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

特許第5177505号
(P5177505)

(45)発行日　平成25年4月3日(2013.4.3)　(24)登録日　平成25年1月18日(2013.1.18)

(51)Int.Cl.　　F I
G06F 21/41 (2013.01)　　G06F 21/20 141
G06F 21/33 (2013.01)　　G06F 21/20 133

請求項の数 6　(全 12 頁)

(21)出願番号　特願2008-44038(P2008-44038)
(22)出願日　平成20年2月26日(2008.2.26)
(65)公開番号　特開2009-205223(P2009-205223A)
(43)公開日　平成21年9月10日(2009.9.10)
審査請求日　平成23年1月14日(2011.1.14)

(73)特許権者　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(73)特許権者　504132272
国立大学法人京都大学
京都府京都市左京区吉田本町３６番地１
(74)代理人　100121706
弁理士　中尾　直樹
(74)代理人　100128705
弁理士　中村　幸雄
(74)代理人　100147773
弁理士　義村　宗洋
(74)代理人　100066153
弁理士　草野　卓

最終頁に続く

(54)【発明の名称】シングルサインオンによるグループ内サービス認可方法と、その方法を用いたグループ内サービス提供システムと、それを構成する各サーバ

(57)【特許請求の範囲】
【請求項１】
認証サーバが、端末から送信される情報を元にユーザを認証して認証情報を生成するユーザ認証過程と、
サービス提供サーバが、上記認証情報を取得するシングルサインオン過程と、
上記認証情報に権限が不足している場合に上記サービス提供サーバが、上記認証サーバに権限委譲情報を問い合わせる権限委譲情報問い合わせ過程と、
上記権限委譲情報の問い合わせがあった場合に上記認証サーバが、上記端末に権限委譲情報を要求する権限委譲情報要求過程と、
上記認証サーバが、上記権限委譲情報を認証して認可情報を生成する権限委譲認証過程と、
上記サービス提供サーバが、上記認可情報を認可する認可過程と、
を有するグループ内サービス認可方法であって、
上記サービス提供サーバにおいて、上記認可過程で認可された認可情報で上記シングルサインオン過程を制御し、上記シングルサインオン過程に対する新たなユーザアカウントを生成しないように制御することを特徴とするグループ内サービス認可方法。
【請求項２】
請求項１に記載のサービス認可方法において、
上記認証情報はＳＡＭＬアサーションであり、上記認可情報は上記ＳＡＭＬアサーションの拡張仕様を用いたものであることを特徴とするグループ内サービス認可方法。

【請求項３】
ユーザの認証情報を取得してシングルサインオンでサービスを提供するサービス提供サーバと、
ユーザの操作により上記サービスを要求する端末と、
上記ユーザと上記端末とを認証する認証サーバとを具備し、
上記認証サーバは、上記端末の権限委譲情報を要求する権限委譲情報要求部と、上記権限委譲情報を認証して認可情報を生成する権限委譲認証部とを備え、
上記サービス提供サーバは、ユーザ情報を認可する認証情報認可部と、上記認証サーバに権限委譲情報を問い合わせる権限委譲情報問い合わせ部と、認可情報を認可する認可部と、
を備え、
上記サービス提供サーバにおいて、上記認可過程で認可された認可情報で上記シングルサインオン過程を制御し、上記シングルサインオン過程に対する新たなユーザアカウントを生成しないように制御することを特徴とするグループ内サービス提供システム。
【請求項４】
請求項３に記載したグループ内サービス提供システムを構成する認証サーバであって、
上記端末から入力されるユーザ情報を認証して認証情報を生成するユーザ認証部と、
上記サービス提供サーバから権限委譲情報の問い合わせに応答して上記端末に権限委譲情報を要求する権限委譲情報要求部と、
上記権限委譲情報を認証して認可情報を生成する権限委譲認証部と、
を具備したことを特徴とする認証サーバ。
【請求項５】
請求項３に記載したグループ内サービス提供システムを構成するサービス提供サーバであって、
上記認証情報を認可する認証情報認可部と、
上記認証情報に権限が不足している場合に上記認証サーバに権限委譲情報を問い合わせる権限委譲情報問い合わせ部と、
上記認証サーバから入力される認可情報を認可する認可部と、
上記認証情報認可部と上記権限委譲認可部の認可結果に基づいてサービスを上記端末に提供するサービス提供部と、
を具備したことを特徴とするサービス提供サーバ。
【請求項６】
請求項５に記載のサービス提供サーバにおいて、
上記認可部の認可結果に基づいて被権限委譲者の一時的なアカウントを生成する一時アカウント生成部も、
具備することを特徴とするサービス提供サーバ。
【発明の詳細な説明】
【技術分野】
【０００１】
この発明は、シングルサインオン環境において電子的なサービスやアプリケーションを代理アクセスして利用する際のグループ内サービス認可方法と、その方法を用いたグループ内サービス提供システムと、そのシステムを構成する各サーバに関する。
【背景技術】
【０００２】
組織においてサービスや業務上の事務処理の電子化が急速であり、特にクライアントーサーバによるＷｅｂアプリケーションが利用されている。このようなオンラインサービスを利用する際には、アクセスしようとするユーザの本人性の確認が必要であり、その手段としてＩＤ／パスワード、ＩＣカード、電子証明書、バイオメトリクスなどの認証情報を利用した本人性の確認、つまり個人認証が行われている。
【０００３】

組織内では、あるユーザ（仮にユーザＡとする）の業務や事務処理を他のユーザ（仮にユーザＢとする）が代理で行うようなケースが考えられる。そのような場合の一手段としては、ユーザＢがユーザＡのＩＤ／パスワードを使ってログインし、ユーザＡに成りすまして業務を行う方法がある。しかしこの方法は、不正利用などの問題をはらんでおり、セキュリティ上好ましい方法とはいえない。

【０００４】

そこで、ある組織の共有リソースに対するアクセス権限の委譲方法については、例えば特許文献１開示されたものが知られている。図９に特許文献１の共有リソース管理システムのブロック構成を示して簡単に説明する。

【０００５】

共有リソース管理システムは、リソース管理サーバ１と、譲渡クライアント２と、被譲渡クライアント３とで構成される。譲渡クライアント２は、リソースに対するｎ個のアクセス権限５１と委譲権限証明書発行機能２１を備え、被譲渡クライアント３に譲渡するアクセス権限情報を委譲権限証明書５２として被譲渡クライアント３に発行する。署名はＰＫＣＳ＃７に基づいた形式とされる。

【０００６】

被譲渡クライアント３は、委譲権限証明書格納機能３２とディジタル代理署名生成機能３１を備え、ディジタル代理署名生成機能３１が委譲権限証明書５２に基づいて図示しないディジタル代理署名５３を生成してリソース管理サーバ１にアクセス要求する。

【０００７】

リソース管理サーバ１は、ディジタル代理署名検証機能１２と委譲権限検証機能１１と管理対象リソース１３を備え、ディジタル代理署名検証機能１２がディジタル代理署名５３を検証する。検証に成功した場合、ディジタル代理署名検証機能１２は委譲権限検証機能１１にディジタル代理署名５３を受け渡す。

【０００８】

委譲権限検証機能１１は、ディジタル代理署名５３から処理要求と委譲権限証明書の委譲内容を抽出し、リソース管理サーバ１が別途保持するアクセスコントロールリストとマッチングをとることによって被譲渡クライアント３が正しくアクセスしているかどうかを検証する。検証が成功した場合のみに管理対象リソース１３へのアクセスを許可する。このようにすることで譲渡された権限の不正利用を防ぐことができる。

【０００９】

また、社内システム向けのソリューションサービスとして、権限委譲を含めたＩＤ管理システムが提供されている（例えば非特許文献１参照）。このサービスでは権限委譲のケースとして、人事異動に伴う権限の再設定や、ヘルプデスク担当や派遣社員への部分的なアクセス権限付与などが挙げられている。人事異動の場合は、アクセス権限を前任者から後任者に付け替えるものであり、権限を与えられた後任者は本人のアカウントでアクセスを実行する。部分的なアクセス権限付与の場合は、システム管理者によって与えられた権限を使って、ユーザ本人としてアプリケーションサービスへアクセスする利用形態が想定されている。

【特許文献１】特開２００２－１６３２３５号公報（図１）

【非特許文献１】京セラコミュニケーションシステム（株）「ＩＤ管理システム（Green Office Directory）,http://www.kccs.co.jp/products/directory/index.html

【発明の開示】

【発明が解決しようとする課題】

【００１０】

しかし、従来の方法は何れもバックエンドアプリケーション側での負荷が大きくなる課題を持つ。つまり、特許文献１の方法では、委譲内容とアクセスコントロールリストとのマッチングをとることによって被譲渡クライアント３を検証することから明らかなように、被譲渡者のアカウントがリソース管理サーバ１に在ることを前提にしている。

【００１１】

また、非特許文献１の方法もアクセスしようとするリソースには少なくともユーザ本人のアカウントを作っている必要があり、もともとアカウントを持っていないユーザに権限を付与する場合にはまずアカウントを生成するという手間が必要となる。

【００１２】

このように従来の代理アクセス方法では、リソース側で権限委譲者と被権限委譲者の関連性を管理した上で認可制御をする必要があり、バックエンドアプリケーション側での負荷が大きくなる課題がある。

【００１３】

一方、バックエンドアプリケーション側におけるユーザ認証処理のコストを抑えるために、認証部分を認証サーバにアウトソースし、認証サーバでの認証結果の連携によってシングルサインオン（Single Sign-On、以下「ＳＳＯ」と称する）を実現する形態が提案されている（参考：Liberty Alliance ID-FF,http://www.projectliberty.org/resource_center/specification/liberty_alliance_id_ff_1_2_specifications）。各アプリケーションサービスプロバイダ（Application Service Provider、以下「ＳＰ」と称する）がそれぞれユーザを認証しなくても、一度認証サーバで認証されれば、認証サーバと信頼関係にあるＳＰに対しては認証処理をすることなく、認証結果を連携することによってログインが可能になる。この認証情報を伝達するプロトコルとしてＳＡＭＬｖ2.0（参考：OASIS SAMLv2.0,http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security）が標準化されている。

【００１４】

しかし、このＳＳＯ環境においても被権限委譲者Ｂがアクセスを許可されたアプリケーションサーバＣにアカウントを所持していない場合、被権限委譲者Ｂは新たにアプリケーションサーバＣにアカウントを作成する必要がある。その場合には一からユーザ登録したり、ＳＳＯ環境を整えたりする必要があり、結局バックエンドアプリケーション側での負荷が増えることになる。ここでＳＳＯ環境とは、ディレクトリへのＰＫＩ情報の格納と統合や、アプリケーションサーバのディレクトリ/ＰＫＩ対応の設定等のことである。

【００１５】

この発明は、このような点に鑑みてなされたものであり、ＳＳＯ環境における組織内（グループ内）の代理アクセスをバックエンドアプリケーション側の負荷を大きくすることなく実現するグループ内サービス認可方法と、その方法を用いたサービス提供システムと、それを構成する各サーバを提供することを目的とする。

【課題を解決するための手段】

【００１６】

この発明のグループ内サービス認可方法は、認証サーバが端末から送信される情報を元にユーザを忍証して認証情報を生成するユーザ認証過程と、サービス提供サーバが上記認証情報を認可するシングルサインオン過程と、認証情報に権限が不足している場合にサービス提供サーバが認証サーバに権限委譲情報を問い合わせる権限委譲情報問い合わせ過程と、認証サーバが端末に権限委譲情報を要求する権限委譲情報要求過程と、認証サーバが権限委譲情報を認証し認可情報を生成する権限委譲認証過程と、サービス提供サーバが認可情報を認可する認可過程と、を有し、サービス提供サーバにおいて、上記認可過程で認可された認可情報でシングルサインオン過程を制御し、シングルサインオン過程に対する新たなユーザアカウントを生成しないように制御する。

【００１７】

また、この発明のグループ内サービス提供システムは、ユーザの認証情報を取得してＳＳＯでサービスを提供するサービス提供サーバと、ユーザの操作によりサービスを要求する端末と、ユーザと端末とを認証して端末とサービス提供サーバを接続する認証サーバとを具備する。認証サーバは、端末の権限委譲情報を要求する権限委譲情報要求部と、権限委譲情報を認証して認可情報を生成する権限委譲認証部とを備える。サービス提供サーバは、認証情報を認可する認証情報認可部と、認証サーバに権限委譲情報を問い合わせる権限委譲情報問い合わせ部と、認可情報を認可する認可部とを備える。

【発明の効果】
【００１８】
この発明のグループ内サービス認可方法及びその方法を用いたグループ内サービス認可システムによれば、ユーザＡの代理アクセスを行うユーザＢの認証情報に権限が不足している場合に、サービス提供サーバが認証サーバに権限委譲情報を問い合わせ、認証サーバが委譲権限情報を認証し認可情報を生成する。そして、サービス提供サーバが認可情報を認可して権限が委譲されたユーザＢにサービスを提供する。したがって、サービス提供サーバにアカウントを持たないユーザＢでも、新たにアカウントを取得することなくサービスを受けることができ、バックエンドアプリケーション側での負荷を増やすことなくグループ内の代理アクセスを可能にする。
【発明を実施するための最良の形態】
【００１９】
以下、この発明の実施の形態を図面を参照して説明する。複数の図面中同一のものには同じ参照符号を付し、説明は繰り返さない。
【実施例１】
【００２０】
図１にこの発明のグループ内サービス提供システムのシステム構成を示す。グループ内サービス提供システムは、ユーザの認証情報を取得してＳＳＯでサービスを提供するサービス提供サーバ５０，５１，５２と、ユーザの操作によりサービスを要求する端末１０と、ユーザと端末１０とを認証して端末１０と各サービス提供サーバ５０，５１，５２を接続する認証サーバ４０とを具備する。各サーバ４０，５０，５１，５２と端末１０とは、ネットワーク（以下「ＮＷ」と称する）２０を介してお互いに接続されている。
【００２１】
認証サーバ４０の配下には、ユーザデータベース４０ｄが接続されており、ユーザデータベース４０ｄにはユーザのアカウント、認証情報、連携先のサービス提供サーバ情報と連携情報が格納される。サービス提供サーバ５０，５１，５２の配下には、ディレクトリデータベース５０ｄ，５１ｄ，５２ｄがそれぞれ接続されており、ユーザのアカウント、認証情報、連携先の認証サーバ情報と連携情報と、サービス情報が格納される。各サービス提供サーバ５０，５１，５２は、認証サーバ４０と信頼関係を構築しており、認証サーバ４０が生成する認証情報に基づいてユーザにサービス情報を提供する。
【００２２】
この発明の基本的な考えは、ユーザＡに代わってユーザＢが、あるアプリケーションＣ（何れかのサービス提供サーバ）にアクセスしてサービスを利用する場合に、ユーザＡは自分の認証情報そのものを渡すのではなく、「ユーザＡがアプリケーションＣのサービスを利用する権限」を示す情報をユーザＢに渡すことにある。ここで、当該権限を委譲する情報を渡す方法としては、属性証明書（権限委譲証明書、電子証明書）を被権限委譲者が所有する媒体（ＰＣ，ＩＣカード，ＵＢＳメモリーなど）に格納する方法や、権限委譲者が代理人のアクセス用に予め設定した第二のパスワードを被権限委譲者に伝えるなどの方法が考えられる。
【００２３】
ユーザＡがユーザＢに、サービス提供サーバ５０へアクセスするための権限委譲を行う場合の初期状態の一例を図２に示す。ユーザＡとユーザＢは、共に認証サーバ４０にアカウント「Yamada Taro」、「Suzuki Hanako」を持っている。ユーザＡはサービス提供サーバ５０にもアカウントを持ち、認証サーバ４０とＩＤ連携済みである。認証サーバ４０が生成する認証情報によりサービス提供サーバ５０は、ユーザＡをＳＳＯ可能である。一方、ユーザＢはサービス提供サーバ５０にアカウントを持たないため、サービス提供サーバ５０のサービスを利用することができない。
【００２４】
このような場合、サービス提供サーバ５０側において、ユーザＢはユーザＡの代理人であることが分かれば、ユーザＡのアカウントのままユーザＢにサービスを提供することが

可能である。そこで、この発明ではユーザＡのアカウントのまま、アカウントの属性を変えてサービス提供サーバ５０にアクセス要求を行う。最も簡単な方法としては、SAML Shared Credential拡張仕様を利用する方法が考えられる。

【００２５】

図１に示したシステム構成のシーケンスを図３に示してこの発明のグループ内サービス認可方法を説明する。ユーザＢは、自身のユーザ情報であるＩＤ/パスワードや電子証明書を端末１０に入力する（ステップＳ１）。端末１０は、ユーザＢのＩＤ/パスワードで認証サーバ４０にログインする（ステップＳ２）。認証サーバ４０は、端末１０から入力されるＩＤ/パスワード等のユーザ情報を認証して認証情報を生成する（ステップＳ３）。認証情報は、例えばＳＡＭＬアサーションである。認証サーバ４０は、ＳＡＭＬアサーションを生成してサービス提供サーバ５０にアクセス要求する（ステップＳ４）。

【００２６】

サービス提供サーバ５０は、ユーザＢのＳＡＭＬアサーションを取得してＳＳＯを行う（ステップＳ５）。しかし、サービス提供サーバ５０は、ユーザＢのアカウントを持たないので、権限委譲情報を認証サーバ４０に問い合わせる（ステップＳ６）。

【００２７】

認証サーバ４０は、権限委譲情報の問い合わせがあった場合に端末１０に権限委譲情報を要求する（ステップＳ７）。端末１０は、図示しないモニターに権限委譲情報が要求されていることを表示して、ユーザＢに権限委譲情報を入力させる（ステップＳ８）。端末１０は権限委譲情報を認証サーバ４０に送信する（ステップＳ９）。認証サーバ４０は、権限委譲情報を認証して認可情報を生成（ステップＳ１０）してサービス提供サーバ５０に再びアクセス要求する（ステップＳ１１）。認可情報は、ＳＡＭＬアサーションの拡張仕様を用いることができる。認可情報は、例えばＳＡＭＬアサーションのShared Credential要素にビット“１”がセットされているものとする。

【００２８】

サービス提供サーバ５０は、認可情報のShared Credential要素のビットが“１”にセットされていることを確認すると、ユーザＢがユーザＡの代理人としてアクセス要求していると判断し、認可情報を認可する（ステップＳ１２）。サービス提供サーバ５０は、認可情報を認可すると、ユーザＢが操作する端末１０からの代理アクセスを許可する（ステップＳ１３）。

【００２９】

以上述べたように、この発明のグループ内サービス認可方法によれば、ユーザＡの代理アクセスを行うユーザＢの認証情報に権限が不足している場合に、サービス提供サーバ５０が認証サーバ４０に権限委譲情報を問い合わせ、認証サーバ４０が権限委譲情報を認証し認可情報を生成する。サービス提供サーバ５０は、認可情報を認可して権限が委譲されたユーザＢにサービスを提供するので、新たにアカウントを取得することなくサービスを受けることが可能である。つまり、バックエンドアプリケーション側での負荷を増やすことなくグループ内の代理アクセスを行うことができる。このように、「誰からどのリソースに対する権限が委譲されている」という情報のみを記述した権限委譲情報でリソース側での認可制御を可能にするので、簡単なグループ内サービス認可方式とすることができる。なお、ユーザ認証過程（ステップＳ３）と、権限委譲認証過程（ステップＳ１０）と二つの段階に分けて認証する例で説明を行ったが、ユーザＢのユーザ情報に権限委譲情報を含めることで一度の認証で、権限委譲されたサービスを提供することも可能である。

【００３０】

また、この発明のグループ内サービス認可方式によれば、従来の方法のように委譲内容とアクセスコントロールリストとのマッチングを取るといったように、権限委譲側が認可種類まで完全に制御する必要はない。認可情報の内容によって、サービス提供側が権限委譲されたユーザに対してどの程度のサービスを認可するかというサービスポリシーの設定も、サービス提供側で設定することが可能である。

【００３１】

この発明のグループ内サービス認可方式を実現する認証サーバ４０とサービス提供サーバ５０の機能構成例を図４と図６に、その動作フローを図５と図７に示してその動作を更に詳しく説明する。

【００３２】

〔認証サーバ〕

認証サーバ４０は、通信インターフェース４１と、機能ブロック４２と、制御手段４３とを備える。機能ブロック４２は、ユーザ認証部４２１と、データベース制御部４２２と、権限委譲認証部４２３と、権限委譲情報要求部４２４を具備する。機能ブロック４２の各部は、制御手段４３によって制御される。機能ブロック４２は、通信インターフェース４１を介してＮＷ２０と接続される。ユーザデータベース４０ｄは、データベース制御部４２２を介して権限委譲認証部４２３と、ユーザ認証部４２１とに接続される。

【００３３】

ユーザ認証部４２１は、端末１０から入力されるユーザＢのＩＤ/パスワードを認証する（ステップＳ３０）。端末１０から入力されたユーザＢのＩＤ/パスワードが、ユーザデータベース４０ｄに登録済みであるかを、データベース制御部４２２を介して検索してユーザ認証を行う。ユーザデータベース４０ｄにユーザＢが未登録の場合、正しいＩＤ/パスワードを要求（ステップＳ３２）して動作を終了する。ユーザＢが登録済みの場合、ユーザ認証部４２１はＳＡＭＬアサーションを生成（ステップＳ３１）し、通信インターフェース４１を介してサービス提供サーバ５０に送信する。

【００３４】

この時、権限委譲情報に不足があれば（ステップＳ４０、不足情報あり）、権限委譲情報要求部４２４が端末１０に対して権限委譲情報を要求する（ステップＳ４１）。不足情報がなければ、ユーザ認証成功の処理（ステップＳ４５）を行い動作を終了する。ユーザ認証成功の処理とは、例えばユーザ認証成功フラグを“１”にセットするような処理である。

【００３５】

権限委譲認証部４２３は、端末１０に入力される権限委譲情報を認証する（ステップＳ４２）。権限委譲情報としては、少なくとも権限委譲者（ユーザＡ）と権限委譲対象の情報が分かればよい。権限委譲認証部４２３は、権限委譲情報が正当なものであるかを、データベース制御部４２２を介してユーザデータベース４０ｄを検索し、正当なもと認められれば（ステップＳ４２、成功）認可情報を生成する（ステップＳ４３）。認可情報とは、上記したように例えばＳＡＭＬアサーションの拡張仕様を用いたものである。権限委譲情報が不当なものであった場合（ステップＳ４２、失敗）、権限委譲認証部４２３は正当な権限委譲情報を端末１０に要求（ステップＳ４４）して動作を終了する。

【００３６】

〔サービス提供サーバ〕

認証サーバ４０で生成されたＳＡＭＬアサーションと認可情報の認可をサービス提供サーバ５０が行う。サービス提供サーバ５０は、通信インターフェース５１と、機能ブロック５２と、制御手段５３とを備える。機能ブロック５２は、認証情報認可部５２１と、データベース制御部５２２と、権限委譲情報問い合わせ部５２３と、認可部５２４と、サービス提供部５２５を具備する。機能ブロック５２の各部は、制御手段５３によって制御される。機能ブロック５２は、通信インターフェース４１を介してＮＷ２０と接続される。ディレクトリデータベース５０ｄは、データベース制御部５２２を介して認証情報認可部５２１と、認可部５２４と、サービス提供部５２５と接続される。

【００３７】

認証サーバ４０が生成したＳＡＭＬアサーションは、認証情報認可部５２１に入力される。認証情報認可部５２１は、取得したＳＡＭＬアサーションをＳＳＯする（ステップＳ５）。ＳＡＭＬアサーションを確認した後（ステップＳ５０）に、ＳＡＭＬアサーションの内容について検証する。つまり認証情報認可部５２１は、ＳＡＭＬアサーションと、ディレクトリデータベース５０ｄ内に登録されたユーザ属性とを、データベース制御部５２

２を介して照合する（ステップＳ５１）。

【００３８】

図２に示した例では、サービス提供サーバ５０がユーザＢのアカウントを持たないので、権限委譲情報問い合わせ部５２３が認証サーバ４０に権限委譲情報を問い合わせる（ステップＳ６）。認証サーバ４０に権限委譲情報を問い合わせた結果、認証サーバ４０で生成された認可情報は、認可部５２４で受信（ステップＳ１２０）される。認可部５２４は、Shared Credentialの値が“１”であることにより、当該アサーションはユーザＡ本人に対して発行されたものではなく、権限を委譲された代理人に対して発行されたものであると判断する（ステップＳ１２１）。サービス提供サーバ５０は、端末１０にアクセスを許可（ステップＳ１３）し、自身の認可ポリシーに従ってユーザＢに対してユーザＡの代理人としての権限を与え、サービス提供部５２５がディレクトリデータベース５０ｄ内のサービス情報を端末１０に提供する（ステップＳ７０）。

【００３９】

以上、被権限委譲者側がアカウントを持たない場合の例で説明を行ったが、被権限委譲者もアカウントを持つが一部のサービスを利用する権限を持たないような場合も考えられる。例えば図８に示すような場合である。ユーザＢは、サービス提供サーバ５０にS.Hanakoのアカウントを有するが、ユーザＡが持つ△△サービスを利用する権限を持たない。このような場合にも、この発明のグループ内サービス認可方法を用いることでバックエンドアプリケーション側での負荷を増やすことなく権限委譲を行うことが可能である。つまり、サービス提供サーバ５０は、Shared Credentialの値が“１”である場合に、サービスを利用する権限が委譲されているユーザＢからのアクセス要求であると判断し、△△サービスの提供を認可する。

【００４０】

また、この発明のグループ内サービス認可方法を用いて一時的にアカウントを作成してもよい。一時的なアカウントは、サービス提供サーバ５０内に破線で示す一時アカウント生成部５２６（図５）で生成することができる。アカウントを生成することは、バックエンドアプリケーション側の負荷を増やすことになるが、一時アカウント生成部５２６で生成するアカウントを所定時間で消去するようにしておけば、サービス提供サーバ５０のメモリ資源を圧迫することがない。よって、メモリ資源を効率的に使用した融通の利いた権限委譲を行うことができる。

【００４１】

また、認可情報を例えばＳＡＭＬアサーションの拡張仕様を用いた例で説明を行ったが、ＳＡＭＬのAttributeやAuthnContextに属性として記述してもよいし、ＩＤ-ＷＳＦ仕様の属性交換により実現することも可能である。

【００４２】

なお、この発明の方法及び各サーバは上述の実施形態に限定されるものではなく、この発明の趣旨を逸脱しない範囲で適宜変更が可能である。また、上記方法及び各サーバにおいて説明した処理は、記載の順に従って時系列に実行されるのみならず、処理を実行するサーバの処理能力あるいは必要に応じて並列的にあるいは個別に実行されるとしてもよい。

【００４３】

また、上記サーバにおける処理内容はプログラムによって記述される。また、各サーバの機能構成部は、コンピュータ上で所定のプログラムを実行させることにより構成することにしてもよいし、これらの処理内容の少なくとも一部をハードウェア的に実現することとしてもよい。

【図面の簡単な説明】

【００４４】

【図１】この発明のグループ内サービス提供システムのシステム構成を示す図。

【図２】ユーザＡが、ユーザＢにサービス提供サーバ５０へアクセスするための権限委譲を行う場合の初期状態の一例を示す図。

【図３】図１のシーケンスを示す図。
【図４】認証サーバ４０の機能構成例を示す図。
【図５】認証サーバ４０の動作フローを示す図。
【図６】サービス提供サーバ５０の機能構成例を示す図。
【図７】サービス提供サーバ５０の動作フローを示す図。
【図８】ユーザＡが、ユーザＢにサービス提供サーバ５０へアクセスするための権限委譲を行う場合に一部のサービス利用権限がない場合を示す図。
【図９】特許文献１に開示された共有リソース管理システムのブロック構成を示す図。

【図１】

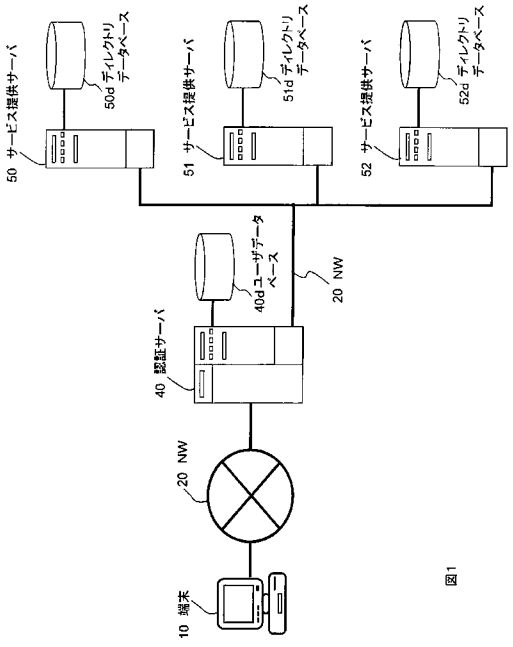

図1

【図２】

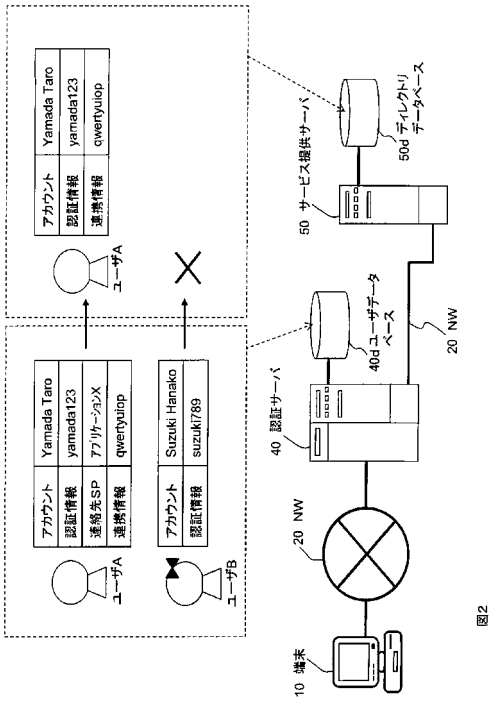

図2

【図３】

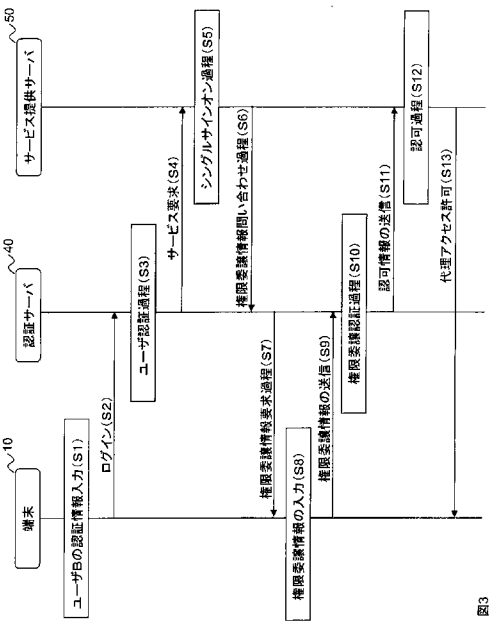

図3

【図４】

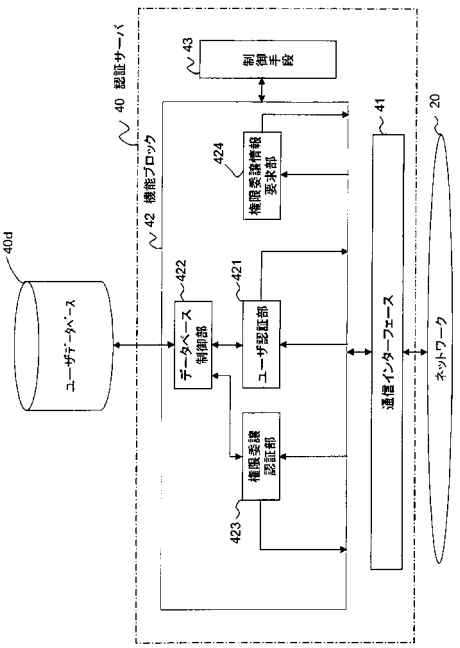

図4

【図５】

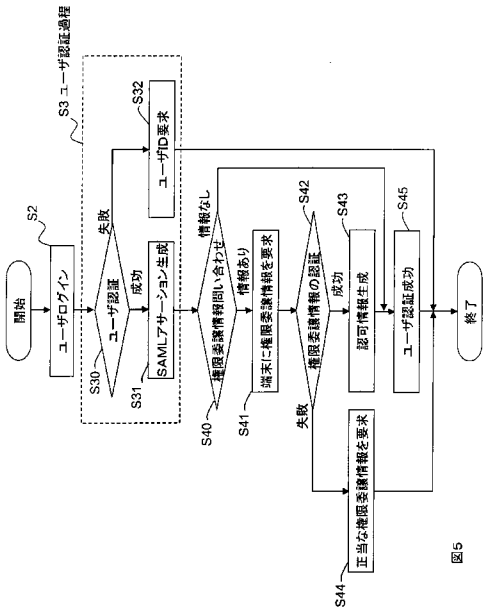

図5

【図６】

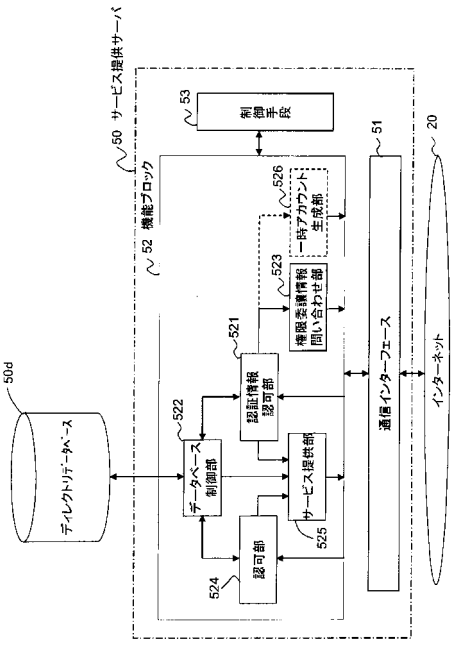

図6

【図７】

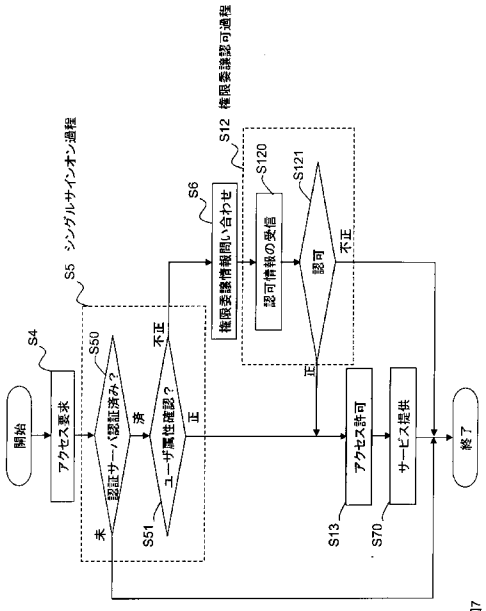

図7

【図８】

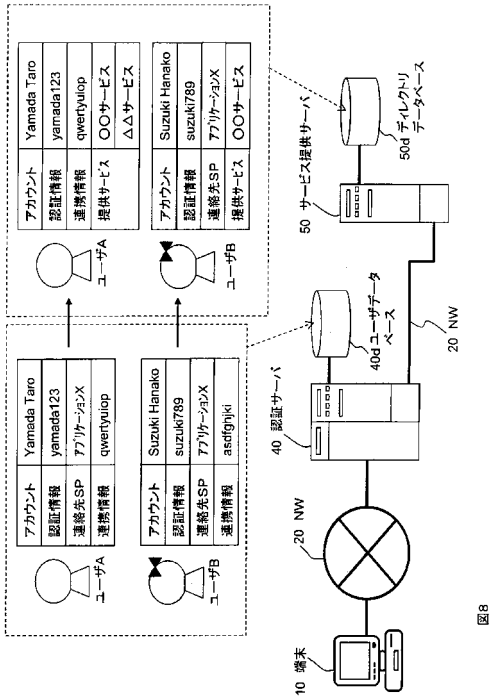

図8

【図９】

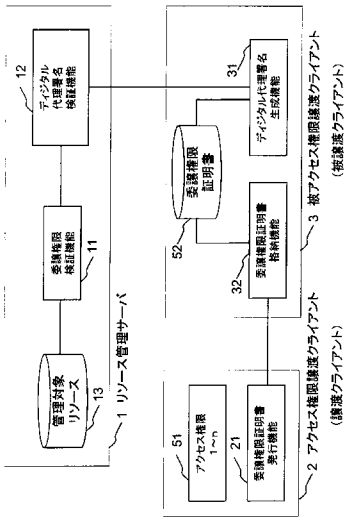

図9

フロントページの続き

(72)発明者　青柳　真紀子
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　高橋　健司
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　永井　靖浩
京都府京都市左京区吉田本町　国立大学法人京都大学大学院情報学研究科内
(72)発明者　古村　隆明
京都府京都市左京区吉田本町　国立大学法人京都大学大学院情報学研究科内

審査官　▲吉▼田　耕一

(56)参考文献　特開２００４－３０２９０７（ＪＰ，Ａ）
特開２００２－２２２２５１（ＪＰ，Ａ）
特開２００６－２２１５０６（ＪＰ，Ａ）
特開２００２－１６３２３５（ＪＰ，Ａ）
特開２００８－０３３６３８（ＪＰ，Ａ）
特開２００６－２６０００２（ＪＰ，Ａ）
特開２００６－１１９７１９（ＪＰ，Ａ）
千葉　昌幸，属性情報プロバイダ：安全な個人属性の活用基盤の提言，情報処理学会論文誌，社団法人情報処理学会，２００６年　3月１５日，Vol.47，No.3，pp.676-685

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／２０