(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3992721号
(P3992721)
(45)発行日　平成19年10月17日(2007.10.17)　(24)登録日　平成19年8月3日(2007.8.3)

(51)Int.Cl.　F I
G06F 9/48 (2006.01)　G06F 9/46 452J

請求項の数 11 (全 16 頁)

(21)出願番号　特願2005-324863(P2005-324863)
(22)出願日　平成17年11月9日(2005.11.9)
(65)公開番号　特開2007-133572(P2007-133572A)
(43)公開日　平成19年5月31日(2007.5.31)
審査請求日　平成19年1月26日(2007.1.26)

早期審査対象出願

(73)特許権者　000005108
株式会社日立製作所
東京都千代田区丸の内一丁目６番６号
(74)代理人　110000198
特許業務法人湘洋内外特許事務所
(72)発明者　金野　正広
神奈川県川崎市幸区鹿島田８９０番地　株式会社日立製作所　情報・通信グループ内
(72)発明者　溝口　幸信
神奈川県川崎市幸区鹿島田８９０番地　株式会社日立製作所　情報・通信グループ内
(72)発明者　丸山　隆史
神奈川県川崎市幸区鹿島田８９０番地　株式会社日立製作所　情報・通信グループ内

最終頁に続く

(54)【発明の名称】情報処理装置およびプロセス制御方法

(57)【特許請求の範囲】
【請求項１】
ＯＳ（Operating System）上で稼動するプロセスを制御する情報処理装置であって、
第１の監視対象プロセスの識別情報を記憶する第１監視対象記憶手段と、
稼動中のプロセスの識別情報を管理するプロセス管理手段と、
稼動中のプロセスを強制終了させる強制終了手段と、
時間を計測するタイマ手段と、
タイマ起動フラグをオン・オフする起動フラグ設定手段と、
強制終了フラグをオン・オフする終了フラグ設定手段と、を有し、
前記起動フラグ設定手段は、
前記プロセス管理手段で管理されている稼動中のプロセスに、前記第１監視対象記憶手段に記憶されている第１の監視対象プロセスがある場合に、前記タイマ起動フラグがオフならば、当該タイマ起動フラグをオンに変更し、
前記タイマ手段は、
前記タイマ起動フラグがオンになると時間の計測を開始し、
前記強制終了手段は、
前記タイマ手段の計測時間が所定時間を超えた場合、あるいは、前記強制終了フラグがオンの場合に、前記プロセス管理手段で管理されている稼動中の、前記第１監視対象記憶手段に記憶されている第１の監視対象プロセスを強制終了させ、
前記終了フラグ設定手段は、

前記第１の監視対象記憶手段に記憶されている第１の監視対象プロセスが終了した場合に、前記強制終了フラグがオフならば、当該強制終了フラグをオンに変更すること
を特徴とする情報処理装置。
【請求項２】
請求項１に記載の情報処理装置であって、
前記強制終了手段により、前記第１監視対象記憶手段に記憶されている第１の監視対象プロセスが強制終了された場合に、メッセージを出力する第１のメッセージ出力手段を有すること
を特徴とする情報処理装置。
【請求項３】
請求項１又は２に記載の情報処理装置であって、
前記第１の監視対象プロセスは、
Ｗｅｂブラウザプログラムのプロセスであること
を特徴とする情報処理装置。
【請求項４】
請求項１乃至３のいずれか一項に記載の情報処理装置であって、
第２の監視対象プロセスの識別情報を記憶する第２監視対象記憶手段をさらに有し、
前記起動フラグ設定手段は、
前記プロセス管理手段で管理されている稼動中のプロセスに、前記第２監視対象記憶手段に記憶されている第２の監視対象プロセスがある場合に、前記タイマ起動フラグがオンならば、当該第２の監視対象プロセスを強制終了させること
を特徴とする情報処理装置。
【請求項５】
請求項４に記載の情報処理装置であって、
前記強制終了手段により、前記第２監視対象記憶手段に記憶されている第２の監視対象プロセスが強制終了された場合に、メッセージを出力する第２のメッセージ出力手段を有すること
を特徴とする情報処理装置。
【請求項６】
請求項４又は５に記載の情報処理装置であって、
前記第２の監視対象プロセスは、
ＲＡＭ（Random Access Memory）の内容をフラッシュＲＯＭ（Read Only Memory）に書き込むアップデートプログラムのプロセスであること
を特徴とする情報処理装置。
【請求項７】
請求項１乃至６のいずれか一項に記載の情報処理装置であって、
第３の監視対象プロセスの識別情報を記憶する第３監視対象記憶手段をさらに有し、
前記起動フラグ設定手段は、
前記第３監視対象記憶手段に記憶されている第３の監視対象プロセスが終了した場合に、前記タイマ起動フラグがオンならば、当該タイマ起動フラグをオフに変更し、
前記終了フラグ設定手段は、
前記第３監視対象記憶手段に記憶されている第３の監視対象プロセスが終了した場合に、前記強制終了フラグがオンならば、当該強制終了フラグをオフに変更すること
を特徴とする情報処理装置。
【請求項８】
請求項７に記載の情報処理装置であって、
前記第３の監視対象プロセスは、
リモートマシンのクライアントプログラムであること
を特徴とする情報処理装置。
【請求項９】

コンピュータで読取り可能なプログラムであって、
前記プログラムは、前記コンピュータを、
第１の監視対象プロセスの識別情報を記憶する第１監視対象記憶手段、
稼動中のプロセスの識別情報を管理するプロセス管理手段、
稼動中のプロセスを強制終了させる強制終了手段、
時間を計測するタイマ手段、
タイマ起動フラグをオン・オフする起動フラグ設定手段、および、
強制終了フラグをオン・オフする終了フラグ設定手段、として機能させ、
前記起動フラグ設定手段は、
前記プロセス管理手段で管理されている稼動中のプロセスに、前記第１監視対象記憶手段に記憶されている第１の監視対象プロセスがある場合に、前記タイマ起動フラグがオフならば、当該タイマ起動フラグをオンに変更し、
前記タイマ手段は、
前記タイマ起動フラグがオンになると時間の計測を開始し、
前記強制終了手段は、
前記タイマ手段の計測時間が所定時間を超えた場合、あるいは、前記強制終了フラグがオンの場合に、前記プロセス管理手段で管理されている稼動中の、前記第１監視対象記憶手段に記憶されている第１の監視対象プロセスを強制終了させ、
前記終了フラグ設定手段は、
前記第１の監視対象記憶手段に記憶されている第１の監視対象プロセスが終了した場合に、前記強制終了フラグがオフならば、当該強制終了フラグをオンに変更すること
を特徴とするコンピュータ読取り可能なプログラム。

【請求項１０】

コンピュータがＯＳ上で稼動するプロセスを制御するプロセス制御方法であって、
稼動中のプロセスに、予め設定された第１の監視対象プロセスがある場合に、タイマ起動フラグがオフならば、当該タイマ起動フラグをオンに変更し、
前記タイマ起動フラグがオンになると時間の計測を開始し、
計測時間が所定時間を超えた場合、あるいは、強制終了フラグがオンの場合に、稼動中の前記第１の監視対象プロセスを強制終了させ、
前記第１の監視対象プロセスが終了した場合に、前記強制終了フラグがオフならば、当該強制終了フラグをオンに変更すること
を特徴とするプロセス制御方法。

【請求項１１】

請求項８に記載の情報処理装置であって、
前記タイマ起動フラグ、前記強制終了フラグ、および、前記タイマ手段による計測値は、当該情報処理装置の再起動により初期値に戻ること
を特徴とする情報処理装置。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、ＯＳ（Operating System）上で稼動するプロセスの制御技術に関する。

【背景技術】

【０００２】

特許文献１には、名前が指定された任意のプロセスを監視対象とし、監視プロセス異常終了時の連動処理を振り分けてプロセス監視開始/終了期間の柔軟な設定が可能なプロセス監視システムが開示されている。特許文献１に記載のプロセス監視システムにおいて、監視プロセス手段は、プロセス監視開始部からの通知を受け取ると、監視プロセス定義ファイルを読込み、監視対象プロセスのプロセス名を取得する。プロセス名を基にプロセスＩＤをオペレーティングシステムのプロセス管理テーブルから検索し、監視対象プロセス群が異常終了した場合に検知できるように設定する。プロセスの異常終了を検知するとそ

の終了コードを取得し、プロセス名、終了コードをキーに監視プロセス定義ファイルを検索し、対応する連動処理を検索、実行する。また、プロセス監視終了部からの通知を受け、プロセス監視を停止する。

【０００３】

【特許文献１】特開２０００－３１１０９９号公報

【発明の開示】

【発明が解決しようとする課題】

【０００４】

近年、いわゆるシンクライアントタイプの情報処理システムが注目されている。シンクライアントタイプの情報処理システムでは、手元にあるリモートマシンを用いて自宅や会社に置いてあるローカルマシンのデスクトップを遠隔操作することで、ローカルマシンに搭載されている各種アプリケーションプログラムおよびデータを利用できる。リモートマシンには、リモートマシンをローカルマシンにネットワーク接続するための通信プログラム、リモートマシンをローカルマシンの入出力装置として機能させるためのリモートデスクトッププログラム、および、これらのプログラムを稼動させるためのＯＳが最低限搭載されていればよい。リモートマシンに各種アプリケーションプログラムおよびデータを搭載しないことで、リモートマシンの盗難等による情報漏えいの可能性を低減できる。

【０００５】

しかし、シンクライアントタイプの情報処理システムにおいて、外部のネットワークサービス（例えば商用の無線アクセスポイントサービス）を利用して、リモートマシンをローカルマシンに接続する場合、通常、サービスを利用するための認証処理（ログイン処理）が要求される。そして、この認証処理に、汎用のＷｅｂブラウザプログラムを利用することがある。近年の汎用のＷｅｂブラウザプログラムは、プラグイン機能等を備えた多機能なものが多い。そして、多機能故に、プラグイン機能等を利用したウイルスプログラムも多く存在する。したがって、セキュリティの観点からすれば、リモートマシンにおけるＷｅｂブラウザプログラムのプロセスは、認証処理の時のみ稼動させることが好ましい。特許文献１に記載のプロセス監視技術はこの点を何ら考慮していない。

【０００６】

本発明は上記事情に鑑みてなされたものであり、本発明の目的は、所定のプログラムの起動回数を制限することにある。

【課題を解決するための手段】

【０００７】

上記課題を解決するために、本発明では、所定のプロセスの稼動を監視し、該プロセスが稼動したならば、その稼動時間を計測する。そして、稼動時間が所定時間以上となったならば、該プロセスを強制終了する。その後はシステムが再起動されない限り、該プロセスが起動された場合は直ちに強制終了する。

【０００８】

例えば、本発明は、ＯＳ上で稼動するプロセスを制御する情報処理装置であって、
第１の監視対象プロセスの識別情報を記憶する第１監視対象記憶手段と、
稼動中のプロセスの識別情報を管理するプロセス管理手段と、
稼動中のプロセスを強制終了させる強制終了手段と、
時間を計測するタイマ手段と、
タイマ起動フラグをオン・オフする起動フラグ設定手段と、
強制終了フラグをオン・オフする終了フラグ設定手段と、を有し、
前記起動フラグ設定手段は、
前記プロセス管理手段で管理されている稼動中のプロセスに、前記第１監視対象記憶手段に記憶されている第１の監視対象プロセスがある場合に、前記タイマ起動フラグがオフならば、当該タイマ起動フラグをオンに変更し、
前記タイマ手段は、
前記タイマ起動フラグがオンになると時間の計測を開始し、

前記強制終了手段は、
前記タイマ手段の計測時間が所定時間を超えた場合、あるいは、前記強制終了フラグがオンの場合に、前記プロセス管理手段で管理されている稼動中の、前記第１監視対象記憶手段に記憶されている第１の監視対象プロセスを強制終了させ、
前記終了フラグ設定手段は、
前記第１の監視対象記憶手段に記憶されている第１の監視対象プロセスが終了した場合に、前記強制終了フラグがオフならば、当該強制終了フラグをオンに変更する。
【発明の効果】
【０００９】
本発明によれば、第１の監視対象プロセス（例えばＷｅｂブラウザプログラムのプロセス）の稼動回数を制限することができる。このため、システムのセキュリティを向上させることができる。
【発明を実施するための最良の形態】
【００１０】
以下、本発明の一実施形態を説明する。
【００１１】
図１は本発明の一実施形態が適用されたリモートデスクトップシステム（シンクライアントタイプの情報処理システム）の概略図である。図示するように、本実施形態のリモートデスクトップシステムは、会社、自宅等に構築された内部ネットワークであるＬＡＮ（Local Area Netwoek）４Ａに接続されるローカルマシン１と、ホテル、駅等の出先に構築された外部ネットワークであるＬＡＮ４Ｂに接続されるリモートマシン２と、を有する。ＬＡＮ４Ａはルータ３Ａを介してＷＡＮ(Wide Area Network）５に接続される。また、ＬＡＮ４Ｂはルータ３ＢをＷＡＮ５に接続される。
【００１２】
なお、本実施形態において、ルータ３Ｂは、ＬＡＮ４Ｂに接続されたネットワーク端末間では自由な通信を許可しているが、ＬＡＮ４ＢおよびＷＡＮ５間の通信は、ＬＡＮ４Ｂに接続されているネットワーク端末に対して汎用のＷｅｂブラウザプログラムを用いた認証処理（ログイン処理）を要求し、当該ネットワーク端末が当該認証処理をパスした場合にのみ認めている。また、ＬＡＮ４ＢおよびＷＡＮ５間の通信に対して課金を行い、この課金を終了させるためには、ＬＡＮ４Ｂに接続されているネットワーク端末に対して汎用のＷｅｂブラウザプログラムを用いた通知処理（ログアウト処理）を要求している。
【００１３】
ローカルマシン１は、リモートマシン２との間にＶＰＮ（Virtual Private Network）を構築し、該ＶＰＮを介して、リモートマシン２から送られてきた入力情報（入力装置の操作内容）を受信し処理すると共に、処理結果を示す映像情報（表示装置のデスクトップ画面）をリモートマシン２に送信する。ローカルマシン１は、ＰＣ（Peasonal Computer）、サーバ等のコンピュータである。
【００１４】
図２はローカルマシン１の概略図である。図示するように、ローカルマシン１は、ＣＰＵ（Central Processing Unit）１０１と、ＣＰＵ１０１のワークエリアとして機能するＲＡＭ（Random Access Memory）１０２と、ＬＡＮ４Ａに接続するためのＮＩＣ（Network Interface Card）１０３と、ＨＤＤ（Hard Disk Drive）１０４と、フラッシュＲＯＭ（Read Only Memory）１０５と、キーボードおよびマウスを接続するためのＩ/Ｏ（Input/Output）コネクタ１０６と、ディスプレイを接続するためのビデオカード１０７と、これらの各部１０１～１０７と接続するバスＢＵＳを中継するブリッジ１０８と、電源１０９と、を有する。
【００１５】
フラッシュＲＯＭ１０５には、ＢＩＯＳ（Basic Input/Output System）１０５０が記憶されている。ＣＰＵ１０１は、電源１０９の投入後、先ずフラッシュＲＯＭ１０５にアクセスしてＢＩＯＳ１０５１０を実行することにより、ローカルマシン１のシステム構成

を認識する。

【００１６】

ＨＤＤ１０４には、ＯＳ（Operating System）１０４１、ＶＰＮ通信プログラム１０４２、リモートサーバプログラム１０４３、および、複数のアプリケーションプログラム１０４４が、少なくとも記憶されている。

【００１７】

ＯＳ１０４１は、ＣＰＵ１０１がローカルマシン１の各部１０２～１０９を統括的に制御して、後述する各プログラム１０４２～１０４４を実行するためのプログラムである。ＣＰＵ１０１は、ＢＩＯＳ１０５０に従い、ＨＤＤ１０４からＯＳ１０４１をＲＡＭ１０２にロードして実行する。これにより、ＣＰＵ１０１は、ローカルマシン１の各部１０２～１０９を統括的に制御する。

【００１８】

ＶＰＮ通信プログラム１０４２は、リモートマシン２との間にＶＰＮを構築するための通信プログラムであり、例えばＩＰｓｅｃ（Security Architecture for the Internet Protocol）を用いた通信プログラムである。ＣＰＵ１０１は、ＯＳ１０４１に従い、ＨＤＤ１０４からＶＰＮ通信プログラム１０４２をＲＡＭ１０２にロードして実行する。これにより、ＣＰＵ１０１は、ＮＩＣ１０３を介してリモートマシン２から受付けた通信開始要求に従い、リモートマシン２との間にＶＰＮを構築し、このＶＰＮを介してリモートマシン２と通信を行なう。

【００１９】

リモートサーバプログラム１０４３は、ローカルマシン１のデスクトップをリモートマシン２から遠隔操作可能とするためのプログラムであり、例えばＡＴ＆Ｔケンブリッジ研究所で開発されたＶＮＣ（Virtual Network Computing）のサーバプログラムである。ＣＰＵ１０１は、ＯＳ１０４１に従い、ＨＤＤ１０４からリモートサーバプログラム１０４３をＲＡＭ１０２にロードして実行する。これにより、ＣＰＵ１０１は、ＶＰＮを介してリモートマシン２から送られてきた入力情報（キーボードおよびマウスの操作内容）を受信し処理すると共に、処理結果を示す映像情報（ディスプレイのデスクトップ画面）をＶＰＮを介してリモートマシン２に送信する。

【００２０】

アプリケーションプログラム１０４４には、汎用のＷｅｂブラウザ、ワープロ、表計算等のプログラムがある。ＣＰＵ１０１は、ＯＳ１０４１に従い、Ｉ/Ｏコネクタ１０６を介してキーボードおよびマウスから受付けた指示、あるいは、リモートサーバプログラム１０４３を介してリモートマシン２から受付けた指示に応答して、ＨＤＤ１０４から所望のアプリケーションプログラム１０４４をＲＡＭ１０２にロードし実行する。そして、この実行結果が反映されたデスクトップ画面を表す映像情報をビデオカード１０７から出力すると共に、リモートサーバプログラム１０４３を介してリモートマシン２へ送信する。

【００２１】

図１に戻って説明を続ける。リモートマシン２は、サーバマシン１との間にＶＰＮを構築し、該ＶＰＮを介して、リモートマシン２に入力された入力情報（入力装置の操作内容）をサーバマシン１へ送信すると共に、サーバマシン１から映像像情（表示装置のデスクトップ画面）を受信し、これをリモートマシン２のディスプレイに表示する。リモートマシン２は、いわゆるＨＤＤレスタイプのＰＣであり、プリンタ、外付けドライブ、外付けメモリ等をローカル接続およびネットワーク接続できないように構成されている。つまり、リモートマシン２は、ローカルマシン１にローカル接続あるいはネットワーク接続されているプリンタ、外付けドライブ、外付けメモリ等のみを使用できるように構成されている。このようにすることで、リモートマシン２の盗難等による情報漏えいの可能性を低減している。

【００２２】

図３はリモートマシン２の概略図である。図示するように、リモートマシン２は、ＣＰＵ２０１と、ＣＰＵ２０１のワークエリアとして機能するＲＡＭ２０２と、ＬＡＮ４Ｂに

接続するためのＮＩＣ２０３と、認証デバイス（ＵＳＢデバイス）６を接続するためのＵＳＢポート２０４と、フラッシュＲＯＭ２０５と、キーボードおよびマウスを接続するためのＩ/Ｏコネクタ２０６と、ディスプレイを接続するためのビデオカード２０７と、これらの各部２０１～２０７と接続するバスＢＵＳを中継するブリッジ２０８と、電源２０９と、を有する。

【００２３】

フラッシュＲＯＭ２０５には、ＢＩＯＳ２０５０、ＯＳ２０５１、ＶＰＮ通信プログラム２０５２、リモートサーバプログラム２０５３、Ｗｅｂブラウザプログラム２０５４Ａ、および、アップデートプログラム２０５４Ｂが、少なくとも記憶されている。

【００２４】

ＣＰＵ２０１は、電源２０９の投入後、先ずフラッシュＲＯＭ２０５にアクセスしてＢＩＯＳ２０５０を実行することにより、リモートマシン２のシステム構成を認識する。

【００２５】

ＯＳ２０５１は、ＣＰＵ２０１がリモートマシン２の各部２０２～２０９を統括的に制御して、後述する各プログラム２０５２～２０５４を実行するためのプログラムである。ＣＰＵ２０１は、ＢＩＯＳ２０５０に従い、フラッシュＲＯＭ２０５からＯＳ２０５１をＲＡＭ２０２にロードして実行する。これにより、ＣＰＵ２０１は、リモートマシン２の各部２１０２～２０９を統括的に制御する。なお、本実施形態のＯＳ２０５１には、組み込み型ＯＳ等のフラッシュＲＯＭ２０５に格納可能な比較的サイズの小さいものが利用される。また、ＯＳ２０５１は、プロセスの稼動を制御するプロセス制御部２０５１０を有する。プロセス制御部２０５１０については後述する。

【００２６】

ＶＰＮ通信プログラム２０５２は、ローカルマシン１との間にＶＰＮを構築するための通信プログラムであり、例えばＩＰｓｅｃを用いた通信プログラムである。ＣＰＵ２０１は、ＯＳ２０５１に従い、フラッシュＲＯＭ２０５からＶＰＮ通信プログラム２０５２をＲＡＭ２０２にロードして実行する。これにより、ＣＰＵ２０１は、ＮＩＣ２０３を介してローカルマシン１へ通信開始要求を送信して、ローカルマシン１との間にＶＰＮを構築し、このＶＰＮを介してローカルマシン１と通信を行なう。

【００２７】

リモートクライアントプログラム２０５３は、リモートマシン２が遠隔からローカルマシン１のデスクトップにアクセスするためのプログラムであり、例えばＶＮＣのクライアント（ビューワ）プログラムである。ＣＰＵ２０１は、ＯＳ２０４１に従い、フラッシュＲＯＭ２０５からリモートクライアントプログラム２０５３をＲＡＭ２０２にロードして実行する。これにより、ＣＰＵ２０１は、Ｉ/Ｏコネクタ２０６の入力情報（キーボードおよびマウスの操作内容）をＶＰＮを介してローカルマシン１に送信すると共に、ＶＰＮを介してローカルサーバ１から送られてきた映像情報（ディスプレイのデスクトップ画面）をビデオカード２０７に接続されたディスプレイ（不図示）に出力する。

【００２８】

なお、リモートクライアントプログラム２０５３は、上述の処理の実行に先立ってＣＰＵ２０１に次の認証処理を行わせる。すなわち、ＣＰＵ２０１は、ビデオカード２０７に接続されたディスプレイにパスワードの入力フォームを表示させ、Ｉ/Ｏコネクタ２０６に接続されたキーボードおよびマウスを介してユーザからパスワードの入力を受付ける。そして、受付けたパスワードをＵＳＢポート２０４に接続されている認証デバイス６に送信してパスワードの認証を依頼する。そして、パスワードの認証が成立した場合にのみ、上述の処理を実行する。

【００２９】

ここで、認証デバイス６について説明する。認証デバイス６は、リモートマシン２の本体から受け取ったパスワードの認証を行い、その検証結果をリモートマシン２の本体へ通知する。図４は認証デバイス６の概略図である。図示するように、認証デバイス６は、リモートマシン２のＵＳＢポート２０４に接続するためのＵＳＢアダプタ６０１と、ＩＣチ

ップ６０２と、を有する。ＩＣチップ６０２には、ユーザのパスワード６０３１および認証プログラム６０３２が記憶されている。認証デバイス６のＵＳＢアダプタ６０１がリモートマシン２のＵＳＢポート２０４に接続され、これにより、リモートマシン２から認証デバイス６へ電源が供給されると、ＩＣチップ６０２は、認証プログラム６０３２を実行する。そして、認証プログラム６０３２に従いリモートマシン２からパスワードを受け取ると、これとフラッシュＲＯＭ６０３に格納されているパスワード６０３１とを比較する。両者が一致する場合は認証成功を示すメッセージをリモートマシン２に出力し、一方、両者が一致しない場合は認証不成立を示すメッセージをリモートマシン２に出力する。なお、本実施形態では、認証デバイス６がＵＳＢデバイスである場合を例にとり説明したが、これに限定されるものではない。認証デバイス６は例えばＩＣカードでもよい。あるいは、Ｂｌｕｅｔｏｏｔｈ（登録商標）等の近距離無線通信を利用するものでもよい。また、認証デバイス６に、フラッシュメモリを外付けできるように構成し、ＩＣチップ６０２内の一部のデータをこのフラッシュメモリに記憶するようにしてもかまわない。

【００３０】

図３に戻って説明を続ける。Ｗｅｂブラウザプログラム２０５４Ａには、市販あるいは無料配布されている汎用のＷｅｂブラウザプログラムが利用される。なお、近年の汎用のＷｅｂブラウザプログラムは、プラグイン機能等を備えた多機能なものが多い。そして、多機能故に、プラグイン機能等を利用したウイルスプログラムも多く存在する。なお、本実施形態において、Ｗｅｂブラウザプログラム２０５４Ａは、ＬＡＮ４ＢからＷＡＮ５へアクセスするためのルータ３Ｂに対する認証処理（ログイン処理）、および、ＬＡＮ４ＢからＷＡＮ５へのアクセスを終了して課金を終了させるためのルータ３Ｂに対する通知処理（ログアウト処理）に、利用される。

【００３１】

アップデートプログラム２０５４Ｂは、ＮＩＣ２０３を介して図示していないサーバにアクセスし、該サーバからＯＳ２０５１等の更新データを入手してＲＡＭ２０２に格納する。そして、ＲＡＭ２０２に格納した更新データをフラッシュＲＯＭ２０５１に格納されているＯＳ２０５１等に反映させる。

【００３２】

プロセス制御部２０５１０は、ＯＳ２０５１上で稼動するプロセスを制御する。図５はプロセス制御部２０５１０を模式的に表した図である。図示するように、プロセス制御部２０５１０は、第１監視対象管理テーブル２０５１１、第２監視対象管理テーブル２０５１２、第３監視対象管理テーブル２０５１３、プロセス管理部２０５１４、強制終了部２０５１５、タイマ部２０５１６、起動フラグ設定部２０５１７、および、終了フラグ設定部２０５１８を有する。

【００３３】

第１監視対象管理テーブル２０５１１には、強制終了の対象となるプロセスのプロセスＩＤおよびモジュール名が登録される。近年の汎用のＷｅｂブラウザプログラムは、プラグイン機能等を備えた多機能なものが多い。そして、多機能故に、プラグイン機能等を利用したウイルスプログラムも多く存在する。そこで、本実施形態では、ＷｅｂブラウザプログラムＡを強制終了の対象となるプロセスのプログラムに設定している。

【００３４】

第２監視対象管理テーブル２０５２２には、強制終了対象プロセスの実行後に、実行することを禁止するプロセスのプロセスＩＤおよびモジュール名が登録される。上述したように、本実施形態では、ＷｅｂブラウザプログラムＡを強制終了対象プロセスのプログラムに設定している。そして、ＷｅｂブラウザプログラムＡは、プラグイン機能等を備えた多機能なものが多い。このプラグイン機能が実施されると、ＷｅｂブラウザプログラムＡの終了後にも、プラグインモジュールがＲＡＭ２０２上に残る場合がある。この状態で、アップデートプログラム２０５４Ｂが実行されると、ＲＡＭ２０２上に残るプラグインモジュールがフラッシュＲＯＭ２０５に書き込まれる可能性があり、この場合、リモートマシン２の動作に悪影響を与えるおそれがある。そこで、本実施

形態では、アップデートプログラム２０５４Ｂを、強制終了対象プロセスの実行後に、実行することを禁止するプロセスのプログラムに設定している。

【００３５】

第３監視対象管理テーブル２０５１３は、強制終了対象プロセスの稼動禁止を解除するプロセスのプロセスＩＤおよびモジュール名が登録される。上述したように、本実施形態では、Ｗｅｂブラウザプログラム２０５４Ａを強制終了対象プロセスのプログラムに設定している。そして、Ｗｅｂブラウザプログラム２０５４Ａは、ルータ３Ｂに対する認証処理（ログイン処理）およびルータ３Ｂに対する通知処理（ログアウト処理）の場合に利用される。ここで、ルータ３Ｂに対する通知処理は、ローカルマシン１へのアクセスを終了し、その結果、ＷＡＮ５を使用する必要がなくなった場合、つまり、リモートクライアントＰＧ２０５３の終了後に発生する。そこで、本実施形態では、リモートクライアントプログラム２０５３を、強制終了対象プロセスの稼動禁止を解除するプロセスのプログラムに設定している。

【００３６】

プロセス管理部２０５１４は、ＯＳ２０５１上で稼動中のプロセスを監視する。具体的には、新たなプロセスが起動されたならば、当該プロセスの識別情報であるプロセスＩＤおよびモジュール名を、プロセス管理部２０５１４が備えるプロセス管理テーブル（不図示）に登録する。また、稼動中のいずれかのプロセスが終了したならば、当該プロセスのプロセスＩＤおよびモジュール名を該プロセス管理テーブルから削除する。

【００３７】

起動フラグ設定部２０５１７は、経過時間の計測開始を指示するタイマ起動フラグを備え、該タイマ起動フラグのオン・オフを設定する。

【００３８】

終了フラグ設定部２０５１８は、強制終了対象プログラムの強制終了の実施を指示する強制終了フラグを備え、該強制終了フラグのオン・オフを設定する。

【００３９】

タイマ部２０５１６は、起動フラグ設定部２０５１７が備えるタイマ起動フラグを監視し、該タイマ起動フラグがオフからオンに遷移したならば、経過時間の計測を開始する。また、該タイマ起動フラグがオンからオフに遷移したならば、経過時間の計測を終了して計測値を０にリセットする。

【００４０】

強制終了部２０５１５は、起動フラグ設定部２０５１７が備えるタイマ起動フラグ、および、終了フラグ設定部２０５１８が備える強制終了フラグのオン・オフに基づいて、第１監視対象管理テーブル２０５１１に登録されているプロセスＩＤおよびモジュール名を持つプロセス（Ｗｅｂブラウザプログラム２０５４Ａのプロセス）、および、第２監視対象管理テーブル２０５１２に登録されているプロセスＩＤおよびモジュール名を持つプロセス（アップデートプログラム２０５４Ｂのプロセス）の実行を制御する。

【００４１】

図６および図７はプロセス制御部２０５１によるＣＰＵ２０１の処理を説明するためのフロー図である。なお、このフローは、本来、ＣＰＵ２０１がプロセス制御部（プログラム）２０５１に従って実行する。しかし、ここでは、説明を簡単にするために、プロセス制御部２０５を構成する各プログラムを実行主体として、フローを説明する。

【００４２】

起動フラグ設定部２０５１７は、プロセス管理部２０５１４が備えるプロセス管理テーブルに、Ｗｅｂブラウザプログラム２０５４Ａのプロセス（第１監視対象）のプロセスＩＤおよびモジュール名が登録されたのを検出すると（Ｓ１００でＹＥＳ）、タイマ起動フラグがオンか否かを調べる（Ｓ１０１）。タイマ起動フラグがオフならば（Ｓ１０１でＮＯ）、これをオンに変更し（Ｓ１０３）、Ｓ１００に戻る。一方、タイマ起動フラグがオンならば（Ｓ１０１でＹＥＳ）、強制終了部２０５１５に、検出したＷｅｂブラウザプログラム２０５４Ａのプロセスのプロセスおよびモジュール名を通知する。これを受け

て、強制終了部２０５１５は、このプロセスＩＤおよびモジュール名を持つＷｅｂブラウザプログラム２０５４Ａのプロセスを強制終了すると共に、ビデオカード２０７に接続されたディスプレイに例えば「利用回数が上限を超えています」などといったメッセージを出力する（Ｓ１０２）。

【００４３】

また、終了フラグ設定部２０５１８は、プロセス管理部２０５１４が備えるプロセス管理テーブルから、Ｗｅｂブラウザプログラム２０５４Ａのプロセスのプロセスおよびモジュール名が削除されたのを検出すると（Ｓ１１０でＹＥＳ）、強制終了フラグがオフか否かを調べる（Ｓ１１１）。強制終了フラグがオフならば（Ｓ１１１でＹＥＳ）、これをオンに変更し（Ｓ１１２）、Ｓ１００に戻る。一方、強制終了フラグがオンならば（Ｓ１１１でＮＯ）、強制終了フラグを変更することなしにＳ１００に戻る。

【００４４】

また、タイマ部２０５１６は、タイマ起動フラグがオンであるか否かを調べる（Ｓ１２０）、タイマ起動フラグがオンである場合（Ｓ１２０でＹＥＳ）、経過時間を計測中であるならば（Ｓ１２１でＹＥＳ）、Ｓ１００に戻る。経過時間を計測中でないならば（Ｓ１２１でＮＯ）、経過時間の計測を開始し（Ｓ１２２）、それからＳ１００に戻る。

【００４５】

また、強制終了部２０５１５は、タイマ部２０５１６の計測値が所定値（少なくともＷｅｂブラウザプログラム２０５４Ａによるルータ３Ｂに対するログインおよびログアウト処理にかかる時間）以上であるか否かを判断する（Ｓ１３０）。計測値が所定値以上である場合（Ｓ１３０でＹＥＳ）、強制終了フラグがオフならば（Ｓ１３１でＮＯ）、Ｗｅｂブラウザプログラム２０５４Ａのプロセスを強制終了すると共に、ビデオカード２０７に接続されたディスプレイに例えば「利用時間を経過しました」などといったメッセージを出力する（Ｓ１３２）。それから、Ｓ１００に戻る。一方、強制終了フラグがオンの場合（Ｓ１３１でＹＥＳ）は、Ｗｅｂブラウザプログラム２０５４Ａのプロセスは既に終了しているので、直ちにＳ１００に戻る。

【００４６】

また、強制終了部２０５１５は、プロセス管理部２０５１４が備えるプロセス管理テーブルに、アップデートプログラム２０５４Ｂのプロセス（第２監視対象）のプロセスＩＤおよびモジュール名が登録されたのを検出すると（Ｓ１４０でＹＥＳ）、タイマ起動フラグがオンか否かを調べる（Ｓ１４１）。タイマ起動フラグがオンならば（Ｓ１４１でＹＥＳ）、このプロセスＩＤおよびモジュール名を持つアップデートプログラム２０５４Ｂのプロセスを強制終了すると共に、ビデオカード２０７に接続されたディスプレイに例えば「Ｗｅｂブラウザを起動した場合は利用できません」などといったメッセージを出力する（Ｓ１４２）。

【００４７】

また、起動フラグ設定部２０５１７は、プロセス管理部２０５１４が備えるプロセス管理テーブルから、リモートクライアントプログラム２０５３のプロセス（第３監視対象）のプロセスＩＤおよびモジュール名が削除されたのを検出すると（Ｓ１５０でＹＥＳ）、タイマ起動フラグがオンならば（Ｓ１５１でＹＥＳ）、これをオフに変更する（Ｓ１５２）。同様に、終了フラグ設定部２０５１８は、プロセス管理テーブルからリモートクライアントプログラム２０５３のプロセスのプロセスＩＤおよびモジュール名が削除されたのを検出すると（Ｓ１５０でＹＥＳ）、強制終了フラグがオンならば（Ｓ１５３でＹＥＳ）、これをオフに変更する（Ｓ１５４）。

【００４８】

なお、タイマ起動フラグ、強制終了フラグおよび経過時間の計測値は、リモートマシン２の再起動等によりＲＡＭ２０２がクリアされることで、初期値(フラグオフ、経過時間「０」）に戻る。

【００４９】

次に、上記構成のリモートデスクトップシステムの概略動作を説明する。

【００５０】
図８はリモートデスクトップシステムの概略動作を説明するための図である。
【００５１】
リモートマシン２において、ユーザの指示に従いＷｅｂブラウザプログラム２０５４Ａが起動され、Ｗｅｂブラウザプログラム２０５４ＡがＷＡＮ５へアクセスしようとすると、ルータ３Ｂがこれを検知し、リモートマシン２にログイン画面を表示して（Ｓ２０２）、ログイン情報の入力を促す。
【００５２】
リモートマシン２において、ユーザがログイン画面にログイン情報を入力すると（Ｓ２０３）、ルータ３Ｂによってこのログイン情報が検証される。ルータ３Ｂは、ログイン情報が正しければ、リモートマシン２のＷＡＮ５へのアクセスを許可する（Ｓ２０４）。
【００５３】
その後、リモートマシン２において、ＶＰＮ通信プログラム２０５２は、ローカルマシン１のＶＰＮ通信プログラム１０４２と連携して、リモートマシン２およびローカルマシン１間にＶＰＮを確立する（Ｓ２０５）。
【００５４】
次に、リモートマシン２において、リモートクライアントプログラム２０５３は、ユーザにパスワードを要求し（Ｓ２０６）、ユーザが入力したパスワードを含む認証依頼を、リモートマシン２に接続された認証デバイス６に送信する（Ｓ２０７）。これを受けて、認証デバイス６は、パスワードの認証を行い、その認証結果をリモートマシン２に返す（Ｓ２０８）。
【００５５】
リモートマシン２において、リモートクライアントプログラム２０５３は、認証デバイス６から受け取った認証結果が認証成立ならば、Ｓ２０５で確立したＶＰＮを用いて、リモートマシン２によるローカルマシン１のデスクトップの遠隔操作を開始する（Ｓ２０９）。これにより、リモートマシン２の入力装置に入力されたユーザの入力情報がローカルマシン１に送信され（Ｓ２１０）、ローカルマシン１からはユーザの入力情報を反映させたローカルマシン１のデスクトップ画面の映像情報がリモートマシン２に送信される（Ｓ２１１）。
【００５６】
さて、リモートマシン２は、ユーザの指示に従いローカルマシン１のリモート操作を終了する（Ｓ２１２）。それから、ユーザの指示に従いＷｅｂブラウザプログラム２０５４Ａを起動し（Ｓ２１３）、ルータ３Ｂに対してログアウト処理を行う（Ｓ２１４）。これにより、ルータ３Ｂは課金処理を終了する（Ｓ２１５）。
【００５７】
その後、リモートマシン２において、ＶＰＮ通信プログラム２０５２は、ローカルマシン１のＶＰＮ通信プログラム１０４２と連携して、リモートマシン２およびローカルマシン１間にＶＰＮを切断する（Ｓ２１６）。
【００５８】
ここで、Ｓ２０１によってＷｅｂブラウザプログラム２０５４Ａが起動されてからＳ２１２によってリモート操作が終了するまでのｔ１の間、タイマ起動フラグおよび強制終了フラグの少なくとも一方がオンとなるので、Ｗｅｂブラウザプログラム２０５４Ａおよびアップデートプログラム２０５４Ｂの起動は直ちに強制終了される。そして、リモート操作が終了すると、タイマ起動フラグおよび強制終了フラグが両方ともオフになるので、Ｗｅｂブラウザプログラム２０５４Ａおよびアップデートプログラム２０５４Ｂの起動停止が解除される。このため、Ｗｅｂブラウザプログラム２０５４Ａを用いたログアウト処理が可能となる。そして、再度Ｗｅｂブラウザプログラム２０５４Ａが起動したならば、その後のｔ２の間は、タイマ起動フラグおよび強制終了フラグの少なくとも一方が常にオンとなるので、Ｗｅｂブラウザプログラム２０５４Ａおよびアップデートプログラム２０５４Ｂの起動は直ちに強制終了される。この状態を解除するためには、例えばリモートマシ

ン２を再起動してＲＡＭ２０２をクリアし、フラグを初期状態（オフ）に戻す。

【００５９】

以上、本発明の一実施形態について説明した。

【００６０】

本実施形態では、リモートマシン２において、第１監視対象プロセスであるＷｅｂブラウザプログラム２０５４Ａの稼動を、リモートクライアントプログラム２０５３の終了前後において、それぞれ１回に規制することができる。つまり、リモートマシン２をローカルマシン１に接続するためにＷＡＮ５へアクセスする際に要求されるルータ３Ｂに対する認証処理（ログイン処理）のため、および、リモートマシン２のローカルマシン１への接続を解除してＷＡＮ５へのアクセスを終了する際に課金を終了させるために要求されるルータ３Ｂに対する通知処理（ログアウト処理）のための２回に限り、Ｗｅｂブラウザプログ２０５４Ａの稼動を許可することができる。

【００６１】

上述したように、近年の汎用のＷｅｂブラウザプログラム２０５４Ａは、プラグイン機能等を備えた多機能なものが多い。そして、多機能故に、プラグイン機能等を利用したウイルスプログラムも多く存在する。本実施形態では、このようなＷｅｂブラウザプログラム２０５４Ａの稼動を必要最低限の回数に限定することができるので、セキュリティを向上させることができる。

【００６２】

また、Ｗｅｂブラウザプログラム２０５４Ａのプラグイン機能が実施されると、Ｗｅｂブラウザプログラム２０５４Ａの終了後にも、プラグインモジュールがＲＡＭ２０２上に残る場合がある。この状態で、アップデートプログラム２０５４Ｂが実行されると、ＲＡＭ２０２上に残るプラグインモジュールがフラッシュＲＯＭ２０５に書き込まれる可能性があり、この場合リモートマシン２の動作に悪影響を与えるおそれがある。本実施形態では、アップデートプログラム２０５４Ｂを、Ｗｅｂブラウザプログラム２０５４Ａの実行後に実行することを禁止している。このようにすることで、リモートマシン２の安定性をいより向上させることができる。

【００６３】

なお、本実施形態の上記の実施形態に限定されるものではなく、その要旨の範囲内で数々の変形が可能である。

【００６４】

例えば、上記の実施形態では、強制終了対象プロセスとして、Ｗｅｂブラウザプログラム２０５４Ａのプロセスを例にとり説明した。しかし、本発明はこれに限定されない。ウイルス感染や不正アクセスの対象となり易いプログラム（例えばプラグイン機能を備えたプログラム）のプロセスを強制終了対象プロセスとするものであればよい。

【００６５】

また、上記の実施形態では、強制終了対象プロセスの実行後に、実行することを禁止するプロセスとして、アップデートプログラム２０５４Ｂのプロセスを例にとり説明した。しかし、本発明はこれに限定されない。ウイルス感染や不正アクセスの影響を拡大し易いプログラム（例えば複製プログラム）のプロセスを、強制終了対象プロセスの実行後に、実行することを禁止するプロセスとしてもよい。

【００６６】

また、上記の実施形態では、強制終了対象プロセスの稼動禁止を解除するプロセスとして、リモートクライアントプログラム２０５３を例にとり説明した。しかし、本発明はこれに限定されない。稼動禁止に設定した強制終了対象プロセスを再度稼動させる必要性が生じたことを検知できるプログラムのプロセスであればよい。例えば、本実施形態では、リモートクライアントプログラム２０５３の代わりに、ＶＰＮ通信プログラム２０５２のプロセスを、強制終了対象プロセスの稼動禁止を解除するプロセスとしてもよい。

【００６７】

また、上記の実施形態では、ローカルマシン１およびリモートマシン２間にＶＰＮを構

築して通信を行なう場合を例にとり説明したが、本発明はこれに限定されない。ＶＰＮを構築することなく、ローカルマシン１およびリモートマシン２間で通信を行なえるようにしてもよい。

【００６８】

また、上記の実施形態では、本発明をいわゆるシンクライアント型の情報処理システムであるリモートデスクトップシステムのリモートマシン２に適用した場合を例にとり説明したが、本発明は通常のＰＣを含む様々な情報処理装置に適用できる。

【図面の簡単な説明】

【００６９】

【図１】図１は本発明の一実施形態が適用されたリモートデスクトップシステムの概略図である。

【図２】図２はローカルマシン１の概略図である。

【図３】図３はリモートマシン２の概略成図である。

【図４】図４は認証デバイス４の概略図である。

【図５】図５はプロセス制御部２０５１０を模式的に表した図である。

【図６】図６はプロセス制御部２０５１０を動作を説明するための図である。

【図７】図７はプロセス制御部２０５１０を動作を説明するための図である。

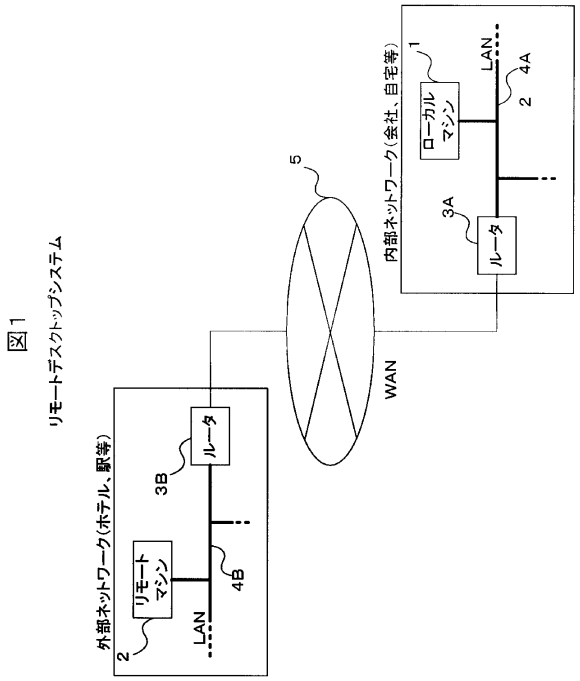
【図８】図８はリモートデスクトップシステムの概略動作を説明するための図である。

【符号の説明】

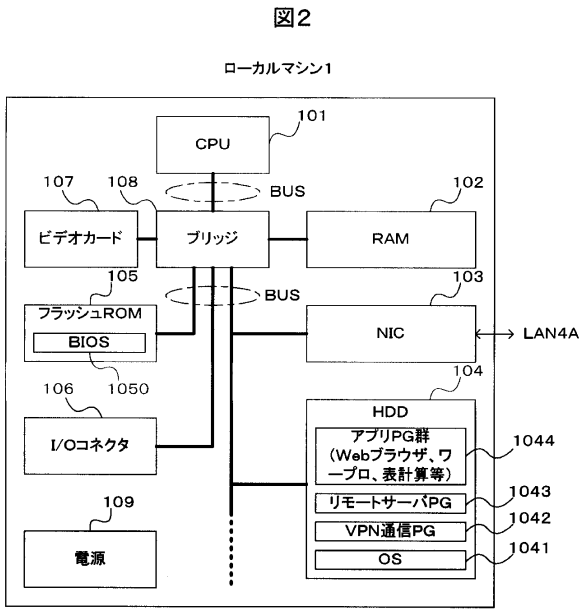
【００７０】

１…ローカルマシン、２…リモートマシン、３Ａ、３Ｂ…ルータ、４Ａ、４Ｂ…ＬＡＮ、５…ＷＡＮ

【図１】

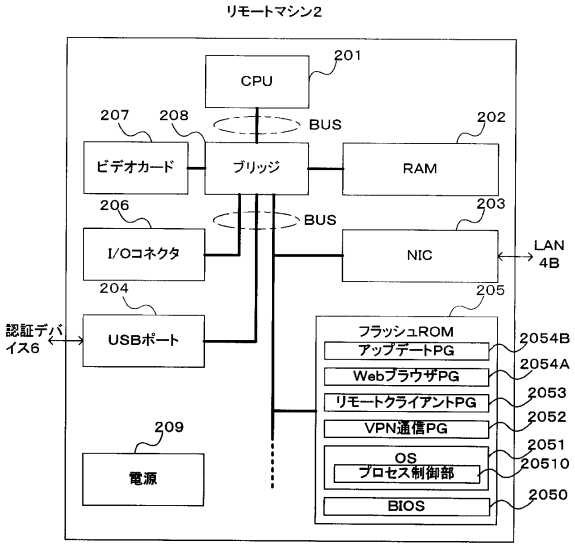


【図２】



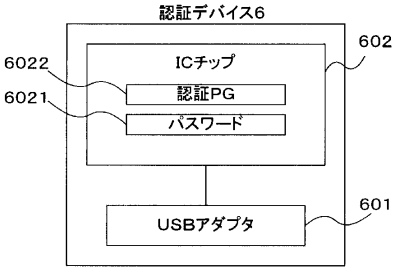
【図３】

図3



【図４】

図4



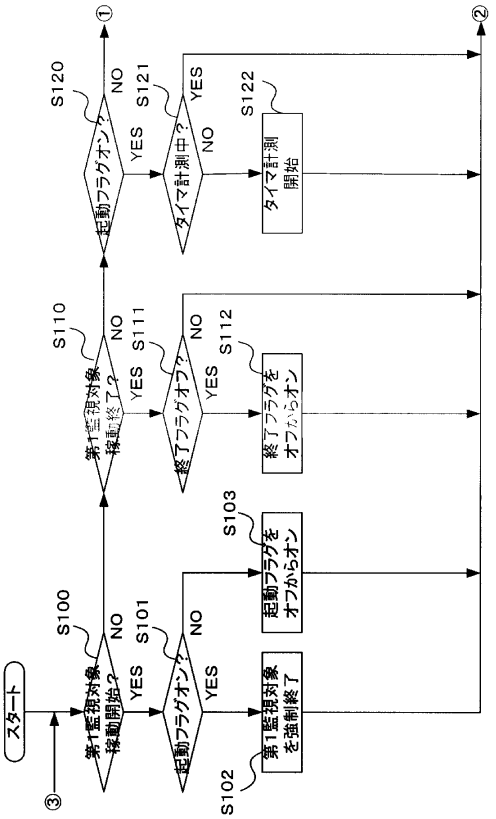
【図５】

図5



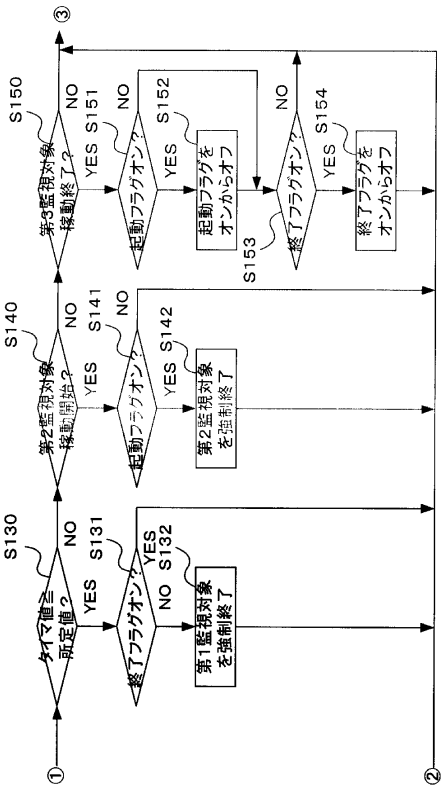
【図６】

図6



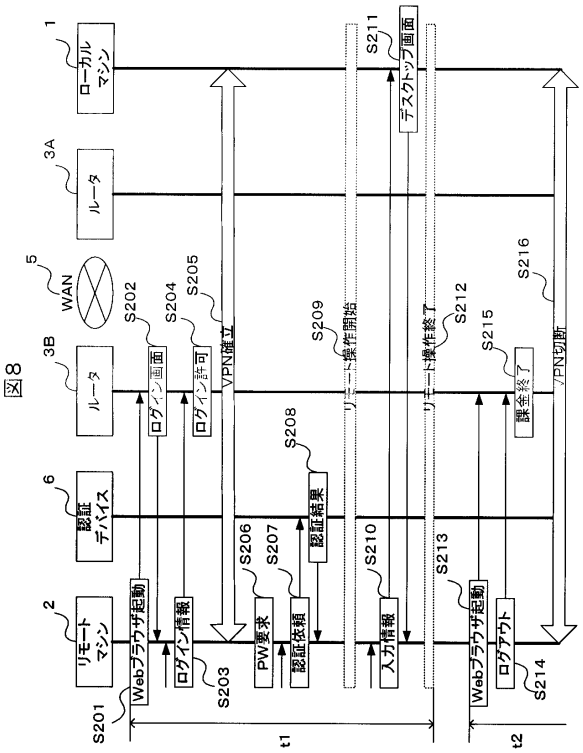
【図７】

図7



【図８】

図8


1
ローカルマシン
3A
ルータ
5
WAN
3B
ルータ
6
認証デバイス
2
リモートマシン
S201
Webブラウザ起動
S202
ログイン画面
S203
ログイン情報
S204
ログイン許可
S205
VPN確立
S206
PW要求
S207
認証依頼
S208
認証結果
S209
リモート操作開始
S210
入力情報
S211
デスクトップ画面
S212
リモート操作終了
S213
Webブラウザ起動
S214
ログアウト
S215
課金終了
S216
VPN切断
t1
t2

フロントページの続き

(72)発明者　小檜山　智久
神奈川県川崎市幸区鹿島田８９０番地　株式会社日立製作所　プラットフォームソリューション事業部内

審査官　殿川　雅也

(56)参考文献　特開２０００－０５７０２０（ＪＰ，Ａ）
特開２００１－００５６９４（ＪＰ，Ａ）
特開２００２－１０８６５８（ＪＰ，Ａ）
特開２００３－１４０７６６（ＪＰ，Ａ）
特開２００６－０４０２１９（ＪＰ，Ａ）
特開２００７－０１８２８２（ＪＰ，Ａ）
米国特許出願公開第２００４／００８８１４１（ＵＳ，Ａ１）
小山健治，やっと時代が追いついた？結局普及には至らない？　「新・シン・クライアントの実力」は本物か，COMPUTERWORLD Get Technology Right，日本，（株）ＩＤＧジャパン，２００５年　４月　１日，第2巻、第5号，第74頁乃至第79頁

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