

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2009-238191

(P2009-238191A)

(43) 公開日 平成21年10月15日(2009. 10. 15)

(51) Int.Cl.	F I	テーマコード (参考)
G 0 6 Q 10/00 (2006.01)	G 0 6 F 17/60 1 5 8	5 B 0 1 7
G 0 6 F 21/24 (2006.01)	G 0 6 F 17/60 1 7 4	
	G 0 6 F 12/14 5 2 0 A	

審査請求 未請求 請求項の数 6 O L (全 16 頁)

(21) 出願番号	特願2008-87027 (P2008-87027)	(71) 出願人	000006013
(22) 出願日	平成20年3月28日 (2008. 3. 28)		
		(74) 代理人	100073759
			弁理士 大岩 増雄
		(74) 代理人	100093562
			弁理士 児玉 俊英
		(74) 代理人	100088199
			弁理士 竹中 考生
		(74) 代理人	100094916
			弁理士 村上 啓吾
		(72) 発明者	福島 繁樹
			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
		Fターム(参考)	5B017 AA01 BA06 BB06 CA16

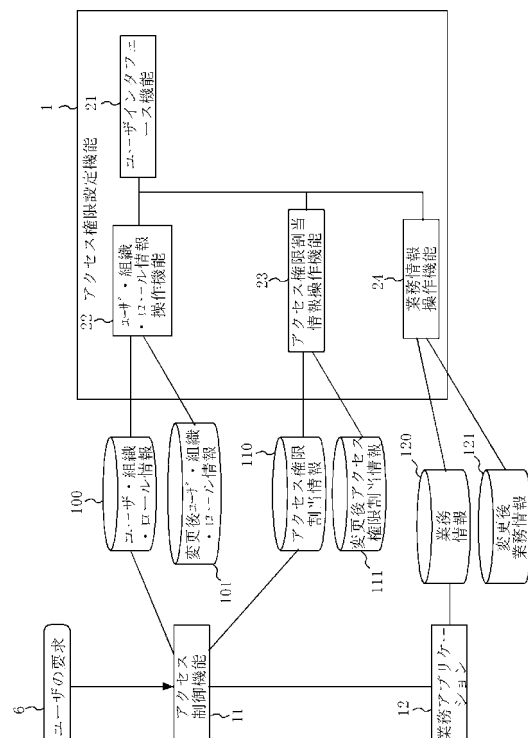
(54) 【発明の名称】 Webアプリケーションシステム

(57) 【要約】

【課題】組織変更時に大量に発生する業務情報に対するアクセス権限の設定作業の効率化を図ることができるWebアプリケーションシステムを得る。

【解決手段】ユーザ情報及び組織情報及び業務の分担を示すロール情報を関連付けて格納したユーザ・組織・ロール情報100を操作するユーザ・組織・ロール情報操作機能22と、ロール情報がアクセスできる業務情報を割り当てたアクセス権限割当情報110を操作するアクセス権限割当情報操作機能23と、業務情報120を操作する業務情報操作機能24を設け、これらをユーザインタフェース機能21の画面上で操作するようにして、組織変更に応じた効率のよい変更作業を行うようにした。

【選択図】 図1



【特許請求の範囲】**【請求項 1】**

業務アプリケーションを提供し、上記業務アプリケーションが取り扱う業務情報に対する操作を、各業務情報に対しそれぞれアクセス権限を有するユーザによって行う Web アプリケーションシステムにおいて、ユーザ情報及び組織情報及びアクセス権限を設定する単位であるロール情報を関連付けて格納したユーザ関連情報、このユーザ関連情報に格納された上記ロール情報について上記業務情報へのアクセス権限を割り当てたアクセス権限割当情報、上記ユーザ関連情報を操作するユーザ関連情報操作手段、上記アクセス権限割当情報を操作するアクセス権限割当情報操作手段、上記業務情報を操作する業務情報操作手段、及び上記ユーザ関連情報操作手段と上記アクセス権限割当情報操作手段と上記業務情報操作手段を用いて操作を行うためのユーザインタフェースを備えたことを特徴とする Web アプリケーションシステム。

10

【請求項 2】

上記ユーザインタフェースは、上記業務情報に対する上記ロール情報のアクセス権限をマトリクス状に画面表示し、指定されたユーザ情報または組織情報に関連する上記業務情報または上記ロール情報のどちらかまたは両方を強調表示することを特徴とする請求項 1 記載の Web アプリケーションシステム。

【請求項 3】

上記業務情報へのアクセス権限の引継ぎ期間を設定するアクセス権限引継ぎ設定手段を備えたことを特徴とする請求項 1 または請求項 2 記載の Web アプリケーションシステム。

20

【請求項 4】

上記業務情報をグループ化する業務種別を定義した業務種別定義情報、及びこの業務種別定義情報を操作する業務種別操作手段を備え、上記アクセス権限割当情報は、上記業務種別に対して上記ロール情報のアクセス権限を割り当て可能とすることを特徴とする請求項 1～請求項 3 のいずれかに記載の Web アプリケーションシステム。

【請求項 5】

上記業務種別に含まれる上記業務情報及びこの業務情報に対する業務操作ごとにアクセス権限を予め格納したアクセス権限割当テンプレート、及びこのアクセス権限割当テンプレートに基づき、上記アクセス権限割当情報を生成するアクセス権限テンプレート手段を備えたことを特徴とする請求項 4 記載の Web アプリケーションシステム。

30

【請求項 6】

上記ユーザまたは上記組織を指定して上記業務情報へのアクセス権限を割り当てることを可能とする業務委託手段を備えたことを特徴とする請求項 1～請求項 5 のいずれかに記載の Web アプリケーションシステム。

【発明の詳細な説明】**【技術分野】****【0001】**

この発明は、ネットワークを介して業務アプリケーションを提供するとともに、業務アプリケーションが行う業務情報の操作に対するユーザのアクセス権限を設定する Web アプリケーションシステムに関するものである。

40

【背景技術】**【0002】**

イントラネットが発達した現在、Web アプリケーションシステムにより、業務サービスを提供する方式が主流となっている。その多くは、個々の業務情報に対するアクセス許可を適切なアクセス権限を持つ利用者によりのみ開示するアクセス制御を行う。

アクセス権限の割当方法については、業務サービスの性質により、たとえば個人情報についてはその個人によりのみアクセス権限を与え、部門内でのみ扱う情報については、その部門に対してアクセス権限を与えるように、アクセス権限の与え方には様々な方式が存在す

50

る。

また、利用者により異なるアクセス権限に基づき業務サービスを提供する場合には、ユーザは、ユーザの操作によりWebブラウザを経由してユーザの要求を送信し、これを受信したアクセス制御部で、ユーザIDを格納しているユーザ情報や、ユーザが業務情報に対する操作を許可されているかどうかを示す情報を格納するアクセス権限割当情報を用いて、業務アプリケーション及び業務情報に対する利用可否を判定するようにしている。

この場合のアクセス権限割当情報及びユーザ情報は、ユーザインターフェース機能を有するアクセス権限設定機能により設定される。

【0003】

大きい組織では、業務アプリケーションを多数のユーザが利用し、また、扱う業務情報も大量に存在する。このため、アクセス権限割当情報も膨大な量となり、その設定を行う労力も膨大なものとなる。

このため、設定の効率化を図る方法として、ユーザIDをグループ化し、グループ単位で権限を割り当てる方法、組織単位でアクセス権限を割り当てる方法、RBAC (Role Based Access Control) モデルに基づき、ロールという単位にアクセス権限を割り当てる方法などが用いられてきた。

特許文献1では、このアクセス権限割当情報の設定を支援する方式として、権限割当のサンプルの提供、アクセスログ情報や、ユーザの要求を監視した結果と現行のアクセス制御の設定との差分を表示することで、アクセス権限を割り当てる人間に、必要とされているアクセス権限割当情報の原案を提示し、作業を効率化する方式を提案している。

【0004】

【特許文献1】特開2004-192601号公報(第7～23頁、図1)

【発明の開示】

【発明が解決しようとする課題】

【0005】

上述のように、アクセス権限割当情報を効率的に設定する方法が検討されてきた。特に、RBACモデルは、業務の分担をロール情報とすることで、その業務を行うメンバーに変更が生じても、アクセス権限割当情報の変更が生じにくくなり、業務アプリケーションに対するアクセス制御の方法として有用とされていた。

しかしながら、実際の業務情報は、組織構造と結びついて作成されていることが多く、組織変更が行われた場合、業務情報自体に移管、分割、統合といった操作が発生する。

このため、業務の分担ごとにロール情報を定義したとしても、その業務情報自体が変更されるため、アクセス権限割当情報を変えなければならなくなる。このため、結果として、アクセス権限割当情報の設定箇所が多岐に渡り、複雑となっている。

【0006】

この発明は、上述の課題を解決するためになされたものであり、組織変更時に大量に発生する業務情報に対するアクセス権限の設定作業の効率化を図ることができるWebアプリケーションシステムを得ることを目的としている。

【課題を解決するための手段】

【0007】

この発明に係わるWebアプリケーションシステムにおいては、業務アプリケーションを提供し、業務アプリケーションが取り扱う業務情報に対する操作を、各業務情報に対しそれぞれアクセス権限を有するユーザによって行うWebアプリケーションシステムにおいて、

ユーザ情報及び組織情報及びアクセス権限を設定する単位であるロール情報を関連付けて格納したユーザ関連情報、このユーザ関連情報に格納されたロール情報について業務情報へのアクセス権限を割り当てたアクセス権限割当情報、ユーザ関連情報を操作するユーザ関連情報操作手段、アクセス権限割当情報を操作するアクセス権限割当情報操作手段、業務情報を操作する業務情報操作手段、及びユーザ関連情報操作手段とアクセス権限割当情報操作手段と業務情報操作手段を用いて操作を行うためのユーザインターフェースを備え

たものである。

【発明の効果】

【0008】

この発明は、以上説明したように、業務アプリケーションを提供し、業務アプリケーションが取り扱う業務情報に対する操作を、各業務情報に対しそれぞれアクセス権限を有するユーザによって行うWebアプリケーションシステムにおいて、ユーザ情報及び組織情報及びアクセス権限を設定する単位であるロール情報を関連付けて格納したユーザ関連情報、このユーザ関連情報に格納されたロール情報について業務情報へのアクセス権限を割り当てたアクセス権限割当情報、ユーザ関連情報を操作するユーザ関連情報操作手段、アクセス権限割当情報を操作するアクセス権限割当情報操作手段、業務情報を操作する業務情報操作手段、及びユーザ関連情報操作手段とアクセス権限割当情報操作手段と業務情報操作手段を用いて操作を行うためのユーザインターフェースを備えたので、ユーザまたは組織の変更に伴うアクセス権限の設定を効率的に行うことが可能となる。

10

【発明を実施するための最良の形態】

【0009】

実施の形態1.

以下、この発明の実施の形態1を図に基づいて説明する。

図1は、この発明の実施の形態1によるWebアプリケーションシステムを示す概略構成図である。

20

図1において、ユーザの要求6には、ユーザを識別するユーザIDや、業務情報に対する操作が含まれている。ユーザの要求6は、ユーザの操作によりWebブラウザを経由して送信される場合もあるし、業務アプリケーション自身をユーザとして、他の業務アプリケーションに対する要求を行うために送信される場合もある。ユーザの要求6は、アクセス制御機能11に送信される。

アクセス制御機能11は、ユーザ及びその属性情報を格納したユーザ・組織・ロール情報100と、ユーザが業務情報に対する操作を許可されているかどうかを示す情報を格納するアクセス権限割当情報110を参照して、ユーザの要求6が、業務アプリケーション12及び業務情報120にアクセス可能かどうかを判定する。

業務アプリケーション12は、アクセス制御機能11によりアクセス可と判定されたユーザの要求6を受け取り、業務情報120に対して操作し、その結果を応答する。アクセス制御機能12における判定結果がアクセス不可であれば、アクセス制御機能12から、要求の送信元にアクセス不可の応答を返す。

30

【0010】

アクセス権限設定機能1は、ユーザインターフェース機能21、ユーザ・組織・ロール情報操作機能22（ユーザ関連情報操作手段）、アクセス権限割当情報操作機能23（アクセス権限割当情報操作手段）、業務情報操作機能24（業務情報操作手段）から構成され、ユーザ・組織・ロール情報100（ユーザ関連情報）、アクセス権限割当情報110を参照し、ユーザインターフェース機能21により、ユーザ・組織・ロール情報100の各情報ごとに業務情報120へのアクセス権限を指定する。

40

ユーザ・組織・ロール情報操作機能22は、ユーザ・組織・ロール情報100を参照する他、ユーザ及び組織の情報が変更された後の情報を格納している変更後ユーザ・組織・ロール情報110を操作する。

アクセス権限割当情報操作機能23は、アクセス権限割当情報110を参照する他、組織変更を行ったのちの情報を格納している変更後アクセス権限割当情報111を操作する機能である。業務情報操作機能24は、業務情報120を参照し、変更後業務情報121を操作する機能である。

【0011】

ユーザ・組織・ロール情報100は、ユーザ情報ごと、組織情報ごと、及びロール情報ごとの識別情報を格納するとともに、ユーザ情報、組織情報及びロール情報を相互に関連

50

付けている。なお、ロール情報は、R B A C モデルにおいてロールと呼ばれる役割に基づいてアクセス権限を業務情報に設定する単位の情報である。

アクセス権限割当情報 1 1 0 は、ロール情報が、業務情報に対する操作を許可されているかどうかを示す情報を格納する。

また、ユーザ・組織・ロール情報 1 0 0、アクセス権限割当情報 1 1 0 は、データベースやディレクトリサービス、テキストファイル、バイナリファイルなどに格納される。

業務情報 1 2 0 は、各業務情報に対する可能な操作が定義され、さらに当該業務情報を保有する主管部門を指定している。

【0012】

図 2 は、この発明の実施の形態 1 による W e b アプリケーションシステムのハードウェア構成例を示す図である。

図 2 において、クライアント端末 2 0 1、操作端末 2 0 2、アプリケーションサーバ 2 0 3、DBサーバ 2 0 4 がネットワーク 2 0 5 により接続されている。

操作端末 2 0 2 にアクセス制御設定機能 1、アプリケーションサーバ 2 0 3 にアクセス制御機能 1 1 及び業務アプリケーション 1 2、DBサーバ 2 0 4 にユーザ・組織・ロール情報 1 0 0、変更後ユーザ・組織・ロール情報 1 0 1、アクセス権限割当情報 1 1 0、変更後アクセス権限割当情報 1 1 1、業務情報 1 2 0、変更後業務情報 1 2 1 がそれぞれ配置される。

ユーザの要求 6 は、クライアント端末 2 0 1 もしくはアプリケーションサーバ 2 0 3 内から、アクセス制御機能 1 1 に送信される。この構成は、1 例であり、例えば操作端末 2 0 2 がアプリケーションサーバ 2 0 3 や DBサーバ 2 0 4 と同一であっても構わないし、アプリケーションサーバ 2 0 3 の機能が複数台のサーバに分かれて存在していても構わない。また、DBサーバ 2 0 4 の各データについても、複数台のサーバに分かれて存在していても構わない。

【0013】

図 3 は、この発明の実施の形態 1 による W e b アプリケーションシステムのユーザ・組織・ロール情報の例を示す図である。

図 3 において、ユーザ情報・組織情報・ロール情報 1 0 0 では、組織情報 1 0 2、ユーザ情報 1 0 3、ロール情報 1 0 4 を有し、ユーザ情報、組織情報及びロール情報は互に関連付けられている。なお、図ではロール情報に含まれるユーザ、組織情報は、それぞれのコードで指定されているが、コードの変更を容易にするため、内部 I D により関連付けても構わない。ロールには、ユーザまたは組織の I D を設定でき、“ R 0 1 0 ” などのように、「 O A 0 0 〆 課長」などのような論理表現も記述できる。なお、論理記号「〆」は、“ A N D ” を意味する。

【0014】

図 4 は、この発明の実施の形態 1 による W e b アプリケーションシステムの業務情報の例を示す図である。

図 4 において、業務情報 1 2 0 の各情報には、業務情報に対する可能な操作が定義され、さらに当該業務情報を保有する主管部門を指定している。

【0015】

図 5 は、この発明の実施の形態 1 による W e b アプリケーションシステムのアクセス権限割当情報の例を示す図である。

図 5 において、アクセス権限割当情報で、業務情報に対する操作を許可されたロール情報が示されている。ここで関連付けられるロール情報、業務情報は、コードで指定してもよいし、コードの変更を容易にするため、内部 I D により関連付けても構わない。図 5 では、「業務情報」と「ロール情報」のどちらも、「コード」と「内部 I D」の両方を示している。

【0016】

図 6 は、この発明の実施の形態 1 による W e b アプリケーションシステムのアクセス権限設定機能の動作を示すフローチャートである。

10

20

30

40

50

図 7 は、この発明の実施の形態 1 による Web アプリケーションシステムで用いられる画面例を示す図である。

【0017】

次に、動作について説明する。

ユーザの要求 6 は、アクセス制御機能 11 に送信される。これを受信したアクセス制御機能 11 は、ユーザ及びその属性情報を格納したユーザ・組織・ロール情報 100 と、ユーザが業務情報に対する操作を許可されているかどうかを示す情報を格納したアクセス権限割当情報 110 を参照して、ユーザの要求 6 が、業務アプリケーション 12 及び業務情報 120 にアクセス可能かどうかを判定する。

業務アプリケーション 12 は、アクセス制御機能 11 によりアクセス可と判定されたユーザの要求 6 を受け取り、業務情報 120 に対して操作し、その結果を応答する。アクセス制御機能 12 における判定結果がアクセス不可であれば、アクセス制御機能 12 から、要求の送信元にアクセス不可の応答を返す。

【0018】

次に、アクセス権限設定機能 1 の動作について図 6 を用いて説明する。

S1001 にて、ユーザ・組織・ロール情報操作機能 22 により、ユーザ・組織・ロール情報 100 及び変更後ユーザ・組織・ロール情報 101 を読み込む。また、業務情報操作機能 24 により、業務情報 120、変更後業務情報 121 を読み込む。また、アクセス権限割当情報操作機能 23 により、アクセス権限割当情報 110 及び変更後アクセス権限割当情報 111 を読み込む。これらの読み込んだデータをユーザインターフェース機能 21 により表示する。

S1002 にて、ユーザインターフェース機能 21 で、S1001 で読み込んだ情報を変更し、その変更された情報をそれぞれ変更後の情報として保存する。

S1003 にて、組織変更の当日に、変更後ユーザ・組織・ロール情報 101 の内容をユーザ・組織・ロール情報 100 に、変更後アクセス権限割当情報 111 の内容をアクセス権限割当情報 110 に、変更後業務情報 121 の内容を、業務情報 120 に反映する。反映後、それ以降のアクセス制御は、組織変更に伴って修正した内容に基づくアクセス可否の判定が実現される。

【0019】

次に、ユーザインターフェース機能 21 により表示する画面例について図 7 により説明する。

画面 301 において、ロール情報をタイトル行とし、業務情報を行として、アクセス権限割当情報 110 の内容を“●”として示す。“●”は別の記号でも構わない。

また、ユーザまたは組織が変更されることで、変更が生じるロール情報の列を強調表示し、さらに、業務情報 120 に含まれる主管部門の情報から、影響する行を強調表示する。列、行の追加・削除が可能であり、列の追加・削除は、変更後ユーザ・組織・ロール情報 101 中のロール情報の追加・削除に相当し、行の追加は、変更後業務情報 121 中の業務情報の追加・削除に相当する。

列のタイトルであるロール情報を選択すると、そのロール情報に含まれるユーザ・組織の変更が行える。また、行のタイトルである業務情報を選択すると、その業務情報の主管部門の変更が行える。これらの変更は、それぞれ変更後ユーザ・組織・ロール情報 101、変更後業務情報 121 に格納される。

また、記号“●”を選択することで、アクセス権限の割当を変更することが可能であり、この変更は、変更後アクセス権限割当情報 111 に格納される。

【0020】

画面 302 は、組織“技術部第 1 課”に対する組織変更が生じた場合に、表示される画面例である。追加・変更・削除予定の列・行・記号は、背景や文字の種類を変えることで、区別される。

【0021】

なお、組織変更において、複数の組織の変更が発生するとき、全ての組織について、情

10

20

30

40

50

報を表示すると、表示が複雑となり、見にくくなることが考えられる。画面 301 には、組織変更される対象のうち、一部を選択し、その範囲のみを変更箇所として表示することもできる。

ユーザまたは組織の情報を変更する前に、ユーザまたは組織を指定して、変更が必要となる範囲を把握することもできる。

【0022】

実施の形態 1 によれば、インターフェースによって組織変更が影響を与えるロール情報、業務情報を視覚的に把握することができる。特に、業務情報を主管する部門を強調表示することで、業務情報に発生する変更も合わせて把握することが可能となる。

また、インターフェースにより、アクセス権限割当情報を変更するだけでなく、同一の画面上で、ロール情報、業務情報をそれぞれ操作するようにしたため、変更箇所を把握するとともに、その箇所に対する変更を同一画面上で行うことが可能となる。

これにより、ユーザまたは組織の変更に伴うアクセス権限の設定を効率的に行うことが可能となる。

【0023】

実施の形態 2.

実施の形態 2 について、図に基づいて説明する。

実施の形態 1 に示した発明では、組織変更時に、アクセス権限を操作することが容易になったが、実際に組織変更を行う場合、その情報が開示されてから組織変更を行うまでの期間が短い場合もある。このため、必ずしも業務情報を利用する先が確定しているとは限らない。また、細かい業務データは、現在担当している人物により振り分ける必要がある場合もある。

このような場合に、組織変更前後に、引継ぎのための期間を設け、その期間内に権限を移行する猶予期間を設けることが求められる。この課題を解決するため、実施の形態 2 は、組織変更前後における、アクセス権限の引継ぎ期間を設けるためのアクセス権限引継ぎ設定機能 25 を設ける。引継ぎ期間では、変更前または変更後のどちらかでアクセス権限を有するものがアクセス可能になる。

【0024】

図 8 は、この発明の実施の形態 2 による Web アプリケーションシステムを示す概略構成図である。

図 8 において、1、6、11、12、21～24、100、101、110、111、120、121 は図 1 におけるものと同一のものである。図 8 では、アクセス権限設定機能 1 に、組織変更前後における、アクセス権限の引継ぎ期間を設けるためのアクセス権限引継ぎ設定機能 25 (アクセス権限引継ぎ設定手段) を設けている。

【0025】

図 9 は、この発明の実施の形態 2 による Web アプリケーションシステムで用いる引継ぎ画面の例を示す図である。

図 9 において、組織変更前に引き継ぐか、組織変更後に引き継ぐかを選択し、部門及び引継ぎ期間を指定し、登録ボタンを押すことによりアクセス権限の引継ぎ期間が登録されるようになっている。

【0026】

図 10 は、この発明の実施の形態 2 による Web アプリケーションシステムのアクセス権限割当情報 110 の例を示す図である。

図 10 において、アクセス権限割当情報 110 は、内部 ID、業務コード、ロールコード、開始日、終了日とから構成されている。

【0027】

次に、図 9 により、アクセス権限引継ぎ設定機能 25 の動作について説明する。

図 8 のアクセス権限引継ぎ設定機能 25 は、図 9 に示す画面例により、引継ぎ期間を指定するための情報を取得する。図 9 の画面例は、ユーザインターフェース機能 21 にて、画面 301 から、業務情報を選択して表示したメニュー等を選ぶことで表示するようにな

10

20

30

40

50

っている。表示方法は別の手段であっても構わない。

【0028】

指定した部門や、引継ぎ期間は、登録ボタンを押すことにより、アクセス権限割当情報110もしくは変更後アクセス権限割当情報111に、開始日と終了日を含めて保存される。

組織変更前に引継ぎ期間を設ける場合は、アクセス権限割当情報110に、組織変更後に引継ぎ期間を設ける場合は、アクセス権限割り当て情報111に情報を格納する。このときに権限を与えるロール情報についても、組織変更前であればユーザ・組織・ロール情報100から、組織変更後であれば変更後ユーザ・組織・ロール情報101から取得する。

10

【0029】

組織変更前に引き継ぎを行う場合であれば、アクセス権限割当情報110に指定された開始日以降であれば、アクセス制御機能11は、アクセスを可とする。また、組織変更後に引き継ぎを行う場合であれば、アクセス制御機能11は、終了日までアクセスを可と判定する。具体的な組織引継ぎに伴う処理は、業務アプリケーション12で行う業務に依存する。

【0030】

実施の形態2によれば、組織の引継ぎを考慮したアクセス権限の設定を可能とし、例えばワークフローなどにより利用中の文書を決裁する場合など、組織変更の引継ぎ期間中に処理する、といったことが実現できる。

20

【0031】

実施の形態3.

この発明の実施の形態2について、図に基づいて説明する。

実施の形態1では、業務情報それぞれに対して、アクセス権限の割当を行っていた。しかしながら、業務情報として指定する内容は、業務アプリケーションごとに異なったり、また、常に増減して、多数に上る。全ての業務情報を一覧表示することは、アクセス権限設定機能を非常に使い難くし、また、実際の業務情報は、種別により扱いが変わるため、全ての情報を表示することは非常に無駄になる場合が考えられる。

実施の形態3は、このように、多数に上る業務情報を効率的に扱うため、業務情報120を直接操作するのではなく、業務情報を種別やアプリケーションによりグループ化し、業務種別によりアクセス権限を設定するための業務種別操作機能26を設ける。

30

【0032】

図11は、この発明の実施の形態3によるWebアプリケーションシステムを示す概略構成図である。

図11において、1、6、11、12、21～23、25、100、101、110、111、120は図8におけるものと同一のものである。図11では、アクセス権限設定機能1に業務種別操作機能26（業務種別操作手段）を設け、業務種別定義情報122を操作して、変更した場合に変更結果を変更後業務種別定義情報123に格納するようにした。

【0033】

図12は、この発明の実施の形態3によるWebアプリケーションシステムの業務種別定義情報の例を示す図である。

40

図12において、業務種別定義情報122には、業務情報をグループ化した業務種別を示す業務種別コードと業務情報との関連付けを行う。このために、業務種別コードと、業務データ名称と、業務コードと、主管部門が内部IDごとに定義されている。

【0034】

次に、業務種別操作機能26の動作について説明する。

図11の業務種別操作機能26は、業務情報120を直接扱わずに、業務種別定義情報122、変更後業務種別定義情報123を扱う。

また、ユーザの要求6及びアクセス制御機能11においても、業務情報の代わりに、業

50

務種別をアクセス権限の判定のために用いる。

【0035】

図12の業務種別定義情報122のデータ例では、業務情報をグループ化した業務種別と、業務情報の関連付けを行っている。この情報は、業務種別コードで指定しても構わないし、業務種別コードの変更が容易なように、内部IDで指定しても構わない。

アクセス権限割当情報110、アクセス権限割当情報111では、業務情報120の代わりに、この業務種別と関連付けされている。

【0036】

実施の形態3によれば、業務情報の全てに対してアクセス権限を割り当てる必要がなく、また、業務種別自体に追加・削除が生じなければ、業務情報の増減が、アクセス権限割当情報110の変更に影響しなくなり、よりアクセス権限の設定の効率化が図れることになる。

【0037】

なお、実施の形態3は、業務種別定義情報のみに基づいてアクセス制御するだけでなく、実施の形態1、2で備えている、業務情報ごとのアクセス権限割当情報と併用することは可能である。

また、階層化された業務種別を用いることもできる。この場合、上位の業務種別のアクセス権限を下位の業務種別では引継ぎ、上位の業務種別とは異なる箇所だけをアクセス権限として設定すればよい。

【0038】

実施の形態4.

実施の形態4について、図により説明する。

実施の形態3により、業務種別や階層化された業務種別ごとにアクセス権限を割り当てる機能を実現したが、業務種別に含まれる全ての業務情報・操作に対して、同一の権限を与えてしまう。階層的に業務種別が構成されている場合、個々の業務情報ごとに指定すればよいが、多数の設定をしなければならず、効率的ではない。

実施の形態4は、これを解決するためのものである。

【0039】

図13は、この発明の実施の形態4によるWebアプリケーションシステムを示す概略構成図である。

図13において、1、6、11、12、21～23、25、26、100、101、110、111、120、122、123は図11におけるものと同一のものである。図13では、業務種別に含まれる業務情報と業務操作について、それぞれ別の権限を与えるようにアクセス権限割当テンプレート28を用意し、その内容に従って、アクセス権限割当情報を出力するアクセス権限テンプレート機能27（アクセス権限テンプレート手段）を、アクセス権限設定機能1に設ける。

【0040】

図14は、この発明の実施の形態4によるWebアプリケーションシステムで用いられるアクセス権限割当テンプレートの例を示す図である。

図14において、業務種別の業務情報及び業務操作ごとのアクセス権限が定められている。

【0041】

実施の形態4では、図13に示すように、業務種別に含まれる業務情報と業務操作について、それぞれ別の権限を与えるようにアクセス権限割当テンプレート28を用意し、その内容に従って、アクセス権限割当情報を出力するアクセス権限テンプレート機能27を設ける。

【0042】

図14の例では、業務種別が“案件1情報”を、あるロールに新規にアクセス権限を割り当てる場合に、その種別に含まれる“全て”の業務情報への“新規作成”操作には、アクセス権限を与えず、“全て”の業務情報への“表示”操作、“ダウンロード”操作、“印

10

20

30

40

50

刷”操作にはアクセス権限を割り当てる。

同様に、業務情報“個人情報”には、“表示”“編集”操作のアクセス権限を割り当てることを意味する。

【0043】

このようなアクセス権限割当テンプレート28を読み込むことで、アクセス権限テンプレート機能27は、業務種別“案件1情報”情報について、個々の業務情報への細かなアクセス権限を一括して設定することが可能となる。

【0044】

アクセス権限割当テンプレート28には、対象ロール欄に、最初に設定するときのみ適用し、その後は個別の業務情報についてアクセス権限を編集してよいことにするか、もしくは固定（アクセス権限を編集できない）とするかを指定し、選択させることもできる。なお、アクセス権限割当テンプレート28の様式は、本内容に限らず、またデータベースなどに格納しても構わない。

【0045】

実施の形態4によれば、個々の業務ごとのアクセス権限の割当を、個別に設定することなく、一括して設定することが可能となり、アクセス権限割当作業の一層の効率化を図ることができる。

【0046】

実施の形態5.

実施の形態5について、図により説明する。

実施の形態4までは、ロール情報を扱ってアクセス権限割当情報を設定していたが、ある特定のユーザや組織に対して、業務を割り当てるニーズも多い。このような場合、わざわざ、ロール情報を意識することは煩雑になる。

実施の形態5は、このような場合に対処するためのものである。

【0047】

図15は、この発明の実施の形態5によるWebアプリケーションシステムを示す概略構成図である。

図15において、1、6、11、12、21～23、25～28、100、101、110、111、120、122、123は図13におけるものと同一のものである。図15では、アクセス権限設定機能1に業務委託機能29（業務委託手段）を設け、選択されている業務情報もしくは業務種別に対するアクセス権限を、特定のユーザに割り当てるようにした。

【0048】

図16は、この発明の実施の形態5によるWebアプリケーションシステムで用いる業務委託画面の例を示す図である。

図16において、選択されている業務情報もしくは業務種別に対するアクセス権限を、特定のユーザに割り当てるように、部門、ユーザ、期間が入力される。ロール入力は自動で行われるが、既存のロールを指定することもできる。

【0049】

実施の形態5は、図15に示すように業務委託機能29を設ける。業務委託情報29では、図16に示す画面例により、選択されている業務情報もしくは業務種別に対するアクセス権限を、入力された特定のユーザに割り当てる。

図16の画面例にある、ロール欄では、既存のロールを指定することもできるが、“自動”を選択した場合、自動的にロール情報を追加する。

自動的に追加されたロールは、自動的に生成されたものであることが分かるように、名称に“AUTO”などの識別子と、ユーザ名、業務情報を列挙した名称を与える。この自動生成したロール情報を画面301に表示することもできるし、別画面に一覧表示することもできる。

【0050】

実施の形態5によれば、ロール情報を意識したくない場合には、ロールを意識せず、ア

10

20

30

40

50

クセス権限の設定が可能となる。

【図面の簡単な説明】

【0051】

【図1】この発明の実施の形態1によるWebアプリケーションシステムを示す概略構成図である。

【図2】この発明の実施の形態1によるWebアプリケーションシステムのハードウェア構成例を示す図である。

【図3】この発明の実施の形態1によるWebアプリケーションシステムのユーザ・組織・ロール情報の例を示す図である。

【図4】この発明の実施の形態1によるWebアプリケーションシステムの業務情報の例を示す図である。 10

【図5】この発明の実施の形態1によるWebアプリケーションシステムのアクセス権限割当情報の例を示す図である。

【図6】この発明の実施の形態1によるWebアプリケーションシステムのアクセス権限設定機能の動作を示すフローチャートである。

【図7】この発明の実施の形態1によるWebアプリケーションシステムで用いられる画面例を示す図である。

【図8】この発明の実施の形態2によるWebアプリケーションシステムを示す概略構成図である。

【図9】この発明の実施の形態2によるWebアプリケーションシステムで用いる引継ぎ画面の例を示す図である。 20

【図10】この発明の実施の形態2によるWebアプリケーションシステムのアクセス権限割当情報110の例を示す図である。

【図11】この発明の実施の形態3によるWebアプリケーションシステムを示す概略構成図である。

【図12】この発明の実施の形態3によるWebアプリケーションシステムの業務種別定義情報の例を示す図である。

【図13】この発明の実施の形態4によるWebアプリケーションシステムを示す概略構成図である。

【図14】この発明の実施の形態4によるWebアプリケーションシステムで用いられるアクセス権限割当テンプレートの例を示す図である。 30

【図15】この発明の実施の形態5によるWebアプリケーションシステムを示す概略構成図である。

【図16】この発明の実施の形態5によるWebアプリケーションシステムで用いる業務委託画面の例を示す図である。

【符号の説明】

【0052】

1 アクセス制御設定機能

6 ユーザの要求

11 アクセス制御機能 40

12 業務アプリケーション

21 ユーザインターフェース機能

22 ユーザ・組織・ロール情報操作機能

23 アクセス権限割当情報操作機能

24 業務情報操作機能

25 権限引継ぎ設定機能

26 業務種別操作機能

27 アクセス権限テンプレート機能

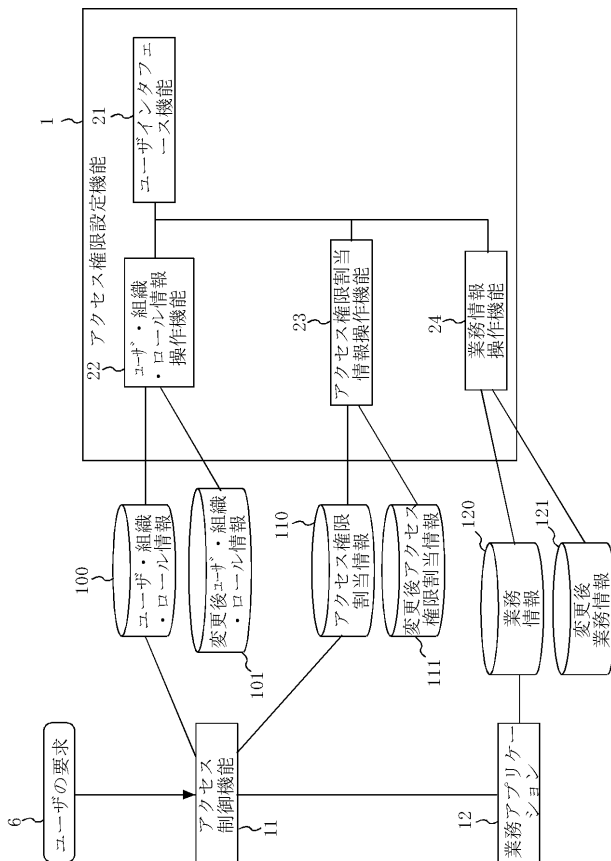
28 アクセス権限割当テンプレート

29 業務委託機能 50

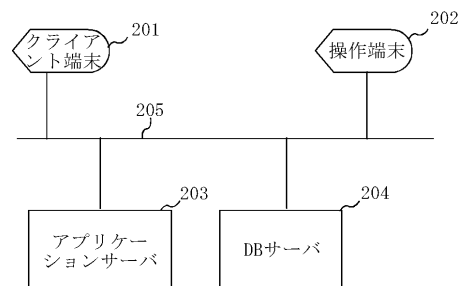
- 1 0 0 ユーザ・組織・ロール情報
- 1 0 1 変更後ユーザ・組織・ロール情報
- 1 0 2 組織情報
- 1 0 3 ユーザ情報
- 1 0 4 ロール情報
- 1 1 0 アクセス権限割当情報
- 1 1 1 変更後アクセス権限割当情報
- 1 2 0 業務情報
- 1 2 1 変更後業務情報
- 1 2 2 業務種別定義情報
- 1 2 3 変更後業務種別定義情報
- 2 0 1 クライアント端末
- 2 0 2 操作端末
- 2 0 3 アプリケーションサーバ
- 2 0 4 DBサーバ
- 2 0 5 ネットワーク
- 3 0 1 アクセス権限割当画面
- 3 0 2 アクセス権限割当画面

10

【図 1】



【図 2】



【図 3】

102

内部ID	部門コード	名称	上位部門
1	O000	会社	O000
2	OA00	総務部	O000
3	OA01	総務部総務 1 課	OA00
4	OA02	総務部総務 2 課	OA00
5	OB00	技術部	O000
6	OB01	技術部第 1 課	OB00
7	OB02	技術部第 2 課	OB00

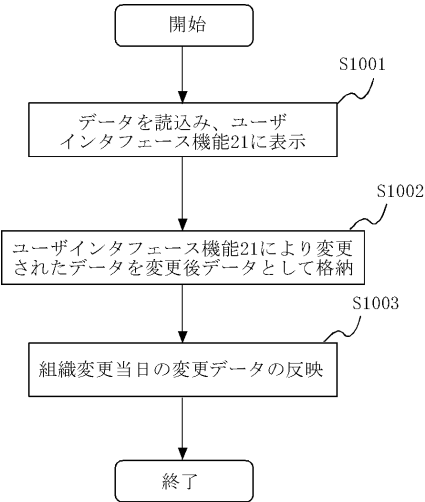
103

内部ID	社員コード	名称	所属部門	役職
1	U001	鈴木一郎	O000	社長
2	U002	鈴木二郎	OA00	部長
3	U003	鈴木三郎	OB00	部長
4	U004	佐藤一郎	OA01	課長
5	U005	佐藤二郎	OA02	課長
6	U006	佐藤三郎	OB01	課長
7	U007	佐藤四郎	OB02	課長
8	U008	田中一郎	OA01	社員
9	U009	田中二郎	OA02	社員
10	U010	田中三郎	OB01	社員
11	U011	田中四郎	OB02	社員
12	U100	高橋太郎	OA00	委託先社員

104

内部ID	ロールコード	ロール名称	ユーザ・組織情報
1	R001	間接	O000,OA00
2	R002	直接	OB00
3	R003	本社	O000,OA00,OA01,OB02
4	R004	支社	OA02,OB00,OB01,U0100
5	R005	案件 1 全員	OB00,OB01
6	R006	案件 2 全員	OB00,OB02
7	R007	案件 1 開発者	OB01
8	R008	案件 2 開発者	OB02,U100
9	R009	案件 3	U004,U008
10	R010	総務部課長	OA00^課長
11	R011	技術部課長	OB00^課長

【図 6】



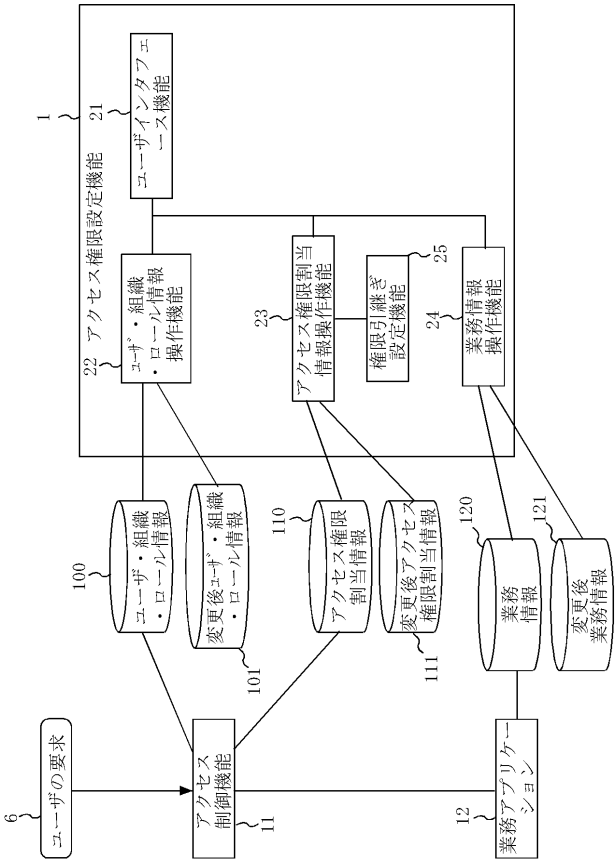
【図 4】

内部ID	業務コード	業務データ名称	対象操作	主管部門
1	J001	総務部データ	表示	総務部
2	J002	総務部データ	編集	総務部
3	J101	案件1技術情報	表示	技術部第 1 課
4	J102	案件1技術情報	編集	技術部第 1 課
5	J201	案件2技術情報	表示	技術部第 2 課
6	J202	案件2技術情報	編集	技術部第 2 課
7	J301	案件3技術情報	表示	技術部第 1 課
8	J302	案件3技術情報	編集	技術部第 1 課
9	J003	本社データ	表示	総務部第 1 課
10	J004	支社データ	表示	総務部第 2 課

【図 5】

内部ID	業務コード*	ロールコード*	業務コード* 内部ID	ロールコード* 内部ID
1	J101	R005	3	5
2	J102	R007	4	7
3	J201	R006	5	6
4	J202	R008	6	8
5	J301	R009	7	9
6	J302	R009	8	9

【図 8】



【図 9】

権限の引継ぎ指定(案件1 技術情報・表示)

方式：◎組織変更前操作 ○組織変更後操作

部門

案件1開発者 ▼

期間

1月1日～1月31日

登録

キャンセル

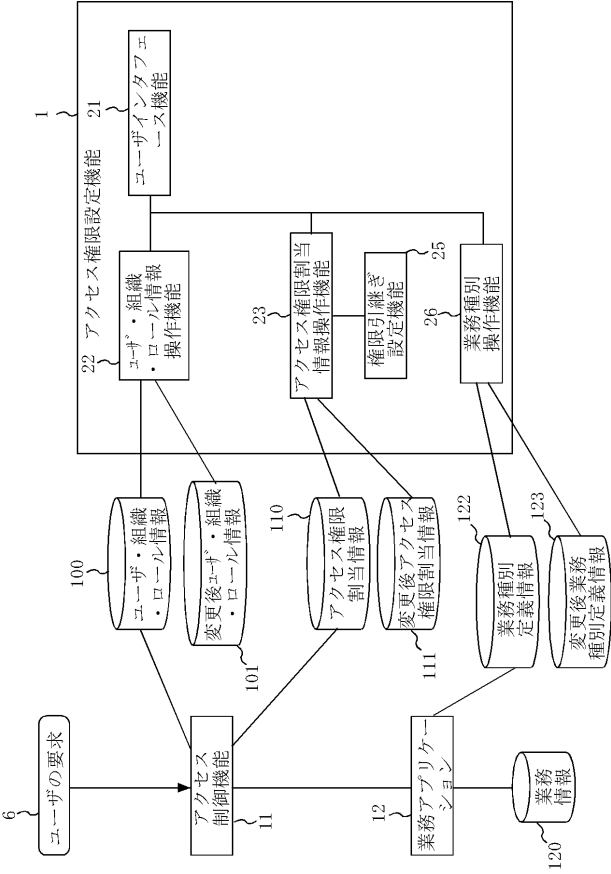
【図 10】

内部ID	業務コード	ロールコード	開始日	終了日
1	J101	R007	2008年2月1日	
2	J102	R007	2008年2月1日	
3	J301	R007	2008年1月1日	2008年1月31日

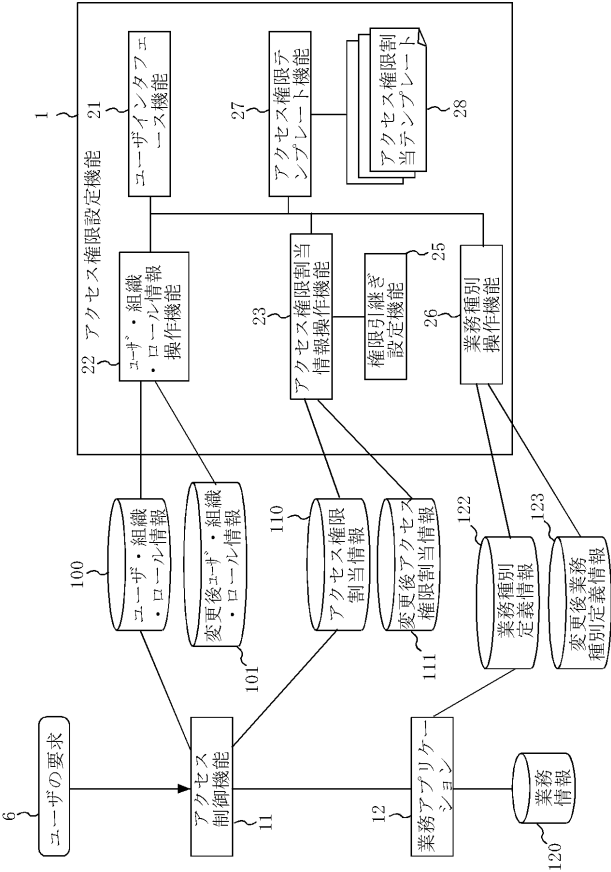
【図 12】

内部ID	業務種別コード	業務データ名称	業務コード	主管部門
1	T001	総務部データ	J001, J002	総務部
2	T101	案件1情報	J101, J102	技術部第1課
3	T201	案件2情報	J201, J202	技術部第2課
4	T301	案件3情報	J301, J302	技術部第1課
5	T003	本社データ	J003	総務部第1課
6	T004	支社データ	J004	総務部第2課

【図 11】



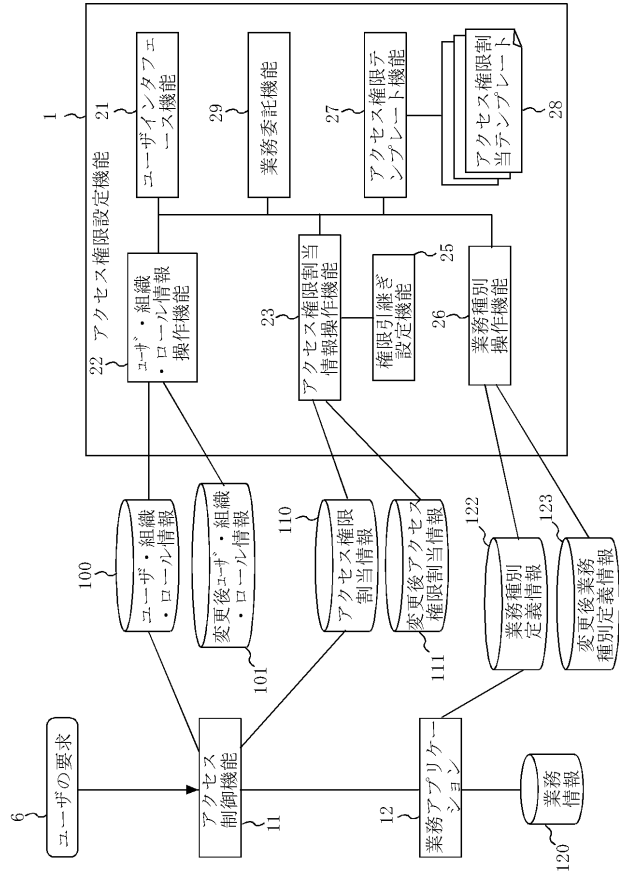
【図 13】



【図 1 4】

業務種別：案件 1 情報		
対象ロール：新規割当時のみ、 固定		
業務情報	業務操作	アクセス権限
全て	新規作成	X
全て	表示	○
全て	ダウンロード	○
全て	印刷	○
全て	編集	X
全て	削除	X
全て	新規作成	X
個人情報	表示	○
個人情報	編集	○

【図 1 5】



【図 1 6】

業務委託（業務種別：案件 1 技術情報）	
部門	技術部第1課 ▼
ユーザ	田中一郎 ▼
ロール	自動 ▼
期間	○月○日～△月△日
登録 キャンセル	

【図 7】

301

表示範囲		技術部第1課 ▼							
業務データ 名称	ロール 操作	支社	案件1 全員	案件2 全員	案件1 開発者	案件2 開発者	案件3	総務部 課長	技術部 課長
総務部データ	表示								
総務部データ	編集								
案件1技術情報	表示		●						●
案件1技術情報	編集				●				
案件2技術情報	表示			●					●
案件2技術情報	編集					●			
案件3技術情報	表示						●		●
案件3技術情報	編集						●		
本社データ	表示								
支社データ	表示								

◀ [] ▶



302

表示範囲		技術部第1課 ▼							
業務データ 名称	ロール 操作	支社	案件1 全員	案件2 全員	案件1 開発者	案件2 開発者	案件3	総務部 課長	技術部 課長
総務部データ	表示								
総務部データ	編集								
案件1技術情報	表示		●						●
案件1技術情報	編集				●				
案件2技術情報	表示			●					●
案件2技術情報	編集					●			
案件3技術情報	表示						●		●
案件3技術情報	編集						●		
本社データ	表示								
支社データ	表示								

◀ [] ▶