(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5423397号
(P5423397)
(45)発行日　平成26年2月19日(2014.2.19)　(24)登録日　平成25年12月6日(2013.12.6)

(51)Int.Cl.　　F I
G06F 21/33 (2013.01)　　G06F 21/20 133
G06F 21/31 (2013.01)　　G06F 21/20 131A
G06F 21/62 (2013.01)　　G06F 21/24 163A

請求項の数 22　(全 31 頁)

(21)出願番号　特願2009-548071 (P2009-548071)
(86)(22)出願日　平成20年12月25日(2008.12.25)
(86)国際出願番号　PCT/JP2008/073644
(87)国際公開番号　WO2009/084601
(87)国際公開日　平成21年7月9日(2009.7.9)
審査請求日　平成23年9月7日(2011.9.7)
(31)優先権主張番号　特願2007-335988 (P2007-335988)
(32)優先日　平成19年12月27日(2007.12.27)
(33)優先権主張国　日本国(JP)

(73)特許権者　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(74)代理人　100130029
弁理士　永井　道雄
(74)代理人　100166338
弁理士　関口　正夫
(74)代理人　100152054
弁理士　仲野　孝雅
(72)発明者　畠山　誠
日本国東京都港区芝五丁目７番１号　日本電気株式会社内

審査官　甲斐　哲雄

最終頁に続く

(54)【発明の名称】アクセス権限管理システム、アクセス権限管理方法及びアクセス権限管理用プログラム

(57)【特許請求の範囲】
【請求項１】
権限を委譲する条件を管理する認証装置と、サービス要求に応じてサービスを提供するサービス提供装置と、前記サービス提供装置へのアクセスを代行するサービス代理アクセス装置とを備え、
前記認証装置は、
他の装置に対してユーザに関する情報が記載されたユーザ認証情報を発行するユーザ認証証明書生成手段と、
権限移譲先のユーザの情報と権限を委譲する条件とに基づいて、権限委譲情報と権限委譲情報に対応するトークンとを他の装置に対して発行する権限委譲証明書・トークン生成手段とを含み、
前記サービス代理アクセス装置は、
他の装置にアクセスするための権限委譲情報とトークンの発行を要求するトークン要求手段と、
トークンを利用して他のサービスにアクセスするユーザ代理アクセス手段とを含み、
前記サービス提供装置は、トークンを利用して前記認証装置からユーザ認証情報を取得するユーザ認証証明書要求手段を含む
ことを特徴とするアクセス権限管理システム。
【請求項２】
サービス提供装置は、

ユーザ認証情報に記載されているユーザの代理として他の装置にアクセスするための権限委譲情報とトークンの発行を要求するトークン要求手段と、
他の装置に対してトークンを利用して他のサービスにアクセスするユーザ代理アクセス手段とを更に含む
請求項１記載のアクセス権限管理システム。
【請求項３】
認証装置は、権限を委譲するユーザが設定したアクセス権限を委譲する条件を格納する権限委譲条件格納手段を更に含み、
権限委譲証明書・トークン生成手段は、前記権限委譲条件格納手段に格納されている権限を委譲する条件に基づいて、権限委譲情報と権限委譲情報に対応するトークンとを発行する
請求項１または請求項２記載のアクセス権限管理システム。
【請求項４】
認証装置は、
権限委譲証明書・トークン生成手段が発行した権限委譲情報と、その権限委譲情報に対応するトークンとを保管する証明書格納手段と、
トークンを受信すると、受信したトークンに対応する権限委譲情報を前記証明書格納手段から取得する証明書要求受付手段とを更に含む
請求項１から請求項３のうちのいずれか１項に記載のアクセス権限管理システム。
【請求項５】
認証装置は、別のユーザへのアクセス権限の委譲を認めるか否か判断する権限ユーザ変換手段を含み、
権限委譲証明書・トークン生成手段は、前記権限ユーザ変換手段が権限委譲を認めると判断した場合に、権限委譲情報と権限委譲情報に対応するトークンとを発行する
請求項１から請求項４のうちのいずれか１項に記載のアクセス権限管理システム。
【請求項６】
サービス要求に応じてサービスを提供するサービス提供装置及び前記サービス提供装置へのアクセスを代行するサービス代理アクセス装置と接続されると共に、権限を委譲する条件を管理する認証装置であって、
前記サービス代理アクセス装置は、
他の装置にアクセスするための権限委譲情報とトークンの発行を要求するトークン要求手段と、
トークンを利用して他のサービスにアクセスするユーザ代理アクセス手段とを含み、
前記サービス提供装置は、トークンを利用して前記認証装置からユーザ認証情報を取得するユーザ認証証明書要求手段を含み、
当該認証装置は、
他の装置に対してユーザに関する情報が記載されたユーザ認証情報を発行するユーザ認証証明書生成手段と、
権限移譲先のユーザの情報と権限を委譲する条件とに基づいて、権限委譲情報と権限委譲情報に対応するトークンとを他の装置に対して発行する権限委譲証明書・トークン生成手段とを備える
ことを特徴とする認証装置。
【請求項７】
別のユーザへのアクセス権限の委譲を認めるか否か判断する権限ユーザ変換手段と、
前記権限ユーザ変換手段が別のユーザへのアクセス権限委譲を認めた場合にサービス提供装置に送付する権限委譲情報と、サービス代理アクセス装置に送付する権限委譲情報に対応するトークンとを発行する手段とを更に備えた請求項６記載の認証装置。
【請求項８】
権限を委譲する条件を管理する認証装置及びサービス要求に応じてサービスを提供するサービス提供装置と接続されると共に、前記サービス提供装置へのアクセスを代行するサ

ービス代理アクセス装置であって、
前記認証装置は、
他の装置に対してユーザに関する情報が記載されたユーザ認証情報を発行するユーザ認証証明書生成手段と、
権限移譲先のユーザの情報と権限を委譲する条件とに基づいて、権限委譲情報と権限委譲情報に対応するトークンとを他の装置に対して発行する権限委譲証明書・トークン生成手段とを含み、
前記サービス提供装置は、トークンを利用して前記認証装置からユーザ認証情報を取得するユーザ認証証明書要求手段を含み、
当該サービス代理アクセス装置は、
他の装置にアクセスするための権限委譲情報とトークンの発行を要求するトークン要求手段と、
トークンを利用して他のサービスにアクセスするユーザ代理アクセス手段とを備える
ことを特徴とするサービス代理アクセス装置。
【請求項９】
アクセス権限を格納する代理アクセス情報格納手段と、
当該サービス代理アクセス装置がユーザの代理としてサービス提供装置に代理アクセスできる場合に、認証装置より取得したトークンを利用してサービス提供装置にアクセスする手段とを更に備えた請求項８記載のサービス代理アクセス装置。
【請求項１０】
権限を委譲する条件を管理する認証装置及び当該サービス提供装置へのアクセスを代行するサービス代理アクセス装置と接続されると共に、サービス要求に応じてサービスを提供するサービス提供装置であって、
前記認証装置は、
他の装置に対してユーザに関する情報が記載されたユーザ認証情報を発行するユーザ認証証明書生成手段と、
権限移譲先のユーザの情報と権限を委譲する条件とに基づいて、権限委譲情報と権限委譲情報に対応するトークンとを他の装置に対して発行する権限委譲証明書・トークン生成手段とを含み、
前記サービス代理アクセス装置は、
他の装置にアクセスするための権限委譲情報とトークンの発行を要求するトークン要求手段と、
トークンを利用して他のサービスにアクセスするユーザ代理アクセス手段とを含み、
当該サービス提供装置は、トークンを利用して前記認証装置からユーザ認証情報を取得するユーザ認証証明書要求手段を備える
ことを特徴とするサービス提供装置。
【請求項１１】
他のサービス提供装置にアクセスするためのトークンを認証装置より取得する手段と、
前記トークンと共に前記サービス提供装置へアクセス要求を送付する手段とを更に備えた請求項１０記載のサービス提供装置。
【請求項１２】
権限委譲条件を管理し、ユーザ認証情報を発行する認証装置が、サービス要求に応じてサービスを提供するサービス提供装置と、前記サービス提供装置へのアクセスを代行するサービス代理アクセス装置に権限委譲に関する情報やトークンを生成、配布するアクセス権限管理方法であって、
前記認証装置が、
他の装置に対してユーザに関する情報が記載されたユーザ認証情報を生成し、
権限移譲先のユーザの情報と権限を委譲する条件とに基づいて、権限委譲情報と権限委譲情報に対応するトークンとを他の装置に対して発行し、
前記サービス代理アクセス装置が、

他の装置にアクセスするための権限委譲情報とトークンの発行を要求し、
トークンを利用し他のサービスにアクセスし、
前記サービス提供装置が、トークンを利用して前記認証装置からユーザ認証情報を取得する
ことを特徴とするアクセス権限管理方法。
【請求項１３】
認証装置が、
別のユーザにアクセス権限を委譲する条件を設定し、
ユーザが設定したアクセス権限を委譲する条件を格納し、
権限委譲証明書・トークン生成ステップで発行された権限委譲情報と権限委譲情報に対応するトークンとを証明書格納手段に保管し、
トークンを受信すると、受信したトークンに対応する権限委譲情報を前記証明書格納手段から取得する
請求項１２記載のアクセス権限管理方法。
【請求項１４】
サービス代理アクセス装置が、
アクセスしているユーザのユーザ認証情報を取得し、
取得したユーザ認証情報を保管する
請求項１２または請求項１３記載のアクセス権限管理方法。
【請求項１５】
サービス提供装置が、他の装置からユーザに関する情報を取得するためのトークンを受信し、
ユーザに関する情報を検証してサービス情報へのアクセスの可否を判定し、
他の装置に提供するサービスを保管する
請求項１２から請求項１４のうちのいずれか１項に記載のアクセス権限管理方法。
【請求項１６】
サービス提供装置が、
他の装置にアクセスするための権限委譲情報とトークンの発行を要求し、
前記トークンを利用して他のサービスにアクセスする
請求項１５記載のアクセス権限管理方法。
【請求項１７】
サービス要求に応じてサービスを提供するサービス提供装置及び前記サービス提供装置へのアクセスを代行するサービス代理アクセス装置と接続されるコンピュータを、権限を委譲する条件を管理する認証装置として機能させる認証プログラムであって、
前記サービス代理アクセス装置は、
他の装置にアクセスするための権限委譲情報とトークンの発行を要求するトークン要求手段と、
トークンを利用して他のサービスにアクセスするユーザ代理アクセス手段とを含み、
前記サービス提供装置は、トークンを利用して前記認証装置からユーザ認証情報を取得するユーザ認証証明書要求手段を含み、
前記コンピュータを、
他の装置に対してユーザに関する情報が記載されたユーザ認証情報を発行するユーザ認証証明書生成手段と、
権限移譲先のユーザの情報と権限を委譲する条件とに基づいて、権限委譲情報と権限委譲情報に対応するトークンとを他の装置に対して発行する権限委譲証明書・トークン生成手段とを備える認証装置として機能させることを特徴とする認証用プログラム。
【請求項１８】
別のユーザへのアクセス権限の委譲を認めるか否か判断する判断する手段と、
前記判断手段が別のユーザへのアクセス権限委譲を認めると、サービス提供装置に送付する権限委譲情報とサービス代理アクセス装置に送付する権限委譲情報に対応するトーク

ンとを発行する手段と、
を更に備える認証装置として前記コンピュータを機能させる請求項１７記載の認証用プログラム。
【請求項１９】
権限を委譲する条件を管理する認証装置及びサービス要求に応じてサービスを提供するサービス提供装置と接続されるコンピュータを、前記サービス提供装置へのアクセスを代行するサービス代理アクセス装置として機能させるサービス代理アクセスプログラムであって、
前記認証装置は、
他の装置に対してユーザに関する情報が記載されたユーザ認証情報を発行するユーザ認証証明書生成手段と、
権限移譲先のユーザの情報と権限を委譲する条件とに基づいて、権限委譲情報と権限委譲情報に対応するトークンとを他の装置に対して発行する権限委譲証明書・トークン生成手段とを含み、
前記サービス提供装置は、トークンを利用して前記認証装置からユーザ認証情報を取得するユーザ認証証明書要求手段を含み、
前記コンピュータを、
他の装置にアクセスするための権限委譲情報とトークンの発行を要求するトークン要求手段と、
トークンを利用して他のサービスにアクセスするユーザ代理アクセス手段とを備えるサービス代理アクセス装置として機能させることを特徴とするサービス代理アクセスプログラム。
【請求項２０】
アクセス権限を格納する代理アクセス情報格納手段と、
前記コンピュータがユーザ代理としてサービス提供装置に代理アクセスできる場合に、認証装置より取得したトークンを利用してサービス提供装置にアクセスする手段とを、
更に備えるサービス代理アクセス装置として前記コンピュータを機能させる請求項１９記載のサービス代理アクセスプログラム。
【請求項２１】
権限を委譲する条件を管理する認証装置及び当該サービス提供装置へのアクセスを代行するサービス代理アクセス装置と接続されるコンピュータを、サービス要求に応じてサービスを提供するサービス提供装置として機能させるサービス提供プログラムであって、
前記認証装置は、
他の装置に対してユーザに関する情報が記載されたユーザ認証情報を発行するユーザ認証証明書生成手段と、
権限移譲先のユーザの情報と権限を委譲する条件とに基づいて、権限委譲情報と権限委譲情報に対応するトークンとを他の装置に対して発行する権限委譲証明書・トークン生成手段とを含み、
前記サービス代理アクセス装置は、
他の装置にアクセスするための権限委譲情報とトークンの発行を要求するトークン要求手段と、
トークンを利用して他のサービスにアクセスするユーザ代理アクセス手段とを含み、
前記コンピュータを、
トークンを利用して前記認証装置からユーザ認証情報を取得するユーザ認証証明書要求手段を備えるサービス提供装置として機能させることを特徴とするサービス提供プログラム。
【請求項２２】
他のサービス提供装置にアクセスするためのトークンを認証装置より取得する手段と、
前記トークンと共に前記他のサービス装置にアクセス要求を送付する手段と、を更に備える認証装置として前記コンピュータを機能させる請求項２１記載のサービス提供プログ

ラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ユーザ間での権限委譲を集中的に管理できるアクセス権限管理システム、アクセス権限管理方法及びアクセス権限管理用プログラムに関する。
【背景技術】
【０００２】
ネットワーク上の各事業者間でユーザに関する情報を連携するための技術として、標準化団体ＯＡＳＩＳで策定された標準技術仕様ＳＡＭＬ（Security Assertion Markup Language）がある。図２２は、非特許文献１に記載されているＳＡＭＬを利用した証明書生成配布システムの一例を示す構成図である。
【０００３】
図２２に示す証明書作成配布システムでは、アイデンティティプロバイダ（以下、ＩｄＰと表記する。）１００とサービスプロバイダ（以下、ＳＰと表記する。）１０１とユーザエージェント（利用者端末装置のソフトウエア）１０２とがネットワークを経由して相互に接続されている。このような構成を有する証明書生成配布システムの典型的な動作として、ＳＡＭＬアーティファクトプロファイルを用いて証明書の作成と配布とを行う手順を説明する。図２２に示す例において、ＩｄＰ１００とＳＰ１０１とは、それぞれユーザエージェント１０２を利用しているユーザに関する情報を、利用者情報１０３及び利用者情報１０４として記憶装置に保有していることを前提にする。
【０００４】
図２２に示す証明書生成配布システムにおいて、ユーザは、ユーザエージェント１０２を通じて、ＳＰ１０１の利用制限があるサービスを利用するために、ＳＰ１０１にアクセスする（図２２におけるステップ（１））。ＳＰ１０１は、利用者の証明書を取得するために、ＩｄＰ１００に対して証明書要求メッセージを送付し（図２２におけるステップ（２－ａ））、ユーザエージェント１０２はＳＰ１０１からの証明書要求メッセージをＩｄＰ１００にリダイレクトする（図２２におけるステップ（２－ｂ））。ＩｄＰ１００は、利用者情報１０３を利用してＸＭＬ（Extensible Markup Language）に準拠して記述された証明書（アサーション）を作成する（図２２におけるステップ（３））。更に、ＩｄＰ１００は、アサーションに対応するチケットの役割を担うアーティファクトを作成し、ユーザエージェント１０２に返信する（図２２におけるステップ（４－ａ））。ユーザエージェント１０２は、アーティファクトをＳＰ１０１に対してリダイレクトする（図２２におけるステップ（４－ｂ））。
【０００５】
ＳＰ１０１は、受信したアーティファクトをＩｄＰ１００に送付し、対応するアサーションを要求する（図２２におけるステップ（５））。ＩｄＰ１００は、ＳＰ１０１から受け取ったアーティファクトを確認し、対応するアサーションをＳＰ１０１に対して返信する（図２２におけるステップ（６））。ＳＰ１０１は、ＩｄＰ１００から受信したアサーションの正当性を確認し、ＳＰ１０１のセキュリティポリシを検証して利用者のサービスへのアクセス要求に対して許可を与えるか否かを判断する。そして、許可を与えると判断した場合にはユーザエージェント１０２に対するサービスの提供を開始する（図２２におけるステップ（７））。
【０００６】
以上のように、ＩｄＰ１００は、ユーザに関する証明書を作成し、それをＳＰ１０１に対して配布する。ここで、ＩｄＰ１００が配布する証明書には、ＳＰ１０１にアクセスしたユーザに関する情報を記載することが可能になっている。ここで、このユーザに関する情報としては例えば、ユーザ識別子情報や、証明書の有効範囲（配布されて有効となる対象の事業者）情報や、その他利用者に関する機密情報等が挙げられる。
【０００７】

また、アクセス権限の委譲を管理するシステムの一例が、特許文献１に記載されている。図２３は、特許文献１に記載された権限の委譲を実現するアクセス管理システムを説明するための説明図である。図２３に示す例では、組織Ａ（１１０）の構成員と組織Ｂ（１１１）の構成員との間での権限委譲を管理するシステムについて示している。或る組織Ａでは、リソース１１３が管理されている。別の組織Ｂでは、リソース１１３が管理されている。また、組織Ｂには、リソース１１３にアクセスするリソースアクセス者１１５が存在する。

【０００８】

図２３に示されたアクセス管理システムはつぎのように動作する。すなわち、最初に、組織Ａの管理者１１２が、組織Ｂの管理者１１４に信用情報を送付する（図２３のステップ（１））。信用情報には、組織Ａの管理者の代わりに組織Ｂのリソースアクセス者１１５がリソースにアクセスするための条件（権限を委譲するための条件）が記載されている。ここでは、リソースアクセス者１１５がリソースにアクセスするための条件を満たしているものとして説明を続ける。次に、組織Ｂの管理者１１４が、組織Ｂのリソースアクセス１１５に対して、組織Ａの管理者１１２の代わりに信用情報を発行する（図２３のステップ（２））。組織Ｂの管理者１１４が発行する信用情報には、組織Ａの管理者１１２が発行した信用情報が含まれる。その後、組織Ｂのリソースアクセス者１１５が、組織Ｂの管理者１１４が発行する信用情報とともに、組織Ａのリソース１１３に対してアクセス要求メッセージを送付する（図２３のステップ（３））。組織Ａのリソース１１３は、組織Ｂのリソースアクセス者１１５から送付された信用情報を元にアクセスの可否を判断し、何らかの情報を組織Ｂのリソースアクセス者１１５に送付する。

【０００９】

以上のように、組織Ａの管理者１１２は、アクセス権限を委譲する相手である組織Ｂに対して、代理アクセスをするための情報を送付することによって、アクセス権限の委譲を実現している。

【００１０】

【特許文献１】特開２００６－２５４４６４号公報

【非特許文献１】オアシス（ＯＡＳＩＳ）、”アサーションズ アンド プロトコル フォー ディ オアシス セキュリティ アサーション マークアップ ラングエッジ（Assertions and Protocol for the OASIS Security Assertion Markup Language） （ＳＡＭＬ）Ｖ２．０”［online］、２００５年3月１５日、［平成１９年１１月２６日検索］、インターネット、＜ＵＲＬ：http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf＞

【発明の開示】

【発明が解決しようとする課題】

【００１１】

もっとも、上述した特許文献１や非特許文献１に記載された技術には、以下のような解決すべき課題があった。

第１の課題は、特許文献１や非特許文献１に記載された技術を利用して、あるユーザ（ユーザ１）が、別のユーザ（ユーザ２）から委譲されたアクセス権限を利用して、サービスプロバイダ（ＳＰ１）に他のサービスプロバイダ（ＳＰ２）への代理アクセスを実行させる場合に、情報が漏洩する可能性が高いことである。代理アクセスするプロバイダ（ＳＰ１）とアクセス先となるサービスプロバイダ（ＳＰ２）との間で、サービスプロバイダが保有する全てのユーザ情報やアクセス権限を交換しなければならないからである

【００１２】

すなわち、特許文献１や非特許文献１に記載された技術では、ユーザ１とユーザ２の両者のアクセス権限情報を記載した証明書をＳＰ１とＳＰ２との間で交換するので、情報が漏えいする可能性が高い。特許文献１に記載された技術では、アクセス権限情報が全て記載された信用情報をサービスプロバイダ間で交換する。つまり、２つのサービスプロバイダは、アクセス権限や権限委譲の設定というユーザに関する全ての情報を交換する。また

、非特許文献１に記載された技術でも、ユーザに関する情報が記載された証明書をプロバイダ間で交換する。その結果、ユーザに関する情報を全て他のプロバイダに開示している。

【００１３】

あるユーザ（ユーザ１）が、別のユーザ（ユーザ２）から委譲されたアクセス権限を利用して、サービスプロバイダ（ＳＰ１）に他のサービスプロバイダ（ＳＰ２）への代理アクセスを実行させる場合に、ＳＰ１はユーザ１からアクセスを受け付けているので、ユーザ２の情報は不要である。また、ＳＰ２はユーザ２の権限で代理アクセスを受け入れているので、ユーザ２の権限情報のみが必要であり、ユーザ１の情報は不要になる。そのため、ＳＰ１とＳＰ２は、両方のユーザ情報を取得する必要がない。つまり、それぞれのサービスプロバイダにとって必要最低限のユーザ情報のみを利用できるようにすることが好ましい。

【００１４】

第２の課題は、あるユーザ（ユーザ１）が、別のユーザ（ユーザ２）から委譲されたアクセス権限を利用して、サービスプロバイダ（ＳＰ１）に他のサービスプロバイダ（ＳＰ２）への代理アクセスを実行させる場合に、ユーザ２は全てのプロバイダにアクセス権限や権限委譲に関する設定をポリシとして規定する必要があり、非効率的になることである。

【００１５】

その理由は、それぞれのプロバイダがアクセスの可否を判断するため情報を独立して管理しているためである。サービスプロバイダは、それぞれがユーザのアクセス可否情報を管理しているので、あるユーザが別のユーザに権限を委譲する場合には、関連する全てのプロバイダに委譲条件を設定する必要がある。非特許文献１に記載された技術では、サービスプロバイダが証明書を受け取ってから証明書を検証してアクセス制御している。よって、ユーザが権限委譲を設定する場合に、ユーザは全てのＳＰに対して権限委譲の設定する必要がある。また、特許文献１に記載された技術でも、アクセス制御する組織Ａの管理者がアクセス制御情報として信用情報を発行している。つまり、アクセスの対象となるリソースやサービスプロバイダ毎に、ユーザの権限委譲に関する設定を保管する必要がある。これらの方式では、リソースの数や連携しているサービスプロバイダの数が増えれば増えるほど、アクセス権限や権限委譲を設定する数が増えるため非効率的である。

【００１６】

そこで、本発明は、ある装置がユーザから委譲された権限で他の装置に代理アクセスする場合に、装置間で交換される情報を減らすことができるアクセス権限管理システム、アクセス権限管理方法及びアクセス権限管理用プログラムを提供することを目的とする。

【００１７】

また、本発明の他の目的は、アクセス制御や権限委譲に関する設定を一箇所で集中管理できるアクセス権限管理システム、アクセス権限管理方法及びアクセス権限管理用プログラムを提供することである。

【課題を解決するための手段】

【００１８】

本発明によるアクセス権限管理システムは、権限を委譲する条件を管理する認証装置と、サービス要求に応じてサービスを提供するサービス提供装置と、サービス提供装置へのアクセスを代行するサービス代理アクセス装置とを備え、認証装置が、他の装置に対してユーザに関する情報が記載されたユーザ認証情報を発行するユーザ認証証明書生成部と、権限移譲先のユーザの情報と権限を委譲する条件とに基づいて、権限委譲情報と権限委譲情報に対応するトークンとを他の装置に対して発行する権限委譲証明書・トークン生成部とを含み、サービス代理アクセス装置が、他の装置にアクセスするための権限委譲情報とトークンの発行を要求するトークン要求部と、トークンを利用して他のサービスにアクセスするユーザ代理アクセス部とを含み、サービス提供装置が、トークンを利用して認証装置からユーザ認証情報を取得するユーザ認証証明書要求部を含むことを特徴とする。

【００１９】
本発明による認証装置は、サービス要求に応じてサービスを提供するサービス提供装置及び前記サービス提供装置へのアクセスを代行するサービス代理アクセス装置と接続されると共に、権限を委譲する条件を管理する認証装置であって、前記サービス代理アクセス装置は、他の装置にアクセスするための権限委譲情報とトークンの発行を要求するトークン要求手段と、トークンを利用して他のサービスにアクセスするユーザ代理アクセス手段とを含み、前記サービス提供装置は、トークンを利用して前記認証装置からユーザ認証情報を取得するユーザ認証証明書要求手段を含み、当該認証装置は、他の装置に対してユーザに関する情報が記載されたユーザ認証情報を発行するユーザ認証証明書生成手段と、権限移譲先のユーザの情報と権限を委譲する条件とに基づいて、権限委譲情報と権限委譲情報に対応するトークンとを他の装置に対して発行する権限委譲証明書・トークン生成手段とを備えることを特徴とする。
【００２０】
本発明によるサービス代理アクセス装置は、権限を委譲する条件を管理する認証装置及びサービス要求に応じてサービスを提供するサービス提供装置と接続されると共に、前記サービス提供装置へのアクセスを代行するサービス代理アクセス装置であって、前記認証装置は、他の装置に対してユーザに関する情報が記載されたユーザ認証情報を発行するユーザ認証証明書生成手段と、権限移譲先のユーザの情報と権限を委譲する条件とに基づいて、権限委譲情報と権限委譲情報に対応するトークンとを他の装置に対して発行する権限委譲証明書・トークン生成手段とを含み、前記サービス提供装置は、トークンを利用して前記認証装置からユーザ認証情報を取得するユーザ認証証明書要求手段を含み、当該サービス代理アクセス装置は、他の装置にアクセスするための権限委譲情報とトークンの発行を要求するトークン要求手段と、トークンを利用して他のサービスにアクセスするユーザ代理アクセス手段とを備えることを特徴とする。
【００２１】
本発明によるサービス提供装置は、権限を委譲する条件を管理する認証装置及び当該サービス提供装置へのアクセスを代行するサービス代理アクセス装置と接続されると共に、サービス要求に応じてサービスを提供するサービス提供装置であって、前記認証装置は、他の装置に対してユーザに関する情報が記載されたユーザ認証情報を発行するユーザ認証証明書生成手段と、権限移譲先のユーザの情報と権限を委譲する条件とに基づいて、権限委譲情報と権限委譲情報に対応するトークンとを他の装置に対して発行する権限委譲証明書・トークン生成手段とを含み、前記サービス代理アクセス装置は、他の装置にアクセスするための権限委譲情報とトークンの発行を要求するトークン要求手段と、トークンを利用して他のサービスにアクセスするユーザ代理アクセス手段とを含み、当該サービス提供装置は、トークンを利用して前記認証装置からユーザ認証情報を取得するユーザ認証証明書要求手段を備えることを特徴とする。
【００２２】
本発明によるアクセス権限管理方法は、権限委譲条件を管理し、ユーザ認証情報を発行する認証装置が、サービス要求に応じてサービスを提供するサービス提供装置と、サービス提供装置へのアクセスを代行するサービス代理アクセス装置に権限委譲に関する情報やトークンを生成、配布するアクセス権限管理方法であって、認証装置が、他の装置に対してユーザに関する情報が記載されたユーザ認証情報を生成するユーザ認証証明書生成ステップと、権限移譲先のユーザの情報と権限を委譲する条件とに基づいて、権限委譲情報と権限委譲情報に対応するトークンとを他の装置に対して発行する権限委譲証明書・トークン生成ステップとを実行し、サービス代理アクセス装置が、他の装置にアクセスするための権限委譲情報とトークンの発行を要求するトークン要求ステップと、トークンを利用し他のサービスにアクセスするユーザ代理アクセスステップとを実行し、サービス提供装置が、トークンを利用して認証装置からユーザ認証情報を取得するユーザ認証証明書要求ステップを実行することを特徴とする。
【００２３】

本発明による認証用プログラムは、サービス要求に応じてサービスを提供するサービス提供装置及び前記サービス提供装置へのアクセスを代行するサービス代理アクセス装置と接続されるコンピュータを、権限を委譲する条件を管理する認証装置として機能させる認証プログラムであって、前記サービス代理アクセス装置は、他の装置にアクセスするための権限委譲情報とトークンの発行を要求するトークン要求手段と、トークンを利用して他のサービスにアクセスするユーザ代理アクセス手段とを含み、前記サービス提供装置は、トークンを利用して前記認証装置からユーザ認証情報を取得するユーザ認証証明書要求手段を含み、前記コンピュータを、他の装置に対してユーザに関する情報が記載されたユーザ認証情報を発行するユーザ認証証明書生成手段と、権限移譲先のユーザの情報と権限を委譲する条件とに基づいて、権限委譲情報と権限委譲情報に対応するトークンとを他の装置に対して発行する権限委譲証明書・トークン生成手段とを備える認証装置として機能させることを特徴とする。

【００２４】

本発明によるサービス代理アクセスプログラムは、権限を委譲する条件を管理する認証装置及びサービス要求に応じてサービスを提供するサービス提供装置と接続されるコンピュータを、前記サービス提供装置へのアクセスを代行するサービス代理アクセス装置として機能させるサービス代理アクセスプログラムであって、前記認証装置は、他の装置に対してユーザに関する情報が記載されたユーザ認証情報を発行するユーザ認証証明書生成手段と、権限移譲先のユーザの情報と権限を委譲する条件とに基づいて、権限委譲情報と権限委譲情報に対応するトークンとを他の装置に対して発行する権限委譲証明書・トークン生成手段とを含み、前記サービス提供装置は、トークンを利用して前記認証装置からユーザ認証情報を取得するユーザ認証証明書要求手段を含み、前記コンピュータを、他の装置にアクセスするための権限委譲情報とトークンの発行を要求するトークン要求手段と、トークンを利用して他のサービスにアクセスするユーザ代理アクセス手段とを備えるサービス代理アクセス装置として機能させることを特徴とする。

【００２５】

本発明によるサービス提供プログラムは、権限を委譲する条件を管理する認証装置及び当該サービス提供装置へのアクセスを代行するサービス代理アクセス装置と接続されるコンピュータを、サービス要求に応じてサービスを提供するサービス提供装置として機能させるサービス提供プログラムであって、前記認証装置は、他の装置に対してユーザに関する情報が記載されたユーザ認証情報を発行するユーザ認証証明書生成手段と、権限移譲先のユーザの情報と権限を委譲する条件とに基づいて、権限委譲情報と権限委譲情報に対応するトークンとを他の装置に対して発行する権限委譲証明書・トークン生成手段とを含み、前記サービス代理アクセス装置は、他の装置にアクセスするための権限委譲情報とトークンの発行を要求するトークン要求手段と、トークンを利用して他のサービスにアクセスするユーザ代理アクセス手段とを含み、前記コンピュータを、トークンを利用して前記認証装置からユーザ認証情報を取得するユーザ認証証明書要求手段を備えるサービス提供装置として機能させることを特徴とする。

【発明の効果】

【００２６】

本発明によれば、セキュリティとプライバシを保護しつつ、アクセス制御や権限委譲を実現できる。

【図面の簡単な説明】

【００２７】

【図１】本発明によるアクセス権限管理システム全体の基本的構成を示すブロック図である。

【図２】本発明によるアクセス権限管理システムの構成を示すブロック図である。

【図３】第１の発明形態における認証装置の構成例を示すブロック図である。

【図４】第１の発明形態における認証装置が発行するユーザ認証証明書の例である。

【図５】第１の発明形態における権限委譲の条件である権限委譲設定者と権限委譲先利用

者とアクセス先サービスＩＤとの対応を示す説明図である。
【図６】第１の発明形態におけるトークンと証明書との対応を示す説明図である。
【図７】第１の発明形態におけるサービス代理アクセス装置の構成を示すブロック図である。
【図８】第１の発明形態におけるサービス提供装置の構成を示すブロック図である。
【図９】第１の発明形態における処理の概要を示す流れ図である。
【図１０】第１の発明形態における、あるユーザが他のユーザに権限委譲を設定するときの認証装置に関する処理を示す流れ図である。
【図１１】第１の発明形態における、ユーザ認証証明書を要求・取得するときのサービス代理アクセス装置に関する処理を示す流れ図である。
【図１２】第１の発明形態における、ユーザ認証証明書を生成するときの認証装置に関する処理を示す流れ図である。
【図１３】第１の発明形態における、他のサービスに代理アクセスするときのサービス代理アクセス装置に関する処理を示す流れ図である。
【図１４】第１の発明形態における、権限委譲の証明書を発行し、証明書に関連するトークンを発行するときの認証装置に関する処理を示す流れ図である。
【図１５】第１の発明形態における、代理アクセスを受け付けるサービス提供装置に関する処理を示す流れ図である。
【図１６】第１の発明形態における、トークンから証明書を取得するときの認証装置に関する処理を示す流れ図である。
【図１７】第２の発明形態におけるサービス提供装置の構成を示すブロック図である。
【図１８】第２の発明形態における、代理アクセスを受け付けるサービス提供装置に関する処理を示す流れ図である。
【図１９】本発明の第３の実施形態の概要を示すブロック図である。
【図２０】本発明によるアクセス管理システムの第１の実施例の構成を示す構成図である。
【図２１】本発明によるアクセス管理システムの第２の実施例の構成を示す構成図である。
【図２２】非特許文献１に記載された証明書の配信を実現するためのシステムの構成を示す構成図である。
【図２３】特許文献１に記載された権限の委譲を実現するアクセス管理システムを説明するための説明図である。
【符号の説明】
【００２８】
１　認証装置
２　サービス代行アクセス装置
３　サービス提供装置
４　サービスアクセスユーザ端末装置
５　権限設定ユーザ端末装置
６　ネットワーク
７　サービス提供装置
１０　ユーザ認証証明書要求受付部
１１　ユーザ情報管理部
１２　ユーザ認証証明書生成部
１３　権限委譲設定情報受付部
１４　権限委譲証明書・トークン生成部
１５　権限ユーザ変換部
１６　権限委譲証明書・トークン管理部
１７　権限委譲証明書要求受付部
１８　証明書要求受付部

２０　ユーザ情報格納部
２１　権限委譲条件格納部
２２　サービス提供装置情報格納部
２３　証明書格納部
３１　ユーザ認証証明書要求部
３２　ユーザ代理アクセス部
３３　アクセス権限トークン要求部
３４　ユーザ証明書管理部
３５　ユーザ証明書検証部
３６　アクセス権限トークン管理部
４１　ユーザ認証証明書格納部
４２　代理アクセス情報格納部
４３　アクセス権限トークン格納部
５０　サービスアクセス受付部
５１　サービス情報管理部
５２　アクセス権限トークン受付部
５３　ユーザ認証証明書要求部
５４　証明書検証部
６０　サービス情報格納部
６１　アクセス権限条件格納部
６２　証明書情報格納部
７１　サービス代理アクセス部
１００　アイデンティティプロバイダ（ＩｄＰ）
１０１　サービスプロバイダ（ＳＰ）
１０２　ユーザエージェント
１０３　利用者情報
１０４　利用者情報
１１０　組織Ａ
１１１　組織Ｂ
１１２　組織Ａの管理者
１１３　リソース
１１４　組織Ｂの管理者
１１５　組織Ｂのリソースアクセス者
２００　認証装置
２０１　ショッピングサイト
２０２　商品購入者
２０２　運送業者
２０４　届け先
２０５　認証装置
２０６　ユーザ端末装置
２０７　サービスプロバイダ
２０８　課金代行サービス
２０９　会社の費用負担部門
Ａ　認証装置
Ｂ　サービス代理アクセス装置
Ｃ　サービス提供装置
Ｄ　認証用プログラム
Ｅ　サービス代理アクセス用プログラム
Ｆ　サービス提供用プログラム
Ｇ　ネットワーク

【発明を実施するための最良の形態】
【００２９】
次に、本発明の実施形態について図面を参照して詳細に説明する。
【００３０】
図１は、本発明の実施形態であるアクセス権限管理システムの全体的な構成を示すブロック図である。本発明の第１の実施形態は、認証装置１と、サービス代理アクセス装置２と、サービス提供装置３と、サービスアクセスユーザ端末装置４と、権限設定ユーザ端末装置５とを有している。そして、これらの装置はそれぞれネットワーク６に接続されている。図１には、認証装置１、サービス代理アクセス装置２、サービス提供装置３、サービスアクセスユーザ端末装置４及び権限設定ユーザ端末装置５をそれぞれ１つずつ図示している。もっとも、これはあくまで例示であり、これら装置は、それぞれ、１つ以上存在してもよい。
【００３１】
他のユーザに権限を委譲するユーザは、権限設定ユーザ端末装置５を介して認証装置１にアクセスする。他のユーザから権限を委譲されたユーザは、サービスアクセスユーザ端末装置４を介してサービス代理アクセス装置２にアクセスする。なお、ユーザは、個人であっても、複数の個人で構成される組織であってもよい。
【００３２】
図２は、本発明によるアクセス権限管理システムの主要構成を示すブロック図である。図２に示すように、アクセス権限管理システムは、権限を委譲する条件を管理する認証装置１と、サービス要求に応じてサービスを提供するサービス提供装置３と、サービス提供装置へのアクセスを代行するサービス代理アクセス装置２とを有している。認証装置１は、ユーザ認証証明書生成部１２と、権限委譲証明書・トークン生成部１４とを含む。ユーザ認証証明書生成部１２は、他の装置に対してユーザに関する情報が記載されたユーザ認証情報を発行する。また、権限委譲証明書・トークン生成部１４は、権限移譲先のユーザの情報と権限を委譲する条件とに基づいて、権限委譲情報と権限委譲情報に対応するトークンとを他の装置に対して発行する。サービス代理アクセス装置２は、トークン要求部３３と、ユーザ代理アクセス部３２とを含む。トークン要求部３３は、他の装置にアクセスするための権限委譲情報とトークンの発行を要求する。また、ユーザ代理アクセス部３２は、トークンを利用して他のサービスにアクセスする。サービス提供装置３は、トークンを利用して認証装置からユーザ認証情報を取得するユーザ認証証明書要求部５３を含む。
【００３３】
また、サービス提供装置３は、他の装置に提供するサービスを保管するサービス情報格納部６０を備え、他の装置からユーザに関する情報を取得するためのトークンを受信するトークン受付部５２を有している。
【００３４】
なお、ユーザ認証証明書要求部５３が取得するユーザ認証情報（例えば、ユーザ認証証明書）は、認証装置１内では、権限委譲情報（例えば、権限委譲証明書）と呼んでいたものである。認証装置１には、権限委譲設定情報があるので、権限委譲情報と判断できる。しかし、サービス提供装置３においては、ユーザに関する情報であり、権限委譲に関する情報がない。サービス提供装置３では権限委譲情報であるか否かは判断できないので、ユーザ認証情報とする。両者は同じ情報を指しているが、前提として持っている情報が装置毎に異なるので呼び方を変えている。
【００３５】
また、本実施の形態の各装置の構成を、下述のように変更してもよい。なお、本発明は記載された実施形態及び実施例に限定されるものではない。本発明の構成や詳細には、本発明の意義を逸脱しない範囲内で当業者が理解し得る様々な変更をすることができることは明らかである。
【００３６】
認証装置１は、権限を委譲するユーザが設定した、アクセス権限を委譲する条件を格納

する権限委譲条件格納部２１を含み、権限委譲証明書・トークン生成部１４は、権限委譲条件格納部２１に格納されている権限を委譲する条件に基づいて、権限委譲情報と権限委譲情報に対応するトークンとを発行するようにしてもよい。また、認証装置１は、権限委譲証明書・トークン生成部１４が発行した権限委譲情報と、その権限委譲情報に対応するトークンとを保管する証明書格納部２３と、トークンを受信すると、受信したトークンに対応する権限委譲情報を証明書格納部から取得する証明書要求受付部１８とを含んでいてもよい。また、認証装置１は、別のユーザへのアクセス権限の委譲を認めるか否か判断する権限ユーザ変換部１５を含み、権限委譲証明書・トークン生成部１４は、権限ユーザ変換部１５が権限委譲を認めると判断した場合に、権限委譲情報と権限委譲情報に対応するトークンとを発行するようにしてもよい。

【００３７】

また、サービス代理アクセス装置２は、アクセスしているユーザのユーザ認証情報を取得するユーザ認証証明書管理部３５と、取得したユーザ認証情報を保管するユーザ認証証明書格納部４１とを有していてもよい。

【００３８】

サービス提供装置３は、更に、ユーザ認証情報に記載されているユーザの代理として他の装置にアクセスするための権限委譲情報とトークンの発行を要求するトークン要求部３３Ａと、他の装置に対してトークンを利用して他のサービスにアクセスするユーザ代理アクセス部３２Ａとを含んでいてもよい。

【００３９】

［第１の実施形態］

次に、本発明の第１の実施形態を説明する。アクセス権限管理システムの全体的な構成は、図１に示されたような構成である。

【００４０】

図３は、認証装置１の構成例を示すブロック図である。図３に示す例では、認証装置１は、ユーザ認証証明書要求受付部１０と、ユーザ情報管理部１１と、ユーザ認証証明書生成部１２と、権限委譲設定情報受付部１３と、権限委譲証明書・トークン生成部１４と、権限ユーザ変換部１５と、権限委譲証明書・トークン管理部１６と、権限委譲証明書要求受付部１７と、証明書要求受付部１８と、ユーザ情報格納部２０と、権限委譲条件格納部２１と、サービス提供情報格納部２２と、証明書格納部２３とを含む。

【００４１】

ユーザ認証証明書要求受付部１０は、ユーザ認証証明書の要求を他の装置から受け付けて、ユーザ認証証明書生成部１２が発行したユーザ認証証明書を、ユーザ認証証明書の要求を行った装置に返信する。ユーザ認証証明書とは、ユーザ情報格納部２０に格納（保管）されているユーザに関する情報を記載した文書であり、ユーザ識別子情報や証明書発行者情報などを含む。なお、ユーザ認証証明書の一例が図４に示されている。ユーザ認証証明書は、例えば、非特許文献１に記載されたＳＡＭＬや、Ｘ．５０９の形式であるが、それらの形式に限定されるものではない。本発明において、ユーザに関する情報が含まれていれば、ユーザ認証証明書は、どのような形式でもよい。

【００４２】

ユーザ情報管理部１１は、ユーザ認証証明書要求受付部１０がユーザ認証証明書の生成要求を受け取ったときに、証明書の対象になるユーザ情報をユーザ情報格納部２０から取得し、ユーザ認証証明書生成部１２に送る。ユーザ認証証明書生成部１２は、ユーザ情報格納部２０の情報を元にユーザ認証証明書を発行する。

【００４３】

権限委譲設定情報受付部１３は、図１に示された権限設定ユーザ端末装置５から権限委譲設定情報を受け付ける。そして権限委譲設定情報受付部１３は、権限委譲設定情報を、ユーザ情報格納部２０に格納されている情報とともに権限委譲条件格納部２１に格納する。ここで、権限委譲設定情報とは、権限委譲元ユーザの識別子と、権限を委譲する先のユーザの識別子と、委譲した権限を利用してアクセスできる対象になるプロバイダＩＤやＵ

ＲＬやリソース等を含む情報である。なお、委譲条件格納部２１に格納される情報の一例が図５に示されている。

【００４４】

権限委譲証明書・トークン生成部１４は、代理アクセスするための権限委譲証明書の発行要求を権限委譲証明書要求受付部１７から取得し、更に、権限ユーザ変換部１５から委譲先ユーザの情報を取得し、権限委譲証明書を発行する。権限委譲証明書の形式は、ユーザ認証証明書の形式と同じである。権限委譲証明書を発行した認証装置１から見れば、権限委譲設定情報に基づいて発行された証明書なので、権限委譲証明書となる。しかし、権限委譲証明書を受け取るサービス提供装置３には権限委譲設定情報はなく、サービス提供装置３から見ると、ユーザの情報が記載されているので、単にユーザ認証証明書になる。

【００４５】

更に、権限委譲証明書・トークン生成部１４は、証明書を一意に特定するためのトークンを発行する。トークンには、証明書を識別するための識別子が記載されている。証明書を一意に特定するためのトークンを、例えば、非特許文献１で挙げたＳＡＭＬが規定するアーティファクトを用いて実現できる。しかし、証明書と一意に対応付けられる文字列であれば、アーティファクト以外のどのような形式のものでもよい。

【００４６】

権限ユーザ変換部１５は、権限委譲証明書要求受付部１７からユーザ認証証明書を取得し、権限委譲条件格納部２１に記載されている条件を元に、権限委譲を認めるか否かを判断する。権限委譲を認めると判断した場合には、権限が委譲されるユーザのユーザ情報をユーザ情報格納部２０から取得する。例えば、ユーザ認証証明書に記載されているユーザの識別子が、権限委譲条件格納部２１に格納されている権限委譲先ユーザの識別子として記載されている場合には、権限を委譲してよいと判断する。そして、権限委譲元ユーザとしてユーザ認証証明書（権限委譲証明書）の発行を認める。

【００４７】

権限委譲証明書・トークン管理部１６は、権限委譲証明書・トークン生成部１４が生成した証明書とトークンを関連付けて証明書格納部２３に登録したり、トークンを利用して証明書格納部２３から証明書を取得したりする。権限委譲証明書要求受付部１７は、代理アクセスするための権限証明書の発行要求とユーザ認証証明書とを別の装置から取得する。そして、権限委譲証明書要求受付部１７は、該認証装置１が生成したアクセス権限に関するトークンを、権限証明書の発行要求が取得された装置に返信する。

【００４８】

証明書要求受付部１８は、他の装置からトークンを取得して、証明書格納部２３に格納されている証明書を返信する。

【００４９】

ユーザ情報格納部２０は、ユーザ情報を格納する。ユーザ情報とは、ユーザ識別子、ユーザのアクセス権限に関する情報（Ｒｅａｄ、Ｗｒｉｔｅ、実行権限など）、及び他の装置に証明書を発行するか否かという情報などが含まれる。ただし、ユーザに関する情報は、それらの情報に限定されるものではない。これらの情報に加えて、又は、替えて他の情報を付加するようにしてもよい。

【００５０】

権限委譲条件格納部２１は、委譲ユーザの識別子、委譲先ユーザの識別子、及びアクセス先装置やアクセス先情報などのユーザの権限委譲情報を格納する。サービス提供情報格納部２２は、図１に示されたサービス提供装置３のアクセス先ＵＲＬなどの情報を格納する。

【００５１】

証明書格納部２３は、証明書とトークンとを対応付けて格納する。証明書格納部２３が格納する情報の一例が図６に示されている。図６に示す例では、トークンをキーとして証明書が格納されている。

【００５２】

図７は、サービス代理アクセス装置２の構成例を示すブロック図である。図７に示すように、サービス代理アクセス装置２は、ユーザ認証証明書要求部３１と、ユーザ代理アクセス部３２と、トークン要求部３３と、ユーザ認証証明書検証部３４と、ユーザ認証証明書管理部３５と、トークン管理部３６と、ユーザ認証証明書格納部４１と、代理アクセス情報格納部４２と、トークン格納部４３とを含む。

【００５３】

ユーザ認証証明書要求部３１は、認証装置１にユーザ認証証明書を要求して、ユーザ認証証明書を取得する。

【００５４】

ユーザ代理アクセス部３２は、代理アクセス情報格納部４２に格納されているアクセス権限を確認し、代理アクセスできる場合には、認証装置１から取得したアクセス権限に関するトークンを利用して、ユーザの代理として他の装置にアクセスする。

【００５５】

トークン要求部３３は、ユーザ認証証明書を利用して認証装置１に権限委譲証明書の発行を依頼し、トークンを取得する。

【００５６】

ユーザ認証証明書検証部３４は、認証装置１から取得したユーザ認証証明書が正しいか否か検証する。ユーザ認証証明書が正しいか否か検証するとは、証明書の有効期間、証明書のフォーマット、証明書の発行者などを確認することによって、証明書に違反がないか確認することである。

【００５７】

ユーザ認証証明書管理部３５は、ユーザ認証証明書をユーザ認証証明書格納部４１に登録したり、アクセスしているユーザの認証証明書を取得したりする。トークン管理部３６は、認証装置１から取得されたトークンをトークン格納部４３に格納する。ユーザ認証証明書格納部４１は、ユーザ認証証明書を格納する。代理アクセス情報格納部４２は、当該装置がユーザの代理として他の装置にアクセスできるか否かというアクセス権限情報を格納する。

【００５８】

図８は、サービス提供装置３の構成例を示すブロック図である。図８に示すように、サービス提供装置３は、サービスアクセス受付部５０と、サービス情報管理部５１と、トークン受付部５２と、ユーザ認証証明書要求部５３と、証明書検証部５４と、サービス情報格納部６０と、アクセス権限条件格納部６１と、証明書情報格納部６２とを含む。

【００５９】

サービスアクセス受付部５０は、他の装置からサービス要求を取得し、サービス要求が、アクセス権限条件格納部６１に格納されているアクセス条件を満たしている場合は、サービスに関する情報を送付する。

【００６０】

サービス情報管理部５１は、サービスに関する情報をサービス情報格納部６０から取得する。トークン受付部５２は、代理アクセスによるサービス要求を取得した際に、サービス要求メッセージからトークンを取得する。ユーザ認証証明書要求部５３は、トークン受付部５２から取得したトークンを認証装置１に送付し、ユーザ認証証明書を取得する。

【００６１】

証明書検証部５４は、ユーザ認証証明書要求部５３が取得したトークンを解析し、証明書が正しいことを確認する。サービス情報格納部６０と、サービス提供装置３が他の装置に提供するサービスに関する情報を格納する。アクセス権限条件格納部６１と、サービスを提供する条件を格納する。証明書情報格納部６２は、ユーザに関する認証証明書を格納する。

【００６２】

次に、図９～図１６を参照して第１の実施形態の動作を説明する。

【００６３】

まず、システム全体の動作の流れを、図９を用いて説明する。権限設定ユーザ端末装置５は、認証装置１にアクセスし、権限委譲の条件を設定する（ステップＩ１）。このとき、すでに認証装置１に権限委譲の条件が設定されている場合には、ステップＩ１の処理を省略することができる。ステップＩ１の処理の詳細については、図１０を参照して後述する。次に、サービスアクセスユーザ端末装置４は、サービス代理アクセス装置２にアクセスする。そして、サービス代理アクセス装置２は、認証装置１からユーザ認証証明書を取得する（ステップＩ２）。ステップＩ２の処理の詳細については、図１１を参照して後述する。その後、サービス代理アクセス装置２は、ユーザの権限を用いてサービス提供装置３に代理アクセスする（ステップＩ３）。ステップＩ３の処理の詳細については、図１３を参照して後述する。

【００６４】

次に、図１０を参照して、あるユーザ（ユーザＡとする）が他のユーザ（ユーザＢとする）にアクセス権限を委譲するための設定動作を説明する。図１０は、あるユーザが他のユーザに権限委譲を設定するときの認証装置１に関する処理を示す流れ図である。

【００６５】

ユーザＡは、権限設定ユーザ端末装置５を介して認証装置１の権限委譲設定情報受付部１３にアクセスする（ステップＡ１）。次に、権限を委譲するユーザＡは、ユーザ情報格納部２０に管理されているユーザ自身のアクセス権限を、別のユーザに委譲するための条件を入力する（ステップＡ２）。そして、入力された権限を権限委譲条件格納部２１に登録する（ステップＡ３）。上記の処理によって、権限委譲を実現するための条件が設定される。ユーザＡは、ユーザＡが設定した権限委譲に関する情報を、ユーザＢに通知する。通知は、ネットワークを介して行われてもよいし、オフラインで行われてもよい。

【００６６】

次に、図１１を参照して、サービスアクセスユーザ端末装置４がサービス代理アクセス装置２にアクセスした際に、サービス代理アクセス装置２が認証装置１からユーザ認証証明書を取得する動作を説明する。図１１は、ユーザ認証証明書を要求して取得するときのサービス代理アクセス装置２に関する処理を示す流れ図である。

【００６７】

まず、権限を委譲されたユーザＢは、サービスアクセスユーザ端末装置４を介してサービス代理アクセス装置２のユーザ認証証明書要求部３１にアクセスする（ステップＢ１）。ユーザ認証証明書要求部３１は、ユーザ認証証明書を要求するためのメ要求ッセージを生成し、認証装置１に送付する（ステップＢ２）。要求ッセージを受信した認証装置１は、ユーザ認証証明書を発行し、サービス代理アクセス装置２に送付する（ステップＢ３）。ステップＢ３の処理の詳細については、図１２を参照して後述する。認証装置１からユーザ認証証明書を取得すると、ユーザ認証証明書検証部３４は、ユーザ認証証明書が正しく発行されているか否か検証する（ステップＢ４）。ステップＢ４の検証処理の結果、証明書が正しくないと判断された場合には、処理を終了する。ステップＢ４の検証の結果、証明書が正しいと判断された場合には、ユーザ認証証明書管理部３５は、ユーザ認証証明書格納部４１に該証明書を登録し、処理を終了する（ステップＢ５）。

【００６８】

次に、図１２を参照して、認証装置１がユーザ認証証明書を発行する処理（図１１におけるステップＢ３）の動作を説明する。図１２は、ユーザ認証証明書を生成するときの認証装置に関する処理を示す流れ図である。

【００６９】

まず、認証装置１は、ユーザ認証証明書要求受付部１０を介して他の装置から証明書要求を受信する（ステップＣ１）。次に、ユーザ情報管理部１１は、証明書に記載するユーザ情報をユーザ情報格納部２０から取得する（ステップＣ２）。更に、ユーザ認証証明書生成部１２は、他の装置からの証明書要求と、ユーザ情報格納部２０から取得したユーザ情報に基づいて、ユーザ認証証明書を発行する（ステップＣ３）。そして、ユーザ認証証明書要求受付部１０は、ユーザ認証証明書を要求した装置にユーザ認証証明書を送付する

（ステップＣ４）。
【００７０】
次に、図１３を参照して、サービス代理アクセス装置２が権限委譲されたユーザＢの要求に従って権限委譲したユーザＡの権限でサービス提供装置３にアクセスする動作について説明する。図１３は、他のサービスに代理アクセスするときのサービス代理アクセス装置２に関する処理を示す流れ図である。
【００７１】
まず、ユーザＢは、サービス代理アクセス装置２のユーザ代理アクセス部３２にアクセスし、サービス代理アクセス装置２に対して代理アクセスを要求する（ステップＤ１）。ユーザ代理アクセス部３２は、代理アクセス情報格納部４２に格納されているアクセス権限を確認し、ユーザＢが代理アクセスを実行できか否か（ユーザＢがサービス代理アクセス装置２を利用できるか否か）を判断する（ステップＤ２）。実行できない場合には、処理を終了する（ステップＤ９）。ステップＤ２の判断の結果、代理アクセスできる場合には、トークン要求部３３は、代理アクセスのためのトークンを要求するメッセージを生成し、生成したメッセージとユーザ認証証明書格納部４１に保管されている（ユーザＢの）ユーザ認証証明書とを認証装置１に送付する（ステップＤ３）。
【００７２】
次に、認証装置１は、権限委譲証明書とトークンとを生成し、トークンをサービス代理アクセス装置２に送付する（ステップＤ４）。ステップＤ４の処理の詳細については、図１４を参照して後述する。その後、トークン管理部３６を介してトークンがトークン格納部４３に登録された後、ユーザ代理アクセス部３２は、サービス提供装置３に対するアクセス要求メッセージを作成する（ステップＤ５）。更に、ユーザ代理アクセス部３２は、アクセス要求メッセージと認証装置１で生成されたトークンとをサービス提供部３に送付する（ステップＤ６）。
【００７３】
また、サービス提供装置３は、アクセス要求メッセージに基づいてサービス情報をサービス代理アクセス装置２に送付する（ステップＤ７）。ステップＤ７の処理の詳細については、図１５を参照して後述する。最後に、ユーザ代理アクセス部３２は、サービスに関する情報を取得し、ユーザＢに代理アクセスの処理結果を送付する（ステップＤ８）。
【００７４】
次に、図１４を参照して、認証装置１が権限委譲証明書とトークンを生成する動作を説明する。図１４は、権限委譲の証明書を発行し、証明書に関連するトークンを発行するときの認証装置に関する処理を示す流れ図である。
【００７５】
まず、認証装置１の権限委譲証明書要求受付部１７は、権限委譲証明書の発行を要求する発行要求メッセージと（ユーザＢの）ユーザ認証証明書とを取得する（ステップＥ１）。次に、権限ユーザ変換部１５は、発行要求メッセージに記載されている情報と（ユーザＢの）ユーザ認証証明書に記載されている情報とを、権限委譲条件格納部２１に格納されている情報（条件）に照合して、（ユーザＡに関する）権限委譲証明書を発行できるか否かを判断する（ステップＥ２）。発行要求メッセージまたはユーザ認証証明書に記載されている情報が条件を満たしていない場合には、処理を終了する（ステップＥ８）。ステップＥ２の判断の結果、証明書を発行できると判断した場合には、発行要求メッセージに記載されている情報と権限委譲条件格納部２１で管理されている情報とに基づいて、委譲したユーザＡの情報をユーザ情報格納部２０から取得する（ステップＥ３）。
【００７６】
次に、権限委譲証明書・トークン生成部１４は、ユーザ情報格納部２０から取得したユーザＡの情報を利用して、権限委譲証明書を発行する（ステップＥ４）。また、権限委譲証明書・トークン生成部１４は、権限委譲証明書に対応するトークンを発行する（ステップＥ５）。その後、権限委譲証明書・トークン管理部１６は、証明書格納部２３にトークンと権限委譲証明書とを登録する（ステップＥ６）。そして、権限委譲証明書要求受付部

１７は、権限委譲証明書を要求した装置に、生成したトークンを送付する（ステップＥ７）。以上のように、権限委譲証明書・トークン生成部１４は、権限を委譲する条件に基づいて、権限委譲情報（具体的には、権限委譲証明書）と権限委譲情報に対応するトークンとを生成し、権限委譲証明書要求受付部１７を介して他の装置に対して発行する。

【００７７】

次に、図１５を参照して、サービス提供装置３が他の装置からのアクセスを受け付けたときの動作を説明する。図１５は、代理アクセスを受け付けるサービス提供装置３に関する処理を示す流れ図である。

【００７８】

サービス提供装置３のサービスアクセス受付部５０は、サービスへのアクセス要求するメッセージを受け付け、トークン受付部５２は、トークンを受け付ける（ステップＦ１）。次に、ユーザ認証証明書要求部５３は、受け付けられたトークンを利用して、ユーザ認証証明書を要求するメッセージを作成し、認証装置１に送付する（ステップＦ２）。

【００７９】

認証装置１は、権限委譲証明書をユーザＡのユーザ認証証明書としてサービス提供装置３に送付する（ステップＦ３）。ステップＦ３の処理の詳細については、図１６を参照して後述する。次に、証明書検証部５４は、認証装置１から送付されたユーザ認証証明書を検証する（ステップＦ４）。検証する内容は、証明書の有効期間の確認や、証明書のフォーマットの確認や、証明書の発行者の確認などである。ユーザＡのユーザ認証証明書が正しくないと判断された場合には、処理を終了する（ステップＦ８）。ステップＦ４の検証の結果、証明書が正しいと判断された場合には、ユーザＡのユーザ認証証明書を証明書情報格納部６２に登録する（ステップＦ５）。

【００８０】

次に、サービスアクセス受付部５０は、取得されたユーザＡのユーザ認証証明書に記載されている内容と、アクセス権限条件格納部６１で管理されている条件とを照合して、ユーザＡがサービス提供装置３にアクセスしてよいか否かを判断する（ステップＦ６）。アクセスできないと判断された場合には、処理を終了する（ステップＦ８）。ステップＦ６の処理の結果、アクセスを認めると判断された場合には、サービスアクセス受付部５０は、サービス情報管理部５１を介してサービス情報格納部６０からサービスに関する情報を取得し、取得した情報をアクセス元に送付する（ステップＦ７）。

【００８１】

次に、図１６を参照して、認証装置１がトークンを取得して証明書を送付する動作を説明する。トークンから証明書を取得するときの認証装置に関する処理を示す流れ図である。

【００８２】

認証装置１の証明書要求受付部１８は、権限委譲証明書の代わりとしてユーザ認証証明書を要求するメッセージとトークンとを受信する（ステップＧ１）。証明書要求受付部１８は、受信されたトークンを利用して、権限委譲証明書・トークン管理部１６を介して証明書格納部２３からトークンに対応する証明書を取得する（ステップＧ２）。そして、証明書要求受付部１８がアクセス元に証明書を送付する（ステップＧ３）。

【００８３】

以上に説明したように、本発明によるアクセス権限管理システムは、図１に示されたように、権限の委譲やユーザ証明書を発行する認証装置１と、ユーザの権限で他のプロバイダにアクセスするサービス代理アクセス装置２と、他のサービスからのからアクセスを受け付けてユーザ情報を確認しサービスを提供するサービス提供装置３と他のユーザから権限を委譲されたユーザがサービスにアクセスするために利用するサービスアクセスユーザ端末装置４と他のユーザに権限を委譲するための設定を登録するユーザが利用する権限設定ユーザ端末装置５が、相互にネットワーク６を介して接続されている。

【００８４】

そして、図３に示されたように、認証装置１は、ユーザ認証証明書要求受付部１０が受

け付けた証明書要求に基づいて、ユーザ情報格納部２０に格納されている情報をユーザ情報管理部１１を介して取得し、ユーザ認証証明書を生成するユーザ認証証明書生成部１２と、ユーザ端末装置からの権限委譲設定情報を受け付けて、権限委譲条件格納部２１に登録する権限委譲設定情報受付部１３と、権限委譲証明書要求受付部１７が受け付けた証明書要求に基づいて、権限ユーザ変換部１５とサービス提供部情報格納部２２から取得した情報を利用して、権限委譲設定情報に基づいて作成するユーザ認証証明書（これを権限委譲証明書という。）と証明書に対応するトークンとを生成する権限委譲証明書・トークン生成部１４と、権限委譲証明書・トークン生成部１４が生成したトークンを権限委譲証明書・トークン管理部１６を介して証明書を関連付けて登録する証明書格納部２３と、受け付けたトークンを利用して証明書格納部２３が格納する証明書を検索して、要求元に返信する証明書要求受付部１８とを備えている。

【００８５】

図７に示されたように、サービス代理アクセス装置２は、ユーザ認証証明書要求部３１が認証装置１からユーザ認証証明書を取得すると、ユーザ認証証明書を検証するユーザ認証証明書検証部３４と、ユーザ認証証明書をユーザ認証証明書格納部４１に格納するユーザ認証証明書管理部３５と、ユーザ認証証明書格納部４１が格納している証明書情報と、代理アクセス情報格納部４２が格納している代理アクセスのための条件とを比較し、合致するか否かを判断し、合致した場合には、トークン要求部３３を介してアクセス権限に関するトークンを要求し、取得したトークンをトークン格納部４３に登録するトークン管理部３６と、トークン要求部３３が取得したトークンを利用して他のプロバイダにユーザの権限で代理アクセスするユーザ代理アクセス部３２を備えている。

【００８６】

図４に示されたように、サービス提供装置３は、アクセス権限条件格納部６１が保管している条件に合致している状況の下で、サービス情報格納部６０に格納されている情報を、サービス情報管理部５１を介して取得し、アクセス元に返送するサービスアクセス受付部５０と、トークン受付部５２が取得したトークンを元に証明書を取得し、証明書検証部５４を用いて証明書を検証し、証明書情報格納部６２に保管させるユーザ認証証明書要求部５３とを備えている。

【００８７】

ユーザ認証証明書要求部５３が取得する証明書は、認証装置１内では、権限委譲証明書と呼んでいたものである。認証装置１には、権限委譲設定情報があるので、権限委譲のための証明書（権限委譲証明書）と判断できる。しかし、サービス提供装置３においては、ユーザの情報が記載されている証明書であり、権限委譲に関する情報がない。サービス提供装置３では権限委譲証明書であると判断できないので、ユーザ認証証明書とする。両者は同じものを指しているが、前提として持っている情報が異なるので呼び方を変えている。

【００８８】

このような構成を採用し、権限を他のユーザに委譲するユーザが権限設定ユーザ端末装置６を介して認証装置１に権限条件を設定し、その後、権限を委譲されたユーザがサービスアクセスユーザ端末装置５を介してサービス代理アクセス装置２にアクセスし、サービス代理アクセス装置２が認証装置１に権限委譲証明書とトークンの発行を依頼し、更に、サービス提供装置３にアクセスしてトークンを送付する。サービス提供装置３が認証装置１からトークンを利用して権限を委譲したユーザの証明書を取得し、委譲したユーザの証明書を用いてアクセスを制御することによって、本発明の目的を達成することができる。

【００８９】

本実施形態の効果を説明する。本実施形態では、認証装置１がアクセスしてきた装置に応じて、適切なユーザ認証証明書を選択的に送付するように構成されているので、不要なユーザ情報を送付する必要がなくなり、情報漏えいの可能性を軽減できる。

【００９０】

また、本実施形態では、更に、権限を委譲するユーザ（ユーザＡ）は認証装置１にのみ

権限委譲条件を設定し、サービス提供装置３は委譲されたユーザ（ユーザＢ）ではなく権限を委譲したユーザ（ユーザＡ）としてアクセス可否を判断するというように構成されている。そのため、権限を委譲するユーザＡは一箇所のみに権限委譲条件を設定すればよい。その結果、権限設定の手間を省くことができる。

【００９１】

また、本実施形態では、更に、権限を委譲するユーザが認証装置１に対して権限委譲条件を入力するので、ユーザの確認やユーザの同意を求めながら、ユーザの意図に沿った権限委譲の設定ができる。

【００９２】

［第２の実施形態］

次に、本発明の第２の実施形態を図面を参照して説明する。図１７は、第２の発明形態におけるサービス提供装置であるサービス提供装置７の構成を示すブロック図である。図１７に示すように、第２の実施形態は、サービス提供装置７が、図８に示された第１の実施形態におけるサービス提供装置３の構成に加えて、代理アクセス部７１を有している点で異なる。また、全体的な構成は、サービス提供装置３に代えて、又は、サービス提供装置３に加えてサービス提供装置７が存在することになるが、図１に示された構成と同じである。

【００９３】

代理アクセス部７１は、ユーザ代理アクセス部３２と、トークン要求部３３と、代理アクセス情報格納部４２と、トークン格納部４３とを含む。代理アクセス部７１に含まれるそれぞれの部は、図４に示された第１の実施形態におけるサービス代理アクセス装置２に含まれるユーザ代理アクセス部３２と、トークン要求部３３と、代理アクセス情報格納部４２と、トークン格納部４３と、それぞれ同じ動作をする。

【００９４】

権限設定ユーザ端末装置５が認証装置１に権限の委譲を設定する処理と、サービス代理アクセス装置２が認証装置１からユーザ認証証明書を取得する処理は、図１０、図１１、図１２に示された第１の実施形態における動作と同じである。また、サービス代理アクセス装置２が代理アクセスのための権限に関する証明書を認証装置１に発行依頼し、その結果トークンを取得し、サービス提供装置７にアクセス要求メッセージを送付する動作は、第１の実施形態における動作（図１３のステップＤ１～Ｄ６までの処理）と同じである。しかし、サービス提供装置７が代理アクセス要求を受けた場合の動作が、第１の実施形態における動作と異なり、図１８の流れ図に示すようになる。

【００９５】

次に、図１８の流れ図を参照して本実施形態の全体の動作を説明する。

【００９６】

サービス提供装置７がアクセス要求を取得すると、認証装置１からユーザ認証証明書を取得し、サービスの提供の可否を判断する（ステップＦ１～Ｆ７）。ステップＦ１～Ｆ７の処理は、図１５に示された第１の実施形態におけるサービス提供装置３の動作と同じである。

【００９７】

第２の実施形態では、サービス提供装置７がサービス情報を送付したときに、サービス装置７が他のサービス装置に対して代理アクセスを行う。代理アクセスを行うために、サービス提供装置７におけるトークン要求部３３は、認証装置１に対して、ステップＦ３の処理で取得したユーザ認証証明書を送付するとともに、代理アクセスを実現するためのトークンの発行要求メッセージを送付する（ステップＨ１０）。認証装置１がトークンの発行要求を受信すると、証明書とその証明書に対応するトークンを発行し、サービス提供装置７に送付する（ステップＨ１１）。ステップＨ１１の処理は、図１４に示された第１の実施形態における認証装置１の処理と同じである。

【００９８】

サービス提供装置７がトークンを取得すると、トークン管理部３６がトークンをトーク

ン格納部４３に登録する。更に、ユーザ代理アクセス部３２は、代理アクセス情報格納部４２の情報を利用して、他のサービス提供装置に対して代理アクセスするためのアクセス要求メッセージを作成する（ステップＨ１２）。そして、ユーザ代理アクセス部３２は、他のサービス提供装置に対してアクセス要求メッセージを送付する（ステップＨ１３）。

【００９９】

アクセス要求メッセージを受信したサービス提供装置は、図１５に示されたサービス提供装置３の処理と同じ処理、または、図１８に示されたサービス提供装置７の処理と同じ処理であるサービス要求受付処理を行う（ステップＨ１４）。その後、ユーザ代理アクセス部３２は、代理アクセスの結果を、サービス提供装置７にアクセスしている装置に対して送付する（ステップＨ１５）。

【０１００】

第２の実施形態の効果を説明する。第２の実施形態では、認証装置１で保管されている権限委譲の条件に関する情報をサービスアクセスユーザ端末装置４が再利用し、権限委譲されたサービス利用装置７が、更に別のサービス利用装置に対して権限を再委譲するというように構成されている。そのため、サービス代理アクセス装置２は、別のサービス利用装置への権限の再委託を考慮することなく権限委譲を設定でき、サービス代理アクセス装置２の権限委譲処理を簡略化できる。

【０１０１】

［第３の実施形態］

次に、本発明の第３の実施形態を図面を参照して説明する。図１９は、第３の実施形態の全体的な構成を示すブロック図である。図１９に示すように、第３の実施形態は、第１及び第２の実施形態と同様に、ネットワークＧを介して通信可能な認証装置Ａとサービス代理アクセス装置Ｂとサービス提供装置Ｃとを備えている。なお、認証装置Ａは、第１及び第２の実施形態における認証装置１に相当する。サービス代理アクセス装置Ｂは、サービス代理アクセス装置２に相当する。サービス提供装置Ｃは、第１及び第２の実施形態におけるサービス提供装置３またはサービス提供装置７に相当する。

【０１０２】

認証装置Ａ、サービス代理アクセス装置Ｂ及びサービス提供装置Ｃは、それぞれＣＰＵを搭載している。認証用プログラムＤは、認証装置Ａの動作を制御し、サービス代理アクセス装置Ｂやサービス提供装置Ｃからの要求に従って、証明書を発行したり、トークンを発行したりするためのプログラムである。認証装置Ａは、認証用プログラムＤに従って制御を実行することによって、第１及び第２の実施形態における認証装置１の処理と同じ処理を実行する。

【０１０３】

サービス代理アクセス用プログラムＥは、サービス代理アクセス装置Ｂの動作を制御し、証明書やトークンを認証装置Ａから取得し、サービス提供装置Ｃにアクセスするためのプログラムである。サービス代理アクセス装置Ｂは、サービス代理アクセス用プログラムＥに従って制御を実行することによって、第１及び第２の実施形態におけるサービス代理アクセス装置２の処理と同じ処理を実行する。

【０１０４】

サービス提供用プログラムＦは、サービス提供装置Ｃの動作を制御し、認証装置Ａから証明書を取得し、サービス代理アクセス装置Ｂにサービスを提供するためのプログラムである。サービス提供装置Ｃは、サービス提供用プログラムＦに従って制御を実行することによって、第１及び第２の実施形態におけるサービス提供装置３，７の処理と同じ処理を実行する。

【実施例】

【０１０５】

［実施例１］

次に、本発明の第１の実施例を、図面を参照して説明する。第１の実施例は本発明の第１の実施形態に対応する実施例である。

【０１０６】
図２０は、アクセス管理システムの第１の実施例の構成を示す構成図である。アクセス権限管理システムは、図２０に示すように、認証装置２００と、ショッピングサイト２０１と、運送業者２０２（具体的には、運送業者におけるサーバ装置等）とを含む。また、図２０には、商品購入者２０３と、商品届け先ユーザ２０４とが示されている。
【０１０７】
認証装置２００は、ンターネット上でユーザ情報を管理し証明書を配布する装置である。ショッピングサイト２０１は、サービス代理アクセス装置として振舞う装置である。運送業者２０２（具体的には、運送業者におけるサーバ装置等）は、サービス提供装置として振舞う装置である。商品購入者２０３は、サービスアクセスユーザ端末装置を介してネットワークにアクセスする。商品届け先ユーザ２０４は、権限設定ユーザ端末装置を介してネットワークにアクセスする。
【０１０８】
本実施例では、商品購入者２０３がショッピングサイト２０２で商品を購入し、届け先ユーザ２０４に贈答するために商品届け先２０４の権限で運送業者２０２に商品の配送を依頼し、運送業者２０２が商品を配送する。本実施例における認証装置として、ＩＳＰ（インターネットサービスプロバイダ）やキャリアなどのユーザ情報を管理する組織が想定されている。
【０１０９】
また、本実施例における運送業者２０２は、すでに商品届け先の連絡先を管理している。連絡先にアクセスできる権限は、商品届け先２０４のユーザが持っているとする。本実施例では、商品届け先の連絡先にアクセスする権限をユーザや装置間で委譲する。
【０１１０】
商品届け先２０４のユーザは、認証装置２００に対して、商品購入者２０３が運送業者２０２内で管理されている連絡先にアクセスする権限を委譲することを認めることを通知する（図２０におけるステップＳ１００）。通知に基づいて、商品購入者がプレゼントとして購入した商品を商品届け先に送付できるようになる。
【０１１１】
以上の条件の下で商品購入者２０３は、ショッピングサイト２０１にアクセスする（図２０におけるステップＳ１０１）。ショッピングサイト２０１は、アクセスしてきたユーザ情報を取得するために、ユーザ認証証明書要求を認証装置２００に送付する（図２０におけるステップＳ１０２）。要求を受信した認証装置２００は、ユーザ認証証明書を発行し（図２０におけるステップＳ１０３）、ショッピングサイト２０１に送付する（図２０におけるステップＳ１０４）。ユーザ認証証明書を見ればユーザを識別できるので、ショッピングサイト２０１は、商品購入者２０３のアクセスに従って商品購入手続きと、商品配送手続きを行う（図２０におけるステップＳ１０５）。
【０１１２】
また、ショッピングサイト２０１は、運送業者２０２に商品発送を依頼するための権限を認証装置２００に要求する（図２０におけるステップＳ１０６）。認証装置２００が権限証明書の発行要求を受信すると、認証装置２００は、商品購入者２０３が運送業者２０２内で管理されている商品届け先２０４の連絡先にアクセスできるか判断する。アクセスを認める場合には、運送業者２０２向けに商品届け先２０４のユーザに関するユーザ認証証明書を発行し、更に、トークンを発行する（図２０におけるステップＳ１０７）。
【０１１３】
次に、認証装置２００がショッピングサイト２０１に、発行されたトークンを送付する（図２０におけるステップＳ１０８）。ショッピングサイトがトークンを受信すると、トークンとともに商品発送要求を送付する（図２０におけるステップＳ１１０）。運送業者２０２が、商品発送要求を受信すると、その要求が誰の権限でアクセスしているのか確認する（図２０におけるステップＳ１１１）。しかし、この段階では、ユーザ認証証明書はなく、トークンのみが受信されているので、運送業者２０２は、認証装置２００にトーク

ンを送付するとともに、証明書を要求する（図２０におけるステップＳ１１２）。認証装置２００は、受信したトークンから証明書を検索して取得する（図２０におけるステップＳ１１３）。そして、証明書を要求している運送業者２０２に送付する（図２０におけるステップＳ１１４）。

【０１１４】

運送業者２０２が証明書を受信すると、権限を確認し、商品届け先２０４の連絡先にアクセスできるか否かを判断する（図２０におけるステップＳ１１５）。アクセスできた場合には、商品届け先住所が分かるので、ショッピングサイト２０１の要求に従って、商品を商品届け先２０４に送付する。

【０１１５】

本実施例では、ショッピングサイトと運送業者は、ユーザの権限に関するトークンを交換するだけであり、ユーザＩＤ等のユーザ情報が記載された文書を交換していない。また、商品届け先２０４のユーザは、認証装置２００にのみ権限委譲を設定するだけでよく、委譲の条件を複数の装置に配布する必要はない。

【０１１６】

［実施例２］

次に、本発明の第２の実施例を、図面を参照して説明する。第２の実施例は本発明の第２の実施形態に対応する実施例である。

【０１１７】

図２１は、アクセス管理システムの第２の実施例の構成を示す構成図である。アクセス権限管理システムは、図２１に示すように、認証装置２０５と、サービスプロバイダ２０７と、課金代行サービス２０８（具体的には、課金代行サービス提供者におけるサーバ装置等）と、費用負担部門２０９（具体的には、費用負担部門におけるサーバ装置等。）を含む。

【０１１８】

認証装置２０５は、インターネット上でユーザ情報を管理し証明書を配布する装置である。サービスプロバイダ２０７は、サービス代理アクセス装置として振舞う装置である。課金代行サービス２０８（具体的には、課金代行サービス提供者におけるサーバ装置等）は、サービス提供と代理アクセスとを行うサービス提供装置として振舞う。ユーザ端末装置２０６は、サービスアクセスユーザ端末装置を介してネットワークにアクセスする社員が利用する装置である。費用負担部門２０９は、課金代行サービスの要求に従って支払い処理を行う会社の部門である。なお、費用負担部門２０９における他者との通信処理などは、具体的には、費用負担部門２０９におけるサーバ装置等で実現される。

【０１１９】

本実施例では、会社の費用負担部門２０９の管理者が権限設定ユーザ端末装置を介して社員に課金代行サービスへのアクセス権限を設定しているとする。また、本実施例では、ユーザがサービスプロバイダ２０７を利用する際に、ユーザ自身の権限で利用するが、そのサービス利用料は会社の費用負担部門２０９が支払うとする。そのサービス利用料の課金は、課金代行サービス２０８が課金処理を行う。サービスプロバイダ２０７は、会社の費用負担部門２０９の権限で課金代行サービスに課金を依頼する。また、課金代行サービス２０８は、サービスプロバイダ２０７の権限で会社の費用負担部門２０９に支払い請求をすることになる。

【０１２０】

社員としての権限を持っているユーザは、ユーザ端末装置２０６を介して、サービスプロバイダ２０７にアクセスする（図２１におけるステップＳ２０１）。サービスプロバイダ２０７は、アクセスしてきたユーザ情報を取得するために、ユーザ認証証明書要求を認証装置２０５に送付する（図２１におけるステップＳ２０２）。要求を受信した認証装置２０５は、ユーザ認証証明書を発行し（図２１におけるステップＳ２０３）、サービスプロバイダ２０７に送付する（図２１におけるステップＳ２０４）。ユーザ認証証明書を見ればユーザを識別できるので、サービスプロバイダ２０７は、ユーザに対してサービスを

提供する（図２１におけるステップＳ２０５）。

【０１２１】

次に、サービスプロバイダ２０７は、課金代行サービス２０８に課金処理を依頼するための権限を認証装置２０５に要求する（図２１におけるステップＳ２０６）。認証装置２０５は、権限証明書の発行要求を受信すると、ユーザが勤めている会社の費用負担部門２０９の情報が記載されたユーザ認証証明書を発行し、更に、トークンを発行する（図２１におけるステップＳ２０７）。次に、認証装置２０５が発行したトークンをサービスプロバイダ２０７に送付する（図２１におけるステップＳ２０８）。サービスプロバイダ２０７がトークンを受信すると、トークンとともに課金代行要求を送付する（図２１におけるステップＳ２１０）。課金代行サービス２０８が、課金代行要求を受信すると、誰に課金するべきか確認する（図２１におけるステップＳ２１１）。

【０１２２】

しかし、この段階では、ユーザ認証証明書はなく、課金代行サービス２０８は、トークンのみを受信している。そこで、認証装置２０５にトークンを送付し、証明書を要求する（図２１におけるステップＳ２１２）。認証装置２０５は、受信したトークンから証明書を検索して取得する（図２１におけるステップＳ２１３）。そして、証明書を要求している課金代行サービス２０８に送付する（図２１におけるステップＳ２１４）。課金代行サービス２０８が証明書を受信すると、権限を確認し、課金処理を行う（図２１におけるステップＳ２１５）。

【０１２３】

更に、課金代行サービス２０８が会社の費用負担部門２０９に請求書を送付する際には、課金代行サービス２０８はサービスプロバイダ２０７の代わりに費用負担部門２０９にアクセスすることになる。そこで、課金代行サービス２０８は、費用負担部門２０９にアクセスするための権限に関する証明書の発行要求を認証装置２０５に送付する（図２１におけるステップＳ２１６）。認証装置２０５は、証明書発行要求を受信すると、サービスプロバイダ２０７が費用負担部門２０９にアクセスするための証明書を発行し、更に、トークンを発行する（図２１におけるステップＳ２１７）。そして、認証装置２０５は、課金代行サービス２０８にトークンを送付する（図２１におけるステップＳ２１８）。

【０１２４】

課金代行サービス２０８がトークンを受信すると、受信したトークンと、支払い請求書とを会社の費用負担部門２０９に送付する（図２１におけるステップＳ２１９）。費用負担部門２０９が支払い要求書を受け付けると、どこのサービスからの要求であるかを確認するために、認証装置２０５に証明書の要求メッセージと受信したトークンを送付する（図２１におけるステップＳ２２０）。認証装置２０５は、受信したトークンに対応付けられた証明書を取得する（図２１におけるステップＳ２２１）。その後、認証装置２０５は、証明書を要求してきた費用負担部門２０９に送付する（図２１におけるステップＳ２２２）。証明書を受け取った費用負担部門２０９は、証明書と支払い要求書を確認して、支払い処理を完了する（図２１におけるステップＳ２２３）。

【０１２５】

本願は、日本の特願２００７－３３５９８８（２００７年１２月２７日に出願）に基づいたものであり、又、特願２００７－３３５９８８に基づくパリ条約の優先権を主張するものである。特願２００７－３３５９８８の開示内容は、特願２００７－３３５９８８を参照することにより本明細書に援用される。

【０１２６】

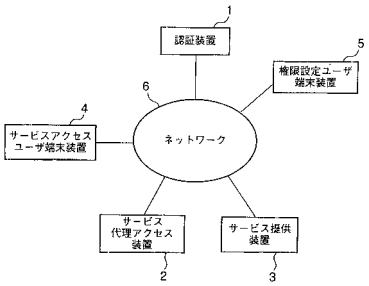
本発明の代表的な実施形態が詳細に述べられたが、様々な変更(changes)、置き換え(substitutions)及び選択(alternatives)が請求項で定義された発明の精神と範囲から逸脱することなくなされることが理解されるべきである。また、仮にクレームが出願手続きにおいて補正されたとしても、クレームされた発明の均等の範囲は維持されるものと発明者は意図する。

【産業上の利用可能性】

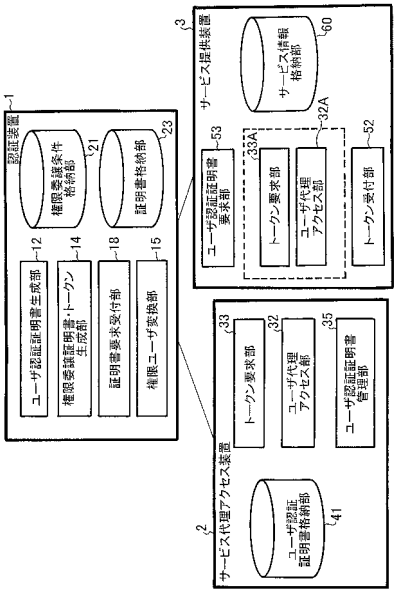
【０１２７】

本発明は、複数のサービスプロバイダが連携してユーザにサービスを提供する状況において、あるユーザが別のユーザから委譲された権限を利用して、サービスプロバイダに代理アクセスを実行することを許可するといった用途に適用可能である。また、インターネットサービス、企業内システム、企業間システム、キャリアシステムなどのネットワーク上で構築される分散システムにおける証明書管理や権限委譲管理システムや、権限管理システムをコンピュータに実現するためのプログラムといった用途に適用可能である。

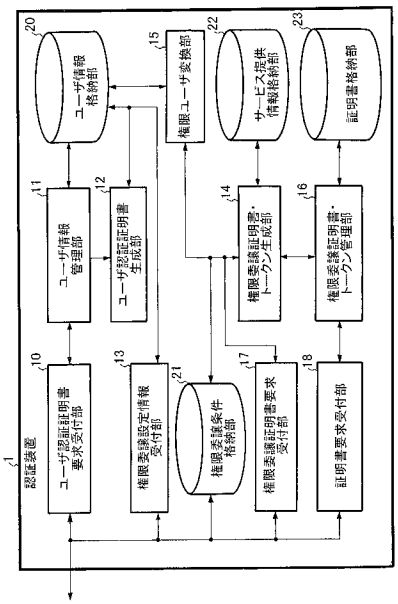
【図１】



【図２】



【図３】



【図４】

```
<Assertion ID="assertion - 12345678910" IssueInstnt="2005-07-01T00:20:02Z"Version="2.0">
  <Issuer> https: //authn200.com </Issuer>
  <ds:Signature> signature by authn200 goes here </ds:Signature>
  <Subject>
      <NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:persistent>
            aabbcc
      </NameID>
  </Subject>
  <Conditions NotBefore="2005-07-01T00:20:02Z" NotOnOrAfter="2005-07-01T00:25:02Z">
    <AudienceRestriction>
        <Audience>http://sp-proxy201.com</Audience>
    </AudienceRestriction>
  </Conditions>
  <AuthnStatement AuthnTnstaInt="2005-07-01T00:20:02Z" Not0N0rAfter="2005-07-
01T00:25:02Z">
    <saml:AuthnContext>
      <saml:AuthnContextClassRef>,
            urn:oasis:names:tc:SAML: 2 0:ac:classes:PasswordProtectedTreansport
      </saml:AuthnContextClassRef>
    </saml:AuthnContext>
  </AuthnStantement
</Assertion>
```

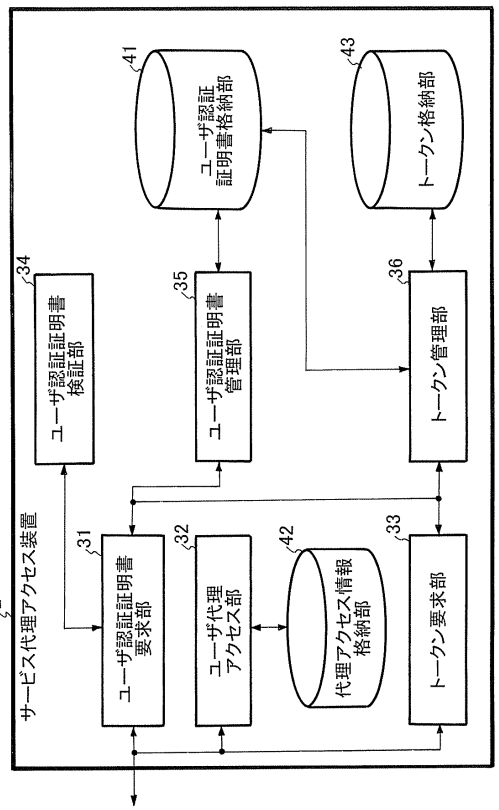
【図５】

権限委譲設定者識別子	権限委譲先利用者識別子	アクセス先サービスID
aabbcc	UserID_123	sp-proxy201.com

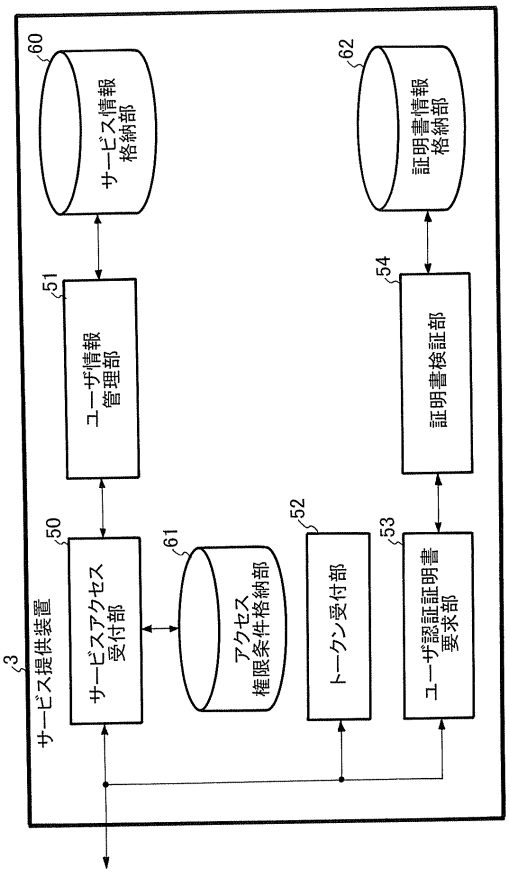
【図６】

トークン	証明書
9df234tr5234rig3485289	<Assertion>＊＊＊＊＊</Assertion>

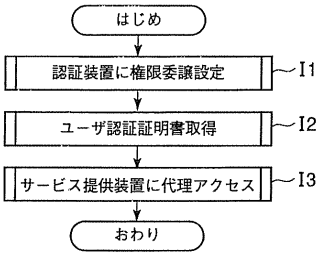
【図７】



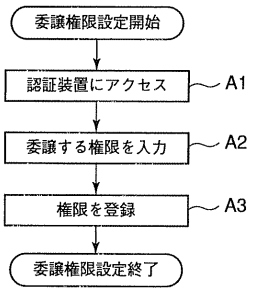
【図８】



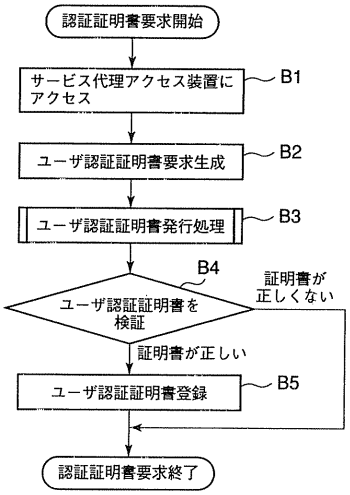
【図９】



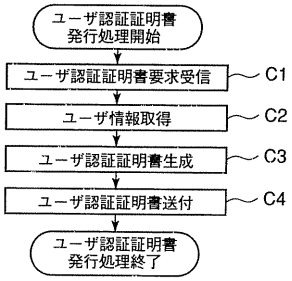
【図１０】



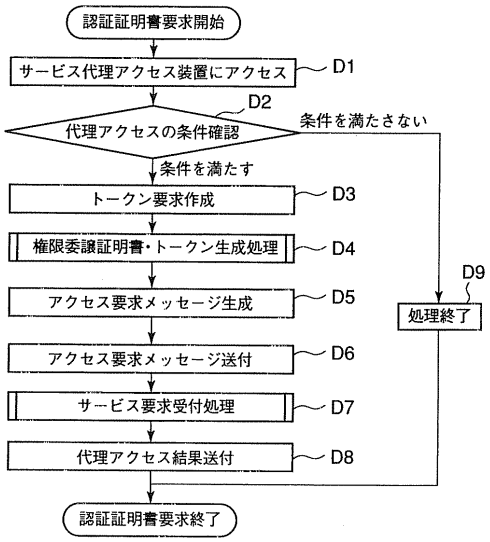
【図１１】



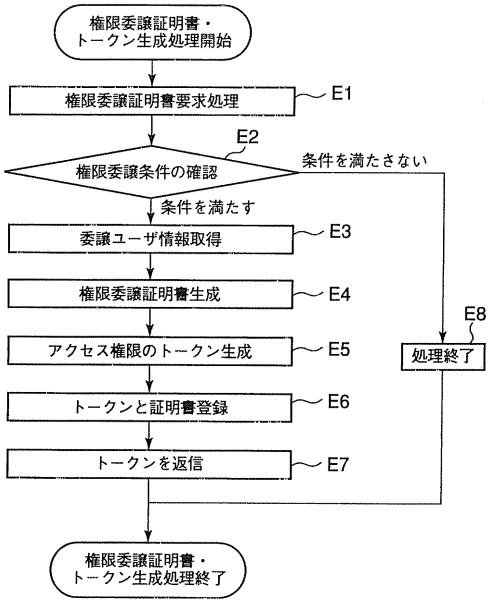
【図１２】



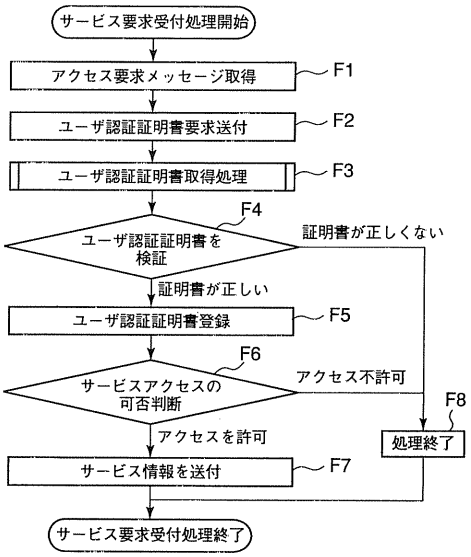
【図１３】



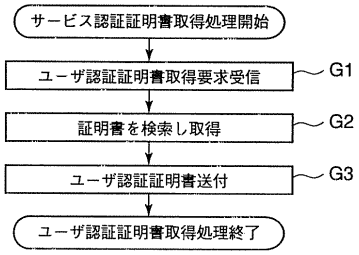
【図１４】



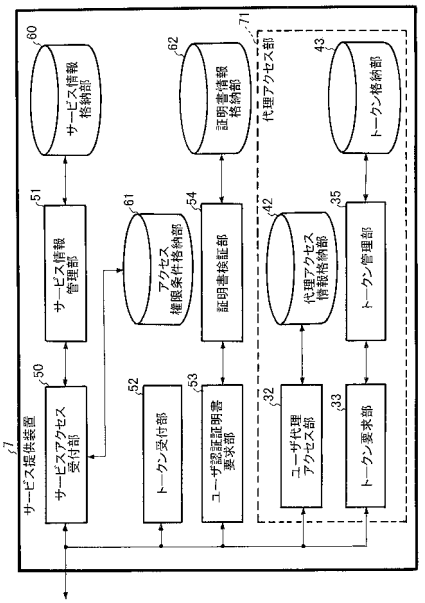
【図１５】



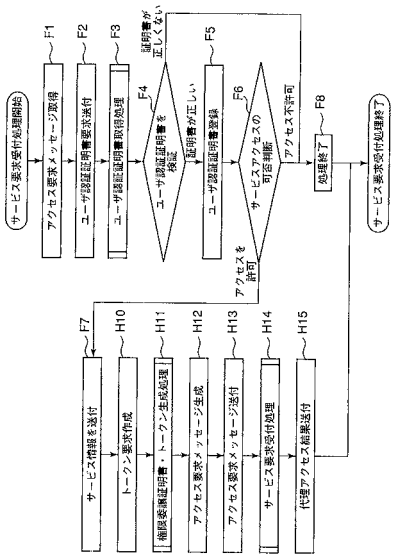
【図１６】



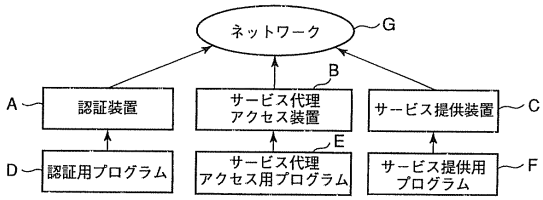
【図１７】



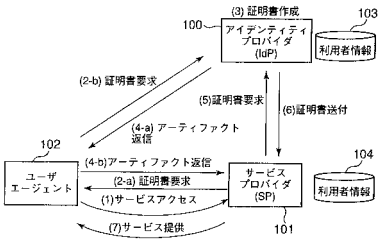
【図１８】



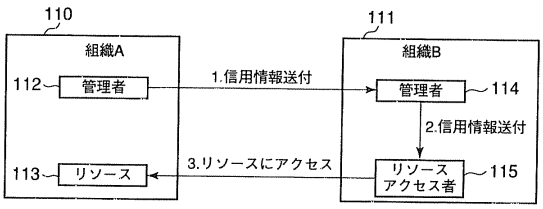
【図１９】



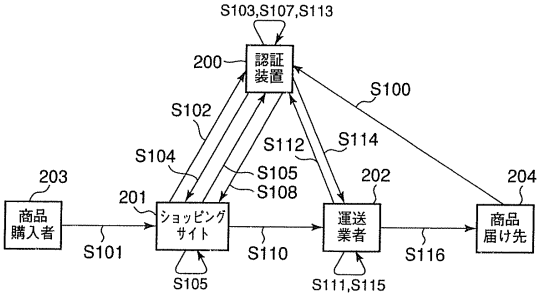
【図２２】



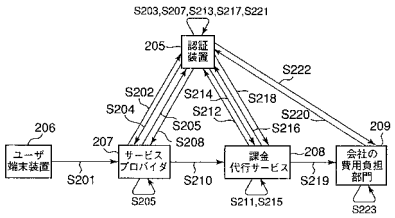
【図２３】



【図２０】



【図２１】



フロントページの続き

(56)参考文献 国際公開第２００９／０４１３１９（WO，Ａ１）
特開２００８－１９８０３２（ＪＰ，Ａ）
特開２００２－０６３４４４（ＪＰ，Ａ）
特開２００７－２３３７０５（ＪＰ，Ａ）
米国特許出願公開第２００７／０２４５４１４（ＵＳ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／３０
Ｇ０６Ｆ　２１／６０