

(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2012 年 9 月 7 日(07.09.2012)



(10) 国際公開番号

WO 2012/117536 A1

- (51) 国際特許分類:
G06F 21/24 (2006.01) **G06F 12/00** (2006.01)
- (21) 国際出願番号: PCT/JP2011/054751
- (22) 国際出願日: 2011 年 3 月 2 日(02.03.2011)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (71) 出願人 (米国を除く全ての指定国について): 富士通株式会社(FUJITSU LIMITED) [JP/JP]; 〒2118588 神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号 Kanagawa (JP).
- (72) 発明者; および
- (75) 発明者/出願人 (米国についてのみ): 柴田 義則 (SHIBATA, Yoshinori) [JP/JP]; 〒2118588 神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号 富士通株式会社内 Kanagawa (JP). 高野 清 (TAKANO, Kiyoshi) [JP/JP]; 〒2118588 神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号 富士通株式会社内 Kanagawa (JP). 鈴木 誠 (SUZUKI, Makoto) [JP/JP]; 〒2118588 神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号 富士通株式会社内 Kanagawa (JP).
- (74) 代理人: 服部 毅巖 (HATTORI, Kiyoshi); 〒1920082 東京都八王子市東町 9 番 8 号 八王子東町センタービル 服部特許事務所 Tokyo (JP).

- (81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.
- (84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, 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 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

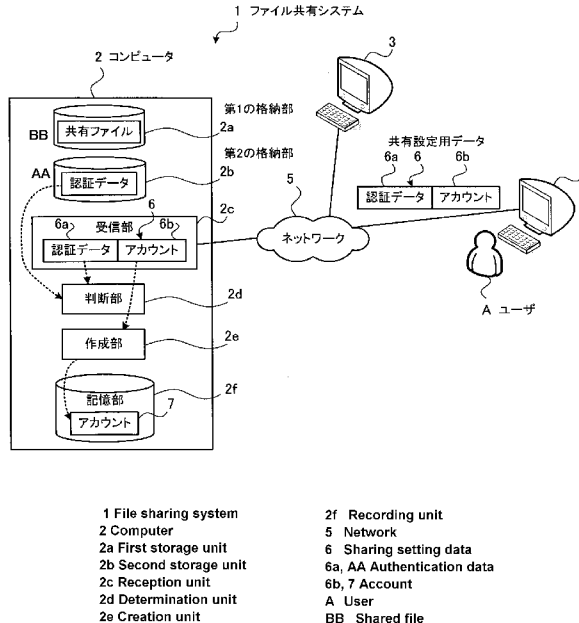
添付公開書類:

— 国際調査報告 (条約第 21 条(3))

(54) Title: FILE SHARING DEVICE, FILE SHARING METHOD, AND PROGRAM

(54) 発明の名称: ファイル共有装置、ファイル共有方法およびプログラム

【図1】



(57) Abstract: The present invention enables the sharing of files using information held in terminal devices. A first storage unit (2a) stores shared files. A second storage unit (2b) stores authentication data that authenticates a specific user. A reception unit (2c) receives sharing setting data (6) via a network (5). A determination unit (2d) determines whether or not authentication data (6a) contained in the sharing setting data (6) matches the authentication data stored in the second storage unit (2b). When it has been determined by the determination unit (2d) that there is a match, on the basis of an account (6b) contained in the sharing setting data (6), a creation unit (2e) creates an account (7) that permits access to the files that are shared with a user (A) requesting access to the shared files. A recording unit (2f) records the account (7) created by the creation unit (2e).

(57) 要約: 各端末装置内で保持する情報を用いてファイルの共有を可能とすること。第1の格納部(2a)は、共有ファイルを格納する。第2の格納部(2b)は、特定のユーザを認証する認証データを格納する。受信部(2c)は、ネットワーク(5)を介して共有設定用データ(6)を受信する。判断部(2d)は、共有設定用データ(6)に含まれる認証データ(6a)が、第2の格納部(2b)に格納されている認証データに一致するか否かを判断する。作成部(2e)は、判

断部(2d)により一致すると判断された場合に共有設定用データ(6)に含まれるアカウント(6b)に基づいて共有ファイルへのアクセスを要求するユーザAの共有対象のファイルへのアクセスを許可するアカウント(7)を作成する。記憶部(2f)は、作成部(2e)が作成したアカウント(7)を記憶する。

WO 2012/117536 A1

明 細 書

発明の名称：

ファイル共有装置、ファイル共有方法およびプログラム

技術分野

[0001] 本発明はファイル共有装置、ファイル共有方法およびプログラムに関する。

背景技術

[0002] 情報処理システムにおいて、例えばネットワークで接続され共有されているリモートコンピュータのファイルを、複数のローカルコンピュータから使用する場合にユーザの認証を行い、アクセスを許可する方法が知られている。この方法を実現する一例として、個人特定用のコンピュータを設け、そのコンピュータに問い合わせを行うことにより、パスワードを取得し、リモートコンピュータにアクセスする方法が知られている。

先行技術文献

特許文献

[0003] 特許文献1：特開2001-14276号公報

発明の概要

発明が解決しようとする課題

[0004] しかしながら、家庭内でファイルの共有を使用するには、サーバはコストや場所の面から一般的ではない。

また、パスワードを自動生成している場合やパスワードを忘れてしまった場合、ネットワーク上でファイル共有することができなかった。このため、ファイルの共有をするために、例えばパスワードの自動生成をやめて、ユーザ自身によるパスワードの作成、管理による運用を行っていた。

[0005] 本発明はこのような点に鑑みてなされたものであり、各端末装置内で保持する情報を用いてファイルの共有を可能とするファイル共有装置、ファイル共有方法およびプログラムを提供することを目的とする。

課題を解決するための手段

- [0006] 上記目的を達成するために、開示のファイル共有装置が提供される。このファイル共有装置は、第1の格納部と、第2の格納部と、受信部と、判断部と、作成部と、記憶部とを有している。
- [0007] 第1の格納部は、共有対象のファイルを格納する。第2の格納部は、特定のユーザを認証する認証データを格納する。受信部は、共有対象のファイルへのアクセスを要求するユーザのアカウントおよび認証データを含む共有設定用データを受信する。判断部は、共有設定用データに含まれる認証データが、第2の格納部に格納されている認証データに一致するか否かを判断する。作成部は、一致する場合に共有設定用データに含まれるアカウントに基づいて共有対象のファイルへのアクセスを要求するユーザの共有対象のファイルへのアクセスを許可するアカウントを作成する。記憶部は、作成されたアカウントを記憶する。

発明の効果

- [0008] システム構成の簡易化を図ることができる。
- 本発明の上記および他の目的、特徴および利点は本発明の例として好ましい実施の形態を表す添付の図面と関連した以下の説明により明らかになるであろう。

図面の簡単な説明

- [0009] [図1] 第1の実施の形態のファイル共有システムを示す図である。
- [図2] 第2の実施の形態のファイル共有システムの構成を示す図である。
- [図3] 共有ファイルの閲覧を許可していないときの端末装置の処理を説明する図である。
- [図4] 共有ファイルの閲覧を許可しているときの端末装置の処理を説明する図である。
- [図5] 第2の実施の形態の端末装置のハードウェアの一構成例を示す図である。
- [図6] 第2の実施の形態の端末装置の機能を示すブロック図である。

[図7] ユーザ管理テーブルを示す図である。

[図8] 共有設定用データのデータ構成を示す図である。

[図9] 端末装置の共有設定用データの送信処理を示すフローチャートである。

[図10] 端末装置のデータ受信処理を示すフローチャートである。

発明を実施するための形態

[0010] 以下、実施の形態のファイル共有システムを、図面を参照して詳細に説明する。

まず、実施の形態のファイル共有システムについて説明し、その後、実施の形態をより具体的に説明する。

[0011] <第1の実施の形態>

図1は、第1の実施の形態のファイル共有システムを示す図である。

第1の実施の形態のファイル共有システム1は、複数のコンピュータ2、3、4を有している。コンピュータ2、3、4は、ネットワーク5により互いに接続されている。

[0012] コンピュータ2は、ファイル共有装置の一例であり、第1の格納部2aと、第2の格納部2bと、受信部2cと、判断部2dと、作成部2eと、記憶部2fとを有している。

第1の格納部2aは、共有対象のファイル（共有ファイル）を格納する。

[0013] 第2の格納部2bは、特定のユーザを認証する認証データを格納する。本実施の形態ではユーザAを認証する認証データが格納されているものとする。認証データとしては、例えばユーザAの指紋データ等、各種生体認証データ等が挙げられる。

[0014] コンピュータ4は、第1の格納部2aに格納されている共有ファイルへのアクセスを要求する共有設定用データ6を作成する。この共有設定用データには、共有ファイルへのアクセスを要求するユーザAのアカウント6bおよびユーザAを認証する認証データ6aが含まれている。ユーザAのアカウント6bは、ユーザAのユーザ名とパスワードを含む。コンピュータ4は、作成した共有設定用データ6を例えばブロードキャストにより配信する。

[0015] 受信部 2 c は、ネットワーク 5 を介して共有設定用データ 6 を受信する。

判断部 2 d は、共有設定用データ 6 に含まれる認証データ 6 a が、第 2 の格納部 2 b に格納されている認証データに一致するか否かを判断する。本実施の形態では第 2 の格納部 2 b にはユーザ A を認証する認証データが格納されているため、判断部 2 d は、一致すると判断する。

[0016] 作成部 2 e は、判断部 2 d により一致すると判断された場合に共有設定用データ 6 に含まれるアカウント 6 b に基づいて共有ファイルへのアクセスを要求するユーザ A の共有対象のファイルへのアクセスを許可するアカウント 7 を作成する。

[0017] 記憶部 2 f は、作成部 2 e が作成したアカウント 7 を記憶する。

なお、コンピュータ 3、4 がコンピュータ 2 と同様の機能を有していてもよい。

次に、ファイル共有システム 1 のファイル共有処理の一例を説明する。

[0018] まず、ユーザ A が、コンピュータ 2 を操作して第 2 の格納部 2 b に認証データを格納する。例えば、ユーザ A が図示しない指紋入力装置に指紋の入力を行うことでコンピュータ 2 がユーザ A の認証データを作成する。そして、コンピュータ 2 は、作成した認証データを第 2 の格納部 2 b に格納する。

[0019] その後、ユーザ A は、コンピュータ 4 を操作して共有設定用データ 6 を作成する。そしてコンピュータ 4 は、作成した共有設定用データ 6 を、ネットワーク 5 に接続されたコンピュータ 2、3 にブロードキャスト送信する。

[0020] コンピュータ 3 は、共有設定用データ 6 を受信すると、共有設定用データ 6 に含まれている認証データ 6 a に一致する認証データを有しているか否かを判断する。一致する認証データを有していない場合、受信した共有設定用データ 6 を破棄する。この状態でコンピュータ 4 からコンピュータ 3 の共有フォルダへアクセスすると、ユーザ名、パスワードの入力を求められる。

[0021] コンピュータ 2 の受信部 2 c が共有設定用データ 6 を受信すると、判断部 2 d は、共有設定用データ 6 に含まれている認証データ 6 a がユーザ A の指紋であるか否かを判断する。認証データが一致するので、作成部 2 e は、共

有設定用データ 6 に含まれるアカウント 6 b に基づいてユーザ A のアカウント 7 を作成する。そして、作成部 2 e は、作成したユーザ A のアカウント 7 を記憶部 2 f に記憶する。

[0022] この状態でユーザ A がコンピュータ 4 を操作してコンピュータ 2 にアクセスすると、共有ファイルの参照ができる。すなわち、コンピュータ 2 は、記憶部 2 f に記憶されているアカウント 7 に対応するアカウントでログオンされているコンピュータ 4 からの共有ファイルへのアクセス要求である場合、共有ファイルへのアクセスを許可する。

[0023] このファイル共有システム 1 によれば、コンピュータ 4 とコンピュータ 2 との間で共有ファイルへのアクセスの許否を判断するので、ユーザを特定する認証サーバ等の別個の機器を使用せずにデータを共有することができる。

[0024] なお、受信部 2 c、判断部 2 d および作成部 2 e は、コンピュータ 2 が有する CPU (Central Processing Unit) が備える機能により実現することができる。また、第 1 の格納部 2 a、第 2 の格納部 2 b および記憶部 2 f は、コンピュータ 2 が有する RAM (Random Access Memory) やハードディスクドライブ (HDD: Hard Disk Drive) 等が備えるデータ記憶領域により実現することができる。

[0025] 以下、実施の形態をより具体的に説明する。

<第 2 の実施の形態>

図 2 は、第 2 の実施の形態のファイル共有システムの構成を示す図である。

[0026] 第 2 の実施の形態のファイル共有システム 100 は、端末装置 10 a、10 b、10 c、10 d を有している。

端末装置 10 a ~ 10 d は、LAN (Local Area Network) 等のネットワーク 50 により互いに接続されている。

[0027] 端末装置 10 a ~ 10 d にはそれぞれ認証アプリケーション (後述) がインストールされている。例えば端末装置 10 a が備える認証アプリケーションは、端末装置 10 a の OS (Operating System) へのログオンを認証によ

り行う。

[0028] 端末装置 10a～10dには、それぞれ認証デバイス20a～20dが接続されている。

認証デバイス20aは、指紋センサを有している。ユーザが端末装置10aへのログオンを希望する場合、指紋センサ上に指を置く。認証デバイス20aは、指紋センサに置かれた指の指紋を読み取り、読み取った指紋の情報（指紋情報）を端末装置10aに送る。端末装置10aは、送られてきた指紋情報を受け取ると、端末装置10a内に保持されている認証用のデータ（認証データ）と照合する。受け取った指紋情報が端末装置10a内に保持されている認証データに一致すると、端末装置10aは、認証データに関連づけられたユーザ名、パスワードに自動的に変換してログオン処理を実行する。この処理により、認証デバイス20aの指紋センサに指を置いたユーザが、端末装置10aにログオンした状態となる。

[0029] なお、指紋認証は認証の一例であり、静脈認証等の他の生体認証や、非接触型ICカードによる認証等、他の認証方法を用いることもできる。

端末装置10a～10dのうち、1つまたは複数の端末装置は、他の端末装置から閲覧や更新等が可能な共有データを格納するフォルダ（以下、共有フォルダと言う）を有している。この共有フォルダには暗号化処理が施されている。以下、端末装置10aが共有フォルダを有するものとして説明する。

[0030] 共有フォルダを有する端末装置10aは、この端末装置10aが予め記憶しておいたアカウント（ユーザー名、パスワード）に一致するアカウントを有するアクセス要求を受け取ることにより、共有フォルダ内のデータの第三者への閲覧や更新等を許可する。

[0031] このアカウントは、指紋を登録する際に端末装置10aが新しいパスワードを生成し、端末装置10a内に記憶する。このため、ユーザは、共有フォルダ内のデータを閲覧や更新するパスワードを知らなくても共有ファイルにアクセスすることができる。

[0032] なお、コンピュータとしては、図に示す設置型のコンピュータに限らず、携帯できるコンピュータであってもよい。

以下、ファイル共有システム 100 のフォルダの共有設定動作を簡単に説明する。以下、端末装置 10b からアクセスを行って端末装置 10a に格納されている共有ファイルを閲覧するものとする。

[0033] また、前提条件として、共有ファイルの閲覧を希望するユーザ A のアカウントが端末装置 10a に予め設定されているものとする。

ユーザ A は、認証デバイス 20b に指紋を入力する。端末装置 10b は、入力された指紋情報に基づいて認証データを作成する。そして、端末装置 10b は、作成した認証データと端末装置 10b の OS のアカウントとを暗号化したデータとを含む共有設定用データを作成する。そして、端末装置 10b は、作成した共有設定用データをブロードキャストでネットワーク 50 に属する端末装置 10a、10c、10d に一斉送信する。

[0034] ブロードキャストした共有設定用データを受信した端末装置 10a、10c、10d は、共有設定用データに含まれている認証データが、それぞれ自端末装置の管理者権限を有するユーザの認証データと一致するか否かを照合する。

[0035] 端末装置 10a、10c、10d は、認証データが一致しない場合は共有ファイルの閲覧を許可しない。

端末装置 10a、10c、10d は、認証データが一致した場合は、ブロードキャストにより送信された情報に含まれている端末装置 10b の OS のアカウントに基づいてユーザ A のアカウントを自端末装置に作成し、記憶する。

[0036] 図 3 は、共有ファイルの閲覧を許可していないときの端末装置の処理を説明する図である。

端末装置 10b を操作するユーザ A は、端末装置 10b に接続されたモニタ 104b を見ながら端末装置 10b に接続されたマウス等を操作して、端末装置 10a の共有フォルダ 31 へのアクセスを要求する。なお、共有フォ

ルダ 31 は、第 1 の格納部の一例である。端末装置 10b は、端末装置 10a の共有フォルダ 31 へのアクセス要求を端末装置 10a に送信する。

[0037] 端末装置 10a がユーザ A への共有ファイルの閲覧を許可していない場合、端末装置 10b は、ユーザ名とパスワードの入力を要求する画面 32 をモニタ 104b に表示する。この場合、ユーザ A は、ファイル共有用のユーザ名とパスワードを入力し、端末装置 10a に認証されれば共有ファイルへのアクセスが可能となる。

[0038] 図 4 は、共有ファイルの閲覧を許可しているときの端末装置の処理を説明する図である。

他方、端末装置 10a がユーザ A への共有ファイルの閲覧を許可している場合、端末装置 10a の OS が、共有フォルダ 31 へのアクセスを許可するユーザ A からのアクセスであることを認識する。このため、端末装置 10a は、パスワードの入力を要求することなく共有フォルダ 31 へのアクセスを許可する。その結果、端末装置 10b は、共有フォルダ 31 の内容を示す画面 33 をモニタ 104b に表示する。

[0039] なお、共有フォルダ 31 の共有を解除する際には、端末装置 10a の OS の機能で共有を解除することができる。

以下、端末装置 10a ~ 10d が有する構成や機能について詳しく説明する。

[0040] 図 5 は、第 2 の実施の形態の端末装置のハードウェアの一構成例を示す図である。端末装置 10a は、CPU 101 によって装置全体が制御されている。CPU 101 には、バス 108 を介して RAM 102 と複数の周辺機器が接続されている。

[0041] RAM 102 は、端末装置 10a の主記憶装置として使用される。RAM 102 には、CPU 101 に実行させる OS のプログラムやアプリケーションプログラムの少なくとも一部が一時的に格納される。また、RAM 102 には、CPU 101 による処理に使用する各種データが格納される。

[0042] バス 108 に接続されている周辺機器としては、ハードディスクドライブ

１０３、グラフィック処理装置１０４、入力インタフェース１０５、ドライブ装置１０６、および通信インタフェース１０７がある。

- [0043] ハードディスクドライブ１０３は、内蔵したディスクに対して、磁氣的にデータの書き込みおよび読み出しを行う。ハードディスクドライブ１０３は、端末装置１０ａの二次記憶装置として使用される。ハードディスクドライブ１０３には、ＯＳのプログラム、アプリケーションプログラム、および各種データが格納される。なお、二次記憶装置としては、フラッシュメモリ等の半導体記憶装置を使用することもできる。
- [0044] グラフィック処理装置１０４には、モニタ１０４ａが接続されている。グラフィック処理装置１０４は、ＣＰＵ１０１からの命令に従って、画像をモニタ１０４ａの画面に表示させる。モニタ１０４ａとしては、ＣＲＴ（Cathode Ray Tube）を用いた液晶表示装置等が挙げられる。
- [0045] 入力インタフェース１０５には、キーボード１０５ａとマウス１０５ｂと認証デバイス２０ａが接続されている。入力インタフェース１０５は、キーボード１０５ａ、マウス１０５ｂおよび認証デバイス２０ａから送られてくる信号をＣＰＵ１０１に送信する。なお、マウス１０５ｂは、ポインティングデバイスの一例であり、他のポインティングデバイスを使用することもできる。他のポインティングデバイスとしては、タッチパネル、タブレット、タッチパッド、トラックボール等が挙げられる。
- [0046] ドライブ装置１０６は、例えば、光の反射によって読み取り可能なようにデータが記録された光ディスクや、ＵＳＢ（Universal Serial Bus）メモリ等の持ち運び可能な記録媒体に記録されたデータの読み取りを行う。例えば、ドライブ装置１０６が光学ドライブ装置である場合、レーザ光等を利用して、光ディスク２００に記録されたデータの読み取りを行う。光ディスク２００には、Ｂｌｕ－ｒａｙ（登録商標）、ＤＶＤ（Digital Versatile Disc）、ＤＶＤ－ＲＡＭ、ＣＤ－ＲＯＭ（Compact Disc Read Only Memory）、ＣＤ－Ｒ（Recordable）／ＲＷ（ReWritable）等が挙げられる。
- [0047] 通信インタフェース１０７は、ネットワーク５０に接続されている。通信

インタフェース 107 は、ネットワーク 50 を介して、他の端末装置 10b、10c、10d や通信機器との間でデータの送受信を行う。

[0048] 以上のようなハードウェア構成によって、本実施の形態の処理機能を実現することができる。なお、図 5 には端末装置 10a のハードウェア構成を示したが、端末装置 10b、10c、10d も端末装置 10a と同様のハードウェア構成である。

[0049] このようなハードウェア構成の端末装置 10a 内には、以下のような機能が設けられる。

図 6 は、第 2 の実施の形態の端末装置の機能を示すブロック図である。

[0050] 端末装置 10a は、認証アプリケーションを実行する認証アプリケーション実行部 11 を有している。認証アプリケーション実行部 11 は、ユーザが端末装置 10a を操作し共有アプリケーションを起動することにより動作する。認証アプリケーション実行部 11 が起動すると、端末装置 10a を操作するユーザに対し、認証デバイス 20a への指紋の入力を促す画面をモニタ 104a に表示する。例えば「共有ファイルのあるパソコンの管理者の指紋を入力して下さい」等の文字をモニタ 104a に表示する。

[0051] この認証アプリケーション実行部 11 は、認証処理部 111 と、アカウント管理部 112 と、認証データ抽出部 113 と、アカウント抽出部 114 と、共有設定部 115 と、暗号化／復号部 116 と、データ送受信部 117 とを有している。

[0052] 認証処理部 111 は、認証デバイス 20a を介して入力された指紋情報や、共有設定用データに含まれる認証データに基づいてユーザの認証を行う。

アカウント管理部 112 は、ユーザに関する情報を管理するユーザ管理テーブル（後述）を有している。なお、ユーザ管理テーブルは、第 2 の格納部の一例である。アカウント管理部 112 は、ユーザ管理テーブルを更新する。

[0053] 認証データ抽出部 113 は、受信した共有設定用データから認証データを抽出する。

アカウント抽出部 114 は、受信した共有設定用データからアカウントを抽出する。

共有設定部 115 は、他の端末装置 10b、10c、10d 内の共有フォルダへのアクセスの許可を依頼する共有設定用データを作成する。そして、共有設定部 115 は、作成した共有データをデータ送受信部 117 に送る。なお、共有設定部 115 は、判断部および作成部の一例である。

[0054] 暗号化／復号部 116 は、共有設定用データに含まれる認証データ、ユーザ名、パスワードを暗号化または復号する。

データ送受信部 117 は、共有設定用データを送受信する。

[0055] 図 7 は、ユーザ管理テーブルを示す図である。

ユーザ管理テーブル 112a には、ID、認証データ、ユーザ名、パスワードの欄が設けられている。横方向に並べられた情報同士が互いに関連づけられている。

[0056] ID の欄には、ユーザ管理テーブル 112a 内の情報を管理する ID が設定されている。

認証データの欄には、ユーザの指紋情報が設定されている。ユーザ名の欄には、ユーザ名を識別する情報が設定されている。パスワードの欄には、ユーザ名毎の個別のパスワードが設定されている。

[0057] 次に、共有設定用データのデータ構成を説明する。

図 8 は、共有設定用データのデータ構成を示す図である。

図 8 に示す共有設定用データ D1 は、イーサネット（Ethernet：登録商標）フレームヘッダ D11、IP（Internet Protocol）フレームヘッダ D12、UDP（User Datagram Protocol）フレームヘッダ D13、UDP データ部 D14 および FCS（Frame Check Sequence）D15 を有している。このうち、UDP データ部 D14 は、暗号化／復号部 116 により、暗号化処理が施されている部分である。この UDP データ部 D14 は、認証データ D141、ユーザ名 142 およびパスワード 143 を有している。

[0058] 認証データ D141 は、ユーザを認証する認証データが設定されている。

ユーザ名 D 1 4 2 には、ユーザ名を識別する情報が設定されている。パスワード D 1 4 3 には、ユーザ名 D 1 4 2 に対応するパスワードが設定されている。

[0059] 次に、端末装置 1 0 a が端末装置 1 0 b、1 0 c、1 0 d に共有設定用データを送信するときの処理を、フローチャートを用いて説明する。

図 9 は、端末装置の共有設定用データの送信処理を示すフローチャートである。

[0060] [ステップ S 1] ユーザの操作により、起動指示があると認証アプリケーション実行部 1 1 は、共有設定アプリケーションを起動する。その後、ステップ S 2 に遷移する。

[ステップ S 2] 認証処理部 1 1 1 は、ユーザの指紋入力を受け付けると指紋情報を作成する。その後、ステップ S 3 に遷移する。

[0061] [ステップ S 3] アカウント管理部 1 1 2 は、ユーザ管理テーブル 1 1 2 a を参照してステップ S 2 にて作成した指紋情報と一致する認証データが存在するか否かを判断する。そして、一致する認証データが存在する場合、一致する認証データに対応するユーザのアカウント（ユーザ名およびパスワード）を取得する。その後、ステップ S 4 に遷移する。

[0062] [ステップ S 4] 共有設定部 1 1 5 は、ステップ S 3 にて取得したアカウントを含む共有設定用データ D 1 を作成する。その後、ステップ S 5 に遷移する。

[ステップ S 5] 暗号化／復号部 1 1 6 は、共有設定用データ D 1 の U D P データ部 D 1 4 を暗号化する。その後、ステップ S 6 に遷移する。

[0063] [ステップ S 6] データ送受信部 1 1 7 は、共有設定用データ D 1 のブロードキャスト送信を行う。その後、認証アプリケーション実行部 1 1 は、図 9 の処理を終了する。

以上で図 9 のデータ送信処理の説明を終了する。

[0064] 次に、端末装置 1 0 a が端末装置 1 0 b、1 0 c、1 0 d のうちのいずれかの端末装置から共有設定用データ D 1 を受信するときの処理を、フローチ

ャートを用いて説明する。

図 10 は、端末装置のデータ受信処理を示すフローチャートである。

[0065] [ステップ S 1 1] データ送受信部 1 1 7 は、共有設定用データ D 1 を受信したか否かを判断する。共有設定用データ D 1 を受信した場合（ステップ S 1 1 の Y e s）、ステップ S 1 2 に遷移する。共有設定用データ D 1 を受信していない場合（ステップ S 1 1 の N o）、共有設定用データの受信を待機する。

[0066] [ステップ S 1 2] 暗号化／復号部 1 1 6 は、共有設定用データ D 1 の UDP データ部 D 1 4 を復号する。その後、ステップ S 1 3 に遷移する。

 [ステップ S 1 3] 認証データ抽出部 1 1 3 は、復号された認証データ D 1 4 1 を取り出す。その後、ステップ S 1 4 に遷移する。

[0067] [ステップ S 1 4] 共有設定部 1 1 5 は、ステップ S 1 3 にて取り出された認証データ D 1 4 1 をユーザ管理テーブル 1 1 2 a に格納されている認証データと照合する。その後、ステップ S 1 5 に遷移する。

[0068] [ステップ S 1 5] 共有設定部 1 1 5 は、ステップ S 1 4 の照合の結果、認証データが一致すれば（ステップ S 1 5 の Y e s）、ステップ S 1 6 に遷移する。認証データが一致しなければ（ステップ S 1 5 の N o）、データ受信処理を終了する。

[0069] [ステップ S 1 6] アカウント抽出部 1 1 4 は、共有設定用データ D 1 からアカウントを取り出す。その後、ステップ S 1 7 に遷移する。

 [ステップ S 1 7] 共有設定部 1 1 5 は、ステップ S 1 6 にて取り出されたアカウントに基づいて、ファイル共有用のアカウントを作成する。その後、データ受信処理を終了する。なお、作成したアカウントは端末装置 1 0 a の O S のファイルシステムで管理される。

[0070] 以上で、図 10 のデータ受信処理の説明を終了する。

以上述べたように、ファイル共有システム 1 0 0 によれば、個人特定のための認証サーバ等の情報機器を使用せずに、各情報機器内で保持している情報（ユーザ名、パスワード、バイオ情報等の認証データ）を使用してデータ

共有することが可能になる。認証サーバ等の情報機器を使用しない情報機器間のデータ共有は、サーバ費用(ハードコストや運用コスト、設置場所)を削減するだけでなく、シンプルな機器構成、通信シーケンスを実現することができる。

[0071] 以上、本発明のファイル共有装置、ファイル共有方法およびファイル共有プログラムを、図示の実施の形態に基づいて説明したが、本発明はこれに限定されるものではなく、各部の構成は、同様の機能を有する任意の構成のものに置換することができる。また、本発明に、他の任意の構成物や工程が付加されていてもよい。

[0072] また、本発明は、前述した各実施の形態のうちの、任意の2以上の構成(特徴)を組み合わせたものであってもよい。

なお、上記の処理機能は、コンピュータによって実現することができる。その場合、コンピュータ2および端末装置10aが有すべき機能の処理内容を記述したプログラムが提供される。そのプログラムをコンピュータで実行することにより、上記処理機能がコンピュータ上で実現される。処理内容を記述したプログラムは、コンピュータで読み取り可能な記録媒体に記録しておくことができる。コンピュータで読み取り可能な記録媒体としては、磁気記憶装置、光ディスク、光磁気記録媒体、半導体メモリ等が挙げられる。磁気記憶装置には、ハードディスクドライブ、フレキシブルディスク(FD)、磁気テープ等が挙げられる。光ディスクには、DVD、DVD-RAM、CD-ROM/RW等が挙げられる。光磁気記録媒体には、MO(Magneto-optical disk)等が挙げられる。

[0073] プログラムを流通させる場合には、例えば、そのプログラムが記録されたDVD、CD-ROM等の可搬型記録媒体が販売される。また、プログラムをサーバコンピュータの記憶装置に格納しておき、ネットワークを介して、サーバコンピュータから他のコンピュータにそのプログラムを転送することもできる。

[0074] プログラムを実行するコンピュータは、例えば、可搬型記録媒体に記録さ

れたプログラムもしくはサーバコンピュータから転送されたプログラムを、自己の記憶装置に格納する。そして、コンピュータは、自己の記憶装置からプログラムを読み取り、プログラムに従った処理を実行する。なお、コンピュータは、可搬型記録媒体から直接プログラムを読み取り、そのプログラムに従った処理を実行することもできる。また、コンピュータは、ネットワークを介して接続されたサーバコンピュータからプログラムが転送される毎に、逐次、受け取ったプログラムに従った処理を実行することもできる。

[0075] また、上記の処理機能の少なくとも一部を、DSP (Digital Signal Processor)、ASIC (Application Specific Integrated Circuit)、PLD (Programmable Logic Device) 等の電子回路で実現することもできる。

[0076] 上記については単に本発明の原理を示すものである。さらに、多数の変形、変更が当業者にとって可能であり、本発明は上記に示し、説明した正確な構成および応用例に限定されるものではなく、対応するすべての変形例および均等物は、添付の請求項およびその均等物による本発明の範囲とみなされる。

符号の説明

[0077] 1、100 ファイル共有システム

2～4 コンピュータ

2a 第1の格納部

2b 第2の格納部

2c 受信部

2d 判断部

2e 作成部

2f 記憶部

5、50 ネットワーク

6、D1 共有設定用データ

6a 認証データ

6b、7 アカウント

10 a、10 b、10 c、10 d 端末装置

11 認証アプリケーション実行部

20 a、20 b、20 c、20 d 認証デバイス

111 認証処理部

112 アカウント管理部

112 a ユーザ管理テーブル

113 認証データ抽出部

114 アカウント抽出部

115 共有設定部

116 暗号化／復号部

117 データ送受信部

請求の範囲

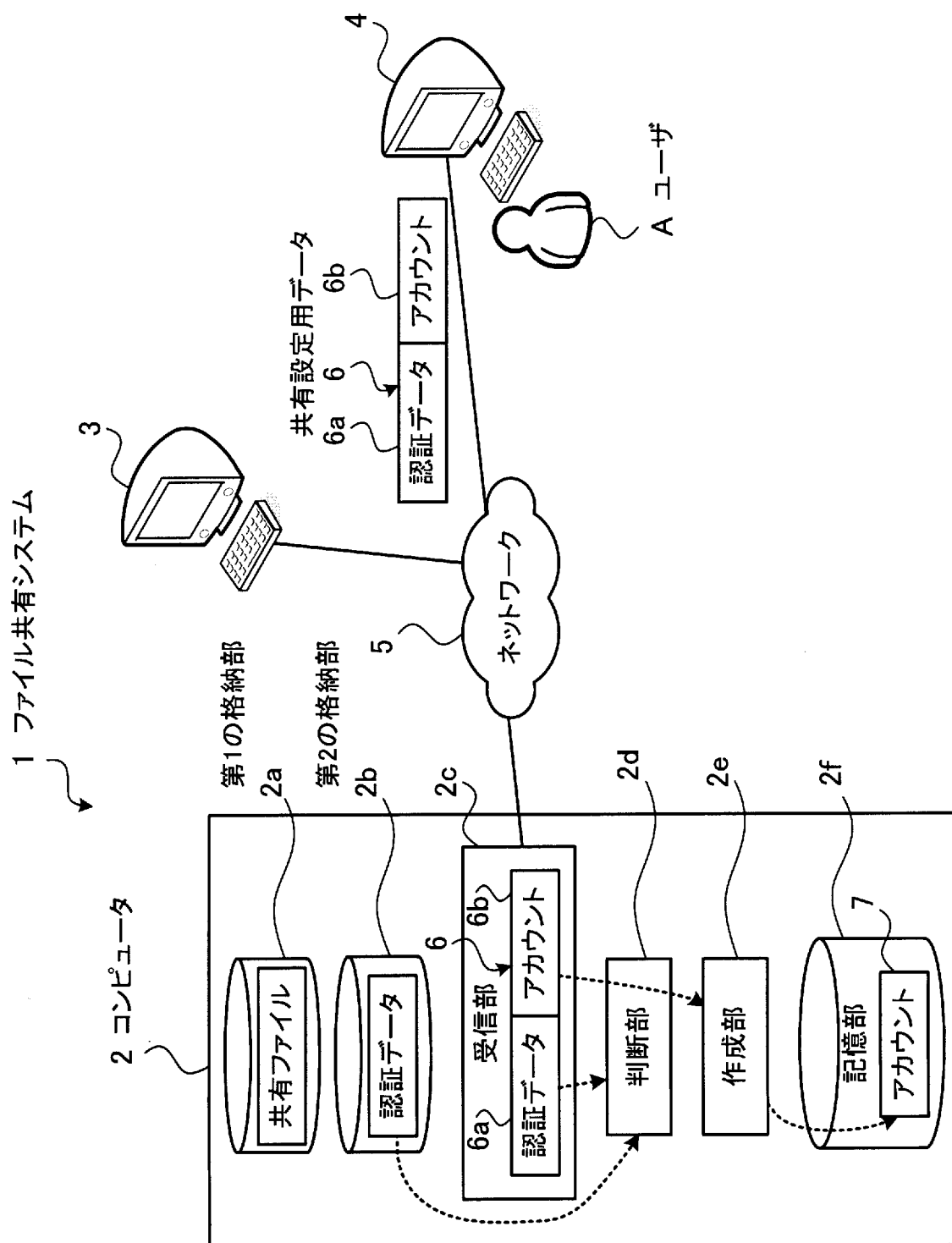
- [請求項1] 共有対象のファイルを格納する第1の格納部と、
 特定のユーザを認証する認証データを格納する第2の格納部と、
 前記共有対象のファイルへのアクセスを要求するユーザのアカウントおよび認証データを含む共有設定用データを受信する受信部と、
 前記共有設定用データに含まれる前記認証データが、前記第2の格納部に格納されている前記認証データに一致するか否かを判断する判断部と、
 一致する場合に前記共有設定用データに含まれる前記アカウントに基づいて前記共有対象のファイルへのアクセスを要求するユーザの前記共有対象のファイルへのアクセスを許可するアカウントを作成する作成部と、
 作成された前記アカウントを記憶する記憶部と、
 を有することを特徴とするファイル共有装置。
- [請求項2] 前記共有設定用データに含まれる前記アカウントはパスワードを含み、前記パスワードは、前記共有設定用データの作成時に任意に作成されることを特徴とする請求の範囲第1項記載のファイル共有装置。
- [請求項3] 前記認証データは、生体認証データであることを特徴とする請求の範囲第1項記載のファイル共有装置。
- [請求項4] 前記共有設定用データは、ブロードキャストにより送信されることを特徴とする請求の範囲第1項記載のファイル共有装置。
- [請求項5] コンピュータが、
 前記コンピュータに格納された共有対象のファイルへのアクセスを要求する任意のユーザのアカウントおよび認証データを含む共有設定用データを受信し、
 前記共有設定用データに含まれる前記認証データが、予め格納しておいた特定のユーザを認証する認証データに一致するか否かを判断し、

一致する場合に前記共有設定用データに含まれる前記アカウントに基づいて前記共有対象のファイルへのアクセスを要求するユーザの前記共有対象のファイルへのアクセスを許可するアカウントを作成し、作成された前記アカウントを記憶する、
ことを特徴とするファイル共有方法。

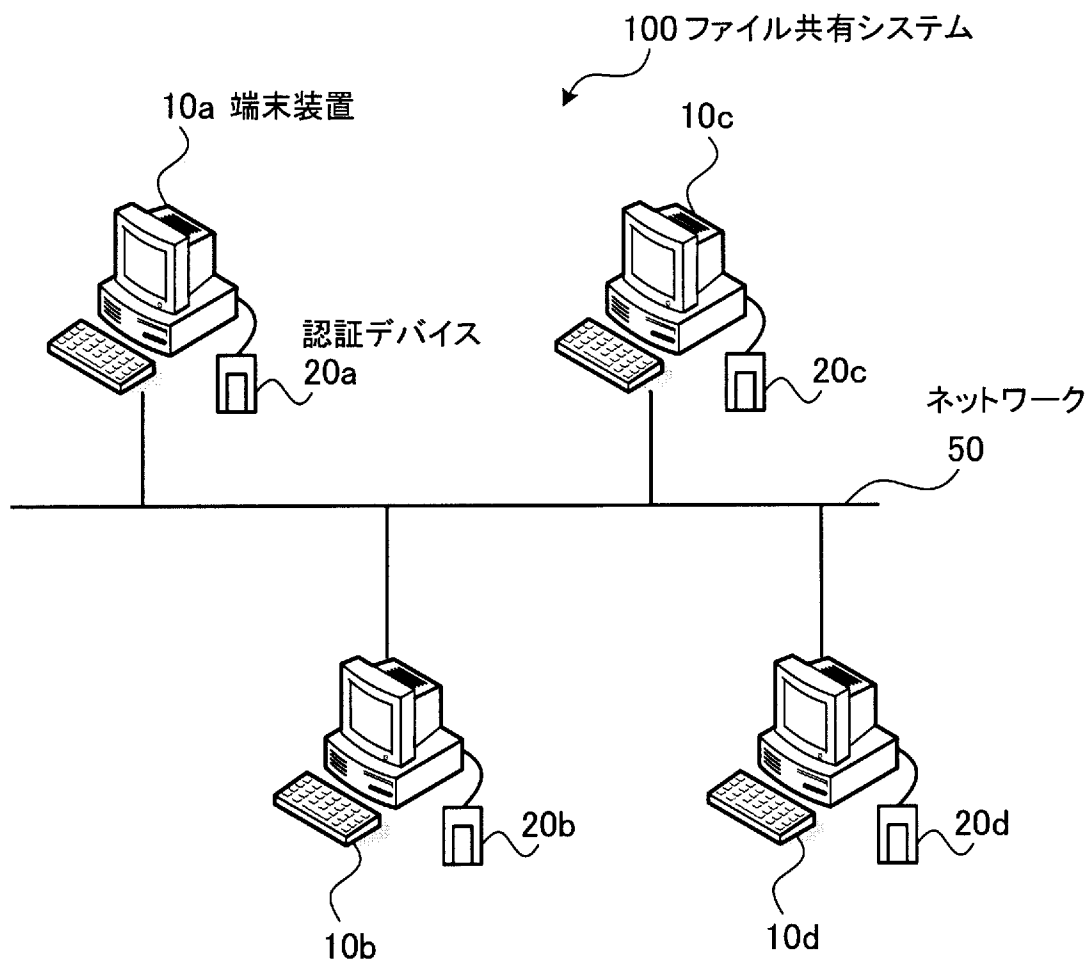
[請求項6]

コンピュータに、
前記コンピュータに格納された共有対象のファイルへのアクセスを要求する任意のユーザのアカウントおよび認証データを含む共有設定用データを受信し、
前記共有設定用データに含まれる前記認証データが、予め格納しておいた特定のユーザを認証する認証データに一致するか否かを判断し、
一致する場合に前記共有設定用データに含まれる前記アカウントに基づいて前記共有対象のファイルへのアクセスを要求するユーザの前記共有対象のファイルへのアクセスを許可するアカウントを作成し、作成された前記アカウントを記憶する、
ことを実行させるためのプログラム。

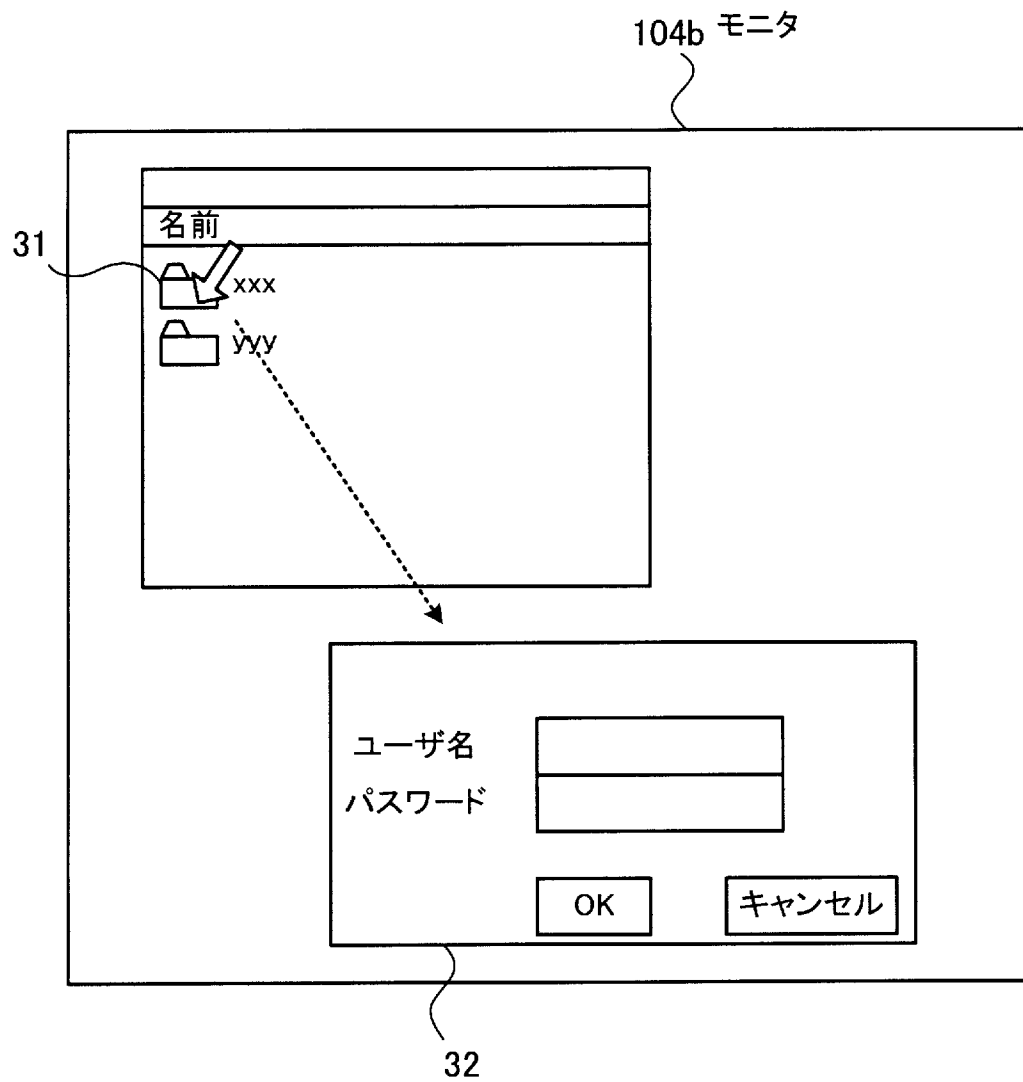
[図1]



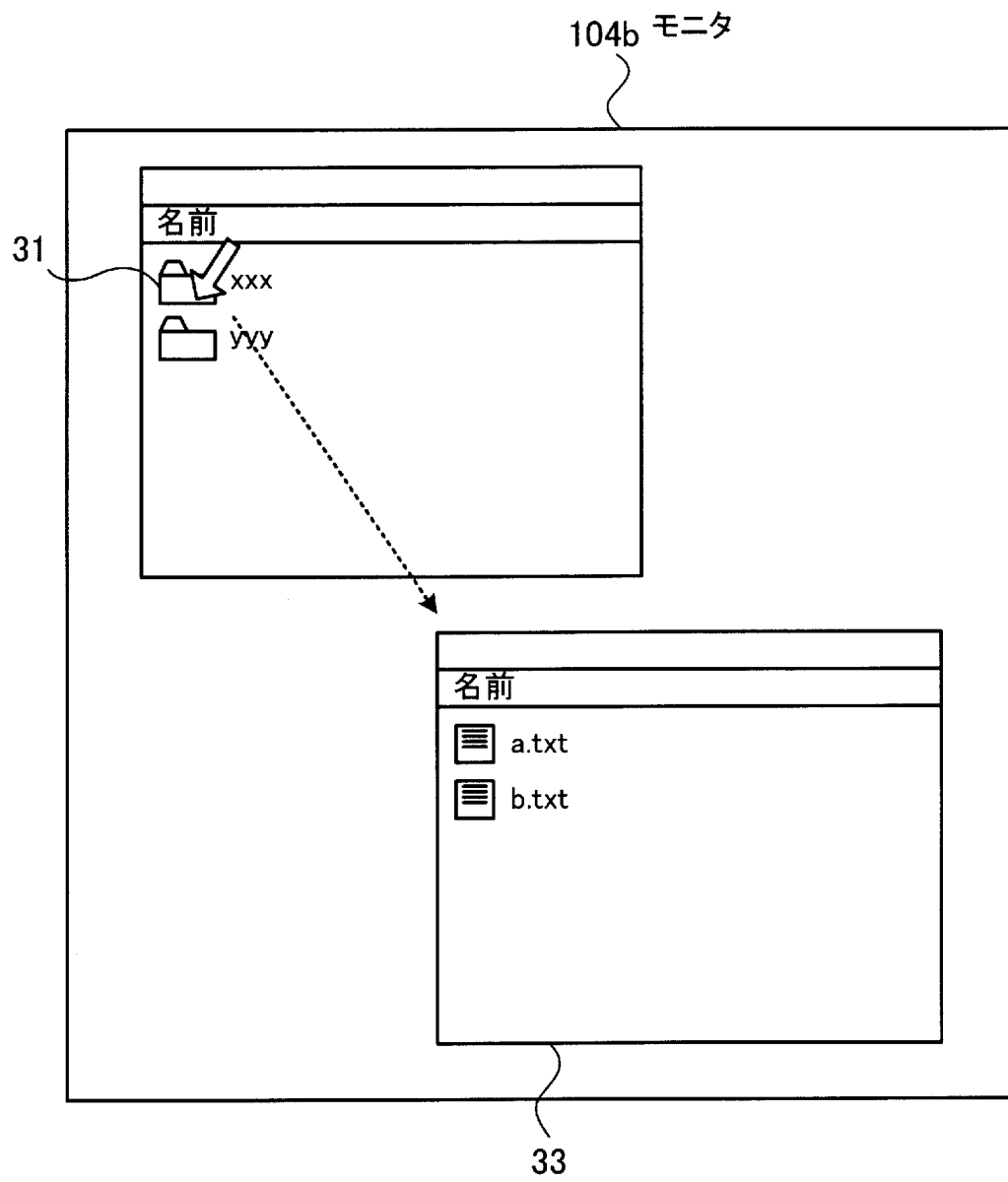
[図2]



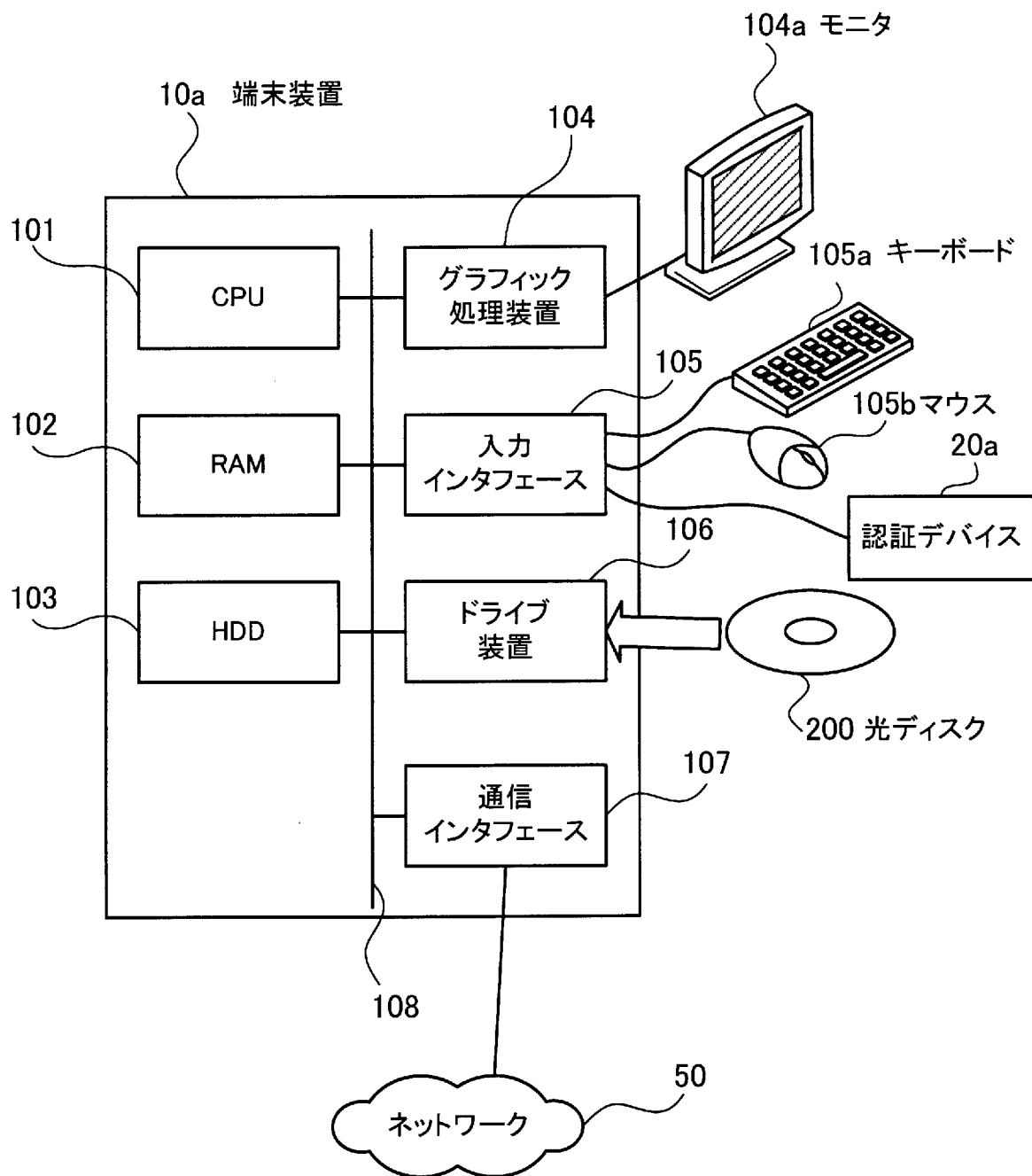
[図3]



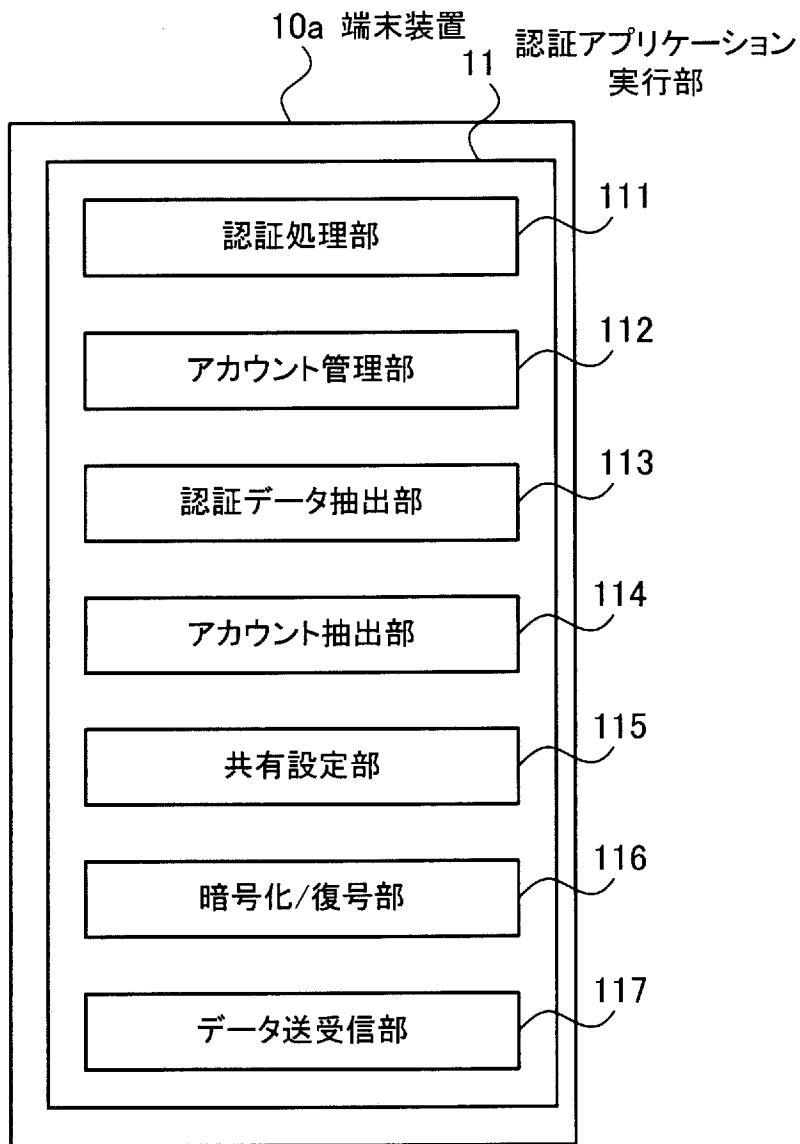
[図4]



[図5]



[図6]

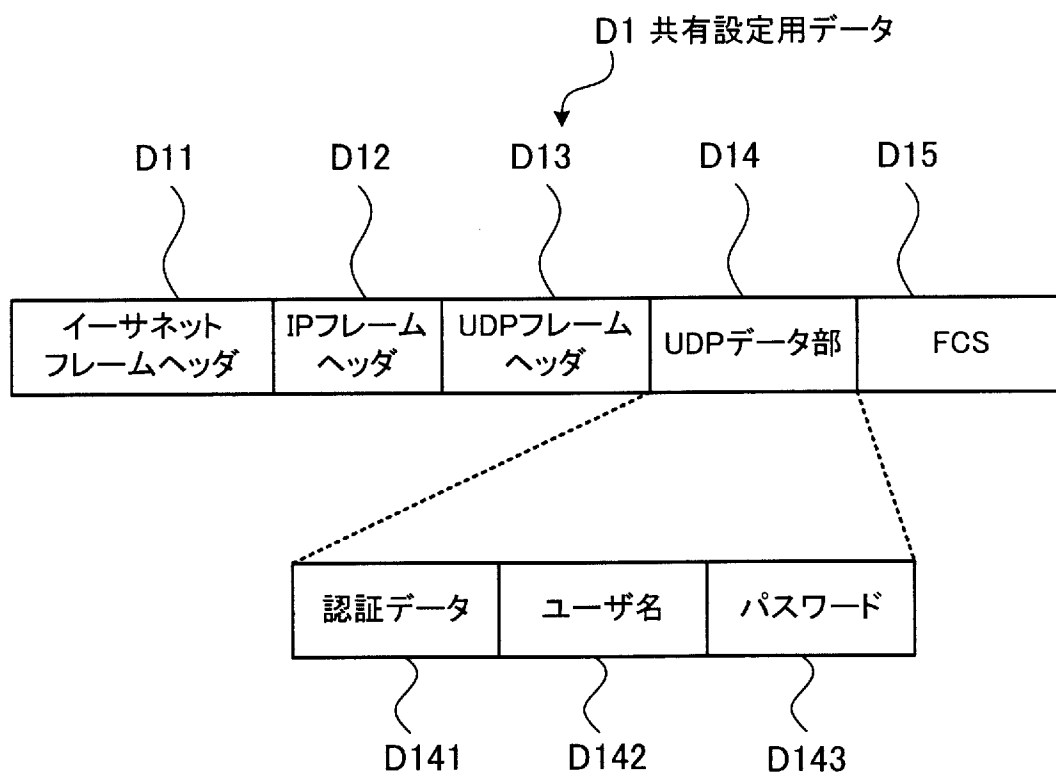


[図7]

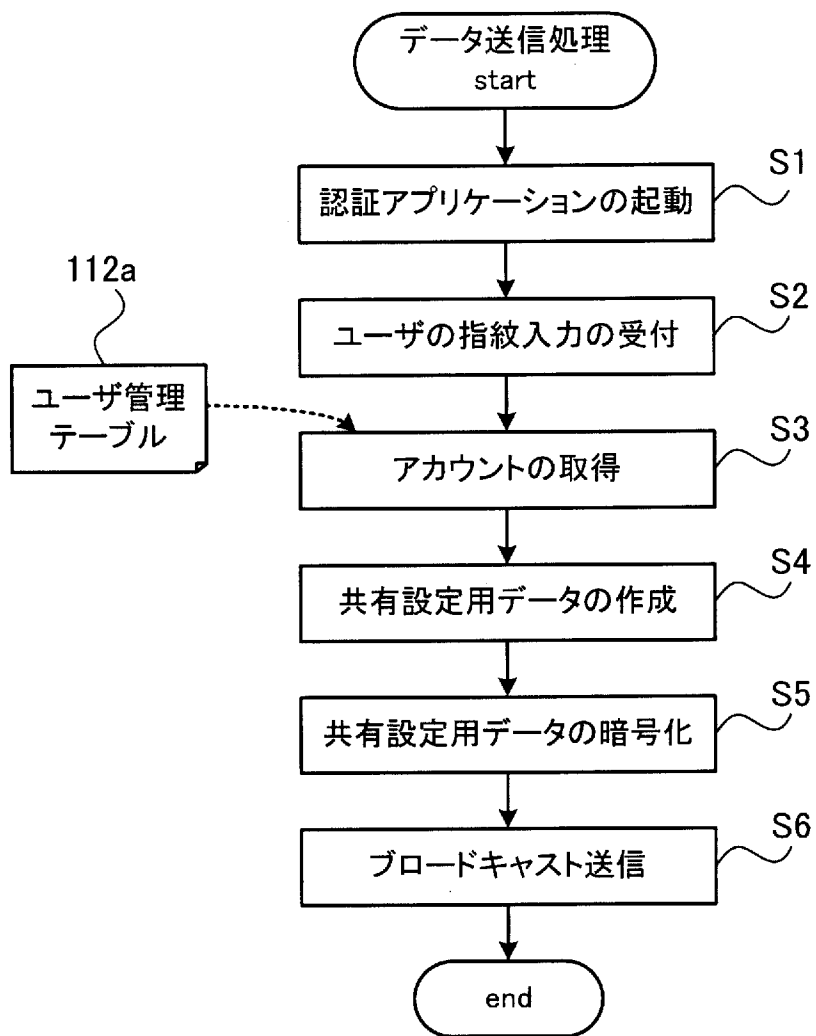
112a ユーザ管理テーブル

ID	認証データ	ユーザ名	パスワード
1	...	UserA	PasswordA
2	...	UserB	PasswordB
⋮	⋮	⋮	⋮
N	...	UserN	PasswordN

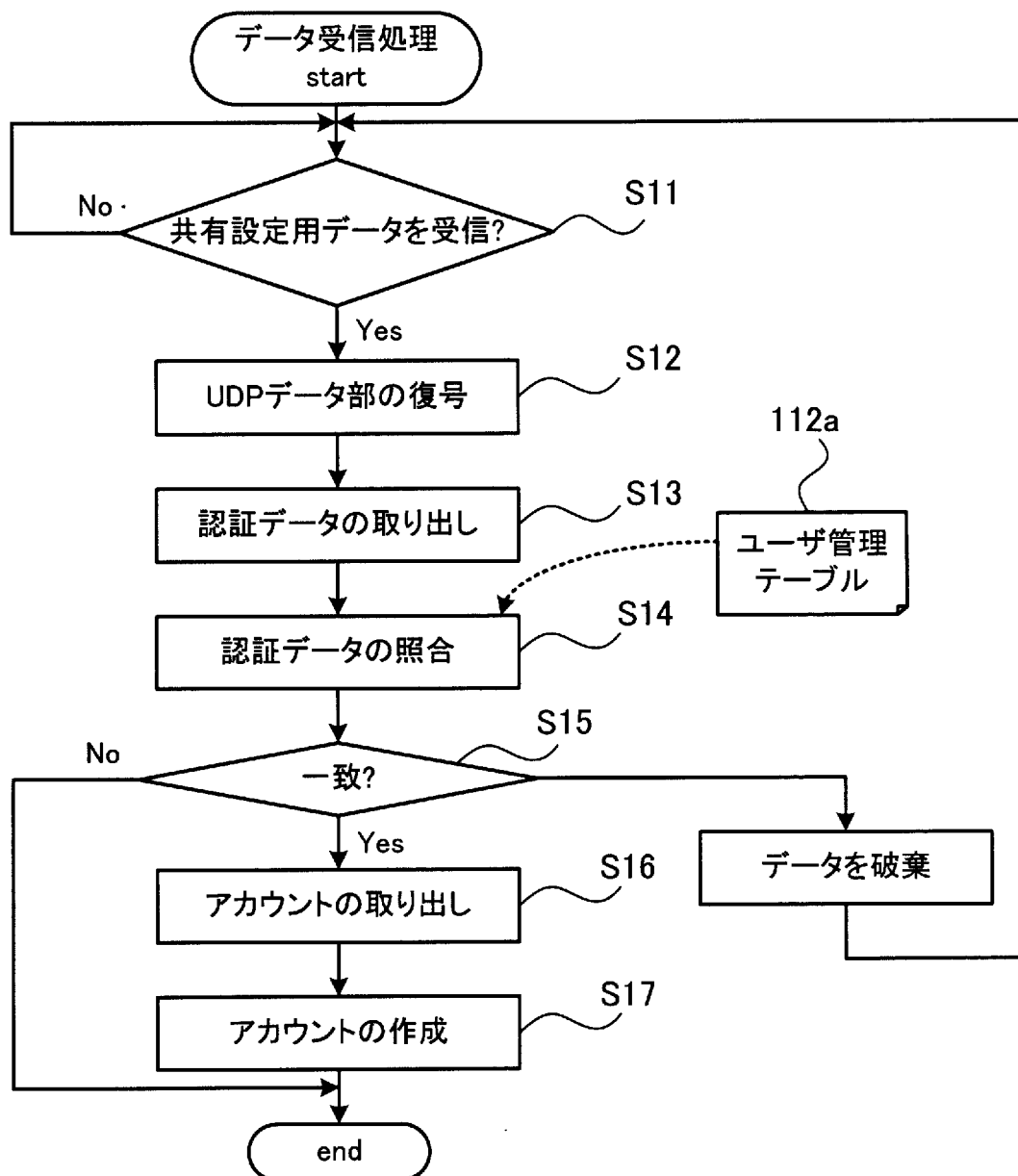
[図8]



[図9]



[図10]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2011/054751

A. CLASSIFICATION OF SUBJECT MATTER

G06F21/24(2006.01) i, G06F12/00(2006.01) i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F21/24, G06F12/00

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

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2011
Kokai Jitsuyo Shinan Koho	1971-2011	Toroku Jitsuyo Shinan Koho	1994-2011

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2009-503632 A (Microsoft Corp.), 29 January 2009 (29.01.2009), entire text; all drawings & US 2007/0016630 A1 & WO 2007/008852 A2 & KR 10-2008-0024513 A & CN 101495986 A	1-6
A	US 2004/0210767 A1 (Sinclair et al.), 21 October 2004 (21.10.2004), entire text; all drawings (Family: none)	1-6
A	JP 2010-239365 A (NTT Docomo Inc.), 21 October 2010 (21.10.2010), abstract (Family: none)	1-6

☒ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:

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

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

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

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

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

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

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

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

“&” document member of the same patent family

Date of the actual completion of the international search
29 March, 2011 (29.03.11)

Date of mailing of the international search report
05 April, 2011 (05.04.11)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2011/054751

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2006-140790 A (Matsushita Electric Industrial Co., Ltd.), 01 June 2006 (01.06.2006), paragraphs [0051] to [0054] & US 2009/0011748 A1 & EP 1811760 A1 & WO 2006/051858 A1	1-6

A. 発明の属する分野の分類 (国際特許分類 (I P C))

Int.Cl. G06F21/24(2006.01)i, G06F12/00(2006.01)i

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (I P C))

Int.Cl. G06F21/24, G06F12/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1 9 2 2 - 1 9 9 6 年
日本国公開実用新案公報	1 9 7 1 - 2 0 1 1 年
日本国実用新案登録公報	1 9 9 6 - 2 0 1 1 年
日本国登録実用新案公報	1 9 9 4 - 2 0 1 1 年

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

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
A	JP 2009-503632 A (マイクロソフト コーポレーション) 2009.01.29, 全文, 全図 & US 2007/0016630 A1 & WO 2007/008852 A2 & KR 10-2008-0024513 A & CN 101495986 A	1-6
A	US 2004/0210767 A1 (Sinclair et al.) 2004.10.21, 全文, 全図 (ファミリーなし)	1-6

☒ C 欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

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

の日の後に公表された文献

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

国際調査を完了した日

2 9 . 0 3 . 2 0 1 1

国際調査報告の発送日

0 5 . 0 4 . 2 0 1 1

国際調査機関の名称及びあて先

日本国特許庁 (I S A / J P)

郵便番号 1 0 0 - 8 9 1 5

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

平井 誠

5 S

9 0 7 1

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

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
A	JP 2010-239365 A (株式会社エヌ・ティ・ティ・ドコモ) 2010. 10. 21, 要約 (ファミリーなし)	1-6
A	JP 2006-140790 A (松下電器産業株式会社) 2006. 06. 01, [0051]-[0054] & US 2009/0011748 A1 & EP 1811760 A1 & WO 2006/051858 A1	1-6