(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5645034号
(P5645034)
(45)発行日　平成26年12月24日(2014.12.24)　(24)登録日　平成26年11月14日(2014.11.14)

(51)Int.Cl.　F I
G06F 21/62 (2013.01)　G06F 21/24 163D
G06F 21/24 165G

請求項の数 10　(全 22 頁)

(21)出願番号　特願2012-508215(P2012-508215)
(86)(22)出願日　平成23年3月11日(2011.3.11)
(86)国際出願番号　PCT/JP2011/056498
(87)国際公開番号　WO2011/122366
(87)国際公開日　平成23年10月6日(2011.10.6)
審査請求日　平成26年2月10日(2014.2.10)
(31)優先権主張番号　特願2010-80187(P2010-80187)
(32)優先日　平成22年3月31日(2010.3.31)
(33)優先権主張国　日本国(JP)

（出願人による申告）平成２０年度　経済産業省セキュア・プラットフォームプロジェクトに係る委託研究、産業技術力強化法第１９条の適用を受ける特許出願

(73)特許権者　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(74)代理人　100077838
弁理士　池田　憲保
(74)代理人　100082924
弁理士　福田　修一
(74)代理人　100129023
弁理士　佐々木　敬
(72)発明者　森田　陽一郎
東京都港区芝五丁目７番１号　日本電気株式会社内

審査官　青木　重徳

最終頁に続く

(54)【発明の名称】アクセス制御プログラム、システム及び方法

(57)【特許請求の範囲】
【請求項１】
一乃至複数のロールと、そのロールを割り当てられたサブジェクトとを関連づけたサブジェクト割当、ロールと、権限と、そのロールを割り当てられたサブジェクトがその権限を実行することの可否とを関連づけた権限割当、及び、ロール間の継承関係を示すロール階層を記憶装置に格納する手順と、
前記サブジェクト割当の中で一のサブジェクトに対して複数のロールが割り当てられているか否かを判定し、割り当てられている場合、該当する複数のロールＲ１、Ｒ２、…、Ｒｍ（ｍは２以上の自然数）を取得する手順と、
前記ロール階層及び権限割当に基づいて、前記複数のロールＲ１、Ｒ２、…、Ｒｍの各ロールに対応する権限可否を継承により導出する第１の権限可否導出手順と、
前記継承により導出した権限可否のうち、前記複数のロールＲ１、Ｒ２、…、Ｒｍの中の別のロールに由来する権限であって、かつ、その可否が異なる権限Ａ１、Ａ２、…、Ａｎ（ｎは自然数）を、前記複数のロールＲ１、Ｒ２、…、Ｒｍの組の間で競合する権限として記憶装置に格納する手順と、
前記ロールＲ１、Ｒ２、…、Ｒｍの組を割り当てられた一のサブジェクトの前記権限Ａ１、Ａ２、…、Ａｎの可否を、入力装置を介して受け付ける手順と、
受け付けた可否に基づいて、前記ロールＲ１、Ｒ２、…、Ｒｍの組に関する前記権限Ａ１、Ａ２、…、Ａｎの可否を、前記ロールＲ１、Ｒ２、…、Ｒｍの組からなる仮想的なロールである例外ロールに対する例外権限割当として記憶装置に記憶する手順と、

前記ロール階層、権限割当及び例外権限割当に基づいて、前記例外ロールの各ロールＲ１、Ｒ２、…、Ｒｍに対応する権限可否を継承により導出する第２の権限可否導出手順とをコンピュータに実行させるためのアクセス制御プログラム。

【請求項２】

前記第２の権限可否導出手順は、

前記ロール階層に基づいて、前記複数のロールＲ１、Ｒ２、…、Ｒｍそれぞれの継承元となるロールを取得する手順と、

前記権限割当に基づいて、前記複数のロールＲ１、Ｒ２、…、Ｒｍ及びこれらロールの継承元となるロールのそれぞれについて権限の可否を取得し、前記例外権限割当に基づいて、前記例外ロールの権限の可否を取得する手順と、

前記例外ロールを割り当てられたサブジェクトの権限可否を継承により導出する手順とを含むことを特徴とする、請求項１に記載のアクセス制御プログラム。

【請求項３】

前記例外ロールを割り当てられたサブジェクトの権限可否を継承により導出する際、前記例外ロールを、前記複数のロールＲ１、Ｒ２、…、Ｒｍを継承元とする多重継承のロールとして扱うことを特徴とする、請求項２に記載のアクセス制御プログラム。

【請求項４】

第１の権限可否導出手順は、

前記ロール階層に基づいて、前記複数のロールＲ１、Ｒ２、…、Ｒｍそれぞれの継承元となるロールを取得する手順と、

前記権限割当に基づいて、前記複数のロールＲ１、Ｒ２、…、Ｒｍ及びこれらロールの継承元となるロールのそれぞれについて権限の可否を取得する手順と、

前記複数のロールＲ１、Ｒ２、…、Ｒｍの各ロールに対応する権限可否を継承により導出する手順と

を含むことを特徴とする請求項１に記載のアクセス制御プログラム。

【請求項５】

一乃至複数のロールと、そのロールを割り当てられたサブジェクトとを関連づけたサブジェクト割当と、ロールと、権限と、そのロールを割り当てられたサブジェクトがその権限を実行することの可否とを関連づけた権限割当と、ロール間の継承関係を示すロール階層とを格納する一乃至複数の記憶装置と、

前記サブジェクト割当の中で一のサブジェクトに対して複数のロールが割り当てられているか否かを判定し、割り当てられている場合、該当する複数のロールＲ１、Ｒ２、…、Ｒｍ（ｍは２以上の自然数）を取得する処理装置と、

前記ロール階層及び権限割当に基づいて、前記複数のロールＲ１、Ｒ２、…、Ｒｍの各ロールに対応する権限可否を継承により導出する第１の権限可否導出処理装置と、

前記継承により導出した権限可否のうち、前記複数のロールＲ１、Ｒ２、…、Ｒｍの中の別のロールに由来する権限であって、かつ、その可否が異なる権限Ａ１、Ａ２、…、Ａｎ（ｎは自然数）を、前記複数のロールＲ１、Ｒ２、…、Ｒｍの組の間で競合する権限として記憶装置に格納する処理装置と、

前記ロールＲ１、Ｒ２、…、Ｒｍの組を割り当てられた一のサブジェクトの前記権限Ａ１、Ａ２、…、Ａｎの可否を、入力装置を介して受け付ける処理装置と、

受け付けた可否に基づいて、前記ロールＲ１、Ｒ２、…、Ｒｍの組に関する前記権限Ａ１、Ａ２、…、Ａｎの可否を、前記ロールＲ１、Ｒ２、…、Ｒｍの組からなる仮想的なロールである例外ロールに対する例外権限割当として記憶装置に記憶する処理装置と、

前記ロール階層、権限割当及び例外権限割当に基づいて、前記例外ロールの各ロールＲ１、Ｒ２、…、Ｒｍに対応する権限可否を継承により導出する第２の権限可否導出処理装置と

を備えることを特徴とするアクセス制御システム。

【請求項６】

前記第２の権限可否導出処理装置は、

前記ロール階層に基づいて、前記複数のロールＲ１、Ｒ２、…、Ｒｍそれぞれの継承元となるロールを取得し、
前記権限割当に基づいて、前記複数のロールＲ１、Ｒ２、…、Ｒｍ及びこれらロールの継承元となるロールのそれぞれについて権限の可否を取得し、前記例外権限割当に基づいて、前記例外ロールの権限の可否を取得し、
前記例外ロールを割り当てられたサブジェクトの権限可否を継承により導出する
ことを特徴とする請求項５に記載のアクセス制御システム。
【請求項７】
前記例外ロールを割り当てられたサブジェクトの権限可否を継承により導出する際、前記例外ロールを、前記複数のロールＲ１、Ｒ２、…、Ｒｍを継承元とする多重継承のロールとして扱うことを特徴とする、請求項６に記載のアクセス制御システム。
【請求項８】
第１の権限可否導出処理装置は、
前記ロール階層に基づいて、前記複数のロールＲ１、Ｒ２、…、Ｒｍそれぞれの継承元となるロールを取得し、
前記権限割当に基づいて、前記複数のロールＲ１、Ｒ２、…、Ｒｍ及びこれらロールの継承元となるロールのそれぞれについて権限の可否を取得し、
前記複数のロールＲ１、Ｒ２、…、Ｒｍの各ロールに対応する権限可否を継承により導出する
ことを特徴とする請求項５に記載のアクセス制御システム。
【請求項９】
一乃至複数のロールと、そのロールを割り当てられたサブジェクトとを関連づけたサブジェクト割当、ロールと、権限と、そのロールを割り当てられたサブジェクトがその権限を実行することの可否とを関連づけた権限割当、及び、ロール間の継承関係を示すロール階層を記憶装置に格納する手順をコンピュータにて実行する段階と、
前記サブジェクト割当の中で一のサブジェクトに対して複数のロールが割り当てられているか否かを判定し、割り当てられている場合、該当する複数のロールＲ１、Ｒ２、…、Ｒｍ（ｍは２以上の自然数）を取得する手順をコンピュータにて実行する段階と、
前記ロール階層及び権限割当に基づいて、前記複数のロールＲ１、Ｒ２、…、Ｒｍの各ロールに対応する権限可否を継承により導出する手順をコンピュータにて実行する第１の権限可否導出段階と、
前記継承により導出した権限可否のうち、前記複数のロールＲ１、Ｒ２、…、Ｒｍの中の別のロールに由来する権限であって、かつ、その可否が異なる権限Ａ１、Ａ２、…、Ａｎ（ｎは自然数）を、前記複数のロールＲ１、Ｒ２、…、Ｒｍの組の間で競合する権限として記憶装置に格納する手順をコンピュータにて実行する段階と、
前記ロールＲ１、Ｒ２、…、Ｒｍの組を割り当てられた一のサブジェクトの前記権限Ａ１、Ａ２、…、Ａｎの可否を、入力装置を介して受け付ける手順をコンピュータにて実行する段階と、
受け付けた可否に基づいて、前記ロールＲ１、Ｒ２、…、Ｒｍの組に関する前記権限Ａ１、Ａ２、…、Ａｎの可否を、前記ロールＲ１、Ｒ２、…、Ｒｍの組からなる仮想的なロールである例外ロールに対する例外権限割当として記憶装置に記憶する手順をコンピュータにて実行する段階と、
前記ロール階層、権限割当及び例外権限割当に基づいて、前記例外ロールの各ロールＲ１、Ｒ２、…、Ｒｍに対応する権限可否を継承により導出する手順をコンピュータにて実行する第２の権限可否導出段階と
を含むことを特徴とするアクセス制御方法。
【請求項１０】
第２の権限可否導出段階は、
前記ロール階層に基づいて、前記複数のロールＲ１、Ｒ２、…、Ｒｍそれぞれの継承元となるロールを取得する手順をコンピュータにて実行する段階と、

前記権限割当に基づいて、前記複数のロールＲ１、Ｒ２、…、Ｒｍ及びこれらロールの継承元となるロールのそれぞれについて権限の可否を取得し、前記例外権限割当に基づいて、前記例外ロールの権限の可否を取得する手順をコンピュータにて実行する段階と、

前記例外ロールを割り当てられたサブジェクトの権限可否を継承により導出する手順をコンピュータにて実行する段階と

を含むことを特徴とする、請求項９に記載のアクセス制御方法。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明はコンピュータセキュリティのアクセス制御に関し、特に、ロールベースアクセス制御（ＲＢＡＣ）に関する。

【背景技術】

【０００２】

一般に、ロールベースアクセス制御では、管理ポリシーの記述に際してロールという概念を利用する。ロールとは役割を示し、役割を遂行する上で必要な権限の集合をロールとしてまとめる。サブジェクトに対しては個々の権限を割り当てるのではなく、ロールを割り当てる。これにより、ルール作成者は個々の主体毎及び対象毎に夫々のアクションを規定した沢山のアクセス制御ルールを記述する必要が無くなり、アクセス制御ルールの作成負担が軽減される。

本発明に関連する技術が記載された文献として特開平１１－３１３１０２号公報（以下特許文献１と記す）の図１、図１９を挙げる。同文献に記載のアクセス制御方法は、アクセス主体種別と、アクセス対象種別と、組織構造に基づく制約条件によって記述されたアクセス制御ポリシーから、アクセス主体と、アクセス対象によって記述されたアクセス制御リストを生成する方法である。このアクセス制御方法は、主体（アクセス主体）と主体種別とを直接に対応付ける主体種別グループ情報と、対象（アクセス対象）と対象種別とを直接に対応付ける対象種別グループ情報と、主体および対象と組織との対応付けを単一の木構造で表現した組織構造情報とを持ち、これを使用して制約条件を満足するアクセス制御リストのみを生成可能としている。

【発明の開示】

【発明が解決しようとする課題】

【０００３】

組織構造やプロジェクトなどのロールが存在し、サブジェクトとして、付与されるロールの組み合わせや順序が異なるユーザが存在する場合があるが、このような場合、従来は、ロールと権限可否の関係を定義する際に、ユーザ毎にすべての権限を書き下す必要があった。

また、特許文献１に記載されているアクセス制御方法では、複数の独立した木構造を持つロール階層の中から、任意の複数のロール（主体種別）を同時に付与されたサブジェクトについて、当該ロール毎にまとめられた権限同士が矛盾する場合に、どのようにアクセス制御ルールを生成すべきかを判断する方法が無いので、複数の独立した木構造を持つロール階層の中から、任意の複数のロールを兼務するサブジェクトに対するアクセス制御内容を記述することができなかった。

本発明はこのような状況に鑑みてなされたものであり、本発明が解決しようとする課題は、組織構造など、複数の独立した木構造を持つロール階層の中から、任意の複数のロールを兼務するサブジェクトが存在し、導出されるアクセス権可否が兼務しているロール間で競合する場合でも、競合を解消することができる、アクセス制御方法、アクセス制御システムおよびアクセス制御用プログラ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】

【０００４】

上述の課題を解決するため、本発明は、次のようなアクセス制御プログラム、システム及び方法を提供する。

即ち、本発明はその一態様として、一乃至複数のロールと、そのロールを割り当てられたサブジェクトとを関連づけたサブジェクト割当、ロールと、権限と、そのロールを割り当てられたサブジェクトがその権限を実行することの可否とを関連づけた権限割当、及び、ロール間の継承関係を示すロール階層を記憶装置に格納する手順と、サブジェクト割当の中で一のサブジェクトに対して複数のロールが割り当てられているか否かを判定し、割り当てられている場合、該当する複数のロールＲ１、Ｒ２、…、Ｒｍ（ｍは２以上の自然数）を取得する手順と、ロール階層及び権限割当に基づいて、複数のロールＲ１、Ｒ２、…、Ｒｍの各ロールに対応する権限可否を継承により導出する第１の権限可否導出手順と、継承により導出した権限可否のうち、複数のロールＲ１、Ｒ２、…、Ｒｍの中の別のロールに由来する権限であって、かつ、その可否が異なる権限Ａ１、Ａ２、…、Ａｎ（ｎは自然数）を、複数のロールＲ１、Ｒ２、…、Ｒｍの組の間で競合する権限として記憶装置に格納する手順と、ロールＲ１、Ｒ２、…、Ｒｍの組を割り当てられた一のサブジェクトの権限Ａ１、Ａ２、…、Ａｎの可否を、入力装置を介して受け付ける手順と、受け付けた可否に基づいて、ロールＲ１、Ｒ２、…、Ｒｍの組に関する権限Ａ１、Ａ２、…、Ａｎの可否を、ロールＲ１、Ｒ２、…、Ｒｍの組からなる仮想的なロールである例外ロールに対する例外権限割当として記憶装置に記憶する手順と、ロール階層、権限割当及び例外権限割当に基づいて、例外ロールの各ロールＲ１、Ｒ２、…、Ｒｍに対応する権限可否を継承により導出する第２の権限可否導出手順とをコンピュータに実行させるためのアクセス制御プログラムを提供する。

また、本発明は他の態様として、一乃至複数のロールと、そのロールを割り当てられたサブジェクトとを関連づけたサブジェクト割当と、ロールと、権限と、そのロールを割り当てられたサブジェクトがその権限を実行することの可否とを関連づけた権限割当と、ロール間の継承関係を示すロール階層とを格納する一乃至複数の記憶装置と、サブジェクト割当の中で一のサブジェクトに対して複数のロールが割り当てられているか否かを判定し、割り当てられている場合、該当する複数のロールＲ１、Ｒ２、…、Ｒｍ（ｍは２以上の自然数）を取得する処理装置と、ロール階層及び権限割当に基づいて、複数のロールＲ１、Ｒ２、…、Ｒｍの各ロールに対応する権限可否を継承により導出する第１の権限可否導出処理装置と、継承により導出した権限可否のうち、複数のロールＲ１、Ｒ２、…、Ｒｍの中の別のロールに由来する権限であって、かつ、その可否が異なる権限Ａ１、Ａ２、…、Ａｎ（ｎは自然数）を、複数のロールＲ１、Ｒ２、…、Ｒｍの組の間で競合する権限として記憶装置に格納する処理装置と、ロールＲ１、Ｒ２、…、Ｒｍの組を割り当てられた一のサブジェクトの権限Ａ１、Ａ２、…、Ａｎの可否を、入力装置を介して受け付ける処理装置と、受け付けた可否に基づいて、ロールＲ１、Ｒ２、…、Ｒｍの組に関する権限Ａ１、Ａ２、…、Ａｎの可否を、ロールＲ１、Ｒ２、…、Ｒｍの組からなる仮想的なロールである例外ロールに対する例外権限割当として記憶装置に記憶する処理装置と、ロール階層、権限割当及び例外権限割当に基づいて、例外ロールの各ロールＲ１、Ｒ２、…、Ｒｍに対応する権限可否を継承により導出する第２の権限可否導出処理装置とを備えることを特徴とするアクセス制御システムを提供する。

更に、本発明は他の態様として、一乃至複数のロールと、そのロールを割り当てられたサブジェクトとを関連づけたサブジェクト割当、ロールと、権限と、そのロールを割り当てられたサブジェクトがその権限を実行することの可否とを関連づけた権限割当、及び、ロール間の継承関係を示すロール階層を記憶装置に格納する手順をコンピュータにて実行する段階と、サブジェクト割当の中で一のサブジェクトに対して複数のロールが割り当てられているか否かを判定し、割り当てられている場合、該当する複数のロールＲ１、Ｒ２、…、Ｒｍ（ｍは２以上の自然数）を取得する手順をコンピュータにて実行する段階と、ロール階層及び権限割当に基づいて、複数のロールＲ１、Ｒ２、…、Ｒｍの各ロールに対応する権限可否を継承により導出する手順をコンピュータにて実行する第１の権限可否導出段階と、継承により導出した権限可否のうち、複数のロールＲ１、Ｒ２、…、Ｒｍの中の別のロールに由来する権限であって、かつ、その可否が異なる権限Ａ１、Ａ２、…、Ａｎ（ｎは自然数）を、複数のロールＲ１、Ｒ２、…、Ｒｍの組の間で競合する権限として

記憶装置に格納する手順をコンピュータにて実行する段階と、ロールＲ１、Ｒ２、…、Ｒｍの組を割り当てられた一のサブジェクトの権限Ａ１、Ａ２、…、Ａｎの可否を、入力装置を介して受け付ける手順をコンピュータにて実行する段階と、受け付けた可否に基づいて、ロールＲ１、Ｒ２、…、Ｒｍの組に関する権限Ａ１、Ａ２、…、Ａｎの可否を、ロールＲ１、Ｒ２、…、Ｒｍの組からなる仮想的なロールである例外ロールに対する例外権限割当として記憶装置に記憶する手順をコンピュータにて実行する段階と、ロール階層、権限割当及び例外権限割当に基づいて、例外ロールの各ロールＲ１、Ｒ２、…、Ｒｍに対応する権限可否を継承により導出する手順をコンピュータにて実行する第２の権限可否導出段階とを含むことを特徴とするアクセス制御方法を提供する。

【発明の効果】

【０００５】

本発明によれば、従来同様にロール毎に権限を記述するだけで、複数のロールを一のサブジェクトに割り当てられたときに発生する、ロール間での権限可否の競合を検出して、競合する権限の可否を例外的に定義した例外権限割当をユーザ入力に応じて生成して、競合を解消する。

このため、本発明によれば、組織構造やプロジェクトなどのロールが存在し、サブジェクトとして、付与されるロールの組み合わせや順序が異なるユーザが存在する場合でも、ロールと権限可否の関係を定義する際に、ユーザ毎にすべての権限を書き下す必要がない。

また、本発明によれば、付与されるロールの組み合わせや順序が異なるユーザが存在する場合でも、ロールと権限可否の関係を定義する際に、ユーザ毎にすべての権限を書き下すことなく従来と同じ方法・システムで記述するだけで、例外的な定義が必要なサブジェクトと権限の組み合わせのみについて、例外的なロールと権限可否の関係を定義し、競合を解消することができる。

【図面の簡単な説明】

【０００６】

図１は本発明の一実施の形態であるアクセス制御システム１００のシステム構成図である。

図２はアクセス制御システム１００の動作を示すフローチャートである。

図３は競合検出部５が実行する競合検出処理について説明するためのフローチャートである。

図４はサブジェクト割当格納部２が記憶する、サブジェクト割当の例である。

図５はロール階層格納部１が記憶する、ロール階層の例である。

図６は権限割当格納部３が記憶する、権限割当の例である。

図７は競合検出部５が生成する、ロールの継承処理後の権限可否の例である。

図８は競合検出部５が生成する、競合を示す情報の例である。

図９は例外権限割当編集部６が実行する例外権限割当編集処理について説明するためのフローチャートである。

図１０は例外権限割当編集部６が生成する例外権限割当の編集を行うユーザインタフェースの例である。

図１１は例外権限割当編集部６が生成する、例外権限割当の例である。

図１２は競合検出部５が生成する、ロールの継承処理後の権限可否の例である。

【発明を実施するための最良の形態】

【０００７】

（用語の説明）

本発明の実施の形態に関する説明に先立って、説明で用いる用語について説明する。

「アクセス権」は、特定のサブジェクト（ｓ）、オブジェクト（ｏ）、アクション（ａ）の組を意味する。「アクセス権可否」は、特定のアクセス権と、アクセス権に対する許可あるいは拒否を示す識別子との組を意味する。

「権限」は、特定のオブジェクト（ｏ）、アクション（ａ）の組を意味する。「権限可

否」は、特定の権限と、権限に対する許可あるいは拒否を示す識別子との組を意味する。

「ロール」は、権限可否の集合に対して付与される識別子である。一般的には所属部署や役職、担当するプロジェクト・業務内容・作業項目などの名称が使用される。各サブジェクトは、０個以上のロールを持つ。一般的に、ロールを持たない（０個のロールを持つ）サブジェクトは、権限を持たない。

「サブジェクト割当」は、ロールに対するサブジェクトの割当の定義である。記述形式としては、ロールのリストとサブジェクトとの組として記述する。一般的に、サブジェクトが複数のロールを持つ際、主要なロールと、副次的なロールなど、ロール間に序列が存在する。同じロールの組み合わせを持つサブジェクト同士でも、サブジェクト毎にロール間の序列が異なると、個々のサブジェクトに対して割り当てたい権限可否の集合は異なる。例えば、ロールとして「総務部」と「経理部」が存在するとき、サブジェクトＡは「総務部」が主務で「経理部」が兼務、サブジェクトＢは「経理部」が主務で「総務部」が兼務などの場合、「総務部」と「経理部」の権限可否が競合すると、サブジェクトＡは「総務部」の権限可否に従うが、サブジェクトＢは「経理部」の権限可否に従うなどの違いが発生する。そこで、ロールに対するサブジェクトの割当の定義では、ロールの序列に基づいて、ロールを序列の順に並べたリストとして扱い、このロールリストとサブジェクトとの組として記述する。従って、序列の有るロールリストとしては、「経理部、総務部」と「総務部、経理部」を別のものとして扱い、組となるサブジェクトも別となる。

ロール間に序列がない場合や、序列を考慮しない場合は、所定の順序に従ってロールリストにロールを並べることとしてもよい。例えば、文字コード順、アルファベット順、５０音順にロール或いはロールに対応する文字列を並べることが考えられる。具体例を挙げると、「経理部、総務部」と「総務部、経理部」を互いに区別しないこととし、５０音順にロール総務部、ロール経理部を並べて、「経理部、総務部」と表記することとしてもよい。

また、ロール間に序列がある場合とない場合の両方が混在する場合、序列の有無に応じて異なる表記形態を用いることが考えられる。例えば、ロール間に序列がある場合は「［］」にてそれらのロールを括り、序列がない場合は「（）」にてそれらのロールを括るといったことが考えられる。具体例として、「（［Ａ株式会社経理部、Ａ株式会社総務部］、［Ｂ株式会社経理部、Ｂ株式会社総務部］）」との表記を考えると、この表記は「（［Ａ株式会社経理部、Ａ株式会社総務部］、［Ｂ株式会社経理部、Ｂ株式会社総務部］）」と「（［Ｂ株式会社経理部、Ｂ株式会社総務部］、［Ａ株式会社経理部、Ａ株式会社総務部］）」の両方を含み、かつ、「（［Ａ株式会社経理部、Ａ株式会社総務部］、［Ｂ株式会社総務部、Ｂ株式会社経理部］）」や「（［Ａ株式会社総務部、Ａ株式会社経理部］、［Ｂ株式会社経理部、Ｂ株式会社総務部］）」などは含まない。

このように、ロールリストを応用すると、一定の表記方法を選択して統一しておくことで、どの範囲のロールの組み合わせをまとめて扱うかを選択でき、ひいては後述する例外権限割当においてどのようなサブジェクトのまとまり毎に権限割当を行うかを選択できる。以降では、ロールリストを、最も一般的な形式である序列の有るロールリストとして扱うが、上記のように応用した場合でも、同様の構成および動作によって処理可能である。

「権限割当」は、ロールに対応する、権限可否の集合を定義する記述である。

「ロール階層」および「階層」は、組織構造などに基づくロールの階層関係を意味する。一般的には、ロール階層は多段階の階層を持つ木構造となる。例えば、ある企業「Ａ株式会社」のロール階層は、１つの木構造となり、「Ａ株式会社」を根とし、その配下に「総務部」と「経理部」を持ち、さらに「総務部」の配下に「秘書課」と「広報課」を持つ。

ロール階層として上述のＡ株式会社の例のような木構造が複数存在することとしてもよい。例えば、Ａ株式会社とは別にＢ株式会社の木構造が同時に存在する場合を考える。Ｂ株式会社の木構造は、「Ｂ株式会社」を根とするロール階層であり、その配下に「Ａ株式会社」を根とするロール階層と同じく、「総務部」と「経理部」を持ち、さらに「総務部」の配下に「秘書課」と「広報課」を持つことが考えられる。或いは、Ｂ株式会社の木構

造は、「Ａ株式会社」を根とするロール階層とは異なり、「開発部」と「営業部」を持つことも考えられる。本発明では、これら独立した木構造を持つ複数のロール階層に跨るようなロール兼務における権限可否の競合の場合でも、単一の木構造を持つロール階層におけるロール兼務における権限可否の競合の場合と同様の構成および動作によって処理可能である。

「ロール継承」および「継承」は、ロール階層に基づく継承関係を意味する。例えば、上記のロール階層における例では、「秘書課」ロールは「総務部」ロールを継承しており、「総務部」ロールは「Ａ株式会社」ロールを継承している。ロールを継承することにより、継承先のロールは、継承元のロールの権限可否の集合を引き継ぐ。継承先の集合は、継承元の集合よりも優先度が高く、継承元の権限可否を継承先の権限可否で修正することが出来る。したがって、継承先のロールを持つサブジェクトは、継承元のロールと継承先のロールの両者の権限可否の集合が適用されるが、両者で同じ権限について可否との組み合わせが異なる場合は、継承先の権限可否が適用される。なお、「例外ロール」を除き、あるロールが継承元とするロールは、１つのみである。

「直系ロール」および「直系」は、継承を子が親を継承する親子関係と見た場合に、ある任意のロールから見て直系の関係にあるロールであり。当該ロールと、先祖にあたるロールと、子孫にあたるロールとを合わせた集合である。先祖にあたるロールとは、木構造を有するロール階層において当該ロールから継承元を根まで辿る際に到達するロール群に属するすべてのロールである。子孫にあたるロールとは、木構造を有するロール階層において当該ロールから継承先を葉まで辿る際に到達するロール群に属するすべてのロールである。したがって、木構造において、直系ロールは、当該ロールと、当該ロールから継承元を根まで辿る際に到達するロール群と、当該ロールから継承先を葉まで辿る際に到達するロール群とを合わせた集合となる。なお、サブジェクトは複数のロールを持つが、それらロール同士は直系の関係にあってはならない。例えば、上記のロール階層における例では、Ａ株式会社総務部秘書課に所属するサブジェクトは、「秘書課」ロールのみを持ち、「Ａ株式会社」ロールや「総務部」ロールは持たない。Ａ株式会社総務部とＡ株式会社経理部を兼務するサブジェクトは、「総務部」ロールと「経理部」ロールを持ち、「Ａ株式会社」ロール・「秘書課」ロール・「広報課」ロールは持たない。

「例外ロール」および「例外」は、ロールの兼務によって権限可否が競合する状態にあるサブジェクトのみを、当該サブジェクトに対応するロールリスト毎に抽出し、抽出されたサブジェクトの集合が自動的に割り当てられる仮想的なロールである。

例外ロールの識別子には、例外ロールを割り当てたサブジェクトに対応するロールリストを使用する。例外ロールの権限割当では、当該サブジェクト集合が持つ各ロールに割り当てられた権限可否のうち、それらロール間で競合している権限のみを提示し、可否を指定する。

例外ロールは、当該ロールリストに挙げられているすべてのロールを継承元とする多重継承のロールとして扱い、継承元となったロールリストにあるロールの権限割当よりも、継承先となった例外ロールの権限割当が優先される。

また例外ロールは、ロールリストにあるロールの直系ロールとなるため、例外ロールを割り当てられたサブジェクトは、ロールリストにあるロールの割当からは仮想的に除外されたものとして扱う。よって、例外ロールを割り当てたサブジェクトについては、ロールリストにあるロールに割り当てられた権限可否のうち、ロール間で競合しない権限可否については例外ロールに継承されることでそのまま適用され、ロール間で競合する権限可否については例外ロールの権限割当に従う。これにより、ロールリストに存在するロールと同じロールを１つ以上持つが、当該例外ロールに割り当てられていないサブジェクト、つまり、ロールを兼務していないか、ロールの割当の組み合わせか序列が異なるサブジェクトについては、当該例外ロールの影響は受けないため、例外ロールによる権限の修正の影響を、それが関係する範囲だけに絞ることができ、また、個々のロールに対する権限割当やサブジェクト割当の際、競合しないよう、事前に権限やサブジェクトの切り分けを意識する必要が無くなる。

「例外権限割当」は、例外ロールに対応する、権限可否の集合を定義する記述である。例外ロールの識別子はロールリストのため、記述形式としては、ロールリストと、権限可否の集合との組である。

（アクセス制御システム１００）

本発明の一実施の形態であるアクセス制御システム１００について説明する。図１を参照すると、アクセス制御システム１００は、ロール階層格納部１、サブジェクト割当格納部２、権限割当格納部３、例外権限割当格納部４、競合検出部５、例外権限割当編集部６を備える。

アクセス制御システム１００は例えばコンピュータシステムで実現される。ロール階層格納部１、サブジェクト割当格納部２、権限割当格納部３、例外権限割当格納部４、競合検出部５、例外権限割当編集部６はそれぞれ別個のコンピュータシステムで構築されていてもよいし、一部または全部が同一のコンピュータシステムで実現されていてもよい。

競合検出部５は、具体的には、プログラムに従って動作する情報処理装置のＣＰＵ、ＲＡＭ等の記憶媒体を備える。また、競合検出部５は、ロール階層格納部１、サブジェクト割当格納部２、権限割当格納部３、例外権限割当格納部４、例外権限割当編集部６の各部と通信を行なうための通信インタフェースを備える。

例外権限割当編集部６は、具体的には、プログラムに従って動作する情報処理装置のＣＰＵ、ＲＡＭ等の記憶媒体を備える。また、例外権限割当編集部６は、例外権限割当格納部４、競合検出部５の各部と通信を行なうための通信インタフェースを備える。

ロール階層格納部１と、サブジェクト割当格納部２と、権限割当格納部３と、例外権限割当格納部４は、具体的には、プログラムに従って動作する情報処理装置のＣＰＵと、ＲＡＭやハードディスク等の記憶媒体によって実現される。

ロール階層格納部１は、ロール階層を記憶し、競合検出部５からの要求に従って、ロール間の関係を検索し、提供する。

サブジェクト割当格納部２は、サブジェクト割当を記憶し、競合検出部５からの要求に従って、サブジェクトとロールリストとの関係を検索し、提供する。

権限割当格納部３は、権限割当を記憶し、競合検出部５からの要求に従って、ロールと権限可否との関係を検索し、提供する。

例外権限割当格納部４は、例外権限割当を記憶し、競合検出部５からの要求に従って、例外ロールの識別子であるロールリストと権限可否との関係を検索し、提供する。また、例外権限割当編集部６から受け渡された例外権限割当を格納する。

競合検出部５は、ロール階層格納部１から、ロール階層を取得し、サブジェクト割当格納部２から、サブジェクト割当を取得し、権限割当格納部３から、権限割当を取得し、例外権限割当格納部４から、例外権限割当を取得し、ロール階層とサブジェクト割当と権限割当と例外権限割当に基づいて、同一のサブジェクトの持つロールに割り当てられた権限可否の中で、同じ権限について可否との組み合わせが異なる権限が存在するかどうかを検査し、そのような権限が存在した場合は、競合として、ロールリストと、競合する権限集合とを、例外権限割当編集部６に受け渡す。競合検出部５は、ロール階層格納部１や、サブジェクト割当格納部２や、権限割当格納部３や、例外権限割当格納部４の格納する内容の更新をトリガとして、自動的に処理を開始してもよいし、例外権限割当編集部６からの要求をトリガとして処理を開始してもよい。

例外権限割当編集部６は、競合検出部５から、競合が存在するロールリストと、競合している権限集合とを取得し、当該権限集合について、可否を編集するためのＵＩ（ユーザーインタフェース）をＷｅｂフォームなどの方法を用いて提供する。ＵＩで編集された結果を受け取ると、その内容から例外権限割当を作成して、例外権限割当格納部４に受け渡す。

（アクセス制御システム１００の動作の概要）

図２を参照してアクセス制御システム１００の動作の概略について説明する。アクセス制御システム１００では、まず、競合処理部５にて競合検出処理（ステップＡ１）を行う。次に、例外権限割当編集部６にて例外権限割当編集処理（ステップＡ２）を行う。

（例外権限割当がないときの競合検出処理）

図３を参照して競合処理部５にて行う競合検出処理について詳細に説明する。

（１）ステップＡ１０１

まず、競合検出部５は、ロール階層格納部１と、サブジェクト割当格納部２と、権限割当格納部３と、例外権限割当格納部４の少なくとも１つに、新規追加や変更などの更新が有るかを確認する。有ればステップＡ１０２に進み、無ければ終了する。

（２）ステップＡ１０２

次に、競合検出部５は、未処理のサブジェクト割当が有るかを確認する。有ればステップＡ１０３に進み、無ければステップＡ１１３に進む。

（３）ステップＡ１０３

次に、競合検出部５は、サブジェクト割当格納部２から、サブジェクト割当を１件取得する。例えば、サブジェクト割当は、図４に示すような情報を持ち、サブジェクト割当１件は図４のテーブルの１レコードに当たる。

（４）ステップＡ１０４

次に、競合検出部５は、取得したサブジェクト割当に記述されたサブジェクトが兼務状態に有るかを確認する。有ればステップＡ１０５に進み、無ければステップＡ１０２に進む。例えば、図４のテーブルのレコードのうち、ロールリストが（経理部、総務部）となっているレコードが兼務状態に有る。

（５）ステップＡ１０５

次に、競合検出部５は、例外権限割当格納部４を参照し、処理中のサブジェクト割当のロールリスト、即ち、ステップＡ１０４にて兼務状態に有ると判定した１件のサブジェクト割当のロールリストについて例外権限割当が有るかを確認する。有ればステップＡ１０６に進み、無ければステップＡ１０７に進む。ここでは一旦、対応する例外権限割当が無かったものとし、有った場合については後述する。

（６）ステップＡ１０６

次に、競合検出部５は、例外権限割当格納部４から、処理中のサブジェクト割当のロールリスト、即ち、ステップＡ４にて兼務状態に有ると判定し、かつ、ステップＡ５にて例外権限割当が有ると判定した１件のサブジェクト割当のロールリストに該当する例外権限割当を取得する。

（７）ステップＡ１０７

次に、競合検出部５は、ロール階層格納部１を参照し、兼務関係にあるサブジェクト割当のロールリストに含まれる各ロールの継承元となる先祖にあたるロールを取得する。

例えば、ロール階層は、図５に示すような情報を持ち、「総務部」ロールの継承元となる先祖にあたるロールは、「Ａ株式会社」ロールであり、「経理部」ロールの継承元となる先祖にあたるロールは「Ａ株式会社」ロールである。参考までに「広報課」ロールについて言及すると、「総務部」ロールだけではなく、「Ａ株式会社」ロールも「広報課」ロールの継承元となる先祖にあたるロールである。

（８）ステップＡ１０８

次に、競合検出部５は、権限割当格納部３を参照し、処理中のサブジェクト割当のロールリストに含まれる各ロールと、その継承元となる先祖のロールについて、ロール毎の権限割当を取得する。例えば、権限割当は、図６に示すような情報を持つ。図６のテーブルにおいて、権限――例えば（ｋａｉｓｈａｆｉｌｅ１、ｒｅａｄ）と、可否――例えばｐｅｒｍｉｔを組とした（ｋａｉｓｈａｆｉｌｅ１、ｒｅａｄ、ｐｅｒｍｉｔ）が権限可否である。なお、ここで「ｐｅｒｍｉｔ」は許可、「ｄｅｎｙ」は拒否の意である。

（９）ステップＡ１０９

次に、競合検出部５は、処理中のサブジェクト割当のロールリストに対応する権限可否を導出する前段階として、次のような処理を行う。即ち、処理中のロールリストに含まれるロールのそれぞれについて、換言すればサブジェクトが兼務するロールのそれぞれについて、先祖にあたるロールが存在するか否かを判定し、存在する場合は、先祖にあたるロールを継承元として処理して、継承後の権限可否を導出する。

このとき、ロールリストに該当する例外権限割当が有れば、例外ロールがロールリストのロール１つを継承した場合の権限可否を、ロールリストの各ロールの権限可否として導出する。例えば、仮に総務部ロールのみを継承した例外ロールの権限可否を総務部ロールの権限可否の導出結果として扱い、仮に経理部ロールのみを継承した例外ロールの権限可否を経理部ロールの導出結果として扱う。ただし、ここでは一旦、対応する例外権限割当が無かったものとし、有った場合については後述する。

例えば、ロールリストに含まれる各ロールに対応する継承処理後の権限可否は、図７に示すような情報となる。継承による修正の例としては、図６において、継承元である「Ａ株式会社」ロールの継承処理前の権限可否は（ｋａｉｓｈａｆｉｌｅ１，ｗｒｉｔｅ，ｄｅｎｙ）であり、継承先である「総務部」ロールの継承処理前の権限可否は（ｋａｉｓｈａｆｉｌｅ１，ｗｒｉｔｅ，ｐｅｒｍｉｔ）であるため、図７における、「総務部」ロールの継承処理後の権限可否は（ｋａｉｓｈａｆｉｌｅ１，ｗｒｉｔｅ，ｐｅｒｍｉｔ）となる。なお仮に、「総務部」ロールを継承元とする「秘書課」ロールや「広報課」ロールの権限可否を導出する場合、「総務部」ロールを継承するため、同様に（ｋａｉｓｈａｆｉｌｅ１，ｗｒｉｔｅ，ｐｅｒｍｉｔ）となる。

（１０）ステップＡ１１０

次に、競合検出部５は、ステップＡ１０９にて導出した各ロールの権限を比較し、異なるロールに対して、同一の権限に関する割当が有るか確認する。有ればステップＡ１１１に進み、無ければステップＡ１０２に進む。

例えば、図７における、「総務部」ロールと「経理部」ロールについて、権限（ｋａｉｓｈａｆｉｌｅ１，ｒｅａｄ）、（ｋａｉｓｈａｆｉｌｅ１，ｗｒｉｔｅ）、（ｋａｉｓｈａｆｉｌｅ２，ｒｅａｄ）、（ｋａｉｓｈａｆｉｌｅ２，ｗｒｉｔｅ）、（ｋａｉｋｅｉｆｉｌｅ１，ｒｅａｄ）、（ｋａｉｋｅｉｆｉｌｅ１，ｗｒｉｔｅ）、（ｍａｎｕａｌｆｉｌｅ１，ｒｅａｄ）、（ｍａｎｕａｌｆｉｌｅ１，ｗｒｉｔｅ）が、異なるロールに対する同一の権限に関する割当である。

なお、ロールリストに対応する例外権限割当が存在する場合、例外権限割当で定義された権限については、どのロールの権限割当においても同じ権限可否となるため、これらの権限についての比較処理は省略してもよい。少なくとも当該比較処理では、継承後の権限のうちロールリストに含まれる各ロールに由来する権限、つまり例外権限割当によって指定されていない権限について比較する。

（１１）ステップＡ１１１

次に、競合検出部５は、異なるロールに対する同一の権限に関する割当について、当該権限と組となる可否が互いに異なるかを比較する。異なる場合はステップＡ１１２に進み、同じである場合はステップＡ１０２に進む。

例えば、図７における、「総務部」ロールと「経理部」ロールについて、権限（ｋａｉｋｅｉｆｉｌｅ１，ｒｅａｄ）、（ｋａｉｋｅｉｆｉｌｅ１，ｗｒｉｔｅ）、（ｍａｎｕａｌ１，ｗｒｉｔｅ）が、異なるロールに対する同一の権限に関する割当について、当該権限と組となる可否が互いに異なる。

なお、ロールリストに対応する例外権限割当が存在する場合、例外権限割当で定義された権限については、どのロールの権限割当においても同じ権限可否となるため、これらの権限についての比較処理は省略してもよい。少なくとも当該比較処理では、継承後の権限のうちロールリストに含まれる各ロールに由来する権限、つまり例外権限割当によって指定されていない権限について比較する。

（１２）ステップＡ１１２

次に、競合検出部５は、当該権限を競合とし、処理中のロールリストとの組として記憶する。例えば、処理中のロールリスト（経理部，総務部）と、ステップＡ１１１の例で検出した権限（ｋａｉｋｅｉｆｉｌｅ１，ｒｅａｄ）、（ｋａｉｋｅｉｆｉｌｅ１，ｗｒｉｔｅ）、（ｍａｎｕａｌｆｉｌｅ１，ｗｒｉｔｅ）を組として記憶する。

（１３）ステップＡ１１３

次に、競合検出部５は、記憶された競合が有るかを確認する。有ればステップＡ１１４

に進み、無ければ終了する。

（１４）ステップＡ１１４

次に、競合検出部５は、競合として記憶されているロールリストと権限の組を、例外権限割当編集部６に対して出力する。例えば、競合として、図８に示すような情報を出力する。

（例外権限割当編集処理）

図９を参照して、例外権限割当編集処理における動作について詳細に説明する。

（１）ステップＡ２０１

まず、例外権限割当編集部６は、競合検出部５から、競合として、ロールリストと権限の集合の組を１つ以上入力される。例えば、競合として、図８に示すような情報を入力される。

（２）ステップＡ２０２

次に、例外権限割当編集部６は、競合が発生しているロールリスト毎に、競合している各権限に対する可否の入力を行うためのＵＩを生成し、入力方法をユーザに対して表示することによって提供する。例えば、例外権限割当編集部６は、図１０に示すようなＵＩを用いて、可否の入力フォームをユーザに提供する。

（３）ステップＡ２０３

次に、例外権限割当編集部６は、生成されたＵＩを利用してユーザが行った入力内容を取得する。例えば、例外権限割当編集部６は、図１０に示すようなＵＩへの入力内容として、権限（ｋａｉｋｅｉｆｉｌｅ１，ｒｅａｄ）と可否ｐｅｒｍｉｔの組と、権限（ｋａｉｋｅｉｆｉｌｅ１，ｗｒｉｔｅ）と可否ｄｅｎｙの組と、権限（ｍａｎｕａｌｆｉｌｅ１，ｗｒｉｔｅ）と可否ｐｅｒｍｉｔの組とを取得する。

（４）ステップＡ２０４

次に、例外権限割当編集部６は、ユーザが入力した可否を用いて、例外権限割当を生成し、例外権限割当格納部４に出力する。例えば、例外権限割当として、図１１に示すような情報を出力する。

（例外権限割当があるときの競合検出処理）

ステップＡ１０４にて兼務状態に有ると判定した１件のサブジェクト割当のロールリストに対し、ステップＡ１０５にて対応する例外権限割当が存在すると判定したときの動作について説明する。ここでは、ステップＡ２０１～Ａ２０４を実行して図１１のような例外権限割当を生成した後に、再度の更新や要求などで、ステップＡ１０１がもう一度実行された場合について述べる。

この場合、ロールリスト（経理部，総務部）を処理中のステップＡ１０５において、図１１に示すような例外権限割当が存在することとなり、対応する例外権限割当が有ることになり、次のステップＡ１０６で、ロールリスト（経理部，総務部）の例外権限割当を取得する。

次に、ステップＡ１０７、Ａ１０８では前記処理と同様の処理を行い、ステップＡ１０９で、ロールリストの各ロール「総務部」と「経理部」以外に、双方の継承先として、ロールリスト（経理部，総務部）の例外権限割当が存在するため、継承処理後の「総務部」ロール、「経理部」ロールに相当する権限可否は、図１２に示すような情報となる。

次に、ステップＡ１１０では、前記処理と同様の結果となるが、ステップＡ１１１において、異なるロールに対する同一の権限に関する割当について、当該権限と組となる可否が互いに異なるかを確認すると、すべての権限について可否が同一であることが分かる。あるいは、ステップＡ１１１において、例外権限割当で定義された権限について比較処理を省略した場合、すべての権限について可否が同一であることが分かる。あるいは、ステップＡ１１０において、例外権限割当で定義された権限について比較処理を省略した場合、組となる可否が異なる可能性を持った、異なるロールに対する同一の権限に関する割当は無くなり、ステップＡ１１１をスキップしてステップＡ１１２に進む。

結果として、ロールリスト（経理部，総務部）は競合しないため、ステップＡ１１３、Ａ１１４で出力される競合から除外される。

例えば、さらにこの後、「総務部」ロールと「経理部」ロールとの間で、例外権限割当で定義されていない、別の権限が競合するように権限割当を更新すると、ステップＡ１０９で、図１１に示すような例外権限割当を用いて処理した結果、更新された別の権限のみについて「総務部」ロールと「経理部」ロールとの間に競合が残るため、ステップＡ１１０で、新たに競合した権限のみが検出される。

これにより、本発明によるアクセス制御システムは、例外ロールの例外権限割当によって既存の競合を解消し、新たな競合だけを検出して、その競合に対する例外権限割当の編集部を提供する。

【実施例】

【０００８】

次に、図４のサブジェクト割当、図５のロール階層、図６の権限割当が格納する値を前提として、アクセス制御システム１００の動作について説明する。今、アクセス制御システム１００の各格納部には次のようなデータが格納されている。

ロール階層格納部１　ロール階層（図５）

サブジェクト割当格納部２　なし

権限割当格納部３　権限割当（図６）

例外権限割当格納部４　なし

ここで、アクセス制御システム１００のオペレータが、サブジェクト割当（図４）を入力し、サブジェクト割当格納部２に格納したとする。

競合検出部５は、サブジェクト割当の格納を更新として検出する（ステップＡ１０１）。サブジェクト割当はすべて未処理（ステップＡ１０２）なので、上から１レコードずつ取得して処理を行う（ステップＡ１０３）。

競合検出部５はサブジェクト割当格納部２に格納されたサブジェクト割当を１レコードずつ参照して、ロール兼務の有無を判定する。第１レコードはロール兼務がないので第２レコードに進む。第２レコードも同様である。第３レコードのロールリストには複数のロール、即ちロール総務部、ロール経理部が格納されており、ロール兼務が存在する（ステップＡ１０４）。

今のところ、例外権限割当格納部４には例外権限割当が格納されていない（ステップＡ１０５）ので、競合検出部５はステップＡ１０６をスキップする。

競合検出部５はロール階層格納部１を参照して、第３レコードのロール総務部の継承元であるロールＡ株式会社、ロール経理部の継承元であるロールＡ株式会社を取得する（ステップＡ１０７）。

競合検出部５は権限割当格納部３を参照して、ロール総務部、ロール経理部、ロールＡ株式会社それぞれの権限割当を取得する（ステップＡ１０８）。

競合検出部５は、ロール総務部の権限可否を、ロール総務部の権限割当と、その継承元であるロールＡ株式会社の権限割当から導出する。同様にして、ロール経理部の権限可否を、ロール経理部の権限割当と、その継承元であるロールＡ株式会社の権限割当から導出する（ステップＡ１０９）。継承先のロールと継承元のロールで同じ権限の可否が不一致のときは継承先のロールの権限可否を優先する。ロール総務部の権限可否の導出を例に挙げて説明する。

ロール総務部の権限割当に定められていないが、ロールＡ株式会社の権限割当には定められている権限可否は、継承元であるロールＡ株式会社の権限割当が適用される。図６の権限割当を参照すると、オブジェクトｋａｉｓｈａｆｉｌｅ２に対するアクションｒｅａｄ及びｗｒｉｔｅの可否は、ロールＡ株式会社には定められているが、ロール総務部には定められていない。このとき、図７の権限可否に示すように、ロール総務部の権限可否はロールＡ株式会社の権限割当を継承する。

逆に、ロール総務部の権限割当に定められているが、ロールＡ株式会社の権限割当には定められていない権限可否は、ロール総務部の権限可否がそのまま適用される。図６を参照すると、オブジェクトｓｏｕｍｕｆｉｌｅ１、ｋａｉｋｅｉｆｉｌｅ１、ｍａｎｕａｌ１それぞれに対するアクションｒｅａｄ及びｗｒｉｔｅの可否はロール総務部には定めら

れているが、ロールＡ株式会社には定められていない。このとき、図７に示すように、ロール総務部の権限可否はロール総務部の権限割当がそのまま適用される。

ロール総務部とロールＡ株式会社の両方に権限割当が定められている権限の可否については、継承先であるロール総務部の権限割当が適用される。図６を参照するとオブジェクトｋａｉｓｈａｆｉｌｅ１に対するアクションｒｅａｄ及びｗｒｉｔｅの可否が両ロールに定められており、特にアクションｗｒｉｔｅの可否が両ロールで異なるが、このときは図７に示すようにロール総務部の権限可否が適用される。

競合検出部５は、ステップＡ１０９にて求めた権限可否において、ロール総務部、ロール経理部が同一の権限について可否を定めたものを検出する（ステップＡ１１０）。ステップＡ１０９にて求めたロール総務部、ロール経理部の権限可否は図７のようになるが、これら権限可否のうち、オブジェクトｋａｉｓｈａｆｉｌｅ１、ｋａｉｓｈａｆｉｌｅ２、ｋａｉｋｅｉｆｉｌｅ１、ｍａｎｕａｌ１に対するアクションｒｅａｄ、ｗｒｉｔｅの権限可否は、どちらのロールに対しても割当がある。尚、該当する権限がない場合はステップＡ１０２に戻り、サブジェクト割当の次のレコードに処理対象を移す。

競合検出部５は、ステップＡ１１０にて求めた別ロール由来の同一権限の可否がロール間で不一致のものを検出する（ステップＡ１１１）。図７を参照すると、オブジェクトｋａｉｋｅｉｆｉｌｅ１アクションｒｅａｄ、ｗｒｉｔｅの権限可否と、オブジェクトｍａｎｕａｌ１に対するアクションｗｒｉｔｅの権限可否とが、ロール総務部とロール経理部とで異なる。尚、該当する権限可否がない場合はステップＡ１０２に戻り、サブジェクト割当の次のレコードに処理対象を移す。ステップＡ１０４～Ａ１１１により、複数のロールを兼務するサブジェクトが存在すること、当該複数ロールのひとつのロールＲ１と、当該複数ロールの他のロールＲ２との両方に対して定められた権限であって、その可否がロールＲ１とロールＲ２とで不一致であるような権限Ａが存在することがわかる。このとき、ロールＲ１及びＲ２からなる仮想的なロールを例外ロールと呼び、例外ロールに対する権限の割当を例外権限割当と呼ぶものとする。

競合検出部５は、ステップＡ１１１にて検出した、可否がロール間で不一致の権限を、ロール間で競合する権限と判定し、その権限とロールリストとを関連づけて記憶（ステップＡ１１２）し、ステップＡ１０２に戻る。つまり、ロールＲ１とロールＲ２からなるロールリスト（Ｒ１、Ｒ２）と、権限Ａとを関連づけるということであり、具体例を挙げれば、ロールリスト（経理部、総務部）と権限（ｋａｉｋｅｉｆｉｌｅ１，ｒｅａｄ）、権限（ｋａｉｋｅｉｆｉｌｅ１，ｗｒｉｔｅ）、権限（ｍａｎｕａｌ１，ｗｒｉｔｅ）とを関連づけて記憶する。

競合検出部５は、ステップＡ１０２～ステップＡ１１２の処理を、サブジェクト割当格納部２に格納したサブジェクト割当の残りのレコードに対して順次実行する。いずれかのレコードにて競合が検出された場合（ステップＡ１１３）、競合検出部５は、ステップＡ１１２にて記憶したロールリストと権限との関連づけを競合として例外権限割当編集部６に出力する（ステップＡ１１４）。

第３レコードの処理を終了した時点で、図４のサブジェクト割当には未処理のレコードとして第４レコード、第５レコードが残っているが、これらレコードはどちらもロール兼務が存在しないので、全レコードの処理を終了後に競合を検出しているのは第３レコードのみとなり、図８のような競合を出力することになる。

例外権限割当編集部６は、図８の競合を競合検出部５から受け取る（ステップＡ２０１）と、この競合を元にして図１０のような入力受付画面を生成し、不図示の画像表示装置（例えばＣＲＴ、液晶ディスプレイ装置）の画面に表示する（ステップＡ２０２）。この入力受付画面は、競合が発生しているロールリスト毎に表示されるものであり、競合が発生しているロールリスト、競合している権限のオブジェクト及びアクション、その権限の可否を示すチェックボックスからなる。図８の競合では競合が発生しているのはロール経理部、ロール総務部からなるロールリストのみなので、図１０のような入力受付画面を生成・表示するのみであるが、競合するロールリストが複数の場合はロールリスト毎に入力受付画面が生成・表示される。

画像表示装置を介して入力受付画面を見たオペレータは、不図示の入力装置（例えばキーボード、マウス）により、競合している権限の可否を新たに設定するための入力を行い、例外権限割当編集部６はこの入力を受け取る（ステップＡ２０３）。図１０の画面では、競合が発生しているロールリスト（経理部、総務部）のオブジェクトｋａｉｋｅｉｆｉｌｅ１に対するアクションｒｅａｄの可否を可（ｐｅｒｍｉｔ）と設定し、同オブジェクトに対するアクションｗｒｉｔｅの可否を不可（ｄｅｎｙ）と設定し、オブジェクトｍａｎｕａｌ１に対するアクションｗｒｉｔｅの可否を可と設定した状態となっている。

このようなオペレータの入力に基づいて、例外権限割当編集部６は例外権限割当を生成し、例外権限割当格納部４に格納する（ステップＡ２０４）。図１０の入力受付画面での入力内容をそのまま反映した例外権限割当が図１１である。

次に、例外権限割当格納部４に例外権限割当が格納されているときのアクセス制御システム１００の動作について説明する。今、アクセス制御システム１００の各格納部には次のようなデータが格納されているものとする。

ロール階層格納部１　ロール階層（図５）
サブジェクト割当格納部２　なし
権限割当格納部３　権限割当（図６）
例外権限割当格納部４　例外権限割当（図１１）

この状態から、アクセス制御システム１００のオペレータが、サブジェクト割当（図４）を入力し、サブジェクト割当格納部２に格納したとする。サブジェクト割当の第１、第２、第４、第５レコードを対象とする競合検出部５の動作は上記説明と同様である。

第３レコードを対象としたときの動作については、例外権限割当が格納されているので、ステップＡ１０５以後が上記説明と異なる。ステップＡ１０５にて、競合検出部５が例外権限割当格納部４を参照すると、第３レコードのロールリスト（経理部、総務部）に対応するロールリストが例外権限割当に存在する（ステップＡ１０５）ので、上記説明とは異なり、例外権限割当にて対応するロールリストの権限、その可否を取得する（ステップＡ１０６）。

競合検出部５はロール階層格納部１を参照して、サブジェクト割当　第３レコードのロール総務部の継承元であるロールＡ株式会社、ロール経理部の継承元であるロールＡ株式会社を取得する（ステップＡ１０７）。

競合検出部５は、ステップＡ１０７にて取得したロール総務部、ロール経理部、ロールＡ株式会社それぞれの権限割当を権限割当格納部３から取得する。更に、競合検出部５は、例外権限割当格納部４を参照して、例外ロール（経理部、総務部）の例外権限割当を取得する（ステップＡ１０８）。

ステップＡ１０８にて取得した権限割当及び例外権限割当に基づいて、競合検出部５は、継承処理後の各ロールの権限可否を導出する（ステップＡ１０９）。例示では、競合検出部５は、ロール経理部、ロール総務部、ロールＡ株式会社それぞれの権限割当、例外ロール（経理部、総務部）の例外権限割当に基づいて、ロール経理部、ロール総務部それぞれの権限可否を導出する。

図６の権限割当と、図１１の例外権限割当とに基づいて導出したロール総務部及びロール経理部の権限可否を図１２に示す。継承先のロールと継承元のロールで同じ権限の可否が不一致のときは継承先のロールの権限可否を優先する。ロール経理部は例外ロールの継承元のロールなので、同じ権限の可否が不一致のときは例外ロールの権限可否を優先する。ロール総務部でも同様である。その結果、例外権限割当がないときの権限可否である図７と比較すると、図１２では、ロール総務部の権限（ｋａｉｋｅｉｆｉｌｅ１，　ｒｅａｄ）の可否、ロール経理部の権限（ｋａｉｋｅｉｆｉｌｅ１，　ｗｒｉｔｅ）の可否、ロール経理部の権限（ｍａｎｕａｌ１，　ｗｒｉｔｅ）の可否が異なっている。

ステップＡ１１０において、競合検出部５は、ステップＡ１０９にて求めた権限可否のうち、ロール総務部、ロール経理部が同一の権限について可否を定めたものを検出する。ステップＡ１０９にて求めたロール総務部、ロール経理部の権限可否はここでは図１２のようになるが、可否の定めがある権限は図７と同じである。

ステップＡ１１１において、競合検出部５は、ステップＡ１１０にて検出した権限の中から、その可否がロール同士の間で不一致なものを検出する。例外権限割当を行う前は、図７のような権限割当であり、可否が不一致な権限が存在したが、こうした可否が不一致な権限にはステップＡ１０９にて既に例外ロールの権限可否を優先的に適用しているので、本ステップではすべての権限について可否が一致するので、サブジェクト割当の第３レコードを対象とする処理を終えて、第４レコードを対象とするステップＡ１０２に移行する。

結果として、図５のロール階層、図４のサブジェクト割当、図６の権限割当、図１１の例外権限割当を対応する各格納部に格納した状態では、競合検出部５はロールリスト（経理部，総務部）の競合を検出しないため、ステップＡ１１４において競合検出部５はロールリスト（経理部，総務部）を出力しない。

この後に続けて、「総務部」ロールと「経理部」ロールとの間で、図１１の例外権限割当では定義されていない、別の権限Ｂが競合するように権限割当を更新した場合を考える。この場合、ステップＡ１０９にて図１１な例外権限割当を用いて処理しても、権限Ｂのみについて「総務部」ロールと「経理部」ロールとの間に競合が残り、ステップＡ１１０で権限Ｂのみが検出される。

このように、アクセス制御システム１００は、同じサブジェクトに割り当てた複数のロール間で可否が異なる権限が存在するとき、まず、競合検出部５にてそのような権限を検出し、オペレータに対してそのような権限の可否を複数ロール間で統一する機会を与える。これに応じて、オペレータが例外権限割当編集部６を介しロール間で可否を統一すると、例外権限割当編集部６は例外権限割当を生成して例外権限割当格納部４に格納する。こうして例外権限割当が生成済みの権限については、競合検出部５は競合を検出せず、新たな競合だけを検出する。また、例外権限割当編集部６を介して、新たに競合を検出した権限の可否をロール間で統一する機会をオペレータに与える。

以上、本発明を実施の形態及び実施例に則して説明したが、本発明はこれに限定されるものではなく、発明の技術的範囲内で自由に変更ができることはいうまでもない。例えば、ロール階層格納部１、サブジェクト割当格納部２、権限割当格納部３、例外権限割当格納部４は同一の記憶装置であってもよいし、それぞれが別の記憶装置であってもよく、更に、それぞれが一乃至複数の記憶装置から構成されることとしてもよい。また、競合検出部５、例外権限割当編集部６は、それぞれの処理に係るプログラムを同じ処理装置にて実行することにより実現してもよいし、別の処理装置にて実行することにより実現してもよい。更に、アクセス制御システム１００は一のコンピュータにて実現してもよいし、連携する複数のコンピュータにより実現してもよい。これらは当業者には明らかであり、説明を要しないであろう。

（付記１）一乃至複数のロールと、そのロールを割り当てられたサブジェクトとを関連づけたサブジェクト割当、ロールと、権限と、そのロールを割り当てられたサブジェクトがその権限を実行することの可否とを関連づけた権限割当、及び、ロール間の継承関係を示すロール階層を記憶装置に格納する手順と、

前記サブジェクト割当の中で一のサブジェクトに対して複数のロールが割り当てられているか否かを判定し、割り当てられている場合、該当する複数のロールＲ１、Ｒ２、…、Ｒｍ（ｍは２以上の自然数）を取得する手順と、

前記ロール階層及び権限割当に基づいて、前記複数のロールＲ１、Ｒ２、…、Ｒｍの各ロールに対応する権限可否を継承により導出する第１の権限可否導出手順と、

前記継承により導出した権限可否のうち、前記複数のロールＲ１、Ｒ２、…、Ｒｍの中の別のロールに由来する権限であって、かつ、その可否が異なる権限Ａ１、Ａ２、…、Ａｎ（ｎは自然数）を、前記複数のロールＲ１、Ｒ２、…、Ｒｍの組の間で競合する権限として記憶装置に格納する手順と、

前記ロールＲ１、Ｒ２、…、Ｒｍの組を割り当てられた一のサブジェクトの前記権限Ａ１、Ａ２、…、Ａｎの可否を、入力装置を介して受け付ける手順と、

受け付けた可否に基づいて、前記ロールＲ１、Ｒ２、…、Ｒｍの組に関する前記権限Ａ

１、Ａ２、…、Ａｎの可否を、前記ロールＲ１、Ｒ２、…、Ｒｍの組からなる仮想的なロールである例外ロールに対する例外権限割当として記憶装置に記憶する手順と、
前記ロール階層、権限割当及び例外権限割当に基づいて、前記例外ロールの各ロールＲ１、Ｒ２、…、Ｒｍに対応する権限可否を継承により導出する第２の権限可否導出手順とをコンピュータに実行させるためのアクセス制御プログラム。
（付記２）前記第２の権限可否導出手順は、
前記ロール階層に基づいて、前記複数のロールＲ１、Ｒ２、…、Ｒｍそれぞれの継承元となるロールを取得する手順と、
前記権限割当に基づいて、前記複数のロールＲ１、Ｒ２、…、Ｒｍ及びこれらロールの継承元となるロールのそれぞれについて権限の可否を取得し、前記例外権限割当に基づいて、前記例外ロールの権限の可否を取得する手順と、
前記例外ロールを割り当てられたサブジェクトの権限可否を継承により導出する手順とを含むことを特徴とする、付記１に記載のアクセス制御プログラム。
（付記３）前記例外ロールを割り当てられたサブジェクトの権限可否を継承により導出する際、前記例外ロールを、前記複数のロールＲ１、Ｒ２、…、Ｒｍを継承元とする多重継承のロールとして扱うことを特徴とする、付記２に記載のアクセス制御プログラム。
（付記４）第１の権限可否導出手順は、
前記ロール階層に基づいて、前記複数のロールＲ１、Ｒ２、…、Ｒｍそれぞれの継承元となるロールを取得する手順と、
前記権限割当に基づいて、前記複数のロールＲ１、Ｒ２、…、Ｒｍ及びこれらロールの継承元となるロールのそれぞれについて権限の可否を取得する手順と、
前記複数のロールＲ１、Ｒ２、…、Ｒｍの各ロールに対応する権限可否を継承により導出する手順と
を含むことを特徴とする付記１に記載のアクセス制御プログラム。
（付記５）一乃至複数のロールと、そのロールを割り当てられたサブジェクトとを関連づけたサブジェクト割当と、ロールと、権限と、そのロールを割り当てられたサブジェクトがその権限を実行することの可否とを関連づけた権限割当と、ロール間の継承関係を示すロール階層とを格納する一乃至複数の記憶装置と、
前記サブジェクト割当の中で一のサブジェクトに対して複数のロールが割り当てられているか否かを判定し、割り当てられている場合、該当する複数のロールＲ１、Ｒ２、…、Ｒｍ（ｍは２以上の自然数）を取得する処理装置と、
前記ロール階層及び権限割当に基づいて、前記複数のロールＲ１、Ｒ２、…、Ｒｍの各ロールに対応する権限可否を継承により導出する第１の権限可否導出処理装置と、
前記継承により導出した権限可否のうち、前記複数のロールＲ１、Ｒ２、…、Ｒｍの中の別のロールに由来する権限であって、かつ、その可否が異なる権限Ａ１、Ａ２、…、Ａｎ（ｎは自然数）を、前記複数のロールＲ１、Ｒ２、…、Ｒｍの組の間で競合する権限として記憶装置に格納する処理装置と、
前記ロールＲ１、Ｒ２、…、Ｒｍの組を割り当てられた一のサブジェクトの前記権限Ａ１、Ａ２、…、Ａｎの可否を、入力装置を介して受け付ける処理装置と、
受け付けた可否に基づいて、前記ロールＲ１、Ｒ２、…、Ｒｍの組に関する前記権限Ａ１、Ａ２、…、Ａｎの可否を、前記ロールＲ１、Ｒ２、…、Ｒｍの組からなる仮想的なロールである例外ロールに対する例外権限割当として記憶装置に記憶する処理装置と、
前記ロール階層、権限割当及び例外権限割当に基づいて、前記例外ロールの各ロールＲ１、Ｒ２、…、Ｒｍに対応する権限可否を継承により導出する第２の権限可否導出処理装置と
を備えることを特徴とするアクセス制御システム。
（付記６）前記第２の権限可否導出処理装置は、
前記ロール階層に基づいて、前記複数のロールＲ１、Ｒ２、…、Ｒｍそれぞれの継承元となるロールを取得し、
前記権限割当に基づいて、前記複数のロールＲ１、Ｒ２、…、Ｒｍ及びこれらロールの

継承元となるロールのそれぞれについて権限の可否を取得し、前記例外権限割当に基づいて、前記例外ロールの権限の可否を取得し、
前記例外ロールを割り当てられたサブジェクトの権限可否を継承により導出する
ことを特徴とする付記５に記載のアクセス制御システム。
（付記７）前記例外ロールを割り当てられたサブジェクトの権限可否を継承により導出する際、前記例外ロールを、前記複数のロールＲ１、Ｒ２、…、Ｒｍを継承元とする多重継承のロールとして扱うことを特徴とする、付記６に記載のアクセス制御システム。
（付記８）第１の権限可否導出処理装置は、
前記ロール階層に基づいて、前記複数のロールＲ１、Ｒ２、…、Ｒｍそれぞれの継承元となるロールを取得し、
前記権限割当に基づいて、前記複数のロールＲ１、Ｒ２、…、Ｒｍ及びこれらロールの継承元となるロールのそれぞれについて権限の可否を取得し、
前記複数のロールＲ１、Ｒ２、…、Ｒｍの各ロールに対応する権限可否を継承により導出する
ことを特徴とする付記５に記載のアクセス制御システム。
（付記９）一乃至複数のロールと、そのロールを割り当てられたサブジェクトとを関連づけたサブジェクト割当、ロールと、権限と、そのロールを割り当てられたサブジェクトがその権限を実行することの可否とを関連づけた権限割当、及び、ロール間の継承関係を示すロール階層を記憶装置に格納する手順をコンピュータにて実行する段階と、
前記サブジェクト割当の中で一のサブジェクトに対して複数のロールが割り当てられているか否かを判定し、割り当てられている場合、該当する複数のロールＲ１、Ｒ２、…、Ｒｍ（ｍは２以上の自然数）を取得する手順をコンピュータにて実行する段階と、
前記ロール階層及び権限割当に基づいて、前記複数のロールＲ１、Ｒ２、…、Ｒｍの各ロールに対応する権限可否を継承により導出する手順をコンピュータにて実行する第１の権限可否導出段階と、
前記継承により導出した権限可否のうち、前記複数のロールＲ１、Ｒ２、…、Ｒｍの中の別のロールに由来する権限であって、かつ、その可否が異なる権限Ａ１、Ａ２、…、Ａｎ（ｎは自然数）を、前記複数のロールＲ１、Ｒ２、…、Ｒｍの組の間で競合する権限として記憶装置に格納する手順をコンピュータにて実行する段階と、
前記ロールＲ１、Ｒ２、…、Ｒｍの組を割り当てられた一のサブジェクトの前記権限Ａ１、Ａ２、…、Ａｎの可否を、入力装置を介して受け付ける手順をコンピュータにて実行する段階と、
受け付けた可否に基づいて、前記ロールＲ１、Ｒ２、…、Ｒｍの組に関する前記権限Ａ１、Ａ２、…、Ａｎの可否を、前記ロールＲ１、Ｒ２、…、Ｒｍの組からなる仮想的なロールである例外ロールに対する例外権限割当として記憶装置に記憶する手順をコンピュータにて実行する段階と、
前記ロール階層、権限割当及び例外権限割当に基づいて、前記例外ロールの各ロールＲ１、Ｒ２、…、Ｒｍに対応する権限可否を継承により導出する手順をコンピュータにて実行する第２の権限可否導出段階と
を含むことを特徴とするアクセス制御方法。
（付記１０）第２の権限可否導出段階は、
前記ロール階層に基づいて、前記複数のロールＲ１、Ｒ２、…、Ｒｍそれぞれの継承元となるロールを取得する手順をコンピュータにて実行する段階と、
前記権限割当に基づいて、前記複数のロールＲ１、Ｒ２、…、Ｒｍ及びこれらロールの継承元となるロールのそれぞれについて権限の可否を取得し、前記例外権限割当に基づいて、前記例外ロールの権限の可否を取得する手順をコンピュータにて実行する段階と、
前記例外ロールを割り当てられたサブジェクトの権限可否を継承により導出する手順をコンピュータにて実行する段階と
を含むことを特徴とする、付記９に記載のアクセス制御方法。
（付記１１）例外ロールを割り当てられたサブジェクトの権限可否を継承により導出す

る際、例外ロールを、複数のロールＲ１、Ｒ２、…、Ｒｍを継承元とする多重継承のロールとして扱うことを特徴とする、付記１０に記載のアクセス制御方法。

（付記１２）第１の権限可否導出段階は、ロール階層に基づいて、複数のロールＲ１、Ｒ２、…、Ｒｍそれぞれの継承元となるロールを取得する段階と、権限割当に基づいて、複数のロールＲ１、Ｒ２、…、Ｒｍ及びこれらロールの継承元となるロールのそれぞれについて権限の可否を取得する段階と、複数のロールＲ１、Ｒ２、…、Ｒｍの各ロールに対応する権限可否を継承により導出する手順をコンピュータにて実行する段階とを含むことを特徴とする付記９に記載のアクセス制御方法。

この出願は、２０１０年３月３１日に出願された日本出願特願第２０１０－０８０１８７号を基礎とする優先権を主張し、その開示のすべてをここに取り込むものである。

【図１】

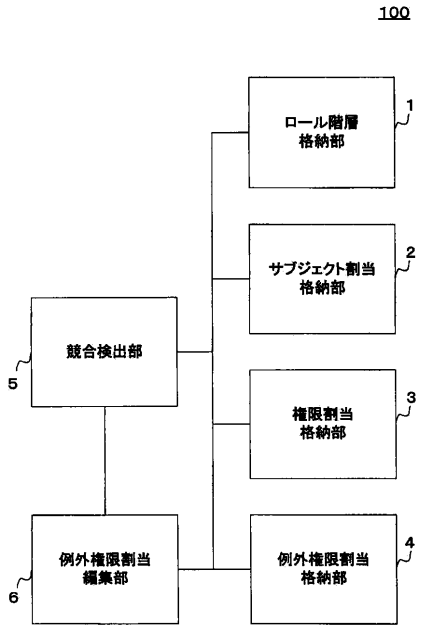

図１

【図２】

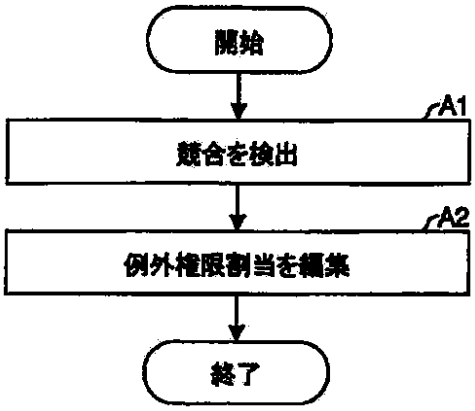

図２

【図３】

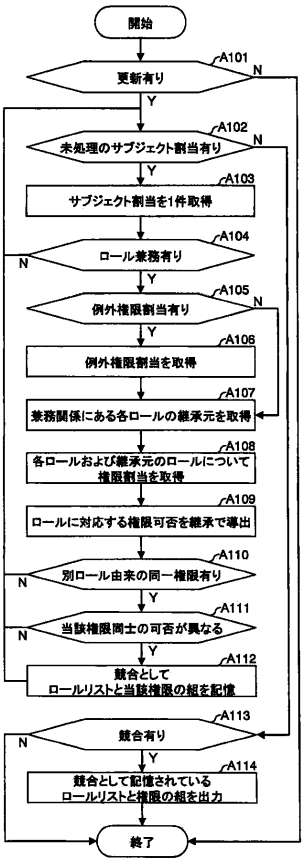

図３

【図４】

ロールリスト	サブジェクト
総務部	k-satou m-suzuki
経理部	t-takahashi t-tanaka
経理部，総務部	h-watanabe n-itou
秘書課	m-yamamoto
広報課	h-nakamura

図４

【図５】

ロール	直接の継承元のロール
A株式会社	
総務部	A株式会社
経理部	A株式会社
秘書課	総務部
広報課	総務部

図５

【図６】

ロール	権限	可否
A株式会社	kaishafile1, read	permit
	kaishafile1, write	deny
	kaishafile2, read	permit
	kaishafile2, write	deny
総務部	kaishafile1, write	permit
	soumufile1, read	permit
	soumufile1, write	permit
	kaikeifile1, read	deny
	kaikeifile1, write	deny
	manual1, read	permit
	manual1, write	permit
経理部	kaishafile1, write	permit
	keirifile1, read	permit
	keirifile1, write	permit
	kaikeifile1, read	permit
	kaikeifile1, write	permit
	manual1, read	permit
	manual1, write	deny
秘書課	hishofile1, read	permit
	hishofile1, write	permit
広報課	kaishafile2, write	permit
	kouhoufile1, read	permit
	kouhoufile1, write	permit

図６

【図７】

ロール	権限	可否
総務部	kaishafile1, read	permit
	kaishafile1, write	permit
	kaishafile2, read	permit
	kaishafile2, write	deny
	soumufile1, read	permit
	soumufile1, write	permit
	kaikeifile1, read	deny
	kaikeifile1, write	deny
	manual1, read	permit
	manual1, write	permit
経理部	kaishafile1, read	permit
	kaishafile1, write	permit
	kaishafile2, read	permit
	kaishafile2, write	deny
	keirifile1, read	permit
	keirifile1, write	permit
	kaikeifile1, read	permit
	kaikeifile1, write	permit
	manual1, read	permit
	manual1, write	deny

図７

【図８】

ロールリスト	権限
経理部，総務部	kaikeifile1，read
	kaikeifile1，write
	manual1，write

図 8

【図９】

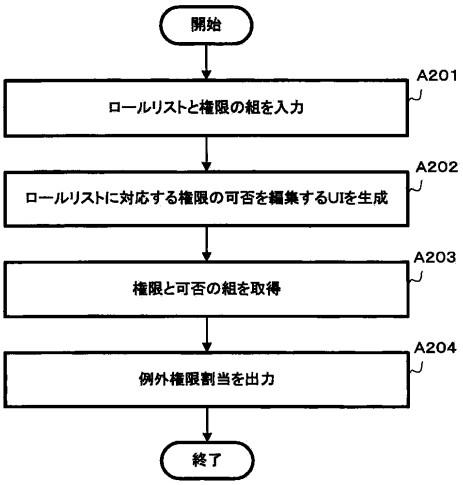

図 9

【図１０】

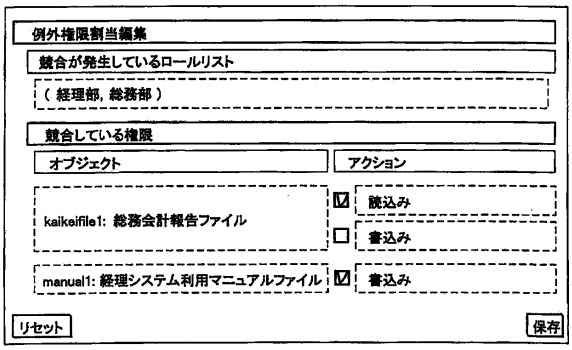

図 10

【図１１】

ロールリスト	権限	可否
経理部，総務部	kaikeifile1，read	permit
	kaikeifile1，write	deny
	manual1，write	permit

図 11

【図１２】

ロール	権限	可否
総務部	kaishafile1，read	permit
	kaishafile1，write	permit
	kaishafile2，read	permit
	kaishafile2，write	deny
	soumufile1，read	permit
	soumufile1，write	permit
	kaikeifile1，read	permit
	kaikeifile1，write	deny
	manual1，read	permit
	manual1，write	permit
経理部	kaishafile1，read	permit
	kaishafile1，write	permit
	kaishafile2，read	permit
	kaishafile2，write	deny
	keirifile1，read	permit
	keirifile1，write	permit
	kaikeifile1，read	permit
	kaikeifile1，write	deny
	manual1，read	permit
	manual1，write	permit

図 12

フロントページの続き

(56)参考文献 特開２００７－４５４９（ＪＰ，Ａ）
特開２０００－２３１５０９（ＪＰ，Ａ）
特開２００９－１１００９９（ＪＰ，Ａ）
特開２００７－２５７５２９（ＪＰ，Ａ）
森田 陽一郎，中江 政行，小川 隆一，“セキュア・プラットフォームの研究開発（２） アクセス制御ポリシー生成・配布”，ＦＩＴ２００９ 第８回情報科学技術フォーラム 講演論文集，日本，社団法人情報処理学会、社団法人電子情報通信学会，２００９年 8月２０日，第４分冊、Ｌ－０２５，ｐ．１８７－１８８
森田 陽一郎，中江 政行，小川 隆一，“ＩＴ全般統制のための職務分掌検証方式”，ＦＩＴ２００７ 第６回情報科学技術フォーラム 一般講演論文集，日本，社団法人情報処理学会、社団法人電子情報通信学会，２００７年 8月２２日，第４分冊、Ｌ－０２４，ｐ．５７－５８
朝倉 義晴，中本 幸一，“分散システムにおけるロールベースアクセス制御の更新問題”，情報処理学会論文誌 ［ＣＤ－ＲＯＭ］，日本，社団法人情報処理学会，２０１０年 3月１５日，Ｖｏｌ．５１、Ｎｏ．３，ｐ．７２８－７３９

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ ２１／６２