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

特許第4987555号
(P4987555)

(45)発行日　平成24年7月25日(2012.7.25)　(24)登録日　平成24年5月11日(2012.5.11)

(51)Int.Cl.　F I
G06F 9/46 (2006.01)　G06F 9/46 350
G06F 15/00 (2006.01)　G06F 15/00 440Z

請求項の数 17　(全 21 頁)

(21)出願番号　特願2007-119837(P2007-119837)
(22)出願日　平成19年4月27日(2007.4.27)
(65)公開番号　特開2008-276546(P2008-276546A)
(43)公開日　平成20年11月13日(2008.11.13)
審査請求日　平成22年1月7日(2010.1.7)

(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　100091351
弁理士　河野　哲
(74)代理人　100088683
弁理士　中村　誠
(74)代理人　100108855
弁理士　蔵田　昌俊
(74)代理人　100075672
弁理士　峰　隆司
(74)代理人　100109830
弁理士　福原　淑弘
(74)代理人　100084618
弁理士　村松　貞男

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】
仮想マシンモニタ上で動作し、お互いのアクセスが制限されている社内用仮想マシンと、外部機器へのデータ出力が制限された社外用仮想マシンとのいずれか一方を選択的に動作する情報処理装置であって、
前記仮想マシンモニタ上で動作し、起動情報に応じて前記社内用仮想マシンおよび前記社外用仮想マシンの一方の仮想マシンを起動する起動手段と、
前記仮想マシンモニタ上で動作し、ネットワークを介して管理サーバとの通信を実行する通信手段と、
前記管理サーバからの指令に応じて前記起動情報を変更する変更手段と、
を具備する情報処理装置。
【請求項２】
前記通信手段は、前記管理サーバに前記情報処理装置の社外への持ち出しを申請するための持ち出し申請手段であり、
前記管理サーバから前記情報処理装置の持ち出しを許可する応答が送信された場合に、前記変更手段は、前記起動情報を前記社内用仮想マシンから前記社外用仮想マシンを示すデータに変更し、
前記起動手段は、前記社内用仮想マシンをシャットダウンした後、前記社外用仮想マシンを起動する
請求項１に記載の情報処理装置。

【請求項３】
前記持ち出し申請手段は、
前記社内用仮想マシン上で動作する、前記管理サーバによって作成された持ち出し承認確認ログインＷｅｂ頁に表示される持ち出し処理開始ボタンが操作された場合に持ち出し処理の開始メッセージを前記管理サーバに送信する開始メッセージ送信手段とを具備する
請求項２に記載の情報処理装置。
【請求項４】
前記通信手段は、前記管理サーバに前記情報処理装置の持ち帰りを申請するための持ち帰り申請手段であり、
前記管理サーバから前記情報処理装置の持ち帰りの応答が送信された場合に、前記変更手段は、前記起動情報を前記社内用仮想マシンから前記社外用仮想マシンを示すデータに変更し、
前記起動手段は、前記社外用仮想マシンをシャットダウンし、前記社内用仮想マシンを起動する
請求項１に記載の情報処理装置。
【請求項５】
前記ネットワークは、第１の社内ＬＡＮと、この第１の社内ＬＡＮと直接接続されていない第２の社内ＬＡＮとを含み、
前記管理サーバは前記第１の社内ＬＡＮに接続され、
前記情報処理装置は前記第２の社内ＬＡＮに接続された時に、前記管理サーバに対して前記社外用仮想マシンから前記社内用仮想マシンに切り替えるための切替申請を送信する送信手段を更に具備する
請求項１に記載の情報処理装置。
【請求項６】
前記切替申請は出張先到着申請であり、
前記管理サーバによって前記社外用仮想マシンから前記社内用仮想マシンへの切替が承認された場合に、前記変更手段は、前記起動情報を前記社内用仮想マシンから前記社外用仮想マシンを示すデータに変更し、
前記起動手段は、前記社外用仮想マシンをシャットダウンした後、前記社内用仮想マシンを起動する
請求項５に記載の情報処理装置。
【請求項７】
前記仮想マシンモニタ上には、管理用仮想マシンが動作しており、
前記管理用仮想マシンは、前記社内用仮想マシンおよび前記社外用仮想マシンからアクセスが可能な共有データ領域を有する、
請求項１記載の情報処理装置。
【請求項８】
前記ネットワークは、インターネットを含む、
前記管理サーバはインターネット上に設置され、複数の仮想マシンのイメージファイルを有し、
前記管理サーバから前記情報処理装置を使用する加入者の契約に応じた仮想マシンのイメージファイルをダウンロードする手段を更に具備する
請求項１に記載の情報処理装置。
【請求項９】
管理サーバと、
前記管理サーバとネットワークを介して接続され、仮想マシンモニタ上で動作し、お互いのアクセスが制限されている社内用仮想マシンと、外部機器へのデータ出力が制限された社外用仮想マシンとのいずれか一方を選択的に動作する情報処理装置を具備する情報処理システムであって、
前記情報処理装置は、

前記仮想マシンモニタ上で動作し、起動情報に応じて前記社内用仮想マシンおよび前記社外用仮想マシンの一方の仮想マシンを起動する起動手段と、
前記仮想マシンモニタ上内で動作し、ネットワークを介して管理サーバとの通信を実行し、前記管理サーバからの指令に応じて前記起動情報を変更する変更手段とを有する
情報処理システム。
【請求項１０】
前記情報処理装置は前記管理サーバに前記情報処理装置の社外への持ち出しを申請するための持ち出し申請手段であり、
前記管理サーバから前記情報処理装置の持ち出しを許可する応答が送信された場合に、前記変更手段は、前記起動情報を前記社内用仮想マシンから前記社外用仮想マシンを示すデータに変更し、
前記起動手段は、前記社内用仮想マシンをシャットダウンした後、前記社外用仮想マシンを起動する
請求項９に記載の情報処理システム。
【請求項１１】
前記情報処理装置は、
前記社内用仮想マシン上で動作する、前記管理サーバによって作成された持ち出し承認確認ログインＷｅｂ頁に表示される持ち出し処理開始ボタンが操作された場合に持ち出し処理の開始メッセージを前記管理サーバに送信する開始メッセージ送信手段を具備し、
前記管理サーバは、前記承認確認ログインＷｅｂ頁を生成するＷｅｂ頁生成手段を具備する、
請求項１０に記載の情報処理システム。
【請求項１２】
前記通信手段は、前記管理サーバに前記情報処理装置の持ち帰りを申請するための持ち帰り申請手段であり、
前記変更手段は、前記管理サーバから前記情報処理装置の持ち帰りの応答が送信された場合に、前記起動情報を前記社内用仮想マシンから前記社外用仮想マシンを示すデータに変更し、
前記起動手段は、前記社外用仮想マシンをシャットダウンし、前記社内用仮想マシンを起動する
請求項９に記載の情報処理システム。
【請求項１３】
前記管理サーバは、前記社内用仮想マシンから前記社外用仮想マシンへの切り替えが行われた情報処理装置を管理するデータベースを有し、
前記情報処理システムは、前記データベースに基づいて前記社内用仮想マシンから前記社外用仮想マシンのへの切り替えが行われているかを検査する検査装置を更に具備する、
請求項９に記載の情報処理システム。
【請求項１４】
前記仮想マシンモニタ上には、管理用仮想マシンが動作しており、
前記管理用仮想マシンは、前記社内用仮想マシンおよび前記社外用仮想マシンからアクセスが可能な共有データ領域を有する、
請求項９に記載の情報処理システム。
【請求項１５】
前記ネットワークは、第１の社内ＬＡＮ、この第１の社内ＬＡＮと直接接続されていない第２の社内ＬＡＮを含み、
前記管理サーバは前記第１の社内ＬＡＮに接続され、
前記情報処理装置は前記第２の社内ＬＡＮに接続された時に、前記管理サーバに対して前記社外用仮想マシンから前記社内用仮想マシンに切り替えるための切替申請を送信する送信手段を更に具備する
請求項９に記載の情報処理システム。

【請求項１６】
前記切替申請は出張先到着申請であり、
前記管理サーバによって前記社外用仮想マシンから前記社内用仮想マシンへの切替が承認された場合に、前記変更手段は、前記起動情報を前記社内用仮想マシンから前記社外用仮想マシンを示すデータに変更し、
前記起動手段は、前記社外用仮想マシンをシャットダウンした後、前記社内用仮想マシンを起動する
請求項１５に記載の情報処理システム。
【請求項１７】
前記ネットワークは、インターネットを含み、
前記管理サーバはインターネット上に設置され、複数の仮想マシンのイメージファイルを有し、
前記情報処理装置は、前記管理サーバから前記情報処理装置を使用する加入者の契約に応じた仮想マシンのイメージファイルをダウンロードする手段を更に具備する
請求項９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、操作場所に応じて環境を変えることが出来る情報処理装置、および情報処理システムに関する。
【背景技術】
【０００２】
従来、パソコンの社外利用による情報漏洩対策として、以下のような対策がある。
【０００３】
１．シンクライアントの利用（パソコンにハードディスクを持たない）。
【０００４】
２．持ち出し専用のパソコン（暗号化ソフト、機密情報なし）の利用。
【０００５】
しかし、シンクライアントの利用には、大規模なシステムの導入が必要となる。また、サーバへアクセスできないところでは利用できない、ネットワークの負荷が高いと応答が遅くなるなどの欠点がある。持ち出し専用パソコンによって情報漏洩対策を行う場合、外出する社員数が多いと持ち出し専用のパソコンの導入コストがかかる。又、持ち出し専用パソコンにはデータを保存しない、万が一データを保存してしまった場合には返却時、借用者が消去するなどの運用ルールの徹底がなかなか難しいのが実情である。
【０００６】
特許文献１には、複数の環境設定情報を保存し、ユーザからの環境切り替え要求により保存されている設定情報に基づいて、動作環境を設定するコンピュータシステムについて記載されている。
【特許文献１】特開２０００－３１１０８０号公報（［０００７］、［０００８］、［００１２］段落）
【発明の開示】
【発明が解決しようとする課題】
【０００７】
普段使っているパソコンを持ち出したい。しかし、下記のような課題がある。
【０００８】
１．外出のために、パソコンの中のデータを削除したりやサーバへ移動するのは面倒。
【０００９】
２．不注意で機密情報を持ち出してしまうことが心配。
【００１０】
３．パソコンを持ち帰った時に、環境（データや設定）を元に戻すのが面倒（必ずしも

徹底できていない）。
【００１１】
４．パソコンを紛失した時に重要なデータを失うのが心配。
【００１２】
５．外出先でウイルスに感染して機密情報を漏洩するのが心配。
【００１３】
６．持ち出し専用パソコンを別途準備するのもコストがかかる。
【００１４】
７．社内で異なる部署へ外出する際も今は普段使っているパソコンの持ち出しを禁止されると、外出時とても不便。（このような場合、同じ会社内なので普段つかっているパソコンで仕事をしたい。）
ところで、家に帰って仕事をするために、家のパソコンに社内で利用している仮想マシンイメージをインストールして仕事をするためのソフトウェア製品がある。この製品は、ユーザ自身が仮想マシンを切り替えることが可能である。そのため、家のパソコンに機密情報やデータをコピーしてしまう恐れがある。
【００１５】
本発明の目的は、ユーザの作業場所に応じて適切な環境にすることが可能になる情報処理装置、および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】
【００１６】
本発明の一例に係わる、情報処理装置は、仮想マシンモニタ上で動作し、お互いのアクセスが制限されている社内用仮想マシンと、外部機器へのデータ出力が制限された社外用仮想マシンとのいずれか一方を選択的に動作する情報処理装置であって、前記仮想マシンモニタ上で動作し、起動情報に応じて前記社内用仮想マシンおよび前記社外用仮想マシンの一方の仮想マシンを起動する起動手段と、前記仮想マシンモニタ上で動作し、ネットワークを介して管理サーバとの通信を実行する通信手段と、前記管理サーバからの指令に応じて前記起動情報を変更する変更手段と、
を具備する。
【発明の効果】
【００１７】
ユーザの作業場所に応じて適切な環境に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】
【００１８】
本発明の実施の形態を以下に図面を参照して説明する。
【００１９】
（第１の実施形態）
図１に、本発明の第１の実施形態に係わるＨｙｂｒｉｄ　ＰＣシステムの構成を示す。図１に示すように、複数のＨｙｂｒｉｄ　ＰＣクライアント２Ａ，２Ｂと、少なくとも１台のＨｙｂｒｉｄ　ＰＣマネージャ３とが社内ＬＡＮ１に接続されている。Ｈｙｂｒｉｄ　ＰＣクライアント２Ａ，２Ｂは、企業において社員が利用するパソコンである。Ｈｙｂｒｉｄ　ＰＣマネージャは、ＩＴ機器の管理者や部門の責任者などの管理者が利用するパソコンあるいはサーバである。
【００２０】
本発明によるＨｙｂｒｉｄ　ＰＣシステムは、社員が普段使っているＨｙｂｒｉｄ　ＰＣクライアント２Ａ～２Ｂを社外に持ち出す場合も、利便性を損なうことなく安心して持ち出せる情報通信基盤を提供することを第１の目的としている。
【００２１】
本システムでは、社員がＨｙｂｒｉｄ　ＰＣクライアントを社外に持ち出すのに先だって、各社員はシステムを経由して、管理者にＨｙｂｒｉｄ　ＰＣの持ち出し申請を行う。そして、持ち出しが許可されると、前記Ｈｙｂｒｉｄ　ＰＣマネージャが、社員が持ち出

すＨｙｂｒｉｄ　ＰＣクライアントに対し、社員が利用できるＨｙｂｒｉｄ　ＰＣクライアントの環境を社外用に切り替える。また、同様に社員が外出先から帰社し、持ち帰り申請をすると、前記Ｈｙｂｒｉｄ　ＰＣマネージャが当該Ｈｙｂｒｉｄ　ＰＣクライアントの環境を社内用に切り替わることが特徴である。

【００２２】

本発明によるＨｙｂｒｉｄ　ＰＣシステムを導入した企業は、社員（ユーザ）にＨｙｂｒｉｄ　ＰＣクライアントを配布する際、下記に示す３種類の仮想マシンをインストール（作成）して配布する。

【００２３】

図２に本発明の第１の実施形態に係わるＨｙｂｒｉｄ　ＰＣクライアントの構成を示す。Ｈｙｂｒｉｄ　ＰＣクライアント２Ａ～２Ｂは、ハードウェア４と、仮想マシンモニター５と、複数の仮想マシン（ソフトウェア資源）６Ａ～６Ｃから構成される。各仮想マシン６Ａ～６Ｃは、オペレーティングシステム（ＯＳ）、アプリケーション、データを各々具備し、各仮想マシンは各々あたかも１台のパソコンのように動作する。

【００２４】

管理用仮想マシン６Ａは、管理用のサービスオペレーティングシステム（ＯＳ）７Ａと管理用アプリケーション（ＡＰＰ）８Ａと、データ領域９Ａとから構成される。管理用仮想マシン６Ａは、社内用仮想マシン６Ｂと社外用仮想マシン６Ｃの作成や削除、使用可・使用不可の制御、ディスク容量やメモリ容量、ＣＰＵ割り当てなどのパラメータ設定などを実行できる特権を持つ。そして、この管理用仮想マシン６Ａは管理者のみが利用可能であり、管理者以外の社員（ユーザ）は利用することができない点が特徴である。

【００２５】

管理用アプリケーション(ＡＰＰ）８Ａとして、ユーザＶＭ（仮想マシン）管理ＡＰＰ２０を有する。ユーザＶＭ管理ＡＰＰ２０は、Ｈｙｂｒｉｄ　ＰＣマネージャ３の命令に応じて、実行するユーザ仮想マシン（社内用仮想マシン６Ｂ、社外用仮想マシン６Ｃ）を切り替えるアプリケーションである。ユーザＶＭ管理ＡＰＰ２０は、構成情報変更部２１、実行許可部２２等を有する。

【００２６】

構成情報変更部２１は、データ領域９Ａ内の仮想マシン構成情報２３を変更する機能を有する。仮想マシン構成情報２３は、社内用仮想マシン６Ｂおよび社外用仮想マシン６Ｃの何れかを実行するのかの情報を有する。実行許可部２２は、システムの起動時等に仮想マシン構成情報２３を参照し、社内用仮想マシン６Ｂおよび社外用仮想マシン６Ｃの一方の実行を許可する。そして、サービスオペレーティングシステム７Ａは、他の仮想マシン６Ｂ，６ＣのゲストＯＳ７Ｂ，７Ｃおよび社内用ＡＰＰ８Ｂ，８Ｃから仮想マシン構成情報２３へのアクセスを制限し、のゲストＯＳ７Ｂ，７Ｃおよび社内用ＡＰＰ８Ｂ，８Ｃから仮想マシン構成情報２３を変更できないようにしている。

【００２７】

社内用仮想マシン６Ｂは、社内で利用するゲストオペレーティングシステム（ＯＳ）７Ｂと、社内用アプリケーション（ＡＰＰ）８Ｂと、機密データを含むデータ領域９Ｂとを有する。社内用ＡＰＰ８Ｂとしては、Ｗｅｂブラウザ２４およびメーラー２５等を有する。

【００２８】

社外用仮想マシン６Ｃは、社外で利用するゲストオペレーティングシステム（ＯＳ）７Ｃと社外用アプリケーション（ＡＰＰ）８Ｃと機密情報を含まないデータを含むデータ領域９Ｃとから構成されている。社外用ＡＰＰ８Ｃとしては、Ｗｅｂブラウザ２６およびメーラー２７等を有する。又、社外用仮想マシン６Ｃが実行されているとき、外部記録装置への書き込みや印刷等の操作が制限ある。

【００２９】

ハードウェア４として、Ｈｙｂｒｉｄ　ＰＣマネージャ３と通信を行うためのＮＩＣ（Network Interface Card）１１が設けられている。

【００３０】
また、各仮想マシン６Ａ～６Ｃは、１つのハードウェアを共有するが、各仮想マシンのリソース（ＯＳやアプリケーション、データ）は分離され、お互いに他の仮想マシンから隔離され、アクセスすることができない。そのため、例えば、社外用仮想マシン６Ｃをつかっていてコンピュータウイルス等に感染したとしても、社内用仮想マシン６Ｂにある機密情報や機密データにウイルスプログラムがアクセスすることができないため、ウイルス感染による情報漏洩を防止することができる。
【００３１】
次に、起動する仮想マシンを切り替える処理について説明する。社員（ユーザ）はＨｙｂｒｉｄ　ＰＣクライアント２Ｂを社外へ持ち出す場合、社内用仮想マシン６Ｂにインストールされている社外持ち出し申請用のアプリケーションを使ってパソコンの持ち出し申請を行う。社員（ユーザ）からパソコンの持ち出し申請は、当該社員の上長や管理者へメール等やグループウェアをつかって通知される。この申請が当該社員の上長や管理者から承認されると、Ｈｙｂｒｉｄ　ＰＣマネージャは、該当するＨｙｂｒｉｄ　ＰＣクライアントの管理アプリケーションを動作させて、社員（ユーザ）が利用できる仮想マシンを社内用仮想マシンＢｂから社外用仮想マシン６Ｃに切り替える。
【００３２】
次に、Ｈｙｂｒｉｄ　ＰＣクライアントのパワーオン時の動作について図３を参照して説明する。ユーザがパワーオンすると、先ず、管理用仮想マシン６Ａが実行される（ステップＳ１）。管理用仮想マシン６Ａの実行に伴って、サービスＯＳ７Ａが起動する。そして、サービスＯＳ７Ａ上でユーザＶＭ管理ＡＰＰ２０が起動する（ステップＳ２）ユーザＶＭ管理ＡＰＰ２０の実行許可部２２は、仮想マシン構成情報２３を読み込む（ステップＳ３）。実行許可部２２は、仮想マシン構成情報２３から実行を許可する仮想マシンが社内用仮想マシン６Ｂであるか否かを判別する（ステップＳ４）。社内用仮想マシン６Ｂを実行すると判断した場合（ステップＳ４のＹｅｓ）、実行許可部２２は社内用仮想マシン６Ｂの実行を許可し、社内用仮想マシン６Ｂを実行させる。また、社内用仮想マシン６Ｂを実行しないと判断した場合（ステップＳ４のＮｏ）、実行許可部２２は社外用仮想マシン６Ｃの実行を許可し、社外用仮想マシン６Ｃを実行させる。
【００３３】
以上で、仮想マシン構成情報２３の情報に応じて、選択的にユーザ仮想マシンを実行することが出来る。
【００３４】
次に、仮想マシンを切り替えるための構成について図４を参照して説明する。なお、図４の構成は、社内用仮想マシン６Ｂから社外用仮想マシン６Ｃに切り替える場合を示している。
【００３５】
図４に示すように、Ｈｙｂｒｉｄ　ＰＣマネージャ３は、Ｗｅｂサーバ３Ａ、およびメールサーバ３Ｂ等を有する。Ｗｅｂサーバ３Ａは、ユーザ認証処理部３１、申請頁作成部３２、承認頁作成部３３、管理者宛メール作成部３４、送信部３５、管理者認証処理部３６、承認頁送信部３７、承認確認頁作成部３８、ユーザ宛メール作成部３９、切替指令部４０等を有する。
【００３６】
ユーザ認証処理部３１は、ブラウザ２４から持ち出し申請用のＷｅｂ頁にリクエストがあった場合に、ユーザＩＤおよびパスワードの入力欄を有する認証頁をブラウザ２４に送信する。ユーザ認証処理部３１は、社内用仮想マシン６Ｂから送信されるユーザＩＤおよびパスワードから、社内用仮想マシン６Ｂを操作している者が正当なユーザであるか判別するための認証処理を行う。
【００３７】
申請頁作成部３２は、ユーザ認証処理部３１が正当なユーザであると判断した場合に、ユーザが管理者に切替を申請するためのＷｅｂ頁を作成し、ブラウザ２４にＷｅｂ頁のデ

ータを送る。

【００３８】

承認頁作成部３３は、ユーザがＷｅｂ頁に必要な事項を記入して送信した場合に、記入されたデータに応じた承認Ｗｅｂ頁を作成し、アップロードする。管理者宛メール作成部３４は、ユーザが申請頁に記入した事項、並びに承認Ｗｅｂ頁のＵＲＬとが記載された管理者宛のメールを作成し、送信部３５に出力する。送信部３５は、管理者宛メール作成部３４およびユーザ宛メール作成部３９によって作成されたメールをメールサーバ３Ｂに送信する。

【００３９】

管理者認証処理部３６は、管理者宛のメールに記載されたＵＲＬへのリクエストがあった場合に、ユーザＩＤおよびパスワードの入力欄を有する認証頁をブラウザ５２に送信する。管理者認証処理部３６は、管理者用ＰＣ５０から送信されるユーザＩＤおよびパスワードから、管理者用ＰＣ５０を操作している者が正当なユーザであるか判別するための認証処理を行う。

【００４０】

承認頁送信部３７は、管理者認証処理部３６が正当な管理者であると判断した場合に、承認頁作成部３３によって作成された承認Ｗｅｂ頁のデータをブラウザ５２に送信する。

【００４１】

承認確認頁作成部３８は、管理者が承認Ｗｅｂ頁によって持ち出しの申請を承認した場合に、ユーザが承認されたことを確認するための承認確認Ｗｅｂ頁を作成し、データをアップロードする。

【００４２】

ユーザ宛メール作成部３９は、承認確認Ｗｅｂ頁のＵＲＬが記載されたユーザ宛のメールを作成し、送信部３５に出力する。

【００４３】

次に、図５，図６，図７のフローチャートを参照して、ユーザ仮想マシンを切り替える処理のシーケンスを説明する。同図は、社員（ユーザ）、社員が使っているパソコンの社に用仮想マシン６Ｂ上のアプリケーション、管理用仮想マシン６Ａ、持ち出し申請処理用のＷｅｂサーバ、メールサーバ、管理者のパソコン、管理者との間でのやり取りを示している。なお、前述したＨｙｂｒｉｄ　ＰＣマネージャは、同図に示す持ち出し申請用のＷｅｂサーバとメールサーバとから構成されるサブシステムとしてよい。

【００４４】

社員（ユーザ）は、パソコンの持ち出し申請をする時、社内用仮想マシン６Ｂ上にインストールされているＷｅｂブラウザ２４を起動し（ステップＳ１１）、持ち出し申請のＷｅｂサーバのＵＲＬ（uniform resource locator）を入力する（ステップＳ１２）。社内用仮想マシン６ＢはＷｅｂブラウザ２４からＷｅｂサーバ３Ａへ持ち出し申請Ｗｅｂページのリクエストを送信する（ステップＳ１３）。

【００４５】

Ｗｅｂサーバ３Ａのユーザ認証処理部３１は、持ち出し申請Ｗｅｂページのデータを Ｗｅｂブラウザ２４にレスポンスする(ステップＳ１４）。Ｗｅｂブラウザ２４によって表示される持ち出し申請ログインＷｅｂページの一例を図８に示す。図８に示すように、持ち出し申請ログインＷｅｂページには、社員のユーザＩＤの入力欄６１とパスワードの入力欄６２がある。社員（ユーザ）は、入力欄６１，６２にそれぞれ自分のユーザＩＤとパスワードを入力する(ステップＳ１５）。ユーザが、ログインボタン６３を押すと、Ｗｅｂブラウザ２４は入力欄６１，６２に入力されているユーザＩＤとパスワードをＷｅｂサーバ３Ａに送信する(ステップＳ１６)。その後、Ｗｅｂサーバ３Ａの認証処理部３１は、受信したユーザＩＤとパスワードをつかって社員（ユーザ）を認証する(ステップＳ１７)。

【００４６】

認証が成功すると、申請頁作成部３２は、ＰＣ持ち出し申請頁をＷｅｂブラウザ２４に

送信する（ステップＳ１８）。Ｗｅｂブラウザ２４によって表示されるＰＣ持ち出し申請Ｗｅｂ頁の一例を図９に示す。図９に示すように、ＰＣ持ち出し申請頁には、持ち出し申請に必要なＰＣ持ち出し情報を入力ための入力欄７１，７２，７３がある。社員はパソコンの機器管理番号や持ち出し期間、持ち出し先などを入力欄７１，７２，７３に入力する（ステップＳ１９）。ユーザが、送信ボタン７４を押すと、Ｗｅｂブラウザ２４は入力欄７１，７２，７３に入力されているＰＣ持ち出し情報をＷｅｂサーバ３Ａに送信する(ステップＳ２０)。承認頁作成部３３は、管理者がＷｅｂブラウザ５２を使用して申請を承認または否認するための承認Ｗｅｂ頁を作成し、アップロードする。承認Ｗｅｂ頁には、社員（ユーザ）からのＰＣ持ち出し情報を含む。管理者宛メール作成部３４は、社員（ユーザ）からのＰＣ持ち出し情報を含む情報、並びに承認Ｗｅｂ頁のＵＲＬとが記載された管理者宛のメールを作成し、送信部３５に送信する。送信部３５は、管理者宛メール作成部３４およびユーザ宛メール作成部３９によって作成されたメールをメールサーバ３Ｂに送信し、メールはメールサーバ３Ｂに蓄積される。（ステップＳ２１）。

【００４７】

管理者の操作（ステップＳ２２）等により、管理者用ＰＣ５０のメーラー５１がメールサーバ３Ｂにメール受信リクエストを発行すると、ＰＣ持ち出し受信メールがメールサーバ３Ｂから管理者ＰＣに送られ、メーラー５１は電子メールを受信する（ステップＳ２４）。メーラー５１が受信するメールの一例を図１０に示す。

【００４８】

管理者が、電子メールの本文に記載されているＵＲＬにアクセスすると（ステップＳ２５）、ＵＲＬがＷｅｂブラウザ５２に渡され、Ｗｅｂブラウザ５２はＷｅｂサーバ３ＡにＰＣ持ち出し承認Ｗｅｂ頁のリクエストを発行する（ステップＳ２６）。

【００４９】

Ｗｅｂサーバ３Ａは、管理者ＰＣ５０のブラウザ５２にＰＣ持ち出し承認Ｗｅｂ頁をＷｅｂブラウザ５２にレスポンスする(ステップＳ２７）。

【００５０】

Ｗｅｂブラウザ２４によって表示される持ち出し承認ログインＷｅｂページの一例を図１１に示す。図１０に示すように、持ち出し承認ログインＷｅｂページには、社員のユーザＩＤの入力欄８１とパスワードの入力欄８２がある。管理者は、入力欄８１，８２にそれぞれ自分のユーザＩＤとパスワードを入力する(ステップＳ２８）。管理者が、ログインボタン８３を押すと、Ｗｅｂブラウザ５２は入力欄８１，８２に入力されているユーザＩＤとパスワードをＷｅｂサーバ３Ａに送信する(ステップＳ２９)。その後、Ｗｅｂサーバ３Ａの認証処理部３１は、受信したユーザＩＤとパスワードをつかって管理者を認証する(ステップＳ３０)。

【００５１】

認証に成功すると、Ｗｅｂサーバ３Ａは、承認頁作成部３３によって作成されたＰＣ持ち出し承認Ｗｅｂページを持ち出し申請承認Ｗｅｂページのデータを管理者のパソコンに送信する（ステップＳ３１）。

【００５２】

Ｗｅｂブラウザ２４によって表示される持ち出し承認Ｗｅｂページの一例を図１２に示す。図１２に示すように、持ち出し承認ページには、申請者の社員名やパソコンの機器管理番号が記載されている。また、持ち出し承認ページには、申請を承認するための承認ボタン９１と、申請を否認するための否認ボタン９２とが設けられている。

【００５３】

管理者は当該持ち出し申請承認ページをチェックして、本ページの社員名やパソコンの機器管理番号を目視で確認し、当該Ｗｅｂページの承認ボタン９１および否認ボタン９２の一方のボタンを選択する（ステップＳ３２）。Ｗｅｂブラウザ５２は、管理者の選択結果を、Ｗｅｂサーバ３Ａに送信される（ステップＳ３３）。管理者の承認が得られると、承認確認頁作成部３８は、ユーザが管理者の承認を確認するためのＷｅｂ頁を作成し、データをアップロードする。そして、ユーザ宛メール作成部３９は、承認確認Ｗｅｂ頁のＵ

ＲＬが記載されたユーザ宛のメールを作成し、送信部３５に出力する。送信部３５は、社員（ユーザ）宛ての電子メール（持ち出し承認メール）を送信する（ステップＳ３４）。

【００５４】

ユーザの操作（ステップＳ３５）等により、社内用仮想マシン６Ｂのメーラー２５がメールサーバ３Ｂにメール受信リクエストを発行すると、ＰＣ持ち出し承認確認メールがメールサーバ３Ｂから社内用仮想マシン６Ｂに送られ、メーラー２５で電子メールを受信する（ステップＳ３７）。メーラー２５が受信するメールの一例を図１３に示す。

【００５５】

管理者が、電子メールの本文に記載されているＵＲＬをアクセスすると（ステップＳ３８）、ＵＲＬがＷｅｂブラウザ２４に渡され、Ｗｅｂブラウザ２４はＷｅｂサーバ３ＡにＰＣ持ち出し承認確認ログインＷｅｂ頁のリクエストを発行する（ステップＳ３９）。

【００５６】

Ｗｅｂサーバ３Ａは、管理者ＰＣ５０のブラウザ５２に承認確認ログインＷｅｂ頁をレスポンスする(ステップＳ４０）。承認確認ログインＷｅｂ頁は、図８と同様なので図示を省略する。

【００５７】

社員（ユーザ）は、入力欄６１，６２にそれぞれ自分のユーザＩＤとパスワードを入力する(ステップＳ４１）。ユーザが、ログインボタンを押すと、Ｗｅｂブラウザ２４は入力欄に入力されているユーザＩＤとパスワードをＷｅｂサーバ３Ａに送信する(ステップＳ４２)。その後、Ｗｅｂサーバ３Ａの認証処理部３１は、受信したユーザＩＤとパスワードをつかって社員（ユーザ）を認証する(ステップＳ４３)。

【００５８】

認証が成功すると、Ｗｅｂサーバ３Ａは、管理者ＰＣ５０のブラウザ５２に承認確認ログインＷｅｂ頁を送信する(ステップＳ４４）。Ｗｅｂブラウザ２４によって表示される持ち出し承認確認Ｗｅｂページの一例を図１４に示す。図１４に示すように、持ち出し承認確認ページには、申請者の社員名やパソコンの機器管理番号が記載されている。また、持ち出し処理をＷｅｂサーバ３Ａに指示するための持ち出し処理開始ボタン１０１が設けられている。ユーザが持ち出し処理開始ボタン１０１を押す（ステップＳ４５）と、持ち出し処理の開始メッセージが切替指令部４０に通知される（ステップＳ４６）。切替指令部４０は、管理者に対してユーザが、管理者の持ち出し承認を確認したことをメールで通知する（ステップＳ４７）。

【００５９】

切替指令部４０は、社員の管理用仮想マシン６Ａの構成情報変更部２１に対し、仮想マシンの切替メッセージ送信する（ステップＳ４８）。本メッセージの送信は、ＳＯＡＰ（simple object access protocol）などのプロトコルによるメッセージを、ｈｔｔｐｓ（hypertext transfer protocol over transport layer security）プロトコルを使って暗号化して送信する。

【００６０】

本メッセージを受信すると構成情報変更部２１は、メッセージが確かにＨｙｂｒｉｄＰＣマネージャ３から送信された者であるかの認証処理を行う（ステップＳ４９）。認証処理が成功すると、構成情報変更部２１は、本管理用仮想マシン６Ａ内に保存される仮想マシン構成情報２３を変更する（ステップＳ５０）。管理用仮想マシン６Ａは、切替処理が終了したことをＷｅｂサーバ３Ａおよび実行許可部２２に通知する（ステップＳ５１）。その後、実行許可部２２は、社内用仮想マシン６Ｂで実行されているアプリケーションおよびＯＳをシャットダウンするように管理用仮想マシン６Ａに指令する。管理用仮想マシン６Ａがシャットダウンしたら、実行許可部２２は、管理用仮想マシン６Ａも一端シャットダウンさせる（ステップＳ５２）。

【００６１】

その後、社員のパソコンを立ち上げると、まず管理用仮想マシン６Ａが立ち上がり、次に社外用仮想マシン６Ｃが実行される。

【００６２】
以上のようにして、社員のパソコンの持ち出し申請、並びに切替処理が行われる。なお、Ｈｙｂｒｉｄ　ＰＣマネージャ３は、ＰＣ持ち出し承認メールを送信した後、ユーザの確認を得ずに、仮想マシンの切替メッセージ送信する処理（ステップＳ４８）を行っても良い。
【００６３】
一方、社員（ユーザ）は、外出先から戻ると、仮想マシン６Ｃにインストールされているパソコンの持ち帰り申請アプリケーションをつかって持ち帰り申請を行う。社員（ユーザ）からの持ち帰り申請は、当該社員の上長や管理者へ通知されるとともにログに記録される。そして、Ｈｙｂｒｉｄ　ＰＣマネージャは、該当するＨｙｂｒｉｄ　ＰＣクライアントの管理アプリケーションを動作させて、社員（ユーザ）が利用できる仮想マシンを社外用仮想マシン６Ｃから社内用仮想マシン６Ｂに切り替える。また、この時、外出時に利用した社外用仮想マシンを一旦削除して、次の外出に備えたり、不要な情報を持ち込まないようにしてもよい。
【００６４】
データの削除やバックアップなどの作業負担を低減することができる。
【００６５】
従来、普段使っているパソコンを社外に持ち出す場合も、社員（ユーザ）は外出の前にその都度パソコンの中のデータを削除したりやサーバへバックアップするなどの作業をする必要があった。本発明によれば、社外用の仮想マシン６Ｃには機密情報や機密データ等は入っていないので、データの削除やバックアップなどの作業負担を低減できる。
【００６６】
本システムによれば、外出前のデータの不正コピーを防止することができる。従来、普段使っているパソコンを社外に持ち出す場合、パソコンに外出前に機密情報や機密データを不正にコピーすることを防止するのは困難であった。本発明によれば、社内で利用している時に社員（ユーザ）は外出用の仮想マシン６Ｃにアクセスできないため、社外用仮想マシン６Ｃに、外出前にデータを不正にコピーすることができない。
【００６７】
不注意による機密情報の漏洩を防止することができる。普段使っているパソコンを社外に持ち出す場合も、従来、うっかり機密情報や機密データを持ち出したり、消去を忘れて、その後、情報漏洩の事故を起こしてしまうという心配があったが、社外用仮想マシン６Ｃには、機密情報や機密データが入っていないため、このような事故を防止できる。
【００６８】
ウイルス感染やファイル交換ソフトなどによる情報漏洩を防止することができる。前述したように仮想マシン間は隔離されているため、外出時に社員が仮想マシン６Ｃで作業をしていてウイルスに感染しても、ウイルスは仮想マシンのデータやＯＳ、アプリケーションにアクセスできないため、ウイルス感染やファイル交換ソフトなどによる情報漏洩を防止できる。
【００６９】
仮想マシンの切替は管理者（システム）を通じて実施するのでユーザの不正を防止することができる。従来の仮想化ソフトをインストールしたＰＣでは、社員（ユーザ）が自由に環境を切り替えが可能であるのに対し、本発明のＨｙｂｒｉｄ　ＰＣシステムは、社員（ユーザ）は自由に環境（仮想マシン）を切り替えることができない。これによって、社員（ユーザ）の不正を防止することが可能となる。
【００７０】
社員が自社の拠点等へ外出時の利便性を向上させることが出来る。従来の持ち出し専用パソコン（機密データなし）を導入した情報漏洩対策を実施して普段使っているパソコンの社外利用を禁じた場合、社員が外出先で過去のメールを見たり、自分が作成した文章をみることができないため、外出時の業務に支障がでるという問題があった。また、シンクライアントシステムを導入した場合、外出先から常にシンクライアントのサーバへアクセ

スが必要となるため、ネットワークのトラヒックによってレスポンスが遅くなるなどの問題があった。これに対し、本発明のＨｙｂｒｉｄ　ＰＣシステムによれば、同一企業内での他部門への出張時、Ｈｙｂｒｉｄ　ＰＣを外出先の社内ＬＡＮに接続して申請すれば、普段自席で使っている仮想マシン６Ｂの環境に切り替えられるので、過去のメールや自分が作成した文章を直接Ｈｙｂｒｉｄ　ＰＣにて参照できるので、外出時の業務効率を高めることができる。

【００７１】

管理者（システム）が承認すると、仮想マシン内の一部のファイルをＥｘｐｏｒｔして社外用仮想マシンにて参照することができる。このＥｘｐｏｒｔオプションを使えば、外出先で急に必要になったデータも参照できるので安心。持ち出し用ＵＳＢメモリも不要となる。

【００７２】

許可されて持ち出したデータのユーザ操作（閲覧・保存・編集、コピー、印刷、メール添付等）をきめ細かく制限したり、操作ログを管理システムへ保存することも可能である。

【００７３】

（第２の実施形態）

図１５（Ａ）、図１５（Ｂ）、および図１６（Ｃ）に示すように、社内ＬＡＮ１Ａ，１Ｂが専用線１１０で接続された複数の拠点（事業所）をもった企業の社員が社内の別の事業所へ出張するような場合、出張先にて社内ＬＡＮで出張先到着申請を行うと、イントラネットを経由して前記Ｈｙｂｒｉｄ　ＰＣマネージャに申請できるようにしてもよい。

【００７４】

図１５（Ａ）に示すように、Ｈｙｂｒｉｄ　ＰＣクライアント２Ｂが拠点Ａの社内ＬＡＮ１Ａに接続している場合、社内用仮想マシン６Ｂが実行される。図１５（Ｂ）に示すように、ＰＣクライアント２Ｂを拠点Ａの外に持ち出す場合、社外用仮想マシン６Ｃが実行される。そして、図１６（Ｃ）に示すように、社内用仮想マシン６Ｂが拠点Ｂに持ち込まれた場合、Ｈｙｂｒｉｄ　ＰＣクライアント２Ｂは、Ｈｙｂｒｉｄ　ＰＣマネージャ３に出張先到着申請を出して、許可を受けることによって、社内用仮想マシン６Ｂが実行できるようにする。また、社員が出張先から出るときは、前述した持ち出し申請と同様に、社内用仮想マシン６Ｂから社外用仮想マシン６Ｃへ切り替えるようにすることもできる。

【００７５】

このようにすれば、自宅のパソコンに機密情報やデータをコピーして、それが後に情報漏洩事故につながることを防止することができる。また、同一企業内での他部門への出張時でも出張先に到着後、普段自席で使っている社内用仮想マシン６Ｂの環境に切り替えられるので、過去のメールや自分が作成した文章を直接にて参照できるので、業務効率を高めることができる。

【００７６】

また、図１７（Ａ）に示すように、社員（ユーザ）はＨｙｂｒｉｄ　ＰＣの持ち出し申請とともに、仮想マシンのバックアップ（移動、差し替えも含む）も指示できる。この場合、上述した仮想マシンの切替と連動して、社内ＬＡＮにあるファイルサーバ１２０へ社員（ユーザ）の社内用仮想マシン６Ｂのイメージファイル（ＯＳ、アプリケーション、データ）を丸ごとバックアップすることができる。

【００７７】

このように、図１７（Ｂ）に示すように、持ち出し時に社内用仮想マシン６Ｂをファイルサーバ１２０に移動しておけば、外出時に途中でＨｙｂｒｉｄ　ＰＣクライアント２Ｂを紛失したり、盗難されたりしたりしても、機密データは無いので安心である。また、普段、社内で利用しているときも定期的に社内用仮想マシン６Ｂのイメージファイルをファイルサーバへバックアップしておき、外出時のバックアップは今までとの差分だけ更新するようにもできる。

【００７８】

（第３の実施形態）
客先への商品説明やプレゼンテーション、あるいは学会などでの発表など、普段つかっているパソコンの中に保存されている一部のファイルを社外に持ち出す必要がある場合がある。このような場合、従来、暗号機能やコピー禁止などの操作制限をするためのプログラムが入ったＵＳＢメモリ等に、必要なファイルをコピーして持ち出している。
【００７９】
本Ｈｙｂｒｉｄ　ＰＣシステムでは、上述したＵＳＢメモリを不要にすることが可能である。また、本Ｈｙｂｒｉｄ　ＰＣシステムでは、社員が持ち出しファイルの不正操作をできないようにするため、持ち出したファイルに対する操作を監視するプログラムを、社員がアクセスできない管理仮想マシン上で実行することが特徴である。
【００８０】
以下、その仕組みについて図１８を参照して説明する。図１８は、仮想マシン間でのファイル共有をつかったデータの持ち出し制御について説明する図である。
【００８１】
ユーザが持ち出すファイルを申請し、管理者から許可されると、社内用仮想マシン６Ｂのデータ領域９Ｂにあるファイル１３１が、一旦管理用仮想マシンのデータ領域９Ａ内の共有データ領域１３０に転送（コピー）される。社員が外出先で社外用仮想マシン６Ｃを使用している状態で、持ち出したファイル１３１を参照したい場合、Ｗｉｎｄｏｗｓ（登録商標）のファイル共有機能などを使って管理用仮想マシンの共有データ領域１３０にあるファイル１３１を参照する。このようにすれば、外出時にウイルス等に感染による事故でのファイルの流出を防止できる。
【００８２】
また、管理用仮想マシン６Ａ上の管理プログラム１３２によって、社員が外出時に持ち出したファイル１３１に何時アクセスしたかログをとる。さらに、管理プログラム１３２の社員（ユーザ）のファイル１３１の操作もモニターしたり、ファイル１３１のコピーや保存や印刷などの操作をきめ細かく制限することもできる。このように管理用仮想マシン６Ａ上の管理プログラム１３２にて、持ち出したファイル１３１に対する操作の監視を行えば、社員（ユーザ）が管理プログラム１３２を勝手に削除できないため、不正を防ぐことができる。
【００８３】
なお、サービスＯＳ７Ａは、社外用仮想マシン６Ｃが共有データ領域１３０以外のデータ領域９Ａに格納されている仮想マシン構成情報等のデータにアクセスすることを禁止する。
【００８４】
（第４の実施形態）
以下に、社内用仮想マシン６Ｂと社外用仮想マシン６Ｃとの切り替えが行われていないコンピュータが社外に持ち出されることを防止する方法について説明する。
【００８５】
図１９は、本発明の第４の実施形態に係わるＨｙｂｒｉｄ　ＰＣクライアントを外に持ち出すときの検査を説明するための図である。
【００８６】
図１９に示すように、入退出門に社内ＬＡＮ１に接続する検査装置１４０を設ける。また、Ｈｙｂｒｉｄ　ＰＣマネージャ３内には、持ち出し申請記録データベース（ＤＢ）１４１を設ける。持ち出し申請記録データベース（ＤＢ）１４１には、持ち出し申請がなされ、仮想マシンの切替処理が行われたＨｙｂｒｉｄ　ＰＣクライアントの資産番号やシリアル番号が管理されている。資産番号やシリアル番号はバーコード化しコンピュータ本体に添付されている。
【００８７】
検査装置１４０は、バーコードリーダによって社外に持ち出されようとしているＨｙｂｒｉｄ　ＰＣクライアント２Ｂに添付されているバーコードを読み取ることによって、資

産番号やシリアル番号を識別する。

【００８８】

そして、読み出した資産番号やシリアル番号が持ち出し申請記録データベース１４１と照合して、仮想マシンの切替処理が行われているか否かをチェックする。

【００８９】

なお、入退出門において警備員等が検査装置を用いてチェックする方法以外にも、出張先で、持ち出したＰＣを社内ネットワークに接続したときに、従来のネットワーク認証技術を用いてチェックすることもできる。

【００９０】

（変形例）

これまで、本発明によるＨｙｂｒｉｄ　ＰＣシステムを企業内に導入し、企業内で運用する例を示してきたが、図２０に示すように、中小企業向けに、Ｈｙｂｒｉｄ　ＰＣマネージャ３やファイルサーバ１２０をインターネット１５０上に置き、ＡＳＰサービスとして提供してもよい。このようなＡＳＰ（application service provider）サービスとするとサーバなどの設備を導入しないで直ぐに利用できる。

【００９１】

また、中小企業などサーバ導入が直ぐにできないような企業でも、Ｈｙｂｒｉｄ　ＰＣサービスを導入すれば、直ぐに上述したようなパソコンの社外持ち出しによる情報漏洩対策を行うことができる。

【００９２】

また、図２１に示すように、各種用途に合わせて種々の仮想マシンイメージファイル（ＯＳ、アプリケーション、データ）１６１，１６２，１６３をファイルサーバ１２０上に置き、加入者の要望や契約にあわせて、仮想マシンイメージを選び、Ｈｙｂｒｉｄ　ＰＣクライアント２にダウンロードするようにしてもよい。

【００９３】

例えば、インターネットカフェに管理用仮想マシン１６０Ａおよび仮想マシン１６０Ｂを有するＨｙｂｒｉｄ　ＰＣクライアント２を設置する。

【００９４】

Ｈｙｂｒｉｄ　ＰＣクライアント２を立ち上げると、仮想マシン１６０Ｂが実行される。ユーザは仮想マシン１６０Ｂを操作して、Ｈｙｂｒｉｄ　ＰＣマネージャ３にダウンロードする仮想マシンイメージファイル１６１，１６２，１６３を通知する。そして、Ｈｙｂｒｉｄ　ＰＣマネージャ３は、管理用仮想マシン１６０Ａの管理用ＯＳ上で動作する管理用アプリケーションと通信を行い、仮想マシンイメージファイルの受信および仮想マシンの切替を指示する。そして、仮想マシンイメージファイルの受信後、管理用仮想マシン１６０Ａの管理用アプリケーションは、仮想マシン１６０Ｂを終了させて、受信した仮想マシンイメージファイルを仮想マシン１６０Ｃとして実行する。

【００９５】

以上のようにユーザの希望に応じて、ファイルサーバ１２０から受信した仮想マシンに切り替えることができる。また、ユーザの利用が終えるとＨｙｂｒｉｄ　ＰＣクライアントの仮想マシンイメージを削除したりしてもよい。

【００９６】

例えば、仮想マシン１６０Ｃ内のアプリケーションを用いてユーザが、仮想マシン１６０Ｃの終了をＨｙｂｒｉｄ　ＰＣマネージャ３に通知する。Ｈｙｂｒｉｄ　ＰＣマネージャ３は、管理用仮想マシン１６０Ａの管理用アプリケーションに仮想マシン１６０Ｃの終了後、仮想マシン１６０Ｃの管理用アプリケーションにイメージファイルを削除することを通知する。そして、管理用仮想マシン１６０Ａの管理用アプリケーションは、仮想マシン１６０Ｃの終了後に仮想マシン１６０Ｃのイメージファイルを削除する。なお、管理用仮想マシン１６０Ａの管理用アプリケーションは、削除する前に仮想マシン１６０Ｃのイメージファイルをファイルサーバ１２０に送信するようにしても良い。

【００９７】

また、特定業種向けのアプリケーションが入った仮想マシンイメージを用意し、ユーザに月々の契約に基づいて提供してもよい。

【００９８】

また、本発明によるＨｙｂｒｉｄ　ＰＣクライアントをインターネットカフェなどに利用すれば、利用者の希望に応じて利用できるアプリケーションを選ぶことが可能できる。また、利用者が変わったときにも前の利用者の履歴やデータを一括して消去することが可能である。

【００９９】

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】

【０１００】

【図１】第１の実施形態に係わる情報処理システムとしてのＨｙｂｒｉｄ　ＰＣシステムの構成を示すブロック図。

【図２】第１の実施形態に係わる情報処理装置としてのＨｙｂｒｉｄ　ＰＣクライアントの構成を示す図。

【図３】第１の実施形態に係わるＨｙｂｒｉｄ　ＰＣクライアントのパワーオン時の動作を示すフローチャート。

【図４】第１の実施形態に係わる仮想マシンを切り替えるための構成を示す図。

【図５】第１の実施形態に係わるユーザ仮想マシンを切り替える処理のシーケンスを示すフローチャート。

【図６】第１の実施形態に係わるユーザ仮想マシンを切り替える処理のシーケンスを示すフローチャート。

【図７】第１の実施形態に係わるユーザ仮想マシンを切り替える処理のシーケンスを示すフローチャート。

【図８】第１の実施形態に係わる持ち出し申請Ｗｅｂページの一例を示す図。

【図９】第１の実施形態に係わるＰＣ持ち出し申請Ｗｅｂ頁の一例を示す図。

【図１０】第１の実施形態に係わるメールの一例を示す図。

【図１１】第１の実施形態に係わる承認ログインＷｅｂページの一例を示す図。

【図１２】第１の実施形態に係わる持ち出し承認Ｗｅｂページの一例を示す図。

【図１３】第１の実施形態に係わるメールの一例を示す図。

【図１４】第１の実施形態に係わる持ち出し承認確認Ｗｅｂページの一例を示す図。

【図１５】第２の実施形態に係わるＨｙｂｒｉｄ　ＰＣシステムの運用例を示す図。

【図１６】第２の実施形態に係わるＨｙｂｒｉｄ　ＰＣシステムの運用例を示す図。

【図１７】第２の実施形態に係わるＨｙｂｒｉｄ　ＰＣクライアントの仮想マシンのバックアップを説明するための図。

【図１８】第３の実施形態に係わるＨｙｂｒｉｄ　ＰＣクライアントのファイル共有を説明するための図。

【図１９】第４の実施形態に係わるＨｙｂｒｉｄ　ＰＣクライアントを外に持ち出すときの検査を説明するための図。

【図２０】Ｈｙｂｒｉｄ　ＰＣクライアントとＨｙｂｒｉｄ　ＰＣマネージャとをインターネットを介して接続した様子を示す図。

【図２１】Ｈｙｂｒｉｄ　ＰＣシステムの運用例を示す図。

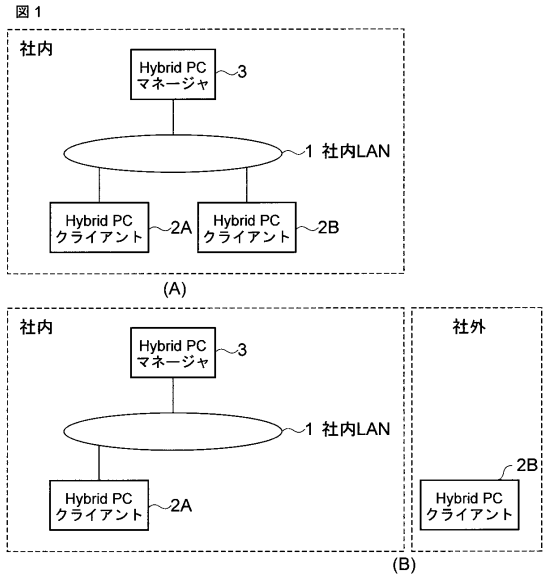
【符号の説明】

【０１０１】

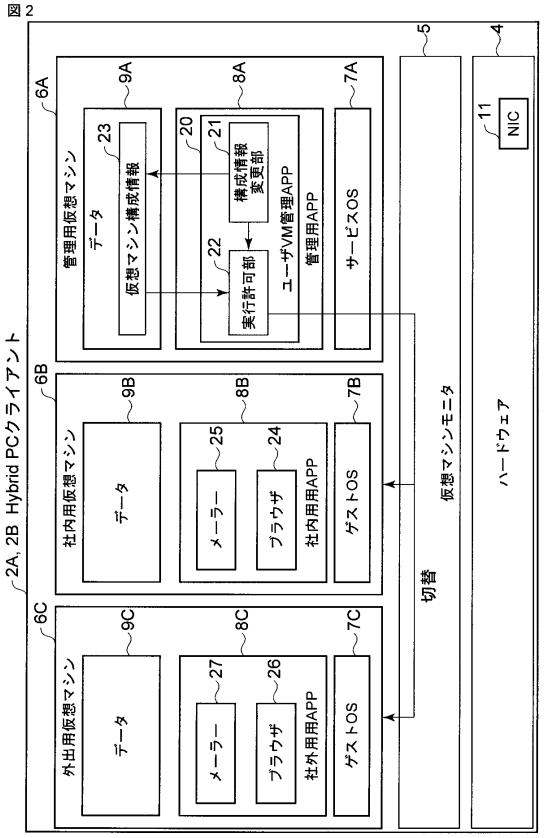
１…社内ＬＡＮ，２Ａ，２Ｂ…Ｈｙｂｒｉｄ　ＰＣクライアント，３…Ｈｙｂｒｉｄ　ＰＣマネージャ，３Ａ…Ｗｅｂサーバ，３Ｂ…メールサーバ，４…ハードウェア，５…仮

想マシンモニター，６Ａ～６Ｃ…仮想マシン，６Ａ…管理用仮想マシン，６Ｂ…社内用仮想マシン，６Ｃ…社外用仮想マシン，７Ａ…サービスオペレーティングシステム，７Ｂ…ゲストオペレーティングシステム，７Ｃ…ゲストオペレーティングシステム，８Ａ…管理用アプリケーション，８Ｂ…社内用アプリケーション，８Ｃ…社外用アプリケーション，９Ｂ…データ領域，９Ａ…データ領域，２１…構成情報変更部，２２…実行許可部，２３…仮想マシン構成情報，２４…ブラウザ，２５…メーラー，２６…ブラウザ，２７…メーラー，３１…ユーザ認証処理部，３２…申請頁作成部，３３…承認頁作成部，３４…管理者宛メール作成部，３５…送信部，３６…管理者認証処理部，３７…承認頁送信部，３８…承認確認頁作成部，３９…ユーザ宛メール作成部，４０…切替指令部，５０…管理者用ＰＣ。

【図１】



【図２】



【図３】

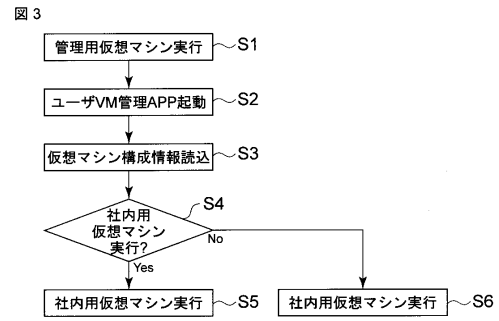


図3
管理用仮想マシン実行
S1
ユーザVM管理APP起動
S2
仮想マシン構成情報読込
S3
社内用仮想マシン実行?
S4
No
Yes
社内用仮想マシン実行
S5
社内用仮想マシン実行
S6

【図４】

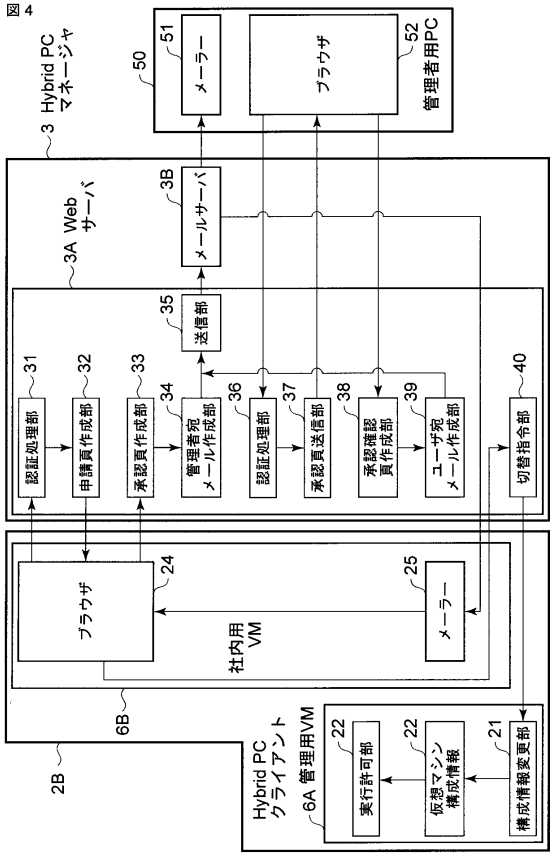


図4
Hybrid PC マネージャ
3
50
51
メーラー
52
管理者用PC
ブラウザ
3A Web サーバ
3B
メールサーバ
35
送信部
31
認証処理部
32
申請票作成部
33
承認票作成部
34
管理者宛メール作成部
36
認証処理部
37
承認票送信部
38
承認確認票作成部
39
ユーザ宛メール作成部
40
切替指令部
24
ブラウザ
25
メーラー
社内用VM
6B
2B
Hybrid PC クライアント
6A 管理用VM
22
実行許可部
22
仮想マシン構成情報
21
構成情報変更部

【図５】

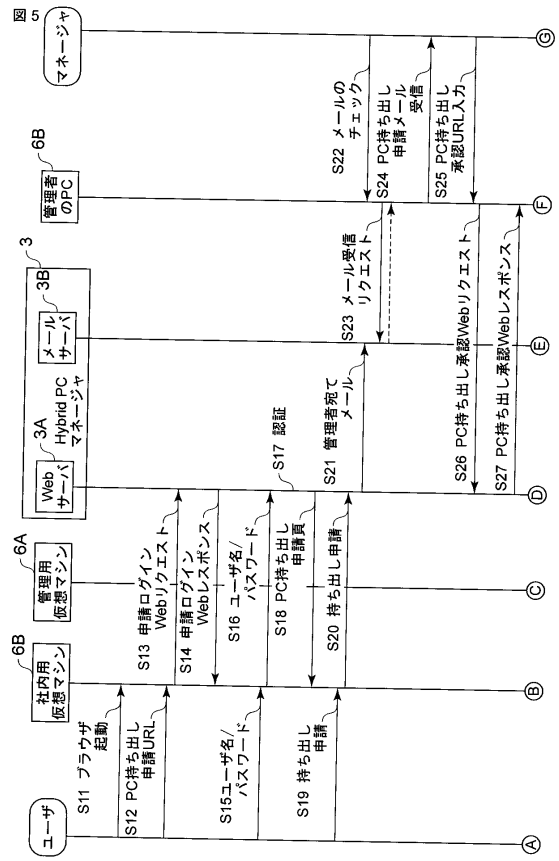


図5
マネージャ
6B
管理者のPC
3
3B
メールサーバ
3A Hybrid PC マネージャ
Web サーバ
6A
管理用仮想マシン
6B
社内用仮想マシン
ユーザ
S11 ブラウザ起動
S12 PC持ち出し申請URL
S13 申請ログイン Webリクエスト
S14 申請ログイン Webレスポンス
S15ユーザ名/パスワード
S16 ユーザ名/パスワード
S17 認証
S18 PC持ち出し申請票
S19 持ち出し申請
S20 持ち出し申請
S21 管理者宛てメール
S22 メールのチェック
S23 メール受信リクエスト
S24 PC持ち出し申請メール受信
S25 PC持ち出し承認URL入力
S26 PC持ち出し承認Webリクエスト
S27 PC持ち出し承認Webレスポンス
A
B
C
D
E
F
G

【図６】

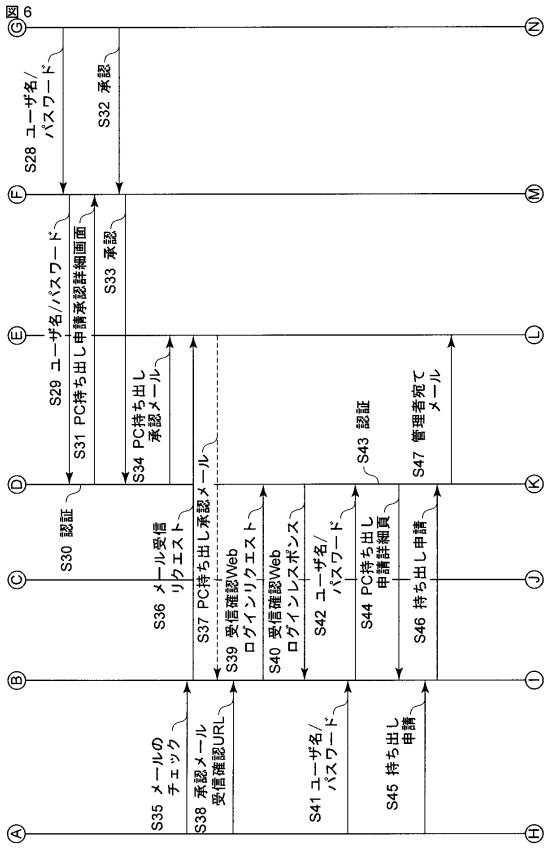
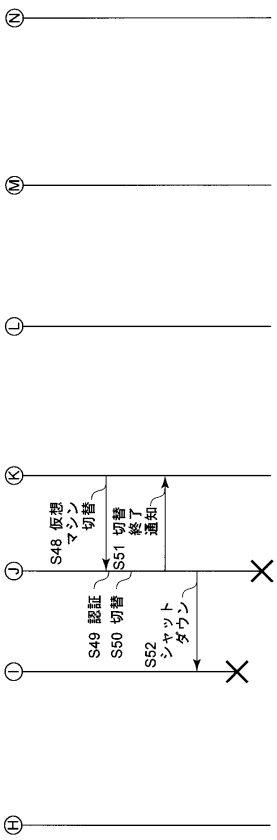


図6
G
N
F
M
E
L
D
K
C
J
B
I
A
H
S28 ユーザ名/パスワード
S32 承認
S29 ユーザ名/パスワード
S31 PC持ち出し申請承認詳細画面
S33 承認
S30 認証
S34 PC持ち出し承認メール
S43 認証
S47 管理者宛てメール
S36 メール受信リクエスト
S37 PC持ち出し承認メール
S39 受信確認Web ログインリクエスト
S40 受信確認Web ログインレスポンス
S42 ユーザ名/パスワード
S44 PC持ち出し申請詳細票
S46 持ち出し申請
S35 メールのチェック
S38 承認メール受信確認URL
S41 ユーザ名/パスワード
S45 持ち出し申請

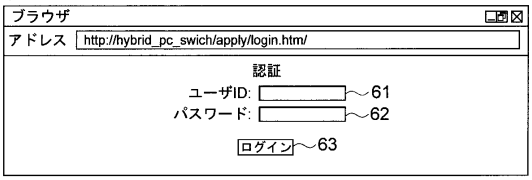
【図７】

図７



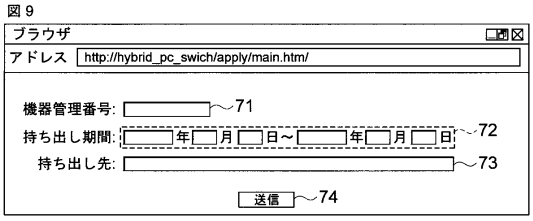
【図８】

図８



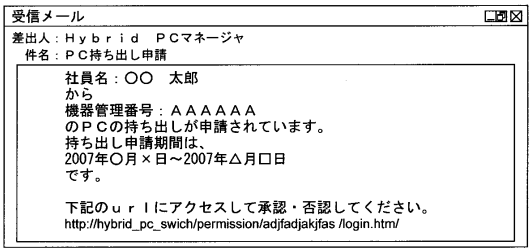
【図９】

図９



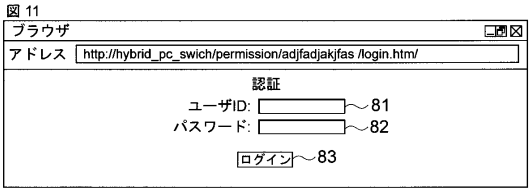
【図１０】

図10



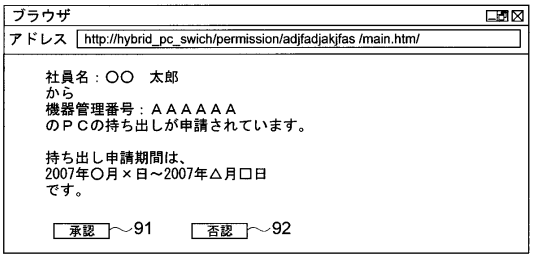
【図１１】

図11



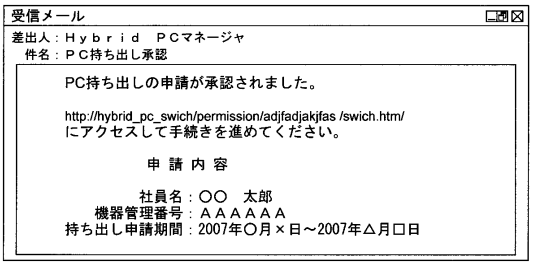
【図１２】

図12



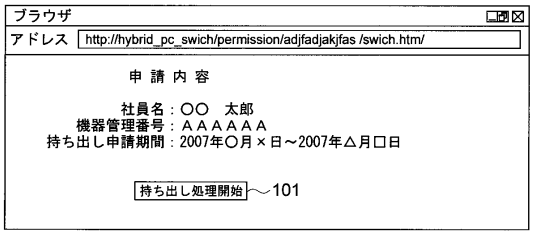
【図１３】

図13



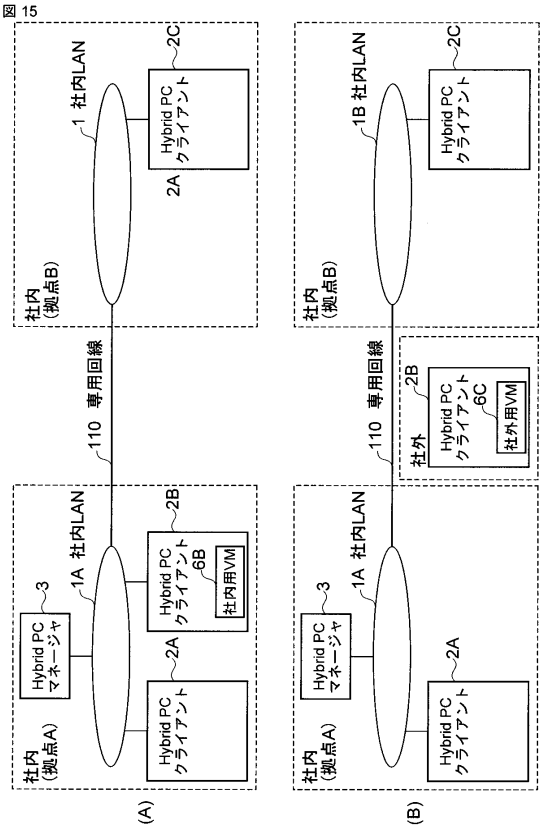
【図１４】

図 14



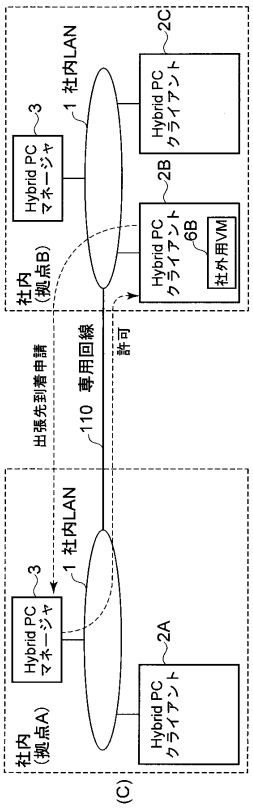
【図１５】

図 15



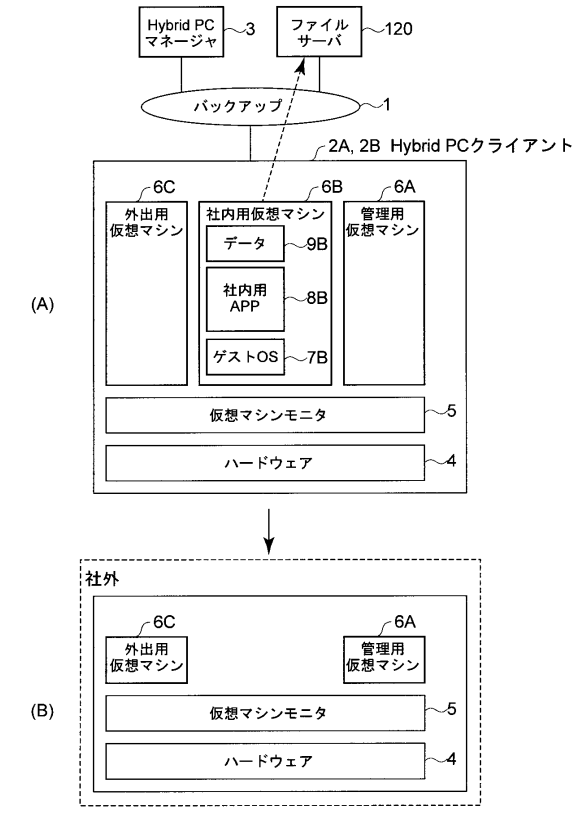
【図１６】

図 16



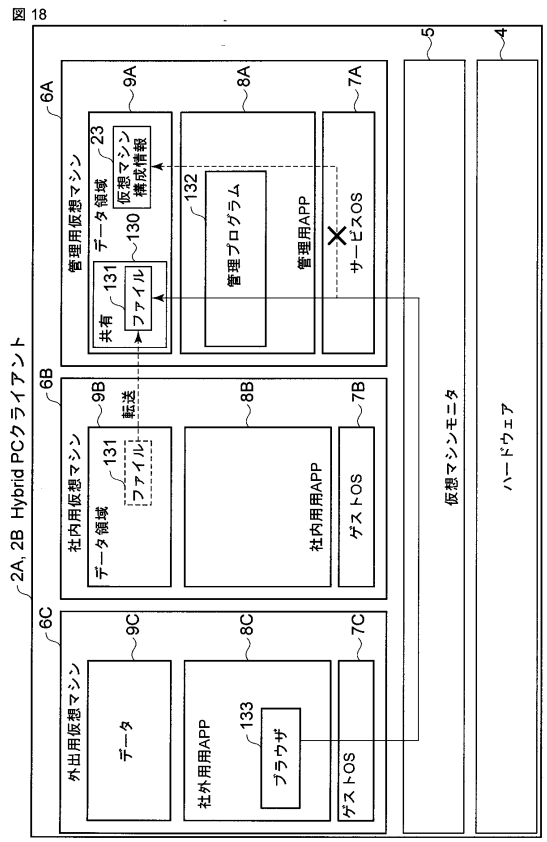
【図１７】

図 17



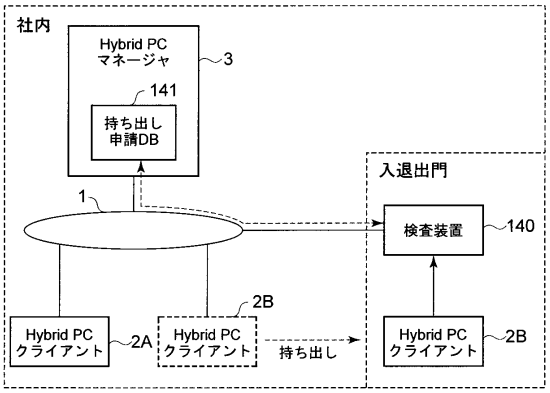
【図１８】

図 18



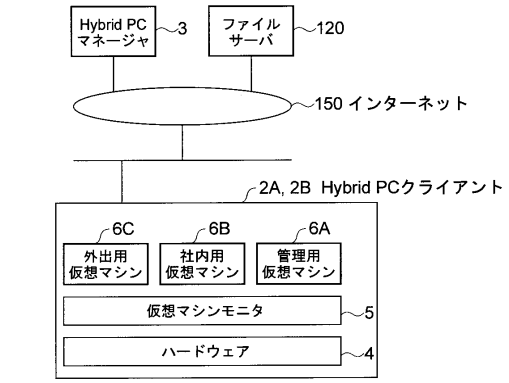
【図１９】

図 19



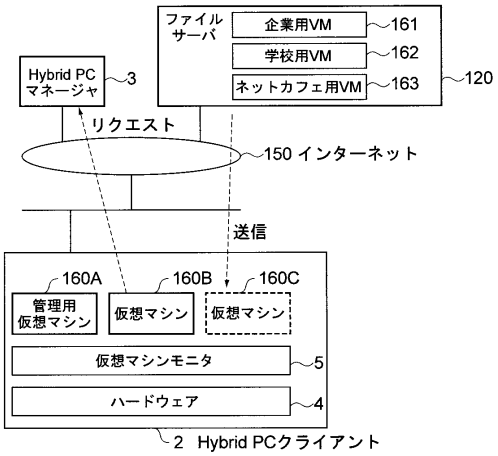
【図２０】

図 20



【図２１】

図 21



フロントページの続き

(74)代理人 100092196
弁理士 橋本 良郎
(72)発明者 嘉村 幸一郎
東京都港区芝浦一丁目１番１号 株式会社東芝内

審査官 井上 宏一

(56)参考文献 特開２０００－１１２７２０（ＪＰ，Ａ）
特開２００１－３１８７９７（ＪＰ，Ａ）
特開２００７－０２６４１２（ＪＰ，Ａ）
特開２００１－１００９８３（ＪＰ，Ａ）
特開２００８－ ７７４１３（ＪＰ，Ａ）
特表２００７－５１３４０５（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ ９／４６ －９／５４
Ｇ０６Ｆ １５／００