(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4863253号
(P4863253)
(45)発行日　平成24年1月25日(2012.1.25)　(24)登録日　平成23年11月18日(2011.11.18)

(51)Int.Cl.　F I
G06F 21/20 (2006.01)　G06F 15/00 330D

請求項の数 3　(全 18 頁)

(21)出願番号　特願2005-280076(P2005-280076)
(22)出願日　平成17年9月27日(2005.9.27)
(65)公開番号　特開2007-94522(P2007-94522A)
(43)公開日　平成19年4月12日(2007.4.12)
審査請求日　平成20年9月24日(2008.9.24)

(73)特許権者　598096991
学校法人東京農業大学
東京都世田谷区桜丘１丁目１番１号
(74)代理人　100122574
弁理士　吉永　貴大
(74)代理人　100116872
弁理士　藤田　和子
(72)発明者　田中　晋
東京都世田谷区桜丘１丁目１番１号　東京農業大学内

審査官　市川　武宜

最終頁に続く

(54)【発明の名称】統合ユーザ管理システム

(57)【特許請求の範囲】
【請求項１】
ユーザのユーザ情報及びポリシから構成されるユーザデータを管理し、認証を行う統合ユーザ管理システムであって、
前記ユーザの認証方法が異なる複数の認証サービスに接続され、前記複数の認証サービスのうち認証が必要とされる認証サービスのユーザデータの同期を統合的に行うアカウント統合機能部と、
実行のために前記ユーザの認証を行う認証モジュールを有する少なくとも１つのアプリケーションと、
前記ユーザデータを記録し、記録された前記ユーザデータを前記アカウント統合機能部及び前記認証モジュールに配信し、配信された前記ユーザデータを使用して、前記認証サービス及び前記認証モジュールの少なくとも一方で前記ユーザの認証が行われるように統合的に管理する論理統合機能部とを備え、
前記ポリシが、所属情報と身分情報とにより分類され、
前記ユーザデータが、所属情報及び身分情報による２つの役割セットと、前記アプリケーションごとにそのアプリケーションの使用に関して所定の権限が設定された前記ユーザの集合であるアプリケーション・ユーザグループとから構成される三次元役割セットに関する情報を含む統合ユーザ管理システム。
【請求項２】
請求項１に記載の統合ユーザ管理システムであって、

前記論理統合機能部が、前記ユーザデータが更新された際に、前記アカウント統合機能部と前記認証モジュールに対して、所定のデータ形式でこの更新されたユーザデータを配信する統合ユーザ管理システム。

【請求項３】

請求項１から２いずれか記載の統合ユーザ管理システムであって、

前記論理統合機能部が、ユーザの認証に使用しないユーザデータであって、前記アプリケーションのいずれかにおいて使用するユーザ情報を、一元的に管理する統合ユーザ管理システム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、統合ユーザ管理システムに関する。さらに具体的には、多数のユーザで共有する情報システムについて、ユーザ情報を総合的に管理し、かつ、ユーザが複数の認証サービス、及び認証を必要とする情報システムに対して円滑にユーザの認証を行い、かつポリシに基づきユーザ情報を流通させ、さらに、閲覧・加工・集計などの２次利用を許可するための統合ユーザ管理システムに関する。

【背景技術】

【０００２】

従来より、情報システムにおいて、多数のユーザから所定の使用許可基準を満たすユーザにのみデータのアクセスを許可したり、アプリケーションの使用を承諾する方法が知られている。この機能を実現するためには、ユーザ毎にポリシを設定し、ポリシの要件を満たすユーザにはアクセスの許可を行うといった方法が知られている。

【０００３】

例えば、ユーザが情報システムを使用するための環境に関する情報を管理することで、認証を行う方法が知られている。この方法では、あるアプリケーションの使用及びユーザが所定のデータにアクセス可能であるかのユーザ権限が記録されたユーザ情報を管理し、このユーザ権限を利用することでアクセスの認証を実現している。この一例としては、ディレクトリ・サービスが知られており、ＬＤＡＰ（Lightweight Directory Access Protocol）や、Active Directory（登録商標）などが知られている。さらに、他の認証方法として、Radius(Remote Authentication Dial In User Service)といった方法も知られている。

【０００４】

上記の各認証方法については、同一組織内の一連の情報システムにおいても、各アプリケーション及びデータベースへのアクセス方法に固有の認証方法が設定されている場合が多く、情報システム提供者が複数のアプリケーションやデータをユーザに提供する場合、複数の認証方法を必要とすることがあり、同一ユーザで使用するシステム間に認証方法が混在してしまう。したがって、例えば、ユーザ情報を更新する際に管理者に多くの変更作業を要求する。

【０００５】

そして、一つの情報システムであっても、ユーザの認証のための認証方法やユーザ情報が複数存在すると、管理者はユーザの情報を更新する際に、このユーザが使用許諾されるべきデータベースやアプリケーション（以下「認証対象」）がどれかを特定し、特定した認証対象のデータを更新する必要が生じる。すなわち、ユーザ情報の変更を行うためには、ユーザ情報を管理している全ての認証対象を特定して、この全ての認証対象一つ一つに対して個別にユーザ情報を更新する必要が生じる。

【０００６】

そこで、情報システムが、複数のディレクトリ・サービスなどの認証サービスを用いている場合に、この複数の認証サービスのパスワード情報を同期することにより効率化を図

る方法が知られている（例えば、特許文献１）。
【特許文献１】特開２００３－３３０８８５号公報
【発明の開示】
【発明が解決しようとする課題】
【０００７】
しかしながら、特許文献１の方法では、情報システム内で使用されるアプリケーション（情報システムの中で独立して動作するソフトウェア）が特定データベースにアクセスする際のユーザ認証の管理を行うことはできない。すなわち、情報システムで使用されるアプリケーションにおいても、アプリケーションが行う特定の機能の利用時や、アプリケーションにて使用するデータへのアクセス時に、ユーザの認証が必要な場合がある。このようなケースのアクセス認証では、アプリケーションへのアクセス認証とは別の、独自の認証方法で認証を行う場合がある。例えば、システムで使用されるグループウェア等のアプリケーションでは、アプリケーションが専用のユーザ・データベースを備え、このユーザ・データベースを用いてアプリケーションの特定機能を使用する際に別途の認証を行う。情報システム全体のユーザ情報を統合し、シームレスなユーザ環境を実現するためには、このようなアプリケーションが個別に備える機能で使用される認証までも考慮した統合的な認証システムであることが望ましい。
【０００８】
一方、情報システムとして、ユーザのデータベースが離散的に管理されている場合がある。例えば、大学等の学内システムにおいては、学生の学務データベースと、教員等の人事データベースが個別に管理されることで、情報システムを使用するユーザの情報を一元的に管理することが困難であった。
【０００９】
また、ユーザ認証のための認証システムでは、認証対象へのアクセス権限を判定するためだけの情報のみを保持することが一般的で、その他のユーザ情報、例えば所属・身分・住所・電話番号・メールアドレスなどの個人情報を同時に管理することは行われていない。また、これらの個人情報等のユーザ情報に関しては、所定の権限に基づいて、閲覧、加工等が可能であることが望ましい。また、従来のユーザ情報には、アプリケーション及びデータアクセスの認証サービスに必要な情報以外にも、所属・身分・住所・電話番号・メールアドレスなどの個人情報が存在しているが、従来は、認証サービスに必要なユーザ情報とは別に管理されていた。
【００１０】
加えて、上述のアプリケーションの中には、このアプリケーション毎に必要となるグループに対応する利用者権限を要求するもの（以下、「アプリケーション・ユーザグループ」）が多い。このような場合、それら各々のアプリケーションの要求にしたがって、企業内のメンバーを、登録、変更することは、管理者にとって煩雑な作業となる。また、大学あるいは一般企業などの企業体における組織構造と、これに対するある個人の組織内での所属に基づいた利用権限設定（以下、「利用ポリシ設定」）を行うことも知られているが、中規模以上の組織構造においては、この利用権限設定から外れる例外の設定を必要とする場合が多い。したがって、このような組織内での所属による利用権限設定のみでは、機能として不十分である場合も多い。
【００１１】
このような課題に鑑みて、本発明では、情報システムを使用するユーザの情報を統合的に管理し、この情報システムを使用するユーザの認証及び、利用権限に関する情報を含むユーザ情報の割当てと流通、さらに、閲覧・加工・集計などの２次利用を円滑に行う統合ユーザ管理システム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】
【００１２】
（１）ユーザのユーザ情報及びポリシから構成されるユーザデータを管理し、認証を行う統合ユーザ管理システムであって、

前記ユーザの認証方法が異なる複数の認証サービスに接続され、前記複数の認証サービスのうち認証が必要とされる認証サービスのユーザデータの同期を統合的に行うアカウント統合機能部と、

実行のために前記ユーザの認証を行う認証モジュールを有する少なくとも１つのアプリケーションと、

前記ユーザデータを記録し、記録された前記ユーザデータを前記アカウント統合機能部及び前記認証モジュールに配信し、配信された前記ユーザデータを使用して、前記認証サービス及び前記認証モジュールの少なくとも一方で前記ユーザの認証が行われるように統合的に管理する論理統合機能部とを備え、

前記ポリシが、所属情報と身分情報とにより分類され、

前記ユーザデータが、所属情報及び身分情報による２つの役割セットと、前記アプリケーションごとにそのアプリケーションの使用に関して所定の権限が設定された前記ユーザの集合であるアプリケーション・ユーザグループとから構成される三次元役割セットに関する情報を含む統合ユーザ管理システム。

【００１３】

したがって、（１）の発明によれば、システムを使用するユーザのユーザデータが論理統合機能部に記録され、このユーザデータに基づいて、複数の認証サービスの同期を行うアカウント統合機能部と、認証が必要な複数のアプリケーションに対応した複数の認証モジュールとのデータベースが管理されるため、ユーザの認証を統合的に管理することが可能である。

【００１４】

さらに、（１）の発明によれば、情報システムを使用するユーザデータ（ユーザ情報とポリシ）を統合的に管理するため、この情報システムを使用するユーザの認証を円滑に行うとともに、ユーザに関するユーザ情報（ユーザに関する個人情報等）を管理することが可能となる。したがって、例えば、アプリケーションがユーザ情報（氏名や生年月日、入社日等）を使用する要求がある場合には、統合的に管理している論理統合機能部にユーザ情報の要求を行い、アプリケーションがユーザ情報を取得し、このアプリケーションにおいて、ユーザ情報の閲覧・加工・集計として２次的に利用させることが可能である。

【００１５】

（２）（１）に記載の統合ユーザ管理システムであって、

前記論理統合機能部が、前記ユーザデータが更新された際に、前記アカウント統合機能部と前記認証モジュールに対して、所定のデータ形式でこの更新されたユーザデータを配信する統合ユーザ管理システム。

【００１６】

すなわち、（２）の発明によれば、ユーザデータが更新された際に、アカウント統合機能部と、配信を必要とするアプリケーションに対して、所定のデータ形式でこの更新されたユーザデータを配信する。結果として、この更新されたユーザデータを受信して、アカウント統合機能部の認証サービスのデータベースと複数の認証モジュールのデータベースを更新することで、統合ユーザ管理システム全体では、ユーザの認証情報とユーザ情報が統合的に管理される。

【００１８】

さらに、（１）の発明によれば、人事の所属情報のみならず、身分情報を含めてユーザの認証のポリシを決定することができる。これにより、同じ所属であっても、異なる権限をユーザに付与し、認証を行うことが可能となることに加えて、所属情報、身分情報のみならず、アプリケーション・ユーザグループを含めた三次元役割セットにより、ユーザの認証における権限を決定することができる。

【００１９】

（３）（１）から（２）いずれか記載の統合ユーザ管理システムであって、

前記論理統合機能部が、ユーザの認証に使用しないユーザデータであって、前記アプリケーションのいずれかにおいて使用するユーザ情報を、一元的に管理する統合ユーザ管理

システム。
【００２０】
したがって、（３）の発明によれば、ユーザの認証に使用しないユーザデータのうち、各アプリケーションで使用するユーザ情報を管理することにより、ユーザに関する情報を一元的に管理することが可能である。例えば、ユーザに関する情報（ユーザ情報）として、氏名・住所・電話番号・ユーザ登録番号などの情報は、一般的には、ユーザの認証を行うシステムとは別に管理する情報であるが、（３）の発明では、これらの情報も併せて統合的に管理するため、ユーザ情報を一元的に管理することが可能となる。
【発明の効果】
【００２１】
したがって、本発明によれば、情報システムを使用するユーザの情報とポリシを統合的に管理し、この情報システムを使用するユーザの認証を円滑に行う統合ユーザ管理システムを提供することが可能である。
【発明を実施するための最良の形態】
【００２２】
以下に、本発明の好適な実施形態を図面に基づいて説明する。
【００２３】
＜統合ユーザ管理システム＞
図１に統合ユーザ管理システム１の構成の一例を示した。統合ユーザ管理システム１は、論理統合機能部１０と、アカウント統合機能部２０と、実行管理機能部３０と、アプリケーションＡ～Ｃ６０、６１、６２（認証モジュールＡ～Ｃ４０、４１、４２を含む）と認証サービスＡ～Ｃ５０、５１、５２とから構成される。ここで、アプリケーションＡ～Ｃとは、アプリケーション・プログラムが動作するコンピュータ装置もしくは、複数のコンピュータにより動作するコンピュータ・システムであってよい。アプリケーション・プログラムにて動作するプログラムは、例えば、情報システム内で使用されるグループウェア等である。
【００２４】
統合ユーザ管理システム１は、情報システムのユーザの認証を行う情報（ポリシ）と、ユーザに関する情報（ユーザ情報）とを含むユーザデータを統合的に管理する。統合ユーザ管理システム１は、論理統合機能部１０と、アプリケーションＡ～Ｃ６０、６１、６２（認証モジュールＡ～Ｃ４０、４１、４２を含む）からのみ構成されていてもよく、また、論理統合機能部１０と、アカウント統合機能部２０と、認証サービスＡ～Ｃ５０、５１、５２とからのみ構成されていてもよい。統合ユーザ管理システム１は、組織内の情報システムにおけるユーザ認証及びユーザの情報を管理するため、図１に示す構成要素以外の装置もしくはシステムが、統合認証ユーザ管理システム１に含まれていてもよい。
【００２５】
統合ユーザ管理システム１は、クライアント（図示せず）と接続されており、クライアントは、統合ユーザ管理システム１の任意の構成要素と通信可能である。図３にて、クライアント４７を、アプリケーションＡ６０に接続させるように図示したが、クライアント４７は、アプリケーションＡ６０のみならず、アカウント統合機能部２０、認証サービスＡ～Ｃ５０、５１、５２と通信可能である。
【００２６】
図１に示すように、論理統合機能部１０は、アプリケーションＡ～Ｃ６０、６１、６２と、アカウント統合機能部２０と、実行管理機能部３０と接続され、アカウント統合機能部２０が、認証サービスＡ～Ｃ５０、５１、５２と接続される。これらの接続は専用線であってもよいし、公衆回線であってもよい。また、統合ユーザ管理システム１を構成する構成要素は、それぞれ通信回線ネットワークに接続されインターネット等を介して全ての構成要素が接続されていてもよい。この場合には、ＶＰＮ（Virtual Private Network）等で接続されていてもよい。
【００２７】

さらに、統合ユーザ管理システム１を構成するアカウント統合機能部２０が複数あり、この複数のアカウント統合機能部２０が互いにＶＰＮ等により接続され、論理統合機能部１０からのユーザ情報の送受信を行ってもよい。

【００２８】

＜論理統合機能部＞

論理統合機能部１０は、ユーザ情報とポリシから構成されるユーザデータを管理し、記録し、システム内に存在する全ての認証対象（認証モジュールにて動作するアプリケーションでの認証および認証サービスでの認証）にて動作する認証を統合的に管理する。さらに、論理統合機能部１０は、認証を管理するのと同時に、ユーザに関する情報（例えば、氏名、住所等の個人情報）を管理する。論理統合機能部１０は、通常のコンピュータ装置であってよい。

【００２９】

論理統合機能部１０は、図２に示すように、制御部１１と、データ管理部１３とポリシ管理部１４とを備えた管理部１２と、ユーザデータ部１６を含む論理データベース１５と、アプリケーションＩ／Ｆ（インターフェース）１７と、アカウント統合機能部Ｉ／Ｆ１８と、実行管理機能部Ｉ／Ｆ１９とを備えている。

【００３０】

制御部１１は、論理統合機能部１０の情報を制御する。制御部１１は、通常の中央処理装置（ＣＰＵ）であってもよい。制御部１１は、管理部１２から管理者により入力された情報を処理し、これらの情報を論理データベース１５に記録し、アプリケーションＩ／Ｆ１７、アカウント統合機能部Ｉ／Ｆ１８、実行管理機能部Ｉ／Ｆ１９を介して、認証モジュールＡ～Ｃ４０、４１、４２、アカウント統合機能部２０、実行管理機能部３０と情報の送受信を行う。

【００３１】

管理部１２は、統合ユーザ管理システム１全体の統合管理を行う。管理部１２は、ユーザ情報を管理するデータ管理部１３と、ユーザのポリシを管理するポリシ管理部１４とを含む。データ管理部１３は、キーボード、マウス等の入力装置から、管理者（管理者でなくても、システムを使用するユーザを管理する担当の者、例えば人事部の者、学務部の者でもよい）からユーザ情報の入力を受け、入力された情報を論理データベース１５に記録する。ポリシ管理部１４は、キーボード、マウス等の入力装置から、管理者からポリシに関する入力を受け、入力された情報を論理データベース１５に記録する。

【００３２】

データ管理部１３は、統合ユーザ管理システム１のユーザ情報を管理する者から、ユーザ情報の更新情報の入力を受け付けることが可能であり、入力された更新情報を論理データベース１５のユーザデータ部１６に記録する。

【００３３】

ポリシ管理部１４は、統合ユーザ管理システム１のポリシを管理する者から、ポリシの更新情報の入力を受け付けることが可能であり、入力された更新情報を論理データベース１５に記録する。ここでポリシとは、ユーザの役割（所属や身分等）により、どのアプリケーションもしくは認証サービスに対して、どの程度までデータのアクセスを可能にするか、もしくはアプリケーションや認証サービスの使用そのものを許可するか等の、ユーザがシステムを利用する際の制限を定めた規則である。

【００３４】

論理データベース１５は、ユーザ情報や、このユーザのポリシ（以下、ユーザ情報とポリシとを、「ユーザデータ」とする）を記録したデータベースである。ここでユーザ情報とは、統合ユーザ管理システム１に使用されるアプリケーションおよび認証サービスにて、認証時に必要とされるユーザに関する全ての情報である。例えば、ユーザ名、役割（所属、身分）、アプリケーションにて設定され権限が割当てられるグループ（アプリケーション・ユーザグループ）、パスワード等であってよい。ここでアプリケーション・ユーザグループとは、あるアプリケーションの使用に関して、所定の権限が設定されたユーザの

集合のことである。例えば、アプリケーションＡでのグループ１は、アプリケーションＡを介して所定のデータにアクセスできる権限をもつが、グループ２は権限を持たないため、この所定のデータにアクセスできないといったように、グループが設定される。論理データベース１５には、上述したユーザ情報を記録するユーザデータ部１６を含む。

【００３５】

アプリケーションＩ／Ｆ１７は、認証モジュールＡ～Ｃ４０、４１、４２とのインターフェース部である。ここで、認証モジュールＡ～Ｃ４０、４１、４２は、アプリケーションＡ～Ｃ６０、６１、６２にて、ユーザの認証を行うプログラムが動作する装置である。すなわち、認証モジュールＡ～Ｃ４０、４１、４２は、アプリケーションＡ～Ｃ６０、６１、６２に含まれ、各アプリケーションのためのユーザ認証を行う。

【００３６】

＜アプリケーション＞

アプリケーションＡ～Ｃ６０、６１、６２は、アプリケーション・プログラムを提供するコンピュータ装置により実現される。アプリケーションＡ～Ｃ６０、６１、６２は、クライアント４７からアクセスされ、クライアント４７と認証モジュールＡ～Ｃ４０、４１、４２間での通信によりアプリケーションが制御される（図３参照）。ここで使用されるアプリケーションにおいて、特定のアプリケーションの機能を利用するため、あるいは、このアプリケーションが利用するデータにアクセスするために、アプリケーションを利用するユーザがこれらの機能およびアクセスを許可されているユーザであるかの認証を認証モジュールＡ～Ｃ４０、４１、４２が行う。ここで、アプリケーションＡ～Ｃ６０、６１、６２には、必ずしも認証モジュールＡ～Ｃ４０、４１、４２を備えなくてよい。この場合には、認証サービスＡ～Ｃ５０～５２からユーザデータを受信して、認証を行う。

【００３７】

認証モジュールＡ～Ｃ４０、４１、４２は、アプリケーションＡ～Ｃ６０、６１、６２のユーザの認証を行ない、クライアント４７にアプリケーション機能の使用の許可や、データへのアクセスの許可を行う。認証モジュールＡ～Ｃ４０、４１、４２は、アプリケーションの一部に組み込まれたモジュール（プログラム）を読み込んだコンピュータ装置であってもよい。また、認証モジュールＡ～Ｃ４０、４１、４２は、アプリケーションにデータを渡す前に動作するモジュール（プログラム）であって、アプリケーションに適したフォーマット等にデータを加工するモジュール（例えば、エージェント）を読み込んだコンピュータ装置であってもよい。

【００３８】

したがって、認証モジュールＡ～Ｃ４０、４１、４２は、アプリケーションにおけるユーザの認証のためのポリシをポリシ記録部４６に備える（図３参照）。そして、ポリシの更新がある場合には、管理部１２からの入力を受けて、アプリケーションＩ／Ｆ１７と、論理統合機能部Ｉ／Ｆ４５を介して、認証モジュールＡ～Ｃ４０、４１、４２に更新した情報が配信され、ポリシが更新される。

【００３９】

次に、アカウント統合機能部Ｉ／Ｆ１８は、アカウント統合機能部２０と通信を行うためのインターフェースである。

【００４０】

＜アカウント統合機能部＞

アカウント統合機能部２０は、統合ユーザ管理システム１の認証が必要な複数の認証サービスＡ～Ｃ５０、５１、５２のユーザデータの同期を統合的に行う。アカウント統合機能部２０は、認証サービスＡ～Ｃ５０、５１、５２が提供する、ＬＤＡＰ、アクティブディレクトリ、Ｒａｄｉｕｓ（Remote Authentication Dial In User Service）等の個々の認証方法に対して、統合的に認証を行う。ここで、認証サービスＡ～Ｃ５０、５１、５２とは、所定の認証方法により認証を実現するサーバ等の装置である。アカウント統合機能部２０は、ユーザデータが更新された際に、個々の認証サービスの認証方法におけるユーザデータを更新する。アカウント統合機能部２０は、通常のコンピュータであって

よく、制御部２１、論理統合機能部Ｉ／Ｆ２２と、管理部２３と、アカウントデータベース２４と、認証サービスＩ／Ｆ２５とを備えてよい（図４参照）。

【００４１】

制御部２１は、アカウント統合機能部２０の情報を制御する。制御部２１は、通常の中央処理装置（ＣＰＵ）であってもよい。管理部２３は、認証サービスＡ～Ｃ５０、５１、５２の認証のためのデータの管理を行う。管理部２３は、キーボード、マウス等の入力装置から、管理者（管理者でなくても、システムを使用するユーザを管理する担当の者、例えば人事部の者、学務部の者でもよい）からユーザ情報やポリシの入力を受け、入力された情報をアカウントデータベース２４に記録する。管理部２３から入力されたユーザ情報やポリシの更新情報は、論理統合機能部Ｉ／Ｆ２２、アカウント統合機能部Ｉ／Ｆ１８を介して、論理統合機能部１０のユーザデータ部１６に記録されてもよい。認証サービスＩ／Ｆ２５は、認証サービスＡ～Ｃ５０、５１、５２との通信のためのインターフェースである。実行管理機能部Ｉ／Ｆ１９は、実行管理機能部３０との接続を行うインターフェースである。

【００４２】

＜認証サービス＞

認証サービスＡ～Ｃ５０、５１、５２は、上述の認証方法を実現するコンピュータであり、ディレクトリ・サービスにより認証される装置であってよい。認証サービスＡ～Ｃ５０、５１、５２には、この認証サービスを利用する複数のクライアントが接続され、接続された各クライアントを認証する。ここで、クライアント４７にて動作するアプリケーションＡ～Ｃ６０、６１、６２の認証を、認証サービスが実行してもよい。認証サービスＡ～Ｃ５０、５１、５２は、アプリケーションとは個別に、独立してユーザ認証を行う点で、認証モジュールＡ～Ｃ４０、４１、４２と相異する。

【００４３】

＜実行管理機能部＞

実行管理機能部３０は、論理統合機能部１０により実行した処理に関するログを記録する。ここで記録するログとは、いつ、どの認証モジュールＡ～Ｃ４０、４１、４２が、何のデータを、どの対象に、何を実行したのかを記録したデータである。また、実行管理機能部３０は、論理統合機能部１０による統合管理の一部の機能を所定の時刻に実行する機能を備えてよい。例えば、データの流入が少ない時間帯に、ユーザデータの更新データをアカウント統合機能部２０と、認証モジュールＡ～Ｃ４０、４１、４２に配信するといったように、実行管理機能部３０にスケジューリングし、実行管理機能部３０が、これを所定の時刻に実行する。

【００４４】

＜ポリシについて＞

次に、ユーザのポリシについて説明する。

【表１】

名前	役割１（身分）	役割２（所属）	アプリケーションAの権限グループ	アプリケーションBの権限グループ	アプリケーションCの権限グループ
山田太郎	教員	A学部	研究者	A学部ユーザ	A学部教職員
山本武	事務員	大学本部	事務員	－	管理者
山口大輔	管理職	A学部事務	管理者	管理者	－
鈴木健一	学生	A学部	学生	A学部ユーザ	－

【００４５】

表１のように、一般的なユーザデータの管理方法では、役割１（例えば、身分）、役割２（例えば、所属）により分類される。この役割１、役割２を二次元役割セットとして、この役割１と役割２の組み合わせにより各ユーザが認証される。したがって、事前にユーザごとに、二次元役割セットが登録される。そして、二次元役割セットに加えて、アプリ

ケーションＡ～Ｃの権限がユーザごとに定められる。論理統合機能部１０は、ユーザデータが更新された際には、適宜、このポリシの権限グループが割当てられているアプリケーションに対して、更新データを送信する。

【００４６】

例えば、表１に挙げられているユーザのポリシが更新された際には、更新されたユーザが、「山田太郎」、「山本武」、「山口大輔」、「鈴木健一」のいずれかであっても、アプリケーションＡが動作する認証モジュールＡ４０に、更新したポリシが、論理統合機能部１０から配信される。

【００４７】

表１のように、各ユーザに対してアプリケーションの権限グループ（アプリケーション・ユーザグループ）が設定されていてもよいが、二次元役割セットとアプリケーションの権限グループが対応づけられていてもよい。

【００４８】

表２、表３のように、ポリシは、身分、所属といった２つの役割のセットに関する情報に加えて、所定のアプリケーションにおいて、ユーザが所属するグループ（アプリケーション・ユーザグループ）に関する情報を含むことで三次元的な役割のセットにより構成される。これらの表のように、論理統合機能部１０がアプリケーションの種類に基づいて異なる権限グループを一元的に管理する。

【表２】

名前	アプリケーションAの権限グループ	アプリケーションBの権限グループ	アプリケーションCの権限グループ
山田太郎	研究者	A学部ユーザ	A学部教職員
山本武	事務員	－	管理者
山口大輔	管理者	管理者	－
鈴木健一	学生	A学部ユーザ	－

【表３】

役割1（身分）	役割2（所属）	アプリケーションAの権限グループ
教員	A学部	研究者
事務員	大学本部	事務員
管理職	A学部事務	管理者
学生	A学部	学生

【００４９】

ここで、役割とアプリケーション・ユーザグループの関係づけは、表３を用いて行われる。例えば、「山田太郎」のアプリケーションＡの権限グループが不明である場合に、「山田太郎」の身分と所属に基づけば、表３のデータに基づいて、アプリケーションＡの権限グループが特定できる。例えば、ユーザ「山田太郎」の身分が「教員」で所属が「Ａ学部」である場合には、表３から、アプリケーションＡの権限グループは、「研究者」であると特定することができる。このように、アプリケーション・ユーザグループを、個々のユーザに対して関係づけを行うのではなく、役割に対して関係づけを行うことで、データ整合の手間を省くことが可能であり、かつ柔軟なデータベースの構築を行うことが可能である。

【００５０】

＜ポリシに基づく、ユーザ情報のアクセスに関する制限について＞

次に、表１～３に基づいて、ユーザ情報のアクセスに関する制限について説明する。ここで、ユーザ情報とは、情報システムを使用するユーザに関する情報であり、例えば、個

人情報である。表２によれば、アプリケーションＡは、全てのユーザで利用可能なアプリケーションであるが、アプリケーションＡ内の情報アクセス権（ユーザ情報のアクセス権であって、ユーザ情報の閲覧・加工・集計などの２次利用に関する権利）などのユーザ使用権限については、アプリケーション内の権限グループ（アプリケーション・ユーザグループ）あるいは、二次元役割セットにより決定されてよい。加えて、この二次元役割セットに、アプリケーションの権限グループを追加したものを三次元役割セットとして、三次元役割セットに基づいて、ユーザ情報のアクセスに関する制限が決定されてもよい。

【００５１】

アプリケーションＡは、「山田太郎」、「山本武」、「山口大輔」、「鈴木健一」のいずれについてもアクセス可能であるが、三次元役割セットに基づいて、アクセス可能なユーザ情報が制限される。アプリケーションＡにおいて、「山口大輔」は「管理者」の権限であるため、アプリケーションＡのユーザ情報のアクセス権の制限がないが、「鈴木健一」は、「学生」の権限であるため、自分のユーザ情報以外はアクセスできないように制限されてよい。

【００５２】

アプリケーションＡでのユーザ情報のアクセス権限は、結果としては、アプリケーションＡのアプリケーション・ユーザグループにより決定されるが、役割１、役割２により、アプリケーション・ユーザグループが決定されるため、アプリケーションＡでのユーザ情報のアクセス権限は、三次元役割セットに基づいて決定される。

【００５３】

また、三次元役割セットを構成することで、例えば、ユーザ「山田太郎」は、アプリケーションＡ～Ｃまでグループが割り当てられているため、山田太郎は、アプリケーションＡ～Ｃ全てを利用することが可能であると判断できる。

【００５４】

表３によれば、「山田太郎」は、役割１が「教員」であり、役割２が「Ａ学部」であるため、アプリケーションＡの権限グループが「研究者」と決定し、アプリケーションＡを利用することが可能である。しかし、ユーザ「山本武」は、役割１が「事務員」であり、役割２が「大学本部」である。表３のデータによれば、この役割では、アプリケーションＢは利用できない。したがって、ユーザ「山本武」のユーザ情報が更新されても、論理統合機能部１０から認証モジュールＢ４１に更新情報は配信されない。

【００５５】

表１、もしくは表２、表３のような、ユーザ情報のデータが、ユーザデータ部１６に記録される。ユーザ情報のデータは、ポリシの認証では使用されないが、アプリケーションで必要なユーザ情報（ユーザの氏名、生年月日等の個人情報など）が含まれていてもよい。例えば、ユーザ情報としては、アプリケーションＡが受験生管理アプリケーションであれば「受験番号」、「受験年度」等の情報であってよい。

【００５６】

また、ポリシには、例外ルールが付加されていてもよい。原則としては、表１のように、役割１、役割２に基づいて、アプリケーションのグループが決定され、これに基づいてユーザの権限が付与される。しかし例外的に、役割１、役割２に基づくことなく、ユーザの権限が付与されるユーザがあってもよい。ここで、例外ルールにおいては、所定のグループがアプリケーションＡを利用可能であるとポリシを設定することを原則として、例外的に、あるユーザに対してアプリケーションＡを利用不可能と設定してもよい。

【００５７】

＜ユーザデータの配信について＞

次に、図５に基づいて、論理統合機能部１０に対して、ユーザデータの入力があり、これを認証対象へ配信する処理について説明する。

【００５８】

論理統合機能部１０の管理部１２が、ユーザデータの入力を受ける。論理統合機能部１０の管理部１２は、ユーザデータの変更を受信する（ステップＳ０１）。この変更に基づ

いて、論理データベース１５を更新する（ステップＳ０２）。そして、制御部１１が、このユーザデータの更新がどの認証対象に更新が必要かを判断し（ステップＳ０３）、更新が必要となる認証対象へ更新データを配信する（ステップＳ０４）。すなわち、上述のように、更新のあったユーザの役割１、役割２から、使用されているアプリケーションを判断し、どのアプリケーション内の認証モジュールへ、更新のあったユーザデータを配信するか判断する。加えて、更新のあったユーザが、所定の認証サービスにて認証されるユーザであれば、ユーザデータをアカウント統合機能部２０に配信し、アカウント統合機能部２０のアカウントデータベース２４を更新してもよい。

【００５９】

＜アプリケーションのユーザ認証＞

次に、ユーザが、アプリケーションＡ～Ｄ６０～６３により認証される際のフローについて、図６に基づいて説明する。

【００６０】

図６に例示したように、クライアント４７を操作するユーザが認証される方法が、４つある。第１に、クライアント４７が、アプリケーションＤ６３に認証される場合は、アプリケーションＤ６３は、認証モジュールを備えユーザデータ７３を保持しているため、認証サービスＡ、Ｂ５０、５１を必要としないで、ユーザの認証を完了する（ステップＳ１０）。

【００６１】

第２に、クライアント４７が、アプリケーションＥ６４に認証される場合は、アプリケーションＥ６４が、認証モジュールを備えないため、認証サービスＡ５０にアクセスして、ユーザデータを取得して、認証を完了する（ステップＳ２０、２１）。

【００６２】

第３に、クライアント４７が、アプリケーションＦ６５に認証される場合は、最初にクライアント４７が、認証サービスＢ５１にアクセスして、ユーザデータ７１を参照して、認証を完了した後に、アプリケーションＦ６５にアクセスする（ステップＳ３０、Ｓ３１）。この場合には、アプリケーションＦ６５が、認証モジュールを備えなくとも、認証を行うことができる。

【００６３】

第４に、クライアント４７が、アプリケーションＧ６６に認証される場合は、最初にクライアント４７が、認証サービスＢ５１にアクセスして、ユーザデータ７１を参照して、認証を完了した後に、アプリケーションＧ６６にアクセスする（ステップＳ４０、Ｓ４１）。この場合には、アプリケーションＧ６６が、認証モジュールを備えており、ユーザデータ７６を保持しているため、ユーザの認証においては、適宜、ユーザデータ７１あるいはユーザデータ７６のいずれかのデータが使用される。

【００６４】

さらに、論理統合機能部１０とアカウント統合機能部２０との間では、ユーザデータの同期において、コマンドにより同期が行われてもよいし、データにより同期が行われる方法であってもよい。すなわち、一つのデータを含んだコマンドを送受信することで同期が行われる方法であってもよいし、複数のデータを含んだ一つのコマンドを送受信することで同期が行われてもよい。

【００６５】

統合ユーザ管理システム１内でのユーザデータの送受信が、ＦＴＰ（File Transfer Protocol）、ＨＴＴＰ(HyperText Transfer Protocol)、ＸＭＬ（eXtensible Markup Language）、ＣＯＲＢＡ（Common Object Request Broker Architecture）、ＬＤＡＰ、ＳＭＴＰ（Simple Mail Transfer Protocol）、Ｆｉｌｅ Ｉ／Ｏ、ＪＤＢＣ（Java DataBase Connectivity）ＯＤＢＣ（Open Database Connectivity）、ＳＯＡＰ（Simple Object Access Protocol）、ＥＪＢ（Enterprise Java Beans）の方式、もしくはプロトコルのいずれかにより行われてよい。

【００６６】

本発明の好適な実施例として、大学等の学内システムに統合ユーザ管理システムが適用されてもよい。学内のアカウントシステムでは、学生の学務データベースと、教員等の人事データベースが個別に管理されることで、情報システムを使用するユーザデータを一元的に管理することが困難であった。しかし、本発明によれば、学務データベースと人事データベースとを論理統合機能部１０に備え、これらのデータベースの更新作業を、論理統合機能部１０にて実行し、このデータベースに対応したアプリケーションのデータや、認証サービスのデータを更新することにより、ユーザの情報を一元的に管理することが可能である。

【００６７】

このような実施形態を実現する統合ユーザ管理システムを、コンピュータやサーバにて実行するためのプログラムにより実現することができる。このプログラムのための記録媒体としては、光学記録媒体、テープ媒体、半導体メモリ等が挙げられる。また、専用通信ネットワークやインターネットに接続されたサーバ・システムに設けられたハードディスク又はＲＡＭ等の記録装置を記録媒体として使用し、ネットワークを介してプログラムを提供してもよい。さらに、この統合ユーザ管理システムを実現する方法、もしくはこの方法を実行するプログラムについても、同様に適用することが可能である。

【００６８】

以上により、本発明では、以下の統合ユーザ管理システムを提供する。

【００６９】

（１）ユーザのユーザ情報及びポリシから構成されるユーザデータを管理し、認証を行う統合ユーザ管理システムであって、

前記ユーザの認証方法が異なる複数の認証サービスに接続され、前記複数の認証サービスのうち認証が必要とされる認証サービスのユーザデータの同期を統合的に行うアカウント統合機能部と、

実行のために前記ユーザの認証を行う認証モジュールを有する少なくとも１つのアプリケーションと、

前記ユーザデータを記録し、記録された前記ユーザデータを前記アカウント統合機能部及び前記認証モジュールに配信し、配信された前記ユーザデータを使用して、前記認証サービス及び前記認証モジュールの少なくとも一方で前記ユーザの認証が行われるように統合的に管理する論理統合機能部と、を備えた統合ユーザ管理システム。

【００７０】

したがって、（１）の発明によれば、システムを使用するユーザのユーザデータが論理統合機能部に記録され、このユーザデータに基づいて、複数の認証サービスの同期を行うアカウント統合機能部と、認証が必要な複数のアプリケーションに対応した複数の認証モジュールとのデータベースが管理されるため、ユーザの認証を統合的に管理することが可能である。

【００７１】

さらに、（１）の発明によれば、情報システムを使用するユーザデータ（ユーザ情報とポリシ）を統合的に管理するため、この情報システムを使用するユーザの認証を円滑に行うとともに、ユーザに関するユーザ情報（ユーザに関する個人情報等）を管理することが可能となる。したがって、例えば、アプリケーションがユーザ情報（氏名や生年月日、入社日等）を使用する要求がある場合には、統合的に管理している論理統合機能部にユーザ情報の要求を行い、アプリケーションがユーザ情報を取得し、このアプリケーションにおいて、ユーザ情報の閲覧・加工・集計として２次的に利用させることが可能である。

【００７２】

（２）（１）に記載の統合ユーザ管理システムであって、

前記論理統合機能部が、前記ユーザデータが更新された際に、前記アカウント統合機能部と前記認証モジュールに対して、所定のデータ形式でこの更新されたユーザデータを配信する統合ユーザ管理システム。

【００７３】

すなわち、（２）の発明によれば、ユーザデータが更新された際に、アカウント統合機能部と、配信を必要とするアプリケーションに対して、所定のデータ形式でこの更新されたユーザデータを配信する。結果として、この更新されたユーザデータを受信して、アカウント統合機能部の認証サービスのデータベースと複数の認証モジュールのデータベースを更新することで、統合ユーザ管理システム全体では、ユーザの認証情報とユーザ情報が統合的に管理される。

【００７４】

（３）　（１）又は（２）に記載の統合ユーザ管理システムであって、

前記論理統合機能部が、前記ポリシが、所属情報と身分情報とにより分類されている統合ユーザ管理システム。

【００７５】

したがって、（３）の発明によれば、人事の所属情報のみならず、身分情報を含めてユーザの認証のポリシを決定することができる。これにより、同じ所属であっても、異なる権限をユーザに付与し、認証を行うことが可能となる。

【００７６】

（４）（３）に記載の統合ユーザ管理システムであって、

前記ユーザデータが、所属情報及び身分情報による２つの役割セットと、前記アプリケーションごとにそのアプリケーションの使用に関して所定の権限が設定された前記ユーザの集合であるアプリケーション・ユーザグループとから構成される三次元役割セットに関する情報を含む統合ユーザ管理システム。

【００７７】

したがって、（４）の発明によれば、所属情報、身分情報のみならず、アプリケーション・ユーザグループを含めた三次元役割セットにより、ユーザの認証における権限を決定することができる。

【００７８】

（５）（１）から（４）いずれか記載の統合ユーザ管理システムであって、

前記論理統合機能部が、前記情報システムを使用するユーザの認証に使用しないユーザデータであって、前記アプリケーションのいずれかにおいて使用するユーザ情報を、一元的に管理する統合ユーザ管理システム。

【００７９】

したがって、（５）の発明によれば、ユーザの認証に使用しないユーザデータのうち、各アプリケーションで使用するユーザ情報を管理することにより、ユーザに関する情報を一元的に管理することが可能である。例えば、ユーザに関する情報（ユーザ情報）として、氏名・住所・電話番号・ユーザ登録番号などの情報は、一般的には、ユーザの認証を行うシステムとは別に管理する情報であるが、（５）の発明では、これらの情報も併せて統合的に管理するため、ユーザ情報を一元的に管理することが可能となる。

【００８０】

（６）　（１）から（５）に記載の統合ユーザ管理システムであって、

前記論理統合機能部が、前記ポリシに基づいて、前記アプリケーションに配信するユーザ情報の２次利用の範囲を制限する統合ユーザ管理システム。

【００８１】

（６）の発明によれば、ユーザに関する情報であるユーザ情報の利用範囲を、論理統合機能部に記録したポリシに基づいて制限する。したがって、ユーザ認証にて用いられるポリシを、ユーザ情報を制限するポリシとして使用させることが可能である。ここで２次利用とは、ユーザ情報を使用するアプリケーションにおいて、このユーザ情報を２次的に使用することであり、例えば、ユーザ情報をアプリケーションにおいて、閲覧、修正を行うことであってよい。

【００８２】

（７）　（６）に記載の統合ユーザ管理システムであって、

前記論理統合機能部が、前記ユーザ情報を配信する前記アプリケーション及び前記ポリシにより、２次利用の範囲を制限し、この制限することをポリシとして記録する統合ユーザ管理システム。

【００８３】

したがって、（７）の発明によれば、（６）の発明に加えて、さらに制限した２次利用の範囲をポリシに記録する。ここで、記録されるポリシは、通常、ユーザ認証にて使用されるポリシであってよい。この場合には、ユーザ認証されるポリシと、ユーザ情報が管理されるポリシとを併せて管理することが可能である。

【００８４】

（８）　（１）から（７）いずれか記載の統合ユーザ管理システムであって、

前記論理統合機能部が、ユーザからのユーザデータの変更に応答して、前記ユーザデータの変更を更新する必要がある前記アカウント統合機能部、前記アプリケーションのいずれかに配信する統合ユーザ管理システム。

【００８５】

（９）　（１）から（５）いずれか記載の統合ユーザ管理システムであって、

前記論理統合機能部による統合管理のログを記録する実行管理機能部を備えた統合ユーザ管理システム。

【００８６】

したがって、（９）の発明によれば、ユーザ情報の管理が行われたことを、ログとして記録するため、例えば、管理の操作を、いつ、誰が、何をしたかを履歴として記録して確認することができる。

【００８７】

（１０）　（１）から（９）いずれか記載の統合ユーザ管理システムであって、

前記論理統合機能部による統合管理を所定の時刻に実行する実行管理機能部を備えた統合ユーザ管理システム。

【００８８】

したがって、（１０）の発明によれば、統合管理を所定の時刻に実行させることができるため、統合管理の操作に対してスケジューリングを行うことができる。

【００８９】

（１１）　（１）から（１０）いずれか記載の統合ユーザ管理システムであって、

前記論理統合機能部、前記アカウント統合機能部、前記アプリケーション、前記認証サービス間の、データの送受信が、ＦＴＰ、ＨＴＴＰ、ＸＭＬ、ＣＯＲＢＡ、ＬＤＡＰ、ＳＭＴＰの方式のいずれかにより行われる統合ユーザ管理システム。

【００９０】

したがって、（１１）の発明によれば、所定のプロトコルや方式によって、通信もしくは認証が行われる場合に、このようなプロトコルや方式に対応して統合管理をすることができる。

【００９１】

（１２）　（１）から（１１）いずれか記載の統合ユーザ管理システムであって、

前記認証サービスが、ディレクトリ・サービスにより認証される統合ユーザ管理システム。

【００９２】

（１３）　（１）から（１２）いずれか記載の統合ユーザ管理システムであって、

前記システムが、学内の情報システムである統合ユーザ管理システム。

【００９３】

したがって、（１３）の発明によれば、ユーザデータが教職員と学生とで複雑になる傾向がある学内の情報システムに対して適用された統合ユーザ管理システムを提供することができる。

【００９４】

以上、本発明の実施形態を説明したが、具体例を例示したに過ぎず、特に本発明を限定

しない。また、本発明の実施形態に記載された効果は、本発明から生じる最も好適な効果を列挙したに過ぎず、本発明による効果は、本発明の実施形態に記載された効果に限定されない。

【図面の簡単な説明】

【００９５】

【図１】本発明の実施例である統合ユーザ管理システムの機能ブロック図である。

【図２】本発明の実施例である論理統合機能部の構成ブロック図である。

【図３】本発明の実施例である認証モジュールの構成ブロック図である。

【図４】本発明の実施例であるアカウント統合機能部の機能ブロック図である。

【図５】ユーザデータの更新があった際のフローチャートを示す図である。

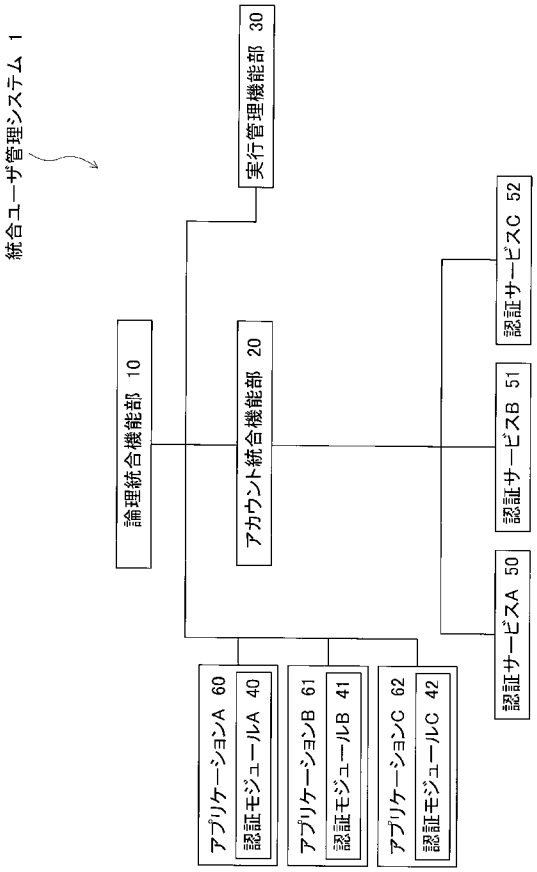
【図６】ユーザがアプリケーションを利用する際のユーザ認証を説明する図である。

【符号の説明】

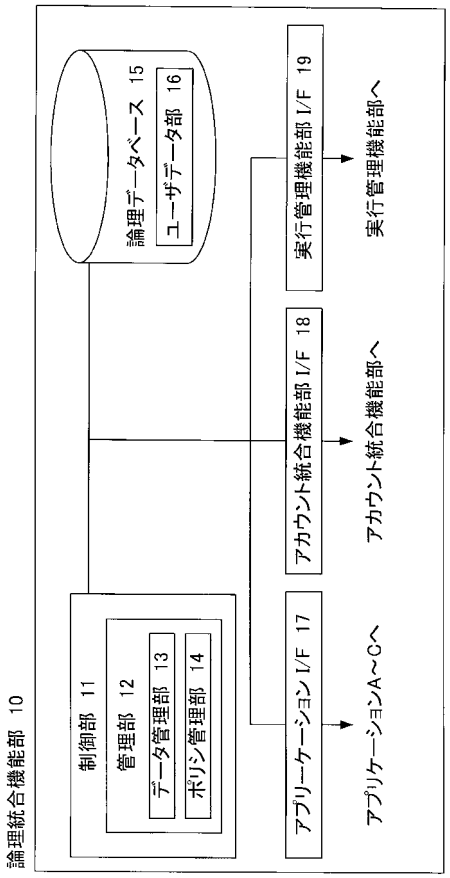
【００９６】

１　統合ユーザ管理システム
１０　論理統合機能部
１１　制御部
１２　管理部
１３　データ管理部
１４　ポリシ管理部
１５　論理データベース
１６　ユーザデータ部
１７　アプリケーションＩ／Ｆ
１８　アカウント統合機能部Ｉ／Ｆ
１９　実行管理機能部Ｉ／Ｆ
２０　アカウント統合機能部
２１　制御部
２２　論理統合機能部Ｉ／Ｆ
２３　管理部
２４　アカウントデータベース
２５　認証サービスＩ／Ｆ
３０　実行管理機能部
４０　認証モジュールＡ
４１　認証モジュールＢ
４２　認証モジュールＣ
４５　論理統合機能部Ｉ／Ｆ
４６　ポリシ記録部
４７　クライアント
６０　アプリケーションＡ
６１　アプリケーションＢ
６２　アプリケーションＣ
６３　アプリケーションＤ
６４　アプリケーションＥ
６５　アプリケーションＦ
６６　アプリケーションＧ
７０，７１，７３，７６　ユーザデータ

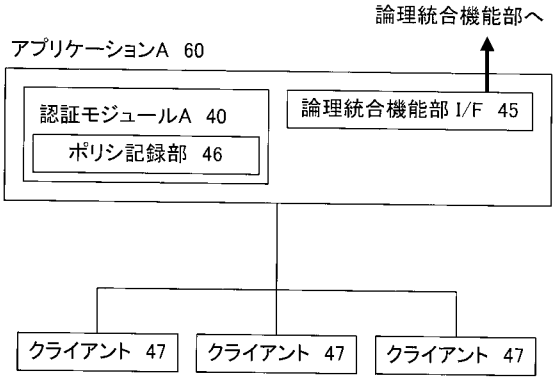
【図１】


統合ユーザ管理システム 1
実行管理機能部 30
論理統合機能部 10
アカウント統合機能部 20
認証サービスC 52
認証サービスB 51
認証サービスA 50
アプリケーションA 60
認証モジュールA 40
アプリケーションB 61
認証モジュールB 41
アプリケーションC 62
認証モジュールC 42

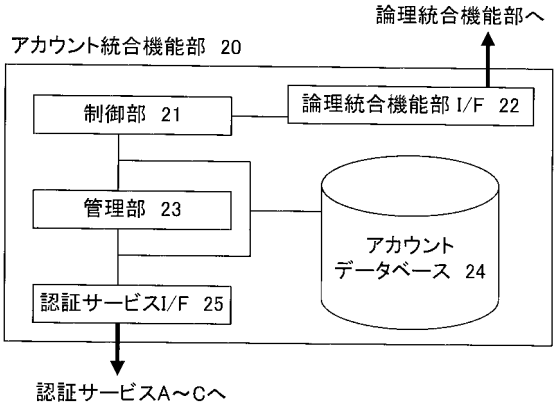
【図２】


論理統合機能部 10
制御部 11
管理部 12
データ管理部 13
ポリシ管理部 14
論理データベース 15
ユーザデータ部 16
アプリケーション I/F 17
アカウント統合機能部 I/F 18
実行管理機能部 I/F 19
アプリケーションA～Cへ
アカウント統合機能部へ
実行管理機能部へ

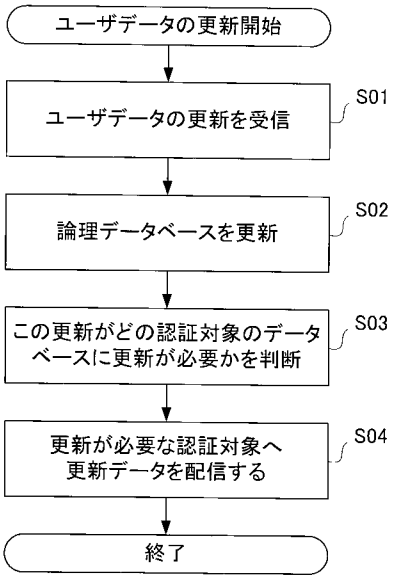
【図３】


論理統合機能部へ
アプリケーションA 60
認証モジュールA 40
ポリシ記録部 46
論理統合機能部 I/F 45
クライアント 47
クライアント 47
クライアント 47

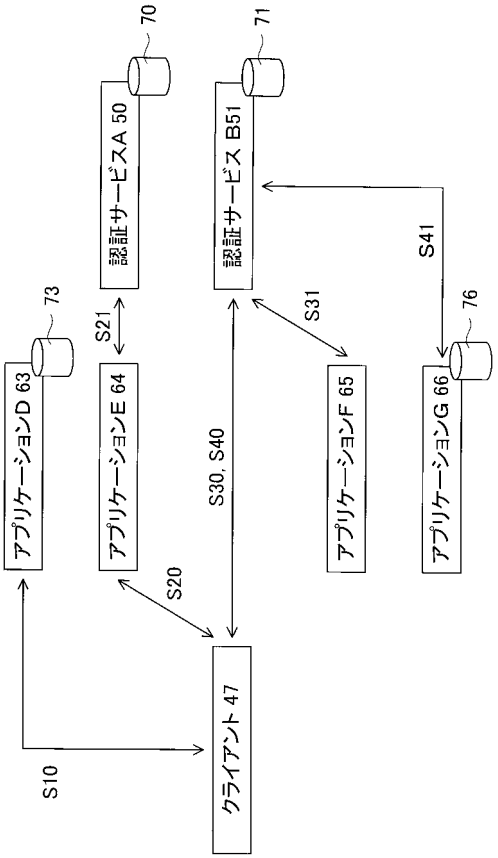
【図４】


論理統合機能部へ
アカウント統合機能部 20
制御部 21
論理統合機能部 I/F 22
管理部 23
アカウント
データベース 24
認証サービスI/F 25
認証サービスA～Cへ

【図５】


ユーザデータの更新開始
ユーザデータの更新を受信
S01
論理データベースを更新
S02
この更新がどの認証対象のデータベースに更新が必要かを判断
S03
更新が必要な認証対象へ更新データを配信する
S04
終了

【図６】


70
認証サービスA 50
71
認証サービス B51
S41
73
S21
S31
76
アプリケーションD 63
アプリケーションE 64
S30, S40
アプリケーションF 65
アプリケーションG 66
S20
クライアント 47
S10

フロントページの続き

(56)参考文献 特開２００５－０５６３９３（ＪＰ，Ａ）
国際公開第２００５／０４８５２６（WO，Ａ１）
特開２００３－０４４４４０（ＪＰ，Ａ）
特開２００３－３３０８８５（ＪＰ，Ａ）
特開２００２－３５８１３５（ＪＰ，Ａ）
特開２００１－００５７２７（ＪＰ，Ａ）
特開２００５－０２５４２７（ＪＰ，Ａ）
特開平０６－１０３２３６（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／２０