(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第6055934号
(P6055934)

(45)発行日　平成28年12月27日(2016.12.27)　(24)登録日　平成28年12月9日(2016.12.9)

(51)Int.Cl.　F I
G06F 21/33 (2013.01)　G06F 21/33 350
G06F 21/62 (2013.01)　G06F 21/62 318

請求項の数 10　(全 18 頁)

(21)出願番号　特願2015-559411 (P2015-559411)
(86)(22)出願日　平成25年9月23日(2013.9.23)
(65)公表番号　特表2016-509319 (P2016-509319A)
(43)公表日　平成28年3月24日(2016.3.24)
(86)国際出願番号　PCT/CN2013/084020
(87)国際公開番号　WO2014/131279
(87)国際公開日　平成26年9月4日(2014.9.4)
審査請求日　平成27年8月31日(2015.8.31)
(31)優先権主張番号　201310066662.4
(32)優先日　平成25年3月1日(2013.3.1)
(33)優先権主張国　中国(CN)

(73)特許権者　500266829
中興通訊股▲分▼有限公司
中華人民共和国広東省深セン市南山区高新技術産業園科技南路中興通訊大厦
(74)代理人　100101454
弁理士　山田　卓二
(74)代理人　100081422
弁理士　田中　光雄
(74)代理人　100125874
弁理士　川端　純市
(74)代理人　100189544
弁理士　柏原　啓伸

最終頁に続く

(54)【発明の名称】双方向許可システム、クライアントおよび方法

(57)【特許請求の範囲】
【請求項１】
双方向許可システムであって、
第一のサービス提供サブシステムの第一の一時的な資格、第二のサービス提供サブシステムの第二の一時的な資格をそれぞれ取得し、第二の一時的な資格をユーザ端末に送信して許可し、ユーザ端末から返された第二の許可資格を受信し、そして第二の許可資格を第二のサービス提供サブシステムに送信して第二のアクセストークンを引き換え、前記第二のアクセストークンに基づいて、第二のサービス提供サブシステムのリソースを取得し、および第一の一時的な資格を第二のサービス提供サブシステムに送信するように構成される第一のサービス提供サブシステムと、
第一のサービス提供サブシステムから送信された第一の一時的な資格を受信し、そして前記第一の一時的な資格における識別子を変更し、変更された第一の一時的な資格をユーザ端末に送信して許可し、ユーザ端末から返された第一の許可資格を受信し、第一の許可資格を第一のサービス提供サブシステムに送信して第一のアクセストークンを引き換え、前記第一のアクセストークンに基づいて第一のサービス提供サブシステムのリソースを取得するように構成される第二のサービス提供サブシステムと、
第一のサービス提供サブシステムから送信された第二の一時的な資格、第二のサービス提供サブシステムから送信された第一の一時的な資格をそれぞれ受信し、第二の一時的な資格、第一の一時的な資格をそれぞれ許可し、そして許可された第二の許可資格、第一の許可資格をそれぞれ第一のサービス提供サブシステム、第二のサービス提供サブシステム

に送信するように構成されるユーザ端末とを含む、前記双方向許可システム。
【請求項２】
前記第一のサービス提供サブシステムは、
第一のオープン許可（ＯＡｕｔｈ：Ｏｐｅｎ　Ａｕｔｈ）サーバ、第二のサービス提供サブシステムへ一時的な資格要求命令をそれぞれ送信し、第一のＯＡｕｔｈサーバ、第二のサービス提供サブシステムからそれぞれ返された第一の一時的な資格、第二の一時的な資格を受信し、第二の一時的な資格をユーザ端末に送信して許可し、ユーザ端末から返された第二の許可資格を受信し、前記第二の許可資格を第二のサービス提供サブシステムに送信して第二のアクセストークンを引き換え、第二のアクセストークンを第二のサービス提供サブシステムに送信して認証し、第二のサービス提供サブシステムで認証に成功した後、第二のサービス提供サブシステムから提供されたリソースにアクセスするように構成され、さらに第一の一時的な資格を第二のサービス提供サブシステムに送信してクライアント識別子を変更するように構成される第一のクライアントと、
第一のクライアントから送信された一時的な資格要求命令を受信し、そして当該命令に応じて第一の一時的な資格を第一のクライアントに返し、第二のサービス提供サブシステムから送信された第一の許可資格を受信し、第一のアクセストークンを第二のサービス提供サブシステムに返し、そして第一のアクセストークンを第一のリソースサーバに送信して認証基準とするように構成される第一のＯＡｕｔｈサーバと、
第二のサービス提供サブシステムから送信された第一のアクセストークンを受信し、そして第一のＯＡｕｔｈサーバから送信された第一のアクセストークンに基づいて前記第二のサービス提供サブシステムから送信された第一のアクセストークンを認証し、認証に成功した後に第一のサービスリソースを第二のサービス提供サブシステムに提供してアクセスするように構成される第一のリソースサーバとを含むことを特徴とする
請求項１に記載の双方向許可システム。
【請求項３】
前記第二のサービス提供サブシステムは、
第一のサービス提供サブシステムから送信された第一の一時的な資格を受信し、そして前記第一の一時的な資格における第一のクライアント識別子を第二のクライアント識別子に変更し、変更された第一の一時的な資格をユーザ端末に送信して許可し、ユーザ端末から返された第一の許可資格を受信し、前記第一の許可資格を第一のサービス提供サブシステムに送信して第一のアクセストークンを引き換え、第一のアクセストークンを第一のサービス提供サブシステムに送信して認証し、第一のサービス提供サブシステムで認証に成功した後に、第一のサービス提供サブシステムから提供された第一のサービスリソースにアクセスするように構成される第二のクライアントと、
第一のサービス提供サブシステムから送信された一時的な資格要求命令を受信し、そして当該命令に応じて第二の一時的な資格を第一のサービス提供サブシステムに返し、第一のサービス提供サブシステムから送信された第二の許可資格を受信し、第二のアクセストークンを第一のサービス提供サブシステムに返し、そして第二のアクセストークンを第二のリソースサーバに送信して認証基準とするように構成される第二のＯＡｕｔｈサーバと、
第一のサービス提供サブシステムから送信された第二のアクセストークンを受信し、そして第二のＯＡｕｔｈサーバから送信された第二のアクセストークンに基づいて前記第一のサービス提供サブシステムから送信された第二のアクセストークンを認証し、認証に成功した後に第二のサービスリソースを第一のサービス提供サブシステムに提供してアクセスするように構成される第二のリソースサーバとを含むことを特徴とする
請求項１に記載の双方向許可システム。
【請求項４】
前記第二のサービス提供サブシステムは、第二のクライアント、第二のＯＡｕｔｈサーバ、第二のリソースサーバを含み、
前記第一のクライアントは、第一のＯＡｕｔｈサーバ、第二のＯＡｕｔｈサーバに一時

的な資格要求命令をそれぞれ送信し、第一のＯＡｕｔｈサーバ、第二のＯＡｕｔｈサーバからそれぞれ返された第一の一時的な資格、第二の一時的な資格を受信し、第二の一時的な資格をユーザ端末に送信して許可し、ユーザ端末から返された第二の許可資格を受信し、前記第二の許可資格を第二のＯＡｕｔｈサーバに送信して第二のアクセストークンを引き換え、第二のアクセストークンを第二のリソースサーバに送信して認証し、第二のリソースサーバで認証に成功した後に、第二のリソースサーバから提供された第二のサービスリソースにアクセスするように構成され、さらに第一の一時的な資格を第二のクライアントに送信するように構成され、

前記第一のＯＡｕｔｈサーバは、第一のクライアントから送信された一時的な資格要求命令を受信し、そして当該命令に応じて第一の一時的な資格を第一のクライアントに返し、第二のクライアントから送信された第一の許可資格を受信し、第一のアクセストークンを第二のクライアントに返し、そして第一のアクセストークンを第一のリソースサーバに送信して認証基準とするように構成され、

前記第一のリソースサーバは、第二のクライアントから送信された第一のアクセストークンを受信し、そして第一のＯＡｕｔｈサーバから送信された第一のアクセストークンに基づいて前記第二のクライアントから送信された第一のアクセストークンを認証し、認証に成功した後に第一のサービスリソースを第二のクライアントに提供してアクセスするように構成され、

前記第二のクライアントは、第一のＯＡｕｔｈサーバから送信された第一の一時的な資格を受信し、そして前記第一の一時的な資格における第一のクライアント識別子を第二のクライアント識別子に変更し、変更された第一の一時的な資格をユーザ端末に送信して許可し、ユーザ端末から返された第一の許可資格を受信し、前記第一の許可資格を第一のＯＡｕｔｈサーバに送信して第一のアクセストークンを引き換え、第一のアクセストークンを第一のリソースサーバに送信して認証し、第一のリソースサーバで認証に成功した後に、第一のリソースサーバから提供された第一のサービスリソースにアクセスするように構成され、

前記第二のＯＡｕｔｈサーバは、第一のクライアントから送信された一時的な資格要求命令を受信し、そして当該命令に応じて第二の一時的な資格を第一のクライアントに返し、第一のクライアントから送信された第二の許可資格を受信し、第二のアクセストークンを第一のクライアントに返し、そして第二のアクセストークンを第二のリソースサーバに送信して認証基準とするように構成され、

前記第二のリソースサーバは、第一のクライアントから送信された第二のアクセストークンを受信し、そして第二のＯＡｕｔｈサーバから送信された第二のアクセストークンに基づいて前記第一のクライアントから送信された第二のアクセストークンを認証し、認証に成功した後に第二のサービスリソースを第一のクライアントに提供してアクセスするように構成されることを特徴とする

請求項２に記載の双方向許可システム。

【請求項５】

前記一時的な資格要求命令は、ＯＡｕｔｈプロトコルによって定義された一時的な資格要求メッセージで搬送されることを特徴とする

請求項３に記載の双方向許可システム。

【請求項６】

サービス提供サブシステムに設置されているクライアントであって、

前記サービス提供サブシステムがオープン許可（ＯＡｕｔｈ：Ｏｐｅｎ　Ａｕｔｈ）サーバ、リソースサーバをさらに含み、当該クライアントが一時的な資格取得モジュール、アクセストークン取得モジュール、リソース取得モジュールを含み、

前記一時的な資格取得モジュールは、本側のサービス提供サブシステムのＯＡｕｔｈサーバ、他側のサービス提供サブシステムのＯＡｕｔｈサーバに一時的な資格要求命令をそれぞれ送信し、本側のサービス提供サブシステムのＯＡｕｔｈサーバから返された第一の一時的な資格、他側のサービス提供サブシステムのＯＡｕｔｈサーバから返された第二の

一時的な資格を受信し、第一の一時的な資格を他側のサービス提供サブシステムのクライアントに送信するように構成され、
前記アクセストークン取得モジュールは、第二の一時的な資格をユーザ端末に送信して許可し、ユーザ端末から返された第二の許可資格を受信し、前記第二の許可資格を他側のサービス提供サブシステムのＯＡｕｔｈサーバに送信して第二のアクセストークンを引き換えるように構成され、
前記リソース取得モジュールは、第二のアクセストークンを他側のサービス提供サブシステムのリソースサーバに送信して認証し、他側のサービス提供サブシステムのリソースサーバで認証に成功した後に、他側のサービス提供サブシステムのリソースサーバから提供されたリソースにアクセスするように構成される、前記クライアント。
【請求項７】
サービス提供サブシステムに設置されているクライアントであって、
前記サービス提供サブシステムがオープン許可（ＯＡｕｔｈ：Ｏｐｅｎ　Ａｕｔｈ）サーバ、リソースサーバをさらに含み、当該クライアントが一時的な資格取得モジュール、アクセストークン取得モジュール、リソース取得モジュールを含み、
前記一時的な資格取得モジュールは、他側のサービス提供サブシステムのＯＡｕｔｈサーバから送信された第一の一時的な資格を受信し、そして前記第一の一時的な資格における他側のサービス提供サブシステムのクライアント識別子を本側のサービス提供サブシステムのクライアント識別子に変更するように構成され、
前記アクセストークン取得モジュールは、変更された第一の一時的な資格をユーザ端末に送信して許可し、ユーザ端末から返された第一の許可資格を受信し、前記第一の許可資格を他側のサービス提供サブシステムのＯＡｕｔｈサーバに送信して第一のアクセストークンを引き換えるように構成され、
前記リソース取得モジュールは、第一のアクセストークンを他側のサービス提供サブシステムのリソースサーバに送信して認証し、他側のサービス提供サブシステムのリソースサーバで認証に成功した後に、他側のサービス提供サブシステムのリソースサーバから提供されたリソースにアクセスするように構成される、前記クライアント。
【請求項８】
双方向許可方法であって、
第一のサービス提供サブシステムが、第一のサービス提供サブシステムの第一の一時的な資格、第二のサービス提供サブシステムの第二の一時的な資格を取得し、第二の一時的な資格をユーザ端末に送信して許可し、第二の許可資格を取得し、第二の許可資格を第二のサービス提供サブシステムに送信して第二のアクセストークンを引き換え、前記第二のアクセストークンに基づいて第二のサービス提供サブシステムのリソースを取得し、第一の一時的な資格を第二のサービス提供サブシステムに送信して識別子を変更することと、
第二のサービス提供サブシステムが、変更された第一の一時的な資格をユーザ端末に送信して許可し、第一の許可資格を取得し、第一の許可資格を第一のサービス提供サブシステムに送信して第一のアクセストークンを引き換え、前記第一のアクセストークンに基づいて第一のサービス提供システムのリソースを取得することとを含む、前記双方向許可方法。
【請求項９】
前記第一のサービス提供サブシステムが第一のサービス提供サブシステムの第一の一時的な資格、第二のサービス提供サブシステムの第二の一時的な資格を取得することは、
第一のサービス提供サブシステムにおける第一のクライアントが第一のサービス提供サブシステムにおける第一のオープン許可（ＯＡｕｔｈ：Ｏｐｅｎ　Ａｕｔｈ）サーバ、第二のサービス提供サブシステムにおける第二のＯＡｕｔｈサーバに一時的な資格要求命令をそれぞれ送信し、第一のＯＡｕｔｈサーバ、第二のＯＡｕｔｈサーバから返された第一の一時的な資格、第二の一時的な資格を受信することを含むことを特徴とする
請求項８に記載の双方向許可方法。
【請求項１０】

前記第一の一時的な資格の許可は、第一のサービス提供サブシステムのユーザ名とパスワードを入力することであり、前記ユーザ名とパスワードは、ユーザ端末が第一のサービス提供サブシステムに登録したユーザ名とパスワードであり、
前記第二の一時的な資格の許可は、第二のサービス提供サブシステムのユーザ名とパスワードを入力することであり、前記ユーザ名とパスワードは、ユーザ端末が第二のサービス提供サブシステムに登録したユーザ名とパスワードであることを特徴とする
請求項８または９に記載の双方向許可方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、インターネットにおける許可技術に関し、特に双方向許可システム、クライアントおよび方法に関する。
【背景技術】
【０００２】
クライアントは、サーバ側で保護されているユーザリソースにアクセスしたいと、例えばユーザ名およびパスワードなどのユーザのＩＤ資格を使用する必要がある。第三者のクライアントがサービス側で保護されているユーザリソースにアクセスしようとする場合、ユーザのＩＤ資格を第三者のクライアントに提供する必要があり、このようにして、深刻な安全上の問題が存在する。
【０００３】
オープン許可（ＯＡｕｔｈ：Ｏｐｅｎ　Ａｕｔｈ）プロトコルは、上記問題を解決するために、ユーザリソースの許可のために安全、オープン、簡易な基準を提供し、１つの中間層によりクライアントとユーザ許可過程を分離させ、第三者のクライアントがユーザの資格情報に触れない場合で当該ユーザリソース許可の取得を請求できる。ＯＡｕｔｈプロトコルにおいてリソース所有者、クライアント、リソースサーバ、許可サーバを含む４つの役が定義される。リソース所有者は、リソースを持つユーザであって、自分のリソースへのクライアントのアクセスを許可できる。クライアントは、保護されているリソースにアクセスするクライアントプログラムである。リソースサーバは、リソース所有者のリソースを保存するサーバであって、リソース所有者により許可されなければ、クライアントがアクセスすることができない。許可サーバは、リソース所有者のユーザ資格を受信した後にアクセストークンを生成してクライアントに送信することを担当する。
【０００４】
ＯＡｕｔｈプロトコルにより、第三者のクライアントは、ユーザからの許可を受信した後に、リソースサーバ側で保護されているユーザリソースにアクセスすることができる。しかし、ＯＡｕｔｈプロトコルが一方向許可プロトコルであるので、第三者のクライアントによってリソースサーバへ一方的な許可を要求しかできなく、クライアントから第三者のリソースサーバへの許可要求を同時に満たすことができない。例えば、クライアントがマイクロブログであり、第三者のクライアントがブログである場合、リソースサーバには、保護されているユーザのマイクロブログ情報であり、第三者のリソースサーバには、保護されているユーザのブログ情報であり、ブログクライアントは、リソース所有者により許可された後に、リソースサーバ側のマイクロブログ情報にアクセスできるが、マイクロブログクライアントは、第三者のリソースサーバ側のブログ情報にアクセスできない。
【発明の概要】
【発明が解決しようとする課題】
【０００５】
これを鑑みて、本発明の実施形態の主な目的は、両側のクライアントが同時に保護された相手側のリソースにアクセスすることができるように、双方向許可システム、クライアントおよび方法を提供することにある。
【課題を解決するための手段】
【０００６】

上記目的を達成するために、本発明の実施形態の技術的解決手段は、以下のように実現される。

【０００７】

双方向許可システムは、

第一のサービス提供サブシステムの第一の一時的な資格、第二のサービス提供サブシステムの第二の一時的な資格をそれぞれ取得し、第二の一時的な資格をユーザ端末に送信して許可し、ユーザ端末から返された第二の許可資格を受信し、そして第二の許可資格を第二のサービス提供サブシステムに送信して第二のアクセストークンを引き換え、前記第二のアクセストークンに基づいて、第二のサービス提供サブシステムのリソースを取得し、および第一の一時的な資格を第二のサービス提供サブシステムに送信するように構成される第一のサービス提供サブシステムと、

第一のサービス提供サブシステムから送信された第一の一時的な資格を受信し、そして前記第一の一時的な資格における識別子を変更し、変更された第一の一時的な資格をユーザ端末に送信して許可し、ユーザ端末から返された第一の許可資格を受信し、第一の許可資格を第一のサービス提供サブシステムに送信して第一のアクセストークンを引き換え、前記第一のアクセストークンに基づいて第一のサービス提供サブシステムのリソースを取得するように構成される第二のサービス提供サブシステムと、

第一のサービス提供サブシステムから送信された第二の一時的な資格、第二のサービス提供サブシステムから送信された第一の一時的な資格をそれぞれ受信し、第二の一時的な資格、第一の一時的な資格をそれぞれ許可し、そして許可された第二の許可資格、第一の許可資格をそれぞれ第一のサービス提供サブシステム、第二のサービス提供サブシステムに送信するように構成されるユーザ端末とを含む。

【０００８】

上記の解決手段において、前記第一のサービス提供サブシステムは、

第一のオープン許可（ＯＡｕｔｈ）サーバ、第二のサービス提供サブシステムへ一時的な資格要求命令をそれぞれ送信し、第一のＯＡｕｔｈサーバ、第二のサービス提供サブシステムからそれぞれ返された第一の一時的な資格、第二の一時的な資格を受信し、第二の一時的な資格をユーザ端末に送信して許可し、ユーザ端末から返された第二の許可資格を受信し、前記第二の許可資格を第二のサービス提供サブシステムに送信して第二のアクセストークンを引き換え、第二のアクセストークンを第二のサービス提供サブシステムに送信して認証し、第二のサービス提供サブシステムで認証に成功した後、第二のサービス提供サブシステムから提供されたリソースにアクセスするように構成され、さらに第一の一時的な資格を第二のサービス提供サブシステムに送信してクライアント識別子を変更するように構成される第一のクライアントと、

第一のクライアントから送信された一時的な資格要求命令を受信し、そして当該命令に応じて第一の一時的な資格を第一のクライアントに返し、第二のサービス提供サブシステムから送信された第一の許可資格を受信し、第一のアクセストークンを第二のサービス提供サブシステムに返し、そして第一のアクセストークンを第一のリソースサーバに送信して認証基準とするように構成される第一のＯＡｕｔｈサーバと、

第二のサービス提供サブシステムから送信された第一のアクセストークンを受信し、そして第一のＯＡｕｔｈサーバから送信された第一のアクセストークンに基づいて前記第二のサービス提供サブシステムから送信された第一のアクセストークンを認証し、認証に成功した後に第一のサービスリソースを第二のサービス提供サブシステムに提供してアクセスするように構成される第一のリソースサーバとを含む。

【０００９】

上記の解決手段において、前記第二のサービス提供サブシステムは、

第一のサービス提供サブシステムから送信された第一の一時的な資格を受信し、そして前記第一の一時的な資格における第一のクライアント識別子を第二のクライアント識別子に変更し、変更された第一の一時的な資格をユーザ端末に送信して許可し、ユーザ端末から返された第一の許可資格を受信し、前記第一の許可資格を第一のサービス提供サブシス

テムに送信して第一のアクセストークンを引き換え、第一のアクセストークンを第一のサービス提供サブシステムに送信して認証し、第一のサービス提供サブシステムで認証に成功した後に、第一のサービス提供サブシステムから提供された第一のサービスリソースにアクセスするように構成される第二のクライアントと、

第一のサービス提供サブシステムから送信された一時的な資格要求命令を受信し、そして当該命令に応じて第二の一時的な資格を第一のサービス提供サブシステムに返し、第一のサービス提供サブシステムから送信された第二の許可資格を受信し、第二のアクセストークンを第一のサービス提供サブシステムに返し、そして第二のアクセストークンを第二のリソースサーバに送信して認証基準とするように構成される第二のＯＡｕｔｈサーバと、

第一のサービス提供サブシステムから送信された第二のアクセストークンを受信し、そして第二のＯＡｕｔｈサーバから送信された第二のアクセストークンに基づいて前記第一のサービス提供サブシステムから送信された第二のアクセストークンを認証し、認証に成功した後に第二のサービスリソースを第一のサービス提供サブシステムに提供してアクセスするように構成される第二のリソースサーバとを含む。

【００１０】

上記の解決手段において、前記第二のサービス提供サブシステムは、第二のクライアント、第二のＯＡｕｔｈサーバ、第二のリソースサーバを含み、

前記第一のクライアントは、第一のＯＡｕｔｈサーバ、第二のＯＡｕｔｈサーバに一時的な資格要求命令をそれぞれ送信し、第一のＯＡｕｔｈサーバ、第二のＯＡｕｔｈサーバからそれぞれ返された第一の一時的な資格、第二の一時的な資格を受信し、第二の一時的な資格をユーザ端末に送信して許可し、ユーザ端末から返された第二の許可資格を受信し、前記第二の許可資格を第二のＯＡｕｔｈサーバに送信して第二のアクセストークンを引き換え、第二のアクセストークンを第二のリソースサーバに送信して認証し、第二のリソースサーバで認証に成功した後に、第二のリソースサーバから提供された第二のサービスリソースにアクセスするように構成され、さらに第一の一時的な資格を第二のクライアントに送信するように構成され、

前記第一のＯＡｕｔｈサーバは、第一のクライアントから送信された一時的な資格要求命令を受信し、そして当該命令に応じて第一の一時的な資格を第一のクライアントに返し、第二のクライアントから送信された第一の許可資格を受信し、第一のアクセストークンを第二のクライアントに返し、そして第一のアクセストークンを第一のリソースサーバに送信して認証基準とするように構成され、

前記第一のリソースサーバが第二のクライアントから送信された第一のアクセストークンを受信し、そして第一のＯＡｕｔｈサーバから送信された第一のアクセストークンに基づいて前記第二のクライアントから送信された第一のアクセストークンを認証し、認証に成功した後に第一のサービスリソースを第二のクライアントに提供してアクセスするように構成され、

前記第二のクライアントは、第一のＯＡｕｔｈサーバから送信された第一の一時的な資格を受信し、そして前記第一の一時的な資格における第一のクライアント識別子を第二のクライアント識別子に変更し、変更された第一の一時的な資格をユーザ端末に送信して許可し、ユーザ端末から返された第一の許可資格を受信し、前記第一の許可資格を第一のＯＡｕｔｈサーバに送信して第一のアクセストークンを引き換え、第一のアクセストークンを第一のリソースサーバに送信して認証し、第一のリソースサーバで認証に成功した後に、第一のリソースサーバから提供された第一のサービスリソースにアクセスするように構成され、

前記第二のＯＡｕｔｈサーバは、第一のクライアントから送信された一時的な資格要求命令を受信し、そして当該命令に応じて第二の一時的な資格を第一のクライアントに返し、第一のクライアントから送信された第二の許可資格を受信し、第二のアクセストークンを第一のクライアントに返し、そして第二のアクセストークンを第二のリソースサーバに送信して認証基準とするように構成され、

前記第二のリソースサーバは、第一のクライアントから送信された第二のアクセストークンを受信し、そして第二のＯＡｕｔｈサーバから送信された第二のアクセストークンに基づいて前記第一のクライアントから送信された第二のアクセストークンを認証し、認証に成功した後に第二のサービスリソースを第一のクライアントに提供してアクセスするように構成される。

【００１１】

上記の解決手段において、前記一時的な資格要求命令は、ＯＡｕｔｈプロトコルによって定義された一時的な資格要求メッセージで搬送される。

【００１２】

クライアントであって、サービス提供サブシステムに設置されており、前記サービス提供サブシステムがＯＡｕｔｈサーバ、リソースサーバをさらに含み、当該クライアントが一時的な資格取得モジュール、アクセストークン取得モジュール、リソース取得モジュールを含み、

前記一時的な資格取得モジュールは、本側のサービス提供サブシステムのＯＡｕｔｈサーバ、他側のサービス提供サブシステムのＯＡｕｔｈサーバに一時的な資格要求命令をそれぞれ送信し、本側のサービス提供サブシステムのＯＡｕｔｈサーバから返された第一の一時的な資格、他側のサービス提供サブシステムのＯＡｕｔｈサーバから返された第二の一時的な資格を受信し、第一の一時的な資格を他側のサービス提供サブシステムのクライアントに送信するように構成され、

前記アクセストークン取得モジュールは、第二の一時的な資格をユーザ端末に送信して許可し、ユーザ端末から返された第二の許可資格を受信し、前記第二の許可資格を他側のサービス提供サブシステムのＯＡｕｔｈサーバに送信して第二のアクセストークンを引き換えるように構成され、

前記リソース取得モジュールは、第二のアクセストークンを他側のサービス提供サブシステムのリソースサーバに送信して認証し、他側のサービス提供サブシステムのリソースサーバで認証に成功した後に、他側のサービス提供サブシステムのリソースサーバから提供されたリソースにアクセスするように構成される。

【００１３】

クライアントであって、サービス提供サブシステムに設置されており、前記サービス提供サブシステムがＯＡｕｔｈサーバ、リソースサーバをさらに含み、当該クライアントが一時的な資格取得モジュール、アクセストークン取得モジュール、リソース取得モジュールを含み、

前記一時的な資格取得モジュールは、他側のサービス提供サブシステムのＯＡｕｔｈサーバから送信された第一の一時的な資格を受信し、そして前記第一の一時的な資格における他側のサービス提供サブシステムのクライアント識別子を本側のサービス提供サブシステムのクライアント識別子に変更するように構成され、

前記アクセストークン取得モジュールは、変更された第一の一時的な資格をユーザ端末に送信して許可し、ユーザ端末から返された第一の許可資格を受信し、前記第一の許可資格を他側のサービス提供サブシステムのＯＡｕｔｈサーバに送信して第一のアクセストークンを引き換えるように構成され、

前記リソース取得モジュールは、第一のアクセストークンを他側のサービス提供サブシステムのリソースサーバに送信して認証し、他側のサービス提供サブシステムのリソースサーバで認証に成功した後に、他側のサービス提供サブシステムのリソースサーバから提供されたリソースにアクセスするように構成される。

【００１４】

本発明の実施形態による双方向許可方法は、

第一のサービス提供サブシステムが、第一のサービス提供サブシステムの第一の一時的な資格、第二のサービス提供サブシステムの第二の一時的な資格を取得し、第二の一時的な資格をユーザ端末に送信して許可し、第二の許可資格を取得し、第二の許可資格を第二のサービス提供サブシステムに送信して第二のアクセストークンを引き換え、前記第二の

アクセストークンに基づいて第二のサービス提供サブシステムのリソースを取得し、第一の一時的な資格を第二のサービス提供サブシステムに送信して識別子を変更することと、
第二のサービス提供サブシステムが、変更された第一の一時的な資格をユーザ端末に送信して許可し、第一の許可資格を取得し、第一の許可資格を第一のサービス提供サブシステムに送信して第一のアクセストークンを引き換え、前記第一のアクセストークンに基づいて第一のサービス提供システムのリソースを取得することとを含む。

【００１５】

上記の解決手段において、前記第一のサービス提供サブシステムが第一のサービス提供サブシステムの第一の一時的な資格、第二のサービス提供サブシステムの第二の一時的な資格を取得することは、具体的に、第一のサービス提供サブシステムにおける第一のクライアントが第一のサービス提供サブシステムにおける第一のＯＡｕｔｈサーバ、第ニのサービス提供サブシステムにおける第二のＯＡｕｔｈサーバに一時的な資格要求命令をそれぞれ送信し、第一のＯＡｕｔｈサーバ、第二のＯＡｕｔｈサーバから返された第一の一時的な資格、第二の一時的な資格を受信することである。

【００１６】

上記の解決手段において、前記第一の一時的な資格の許可は、第一のサービス提供サブシステムのユーザ名とパスワードを入力することであり、前記ユーザ名とパスワードは、ユーザ端末が第一のサービス提供サブシステムに登録したユーザ名とパスワードであり、前記第二の一時的な資格の許可は、第二のサービス提供サブシステムのユーザ名とパスワードを入力することであり、前記ユーザ名とパスワードは、ユーザ端末が第二のサービス提供サブシステムに登録したユーザ名とパスワードである。

【発明の効果】

【００１７】

本発明の実施形態における双方向許可システム、クライアントおよび方法において、第一のサービス提供サブシステムが自体の第一の一時的な資格、第二のサービス提供サブシステムの第二の一時的な資格をそれぞれ取得し、第二の一時的な資格をユーザ端末に送信して許可し、そして許可された第二の許可資格を第二のサービス提供サブシステムに送信して第二のアクセストークンを引き換え、前記第二のアクセストークンに基づいて第二のサービス提供サブシステムのリソースを取得し、第一の一時的な資格を第二のサービス提供サブシステムに送信して識別子を変更し、第二のサービス提供サブシステムが変更後の第一の一時的な資格をユーザ端末に送信して許可し、そして許可された第一の許可資格を第一のサービス提供サブシステムに送信して第一のアクセストークンを引き換え、前記第一のアクセストークンに基づいて第一のサービス提供サブシステムの第一のサービスリソースを取得する。このようにして、第一のサービス提供サブシステムが第二のサービス提供サブシステムのリソースにアクセスするとともに、第二のサービス提供サブシステムが第一のサービス提供サブシステムのリソースにアクセスすることもできることを実現できる。

【図面の簡単な説明】

【００１８】

【図１】本発明の実施形態による双方向許可システムの構成構造図１である。
【図２】本発明の実施形態による双方向許可システムの構成構造図２である。
【図３】本発明の実施形態による双方向許可システムにおけるクライアントの構成構造図である。
【図４】本発明の実施形態による双方向許可方法のプローチャートである。

【発明を実施するための形態】

【００１９】

本発明の実施形態の特徴と技術内容をより詳しく理解することができるように、以下に図面を参照して本発明の実施形態の実現を詳しく説明し、添付された図面が説明を参照するためだけであるが、本発明の実施形態を限定することに用いられるものではない。

【００２０】

図１は本発明の実施形態による双方向許可システムの構成構造図１である。図１に示すように、当該システムは、第一のサービス提供サブシステム１１、第二のサービス提供サブシステム１２、およびユーザ端末１３を含む。

【００２１】

前記第一のサービス提供サブシステム１１は、第一のサービス提供サブシステム１１の第一の一時的な資格（ｔｅｍｐｏｒａｒｙ　ｃｒｅｄｅｎｔｉａｌ）、第二のサービス提供サブシステム１２の第二の一時的な資格をそれぞれ取得し、第二の一時的な資格をユーザ端末１３に送信して許可し、ユーザ端末１３から返された第二の許可資格を受信し、そして第二の許可資格を第二のサービス提供サブシステム１２に送信して第二のアクセストークンを引き換え、前記第二のアクセストークンに基づいて、第二のサービス提供サブシステム１２のリソースを取得し、および第一の一時的な資格を第二のサービス提供サブシステム１２に送信するように構成される。

【００２２】

前記第二のサービス提供サブシステム１２は、第一のサービス提供サブシステム１１から送信された第一の一時的な資格を受信し、そして前記第一の一時的な資格における識別子を変更し、変更された第一の一時的な資格をユーザ端末１３に送信して許可し、ユーザ端末１３から返された第一の許可資格を受信し、第一の許可資格を第一のサービス提供サブシステム１１に送信して第一のアクセストークンを引き換え、前記第一のアクセストークンに基づいて第一のサービス提供サブシステム１１のリソースを取得するように構成される。

【００２３】

前記ユーザ端末１３は、第一のサービス提供サブシステム１１から送信された第二の一時的な資格、第二のサービス提供サブシステム１２から送信された第一の一時的な資格をそれぞれ受信し、第二の一時的な資格、第一の一時的な資格をそれぞれ許可し、そして許可された第二の許可資格、第一の許可資格をそれぞれ第一のサービス提供サブシステム１１、第二のサービス提供サブシステム１２に送信するように構成される。

【００２４】

実際の応用において、前記双方向許可システムにおける第一のサービス提供サブシステム１１、第二のサービス提供サブシステム１２は、サービス機能を提供するサーバにより実現されることができ、ユーザ端末１３は、いずれかの形態の端末、例えば携帯電話、コンピューターなどにより実現されることができる。

【００２５】

図２は本発明の実施形態による双方向許可システムの構成構造図２である。図２に示すように、第一のサービス提供サブシステムは、第一のクライアント１１１、第一のオープン許可（ＯＡｕｔｈ）サーバ１１２、第一のリソースサーバ１１３を含み、第二のサービス提供サブシステムは、第二のクライアント１２１、第二のＯＡｕｔｈサーバ１２２、第二のリソースサーバ１２３を含む。

【００２６】

前記第一のクライアント１１１は、第一のＯＡｕｔｈサーバ１１２、第二のサービス提供サブシステムへ一時的な資格要求命令をそれぞれ送信し、第一のＯＡｕｔｈサーバ１１２、第二のサービス提供サブシステムからそれぞれ返された第一の一時的な資格、第二の一時的な資格を受信し、第二の一時的な資格をユーザ端末１３に送信して許可し、ユーザ端末１３から返された第二の許可資格を受信し、前記第二の許可資格を第二のサービス提供サブシステムに送信して第二のアクセストークンを引き換え、第二のアクセストークンを第二のサービス提供サブシステムに送信して認証し、第二のサービス提供サブシステムで認証に成功した後、第二のサービス提供サブシステムから提供されたリソースにアクセスするように構成され、および第一の一時的な資格を第二のサービス提供サブシステムに送信するように構成される。

【００２７】

ここで、第二のサービス提供サブシステムへ一時的な資格要求命令を送信し、第二のサ

ービス提供サブシステムから返された第二の一時的な資格を受信することは、具体的に、第二のサービス提供サブシステムにおける第二のＯＡｕｔｈサーバ１２２へ一時的な資格要求命令を送信し、第二の第二のサービス提供サブシステムにおける第二のＯＡｕｔｈサーバ１２２から返された第二の一時的な資格を受信することである。

【００２８】

ここで、第一の一時的な資格を第二のサービス提供サブシステムに送信してクライアント識別子を変更することは、具体的に、第一の一時的な資格を第二のサービス提供サブシステムにおける第二のクライアント１２１に送信してクライアント識別子を変更することである。

【００２９】

ここで、前記第二の許可資格を第二のサービス提供サブシステムに送信して第二のアクセストークンを引き換えることは、具体的に、前記第二の許可資格を第二のサービス提供サブシステムにおける第二のＯＡｕｔｈサーバ１２２に送信して第二のアクセストークンを引き換えることである。

【００３０】

ここで、第二のアクセストークンを第二のサービス提供サブシステムに送信して認証し、第二のサービス提供サブシステムで認証に成功した後に、第二のサービス提供サブシステムから提供された第二のサービスリソースにアクセスすることは、具体的に、第二のアクセストークンを第二のサービス提供サブシステムにおける第二のリソースサーバ１２３に送信して認証し、第二のサービス提供サブシステムにおける第二のリソースサーバ１２３で認証に成功した後に、第二のサービス提供サブシステムにおける第二のリソースサーバ１２３から提供された第二のサービスリソースにアクセスすることである。

【００３１】

前記第一のＯＡｕｔｈサーバ１１２は、第一のクライアント１１１から送信された一時的な資格要求命令を受信し、そして当該命令に応じて第一の一時的な資格を第一のクライアント１１１に返し、第二のサービス提供サブシステムから送信された第一の許可資格を受信し、第一のアクセストークンを第二のサービス提供サブシステムに返し、そして第一のアクセストークンを第一のリソースサーバ１１３に送信して認証資格とするように構成される。

【００３２】

ここで、前記第二のサービス提供サブシステムは、具体的に第二のサービス提供サブシステムにおける第二のクライアント１２１である。

【００３３】

前記第一のリソースサーバ１１３は、第二のサービス提供サブシステムから送信された第一のアクセストークンを受信し、そして第一のＯＡｕｔｈサーバ１１２から送信された第一のアクセストークンに基づいて第二のサービス提供サブシステムから送信された第一のアクセストークンを認証し、認証に成功した後に第一のサービスリソースを第二のサービス提供サブシステムに提供してアクセスするように構成される。

【００３４】

ここで、前記第二のサービス提供サブシステムは、具体的に第二のサービス提供サブシステムにおける第二のクライアント１２１である。

【００３５】

ここで、前記認証は、２つのアクセストークンを比較し、２つのアクセストークンが同じであると、認証に成功し、２つのアクセストークンが異なると、認証に失敗することである。

【００３６】

上記の解決手段において、前記一時的な資格要求命令がオープン許可（ＯＡｕｔｈ）プロトコルによって定義された一時的な資格要求メッセージで搬送され、前記メッセージはクライアント識別子を含み、好ましくは、第一のサービス提供サブシステムから送信された一時的な資格要求命令であるので、前記一時的な資格要求命令は第一のクライアント識

別子を含む。
【００３７】
上記の解決手段において、前記第一の一時的な資格、第二の一時的な資格がＯＡｕｔｈプロトコルによって定義された応答メッセージで伝送され、前記メッセージは第一のクライアント識別子を含む。そのため、第一の一時的な資格が第二のクライアント１２１に送信される場合、それに含まれている第一のクライアント識別子を第二のクライアント識別子に変更する必要がある。
【００３８】
上記の解決手段において、前記一時的な資格の要求と取得は、ハイパーテキスト伝送プロトコル（ＨＴＴＰ：ＨｙｐｅｒＴｅｘｔ　Ｔｒａｎｓｐｏｒｔ　Ｐｒｏｔｏｃｏｌ）方式を使用し、且つセキュア-ソケット-レイヤー（ＳＳＬ：Ｓｅｃｕｒｅ　Ｓｏｃｋｅｔｓ　Ｌａｙｅｒ）または同じ安全レベルの方式を使用して一時的な資格の安全性を保証する。
【００３９】
上記の解決手段において、前記第二の一時的な資格の認可は、具体的に、第二のサービス提供サブシステムのユーザ名とパスワードを入力することであり、前記第一の一時的な資格の認可は、具体的に、第一のサービス提供サブシステムのユーザ名とパスワードを入力することである。
【００４０】
前記第二のクライアント１２１は、第一のサービス提供サブシステムから送信された第一の一時的な資格を受信し、そして前記第一の一時的な資格における第一のクライアント識別子を第二のクライアント識別子に変更し、変更された第一の一時的な資格をユーザ端末１３に送信して許可し、ユーザ端末１３から返された第一の許可資格を受信し、前記第一の許可資格を第一のサービス提供サブシステムに送信して第一のアクセストークンを引き換え、第一のアクセストークンを第一のサービス提供サブシステムに送信して認証し、第一のサービス提供サブシステムで認証に成功した後に、第一のサービス提供サブシステムから提供された第一のサービスリソースにアクセスするように構成される。
【００４１】
ここで、第一のサービス提供サブシステムから送信された第一の一時的な資格を受信することは、具体的に、第一のサービス提供サブシステムにおける第一のクライアント１１１から送信された第一の一時的な資格を受信することである。
【００４２】
ここで、第一の許可資格を第一のサービス提供サブシステムに送信して第一のアクセストークンを引き換えることは、具体的に、第一の許可資格を第一のサービス提供サブシステムにおける第一のＯＡｕｔｈサーバ１１２に送信して第一のアクセストークンを引き換えることである。
【００４３】
ここで、第一のアクセストークンを第一のサービス提供サブシステムに送信して認証し、第一のサービス提供サブシステムで認証に成功した後に、第一のサービス提供サブシステムから提供された第一のサービスリソースにアクセスすることは、具体的に、第一のアクセストークンを第一のサービス提供サブシステムにおける第一のリソースサーバ１１３に送信して認証し、第一のサービス提供サブシステムにおける第一のリソースサーバ１１３で認証に成功した後に、第一のサービス提供サブシステムにおける第一のリソースサーバ１１３から提供される第一のサービスリソースにアクセスすることである。
【００４４】
前記第二のＯＡｕｔｈサーバ１２２は、第一のサービス提供サブシステムから送信された一時的な資格要求命令を受信し、そして当該命令に応じて第二の一時的な資格を第一のサービス提供サブシステムに返し、第一のサービス提供サブシステムから送信された第二の許可資格を受信し、第二のアクセストークンを第一のサービス提供サブシステムに返し、そして前記第二のアクセストークンを第二のリソースサーバ１２３に送信して認証資格

とするように構成される。

【００４５】

ここで、前記第一のサービス提供サブシステムは、具体的に第一のサービス提供サブシステムにおける第一のクライアント１１１である。

【００４６】

前記第二のリソースサーバ１２３は、第一のサービス提供サブシステムから送信された第二のアクセストークンを受信し、そして第二のＯＡｕｔｈサーバ１２２から送信された第二のアクセストークンに基づいて第一のサービス提供サブシステムから送信された第二のサービストークンを認証し、認証に成功した後に第二のサービスリソースを第一のサービス提供サブシステムに提供してアクセスするように構成される。

【００４７】

ここで、前記第一のサービス提供サブシステムは、具体的に第一のサービス提供サブシステムにおける第一のクライアント１１１である。

【００４８】

上記の解決手段において、前記第一の一時的な資格は第一のリソースサーバに対する第一のクライアントの一時的な資格であり、第二の一時的な資格は第二のリソースサーバに対する第一のクライアントの一時的な資格である。第一の一時的な資格に対してクライアント識別子を変更した後、第一の一時的な資格は第一のリソースサーバに対する第二のクライアントの一時的な資格となり、それに応じて、第一の許可資格は第一のリソースサーバに対する第二のクライアントの許可資格である。第二の許可資格は第二のリソースサーバに対する第一のクライアントの許可資格であり、それに応じて、第一のアクセストークンは第一のリソースサーバに対する第二のクライアントのアクセストークンであり、第二のアクセストークンは第二のリソースサーバに対する第一のクライアントのアクセストークンである。

【００４９】

上記の解決手段において、第一のサービス提供サブシステムを開始側のサービス提供サブシステムとし、第二のサービス提供サブシステムを受信側のサービス提供サブシステムとする。実際の適用において、第二のサービス提供サブシステムを開始側のサービス提供サブシステムとし、第一のサービス提供サブシステムを受信側のサービス提供サブシステムとすることもできる。それに応じて、第二のサービス提供サブシステムに含まれる第二のクライアント１２１、第二のＯＡｕｔｈサーバ１２２、第二のリソースサーバ１２３がそれぞれ第一のクライアント１１１、第一のＯＡｕｔｈサーバ１１２、第一のリソースサーバ１１３により実行される機能を実行し、第一のサービス提供サブシステムに含まれる第一のクライアント１１１、第一のＯＡｕｔｈサーバ１１２、第一のリソースサーバ１１３がそれぞれ第二のクライアント１２１、第二のＯＡｕｔｈサーバ１２２、第二のリソースサーバ１２３により実行される機能を実行する。

【００５０】

実際の適用において、前記第一のサービス提供サブシステムにおける第一のクライアント１１１、第一のＯＡｕｔｈサーバ１１２は、第一のサービス提供サブシステムにおける中央プロセッサ（ＣＰＵ：Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）、またはデジタル信号プロセッサ（ＤＳＰ：Ｄｉｇｉｔａｌ　Ｓｉｇｎａｌ　Ｐｒｏｃｅｓｓｏｒ）、プログラマブルゲートアレイ（ＦＰＡＧ：Ｆｉｅｌｄ－Ｐｒｏｇｒａｍｍａｂｌｅ　Ｇａｔｅ　Ａｒｒａｙ）により実現されることができ、第一のリソースサーバ１１３は、第一のサービス提供サブシステムにおけるメモリにより実現されることができる。

【００５１】

前記第二のサービス提供サブシステムにおける第二のクライアント１２１、第二のＯＡｕｔｈサーバ１２２は、第二のサービス提供サブシステムにおけるＣＰＵ、またはＤＳＰ、またはＦＰＧＡにより実現されることができ、第二のリソースサーバ１２３は、第二のサービス提供サブシステムにおけるメモリにより実現されることができる。

【００５２】

図３は、本発明の実施形態による双方向許可システムにおけるクライアントの構成構造図である。当該クライアントは、サービス提供サブシステムに設置され、前記サービス提供サブシステムは、クライアント、ＯＡｕｔｈサーバ、リソースサーバを含み、前記クライアントは、一時的な資格取得モジュール３１、アクセストークン取得モジュール３２、リソース取得モジュール３３を含む。ここで、クライアントが開始側のクライアントである場合は、

前記一時的な資格取得モジュール３１は、本側のサービス提供サブシステムのＯＡｕｔｈサーバ、他側のサービス提供サブシステムのＯＡｕｔｈサーバへ一時的な資格要求命令をそれぞれ送信し、本側のサービス提供サブシステムのＯＡｕｔｈサーバ、他側のサービス提供サブシステムのＯＡｕｔｈサーバからそれぞれ返された第一の一時的な資格、第二の一時的な資格を受信し、第一の一時的な資格を他側のサービス提供サブシステムのクライアントに送信するように構成され、

前記アクセストークン取得モジュール３２は、第二の一時的な資格をユーザ端末に送信して許可し、ユーザ端末から返された第二の許可資格を受信し、前記第二の許可資格を他側のサービス提供サブシステムのＯＡｕｔｈサーバに送信して第二のアクセストークンを引き換えるように構成され、

前記リソース取得モジュール３３は、第二のアクセストークンを他側のサービス提供サブシステムのリソースサーバに送信して認証し、他側のサービス提供サブシステムのリソースサーバで認証に成功した後に、他側のサービス提供サブシステムのリソースサーバから提供されたリソースにアクセスするように構成される。

【００５３】

クライアントが受信側のクライアントである場合は、

前記一時的な資格取得モジュール３１は、他側のサービス提供サブシステムのＯＡｕｔｈサーバから送信された第一の一時的な資格を受信し、そして前記第一の一時的な資格における他側のサービス提供サブシステムのクライアント識別子を本側のサービス提供サブシステムのクライアント識別子に変更するように構成され、

前記アクセストークン取得モジュール３２は、変更された第一の一時的な資格をユーザ端末に送信して許可し、ユーザ端末から返された第一の許可資格を受信し、前記第一の許可資格を他側のサービス提供サブシステムのＯＡｕｔｈサーバに送信して第一のアクセストークンを引き換えるように構成され、

前記リソース取得モジュール３３は、第一のアクセストークンを他側のサービス提供サブシステムのリソースサーバに送信して認証し、他側のサービス提供サブシステムのリソースサーバで認証に成功した後に、他側のサービス提供サブシステムのソースサーバから提供されたリソースにアクセスするように構成される。

【００５４】

実際の適用において、前記クライアントにおける一時的な資格取得モジュール３１、アクセストークン取得モジュール３２、リソース取得モジュール３３は、クライアントにおけるＣＰＵ、またはＤＳＰ、またはＦＰＧＡにより実現されることができる。

【００５５】

図４は本発明の実施形態による双方向許可方法のフローチャートであり、図４に示すように、当該方法は、以下のステップを含む。

【００５６】

ステップ４０１において、第一のサービス提供サブシステムは、第一のサービス提供サブシステムの第一の一時的な資格、第二のサービス提供サブシステムの第二の一時的な資格を取得し、第二の一時的な資格をユーザ端末に送信して許可し、第二の許可資格を取得し、第二の許可資格を第二のサービス提供サブシステムに送信して第二のアクセストークンを引き換え、前記第二のアクセストークンに基づいて第二のサービス提供サブシステムのリソースを取得し、第一の一時的な資格を第二のサービス提供サブシステムに送信して識別子を変更するように構成される。

【００５７】

ここで、前記第一のサービス提供サブシステムが第一のサービス提供サブシステムの第一の一時的な資格、第二のサービス提供サブシステムの第二の一時的な資格を取得することは、具体的に、第一のサービス提供サブシステムにおける第一のクライアントが第一のサービス提供サブシステムにおける第一のＯＡｕｔｈサーバ、第二のサービス提供サブシステムにおける第二のＯＡｕｔｈサーバへ一時的な資格要求命令をそれぞれ送信し、第一のＯＡｕｔｈサーバ、第二のＯＡｕｔｈサーバから返された第一の一時的な資格、第二の一時的な資格を受信することである。

【００５８】

上記の解決手段において、前記一時的な資格要求命令がＯＡｕｔｈプロトコルによって定義されたメッセージで実現されることができ、前記メッセージはクライアント識別子を含み、好ましくは、第一のサービス提供サブシステムから送信された一時的な資格要求命令であるので、前記一時的な資格要求命令は第一のクライアント識別子、例えばｄｐｆ４３ｆ３ｐ２１４ｋ３１０３を含む。

【００５９】

上記の解決手段において、前記第一の一時的な資格、第二の一時的な資格がＯＡｕｔｈプロトコルによって定義された応答メッセージで伝送され、前記応答メッセージは第一のクライアント識別子と第一の一時的な資格、または第一のクライアント識別子と第二の一時的な資格、例えばｈｈ５ｓ９３ｊ４ｈｄｉｄｐｏｌａを含む。

【００６０】

上記の解決手段において、前記一時的な資格の要求および取得は、ＨＴＴＰ方式を使用し、且つＳＳＬまたは同じ安全レベルの方式を使用して伝送して一時的な資格の安全を保証する。

【００６１】

上記の解決手段において、第二の一時的な資格の許可は、具体的に、第二のサービス提供サブシステムのユーザ名とパスワードを入力することであり、前記ユーザ名とパスワードは、ユーザ端末が第二のサービス提供サブシステムに登録したユーザ名とパスワードである。

【００６２】

上記の解決手段において、前記第二のアクセストークンに基づいて第二のサービス提供サブシステムにおける第二のサービスリソースを取得することは、具体的に、第二のアクセストークンを第二のサービス提供サブシステムに送信して認証し、第二のサービス提供サブシステムで認証に成功した後に、第二のサービス提供サブシステムから提供された第二のサービスリソースにアクセスすることを含む。

【００６３】

ここで、前記第一の一時的な資格は第一のクライアント識別子を含む。そのため、第一の一時的な資格が第二のクライアントへ送信された場合、それに含まれている第一のクライアント識別子を第二のクライアント識別子に変更する必要がある。

【００６４】

ステップ４０２において、第二のサービス提供サブシステムは、変更された第一の一時的な資格をユーザ端末に送信して許可し、第一の許可資格を取得し、第一の許可資格を第一のサービス提供サブシステムに送信して第一のアクセストークンを引き換え、前記第一のアクセストークンに基づいて第一のサービス提供サブシステムのリソースを取得する。

【００６５】

上記の解決手段において、前記第一の一時的な資格の許可は、具体的に、第一のサービス提供サブシステムのユーザ名とパスワードを入力することであり、前記ユーザ名とパスワードは、ユーザ端末が第一のサービス提供サブシステムに登録したユーザ名とパスワードである。

【００６６】

上記の解決手段において第一のサービス提供サブシステムを開始側のサービス提供サブシステムとし、第二のサービス提供サブシステムを受信側のサービス提供サブシステムと

する。実際の適用において、第二のサービス提供サブシステムを開始側のサービス提供サブシステムとし、第一のサービス提供サブシステムを受信側のサービス提供サブシステムとすることもでき、それに応じて、第二のサービス提供サブシステムがステップ４０１を実行し、第一のサービス提供サブシステムがステップ４０２を実行する。

【００６７】

以下に具体的な実施形態を参照して本発明による双方向許可方法をさらに説明する。

【００６８】

ビデオサイトとマイクロブログサイトが本発明の実施形態における２つのサービス提供サブシステムであると仮定する。ユーザ端末は、ビデオサイトにユーザ名とパスワードを登録し、マイクロブログサイトにもユーザ名とパスワードを登録した。ビデオサイトとマイクロブログサイトがそれぞれのクライアント、ＯＡｕｔｈサーバおよびリソースサーバを含み、ビデオサイト側のリソースサーバがユーザ端末のビデオリソースを記憶するように構成され、マイクロブログサイト側のリソースサーバがユーザ端末のマイクロブログリソースを記憶するように構成される。

【００６９】

ユーザ端末がそのビデオサイトでのリソースをマイクロブログサイトに共有するとともに、そのマイクロブログサイトでのリソースをビデオサイトに共有する場合、マイクロブログサイト側のクライアントは、マイクロブログサイト側のＯＡｕｔｈサーバおよびビデオサイト側のＯＡｕｔｈサーバへ一時的な資格要求命令を送信する必要がある。マイクロブログサイト側のＯＡｕｔｈサーバが第一の一時的な資格をマイクロブログサイト側のクライアントに返し、ビデオサイト側のＯＡｕｔｈサーバが第二の一時的な資格をマイクロブログサイト側のクライアントに返す。マイクロブログサイト側のクライアントが前記第二の一時的な資格をユーザ端末に送信し、ユーザ端末がユーザ名とパスワードを入力するように提示する。ユーザ端末がそのビデオサイト側に登録したユーザ名とパスワードを入力した後、第二の許可資格をマイクロブログサイト側のクライアントに返し、マイクロブログサイト側のクライアントが前記第二の許可資格をビデオサイト側のＯＡｕｔｈサーバに送信して第二のアクセストークンを引き換える。このようにして、マイクロブログサイト側のクライアントが前記第二のアクセストークンによりビデオサイト側のリソースを共有することができる。それと同時にマイクロブログサイト側のクライアントが第一の一時的な資格をビデオサイト側のクライアントに送信し、ビデオサイト側のクライアントが第一の一時的な資格を変更してユーザ端末に送信し、そしてユーザ端末がユーザ名とパスワードを入力するように提示する。ユーザ端末がそのマイクロブログサイトに登録したユーザ名とパスワードを入力した後、第一の許可資格をビデオサイト側のクライアントに返し、ビデオサイト側のクライアントが前記第一の許可資格をマイクロブログサイト側のＯＡｕｔｈサーバに送信して第一のアクセストークンを引き換える。このようにして、ビデオサイト側のクライアントが前記第一のアクセストークンによりマイクロブログサイト側のリソースを共有する。

【００７０】

上述したように、本発明の実施形態による双方向許可方法により、ユーザ端末は、ビデオサイトのリソースをマイクロブログサイト側に共有するとともに、そのマイクロブログサイトでのリソースをビデオサイトに共有することができる。

【００７１】

上記は、本発明の好ましい実施形態に過ぎなく、本発明の保護範囲を限定することに用いられるものではない。

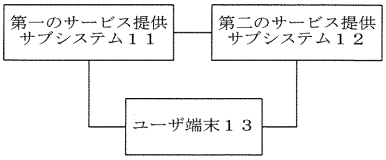
【符号の説明】

【００７２】

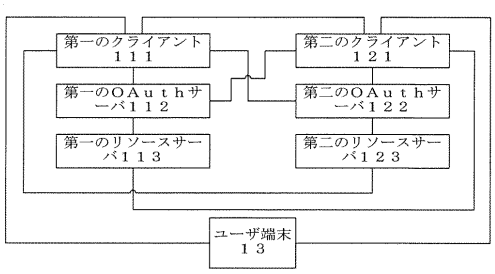
１１・・・第一のサービス提供サブシステム、１２・・・第二のサービス提供サブシステム、１３・・・ユーザ端末、３１・・・一時的な資格取得モジュール、３２・・・アクセストークン取得モジュール、３３・・・リソース取得モジュール、１１１・・・第一のクライアント、１１２・・・第一のＯＡｕｔｈサーバ、１１３・・・第一のリソースサーバ

、１２１・・・第二のクライアント、１２２・・・第二のＯＡｕｔｈサーバ、１２３・・・第二のリソースサーバ。

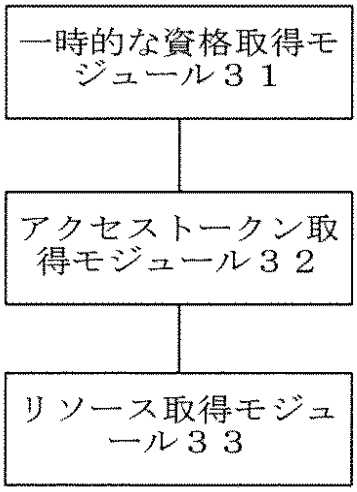
【図１】



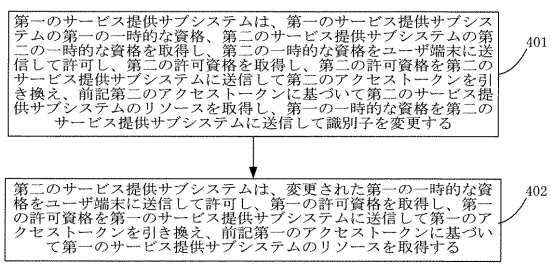
【図２】



【図３】



【図４】



フロントページの続き

(72)発明者　劉　先
中華人民共和国５１８０５７広東省深セン市南山区高新技術産業園科技南路中興通訊大厦

審査官　児玉　崇晶

(56)参考文献　米国特許出願公開第２０１３／００１９２９５（ＵＳ，Ａ１）
特開２００２－３００１５５（ＪＰ，Ａ）
特開２００３－１３２２５３（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／３３
Ｇ０６Ｆ　２１／６２