

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2009-205223
(P2009-205223A)

(43) 公開日 平成21年9月10日(2009.9.10)

(51) Int.Cl.
G06F 21/20 (2006.01)

F I
G06F 15/00 330D

テーマコード(参考)
5B285

審査請求 未請求 請求項の数 6 O L (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)

(71) 出願人 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
(71) 出願人 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 100066153
弁理士 草野 卓
(74) 代理人 100128705
弁理士 中村 幸雄
(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

最終頁に続く

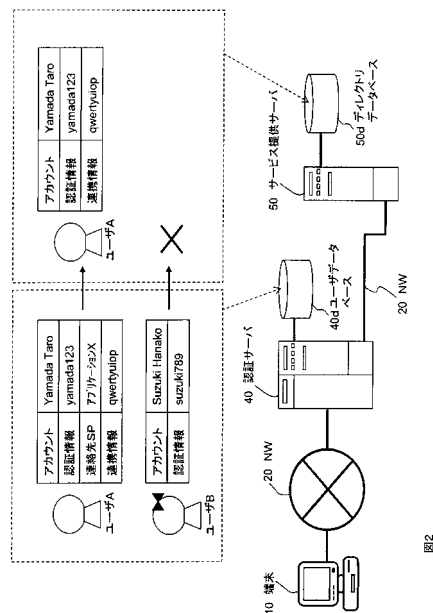
(54) 【発明の名称】 シングルサインオンによるグループ内サービス認可方法と、その方法を用いたグループ内サービス提供システムと、それを構成する各サーバ

(57) 【要約】

【課題】 S S O 環境における組織内 (グループ内) の代理アクセスを簡単に行う。

【解決手段】 この発明のグループ内サービス認可方法は、サービス提供サーバが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委譲情報要求過程と、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委譲権限認証過程と、サービス提供サーバが認可情報を認可する委譲権限認可過程と、を有する。認可情報には、例えば S A M L アサーションの拡張仕様を用いる。

【選択図】 図 2



【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。

【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 S A M L アセッションであり、上記認可情報は上記 S A M L アセッ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、

を備えた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】

ネットワークを介してサービス提供サーバと端末とに接続され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】

認証サーバからの認証情報を取得して端末にサービスを提供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。

10

20

30

40

50

【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。

10

【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。

20

【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とデジタル代理署名生成機能31を備え、デ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。

30

【0007】

リソース管理サーバ1は、デ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、デジタル代理署名検証機能12がデジタル代理署名53を検証する。検証に成功した場合、デジタル代理署名検証機能12は委譲権限検証機能11にデジタル代理署名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。

40

【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

50

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。

10

【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。

20

【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SAML v2.0(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。

30

【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。

40

【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

50

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。

10

【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。

20

【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。

30

【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。

40

【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

50

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

10

20

30

40

50

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。

10

【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。

20

【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。

30

【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、正当なものと認められれば（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。

40

【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

50

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522を介して照合する(ステップS51)。

10

【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)。

20

【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.Hana ko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。

30

【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。

40

【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

50

サーバの処理能力あるいは必要に応じて並列的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。

10

【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。

20

【図1】

【図2】

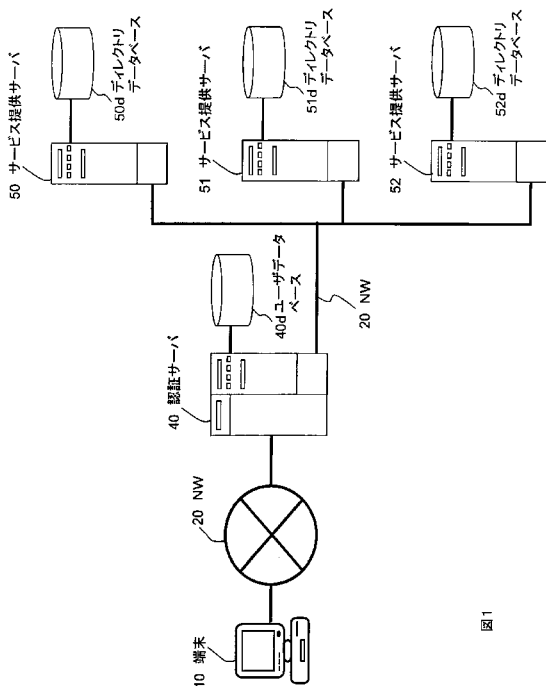


図1

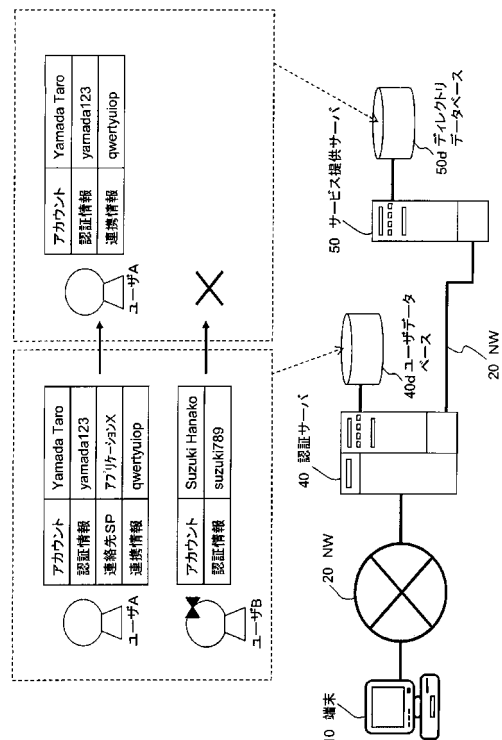


図2

【 図 3 】

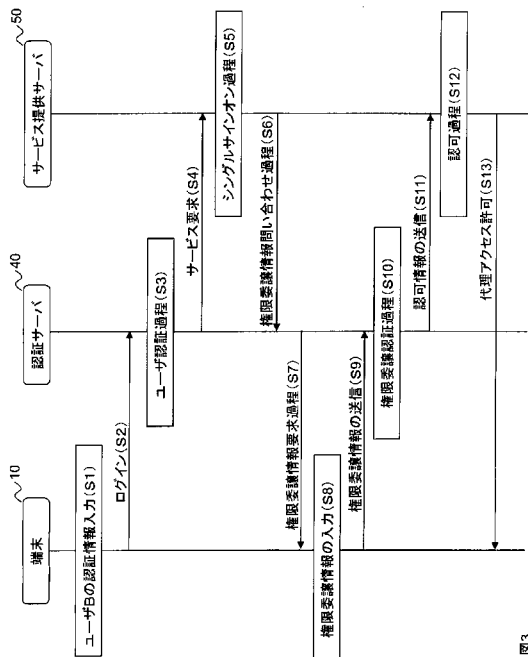


図3

【 図 4 】

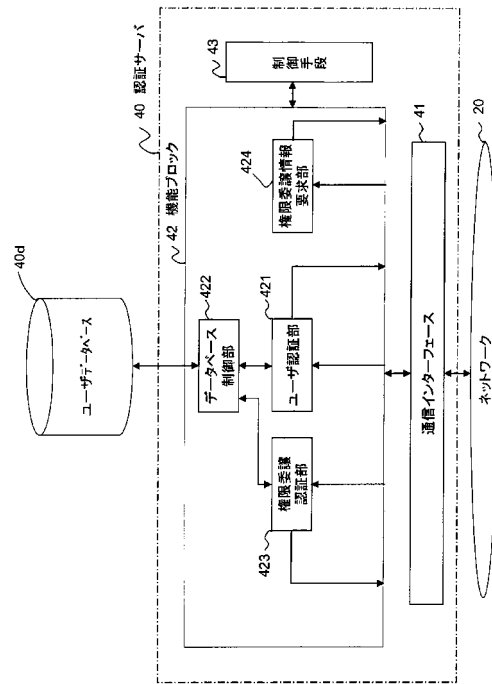


図4

【 図 5 】

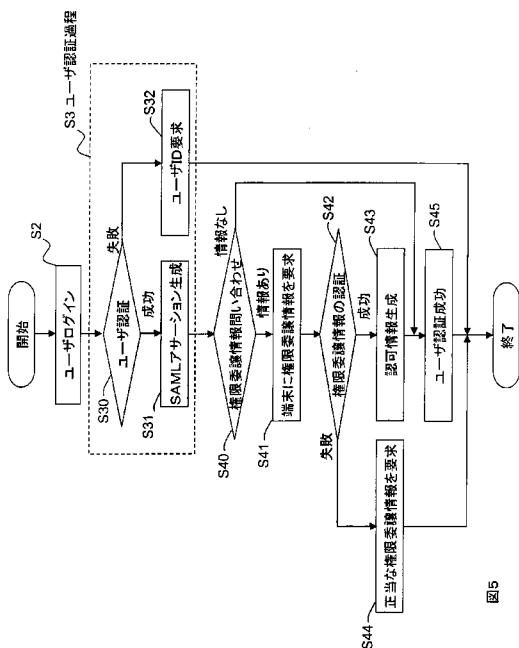


図5

【 図 6 】

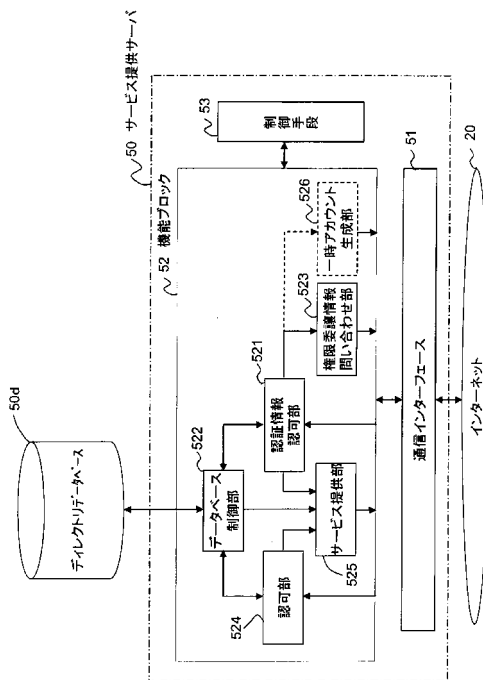


図6

【 図 7 】

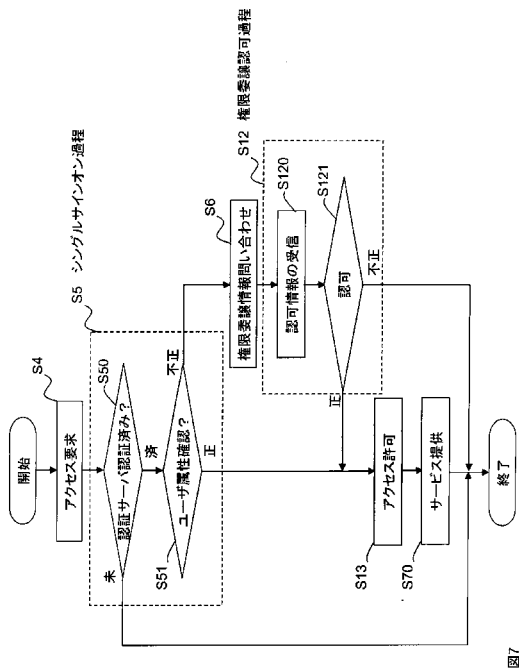


図7

【 図 8 】

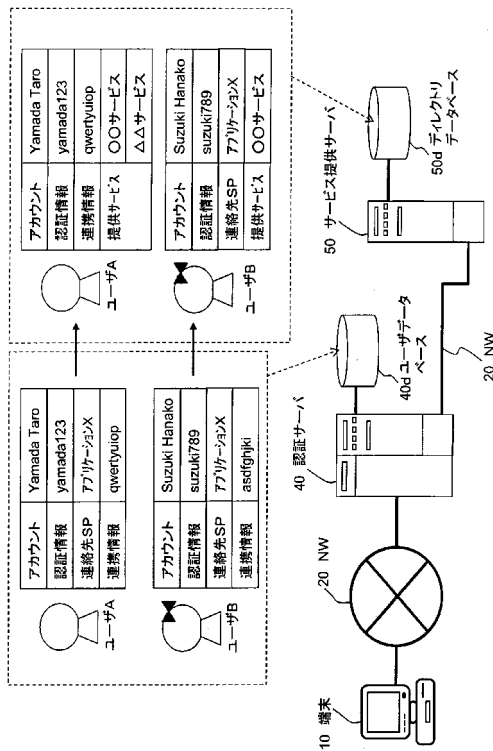


図8

【 図 9 】

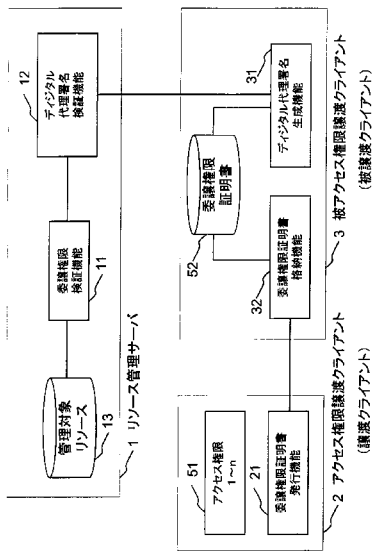


図9

フロントページの続き

(72)発明者 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

Fターム(参考) 5B285 BA01 CA44 CB02 CB47 CB52 CB53 CB55 CB73 CB90