

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第5546486号
(P5546486)

(45) 発行日 平成26年7月9日(2014.7.9)

(24) 登録日 平成26年5月23日(2014.5.23)

(51) Int.Cl. F I
G06F 21/31 (2013.01) G O 6 F 21/20 1 3 1 A
G06Q 10/06 (2012.01) G O 6 Q 10/06 1 1 0

請求項の数 4 (全 17 頁)

<p>(21) 出願番号 特願2011-63494 (P2011-63494) (22) 出願日 平成23年3月23日 (2011. 3. 23) (65) 公開番号 特開2012-94106 (P2012-94106A) (43) 公開日 平成24年5月17日 (2012. 5. 17) 審査請求日 平成25年7月23日 (2013. 7. 23) (31) 優先権主張番号 特願2010-214635 (P2010-214635) (32) 優先日 平成22年9月27日 (2010. 9. 27) (33) 優先権主張国 日本国(JP)</p>	<p>(73) 特許権者 501158538 三菱電機インフォメーションテクノロジー株式会社 東京都港区芝浦四丁目6番8号 (73) 特許権者 000006013 三菱電機株式会社 東京都千代田区丸の内二丁目7番3号 (74) 代理人 100099461 弁理士 溝井 章司 (72) 発明者 木幡 康博 東京都港区芝浦四丁目15番33号 三菱電機インフォメーションテクノロジー株式会社内</p>
---	---

最終頁に続く

(54) 【発明の名称】 情報処理装置及びプログラム

(57) 【特許請求の範囲】

【請求項1】

特定のシステム利用権限が指定されているロールの識別子であるロールID (I d e n t i f i c a t i o n) と当該ロールが割り付けられる組織の識別子である組織IDとが記述されるロール割付け情報を記憶するロール割付け情報記憶装置と、

所定の日時において組織IDが変更になる組織に対して変更前の組織IDと変更後の組織IDと変更日時とが記述されるID変更情報を記憶するID変更情報記憶装置とに接続されている情報処理装置であって、

前記ロール割付け情報記憶装置に記憶されているロール割付け情報のうち、前記ID変更情報に記述されている変更前の組織IDが記述されているロール割付け情報を抽出する情報抽出部と、

前記情報抽出部により抽出されたロール割付け情報に記述されているロールIDと前記ID変更情報に記述されている変更後の組織IDとが記述され、前記ID変更情報に記述されている変更日時にて有効になるロール割付け情報を新たに生成し、前記ID変更情報に記述されている変更前の組織IDが記述されている既存のロール割付け情報が前記ID変更情報に記述されている変更日時に無効化されるようにする情報管理部とを有することを特徴とする情報処理装置。

【請求項2】

前記情報処理装置は、

ロールIDと当該ロールIDのロールが割り付けられるユーザの識別子であるユーザID

Dとが記述されるロール割付け情報を記憶するロール割付け情報記憶装置と、

所定の日時においてユーザIDが変更になるユーザに対して変更前のユーザIDと変更後のユーザIDと変更日時とが記述されるID変更情報を記憶するID変更情報記憶装置とに接続され、

前記情報抽出部は、

前記ロール割付け情報記憶装置に記憶されているロール割付け情報のうち、前記ID変更情報に記述されている変更前のユーザIDが記述されているロール割付け情報を抽出し、

前記情報管理部は、

前記情報抽出部により抽出されたロール割付け情報に記述されているロールIDと前記ID変更情報に記述されている変更後のユーザIDとが記述され、前記ID変更情報に記述されている変更日時にて有効になるロール割付け情報を新たに生成し、前記ID変更情報に記述されている変更前のユーザIDが記述されている既存のロール割付け情報が前記ID変更情報に記述されている変更日時に無効化されるようにすることを特徴とする請求項1に記載の情報処理装置。

10

【請求項3】

特定のシステム利用権限が指定されているロールの識別子であるロールID (Identification) と当該ロールが割り付けられる組織の識別子である組織IDとが記述されるロール割付け情報を記憶するロール割付け情報記憶装置と、

所定の日時において組織IDが変更になる組織に対して変更前の組織IDと変更後の組織IDと変更日時とが記述されるID変更情報を記憶するID変更情報記憶装置とに接続されているコンピュータに、

20

前記ロール割付け情報記憶装置に記憶されているロール割付け情報のうち、前記ID変更情報に記述されている変更前の組織IDが記述されているロール割付け情報を抽出する情報抽出処理と、

前記情報抽出処理により抽出されたロール割付け情報に記述されているロールIDと前記ID変更情報に記述されている変更後の組織IDとが記述され、前記ID変更情報に記述されている変更日時にて有効になるロール割付け情報を新たに生成し、前記ID変更情報に記述されている変更前の組織IDが記述されている既存のロール割付け情報が前記ID変更情報に記述されている変更日時に無効化されるようにする情報管理処理とを実行させることを特徴とするプログラム。

30

【請求項4】

前記情報処理装置は、

組織の識別子である組織IDと、当該組織に関係があるが当該組織に正規には所属していない非正規ユーザの識別子である非正規ユーザIDとが対応付けられる非正規ユーザ組織割付け情報を記憶する非正規ユーザ組織割付け情報記憶装置に接続され、

前記情報管理部は、

前記ID変更情報に記述されている変更前の組織IDと非正規ユーザ組織割付け情報において対応付けられている非正規ユーザIDと、前記ID変更情報に記述されている変更後の組織IDとが対応付けられ、前記ID変更情報に記述されている変更日時にて有効になる新たな非正規ユーザ組織割付け情報を生成し、

40

前記ID変更情報に記述されている変更前の組織IDが記述されている既存の非正規ユーザ組織割付け情報が前記ID変更情報に記述されている変更日時にて無効化されるようにすることを特徴とする請求項1又は2に記載の情報処理装置。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、企業等の組織において業務システムに対する利用権限や入退室管理システムに対する通行権限等を効率的に管理する技術に関する。

【背景技術】

50

【 0 0 0 2 】

企業等における人事DB (Database) では、個人情報、組織情報、配属情報を管理している。

また、ID (Identification) 管理サーバは、一般的に、人事DBと連携し、個人情報、組織情報、配属情報、人事異動情報を自動的に受信できる。

また、IC (Integrated Circuit) カード業者からICカードのID情報をCSV (Comma Separated Values) ファイルで受け取り、情報を取り込み、個人とカードの割り付けを行うこともできる。

ID管理サーバでは、個人情報、組織情報、配属情報、ICカード情報、各種業務システムのための個人に割り付ける利用権限を管理する。

10

各種業務システムサーバでは、ID管理サーバから個人情報、ICカード情報、利用権限を受信し、例えば、個人がもつICカードで利用可能な権限を管理する。

ID管理サーバでは、利用権限を各個人毎に設定できるが、個人毎に設定すると、人事異動等による権限の変更処理が煩雑となり、管理負荷が高くなる。

この点に関し、利用権限を組織や役職に割り当てることで、人事異動による組織対応での権限の変更に対して、利用権限の設定処理の自動化を図ることができる。

このような利用権限の管理を効率的に行う技術として、例えば、特許文献1に記載の技術がある。

【 先行技術文献 】

【 特許文献 】

20

【 0 0 0 3 】

【 特許文献1 】 特開 2 0 0 7 - 1 7 2 3 7 9 号公報

【 発明の概要 】

【 発明が解決しようとする課題 】

【 0 0 0 4 】

企業等においては、組織の改編等により、組織の実体と同じでありながら組織IDや組織名が変更となることがある。

このような場合、システムとしては、変更前の組織と変更後の組織は、別組織として扱われるので、これまで利用できていた業務システムを継続して利用できるようにするためには、新しい組織IDに対して、以前と同じ権限が割りつけられるように権限割り付けの再設定が必要となる。

30

特許文献1の技術では、このような組織の実体と同じであるが組織IDが変更になる場合には対応しておらず、特許文献1によっても人手による権限割り付けの再設定が必要となる。

大きな企業では、組織の数が多く、組織改編時の権限の割り付け処理の負荷が大きい。

【 0 0 0 5 】

本発明は、上記の事情に鑑みたものであり、組織の実体と同じであるが組織IDが変更になる場合に、新しい組織IDに対して権限を割り付ける際の処理負担を軽減することを主な目的とする。

【 課題を解決するための手段 】

40

【 0 0 0 6 】

本発明に係る情報処理装置は、

特定のシステム利用権限が指定されているロールの識別子であるロールID (Identification) と当該ロールが割り付けられる組織の識別子である組織IDとが記述されるロール割付け情報を記憶するロール割付け情報記憶装置と、

所定の日時において組織IDが変更になる組織に対して変更前の組織IDと変更後の組織IDと変更日時とが記述されるID変更情報を記憶するID変更情報記憶装置とに接続されている情報処理装置であって、

前記ロール割付け情報記憶装置に記憶されているロール割付け情報のうち、前記ID変更情報に記述されている変更前の組織IDが記述されているロール割付け情報を抽出する

50

情報抽出部と、

前記情報抽出部により抽出されたロール割付け情報に記述されているロールIDと前記ID変更情報に記述されている変更後の組織IDとが記述され、前記ID変更情報に記述されている変更日時にて有効になるロール割付け情報を新たに生成し、前記ID変更情報に記述されている変更前の組織IDが記述されている既存のロール割付け情報が前記ID変更情報に記述されている変更日時に無効化されるようにする情報管理部とを有することを特徴とする。

【発明の効果】

【0007】

本発明によれば、ID変更情報に基づき、変更前の組織IDに割り付けられているロールIDが変更後の組織IDに割り付けられ変更日時に有効になる新たなロール割付け情報を生成し、また、既存のロール割付け情報を変更日時において無効化するので、変更後の組織IDとロールIDとの割り付けを変更日時から有効にすることができ、新しい組織IDに対して権限を割り付ける際の処理負担を軽減することができる。

10

【図面の簡単な説明】

【0008】

【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に係るテーブル構成例を示す図。

【図3】実施の形態1に係るテーブル要素の例を示す図。

【図4】実施の形態1に係るID変更組織テーブルの例を示す図。

20

【図5】実施の形態1に係るロール割付け更新例を示す図。

【図6】実施の形態1に係るID管理システムの動作例を示すフローチャート図。

【図7】実施の形態1に係るID管理システムの動作例を示すフローチャート図。

【図8】実施の形態1に係るID管理システムのハードウェア構成例を示す図。

【図9】実施の形態2に係る非正規ユーザ組織割付けテーブルの更新を説明する図。

【発明を実施するための形態】

【0009】

実施の形態1 .

本実施の形態では、実体が同じでありながら組織IDが変更になる組織に対して、旧組織IDと新組織IDとを対応付けておき、組織改編時に対応付けに基づき、各種業務システムの利用権限を自動的に新組織に割り付ける技術を説明する。

30

【0010】

図1は、本実施の形態に係るシステム構成例を示す。

【0011】

ID管理システム100は、組織又は個人に対して業務システム330の利用権限を割り当てる。

より詳しくは、ID管理システム100は、組織又は個人に対してロールを設定し、ロールごとに業務システム330の利用権限を割り当てる。

ID管理システム100は情報処理装置の例である。

なお、ID管理システム100の内部構成については後述する。

40

【0012】

ID管理システム100は、ID管理システムDB(Database)150と接続されている。

ID管理システムDB150は図2及び図3に示す各種テーブル、更には、図4に示すID変更組織テーブルを格納している。

図2及び図3に示すテーブル、図4に示すID変更組織テーブルの詳細は後述する。

なお、ID管理システムDB150は、ロール割付け情報記憶装置及びID変更情報記憶装置の例である。

また、ID管理システム100は、ディスプレイ装置200、キーボード210に接続されている。

50

【 0 0 1 3 】

また、ID管理システム100は、LAN(Local Area Network)300を介して人事DBシステム310、ユーザ端末装置320、業務システム330に接続されている。

人事DBシステム310は、個人情報、組織情報、配属情報を管理している。

ユーザ端末装置320は、ユーザ(従業員等)が利用する端末装置であり、業務システム330にログインし、業務システム330のデータやリソースを利用する。

業務システム330は、業務に用いられるコンピュータシステムであり、アクセスのあったユーザに認められている利用権限の範囲内でユーザにサービスを提供する。

業務システム330は、業務システムDB340に接続されている。

ユーザ端末装置320及び業務システム330は、複数存在する。

10

【 0 0 1 4 】

ID管理システム100では、図2及び図3に示すテーブルを利用し、各業務システム330についての利用権限を管理する。

図2はテーブル間の連携を示しており、図3は各テーブルのテーブル要素の例を示している。

図中、ロールとは、複数の組織や複数の個人をグループ化するための器として利用するもので、共通のロールが設定される組織や個人は、共通の業務システム330に対して、共通の利用権限を持つ。

例えば、複数の組織(個人)をロール(R1)に設定し、このロール(R1)に業務システム(K1)の特定の機能の利用を可能にする利用権限を割り付ける。

このようにすることで、ロール(R1)が設定されている組織に属する個人は原則として一律に、業務システム(K1)の特定の機能についての利用権限が与えられる。

このように、ロールを用いることにより、組織ごと、個人ごとに利用権限を設定することに比べて利用権限の割付け負担が軽減される。

20

【 0 0 1 5 】

図2及び図3において、ユーザテーブルには各ユーザ(従業員等)の情報が記述されている。

組織テーブルには、各組織の情報が記述されている。

ユーザと組織は、組織割付けテーブルにより、対応付けられている。

また、ロールテーブルには、各ロールの情報が記述されている。

組織とロールは、ロール割付け情報により、対応付けられている。

また、ユーザとロールが、ロール割付け情報により対応付けられる場合もある。

システムテーブルには、各業務システムの情報が記述されている。

ロールとシステムは、システム割付けテーブルにより、対応付けられている。

図2に示すように、例えば、ユーザ(P1)は、組織割付けテーブル(P1-a)により組織(a)と対応付けられている(組織(a)に属している)。

更に、組織(a)は、ロール割付けテーブル(a-R1)によりロール(R1)に対応付けられ、ロール(R1)はシステム割付けテーブル(R1-K1)によりシステム(K1)と対応付けられている。

30

40

この結果、ユーザ(P1)は、ロール(R1)に割り当てられている利用権限の範囲内でシステム(K1)を利用することができる。

なお、ロール(R1)、ロール(R2)、ロール(R3)は、それぞれシステム(K1)に対応付けられているが、システム(K1)で許可されている利用権限が異なる。システムK1には、実際の業務システムと接続するための接続先IPアドレスが、設定されており、この接続先に、システムK1に割り付いているロールの情報とロールに割り付いているユーザの情報を送信することで、業務システム側では、利用可能なユーザとロールに対応した利用権限を設定できる。

【 0 0 1 6 】

各テーブルのテーブル要素は、図3に示す通りであるが、本実施の形態に密接するテ

50

ブルがロール割付けテーブルであるため、ロール割付けテーブルのテーブル要素について説明する。

ロールIDは、ロールテーブルに含まれるロールIDであり、組織/ユーザIDは、組織テーブルに含まれる組織ID又はユーザテーブルに含まれるユーザIDである。

ロール割付けテーブルにおいてロールIDに対応するロールと組織/ユーザIDに対応する組織/ユーザが対応付けられる。

有効開始日時はロールと組織(ユーザ)の対応付けが有効になる日時であり、有効終了日時はロールと組織(ユーザ)の対応付けが無効になる日時である。

【0017】

ユーザが人事異動でロール(R1)に該当する組織に配属になったり、別組織に異動になった時には、人事異動に対応して、業務システムに個人情報配信することで、人事異動時に自動的に利用権限が設定される。

しかしながら、実質的には同じ組織でありながら組織名や組織IDが変更になる場合がある。

このような場合には、ロールに割りつけられる組織が別組織として扱われるために、ロール割り付けを再設定する必要がある。

組織の数が多く、業務システムが多い企業では、利用権限の再設定のための管理設定負荷が高くなる。

【0018】

この点について、本実施の形態に係るID管理システム100は、例えば図4に示すようなID変更組織テーブルをID管理システムDB150に保持し、ID変更組織テーブルを用いて、組織改編時に、新しい組織名、組織IDに対して以前と同じ権限を割り付ける処理を自動に行う。

図4のID変更組織テーブルは、組織改編時に組織名は変更されないが組織IDが変更になる組織についてのテーブルである。

図4において、新組織IDは、有効開始日時から新たに使用される変更後の組織IDである。

元組織IDは、新組織IDの有効開始日時の直前まで使用される変更前の組織IDである。

有効開始日時は、組織改編日時、換言すれば、元組織IDから新組織IDに変更になる変更日時(例えば、4月1日0時0分0秒)である。

有効終了日時は、新組織IDの使用が中止になる日時である。

通常は、次の組織改編が具体的になるまで新組織IDの有効終了日時は未定である。

このため、有効終了日時が未定の間は、例えばID管理システム100で許容される最大の日時(例えば、9999年12月31日23時59分59秒)が設定される。

なお、ID変更組織テーブルはID変更情報の例である。

【0019】

以上の説明を前提に、本実施の形態に係るID管理システム100の内部構成について説明する。

【0020】

制御部101は、通信部102、入出力部103、組織変更マッピング情報設定部104、ロール設定部105、割付け設定部106、ロール割付け変更部107、権限情報出力部108、ID管理システムDB150の各要素の動作及び要素間のデータのやり取りを制御する。

【0021】

通信部102は、ID管理システムDB150、人事DBシステム310、業務システム330と通信を行う。

【0022】

入出力部103は、キーボード210から情報を入力し、また、ディスプレイ装置200に情報を出力する。

10

20

30

40

50

【 0 0 2 3 】

人事情報設定部 1 0 9 は、人事 D B システム 3 1 0 からユーザ情報、組織情報、配属情報を人事異動に伴い随時通信部 1 0 2 からファイルとして情報を取り込み、図 2 に示すユーザテーブル、組織テーブル、組織割り付けテーブルを作成し、I D 管理システム D B 1 5 0 に登録する。

組織変更マッピング情報設定部 1 0 4 は、図 4 に例示する I D 変更組織テーブルを生成し、生成した I D 変更組織テーブルを I D 管理システム D B 1 5 0 に格納する。

より具体的には、I D 管理システム 1 0 0 のオペレータによりキーボード 2 1 0 を用いて、又はファイル読み込みにより入力された図 4 の各要素（新組織 I D、組織名、有効開始日時、有効終了日時、元組織 I D）を入出力部 1 0 3 から取得して、I D 変更組織テーブルを生成する。組織変更マッピング情報の入力、人事システム 3 1 0 で行われ、ファイルとして通信部 1 0 2 を経由して組織変更マッピング情報設定部 1 0 4 に取り込まれ、I D 変更組織テーブルを生成しても良い。

10

そして、生成した I D 変更組織テーブルを通信部 1 0 2 を介して I D 管理システム D B 1 5 0 に格納する。

【 0 0 2 4 】

ロール設定部 1 0 5 は、図 2 に例示したロールを生成する。

より具体的には、I D 管理システム 1 0 0 のオペレータによりキーボード 2 1 0 を用いて、又はファイル読み込みにより入力された図 3 のロールテーブルの各要素（ロール I D、ロール名、有効開始日時、有効終了日時）を入出力部 1 0 3 から取得して、ロールテーブルを生成する。

20

そして、生成したロールテーブルを通信部 1 0 2 を介して I D 管理システム D B 1 5 0 に格納する。

【 0 0 2 5 】

割付け設定部 1 0 6 は、図 2 及び図 3 に例示した割付けテーブル（組織割付けテーブル、ロール割付けテーブル、システム割付けテーブル）を生成する。

より具体的には、I D 管理システム 1 0 0 のオペレータによりキーボード 2 1 0 を用いて、又はファイル読み込みにより入力された図 3 の各割付けテーブルの各要素（ユーザ I D、組織 I D、ロール I D、システム I D、有効開始日時、有効終了日時等）を入出力部 1 0 3 から取得して、各割付けテーブルを生成する。

30

そして、生成した各割付けテーブルを通信部 1 0 2 を介して I D 管理システム D B 1 5 0 に格納する。

【 0 0 2 6 】

ロール割付け変更部 1 0 7 は、図 4 の I D 変更組織テーブルに示される新組織 I D に対する新たなロール割付けテーブルを生成する。

また、図 4 の I D 変更組織テーブルに示される元組織 I D に対するロール割付けテーブルを無効にする。

つまり、ロール割付け変更部 1 0 7 は、ロール割付け情報（図 3）のうち、I D 変更組織テーブル（図 4）に記述されている元組織 I D が記述されているロール割付け情報を抽出する。

40

そして、ロール割付け変更部 1 0 7 は、抽出したロール割付け情報に記述されているロール I D と I D 変更組織テーブルに記述されている新組織 I D とが記述され、I D 変更組織テーブルに記述されている有効開始日時が有効開始日時として記述されるロール割付けテーブルのレコードを新たに生成する。

また、ロール割付け変更部 1 0 7 は、I D 変更組織テーブルに記述されている元組織 I D が記述されている既存のロール割付け情報（抽出したロール割付け情報）が I D 変更組織テーブルに記述されている有効開始日時に無効化されるようにする。

無効化の処理は、既存のロール割付け情報の有効終了日時の欄に、I D 変更組織テーブルに記載の新組織 I D の有効開始日時の直前の時刻を記述することにより行う。

例えば、新組織 I D の有効開始日時が 2 0 1 0 年 4 月 1 日 0 時 0 分 0 秒であれば、既存

50

のロール割付け情報（元組織IDが記述されているロール割付け情報）の有効終了日時の欄に2010年3月31日23時59分59秒を記述する。

なお、ロール割付け変更部107は、情報抽出部と情報管理部の例である。

【0027】

権限情報出力部108は、業務システム330に割り付いている図2のシステムテーブルから対応するロールを抽出し、ロールに割り付いているユーザとロール情報を業務システム330に通知する。業務システム330は、ID管理システム100から通知されたユーザとロールの組み合わせ情報を業務システム330利用可能ユーザとし、ロールにより、別々の利用権限（参照権限、書き込み権限等）として業務システムDB340に登録する。

10

例えば、図2に例示したシステム（K1）が業務システム330に対応しており、ユーザ（P1）がユーザ端末装置320を利用して業務システム330にログインしようとするときに、ユーザ（P1）は、ロール（R1）に対応した利用権限で業務システム330にログインできる。

【0028】

次に、図5及び図6を用いて本実施の形態に係るロール割付け変更部107の動作例を説明する。

図5は、本実施の形態に係るロール割付け更新の具体例を示し、図6は、本実施の形態に係るロール割付け変更部107の動作例を示すフローチャートである。

本実施の形態では、ロール割付け変更部107は、毎日24時よりも前の時間（例えば、23時）に図6のフローを行うものとする。

20

但し、組織改編日が特定の日（4月1日、10月1日等）に限られている場合は、組織改編日の前日（3月31日、9月31日等）の24時よりも前の時間（例えば、23時）に図6のフローを行うようにしてもよい。

以下の説明では、2010年3月31日に図6のフローを実施する例を説明する。

【0029】

図6のフローチャートにおいて、まず、ロール割付け変更部107は、ID管理システムDB150内において、有効開始日が次の日であるID変更組織テーブル（図4）を通信部102を介して検索する（情報抽出処理）（S101）。

つまり、ロール割付け変更部107は、有効開始日時が2010年4月1日0時0分0秒となっているID変更組織テーブルを検索する。

30

【0030】

該当するID変更組織テーブルを抽出した場合（S102でYES）（情報抽出処理）には、ロール割付け変更部107は、抽出したID変更組織テーブルに記述されている元組織IDが組織IDの欄に記述されているロール割付けテーブル（図3）を通信部102を介してID管理システムDB150内で検索する（S103）（情報抽出処理）。

【0031】

該当するロール割付けテーブルを抽出できない場合（S104でNO）（情報抽出処理）には、次のID変更組織テーブルを検索処理を行う。

【0032】

一方、該当するロール割付けテーブルが抽出できた場合（S104でYES）（情報抽出処理）には、ロール割付け変更部107は、抽出したロール割付けテーブルのロールIDと、S102で抽出したID変更組織テーブルに記述されている新組織IDとが記述され、S102で抽出したID変更組織テーブルに記述されている有効開始日時（2010年4月1日0時0分0秒）が有効開始日時として記述されるロール割付け情報を新たに生成する（S106）（情報管理処理）。

40

なお、有効終了日時は、例えば、システムで許容される最大の日時にする。

【0033】

また、ロール割付け変更部107は、S104で抽出したロール割付けテーブルの有効終了日時を当日（本日）の最終時刻（例えば、2010年3月31日23時59分59秒

50

)にする(S107)(情報管理処理)。

これにより、既存のロール割付けテーブルは、2010年4月1日0時0分0秒には無効になっており、代わりに、S106で生成した新たなロール割付けテーブル(新組織IDが記述されているロール割付けテーブル)が2010年4月1日0時0分0秒から有効になり、4月1日以降は、新組織IDとロールとの対応付けが用いられる。

【0034】

また、未処理のロール割り付けテーブルがある場合(S108でYES)は、ロール割付け変更部107は、未処理のID変更組織テーブルに対してS103以降の処理を行う。更に、未処理のID変更組織テーブルがある場合(S109でYES)は、ロール割付け変更部107は、未処理のID変更組織テーブルに対してS101以降の処理を行う。

10

また、未処理のID変更組織テーブルがない場合(S109でNO)は、ロール割付け変更部107は、S106で生成した新たなロール割付け情報及びS107で有効終了日時を変更した既存のロール割付け情報を通信部102を介してID管理システムDB150に格納する。

【0035】

例えば、図5(a)に示すように、組織改編前に、組織IDがaの組織がロール割付け情報(a-R1)によりロール(R1)と割り付けられている場合に、図5(b)に示すように、組織改編により組織の実体には変動がなく組織IDのみがxに変更になる例を考える。

ロール割付け変更部107は組織改編日の前日に図6に示すフローを実施し、図5(c)に示すように、組織IDの変更を反映させて、組織ID:xとロール(R1)を結び付けるロール割付け情報(x-R1)を生成する。

20

一方、組織ID:aとロール(R1)を結び付けていたロール割付け情報(a-R1)は、組織改編日には無効になっている。

このため、組織ID:aは、いずれのロールとも結び付いていない。

なお、新たな組織割付けテーブル(P1-x)及び(P2-x)は、人事情報設定部109で生成される。

【0036】

次に、本実施の形態に係る権限情報出力部108の動作例を図7に示す。

【0037】

30

権限情報出力部108は、毎日、0時0分に起動され、各業務システムに割り付けられている図3のシステムテーブルに割り付けられているロールとユーザ情報を各業務システム対応に抽出し、通信部102を介して、各業務システム330に送信する。この時に、送信されるユーザ情報としては、ユーザID、パスワード、ロールID等の情報が渡される。業務システム330側では、渡されたユーザID、パスワードで業務システム330にログインするユーザに対してのみログインを許可する。また、ユーザIDに対応するロールIDにより、利用権限を識別し、ロールIDに対応した利用権限での操作が許可される。また、毎日、0時0分に起動されることで、該当日に有効なロール割り付け情報で有効なロールに割り付けられている有効なユーザのユーザ情報とロール情報を送信することで、該当日に利用可能なユーザだけが各業務システムを利用できる。なお、有効なユーザとは、有効開始日時が現在時刻よりも前であって有効終了日時が現在時刻よりも後のユーザテーブルである。有効なロールとは、有効開始日時が現在時刻よりも前であって有効終了日時が現在時刻よりも後のロールテーブルである。有効なロール割り付け情報とは、有効開始日時が現在時刻よりも前であって有効終了日時が現在時刻よりも後のロール割り付けテーブルである。

40

【0038】

権限情報出力部108は、システムテーブルを検索し、システムテーブルを順次抽出する(S201)。システムテーブルが抽出されるとシステムテーブルに割り付いているロールテーブルを検索する(S203)。システムテーブルに割り付いているロールテーブルが見つかり、ロールテーブルに割り付いている組織テーブル/ユーザテーブルからユ

50

ーザ情報を取り出し、ロール情報との対応情報を生成し、システムテーブル設定された業務システムにユーザ情報とロール情報を送信する（S206）。この処理を、全てのシステムテーブルに対して実施する。

【0039】

以上の処理の後、ユーザ端末320からユーザがユーザID、パスワードにより業務システムにログインする。業務システム330は、権限情報出力部108から受信したユーザIDとパスワードによりユーザ認証を行うとともに、権限情報出力部108から出力されたロールIDに認められている権限範囲内において、ユーザのデータアクセス等のサービスをユーザに提供する。

【0040】

以上では、組織の実体に変化がなく組織IDが変化する場合に対応させて説明を行った。

図3のロール割付け情報に示すように、ユーザIDに対してロールIDを割り付けることも可能である。

このため、ユーザの実体に変化がないがユーザIDが変化する場合にも、ロール割付け変更部107は、図5及び図6に示す処理を行い、新しいユーザIDとロールIDとを結び付ける新たなロール割付け情報を生成し、既存のロール割付け情報を有効開始日時に無効化することも可能である。

【0041】

また、以上では、システム利用権限として業務システム330に対する利用権限を例にし、業務システム330に対する利用権限が指定されているロールを新組織にも継続して割り付けるための仕組みを説明した。

この点、入退室管理システムに対する通行権限をシステム利用権限の例とし、本実施の形態に係るID管理システム100を用いて、入退室管理システムに対する通行権限が指定されているロールを新組織にも継続して割り付けるための仕組みを実現することができる。

【0042】

本実施の形態によれば、ID変更組織テーブルに基づき、元組織IDに割り付けられているロールIDが新組織IDに割り付けられ、有効開始日時に有効になる新たなロール割付け情報を生成し、また、既存のロール割付け情報を有効開始日時において無効化するので、新組織IDとロールIDとの割り付けを有効開始日時から有効にすることができ、新組織IDに対して権限を割り付ける際の処理負担を軽減することができる。

【0043】

実施の形態2.

実施の形態1では、組織としての実体は同じであり、組織IDのみが変更になる場合に、新組織IDとロールとを対応付けることを説明した。

組織ID変更後も、対象組織に所属する個人に対してロールの割付けを引き続き有効とするためには、図3に示す組織割付けテーブルを更新して、各ユーザIDを新組織IDと対応付ける必要がある。

図9に示すように、正社員といった人事DBシステム310で一元管理されている正規ユーザであれば、組織割付けテーブルは人事DBシステム310で自動更新されるため、手動で組織割付けテーブルを更新する必要がない。

一方で、企業等では、派遣社員や協力会社社員といった、組織には関係があるが当該組織に正規には所属していない非正規ユーザも就業していることが多い。

このような非正規ユーザは、人事DBシステム310では管理されていないので、実施の形態1で示した新組織IDとロールとの対応付けが行われても、非正規ユーザの組織割付けテーブルは自動的に更新されないため、非正規ユーザの組織割付けテーブルの更新は手動で行う必要がある。

本実施の形態では、このような非正規ユーザの組織割付けテーブルの更新をロール割付け変更部107が行う例を説明する。

10

20

30

40

50

なお、本実施の形態では、正規ユーザのユーザテーブルを正規ユーザテーブルといい、正規ユーザの組織割付けテーブルを正規ユーザ組織割付けテーブルという。

また、非正規ユーザのユーザテーブルを非正規ユーザテーブルといい、非正規ユーザの組織割付けテーブルを非正規ユーザ組織割付けテーブルという。

【 0 0 4 4 】

本実施の形態に係るシステム構成例は図 1 と同様である。

但し、ID 管理システム DB 150 は、正規ユーザテーブル及び正規ユーザ組織割付けテーブルに加え、非正規ユーザテーブル及び非正規ユーザ組織割付けテーブルも記憶している。

非正規ユーザテーブルには、図 9 に示した通り、非正規ユーザの識別子であるユーザ ID、非正規ユーザの名前、非正規ユーザの協力スタッフ区分（派遣社員か、協力会社社員かといった区分）、非正規ユーザのパスワード、非正規ユーザテーブルの有効開始日時と有効終了日時等が記述される。

また、非正規ユーザ組織割付けテーブルには、図 9 に示した通り、非正規ユーザの識別子であるユーザ ID、非正規ユーザが関係する組織の識別子である組織 ID、非正規ユーザ組織割付けテーブルの有効開始日時と有効終了日時が記述される。

なお、非正規ユーザ組織割付けテーブルは非正規ユーザ組織割付け情報の例であり、また、ID 管理システム DB 150 は、非正規ユーザ組織割付け情報記憶装置の例でもある。

【 0 0 4 5 】

ロール割付け変更部 107 は、実施の形態 1 で説明した動作を行うとともに、非正規ユーザ組織割付けテーブルの更新を行う。

ロール割付け変更部 107 は、例えば、図 6 の動作を行った後、図 6 の S 101 及び S 102 で抽出した ID 変更組織テーブル（図 4）の元組織 ID が組織 ID の欄に記述されている非正規ユーザ組織割付けテーブルを検索し、検索した非正規ユーザ組織割付けテーブルの複製を生成するとともに、複製の非正規ユーザ組織割付けテーブルの組織 ID の欄を新組織 ID（ID 変更組織テーブルに記述されている新組織 ID）にする。

そして、元組織 ID が記述されている非正規ユーザ組織割付けテーブルの有効終了日時を当日（本日）の最終時刻（例えば、2010 年 3 月 31 日 23 時 59 分 59 秒）とする。

更に、新組織 ID が記述されている非正規ユーザ組織割付けテーブルの有効開始日時を ID 変更組織テーブルに記述されている有効開始日時（例えば、2010 年 4 月 1 日 0 時 0 分 0 秒）とし、有効終了日時をシステムで許容される最大の日時とする。

そして、ロール割付け変更部 107 は、元組織 ID が記述されている非正規ユーザ組織割付けテーブルと新組織 ID が記述されている非正規ユーザ組織割付けテーブルを ID 管理システム DB 150 に格納する。

このようにすることで、ロール割付け変更部 107 は、非正規ユーザ組織割付けテーブルを更新することができ、手動による更新を不要とすることができる。

【 0 0 4 6 】

以上、本実施の形態によれば、非正規ユーザ組織割付けテーブルも自動で更新されるので、組織改編時の個別の入力設定が不要となり、組織改編時の処理負担を軽減することができる。

【 0 0 4 7 】

最後に、実施の形態 1 及び 2 に示した ID 管理システム 100 のハードウェア構成例について説明する。

図 8 は、実施の形態 1 及び 2 に示す ID 管理システム 100 のハードウェア資源の一例を示す図である。

なお、図 8 の構成は、あくまでも ID 管理システム 100 のハードウェア構成の一例を示すものであり、ID 管理システム 100 のハードウェア構成は図 8 に記載の構成に限らず、他の構成であってもよい。

10

20

30

40

50

【0048】

図8において、ID管理システム100は、プログラムを実行するCPU911(Central Processing Unit、中央処理装置、処理装置、演算装置、マイクロプロセッサ、マイクロコンピュータ、プロセッサともいう)を備えている。

CPU911は、バス912を介して、例えば、ROM(Read Only Memory)913、RAM(Random Access Memory)914、通信ボード915、表示装置901、キーボード902、マウス903、磁気ディスク装置920と接続され、これらのハードウェアデバイスを制御する。

更に、CPU911は、FDD904(Flexible Disk Drive)、コンパクトディスク装置905(CDD)、プリンタ装置906、カードリーダ装置907と接続していてもよい。また、磁気ディスク装置920の代わりに、光ディスク装置、メモリカード(登録商標)読み書き装置などの記憶装置でもよい。

RAM914は、揮発性メモリの一例である。ROM913、FDD904、CDD905、磁気ディスク装置920の記憶媒体は、不揮発性メモリの一例である。これらは、記憶装置の一例である。

実施の形態1及び2で説明したID管理システムDB150は、RAM914、磁気ディスク装置920等により実現される。

通信ボード915、キーボード902、マウス903、カードリーダ装置907、FDD904などは、入力装置の一例である。

また、通信ボード915、表示装置901、プリンタ装置906などは、出力装置の一例である。

【0049】

通信ボード915は、図1に示すように、ネットワークに接続されている。例えば、通信ボード915は、LANのほか、インターネット、WAN(Wide Area Network)、SAN(Storage Area Network)などに接続されていても構わない。

【0050】

磁気ディスク装置920には、オペレーティングシステム921(OS)、ウィンドウシステム922、プログラム群923、ファイル群924が記憶されている。

プログラム群923のプログラムは、CPU911がオペレーティングシステム921、ウィンドウシステム922を利用しながら実行する。

【0051】

また、RAM914には、CPU911に実行させるオペレーティングシステム921のプログラムやアプリケーションプログラムの少なくとも一部が一時的に格納される。

また、RAM914には、CPU911による処理に必要な各種データが格納される。

【0052】

また、ROM913には、BIOS(Basic Input Output System)プログラムが格納され、磁気ディスク装置920にはブートプログラムが格納されている。

ID管理システム100の起動時には、ROM913のBIOSプログラム及び磁気ディスク装置920のブートプログラムが実行され、BIOSプログラム及びブートプログラムによりオペレーティングシステム921が起動される。

【0053】

上記プログラム群923には、実施の形態1及び2の説明において「～部」として説明している機能を実行するプログラムが記憶されている。プログラムは、CPU911により読み出され実行される。

【0054】

ファイル群924には、実施の形態1及び2の説明において、「～の判断」、「～の決定」、「～の比較」、「～の生成」、「～の更新」、「～の設定」、「～の登録」、「～の選択」、「～の検索」、「～の抽出」等として説明している処理の結果を示す情報やデ

10

20

30

40

50

ータや信号値や変数値やパラメータが、「～ファイル」や「～データベース」の各項目として記憶されている。

「～ファイル」や「～データベース」は、ディスクやメモリなどの記録媒体に記憶される。ディスクやメモリなどの記憶媒体に記憶された情報やデータや信号値や変数値やパラメータは、読み書き回路を介してCPU911によりメインメモリやキャッシュメモリに読み出され、抽出・検索・参照・比較・演算・計算・処理・編集・出力・印刷・表示などのCPUの動作に用いられる。

抽出・検索・参照・比較・演算・計算・処理・編集・出力・印刷・表示のCPUの動作の間、情報やデータや信号値や変数値やパラメータは、メインメモリ、レジスタ、キャッシュメモリ、バッファメモリ等に一時的に記憶される。

また、実施の形態1及び2で説明しているフローチャートの矢印の部分は主としてデータや信号の入出力を示し、データや信号値は、RAM914のメモリ、FDD904のフレキシブルディスク、CDD905のコンパクトディスク、磁気ディスク装置920の磁気ディスク、その他光ディスク、ミニディスク、DVD等の記録媒体に記録される。また、データや信号は、バス912や信号線やケーブルその他の伝送媒体によりオンライン伝送される。

【0055】

また、実施の形態1及び2の説明において「～部」として説明しているものは、「～回路」、「～装置」、「～機器」であってもよく、また、「～ステップ」、「～手順」、「～処理」であってもよい。すなわち、「～部」として説明しているものは、ROM913に記憶されたファームウェアで実現されていても構わない。或いは、ソフトウェアのみ、或いは、素子・デバイス・基板・配線などのハードウェアのみ、或いは、ソフトウェアとハードウェアとの組み合わせ、さらには、ファームウェアとの組み合わせで実施されても構わない。ファームウェアとソフトウェアは、プログラムとして、磁気ディスク、フレキシブルディスク、光ディスク、コンパクトディスク、ミニディスク、DVD等の記録媒体に記憶される。プログラムはCPU911により読み出され、CPU911により実行される。すなわち、プログラムは、実施の形態1及び2の「～部」としてコンピュータを機能させるものである。あるいは、実施の形態1及び2の「～部」の手順や方法をコンピュータに実行させるものである。

【0056】

このように、実施の形態1及び2に示すID管理システム100は、処理装置たるCPU、記憶装置たるメモリ、磁気ディスク等、入力装置たるキーボード、マウス、通信ボード等、出力装置たる表示装置、通信ボード等を備えるコンピュータであり、上記したように「～部」として示された機能をこれら処理装置、記憶装置、入力装置、出力装置を用いて実現するものである。

【符号の説明】

【0057】

100 ID管理システム、101 制御部、102 通信部、103 入出力部、104 組織変更マッピング情報設定部、105 ロール設定部、106 割付け設定部、107 ロール割付け変更部、108 権限情報出力部、150 ID管理システムDB、200 ディスプレイ装置、210 キーボード、300 LAN、310 人事DBシステム、320 ユーザ端末装置、330 業務システム、340 業務システムDB

。

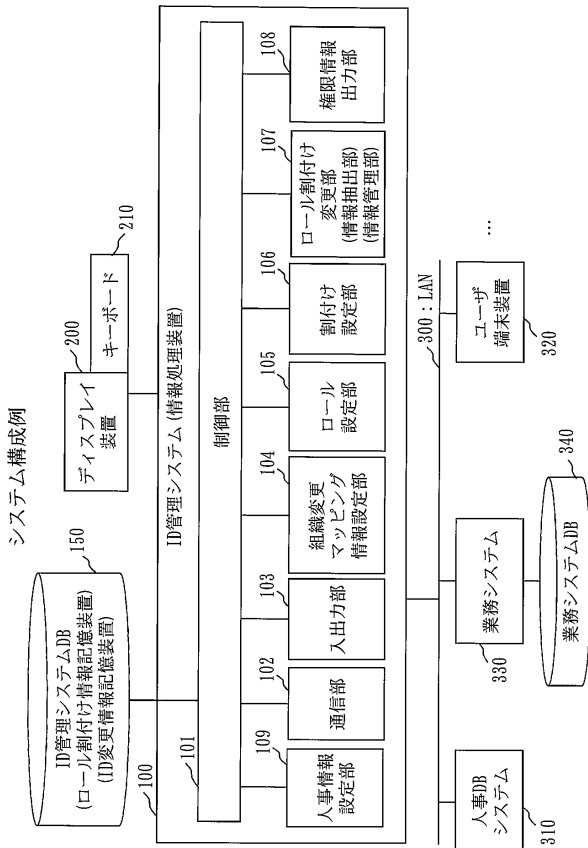
10

20

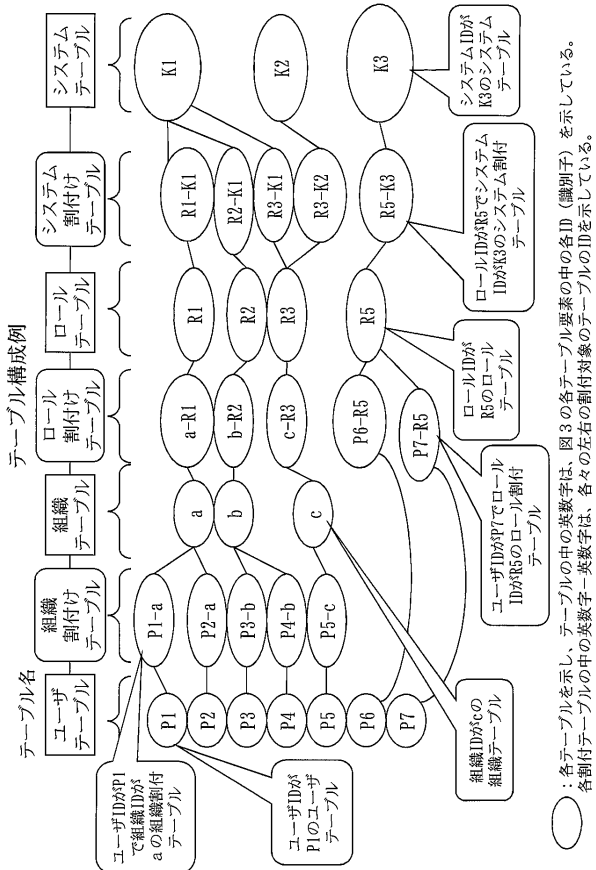
30

40

【 図 1 】



【 図 2 】



【 図 3 】

テーブル要素例

ユーザーテーブル	ユーザーID	名前	社員区分	パスワード	...	有効開始日時	有効終了日時
組織割付けテーブル	ユーザーID	組織ID	有効開始日時	有効終了日時			
組織テーブル	組織ID	組織名	...	有効開始日時	有効終了日時		
ルール割付けテーブル	ルールID	組織/ユーザーID	有効開始日時	有効終了日時			
ルールテーブル	ルールID	ルール名	有効開始日時	有効終了日時			
システム割付けテーブル	ルールID	システムID	有効開始日時	有効終了日時			
システムテーブル	システムID	システム名	...	送信先IPアドレス			

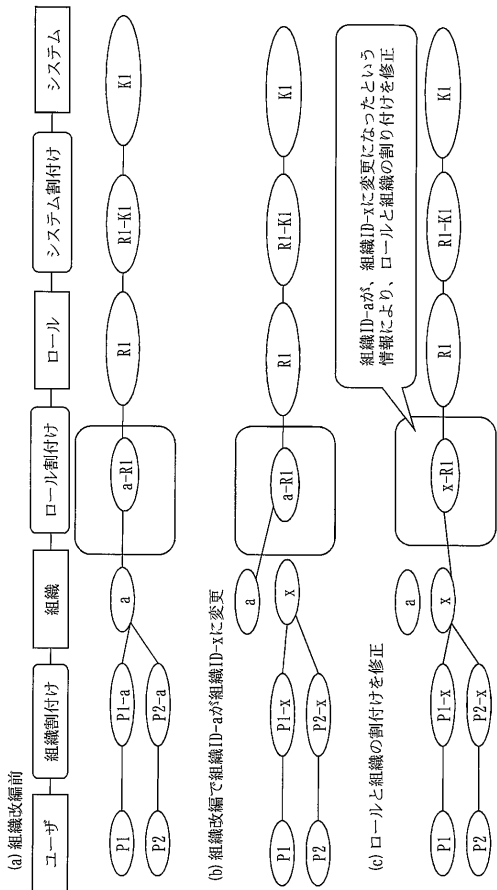
【 図 4 】

ID変更組織テーブルの例

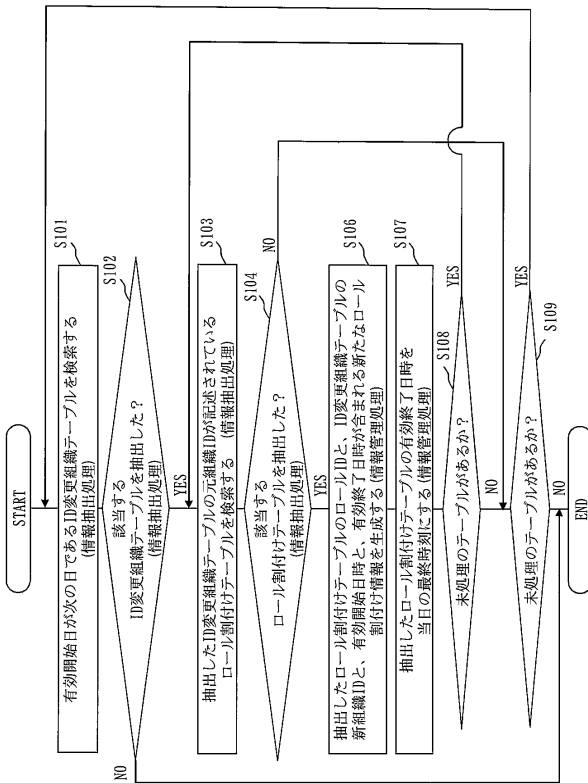
ID変更組織テーブル
新組織ID
組織名
有効開始日時
有効終了日時
元組織ID

【図5】

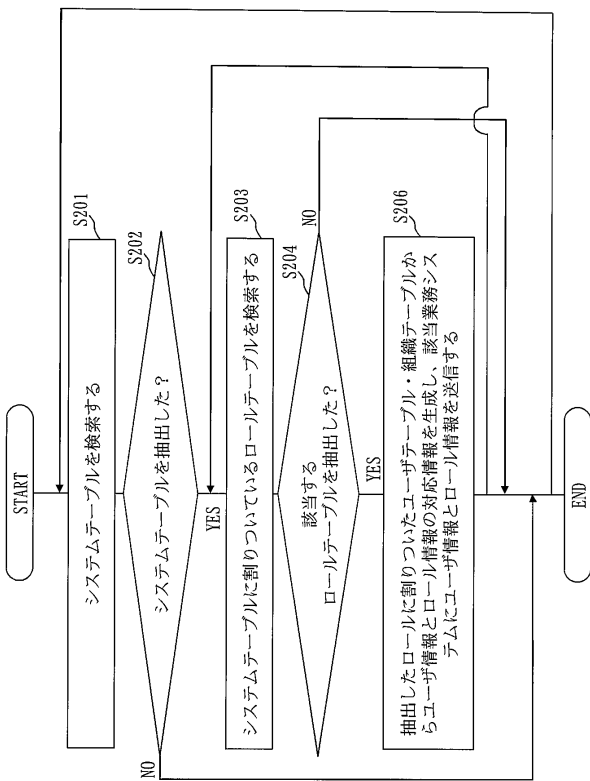
ルール割付け更新例



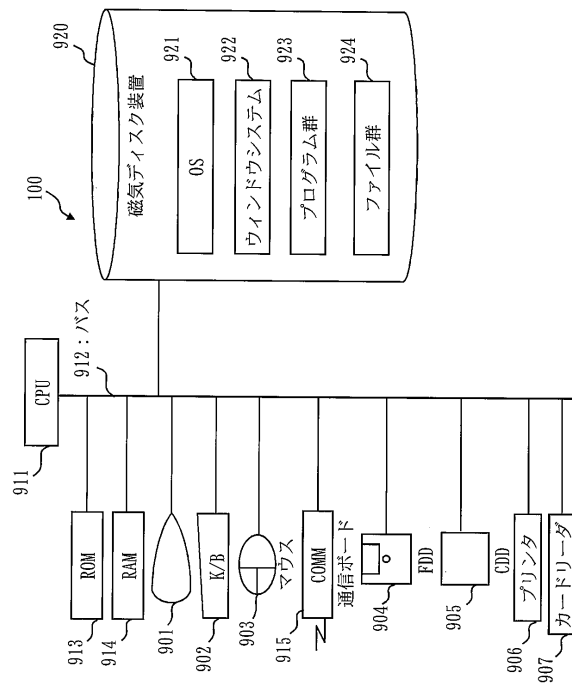
【図6】



【図7】

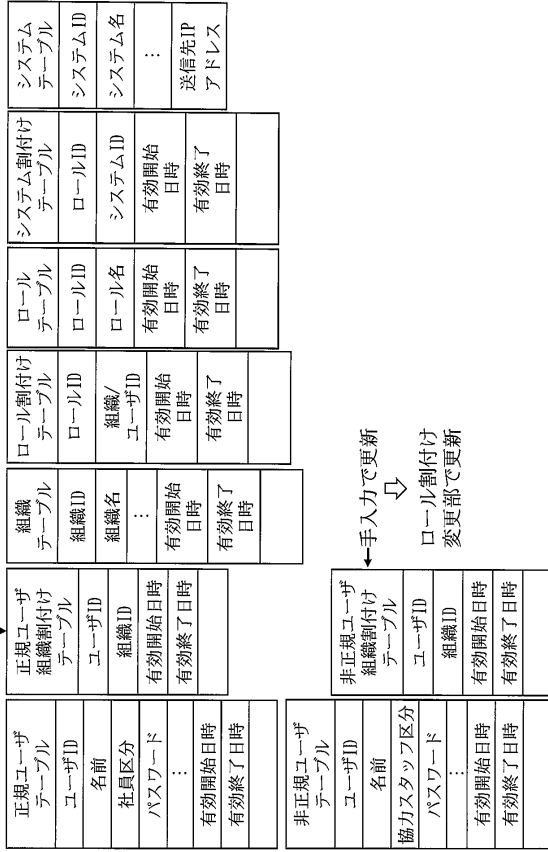


【図8】



【 図 9 】

人事DBシステムで更新 テーブル要素例



フロントページの続き

- (72)発明者 及川 和彦
東京都港区芝浦四丁目15番33号 三菱電機インフォメーションテクノロジー株式会社内
- (72)発明者 入不二 経勝
東京都港区芝浦四丁目15番33号 三菱電機インフォメーションテクノロジー株式会社内
- (72)発明者 水間 寿一
東京都港区芝浦四丁目15番33号 三菱電機インフォメーションテクノロジー株式会社内
- (72)発明者 齋藤 篤男
東京都港区芝浦四丁目15番33号 三菱電機インフォメーションテクノロジー株式会社内
- (72)発明者 山足 光義
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
- (72)発明者 小宮 崇
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

審査官 脇岡 剛

- (56)参考文献 特開2003-006397(JP,A)
特開2005-228059(JP,A)
特開2009-245229(JP,A)
特開2010-140430(JP,A)
特開2010-117885(JP,A)

- (58)調査した分野(Int.Cl., DB名)
G06F 21/31
G06Q 10/06