

(19) 世界知的所有権機関  
国際事務局



(43) 国際公開日  
2006 年 6 月 8 日 (08.06.2006)

PCT

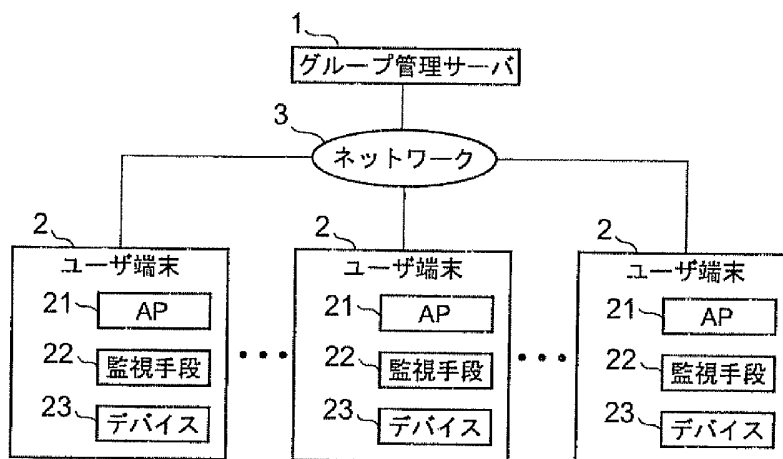
(10) 国際公開番号  
WO 2006/059639 A1

- (51) 国際特許分類:  
G06F 21/24 (2006.01) G06F 12/00 (2006.01)
- (21) 国際出願番号: PCT/JP2005/021982
- (22) 国際出願日: 2005 年 11 月 30 日 (30.11.2005)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:  
特願 2004-346703  
2004 年 11 月 30 日 (30.11.2004) JP
- (71) 出願人 (米国を除く全ての指定国について): 日本電気株式会社 (NEC CORPORATION) [JP/JP]; 〒1080014 東京都港区芝五丁目 7 番 1 号 Tokyo (JP).
- (72) 発明者; および
- (75) 発明者/出願人 (米国についてのみ): 中江 政行 (NAKAE, Masayuki) [JP/JP]; 〒1080014 東京都港区芝五丁目 7 番 1 号 日本電気株式会社内 Tokyo (JP).
- (74) 代理人: 山下 穰平 (YAMASHITA, Johei); 〒1050001 東京都港区虎ノ門五丁目 1 3 番 1 号 虎ノ門 4 O M T ビル 山下国際特許事務所 Tokyo (JP).
- (81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.
- (84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR),

[続葉有]

(54) Title: INFORMATION SHARING SYSTEM, INFORMATION SHARING METHOD, GROUP MANAGEMENT PROGRAM, AND COMPARTMENT MANAGEMENT PROGRAM

(54) 発明の名称: 情報共有システム、情報共有方法、グループ管理プログラム及びコンパートメント管理プログラム



- 1.. GROUP MANAGEMENT SERVER  
3.. NETWORK  
2.. USER TERMINAL  
22.. MONITORING MEANS  
23.. DEVICE

(57) Abstract: An information sharing system manages calculation resources such as a file and a process by virtually allocating them to a compartment as a unique area identified by a group ID. When the information sharing system detects an object file input event by using the compartment, it allows reference of only files belonging to the same compartment or the compartment of a lower node. Moreover, when the information sharing system detects an object file output event, it arranges a file only in the same compartment. Thus, it is possible to share confidential information in a group of users existing at remote places and share normal wide information.

[続葉有]



OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML,  
MR, NE, SN, TD, TG).

添付公開書類:

— 国際調査報告書

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

---

(57) 要約: 情報共有システムは、ファイルやプロセス等の計算資源を、グループIDで識別される固有領域としてのコンパートメントに仮想的に割り当てて管理する。このコンパートメントを用いて、情報共有システムは、オブジェクトのファイル入力イベントを検出すると、同一コンパートメントもしくは下位のコンパートメントに属するファイル参照のみを許可する。また、この情報共有システムは、オブジェクトのファイル出力イベントを検出すると、同一コンパートメント内のみファイルに配置させる。こうすることで、遠隔地に離れて存在するユーザグループ内部での適切な機密情報の共有と通常の広範な情報共有とを両立できるようにする。

## 明 細 書

### 情報共有システム、情報共有方法、グループ管理プログラム及びコンパートメント管理プログラム

#### 技術分野

[0001] 本発明は、グループ内で情報を共有するための情報共有システム及び情報共有方法に関し、特に機密漏洩を防止しながら遠隔地間でのグループ情報共有を可能とする情報共有システム及び情報共有方法に関する。また、本発明は、情報共有システムのサーバ及びユーザ端末に関する。また、本発明は、情報共有システムのサーバが搭載するグループ管理プログラム、及びユーザ端末が搭載するコンパートメント管理プログラムに関する。

#### 背景技術

[0002] 従来、複数の機密レベルをもつコンテンツの編集や参照を認めながら、機密漏洩を防止できるシステムとして、マルチレベルセキュリティ(MLS)システムと呼ばれるシステムがある。

[0003] 例えば、特許文献1には、MLSシステムを用いた方式として、ファイルシステムのアクセス権管理制御方式が記載されている。これによれば、「アクセス権番号」と呼ばれる2段階以上の機密レベルを扱うアクセス制御方式が示されている。この方式では、サブジェクトとなりえるのはユーザだけであり、オブジェクトはデータベースのテーブル又はファイルシステム上のファイルである。また、サブジェクトとオブジェクトとの両者には予めアクセス権番号が割り当てられている。そして、あるユーザがあるファイルをアクセスしようとする時、ユーザのアクセス権番号がファイルのアクセス権番号以下である場合そのアクセスを許可し、ユーザのアクセス権番号がファイルのアクセス権番号以下でない場合そのアクセスを拒否する。

[0004] また、特許文献2には、MLSシステムを用いた方法として、安全なデータ転送を行うための方法及び機密レベル変更選択機構が記載されている。これによれば、各ウィンドウが機密レベルをもつようなXウィンドウシステムにおけるMLSベースのコピー&ペースト制御方式が示されている。MLSベースのコピー&ペースト制御とは、通常レ

ベルのウィンドウから機密レベルのウィンドウへのコピー&ペーストを認めるが、その逆に機密レベルから通常レベルのウィンドウへのコピー&ペーストを認めないか、ペースト先を機密レベルに昇格させるようにする制御である。また、特許文献2では、独自拡張されたXサーバを用いて、コピー&ペーストのためのあらゆるウィンドウ間通信を所定の「選択マネージャ」で中継し、機密レベルに基づくペースト制御を一括管理する実装方式が示されている。

[0005] また、特許文献3には、MLSシステムを用いた情報処理装置が記載されている。この情報処理装置は、オペレーティングシステム(OS)を用いて2次元の機密レベルをもつMLSをサポートしている。この2次元の機密レベルは、アクセス権レベル $l$ とアクセス権範囲 $n$ との組 $(l, n)$ で表される。アクセス権レベル $l$ は大小比較ができる値であり、アクセス権範囲 $n$ は同値関係だけが定義された文字列である。そして、任意のプロセスとファイルには、予め組 $(l, n)$ の形式の機密レベルが設定されている。例えば、機密レベル $(Pl, Pn)$ のプロセスが、機密レベル $(Fl, Fn)$ のファイルにアクセスしようとした場合を考える。この場合、情報処理装置は、「 $Pl \geq Fl$ 」且つ「 $Pn = Fn$ 」という関係が満たされた場合のみ、該プロセスから該ファイルへのアクセスを認める。

[0006] 上記の機密レベルのうち、アクセス権レベルは、例えば「機密」又は「通常」を示す値と考えてよい。一方、アクセス権範囲は、互いに性格が異なる情報のカテゴリと捉えられる。特許文献3に記載された情報処理装置では、これらアクセス権レベル及びアクセス権範囲を組み合わせた2次元の機密レベルを用いている。こうすることで、例えば、機密レベルのアクセス権範囲として「個人情報」及び「技術情報」という2つの情報カテゴリを扱う場合、それぞれの情報カテゴリ毎に独立した機密情報を管理することができる。例えば、機密レベルのアクセス権範囲が「個人情報」の情報カテゴリに該当するファイルにアクセス可能なプロセスがあったとしても、そのプロセスは機密レベルのアクセス権範囲が「技術情報」の情報カテゴリに該当するファイルに一切アクセスできない。

[0007] 特許文献1:特開平5-181734号公報(段落0028-0030、図8)

特許文献2:特開平8-255132号公報(段落0020-0024、図1、図4)

特許文献3:特開2001-350663号公報(段落0039-0047、図1、図7)

## 発明の開示

### 発明が解決しようとする課題

- [0008] 前述したMLSシステムを用いた従来例の機密保護技術では、いずれも機密保護が各ユーザ端末内のファイル操作に限定されており、遠隔地にあるユーザ端末への機密送信等を制御することはできない。そのため、ネットワークを介して遠隔地間で情報共有を行う場合に、グループ内の機密情報の確実な保護を行うことは困難である。
- [0009] また、従来例の機密保護技術では、いずれもグループ間の包含関係と各情報の機密レベル設定との関係を同期させることができない。そのため、複数グループが存在する場合に、グループ内部で閉じた情報共有を行うことに加えて、より広範なグループとその部分グループとの間での自由な情報共有を実現しながら、無関係なグループ(例えば社外)への機密漏洩を防止することは困難である。例えば、ある企業全体で共有される情報を参照しながら、各部門で限定的に共有される情報を取り扱うことはできない。
- [0010] 以上説明したように、MLSシステムを用いた従来例では、いずれも1つのユーザ端末内におけるアプリケーション(AP)によるファイル操作を制御するに留まっている。このため、遠隔地に離れて存在する複数のユーザ端末間でコンテンツへのアクセスを一貫して制御することはできない。また、ユーザのグループが複数存在するときに、グループ内部あるいはグループ間での情報共有を行っている。このために、機密レベル設定等のコンテンツアクセス制御設定を一貫して行うことはできない。
- [0011] そこで、本発明は、ネットワークを介して遠隔地間で情報共有を行う場合に、グループ内の機密情報の確実な保護を行えることを目的とする。
- [0012] また、本発明は、複数のグループが存在する場合に、グループ内部で閉じた情報共有を行うことに加えて、より広範なグループとその部分グループとの間での自由な情報共有を実現しながら、無関係なグループへの機密漏洩を防止することを目的とする。

### 課題を解決するための手段

- [0013] 上記目的を達成するため、本発明による情報共有システムは、グループ内で情報

を共有するためのコンピュータを用いた情報共有システムであって、前記グループと当該グループに属するメンバとの対応関係を管理し、前記メンバを識別するためのメンバ識別情報を入力すると、少なくとも1以上の前記グループを識別するためのグループ識別情報を出力するグループ管理手段と、前記グループ識別情報に基づいて、前記コンピュータ内のソフトウェア及びファイルを含む計算資源を前記グループに対応付けて割り当てるための仮想的に区画化されたグループ専用領域であり且つ前記グループ間で互いの関係が解析可能に構成されたコンパートメントを生成するコンパートメント生成手段と、前記計算資源にアクセスするアプリケーションソフトウェアの動作を監視して、前記コンパートメントと前記アプリケーションソフトウェアとの所属関係を解析し、その解析結果に基づいて前記アプリケーションソフトウェアと前記計算資源との間の入出力処理の実行可否を制御する監視手段とを有することを特徴とする。

前記グループ管理手段は、例えば、グループ管理サーバの制御部及びグループ管理データベースによって実現される。前記計算資源は、例えば、ファイルやプロセス、ネットワークである。前記コンパートメント生成手段は、例えば、コンパートメント生成指示手段の指示に従って動作するコンパートメント構成管理手段によって実現される。前記メンバ識別情報は、例えば、メンバIDである。前記グループ識別情報は、例えば、グループID及び認証キーである。監視手段は、例えば、同一コンパートメント内の任意のアプリケーションソフトウェア間での入出力処理を許可し、且つ異なるコンパートメントへの入出力処理を禁止する。

[0014] また、好適な実施態様として、前記グループ管理手段は、サーバに設けられ、前記コンパートメント生成手段及び前記監視手段は、前記サーバに通信ネットワークを介して通信可能に接続されるユーザ端末に設けられる。この構成で、前記グループ管理手段は、前記グループを識別するためのグループ識別情報と、前記メンバを識別するためのメンバ識別情報とを対応付けて蓄積し、前記ユーザ端末から前記メンバ識別情報を受信すると、受信した前記メンバ識別情報に対応するグループ識別情報を抽出し、抽出した前記グループ識別情報を、前記通信ネットワークを介して前記ユーザ端末に送信する。前記コンパートメント生成手段は、前記グループ管理手段から

受信した前記グループ識別情報に基づいて前記コンパートメントを生成する。前記監視手段は、前記ユーザ端末が搭載するアプリケーションソフトウェアの動作を監視して、前記アプリケーションソフトウェアのイベントを検出し、前記イベントを検出したアプリケーションソフトウェアが属する前記コンパートメントを特定し、特定した前記コンパートメントに基づいて前記アプリケーションソフトウェアと前記計算資源との間の前記イベントに応じた入出力処理の実行可否を制御する。前記サーバは、例えば、グループ管理サーバで構成される。

[0015] 上記の構成において、前記情報共有システムは、通信ネットワークを介して相互に接続された各ユーザ端末に、アプリケーションソフトウェアによる新たな他のアプリケーションソフトウェアの起動、又はファイル入出力やネットワークアクセス等のデバイスに対する操作に関するアプリケーション動作イベントを監視するようにしてもよい。

[0016] また、好適な実施態様として、前記情報共有システムは、機密を有するユーザグループとそのメンバ構成とを管理するサーバを備え、同一グループに属するメンバのユーザ端末の監視手段に、前記グループ識別情報としてグループID及び認証キーの系列(グループID／認証キー系列)を予め配布する。グループID／認証キー系列の配布を受けた監視手段は、アプリケーションソフトウェアやファイル、ネットワーク等の計算資源の割り当て先として、グループIDで識別される固有領域であるコンパートメントを仮想的に生成する。監視手段は、各コンパートメントについて機密レベルに関する半順序関係を管理しており、アプリケーション動作を監視しながら、以下のような規則に基づいてアプリケーションソフトウェアによる計算資源へのアクセスを制御する。

[0017] (1)コンパートメントAに属するアプリケーションソフトウェアは、同一のコンパートメントAに属する計算資源に読み込みや書き込みのアクセスをできる。(2)コンパートメントAが他のコンパートメントBよりも上位の機密レベルを有している場合、コンパートメントAに属するアプリケーションソフトウェアは、コンパートメントBに属する計算資源に読み込みのアクセスのみできる。(3)コンパートメントAが他のコンパートメントCよりも下位の機密レベルを有している場合、コンパートメントAに属するアプリケーションソフトウェアは、コンパートメントCに属する計算資源に書き込みのアクセスのみできる。(4

)上位／下位の関係が成り立たない各コンパートメントに属する計算資源については、一切のアクセスを禁止する。

- [0018] 上記(1)～(4)までの規則に従ってアクセス制御を行うために、各ユーザ端末の監視手段は、アプリケーションソフトウェアの起動イベントを検出する度に、アプリケーションソフトウェアのプロセスもしくはウィンドウ等のオブジェクトを適切なコンパートメントに割り当てる。そして、監視手段は、オブジェクトのファイル読込イベントに対して、同一コンパートメントもしくは同一コンパートメントよりも下位のコンパートメントに属するファイル参照のみを許可する。また、監視手段は、オブジェクトのファイル書込イベントに対しては、同一コンパートメント内のみにファイルを配置させる。
- [0019] 上記のようにすることによって、複数のグループに所属するユーザが同時にグループ内の機密情報を参照又は編集する際に、特定グループの機密情報が他のグループに漏洩することを防止できる。また、下位のコンパートメントにあるより広範な共有が認められたファイルが、より限定的な共有を意味する上位コンパートメントに配置された場合にも、下位コンパートメントにあるファイルを保存できる。そのため、ユーザが意図しない共有範囲の縮小を引き起こすことなく、自由な情報共有を行うことができる。
- [0020] さらに、あるユーザ端末の監視手段が、特定のコンパートメントに属するアプリケーションソフトウェアから他のユーザ端末のアプリケーションソフトウェアに対するネットワーク接続イベントを検出した際に、アプリケーションソフトウェア同士の通信処理を行う前に、双方の端末の監視手段同士で関係する2つのアプリケーションソフトウェアが特定コンパートメントに確かに属していることを認証キーを用いて相互認証した後、アプリケーションソフトウェア同士の通信処理を開始する。そのようにすることによって、遠隔地に離れて存在する同一グループのメンバ同士が、機密情報を安全に共有することができる。
- [0021] また、グループ管理手段は、メンバ識別情報に基づいて、少なくとも1以上のグループIDと認証キーとの組をグループ識別情報として出力するものであってもよい。
- [0022] また、監視手段は、コンパートメントとアプリケーションソフトウェアとの所属関係に基づいて、少なくともファイル入出力イベント又はネットワーク入出力イベントの実行可否を制御するものであってもよい。そのような構成によれば、アプリケーションソフトウ

ェア間のファイルの入出力処理の可否を制御することができる。また、通信ネットワークを介したデータの送受信の可否を制御することができる。

- [0023] また、コンパートメント生成手段は、グループ識別情報に基づいて、所定の構成情報を生成することによってコンパートメントを生成するものであってもよい。そのような構成によれば、所定の構成情報を生成することによって、コンパートメントを仮想的に生成することができる。所定の構成情報は、例えば、データ構造のグラフの要素であるノードを構成するコンパートメントノードと、その属性としてのオブジェクトツリー及びファイル配置テーブルを有している。オブジェクトツリーは、アプリケーションソフトウェアに対応するオブジェクトのツリー構造を示すものである。ファイル配置テーブルは、ファイルがどの場所に格納されているかの情報を示すものである。
- [0024] また、グループ管理手段は、グループとグループとは別のグループとの包含関係を示す隣接行列を生成する手段を含み、コンパートメント生成手段は、生成した隣接行列に基づいて、生成したコンパートメント間に有向辺を付加することによって、コンパートメント間の順序関係を設定する手段を含むものであってもよい。
- [0025] 上記の構成によれば、情報共有システムは、グループ管理サーバにグループ変更手段を備え、任意グループのメンバ構成の変更を管理させてもよい。また、情報共有システムは、グループ関係計算手段を備え、ユーザ端末からグループID／認証キー系列の要求を受ける度に、グループ管理データベースを参照してグループID／認証キー系列を生成してもよい。また、グループ関係計算手段は、そのグループ間の包含関係を示す隣接行列を生成して、要求元ユーザ端末に応答してもよい。
- [0026] ユーザ端末は、グループID／認証キー系列と隣接行列とを受け取ると、コンパートメント再編手段を用いて、各グループIDに対応するコンパートメントを作成してもよい。また、ユーザ端末は、隣接行列を参照して、より部分的なグループのコンパートメントの機密レベルが、そのコンパートメントを含むより広範なグループのコンパートメントの機密レベルよりも必ず高くなるように、機密レベルを設定してもよい。
- [0027] 上記のようにすることによって、グループ内部で閉じた情報共有に加えて、より広範なグループとその部分グループ間での自由な情報共有を実現しながら、無関係なグループ(例えば社外)への機密漏洩を防止できる。例えば、ある企業全体で共有され

る情報を参照しながら、各部門で限定的に共有される情報を取り扱うことができる。

[0028] また、監視手段は、コンパートメントとアプリケーションソフトウェアとの所属関係を示すデータ構造のグラフとして、ノードとそのノードを結ぶ辺から成るコンパートメント構成グラフを管理するコンパートメント構成グラフ管理手段を含むものであってもよい。この手段は、例えば、コンパートメント構成管理手段によって実現される。なお、「コンパートメント構成グラフ」を管理するとは、例えば、コンパートメント構成グラフを保持し、アプリケーションソフトウェアのイベント検出等に応じてコンパートメント構成グラフを更新することをいう。

[0029] また、監視手段は、コンパートメント構成グラフに基づいて、アプリケーションソフトウェアがアクセスできるファイルの範囲を、アプリケーションソフトウェアが属するコンパートメントと、コンパートメントの下位コンパートメントとのいずれかに属するファイルに限定するファイルアクセス制御手段を含むものであってもよい。この手段は、例えば、コンパートメント構成管理手段によって実現される。そのような構成によれば、アプリケーションソフトウェアがファイルにアクセスする場合に、無関係なグループへの情報漏洩を防止することができる。

[0030] また、監視手段は、コンパートメント構成グラフに基づいて、アプリケーションソフトウェアが同一のホストコンピュータ内でメッセージを送信できる範囲を、アプリケーションソフトウェアが属するコンパートメントと、コンパートメントの下位コンパートメントのいずれかに属するアプリケーションソフトウェアとに限定するメッセージング制御手段を含むものであってもよい。この手段は、例えば、コンパートメント構成管理手段によって実現される。そのような構成によれば、アプリケーションソフトウェアが同一ホスト内でメッセージ送信する場合に、無関係なグループへの情報漏洩を防止することができる。

[0031] また、監視手段は、コンパートメント構成グラフに基づいて、アプリケーションソフトウェアが同一のホストコンピュータ内、又はネットワークを介して接続されるホストコンピュータとは別のホストコンピュータにメッセージを送信できる範囲を、同一のコンパートメントに属するアプリケーションソフトウェアに限定するネットワークアクセス制御手段を含むものであってもよい。この手段は、例えば、コンパートメント構成管理手段によ

って実現される。そのような構成によれば、アプリケーションソフトウェアがネットワークを介してメッセージを送信する場合に、無関係なグループへの情報漏洩を防止することができる。

[0032] また、監視手段は、ユーザからの指示に応じて、アプリケーションソフトウェアが属するコンパートメントの変更、又はコンパートメントごとのファイル管理を行うコンパートメント管理手段を含むものであってもよい。コンパートメント管理手段は、例えば、コンパートメント再編指示手段の指示に従って動作するコンパートメント構成管理手段によって実現される。そのような構成によれば、グループの変更等に伴ってコンパートメントを更新することができる。

[0033] また、グループ管理手段は、グループの新規作成、グループの抹消、メンバの追加、又はメンバの削除を行うグループ変更手段を含むものであってもよい。

[0034] 本発明による情報共有システムのサーバは、グループ内で情報を共有するための情報共有システムにおける、グループとグループに属するメンバとの対応関係を管理するサーバ(例えば、グループ管理サーバ)であって、メンバを識別するためのメンバ識別情報を入力すると、少なくとも1以上のグループIDと認証キーとの組を出力するグループ管理手段を備えている。サーバは、例えば、グループ管理サーバで構成される。

[0035] また、情報共有システムのサーバは、グループとグループとは別のグループとの包含関係を示す行列である隣接行列を生成する隣接行列生成手段を備えたものであってもよい。そのような構成によれば、複数のグループが存在する場合に、グループ内部で閉じた情報共有を行うことに加えて、より広範なグループとその部分グループとの間での自由な情報共有を実現しながら、無関係なグループへの機密漏洩を防止することができる。

[0036] 本発明による情報共有システムのユーザ端末は、グループ内で情報を共有するための情報共有システムにおけるユーザ端末であって、前記グループを識別するグループIDと認証キーとの各組に対応して、当該ユーザ端末を構成するコンピュータ内のソフトウェア及びファイルを含む計算資源をグループに対応付けて割り当てるための仮想的に区画化されたグループ固有領域であり且つ前記グループ間で互いの関

係が解析可能に構成された区画であるコンパートメントを生成するコンパートメント生成手段と、アプリケーションソフトウェアの動作を監視し、各コンパートメントとアプリケーションソフトウェアとの所属関係に基づいて、ファイル入出力イベント及びネットワーク入出力イベントの少なくとも一方の実行可否を制御する監視手段とを備える。

[0037] また、情報共有システムのユーザ端末は、グループとグループとは別のグループとの包含関係を示す行列である隣接行列を生成する隣接行列生成手段と、隣接行列生成手段が生成した隣接行列に基づいて、コンパートメント生成手段が生成したコンパートメント間に有向辺を付加することによって、コンパートメント間の順序関係を設定する有向辺付加手段とを備えたものであってもよい。そのような構成によれば、複数のグループが存在する場合に、グループ内部で閉じた情報共有を行うことに加えて、より広範なグループとその部分グループとの間での自由な情報共有を実現しながら、無関係なグループへの機密漏洩を防止することができる。

[0038] 本発明による情報共有方法は、サーバと、このサーバに通信ネットワークを介して通信可能に接続されたユーザ端末とを備えた情報共有システムを用いて、グループ内で情報を共有するものであって、前記サーバが、グループとグループに属するメンバとの対応関係を管理し、メンバを識別するためのメンバ識別情報を入力すると、少なくとも1以上のグループIDと認証キーとの組を、通信ネットワークを介してユーザ端末に送信するステップと、前記ユーザ端末が、サーバから受信したグループIDと認証キーとの各組に対応して、コンピュータ内のソフトウェア及びファイルを含む計算資源を前記グループに対応付けて割り当てるための仮想的に区画化されたグループ専用領域であり且つ前記グループ間で互いの関係が解析可能に構成されたコンパートメントを生成するステップと、前記ユーザ端末が、少なくともコンパートメント間の順序関係、コンパートメントとアプリケーションソフトウェアとの所属関係、又はコンパートメントとファイルとの所属関係の情報を含むデータ構造のグラフとして、ノードとそのノードを結ぶ辺から成るコンパートメント構成グラフとを生成するステップと、前記ユーザ端末が、前記アプリケーションソフトウェアの動作を監視して、前記コンパートメント構成グラフに基づいて、ファイル入出力イベント及びネットワーク入出力イベントの少なくとも一方の実行可否を制御するステップとを含むことを特徴とする。

- [0039] また、情報共有方法は、サーバが、メンバ識別情報を入力すると、グループとグループとは別のグループとの包含関係を示す行列である隣接行列を生成するステップと、サーバが、グループIDと認証キーとの組とともに、生成した隣接行列を、通信ネットワークを介してユーザ端末に送信するステップと、ユーザ端末が、サーバから受信したグループIDと認証キーとの各組及び隣接行列に基づいて前記コンパートメント構成グラフを生成するステップと、ユーザ端末が、アプリケーションソフトウェアの動作を監視して、生成したコンパートメント構成グラフに基づいて、一のグループのコンパートメントに属する情報に対して、グループを包含する他のグループのコンパートメントに属するアプリケーションソフトウェアからの読みこみアクセスを許可するように、アプリケーションソフトウェアの実行可否を制御するステップとを含むものであってもよい。そのような構成によれば、複数のグループが存在する場合に、グループ内部で閉じた情報共有を行うことに加えて、より広範なグループとその部分グループとの間での自由な情報共有を実現しながら、無関係なグループへの機密漏洩を防止することができる。
- [0040] 本発明によるグループ管理プログラムは、グループ内で情報を共有するための情報共有システムで用いるもので、コンピュータに、グループとグループに属するメンバとの対応関係を管理し、メンバを識別するためのメンバ識別情報を入力すると、少なくとも1以上のグループIDと認証キーとの組を生成するグループ管理処理を実行させることを特徴とする。
- [0041] また、グループ管理プログラムは、コンピュータに、グループとグループとは別のグループとの包含関係を示す行列である隣接行列を生成する隣接行列生成処理を実行させるものであってもよい。そのような構成によれば、複数のグループが存在する場合に、グループ内部で閉じた情報共有を行うことに加えて、より広範なグループとその部分グループとの間での自由な情報共有を実現しながら、無関係なグループへの機密漏洩を防止することができる。
- [0042] 本発明によるコンパートメント管理プログラムは、グループ内で情報を共有するための情報共有システムで用いるもので、コンピュータに、計算資源をグループに対応付けて割り当てるための区画であるコンパートメントを管理し、グループIDと認証キーと

の各組に対応して、前記コンピュータ内のソフトウェア及びファイルを含む計算資源を前記グループに対応付けて割り当てるための仮想的に区画化されたグループ専用領域であり且つ前記グループ間で互いの関係が解析可能に構成されたコンパートメントを生成する処理と、コンパートメント間の順序関係、コンパートメントとアプリケーションソフトウェアとの所属関係、及びコンパートメントとファイルとの所属関係の少なくとも1つの情報を含むデータ構造のグラフとして、ノードとそのノードを結ぶ辺から成るコンパートメント構成グラフを生成する処理と、アプリケーションソフトウェアの動作を監視して、コンパートメント構成グラフに基づいて、少なくともファイル入出力イベント又はネットワーク入出力イベントの実行可否を制御するアクセス制御処理とを実行させることを特徴とする。

- [0043] また、コンパートメント管理プログラムは、コンピュータに、コンパートメント生成処理で、グループIDと認証キーとの各組及び隣接行列に基づいて、コンパートメント間の順序関係、コンパートメントとアプリケーションソフトウェアとの所属関係、及びコンパートメントとファイルとの所属関係の少なくとも1つの情報を含むデータ構造のグラフとして、コンパートメント構成グラフを生成する処理を実行させるものであってもよい。そのような構成によれば、複数のグループが存在する場合に、グループ内部で閉じた情報共有を行うことに加えて、より広範なグループとその部分グループとの間での自由な情報共有を実現しながら、無関係なグループへの機密漏洩を防止することができる。

### 発明の効果

- [0044] 本発明によれば、コンピュータ内の計算資源を、メンバが属するグループの専用領域であり且つグループ間で互いの関係が解析可能に構成されたコンパートメントに対応付けて管理するように構成している。このため、ネットワークを介して遠隔地間で情報共有を行う場合に、グループ内の機密情報の確実な保護を行うことができる。また、複数のグループが存在する場合に、グループ内部で閉じた情報共有を行うことに加えて、より広範なグループとその部分グループとの間での自由な情報共有を実現しながら、無関係なグループへの機密漏洩を防止することもできる。

### 図面の簡単な説明

[0045] [図1]本発明による情報共有システムの第1の実施の形態の構成の一例を示すブロック図である。

[図2]第1の実施の形態において、グループ管理サーバ及びユーザ端末の構成の一例を示すブロック図である。

[図3]第1の実施の形態において、ユーザ端末がコンパートメントを生成するコンパートメント生成処理の一例を示す流れ図である。

[図4]第1の実施の形態において、アプリケーションの起動イベントに対しユーザ端末が行う処理の一例を示す流れ図である。

[図5]第1の実施の形態において、コンパートメント構成グラフの一例を示す説明図である。

[図6]第1の実施の形態において、第1アプリケーションから第2アプリケーションにメッセージが送信されたときに監視手段が行う処理の一例を示す流れ図である。

[図7]第1の実施の形態において、マージしたオブジェクトツリーの例を示す説明図である。

[図8]第1の実施の形態において、コンパートメント構成グラフにおけるコンパートメントのファイル配置テーブルの一例を示す説明図である。

[図9]第1の実施の形態において、アプリケーションがファイル一覧を行う際に監視手段が行う処理の一例を示す流れ図である。

[図10]第1の実施の形態において、統合FT(ファイル配置テーブル)の例を示す説明図である。

[図11]第1の実施の形態において、アプリケーションがファイル読み込みを行う際に監視手段が行う処理の一例を示す流れ図である。

[図12]第1の実施の形態において、アプリケーションがファイル書込み等の変更を行う際に監視手段が行う処理の一例を示す流れ図である。

[図13]第1の実施の形態において、ファイル配置テーブルと2次記憶デバイス上のファイル実体との関係を示す説明図である。

[図14]第1の実施の形態において、ネットワークを介して接続された2つのユーザ端末間で通信を行う場合の処理の一例を示す流れ図である。

[図15]第1の実施の形態による情報共有システムを適用した遠隔会議システムの実施例の具体的な構成を示すブロック図である。

[図16]実施例において、グループ管理データベースの例を示す説明図である。

[図17]実施例において、コンパートメントノードN[Group-1]の登録後のコンパートメント構成グラフの例を示す説明図である。

[図18]実施例において、コンパートメントノードN[Group-1]とN[Group-2]との登録後のコンパートメント構成グラフの例を示す説明図である。

[図19]実施例において、ユーザ端末2-1でのアプリケーション実行時のオブジェクトツリーを示す説明図である。

[図20]実施例において、動画配信時の遠隔会議システムの具体的な動作を示す説明図である。

[図21]実施例において、ファイル新規作成時の監視手段の具体的な動作を示す説明図である。

[図22]実施例において、ファイル配置テーブルの一具体例を示す説明図である。

[図23]実施例において、ファイル配置テーブルをマージして生成したファイル配置テーブルの具体例を示す説明図である。

[図24]実施例において、会議クライアントアプリケーションのファイル選択ダイアログの例を示す説明図である。

[図25]実施例において、ファイル読み込み時の監視手段の具体的な動作を示す説明図である。

[図26]実施例において、ファイルアップロード処理を示す説明図である。

[図27]実施例において、ファイルダウンロード処理を示す説明図である。

[図28]実施例において、ユーザ端末2間のファイル交換処理を示す説明図である。

[図29]本発明による情報共有システムの第2の実施の形態において、グループ管理サーバ及びユーザ端末の構成例を示すブロック図である。

[図30]第2の実施の形態において、グループ管理サーバが行うグループ変更処理の一例を示す流れ図である。

[図31]第2の実施の形態において、グループ管理サーバのグループ関係計算手段

がグループ間の関係を計算するグループ関係計算処理の一例を示す流れ図である。

[図32]第2の実施の形態において、グループ関係計算手段が隣接行列を計算して求める隣接行列計算処理の一例を示す流れ図である。

[図33]第2の実施の形態において、コンパートメント再編指示手段がコンパートメントの再編を指示する処理の一例を示す流れ図である。

[図34]第2の実施の形態において、コンパートメントノードのコンパートメント構成グラフへの登録処理の具体例を示す流れ図である。

[図35]第2の実施の形態において、組織の包含関係の例を示す説明図である。

[図36]本発明による情報共有システムの第3の実施の形態において、ユーザ端末の構成例を示すブロック図である。

[図37]第3の実施の形態において、コンパートメント切替手段がコンパートメントの切り替えを行うコンパートメント切替処理の一例を示す流れ図である。

[図38]第3の実施の形態において、ユーザ端末が表示するコンパートメント切替ダイアログの例を示す説明図である。

[図39]第3の実施の形態において、コンパートメント切り替えに伴うコンパートメント構成グラフの変化の例を示す説明図である。

[図40]第3の実施の形態において、ユーザ端末が表示するコンパートメント切替ダイアログの他の例を示す説明図である。

## 符号の説明

- [0046]
- 1 グループ管理サーバ
  - 2 ユーザ端末
  - 3 ネットワーク
  - 4 遠隔会議サーバ
  - 11 通信インタフェース手段
  - 12 グループ管理データベース
  - 13 グループ変更手段
  - 14 グループ関係計算手段

- 21 アプリケーション
- 22 監視手段
- 23 デバイス
- 221 イベント取得手段
- 222 コンパートメント生成指示手段
- 223 コンパートメント構成管理手段
- 224 デバイス制御手段
- 225 コンパートメント再編指示手段
- 226 コンパートメント切替手段
- 231 ネットワークデバイス
- 232 1次記憶デバイス
- 233 2次記憶デバイス
- 234 表示デバイス
- 235 入力デバイス
- 411 動画配信アプリケーション
- 412 ファイル共有アプリケーション

#### 発明を実施するための最良の形態

[0047] 以下、図面を参照しながら、本発明の実施の形態について説明する。

##### (実施の形態1)

まず、本発明の第1の実施の形態を図面を参照して説明する。図1は、本実施の形態による情報共有システムの構成の一例を示すブロック図である。図1に示すように、情報共有システムは、グループ管理サーバ1と、複数のユーザ端末2とを含む。また、図1に示すように、情報共有システムにおいて、少なくとも1台のグループ管理サーバ1と、少なくとも2台のユーザ端末2とが、インターネット等のネットワーク3を介して相互に通信可能に接続される。

[0048] 図1に示すように、ユーザ端末2は、機能上、各種アプリケーションソフトウェア(以下、単にアプリケーション(AP)という)21が搭載され、監視手段22及び各種デバイス23を備える。ユーザ端末2は、監視手段22を用いて、アプリケーション21とデバイス2

3との間で行われる入出力動作を監視し、グループに対応するコンパートメント(後述参照)間の不正な情報のコピーや移動、参照をブロック(阻止)する。

[0049] 図2は、グループ管理サーバ1及びユーザ端末2の構成の一例を示すブロック図である。グループ管理サーバ1は、例えば、グループ内の情報共有を管理する情報共有管理サービスを提供する情報共有管理事業者が運営するサーバである。グループ管理サーバ1は、具体的には、ワークステーションやパーソナルコンピュータ等のプログラム制御により動作するCPU(Central Processing Unit)を有するコンピュータ機からなる情報処理装置である。図2に示すように、グループ管理サーバ1は、機能上、全体制御を担う制御部(図示しない)のほか、通信インタフェース(I/F)手段11と、グループ管理データベース(DB)12とを備える。

[0050] 通信インタフェース手段11は、ネットワーク3を介してデータを送受信する機能を備える。本実施の形態では、通信インタフェース手段11は、ユーザ端末2から、ネットワーク3を介して、ユーザであるメンバを識別するためのメンバIDを受信する。また、グループ管理サーバ1は、メンバが属するグループを識別するためのグループID及び所定の認証キーをグループ管理データベース12から抽出し、抽出したグループID及び認証キーをユーザ端末2に配布する機能を備える。本実施の形態では、通信インタフェース手段11は、抽出したグループID及び認証キーを、ネットワーク3を介してユーザ端末2に送信する。

[0051] グループ管理データベース12は、グループID、認証キー及びメンバIDの関係を保持するデータベースである。本実施の形態では、グループ管理データベース12は、グループIDと認証キーとメンバIDとを対応付けて記憶する。本実施の形態では、グループ管理サーバ1は、通信インタフェース手段11からの要求に応じてメンバIDに対応するグループID及び認証キーを抽出し、通信インタフェース手段11に返す。

[0052] ユーザ端末2は、具体的には、パーソナルコンピュータ等のプログラム制御により動作するCPUを有するコンピュータ機からなる情報処理端末である。図2に示すように、ユーザ端末2は、機能上、各種アプリケーション21と、監視手段22と、各種デバイス23とを含む。デバイス23には、少なくともネットワークデバイス231と、1次記憶デバイス232と、2次記憶デバイス233とが含まれる。

- [0053] 監視手段22は、具体的には、予め設定されたプログラムに従って動作するユーザ端末2のCPUによって実現される。図2に示すように、監視手段22は、その内部構成として、機能上、イベント取得手段221と、コンパートメント生成指示手段222と、コンパートメント構成管理手段223と、デバイス制御手段224とを備える。
- [0054] イベント取得手段221は、アプリケーション21のイベントを検出し、検出したイベントをコンパートメント構成管理手段223に渡す機能を備える。例えば、イベント取得手段221は、アプリケーション21による少なくともアプリケーション21の起動やデバイス23への入出力等に関する動作イベントを所定の方法により取得(検出)し、取得したイベントをコンパートメント構成管理手段223に伝達(出力)する。アプリケーション21の動作イベントを検出する方法としては、例えば、一般にイベントフックと呼ばれる方法を用いることができる。
- [0055] コンパートメント生成指示手段222は、デバイス制御手段224及びネットワークデバイス231を介して、ネットワーク3に接続されている。コンパートメント生成指示手段222は、デバイス制御手段224及びネットワークデバイス231を介して、グループ管理サーバ1からユーザ端末2のユーザが属するグループのグループID及び認証キーを受信してその配布を受ける機能を備える。また、コンパートメント生成指示手段222は、受信したグループIDと認証キーとを持つコンパートメントの生成を、コンパートメント構成管理手段223に指示する機能を備える。
- [0056] なお、本明細書で用いる「コンパートメント」とは、コンピュータ内のソフトウェア及びファイルを含む計算資源をグループに対応付けて割り当てるための仮想的に区画化されたグループ専用領域であり、グループ間で互いの関係が解析可能に構成された区画に対応するものである。例えば、「コンパートメント」は、グループIDで識別されるグループの固有領域である。具体的には、「コンパートメント」は、情報を共有するグループ単位で作成されるファイルの区画やオブジェクトの区画であり、コンピュータ内の計算資源が仮想的に区画化された資源集合という概念を表す。コンピュータ内の計算資源としては、例えばファイル、プロセス(アプリケーション、ウィンドウ、又はオブジェクト等)、ネットワーク(共有範囲)が含まれる。本実施の形態では、後述するように、コンパートメント生成指示手段222の指示に従って、コンパートメント構成管理手段

223がコンパートメントを構成する構成情報を生成する。これによって、コンパートメントが仮想的に生成される。

- [0057] コンパートメント構成管理手段223は、コンパートメント生成指示手段222からの指示に従ってコンパートメントの構成情報を生成し、生成したコンパートメントの構成情報を保持する機能を備える。また、コンパートメント構成管理手段223は、イベント取得手段221から入力した動作イベントに基づいて、オブジェクトやファイル、アプリケーションの所属するコンパートメントを特定する機能を備える。例えば、コンパートメント構成管理手段223は、1次記憶デバイス232上に配置されたオブジェクトや、2次記憶デバイス233上に配置されたファイル、ネットワークデバイス231を介して接続される他のユーザ端末2上のアプリケーション等の所属するコンパートメントを特定する。
- [0058] また、コンパートメント構成管理手段223は、コンパートメント間の不正なデータ流を発見し、不正なデータ流を発見すると、そのデータ流に対応する動作イベントをブロック(阻止)する機能を備える。また、コンパートメント構成管理手段223は、コンパートメント間のデータ流が正当なデータ流である場合、そのデータ流に対応する動作イベントをデバイス制御手段224に渡す機能を備える。本実施の形態では、コンパートメント構成管理手段223は、動作イベントによるデータ流が同一コンパートメント内のデータ流である場合、もしくは下位コンパートメントから上位コンパートメントへのデータ流である場合には、その動作イベントをデバイス制御手段224に伝達する。
- [0059] デバイス制御手段224は、コンパートメント構成管理手段223から伝達された動作イベントについて、コンパートメント構成管理手段223が保持する情報(コンパートメントの構成情報)に基づいて、デバイス23を制御する機能を備える。本実施の形態ではデバイス制御手段224は、コンパートメントの構成情報に基づいて、ネットワークデバイス231を介したアプリケーション21間の通信に際して、監視手段22同士とのトンネル確立及び相互認証処理を行う。また、デバイス制御手段224は、コンパートメントの構成情報に基づいて、1次記憶デバイス232が記憶するオブジェクト間のメッセージング処理を行ったり、2次記憶デバイス233が記憶するファイル実体への入出力処理を行ったりする。
- [0060] ネットワークデバイス231は、デバイス制御手段224の指示に従って、ネットワーク3

を介してデータを送受信する機能を備える。また、1次記憶デバイス232は、各種オブジェクトを記憶する。また、2次記憶デバイス233は、各種ファイルを記憶する。

[0061] なお、本実施の形態において、グループ管理サーバ1の記憶装置(図示せず)は、グループを管理するための各種プログラムを記憶している。例えば、グループ管理サーバ1の記憶装置は、コンピュータに、メンバを識別するためのメンバ識別情報を入力すると、少なくとも1以上のグループIDと認証キーとの組を生成するグループ管理処理を実行させるためのグループ管理プログラムを記憶している。

[0062] また、本実施の形態において、ユーザ端末2の記憶装置(図示せず)は、コンパートメントを生成し管理するための各種プログラムを記憶している。ユーザ端末2の記憶装置は、コンピュータに、グループIDと認証キーとの各組に対応するコンパートメントと、少なくともコンパートメント間の順序関係、コンパートメントとアプリケーションソフトウェアとの所属関係、又はコンパートメントとファイルとの所属関係の情報を含むコンパートメント構成グラフを生成するコンパートメント生成処理と、アプリケーションソフトウェアの動作を監視して、コンパートメント構成グラフに基づいて、少なくともファイル入出力イベント又はネットワーク入出力イベントの実行可否を制御するアクセス制御処理とを実行させるためのコンパートメント管理プログラムを記憶している。

[0063] 次に、本実施の形態の動作について説明する。

(コンパートメントの生成動作)

まず、ユーザ端末2がコンパートメントを生成するコンパートメント生成動作を説明する。図3は、ユーザ端末2がコンパートメントを生成するコンパートメント生成処理の一例を示す流れ図である。本実施の形態では、ユーザ端末2の各ユーザは、情報共有管理サービスの提供を受けることについて、予め情報共有管理事業者と契約を締結している。また、各ユーザは、予めメンバIDを付与され、自分が所属するグループを予めグループ管理サーバ1に登録している。また、グループ管理サーバ1は、ユーザの登録内容に応じて、メンバIDとグループIDとを対応付けてグループ管理データベース12に記憶している。

[0064] なお、本実施の形態では、例えば、グループnに対して生成されるコンパートメントをコンパートメントCnと表現する。また、本実施の形態では、例えば、グループnに付

与されているグループIDをID[Cn]と表現する。

- [0065] 図3に示すように、ユーザ端末2は、ネットワーク3を介して、所定のメンバIDをグループ管理サーバ1に送信する(ステップS11)。例えば、ユーザによってユーザ端末2の起動操作がなされると、ユーザ端末2は、メンバIDをネットワーク3を介してグループ管理サーバ1に送信する。この場合、ユーザ端末2のネットワークデバイス231が、コンパートメント生成指示手段222の指示に従って、メンバIDをグループ管理サーバ1に送信する。グループ管理サーバ1の通信インタフェース手段11は、ユーザ端末2からネットワーク3を介してメンバIDを受信する。
- [0066] 例えば、ユーザ端末2は、メンバIDとして、パスワードやユーザ証明書等任意の認証方式に基づいてユーザ端末2にログインしているユーザIDや、ユーザ端末2内の耐タンパデバイス(図示しない)に格納される機器IDを、グループ管理サーバ1に送信する。また、例えば、ユーザ端末2がそれらユーザIDや機器IDを併せて送信することによって、グループ管理サーバ1が多要素認証を行ってもよい。
- [0067] 次いで、グループ管理サーバ1は、受信したメンバIDに基づいてグループ管理データベース12を検索し、メンバIDに対応するグループIDと認証キーとを抽出する。そして、グループ管理サーバ1は、抽出したグループIDと認証キーとの組から成る系列を生成し、ネットワーク3を介してユーザ端末2に送信する(ステップS12)。この場合、グループ管理サーバ1は、新たに所属したグループを発見すると、グループ管理データベース12から全てのグループIDと認証キーとの組からなる系列(以下、グループID／認証キー系列ともいう)を抽出し、ユーザ端末2に配布する。
- [0068] 次いで、ユーザ端末2のコンパートメント生成指示手段222は、ネットワーク3及びネットワークデバイス231を介して、グループID／認証キー系列を受信する。また、コンパートメント生成指示手段222は、各グループID(ID[Cn])と認証キーとを属性として含むコンパートメントノードN[Cn]を新たに生成するように、コンパートメント構成管理手段223に指示する。すると、コンパートメント構成管理手段223は、コンパートメント生成指示手段222の指示に従って、コンパートメントノードN[Cn]を生成する(ステップS13)。
- [0069] 次いで、コンパートメント構成管理手段223は、生成したコンパートメントノードN[C

n]を所定のコンパートメント構成グラフGに登録する(ステップS14)。「コンパートメント構成グラフG」は、コンパートメント構成管理手段223が生成するコンパートメント間の関係及びその構成情報を示すグラフ、すなわちノードの集合およびそのノード間を結ぶ辺(有向辺および無向辺)の集合から構築されるデータ構造である。例えば、「コンパートメント構成グラフG」は、コンパートメントとアプリケーションソフトウェアとの所属関係を示す。コンパートメント構成グラフGは、2次記憶デバイス233に格納するようにしてもよく、別途備えた耐タンパデバイスに格納するようにしてもよい。なお、コンパートメント構成管理手段223によるコンパートメント構成グラフGに関する処理は、例えばコンピュータ上で動作可能なグラフアルゴリズムに基づくグラフに関する処理プログラムを用いて行うことが可能である。

[0070] また、本実施の形態において、コンパートメント構成グラフGは、初期値として、最低の機密レベル(すなわち、未分類(Unclassified)レベル)をもつコンパートメントノードN[Unclassified]だけから成るものとする。また、コンパートメント構成管理手段223は、コンパートメントノードN[Cn]を生成すると、新たに生成したN[Cn]をN[Unclassified]から少なくとも1本の有向辺で辿れる箇所に追加することによって、生成したコンパートメントノードN[Cn]をコンパートメント構成グラフGに登録する。

[0071] 次いで、コンパートメント構成管理手段223は、コンパートメントノードN[Cn]に対応するオブジェクトのツリー構造を示すオブジェクトツリーOT[Cn]、及びコンパートメントノードN[Cn]に対応するファイルの配置(格納場所)を示すファイル配置テーブルFT[Cn]を新たに生成する。そして、コンパートメント構成管理手段223は、生成したオブジェクトツリーOT[Cn]及びファイル配置テーブルFT[Cn]を、コンパートメントノードN[Cn]の属性として、コンパートメント構成グラフGに格納する(ステップS15)。

[0072] 以上のように、ステップS11～S15までの処理が実行されることによって、例えば、ユーザ端末2の起動時にコンパートメント生成指示手段222が自動的にグループ管理サーバ1に接続し、新たなユーザグループの作成に伴ってメンバのユーザ端末2内に適切なコンパートメントを生成することができる。すなわち、コンパートメント構成管理手段223は、コンパートメントノードN[Cn]やオブジェクトツリーOT[Cn]、ファイル配置テーブルFT[Cn]等の構成情報を生成することによって、コンパートメントCn

を仮想的に生成する。なお、その他の動作として、新規グループの作成を通知するメールを受けて、コンパートメント生成指示手段222がグループ管理サーバ1に接続し、ユーザ端末2にコンパートメントを生成するようにしてもよい。

[0073] (アプリケーションの起動イベントに対する動作)

次に、アプリケーション21の起動イベントに対する動作を説明する。図4は、アプリケーション21の起動イベントに対しユーザ端末2が行う処理の一例を示す流れ図である。本実施の形態では、ユーザ端末2において、既に起動されているアプリケーション(以下、「起動済アプリケーション」ともいう)が他のアプリケーション(以下、「被起動アプリケーション」ともいう)を起動する場合を説明する。なお、本実施の形態では、「アプリケーションが起動する」等の表現を用いるが、実際には、ユーザ端末2のCPUが各種アプリケーションに従って処理を実行する。

[0074] 図4に示すように、既に起動されているアプリケーションが他のアプリケーションを起動するとき、イベント取得手段221は、被起動アプリケーションの起動イベントを取得(検出)し(ステップS21)、コンパートメント構成管理手段223に出力する。なお、イベント取得手段221が取得するイベントは、少なくとも発生源となったアプリケーションのオブジェクトを識別するためのオブジェクトIDを属性としてもつものとする。

[0075] 次いで、コンパートメント構成管理手段223は、イベント取得手段221から入力した被起動アプリケーションの起動イベントの属性である起動済アプリケーションのオブジェクトIDに基づいて、コンパートメント構成グラフGの各コンパートメントノードを探索する。そして、コンパートメント構成管理手段223は、起動済アプリケーションのオブジェクトノードを有するオブジェクトツリーOT[Ci]を特定する(ステップS22)。

[0076] 次いで、オブジェクトツリーOT[Ci]を特定すると、コンパートメント構成管理手段223は、被起動アプリケーションのオブジェクトノードを新たに生成し、起動済アプリケーションのオブジェクトノードの子ノードとしてオブジェクトツリーOT[Ci]に登録する(ステップS23)。この際、コンパートメント構成管理手段223は、被起動アプリケーションのオブジェクトIDも生成して、被起動アプリケーションのオブジェクトノードの属性としてオブジェクトツリーOT[Ci]に格納する。

[0077] 以上のように、ステップS21～S23までの処理が実行されることによって、新たに起

動されたアプリケーションを適切なコンパートメントに所属させることができる。また、起動する側のアプリケーションとして、所属コンパートメントを任意に選択できる特殊なランチャーを設けることによって、ユーザが複数のグループに所属する場合に、アクセスしたいコンパートメントを選択できるユーザインタフェースを設けることができる。

[0078] (オブジェクト間のメッセージ送信イベントに対する動作)

次に、オブジェクト間のメッセージを送信するオブジェクト間メッセージ送信イベントに対する動作を説明する。図5は、コンパートメント構成グラフGの一例を示す説明図である。本実施の形態では、ユーザ端末2が図5に示すコンパートメント構成グラフGを記憶している場合を説明する。本実施の形態では、図5に示すように、コンパートメント構成管理手段223は、コンパートメント構成グラフGに基づいて、4つのコンパートメントC0、C1、C2、C3を管理している。

[0079] コンパートメントノード同士は互いに有向辺で接続されており、出次側(有向辺の矢印が無い側)のコンパートメントは、入次側(有向辺の矢印が存在する側)のコンパートメントよりも下位の関係にあることを示す。この上下関係は推移的であり、例えば、あるコンパートメントノードN[C]と、N[C]から複数の有向辺を順方向(有向辺の矢印の方向)に辿って到達可能な任意のコンパートメントノードN[D]とは、 $N[D] > N[C]$ の関係(すなわち、コンパートメントDがコンパートメントCより上位である関係)にあると解釈するものとする。一方、N[C]から複数の有向辺を逆方向(有向辺の矢印とは逆方向)に辿って到達可能な任意のコンパートメントノードN[E]とは、 $N[C] > N[E]$ の関係(すなわち、コンパートメントCがコンパートメントEより上位である関係)にあると解釈するものとする。また、コンパートメント構成グラフG上で有向辺を辿って到達不能なコンパートメントは「比較不能」であるものとする。

[0080] 例えば、図5に示す例では、 $N[C0] < N[C1]$ 、 $N[C0] < N[C2]$ 、 $N[C1] < N[C3]$ 、 $N[C2] < N[C3]$ の関係にあり、N[C1]とN[C2]とは互いに比較不能であることが分かる。すなわち、コンパートメントC1及びC2は、コンパートメントC0より上位であり、コンパートメントC3は、コンパートメントC1及びC2より上位である関係にある。また、コンパートメントC1とC2とは互いに上下関係が比較不能である。

[0081] 本実施の形態では、2つのアプリケーション21(第1アプリケーション及び第2アプリ

ケーション)があり、それぞれ第1アプリケーションがコンパートメントC0に属し、第2アプリケーションがコンパートメントC1に属するものとする。この場合に、第1アプリケーションから第2アプリケーションにメッセージ(シグナル)が送信されたときの監視手段22の動作を説明する。図6は、第1アプリケーションから第2アプリケーションにメッセージが送信されたときに監視手段22が行う処理の一例を示す流れ図である。

- [0082] 同図において、イベント取得手段221は、第1アプリケーションから第2アプリケーションへのメッセージ送信イベントを取得(検出)し(ステップS31)、コンパートメント構成管理手段223に伝達(出力)する。すると、コンパートメント構成管理手段223は、コンパートメント構成グラフGのうちコンパートメントノードN[C0]及びN[C1]を参照する。そして、コンパートメント構成管理手段223は、コンパートメントノードN[C0]及びN[C1]に基づいて、それぞれ第1アプリケーション及び第2アプリケーションが属するオブジェクトツリーOT[C0]及びOT[C1]を抽出する(ステップS32)。
- [0083] 次いで、コンパートメント構成管理手段223は、図7に示すように、次の処理を行う。まず、コンパートメントノードN[C0]及びN[C1]にそれぞれ対応する仮想オブジェクトVO[C0]及びVO[C1]を生成する。次に、その仮想オブジェクトVO[C0]及びVO[C1]の子として、オブジェクトツリーOT[C0]及びOT[C1]をそれぞれ接続する。さらに、仮想オブジェクトVO[C0]とVO[C1]との間に、コンパートメントノードN[C0]、N[C1]間と同じ方向をもつ有向辺を追加する。これによって、オブジェクトツリーOT[C0]及びOT[C1]を互いにマージ(結合)したツリーを生成する(ステップS33)。
- [0084] 次いで、コンパートメント構成管理手段223は、上記のようにマージしたツリー上で、第1アプリケーションが属するコンパートメントC0に対応する仮想オブジェクトVO[C0]からその無向辺及び有向辺を順方向に辿って第2アプリケーションが属するコンパートメントC1に対応する仮想オブジェクトVO[C1]に辿りつけるか否かを検査(判定)する(ステップS34)。この場合、無向辺については、双方向に辿ることができる有向辺として扱う。
- [0085] その結果、第2アプリケーションに到達可能であると判定すると、コンパートメント構成管理手段223は、第1アプリケーションから第2アプリケーションへのメッセージ送信イベントの通過(出力)を許可する(ステップS35)。また、第2アプリケーションに到

達可能でないと判定すると、コンパートメント構成管理手段223は、第1アプリケーションから第2アプリケーションへのメッセージ送信イベントの通過をブロック(阻止)する(ステップS36)。この場合、例えば、コンパートメント構成管理手段223は、第1アプリケーションから第2アプリケーションへのメッセージ送信イベントを通過させないように制御する。

[0086] 以上のように、ステップS31からステップS36までの処理が実行されることによって、例えば、コンパートメントC0に属するクリップボード(第1アプリケーション)から、コンパートメントC1に属するエディタ(第2アプリケーション)へのペースト操作を許可することができる。また、例えば、その逆のエディタからクリップボードへのコピー操作を禁止することができる。そのようにすることによって、コピー&ペースト操作による下位又は比較不能な別のコンパートメントへの情報漏洩を防止することができる。

[0087] (ファイル入出力イベントに対する動作)

次に、ファイルを入出力するファイル入出力イベントに対する動作を説明する。本実施の形態において、ファイル配置テーブルFTは、ファイル名と2次記憶デバイス233上のファイル実体とを対応付けた対応表である。また、本実施の形態では、アプリケーションからファイルアクセスする場合、ファイル配置テーブルFTに基づいてファイル名から配置アドレスを求めることによって、ファイル実体にアクセスできるものとする。

[0088] 図8は、図5に示したコンパートメント構成グラフGにおけるコンパートメントC0及びC1それぞれのファイル配置テーブルFT[C0]及びFT[C1]の一例を示す説明図である。本実施の形態では、図8に示すファイル配置テーブルを用いて、コンパートメントC1に属するアプリケーションからファイル実体へアクセスするアクセス制御方法を考える。以下、(1)アプリケーションがファイル読み込み、又はファイル一覧を行う場合と、(2)アプリケーションがファイル書き込み等の変更を行う場合とに分けて、ファイル制御方法を説明する。

[0089] (1)ファイル読み込み時又はファイル一覧時の動作

まず、アプリケーションがファイル読み込み、又はファイル一覧を行う場合を説明する。図9は、アプリケーションがファイル一覧を行う際に監視手段22が行う処理の一例を

示す流れ図である。同図において、イベント取得手段221は、アプリケーションによるファイル一覧イベントを取得(検出)し(ステップS41)、コンパートメント構成管理手段223に伝達(出力)する。

- [0090] 次いで、コンパートメント構成管理手段223は、入力したファイル一覧イベントに基づいて、アプリケーションがいずれのコンパートメントに属するかを判断する。本実施の形態では、アプリケーションがコンパートメントC1に属すると判断する。その結果、アプリケーションがコンパートメントC1に属することを確認すると、コンパートメントC1に対応するファイル配置テーブルFT[C1]を抽出する(ステップS42)。
- [0091] 次いで、コンパートメント構成管理手段223は、コンパートメントC1の下位コンパートメントであるコンパートメントC0に対応するファイル配置テーブルFT[C0]を抽出する。そして、コンパートメント構成管理手段223は、ファイル配置テーブルFT[C1]とFT[C0]とをマージ(結合)し(ステップS43)、2つのファイル配置テーブルFT[C1]及びFT[C0]をマージした結合ファイル配置テーブル(結合FTともいう)を生成する。この際、コンパートメント構成管理手段223は、同じファイル名がある場合には、上位のファイル配置テーブルFTのレコード(ファイル名と配置アドレスとの組)を採用して、結合FTを生成する。本実施の形態では、コンパートメント構成管理手段223は、図10に示す統合FTを構成する。
- [0092] 次いで、コンパートメント構成管理手段223は、入力したイベントがファイル一覧を要求するイベントであるか否かを判断する。その結果、ファイル一覧を要求する入力イベントであると判断すると、コンパートメント構成管理手段223は、統合FTのファイル名一覧を抽出しアプリケーションに返す(ステップS44)。
- [0093] 図11は、アプリケーションがファイル読み込みを行う際に監視手段22が行う処理の一例を示す流れ図である。同図において、イベント取得手段221は、アプリケーションによるファイル読込イベントを取得(検出)し(ステップS41b)、コンパートメント構成管理手段223に伝達(出力)する。コンパートメント構成管理手段223は、ファイル一覧の場合の処理と同様に、ファイル配置テーブルFT[C1]及びFT[C0]を抽出し、ファイル配置テーブルFT[C1]とFT[C0]とをマージする(ステップS42, S43)。
- [0094] 次いで、コンパートメント構成管理手段223は、マージしたファイル配置テーブルの

ファイル名のコラムを検索して、読み込み対象のファイルに対応する配置アドレスを抽出する。また、配置アドレスを得ると、コンパートメント構成管理手段223は、デバイス制御部224を介して、2次記憶デバイス233のファイル実体を読み込み、入力したファイル実体をアプリケーションに返す(ステップS45)。

[0095] (2)ファイル書込み等の変更時の動作

次に、アプリケーションがファイル書込み等の変更を行う場合を説明する。図12は、アプリケーションがファイル書込み等の変更を行う際に監視手段22が行う処理の一例を示す流れ図である。同図において、イベント取得手段221は、アプリケーションによるファイル出力イベントを取得(検出)し(ステップS51)、コンパートメント構成管理手段223に伝達(出力)する。

[0096] 次いで、コンパートメント構成管理手段223は、アプリケーションがコンパートメントC1に属することを確認すると、入力イベントの処理の場合とは異なり、コンパートメントC1に対応するファイル配置テーブルFT[C1]のみを抽出する(ステップS52)。そして、コンパートメント構成管理手段223は、ファイル名の変更やファイルの削除等をファイル配置テーブルFT[C1]のみに対して行う。また、コンパートメント構成管理手段223は、ファイル更新については、ファイル配置テーブルFT[C1]に記載された配置アドレスをデバイス制御部224に入力し、更新内容を2次記憶デバイス233のファイル実体書き込む(ステップS53)。

[0097] 以上のように、ステップS51からステップS53までの処理が実行されることによって、同じファイル名でファイル書き出しを行う場合であっても、コンパートメント毎に異なるファイル実体として格納することができる。例えば、図13に示すように、コンパートメントC0とC1とに属するそれぞれのアプリケーションが、同じファイル名「file1」でファイル書き出しを行う場合でも、2次記憶デバイス233上では、コンパートメント毎に異なるファイル実体として格納される。そのため、コンパートメントC1に属するアプリケーションから下位コンパートメントC0への情報漏洩を防ぐことができる。

[0098] また、当初コンパートメントC1に「file1」がない場合、コンパートメントC1に属するアプリケーションは、下位コンパートメントC0の「file1」を読み込むことができる。その後、そのアプリケーションにより何らかの機密が追加されて、同じファイル名「file1」で保

存されたとする。この場合、更新後の「file1」は自動的に上位コンパートメントC1に属するファイルとして2次記憶デバイス233に格納されるが、更新前の「file1」は依然としてコンパートメントC0に属するファイルとして維持される。

[0099] さらに、従来のMLSシステムでは、同様の操作によって、「file1」の機密レベル昇格、例えば、コンパートメントC0からC1への所属変更が発生した際、コンパートメントC0に属する「file1」が消滅してしまい、その結果、コンパートメントC0に相当する広範なグループでの情報共有を妨げるおそれがあった。これに対し、本実施の形態によれば、特定グループでの限定的な機密を保護できるとともに、より広範なグループでの情報共有を妨げないようにできる。

[0100] (ネットワークイベントに対する動作)

次に、ユーザ端末2間でネットワーク3を介して通信する際のネットワークイベントに対する動作を説明する。図14は、ネットワーク3を介して接続された1つのユーザ端末(以下、ユーザ端末U1という)と、他のユーザ端末(以下、ユーザ端末U2という)との間で通信を行う場合の処理の一例を示す流れ図である。

[0101] 同図において、ユーザ端末U1のアプリケーション(以下、アプリケーション(AP1)という)は、ユーザ端末U2のアプリケーション(以下、アプリケーション(AP2)という)に接続を要求する(ステップS61)。すると、ユーザ端末U1のイベント取得手段221は、アプリケーション(AP1)によるネットワーク接続要求イベントを取得(検出)し、コンパートメント構成管理手段223に伝達(出力)する。

[0102] 次いで、ユーザ端末U1のコンパートメント構成管理手段223は、アプリケーション(AP1)のコンパートメントがコンパートメントCiであることを確認する。そして、ユーザ端末U1及びユーザ端末U2双方のデバイス制御手段224及びネットワークデバイス231を介して、ユーザ端末U2のコンパートメント構成管理手段223にコンパートメントCiに属するトンネルTUN[Ci, AP2]の確立を要求する(ステップS62)。

[0103] 次いで、トンネルTUN[Ci, AP2]の確立要求を受信すると、ユーザ端末U2のコンパートメント構成管理手段223は、コンパートメント構成グラフからコンパートメントノードN[Ci]に対応するオブジェクトツリーOT[Ci]を探索する。そして、アプリケーション(AP2)がコンパートメントCiに属するか否かを判定する(ステップS63)。その結果、

コンパートメントCiに属することを確認できなかった場合、コンパートメント構成管理手段223は、直ちに確立要求を拒否する(ステップS642)。

[0104] 一方、アプリケーション(AP2)がコンパートメントCiに属すると判定すると、ユーザ端末U1及びユーザ端末U2のコンパートメント構成管理手段223は、コンパートメントCiの認証キーAK[Ci]を持っていることを相互に認証する(ステップS64a、S64b)。具体的には、例えば、ユーザ端末U2がユーザ端末U1に乱数r12を送信する。この場合、ユーザ端末U1がユーザ端末U2に認証メッセージM12 = (h[AK[Ci]](r12), r21)を送信する。すると、ユーザ端末U2がユーザ端末U1に認証メッセージM21 = (h[AK[Ci]](r21))を返す。そして、ユーザ端末U1及びユーザ端末U2それぞれがH[Rb](AK[Ci])とH[Ra](AK[Ci])とを計算して、受信した認証メッセージM21及びM12が正しいことを検証する。なお、乱数r12と乱数r21とは異なる乱数であり、h[k](m)は鍵kによるmの鍵付き一方向性ハッシュ関数であるものとする。

[0105] その結果、ユーザ端末U1及びU2のいずれかが他方の認証メッセージの検証に失敗すると、ユーザ端末U1及びU2は、共に直ちにトンネルTUN[Ci, AP2]の接続処理を中断(許否)する(ステップS641、S642)。

[0106] 一方、ユーザ端末U1及びU2が相互認証に成功すると、ユーザ端末U2のコンパートメント構成管理手段223は、トンネルTUN[Ci, AP2]の確立許可をユーザ端末U1に伝える(ステップS65)。この場合、ユーザ端末U2は、確立許可の通知情報を、ネットワーク3を介してユーザ端末U1に送信する。そして、ユーザ端末U1のコンパートメント構成管理手段223は、確立許可のアクノリジメントをユーザ端末U2に伝えて(ステップS66)、トンネルTUN[Ci, AP2]の確立処理を完了する。この場合、ユーザ端末U1は、確立許可の通知を受け取った旨の通知情報(アクノリジメント)を、ネットワーク3を介してユーザ端末2に送信する。

[0107] その後、ユーザ端末U1及びU2は、トンネルTUN[Ci, AP2]を用いて、アプリケーション(AP1)とアプリケーション(AP2)間でアプリケーション依存の接続確立処理を行う(ステップS67a、S67b)。そして、ユーザ端末U1及びU2は、トンネルTUN[Ci, AP2]上で所定のプロトコルによる通信を行う(ステップS68a、S68b)。

[0108] 以上のように、ステップS61からステップS68までの処理が実行されることによって、

遠隔地にいる同一グループのメンバー同士のみで安全に機密を共有することができる。また、機密共有の通信時に、いかなる第三者サーバも利用しないので、IrDAやブルートゥース(Bluetooth)等の近接通信への親和性が高い。さらに、IPカプセル化によるトンネリング手法を用いれば、アプリケーション(AP1)及びアプリケーション(AP2)間で任意のプロトコルを用いることができる。

[0109] 以上のように、本実施の形態によれば、各メンバーが用いるユーザ端末2の監視手段22は、アプリケーションやファイルシステム、ネットワークを、メンバーが属するグループ専用領域であるコンパートメントに結び付けて管理する。また、監視手段22は、同一コンパートメント内の任意のアプリケーション間でのファイルアクセスやネットワーク転送を許可し、且つ異なるコンパートメントへのファイル書き出しやネットワーク転送を禁止する。そのため、グループ毎に遠隔地に離れて存在するメンバー間での自由な情報共有と、グループ外への情報漏洩を防止することができる。従って、ネットワークを介して遠隔地間で情報共有を行う場合に、グループ内の機密情報の確実な保護を行えるようにすることができる。

[0110] また、本実施の形態によれば、中央のグループ管理サーバ1は、各グループとそれらグループのメンバー構成だけを管理する。本実施の形態によれば、グループ管理サーバ1が個々の情報やユーザ端末間の通信状況を管理しなくても、各メンバーのユーザ端末2の監視手段22同士で相互にコンパートメント認証を行うことによって、情報共有及び漏洩防止を行う。従って、各グループで共有される情報の数、あるいは情報共有のための通信頻度が増大しても、情報共有システム全体を安定的に運用することができる。

[0111] (実施例)

次に、具体的な実施例を用いて、本実施の形態の動作を説明する。図15は、情報共有システムを適用したシステムの具体的な構成の一例を示すブロック図である。本実施例では、情報共有システムを適用した遠隔会議システムを例に説明する。本実施例では、図15に示すように、遠隔会議システムにおいて、グループ管理サーバ1、N台のユーザ端末2-1～N及び遠隔会議サーバ4が、それぞれネットワーク3を介して相互に接続されている。

[0112] 本実施例において、遠隔会議サーバ4は、図1に示すユーザ端末2と同様に、監視手段22とデバイス23とを備える。また、遠隔会議サーバ4は、動画配信アプリケーション411及びファイル共有アプリケーション412が搭載されている。動画配信アプリケーション411は、ユーザ端末2-1～N上の任意の会議クライアントから送信される動画データを他のユーザ端末2-1～Nの全ての会議クライアントに送信するためのアプリケーションである。また、ファイル共有アプリケーション412は、ユーザ端末2-1～N上の任意の会議クライアントから送信される会議資料データを格納するためのアプリケーションである。

[0113] (A) セットアップ時の動作

まず、遠隔会議システムのセットアップ時の動作を説明する。ユーザ端末2-1～N及び遠隔会議サーバ4の各ホストの監視手段22は、グループ管理サーバ1に、ネットワーク3を介して、それぞれユーザ端末2-1～N及び遠隔会議サーバ4が用いるメンバIDを送信する(図3のステップS11)。メンバIDの具体例としては、CPUの固有IDや2次記憶デバイスの固有ID等を用いることができるが、監視手段22だけがアクセスできる読み出し専用の耐タンパデバイスに、各ユーザ固有のメンバIDを格納しておくことが望ましい。本実施例では、ユーザ端末2-1～NのメンバIDをそれぞれ「USER-1」～「USER-N」とし、遠隔会議サーバ4のメンバIDを「CONF-SERV」とする。

[0114] 次に、グループ管理サーバ1は、メンバIDを受信し、受信したメンバIDに基づいて適切なグループID及び認証キーの組を特定する。そして、グループ管理サーバ1は、グループID及び認証キーの組を、メンバIDの送信元ホストに配布(送信)する(図3のステップS12)。グループID及び認証キーを特定するための具体的な方法として、例えば、図16に示すように、グループID、認証キー及びメンバID群の対応を保持したグループ管理データベース11を予め定義しておいてもよい。この場合、グループ管理サーバ1は、受信したメンバIDをキーとして、受信したIDをもつメンバID群を検索して特定し、特定したメンバIDに対応するグループID及び認証キーの組を求める。

[0115] なお、図16に示す「CONF-SERV」や「USER-2」等のメンバIDのように、同じ

メンバIDが複数のエントリに重複して存在していてもよい。この場合、グループ管理サーバ1は、対応するグループID及び認証キーの組の全てを求めて、その求めた系列をメンバIDの送信元ホストに応答する。従って、例えば、グループ管理サーバ1は、ユーザ端末2-1 (USER-1) には[(Group-1, A8BC0F)]を配布し、ユーザ端末2-2 (USER-2) と遠隔会議サーバ4 (CONF-SERV) とには[(Group-1, A8BC0F) (Group-2, 21AAB3)]という系列を配布する。

[0116] また、送信元ホストであるユーザ端末2-1~Nのうちのいずれかの端末又は遠隔会議サーバ4の監視手段22は、グループ管理サーバ1から配布されたグループID及び認証キーの組(又はその系列)を受信する。そして、監視手段22は、それぞれの組を属性としてもつコンパートメントノードNを生成する(図3のステップS13)。例えば、ユーザ端末2-1はコンパートメントノードN[Group-1]を生成し、ユーザ端末2-2及び遠隔会議サーバ4は2つのコンパートメントノードN[Group-1]、N[Group-2]を生成する。

[0117] そして、監視手段22は、新たに生成したコンパートメントノードNをコンパートメント構成グラフGに登録し(図3のステップS14)、オブジェクトツリーOT及びファイル配置テーブルFTをNの属性として格納する(図3のステップS15)。

[0118] 本実施例では、コンパートメント構成グラフGの初期値として、最低の機密レベルをもつ未分類(Unclassified)コンパートメントに相当するコンパートメントノードN[PUBLIC]がコンパートメント構成グラフGに含まれるものとする。監視手段22は、新たに生成した任意のコンパートメントノードNを、N[PUBLIC]<Nの関係を満たすようにコンパートメント構成グラフGに登録する。そのようにすることによって、例えば、ユーザ端末2-1は、図17に示すN[Group-1]の登録後のコンパートメント構成グラフGを構成する。また、例えば、ユーザ端末2-2及び遠隔会議サーバ4は、図18に示すN[Group-1]とN[Group-2]との登録後のコンパートメント構成グラフGを構成する。

[0119] (B) 遠隔会議実施時の動作

次に、遠隔会議の実施の際の動作を説明する。本実施例では、ユーザ端末2-1とユーザ端末2-2とが、遠隔会議サーバ4を介して相互に遠隔会議を開始する場合

の遠隔会議システムの動作を説明する。

[0120] (B-1) 会議クライアントアプリケーション起動時の動作

まず、会議クライアントアプリケーションを起動する際の動作を説明する。ユーザ端末2-1を用いるユーザは、ユーザ端末2-1を操作して、会議クライアントアプリケーション211の起動操作を行う。この場合、ユーザ端末2-1の監視手段22は、会議クライアントアプリケーション211の起動イベントを捕捉(検出)する(図4のステップS21)。なお、本実施例では、アプリケーション21の一種であるシェル212を用いて、会議クライアントアプリケーション211を起動したものとする。また、シェル212は、グループ(Group-1)のコンパートメントに属しているものとする。

[0121] 次いで、監視手段22は、シェル212に相当するオブジェクトノードO[SHELL]を格納しているGroup-1コンパートメントに属するオブジェクトツリーOT[Group-1]を、コンパートメント構成グラフGが含むオブジェクトツリーのうちから特定する。この場合、監視手段22は、シェル212のオブジェクトIDをキーとして検索し、オブジェクトツリーを特定する(図4のステップS22)。

[0122] 次いで、監視手段22は、会議クライアントアプリケーション211のオブジェクトノードO[CLIENT]を新たに生成して、O[SHELL]の子ノードとして、オブジェクトツリーOT[Group-1]に登録する(図4のステップS23)。

[0123] 以上の動作によって、ユーザ端末2-1は、図19に示すオブジェクトツリーOT[Group-1]に登録し、会議クライアントアプリケーション211の起動処理を完了する。なお、ユーザ端末2-2も、ユーザ端末2-1と同様の処理に従って、会議クライアントアプリケーション211の起動処理を行う。

[0124] (B-2) 遠隔会議サーバ接続時の動作

次に、会議クライアントアプリケーションから遠隔会議サーバ4に接続する際の動作を説明する。ユーザ端末2-1は、会議クライアントアプリケーション211を用いて、遠隔会議サーバ4への接続を開始する。この場合、監視手段22は、会議クライアントアプリケーション211からの遠隔会議サーバ4上の動画配信アプリケーション411への接続要求イベントを捕捉する(図14のステップS61)。

[0125] 次いで、監視手段22のコンパートメント構成管理手段223は、会議クライアントアプ

リケーション211がGroup-1コンパートメントに属することを、オブジェクトツリーOT[Group-1]を親ノード方向に探索することによって確認する。また、コンパートメント構成管理手段223は、デバイス制御手段224及びネットワークデバイス231を介して、遠隔会議サーバ4のコンパートメント構成管理手段223にGroup-1コンパートメントに属するトンネルTUN[Group-1, P411]の確立を要求する(図14のステップS62)。なお、P411は、動画配信アプリケーション411がリスンしている待ち受けポートを示す。

[0126] 次いで、TUN[Group-1, P411]の確立要求を受けた遠隔会議サーバ4のコンパートメント構成管理手段223は、コンパートメント構成グラフからコンパートメントノードN[Group-1]のオブジェクトツリーOT[Group-1]を探索する。そして、動画配信アプリケーション411がGroup-1コンパートメントに属することを確認する(図14のステップS63)。なお、本実施例では、動画配信アプリケーション411は、既にGroup-1コンパートメントの下で起動しているものとする。

[0127] 次いで、ユーザ端末2-1及び遠隔会議サーバ4の各コンパートメント構成管理手段223は、Group-1の認証キー「A8BC0F」を持っていることを相互に認証する(図14のステップS64a、S64b)。本実施例では、前述の(A)セットアップ時の処理で、ユーザ端末2-1及び遠隔会議サーバ4双方のホストは、グループ管理サーバ1から認証キーの配布を受けているので、この相互認証を成功と判定する。

[0128] 次いで、遠隔会議サーバ4のコンパートメント構成管理手段223は、TUN[Group-1, P411]の確立許可をユーザ端末2-1に伝える(図14のステップS65)。また、ユーザ端末2-1のコンパートメント構成管理手段223は、その確立許可のアクノリジメントを遠隔会議サーバ4に伝えて、トンネルTUN[Group-1, P411]の確立処理を完了する(図14のステップS66)。

[0129] 以上の動作により、会議クライアントアプリケーション211と動画配信アプリケーション411との間の通信が、TUN[Group-1, P411]上で開始される(図14のステップS67)。また、ユーザ端末2-1及び遠隔会議サーバ4と同様の処理に従って、図20に示すように、ユーザ端末2-2の会議クライアントアプリケーション211と遠隔会議サーバ4の動画配信アプリケーション411との間の通信が、TUN[Group-1, P411]

上で開始される。

[0130] (C)遠隔会議中の資料共有時の動作

次に、遠隔会議中の資料共有を行う際の動作を説明する。本実施例では、ユーザ端末2-1で作成された会議資料ファイルを、遠隔会議サーバ4を介してユーザ端末2-2がダウンロードしてその会議資料ファイルを共有する場合の遠隔会議システムの動作を説明する。

[0131] (C-1)会議資料ファイルの新規作成時の動作

まず、会議資料ファイルの新規作成を行う際の動作を説明する。ユーザ端末2-1を用いるユーザは、ユーザ端末2-1を操作して、図21に示すように、ワードプロセッサ等の編集アプリケーション213を用いて新たな会議資料ファイルを作成する。この場合、まず、前述の(B-1)会議クライアントアプリケーション211の起動と同様に、監視手段22は、編集アプリケーション213をGroup-1コンパートメント内で起動する。

[0132] 次いで、ユーザ端末2-1のユーザは、編集アプリケーション213を操作して、新たな会議資料ファイル(本例では、ファイル名「PROPOSAL」とする)を編集し、ユーザ端末2-1内の2次記憶デバイス233への保存の指示操作をする。すると、編集アプリケーション213は、ファイル出力イベントを発行する。この場合、監視手段22は、そのファイル出力イベントを補足し、コンパートメント構成管理手段223に伝達する(図12のステップS51)。

[0133] 次いで、コンパートメント構成管理手段223は、編集アプリケーション213のオブジェクトIDをキーとして、オブジェクトツリーOT[Group-1]を根方向に探索する。そして、コンパートメント構成管理手段223は、コンパートメントノードN[Group-1]を特定し、ファイル配置テーブルFT[Group-1]を参照して抽出する(図12のステップS52)。

[0134] さらに、コンパートメント構成管理手段223は、ファイル配置テーブルFT[Group-1]からファイル名「PROPOSAL」を検索して、ファイル名「PROPOSAL」のファイルのファイル配置エントリの取得を試みる。本例では、ファイル「PROPOSAL」が新規ファイルであるので、コンパートメント構成管理手段223は、ファイル配置エントリの取得に失敗する。そのため、コンパートメント構成管理手段223は、新たなファイル配置

エントリを作成する。

- [0135] 次いで、コンパートメント構成管理手段223は、会議資料ファイル「PROPOSAL」のファイル配置エントリを参照して、2次記憶デバイス233上の論理アドレスを特定する。そして、コンパートメント構成管理手段223は、図21に示すように、2次記憶デバイス233上のその論理アドレスで示される位置に、会議資料ファイル「PROPOSAL」のファイル実体を書き出す(図12のステップS53)。

- [0136] (C-2) 会議資料ファイルのアップロード時の動作

次に、会議資料ファイルのアップロードを行う際の動作を説明する。ユーザ端末2-1のユーザは、会議クライアントアプリケーション211を用いてユーザ端末2-1を操作して、先に作成した会議資料ファイル「PROPOSAL」の遠隔会議サーバ4へのアップロードを指示する。この場合、ユーザ端末2-1の会議クライアントアプリケーション211は、以下のように処理を行う。

- [0137] (C-2-1) 会議資料ファイル読み込み時の動作

まず、会議クライアントアプリケーション211は、会議資料ファイル「PROPOSAL」を読み込む。ユーザ端末2-1のユーザは、会議クライアントアプリケーション211を用いてユーザ端末2-1を操作して、アップロード対象となる会議資料ファイル「PROPOSAL」を指定する。この場合、会議クライアントアプリケーション211は、ファイル一覧イベントを発行して、2次記憶デバイス233に格納されたファイル一覧の取得を試みる。

- [0138] 次いで、監視手段22は、会議クライアントアプリケーション211によるファイル一覧イベントを補足すると、取得したファイル一覧イベントをコンパートメント構成管理手段223に伝達する(図9のステップS41)。

- [0139] 次いで、コンパートメント構成管理手段223は、編集アプリケーション213のオブジェクトIDをキーとして、オブジェクトツリーOT[Group-1]を根方向に探索する。そして、コンパートメントノードN[Group-1]を特定し、ファイル配置テーブルFT[Group-1]を参照して抽出する(図9のステップS42)。

- [0140] 次いで、コンパートメント構成管理手段223は、コンパートメント構成グラフGにおいて、N[Group-1]の有向辺を逆方向に辿って、下位の機密レベルをもつPUBLIC

コンパートメントに対応するコンパートメントノードN[PUBLIC]を求める。また、そのPUBLICコンパートメントに対応するファイル配置テーブルFT[PUBLIC]を抽出する。そして、ファイル配置テーブルFT[Group-1]及びFT[PUBLIC]をマージしたファイル配置テーブルFT[Group-1, PUBLIC]を生成する(図9のステップS43)。

[0141] 図22は、ファイル配置テーブルFT[Group-1]及びFT[PUBLIC]の一具体例を示す説明図である。本例では、図22に示すように、ファイル配置テーブルFT[Group-1]に会議資料ファイル「PROPOSAL」のFTレコードが存在するが、その他に、例えば「MINUTE」という名前の議事録ファイルが存在するものとする。また、ファイル配置テーブルFT[PUBLIC]には、「PAPER」という名前の論文ファイルと、「PROPOSAL」という名前の公開資料があるものとする。

[0142] 図23は、図22に示すファイル配置テーブルをマージして生成したファイル配置テーブルFT[Group-1, PUBLIC]の具体例を示す説明図である。図23に示すように、マージ後のファイル配置テーブルFT[Group-1, PUBLIC]には、会議資料ファイル「PROPOSAL」と、議事録ファイル「MINUTE」と、論文ファイル「PAPER」との合計3つのFTレコードが存在する。

[0143] 次いで、コンパートメント構成管理手段223は、ファイル配置テーブルFT[Group-1, PUBLIC]の各FTレコードを参照する。そして、コンパートメント構成管理手段223は、ファイル名の一覧として「PROPOSAL」、「MINUTE」及び「PAPER」を含むファイル名一覧を抽出し、抽出したファイル名一覧を会議クライアントアプリケーション211に返す(図9のステップS44)。

[0144] 次いで、ファイル名一覧を得ると、会議クライアントアプリケーション211は、例えば、図24に示すダイアログを表示し、ファイル名一覧をユーザ端末2-1のユーザに提示する。また、会議クライアントアプリケーション211は、ダイアログを表示することによって、ユーザに読み込み対象となるファイルの指定を促す。例えば、ユーザがファイル「PROPOSAL」を選択指示すると、会議クライアントアプリケーション211は、図25に示すように、「PROPOSAL」という名前のファイルに対する読み込みイベントを発行する。

[0145] 次いで、監視手段22は、ファイル読み込みイベントを捕捉すると(図11のステップS41b

)、ファイル一覧イベントの取得の処理と同様に、ファイル配置テーブルFT[C1]を求める(図11のステップS42)。また、監視手段22は、ファイル配置テーブルFT[C0]とマージしたファイル配置テーブルFT[Group-1, PUBLIC]を生成し(図11のステップS43)、「PROPOSAL」というファイル名をもつFTレコードを特定する。

- [0146] 本例では、「PROPOSAL」という名前のファイルについて、ファイル配置テーブルFT[Group-1]で管理されている会議資料ファイルと、ファイル配置テーブルFT[PUBLIC]で管理されている公開資料ファイルとの同名のファイルが存在する。本実施例のファイル配置テーブルのマージ方法では、監視手段22は、より機密レベルの高いファイル配置テーブルFT[Group-1]のFTエントリを優先する。そのため、監視手段22は、ファイル配置テーブルFT[Group-1, PUBLIC]の「PROPOSAL」ファイルのFTレコードとして、FT[Group-1]のレコードを採用しマージする。従って、監視手段22は、FT[Group-1]に由来する「PROPOSAL」ファイルのFTレコードに記載された論理アドレスに配置されている会議資料ファイルのファイル実体を2次記憶デバイス233から読み込む。そして、監視手段22は、読み込んだファイル実体を、会議クライアントアプリケーション211に渡す(図11のステップS45)。

- [0147] (C-2-2) 会議資料ファイル転送時の動作

次に、遠隔会議サーバ4への会議資料ファイルの転送の際の動作を説明する。会議資料ファイルを読み取ると、ユーザ端末2-1の会議クライアントアプリケーション211は、その会議資料ファイルを遠隔会議サーバ4のファイル共有アプリケーション412に転送する。この場合、ユーザ端末2-1の監視手段22と、遠隔会議サーバ4の監視手段22とは、前述の(B-2)遠隔会議サーバ4への接続と同様の処理に従って、図26に示すように、トンネルTUN[Group-1, P412]を確立する。そして、会議クライアントアプリケーション211は、ファイル共有アプリケーション412に会議資料ファイルの転送を行う。なお、P412は、ファイル共有アプリケーション412がリスンしている待ち受けポートを示す。

- [0148] 会議資料ファイルを受信すると、ファイル共有アプリケーション412は、受信した会議資料ファイルを遠隔会議サーバ4の2次記憶デバイス233に保存する。この場合、遠隔会議サーバ4の監視手段22は、前述の(C-1)会議資料ファイルの新規作成の

際の監視手段22の処理と同様の処理に従って、Group-1コンパートメントのファイル配置テーブルFT[Group-1]を特定する。そして、監視手段22は、ファイル名「PROPOSAL」のFTレコードを生成し、アップロードされた会議資料ファイルのファイル実体を2次記憶デバイス233に格納する。

[0149] (C-3) 会議資料ファイルのダウンロード時の動作

次に、会議資料ファイルのダウンロードの際の動作を説明する。ユーザ端末2-2から会議資料ファイル「PROPOSAL」を参照する際、ユーザ端末2-2の会議クライアントアプリケーション211は、遠隔会議サーバ4のファイル共有アプリケーション412への接続要求を行う。また、接続要求に伴って、ユーザ端末2-2及び遠隔会議サーバ4双方の監視手段22は、トンネルTUN[Group-1, P412]を確立する。

[0150] また、会議クライアントアプリケーション211からのファイル一覧要求に応じて、ファイル共有アプリケーション412は、2次記憶デバイス233に対してファイル一覧イベントを発行する。この場合、遠隔会議サーバ4の監視手段22は、前述の(C-2-1)会議資料ファイルの読み込みと同様の処理に従って、Group-1コンパートメントとPUBLICコンパートメントとのそれぞれに属するファイル配置テーブルをマージしたファイル配置テーブルFT[Group-1, PUBLIC]を生成する。また、監視手段22は、各FTレコードに記載されているファイル名を抽出して、ファイル共有アプリケーション412に渡す。そして、ファイル共有アプリケーション412は、渡されたファイル名一覧をユーザ端末2-2の会議クライアントアプリケーション211に応答する。

[0151] なお、ファイル配置テーブルFT[Group-1, PUBLIC]には、必ず「PROPOSAL」ファイルが存在し、且つその「PROPOSAL」ファイルのファイル実体はユーザ端末2-1からアップロードされた会議資料ファイルである。そのため、ユーザ端末2-2が「PROPOSAL」というファイル名で参照できるファイル実体も会議資料ファイルである。これは、前述の(C-2-1)会議資料ファイルの読み込み動作で述べたように、ファイル配置テーブルFT[Group-1]とFT[PUBLIC]とに同名のファイルが存在する場合であっても、ファイル配置テーブルFT[Group-1, PUBLIC]には、FT[Group-1]にある「PROPOSAL」ファイルのFTレコードが引き継がれるためである。

[0152] 従って、ユーザ端末2-2の会議クライアントアプリケーション211が「PROPOSAL」ファイルを遠隔会議サーバ4のファイル共有アプリケーション412からダウンロードしたときのそのダウンロードしたファイル実体は、確実に最新の会議資料ファイルとすることができる。また、ユーザ端末2-2にダウンロードされた会議資料ファイルは、ユーザ端末2-2の監視手段22によって、図27に示すように、会議クライアントアプリケーション211と同じGroup-1コンパートメントに格納される。

[0153] (D)遠隔会議以外でのグループメンバ間の情報共有時の動作

次に、遠隔会議以外でのグループメンバ間の情報共有の動作を説明する。以上の(A)～(C)の処理に従って、Group-1コンパートメントをもつ各ホストは、コンパートメント内のファイル実体を相互に共有できる。また、ファイル共有のための通信を行う場合、通信元及び通信先の2台のホスト間で相互認証を行うだけであり、いわゆる鍵サーバ等の第三者サーバを必要としない。

[0154] 上記のファイル共有や相互認証の性質を利用すると、遠隔会議に参加しなかったGroup-1メンバに対して、ユーザ端末同士による直接通信を行うことによって、会議資料ファイルを配布することができる。以下、本実施例では、例えば、ユーザ端末2-3は、遠隔会議に参加しなかったGroup-1メンバが使用する端末であるものとする。

[0155] ユーザ端末2-2は、遠隔会議でダウンロードした会議資料ファイルを、Group-1コンパートメント内に格納している。この場合、会議後に、ユーザ端末2-2を用いるユーザがユーザ端末2-3を用いるユーザと出会った際に、その会議資料ファイルを配布する場合を考える。本実施例では、ユーザ端末2-2及びユーザ端末2-3は、相互にファイル転送を行うことができるファイル交換アプリケーション213をインストールされている。また、ユーザ端末2-2及びユーザ端末2-3のファイル交換アプリケーション213は、共にGroup-1コンパートメントに属するオブジェクトとして既に起動されている。

[0156] まず、ユーザ端末2-2のファイル交換アプリケーション213は、ユーザ端末2-3のファイル交換アプリケーション213への接続要求イベントを発行する。この場合、ユーザ端末2-2及びユーザ端末2-3のそれぞれの監視手段22の間で、Group-1の認証キーを用いた相互認証を行い、トンネルTUN[Group-1, P213]を確立する。

なお、P213は、ファイル交換アプリケーション213がリスンしている待ち受けポートを示す。

[0157] また、ユーザ端末2-2のファイル交換アプリケーション213は、ユーザ端末2-3のファイル交換アプリケーション213に会議資料ファイルを転送する。そして、ユーザ端末2-3のファイル交換アプリケーション213は、図28に示すように、転送された会議資料ファイルを、Group-1コンパートメントに属するファイルとして、2次記憶デバイス233に格納する。

[0158] 仮に、Group-1に属さないユーザ端末2-4は、ユーザ端末2-2のファイル交換アプリケーション213から会議資料ファイルを取得しようとしても、ユーザ端末2-2及びユーザ端末2-4それぞれの監視手段22間で相互認証に失敗する。そのため、ユーザ端末2-2のファイル交換アプリケーション213は、会議資料ファイルを転送できない。

[0159] また、ユーザ端末2-3がGroup-1とは別のグループGroup-2にも属している場合を考える。この場合、Group-2だけに属するユーザ端末2-5に会議資料ファイルを転送しようとしても、ユーザ端末2-3上で会議資料ファイルにアクセス可能なアプリケーション21は、Group-1コンパートメントに属するオブジェクトに限られる。そのため、ユーザ端末2-3及びユーザ端末2-5のそれぞれの監視手段22間で相互認証に失敗するので、ユーザ端末2-5に会議資料ファイルを転送することができない。このことは、Group-1コンパートメントとGroup-2コンパートメントとで、同じファイル交換アプリケーション213が動作している場合にも当てはまる。

[0160] 従って、同一グループに属するユーザ端末2同士は、その共有方法にかかわらず、自由に共有可能であるとともに、グループに属さないユーザ端末への漏洩を発生しないようにできる。

[0161] (実施の形態2)

次に、本発明の第2の実施の形態を図面を参照して説明する。図29は、グループ管理サーバ1及びユーザ端末2の他の構成例を示すブロック図である。図29に示すように、本実施の形態では、グループ管理サーバ1は、第1の実施の形態で示したグループ管理サーバ1の構成要素に加えて、グループ変更手段13とグループ関係計

算手段14とを備える。また、本実施の形態では、ユーザ端末2の監視手段22は、第1の実施の形態で示したコンパートメント生成手段221に代えて、コンパートメント再編指示手段225を備える。

[0162] グループ変更手段13及びグループ関係計算手段14は、具体的には、プログラムに従って動作するグループ管理サーバ1のCPUによって実現される。グループ変更手段13は、通信インタフェース手段11がいずれかのユーザ端末2から新たなグループへの参加やグループの脱退等のグループ所属変更要求を受信すると、グループ管理データベース12を更新して、グループ構成を変更する機能を備える。

[0163] グループ関係計算手段14は、通信インタフェース手段11がいずれかのユーザ端末2からメンバIDを受信すると、グループ管理データベース12に基づいて、受信したメンバIDを含む全てのグループを参照する機能を備える。また、グループ関係計算手段14は、グループ管理データベース12から、ユーザ端末2に応答すべき全てのグループIDと認証キーとの系列(グループID／認証キー系列という)を抽出する機能を備える。また、グループ関係計算手段14は、グループ間の包含関係に基づいて、グループ間の隣接関係や包含関係を示す行列であるグループ隣接行列を生成する機能を備える。また、グループ関係計算手段14は、グループID／認証キー系列及びグループ隣接行列を、通信インタフェース手段11及びネットワーク3を介してユーザ端末2に応答(送信)する機能を備える。

[0164] コンパートメント再編指示手段225は、グループ管理サーバ1から配布されたグループID／認証キー系列を、ネットワーク3、デバイス制御手段224及びネットワークデバイス231を介して受信する機能を備える。また、コンパートメント再編指示手段225は、配布されたグループID／認証キー系列及びグループ隣接行列に基づいて、コンパートメント構成グラフGの構成変更を、コンパートメント構成管理手段223に指示する機能を備える。

[0165] なお、本実施の形態では、グループ管理サーバ1がグループ関係計算手段14を備える場合を説明するが、ユーザ端末2がグループ関係計算手段14を備えるようにしてもよい。この場合、ユーザ端末2は、グループ関係計算手段14を用いてグループ隣接行列を生成し、生成したグループ隣接行列に基づいてコンパートメントを再編す

る。

[0166] 次に、動作について説明する。まず、グループを変更するグループ変更処理の動作を説明する。図30は、グループ管理サーバ1が行うグループ変更処理の一例を示す流れ図である。まず、ユーザ端末2のユーザは、グループ変更を行いたい場合、ユーザ端末2を操作してグループ管理サーバ1への接続を指示する。グループ変更を行いたいユーザのユーザ端末2は、ネットワーク3を介してグループ管理サーバ1に接続する。そして、ユーザ端末2は、変更操作の識別子(追加や削除等)と、グループIDと、ユーザのメンバIDとを少なくとも含むグループ変更要求を送信する。すると、グループ管理サーバ1は、ネットワーク3を介してグループ変更要求を受信する(ステップS71)。

[0167] グループ変更要求は、通信インタフェース手段11を介して、グループ変更手段13に伝達される。グループ変更手段13は、通信インタフェース手段11からグループ変更要求を入力すると、グループ変更要求の操作識別子に基づいて、変更要求の種別がグループの「追加」であるか「削除」であるかを判定する(ステップS72)。その結果、「追加」であるか「削除」であるかの判定結果に従って、以下のようにグループ追加又はグループ削除の変更処理に移行する。

[0168] (A)グループ追加の変更処理

まず、グループを追加する場合の変更処理を説明する。グループ変更要求の操作識別子が「追加」である場合、グループ変更手段13は、グループ変更要求に含まれるグループIDをキーとして、グループ管理データベース12のレコードを検索する。そして、グループ変更手段13は、グループ管理データベース12に、グループIDに対応するレコードが含まれるか否かを判断する(ステップS73)。

[0169] その結果、対応するレコードがない場合、グループ変更手段13は、新規レコードをグループ管理データベース12に作成する(ステップS74)。この場合、グループ変更手段13は、新規認証キーをランダムに生成し、グループ変更要求に含まれるグループID及びメンバIDと対応付けて、生成した新規レコードに格納する。例えば、グループ変更手段13は、乱数を用いて、認証キーをランダムに生成する。なお、新規に認証キーを生成する際、グループ変更手段13は、グループ管理データベース12のい

ずれの認証キーとも異なるキーを生成する。

[0170] 一方、ステップS73でレコードを検索できた場合(グループIDに対応するレコードがあった場合)、グループ変更手段13は、対応するレコードに、新たなメンバIDとして、グループ変更要求に含まれるメンバIDを追加し、グループ変更処理を終了する(ステップS75)。

[0171] (B)グループ削除の変更処理

次に、グループを削除する場合の変更処理を説明する。グループ変更要求の操作識別子が「削除」である場合、グループ変更手段13は、グループ変更要求に含まれるグループIDとメンバIDとに基づいて、グループ管理データベース12からグループIDに対応するレコードを抽出する。そして、グループ変更手段13は、グループ変更要求に含まれるメンバIDを、抽出したレコードから削除する(ステップS76)。

[0172] 次いで、グループ変更手段13は、メンバID削除後のレコードにメンバIDが1つ以上含まれているか否かを判断する(ステップS77)。その結果、1つ以上のメンバIDが含まれていると判断すると、グループ変更手段13は、直ちにグループ変更処理を終了する。一方、レコードにいかなるメンバIDも含まれていないと判断すると、グループ変更手段13は、レコードをグループ管理データベース12から削除して、グループ変更処理を終了する(ステップS78)。

[0173] 次に、コンパートメントを再構成するコンパートメント再編処理の動作を説明する。以下、コンパートメント再編処理を行う際に、グループ管理サーバ1が行う処理とユーザ端末2が行う処理とに分けて説明する。

[0174] (A)グループ管理サーバの処理

まず、グループ管理サーバ1が行う処理を説明する。図31は、グループ管理サーバ1のグループ関係計算手段14がグループ間の関係を計算するグループ関係計算処理の一例を示す流れ図である。同図において、ユーザ端末2のコンパートメント再編指示手段225は、例えばユーザ端末2の起動時等に、ネットワーク3、ネットワークデバイス231及びデバイス制御手段224を介して、メンバIDをグループ管理サーバ1に送信する。すると、グループ管理サーバ1の通信インタフェース手段11は、ユーザ端末2からメンバIDを受信する(ステップS81)。

- [0175] 次いで、通信インタフェース手段11は、受信したメンバIDをグループ関係計算手段14に伝達(出力)する。すると、グループ関係計算手段14は、入力したメンバIDを含む全てのレコードを、グループ管理データベース12から抽出する(ステップS82)。また、グループ関係計算手段14は、抽出した各レコードに基づいて、グループID／認証キー系列を生成する(ステップS83)。
- [0176] 次いで、グループ関係計算手段14は、抽出したグループID／認証キー系列に含まれるグループ間の順序関係を示す隣接行列を生成する(ステップS84)。そして、グループ関係計算手段14は、生成したグループID／認証キー系列と隣接行列とを、通信インタフェース手段11及びネットワーク3を介して、ユーザ端末2のコンパートメント再編指示手段225に応答(送信)する(ステップS85)。
- [0177] ここで、ステップS84において隣接行列を算出する処理を説明する。図32は、グループ関係計算手段14が隣接行列を計算して求める隣接行列計算処理の一例を示す流れ図である。同図において、まず、グループ関係計算手段14は、ステップS82で抽出したレコード系列のレコード数がNである場合、 $N \times N$ の隣接行列を生成し、生成した行列の各値を0に初期化する(ステップS841)。すなわち、グループ関係計算手段14は、まず隣接行列の初期行列を生成する。
- [0178] 次いで、グループ関係計算手段14は、レコード系列中の各レコードに基づいて、それぞれのメンバID集合に含まれるID数をカウントする。そして、求めたID数の昇順にレコード系列をソートして、ソート済みレコード系列RSを求める(ステップS842)。次いで、グループ関係計算手段14は、レコード系列RSのレコード数をカウントして、レコード数が0か否かをテスト(判断)する(ステップS843)。その結果、レコード系列RSのレコード数が0であると判断すると、グループ関係計算手段14は、直ちに計算処理を終了する。
- [0179] 一方、レコード系列RSに少なくとも1以上のレコードが含まれると判断すると、グループ関係計算手段14は、レコード系列RSの先頭レコードRS[0]を所定の変数rに一時退避(格納)し、先頭レコードRS[0]をレコード系列RSから削除する(ステップS844)。そして、グループ関係計算手段14は、変数rのメンバID集合M1と、レコード系列RSの各レコードRS[i]のメンバID集合M2とを抽出し、それらメンバID集合M1

とM2との包含関係を以下の手順に従って比較する(ステップS845)。

- [0180] まず、グループ関係計算手段14は、メンバID集合M1がM2に「真」に含まれるか否か、すなわち、 $M1 \subset M2$ であるか否かをテスト(判断)する(ステップS846)。その結果、 $M1 \subset M2$ であると判断すると、グループ関係計算手段14は、変数rのグループID( $r[G]$ )と、レコードRS[i]のグループID( $RS[i][G]$ )とについて、隣接行列中のr[G]行RS[i][G]列に位置する値( $r[G]$ ,  $RS[i][G]$ )を1に設定し(ステップS847)、ステップS843に戻る。
- [0181] 一方、 $M1 \subset M2$ でないと判断すると、グループ関係計算手段14は、 $M1 = M2$ であるか否かをテスト(判断)する(ステップS848)。その結果、 $M1 = M2$ であると判断すると、グループ関係計算手段14は、行列要素( $r[G]$ ,  $RS[i][G]$ )と( $RS[i][G]$ ,  $r[G]$ )との2つの値を1に設定し(ステップS849)、ステップS843に戻る。
- [0182] 以上のように、ステップS841～S849までの処理が実行されることによって、ユーザ端末2のメンバIDを含む任意のグループについて、メンバ構成の包含関係及び同値関係を隣接行列として符号化することができる。
- [0183] (B)ユーザ端末の処理
- 次に、ユーザ端末2が行う処理を説明する。図33は、コンパートメント再編指示手段225がコンパートメントの再編を指示する処理の一例を示す流れ図である。同図において、ステップS84で隣接行列を生成すると、ユーザ端末2のコンパートメント再編指示手段225は、グループID／認証キー系列と隣接行列とを、ネットワーク3、ネットワークデバイス231及びデバイス制御手段224を介して、グループ管理サーバ1から受信する(ステップS91)。次いで、コンパートメント再編指示手段225は、第1の実施の形態で示したコンパートメント生成指示手段222と同様に、グループID／認証キー系列に含まれるそれぞれのグループIDと認証キーとの組に基づいて、コンパートメントノードの生成を指示する(ステップS92)。
- [0184] 次いで、コンパートメント再編指示手段225は、生成した各コンパートメントノードを、コンパートメント構成管理手段223が管理するコンパートメント構成グラフGに登録させる。この場合、コンパートメント再編指示手段225は、隣接行列に基づいて、登録したコンパートメントノード間の有向辺の付加を指示する(ステップS93)。

- [0185] 図34は、コンパートメントノードのコンパートメント構成グラフへの登録処理の具体例を示す流れ図である。同図において、コンパートメント再編指示手段225は、より具体的には、図34に示すように、ステップS92で生成したコンパートメントノードN[C1]の登録を、第1の実施の形態におけるコンパートメント生成指示手段221と同様に、コンパートメント構成管理手段223に指示する(ステップS931)。
- [0186] 次いで、コンパートメント再編指示手段225は、未登録コンパートメントノードがまだ存在するか否かを判断する(ステップS932)。その結果、未登録コンパートメントノードがないと判断すると、コンパートメント再編指示手段225は、直ちにステップS939の処理に遷移する。
- [0187] 一方、未登録コンパートメントが存在すると判断すると、コンパートメント再編指示手段225は、(2つ目以降の)未登録コンパートメントノードN[Cn]を、コンパートメント構成グラフGに登録させる(ステップS933)。また、コンパートメント再編指示手段225は、これまでに登録した各コンパートメントノードN[Ck]について、隣接行列の(Cn, Ck)及び(Ck, Cn)の値を参照する(ステップS934)。
- [0188] 次いで、コンパートメント再編指示手段225は、(Cn, Ck)の値が1であるか否かを判断する(ステップS935)。その結果、(Cn, Ck)の値が1であると判断すると、N[Ck]からN[Cn]に向かう有向辺を付加させ(ステップS936)、ステップS932に戻る。一方、(Cn, Ck)の値が1でないと判断すると、(Ck, Cn)の値が1であるか否かを判断する(ステップS937)。その結果、(Ck, Cn)の値が1であると判断すると、コンパートメント再編指示手段225は、N[Cn]からN[Ck]に向かう有向辺を付加させ(ステップS938)、ステップS932に戻る。一方、(Ck, Cn)の値が1でないと判断すると、ステップS932に戻る。
- [0189] 上記のステップS932にて、未登録コンパートメントノードがないと判断すると、コンパートメント再編指示手段225は、その時点でのコンパートメント構成グラフGにおいてN[Cn]に接続されている全ての有向辺を逐次参照し、N[Cn]に向かう有向辺の有無を判断する。有向辺がないと判断すると、コンパートメント再編指示手段225は、最下位レベルのコンパートメントノードN[C0]からN[Cn]への有向辺の付加を指示する(ステップS939)。

- [0190] 次いで、有向辺を追加させると、図33に示すように、コンパートメント再編指示手段225は、第1の実施の形態で示したコンパートメント生成手段221と同様に、登録した各コンパートメントノードN[Cn]について、オブジェクトツリーOT[Cn]とファイル配置テーブルFT[Cn]とを新たに生成指示する。そして、コンパートメント再編指示手段225は、生成したオブジェクトツリーOT[Cn]及びファイル配置テーブルFT[Cn]を、コンパートメントノードN[Cn]の属性として登録させる(ステップS94)。
- [0191] 以上のように、図33のステップS91～S94(図34のステップS931～S939を含む)までの処理が実行される。これによって、ユーザ端末2のコンパートメント構成管理手段223が管理するコンパートメント構成グラフGの構造が、あるグループGnに対応するコンパートメントCnと、そのグループGnに包含されるグループGmに対応するコンパートメントCmとについて、それぞれの機密レベルが $C_n < C_m$ の関係を満たすようにできる。すなわち、グループGn内で共有される任意の情報はグループGmでも共有可能にできるが、その逆にグループGm内で共有される任意の情報はグループGnでは共有可能にできない。これにより、グループGmからグループGnへの情報の流れを禁止できる。
- [0192] 例えば、情報共有システムを用いれば、図35に示すように、組織の包含関係に合わせて、コンパートメント構成グラフを自動的に構築することができる。具体的には、図35に示す例では、「〇〇営業部」のメンバは、「〇〇営業部」限定の情報を共有できるだけでなく、「営業本部」及び「会社全体」という上位組織の情報も共有することができる。しかし、「〇〇営業部」と「××事業部」とのように包含関係が成り立たない組織間では、例え双方の組織を兼務するメンバであっても、双方で限定的に共有される情報を漏洩させることができない。
- [0193] 以上のように、本実施の形態によれば、グループ管理サーバ1のグループ関係計算手段14は、各ユーザが所属する任意のグループを抽出するとともに、グループ間の包含関係を計算して隣接行列を生成する。また、ユーザ端末2のコンパートメント再編手段225は、各グループに対応するコンパートメントを生成するとともに、隣接行列に基づいて、より部分的なグループのコンパートメントの機密レベルが、そのグループを含むより広範なグループのコンパートメントの機密レベルよりも必ず高くなるよう

に設定する。

- [0194] そのようにすることにより、任意の部分グループのユーザが、部分グループで限定的に共有される情報を自由に編集しながら、より広範なグループで共有される情報についても参照や編集する等して、部分グループ内へ取り込んで共有できるようにすることができる。また、包含関係を持たない無関係なグループに対しては一切情報をやり取りできないようにすることができる。従って、グループ内部で閉じた情報共有を行うことに加えて、より広範なグループとその部分グループとの間での自由な情報共有を実現しながら、無関係なグループへの機密漏洩を防止することができる。

- [0195] （実施の形態3）

次に、本発明の第3の実施の形態を図面を参照して説明する。図36は、ユーザ端末2の更に他の構成例を示すブロック図である。図36に示すように、本実施の形態では、ユーザ端末2の監視手段22は、第1の実施の形態で示した監視手段22の構成要素に加えて、コンパートメント切替手段226を備える。また、ユーザ端末2は、第1の実施の形態で示した各種デバイスに加えて、デバイス23として表示デバイス234及び入力デバイス235を含む。

- [0196] 表示デバイス234は、具体的には、ユーザ端末2のCRT等の表示装置である。また、入力デバイス235は、具体的には、キーボード・マウス等の入力装置である。表示デバイス234と入力デバイス235とは、デバイス制御部224を介して、コンパートメント切替手段226に接続されている。コンパートメント切替手段226は、ユーザによって入力デバイス235から所定の入力となされると、デバイス制御手段224を介して、表示デバイス234にコンパートメント切替ダイアログを表示させる機能を備える。また、コンパートメント切替手段226は、ユーザからのコンパートメント切替操作に従って、コンパートメント構成管理手段223にコンパートメント切替要求を伝達(出力)する機能を備える。

- [0197] 次に、本実施の形態の動作について説明する。図37は、本実施の形態において、コンパートメント切替手段226がコンパートメントの切り替えを行うコンパートメント切替処理の一例を示す流れ図である。同図において、ユーザは、ユーザ端末2の入力デバイス235を用いて、コンパートメント切り替えのための所定の入力指示(例えば、キ

一押下等)を行う。コンパートメント切替手段226は、ユーザの指示操作に従って、コンパートメント切替入力を受け付ける(ステップS101)。すると、コンパートメント切替手段226は、表示デバイス234に、コンパートメントの切り替え操作をするためのコンパートメント切替ダイアログを表示させる(ステップS102)。

[0198] 図38は、ユーザ端末2が表示するコンパートメント切替ダイアログの例を示す説明図である。コンパートメント切替ダイアログには、例えば、図38に示すように、少なくともコンパートメント構成管理手段223が管理する全てのコンパートメントについて、それぞれの識別子であるグループIDの一覧と、それぞれのコンパートメントに属するオブジェクトツリーで管理されているアプリケーション21の一覧とが含まれる。

[0199] 次いで、ユーザは、さらに入力デバイス235を操作して、コンパートメント切替の対象とするアプリケーション21を選択指示し、切替先のコンパートメントを指定する。コンパートメント切替手段226は、ユーザの指示操作に従って、アプリケーション21を選択し、切替先のコンパートメントを入力する(ステップS103)。

[0200] なお、切替先コンパートメントの指定時に、コンパートメント切替手段226は、切替先コンパートメントCnの機密レベルがアプリケーション21が現在属しているコンパートメントCmの機密レベル以上であることを判定し確認するようにすることが望ましい。そして、切替先コンパートメントCnの機密レベルがコンパートメントCmの機密レベル以上でない場合、コンパートメント切替手段226は、エラーメッセージを表示させて、ステップS103の処理に戻るようにすることが望ましい。この場合、コンパートメント切替手段226は、コンパートメント間の機密レベルの比較を、コンパートメント構成グラフGにおいて、コンパートメントN[Cm]からコンパートメントノードN[Cn]に有向辺を辿って到達可能であるか否かを判断することにより行えばよい。

[0201] 次いで、コンパートメント切替手段226は、切替対象のアプリケーション21の選択と切替先コンパートメントとを入力すると、アプリケーション21のオブジェクトノードの現在のオブジェクトツリーからの削除を、コンパートメント構成管理手段223に指示する(ステップS104)。そして、コンパートメント切替手段226は、切替対象アプリケーションを、切替先コンパートメントのオブジェクトツリーに登録させる(ステップS105)。

[0202] 具体的には、図39に示すように、監視手段22は、アプリケーション21のオブジェク

トノードONについて、現在のオブジェクトツリーOT1における親ノードへのリンクを削除し、全ての子ノードを親ノードの新たな子ノードとしてOT1に再登録する。そして、監視手段22は、オブジェクトノードONを、切替先コンパートメントに属するオブジェクトツリーOT2の根ノードの新たな子ノードとして登録する。

[0203] 以上のように、ステップS101～S105までの処理が実行されることによって、ユーザは、現在作業中のコンパートメントを容易に把握できるとともに、アプリケーション21毎に作業コンパートメントを明示的に指定することができる。

[0204] なお、ステップS102において、図40に示すように、コンパートメント切替手段226は、コンパートメント切替ダイアログに、各コンパートメント毎のファイル一覧をアプリケーション21の一覧と併せて表示させるようにしてもよい。そのようにすれば、どの情報がどのコンパートメントに属するかを、ユーザが簡単に確認することができる。

#### 産業上の利用可能性

[0205] 本発明は、社内文書ファイルを共有するためのファイルサーバ装置や、ファイルサーバ装置をコンピュータを用いて実現するためのプログラムの用途に適用できる。また、本発明は、ネットワークを介して相互にファイルを交換／共有するファイル交換装置や、ファイル交換装置をコンピュータを用いて実現するためのプログラムの用途にも適用できる。

## 請求の範囲

- [1]      グループ内で情報を共有するためのコンピュータを用いた情報共有システムであつて、
- 前記グループと当該グループに属するメンバとの対応関係を管理し、前記メンバを識別するためのメンバ識別情報を入力すると、少なくとも1以上の前記グループを識別するためのグループ識別情報を出力するグループ管理手段と、
- 前記グループ識別情報に基づいて、前記コンピュータ内のソフトウェア及びファイルを含む計算資源を前記グループに対応付けて割り当てるための仮想的に区画化されたグループ専用領域であり且つ前記グループ間で互いの関係が解析可能に構成されたコンパートメントを生成するコンパートメント生成手段と、
- 前記計算資源にアクセスするアプリケーションソフトウェアの動作を監視して、前記コンパートメントと前記アプリケーションソフトウェアとの所属関係を解析し、その解析結果に基づいて前記アプリケーションソフトウェアと前記計算資源との間の入出力処理の実行可否を制御する監視手段とを有することを特徴とする情報共有システム。
- [2]      前記グループ管理手段は、サーバに設けられ、
- 前記コンパートメント生成手段及び前記監視手段は、前記サーバに通信ネットワークを介して通信可能に接続されるユーザ端末に設けられ、
- 前記グループ管理手段は、前記グループを識別するためのグループ識別情報と、前記メンバを識別するためのメンバ識別情報とを対応付けて蓄積し、前記ユーザ端末から前記メンバ識別情報を受信すると、受信した前記メンバ識別情報に対応する前記グループ識別情報を抽出し、抽出した前記グループ識別情報を、前記通信ネットワークを介して前記ユーザ端末に送信し、
- 前記コンパートメント生成手段は、前記グループ識別情報に基づいて前記グループに対応する前記コンパートメントを生成し、
- 前記監視手段は、前記ユーザ端末が搭載するアプリケーションソフトウェアの動作を監視して、前記アプリケーションソフトウェアのイベントを検出したときに、前記イベントを検出したアプリケーションソフトウェアが属する前記コンパートメントを特定し、特定した前記コンパートメントに基づいて前記アプリケーションソフトウェアと前記計算資

源との間の前記イベントに応じた入出力処理の実行可否を制御することを特徴とする請求項1記載の情報共有システム。

- [3] 前記グループ管理手段は、前記メンバ識別情報に基づいて、少なくとも1つ以上のグループIDと認証キーとの組を前記グループ識別情報として出力する請求項1又は請求項2記載の情報共有システム。
- [4] 前記監視手段は、前記入出力処理の実行可否として、ファイル入出力イベント及びネットワーク入出力イベントの少なくとも一方の実行可否を制御する請求項1から請求項3のうちのいずれか1項に記載の情報共有システム。
- [5] 前記コンパートメント生成手段は、前記グループ識別情報に基づいて、所定の構成情報を生成することによって前記コンパートメントを生成する請求項2から請求項4のうちのいずれか1項に記載の情報共有システム。
- [6] 前記グループ管理手段は、前記グループと当該グループとは別のグループとの包含関係を示す隣接行列を生成する手段を含み、  
前記コンパートメント生成手段は、前記隣接行列に基づいて、生成した前記コンパートメント間に有向辺を付加することによって、前記コンパートメント間の順序関係を設定する手段を含む請求項1から請求項5のうちのいずれか1項に記載の情報共有システム。
- [7] 前記監視手段は、少なくとも前記コンパートメントと前記アプリケーションソフトウェアとの所属関係の情報を含むデータ構造のグラフとして、ノードとそのノード間を結ぶ辺から成るコンパートメント構成グラフを解析可能に管理する手段を含む請求項1から請求項6のうちのいずれか1項に記載の情報共有システム。
- [8] 前記監視手段は、前記コンパートメント構成グラフに基づいて、前記アプリケーションソフトウェアがアクセスできるファイルの範囲を、当該アプリケーションソフトウェアが属する前記コンパートメントと、当該コンパートメントに対して下位の関係にある下位コンパートメントとのいずれかに属するファイルに限定する手段を含む請求項7記載の情報共有システム。
- [9] 前記監視手段は、前記コンパートメント構成グラフに基づいて、前記アプリケーションソフトウェアが同一のホストコンピュータ内でメッセージを送信できる範囲を、当該ア

アプリケーションソフトウェアが属するコンパートメントと、当該コンパートメントに対して下位の関係にある下位コンパートメントのいずれかに属するアプリケーションソフトウェアとに限定する手段を含む請求項7又は請求項8記載の情報共有システム。

[10] 前記監視手段は、前記コンパートメント構成グラフに基づいて、前記アプリケーションソフトウェアが同一のホストコンピュータ内、又はネットワークを介して接続される当該ホストコンピュータとは別のホストコンピュータにメッセージを送信できる範囲を、同一のコンパートメントに属するアプリケーションソフトウェアに限定する手段を含む請求項7から請求項9のうちのいずれか1項に記載の情報共有システム。

[11] 前記監視手段は、前記メンバを構成するユーザからの指示に応じて、前記アプリケーションソフトウェアが属する前記コンパートメントの変更、及び前記コンパートメントごとのファイル管理を行う手段を含む請求項1から請求項10のうちのいずれか1項に記載の情報共有システム。

[12] 前記グループ管理手段は、前記グループの新規作成、前記グループの抹消、前記メンバの追加、及び前記メンバの削除の少なくとも1つを行う手段を含む請求項1から請求項11のうちのいずれか1項に記載の情報共有システム。

[13] グループ内で情報を共有するための情報共有システムで用いるサーバであって、前記グループと当該グループに属するメンバとの対応関係を管理するグループ管理手段を備え、

前記グループ管理手段は、前記メンバを識別するためのメンバ識別情報を入力すると、少なくとも1以上のグループIDと認証キーとの組を出力することを特徴とする情報共有システムのサーバ。

[14] 前記グループ管理手段は、前記グループと当該グループとは別のグループとの包含関係を示す隣接行列を生成する手段をさらに備えた請求項13記載の情報共有システムのサーバ。

[15] グループ内で情報を共有するための情報共有システムで用いるユーザ端末であって、

前記グループを識別するグループIDと認証キーとの各組に対応して、前記ユーザ端末を構成するコンピュータ内のソフトウェア及びファイルを含む計算資源をグルー

プに対応付けて割り当てるための仮想的に区画化されたグループ専用領域であり且つ前記グループ間で互いの関係が解析可能に構成されたコンパートメントを生成するコンパートメント生成手段と、

前記計算資源にアクセスするアプリケーションソフトウェアの動作を監視する監視手段とを備え、

前記監視手段は、前記コンパートメントと前記アプリケーションソフトウェアとの所属関係を解析し、その解析結果に基づいて、ファイル入出力イベント及びネットワーク入出力イベントの少なくとも一方の実行可否を制御することを特徴とする情報共有システムのユーザ端末。

- [16] 前記グループと当該グループとは別のグループとの包含関係を示す隣接行列を生成する手段と、

前記隣接行列に基づいて、前記コンパートメント間に有向辺を付加することによって、前記コンパートメント間の順序関係を設定する手段とをさらに備えた請求項15記載の情報共有システムのユーザ端末。

- [17] サーバと、このサーバに通信ネットワークを介して通信可能に接続されたユーザ端末とを備えた情報共有システムを用いて、グループ内で情報を共有する情報共有方法であって、

前記サーバが、前記グループと当該グループに属するメンバとの対応関係を管理し、前記メンバを識別するためのメンバ識別情報を入力すると、少なくとも1以上のグループIDと認証キーとの組を、前記通信ネットワークを介して前記ユーザ端末に送信するステップと、

前記ユーザ端末が、前記サーバから受信したグループIDと認証キーとの各組に対応して、前記コンピュータ内のソフトウェア及びファイルを含む計算資源を前記グループに対応付けて割り当てるための仮想的に区画化されたグループ専用領域であり且つ前記グループ間で互いの関係が解析可能に構成されたコンパートメントを生成するステップと、

前記ユーザ端末が、前記コンパートメント間の順序関係、前記コンパートメントとアプリケーションソフトウェアとの所属関係、及び前記コンパートメントとファイルとの所属

関係の少なくとも1つの情報を含むデータ構造のグラフとして、コンパートメント構成グラフを生成するステップと、

前記ユーザ端末が、前記アプリケーションソフトウェアの動作を監視して、前記コンパートメント構成グラフに基づいて、ファイル入出力イベント及びネットワーク入出力イベントの少なくとも一方の実行可否を制御するステップとを含むことを特徴とする情報共有方法。

- [18] 前記サーバが、前記メンバ識別情報を入力すると、前記グループと当該グループとは別のグループとの包含関係を示す隣接行列を生成するステップと、

前記サーバが、前記グループIDと認証キーとの組とともに、前記生成した隣接行列を、前記通信ネットワークを介して前記ユーザ端末に送信するステップと、

前記ユーザ端末が、前記サーバから受信したグループIDと認証キーとの各組及び前記隣接行列に基づいて、前記コンパートメント間の順序関係、前記コンパートメントとアプリケーションソフトウェアとの所属関係、及び前記コンパートメントとファイルとの所属関係の少なくとも1つの情報を含むデータ構造のグラフとして、ノードとそのノードを結ぶ辺から成るコンパートメント構成グラフを生成するステップと、

前記ユーザ端末が、前記アプリケーションソフトウェアの動作を監視して、前記コンパートメント構成グラフに基づいて、一のグループの前記コンパートメントに属する情報に対して、当該グループを包含する他のグループの前記コンパートメントに属するアプリケーションソフトウェアからの読み込みアクセスを許可するように、前記アプリケーションソフトウェアの実行可否を制御するステップとを含む請求項17記載の情報共有方法。

- [19] グループ内で情報を共有するための情報共有システムで用いるプログラムであって、

コンピュータに、前記グループと当該グループに属するメンバとの対応関係を管理し、前記メンバを識別するためのメンバ識別情報を入力すると、少なくとも1以上のグループIDと認証キーとの組を生成する処理を実行させるためのグループ管理プログラム。

- [20] 前記コンピュータに、前記グループと当該グループとは別のグループとの包含関係

を示す隣接行列を生成する処理をさらに実行させる請求項19記載のグループ管理プログラム。

- [21]      グループ内で情報を共有するための情報共有システムで用いるプログラムであって、

コンピュータに、

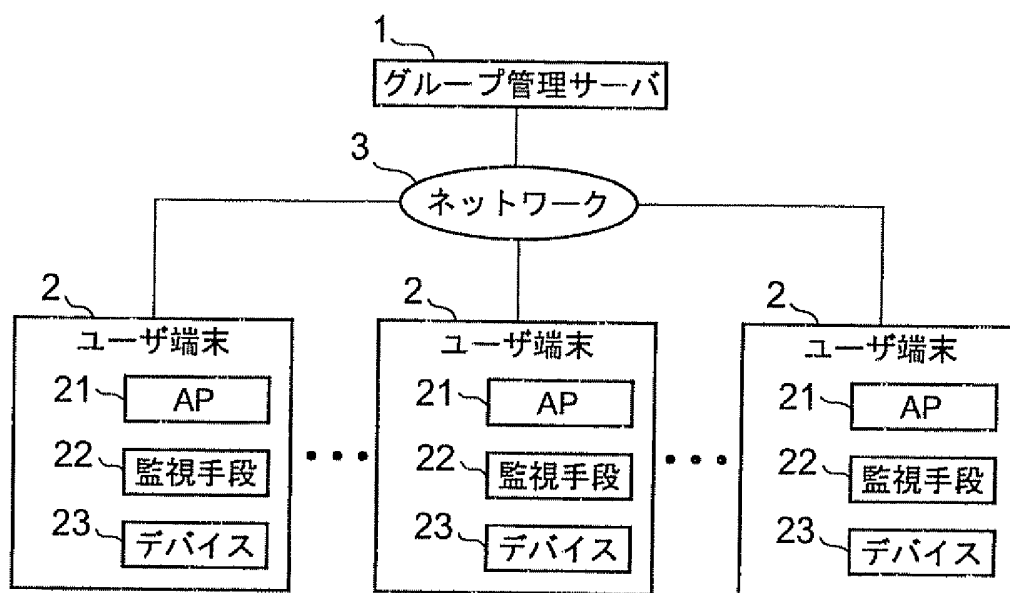
前記グループを識別するためのグループIDと認証キーとの各組に対応して、前記コンピュータ内のソフトウェア及びファイルを含む計算資源を前記グループに対応付けて割り当てるための仮想的に区画化されたグループ専用領域であり且つ前記グループ間で互いの関係が解析可能に構成されたコンパートメントを生成する処理と、

前記コンパートメント間の順序関係、前記コンパートメントとアプリケーションソフトウェアとの所属関係、及び前記コンパートメントとファイルとの所属関係の少なくとも1つの情報を含むデータ構造のグラフとして、ノードとそのノードを結ぶ辺から成るコンパートメント構成グラフを生成する処理と、

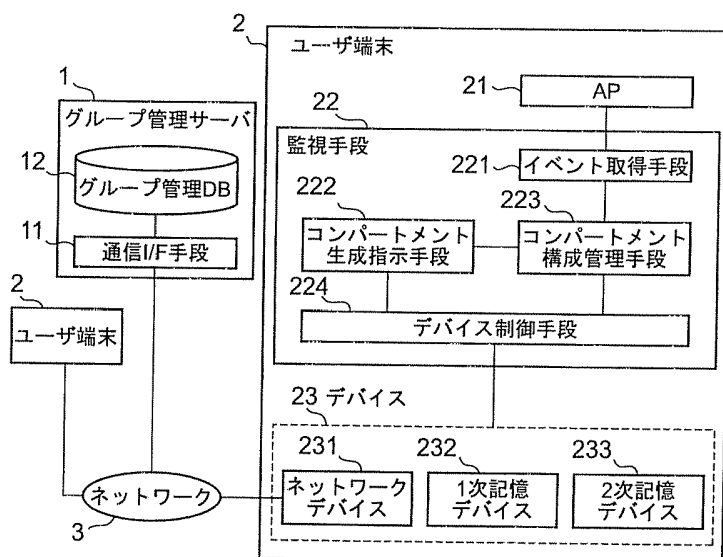
前記アプリケーションソフトウェアの動作を監視して、前記コンパートメント構成グラフに基づいて、ファイル入出力イベント及びネットワーク入出力イベントの少なくとも一方の実行可否を制御する処理とを実行させるためのコンパートメント管理プログラム。

- [22]      前記コンパートメント構成グラフと生成する処理は、前記グループIDと認証キーとの各組と共に、前記グループと当該グループとは別のグループとの包含関係を示す隣接行列を入力し、前記グループIDと認証キーとの各組及び前記隣接行列に基づいて前記コンパートメント構成グラフを生成する処理を含む請求項21記載のコンパートメント管理プログラム。

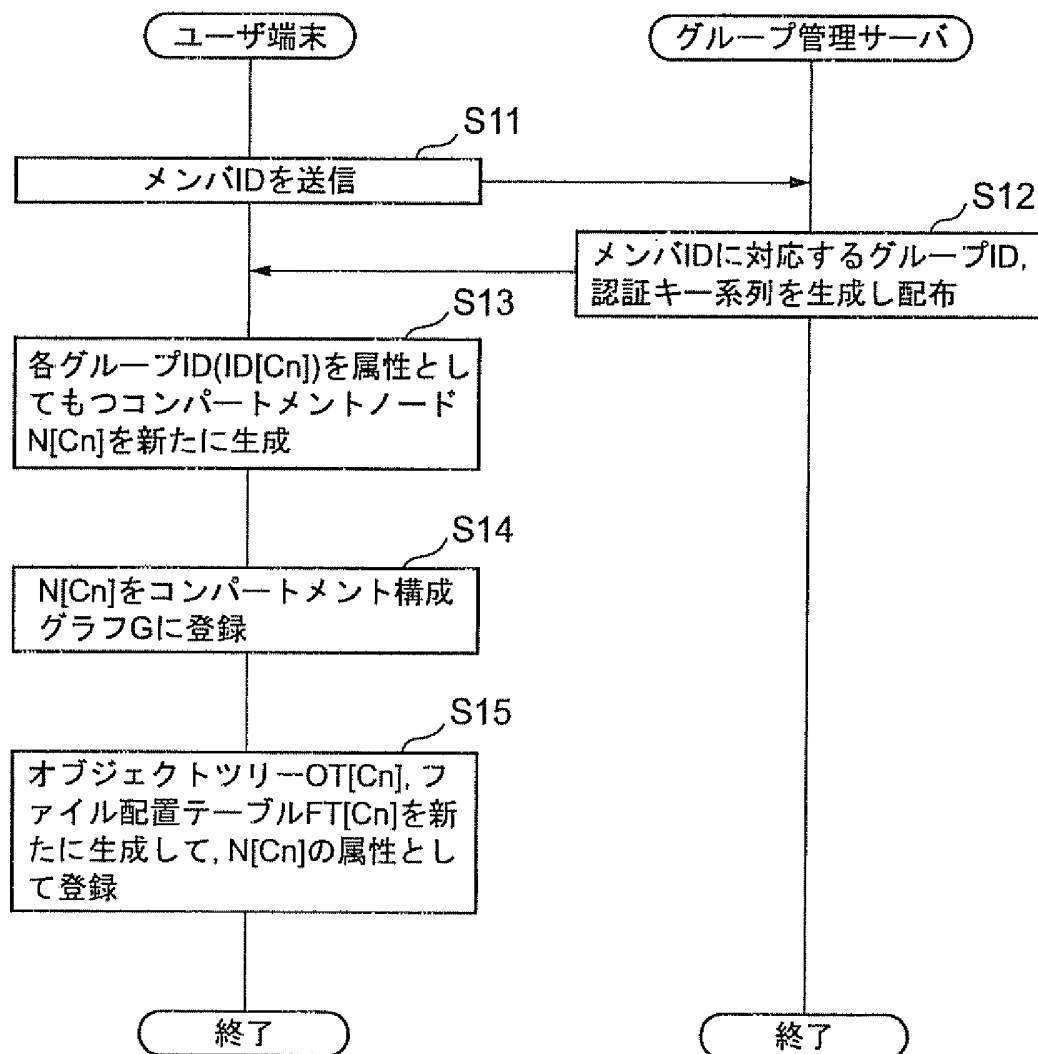
[図1]



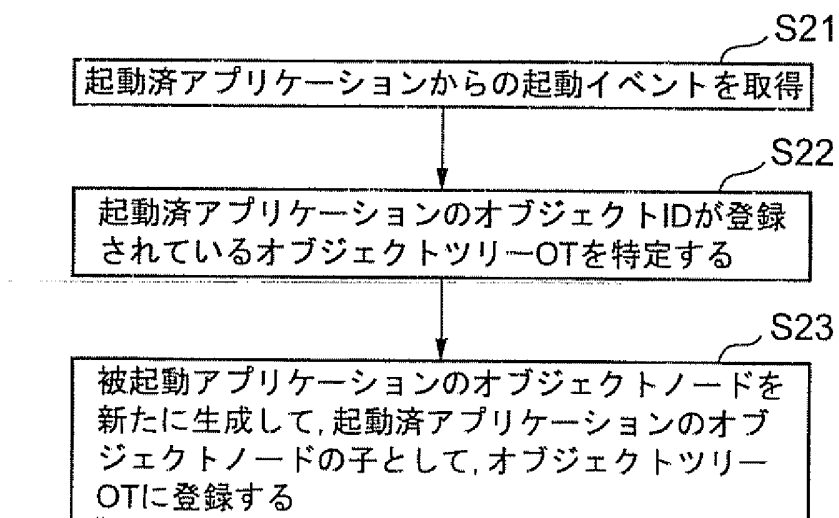
[図2]



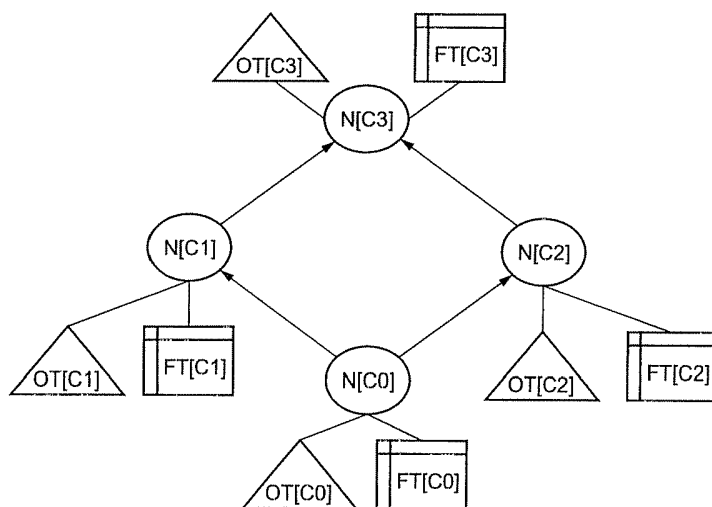
[図3]



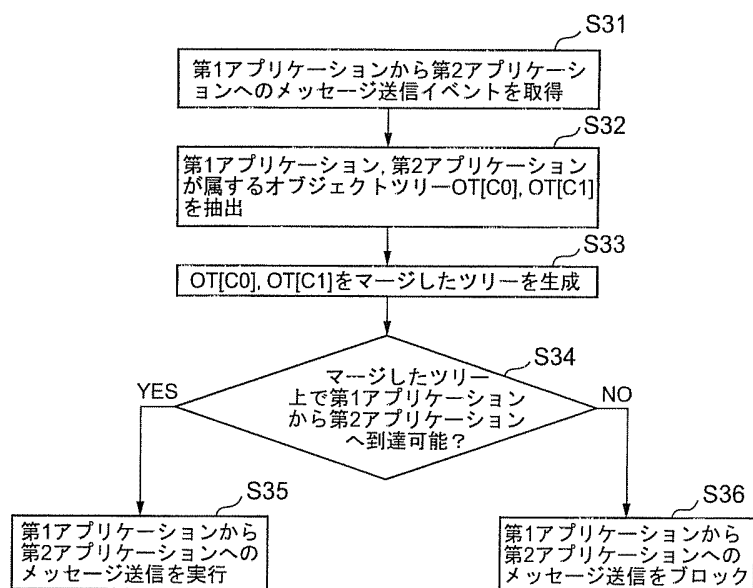
[図4]



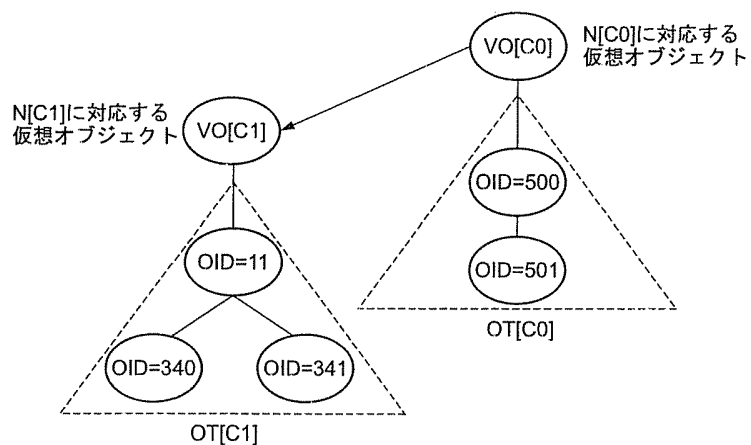
[図5]



[図6]



[図7]



[図8]

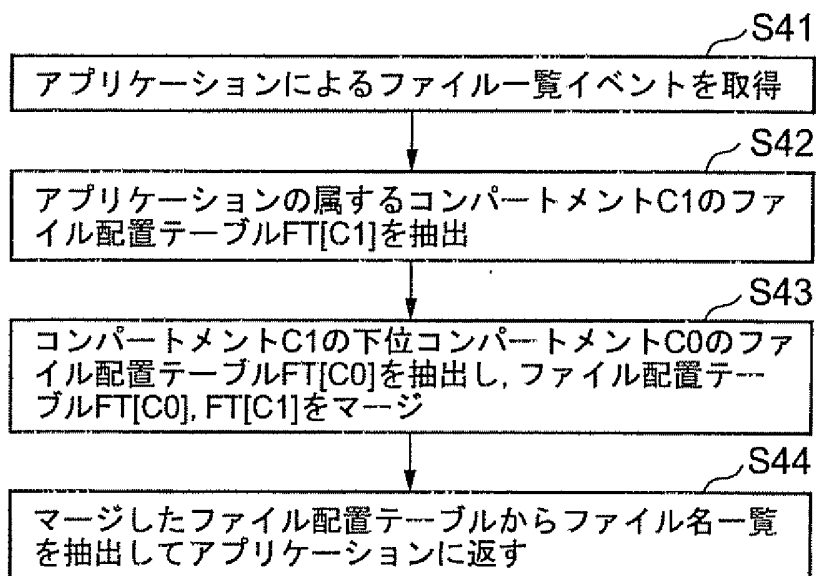
FT[C1]

| ファイル名              | 配置アドレス   |
|--------------------|----------|
| /dir1/dir1-1/file1 | 10350862 |
| /dir2/file2        | 8394     |

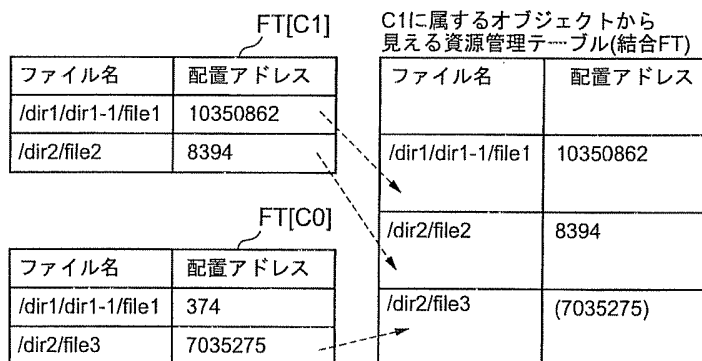
FT[C0]

| ファイル名              | 配置アドレス  |
|--------------------|---------|
| /dir1/dir1-1/file1 | 374     |
| /dir2/file3        | 7035275 |

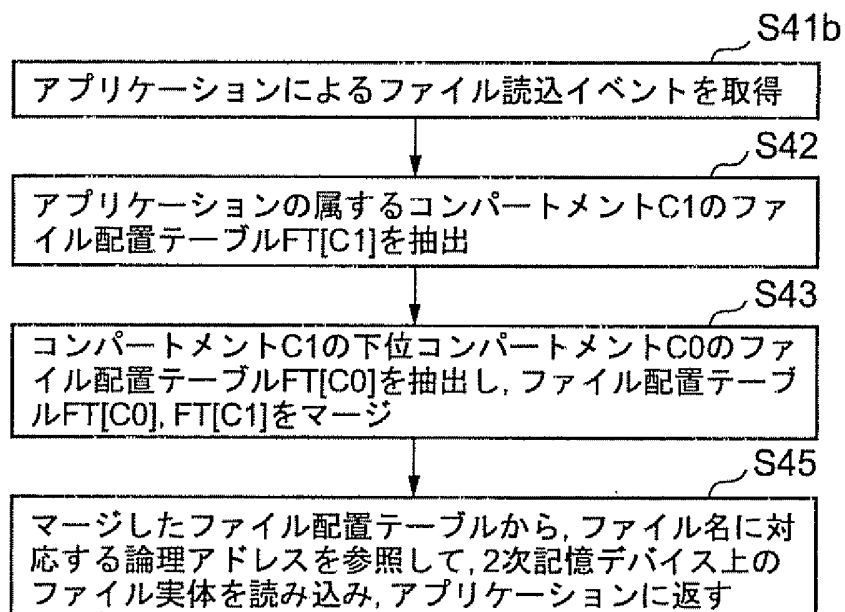
[図9]



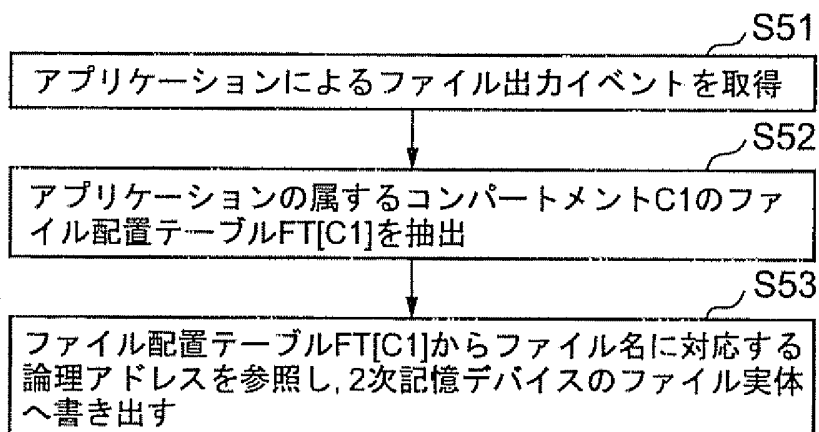
[図10]



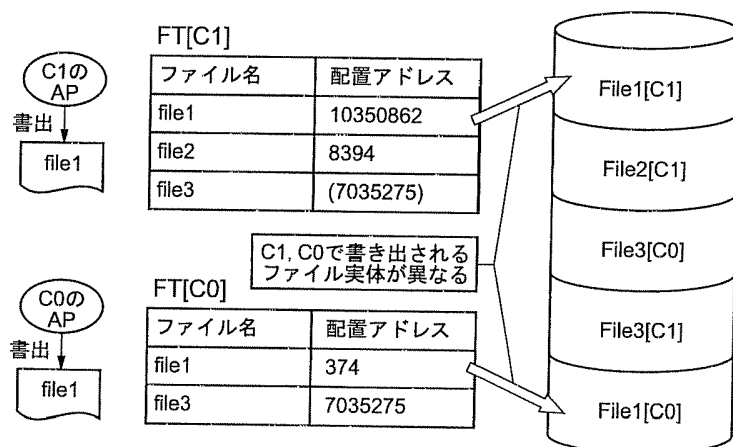
[図11]



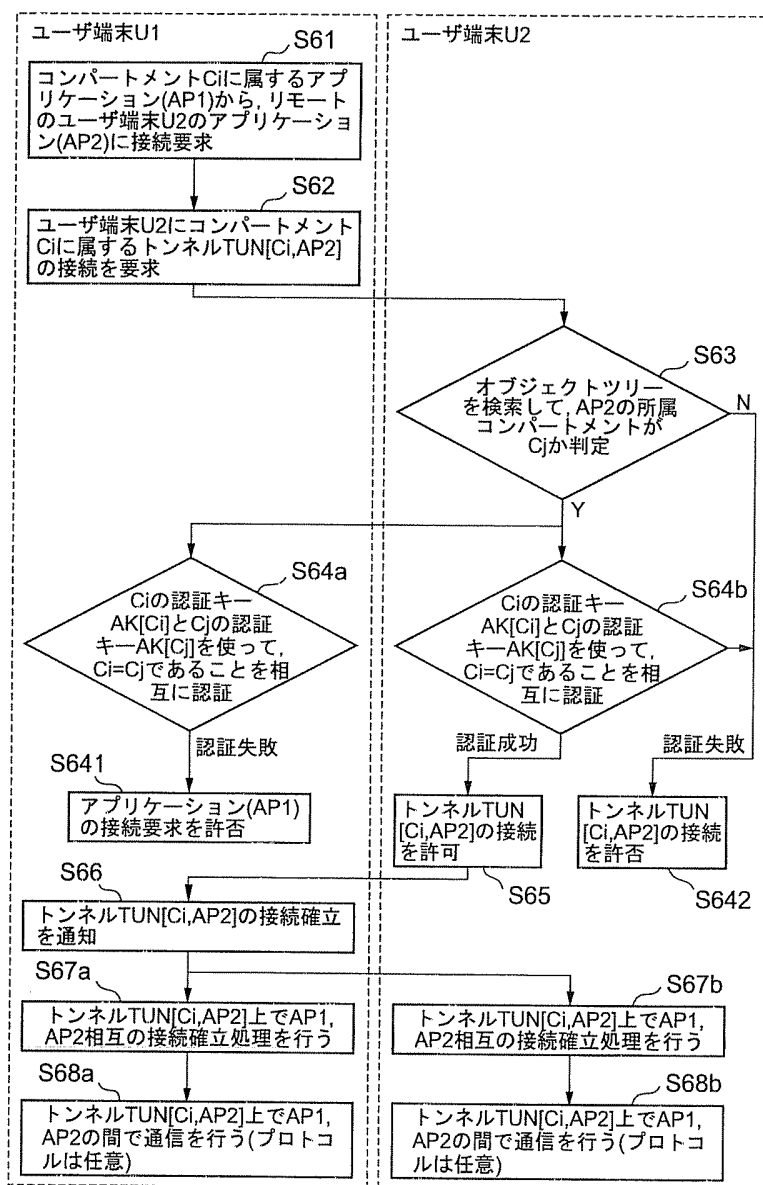
[図12]



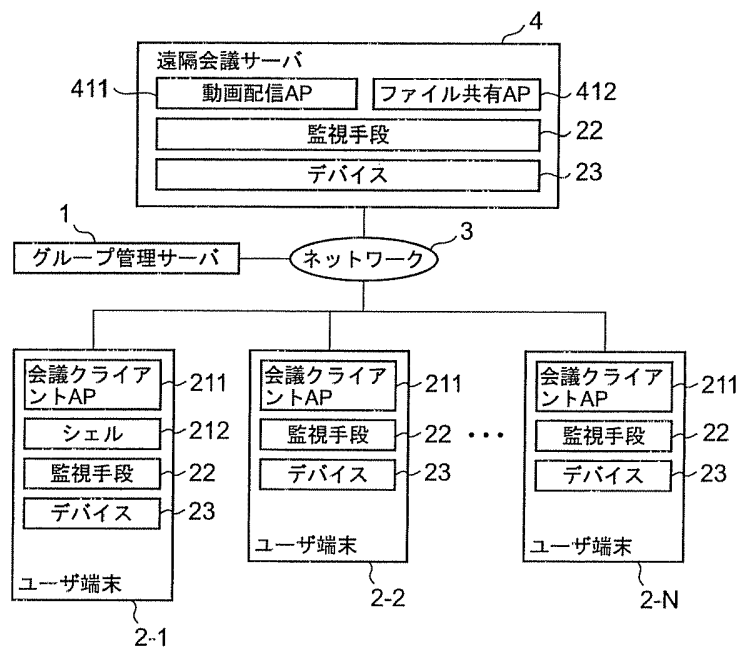
[図13]



[図14]



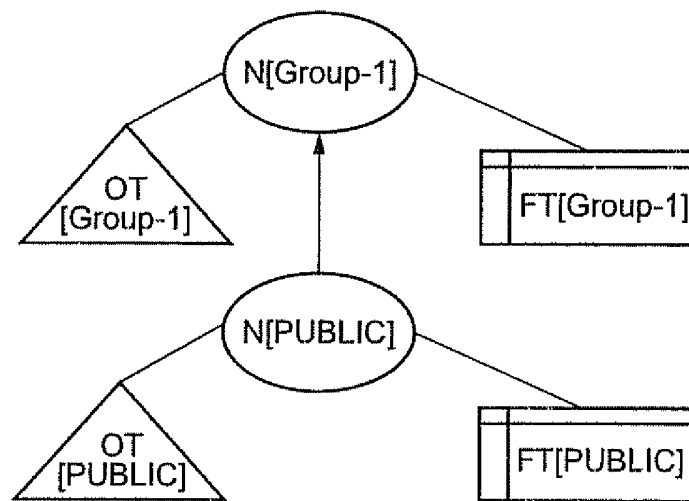
[図15]



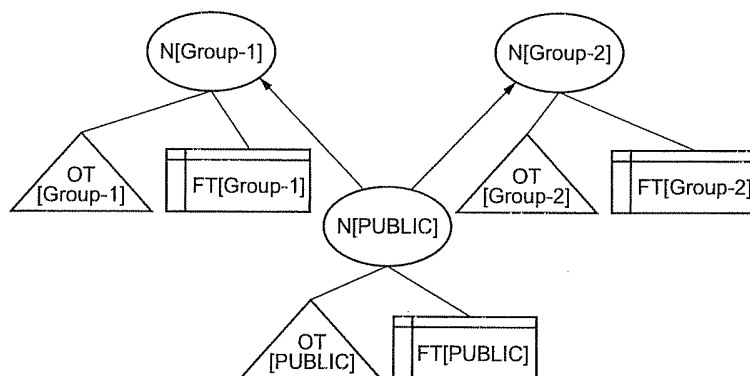
[図16]

| グループID  | 認証キー   | メンバID                                   |
|---------|--------|-----------------------------------------|
| Group-1 | A8BC0f | USER-1<br>USER-2<br>USER-3<br>CONF-SERV |
| Group-2 | 21AAB3 | USER-2<br>USER-4<br>USER-5<br>CONF-SERV |
| ⋮       | ⋮      | ⋮                                       |

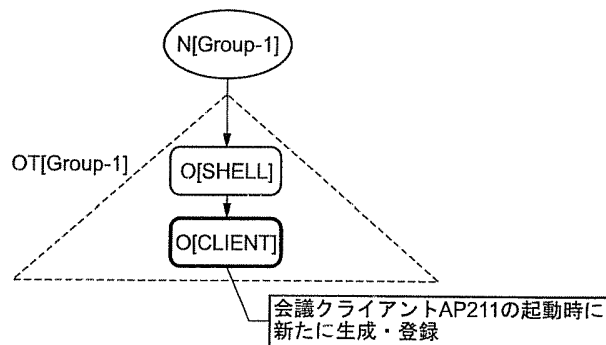
[図17]



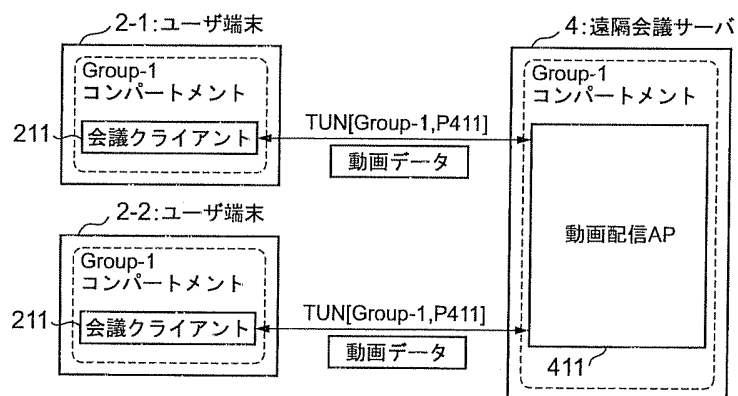
[図18]



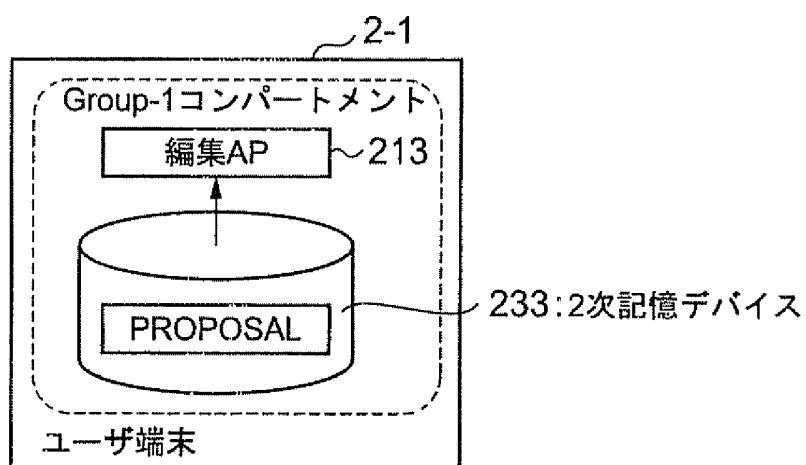
[図19]



[図20]



[図21]



[図22]

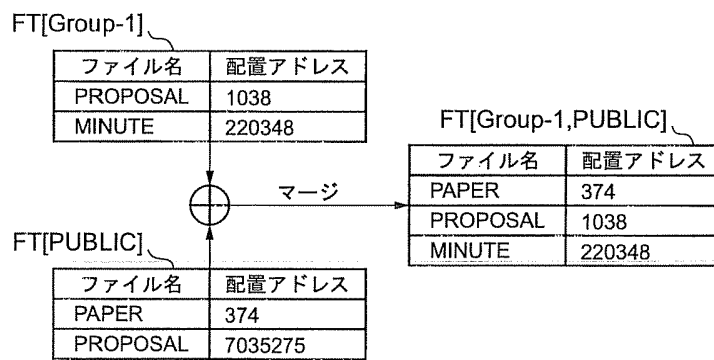
FT[Group-1]

| ファイル名    | 配置アドレス  |
|----------|---------|
| PROPOSAL | 374     |
| MINUTE   | 7035275 |

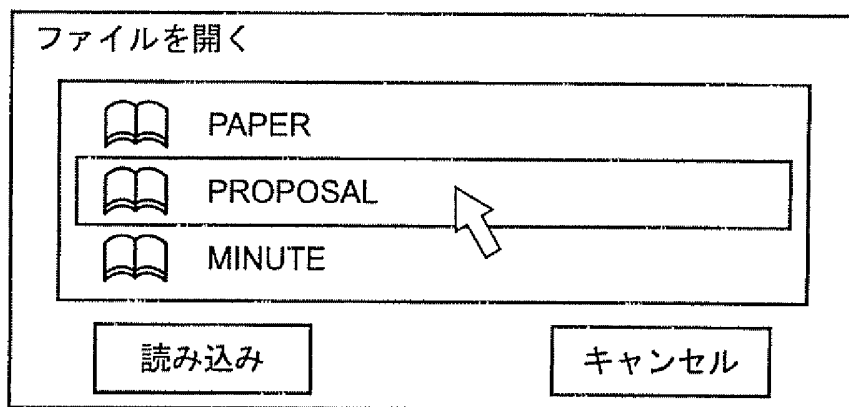
FT[PUBLIC]

| ファイル名    | 配置アドレス  |
|----------|---------|
| PAPER    | 374     |
| PROPOSAL | 7035275 |

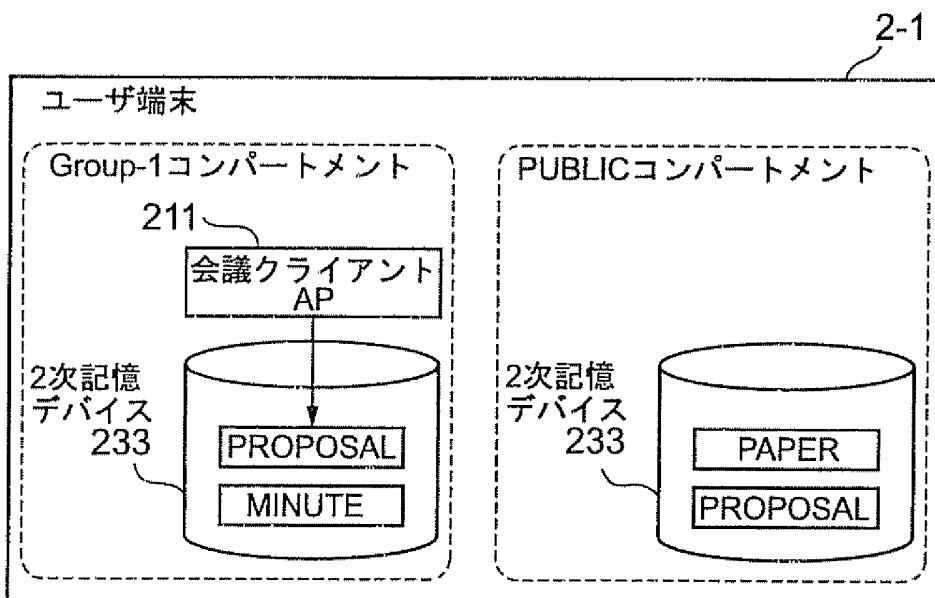
[図23]



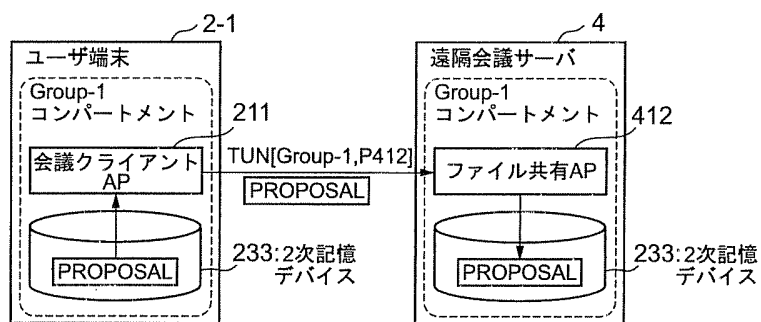
[図24]



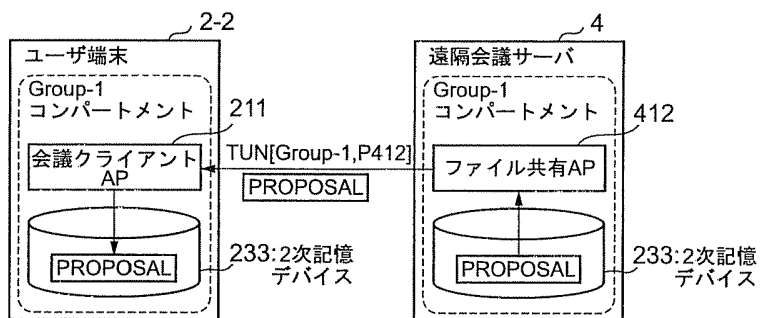
[図25]



[図26]

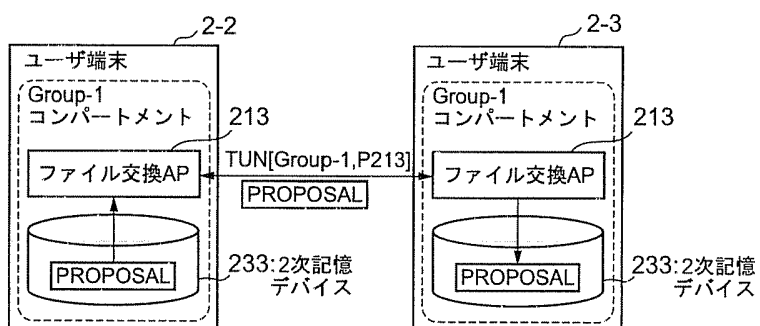


[図27]

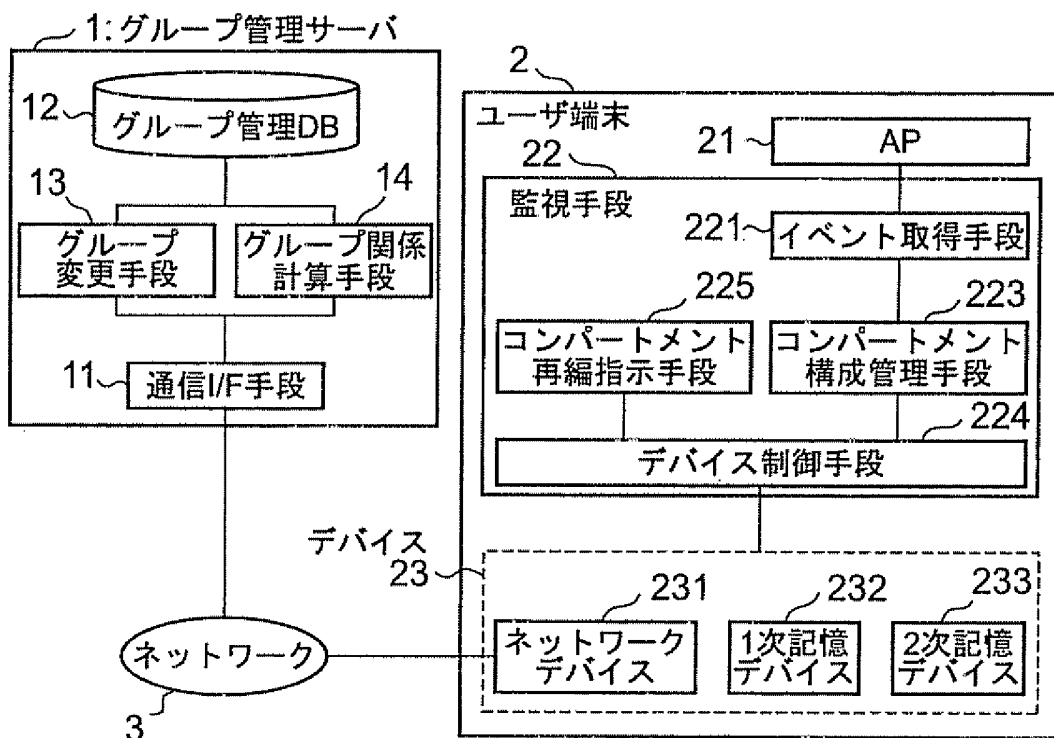


[図28]

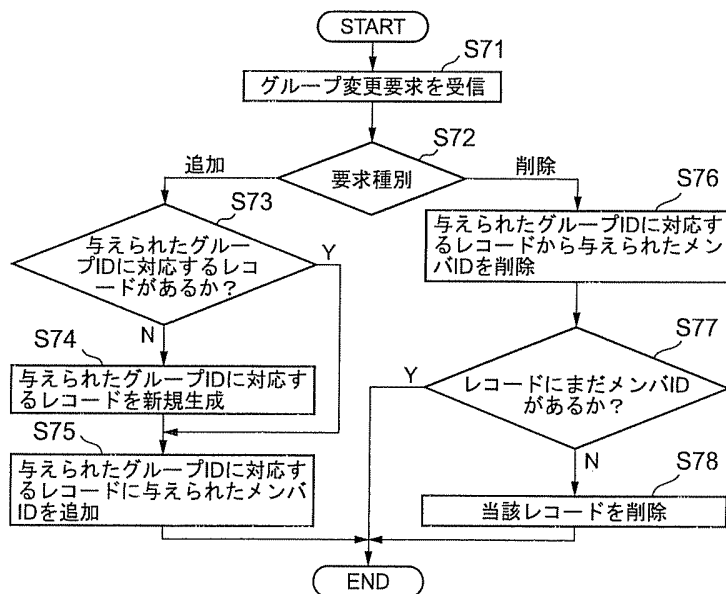
【図28】



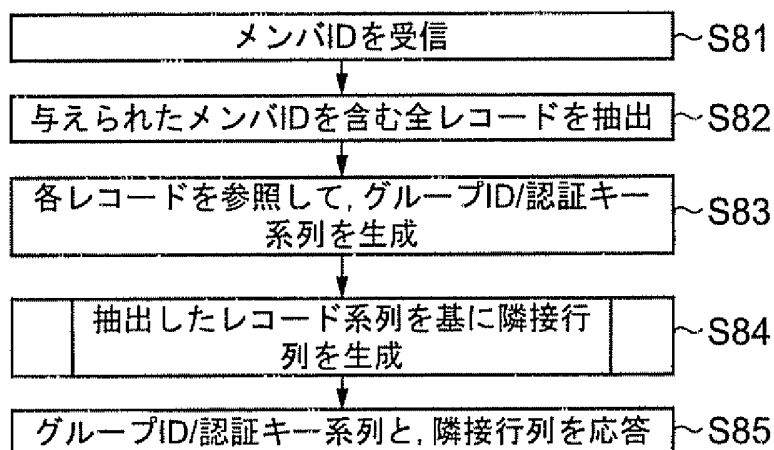
[図29]



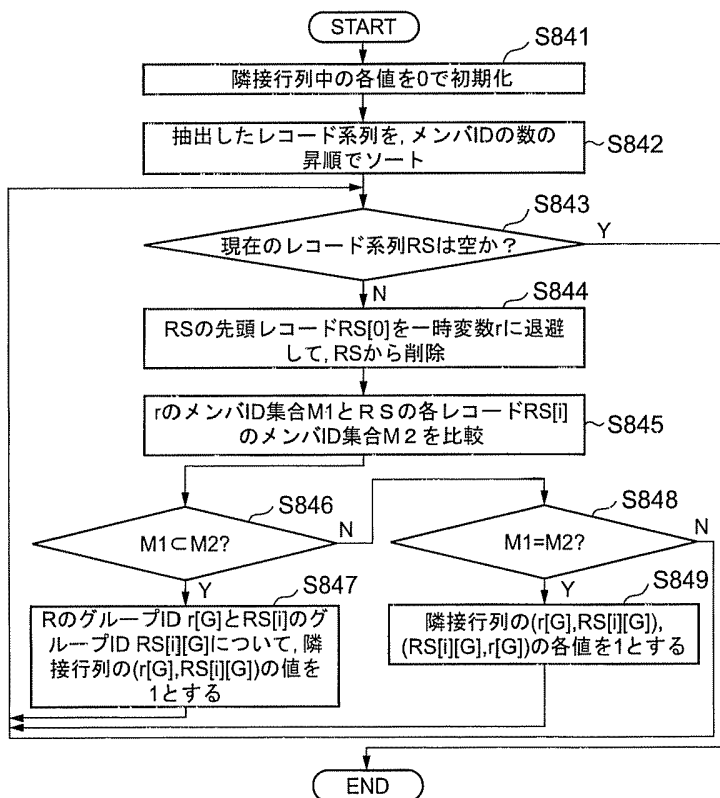
[図30]



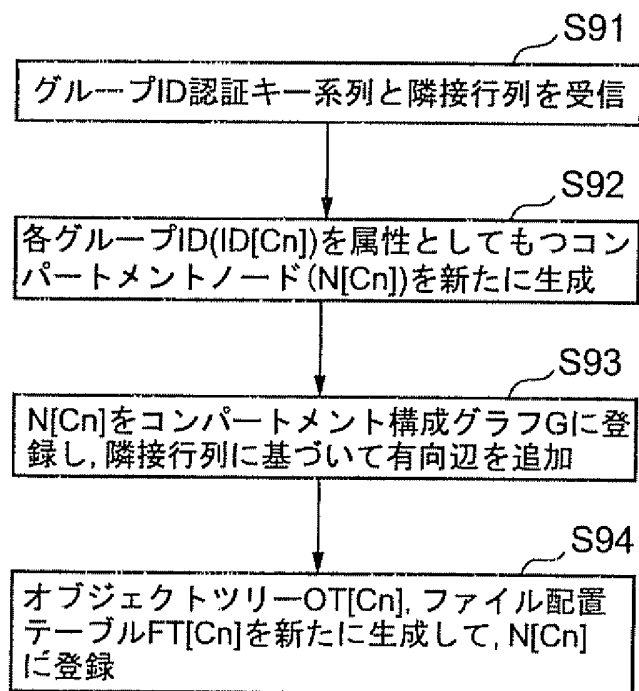
[図31]



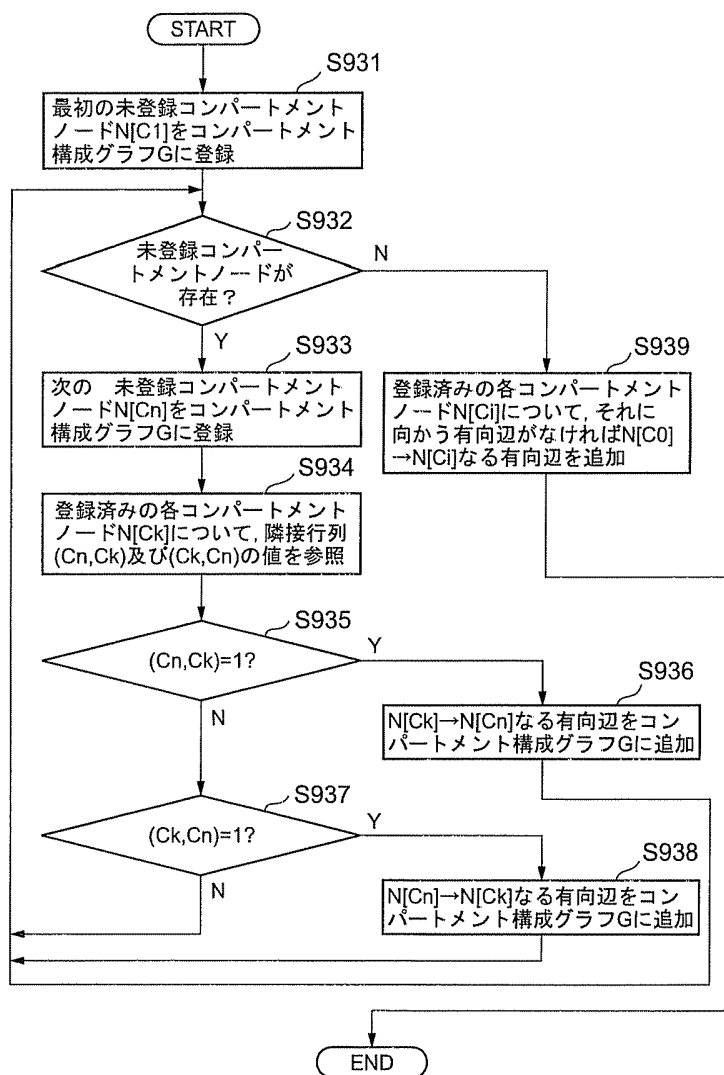
[図32]



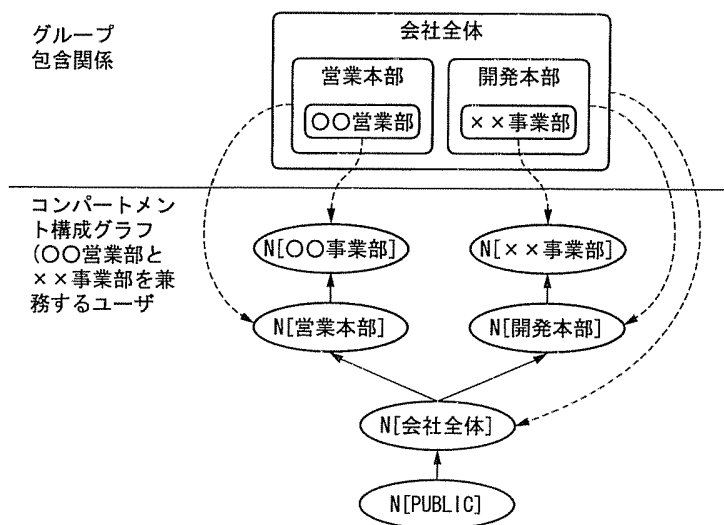
[図33]



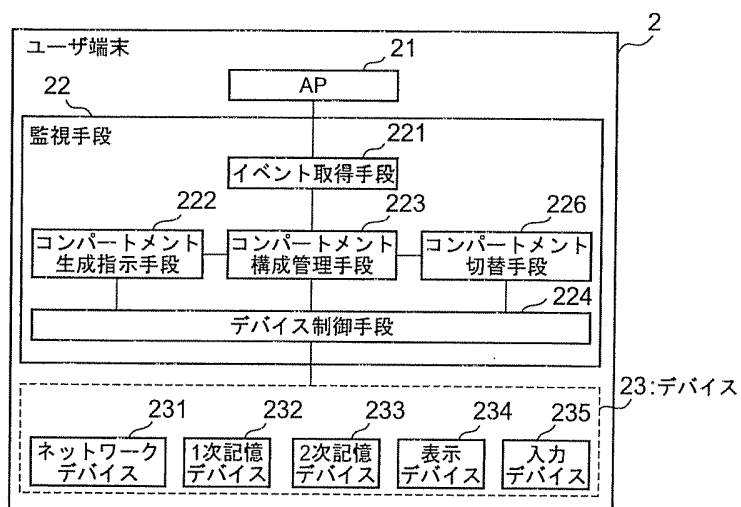
[図34]



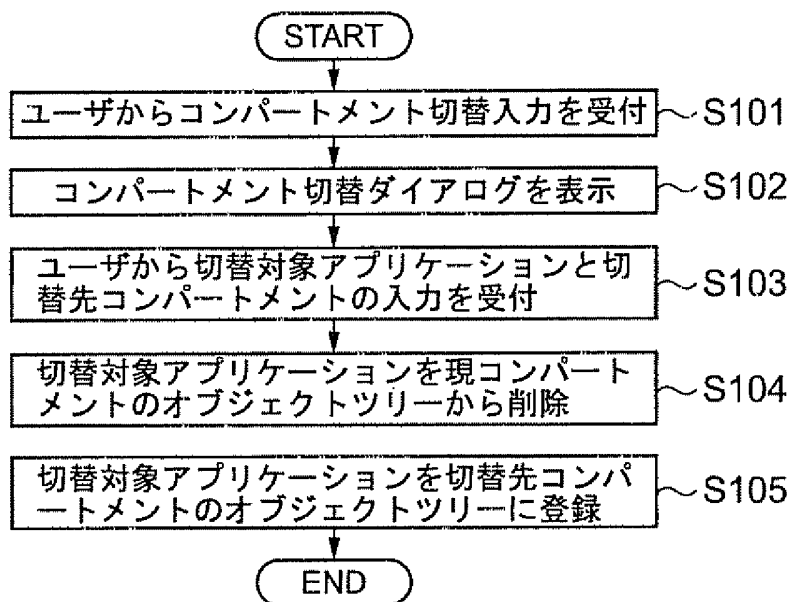
[図35]



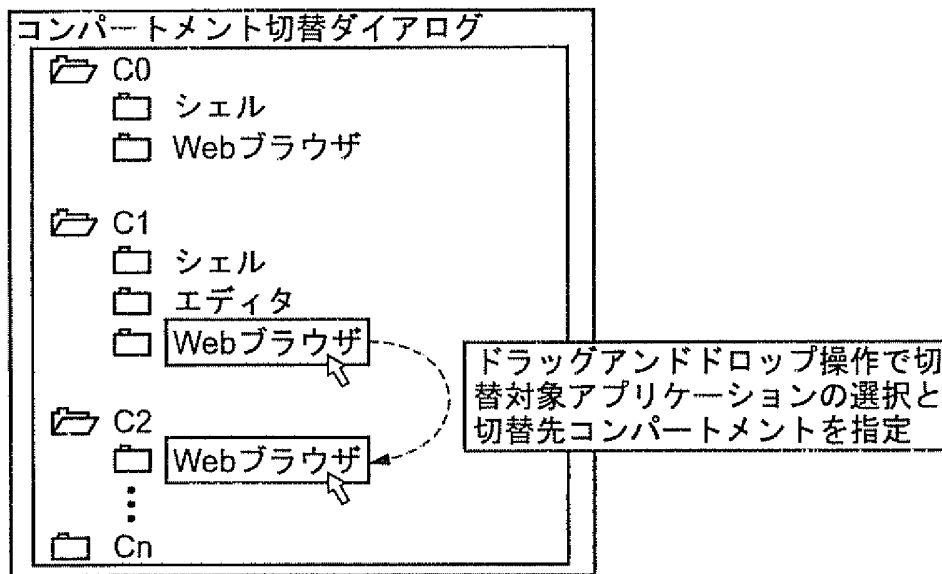
[図36]



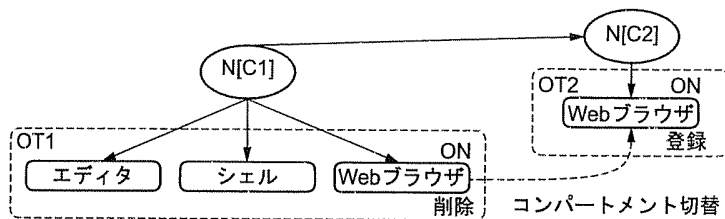
[図37]



[図38]



[図39]



[図40]

## コンパートメント切替ダイアログ

 C0 アプリケーション ファイル ファイル1 ファイル3 C1 アプリケーション シェル エディタ Webブラウザ ファイル ファイル1 ファイル2

# INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2005/021982

## A. CLASSIFICATION OF SUBJECT MATTER

**G06F21/24** (2006.01), **G06F12/00** (2006.01)

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

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

**G06F21/24** (2006.01), **G06F12/00** (2006.01)

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

|                           |           |                            |           |
|---------------------------|-----------|----------------------------|-----------|
| Jitsuyo Shinan Koho       | 1922-1996 | Jitsuyo Shinan Toroku Koho | 1996-2006 |
| Kokai Jitsuyo Shinan Koho | 1971-2006 | Toroku Jitsuyo Shinan Koho | 1994-2006 |

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

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages                                                                                                                                                                                                         | Relevant to claim No. |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| Y         | Yuichi NAKAMURA, "SELinux Nyumon Secure OS de Anzen na Sever o Kochiku suru", Nikkei Linux, Vol.5, No.10, Nikkei Business Publications, Inc., 08 September, 2003 (08.09.03), pages 141 to 148                                                                                              | 1-22                  |
| Y         | Reality Check: Security for Your Information Assets: Part III- The Trusted Solaris Advantage, [online], 20 December, 2003 (20.12.03), Sun Microsystems, Inc., [retrieval date 14 February, 2006 (14.02.06)], Internet <URL:http://www.sun.com/executives/realitycheck/reality-122003.html> | 1-22                  |

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

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

Date of the actual completion of the international search  
14 February, 2006 (14.02.06)

Date of mailing of the international search report  
21 February, 2006 (21.02.06)

Name and mailing address of the ISA/  
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

**INTERNATIONAL SEARCH REPORT**

International application No.

PCT/JP2005/021982

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages                                                                                                                                                                         | Relevant to claim No. |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| Y         | JP 2004-272380 A (Nippon Telegraph And Telephone Corp.),<br>30 September, 2004 (30.09.04),<br>Full text; all drawings<br>(Family: none)                                                                                                                    | 3, 13-22              |
| Y         | Shiro OOTSURU, "Zentaizo to Saishin Doko o Fukan suru Tameno Security Saishin Gijutsu Matrix Part2-6 Trusted OS no Kino to Donyu no Point", SECURITY MAGAZINE VOL.8, Kabushiki Kaisha Shoeisha, 01 April, 2003 (01.04.03), pages 85 to 90                  | 6, 14, 16, 18, 20, 22 |
| Y         | Hiroshi NAGASE et al., "Kaisoteki Security Level no Jiyudo o Mochiita Access-Ken Setteiho", Transactions of Information Processing Society of Japan, Vol.41, No.8, Information Processing Society of Japan, 15 August, 2000 (15.08.00), pages 2255 to 2262 | 7-10, 17, 18, 21, 22  |
| Y         | JP 2004-529408 A (Hewlett-Packard Co.),<br>24 September, 2004 (24.09.04),<br>Full text; all drawings<br>& WO 2002/061554 A1                                                                                                                                | 9, 10                 |
| A         | JP 3-68042 A (NEC Corp.),<br>25 March, 1991 (25.03.91),<br>Full text; all drawings<br>(Family: none)                                                                                                                                                       | 1-22                  |
| A         | JP 2003-91660 A (Toshiba Corp.),<br>28 March, 2003 (28.03.03),<br>Full text; all drawings<br>(Family: none)                                                                                                                                                | 1-22                  |

## A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int.Cl. G06F21/24(2006.01), G06F12/00(2006.01)

## B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int.Cl. G06F21/24(2006.01), G06F12/00(2006.01)

最小限資料以外の資料で調査を行った分野に含まれるもの

|             |            |
|-------------|------------|
| 日本国実用新案公報   | 1922-1996年 |
| 日本国公開実用新案公報 | 1971-2006年 |
| 日本国実用新案登録公報 | 1996-2006年 |
| 日本国登録実用新案公報 | 1994-2006年 |

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

## C. 関連すると認められる文献

| 引用文献の<br>カテゴリー* | 引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示                                                                                                                                                                                                                        | 関連する<br>請求の範囲の番号 |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| Y               | 中村 雄一, SELinux入門 セキュア OS で安全なサーバーを構築する,<br>日経 Linux 第5巻 第10号, 日経 BP 社 2003.09.08, p.141-p.148                                                                                                                                                            | 1-22             |
| Y               | Reality Check: Security for Your Information Assets: Part III<br>- The Trusted Solaris Advantage, [online], 2003.12.20,<br>Sun Microsystems, Inc., [検索日 2006.02.14], インターネット<br><URL:http://www.sun.com/executives/realitycheck/reality-1220<br>03.html> | 1-22             |

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

## \* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの  
「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの  
「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)  
「O」 口頭による開示、使用、展示等に言及する文献  
「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの  
「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの  
「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの  
「&」 同一パテントファミリー文献

国際調査を完了した日

14.02.2006

国際調査報告の発送日

21.02.2006

国際調査機関の名称及びあて先

日本国特許庁 (ISA/J P)

郵便番号 100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

平井 誠

電話番号 03-3581-1101 内線 3546

5 S

3449

| C (続き) . 関連すると認められる文献 |                                                                                                                                       |                          |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
| 引用文献の<br>カテゴリー*       | 引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示                                                                                                     | 関連する<br>請求の範囲の番号         |
| Y                     | JP 2004-272380 A (日本電信電話株式会社) 2004. 09. 30,<br>全文, 全図 (ファミリーなし)                                                                       | 3, 13-22                 |
| Y                     | 大津留 史郎, 全体像と最新動向を俯瞰するためのセキュリティ最新技術マトリクス Part2-6 トラステッド OS の機能と導入のポイント, SECURITY MAGAZINE VOL. 8, 株式会社翔泳社 2003. 04. 01,<br>p. 85-p. 90 | 6, 14, 16,<br>18, 20, 22 |
| Y                     | 永瀬 宏, 他 2 名, 階層的セキュリティレベルの自由度を用いたアクセス権設定法, 情報処理学会論文誌 第 41 巻 第 8 号, 社団法人情報処理学会 2000. 08. 15, p. 2255-p. 2262                           | 7-10, 17,<br>18, 21, 22  |
| Y                     | JP 2004-529408 A (ヒューレット・パカード・カンパニー)<br>2004. 09. 24, 全文, 全図 & WO 2002/061554 A1                                                      | 9, 10                    |
| A                     | JP 3-68042 A (日本電気株式会社) 1991. 03. 25,<br>全文, 全図 (ファミリーなし)                                                                             | 1-22                     |
| A                     | JP 2003-91660 A (株式会社東芝) 2003. 03. 28,<br>全文, 全図 (ファミリーなし)                                                                            | 1-22                     |