(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
2021年5月27日(27.05.2021)

WIPO | PCT

(10) 国際公開番号
WO 2021/100533 A1

(51) 国際特許分類:
G06F 21/35 (2013.01) *G06F 21/62* (2013.01)

(21) 国際出願番号： PCT/JP2020/041802

(22) 国際出願日： 2020年11月10日(10.11.2020)

(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 2019-208994 2019年11月19日(19.11.2019) JP

(71) 出願人: キヤノン株式会社 (**CANON KABUSHIKI KAISHA**) [JP/JP]; 〒1468501 東京都大田区下丸子３丁目３０番２号 Tokyo (JP).

(72) 発明者: 山中嶋 和成 (**YAMANAKAJIMA Kazunari**); 〒1468501 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 Tokyo (JP).

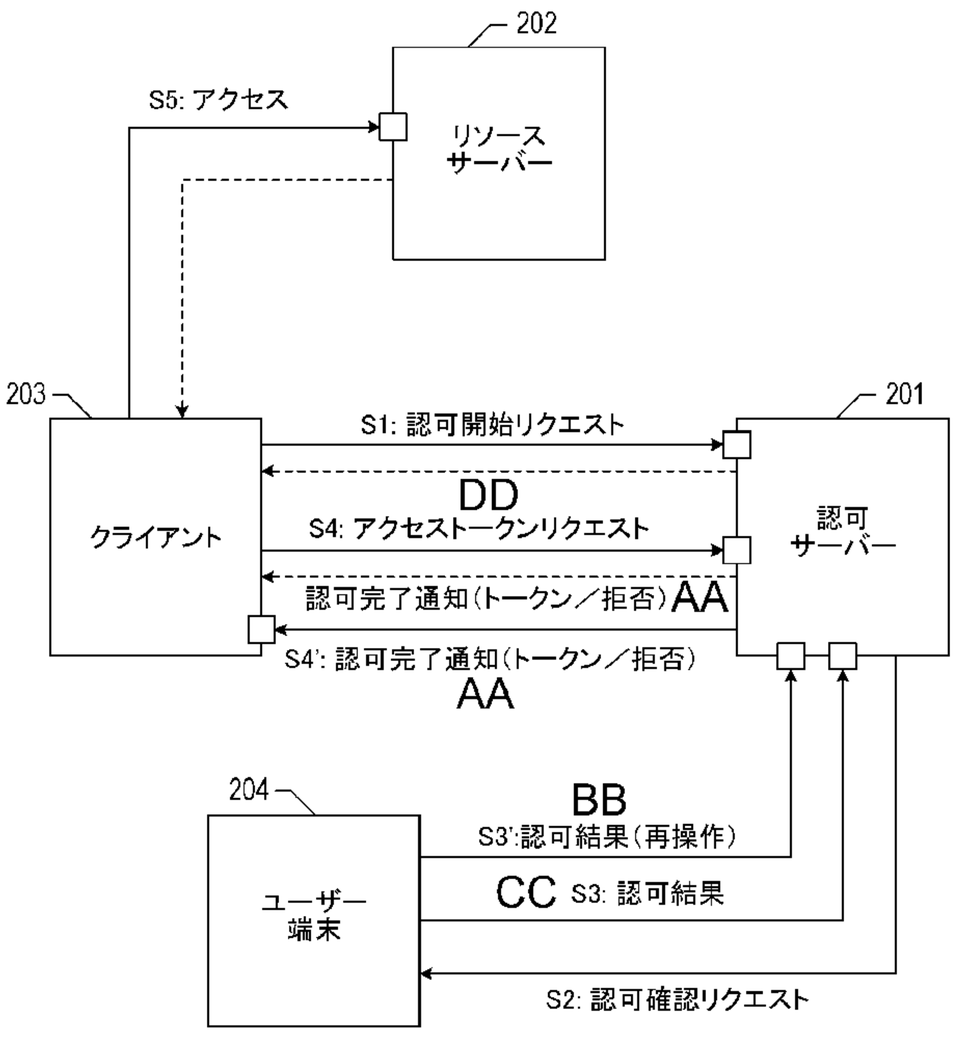
(74) 代理人: 阿部 琢磨，外 (**ABE Takuma** et al.); 〒1468501 東京都大田区下丸子３丁目３０番２号キヤノン株式会社内 Tokyo (JP).

(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, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, 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, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, 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,

(54) Title: AUTHORIZATION SERVER, SYSTEM, METHOD FOR SYSTEM, AND PROGRAM FOR AUTHORIZATION SERVER

(54) 発明の名称： 認可サーバー、システム、システムの方法、および認可サーバーのプログラム



201 Authorization server
202 Resource server
203 Client
204 User terminal
S1 Authorization start request
S2 Authorization confirmation request
S5 Access
AA Authorization completion notice (token/reject)
BB Authorization result (re-operation)
CC Authorization result
DD Access token request

(57) Abstract: Upon receipt of an authorization result from a user, this authorization server sets a deadline for reauthorization, performs a waiting process until the deadline, and then issues an access token.

(57) 要約：認可サーバーがユーザーからの認可結果を受信した後、再認可を行える期限を設け、期限がくるまで待ち処理を行いその後アクセストークンの発行を行う。

［続葉有］

WO 2021/100533 A1

SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

添付公開書類：

一　国際調査報告（条約第21条(3)）

明　細　書

発明の名称 ：

認可サーバー、システム、システムの方法、および認可サーバーのプログラム

技術分野

[0001] 本発明は、リソースにアクセスする権限が委譲されたことに応じてアクセストークンを発行する認可サーバー、システム、システムの方法、および認可サーバーのプログラムに関する。

背景技術

[0002] ウェブシステムにおいてＯＡｕｔｈ２．０による権限委譲の仕組みが実現されている。特許文献１ではシステム連携を設定する際、ユーザーはクライアントと認可サーバーの両方をウェブブラウザで操作し、認可操作を行うことでユーザーの権限をクライアントに委譲することを開示している。クライアントは、委譲されたユーザーの権限を用いてユーザーのリソースにアクセスでき、システム連携が実現する。ＯＡｕｔｈ２．０でユーザーの権限をクライアントに委譲するためには、ユーザーがクライアントにウェブブラウザでアクセスすることが必要になる。

先行技術文献

特許文献

[0003] 特許文献1：特許５６２３２３４号公報

発明の概要

発明が解決しようとする課題

[0004] 従来の手法では、ユーザーがクライアントに権限委譲するための操作を行うことで権限委譲のフローが開始された。しかし、ＩｏＴデバイスの普及やスマートフォンのような携帯端末の普及により、クライアントが自律的に権限委譲の要求を行うと権限委譲のフローが開始され、ユーザーが物理的およ

び／またはシステム的に離れたところで認可操作を行う形態が新たに考えられる。

[0005] しかしながら、この形態の場合、ユーザーは一度行った認可操作を訂正したくとも、クライアントの認可要求とユーザーの認可操作が独立してしまうためユーザー側から再認可操作を行うことができなくなる懸念がある。そこで、本願発明の目的は、クライアントの認可要求とユーザーの認可操作が独立している形態において、ユーザーは再認可操作を行うことが可能な仕組みを提供することにある。

課題を解決するための手段

[0006] 本実施形態に係る認可サーバーは、ユーザーのリソースを提供するリソースサーバー、前記リソースへアクセスするクライアント、前記クライアントが前記リソースへアクセスすることがユーザーにより許可されたことを示すアクセストークンを発行する認可サーバー、およびユーザー端末とから構成されるシステムにおける前記認可サーバーであって、前記クライアントから認可開始リクエストを受信する受信手段と、前記受信手段により認可開始リクエストが受信されたことに応じて、認可確認リクエストの送信先となるユーザー端末を特定する特定手段と、特定されたユーザー端末に対して認可確認リクエストを送信し、応答として認可確認の結果を受信し、再認可が可能な期間まで前記認可確認の結果を一時的に記憶する認可手段と、再認可が可能な期間を超えたことに応じて一時的に記憶されている前記認可確認の結果に応じたアクセストークンの発行の制御を行い、前記アクセストークンを発行した場合は前記認可開始リクエストを送信した前記クライアントへ前記アクセストークンを送信する発行手段と、を有することを特徴とする。

発明の効果

[0007] クライアントの認可要求とユーザーの認可操作が独立している形態において、ユーザーは再認可操作を行うことができる仕組みを提供する。

図面の簡単な説明

[0008] [図1]コンピュータの構成図

[図2]システムのネットワーク構成図

[図3A]権限移譲システムの機能ブロック図

[図3B]権限移譲システムの機能ブロック図

[図3C]権限移譲システムの機能ブロック図

[図3D]権限移譲システムの機能ブロック図

[図4A]認可開始リクエストおよび認可確認リクエストフロー

[図4B]認可開始リクエストおよび認可確認リクエストフロー

[図4C]認可開始リクエストおよび認可確認リクエストフロー

[図5A]アクセストークン発行フロー

[図5B]アクセストークン発行フロー

[図5C]アクセストークン発行フロー

[図5D]アクセストークン発行フロー

[図6]権限委譲システムのシーケンス図

[図7]権限委譲システムにおける再認可処理のシーケンス図

[図8A]再認可処理に関するフローチャート

[図8B]再認可処理に関するフローチャート

[図9A]認可確認画面

[図9B]認可確認画面

[図9C]認可確認画面

[図9D]認可確認画面

[図10A]認可履歴画面のフローチャート

[図10B]認可履歴画面のフローチャート

[図11]実施例２における認可開始リクエストで送付される情報

[図12]実施例２における認可結果受信のフローチャート

[図13]実施例２におけるアクセストークンレスポンスフローチャート

[図14]実施例２における認可履歴描画のフローチャート

発明を実施するための形態

[0009] ［実施例１］

以下、本発明を実施するための形態について図面を用いて説明する。図１は、本発明を実施するための一実施形態に係る情報処理装置の構成を示す図である。図１において、情報処理装置は、ＣＰＵ１０２、メモリ１０３、記憶装置１０４、ビデオインタフェース１０５、Ｉｎｐｕｔ／Ｏｕｔｐｕｔ（以下Ｉ／Ｏと略称）インタフェース１０６、通信インタフェース１０７を備えている。また、情報処理装置内の各構成要素はシステムバス１０１を介して互いに接続されている。ＣＰＵ１０２は、システムバス１０１を介して各構成要素を制御したり、データの計算や加工を行ったりする中央処理装置である。メモリ１０３は、データやプログラムを記憶する装置で、ＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）やＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）から構成される。

[0010] 記憶装置１０４は、記憶されたデータの書き込み／読み出しを行う。記憶装置１０４には、ハードディスクドライブ（ＨＤＤ）１１１、不揮発性のデータソースとして利用されるＤＶＤ－ＲＯＭドライブ１１２、半導体メモリを用いたソリッドステートドライブ（ＳＳＤ）１１３がある。図１には示されていないが、記憶装置１０４として、磁気テープドライブ、フロッピー（登録商標）ディスクドライブ（ＦＤＤ）、ＣＤ－ＲＯＭドライブ、ＣＤ／ＤＶＤ－ＲＡＭドライブ、ＵＳＢフラッシュドライブなども使用されることがある。

[0011] 本実施形態に係るプログラムは、記憶装置１０４から読み込まれ、メモリ１０３に格納した上で、ＣＰＵ１０２によって実行される。なお、本実施形態ではプログラムを記憶装置１０４から読み込む構成としているが、ＲＯＭ（不図示）から読み込んだり、通信インタフェース１０７を介して外部から読み込んだりする構成としてもよい。

[0012] ビデオインタフェース１０５は、ディスプレイ装置１１４への表示出力を制御する。ディスプレイ装置１１４には、ＣＲＴや液晶等の方式を用いたものがある。Ｉ／Ｏインタフェース１０６には、キーボード１１５やポインティングデバイス１１６等の入力装置が接続される。操作者は、キーボード１

１５を操作することにより情報処理装置に対する動作指令等を行う。ポインティングデバイス１１６は、ディスプレイ装置１１４上のカーソルを移動させてメニューやオブジェクトの選択や操作等を行う。また、ディスプレイ装置１１４には、タッチパネル等による操作の入力を行えるものもある。この場合、ディスプレイ装置１１４は出力装置と入力装置を兼ねることになる。

[0013] 通信インタフェース１０７は、コンピュータネットワーク１１７を通して外部機器との通信を行う。接続先のネットワークには、ＬＡＮやＷＡＮ、インターネットのような公衆回線等があり、有線であっても無線であっても構わない。また、通信インタフェース１０７は、ローカルプリンタ１１８などの他デバイスとの通信も行う。

[0014] 図２は、本実施形態に係る権限移譲システムのネットワーク構成図である。図２に図示されるサーバー、クライアント、ユーザー端末はいずれも、図１で示した装置の構成を備えているものとする。ただし、図１の構成に限定するものではなく、他の機能を備えている場合や、単体のコンピュータに限らないラックマウント型のシステムであっても構わない。また、後述の全ての説明において、特に断りのない限りサーバーやクライアントの実行の主体はＣＰＵ１０２であり、ソフトウェア上の主体は記憶装置１０４に保管されたプログラムである。

[0015] 図２において、コンピュータネットワーク２００には、認可サーバー２０１、リソースサーバー２０２、クライアント２０３、および、ユーザー端末２０４が接続されている。ユーザー端末２０４の形態としては、例えば、スマートフォンやタブレット端末等のような携帯可能なコンピュータや、クライアントパーソナルコンピュータ等がある。コンピュータネットワーク２００には、ＬＡＮ、ＷＡＮ、インターネット等があり、有線であっても無線であっても構わない。

[0016] 本実施形態において、ユーザー端末２０４は、コンピュータネットワーク２００を通じて認可サーバー２０１と通信を行い、クライアント２０３はコンピュータネットワーク２００を通じて認可サーバー２０１やリソースサー

バー２０２と通信を行う。ユーザー端末２０４は、データを受信するとＷｅｂブラウザあるいは専用のクライアントアプリケーションが取得したデータをクライアント端末のディスプレイ装置１１４に表示する。

[0017] 図３は本実施の形態に係る権限移譲システムの機能ブロック図である。図３Ａはクライアント２０３、図３Ｂは認可サーバー２０１、図３Ｃはリソースサーバー２０２、図３Ｄはユーザー端末２０４の機能ブロックを示す。クライアント２０３は認可開始リクエスト発行部３３１、アクセストークン要求部３３３、アクセストークン管理部３３４、リソースアクセス部３３２を持つ。認可サーバー２０１は認可リクエスト管理部３１１、認可確認リクエスト送信先解決部３１２、認可確認部３１３、アクセストークン発行部３１４を持つ。リソースサーバー２０２はリソース管理部３２１を持つ。ユーザー端末２０４は認可操作受付部３４１、認可結果送信部３４２、認可履歴管理部３４３、画面表示部３４４を持つ。

[0018] 認可サーバー２０１の認可リクエスト管理部３１１は、クライアント２０３の認可開始リクエスト発行部３３１の要求に従い、認可開始リクエストを処理する。ここで認可開始リクエストにはクライアント２０３がアクセスしようとするリソースのリソース情報、リソースに対して行う処理の種別、クライアント情報などが含まれる。認可確認リクエスト送信先解決部３１２は認可開始リクエストに含まれるリソース情報、処理種別、クライアント情報などを用いて、認可確認リクエストの送信先となるユーザー端末を決定する。認可確認部３１３は認可確認リクエスト送信先解決部３１２で決定されたユーザー端末２０４に対して認可確認リクエストを行う。ユーザー端末２０４を利用するユーザーが認可操作を行うと、クライアント２０３は認可サーバー２０１からアクセストークンを取得できるようになり、アクセストークンを使ってリソースサーバーにアクセスできるようになる。

[0019] ＯＡｕｔｈ２．０と同様、クライアント２０３は、実施例１のプロトコルフローを開始する以前に認可サーバー２０１に登録されていなければならない。クライアント２０３を認可サーバー２０１に登録させるため、認可サー

バー２０１はクライアント２０３登録者との対話を伴うＨＴＭＬ登録フォーム（不図示）を提供する。また、本実施例のクライアント２０３の登録においては、クライアント２０３と認可サーバー２０１の間に直接的なやりとりは必須ではない。例えば、クライアント２０３自身あるいはサードパーティーが発行したアサーションの使用や、認可サーバー２０１のセキュアなチャネルを使用したクライアント２０３をディスカバリーで、クライアント２０３を認可サーバー２０１へ登録することもできる。

[0020] 実施例１において認可サーバー２０１にクライアント２０３を登録する場合、クライアント２０３の登録者は、クライアントタイプ（ＯＡｕｔｈ２．０定義の“Ｃｏｎｆｉｄｅｎｔｉａｌ”）、アプリケーション名、サービス名、ロゴイメージ、利用規則を指定する。また登録の際、クライアント２０３に対して認可サーバー２０１はクライアント識別子とクライアントＳｅｃｒｅｔを発行する。クライアント２０３は発行されたクライアント識別子とクライアントＳｅｃｒｅｔを認可開始リクエスト発行部３３１に記憶しておく。

[0021] また、認可サーバー２０１は、クライアント２０３から受信した情報を認可確認リクエスト送信先解決部３１２内のクライアント登録テーブル（表１）に登録する。

[0022] [表1]

クライアント登録テーブル

クライアント識別子	クライアントSecret	アプリケーション名	サービス名	ロゴイメージ	利用規則
Client_1	xxxxxxx	App_1	Serv_1	Logo.png	Yyyyyyy

[0023] さらに、ユーザー端末２０４は、実施例１のプロトコルフローを開始する以前に、認可サーバー２０１に登録されていなければならない。ユーザー端末２０４を認可サーバー２０１に登録させるため、認可サーバー２０１はユーザー端末２０４登録者との対話を伴うＨＴＭＬ登録フォーム（不図示）を提供する。

[0024] また、実施例１のユーザー端末２０４の登録において、ユーザー端末２０４と認可サーバー２０１の間に直接的なやりとりは必須ではない。例えば、ユーザー端末２０４が発行したアサーションを使用したり、認可サーバー２０１がセキュアなチャンネルを使用してユーザー端末２０４のディスカバリーを行ったりすることで、ユーザー端末２０４を登録することもできる。ユーザー端末は複数登録が可能である。

[0025] 登録の際、ユーザー端末２０４に対して認可サーバー２０１は、各々端末ＩＤと端末Ｓｅｃｒｅｔを発行する。クライアント２０３は発行された端末ＩＤと端末Ｓｅｃｒｅｔを認可操作受付部３４１に記憶しておく。実施例１において、認可サーバー２０１にユーザー端末２０４を登録する場合、ユーザー端末２０４の登録者は以下の情報を指定する。ユーザー端末情報（後述の認可確認リクエストを通知する通信のエンドポイント）、サービス名、アプリケーション名（共にクライアント２０３の登録の際に指定したもの）、ユーザー識別子（ユーザー名）である。

[0026] ユーザー端末２０４登録の際に、登録内容は、図３Ｂで示される認可サーバー２０１の認可確認リクエスト送信先解決部３１２内のユーザー端末登録テーブル（表２）に登録される。

[0027] [表2]

ユーザー端末登録テーブル

ユーザー端末情報	端末 ID	端末 Secret	クライアント識別子	アプリケーション名	サービス名	ユーザー識別子
192.168.0.1	Device_1	wwwwww	Client_1	App_1	Serv_1	user_A
192.168.0.2	Device_2	zzzzzzzzz	Client_1	App_1	Serv_1	user_B

[0028] 実施例１において、ユーザー端末２０４の情報は、ユーザー端末情報“１９２．１６８．０．１”、端末ＩＤ“Ｄｅｖｉｃｅ＿１”、端末Ｓｅｃｒｅｔ“ｗｗｗｗｗｗ”、クライアント識別子“Ｃｌｉｅｎｔ＿１”、アプリケーション名“Ａｐｐ＿１”、サービス名“Ｓｅｒｖ＿１”、ユーザー識別子“ｕｓｅｒ＿Ａ”である。また、表２には別のユーザー端末として、ユーザー端末情報“１９２．１６８．０．２”、端末ＩＤ“Ｄｅｖｉｃｅ＿２”、

端末Ｓｅｃｒｅｔ“ｚｚｚｚｚｚｚｚｚｚ”、クライアント識別子“Ｃｌｉｅｎｔ＿１”、アプリケーション名“Ａｐｐ＿１”、サービス名“Ｓｅｒｖ＿１”、ユーザー識別子“ｕｓｅｒ＿Ｂ”が登録されている。

[0029] 図４Ａはクライアント２０３が認可サーバー２０１に対し認可開始リクエストを行うフローである。本フローはクライアント２０３がリソースサーバー２０２上のリソースへのアクセスに先立ち、アクセストークンが必要になった際に開始される。

[0030] ステップＳ４０１で認可開始リクエスト発行部３３１は、クライアント識別子、操作対象のリソース識別子、スコープおよび対象となるユーザーを特定するためのヒント情報を含む認可開始リクエストを、認可サーバー２０１に対して送信する。ここで各用語について補足する。スコープとは、リソースのアクセス範囲を示すもので、例えば、リソースであるデータを取得したい場合は“ｇｅｔ－ｄａｔａ”、取得以外に編集などのそれ以外のアクセスを行いたい場合は“ｇｅｔ－ａｌｌ”を指定することになる。対象となるユーザーを特定するためのヒント情報は、ユーザー識別子を示す。またヒント情報は、過去ユーザーに対して発行されたＩＤトークン、ユーザーのメールアドレス、ユーザー識別子のいずれかの情報であってもよい。

[0031] ステップＳ４０２で認可開始リクエスト発行部３３１は、認可サーバー２０１からレスポンスを受信する。このレスポンスには、認可サーバー２０１が発行した認可リクエスト識別子が含まれる。ステップＳ４０３で認可開始リクエスト発行部３３１は、ステップＳ４０２で受信したレスポンスに含まれる認可リクエスト識別子を、ステップＳ４０１の操作対象リソースおよびスコープとともに記憶してフローを終了する。

[0032] 表３はクライアント２０３が記憶する認可リクエスト管理テーブルの例である。

[0033]

[表3]

認可リクエスト管理テーブル

認可リクエスト識別子	リソース識別子	スコープ	アクセストークン識別子
auth_req_id_12345	/datalake/iot0010/data	get-data	(空欄)
auth_req_id_98765	/datalake/iot0011/data	get-data	actk111222333

[0034] 表３ではリソース識別子“／ｄａｔａｌａｋｅ／ｉｏｔ００１０／ｄａｔａ”で示されるリソースに対し、スコープ“ｇｅｔ－ｄａｔａ”で行った認可開始リクエストが、認可リクエスト識別子“ａｕｔｈ＿ｒｅｑ＿ｉｄ＿１２３４５”に紐付けて記憶されている。また認可リクエスト識別子“ａｕｔｈ＿ｒｅｑ＿ｉｄ＿９８７６５”に対しては、“ａｃｔｋ１１１２２２３３３”で示されるアクセストークンを取得済みであることを示す。ここでリソース識別子が示すリソースは、ファイルシステム上の１つのファイルを示してもよく、データベース上の特定のレコードを示してもよい。またそれらの集合を示してもよい。

[0035] 図４Ｂは認可サーバー２０１における認可開始リクエストの受信フローである。本フローは認可サーバー２０１がクライアント２０３から認可開始リクエストを受信することで開始される。

[0036] ステップＳ４１１で認可リクエスト管理部３１１は、クライアント２０３から認可開始リクエストを受け付ける。ここで認可開始リクエストには、クライアント２０３のクライアント識別子と、クライアント２０３が操作対象としているリソース識別子と、クライアント２０３が要求するスコープと、クライアント２０３が要求するヒント情報が含まれる。

[0037] ステップＳ４１２で認可リクエスト管理部３１１は、ステップＳ４１１で受信した認可開始リクエストに対応する認可リクエスト識別子を生成する。ステップＳ４１３で認可リクエスト管理部３１１は、ステップＳ４１２で生成した認可リクエスト識別子に、認可リクエストの情報を紐付けて記憶する。ここで認可リクエストの情報とは、ステップＳ４１１で受信したクライア

ント識別子、操作対象のリソース識別子、スコープと、ヒント情報を含む。

[0038] 表４は認可リクエスト管理部３１１が記憶する認可確認状況管理テーブルの例である。

[0039] [表4]

認可確認状況管理テーブル

認可リクエスト識別子	クライアント識別子	リソース	スコープ	ヒント情報	認可結果
auth_req_id_12345	Client_1	/datalake/iot0010/data	get-data	user_A	(空欄)
auth_req_id_98765	Client_1	/datalake/iot0011/data	get-data	user_B	approved
auth_req_id_44444	Client_2	/datalake/iot0011/data	get-all	user_abcde	disapproved

[0040] 表４では、クライアント識別子“Ｃｌｉｅｎｔ＿１”で示されるクライアントが、リソース識別子“／ｄａｔａｌａｋｅ／ｉｏｔ００１０／ｄａｔａ”で示されるリソースに対し、スコープ“ｇｅｔ－ｄａｔａ”で行った認可開始リクエストが、認可リクエスト識別子“ａｕｔｈ＿ｒｅｑ＿ｉｄ＿１２３４５”に紐付けて記憶されている。また認可リクエスト識別子“ａｕｔｈ＿ｒｅｑ＿ｉｄ＿１２３４５”にはヒント情報としてユーザー識別子“ｕｓｅｒ＿Ａ”が紐付けられているが、これはリソース“／ｄａｔａｌａｋｅ／ｉｏｔ００１０／ｄａｔａ”のリソース所有者がユーザー識別子“ｕｓｅｒ＿Ａ”であることを示している。なお認可リクエスト識別子“ａｕｔｈ＿ｒｅｑ＿ｉｄ＿１２３４５”の認可結果が“（空欄）”となっているのは、ユーザーがまだ認可操作を行っていないことを示している。それに対し認可リクエスト識別子“ａｕｔｈ＿ｒｅｑ＿ｉｄ＿９８７６５”の認可結果は“ａｐｐｒｏｖｅｄ”で、認可リクエスト識別子“ａｕｔｈ＿ｒｅｑ＿ｉｄ＿４４４４４”の認可結果は“ｄｉｓａｐｐｒｏｖｅｄ”である。これらはそれぞれ、ユーザーが認可を行ったことと、認可を拒否したことを示す認可確認の結果である。ステップＳ４１６で認可リクエスト管理部３１１は、ステップＳ４１１の応答として、ステップＳ４１４で生成した認可リクエスト識別子をクライアント２０３に返し、フローを終了する。

[0041] 図４Ｃは認可サーバー２０１における認可確認リクエストを行うフローで

ある。本フローはステップＳ４１３で認可リクエストの情報を記憶したことを受けて開始される。ステップＳ４２１で認可確認部３１３は、ステップＳ４１３で記憶した認可リクエスト識別子に紐付くクライアント識別子を取得する。

[0042] ここで、ステップＳ４１３で記憶した認可リクエスト識別子が“ａｕｔｈ＿ｒｅｑ＿ｉｄ＿１２３４５”であれば、紐付くクライアント識別子は“Ｃｌｉｅｎｔ＿１”、ヒント情報は“ｕｓｅｒ＿Ａ”である。ステップＳ４２２で認可確認部３１３は、ステップＳ４２１で取得したクライアント識別子とヒント情報から認可確認リクエストを行うユーザー端末を特定する。例えば、認可確認部３１３はクライアント識別子“Ｃｌｉｅｎｔ＿１”とヒント情報“ｕｓｅｒ＿Ａ”に紐づくユーザー端末として、認可確認リクエスト送信先解決部３１２内の表２ユーザー端末登録テーブルよりユーザー端末２０４を特定する。また、認可確認リクエストを通知する通信のエンドポイントは“１９２．１６８．０．１”であることが分かる。

[0043] ステップＳ４２３で認可確認部３１３は、ステップＳ４１３で記憶した認可リクエスト識別子に紐付くクライアント識別子およびスコープを取得する。ステップＳ４１３で記憶した認可リクエスト識別子が“ａｕｔｈ＿ｒｅｑ＿ｉｄ＿１２３４５”であれば、紐付くクライアント識別子およびスコープは“Ｃｌｉｅｎｔ＿１”および“ｇｅｔ－ｄａｔａ”である。

[0044] ステップＳ４２４で認可確認部３１３は、ステップＳ４２２で特定したユーザー端末２０４に対し、ステップＳ４２３で取得したクライアント識別子およびスコープを含めて認可確認リクエストを送信する。なお認可確認リクエストの送信方法は、ユーザー端末２０４のエンドポイントを指定した通信方法でもよいし、ＭＱＴＴをはじめとするＰＵＳＨ通知を用いた方法や、その他の方法でもよいが、本実施例では認可エンドポイントを指定した直接通信とする。ユーザー端末２０４の画面表示部３４４は、後述の図９Ｂに示すような認可確認画面を表示し、端末のユーザーに認可を求める。

[0045] ステップＳ４２５で認可確認部３１３は、ステップＳ４２４で送信した認

可確認リクエストの応答として、ユーザー端末２０４から認可結果を受信する。ステップＳ４２６で認可確認部３１３は、ステップＳ４２５で受信した認可結果を、ステップＳ４１５で記憶した認可リクエスト識別子に紐付けて記憶してフローを終了する。表４では、認可リクエスト識別子“ａｕｔｈ＿ｒｅｑ＿ｉｄ＿９８７６５”に対し認可されたことを示す“ａｐｐｒｏｖｅｄ”が記憶されている。以上がクライアントから権限委譲要求を行いユーザーにより認可操作されるまでのフローである。ＯＡｕｔｈ２．０と異なるのは、クライアントがユーザーの指示なく自律的に認可要求を行う点と、認可操作を行うユーザーはクライアントを操作する意思はなく、あくまで認可操作を行うか否かの意思決定にのみ関わるという点である。

[0046] 図５Ａは本実施の形態に係る、認可サーバー２０１がクライアント２０３に認可完了通知を行うフローである。本フローはステップＳ４２６で認可結果を記憶したことを受けた後で開始される。ステップＳ５０１で認可確認部３１３は、ステップＳ４２６で記憶した認可リクエスト識別子を取得する。ステップＳ５０２で認可確認部３１３は、ステップＳ５０１で取得した認可リクエスト識別子に紐付くクライアントの接続先情報であるクライアントエンドポイントを取得する。

[0047] 表５はクライアント識別子とクライアントエンドポイントの対応を管理する、クライアント管理テーブルの例である。

[0048] [表5]

クライアント管理テーブル

クライアント識別子	クライアントエンドポイント
Client_1	10.0.0.1
Client_2	10.0.1.1
Client_3	10.0.2.1

[0049] 表５では、クライアント識別子“Ｃｌｉｅｎｔ＿１”のクライアントエンドポイントが、“１０．０．０．１”であることを示している。ステップＳ５０３で認可確認部３１３は、ステップＳ５０２で取得したクライアントエ

ンドポイントに対し、ユーザーが認可したことを通知し、フローを終了する。なおここでクライアントエンドポイントに通知する内容は、ステップＳ５０１で取得した認可リクエスト識別子でもよく、またユーザーの認可に対応して発行したアクセストークンでもよい。アクセストークンを発行する際は後述の図５Ｃに示されるようなフローを実行する。

[0050] 図５Ｂは本実施の形態に係る、クライアント２０３が認可サーバー２０１にアクセストークンリクエストを行うフローである。本フローはクライアント２０３が認可サーバー２０１からステップＳ５０３の認可完了通知を受けて開始される。または本フローは、クライアント２０３が、定期的に実行してもよい。

[0051] ステップＳ５１１でアクセストークン要求部３３３は、アクセストークンリクエストを行う認可リクエスト識別子を決定する。ここで本フローが定期的に実行される場合には、認可リクエスト識別子は、表３に示される認可リクエスト管理テーブルでアクセストークン未取得のものから選ばれる。また本フローが認可サーバー２０１からの通知を受けて開始される場合は、認可サーバー２０１からの通知に含まれる認可リクエスト識別子が用いられる。ステップＳ５１２でアクセストークン要求部３３３は、ステップＳ５１１で決定した認可リクエスト識別子を指定して、認可サーバー２０１に対してアクセストークンリクエストを行う。ステップＳ５１３でアクセストークン管理部３３４は、ステップＳ５１２の応答として受信したアクセストークンを記憶してフローを終了する。表３では、認可リクエスト識別子“ａｕｔｈ＿ｒｅｑ＿ｉｄ＿９８７６５”に対して取得できた、アクセストークン“ａｃｔｋ１１１２２２３３３”を記憶している様子を示す。

[0052] 図５Ｃは本実施の形態に係る、認可サーバー２０１がアクセストークンを発行するフローである。本フローは認可サーバー２０１がクライアント２０３からアクセストークンリクエストを受信したことで開始される。

[0053] ステップＳ５２１でアクセストークン発行部３１４は、クライアント２０３から受信したアクセストークンリクエストから、認可リクエスト識別子を

取得する。ステップＳ５２２でアクセストークン発行部３１４は、アクセストークン発行可否を判断する。ステップＳ５２３でアクセストークン発行部３１４は、ステップＳ５２２の結果、アクセストークンを発行可能であると判断されたか確認する。

[0054] アクセストークンを発行可能と判断された場合はステップＳ５２４に遷移する。またアクセストークンを発行不可能と判断された場合はステップＳ５２５に遷移する。ステップＳ５２４でアクセストークン発行部３１４は、ステップＳ５２１で取得した認可リクエスト識別子に紐付けられたユーザー識別子およびスコープに対応するアクセストークンを発行する。また発行したアクセストークンをクライアント２０３に送信しフローを終了する。

[0055] 表６はアクセストークン発行部３１４で発行されたアクセストークンを管理する、アクセストークン管理テーブルの例である。

[0056] [表6]

アクセストークン管理テーブル

アクセストークン識別子	ユーザー識別子	スコープ
actk111222333	user_abcde	get-data

[0057] 表６では、ユーザー“ｕｓｅｒ＿ａｂｃｄｅ”がスコープ“ｇｅｔ－ｄａｔａ”の権限委譲を行ったことを示すアクセストークンが、アクセストークン識別子“ａｃｔｋ１１１２２２３３３”として発行されていることを示す。なお、ステップＳ５２４でクライアント２０３に返すアクセストークンはアクセストークン識別子だけでもよく、またアクセストークン識別子に加えユーザー識別子およびスコープを含む構造化されたデータでもよい。ステップＳ５２５でクセストークン発行モジュール３５４は、アクセストークンを発行できないことをクライアント２０３に通知してフローを終了する。

[0058] 図５Ｄは実施例１に係るアクセストークン発行可否判断を行うステップＳ５２２の詳細フローである。ステップＳ５３１でアクセストークン発行部３１４は、表４の認可確認状況管理テーブルを参照し、指定された認可リクエ

スト識別子に対応する認可結果を確認する。ステップＳ５３２でアクセストークン発行部３１４は、ステップＳ５３１の確認した認可結果が、認可されていることを表しているか判断する。認可されていることを表していた場合はステップＳ５３３に遷移し、その他の場合はステップＳ５３４に遷移する。ステップＳ５３３でアクセストークン発行部３１４は、アクセストークンを発行可能と判断してフローを終了する。ステップＳ５３４でアクセストークン発行部３１４は、アクセストークンを発行不可能と判断してフローを終了する。

[0059] 図６は権限委譲システムのシーケンス図である。クライアント２０３は認可サーバー２０１に対し認可開始リクエストを行い、応答として認可リクエスト識別子を取得する（Ｓ１）。認可開始リクエストはステップＳ４０１およびステップＳ４１１に対応する。

[0060] 認可サーバー２０１はリソース所有者の解決をすると、リソース所有者に紐付けられたユーザー端末２０４に対し認可確認リクエストを行う（Ｓ２）。ユーザー端末２０４では後述の図９Ｂに示すような認可確認画面が表示され、端末のユーザーが認可操作を行う。ユーザーが認可操作を行うと、ユーザー端末２０４は認可サーバー２０１に認可結果を送信する（Ｓ３）。Ｓ２はステップＳ４２４に、Ｓ３はステップＳ４２５に、それぞれ対応する。

[0061] 認可サーバー２０１が認可結果を受信した後、クライアント２０３が認可の完了とその内容を知る必要があるが、認可完了の通知には、クライアント２０３が認可サーバー２０１に確認する方法と認可サーバー２０１がクライアント２０３に通知する方法がある。前者の場合、クライアント２０３が定期的に認可サーバー２０１にアクセストークンリクエストを送信し（Ｓ４）、その応答として認可サーバー２０１が認可結果を返す。

[0062] この際、Ｓ３で許可が返されている場合、認可サーバーはリソースサーバーへのアクセストークンを発行して返し、Ｓ３で拒否が返されている場合は拒否されたことを示す結果を返す。なお、クライアント２０３は定期的にＳ４のリクエストを送信するため、未だＳ３の認可結果が返されていない場合

があるが、この場合は引き続き確認を継続する旨の結果を返す。後者は認可サーバー２０１がクライアント２０３に認可結果通知を送信する（Ｓ４’）。

[0063] 後者のケースはクライアント２０３が認可完了通知を受信するためのエンドポイントを持っている場合に行える方法となる。認可結果の内容は前者と同じで、許可された場合はアクセストークンを発行して渡し、拒否された場合は拒否されたことを示す結果を返す。Ｓ４はステップＳ５１２およびステップＳ５２１に、Ｓ４’はステップＳ５０３にそれぞれ対応する。クライアント２０３は、Ｓ４もしくはＳ４’で受信したアクセストークンを利用してリソースサーバー２０２にアクセスを行う（Ｓ５）。

[0064] このように、クライアント２０３とは物理的、システム的に離れたユーザーがクライアント２０３に権限委譲を行うことが可能となる。しかし、物理的、システム的に離れたことによって、認可を行うユーザーが再認可することができない課題が発生している。なぜなら、ユーザー端末２０４とクライアント２０３が密に連携しておらず疎であるため、ユーザー端末２０４を操作するユーザーはクライアント２０３を操作することも、ユーザー端末２０４からクライアント２０３へ再認可の要求を送ることも叶わないからである。

[0065] だが、ユーザーは認可操作を行なった後、認可操作を訂正したいと考える可能性もありうる。また、ユーザー端末、とりわけスマートフォンのような小型の端末では、情報の表示領域が少なく操作パネルも小さいため、ユーザーの認識違いによるミスや操作ミスが起こる可能性も高くなる。そのため、認可操作を再び行えるようにする必要性が出てくる。

[0066] 図７は権限委譲システムにおける再認可処理のシーケンス図である。ユーザー端末２０４が認可サーバー２０１に認可結果を送信する（Ｓ３）ところまでは図６と同様である。ここで、ユーザーが認可結果を訂正したい場合、ユーザーは図９Ｄに示すような再認可確認画面で再認可の操作を行うことができる。ユーザーが再認可操作を行うと、ユーザー端末２０４は認可サーバ

ー２０１に再認可結果を送信する（Ｓ３’）。再認可結果の内容は認可結果と同様である。なお、図６では、認可サーバー２０１における再認可結果受信（Ｓ３’）のエンドポイントを認可結果受信（Ｓ３）と分けているが、共通にする実装であってもよい。

[0067] シーケンス図のフローは図７の通りであるが、クライアント２０３がアクセストークンを使って行う処理は実施後の取り消しが難しい場合も想定される。従って、認可サーバー２０１がクライアント２０３への認可完了通知を待つ必要があるケースも考えられる。

[0068] 表７は、表４で示した認可リクエスト管理部３１１が記憶する認可確認状況管理テーブルに、認可期限を追加した例である。

[0069] [表7]

再認可可能な認可確認状況管理テーブル

認可リクエスト識別子	クライアント識別子	リソース	スコープ	ヒント情報	認可結果	認可期限
auth_req_id_12345	Client_1	/datalake/iot0010/data	get-data	user_A	disapproved	2019/10/08 10:32:48
auth_req_id_98765	Client_1	/datalake/iot0011/data	get-data	user_B	approved	2019/10/08 10:27:53
auth_req_id_44444	Client_2	/datalake/iot0011/data	get-all	user_abcde	(空欄)	(空欄)

[0070] 表７の一行目では、認可結果が“ｄｉｓａｐｐｒｏｖｅｄ”となっており、ユーザーからの認可結果が拒否であったことを示しているが、一方、認可期限である２０１９年１０月８日１０時３２分４８秒までは再認可が可能であることを示している。認可期限前にユーザーから再認可の指示を受信した場合、認可結果は更新される。つまり、ユーザーの認可操作の結果である認可結果は認可期限までバッファリングされる。ポイントは、バッファリングされている認可結果に基づく処理は実行されないという点である。たとえユーザーが認可したとしても、バッファリングされている間はアクセストークンが発行されない。

[0071] 表７の３行目は、未だ認可結果を受信していない状態となっているが、認可期限も設定されていない。これは認可期限が再認可待ちの時間を考慮して

設定されることを想定したもので、認可を受信してから再認可期限を算出して設定するためである。なお、認可期限の設定に関して認可結果を受信する前、例えば、認可リクエストを受信した時点で認可期限を設ける実装であってもよい。また、認可期限の間隔に関しては認可サーバー２０１の認可リクエスト管理部３１１に予め設定された値によって決定する実装や、クライアント２０３から認可開始リクエスト時に受信する実装などがあってもよい。さらに、認可期限は認可結果（Ｓ３）の応答で、ユーザー端末２０４に渡され、ユーザー端末の認可確認画面でも利用される。

[0072] 図８は再認可処理に関するフローチャートである。図８のフローチャートは認可サーバー２０１の認可確認部３１３、アクセストークン発行部３１４で実行される。図８Ａは、図７の認可結果の受信（Ｓ３）および再認可結果受信（Ｓ３’）のフローチャートで、図４Ｃで説明した認可結果の受信（Ｓ４２５）部分からのフローを示している。

[0073] 認可サーバー２０１の認可確認部３１３は、認可結果を受信すると該当する認可リクエスト識別子に紐付く情報に認可結果を保存する（Ｓ４２６）。そしてさらに、該当する認可リクエスト識別子に紐付く情報に認可期限が設定されているかを確認し（Ｓ８０１）、認可期限が設定されていない場合は、再認可が可能な期間を取得する（Ｓ８０２）。再認可が可能な期間は認可サーバー２０１の認可リクエスト管理部３１１に予め設定された値によって決定する実装や、クライアント２０３から認可開始リクエスト時に受信する実装などがあってもよい。そして、現在日時から再認可可能な期限となる日時を算出した上で（Ｓ８０３）、該当する認可リクエスト識別子の情報に期限を設定する（Ｓ８０４）。例えばＳ８０２で取得した値が３分であり、現在日時が２０１９年１０月８日１０時２９分４８秒であったとすると、期限は２０１９年１０月８日１０時３２分４８秒となる。つまり、認可結果は２０１９年１０月８日１０時３２分４８秒までバッファリングされる。なお、再認可を許容しない場合には、期限には現在日時が設定される。

[0074] 次に、認可サーバー２０１の認可確認部３１３は、完了通知が図７のＳ４

’で示す認可サーバー２０１側からクライアント２０３に通知するＰＵＳＨ型の方法かどうかを確認する（Ｓ８０５）。そしてＰＵＳＨ型の通知であれば、期限タイマーイベントを作成する（Ｓ８０６）。期限タイマーイベントは、期限の日時になった際にイベントを発行するもので、期限がきた時に認可サーバー２０１が図７のＳ４’で示す認可完了通知を行うために作成される。そして認可サーバー２０１は認可結果を受信した旨と共に、認可期限をユーザー端末２０４に返す（Ｓ８０７）。

[0075] 図８Ｂは、図７のアクセストークンリクエスト（Ｓ４）を受信した際の認可サーバー２０１のアクセストークンレスポンスフローチャートである。図５Ｃで説明したアクセストークンリクエストに該当する認可リクエスト識別子の情報を取得する（Ｓ５２１）部分からのフローを示している。該当する認可リクエスト識別子に紐付く情報を取得したら、認可結果が設定されているかを確認し（Ｓ８１１）、認可結果がない場合は未だ認可結果がきていないことをクライアント２０３に通知する（Ｓ８１２）。

[0076] 認可結果が設定されている場合は再認可期限を越えているかどうかを確認する（Ｓ８１３）。ここで、期限を越えていなかった場合、未だ認可結果がきていないことを通知して（Ｓ８１２）、ユーザーからの再認可確認を待つ。期限を越えていた場合は図５で示したように、認可結果を確認し（Ｓ５３１）、許可された場合（Ｓ５３２）はアクセストークンを発行して返し（Ｓ５２４）、拒否された場合はその旨を通知する（Ｓ５２５）。なお、図７のＳ４’で示した認可サーバー２０１からクライアント２０３へ認可完了通知を返す方法に関しては、図８ＡのＳ８０６で説明したイベントによって認可完了通知処理が開始される。

[0077] 図９はユーザー端末２０４で行う認可確認画面である。図９Ａは認可確認リスト画面、図９Ｂは認可確認画面、図９Ｃは認可履歴画面、図９Ｄは再認可確認画面である。ユーザー端末２０４上に認可確認を行うためのソフトウェアがインストールされており、ソフトウェアの画面を起動すると、図９Ａの認可確認リスト画面が表示される。

[0078] 図９Ａは認可確認リスト画面で、図７のＳ２で示す認可確認リクエストで受信した認可確認項目をリスト表示する。９０１は認可確認項目の一つで、受信日時、リソース情報など認可対象がわかる情報を表示している。リソース情報に関しては、表７で示しめしたリソース情報をそのまま全部または一部表示する実装の他、リソースに対してユーザーが名前を設定して表示するような実装であってもよい。認可確認項目９０１の右端にある“＞”は、図９Ｂで示す認可確認画面へ遷移するリンクである。９０２は、認可確認リスト画面と図９Ｃの認可履歴画面とを切替えるタブで選択されているタブがハイライトされている。

[0079] 図９Ｂは認可確認画面で、この画面で認可確認を行う。ＩＤ９１１は認可リクエスト識別子を示しており、認可する対象を一意に特定することができる。なお、ＩＤ９１１下の情報欄に関しては特に詳細は記載しないが、ユーザーが認可リクエストを識別するための補足情報をクライアント２０３や認可サーバー２０１から受信し表示するような実装が考えられる。許可ボタン９１２は認可確認に対して許可することを指示し、拒否ボタン９１３は認可を不許可とすることを指示するボタンである。ユーザーは、許可ボタン９１２または拒否ボタン９１３を押下することで認可操作を行うと、認可結果送信部３４２によって、図７のＳ３で示した認可結果の送信が行われる。

[0080] 図９Ｃは認可履歴画面で、過去の認可履歴をリストで参照することができる。図９Ｂで認可確認を行うと、認可履歴管理部３４３に履歴として保存され、過去の認可履歴を参照することができるようになる。９２１は認可履歴の一つで、認可確認を行った日時、リソースなど認可対象がわかる情報、認可結果を表示している。認可履歴９２１の右端にある“＞”は、図９Ｄで示す再認可確認画面へ遷移するリンクである。９２２も認可履歴の一つで表示される書誌情報は認可履歴９２１と同じであるが、グレー表示されると共に再認可確認画面へ遷移するリンクは表示されない。これは、対象となる認可確認項目の認可期限が切れたため、再認可操作が行えないことを示している。なお、認可履歴画面のリストに関しては対象となるリソースに絞る等のフ

ィルタリング機能を持った実装があってもよい。

[0081] 図９Ｄは再認可確認画面である。表示される情報は図９Ｂの認可確認画面と同様であるが、再認可期限９３１を表示している。９３２は認可操作を行うボタンで、前回の認可確認で行った操作が拒否であったため、再認可では前回の操作を取り消す許可ボタンが表示される。逆に、前回の認可確認で行った操作が許可であった場合、認可操作ボタン９３２は拒否ボタンが表示される。なお、再認可確認画面でも図９Ｂのように許可ボタンと拒否ボタン両方を表示する実装であってもよい。

[0082] 再認可確認画面で認可確認を再度行うと、認可結果送信部３４２によって、図７のＳ３’で示した認可結果の送信が行われる。再認可確認は期限内であれば何度でもユーザーは再認可の操作ができる実装であってよいし、再認可操作の回数に制限を設ける実装であってもよい。例えば、クライアント２０３から送信される認可開始リクエストにその回数を含めることでクライアント２０３からの要求で回数を指定することなどが考えられる。さらに、許可あるいは拒否のどちらかが行われたら再認可できなくなるといった制限を設ける実装であってもよい。

[0083] 図１０Ａは、図９Ｃで述べた認可履歴画面のフローチャートである。本フローチャートはユーザー端末２０４で実行される。ソフトウェアの画面を起動すると、図９Ａの認可確認リスト画面が表示されるが、そこで画面切替えタブ９０２で図９Ｃの認可履歴画面に切替えられたところから処理が開始される（Ｓ１００１）。

[0084] まず、画面表示部３４４は、認可履歴管理部３４３から認可履歴を取得する（Ｓ１００２）。そして、取得した履歴の中から期限が過ぎていない認可履歴すなわち再認可操作が可能な履歴について（Ｓ１００３）、期限となる日時から現在日時を差し引いて残時間の算出を行う（Ｓ１００４）。そして、期限に達した際に起動するタイマーイベントを作成する（Ｓ１００５）。次に画面表示部３４４は、ユーザー端末２０４のディスプレイ装置１１４に図９Ｃで述べた認可履歴画面を表示する（Ｓ１００６）。

[0085] 認可履歴画面では、図９Ｃで述べたように、再認可操作が可能な認可履歴は図９Ｄの再認可確認画面へのリンクを表示し、認可期限を過ぎた認可履歴はリンクを表示しない。その後は画面操作やＳ１００５で作成した期限イベントを待ち（Ｓ１００７）、イベントを受信したらその内容に応じた処理を実施する（Ｓ１００８）。期限イベントを受信した場合は認可履歴画面を描画して表示内容を更新する（Ｓ１００９）。画面を更新したことによって、画面表示において、期限に達した認可履歴から再認可確認画面へのリンクがなくなる。イベント受信で図９の９２１にある認可履歴リスト項目のリンクをクリックしたイベントを受信した場合、選択された認可履歴の項目の再認可確認画面へ遷移する（Ｓ１０１０）。図９の９０２で説明した認可確認タブをクリックしたイベントを受信した場合、認可確認リスト画面へ遷移する（Ｓ１０１１）。

[0086] 図１０Ｂは、図１０Ａ内の認可履歴描画のサブフローチャートである。認可履歴の数分内容を確認し（Ｓ１０２１）、期限が過ぎているかどうかを判定（Ｓ１０２２）、期限が過ぎていなければ再認可画面へ遷移するリンクを入れたリスト項目を表示する（Ｓ１０２３）。期限を過ぎていた場合は再認可画面へ遷移するリンクは入れずにリスト項目を表示する（Ｓ１０２４）。

[0087] 以上、実施例１では、ユーザーが認可操作を訂正したい場合あるいは認識違いによるミスや操作ミスが起こった場合に、認可確認の再操作を行うことが可能となる。

[0088] ［実施例２］

実施例１では認可サーバー２０１で認可確認の再操作を可能とする時間だけ待ち処理を行う実施例を示した。しかし、再認可を許容するかどうか、待ち処理による応答の遅延を許容するかどうかは、クライアント２０３がリソースサーバー２０２に対して行う処理内容に関係すると考えられる。例えば、対面での商品購入の決済に端末を使った認可フローを行うようなケースでは、待ち処理を行う必要はない。そのため、認可サーバー２０１が待ち処理を行うと、クライアント２０３にとっては不都合な場合もある。

[0089] そのような課題が考えられる場合、クライアント２０３が認可開始リクエストを行う際（Ｓ４０１）に再認可を許容するかどうか、応答期限はどのくらいか、といった指示を含めることができるようにする実装も必要となる。なお、実施例２においても権限委譲システムにおける再認可処理のシーケンスは実施例１と同様であり、説明を省略している部分は実施例１と同じ構成や処理となる。

[0090] 図１１は認可開始リクエストで送付される情報を示している。“ｓｃｏｐｅ”は、クライアント２０３がリソースサーバー２０２に対して行う処理に必要となる権限範囲を示し、“ｈｉｎｔ”はヒント情報を示す。“ｒｅｔｒｙ”は、再認可が可能かどうかを示す。ｔｒｕｅであれば再認可は可能、ｆａｌｓｅであれば再認可は不可能となる。なお、実施例２では再認可可否の値を示したが再認可の回数などを指定するような実装であってもよい。“ｅｘｐｉｒｅｓ＿ｉｎ”は認可の期限を示し、１８００の場合は１８００秒以内に認可を行う必要があることを示す。なお、図１１には上記の４項目を例示しているが、これに限らなくてもよい。例えば、図７のＳ４’で認可完了通知を出す場合にはクライアントのエンドポイントの情報を含める必要があったり、ユーザー端末等で表示するためのメッセージ文字列を含めたりする実装であってもよい。

[0091] 表８は、表７で示した認可リクエスト管理部３１１が記憶する認可確認状況管理テーブルに、クライアント２０３から渡される再認可の可否や応答期限といった指示を保管する領域を追加したものである。表７で示したクライアント識別子、リソース、スコープは省略している。

[0092]

[表8]

再認可に関する指示を指定した認可確認状況管理テーブル

認可リクエスト識別子	・・・	ヒント情報	再認可	期限（秒）	認可結果	認可期限
auth_req_id_12345	・・・	user_A	true	1800	disapproved	2019/10/08 10:32:48
auth_req_id_98765	・・・	user_B	false	300	(空欄)	2019/10/08 10:27:53
auth_req_id_67890	・・・	user_C	false	(空欄)	(空欄)	(空欄)
auth_req_id_44444	・・・	user_abcde	true	(空欄)	approved	(空欄)

[0093] 表８の一行目では、再認可が“ｔｒｕｅ”となっており、再認可可能であることを示す。また応答期限が“１８００”となっており、認可サーバー２０１からの認可完了通知まで１８００秒待つことが可能な指示となっている。認可サーバー２０１は、認可リクエストを受信すると現在日時に応答期限を加えた日時を認可期限に設定する。ただし、図７のＳ４で示したアクセストークンリクエストに対して認可完了通知を応答する場合、クライアントからのポーリング間隔も考慮して認可期限を設定する必要がある。次のポーリングまでの間隔は認可開始リクエストＳ１やアクセストークンリクエストＳ４の応答で指定することはできるが、処理のオーバヘッドも考慮して少し短く設定するような実装も考えられる。Ｓ４’のように認可サーバー２０１からクライアント２０３に応答を返す場合であっても、処理のオーバヘッドも考慮して少し短く設定するような実装が考えられる。

[0094] 表８の二行目では、再認可が“ｆａｌｓｅ”となっており、再認可を許容しないリクエストであることを示す。また応答期限が“３００”となっており、認可サーバー２０１からの認可完了通知まで３００秒待つことが可能な指示となっている。すなわち、この認可期限は再認可のための期限ではなく、最初の認可までの期限となる。例えば、対面での商品購入の決済に端末を使った認可フローを行うようなケースでは、待ち処理を行う必要はなく、応答も即座に返されるため応答期限は短く設定されている。認可サーバー２０

１は、認可リクエストを受信すると現在日時に応答期限を加えた日時を認可期限に設定する。また、再認可が不可であるため、認可サーバー２０１は、図７のＳ３でユーザー端末２０４から認可結果を受信すると、受信したときの日時を認可期限に設定する。再認可が可能な期間は認可確認の結果はバッファリングされアクセストークンの発行制御はすぐには行われない。

[0095] 表８の三行目では、再認可が“ｆａｌｓｅ”となっており、再認可を許容しないリクエストであることを示す。また応答期限は指定されていない。この場合、認可サーバー２０１は、認可リクエストを受信した際に認可期限の設定は行わず、図７のＳ３でユーザー端末２０４から認可結果を受信すると、受信したときの日時を認可期限に設定してもよい。再認可のためのバッファリングは行われないのが三行目の場合の特徴である。なお、表８の二行目と三行目はバッファリングを行うか否かで差異はあるが、どちらもユーザーは再認可することはできない。

[0096] 表８の四行目では、再認可が“ｔｒｕｅ”、期限は設定されておらず、再認可可能で期限も存在しないことを示す。このようなユースケースは少ないと思われるが、クライアント２０３がリソースサーバー２０２に対して行う処理が何度でも再実行可能な処理であり、特に期限も設定しないケースが考えられる。この場合、認可サーバー２０１は、認可リクエストを受信した際に認可期限の設定は行わず、図７のＳ３でユーザー端末２０４から認可結果を受信しても、認可期限は設定しない。

[0097] 図１２は実施例２における認可結果受信のフローチャートである。図１２のフローチャートは認可サーバー２０１の認可確認部３１３、アクセストークン発行部３１４で実行される。図１２は、図７の認可結果の受信（Ｓ３）および再認可結果受信（Ｓ３’）のフローチャートで、図４Ｃで説明した認可結果の受信（Ｓ４２５）部分からのフローを示している。

[0098] 認可サーバー２０１の認可確認部３１３は、認可結果を受信すると該当する認可リクエスト識別子に紐付く情報に認可結果を保存する（Ｓ４２６）。認可サーバー２０１の認可確認部３１３は、完了通知が図７のＳ４’で示す

認可サーバー２０１側からクライアント２０３に通知するＰＵＳＨ型の方法かどうかを確認する（Ｓ１２０１）。そして再認可期限が設定されているかどうかを確認する（Ｓ１２０２）。実施例１では再認可期限を設定するフローを説明したが、実施例２では再認可期限が設定されない場合もある。再認可期限が設定されている場合は、対象となる認可リクエスト識別子の完了通知を行うための期限タイマーイベントが既に存在しているかを確認し（Ｓ１２０３）、存在しなければ期限タイマーイベントを作成する（Ｓ１２０４）。完了通知がＰＵＳＨ型で再認可期限が設定されていない場合は、即時に認可完了通知を行うことになる。

[0099] 認可サーバー２０１のアクセストークン発行部３１４は認可結果を確認する（Ｓ５３１）。許可された場合（Ｓ５３２）はアクセストークンを発行して返し（Ｓ５２４）、拒否された場合はその旨を通知する（Ｓ５２５）。なお、即時に認可完了通知を行うのではなく、認可完了通知を行うためのイベントあるいはキューを作成して、別処理として認可完了通知を行う実装であってもよい。

[0100] そして、認可サーバー２０１の認可確認部３１３は前記表８の再認可列の値を参照して、対象となる認可リクエスト識別子の認可が再認可可能かどうかを確認し（Ｓ１２０５）、認可結果を受信した旨と共に、認可期限をユーザー端末２０４に返す（Ｓ１２０６）。また、表８の再認可列で示した再認可が可能かどうかの情報もＳ１２０６でユーザー端末に返してもよい。なお、Ｓ１２０４でタイマーイベントを作成している場合は、タイマーイベントの起動によって認可完了通知処理が開始される。

[0101] 図１３は、実施例２における図７のアクセストークンリクエスト（Ｓ４）を受信した際の認可サーバー２０１のアクセストークンレスポンスフローチャートである。図１３のフローチャートは認可サーバー２０１のアクセストークン発行部３１４で実行される。図１３のフローチャートは、図５Ｃで説明したアクセストークンリクエストに該当する認可リクエスト識別子の情報を取得する（Ｓ５２１）部分からのフローを示している。

[0102] 該当する認可リクエスト識別子に紐付く情報を取得したら、認可結果が設定されているかを確認する（Ｓ８１１）。認可結果がない場合、再認可期限を越えていないかどうかを確認し（Ｓ１３０１）、再認可期限を越えていない場合は未だ認可結果がきていないことをクライアント２０３に通知する（Ｓ８１２）。再認可期限を越えていた場合は認可が行われなかったことを通知する（Ｓ１３０２）。実施例１において、再認可期限の設定は認可が一度行われた場合に設定する例を示したが、実施例２では認可開始リクエスト受信時に設定されるため、認可が行われずに期限を越える場合もありうる。

[0103] Ｓ８１１で認可結果が設定されている場合は再認可期限を越えているかどうかを確認する（Ｓ８１３）。ここで、期限を越えていなかった場合、未だ認可結果がきていないことを通知して（Ｓ８１２）、ユーザーからの再認可確認を待つ。期限を越えていた場合は図５で示したように、認可結果を確認する（Ｓ５３１）。許可された場合（Ｓ５３２）はアクセストークンを発行して返し（Ｓ５２４）、拒否された場合はその旨を通知する（Ｓ５２５）。

[0104] 図１４のフローチャートは、図１０Ｂで説明したユーザー端末２０４上の画面表示部３４４で実行される認可履歴描画のフローチャートを、実施例２における再認可処理のフローに対応したものである。Ｓ１０２１からＳ１０２４のステップは図１０と同じであるが、ステップＳ１４０１で期限が設定されているかどうかの判定が行われている。

[0105] 図８Ａで説明したように、再認可が可能な場合は再認可可能な期間を上乗せした日時を期限に設定し、再認可を許可しない場合は現在日時を期限に設定する実装例を示した。実施例２の再認可処理のフローでは再認可期限が設定されない場合もありうる。期限が設定されない場合は認可サーバー２０１から期限情報は渡されず、履歴情報にも期限が設定されていない状態となる。期限が設定されていない場合、再認可画面へ遷移するリンクを入れたリスト項目を表示する（Ｓ１０２３）。なお、この場合、図９Ｄで示した９３１の期限は表示されない。

[0106] また、実施例２では表８の再認可列で再認可が可能かどうかを判断する情

報もある。Ｓ１２０６で受信した再認可が可能かどうかの情報を使って、再認可が不可であった場合は、図９Ｂの画面に再認可ができない旨の注記を表示したり、９１２または９１３のボタン押下時に確認のダイアログボックスを表示したりする実装であってもよい。

[0107] 以上、クライアント２０３側で再認可を許容するかどうか、待ち処理による応答の遅延を許容するかどうかの指示を行うことが可能となる。その結果、例えば対面での商品購入の決済に端末を使った認可フローを行うようなケースでは、待ち処理を行う必要はなくなるのでアクセストークンの発行を早期に行うことができる。その一方で、ユーザーが一度行った認可操作を訂正したいケースでは、再認可ができる。

[0108] ［その他の実施例］

実施例１および２では、認可結果を一時的に記憶する形態として、ＲＡＭの中に用意された専用記憶領域を使ったバッファリングを説明したが、バッファリングではなくとも一時的に記憶する形態であればどのような記憶方法であっても良い。例えば、永続記憶領域に認可確認の結果を記憶し、後で消去するような一時的な記憶方法が考えられる。

[0109] 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。

[0110] 本発明は上記実施の形態に制限されるものではなく、本発明の精神及び範囲から離脱することなく、様々な変更及び変形が可能である。従って、本発明の範囲を公にするために以下の請求項を添付する。

[0111] 本願は、２０１９年１１月１９日提出の日本国特許出願特願２０１９－２０８９９４を基礎として優先権を主張するものであり、その記載内容の全てをここに援用する。

請求の範囲

[請求項1] ユーザーのリソースを提供するリソースサーバー、前記リソースへアクセスするクライアント、前記クライアントが前記リソースへアクセスすることがユーザーにより許可されたことを示すアクセストークンを発行する認可サーバー、およびユーザー端末とから構成されるシステムにおける前記認可サーバーであって、

前記クライアントから認可開始リクエストを受信する受信手段と、

前記受信手段により認可開始リクエストが受信されたことに応じて、認可確認リクエストの送信先となるユーザー端末を特定する特定手段と、

特定されたユーザー端末に対して認可確認リクエストを送信し、応答として認可確認の結果を受信し、再認可が可能な期間まで前記認可確認の結果を一時的に記憶する認可手段と、

再認可が可能な期間を超えたことに応じて一時的に記憶されている前記認可確認の結果に応じたアクセストークンの発行の制御を行い、前記アクセストークンを発行した場合は前記認可開始リクエストを送信した前記クライアントへ前記アクセストークンを送信する発行手段と、を有することを特徴とする認可サーバー。

[請求項2] 前記発行手段は、再認可が可能な期間を超えたことに応じて一時的に記憶されている前記認可確認の結果を確認し、前記アクセストークンを発行しない場合、再認可が可能な期間を超えてから拒否された旨を前記クライアントへ送信することを特徴とする請求項１に記載の認可サーバー。

[請求項3] 前記認可手段は、前記クライアントから再認可の指示を受け付けた場合、一時的に記憶している前記認可確認の結果を前記再認可の指示に基づき更新することを特徴とする請求項１または２に記載の認可サーバー。

[請求項4] 前記期間は、前記認可確認の結果を受信した日時とあらかじめ設定

された値から算出した値、もしくは前記クライアントが送信する前記認可開始リクエストで指定された値によって設定されることを特徴とする請求項１乃至３の何れか１項に記載の認可サーバー。

[請求項5] 前記受信手段により受信された認可開始リクエストが再認可は不可能であることを示すリクエストであった場合、前記発行手段は、再認可が可能な期間を超えるのを待たずに前記認可確認の結果に応じたアクセストークンの発行の制御を行うことを特徴とする請求項４に記載の認可サーバー。

[請求項6] 前記受信手段により受信された認可開始リクエストが再認可は不可能であることを示すリクエストであった場合、前記認可手段は受信した認可確認の結果を一時的に記憶しないことを特徴とする請求項５に記載の認可サーバー。

[請求項7] 前記受信手段により受信された認可開始リクエストが再認可は可能であることを示すリクエストであった場合、認可結果を受信した旨とともに認可期限を前記ユーザー端末へ送信することを特徴とする請求項５または６に記載の認可サーバー。

[請求項8] ユーザーのリソースを提供するリソースサーバー、前記リソースへアクセスするクライアント、前記クライアントが前記リソースへアクセスすることがユーザーにより許可されたことを示すアクセストークンを発行する認可サーバー、およびユーザー端末とから構成されるシステムであって、

前記クライアントから認可開始リクエストを受信する受信手段と、

前記受信手段により認可開始リクエストが受信されたことに応じて、認可確認リクエストの送信先となるユーザー端末を特定する特定手段と、

特定されたユーザー端末に対して認可確認リクエストを送信する送信手段と、

前記認可確認リクエストの認可確認項目を表示し、前記認可確認リ

クエストに対する許可もしくは不許可の指示を受け付ける第１の受付手段と、

前記認可確認リクエストの応答として認可確認の結果を受信し、再認可が可能な期間まで前記認可確認の結果を一時的に記憶する認可手段と、

前記認可確認リクエストに対する許可もしくは不許可の指示を受け付けた後、再認可の指示を受け付ける第２の受付手段と、

再認可が可能な期間を超えたことに応じて一時的に記憶されていた前記認可確認の結果に応じたアクセストークンの発行の制御を行い、前記アクセストークンを発行した場合は前記認可開始リクエストを送信した前記クライアントへ前記アクセストークンを送信する発行手段と、を有することを特徴とするシステム。

[請求項9] 前記第２の受付手段は、再認可が可能な期間を超えた前記認可確認リクエストに対する再認可の指示を受け付けないことを特徴とする請求項８に記載のシステム。

[請求項10] ユーザーのリソースを提供するリソースサーバー、前記リソースへアクセスするクライアント、前記クライアントが前記リソースへアクセスすることがユーザーにより許可されたことを示すアクセストークンを発行する認可サーバー、およびユーザー端末とから構成されるシステムで実行される方法であって、

前記クライアントから認可開始リクエストを受信する受信ステップと、

前記受信ステップにより認可開始リクエストが受信されたことに応じて、認可確認リクエストの送信先となるユーザー端末を特定する特定ステップと、

特定されたユーザー端末に対して認可確認リクエストを送信する送信ステップと、

前記認可確認リクエストの認可確認項目を表示し、前記認可確認リ

クエストに対する許可もしくは不許可の指示を受け付ける第１の受付ステップと、

前記認可確認リクエストの応答として認可確認の結果を受信し、再認可が可能な期間まで前記認可確認の結果を一時的に記憶するステップと、

前記認可確認リクエストに対する許可もしくは不許可の指示を受け付けた後、再認可の指示を受け付ける第２の受付ステップと、

再認可が可能な期間を超えたことに応じて一時的に記憶されていた前記認可確認の結果に応じたアクセストークンの発行の制御を行い、前記アクセストークンを

発行した場合は前記認可開始リクエストを送信した前記クライアントへ前記アクセストークンを送信する発行ステップと、を含むことを特徴とする方法。

[請求項11] ユーザーのリソースを提供するリソースサーバー、前記リソースへアクセスするクライアント、前記クライアントが前記リソースへアクセスすることがユーザーにより許可されたことを示すアクセストークンを発行する認可サーバー、およびユーザー端末とから構成されるシステムにおける前記認可サーバーで実行されるプログラムであって、

前記クライアントから認可開始リクエストを受信させる受信ステップと、

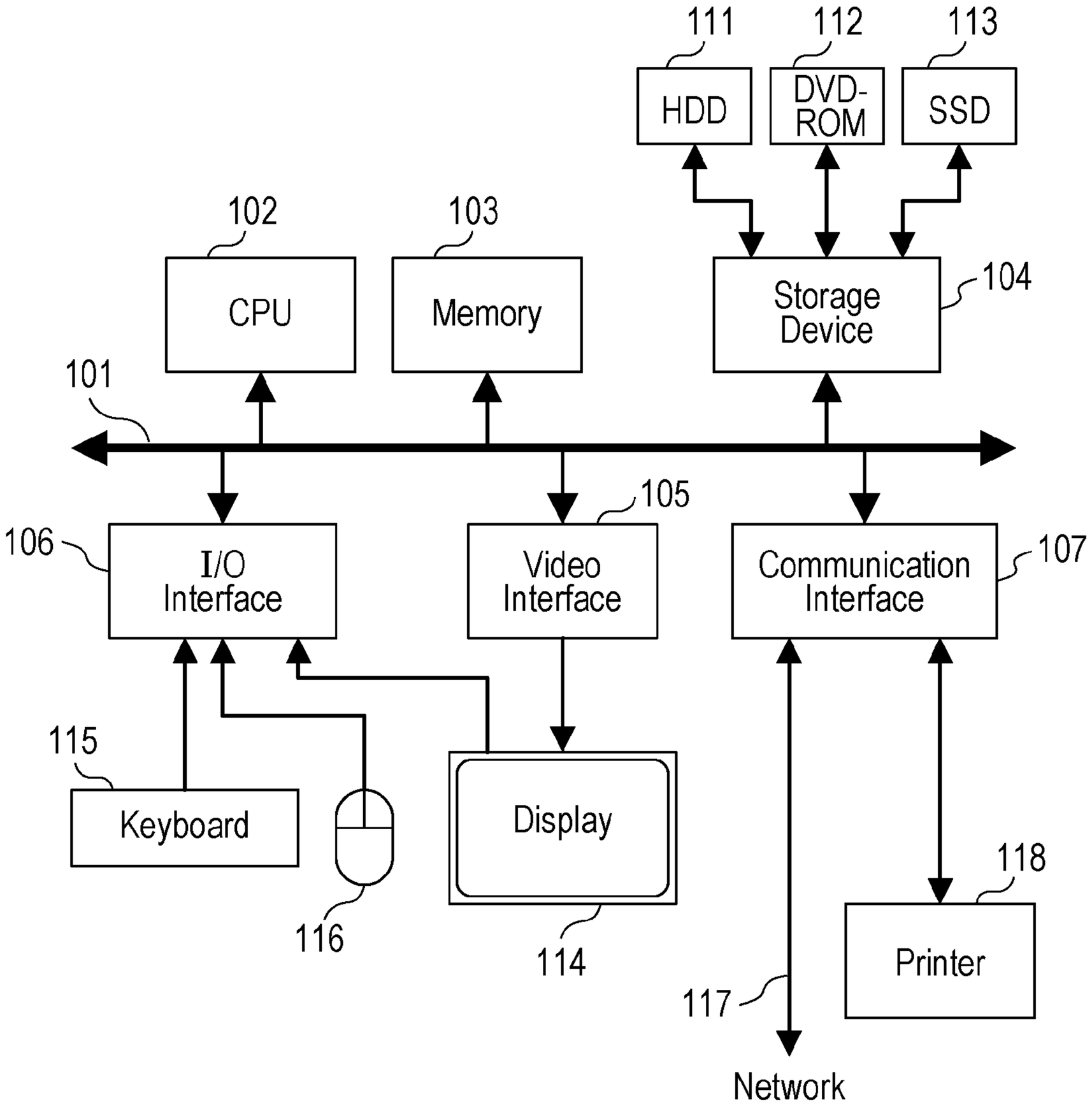
前記受信ステップによって認可開始リクエストが受信されたことに応じて、認可確認リクエストの送信先となるユーザー端末を特定させる特定ステップと、

特定されたユーザー端末に対して認可確認リクエストを送信させ、応答として認可確認の結果を受信させ、再認可が可能な期間まで前記認可確認の結果を一時的に記憶させる認可ステップと、

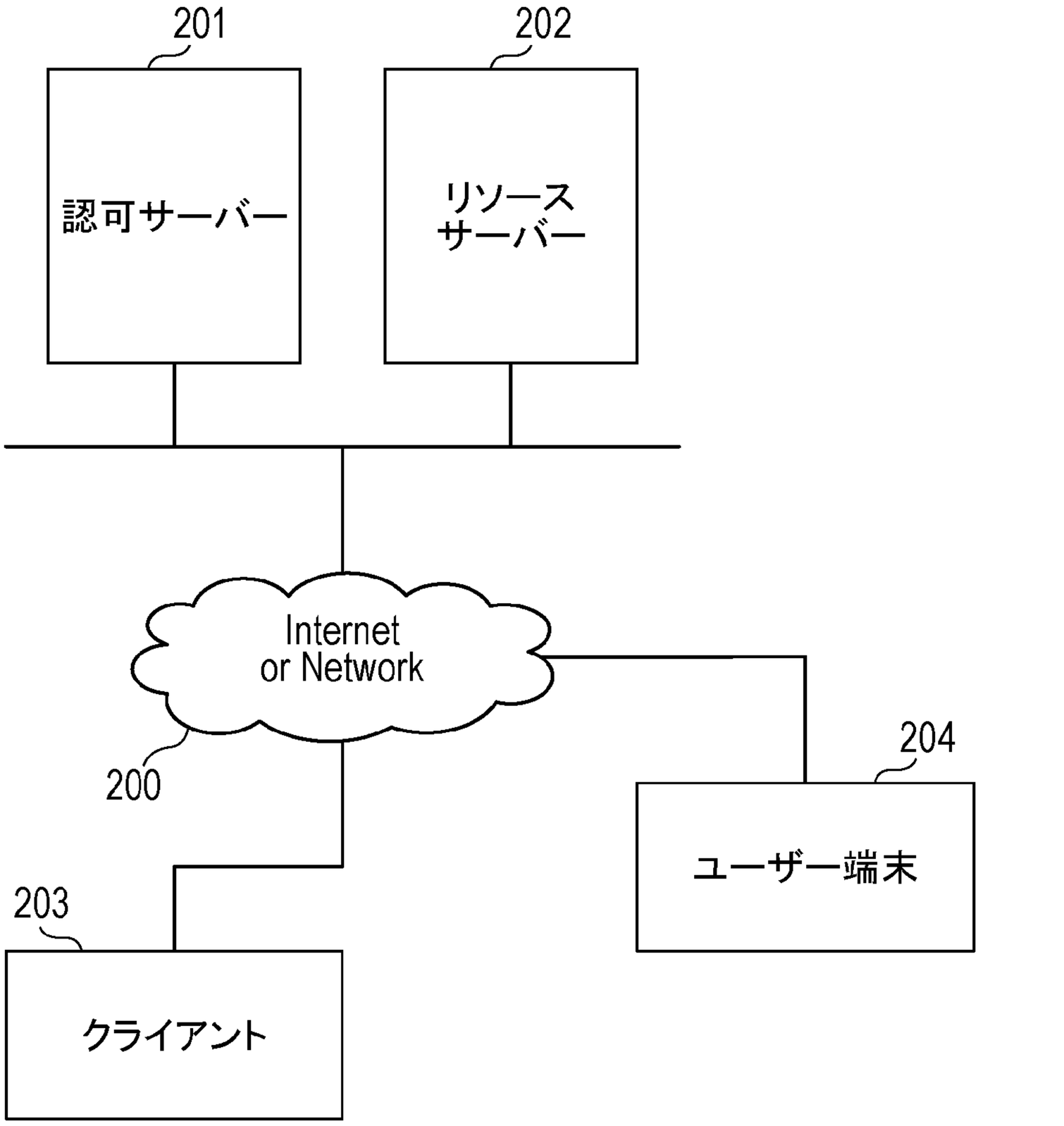
再認可が可能な期間を超えたことに応じて一時的に記憶されていた前記認可確認の結果に応じたアクセストークンの発行の制御を行わせ

、前記アクセストークンを発行した場合は前記認可開始リクエストを送信した前記クライアントへ前記アクセストークンを送信させる発行ステップと、を含むプログラム。

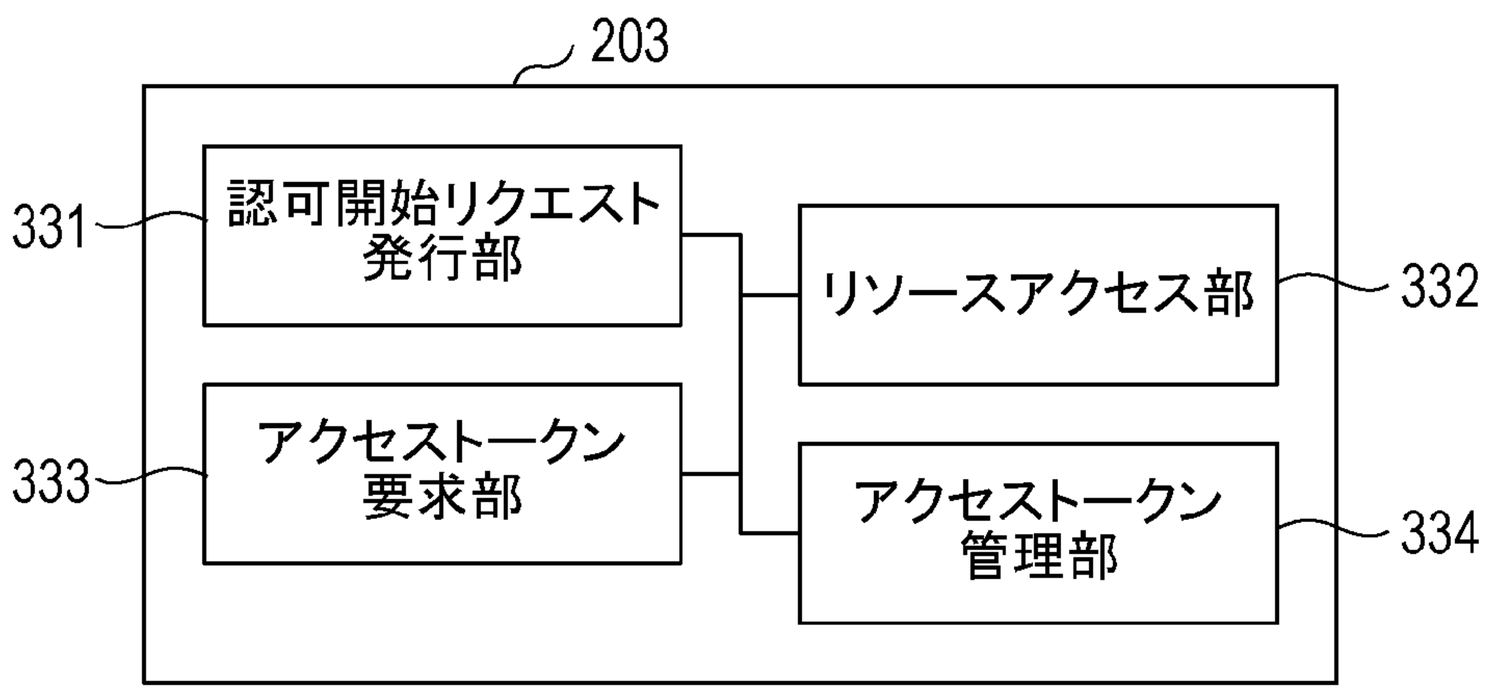
[図1]


111
112
113
HDD
DVD-ROM
SSD
102
103
CPU
Memory
Storage Device
104
101
105
106
I/O Interface
Video Interface
Communication Interface
107
115
Keyboard
Display
118
116
114
Printer
117
Network

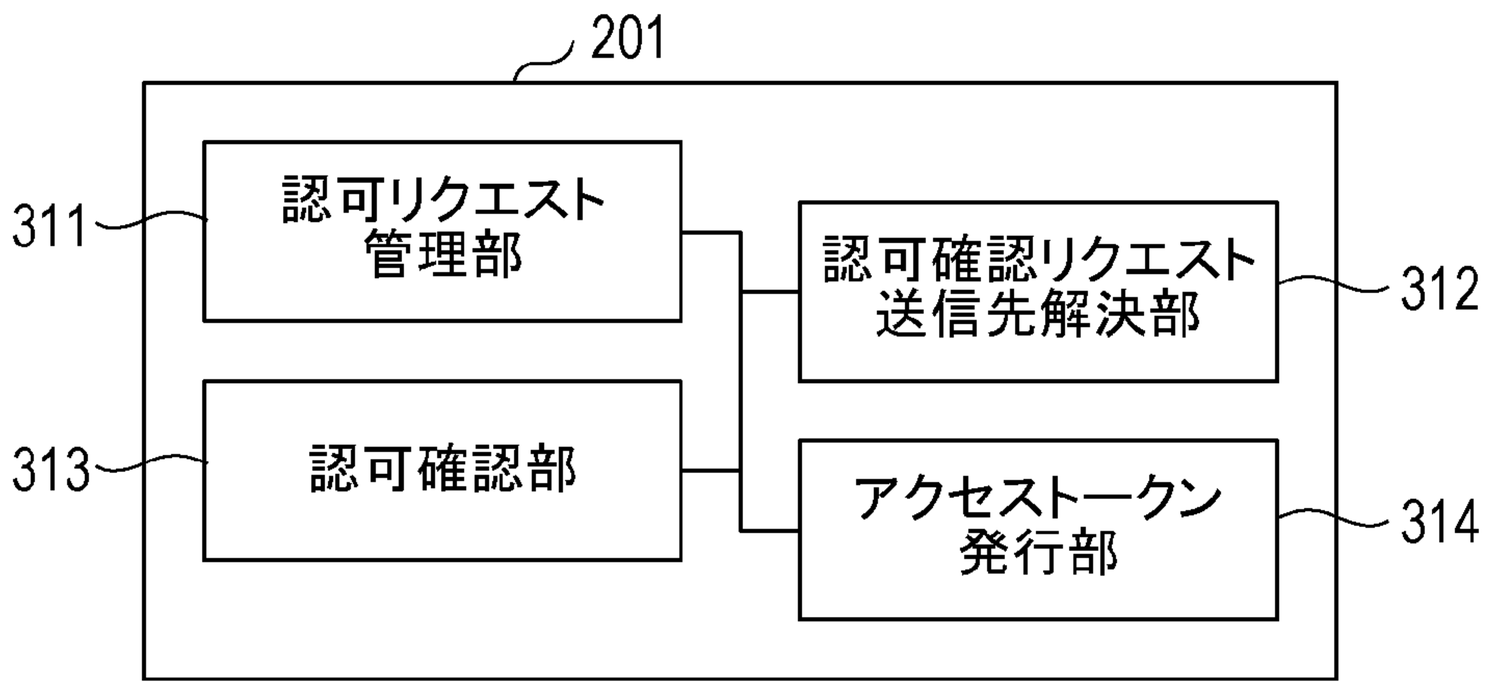
[図2]


201
202
認可サーバー
リソース
サーバー
Internet
or Network
200
204
ユーザー端末
203
クライアント

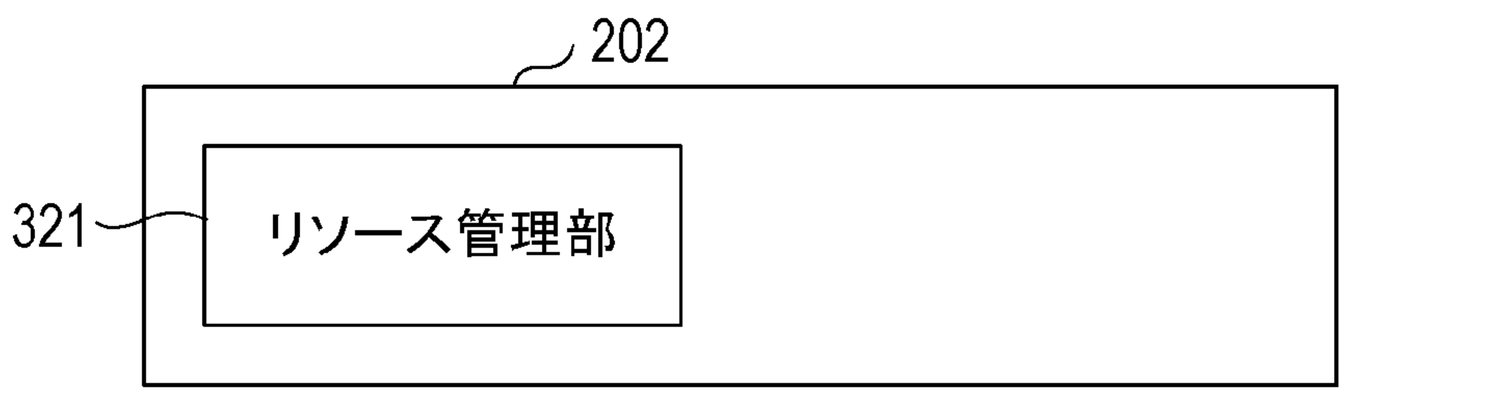
[図3A]


203
331
認可開始リクエスト
発行部
リソースアクセス部
332
333
アクセストークン
要求部
アクセストークン
管理部
334

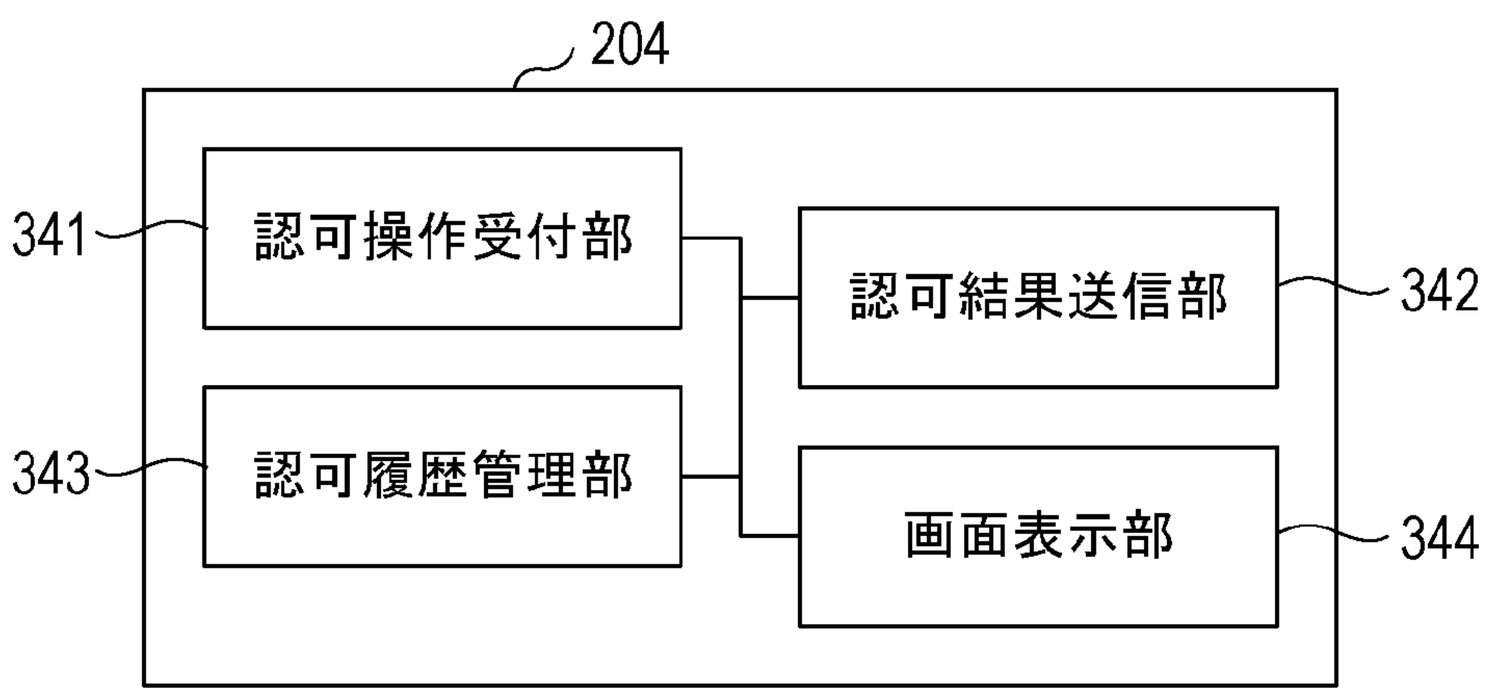
[図3B]


201
311
認可リクエスト
管理部
認可確認リクエスト
送信先解決部
312
313
認可確認部
アクセストークン
発行部
314

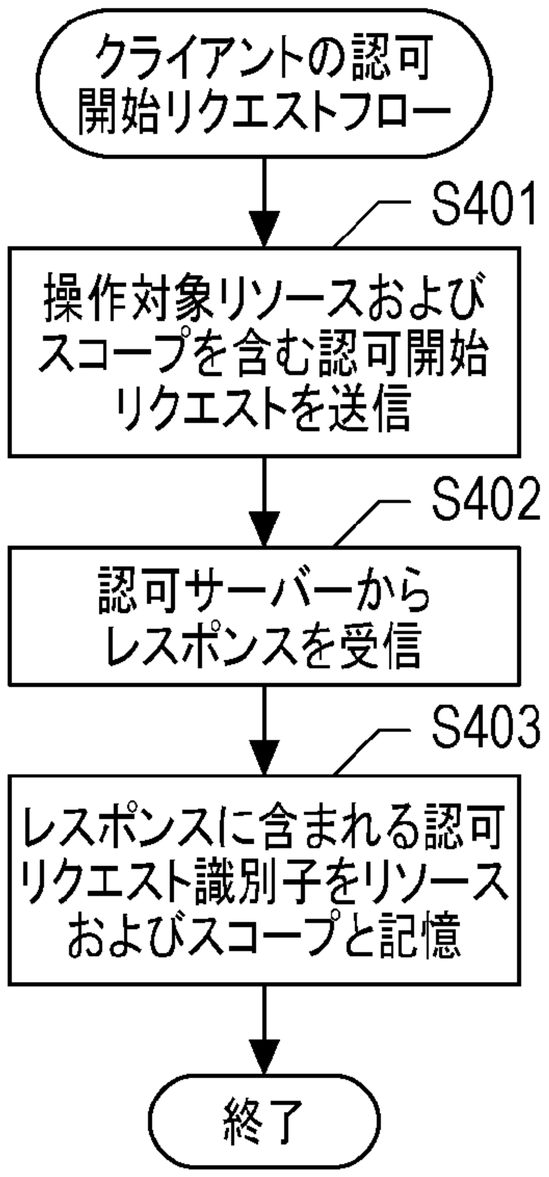
[図3C]


202
321
リソース管理部

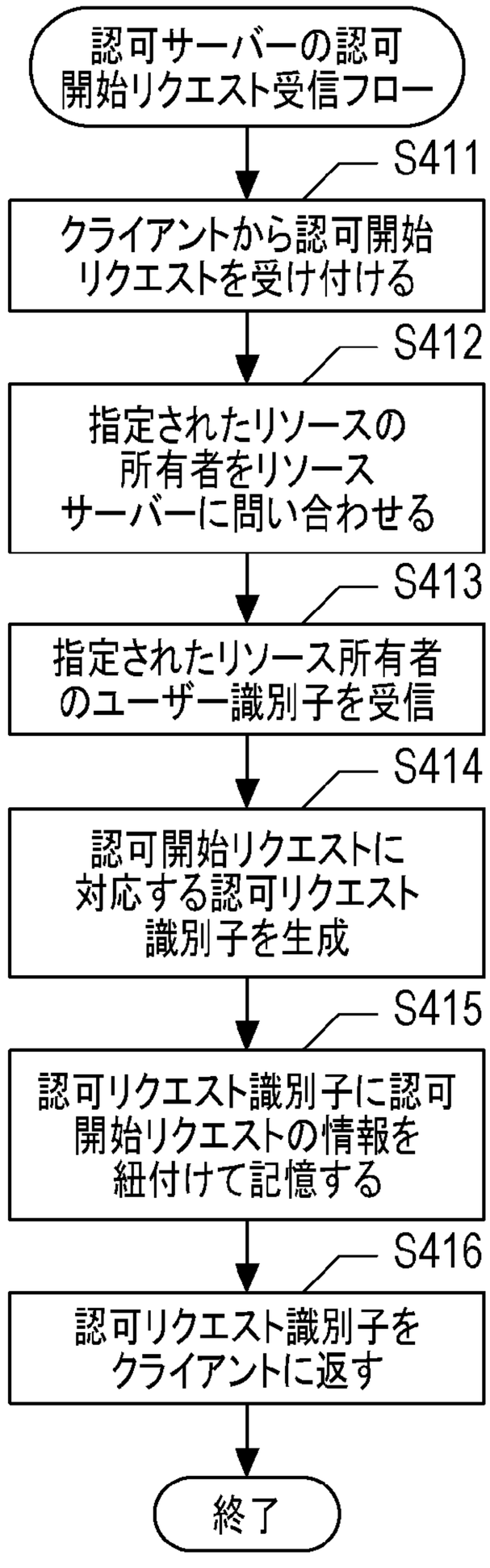
[図3D]


204
341
認可操作受付部
認可結果送信部
342
343
認可履歴管理部
画面表示部
344

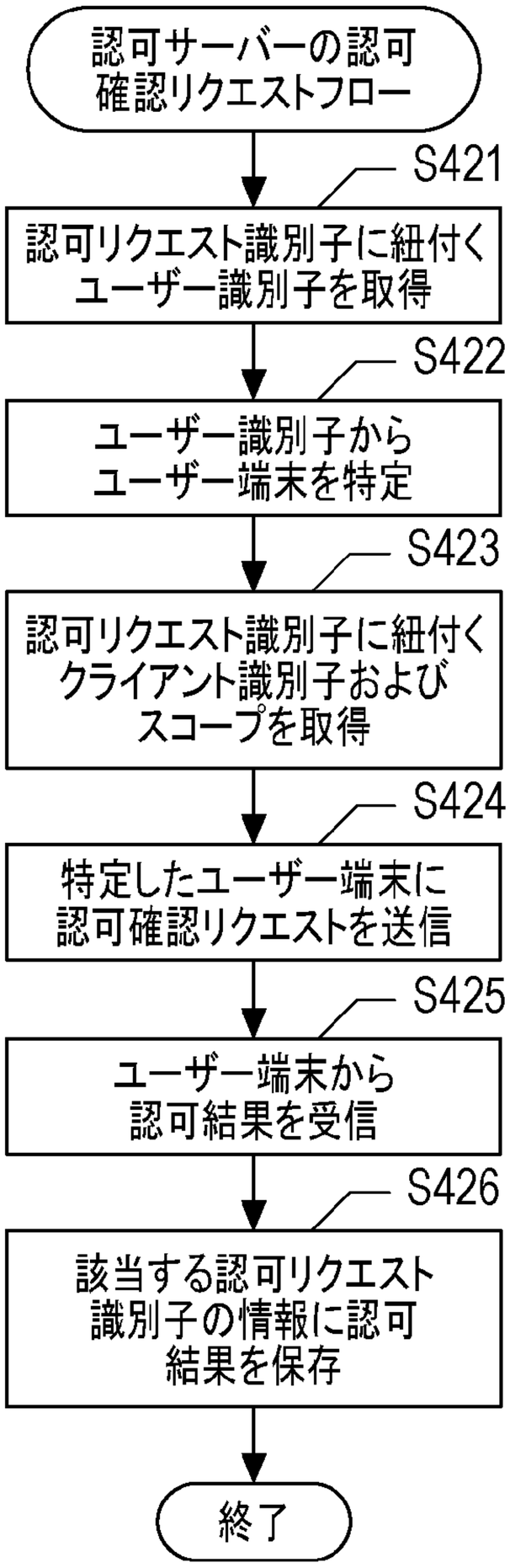
[図4A]


クライアントの認可
開始リクエストフロー
S401
操作対象リソースおよび
スコープを含む認可開始
リクエストを送信
S402
認可サーバーから
レスポンスを受信
S403
レスポンスに含まれる認可
リクエスト識別子をリソース
およびスコープと記憶
終了

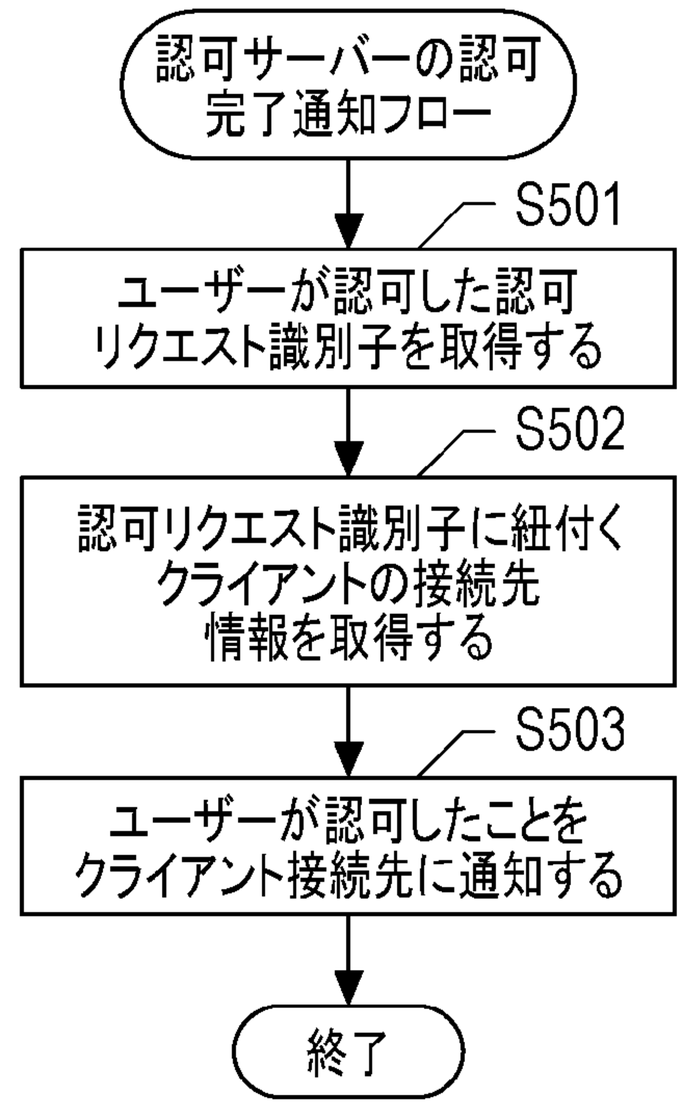
[図4B]


認可サーバーの認可
開始リクエスト受信フロー
S411
クライアントから認可開始
リクエストを受け付ける
S412
指定されたリソースの
所有者をリソース
サーバーに問い合わせる
S413
指定されたリソース所有者
のユーザー識別子を受信
S414
認可開始リクエストに
対応する認可リクエスト
識別子を生成
S415
認可リクエスト識別子に認可
開始リクエストの情報を
紐付けて記憶する
S416
認可リクエスト識別子を
クライアントに返す
終了

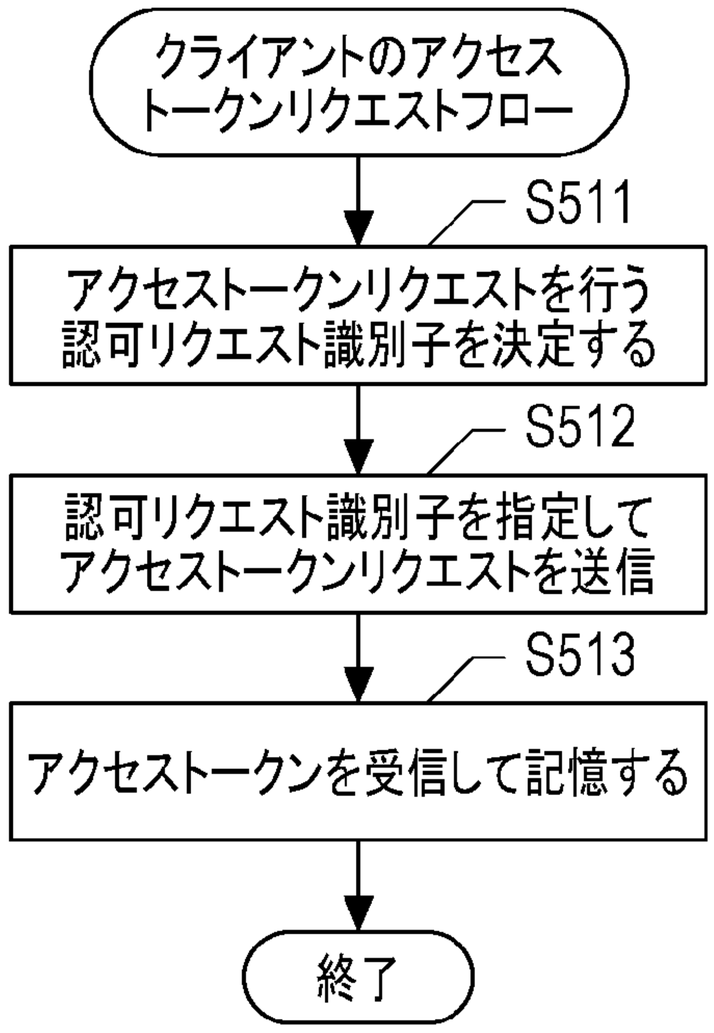
[図4C]


認可サーバーの認可
確認リクエストフロー
S421
認可リクエスト識別子に紐付く
ユーザー識別子を取得
S422
ユーザー識別子から
ユーザー端末を特定
S423
認可リクエスト識別子に紐付く
クライアント識別子および
スコープを取得
S424
特定したユーザー端末に
認可確認リクエストを送信
S425
ユーザー端末から
認可結果を受信
S426
該当する認可リクエスト
識別子の情報に認可
結果を保存
終了

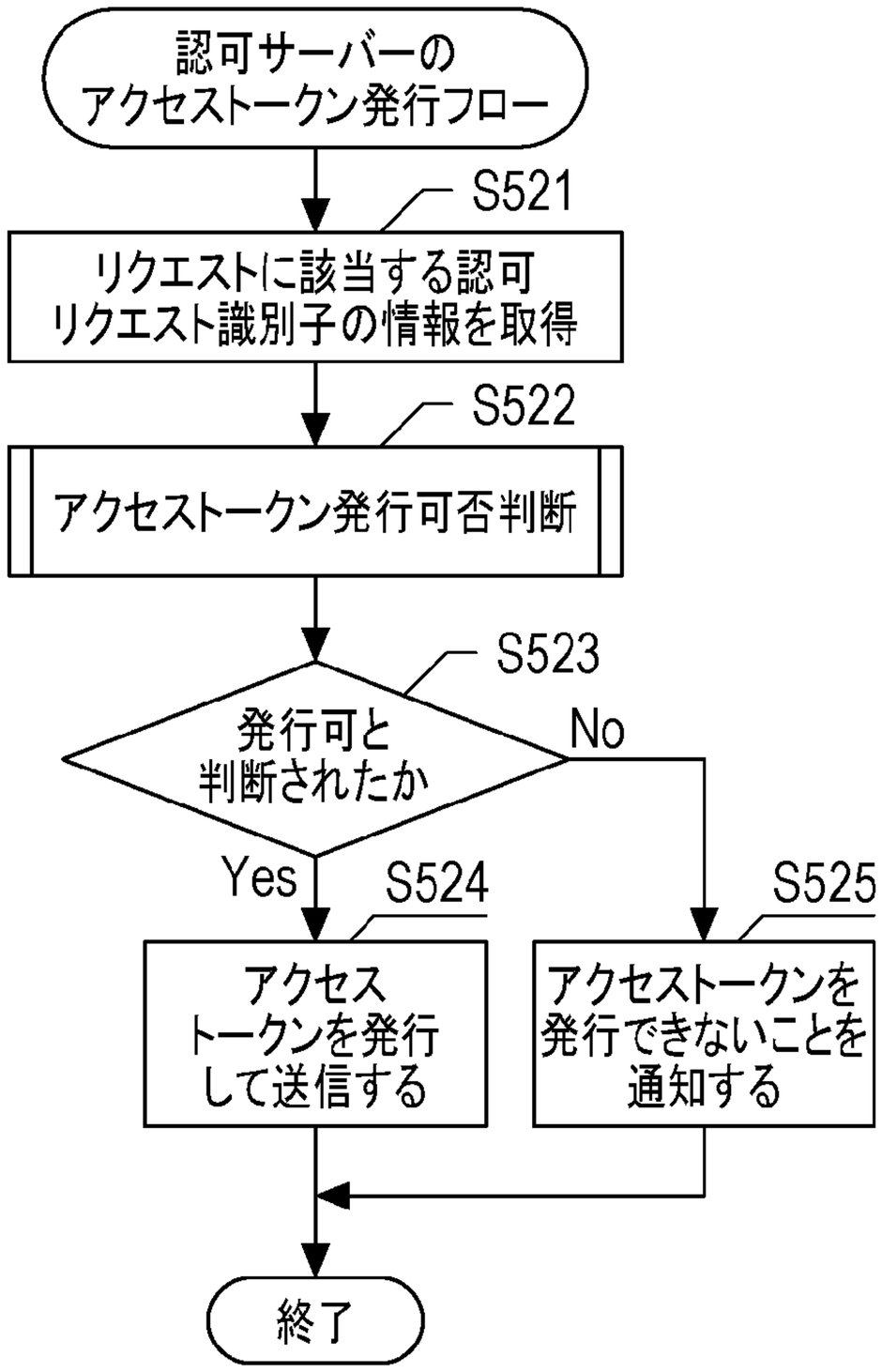
[図5A]


認可サーバーの認可
完了通知フロー
S501
ユーザーが認可した認可
リクエスト識別子を取得する
S502
認可リクエスト識別子に紐付く
クライアントの接続先
情報を取得する
S503
ユーザーが認可したことを
クライアント接続先に通知する
終了

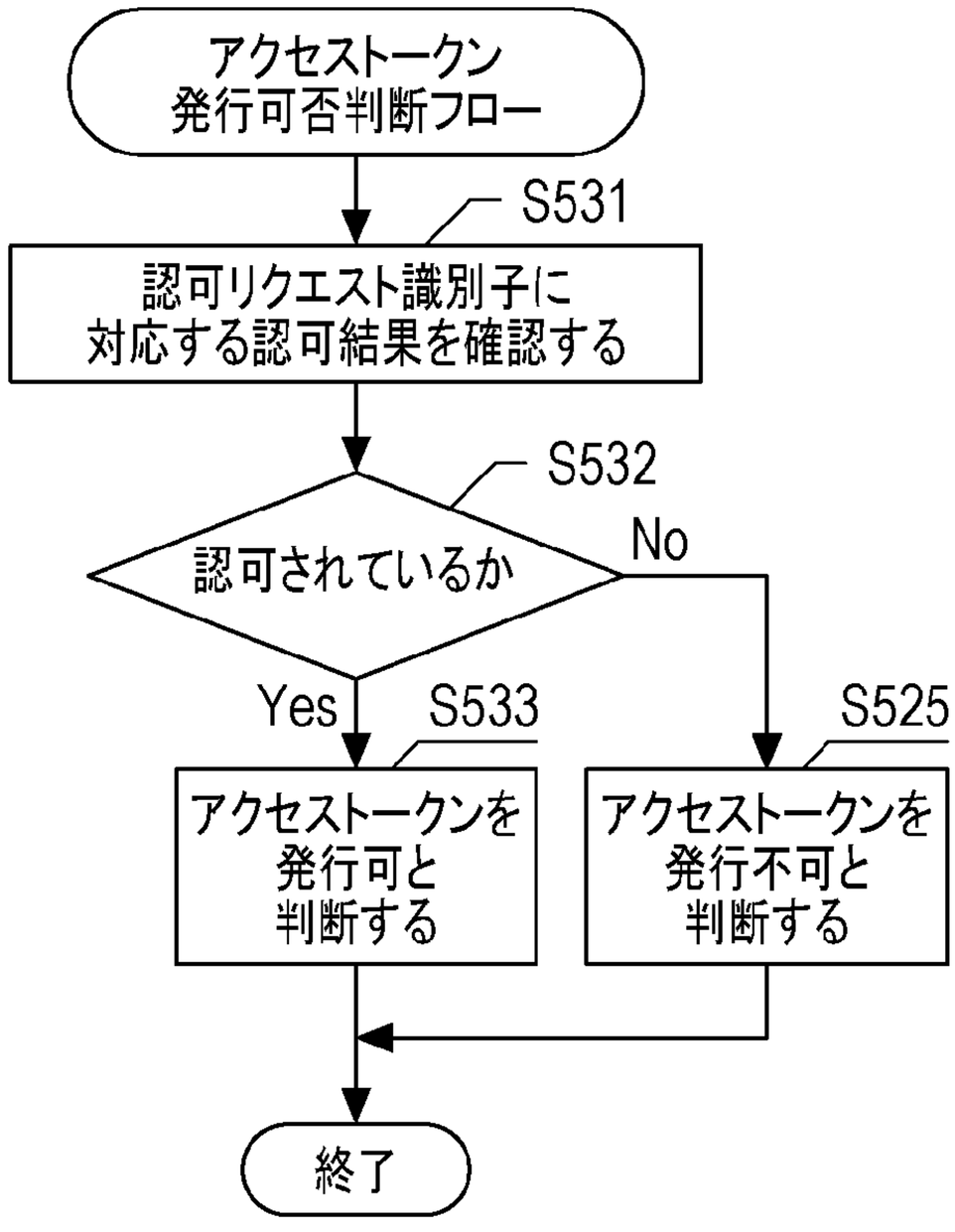
[図5B]


クライアントのアクセス
トークンリクエストフロー
S511
アクセストークンリクエストを行う
認可リクエスト識別子を決定する
S512
認可リクエスト識別子を指定して
アクセストークンリクエストを送信
S513
アクセストークンを受信して記憶する
終了

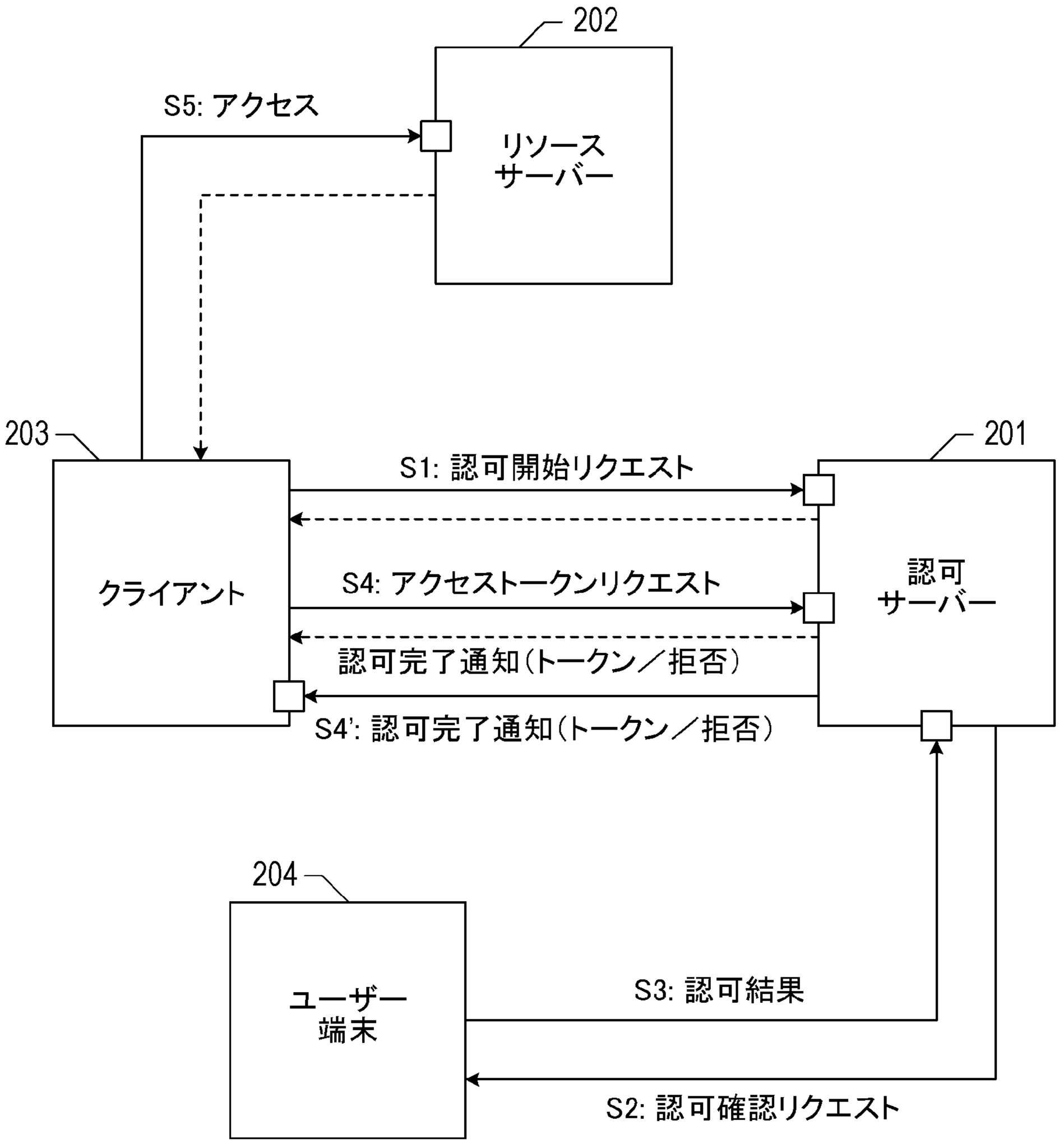
[図5C]


認可サーバーの
アクセストークン発行フロー
S521
リクエストに該当する認可
リクエスト識別子の情報を取得
S522
アクセストークン発行可否判断
S523
発行可と
判断されたか
No
Yes
S524
アクセス
トークンを発行
して送信する
S525
アクセストークンを
発行できないことを
通知する
終了

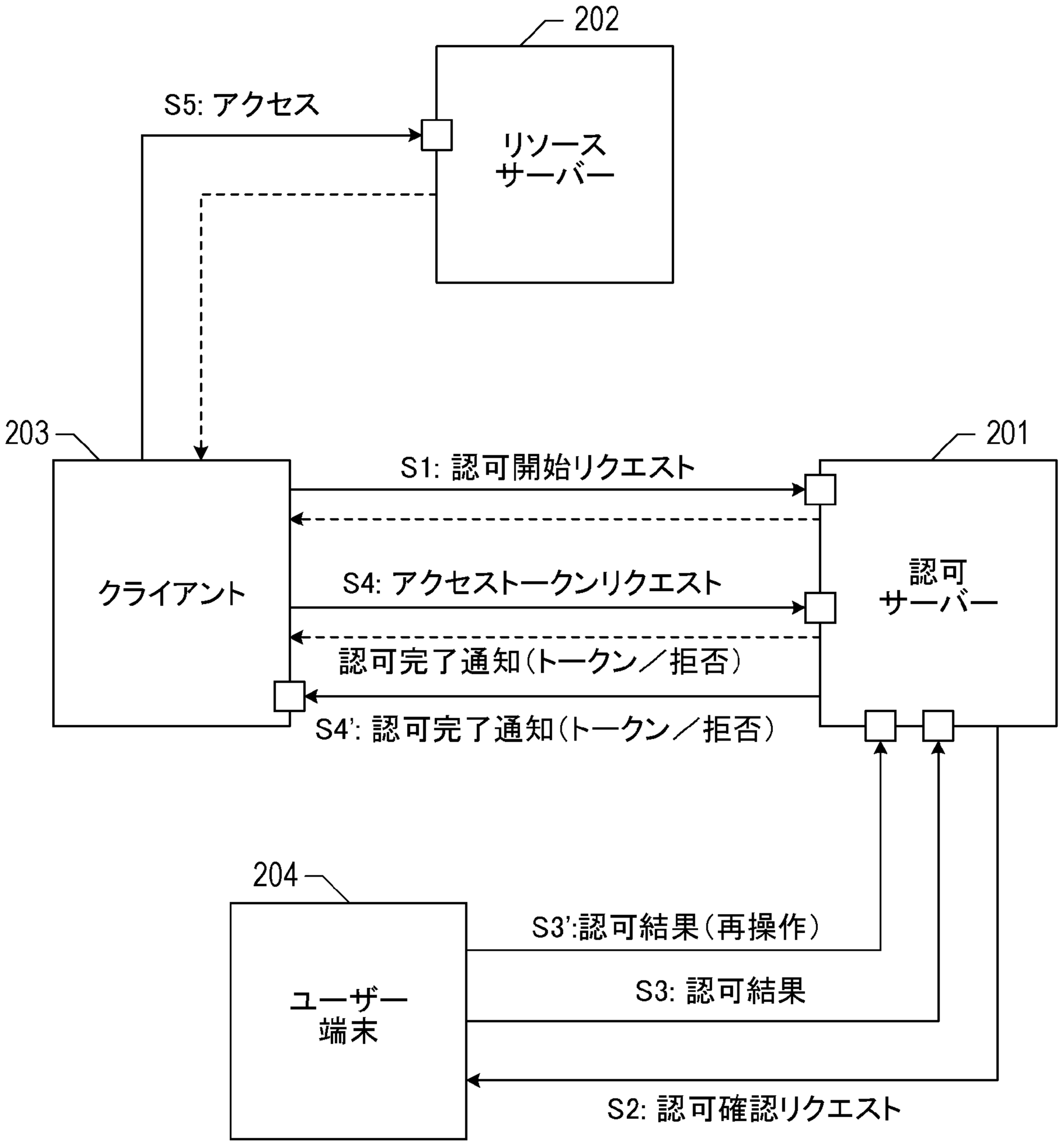
[図5D]


アクセストークン
発行可否判断フロー
S531
認可リクエスト識別子に
対応する認可結果を確認する
S532
認可されているか
No
Yes
S533
アクセストークンを
発行可と
判断する
S525
アクセストークンを
発行不可と
判断する
終了

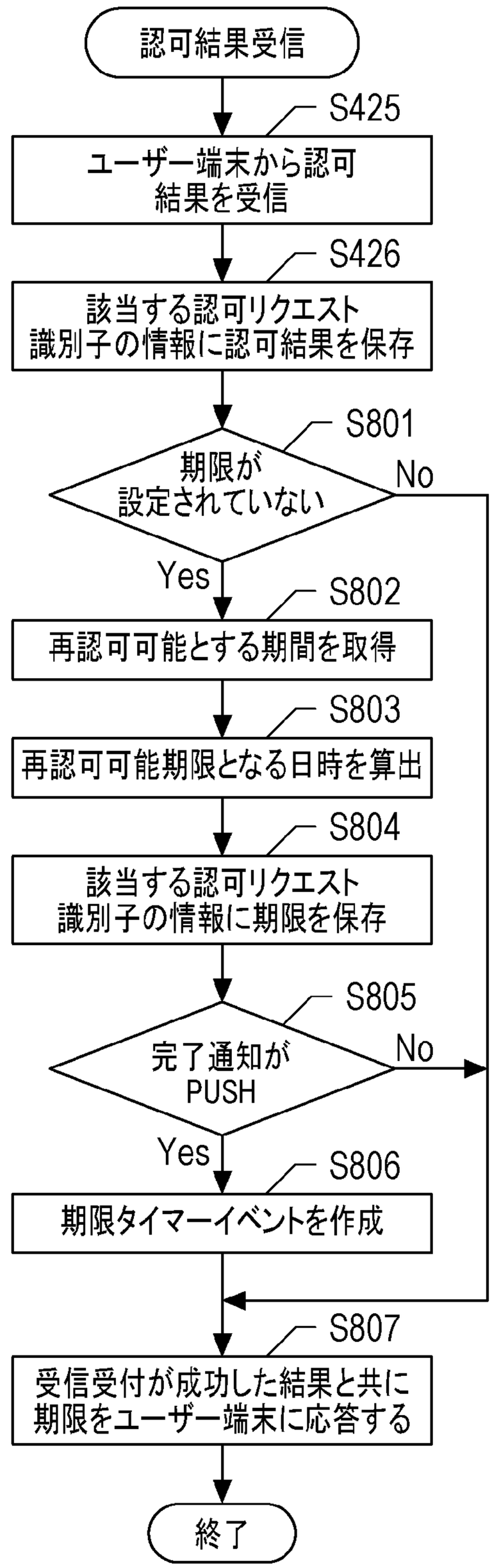
[図6]


202
S5: アクセス
リソース
サーバー
203
201
S1: 認可開始リクエスト
クライアント
S4: アクセストークンリクエスト
認可
サーバー
認可完了通知(トークン／拒否)
S4': 認可完了通知(トークン／拒否)
204
ユーザー
端末
S3: 認可結果
S2: 認可確認リクエスト

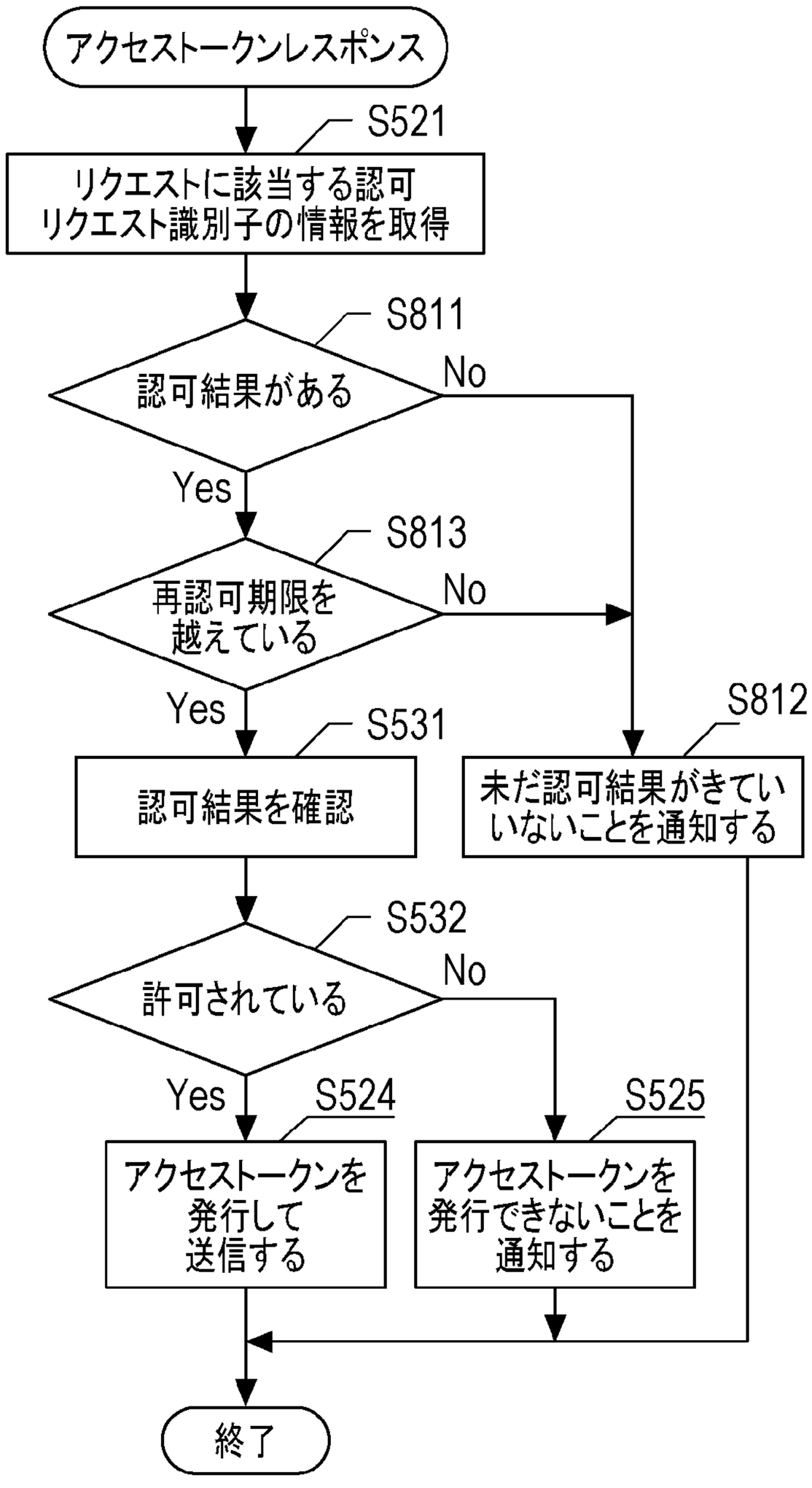
[図7]


202
S5: アクセス
リソース
サーバー
203
201
S1: 認可開始リクエスト
クライアント
S4: アクセストークンリクエスト
認可
サーバー
認可完了通知(トークン／拒否)
S4': 認可完了通知(トークン／拒否)
204
S3':認可結果(再操作)
ユーザー
端末
S3: 認可結果
S2: 認可確認リクエスト

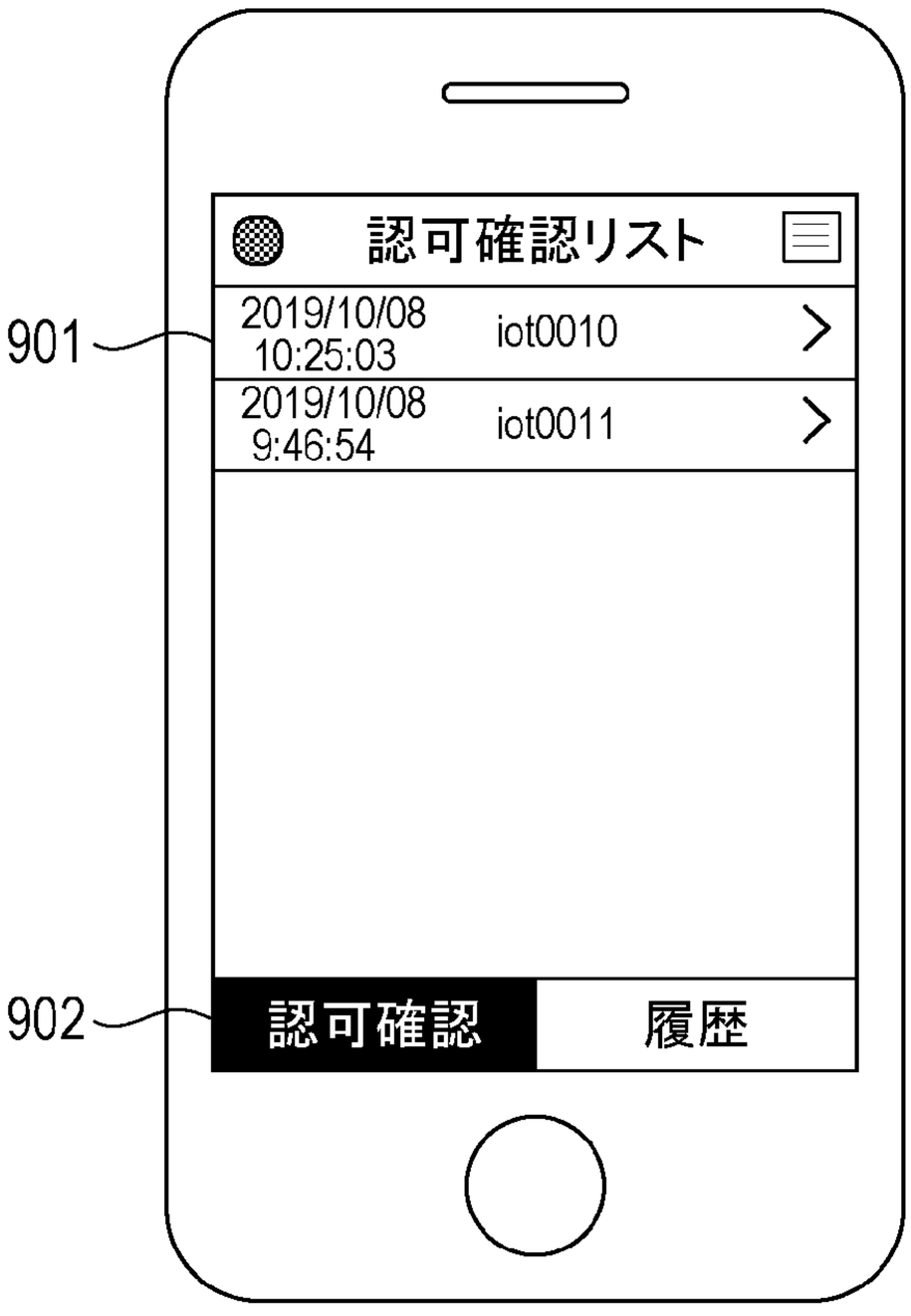
[図8A]


認可結果受信
S425
ユーザー端末から認可
結果を受信
S426
該当する認可リクエスト
識別子の情報に認可結果を保存
S801
期限が
設定されていない
No
Yes
S802
再認可可能とする期間を取得
S803
再認可可能期限となる日時を算出
S804
該当する認可リクエスト
識別子の情報に期限を保存
S805
完了通知が
PUSH
No
Yes
S806
期限タイマーイベントを作成
S807
受信受付が成功した結果と共に
期限をユーザー端末に応答する
終了

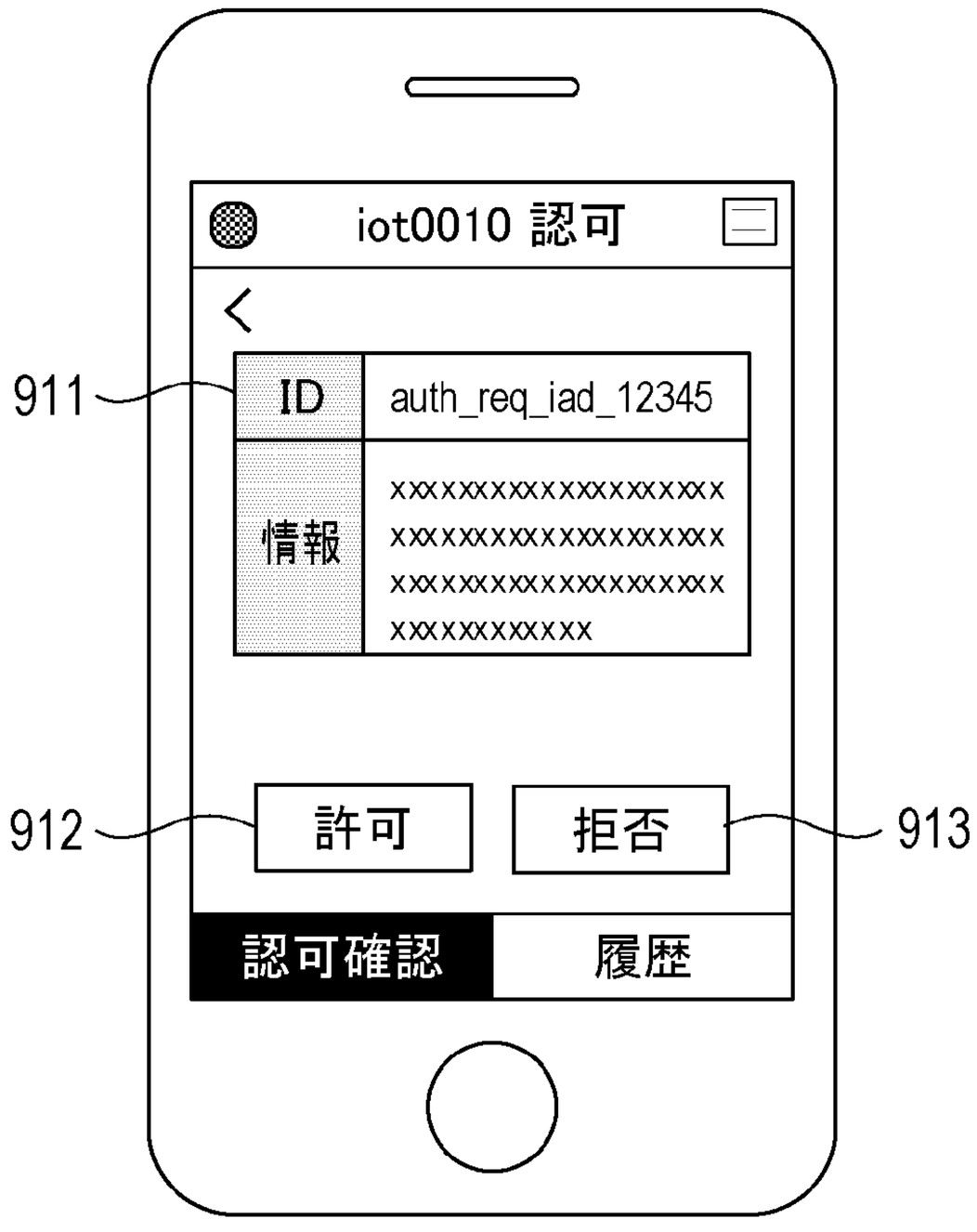
[図8B]


アクセストークンレスポンス
S521
リクエストに該当する認可
リクエスト識別子の情報を取得
S811
認可結果がある
No
Yes
S813
再認可期限を
越えている
No
Yes
S531
認可結果を確認
S812
未だ認可結果がきてい
いないことを通知する
S532
許可されている
No
Yes
S524
アクセストークンを
発行して
送信する
S525
アクセストークンを
発行できないことを
通知する
終了

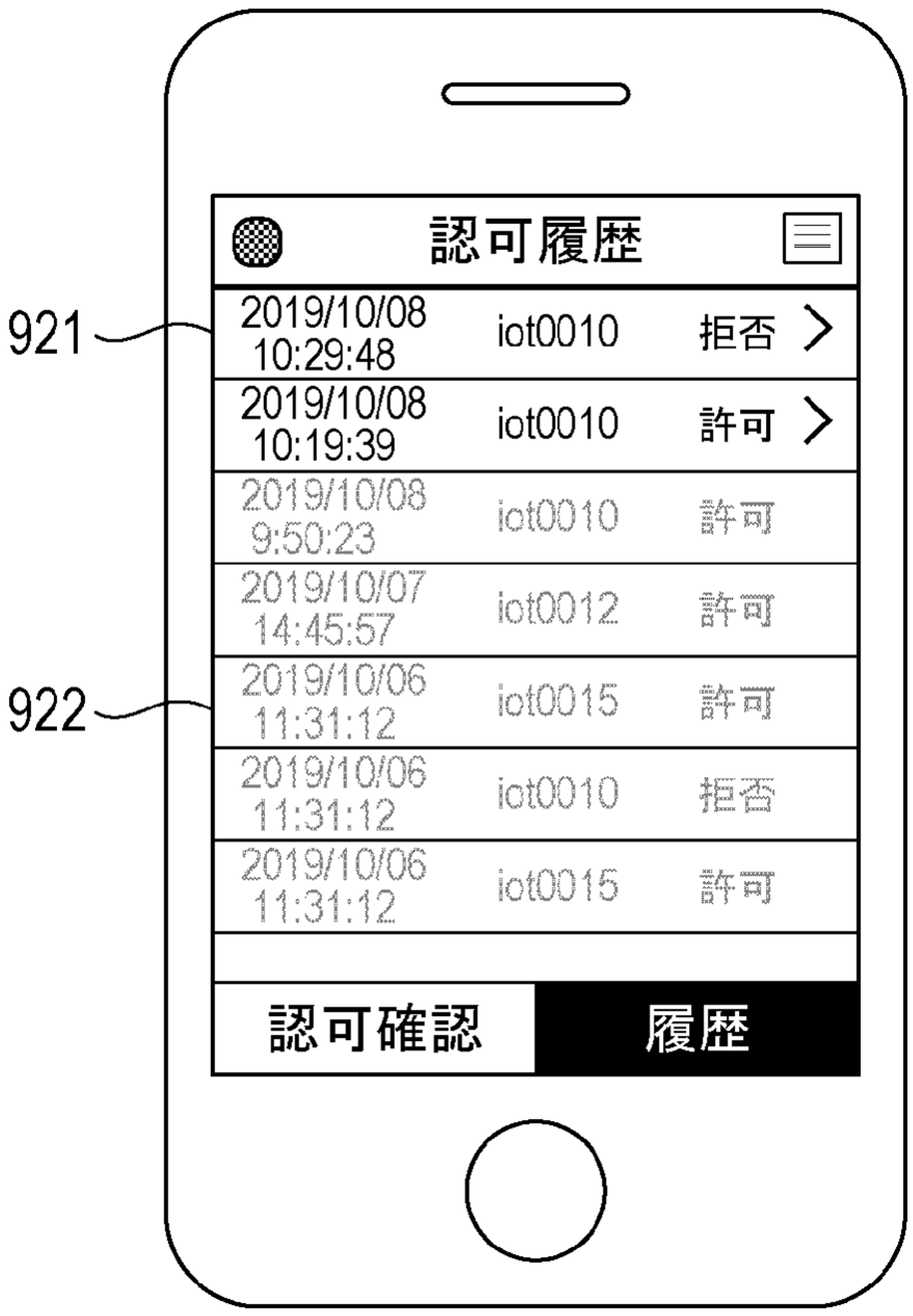
[図9A]


認可確認リスト
2019/10/08 10:25:03
iot0010
2019/10/08 9:46:54
iot0011
901
902
認可確認
履歴

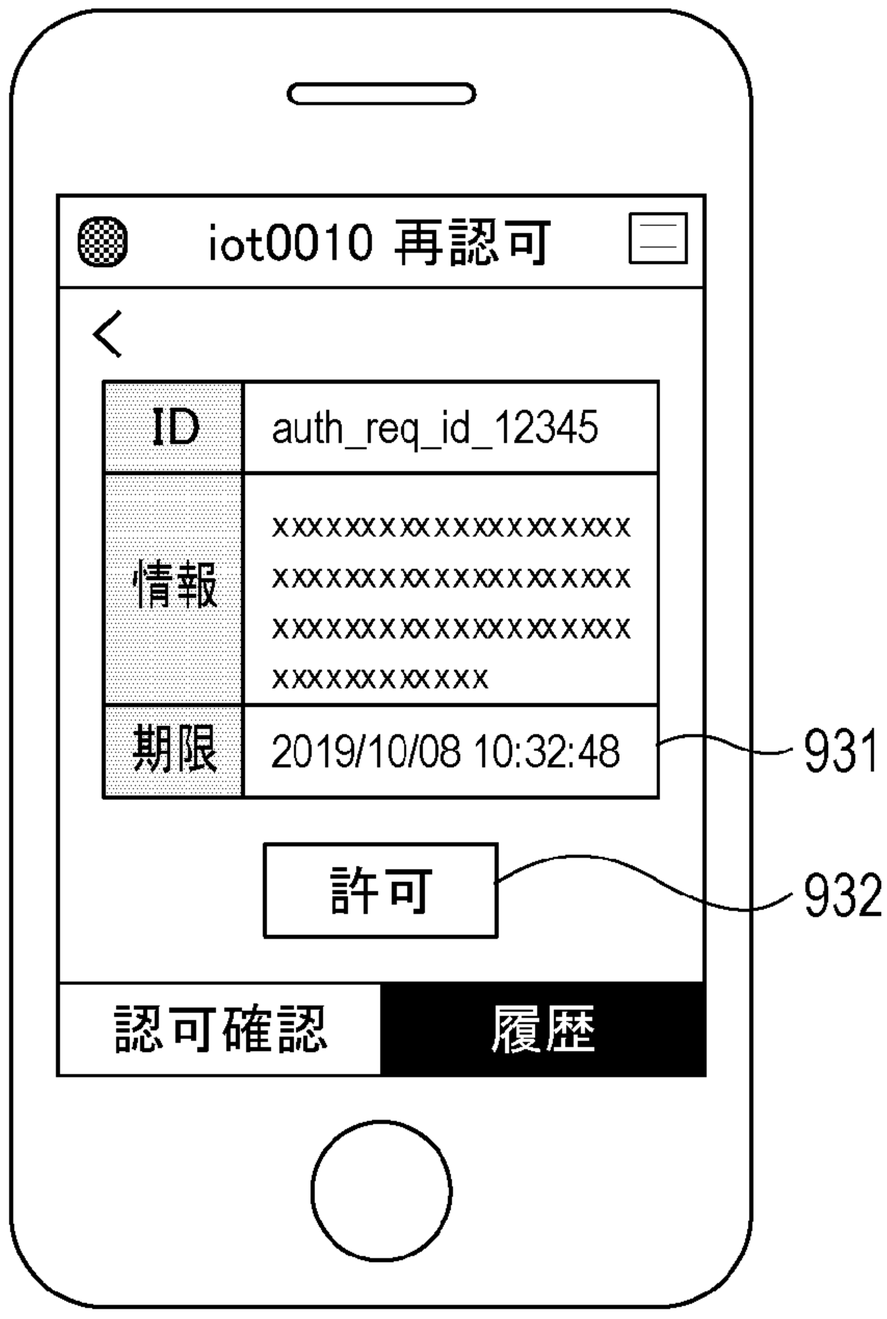
[図9B]


iot0010 認可
ID
auth_req_iad_12345
情報
xxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxx
xxxxxxxxxxx
911
912
許可
拒否
913
認可確認
履歴

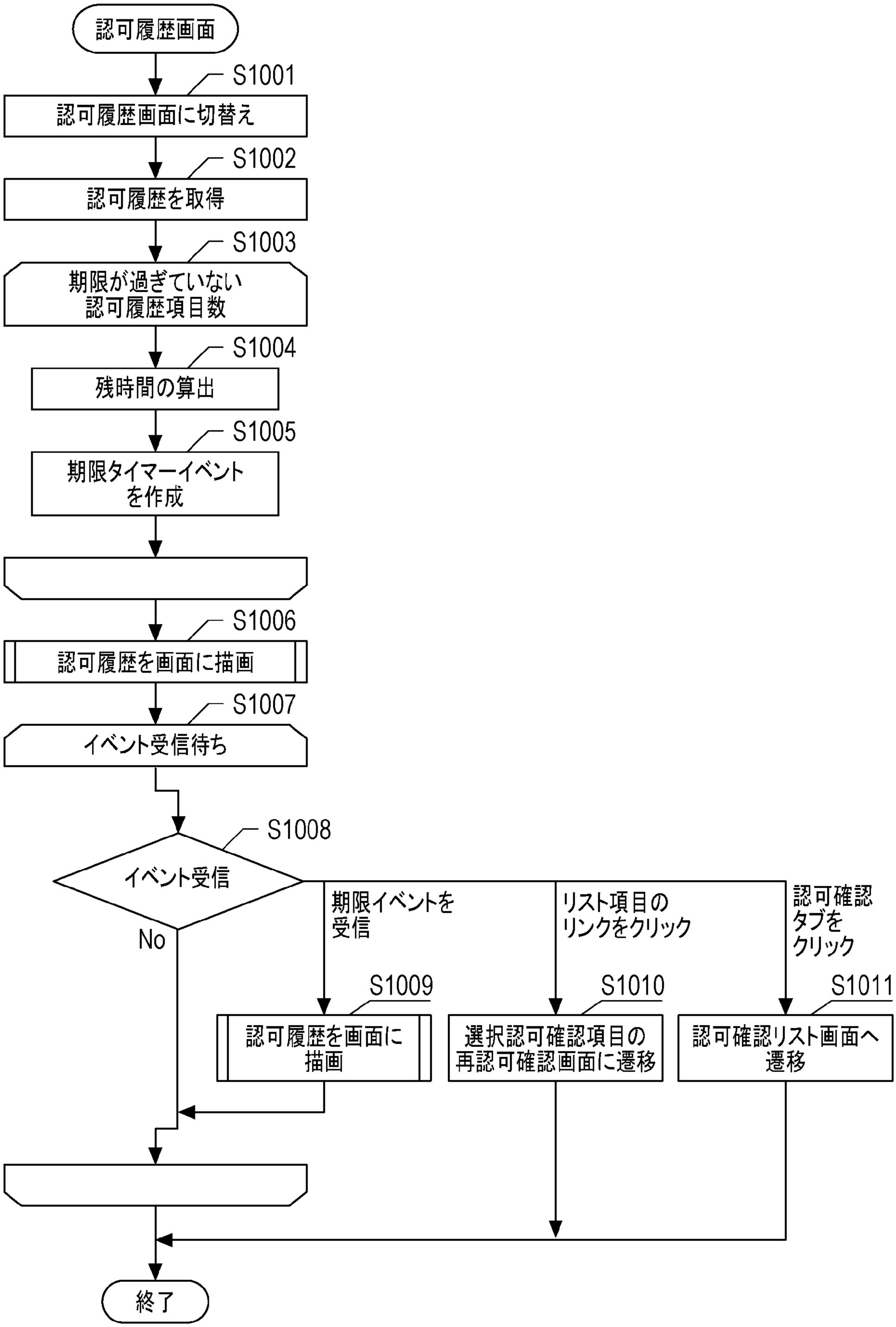
[図9C]


認可履歴
2019/10/08 10:29:48 iot0010 拒否
2019/10/08 10:19:39 iot0010 許可
2019/10/08 9:50:23 iot0010 許可
2019/10/07 14:45:57 iot0012 許可
2019/10/06 11:31:12 iot0015 許可
2019/10/06 11:31:12 iot0010 拒否
2019/10/06 11:31:12 iot0015 許可
認可確認
履歴
921
922

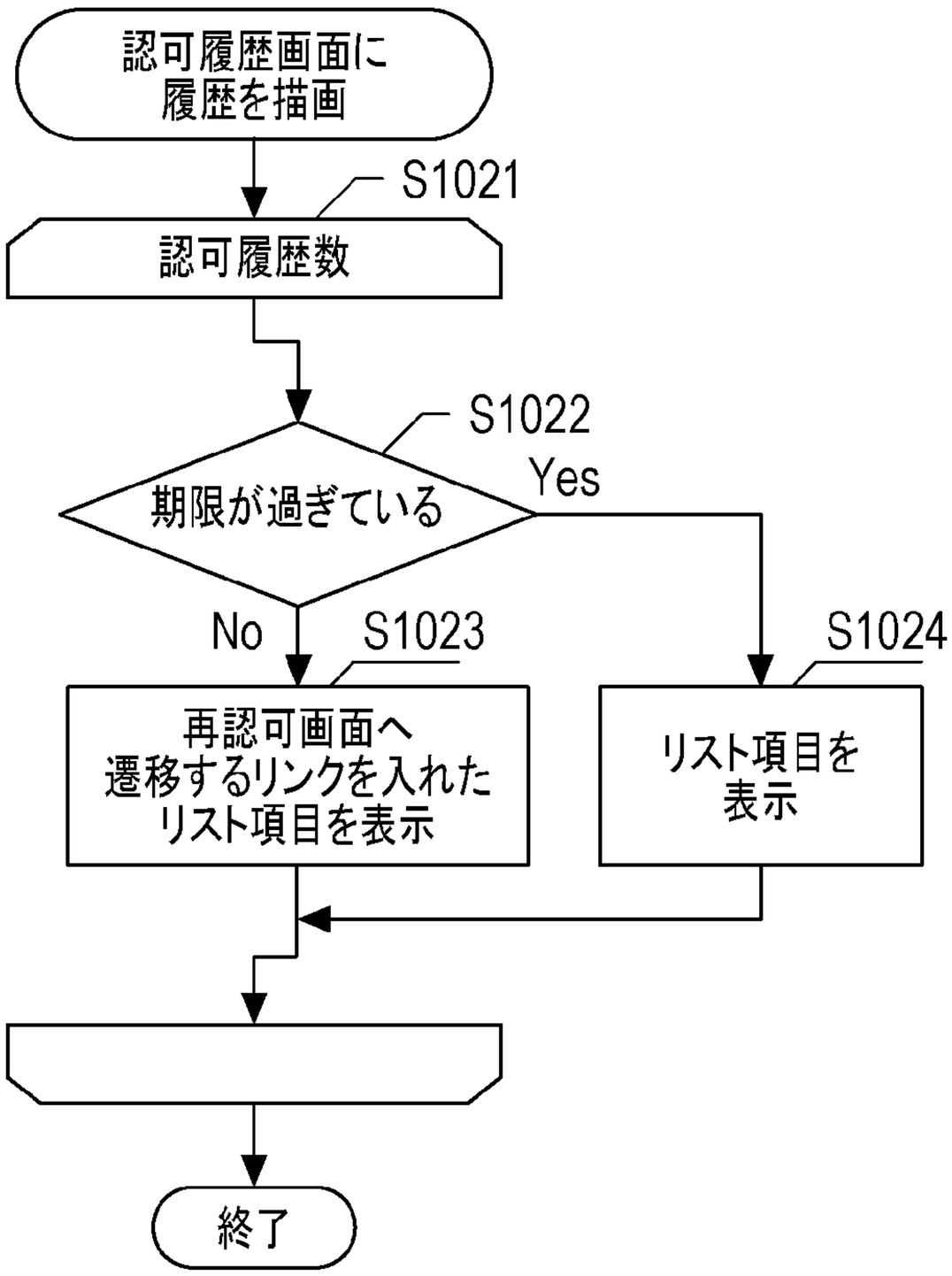
[図9D]


iot0010 再認可
ID
auth_req_id_12345
情報
xxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxx
xxxxxxxxxxx
期限
2019/10/08 10:32:48
許可
認可確認
履歴
931
932

[図10A]


認可履歴画面
S1001
認可履歴画面に切替え
S1002
認可履歴を取得
S1003
期限が過ぎていない
認可履歴項目数
S1004
残時間の算出
S1005
期限タイマーイベント
を作成
S1006
認可履歴を画面に描画
S1007
イベント受信待ち
S1008
イベント受信
No
期限イベントを
受信
リスト項目の
リンクをクリック
認可確認
タブを
クリック
S1009
認可履歴を画面に
描画
S1010
選択認可確認項目の
再認可確認画面に遷移
S1011
認可確認リスト画面へ
遷移
終了

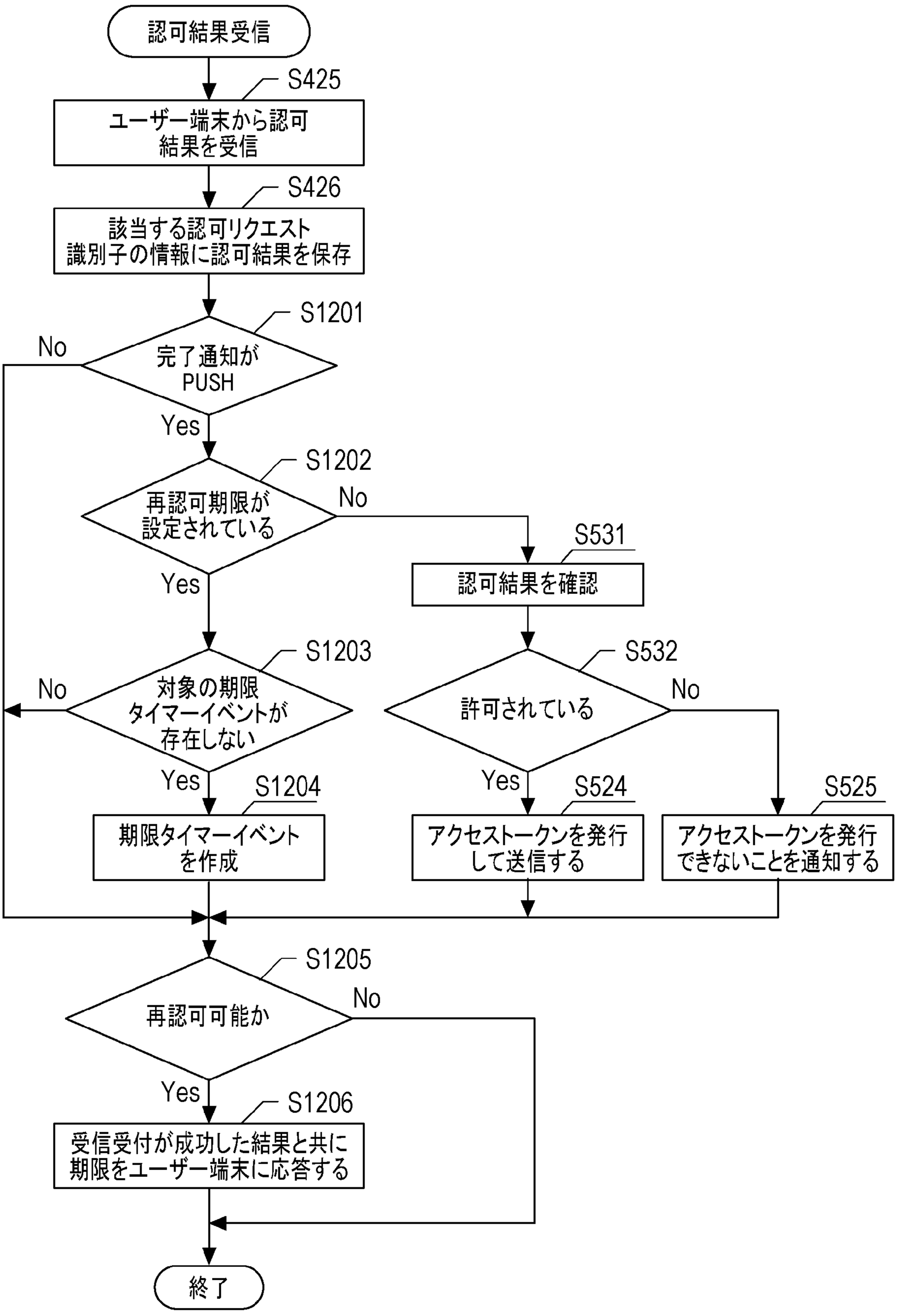
[図10B]



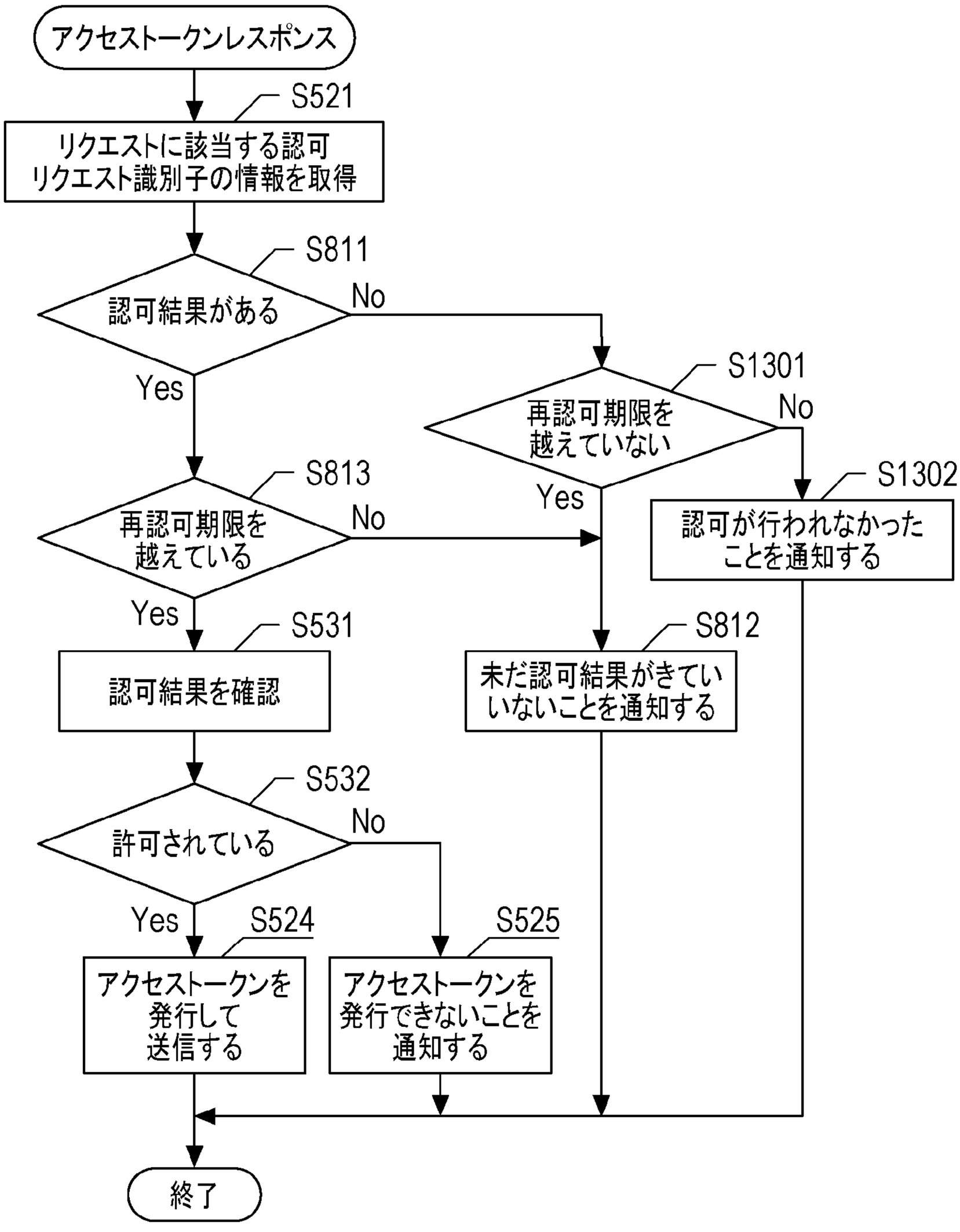
[図11]

```
{
   "scope"="/datalake/iot0010/data/get-data",
   "hint"="user_A",
   "retry"=true,
   "expires_in"=1800
}
```

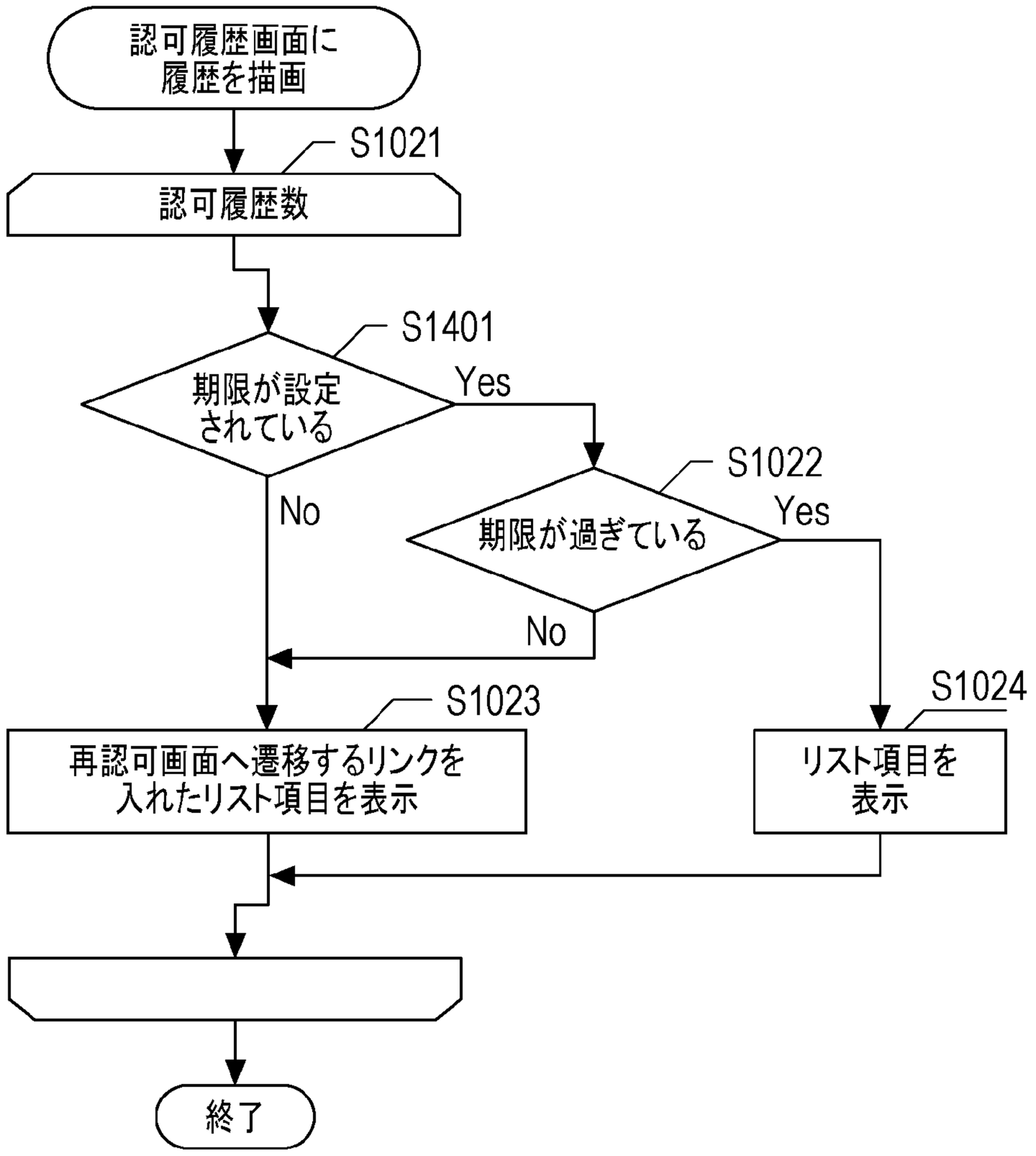
[図12]


認可結果受信
S425
ユーザー端末から認可結果を受信
S426
該当する認可リクエスト識別子の情報に認可結果を保存
S1201
完了通知がPUSH
No
Yes
S1202
再認可期限が設定されている
No
Yes
S531
認可結果を確認
S1203
対象の期限タイマーイベントが存在しない
No
Yes
S532
許可されている
No
Yes
S1204
期限タイマーイベントを作成
S524
アクセストークンを発行して送信する
S525
アクセストークンを発行できないことを通知する
S1205
再認可可能か
No
Yes
S1206
受信受付が成功した結果と共に期限をユーザー端末に応答する
終了

[図13]


アクセストークンレスポンス
S521
リクエストに該当する認可
リクエスト識別子の情報を取得
S811
認可結果がある
No
Yes
S1301
再認可期限を
越えていない
No
Yes
S1302
認可が行われなかった
ことを通知する
S813
再認可期限を
越えている
No
Yes
S531
認可結果を確認
S812
未だ認可結果がきてい
いないことを通知する
S532
許可されている
No
Yes
S524
アクセストークンを
発行して
送信する
S525
アクセストークンを
発行できないことを
通知する
終了

[図14]


認可履歴画面に
履歴を描画
S1021
認可履歴数
S1401
期限が設定
されている
Yes
No
S1022
期限が過ぎている
Yes
No
S1023
再認可画面へ遷移するリンクを
入れたリスト項目を表示
S1024
リスト項目を
表示
終了

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2020/041802

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl. G06F21/35(2013.01)i, G06F21/62(2013.01)i
FI: G06F21/35, G06F21/62

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.Cl. G06F21/35, G06F21/62

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Published examined utility model applications of Japan 1922-1996
Published unexamined utility model applications of Japan 1971-2021
Registered utility model specifications of Japan 1996-2021
Published registered utility model applications of Japan 1994-2021

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 2017-037407 A (NIPPON TELEGRAPH AND TELEPHONE CORPORATION) 16 February 2017 (2017-02-16), abstract	1-11
A	JP 2016-535880 A (ORACLE INTERNATIONAL CORPORATION) 17 November 2016 (2016-11-17), paragraph [0107]	1-11

☐ 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	Date of mailing of the international search report
26 January 2021	02 February 2021
Name and mailing address of the ISA/ Japan Patent Office 3-4-3, Kasumigaseki, Chiyoda-ku, Tokyo 100-8915, Japan	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/JP2020/041802

JP 2017-037407 A	16 February 2017	(Family: none)	
JP 2016-535880 A	17 November 2016	US 2015/0089596 A1 paragraph [0123] WO 2015/042349 A1 CN 105659558 A	

国際調査報告

国際出願番号
PCT/JP2020/041802

A.　発明の属する分野の分類（国際特許分類（ＩＰＣ））

G06F 21/35(2013.01)i; G06F 21/62(2013.01)i
FI: G06F21/35; G06F21/62

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））

G06F21/35; G06F21/62

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　１９７１－２０２１年
日本国実用新案登録公報　１９９６－２０２１年
日本国登録実用新案公報　１９９４－２０２１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 2017-037407 A（日本電信電話株式会社）16.02.2017（2017-02-16） 要約	1-11
A	JP 2016-535880 A（オラクル・インターナショナル・コーポレイション）17.11.2016（2016-11-17） 段落[0107]	1-11

☐ 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抵触するものではなく、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	国際調査報告の発送日
26.01.2021	02.02.2021

名称及びあて先
日本国特許庁(ISA/JP)
〒100-8915
日本国
東京都千代田区霞が関三丁目４番３号

権限のある職員（特許庁審査官）
田名網　忠雄　5S　6306

電話番号　03-3581-1101　内線　3546

国際調査報告
パテントファミリーに関する情報

国際出願番号
PCT/JP2020/041802

引用文献	公表日	パテントファミリー文献	公表日
JP 2017-037407 A	16.02.2017	（ファミリーなし）	
JP 2016-535880 A	17.11.2016	US 2015/0089596 A1 段落[0123] WO 2015/042349 A1 CN 105659558 A	

様式 PCT/ISA/210（パテントファミリー用別紙）（２０１５年１月）