(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2005-242547
(P2005-242547A)
(43)公開日　平成17年9月8日(2005.9.8)

(51)Int.Cl.[7]	F I			テーマコード（参考）
G06F 15/00	G06F	15/00	330A	5B085
G06F 13/00	G06F	13/00	510A	5J104
H04L 9/08	H04L	9/00	601B	

審査請求 未請求　請求項の数 10　ＯＬ　（全 9 頁）

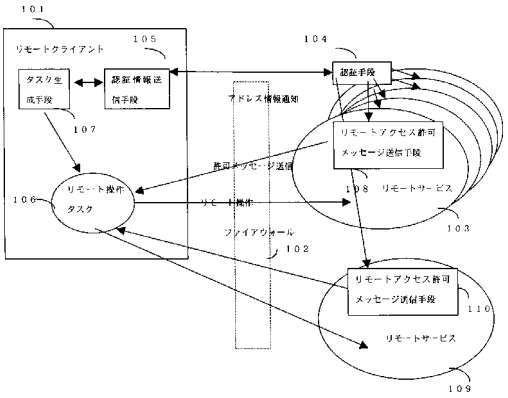
(21)出願番号　特願2004-49648(P2004-49648)
(22)出願日　平成16年2月25日(2004.2.25)

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真１００６番地
(74)代理人　100097445
弁理士　岩橋　文雄
(74)代理人　100103355
弁理士　坂口　智康
(74)代理人　100109667
弁理士　内藤　浩樹
(72)発明者　伊藤　由起子
大阪府門真市大字門真１００６番地　松下電器産業株式会社内
(72)発明者　張　聰
大阪府門真市大字門真１００６番地　松下電器産業株式会社内

最終頁に続く

(54)【発明の名称】リモートサービス実行方法、リモートクライアント及びリモートサービスサーバ

(57)【要約】
【課題】外部ネットワークからのアクセスを制限することによってセキュリティを強化したリモート操作サービスを、ユーザに使い勝手よく提供する。サービスが複数存在する環境や、リモート操作のトラヒックが大きい環境にも対応できる様にする。
【解決手段】サービスの実施を求める認証情報送信手段１０５と、サービスの実施の許可判断を行う認証手段１０４とを備え、認証情報送信手段１０５は、サービスの実施が許可された場合に、リモートサービス１０３の操作を行うリモート操作タスク１０６のアドレス情報を認証手段１０４に送信し、リモートアクセス許可メッセージ送信手段１０８が認証手段１０４からアドレス情報をうけとって、リモート操作タスク１０６に対してサービス許可メッセージを送信することによってリモート操作を開始する。
【選択図】図１



【特許請求の範囲】
【請求項１】
特定のリモートクライアントにのみ実行が許可されている単数或いは複数のリモートサービスに対して、前記リモートクライアントから前記リモートサービスを実行するリモートサービス実行方法において、
　前記リモートクライアントが前記リモートサービスを実行するためのアドレス情報と、認証データとを送信するステップと、
　前記認証データに基づいて、前記リモートクライアントが要求したリモートサービスの実行を許可するかどうかを判定するステップと、
　前記リモートサービスの実行を許可する場合に、前記アドレス情報を前記リモートサービスに通知するステップと、
　前記アドレス情報に基づいて、前記リモートサービスから前記リモートクライアントとの通信路を設定するステップ
　とで構成されることを特徴とするリモートサービス実行方法。
【請求項２】
前記アドレス情報は前記リモートクライアントのＩＰアドレス及びポート番号であることを特徴とする請求項１記載のリモートサービス実行方法。
【請求項３】
前記リモートクライアントと前記リモートサービスとの間でやりとりされる情報は暗号化されていることを特徴とする請求項１記載のリモートサービス実行方法。
【請求項４】
前記リモートクライアントとの通信路を設定するステップにおいて、前記リモートサービスが鍵情報を送信し、前記リモートクライアントは、前記鍵情報を用いてサービス実行中の送受信データを暗号化及び復号化する
　ことを特徴とする請求項１記載のリモートサービス実行方法。
【請求項５】
前記認証データに基づいて、前記リモートクライアントに対して許可可能なサービスの一覧を前記リモートクライアントに対して通知するステップ
　を更に有することを特徴とする請求項１記載のリモートサービス実行方法。
【請求項６】
前記リモートクライアントが前記リモートサービスとの通信路を設定した後に、通信路を設定した前記リモートサービスが管理する他のリモートサービスの実行を要求するステップと、
　前記通信路を設定したリモートサービスが、前記リモートクライアントの前記アドレス情報を前記他のリモートサービスに対して通知するステップと、
　前記他のリモートサービスから前記リモートクライアントとの通信路を設定するステップ
　を更に有することを特徴とする請求項１記載のリモートサービス実行方法。
【請求項７】
特定のリモートクライアントにのみ実行が許可されている単数或いは複数のリモートサービスに対して、前記リモートサービスを実行するリモートクライアントにおいて、
　前記リモートサービスを実行するためのアドレス情報と、認証データとを送信する認証情報送信手段と、
　前記リモートサービスから設定された通信路を用いてリモートサービスを実行するリモート操作手段
　とを有することを特徴とするリモートクライアント。
【請求項８】
単数或いは複数のリモートサービスを特定のリモートクライアントにのみ実行を許可するリモートサービスサーバにおいて、
　前記リモートクライアントが前記リモートサービスを実行するためのアドレス情報を受

信し、前記アドレス情報に基づいて、前記リモートクライアントとの通信路を設定するリモートアクセス許可メッセージ送信手段
を有することを特徴とするリモートサービスサーバ。
【請求項９】
前記リモートクライアントが前記リモートサービスを実行するためのアドレス情報と、認証データとを受信し、前記認証データに基づいて、前記リモートクライアントに対して前記リモートサービスの実行を許可するかどうかを判定し、前記リモートサービスの実行を許可する場合は、前記アドレス情報を前記リモートアクセス許可メッセージ送信手段に送信する認証手段
を更に有することを特徴とする請求項８記載のリモートサービスサーバ。
【請求項１０】
請求項７記載のリモートクライアントと、請求項９記載のリモートサービスサーバとで構成されることを特徴とするリモートサービスシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、主として、リモートから、アクセスが制限されたサービスを利用するためのリモートサービス実行方法、リモートクライアント及びリモートサービスサーバに関する。
【背景技術】
【０００２】
インターネットの普及によって、ネットワークを介して様々な情報をやりとりするサービスが多々登場してきた。Ｗｅｂをつかった商用サービス、電子メールやＩＰ電話、そしてネット家電などネットワークを利用する機器や用途は様々になりつつあり、増加してきている。ネットワークを用いて必要な情報を簡単に入手したり、機器の制御を行ったりする利便性が増える一方、不正アクセスによる被害もふえつつある。こうした中で、外部ネットワークから、宅内の内部ネットワークへのアクセスを制限するファイアウォールは必須機能となっている。ファイアウォール環境下では、外部ネットワークに接続された機器から、内部ネットワークへの機器へのアクセスは禁止される一方で、内部ネットワークから外部ネットワークへのアクセスは許可されている。しかしながら、外部ネットワーク機器から、内部機器のサービスを利用したいという要求も存在する。
【０００３】
こうした要求の解決手段として、外部ネットワークから内部ネットワークのサービスにアクセスする場合には、認証処理の上、許可したアクセスを内部ネットワークのサービスに中継するリレー手段を設けたものがある（特許文献１参照）。
【特許文献１】特開２００１－３５０７１８号公報
【発明の開示】
【発明が解決しようとする課題】
【０００４】
しかしながら、特許文献１のような従来の構成では、例えば、映像情報の送信など、リモート操作のトラヒックが大きいサービスが存在する環境や、リモート操作を行う宅内の機器やサービスが多数の環境になると、リレー手段の負荷が増大し、サービスに対応できなくなる可能性があるという課題を有していた。
【０００５】
本発明は、前記の課題を解決するもので、ファイアウォール装置に特別な機能をもたせることなく、サービスが多種類存在する環境や、リモート操作のトラヒックが大きい環境でも、特定の機能部に処理負荷を集中させること無くサービスに対応できるリモート操作装置及び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】
【０００６】

前記従来の課題を解決するために、本発明のリモートサービス実行方法は、特定のリモートクライアントにのみ実行が許可されている単数或いは複数のリモートサービスに対して、前記リモートクライアントから前記リモートサービスを実行するリモートサービス実行方法において、前記リモートクライアントが前記リモートサービスを実行するためのアドレス情報と、認証データとを送信するステップと、前記認証データに基づいて、前記リモートクライアントが要求したリモートサービスの実行を許可するかどうかを判定するステップと、前記リモートサービスの実行を許可する場合に、前記アドレス情報を前記リモートサービスに通知するステップと、前記アドレス情報に基づいて、前記リモートサービスから前記リモートクライアントとの通信路を設定するステップとで構成されることを特徴とするものである。

【０００７】

また、本発明のリモートクライアントは、特定のリモートクライアントにのみ実行が許可されている単数或いは複数のリモートサービスに対して、前記リモートサービスを実行するリモートクライアントにおいて、前記リモートサービスを実行するためのアドレス情報と、認証データとを送信する認証情報送信手段と、前記リモートサービスから設定された通信路を用いてリモートサービスを実行するリモート操作手段とを有することを特徴とするものである。

【０００８】

また、本発明のリモートサービスサーバは、単数或いは複数のリモートサービスを特定のリモートクライアントにのみ実行を許可するリモートサービスサーバにおいて、前記リモートクライアントが前記リモートサービスを実行するためのアドレス情報を受信し、前記アドレス情報に基づいて、前記リモートクライアントとの通信路を設定するリモートアクセス許可メッセージ送信手段を有することを特徴とするものである。

【発明の効果】

【０００９】

本発明のリモートサービス実行方法によれば、ファイアウォールによって外部ネットワークからのアクセスが制限され、セキュリティ保護された環境において、認証手段により、許可されたユーザのみにリモート操作サービスを提供できる。さらに、認証手段でサービスの実施が許可された場合に、リモートサービスの操作を行うリモート操作タスクのアドレス情報を前記認証手段に送信し、前記認証手段は、前記アドレス情報を、サービスを許可したリモートサービスのリモートアクセス許可メッセージ送信手段に送信し、前記リモートアクセス許可メッセージ送信手段が前記リモート操作タスクに対してサービス許可メッセージを送信することによって通信路を設定し、リモート操作タスクからのリモート操作を開始する機能を有することにより、許可されたリモート端末とリモートサービス各々が直接通信を行う環境を構築でき、処理の負荷を分散させることが可能となる。

【発明を実施するための最良の形態】

【００１０】

以下本発明の実施の形態について、図面を参照しながら説明する。

【００１１】

（実施の形態１）

図１は、本発明の実施の形態１におけるリモートサービスシステムの構成図である。図１において、１０１はリモート操作を行うリモートクライアントであり、リモートクライアント１０１は、ネットワークを介して様々な機器と通信することができる。１０２は、ファイアウォールであり、内部ネットワークへの外部からのアクセスを禁止している。１０３、１０９は、ファイアウォール１０２の内部ネットワークに存在するリモートサービスである。１０４は、リモートサービス１０３及び１０９について、サービスの利用を許可するかどうかを判断する認証手段である。リモートクライアント１０１には、リモートサービス１０３、１０９の利用を許可するかどうかを判断するための認証情報を送信し、判断を仰ぐ認証情報送信手段１０５と、リモート操作を実行するリモート操作タスク１０６と、リモート操作タスクが動作するアドレスを決定してリモート操作タスク１０６を生

成するタスク生成手段１０７が存在する。リモートサービス１０３には、認証手段１０４がサービスの実施を許可した場合に、リモート操作タスク１０６に対してサービス許可メッセージを送信するリモートアクセス許可メッセージ送信手段１０８が存在する。また、リモートサービス１０９には、認証手段１０４がサービスの実施を許可した場合に、リモート操作タスク１０６に対してサービス許可メッセージを送信するリモートアクセス許可メッセージ送信手段１１０が存在する。

【００１２】

認証情報送信手段１０５と、認証手段１０４の間でやりとりされるメッセージは、暗号化によりセキュアな通信路で実現される。

【００１３】

認証手段１０４では、認証情報と、許可するサービスの種類、それぞれのサービスのアクセス先のアドレス情報を管理している。

【００１４】

図２は、認証手段１０４で管理している認証情報管理テーブルの例である。認証手段１０４では、認証情報として、許可する認証ＩＤのリストを管理している。図２の例では、「ＩＤ１」「ＩＤ２」「ＩＤ３」「ＩＤ４」それぞれが、認証を許可する認証ＩＤを示す。そして、それぞれの認証ＩＤに対応させて、許可するサービスの種類を管理している。表において、「Ｓ１」「Ｓ２」などはそれぞれサービスの種類を示す識別子を示す。たとえば、Ｓ１がネットワークに接続された録画機器への録画予約動作に対応したり、Ｓ２がネットワークに接続されたエアコンの電源操作に対応したり、といったことに対応する。

【００１５】

図３は、認証手段１０４で管理しているリモートサービスへのアクセス先のアドレス情報の例である。リモートサービスの種類ごとにたとえば、アクセス先のＩＰアドレスとポート番号を管理している。

【００１６】

図４は、図１に示したリモート操作装置の動作シーケンス図を示す。以下、図１～図４を用いてリモート操作装置の動作を説明する。

【００１７】

リモートクライアント１０１が、リモートサービス１０３のリモート操作を行う場合、まず、認証情報送信手段１０５が、認証手段１０４に、認証ＩＤとともにサービスの一覧を要求するメッセージを送信する（図４のＳ４０１の矢印）。認証手段１０４は、メッセージを受信すると、対応する認証ＩＤが、認証情報管理テーブルに存在するかどうか調べ、存在する場合には、許可するサービスの一覧を送信する（図４のＳ４０２の矢印）。たとえば、「ＩＤ１」が送信された場合には、「ＩＤ１」で許可しているサービスの種類「Ｓ１、Ｓ２、Ｓ３」が一覧で送信される。認証情報送信手段１０５では、送信されたサービスの一覧の中からサービスを選択する（図４のＳ４０３）。認証情報送信手段１０５は、選択したサービスの種類を認証手段１０２に送信し（図４のＳ４０４）、認証手段１０４はそのサービスの許可判断を行い判断結果を認証情報送信手段１０５に送信する（図４のＳ４０５）。サービスが許可された場合には、認証情報送信手段１０５は、タスク生成手段１０７に依頼し、リモート操作タスクのアドレス、例えばポート番号を決定する（図４のＳ４０６）。そして、決定したアドレスでのリモート操作タスクを生成する（図４のＳ４０７）。認証情報送信手段１０５は、生成したリモート操作タスクのアドレス情報を認証手段１０４に送信し（図４のＳ４０８）、アドレス情報を受信した認証手段１０４は、選択されているリモートサービス１０３のリモートアクセス許可メッセージ送信手段１０８にアドレス情報を送信する（図４のＳ４０９）。このアドレス情報は例えば、ＩＰアドレスとポート番号といったものである。アドレス情報を受信したリモートアクセス許可メッセージ送信手段１０８では、アドレス情報のアドレスに対してサービス許可メッセージを、リモート操作のメッセージ暗号化のための鍵情報とともに送信する。このメッセージは、ファイアウォールの内部ネットワークから外部ネットワークへの通信なので、ファイアウォールを通過することができ、リモートサービス１０３側からリモート操作タスク

１０６との通信路を設定することができる（図４のＳ４１０）。こうして設定された通信路を用いて、リモート操作タスク１０６は、リモートサービス１０９に対して、リモート操作を実行する（図４のＳ４１１）。

【００１８】

かかる構成によれば、認証情報送信手段１０５、認証手段１０４及びリモートアクセス許可メッセージ送信手段１０８を設け、認証許可されたアクセスについては、リモート操作タスクのアドレス情報を認証情報送信手段１０５により通知し、リモートアクセス許可メッセージ送信手段１０８は通知されたアドレスに許可メッセージを送信することにより、許可されたアクセスのみにリモート操作サービスを自動的に提供できる。さらに、許可されたリモート端末とリモートサービス各々が直接通信を行うことができ、処理の負荷を分散させることが可能となる。

【００１９】

また、認証情報送信手段１０５と認証手段１０４でやりとりする情報を暗号化することにより、よりセキュアにリモートサービスを提供できる。

【００２０】

さらに、リモートアクセス許可メッセージ送信手段１０８より、リモート操作タスク１０６とリモートサービス１０３でやりとりする情報の暗号化のための鍵情報を送信する機能を設けることにより、リモート操作情報の秘匿化を実現できる。

【００２１】

なお、本実施の形態の動作シーケンス図において、初めに認証情報送信手段１０５がサービス一覧要求Ｓ４０１を送信し、サービス一覧情報を取得した（Ｓ４０２）が、この手順は必ずしも必須ではない。あらかじめ認証情報送信手段１０５が利用できるサービスの情報を保持している場合もある。

【００２２】

また、サービスの選択情報とともに送信される認証情報は、サービスを利用しようとする認証情報送信手段１０５を識別するためのものであり、認証手段１０４が一覧として記憶している認証ＩＤの値そのものであるとは限らない。たとえば、認証ＩＤによる認証手順実施ののち、認証を許可したセッションＩＤを認証情報として利用する場合なども含める。

【００２３】

なお、認証手段はリモートサービスサーバ内部に含まれず、独立した認証サーバとして構成されても良いし、リモートサービス１０３、１０９及び認証手段１０４がリモートサービスサーバを構成するものとしてもよい。リモートサービスサーバと認証サーバとが独立する場合、リモートサービスサーバと認証サーバとの間でアドレス情報を通信することによって、リモートサービス１０３、１０９及び認証手段１０４がリモートサービスサーバを構成する場合と同様の効果が得られる。

【００２４】

（実施の形態２）

図５は、本発明の実施の形態２のリモート操作装置の動作シーケンス図を示す。

【００２５】

図５において、図４と同様の手順については、同じ符号を用い、説明を省略する。（図５のＳ４０１～Ｓ４１０）図４と同様の手順でサービス許可メッセージを受信したリモート操作タスク１０６は、リモートアクセス許可メッセージ送信手段１０８が存在するリモートサービス１０３に対し、詳細なサービスの一覧を要求する（図５のＳ５０１）。リモートサービス１０３では、提供できる詳細サービスの一覧を記憶している。

【００２６】

図６は、リモートサービス１０３で記憶している提供できる詳細サービスの一覧の例である。リモートサービス１０３は、図６に示したような詳細サービスの一覧をリモート操作タスク１０６に送信する（図５のＳ５０２）。リモート操作タスクでは、詳細サービスの一覧から選択されたサービスの情報をリモートタスク１０３に送信する（図５のＳ５０

３）。指定されたサービスの種類に応じて、該当するリモートタスク１０９のリモートアクセス許可メッセージ送信手段１１０に対し、リモート操作タスクのＩＰアドレス、ポート番号を通知する（図５のＳ５０４）。リモートアクセス許可メッセージ送信手段１１０では、通知されたリモート操作タスクのアドレスに対してサービス許可メッセージを送信し、リモート操作タスク１０６との通信路を確保する（図４のＳ５０５）。こうして設定された通信路を用いて、リモート操作タスク１０６はリモート操作を実行する（図４のＳ５０６）。

【００２７】

かかる構成によれば、リモートサービス１０３が詳細サービスの一覧をリモート操作タスク１０６に提供し、選択されたサービスを実行するリモートサービス１０９にリモート操作タスク１０６のアドレス情報を通知する機能を設けることにより、認証によって許可されるサービスの集合を内部機器の複数のリモートサービスで分散管理することが可能となり、認証手段１０４での管理情報の集中化を避けて、サービスを階層管理することが可能となる。

【産業上の利用可能性】

【００２８】

本発明にかかるリモート操作装置及び方法は、認証手段及びリモートアクセス許可メッセージ送信手段を有し、外部ネットワークにおいて、ファイアウォールでセキュリティが守られた内部機器のサービスを利用する場合に有用である。

【図面の簡単な説明】

【００２９】

【図１】本発明の実施の形態におけるリモート操作装置の構成図

【図２】本発明の実施の形態における認証手段１０４で管理している認証情報管理テーブルの例を示す図

【図３】本発明の実施の形態における認証手段１０４で管理しているリモートサービスへのアクセス先のアドレス情報の例を示す図

【図４】本発明の実施の形態１におけるリモート操作装置の動作シーケンスを示す図

【図５】本発明の実施の形態２におけるリモート操作装置の動作シーケンスを示す図

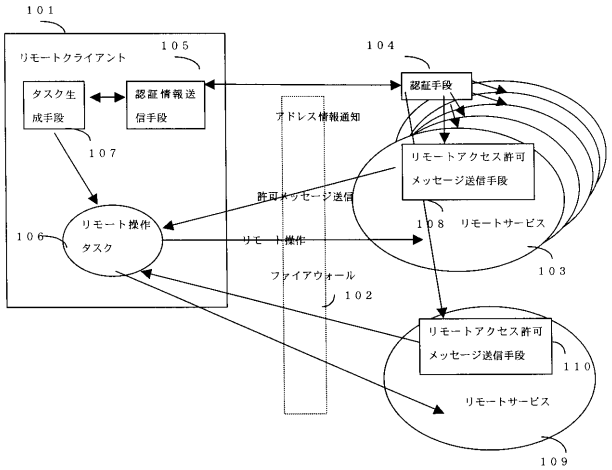
【図６】本発明の実施の形態２におけるリモートサービス１０３で記憶している提供できる詳細サービスの一覧の例を示す図

【符号の説明】

【００３０】

１０１　リモートクライアント
１０２　ファイアウォール
１０３，１０９　リモートサービス
１０４　認証手段
１０５　認証情報送信手段
１０６　リモート操作タスク
１０７　タスク生成手段
１０８，１１０　リモートアクセス許可メッセージ送信手段

【図１】



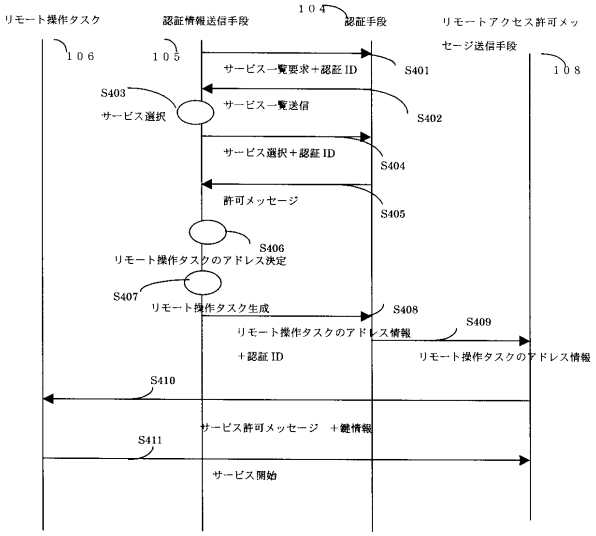
【図２】

認証 ID	許可するサービスの種類
ID1	S1,S2,S3
ID2	S1
ID3	S1,S2,S3,S4,S5
ID4	

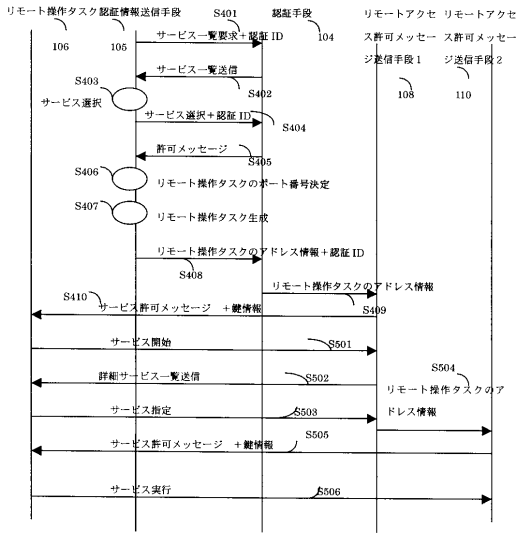
【図３】

サービスの種類	アドレス情報	
	IP アドレス	ポート番号
S1	192.168.0.10	20000
S2	192.168.0.10	30000
S3	192.168.0.9	40000
S4	192.168.0.8	50000
S5	192.168.0.7	60000

【図４】



【図５】



【図６】

詳細サービスの種類
F1
F2
F3
F4
F5

フロントページの続き

Ｆターム(参考) 5B085 AE00 AE01 AE04 AE06 AE29
5J104 EA16 KA02 PA07