(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4314311号
(P4314311)

(45)発行日　平成21年8月12日(2009.8.12)　(24)登録日　平成21年5月22日(2009.5.22)

(51)Int.Cl.　　F I
G06F 21/24 (2006.01)　　G06F 12/14 520E
G06F 12/00 (2006.01)　　G06F 12/00 537A

請求項の数 17　(全 19 頁)

(21)出願番号　特願2008-114237 (P2008-114237)
(22)出願日　平成20年4月24日 (2008.4.24)
(65)公開番号　特開2009-176265 (P2009-176265A)
(43)公開日　平成21年8月6日 (2009.8.6)
審査請求日　平成21年1月23日 (2009.1.23)
(31)優先権主張番号　特願2007-338218 (P2007-338218)
(32)優先日　平成19年12月27日 (2007.12.27)
(33)優先権主張国　日本国(JP)

早期審査対象出願

(73)特許権者　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(74)代理人　100058479
弁理士　鈴江　武彦
(74)代理人　100108855
弁理士　蔵田　昌俊
(74)代理人　100091351
弁理士　河野　哲
(74)代理人　100088683
弁理士　中村　誠
(74)代理人　100109830
弁理士　福原　淑弘
(74)代理人　100075672
弁理士　峰　隆司

最終頁に続く

(54)【発明の名称】情報処理装置および情報処理システム

(57)【特許請求の範囲】
【請求項１】
オペレーティングシステムと前記オペレーティングシステム上で動作するプログラムとデータとを備えた複数のソフトウェア資源が一つのハードウェア資源上で同時動作するために各ソフトウェア資源を制御するためのモニタ手段を備えた情報処理装置であって、
前記情報処理装置のハードウェア資源上で動作するソフトウェア資源の一つは、サーバとして動作するサーバ用ソフトウェア資源であり、
前記情報処理装置のハードウェア資源上で動作するソフトウェア資源の一つは、前記サーバ用ソフトウェア資源のサービスを利用するクライアント用ソフトウェア資源であり、
前記ハードウェア資源は、前記クライアント用ソフト資源が使用するためのデータが格納されるユーザ・ディスク・スペースを有し、
前記サーバ用ソフトウェア資源は、前記クライアント用ソフトウェア資源が起動された場合に、ネットワークを介して接続される管理サーバと通信を試み、前記管理サーバからアクセスキーを取得し、取得した前記アクセスキーの認証を行い、前記アクセスキーが正当であると判断した場合に、前記クライアント用ソフトウェア資源に対して前記ユーザ・ディスク・スペースへのアクセス権を与えるアクセス権制御手段を具備することを特徴とする情報処理装置。
【請求項２】
前記アクセス権制御手段は、前記管理サーバの存在を確認するために前記管理サーバと定期的に通信を試み、

前記管理サーバと通信が行えなかった場合に、前記クライアント用ソフトウェア資源の前記ユーザ・ディスク・スペースへの前記アクセス権を取り上げることを特徴とする請求項１に記載の情報処理装置。

【請求項３】

前記管理サーバと通信が行えなかった後、前記アクセス権制御手段は、前記管理サーバの存在を確認するために前記管理サーバと定期的に通信を試み、

前記管理サーバと通信が行えた場合、前記アクセス権制御手段は、前記クライアント用ソフトウェア資源に対して前記ユーザ・ディスク・スペースへのアクセス権を与えることを特徴とする請求項２に記載の情報処理装置。

【請求項４】

前記ユーザの要求に応じて、前記前記アクセス権制御手段は、前記クライアント用ソフトウェア資源の前記ユーザ・ディスク・スペースに対するアクセスレベルをＲｅａｄ権に設定し、前記アクセスキーの認証を行わずに前記クライアント用ソフトウェア資源に対して前記ユーザ・ディスク・スペースへのアクセス権を与えることを特徴とする請求項１ないし請求項３の何れか１項に記載の情報処理装置。

【請求項５】

前記アクセス権制御手段は、前記第２ユーザ・ディスク・スペースを用意し、

前記クライアント用ソフトウェア資源の前記第２ユーザ・ディスク・スペースに対するアクセスレベルをＲｅａｄ権／Ｗｒｉｔｅ権に設定し、前記アクセスキーの認証を行わずに前記クライアント用ソフトウェア資源に対して前記第２ユーザ・ディスク・スペースへのアクセス権を与えることを特徴とする請求項４記載の情報処理装置。

【請求項６】

挿抜可能なアクセスキーの複製が格納されたリムーバル記憶装置からデータを読み出す手段を具備し、

前記アクセス権制御手段は、前記リムーバル記憶装置から前記アクセスキーを読み出し、前記読み出したアクセスキーの認証を行い、前記アクセスキーが正当であると判断した場合に、前記クライアント用ソフトウェア資源に対して前記ユーザ・ディスク・スペースへのアクセス権を与えることを特徴とする請求項１に記載の情報処理装置。

【請求項７】

前記ユーザからの要求に応じて、前記アクセス権制御手段は、前記管理サーバからデータの提供を受け、前記クライアント用ソフトウェア資源に対して前記データが格納された第３ディスク・スペースのアクセス権を与えることを特徴とする請求項１ないし請求項６の何れか１項に記載の情報処理装置。

【請求項８】

オペレーティングシステムと前記オペレーティングシステム上で動作するプログラムとデータとを備えた複数のソフトウェア資源が一つのハードウェア資源上で同時動作するために各ソフトウェア資源を制御するためのモニタ手段を備えた情報処理装置と、前記情報処理装置とネットワークを介して接続される管理サーバとを有する情報処理システムであって、

前記情報処理装置のハードウェア資源上で動作するソフトウェア資源の一つは、サーバとして動作するサーバ用ソフトウェア資源であり、

前記情報処理装置のハードウェア資源上で動作するソフトウェア資源の一つは、前記サーバ用ソフトウェア資源のサービスを利用するクライアント用ソフトウェア資源であり、

前記ハードウェア資源は、前記クライアント用ソフト資源が使用するためのデータが格納されるユーザ・ディスク・スペースを有し、

前記管理サーバは、前記クライアント用ソフト資源がユーザ・ディスク・スペースを使用するためのアクセスキーを有し、

前記サーバ用ソフトウェア資源は、前記クライアント用ソフトウェア資源が起動された場合に、ネットワークを介して接続される管理サーバと通信を試み、ネットワークを介して接続される管理サーバと通信を試み、前記管理サーバと通信が行えた場合に、前記管理

サーバからアクセスキーを取得し、取得した前記アクセスキーの認証を行い、前記アクセスキーが正当であると判断した場合に、前記クライアント用ソフトウェア資源に対して前記ユーザ・ディスク・スペースへのアクセス権を与えるアクセス権制御手段を具備することを特徴とする情報処理システム。

【請求項９】

前記アクセス権制御手段は、前記管理サーバの存在を確認するために前記管理サーバと定期的に通信を試み、

前記管理サーバと通信が行えなかった場合、前記アクセス権制御手段は、前記クライアント用ソフトウェア資源の前記ユーザ・ディスク・スペースへの前記アクセス権を取り上げることを特徴とする請求項８に記載の情報処理システム。

【請求項１０】

前記管理サーバと通信が行えなかった後、前記アクセス権制御手段は、前記管理サーバの存在を確認するために前記管理サーバと定期的に通信を試み、

前記管理サーバと通信が行えた場合、前記アクセス権制御手段は、前記クライアント用ソフトウェア資源に対して前記ユーザ・ディスク・スペースへのアクセス権を与えることを特徴とする請求項９に記載の情報処理システム。

【請求項１１】

前記ユーザからの要求に応じて、前記アクセス権制御手段は、前記クライアント用ソフトウェア資源の前記ユーザ・ディスク・スペースに対するアクセスレベルをＲｅａｄ権に設定し、前記アクセスキーの認証を行わずに前記クライアント用ソフトウェア資源に対して前記ユーザ・ディスク・スペースへのアクセス権を与えることを特徴とする請求項８ないし請求項１０の何れか１項に記載の情報処理システム。

【請求項１２】

前記アクセス権制御手段は、前記第２ユーザ・ディスク・スペースを用意し、

前記アクセス権制御手段は、前記クライアント用ソフトウェア資源の前記第２ユーザ・ディスク・スペースに対するアクセスレベルをＲｅａｄ権／Ｗｒｉｔｅ権に設定し、前記アクセスキーの認証を行わずに前記クライアント用ソフトウェア資源に対して前記第２ユーザ・ディスク・スペースへのアクセス権を与えることを特徴とする請求項１１記載の情報処理システム。

【請求項１３】

挿抜可能なアクセスキーの複製が格納されたリムーバル記憶装置からデータを読み出す手段を具備し、

前記アクセス権制御手段は、前記リムーバル記憶装置から前記アクセスキーを読み出し、前記読み出したアクセスキーの認証を行い、前記アクセスキーが正当であると判断した場合に、前記クライアント用ソフトウェア資源に対して前記ユーザ・ディスク・スペースへのアクセス権を与えることを特徴とする請求項８記載の情報処理システム。

【請求項１４】

前記ユーザからの要求に応じて、前記サーバ用ソフトウェア資源は、前記管理サーバに対して１以上のデータの提供を要求し、

前記管理サーバは、前記サーバ用ソフトウェア資源からの要求に応じて前記データを提供し、

前記アクセス権制御手段は、前記データが格納された第３ディスク・スペースを用意し、前記クライアント用ソフトウェア資源に対して前記第３ディスク・スペースへのアクセス権を与えることを特徴とする請求項８ないし請求項１３の何れか１項に記載の情報処理システム。

【請求項１５】

前記サーバ用ソフトウェア資源は、前記ネットワークを介して接続されている前記情報処理装置が有するユーザ・ディスク・スペースに格納されているファイルの一覧の情報を生成する処理と、前記クライアント用ソフトウェア資源からの情報の送信を要求に応じて当該クライアント用ソフトウェア資源が動作している情報処理装置のユーザ・ディスク・

スペースに前記ファイルの一覧の情報を送信する処理とを実行し、
前記クライアント用ソフトウェア資源は、前記管理サーバに対して前記ファイルの一覧の情報の送信を要求する処理を実行することを特徴とする請求項８に記載の情報処理システム。
【請求項１６】
前記クライアント用ソフトウェア資源は、前記ファイルの一覧の情報から名称をキーワードにファイル検索処理を実行することを特徴とする請求項１５に記載の情報処理システム。
【請求項１７】
前記アクセス権制御手段は、前記クライアント用ソフトウェア資源から前記ファイルの一覧の情報に登録されているファイルへのアクセス要求があった場合に、前記ファイルの一覧の情報に登録されているファイルにアクセスして良いか否かを前記管理サーバに問い合わせる処理と、前記管理サーバが前記ファイルへのアクセスを許可した場合に、前記管理サーバに対して前記ファイルのアクセス要求を送信する処理とを実行し、
前記アクセス権制御手段は、前記ファイルにアクセスして良いか否かの問い合わせに対して前記情報処理装置のユーザに基づいて前記ファイルにアクセスして良いか否かを判定し、前記判定の結果を送信する処理と、前記ファイルにアクセスして良いと判断して、前記情報処理装置からのアクセス要求があった場合に、前記別の情報処理装置に対して前記アクセス要求の種類に応じたアクセスを実行する処理と、アクセス結果を前記情報処理装置に送信する処理とを実行することを特徴とする請求項１５に記載の情報処理システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、仮想化技術を利用した情報処理装置および情報処理システムに関する。
【背景技術】
【０００２】
従来、個人データが保存されたディスクに対して通常はユーザＯＳだけの管理の下アクセス可能であった。しかし、このことはユーザが上記ＰＣを管理サーバへの接続をすることなく、ＰＣを使用した場合、ユーザが作為的、もしくは不作為的に関係なく、個人データディスクに保存された未承認の情報等が悪意ある第３者へ流出が発生し、場合によっては企業活動等に重大な支障するという問題があった。
【０００３】
特許文献1には、仮想計算機システムにおいて、各ファイルにアクセス可能なオペレーティングシステムを設定して、ファイルを保護する方法が開示されている。
【特許文献１】特開２０００－１１２８０４号公報（要約、請求項１）
【発明の開示】
【発明が解決しようとする課題】
【０００４】
上述した技術では、各ファイルにアクセス可能なオペレーティングシステムを設定するのでは、多くのディスク資源を必要とする。
【０００５】
本発明の目的は、多くのディスク資源を必要とせずに、未許可状態での持ち出しによる機密情報データ等の漏洩を防止することが可能な情報処理装置および情報処理システムを提供することにある。
【課題を解決するための手段】
【０００６】
本発明の一例に係わる情報処理装置は、オペレーティングシステムと前記オペレーティングシステム上で動作するプログラムとデータとを備えた複数のソフトウェア資源が一つのハードウェア資源上で同時動作するために各ソフトウェア資源を制御するためのモニタ手段を備えた情報処理装置であって、前記情報処理装置のハードウェア資源上で動作する

ソフトウェア資源の一つは、サーバとして動作するサーバ用ソフトウェア資源であり、前記情報処理装置のハードウェア資源上で動作するソフトウェア資源の一つは、前記サーバ用ソフトウェア資源のサービスを利用するクライアント用ソフトウェア資源であり、前記ハードウェア資源は、前記クライアント用ソフト資源が使用するためのデータが格納されるユーザ・ディスク・スペースを有し、前記サーバ用ソフトウェア資源は、前記クライアント用ソフトウェア資源が起動された場合に、ネットワークを介して接続される管理サーバと通信を試み、前記管理サーバからアクセスキーを取得し、取得した前記アクセスキーの認証を行い、前記アクセスキーが正当であると判断した場合に、前記クライアント用ソフトウェア資源に対して前記ユーザ・ディスク・スペースへのアクセス権を与えることを特徴とする。

【発明の効果】

【０００７】

本発明によれば、多くのディスク資源を必要とせずに、未許可状態での持ち出しによる機密情報データ等の漏洩を防止することが可能になる。

【発明を実施するための最良の形態】

【０００８】

本発明の実施の形態を以下に図面を参照して説明する。

【０００９】

図１に示すように、管理サーバ１００に複数のクライアントＰＣ２Ａ～２Ｃが接続されている。

管理サーバ１００は、クライアントＰＣ上に搭載されてユーザ用仮想マシンとして実行されるユーザ・システム・ディスク１２０、及びクライアントＰＣ２Ａ～２Ｃと通信するためのコントローラ機能を実行するためのサーバソフトウェア１１０を有する。

【００１０】

クライアントＰＣ２Ａ～２Ｃには、例えば、ＸＥＮ，ＶＭＷＡＲＥなどで提供される仮想化技術（Virtual Monitor）を実行する環境が整えられている。クライアントＰＣ２Ａ～２Ｃに含まれるユーザシステム空間は、ユーザ・システム・ディスク１２０に格納されたユーザＯＳ（Windows XP（登録商標），Vista（登録商標）など）や各種クライアントソフト、システム設定、セキュリティポリシーにより提供され、ユーザがキーボード入出力等による直接作業可能なプロセス領域である。なお、クライアントＰＣ２Ｂ，２Ｃは、クライアントＰＣ２Ａと同様な構成であるが、図示を省略している。

【００１１】

クライアントＰＣ２Ａは、ハードウェア層４、仮想マシンモニタ５、管理用仮想マシン（サーバ用ソフトウェア資源）６Ａ、ユーザ用仮想マシン６Ｂ（クライアント用ソフトウェア資源）、ユーザ・ディスク・スペース６Ｃ等を有する。

【００１２】

ハードウェア層４は、ディスプレイ、ハードディスクドライブ（ＨＤＤ）、ネットワークインターフェスカード、キーボード、およびマウス等を有する。

【００１３】

仮想マシンモニタ５は、ハードウェア層４を管理し、各仮想マシン６Ａ，６Ｂに対してリソース割り当てを行う。また仮想マシンモニタ５は、仮想マシンの実行スケジュールと仮想マシンからのＩ／Ｏ要求をハードウェア層４へ振り分ける。

【００１４】

管理用仮想マシン６Ａは、サービスオペレーティングシステム（サービスＯＳ）８Ａ、管理用アプリケーション（管理用ＡＰＰ）９Ａ等を有する。サービスオペレーティングシステム８Ａは、管理用アプリケーション９Ａを動作させるためのオペレーティングシステムである。例えば、Ｌｉｎｕｘ（登録商標）がサービスオペレーティングシステム８Ａとして用いられる。アクセス権制御ソフトウェア２０１は、ユーザ用仮想マシン６Ｂからユーザ・ディスク・スペース６Ｃへのアクセスを制御するためのアプリケーションである。

【００１５】

ユーザ用仮想マシン６Ｂは、ユーザオペレーティングシステム（ユーザＯＳ）８Ｂ、ユーザアプリケーション（ユーザＡＰＰ）９Ｂ等を有する。ユーザオペレーティングシステム８Ｂは、ユーザが一般的に使用する環境を提供するためのオペレーティングシステムである。一般的には、ユーザオペレーティングシステム８Ｂとしては、ウインドウズ（登録商標）系のオペレーティングシステムが用いられる。ユーザアプリケーション９Ｂは、ユーザオペレーティングシステム８Ｂ上で動作するアプリケーションソフトウェアである。例えば、ワードプロセッサ、スプレッドシート、プレゼンテーション資料作成ソフト、メーラ、Ｗｅｂブラウザ等である。

【００１６】

なお、ユーザ用仮想マシン６Ｂは、管理用仮想マシン６Ａ内のデータをみることが出来ず、データに直接アクセスすることができない。

【００１７】

ユーザ・ディスク・スペース６Ｃは、ハードディスクドライブ中に割り当てられたスペースである。ユーザ・ディスク・スペース６Ｃ内には、ユーザアプリケーション９Ｂを用いて作成されるデータ、或いは閲覧することが出来るデータが格納される。

【００１８】

クライアントＰＣ２Ａ～２Ｃに含まれる管理用仮想マシン６Ａは、サービスオペレーティングシステム８Ａやその上で動作する管理用アプリケーション９Ａにより、
（ａ）ユーザシステムに対して、個人データディスクの提供の実施、
（ｂ）ユーザシステム空間のオープン、及びクローズ、
（ｃ）ユーザ・システム・ディスクの置換を実施、及び
（ｄ）リモート上にある管理サーバと通信し、左記の（ａ）や（ｂ）の処理との連携を実施する
プロセス領域である。

【００１９】

例として、仮想マシンモニタがＸＥＮによって提供され、ユーザシステム空間（ユーザ用仮想マシン）（Ｄｏｍａｉｎ－Ｕ）がＷｉｎｄｏｗｓ（登録商標） ＯＳ、Ｄｏｍａｉｎ－０がサービスシステム空間（管理用仮想マシン）であるクライアントＰＣに対して、管理サーバ上のコントローラが、ネットワークに接続されたリモート上にあるクライアントＰＣ上のＷｉｎｄｏｗｓのパッチ情報、システム設定情報、セキュリティポリーシ、各種ユーザソフトウェアのレビジョン等が管理サーバ上で保持しているユーザ・システム・ディスク内の左記情報と異なることを検知した場合、コントローラーは、クライアントＰＣ上にあるＤｏｍａｉｎ－０上のサービスソフト（アクセス権制御ソフトウェア２０１に相当）と連携して、Ｄｏｍａｉｎ－Ｕがオープンしていた場合はクローズ（Shutdown）し、ユーザ・システム・ディスクを管理サーバ上にあるユーザ・システム・ディスク に書き換え、先にDomain-Uをクローズした場合は再オープン（Ｗａｋｅｕｐ）する。システム上にある１個以上のクライアントＰＣに対してこれを実行することにより、管理者はシステム内のクライアントＰＣのセキュリティポリシーの一元化が可能になる。

【００２０】

次に、ユーザ用仮想マシン６Ｂからユーザ・ディスク・スペース６Ｃへのアクセスについて説明する。

仮想マシンモニタ５は、ユーザ用仮想マシン６Ｂからユーザ・ディスク・スペース６Ｃへのアクセスを監視する。ユーザ用仮想マシン６Ｂからユーザ・ディスク・スペース６Ｃへのアクセスがあった場合、アクセス権制御ソフトウェア２０１がユーザ用仮想マシン６Ｂに対してユーザ・ディスク・スペース６Ｃへのアクセス権を与えているときに、仮想マシンモニタ５は、ユーザ用仮想マシン６Ｂからユーザ・ディスク・スペース６Ｃへのアクセスへのアクセスを許可する。

【００２１】

アクセス権制御ソフトウェア２０１は、ユーザ用仮想マシン６Ｂが起動するときに、管理サーバ１００との通信を試みる。通信が成功した場合、アクセス権制御ソフトウェア２

０１は、サーバソフトウェア１１０に対してアクセスキー１３０の送信を要求する。そして、アクセス権制御ソフトウェア２０１は、サーバソフトウェア１１０が送ってきたアクセスキー１３０の認証処理を実行する。認証処理が成功した場合、アクセス権制御ソフトウェア２０１は、仮想マシンモニタ５にユーザ用仮想マシン６Ｂに対してユーザ・ディスク・スペース６Ｃへのアクセス権を与えることを通知する。認証処理が失敗した場合、アクセス権制御ソフトウェア２０１は、仮想マシンモニタ５にユーザ用仮想マシン６Ｂに対してユーザ・ディスク・スペース６Ｃへのアクセス権を与えることを通知しない。

【００２２】

この処理を図２のフローチャートを参照して説明する。

アクセス権制御ソフトウェア２０１は、管理サーバ１００との通信を試みる（ステップＳ１１）。通信に成功したら（ステップＳ１２のＹＥＳ）、アクセス権制御ソフトウェア２０１は管理サーバ１００に対してアクセスキー１３０の送信を要求する（ステップＳ１３）。管理サーバ１００は、要求に応じてアクセスキー１３０を送信する（ステップＳ１４）。アクセス権制御ソフトウェア２０１は、受信したアクセスキー１３０が正当な者であるか否かを判別するために認証処理を行う（ステップＳ１５）。

【００２３】

認証に成功したら（ステップＳ１６のＹＥＳ）、アクセス権制御ソフトウェア２０１は、ユーザ用仮想マシン６Ｂに対して、ユーザ・ディスク・スペース６Ｃへのアクセス権を与える（ステップＳ１７）。

【００２４】

このように、アクセス権制御ソフトウェア２０１は、管理サーバ１００が有するアクセスキー１３０と認証処理を行って、認証が成功した場合にユーザ用仮想マシン６Ｂに対してユーザ・ディスク・スペース６Ｃのアクセス権を与えることで、多くのディスク資源を必要とせずに、未許可状態での持ち出しによる機密情報データ等の漏洩を防止することが出来る。

【００２５】

例えば、仮想マシンモニタがＸＥＮで提供され、かつＤｏｍａｉｎ　０のサービスシステム空間（管理用仮想マシン）がユーザ・ディスク・スペース６Ｃを仮想ディスクイメージとして保有するクライアントＰＣを挙げる。サービスシステム内のサービスソフト（アクセス権制御ソフトウェア２０１に相当）が管理サーバに対してアクセスキーの取得を試み、一定期間内でアクセスキーの取得ができ、かつ正当であると判断されたとき、ＸＥＮのＤｏｍａｉｎ　０のサービスソフトはユーザシステム（Ｄｏｍａｉｎ－Ｕ）を起動するＸＥＮスクリプト上に左記仮想ディスクイメージが存在するファイル、もしくはディスク名が明記されたスクリプトを実行する。これにより、ユーザシステム起動時に個人データディスクが提供される。

【００２６】

［Ｋｅｅｐ　Ａｌｉｖｅ処理］

また、図３に示すように、アクセス権制御ソフトウェア２０１は、管理サーバ１００との間で一定間隔の通信（Keep Alive）を実施し、管理サーバ１００との接続が有効であるか確認する。そして、アクセス権制御ソフトウェア２０１は、確認状態によりユーザ用仮想マシン６Ｂに対してダイナミックにユーザ・ディスク・スペース６Ｃのアクセス権の提供を停止（Ｓｕｓｐｅｎｄ）、及び再開（Ｒｅｓｕｍｅ）する。

【００２７】

アクセス権制御ソフトウェア２０１が管理サーバ１００から一定期間応答が無いと判断した場合にユーザ用仮想マシン６Ｂに対するユーザ・ディスク・スペース６Ｃへのアクセス権の提供を停止する。その後、アクセス権制御ソフトウェア２０１が管理サーバ１００へのKeep Aliveを引き続き試み、もし、管理サーバ１００からの応答が回復した場合にユーザ用仮想マシン６Ｂに対してユーザ・ディスク・スペース６Ｃへのアクセス権の提供を再開する。

【００２８】

この処理を図４のフローチャートを参照して説明する。
アクセス権制御ソフトウェア２０１は、管理サーバ１００との間で一定間隔の通信（Keep Alive）を実施する（ステップＳ２１）。管理サーバ１００からの応答が無い場合（ステップＳ２２のＮＯ）、アクセス権制御ソフトウェア２０１は、ユーザ用仮想マシン６Ｂに対するユーザ・ディスク・スペース６Ｃへのアクセス権の提供を停止する（ステップＳ２３）。
【００２９】
そして、管理サーバ１００との間で一定間隔の通信（Keep Alive）を実施する（ステップＳ２４）。管理サーバ１００からの応答があった場合、アクセス権制御ソフトウェア２０１は、ユーザ用仮想マシン６Ｂに対してユーザ・ディスク・スペース６Ｃへのアクセス権を再び与える（ステップＳ２６）。
【００３０】
このように、管理サーバ１００との通信がとぎれたら、アクセス権の提供を停止することによって、認証後にクライアントＰＣ２Ａが持ち出されても、機密情報データ等の漏洩を防止することが出来る。
【００３１】
例として、仮想マシンモニタがＸＥＮで提供され、サービスシステム（管理用仮想マシン）がＤｏｍａｉｎ－０，ユーザシステムＤｏｍａｉｎ－Ｕ（ユーザ用仮想マシン）がＷｉｎｄｏｗｓ　ＸＰであるクライアントＰＣを挙げる。このクライアントＰＣ上のサービスシステム内のサービスソフト（アクセス権制御ソフトウェア２０１に相当）が管理サーバとのＫｅｅｐ　Ａｌｉｖｅに対して応答がないと判断した場合、ユーザシステム（Ｄｏｍａｉｎ－Ｕ）上の個人データディスク（ユーザ・ディスク・スペース）への仮想ディスクＩＯドライバを切断する。このとき、Ｗｉｎｄｏｗｓからは、個人データディスクをマウントしているドライブが外れたと検知（Ｐｌｕｇ　Ｏｕｔ）し、以後ユーザによる個人データディスクへのアクセスが不可能になる。その後、サービスソフトが管理サーバとのＫｅｅｐ　Ａｌｉｖｅが再開したと判断した場合、再びＤｏｍａｉｎ－Ｕの左記仮想ディスクＩＯドライバをオープンする。このとき、Ｗｉｎｄｏｗｓは、個人データディスクをマウントしているドライブが接続された検知（Ｐｌｕｇ　Ｉｎ）し、ユーザによる個人データディスクへの接続が可能となる。
【００３２】
［クライアントＰＣ持出時のディスク・スペース入れ替え］
図５は、管理サーバ１００がユーザ用・ディスク・スペース６Ｃを持出用ディスク・スペース６Ｄに入れ替えることを示している。ユーザがクライアントＰＣ２Ａを外部へ持ち出して、他者にデータを開示するようなとき、ユーザ・ディスク・スペース６Ｃには、機密情報が含まれている可能性があり、場合によっては覗き見や紛失等により情報漏洩する場合がある。
【００３３】
これを防止するために管理者が予め管理サーバ１００上に１以上のデータを含む仮想的な持出用ディスク１４０を準備しておく。
【００３４】
クライアントＰＣ２Ａを外部に持ち出す際に、ユーザが管理サーバ１００に対して持ち出すための準備を行うように要求する。管理サーバ１００は、ユーザからの要求に応じて、クライアントＰＣ２Ａ上の管理用仮想マシン６Ａ内で動作するアクセス権制御ソフトウェア２０１と連携して、クライアントＰＣ２Ａ内に持出用・ディスク・スペース６Ｄを作成し、持出用・ディスク・スペース６Ｄ内に持出用ディスク１４０内のデータを格納する。アクセス権制御ソフトウェア２０１は、ユーザ用仮想マシン６Ｂが利用するディスク・スペースをユーザ・ディスク・スペース６Ｃから持出用・ディスク・スペース６Ｄに置き換える。
【００３５】
図６のフローチャートを参照してこの処理の手順を説明する。

ユーザが管理サーバ１１０に対してクライアントＰＣ２Ａの持出処理を行うように要求する。この要求は、例えばユーザ用仮想マシン６Ｂから送信される。管理サーバ１００は、アクセス権制御ソフトウェア２０１に対して、持出処理実行命令を送信する（ステップＳ３１）。

【００３６】

アクセス権制御ソフトウェア２０１は、要求に応じてユーザ用仮想マシン６Ｂに与えていたユーザ・ディスク・スペース６Ｃへのアクセス権を停止する（ステップＳ３２）。そして、持出用・ディスク・スペース６Ｄを準備する（ステップＳ３３）。管理サーバ１００は、持出用ディスク１４０内のデータをアクセス権制御ソフトウェア２０１に送信する（ステップＳ３４）

アクセス権制御ソフトウェア２０１は、管理サーバ１００から送信された持出用ディスク１４０内のデータを持出用・ディスク・スペース６Ｄ内に格納する（ステップＳ３５）。そして、アクセス権制御ソフトウェア２０１は、ユーザ用仮想マシン６Ｂに対して持出用・ディスク・スペース６Ｄのアクセス権を与える（ステップＳ３６）。なお、持出用・ディスク・スペース６Ｄのアクセス権の付与は、再起動後であっても、管理サーバ１００内のアクセスキー１３０の認証処理を行わずに行われる。

【００３７】

ユーザがクライアントＰＣ２Ａを外部へ持ち出して、他者にデータを開示するようなとき、機密情報が含まれてない持出用・ディスク・スペース６Ｄを準備して、ユーザ用仮想マシン６Ｂにアクセス権を与えることによって、機密情報データ等の漏洩を防止することが出来る。

【００３８】

例として、仮想マシンモニタがＸＥＮで提供され、サービスシステム（管理用仮想マシン）がＤｏｍａｉｎ－０、ユーザシステムＤｏｍａｉｎ－Ｕ（ユーザ用仮想マシン）がＷｉｎｄｏｗｓ　ＸＰであるクライアントＰＣを挙げる。このクライアントＰＣ上のサービスシステム内のサービスソフト（アクセス権制御ソフトウェア２０１に相当）は、まず、管理サーバ上からの個人データディスク（ユーザ・ディスク・スペース）入れ替え要求を受け付け、Ｄｏｍａｉｎ－Ｕが存在していればそれをクローズし、管理サーバから仮想ディスクイメージである持ち出し管理ディスクを受信し、ＸＥＮが提供するＤｏｍａｉｎ－Ｕスクリプト内の個人データディスクのファイル名、もしくはディスク名を書き換え、Ｄｏｍｉｎ－ＵをＤｏｍａｉｎ－０により必要なとき再起動（オープン）する。

【００３９】

［クライアントＰＣ持出時のアクセスレベル変更］

図７は、管理サーバ１００上で動作するサーバソフトウェア１１０からユーザ・ディスク・スペース６Ｃへのアクセスレベル（Ｒｅａｄ権／Ｗｒｉｔｅ権）の設定が可能であることを示している。

【００４０】

クライアントＰＣ２Ａを外部に持ち出す際に、ユーザが管理サーバ１００に対して持ち出すための準備を行うように要求する。管理サーバ上で動作するサーバソフトウェア１１０は、要求に応じて、管理用仮想マシン６Ａ内で動作するアクセス権制御ソフトウェア２０１と連携してユーザ・ディスク・スペース６Ｃのアクセスレベルを Ｒｅａｄ＋Ｗｒｉｔｅ権からＲｅａｄ権に入れ替える。

【００４１】

図８のフローチャートを参照してこの処理の手順を説明する。

ユーザが管理サーバ１００に対してクライアントＰＣ２Ａの持出処理を行うように要求する。この要求は、例えばユーザ用仮想マシン６Ｂから送信される。管理サーバ１００は、アクセス権制御ソフトウェア２０１に対して、持出処理実行命令を送信する（ステップＳ４１）。

【００４２】

アクセス権制御ソフトウェア２０１は、要求に応じてユーザ用仮想マシン６Ｂに与えて

いたユーザ・ディスク・スペース６Ｃへのアクセス権を停止する（ステップＳ４２）。アクセス権制御ソフトウェア２０１は、ユーザ用仮想マシン６Ｂのユーザ・ディスク・スペース６Ｃへのアクセスレベルを Ｒｅａｄ＋Ｗｒｉｔｅ権からＲｅａｄ権に変更する（ステップＳ４３）。そして、アクセス権制御ソフトウェア２０１は、ユーザ用仮想マシン６Ｂにユーザ・ディスク・スペース６Ｃへのアクセス権を与える。

【００４３】

なお、アクセスレベルがＲｅａｄ権のみに設定されたユーザ・ディスク・スペース６Ｃのアクセス権の付与は、再起動後であっても、管理サーバ１００内のアクセスキー１３０の認証処理を行わずに行われる。

【００４４】

このことにより、ユーザがクライアントＰＣ２Ａを外部に持ち出した際に機密情報を作為、不作為にかかわらず他者の機密情報などを個人データディスクに入れるて持ち帰るような不正、及びユーザによって改竄された情報の他者への提供を防止することが可能になる。

【００４５】

例として、仮想マシンモニタがＸＥＮで提供され、サービスシステム（管理用仮想マシン）がＤｏｍａｉｎ－０、ユーザシステムＤｏｍａｉｎ－Ｕ（ユーザ用仮想マシン）がＷｉｎｄｏｗｓ　ＸＰであるクライアントＰＣを挙げる。このクライアントＰＣ上のサービスシステム内のサービスソフト（アクセス権制御ソフトウェア２０１に相当）は、まず、管理サーバ１００上からのユーザ・ディスク・スペース６Ｃのアクセス権変更要求を受け付け、Ｄｏｍａｉｎ－Ｕが存在していればそれをクローズし、ＸＥＮが提供するＤｏｍａｉｎ－Ｕスクリプト内の個人データディスクのファイル名、もしくはディスク名のアクセスレベルの設定を変更（Ｒｅａｄ＋ＷｒｉｔｅからＲｅａｄへ）し、Ｄｏｍｉｎ－ＵをＤｏｍａｉｎ－０により必要なとき再起動（オープン）する。

【００４６】

［複数のユーザ・ディスク・スペース］

図９は、アクセス権制御ソフトウェア２０１が、それぞれにアクセスレベルが設定された複数の個人ユーザ・ディスク・スペースを用意して、ユーザ用仮想マシン６Ｂにアクセス権を与えることを示している。例えば、外出の際、管理サーバから与えられたＲｅａｄ権のみをもつ持出用・ディスク・スペース６Ｄ、Ｒｅａｄ＋Ｗｒｉｔｅ権をもつ空データのディスク・スペース６Ｅを提供する。

【００４７】

これにより、外出時に開示可能な情報のみが持出用・ディスク・スペース６Ｄから他者に情報提供され、かつ入手した必要な情報をディスク・スペース６Ｅに格納可能になる。このとこは、１個のユーザ・ディスク・スペースが提供されている場合と比較して、持ち出したクライアントＰＣ内での左記にあげた開示情報と入手情報の混在による情報の誤使用が防止される効果がある。

【００４８】

［アクセスキーのコピー］

図１０は、クライアントＰＣ２Ａを外部に持ち出す際の管理サーバからのアクセスキーの配布において、ネットワーク経由ではなく、挿抜可能な記憶装置（ＳＤカード、ＵＳＢメモリ）４００を経由して配布することを示している。

【００４９】

図１で提示した方法では、管理サーバ１００と物理的にアクセス不可能な環境にクライアントＰＣ２Ａを持ち出したとき、ユーザによるユーザ・ディスク・スペース６Ｃへのアクセスが不可能になる。これを回避するために、管理者が管理サーバ１００上にある持ち出し対象であるクライアントＰＣ２Ａのアクセスキーを記憶装置４００にコピーし、これを入手したユーザがクライアントＰＣ２Ａ上のドライブ装置４０１に差し込んだ後、アクセス権制御ソフトウェア２０１が認証処理を行うことによって、ユーザ用仮想マシン６Ｂに対してユーザ・ディスク・スペース６Ｃの提供が可能になる。

【００５０】
この処理を図１１のフローチャートを参照して説明する。
管理サーバ１００との通信を試みて、通信を行うことが出来なかったら（図２のステップＳ１２のＮＯに相当）、アクセス権制御ソフトウェア２０１は、ドライブ装置４０１にアクセスキーが格納された記憶装置４００が挿入されているかを検出する（ステップＳ５１）。検出できなかった場合（ステップＳ５１のＮＯ）、アクセス権制御ソフトウェア２０１は処理を終了する。
【００５１】
検出できた場合（ステップＳ５１のＹＥＳ）、アクセス権制御ソフトウェア２０１は記憶装置４００からアクセスキーを読み出す（ステップＳ５２）。アクセス権制御ソフトウェア２０１は、読み出したアクセスキーが正当な者であるか否かを判別するために認証処理を行う（ステップＳ５３）。
【００５２】
認証に成功したら（ステップＳ５３のＹＥＳ）、アクセス権制御ソフトウェア２０１は、ユーザ用仮想マシン６Ｂに対して第１サーバ１０に対して、ユーザ・ディスク・スペースへのアクセス権を与える（ステップＳ１７）。認証に失敗したら（ステップＳ５３のＮＯ）、アクセス権制御ソフトウェア２０１は処理を終了する。
【００５３】
例として、仮想マシンモニタがＸＥＮで提供され、サービスシステム（管理用仮想マシン）がＤｏｍａｉｎ－０，ユーザシステムＤｏｍａｉｎ－Ｕ（ユーザ用仮想マシン）がＷｉｎｄｏｗｓ　ＸＰであるクライアントＰＣを挙げる。クライアントＰＣがネットワークに接続されていない状況でユーが外部に持ち出したクライアントＰＣの電源をＯＮにする。まず、サービスシステム空間（Ｄｏｍａｉｎ－０）が起動し、サービスシステム内のサービスソフト（アクセス権制御ソフトウェア２０１に相当）は、管理サーバと通信可能かをチェックする。もし、通信不可能なとき、仮想ＰＣ上のドライブにアクセスキーの入った物理媒体が差し込まれているかをチェックし、物理媒体が存在し、かつそれに含まれるアクセスキーが正当なものと判断されたとき、サービスシステムは個人データディスクを構成するＤｏｍａｉｎ－０上の仮想ディスクイメージ、もしくはデバイスを含むＸＥＮスクリプト実行することにより、Ｄｏｍａｉｎ－Ｕ（Ｗｉｎｄｏｗｓ）はサービスシステムから個人データディスクが提供された状態で起動する。
【００５４】
［ファイル一覧情報］
図１２は、本発明の一実施形態に係わる情報処理システムの概略構成を示す図である。なお、図１２において、図１と同一な部位には同一符号を付し、説明を省略する。
【００５５】
この管理サーバ１００のサーバソフトウェア１１０は、管理サーバ１００にネットワークを介して接続されている各クライアントＰＣ２Ａ～２Ｃのユーザ・ディスク・スペース６Ｃに格納されている各ファイルのパス（ファイル名を含む）およびファイルが格納されているユーザ・ディスク・スペース６Ｃを使用しているユーザ等の情報が登録されているファイル一覧情報５０１Ａを作成する。なお、ファイル一覧情報５０１Ａにはファイル内のテキスト情報を登録しても良い。
【００５６】
サーバソフトウェア１１０は、管理用ＡＰＰ９Ａの一つであるファイル一覧取得/送信ソフト５１１に対してユーザ・ディスク・スペース６Ｃに格納されているファイルの一覧を送信するように指示し、指示に基づいて送信された各クライアントＰＣ２Ａ～２Ｃのファイル一覧に基づいてファイル一覧情報５０１Ａを作成する。ファイル一覧/送信ソフト５１１は、サーバソフトウェア１１０からの要求に基づいて、ユーザ・ディスク・スペース６Ｃにアクセスしてファイルの一覧を取得する。
【００５７】
そして、サーバソフトウェア１１０は、クライアントＰＣ２Ａ～２Ｃのユーザ用仮想マ

シン６Ｂ内で動作するユーザアプリケーション９Ｂの一つであるファイル一覧情報要求ソフト５２１からの要求に応じて、要求があったクライアントＰＣ２Ａ～２Ｃのユーザ・ディスク・スペース６Ｃにファイル一覧情報５０１Ａの複製であるファイル一覧情報５０１Ｂを作成する処理を実行する。

【００５８】

ユーザアプリケーション９Ｂとしての検索ソフト５０３は、ファイル一覧情報５０１Ｂからファイル名やファイル内のテキスト情報等を用いてキーワード検索を行うを有する。

【００５９】

以下に、管理サーバ１００が、ファイル一覧情報を作成する処理の手順を図１３のフローチャートを参照して説明する。

管理サーバ１００上で動作するサーバソフトウェア１１０は、各クライアントＰＣ２Ａ～２Ｃのファイル一覧取得/送信ソフト５１１に対してファイル一覧の送信を要求する（ステップＳ６１）。各クライアントＰＣ２Ａ、２Ｂのファイル一覧取得/送信ソフト５１１は、それぞれのユーザ・ディスク・スペース６Ｃにアクセスして（ステップＳ６２Ａ，６２Ｂ）、ユーザ・ディスク・スペース６Ｃに格納されているファイルのパスの一覧を取得する（ステップＳ６３Ａ，６３Ｂ）。そして、取得したファイルのパスの一覧をユーザ名と共に管理サーバ１００に対して送信する（ステップＳ６４Ａ，６４Ｂ）。管理サーバ１００は、各クライアントＰＣのファイルのパスの一覧を取得し（ステップＳ６５）、ファイル一覧情報５０１Ａを生成する（ステップＳ６６）。

【００６０】

なお、上記処理は、図１４のフローチャートに示すように、サーバソフトウェア１１０は、ユーザ等の要求があった場合、或いは定期的にファイル一覧情報の更新処理を実行する。

図１４のフローチャートに示す処理を以下に説明する。サーバソフトウェア１１０は、クライアントＰＣ２Ａ～２Ｃからファイルの一覧更新要求が有ったか否かを判別する（ステップＳ７１）。要求がなかったと判断した場合（ステップＳ７１のＮＯ）、最後にファイル一覧を生成してからＮ秒経過したか否かを判別する（ステップＳ７２）。Ｎ病経過していないと判断した場合（ステップＳ７２のＮＯ）、一定時間後にステップＳ７１の処理を実行する。ステップＳ７１において要求があったと判断した場合（ステップＳ７１のＹＥＳ）、或いはステップＳ７２においてＮ秒経過したと判断した場合（ステップＳ７２のＹＥＳ）、サーバソフトウェア１１０は上述した、各クライアントＰＣからファイルの一覧を取得し、ファイル一覧情報の更新処理を実行する（ステップＳ７３）。

【００６１】

次に、あるクライアントＰＣ２Ｂ上にあるユーザが、同一グループにある他ユーザのクライアントＰＣ２Ａのユーザディスク上にあるァイルへのリモートアクセスする手順を図１５のフローチャートを参照して説明する。

【００６２】

まず、管理サーバ上のサーバソフトウェアは１個以上のユーザからなる１個のグループをあらかじめ作成する。次に図１３の方法を用いて管理サーバ１００にファイル一覧情報５０１Ａを作成する（ステップＳ８１）。

【００６３】

クライアントＰＣ２Ｂ内で動作するファイル一覧情報要求ソフト５２１は、管理サーバ１００に対してファイル一覧の取得要求を送信する（ステップＳ８２）。管理サーバ１００のサーバソフトウェア１１０は、取得要求を受信すると（ステップＳ８３）、クライアントＰＣ２Ｂのユーザ・ディスク・スペース６Ｃに対して、ファイル一覧情報５０１Ａを送信する（ステップＳ８４）。クライアントＰＣ２Ｂは、受信したデータからユーザ・ディスク・スペース６Ｃ内にファイル一覧情報５０１Ｂを作成する（ステップＳ８５）。

【００６４】

ファイル一覧情報５０１Ｂの中から検索ソフト５０３を用いて検索されたクライアントＰＣ２Ａのユーザ・ディスク・スペース６Ｃ内に格納されているファイル名ａ１に対して

クライアントＰＣ２Ｂを使用しているユーザがアクセスしたいと考えた場合を説明する。

【００６５】

ユーザの操作に応じて、クライアントＰＣ２Ｂのユーザアプリケーション９Ｂは、管理サーバ１００に対してファイル名ａ１のパスと要求元ユーザ名とを含むアクセス可否要求を送信する（ステップＳ８６）。管理サーバ１００がファイルアクセス可否要求を受信すると（ステップＳ８７）、要求元ユーザ名（ユーザｂ）が、ファイルａ１が格納されているクライアントＰＣ２Ａの使用者であるユーザａと同一グループであるか否かを判別する（ステップＳ８８）。管理サーバ１００は、判別結果に応じたアクセス要求に対する可否通知をクライアントＰＣ２Ｂに送信する（ステップＳ８９）。管理サーバ１００は、ユーザｂとユーザａとが同じグループであれば“ＹＥＳ”、異なるグループであれば“ＮＯ”を送信する。

【００６６】

クライアントＰＣ２Ｂのユーザアプリケーション９Ｂは、可否通知を受信すると（ステップＳ９０）、アクセスが可能であるか否かを判別する（ステップＳ９１）。アクセス可ではないと判断した場合（ステップＳ９１のＮＯ）、クライアントＰＣ２Ｂはファイル名ａ１に関するアクセス処理を終了する。アクセス可であると判断した場合（ステップＳ９１のＹＥＳ）、クライアントＰＣ２Ｂのユーザアプリケーション９Ｂは管理サーバ１００に対してアクセス種別に応じたアクセス要求を送信する（ステップＳ９２）。ユーザｂからのファイル名ａ１へのアクセス要求を受信すると（ステップＳ９３）、管理サーバ１００は、ユーザｂからのファイル名ａ１へのアクセス実施要求をクライアントＰＣ２Ａに対して送信する（ステップＳ９４）。

【００６７】

アクセス実施要求を受信すると（ステップＳ９５）、クライアントＰＣ２Ａは、ファイル名ａ１へのアクセスを実施する（ステップＳ９６）。クライアントＰＣ２Ａは、ユーザｂ宛のファイル名ａ１へのアクセス実施結果を管理サーバ１００に送信する（ステップＳ９７）。

【００６８】

管理サーバ１００は、アクセス実施結果を受信すると（ステップＳ９８）、ユーザｂ宛のファイル名ａ１へのアクセス実施結果をクライアントＰＣ２Ｂに送信する（ステップＳ９９）。クライアントＰＣ２Ｂは、ファイル名ａ１へのアクセス結果を受信すると（ステップＳ１００）、ファイル名ａ１へのアクセスを実施するか否かを判別し（ステップＳ１０１）する。実施する場合（ステップＳ１０１のＹＥＳ）、ステップＳ９２に戻って、再度アクセス実施要求を送信する。また、実施しない場合（ステップＳ１０１のＮＯ）、処理を終了する。

【００６９】

上述したシステムによれば、各クライアントＰＣ上のユーザ・ディスク・スペース６Ｃ内に格納されているファイル一覧の取得、取得された情報を用いた検索や、同一グループに所属する別クライアントＰＣのユーザ・ディスク・スペース６Ｃへの共有アクセスを可能にすることにより、大容量のファイルサーバを使用することなく、少ないディスク資源を有効活用できる等の効果がある。

【００７０】

なお、本発明は、上記実施形態そのままに限定されるものではなく、実施段階ではその要旨を逸脱しない範囲で構成要素を変形して具体化できる。また、上記実施形態に開示されている複数の構成要素の適宜な組み合せにより種々の発明を形成できる。例えば、実施形態に示される全構成要素から幾つかの構成要素を削除してもよい。更に、異なる実施形態に亘る構成要素を適宜組み合せてもよい。

【図面の簡単な説明】

【００７１】

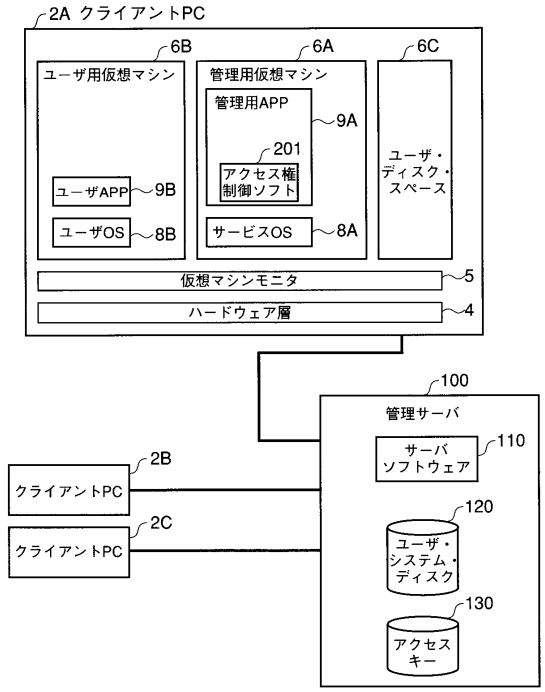
【図１】本発明の一実施形態に係わる情報処理システムの構成を示すブロック図。

【図２】クライアントＰＣと管理サーバとの間で行われる認証処理の手順を示すフローチ

ャート。
【図３】本発明の一実施形態に係わる情報処理システムにおけるＫｅｅｐ　Ａｌｉｖｅ処理を行っている状態を示す図。
【図４】Ｋｅｅｐ　Ａｌｉｖｅ処理の手順を示すフローチャート。
【図５】管理サーバがユーザ・ディスク・スペースを持出用・ディスク・スペースに入れ替えることを示す図。
【図６】ユーザ・ディスク・スペースを持出用・ディスク・スペースに入れ替える手順を示すフローチャート。
【図７】ユーザ・ディスク・スペースへのアクセスレベルの変更を示す図。。
【図８】ユーザ・ディスク・スペースへのアクセスレベルを変更する手順を示すフローチャート。
【図９】複数のユーザ・ディスク・スペースをユーザシステムに提供し、それぞれにアクセスレベルを設定をしている状態を示す図。
【図１０】記憶装置にアクセスキーを格納して、認証処理を行う状態を示す図。
【図１１】記憶装置に格納されたアクセスキーによって認証処理を行う手順を示すフローチャート。
【図１２】本発明の一実施形態に係わる情報処理システムの概略構成を示す図。
【図１３】管理サーバがファイル一覧情報を作成する処理の手順を示すフローチャート。
【図１４】ファイル一覧情報の更新処理の手順を示すフローチャート。
【図１５】クライアントＰＣ上にあるユーザが、同一グループにある他ユーザのクライアントＰＣのユーザディスク上にあるァイルへのリモートアクセスする手順を示すフローチャート。
【符号の説明】
【００７２】
６Ａ…管理用仮想マシン，６Ｂ…ユーザ用仮想マシン，６Ｃ…ユーザ・ディスク・スペース，６Ｄ…持出用・ディスク・スペース，６Ｅ…ディスク・スペース，８Ａ…サービスオペレーティングシステム，８Ｂ…ユーザオペレーティングシステム，９Ａ…管理用アプリケーション，９Ｂ…ユーザアプリケーション，１００…管理サーバ，１１０…サーバソフトウェア，１２０…ユーザ・システム・ディスク，１３０…アクセスキー，１４０…持出用ディスク，２０１…アクセス権制御ソフトウェア，４００…記憶装置，４０１…ドライブ装置。

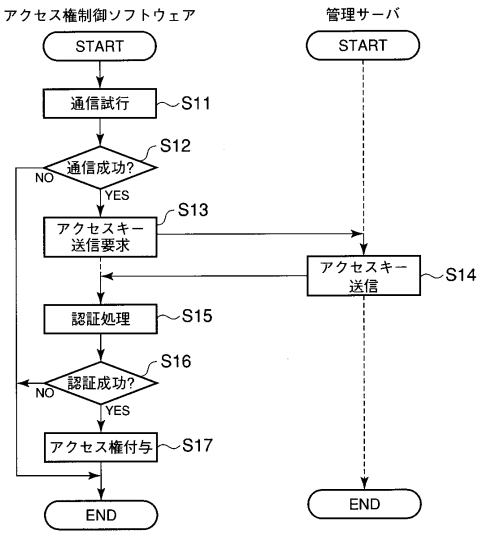
【図１】

図１



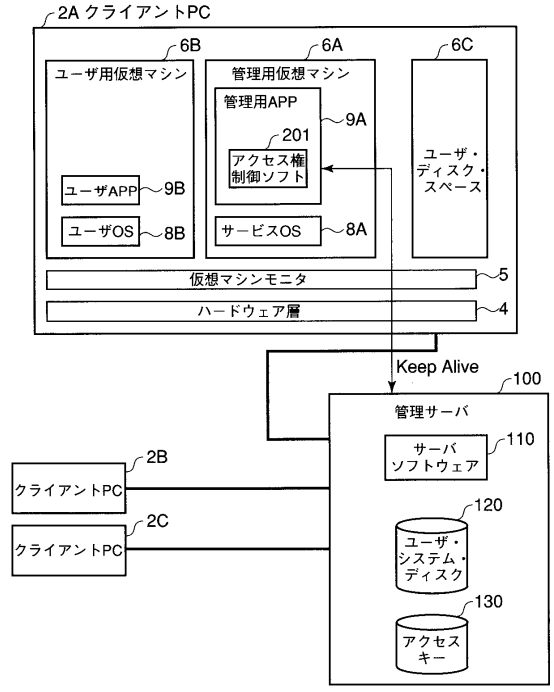
【図２】

図２



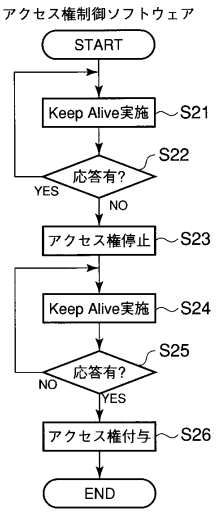
【図３】

図３



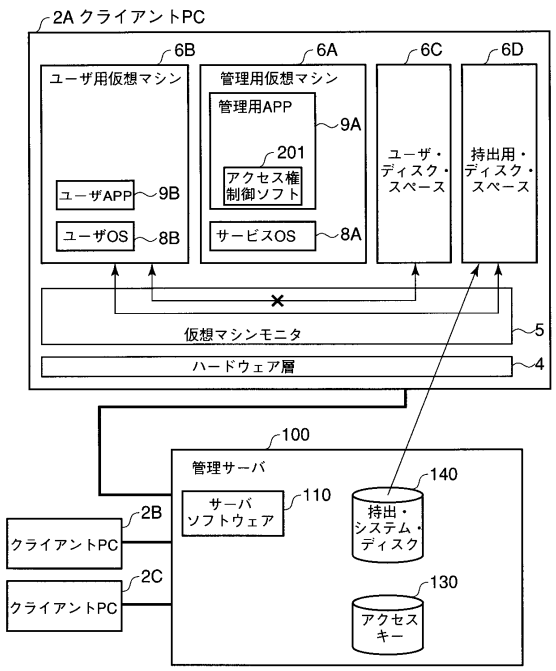
【図４】

図４



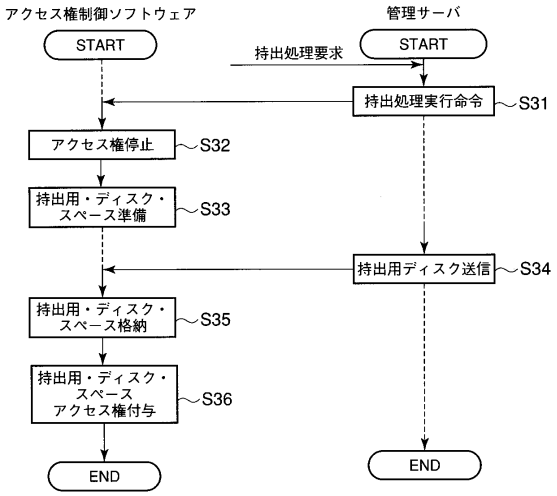
【図５】

図５



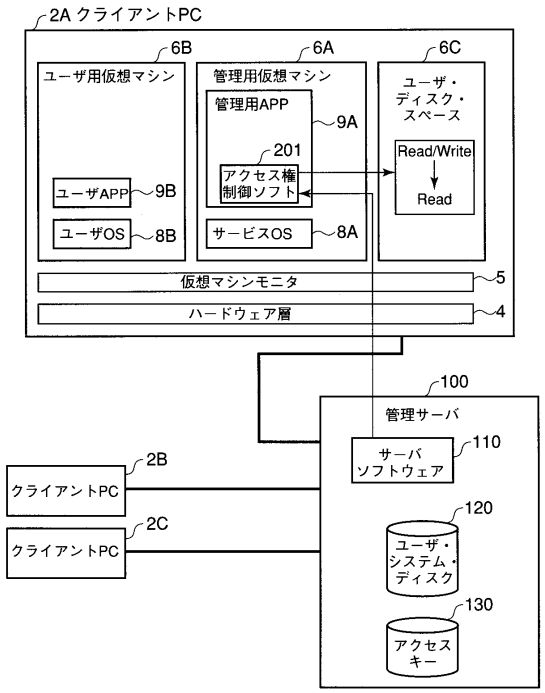
【図６】

図６



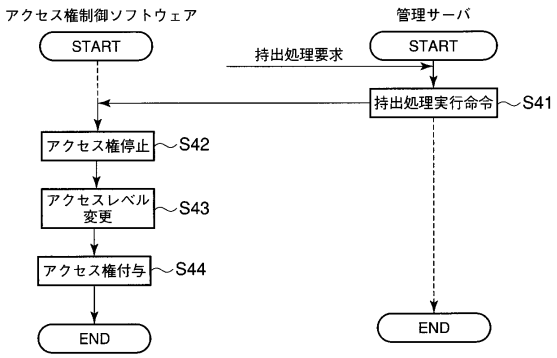
【図７】

図７



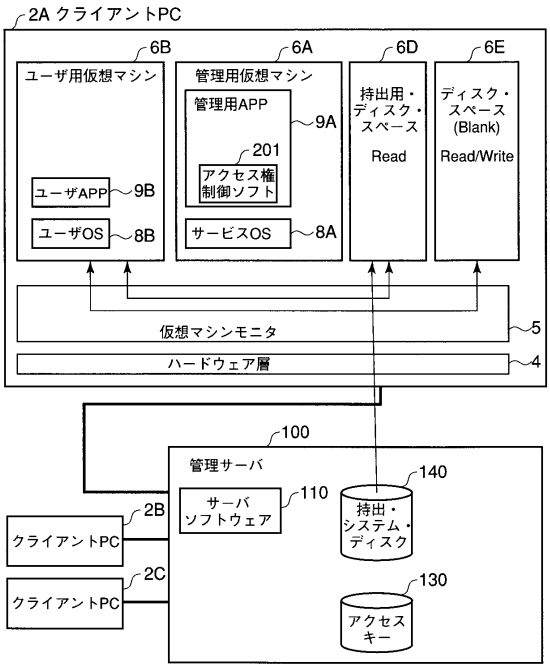
【図８】

図８



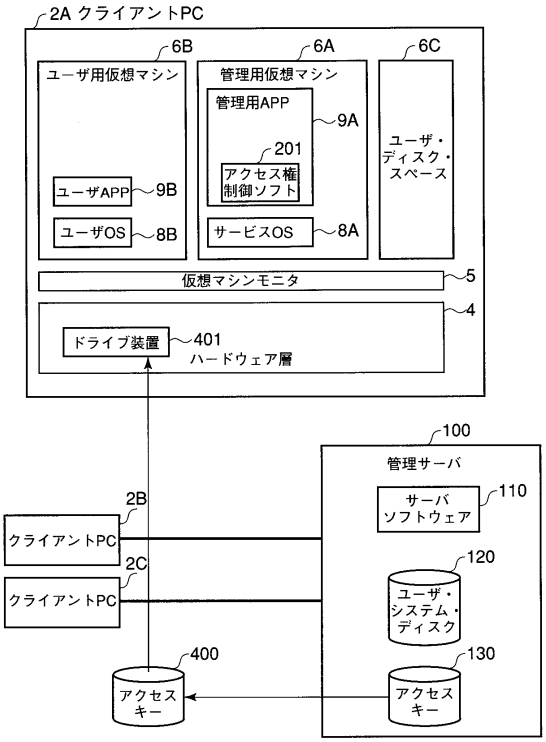
【図９】

図9



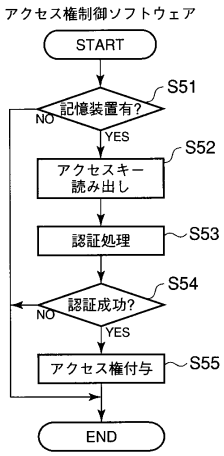
【図１０】

図10



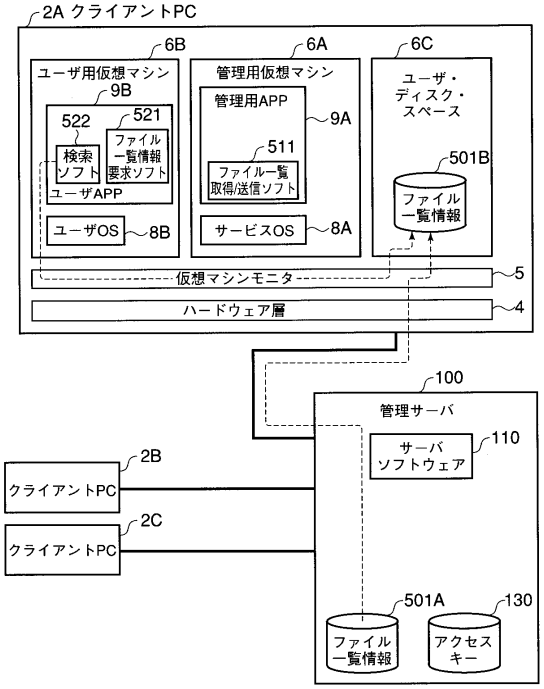
【図１１】

図11



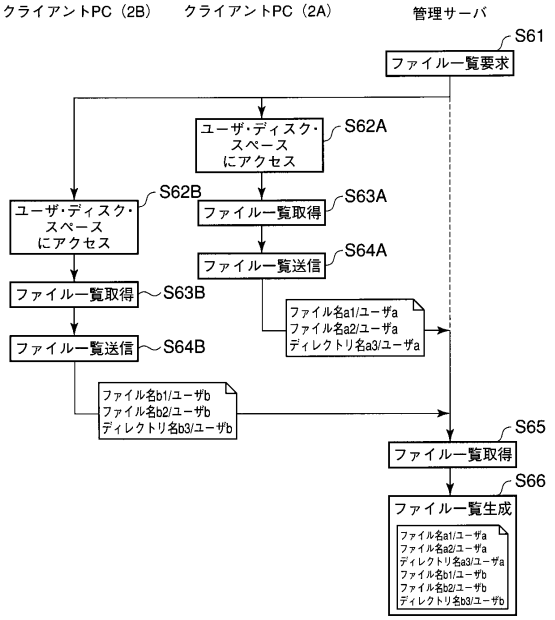
【図１２】

図12



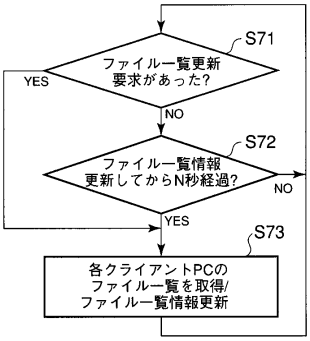
【図１３】

図 13



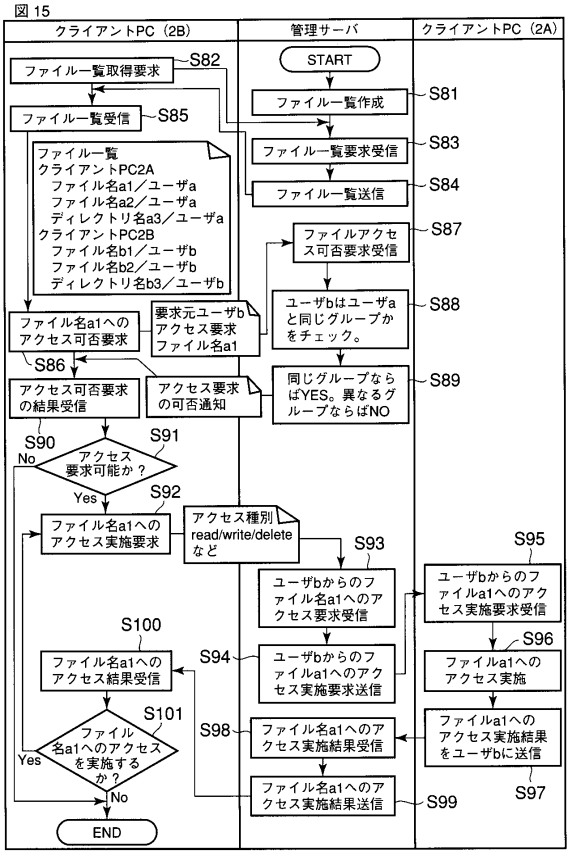
【図１４】

図 14



【図１５】

図 15



フロントページの続き

(74)代理人 100095441
弁理士 白根 俊郎
(74)代理人 100084618
弁理士 村松 貞男
(74)代理人 100103034
弁理士 野河 信久
(74)代理人 100119976
弁理士 幸長 保次郎
(74)代理人 100153051
弁理士 河野 直樹
(74)代理人 100140176
弁理士 砂川 克
(74)代理人 100101812
弁理士 勝村 紘
(74)代理人 100092196
弁理士 橋本 良郎
(74)代理人 100100952
弁理士 風間 鉄也
(74)代理人 100070437
弁理士 河井 将次
(74)代理人 100124394
弁理士 佐藤 立志
(74)代理人 100112807
弁理士 岡田 貴志
(74)代理人 100111073
弁理士 堀内 美保子
(74)代理人 100134290
弁理士 竹内 将訓
(74)代理人 100127144
弁理士 市原 卓三
(74)代理人 100141933
弁理士 山下 元
(72)発明者 六波羅 勉
東京都港区芝浦一丁目１番１号 株式会社東芝内
(72)発明者 押切 洋
東京都港区芝浦一丁目１番１号 株式会社東芝内

審査官 岸野 徹

(56)参考文献 特開２００３－３４５６５４（ＪＰ，Ａ）
国際公開第２００７／０４９６２５（WO，Ａ１）
特開２００４－３１８７２０（ＪＰ，Ａ）
特開２００８－２６９５４４（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ ２１／２４
Ｇ０６Ｆ １２／００