(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3810998号
(P3810998)
(45)発行日　平成18年8月16日(2006.8.16)　(24)登録日　平成18年6月2日(2006.6.2)

(51)Int.Cl.		F I		
G06F 13/00	(2006.01)	G06F	13/00	351N
H04L 12/56	(2006.01)	G06F	13/00	353B
H04L 29/14	(2006.01)	H04L	12/56	400Z
		H04L	13/00	313

請求項の数 8　(全 12 頁)

(21)出願番号　特願2000-357242(P2000-357242)
(22)出願日　平成12年11月24日(2000.11.24)
(65)公開番号　特開2002-163162(P2002-163162A)
(43)公開日　平成14年6月7日(2002.6.7)
審査請求日　平成13年1月15日(2001.1.15)
審判番号　不服2004-25038(P2004-25038/J1)
審判請求日　平成16年12月8日(2004.12.8)

早期審理対象出願

(73)特許権者　500542745
株式会社ホライズン・デジタル・エンタープライズ
東京都渋谷区桜丘町３１番１５号
(74)代理人　100141173
弁理士　西村　啓一
(74)代理人　100088856
弁理士　石橋　佳之夫
(72)発明者　川下　真
東京都渋谷区道玄坂一丁目１２番１号　株式会社ホライズン・デジタル・エンタープライズ内

最終頁に続く

(54)【発明の名称】コンピュータ遠隔管理方法

(57)【特許請求の範囲】
【請求項１】
ファイアウォールを介して接続した被管理コンピュータからＰＯＳＴメソッドのリクエストを受信した管理コンピュータが、このリクエストに含まれる情報を処理した結果としての情報を上記リクエストに対するＰＯＳＴメソッドのレスポンスとして上記ファイアウォールを介して上記被管理コンピュータに送信することで上記被管理コンピュータを遠隔管理する方法であって、
上記管理コンピュータが、上記被管理コンピュータの稼働状況を示す情報を、ＰＯＳＴメソッドのリクエスト（以下、「第１リクエスト」という）として、上記被管理コンピュータから受信するステップと、
上記管理コンピュータが、特定の監視項目に関する情報の送信を指示する情報を、上記第１リクエストに対するＰＯＳＴメソッドのレスポンスとして、上記被管理コンピュータに送信するステップと、
上記管理コンピュータが、上記特定の監視項目に関する情報を、ＰＯＳＴメソッドのリクエスト（以下、「第２リクエスト」という）として、上記被管理コンピュータから受信するステップと、
上記管理コンピュータが、上記被管理コンピュータを遠隔操作するための指示情報を、上記第２リクエストに対するＰＯＳＴメソッドのレスポンスとして、上記被管理コンピュータに送信するステップと、
を有してなることを特徴とするコンピュータ遠隔管理方法。

【請求項２】
管理コンピュータが、被管理コンピュータの稼働状況を示す情報を定期的に受信する請求項１記載のコンピュータ遠隔管理方法。
【請求項３】
管理コンピュータと被管理コンピュータとの間の通信は暗号化通信とする請求項１または２記載のコンピュータ遠隔管理方法。
【請求項４】
１つの管理コンピュータが複数の被管理コンピュータを遠隔監視する請求項１乃至３のいずれかに記載のコンピュータ遠隔管理方法。
【請求項５】
ファイアウォールを介して接続した被管理コンピュータからＰＯＳＴメソッドのリクエストを受信し、このリクエストに含まれる情報を処理した結果としての情報を上記リクエストに対するＰＯＳＴメソッドのレスポンスとして上記ファイアウォールを介して上記被管理コンピュータに送信するコンピュータであって、
上記被管理コンピュータの稼働状況を示す情報を、ＰＯＳＴメソッドのリクエスト（以下、「第１リクエスト」という）として、上記被管理コンピュータから受信する手段と、
特定の監視項目に関する情報の送信を指示する情報を、上記第１リクエストに対するＰＯＳＴメソッドのレスポンスとして、上記被管理コンピュータに送信する手段と、
上記特定の監視項目に関する情報を、ＰＯＳＴメソッドのリクエスト（以下、「第２リクエスト」という）として、上記被管理コンピュータから受信する手段と、
上記被管理コンピュータを遠隔操作するための指示情報を、上記第２リクエストに対するＰＯＳＴメソッドのレスポンスとして、上記被管理コンピュータに送信する手段と、
を有してなることを特徴とする管理コンピュータ。
【請求項６】
被管理コンピュータの稼働状況を示す情報を定期的に受信する請求項５記載の管理コンピュータ。
【請求項７】
管理コンピュータと被管理コンピュータとの間の通信は暗号化通信とする請求項５または６記載の管理コンピュータ。
【請求項８】
１つの管理コンピュータが複数の被管理コンピュータを遠隔監視する請求項５乃至７のいずれかに記載の管理コンピュータ。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、管理コンピュータが通信回線を介して被管理コンピュータを遠隔監視、及び遠隔操作するためのコンピュータ遠隔管理方法に関するものである。
【０００２】
【従来の技術】
近年の通信技術の発達に伴い、コンピュータネットワークをはじめとする各種通信回線に接続するコンピュータ等の情報処理端末の数は増加している。情報処理端末の利用者は、用途や目的に応じて通信先の情報処理端末を選択し、適宜通信プロトコルを使い分けて通信を行う。
図８は、コンピュータネットワーク１００の利用者が、コンピュータ１０１を用いてＷＥＢサーバ１０２、あるいはメールサーバ１０３に接続している例である。通信１０１－２、１０２－１はそれぞれ、プロトコルにＨＴＴＰ（Ｈｙｐｅｒ　Ｔｅｘｔ　Ｔｒａｎｓｆｅｒ　Ｐｒｏｔｏｃｏｌ）を用いた通信を示し、通信１０１－３，１０３－１はそれぞれ、プロトコルにＳＭＴＰ（Ｓｉｍｐｌｅ　Ｍｅｓｓａｇｅ　Ｔｒａｎｓｆｅｒ　Ｐｒｏｔｏｃｏｌ），ＰＯＰ３（ＰｏｓｔＯｆｆｉｃｅ　Ｐｒｏｔｏｃｏｌ　Ｖｅｒｓｉｏｎ　３）を用いた通信を示している。なお、コンピュータ１０１，１０２，１０３がコンピュー

タネットワーク１００と接続するための通信回線などについては記載を省略してある（以下、同じ）。

【０００３】

コンピュータの運用者は、管理対象のコンピュータ（以下、「被管理コンピュータ」という）を正常に稼動させるために、被管理コンピュータの稼動状況を監視しておき、監視結果に応じて適切な対応を採る。また、コンピュータネットワークに接続された複数の被管理コンピュータを運用管理する場合には、コンピュータの運用者は、被管理コンピュータとは別の管理用のコンピュータ（以下、「管理コンピュータ」という）から被管理コンピュータの稼動状況を監視する遠隔監視、あるいは、管理コンピュータから被管理コンピュータを操作する遠隔操作、等の遠隔管理を行うのが一般的である。

遠隔監視の方法としては、管理コンピュータから複数の被管理コンピュータに監視情報の送信要求をし、運用者は各被管理コンピュータから受信した監視情報により、各被管理コンピュータの稼動状況等を把握する。監視情報とは、運用者が被管理コンピュータの稼動状況を監視するために必要な情報であり、例えば、被管理コンピュータに予め設定されている「コンピュータの識別名称」や「アドレス情報」等の監視項目からなる管理情報や、監視情報の送信要求を受付けた時点での被管理コンピュータの稼動状況を示す「ＣＰＵ使用率」や、「プロセス情報」等の監視項目からなる稼動情報、等がある。

管理コンピュータが被管理コンピュータに監視情報の送信要求を行い、受け取るための通信プロトコルの例としては、ＳＮＭＰ（Ｓｉｍｐｌｅ　Ｎｅｔｗｏｒｋ　Ｍａｎａｇｅｍｅｎｔ　Ｐｒｏｔｏｃｏｌ）がある。

図９は、ＳＮＭＰを利用した通信例を示す図である。ここでは、ＷＥＢサーバ１０２とメールサーバ１０３の運用者が、コンピュータ１０４を用いて、ＷＥＢサーバ１０２とメールサーバ１０３を遠隔監視している例であり、コンピュータ１０４が管理コンピュータ、ＷＥＢサーバ１０２とメールサーバ１０３が被管理コンピュータである（ＳＮＭＰの場合、管理コンピュータはマネージャ、被管理コンピュータはエージェントと呼ばれる）。

管理コンピュータ１０４は、被管理コンピュータ１０２に対して監視情報の送信要求をする（通信１０４－２）。監視情報の送信要求を受けた被管理コンピュータ１０２は、管理コンピュータ１０４が要求している監視項目をＭＩＢ１２２に基づいて収集し、管理コンピュータ１０４に送信する（通信１０２－４）。ＭＩＢ（Ｍａｎａｇｅｍｅｎｔ　Ｉｎｆｏｒｍａｔｉｏｎ　Ｂａｓｅ）とは、ＳＮＭＰを利用する場合に、被管理コンピュータが自己の管理情報や稼動情報等を格納しておくデータベースである。通信１０４－３と１０３－４は、管理コンピュータ１０４がＳＮＭＰを用いて被管理コンピュータ１０３を遠隔監視するための通信を示す。

また、遠隔操作の方法としては、管理コンピュータから被管理コンピュータに対して指示情報を送信し、指示情報を受信した被管理コンピュータは、指示情報に基づいて動作する。指示情報とは、被管理コンピュータを操作するための情報であり、例えば、「被管理コンピュータに設定されているユーザ情報の変更」あるいは、「被管理コンピュータで動作しているプロセスの終了」等がある。ただし、被管理コンピュータを操作するためには、被管理コンピュータにおける操作のための権限（いわゆるルート権限）が必要であり、遠隔操作の場合、当該権限用のパスワード等の認証情報を指示情報と共に送信することが一般的である。すなわち、被管理コンピュータは、指示情報に基づいて動作する際、いっしょに受信したパスワード等を確認して、当該指示情報の正当性を確認するのである。

【０００４】

インターネット等の不特定多数の利用者が接続することを前提としたコンピュータネットワークでは、コンピュータネットワークに接続している各コンピュータは、他のコンピュータからの不正アクセスの脅威にさらされる。この不正アクセスを排除するためには、ファイアウォールを設置して接続を制限するのが一般的である。ＩＰ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）を用いた通信の場合、ファイアウォールは、ＩＰパケットを受信すると、ＩＰヘッダに格納されている通信する互いのコンピュータのＩＰアドレス、あるいはＴＣＰやＵＤＰヘッダに格納されている通信する互いのコンピュータのポート番号を用い

て、もしくはＩＰアドレスとポート番号の組合せ（ソケットという）を用いて接続を制限することが多い。不特定多数の利用者のコンピュータからの接続を前提とするインターネットに接続されたＷＥＢサーバ等のコンピュータの場合は、ファイアウォールは利用者のコンピュータのＩＰアドレスを予め特定しておくことができないため、ポート番号で接続を制限する、いわゆるポート番号によるフィルタリングを行う。なお、ポート番号には、接続元のポート番号（Ｓｏｕｒｃｅ　Ｐｏｒｔ　Ｎｕｍｂｅｒ）と接続先のポート番号（Ｄｅｓｔｉｎａｔｉｏｎ　ｐｏｒｔ　Ｎｕｍｂｅｒ）とがあるが、通常ファイアウォールが接続を制限するために用いるポート番号は、接続先のポート番号である。

図１０を用いてポート番号による接続の制限について説明する。コンピュータ１０１は、コンピュータネットワーク１００を介してＷＥＢサーバ１０２に接続する。ここで、ＷＥＢサーバ１０２は、ファイアウォール１０５を介してコンピュータネットワーク１００に接続している。ファイアウォール１０５は、コンピュータネットワーク１００からＷＥＢサーバ１０２へのアクセス要求のＩＰパケットを受信して接続先のポート番号を確認し、ＷＥＢサーバ用のポート番号「８０」であれば接続を許可し、それ以外のポート番号であれば接続を拒否するように設定してある（「８０」はＷｅｌｌ　Ｋｎｏｗｎ　Ｐｏｒｔ　Ｎｕｍｂｅｒ　として規定されたポート番号）。ここで、コンピュータ１０１からＷＥＢサーバ１０２への通信１０１－２は、接続先のポート番号に「８０」を設定したＩＰパケットであるため、ファイアウォール１０５は接続を許可し、コンピュータ１０１は、ＷＥＢサーバ１０２からの応答のＩＰパケットを受け取ることができる（通信１０２－１）。

【０００５】

【発明が解決しようとする課題】

しかしながら、運用者が前述のプロトコルＳＮＭＰを用いて管理コンピュータ１０４からＷＥＢサーバ１０２を監視する場合、監視情報の送信要求のための通信１０４－２は、接続先のポート番号がＳＮＭＰ用の「１６１」であるため、ファイアウォール１０５で接続を拒否される（通信１０５－１は、接続を拒否した旨の通知であり、送信されないこともある）。したがって、運用者はＷＥＢサーバ１０２の稼動状況を遠隔監視することができない。管理コンピュータ１０４からＷＥＢサーバ１０２を遠隔監視するためには、ファイアウォール１０５に、接続を許可するポート番号として、既に設定されている「８０」に加えて「１６１」を設定する必要がある。

【０００６】

ただし、ファイアウォールにおいて、接続を許可するポート番号を増やすことは、他のコンピュータからの不正アクセスの機会の増加を招くため、コンピュータセキュリティ上、望ましくない。

また、インターネット等のように複数の運用者により管理されているコンピュータネットワークでは、管理コンピュータと被管理コンピュータの通信経路上のすべてのファイアウォールにおいて、ポート番号「１６１」が接続可能に設定されていることは期待できず、被管理コンピュータの数が増加すれば、遠隔監視を行うことは困難あるいは不可能となる。

一方、遠隔操作の場合、指示情報と共にいわゆるルート権限用のパスワード等の認証情報も送信する必要があることから、第三者による盗聴の危険性があり、ひいては被管理コンピュータへの不正アクセスを誘発してしまい、セキュリティ上好ましくない。

【０００７】

本発明は以上のような従来技術の問題点を解消するためになされたもので、管理コンピュータがコンピュータネットワーク等の通信回線に接続された被管理コンピュータを遠隔管理する場合において、被管理コンピュータが待機しながら管理コンピュータからの要求に応答する従来の遠隔管理方法に対して、被管理コンピュータが管理コンピュータからの要求を待つことなく情報を送信するようにしたことにより、遠隔監視の場合において被管理コンピュータは管理コンピュータからの要求を受付けるためのポート番号を開けておく必要がなく、また遠隔操作の場合においてパスワード等の認証情報の送受信が不要となることから、従来の遠隔管理方法に対してセキュリティレベルの高いコンピュータ遠隔管理方

法を提供することを目的とする。

【０００８】

【課題を解決するための手段】

請求項１記載の発明は、ファイアウォールを介して接続した被管理コンピュータからＰＯＳＴメソッドのリクエストを受信した管理コンピュータが、このリクエストに含まれる情報を処理した結果としての情報をリクエストに対するＰＯＳＴメソッドのレスポンスとしてファイアウォールを介して被管理コンピュータに送信することで被管理コンピュータを遠隔管理する方法であって、管理コンピュータが、被管理コンピュータの稼働状況を示す情報を、ＰＯＳＴメソッドのリクエスト（以下、「第１リクエスト」という）として、被管理コンピュータから受信するステップと、管理コンピュータが、特定の監視項目に関する情報の送信を指示する情報を、第１リクエストに対するＰＯＳＴメソッドのレスポンスとして、被管理コンピュータに送信するステップと、管理コンピュータが、特定の監視項目に関する情報を、ＰＯＳＴメソッドのリクエスト（以下、「第２リクエスト」という）として、被管理コンピュータから受信するステップと、管理コンピュータが、被管理コンピュータを遠隔操作するための指示情報を、第２リクエストに対するＰＯＳＴメソッドのレスポンスとして、被管理コンピュータに送信するステップと、を有してなることを特徴とする。

【０００９】

請求項２記載の発明は、請求項１記載の発明において、管理コンピュータが、被管理コンピュータの稼働状況を示す情報を定期的に受信することを特徴とする。

【００１０】

請求項３記載の発明は、請求項１または２記載の発明において、管理コンピュータと被管理コンピュータとの間の通信は暗号化通信とすることを特徴とする。

【００１１】

請求項４記載の発明は、請求項１乃至３のいずれかに記載の発明において、１つの管理コンピュータが複数の被管理コンピュータを遠隔監視することを特徴とする。

【００１２】

請求項５記載の発明は、ファイアウォールを介して接続した被管理コンピュータからＰＯＳＴメソッドのリクエストを受信し、このリクエストに含まれる情報を処理した結果としての情報をリクエストに対するＰＯＳＴメソッドのレスポンスとしてファイアウォールを介して被管理コンピュータに送信するコンピュータであって、被管理コンピュータの稼働状況を示す情報を、ＰＯＳＴメソッドのリクエスト（以下、「第１リクエスト」という）として、被管理コンピュータから受信する手段と、特定の監視項目に関する情報の送信を指示する情報を、第１リクエストに対するＰＯＳＴメソッドのレスポンスとして、被管理コンピュータに送信する手段と、特定の監視項目に関する情報を、ＰＯＳＴメソッドのリクエスト（以下、「第２リクエスト」という）として、被管理コンピュータから受信する手段と、被管理コンピュータを遠隔操作するための指示情報を、第２リクエストに対するＰＯＳＴメソッドのレスポンスとして、被管理コンピュータに送信する手段と、を有してなることを特徴とする。

【００１３】

請求項６記載の発明は、請求項５記載の発明において、被管理コンピュータの稼働状況を示す情報を定期的に受信することを特徴とする。

請求項７記載の発明は、請求項５または６記載の発明において、管理コンピュータと被管理コンピュータとの間の通信は暗号化通信とすることを特徴とする。

請求項８記載の発明は、請求項５乃至７のいずれかに記載の発明において、１つの管理コンピュータが複数の被管理コンピュータを遠隔監視することを特徴とする。

【００１４】

【発明の実施の形態】

以下、図面を参照しながら本発明にかかるコンピュータ遠隔管理方法の実施の形態について説明する。図１は、本発明にかかるコンピュータ遠隔管理方法の実施の形態を示したブ

ロック図である。
符号１は管理コンピュータを示し、符号２，３は被管理コンピュータを示す。また、符号１０は通信回線を示し、管理コンピュータ１と被管理コンピュータ２，３とは、それぞれ通信回線１０を介して通信する。
通信回線１０には、インターネットやＬＡＮ（Ｌｏｃａｌ Ａｒｅａ Ｎｅｔｗｏｒｋ）等のコンピュータネットワークや、電話回線、衛星通信回線等がある。
被管理コンピュータ２，３は、それぞれＨＴＴＰのＰＯＳＴメッセージのリクエストを送信でき、またＰＯＳＴメッセージのレスポンスを受信できるものであり、一方管理コンピュータ１は、ＰＯＳＴメッセージのリクエストを受信して、ＰＯＳＴメッセージのレスポンスを送信できるものである。管理コンピュータ１や被管理コンピュータ２，３の例としては、ＬｉｎｕｘやＷｉｎｄｏｗｓ等が動作するパソコンや、ＵＮＩＸマシン、あるいは、携帯電話やＰＤＡ等の携帯情報処理端末等がある。ただし、管理コンピュータ１や被管理コンピュータ２，３の動作する機器としてはこれらに限定されるものではなく、先の条件に該当するものであればよい。
なお、図１は、１つの管理コンピュータ１が２つの被管理コンピュータ２，３を遠隔管理する例を示しているが、１つの管理コンピュータにより遠隔管理される被管理コンピュータの数はこれに限定されるものではなく、用途や目的等に応じて適宜１以上の被管理コンピュータを選定できる。
【００１５】
図２は図１の実施の形態における通信の順序を時系列で示した図であり、図の上方から下方に向かう順に通信が行われることを示している。図２を用いて、図示しない被管理コンピュータ２，３の運用者が、管理コンピュータ１を用いて被管理コンピュータ２の稼動状況を遠隔監視する方法について説明する。
先ず、被管理コンピュータ２が監視情報をＨＴＴＰのＰＯＳＴメソッドのリクエストとして管理コンピュータ１に送信する（通信２－１）。ここで監視情報とは、運用者が被管理コンピュータ２の稼動状況を遠隔監視するために必要な情報であり、管理情報と稼動情報とからなる。管理情報とは、運用者が被管理コンピュータ２に予め設定している情報であり、例えば「コンピュータの識別名称」や「アドレス情報」等の監視項目からなる。また、稼動情報とは、被管理コンピュータ２の稼動状況を示す情報であり、例えば「ＣＰＵ使用率」や「プロセス情報」等の監視項目からなる。図３，４は、それぞれ管理情報と稼動情報の監視項目の例である。なお、監視項目はこれらに限定されるものではなく、運用者が適宜決定する。また監視項目は、遠隔監視をはじめた後においても、運用者が適宜変更できる。
【００１６】
被管理コンピュータ２から監視情報を受信した管理コンピュータ１は、図示しないコンピュータプログラムを用いて、当該監視情報を処理する。処理の内容は、受信した監視情報の各監視項目について、予め設定してある各監視項目のしきい値との比較、あるいは、受信した監視情報を図示しない管理コンピュータ１内部の情報記憶装置に格納する等があり、運用者が適宜決めておく。
【００１７】
監視情報を処理した管理コンピュータ１は、結果情報をＰＯＳＴメソッドのレスポンスとして被管理コンピュータ２に送信する（通信１－２）。結果情報とは、管理コンピュータ１が監視情報を処理した結果を被管理コンピュータ２に通知するためのものである。結果情報を受信した被管理コンピュータ２は、先に送信（通信２－１）した監視情報を管理コンピュータ１が処理できたか否かの確認等ができる。
以上説明したように、本発明にかかるコンピュータ遠隔管理方法においては、被管理コンピュータは管理コンピュータからの要求を受付けるためのポートを開けておく必要がなく、セキュリティレベルの向上を図ることができる。また、管理コンピュータ１と被管理コンピュータ２との間の通信２－１，１－２は、コンピュータネットワークでの利用度が極めて高く、そのためファイアウォールで接続を制限されることのないＨＴＴＰ（その中の

ＰＯＳＴメソッド）を用いているため、管理コンピュータ１と被管理コンピュータ２との通信経路上にファイアウォールが設置されていたとしても、管理コンピュータ１が被管理コンピュータ２を遠隔監視する上で支障はない。
管理コンピュータ１が被管理コンピュータ３を遠隔監視する場合も、通信３－１－、１－３により同様に行える。
なお、管理コンピュータ１と被管理コンピュータ２，３との間で送受信される監視情報、結果情報のフォーマット等については、予め決めておく。

【００１８】

図１の実施の形態において、被管理コンピュータ２あるいは３が監視情報を管理コンピュータ１に送信するタイミングを、例えば「５分間隔」、「毎週月曜日の朝７時」等、定期的としてもよいし、監視項目がしきい値を超えた場合、例えば「ディスク使用率が７５％に達した時」等、不定期としてもよい。
定期的とすると、監視情報の送信間隔を短くすることで、管理コンピュータ１は、被管理コンピュータ２，３の稼動状況を常に監視することができる。一方不定期とすると、必要なときに監視情報を送信する等、管理コンピュータ１と被管理コンピュータ２，３の双方に処理負担が少なくなり、また、通信回線１０の通信トラフィックを抑えることもできる。運用者は、監視情報の送信のタイミングを定期的、不定期、あるいは両者を組み合わせる等、遠隔監視の目的等に応じて決める。

【００１９】

また図１の実施の形態において、管理コンピュータ１と被管理コンピュータ２，３との間の通信は、ＳＳＬ（Ｓｅｃｕｒｅ　Ｓｏｃｋｅｔ　Ｌａｙｅｒ）等を用いた暗号化通信としてもよい。暗号化通信とすることで、第三者による管理コンピュータ１と被管理コンピュータ２，３との間の通信が盗聴されるのを排除できるため、通信の安全性を高めることができる。なお、管理コンピュータ１と被管理コンピュータ２，３との間の通信にＨＴＴＰを用いる場合、ＨＴＴＰとＳＳＬとの親和性が高いことから、ＳＳＬの実装は容易となる。

【００２０】

さらに図１の実施の形態において、被管理コンピュータ２と被管理コンピュータ３が管理コンピュータ１に送信する監視情報の監視項目は、一致してもよいし、一致していなくてもよく、運用者が遠隔監視の目的等に応じて適宜決める。

【００２１】

図１の実施の形態によれば、被管理コンピュータ２が管理コンピュータ１に通信回線を介して監視情報を送信することで、上記管理コンピュータ１が上記被管理コンピュータ２の稼動状況を監視するコンピュータ遠隔管理方法において、上記管理コンピュータ１から送信要求を受けることなく、上記被管理コンピュータ２が上記管理コンピュータ１に上記監視情報を送信することで、被管理コンピュータ２は管理コンピュータ１からの要求を受付けるためのポート番号を開けておく必要がなく、セキュリティレベルの向上を図ることができる。また、被管理コンピュータ２は、管理コンピュータ１とは無関係に管理コンピュータ１に監視情報を送信できるので、送信するタイミングを定期的とすると、運用者は、被管理コンピュータ２の稼動状況の時間的変化を容易に把握でき、遠隔監視の効果を高めることができる。

【００２２】

また、監視情報をＰＯＳＴメソッドのリクエストとして管理コンピュータ１に送信することで、管理コンピュータ１と被管理コンピュータ２との通信経路上にファイアフォールが設置されていた場合でも、接続を制限されることなく遠隔監視が実現でき、遠隔監視とファイアウォールの並行運用が可能となる。

【００２３】

次に、本発明にかかるコンピュータ遠隔管理方法の別の実施の形態について説明する。
図１の実施の形態は、管理コンピュータが被管理コンピュータから監視情報を受信するものであったが、本実施の形態は、管理コンピュータが被管理コンピュータから監視情報を

受信するのに加えて、さらに被管理コンピュータを遠隔操作するものである。
図５は、本実施の形態における管理コンピュータ１と被管理コンピュータ４との通信の順序を時系列で示した図である。なお、管理コンピュータ１と被管理コンピュータ４とが通信回線を介して互いに通信できるのは、図１の実施の形態と同様である。
被管理コンピュータ４が管理コンピュータ１に監視情報を送信する「通信４－１」は、図１の実施の形態の「通信２－１」と同様である。
図１の実施の形態との違いは、監視情報を受信（通信４－１）した管理コンピュータ１は、当該監視情報を処理した後に、結果情報を送信せずに指示情報を被管理コンピュータ４に送信（通信１－４－１）する。指示情報とは、管理コンピュータ１が被管理コンピュータ４を遠隔操作するための情報であり、例えば特定の監視項目に関する情報の送信の指示、あるいは、先に送信した監視情報の再送信、等がある。
指示情報を受信した被管理コンピュータ４は、当該指示情報が、先の通信４－１のレスポンスとして送信されていることを確認して、指示情報の内容に基づいて動作する。ここでは、監視情報を管理コンピュータ１に送信する例を示している（通信４－１－１）。
監視情報を受信した管理コンピュータ１は、さらに別の指示情報を送信してもよいし、結果情報を送信してもよい。図５は、２度の指示情報を送信（通信１－４－１、１－４－２）した後に、結果情報を送信（通信１－４）しているが、指示情報の送信回数は、これに限定されるものではない。なお、通信１－４で送信する結果情報は、図１の実施の形態における「通信１－２」で送信する結果情報と同様のものである。

【００２４】

図６は、本実施の形態における管理コンピュータ１と被管理コンピュータ４との別の通信の順序を時系列で示した図である。
図５の通信との違いは、監視情報を受信（通信４－１－１）した管理コンピュータ１は、結果情報を送信せずに被管理コンピュータ４に指示情報付き結果情報を送信（通信１－４－０）する点である。指示情報付き結果情報とは、図５の通信における指示情報を含んだ結果情報であり、指示情報付き結果情報を受信した被管理コンピュータ４は、管理コンピュータ１が監視情報を処理した結果を判断すると共に、指示情報に基づいて動作する。ただし、指示情報付き結果情報に基づいた動作には、監視情報を管理コンピュータ１に送信することは含まない。指示情報の内容としては、例えば被管理コンピュータ４のシステム再起動、被管理コンピュータ４の特定プロセスの終了、あるいは、被管理コンピュータ４のハードディスク内部のデータの外部記憶装置への退避、等がある。
なお図６では、１度の指示情報を送信（通信１－４－１）した後に指示情報付き結果情報を送信（通信１－４－０）しているが、指示情報の送信をすることなく、監視情報を受信（通信４－１）した後に、指示情報付き結果情報を送信することもできる。

【００２５】

図７は、本実施の形態における管理コンピュータ１と被管理コンピュータ４とのさらに別の通信の順序を時系列で示した図である。
図５の通信との違いは、被管理コンピュータ４が、監視情報ではなく、指示待ち情報を先ず管理コンピュータ１に送信（通信４－０）する点である。指示待ち情報とは、被管理コンピュータ４が管理コンピュータ１に対して指示情報の送信を依頼するための情報である。指示待ち情報を受信した管理コンピュータ１は、指示情報を被管理コンピュータ４に送信（通信１－４－１）する。指示情報を受信した被管理コンピュータ４は、図６の通信の場合と同様に指示情報に基づいて動作する。
ここで、指示待ち情報を受信した管理コンピュータ１は、指示情報を送信する代わりに、図６の指示情報付き結果情報を送信することもできる。また、遠隔操作の必要がない場合には、単に結果情報を送信することもできる。
なお、本実施の形態における指示情報、指示情報付き結果情報、および指示待ち情報のフォーマット等については、予め決めておく。

【００２６】

以上説明した実施の形態によると、監視情報を受信した管理コンピュータ１が、指示情報

をＰＯＳＴメソッドのレスポンスとして被管理コンピュータ４に送信することで、上記管理コンピュータ１が上記被管理コンピュータ４を遠隔操作できるようにしたため、管理コンピュータ１と被管理コンピュータ４との間で遠隔操作のためのパスワード等の送受信が不要となり、セキュリティレベルの向上を図ることができる。

【００２７】

【発明の効果】

本発明によれば、被管理コンピュータが管理コンピュータに通信回線を介して監視情報を送信することで、上記管理コンピュータが上記被管理コンピュータの稼動状況を監視するコンピュータ遠隔管理方法において、上記管理コンピュータから送信要求を受けることなく、上記被管理コンピュータが上記管理コンピュータに上記監視情報を送信することで、被管理コンピュータは管理コンピュータからの要求を受付けるためのポート番号を開けておく必要がなく、セキュリティレベルの向上を図ることができる。また、被管理コンピュータは、管理コンピュータとは無関係に管理コンピュータに監視情報を送信できるので、運用者は、被管理コンピュータの稼動状況の時間的変化を容易に把握でき、遠隔監視の効果を高めることができる。

【００２８】

また本発明によれば、監視情報をＰＯＳＴメソッドのリクエストとして管理コンピュータに送信することで、管理コンピュータと被管理コンピュータとの通信経路上にファイアフォールが設置されていた場合でも、接続を制限されることなく遠隔監視が実現でき、遠隔監視とファイアウォールの並行運用が可能となる。

【００２９】

さらに本発明によれば、監視情報を受信した管理コンピュータが、指示情報をＰＯＳＴメソッドのレスポンスとして被管理コンピュータに送信することで、上記管理コンピュータが上記被管理コンピュータを遠隔操作できるようにしたため、管理コンピュータと被管理コンピュータとの間で遠隔操作のためのパスワード等の送受信が不要となり、セキュリティレベルの向上を図ることができる。

【図面の簡単な説明】

【図１】本発明にかかるコンピュータ遠隔管理方法の実施の形態を示すブロック図である。

【図２】図１の実施の形態における通信の順序を時系列で示したフローチャート図である。

【図３】図１の実施の形態における管理情報の監視項目の例である。

【図４】図１の実施の形態における稼動情報の監視項目の例である。

【図５】本発明にかかるコンピュータ遠隔管理方法の別の実施の形態における通信の順序を時系列で示したフローチャート図である。

【図６】本発明にかかるコンピュータ遠隔管理方法の別の実施の形態における別の通信の順序を時系列で示したフローチャート図である。

【図７】本発明にかかるコンピュータ遠隔管理方法の別の実施の形態におけるさらに別の通信の順序を時系列で示したフローチャート図である。

【図８】従来のコンピュータ遠隔管理方法を説明するためのブロック図である。

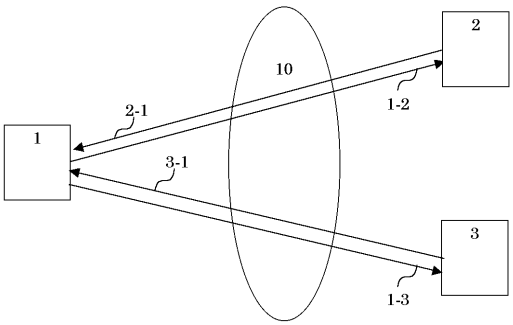
【図９】従来のコンピュータ遠隔管理方法の例について示すブロック図である。

【図１０】従来のコンピュータ遠隔管理方法の例について示すブロック図である。

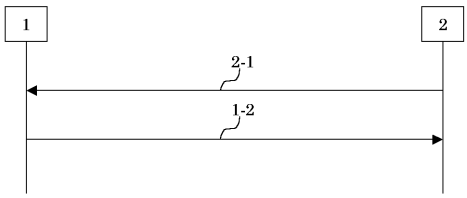
【符号の説明】

１	管理コンピュータ
２，３，４	被管理コンピュータ
１０	通信回線

【図１】



【図２】



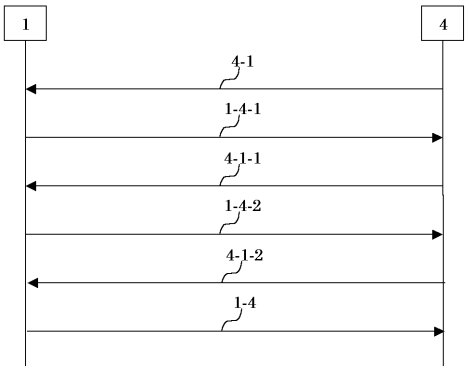
【図３】

インベントリ管理	識別名 ホスト名 ドメイン名 コメント IPアドレス MACアドレス 稼働時間 接続ユーザー情報 CPU情報 HDD情報 NIC情報 カーネルバージョン情報 ディストリビューション情報 rpm情報
障害報告管理	障害報告の管理
ログ管理	LCEログ管理機能
ジョブ管理	LC設定配信 rpm配信 配信予約 配信履歴 電源管理
レポーティング	レポート発行機能
ヘルプデスク	高機能な障害報告管理

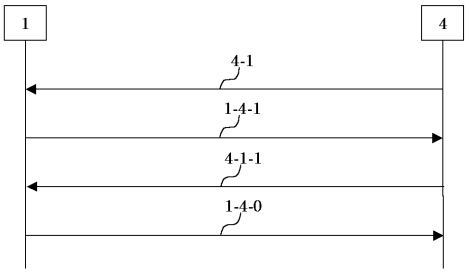
【図４】

ステータス監視	システム負荷 CPU使用率 HDD Read HDD Write NIC In NIC Out 物理メモリ使用量 仮想メモリ使用量
リソース監視	HDD 使用量 物理メモリ使用量 仮想メモリ使用量 CPU使用量
プロセス監視	プロセス情報 プロセス監視 未知のプロセスの監視
セキュリティ監視	ポート情報 ログ監視 ログイン監視
サービス監視	Ping Socket Ping Trace Route
障害報告一覧	監視項目に対する注意・警告一覧
ハードウェア監視	CPUの温度監視 筐体内部の温度監視 ファンの回転数監視 HDD障害監視
Oracle監視	DBの状態監視

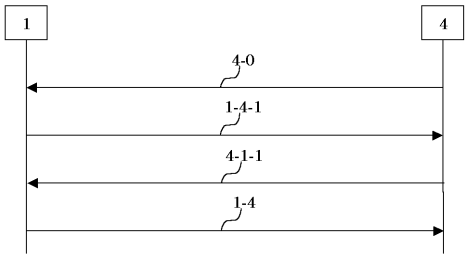
【図５】



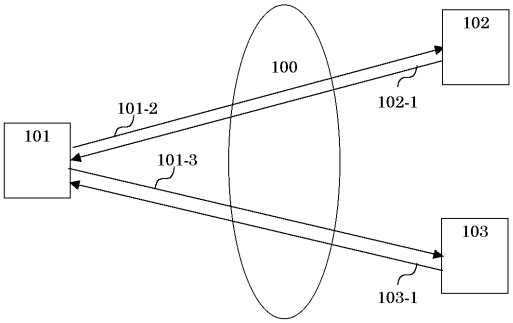
【図６】



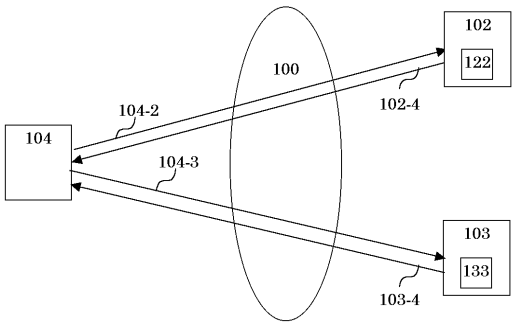
【図７】


1
4
4-0
1-4-1
4-1-1
1-4

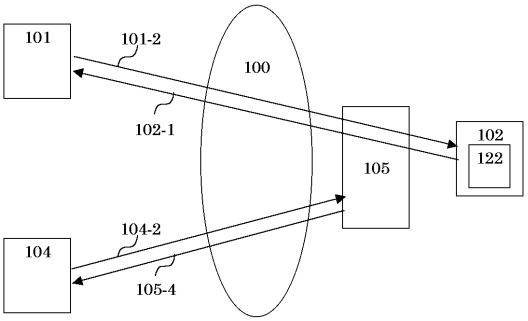
【図８】


100
101
101-2
101-3
102
102-1
103
103-1

【図９】


100
104
104-2
104-3
102
122
102-4
103
133
103-4

【図１０】


101
101-2
102-1
100
105
102
122
104
104-2
105-4

フロントページの続き

合議体
審判長　大日方　和幸
審判官　植松　伸二
審判官　山崎　慎一

(56)参考文献　特開平１１－２３４２７１（ＪＰ，Ａ）
特開平８－２１２０１４（ＪＰ，Ａ）
特開平１０－４９３９４（ＪＰ，Ａ）
特開２０００－１３２４７５（ＪＰ，Ａ）
特開平１１－２７５０８８（ＪＰ，Ａ）
特開平１１－２１５１５９（ＪＰ，Ａ）
特開２０００－１７２５９７（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F13/00,351