

(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2007-94522

(P2007-94522A)

(43) 公開日 平成19年4月12日(2007.4.12)

(51) Int. Cl. F I テーマコード (参考)  
**G06F 21/20 (2006.01)** G06F 15/00 330D 5B285

審査請求 未請求 請求項の数 4 O L (全 17 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)

(特許庁注：以下のものは登録商標)  
 1. J A V A

(71) 出願人 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 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  
 Fターム(参考) 5B285 AA01 BA10 BA11 CA02 CA03  
 CA06 CA12 CB62 CB73

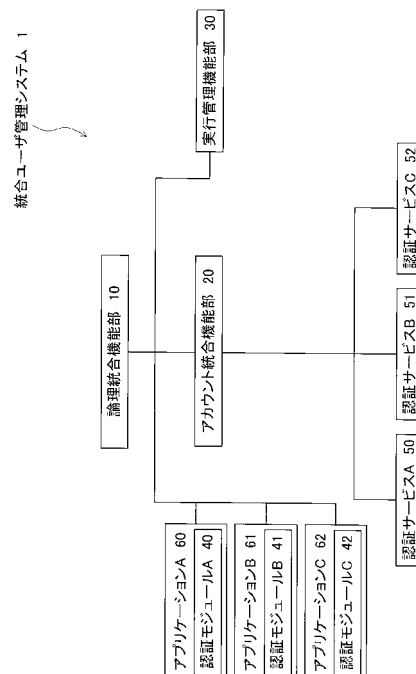
(54) 【発明の名称】 統合ユーザ管理システム

(57) 【要約】

【課題】 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。

【解決手段】 情報システムを使用するユーザ情報を管理し、認証を行う統合ユーザ管理システムであって、認証が必要な認証サービスの同期を行うアカウント統合機能部と、アプリケーションの認証を行う認証モジュールと、ユーザ情報及びポリシー(ユーザデータ)を記録し、ユーザ情報をアプリケーションのいずれかに配信し、ユーザデータを使用して、アカウント統合機能部と認証モジュールとを連携させて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。

【選択図】 図1



**【特許請求の範囲】****【請求項 1】**

情報システムを使用するユーザのユーザ情報を管理し、認証を行う統合ユーザ管理システムであって、

認証が必要な認証サービスの同期を行うアカウント統合機能部と、

アプリケーションの認証を行う認証モジュールと、

前記ユーザ情報及びポリシー（ユーザデータ）を記録し、前記ユーザ情報を前記アプリケーションのいずれかに配信し、前記ユーザデータを使用して、前記アカウント統合機能部と前記認証モジュールとを連携させて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。

10

**【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統合ユーザ管理システム。

**【請求項 3】**

請求項 1 又は 2 に記載の統合ユーザ管理システムであって、

前記ポリシーが、所属情報と身分情報とにより分類され、

前記論理統合機能部が記録するユーザデータが、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における前記ユーザが属するグループ（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み、

20

前記論理統合機能部が、前記三次元役割セットに関する情報を含むユーザデータを、前記アカウント統合機能部、前記認証モジュール、前記アプリケーションに配信する統合ユーザ管理システム。

**【請求項 4】**

請求項 1 から 3 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、統合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】**

30

**【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、かつポリシー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、ユーザ毎にポリシーを設定し、ポリシー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。

40

**【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

50

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ある。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ある。

10

【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)。

20

【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す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。

30

【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。

40

【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と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。

50

## 【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な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、「利用ポリシー設定」）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。

10

## 【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) 情報システムを使用するユーザのユーザ情報を管理し、認証を行う統合ユーザ管理システムであって、

認証が必要な認証サービスの同期を行うアカウント統合機能部と、

20

アプリケーションの認証を行う認証モジュールと、

前記ユーザ情報及びポリシー（この双方を「ユーザデータ」とする）を記録（統合的に管理）し、前記ユーザ情報を前記アプリケーションのいずれかに配信し、前記ユーザデータを使用して、前記アカウント統合機能部と前記認証モジュールとを連携させて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。

## 【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。

30

## 【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ー）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】

40

(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

50

統合的に管理される。

【0017】

(3) (1)又は(2)に記載の統合ユーザ管理システムであって、

前記ポリシーが、所属情報と身分情報とにより分類され、

前記論理統合機能部が記録するユーザデータが、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における前記ユーザが属するグループ(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み、

前記論理統合機能部が、前記三次元役割セットに関する情報を含むユーザデータを、前記アカウント統合機能部、前記認証モジュール、前記アプリケーションに配信する統合ユーザ管理システム。

10

【0018】

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ー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】

(4) (1)から(3)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、統合的に管理する統合ユーザ管理システム。

20

【0020】

したがって、(4)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、(4)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ーを統合的に管理し、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。

30

【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。

40

【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(ポリシー)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

50

( 認証モジュール A ~ C 4 0、4 1、4 2 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 1 0 と、アカウント統合機能部 2 0 と、認証サービス A ~ C 5 0、5 1、5 2 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。

**【 0 0 2 5 】**

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 4 7 を、アプリケーション A 6 0 に接続させるように図示したが、クライアント 4 7 は、アプリケーション A 6 0 のみならず、アカウント統合機能部 2 0、認証サービス A ~ C 5 0、5 1、5 2 と通信可能である。

10

**【 0 0 2 6 】**

図 1 に示すように、論理統合機能部 1 0 は、アプリケーション A ~ C 6 0、6 1、6 2 と、アカウント統合機能部 2 0 と、実行管理機能部 3 0 と接続され、アカウント統合機能部 2 0 が、認証サービス A ~ C 5 0、5 1、5 2 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、V P N ( Virtual Private Network ) 等で接続されていてもよい。

**【 0 0 2 7 】**

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 2 0 が複数あり、この複数のアカウント統合機能部 2 0 が互いに V P N 等により接続され、論理統合機能部 1 0 からのユーザ情報の送受信を行ってもよい。

20

**【 0 0 2 8 】****< 論理統合機能部 >**

論理統合機能部 1 0 は、ユーザ情報とポリシー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 1 0 は、認証を管理すると同時に、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 1 0 は、通常のコンピュータ装置

30

**【 0 0 2 9 】**

論理統合機能部 1 0 は、図 2 に示すように、制御部 1 1 と、データ管理部 1 3 とポリシー管理部 1 4 とを備えた管理部 1 2 と、ユーザデータ部 1 6 を含む論理データベース 1 5 と、アプリケーション I / F ( インターフェース ) 1 7 と、アカウント統合機能部 I / F 1 8 と、実行管理機能部 I / F 1 9 とを備えている。

**【 0 0 3 0 】**

制御部 1 1 は、論理統合機能部 1 0 の情報を制御する。制御部 1 1 は、通常の中央処理装置 ( C P U ) であってもよい。制御部 1 1 は、管理部 1 2 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 1 5 に記録し、アプリケーション I / F 1 7、アカウント統合機能部 I / F 1 8、実行管理機能部 I / F 1 9 を介して、認証モジュール A ~ C 4 0、4 1、4 2、アカウント統合機能部 2 0、実行管理機能部 3 0 と情報の送受信を行う。

40

**【 0 0 3 1 】**

管理部 1 2 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 1 2 は、ユーザ情報を管理するデータ管理部 1 3 と、ユーザのポリシーを管理するポリシー管理部 1 4 とを含む。データ管理部 1 3 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 1 5 に記録する。ポリシー管理部 1 4 は、キーボード、マウス等の入力装置から、管理者からポリシーに

50

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】

ポリシー管理部 14 は、統合ユーザ管理システム 1 のポリシーを管理する者から、ポリシー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。ここでポリシーとは、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。

10

【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ー（以下、ユーザ情報とポリシーとを、「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。

20

【0035】

アプリケーション I / F 17 は、認証モジュール A ~ C 40、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 ~ C 40、41、42 は、アプリケーション A ~ C 60、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 ~ C 40、41、42 は、アプリケーション A ~ C 60、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。

30

【0036】

<アプリケーション>

アプリケーション A ~ C 60、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 ~ C 60、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 ~ C 40、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 ~ C 40、41、42 が行う。ここで、アプリケーション A ~ C 60、61、62 には、必ずしも認証モジュール A ~ C 40、41、42 を備えなくてよい。この場合には、認証サービス A ~ C 50 ~ 52 からユーザデータを受信して、認証を行う。

40

【0037】

認証モジュール A ~ C 40、41、42 は、アプリケーション A ~ C 60、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 ~ C 40、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 ~ C 40、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

50

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ーをポリシー記録部46に備える(図3参照)。そして、ポリシー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、ポリシーが更新される。

【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。

10

【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)。

20

【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ーの入力を受け、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ーの更新情報は、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。

30

【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もよい。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と相異なる。

40

【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

50



アカウント統合機能部 20 と、認証モジュール A ~ C 40、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	-

10

【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。

20

【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。

30

【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	-

40

【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】

10

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】

20

< 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。

30

## 【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。

40

## 【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、

50

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 B 4 1 に更新情報は配信されない。

【 0 0 5 5 】

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、ポリシー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。

【 0 0 5 6 】

また、ポリシーには、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ー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。

【 0 0 5 7 】

< 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。

【 0 0 5 8 】

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 S 0 1）。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 S 0 2）。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 S 0 3）、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 S 0 4）。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。

【 0 0 5 9 】

< 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 ~ D 6 0 ~ 6 3 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。

【 0 0 6 0 】

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 D 6 3 に認証される場合は、アプリケーション D 6 3 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、B 5 0、5 1 を必要としないで、ユーザの認証を完了する（ステップ S 1 0）。

【 0 0 6 1 】

第 2 に、クライアント 47 が、アプリケーション E 6 4 に認証される場合は、アプリケーション E 6 4 が、認証モジュールを備えないため、認証サービス A 5 0 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 S 2 0、2 1）。

【 0 0 6 2 】

第 3 に、クライアント 47 が、アプリケーション F 6 5 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 B 5 1 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 F 6 5 にアクセスする（ステップ S 3 0、S 3 1）。この場合には、アプリケーション F 6 5 が、認証モジュールを備えなくとも、認証を

10

20

30

40

50

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) 情報システムを使用するユーザのユーザ情報を管理し、認証を行う統合ユーザ管理システムであって、

認証が必要な認証サービスの同期を行うアカウント統合機能部と、

アプリケーションの認証を行う認証モジュールと、

前記ユーザ情報及びポリシー(この双方を「ユーザデータ」とする)を記録(統合的に管理)し、前記ユーザ情報を前記アプリケーションのいずれかに配信し、前記ユーザデータを使用して、前記アカウント統合機能部と前記認証モジュールとを連携させて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。

10

20

30

40

50

## 【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ー)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】

(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、前記ポリシーが、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ー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、

前記論理統合機能部が記録するユーザデータが、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における前記ユーザが属するグループ(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み、

前記論理統合機能部が、前記三次元役割セットに関する情報を含むユーザデータを、前記アカウント統合機能部、前記認証モジュール、前記アプリケーションに配信する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、統合

10

20

30

40

50

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、前記ポリシーに基づいて、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。

10

【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ー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ーを、ユーザ情報を制限するポリシー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ーにより、2次利用の範囲を制限し、この制限することをポリシーとして記録する統合ユーザ管理システム。

20

【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ーに記録する。ここで、記録されるポリシーは、通常、ユーザ認証にて使用されるポリシーであってよい。この場合には、ユーザ認証されるポリシーと、ユーザ情報が管理されるポリシー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。

30

【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。

40

【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】

50

(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。

10

【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。

20

【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。

30

【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】

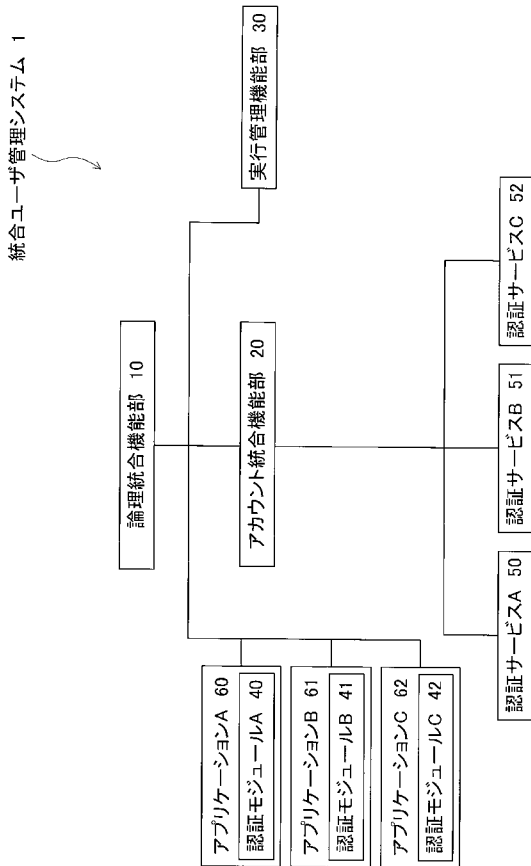
- 1 統合ユーザ管理システム
- 10 論理統合機能部
- 11 制御部
- 12 管理部
- 13 データ管理部
- 14 ポリシ管理部
- 15 論理データベース
- 16 ユーザデータ部
- 17 アプリケーションI/F
- 18 アカウント統合機能部I/F
- 19 実行管理機能部I/F
- 20 アカウント統合機能部
- 21 制御部
- 22 論理統合機能部I/F
- 23 管理部
- 24 アカウントデータベース

40

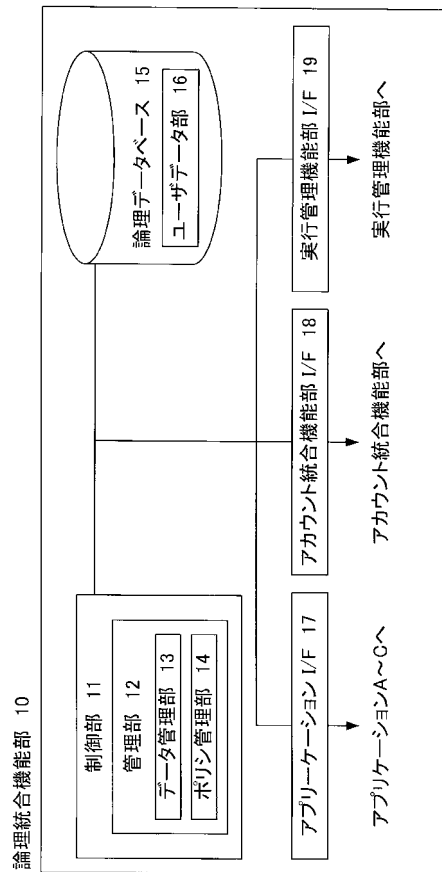
50

- 2 5 認証サービス I / F
- 3 0 実行管理機能部
- 4 0 認証モジュール A
- 4 1 認証モジュール B
- 4 2 認証モジュール C
- 4 5 論理統合機能部 I / F
- 4 6 ポリシ記録部
- 4 7 クライアント
- 6 0 アプリケーション A
- 6 1 アプリケーション B
- 6 2 アプリケーション C
- 6 3 アプリケーション D
- 6 4 アプリケーション E
- 6 5 アプリケーション F
- 6 6 アプリケーション G
- 7 0 , 7 1 , 7 3 , 7 6 ユーザデータ

【 図 1 】

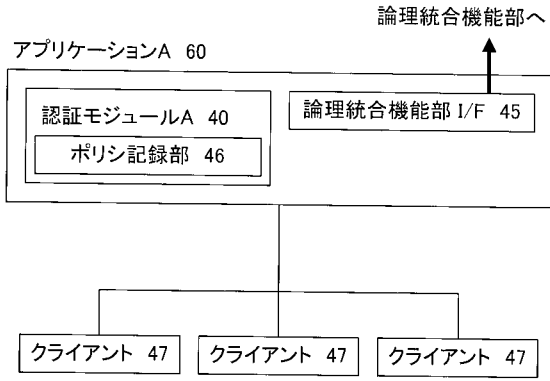


【 図 2 】

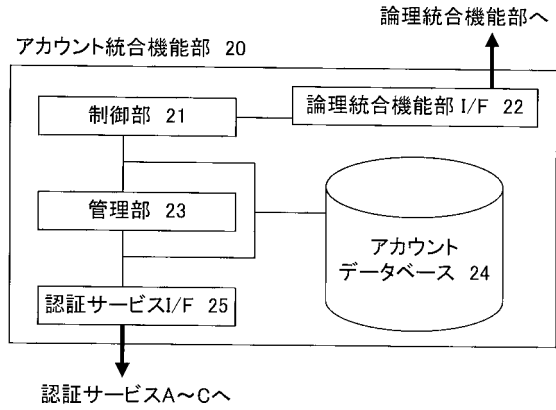




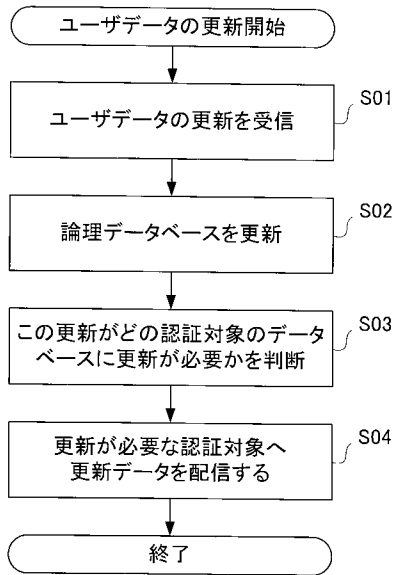
【 図 3 】



【 図 4 】



【 図 5 】



【 図 6 】

