(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2009-31896
(P2009-31896A)
(43)公開日　平成21年2月12日(2009.2.12)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/20	(2006.01)	G06F	15/00	330G	5B035
G06K 19/00	(2006.01)	G06K	19/00	T	5B285
G06K 19/10	(2006.01)	G06K	19/00	R	5J104
H04L 9/32	(2006.01)	H04L	9/00	673E	
G06F 13/00	(2006.01)	G06F	13/00	510A	

審査請求 未請求　請求項の数 11　ＯＬ　（全 21 頁）

(21)出願番号　特願2007-193028 (P2007-193028)
(22)出願日　平成19年7月25日 (2007.7.25)

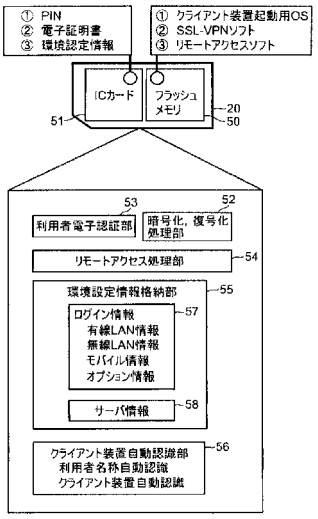
(71)出願人　000153443
株式会社日立情報制御ソリューションズ
茨城県日立市大みか町５丁目２番１号
(74)代理人　100074631
弁理士　高田　幸彦
(72)発明者　茅根　隆昭
茨城県日立市大みか町五丁目２番１号　株式会社日立情報制御ソリューションズ内
(72)発明者　松崎　健二
茨城県日立市大みか町五丁目２番１号　株式会社日立情報制御ソリューションズ内

最終頁に続く

(54)【発明の名称】リモートアクセスシステム、これに使用する補助記憶装置、リモートアクセス方法

(57)【要約】
【課題】利用シーンに応じた登録機能を有してクライアント装置を接続する時の設定の煩わしさから解放し、短時間での起動を実現することのできるようにする。
【解決手段】補助記憶媒体は、予め特定された利用シーン情報を格納しており、特定されたクライアント装置に接続されると、利用者名称情報、機器情報および接続経路情報を前記特定されたクライアント装置に特定し、当該クライアント装置から前記特定されたサーバへの接続を可能とする。
【選択図】図２

図　2



【特許請求の範囲】
【請求項１】
クライアント装置を起動する手段、該クライアント装置をサーバに通信手段を介してリモートアクセスさせる手段を備え、特定されたサーバにクライアント装置からリモートアクセスするときに、クライアント装置についての機器情報および前記クライアント装置から前記特定されたサーバに接続するための接続経路からなる環境設定情報を格納可能で、通常のジャケットのポケット等の小形収納手段に収納可能な小形の可搬型の補助記憶媒体であって、
予め特定された環境設定情報を格納しており、特定されたクライアント装置に接続されると、直ちに特定された環境設定情報を前記特定されたクライアント装置に特定し、当該クライアント装置から前記特定されたサーバへの接続を可能とすること
を特徴とする補助記憶媒体。
【請求項２】
クライアント装置を起動する手段、該クライアント装置をサーバに通信手段を介してリモートアクセスさせる手段を備え、特定されたサーバにクライアント装置からリモートアクセスするときに、クライアント装置についての利用者名称情報と、クライアント装置についての機器情報および前記クライアント装置から前記特定されたサーバに接続するための接続経路情報からなる利用シーン情報を格納可能で、通常のジャケットのポケット等の小形収納手段に収納可能な小形の可搬型の補助記憶媒体であって、
予め特定された利用シーン情報を格納しており、特定されたクライアント装置に接続されると、利用者名称情報、機器情報および接続経路情報を前記特定されたクライアント装置に特定し、当該クライアント装置から前記特定されたサーバへの接続を可能とすること
を特徴とする補助記憶媒体。
【請求項３】
クライアント装置を起動する手段、該クライアント装置をサーバに通信手段を介してリモートアクセスさせる手段を備えたシステムにおいて、クライアント装置の起動時に、クライアント装置のハードウェア属性情報（例えば、デバイス名称、ベンダＩＤ、プロダクトＩＤ等）から、クライアント装置に実装されているハードウェアを特定し、クライアント装置のハードウェアに合う制御ソフトを自動的に割当てることで、利用者によるクライアント装置ごとの制御ソフトのインストールを不要とすること
を特徴とする補助記憶媒体。
【請求項４】
クライアント装置を起動する手段、該クライアント装置をサーバに通信手段を介してリモートアクセスさせる手段を備え、特定されたサーバにクライアント装置からリモートアクセスするときに、クライアント装置についての利用者名称情報と、クライアント装置についての機器情報および前記クライアント装置から前記特定されたサーバに接続するための接続経路情報からなる環境設定情報を備えた利用シーン情報を格納可能で、通常のジャケットのポケット等の小形収納手段に収納可能な小形の可搬型の補助記憶媒体であって、
予め特定された利用シーン情報を格納しており、特定されたクライアント装置に接続されると、入力された利用認識情報が予め格納された利用者認識情報と一致すると、
前記特定された環境設定情報を前記特定されたクライアント装置に特定し、当該クライアント装置から前記特定されたサーバへの接続を可能とすること
を特徴とする補助記憶媒体。
【請求項５】
請求項１から４のいずれかにおいて、前記特定のクライアント装置は１台もしくは複数台であって、接続されたクライアント装置から前記サーバへの接続が直ちになされることを特徴とする補助記憶媒体。
【請求項６】
請求項１から４のいずれかにおいて、クライアント装置に接続されると当該クライアント装置が予め特定されたクライアント装置に一致するかを判定する判定手段を備えること

を特徴とする補助記憶媒体。
【請求項７】
請求項６において、前記判定する手段は、予め定められた判定順位に従って、判定することを特徴とする補助記憶媒体。
【請求項８】
クライアント装置を起動する手段、該クライアント装置をサーバにリモートアクセスさせる手段を格納したフラッシュメモリと、特定されたサーバにクライアント装置からリモートアクセスするときに、クライアント装置についての機器情報および前記クライアント装置から前記サーバへの接続するための接続経路情報からなる環境設定情報並びに利用者名称情報からなる利用者による利用シーン情報を格納可能な耐タンパ性媒体部とからなり、通常のジャケットのポケット等の小形の収納手段に収納可能な小形の可搬型の補助記憶媒体であって、
前記耐タンパ性媒体部は、予め特定された利用シーン情報を格納しており、クライアント装置が接続されると当該クライアント装置が予め特定されたクライアント装置に一致するかを判定する判定手段、利用者認識情報を入力する手段および入力された利用者認識情報が予め特定された利用者認識情報と一致するかを判定する手段を備え、利用者認識情報が一致すると特定された利用者認識情報および環境設定情報を前記特定されたクライアント装置に特定し、当該クライアント装置から前記特定されたサーバへの接続を可能とすること
を特徴とする補助記憶媒体。
【請求項９】
請求項１から８のいずれかにおいて、前記補助記憶媒体を用いたリモートアクセスシステム。
【請求項１０】
クライアント装置を起動する手段、該クライアント装置をサーバに通信手段を介してリモートアクセスさせる手段を備え、特定されたサーバにクライアント装置からリモートアクセスするときに、クライアント装置についての利用者名称情報と、クライアント装置についての機器情報および前記クライアント装置から前記特定されたサーバに接続するための接続経路情報からなる環境設定情報を備えた利用シーン情報を格納可能で、通常のジャケットのポケット等の小形収納手段に収納可能な小形の可搬型の補助記憶媒体を用いたリモートアクセス方法において、
前記補助記憶媒体に予め特定された利用シーン情報を格納し、前記補助記憶媒体を特定されたクライアント装置に接続し、入力された利用認識情報が予め格納された利用認識情報と一致するかを判定し、一致すると、前記特定された利用者名称情報および環境設定情報を前記特定されたクライアント装置に特定し、当該クライアント装置から前記特定されたサーバへの接続を可能とすること
を特徴とする補助記憶媒体を用いたリモートアクセス方法。
【請求項１１】
請求項１０において、前回に使用したクライアント装置について優先した、特定されたクライアント装置として接続し、利用者名称情報および環境設定情報を特定することを特徴とする補助記憶媒体を用いたリモートアクセス方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ネットワークシステムにおけるリモートアクセスシステム、これに使用する補助記憶装置、リモートアクセス方法、補助記憶装置の使用方法、補助記憶装置の情報格納方法に関する。
【背景技術】
【０００２】
ブロードバンド環境の急速な普及に伴い、企業では自宅をはじめとする外部の複数の拠

点から社内ネットワークシステムへリモートアクセスし、データやソフトを利用するといったシーン（場面）が急速に増加している。

【０００３】

その一方で機密情報や個人情報を格納したクライアント装置（パソコン）を持ち歩くことにより、クライアント装置の盗難・紛失など情報漏洩のリスクは拡大しており、多くの企業がクライアント装置の外部持ち出しを禁止している状況にある。

【０００４】

現在、企業における情報漏洩対策として注目されているのが、シンクライアントシステムである。シンクライアントシステムは、クライアントには最低限の機能しか持たない低価格なコンピュータを配し、サーバ側でアプリケーションソフトやファイルなどの資源を管理するシステムで、メンテナンスなど管理・運用コストを削減できるということで利用されてきた。最近では、クライアントにＨＤＤなど記憶装置を使用せず、データを保有しない特徴が、情報漏洩対策として注目されている。

【０００５】

特許文献１には、一対のコンピュータにおける一方のコンピュータと他方のコンピュータとを少なくとも無線媒体を介させて接続されているネットワークで接続したリモートアクセスシステムであって、上記一方のコンピュータは、リモートアクセスを許可するためのアクセスコードを登録してあるとともに、可搬性のある着脱可能な不揮発性メモリを接続可能であり、上記アクセスコードを所定の方法で暗号化して同不揮発性メモリに記憶し、上記他方のコンピュータは、上記不揮発性メモリを装着可能であるとともに、同不揮発性メモリを装着したときに、上記暗号化されたアクセスコードを解読し、同解読したアクセスコードを使用して上記一方のコンピュータにアクセス可能とすることを特徴とするリモートアクセスシステムが記載されている。

【０００６】

この特許文献には、更に上記不揮発性メモリは、スマートメディアであること、あるいはＵＳＢメモリであることが記載されている。

【０００７】

特許文献２には、パーソナルコンピュータ上の構成プログラムが、シンクライアント装置の、ネットワーク設定を含む構成データの作成でユーザを支援し、構成データを含むＸＭＬファイルを生成し、ＸＭＬファイルを可搬型媒体に書き込み、次に可搬型媒体をシンクライアント装置に接続し、シンクライアント装置は、可搬型媒体を検出し、ＸＭＬファイルから構成データを自動的にロードすることが記載されている。

【０００８】

特許文献３には、暗号化された電話番号を記憶する第１の記憶手段と、暗号化されたＩＤ及びパスワードを記憶する第２の記憶手段と、前記第１の記憶手段に記憶された電話番号を復号化すると共に、前記第２の記憶手段に記憶されたＩＤ及びパスワードを復号化する復号化手段と、前記復号化手段により復号化された電話番号先にダイアルし、前記復号化手段により復号化されたＩＤ及びパスワードを送信する通信手段と、を備えることを特徴とする通信端末が記載されている。

【０００９】

特許文献４には、双方向のデータ通信を行う複数の通信装置を含むデータ通信システムであって、前記複数の通信装置のいずれかに読み取られ、通信相手となる相手側通信装置のアドレス情報、前記相手側通信装置に固有の暗号鍵で生成された電子署名、該電子署名に対応する認証用情報を記録したカード状記録媒体と、前記カード状記録媒体の記録情報を読み取った通信装置を通じて当該記録情報を取得するとともに、前記アドレス情報により特定される相手側通信装置の復号鍵で前記電子署名を復号化して前記認証用情報と照合することにより、前記通信装置が前記相手側通信装置に対して行うデータ通信の正当性を判定する認証手段と、を有することを特徴とするデータ通信システムが記載されている。

【００１０】

【特許文献１】特開２００５－８５１６９号公報

【特許文献２】特開２００５－２１６２９２号公報
【特許文献３】特開２００３－１０８５２５号公報
【特許文献４】特開平１１－２５２０６８号公報
【発明の開示】
【発明が解決しようとする課題】
【００１１】
上述のように、従来のリモートアクセスシステムは、情報漏洩対策を特に考慮して設計されており、利用者についての確実な認証を行う手段、方法が提供されている。また、シンクライアント装置にファイルを書き込んだ可搬型媒体を組み込んで構成データを自動的にロードする手段、方法が提供されている。リモートアクセスシステムの構築に当っては、利用者が安心して、どこからでも、誰でも簡単にサーバに接続でき、容易に環境設定できること、すなわち使い勝手がよいことが求められて来ている。
【００１２】
本発明は、かかる点に鑑み利用シーンに応じた登録機能を有してクライアントクライアント装置を接続する時の設定の煩わしさから解放し、短時間での起動を実現することのできるリモートアクセスシステム、これに使用する補助記憶装置、例えばＵＳＢ（Universal Serial Bus）端子およびリモートアクセス方法を提供することを目的とする。
【００１３】
本発明は、更に上述の機能によって補助記憶装置の使用方法、補助記憶装置の情報格納方法およびシンクライアント装置のネットワーク設定方法を提供することを目的とする。
【課題を解決するための手段】
【００１４】
本発明は、クライアント装置を起動する手段、該クライアント装置をサーバに通信手段を介してリモートアクセスさせる手段を備え、特定されたサーバにクライアント装置からリモートアクセスするときに、クライアント装置についての機器情報および前記クライアント装置から前記特定されたサーバに接続するための接続経路からなる環境設定情報を格納可能で、通常のジャケットのポケット等の小形収納手段に収納可能な小形の可搬型の補助記憶媒体であって、
予め特定された環境設定情報を格納しており、特定されたクライアント装置に接続されると、直ちに特定された環境設定情報を前記特定されたクライアント装置に特定し、当該クライアント装置から前記特定されたサーバへの接続を可能とすること
を特徴とする補助記憶媒体を提供する。
【００１５】
本発明は、クライアント装置を起動する手段、該クライアント装置をサーバに通信手段を介してリモートアクセスさせる手段を備え、特定されたサーバにクライアント装置からリモートアクセスするときに、クライアント装置についての利用者名称情報と、クライアント装置についての機器情報および前記クライアント装置から前記特定されたサーバに接続するための接続経路情報からなる利用シーン情報を格納可能で、通常のジャケットのポケット等の小形収納手段に収納可能な小形の可搬型の補助記憶媒体であって、
予め特定された利用シーン情報を格納しており、特定されたクライアント装置に接続されると、利用者名称情報、機器情報および接続経路情報を前記特定されたクライアント装置に特定し、当該クライアント装置から前記特定されたサーバへの接続を可能とすること
を特徴とする補助記憶媒体を提供する。
【００１６】
本発明は、クライアント装置を起動する手段、該クライアント装置をサーバに通信手段を介してリモートアクセスさせる手段を備え、特定されたサーバにクライアント装置からリモートアクセスするときに、クライアント装置についての利用者名称情報と、クライアント装置についての機器情報および前記クライアント装置から前記特定されたサーバに接続するための接続経路情報からなる環境設定情報を備えた利用シーン情報を格納可能で、通常のジャケットのポケット等の小形収納手段に収納可能な小形の可搬型の補助記憶媒体

であって、
予め特定された利用シーン情報を格納しており、特定されたクライアント装置に接続されると、入力された利用認識情報が予め格納された利用者認識情報と一致すると、
前記特定された環境設定情報を前記特定されたクライアント装置に特定し、当該クライアント装置から前記特定されたサーバへの接続を可能とすること
を特徴とする補助記憶媒体を提供する。
【００１７】
本発明は、更に、補助記憶媒体において、前記特定のクライアント装置は１台もしくは複数台であって、接続されたクライアント装置から前記サーバへの接続が直ちになされることを特徴とする。
【００１８】
本発明は、更に、補助記憶媒体において、クライアント装置に接続されると当該クライアント装置が予め特定されたクライアント装置に一致するかを判定する判定手段を備えることを特徴とする。
【００１９】
本発明は、更に、補助記憶媒体において、前記判定する手段は、予め定められた判定順位に従って、判定することを特徴とする。
【００２０】
本発明は、クライアント装置を起動する手段、該クライアント装置をサーバにリモートアクセスさせる手段を格納したフラッシュメモリと、特定されたサーバにクライアント装置からリモートアクセスするときに、クライアント装置についての機器情報および前記クライアント装置から前記サーバへの接続するための接続経路情報からなる環境設定情報並びに利用者名称情報からなる利用者による利用シーン情報を格納可能な耐タンパ性媒体部とからなり、通常のジャケットのポケット等の小形の収納手段に収納可能な小形の可搬型の補助記憶媒体であって、
前記耐タンパ性媒体部は、予め特定された利用シーン情報を格納しており、クライアント装置が接続されると当該クライアント装置が予め特定されたクライアント装置に一致するかを判定する判定手段、利用者認識情報を入力する手段および入力された利用者認識情報が予め特定された利用者認識情報と一致するかを判定する手段を備え、利用者認識情報が一致すると特定された利用者認識情報および環境設定情報を前記特定されたクライアント装置に特定し、当該クライアント装置から前記特定されたサーバへの接続を可能とすること
を特徴とする補助記憶媒体を提供する。
【００２１】
本発明は、更に、リモートアクセスシステムにおいて、前記補助記憶媒体を用いることを特徴とする。
【００２２】
本発明は、クライアント装置を起動する手段、該クライアント装置をサーバに通信手段を介してリモートアクセスさせる手段を備え、特定されたサーバにクライアント装置からリモートアクセスするときに、クライアント装置についての利用者名称情報と、クライアント装置についての機器情報および前記クライアント装置から前記特定されたサーバに接続するための接続経路情報からなる環境設定情報を備えた利用シーン情報を格納可能で、通常のジャケットのポケット等の小形収納手段に収納可能な小形の可搬型の補助記憶媒体を用いたリモートアクセス方法において、
前記補助記憶媒体に予め特定された利用シーン情報を格納し、前記補助記憶媒体を特定されたクライアント装置に接続し、入力された利用認識情報が予め格納された利用認識情報と一致するかを判定し、一致すると、前記特定された利用者名称情報および環境設定情報を前記特定されたクライアント装置に特定し、当該クライアント装置から前記特定されたサーバへの接続を可能とすること
を特徴とする補助記憶媒体を用いたリモートアクセス方法を提供する。

【００２３】
本発明は、更に、リモートアクセス方法において、前回に使用したクライアント装置について優先した、特定されたクライアント装置として接続し、利用者名称情報および環境設定情報を特定することを特徴とする補助記憶媒体を用いることを特徴とする。
【発明の効果】
【００２４】
本発明によれば、利用者に煩わしい操作を行わせることなく、容易に環境設定させ、使い勝手をよくすることのできるリモートアクセスシステム、これに使用する補助記憶装置およびリモートアクセス方法を提供することができる。
【００２５】
本発明は、更に上述の機能によって補助記憶装置の使用方法、補助記憶装置の格納方法およびシンクライアント装置のネットワーク設定方法を提供することができる。
【００２６】
具体的には、本発明は、使い勝手向上について次のような効果を有する。
ａ）使用時の環境設定が簡単
１）利用シーンに応じた登録ができる。
環境設定情報を備えた利用シーン情報は、複数登録できるため、会社，自宅，出先など、各利用シーンにおいて、毎回設定変更することなく使用できる。
２）設定の煩わしさから解放できる。
シンクライアント装置を接続するＬＡＮ（Local Area Net Work）にてＤＨＣＰ（Dynamic Host Configuration Protcol）を使用すると、１つの利用シーン情報で、使用可能とすることができる。
３）クライアント装置構成を自動認識することができる。
クライアント装置の構成を自動認識して自動的にクライアント装置のログイン情報を取得するため、利用者は特別な機器の設定を行う必要がない。
ｂ）短時間での起動，停止
すばやい起動，停止ができ、使いたいとき直ちに使用、止めたいときに速やかに停止することができる。
【発明を実施するための最良の形態】
【００２７】
以下、本発明の実施例を図面に基づいて説明する。
【実施例】
【００２８】
利用シーン情報として、サーバ情報とログイン情報を分け、複数定義した実施例について記載する。
【００２９】
図１は、本発明の実施例であるリモートアクセスシステム１００が適用されるデータ通信システム１の概要を示す。本実施例においては、ＵＳＢ端子（ＵＳＢデバイス）などの着脱可能な補助記憶装置が使用され、ＩＣカードなどの耐タンパ性を備えた媒体が使用され、ＰＣ（Personal Computer）などのモニタなど出力装置、キーボードなど入力装置、外部との通信装置、各種端末などのクライアント装置が使用し得るが以下の説明ではＵＳＢ端子、ＩＣカード、クライアント装置を例に取って説明する。しかしながら、本発明はこれらの実施例には限定されない。
【００３０】
データ通信システム１は、可搬型媒体としての補助記憶装置２０の装着機構を備えた複数のクライアント装置１０と、各クライアント装置１０からのリモートアクセスを受け付けるリモートアクセスサーバ３０および情報サーバ３１とを含み、各クライアント装置１０とリモートアクセスサーバ３０および情報サーバ３１とはネットワークシステム３４およびネットワークを構成するネットワークシステム４０に接続されたＬＡＮ３３によって結ばれる。この接続によって双方向通信が可能とされる。なお、補助記憶装置は、ＵＳＢ

メモリとして知られており、ＵＳＢポートを用いてデータを転送する小型の記憶装置の一種である。

【００３１】

また、ＬＡＮ３３には、管理者クライアント装置３７およびＳＳＬ－ＶＰＮ（Secure Socket Layer Virtual Private Network）装置３８が接続される。

【００３２】

クライアント装置１０は、通信制御部１１、データ処理部１２およびデータ入出力部１４を備え、リモート操作プログラム、一時記録プログラムを含み、オペレーティングシステム（ＯＳ）下で上述のプログラムを読み込み実行するように構成される。データ入出力部１４は、補助記憶装置２０のデータ入出力部２４との間で情報の授受を行う。

【００３３】

補助記憶装置２０は通常のジャケット等の小形収納手段に収納可能な小形の、例えば数ｃｍの大きさの可搬型として形成され、データ処理，格納部２１、認証処理部２２、クライアント装置構成自動認識部２３およびデータ入出力部２４を有して、クライアント装置１０に装着可能とされる。上述のように、データ入出力部２４とデータ入出力部１４は情報の授受が可能とされる。補助記憶装置２０の形状及びハードウェア構成は公知のものが援用可能である。補助記憶装置２０には、ＣＰＵ（処理部）、ＲＯＭおよびＲＡＭ等のデータ格納部２１を形成する記憶部、Ｉ／Ｏポートを有するカード部がカード上に固定されている。

【００３４】

リモートアクセスサーバ３０および情報サーバ３１（双方を合わせてサーバという場合があり、それらに格納された情報をサーバ情報として扱う。）は特定の拠点、例えば社内に設置される。点線４０が社内と社外を分ける環境分割線であり、社外例すなわち外部側が環境１とされ、社内側すなわち内部側が環境２とされる。環境とは、コンピュータやネットワークを構成するハードウェアやソフトウェアの組み合わせと、それぞれの状態や設定の総体を現わす用語として使用されている。本実施例では、環境分割線によって全体の環境を２つの環境１，２に分割し、一方においてログイン情報の設定される環境側とし、他方においてサーバ情報の設定される環境側２としている。

【００３５】

リモートアクセスサーバ３０は、クライアント装置１０からリモートアクセスがあった時に、認証処理を行う機能を有して、所定の暗号アルゴリズムに基づいた暗号化及び復号化を行い、補助記憶装置２０との間で相互認証を行う。

【００３６】

情報サーバ３１は、文書、図面等の情報３６を格納しており、リモートアクセスサーバ３０でアクセスの正当性が確認された情報を検索して提供することを行う。このため、複数種のデータベース検索処理を行うデータベースサーバを含んで構成される。これらのサーバ３０，３１は社内配設のＬＡＮ３３に接続される。

【００３７】

ネットワークシステム３４は、インターネットなどの通信欄であり、無線通信網、公衆網が含まれる。後述するＳＳＬ－ＶＰＮの利用によってネットワークに暗号化された仮想回線が構築され、遠隔の地にあるサーバ３０，３１に他の拠点にあるクライアント装置１０からリモートアクセスされる。

【００３８】

通信制御部１１は、リモートアクセスサーバ３０とのデータ通信をネットワークシステム３４を介して行う。データ処理部１２は、後述するように補助記憶装置２０に格納された環境設定に基づいてデータ通信を制御処理する。

【００３９】

補助記憶装置２０の認証処理部２２は、記録情報の暗号化及び受信情報の復号化を行って、リモートアクセスサーバ３０との間の相互認証を行う。

【００４０】

データ格納部２１には、利用者認証用の暗号情報（クライアントの公開鍵，自己の秘密鍵等）、補助記憶装置２０の所有者を表す利用者名称、ユーザのパスワード、リモートアクセスサーバ３０の通信装置のＩＰアドレス、情報サーバ３１に固有の暗号鍵で生成された電子証明書が記録されている。クライアント装置構成自動認識部２３は、利用者が使用して補助記憶装置２０をクライアント装置１０に装着した時に、その使用したクライアント装置１０の利用者名称情報（クライアント名称情報ともいう）、クライアント装置構成を示す機器情報をＩＰアドレスを含めて自動認識する。この自動認識のために特別な機器の設定を必要としない。

【００４１】

このように、利用者認識情報が予め格納された利用者情報と一致した時にサーバに接続可能とされ、電子認証手段を備える。

【００４２】

リモートアクセスサーバ３０またはＳＳＬ－ＶＰＮ（Secure Socket Layer Virtual Private Network）装置３８が備える認証処理部３５は、認証完了済みの補助記憶装置２０を具備したクライアント装置１０から情報アクセス要求を受け付ける。この情報アクセス要求には、補助記憶装置２０の記録情報のうち、電子証明書及び情報サーバ３１のＩＰアドレスが含まれる。認証処理部３５は、情報アクセス要求を解析し、ＩＰアドレスによって複数の情報サーバから特定できる情報サーバ３１から復号鍵を取得し、取得した復号鍵を用いて電子証明書を復号化する。復号化結果と認証用情報とを照合することで、クライアント装置１０の情報サーバ３１に対する正当性を判定する。なお、ＳＳＬ－ＶＰＮは、暗号化にＳＳＬを利用するＶＰＮ技術として知られている。

【００４３】

認証処理部３５は、判定結果をクライアント装置１０へ送信するとともに、判定結果に基づいて、クライアント装置１０とリモートアクセスサーバ３０と情報サーバ３１間の通信路を確立する。

【００４４】

図２は、補助記憶装置２０の詳細を示す。補助記憶装置２０は、フラッシュメモリ５０および耐タンパ性媒体部５１を備える。フラッシュメモリ５０は、１）クライアント装置起動用ＯＳ、２）ＳＳＬ－ＶＰＮソフト、３）リモートアクセスソフトを備える。耐タンパ性媒体部５１には、１）ＰＩＮ（Personal Identification Number個人用識別番号）、２）電子証明書、３）環境設定情報が格納される。

【００４５】

以上の構成によって補助記憶装置２０には、具体的には、暗号化，復号化処理部５２、利用者電子認証部５３、リモートアクセス処理部５４（図１のデータ処理、格納部２１に対応）、環境設定情報格納部５５（図１のデータ処理、格納部２１に対応）およびクライアント装置自動認識部５６（図１におけるクライアント装置構成自動認識部２３に対応）が構成される。

【００４６】

（１）情報漏洩対策

利用者電子認証部５３は、利用者の認証を次の２段階で行う。

・クライアント装置へのログオン時

・ＳＳＬ－ＶＰＮ装置へのログオン時

ｉ）クライアント装置のクライアントへのログオン時

起動時、最大１６文字のＰＩＮを入力する。入力されたＰＩＮは、耐タンパ性媒体部５１に登録されたものと一致した場合のみ、クライアント装置１０へログオン可能となる。

ｉｉ）ＳＳＬ－ＶＰＮ装置３８へのログオン時

ＳＳＬ－ＶＰＮ装置３８と電子証明書による相互認証機能を備える。電子証明書、ＳＳＬ－ＶＰＮ装置３８には一般の製品が使用可能とされ、暗号化、復号化処理部５２が形成される。

電子証明書は、システム管理者が管理者クライアント装置３７を介して発行し、補助記憶装置２０およびＳＳＬ－ＶＰＮ装置３８に登録する。リモートアクセスでの情報漏洩防止部（図示せず）は、ＳＳＬ－ＶＰＮを使用して対処し、社外からのリモートアクセスに対する情報漏洩防止機能を備える。

ＰＩＮおよび電子証明書は、耐タンパ性に優れた耐タンパ性媒体部５１に格納される。

【００４７】

（２）使い勝手

補助記憶装置２０は、リモートアクセス処理部５４、環境設定情報格納部５５およびクライアント装置自動認識部５６を備え、環境設定情報格納部５５はログイン情報５７およびサーバ情報５８を格納する。リモートアクセス処理部５４は、サーバ３０，３１にリモートアクセスしてサーバを遠隔操作する。クライアント装置自動認識部５６は、補助記憶装置２０がクライアント装置１０に装着された時に、利用者名称および当該クライアント装置１０のクライアント装置の機器構成およびＩＰアドレスを自動認識し、使用のクライアント装置のログイン情報を取得することができ、利用者に外部から利用者名称クライアント装置の機器構成およびＩＰアドレスの入力を要求しない。

【００４８】

次に、図３－図１３を用いて、初回に設定するＰＩＮ入力、サーバ情報設定、ログイン情報設定について説明する。

【００４９】

図３は、ＰＩＮ入力、サーバ情報設定、ログイン情報設定のフローを示す。利用シーンを規定する環境としてログイン情報設定がなされ、利用シーンを規定する環境２としてサーバ情報設定がなされる。

【００５０】

図３において、ＰＩＮ入力し（Ｓ１１）、ログイン設定し（Ｓ１２）、サーバ登録（Ｓ１３）およびログイン情報設定（Ｓ１４）を行い、サーバ登録してサーバ情報設定（Ｓ１５）を行う。ログイン情報設定には、有線ＬＡＮ設定（Ｓ１６）、無線ＬＡＮ設定（移動無線設定を含む。）（Ｓ１７）、モバイル設定（Ｓ１８）を行う。ログイン情報設定してオプション設定（Ｓ１９）を行う。

【００５１】

図４は、ＰＩＮ入力を行う画面設定を示す。この画面は、立ち上がり画面で、パスワード（ＰＩＮ）を入力し、リモートアクセスサーバへログインしたり、ログイン用の設定へ進む画面である。後述するログイン情報が設定されており、立ち上げたクライアント装置１０よりリモートアクセスサーバに接続できる情報が取得できた場合には、ログインできる接続名称６１が表示される。使用するログイン名称が表示されている場合は、該当のログイン名称をプルダウンメニューから選択し、ＰＩＮ入力後、〔ログイン〕ボタンを押す。

【００５２】

図５は、ログイン設定を行う画面である。ログイン情報を図５の画面に表示する。ログイン設定は、接続するサーバ情報の設定と、ログイン情報の設定に分かれる。サーバ登録およびログイン情報設定を行う。

【００５３】

図６は、サーバ登録を行う画面である。接続するサーバの情報を設定する。

図７は、サーバ情報設定を行う画面である。図７において、接続するサーバの名称をサーバ名称欄に入力する。サーバに接続するアプリケーションを選択する。図７には、ＩＣＡクライアント、ＩＣＡクライアント（Ｗｅｂインタフェース）、ＲＤＰクライアントが表示してある。

接続するサーバの情報を設定する。接続するサーバのＩＰアドレスまたはＵＲＬで入力する。

ＳＳＬ－ＶＰＮについて、ＳＳＬ－ＶＰＮ装置を使用する場合にＳＳＬ－ＶＰＮ装置のＩＰアドレスを入力する。ＳＳＬ－ＶＰＮ装置を使用する場合、接続するＳＳＬ－ＶＰＮ

装置を選択する。図７を使用して、環境２としての環境設定情報が取得され、格納される。

【００５４】

図８で、ログイン情報を設定する。

ＰＩＮ入力画面（図４）での選択や、ログイン設定画面（図５）に表示されるログイン名称を入力する。接続するログイン名称をログイン名称欄に入力する。

利用するネットワークシステムの情報を設定する。

接続するサーバを設定する。図８を利用して、環境１としての環境設定情報が取得され、格納される。オプション設定によって、画面表示サイズ、Num Lock（ナムロックキー）の設定を行う。オプション設定画面を図９に示す。

図８のログイン情報設定の、ネットワーク設定にて有線ＬＡＮを選択した場合、図１０に示す画面が表示される。ＩＰアドレスを自動的に取得するか、あるいはＩＰアドレスを指定する。

【００５５】

ＤＮＳ（Domain Name System）を自動的に取得するか、あるいはＤＮＳを指定する。ＰＰｏＥ（PPP over Ethernet（登録商標） PPPの機能をEthernet（登録商標）を通して利用するためのプロトコル）設定を行う。

プロキシ設定を行う。

図８のログイン情報設定の、ネットワーク設定にて無線ＬＡＮを選択した場合、図１１に示す画面が表示される。ＩＰアドレスを自動的に取得するか、あるいはＩＰアドレスを指定する。

ＤＮＳを自動的に取得するか、あるいはＤＮＳを指定する。

ＥＳＳＩＤ（Extended Service Set Identifier）およびＷＥＰ（Wired Equivalent Privacy）ＫＥＹを入力する。

プロキシ設定する。

【００５６】

図８のログイン情報設定の、ネットワーク設定にてモバイルを選択した場合、図１２に示す画面が表示される。

通信カードを選択し、ダイヤルアップ情報を設定する。図８のログイン情報設定の、オプション設定にて〔オプション設定〕を選択した場合、図１３に示す画面が表示される。

画面サイズの設定、ウィンドウの色数の設定、Num Lockキーの設定を行う。

【００５７】

図３において、リモートアクセスサーバログインを行う（Ｓ２０）。

以上説明した画面を使用してサーバ情報およびログイン情報を、環境設定情報として登録する。環境設定情報は、複数登録することができる。この結果、会社、自宅、出先など、各利用シーンに合わせて毎回設定変更することなく補助記憶装置２０が使用可能になる。ログイン情報、サーバ情報を設定することによって使用可能になる。ＬＡＮは、自動認識される。

【００５８】

もう一つの実施例として、１つのログインに対し複数の接続経路情報を割付け、クライアント装置のハードウェアを自動認識して、クライアント装置からサーバへの接続を可能とする例を、図７、図９－図１７を用いて説明する。

【００５９】

図１４は、ＰＩＮ入力を行う画面設定を示す。この画面は、立ち上がり画面で、パスワード（ＰＩＮ）を入力し、リモートアクセスサーバへログインしたり、ログイン用の設定へ進む画面である。後述するログイン情報が設定されており、立ち上げたクライアント装置１０よりリモートアクセスサーバに接続できる情報が取得できた場合には、ログインできる接続名称６２が表示される。使用するログイン名称が表示されている場合は、該当のログイン名称をプルダウンメニューから選択し、ＰＩＮ入力後、〔ログイン〕ボタンを押す。

【００６０】
図１５は、ログイン設定を行う画面である。ログイン情報を図１５の画面に表示する。ログイン設定は、接続するサーバ情報の設定と、ログイン情報の設定に分かれる。サーバ登録およびログイン情報設定を行う。
図１６は、サーバ登録を行う画面である。接続するサーバの情報を設定する。
【００６１】
図７は、サーバ情報設定を行う画面である。図７において、接続するサーバの名称をサーバ名称欄に入力する。サーバに接続するアプリケーションを選択する。図７には、ＩＣＡクライアント、ＩＣＡクライアント（Ｗｅｂインタフェース）、ＲＤＰクライアントが表示してある。
【００６２】
接続するサーバの情報を設定する。接続するサーバのＩＰアドレスまたはＵＲＬで入力する。
ＳＳＬ－ＶＰＮについて、ＳＳＬ－ＶＰＮ装置を使用する場合にＳＳＬ－ＶＰＮ装置のＩＰアドレスを入力する。ＳＳＬ－ＶＰＮ装置を使用する場合、接続するＳＳＬ－ＶＰＮ装置を選択する。図７を使用して、環境２としての環境設定情報が取得され、格納される。
【００６３】
図１７で、ログイン情報を設定する。
ＰＩＮ入力画面（図１４）での選択や、ログイン設定画面（図１５）に表示されるログイン名称を入力する。接続するログイン名称をログイン名称欄に入力する。
利用するネットワークシステムの情報を設定する。
接続するサーバを設定する。図１７を利用して、環境１としての環境設定情報が取得され、格納される。オプション設定によって、画面表示サイズ、Num Lock（ナムロックキー）の設定を行う。オプション設定画面を図９に示す。
図１７のログイン情報設定の、ネットワーク設定にて有線ＬＡＮを選択した場合、図１０に示す画面が表示される。ＩＰアドレスを自動的に取得するか、あるいはＩＰアドレスを指定する。
ＤＮＳ（Domain Name System）を自動的に取得するか、あるいはＤＮＳを指定する。ＰＰＰｏＥ（PPP over Ethernet（登録商標） PPPの機能をEthernet（登録商標）を通して利用するためのプロトコル）設定を行う。
プロキシ設定を行う。
図１７のログイン情報設定の、ネットワーク設定にて無線ＬＡＮを選択した場合、図１１に示す画面が表示される。ＩＰアドレスを自動的に取得するか、あるいはＩＰアドレスを指定する。
【００６４】
ＤＮＳを自動的に取得するか、あるいはＤＮＳを指定する。
ＥＳＳＩＤ（Extended Service Set Identifier）およびＷＥＰ（Wired Equivalent Privacy）ＫＥＹを入力する。
プロキシ設定する。
図１７のログイン情報設定の、ネットワーク設定にてモバイルを選択した場合、図１２に示す画面が表示される。
通信カードを選択し、ダイヤルアップ情報を設定する。図１７のログイン情報設定の、オプション設定にて〔オプション設定〕を選択した場合、図１３に示す画面が表示される。
画面サイズの設定、ウィンドウの色数の設定、Num Lockキーの設定を行う。
【００６５】
図３において、リモートアクセスサーバログインを行う（Ｓ２０）。
以上説明した画面を使用してサーバ情報およびログイン情報を、環境設定情報として登録する。１つのサーバ情報を指定した接続名称６２に対し、有線ＬＡＮ設定情報、無線Ｌ

ＡＮ設定情報、モバイル設定情報などの各接続経路情報を複数割付けることができる。この結果、会社、自宅、出先など、各利用シーンに合わせて使用するクライアント装置のハードウェアを自動認識し、対応する制御ソフトを割当てて動作可能とすることで、毎回設定変更することなく補助記憶装置２０が使用可能になる。

【００６６】

【表１】

表1 設定情報と利用シーン情報

#	分類	設定情報	毎回・一時	利用シーン情報
1	ｻｰﾊﾞ情報	ｻｰﾊﾞ情報	初回のみ設定すれば再定義不要	社内、社外とも再利用可能
2	SSL-VPN装置情報	SSL-VPN装置ｱﾄﾞﾚｽ	初回のみ設定すれば再定義不要	社外からのみ再利用
3	接続(経路)情報	有線LAN情報	有線LAN使用時の初回のみ不要	社内・自宅などLANがあり、DHCP使用時(Ipaddr自動設定)に再利用可能
4		無線LAN情報	無線LAN使用時の初回のみ不要	社内・自宅など無線LANがあり、DHCP使用時(Ipaddr自動設定)に再利用可能
5		移動無線情報	移動無線使用時の初回のみ不要	移動無線使用時(型式が同じ場合のみ)に再利用可能
6	ｸﾗｲｱﾝﾄ装置(PC)情報	ClinetのKeyBoard (Numlockなど)	初回のみ設定すれば再定義不要	同じPC使用時に再利用可能
7		ﾓﾆﾀ (XGA/SXGAなど)	初回のみ設定すれば再定義不要	同じPC使用時に再利用可能

【００６７】

設定情報と再度利用する場面を示す利用シーン情報の関係は表１に示す通りとなる。表１に示すように、サーバ情報、ＳＳＬ－ＶＰＮ装置情報、接続、すなわち経路情報、クライアント装置情報共に、初回のみに設定すれば再定義を要することなく各利用者シーンにおいて直ちに利用可能となる。利用シーン情報については表１に示す通りであり、登録した利用者名称（クライアント名称）において特定されたクライアント装置を使用して特定の地点で、特定の接続（経路）で補助記憶装置２０を装着するのみで直ちに当該クライアント装置から特定のサーバ装置３０、３１へのリモートアクセスが可能となる。

【００６８】

従って、補助記憶媒体２０は、クライアント装置を起動する手段、該クライアント装置をサーバに通信手段を介してリモートアクセスさせる手段を備え、特定されたサーバにクライアント装置からリモートアクセスするときに、クライアント装置についての機器情報および前記クライアント装置から前記特定されたサーバに接続するための接続経路からなる環境設定情報を格納可能で、通常のジャケットのポケット等の小形収納手段に収納可能な小形の可搬型の補助記憶媒体として構成される。

【００６９】

上述のように、補助記憶装置２０は、複数のサーバ３０，３１を遠隔操作するリモートアクセス処理部５４とネットワーク上の暗号化された通信を復号化する復号化処理部（暗号化，復号化処理部５２）を備えたフラッシュメモリ５０と、電子証明書、ＰＩＮを格納し、利用者認証を行う利用者認証部５３を備えたカード部５１を有して、耐タンパ性媒体部５１に、サーバ３０，３１にクライアント装置１０がリモートアクセスする利用シーンを規定する環境１，２に対応したログイン情報とサーバ情報についての複数の環境設定情報を格納可能とする。これらの環境設定情報は、環境設定情報格納部５５に格納される。

【００７０】

補助記憶装置は、複数のクライアント装置１０に共通して接続可能とされ、補助記憶装置２０を１個ポケットに収納しておけばクライアント装置を持ち運びすることなく利用者はクライアント装置を利用していずこの拠点にあっても予め指定のサーバ３０，３１にリモートアクセスしてコンピュータ操作を行うことができる。

【００７１】

サーバ３０，３１にクライアント装置１０がリモートアクセスする利用シーンを規定する環境１，２に対応したログイン情報とサーバ情報についての複数の環境情報を設定した環境設定情報格納部５５およびクライアント装置１０のクライアント装置情報を認識してこのクライアント装置１０のログイン情報を取得するクライアント装置自動認識部５６を補助記憶装置２０に備えてリモートアクセスシステム１００が構成される。

【００７２】
補助記憶装置２０を任意のクライアント装置１０に接続して該クライアント装置のログイン情報を取得し、該クライアント装置のログイン情報に対応してクライアント装置１０とサーバ３０，３１間を、当該クライアント装置にキーボードなどを使用して外部からログイン設定およびサーバ設定を行うことなしに、直ちに通信可能とする。これによって、リモートアクセス方法が構成される。
【００７３】
次に運用例について説明する。
本運用例は、複数拠点での執務や利用者がクライアント装置を共有する場合、ホテルでの貸出クライアント装置を利用する場合などの利用シーンで効果が発揮される。次のようなケースがある。
１）自席、支社、自宅といった外出先など、複数の拠点で仕事をするケース
２）研修所や病院など複数の人が共有のクライアント装置を使用するケース
３）派遣社員用に共有のクライアント装置を設置するケース
４）プロジェクトルームなど人の移動、出入りが多いケース
【００７４】
図１８は、上述したケースについて運用例を示す。図１９はオフィス内外で使用しているクライアント装置に補助記憶装置２０を差し込んで、社内サーバにアクセスするケースを示す。
【００７５】
図１８において、リモートアクセスシステム１００は、社内ネットワーク７１は社外ネットワーク７２にインターネット７３で接続して構成される社内専用ＬＡＮ７４とインターネット７３との間であって社内ネットワーク上に接続用のファイアウォール７７が設けてある。本社と支社を結ぶ社内専用ＬＡＮ７４には複数のサーバ７５が接続されている。インターネット７３を介しての社外からのリモートアクセスにはＳＳＬ－ＶＰＮを使用する。利用者７６は、出張、外出、帰宅時は、ポケットサイズ（ポケットに悠々入る程度の大きさ）の補助記憶装置２０を持ち歩く。利用者７６は、出張先ではホテルの貸出クライアント装置に補助記憶装置２０を差し込んで、外出先ではネットカフェでクライアント装置に補助記憶装置２０を差し込んで、あるいは自宅で自宅のクライアント装置に補助記憶装置２０を差し込んで使用する。これらで使用するクライアント装置がシンクライアントである場合には、シンクライアントのネットワーク設定を次のようにして行い得る。
【００７６】
サーバ３０，３１を遠隔操作するリモートアクセス処理部５４と、ネットワーク上の暗号化された通信を復号化する復号化処理部を備えたフラッシュメモリ５０と、電子証明書を格納する耐タンパ性媒体部５１と、を備え、サーバ３０，３１にシンクライアント（クライアント装置１０）がリモートアクセスする利用シーンを規定する環境に対応したログイン情報とサーバ情報についての複数の環境情報を耐タンパ性媒体部５１に設定した環境設定情報格納部５５およびシンクライアントのクライアント装置情報の認識を行ってログイン情報を取得するクライアント装置自動認識部５６を備えた補助記憶装置２０が準備される。
【００７７】
補助記憶装置２０を任意のシンクライアントに接続し、当該シンクライアントのログイン情報を取得する
リモートアクセス処理部５４によって、シンクライアントのログイン情報に基づいて利用シーンを規定する環境情報から耐タンパ性媒体部５１に格納されたサーバ情報を読み込み、サーバ情報に対応するサーバ３０，３１からネットワークを介して所定のデータを送信させる。
【００７８】
格納された構成データを使用してシンクライアント実行の構成データを自動的に構成する。このようにして、シンクライアントのネットワーク設定方法を構成する。

【００７９】
図１９は、オフィス内外で使用しているクライアント装置をクライアント装置として使用し、クライアント装置に補助記憶装置２０を差し込むだけで社内サーバにリモートアクセスする導入システム例を示す。
【００８０】
社内ネットワークに組み込まれた情報センター８９内に社内専用ＬＡＮ７４が配設されており、このＬＡＮ７４にサーバ３０，３１、管理者クライアント装置３７、ＳＳＬ－ＶＰＮ装置３８が接続された構成は図１８に示す例と同様である。そして、オフィス外８３にあるクライアント装置８４をインターネット７３を介し、ＳＳＬ－ＶＮＰを使用して社内専用ＬＡＮ７４に接続する方法、手段についても同様である。
【００８１】
オフィス８２で使用したクライアント装置８５に補助記憶装置２０を装置して社内専用ＬＡＮ７４に接続された社内ＬＡＮ８６を介してサーバ３０，３１からデータを取得する。この場合、社内ＬＡＮ８６にはＳＳＬ－ＶＰＮは不要とされる。
【００８２】
利用者７６は、出張の時にオフィス外８３にあるクライアント装置８４に補助記憶装置２０を装着し、前述同様にしてサーバ３０，３１から画像データなどの所定のデータを取得することを行う。
【００８３】
【表２】

表2 利用シーン情報と初回設定情報

#	利用シーン情報	設定情報
1	ｵﾌｨｽ	ｸﾗｲｱﾝﾄ名称及びｸﾗｲｱﾝﾄPC情報、経路情報、ｻｰﾊﾞ情報
2	出張先(自社の他事業所でｲﾝﾄﾗで自社接続)	同上(DHCP使用時は、上記情報で再利用可能(再設定不要))
3	出張先(他社からｲﾝﾀｰﾈｯﾄで自社接続)	利用者名称及びｸﾗｲｱﾝﾄ機器情報、接続(経路)情報(他社NetWork)、SSL-VPN装置情報、ｻｰﾊﾞ情報
4	自宅	利用者名称及びｸﾗｲｱﾝﾄ機器情報、接続(経路)情報(ADSLなど自宅回線)、SSL-VPN装置情報、ｻｰﾊﾞ情報
5	親戚宅	利用者名称及びｸﾗｲｱﾝﾄ機器情報、接続(経路)情報(ADSLなど自宅回線)、SSL-VPN装置情報、ｻｰﾊﾞ情報
6	ﾎﾃﾙ	利用者名称及びｸﾗｲｱﾝﾄ機器情報、接続(経路)情報(ADSLなどﾎﾃﾙ回線)、SSL-VPN装置情報、ｻｰﾊﾞ情報
7	ﾈｯﾄｶﾌｪ	利用者名称及びｸﾗｲｱﾝﾄ機器情報、接続(経路)情報(無線LAN)、SSL-VPN装置情報、ｻｰﾊﾞ情報
8	ﾓﾊﾞｲﾙ(電車内など)	利用者名称及びｸﾗｲｱﾝﾄ機器情報、接続(経路)情報(移動無線)、SSL-VPN装置情報、ｻｰﾊﾞ情報

【００８４】
表２は、利用シーン情報と初回設定情報との関係を示す。利用情報は、利用シーンおよび優先順位を含めて設定される。利用シーンとしては、オフィス、出張先（自社の他事業所でイントラで自社接続）、出張先（他社からインターネットで自社接続）、自宅、親戚宅、ホテル、ネットカフェ、モバイル（電車内など）でのクライアント装置が設定可能であり、優先順位についてもこの順位で設定可能とされる。
【００８５】
クライアント装置はこのように、複数設定すなわち定義することができる。１つのクライアント装置であってもよい。上述の例では８個以内としている。クライアント装置を複数設定した場合のメニュー表示方法としては、一番執務する可能性の高い、すなわち優先順位の高い場所に設置したクライアント装置をデフォルトとして設定し、デフォルトをプルダウンメニューの最初に自動表示し得るようにする。接続（経路）情報とクライアント装置の機器情報についても優先順位に従って自動認識し、一番近い設定をプルダウンメニューの最初に表示する。この順位を順次下げて表示し得るようにする。
【００８６】
上述した補助記憶媒体２０は、予め特定された環境設定情報を格納しており、特定されたクライアント装置に接続されると、直ちに特定された環境設定情報を特定されたクライ

アント装置に特定し、当該クライアント装置から前記特定されたサーバへの接続を可能とする。

【００８７】

予め特定された利用シーン情報を格納しており、特定されたクライアント装置に接続されると、利用者名称情報、機器情報および接続経路情報を特定されたクライアント装置に特定し、当該クライアント装置から前記特定されたサーバへの接続を可能とする。

【００８８】

予め特定された利用シーン情報を格納しており、特定されたクライアント装置に接続されると、入力された利用認識情報が予め格納された利用者認識情報と一致すると、特定された環境設定情報を前記特定されたクライアント装置に特定し、当該クライアント装置から前記特定されたサーバへの接続を可能とする。

【００８９】

本実施例は、使い勝手向上について次のような効果を有する。

ａ）使用時の環境設定が簡単

１）利用シーンに応じた登録ができる。

環境設定情報を備えた利用シーン情報は、複数登録できるため、会社，自宅，出先など、各利用シーンにおいて、毎回設定変更することなく使用できる。

２）設定の煩わしさから解放できる。

シンクライアント装置を接続するＬＡＮにてＤＨＣＰを使用すると、１つの利用シーン情報で、使用可能とすることができる。

３）クライアント装置構成を自動認識することができる。

クライアント装置の構成を自動認識して自動的にクライアント装置のログイン情報を取得するため、利用者は特別な機器の設定を行う必要がない。

ｂ）短時間での起動，停止

すばやい起動，停止ができ、使いたいとき直ちに使用、止めたいときに速やかに停止することができる。

ｃ）ＨＤＤへアクセスしないので、使用したクライアント装置にデータを一切残さない。

また、専用のクライアント装置を購入する場合に比べてコストを抑えることが可能となる。既存のクライアント装置は、補助記憶装置を使わずに起動すれば、普通のクライアント装置として使用が可能である。

従って、シンクライアントとリッチクライアントとして併用が可能となる。

【図面の簡単な説明】

【００９０】

【図１】本発明の実施例の構成を示すブロック図。

【図２】補助記憶装置の具体的な構成を示す図。

【図３】環境設定情報の入力フローを示す図。

【図４】ＰＩＮ入力図。

【図５】ログイン設定図。

【図６】サーバ登録図。

【図７】サーバ情報設定図。

【図８】ログイン情報設定図。

【図９】オプション設定図。

【図１０】有線ＬＡＮ設定図。

【図１１】無線ＬＡＮ設定図。

【図１２】モバイル設定図。

【図１３】オプション設定図。

【図１４】ＰＩＮ入力図。

【図１５】ログイン設定図。

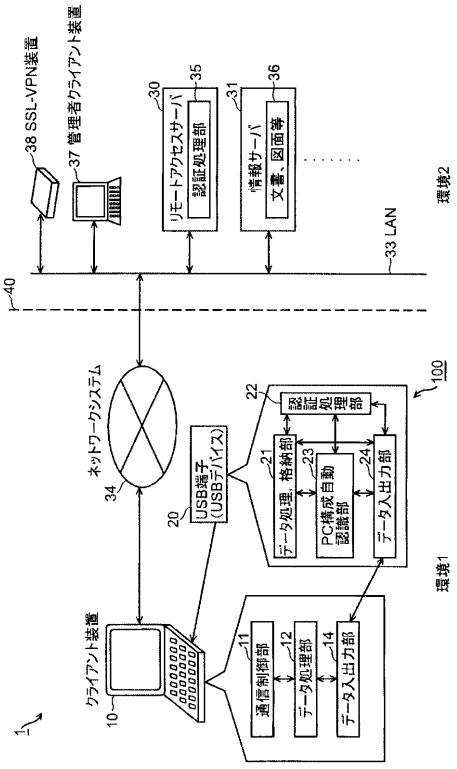
【図１６】サーバ登録図。

【図１７】ログイン情報設定図。

【図１８】運用例を示す図。
【図１９】他の運用例を示す図。
【符号の説明】
【００９１】
１…データ通信システム、１０…クライアント装置、１１…通信制御部、１２…データ処理部、１４…データ入出力部、２０…補助記憶装置、２１…データ処理，格納部、２２…認証処理部、２３…クライアント装置構成自動認識部、２４…データ入出力部、３０…リモートアクセスサーバ（サーバ）、３１…情報サーバ（サーバ）、３３…ＬＡＮ、３４…ネットワークシステム、３５…認証処理部、３６…文書，図面等、３７…管理者クライアント装置、３８…ＳＳＬ－ＶＰＮ装置、５０…フラッシュメモリ、５１…耐タンパ性媒体部、５２…暗号化，復号化処理部（復号化処理部）、５３…利用者認証部、５４…リモートアクセス処理部、５５…環境設定情報格納部、５６…クライアント装置自動認識部、５７…ログイン情報、５８…サーバ情報、１００…リモートアクセスシステム。

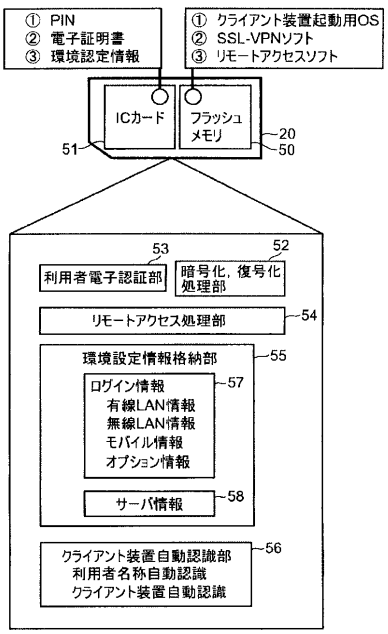
【図１】

図 1



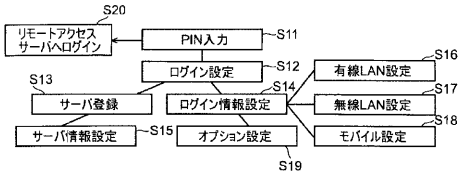
【図２】

図 2



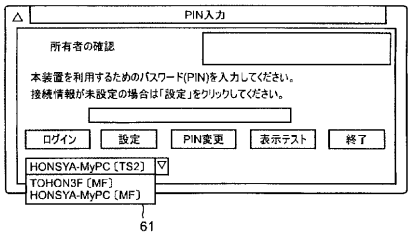
【図３】

図 3



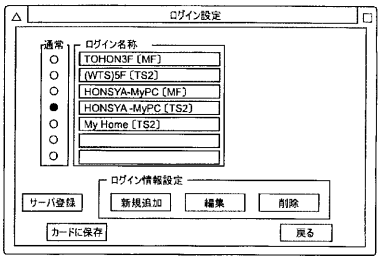
【図４】

図 4



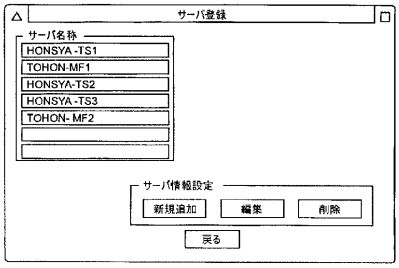
【図５】

図 5



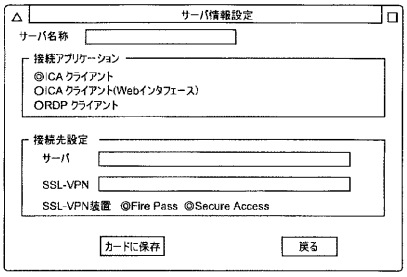
【図６】

図 6



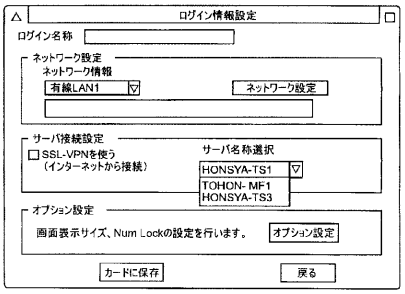
【図７】

図 7



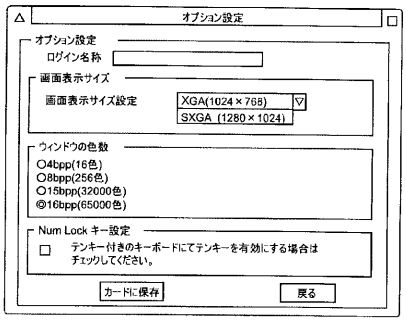
【図８】

図 8



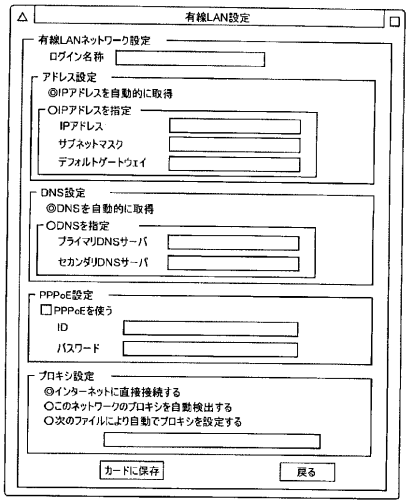
【図９】

図 9



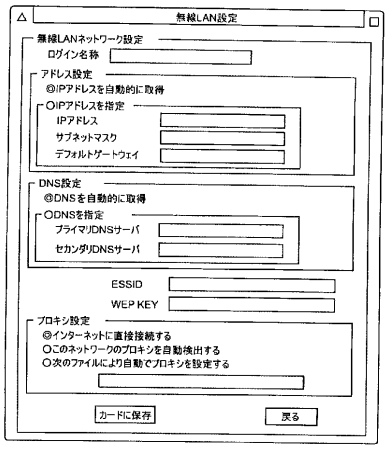
【図１０】

図 10



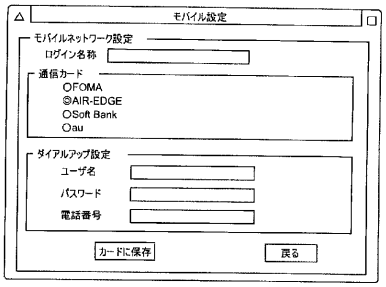
【図１１】

図 11



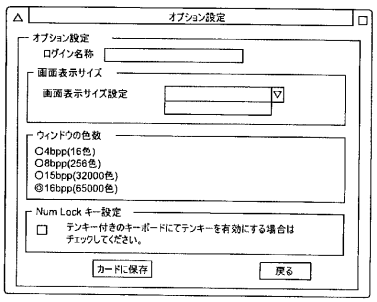
【図１２】

図 12



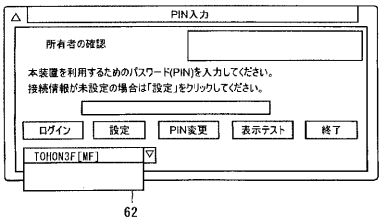
【図１３】

図 13



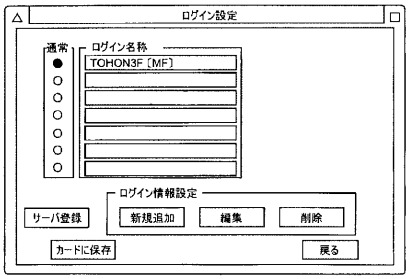
【図１４】

図 14



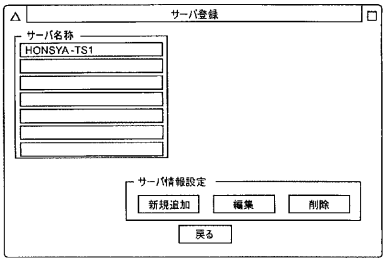
【図１５】

図 15



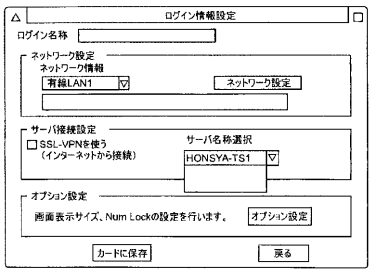
【図１６】

図 16



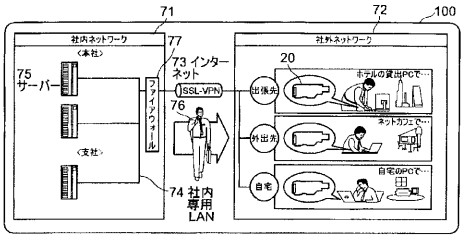
【図１７】

図 17



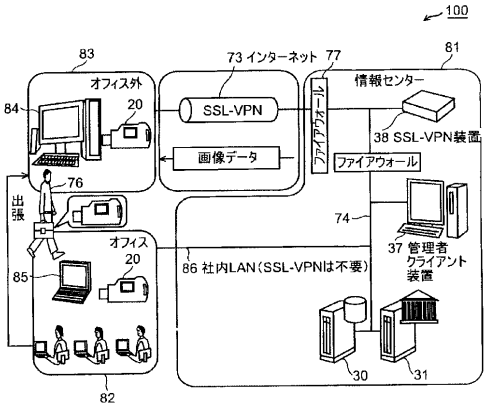
【図１８】

図 18



【図１９】

図 19



フロントページの続き

(72)発明者　須田　滋
茨城県日立市大みか町五丁目２番１号　株式会社日立情報制御ソリューションズ内
(72)発明者　石川　満章
茨城県日立市大みか町五丁目２番１号　株式会社日立情報制御ソリューションズ内

Ｆターム(参考) 5B035 AA13 BB09 BC03 CA11
5B285 AA01 BA02 BA03 CA41 CA42 CA43 CA52 CB06 CB07 CB47
CB52 CB55 CB62 CB64 CB73 CB85 DA01 DA03 DA05 DA09
5J104 AA07 AA16 EA03 EA16 EA22 EA26 KA02 NA05 NA35 NA36
NA38 NA41 NA42 PA07