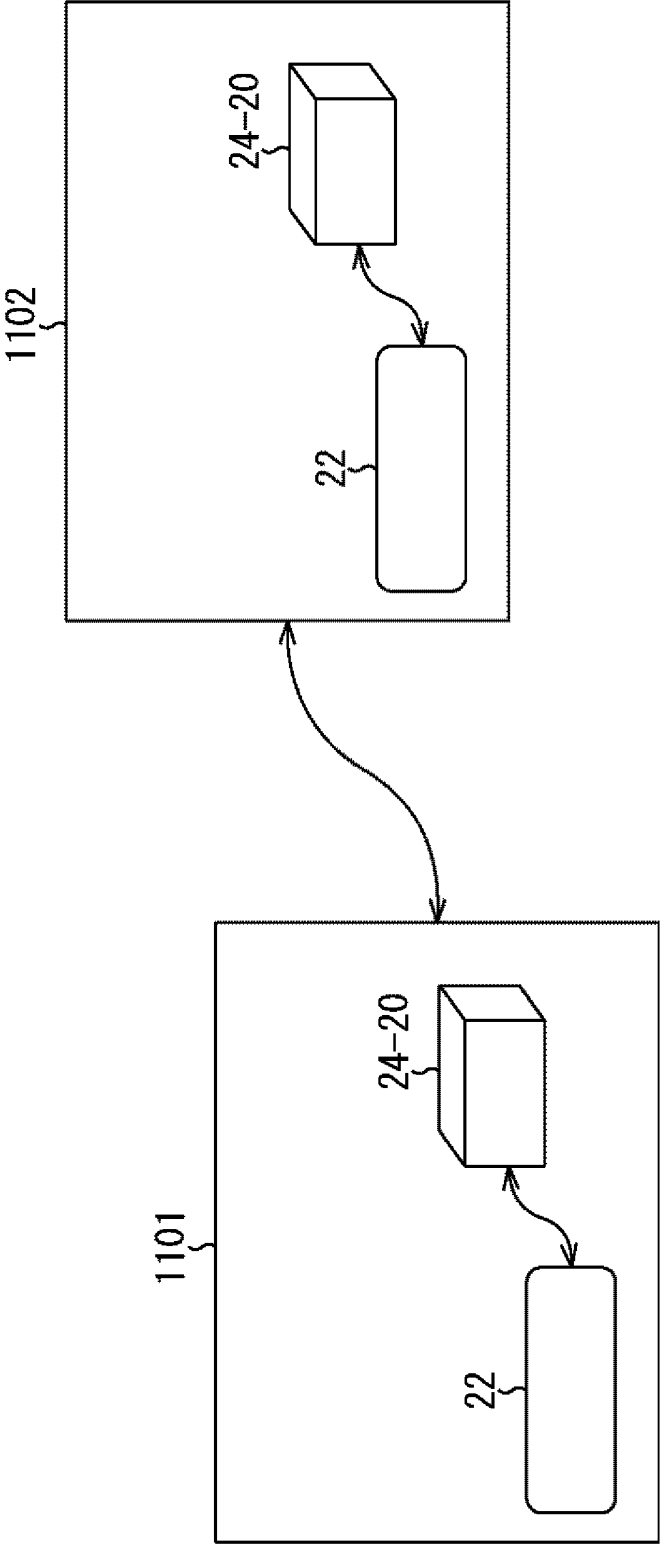
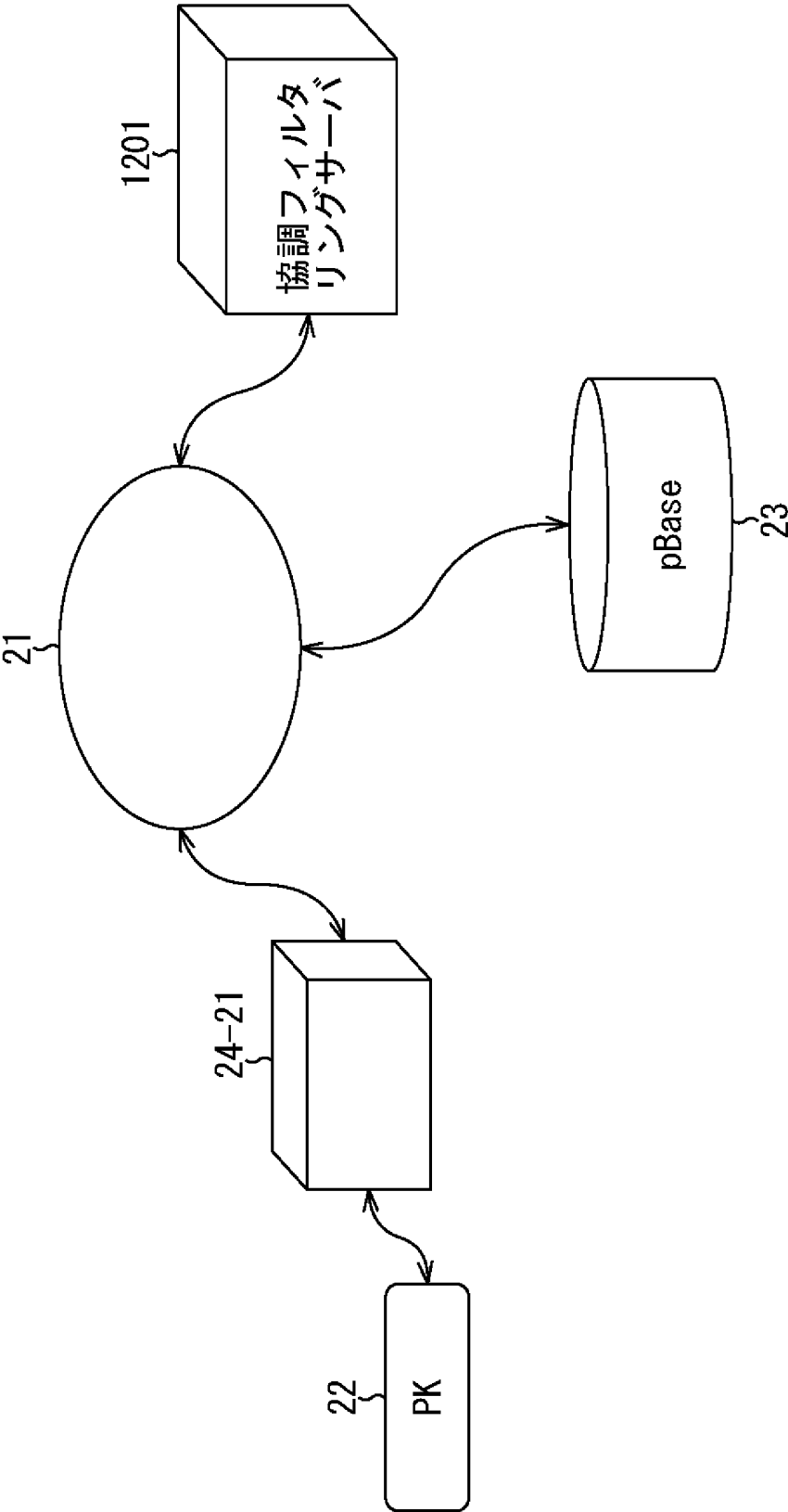


図60



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/011160

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl⁷ G06F15/00

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)

Int.Cl⁷ G06F15/00, 12/14, G06K17/00, H04L9/32

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	1996-2004
Kokai Jitsuyo Shinan Koho	1971-2004	Toroku Jitsuyo Shinan Koho	1994-2004

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	TAKAKURA et al., "IC Card Service no Tameno Kojin Joho Kanri System no Kento", Joho Shori Gakkai Kenkyu Hokoku, Information Processing Society of Japan, 14 September, 2001 (14.09.01), Vol.2001, No.88 (2001-DPS-104), pages 25 to 30	1-8, 10-14
Y	Same as the above	9
A	Same as the above	15-26



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

21 October, 2004 (21.10.04)

Date of mailing of the international search report

09 November, 2004 (09.11.04)

Name and mailing address of the ISA/

Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/011160

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 2001-216045 A (NEC Corp.), 10 August, 2001 (10.08.01), Par. No. [0008] & AU 1827301 A & CA 2333864 A1 & US 2001025342 A1	9
X	JP 2003-16393 A (NTT Data Corp.), 17 January, 2003 (17.01.03), Full text; Figs. 1 to 10 (Family: none)	15, 24-26
Y	JP 2002-320246 A (Matsushita Electric Industrial Co., Ltd.), 31 October, 2002 (31.10.02), Full text; Figs. 1 to 26 & EP 1225766 A2 & US 2002-107855 A1 & CN 1371190 A	1-14
A	JP 2001-357242 A (NEC Corp.), 26 December, 2001 (26.12.01), Full text; Figs. 1 to 10 (Family: none)	1-26
A	JP 2003-85493 A (Nippon Telegraph And Telephone Corp.), 20 March, 2003 (20.03.03), Full text; Figs. 1 to 9 (Family: none)	1-26
A	JP 2002-342362 A (Omron Corp.), 29 November, 2002 (29.11.02), Full text; Figs. 1 to 20 (Family: none)	1-26

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/011160

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

(See extra sheet.)

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

- ☐ The additional search fees were accompanied by the applicant's protest.
- ☒ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/011160

Continuation of Box No.III of continuation of first sheet(2)

The matter common to the inventions of claims 1-26 relate to that the information processing device containing user information communicates with another information processing device and reads out or modifies the user information. However, the search has revealed that this common matter is not novel since it is disclosed in:

Document 1: JP 2001-14321 A (Sony Corporation), 19 January, 2001 (19.01.01), all the pages, all the figures, and

Document 2: JP 2002-269479 A (Sony Corporation), 20 September, 2002 (20.09.02), all the pages, all the figures.

As a result, the aforementioned common matter makes no contribution over the prior art and cannot be a special technical feature within the meaning of PCT Rule 13.2, second sentence.

Accordingly, there exists no matter common to all the inventions of claims 1-26.

The inventions of claims 1-14 relate to an information processing device including means for presenting user information, means for specifying permission of read-out or modification of the presented user information by another information processing device, means for identifying the another information processing device, and storage means for correlating the identified another information processing device with the user information to be read out or modified and storing them. The inventions of claims 15-26 relate to an information processing device including communication means for communicating with a mobile terminal, means for acquiring user information stored in the mobile terminal, update means for updating the user information by the acquired user information, and generation means for generating data for updating the user information to be stored in the mobile terminal. Between the inventions of claims 1-14 and the inventions of claims 15-26, there exists no other common feature which can be considered as a special technical feature within the meaning of PCT Rule 13.2, second sentence and accordingly, no technical relationship within the meaning of PCT Rule 13 can be seen between the inventions of claims 1-14 and the inventions of claims 15-26.

Consequently, it is obvious that the inventions of claims 1-14 and the inventions of claims 15-26 do not satisfy the requirement of unity of invention.

第II欄 請求の範囲の一部の調査ができないときの意見（第1ページの2の続き）

法第8条第3項（PCT17条(2)(a)）の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1. ☐ 請求の範囲 _____ は、この国際調査機関が調査をすることを要しない対象に係るものである。つまり、
2. ☐ 請求の範囲 _____ は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、
3. ☐ 請求の範囲 _____ は、従属請求の範囲であってPCT規則6.4(a)の第2文及び第3文の規定に従って記載されていない。

第III欄 発明の単一性が欠如しているときの意見（第1ページの3の続き）

次に述べるようにこの国際出願に二以上の発明があるところの国際調査機関は認めた。

（特別ページ）参照。

1. ☒ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。
2. ☐ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。
3. ☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったので、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。
4. ☐ 出願人が必要な追加調査手数料を期間内に納付しなかったので、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

追加調査手数料の異議の申立てに関する注意

- ☐ 追加調査手数料の納付と共に出願人から異議申立てがあった。
- ☒ 追加調査手数料の納付と共に出願人から異議申立てがなかった。

(第Ⅲ欄の続き)

請求の範囲1-26に係る発明の共通の事項は、ユーザ情報を記憶した情報処理装置が、他の情報処理装置と通信を行い、ユーザ情報を読み出したり変更したりすることであるが、調査の結果、当該共通事項は、

文献1: JP 2001-14324 A (ソニー株式会社)、
2001.01.19、全頁、全図、及び、

文献2: JP 2002-269479 A (ソニー株式会社)、
2002.09.20、全頁、全図

に記載されているから、新規でないことが明らかとなった。

結果として、前記共通事項は、先行技術の域を出ないから、PCT規則13.2の第2文の意味において、特別な技術的特徴ではない。

したがって、請求の範囲1-26に係る発明全てに共通の事項はない。

そして、請求の範囲1-14に係る発明は、情報処理装置が、ユーザ情報を提示する手段と、提示されたユーザ情報の他の情報処理装置による読み出し又は変更の許可を指定する手段と、他の情報処理装置を特定する手段と、特定された他の情報処理装置と読み出し又は変更が行われるユーザ情報とを関連付けて記憶する記憶手段とを備えていることを特徴としているのに対し、請求の範囲15-26に係る発明は、情報処理装置が、携帯端末と通信する通信手段と、携帯端末に記憶されたユーザ情報を取得する手段と、取得したユーザ情報により自身のユーザ情報を更新する更新手段と、携帯端末に記憶されるユーザ情報を更新するデータを作成する作成手段を備えていることを特徴としているから、請求の範囲1-14に係る発明と請求の範囲15-26に係る発明との間には、PCT規則13.2の第2文の意味において特別な技術的特徴と考えられる他の共通の事項は存在しないので、請求の範囲1-14に係る発明と請求の範囲15-26に係る発明との間にPCT規則13の意味における技術的な関連を見いだすことはできない。

よって、請求の範囲1-14に係る発明と請求の範囲15-26に係る発明とは、発明の単一性の要件を満たしていないことが明らかである。

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl⁷ G06F15/00

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 (IPC))

Int. Cl⁷ G06F15/00、12/14、G06K17/00、H04L9/32

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1922-1996年

日本国公開実用新案公報 1971-2004年

日本国実用新案登録公報 1996-2004年

日本国登録実用新案公報 1994-2004年

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

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	高倉、外3名著、 ”ICカードサービスのための個人情報管理システムの検討”、 情報処理学会研究報告、(社)情報処理学会、2001.09.14、 第2001巻、第88号 (2001-DPS-104)、第25-30頁	1-8, 10-14
Y	同上	9
A	同上	15-26

☒ 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

21.10.2004

国際調査報告の発送日

09.11.2004

国際調査機関の名称及びあて先

日本国特許庁 (ISA/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)

林 毅

5B

9193

電話番号 03-3581-1101 内線 3546

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	J P 2001-216045 A (日本電気株式会社) 2001.08.10、段落【0008】 & AU 1827301 A & CA 2333864 A1 & US2001025342 A1	9
X	J P 2003-16393 A (株式会社エヌ・ティ・ティ・データ) 2003.01.17、全文、第1-10図 (ファミリーなし)	15、24-26
Y	J P 2002-320246 A (松下電器産業株式会社) 2002.10.31、全文、第1-26図 & EP 1225766 A2 & US 2002-107855 A1 & CN 1371190 A	1-14
A	J P 2001-357242 A (日本電気株式会社) 2001.12.26、全文、第1-10図 (ファミリーなし))	1-26
A	J P 2003-85493 A (日本電信電話株式会社) 2003.03.20、全文、第1-9図 (ファミリーなし)	1-26
A	J P 2002-342362 A (オムロン株式会社) 2002.11.29、全文、第1-20図 (ファミリーなし)	1-26