(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6073120号
(P6073120)
(45)発行日　平成29年2月1日(2017.2.1)　(24)登録日　平成29年1月13日(2017.1.13)

(51)Int.Cl.　　F I
H04L 12/66 (2006.01)　　H04L 12/66 B
G06F 21/41 (2013.01)　　G06F 21/41

請求項の数 8　(全 22 頁)

(21)出願番号　特願2012-263598(P2012-263598)
(22)出願日　平成24年11月30日(2012.11.30)
(65)公開番号　特開2014-110515(P2014-110515A)
(43)公開日　平成26年6月12日(2014.6.12)
審査請求日　平成27年11月27日(2015.11.27)

(73)特許権者　591008605
株式会社日本デジタル研究所
東京都江東区新砂１丁目２番３号
(74)代理人　100089118
弁理士　酒井　宏明
(72)発明者　大渕　徹
東京都江東区新砂１－２－３　株式会社日本デジタル研究所内
(72)発明者　尾上　涼一
東京都江東区新砂１－２－３　株式会社日本デジタル研究所内
(72)発明者　嘉陽田　朝史
東京都江東区新砂１－２－３　株式会社日本デジタル研究所内

最終頁に続く

(54)【発明の名称】接続認証システムおよび接続認証方法

(57)【特許請求の範囲】
【請求項１】
ユーザが携帯するモバイル端末と、認証管理サーバを介して前記モバイル端末を認証するファイアウォール装置と、クライアント端末に接続されているサーバとを有する接続認証システムであって、
前記モバイル端末は、
前記認証管理サーバを介して前記ファイアウォール装置に対して、認証の要求を行うとともに、該モバイル端末のアドレス情報を通知する認証要求部と、
前記ファイアウォール装置から受信した接続先クライアント端末のアドレス情報とポート番号とを用いて、前記ファイアウォール装置に対して、前記接続先クライアント端末とのリモート接続を要求するリモート接続要求部とを備え、
前記ファイアウォール装置は、
前記認証管理サーバを介して前記モバイル端末から認証の要求を受け付けると、該モバイル端末の認証を行う認証部と、
前記認証部によって前記モバイル端末の認証を行った結果、該モバイル端末が正当であると判定した場合には、該モバイル端末のアドレス情報を格納する格納部と、
前記サーバから接続先クライアント端末のアドレス情報を受信すると、該アドレス情報と前記モバイル端末の接続を許可するポートを識別するポート識別情報とを対応付けて登録する登録部と、
前記登録部によって登録された接続先クライアント端末のアドレス情報とポート識別情

報とを、前記モバイル端末に送信する送信部と、
前記モバイル端末からリモート接続の要求を受け付けると、該モバイル端末のアドレス情報と、前記格納部によって格納されたアドレス情報とを比較し、両アドレス情報が一致する場合には、前記モバイル端末と前記接続先クライアント端末とのリモート接続を確立する接続確立部とを備え、
前記接続確立部は、両アドレス情報が一致する場合には、該モバイル端末と前記接続先クライアント端末とのリモート接続を確立する一方で、両アドレス情報が一致しない場合には、第１の認証によって正当なモバイル端末と判断された場合でも、該モバイル端末と前記接続先クライアント端末とのリモート接続を拒否し、
前記サーバは、前記ファイアウォール装置によって前記モバイル端末が正当であると判定された場合には、前記モバイル端末が接続する接続先クライアント端末のアドレス情報を前記ファイアウォール装置に通知するアドレス通知部を備えることを特徴とする接続認証システム。
【請求項２】
前記サーバは、前記ファイアウォール装置によって前記モバイル端末が正当であると判定した場合であって、接続先クライアント端末が複数ある場合には、接続先クライアント端末の一覧を前記モバイル端末に通知する一覧通知部をさらに備え、
前記モバイル端末は、前記サーバから通知された接続先クライアント端末の一覧のうち、前記ユーザによって選択指示された接続先クライアントを識別するクライアント識別情報を前記ファイアウォール装置に通知する選択指示部をさらに備え、
前記アドレス通知部は、前記ファイアウォール装置に通知されたクライアント識別情報により識別される接続先クライアント端末のアドレス情報を前記ファイアウォール装置に通知することを特徴とする請求項１に記載の接続認証システム。
【請求項３】
ユーザが携帯するモバイル端末と、認証管理サーバを介して前記モバイル端末を認証するファイアウォール装置と、クライアント端末に接続されているサーバとを有する接続認証システムであって、
前記モバイル端末は、
前記ファイアウォール装置のドメイン情報またはアドレス情報と、前記認証管理サーバの資源位置指定子とが組み合わされた特定の資源位置指定子を用いて、前記認証管理サーバにアクセスし、前記認証管理サーバを介して前記ファイアウォール装置に対して、認証の要求を行うとともに、該モバイル端末のアドレス情報を通知する認証要求部と、
前記ファイアウォール装置から受信した接続先クライアント端末のアドレス情報とポート番号とを用いて、前記ファイアウォール装置に対して、前記接続先クライアント端末とのリモート接続を要求するリモート接続要求部とを備え、
前記ファイアウォール装置は、
前記認証管理サーバを介して前記モバイル端末から認証の要求を受け付けると、該モバイル端末の認証を行う認証部と、
前記認証部によって前記モバイル端末の認証を行った結果、該モバイル端末が正当であると判定した場合には、該モバイル端末のアドレス情報を格納する格納部と、
前記サーバから接続先クライアント端末のアドレス情報を受信すると、該アドレス情報と前記モバイル端末の接続を許可するポートを識別するポート識別情報とを対応付けて登録する登録部と、
前記登録部によって登録された接続先クライアント端末のアドレス情報とポート識別情報とを、前記モバイル端末に送信する送信部と、
前記モバイル端末からリモート接続の要求を受け付けると、該モバイル端末のアドレス情報と、前記格納部によって格納されたアドレス情報とを比較し、両アドレス情報が一致する場合には、前記モバイル端末と前記接続先クライアント端末とのリモート接続を確立する接続確立部とを備え、
前記サーバは、前記ファイアウォール装置によって前記モバイル端末が正当であると判

定された場合には、前記モバイル端末が接続する接続先クライアント端末のアドレス情報を前記ファイアウォール装置に通知するアドレス通知部を備えることを特徴とする接続認証システム。

【請求項４】

前記サーバは、前記ファイアウォール装置によって前記モバイル端末が正当であると判定した場合には、前記モバイル端末と前記接続先クライアント端末とのリモート接続を確立する契約が有効であるか否かを示す契約状況を前記認証管理サーバに問い合わせる問い合わせ部をさらに備え、

前記認証管理サーバは、前記サーバから問い合わせを受け付けた場合には、前記契約状況が有効であるか否かを確認し、該確認の結果を前記サーバに送信する確認部を備え、

前記一覧通知部は、前記契約状況が有効であって、接続先クライアント端末が複数ある場合には、接続先クライアント端末の一覧を前記モバイル端末に通知することを特徴とする請求項２に記載の接続認証システム。

【請求項５】

前記ファイアウォールは、前記接続確立部によって前記モバイル端末と前記接続先クライアント端末とのリモート接続を確立した後に、所定時間が経過したか否かを監視し、所定時間が経過した場合には、接続を許可したポートを閉じてリモート接続を切断する切断部をさらに備えることを特徴とする請求項１～４のいずれか一つに記載の接続認証システム。

【請求項６】

前記接続確立部は、前記接続先クライアント端末の電源がオフである場合には、該接続先クライアント端末を起動指示で起動させた後に、リモート接続を確立することを特徴とする請求項１～５のいずれか一つに記載の接続認証システム。

【請求項７】

前記接続確立部は、前記接続先クライアント端末に代えて、該接続先クライアント端末を前記サーバ上で仮想的に構築された仮想クライアント端末と前記モバイル端末とのリモート接続を確立することを特徴とする請求項１～６のいずれか一つに記載の接続認証システム。

【請求項８】

ユーザが携帯するモバイル端末と、認証管理サーバを介して前記モバイル端末を認証するファイアウォール装置と、クライアント端末に接続されているサーバとを有する接続認証システムで実行される接続認証方法であって、

前記モバイル端末が、前記認証管理サーバを介して前記ファイアウォール装置に対して、認証の要求を行うとともに、該モバイル端末のアドレス情報を通知する認証要求ステップと、

前記ファイアウォール装置が、前記認証管理サーバを介して前記モバイル端末から認証の要求を受け付けると、該モバイル端末の認証を行う認証ステップと、

前記ファイアウォール装置が、前記認証ステップによって前記モバイル端末の認証を行った結果、該モバイル端末が正当であると判定した場合には、該モバイル端末のアドレス情報を格納する格納ステップと、

前記サーバは、前記ファイアウォール装置によって前記モバイル端末が正当であると判定された場合には、前記モバイル端末が接続する接続先クライアント端末のアドレス情報を前記ファイアウォール装置に通知するアドレス通知ステップと、

前記ファイアウォール装置が、前記サーバから接続先クライアント端末のアドレス情報を受信すると、該アドレス情報と前記モバイル端末の接続を許可するポートを識別するポート識別情報とを対応付けて登録する登録ステップと、

前記ファイアウォール装置が、前記登録ステップによって登録された接続先クライアント端末のアドレス情報とポート識別情報とを、前記モバイル端末に送信する送信ステップと、

前記モバイル端末が、前記ファイアウォール装置から受信した接続先クライアント端末

のアドレス情報とポート番号とを用いて、前記ファイアウォール装置に対して、前記接続先クライアント端末とのリモート接続を要求するリモート接続要求ステップと、

前記ファイアウォール装置が、前記モバイル端末からリモート接続の要求を受け付けると、該モバイル端末のアドレス情報と、前記格納ステップによって格納されたアドレス情報とを比較し、両アドレス情報が一致する場合には、前記モバイル端末と前記接続先クライアント端末とのリモート接続を確立する一方で、両アドレス情報が一致しない場合には、第１の認証によって正当なモバイル端末と判断された場合でも、該モバイル端末と前記接続先クライアント端末とのリモート接続を拒否する接続確立ステップと、

を含んだことを特徴とする接続認証方法。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、接続認証システムおよび接続認証方法に関する。

【背景技術】

【０００２】

従来から、ユーザが携帯するモバイル端末と、室内（例えば、会計事務所内）等に設置されたクライアント端末とをリモート接続することで、クライアント端末が目の前にある時と同じように直接操作することができる技術が知られている。ところが、モバイル端末とクライアント端末とが一度接続されてしまうと、モバイル端末からクライアント端末が保持する情報を誰でも閲覧することができてしまうため、接続の際に認証処理等を行ってセキュリティを向上させる必要がある。

【０００３】

例えば、セキュリティを向上させる手法として、ＶＰＮ（Virtual Private Network）接続により、モバイル端末とクライアント端末との間で暗号化したデータを通信する技術が知られている。

【０００４】

また、セキュリティを向上させる手法として、例えば、モバイル端末とクライアント端末とを中継する専用のセンタ（例えば、中継サーバ）が認証を行い、認証に成功した場合には、全ての通信をセンタを経由させてモバイル端末とクライアント端末とを接続させる技術が知られている。

【先行技術文献】

【特許文献】

【０００５】

【特許文献１】特開２００２－１３５８６７号公報

【発明の概要】

【発明が解決しようとする課題】

【０００６】

しかしながら、上記のＶＰＮ接続による暗号化したデータで通信を行う技術では、モバイル端末とクライアント端末との間で通信を行うたびに、暗号化および復号化を行う必要があるため、通信負荷が高くなり、通信速度が低下するという課題があった。より詳細には、送受信するパケットの内、ユーザデータだけでなくローカルＩＰヘッダやＴＣＰヘッダ（ポート番号を含む）なども含めて暗号化され、パケットを送受信するたびに暗号化および復号化の処理を経ることによる処理速度の低下である。例えば、モバイル端末を利用して、事務所側の端末（ないし仮想端末）に対しリモート接続を行う場合には、ＲＤＰ（リモートデスクトッププロトコル）を利用する場合が多いが、この場合、事務所側の端末からモバイル端末に対して画像データを転送したり、モバイル端末から事務所側の端末に入力操作を送信したりすることが複合して行われるため、この際のレスポンスにおいて処理速度の低下は特に重要な問題となる。

【０００７】

また、上記のセンタを経由させてモバイル端末とクライアント端末とを接続させる技術

では、全ての通信がセンタを経由するので、通信速度と安全性がセンタに依存してしまい、通信速度および安全性が低下するおそれがあるという課題があった。

【０００８】

そこで、この発明は、上述した従来技術の課題を解決するためになされたものであり、通信負荷による通信速度の低下を軽減しつつも、接続に至るまでの手順（プロトコル）を工夫することで安全性を高くすることを目的とする。

【課題を解決するための手段】

【０００９】

上述した課題を解決し、目的を達成するため、本発明に係る接続認証システムは、ユーザが携帯するモバイル端末と、認証管理サーバを介して前記モバイル端末を認証するファイアウォール装置と、クライアント端末に接続されているサーバとを有する接続認証システムであって、前記モバイル端末は、前記認証管理サーバを介して前記ファイアウォール装置に対して、認証の要求を行うとともに、該モバイル端末のアドレス情報を通知する認証要求部と、前記ファイアウォール装置から受信した接続先クライアント端末のアドレス情報とポート番号とを用いて、前記ファイアウォール装置に対して、前記接続先クライアント端末とのリモート接続を要求するリモート接続要求部とを備え、前記ファイアウォール装置は、前記認証管理サーバを介して前記モバイル端末から認証の要求を受け付けると、該モバイル端末の認証を行う認証部と、前記認証部によって前記モバイル端末の認証を行った結果、該モバイル端末が正当であると判定した場合には、該モバイル端末のアドレス情報を格納する格納部と、前記サーバから接続先クライアント端末のアドレス情報を受信すると、該アドレス情報と前記モバイル端末の接続を許可するポートを識別するポート識別情報とを対応付けて登録する登録部と、前記登録部によって登録された接続先クライアント端末のアドレス情報とポート識別情報とを、前記モバイル端末に送信する送信部と、前記モバイル端末からリモート接続の要求を受け付けると、該モバイル端末のアドレス情報と、前記格納部によって格納されたアドレス情報とを比較し、両アドレス情報が一致する場合には、前記モバイル端末と前記接続先クライアント端末とのリモート接続を確立する接続確立部とを備え、前記サーバは、前記ファイアウォール装置によって前記モバイル端末が正当であると判定された場合には、前記モバイル端末が接続する接続先クライアント端末のアドレス情報を前記ファイアウォール装置に通知するアドレス通知部を備えることを特徴とする。

【００１０】

また、本発明に係る接続認証方法は、ユーザが携帯するモバイル端末と、認証管理サーバを介して前記モバイル端末を認証するファイアウォール装置と、クライアント端末に接続されているサーバとを有する接続認証システムで実行される接続認証方法であって、前記モバイル端末が、前記認証管理サーバを介して前記ファイアウォール装置に対して、認証の要求を行うとともに、該モバイル端末のアドレス情報を通知する認証要求ステップと、前記ファイアウォール装置が、前記認証管理サーバを介して前記モバイル端末から認証の要求を受け付けると、該モバイル端末の認証を行う認証ステップと、前記ファイアウォール装置が、前記認証ステップによって前記モバイル端末の認証を行った結果、該モバイル端末が正当であると判定した場合には、該モバイル端末のアドレス情報を格納する格納ステップと、前記サーバは、前記ファイアウォール装置によって前記モバイル端末が正当であると判定された場合には、前記モバイル端末が接続する接続先クライアント端末のアドレス情報を前記ファイアウォール装置に通知するアドレス通知ステップと、前記ファイアウォール装置が、前記サーバから接続先クライアント端末のアドレス情報を受信すると、該アドレス情報と前記モバイル端末の接続を許可するポートを識別するポート識別情報とを対応付けて登録する登録ステップと、前記ファイアウォール装置が、前記登録ステップによって登録された接続先クライアント端末のアドレス情報とポート識別情報とを、前記モバイル端末に送信する送信ステップと、前記モバイル端末が、前記ファイアウォール装置から受信した接続先クライアント端末のアドレス情報とポート番号とを用いて、前記ファイアウォール装置に対して、前記接続先クライアント端末とのリモート接続を要求す

るリモート接続要求ステップと、前記ファイアウォール装置が、前記モバイル端末からリモート接続の要求を受け付けると、該モバイル端末のアドレス情報と、前記格納ステップによって格納されたアドレス情報とを比較し、両アドレス情報が一致する場合には、前記モバイル端末と前記接続先クライアント端末とのリモート接続を確立する接続確立ステップと、を含んだことを特徴とする。

【発明の効果】

【００１１】

発明によれば、認証処理については、認証管理サーバを介して行うことで安全性を高め、一方、接続処理については、ファイアウォールを通してモバイル端末とクライアント端末とでダイレクトに行うことで、通信負荷を軽くする。これにより、通信負荷による通信速度の低下を軽減するとともに、安全性を高めることができるという効果を奏する。

【図面の簡単な説明】

【００１２】

【図１】図１は、実施例１に係る接続認証システムの構成を示すブロック図である。

【図２】図２は、実施例１に係るモバイル端末の構成を示すブロック図である。

【図３】図３は、実施例１に係る認証管理サーバの構成を示すブロック図である。

【図４】図４は、契約情報管理テーブルのデータ例を示す図である。

【図５】図５は、実施例１に係るファイアウォールの構成を示すブロック図である。

【図６】図６は、ポート管理テーブルのデータ例を示す図である。

【図７】図７は、モバイル端末ＩＰ管理テーブルのデータ例を示す図である。

【図８】図８は、ＤＮＳ情報のデータ例を示す図である。

【図９】図９は、実施例１に係るサーバの構成を示すブロック図である。

【図１０】図１０は、ＩＤ管理テーブルのデータ例を示す図である。

【図１１】図１１は、接続先管理テーブルのデータ例を示す図である。

【図１２】図１２は、ユーザ契約コードのデータ例を示す図である。

【図１３】図１３は、アクセス管理テーブルのデータ例を示す図である。

【図１４】図１４は、接続認証システムにおける認証処理および接続処理の概要について説明する図である。

【図１５】図１５は、接続認証システムにおけるリモート接続処理について説明する図である。

【図１６】図１６は、接続認証システムによる全体の処理の流れを示すシーケンス図である。

【図１７】図１７は、認証要求を行う際にモバイル端末に表示される画面例を示す図である。

【図１８】図１８は、接続先のコンピュータ名一覧をモバイル端末に表示した画面例を示す図である。

【図１９】図１９は、接続先のコンピュータに関する情報を表示した画面例を示す図である。

【発明を実施するための形態】

【００１３】

以下に添付図面を参照して、この発明に係る接続認証システムおよび接続認証方法の実施例を詳細に説明する。なお、この実施例によりこの発明が限定されるものではない。

【実施例１】

【００１４】

以下の実施例では、実施例１に係る接続認証システムの構成、モバイル端末の構成、認証管理サーバの構成、ファイアウォールの構成、サーバの構成および接続認証システムの処理の流れを順に説明し、最後に実施例１による効果を説明する。なお、以下では、会計事務所内にファイアウォール、サーバおよびクライアントＰＣが設置されており、会計事務所外でユーザがモバイル端末を利用している場合を例として説明する。

【００１５】

［実施例１に係る接続認証システムの構成］
まず、図１を用いて、第１の実施形態に係る接続認証システムの構成について説明する。図１は、第１の実施形態に係る接続認証システムの構成を示すブロック図である。
【００１６】
図１に例示するように、第１の実施形態に係る接続認証システム１００は、モバイル端末１０と、認証管理サーバ２０と、ファイアウォール３０と、サーバ４０と、複数のクライアントＰＣ（Personal Computer）５０ａ～５０ｃとで構成される。また、接続認証システム１００では、モバイル端末１０、認証管理サーバ２０、および、ファイアウォール３０は、インターネット６０を介して接続されている。なお、クライアントＰＣ５０ａ～５０ｃについて、特に区別無く説明する場合には、クライアントＰＣ５０と記載する。
【００１７】
モバイル端末１０は、例えば、携帯電話機、スマートフォン、ＰＤＡ（Personal Digital Assistant）、タブレット型ＰＣ、ノート型ＰＣ等の情報処理装置であり、ユーザが会計事務所外に持ち運んで使用する端末である。モバイル端末１０は、事前準備として、認証管理サーバ２０へアクセスするＵＲＬを保持している。そして、モバイル端末１０は、該ＵＲＬを用いて認証管理サーバ２０にアクセスし、ＩＤ、パスワードを入力して、認証管理サーバ２０を介してファイアウォール３０に認証要求を行うとともに、クライアントＰＣ５０とのリモート接続を要求する。そして、モバイル端末１０では、クライアントＰＣ５０とのリモート接続が確立した後、リモートアクセスすることによって該クライアントＰＣ５０が目の前にある時と同様に直接操作することができる。
【００１８】
認証管理サーバ２０は、認証に関する情報や、ユーザの契約に関する情報を管理するサーバであり、モバイル端末１０からの認証要求を受け付ける。また、例えば、この認証管理サーバ２０は、サーバ４０からユーザが契約状況の問い合わせを受け付け、契約状況を応答する。
【００１９】
ファイアウォール３０は、会計事務所内のネットワークに対する外部からの不正な侵入を防ぐ機能を有するソフトウェアを搭載した装置である。このファイアウォール３０は、デフォルト状態では、認証管理サーバ２０からのアクセスのみを許可し、他装置からのアクセスを拒否することで、安全性を確保している。また、後述するように、ファイアウォール３０は、認証管理サーバ２０からの指示を受けて、認証管理サーバ２０が認証に成功したモバイル端末１０のみリモート接続を許可するので、さらに安全性を確保している。
【００２０】
サーバ４０は、会計事務所内に設置されたサーバ装置であり、同会計事務所内に設置されたクライアントＰＣ５０ａ～５０ｃに関する情報を管理している。また、サーバ４０は、事前準備として、各クライアントＰＣ５０ａ～５０ｃからユーザＩＤとパスワードの登録を受け付け、該ユーザＩＤとパスワードを後述するＩＤ管理テーブル４３ａに記憶する。また、図１の例では、サーバ４０上において、クライアントＰＣ５０を仮想的に構築した仮想クライアントＰＣ４０ａを動作させており、この仮想クライアントＰＣ４０ａをモバイル端末１０とリモート接続される接続先端末としてもよい。
【００２１】
クライアントＰＣ５０は、会計事務所内に設置されたＰＣであり、例えば、デスクトップ型ＰＣ等の情報処理装置であって、ユーザが会計事務所内で使用する端末である。また、このクライアントＰＣ５０は、ファイアウォール３０が認証したモバイル端末１０とリモート接続される端末である。
【００２２】
以下に、図を用いて、モバイル端末１０の構成、認証管理サーバ２０の構成、ファイアウォール３０の構成、サーバ４０の構成を順に説明していく。
【００２３】
［モバイル端末１０の構成］

まず、図２を用いて、図１に示したモバイル端末１０の構成を説明する。図２は、実施例１に係るモバイル端末１０の構成を示すブロック図である。図２に示すように、このモバイル端末１０は、入力部１１、出力部１２、通信部１３、制御部１４、記憶部１５を備える。以下にこれらの各部の処理を説明する。

【００２４】

入力部１１は、ユーザＩＤやパスワード、接続先のコンピュータ名の選択指示などを入力するものであり、キーボードやマウス、マイクなどを備えて構成される。また、出力部１２は、ユーザＩＤおよびパスワードを入力可能な認証画面（後述する図１７参照）や、接続先のコンピュータ名一覧を表示した画面（後述する図１８参照）、リモート接続要求時の画面（後述する図１９参照）を表示するものであり、モニタ（ディスプレイ、タッチパネル）やスピーカを備えて構成される。

【００２５】

通信部１３は、接続される認証管理サーバ２０およびファイアウォール３０との間でやり取りする各種情報に関する通信を制御する。具体的には、通信部１３は、ユーザＩＤやパスワードを認証管理サーバ２０に送信し、接続先のコンピュータの一覧を認証管理サーバ２０から受信する。また、通信部１３は、接続先端末情報とポート番号をファイアウォール３０から受信し、リモート接続の要求をファイアウォール３０に送信する。

【００２６】

制御部１４は、各種の処理手順などを規定したプログラムおよび所要データを格納するための内部メモリを有し、これらによって種々の処理を実行するが、特に本発明に密接に関連するものとしては、認証要求部１４ａ、選択指示部１４ｂ、リモート接続要求部１４ｃを有する。

【００２７】

認証要求部１４ａは、モバイル端末１０から認証管理サーバ２０を介してファイアウォール３０に対して、認証の要求を行うとともに、該モバイル端末１０のグローバルＩＰを通知する。具体的には、認証要求部１４ａは、認証の要求を行う際には、ファイアウォール３０内のＤＮＳ（Domain Name System）と認証管理サーバ２０のＵＲＬとが組み合わされた特定ＵＲＬを用いて、認証管理サーバ２０にアクセスする。なお、この特定ＵＲＬは、事前にサーバ４０から通知されたものであり、例えば、ブックマークに登録されているものとする。

【００２８】

選択指示部１４ｂは、サーバ４０から通知された接続先クライアント端末の一覧のうち、ユーザによって選択指示されたコンピュータ名をファイアウォール３０に通知する。具体的には、選択指示部１４ｂは画面に表示されたコンピュータ名のうち、いずれかのコンピュータ名がユーザに選択指示されると、該コンピュータ名をファイアウォール３０に通知する。

【００２９】

リモート接続要求部１４ｃは、ファイアウォール３０から受信した接続先クライアント端末のアドレス情報とポート番号とを用いて、ファイアウォール３０に対して、接続先クライアント端末とのリモート接続を要求する。具体的には、リモート接続要求部１４ｃは、ＲＤＰ（Remote Desktop Protocol）ツールにより接続アドレス、ポート番号を取得して、リモート接続をファイアウォール３０へ要求する。

【００３０】

記憶部１５は、制御部１４による各種処理に必要なデータおよびプログラムを格納するものであり、例えば、ＲＡＭ（Random Access Memory）、ＲＯＭ（Read Only Memory）、フラッシュメモリ（flash memory）などの半導体メモリ素子、または、ハードディスク、光ディスクなどの記憶装置である。

【００３１】

［認証管理サーバ２０の構成］

次に、図３を用いて、図１に示した認証管理サーバ２０の構成を説明する。図３は、実

施例１に係る認証管理サーバ２０の構成を示すブロック図である。図３に示すように、この認証管理サーバ２０は、通信部２１、制御部２２、記憶部２３を備える。以下にこれらの各部の処理を説明する。

【００３２】

通信部２１は、接続されるモバイル端末１０およびファイアウォール３０との間でやり取りする各種情報に関する通信を制御する。具体的には、通信部２１は、ユーザＩＤやパスワードをモバイル端末１０から受信し、ファイアウォール３０に転送する。また、通信部２１は、接続先のコンピュータの一覧をファイアウォール３０から受信し、モバイル端末１０に転送する。

【００３３】

記憶部２３は、制御部２２による各種処理に必要なデータおよびプログラムを格納するものであり、特に本発明に密接に関連するものとしては、契約情報管理テーブル２３ａを記憶する。

【００３４】

契約情報管理テーブル２３ａは、契約状況に関する情報が登録されたテーブルである。具体的には、図４に例示するように、契約情報管理テーブル２３ａは、契約を一意に識別するコードである「ユーザ契約コード」と、契約が有効であるか無効であるかを示す「契約状況」とを対応付けて記憶する。例えば、図４の例では、契約情報管理テーブル２３ａは、ユーザ契約コード「ｔｏｋｙｏ６３４」と、契約状況「有効」とを対応付けて記憶している。これは、ユーザ契約コード「ｔｏｋｙｏ６３４」の契約が「有効」であることを示している。

【００３５】

制御部２２は、各種の処理手順などを規定したプログラムおよび所要データを格納するための内部メモリを有し、これらによって種々の処理を実行するが、特に本発明に密接に関連するものとしては、認証接続部２２ａおよび確認部２２ｂを有する。

【００３６】

認証接続部２２ａは、モバイル端末１０から、ユーザＩＤおよびパスワードの入力を受け付ける。そして、認証接続部２２ａは、モバイル端末１０のグローバルＩＰを取得し、受け付けたユーザＩＤおよびパスワードとともに、モバイル端末１０のグローバルＩＰをファイアウォール３０に送信する。

【００３７】

確認部２２ｂは、サーバ４０から問い合わせを受け付けた場合には、契約状況が有効であるか否かを確認し、該確認の結果をサーバ４０に送信する。具体的には、確認部２２ｂは、サーバ４０からユーザ契約コードとともに、契約状況を確認する旨の問い合わせを受け付けると、サーバ４０から受け付けたユーザ契約コードと一致するユーザ契約コードを契約情報管理テーブル２３ａから検索し、該ユーザ契約コードに対応する契約状況（有効または無効）を取得して、該契約状況をサーバ４０に返信する。

【００３８】

［ファイアウォール３０の構成］

次に、図５を用いて、図１に示したファイアウォール３０の構成を説明する。図５は、実施例１に係るファイアウォール３０の構成を示すブロック図である。図５に示すように、このファイアウォール３０は、通信部３１、制御部３２、記憶部３３を備える。以下にこれらの各部の処理を説明する。

【００３９】

通信部３１は、接続されるモバイル端末１０、認証管理サーバ２０、ファイアウォール３０およびサーバ４０との間でやり取りする各種情報に関する通信を制御する。具体的には、通信部３１は、ユーザＩＤやパスワードを認証管理サーバ２０から受信し、ユーザＩＤ、パスワードの問い合わせをサーバ４０に送信する。また、通信部３１は、接続先のコンピュータ名一覧をサーバ４０から受信し、その接続先のコンピュータ名一覧を認証管理サーバ２０に送信する。

【００４０】
また、通信部３１は、選択指示された接続先のコンピュータ名をモバイル端末１０から受信し、そのコンピュータ名をサーバ４０に送信する。また、通信部３１は、リモート接続が許可されたクライアントＰＣ５０（以下、接続先コンピュータという）のＩＰアドレスをサーバ４０から受信する。また、通信部３１は、接続先端末情報（ＩＰアドレス）と、開放するポートのポート番号をモバイル端末１０に送信する。また、通信部３１は、リモート接続をモバイル端末１０から受信する。
【００４１】
記憶部３３は、制御部３２による各種処理に必要なデータおよびプログラムを格納するものであり、特に本発明に密接に関連するものとしては、ポート管理テーブル３３ａ、モバイル端末ＩＰ管理テーブル３３ｂ、ＤＮＳ情報３３ｃを記憶する。
【００４２】
ポート管理テーブル３３ａは、接続先コンピュータのＩＰアドレスと、開放される外部ポートのポート番号とを対応付けて記憶する。具体的には、図６に例示するように、ポート管理テーブル３３ａは、接続先コンピュータの「ＩＰアドレス」と、開放されるポートのポート番号を示す「外部ポート」とを対応付けて記憶する。例えば、図６の例を用いて説明すると、ＩＰアドレス「１７２．１６．１．１１」と、外部ポート「９００４」とを対応付けて記憶している。
【００４３】
モバイル端末ＩＰ管理テーブル３３ｂは、認証の要求を行ったモバイル端末１０のグローバルＩＰを記憶する。具体的には、図７に例示するように、モバイル端末ＩＰ管理テーブル３３ｂは、認証の要求を行ったモバイル端末１０のグローバルＩＰである「モバイル端末グローバルＩＰ」を記憶する。例えば、図７の例を用いて説明すると、モバイル端末グローバルＩＰとして「１９２．０．２．０／２４」を記憶する。
【００４４】
また、ＤＮＳ情報３３ｃは、ファイアウォール３０のＤＮＳである。例えば、記憶部３３は、図８に例示するように、ファイアウォール３０のＤＮＳ情報として「ｊｗ４０１０００００１１．ｅｘａｍｐｌｅ．ｊｐ」を記憶する。なお、記憶部３３は、このＤＮＳ情報の代わりに、ファイアウォール３０の固定ＩＰを記憶していてもよく、例えば、ファイアウォール３０の固定ＩＰとして「１１１．２２２．３３．４４」を記憶する。
【００４５】
制御部３２は、各種の処理手順などを規定したプログラムおよび所要データを格納するための内部メモリを有し、これらによって種々の処理を実行するが、特に本発明に密接に関連するものとしては、認証部３２ａ、格納部３２ｂ、登録部３２ｃ、送信部３２ｄ、接続確立部３２ｅおよび切断部３２ｆを有する。
【００４６】
認証部３２ａは、認証管理サーバ２０を介してモバイル端末１０から認証の要求を受け付けると、該モバイル端末１０の認証を行う。具体的には、認証部３２ａは、認証管理サーバ２０を介してモバイル端末１０から認証の要求を受け付けるとともに、ユーザＩＤ、パスワードおよびモバイル端末１０のグローバルＩＰを受け付ける。そして、認証部３２ａは、ユーザＩＤおよびパスワードがサーバ４０に事前に登録されているものと一致するか否かを問い合わせ、ユーザＩＤおよびパスワードがサーバ４０に事前に登録されているものと一致するものである場合には、モバイル端末１０が正当であると判定する。
【００４７】
格納部３２ｂは、認証部３２ａによってモバイル端末１０の認証を行った結果、該モバイル端末１０が正当であると判定した場合には、該モバイル端末１０のグローバルＩＰをモバイル端末ＩＰ管理テーブル３３ｂに格納する。
【００４８】
登録部３２ｃは、サーバ４０から接続先コンピュータのＩＰアドレスを受信すると、該ＩＰアドレスとモバイル端末１０の接続を許可するポートを識別するポート番号とを対応

付けて登録する。具体的には、登録部３２ｃは、サーバ４０から接続先コンピュータのＩＰアドレスとともにポートマッピングの指示を受け付けると、サーバ４０から接続先コンピュータのＩＰとモバイル端末１０の接続を許可するポートを識別するポート番号とを紐付けてポート管理テーブル３３ａに登録する。

【００４９】

送信部３２ｄは、登録された接続先コンピュータのＩＰアドレスとポート番号とを、モバイル端末１０に送信する。なお、送信部３２ｄは、暗号化を行って、ＩＰアドレスとポート番号をモバイル端末１０に送るようにしてもよい。例えば、ＴＣＰヘッダ（ポート番号）だけを暗号化したり、ユーザデータだけを暗号化する等により、処理速度をできるだけ低下させずに、さらにセキュリティレベルを向上させることが考えられる。その他、ポート番号をスクランブル処理することで、セキュリティレベルを向上させることも考えられる。

【００５０】

接続確立部３２ｅは、モバイル端末１０からリモート接続の要求を受け付けると、該モバイル端末１０のグローバルＩＰを取得し、取得したグローバルＩＰと、モバイル端末ＩＰ管理テーブル３３ｂに格納されたグローバルＩＰとを比較し、両グローバルＩＰが一致する場合には、モバイル端末１０と接続先コンピュータとのリモート接続を確立する。また、接続確立部３２ｅは、接続先コンピュータの電源がオフである場合には、該接続先コンピュータをＷａｋｅ　ｏｎ　ＬＡＮの起動指示で接続先コンピュータを起動させた後に、リモート接続を確立する。なお、ここでリモート接続を確立するのは、クライアントＰＣ５０であってもよいし、サーバ４０上で動作する仮想クライアントＰＣ４０ａであってもよい。

【００５１】

切断部３２ｆは、接続確立部３２ｅによってモバイル端末１０と接続先コンピュータとのリモート接続を確立した後に、所定時間（例えば、１時間）が経過したか否かを監視し、所定時間が経過した場合には、接続を許可したポートを閉じてリモート接続を切断する。なお、リモート接続を切断するタイミングは、任意に設定することができる。例えば、モバイル端末１０を操作しているユーザがセッションを終了させた場合には、すぐにポートを閉じてリモート接続を切断するようにしてもよい。

【００５２】

［サーバ４０の構成］

次に、図９を用いて、図１に示したサーバ４０の構成を説明する。図９は、実施例１に係るサーバ４０の構成を示すブロック図である。図９に示すように、このサーバ４０は、通信部４１、制御部４２、記憶部４３を備える。以下にこれらの各部の処理を説明する。

【００５３】

通信部４１は、接続されるファイアウォール３０およびクライアントＰＣ５０との間でやり取りする各種情報に関する通信を制御する。具体的には、通信部４１は、ファイアウォール３０からユーザＩＤおよびパスワードの問い合わせを受信する。また、通信部４１は、認証管理サーバ２０に契約状況の問い合わせを送信する。また、通信部４１は、接続先のコンピュータ名一覧をファイアウォール３０に送信する。また、通信部４１は、接続先コンピュータのＩＰアドレスとともに、ポートマッピングの指示をファイアウォール３０に送信する。

【００５４】

記憶部４３は、制御部４２による各種処理に必要なデータおよびプログラムを格納するものであり、特に本発明に密接に関連するものとしては、ＩＤ管理テーブル４３ａ、接続先管理テーブル４３ｂ、ユーザ契約コード４３ｃ、アクセス管理テーブル４３ｄを記憶する。

【００５５】

ＩＤ管理テーブル４３ａは、事前準備で登録されたユーザＩＤおよびパスワードの組を記憶する。具体的には、ＩＤ管理テーブル４３ａは、図１０に例示するように、ユーザを

一意に識別する「ユーザＩＤ」と、認証時に使用される「パスワード」とを対応付けて記憶する。例えば、図１０の例を用いて説明すると、ＩＤ管理テーブル４３ａは、ユーザＩＤ「ｍｅｒｃｕｒｙ」と、パスワード「ｓｕｉｓｅｉ０１」とを対応付けて記憶する。

【００５６】

接続先管理テーブル４３ｂは、リモート接続されるクライアントＰＣ５０に関する情報を記憶する。具体的には、接続先管理テーブル４３ｂは、図１１に例示するように、各クライアントＰＣ５０について、「コンピュータ名」と、「ＩＰアドレス」と、「ＭＡＣアドレス」と、実機か仮想クライアントＰＣであるかを示す「実機／仮想」と、接続される内部のポート番号を示す「内部ポート」と、最新の状態を示す「状態」とを対応付けて記憶する。例えば、図１１の例を用いて説明すると、接続先管理テーブル４３ｂは、コンピュータ名「ＷＯＲＫＡＺ０１２３」と、ＩＰアドレス「１７２．１６．１．１１」と、ＭＡＣアドレス「０２－Ａ３－３２－５Ｄ－３Ｃ－４３」と、実機／仮想「実機」と、内部ポート「３３８９」と、状態「接続可能」とを対応付けて記憶する。

【００５７】

ユーザ契約コード４３ｃは、契約を一意に識別するコードである。例えば、記憶部４３は、図１２に例示するように、ユーザ契約コードとして「ｔｏｋｙｏ６３４」を記憶する。なお、サーバ４０は、このユーザ契約コードをもとに、認証管理サーバ２０に契約状況を問い合わせる。

【００５８】

アクセス管理テーブル４３ｄは、ユーザごとに、リモート接続可能なクライアントＰＣ５０のコンピュータ名を記憶する。具体的には、アクセス管理テーブル４３ｄは、図１３に例示するように、「ユーザＩＤ」および「コンピュータ名」の項目を有し、「ユーザＩＤ」の行、「コンピュータ」の列に対応するセルに、「アクセス可」または「アクセス不可」を記憶する。例えば、図１３の例を用いて説明すると、ユーザＩＤ「ｍｅｒｃｕｒｙ」は、コンピュータ名が「ＷＯＲＫＡＺ０１２３」、「ＶＷＯＲＫＡＺ－１」、「ＴＥＲＭＩＮＡＬ８」および「ＶＩＲＴ－ＰＣ」のクライアントＰＣ５０全てが「アクセス可」であり、各クライアントＰＣ５０についてリモートアクセスすることが可能であることを示している。

【００５９】

また、ユーザＩＤ「ｖｅｎｕｓ」は、コンピュータ名が「ＷＯＲＫＡＺ０１２３」および「ＶＩＲＴ－ＰＣ」のクライアントＰＣ５０が「アクセス可」であり、「ＶＷＯＲＫＡＺ－１」および「ＴＥＲＭＩＮＡＬ８」のクライアントＰＣ５０が「アクセス不可」であり、コンピュータ名が「ＷＯＲＫＡＺ０１２３」および「ＶＩＲＴ－ＰＣ」のクライアントＰＣ５０についてはリモートアクセスすることが可能であり、「ＶＷＯＲＫＡＺ－１」および「ＴＥＲＭＩＮＡＬ８」のクライアントＰＣ５０についてはリモートアクセスすることが出来ないことを示している。

【００６０】

制御部４２は、各種の処理手順などを規定したプログラムおよび所要データを格納するための内部メモリを有し、これらによって種々の処理を実行するが、特に本発明に密接に関連するものとしては、事前登録部４２ａ、問い合わせ部４２ｂ、一覧通知部４２ｃ、アドレス通知部４２ｄを有する。

【００６１】

事前登録部４２ａは、クライアントＰＣ５０からユーザＩＤおよびパスワードを受け付けて事前にＩＤ管理テーブル４３ａに登録する。つまり、事前登録部４２ａは、モバイル端末１０が認証の要求を行う際に入力するユーザＩＤおよびパスワードが正当なものか否かを認証するために、事前に正当なユーザＩＤおよびパスワードをＩＤ管理テーブル４３ａに登録する。この他、モバイル端末１０からの事前登録依頼を受け付けて事前登録するようにしても良い。

【００６２】

問い合わせ部４２ｂは、ファイアウォール３０によってモバイル端末１０が正当である

と認証された場合には、モバイル端末１０と接続先コンピュータとのリモート接続を確立する契約が有効であるか否かを認証管理サーバ２０に問い合わせる。具体的には、問い合わせ部４２ｂは、ファイアウォール３０によってモバイル端末１０が正当であると認証された場合には、ユーザ契約コードを記憶部４３から読み出し、該ユーザ契約コードをもとに、認証管理サーバ２０に契約状況を問い合わせる。そして、問い合わせ部４２ｂは、認証管理サーバ２０から契約が有効であるか否かを示す契約状況を受信する。

【００６３】

一覧通知部４２ｃは、契約が有効であった場合であった場合には、接続先コンピュータ名の一覧をモバイル端末１０に通知する。具体的には、一覧通知部４２ｃは、契約が有効であった場合には、アクセス管理テーブル４３ｄを参照し、ユーザＩＤからアクセス可能なクライアントＰＣ５０を特定し、アクセス可能なクライアントＰＣ５０のコンピュータ名一覧をモバイル端末１０に通知する。例えば、図１３の例を用いて説明すると、ユーザＩＤが「ｖｅｎｕｓ」である場合には、アクセス可能なクライアントＰＣ５０が「ＷＯＲＫＡＺ０１２３」および「ＶＩＲＴ－ＰＣ」であると特定し、「ＷＯＲＫＡＺ０１２３」および「ＶＩＲＴ－ＰＣ」をアクセス可能なコンピュータ名一覧としてモバイル端末１０に通知する。

【００６４】

アドレス通知部４２ｄは、ファイアウォール３０によってモバイル端末１０が正当であると認証された場合には、モバイル端末１０が接続する接続先コンピュータのＩＰアドレスをファイアウォール３０に通知する。具体的には、アドレス通知部４２ｄは、ファイアウォール３０によってモバイル端末１０が正当であると認証された場合には、モバイル端末１０が接続する接続先コンピュータのＩＰアドレスをファイアウォール３０に通知するとともに、ポートマッピングを指示する。

【００６５】

以上のように、接続認証システム１００に含まれるモバイル端末１０、認証管理サーバ２０、ファイアウォール３０およびサーバ４０の構成それぞれについて説明した。ここで、図１４を用いて、接続認証システム１００における認証処理およびリモート接続処理の概要について説明する。図１４は、接続認証システムにおける認証処理および接続処理の概要について説明する図である。

【００６６】

図１４に示すように、接続認証システム１００では、まず、認証を要求するモバイル端末１０は、認証管理サーバ２０を介して認証の要求を行う（図１４の（１）参照）。ここで、ファイアウォール３０は、特定の認証管理サーバ２０からのアクセスのみを許可しているため、モバイル端末１０との間で認証処理を直接行うのではなく、認証管理サーバ２０を経由してモバイル端末１０の認証を行う。このため、認証処理の安全性を向上させることができる。

【００６７】

そして、ファイアウォール３０は、認証を行った結果、モバイル端末１０のリモート接続を許可する場合には、開放する外部ポートのポート番号をモバイル端末１０に通知する（図１４の（２）参照）。その後、モバイル端末１０とクライアントＰＣ５０ｂとのリモート接続が確立する（図１４の（３）参照）。上記の認証処理は、認証管理サーバ２０を介して行われたが、接続処理は、ファイアウォール３０を通して、モバイル端末１０とクライアントＰＣ５０ｂとがダイレクトに行う。このため、ＶＰＮ等の暗号化処理を行った場合や外部の認証サーバを中間に介在させた場合等に比して、通信負荷を軽減し、通信速度の低下を軽減することができる。なお、図１４の例では、便宜上、リモート接続として、モバイル端末１０とクライアントＰＣ５０ｂとが直接矢印で繋がっているが、実際はファイアウォール３０を介して接続されているものとする。

【００６８】

そこで、図１５を用いて、接続認証システム１００における接続処理について具体的に説明する。図１５は、接続認証システムにおけるリモート接続処理について説明する図で

ある。図１５の例では、モバイル端末１０ａとクライアントＰＣ５０ａとがリモート接続しているものとし、モバイル端末１０ｂとクライアントＰＣ５０ｂとがリモート接続しているものとする。また、図１５の例では、モバイル端末１０ａのＩＰアドレスが「Ａ」であり、モバイル端末１０ｂのＩＰアドレスが「Ｂ」であり、クライアントＰＣ５０ａのＩＰアドレスが「１７２．１６．１．１１」であり、クライアントＰＣ５０ｂのＩＰアドレスが「１７２．１６．１．２１」であるものとする。

【００６９】

また、図１５の例では、ファイアウォール３０は、図６に例示したポート管理テーブル３３ａにおいて、クライアントＰＣ５０ａのＩＰアドレス「１７２．１６．１．１１」と外部ポート「９００４」とが紐付けしており、また、ＩＰアドレス「１７２．１６．１．２１」と外部ポート「９００５」とが紐付けしているものとする。

【００７０】

そして、ファイアウォール３０は、モバイル端末１０ａから外部ポート「９００４」宛パケットを受け付けると、外部ポート「９００４」に紐付けられたＩＰアドレス「１７２．１６．１．１１」をポート管理テーブル３３ａから取得し、ＩＰアドレス「１７２．１６．１．１１」に対応する内部ポート「３３８９」（図示せず）にパケットを転送する。

【００７１】

また、同様に、ファイアウォール３０は、モバイル端末１０ｂから外部ポート「９００５」宛パケットを受け付けると、外部ポート「９００５」に紐付けられたＩＰアドレス「１７２．１６．１．２１」をポート管理テーブル３３ａから取得し、ＩＰアドレス「１７２．１６．１．２１」に対応する内部ポート「３３８９」にパケットを転送する。

【００７２】

このように、ファイアウォール３０は、ＩＰアドレスとポート番号との紐付け、すなわちポートマッピングを行って、認証したモバイル端末１０ａ、１０ｂに限定して通信を許可しているため、例えば、不正な通信を行う者７０が認証した端末以外の端末を用いて、不正に会計事務所内の所内ＬＡＮに侵入しようとした場合であっても侵入を防止することができる。

【００７３】

［接続認証システムによる処理］

次に、図１６を用いて、実施例１に係る接続認証システム１００による処理を説明する。図１６は、接続認証システムによる全体の処理の流れを示すシーケンス図である。

【００７４】

まず、接続認証システム１００では、認証処理および接続処理を行う前に、事前準備として、ステップＳ１～ステップＳ３の処理を行う。図１６に示すように、接続認証システム１００のサーバ４０は、事前準備として、ユーザＩＤおよびパスワードの登録をクライアントＰＣ５０から受け付け（ステップＳ１）、ユーザＩＤとパスワードの組をＩＤ管理テーブル４３ａに登録する。

【００７５】

続いて、サーバ４０は、ファイアウォール３０からＤＮＳ情報３３ｃを取得する（ステップＳ２）。なお、ＤＮＳ情報の代わりに固定ＩＰでもよい。そして、サーバ４０は、認証管理サーバ２０へアクセスするＵＲＬをメールでモバイル端末１０に対して通知する（ステップＳ３）。なお、このＵＲＬは、ファイアウォール３０内のＤＮＳ情報と認証管理サーバ２０のＵＲＬの組み合わせである。

【００７６】

そして、モバイル端末１０は、メールで受け取ったＵＲＬを用いて、認証管理サーバ２０にアクセスして、ユーザＩＤおよびパスワードを入力して認証の要求を行う（ステップＳ４）。

【００７７】

ここで、ステップＳ４において、認証の要求を行う際にブラウザ上に表示される画面例を図１７に例示する。図１７に示すように、メールで受け取ったアクセス先のＵＲＬのパ

ラメータからファイアウォール３０のＤＮＳ情報である「接続先アドレス」が自動で入力される。また、「ユーザＩＤ」および「パスワード」の項目には、ユーザのアカウントが入力される。このように、モバイル端末１０から認証管理サーバ２０へブラウザベースでアクセスして認証処理を行うことができるので、ＯＳ毎にアプリを用意する必要がないので、汎用性が高くなる。

【００７８】

次に、認証管理サーバ２０は、モバイル端末１０からユーザＩＤおよびパスワードの入力を受け付けると、モバイル端末１０のグローバルＩＰを取得し、受け付けたユーザＩＤおよびパスワードとともに、モバイル端末１０のグローバルＩＰをファイアウォール３０に送信する（ステップＳ５）。

【００７９】

そして、ファイアウォール３０は、認証管理サーバ２０を介してユーザＩＤ、パスワードおよびモバイル端末１０のグローバルＩＰを受け付けると、ユーザＩＤおよびパスワードがサーバ４０に事前に登録されているものと一致するか否かを問い合わせる（ステップＳ６）。この結果、ファイアウォール３０は、ユーザＩＤおよびパスワードがサーバ４０に事前に登録されているものと一致するものである場合には、モバイル端末１０が正当であると判定する。また、ファイアウォール３０は、モバイル端末１０が正当であると判定した場合には、該モバイル端末１０のグローバルＩＰをモバイル端末ＩＰ管理テーブル３３ｂに格納する。

【００８０】

そして、サーバ４０は、ファイアウォール３０によってモバイル端末１０が正当であると認証された場合には、モバイル端末１０と接続先コンピュータとのリモート接続を確立する契約が有効であるか否かを認証管理サーバ２０に問い合わせる（ステップＳ７）。その後、認証管理サーバ２０は、サーバ４０から問い合わせを受け付けた場合には、契約状況が有効であるか否かを確認し、契約状況をサーバ４０に応答する（ステップＳ８）。

【００８１】

そして、サーバ４０は、契約が有効であった場合には、アクセス管理テーブル４３ｄを参照し、アクセス可能なクライアントＰＣ５０を特定し、アクセス可能なクライアントＰＣ５０のコンピュータ名一覧を、ファイアウォール３０および認証管理サーバ２０を介して、モバイル端末１０に通知する（ステップＳ９）。

【００８２】

そして、モバイル端末１０は、サーバ４０から通知された接続先クライアント端末の一覧のうち、ユーザによって選択指示されたコンピュータ名をファイアウォール３０に通知する（ステップＳ１０）。ここで、図１８を用いて、モバイル端末１０におけるコンピュータ名一覧の表示画面例について説明する。図１８に例示するように、「認証に成功しました　接続先のコンピュータを選択してくだい」というメッセージとともに、接続可能なコンピュータ名が４つ表示されている。モバイル端末１０は、表示されているコンピュータ名のなかから接続先のコンピュータの選択指示を受け付ける。なお、図１８の例では、接続可能な全てのコンピュータ名が４つ表示されているが、接続先の端末の（各ユーザ毎の）アクセス権限に対応して、表示される数を制限するようにしてもよい。

【００８３】

続いて、ファイアウォール３０は、接続先コンピュータ名をサーバ４０に渡す（ステップＳ１１）。そして、サーバ４０は、受け取った接続先コンピュータ名の接続先コンピュータの最新状態を取得し（ステップＳ１２）、接続先管理テーブル内の「状態」を更新する。

【００８４】

そして、サーバ４０は、ファイアウォール３０によってモバイル端末１０が正当であると認証された場合には、モバイル端末１０が接続する接続先コンピュータのＩＰアドレスをファイアウォール３０に通知するとともに、ポートマッピングを指示する（ステップＳ１３）。ファイアウォール３０は、サーバ４０から接続先コンピュータのＩＰアドレスと

ともにポートマッピングの指示を受け付けると、サーバ４０から接続先コンピュータのＩＰとモバイル端末１０の接続を許可するポートを識別するポート番号とを紐付けてポート管理テーブル３３ａに登録する。

【００８５】

続いて、ファイアウォール３０は、登録された接続先コンピュータのＩＰアドレスとポート番号とを、モバイル端末１０に通知する（ステップＳ１４）。なお、ファイアウォール３０は、通知した直後からタイムアウトを監視する。そして、モバイル端末１０は、ＲＤＰツールにより接続アドレス、ポート番号を取得して、リモート接続をファイアウォール３０へ要求する（ステップＳ１５）。

【００８６】

ここで、ファイアウォール３０から接続先コンピュータのＩＰアドレスとポート番号とが通知されたモバイル端末１０の画面表示例を図１９に示す。図１９に例示するように、接続先コンピュータの「コンピュータ名」および接続先コンピュータとの接続状態を示す「状態」が表示されるとともに、状態が「接続可能」である場合には、通知された「接続先アドレス」と「ポート番号」とが表示される。図１９の例では、接続先アドレスとして「ｊｗ４０１０００００１ａ．ｅｘａｍｐｌｅ．ｊｐ」、ポート番号として「９００４」が表示されている。

【００８７】

続いて、ファイアウォール３０は、モバイル端末１０からリモート接続の要求を受け付けると、該モバイル端末１０のグローバルＩＰを取得し、取得したグローバルＩＰと、モバイル端末ＩＰ管理テーブル３３ｂに格納されたグローバルＩＰとを比較して認証する（ステップＳ１６）。

【００８８】

この結果、ファイアウォール３０は、両グローバルＩＰが一致する場合には、モバイル端末１０と接続先コンピュータとのリモート接続を確立する（ステップＳ１７）。なお、接続先コンピュータの電源がオフである場合には、該接続先コンピュータをＷａｋｅ　ｏｎ　ＬＡＮの起動指示で接続先コンピュータを起動させた後に、リモート接続を確立する。また、リモート接続を確立する時や確立後のモバイル端末１０と接続先コンピュータ間のデータ通信は暗号化により、セキュリティが保たれている。

【００８９】

その後、ファイアウォール３０は、モバイル端末１０と接続先コンピュータとのリモート接続を確立した後に、所定時間（例えば、１時間）が経過したか否かを監視し、タイムアウトとなった場合には、接続を許可したポートを閉じてリモート接続を切断する（ステップＳ１８）。

【００９０】

[実施例１の効果]

上述してきたように、実施例１に係る認証接続システム１００では、認証処理については、認証管理サーバ２０を介して行うことで安全性を高め、一方、接続処理については、ファイアウォール３０を通してモバイル端末１０とクライアントＰＣ５０とでダイレクトに行うことで、通信負荷を軽くしている。これにより、認証接続サーバ１００では、通信負荷による通信速度の低下を軽減するとともに、安全性を高くすることが可能である。

【００９１】

また、実施例１によれば、サーバ４０は、ファイアウォール３０によってモバイル端末１０が正当であると判定した場合であって、接続先コンピュータが複数ある場合には、接続先クライアント端末の一覧をモバイル端末に通知する。そして、モバイル端末１０は、サーバから通知された接続先コンピュータの一覧のうち、ユーザによって選択指示された接続先クライアントを識別するコンピュータ名をファイアウォール３０に通知する。このため、リモート接続可能な接続先コンピュータが複数ある場合には、ユーザに接続先コンピュータを選択させることが可能である。

【００９２】

また、実施例１によれば、ファイアウォール３０のＤＮＳ情報または固定ＩＰと、認証管理サーバ２０のＵＲＬとが組み合わされた特定のＵＲＬを用いて、認証管理サーバ２０にアクセスし、認証の要求を行う。このため、ファイアウォール３０から取得されたＤＮＳ情報または固定ＩＰからＵＲＬを生成するので、接続先を生成する時点から、安全性を高くすることが可能である。

【００９３】

また、実施例１によれば、ファイアウォール３０によってモバイル端末１０が正当であると判定した場合には、モバイル端末１０と接続先コンピュータのリモート接続を確立する契約が有効であるか否かを認証管理サーバ２０に問い合わせるので、契約状況を確認して、リモート接続の許可または拒否をサーバ４０で判断することができる結果、不正利用を防止することが可能である。

【００９４】

また、実施例１によれば、ファイアウォール３０は、モバイル端末１０と接続先コンピュータとのリモート接続を確立した後に、所定時間が経過したか否かを監視し、所定時間が経過した場合には、接続を許可したポートを閉じてリモート接続を切断する。このため、リモート接続終了後はポートを自動で閉じるので、外部用にポートを開放する時間が最小限となり、安全性を高くすることが可能である。

【００９５】

また、実施例１によれば、接続先コンピュータの電源がオフである場合には、該接続先コンピュータを起動指示で起動させた後に、リモート接続を確立する。このため、電源ＯＦＦのコンピュータへリモート接続する時は、Ｗａｋｅ　Ｏｎ　ＬＡＮで電源ＯＮしてからリモート接続するので、利便性を高くすることが可能である。

【００９６】

また、実施例１によれば、接続コンピュータに代えて、該接続コンピュータをサーバ４０上で仮想的に構築された仮想クライアントＰＣ４０ａとモバイル端末１０とのリモート接続を確立するので、仮想クライアントＰＣ４０ａへのリモート接続も出来るようになる結果、利便性を向上させることが可能である。

【００９７】

なお、図示した各装置の各構成要素は機能概念的なものであり、必ずしも物理的に図示の如く構成されていることを要しない。すなわち、各装置の分散・統合の具体的形態は図示のものに限られず、その全部または一部を、各種の負荷や使用状況などに応じて、任意の単位で機能的または物理的に分散・統合して構成することができる。さらに、各装置にて行なわれる各処理機能は、その全部または任意の一部が、ＣＰＵおよび当該ＣＰＵにて解析実行されるプログラムにて実現され、あるいは、ワイヤードロジックによるハードウェアとして実現され得る。

【００９８】

また、本実施例において説明した各処理のうち、自動的におこなわれるものとして説明した処理の全部または一部を手動的におこなうこともでき、あるいは、手動的におこなわれるものとして説明した処理の全部または一部を公知の方法で自動的におこなうこともできる。この他、上記文書中や図面中で示した処理手順、制御手順、具体的名称、各種のデータやパラメータを含む情報については、特記する場合を除いて任意に変更することができる。

【００９９】

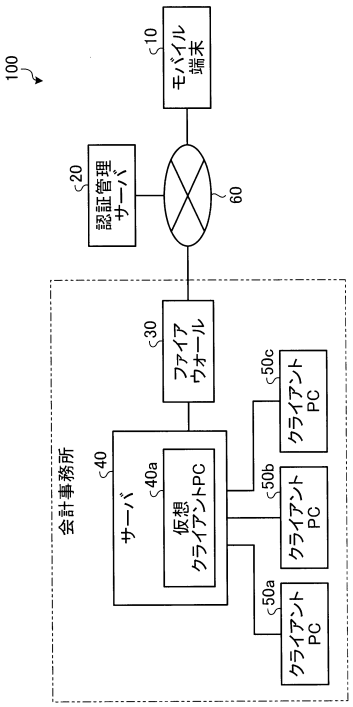
また、本実施例で説明した接続認証方法は、あらかじめ用意されたプログラムをパーソナルコンピュータやワークステーションなどのコンピュータで実行することによって実現することができる。このプログラムは、インターネットなどのネットワークを介して配布することができる。また、このプログラムは、ハードディスク、フレキシブルディスク（ＦＤ）、ＣＤ－ＲＯＭ、ＭＯ、ＤＶＤなどのコンピュータで読み取り可能な記録媒体に記録され、コンピュータによって記録媒体から読み出されることによって実行することもできる。

【符号の説明】

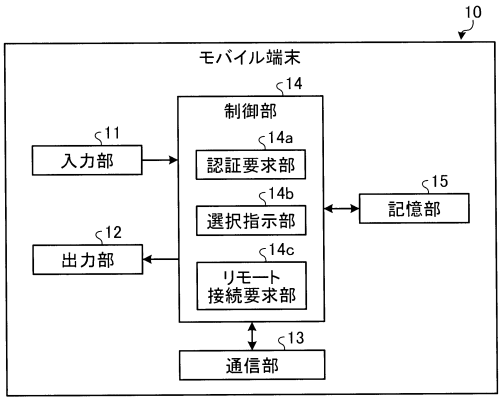
【０１００】

１０　モバイル端末
１１　入力部
１２　出力部
１３　通信部
１４　制御部
１４ａ　認証要求部
１４ｂ　選択指示部
１４ｃ　リモート接続要求部
１５　記憶部
２０　認証管理サーバ
３０　ファイアウォール
４０　サーバ
４０ａ　仮想クライアントＰＣ
５０ａ～５０ｃ　クライアントＰＣ
１００　接続認証システム

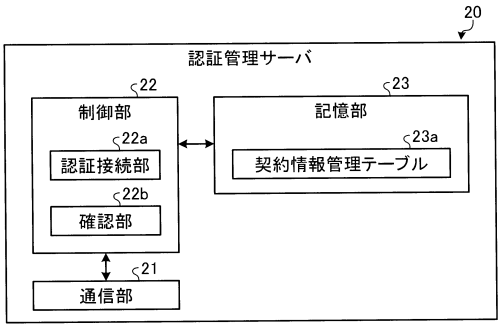
【図１】



【図２】



【図３】

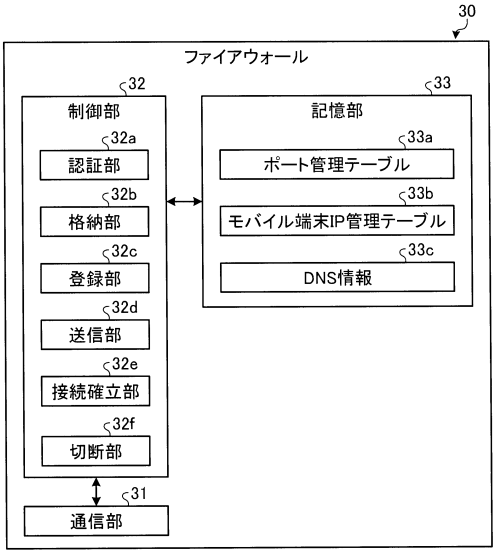


【図４】

契約情報管理テーブル

ユーザ契約コード	契約状況
tokyo634	有効
aomori08	無効
akita14	無効
chiba53	有効
⋮	⋮

【図５】



【図６】

ポート管理テーブル

IPアドレス	外部ポート
172.16.1.11	9004

【図７】

モバイル端末IP管理テーブル

モバイル端末グローバルIP
192.0.2.0/24
⋮

【図８】

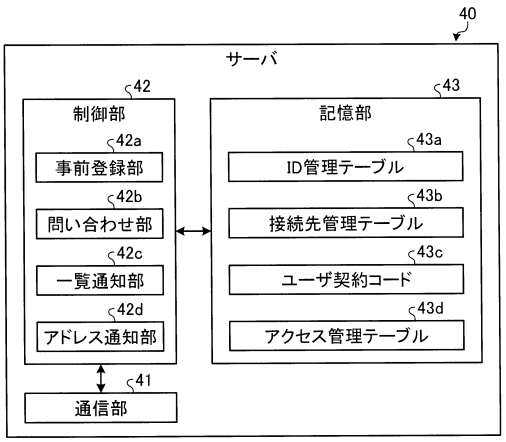
DNS情報

jw401000011.example.jp

固定IP

111.222.33.44

【図９】



【図１０】

ID管理テーブル

ユーザID	パスワード
mercury	suisei01
venus	kinsei02
⋮	⋮

【図１１】

接続先管理テーブル

コンピュータ名	IPアドレス	MACアドレス	実機/仮想	内部ポート	状態
WORKAZ0123	172.16.1.11	02-A3-32-5D-3C-43	実機	3389	接続可能
VWORKAZ-1	172.16.1.21	02-A3-32-5E-2A-27	実機	3389	電源OFF
TERMINAL8	172.16.1.31	12-C5-7A-6C-88-28	実機	3389	使用中
VIRT-PC	172.16.1.41	28-D8-6E-5B-76-36	仮想	3389	接続可能
…	…	…	…	…	…

【図１２】

ユーザ契約コード

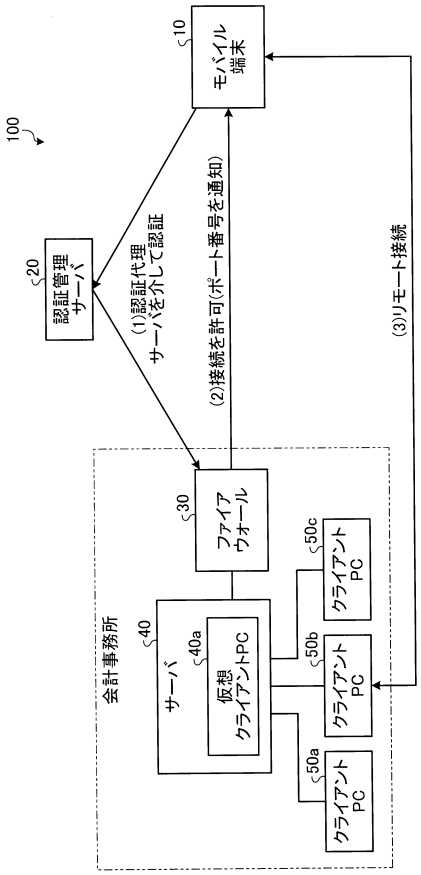
ユーザ契約コード
tokyo634

【図１３】

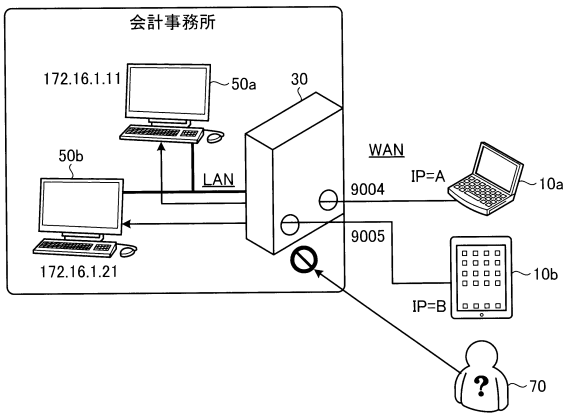
アクセス管理テーブル

	コンピュータ名				
ユーザID	WORKAZ0123	VWORKAZ-1	TERMINAL8	VIRT-PC	…
mercury	アクセス可	アクセス可	アクセス可	アクセス可	…
venus	アクセス可	アクセス不可	アクセス不可	アクセス可	…
…	…	…	…	…	…

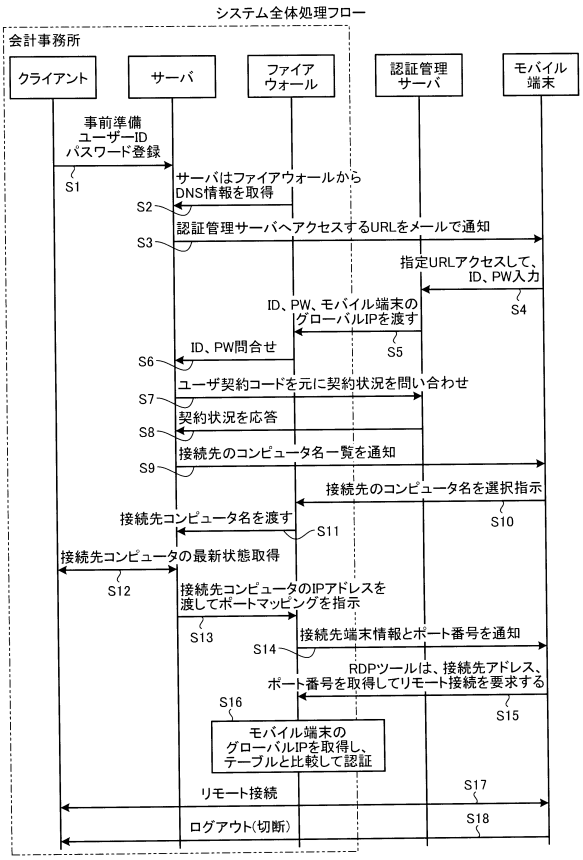
【図１４】



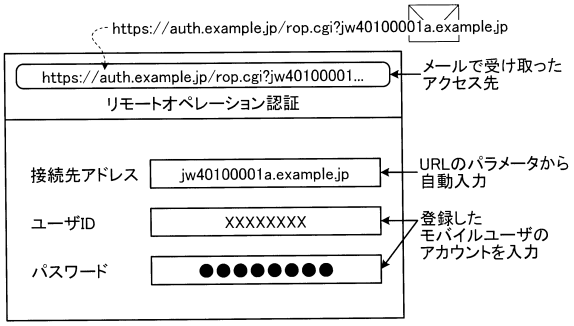
【図１５】



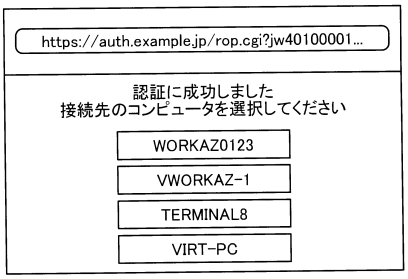
【図１６】



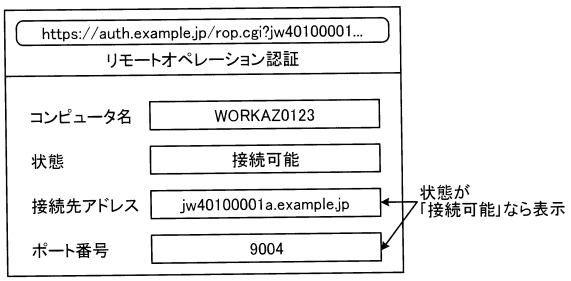
【図１７】



【図１８】



【図１９】



フロントページの続き

審査官　森谷　哲朗

(56)参考文献　特開２００５－０１２７７５（ＪＰ，Ａ）
特開２０１０－２７８７７８（ＪＰ，Ａ）
国際公開第２００６／０９０４６５（WO，Ａ１）
特開２００６－１４８６６１（ＪＰ，Ａ）
特開２０１３－０９８７７８（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　１２／６６
Ｇ０６Ｆ　２１／４１
Ｇ０６Ｆ　１３／００