(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6376869号
(P6376869)
(45)発行日　平成30年8月22日(2018.8.22)　(24)登録日　平成30年8月3日(2018.8.3)

(51)Int.Cl.　F I
G06F 12/00 (2006.01)　G06F 12/00 533J
G06F 12/00 546A

請求項の数 6　(全 18 頁)

(21)出願番号　特願2014-142726(P2014-142726)
(22)出願日　平成26年7月10日(2014.7.10)
(65)公開番号　特開2016-18507(P2016-18507A)
(43)公開日　平成28年2月1日(2016.2.1)
審査請求日　平成29年7月7日(2017.7.7)

(73)特許権者　000001007
キヤノン株式会社
東京都大田区下丸子３丁目３０番２号
(74)代理人　100126240
弁理士　阿部　琢磨
(74)代理人　100124442
弁理士　黒岩　創吾
(72)発明者　▲浜▼渦　奨
東京都大田区下丸子３丁目３０番２号キヤノン株式会社内

審査官　福田　正悟

最終頁に続く

(54)【発明の名称】データ同期システム、その制御方法、認可サーバー、およびそのプログラム

(57)【特許請求の範囲】
【請求項１】
データの更新を行う端末と、前記端末にて前記データが更新されたことに応じて別の端末に対し更新された前記データを同期させるサーバーシステムと、認可サーバーとを含むデータ同期システムであって、
前記端末にて表示される認証画面を介しユーザーから入力された認証情報を基に、前記ユーザーが正規なユーザーであるか否かを判断する認証手段と、
前記認証手段により正規なユーザーであると判断された前記ユーザーが前記端末にて表示される認可確認画面を介して前記認可サーバーにおける前記ユーザーの権限を前記サーバーシステムへ移譲することを許可する指示をした場合に、前記ユーザーの権限が前記サーバーシステムへ移譲されたことを示す権限情報を発行する発行手段と、
前記データを同期させる端末の識別情報を前記認可サーバーに対し前記サーバーシステムが要求する際に送信した前記権限情報を基に、前記ユーザーに関連付く前記端末の識別情報を前記サーバーシステムへ送信する送信手段と、
前記ユーザーに関連付く前記端末の識別情報を基に、更新された前記データの同期を前記端末の識別情報が示す端末に対して実行させる旨と、前記端末の識別情報とを含む前記認可確認画面を前記端末へ提供する提供手段と、を有し、
前記サーバーシステムは、前記送信手段により送信された前記端末の識別情報に含まれる別の端末の識別情報を特定したことに応じて、前記別の端末に対し更新された前記データを同期させ、

前記発行手段は、前記提供手段により提供される前記認可確認画面を介し、前記認可サーバーにおける前記ユーザーの権限を前記サーバーシステムへ移譲することを許可する指示をした場合に、前記ユーザーの権限が前記サーバーシステムへ移譲されたことを示す権限情報を発行し、

前記認可サーバーにおける前記ユーザーの権限を前記サーバーシステムへ移譲することを許可する指示がなされた場合において前記端末へ提供された前記認可確認画面に含まれる前記端末の識別情報と、その際に発行された前記権限情報とを関連づけた情報を、前記ユーザーに関連付く前記端末の識別情報とは別に保存する保存手段を更に有し、

前記送信手段は、前記サーバーシステムが送信した前記権限情報に関連付く前記端末の識別情報を取得し、取得した前記端末の識別情報を前記ユーザーに関連付く前記端末の識別情報として前記サーバーシステムへ送信することを特徴とするデータ同期システム。

【請求項２】

前記発行手段は、前記権限情報を発行する際、前記ユーザーに関連付く前記端末の識別情報と、前記保存手段により保存された前記端末の識別情報とが同一である場合は、前記認可サーバーにおける前記ユーザーの権限を前記サーバーシステムへ移譲することを許可する指示を受け付けることなく、前記権限情報を発行することを特徴とする請求項１に記載のデータ同期システム。

【請求項３】

前記提供手段は、前記権限情報が発行される際、前記ユーザーに関連付く前記端末の識別情報と、前記保存手段により保存された前記端末の識別情報とが同一である場合は、前記認可確認画面を前記端末へ提供せず、

前記発行手段は、前記認可サーバーにおける前記ユーザーの権限を前記サーバーシステムへ移譲することを許可する指示を受け付けることなく、前記権限情報を発行することを特徴とする請求項１または２に記載のデータ同期システム。

【請求項４】

データの更新を行う端末と、前記端末にて前記データが更新されたことに応じて別の端末に対し更新された前記データを同期させるサーバーシステムと、認可サーバーとを含むデータ同期システムを制御する方法であって、

認証手段は、前記端末にて表示される認証画面を介しユーザーから入力された認証情報を基に、前記ユーザーが正規なユーザーであるか否かを判断し、

発行手段は、前記認証手段により正規なユーザーであると判断された前記ユーザーが前記端末にて表示される認可確認画面を介して前記認可サーバーにおける前記ユーザーの権限を前記サーバーシステムへ移譲することを許可する指示をした場合に、前記ユーザーの権限が前記サーバーシステムへ移譲されたことを示す権限情報を発行し、

送信手段は、前記データを同期させる端末の識別情報を前記認可サーバーに対し前記サーバーシステムが要求する際に送信した前記権限情報を基に、前記ユーザーに関連付く前記端末の識別情報を前記サーバーシステムへ送信し、

提供手段は、前記ユーザーに関連付く前記端末の識別情報を基に、更新された前記データの同期を前記端末の識別情報が示す端末に対して実行させる旨と、前記端末の識別情報とを含む前記認可確認画面を前記端末へ提供し、

前記サーバーシステムは、前記送信手段により送信された前記端末の識別情報に含まれる別の端末の識別情報を特定したことに応じて、前記別の端末に対し更新された前記データを同期させ、

前記発行手段は、前記提供手段により提供される前記認可確認画面を介し、前記認可サーバーにおける前記ユーザーの権限を前記サーバーシステムへ移譲することを許可する指示をした場合に、前記ユーザーの権限が前記サーバーシステムへ移譲されたことを示す権限情報を発行し、

保存手段は、前記認可サーバーにおける前記ユーザーの権限を前記サーバーシステムへ移譲することを許可する指示がなされた場合において前記端末へ提供された前記認可確認画面に含まれる前記端末の識別情報と、その際に発行された前記権限情報とを関連づけた

情報を、前記ユーザーに関連付く前記端末の識別情報とは別に保存し、
前記送信手段は、前記サーバーシステムが送信した前記権限情報に関連付く前記端末の識別情報を取得し、取得した前記端末の識別情報を前記ユーザーに関連付く前記端末の識別情報として前記サーバーシステムへ送信することを特徴とする方法。
【請求項５】
前記発行手段は、前記権限情報を発行する際、前記ユーザーに関連付く前記端末の識別情報と、前記保存手段により保存された前記端末の識別情報とが同一である場合は、前記認可サーバーにおける前記ユーザーの権限を前記サーバーシステムへ移譲することを許可する指示を受け付けることなく、前記権限情報を発行することを特徴とする請求項４に記載の方法。
【請求項６】
前記提供手段は、前記権限情報が発行される際、前記ユーザーに関連付く前記端末の識別情報と、前記保存手段により保存された前記端末の識別情報とが同一である場合は、前記認可確認画面を前記端末へ提供せず、
前記発行手段は、前記認可サーバーにおける前記ユーザーの権限を前記サーバーシステムへ移譲することを許可する指示を受け付けることなく、前記権限情報を発行することを特徴とする請求項４または５に記載の方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ネットワークを介して接続される複数の端末のデータを同期するためのデータ同期システム、その制御方法、認可サーバー、およびそのプログラムに関する。
【背景技術】
【０００２】
近年、インターネット上のシステムを介して複数の端末のデータを同期するサービスが提供されている。たとえば、辞書情報が更新されるとユーザーの所有する全ての端末に更新された辞書情報を転送するサービス（特許文献１）や写真を保存するとユーザーの所有する他の端末に転送するサービス（Ａｐｐｌｅ社　ｉＣｌｏｕｄ（登録商標）のフォトストリーム）などが、このようなサービスに該当する。
【先行技術文献】
【特許文献】
【０００３】
【特許文献１】特開２０１１－０６５５４２
【発明の概要】
【発明が解決しようとする課題】
【０００４】
データ同期サービスを利用して複数端末間のデータ同期をするために、データ同期サービスはユーザーの所有端末リストを取得する必要がある。背景技術において紹介したサービスではユーザーがサービスにユーザーの所有端末リストを登録することで、サービスがユーザーの所有端末リストを取得している。
【０００５】
しかしながら、前述の方法では、ユーザーの所有端末リストを複数のサービスに提供できない。そのため、ユーザーはサービス毎に端末を登録することになる。端末の追加・削除をする場合、ユーザーは複数のサービスに対してユーザーの所有端末リストを更新しなければならない。サービス毎に端末を追加・削除することは、複数のデータ同期サービスを併用するユーザーにとって手間である。
【０００６】
また、別の課題として、複数のサービスでユーザーの所有端末リストを分散管理した場合情報漏洩の危険性が高まるという課題がある。複数のサービスでユーザーの所有端末リストを分散管理する場合、サービス毎にセキュリティ対策が異なっていることが予想され

る。セキュリティ対策に問題があるサービスは、意図せずにユーザーの所有端末リストが漏洩する可能性がある。ユーザーの許可なく、ユーザーの所有端末リストが他者に提供されてしまう可能性もある。

【０００７】

本発明は、上述した課題の内少なくとも１つの課題を解決することを目的としている。目的を達成するため本発明は、ユーザーが信頼できるサーバーでユーザーの所有端末リストを集約管理し、ユーザーが許可したサービスにのみユーザーの所有端末リストを提供できるようにすることを特徴とする。

【課題を解決するための手段】

【０００８】

本発明の一実施形に係るデータ同期システムは、データの更新を行う端末と、前記端末にて前記データが更新されたことに応じて別の端末に対し更新された前記データを同期させるサーバーシステムと、認可サーバーとを含むデータ同期システムであって、前記端末にて表示される認証画面を介しユーザーから入力された認証情報を基に、前記ユーザーが正規なユーザーであるか否かを判断する認証手段と、前記認証手段により正規なユーザーであると判断された前記ユーザーが前記端末にて表示される認可確認画面を介して前記認可サーバーにおける前記ユーザーの権限を前記サーバーシステムへ移譲することを許可する指示をした場合に、前記ユーザーの権限が前記サーバーシステムへ移譲されたことを示す権限情報を発行する発行手段と、前記データを同期させる端末の識別情報を前記認可サーバーに対し前記サーバーシステムが要求する際に送信した前記権限情報を基に、前記ユーザーに関連付く前記端末の識別情報を前記サーバーシステムへ送信する送信手段と、前記ユーザーに関連付く前記端末の識別情報を基に、更新された前記データの同期を前記端末の識別情報が示す端末に対して実行させる旨と、前記端末の識別情報とを含む前記認可確認画面を前記端末へ提供する提供手段と、を有し、前記サーバーシステムは、前記送信手段により送信された前記端末の識別情報に含まれる別の端末の識別情報を特定したことに応じて、前記別の端末に対し更新された前記データを同期させ、前記発行手段は、前記提供手段により提供される前記認可確認画面を介し、前記認可サーバーにおける前記ユーザーの権限を前記サーバーシステムへ移譲することを許可する指示をした場合に、前記ユーザーの権限が前記サーバーシステムへ移譲されたことを示す権限情報を発行し、

前記認可サーバーにおける前記ユーザーの権限を前記サーバーシステムへ移譲することを許可する指示がなされた場合において前記端末へ提供された前記認可確認画面に含まれる前記端末の識別情報と、その際に発行された前記権限情報とを関連づけた情報を、前記ユーザーに関連付く前記端末の識別情報とは別に保存する保存手段を更に有し、

前記送信手段は、前記サーバーシステムが送信した前記権限情報に関連付く前記端末の識別情報を取得し、取得した前記端末の識別情報を前記ユーザーに関連付く前記端末の識別情報として前記サーバーシステムへ送信することを特徴とする。

【発明の効果】

【０００９】

ユーザーが信頼できるサーバーでユーザーの所有端末リストを集約管理し、ユーザーが許可したサービスにのみユーザーの所有端末リストを提供できるようになる。

【図面の簡単な説明】

【００１０】

【図１】システム構成図
【図２】サービスを利用するまたは提供する装置のハードウェア構成図
【図３】本実施の形態に係る各装置のソフトウェアモジュール構成図
【図４】本実施の形態に係る認可サーバーで管理するテーブル構造
【図５】本実施の形態に係るトークン取得とデータ同期のシーケンス図
【図６】本実施の形態に係るログイン／認可確認の画面例
【図７】本実施の第２の実施系に係るシーケンス図
【図８】本実施の第２の実施系に係る認可確認の画面例

【図９】本実施の第３の実施系に係るテーブル構造
【図１０】本実施の第３の実施系に係るシーケンス図
【図１１】本実施の第４の実施系に係るシーケンス図
【図１２】本実施の第５の実施系に係るシーケンス図
【図１３】本実施の第５の実施系に係る画面例
【発明を実施するための形態】
【００１１】
以下、本発明を実施するための最良の形態について図面を用いて説明する。
【実施例１】
【００１２】
本実施の形態に係るデータ同期システムは図１に示すような構成のネットワーク上に実現される。１００は、Ｗｉｄｅ　Ａｒｅａ　Ｎｅｔｗｏｒｋ（WAN１００）であり、本発明ではＷｏｒｌｄ　Ｗｉｄｅ　Ｗｅｂ（WWW）システムが構築されている。１０１はＬｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ（ＬＡＮ１０１）である。２００、２２０、２４０はユーザーが操作する端末である。３００は認可サーバーである。４００はデータ同期サーバーである。
【００１３】
端末２００、２２０、２４０、認可サーバー３００、データ同期サーバー４００はそれぞれＷＡＮネットワーク１００およびＬＡＮ１０１を介して接続されている。なお認可サーバー３００、データ同期サーバー４００はそれぞれ個別のＬＡＮ上に構成されていてもよいし同一のＬＡＮ上に構成されていてもよい。また同一の装置上に構成されていてもよい。また、本実施例では認可サーバー３００、データ同期サーバー４００は１台として説明するが、夫々の装置が複数台で構成されているシステムであっても良い。このように本発明の実施に際し台数に特に制限はないため、サーバーシステムと称した場合は１台または複数台のサーバーから構成されるものとする。
【００１４】
本実施の形態では、ＯＡｕｔｈと呼ばれる権限委譲の標準プロトコルを用いて、ネットワーク上の端末２００、２２０、２４０、認可サーバー３００、データ同期サーバー４００の連携し、端末間のデータ同期を実現する。ＯＡｕｔｈについては以降でさらに詳細に説明する。
【００１５】
ＯＡｕｔｈによれば、例えばあるサービスＡが管理するユーザーのデータに、そのユーザーから認められた外部サービスＢがアクセスすることができる。このときサービスＡは、外部サービスＢからアクセスされる範囲を明らかにした上で、外部サービスＢによるアクセスに対してユーザーの明示的な認可を得ることになっている。ユーザーが明示的に認可を行うことを認可操作と称する。ユーザーが認可操作を行うと、外部サービスＢはサービスＡからアクセスを認められたことを証明するトークン（以下、認可トークンと称する）　を受け取る。以降、認可トークンを使うことで、外部サービスＢはサービスＡの認可を受けた範囲にアクセス可能となる。なお、認可トークンの様にユーザーの権限を外部サービスＢのような連携要求元に移譲したことを示す情報を権限情報と称する。ＯＡｕｔｈにおいて、サービスＡのようにサービスを提供するサーバーは、リソースサーバーと呼ばれる。また、外部サービスＢのように、サービスの利用者は、クライアントと呼ばれる。
【００１６】
次に、各構成要素の役割を説明する。端末２００、２２０、２４０はＰＣ、タブレット、スマートフォン、フューチャーフォンなどの情報機器である。ユーザーは端末を操作し、端末内にデータ同期対象のファイルの追加・変更・削除をする。ファイルの例としては、文書、写真イメージ、辞書データなどがあげられる。また、ユーザーは端末でＯＡｕｔｈの認可操作をする。認可サーバー３００はＯＡｕｔｈの認可サーバー兼、リソースサーバーである。認可サーバー３００はユーザーの認可操作を求め、認可トークンを発行するサーバーである。データ同期サーバー４００はＯＡｕｔｈのクライアントである。データ

同期サーバー４００は認可サーバー３００から認可トークンを受け取り、その認可トークンを利用して認可サーバー３００のサービスとして公開するリソースを取得する。

【００１７】

図２は本実施の形態に係るサービスを利用するまたはサービスを提供する端末の構成を示す図である。尚、図２に示されるハードウェアブロック図は一般的な情報処理装置のハードウェアブロック図に相当するものとし、本実施形態の端末２００、２２０、２４０、認可サーバー３００、データ同期サーバー４００には一般的な情報処理装置のハードウェア構成を適用できる。

【００１８】

図２において、ＣＰＵ２０１は、ＲＯＭ２０３のプログラム用ＲＯＭに記憶された、或いは外部メモリ２１１からＲＡＭ２０２にロードされたＯＳやアプリケーション等のプログラムを実行する。ここでＯＳとはコンピュータ上で稼動するオペレーティングシステムの略語であり、以下オペレーティングシステムのことをＯＳと呼ぶ。後述する各処理はこのプログラムの実行により実現できる。ＲＡＭ２０２は、ＣＰＵ２０１の主メモリ、ワークエリア等として機能する。キーボードコントローラ（ＫＢＣ）２０５は、キーボード２０９や不図示のポインティングデバイスからのキー入力を制御する。ディスプレイコントローラ（ＤＩＳＰＣ）２０６は、ディスプレイ（ＤＩＳＰ）２１０の表示を制御する。ディスクコントローラ（ＤＫＣ）２０７は各種データを記憶する外部メモリ２１１（ハードディスク（ＨＤ）やシリコンディスク（ＳＳＤ）等）におけるデータアクセスを制御する。ＮＣ２０８はネットワークに接続されて、ネットワークに接続された他の機器との通信制御処理を実行する。なお、後述の全ての説明においては、特に断りのない限り実行のハード上の主体はＣＰＵ２０１であり、ソフトウェア上の主体は外部メモリ２１１にインストールされたアプリケーションプログラムである。

【００１９】

図３は本実施の形態に係る各装置のソフトウェアモジュール構成を示す図である。端末２００、２２０、２４０はデータ同期アプリケーション５００、５２０、５４０を持つ。認可サーバー３００は認可モジュール６００を持つ。またデータ同期サーバー４００はデータ同期モジュール７００を持つ。各モジュールは、各ハードの外部メモリ２１１にアプリケーションプログラムとしてインストールされている。各モジュールの処理詳細については後述する。

【００２０】

図４ａ、図４ｂ、図４ｃ、図４ｄ、図４ｅは認可サーバー３００が外部メモリ２１１に記憶するデータテーブルである。これらデータテーブルは、認可サーバー３００の外部メモリ２１１ではなく、ＬＡＮ１０１を介して通信可能に構成された別のサーバーに記憶するよう構成する事も出来る。図４ａはユーザー管理テーブル１０００である。ユーザー管理テーブル１０００は、ユーザーＩＤ１００１、パスワード１００２から成る。認可サーバー３００は、ユーザーＩＤ１００１、パスワード１００２の情報の組を検証し、正しければ認証情報を生成することで、各ユーザーを認証する機能を備える。

【００２１】

図４ｂはクライアント管理テーブル１１００である。クライアント管理テーブル１１００は、クライアントＩＤ１１０１、クライアント名１１０２、パスワード１１０３、リダイレクトＵＲＩ１１０４から成る。認可モジュール６００はＯＡｕｔｈのプロトコルを利用して他サービスに権限委譲する際に、クライアント管理テーブル１１００を参照し、他サービスがＯＡｕｔｈクライアントとして登録済みであることを確認する。図４ｃは端末管理テーブル１２００である。端末管理テーブル１２００はユーザーＩＤ１２０１、端末ＩＤ１２０２、端末名１２０３、デバイストークン１２０４から成る。

【００２２】

ユーザーＩＤ１２０１は端末の所有者を特定するための値である。ユーザーＩＤ１２０１はユーザテーブル１０００のユーザーＩＤ１００１と関連付いており、互いに参照可能となっている。端末ＩＤ１２０２は端末（２００、２２０、２４０）をユニークに識別可

能な値であり、端末を一意に識別するための識別情報である。端末名１２０３は後述の画面例で利用される値である。なお、識別情報は端末ＩＤとしたがそれに限られることはなく、例えば、端末名であっても良い。デバイストークン１２０４はデバイスにＰｕｓｈ通知を送るために使用されるＰｕｓｈ通知システム側で発行される値である。Ｐｕｓｈ通知をサポートしている端末は、デバイストークン１２０４に値を保存しておける。端末間のデータ同期におけるＰｕｓｈ通知については後述する。

【００２３】

図４ｄは同期データ管理テーブル１３００である。同期データ管理テーブル１３００はデータＩＤ１３０１、ユーザーＩＤ１３０２、更新区分１３０３、ファイルパス１３０４、ファイル名１３０５、同期時刻１３０６から成る。同期データ管理テーブル１３００の処理中での利用については後述する。

【００２４】

図４ｅは認可トークン管理テーブル１４００である。認可トークン管理テーブル１４００は、認可トークンＩＤ１４０１、トークン種別１４０２、有効期限１４０３、スコープＩＤ１４０４、リフレッシュトークンＩＤ１４０５、リフレッシュ期限１４０６、端末ＩＤ１４０７、ユーザーＩＤ１４０８、リダイレクトＵＲＩ１４０９から成る。これら認可トークン管理テーブル１４００の処理中での利用については後述する。

【００２５】

図５は本実施の形態に係るトークン取得とデータ同期のシーケンスを示す図である。まずユーザーが端末２００において、データ同期アプリケーション５００が管理するディレクトリ配下に対してファイルの追加・更新・削除をする（ｓ１．１）。以降、この操作を端末２００のデータ更新と呼ぶ。なお、ディレクトリ配下と言うのは端末２００自身のメモリのディレクトリの他に、端末２００がネットワークを介して通信を行う外部装置のメモリのディレクトリも含む。

【００２６】

データ同期アプリケーション５００が端末２００のデータ更新を検知して、データ同期モジュール７００に対してデータ同期要求をする（ｓ１．２）。データ同期アプリケーション５００は、同期データ情報として、端末ＩＤ、端末２００にて発行されるユニークＩＤ、端末所有者のユーザーＩＤ、端末２００でのデータ更新内容、ファイルパス、ファイル名をデータ同期モジュール７００に送信する。端末２００でのデータ更新内容は、データ更新がデータに対する追加、更新、削除のいずれの操作であるかを示すものである。

【００２７】

ファイルパスは、データ同期アプリケーション５００が管理するディレクトリ配下からの相対パスである。なお、以降、端末ＩＤ、ユニークＩＤを合わせてデータＩＤと呼称する。データ同期モジュール７００が同期データ情報を受け取ると、次の処理をする。データＩＤを同期データ管理テーブル１３００のデータＩＤ１３０１に保存する。端末所有者のユーザーＩＤを同期データ管理テーブル１３００のユーザーＩＤ１３０２に保存する。端末２００でのデータ更新内容を同期データ管理テーブル１３００の更新区分１３０３に保存する。ファイルパスを同期データ管理テーブル１３００のファイルパス１３０４に保存する。ファイル名を同期データ管理テーブル１３００のファイル名１３０５に保存する。また、データ更新内容が追加／更新の場合、データ同期アプリケーション５００はデータ同期モジュール７００にファイルそのものを送信する。同期データ管理テーブル１３００の同期時刻１３０５に、データ同期モジュール７００が同期データ情報を受け取った時刻を保存する。

【００２８】

データ同期モジュール７００は、データ同期アプリケーション５００内のブラウザのリダイレクトにより、認可モジュール６００の認可エンドポイントのＵＲＬに対して、ＯＡｕｔｈの認可要求を送信する（ｓ１．３）。この認可要求には、認可コードを返却してもらうためのレスポンスタイプ、クライアントＩＤ、リダイレクトＵＲＩ、スコープＩＤがパラメータとして含まれる。スコープＩＤとは、ＯＡｕｔｈで認可を受けたい権限範囲を

示すパラメータである。本実施例では、スコープＩＤとして、端末リストの取得を指定する。認可要求はＨＴＴＰ　Ｇｅｔメソッドまたは ＨＴＴＰ　Ｐｏｓｔメソッドである。

【００２９】

認可モジュール６００は認可リクエストを受け取ると、認可要求の検証のため、次のことをする。認可要求にレスポンスタイプ、クライアントＩＤがパラメータとして含まれていることを確認する。認可要求の送信元が登録済みのクライアントであることを確認する。そのために、クライアント管理テーブル１１００から、クライアントＩＤ１１０１の値と認可リクエストに含まれているクライアントＩＤが一致するレコードを取得できることを確認する。

【００３０】

認可要求に含まれるリダイレクトＵＲＩが登録済みクライアントのリダイレクトＵＲＩと一致することを確認する。そのため、クライアント管理テーブル１１００から、クライアントＩＤ１１０１の値と認可要求に含まれているクライアントＩＤが一致するレコードを取得し、認可要求で送られてきたリダイレクトＵＲＩの値とクライアント管理テーブル１１００に登録されているリダイレクトＵＲＩ１１０４の値が一致することを確認する。認可要求ｓ１．３を受けた認可モジュール６００は、ユーザーを認証するための認証画面である図６ａに示すログイン画面１８０１をデータ同期アプリケーション５００のブラウザに応答する（ｓ１．４）。

【００３１】

ユーザーはブラウザに示されたログイン画面１８０２に対して、ユーザーＩＤ、パスワードを入力しログインを実行する（ｓ１．５）。認可モジュール６００は受け付けたユーザーＩＤ、パスワードの組がユーザー管理テーブル１０００に登録されている情報と合致するかを検証する。合致
した場合、ユーザーＩＤ、パスワードを入力したユーザーが正規なユーザーであると判断される。検証に問題がなければ、認可モジュール６００はユーザーＩＤが紐づいたログイン情報を生成する（ｓ１．６）。なお一度ログインが済んでいて既に有効なログイン情報が生成されている場合はｓ１．４～ｓ１．６の手続きは不要にしてもよい。

【００３２】

有効なログイン情報が生成されている場合、認可モジュールは図６ｂに示す認可確認画面１８０２をデータ同期アプリケーション５００のブラウザに表示する（ｓ１．７）。この認可確認画面１８０２は、スコープＩＤに基づいて、認可サーバーが管理しているユーザーの所有端末リストにアクセスする権限をデータ同期モジュール７００に委譲してよいかをユーザーに確認するための画面である。データ同期モジュール７００にユーザーの所有端末リストの取得権限を委譲してもよい場合は、許可を選択する。データ同期モジュール７００にユーザーの所有端末リストの取得権限を委譲させない場合は、拒否を選択する。この選択を行うことによりユーザーは権限の移譲を指示する。

【００３３】

Ｓ１．８でユーザーが認可確認画面１８０２にて許可を選んだ場合、つまり、認可操作を行った場合は、次の振る舞いをする。データ同期アプリケーション５００は認可モジュール６００に認可確認の結果を送信する（ｓ１．９）。許可を受けた認可モジュール６００の認可エンドポイントは次の処理を実行する。認可トークン管理テーブル１４００に認可コードを発行し登録する。その際、認可トークンＩＤ１４０１に発行したトークンＩＤ、トークン種別１４０２に認可コード、有効期限１４０３に認可トークンの有効期限、スコープＩＤ１４０４にデータ同期モジュール７００に委譲する権限を示すスコープＩＤ、クライアントＩＤ１４０７に認可リクエストに含まれるクライアントＩＤ、ユーザーＩＤ１４０８にデータ同期モジュール６００から送信された認証情報に紐付くユーザーＩＤ、リダイレクトＵＲＩ１４０９に認可リクエストに含まれているリダイレクトＵＲＩを登録する。

【００３４】

そして認可モジュール６００は、データ同期アプリケーション５００のブラウザを経由

して、データ同期モジュール７００に認可応答を返す（ｓ１．１０）。この認可応答には、認可コードが含まれている。認可コードは、後述のトークンエンドポイントに送信することで、認可トークンと交換できる。このように、認可コードと認可トークンを交換させる方式はセキュリティを高める効果がある。仮に悪意のある第三者に認可コードを詐取されたとしても、認可コードを用いて直接データ同期操作を行うことはできない。

【００３５】

ｓ１．８にてユーザーが認可確認画面１８０２にて拒否を選んだ場合は、次の振る舞いをする。データ同期アプリケーション５００は認可モジュール６００に認可確認の結果を送信する（ｓ１．９）認可モジュール６００は、データ同期アプリケーション５００にエラー応答を返す（ｓ１．１０）。エラー応答には、ＯＡｕｔｈで定められているエラーコードａｃｃｅｓｓ＿ｄｅｎｉｅｄが含まれている。データ同期アプリケーション５００はこのエラー応答を受け取ると、認可されなかった旨を画面に表示する。ここで処理が終了となる。

【００３６】

認可応答を受けたデータ同期モジュールは、認可モジュール６００のトークンエンドポイントのＵＲＬに対してトークン要求を送信する（ｓ１．１１）。トークン要求は、ＨＴＴＰ　Ｐｏｓｔリクエストである。このトークン要求は、認可応答で取得した認可コード、クライアントＩＤ、パスワード、リダイレクトＵＲＩを含む。

【００３７】

トークン要求を受けた認可モジュール６００は以下の検証を行う。トークン要求ｓ１．１１に必須パラメータが含まれていることを検証する。具体的には、グラントタイプ、認可コード、リダイレクトＵＲＩ、クライアントＩＤ、パスワードがトークン要求ｓ１．１１に含まれていることを検証する。グラントタイプの値がａｕｔｈｏｒｉｚａｔｉｏｎ＿ｃｏｄｅであることを確認する。トークン要求ｓ１．１１の認可コードが認可モジュール６００で発行したものであることを検証する。その際、トークン要求で受けつけた認可コードの認可トークンＩＤが、認可トークン管理テーブル１４００に登録されているかを確認する。また、有効期限１４０３を確認し、有効期限切れでないことを検証する。

【００３８】

トークン要求ｓ１．１１のクライアントＩＤ、パスワードの組み合わせが、クライアント管理テーブル１１００に登録されているクライアントＩＤ１１０１、パスワード１１０３の組み合わせと一致するか検証する。トークン要求ｓ１．１１の検証に問題がなければ、認可モジュール６００は認可トークンを発行してデータ同期モジュール７００に返却する（ｓ１．１２）。その際、認可トークン管理テーブル１４００に、次のように認可トークンを登録する。

【００３９】

認可トークンＩＤ１４０１に発行したトークンのＩＤ、トークン種別１４０２に認可トークン、有効期限１４０３、クライアントＩＤ１４０７、ユーザーＩＤ１４０８に認可コードから引き継ぐクライアントＩＤ、ユーザーＩＤ、スコープＩＤを登録する。この際、認可トークンをリフレッシュするためのリフレッシュトークンを発行し、リフレッシュトークンＩＤ１４０５、リフレッシュ期限１４０６に登録する。ここで、認可コードが認可トークンに交換される。なお、セキュリティ上の理由により、認可コードは１度しか利用できないにする。その方法としては、認可トークン管理テーブル１４００の認可コードのレコードを削除してもよいし、削除状態を管理するカラムを設けてフラグ情報を付与してもよい。

【００４０】

認可トークンを受領すると、データ同期モジュール７００は認可モジュール６００の端末リスト取得エンドポイントのＵＲＬに対して、同期端末リスト要求を送信する（ｓ１．１３）。この同期端末リスト要求ｓ１．１３はトークン応答ｓ１．１２で受け取った認可トークンを含む。認可モジュール６００は同期端末リスト取得要求ｓ１．１３を受信時に認可トークンの検証として次のことを行う。認可トークンテーブル１４００から、認可ト

ークンのトークンＩＤが一致するレコードを取得する。レコードの有効期限１４０３の値を参照し、認可トークンの有効期限が切れていないことを確認する。また、レコードのスコープＩＤ１４０４を参照し、スコープＩＤとして端末リストの取得が含まれていることを確認する。これにより、データ同期モジュール７００が認可モジュール６００の端末リストの取得の権限を委譲されていることが確認できる。

【００４１】

データ同期モジュール７００にユーザーの所有端末リストの取得権限が委譲されていた場合に、認可モジュール６００は端末管理テーブル１２００からユーザーの所有端末リストを取得して、データ同期モジュール７００に返送する（ｓ１．１４）。この際に返送されるユーザーの所有端末リストは、端末管理テーブル１２００のうち、同期端末リスト要求ｓ１．１３に含まれるユーザーＩＤと同期設定管理テーブル１２００のユーザーＩＤ１２０１が一致し、かつ、同期端末リスト要求ｓ１．１３に含まれる端末ＩＤと端末ＩＤ１２０２が一致しないレコードである。同期端末リスト応答ｓ１．１４を受けると、データ同期モジュール７００はユーザーの所有端末リストに含まれる端末のデータ同期アプリケーション（５２０ｅｔｃ）に対して、デバイストークン１５０５を使って、データＩＤ１３０１をｐｕｓｈ通知をする。（ｓ１．１５）。

【００４２】

その後、ｐｕｓｈ通知を受けた端末２２０のデータ同期アプリケーション５２０が、データ同期要求をデータ同期モジュール７００に送る。（ｓ１．１６）。そのデータ同期要求には、ユーザーＩＤ、端末ＩＤ、ｐｕｓｈ通知で受け取ったデータＩＤがパラメータとして含まれている。データ同期モジュール７００は、端末２２０のデータ同期アプリケーション５２０からデータ同期要求を受け取ると、データ更新内容を返却する。その際、データ同期モジュール７００は、データ更新内容を取得するために、同期データ管理テーブル１３００を参照し、データ同期要求に含まれるデータＩＤと同期データ管理テーブル１３００のデータＩＤ１３０１が一致するレコードを取得する。データ同期アプリケーション５２０は、受け取ったデータ更新内容を元に、追加・更新ファイルをデータ同期サーバー４００から取得し、端末２２０に反映する。またデータ更新内容を元に、端末２２０のファイルを削除する。

【００４３】

本実施形態によれば、ユーザーの所有端末リストを集約管理し、ユーザーが許可したサービスにのみユーザーの所有端末リストを提供できるようになる。

【実施例２】

【００４４】

次に、本発明を実施するための第２の実施形態について図面を用いて説明する。第１の実施例では、データ同期をする際に、ユーザーがどの端末に対してデータ同期されるかを確認できないという課題がある。ユーザーはどの端末にデータ同期するかの設定を購入時等において事前にしている。しかし、ユーザーがこの設定を忘れている可能性がある。また、ユーザーが端末を他のユーザーに譲渡した際に、端末のデータ同期設定の解除を忘れているケースもある。そのため、ユーザーがデータ同期をした際に、意図しない端末にデータ同期される可能性がある。そこで、第２の実施形態では、ユーザーがどの端末とデータ同期するかをユーザーが視認できるようにし、かつ、確認した端末に対してデータ同期することを目的とする。

【００４５】

図７は本発明の第２の実施の形態に係る、データ同期のシーケンスを示す図である。ここでの説明は前述の実施例の図５とほぼ同様なため、異なる部分のみを以下、説明する。有効なログイン情報が生成されている場合、認可モジュール６００は次の処理を行う（ｓ２．７）。認可モジュール６００は、データ同期する端末リストを取得する。データ同期する端末リストは、端末管理テーブル１２００に保存されている。データ同期する端末リストを取得するために、認可モジュール６００は、端末管理テーブル１２００の中から、ユーザーＩＤ１２０１とｓ２．７に含まれるユーザーＩＤが一致し、かつ、端末ＩＤ１２

０２が端末２００の端末ＩＤと一致しないレコードを取得する。認可モジュール６００はデータ同期アプリケーション５００に対して、データ同期する所有端末リストが含まれている応答を返す。データ同期アプリケーション５００は図８に示す認可確認画面１８０３を表示する（ｓ２．７）。

【００４６】

その際、認可確認画面１８０３には、ユーザーに対する権限委譲を確認する文言以外に、データ同期する所有端末リストが表示される。認可確認画面１８０３の画面例では、端末名を表示している。認可確認画面１８０３には、端末名以外に端末ＩＤを表示させてもよく、端末の識別情報を表示することでユーザーは同期が行われる対象の端末を認識することができる。この表示を行うことで、ユーザーは認可確認画面１８０３を閲覧しどの端末にデータ同期されるのかを視認できる。この後、図７のｓ２．８以降の処理を実施することで、ユーザーが視認した端末に対してデータが同期される。なお、認可確認画面１８０３では認可確認とデータ同期する端末リストを１つの画面に表示しているが、認可確認の表示画面とデータ同期する端末リストの表示画面のように２つに表示内容を分割してもよい。

【００４７】

本実施の第２の形態によれば、ユーザーは、認可確認するタイミングでデータ同期するユーザーの所有端末リストを確認できるようになる。

【実施例３】

【００４８】

次に、本発明を実施するための第３の実施形態について図面を用いて説明する。第２の実施例では、認可確認画面でデータ同期する端末リストを確認してからデータ同期されるまでの間に端末管理テーブル１２００にあるユーザーの所有端末が追加・変更・削除されることを想定した。その場合、認可確認画面で確認した端末にデータ同期がされなかったり、逆に認可確認画面で確認した端末以外の端末にデータ同期がされたりするという課題がある。そこで第３の実施形態では、認可確認画面でデータ同期する端末リストを確認してからデータ同期されるまでの間に端末管理テーブル１２００にあるユーザーの所有端末が追加・変更・削除されたとしても、認可確認画面で確認した端末に対して確実にデータ同期することを目的とする。

【００４９】

図９は本発明の第３の実施の形態に係る、同期端末保存テーブル１５００である。同期端末保存テーブル１５００は、認可トークンＩＤ１５０１、ユーザーＩＤ１５０２、端末ＩＤ１５０３、端末名１５０４、デバイストークンＩＤ１５０５からなる。同期端末保存テーブル１５００の利用方法は後述する。

【００５０】

図１０は本発明の第３の実施の形態に係る、データ同期のシーケンスを示す図である。ここでの説明は前述の実施例の図７とほぼ同様なため、異なる部分のみを以下、説明する。認可モジュール６００は、ｓ３．７で認可確認画面に表示したデータ同期する所有端末リストをトークンＩＤ１４０１と紐づけて同期端末保存テーブル１５００に保存する（ｓ３．１０）。トークンＩＤと関連付けて保存したデータ同期する所有端末リストをスナップショットと称する。スナップショットを同期端末保存テーブル１５００に保存する際に、過去に保存されているスナップショットがあれば削除してから、スナップショットを保存する。スナップショットついては後述する。認可モジュール６００は、データ同期モジュール７００にデータ同期する端末リストを返却する（ｓ３．１５）。この際に返却されるデータ同期する端末リストは、同期端末保存テーブル１５００のうち、ｓ３．１４で受け取ったトークンとトークンＩＤが一致するレコードである。

【００５１】

ここで、何故スナップショット使うのかを説明する。データ同期する端末リストは端末管理テーブル１２００に保存されている。もし認可確認（実施例３のｓ３．９）から端末にデータ同期される（実施例３のｓ３．１４）までの間に端末管理テーブル１２００のデ

ータが書き換えられると、認可確認画面で視認したデータ同期する端末リストとは異なる端末に対してデータ同期されてしまう。そのため、認可確認画面でユーザーが確認したときのデータ同期する端末リストをスナップショットとして、同期端末保存テーブル１５００に保存しておく。そして、データ同期の際に同期端末保存テーブル１５００からデータ同期する端末リストを取得するようにする。以降、図１０のｓ３．１６～ｓ３．１７の処理をもって、認可確認画面で確認した端末にのみデータ同期が行われる。

【００５２】

スナップショットを使うことで、仮に認可確認（実施例３のｓ３．９）から端末にデータ同期される（実施例３のｓ３．１４）までの間に端末管理テーブル１２００に登録されているユーザーの所有端末リストが変更されたとしても、認可確認画面で確認した端末に対して確実にデータ同期をすることができる。なお、スナップショットの保存方法は、ＤＢのテーブルに保存してもよいし、メモリ上に保存しておいてもよい。

【００５３】

本実施の第３の形態によれば、認可確認画面でデータ同期する端末リストを確認してからデータ同期が実行されるまでの間に、端末管理テーブル１２００にユーザーの所有端末が追加・変更・削除されたとしても、認可確認画面で確認した端末に対して確実にデータ同期をすることができる。

【実施例４】

【００５４】

次に、本発明を実施するための第４の形態について図面を用いて説明する。第３の実施例では、データ同期する端末リストに変更がない場合でも認可確認画面が表示されるため、データ同期をする度に、ユーザーは同じ内容の認可確認をしなければならないという課題がある。そこで第４の実施形態では、データ同期する端末リストに変更がない場合は、認可確認画面を表示せずに、データ同期することを目的とする。

【００５５】

図１１は本発明の第４の実施の形態に係る、データ同期のシーケンスを示す図である。ここでの説明は前述の実施例の図１０とほぼ同様なため、異なる部分のみを以下、説明する。認可モジュール６００は、データ同期する端末リストの変更があるかどうかを確認するために、次の処理を実行する（ｓ４．７）。

【００５６】

認可モジュール６００は、ｓ４．６のログイン情報からユーザーＩＤを取得する。認可モジュール６００は、現在のデータ同期する端末リストとして、端末管理テーブル１２００からユーザーＩＤ１２０１と取得したユーザーＩＤが一致するレコードを取得する。認可モジュール６００は、前回データ同期した端末リストのスナップショットを取得するため、同期端末保存テーブル１５００から取得したユーザーＩＤとユーザーＩＤ１５０２が一致するレコードを取得する。

【００５７】

認可モジュール６００は、現在のデータ同期する端末リストと前回データ同期した端末リストのスナップショットを比較して、データ同期する端末リストの変更があるかどうかを確認する。データ同期する端末リストに変更がない場合は、ｓ４．８～ｓ４．１１の処理をスキップする。以降、図１１のｓ４．１２～ｓ４．１８の処理をもって、データ同期する端末リストに変更がない場合に、認可確認画面を表示せずにデータ同期できる。

【００５８】

本実施の第４の形態によれば、ユーザーはデータ同期する端末リストに変化がなければ、認可確認画面を介した権限を移譲する指示を行わなくてよくなり、ユーザビリティーが向上する。

【実施例５】

【００５９】

次に、本発明を実施するための第５の形態について図面を用いて説明する。

【００６０】

第３の実施例では、認可確認画面に表示されるユーザーの所有端末リスト内の端末すべてにデータ同期がされる。ユーザーは端末毎にデータ同期するかしないかを選択したい場合には対応できないという課題がある。そこで第５の実施形態では、ユーザーが端末毎にデータ同期するかしないかを選択できるようにすることを目的とする。ここでの説明は前述の実施例の図１０とほぼ同様なため、異なる部分のみを以下、説明する。

【００６１】

ユーザーがログイン状態の場合、認可モジュール６００は図１３に示す認可確認画面１８０４をデータ同期アプリケーション５００のブラウザに表示する（ｓ５．７）。認可確認画面１８０４は、ユーザーに対する権限委譲を確認する文言以外に、データ同期する端末リストの選択欄を表示する。ユーザーは、認可確認画面１８０４でデータ同期する端末を指定して認可をする（ｓ５．８）。データ同期アプリケーション５００が、認可モジュール６００に認可確認の結果、データ同期する端末リストを送信する（ｓ５．９）。

【００６２】

認可モジュール６００は、ｓ５．９で受信したデータ同期する端末リストを、トークンＩＤ１３０５と紐づけて同期端末保存テーブル１５００に保存する（ｓ５．１０）。その際、もし同期端末保存テーブル１５００に過去に保存されているスナップショットがあれば削除する。以降、図１２のｓ５．１１～ｓ５．１７の処理をもって、ユーザーが認可確認画面で指定した端末に対してデータ同期がなされる。

【００６３】

本実施の第５の形態によれば、ユーザーは、認可確認画面でデータ同期する端末を指定できる。

【００６４】

（その他の実施例）

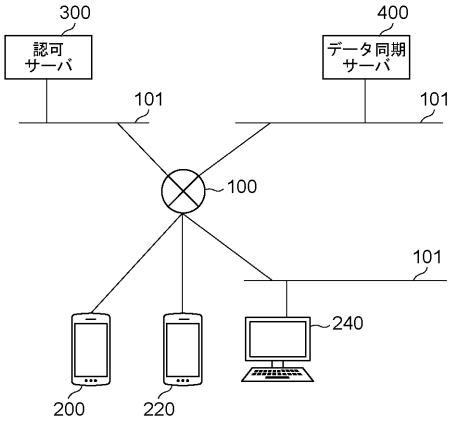
本発明は、以下の処理を実行することによっても実現される。即ち、上述した実施例の機能を実現するソフトウェア（プログラム）を、ネットワーク又は各種記憶媒体を介してシステム或いは装置に供給し、そのシステム或いは装置のコンピュータ（またはＣＰＵやＭＰＵ等）がプログラムを読み出して実行する処理である。

【符号の説明】

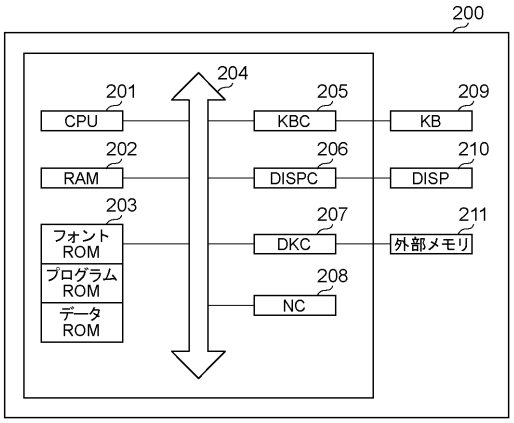
【００６５】

３００　認可サーバー
４００　データ同期モジュール
５００　データ同期アプリケーション
６００　認可モジュール
７００　データ同期モジュール
１１００　同期設定管理テーブル
１８０３　認可確認・同期端末表示画面

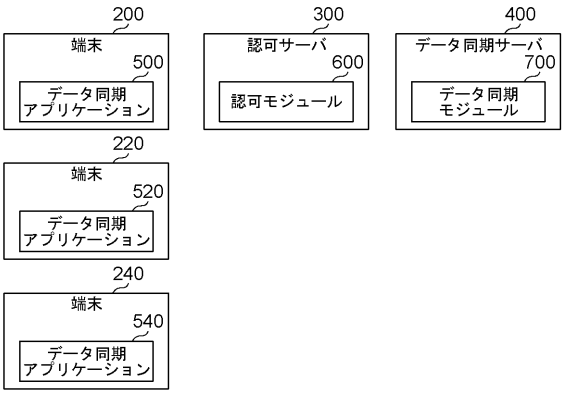
【図１】



【図２】



【図３】



【図４】

(a) 1000

ユーザ管理テーブル

1001 ユーザID	1002 パスワード
uid00000001	*****
uid00000002	******
uid00000003	*****

(b) 1100

クライアント管理テーブル

1101 クライアントID	1102 クライアント名	1103 パスワード	1104 リダイレクトURI
client00000001	データ同期サービス	*******	https://datasync.example.com

(c) 1200

端末管理テーブル

1201 ユーザID	1202 端末ID	1203 端末名	1204 デバイストークン
uid00000001	dev00000001	user1_dev1	APA91bHJDc0UZ…
uid00000001	dev00000002	user1_dev2	u7IJl6DfjlHTe…
uid00000001	dev00000003	user1_dev3	18ITPaRC4Go5…
uid00000002	dev00000004	user2_dev1	

(d) 1300

同期データ管理テーブル

1301 データID	1302 ユーザID	1303 更新区分	1304 ファイルパス	1305 ファイル名
dev00000001_sync0000001	uid00000001	追加	/test/	addfile.txt
dev00000001_sync0000001	uid00000001	更新	/test2/	updatefile.txt
dev00000001_sync0000001	uid00000001	削除	/test3/	delfile.txt

(e) 1400

認可トークン管理テーブル

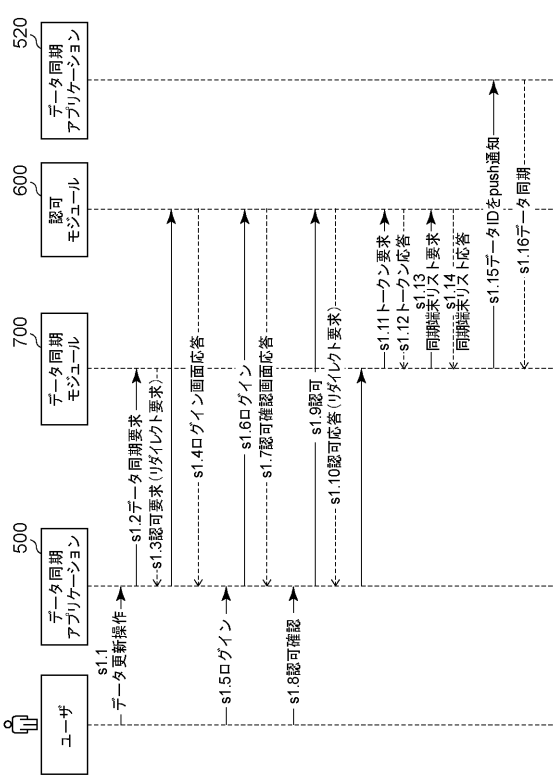
1401 認可トークンID	1402 トークン種別	1403 有効期限	1404 スコープID
AT_000000	認可コード	2014/04/30 11:00	端末リストの取得
AT_000001	認可トークン	2014/04/30 12:00	端末リストの取得
AT_000002	認可トークン	2014/04/30 13:00	端末リストの取得
AT_000003	認可トークン	2014/04/30 16:00	端末リストの取得

1405 リフレッシュトークンID	1406 リフレッシュ期限	1407 クライアントID	1408 ユーザID
		client00000001	uid00000001
RT_000001	2014/4/30 14:00	client00000001	uid00000001
RT_000002	2014/4/30 15:00	client00000001	uid00000001
RT_000003	2014/4/30 18:00	client00000001	uid00000002

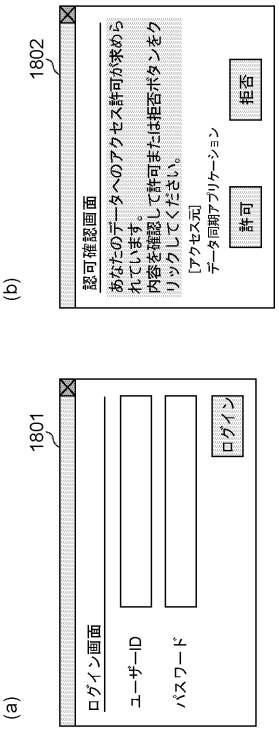
1409

リダイレクトURI
https://datasync.example.com

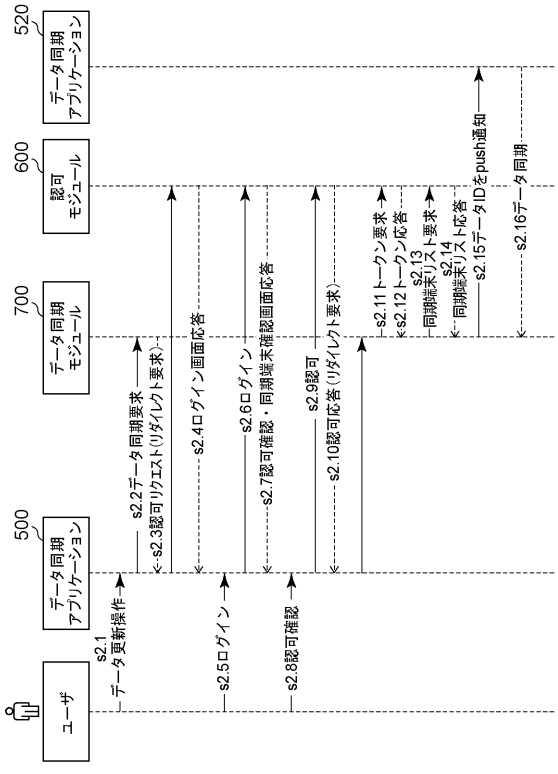
【図５】


ユーザ
データ同期アプリケーション
データ同期モジュール
認可モジュール
データ同期アプリケーション
s1.1 データ更新操作
s1.2データ同期要求
s1.3認可要求（リダイレクト要求）
s1.4ログイン画面応答
s1.5ログイン
s1.6ログイン
s1.7認可確認画面応答
s1.8認可確認
s1.9認可
s1.10認可応答（リダイレクト要求）
s1.11トークン要求
s1.12トークン応答
s1.13 同期端末リスト要求
s1.14 同期端末リスト応答
s1.15データIDをpush通知
s1.16データ同期

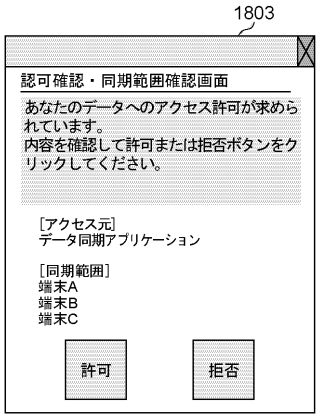
【図６】


(a)
1801
ログイン画面
ユーザーID
パスワード
ログイン
(b)
1802
認可確認画面
あなたのデータへのアクセス許可が求められています。
内容を確認して許可または拒否ボタンをクリックしてください。
[アクセス元]
データ同期アプリケーション
許可
拒否

【図７】


ユーザ
データ同期アプリケーション
データ同期モジュール
認可モジュール
データ同期アプリケーション
s2.1 データ更新操作
s2.2データ同期要求
s2.3認可リクエスト（リダイレクト要求）
s2.4ログイン画面応答
s2.5ログイン
s2.6ログイン
s2.7認可確認・同期端末確認画面応答
s2.8認可確認
s2.9認可
s2.10認可応答（リダイレクト要求）
s2.11トークン要求
s2.12トークン応答
s2.13 同期端末リスト要求
s2.14 同期端末リスト応答
s2.15データIDをpush通知
s2.16データ同期

【図８】


1803
認可確認・同期範囲確認画面
あなたのデータへのアクセス許可が求められています。
内容を確認して許可または拒否ボタンをクリックしてください。
[アクセス元]
データ同期アプリケーション
[同期範囲]
端末A
端末B
端末C
許可
拒否

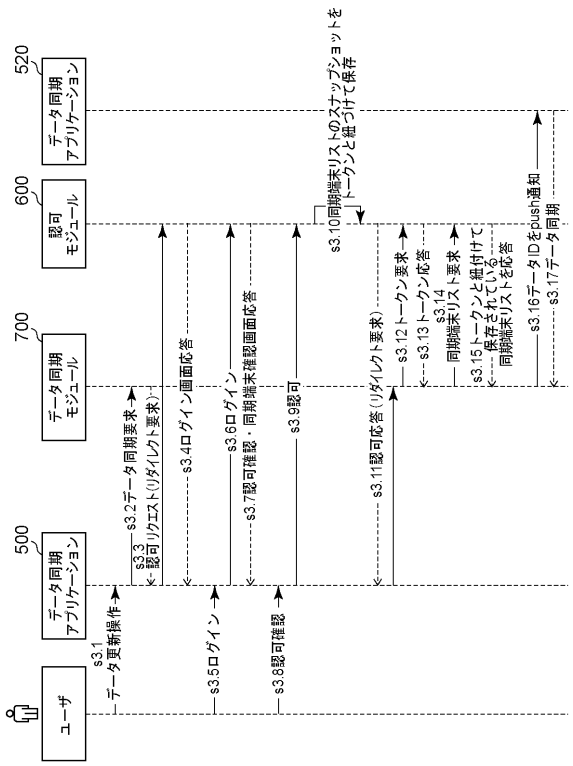
【図９】

1500

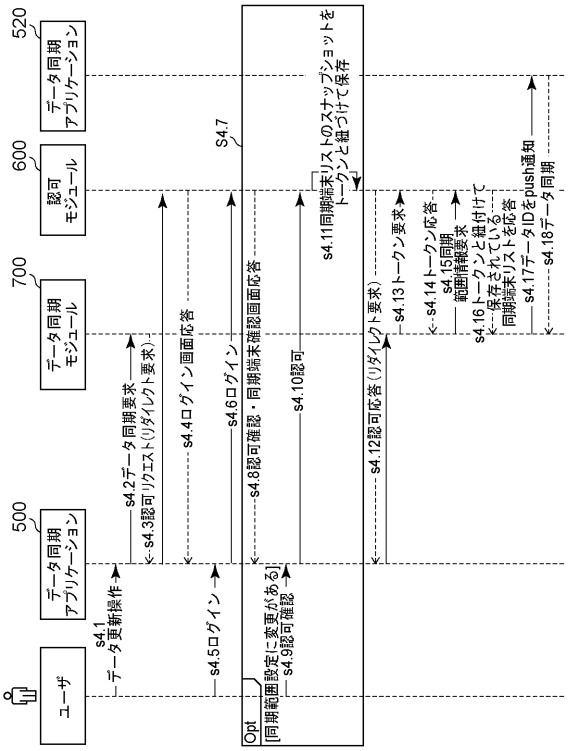
同期端末保存テーブル

1501 認可トークンID	1502 ユーザID	1503 端末ID	1504 端末名	1505 デバイストークン
AT_000001	uid00000001	dev00000002	user1_dev2	u7IJl6DfjHTe…
AT_000001	uid00000001	dev00000003	user1_dev3	18ITPaRC4Go5…

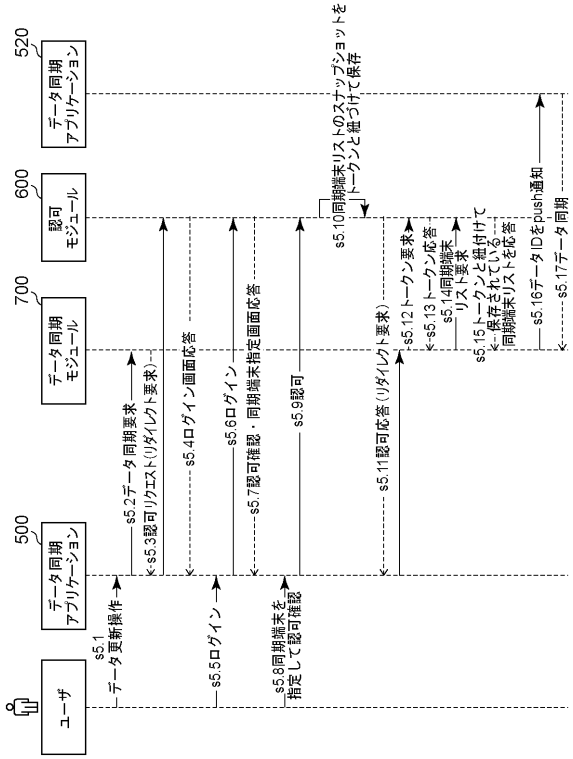
【図１０】



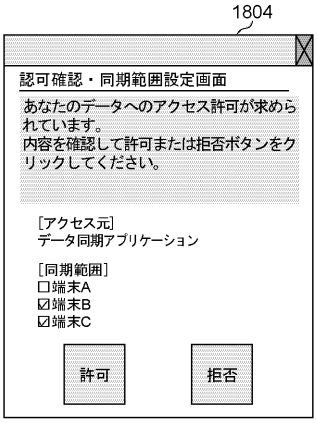
【図１１】



【図１２】



【図１３】


1804
認可確認・同期範囲設定画面
あなたのデータへのアクセス許可が求められています。
内容を確認して許可または拒否ボタンをクリックしてください。
[アクセス元]
データ同期アプリケーション
[同期範囲]
☐端末A
☑端末B
☑端末C
許可
拒否

フロントページの続き

(56)参考文献 特開２００５－１２２３７９（ＪＰ，Ａ）
国際公開第２０１３／１７５９０１（WO，Ａ１）
特開２００７－０４１９７６（ＪＰ，Ａ）
特開２０１３－０８８９０１（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　１２／００