(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2014 年 11 月 27 日(27.11.2014)

WIPO | PCT

(10) 国際公開番号
WO 2014/188743 A1

(51) 国際特許分類:
G06F 21/62 (2013.01)

(21) 国際出願番号: PCT/JP2014/052851

(22) 国際出願日: 2014 年 2 月 7 日(07.02.2014)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願 2013-108925 2013 年 5 月 23 日(23.05.2013) JP

(71) 出願人: 三菱電機株式会社(MITSUBISHI ELECTRIC CORPORATION) [JP/JP]; 〒1008310 東京都千代田区丸の内二丁目７番３号 Tokyo (JP).

(72) 発明者: 小杉 優(KOSUGI, Yu); 〒1008310 東京都千代田区丸の内二丁目７番３号 三菱電機株式会社内 Tokyo (JP). 佐藤 雅之(SATO, Masayuki); 〒1008310 東京都千代田区丸の内二丁目７番３号 三菱電機株式会社内 Tokyo (JP). 楓 仁志(KAEDE, Satoshi); 〒1008310 東京都千代田区丸の内二丁目７番３号 三菱電機株式会社内 Tokyo (JP). 山足 光義(YAMATARI, Mitsuyoshi); 〒1008310 東京都千代田区丸の内二丁目７番３号 三菱電機株式会社内 Tokyo (JP).

(74) 代理人: 溝井 章司, 外(MIZOI, Shoji et al.); 〒2470056 神奈川県鎌倉市大船二丁目１７番１０号 ＮＴＡ大船ビル３階 溝井国際特許事務所 Kanagawa (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

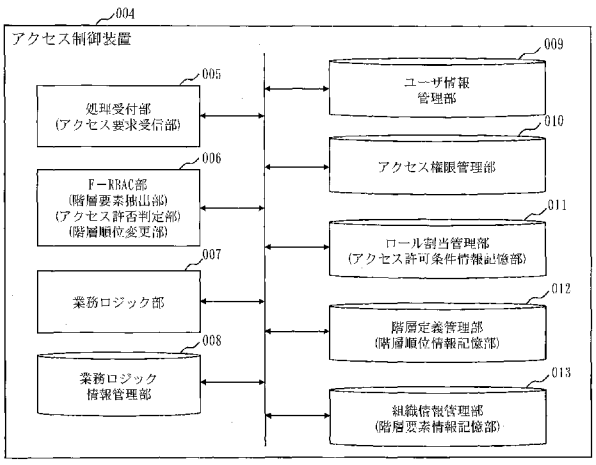
(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシ

[続葉有]

(54) **Title**: ACCESS CONTROL DEVICE AND ACCESS CONTROL METHOD AND PROGRAM

(54) 発明の名称 : アクセス制御装置及びアクセス制御方法及びプログラム

[図2]



004 Access control device
005 Process reception unit
(Access request receiving unit)
006 F-RBAC unit
(Hierarchy element extraction unit)
(Access permission determination unit)
(Hierarchy priority change unit)
007 Work logic unit
008 Work logic information management unit
009 User information management unit
010 Access authority management unit
011 Role allocation management unit
(Access permission conditions information memory unit)
012 Hierarchy definition management unit
(Hierarchy priority information memory unit)
013 Organization information management unit
(Hierarchy element information memory unit)

(57) **Abstract**: A hierarchy definition management unit (012) stores priority between hierarchy levels. An organization information management unit (013) stores information that indicates pairs of hierarchy elements for each hierarchy level combination. A role allocation management unit (011) stores information by which a condition that permits access is correlated with a specific hierarchy element. A process reception unit (005) inputs, from a user, an operation request requesting access to resources. An F-RBAC unit (006) identifies a hierarchy element corresponding to the user, extracts from the information of the organization information management unit (013) of a hierarchy element that is paired with and is one hierarchy above the identified hierarchy element, on the basis of priority between hierarchy levels, repeats the operation to extract a hierarchy element of a level that is paired with and is one level above the extracted hierarchy element, compares the identified hierarchy element and the extracted hierarchy elements to the hierarchy elements defined by the role allocation management unit (011), and determines whether to allow access.

(57) 要約:

[続葉有]

WO 2014/188743 A1

ア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

添付公開書類:

— 国際調査報告（条約第 21 条(3)）

階層定義管理部（０１２）は、階層間の順位を記憶する。組織情報管理部（０１３）は、階層要素の対が、階層の組合せごとに示される情報を記憶する。ロール割当管理部（０１１）は、アクセスを許可する条件が特定の階層要素に対応付けられている情報を記憶する。処理受付部（００５）は、ユーザからの、リソースへのアクセスを要求する操作要求を入力する。Ｆ－ＲＢＡＣ部（００６）は、前記ユーザと対応付けられている階層要素を判別し、階層間の順位に基づき、判別した階層要素と対になっている一つ上の階層の階層要素を織情報管理部（０１３）の情報から抽出し、抽出した階層要素と対になっている一つ上の階層の階層要素を抽出する動作を繰り返し、判別した階層要素及び抽出した階層要素とロール割当管理部（０１１）で定義される階層要素とを照合して、アクセス許否を判定する。

明　細　書

発明の名称 ：

アクセス制御装置及びアクセス制御方法及びプログラム

技術分野

[0001] 本発明は、階層構造を用いたアクセス制御に関する。

背景技術

[0002] クラウドサービスやＳａａＳ（Ｓｏｆｔｗａｒｅ　ａｓ　ａ　Ｓｅｒｖｉｃｅ）を実現するための基盤技術として、一つのアプリケーションプログラム（以下、アプリケーションという）を複数の企業（テナント）で共用させる「マルチテナント管理技術」がある。

マルチテナント管理技術の目的として、複数企業によるアプリケーション共用によってハードウェア（Ｈ／Ｗ）リソース及びソフトウェア（Ｓ／Ｗ）リソースを削減し、コストを削減することが挙げられる。

[0003] 従来技術では、ユーザの属性をアクセス権限と対応付けることにより柔軟なアクセス権限の設定を可能にしている（例えば、特許文献１）。

特許文献１では、「ユーザ情報表」で、ユーザだけでなくテナント・部門等の属性を管理しており、「アクセス権限割当表」で、アクセス制御を行う権限ごとに、どのような属性をもつユーザがアプリケーションを利用可能かを管理している。

先行技術文献

特許文献

[0004] 特許文献1：特開２０１２－６９０８７号公報

発明の概要

発明が解決しようとする課題

[0005] マルチテナントアプリケーションでは、新規にシステムを開発するだけでなく、開発コストを削減するために従来単一のテナントで利用していたアプリケーションを最大限有効活用してマルチテナントで利用可能にすることが

ある。

また、元々あるビルで利用していたアプリケーションを、サービス範囲を拡大するために他のビルや他のビルに属するテナントも利用可能にすることがある。

つまり、ビルに属しているあるテナントが、別のビルにも入居したため、ビルを跨ってテナントにアクセス制御を設定する必要がある。

そのため、ビル、テナント、会社内の総務部、営業部といった組織という順序の階層構造から、ある時点で、テナント、ビル、組織という階層構造に変更する必要が出てくる。

[0006] 特許文献１では、履歴管理に関する言及がなされていない上に、組織階層構造に対する言及もなされていない。

仮に、特許文献１の技術を元に、上記要求を実現しようとする場合、組織階層構造が変更になった場合に、組織階層構造が変更になった時点で設定されているアクセス権限割当を全て見直す必要がある。

[0007] 本発明はこのような課題を解決することを主な目的としており、階層構造の定義が変更された場合にも、変更に伴うデータ改修作業の作業量を最小限にとどめることを主な目的とする。

課題を解決するための手段

[0008] 本発明に係るアクセス制御装置は、

複数の階層で構成される階層構造における階層間の順位が示される階層順位情報を記憶する階層順位情報記憶部と、

階層を構成する要素である階層要素の対であって、異なる二つの階層に属する互いに関連する階層要素の対が、階層の組合せごとに示される階層要素情報を記憶する階層要素情報記憶部と、

アクセスが制限されるアクセス制限リソースへのアクセスを許可する条件であるアクセス許可条件が特定の階層要素に対応付けて示されるアクセス許可条件情報を記憶するアクセス許可条件情報記憶部と、

いずれかの階層要素と対応付けられているユーザからの、アクセス制限リ

ソースへのアクセスを要求するアクセス要求を受信するアクセス要求受信部と、

前記ユーザと対応付けられている階層要素を判別するとともに、前記階層順位情報に示される階層間の順位に基づき、判別した階層要素と対になっている一つ上の階層の階層要素又は一つ下の階層の階層要素を前記階層要素情報から抽出し、抽出した階層要素と対になっている一つ上の階層の階層要素又は一つ下の階層の階層要素を前記階層要素情報から抽出する動作を特定の階層に到達するまで繰り返す階層要素抽出部と、

前記階層要素抽出部により判別された階層要素及び抽出された階層要素と前記アクセス許可条件に示される前記特定の階層要素とを照合して、前記アクセス要求に対して前記アクセス制限リソースへのアクセスを許可するか否かを判定するアクセス許否判定部とを有することを特徴とする。

発明の効果

[0009] 本発明では、階層間の順位が示される階層順位情報を記憶し、また、異なる二つの階層に属する互いに関連する階層要素の対が、階層の組合せごとに示される階層要素情報を記憶し、アクセス要求があった時点で、アクセス要求を行ったユーザに対応付けられている階層要素を起点にして階層順位情報と階層要素情報に基づいて階層構造を構築する。

このように、本発明では、階層間の上下関係が定義されるのみで階層要素間の上下関係は定義されていないので、階層構造に変更があった場合でも階層順位情報の改修ですみ、改修作業の作業量を最小限にとどめることができる。

図面の簡単な説明

[0010] [図1]実施の形態１に係るシステム構成例を示す図。

[図2]実施の形態１に係るアクセス制御装置の構成例を示す図。

[図3]実施の形態１に係る操作要求の構成例を示す図。

[図4]実施の形態１に係るユーザ情報管理部で管理されているユーザ情報の例を示す図。

[図5]実施の形態１に係るアクセス権限管理部で管理されているアクセス権限情報の例を示す図。

[図6]実施の形態１に係るロール割当管理部で管理されているロール割当情報の例を示す図。

[図7]実施の形態１に係る階層定義管理部で管理されている階層定義情報の例を示す図。

[図8]実施の形態１に係る組織情報管理部で管理されている情報の例を示す図。

[図9]実施の形態１に係る業務ロジック部の構成例を示す図。

[図10]実施の形態１に係る業務ロジック情報管理部の構成例を示す図。

[図11]実施の形態１に係る処理受付部の動作例を示すフローチャート図。

[図12]実施の形態１に係るＦ－ＲＢＡＣ部の動作例を示すフローチャート図。

[図13]実施の形態１に係る業務ロジック部の動作例を示すフローチャート図。

[図14]実施の形態１に係る階層構造変更要求の例を示す図。

[図15]実施の形態１に係るＦ－ＲＢＡＣ部の動作例を示すフローチャート図。

[図16]実施の形態１に係る階層定義管理部で管理されている階層順位変更後の階層定義情報の例を示す図。

[図17]実施の形態２に係る階層定義管理部で管理されている階層定義情報の例を示す図。

[図18]実施の形態２に係る業務ロジック情報管理部の構成例を示す図。

[図19]実施の形態１に係るユーザと所属組織と所属ビルと所属テナントとの関係を示す図。

[図20]実施の形態１に係るアクセス制御装置のハードウェア構成例を示す図。

発明を実施するための形態

[0011] 実施の形態１．

本実施の形態では、様々な利用者に対し同一アプリケーションを共用可能にするために、マルチテナント型アプリケーションでのデータへのアクセス権やアプリケーションの利用権（以下、アクセス権限）を効率よく管理するための構成を説明する。

より具体的には、本実施の形態では、階層構造の定義が変更された場合にも、変更に伴うデータ改修作業の作業量を最小限にとどめる構成を説明する。

[0012] また、本実施の形態では、保持する操作履歴の情報を最小限にとどめる構成を説明する。

企業等においては、内部統制の関係から、アプリケーション操作に対する操作履歴を管理し、履歴の追跡を実施する必要がある。

そのため、過去の時刻における階層構造を再現する必要がある。

特許文献１の技術では、操作履歴として保持しなければならないデータも膨大になってしまうが、本実施の形態によれば、保持する操作履歴の情報を最小限にすることができる。

[0013] 図１は、本実施の形態に係るシステム構成例を示す。

[0014] 図１において、端末００１、端末００２は、サービスを利用するテナント企業に配置されている端末装置であり、パーソナルコンピュータ、モバイル端末等を想定している。

端末００１、端末００２内にはＷｅｂブラウザ００１ａ、００２ａがインストールされている。

なお、端末００１、００２を操作するユーザは別のテナント企業の従業員を想定している。

また、同一テナント企業内で複数の端末を設置したり、同一のアプリケーションを３テナント企業以上で利用したりすることも可能である。

[0015] 端末０００は、図１に示すシステムを管理するシステム管理者、運用者が利用する端末装置であり、パーソナルコンピュータ、モバイル端末等を想定

している。

端末０００内にはＷｅｂブラウザ０００ａがインストールされている。

[0016] ネットワーク００３は、端末００１、００２がアクセス制御装置００４を利用する際に用いる通信路であり、インターネットおよびＬＡＮ（Ｌｏｃａｌ Ａｒｅａ Ｎｅｔｗｏｒｋ）であってもよい。

[0017] アクセス制御装置００４は、アクセスが制限されるアクセス制限リソースへのアクセスを許可するか否かを判定する。

なお、以下では、特定の組織に属するユーザ、特定の属性を有するユーザにのみアクセスが許可される業務ロジック（アプリケーション）をアクセス制限リソースの例として用いる。

[0018] アクセス制御装置００４は、図２に示すように、処理受付部００５、フレキシブルロールベースアクセスコントロール部（Ｆｌｅｘｉｂｌｅ Ｒｏｌｅ－ｂａｓｅｄ Ａｃｃｅｓｓ Ｃｏｎｔｒｏｌ部；以下、Ｆ－ＲＢＡＣ部とする）００６、業務ロジック部００７、業務ロジック情報管理部００８、ユーザ情報管理部００９、アクセス権限管理部０１０、ロール割当管理部０１１、階層定義管理部０１２、組織情報管理部０１３を有する。

[0019] アクセス制御装置００４において、処理受付部００５は、端末００１、００２から発信されたリクエストを受信し、後述する処理を実施する。

処理受付部００５は、例えば、端末００１、００２から、アクセス制限リソースへのアクセスを要求するリクエストである操作要求（アクセス要求）を受信する。

処理受付部００５は、アクセス要求受信部の例に相当する。

[0020] Ｆ－ＲＢＡＣ部００６は、端末００１、００２のリクエスト内容とアクセス制御装置００４内で管理している情報を元に、アクセス権限の有無を判定する。

Ｆ－ＲＢＡＣ部００６は、階層要素抽出部、アクセス許否判定部、階層順位変更部の例に相当する。

[0021] 業務ロジック部００７は、就業管理や経理処理といった業務用処理を実施

する。

[0022] 業務ロジック情報管理部００８は、業務ロジック部００７で利用する情報を管理する。

[0023] ユーザ情報管理部００９は、アプリケーション操作が可能なユーザの情報を管理する。

[0024] アクセス権限管理部０１０は、業務ロジックのアクセス権限を管理する。

[0025] ロール割当管理部０１１は、業務ロジックへアクセス可能な組織をアクセス権限情報と組織情報の対応関係によって管理する。

ロール割当管理部０１１は、アクセス許可条件情報記憶部の例に相当する。

[0026] 階層定義管理部０１２は、システムで利用する組織階層構造の定義を管理する。

階層定義管理部０１２は、階層順位情報記憶部の例に相当する。

[0027] 組織情報管理部０１３は、アプリケーションを利用する組織の情報を管理する。

組織情報管理部０１３は、階層要素情報記憶部の例に相当する。

[0028] なお、図２内の各要素を複数存在させ、冗長構造を持たせることが可能である。

[0029] 図３の操作要求２０１は、端末００１、００２から送信されるリクエスト内容の一例である。

操作要求２０１は、操作要求２０１の発行元のユーザのユーザＩＤ、パスワード等の認証情報、業務ロジック部００７への操作内容、通信を行う上で必要なヘッダ情報を含む。

なお、本実施の形態ではＨＴＴＰ（ＨｙｐｅｒＴｅｘｔ　Ｔｒａｎｓｆｅｒ　Ｐｒｏｔｏｃｏｌ）形式を利用するものとしているが、プロトコルに関してＦＴＰ（Ｆｉｌｅ　Ｔｒａｎｓｆｅｒ　Ｐｒｏｔｏｃｏｌ）、ＪＭＳ（Ｊａｖａ（登録商標）　Ｍｅｓｓａｇｅ

Ｓｅｒｖｉｃｅ）等であっても上記内容を持たせることが可能であれば代

用可能である。

[0030] 操作要求２０１は、通信ヘッダ２０２、認証情報２０３、操作内容２０４を有する。

通信ヘッダ２０２は、端末００１とアクセス制御装置００４との間で通信を行う上で必要なヘッダ情報であり、リクエスト送信元、リクエスト送信先の情報を有する。

認証情報２０３は、リクエスト送信元ユーザの認証情報を示し、例としてユーザのユーザＩＤ、パスワードを有する。

操作内容２０４は、リクエスト送信元ユーザの業務ロジック部００７への操作要求内容を示し、例として業務ロジックの種類、操作内容（データの参照、データの更新等）を有する。

[0031] 図４は、ユーザ情報管理部００９で管理されるユーザ情報３０１の例を示す。

ユーザ情報３０１は、アクセス制御装置００４を利用するユーザの情報を保持しており、ユーザＩＤにより各ユーザを一意に識別可能であるものとする。

なお、ユーザ情報３０１は、ユーザＩＤ以外に、ユーザ名称や、ユーザの属する組織の組織ＩＤ、ユーザの認証に必要なパスワードを有する。

[0032] 図５は、アクセス権限管理部０１０で管理されるアクセス権限情報４０１の例を示す。

アクセス権限情報４０１は、アクセス制御装置００４で管理する業務ロジック部００７の操作権限範囲やアクセス制御装置００４自体の操作権限範囲の情報を保持している。

例えば、業務ロジックＡに対する操作可否や、アクセス権限の操作可否が操作可能内容として保持されている。

なお、操作可否については参照のみ可能等、一部制限をつけることが可能とする。

[0033] 図６は、ロール割当管理部０１１で管理されるロール割当情報５０１の例

を示す。

ロール割当情報５０１は、アクセス権限情報４０１と組織情報との対応関係を管理し、どの組織がその操作を実施することが可能かの情報を保持している。

なお、権限の割当対象は、組織だけでなくビル全体、テナント全体といった設定も可能である。

さらに、組織の配下（指定した組織の子組織以下も該当する場合）や、直下（指定した組織の子組織は含まず）といった指定も可能とする。

なお、ロール割当情報はロール自体の情報と、ロールと組織との対応関係を表す情報に分割することも可能である。

図６に示すように、ロール割当情報５０１には、アクセス制限リソース（テナントＡ業務ロジック、ビルＡ業務ロジック）へのアクセス（操作、参照）を許可する条件であるアクセス許可条件が特定の階層要素（Ｔ００１配下、Ｂ００１配下）に対応付けて示さている。

なお、Ｔ００１とＢ００１は、図８に示すように、それぞれテナントのＩＤとビルのＩＤである。

ロール割当情報５０１は、アクセス許可条件情報の例に相当し、ロール割当管理部０１１は、前述したように、アクセス許可条件情報記憶部の例に相当する。

[0034] 図７は、階層定義管理部０１２で管理される階層定義情報６０１を示す。

階層定義情報６０１は、アクセス制御装置００４を利用するビル、テナント、組織等のエンティティ間の順位、及び階層構造が有効である期間を示す有効期限を有する。

例えば、図７中の階層ＩＤ：ＳＴ００１は、階層構造の頂点にビルを配し、ビルの下にテナント、テナントの下に組織を配する構造を定義している。

なお、図７では、階層の例としてビル、テナント、組織を挙げているが、例えばビルの上位階層に地域というエンティティを定義したり、テナントの下に支社というエンティティを定義したりすることも可能である。

図７に示すように、階層定義情報６０１には、階層構造における階層間の順位が示されており、階層順位情報の例に相当する。

そして、階層定義管理部０１２は、階層順位情報記憶部の例に相当する。

[0035] 図８は、組織情報管理部０１３で管理される情報を示す。

組織情報管理部０１３は、ビル情報７０１、テナント情報７０２、組織情報７０３、ビル・テナント対応情報７０４、テナント・組織対応情報７０５、ビル・組織対応情報７０６を有する。

[0036] ビル情報７０１は、アクセス制御装置００４を利用するビルの情報を保持する。

各ビルは、ビルＩＤにより識別可能である。

また、ビルＩＤ以外にビル名称、ビルの所在地といった属性情報を保持することも可能である。

[0037] テナント情報７０２は、アクセス制御装置００４を利用するテナントの情報を保持する。

各テナントは、テナントＩＤにより識別可能である。

また、テナントＩＤ以外にテナント名称、テナントの契約内容といった属性情報を保持することも可能である。

[0038] 組織情報７０３は、アクセス制御装置００４を利用する組織の情報を保持する。

各組織は、組織ＩＤにより識別可能である。

また、組織ＩＤ以外に組織名称、組織における責任者（組織長）といった属性情報を保持することも可能である。

なお、組織については部の配下に課が置かれるケースのように組織間での階層構造も考えられるため、組織の上位階層に当たる組織（親組織）についても情報として有する。

[0039] ビル・テナント対応情報７０４は、ビル情報７０１で管理するビルと、テナント情報７０２で管理するテナントとの対応関係を示す。

ビル・テナント対応情報７０４は、ビルＩＤ・テナントＩＤのようにビル

とテナントとを一意に特定できる属性を保持している。

また、ビル・テナントの対応関係に有効期限がある場合は、属性として有効期限を保持する。

[0040] テナント・組織対応情報７０５は、テナント情報７０２で管理するテナントと組織情報７０３で管理する組織との対応関係を示す。

テナント・組織対応情報７０５は、テナントＩＤ・組織ＩＤのようにテナントと組織とを一意に特定できる属性を保持している。

また、テナント・組織の対応関係に有効期限がある場合は、属性として有効期限を保持する。

[0041] ビル・組織対応情報７０６は、ビル情報７０１で管理するビルと組織情報７０３で管理する組織との対応関係を示す。

ビル・組織対応情報７０６は、ビルＩＤ・組織ＩＤのようにビルと組織とを一意に特定できる属性を保持している。

また、ビル・組織の対応関係に有効期限がある場合は、属性として有効期限を保持する。

[0042] ビル・テナント対応情報７０４、テナント・組織対応情報７０５、ビル・組織対応情報７０６では、階層を構成する要素である階層要素の対であって、異なる二つの階層に属する互いに関連する階層要素の対が、階層の組合せごとに示されている。

具体的には、ビル階層とテナント階層については、ビル・テナント対応情報７０４において、ビル階層の階層要素であるＢ００１とテナント階層の階層要素であるＴ００１との対、ビル階層の階層要素であるＢ００１とテナント階層の階層要素であるＴ００２との対が記述されている。

また、テナント階層と組織階層については、テナント・組織対応情報７０５において、テナント階層の階層要素であるＴ００１と組織階層の階層要素であるＯＲＧＴ００１との対、テナント階層の階層要素であるＴ００１と組織階層の階層要素であるＯＲＧＴ００２との対等が記述されている。

また、ビル階層と組織階層については、ビル・組織対応情報７０６におい

て、ビル階層の階層要素であるＢ００１と組織階層の階層要素であるＯＲＧＴ００１との対、ビル階層の階層要素であるＢ００１と組織階層の階層要素であるＯＲＧＴ００２との対等が記述されている。

ビル・テナント対応情報７０４、テナント・組織対応情報７０５、ビル・組織対応情報７０６は、階層要素情報の例に相当する。

そして、組織情報管理部０１３は、前述したように、階層要素情報記憶部の例に相当する。

[0043] 図９は、業務ロジック部００７の内部構成を示している。

業務ロジック部００７は内部に業務ロジック部Ａ８０１、業務ロジック部Ｂ８０２、業務ロジック部Ｃ８０３を有しており、それぞれ担当する業務ロジックが異なる。

例えば、業務ロジック部Ａ８０１では就業管理、業務ロジック部Ｂ８０２では経理管理、業務ロジック部Ｃ８０３では入退室管理といったように別々の業務を担当する。

なお、業務ロジック部００７内にあるロジックの数は任意でありアクセス制御装置００４で扱う業務ロジックの増減にあわせて、内部の業務ロジックの数も増減可能とする。

[0044] 図１０は、業務ロジック情報管理部００８の内部構成を示す。

業務ロジック情報管理部００８では、業務ロジックＡ情報管理部９０１、業務ロジックＢ情報管理部９０２、業務ロジックＣ情報管理部９０３を有している。

それぞれ、業務ロジックＡ情報管理部９０１は業務ロジック部Ａ８０１、業務ロジックＢ情報管理部９０２は業務ロジック部Ｂ８０２、業務ロジックＣ情報管理部９０３は業務ロジック部Ｃ８０３で扱う情報を管理している。

例えば業務ロジックＡ情報管理部９０１では就業管理ロジックで利用する社員名簿、勤怠記録、出勤日のカレンダー等を有する。

なお、業務ロジック部００７と同様に内部で持つ情報の数も増減可能である。

また、各情報管理部で共通に利用する情報がある場合、共用することも可能である。

[0045] 次に、アクセス制御装置００４を利用するユーザが自身の端末から業務ロジック操作要求を出す場合の、動作について説明する。

[0046] テナントＡに所属するユーザＡがアクセス制御装置００４内の業務ロジックＡの操作を行う場合、ユーザＡは、端末００１のＷｅｂブラウザ００１ａを用いてアクセス制御装置００４に対し自身の認証情報及び業務ロジックの操作内容を操作要求２０１の形式で要求を出す。

[0047] アクセス制御装置００４では、端末から操作要求を受信した際の、リクエストの管理及びレスポンスの生成を一元的に処理受付部００５で実施する。

[0048] 図１１のフローチャートを参照して、処理受付部００５の動作について述べる。

なお、以下では、図３に示す操作要求２０１が受信された場合を例にして説明を進める。

図３では、ユーザＩＤ：Ｕ００１のユーザが端末００１を利用して送信した操作要求２０１であって、業務ロジックＡ（業務ＩＤ：Ｌ００１）のデータ参照を要求する操作要求２０１が示されている。

なお、図１９に示すように、ユーザＡは、組織ＩＤ：ＯＲＧ００１の組織に属し、組織ＩＤ：ＯＲＧ００１の組織は、テナントＩＤ：Ｔ００１のテナントに属し、テナントＩＤ：Ｔ００１のテナントは、ビルＩＤ：Ｂ００１のビルに属している。

しかしながら、アクセス制御装置００４では、図１９に示すような階層要素間の上下関係が予め定義した情報は保持しておらず、操作要求２０１を受信した際に、後述するように、Ｆ－ＲＢＡＣ部００６が、図７及び図８に示す情報を用いて、階層要素間の上下関係を分析する。

[0049] 処理受付部００５は、受信した操作要求２０１から認証情報２０３、操作内容２０４を取得し、認証情報２０３、操作内容２０４をＦ－ＲＢＡＣ部００６に出力し、要求元のユーザの業務ロジックへの操作可否をＦ－ＲＢＡＣ

部００６に問い合わせる（Ｓ１０１）。

[0050] 次に、処理受付部００５は、Ｆ－ＲＢＡＣ部００６の問い合わせ結果からユーザの操作可否を判定する（Ｓ１０２）。

[0051] Ｓ１０２の結果が操作可能であった場合（Ｓ１０２でＹＥＳ）、処理受付部００５は、操作要求２０１の操作内容２０４を業務ロジック部００７へ受け渡す（Ｓ１０３）。

そして、処理受付部００５は、業務ロジック部００７への操作要求結果を端末００１ａにレスポンスとして返却する（Ｓ１０４）。

[0052] 一方、Ｓ１０２の結果が操作不可であった場合（Ｓ１０２でＮＯ）は、処理受付部００５は、操作不可であることをレスポンスとして端末００１ａにレスポンスとして返却する（Ｓ１０５）。

[0053] 次に、図１２のフローチャートを参照して、Ｆ－ＲＢＡＣ部００６のユーザの操作可否の判定処理の動作を説明する。

[0054] Ｆ－ＲＢＡＣ部００６は、処理受付部００５から受信した認証情報２０３からユーザＩＤ及びパスワード等の認証に必要な情報を取得する（Ｓ２０１）。

[0055] 次に、Ｆ－ＲＢＡＣ部００６は、ユーザ情報管理部００９に対し、認証情報２０３から取得したユーザＩＤを持つユーザの情報を問い合わせる（Ｓ２０２）。

[0056] 次に、Ｆ－ＲＢＡＣ部００６は、ユーザ認証に成功したかどうかを検証する（Ｓ２０３）。

具体的には、Ｆ－ＲＢＡＣ部００６は以下の手順により検証する。

Ｆ－ＲＢＡＣ部００６は、ユーザ情報管理部００９のレスポンスより、Ｓ２０１で取得したユーザＩＤを持つユーザが存在するかどうか確認する。

該当するユーザが存在しない場合は認証不可とする。

また、該当するユーザが存在する場合、認証情報２０３から取得したパスワードが、ユーザ情報管理部００９で管理されているパスワードと一致するかどうかを判定する。

パスワードが一致した場合は認証成功、一致しない場合は認証失敗とする。

[0057] Ｆ－ＲＢＡＣ部００６は、Ｓ２０３において認証成功であった場合（Ｓ２０３でＹＥＳ）は、処理受付部００５から受信した操作内容２０４からユーザの操作対象となる業務ロジックの業務ＩＤを取得し、アクセス権限管理部０１０に当該業務ＩＤのロジックが紐付いているアクセス権限の一覧を取得する（Ｓ２０４）。

Ｆ－ＲＢＡＣ部００６は、図３の操作内容２０４であれば、業務ＩＤ：Ｌ００１に基づき、図５の権限ＩＤ：Ａ００１のレコードと、権限ＩＤ：Ａ００２のレコードを取得する。

[0058] 次に、Ｆ－ＲＢＡＣ部００６は、階層定義管理部０１２から現時点における階層順位の情報を取得する（Ｓ２０５）。

図７の例では、「ビル＞テナント＞組織」が記述された階層順位の情報を取得する。

[0059] Ｆ－ＲＢＡＣ部００６は、ユーザ情報管理部００９より取得したユーザ情報からユーザの所属する組織の組織ＩＤの情報を元に、組織情報管理部０１３からユーザの所属する組織の情報を取得する（Ｓ２０６）。

図３の操作要求２０１の場合は、ユーザＩＤ：Ｕ００１であるため、図４から、対象となるユーザＡが所属する組織は、組織ＩＤ：ＯＲＧ００１の組織である。

[0060] 次に、Ｆ－ＲＢＡＣ部００６は、階層定義管理部０１２より取得した階層順位の情報と、組織情報管理部０１３から取得した組織の情報とを元に、より上位の階層に属するビル、テナント、組織の情報の取得を、上位階層の組織が存在しなくなるまで繰り返す（Ｓ２０７）。

Ｓ２０５で取得した階層順位が「ビル＞テナント＞組織」であるため、Ｆ－ＲＢＡＣ部００６は、まず、組織の一つ上の階層であるテナント階層で組織ＩＤ：ＯＲＧ００１と対になっている階層要素を探す。

具体的には、Ｆ－ＲＢＡＣ部００６は、図８のテナント・組織対応情報７

０５を検索して、組織ＩＤ：ＯＲＧ００１と対になっているテナントＩＤ：Ｔ００１を抽出する。

次に、Ｆ－ＲＢＡＣ部００６は、階層順位「ビル＞テナント＞組織」より、テナントの１つの上の階層であるビル階層でテナントＩＤ：Ｔ００１と対になっている階層要素を探す。

具体的には、Ｆ－ＲＢＡＣ部００６は、図８のビル・テナント対応情報７０４を検索して、テナントＩＤ：Ｔ００１と対になっているビルＩＤ：Ｂ００１を抽出する。

[0061] 次に、Ｆ－ＲＢＡＣ部００６は、ロール割当管理部０１１から、Ｓ２０４で取得したアクセス権限とＳ２０６、Ｓ２０７で取得した組織、テナント、ビルと合致するロール割当情報を取得する（Ｓ２０８）。

図６の例では、Ｆ－ＲＢＡＣ部００６は、ロール割当ＩＤ：Ｒ００１のレコードと、ロール割当ＩＤ：Ｒ００２のレコードを取得する。

[0062] 次に、Ｆ－ＲＢＡＣ部００６は、Ｓ２０８において取得したロール割当が存在するかどうか判定する（Ｓ２０９）。

なお、組織については上位階層から順に割当があるかどうか確認を行う。

[0063] Ｆ－ＲＢＡＣ部００６は、Ｓ２０９で割当が存在していた場合、認証成功と判断し処理受付部００５に対して成功のレスポンスを返す（Ｓ２１０）。

図３の操作要求２０１では、データ参照が要求されているため、図６の「ロール名称：ビル業務ロジックＡ参照のみ可能」に合致し、Ｆ－ＲＢＡＣ部００６は、処理受付部００５に成功のレスポンスを返す。

[0064] Ｓ２０３で認証失敗もしくはＳ２０９でロールの割当が存在しなかった場合は、Ｆ－ＲＢＡＣ部００６は、認証失敗と判断し、処理受付部００５に失敗のレスポンスを返す（Ｓ２１１）。

[0065] 図１３のフローチャートを参照して、業務ロジック部００７の動作を説明する。

[0066] 業務ロジック部００７は、処理受付部００５から受信した操作内容２０４から、業務ロジック部００７内のどの業務ロジック内の操作が指定されてい

るかを判定し、内部の業務ロジックへ操作内容を受け渡す（Ｓ３０１）。

なお、以下では、図９の業務ロジック部Ａ８０１が指定されたものとして動作を説明する。

[0067] 業務ロジック部Ａ８０１は、Ｓ３０１で業務ロジック部００７より受信した操作内容を元に業務ロジック情報管理部００８内の業務ロジックＡ情報管理部９０１で扱う情報を参照・更新しながら操作を行う（Ｓ３０２）。

業務ロジック部Ａ８０１は、Ｓ３０２を実施した結果について業務ロジック部００７経由で処理受付部００５へレスポンスを返却する（Ｓ３０３）。

[0068] 次に、アクセス制御装置の管理者（以下、システムユーザ）が、アクセス制御装置００４の階層構造を変更する際の動作について説明する。

[0069] 図１４は、アクセス制御装置００４の階層構造を変更する際に、システムユーザが端末０００を用いてアクセス制御装置００４に対して送信するリクエストである階層構造変更要求の一例を示す。

[0070] アクセス制御装置００４を管理するシステムユーザは、端末０００のＷｅｂブラウザ０００ａを用いてアクセス制御装置００４に階層構造変更要求１３０１を送信する。

階層構造変更要求１３０１は、図７の階層定義情報６０１内の階層順位を変更することを要求するリクエストである。

アクセス制御装置００４では、処理受付部００５が階層構造変更要求１３０１を受信し、Ｆ－ＲＢＡＣ部００６がシステムユーザの認証を実施した後に、Ｆ－ＲＢＡＣ部００６は階層定義情報６０１内の階層順位を変更する。

なお、処理受付部００５の動作、Ｆ－ＲＢＡＣ部００６の認証までの動作は前述のＳ１０１～Ｓ１０５、Ｓ２０１～Ｓ２０３と同様である。

階層順位の変更後、処理受付部００５が端末０００に対してレスポンスを返却する。

[0071] 図１５のフローチャートを参照して、階層構造定義変更の際のＦ－ＲＢＡＣ部００６の動作を説明する。

[0072] Ｆ－ＲＢＡＣ部００６は、処理受付部００５より受信した階層構造変更要

求１３０１から、階層構造の変更情報が記載されている操作内容１３０４を取得する（Ｓ４０１）。

次に、Ｆ－ＲＢＡＣ部００６は、Ｓ４０１で取得した操作内容１３０４について、階層定義管理部０１２へ階層構造定義の変更要求を出す（Ｓ４０２）。

階層定義管理部０１２は、Ｓ４０２で受け取った要求に沿って、例えば図７の階層定義情報６０１を図１６の階層定義情報６０２に変更する。

図１６では、新たな階層順位として「テナント＞ビル＞組織」が定義されている。

また、変更前の階層順位「ビル＞テナント＞組織」は、有効期限とともに階層定義情報６０２に保持される。

Ｆ－ＲＢＡＣ部００６は、階層定義管理部０１２の処理が完了した後に、処理受付部００５に対し操作結果を返却する（Ｓ４０３）。

[0073] また、以上の手順により階層定義情報の階層順位が変更された後に操作要求２０１を受信した場合は、Ｆ－ＲＢＡＣ部００６は、変更後の階層順位に基づいて図１２の処理を行う。

[0074] 以上の動作により、システム内で管理する組織の階層構造が時間の経過とともに変更する場合でも、有効期限を持つ階層構造定義を持つことにより、階層構造の定義の変更に合わせて、階層構造定義のみを変更することが可能である。

また、階層構造が有効期限を持つことにより、指定した時刻での階層構造を再現することが可能である。

また、アクセス権限の割当情報の更新が不要となりシステムで管理するデータの変更を最小限にとどめ、かつシステムで保持する過去のログ情報も含めたデータ量を最小限にとどめることができる。

[0075] なお、図１１の説明では、上位階層に向かう方向で階層要素を検索した（Ｓ２０７）が、これに代えて、下位階層に向かう方向で階層要素を検索するようにしてもよい。

[0076] 以上、本実施の形態では、

ロールと、複数の個人及び組織とロールとの対応関係を示すロール割当情報を管理するロール割当管理部と、

組織階層の構造及び階層構造の有効期間を管理する階層定義管理部と、

ロール割当管理部と階層定義部が持つ階層構造定義を元に組織階層構造を解釈しながら上位から順に階層を辿っていき、ロール割当対象とシステムを利用するユーザの所属する組織階層位置とを比較し、システムで管理する情報へのアクセス権限やシステムの利用権限が保持されているかどうかを判定するアクセス制御部を備えたテナントアクセス制御装置、方式、及びプログラムを説明した。

[0077] また、本実施の形態では、

組織の階層構造を任意時刻に変更する際に、階層構造の有効期限を変更することで、システム内の階層構造の変更を実現するアクセス制御部を備えたテナントアクセス制御装置、方式、及びプログラムを説明した。

[0078] また、本実施の形態では、

システム内のアプリケーションごとのアクセス可否を管理するアクセス権限管理部を備え、

個人がシステム内のアプリケーションを利用する際に、アクセス権限管理部のアクセス可否の情報を元にアクセス可否を判断するアクセス制御部を備えた、テナントアクセス制御装置、方式、及びプログラムを説明した。

[0079] 実施の形態２.

本実施の形態では、実施の形態１との相違点を述べる。

以下で説明している以外の動作、構成は、実施の形態１と同じである。

[0080] 図１７は、本実施の形態に係る階層定義管理部０１２の階層定義情報６１０を示す。

図１７の階層定義情報６１０では、図７の階層定義情報６０１と比較して、属性として業務ＩＤのように業務ロジックに対応する情報が付加されている。

本実施の形態では、図１７に示すように、業務ロジックごとに階層構造を変更できるようにしている。

つまり、本実施の形態に係る階層定義情報６１０では、業務ロジック（アクセス制限リソース）ごとに、階層順位が定義されている。

[0081] 図１８は、本実施の形態に係る業務ロジック情報管理部００８の業務ロジック定義９１０を示す。

図１０と異なり、図１８では、業務ロジックごとに業務ＩＤを割り振っている。

ユーザが端末を用いて業務ロジックの操作要求２０１を送信した場合に、図１２のＳ２０５において、階層順位を取得する際に、Ｆ－ＲＢＡＣ部００６は、操作要求２０１中から業務ＩＤを取得し、取得した業務ＩＤに対応する階層順位を取得し、取得した階層順位を、以後のアクセス権限有無の判定に用いる。

[0082] このような構成にすることで、実施の形態１と同様の効果が得られると同時に、アプリケーションごとに用いる階層構造定義を切り替えることができる。

このため、様々なアプリケーションを一つのシステムに集約しつつ、共通のロジックが利用できるため、集約度が高くなる効果が得られる。

[0083] 以上、本実施の形態では、

システム内のアプリケーションごとの組織の階層構造を持つ階層定義管理部を備え、

個人がシステム内のアプリケーションを利用する際に階層定義管理部によりアプリケーションごとに組織階層構造を切り替えてアクセス可否を判断するアクセス制御部を備えたテナントアクセス制御装置、方式、及びプログラムを説明した。

[0084] 最後に、実施の形態１及び２に示したアクセス制御装置００４のハードウェア構成例を図２０を参照して説明する。

アクセス制御装置００４はコンピュータであり、アクセス制御装置００４

の各要素をプログラムで実現することができる。

アクセス制御装置００４のハードウェア構成としては、バスに、演算装置１９０１、外部記憶装置１９０２、主記憶装置１９０３、通信装置１９０４、入出力装置１９０５が接続されている。

[0085] 演算装置１９０１は、プログラムを実行するＣＰＵ（Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）である。

外部記憶装置１９０２は、例えばＲＯＭ（Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）やフラッシュメモリ、ハードディスク装置である。

主記憶装置１９０３は、ＲＡＭ（Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ）である。

図２に示した「～管理部」は、外部記憶装置１９０２又は主記憶装置１９０３により実現される。

通信装置１９０４は、処理受付部００５の物理層に対応する。

入出力装置１９０５は、例えばマウス、キーボード、ディスプレイ装置等である。

[0086] プログラムは、通常は外部記憶装置１９０２に記憶されており、主記憶装置１９０３にロードされた状態で、順次演算装置１９０１に読み込まれ、実行される。

プログラムは、図２に示す「～部」（但し、「～管理部」を除く。以下も同様）として説明している機能を実現するプログラムである。

更に、外部記憶装置１９０２にはオペレーティングシステム（ＯＳ）も記憶されており、ＯＳの少なくとも一部が主記憶装置１９０３にロードされ、演算装置１９０１はＯＳを実行しながら、図１に示す「～部」の機能を実現するプログラムを実行する。

また、実施の形態１及び２の説明において、「～の判断」、「～の判定」、「～の判別」、「～の抽出」、「～の照合」、「～の取得」、「～の設定」、「～の登録」、「～の選択」、「～の生成」、「～の受信」、「～の出力」等として説明している処理の結果を示す情報やデータや信号値や変数値

が主記憶装置１９０３にファイルとして記憶されている。

また、暗号鍵・復号鍵や乱数値やパラメータが、主記憶装置１９０３にファイルとして記憶されてもよい。

[0087] なお、図２０の構成は、あくまでもアクセス制御装置００４のハードウェア構成の一例を示すものであり、アクセス制御装置００４のハードウェア構成は図２０に記載の構成に限らず、他の構成であってもよい。

[0088] また、実施の形態１及び２に示す手順により、本発明に係るアクセス制御方法を実現可能である。

符号の説明

[0089] ０００　端末、００１　端末、００２　端末、００３　ネットワーク、００４　アクセス制御装置、００５　処理受付部、００６　Ｆ－ＲＢＡＣ部、００７　業務ロジック部、００８　業務ロジック情報管理部、００９　ユーザ情報管理部、０１０　アクセス権限管理部、０１１　ロール割当管理部、０１２　階層定義管理部、０１３　組織情報管理部。

請求の範囲

[請求項1] 複数の階層で構成される階層構造における階層間の順位が示される階層順位情報を記憶する階層順位情報記憶部と、

階層を構成する要素である階層要素の対であって、異なる二つの階層に属する互いに関連する階層要素の対が、階層の組合せごとに示される階層要素情報を記憶する階層要素情報記憶部と、

アクセスが制限されるアクセス制限リソースへのアクセスを許可する条件であるアクセス許可条件が特定の階層要素に対応付けて示されるアクセス許可条件情報を記憶するアクセス許可条件情報記憶部と、

いずれかの階層要素と対応付けられているユーザからの、アクセス制限リソースへのアクセスを要求するアクセス要求を受信するアクセス要求受信部と、

前記ユーザと対応付けられている階層要素を判別するとともに、前記階層順位情報に示される階層間の順位に基づき、判別した階層要素と対になっている一つ上の階層の階層要素又は一つ下の階層の階層要素を前記階層要素情報から抽出し、抽出した階層要素と対になっている一つ上の階層の階層要素又は一つ下の階層の階層要素を前記階層要素情報から抽出する動作を特定の階層に到達するまで繰り返す階層要素抽出部と、

前記階層要素抽出部により判別された階層要素及び抽出された階層要素と前記アクセス許可条件に示される前記特定の階層要素とを照合して、前記アクセス要求に対して前記アクセス制限リソースへのアクセスを許可するか否かを判定するアクセス許否判定部とを有することを特徴とするアクセス制御装置。

[請求項2] 前記階層要素情報記憶部は、

異なる二つの階層に属する上下関係にある階層要素の対が、いずれの階層要素が上位でいずれの階層要素が下位であるかの定義を含まずに、階層の組合せごとに示される階層要素情報を記憶していることを

特徴とする請求項１に記載のアクセス制御装置。

[請求項3] 前記アクセス制御装置は、更に、

前記階層順位情報の階層間の順位を変更する階層順位変更部を有し、

前記アクセス許否判定部は、

前記階層順位変更部により前記階層順位情報の階層間の順位が変更された後に受信されたアクセス要求に対しては、変更後の階層間の順位に基づき、階層要素を抽出することを特徴とする請求項１に記載のアクセス制御装置。

[請求項4] 前記階層順位変更部は、

前記階層順位情報の階層間の順位を変更する場合に、変更前の階層間の順位を、有効期限とともに前記階層順位情報記憶部に保持させておくことを特徴とする請求項３に記載のアクセス制御装置。

[請求項5] 前記アクセス許可条件情報記憶部は、

アクセス許可条件が特定のユーザに対応付けて示されるアクセス許可条件情報を記憶し、

前記アクセス許否判定部は、

前記アクセス要求の送信元のユーザが、前記アクセス許可条件情報に示される前記特定のユーザに該当するか否かを判断して、前記アクセス要求に対して前記アクセス制限リソースへのアクセスを許可するか否かを判定することを特徴とする請求項１に記載のアクセス制御装置。

[請求項6] 前記アクセス制御装置は、

複数のアクセス制限リソースについてのアクセス制御を行っており、

前記階層順位情報記憶部は、

各アクセス制限リソースに対して、階層順位情報を記憶しており、

前記アクセス要求受信部は、

いずれかのアクセス制限リソースへのアクセスを要求するアクセス要求を受信し、

前記アクセス許否判定部は、

前記アクセス要求でアクセスが要求されているアクセス制限リソースに対する階層順位情報に示される階層間の順位に基づき、階層要素を抽出することを特徴とする請求項１に記載のアクセス制御装置。

[請求項7] 複数の階層で構成される階層構造における階層間の順位が示される階層順位情報を、コンピュータが記憶領域から読み出し、

階層を構成する要素である階層要素の対であって、異なる二つの階層に属する互いに関連する階層要素の対が、階層の組合せごとに示される階層要素情報を、前記コンピュータが前記記憶領域から読み出し、

アクセスが制限されるアクセス制限リソースへのアクセスを許可する条件であるアクセス許可条件が特定の階層要素に対応付けて示されるアクセス許可条件情報を、前記コンピュータが前記記憶領域から読み出し、

いずれかの階層要素と対応付けられているユーザからの、アクセス制限リソースへのアクセスを要求するアクセス要求を前記コンピュータが受信し、

前記コンピュータが、前記ユーザと対応付けられている階層要素を判別するとともに、前記階層順位情報に示される階層間の順位に基づき、判別した階層要素と対になっている一つ上の階層の階層要素又は一つ下の階層の階層要素を前記階層要素情報から抽出し、抽出した階層要素と対になっている一つ上の階層の階層要素又は一つ下の階層の階層要素を前記階層要素情報から抽出する動作を特定の階層に到達するまで繰り返し、

前記コンピュータが、判別された階層要素及び抽出された階層要素と前記アクセス許可条件に示される前記特定の階層要素とを照合して

、前記アクセス要求に対して前記アクセス制限リソースへのアクセスを許可するか否かを判定することを特徴とするアクセス制御方法。

[請求項8] 複数の階層で構成される階層構造における階層間の順位が示される階層順位情報を、記憶領域から読み出す階層順位情報読み出し処理と、

階層を構成する要素である階層要素の対であって、異なる二つの階層に属する互いに関連する階層要素の対が、階層の組合せごとに示される階層要素情報を、前記記憶領域から読み出す階層要素情報読み出し処理と、

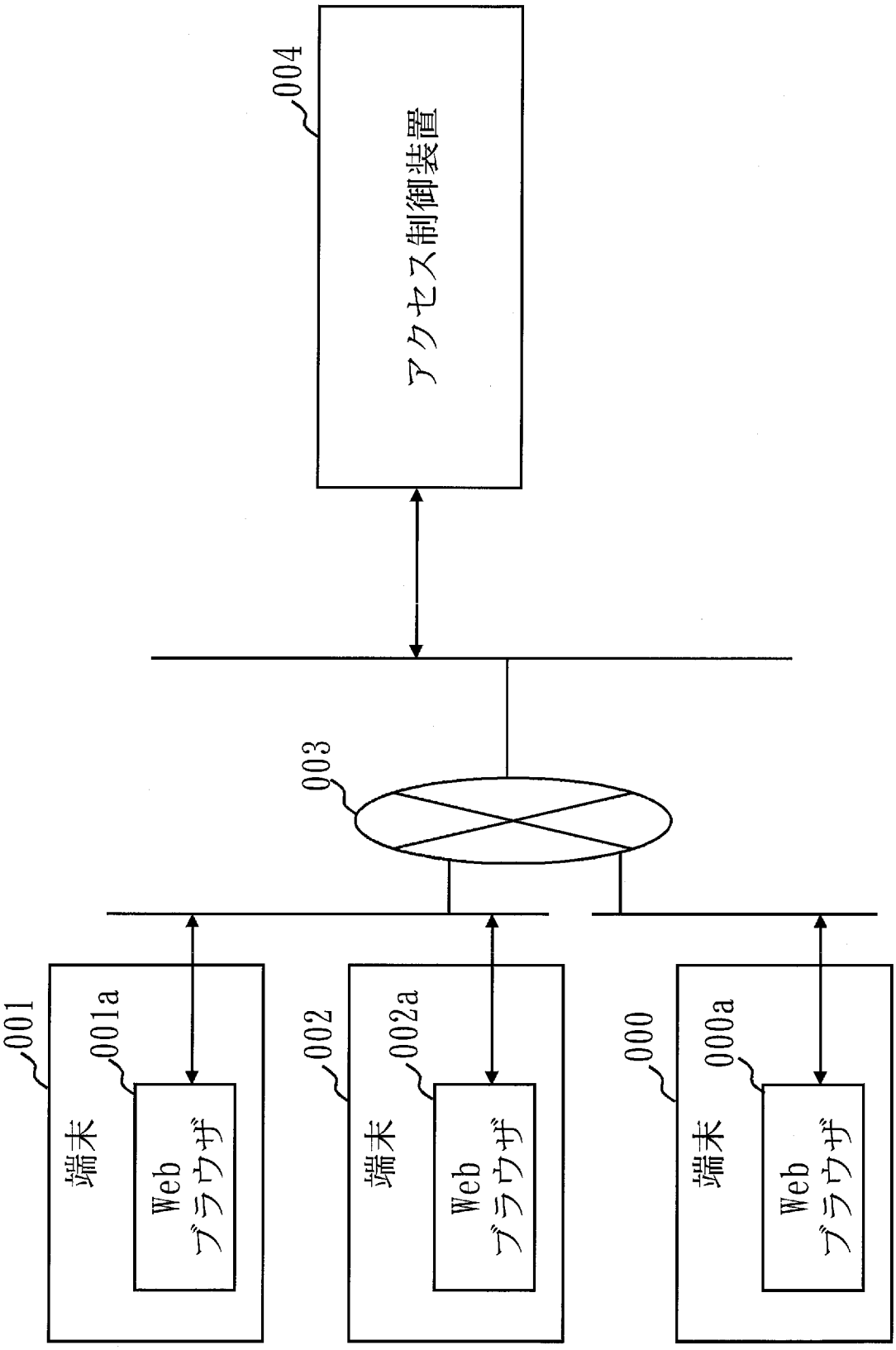
アクセスが制限されるアクセス制限リソースへのアクセスを許可する条件であるアクセス許可条件が特定の階層要素に対応付けて示されるアクセス許可条件情報を、前記記憶領域から読み出すアクセス許可条件情報読み出し処理と、

いずれかの階層要素と対応付けられているユーザからの、アクセス制限リソースへのアクセスを要求するアクセス要求を受信するアクセス要求受信処理と、

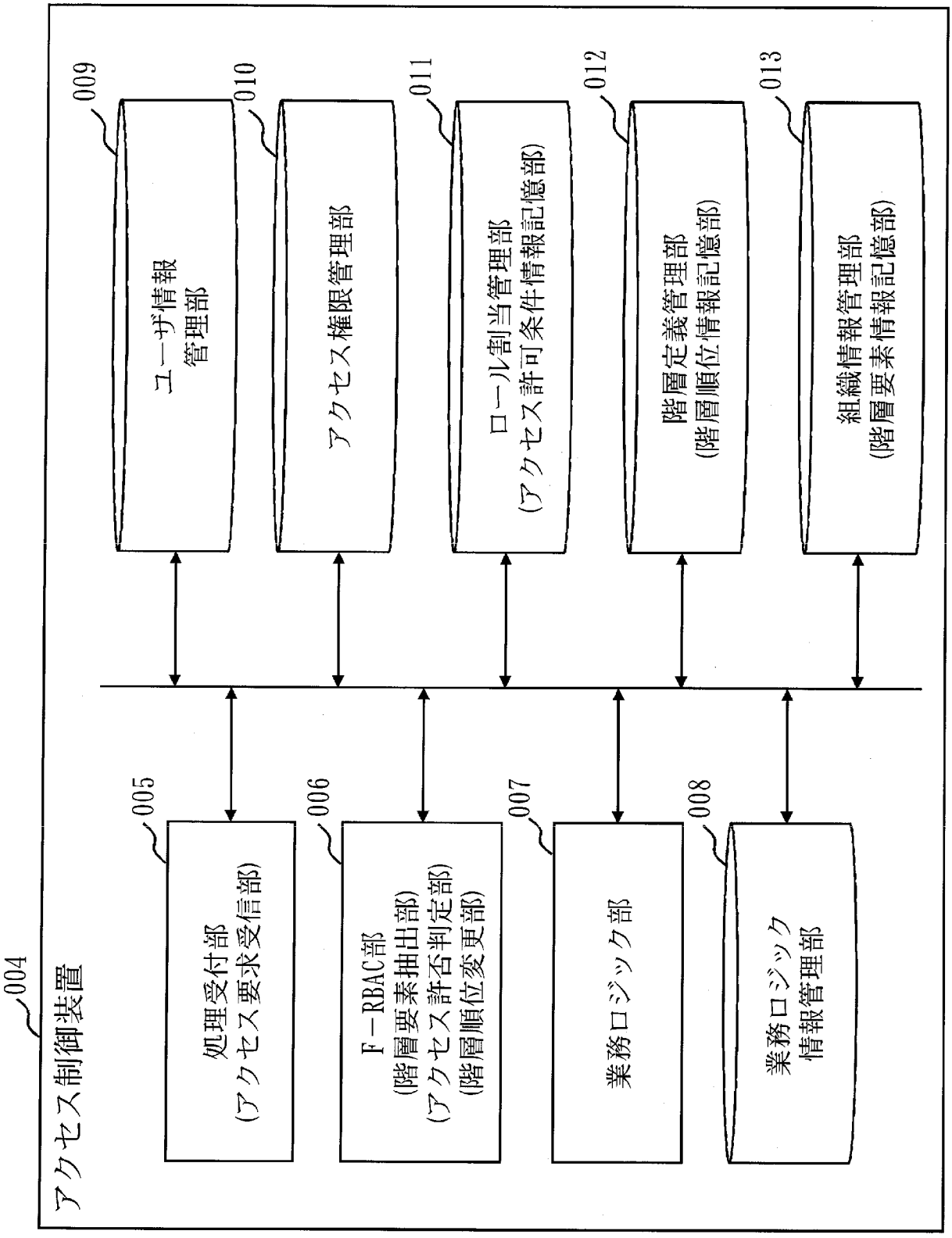
前記ユーザと対応付けられている階層要素を判別するとともに、前記階層順位情報に示される階層間の順位に基づき、判別した階層要素と対になっている一つ上の階層の階層要素又は一つ下の階層の階層要素を前記階層要素情報から抽出し、抽出した階層要素と対になっている一つ上の階層の階層要素又は一つ下の階層の階層要素を前記階層要素情報から抽出する動作を特定の階層に到達するまで繰り返す階層要素抽出処理と、

前記階層要素抽出処理により判別された階層要素及び抽出された階層要素と前記アクセス許可条件に示される前記特定の階層要素とを照合して、前記アクセス要求に対して前記アクセス制限リソースへのアクセスを許可するか否かを判定するアクセス許否判定処理とをコンピュータに実行させることを特徴とするプログラム。

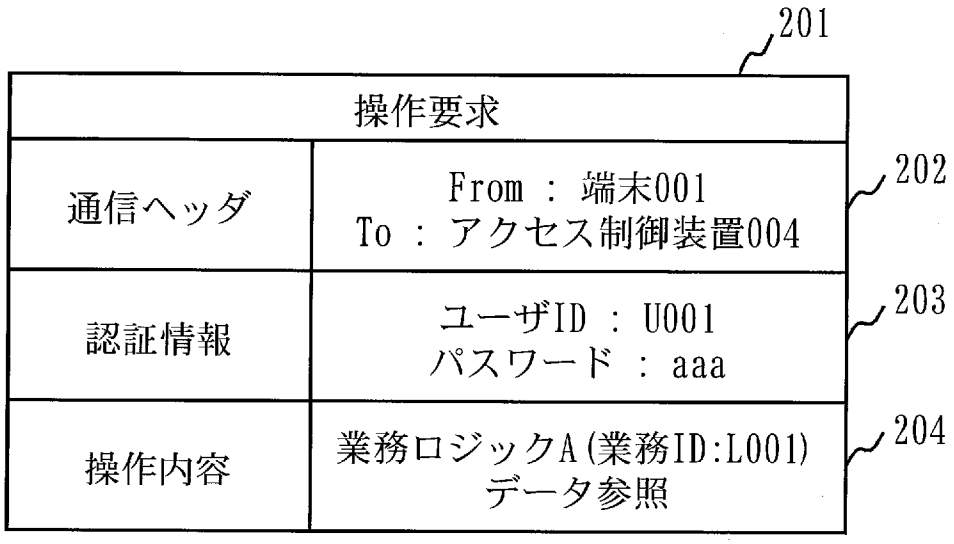
[図1]


004
アクセス制御装置
003
001
001a
端末
Web
ブラウザ
002
002a
端末
Web
ブラウザ
000
000a
端末
Web
ブラウザ

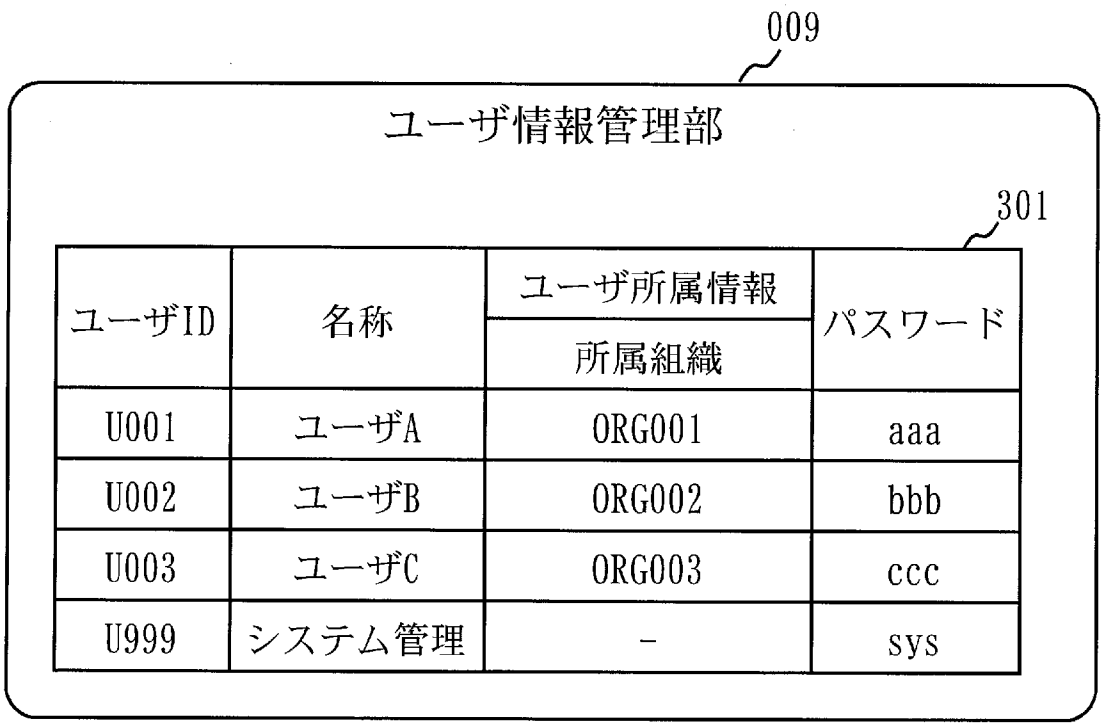
[図2]


004
アクセス制御装置
005
処理受付部
(アクセス要求受信部)
006
F－RBAC部
(階層要素抽出部)
(アクセス許否判定部)
(階層順位変更部)
007
業務ロジック部
008
業務ロジック
情報管理部
009
ユーザ情報
管理部
010
アクセス権限管理部
011
ロール割当管理部
(アクセス許可条件情報記憶部)
012
階層定義管理部
(階層順位情報記憶部)
013
組織情報管理部
(階層要素情報記憶部)

[図3]

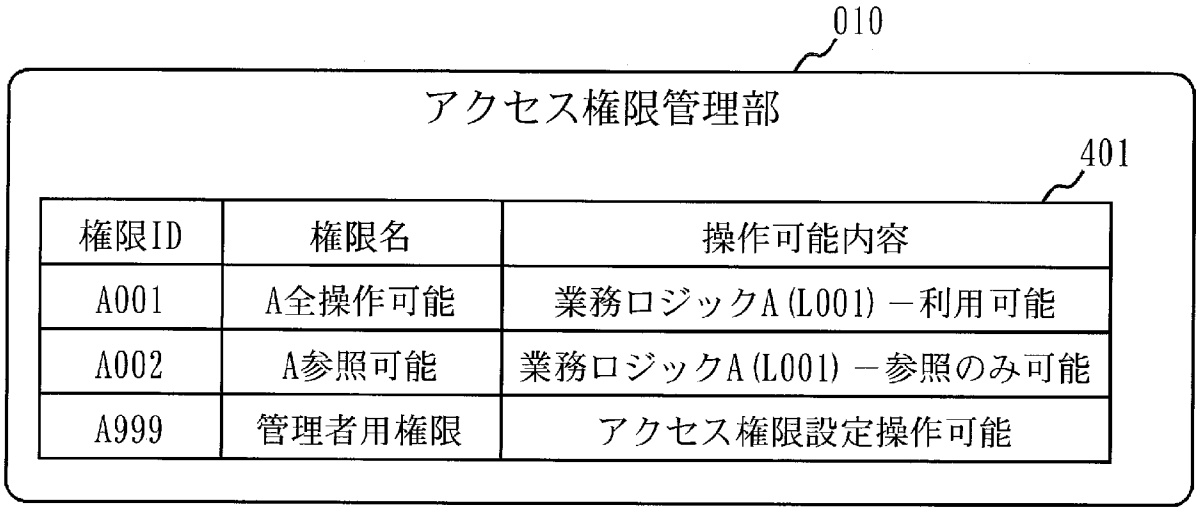


[図4]



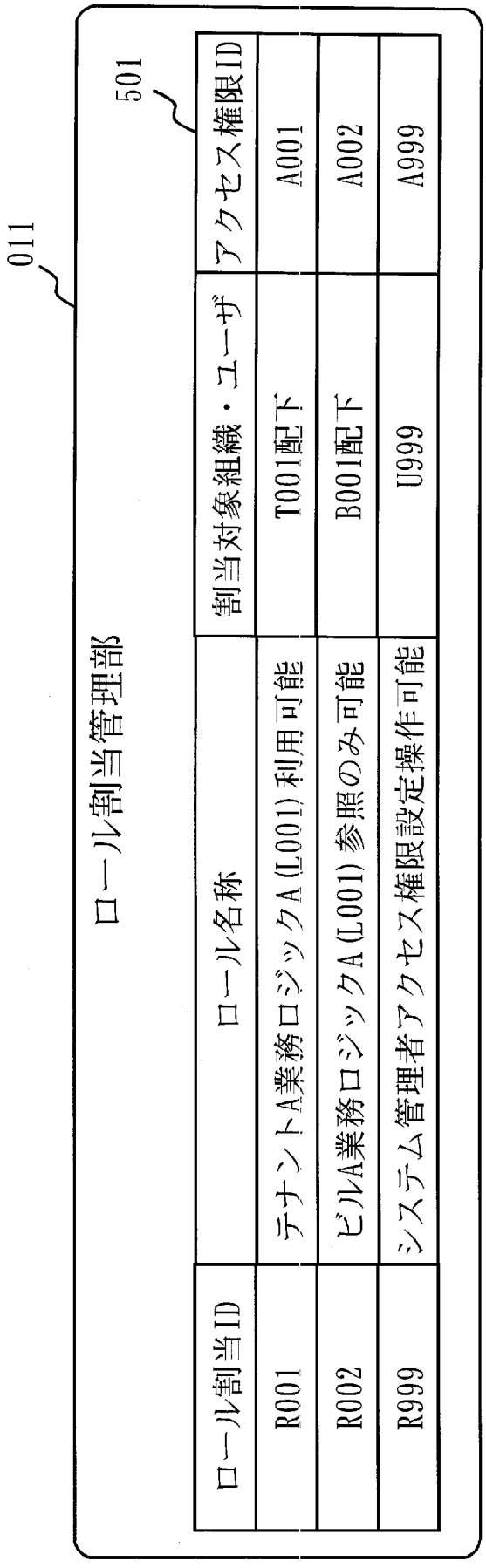
ユーザID	名称	ユーザ所属情報	パスワード
		所属組織	
U001	ユーザA	ORG001	aaa
U002	ユーザB	ORG002	bbb
U003	ユーザC	ORG003	ccc
U999	システム管理	-	sys

[図5]

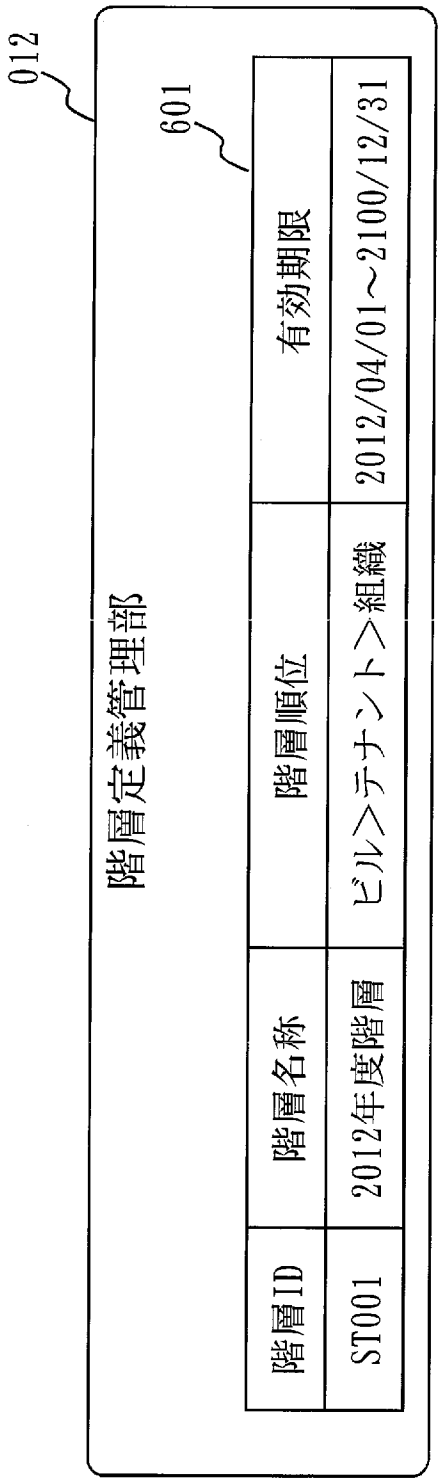


権限ID	権限名	操作可能内容
A001	A全操作可能	業務ロジックA(L001)－利用可能
A002	A参照可能	業務ロジックA(L001)－参照のみ可能
A999	管理者用権限	アクセス権限設定操作可能

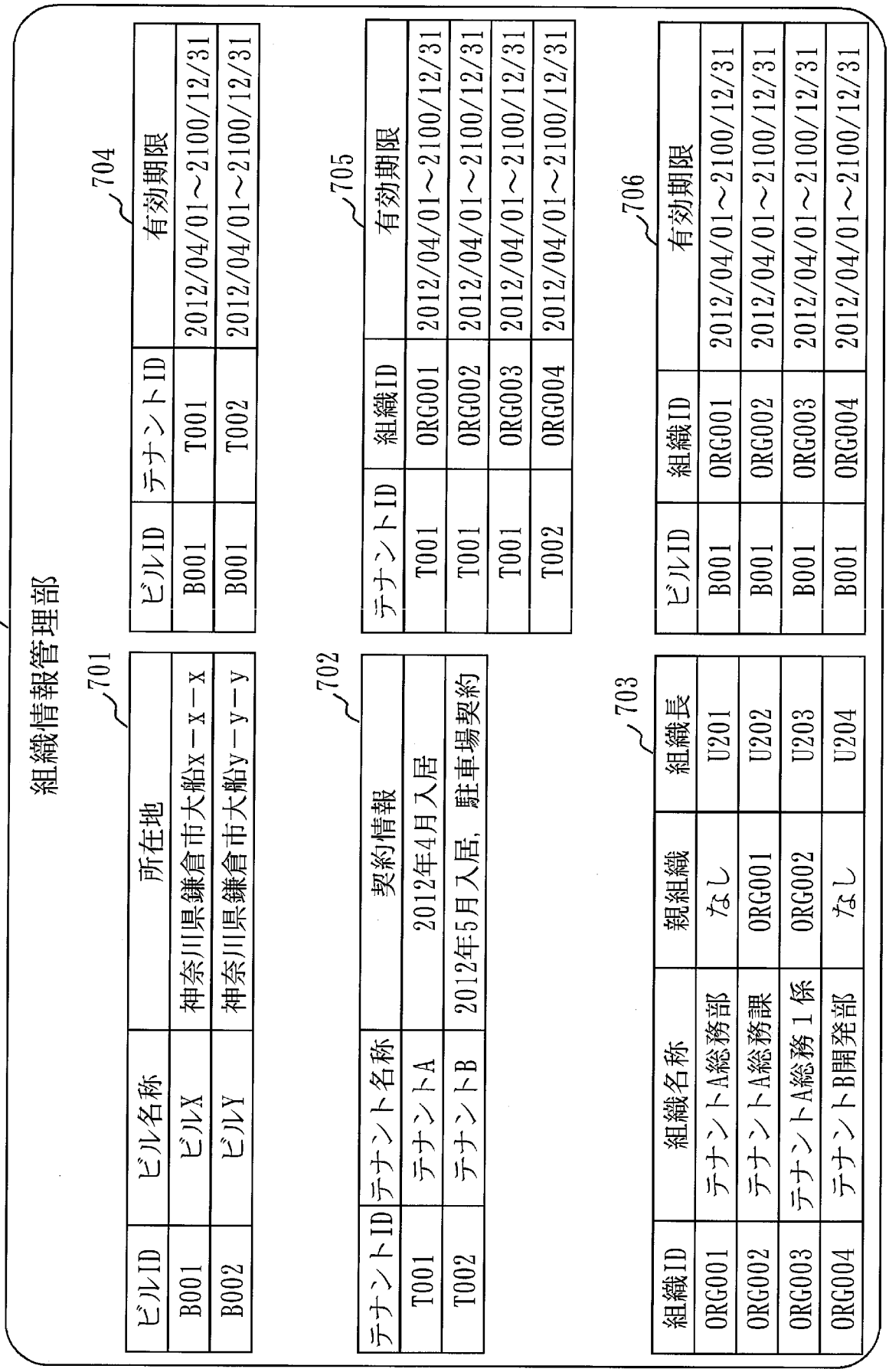
[図6]


011
ロール割当管理部
501
ロール割当ID
ロール名称
割当対象組織・ユーザ
アクセス権限ID
R001
テナントA業務ロジックA(L001)利用可能
T001配下
A001
R002
ビルA業務ロジックA(L001)参照のみ可能
B001配下
A002
R999
システム管理者アクセス権限設定操作可能
U999
A999

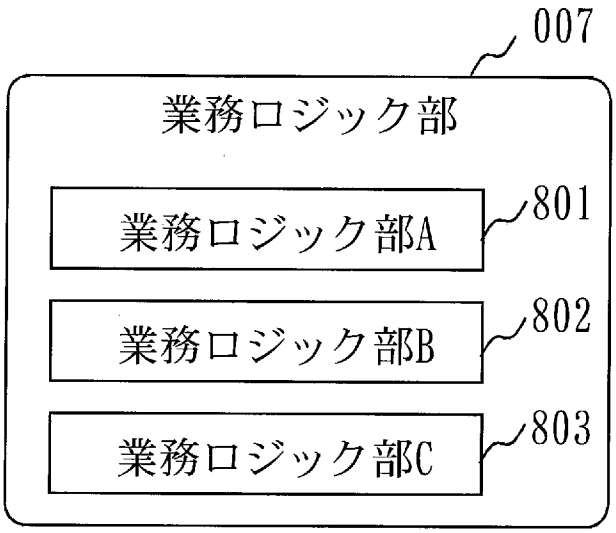
[図7]


012
601
階層定義管理部
階層ID
階層名称
階層順位
有効期限
ST001
2012年度階層
ビル＞テナント＞組織
2012/04/01～2100/12/31

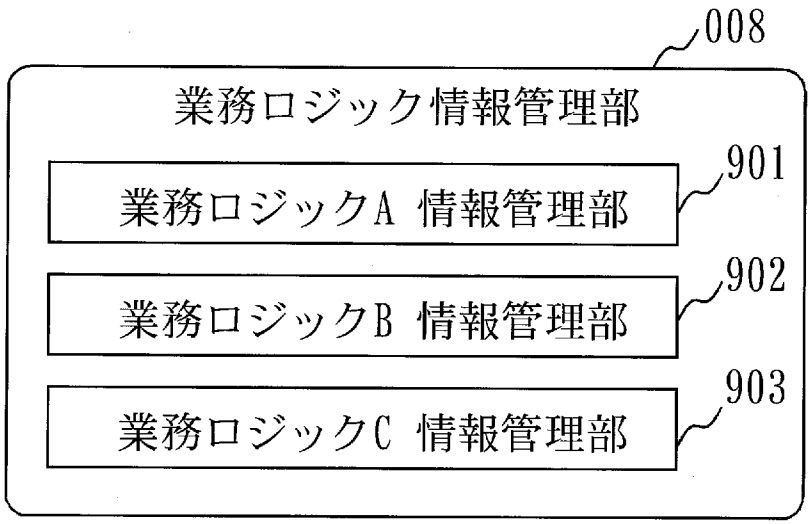
[図8]


013
組織情報管理部
701
ビルID | ビル名称 | 所在地
B001 | ビルX | 神奈川県鎌倉市大船x－x－x
B002 | ビルY | 神奈川県鎌倉市大船y－y－y
702
テナントID | テナント名称 | 契約情報
T001 | テナントA | 2012年4月入居
T002 | テナントB | 2012年5月入居，駐車場契約
703
組織ID | 組織名称 | 親組織 | 組織長
ORG001 | テナントA総務部 | なし | U201
ORG002 | テナントA総務課 | ORG001 | U202
ORG003 | テナントA総務１係 | ORG002 | U203
ORG004 | テナントB開発部 | なし | U204
704
ビルID | テナントID | 有効期限
B001 | T001 | 2012/04/01～2100/12/31
B001 | T002 | 2012/04/01～2100/12/31
705
テナントID | 組織ID | 有効期限
T001 | ORG001 | 2012/04/01～2100/12/31
T001 | ORG002 | 2012/04/01～2100/12/31
T001 | ORG003 | 2012/04/01～2100/12/31
T002 | ORG004 | 2012/04/01～2100/12/31
706
ビルID | 組織ID | 有効期限
B001 | ORG001 | 2012/04/01～2100/12/31
B001 | ORG002 | 2012/04/01～2100/12/31
B001 | ORG003 | 2012/04/01～2100/12/31
B001 | ORG004 | 2012/04/01～2100/12/31

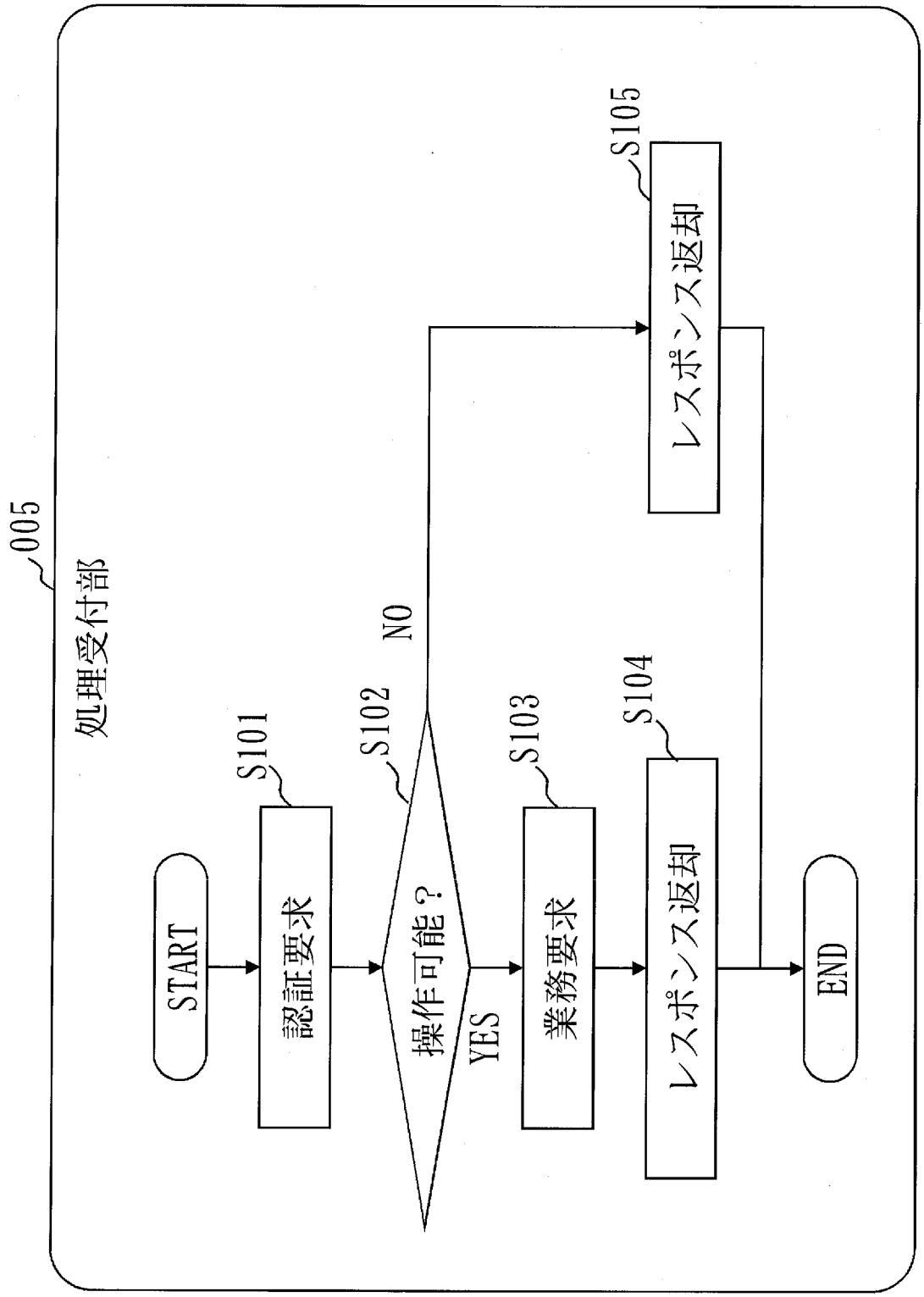
[図9]


007
業務ロジック部
業務ロジック部A
801
業務ロジック部B
802
業務ロジック部C
803

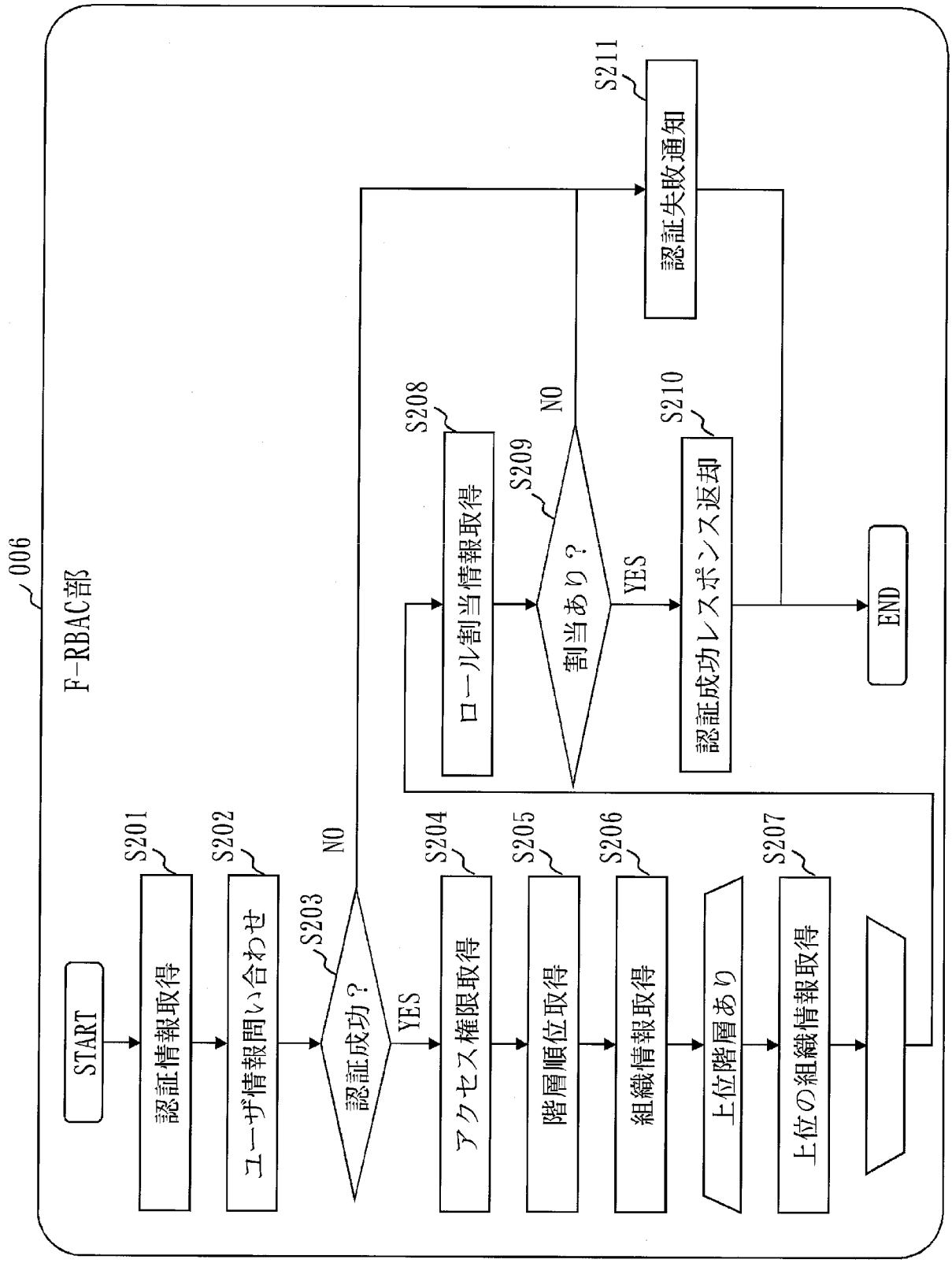
[図10]


008
業務ロジック情報管理部
業務ロジックA 情報管理部
901
業務ロジックB 情報管理部
902
業務ロジックC 情報管理部
903

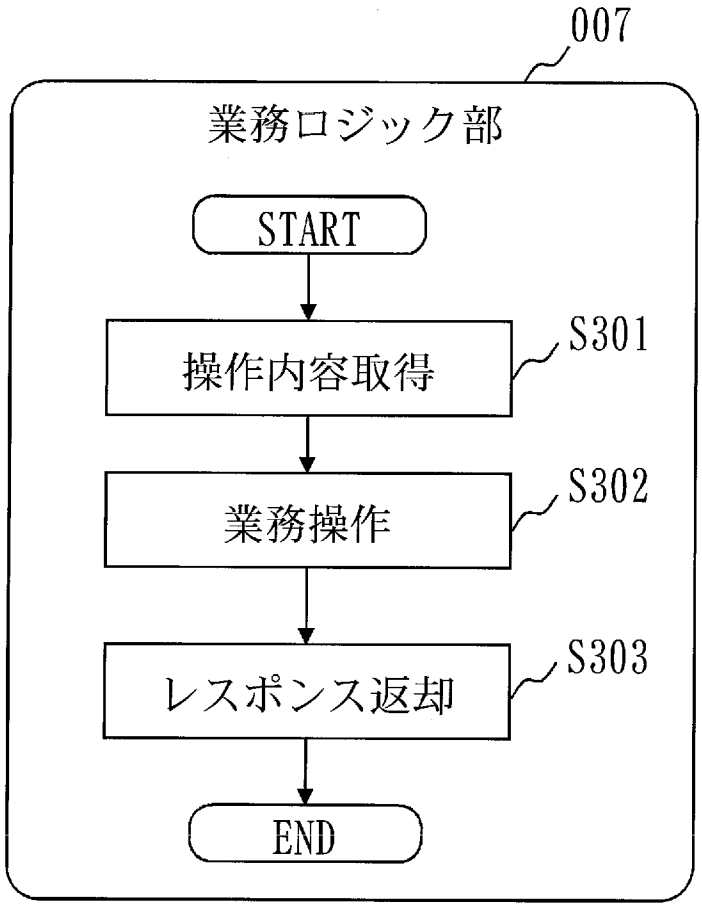
[図11]


005
処理受付部
START
S101
認証要求
S102
操作可能？
NO
YES
S103
業務要求
S104
レスポンス返却
S105
レスポンス返却
END

[図12]


006
F-RBAC部
START
S201
認証情報取得
S202
ユーザ情報問い合わせ
S203
認証成功？
NO
YES
S204
アクセス権限取得
S205
階層順位取得
S206
組織情報取得
上位階層あり
S207
上位の組織情報取得
S208
ロール割当情報取得
S209
割当あり？
NO
YES
S210
認証成功レスポンス返却
S211
認証失敗通知
END

[図13]



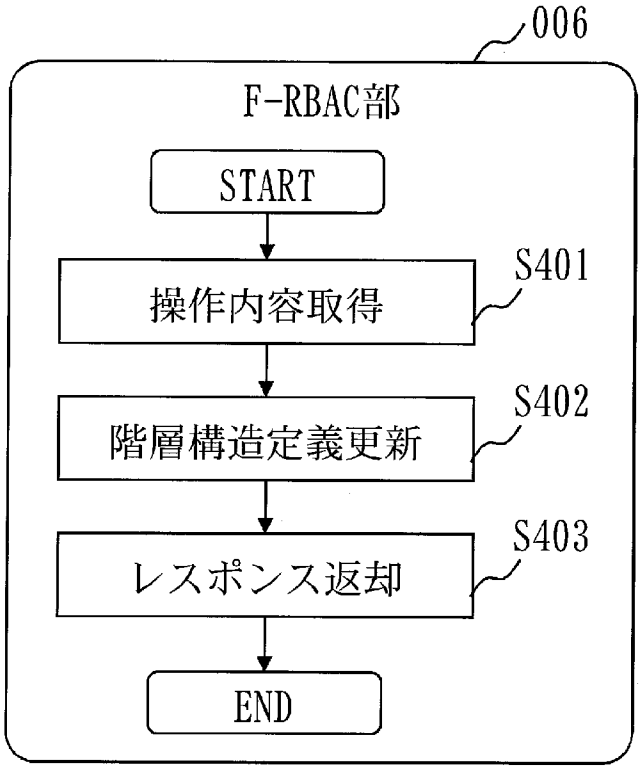
[図14]

1301

階層構造変更要求	
通信ヘッダ	From ： 端末000 To ： アクセス制御装置004
認証情報	ユーザID ： U999 パスワード ： sys
操作内容	階層構造変更

1302
1303
1304

[図15]



[図16]

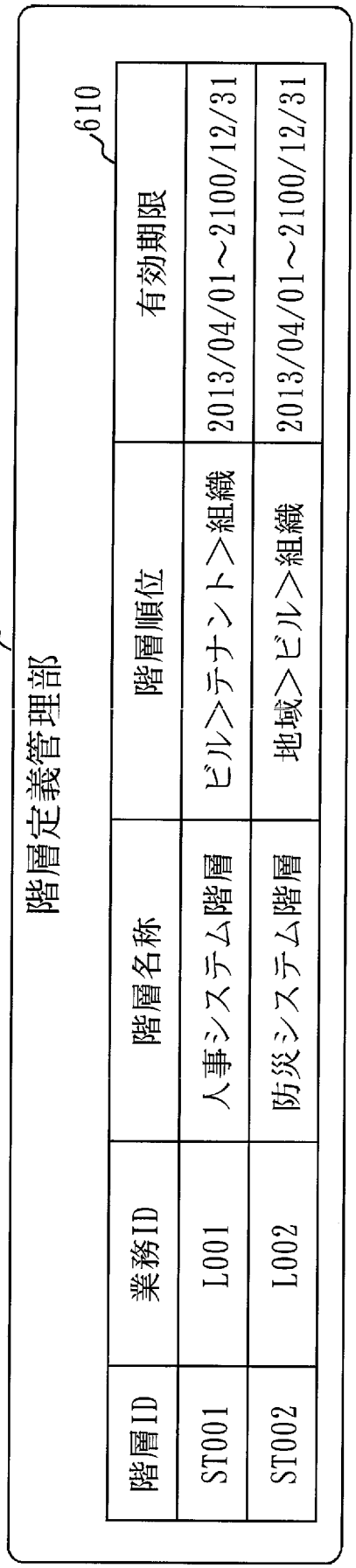
012

階層定義管理部

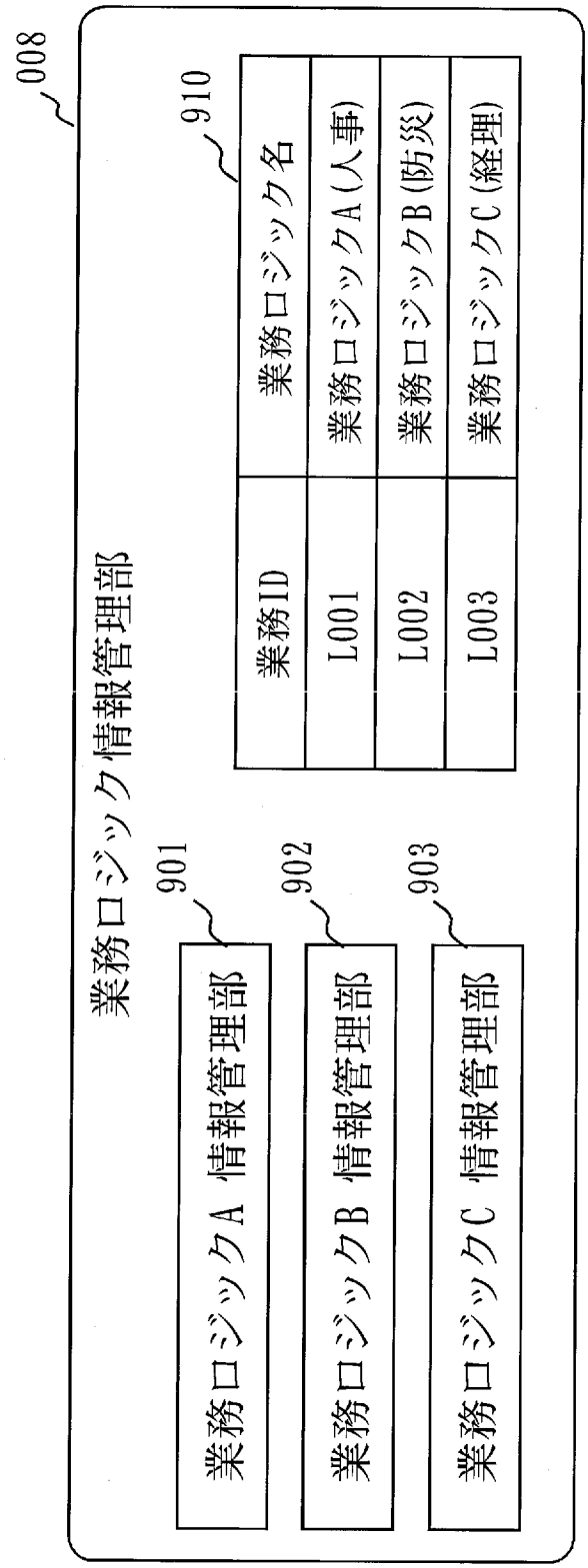
602

階層ID	階層名称	階層順位	有効期限
ST001	2012年度階層	ビル＞テナント＞組織	2012/04/01～2013/03/31
ST002	2013年度階層	テナント＞ビル＞組織	2013/04/01～2100/12/31

[図17]


012
階層定義管理部
610
階層ID
業務ID
階層名称
階層順位
有効期限
ST001
L001
人事システム階層
ビル>テナント>組織
2013/04/01～2100/12/31
ST002
L002
防災システム階層
地域>ビル>組織
2013/04/01～2100/12/31

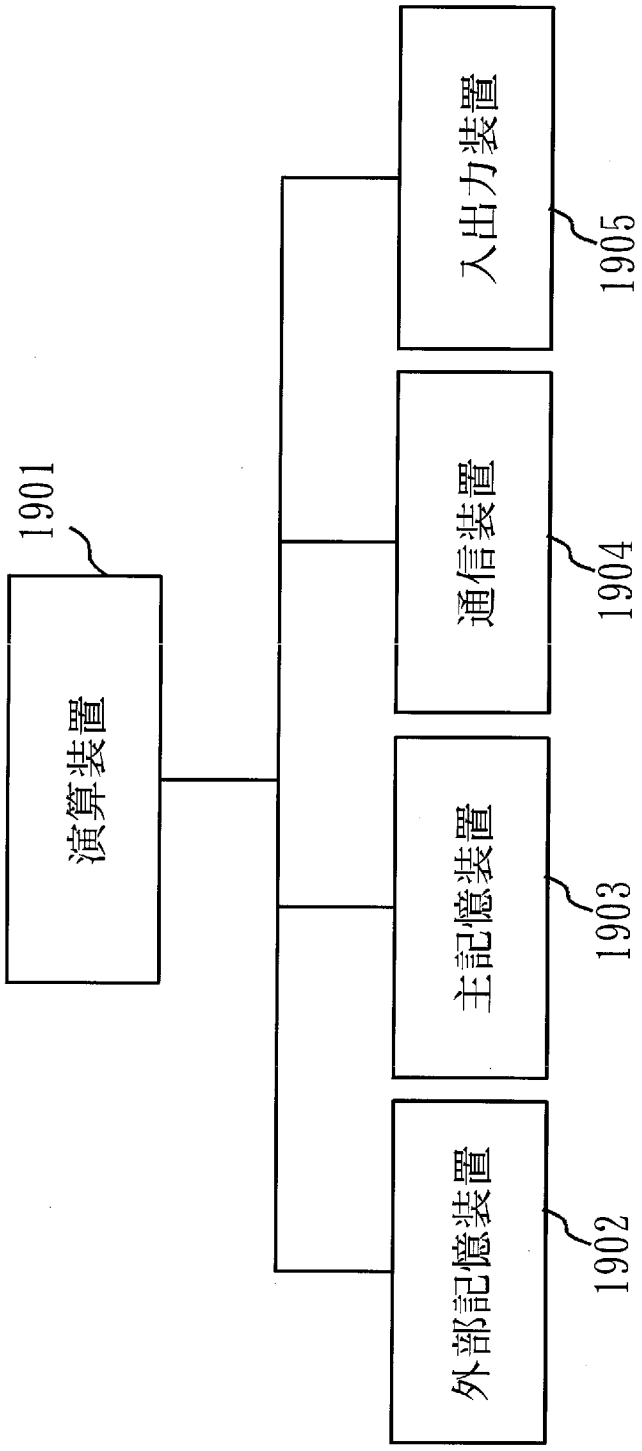
[図18]


008
業務ロジック情報管理部
901
業務ロジックA 情報管理部
902
業務ロジックB 情報管理部
903
業務ロジックC 情報管理部
910
業務ID
業務ロジック名
L001
業務ロジックA(人事)
L002
業務ロジックB(防災)
L003
業務ロジックC(経理)

[図19]

	所属組織	所属テナント	所属ビル
U001	ORG001	T001	B001
U002	ORG002	T002	B002
U003	ORG003	T001	B001

[図20]



INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2014/052851

A. CLASSIFICATION OF SUBJECT MATTER
G06F21/62(2013.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F21/62

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2014
Kokai Jitsuyo Shinan Koho	1971-2014	Toroku Jitsuyo Shinan Koho	1994-2014

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2011-76569 A (Ariel Networks, Inc.), 14 April 2011 (14.04.2011), claim 1; paragraphs [0040] to [0052]; fig. 2 to 4 (Family: none)	1-8
A	JP 2008-210376 A (Hitachi Software Engineering Co., Ltd.), 11 September 2008 (11.09.2008), paragraphs [0023] to [0039] (Family: none)	1-8
A	JP 2007-172154 A (Mitsubishi Space Software Co., Ltd.), 05 July 2007 (05.07.2007), paragraphs [0061] to [0069]; fig. 7 to 9 (Family: none)	1-8

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search 02 May, 2014 (02.05.14)	Date of mailing of the international search report 13 May, 2014 (13.05.14)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2014/052851

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2011/0213789 A1 (Kedar Doshi et al.), 01 September 2011 (01.09.2011), claims 1 to 3 (Family: none)	1-8

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１４／０５２８５１

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　G06F21/62(2013.01)i

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.　G06F21/62

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２０１４年
日本国実用新案登録公報	１９９６－２０１４年
日本国登録実用新案公報	１９９４－２０１４年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
A	JP 2011-76569 A (アリエル・ネットワーク株式会社) 2011.04.14, 請求項 1,[0040]-[0052],図 2-図 4 (ファミリーなし)	1-8
A	JP 2008-210376 A (日立ソフトウエアエンジニアリング株式会社) 2008.09.11, [0023]-[0039] (ファミリーなし)	1-8
A	JP 2007-172154 A (三菱スペース・ソフトウエア株式会社) 2007.07.05, [0061]-[0069],図 7-図 9 (ファミリーなし)	1-8

☑　Ｃ欄の続きにも文献が列挙されている。

☐　パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
０２．０５．２０１４	１３．０５．２０１４

国際調査機関の名称及びあて先
日本国特許庁（ＩＳＡ／ＪＰ）
郵便番号１００－８９１５
東京都千代田区霞が関三丁目４番３号

特許庁審査官（権限のある職員）　５Ｓ　９５５５
宮司　卓佳
電話番号　０３－３５８１－１１０１　内線　３５４６

C（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
A	US 2011/0213789 A1 (Kedar Doshi et al.) 2011.09.01, claim.1-claim.3 (ファミリーなし)	1-8