(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6815744号
(P6815744)
(45)発行日　令和3年1月20日(2021.1.20)　(24)登録日　令和2年12月25日(2020.12.25)

(51)Int.Cl.　F I
G06F 21/62 (2013.01)　G06F 21/62 318

請求項の数 15 (全 19 頁)

(21)出願番号　特願2016-88411(P2016-88411)
(22)出願日　平成28年4月26日(2016.4.26)
(65)公開番号　特開2017-199145(P2017-199145A)
(43)公開日　平成29年11月2日(2017.11.2)
審査請求日　平成31年4月19日(2019.4.19)

(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　100090273
弁理士　國分　孝悦
(72)発明者　児玉　淳一
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　平井　誠

最終頁に続く

(54)【発明の名称】サーバ装置、システム、情報処理方法及びプログラム

(57)【特許請求の範囲】
【請求項１】
第一のクライアント装置を権限委譲の対象のクライアント装置と決定した際に、前記第一のクライアント装置と関連する第二のクライアント装置が存在する場合、前記第二のクライアント装置を更に前記権限委譲の対象のクライアント装置と決定する決定手段と、
前記決定手段により前記権限委譲の対象のクライアント装置と決定されたクライアント装置に対応する許可画面を生成する生成手段と、
前記生成手段により生成された前記許可画面を送信する第１の送信手段と、
を有し、
前記許可画面には、前記第一のクライアント装置に対して委譲する権限スコープと前記第二のクライアント装置に対して委譲する権限スコープとが含まれ、各権限スコープを許可するか否かをリソースごとに個別に選択可能なオブジェクトが含まれることを特徴とするサーバ装置。
【請求項２】
認可トークン取得要求をクライアント装置より受信する受信手段を更に有し、
前記決定手段は、前記受信手段により受信された前記認可トークン取得要求に含まれる前記クライアント装置のクライアントの情報に基づき前記第一のクライアント装置を権限委譲の対象のクライアント装置と決定した際に、前記第一のクライアント装置と関連する第二のクライアント装置が存在する場合、前記第二のクライアント装置を更に前記権限委譲の対象のクライアント装置と決定する請求項１記載のサーバ装置。

【請求項３】
前記第一のクライアント装置と関連する第二のクライアント装置が存在するか否かを判定する判定手段を更に有し、
前記判定手段により前記第一のクライアント装置と関連する第二のクライアント装置が存在すると判定された場合、前記決定手段は、前記第二のクライアント装置を更に前記権限委譲の対象のクライアント装置と決定する請求項１又は２記載のサーバ装置。
【請求項４】
前記判定手段は、前記第一のクライアント装置と同一のグループに属するクライアント装置が存在する場合、前記第一のクライアント装置と関連する第二のクライアント装置が存在すると判定する請求項３記載のサーバ装置。
【請求項５】
前記判定手段は、前記第一のクライアント装置の次に処理するクライアント装置がワークフロー情報で定義されている場合、前記第一のクライアント装置と関連する第二のクライアント装置が存在すると判定する請求項３記載のサーバ装置。
【請求項６】
前記判定手段は、前記第一のクライアント装置と同一のユーザのクライアント装置が存在する場合、前記第一のクライアント装置と関連する第二のクライアント装置が存在すると判定する請求項３記載のサーバ装置。
【請求項７】
前記第１の送信手段は、前記許可画面をユーザ端末装置に送信する請求項１乃至６何れか１項記載のサーバ装置。
【請求項８】
前記許可画面を介して許可指示を受け取った場合、前記第一のクライアント装置の認可トークンと前記第二のクライアント装置の認可トークンとを発行する発行手段と、
前記発行手段により発行された前記第一のクライアント装置の認可トークンと前記第二のクライアント装置の認可トークンとを送信する第２の送信手段と、
を更に有する請求項１乃至７何れか１項記載のサーバ装置。
【請求項９】
前記発行手段により発行された前記第一のクライアント装置の認可トークンと前記第二のクライアント装置の認可トークンとを関連付けて格納する格納手段を更に有する請求項８記載のサーバ装置。
【請求項１０】
認可トークンを削除する際に、前記格納手段により前記認可トークンと関連付けられて格納された認可トークンのうち送信待ちの状態の認可トークンが存在する場合、前記認可トークンも削除する削除手段を更に有する請求項９記載のサーバ装置。
【請求項１１】
認可トークンを削除する際に、前記格納手段により格納された認可トークンのうち削除する認可トークンに関するユーザの認可トークンが存在する場合、前記認可トークンも削除する削除手段を更に有する請求項９記載のサーバ装置。
【請求項１２】
クライアント装置と、サーバ装置と、ユーザ端末装置と、を含むシステムであって、
前記クライアント装置は、
前記サーバ装置に認可トークン取得要求を送信する第１の送信手段を有し、
前記サーバ装置は、
前記認可トークン取得要求を前記クライアント装置より受信する第１の受信手段と、
前記第１の受信手段により受信された前記認可トークン取得要求に含まれる前記クライアント装置のクライアント情報に基づき第一のクライアント装置を権限委譲の対象のクライアント装置と決定した際に、前記第一のクライアント装置と関連する第二のクライアント装置が存在する場合、前記第二のクライアント装置を更に前記権限委譲の対象のクライアント装置と決定する決定手段と、

前記決定手段により前記権限委譲の対象のクライアント装置と決定されたクライアント装置に対応する許可画面を生成する生成手段と、
前記生成手段により生成された前記許可画面を前記ユーザ端末装置に送信する第２の送信手段と、
を有し、
前記ユーザ端末装置は、
前記許可画面を前記サーバ装置より受信する第２の受信手段と、
前記第２の受信手段により受信された前記許可画面を表示する表示手段と、
を有し、
前記サーバ装置の前記生成手段が生成する前記許可画面には、前記第一のクライアント装置に対して委譲する権限スコープと前記第二のクライアント装置に対して委譲する権限スコープとが含まれ、各権限スコープを許可するか否かをリソースごとに個別に選択可能なオブジェクトが含まれることを特徴とするシステム。
【請求項１３】
サーバ装置が実行する情報処理方法であって、
第一のクライアント装置を権限委譲の対象のクライアント装置と決定した際に、前記第一のクライアント装置と関連する第二のクライアント装置が存在する場合、前記第二のクライアント装置を更に前記権限委譲の対象のクライアント装置と決定する決定ステップと、
前記決定ステップにより前記権限委譲の対象のクライアント装置と決定されたクライアント装置に対応する許可画面を生成する生成ステップと、
前記生成ステップにより生成された前記許可画面を送信する送信ステップと、
を含み、
前記許可画面には、前記第一のクライアント装置に対して委譲する権限スコープと前記第二のクライアント装置に対して委譲する権限スコープとが含まれ、各権限スコープを許可するか否かをリソースごとに個別に選択可能なオブジェクトが含まれることを特徴とする情報処理方法。
【請求項１４】
クライアント装置と、サーバ装置と、ユーザ端末装置と、を含むシステムにおける情報処理方法であって、
前記クライアント装置が、前記サーバ装置に認可トークン取得要求を送信する第１の送信ステップと、
前記サーバ装置が、前記認可トークン取得要求を前記クライアント装置より受信する第１の受信ステップと、
前記サーバ装置が、前記第１の受信ステップにより受信された前記認可トークン取得要求に含まれる前記クライアント装置のクライアント情報に基づき第一のクライアント装置を権限委譲の対象のクライアント装置と決定した際に、前記第一のクライアント装置と関連する第二のクライアント装置が存在する場合、前記第二のクライアント装置を更に前記権限委譲の対象のクライアント装置と決定する決定ステップと、
前記サーバ装置が、前記決定ステップにより前記権限委譲の対象のクライアント装置と決定されたクライアント装置に対応する許可画面を生成する生成ステップと、
前記サーバ装置が、前記生成ステップにより生成された前記許可画面を前記ユーザ端末装置に送信する第２の送信ステップと、
前記ユーザ端末装置が、前記許可画面を前記サーバ装置より受信する第２の受信ステップと、
前記ユーザ端末装置が、前記第２の受信ステップにより受信された前記許可画面を表示する表示ステップと、
を含み、
前記サーバ装置が前記生成ステップで生成する前記許可画面には、前記第一のクライアント装置に対して委譲する権限スコープと前記第二のクライアント装置に対して委譲する

権限スコープとが含まれ、各権限スコープを許可するか否かをリソースごとに個別に選択可能なオブジェクトが含まれることを特徴とする情報処理方法。

【請求項１５】

コンピュータを、請求項１乃至１１何れか１項記載のサーバ装置の各手段として機能させるためのプログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、権限を委譲する際のユーザの操作負荷を軽減するサーバ装置、システム、情報処理方法及びプログラムに関する。

【背景技術】

【０００２】

近年、サーバ装置が提供する様々な機能を、ユーザが使用するユーザ端末からネットワーク経由で利用可能にするサービスが広く展開されている。このようなサービスでは、多くの場合、サービスが保有するリソースへのアクセスをユーザ端末から要求された際に、ユーザＩＤ及びパスワード等の認証情報を用いてユーザを認証することを要求する。ユーザはユーザ端末に認証情報を入力する。認証が成功するとサービスから認証トークンが発行される。ユーザ端末は発行された認証トークンを付加して、サービスに処理の実行を要求する。サービスは、認証トークンの示すユーザが有する権限の範囲内で処理の実行を許可する。

また、認証されたユーザが、自身が有する権限をクライアント１０３に委譲することで、クライアントが権限を獲得して処理を実行するようなことも行われている。ここで、クライアントとは、サービスが保有するリソースを使用するアプリケーションが動作するサーバ装置やモバイル端末等である。クライアントは、権限を委譲される対象としてサービスに登録される。権限を委譲する方法として、例えば、ＯＡｕｔｈ２．０（非特許文献１）等が広く用いられている。この方法においては、認証されたユーザに、クライアントに対して指定された権限を許可するか否かの判定を依頼する許可画面が提示される。ユーザが許可を選択すると、クライアントにリソースにアクセスするための権限を示す認可トークンが発行される。そのため、ユーザは自分自身の認証情報をクライアントに入力することなく、リソースにアクセスするための権限を委譲することができる。

【０００３】

ここで、ＯＡｕｔｈ２．０のような権限の委譲では、ユーザに対して、どのクライアントにどの権限を許可するかの判定を、クライアントが権限を必要としたタイミングでその都度、依頼することで、リソースのセキュリティを確保している。しかし、クライアントが複数存在する場合、ユーザはクライアントごとに許可を行うという煩雑な操作が必要となり、操作性を損なうことが問題となる。

このような問題を解決する手段として、ユーザの許可操作を簡易化する方法が開示されている。

例えば、特許文献１では、Ｗｅｂ情報の所有者であるユーザが設定したポリシー情報を認可サーバに事前に登録し、被譲渡者が使用するクライアントからアクセス要求が発生した場合に、ポリシー情報をもとに認可トークンを発行する。これによって、ユーザが事前に設定した条件で、クライアントに権限を委譲でき、セキュリティを高めつつユーザの操作負荷を軽減できる。

また、特許文献２では、まず、ユーザの許可操作によって、デバイス装置に第一の認可トークンを発行する。次に、第一の認可トークンを使うことによって、デバイス装置にインストールされている各アプリケーションにユーザの許可操作なしで第二の認可トークンを発行する。これによって、デバイス装置にインストールされている複数のアプリケーションが権限委譲の対象となる場合に、ユーザの操作負荷を軽減できる。

これらの技術によって、クライアントが複数存在する場合に、ユーザの許可操作の負荷を軽減できる。

【先行技術文献】
【特許文献】
【０００４】
【特許文献１】特開２０１５－２０１０９８号公報
【特許文献２】特開２０１４－６７３７９号公報
【非特許文献】
【０００５】
【非特許文献１】Ｔｈｅ　ＯＡｕｔｈ　２．０　Ａｕｔｈｏｒｉｚａｔｉｏｎ　Ｆｒａｍｅｗｏｒｋ（ｈｔｔｐ：／／ｔｏｏｌｓ．ｉｅｔｆ．ｏｒｇ／ｈｔｍｌ／ｒｆｃ６７４９）
【発明の概要】
【発明が解決しようとする課題】
【０００６】
しかしながら、事前に登録されたポリシー情報に基づいて認可トークンを発行する方法では、ポリシー情報に変更が必要となった場合に対応することが難しい。ポリシー情報に変更が必要な場合とは、例えば、権限委譲の対象となるクライアントが変更された場合や、クライアントに委譲すべき権限の内容が変更された場合等である。
また、デバイス装置に発行された認可トークンに基づいて各アプリケーションに認可トークンを発行する方法では、権限委譲の対象となるアプリケーションごとの権限をユーザに提示して許可の判定を依頼することができない。そのため、権限委譲の対象に応じて適切な権限の許可を判定することが難しい。
本発明は、事前にポリシー情報を登録することなく、権限委譲の対象ごとの権限を考慮したうえで、権限を委譲する際のユーザの操作負荷を軽減する技術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】
【０００７】
本発明のサーバ装置は、第一のクライアント装置を権限委譲の対象のクライアント装置と決定した際に、前記第一のクライアント装置と関連する第二のクライアント装置が存在する場合、前記第二のクライアント装置を更に前記権限委譲の対象のクライアント装置と決定する決定手段と、前記決定手段により前記権限委譲の対象のクライアント装置と決定されたクライアント装置に対応する許可画面を生成する生成手段と、前記生成手段により生成された前記許可画面を送信する第１の送信手段と、を有し、前記許可画面には、前記第一のクライアント装置に対して委譲する権限スコープと前記第二のクライアント装置に対して委譲する権限スコープとが含まれ、各権限スコープを許可するか否かをリソースごとに個別に選択可能なオブジェクトが含まれることを特徴とする。
【発明の効果】
【０００８】
本発明によれば、事前にポリシー情報を登録することなく、権限委譲の対象ごとの権限を考慮したうえで、権限を委譲する際のユーザの操作負荷を軽減する技術を提供することができる。
【図面の簡単な説明】
【０００９】
【図１】認可システムのシステム構成の一例を示す図である。
【図２】認可サーバのハードウェア構成の一例を示す図である。
【図３】認可システムの機能構成の一例を示す図である。
【図４】ユーザやグループの情報の一例を示す図である。
【図５】認証トークン情報や認可トークン情報の一例を示す図である。
【図６】認可システムの情報処理の一例を示すフローチャートである。
【図７】認可トークンの取得処理の一例を示すフローチャートである。
【図８】メッセージの一例を示す図である。

【図９】認証画面や許可画面の一例を示す図である。
【図１０】許可画面の生成処理の一例を示すフローチャートである。
【図１１】認可トークンの生成処理の一例を示すフローチャートである。
【図１２】認可トークンの検証処理の一例を示すフローチャートである。
【図１３】認可トークンの破棄処理の一例を示すフローチャートである。
【図１４】許可画面の一例を示す図である。
【図１５】ワークフロー情報や登録クライアント情報の一例を示す図である。
【発明を実施するための形態】
【００１０】
以下、本発明の実施形態について図面に基づいて説明する。
【００１１】
＜実施形態１＞
まず、本実施形態に係る認可システムの構成例について、図１を用いて説明する。
認可システムは、認可サーバ１０１、リソースサーバ１０２、クライアント１０３、ユーザ端末１０４から構成される。認可サーバ１０１、リソースサーバ１０２、クライアント１０３、ユーザ端末１０４は、ネットワーク１０５を介して互いに通信が可能である。ネットワーク１０５は、ＬＡＮ等の同一のネットワークとして接続されていてもよいし、インターネット等の外部ネットワークとして接続されていてもよいし、それらの混合であってもよい。また、認可サーバ１０１、リソースサーバ１０２、クライアント１０３は、それぞれ複数の台数、認可システムに含まれてもよい。
認可サーバ１０１は、リソースサーバ１０２が保有するリソースをユーザやクライアント１０３がアクセスするための権限を管理する。認可サーバ１０１は、リソースサーバ１０２にリソースを保有するユーザのユーザ情報を保有している。また、認可サーバ１０１は、リソースサーバ１０２が保有しているリソースにアクセスするクライアント１０３のクライアント情報を保有している。更に、認可サーバ１０１は、クライアント１０３からの要求に応じて認可トークンを発行したり、リソースサーバ１０２からの要求に応じて認可トークンの有効性を検証したりする。ここで、認可トークンとは、認証されたユーザに対して与えられる権限情報、又は認証されたユーザがクライアント１０３に対して委譲した権限情報が記述されたデータのことである。認可トークンは、例えば、ＯＡｕｔｈ２．０におけるアクセストークンである。クライアント１０３は、リソースサーバ１０２にリソースへのアクセスを要求する際に、認可トークンを取得してリソースアクセス要求と共に送信する。リソースサーバ１０２は、受信した認可トークンの有効性を検証し、要求の可否を決定する。
リソースサーバ１０２は、ユーザのリソースを保有する。ここで、リソースとは、Ｗｅｂでアクセス可能なあらゆるデータや処理のことである。データとしては、ユーザのパーソナルデータ、画像データ、文書データ等、様々なものがある。また、リソースサーバ１０２は、クライアント１０３からのリソースアクセス要求に応じてリソースを提供する。
クライアント１０３は、ユーザ端末１０４からの処理要求に応じて、各種処理を行うアプリケーションが動作するサーバやモバイル端末等である。クライアント１０３は、権限委譲の対象として認可サーバ１０１に登録される。クライアント１０３は、処理を実行する際には、リソースサーバ１０２に処理に必要なリソースへのアクセスを要求する。また、クライアント１０３は、リソースサーバ１０２にリソースへのアクセスを要求するために、認可サーバ１０１に認可トークンの取得を要求する。
ユーザ端末１０４は、ユーザが操作する端末であり、パーソナルコンピュータやモバイル端末等である。
【００１２】
次に、本実施形態に係る認可システムを構成する、認可サーバ１０１のハードウェア構成例について、図２を用いて説明する。なお、リソースサーバ１０２、クライアント１０３、ユーザ端末１０４についても同様の構成である。
認可サーバ１０１は、ＣＰＵ２０１、ＲＡＭ２０２、ＲＯＭ２０３、ネットワークイン

タフェース２０４、外部記憶装置２０５、表示装置２０６、入力装置２０７を少なくとも備えている。

ＣＰＵ２０１は、認可サーバ１０１を構成する各部の動作制御を行うと共に、認可サーバ１０１が行うものとして後述する各種の処理を実行する主体となる。

ＲＡＭ２０２は、データや制御情報を一時的に格納するメモリであり、ＣＰＵ２０１が各種の処理を実行する際に用いるワークエリアとなる。

ＲＯＭ２０３には、認可サーバ１０１の固定の動作パラメータやプログラム等が格納される。

ネットワークインタフェース２０４は、ネットワーク１０５に接続して通信するための機能を提供するものである。認可サーバ１０１は、このネットワークインタフェース２０４によって、外部装置とデータの送受信を行うことができる。

外部記憶装置２０５は、データを記憶する装置であり、データの読み書きを行うためのＩ／Ｏコマンドを受け付けるインタフェースを持つ。外部記憶装置２０５は、ハードディスクドライブ（ＨＤＤ）、ソリッドステートドライブ（ＳＳＤ）、光ディスクドライブ、半導体記憶装置又はその他の記憶装置であってもよい。外部記憶装置２０５には、プログラムやデータが格納されている。

表示装置２０６は、例えば、ＬＣＤ（Ｌｉｑｕｉｄ　Ｃｒｙｓｔａｌ　Ｄｉｓｐｌａｙ）等であり、ユーザに必要な情報を表示する。

入力装置２０７は、例えば、キーボードやマウス、タッチパネル等であり、ユーザから必要な入力を受け付ける。

【００１３】

認可サーバ１０１のＣＰＵ２０１が、認可サーバ１０１のＲＯＭ２０３又は外部記憶装置２０５に記憶されているプログラムに基づき処理を実行することによって、後述する図３の認可サーバ１０１の機能構成が実現される。また、認可サーバ１０１のＣＰＵ２０１が、認可サーバ１０１のＲＯＭ２０３又は外部記憶装置２０５に記憶されているプログラムに基づき処理を実行することによって、後述する図７、図１２のうち認可サーバ１０１のフローチャートの処理が実現される。また、認可サーバ１０１のＣＰＵ２０１が、認可サーバ１０１のＲＯＭ２０３又は外部記憶装置２０５に記憶されているプログラムに基づき処理を実行することによって、後述する図１０、図１１、図１３のフローチャートの処理が実現される。

同様にリソースサーバ１０２のＣＰＵ２０１が、リソースサーバ１０２のＲＯＭ２０３又は外部記憶装置２０５に記憶されているプログラムに基づき処理を実行することによって、後述する図３のリソースサーバ１０２の機能構成が実現される。またリソースサーバ１０２のＣＰＵ２０１が、リソースサーバ１０２のＲＯＭ２０３又は外部記憶装置２０５に記憶されているプログラムに基づき処理を実行することによって、後述する図６、図１２のうちリソースサーバ１０２のフローチャートの処理が実現される。

同様にユーザ端末１０４のＣＰＵ２０１が、ユーザ端末１０４のＲＯＭ２０３又は外部記憶装置２０５に記憶されているプログラムに基づき処理を実行することによって、後述する図３のユーザ端末１０４の機能構成が実現される。またユーザ端末１０４のＣＰＵ２０１が、ユーザ端末１０４のＲＯＭ２０３又は外部記憶装置２０５に記憶されているプログラムに基づき処理を実行することによって、後述する図６、図７のうちユーザ端末１０４のフローチャートの処理が実現される。

同様にクライアント１０３のＣＰＵ２０１が、クライアント１０３のＲＯＭ２０３又は外部記憶装置２０５に記憶されているプログラムに基づき処理を実行することによって、後述する図３のクライアント１０３の機能構成が実現される。またクライアント１０３のＣＰＵ２０１が、クライアント１０３のＲＯＭ２０３又は外部記憶装置２０５に記憶されているプログラムに基づき処理を実行することによって、後述する図６、図７のうちクライアント１０３のフローチャートの処理が実現される。

【００１４】

次に、本実施形態に係る認可システムの機能構成例について、図３を用いて説明する。

認可サーバ１０１は、認証部３０２、認可部３０７、ユーザ情報格納部３０１、認証トークン格納部３０５、クライアント情報格納部３０６、認可トークン格納部３１１を備える。認証部３０２は、認証トークン発行部３０３、認証トークン検証部３０４を備える。認可部３０７は、認可トークン発行部３０８、認可トークン検証部３０９、認可トークン破棄部３１０を備える。

ユーザ情報格納部３０１には、ユーザを認証するためのユーザ情報が格納されている。

ユーザ情報格納部３０１に格納されているユーザ情報の一例を図４(ａ)に示す。ユーザＩＤ４０１に関連付けて、パスワード４０２が格納されている。ユーザＩＤ４０１は、リソースサーバ１０２にリソースを保有するユーザを一意に識別するＩＤである。パスワード４０２は、ユーザが本人であることを検証するための文字列である。ここでは、ユーザを認証するためにパスワード４０２を用いているが、他の認証情報を用いてもよい。

認証トークン発行部３０３は、外部装置から認証トークン発行要求を受信した際に、ユーザ情報格納部３０１に格納されているユーザ情報に基づいてユーザを認証し、認証トークンを発行する。発行された認証トークンは認証トークン格納部３０５に格納される。

認証トークン格納部３０５に格納されている認証トークン情報の一例を図５（ａ）に示す。認証トークンＩＤ５０１に関連付けて、ユーザＩＤ５０２と有効期限５０３とが格納されている。ユーザＩＤ５０２は、認証されたユーザを表している。有効期限５０３は、認証トークンの有効期限であり、期限を過ぎた認証トークンは無効となる。

認証トークン検証部３０４は、認証トークン格納部３０５に格納されている認証トークン情報に基づいて認証トークンの正当性を検証する。

【００１５】

クライアント情報格納部３０６には、クライアント１０３が権限を委譲されるために必要なクライアント情報及びクライアント１０３のグループ情報が格納されている。

クライアント情報格納部３０６に格納されているクライアント情報の一例を図４（ｂ）に示す。クライアントＩＤ４０３に関連付けて、パスワード４０４、権限スコープ４０５、デフォルトグループ４０６が格納されている。クライアントＩＤ４０３は、クライアント１０３を一意に識別するＩＤである。パスワード４０４は、クライアント１０３を認証するための文字列である。ここでは、クライアント１０３を認証するための情報としてパスワードを用いているが、他の認証情報を用いてもよい。権限スコープ４０５は、クライアント１０３が有する権限の適用範囲を表している。デフォルトグループ４０６は、クライアント１０３が所属するグループの初期設定値を表している。

クライアント情報格納部３０６に格納されているクライアント１０３のグループ情報の一例を図４（ｃ）に示す。グループＩＤ４０７に関連付けて、所属クライアント４０８が格納されている。グループＩＤ４０７は、クライアント１０３のグループを一意に識別するＩＤである。所属クライアント４０８は、そのグループに所属しているクライアント１０３のクライアントＩＤを表している。

【００１６】

認可トークン発行部３０８は、外部装置から認可トークン発行要求を受信した際に、認証トークン発行部３０３によって認証されたユーザによる許可に基づいて、認可トークンを行う。この際、認可トークン発行部３０８は、クライアント情報格納部３０６に格納されているクライアント情報に基づいて権限委譲の対象となるクライアント１０３の有効性を検証する。発行された認可トークンは、認可トークン格納部３１１に格納される。認可トークン格納部３１１に格納されている認可トークン情報の一例を図５（ｂ）に示す。認可トークンＩＤ５０４に関連付けて、クライアントＩＤ５０５、権限スコープ５０６、有効期限５０７、関連認証トークンＩＤ５０８、関連認可トークンＩＤ５０９が格納されている。クライアントＩＤ５０５は、権限が委譲された、即ち認可トークンが発行されたクライアント１０３を表している。権限スコープ５０６は、認可トークンが有する権限の適用範囲を表している。有効期限５０７は、認可トークンの有効期限であり、期限を過ぎた認可トークンは無効となる。関連認証トークンＩＤ５０８は、権限の委譲を許可したユーザの認証トークンを表している。関連認可トークンＩＤ５０９は、その認可トークンと同

時に生成された認可トークンを表している。送信状態５１０は、その認可トークンが対象となるクライアント１０３に送信済みであるか否かを表している。

認可トークン検証部３０９は、外部装置から認可トークン検証要求を受信した際に、認可トークン格納部３１１に格納されている認可トークン情報に基づいて認可トークンの正当性を検証する。

認可トークン破棄部３１０は、外部装置から認可トークン破棄要求を受信した際に、認可トークン格納部３１１に格納されている認可トークンを破棄する。

【００１７】

リソースサーバ１０２は、リソース提供部３１２とリソース格納部３１３とを備える。

リソース格納部３１３には、ユーザが保有するリソースが格納されている。リソース提供部３１２は、外部装置からリソース取得要求を受信した際に、リソース格納部３１３に格納されているリソースを提供する。このとき、リソース提供部３１２は、リソース取得要求に付加されている認可トークンが、リソースに対する権限を保有しているか否かを、認可サーバの認可トークン検証部３０９に問い合わせて検証する。

クライアント１０３は、要求処理部３１４を備える。

要求処理部３１４は、ユーザ端末からの処理要求に応じて、リソースサーバ１０２にリソース提供要求を送信して、処理に必要なリソースを取得する。要求処理部３１４は、リソース提供要求には、認可サーバの認可トークン発行部３０８から取得した認可トークンを付与する。

ユーザ端末は、ユーザエージェント３１５を備える。

ユーザエージェント３１５は、Ｗｅｂブラウザ等、ユーザがＷｅｂサイトにアクセスするための機能を提供する。

【００１８】

次に、本実施形態に係る認可システムの動作について説明し、併せて、本実施形態に係る認可方法について説明する。

図６は、本実施形態に係る認可システムの情報処理の一例を示すフローチャートである。なお、本実施形態では、クライアント１０３としてウェブアプリケーションを提供するサーバを想定して記載するが、クライアント１０３はモバイル端末のアプリケーション等、他の形態であってもよい。

まず、ユーザ端末のユーザエージェント３１５は、ユーザ操作に応じて、クライアント１０３に対する処理要求を受け取ると、クライアント１０３に処理要求を送信する（Ｓ６０１）。クライアント１０３の要求処理部３１４は、処理要求を受信する（Ｓ６０２）。要求処理部３１４は、処理の実行にリソースサーバ１０２が保有するリソースが必要な場合には、認可サーバから認可トークンを取得する（Ｓ６０３）。認可トークンの取得処理については、図７を用いて後述する。認可トークンが取得できた場合、要求処理部３１４は、認可トークンを付加したリソース取得要求をリソースサーバ１０２に送信する（Ｓ６０４）。リソースサーバ１０２のリソース提供部３１２は、リソース取得要求を受信する（Ｓ６０５）。リソース提供部３１２は、リソース提供要求に付加されている認可トークンが有効なものであるか否かを検証する（Ｓ６０５）。認可トークンの検証処理については、図１２を用いて後述する。認可トークンが有効なものである場合、リソース提供部３１２は、リソースをクライアント１０３に送信する（Ｓ６０８）。クライアント１０３の要求処理部３１４は、送信されたリソースを受信する（Ｓ６０８）。要求処理部３１４は、受信したリソースを使用して処理要求に対応した処理を実行し、処理結果をユーザ端末に送信する（Ｓ６０９）。ユーザ端末のユーザエージェント３１５は、処理結果を受信し、ユーザ端末の表示装置２０６に表示することでユーザに提示する（Ｓ６１０）。

【００１９】

次に、本実施形態に係る認可システムで行われる認可トークンの取得処理について図７を用いて説明する。なお、図７では、ＯＡｕｔｈ２．０のプロトコルに基づいた処理フローとなっているが、同様の処理フローを備えた他のプロトコルであってもよい。

まず、クライアント１０３の要求処理部３１４は、認可サーバ１０１に認可トークン取

得要求を送信する（Ｓ７０１）。認可トークン取得要求は、実際には、ユーザ端末を経由してクライアント１０３から認可サーバに送信される。

認可トークン取得要求のメッセージの一例を図８（ａ）に示す。図８（ａ）は、ＨＴＴＰ（Ｈｙｐｅｒｔｅｘｔ Ｔｒａｎｓｆｅｒ Ｐｒｏｔｏｃｏｌ）のプロトコルに従った構文によってメッセージが形成されている。ＵＲＬ（Ｕｎｉｆｏｒｍ Ｒｅｓｏｕｒｃｅ Ｌｏｃａｔｏｒ）部１２０１に要求の宛先が指定され、末尾にＵＲＬパラメータとして、クライアント１０３のクライアントＩＤが指定されている。これによって、認可サーバ１０１では、どのクライアント１０３が認可トークン取得要求を行っているのかを特定することができる。また、ＵＲＬパラメータとして、クライアントのグループＩＤが指定されている。これによって、認可サーバでは、どのグループのクライアント１０３に対して一括して許可判定を依頼し、認可トークンを生成するかを特定することができる。ヘッダ部１２０２には、許可判定の依頼を行うユーザの認証情報が指定されている。

認可サーバ１０１の認可トークン発行部３０８は、クライアント１０３から送信された認可トークン取得要求を受信する（Ｓ７０２）。認可トークン発行部３０８は、認可トークンを発行するために許可を行うユーザが認証済みか否かを判定する（Ｓ７０３）。認可トークン発行部３０８は、認可トークン取得要求に認証トークンが付加されているか、付加されている認証トークンが有効かによって認証済みか否かを判定する。認証済みでないと判定した場合（Ｓ７０３においてＮｏ）、認可トークン発行部３０８は、ユーザに認証を要求するための認証画面をユーザ端末に送信する（Ｓ７０４）。

【００２０】

認証画面の一例を図９（ａ）に示す。認証画面１１０１は、ユーザの認証情報（例えば、ユーザＩＤ及びパスワード）を入力する領域１１０２と、入力した認証情報を確定し、認可サーバ１０１に送信するためのボタン１１０３とから構成されている。

ユーザ端末のユーザエージェント３１５は、認可サーバ１０１から送信された認証画面を受信し、表示装置２０６に表示する（Ｓ７０５）。ユーザエージェント３１５は、入力装置２０７を介してユーザによって入力された認証情報を受け取ると（Ｓ７０６）、認証情報を認可サーバ１０１に送信する。認可サーバ１０１の認証トークン発行部３０３は、認証情報を受信する（Ｓ７０７）。認証トークン発行部３０３は、受信された認証情報で認証が成功すると、認証トークンを発行する（Ｓ７０８）。認証トークン発行部３０３は、発行した認証トークンを認可トークン取得要求に付加して、認可トークン発行部３０８に渡す。すると、認可トークン発行部３０８は、認証済みのユーザに許可判定を依頼するための許可画面を生成する（Ｓ７１０）。許可画面の生成処理については、図１０を用いて後述する。認可トークン発行部３０８は、生成した許可画面をユーザ端末に送信する（Ｓ７１１）。一方、認証済みであると判定した場合（Ｓ７０３においてＹｅｓ）、認可トークン発行部３０８は、認証トークンに関連付けられている送信待ちの認可トークンが存在するか否かを検証する（Ｓ７０９）。送信待ちの認可トークンが存在しない場合（Ｓ７０９においてＮｏ）、認可トークン発行部３０８は、Ｓ７１０にて同様に許可画面を生成する。ユーザ端末のユーザエージェント３１５は、認可サーバ１０１から送信された許可画面を受信し、表示装置２０６に表示する（Ｓ７１２）。ユーザエージェント３１５は、入力装置２０７を介したユーザ操作に応じて、許可指示の入力を受け付けると、許可判定情報を認可サーバ１０１に送信する（Ｓ７１３）。認可サーバ１０１の認可トークン発行部３０８は、許可判定情報を受信する（Ｓ７１４）。認可トークン発行部３０８は、許可判定情報に基づいて、認可トークンを生成する（Ｓ７１５）。認可トークンの生成処理については、図１１を用いて後述する。

【００２１】

認可トークン発行部３０８は、生成された認可トークンのうち、認可トークン取得要求で権限委譲の対象となっているクライアント１０３の認可トークンをクライアント１０３に送信し、送信状態を"送信済み"にセットする（Ｓ７１６）。一方、送信待ちの認可トークンが存在すると判定した場合（Ｓ７０９においてＹｅｓ）、認可トークン発行部３０８は、Ｓ７１６においてその認可トークンを送信し、送信状態を"送信済み"にセットする。

クライアント１０３の要求処理部３１４は、認可トークンを受信する（Ｓ７１７）。Ｓ７１６からＳ７１７までの処理は、実際には、まず一時的認可情報が含まれる認可結果がユーザ端末を経由してクライアント１０３に送信される。そして、クライアント１０３は、一時的認可情報を使って認可サーバから認可トークンを取得する。

認可結果のメッセージの一例を図８（ｂ）に示す。図８（ｂ）には、ＨＴＴＰのレスポンスとしてメッセージが形成されている。ステータス部１２０３には、認可要求の結果を示すステータスがセットされている。また、ヘッダ部１２０４には、一時的認可情報が含まれている。一時的認可情報は、クライアント１０３が認可トークンを取得するために使用される。

【００２２】

一時的認可情報を使った認可トークン取得要求のメッセージの一例を図８（ｃ）に示す。図８（ｃ）は、ＨＴＴＰのプロトコルに従った構文によってメッセージが形成されている。ＵＲＬ部１２０５には、要求の宛先が指定されている。ヘッダ部１２０６には、クライアント１０３の認証情報が指定されている。これによって、認可サーバ１０１では、認証が成功したクライアント１０３に対してのみ、要求の実行を許可することができる。ボディ部１２０７には、一時的認可情報が指定されている。

クライアント１０３に送信される認可トークンのメッセージの一例を図８（ｄ）に示す。図８（ｄ）は、ＨＴＴＰのレスポンスとして、メッセージが形成されている。ステータス部１２０８には、認可トークン取得要求が成功したことを示すステータスがセットされている。ボディ部１２０９には、認可トークンと、認可トークンの有効期限等がセットされている。

このように、本実施形態に係る認可トークンの取得処理では、認可サーバ１０１は、認証されたユーザに許可判定を依頼し、ユーザの許可判定に基づいて、譲渡された権限を表す認可トークンを生成し、クライアント１０３に送信する。また、認可サーバ１０１は、事前に認可トークンが生成済みの場合には、ユーザに許可判定の依頼をすることなく認可トークンをクライアント１０３に送信する。

【００２３】

次に、本実施形態に係る認可サーバが行う許可画面の生成処理について、同処理のフローチャートを示す図１０を用いて説明する。

まず、認可トークン発行部３０８は、認可トークン取得要求で指定されたクライアントを第一のクライアントとして抽出する（Ｓ８０１）。認可トークン発行部３０８は、第一のクライアントが正当であるか否かをクライアント情報格納部３０６に格納されているクライアント情報を使用して検証する（Ｓ８０２）。認可トークン発行部３０８は、正当なクライアントである場合、第一のクライアントを権限委譲の対象として判定する（Ｓ８０３）。次に、認可トークン発行部３０８は、第一のクライアントと同一のグループに属する第二のクライアントが存在するか否かを、クライアント情報格納部３０６に格納されているクライアントのグループ情報を使用して検証する（Ｓ８０４）。認可トークン発行部３０８は、対象のグループを認可トークン発行要求で指定されているグループＩＤから判定する。認証トークン発行要求にグループＩＤが含まれていない場合（Ｓ８０４においてＮｏ）、認可トークン発行部３０８は、第一のクライアント情報にセットされているデフォルトグループＩＤを使用する。グループＩＤが含まれている場合（Ｓ８０４においてＹｅｓ）、認可トークン発行部３０８は、第二のクライアントを権限委譲の対象として判定する（Ｓ８０５）。ここでは第二のクライアントは一つとして記載しているが、認可トークン発行部３０８は、同一のグループに属するすべてのクライアント１０３を第二のクライアントとして判定する。この際、認可トークン発行部３０８は、同一のユーザ及び権限スコープの認可トークンが存在しているクライアント１０３については、第二のクライアントから除外してもよい。最後に、認可トークン発行部３０８は、権限委譲の対象として判定されたクライアントへの許可判定を依頼する許可画面を生成する（Ｓ８０６）。

許可画面の一例を図９（ｂ）に示す。許可画面１１０４は、第一のクライアントに対して委譲する権限スコープの一覧１１０５と、第二のクライアントに対して委譲する権限ス

コープの一覧１１０６と、許可するか否かを確定するためのボタン１１０７と、から構成されている。

このように、本実施形態に係る認可画面の生成処理では、認可サーバ１０１は、認可トークン取得要求で指定された第一のクライアントだけでなく、第一のクライアントと同一のグループに属する第二のクライアントに対する許可判定を一括してユーザに依頼する。

【００２４】

次に、本実施形態に係る認可サーバが行う認可トークンの生成処理について、同処理のフローチャートを示す図１１を用いて説明する。

まず、認可トークン発行部３０８は、ユーザ端末から受信した許可判定情報が、第一のクライアントを許可しているか否かを判定する（Ｓ９０１）。許可されている場合（Ｓ９０１においてＹｅｓ）、認可トークン発行部３０８は、第一のクライアントに対して第一の認可トークンを生成する（Ｓ９０２）。発行された第一の認可トークンは認可トークン格納部３１１に格納される。この際、第一の認可トークンの送信状態は"送信待ち"にセットされる。一方、許可されていない場合（Ｓ９０１においてＮｏ）、認可トークン発行部３０８は、Ｓ９０３に処理を進める。認可トークン発行部３０８は、許可指示が第二のクライアントを許可しているか否かを判定する（Ｓ９０３）。許可されている場合（Ｓ９０３においてＹｅｓ）、認可トークン発行部３０８は、第二のクライアントに対して第二の認可トークンを生成する（Ｓ９０４）。発行された第二の認可トークンは、許可判定情報に付加されている認証トークン、及び第一の認可トークンに関連付けられて認可トークン格納部３１１に格納される。この際、第二の認可トークンの送信状態は"送信待ち"にセットされる。許可されていない場合（Ｓ９０３においてＮｏ）、認可トークン発行部３０８は、図１１に示す処理を終了する。

本実施形態に係る認可トークンの生成処理では、ユーザ端末から受信した許可判定情報に基づいて、認可トークン取得要求で指定された第一のクライアントだけでなく、第一のクライアントと同一のグループに属する第二のクライアントに対する認可トークンを一括して生成する。

【００２５】

次に、本実施形態に係る認可システムが行う認可トークンの検証処理について、同処理のフローチャートを示す図１２を用いて説明する。

まず、リソースサーバ１０２のリソース提供部３１２は、認可サーバ１０１に認可トークン検証要求を送信する（Ｓ１００１）。認可サーバ１０１の認可トークン検証部３０９は、認可トークン検証要求を受信する（Ｓ１００２）。認可トークン検証部３０９は、認可トークン検証要求に付加されている認可トークンが正規のものであるか否かを判定する（Ｓ１００３）。認可トークン検証部３０９は、正規のものであるか否かを、認可トークン格納部３１１に格納されているか否かによって判定する。認可トークンが正規のものでないと判定した場合（Ｓ１００３においてＮｏ）、認可トークン検証部３０９は、認可トークンは無効であると判定する（Ｓ１００４）。認可トークンが正規のものであると判定した場合（Ｓ１００３においてＹｅｓ）、認可トークン検証部３０９は、認可トークンが有効期限内であるか否かを判定する（Ｓ１００５）。有効期限を過ぎていると判定した場合（Ｓ１００５においてＮｏ）、認可トークン検証部３０９は、認可トークンは無効であると判定する（Ｓ１００４）。有効期限内であると判定した場合（Ｓ１００５においてＹｅｓ）、認可トークン検証部３０９は、認可トークン検証要求で指定された権限スコープが正当であるか否かを判定する（Ｓ１００６）。認可トークン検証部３０９は、権限スコープが正当であるか否かの判定を、認可トークン格納部３１１において、権限スコープが認可トークンに関連付けられているか否かによって判定する。権限スコープが正当でないと判定された場合（Ｓ１００６においてＮｏ）、認可トークン検証部３０９は、認可トークンは無効であると判定する（Ｓ１００４）。権限スコープが正当であると判定した場合（Ｓ１００６においてＹｅｓ）、認可トークン検証部３０９は、認可トークンが有効であると判定する（Ｓ１００７）。認可トークン検証部３０９は、検証結果を、リソースサーバ１０２に送信する（Ｓ１００８）。リソースサーバ１０２のリソース提供部３１２は、

検証結果を受信する（Ｓ１００９）。

【００２６】

次に、本実施形態に係る認可サーバが行う認可トークンの破棄処理について、同処理のフローチャートを示す図１３（ａ）を用いて説明する。認可トークンの破棄処理は、外部装置からの認可トークン破棄要求を受信した際や、有効期限切れの認可トークンを破棄する定期的なバッチ処理によって実行される。

まず、認可トークン破棄部３１０は、破棄対象の認可トークンを認可トークン格納部３１１から削除する（Ｓ１５０１）。破棄対象の認可トークンとは、認可トークン破棄要求で指定された認可トークンや、バッチ処理で有効期限切れと判定された認可トークンである。次に、認可トークン破棄部３１０は、破棄対象の認可トークンを関連認可トークンとしている他の認可トークンのうち、送信状態が"送信待ち"となっているものが存在するか否かを検証する（Ｓ１５０２）。存在する場合（Ｓ１５０２においてＹｅｓ）、認可トークン破棄部３１０は、その認可トークンを認可トークン格納部３１１から削除する（Ｓ１５０３）。存在しない場合（Ｓ１５０２においてＮｏ）、認可トークン破棄部３１０は、図１３（ａ）に示す処理を終了する。

このように、本実施形態に係る認可トークンの破棄処理では、第一の認可トークンを破棄する際に、同時に生成された第二の認可トークンが"送信待ち"の場合には第二の認可トークンも破棄する。

ここでは、送信状態が"送信待ち"の場合に第二の認可トークンを破棄する例を示したが、送信状態に関わらず第二の認可トークンを破棄してもよい。

本実施形態に係る認可システムによれば、同一のグループに属するクライアントに対する許可判定の依頼と、認可トークンの生成とを一括して行うことができる。そのため、クライアント各々の対する権限の許可を考慮した方法で、ユーザの許可操作の負荷を軽減することができる。

【００２７】

＜実施形態２＞

実施形態１では、許可画面の生成処理において、第一のクライアント及び第二のクライアントに対する許可判定の依頼を一括して行う例を示した。本実施形態では、許可判定の依頼を一括して行う際に、どのクライアントにどの権限を許可するかの選択を可能にする例を示す。

本実施形態に係る認可サーバの認可トークン発行部３０８が生成する許可画面の一例を図１４に示す。許可画面１３０１は、第一のクライアントに対して委譲する権限スコープの一覧１３０２と、第二のクライアントに対して委譲する権限スコープの一覧１３０３と、許可判定を確定するためのボタン１３０４とから構成されている。権限スコープの一覧１３０２と１３０３とでは、各クライアントを許可するのか、各クライアントにどの権限スコープを許可するのかをチェックボックスで選択可能になっている。チェックボックスは、権限スコープを許可するか否かを選択可能なオブジェクトの一例である。

このように、本実施形態に係る認可画面の生成処理では、第一のクライアント及び第二のクライアントに対する許可判定を一括して行う際に、許可するクライアント及び権限が選択可能である。そのため、ユーザがより柔軟に一括した許可判定を行うことができる。

【００２８】

＜実施形態３＞

実施形態１では、許可画面の生成処理において、同一のグループに属するクライアント１０３を第二のクライアントと判定して、一括して許可判定の依頼を行う例を示した。本実施形態では、予め設定されたワークフロー情報に基づいて、第二のクライアントを判定する例を示す。

本実施形態に係る認可サーバのクライアント情報格納部３０６に格納されているワークフロー情報の一例を図１５（ａ）に示す。ワークフロー情報１４０１には、ワークフローＩＤに関連づけて、どの順番でどのクライアントを実行するか、またその際に必要な権限スコープは何かが定義されている。クライアント１０３は、対象となるワークフローＩＤ

を指定して認証トークン取得要求を送信する。認可サーバの認可トークン発行部３０８は、指定されたワークフローに定義されているクライアントを第二のクライアントと判定して、許可画面を生成する。

このように、本実施形態に係る許可画面の生成処理では、ワークフローに基づいて第二のクライアントを判定する。そのため、クライアント同士の連携を考慮した上で、一括して許可判定の依頼を行うことができる。

【００２９】

＜実施形態４＞

実施形態１では、許可画面の生成処理において、同一のグループに属するクライアント１０３を第二のクライアントと判定して、一括して許可判定の依頼を行う例を示した。本実施形態では、ユーザに関連付けられているクライアント１０３を、第二のクライアントとして判定する例を示す。

本実施形態に係る認可サーバのクライアント情報格納部３０６に格納されている登録クライアント情報を図１５（ｂ）に示す。ユーザＩＤ１４０２に関連づけて、登録クライアント１４０３が格納されている。認可部３０７は、入力装置２０７等を介したユーザ操作に基づいて登録クライアントを登録してもよいし、ユーザのクライアントへのアクセス履歴に基づいて登録してもよい。認可サーバの認可トークン発行部３０８は、登録クライアントとして登録されているクライアントを第二のクライアントとして判定して、許可画面を生成する。

このように、本実施形態に係る許可画面の生成処理では、ユーザに関連付けられているクライアントを、第二のクライアントとして判定する。そのため、ユーザの特性を考慮した上で、一括して許可判定の依頼を行うことができる。

【００３０】

＜実施形態５＞

実施形態１では、認可トークンの破棄処理において、第一の認可トークンを破棄する際に、同時に生成された第二の認可トークンも破棄する例を示した。本実施形態では、認可トークンを破棄する際に、当該認可トークンがどのユーザの許可に基づいているのかを判定し、当該ユーザに関連付けられている他の認可トークンも破棄する例を示す。

本実施形態に係る認可サーバが行う認可トークンの破棄処理について、同処理のフローチャートを示す図１３（ｂ）を用いて説明する。まず、認可トークン破棄部３１０は、破棄対象の認可トークンを認可トークン格納部３１１から削除する（Ｓ１５０４）。次に、認可トークン破棄部３１０は、破棄対象の認可トークンがどのユーザに関連付けられているかを判定する（Ｓ１５０５）。認可トークン破棄部３１０は、認可トークン格納部３１１に格納されている関連認証トークンＩＤ５０８で関連する認証トークンを特定し、認証トークン格納部３０５に格納されているユーザＩＤ５０２でユーザを特定することによって判定する。次に、認可トークン破棄部３１０は、当該ユーザに関連付けられている認可トークンが存在するか否かを検証する（Ｓ１５０６）。当該ユーザに関連付けられている認可トークンが存在する場合（Ｓ１５０６においてＹｅｓ）、認可トークン破棄部３１０は、その認可トークンを認可トークン格納部３１１から削除する（Ｓ１５０７）。一方、当該ユーザに関連付けられている認可トークンが存在しない場合等（Ｓ１５０６においてＮｏ）、認可トークン破棄部３１０は、図１３（ｂ）に示す処理を終了する。

このように、本実施形態に係る認可トークンの破棄処理では、認可トークンを破棄する際に、同一のユーザに関連付けられている他の認可トークンも破棄する。そのため、ユーザに関連付けられている認可トークンを一括して破棄することができる。

【００３１】

＜その他の実施形態＞

本発明は、上述の実施形態の１以上の機能を実現するプログラムを、ネットワーク又は記憶媒体を介してシステム又は装置に供給する。そして、そのシステム又は装置のコンピュータにおける１つ以上のプロセッサーがプログラムを読み出し実行する処理でも実現可能である。また、１以上の機能を実現する回路（例えば、ＡＳＩＣ）によっても実現可能

である。

【００３２】

以上、本発明の好ましい実施形態について詳述したが、本発明は係る特定の実施形態に限定されるものではない。上述した実施形態の処理は、ＯＡｕｔｈ２．０のプロトコルに従った構成で記載した。しかし、上述した実施形態の処理は、ＯＡｕｔｈ２．０のプロトコルに限定されるものではない。また、上述した実施形態を任意に組み合わせて実施してもよい。

【００３３】

以上、上述した各実施形態によれば、事前にポリシー情報を登録することなく、権限委譲の対象ごとの権限を考慮したうえで、権限を委譲する際のユーザの操作負荷を軽減する技術を提供することができる。

【符号の説明】

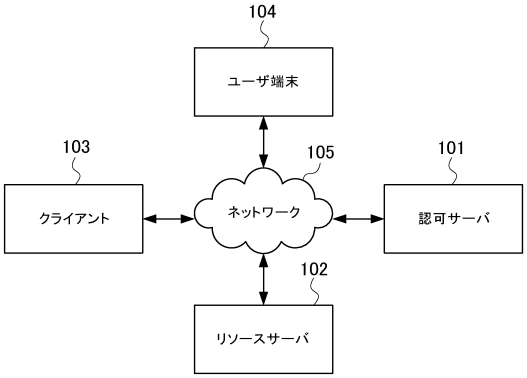
【００３４】

１０１　認可サーバ

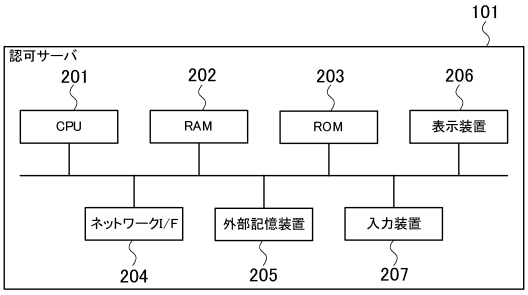
１０４　ユーザ端末

２０１　ＣＰＵ

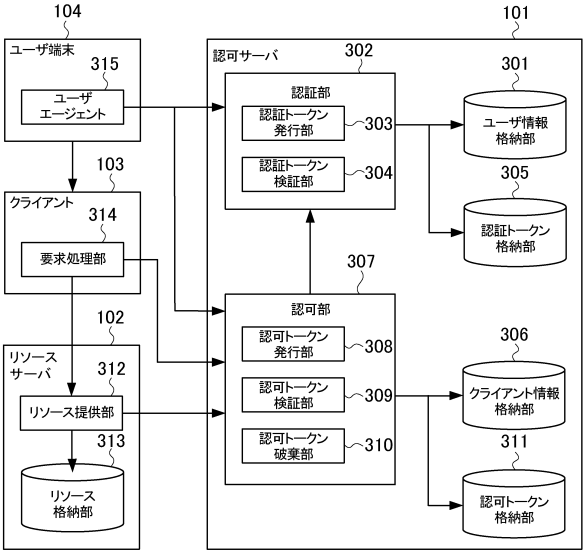
【図１】



【図２】



【図３】



【図４】

401 402

ユーザID	パスワード
User001	aaa
User002	bbb
…	…

(a)

403 404 405 406

クライアントID	パスワード	権限スコープ	デフォルトグループ
Client001	aaa	Scope001, Scope002	Group001
Client002	bbb	Scope002	Group001
…	…	…	…

(b)

407 408

グループID	所属クライアント
Group001	Client001, Client002
Group002	Client001, Client003
…	…

(c)

【図５】

501 502 503

認証トークンID	ユーザID	有効期限
AuthnToken001	User001	201601011200
AuthnToken002	User002	201601011200
…	…	…

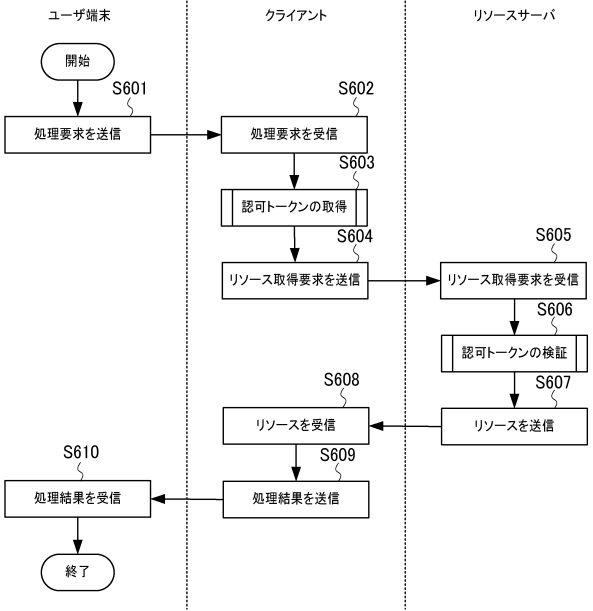
(a)

504 505 506 507 508 509 510

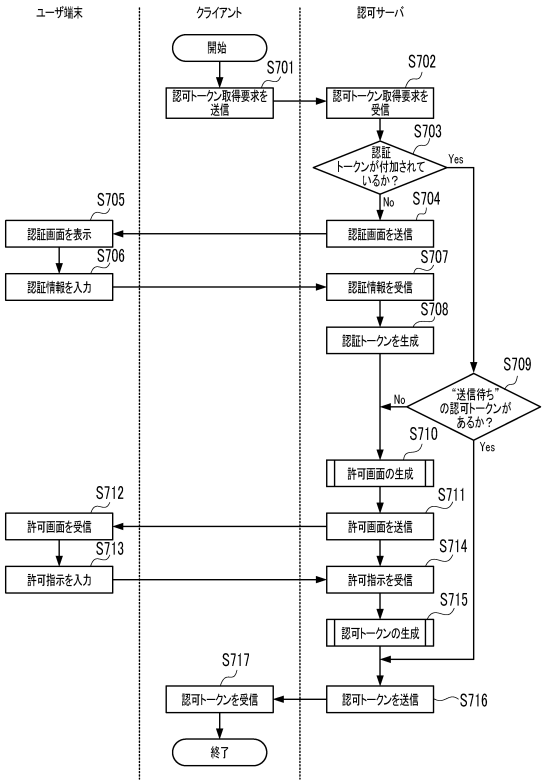
認可トークンID	クライアントID	権限スコープ	有効期限	関連認証トークンID	関連認可トークンID	送信状態
AccessToken001	Client001	Scope001	201601011200	AuthnToken001	-	送信済み
AccessToken002	Client002	Scope002	201601011200	AuthnToken002	AccessToken001	送信待ち
…	…	…	…	…	…	…

(b)

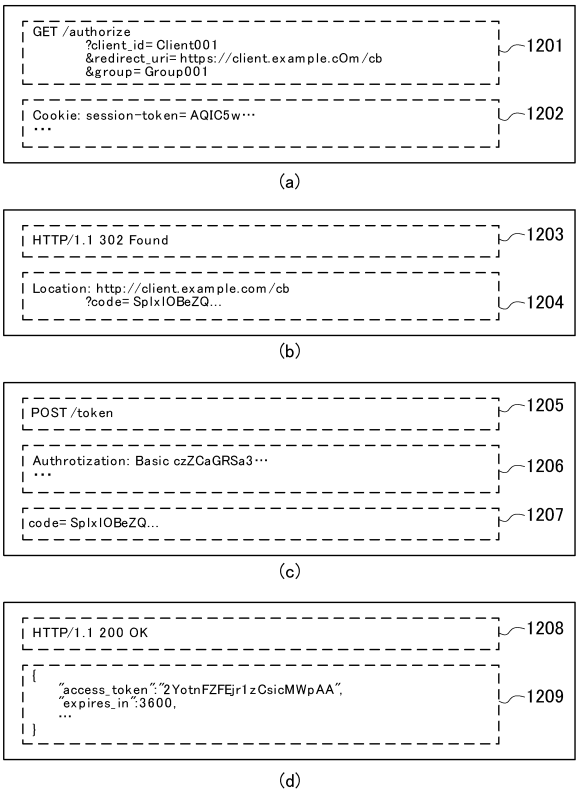
【図６】



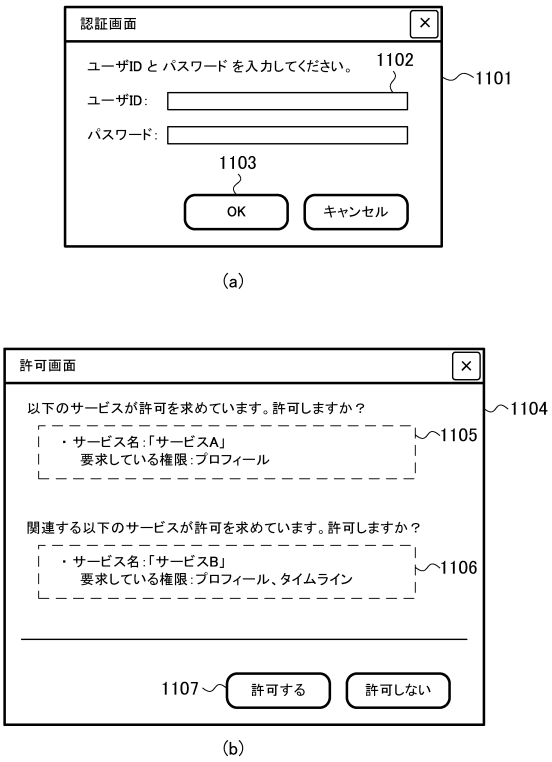
【図７】



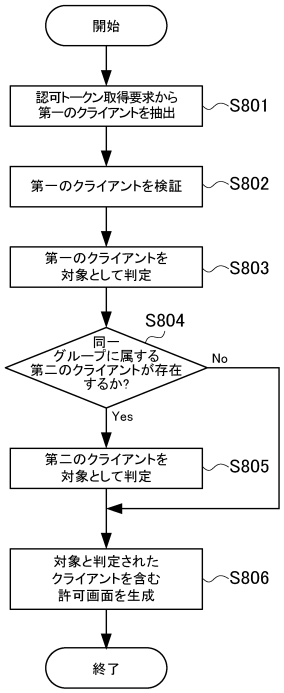
【図８】


GET /authorize
?client_id= Client001
&redirect_uri= https://client.example.cOm/cb
&group= Group001
1201
Cookie: session-token= AQIC5w…
…
1202
(a)
HTTP/1.1 302 Found
1203
Location: http://client.example.com/cb
?code= SplxlOBeZQ...
1204
(b)
POST /token
1205
Authrotization: Basic czZCaGRSa3…
…
1206
code= SplxlOBeZQ...
1207
(c)
HTTP/1.1 200 OK
1208
{
"access_token":"2YotnFZFEjr1zCsicMWpAA",
"expires_in":3600,
…
}
1209
(d)

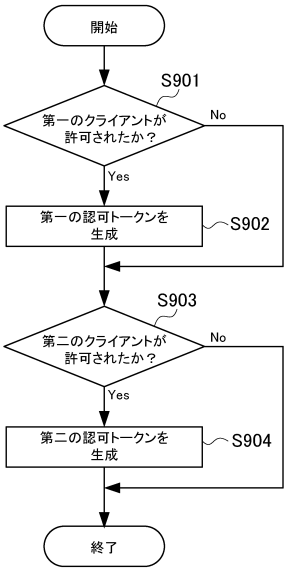
【図９】


認証画面
ユーザID と パスワード を入力してください。
1102
1101
ユーザID:
パスワード:
1103
OK
キャンセル
(a)
許可画面
以下のサービスが許可を求めています。許可しますか？
1104
・サービス名:「サービスA」
要求している権限:プロフィール
1105
関連する以下のサービスが許可を求めています。許可しますか？
・サービス名:「サービスB」
要求している権限:プロフィール、タイムライン
1106
1107
許可する
許可しない
(b)

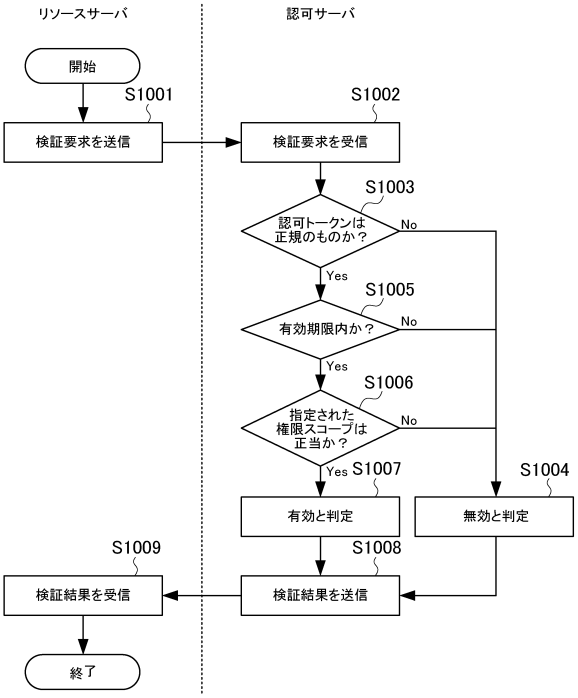
【図１０】


開始
認可トークン取得要求から
第一のクライアントを抽出
S801
第一のクライアントを検証
S802
第一のクライアントを
対象として判定
S803
S804
同一
グループに属する
第二のクライアントが存在
するか?
No
Yes
第二のクライアントを
対象として判定
S805
対象と判定された
クライアントを含む
許可画面を生成
S806
終了

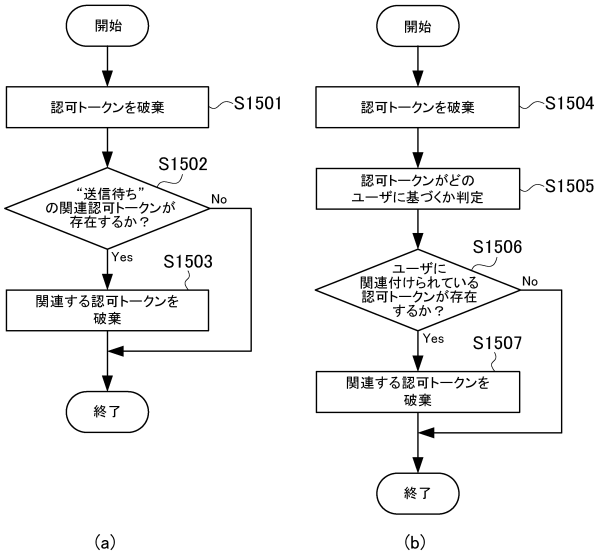
【図１１】


開始
S901
第一のクライアントが
許可されたか？
No
Yes
第一の認可トークンを
生成
S902
S903
第二のクライアントが
許可されたか？
No
Yes
第二の認可トークンを
生成
S904
終了

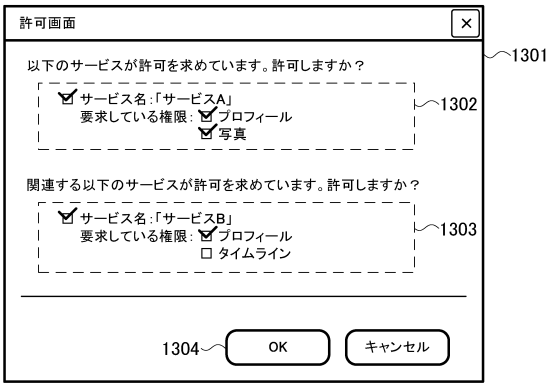
【図１２】



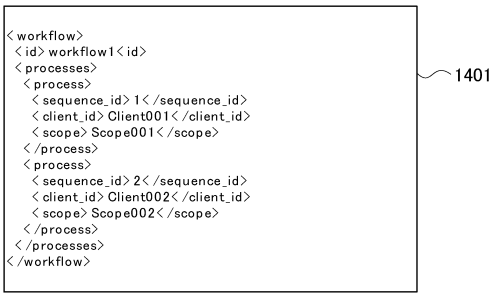
【図１３】



【図１４】



【図１５】



1402 1403

ユーザID	登録クライアント
User001	Client001, Client002
User002	Client001, Client003
…	…

(b)

フロントページの続き

(56)参考文献 特開２０１７－０９１２０７（ＪＰ，Ａ）
特開２０１４－１４６１３２（ＪＰ，Ａ）
小倉 孝夫，マルチサービス連携における同意制御方式の提案，ＳＣＩＳ２０１６，２０１６年
1月１９日，p.1-7

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ ２１／００－８８