(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2006-146559
(P2006-146559A)
(43)公開日　平成18年6月8日(2006.6.8)

(51)Int.Cl.		F I			テーマコード（参考）
G06Q 10/00	(2006.01)	G06F	17/60	174	5B085
G06F 21/20	(2006.01)	G06F	15/00	330B	

審査請求 未請求　請求項の数 19　ＯＬ　（全 26 頁）

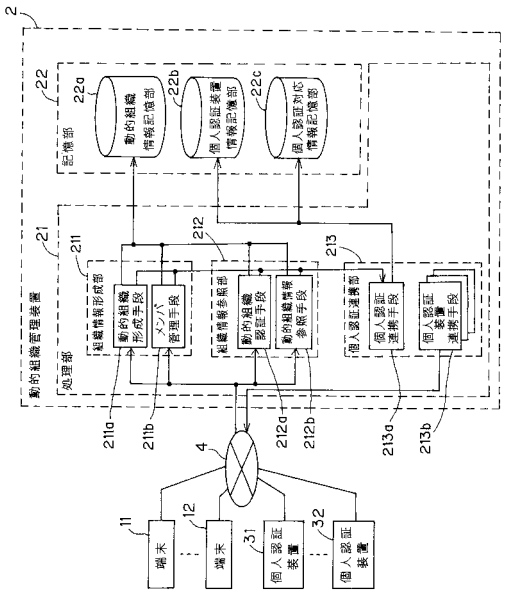
(21)出願番号　特願2004-335805 (P2004-335805)
(22)出願日　平成16年11月19日 (2004.11.19)

(71)出願人　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　100103090
弁理士　岩壁　冬樹
(74)代理人　100124501
弁理士　塩川　誠人
(72)発明者　坂口　基彦
東京都港区芝五丁目７番１号　日本電気株式会社内
(72)発明者　坂上　秀和
東京都港区芝五丁目７番１号　日本電気株式会社内

最終頁に続く

(54)【発明の名称】動的組織管理システム、動的組織管理方法、動的組織管理装置および動的組織管理プログラム

(57)【要約】
【課題】　管理者の手間を増加させることなく柔軟な組織構造を管理する。
【解決手段】　個人認証対応情報記憶部２２ｃは、静的組織におけるメンバを個人認証する個人認証装置を示す情報を記憶する。個人認証装置情報記憶部２２ｂは、個人認証装置を示す情報に対応させて、個人認証装置が用いる認証方式を記憶する。個人認証連携部２１３は、それぞれが特定の個人認証方式にもとづく認証要求を出力する１つ以上の個人認証装置連携手段２１３ｂと、要求に応じて、個人認証対応情報記憶部２２ｃに記憶されている個人認証装置を示す情報にもとづいて個人認証装置を特定し、特定した個人認証装置に対応する認証方式を個人認証装置情報記憶部２２ｂから抽出する個人認証連携手段２１３ａとを含み、個人認証連携手段２１３ａによって抽出された個人認証装置連携手段２１３ｂが、通信回線４を介して、個人認証装置にメンバの個人認証を依頼する。
【選択図】　図１



【特許請求の範囲】
【請求項１】
木構造で管理されている静的組織の１つ以上のメンバで構成される動的組織の管理を行う動的組織管理装置であって、
動的組織の所属メンバの信頼性を、メンバが属する静的組織におけるメンバを個人認証する個人認証装置と連携して判断する個人認証連携部を備えた
こと特徴とする動的組織管理装置。
【請求項２】
静的組織におけるメンバを個人認証する個人認証装置を示す情報を記憶する個人認証対応情報記憶部を備え、
個人認証連携部は、前記個人認証対応情報記憶部に記憶されている個人認証装置を示す情報にもとづいて個人認証装置を特定し、特定した個人認証装置にメンバの個人認証を依頼する
請求項１記載の動的組織管理装置。
【請求項３】
動的組織に関する処理を実行する動的組織処理実行部と、
個人認証装置を示す情報に対応させて、個人認証装置が用いる認証方式を記憶する個人認証装置情報記憶部とを備え、
個人認証連携部は、
それぞれが特定の個人認証方式にもとづく認証要求を出力する１つ以上の個人認証装置連携手段と、
前記動的組織処理実行部からの要求に応じて、個人認証対応情報記憶部に記憶されている個人認証装置を示す情報にもとづいて個人認証装置を特定し、特定した個人認証装置に対応する認証方式を前記個人認証装置情報記憶部から抽出する個人認証連携手段とを含み、
前記個人認証連携手段によって抽出された前記個人認証装置連携手段が、個人認証装置にメンバの個人認証を依頼する
請求項２記載の動的組織管理装置。
【請求項４】
動的組織処理実行部は、処理の要求に応じて個人認証連携部に要求者の認証を依頼し、要求者が動的組織のメンバであることを前記個人認証連携部が確認したら、処理を実行する
請求項３記載の動的組織管理装置。
【請求項５】
動的組織処理実行部は、動的組織の作成または削除の処理を実行する組織情報形成部を含む
請求項４記載の動的組織管理装置。
【請求項６】
動的組織処理実行部は、動的組織へのメンバの追加または動的組織からのメンバの削除の処理を実行するメンバ管理手段を含む
請求項４または請求項５記載の動的組織管理装置。
【請求項７】
動的組織処理実行部は、動的組織にメンバが所属していることを認証する動的組織認証手段を含む
請求項４から請求項６のうちのいずれか１項に記載の動的組織管理装置。
【請求項８】
動的組織処理実行部は、動的組織に関する情報を参照する処理を実行する動的組織情報参照手段を含む
請求項４から請求項７のうちのいずれか１項に記載の動的組織管理装置。
【請求項９】

動的組織処理実行部は、要求者が動的組織に所属しているか否かによって、要求者の処理実行権限を決定する
請求項４から請求項８のうちのいずれか１項に記載の動的組織管理装置。
【請求項１０】
動的組織の所属メンバの権限を、メンバが属する静的組織に応じて管理する権限管理部を備えた
請求項１から請求項９のうちのいずれか１項に記載の動的組織管理装置。
【請求項１１】
動的組織の所属メンバの権限を、メンバが属する静的組織に応じて管理する権限管理部と、それぞれの静的組織に付与される権限を記憶する権限情報記憶部とを備え、
前記権限管理部は、動的組織処理実行部の要求に応じて、個人認証対応情報記憶部の記憶内容にもとづいてメンバが属する静的組織を特定し、特定した静的組織に付与される権限を前記権限情報記憶部から抽出し、抽出した権限を前記動的組織処理実行部に返す
請求項４から請求項９のうちのいずれか１項に記載の動的組織管理装置。
【請求項１２】
木構造で管理されている静的組織の１つ以上のメンバで構成される動的組織の管理を行う動的組織管理システムであって、
動的組織に関する処理の要求を行う端末と、
前記端末から要求を受けたときに、前記端末を操作した動的組織の所属メンバの信頼性を、メンバが属する静的組織におけるメンバを個人認証する個人認証装置と連携して判断する個人認証連携部を含む動的組織管理装置とを備えた
こと特徴とする動的組織管理システム。
【請求項１３】
動的組織管理装置は、端末から処理の要求を受けると、個人認証連携部に要求者の認証を依頼し、要求者が動的組織のメンバであることを前記個人認証連携部が確認したら、処理を実行する動的組織処理実行部を含む
請求項１２記載の動的組織管理システム。
【請求項１４】
動的組織処理実行部は、動的組織の作成または削除の処理を実行する組織情報形成部、動的組織へのメンバの追加または動的組織からのメンバの削除の処理を実行するメンバ管理手段、動的組織にメンバが所属していることを認証する動的組織認証手段、および動的組織に関する情報を参照する処理を実行する動的組織情報参照手段を含む
請求項１３記載の動的組織管理システム。
【請求項１５】
動的組織管理装置は、動的組織の所属メンバの権限を、メンバが属する静的組織に応じて管理する権限管理部を含む
請求項１２から請求項１４のうちのいずれか１項に記載の動的組織管理システム。
【請求項１６】
木構造で管理されている静的組織の１つ以上のメンバで構成される動的組織の管理を行う動的組織管理方法であって、
動的組織の所属メンバの信頼性を、メンバが属する静的組織におけるメンバを個人認証する個人認証装置と連携して判断する
こと特徴とする動的組織管理方法。
【請求項１７】
動的組織の所属メンバの権限を、メンバが属する静的組織に応じて管理する
請求項１６記載の動的組織管理方法。
【請求項１８】
木構造で管理されている静的組織の１つ以上のメンバで構成される動的組織の管理を行う動的組織管理装置で実行されるプログラムあって、
前記動的組織管理装置におけるコンピュータに、

静的組織におけるメンバを個人認証する個人認証装置を示す情報を記憶する個人認証対応情報記憶部に記憶されている情報にもとづいて個人認証装置を特定する処理と、
個人認証装置を示す情報に対応させて個人認証装置が用いる認証方式を記憶する個人認証装置情報記憶部に記憶されている情報にもとづいて個人認証装置が用いる認証方式を特定する処理と、
通信回線を介して、特定された前記個人認証装置に、特定された前記認証方式に従ったメンバの個人認証の要求を送信する処理と
を実行させるための動的組織管理プログラム。
【請求項１９】
木構造で管理されている静的組織の１つ以上のメンバで構成される動的組織の管理を行う動的組織管理装置で実行されるプログラムあって、
前記動的組織管理装置におけるコンピュータに、
静的組織におけるメンバを個人認証する個人認証装置を示す情報を記憶する個人認証対応情報記憶部に記憶されている情報にもとづいて個人認証装置を特定する処理と、
個人認証装置を示す情報に対応させて個人認証装置が用いる認証方式を記憶する個人認証装置情報記憶部に記憶されている情報にもとづいて個人認証装置が用いる認証方式を特定する処理と、
通信回線を介して、特定された前記個人認証装置に、特定された前記認証方式に従ったメンバの個人認証の要求を送信する処理と、
前記個人認証対応情報記憶部の記憶内容にもとづいてメンバが属する静的組織を特定する処理と、
静的組織に付与される権限を記憶する権限情報記憶部から、特定された前記静的組織に付与される権限を抽出する処理とを
を実行させるための動的組織管理プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、構成メンバが頻繁に変更されるような組織である動的組織を管理するための動的組織管理システム、動的組織管理方法および動的組織管理プログラムに関し、特に、メンバの信頼性を確保することが必要な動的組織を管理するための動的組織管理システム、動的組織管理方法、動的組織管理装置および動的組織管理プログラムに関する。
【背景技術】
【０００２】
企業において、部や課などの組織および組織を構成する社員（メンバ）は、図１８に示すような木構造で管理されている。木構造の組織を管理する技術として、非特許文献１に示されるＬＤＡＰ（Ｌｉｇｈｔｗｅｉｇｈｔ Ｄｉｒｅｃｔｏｒｙ Ａｃｃｅｓｓ Ｐｒｏｔｏｃｏｌ）を採用したシステムが用いられている。ＬＤＡＰでは、部、課、社員などを１つのノードとして扱い、１つのノード下に複数のノードが配置される。一方、１つのノードに対して、親（上）ノードは１つしか存在しないというルール、つまり木構造で組織構造が管理される。
【０００３】
一方、コミュニティと呼ばれる共通の趣味などを持つメンバの集合が存在する。コミュニティを管理する技術の一例が、特許文献１に記載されている。特許文献１に記載されたシステムでは、コミュニティ（具体的にはメーリングリスト）に所属するメンバ（具体的にはメールアドレス）の情報が管理される。そして、そのコミュニティは、木構造ではない。部や課といった組織の場合には、管理者が組織構造を管理するのに対して、コミュニティでは、メンバが主体的に組織構造を管理する。そのため、特許文献１に記載されたシステムでは、メンバが主体的に組織構造を管理するための機能を有している。また、図１９に示すように、メンバは、同時に複数のコミュニティ（組織）に属すことがある。
【０００４】

また、コミュニティにおいてメンバの信頼性を保証することが要求される場合があるが、信頼性を保証する技術に関しては、公開鍵基盤（ＰＫＩ：Ｐｕｂｌｉｃ Ｋｅｙ Ｉｎｆｒａｓｔｕｃｔｕｒｅ）を利用して身分証明書発行し、個人を認証する技術が知られている。ＰＫＩでは、公開鍵と、その持ち主を証明する認証局を設けることで個人認証を可能にする。

【０００５】

また、複数のコミュニティ間で、個人の信頼性を共有する技術として、非特許文献２に示されるような個人認証の相互利用技術がある。非特許文献２に示される個人認証技術では、個人を管理するシステム間で、トラストサークルという信頼関係の輪を構築する。トラストサークル内のあるシステムで個人が認証されていれば、他のシステムでも、その個人を信頼するという仕組みになっている。

【０００６】

【特許文献１】特開２００１－１６８９０１号公報

【非特許文献１】M. Wahl他, Lightweight Directory Access Protocol (v3) [online], Internet Engineering Task Force(IETF), http://www.ietf.org/rfc/rfc2251.txt?number=2251

【非特許文献２】Thomas Wason他, Liberty ID-FF Architecture Overview, Version 1.2 [online], LIBERTY ALLIANCE PROJECT, http://www.projectliberty.org/

【発明の開示】

【発明が解決しようとする課題】

【０００７】

企業などの組織においては、部や課などの木構造で管理される組織の管理に重点がおかれているので、部や課にまたがったメンバで構成されるような柔軟性を持つ組織を管理することは困難である。すなわち、近年、企業において重要とされている部門を横断したプロジェクトなどの組織管理を行うことが難しい。

【０００８】

企業では、部や課などのように木構造で管理され頻繁に構成が変化することがない組織（以下、静的組織と称する）をＬＤＡＰサーバなどで管理している。しかし、それぞれのメンバが異なる静的組織に属するメンバで構成される部門横断プロジェクトなどの組織では、上記のコミュニティのように、メンバが複数のプロジェクトに参加することもある。そのために、ＬＤＡＰで表現される木構造の管理だけでは、部門横断プロジェクトなどの組織を管理しきれない。

【０００９】

例えば、ファイルなどの組織がもつ情報の公開管理を考えると、部や課などの静的組織単位でファイル公開の範囲を制限することは容易である。従来のＬＤＡＰを用いた組織管理システムと連携すれば、Ａ部に所属する社員にのみファイルを公開するといった制御ができる。一方、プロジェクト単位で公開範囲を制限する場合は、社員がプロジェクトＡ（組織Ａ）とプロジェクトＢ（組織との両方に所属することもあり、木構造の管理だけでは対応できない。

【００１０】

さらに、ＬＤＡＰを用いた組織管理システムでは、管理者が組織の作成やメンバの追加などを集中的に管理することが普通である。従って、メンバが頻繁に追加・削除されるプロジェクトなどの柔軟な組織を管理する場合、管理者の手間が増大することも問題である。以降、静的組織をまたがったメンバで構成され、かつ、動的にメンバが追加・削除される組織を動的組織という。

【００１１】

また、静的組織に比べて、動的組織では構成メンバが広範囲にわたり、加えて、メンバの追加、削除が頻繁に発生するので、情報漏洩などの脅威に対して安全性を確保することが困難になる。従って、安全性を確保するためには動的組織の所属メンバの信頼性を保証することが重要になる。

【００１２】
特許文献１に記載されているような柔軟性を重視するコミュニティ管理技術では、メンバは複数のコミュニティに所属することができ、かつ、管理者の手間を増大させずにコミュニティを管理することができる。しかし、従来のコミュニティ管理技術は、範囲を限定せず多様なメンバでコミュニティを構成することを重視し、組織を構成するメンバの信頼性を考慮していない。信頼性を考慮する場合でも、メンバを限定しないという特性上、ＰＫＩによる公的認証局を利用してメンバの個人認証を行うことが普通である。このようなコミュニティのメンバ認証方法を企業に適用することを考えると、企業では静的組織に関して社員認証をすでに管理しているので、公的認証局を利用した認証を行なうことは二重の管理になり、かつ、公開鍵の登録や証明書発行などの手間がかかり効率的でない。

【００１３】
また、一般に、メンバの信頼性を保証する方法は、それぞれの静的組織で異なっている。例えば、社員の信頼性を保証する方法は、それぞれの企業で異なっている。そのために、複数の企業間にまたがるプロジェクトなどの動的組織に、静的組織におけるメンバの信頼性を保証する方法を適用することは難しい。非特許文献２に記載された個人認証技術では、異なる組織間で個人認証を相互利用することはできるが、認証方式を統一することが前提になっている。また、複数の静的組織で管理される個人認証を結合する技術としてＰＫＩのブリッジ機能が存在するが、あくまで静的組織の統合が目的で、動的組織の認証への適用は考慮されていない。

【００１４】
また、従来のコミュニティ管理などの動的組織管理技術では、動的組織の管理とメンバが所属する静的組織との関連付けを行なう仕組みが存在しない。すなわち、静的組織をまたがって動的組織を構成する場合に、メンバが所属する静的組織との関連が考慮されていない。従って、静的組織を考慮した動的組織の権限管理を行うことも難しい。例えば、企業Ａと企業Ｂとでプロジェクトαを構成し、企業Ａの社員だけがプロジェクトαにメンバ追加をできるといった、静的組織を考慮した動的組織の権限管理ができない。

【００１５】
そこで、本発明は、企業などが静的組織の管理に利用している社員の信頼性保証の機構と連携して、所属するメンバの信頼性を保証し、かつ、管理者の手間を増加させることなく柔軟な組織構造を管理できる動的組織管理システムを提供することを目的とする。

【００１６】
本発明の他の目的は、メンバの信頼性を保証する方法が異なる静的組織間で、柔軟な組織構成を管理する動的組織管理システムを提供することである。

【００１７】
本発明のさらに他の目的は、メンバが所属する静的組織との関連を考慮した、動的組織における権限管理を行なうことができる動的組織管理システムを提供することである。

【課題を解決するための手段】

【００１８】
本発明による動的組織管理装置は、木構造で管理されている静的組織の１つ以上のメンバで構成される動的組織の管理を行う動的組織管理装置であって、動的組織の所属メンバの信頼性を、メンバが属する静的組織におけるメンバを個人認証する個人認証装置と連携して判断する個人認証連携部を備えたこと特徴とする。

【００１９】
このような構成を採用することによって、メンバ自身による動的組織の管理と、静的組織の個人認証との連携による動的組織所属メンバの信頼性保証とを実現でき、本発明の目的を達成することができる。

【００２０】
動的組織管理装置は、静的組織におけるメンバを個人認証する個人認証装置を示す情報を記憶する個人認証対応情報記憶部を備え、個人認証連携部が、個人認証対応情報記憶部に記憶されている個人認証装置を示す情報にもとづいて個人認証装置を特定し、特定した

個人認証装置にメンバの個人認証を依頼するように構成されていてもよい。

【００２１】

動的組織管理装置は、動的組織に関する処理を実行する動的組織処理実行部（例えば、動的組織形成手段２１１ａ、メンバ管理手段２１１ｂ、動的組織認証手段２１２ａ、動的組織情報参照手段２１２ｂ）と、個人認証装置を示す情報に対応させて、個人認証装置が用いる認証方式を記憶する個人認証装置情報記憶部とを備え、個人認証連携部が、それぞれが特定の個人認証方式にもとづく認証要求を出力する１つ以上の個人認証装置連携手段と、動的組織処理実行部からの要求に応じて、個人認証対応情報記憶部に記憶されている個人認証装置を示す情報にもとづいて個人認証装置を特定し、特定した個人認証装置に対応する認証方式を個人認証装置情報記憶部から抽出する個人認証連携手段とを含み、個人認証連携手段によって抽出された個人認証装置連携手段が、個人認証装置にメンバの個人認証を依頼するように構成されていてもよい。

【００２２】

個人認証連携手段が認証方式に適する個人認証装置連携手段を選択することによって、認証方式が異なる複数の静的組織間でも動的組織を構築することができる。

【００２３】

動的組織処理実行部は、処理の要求に応じて個人認証連携部に要求者の認証を依頼し、要求者が動的組織のメンバであることを個人認証連携部が確認したら、処理を実行することが好ましい。

【００２４】

動的組織処理実行部は、例えば、動的組織の作成または削除の処理を実行する組織情報形成部、動的組織へのメンバの追加または動的組織からのメンバの削除の処理を実行するメンバ管理手段、動的組織にメンバが所属していることを認証する動的組織認証手段、または動的組織に関する情報を参照する処理を実行する動的組織情報参照手段を含む。

【００２５】

動的組織処理実行部が、要求者が動的組織に所属しているか否かによって、要求者の処理実行権限を決定するようにしてもよい。

【００２６】

動的組織管理装置は、動的組織の所属メンバの権限を、メンバが属する静的組織に応じて管理する権限管理部を備えていてもよい。

【００２７】

そのような構成によって、メンバの所属する静的組織と関連付けて動的組織におけるメンバの権限を管理することできる。

【００２８】

権限管理部は、動的組織処理実行部の要求に応じて、個人認証対応情報記憶部の記憶内容にもとづいてメンバが属する静的組織を特定し、特定した静的組織に付与される権限を権限情報記憶部から抽出し、抽出した権限を動的組織処理実行部に返すように構成されていてもよい。

【００２９】

本発明による動的組織管理システムは、木構造で管理されている静的組織の１つ以上のメンバで構成される動的組織の管理を行う動的組織管理システムであって、動的組織に関する処理の要求を行う端末と、端末から要求を受けたときに、端末を操作した動的組織の所属メンバの信頼性を、メンバが属する静的組織におけるメンバを個人認証する個人認証装置と連携して判断する個人認証連携部を含む動的組織管理装置とを備えたこと特徴とする。

【００３０】

そのような構成によって、信頼性を保証されたメンバ自身が動的組織の作成・削除や所属メンバの追加・削除等を行なうことができるようになり、動的組織の管理に関して管理者の手間を増加させることなく、信頼性が保証された動的組織の管理を実行することができる。

【００３１】
本発明による動的組織管理方法は、木構造で管理されている静的組織の１つ以上のメンバで構成される動的組織の管理を行う動的組織管理方法であって、動的組織の所属メンバの信頼性を、メンバが属する静的組織におけるメンバを個人認証する個人認証装置と連携して判断すること特徴とする。さらに、動的組織の所属メンバの権限を、メンバが属する静的組織に応じて管理することが好ましい。
【００３２】
本発明による動的組織管理プログラムは、動的組織管理装置におけるコンピュータに、静的組織におけるメンバを個人認証する個人認証装置を示す情報を記憶する個人認証対応情報記憶部に記憶されている情報にもとづいて個人認証装置を特定する処理と、個人認証装置を示す情報に対応させて個人認証装置が用いる認証方式を記憶する個人認証装置情報記憶部に記憶されている情報にもとづいて個人認証装置が用いる認証方式を特定する処理と、通信回線を介して、特定された個人認証装置に、特定された認証方式に従ったメンバの個人認証の要求を送信する処理とを実行させることを特徴とする。
【００３３】
本発明による他の態様の動的組織管理プログラムは、動的組織管理装置におけるコンピュータに、静的組織におけるメンバを個人認証する個人認証装置を示す情報を記憶する個人認証対応情報記憶部に記憶されている情報にもとづいて個人認証装置を特定する処理と、個人認証装置を示す情報に対応させて個人認証装置が用いる認証方式を記憶する個人認証装置情報記憶部に記憶されている情報にもとづいて個人認証装置が用いる認証方式を特定する処理と、通信回線を介して、特定された個人認証装置に、特定された認証方式に従ったメンバの個人認証の要求を送信する処理と、個人認証対応情報記憶部の記憶内容にもとづいてメンバが属する静的組織を特定する処理と、静的組織に付与される権限を記憶する権限情報記憶部から、特定された静的組織に付与される権限を抽出する処理とをを実行させることを特徴とする。
【発明の効果】
【００３４】
本発明の第１の効果は、動的組織を構成するメンバの信頼性を容易に保証することができ、その結果、動的組織の信頼性も保証されることである。その理由は、静的組織での個人認証装置と連携する個人認証連携手段を有することによって、静的組織での個人認証装置と連携して動的組織のメンバの信頼性を保証することができるようになるからである。
【００３５】
本発明の第２の効果は、動的組織の管理に関して管理者の手間を増加させることなく、信頼性が保証された動的組織を管理することができることである。その理由は、信頼性を保証されたメンバ自身が動的組織の作成・削除や所属メンバの追加・削除を行なうことができるからである。
【００３６】
本発明の第３の効果は、動的組織のメンバの信頼性を保証するために、動的組織専用の個人認証装置を新たに導入する必要がないことである。従って、個人認証装置の運用で必要なメンバＩＤ発行などの管理作業、パスワード忘れの対応など、運用の手間の増加が発生しない。その理由は、静的組織で運用している個人認証装置と連携して、メンバの信頼性を保証するためである。
【００３７】
本発明の第４の効果は、動的組織を構成するメンバが企業間など静的組織をまたがっても、信頼性を保証した動的組織を構成できることである。その理由は、一般的に企業間では静的組織を管理する方法が統一されていないので、個人認証を行なう方式やシステムが異なっているが、本発明の個人認証連携手段は個人認証装置に適した個人認証装置連携手段を自動的に選択することによって、動的組織を構成するメンバの個人認証を統一的に行なうことができるからである。
【００３８】

本発明の第５の効果は、メンバが所属する静的組織と関連付けて動的組織におけるメンバの権限を管理することによって、権限設定の手間が削減されることである。企業間など静的組織をまたがって構成する動的組織では、所属する静的組織に応じて動的組織での権限を付与することがある。たとえば、親会社Ａと子会社Ｂでプロジェクトαを構成する場合、親会社Ａの社員にはプロジェクトαの機密書類を参照可能にするが、子会社Ｂの社員には機密書類を参照させないというような場合である。本発明では、そのような権限管理を、安全に、かつ、容易に実現できる。

【００３９】

すなわち、本発明の権限管理手段は、個人認証対応情報記憶部に記憶される情報からメンバが所属する静的情報を取得してメンバの権限を判断するため、メンバが所属する静的組織を偽ることが困難になり、かつ、権限管理のため個々のメンバに対して所属する静的組織情報を付与することが不要になる。

【発明を実施するための最良の形態】

【００４０】

次に本発明を実施するための最良の形態について図面を参照して詳細に説明する。

【００４１】

図１は、本発明の第１の実施の形態の構成を示すブロック図である、図１に示す動的組織管理システムは、１つ以上の端末１１，１２と、動的組織管理装置２と、１つ以上の個人認証装置３１，３２と、通信回線（通信ネットワーク）４とを含む。

【００４２】

端末１１，１２は、ユーザ（動的組織のメンバ）、または、ＥＲＰ（Ｅｎｔｅｒｐｒｉｓｅ　Ｒｅｓｏｕｒｃｅ　Ｐｌａｎｎｉｎｇ）ソフトウェアなどのシステムが、動的組織の形成や動的組織情報の参照を要求するために使用する端末である。端末１１，１２として、デスクトップ型パーソナルコンピュータ、ノート型パーソナルコンピュータ、モバイルツール、ＳＴＢ（Ｓｅｔ－Ｔｏｐ　ＢＯＸ）などのほか、携帯電話機、ＰＨＳ端末、ＰＤＡ（携帯情報端末：Ｐｅｒｓｏｎａｌ　Ｄｉｇｉｔａｌ　Ａｓｓｉｓｔａｎｔｓ）などを用いることができる。

【００４３】

動的組織管理装置２は、処理部２１と記憶部２２とを備えている。処理部２１は、組織情報形成部２１１と組織情報参照部２１２と個人認証連携部２１３とを含む。組織情報形成部２１１は、動的組織形成手段２１１ａとメンバ管理手段２１１ｂとを含む。

【００４４】

動的組織形成手段２１１ａは、端末１１，１２からの動的組織作成や動的組織削除の要求を受け、動的組織情報記憶部２２ａに動的組織情報を登録したり、動的組織情報記憶部２２ａから動的組織情報を削除する処理を行なう。動的組織形成手段２１１ａは、端末１１，１２から要求を受けたときに、個人認証連携手段２１３ａと連携して、端末１１，１２から要求を出したユーザの信頼性を確認する。

【００４５】

メンバ管理手段２１１ｂは、端末１１，１２からの動的組織へのメンバ追加や削除の要求を受け、動的組織情報記憶部２２ａに、動的組織に所属するメンバを登録したり、動的組織情報記憶部２２ａからメンバを削除する処理を行なう。メンバ管理手段２１１ｂは、端末１１，１２から要求を受けたときに、個人認証連携手段２１３ａと連携して、端末１１，１２から要求を出したユーザの信頼性を確認する。

【００４６】

組織情報参照部２１２は、動的組織認証手段２１２ａと動的組織情報参照手段２１２ｂとを含む。動的組織認証とは、メンバが動的組織に所属していることを証明することである。動的組織認証手段２１２ａは、端末１１，１２からの動的組織認証の要求を受け、指定されたメンバが指定された動的組織に所属するか否かを動的組織情報記憶部２２ａから検索し、認証結果を端末１１，１２に返す手段である。動的組織情報参照手段２１２ｂは、端末１１，１２からの動的組織に関する情報参照要求を受け、要求された動的組織に関

する所属メンバなどの情報を動的組織情報記憶部２２ａから取得し、個人認証連携手段２１３ａと連携して要求者の信頼性を確認したのち、その要求者に公開可能な情報を返す手段である。

【００４７】

個人認証連携部２１３は、個人認証連携手段２１３ａと、それぞれが特定の個人認証方式にもとづく認証要求を出力する１つ以上の個人認証装置連携手段２１３ｂとを含む。個人認証連携手段２１３ａは、組織情報形成部２１１や組織情報参照部２１２からメンバの信頼性確認の要求（以下、メンバ認証という。）を受け、個人認証装置３１，３２と連携してメンバ認証を行なう手段である。個人認証連携手段２１３ａは、個人認証対応情報記憶部２２ｃから、どの個人認証装置で対象メンバの信頼性を確認すればよいかの情報（具体的には個人認証装置ＩＤ）を取得し、個人認証装置情報記憶部２２ｂからその個人認証装置ＩＤに対応する認証方式を取得する。そして、その認証方式に対応する個人認証装置連携手段２１３ｂを選択して認証を実行させる。

【００４８】

また、個人認証連携手段２１３ａが、信頼性確認の対象であるメンバに対応する個人認証装置ＩＤが個人認証対応情報記憶部２２ｃに存在しない場合には、メンバ認証を要求する手段によって指定された個人認証装置に対して認証を要求するか、または、個人認証装置情報記憶部２２ｂに登録されている全ての個人認証装置３１，３２に対して順に認証を要求し、認証が成功した場合に、新規にそのメンバに対応する個人認証対応情報（メンバのＩＤとメンバを認証する個人認証装置の個人認証装置ＩＤとの組み）を個人認証対応情報記憶部２２ｃに追加するようにしてもよい。

【００４９】

個人認証装置連携手段２１３ｂは、連携する個人認証装置３１，３２の認証方式（ＬＤＡＰなど）ごとに１つ以上存在する。例えば、システム内に存在する全ての個人認証装置３１，３２が、ＬＤＡＰにもとづく認証方式（認証方式Ｐとする。）とそれ以外の１種類の認証方式（認証方式Ｑとする。）とのいずれかを使用している場合には、認証方式Ｐに対応する個人認証装置連携手段２１３ｂと、認証方式Ｑに対応する個人認証装置連携手段２１３ｂとの２つが設けられる。個人認証装置連携手段２１３ｂは、個人認証連携手段２１３ａからのメンバ認証の要求を、認証方式ごとの要求に変換し、連携する個人認証装置に対して、メンバの認証の要求を通信回線４を介して送信する手段である。そして、要求に応じてメンバの認証を実行した個人認証装置から、通信回線４を介して認証結果を受信し、受信した認証結果を個人認証連携手段２１３ａに返す。

【００５０】

記憶部２２は、動的組織情報記憶部２２ａ、個人認証装置情報記憶部２２ｂおよび個人認証対応情報記憶部２２ｃを含む。動的組織情報記憶部２２ａは、動的組織のＩＤ、組織名称および動的組織の所属メンバのＩＤを記憶している。

【００５１】

個人認証装置情報記憶部２２ｂは、動的組織管理装置２と信頼関係を持つ個人認証装置３１，３２に関する情報を記憶し、個人認証装置のＩＤ（以下、個人認証装置ＩＤという。）と認証方式とサーバのアドレスなどの連携に必要な情報（個人認証装置をアクセスするための情報）とを、対応させてあらかじめ記憶している。例えば、動的組織管理装置２の管理者が、システムを稼働させるときや、システム稼働後の必要なときに、入力手段（図示せず）から、個人認証装置ＩＤ、および、それに対応する認証方式とサーバのアドレスなどの連携に必要な情報とを、個人認証装置情報記憶部２２ｂに登録する。

【００５２】

個人認証対応情報記憶部２２ｃは、個人認証対応情報、つまり、メンバのＩＤとメンバを認証する個人認証装置の個人認証装置ＩＤとの組みを記憶している。

【００５３】

個人認証装置３１，３２は、企業などの組織において、情報システムの利用を目的した社員認証などの個人認証の仕組みを提供する装置で、一般に、メンバのＩＤやパスワード

を管理している。加えて、部や課などの静的組織の情報を管理する機能を合わせて有していてもよい。たとえば、ＬＤＡＰサーバ、マイクロソフト社のＡｃｔｉｖｅＤｉｒｅｃｔｏｒｙサーバ、または単純に社員ＩＤおよびパスワードをデータベースに格納して認証結果を返す装置などを用いることができる。

【００５４】

通信回線４として、公知の公衆回線、商業回線、または専用回線を用いることができる。また、端末11，１２と動的組織管理装置２の間と、個人認証装置３１，３２と動的組織管理装置２の間とで、同一または別の通信回線を用いてもよい。さらに、通信回線４は、端末11，１２、動的組織管理装置２、個人認証装置３１，３２のそれぞれの間を、無線あるいは有線で接続可能な回線であり、例えば、携帯電話網、公衆回線網、専用回線網、インターネットおよびイントラネットで構成することができる。

【００５５】

なお、動的組織管理装置２として、サーバ装置を用いることができる。その場合、組織情報形成部２１１、組織情報参照部２１２および個人認証連携部２１３は、それらが実行する処理を実現するためのサーバ装置に搭載されたプログラムと、プログラムに従って処理を実行するＣＰＵとで実現される。

【００５６】

次に、図１および図２～図８のフローチャートを参照して第１の形態の動作について説明する。本実施の形態では、（１）動的組織の作成・削除、（２）動的組織への所属メンバ追加・削除、（３）動的組織認証、（４）動的組織情報参照の４つ処理が行われる。４つの処理において、メンバの信頼性を保証するために、（５）メンバ認証が実行される。

【００５７】

まず、（５）メンバ認証の処理について、図２のフローチャートを参照して説明する。個人認証連携手段２１３ａは、メンバ認証を要求した手段（組織情報形成部２１１または組織情報参照部２１２）から、個人認証に必要とされるメンバのＩＤ（個人認証ＩＤ）と認証方法ごとに異なるパスワードなどの情報（以下、個人認証用情報という。）とを受け取る（ステップＳ１）。次に、受け取った個人認証ＩＤに対応する個人認証装置ＩＤを個人認証対応情報記憶部２２ｃから取得する（ステップＳ２）。

【００５８】

個人認証対応情報記憶部２２ｃに個人認証ＩＤに対応する個人認証装置ＩＤが存在した場合には（ステップＳ３）、個人認証連携手段２１３ａは、個人認証装置ＩＤに対応する個人認証装置の情報を個人認証装置情報記憶部２２ｂから取得する（ステップＳ４）。個人認証装置の情報は、ＬＤＡＰなどの認証方式と、個人認証装置ＩＤに対応する個人認証装置に接続するため情報（以下、個人認証装置連携手段用情報という。）とを含む。個人認証装置連携手段用情報は、例えば個人認証装置ＩＤに対応するＬＤＡＰサーバアドレスである。以下、個人認証装置情報記憶部２２ｂから、個人認証装置ＩＤとして、個人認証装置３１を示す個人認証装置ＩＤが取得されたとして説明を進める。

【００５９】

個人認証連携手段２１３ａは、個人認証装置情報記憶部２２ｂから取得した認証方式に適した個人認証装置連携手段２１３ｂを選択し（ステップＳ５）、認証に必要な個人認証ＩＤ、個人認証用情報、および個人認証装置ＩＤに対応する個人認証装置連携手段用情報を、選択した個人認証装置連携手段２１３ｂに出力する。個人認証装置連携手段２１３ｂは、個人認証装置連携手段用情報を用いて、個人認証装置ＩＤに対応する個人認証装置３１に対して個人認証を要求し、認証成功／認証失敗の結果を取得する（ステップＳ６）。このように、個人認証連携手段２１３ａは、個人認証ＩＤに対応する個人認証装置に適した認証方式を個人認証装置情報記憶部２２ｂから抽出し、個人認証連携手段によって抽出された個人認証装置連携手段２２ｂが、個人認証装置に静的組織におけるメンバの個人認証を依頼する。そして、個人認証連携手段２１３ａは、認証結果を個人認証装置連携手段２１３ｂから取得し、メンバ認証を要求した手段に返す（ステップＳ７）。メンバ認証を要求した手段（動的組織処理実行部）は、認証成功の結果を受けたら、すなわち、処理（

動的組織の作成・削除、動的組織への所属メンバ追加・削除、動的組織認証、動的組織情報参照等）の要求者が動的組織のメンバであることを個人認証連携部２１３が確認したら、処理を実行する。

【００６０】

個人認証対応情報記憶部２２ｃに個人認証ＩＤに対応する個人認証対応情報が存在しない場合、すなわち個人認証ＩＤに対応する個人認証装置ＩＤが存在しない場合には（ステップＳ３）、個人認証連携手段２１３ａは、個人認証を行う個人認証装置３１の個人認証装置ＩＤが、メンバ認証を要求した手段によって指定されているか判断し（ステップＳ８）、指定されていない場合には、メンバ認証を要求した手段に対して個人認証装置ＩＤの指定（選択）を要求する（ステップＳ９）。そして、指定された個人認証装置ＩＤに対応する個人認証装置３１の情報を個人認証装置情報記憶部２２ｂから取得する（ステップＳ１０）。ステップＳ１０では、個人認証連携手段２１３ａは、ステップＳ５の処理と同様に、認証方式に適した個人認証装置連携手段２１３ｂを選択する（ステップＳ１１）。

【００６１】

個人認証装置連携手段２１３ｂは、個人認証装置３１に対して個人認証を要求し、認証成功／認証失敗の結果を取得する（ステップＳ１２）。認証成功した場合には、個人認証連携手段２１３ａは、個人認証対応情報記憶部２２ｃに、新規の個人認証対応情報（個人認証ＩＤと個人認証装置ＩＤとのを組み）を追加する。

【００６２】

なお、ステップＳ８において、メンバ認証を要求する手段（組織情報形成部２１１または組織情報参照部２１２）に、個人認証装置ＩＤを明示的に指定させるのではなく、個人認証連携手段２１３ａが、個人認証装置情報記憶部２２ｂに登録されている全ての個人認証装置３１，３２に、個人認証ＩＤと個人認証用情報で個人認証を実行させ、認証成功した個人認証装置の個人認証装置ＩＤを含む個人認証対応情報を個人認証対応情報記憶部２２ｃに登録してもよい。

【００６３】

動的組織管理装置２が１つ以上の個人認証装置３１，３２と連携した場合、個人認証ＩＤが重複する可能性がある。例えば、個人認証装置３１が記憶しているメンバのＩＤやパスワードが個人認証装置３２が記憶しているメンバのＩＤやパスワードと、たまたま一致するような場合である。その場合の対策として、個人認証ＩＤと個人認証装置ＩＤを連結したＩＤを個人認証ＩＤとして利用することができる。例えば、“個人認証ＩＤ．（ドット）個人認証装置ＩＤ”とする。

【００６４】

次に、（１）動的組織の作成・削除の処理について説明する。

まず、動的組織を新規に作成する処理について図３のフローチャートを参照して説明する。動的組織を生成するユーザは、まず、例えば端末１１に、動的組織作成の要求と、後述する必要な情報とを入力する。なお、動的組織作成の要求と必要な情報とは、ユーザから入力されるのではなく、端末１１に実装されているアプリケーションプログラムや他の装置から入力されることもある。このことは、以下に説明する他の処理（動的組織の削除、動的組織への所属メンバ追加・削除、動的組織認証、動的組織情報参照）においても同様である。

【００６５】

端末１１は、入力された要求および情報を通信回線４を介して動的組織管理装置２に送信する。動的組織管理装置２において、動的組織形成手段２１１ａは、端末１１から動的組織作成の要求を受け取る（ステップＳ２１）。要求には、作成する動的組織のＩＤ（動的組織ＩＤ）や組織名称などの情報、および、要求を出したメンバの認証用の個人認証ＩＤと認証用の個人認証用情報とが付随する。

【００６６】

動的組織形成手段２１１ａは、個人認証連携手段２１３ａに個人認証ＩＤおよび個人認証用情報を渡しメンバ認証を実行させる（ステップＳ２２）。メンバ認証の仕方は既に説

明したとおりである（図２参照）。動的組織形成手段２１１ａは、認証成功の場合には、動的組織情報記憶部２２ａを検索して動的組織ＩＤの重複がないか確認し（ステップＳ２３，Ｓ２４）、重複がなければ新規の動的組織として動的組織ＩＤなどの情報を動的組織情報記憶部２２ａに追加する（ステップＳ２５）。また、動的組織作成の要求を出したユーザを、動的組織の所属メンバとして動的組織情報記憶部２２ａに登録する。

【００６７】

次に、動的組織を削除する処理について図４のフローチャートを参照して説明する。動的組織に所属するユーザは、動的組織を削除しようとするときに、例えば端末１１に、動的組織削除の要求と、後述する必要な情報とを入力する。端末１１は、入力された要求および情報を通信回線４を介して動的組織管理装置２に送信する。動的組織管理装置２において、動的組織形成手段２１１ａは、端末１から動的組織削除の要求を受け取る（ステップＳ３１）。要求には、削除する動的組織ＩＤ、および、要求を出したメンバの認証用の個人認証ＩＤと個人認証用情報とが付随する。

【００６８】

次に、動的組織形成手段２１１ａは、個人認証連携手段２１３ａに個人認証ＩＤと個人認証用情報を渡しメンバ認証を実行させる（ステップＳ３２）。メンバ認証の仕方は既に説明したとおりである（図２参照）。動的組織形成手段２１１ａは、認証成功の場合には、動的組織情報記憶部２２ａを検索して、要求を出したユーザが、削除する動的組織の所属メンバであるか否か確認する（ステップＳ３３，Ｓ３４）。その確認は、動的組織に所属するメンバにのみ削除の権限を付与するために実行される。メンバが、削除する動的組織に含まれているメンバであれば、動的組織形成手段２１１ａは、指定された動的組織の情報を動的組織情報記憶部２２ａから削除する（ステップＳ３５）。なお、動的組織に所属するメンバのうちの特定のメンバに管理者の権限を付与し、管理者しか削除できないようにしてもよい。

【００６９】

次に、（２）動的組織への所属メンバ追加・削除の処理について説明する。

まず、動的組織に所属するメンバを追加する処理について図５のフローチャートを参照して説明する。動的組織にメンバを追加しようと意図するユーザは、まず、例えば端末１１に、所属メンバ追加の要求と、後述する必要な情報とを入力する。端末１１は、入力された要求および情報を通信回線４を介して動的組織管理装置２に送信する。動的組織管理装置２において、メンバ管理手段２１１ｂは、端末１１から所属メンバ追加の要求を受け取る（ステップＳ４１）。要求には、追加対象の動的組織ＩＤ、追加するメンバの個人認証ＩＤ、および、要求を出したメンバの認証用の個人認証ＩＤと個人認証用情報とが付随する。

【００７０】

次に、メンバ管理手段２１１ｂは、要求を出したメンバの個人認証ＩＤと個人認証用情報とを個人認証連携手段２１３ａに渡しメンバ認証を実行させる（ステップＳ５２）。メンバ認証の仕方は既に説明したとおりである（図２参照）。メンバ管理手段２１１ｂは、認証成功の場合には、動的組織情報記憶部２２ａを検索して、要求を出したユーザが、メンバを追加する動的組織の所属メンバであるか否か確認する（ステップＳ５３，Ｓ５４）。その確認は、動的組織に所属するメンバにのみメンバを追加する権限を付与するために実行される。要求を出したユーザが動的組織に所属していれば、メンバ管理手段２１１ｂは、動的組織の所属メンバとして動的組織情報記憶部２２ａに追加する（ステップＳ４５）。

【００７１】

動的組織に所属するメンバを削除する動作について図６のフローチャートを参照して説明する。動的組織からメンバ削除しようと意図するユーザは、まず、例えば端末１１に、所属メンバ削除の要求と、後述する必要な情報とを入力する。端末１１は、入力された要求および情報を通信回線４を介して動的組織管理装置２に送信する。動的組織管理装置２において、メンバ管理手段２１１ｂは、端末１から所属メンバ削除の要求を受け取る（ス

テップＳ５１）。要求には、削除対象の動的組織ＩＤ、削除するメンバの個人認証ＩＤ、および、要求を出したメンバの認証用の個人認証ＩＤと個人認証用情報とが付随する。基本的には、削除するメンバ自身が所属メンバ削除の権限を保有するが、動的組織に所属するメンバのうちの特定のメンバに管理者の権限を付与し、管理者が所属メンバ削除の要求を出せるようにしてもよい。

【００７２】

次に、メンバ管理手段２１１ｂは、要求を出したメンバの個人認証ＩＤと個人認証用情報とを個人認証連携手段２１３ａに渡しメンバ認証を実行させる（ステップＳ５２）。メンバ認証の仕方は既に説明したとおりである（図２参照）。メンバ管理手段２１１ｂは、認証成功の場合には、動的組織情報記憶部２２ａから指定メンバを削除する（ステップＳ５６）。メンバを削除した結果、動的組織に所属するメンバが存在しなくなった場合には、メンバ管理手段２１１ｂは、動的組織自体を動的組織情報記憶部２２ａから削除する（ステップＳ５５，Ｓ５６）。

【００７３】

次に、（３）動的組織認証の処理について、図７のフローチャートを参照して説明する。動的組織認証とは、指定された動的組織に指定されたメンバが所属していることを認証することであるが、ファイル管理システムなどが、動的組織が所有するファイルを、要求したメンバに対して公開してよいか判断する場合などに使用される。

【００７４】

動的組織認証を意図するユーザは、まず、例えば端末１１に、動的組織認証の要求と、後述する必要な情報とを入力する。端末１１は、入力された要求および情報を通信回線４を介して動的組織管理装置２に送信する。動的組織管理装置２において、動的組織認証手段２１２ａは、端末１１から動的組織認証の要求を受け取る（ステップＳ６１）。要求には、認証の対象となる動的組織の動的組織ＩＤと、要求したメンバの個人認証ＩＤおよび個人認証用情報が含まれる。次に、動的組織認証手段２１２ａは、要求を出したメンバの個人認証ＩＤと個人認証用情報とを個人認証連携手段２１３ａに渡しメンバ認証を実行させる（ステップＳ６２）。メンバ認証の仕方は既に説明したとおりである（図２参照）。動的組織認証手段２１２ａは、メンバ認証に成功した場合には、動的組織情報記憶部２２ａを検索して、そのメンバが認証の対象となる動的組織に所属するか否か確認する（ステップＳ６３，Ｓ６４）。そして、所属していた場合は認証成功の結果を要求者（具体的には端末１１）に返す（ステップＳ６５）。また、所属していない場合は認証失敗の結果を要求者に返す（ステップＳ６６）。

【００７５】

最後に、（４）動的組織情報参照の処理について、図８のフローチャートを参照して説明する。動的組織情報参照は、動的組織のメンバが自分が所属する動的組織についてメンバの一覧などの情報を参照するときに使用される。

【００７６】

動的組織情報参照を意図するユーザは、まず、例えば端末１１に、動的組織情報参照の要求と、後述する必要な情報とを入力する。端末１１は、入力された要求および情報を通信回線４を介して動的組織管理装置２に送信する。動的組織管理装置２において、動的組織情報参照手段２１２ｂは、端末１１から動的組織情報参照の要求を受け取る（ステップＳ７１）。要求には、動的組織情報の参照を要求を出したメンバの個人認証ＩＤと個人認証用情報とが付随する。次に、動的組織情報参照手段２１２ｂは、個人認証連携手段２１３ａに要求を出したメンバの個人認証ＩＤと個人認証用情報とを渡してメンバ認証を実行させる（ステップＳ７２）。メンバ認証の仕方は既に説明したとおりである（図２参照）。動的組織情報参照手段２１２ｂは、認証成功の場合には、動的組織情報記憶部２２ａから指定メンバが所属するすべての動的組織に関する情報を取得する（ステップＳ７３，Ｓ７４）。そして、取得した所属メンバなどの動的組織の情報を要求者に返す（ステップＳ７５）。

【００７７】

なお、動的組織形成手段２１１ａが動的組織を削除する処理を行うとき、メンバ管理手段２１１ｂが動的組織にメンバを追加したり動的組織からメンバを削除するとき、動的組織認証手段２１２ａが動的組織認証の処理を行うとき、および組織情報参照手段２１２ｂが動的組織情報記憶部２２ａから動的組織に関する情報を取得するとき（動的組織に関する情報を参照する処理を実行するとき）に、処理の要求者が動的組織情報記憶部２２ａに動的組織のメンバとして登録されていない場合には、個人認証連携部２１３に要求者の認証を依頼することなく、処理を実行しないようにしてもよい。すなわち、指定された動的組織に要求者が所属しているか否かによって、要求者の処理実行権限を認めたり制限したりするようにしてもよい。

【００７８】

本実施の形態の効果について説明する。本実施の形態では、動的組織管理装置が、静的組織において個人認証を行なう個人認証装置と連携して動的組織に所属するメンバの信頼性を保証することによって、信頼性の高い動的組織管理を行なうことができる。また、信頼性を保証されたメンバ自身が動的組織の作成・削除や所属メンバの追加・削除を行なうことによって、管理者の手間を増加させない動的組織の管理を実現することができる。

【００７９】

加えて、個人認証装置との連携手段を適切なものに自動選択する個人認証連携手段２１３ａを有することで、メンバの信頼性を保証する方法が異なる静的組織間でも動的組織を管理することができる。

【００８０】

次に、本発明の第２の実施の形態について図面を参照して説明する。

図９は、本発明の第２の実施の形態の構成を示すブロック図である、図９に示す第２の実施の形態の動的組織管理システムは、動的組織管理装置２０における制御部２１が権限管理部２１４を有し、記憶部２２が権限情報記憶部２２ｄを有する点で、第１の実施の形態とは異なる。

【００８１】

権限管理部２１４は、権限確認手段２１４ａと権限設定手段２１４ｂとを含む。権限確認手段２１４ａは、動的組織形成手段２１１ａ、メンバ管理手段２１１ｂ、動的組織認証手段２１２ａまたは動的組織情報参照手段２１２ｂの要求に応じて動作し、要求を出したメンバが各手段を実行する権限を保有しているか否か判断する。具体的には、要求を出したメンバが所属する静的組織つまり個人認証装置ＩＤを個人認証対応情報記憶部２２ｃから取得し、その静的組織が権限を保有しているか否かを権限情報記憶部２２ｄから検索する。権限確認手段２１４ａと権限設定手段２１４ｂは、それらが実行する処理を実現するためのサーバ装置に搭載されたプログラムと、プログラムに従って処理を実行するＣＰＵとで実現される。

【００８２】

権限設定手段２１４ｂは、端末１１，１２からの権限設定の要求を受け、権限情報記憶部２２ｄに権限情報を設定する手段である。権限設定の要求は、静的組織単位つまり個人認証装置ＩＤ単位で、動的組織の作成権限・削除権限、所属メンバの追加権限・削除権限、動的組織情報の参照権限、権限の設定権限などの権限を付与・剥奪するという内容になる。このとき、権限設定手段２１４ｂは、個人認証連携手段２１３ａと連携して端末１１，１２から要求を出したユーザの信頼性を確認し、また、権限確認手段２１４ａと連携して要求者が権限設定をする権限を保持するかを確認する。

【００８３】

権限情報記憶部２２ｄは、静的組織が保持する権限、具体的には、個人認証装置ＩＤと権限種別（動的組織の作成権限など）の組みを記憶している。換言すれば、それぞれの静的組織（具体的には静的組織のメンバ）に付与される権限を記憶している。例えば、動的組織管理装置２の管理者が、システムを稼働させるときや、システム稼働後の必要なときに、入力手段（図示せず）から、個人認証装置ＩＤ、およびそれに対応する権限種別を権限情報記憶部２２ｄに登録する。

【００８４】
次に、図１０のフローチャートを参照して権限確認の動作について説明する。権限確認手段２１４ａは、動的組織形成手段２１１ａ、メンバ管理手段２１１ｂ、動的組織認証手段２１２ａまたは動的組織情報参照手段２１２ｂから権限確認の要求を受けたときに動作する。要求を受けるタイミングは、それぞれの動作においてメンバ認証が成功した直後になる。たとえば、図３に示された動的組織の作成においては、ステップＳ２５の動的組織情報登録の直前になる。
【００８５】
権限確認手段２１４ａは、それぞれの手段から、要求の内容として、確認する権限種別と対象となるメンバの個人認証ＩＤを受け取る（ステップＳ１０１）。次に、対象となるメンバを認証する個人認証装置の個人認証装置ＩＤを個人認証対応情報記憶部２２ｃから取得する。つまり、対象となるメンバが所属する静的組織を示す情報を取得する（ステップＳ１０２）。さらに、権限確認手段２１４ａは、個人認証装置ＩＤをキーに権限情報記憶部２２ｄを検索し、対象となる権限を静的組織が保有しているか否かの情報を取得する（ステップＳ１０３）。最後に、権限確認手段２１４ａは、権限を保有しているか否かの情報を、権限確認を要求した手段に返す（ステップＳ１０４）。権限確認を要求した手段は、権限を保有していないという情報を受けた場合には、動的組織作成などの処理を取りやめる。
【００８６】
以上のように、本実施の形態では、権限管理部２１４は、動的組織処理実行部（組織情報形成部２１１または組織情報参照部２１２）の要求に応じて、個人認証対応情報記憶部２２ｂの記憶内容にもとづいてメンバが属する静的組織を特定し、特定した静的組織に付与される権限を権限情報記憶部２２ｄから抽出し、抽出した権限を動的組織処理実行部に返す。動的組織処理実行部は、処理の要求を行ったメンバが、処理の権限がないことを権限情報記憶部２２ｄから通知されると、処理を実行しない。
【００８７】
本実施の形態の効果について説明する。本実施の形態では、動的組織管理装置が、個人認証の情報からメンバが所属する静的組織を判断して、動的組織作成・削除や所属メンバ追加・削除、動的組織情報の参照などの動的組織における権限を制御することができる。このため、メンバが、所属する静的組織を偽ることが困難になる。加えて、静的組織に依存した権限制御を行なうための、メンバ個々への権限付与の手間を軽減できる。
【実施例】
【００８８】
次に、本発明の第１の実施例を、図面を参照して説明する。第１の実施例は本発明の第１の実施の形態に対応する。この実施例では、３つの企業間の社員で動的組織を構成されるとする。企業Ａは、ＬＤＡＰで社員を管理する個人認証装置Ａを、企業Ｂは、ＬＤＡＰで社員を管理する個人認証装置Ｂを、企業Ｃは、データベースを利用した独自の認証管理を行っているとする。
【００８９】
図１１は、個人認証装置情報記憶部２２ｂに記憶されている個人認証装置の情報の例を示す説明図である。個人認証装置の情報として、静的組織ごとの個人認証装置を識別するための個人認証装置ＩＤと、認証方式と、個人認証装置連携手段２１３ｂが動作するために必要となる個人認証装置連携手段用情報とが、対応付けて記憶されている。
【００９０】
図１２は、個人認証対応情報記憶部２２ｃに記憶される情報の例を示す説明図である。個人認証対応情報には、個人認証ＩＤと、メンバの認証を行なう個人認証装置の個人認証装置ＩＤとが組みで記憶される。この例では、個人認証装置連携手段２１３ｂとして、ＬＤＡＰ用個人認証装置連携手段と、データベースを利用した独自の認証装置連携手段の２種類が存在する。
【００９１】

企業Ａの社員山田太郎氏（個人認証ＩＤ：yamada taro）が企業Ａ、Ｂ、Ｃを横断して構成する動的組織プロジェクトＸ（動的組織ＩＤ：PROJECT_X）の作成要求を例えば端末１１から動的組織管理装置２に出したとする。山田太郎氏は、自分の個人認証ＩＤ、および認証のために必要な個人認証用情報としてのパスワードも送る。

【００９２】

動的組織の作成の要求を受けた動的組織形成手段２１１ａは、要求を出した山田太郎氏の信頼性を確認するために、個人認証連携手段２１３ａに個人認証ＩＤ yamada taro とパスワードを渡し、メンバ認証を行なわせる。個人認証連携手段２１３ａは、個人認証対応情報記憶部２２ｃの個人認証ＩＤ yamada taroの情報（図１２に示す情報１４０１）から、山田太郎氏の認証は個人認証装置ＩＤ kigyo_Aで行なわれると判断する。

【００９３】

次に、個人認証連携手段２１３ａは、個人認証装置情報記憶部２２ｂから個人認証装置ＩＤ kigyo_Aの情報（図１１に示す情報１３０１）を取得し、認証方式の情報からＬＤＡＰ用個人認証装置連携手段に対して、山田太郎氏の個人認証ＩＤ yamada taroとパスワードとを渡す。ＬＤＡＰ用個人認証装置連携手段は、個人認証装置情報記憶部２２ｂから個人認証装置ＩＤ kigyo_Aの個人認証装置連携手段用情報（図１１に示す情報１３０１）を取得し、指定された個人認証装置Ａに対して個人認証を要求し、認証成功の結果を取得する。ＬＤＡＰ用個人認証装置連携手段は、認証成功の結果を個人認証連携手段２１３ａに返す。

【００９４】

個人認証連携手段２１３ａは、結果を、動的組織形成手段２１１ａに出力する。動的組織形成手段２１１ａは、山田太郎氏の信頼性が確認されたので、動的組織ＩＤ PROJECT_Xの重複がないか否か確認して、重複がない場合には、動的組織情報記憶部２２ａに動的組織ＩＤ PROJECT_Xの動的組織を登録し、さらに、山田太郎氏を所属メンバとして登録する。図１３は、このときの動的組織情報記憶部２２ａに記憶される情報の例を示す。動的組織プロジェクトＸに関する情報は情報１５０１になる。

【００９５】

次に、山田太郎氏が企業Ｂの社員鈴木花子氏（個人認証ＩＤ：suzuki hanako）、企業Ｃの佐藤次郎氏（個人認証ＩＤ：sato jiro）および企業Ａの社員林三郎氏（個人認証ＩＤ：hayashi saburo）を動的組織プロジェクトＸのメンバとして追加したとする。すると、図１４に示すように、動的組織情報記憶部２２ａに情報が記憶され、動的組織プロジェクトＸに関する情報は情報１６０１になる。

【００９６】

次に、企業Ｃの佐藤次郎氏（個人認証ＩＤ：sato jiro）が、動的組織プロジェクトＸ（動的組織ＩＤ：PROJECT_X）の所属メンバから自分を削除する要求を例えば端末１２から動的組織管理装置２に出したとする。佐藤次郎氏は、自分の個人認証ＩＤおよび認証のために必要なパスワードも送る。所属メンバの削除の要求を受けたメンバ管理手段２１１ｂは、要求を出した佐藤次郎氏の信頼性を確認する。すなわち、メンバ認証を行う。

【００９７】

メンバ認証の方法は、基本的に山田太郎氏の場合と同様であるが、佐藤次郎氏が所属する企業Ｃの認証方法に対応する企業Ｃ用個人認証装置連携手段が使用される点が異なる。つまり、個人認証連携手段２１３ａは、個人認証装置情報記憶部２２ｂから個人認証装置ＩＤ kigyo_Cの個人認証装置連携手段用情報（図１１に示す情報１３０２）を取得し、指定された個人認証装置Ｃに対して個人認証を要求する。認証が成功した場合には、メンバ管理手段２１１ｂは、メンバ認証に成功した佐藤次郎氏を動的組織プロジェクトＸの所属メンバから削除する。このとき、佐藤次郎氏が所属メンバから削除されても所属メンバの数が０にならないので動的組織プロジェクトＸは削除されない。

【００９８】

次に、本発明の第２の実施例を、図面を参照して説明する。第２の実施の形態は本発明の第２の実施の形態に対応する。

【００９９】
図１５は、権限情報記憶部２２ｄが記憶する情報を示す説明図である。図１５に示される例では、企業Ａには動的組織に関するすべての権限が与えられている（図１５における情報１７０１参照）のに対して、企業Ｃには動的組織参照権限しか与えられていない（図１５における情報１７０２参照）。図１５に示す例では、対象動的組織ＩＤの情報１７０３があるが、情報１７０３は、所属メンバ追加などの権限制御の対象を特定の動的組織に限定する場合に利用される。
【００１００】
第１の実施例と同様に、企業Ａの社員山田太郎氏（個人認証ＩＤ：yamada taro ） が動的組織プロジェクトＸ（動的組織ＩＤ：PROJECT_X ）の作成要求を端末１１から動的組織管理装置２に出したとする。山田太郎氏のメンバ認証が成功するまでの動作は、第１の実施例の場合と同様である。次に、動的組織形成手段２１１ａは、山田太郎氏が動的組織作成の権限を持つか否か確認するために、権限確認手段２１４ａに、個人認証ＩＤ yamada taroと確認対象の権限として「動的組織作成」を渡す。権限確認手段２１４ａは、個人認証対応情報記憶部２２ｃの個人認証ＩＤ yamada taroの情報（図１２に示す情報１４０１）から、山田太郎氏は個人認証装置ＩＤ kigyo_Aで認証される静的組織に所属すると判断する。
【００１０１】
次に、権限確認手段２１４ａは、個人認証装置ＩＤ kigyo_A が権限「動的組織作成」を持つか否かを権限情報記憶部２２ｄから検索する。この場合、権限「動的組織作成」を持つので（図１５参照）、動的組織形成手段２１１ａは、第１の実施例の場合と同様の処理を行う。
【００１０２】
次に、山田太郎氏が企業Ｃの佐藤次郎氏（個人認証ＩＤ：sato jiro ）を動的組織プロジェクトＸのメンバとして追加したとする。そのあと、企業Ｃの佐藤次郎氏が企業Ｂの社員 鈴木花子氏（個人認証ＩＤ：suzuki hanako ）を動的組織プロジェクトＸの所属メンバとして追加する要求を端末１２から動的組織管理装置２に出したとする。佐藤次郎氏のメンバ認証成功までの動作は第１の実施例の場合と同様である。メンバ管理手段２１１ｂは、佐藤次郎氏が所属メンバ追加の権限を持つか否か確認するために、権限確認手段２１４ａに、個人認証ＩＤ sato jiroと確認対象の権限として「所属メンバ追加」を渡す。権限確認手段２１４ａは、個人認証対応情報記憶部２２ｃの個人認証ＩＤ sato jiroの情報（図１２に示す情報１４０２参照）から、佐藤次郎氏は個人認証装置ＩＤ kigyo_Cで認証される静的組織に所属すると判断する。
【００１０３】
次に、権限確認手段２１４ａは、個人認証装置ＩＤ kigyo_Cが権限「所属メンバ追加」を持つか否かを権限情報記憶部２２ｄから検索する。この場合、権限として「所属メンバ追加」を持たないので（図１５における情報１７０２参照）、メンバ管理手段２１１ｂは、佐藤次郎氏の所属メンバ追加の要求を処理しない。
【００１０４】
次に、本発明の第３の実施例を、図面を参照して説明する。図１６は、第３の実施例の動的組織管理システムの構成を示すブロック図である。図１６に示す構成では、図１に示された構成に加えて、ファイル権限管理装置５が追加されている。また、端末１１に端末記憶部１１Ａが接続されている。端末記憶部１１Ａは、端末１１に内蔵されるハードディスク等であってもよい。この実施例では、ファイル権限管理装置５は、動的組織管理装置２と連携して、動的組織のメンバのファイル参照（読み出しや編集など）を管理する。なお、動的組織管理システムの第３の実施例において、図９に示された動的組織管理装置２０を用いてもよい。また、ファイル権限管理装置５は、例えばサーバ装置で実現される。
【００１０５】
既に説明したような処理によって、動的組織Ｓが生成されているとする。動的組織Ｓに属するメンバｓが、動的組織Ｓのメンバにのみ公開するファイルを作成したとする。メン

バｓは、そのファイルについて、動的組織Ｓのメンバにのみ公開するファイルであることを示す権限情報を作成することを、端末１１からファイル権限管理装置５に依頼する。ファイル権限管理装置５は、端末１１からの依頼に応じて、動的組織Ｓを示すファイル権限情報を作成し、それを暗号化する。また、端末記憶部１１Ａに格納されるファイル自体も暗号化する。そして、暗号化されたファイル権限情報を付随させた暗号化されたファイルを、端末記憶部１１Ａに格納する。なお、暗号化されたファイル権限情報を付随させた暗号化されたファイルは、ファイル権限管理装置５に格納されていてもよい。

【０１０６】

他のメンバが、端末記憶部１１Ａに格納されているファイルを参照するために、例えば端末１２から、端末１１を介して、端末記憶部１１Ａに格納されているファイルをダウンロードしたとする。上記のように、そのファイルは暗号化され、暗号化されたファイル権限情報が付随している。

【０１０７】

端末１２は、搭載されているファイル管理用プログラムに従って動作し、暗号化されたファイル権限情報をファイル権限管理装置５に送信する。ファイル権限管理装置５は、端末１２から受信したファイル権限情報を復号し、ファイル権限情報が、当該ファイルが動的組織Ｓのメンバにのみ公開されるファイルであることを示していることを認識する。そこで、ファイル権限管理装置５は、端末１２に対して、動的組織認証を受けるべきであることを指示する情報を送信する。

【０１０８】

端末１２は、動的組織認証を受けるべきであることを指示する情報を受信すると、図７に示された処理を経て、動的組織管理装置２における動的組織認証手段２１２ａから、認証成功または認証失敗の結果の返送を受ける。端末１２は、その結果を、ファイル権限管理装置５に送信する。

【０１０９】

ファイル権限管理装置５は、認証成功の結果を受信した場合には、例えば、暗号化されているファイルを復号するためのキーを端末１２に送信する。端末１２は、受信したキーを用いてファイルを復号する。よって、端末１２のユーザは、ファイルを参照できる状況になる。なお、端末１２に搭載されているファイル管理用プログラムは、ファイルを復号したら、ファイル権限管理装置５から受信したキーを、端末１２から消滅させる。例えば、再現不能になるように消去する。また、ファイル権限管理装置５は、認証失敗の結果を受信した場合には、ファイルを復号するためのキーを端末１２に送信しない。以上のような処理によって、端末記憶部１１Ａに格納されているファイルを、動的組織Ｓに所属していない者に参照させないようにすることができる。

【０１１０】

一般的なファイル管理システムでは、ファイル権限管理装置が、例えば、暗号化したファイルに、ファイルの参照を許可するメンバを列挙したファイル権限情報を付随させる。そのようなファイル権限管理装置を動的組織における管理に適用した場合には、動的組織のメンバが追加されたり削除されたりすると、ファイル権限情報を更新する必要がある。ファイル権限情報の更新がなされないと、動的組織から抜けたメンバがファイルを参照できてしまう。すなわち、ファイルの内容が、動的組織外に漏洩してしまう。

【０１１１】

ところが、この実施例では、動的組織管理装置２において動的組織Ｓのメンバが追加されたり削除されたりするので、ファイル権限管理装置５は、メンバの追加・削除を意識することなく、ファイル権限管理を行うことができる。そして、動的組織管理装置２が動的組織認証を実行してメンバの信頼性を証明するので、ファイルの内容が動的組織外に漏洩してしまうことは防止される。

【０１１２】

次に、本発明の第４の実施例を、図面を参照して説明する。図１７は、第４の実施例の動的組織管理システムの構成を示すブロック図である。図１７に示す構成では、図１に示

された構成に加えて、ネットワーク管理装置６が追加されている。ネットワーク管理装置６は、端末１１，１２に対して、物理的には通信回線４を用いるＶＰＮ（Virtual Private Network ）による通信の実行許可を与える管理装置である。

【０１１３】

また、端末１１，１２において、通信手段１１Ｂ，１２Ｂが明示されている。通信手段１１Ｂ，１２Ｂは、通信回線４を介して他の装置との間の送受信を実現するためのハードウェアとソフトウェアとを含む。また、通信手段１１Ｂ，１２Ｂには、ＶＰＮを介する通信（ＶＰＮ通信）を実現するための通信プロトコルに従って通信を実行するソフトウェアも実装されている。なお、第４の実施例において、図９に示された動的組織管理装置２０を用いてもよい。また、ネットワーク管理装置６は、例えばＰＰＴＰ（Point to Point Tunneling Protocol ）サーバなどのサーバ装置で実現される。

【０１１４】

既に説明したような処理によって、動的組織Ｓが生成されているとする。また、動的組織Ｓのメンバ間でのみ通信を行うことが可能なＶＰＮが定義されているとする。動的組織Ｓに属するメンバｓが、端末１１を用いてＶＰＮ通信を行うことができる環境に参加することを意図した場合には、端末１１からネットワーク管理装置６に、ＶＰＮ通信の許可を求める要求を送信する。ネットワーク管理装置６は、ＶＰＮ通信の許可を求める要求を受信すると、要求を出した端末１１に対して、動的組織認証を受けるべきであることを指示する情報を送信する。

【０１１５】

端末１１は、動的組織認証を受けるべきであることを指示する情報を受信すると、図７に示された処理を経て、動的組織管理装置２における動的組織認証手段２１２ａから、認証成功または認証失敗の結果の返送を受ける。端末１１は、その結果を、ネットワーク管理装置６に送信する。すると、ネットワーク管理装置６は、端末１１に対して、ＶＰＮ通信を実行するために必要な情報を端末１１に送信することによって、端末１１に、ＶＰＮ通信を行うことができる環境に参加することを許可する。例えば、端末１１が実際にＶＰＮ通信を開始する際の、端末１１を使用するメンバｓのログイン操作にもとづくユーザ認証の結果を、認証成功とする。

【０１１６】

複数の静的組織をまたがって構築された動的組織のメンバがメンバ間でセキュアな通信を行うために、ＶＰＮを利用することが得策である。一般的なＶＰＮ通信システムでは、ＶＰＮ管理サーバなどのネットワーク管理装置が、例えば、ＶＰＮ通信が許可されているメンバを列挙したリストを保持し、そのリストを管理する。すなわち、要求者が端末からＶＰＮ通信の許可の要求を送信すると、ネットワーク管理装置が、許可を要求した要求者がリストに掲載されていれば、要求を出した端末をＶＰＮ通信可能な状態に設定する。そのようなットワーク管理装置を動的組織における管理に適用した場合には、動的組織のメンバが追加されたり削除されたりすると、リストを更新する必要がある。リストの更新がなされないと、動的組織から抜けたメンバがＶＰＮ通信を実行できてしまう。すなわち、ＶＰＮ通信のセキュリティが損なわれてしまう。

【０１１７】

ところが、この実施例では、動的組織管理装置２において動的組織Ｓのメンバが追加されたり削除されたりするので、ネットワーク管理装置６は、メンバの追加・削除を意識することなく、ＶＰＮ通信管理を行うことができる。そして、動的組織管理装置２が動的組織認証を実行してメンバの信頼性を証明するので、参加資格のない者がＶＰＮ通信に参加してしまうことは防止される。

【図面の簡単な説明】

【０１１８】

【図１】本発明の第１の実施の形態の構成を示すブロック図である。

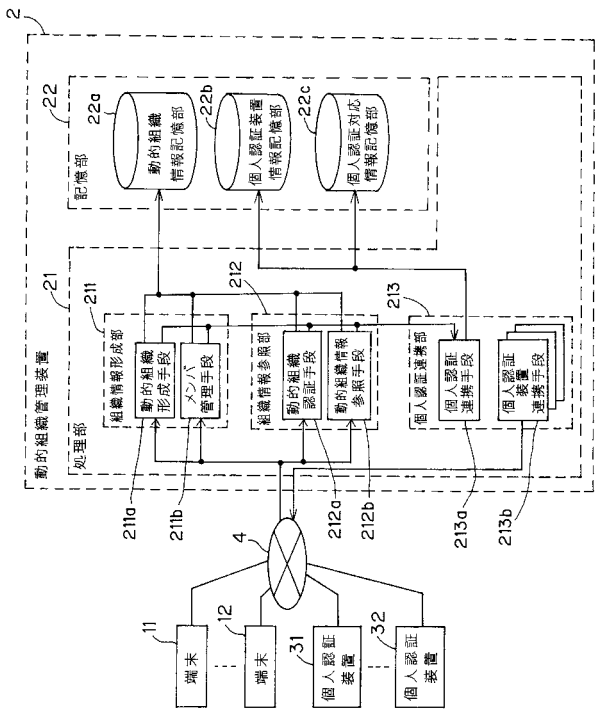
【図２】第１の実施の形態におけるメンバ認証の処理を示すフローチャートである。

【図３】第１の実施の形態における動的組織作成の処理を示すフローチャートである。

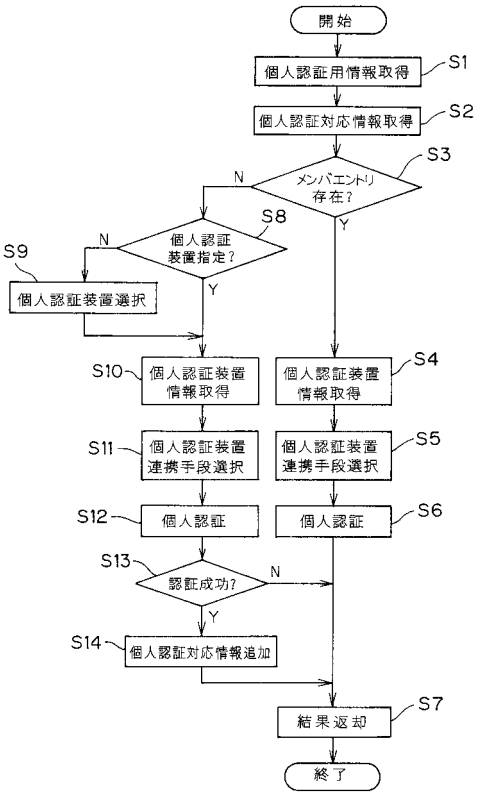
【図４】第１の実施の形態における動的組織削除の処理を示すフローチャートである。
【図５】第１の実施の形態における所属メンバ追加の処理を示すフローチャートである。
【図６】第１の実施の形態における所属メンバ削除の処理を示すフローチャートである。
【図７】第１の実施の形態における動的組織認証の処理を示すフローチャートである。
【図８】第１の実施の形態における動的組織情報参照の処理を示すフローチャートである。
【図９】本発明の第２の実施の形態の構成を示すブロック図である。
【図１０】第２の実施の形態の動作を示すフローチャートである。
【図１１】第１の実施例における個人認証装置情報記憶部に記憶されている個人認証装置の情報の一例を示す説明図である。
【図１２】第１の実施例における個人認証対応情報記憶部に記憶される情報の一例を示す説明図である。
【図１３】第１の実施例における動的組織情報記憶部に記憶される情報（動的組織作成時）の一例を示す説明図である。
【図１４】第１の実施例における動的組織情報記憶部に記憶される情報（所属メンバ追加時）の一例を示す説明図である。
【図１５】第２の実施例における権限情報記憶部に記憶される情報の一例を示す説明図である。
【図１６】第３の実施例の動的組織管理システムの構成を示すブロック図である。
【図１７】第４の実施例の動的組織管理システムの構成を示すブロック図である。
【図１８】木構造で管理される組織の例を表す図である。
【図１９】コミュニティの例を表す図である。
【符号の説明】
【０１１９】

１１，１２	端末
２	動的組織管理装置
３１，３２	個人認証装置
４	通信回線
５	ファイル権限管理装置
６	ネットワーク管理装置
２１	処理部
２２	記憶部
２２ａ	動的組織情報記憶部
２２ｂ	個人認証装置情報記憶部
２２ｃ	個人認証対応情報記憶部
２２ｄ	権限情報記憶部
２１１	組織情報形成部
２１１ａ	動的組織形成手段
２１１ｂ	メンバ管理手段
２１２	組織情報参照部
２１２ａ	動的組織認証手段
２１２ｂ	動的組織情報参照手段
２１３	個人認証連携部
２１３ａ	個人認証連携手段
２１３ｂ	個人認証装置連携手段
２１４	権限管理部
２１４ａ	権限確認手段
２１４ｂ	権限設定手段

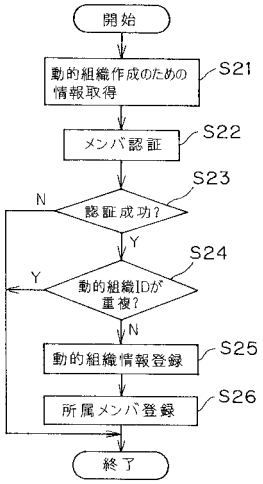
【図１】


2
22
22a
動的組織情報記憶部
22b
個人認証装置情報記憶部
22c
個人認証対応情報記憶部
記憶部
21
211
212
213
動的組織管理装置
処理部
組織情報形成部
動的組織形成手段
メンバ管理手段
組織情報参照部
動的組織認証手段
動的組織情報参照手段
個人認証連携部
個人認証連携手段
個人認証装置連携手段
211a
211b
212a
212b
213a
213b
4
11
端末
12
端末
31
個人認証装置
32
個人認証装置

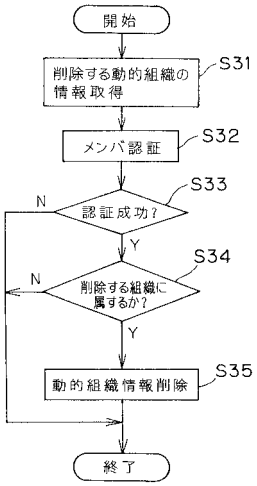
【図２】


開始
個人認証用情報取得
S1
個人認証対応情報取得
S2
メンバエントリ存在？
S3
N
Y
個人認証装置指定？
S8
N
Y
S9
個人認証装置選択
S10
個人認証装置情報取得
S4
個人認証装置情報取得
S11
個人認証装置連携手段選択
S5
個人認証装置連携手段選択
S12
個人認証
S6
個人認証
S13
認証成功？
N
Y
S14
個人認証対応情報追加
S7
結果返却
終了

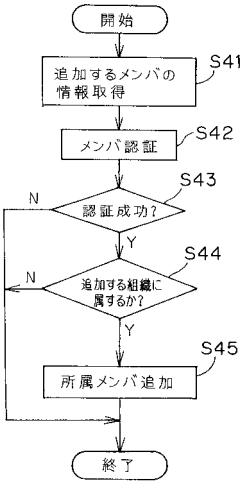
【図３】


開始
動的組織作成のための情報取得
S21
メンバ認証
S22
認証成功？
S23
N
Y
動的組織IDが重複？
S24
Y
N
動的組織情報登録
S25
所属メンバ登録
S26
終了

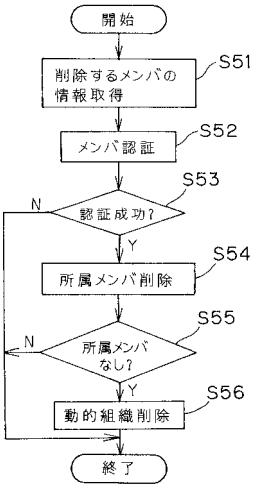
【図４】


開始
削除する動的組織の情報取得
S31
メンバ認証
S32
認証成功？
S33
N
Y
削除する組織に属するか？
S34
N
Y
動的組織情報削除
S35
終了

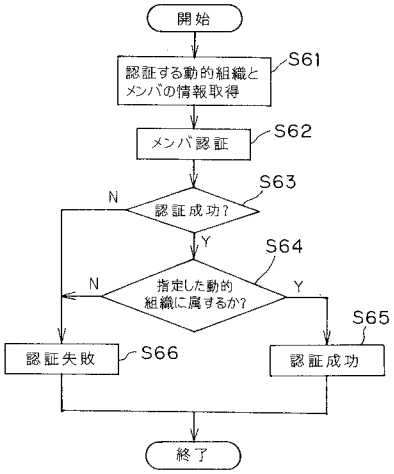
【図５】


開始
追加するメンバの情報取得
S41
メンバ認証
S42
認証成功?
S43
N
Y
追加する組織に属するか?
S44
N
Y
所属メンバ追加
S45
終了

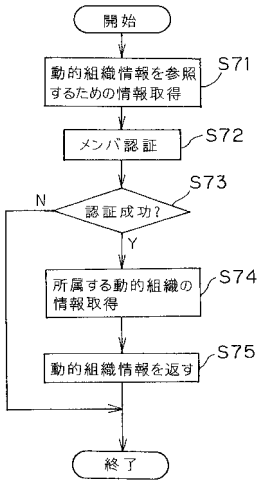
【図６】


開始
削除するメンバの情報取得
S51
メンバ認証
S52
認証成功?
S53
N
Y
所属メンバ削除
S54
所属メンバなし?
S55
N
Y
動的組織削除
S56
終了

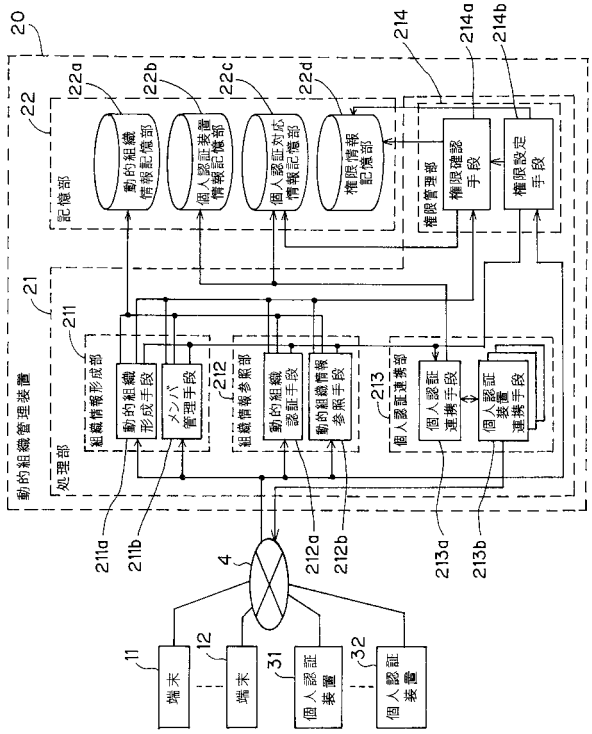
【図７】


開始
認証する動的組織とメンバの情報取得
S61
メンバ認証
S62
認証成功?
S63
N
Y
指定した動的組織に属するか?
S64
N
Y
S65
認証失敗
S66
認証成功
終了

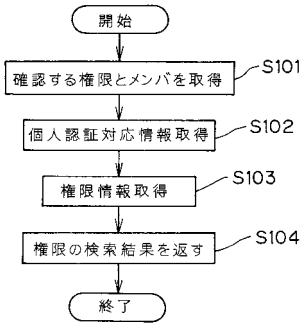
【図８】


開始
動的組織情報を参照するための情報取得
S71
メンバ認証
S72
認証成功?
S73
N
Y
所属する動的組織の情報取得
S74
動的組織情報を返す
S75
終了

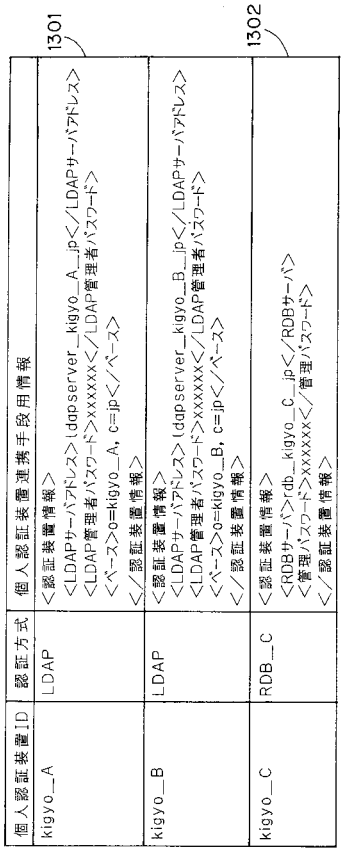
【図９】



【図１０】



【図１１】



【図１２】

個人認証ID	個人認証装置ID
yamada taro	kigyo_A
suzuki hanako	kigyo_B
sato jiro	kigyo_C
hayashi saburo	kigyo_A

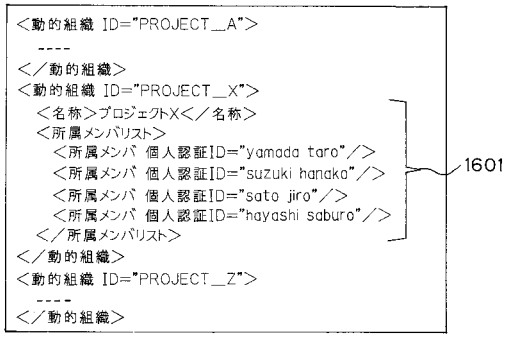
1401
1402

【図１３】

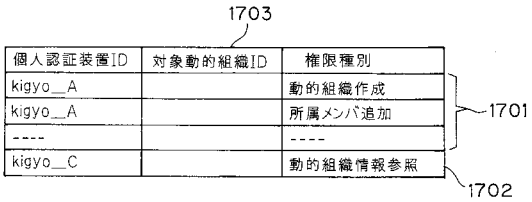
```
<動的組織 ID="PROJECT_A">
  ----
</動的組織>
<動的組織 ID="PROJECT_X">
  <名称>プロジェクトX</名称>
  <所属メンバリスト>
    <所属メンバ 個人認証ID="yamada taro"/>
  </所属メンバリスト>
</動的組織>
<動的組織 ID="PROJECT_Z">
  ----
</動的組織>
```

1501

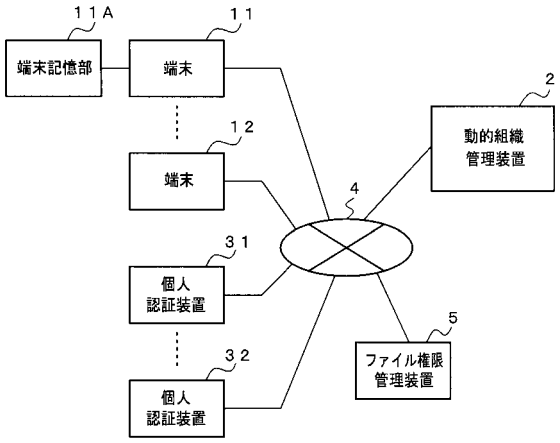
【図１４】



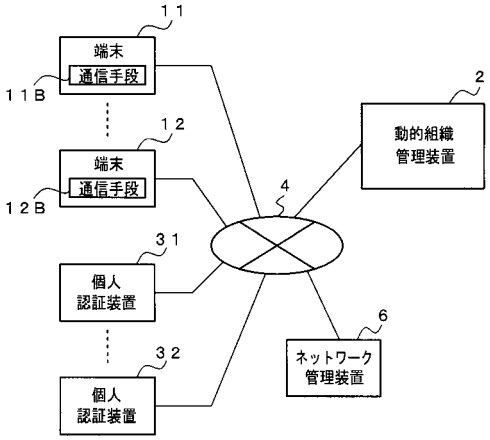
【図１５】



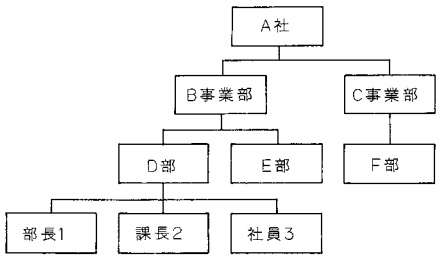
【図１６】



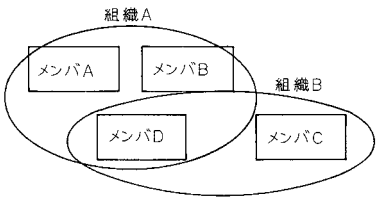
【図１７】



【図１８】



【図１９】



フロントページの続き

(72)発明者　延藤　里奈
東京都港区芝五丁目７番１号　日本電気株式会社内

Ｆターム(参考) 5B085 AE02　AE03　AE23　BA06　BG07