(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3789348号
(P3789348)
(45)発行日　平成18年6月21日(2006.6.21)　(24)登録日　平成18年4月7日(2006.4.7)

(51)Int.Cl.		F I		
H04L 12/56	(2006.01)	H04L	12/56	H
H04L 12/46	(2006.01)	H04L	12/56	B
		H04L	12/46	A

請求項の数 20　(全 49 頁)

(21)出願番号　特願2001-350783(P2001-350783)
(22)出願日　平成13年11月15日(2001.11.15)
(65)公開番号　特開2002-335273(P2002-335273A)
(43)公開日　平成14年11月22日(2002.11.22)
審査請求日　平成16年2月9日(2004.2.9)
(31)優先権主張番号　特願2001-63453(P2001-63453)
(32)優先日　平成13年3月7日(2001.3.7)
(33)優先権主張国　日本国(JP)

(73)特許権者　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(74)代理人　100071113
弁理士　菅　隆彦
(72)発明者　中濱　清志
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　山田　敬信
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

審査官　清水　稔

最終頁に続く

(54)【発明の名称】リモートメンテナンス実施方法、システム及びプログラム並びにリモートメンテナンス実施プログラムを記録した記録媒体

(57)【特許請求の範囲】

【請求項１】

各ローカルネットワークにより任意数の内線端末とＩＰ接続してそれぞれのインターネットゲートウェイ端末の支配下とする一方、当該それぞれのインターネットゲートウェイ端末とインターネットを介してＶＰＮゲートウェイ間でＯＳＩ参照モデルのネットワーク層においてＶＰＮセッションを実現するＩＰｓｅｃを確立することにより、当該ＶＰＮゲートウェイを含む保守センタからリモートメンテナンスを行う実施方法であって、

前記それぞれのインターネットゲートウェイ端末におけるルータ部内に、そのローカルネットワークとＶＰＮ処理部との間にＶＰＮＮＡＴを設け、グローバル側のアドレスをＶＰＮＮＡＴ用ローカルＩＰアドレスとして前記保守センタの保守サーバから付与及び解放を行うことにより前記リモートメンテナンスを実施する、

ことを特徴とするリモートメンテナンス実施方法。

【請求項２】

前記実施方法における前記リモートメンテナンスの要求は、

当該要求を行う前記インターネットゲートウェイ端末が、リモートメンテナンス対象である内線端末名及び当該インターネットゲートウェイ端末のグローバルＩＰアドレスを、リモートメンテナンス要求コマンドとして前記保守サーバに通知すると、

当該通知を受けた当該保守サーバが、当該通知したリモートメンテナンス対象の前記内線端末に付与するＶＰＮＮＡＴ用ローカルＩＰアドレス及び内線端末名を、当該通知をしてきたインターネットゲートウェイ端末にリモートメンテナンス要求レスポンスとしてレ

スポンスすると共に、当該インターネットゲートウェイ端末のグローバルＩＰアドレスとの間において設置通知の際に共有されるＩＰｓｅｃの認証鍵を用いたＩＰｓｅｃによるＶＰＮトンネルの確立を自己のＶＰＮゲートウェイに設定させ、当該ＶＰＮゲートウェイに対してＶＰＮＮＡＴ用ローカルＩＰアドレス宛のパケットを前記確立したＶＰＮトンネルのＶＰＮ処理対象パケットとする設定を行い、

前記レスポンスを受けたインターネットゲートウェイ端末が、受けた前記内線端末名に対する実ローカルＩＰアドレスを取得して、当該内線端末名に対する実ローカルＩＰアドレスと前記ＶＰＮＮＡＴ用ローカルＩＰアドレスとを静的ＮＡＴとし自己のルータ部に対して設定を行う、

以上の一連の処理を順次実施する、

ことを特徴とする請求項１に記載のリモートメンテナンス実施方法。

【請求項３】

前記リモートメンテナンスの実施は、

前記リモートメンテナンス対象である前記内線端末に対して、前記ＶＰＮＮＡＴ用ローカルＩＰアドレスで前記確立されたＶＰＮトンネルを経由して、前記保守センタから行われる、

ことを特徴とする請求項２に記載のリモートメンテナンス実施方法。

【請求項４】

前記リモートメンテナンスの終了は、

先ず、前記ＶＰＮＮＡＴ用ローカルＩＰアドレスで前記確立されたＶＰＮトンネルを経由して、当該ＶＰＮトンネルを確立させた前記インターネットゲートウェイ端末のサーバ部に対して、リモートメンテナンス終了コマンドを送信し、

次に、当該送信を受けたサーバ部において、当該リモートメンテナンス終了コマンドに係る処理を行い、リモートメンテナンス終了レスポンスを送信し、

その後、当該リモートメンテナンス終了レスポンスを受信した保守サーバにて、該当内線端末に対するメンテナンスが全て終了したかの第１判断を行い、当該第１判断にて肯定の場合には当該終了した内線端末は前記インタネットゲートウェイ端末の前記サーバ部、前記ルータ部の何れかであるかの第２判断を行う一方、否定の場合には判断処理を終了し、当該第２判断にて否定の場合にはＶＰＮＮＡＴ解放処理へ移行し、他方肯定の場合には対応する前記インタネットゲートウェイ端末に対するリモートメンテナンスを全て終了したかの第３判断を行い、当該第３判断にて肯定の場合にはＶＰＮ終了処理へ移行するとともに否定の場合には当該判断処理を終了する、

以上の一連の処理を順次実施する、

ことを特徴とする請求項２又は３に記載のリモートメンテナンス実施方法。

【請求項５】

前記ＶＰＮＮＡＴ解放処理は、

先ず、前記保守サーバが、前記リモートメンテナンスの要求の際に設定した前記リモートメンテナンス対象の内線端末名に対するＶＰＮＮＡＴ用ローカルＩＰアドレスを、前記確立したＶＰＮトンネルへのＶＰＮ処理対象パケットから解除する一方で、前記インターネットゲートウェイ端末に対して当該リモートメンテナンス対象の内線端末名を通知した後に、当該通知を受けたインターネットゲートウェイ端末が、当該受けた内線端末名に対する実ローカルＩＰアドレスを取得して、それに対するＶＰＮＮＡＴ用ローカルアドレスとの静的ＮＡＴを解放し、

引続き、前記保守サーバが、前記第３判断を行いその判断結果に従う、

以上の一連の処理を順次実施する、

ことを特徴とする請求項４に記載のリモートメンテナンス実施方法。

【請求項６】

前記ＶＰＮ終了処理は、

前記保守サーバが、ＩＰｓｅｃセッションの終了をＶＰＮ終了コマンドとして、前記インターネットゲートウェイ端末に通知して、当該通知を受けたインターネットゲートウェ

イ端末が、当該ＶＰＮ終了コマンドに対する返答を当該保守サーバにＶＰＮ終了レスポンスとして送信し、
前記保守サーバが、前記ＶＰＮゲートウェイに、前記リモートメンテナンスの要求に際に設定した前記ＶＰＮトンネルを解除させ、当該ＶＰＮゲートウェイと前記インターネットゲートウェイ端末間で確立されているＶＰＮトンネル処理を終了する、
以上の一連の処理を順次実施する、
ことを特徴とする請求項４又は５に記載のリモートメンテナンス実施方法。
【請求項７】
前記設置通知は、
新たに設置された前記インターネットゲートウェイ端末の前記サーバ部から、当該設置について前記保守サーバに設置通知コマンドを通知し、
当該設置通知コマンドを受けた当該保守サーバにより、前記リモートメンテナンスのための共通情報であるＩＰｓｅｃの認証鍵を生成して、当該設置通知コマンドを通知してきた前記インターネットゲートウェイ端末にレスポンスし、
当該レスポンスを受信した前記インターネットゲートウェイ端末は、ＩＰｓｅｃの認証鍵を自己の前記ルータ部に対して設定する、
以上の一連の処理を順次実施する、
ことを特徴とする請求項２、３、４、５又は６に記載のリモートメンテナンス実施方法。
【請求項８】
前記実施方法は、
前記リモートメンテナンスの要求、前記設定通知の何れか一方において、前記インターネットゲートウェイ端末の前記サーバ部及び前記ルータ部へのＶＰＮＮＡＴ設定処理を実施する、
ことを特徴とする請求項２、３、４、５、６又は７に記載のリモートメンテナンス実施方法。
【請求項９】
前記実施方法は、
前記インターネットゲートウェイ端末に故障発生を検知した場合には、
先ず、当該インターネットゲートウェイ端末が、故障通知コマンドとして故障に係る情報を前記保守サーバに送信し、
次に、前記保守サーバが前記故障通知コマンドを受信すると当該故障に係る情報を処理して、当該故障通知コマンドを送信した前記インターネットゲートウェイ端末に故障通知レスポンスとして送信し、
更に、当該故障通知レスポンスを受信した当該インターネットゲートウェイ端末が前記リモートメンテナンスの要求に移行する、
以上の一連の処理を順次実施する、
ことを特徴とする請求項２、３、４、５、６、７又は８に記載のリモートメンテナンス実施方法。
【請求項１０】
各ローカルネットワークにより任意数の内線端末とＩＰ接続してそれぞれのインターネットゲートウェイ端末の支配下とする一方、当該それぞれのインターネットゲートウェイ端末とインターネットを介してＶＰＮゲートウェイ間でＯＳＩ参照モデルのネットワーク層においてＶＰＮセッションを実現するＩＰｓｅｃを確立することで、当該ＶＰＮゲートウェイを含む保守センタからリモートメンテナンスを行うシステムであって、
前記インターネットゲートウェイ端末におけるルータ部内にそのローカルネットワークとＶＰＮ処理部との間にＮＡＴを設け、グローバル側のアドレスをＶＰＮＮＡＴ用ローカルＩＰアドレスとして前記保守センタから付与及び解放を行う機能構成にシステム構築する、
ことを特徴とするリモートメンテナンス実施システム。

【請求項１１】
前記保守センタは、
前記インターネットゲートウェイ端末からリモートメンテナンス対象の内線端末名の通知を受けて当該リモートメンテナンス対象の内線端末名に対応するＶＰＮアクセス用のＶＰＮＮＡＴ用ローカルアドレスの付与を行う保守サーバと、
前記リモートメンテナンスを行うリモートメンテナンス装置と、
当該リモートメンテナンス装置からの、当該リモートメンテナンス対象の内線端末名に対応するＶＰＮＮＡＴ用ローカルＩＰアドレスへアクセスを経由するＶＰＮゲートウェイとを、
保守センタローカルネットワークにてネットワーク構築する、
ことを特徴とする請求項１０に記載のリモートメンテナンス実施システム。
【請求項１２】
前記インターネットゲートウェイ端末は、
前記保守センタにリモートメンテナンス対象の内線端末名を通知するサーバ部と、
当該通知したことにより当該保守センタから付与されたＶＰＮアクセス用のＶＰＮＮＡＴ用ローカルＩＰアドレスと当該リモートメンテナンス対象の内線端末名のＩＰアドレスを割りつけるＶＰＮＮＡＴ及び当該保守センタの前記ＶＰＮゲートウェイとＶＰＮトンネルを確立するＶＰＮ処理部のルータ部とで構成して、
前記ＶＰＮゲートウェイを介した、リモートメンテナンス対象端末名に対するＶＰＮＮＡＴ用ローカルＩＰアドレスへのアクセスにより、前記リモートメンテナンスを行うリモートメンテナンス装置からの、前記内線端末へのパケット転送を可能ならしめる機能を構築する、
ことを特徴とする請求項１０又は１１に記載のリモートメンテナンス実施システム。
【請求項１３】
各ローカルネットワークにより任意数の内線端末とＩＰ接続してそれぞれのインターネットゲートウェイ端末の支配下とする一方、当該それぞれのインターネットゲートウェイ端末とインターネットを介してＶＰＮゲートウェイ間でＯＳＩ参照モデルのネットワーク層においてＶＰＮセッションを実現するＩＰｓｅｃを確立することで、当該ＶＰＮゲートウェイを含む保守センタからリモートメンテナンスを行うシステムにおける、当該インターネットゲートウェイ端末で用いられるプログラムであって、
当該インターネットゲートウェイ端末が設置された後に、リモートメンテナンスサービスを利用する場合に、前記保守センタに対して設置した旨を通知する設置通知処理を当該インターネットゲートウェイ端末に行わせる前記プログラムの実行により、
前記設置について前記保守センタの保守サーバに設置通知コマンドを通知した後に、当該保守サーバからの当該設置通知コマンドに対するレスポンスを受信すると当該レスポンスとして受けたＩＰｓｅｃの認証鍵を自己のルータ部に対して設定する、
以上の一連の手順を踏む、
ことを特徴とするリモートメンテナンス実施プログラム。
【請求項１４】
各ローカルネットワークにより任意数の内線端末とＩＰ接続してそれぞれのインターネットゲートウェイ端末の支配下とする一方、当該それぞれのインターネットゲートウェイ端末とインターネットを介してＶＰＮゲートウェイ間でＯＳＩ参照モデルのネットワーク層においてＶＰＮセッションを実現するＩＰｓｅｃを確立することで、当該ＶＰＮゲートウェイを含む保守センタからリモートメンテナンスを行うシステムにおける、当該インターネットゲートウェイ端末にて用いられるプログラムであって、
当該インターネットゲートウェイ端末への、前記内部端末からのＷＥＢアクセス、当該インターネットゲートウェイ端末の操作者によるボタン操作の何れかにより、リモートメンテナンスを要求するリモートメンテナンス要求処理を当該インターネットゲートウェイ端末に行わせる前記プログラムの実行により、
リモートメンテナンス対象である前記内線端末名及び前記インターネットゲートウェイ

端末のグローバルＩＰアドレスを、リモートメンテナンス要求コマンドとして前記保守サーバに通知した後に、
前記リモートメンテナンス要求コマンドに対するレスポンスを受けて、当該レスポンスとして受けた、内線端末名に対する実ローカルＩＰアドレスを取得して、当該内線端末名に対する実ローカルＩＰアドレスと当該レスポンスとして受けたＶＰＮＮＡＴ用ローカルＩＰアドレスとを静的ＮＡＴとして設定させる、
以上の一連の手順を踏む、
ことを特徴とするリモートメンテナンス実施プログラム。
【請求項１５】
各ローカルネットワークにより任意数の内線端末とＩＰ接続してそれぞれのインターネットゲートウェイ端末の支配下とする一方、当該それぞれのインターネットゲートウェイ端末とインターネットを介してＶＰＮゲートウェイ間でＯＳＩ参照モデルのネットワーク層においてＶＰＮセッションを実現するＩＰｓｅｃを確立することで、当該ＶＰＮゲートウェイを含む保守センタからリモートメンテナンスを行うシステムにおける、当該インターネットゲートウェイ端末にて用いられるプログラムであって、
前記保守センタより行われる前記リモートメンテナンスの作業が終了した旨の通知に係るリモートメンテナンス終了処理を、当該通知を受けた前記インフェースゲートウェイ端末に行わせる前記プログラムの実行により、
前記保守センタからのリモートメンテナンス終了コマンドの受信を契機に、当該リモートメンテナンス終了コマンドに関する処理を行い、リモートメンテナンス終了レスポンスを送信して、
前記保守センタからＶＰＮ解放コマンドとしてリモートメンテナンス対象の内線端末名の通知を受けた場合には、当該受けた内線端末名に対する実ローカルＩＰアドレスを取得し、取得した実ローカルＩＰアドレスに対するＶＰＮＮＡＴ用ローカルアドレスとの静的ＮＡＴを解放する、
以上の一連の手順を踏む、
ことを特徴とするリモートメンテナンス実施プログラム。
【請求項１６】
各ローカルネットワークにより任意数の内線端末とＩＰ接続してそれぞれのインターネットゲートウェイ端末の支配下とする一方、当該それぞれのインターネットゲートウェイ端末とインターネットを介してＶＰＮゲートウェイ間でＯＳＩ参照モデルのネットワーク層においてＶＰＮセッションを実現するＩＰｓｅｃを確立することで、当該ＶＰＮゲートウェイを含む保守センタからリモートメンテナンスを行うシステムにおいて、当該保守センタにて用いられるプログラムであって、
前記リモートメンテナンスの要求に対応するリモートメンテナンス要求処理を前記保守サーバに行わせる前記プログラムの実行により、
前記要求を受けて、前記リモートメンテナンスの要求に係るリモートメンテナンス対象の前記内線端末に付与するＶＰＮＮＡＴ用ローカルＩＰアドレス及び内線端末名を、当該要求を行った前記インターネットゲートウェイ端末にリモートメンテナンス要求レスポンスとして送信すると共に、当該インターネットゲートウェイ端末のグローバルＩＰアドレスとの間において共有されるＩＰｓｅｃの認証鍵を用いたＩＰｓｅｃによるＶＰＮトンネルの確立を、自己のＶＰＮゲートウェイに指示し、自己の当該ＶＰＮゲートウェイに対して、ＶＰＮＮＡＴ用ローカルＩＰアドレス宛のパケットを、当該指示により確立されるＶＰＮトンネルのＶＰＮ処理対象パケットとする設定を行う、
以上の一連の手順を踏む、
ことを特徴とするリモートメンテナンス実施プログラム。
【請求項１７】
各ローカルネットワークにより任意数の内線端末とＩＰ接続してそれぞれのインターネットゲートウェイ端末の支配下とする一方、当該それぞれのインターネットゲートウェイ端末とインターネットを介してＶＰＮゲートウェイ間でＯＳＩ参照モデルのネットワーク層

においてＶＰＮセッションを実現するＩＰｓｅｃを確立することで、当該ＶＰＮゲートウェイを含む保守センタからリモートメンテナンスを行うシステムにて、当該保守センタにて用いられるプログラムであって、
新たに設置された前記インターネットゲートウェイ端末からの設置通知コマンドを処理する設定通知コマンド処理を前記保守センタに行わせる前記プログラムの実行により、
前記設置通知コマンドに応じて、前記リモートメンテナンスのための共通情報であるＩＰｓｅｃの認証鍵を生成して、当該設置通知コマンドを通知してきた前記インターネットゲートウェイ端末にレスポンスする、
以上の一連の手順を踏む、
ことを特徴とするリモートメンテナンス実施プログラム。

【請求項１８】
各ローカルネットワークにより任意数の内線端末とＩＰ接続してそれぞれのインターネットゲートウェイ端末の支配下とする一方、当該それぞれのインターネットゲートウェイ端末とインターネットを介してＶＰＮゲートウェイ間でＯＳＩ参照モデルのネットワーク層においてＶＰＮセッションを実現するＩＰｓｅｃを確立することで、当該ＶＰＮゲートウェイを含む単一の保守センタからリモートメンテナンスを行うシステムにおいて、当該保守センタにて用いられるプログラムであって、
前記保守センタにおける終了ボタンが押されたことを契機に、前記リモートメンテナンスの作業が終了したことを通知するリモートメンテナンス終了処理を、前記保守サーバに行わせる前記プログラムの実行により、
ＶＰＮＮＡＴ用ローカルＩＰアドレスで確立されたＶＰＮトンネルを経由して、当該ＶＰＮトンネルを確立させた前記インターネットゲートウェイ端末のサーバ部に対して、リモートメンテナンス終了コマンドを送信した後に、
当該リモートメンテナンス終了のレスポンスを受信すると、該当内線端末に対するメンテナンスが全て終了したかのを第１判断を行い、
当該第１判断にて肯定の場合には当該終了した前記内線端末は前記インターネットゲートウェイ端末の前記サーバ部かルータ部かの何れかであるかの第２判断を行う一方、否定の場合にはこのプログラムを終了し、
当該第２判断にて否定の場合にはＶＰＮＮＡＴ解放処理へ移行する一方、肯定の場合には対応する前記インターネットゲートウェイ端末に対するリモートメンテナンスを全て終了したかの第３判断を行い、
当該第３判断にて肯定の場合にはＶＰＮ終了処理へ移行する一方、否定の場合にはこのプログラムを終了する、
以上の一連の手順を踏む、
ことを特徴とするリモートメンテナンス実施プログラム。

【請求項１９】
前記ＶＰＮＮＡＴ解放処理は、
リモートメンテナンス要求を受けて設定したリモートメンテナンス対象の内線端末名に対するＶＰＮＮＡＴ用ローカルＩＰアドレスを、確立した前記ＶＰＮトンネルへのＶＰＮ処理対象パケットから解除する様、前記ＶＰＮゲートウェイに対して行い、前記インターネットゲートウェイ端末に対して、リモートメンテナンス対象の内線端末名を通知し、その後、前記第３判断にリターンする一連の処理であり、
前記ＶＰＮ終了処理は、
ＩＰｓｅｃセッションの終了をＶＰＮ終了コマンドとして、前記インターネットゲートウェイ端末に対して送信して、前記ＶＰＮゲートウェイに、リモートメンテナンス実施要求の際に設定した前記ＶＰＮトンネルの解除させ、当該ＶＰＮゲートウェイと当該インターネットゲートウェイ端末間で確立されているＶＰＮトンネル処理を終了させる一連の処理である、
ことを特徴とする請求項１８に記載のリモートメンテナンス実施プログラム。

【請求項２０】

請求項１３、１４、１５、１６、１７、１８又は１９に記載のリモートメンテナンス実施プログラムによる一連の手続を実録した、
　ことを特徴とするリモートメンテナンス実施プログラムを記録した記録媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、インターネットに接続された保守センタからインターネットゲートウェイ端末自体及びそのインターネットゲートウェイ端末配下のローカルネットワークに接続されたパソコン等の内線端末をインターネット経由でＶＰＮを利用してリモートメンテナンスを行うリモートメンテナンス実施方法、その実施に直接使用するリモートメンテナンスシステム、プログラム及び同記録媒体に関するものである。
【０００２】
【従来の技術】
従来、インターネットに接続された保守センタからインターネットゲートウェイ端末（以下、情流ＧＷ端末）自体及びその情流ＧＷ端末に接続されたローカルネットワーク上のパソコン（以下、内線端末）をインターネット経由でＶＰＮを利用してリモートメンテナンスを行うリモートメンテナンス実施方法（以下、ＶＰＮリモートメンテナンスと呼ぶ）として、特願平２０００－０００４９６で提案されている方法がある。
【０００３】
しかし、特願平２０００－０００４９６の方法で提案されているＶＰＮリモートメンテナンスでは、複数の情流ＧＷ端末に対して同時にリモートメンテナンスを行う際、対象となる情流ＧＷ端末配下のローカルネットワークアドレスが重複している場合、保守センタからＶＰＮ経由でリモートメンテナンス対象の情流ＧＷ端末及びその配下の内線端末にパケットを送るとき、対象ローカルＩＰアドレスがバッティングするため、保守センタ側のＶＰＮゲートウェイでは、どちらのローカルネットワークへパケットを送出してよいか判断できず、同時に同じローカルネットワークアドレスを持つ複数の情流ＧＷへのメンテナンスを行うことが不可能であった。
【０００４】
そこで、保守センタのローカルネットワーク内から、配下に同じローカルネットワークアドレスを持つ複数の情流ＧＷへ同時にメンテナンスを行う方法として、インターネット側から各々の情流ＧＷの内部ネットワークを見たときにそのローカルネットワークアドレスがユニークになるようにする手法が考えられる。
【０００５】
具体的には、情流ＧＷの内部に、保守センタ側とＶＰＮ通信するための仮のローカルネットワークアドレス（以下、ＶＰＮＮＡＴ用ＩＰアドレス）とローカルネットワークアドレスを固定して結びつける処理部（以下、ＮＡＴＢＯＸ）を設けるという手法であり、図３２を元に動作を説明する。
【０００６】
図３２において、クライアントＰＣ（ａ）からサーバＰＣ（ｂ）へＶＰＮＮＡＴ経由でＩＰ通信を行う場合の、パケットのアドレスの変化を示すために、まず、各ノードの接続形態を説明する。
クライアントＰＣ（ａ）は、プライベートネットワーク（ｃ）に接続されており192.168.2.103のプライベートＩＰアドレスを持つ。ＶＰＮゲートウェイ（ｄ）は、プライベートネットワーク（ｃ）に接続されており、インターネット（ｅ）側のグローバルＩＰアドレスとして211.0.0.1を持つ。
【０００７】
ＶＰＮルータ（ｆ）は、プライベートネットワーク（ｇ）に接続されており、インターネット側のグローバルＩＰアドレスとして210.0.0.1を持つ。サーバＰＣ（ｂ）はプライベートネットワーク（ｃ）に接続されており、192.168.1.1～192.168.1.254のプライベートＩＰアドレスを持つ。

【０００８】
また、ＶＰＮゲートウェイ（ｄ）と情流ＧＷ（以下、ＶＰＮルータとも呼ぶ）は、ＶＰＮのトンネル（ｈ）を構築している。ＶＰＮゲートウェイ（ｄ）ではＶＰＮルータ（ｂ）へのＶＰＮトンネル（ｈ）に対してのＶＰＮ対象パケットとして10.0.0.0/24が設定されており、ＶＰＮルータ（ｂ）では、ＶＰＮゲートウェイ（ｄ）へのＶＰＮトンネル（ｈ）に対してのＶＰＮ対象パケットとして192.168.2.0/24が設定されている。
【０００９】
また、ＮＡＴＢＯＸ（ｆ１０）は、インターネット（ｅ）側にＶＰＮＮＡＴ用ＩＰアドレスとして10.0.0.1～10.0.0.254のアドレスを持ち、10.0.0.1と192.168.1.1、10.0.0.2と192.168.1.2、…（省略）、…、10.0.0.254と192.168.1.254で静的ＮＡＴが設定されている。
【００１０】
ここで、192.168.1.1のサーバＰＣ（ｂ）について着目すると、ＮＡＴＢＯＸ（ｆ１０）のプライベートネットワーク（ｇ）側から送信元アドレス192.168.1.1のパケットが送出される際は送信元アドレスが10.0.0.1に書き換えられてＮＡＴＢＯＸ（ｆ１０）のインターネット側へ送出され、ＮＡＴＢＯＸ（ｆ１０）のインターネット（ｅ）側から送信先10.0.0.1宛てのパケットが到着すると、送信先アドレスが192.168.1.1に書き換えられてＮＡＴＢＯＸ（ｆ１０）のプライベートネットワーク（ｃ）側に送出される。
【００１１】
以下、クライアントＰＣ（ａ）とサーバＰＣ（ｂ）間で通信を行う際のパケットのアドレス変化を示す。
ここで、クライアントＰＣ（ａ）からサーバＰＣ（ｂ）宛てのオリジナルパケットは、「送信元192.168.2.103：送信先10.0.0.1」で送出され、ＶＰＮゲートウェイ（ｄ）に到着する。
【００１２】
ＶＰＮゲートウェイ（ｄ）は、10.0.0.1のパケットを受信したのでＶＰＮルータ（ｆ）へのＶＰＮトンネル（ｈ）に対してのＶＰＮ対象パケットと判断し、「送信元211.0.0.1：送信先210.0.0.1」の新ＩＰヘッダを付加し、カプセル化を行う。
オリジナルパケットは暗号化されてデータ部に入る。このパケットは、ＶＰＮトンネルを経由してＶＰＮルータのＶＰＮ処理部（ｆ１１）に到達する。
【００１３】
ＶＰＮルータのＶＰＮ処理部（ｆ１１）では、オリジナルパケットが復号化され、「送信元192.168.2.103：送信先10.0.0.1」としてＮＡＴＢＯＸ（ｆ１０）に送出する。ＮＡＴＢＯＸ（ｆ１０）では、外側10.0.0.1と内側192.168.1.1で静的ＮＡＴが設定されており、送信先アドレスが10.0.0.1にマッチするので、アドレス変換が行われ、「送信元192.168.2.103：送信先192.168.1.1」となり、プライベートネットワーク（ｃ）のネットワークに送出される。したがって、このパケットは、サーバＰＣ（ｂ）に到着することができる。
【００１４】
また、サーバＰＣ（ｂ）からクライアントＰＣ（ａ）へのレスポンスオリジナルパケットは、「送信元192.168.1.1：送信先192.168.2.103」で送出され、ＶＰＮルータ（ｆ）に到着する。ＶＰＮルータ（ｆ）では、192.168.2.0/24のパケットを受信したのでＶＰＮゲートウェイ（ｄ）へのＶＰＮトンネル（ｈ）に対してのＶＰＮ対象パケットと判断し、まずＮＡＴＢＯＸ（ｆ１０）にパケットが送られる。
【００１５】
ＮＡＴＢＯＸ（ｆ１０）では、外側10.0.0.1と内側192.168.1.1で静的ＮＡＴが設定されており、送信元アドレスが192.168.1.1にマッチするので、アドレス変換が行われ「送信元10.0.0.1：送信先192.168.2.103」となり、ＶＰＮ処理部（ｂ１１）へ送られる。
【００１６】
ＶＰＮ処理部（ｆ１１）では「送信元210.0.0.1：送信先211.0.0.1」となり新ＩＰヘッダ

を付加し、カプセル化を行う。レスポンスオリジナルパケットは暗号化されてデータ部に入る。このパケットは、ＶＰＮトンネル（ｈ）を経由してＶＰＮゲートウェイ（ｄ）に到達する。ＶＰＮゲートウェイ（ｄ）では、レスポンスオリジナルパケットが復号化され、「送信元10.0.0.1：送信先192.168.2.103」となり、プライベートネットワーク（ｃ）のネットワークに送出される。したがって、このパケットは、クライアントＰＣ（ａ）に到着することができる。

【００１７】

以上、保守センタから情流ＧＷ（ｆ）１台で配下のローカルネットワークが１つの場合について保守センタのプライベートネットワーク（ｇ）と情流ＧＷ（ｆ）配下のプライベートネットワーク（ｃ）を静的ＶＰＮＮＡＴ機能を適用して通信を行った場合の動作概要について説明した。なお、図中（ｆ１）はＮＡＴＢＯＸ（ｆ１０）とＶＰＮ処理部（ｆ１１）で構成されるルータ部である。

【００１８】

次に、保守センタから情流ＧＷ（ｆ′）（ｆ″）２台の配下のプライベートネットワーク（ｇ′）（ｇ″）が２つあり、そのプライベートネットワークアドレスが重複している場合について、保守センタのプライベートネットワーク（ｃ）から各々の情流ＧＷ（ｆ′）（ｆ″）配下のプライベートネットワーク（ｇ′）（ｇ″）に対して静的ＶＰＮＮＡＴ機能を適用して通信を行う場合の動作概要について説明する。

【００１９】

図３３に情流ＧＷ（ｆ′）（ｆ″）２台の配下のプライベートネットワークネットワークアドレスが同じケースにおいて、静的ＶＰＮＮＡＴ機能を用いて保守センタから２つの情流ＧＷ（ｆ′）（ｆ″）配下のアドレスのサーバＰＣ（ｂ１）～（ｂ４）に同時にアクセスする方法を示す。

【００２０】

ここで、クライアントＰＣ（ａ）からサーバＰＣ（ｂ１）～（ｂ４）へＶＰＮＮＡＴ経由でＩＰ通信を行う場合の、パケットのアドレスの変化を示すために、まず、各ノードの接続形態を説明する。クライアントＰＣ（ａ）は、プライベートネットワーク（ｇ′）（ｇ″）に接続されており192.168.2.103のプライベートＩＰアドレスを持つ。ＶＰＮゲートウェイ（ｄ）は、プライベートネットワーク（ｃ）に接続されており、インターネット（ｅ）側のグローバルＩＰアドレスとして211.0.0.1を持つ。

【００２１】

ＶＰＮルータ（ｆ′）は、プライベートネットワーク（ｇ′）に接続されており、インターネット（ｅ）側のグローバルＩＰアドレスとして210.0.0.1を持つ。サーバＰＣ（ｂ１）（ｂ２）はＶＰＮルータ（ｆ′）の内部ローカルネットワーク192.168.1.0/24に接続されており、192.168.1.1～192.168.1.254のプライベートＩＰアドレスを持つ。また、ＶＰＮゲートウェイ（ｄ）とＶＰＮルータ（ｆ′）は、ＶＰＮのトンネル（ｈ′）を構築している。

【００２２】

ＶＰＮゲートウェイ（ｄ）ではＶＰＮルータ（ｆ′）へのＶＰＮトンネル（ｈ′）に対してのＶＰＮ対象パケットとして10.0.0.0/24が設定されており、ＶＰＮルータ（ｆ′）では、ＶＰＮゲートウェイ(ｄ)へのＶＰＮトンネル（ｈ′）に対してのＶＰＮ対象パケットとして192.168.2.0/24が設定されている。

【００２３】

また、ＮＡＴＢＯＸ（ｆ１０′）は、インターネット（e）側にＶＰＮＮＡＴ用ＩＰアドレスとして10.0.0.1～10.0.0.254のアドレスを持ち、10.0.0.1と192.168.1.1、10.0.0.2と192.168.1.2、…、（省略）、…、10.0.0.254と192.168.1.254で静的ＮＡＴが設定されている。

【００２４】

ここで、192.168.1.1のサーバＰＣ（ｂ１）（ｂ２）について着目すると、ＮＡＴＢＯＸ（ｆ１０）のプライベートネットワーク（ｇ′）側から送信元アドレス192.168.1.1のパ

ケットが送出される際は送信元アドレスが10.0.0.1に書き換えられてＮＡＴＢＯＸ（ｆ１０′）のインターネット側へ送出され、ＮＡＴＢＯＸ（ｆ１０′）のインターネット（ｅ）側から送信先10.0.0.1宛てのパケットが到着すると、送信先アドレスが192.168.1.1に書き換えられてＮＡＴＢＯＸ（ｆ′）のプライベートネットワーク側に送出される。

【００２５】

ＶＰＮルータ（ｆ″）は、プライベートネットワーク（ｇ″）に接続されており、インターネット（ｅ）側のグローバルＩＰアドレスとして210.0.1.1を持つ。サーバＰＣ（ｂ３）（ｂ４）はＶＰＮルータ（ｆ″）の内部ローカルネットワーク192.168.1.0/24に接続されており、192.168.1.1～192.168.1.254のプライベートＩＰアドレスを持つ。

【００２６】

また、ＶＰＮゲートウェイ（ｄ）とＶＰＮルータ（ｆ″）は、ＶＰＮのトンネル（ｈ″）を構築している。ＶＰＮゲートウェイ（ｄ）ではＶＰＮルータ（ｆ″）へのＶＰＮトンネル（ｈ″）に対してのＶＰＮ対象パケットとして10.0.1.0/24が設定されており、ＶＰＮルータ（ｆ″）では、ＶＰＮゲートウェイ（ｄ）へのＶＰＮトンネル（ｈ″）に対してのＶＰＮ対象パケットとして192.168.2，0/24が設定されている。

【００２７】

また、ＮＡＴＢＯＸ（ｆ１０″）は、インターネット（ｅ）側にＶＰＮＮＡＴ用ＩＰアドレスとして10.0.1.1～10.0.1.254のアドレスを持ち、10.0.1.1と192.168.1.1、10.0.1.2と192.168.1.2、…、（省略）、…、10.0.1.254と192.168.1.254で静的ＮＡＴが設定されている。

【００２８】

ここで、192.168.1.1のサーバＰＣＢについて着目すると、ＮＡＴＢＯＸ（ｆ″）のプライベートネットワーク（ｇ″）側から送信元アドレス192.168.1.1のパケットが送出される際は送信元アドレスが10.0.1.1に書き換えられてＮＡＴＢＯＸ（ｆ″）のインターネット（ｅ）側へ送出され、ＮＡＴＢＯＸ（ｆ″）のインターネット（ｅ）側から送信先10.0.1.1宛てのパケットが到着すると、送信先アドレスが192.168.1.1に書き換えられてＮＡＴＢＯＸ（ｆ″）のプライベートネットワーク（ｇ″）側に送出される。

【００２９】

以上、保守センタから情流ＧＷ（ｆ′）（ｆ″）２台の配下のプライベートネットワーク（ｇ′）（ｇ″）が２つあり、そのプライベートネットワークアドレスが重複している場合について、保守センタのプライベートネットワーク（ｃ）から各々の情流ＧＷ（ｆ′）（ｆ″）配下のプライベートネットワーク（ｇ′）（ｇ″）に対して静的ＶＰＮＮＡＴ機能を適用して通信を行う場合の動作概要について説明した。

【００３０】

言うまでもないが、前記示した「情流ＧＷ２台の配下のプライベートネットワークが２つあり、そのプライベートネットワークアドレスが重複している場合」の動作は、「情流ＧＷＮ（Ｎは任意の自然数）台の配下のプライベートネットワークがＮ個あり、そのプライベートネットワークアドレスが重複している場合」にも適用できる。

【００３１】

従って、図３３に示す方法で、静的ＶＰＮＮＡＴを構築した上で保守センタからアクセスすることにより、複数の情流ＧＷ端末（ＶＰＮルータ）に対して同時にリモートメンテナンスを行う際、対象となる情流ＧＷ端末配下のプライベートネットワークアドレスが重複している場合でも、保守センタからＶＰＮ経由でリモートメンテナンス対象の情流ＧＷ端末及びその配下の内線端末（サーバＰＣ）にパケットを送るとき、対象プライベートＩＰアドレスを静的ＶＰＮＮＡＴで割り付けたＮＡＴＢＯＸのインターネット側のアドレス向けに送出することにより、保守センタ側のＶＰＮゲートウェイでは、どちらのプライベートネットワークへパケットを送出してよいか判断でき、同時に同じプライベートネットワークアドレスを持つ複数の情流ＧＷ端末へのメンテナンスを行うことが可能となる。以下、これを「静的ＶＰＮＮＡＴ方式」と呼ぶことにする。

【００３２】

また、特願平２０００－０００４９６にて提案されているＶＰＮリモートメンテナンスでは、保守センタのＶＰＮゲートウェイのグローバルＩＰアドレスを情流ＧＷ端末が事前に知っていることを必須とし、その対応策とて、事前に情流ＧＷ端末にＶＰＮゲートウェイのグローバルＩＰアドレスを埋め込んで出荷するという方法が採られていた。

【００３３】

【発明が解決しようとする課題】

しかし、前記説明した「静的ＶＰＮＮＡＴ」方式により保守センタのプライベートネットワークから情流ＧＷ端末配下の全てのプライベートネットワークに対してアクセスする場合は、情流ＧＷ端末とＶＰＮゲートウェイ間でＶＰＮを構築する時点で、情流ＧＷ端末においてＶＰＮＮＡＴ用ＩＰアドレスとプライベートネットワークの実ローカルＩＰアドレスを事前に静的ＶＰＮＮＡＴで割り付けておく必要があった。

【００３４】

この場合、保守センタ側がユニークに管理するＶＰＮＮＡＴ用ＩＰアドレスリソース（プライベートＩＰアドレス）を保守対象の情流ＧＷ端末配下のプライベートネットワークの端末台数分だけ事前に割り当てる必要があり、実際にメンテナンスを行う対象端末数に対して、非常に膨大な数のＶＰＮＮＡＴ用ＩＰアドレスリソースを必要とした。すなわち静的ＶＰＮＮＡＴ方式では、同クラスのプライベートＩＰアドレスを使った場合、最大約１６７０万台の情流ＧＷ端末配下の内線端末だけがリモートメンテナンス対象端末であった。

【００３５】

例えば、同クラスのプライベートアドレスをＶＰＮＮＡＴ用ＩＰアドレスリソースとして利用し、情流ＧＷ端末配下のプライベートネットワークのサブネットマスクが全て２４ビットだった場合は最大約６万５千加入情流ＧＷ端末配下のプライベートネットワークのサブネットマスクが全て１６ビットだった場合は最大約２５６加入の情流ＧＷ端末配下の端末しかメンテナンス対象とできないという制約事項があった。

【００３６】

また、静的ＶＰＮＮＡＴ方式を使って、特願平２０００－０００４９６の方法で提案されているＶＰＮリモートメンテナンスを行う場合は、リモートメンテナンス要求をあげた情流ＧＷ端末配下の全ての内線端末リソースに保守センタからアクセスが可能となってしまうという問題点があった。

【００３７】

また、ＶＰＮリモートメンテナンスの設置通知数が増大し、ＶＰＮリモートメンテナンスサービスの同時利用者がＶＰＮゲートウェイの許容ＶＰＮセッション数を超える場合、保守センタ側でＶＰＮゲートウェイを増設して設置する必要があり、その場合、ＶＰＮゲートウェイのグローバルＩＰアドレスを端末に設定させる手段が存在しなかった。また、保守センタのＶＰＮゲートウェイアドレスを何らかの手段でインターネットゲートウェイ管理者に通知し、手動でＶＰＮゲートウェイアドレスを設定させる方法は、リモートメンテナンスの際に人手が伴うので、ＶＰＮリモートメンテナンスには適用できないという問題点があった。

【００３８】

ここにおいて、本発明の解決すべき主要な目的は次の通りである。

【００３９】

本発明の第１の目的は、保守センタからインターネットのＶＰＮ経由で、配下のプライベート（ローカル）ネットワークアドレスの重複を許容した複数の情流ＧＷ端末及びその内線端末を同時にリモートメンテナンスする際、リモートメンテナンス対象の情流ＧＷ端末及び内線端末数の制限を、保守センタ側で管理するＩＰアドレスリソースの上限まで許容し、可能な限り多数の情流ＧＷ端末及びその配下の内線端末のリモートメンテナンスを同時に行うことを可能とするリモートメンテナンス実施方法、システム、プログラム及び記録媒体を提供せんとするものである。

【００４０】

本発明の第２の目的は、保守センタ側がユニークに管理するＶＰＮＮＡＴ要ＩＰアドレスリソースを保守対象の情流ＧＷ端末配下のプライベートネットワークの端末台数分だけ事前に割り当てる必要のないリモートメンテナンス実施方法、システム、プログラム及び記録媒体を提供せんとするものである。

【００４１】

本発明の第３の目的は、ＶＰＮリモートメンテナンスを行う場合に、リモートメンテナンス要求をあげた情流ＧＷ端末配下のすべての内線端末リソースに保守センタからのアクセスが起こらないようにしたリモートメンテナンス実施方法、システム、プログラム及び記録媒体を提供せんとするものである。

【００４２】

本発明の第４の目的は、ＶＰＮリモートメンテナンスの設置通知数が増大しＶＰＮリモートメンテナンスの同時利用者が、ＶＰＮゲートウェイの許容ＶＰＮセッション数を超える場合、保守センタ側でＶＰＮゲートウェイを増設して設置する必要があるが、その場合にＶＰＮゲートウェイのグローバルＩＰアドレスを端末に設定するようにしたリモートメンテナンス実施方法、システム、プログラム及び記録媒体を提供せんとするものである。

【００４３】

本発明の他の目的は、明細書、図面、特に特許請求の範囲の各請求項の記載から自ずと明らかとなろう。

【００４４】

【課題を解決するための手段】

本発明方法は、上記課題の解決に当たり、各ローカルネットワークにより任意数の内線端末とＩＰ接続してそれぞれのインターネットゲートウェイ端末の支配下とする一方、当該それぞれのインターネットゲートウェイ端末とインターネットを介してＶＰＮゲートウェイ間でＯＳＩ参照モデルのネットワーク層においてＶＰＮセッションを実現するＩＰｓｅｃを確立することで、当該ＶＰＮゲートウェイを含む単一の保守センタからリモートメンテナンスを行う実施方法であり、当該インターネットゲートウェイ端末におけるルータ部内に、その前記ローカルネットワークとＶＰＮ処理部との間にＶＰＮＮＡＴを設け、グローバル側のアドレスをＶＰＮＮＡＴ用ローカルＩＰアドレスとして当該保守センタから付与及び解放を行うことで実施した、特徴的構成手法を講じる。

【００４５】

本発明システムは、上記課題の解決に当たり、各ローカルネットワークにより任意数の内線端末とＩＰ接続してそれぞれのインターネットゲートウェイ端末の支配下とする一方、当該それぞれのインターネットゲートウェイ端末とインターネットを介してＶＰＮゲートウェイ間でＯＳＩ参照モデルのネットワーク層においてＶＰＮセッションを実現するＩＰｓｅｃを確立することで、当該ＶＰＮゲートウェイを含む単一の保守センタからリモートメンテナンスを行う実施システムであり、当該インターネットゲートウェイ端末におけるルータ部内に、その前記ローカルネットワークとＶＰＮ処理部との間にＶＰＮＮＡＴ手段を設け、グローバル側のアドレスをＶＰＮＮＡＴ用ローカルＩＰアドレスとして当該保守センタから付与及び解放を行える機能構成にシステム構築した、特徴的構成手段を講じる。

【００４６】

本発明プログラムは、上記課題の解決に当たり、各ローカルネットワークにより任意数の内線端末とＩＰ接続してそれぞれのインターネットゲートウェイ端末の支配下とする一方、当該それぞれのインターネットゲートウェイ端末とインターネットを介してＶＰＮゲートウェイ間でＯＳＩ参照モデルのネットワーク層においてＶＰＮセッションを実現するＩＰｓｅｃを確立することで、当該ＶＰＮゲートウェイを含む保守センタからリモートメンテナンスを行うシステムにて、当該インターネットゲートウェイ端末、当該保守センタにて用いられるプログラムで、グローバル側のアドレスをＶＰＮＮＡＴ用ローカルＩＰアドレスとして当該保守センタから付与、解放を行う各種の処理手順を実行した、特徴的構成手順を講じる。

【００４７】
本発明記録媒体は、上記課題の解決に当たり、本発明プログラムにより一連の完結手続を実録した、特徴的構成手続を講じる。
【００４８】
更に具体的に詳説すると、当該課題の解決では、本発明が次に列挙する新規な各特徴的構成手法、手段、手順又は手続を講じることにより、上記目的を達成する様になされる。
【００４９】
本発明方法の第１の特徴は、各ローカルネットワークにより任意数の内線端末とＩＰ接続してそれぞれのインターネットゲートウェイ端末の支配下とする一方、当該それぞれのインターネットゲートウェイ端末とインターネットを介してＶＰＮゲートウェイ間でＯＳＩ参照モデルのネットワーク層においてＶＰＮセッションを実現するＩＰｓｅｃを確立することにより、当該ＶＰＮゲートウェイを含む保守センタからリモートメンテナンスを行う実施方法であって、前記それぞれのインターネットゲートウェイ端末におけるルータ部内に、その前記ローカルネットワークとＶＰＮ処理部との間にＶＰＮＮＡＴを設け、グローバル側のアドレスをＶＰＮＮＡＴ用ローカルＩＰアドレスとして前記保守センタの保守サーバから付与及び解放を行うことにより前記リモートメンテナンスを実施してなるリモートメンテナンス実施方法の構成採用にある。
【００５０】
本発明方法の第２の特徴は、上記本発明方法の第１の特徴における前記実施方法における前記リモートメンテナンスの要求が、当該要求を行う前記インターネットゲートウェイ端末が、リモートメンテナンス対象である内線端末名及び当該インターネットゲートウェイ端末のグローバルＩＰアドレスを、リモートメンテナンス要求コマンドとして前記保守サーバに通知すると、当該通知を受けた当該保守サーバが、当該通知したリモートメンテナンス対象の前記内線端末に付与するＶＰＮＮＡＴ用ローカルＩＰアドレス及び内線端末名を、当該通知をしてきたインターネットゲートウェイ端末にリモートメンテナンス要求レスポンスとしてレスポンスすると共に、当該インターネットゲートウェイ端末のグローバルＩＰアドレスとの間において設置通知の際に共有されるＩＰｓｅｃの認証鍵を用いたＩＰｓｅｃによるＶＰＮトンネルの確立を自己のＶＰＮゲートウェイに設定させ、当該ＶＰＮゲートウェイに対してＶＰＮＮＡＴ用ローカルＩＰアドレス宛のパケットを前記確立したＶＰＮトンネルのＶＰＮ処理対象パケットとする設定を行い、前記レスポンスを受けたインターネットゲートウェイ端末が、受けた前記内線端末名に対する実ローカルＩＰアドレスを取得して、当該内線端末名に対する実ローカルＩＰアドレスと前記ＶＰＮＮＡＴ用ローカルＩＰアドレスとを静的ＮＡＴとし自己のルータ部に対して設定を行う、以上の一連の処理を順次実施してなる、リモートメンテナンス実施方法の構成採用にある。
【００５１】
本発明方法の第３の特徴は、上記本発明方法の第２の特徴における前記リモートメンテナンスの実施が、前記リモートメンテナンス対象である前記内線端末に対して、前記ＶＰＮＮＡＴ用ローカルＩＰアドレスで前記確立されたＶＰＮトンネルを経由して、前記保守センタから行われてなる、リモートメンテナンス実施方法の構成採用にある。
【００５２】
本発明方法の第４の特徴は、上記本発明方法の第２又は第３の特徴における前記リモートメンテナンスの終了が、先ず、前記ＶＰＮＮＡＴ用ローカルＩＰアドレスで前記確立されたＶＰＮトンネルを経由して、当該ＶＰＮトンネルを確立させた前記インターネットゲートウェイ端末のサーバ部に対して、リモートメンテナンス終了コマンドを送信し、次に、当該送信を受けたサーバ部において、当該リモートメンテナンス終了コマンドに係る処理を行い、リモートメンテナンス終了レスポンスを送信し、その後、当該リモートメンテナンス終了レスポンスを受信した保守サーバにて、該当内線端末に対するメンテナンスが全て終了したかの第１判断を行い、当該第１判断にて肯定の場合には当該終了した内線端末は前記インターネットゲートウェイ端末の前記サーバ部、前記ルータ部の何れかであるかの第２判断を行う一方、否定の場合には判断処理を終了し、当該第２判断にて否定の場合

にはＶＰＮＮＡＴ解放処理へ移行し、他方肯定の場合には対応する前記インターネットゲートウェイ端末に対するリモートメンテナンスを全て終了したかの第３判断を行い、当該第３判断にて肯定の場合にはＶＰＮ終了処理へ移行するとともに否定の場合には当該判断処理を終了する、以上の一連の処理を順次実施してなる、リモートメンテナンス実施方法の構成採用にある。

【００５３】

本発明方法の第５の特徴は、上記本発明方法の第４の特徴における前記ＶＰＮＮＡＴ解放処理が、先ず、前記保守サーバが、前記リモートメンテナンスの要求の際に設定した前記リモートメンテナンス対象の内線端末名に対するＶＰＮＮＡＴ用ローカルＩＰアドレスを、前記確立したＶＰＮトンネルへのＶＰＮ処理対象パケットから解除する一方で、前記インターネットゲートウェイ端末に対して当該リモートメンテナンス対象の内線端末名を通知した後に、当該通知を受けたインターネットゲートウェイ端末が、当該受けた内線端末名に対する実ローカルＩＰアドレスを取得して、それに対するＶＰＮＮＡＴ用ローカルアドレスとの静的ＮＡＴを解放し、引続き、前記保守サーバが、前記第３判断を行いその判断結果に従う、以上の一連の処理を順次実施してなる、リモートメンテナンス実施方法の構成採用にある。

【００５４】

本発明方法の第６の特徴は、上記本発明方法の第４又は第５の特徴における前記ＶＰＮ終了処理が、前記保守サーバが、ＩＰｓｅｃセッションの終了をＶＰＮ終了コマンドとして、前記インターネットゲートウェイ端末に通知して、当該通知を受けたインターネットゲートウェイ端末が、当該ＶＰＮ終了コマンドに対する返答を当該保守サーバにＶＰＮ終了レスポンスとして送信し、前記保守サーバが、前記ＶＰＮゲートウェイに、前記リモートメンテナンスの要求に際に設定した前記ＶＰＮトンネルを解除させ、当該ＶＰＮゲートウェイと前記インターネットゲートウェイ端末間で確立されているＶＰＮトンネル処理を終了する、以上の一連の処理を順次実施してなるリモートメンテナンス実施方法の構成採用にある。

【００５５】

本発明方法の第７の特徴は、上記本発明方法の第２、第３、第４、第５又は第６の特徴における前記設置通知が、新たに設置された前記インターネットゲートウェイ端末の前記サーバ部から、当該設置について前記保守サーバに設置通知コマンドを通知し、当該設置通知コマンドを受けた当該保守サーバにより、前記リモートメンテナンスのための共通情報であるＩＰｓｅｃの認証鍵を生成して、当該設置通知コマンドを通知してきた前記インターネットゲートウェイ端末にレスポンスし、当該レスポンスを受信した前記インターネットゲートウェイ端末は、ＩＰｓｅｃの認証鍵を自己の前記ルータ部に対して設定する、以上の一連の処理を順次実施してなるリモートメンテナンス実施方法の構成採用にある。

【００５６】

本発明方法の第８の特徴は、上記本発明方法の第２、第３、第４、第５、第６又は第７の特徴における前記実施方法が、前記リモートメンテナンスの要求、前記設定通知の何れか一方において、前記インターネットゲートウェイ端末の前記サーバ部及び前記ルータ部へのＶＰＮＮＡＴ設定処理を実施してなるリモートメンテナンス実施方法の構成採用にある。

【００５７】

本発明方法の第９の特徴は、上記本発明方法の第２、第３、第４、第５、第６、第７又は第８の特徴における前記実施方法が、前記インターネットゲートウェイ端末に故障発生を検知した場合には、先ず、当該インターネットゲートウェイ端末が、故障通知コマンドとして故障に係る情報を前記保守サーバに送信し、次に、前記保守サーバが前記故障通知コマンドを受信すると当該故障に係る情報を処理して、当該故障通知コマンドを送信した前記インターネットゲートウェイ端末に故障通知レスポンスとして送信し、更に、当該故障通知レスポンスを受信した当該インターネットゲートウェイ端末が前記リモートメンテナンスの要求に移行する、以上の一連の処理を順次実施してなるリモートメンテナンス実施

方法の構成採用にある。

【００５９】

本発明システムの第１の特徴は、各ローカルネットワークにより任意数の内線端末とＩＰ接続してそれぞれのインターネットゲートウェイ端末の支配下とする一方、当該それぞれのインターネットゲートウェイ端末とインターネットを介してＶＰＮゲートウェイ間でＯＳＩ参照モデルのネットワーク層においてＶＰＮセッションを実現するＩＰｓｅｃを確立することで、当該ＶＰＮゲートウェイを含む保守センタからリモートメンテナンスを行うシステムであって、前記インターネットゲートウェイ端末におけるルータ部内にそのローカルネットワークとＶＰＮ処理部との間にＮＡＴを設け、グローバル側のアドレスをＶＰＮＮＡＴ用ローカルＩＰアドレスとして前記保守センタから付与及び解放を行う機能構成にシステム構築してなるリモートメンテナンス実施システムの構成採用にある。

【００６０】

本発明システムの第２の特徴は、上記本発明システムの第１の特徴における前記保守センタが、前記インターネットゲートウェイ端末からリモートメンテナンス対象の内線端末名の通知を受けて当該リモートメンテナンス対象の内線端末名に対応するＶＰＮアクセス用のＶＰＮＮＡＴ用ローカルアドレスの付与を行う保守サーバと、前記リモートメンテナンスを行うリモートメンテナンス装置と、当該リモートメンテナンス装置からの、当該リモートメンテナンス対象の内線端末名に対応するＶＰＮＮＡＴ用ローカルＩＰアドレスへアクセスを経由するＶＰＮゲートウェイとを、保守センタローカルネットワークにてネットワーク構築してなるリモートメンテナンス実施システムの構成採用にある。

【００６１】

本発明システムの第３の特徴は、上記本発明システムの第１又は第２の特徴における前記インターネットゲートウェイ端末が、前記保守センタにリモートメンテナンス対象の内線端末名を通知するサーバ部と、当該通知したことにより当該保守センタから付与されたＶＰＮアクセス用のＶＰＮＮＡＴ用ローカルＩＰアドレスと当該リモートメンテナンス対象の内線端末名のＩＰアドレスを割りつけるＶＰＮＮＡＴ及び当該保守センタの前記ＶＰＮゲートウェイとＶＰＮトンネルを確立するＶＰＮ処理部のルータ部とで構成して、前記ＶＰＮゲートウェイを介した、リモートメンテナンス対象端末名に対するＶＰＮＮＡＴ用ローカルＩＰアドレスへのアクセスにより、前記リモートメンテナンスを行うリモートメンテナンス装置からの、前記内線端末へのパケット転送を可能ならしめる機能を構築してなるリモートメンテナンス実施システムの構成採用にある。

【００６３】

本発明プログラムの第１の特徴は、各ローカルネットワークにより任意数の内線端末とＩＰ接続してそれぞれのインターネットゲートウェイ端末の支配下とする一方、当該それぞれのインターネットゲートウェイ端末とインターネットを介してＶＰＮゲートウェイ間でＯＳＩ参照モデルのネットワーク層においてＶＰＮセッションを実現するＩＰｓｅｃを確立することで、当該ＶＰＮゲートウェイを含む保守センタからリモートメンテナンスを行うシステムにおける、当該インターネットゲートウェイ端末で用いられるプログラムであって、当該インターネットゲートウェイ端末が設置された後に、リモートメンテナンスサービスを利用する場合に、前記保守センタに対して設置した旨を通知する設置通知処理を当該インターネットゲートウェイ端末に行わせる前記プログラムの実行により、前記設置について前記保守センタの保守サーバに設置通知コマンドを通知した後に、当該保守サーバからの当該設置通知コマンドに対するレスポンスを受信すると当該レスポンスとして受けたＩＰｓｅｃの認証鍵を自己のルータ部に対して設定する、一連の手順を踏んでなるリモートメンテナンス実施プログラムの構成採用にある。

【００６４】

本発明プログラムの第２の特徴は、各ローカルネットワークにより任意数の内線端末とＩＰ接続してそれぞれのインターネットゲートウェイ端末の支配下とする一方、当該それぞれのインターネットゲートウェイ端末とインターネットを介してＶＰＮゲートウェイ間でＯＳＩ参照モデルのネットワーク層においてＶＰＮセッションを実現するＩＰｓｅｃを確

立することで、当該ＶＰＮゲートウェイを含む保守センタからリモートメンテナンスを行うシステムにおける、当該インターネットゲートウェイ端末にて用いられるプログラムであって、当該インターネットゲートウェイ端末への、前記内部端末からのＷＥＢアクセス、当該インターネットゲートウェイ端末の操作者によるボタン操作の何れかにより、リモートメンテナンスを要求するリモートメンテナンス要求処理を当該インターネットゲートウェイ端末に行わせる前記プログラムの実行により、リモートメンテナンス対象である前記内線端末名及び前記インターネットゲートウェイ端末のグローバルＩＰアドレスを、リモートメンテナンス要求コマンドとして前記保守サーバに通知した後に、前記リモートメンテナンス要求コマンドに対するレスポンスを受けて、当該レスポンスとして受けた、内線端末名に対する実ローカルＩＰアドレスを取得して、当該内線端末名に対する実ローカルＩＰアドレスと当該レスポンスとして受けたＶＰＮＮＡＴ用ローカルＩＰアドレスとを静的ＮＡＴとして設定させる、以上の一連の手順を踏んでなるリモートメンテナンス実施プログラムの構成採用にある。

【００６５】

本発明プログラムの第３の特徴は、各ローカルネットワークにより任意数の内線端末とＩＰ接続してそれぞれのインターネットゲートウェイ端末の支配下とする一方、当該それぞれのインターネットゲートウェイ端末とインターネットを介してＶＰＮゲートウェイ間でＯＳＩ参照モデルのネットワーク層においてＶＰＮセッションを実現するＩＰｓｅｃを確立することで、当該ＶＰＮゲートウェイを含む保守センタからリモートメンテナンスを行うシステムにおける、当該インターネットゲートウェイ端末にて用いられるプログラムであって、前記保守センタより行われる前記リモートメンテナンスの作業が終了した旨の通知に係るリモートメンテナンス終了処理を、当該通知を受けた前記インフェースゲートウェイ端末に行わせる前記プログラムの実行により、前記保守センタからのリモートメンテナンス終了コマンドの受信を契機に、当該リモートメンテナンス終了コマンドに関する処理を行い、リモートメンテナンス終了レスポンスを送信して、前記保守センタからＶＰＮ解放コマンドとしてリモートメンテナンス対象の内線端末名の通知を受けた場合には、当該受けた内線端末名に対する実ローカルＩＰアドレスを取得し、取得した実ローカルＩＰアドレスに対するＶＰＮＮＡＴ用ローカルアドレスとの静的ＮＡＴを解放する、以上の一連の手順を踏んでなるリモートメンテナンス実施プログラムの構成採用にある。

【００６６】

本発明プログラムの第４の特徴は、各ローカルネットワークにより任意数の内線端末とＩＰ接続してそれぞれのインターネットゲートウェイ端末の支配下とする一方、当該それぞれのインターネットゲートウェイ端末とインターネットを介してＶＰＮゲートウェイ間でＯＳＩ参照モデルのネットワーク層においてＶＰＮセッションを実現するＩＰｓｅｃを確立することで、当該ＶＰＮゲートウェイを含む保守センタからリモートメンテナンスを行うシステムにおいて、当該保守センタにて用いられるプログラムであって、前記リモートメンテナンスの要求に対応するリモートメンテナンス要求処理を前記保守サーバに行わせる前記プログラムの実行により、前記要求を受けて、前記リモートメンテナンスの要求に係るリモートメンテナンス対象の前記内線端末に付与するＶＰＮＮＡＴ用ローカルＩＰアドレス及び内線端末名を、当該要求を行った前記インターネットゲートウェイ端末にリモートメンテナンス要求レスポンスとして送信すると共に、当該インターネットゲートウェイ端末のグローバルＩＰアドレスとの間において共有されるＩＰｓｅｃの認証鍵を用いたＩＰｓｅｃによるＶＰＮトンネルの確立を、自己のＶＰＮゲートウェイに指示し、自己の当該ＶＰＮゲートウェイに対して、ＶＰＮＮＡＴ用ローカルＩＰアドレス宛のパケットを、当該指示により確立されるＶＰＮトンネルのＶＰＮ処理対象パケットとする設定を行う、以上の一連の手順を踏んでなるリモートメンテナンス実施プログラムの構成採用にある。

【００６７】

本発明プログラムの第５の特徴は、各ローカルネットワークにより任意数の内線端末とＩＰ接続してそれぞれのインターネットゲートウェイ端末の支配下とする一方、当該それぞ

れのインターネットゲートウェイ端末とインターネットを介してＶＰＮゲートウェイ間でＯＳＩ参照モデルのネットワーク層においてＶＰＮセッションを実現するＩＰｓｅｃを確立することで、当該ＶＰＮゲートウェイを含む保守センタからリモートメンテナンスを行うシステムにて、当該保守センタにて用いられるプログラムであって、新たに設置された前記インターネットゲートウェイ端末からの設置通知コマンドを処理する設定通知コマンド処理を前記保守センタに行わせる前記プログラムの実行により、前記設置通知コマンドに応じて、前記リモートメンテナンスのための共通情報であるＩＰｓｅｃの認証鍵を生成して、当該設置通知コマンドを通知してきた前記インターネットゲートウェイ端末にレスポンスする、以上の一連の手順を踏んでなるリモートメンテナンス実施プログラムの構成採用にある。

【００６８】

本発明プログラムの第６の特徴は、各ローカルネットワークにより任意数の内線端末とＩＰ接続してそれぞれのインターネットゲートウェイ端末の支配下とする一方、当該それぞれのインターネットゲートウェイ端末とインターネットを介してＶＰＮゲートウェイ間でＯＳＩ参照モデルのネットワーク層においてＶＰＮセッションを実現するＩＰｓｅｃを確立することで、当該ＶＰＮゲートウェイを含む単一の保守センタからリモートメンテナンスを行うシステムにおいて、当該保守センタにて用いられるプログラムであって、前記保守センタにおける終了ボタンが押されたことを契機に、前記リモートメンテナンスの作業が終了したことを通知するリモートメンテナンス終了処理を、前記保守サーバに行わせる前記プログラムの実行により、ＶＰＮＮＡＴ用ローカルＩＰアドレスで確立されたＶＰＮトンネルを経由して、当該ＶＰＮトンネルを確立させた前記インターネットゲートウェイ端末のサーバ部に対して、リモートメンテナンス終了コマンドを送信した後に、当該リモートメンテナンス終了のレスポンスを受信すると、該当内線端末に対するメンテナンスが全て終了したかのを第１判断を行い、当該第１判断にて肯定の場合には当該終了した前記内線端末は前記インターネットゲートウェイ端末の前記サーバ部かルータ部かの何れかであるかの第２判断を行う一方、否定の場合にはこのプログラムを終了し、当該第２判断にて否定の場合にはＶＰＮＮＡＴ解放処理へ移行する一方、肯定の場合には対応する前記インターネットゲートウェイ端末に対するリモートメンテナンスを全て終了したかの第３判断を行い、当該第３判断にて肯定の場合にはＶＰＮ終了処理へ移行する一方、否定の場合にはこのプログラムを終了する、以上の一連の手順を踏んでなるリモートメンテナンス実施プログラムの構成採用にある。

【００６９】

本発明プログラムの第７の特徴は、上記本発明プログラムの第６の特徴における前記ＶＰＮＮＡＴ解放処理が、リモートメンテナンス要求を受けて設定したリモートメンテナンス対象の内線端末名に対するＶＰＮＮＡＴ用ローカルＩＰアドレスを、確立した前記ＶＰＮトンネルへのＶＰＮ処理対象パケットから解除する様、前記ＶＰＮゲートウェイに対して行い、前記インターネットゲートウェイ端末に対して、リモートメンテナンス対象の内線端末名を通知し、その後、前記第３判断にリターンする一連の処理であり、前記ＶＰＮ終了処理が、ＩＰｓｅｃセッションの終了をＶＰＮ終了コマンドとして、前記インターネットゲートウェイ端末に対して送信して、前記ＶＰＮゲートウェイに、リモートメンテナンス実施要求の際に設定した前記ＶＰＮトンネルの解除させ、当該ＶＰＮゲートウェイと当該インターネットゲートウェイ端末間で確立されているＶＰＮトンネル処理を終了させる一連の処理であるリモートメンテナンス実施プログラムの構成採用にある。

【００７２】

本発明記録媒体の第１の特徴は、上記本発明プログラムの第１、第２、第３、第４、第５、第６又は第７の特徴における前記プログラムによる一連の手続を実録してなるリモートメンテナンス実施プログラムを記録した記録媒体の構成採用にある。

【００７４】

【発明の実施の形態】

以下、添付図面を参照して、本発明の実施の形態をそのシステム例、方法例、記録媒体例

及びプログラム例について詳細を説明する。

【００７５】

（システム例）

図１に本発明の一実施形態であるリモートメンテナンス実施システム例の構成図を示す。リモートメンテナンスシステムは、インターネットゲートウェイ端末１（以下、情流ＧＷ端末）、内線端末２ａ～２ｎ（ｎは任意の自然数を表す）、保守サーバ３、リモートメンテナンス装置４、ＶＰＮゲートウェイ５（５ａ～５ｎ）の５つのノードからシステム構築される。

【００７６】

前記情流ＧＷ端末１は、通常インターネット６（ＷＡＮ）側とローカルネットワークである内線（ＬＡＮ）７側のいずれともＴＣＰ／ＩＰで通信することを前提とする。また、保守サーバ３側のＬＡＮ８上のＶＰＮゲートウェイ５（５ａ～５ｎ）とＶＰＮを構築できる機能を持つことが必要がある。

【００７７】

従来のルータｆやアプリケーションゲートウェイと呼ばれる物が対象となる。従来のＩＳＤＮターミナルアダプタのように、それ自体ではＴＣＰ／ＩＰの通信を行わない物は対象としない。

以下の記述において、単に「端末」の呼称は、情流ＧＷ端末１を指す。

【００７８】

前記内線端末２ａ～２ｎは、前記情流ＧＷ端末１配下の内線ＬＡＮ７に接続するＰＣ（パソコン）等の端末（群）である。内線ＬＡＮ７に接続されている情流ＧＷ端末１本体に含まれるサーバ部１０やルータ部１１も内線端末２ａ～２ｎとして扱う。

前記保守センタ９は、保守サーバ３、リモートメンテナンス装置４、ＶＰＮゲートウェイ５（５ａ～５ｎ）を構成要素とするリモート保守を行うセンタの総称である。

【００７９】

前記保守サーバ３は、情流ＧＷ端末１や内線端末２ａ～２ｎのリモートメンテナンスに関する情報を管理するインターネット６上のサーバで、インターネット６側とリモートメンテナンス装置４が存在するＬＡＮ８側に各々ＬＡＮインターフェースを持つ。

【００８０】

前記リモートメンテナンス装置４は、情流ＧＷ端末１や内線端末２ａ～２ｎのリモートメンテナンスを行うオペレーティング装置で、ＷＥＢブラウザ機能を持つことが前提である。

前記ＶＰＮゲートウェイ５ａ～５ｎは、インターネット６経由で、情流ＧＷ端末１と保守センタ９を結ぶＶＰＮを構築するためのＶＰＮゲートウェイ装置である。

【００８１】

前記情流ＧＷ端末１は、ｈｔｔｐサーバ処理を行うｈｔｔｐサーバ部１００と、ｈｔｔｐサーバから呼ばれて内部処理を行うＣＧＩ処理部１０１と、ルータ部１１への制御コマンドを発行するルータ設定処理部１０２と、保守サーバ３にコマンドを送信するコマンド送出処理部１０３を含むサーバ部１０と、ＩＰｓｅｃを含んだＩＰルータ処理を制御するルータ部１１から構成される。

【００８２】

前記保守サーバ３は、端末１からのｈｔｔｐコマンドを受信するｈｔｔｐサーバ部３０と、ｈｔｔｐサーバ部３０から呼ばれて内部処理を行うＣＧＩ処理部３１と、ＶＰＮゲートウェイ１へｔｅｌｎｅｔコマンドを発行するＶＰＮゲートウェイ設定処理部３２から構成される。

前記ＶＰＮゲートウェイ５ａ～５ｎは、端末１のルータ部１１とＶＰＮセッションを行うＶＰＮ処理部５０と、保守サーバ３からのｔｅｌｎｅｔコマンドを受信する設定コマンド受信処理部５１から構成される。

【００８３】

前記リモートメンテナンス装置４は、端末１のサーバ部１０へｈｔｔｐプロトコル等でコ

マンドを送出するメンテナンスコマンド処理部４０から構成される。以上、示した、保守サーバ３と、ＶＰＮゲートウェイ５ａ～５ｎと、リモートメンテナンス装置４を使って、保守センタ９からインターネット６のＶＰＮトンネル１２経由で、複数の情流ＧＷ端末１及びその内線端末２ａ～２ｎをリモートメンテナンスする際、情流ＧＷ端末１配下のローカルネットワークアドレスが如何なる場合でも、同時にＶＰＮリモートメンテナンスを実現する。

【００８４】

（方法例）

前記システム例に適用する本方法例におけるＶＰＮリモートメンテナンスは、設置通知処理と、ＶＰＮＧＷアドレス要求と、リモートメンテナンス要求処理と、リモートメンテナンス終了処理と、ＶＰＮＮＡＴ解放処理と、ＶＰＮ終了処理と、故障通知処理との７つの「通知コマンド及びレスポンス」と、実際に保守センタ９のオペレータが行う「リモートメンテナンス実施」（本リモートメンテナンスプロトコルにおいては、実際のメンテナンス作業のプロトコルについては、特に規定しない。それは、ＴＣＰ／ＩＰを利用していれば、汎用のアプリケーションであってもよいし、独自のプロトコルでもよい。）を通信プロトコルとして構成される。

【００８５】

ここで、リモートメンテナンス実施以外の７つの通信プロトコルは実際のメンテナンス作業（以下、リモートメンテナンス実施）を行うための、手法にすぎず、あくまでも主旨は、以下の通りである。

【００８６】

すなわち、第一の主旨は、リモートメンテナンス装置４からメンテナンス対象内線端末２ａ～２ｎに対して、ＶＰＮのトンネル１２を利用してＴＣＰ／ＩＰプロトコルを利用するアプリケーションで行い、このとき、保守センタ９のリモートメンテナンス装置４から、メンテナンス対象内線端末２ａ～２ｎへのＩＰ接続をＶＰＮＮＡＴ用ローカルＩＰアドレスを用いて、ルータ部１１内に機能構成する後記ＶＰＮＮＡＴ１１０で行うことにより、先に述べた複数の情流ＧＷ端末１へのアクセスをその配下のＩＰアドレスが重複している場合でも確実に実施することにある。ただし、当該ＮＡＴを経由すると実施不可能なアプリケーションは実施できないのは、制限事項である。

【００８７】

また、第２の主旨は、リモートメンテナンス装置４からメンテナンス対象内線端末２ａ～２ｎに対して、ＶＰＮのトンネル１２を利用してＴＣＰ／ＩＰプロトコルを利用するアプリケーションで行い、このとき、保守センタ９のＶＰＮゲートウェイ５ａ～５ｎが増設などによりアドレスが変更された場合でも、リモートメンテナンス装置４から任意のＶＰＮゲートウェイ５ａ～５ｎ及びインターネットゲートウェイを介して、メンテナンス対象内線端末へのＩＰ接続が確実に実行されることにある。

【００８８】

以下、前記第一の主旨を達成するための、本方法例を以下図面を参照して説明する。

当該本方法例はルータ部１１内に機能構成するＶＰＮＮＡＴ１１０に動的にＶＰＮＮＡＴ用ローカルＩＰアドレスを付与することにある。

図２をもとにＶＰＮＮＡＴ１１０に動的にＶＰＮＮＡＴ用ローカルＩＰアドレスを付与する機能の概略を説明する。

【００８９】

まず、▲１▼で保守センタ９にリモートメンテナンス対象端末の内線端末２ａ～２ｎ名を通知する。▲２▼で、保守センタ９は、情流ＧＷ端末１に対して、情流ＧＷ端末１のサーバ部１０経由でリモートメンテナンス対象内線端末２ａ～２ｎ名に対応するＶＰＮアクセス用のＶＰＮＮＡＴ用ローカルＩＰアドレス（10.0.0.1）を付与する。これは、基本的にリモートメンテナンス要求の時点で行われる。

【００９０】

次に▲３▼で、ＶＰＮＮＡＴ用ローカルＩＰアドレスとリモートメンテナンス対象内線端

末２ａ～２ｎのＩＰアドレスを静的ＮＡＴ１１０で割り付ける。これも、▲２▼に引き続きリモートメンテナンス要求時に行われる。
次に▲４▼でリモートメンテナンス実施時にＶＰＮトンネル１２の中を通してＶＰＮＮＡＴ用ローカルＩＰアドレスへアクセスする。そうすると、▲５▼に示すように、リモートメンテナンス対象内線端末２ａ～２ｎへパケットが転送されアクセス可能になる。

【００９１】
このように事前に静的にＶＰＮＮＡＴ用ローカルＩＰアドレスを割り付けなくても動的にＶＰＮＮＡＴ用ローカルＩＰアドレスを付与することにより、複数の情流ＧＷ端末１へのアクセスをその配下のＩＰアドレスが重複している場合でも同時に実施とすることができるようになる。

【００９２】
以下、第２の主旨を達成する方法例として、ＶＰＮ構築に先立ち、保守センタ９がその配下の複数のＶＰＮゲートウェイ５ａ～５ｎからＶＰＮの空のリソースのあるＶＰＮゲートウェイ５ｉを動的に選択し、情流ＧＷ端末のルータ部１１に通知することにより、ルータ部１１内に設置されるＶＰＮゲートウェイのグローバルＩＰアドレスを動的にＶＰＮの対向ホストとして設定付与することにある。

【００９３】
以下、本方法例を実現するための６つのプロトコルについて概要を説明する。
前記設置通知処理は、情流ＧＷ端末１が設置されたことを保守サーバ３に通知し、保守サーバ３からリモートメンテナンスのための共有情報（ＩＰｓｅｃのPreshared Key、端末認証パスワード（以下、Secret（ID2))等）を暗号化して受け取ることが主旨である。

【００９４】
また、前記主旨を実現するために、設置通知処理内でも、情流ＧＷ端末１のサーバ部１０とルータ部１１に対してＶＰＮＮＡＴ１１０を構築するのも本方法例においては大きな目的である。

【００９５】
前記ＶＰＮＧＷアドレス要求処理は、保守サーバ３が保守センタ９配下の複数のＶＰＮゲートウェイ５ａ～５ｎからＶＰＮの空きのリソースのあるＶＰＮゲートウェイ５ｉを動的に選択して、そのＶＰＮゲートウェイ５ｉのグローバルＩＰアドレスをＶＰＮゲートウェイ通知レスポンスとして情流ＧＷ端末１に通知し、情流ＧＷ端末ルータ部１１は通知されたＶＰＮゲートウェイ５ｉのグローバルＩＰアドレスをＶＰＮの対向ホストとして設定を行うことも本方法においては大きな主旨である。

【００９６】
前記リモートメンテナンス要求処理は、ＩＰｓｅｃによるリモートメンテナンスの実施を保守サーバ３に要求することを主旨とする。リモートメンテナンス要求処理に対応するメンテナンス対象端末は、情流ＧＷ端末１本体、及び、内線端末２ａ～２ｎとする。また、主旨を実現するために、リモートメンテナンス要求処理内でも、情流ＧＷ端末１のサーバ部１０とルータ部１１以外の内線端末２ａ～２ｎに対してＶＰＮＮＡＴ１１０を構築するのも本方法例においては大きな主旨である。

【００９７】
前記リモートメンテナンス終了処理は、リモートメンテナンス装置４を使って実際にリモートメンテナンスが終了したことを対象となる情流ＧＷ端末１に伝えることを主旨とする。

【００９８】
前記ＶＰＮＮＡＴ１１０解放処理は、リモートメンテナンスが終了した情流ＧＷ端末１のサーバ部１０とルータ部１１以外の内線端末２ａ～２ｎについてＶＰＮＮＡＴ１１０を解放することを目的とする。これにより、後の効果に述べるように、ＶＰＮＮＡＴ用ローカルＩＰアドレス資源を有効活用可能となる。
ＶＰＮ終了処理は、ＩＰｓｅｃセッションを終了することを主旨とする。

【００９９】

（プログラム例、記録媒体例）
本方法例を実施するためのプログラム例及び記録媒体例を図面につき説明する。
リモートメンテナンスの全体処理フロー図３～図９を用いて、各通信データの流れを示す。各図の“→”は、設置通知処理、ＶＰＮＧＷアドレス要求処理、リモートメンテンナンス要求処理、リモートメンテナンス終了処理、ＶＰＮＮＡＴ解放処理、ＶＰＮ終了処理、故障通知処理の際の通信シーケンスにおけるコマンド送出及び受信を示した手順及び手続の流れである。
【０１００】
処理形態は、情流ＧＷ端末１設置時に一度だけ、情流ＧＷ端末１設置者の操作を契機として、図３に示す設置通知処理の▲１▼設置通知コマンド（端末ＩＤ、公開鍵、原文、ＭＡＣ）→▲２▼設置通知レスポンス（暗号化Preshared Key、暗号化Secret ID2、暗号化保守者パスワード、暗号化サーバ部用ＶＰＮＮＡＴ用ローカルＩＰアドレス、暗号化ルータ部用ＶＰＮＮＡＴ用ローカルＩＰアドレス、暗号化ルータ部用ＶＰＮＮＡＴ用ローカルＩＰアドレス）→▲３▼ルータ設定（ＶＰＮＮＡＴ１１０、暗号化Preshared Key）が行われる。
【０１０１】
その後、内線端末２ａ～２ｎユーザ（以下、ユーザ）が情流ＧＷ端末１から保守センタ９（以下、センタ）に対して、内線端末２ａ～２ｎのリモートメンテナンスの要求をすると思い立った度毎に、内線端末ユーザの操作を契機として、図４に示すＶＰＮＧＷアドレス要求の▲１▼ＶＰＮＧＷアドレス要求コマンド（端末ＩＤ、公開鍵、原文、ＭＡＣ）→▲２▼ＶＰＮＧＷ選択処理→▲３▼ＶＰＮＧＷアドレス要求レスポンス（ＶＰＮゲートウェイグローバルＩＰアドレス）→▲４▼ルータ設定（ＶＰＮゲートウェイグローバルＩＰアドレス）が行われる。
【０１０２】
次に、ＶＰＮＧＷアドレス要求の処理終了を契機として、図５に示すリモートメンテナンス要求の▲１▼リモートメンテナンス要求コマンド（端末ＩＤ、内線端末２ａ～２ｎ名、情流ＧＷ端末グローバルアドレス、要求者レベル、緊急度、要求者名、電話番号、要求内容）→▲２▼ＶＰＮＮＡＴ用ローカルＩＰアドレス割り当て処理→▲３▼ＶＰＮＮＡＴ用ローカルＩＰアドレス向けルーティング設定→▲４▼ＩＰｓｅｃ設定処理→▲５▼リモートメンテナンス要求レスポンス（内線端末２ａ～２ｎ名、ＶＰＮＮＡＴ用ローカルＩＰアドレス、受付番号）→▲６▼ＶＰＮＮＡＴ用ローカルＩＰアドレスのＶＰＮＮＡＴ１１０設定が行われる。
【０１０３】
センタ９では、オペレータがリモートメンテナンス装置４からリモートメンテナンス要求の受信を随時確認している。
オペレータが、各々のリモートメンテナンス要求処理に対するリモートメンテナンスを実施すると思い立った度毎に、オペレータの操作により、図６に示す▲１▼リモートメンテナンス実施が行われる。
【０１０４】
センタ９では、各々のリモートメンテナンス要求処理に対するリモートメンテナンスが終了した度毎に、オペレータの操作により、図７に示すリモートメンテナンス終了処理の▲１▼リモートメンテナンス終了コマンド（受付番号）→▲２▼リモートメンテナンス終了レスポンスが行われる。
【０１０５】
リモートメンテナンス終了処理後、保守サーバ３の判断により、必要に応じて、自動的に、図８に示すＶＰＮＮＡＴ解放処理の▲１▼ＶＰＮＮＡＴ１１０解放コマンド（内線端末２ａ～２ｎ名）→▲２▼ＶＰＮＮＡＴ用ローカルＩＰアドレスＶＰＮＮＡＴ設定解除→▲３▼ＶＰＮＮＡＴ１１０解放レスポンス→▲４▼ＶＰＮＮＡＴ用ローカルＩＰアドレス変換処理→▲５▼ＶＰＮＮＡＴ用ローカルＩＰアドレスルーティング設定解除が行われる。
【０１０６】

ＶＰＮＮＡＴ１１０解放終了後、保守サーバ３の判断により、必要に応じて、自動的に図９に示すＶＰＮ終了の▲１▼ＶＰＮ終了コマンド→▲２▼ＶＰＮＮＡＴ用ローカルＩＰアドレス初期化設定→▲３▼ＶＰＮ終了レスポンス→▲４▼ＶＰＮＮＡＴ用ローカルＩＰアドレス向けルーティング初期化→▲５▼ＩＰｓｅｃ設定解除が行われる。

【０１０７】

以上が、全体フローの概略である。なお、情流ＧＷ端末１台に着目した場合の情流ＧＷ端末１及び保守センタ９の処理フローを図１０、図１１のフローチャートに示す。

【０１０８】

即ち、図１０に示す情流ＧＷ端末１側フローチャートについては、設置通知ＳＴｃはＳＴａ→ＳＴｂを順次踏んで実践され、リモートメンテナンス終了処理ＳＴｈは設置通知ＳＴｃからＳＴｄ→ＳＴｅを踏んで、ＶＰＮＮＡＴ解放処理ＳＴｉは設置通知ＳＴｃからＳＴｄ→ＳＴｅ→ＳＴｆを踏んで、ＶＰＮ終了処理ＳＴｊは設置通知ＳＴｃからＳＴｄ→ＳＴｅ→ＳＴｆ→ＳＴｇを踏んで、故障通知ＳＴｎは設置通知ＳＴｃからＳＴｄ→ＳＴｋ→ＳＴｌを踏んで、ＶＰＮＧＷアドレス要求ＳＴｏは設置通知ＳＴｃからＳＴｄ→ＳＴｋを踏むか故障通知ＳＴｎから直結して踏んで、リモートメンテナンス要求ＳＴｍは設置通知ＳＴｃからＳＴｄ→ＳＴｋ→ＳＴｏを踏むかＳＴｄ→ＳＴｋ→ＳＴｌ→ＳＴｎ→ＳＴｏを踏んで、それぞれ実践され、その間必要に応じて繰り返しが入る。

【０１０９】

図１１に示すセンタ９側フローチャート（情流ＧＷＩＤ＝Ｎ）については、設置通知処理ＳＴ６はＳＴ１→ＳＴ２→ＳＴ３を、ＶＰＮＧＷアドレス要求処理ＳＴ１６はＳＴ１→ＳＴ２→ＳＴ３→ＳＴ１５を、リモートメンテナンス要求処理ＳＴ７はＳＴ１→ＳＴ２→ＳＴ３→ＳＴ１５→ＳＴ４を、故障通知処理ＳＴ８はＳＴ１→ＳＴ２→ＳＴ３→ＳＴ１５→ＳＴ４→ＳＴ５を、それぞれ順次踏んで実践される。

【０１１０】

リモートメンテナンス終了ＳＴ９はＳＴ１→ＳＴ２を踏んで、ＶＰＮＮＡＴ解放ＳＴ１２はリモートメンテナンス終了ＳＴ９からＳＴ１０→ＳＴ１１を踏んで、ＶＰＮ終了ＳＴ１４はＶＰＮＮＡＴ解放ＳＴ１２からＳＴ１３を踏んで、それぞれ実践され、その間必要に応じて繰り返しが入る。

なお、図２６に示す故障通知は、故障発生時に通知されるが、全体の流れとは独立な処理なのでここでは詳細にはふれない。

【０１１１】

［リモートメンテナンス実施のための前提条件］

なお、本実施形態例を実行するためには、以下の前提条件が必要である。

（１）保守サーバ３と端末１では、共有稼密情報（以下、Secret（ID))を事前に共有していること。Secret（ID）は、出荷時に端末１にＲＯＭ等に埋め込み、保守サーバ３と共有することで対応する。なおSecret（ID）は、保守サーバ３がリモートメンテを行うすべての端末１に共通とする。

【０１１２】

（２）端末１のルータ部１１は、ＩＰｓｅｃ等のＩＰレベルのＶＰＮ機能を持つこと。また、ＶＰＮセッションについて、セッション待ち受け側の設定を事前に行っておくこと（ＩＰｓｅｃの場合は、レスポンダとして設定しておくこと）。また、Preshared keyはダミーデータを設定しておくこと。

（３）保守センタ９のＶＰＮゲートウェイ５は、ＶＰＮセッションについて、セッション確立側の設定を事前に行っておくこと（ＩＰｓｅｃの場合は、イニシエータとして設定しておくこと）。

【０１１３】

（４）ＶＰＮゲートウェイ５は、端末１のルータ部１１と通信互換性のあるＶＰＮ機能を持つこと。

（５）端末１のルータ部１１は、保守サーバ３の公開されたグローバルＩＰアドレス（または、インターネットホスト名）を設置通知の時点までに事前に知っていること。また、

インターネット６へ接続設定が完了していること。
【０１１４】
（６）ルータ設定処理部１０２からルータ部１１への各種設定はリモートコンソール（以下、ｔｅｌｎｅｔ）、またはプロセス間通信（ソケット通信等）で行えること。
（７）保守サーバ３のＶＰＮゲートウェイ設定処理部３２からＶＰＮゲートウェイ５の設定コマンド受信処理部５１への各種設定はｔｅｌｎｅｔまたはプロセス間通信（ソケット通信等）で行えること。
【０１１５】
（８）保守サーバ３上には、ＶＰＮＮＡＴ１１０ＤＢを持つ。テーブルは、ＶＰＮＮＡＴ用ローカルＩＰアドレスをキーとした複数レコードから構成され、フィールドとして、割り当て情流ＧＷ端末ＩＤ／端末名を持つ。
（９）情流ＧＷ端末１には、ホストテーブルを持つ。テーブルは、内線端末２ａ～２ｎ名をキーとした複数レコードから構成され、フィールドとして、実ＩＰアドレス、ＶＰＮＮＡＴ用ローカルＩＰアドレスを持つ。初期状態では、ホストテーブルは空である。
【０１１６】
（１０）保守サーバ３上のＶＰＮＧＷ５（５ａ～５ｎ）は複数の存在を可能とする。一つのＶＰＮＧＷ５はそのＶＰＮＧＷ５が許容する複数個のＶＰＮトンネル１２を構成可能とする。
（１１）保守サーバ３上にはＶＰＮＧＷトンネルテーブルを持つ。テーブルは、ＶＰＮゲートウェイ５のＩＰアドレス及びＶＰＮトンネル番号をキーとした複数のレコードから構成され、フィールドの値として、割り当て情流ＧＷＩＤを持つ。
【０１１７】
［処理シーケンスの説明］
以下、図３～図９と、図１２～図２５を用いて、各処理の手順について詳細を説明する。書中左に振っている番号ｎ－ｎ（ｎは任意の自然数）は、図中のステップ処理番号に対応する。
【０１１８】
＜設置通知処理＞
図３、図１２及び図１３に示すよう設置通知は、端末１が設置されたことを保守サーバ３に通知し、保守サーバ３からリモートメンテナンスのための共有情報（ＩＰｓｅｃのPres hared Key、端末１認証パスワード（以下、Secret（ID2))、保守者パスワード）を暗号化して受け取り、それを設定することが目的である。
【０１１９】
設置通知処理以降の端末認証処理にSecret（ID）の代わりに、Secret（ID2）を使うのは、端末１全てに共通であるSecret（ID）よりも、Secret（ID2）を使った方がセキューリティが強化されるためである。
また、ＶＰＮを構築する際、各情流ＧＷ端末１配下のプライベートＩＰアドレスの重複が考えられるため、それを避けるために、ＶＰＮＮＡＴ処理を行う。そのための、ＶＰＮ用ダミープライベートＩＰアドレス（以下、ＶＰＮＮＡＴ用ローカルＩＰアドレス）を保守サーバ３から受け取ることが第２の目的である。
【０１２０】
▲１▼設置通知コマンド（端末サーバ部１０→保守センタ９）
((通信契機))
１－１　端末１設置終了後、ルータ部１１がインターネット６への接続設定が完了した時点で、サーバ部１０に対するボタン操作により行う。設置通知は一度だけ行えばよい。
【０１２１】
((端末前処理))
１－２　サーバ部１０のコマンド送出処理部１０３は、秘密鍵と公開鍵を生成する。アルゴリズムにはＲＳＡ等の公開鍵暗号を使用する。
１－３　「端末１のユニークなＩＤ＋タイムスタンプ」から認証のための原文を作成する

。
１－４　原文に対して、Secret（ID）を用いたメッセージ認証子（ＭＡＣ）を生成する（ISO9797－1、ISO9797－2に準拠することが望ましい）。
【０１２２】
((コマンド送信処理))
１－５　端末ＩＤ、公開鍵、原文、ＭＡＣをパラメータとして、端末１（サーバ部１０／コマンド送出処理部１０３）から保守サーバ３（ｈｔｔｐサーバ部３０）へのｈｔｔｐコマンドで＜非ＩＰｓｅｃセッション＞として設置通知コマンドを送信する。
【０１２３】
▲２▼設置通知レスポンス（保守サーバ３→端末サーバ部１０）
((保守サーバ処理))
１－６　保守サーバ３のｈｔｔｐサーバ部３０は、受信したコマンド名とパラメータをＣＧＩ処理部３１に渡し、ＣＧＩ処理部３１は、原文に対して、Secret（ID）を用いたメッセージ認証子（ＭＡＣ）を生成して（端末１と同様の演算）、受信したＭＡＣと一致することを確認する（端末認証）。
【０１２４】
１－７　ＣＧＩ処理部３１は、ＩＰｓｅｃの認証鍵（Preshared Key）、Secret（ID2）をランダムに生成し、保守者パスワードを設定ファイルから取得し、端末１ＤＢの中の端末ＩＤに対応するレコードを新規にクリエイトし（既に存在する場合は上書き）、該当レコードの各フィールドに保持する。
【０１２５】
１－８　ＣＧＩ処理部３１は、ＶＰＮＮＡＴＤＢ９１から空きＶＰＮＮＡＴ用ローカルＩＰアドレスをサーバ部１０用とルータ部１１用に二つ選択し、該当レコードの割り当て状況フィールドに情流ＧＷ端末ＩＤ／端末名を保持するとともに、端末１ＤＢのサーバ部１０ＶＰＮＮＡＴ用ローカルＩＰアドレス及びルータ部１１ＶＰＮＮＡＴ用ローカルＩＰアドレスフィールドにＶＰＮＮＡＴ用ローカルＩＰアドレスを保持する。
【０１２６】
１－９　ＣＧＩ処理部３１は、ＩＰｓｅｃの認証鍵（Preshared Key）、Secret（ID2）、保守者パスワード、サーバ部１０及びルータ部１１用ＶＰＮＮＡＴ用ローカルＩＰアドレスを、情流ＧＷ端末１の公開鍵で暗号化する。
【０１２７】
((レスポンス送信処理))
１－１０　保守サーバ３のｈｔｔｐサーバ部３０は、ステータス（正常またはエラーステータス（認証異常等））、端末１の公開鍵で暗号化したＩＰｓｅｃの認証鍵（Preshared Key）、端末１の公開鍵で暗号化したSecret（ID2）、端末１の公開鍵で暗号化した保守者パスワード、端末１の公開鍵で暗号化したサーバ部用ＶＰＮＮＡＴ用ローカルＩＰアドレス、端末１の公開鍵で暗号化したルータ部用ＶＰＮＮＡＴ用ローカルＩＰアドレスをパラメータとしたデータをＣＧＩ処理部３１から受けて、保守サーバ３（ｈｔｔｐサーバ部３０）から端末１（サーバ部１０／コマンド送出処理部１０３）へのｈｔｔｐレスポンス＜非ＩＰｓｅｃセッション＞としてレスポンスを送信する。
【０１２８】
▲３▼サーバ部１０とルータ部１１のＶＰＮＮＡＴ１１０設定（端末サーバ部１０→端末ルータ部１１）
((端末後処理))
１－１１　端末サーバ部１０は、端末１の秘密鍵で、ＩＰｓｅｃの認証鍵（Preshared Key）、Secret（ID2）、保守者用パスワード、サーバ部用ＶＰＮＮＡＴ用ローカルＩＰアドレス、ルータ部用ＶＰＮＮＡＴ用ローカルＩＰアドレスを復号化し、保持する。
【０１２９】
１－１２　端末サーバ部１０は、ＶＰＮゲートウェイ５をＩＰｓｅｃ対象ホストとしたPreshared Key、サーバ部用ＶＰＮＮＡＴ用ローカルＩＰアドレス、ルータ部用ＶＰＮＮＡ

Ｔ用ローカルＩＰアドレスの設定コマンド（ルータ部１１のｔｅｌｎｅｔコマンドの実装により異なる）を作成する。この時、ＶＰＮゲートウェイのアドレスはダミーで設定する。

【０１３０】

((コマンド送信処理))

１－１３　前の処理で作成したコマンドをパラメータとして、端末（ルータ設定処理部１０２）から端末１（ルータ部１１）へのｔｅｌｎｅｔコマンド＜ローカルネットワークセッション＞として、コマンドを送出する。

((端末ルータ部処理))

１－１４　受信したPreshared Keyの設定及びＶＰＮＮＡＴ１１０の設定をルータ部１１に書き込む。

【０１３１】

((レスポンス送信処理))

１－１５　ステータス（正常またはエラーステータス（コマンド異常等))をパラメータとして、端末１（ルータ部１１）から端末１（サーバ部１０／コマンド送出処理部１０３）へのｔｅｌｎｅｔレスポンス＜非ＩＰｓｅｃセッション＞としてレスポンスを送信する。

((端末ルータ設定部後処理))

なし

上記で設置通知処理が完了となる。

【０１３２】

＜故障通知処理＞

図２６のシーケンス図と図２７の処理フローの手順図を示すよう、故障通知処理は、端末１が故障したことを検知し、保守サーバ３に通知する。端末１（サーバ部１０）では、端末１のサーバ部１０及びルータ部１１の故障の発生、復旧を常時監視して、故障が発生したら故障通知処理を起動する。

即ち、故障通知処理の▲１▼故障通知コマンド（端末ＩＤ、原文、ＭＡＣ、故障コード）→▲２▼故障通知レスポンス→▲３▼リモートメンテナンス要求起動が行われる。

【０１３３】

((通信契機))

７－１　端末１で故障発生を検知した場合、端末１が自律的に行う。

((端末前処理))

７－２　「端末１のユニークなＩＤ＋タイムスタンプ」から認証のための原文を作成する。

７－３　原文に対して、Secret（ID2）を用いたメッセージ認証子（ＭＡＣ）を生成する（IS09797－1、IS09797－2に準拠することが望ましい）。

【０１３４】

((コマンド送信処理))

７－４　端末ＩＤ、原文、ＭＡＣ、故障のコードをパラメータとして、端末１（サーバ部１０／コマンド送出処理部１０３）から保守サーバ３（ｈｔｔｐサーバ部３０）へのｈｔｔｐコマンドで＜非ＩＰｓｅｃセッション＞として故障通知コマンドを送信する。

【０１３５】

((保守サーバ処理))

７－５　保守サーバ３のｈｔｔｐサーバ部３０は、受信したコマンド名とパラメータをＣＧＩ処理部３１に渡す。ＣＧＩ処理部３１は、原文に対して、Secret（ID2）を用いたメッセージ認証子（ＭＡＣ）を生成して（端末１と同様の演算）、受信したＭＡＣと一致することを確認する（端末認証）。

７－６　ＣＧＩ処理部３１は、受信した故障コードを保持する。

【０１３６】

((レスポンス送信処理))

７－７　保守サーバ３のｈｔｔｐサーバ部３０は、ステータス（正常またはエラーステー

タス（認証異常等))をパラメータとしたデータをＣＧＩ処理部３１から受けて、保守サーバ３（ｈｔｔｐサーバ部３１）から端末１（サーバ部１０／コマンド送出処理部１０３）へのｈｔｔｐレスポンス＜非ＩＰｓｅｃセッション＞としてレスポンスを送信する。

【０１３７】

((端末後処理))

７－８　ＶＰＮＧＷアドレス要求処理を起動する。

なお、故障通知処理によって保持した故障コードは、リモートメンテナンス装置４からｈｔｔｐアクセス等で参照できることが望ましい（故障確認処理）。

【０１３８】

＜ＶＰＮＧＷアドレス要求処理＞

図４のシーケンス図及び図１４、図１５の処理フロー手順のように、ＶＰＮＧＷアドレス要求は、保守サーバ３が選択した保守センタ９のＶＰＮゲートウェイ５ｉのアドレスを情流ＧＷ端末１に通知することを主旨とする。基本的には、内線端末２ａ～２ｎから情流ＧＷ端末１にリモートメンテナンス要求の登録があった時点で、ＶＰＮＧＷアドレス要求が通知されるものの、端末管理者が情流ＧＷ端末１本体のボタン操作でＶＰＮＧＷアドレス要求を通知することも可能とする。

【０１３９】

▲１▼ＶＰＮＧＷアドレス要求コマンド（端末サーバ部１０→保守サーバ３）

（通信契機）

９－１　内線端末２ａ～２ｎから情流ＧＷ端末１へのＷＥＢアクセス又は端末管理者のボタン操作などによる情流ＧＷ端末１へのアクションによる。

【０１４０】

（端末前処理）

９－２　内線端末２ａ～２ｎからのブラウザアクセスにより起動される場合は、リモートメンテナンス要求で必要な情報である「要求者名、要求者レベル、内線端末名（複数設定可）、緊急度、電話番号、要求内容」をブラウザから入力させることにより、取得し、リモートメンテナンス情報として保持する。画面イメージでは、ブラウザ画面の通りである。情流ＧＷ端末１のボタン操作により起動される場合は、「要求者名、要求者レベル、端末名、緊急度、電話番号、要求内容」を事前に登録されたテーブルから取得し、保持する。要求者レベルは、一般又は管理者を設定可能とする。尚、内線端末名は、リモートメンテナンス対象としたい内線端末の名称であり、他の情報は、保守センタ９のオペレータが、リモートメンテナンス要求を起動したユーザがセンタ９のオペレータにリモートメンテナンスを実施してもらうにあたり、その意向を示すための情報である。

【０１４１】

９－３　サーバ部１０のコマンド送出処理部１０３は、秘密鍵と公開鍵を生成する。アルゴリズムにはＲＳＡ等の公開鍵暗号を使用する。

９－４　「端末のユニークなＩＤ＋タイムスタンプ」から認証のための原文を生成する。

９－５　原文に対して、Ｓｅｃｒｅｔ（ｉｄ２）を用いたメッセージ認証子（ＭＡＣ）を生成する。（ＩＳＯ９７９７－１，ＩＳＯ９７９７－２）に準拠することが望ましい。）

【０１４２】

（コマンド送信処理）

９－６　端末ＩＤ，原文，ＭＡＣ，公開鍵をパラメータとして、端末１（サーバ部１０／コマンド送出処理部１０３）から保守サーバ３（ｈｔｔｐサーバ部３０）へのｈｔｔｐコマンドで＜非Ｉｐｓｅｃセッション＞としてリモートメンテナンス要求コマンドを送信する。

【０１４３】

▲２▼ＶＰＮＧＷ選択処理

（保守サーバ処理部）

９－７　保守サーバ３のｈｔｔｐサーバ部３０は、受信したコマンド名とパラメータをＣＧＩ処理部３１に渡す。ＣＧＩ処理部３１は、原文に対して、Ｓｅｃｒｅｔ（ｉｄ２）を

用いたメッセージ認証子（ＭＡＣ）を生成して（端末１と同様の演算）、受信したＭＡＣと一致することを確認する。（端末認証）

【０１４４】

９－８　保守サーバ３はＶＰＮＧＷトンネルＤＢを読み出し、ＶＰＮＧＷトンネルＤＢの割り当て状況のトンネルを先頭から検索し、フィールドの値が「未使用」のトンネル番号を取得する。また、当該取得したトンネル番号に対応するフィールドを「未使用」から「端末ＩＤ」に書き換え、対応するＶＰＮＧＷグローバルＩＰアドレスを取得する。以下、このグローバルＩＰアドレスに対応するＶＰＮＧＷを「５ｉ」とする。ここで示したＶＰＮゲートウェイ５ａ～５ｎの選択処理は、本発明の特徴の一つである。

【０１４５】

９－９　レスポンスのパラメータの前記「ＶＰＮＧＷグローバルＩＰアドレス」を受信した公開鍵で暗号化する。

【０１４６】

▲３▼ＶＰＮＧＷアドレス要求レスポンス（保守サーバ３→端末サーバ部１０）

（レスポンス送信処理）

９－１０　保守サーバ３のｈｔｔｐサーバ部３０は、ステータス（正常又はエラーステータス（認証異常等））、端末１の公開鍵で暗号化したＶＰＮＧＷグローバルＩＰアドレスをパラメータとしたデータをＣＧＩ処理部３１から受けて、保守サーバ３（ｈｔｔｐサーバ部３０）から端末１（サーバ部１０／コマンド送出処理部１０３）へのｈｔｔｐレスポンス＜非セッション＞としてレスポンスを送信する。

【０１４７】

▲４▼ＶＰＮＮＧアドレス要求レスポンス受信後処理（端末サーバ部１０→端末ルータ部１１）

（端末前処理）

９－１１　端末サーバ部１０は、端末１の秘密鍵で、ＶＰＮＧＷグローバルＩＰアドレスを復号化し、保持する。

【０１４８】

９－１２　端末サーバ部１０は、ＶＰＮＧＷグローバルＩＰアドレスをＶＰＮ対向ホストとして設定するためのコマンド（ルータ部１１のｔｅｌｎｅｔコマンドの実装により異なる。）を作成する。

９－１３　前の処理で作成したコマンドをパラメータとして、端末１（ルータ設定処理部１０２）から端末１（ルータ部１１）へのｔｅｌｎｅｔコマンド＜ローカルネットワークセッション＞として、コマンドを送出する。

【０１４９】

（端末ルータ部処理）

９－１４　ＶＰＮＧＷグローバルアドレスをＶＰＮ対向ホストとする設定をルータ部１１に書き込む。

（レスポンス送信処理）

９－１５　ステータス（正常又はエラーステータス（コマンド異常等））をパラメータとして、端末１（ルータ部１１）から端末１（サーバ部１０／コマンド送出処理部１０３）へのｔｅｌｎｅｔレスポンス＜非Ｉｐｓｅｃセッション＞としてレスポンスを送信する。

【０１５０】

（端末ルータ設定部後処理）

９－１６　リモートメンテナンス要求処理を起動する。

以上によりＶＰＮＧＷアドレス要求処理が完了となる。この本処理が発明のポイントの一つである。

【０１５１】

＜リモートメンテナンス要求処理＞

図５のシーケンス図と図１６乃至図１９の処理フローの手順図に示すよう、リモートメンテナンス要求処理は、ＩＰｓｅｃによるリモートメンテナンスの実施を保守サーバ３に要

求することを主旨とする。
【０１５２】
また、リモートメンテナンス要求処理では、ＶＰＮを構築するための情流ＧＷ端末１のＩＰアドレスをセンタ９に通知することも主旨の一つである。リモートメンテナンス要求は、ｈｔｔｐプロトコルで行われその環境変数から、保守サーバ３は、情流ＧＷ端末１に受信したＩＰアドレスを取得する。そのＩＰアドレスをもとに保守センタ９のＶＰＮゲートウェイ５ｉに対して、ＶＰＮ鍵、端末ＩＰアドレスを設定する。
【０１５３】
更に、ＶＰＮを構築する際、各情流ＧＷ端末１配下の内線端末２ａ～２ｎに対してＩＰレベルの通信を行えるようにするために、センタ９からリモートメンテナンス対象内線端末２ａ～２ｎに対するＶＰＮＮＡＴ用ローカルＩＰアドレスを取得し、ＶＰＮＮＡＴ処理を行う。
【０１５４】
ＶＰＮＮＡＴ処理を行うことにより、情流ＧＷ端末１配下のローカルＬＡＮアドレスが同一である複数の情流ＧＷ端末１へのメンテナンスを行う場合でも（例えば、メンテナンス対象の情流ＧＷ端末１が二つ存在し、二つの情流ＧＷ端末１が共に192.168.0.0/24のローカルネットを持つような場合）、保守センタ９のオペレータ端末から情流ＧＷ端末１及びその配下の内線端末２ａ～２ｎに対してＩＰリチャーブルな環境を構築できる。
【０１５５】
▲１▼リモートメンテナンス要求コマンド（端末サーバ部１０→保守サーバ３）
((通信契機))
２－１　ＶＰＮＧＷアドレス要求の処理終了後に、起動される。
【０１５６】
((端末前処理))
２－２　ＶＰＮＧＷアドレス要求で保持したリモートメンテナンス情報を取得する。
【０１５７】
２－３　サーバ部１０のコマンド送出処理部１０３は、秘密鍵と公開鍵を生成する。アルゴリズムにはＲＳＡ等の公開鍵暗号を使用する。
２－４　「端末１のユニークなＩＤ＋タイムスタンプ」から認証のための原文を作成する。
【０１５８】
２－５　原文に対して、Secret（ID2）を用いたメッセージ認証子（ＭＡＣ）を生成する（IS09797－1、IS09797－2に準拠することが望ましい）。
２－６　保守センタ９に通知するためのパラメータのうち、「要求者名、内線端末名、電話番号、要求内容」を情流ＧＷ端末１に保持されているSecret（ID2）で暗号化する。
【０１５９】
((コマンド送信処理))
２－７　端末ＩＤ、原文、ＭＡＣ、公開鍵、要求者レベル、緊急度、暗号化要求者名、暗号化内線端末名（複数可）、暗号化電話番号、暗号化要求内容をパラメータとして、端末１（サーバ部１０／コマンド送出処理部１０３）から保守サーバ３（ｈｔｔｐサーバ部３０）へのｈｔｔｐコマンドで＜非ＩＰｓｅｃセッション＞としてリモートメンテナンス要求コマンドを送信する。
【０１６０】
▲２▼ＶＰＮＮＡＴ用ローカルＩＰアドレス割り当て処理
((保守サーバ処理))
２－８　保守サーバ３のｈｔｔｐサーバ部３０は、受信したコマンド名とパラメータをＣＧＩ処理部３１に渡す。ＣＧＩ処理部３１は、原文に対して、Secret（ID2）を用いたメッセージ認証子（ＭＡＣ）を生成して（端末と同様の演算）、受信したＭＡＣと一致することを確認する（端末認証）。
【０１６１】

２－９　ＣＧＩ処理部３１は、受付番号を生成し、リモートメンテナンス要求ＤＢ９２のレコードを新規にクリエイトし、受付番号、受信時刻、メンテンナンス状態（この時点では、常に対応待ち）を保守端末ブラウザの端末ＤＢ９０に保持する。また、テーブル名には、要求者レベルが管理者の場合は、「管理者」として保持し、要求者レベルが一般の場合は、内線端末２ａ～２ｎ名を保持する。なお、端末ＤＢ９０のレコードを図２６に示す。

【０１６２】

２－１０　ＣＧＩ処理部３１は、環境変数REMOTE_ADDRから情流ＧＷ端末１のグローバルＩＰアドレスを取得し、前記リモートメンテナンス要求ＤＢ９２のレコードに保持する。

２－１１　ＣＧＩ処理部３１は、端末ＩＤ、要求者レベル、緊急度を前記リモートメンテナンス要求ＤＢ９２のレコードに保持する。

【０１６３】

２－１２　ＣＧＩ処理部３１は、暗号化内線端末名、暗号化要求者名、暗号化電話番号、暗号化要求内容をSecret（ID2）で復号化し前記リモートメンテナンス要求ＤＢ９２のレコードに保持する。なお、リモートメンテナンス要求ＤＢ９２のレコードを図２７に示す。

【０１６４】

２－１３　ＣＧＩ処理部３１は、通知された端末ＩＤ／内線端末名（複数端末名が存在する場合は、それぞれの端末名について）をキーとして、ＶＰＮＮＡＴＤＢ９１を検索し、その端末１にＶＰＮＮＡＴ用ローカルＩＰアドレスが割り当てられているかどうかを判断する。

【０１６５】

ＶＰＮＮＡＴ用ローカルＩＰアドレスが割り当てられていれば、割り当て済みのＶＰＮＮＡＴ用ローカルＩＰアドレスを前記リモートメンテナンス要求ＤＢ９２のレコードに保持し、ＶＰＮＮＡＴ用ローカルＩＰアドレスが割り当てられていなければ、ＶＰＮＮＡＴＤＢ９１から空きＶＰＮＮＡＴ用ローカルＩＰアドレスを選択する。

【０１６６】

該当レコードの割り当て状況フィールドに情流ＧＷ端末ＩＤ／内線端末名を保持するとともに、保持したＶＰＮＮＡＴ用ローカルＩＰアドレスを前記リモートメンテナンス要求ＤＢ９２のレコードにも保持する。

なお、ＶＰＮＮＡＴＤＢ９１のレコードを図３０に示す。

【０１６７】

２－１４　ＣＧＩ処理部３１は、リモートメンテナンス装置４のＷＥＢブラウザ上に、リモートメンテナンス要求を受信した旨を表示できるようにページを作成する。表示内容は、受付番号、端末ＩＤ、グローバルＩＰアドレス、要求者名、要求者レベル、電話番号、緊急度、要求内容、受信時刻、ＶＰＮＮＡＴ用ローカルＩＰアドレス、テーブル名、メンテナンス状態を表示する（図２９参照）。

【０１６８】

▲５▼リモートメンテナンス要求レスポンス処理（保守サーバ３→端末サーバ部１０）

（保守サーバ部）

２－２６　レスポンス処理の内、「内線端末名とダミーＩＰアドレスの組」を受信した公開鍵で暗号化する。

（レスポンス送信処理）

２－２７　保守サーバ３のｈｔｔｐサーバ部３０は、ステータス（正常又はエラーステータス（認証異常等））、受付番号、端末１の公開鍵で暗号化した内線端末名とＶＰＮＮＡＴ用ローカルＩＰアドレスの組（複数可）をパラメータとしたデータをＣＧＩ処理部３１から受けて、保守サーバ３（ｈｔｔｐサーバ部３０）から端末１（サーバ部１０／コマンド送出処理部１０３）へのｈｔｔｐレスポンス＜非Ｉｐｓｅｃセッション＞としてレスポンスを送信する。

【０１６９】

▲３▼ＩＰｓｅｃ処理対象パケット設定（保守センタ９→ＶＰＮゲートウェイ５ｉ）
（コマンド送信処理）
２－１５　ＶＰＮゲートウェイ設定処理部３２は、リモートメンテナンス要求ＤＢの該当レコードから、端末ＩＤおよび▲２▼の処理で保持したＶＰＮＮＡＴ用ローカルＩＰアドレス向けパケットを取得する。
２－１６　ＶＰＮゲートウェイ設定処理部３２は、ＶＰＮＮＡＴ用ローカルＩＰアドレス向けパケットを端末ＩＤに対応したＶＰＮトンネル１２に割り付けるための設定（ＶＰＮゲートウェイ５ｉのｔｅｌｎｅｔコマンドの実装により異なる。）をパラメータとして、保守サーバ３（ＶＰＮゲートウェイ設定処理部３２）からＶＰＮゲートウェイ５ｉ（設定コマンド受信処理部５１）へのｔｅｌｎｅｔコマンド＜ローカルネットワークセッション＞としてコマンドを送信する。

【０１７０】
（ＶＰＮゲートウェイ処理）
２－１７　受信したＶＰＮＮＡＴ用ローカルＩＰアドレスをＩＰｓｅｃ処理対象ホストとするための設定をＶＰＮゲートウェイ５ｉに書き込む。
（レスポンス送信処理）
２－１８　ステータス（正常又はエラーステータス（コマンド異常など））をパラメータとして、ＶＰＮゲートウェイ５ｉ（設定コマンド受信処理部５１）から保守サーバ３（ＶＰＮゲートウェイ設定処理部３２）へのｔｅｌｎｅｔレスポンス＜ローカルネットワークセッション＞としてレスポンスを送信する。

【０１７１】
（ＶＰＮゲートウェイ設定処理部後処理）
２－１９　ＶＰＮゲートウェイ設定処理部３２は、「▲１▼リモートメンテナンス要求コマンド」で受信した端末ＩＤを持つ情流ＧＷ端末１との間にＶＰＮが確立しているかをＶＰＮゲートウェイ５ｉから取得する。
２－２０　ＶＰＮゲートウェイ５ｉのＶＰＮ確立状況より、ＶＰＮが確立している場合は、プロセスを終了する。ＶＰＮが確立していない場合は、▲４▼ＩＰｓｅｃ設定処理を起動する。

【０１７２】
▲４▼ＩＰｓｅｃ設定処理（保守センタ９→ＶＰＮゲートウェイ５ｉ）
（ＶＰＮゲートウェイ設定処理部前処理）
２－２１　保守サーバ３／ＣＧＩ処理部３１からＩＰｓｅｃの認証鍵（ＰｒｅｓｈａｒｅｄＫｅｙ）、端末ルータ部１１のグローバルＩＰアドレスを取得し、コマンドを生成する。

【０１７３】
（コマンド送信処理）
２－２２　端末ルータ部１１のグローバルＩＰアドレスをＩＰｓｅｃ対象ホストとしたＰｒｅｓｈａｒｅｄｋｅｙの設定及び端末ＩＤに対応したＶＰＮトンネル１２を確立するための設定（ＶＰＮゲートウェイ５ｉのｔｅｌｎｅｔコマンドの実装により異なる。）をパラメータとして、保守サーバ３（ＶＰＮゲートウェイ設定処理部３２）からＶＰＮゲートウェイ５ｉ（設定コマンド受信処理部５１）へのｔｅｌｎｅｔコマンド＜ローカルネットワークセッション＞としてコマンドを送信する。

【０１７４】
（ＶＰＮゲートウェイ処理）
２－２３　受信したＰｒｅｓｈａｒｅｄｋｅｙ及びＶＰＮトンネル１２を確立するための設定をＶＰＮゲートウェイ５ｉに書き込む。
（レスポンス送信処理）
２－２４　ステータス（正常又はエラーステータス（コマンド異常など））をパラメータとして、ＶＰＮゲートウェイ５ｉ（設定コマンド受信処理部５１）から保守サーバ３（ＶＰＮゲートウェイ設定処理部３２）へのｔｅｌｎｅｔレスポンス＜ローカルネットワーク

セッション＞としてレスポンスを送信する。
【０１７５】
（保守サーバ後処理）
２－２５　ＶＰＮゲートウェイ設定処理部３２は、「▲１▼リモートメンテナンス要求コマンド」で受信した端末ＩＤを持つ情流ＧＷ端末１との間にＶＰＮの確立が完了しているかをＶＰＮゲートウェイ５ｉから取得する。確立が完了していない場合は、数秒間隔でＶＰＮ確立の完了を確認するまで同様の取得処理を繰り返す。ＶＰＮの確立完了が確認できた時点で、▲５▼リモートメンテナンス要求レスポンス処理を起動する。尚、ＶＰＮ設定が完了した段階で、その状態が、リモートメンテナンス装置４から確認できることが望ましい。理由は、ＶＰＮ設定が完了したことを確認した上で、▲６▼リモートメンテナンス開始指示を行えた方が保守者の作業効率がよいからである。
【０１７６】
▲６▼サーバ部１０とルータ部１１のＶＰＮＮＡＴ設定（端末サーバ部１０→端末ルータ部１１）
（端末処理部）
２－２８　リモートメンテナンス要求レスポンスを受信した端末サーバ部１０は、受付番号を保持する。
２－２９　端末サーバ部１０は、端末１の秘密鍵で、内線端末名とＶＰＮＮＡＴ用ローカルＩＰアドレスの組（複数の場合あり）を復号化し、ホストテーブルに保持する。
【０１７７】
２－３０　端末サーバ部１０は、内線端末名をキーとして、端末サーバ部１０がもつている内線端末名と実ＩＰアドレスの組のテーブル（ＤＮＳなどで参照）から端末名に対応する実ＩＰアドレスを取得し、端末名に対応するＶＰＮＮＡＴ用ローカルＩＰアドレスと実ＩＰアドレスをＶＰＮＮＡＴ１１０で対応付ける設定コマンド（複数の場合あり）（ルータ部１１のｔｅｌｎｅｔコマンドの実装により異なる。）を作成する。
（コマンド送信処理）
２－３１　２－３０で作成したコマンドをパラメータとして、端末１（ルータ設定処理部１０２）から端末１（ルータ部１１）へのｔｅｌｎｅｔコマンド＜ローカルネットワークセッション＞として、コマンドを送出する。
【０１７８】
（端末ルータ部処理）
２－３２　ＶＰＮＮＡＴ１１０の設定をルータ部１１に書き込む。
（レスポンス送信処理）
２－３３　ステータス（正常又はエラーステータス（コマンド異常等））をパラメータとして、端末１（ルータ部１１）から端末１（サーバ部１０／コマンド送出処理部１０２）へのｔｅｌｎｅｔレスポンス＜非Ｉｐｓｅｃセッション＞としてレスポンスを送信する。
（端末ルータ設定部後処理）
なし
以上により、リモートメンテナンス要求処理が完了となる。
【０１７９】
＜リモートメンテナンス実施処理＞
（リモートメンテナンス装置４→内線端末２ａ～２ｎ）
図６のシーケンス図及び図１９の手順フロー図に示すように、リモートメンテナンス実施処理は、前記リモートメンテナンス要求処理を受けて、ＩＰｓｅｃ等のＶＰＮによるトンネル１２を経由してリモートメンテナンス装置４から情流ＧＷ端末１本体及びその内線端末２ａ～２ｎに対してセキュアなリモートメンテナンスを行い（ＶＰＮ経由で行うため、伝送路が暗号化できる）、端末１の故障の復旧、パソコンへのアプリケーションのリモートインストール等を実施することを主旨とする。
【０１８０】
リモートメンテナンス装置４は、特殊なものではなく、ローカルネットワーク８上で内線

端末２ａ～２ｎに対してコマンドを送出することにより、内線端末２ａ～２ｎをメンテナンスできる装置であればそれを転用できる。機能としては、故障（例えば、Proxy故障）について、復旧動作（proxyの起動、端末１の再起動）を行い故障を復旧する。また、端末１のログの表示や、ルータ部１１の設定の確認も行える。ツールとしては、ｈｔｔｐクライアント（WeBブラウザ）や、ｔｅｌｎｅｔツール等である。

【０１８１】

また、パソコンに対するリモートインストールについては、ＶＮＣ等の遠隔制御ソフト等による。従って、この処理は、リモートメンテナンス装置４から、メンテナンスを行う内線端末２ａ～２ｎへの通信プロトコルに依存した汎用的なものであるため、詳しくは言及しない。

【０１８２】

繰り返しになるが、センタ９から内線端末２ａ～２ｎへの接続は、リモートメンテナンス要求時に付与したＶＰＮＮＡＴ用ローカルＩＰアドレスに対して行うことが本実施形態例のポイントである。

【０１８３】

▲１▼リモートメンテナンス開始処理(リモートメンテナンス装置４→保守サーバ３)

((通信契機))

ＶＰＮトンネル１２が張られている状態において、リモートメンテナンス装置４（図中保守端末）上のＷＥＢブラウザから、リモートメンテナンス保守者の任意の契機で起動される（前述した故障確認処理で故障を検知した時点でも、それに同期して起動するのが望ましい）。

【０１８４】

((リモートメンテナンス開始処理))

３－１　保守サーバ３のリモートメンテナンス要求確認画面にアクセスし、対象とするリモートメンテナンス要求に対するリモートメンテナンスを開始したことをＣＧＩ処理部３１で、保守サーバ３に通知する。

【０１８５】

((サーバ処理))

３－２　ＣＧＩ処理部３１でリモートメンテナンス開始を起動されると、リモートメンテナンス要求ＤＢ９２の該当テーブルのメンテナンス状態が「対応中」となる。

【０１８６】

▲２▼リモートメンテナンス実施処理（リモートメンテナンス装置４→内線端末２ａ～２ｎ）

((リモートメンテンナンス実施))

３－３　リモートメンテナンスを実施する。リモートメンテナンスでは、リモートメンテナンス要求を受けたＶＰＮＮＡＴ用ローカルＩＰアドレスに対してＶＰＮ経由でＩＰ接続を行う。

リモートメンテナンス実施時には、リモートメンテナンス要求ＤＢ９２を参照しながら作業を行えるようにサーバ側のユーザインタフェースを設計することを強く推奨する。

【０１８７】

＜リモートメンテナンス終了処理＞

図７のシーケンス図と図２０の手順フロー図に示すよう、リモートメンテナンス終了処理は、リモートメンテナンス要求で要求されたリモートメンテナンス作業が終了したことを、保守サーバ３から情流ＧＷ端末１に伝えることを主旨とする。

【０１８８】

▲１▼リモートメンテナンス終了コマンド送信処理（保守サーバ３→端末サーバ部１０）

((通信契機))

４－１　ＶＰＮトンネル１２が張られている状態において、要求されたリモートメンテナンス作業が終了した時点で、リモートメンテナンス装置４上のＷＥＢブラウザから保守サーバ３に対するリモートメンテナンス保守者によるＣＧＩ処理部３１のキックで起動され

る。
【０１８９】
((サーバ前処理))
４－２　ＣＧＩ処理部３１でリモートメンテナンス終了を起動されると、リモートメンテナンス要求ＤＢ９２の該当テーブルのメンテナンス状態が「終了」となる。なお、図３１にリモートメンテナンス要求ＤＢ９２のテーブルレコードを示す。
【０１９０】
４－３　保守サーバ３は、リモートメンテナンス要求ＤＢ９２の該当テーブルのメンテナンス状態が「終了」となったこと検知すると、受付番号ををパラメータとして、該当テーブルの受付番号を取得し、受付番号をバラメータとしてリモートメンテナンス終了コマンドを作成する。この受付番号は、後に説明するＶＰＮＮＡＴ１１０解放処理及びＶＰＮ終了処理でも参照される。
【０１９１】
((コマンド送信処理))
４－４　前の処理で作成したコマンドをパラメータとして保守サーバ３から端末１（ｈｔｔｐサーバ部１００）へのｈｔｔｐコマンドで＜ＩＰｓｅｃセッション＞としてリモートメンテナンス終了コマンドを送信する。
【０１９２】
▲２▼リモートメンテナンス終了コマンド受信処理（端末サーバ部１０→保守サーバ３）
((端末サーバ部処理))
４－５　リモートメンテナンス終了を受信すると、パラメータから受付番号を抽出し、保持していた受付番号の状態を終了とする。
【０１９３】
((レスポンス送信処理))
４－６　端末１のｈｔｔｐサーバ部１００は、ステータス（正常またはエラーステータス）をパラメータとし、端末１（ｈｔｔｐサーバ部１００）から保守センタ９へのｈｔｔｐレスポンス＜ＩＰｓｅｃセッション＞としてレスポンスを送信する。
【０１９４】
▲３▼リモートメンテナンス終了レスポンス受信後処理（保守サーバ３）
((サーバ後処理))
４－７　レスポンス受信後、該当内線端末２ａ～２ｎに対するメンテナンスが全て終了したかを判断し、該当内線端末２ａ～２ｎに対するメンテナンスが全て終了していなかったら処理を終了する。
該当内線端末２ａ～２ｎに対するメンテナンスが全て終了ていたら、さらに、終了した内線端末は情流ＧＷ端末１のサーバ部１０又はルータ部１１かを判断し、端末１のサーバ部１０又はルータ部１１でない場合は、ＶＰＮＮＡＴ解放処理を起動する。
【０１９５】
端末１のサーバ部１０又はルータ部１１の場合は、対応する情流ＧＷ端末１に対するリモートメンテナンスを全て終了したかを判断し、全て終了していたら、ＶＰＮ終了処理を起動し、全て終了していなかったら、処理を終了する。
以上で、リモートメンテナンス終了処理が完了となる。
【０１９６】
＜ＶＰＮＮＡＴ解放処理＞
図８のシーケンス図及び図２１、図２２の手順フロー図に示すよう、ＶＰＮＮＡＴ１１０解放処理は、リモートメンテナンス要求時に保守センタ９から情流ＧＷ端末１に割り振られたＶＰＮＮＡＴ用のＶＰＮＮＡＴ用ローカルＩＰアドレスを解放することを主旨とする。
【０１９７】
▲１▼ＶＰＮＮＡＴ１１０解放コマンド送信処理（保守サーバ３→端末サーバ部１０）
((通信契機))

５－１　ＶＰＮトンネル１２が張られている状態において、リモートメンテナンス終了後、該当内線端末２ａ～２ｎに対するメンテナンスが全て終了し、その内線端末２ａ～２ｎが情流ＧＷ端末１のサーバ部１０又はルータ部１１以外の場合に起動される。

【０１９８】

((サーバ前処理))

５－２　ＶＰＮＮＡＴ１１０解放コマンドを作成する。なお、リモートメンテナンス要求ＤＢ９２のテーブルレコードは図３１と同一である。

((コマンド送信処理))

５－３　保守サーバ３は、内線端末名をパラメータとして、保守サーバ３から端末１（ｈｔｔｐサーバ部１００）へのｈｔｔｐコマンドで＜ＩＰｓｅｃセッション＞としてＶＰＮＮＡＴ解放コマンドを送信する。

【０１９９】

▲２▼ＶＰＮＮＡＴ解放コマンド受信処理（端末サーバ部１０→端末ルータ部１１）

((端末前処理))

５－４　端末サーバ部１０は、ＶＰＮＮＮＡＴ１１０解放コマンドを受信し、パラメータの内線端末２ａ～２ｎ名をキーとして、端末サーバ部１０がもっている端末名と実ＩＰアドレスの組のテーブル（ＤＮＳ等で参照）から端末名に対応する実ＩＰアドレスを取得する。

【０２００】

そして、端末名に対応するＶＰＮＮＡＴ用ローカルＩＰアドレスと実ＩＰアドレスのＶＰＮＮＡＴ１１０を解放するコマンド（複数の場合あり）（ルータ部１１のｔｅｌｎｅｔコマンドの実装により異なる）を作成する。

【０２０１】

((コマンド送信処理))

５－５　前の処理で作成したコマンドをパラメータとして、端末１（ルータ設定処理部１０２）から端末１（ルータ部１１）へのｔｅｌｎｅｔコマンド＜ローカルネットワークセッション＞として、コマンドを送出する。

((端末ルータ部処理))

５－６　ＶＰＮＮＡＴ１１０解放の設定をルータ部１１に書き込む。

【０２０２】

((レスポンス送信処理))

５－７　ステータス（正常またはエラーステータス（コマンド異常等))をパラメータとして、端末１（ルータ部１１）から端末１（サーバ部１０／コマンド送出処理部１０３）へのｔｅｌｎｅｔレスポンス＜非ＩＰｓｅｃセッション＞としてレスポンスを送信する。

((端末ルータ設定部後処理))

５－８　ホストテーブルの端末名に対応するレコードを削除する。

【０２０３】

▲３▼ＶＰＮＮＡＴ１１０解放レスポンス送信処理（端末サーバ部１０→保守サーバ３）

((レスポンス送信処理))

５－９　端末１のｈｔｔｐサーバ部１００は、ステータス（正常またはエラーステータス）をパラメータとし、端末１（サーバ部１０）から保守センタ９へのｈｔｔｐレスポンス＜ＩＰｓｅｃセッション＞としてレスポンスを送信する。

【０２０４】

▲４▼保守サーバ側ＶＰＮＮＡＴ用ローカルＩＰアドレス変換処理（保守サーバ３）

((ＶＰＮＮＡＴ用ローカルＩＰアドレス変換処理))

５－１０　サーバ側で処理中の受付番号に対応する内線端末２ａ～２ｎに対応するＶＰＮＮＡＴ用ローカルＩＰアドレスをリモートメンテナンス要求ＤＢ９２から取得し、保持するとともに、ＶＰＮＮＡＴＤＢ９１の対応ＶＰＮＮＡＴ用ローカルＩＰアドレスを解放する。

【０２０５】

▲５▼ＩＰｓｅｃ処理対象パケット解除設定（保守サーバ３→ＶＰＮゲートウェイ５）
((コマンド送信処理))
５－１１　ＶＰＮゲートウェイ設定処理部３２は、リモートメンテナンス要求ＤＢ９２の処理中の受付番号に該当するレコードから、端末ＩＤ、ＶＰＮＮＡＴ用ローカルＩＰアドレスを取得する。
【０２０６】
５－１２　ＶＰＮゲートウェイ設定処理部３２は、ＶＰＮＮＡＴ用ローカルＩＰアドレス向けパケットを端末ＩＤに対応したＶＰＮトンネル１２に割り付けるための設定を解除するためのコマンド（ＶＰＮゲートウェイ５のｔｅｌｎｅｔコマンドの実装により異なる）をパラメータとして、保守サーバ３（ＶＰＮゲートウェイ設定処理部３２）からＶＰＮゲートウェイ５（設定コマンド受信処理部５１）へのｔｅｌｎｅｔコマンド＜ローカルネットワークセッション＞としてコマンドを送信する。
【０２０７】
((ＶＰＮゲートウェイ処理))
５－１３　受信したＶＰＮＮＡＴ用ローカルＩＰアドレス向けルーティングの設定をＶＰＮゲートウェイ５から解除する。
【０２０８】
（レスポンス送信処理）
５－１４　ステータス（正常またはエラーステータス（コマンド異常等))をパラメータとして、ＶＰＮゲートウェイ５（設定コマンド受信処理部５１）から保守サーバ３（ＶＰＮゲートウェイ設定処理部３２）へのｔｅｌｎｅｔレスポンス＜ローカルネットワークセッション＞としてレスポンスを送信する。
【０２０９】
((ＶＰＮゲートウェイ設定処理部後処理))
５－１５　対応する情流ＧＷ端末１に対するリモートメンテナンスを全て終了したかを判断し、全て終了していたら、ＶＰＮ終了処理を起動し、全て終了していいなかったら、処理を終了する。
【０２１０】
＜ＶＰＮ終了処理＞
図９のシーケンス図及び図２３乃至図２５の手順フロー図に示すよう、ＶＰＮ終了処理は、リモートメンテナンス要求時に保守センタ９から構築されたＶＰＮを終了することを主旨とする。
【０２１１】
▲１▼ＶＰＮ終了コマンド送信処理（保守サーバ３→端末サーバ部１０）
((通信契機))
６－１　ＶＰＮトンネル１２が張られている状態において、リモートメンテナンス終了後、対応する情流ＧＷ端末１に対するメンテナンスが全て終了した場合に起動される。
【０２１２】
((サーバ前処理))
６－２　ＶＰＮ終了コマンドを作成する。なお、リモートメンテナンス要求ＤＢ９２のテーブルレコードは図２９と同一である。
（コマンド送信処理）
６－３　保守サーバ３は、保守サーバ３から端末１（ｈｔｔｐサーバ部１００）へのｈｔｔｐコマンドで＜ＩＰｓｅｃセッション＞としてＶＰＮ終了コマンドを送信する。
【０２１３】
▲２▼ＶＰＮ終了コマンド受信処理（端末サーバ部１０→端末ルータ部１１）
((端末前処理))
６－４　端末サーバ部１０は、ＶＰＮ終了コマンドを受信し、全てのＶＰＮＮＡＴ１１０を解放するコマンド（複数の場合あり）（ルータ部１１のｔｅｌｎｅｔコマンドの実装により異なる）を作成する。

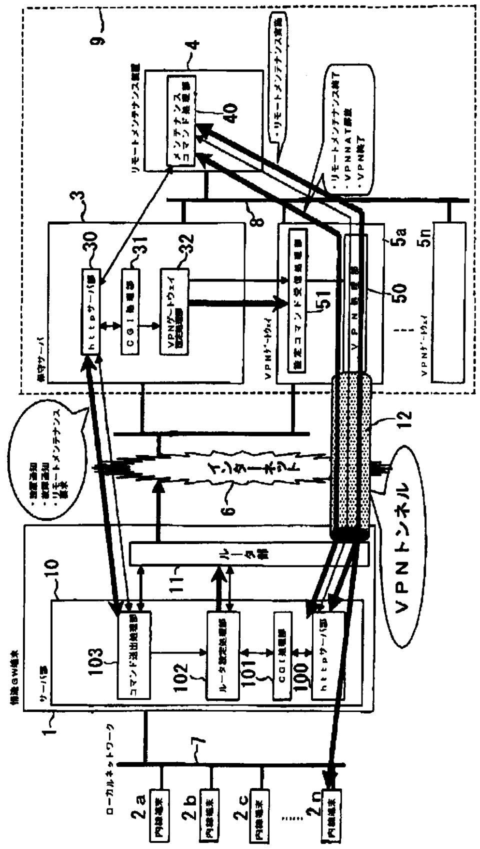
【０２１４】
((コマンド送信処理))
６－５　前の処理で作成したコマンドをパラメータとして、端末１（ルータ設定処理部１０２）から端末１（ルータ部１１）へのｔｅｌｎｅｔコマンド＜ローカルネットワークセッション＞として、コマンドを送出する。
▲３▼ＶＰＮＮＡＴ設定初期化コマンド受信及び処理（ルータ部１１）
((端末ルータ部処理))
６－６　ＶＰＮＮＡＴ１１０解放の設定をルータ部１１に書き込む。
【０２１５】
((レスポンス送信処理))
６－７　ステータス（正常またはエラーステータス（コマンド異常等))をパラメータとして、端末１（ルータ部１１）から端末１（サーバ部１０／コマンド送出処理部１０３）へのｔｅｌｎｅｔレスポンス＜ローカルセッション＞としてレスポンスを送信する。
((端末ルータ設定部後処理))
６－８　ホストテーブルを全て削除する。
【０２１６】
▲４▼ＶＰＮ終了レスポンス送信処理（端末サーバ部１０→保守サーバ１１）
((レスポンス送信処理))
６－９　端末１のｈｔｔｐサーバ部１００は、ステータス（正常またはエラーステータス）をパラメータとし、端末１（ｈｔｔｐサーバ部１００）から保守センタ９へのｈｔｔｐレスポンス＜ＩＰｓｅｃセッション＞としてレスポンスを送信する。
【０２１７】
▲５▼保守サーバ側ＶＰＮＮＡＴ用ローカルＩＰアドレス変換処理（保守サーバ３）
((ＶＰＮＮＡＴ用ローカルＩＰアドレス変換処理))
６－１０　サーバ側で処理中の受付番号に対応するＶＰＮＮＡＴ用ローカルＩＰアドレスを全てリモートメンテナンス要求ＤＢ９２から取得し、保持するとともに、ＶＰＮＮＡＴＤＢ９１の対応ＶＰＮＮＡＴ用ローカルＩＰアドレスを解放する。
【０２１８】
▲６▼ＩＰＳｅｃ処理対象パケット解除設定（保守サーバ３→ＶＰＮゲートウェイ５）
((コマンド送信処理))
６－１１　ＶＰＮゲートウェイ設定処理部３２は、リモートメンテナンス要求ＤＢ９２の該当レコードから、端末ＩＤに対応するすべての端末ＩＤ、ＶＰＮＮＡＴ用ローカルＩＰアドレスを取得する。
【０２１９】
６－１２　ＶＰＮゲートウェイ設定処理部３２は、ＶＰＮＮＡＴ用ローカルＩＰアドレス向けパケットを端末ＩＤに対応したＶＰＮトンネル１２に割り付けるための設定を解除するためのコマンド（ＶＰＮゲートウェイ５のｔｅｌｎｅｔコマンドの実装により異なる）をパラメータとして、保守サーバ３（ＶＰＮゲートウェイ設定処理部３２）からＶＰＮゲートウェイ５（設定コマンド受信処理部５１）へのｔｅｌｎｅｔコマンド＜ローカルネットワークセッション＞としてコマンドを送信する。
【０２２０】
((ＶＰＮゲートウェイ処理))
６－１３　受信したＶＰＮＮＡＴ用ローカルＩＰアドレス向けルーティングの設定をＶＰＮゲートウェイ５ｉから解除する。
【０２２１】
((レスポンス送信処理))
６－１４　ステータス（正常またはエラーステータス（コマンド異常等))をパラメータとして、ＶＰＮゲートウェイ５（設定コマンド受信処理部５１）から保守サーバ３（ＶＰＮゲートウェイ設定処理部３２）へのｔｅｌｎｅｔレスポンス＜ローカルネットワークセッション＞としてレスポンスを送信する。

【０２２２】
▲７▼ＩＰｓｅｃ設定解除コマンド送信処理（保守サーバ３→ＶＰＮゲートウェイ５）
((コマンド送信処理))
６－１５　ＶＰＮゲートウェイ設定処理部３２は、処理中の受付番号に対応するリモートメンテナンス要求ＤＢ９２のレコードから、端末ＩＤを取得する。
【０２２３】
６－１６　ＶＰＮゲートウェイ設定処理部３２は、端末ＩＤに対応したＶＰＮトンネル１２を解除するための設定（ＶＰＮゲートウェイ５のｔｅｌｎｅｔコマンドの実装により異なる）をパラメータとして、保守サーバ３（ＶＰＮゲートウェイ設定処理部３２）からＶＰＮゲートウェイ５（設定コマンド受信処理部５１）へのｔｅｌｎｅｔコマンド＜ローカルネットワークセッション＞としてコマンドを送信する。
【０２２４】
▲８▼ＩＰｓｅｃ設定解除コマンド受信及び処理（ＶＰＮゲートウェイ５）
((ＶＰＮゲートウェイ処理))
６－１７　受信した端末ＩＤに対応するＶＰＮの設定をＶＰＮゲートウェイ５から解除する。
【０２２５】
((レスポンス送信処理))
６－１８　ステータス（正常またはエラーステータス（コマンド異常等))をパラメータとして、ＶＰＮゲートウェイ５（設定コマンド受信処理部５１）から保守サーバ３（ＶＰＮゲートウェイ設定処理部３２）へのｔｅｌｎｅｔレスポンス＜ローカルネットワークセッション＞としてレスポンスを送信する。
【０２２６】
((ＶＰＮゲートウェイ設定処理部後処理))
６－１９　ＶＰＮＧＷアドレス要求処理でＶＰＮゲートウェイトンネルＤＢから取得保持し「端末ＩＤ」を書き込んだフィールドを「未使用」に書き換え、ＶＰＮトンネルリソースを解放する。
上記でリモートメンテナンス終了処理が完了となる。
以上、シーケンス図３～シーケンス図９及び手順フロー図１３～手順フロー図２５をもとに、リモートメンテナンスの処理手順を説明した。
【０２２７】
本記録媒体例は、当該リモートメンテナンスの処理プログラム手順の一連の完結手続をコンピュータ読取り自在に実録したものである。
【０２２８】
本実施形態例では、情流ＧＷ端末１本体のサーバ部１０及びルータ部１１へのＶＰＮＮＡＴ１１０の設定は設置通知時に行っているが、これはリモートメンテナンス要求なしに、保守センタ９側から任意の契機で情流ＧＷ端末１にＶＰＮアクセスを可能とするための機能である。したがって、情流ＧＷ端末１本体のサーバ部１０及びルータ部１１へのＶＰＮＮＡＴ１１０の設定を特別扱いせずに、リモートメンテナンス要求時にＶＰＮＮＡＴ１１０を設定し、それをＶＰＮＮＡＴ１１０解放時に解放する手順でもよいのは言うまでもない。
【０２２９】
本実施例においては、ＶＰＮにＩＰｓｅｃを用いて説明しているが、本発明はレイヤ３レベルのＶＰＮであればＩＰｓｅｃ以外に対しても適用可能なことは言うまでもない。
【０２３０】
【発明の効果】
かくして、本発明によれば、ＶＰＮＮＡＴに用いる有限のＶＰＮＮＡＴ用ローカルＩＰアドレスリソースが、リモートメンテナンス要求端末に対してだけ割り当てられて、リモートナンス終了時にＶＰＮＮＡＴ解放プロセスで解放されることにより、ＩＰアドレス資源が節約でき、静的ＶＰＮＮＡＴ方式と比較して同時に多くの端末をリモートメンテナンス

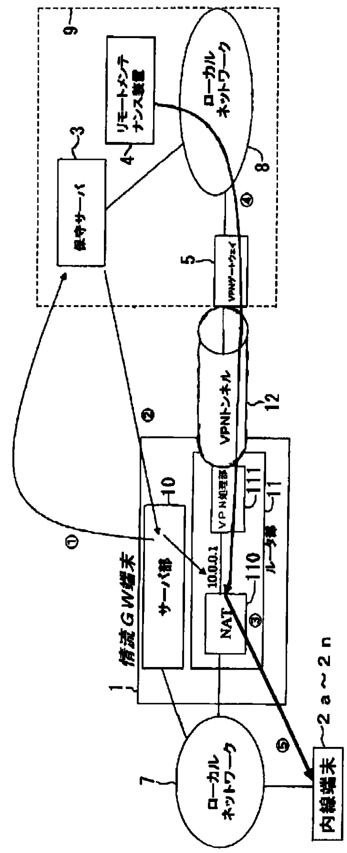
できる。
【０２３１】
言い換えれば、従来は最大「ＶＰＮＮＡＴ用ローカルＩＰアドレスリソース」分の内線端末をリモートメンテナンス対象端末となっていたのに対し、本発明を用いることにより、同時に「ＶＰＮＮＡＴ用ローカルＩＰアドレスリソース」分の内線端末をリモートメンテナンス対象端末とすることが可能になり、リモートメンテナンスサービス対象端末の加入者数を大幅に増やすことができる。
【０２３２】
しかも、ＶＰＮＮＡＴに用いる有限のＶＰＮＮＡＴ用ローカルＩＰアドレスリソースが、リモートメンテナンス要求端末に対してだけ割り当てられて、リモートナンス終了時にＶＰＮＮＡＴ解放プロセスで解放されることにより、リモートメンテナンス要求対象とした内線端末に対してだけ保守センタからのアクセスを許すリモートメンテナンス方法を実現することができる。
【０２３３】
また、リモートメンテナンスサービス提供者にとっては、保守センタがＶＰＮゲートウェイの設備を設置する際、ＶＰＮリモートメンテナンスのアクセス数に応じてＶＰＮゲートウェイの設備を増設設置することができ、ひいては、ＶＰＮゲートウェイの設備コストを最適化できる。
【０２３４】
前述の効果から、リモートメンテナンスサービスを享受するお客様にとっては、保守センタとＶＰＮを構築する際ＶＰＮのリソース不足となることが少なくなり、ＶＰＮ構築失敗でリモートメンテナンスを受けられなくなるケースが減少する。
【図面の簡単な説明】
【図１】本発明の実施の形態を示すシステム例のシステム構成図である。
【図２】同上において、ＶＰＮＮＡＴに動的にＶＰＮＮＡＴ用ローカルＩＰアドレスを付与する機能説明図である。
【図３】本発明の実施の形態を示す方法例における設置通知処理のシーケンス図である。
【図４】同上におけるＶＰＮＧＷアドレス要求処理のシーケンス図である。
【図５】同上におけるリモートメンテナンス要求処理のシーケンス図である。
【図６】同上におけるリモートメンテナンス実施処理のシーケンス図である。
【図７】同上におけるリモートメンテナンス終了処理のシーケンス図である。
【図８】同上におけるＶＰＮＮＡＴ解放処理のシーケンス図である。
【図９】同上におけるＶＰＮ終了処理のシーケンス図である。
【図１０】本発明の実施の形態を示すプログラム例及び記録媒体例における情報ＧＷ端末側概括フローチャートである。
【図１１】同上における保守センタ側概括フローチャートである。
【図１２】同上における設置通知処理の前半フロー手順図である。
【図１３】同上における設置通知処理の後半フロー手順図である。
【図１４】同上におけるＶＰＮＧＷアドレス要求処理の前半フロー手順図である。
【図１５】同上におけるＶＰＮＧＷアドレス要求処理の後半フロー手順図である。
【図１６】同上におけるリモートメンテナンス要求処理の初期段階フロー手順図である。
【図１７】同上におけるリモートメンテナンス要求処理の第２段階フロー手順である。
【図１８】同上におけるリモートメンテナンス要求処理の最終段階フロー手順図である。
【図１９】同上におけるリモートメンテナンス実施処理のフロー手順図である。
【図２０】同上におけるリモートメンテナンス終了処理のフロー手順図である。
【図２１】同上におけるＶＰＮＮＡＴ解放処理の前半フロー手順図である。
【図２２】同上におけるＶＰＮＮＡＴ解放処理の後半フロー手順図である。
【図２３】同上におけるＶＰＮ終了処理の初期フロー手順図である。
【図２４】同上におけるＶＰＮ終了処理の中間フロー手順図である。
【図２５】同上におけるＶＰＮ終了処理の最終フロー手順図である。

【図２６】本発明の実施の形態を示す方法例における故障通知処理のシーケンス図である。
【図２７】本発明の実施の形態を示すプログラム例及び記録媒体例における故障通知処理のフロー手順図である。
【図２８】図１６中、端末ＤＢ９０のレコード内容を示すテーブルである。
【図２９】図１６中、リモートメンテナンス要求ＤＢ９２のレコード内容を示すテーブルである。
【図３０】図１６中、ＶＰＮＮＡＴＤＢ９１のレコード内容を示すテーブルである。
【図３１】図２０中、リモートメンテナンス要求ＤＢ９２のレコード内容を示すテーブルである。
【図３２】従来システムにおけるＶＰＮＮＡＴの機能説明図である。
【図３３】同上における２地点同時接続のＶＰＮＮＡＴの機能説明図である。
【符号の説明】
１…インターネットゲートウェイ端末（端末情流ＧＷ端末）
２ａ～２ｎ…内線端末
３…保守サーバ
４…リモートメンテナンス装置
５、５ａ、５ｉ、５ｎ…ＶＰＮゲートウェイ（ＶＰＮＧＷ）
６…インターネット
７，８…ローカルネットワーク（ＬＡＮ）
９…保守センタ（センタ）
１０…サーバ部（端末サーバ部）
１１…ルータ部（端末ルータ部、ＶＰＮルータ部）
１２…ＶＰＮトンネル
３０，１００…ｈｔｔｐサーバ部
３１，１０１…ＣＧＩ処理部
３２…ＶＰＮゲートウェイ設定処理部
４０…メンテナンスコマンド処理部
５０…ＶＰＮ処理部
５１…設定コマンド受信処理部
１０２…ルータ設定処理部
１０３…コマンド送出処理部
１１０…ＮＡＴ（ＶＰＮＮＡＴ）

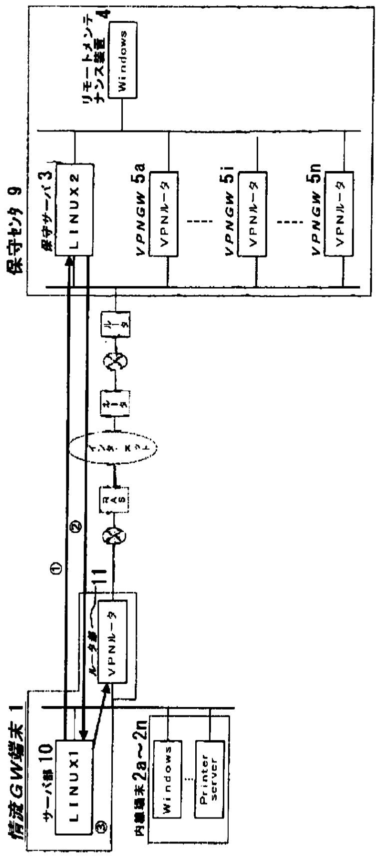
【図１】


VPNトンネル
インターネット
ローカルネットワーク

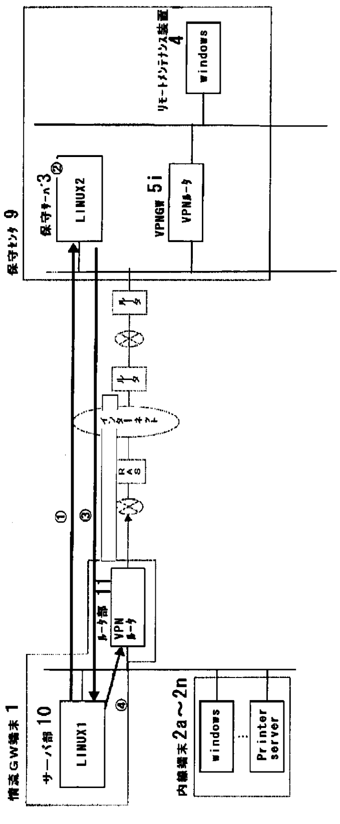
【図２】


情流GW端末
サーバ部
ルータ部
NAT
10.0.0.1
VPN処理部
VPNトンネル
保守サーバ
リモートメンテナンス装置
ローカルネットワーク
内線端末
2a～2n

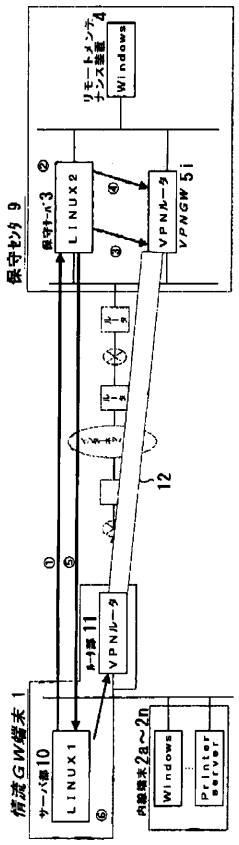
【図３】


保守センタ 9
保守サーバ 3
LINUX2
リモートメンテナンス装置 4
Windows
VPNGW 5a
VPNGW 5i
VPNGW 5n
VPNルータ
情流GW端末 1
サーバ部 10
LINUX1
ルータ部
内線端末2a～2n
Windows
Printer server

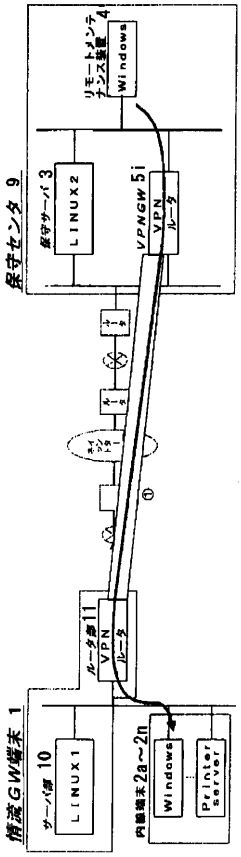
【図４】


保守センタ 9
LINUX2
VPNGW 5i
VPNルータ
windows
情流GW端末 1
サーバ部 10
LINUX1
ルータ部
内線端末2a～2n
windows
Printer server

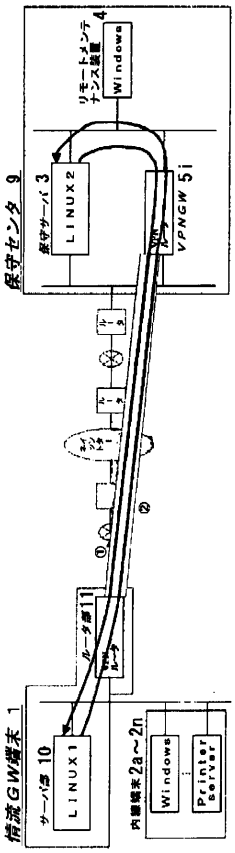
【図５】


保守センタ 9
保守サーバ3
LINUX2
リモートメンテナンス装置 4
Windows
VPNルータ
VPNGW 5i
12
情流GW端末 1
サーバ部10
LINUX1
ルータ部11
VPNルータ
内線端末2a～2n
Windows
Printer server

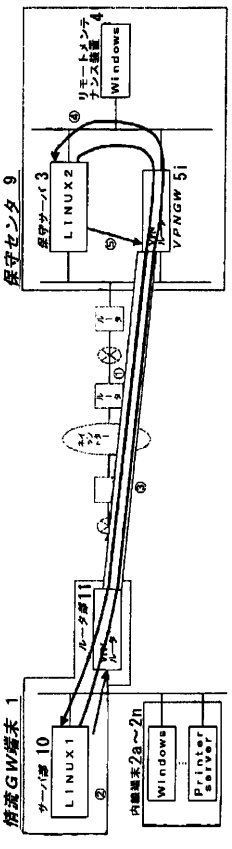
【図６】


保守センタ 9
保守サーバ3
LINUX2
リモートメンテナンス装置 4
Windows
VPNGW 5i
VPN ルータ
情流GW端末 1
サーバ部 10
LINUX1
ルータ部11
VPN ルータ
内線端末2a～2n
Windows
Printer server

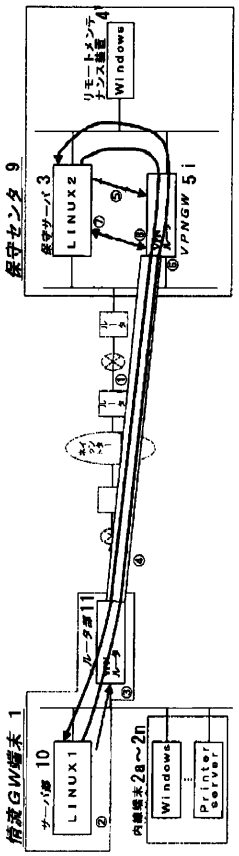
【図７】


保守センタ 9
保守サーバ3
LINUX2
リモートメンテナンス装置 4
Windows
VPNGW 5i
情流GW端末 1
サーバ部 10
LINUX1
ルータ部11
内線端末2a～2n
Windows
Printer server

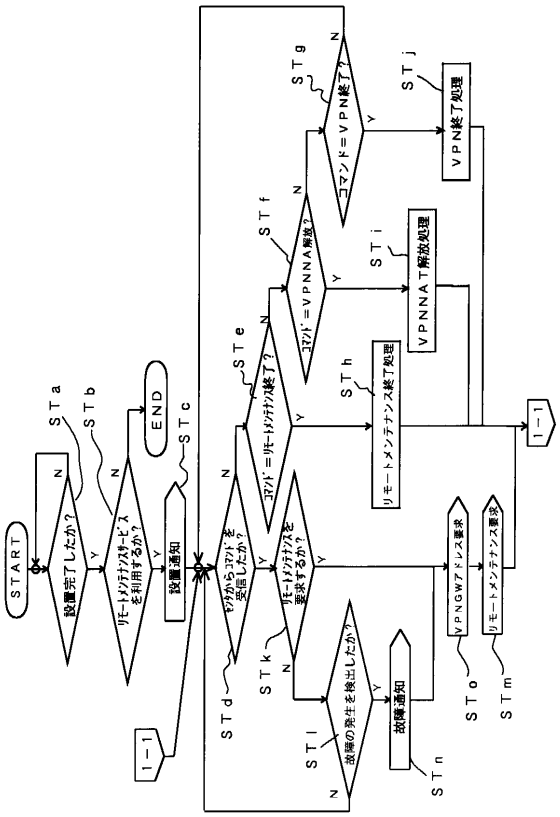
【図８】


保守センタ 9
保守サーバ3
LINUX2
リモートメンテナンス装置 4
Windows
VPNGW 5i
情流GW端末 1
サーバ部 10
LINUX1
ルータ部11
内線端末2a～2n
Windows
Printer server

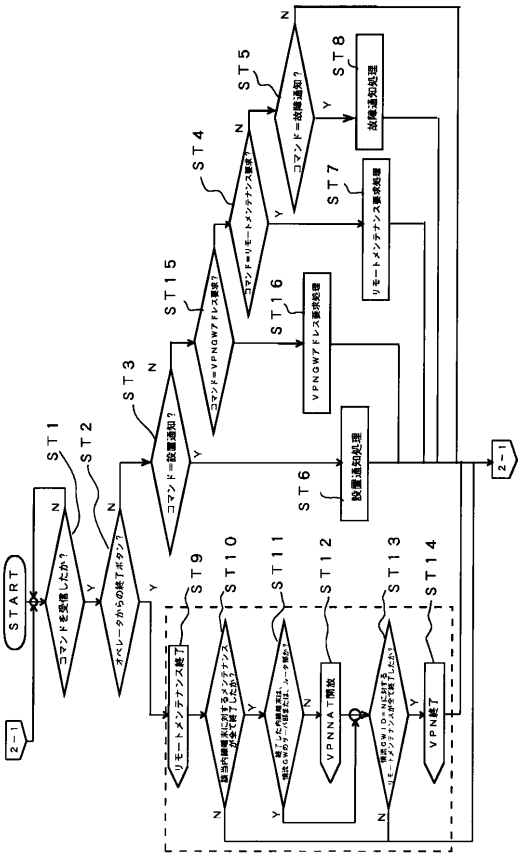
【図９】



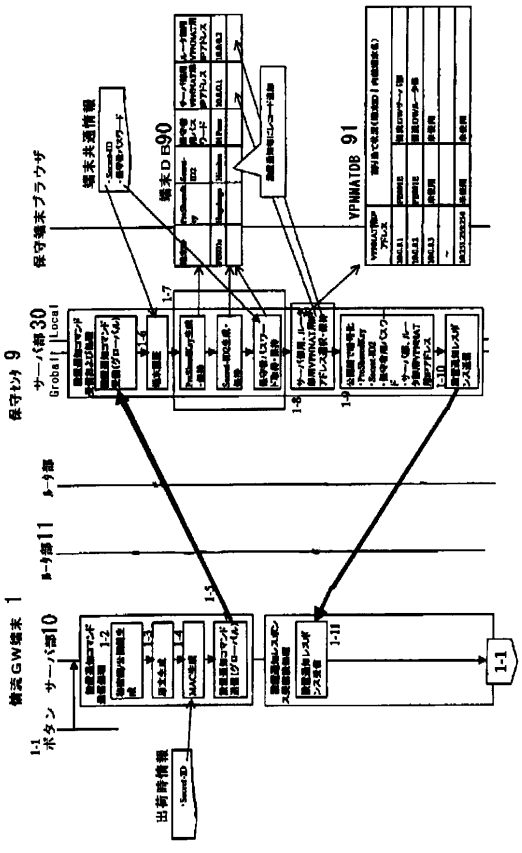
【図１０】



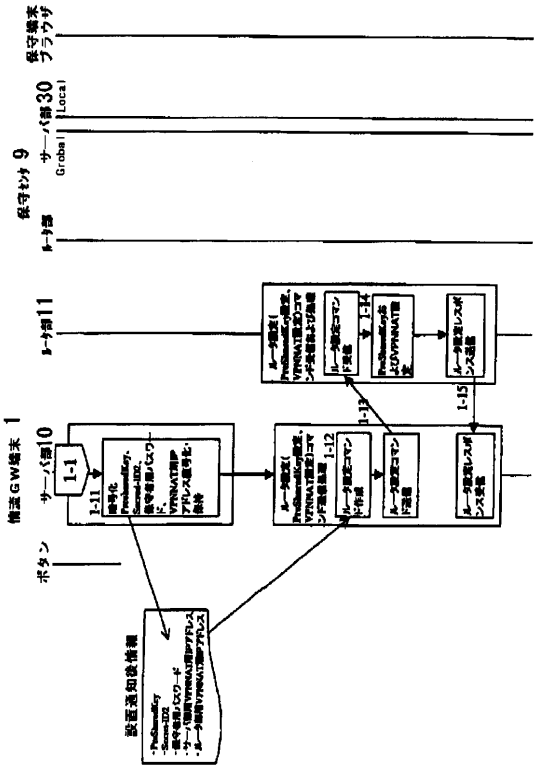
【図１１】



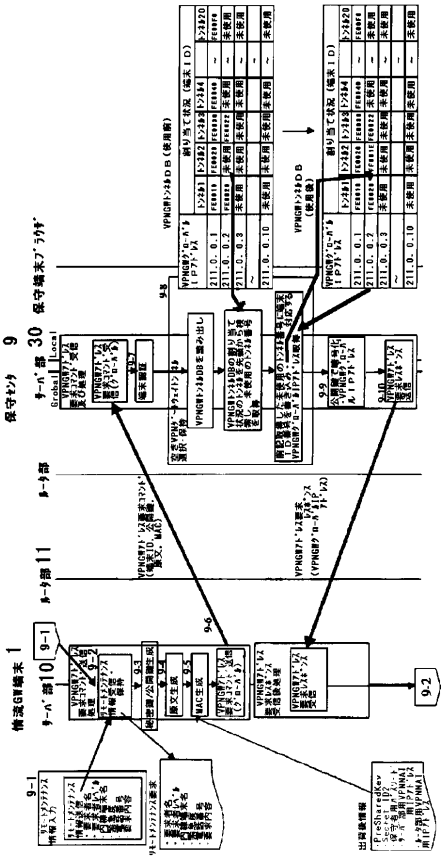
【図１２】



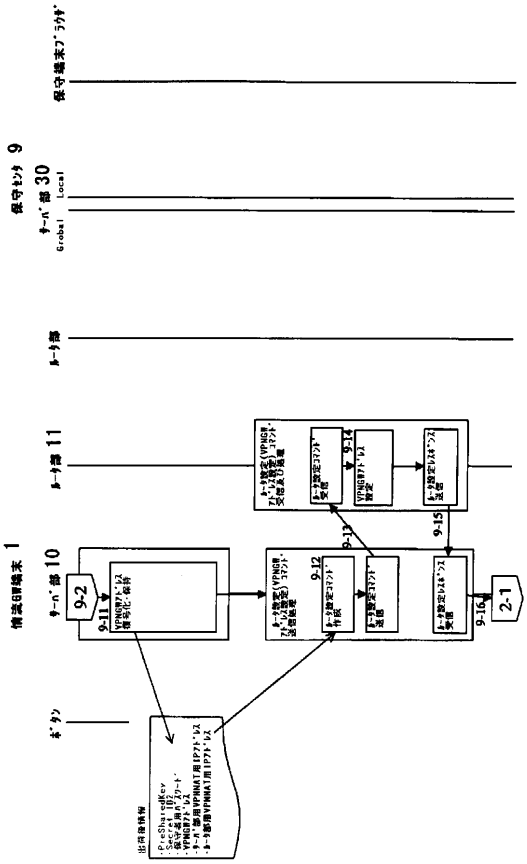
【図１３】



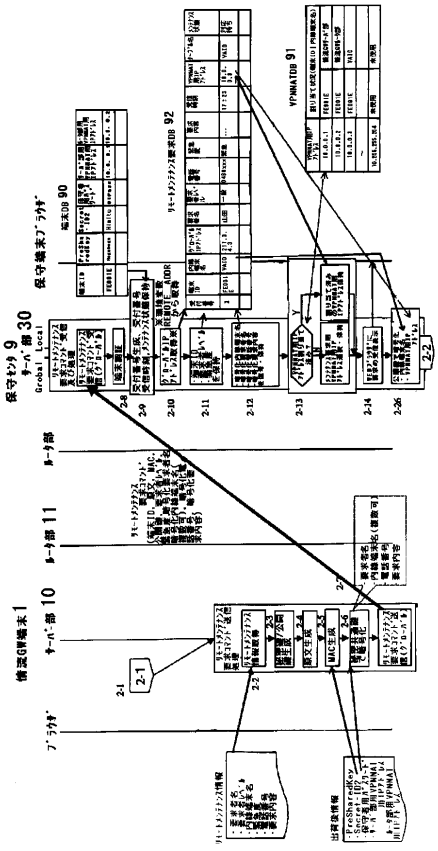
【図１４】



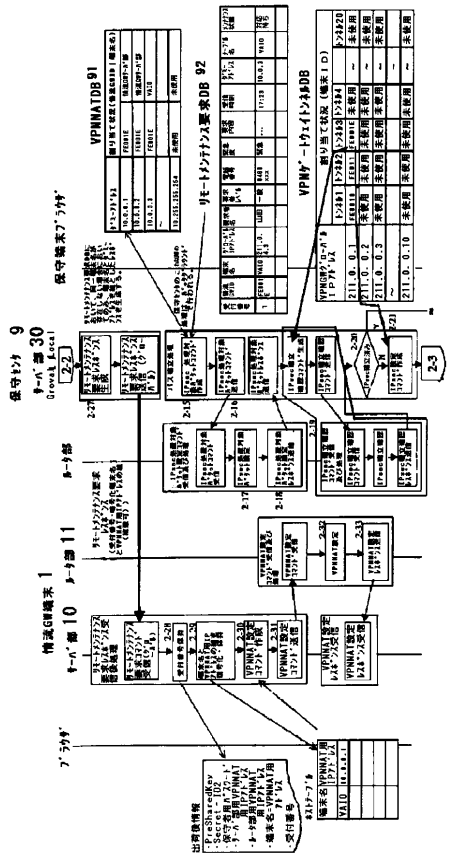
【図１５】



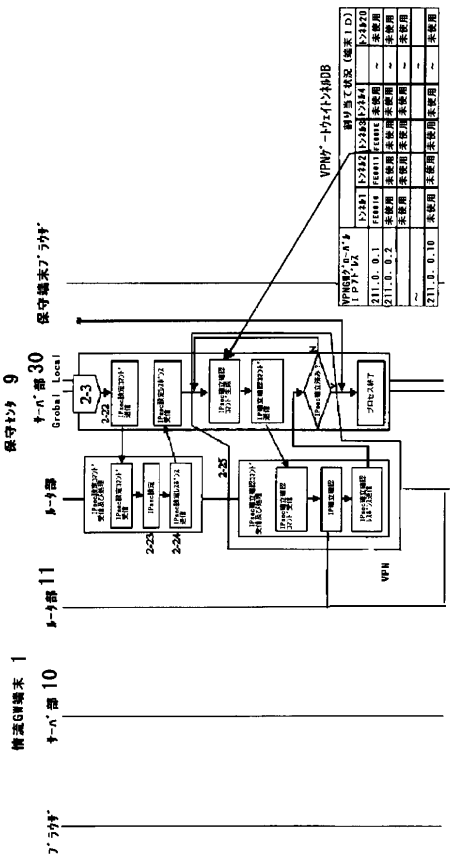
【図１６】



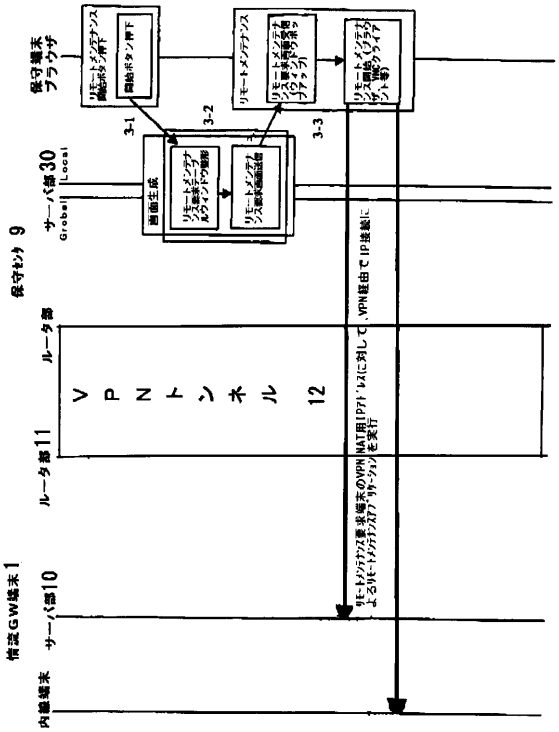
【図１７】



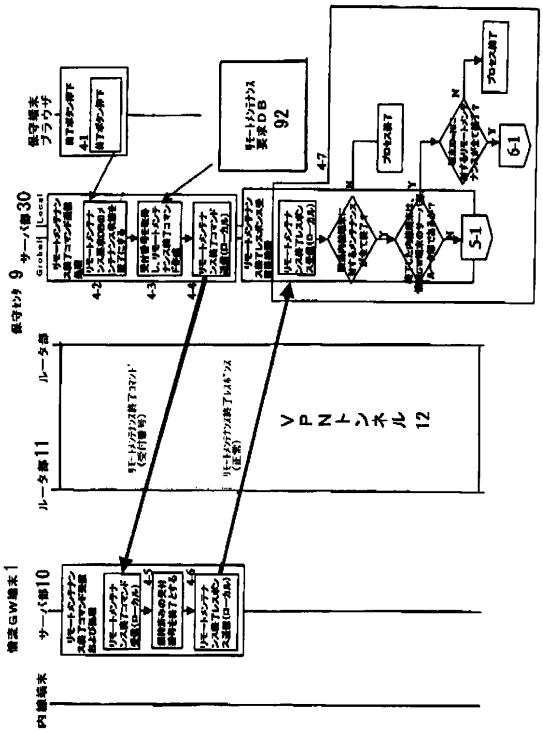
【図１８】



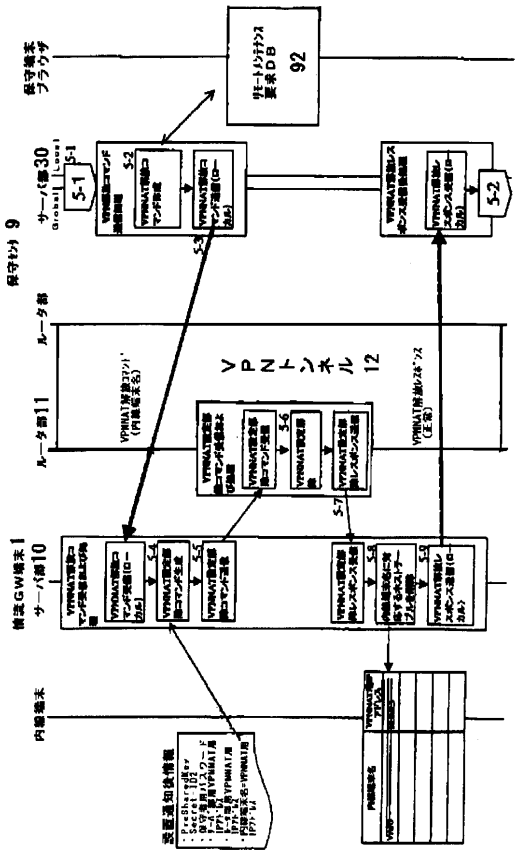
【図１９】



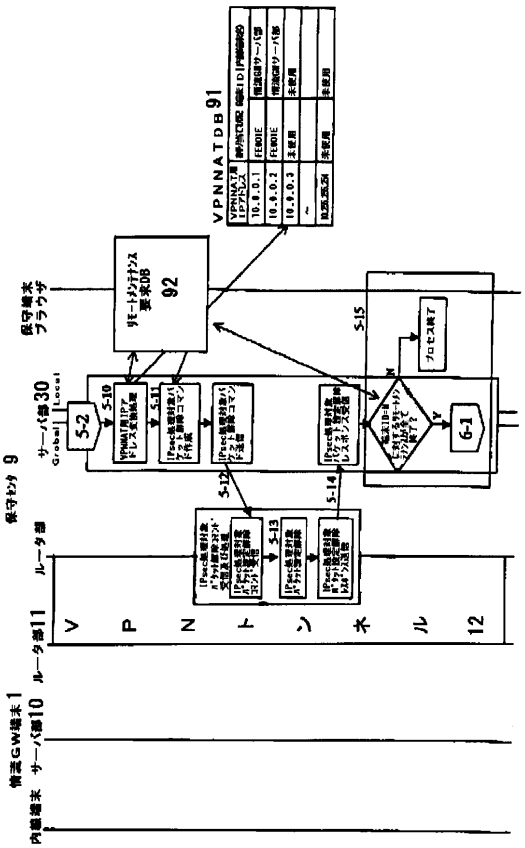
【図２０】



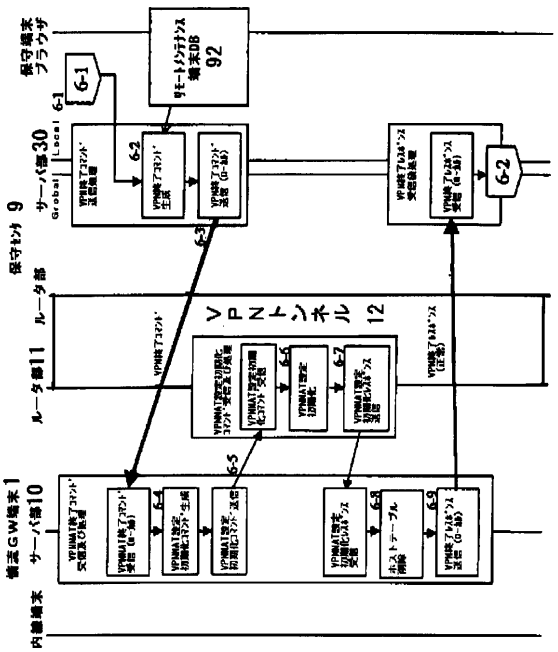
【図２１】



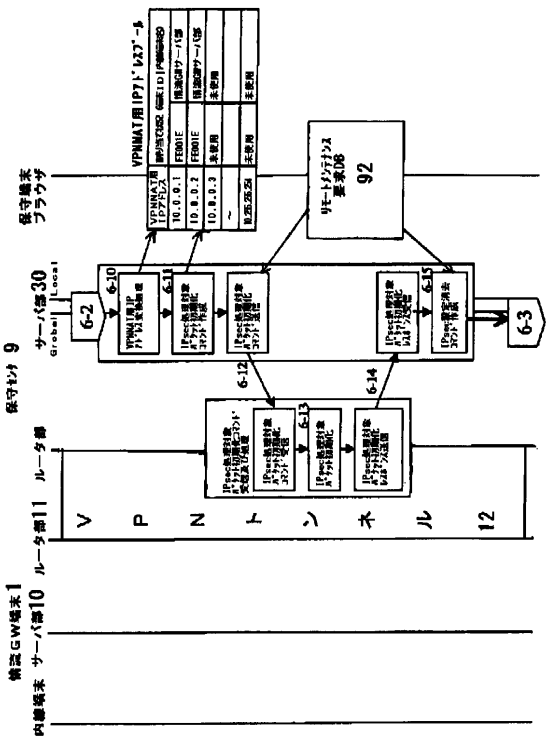
【図２２】



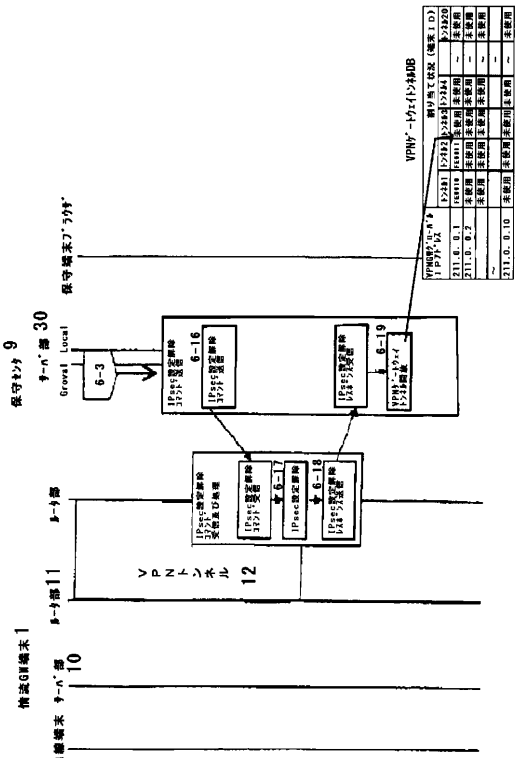
【図２３】



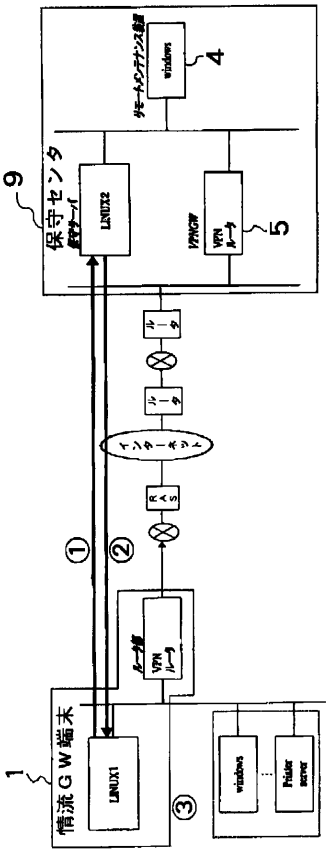
【図２４】



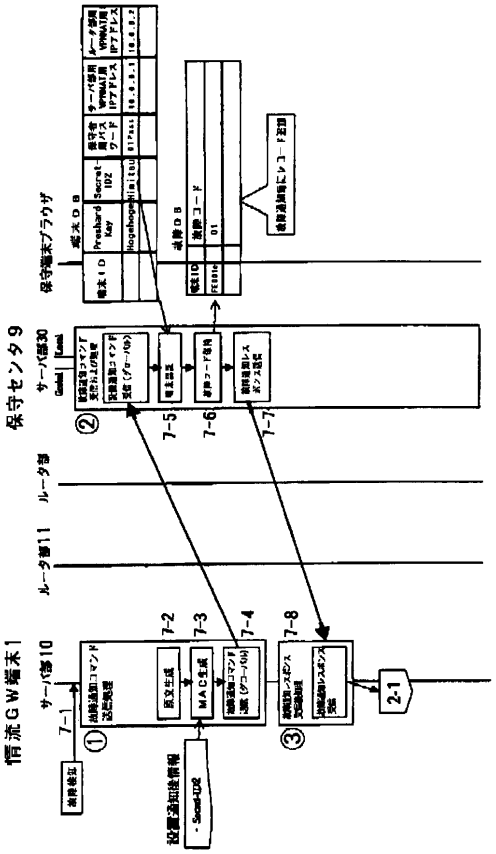
【図２５】



【図２６】



【図２７】



【図２８】

端末ＤＢ９０

端末ID	Presharedkey	Secret-ID2	保守者用パスワード	サーバ部用VPNNAT用IPアドレス	ルータ部用VPNNAT用IPアドレス
FE001E	Hogehoge	Hiaitsu	01Pass	10.0.0.1	10.0.0.2

【図２９】

リモートメンテナンス要求ＤＢ９２

受付番号	端末ＩＤ	内線端末名	グローバルIPアドレス	要求者名	要求者レベル	電話番号	緊急度	要求内容	受信時刻	VPNNAT用IPアドレス	テーブル名	メンテナンス状態
1	FE001E	VAIO	211.0.4.3	山田	一般	0468xxx	緊急	…	17:23	10.0.0.03	VAIO	対応待ち

【図３０】

ＶＰＮＮＡＴＤＢ９１

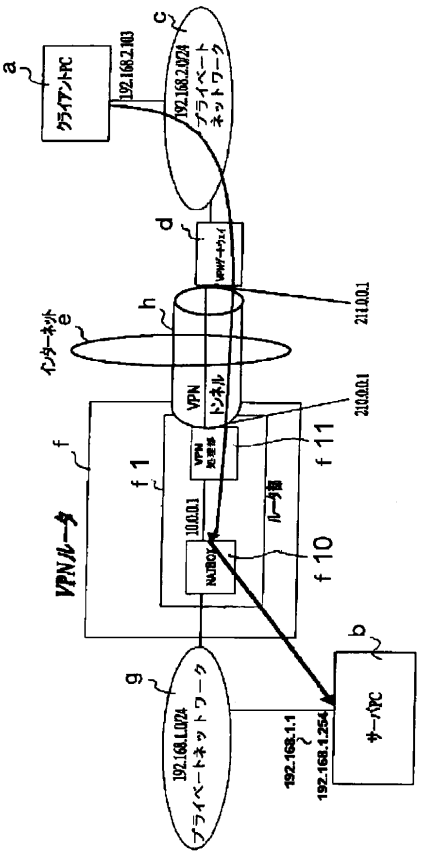
VPNNAT用IPアドレス	割り当て状況（端末ID	内線端末名）
10.0.0.01	FE001E	情流 GW サーバ部
10.0.0.02	FE001E	情流 GW サーバ部
10.0.0.03	FE001E	VAIO
～		
10.255.255.254	未使用	未使用

【図３１】

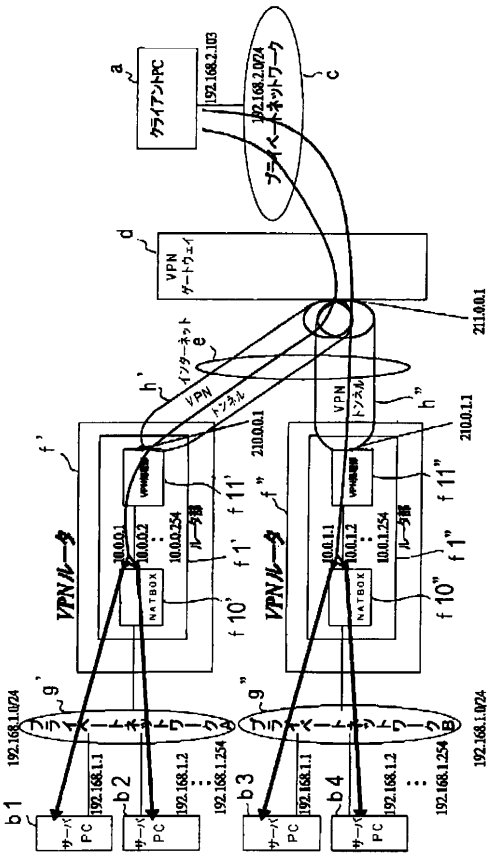
リモートメンテナンス要求ＤＢ　９２

受付番号	端末ＩＤ	内線端末名	グローバルIPアドレス	要求者名	要求者レベル	電話番号	緊急度	要求内容	受信時刻	VPNNAT用IPアドレス	テーブル名	メンテナンス状態
1	FE001E	VAIO	211.0.4.3	山田	一般	0468xxx	緊急	…	17:23	10.0.0.03	VAIO	終了

【図３２】



【図３３】


a
クライアントPC
192.168.2.103
c
プライベートネットワーク
192.168.2.0/24
d
VPN
ゲートウェイ
211.0.0.1
e
インターネット
h'
VPN
トンネル
h"
210.0.0.1
210.0.1.1
f'
f"
VPNルータ
10.0.0.1
10.0.0.2
10.0.0.254
10.0.1.1
10.0.1.2
10.0.1.254
ルータ
NATBOX
f 11'
f 1'
f 10'
f 11"
f 1"
f 10"
g'
g"
プライベートネットワーク
192.168.1.0/24
192.168.1.1
192.168.1.2
192.168.1.254
b1
b2
b3
b4
サーバPC

フロントページの続き

(56)参考文献 赤松康至, グローバルR＆Dのためのインフラ構築, OMRON TECHNICS, 日本, オムロン株式会社, １９９８年 9月２０日, Vol.38 No.3, pp.68-73
現実のものとなったＶｉｒｔｕａｌ Ｐｒｉｖａｔｅ Ｎｅｔｗｏｒｋ, 日経コミュニケーション, 日本, 日経ＢＰ社, １９９８年 9月２１日, 第２７８号, pp.20-23

(58)調査した分野(Int.Cl., ＤＢ名)
H04L 12/56
H04L 12/46