(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3764125号
(P3764125)
(45)発行日　平成18年4月5日(2006.4.5)　(24)登録日　平成18年1月27日(2006.1.27)

(51)Int.Cl.		F I		
H04L 12/66	(2006.01)	H04L	12/66	B
H04L 12/28	(2006.01)	H04L	12/28	300Z

請求項の数 10　(全 34 頁)

(21)出願番号　特願2002-125261(P2002-125261)
(22)出願日　平成14年4月26日(2002.4.26)
(65)公開番号　特開2003-318992(P2003-318992A)
(43)公開日　平成15年11月7日(2003.11.7)
審査請求日　平成15年12月24日(2003.12.24)

(73)特許権者　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(74)代理人　100092152
弁理士　服部　毅巖
(72)発明者　川合　守久
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　斎藤　武
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　大西　照彦
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
最終頁に続く

(54)【発明の名称】ゲートウェイ、通信端末装置、および通信制御プログラム

(57)【特許請求の範囲】
【請求項１】
無線ネットワークと他のネットワークとの間で送受信されるデータを中継するためのゲートウェイ側の通信制御プログラムにおいて、
コンピュータに、
前記無線ネットワーク上に、セキュリティ機能を有することを示すメッセージをブロードキャストで定期的に送信し、
前記メッセージを受信した通信端末装置からの要求に応じて前記通信端末装置との間で相互通信を行い、認証方式と互いに通信するデータの暗号化規則と復号規則とを決定し、前記認証方式に従い前記通信端末装置との間で互いを認証し、
前記通信端末装置宛のデータを前記暗号化規則に従って暗号化して前記無線ネットワーク経由で送信し、前記無線ネットワーク経由で前記通信端末装置から受信した暗号データを前記復号規則で復号する、
処理を実行させることを特徴とするゲートウェイ側の通信制御プログラム。
【請求項２】
無線ネットワークを経由して通信を行うための通信端末装置側の通信制御プログラムにおいて、
コンピュータに、
前記無線ネットワークによる通信可能範囲に入り、該無線ネットワークと他のネットワークとの間で送受信されるデータを中継するゲートウェイから、該ゲートウェイがセキュ

リティ機能を有することを示すメッセージがブロードキャストで送信されると、該メッセージを前記無線ネットワーク経由で受信し、セキュリティ機能を有するゲートウェイのアドレスを該メッセージから取得し、

取得した前記アドレスに基づき前記ゲートウェイとの間で相互通信を行い、認証方式と互いに通信するデータの暗号化規則と復号規則とを決定し、前記認証方式に従い前記ゲートウェイとの間で互いを認証し、

他のコンピュータ宛のデータを前記暗号化規則に従って暗号化して前記無線ネットワーク経由で前記ゲートウェイへ送信し、前記無線ネットワーク経由で前記ゲートウェイから受信した暗号データを前記復号規則で復号する、

処理を実行させることを特徴とする通信端末装置側の通信制御プログラム。

【請求項３】

前記ゲートウェイのアドレスを取得する際には、前記無線ネットワークに対して前記ゲートウェイがブロードキャストで定期的に送信しているメッセージから、前記アドレスを取得することを特徴とする請求項２記載の通信端末装置側の通信制御プログラム。

【請求項４】

前記ゲートウェイのアドレスを取得する際には、他のサーバから前記ゲートウェイのアドレスを取得することにより、前記通信端末装置と前記ゲートウェイとの間において相互通信を行い、前記認証方式と前記暗号化規則と復号規則とを自動的に決定することを特徴とする請求項２記載の通信端末装置側の通信制御プログラム。

【請求項５】

前記認証方式と前記暗号化規則と復号規則の決定は、前記アドレスの取得時において前記ゲートウェイのアドレス変更を検出した場合、前記ゲートウェイとの間において相互通信を行い、前記認証方式と前記暗号化規則と復号規則とを自動的に再決定することを特徴とする請求項４記載の通信端末装置側の通信制御プログラム。

【請求項６】

前記通信端末装置が複数の通信手段を有する場合、

予めどの通信手段が使用可能であるかを調べ、使用できる通信手段が複数あるときに、その優先順位を前記通信端末装置内に定義し、

前記通信端末装置にて、前記優先順位に従って通信手段を自動選択し、使用する通信手段以外を無効にして、使用する通信手段で前記ゲートウェイとの間において相互通信を行い、前記認証方式と前記暗号化規則と復号規則とを決定することを特徴とする請求項２記載の通信端末装置側の通信制御プログラム。

【請求項７】

無線ネットワークと他のネットワークとの間で送受信されるデータを中継するためのゲートウェイ側の通信制御方法において、

前記無線ネットワーク上に、セキュリティ機能を有することを示すメッセージをブロードキャストで定期的に送信し、

前記メッセージを受信した通信端末装置からの要求に応じて前記通信端末装置との間で相互通信を行い、認証方式と互いに通信するデータの暗号化規則と復号規則とを決定し、前記認証方式に従い前記通信端末装置との間で互いを認証し、

前記通信端末装置宛のデータを前記暗号化規則に従って暗号化して前記無線ネットワーク経由で送信し、前記無線ネットワーク経由で前記通信端末装置から受信した暗号データを前記復号規則で復号する、

ことを特徴とするゲートウェイ側の通信制御方法。

【請求項８】

無線ネットワークを経由して通信を行うための通信端末装置側の通信制御方法において、

前記無線ネットワークによる通信可能範囲に入り、該無線ネットワークと他のネットワークとの間で送受信されるデータを中継するゲートウェイから、該ゲートウェイがセキュリティ機能を有することを示すメッセージがブロードキャストで送信されると、該メッセ

ージを前記無線ネットワーク経由で受信し、セキュリティ機能を有するゲートウェイのアドレスを該メッセージから取得し、
取得した前記アドレスに基づき前記ゲートウェイとの間で相互通信を行い、認証方式と互いに通信するデータの暗号化規則と復号規則とを決定し、前記認証方式に従い前記ゲートウェイとの間で互いを認証し、
他のコンピュータ宛のデータを前記暗号化規則に従って暗号化して前記無線ネットワーク経由で前記ゲートウェイへ送信し、前記無線ネットワーク経由で前記ゲートウェイから受信した暗号データを前記復号規則で復号する、
ことを特徴とする通信端末装置側の通信制御方法。
【請求項９】
無線ネットワークと他のネットワークとの間で送受信されるデータを中継するためのゲートウェイにおいて、
前記無線ネットワーク上に、セキュリティ機能を有することを示すメッセージをブロードキャストで定期的に送信する接続確認部と、
前記メッセージを受信した通信端末装置からの要求に応じて前記通信端末装置との間で相互通信を行い、認証方式と互いに通信するデータの暗号化規則と復号規則とを決定し、前記認証方式に従い前記通信端末装置との間で互いを認証する通信経路自動確立部と、
前記通信端末装置宛のデータを前記暗号化規則に従って暗号化して前記無線ネットワーク経由で送信し、前記無線ネットワーク経由で前記通信端末装置から受信した暗号データを前記復号規則で復号する暗号化通信部と、
を有することを特徴とするゲートウェイ。
【請求項１０】
無線ネットワークを経由して通信を行うための通信端末装置において、
前記無線ネットワークによる通信可能範囲に入り、該無線ネットワークと他のネットワークとの間で送受信されるデータを中継するゲートウェイから、該ゲートウェイがセキュリティ機能を有することを示すメッセージがブロードキャストで送信されると、該メッセージを前記無線ネットワーク経由で受信し、セキュリティ機能を有するゲートウェイのアドレスを該メッセージから取得する受信データ処理部と、
取得した前記アドレスに基づき前記ゲートウェイとの間で相互通信を行い、認証方式と互いに通信するデータの暗号化規則と復号規則とを決定し、前記認証方式に従い前記ゲートウェイとの間で互いを認証する通信経路自動確立部と、
他のコンピュータ宛のデータを前記暗号化規則に従って暗号化して前記無線ネットワーク経由で前記ゲートウェイへ送信し、前記無線ネットワーク経由で前記ゲートウェイから受信した暗号データを前記復号規則で復号する暗号化通信部と、
を有することを特徴とする通信端末装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は無線を使用して通信制御を行うゲートウェイ、通信端末装置、および通信制御プログラムに関し、特にデータを送受信する移動可能な通信端末装置と、セキュリティ機能を持つゲートウェイとの間で通信制御を行うゲートウェイ、通信端末装置、および通信制御プログラムに関する。
【０００２】
【従来の技術】
近年ハードウェアベンダでは、無線LAN（Wireless Local Area Network）を始めとする無線通信インタフェースを内蔵した、移動する通信端末装置(ノート型PC（Personal Computer）やPDA(Personal Digital Assistant)など)を次々と出荷している。また、従来仕様を高速化したIEEE802.11aやIEEE802.11g（共に、無線LANの標準プロトコル）などをサポートした製品(アクセスポイントやPCカードなど)も登場し、無線通信技術は企業ネットワークのインフラとしての位置を獲得しつつある。

【０００３】
このような状況の中で、無線通信技術を企業ネットワークに導入することを考えた場合、セキュリティの確保が不可欠となる。例えば、無線LAN通信のセキュア化技術の主流であるWEP（Wired Equivalent Privacy）は、その脆弱さを露呈してきており，新たなソリューションの開発が望まれている。更に、無線通信を既存の有線による通信と比較した場合の特徴として、無線通信インタフェースを実装した通信端末装置は移動するということが挙げられる。
【０００４】
このため、無線通信技術を企業に導入する際のセキュリティを保つ手段として、従来は、無線ネットワークと既存の有線ネットワークとの間にセキュリティを確保するためのゲートウェイコンピュータを設置することが考えられる。また、通信端末装置が移動するということは、インターネットを介してのファイアウォール間、あるいは、クライアントとファイアウォール間におけるVPN（Virtual Private Network）通信と異なり、通信端末装置がセキュアな通信経路を確立する必要があるゲートウェイコンピュータが変化するということを意味する。
【０００５】
【発明が解決しようとする課題】
しかしながら、従来のような技術では、通信端末装置の移動に際し、ゲートウェイコンピュータが変化する度に通信環境の設定やシステムのリブートをユーザが手動操作で設定しなければならなかった。そのため、このような設定をユーザに強いるようでは通信端末装置本来の価値を失ってしまう。以下、このような点を具体的に示す。
【０００６】
（１）通信端末装置のサブネットを跨いだ移動に伴い、ゲートウェイコンピュータのアドレスは変化する。この場合、通信端末装置がゲートウェイコンピュータのアドレスを更新し、セキュア（安全）な通信経路を確立するためには、OSのリブートや手動による通信環境の再設定が必要となる。
【０００７】
（２）通信端末装置がゲートウェイコンピュータのサービスエリアから離れた場合、サービスエリアから離れたことを迅速に検出する手段がないため、ユーザはリカバリ処理に時間を要する。
【０００８】
（３）複数の通信インタフェースを実装している通信端末装置において、有効／無効にするインタフェースを決定する手段が無いため、ユーザは状況に適したインタフェースの選択ができない。また、通信にオーバヘッドが生じる。さらに、有効なインタフェースの選択や、セキュアな通信経路の確立には、ユーザは手動による通信環境の設定が必要となる。
【０００９】
本発明はこのような点に鑑みてなされたものであり、セキュリティを保ちつつ、ゲートウェイコンピュータ毎の通信設定やセキュアな通信経路の確保などを自動化することができる通信制御方法、ゲートウェイ、通信端末装置、および通信制御プログラムの提供を目的とする。
【００１０】
【課題を解決するための手段】
本発明では上記課題を解決するために、図１に示すようなゲートウェイ側の通信制御プログラムが提供される。本発明のゲートウェイ側の通信制御プログラムは、無線ネットワークと他のネットワークとの間で送受信されるデータを中継する場合に適用される。
【００１１】
本発明では、前記無線ネットワーク上に、セキュリティ機能を有することを示すメッセージを、ブロードキャストで定期的に送信する（ステップＳ１）。また、前記メッセージを受信した通信端末装置からの要求に応じて前記通信端末装置との間で相互通信を行い、

認証方式と互いに通信するデータの暗号化規則と復号規則とを決定し、前記認証方式に従い前記通信端末装置との間で互いを認証する（ステップＳ３）。そして、前記通信端末装置宛のデータを前記暗号化規則に従って暗号化して前記無線ネットワーク経由で送信し、前記無線ネットワーク経由で前記通信端末装置から受信した暗号データを前記復号規則で復号する（ステップＳ４）。すなわち、ゲートウェイコンピュータ３０は、無線ネットワーク上に、セキュリティ機能を有することを示すメッセージを、通信端末装置１０に対してブロードキャストで一定時間間隔に送信する。また、ゲートウェイコンピュータ３０は、メッセージを受信した通信端末装置１０からの要求に応じて通信端末装置１０との間で相互通信を行い、認証方式と互いに通信するデータの暗号化規則と復号規則とを決定し、この認証方式に従い互いを認証することでセキュアな通信経路を確立する。そして、ゲートウェイコンピュータ３０は、通信端末装置１０宛のデータを暗号化規則に従って暗号化して無線ネットワーク経由で通信端末装置１０に対して送信する。逆に、ゲートウェイコンピュータ３０は、無線ネットワーク経由で通信端末装置１０から受信した別の暗号データを、復号規則で復号することでデータ通信を行う。

【００１２】

このようなゲートウェイ側の通信制御プログラムによれば、ゲートウェイコンピュータ３０により、無線ネットワーク上に、セキュリティ機能を有することを示すメッセージが、通信端末装置１０に対してブロードキャストで一定時間間隔に送信される。また、ゲートウェイコンピュータ３０により、メッセージを受信した通信端末装置１０からの要求に応じて通信端末装置１０との間で相互通信が行われ、認証方式と互いに通信するデータの暗号化規則と復号規則とが決定され、互いを認証することでセキュアな通信経路が確立される。そして、ゲートウェイコンピュータ３０により、通信端末装置１０宛のデータが暗号化規則に従って暗号化されて無線ネットワーク経由で通信端末装置１０へ送信される。逆に、ゲートウェイコンピュータ３０により、無線ネットワーク経由で通信端末装置１０から受信した別の暗号データが、復号規則で復号されることでデータ通信が行われる。

【００１３】

また、上記課題を解決するために、図１に示すような通信端末装置側の通信制御プログラムが提供される。本発明の通信端末装置側の通信制御プログラムは、無線ネットワークを経由してデータ通信を行う場合に適用される。

【００１４】

本発明では、前記無線ネットワークによる通信可能範囲に入ると、前記無線ネットワーク経由で、セキュリティ機能を有するゲートウェイのアドレスを取得する（ステップＳ２）。また、取得した前記アドレスに基づき前記ゲートウェイとの間で相互通信を行い、認証方式と互いに通信するデータの暗号化規則と復号規則とを決定し、前記認証方式に従い前記ゲートウェイとの間で互いを認証する（ステップＳ３）。そして、他のコンピュータ宛のデータを前記暗号化規則に従って暗号化して前記無線ネットワーク経由で前記ゲートウェイへ送信し、前記無線ネットワーク経由で前記ゲートウェイから受信した暗号データを前記復号規則で復号する（ステップＳ４）。すなわち、通信端末装置１０は、無線ネットワークによる通信可能範囲に入ると、無線ネットワーク経由で、セキュリティ機能を有するゲートウェイコンピュータ３０のアドレスを取得する。また、通信端末装置１０は、取得したアドレスに基づきゲートウェイコンピュータ３０との間で相互通信を行い、認証方式と互いに通信するデータの暗号化規則と復号規則とを決定し、この認証方式に従い互いを認証することでセキュアな通信経路を確立する。そして、通信端末装置１０は、他のコンピュータ宛のデータを暗号化規則に従って暗号化して無線ネットワーク経由でゲートウェイコンピュータ３０へ送信する。逆に、通信端末装置１０は、無線ネットワーク経由でゲートウェイコンピュータ３０から受信した別の暗号データを、復号規則で復号することでデータ通信を行う。

【００１５】

このような通信端末装置側の通信制御プログラムによれば、通信端末装置１０が無線ネットワークによる通信可能範囲に入ると、通信端末装置１０により、無線ネットワーク経

由でセキュリティ機能を有するゲートウェイコンピュータ３０のアドレスが取得される。また、通信端末装置１０により、取得したアドレスに基づきゲートウェイコンピュータ３０との間で相互通信が行われ、認証方式と互いに通信するデータの暗号化規則と復号規則とが決定され、互いを認証する。そして、通信端末装置１０により、他のコンピュータ宛のデータが暗号化規則に従って暗号化されて、無線ネットワーク経由でゲートウェイコンピュータ３０へ送信される。逆に、通信端末装置１０により、無線ネットワーク経由でゲートウェイコンピュータ３０から受信した別の暗号データが、復号規則で復号されることでデータ通信が行われる。

【００１６】

その結果、セキュリティを保ちつつ、ゲートウェイコンピュータ毎の通信設定やセキュアな通信経路の確保などを自動化することができ、ゲートウェイコンピュータの変化にともなうユーザ設定項目を減らし、ユーザの負担を軽減することが可能となる。

【００１７】

【発明の実施の形態】

以下、本発明の実施の形態を図面を参照して説明する。

図１は、本発明の原理構成図である。本発明に係わるゲートウェイ側の通信制御プログラムは、無線ネットワークと他のネットワークとの間で送受信されるデータを中継する場合に適用される。また、本発明の通信端末装置側の通信制御プログラムは、無線ネットワークを経由してデータ通信を行う場合に適用される。以下、これらの２つのプログラムの手順をステップ番号に沿って、組み合わせて説明する。

【００１８】

図１によると、本発明では、無線ネットワークを経由してデータ通信を行う通信端末装置１０と、無線ネットワークと他のネットワークとの間で送受信されるデータを中継するゲートウェイ（以下、ゲートウェイコンピュータと称する）３０との間においてデータ通信を行う手順を示している。

【００１９】

まず、ゲートウェイコンピュータ３０は、無線ネットワーク上に、セキュリティ機能を有することを示すメッセージを、通信端末装置１０に対してブロードキャストで一定時間間隔に送信する（ステップＳ１）。

【００２０】

次に、通信端末装置１０は、無線ネットワークによる通信可能範囲に入ると、無線ネットワーク経由で、セキュリティ機能を有するゲートウェイコンピュータ３０のアドレスを取得する（ステップＳ２）。また、通信端末装置１０は、取得したアドレスに基づきゲートウェイコンピュータ３０との間で相互通信を行い、認証方式と互いに通信するデータの暗号化規則と復号規則とを決定する（以下、暗号化規則と復号規則の決定、あるいは相互認証等のセキュア化技術を総じて、セキュアな通信経路の確立と定義する）。一方、ゲートウェイコンピュータ３０は、メッセージを受信した通信端末装置１０からの要求に応じて通信端末装置１０との間で相互通信を行い、互いに通信するデータのセキュアな通信経路を確立する（ステップＳ３）。

【００２１】

そして、ゲートウェイコンピュータ３０は、通信端末装置１０宛のデータを暗号化規則に従って暗号化して無線ネットワーク経由で通信端末装置１０に対して送信する。また、ゲートウェイコンピュータ３０は、無線ネットワーク経由で通信端末装置１０から受信した別の暗号データを復号規則で復号することでデータ通信を行う。一方、通信端末装置１０は、他のコンピュータ宛のデータを暗号化規則に従って暗号化して無線ネットワーク経由でゲートウェイコンピュータ３０へ送信する。また、通信端末装置１０は、無線ネットワーク経由でゲートウェイコンピュータ３０から受信した別の暗号データを、復号規則で復号することでデータ通信を行う（ステップＳ４）。

【００２２】

このように本発明では、ゲートウェイコンピュータ３０により、無線ネットワーク上に

、セキュリティ機能を有することを示すメッセージが、通信端末装置１０に対してブロードキャストで一定時間間隔に送信される。

【００２３】

また、通信端末装置１０が無線ネットワークによる通信可能範囲に入ると、この通信端末装置１０により、無線ネットワーク経由で、セキュリティ機能を有するゲートウェイコンピュータ３０のアドレスが取得される。また、通信端末装置１０により、取得したアドレスに基づきゲートウェイコンピュータ３０との間で相互通信が行われ、互いに通信するデータのセキュアな通信経路が確立される。一方、ゲートウェイコンピュータ３０により、メッセージを受信した通信端末装置１０からの要求に応じて通信端末装置１０との間で相互通信が行われ、互いに通信するデータのセキュアな通信経路が確立される。

【００２４】

そして、ゲートウェイコンピュータ３０により、通信端末装置１０宛のデータが暗号化規則に従って暗号化されて、無線ネットワーク経由で通信端末装置１０に対して送信される。また、ゲートウェイコンピュータ３０により、無線ネットワーク経由で通信端末装置１０から受信した別の暗号データが、復号規則で復号されることでデータ通信が行われる。一方、通信端末装置１０により、他のコンピュータ宛のデータが暗号化規則に従って暗号化されて、無線ネットワーク経由でゲートウェイコンピュータ３０へ送信される。また、通信端末装置１０により、無線ネットワーク経由でゲートウェイコンピュータ３０から受信した別の暗号データが、復号規則で復号されることでデータ通信が行われる。

【００２５】

これにより、セキュリティを保ちつつ、ゲートウェイコンピュータ毎の通信設定やセキュアな通信経路の確保などを自動化することができ、ゲートウェイコンピュータの変化にともなうユーザ設定項目を減らし、ユーザの負担を軽減することが可能となる。

【００２６】

以下に、本発明の実施の形態について具体的に説明する。

まず、本発明の実施の形態を適用したシステムについて、図２を参照して説明する。

【００２７】

図２は、本発明の実施の形態を適用したシステム構成図である。なお、以下の実施の形態は、ＩＰ（Internet Protocol）による通信システムに本発明を適用したものである。

【００２８】

本発明の実施の形態は、無線通信インタフェースを有する通信端末装置１０ａ～１０ｆ、無線通信インタフェースを有する複数のＬＡＮノード（中継装置２０ａ，アクセスポイント２０ｂ）、セキュリティ機能を実装したゲートウェイコンピュータ３０ａ、および、各装置のＩＰアドレスを動的に割り当てるＤＨＣＰサーバ４０から構成されるＬＡＮシステムにおいて適用される。このＬＡＮシステムは、ゲートウェイコンピュータ３０ａにより全体のネットワークが論理的に分断され、サブネットＡが構成されている。このサブネットＡは、ゲートウェイコンピュータ３０ａの管理配下のネットワークである。また、サブネットＢは、他のゲートウェイコンピュータの管理配下のネットワークである。なお、通信端末装置１０のＩＰアドレスは、固定ではなくＤＨＣＰ（Dynamic Host Configuration Protocol）サーバにより動的に割り当てられる。また、通信端末装置１０のＩＰアドレスは、ＰＰＰ（Point-to-Point Protocol）プロトコルのＩＰＣＰ（Internet Protocol Control Protocol）機能をもったリモート・アクセス・サーバ（Remote Access Server）などにより自動的に割り当てられる。ここで、サブネットＡ内には、中継装置２０ａ、アクセスポイント２０ｂ、通信端末装置１０ｅ、および通信端末装置１０ｆが存在し、それらがＬＡＮ９０ａを介してゲートウェイコンピュータ３０ａに接続され、且つサブネット固有のセキュアな通信経路が確立されている。なお、ＬＡＮ（Local Area Network）９０ａは、複数のコンピュータが互いに通信可能な有線通信手段であればどのようなものでもよい。

【００２９】

通信端末装置１０ａ及び通信端末装置１０ｂは、ＷＡＮ９０ｂに接続されており、サブ

ネットＡあるいは他のサブネット内にあるコンピュータとデータ通信を行う。また、データ通信を行うための通信経路確立の際、通信端末装置１０ａ及び通信端末装置１０ｂは、ゲートウェイコンピュータ３０ａから一定時間間隔に通知されるセキュアな通信を行うためのメッセージを受信して、セキュアな通信経路確立を動的に行う。なお、ＷＡＮ（Wide Area Network）９０ｂは、中継装置２０ａが遠隔地のコンピュータとの間においてデータ通信が可能であればどのようなものでもよい。また、通信端末装置１０ａ及び通信端末装置１０ｂの詳細については、図３にて後述する。

【００３０】

通信端末装置１０ｃ及び通信端末装置１０ｄは、無線ＬＡＮ９０ｃに接続されており、サブネットＡあるいは他のサブネット内にあるコンピュータとデータ通信を行う。また、データ通信を行うための通信経路確立の際、通信端末装置１０ｃ及び通信端末装置１０ｄは、ゲートウェイコンピュータ３０ａから一定時間間隔に通知されるセキュアな通信を行うためのメッセージを受信して、セキュアな通信経路確立を動的に行う。なお、無線ＬＡＮ９０ｃは、アクセスポイント２０ｂが無線により接続されたコンピュータとの間においてデータ通信が可能であればどのようなものでもよい。また、通信端末装置１０ｃ及び通信端末装置１０ｄの詳細については、図３にて後述する。

【００３１】

通信端末装置１０ｅ及び通信端末装置１０ｆは、ＬＡＮ９０ａに接続されており、サブネットＡあるいは他のサブネット内にあるコンピュータとデータ通信を行う。また、データ通信を行うための通信経路確立の際、通信端末装置１０ｅ及び通信端末装置１０ｆは、ゲートウェイコンピュータ３０ａから一定時間間隔に通知されるセキュアな通信を行うためのメッセージを受信して、セキュアな通信経路確立を動的に行う。なお、通信端末装置１０ｅ及び通信端末装置１０ｆの詳細については、図３にて後述する。

【００３２】

中継装置２０ａは、ゲートウェイコンピュータ３０ａとＷＡＮ９０ｂに接続されており、通信端末装置１０ａ又は通信端末装置１０ｂとゲートウェイコンピュータ３０ａとのデータ通信を中継する。なお、中継装置２０ａは、２つのネットワークを接続するブリッジやスイッチとして機能すればどのようなものでもよく、例えばルータ（router）やリモート・アクセス・サーバなどである。

【００３３】

アクセスポイント２０ｂは、ゲートウェイコンピュータ３０ａと無線ＬＡＮ９０ｃに接続されており、通信端末装置１０ｃ又は通信端末装置１０ｄとゲートウェイコンピュータ３０ａとのデータ通信を中継する。なお、中継装置２０ａは、２つのネットワークを接続するブリッジとして機能すればどのようなものでもよい。

【００３４】

ゲートウェイコンピュータ３０ａは、中継装置２０ａ、アクセスポイント２０ｂ、通信端末装置１０ｅ、および通信端末装置１０ｆにＬＡＮ９０ａを介して接続されており、サブネットＡ内のコンピュータ同士、ならびに、サブネットＡ内のコンピュータと他のサブネット内のコンピュータとのデータ通信を中継する。また、ゲートウェイコンピュータ３０ａは、セキュアな通信経路確立のためのメッセージをサブネットＡ内のコンピュータへ一定時間間隔で通知する。なお、ゲートウェイコンピュータ３０ａの詳細については、図４にて後述する。

【００３５】

ＤＨＣＰサーバ４０は、サブネットＡ内の各装置に接続されており、各装置のＩＰアドレスを動的に割り当てる。

このような構成によると、例えば、ゲートウェイコンピュータ３０ａにより、無線ＬＡＮ９０ｃ上に、セキュリティ機能を有することを示すメッセージが、通信端末装置１０ｃに対してブロードキャストで一定時間間隔に送信される。また、ゲートウェイコンピュータ３０ａにより、メッセージを受信した通信端末装置１０ｃからの要求に応じて通信端末装置１０ｃとの間で相互通信が行われ、互いに通信するデータのセキュアな通信経路が確

立される。そして、ゲートウェイコンピュータ３０ａにより、通信端末装置１０ｃ宛のデータが暗号化規則に従って暗号化されて無線ＬＡＮ９０ｃ経由で通信端末装置１０ｃへ送信される。逆に、ゲートウェイコンピュータ３０ａにより、無線ＬＡＮ９０ｃ経由で通信端末装置１０ｃから受信した別の暗号データが、復号規則で復号されることでデータ通信が行われる。

【００３６】

一方、通信端末装置１０ｃにより、無線ＬＡＮ９０ｃ経由でセキュリティ機能を有するゲートウェイコンピュータ３０ａのアドレスが取得される。また、通信端末装置１０ｃにより、取得したアドレスに基づきゲートウェイコンピュータ３０ａとの間で相互通信が行われ、互いに通信するデータのセキュアな通信経路が確立される。そして、通信端末装置１０ｃにより、他のコンピュータ（例えばサーバコンピュータ）宛のデータが、暗号化規則に従って暗号化されて無線ＬＡＮ９０ｃ経由でゲートウェイコンピュータ３０ａへ送信される。逆に、通信端末装置１０ｃにより、無線ＬＡＮ９０ｃ経由でゲートウェイコンピュータ３０ａから受信した他のコンピュータ（例えばサーバコンピュータ）からの別の暗号データが、復号規則で復号されることでデータ通信が行われる。

【００３７】

これにより、セキュリティを保ちつつ、セキュアな通信経路の確保などを自動化することができる。

次に、本発明の実施の形態における通信端末装置１０の機能構成について、図３を参照して具体的に説明する。

【００３８】

図３は、本発明の実施の形態における通信端末装置の機能ブロック図である。

図３によると、通信端末装置１０は、セキュアな通信経路自動確立あるいは通信経路手動確立の選択を行うサービス選択部１１、通信デバイスの優先順位による自動選択を行う通信デバイス選択部１２、データ通信を行うためのセキュアな通信経路の自動確立を行うセキュアな通信経路自動確立部１３、データを送信するデータ送信部１４、他のコンピュータとの間で暗号データの送受信を行う暗号化通信部１５、メッセージＤ３１と通常データＤ３３と復号されたデータとを受信するデータ受信部１６、受信したデータの種別に対応した処理を行う受信データ処理部１７、データ通信を行うための通信経路を手動により確立する通信経路手動確立部１８、ゲートウェイコンピュータ３０のアドレス等の情報を格納するクライアント側管理テーブルＭ１０、および、現在時刻を計時するタイマＴ１０から構成されている。

【００３９】

サービス選択部１１は、通信デバイス選択部１２と通信経路手動確立部１８に接続されており、セキュアな通信経路自動確立あるいは通信経路手動確立の選択を行う。ここで、サービス選択部１１は、電源投入、サービスエリアからの離脱、通信断、あるいは予め決められた任意のタイミングを契機に動作する。このサービス選択部１１は、例えば電源投入等が行われると、サービス（セキュアな通信経路自動確立）の開始を選択するようにユーザへ促す。そして、ユーザがサービス（セキュアな通信経路自動確立）の開始を選択した場合、通信デバイス選択部１２へ制御を移行する。一方、ユーザがサービス（通信経路手動確立）を選択した場合、通信経路手動確立部１８へ制御を移行する。

【００４０】

通信デバイス選択部１２は、サービス選択部１１とセキュアな通信経路自動確立部１３に接続されており、通信デバイスの優先順位による自動選択を行う。ここで、通信デバイス選択部１２は、優先順位テーブル（後述）において、最も高い優先順位が設定された通信デバイスを検索する。さらに、通信デバイス選択部１２は、検索した結果、通信デバイスが見つかったかどうかを判定する。そして、通信可能な通信デバイスが存在した場合、セキュアな通信経路自動確立部１３へ制御を移行する。一方、通信可能な通信デバイスが存在しない場合、全ての通信デバイスが使用不能であることをＴＣＰ／ＩＰ層の管理機能へ通知する。この通知により、通信端末装置１０は、ＴＣＰ／ＩＰプロトコルを使用して

いるアプリケーションソフトウェアに通信エラーを認識させることができる。なお、通信デバイス選択部１２の詳細は後述する。

【００４１】

セキュアな通信経路自動確立部１３は、通信デバイス選択部１２、データ送信部１４、受信データ処理部１７、およびクライアント側管理テーブルＭ１０に接続されており、データ通信を行うための通信経路の自動確立を行う。ここで、セキュアな通信経路自動確立部１３は、クライアント側管理テーブルＭ１０のゲートウェイコンピュータ３０のアドレスを取得して、セキュアプロトコル層において、ゲートウェイコンピュータとの間にセキュリティプロトコル（セキュアな通信経路）の確立シーケンスを実行する。そして、セキュアな通信経路の確立後に、セキュアな通信経路自動確立部１３は、データ送信部１４へ制御を移行するとともにセキュアな通信経路が確立したことを知らせる。

【００４２】

データ送信部１４は、セキュアな通信経路自動確立部１３、暗号化通信部１５、および通信経路手動確立部１８に接続されており、所定のデータを送信する。ここで、データ送信部１４は、ＴＣＰ／ＩＰ層において、ユーザから指定されたデータを送信するため、このデータを暗号化通信部１５へ渡す。一方、暗号化する必要がない場合には、そのデータを通常データＤ１３として、ネットワーク上に送信する。

【００４３】

暗号化通信部１５は、データ送信部１４とデータ受信部１６に接続されており、他のコンピュータとの間で暗号データの送受信を行う。ここで、暗号化通信部１５は、セキュアプロトコル層において、データ送信部１４から渡されたデータを暗号化して、暗号データＤ１２をゲートウェイコンピュータ３０に対して送信する。一方、暗号化通信部１５は、セキュアプロトコル層において、ゲートウェイコンピュータ３０から送信された暗号データＤ３２を受信すると、暗号データＤ３２を復号して、そのデータをデータ受信部１６へ渡す。

【００４４】

データ受信部１６は、暗号化通信部１５と受信データ処理部１７に接続されており、メッセージＤ３１と通常データＤ３３と復号されたデータとを受信する。ここで、データ受信部１６は、ＴＣＰ／ＩＰ層において、暗号化通信部１５から渡されたデータを受信して、受信データ処理部１７へ渡す。また、データ受信部１６は、ＴＣＰ／ＩＰ層において、ゲートウェイコンピュータ３０からのメッセージＤ３１を受信する。そして、データ受信部１６は、受信したメッセージＤ３１を受信データ処理部１７へ渡す。なお、通信端末装置１０は、ゲートウェイコンピュータ３０のＩＰアドレスを要求する際に、自身のＩＰアドレスもＤＨＣＰプロトコルによりＤＨＣＰサーバ４０から再取得することが可能である。この場合、通信端末装置１０がＤＨＣＰサーバ４０に対してゲートウェイコンピュータ３０のＩＰアドレスを要求した後、データ受信部１６では、ＤＨＣＰサーバ４０からのＩＰアドレスを受信し、受信データ処理部１７へ渡す。

【００４５】

受信データ処理部１７は、通信経路自動確立部１３、データ受信部１６、クライアント側管理テーブルＭ１０、およびタイマＴ１０に接続されており、受信したデータの種別に対応した処理を行う。ここで、受信データ処理部１７は、ゲートウェイコンピュータ３０からセキュアな通信を行うためのメッセージＤ３１を受信すると、メッセージＤ３１に含まれるアドレスを、通信端末装置１０との間でセキュリティ通信を行う対向ノードと見なしクライアント側管理テーブルＭ１０に格納（設定）する。その際、受信データ処理部１７は、セキュアな通信経路自動確立部１３へ制御を移行するとともにメッセージＤ３１を正常に受信処理したことを知らせる。

【００４６】

また、受信データ処理部１７は、新旧メッセージ（ＩＰアドレス）の比較も行う。この受信データ処理部１７は、ゲートウェイコンピュータ３０からのメッセージＤ３１を新たに受信すると、以前に受信した、送信元が旧ゲートウェイコンピュータであるメッセージ

（ＩＰアドレス）を、クライアント側管理テーブルＭ１０から取得する。さらに、通信端末装置１０が別のサブネットへ移動した場合、受信データ処理部１７は、取得した、送信元が旧ゲートウェイコンピュータであるメッセージ（ＩＰアドレス）と、新たに受信した新ゲートウェイコンピュータのメッセージＤ３１（ＩＰアドレス）とを比較して、送信元が異なることを検出する。そして、受信データ処理部１７は、送信元が異なることが検出されたので、以前とは異なるサブネットに接続したと判断し、クライアント側管理テーブルＭ１０に送信元ＩＰアドレスを格納する。以後、通信端末装置１０からの通信は、その新ゲートウェイコンピュータを介して行なう。

【００４７】

さらに、受信データ処理部１７は接続状態も監視する。この受信データ処理部１７は、メッセージＤ３１を受け取ると同時にタイマＴ１０から現在時刻を取得する。また、受信データ処理部１７は、取得した現在時刻をクライアント側管理テーブルＭ１０へ格納する。さらに、受信データ処理部１７は、現在時刻を格納すると同時にタイマカウンタをリセット（規定値をセット）する。以後、タイマＴ１０からの現在時刻をもとにタイマカウンタをカウントダウンしていく。つまり、受信データ処理部１７は、一定時間毎に受信されるゲートウェイコンピュータ３０からのメッセージを監視している。そして、受信データ処理部１７は、カウントダウンしたタイマカウンタが、一定時間経過して“０”となった場合、ゲートウェイコンピュータ３０管理配下のネットワーク離脱と判断する。すなわち、一定時間メッセージＤ３１が受信できなかったので、通信端末装置１０は、アクセスポイントのサービスエリア圏外（サポートエリアから離脱）であると判断する。あるいは、通信端末装置１０とアクセスポイントとの間の回線は、切断されたと判断する。この結果、受信データ処理部１７は、通信端末装置１０がネットワークの離脱と判断されたので、ネットワークが切り離され使用不能となったことをＴＣＰ／ＩＰ層を利用しているアプリケーションソフトウェア等に通知する。

【００４８】

そして、受信データ処理部１７は、通信デバイスのネットワーク接続可否の確認も行う。まず、通信デバイス選択部１２にて新たに通信デバイスが選択された場合、受信データ処理部１７は、この通信デバイスにおいて、ゲートウェイコンピュータ３０からのメッセージＤ３１の受信を一定時間待ち合わせる。次に、待ち合わせた結果をもとに、受信データ処理部１７は、メッセージＤ３１が受信できたかどうかを判定する。ここでメッセージＤ３１が受信できれば、当該通信デバイスが使用可能であること、及びそれ以外の通信デバイスが使用不能であることを、ＴＣＰ／ＩＰ層やセキュアプロトコル層を使用する通信経路自動確立部１３、データ送信部１４、あるいは他のアプリケーションソフトウェアへ通知する。一方、ここでメッセージＤ３１が受信できなければ、当該通信デバイスが使用できないと判断し、通信デバイス選択部１２に制御を移行する。

【００４９】

通信経路手動確立部１８は、サービス選択部１１とデータ送信部１４に接続されており、データ通信を行うための通信経路を手動により確立する。ここで、通信経路手動確立部１８は、サービス選択部１１により通信経路手動確立処理が選択されると、ユーザからの操作入力に応答して通信経路の確立を行い、データ送信部１４へ通信経路手動確立処理であることを通知する。

【００５０】

クライアント側管理テーブルＭ１０は、セキュアな通信経路自動確立部１３と受信データ処理部１７に接続されており、ゲートウェイコンピュータ３０のアドレス等の情報を格納する。ここで、クライアント側管理テーブルＭ１０には、受信データ処理部１７により受信したメッセージＤ３１、暗号データＤ３２を復号したデータ、あるいは通常データＤ３３が格納される。また、クライアント側管理テーブルＭ１０からは、セキュアな通信経路自動確立部１３や受信データ処理部１７によりゲートウェイコンピュータ３０のアドレスが取得される。なお、クライアント側管理テーブルＭ１０の詳細については、図９及び図１０にて後述する。

【００５１】
このような構成によると、サービス選択部１１により、セキュアな通信経路自動確立あるいは通信経路手動確立の選択が行われる。この選択でセキュアな通信経路自動確立処理が指定されると、通信デバイス選択部１２により、通信デバイスの優先順位による自動選択が行われる。通信デバイスが自動選択されると、セキュアな通信経路自動確立部１３により、データ通信を行うための通信経路の自動確立が行われる。通信経路が確立すると、データ送信部１４は、所定のデータを送信する。また、この所定のデータは、暗号化通信部１５により、他のコンピュータとの間で暗号データとして送受信される。
【００５２】
一方、受信側では、データ受信部１６により、メッセージＤ３１と通常データＤ３３と復号されたデータとが受信される。この受信されたデータをもとに、受信データ処理部１７により、受信したデータの種別に対応した処理が行われる。
【００５３】
また、サービス選択部１１で通信経路手動確立処理が指定されると、通信経路手動確立部１８により、データ通信を行うための通信経路が手動により確立される。
【００５４】
これにより、セキュリティを保ちつつ、セキュアな通信経路の確保などを自動化することができる。
次に、本発明の実施の形態におけるゲートウェイコンピュータ３０の機能構成について、図４を参照して具体的に説明する。
【００５５】
図４は、本発明の実施の形態におけるゲートウェイコンピュータの機能ブロック図である。
図４によると、ゲートウェイコンピュータ３０は、一定時間間隔でメッセージＤ３１を送信する接続確認部３１、データ通信を行うためのセキュアな通信経路の自動確立を行うセキュアな通信経路自動確立部３２、データを送信するデータ送信部３３、他のコンピュータとの間で暗号データの送受信を行う暗号化通信部３４、メッセージＤ１１と通常データＤ１３と復号されたデータとを受信するデータ受信部３５、受信したデータの種別に対応した処理を行う受信データ処理部３６、通信端末装置１０のアドレス等の情報を格納するゲートウェイコンピュータ側管理テーブルＭ３０、および、現在時刻を計時するタイマＴ３０から構成されている。
【００５６】
接続確認部３１は、タイマＴ３０に接続されており、一定時間間隔でメッセージＤ３１をネットワーク内へ送信する。ここで、例えばゲートウェイコンピュータ３０に電源投入等がされると、接続確認部３１は、サブネット全体に対し、一定時間間隔でメッセージＤ３１をIPブロードキャストで送信する。
【００５７】
セキュアな通信経路自動確立部３２は、受信データ処理部３６とゲートウェイコンピュータ側管理テーブルＭ３０に接続されており、データ通信を行うためのセキュアな通信経路の自動確立を行う。ここで、セキュアな通信経路自動確立部３２は、ゲートウェイコンピュータ側管理テーブルＭ３０の通信端末装置１０のアドレスを取得して、セキュアプロトコル層において、通信端末装置１０との間にセキュリティプロトコル（セキュアな通信経路）の確立シーケンスを実行する。そして、セキュアな通信経路の確立後に、セキュアな通信経路自動確立部３２は、データ送信部３３へ制御を移行するとともにセキュアな通信経路が確立したことを知らせる。
【００５８】
データ送信部３３は、暗号化通信部３４と受信データ処理部３６に接続されており、所定のデータを送信する。ここで、データ送信部３３は、ＴＣＰ／ＩＰ層において、受信データ処理部３６から渡されたデータを対向するコンピュータに対して中継するため、そのデータを暗号化通信部３４へ渡す。一方、暗号化する必要がない場合には、そのデータを

通常データＤ３３として、ネットワーク上に送信する。

【００５９】

暗号化通信部３４は、データ送信部３３とデータ受信部３５に接続されており、他のコンピュータとの間で暗号データの送受信を行う。ここで、暗号化通信部３４は、セキュアプロトコル層において、通信端末装置１０から送信された暗号データＤ１２を受信して復号し、この復号したデータをデータ受信部３５へ渡す。また、暗号化通信部３４は、セキュアプロトコル層において、データ送信部３３により渡されたデータを、暗号化して暗号データＤ３２として対向するコンピュータへ送信する。

【００６０】

データ受信部３５は、受信データ処理部３６に接続されており、メッセージＤ１１と通常データＤ１３と復号されたデータとを受信する。ここで、データ受信部３５は、暗号化通信部３４から渡されたデータを受信データ処理部３６へ渡す。また、通信端末装置１０からのメッセージＤ１１又は通常データＤ１３を受信し、受信データ処理部３６へ渡す。

【００６１】

受信データ処理部３６は、セキュアな通信経路自動確立部３２、データ送信部３３、データ受信部３５、およびゲートウェイコンピュータ側管理テーブルＭ３０に接続されており、受信したデータの種別に対応した処理を行う。ここで、受信データ処理部３６では、データ受信部３５から渡されたデータを他のコンピュータへ中継するためにデータ送信部３３へ渡す。また、受信データ処理部３６は、通信端末装置１０からセキュアな通信を行うためのメッセージＤ１１を受信すると、メッセージＤ１１に含まれるアドレスと認証・暗号化情報とをゲートウェイコンピュータ側管理テーブルＭ３０に格納する。その際、受信データ処理部３６は、セキュアな通信経路自動確立部３２へ制御を移行するとともに、メッセージＤ１１を正常に受信処理したことを知らせる。

【００６２】

ゲートウェイコンピュータ側管理テーブルＭ３０は、セキュアな通信経路自動確立部３２と受信データ処理部３６に接続されており、通信端末装置１０のアドレス等の情報を格納する。ここで、ゲートウェイコンピュータ側管理テーブルＭ３０には、受信されたメッセージＤ１１もしくは通常データＤ１３、あるいは暗号化通信部３４で復号されたデータが、受信データ処理部３６により格納される。また、ゲートウェイコンピュータ側管理テーブルＭ３０からは、セキュアな通信経路自動確立部３２により通信端末装置１０のアドレスが取得される。なお、ゲートウェイコンピュータ側管理テーブルＭ３０の詳細については、図１１にて後述する。

【００６３】

このような構成によると、接続確認部３１により、一定時間間隔でメッセージＤ３１がネットワーク内へ送信される。対向する通信端末装置１０から通信経路の確立要求があると、セキュアな通信経路自動確立部３２により、データ通信を行うための通信経路の自動確立が行われる。受信データ処理部３６からデータが渡されると、データ送信部３３により、所定のデータが中継送信される。そして、暗号化の必要があれば、暗号化通信部３４により、他のコンピュータとの間で暗号データの送受信が行われる。

【００６４】

一方、受信側では、データ受信部３５により、メッセージＤ１１と通常データＤ１３と復号されたデータとが受信される。この受信されたデータが渡されると、受信データ処理部３６では、受信したデータの種別に対応した処理が行われる。

【００６５】

これにより、セキュリティを保ちつつ、セキュアな通信経路の確保などを自動化することができる。

次に、本発明の実施の形態における通信端末装置１０とゲートウェイコンピュータ３０のハードウェア構成例について、図５を参照して具体的に説明する。なお、通信端末装置１０とゲートウェイコンピュータ３０は、同様のハードウェア構成により実現可能であり、この図５では、通信端末装置１０とゲートウェイコンピュータ３０を単にコンピュータ

１００として表現する。

【００６６】

図５は、本発明の実施の形態における通信端末装置及びゲートウェイコンピュータのハードウェア構成例を示す図である。コンピュータ１００は、ＣＰＵ(Central Processing Unit)１０１によって装置全体が制御されている。ＣＰＵ１０１には、バス１０７を介してＲＡＭ(Random Access Memory)１０２、ハードディスクドライブ（ＨＤＤ:Hard Disk Drive、以下、ＨＤＤと称する）１０３、グラフィック処理装置１０４、入力インタフェース１０５、および通信インタフェース１０６が接続されている。

【００６７】

ＲＡＭ１０２には、ＣＰＵ１０１に実行させるＯＳ(Operating System)のプログラムやアプリケーションプログラムの少なくとも一部が一時的に格納される。また、ＲＡＭ１０２には、ＣＰＵ１０１による処理に必要な各種データが格納される。ＨＤＤ１０３には、ＯＳやアプリケーションプログラム、あるいは各種データが格納される。

【００６８】

グラフィック処理装置１０４には、モニタＰ１１１が接続されている。グラフィック処理装置１０４は、ＣＰＵ１０１からの命令に従って、画像をモニタＰ１１１の画面に表示させる。入力インタフェース１０５には、キーボードＰ１１２とマウスＰ１１３とが接続されている。入力インタフェース１０５は、キーボードＰ１１２やマウスＰ１１３から送られてくる信号を、バス１０７を介してＣＰＵ１０１に送信する。

【００６９】

通信インタフェース１０６は、ネットワーク９０に接続されている。ネットワーク９０は、例えば、図２で前述したＬＡＮ９０ａ、ＷＡＮ９０ｂ、無線ＬＡＮ９０ｃ、あるいは、インターネットのような広域ネットワークである。この通信インタフェース１０６は、ネットワーク９０を介して、他のコンピュータとの間でデータの送受信を行う。

【００７０】

以上のようなハードウェア構成によって、通信端末装置１０とゲートウェイコンピュータ３０における本実施の形態の処理機能を実現することができる。たとえば、図３に示したコンピュータの電源が投入されると、ＨＤＤ１０３に格納されたＯＳのプログラムの一部が、ＲＡＭ１０２に読み込まれる。そして、ＣＰＵ１０１によりＯＳのプログラムが実行される。これにより、ＣＰＵ１０１上でＯＳの動作が開始する。そして、そのＯＳによって、本発明の実施の形態における各機能を実現するプログラムが実行管理される。

【００７１】

次に、本発明の実施の形態におけるプロトコルスタックの階層構造について、図６を参照して具体的に説明する。

図６は、本発明の実施の形態におけるプロトコルスタックを示す図である。

【００７２】

図６によると、まず、通信端末装置１０のプロトコルスタックは、下から最下位層にネットワークアダプタＰ１１、セキュアプロトコル層Ｐ１２、ＴＣＰ／ＩＰ層Ｐ１３、通信端末装置１０上のアプリケーションソフトウェアＰ１４の４階層構造となっている。また、ゲートウェイコンピュータ３０のプロトコルスタックは、下から最下位層にネットワークアダプタＰ３１ａ，Ｐ３１ｂ、セキュアプロトコル層Ｐ３２、ＴＣＰ／ＩＰ層Ｐ３３の３階層構造となっている。なお、セキュアプロトコル層以下の層においては、暗号化されたデータの受け渡しが行われる。

【００７３】

次に、通信端末装置１０において優先順位選択される通信デバイスについて、図７及び図８を参照して具体的に説明する。

図７は、通信端末装置における通信デバイスの実装例を示す図である。

【００７４】

図７によると、通信端末装置１０には、通信デバイスＭＵ１１ａ（有線ＬＡＮカード）、通信デバイスＭＵ１１ｂ（無線ＬＡＮカード）、および通信デバイスＭＵ１１ｃ（モデ

ム）が装着されており、それらが通信デバイス選択装置ＭＵ１２に接続されている。また、この通信デバイス選択装置ＭＵ１２には、ＴＣＰ／ＩＰ層においてデータの通信制御を行う部位であるＴＣＰ／ＩＰ管理部（ＭＵ１３）が接続されている。さらに、このＴＣＰ／ＩＰ管理部（ＭＵ１３）には、本発明の通信制御プログラムを利用するアプリケーションソフトウェアＭＵ１４が接続される。

【００７５】

一方、通信デバイスＭＵ１１ａ（有線ＬＡＮカード）には、ＨＵＢ２０ｃが接続されている。また、通信デバイスＭＵ１１ｂ（無線ＬＡＮカード）には、無線ＬＡＮアクセスポイント２０ｂが接続されている。さらに、通信デバイスＭＵ１１ｃ（モデム）には、ルータ２０ａが接続されている。そして、これら無線ＬＡＮアクセスポイント２０ｂ、ルータ２０ａ、およびＨＵＢ２０ｃには、ゲートウェイコンピュータ３０が接続されている。

【００７６】

ここで、通信端末装置１０の通信デバイス選択装置ＭＵ１２は、選択する通信デバイスの優先順位テーブルを予め設定保持しており、この優先順位により各通信デバイスを自動的に選択決定する。なお、通信デバイス選択装置ＭＵ１２は、前述した通信デバイス選択部１２により処理される。また、優先順位テーブルの詳細については、図８にて後述する。さらに、通信デバイス選択処理については、図１９にて後述する。

【００７７】

このような通信デバイスの実装構成により、通信デバイス選択装置ＭＵ１２が各通信デバイスを優先順位により自動的に選択することができ、所望の通信方式におけるデータ通信を、他のコンピュータやサーバコンピュータとの間で行うことが可能となる。

【００７８】

図８は、通信端末装置における通信デバイスの優先順位を示すテーブル構成例である。

図８によると、優先順位テーブルＹ１０には、優先順位、通信デバイス、およびセキュリティの項目がある。これらの各項目には、例えば、優先順位“１”として通信デバイス“有線ＬＡＮ”、セキュリティ“無”が設定されている。以下同じように、優先順位“２”として通信デバイス“無線ＬＡＮ”、セキュリティ“有”が設定され、優先順位“３”として通信デバイス“モデム”、セキュリティ“有”が設定されている。

【００７９】

このような優先順位により、例えば、図８における全ての通信デバイスがネットワーク接続可能な状態で接続されている場合、通信デバイス選択装置ＭＵ１２は、優先順位“１”であるので、通信デバイス “有線ＬＡＮ”を選択する。そして、通信端末装置１０は、セキュリティが“無”であるので本実施の形態におけるセキュアな通信経路の確立を行わずに、通常の通信経路の確立を行うことになる。

【００８０】

次に、本発明の実施の形態におけるデータ構造について説明する。なお、図９と図１０は、前述したクライアント側管理テーブルＭ１０のデータ構造図であり、ここでは便宜上、クライアント側管理テーブルＭ１０ａとクライアント側管理テーブルＭ１０ｂの２つに分けて、それぞれ図９と図１０にて説明する。

【００８１】

図９は、通信端末装置内に格納されるデータ構造図である。

図９によると、クライアント側管理テーブルＭ１０ａは、接続するゲートウェイコンピュータ３０におけるセキュアな通信経路を確立するための情報が格納されている。このクライアント側管理テーブルＭ１０ａには、接続するゲートウェイコンピュータ３０の“アドレス”、通信相手を認証するための“認証アルゴリズム”、データを暗号化する“暗号化アルゴリズム”、データの暗号化に使用する“鍵”、および、鍵を定期的に更新するための“鍵の更新時間”などの項目がある。これらの各項目には、例えば、アドレスとして“ｗ．ｘ．ｙ．ｚ１”、認証アルゴリズムとして“ＳＨＡ－１（Secure Hashing Algorithm 1）”、暗号化アルゴリズムとして“３ＤＥＳ（triple DES）”、鍵として“xxxxxxxxxx”、および、鍵の更新時間として“１８０秒”が設定されている。

【００８２】
このような情報により、例えば、アドレス“ｗ．ｘ．ｙ．ｚ１”に指定されたゲートウェイコンピュータ３０との間において、認証アルゴリズム“ＳＨＡ－１”、暗号化アルゴリズム“３ＤＥＳ”に基づいたセキュアな通信経路の確立とデータ通信が行われる。なお、このセキュアな通信経路の確立とデータ通信には、鍵“xxxxxxxxxx”が使用され、データの秘匿性が保たれる。また、鍵の更新時間“１８０秒”として定期的に更新することにより暗号データの強度が保たれる。

【００８３】
図１０は、タイマのカウント時において、接続する通信端末装置内に格納されるデータ構造図である。

図１０によると、クライアント側管理テーブルＭ１０ｂは、接続するゲートウェイコンピュータ３０における接続状態を監視するための情報が格納されている。このクライアント側管理テーブルＭ１０ｂには、接続するゲートウェイコンピュータ３０の“アドレス”、メッセージの受信時刻を示す“受信時刻”、および、受信時刻からの経過時間を示す“タイマカウンタ”の項目がある。これらの各項目には、例えば、アドレスとして“ｗ．ｘ．ｙ．ｚ１”、受信時刻として“１２：２５：４５”、および、タイマカウンタとして“１８０”が設定されている。

【００８４】
このようなクライアント側管理テーブルＭ１０ｂにより、アドレスに指定されたゲートウェイコンピュータ３０との間において、通信端末装置１０がゲートウェイコンピュータ３０からメッセージを受信した際に、通信端末装置１０とゲートウェイコンピュータ３０とが接続されていることを監視することができる。ここで、このクライアント側管理テーブルＭ１０ｂには、通信端末装置１０が受信のタイミングにより受信時刻を設定し、タイマカウンタをリセット（規定値にセット）する。また、このクライアント側管理テーブルＭ１０ｂには、通信端末装置１０によりタイマカウンタのカウントダウンが常に続けられて、メッセージ受信によるリセットのタイミングでタイマカウンタに規定値（図１０の例では１８０）がセットされる。そして、このクライアント側管理テーブルＭ１０ｂのタイマカウンタは、通信端末装置１０によりリセット後に再びカウントダウンが続けられて、タイマカウンタが“０”に達したときにタイムアウトと判断される。

【００８５】
図１１は、接続するゲートウェイコンピュータ内に格納されるデータ構造図である。

図１１によると、ゲートウェイコンピュータ側管理テーブルＭ３０は、接続する通信端末装置１０におけるセキュアな通信経路を確立するための情報が格納されている。このゲートウェイコンピュータ側管理テーブルＭ３０には、接続する通信端末装置１０の“アドレス”、通信相手を認証するための“認証アルゴリズム”、データを暗号化する“暗号化アルゴリズム”、データの暗号化に使用する“鍵”、および、鍵を定期的に更新するための“鍵の更新時間”などの項目がある。これらの各項目には、例えば、アドレスとして“ａ．ｂ．ｃ．ｄ１”、認証アルゴリズムとして“ＳＨＡ－１（Secure Hashing Algorithm 1）”、暗号化アルゴリズムとして“３ＤＥＳ（triple DES）”、鍵として“xxxxxxxxxx”、および、鍵の更新時間として“１８０秒”が設定されている。なお、接続する通信端末装置１０は複数設定登録することができ、以下、図１１のように設定されている。

【００８６】
このような情報により、例えば、アドレス“ａ．ｂ．ｃ．ｄ１”に指定された通信端末装置１０“通信端末装置（１）”との間において、認証アルゴリズム“ＳＨＡ－１”、暗号化アルゴリズム“３ＤＥＳ”に基づいたセキュアな通信経路の確立とデータ通信が行われる。なお、このセキュアな通信経路の確立とデータ通信には、鍵“xxxxxxxxxx”が使用され、データの秘匿性が保たれる。また、鍵の更新時間“１８０秒”として定期的に更新することにより暗号データの強度が保たれる。

【００８７】
次に、本発明の実施の形態の基本動作について、図１２～図１９を参照して具体的に説

明する。なお、図１２～図１９で送受信されるメッセージは、図３にて前述したメッセージＤ１１を、ＩＰブロードキャストの場合にメッセージＡ１とし、セキュアな通信経路を確立する場合にメッセージＢ１，Ｂ２に置き換えて説明する。

【００８８】

図１２は、本発明の実施の形態における通信制御プログラムの全体動作を示すフローチャートである。この処理は、通信端末装置１０とゲートウェイコンピュータ３０に対して、電源投入、サービスエリアからの離脱、通信断、あるいは予め決められた任意のタイミングを契機に動作し、ＣＰＵ１０１において実行させる処理である。以下、図１２の処理をステップ番号に沿って説明する。なお、本フローチャートにおける各機能の名称については、図２～図４をもとに説明する。

【００８９】

［ステップＳ１０１］　まず、ゲートウェイコンピュータ３０の接続確認部３１は、サブネットA全体に対し、一定時間間隔でメッセージＡ１をIPブロードキャストで送信する。

【００９０】

［ステップＳ１０２］　通信端末装置１０のデータ受信部１６では、メッセージＡ１を受信する。また、受信データ処理部１７は、メッセージの送信元ＩＰアドレスがゲートウェイコンピュータ３０であると判断し、クライアント側管理テーブルＭ１０に送信元ＩＰアドレスを格納する。以後、通信端末装置１０からの通信は、そのゲートウェイコンピュータ３０を介して行なう。

【００９１】

［ステップＳ１０３］　通信端末装置１０のセキュアな通信経路自動確立部１３は、接続するゲートウェイコンピュータ３０のＩＰアドレスを取得すると、セキュアプロトコル層において、ゲートウェイコンピュータとの間にセキュリティプロトコル（セキュアな通信経路）の確立シーケンスを実行する。

【００９２】

［ステップＳ１０４］　ゲートウェイコンピュータ３０のセキュアな通信経路自動確立部３２は、セキュアプロトコル層において、通信端末装置１０との間にセキュリティプロトコル（セキュアな通信経路）の確立シーケンスを実行する。

【００９３】

ここで、ステップＳ１０３とステップＳ１０４により、認証方式と互いに通信するデータの暗号化規則と復号規則とが決定され、この認証方式に従い通信端末装置１０とゲートウェイコンピュータ３０との間で互いが認証されることになる。

【００９４】

［ステップＳ１０５］　通信端末装置１０のデータ送信部１４は、ＴＣＰ／ＩＰ層において、ユーザから指定されたデータを送信するため、暗号化通信部１５へ渡す。

【００９５】

［ステップＳ１０６］　通信端末装置１０の暗号化通信部１５は、セキュアプロトコル層において、ステップＳ１０５にてデータ送信部１４から渡されたデータを暗号化して、暗号データＤ１２をゲートウェイコンピュータ３０に対して送信する。

【００９６】

［ステップＳ１０７］　ゲートウェイコンピュータ３０の暗号化通信部３４は、セキュアプロトコル層において、ステップＳ１０６にて通信端末装置１０から送信された暗号データＤ１２を受信して復号し、この復号したデータをデータ受信部３５へ渡す。

【００９７】

［ステップＳ１０８］　ゲートウェイコンピュータ３０のデータ受信部３５は、暗号化通信部３４から渡されたデータを受信データ処理部３６へ渡す。このデータを渡された受信データ処理部３６では、データを他のコンピュータへ中継するためにデータ送信部３３へ渡す。そして、データ送信部３３では、対向するコンピュータに対して渡されたデータを送信するため、このデータを暗号化通信部３４へ渡す。

【００９８】
［ステップＳ１０９］　ゲートウェイコンピュータ３０の暗号化通信部３４は、セキュアプロトコル層において、ステップＳ１０８にてデータ送信部３３により渡されたデータを暗号化して、暗号データＤ３２として対向するコンピュータへ送信する。なお、図１２に示す例では、対向するコンピュータは説明の便宜上のため、通信端末装置１０としている。
【００９９】
［ステップＳ１１０］　一方、通信端末装置１０の暗号化通信部１５は、セキュアプロトコル層において、ゲートウェイコンピュータ３０から送信された暗号データＤ３２を受信すると、暗号データＤ３２を復号して、そのデータをデータ受信部１６へ渡す。
【０１００】
［ステップＳ１１１］　通信端末装置１０のデータ受信部１６は、ＴＣＰ／ＩＰ層において、ステップＳ１１０にて渡されたデータを受信して、受信データ処理部１７へ渡す。そして、受信データ処理部１７では、渡されたデータをアプリケーションソフトウェア等に渡す。
【０１０１】
図１３は、図１２の通信制御プログラムの全体動作において、ゲートウェイコンピュータがデフォルトゲートウェイである場合の例を示すフローチャートである。この処理は、通信端末装置１０とゲートウェイコンピュータ３０に対して、電源投入、サービスエリアからの離脱、通信断、あるいは予め決められた任意のタイミングを契機に動作し、ＣＰＵ１０１において実行させる処理である。以下、図１３の処理をステップ番号に沿って説明する。なお、本フローチャートにおける各機能の名称については、図２～図４をもとに説明する。また、図１３には、ＤＨＣＰサーバ４０を図示している。ゲートウェイコンピュータ３０がデフォルトゲートウェイである場合には、一般的にこのＤＨＣＰサーバ４０を設置することによって、ＤＨＣＰサーバ４０を介してゲートウェイコンピュータ３０のＩＰアドレスが取得できる。なお、この例では、ＤＨＣＰサーバ４０を使用して、ゲートウェイコンピュータ３０のＩＰアドレスを取得しているが、他の取得手段でもよい。
【０１０２】
［ステップＳ２０１］　まず、通信端末装置１０は、ＤＨＣＰサーバ４０に対してゲートウェイコンピュータ３０のＩＰアドレスを要求する。通信端末装置１０のデータ受信部１６では、ＤＨＣＰサーバ４０からのＩＰアドレスを受信し、受信データ処理部１７へ渡す。また、受信データ処理部１７は、渡されたゲートウェイコンピュータ３０のＩＰアドレスをクライアント側管理テーブルＭ１０に格納する。以後、通信端末装置１０からの通信は、そのゲートウェイコンピュータ３０を介して行なう。
【０１０３】
［ステップＳ２０２］　通信端末装置１０の通信経路自動確立部１３は、接続するゲートウェイコンピュータ３０のＩＰアドレスを取得すると、セキュアプロトコル層において、ゲートウェイコンピュータとの間にセキュリティプロトコル（セキュアな通信経路）の確立シーケンスを実行する。
【０１０４】
［ステップＳ２０３］　ゲートウェイコンピュータ３０の通信経路自動確立部３２は、セキュアプロトコル層において、通信端末装置１０との間にセキュリティプロトコル（セキュアな通信経路）の確立シーケンスを実行する。
【０１０５】
ここで、ステップＳ２０２とステップＳ２０３により、認証方式と互いに通信するデータの暗号化規則と復号規則とが決定され、この認証方式に従い通信端末装置１０とゲートウェイコンピュータ３０との間で互いが認証されることになる。
【０１０６】
［ステップＳ２０４］　通信端末装置１０のデータ送信部１４は、ＴＣＰ／ＩＰ層において、ユーザから指定されたデータを送信するため、暗号化通信部１５へ渡す。

【０１０７】
［ステップＳ２０５］　通信端末装置１０の暗号化通信部１５は、セキュアプロトコル層において、ステップＳ２０４にてデータ送信部１４から渡されたデータを暗号化して、暗号データＤ１２をゲートウェイコンピュータ３０に対して送信する。
【０１０８】
［ステップＳ２０６］　ゲートウェイコンピュータ３０の暗号化通信部３４は、セキュアプロトコル層において、ステップＳ２０５にて通信端末装置１０から送信された暗号データＤ１２を受信して復号し、この復号したデータをデータ受信部３５へ渡す。
【０１０９】
［ステップＳ２０７］　ゲートウェイコンピュータ３０のデータ受信部３５は、データ受信部３５から渡されたデータを受信データ処理部３６へ渡す。このデータを渡された受信データ処理部３６では、データを他のコンピュータへ中継するためにデータ送信部３３へ渡す。そして、データ送信部３３では、対向するコンピュータに対して渡されたデータを送信するため、このデータを暗号化通信部３４へ渡す。
【０１１０】
［ステップＳ２０８］　ゲートウェイコンピュータ３０の暗号化通信部３４は、セキュアプロトコル層において、ステップＳ２０７にてデータ送信部３３により渡されたデータを暗号化して、暗号データＤ３２として対向するコンピュータへ送信する。なお、図１３に示す例では、対向するコンピュータは説明の便宜上のため、通信端末装置１０としている。
【０１１１】
［ステップＳ２０９］　一方、通信端末装置１０の暗号化通信部１５は、セキュアプロトコル層において、ゲートウェイコンピュータ３０から送信された暗号データＤ３２を受信すると、暗号データＤ３２を復号して、そのデータをデータ受信部１６へ渡す。
【０１１２】
［ステップＳ２１０］　通信端末装置１０のデータ受信部１６は、ＴＣＰ／ＩＰ層において、ステップＳ２０９にて渡されたデータを受信して、受信データ処理部１７へ渡す。そして、受信データ処理部１７では、渡されたデータをアプリケーションソフトウェア等に渡す。
【０１１３】
ここで、通信端末装置１０があるサブネットから別のサブネットへ移動した場合について、図１４～図１６を参照して具体的に説明する。
図１４は、本実施の形態を適用したＬＡＮシステムにおいて、通信端末装置１０が別のサブネットへ移動した場合の例を示す図である。
【０１１４】
図１４によると、サブネットＢ内には、ゲートウェイコンピュータ３０ｂ、アクセスポイント２０ｃ、通信端末装置１０ｇ，１０ｈ（点線）がある。また、サブネットＣ内には、ゲートウェイコンピュータ３０ｃ、アクセスポイント２０ｄ、通信端末装置１０ｉがある。
【０１１５】
このような初期状態において、今、通信端末装置１０ｈ（点線）がアクセスポイント２０ｃを経由してゲートウェイコンピュータ３０ｂに接続された状態から、通信端末装置１０ｈ（実線）の位置に移動したとする。
【０１１６】
このとき、図１５及び図１６のようなフローチャートにより処理が行われる。
図１５は、本発明の実施の形態における通信端末装置が移動した場合の全体動作を示すフローチャートである。この処理は、通信端末装置１０ｈがゲートウェイコンピュータ３０ｂの管理するサブネットＢを離脱し、ゲートウェイコンピュータ３０ｃの管理する他のサブネットＣへ参加したのを契機に動作し、ＣＰＵ１０１において実行させる処理である。以下、図１５の処理をステップ番号に沿って説明する。なお、本フローチャートにおけ

る各機能の名称については、図２～図４、および図１４をもとに説明する。

【０１１７】

［ステップＳ３０１］　まず、ゲートウェイコンピュータ３０ｃの接続確認部３１は、サブネットＣ全体に対し、一定時間間隔でメッセージＡ１をIPブロードキャストで送信する。

【０１１８】

［ステップＳ３０２］　移動した通信端末装置１０ｈのデータ受信部１６では、ＴＣＰ／ＩＰ層において、ゲートウェイコンピュータ３０ｃからのメッセージＡ１を受信する。そして、データ受信部１６は、受信したメッセージＡ１を受信データ処理部１７へ渡す。

【０１１９】

［ステップＳ３０３］　通信端末装置１０ｈの受信データ処理部１７は、以前に受信した、送信元がゲートウェイコンピュータ３０ｂであるメッセージと、新たに受信したメッセージＡ１とを比較して、送信元が異なることを検出する。また、受信データ処理部１７は、ステップＳ３０２にて送信元が異なることが検出されたので、以前とは異なるサブネットに接続したと判断する。

【０１２０】

［ステップＳ３０４］　通信端末装置１０ｈは、自身のIPアドレスをDHCPプロトコルによりＤＨＣＰサーバ４０から再取得した後、以後、使用するゲートウェイコンピュータとしてゲートウェイコンピュータ３０ｃを使用するよう認識する。

【０１２１】

［ステップＳ３０５］　通信端末装置１０ｈは、ステップＳ３０４にてゲートウェイコンピュータ３０ｃを使用するよう認識されたので、セキュアな通信経路の確立、およびデータ通信をゲートウェイコンピュータ３０ｃとの間で行う。なお、セキュアな通信経路の確立、およびデータ通信は、図１２のステップＳ１０３以降の処理と同様であるので、詳細については省略する。

【０１２２】

図１６は、本発明の実施の形態における通信端末装置が移動した場合、且つゲートウェイコンピュータがデフォルトゲートウェイである場合の全体動作を示すフローチャートである。この処理は、通信端末装置１０ｈがゲートウェイコンピュータ３０ｂの管理するサブネットＢを離脱し、ゲートウェイコンピュータ３０ｃの管理する他のサブネットＣへ参加したのを契機に動作し、ＣＰＵ１０１において実行させる処理である。以下、図１５の処理をステップ番号に沿って説明する。なお、本フローチャートにおける各機能の名称については、図２～図４、および図１４をもとに説明する。

【０１２３】

［ステップＳ４０１］　まず、サブネットＣに参加してきた通信端末装置１０ｈは、ＤＨＣＰサーバ４０に対してゲートウェイコンピュータ３０ｃのＩＰアドレスを要求する。通信端末装置１０ｈのデータ受信部１６では、ＤＨＣＰサーバ４０からのＩＰアドレスを受信し、受信データ処理部１７へ渡す。また、受信データ処理部１７は、渡されたゲートウェイコンピュータ３０ｃのＩＰアドレスをクライアント側管理テーブルＭ１０に格納する。以後、通信端末装置１０ｈからの通信は、そのゲートウェイコンピュータ３０ｃを介して行なう。なお、通信端末装置１０ｈは、上述のゲートウェイコンピュータ３０ｃのＩＰアドレスを要求する際に、自身のIPアドレスもDHCPプロトコルによりＤＨＣＰサーバ４０から再取得することが可能である。この図１６の例では、自身のＩＰアドレスは予め再取得されたものと仮定している。

【０１２４】

［ステップＳ４０２］　通信端末装置１０ｈの受信データ処理部１７は、以前に受信したゲートウェイコンピュータ３０ｂのアドレスと、新たに受信したゲートウェイコンピュータ３０ｃのアドレスとを比較して、ゲートウェイコンピュータが異なることを検出し、以前とは異なるサブネットに接続したと判断する。以後、使用するゲートウェイコンピュータとしてゲートウェイコンピュータ３０ｃを使用するよう認識する。

【０１２５】
［ステップＳ４０３］　通信端末装置１０ｈは、ステップＳ４０２にてゲートウェイコンピュータ３０ｃを使用するよう認識されたので、セキュアな通信経路の確立、およびデータ通信をゲートウェイコンピュータ３０ｃとの間で行う。なお、セキュアな通信経路の確立、およびデータ通信は、図１２のステップＳ１０３以降の処理と同様であるので、詳細については省略する。
【０１２６】
このような通信制御手順により、従来技術では、異なるネットワークに接続し直した場合、セキュリティプロトコル（セキュアな通信経路）の再確立のためにOSの再起動などの何らかの手動操作が必要であった。しかし、本発明の実施の形態では、通信端末装置１０ｈにて、ゲートウェイコンピュータ３０ｃからのメッセージを調べることにより、異なるネットワークに接続されたことを自動的に早く検出できるようになった。
【０１２７】
またここで、通信端末装置１０ｈがアクセスポイント２０ｃを使用できなくなった場合であって、例えばアクセスポイント２０ｃのサービスエリア圏外へ移動した場合等について、図１７～図１８を参照して具体的に説明する。
【０１２８】
図１７は、本実施の形態を適用したＬＡＮシステムにおいて、通信端末装置がサービスエリア圏外へ移動した場合の例を示す図である。
図１７によると、サブネットＢ内には、ゲートウェイコンピュータ３０ｂ、アクセスポイント２０ｃ、通信端末装置１０ｇ，１０ｈ（点線）がある。
【０１２９】
このような初期状態において、今、通信端末装置１０ｈ（点線）がアクセスポイント２０ｃ（ここでは、例として無線ＬＡＮ等）を経由してゲートウェイコンピュータ３０ｂに接続された状態（サポートエリア）から、離脱するなどの原因により、ネットワーク（サブネットＢ）から切り離されたとする。例えば、図１７において、通信端末装置１０ｈ（点線）がアクセスポイント２０ｃのサービスエリア圏外である通信端末装置１０ｈ（実線）の位置に移動したとする。
【０１３０】
このとき、図１８のようなフローチャートにより処理が行われる。
図１８は、本発明の実施の形態における通信端末装置が、サービスエリア圏外に移動した場合の全体動作を示すフローチャートである。この処理は、ゲートウェイコンピュータ３０ｂが管理するサブネットＢにおいて、通信端末装置１０ｈがアクセスポイント２０ｃのサービスエリア圏外へ移動したのを契機に動作し、ＣＰＵ１０１において実行させる処理である。以下、図１８の処理をステップ番号に沿って説明する。なお、本フローチャートにおける各機能の名称については、図２～図４、および図１７をもとに説明する。
【０１３１】
［ステップＳ５０１］　まず、ゲートウェイコンピュータ３０ｂの接続確認部３１は、サブネットＢ全体に対し、一定時間間隔でメッセージＡ１をIPブロードキャストで送信する。
【０１３２】
［ステップＳ５０２］　移動した通信端末装置１０ｈのデータ受信部１６では、ＴＣＰ／ＩＰ層において、ゲートウェイコンピュータ３０ｂからのメッセージＡ１を受信する。また、データ受信部１６は、受信したメッセージＡ１を受信データ処理部１７へ渡す。受信データ処理部１７では、メッセージＡ１を受け取ると同時にタイマＴ１０から現在時刻を取得する。また、受信データ処理部１７では、取得した現在時刻をクライアント側管理テーブルＭ１０へ格納する。さらに、受信データ処理部１７は、現在時刻を格納すると同時にタイマカウンタをリセット（規定値をセット）する。以後、タイマＴ１０からの現在時刻をもとにタイマカウンタをカウントダウンしていく。つまり、通信端末装置１０ｈは、一定時間毎に中継送信されるアクセスポイント２０ｃからのメッセージを監視している

。

【０１３３】

［ここで、通信端末装置１０ｈがアクセスポイント２０ｃのサービスエリア圏外へ移動する。］

［ステップＳ５０３］　再びゲートウェイコンピュータ３０ｂの接続確認部３１は、サブネットＢ全体に対し、メッセージＡ１をIPブロードキャストで送信する。なお、図１８の例では、既に通信端末装置１０ｈがネットワークから離脱しているので、メッセージＡ１が届かない。

【０１３４】

［ステップＳ５０４］　通信端末装置１０ｈの受信データ処理部１７は、ステップＳ５０２にてカウントダウンしたタイマカウンタが、一定時間経過して“０”となったので、ネットワークの離脱を判断する。つまり、一定時間メッセージＡ１が受信できなかったので、通信端末装置１０ｈの移動場所は、アクセスポイント２０ｃのサービスエリア圏外（サポートエリアから離脱）であると判断する。あるいは、通信端末装置１０ｈとアクセスポイント２０ｃとの間の回線は、切断されたと判断する。

【０１３５】

［ステップＳ５０５］　通信端末装置１０ｈの受信データ処理部１７は、ステップＳ５０３にてネットワークの離脱と判断されたので、ネットワークが切り離され使用不能となったことをＴＣＰ／ＩＰ層を利用しているデバイスドライバやＡＰＩ等に通知する。

【０１３６】

［ステップＳ５０６］　ＴＣＰ／ＩＰ層を利用しているデバイスドライバやＡＰＩ等はネットワークが切り離され使用不能になったことを受信する。

これにより通信端末装置１０ｈは、ＴＣＰ／ＩＰプロトコルを使用しているアプリケーションソフトウェアに対して、通信エラーを認識させることができる。そして、これ以降は、通信端末装置１０ｈからの通信は不能となる。

【０１３７】

従来技術では、通信端末装置１０ｈとゲートウェイコンピュータ３０ｂとの間の接続が絶たれたことを検出する手段がなかったため、通信端末装置１０ｈにおいてリカバリ処理などの動作に移るために通信端末装置１０ｈ上で手動操作を行なう必要があった。しかし、本発明の実施の形態では、自動的にゲートウェイコンピュータ３０ｂとの接続の切断を検出できるため、ユーザはリカバリ処理に要する時間を短縮することが可能となる。

【０１３８】

次に、図７の通信デバイス選択装置ＭＵ１２、および図３の通信デバイス選択部１２における通信デバイス選択処理について、図１９を参照して具体的に説明する。

【０１３９】

図１９は、本発明の実施の形態における通信デバイス選択処理の基本動作を示すフローチャートである。この処理は、通信端末装置１０にて、通信デバイス選択部１２に制御が移行、すなわちサービス選択部１１にて通信経路自動確立処理が選択されたのを契機に動作し、ＣＰＵ１０１において実行させる処理である。以下、図１９の処理をステップ番号に沿って説明する。なお、本フローチャートにおける各機能の名称については、図３をもとに説明する。

【０１４０】

［ステップＳ６０１］　通信端末装置１０の通信デバイス選択部１２は、通信デバイスの優先順位テーブルＹ１０のうちで、最も優先順位が高いものを検索する。

【０１４１】

［ステップＳ６０２］　通信デバイス選択部１２は、ステップＳ６０１にて検索した結果、通信デバイスが見つかったかどうかを判定する。ここで、通信デバイスが見つかった場合には、ステップＳ６０３へ進む。また、通信デバイスが見つからない場合には、ステップＳ６０４へ進む。

【０１４２】

［ステップＳ６０３］　ステップＳ６０２にて通信デバイスが見つかったので、通信端末装置１０の受信データ処理部１７は、この通信デバイスにおいて、ゲートウェイコンピュータ３０からのメッセージＤ３１の受信を一定時間待ち合わせる。

【０１４３】

［ステップＳ６０４］　ステップＳ６０２にて通信デバイスが見つからなかったので、全ての通信デバイスが使用不能であることをＴＣＰ／ＩＰ層へ通知する。これにより、通信端末装置１０は、ＴＣＰ／ＩＰプロトコルを使用しているアプリケーションソフトウェアに通信エラーを認識させることができる。

【０１４４】

［ステップＳ６０５］　受信データ処理部１７は、ステップＳ６０３にて待ち合わせた結果、メッセージＤ３１が受信できたかどうかを判定する。ここで、メッセージＤ３１が受信できた場合には、ステップＳ６０６へ進む。また、メッセージＤ３１が受信できない場合には、ステップＳ６０７へ進む。

【０１４５】

［ステップＳ６０６］　ステップＳ６０４にてメッセージＤ３１が受信できたので、当該通信デバイスが使用可能であること、及びそれ以外の通信デバイスが使用不能であることをＴＣＰ／ＩＰ層及びセキュアプロトコル層を使用する通信経路自動確立部１３、データ送信部１４へ通知する。

【０１４６】

［ステップＳ６０７］　ステップＳ６０４にてメッセージＤ３１が受信できなかったので、当該通信デバイスが使用できないと判断し、次に優先順位の高い通信デバイスを検索する。

【０１４７】

［ステップＳ６０８］　当該通信デバイスが使用可能であるので、セキュアな通信経路自動確立部１３は、セキュアな通信経路の確立を行う。

このような通信制御手順により、セキュリティを保ちつつ、ゲートウェイコンピュータ毎の通信設定やセキュアな通信経路の確保などを自動化することができ、ゲートウェイコンピュータの変化にともなうユーザ設定項目を減らし、ユーザの負担を軽減することが可能となる。

【０１４８】

以上説明した処理は、コンピュータプログラムに記述し、コンピュータで実行することにより、本発明の機能を実現することができる。また、コンピュータで実行する際には、コンピュータ内のハードディスク等にコンピュータプログラムを予め格納しておき、メインメモリにロードして実行する。なお、コンピュータプログラムは、コンピュータで読み取り可能な記録媒体に記録しておくことができる。コンピュータで読み取り可能な記録媒体としては、磁気記録媒体、光ディスク、光磁気記録媒体、半導体メモリなどがある。磁気記録媒体には、ハードディスク、フレキシブルディスク（FD）、ＺＩＰ（Zip:磁気ディスクの一種）、磁気テープなどがある。光ディスクには、ＤＶＤ（Digital Versatile Disc）、ＤＶＤ－ＲＡＭ（DVD Random Access Memory）、ＣＤ－ＲＯＭ（Compact Disc Read Only Memory）、ＣＤ－Ｒ（CD Recordable）、ＣＤ－ＲＷ（CD Rewritable）などがある。光磁気記録媒体には、ＭＯ（Magneto Optical Disk）などがある。半導体メモリには、フラッシュ・メモリ（Flash Memory）などがある。

【０１４９】

また、コンピュータプログラムを流通させる場合には、例えば各コンピュータプログラムが記録されたＤＶＤ、ＣＤ－ＲＯＭなどの可搬型記録媒体が販売される。また、コンピュータプログラムをサーバの記憶装置に格納しておき、ネットワークを介して、サーバからクライアントへコンピュータプログラムを転送することもできる。

［本実施の形態の効果］

以上説明した本実施の形態の効果について、以下に述べる。

【０１５０】

（１）　通信開始時(PCのブート時など)に本発明の実施の形態が提供するサービスの開始をユーザに選択させることにより、セキュアな通信経路を介しての通信と、(本発明の実施の形態を使わない)従来環境での通信の双方とを使い分けることが可能となる。

【０１５１】

（２）通信開始時や、通信端末装置がサブネットを跨いで移動した際、ゲートウェイコンピュータのアドレスの設定／変更やセキュアな通信経路の確立を自動化することにより、環境設定の負担を解消することが可能となる。

【０１５２】

（３）通信端末装置がゲートウェイコンピュータのサービスエリアから離れたことを迅速に検出することにより、ユーザはリカバリ処理に要する時間を短縮することが可能となる。

【０１５３】

（４）複数の通信インタフェースを実装している通信端末装置において、装置内で定義した優先順位に従い通信インタフェースを自動で選択することにより、通信インタフェースの変更に伴う通信環境の変更や、セキュアな通信経路の確立を自動化し、ユーザから不可視化することにより、ユーザによる環境設定の負担を解消することが可能となる。

【０１５４】

（付記１）　無線ネットワークと他のネットワークとの間で送受信されるデータを中継するためのゲートウェイ側の通信制御プログラムにおいて、

コンピュータに、

前記無線ネットワーク上に、セキュリティ機能を有することを示すメッセージをブロードキャストで定期的に送信し、

前記メッセージを受信した通信端末装置からの要求に応じて前記通信端末装置との間で相互通信を行い、認証方式と互いに通信するデータの暗号化規則と復号規則とを決定し、前記認証方式に従い前記通信端末装置との間で互いを認証し、

前記通信端末装置宛のデータを前記暗号化規則に従って暗号化して前記無線ネットワーク経由で送信し、前記無線ネットワーク経由で前記通信端末装置から受信した暗号データを前記復号規則で復号する、

処理を実行させることを特徴とするゲートウェイ側の通信制御プログラム。

【０１５５】

（付記２）　前記認証方式と前記暗号化規則と復号規則の決定の際には、前記認証方式と前記暗号化規則と復号規則の決定時に受信されるメッセージ内に含まれる前記通信端末装置のアドレスを、装置内部の記憶媒体に格納することを特徴とする付記１記載のゲートウェイ側の通信制御プログラム。

【０１５６】

（付記３）　前記認証方式と前記暗号化規則と復号規則の決定の際には、前記記憶媒体に格納された前記通信端末装置の前記アドレスをもとに行うことを特徴とする付記２記載のゲートウェイ側の通信制御プログラム。

【０１５７】

（付記４）　無線ネットワークを経由して通信を行うための通信端末装置側の通信制御プログラムにおいて、

コンピュータに、

前記無線ネットワークによる通信可能範囲に入ると、前記無線ネットワーク経由で、セキュリティ機能を有するゲートウェイのアドレスを取得し、

取得した前記アドレスに基づき前記ゲートウェイとの間で相互通信を行い、認証方式と互いに通信するデータの暗号化規則と復号規則とを決定し、前記認証方式に従い前記ゲートウェイとの間で互いを認証し、

他のコンピュータ宛のデータを前記暗号化規則に従って暗号化して前記無線ネットワーク経由で前記ゲートウェイへ送信し、前記無線ネットワーク経由で前記ゲートウェイから受信した暗号データを前記復号規則で復号する、

処理を実行させることを特徴とする通信端末装置側の通信制御プログラム。

【０１５８】

（付記５） 前記メッセージの受信の際には、前記メッセージ内にある前記ゲートウェイの前記アドレスを取得すると共に、前記アドレスを装置内部の記憶媒体に格納することを特徴とする付記４記載の通信端末装置側の通信制御プログラム。

【０１５９】

（付記６） 前記認証方式と前記暗号化規則と復号規則の決定は、前記記憶媒体に格納された前記ゲートウェイの前記アドレスをもとにして行うことを特徴とする付記５記載の通信端末装置側の通信制御プログラム。

【０１６０】

（付記７） 前記ゲートウェイのアドレスを取得する際には、前記無線ネットワークに対して前記ゲートウェイがブロードキャストで定期的に送信しているメッセージから、前記アドレスを取得することを特徴とする付記４記載の通信端末装置側の通信制御プログラム。

【０１６１】

（付記８） 前記ゲートウェイのアドレスを取得する際には、他のサーバから前記ゲートウェイのアドレスを取得することにより、前記通信端末装置と前記ゲートウェイとの間において相互通信を行い、前記認証方式と前記暗号化規則と復号規則とを自動的に決定することを特徴とする付記４記載の通信端末装置側の通信制御プログラム。

【０１６２】

（付記９） 前記暗号化規則と復号規則の決定は、前記アドレスの取得時において前記ゲートウェイのアドレス変更を検出した場合、前記ゲートウェイとの間において相互通信を行い、前記認証方式と前記暗号化規則と復号規則とを自動的に再決定することを特徴とする付記８記載の通信端末装置側の通信制御プログラム。

【０１６３】

（付記１０） 前記通信端末装置が複数の通信手段を有する場合、

予めどの通信手段が使用可能であるかを調べ、使用できる通信手段が複数あるときに、その優先順位を前記通信端末装置内に定義し、

前記通信端末装置にて、前記優先順位に従って通信手段を自動選択し、使用する通信手段以外を無効にして、使用する通信手段で前記ゲートウェイとの間において相互通信を行い、前記認証方式と前記暗号化規則と復号規則とを決定することを特徴とする付記４記載の通信端末装置側の通信制御プログラム。

【０１６４】

（付記１１） 無線ネットワークと他のネットワークとの間で送受信されるデータを中継するためのゲートウェイ側の通信制御方法において、

前記無線ネットワーク上に、セキュリティ機能を有することを示すメッセージをブロードキャストで定期的に送信し、

前記メッセージを受信した通信端末装置からの要求に応じて前記通信端末装置との間で相互通信を行い、認証方式と互いに通信するデータの暗号化規則と復号規則とを決定し、前記認証方式に従い前記通信端末装置との間で互いを認証し、

前記通信端末装置宛のデータを前記暗号化規則に従って暗号化して前記無線ネットワーク経由で送信し、前記無線ネットワーク経由で前記通信端末装置から受信した暗号データを前記復号規則で復号する、

ことを特徴とするゲートウェイ側の通信制御方法。

【０１６５】

（付記１２） 無線ネットワークを経由して通信を行うための通信端末装置側の通信制御方法において、

前記無線ネットワークによる通信可能範囲に入ると、前記無線ネットワーク経由で、セキュリティ機能を有するゲートウェイのアドレスを取得し、

取得した前記アドレスに基づき前記ゲートウェイとの間で相互通信を行い、認証方式と

互いに通信するデータの暗号化規則と復号規則とを決定し、
　他のコンピュータ宛のデータを前記暗号化規則に従って暗号化して前記無線ネットワーク経由で前記ゲートウェイへ送信し、前記無線ネットワーク経由で前記ゲートウェイから受信した暗号データを前記復号規則で復号する、
　ことを特徴とする通信端末装置側の通信制御方法。
【０１６６】
　（付記１３）　無線ネットワークと他のネットワークとの間で送受信されるデータを中継するためのゲートウェイにおいて、
　前記無線ネットワーク上に、セキュリティ機能を有することを示すメッセージをブロードキャストで定期的に送信する接続確認部と、
　前記メッセージを受信した通信端末装置からの要求に応じて前記通信端末装置との間で相互通信を行い、認証方式と互いに通信するデータの暗号化規則と復号規則とを決定し、前記認証方式に従い前記通信端末装置との間で互いを認証する通信経路自動確立部と、
　前記通信端末装置宛のデータを前記暗号化規則に従って暗号化して前記無線ネットワーク経由で送信し、前記無線ネットワーク経由で前記通信端末装置から受信した暗号データを前記復号規則で復号する暗号化通信部と、
　を有することを特徴とするゲートウェイ。
【０１６７】
　（付記１４）　無線ネットワークを経由して通信を行うための通信端末装置において、
　前記無線ネットワークによる通信可能範囲に入ると、前記無線ネットワーク経由で、セキュリティ機能を有するゲートウェイのアドレスを取得する受信データ処理部と、
　取得した前記アドレスに基づき前記ゲートウェイとの間で相互通信を行い、認証方式と互いに通信するデータの暗号化規則と復号規則とを決定し、前記認証方式に従い前記ゲートウェイとの間で互いを認証する通信経路自動確立部と、
　他のコンピュータ宛のデータを前記暗号化規則に従って暗号化して前記無線ネットワーク経由で前記ゲートウェイへ送信し、前記無線ネットワーク経由で前記ゲートウェイから受信した暗号データを前記復号規則で復号する暗号化通信部と、
　を有することを特徴とする通信端末装置。
【０１６８】
　（付記１５）　無線ネットワークと他のネットワークとの間で送受信されるデータを中継するためのゲートウェイ側のプログラムを記録したコンピュータ読み取り可能な記録媒体において、
　前記コンピュータに、
　前記無線ネットワーク上に、セキュリティ機能を有することを示すメッセージをブロードキャストで定期的に送信し、
　前記メッセージを受信した通信端末装置からの要求に応じて前記通信端末装置との間で相互通信を行い、認証方式と互いに通信するデータの暗号化規則と復号規則とを決定し、前記認証方式に従い前記通信端末装置との間で互いを認証し、
　前記通信端末装置宛のデータを前記暗号化規則に従って暗号化して前記無線ネットワーク経由で送信し、前記無線ネットワーク経由で前記通信端末装置から受信した暗号データを前記復号規則で復号する、
　処理を実行させることを特徴とするゲートウェイ側のプログラムを記録したコンピュータ読み取り可能な記録媒体。
【０１６９】
　（付記１６）　無線ネットワークを経由して通信を行うための通信端末装置側のプログラムを記録したコンピュータ読み取り可能な記録媒体において、
　前記コンピュータに、
　前記無線ネットワークによる通信可能範囲に入ると、前記無線ネットワーク経由で、セキュリティ機能を有するゲートウェイのアドレスを取得し、
　取得した前記アドレスに基づき前記ゲートウェイとの間で相互通信を行い、認証方式と

互いに通信するデータの暗号化規則と復号規則とを決定し、前記認証方式に従い前記ゲートウェイとの間で互いを認証し、

他のコンピュータ宛のデータを前記暗号化規則に従って暗号化して前記無線ネットワーク経由で前記ゲートウェイへ送信し、前記無線ネットワーク経由で前記ゲートウェイから受信した暗号データを前記復号規則で復号する、

処理を実行させることを特徴とする通信端末装置側のプログラムを記録したコンピュータ読み取り可能な記録媒体。

【０１７０】

【発明の効果】

以上説明したように本発明では、対向する通信端末装置に対して、ゲートウェイコンピュータから定期的にアドレスを送信し、通信端末装置とゲートウェイコンピュータとの間で認証方式と暗号化規則と復号規則を決定するようにしたので、セキュリティを保ちつつ、ゲートウェイコンピュータ毎の通信設定やセキュアな通信経路の確保などを自動化することができる。このため、ゲートウェイコンピュータの変化にともなうユーザ設定項目を減らし、ユーザの負担を軽減することが可能となる。

【図面の簡単な説明】

【図１】　本発明の原理構成図である。

【図２】　本発明の実施の形態を適用したシステム構成図である。

【図３】　本発明の実施の形態における通信端末装置の機能ブロック図である。

【図４】　本発明の実施の形態におけるゲートウェイコンピュータの機能ブロック図である。

【図５】　本発明の実施の形態における通信端末装置及びゲートウェイコンピュータのハードウェア構成例を示す図である。

【図６】　本発明の実施の形態におけるプロトコルスタックを示す図である。

【図７】　通信端末装置における通信デバイスの実装例を示す図である。

【図８】　通信端末装置における通信デバイスの優先順位を示すテーブル構成例である。

【図９】　通信端末装置内に格納されるデータ構造図である。

【図１０】　タイマのカウント時において、接続する通信端末装置内に格納されるデータ構造図である。

【図１１】　接続するゲートウェイコンピュータ内に格納されるデータ構造図である。

【図１２】　本発明の実施の形態における通信制御プログラムの全体動作を示すフローチャートである。

【図１３】　図１２の通信制御プログラムの全体動作において、ゲートウェイコンピュータがデフォルトゲートウェイである場合の例を示すフローチャートである。

【図１４】　本実施の形態を適用したＬＡＮシステムにおいて、通信端末装置１０が別のサブネットへ移動した場合の例を示す図である。

【図１５】　本発明の実施の形態における通信端末装置が移動した場合の全体動作を示すフローチャートである。

【図１６】　本発明の実施の形態における通信端末装置が移動した場合、且つゲートウェイコンピュータがデフォルトゲートウェイである場合の全体動作を示すフローチャートである。

【図１７】　本実施の形態を適用したＬＡＮシステムにおいて、通信端末装置がサービスエリア圏外へ移動した場合の例を示す図である。

【図１８】　本発明の実施の形態における通信端末装置が、サービスエリア圏外に移動した場合の全体動作を示すフローチャートである。

【図１９】　本発明の実施の形態における通信デバイス選択処理の基本動作を示すフローチャートである。

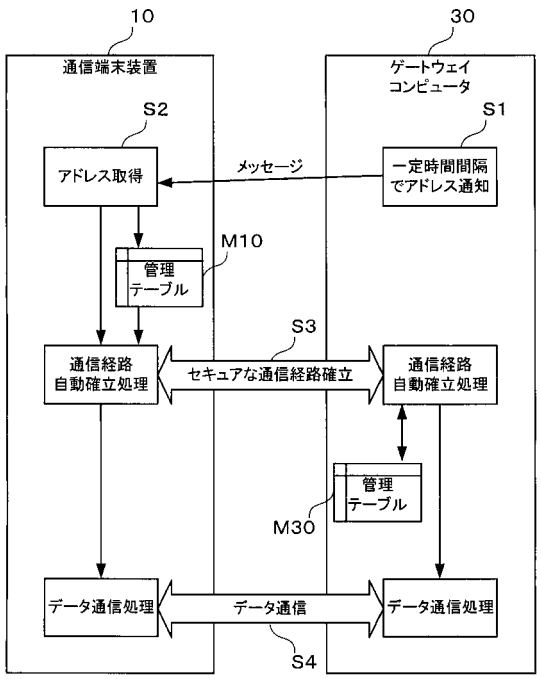
【符号の説明】

１０　通信端末装置

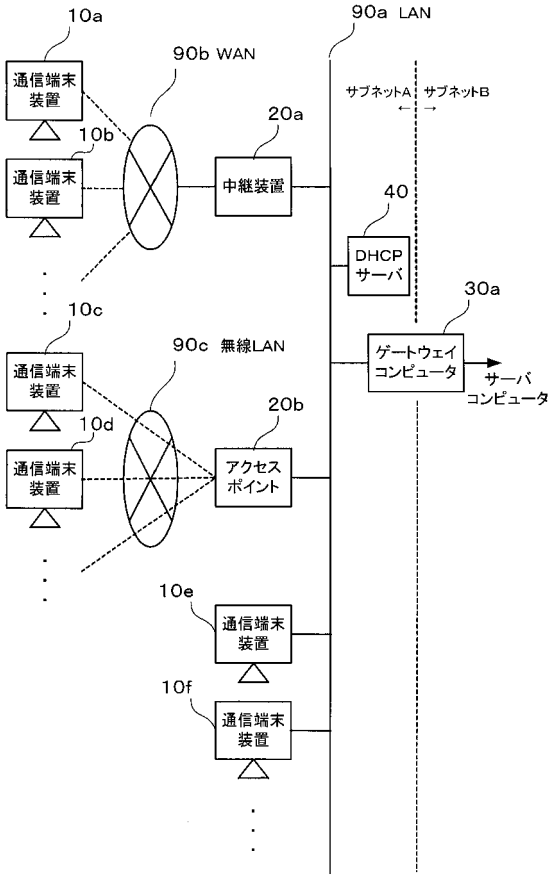
３０　ゲートウェイコンピュータ

Ｍ１０　クライアント側管理テーブル
Ｍ３０　ゲートウェイコンピュータ側管理テーブ

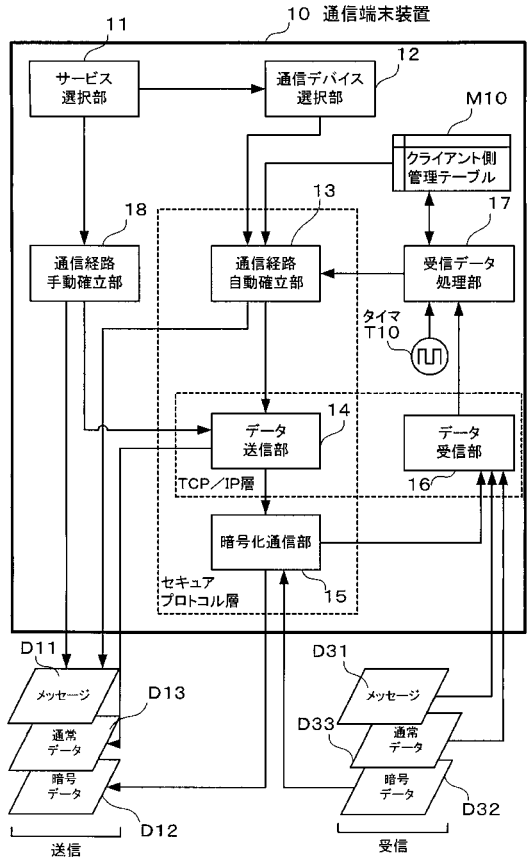
【図１】



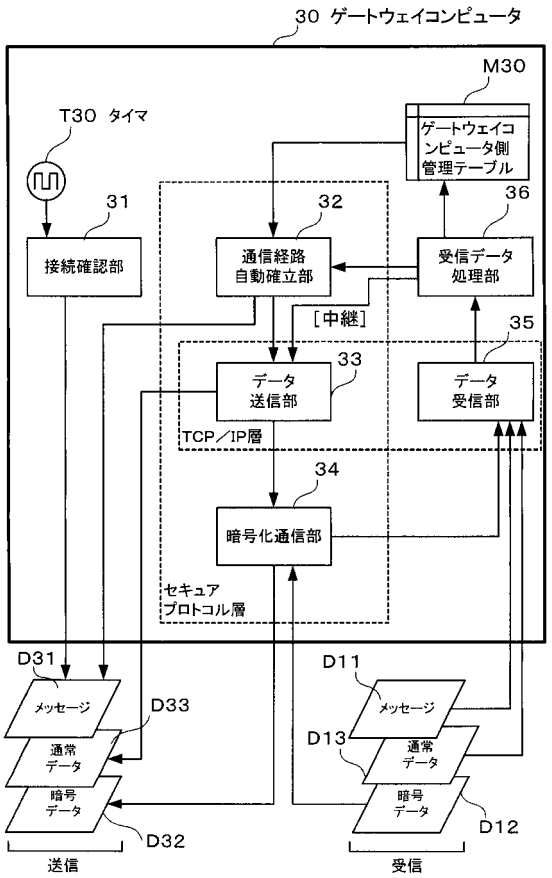
【図２】



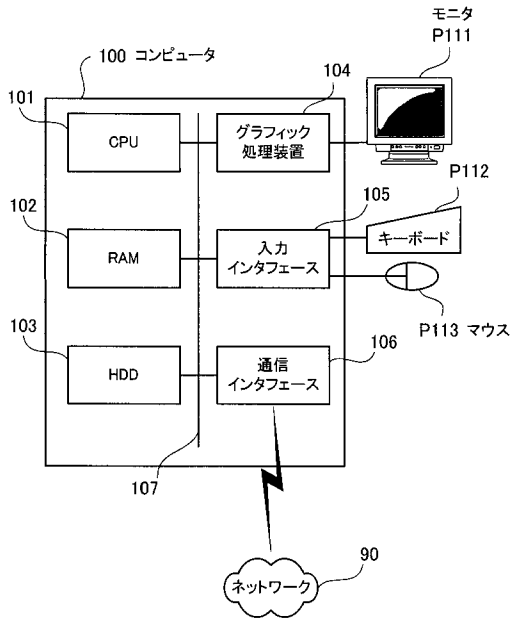
【図３】


10 通信端末装置
11
サービス選択部
12
通信デバイス選択部
M10
クライアント側管理テーブル
13
17
18
通信経路手動確立部
通信経路自動確立部
受信データ処理部
タイマ T10
14
データ送信部
データ受信部
16
TCP／IP層
暗号化通信部
15
セキュアプロトコル層
D11
D31
メッセージ
D13
D33
通常データ
暗号データ
D32
D12
送信
受信

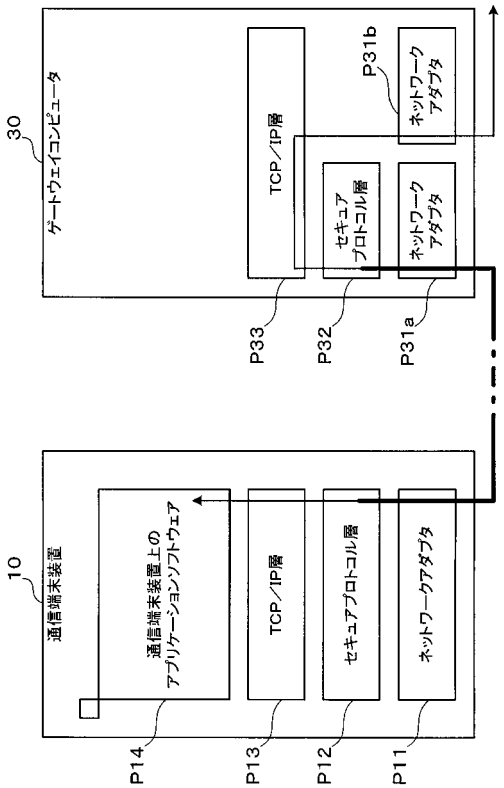
【図４】


30 ゲートウェイコンピュータ
M30
ゲートウェイコンピュータ側管理テーブル
T30 タイマ
31
32
36
接続確認部
通信経路自動確立部
受信データ処理部
［中継］
35
33
データ送信部
データ受信部
TCP／IP層
34
暗号化通信部
セキュアプロトコル層
D31
D11
メッセージ
D33
D13
通常データ
暗号データ
D32
D12
送信
受信

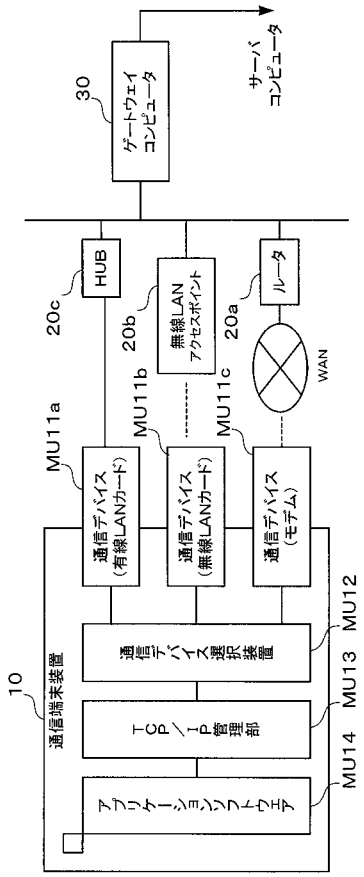
【図５】


モニタ
P111
100 コンピュータ
104
101
CPU
グラフィック処理装置
P112
105
102
RAM
入力インタフェース
キーボード
P113 マウス
103
HDD
通信インタフェース
106
107
90
ネットワーク

【図６】


30
ゲートウェイコンピュータ
TCP／IP層
P31b
ネットワークアダプタ
セキュアプロトコル層
ネットワークアダプタ
P33
P32
P31a
10
通信端末装置
通信端末装置上のアプリケーションソフトウェア
TCP／IP層
セキュアプロトコル層
ネットワークアダプタ
P14
P13
P12
P11

【図７】



【図８】

Y10 優先順位テーブル

優先順位	通信デバイス	セキュリティ
1	有線LAN	無
2	無線LAN	有
3	モデム	有

【図９】

M10a クライアント側管理テーブル

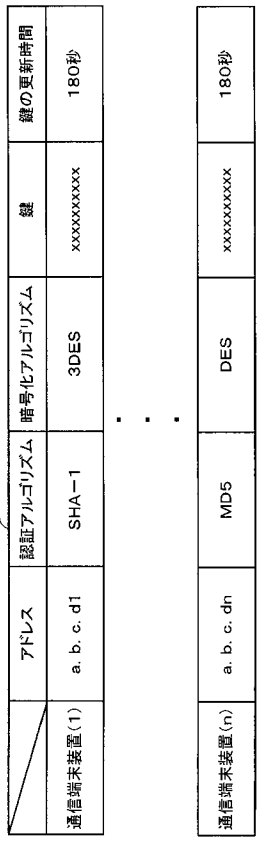
／	アドレス	認証アルゴリズム	暗号化アルゴリズム	鍵	鍵の更新時間
接続ゲートウェイコンピュータ	w. x. y. z1	SHA－1	3DES	xxxxxxxxxx	180秒

【図１０】

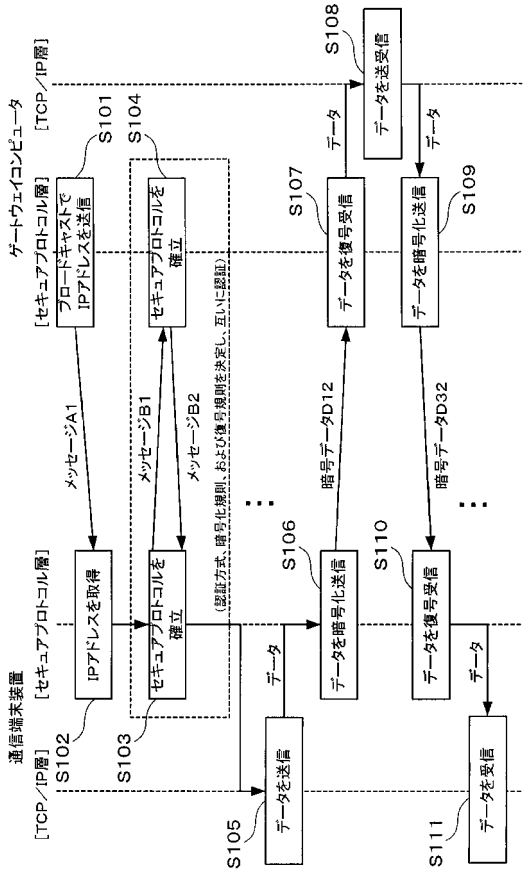
M10b クライアント側管理テーブル

／	アドレス	受信時刻	タイマカウンタ
接続ゲートウェイコンピュータ	w. x. y. z1	12:25:45	180

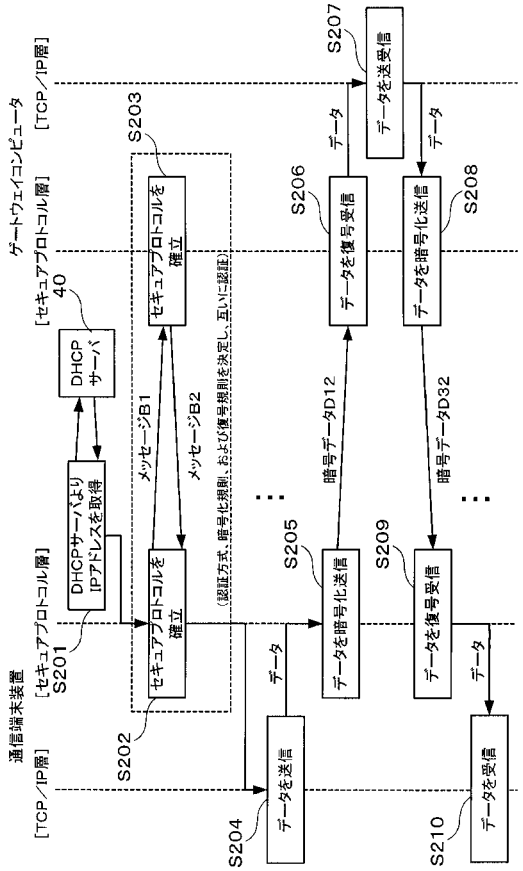
【図１１】



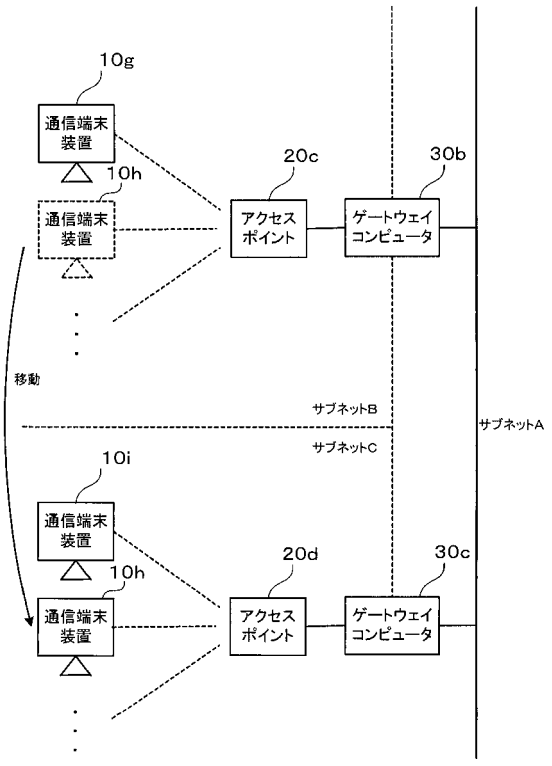
【図１２】



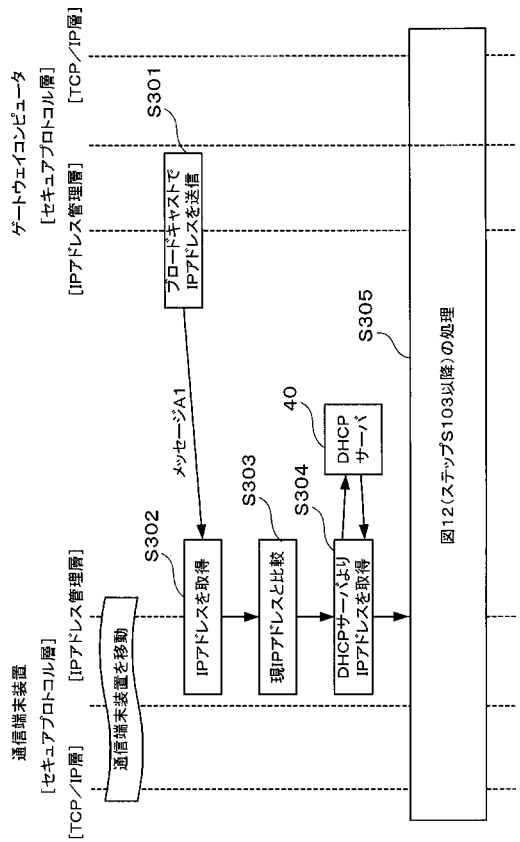
【図１３】



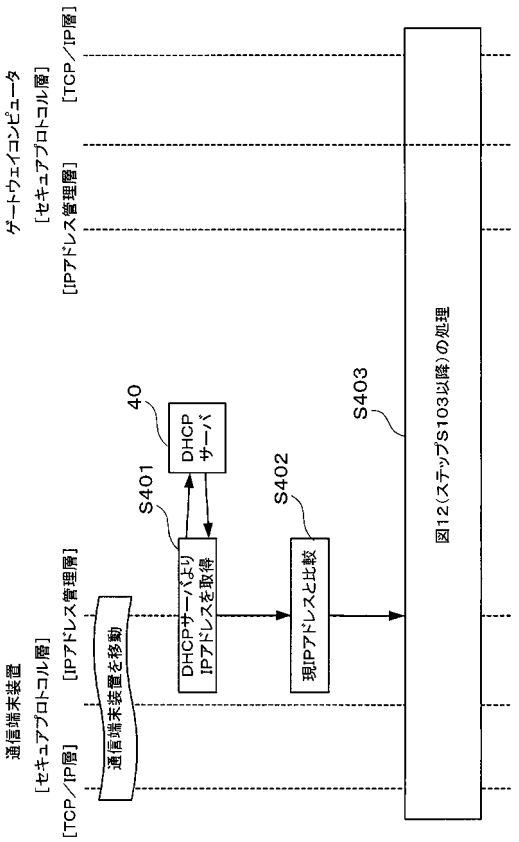
【図１４】



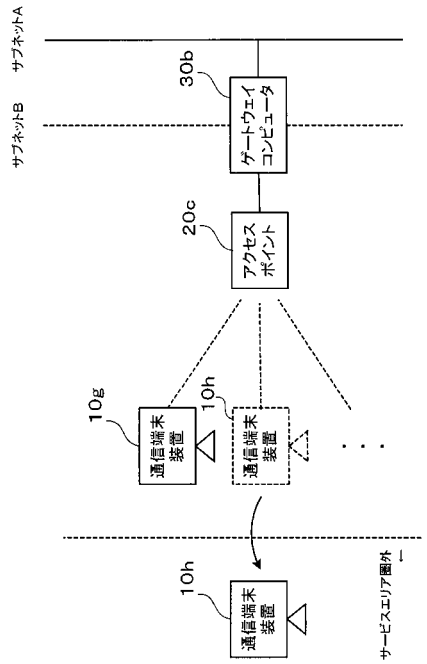
【図１５】



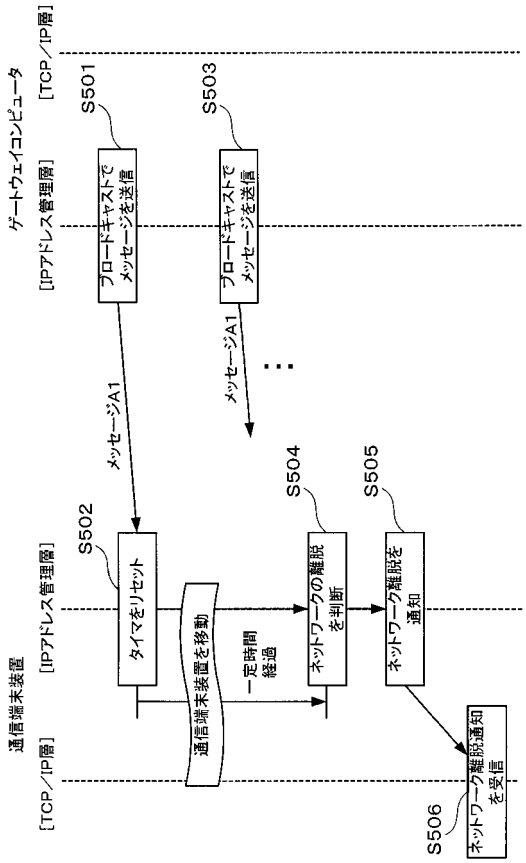
【図１６】



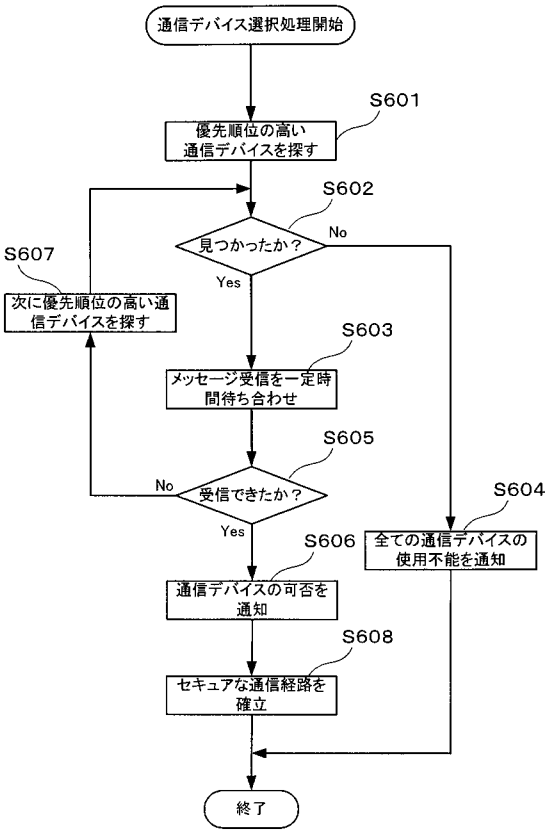
【図１７】



【図１８】



【図１９】


通信デバイス選択処理開始
S601
優先順位の高い通信デバイスを探す
S602
見つかったか？
No
Yes
S607
次に優先順位の高い通信デバイスを探す
S603
メッセージ受信を一定時間待ち合わせ
S605
No
受信できたか？
Yes
S604
全ての通信デバイスの使用不能を通知
S606
通信デバイスの可否を通知
S608
セキュアな通信経路を確立
終了

フロントページの続き

(72)発明者　竹川　郁男
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　竹間　智
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

審査官　▲高▼橋　真之

(56)参考文献　特開２００１－３１３６７２（ＪＰ，Ａ）
特開平１１－２３４２６０（ＪＰ，Ａ）
特開２０００－２８７１９２（ＪＰ，Ａ）
特開２０００－３５８０２２（ＪＰ，Ａ）
特開２００１－３０９４４５（ＪＰ，Ａ）
特開２００１－３３１４４６（ＪＰ，Ａ）
電子情報通信学会誌，第８０巻，第４号，第３２４－３３０頁

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L 12/66
H04L 12/28
H04L 12/56
H04B 7/24-7/26
H04Q 7/00-7/38