(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2011-15327
(P2011-15327A)
(43)公開日　平成23年1月20日(2011.1.20)

(51)Int.Cl.		F I			テーマコード（参考）
H04W 12/02	(2009.01)	H04Q	7/00	181	5J104
H04W 12/04	(2009.01)	H04Q	7/00	182	5K067
H04W 84/12	(2009.01)	H04Q	7/00	630	
H04W 84/00	(2009.01)	H04Q	7/00	621	
H04W 8/02	(2009.01)	H04Q	7/00	141	

審査請求 未請求　請求項の数 6　ＯＬ　（全 35 頁）　最終頁に続く

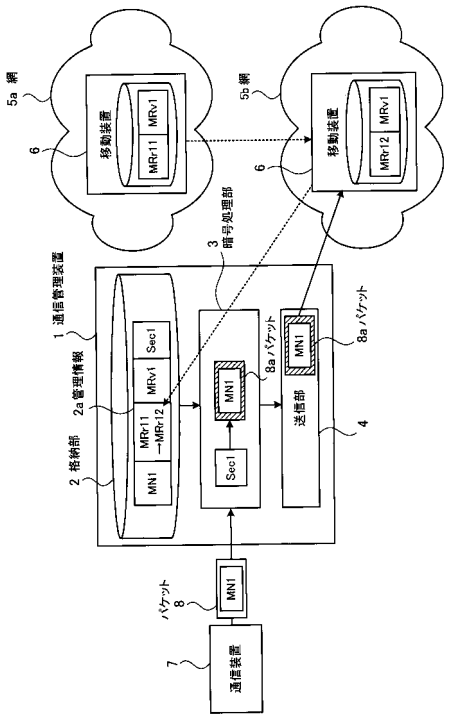
(21)出願番号　特願2009-159596 (P2009-159596)
(22)出願日　平成21年7月6日 (2009.7.6)

(71)出願人　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　宇式　一雅
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　藤野　信次
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】通信管理装置および通信管理プログラム

(57)【要約】
【課題】網間移動時の手順を短時間で行うこと。
【解決手段】通信管理装置１は、格納部２と、暗号処理部３と、送信部４とを有している。格納部２は、複数の網５ａ、５ｂ間を移動する移動装置６の、網５ａ、５ｂ毎に設定された第１のアドレスと網５ａ、５ｂ間で共通する第２のアドレスとこの第２のアドレスに対応するセキュリティ情報とを対応づけた管理情報２ａを格納する。暗号処理部３は、第２のアドレス宛のパケット８を受信した場合、受信した第２のアドレスに対応する管理情報２ａのセキュリティ情報に基づいてパケット８を暗号化する。送信部４は、暗号化が施されたパケット８ａを、受信した第２のアドレスに対応する第１のアドレス宛に送信する。
【選択図】図１



【特許請求の範囲】
【請求項１】
複数の網間を移動する移動装置の、前記網毎に設定された第１のアドレスと前記複数の網間で共通する第２のアドレスと前記第２のアドレスに対応するセキュリティ情報とを対応づけた管理情報を格納する格納部と、
前記第２のアドレス宛のパケットを受信した場合、受信した前記第２のアドレスに対応する前記管理情報のセキュリティ情報に基づいて前記パケットを暗号化する暗号処理部と、
前記暗号化が施されたパケットを、受信した前記第２のアドレスに対応する前記第１のアドレス宛に送信する送信部と、
を有することを特徴とする通信管理装置。
【請求項２】
前記移動装置からの通信確立要求に応じて前記セキュリティ情報を更新するか否かを判断する判断部をさらに有することを特徴とする請求項１記載の通信管理装置。
【請求項３】
前記判断部は、前記移動装置の移動速度に基づいて、前記セキュリティ情報を更新するか否かを判断することを特徴とする請求項２記載の通信管理装置。
【請求項４】
前記判断部は、前記移動装置と通信するプロトコル情報に基づいて、前記セキュリティ情報を更新するか否かを判断することを特徴とする請求項２または３記載の通信管理装置。
【請求項５】
前記判断部は、前記移動装置と通信する時間を測定した測定時間情報に基づいて、前記セキュリティ情報を更新するか否かを判断することを特徴とする請求項２ないし４のいずれかに記載の通信管理装置。
【請求項６】
コンピュータを、
複数の網間を移動する移動装置の、前記網毎に設定された第１のアドレスと前記複数の網間で共通する第２のアドレスと前記第２のアドレスに対応するセキュリティ情報とを対応づけた管理情報を格納する格納手段、
前記第２のアドレス宛のパケットを受信した場合、受信した前記第２のアドレスに対応する前記管理情報のセキュリティ情報に基づいて前記パケットを暗号化する暗号処理手段、
前記暗号化が施されたパケットを、受信した前記第２のアドレスに対応する前記第１のアドレス宛に送信する送信手段、
として機能させることを特徴とする通信管理プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は通信管理装置および通信管理プログラムに関する。
【背景技術】
【０００２】
ＩＰＳｅｃ（IP Security Protocol）等のＶＰＮ（Virtual Private Network）を用いて、例えば、車載移動局が、移動しながらサーバ等と無線通信を行う技術が知られている。
【０００３】
ＩＰＳｅｃ等のＶＰＮを用いた場合、ＶＰＮサーバ等の暗号化（復号）を行う装置は、移動局に割り当てられた実ＩＰアドレスと、当該実ＩＰアドレスが付与されたパケットの暗号化（復号）を行う際に用いる暗号鍵の対応関係を保持する。この対応関係は例えば、ＶＰＮを用いた通信を開始する前に設定される。

【０００４】
確立されたＶＰＮを用いて通信を行っている移動局が移動し、接続先の移動網を変える場合、移動先網のＤＨＣＰ（Dynamic Host Configuration Protocol）サーバ等から新規に実ＩＰアドレスが割り当てられる。
【０００５】
この際、移動局の移動前にＶＰＮサーバで管理されていた実ＩＰアドレスと暗号鍵等のセキュリティ情報の対応関係は一致しなくなる。
このため、移動先網から割り当てられた新たな実ＩＰアドレスに基づいてＶＰＮ通信を行うために、暗号鍵の再設定が必要となる。
【先行技術文献】
【特許文献】
【０００６】
【特許文献１】特開２００４－１３５２４８号公報
【発明の概要】
【発明が解決しようとする課題】
【０００７】
このセキュリティ情報の再設定を行うにあたっては、移動局とＶＰＮサーバとの間で数回の通信が必要となる。このとき、セキュリティ情報の再設定が完了するまで通信が中断してしまうという問題がある。
【０００８】
本発明はこのような点に鑑みてなされたものであり、網間移動時の手順を短時間で行うことができる通信管理装置および通信管理プログラムを提供することを目的とする。
【課題を解決するための手段】
【０００９】
上記目的を達成するために、開示の通信管理装置が提供される。この通信管理装置は、格納部と、暗号処理部と、送信部とを有している。
格納部は、複数の網間を移動する移動装置の、網毎に設定された第１のアドレスと複数の網間で共通する第２のアドレスとこの第２のアドレスに対応するセキュリティ情報とを対応づけた管理情報を格納する。
【００１０】
暗号処理部は、第２のアドレス宛のパケットを受信した場合、受信した第２のアドレスに対応する管理情報のセキュリティ情報に基づいてパケットを暗号化する。
送信部は、暗号化が施されたパケットを、受信した第２のアドレスに対応する第１のアドレス宛に送信する。
【発明の効果】
【００１１】
開示の通信管理装置によれば、移動装置の通信の遮断を防止することができる。
【図面の簡単な説明】
【００１２】
【図１】第１の実施の形態の通信管理装置の概要を示す図である。
【図２】第２の実施の形態のシステムを示す図である。
【図３】ＶＰＮサーバのハードウェア構成例を示す図である。
【図４】移動親局のハードウェア構成例を示す図である。
【図５】ＶＰＮサーバの機能を示すブロック図である。
【図６】通信エリアデータを示す図である。
【図７】サーバ側ＶＰＮ管理テーブルを示す図である。
【図８】移動親局の機能を示すブロック図である。
【図９】移動親局のＶＰＮ管理部が管理するデータ構造を示す図である。
【図１０】移動子局の機能を示すブロック図である。
【図１１】システムの処理を示すシーケンス図である。

【図１２】システムの処理を示すシーケンス図である。
【図１３】通信用のパケットを示す図である。
【図１４】ＶＰＮサーバのパケット転送処理を示すフローチャートである。
【図１５】固定局宛パケット受信時処理を示すフローチャートである。
【図１６】移動親局の処理を示すフローチャートである。
【図１７】移動親局の処理を示すフローチャートである。
【図１８】移動網の移動後に移動親局とＶＰＮサーバ間でやり取りされるパケットを示す図である。
【図１９】ＶＰＮサーバのアドレス通知受信処理を示す図である。
【図２０】暗号鍵交換処理要否判定処理を示すフローチャートである。
【図２１】暗号鍵交換処理要否判定処理の詳細を示すフローチャートである。
【図２２】第３の実施の形態のシステムを示す図である。
【図２３】第３の実施の形態の移動親局の処理を示すフローチャートである。
【図２４】第４の実施の形態のシステムを示す図である。
【図２５】第４の実施の形態のＶＰＮサーバの処理を示すフローチャートである。
【発明を実施するための形態】
【００１３】
以下、実施の形態を、図面を参照して詳細に説明する。
まず、実施の形態の通信管理装置の概要について説明し、その後、実施の形態をより具体的に説明する。
【００１４】
＜第１の実施の形態＞
図１は、第１の実施の形態の通信管理装置の概要を示す図である。
実施の形態の通信管理装置１は、例えば、ＶＰＮ等の仮想私設網を用いて通信装置間の通信を実現する装置である。
【００１５】
図１では通信装置として移動装置６と通信装置７を示している。
移動装置６は、例えば、交通機関（バス、電車）等に設置されており、交通機関の移動に伴って移動することにより、通信装置７との通信用の網（ネットワーク）５ａまたは網５ｂに接続する。
【００１６】
通信装置７は、例えば、移動装置６と同様に交通機関等に設置されている装置、または、所定の固定箇所に設置された装置である。
通信管理装置１は、格納部２と、暗号処理部３と、送信部４とを有している。
【００１７】
格納部２は、網５ａ、５ｂ間を移動する移動装置６が備える、網５ａ、５ｂ毎に設定された第１のアドレスと網５ａ、５ｂ間で共通する第２のアドレス（ＭＲｖ１）と第２のアドレス（ＭＲｖ１）に対応するセキュリティ情報（Ｓｅｃ１）とを対応づけた管理情報２ａを格納する。
【００１８】
ここで、格納部２に格納される第１のアドレスは、例えば、移動装置６の電源がＯＮされる度に、図示しないサーバ等から供給されるアドレスである。
また、このアドレスは、網５ａ、５ｂ間を移動すると、変化する。具体的には、移動装置６が、網５ａに接続されている状態では、第１のアドレスは、「ＭＲｒ１１」である。そして、移動装置６が、網５ａから網５ｂに移動したとき、第１のアドレスは、「ＭＲｒ１２」となる。
【００１９】
第２のアドレスは、移動装置６の通信用に仮想的に付与されたアドレスである。この第２のアドレスは、移動装置６の網５ａから網５ｂへの移動時に、移動装置６が通信管理装置１に通知するものである。

【００２０】
この情報は、移動装置６が、網５ａから網５ｂに移動したときも、また、網５ｂから網５ａに移動したときも、変わらず「ＭＲｖ１」である。
セキュリティ情報は、仮想私設網通信におけるデータの暗号化に必要な情報である。このセキュリティ情報は、例えば、暗号化方法の情報と暗号鍵の情報とを有している。
【００２１】
暗号処理部３は、通信装置７から第２のアドレス宛のパケット８を受信した場合、受信した第２のアドレスに対応する管理情報２ａのセキュリティ情報に基づいてパケット８を暗号化する。
【００２２】
ここで、図１では、移動装置６が網５ａから網５ｂに移動した場合でも、管理情報２ａのセキュリティ情報（Ｓｅｃ１）を変更せずに、そのセキュリティ情報（Ｓｅｃ１）を用いてパケット８を暗号化している。
【００２３】
換言すると、移動装置の第１のアドレスが、移動により、「ＭＲｒ１１」から「ＭＲｒ１２」に変わっても、第２のアドレス（ＭＲｖ１）は変わらないため、セキュリティ情報（Ｓｅｃ１）を変更せずに、そのセキュリティ情報（Ｓｅｃ１）を用いてパケット８を暗号化している。
【００２４】
送信部４は、暗号化が施されたパケット８ａを、受信した第２のアドレスＭＲｖ１に対応する第１のアドレス宛に送信する。
このように、第２のアドレスを設定することで、移動装置６の網５ａ、網５ｂ間の移動によるセキュリティ情報の変更処理を省略することができる。これにより、網５ａ、網５ｂ間の移動に伴う通信確立のための設定に必要な時間の短縮を図ることができる。従って、通信品質が向上する。
【００２５】
なお、セキュリティの質を保つために、例えば、通信管理装置１が、移動装置６との通信時間を計測しておき、この通信時間が一定時間を経過した場合には、セキュリティ情報（Ｓｅｃ１）を更新するようにするのが好ましい。
【００２６】
すなわち、通信装置７から第２のアドレス宛のパケット８を受信した場合にこの一定時間を経過していた場合は、更新したセキュリティ情報を用いて、暗号化の再設定（移動装置６と暗号化方式の交渉および暗号鍵の交換等）を行うようにするのが好ましい。
【００２７】
なお、この時間は、移動装置６が接続している網の種別（無線ＬＡＮ、セルラー等）によって、異なる時間に設定するようにしてもよい。
これにより、セキュリティの質を保つことができる。
【００２８】
但し、一定時間を経過していても、移動装置６の移動速度や、移動装置６の特定の通信プロトコル種別等によっては、暗号化の再設定を行わないようにしてもよい。
前者の場合、例えば、移動装置６の移動速度と網５ａ、５ｂの通信エリアから移動装置の通過時間を算出し、この通過時間が予め定められた時間よりも短い場合は、暗号化の再設定を行わないようにしてもよい。
【００２９】
後者の場合、例えば、通信プロトコルが、音声や、静止画像、動画像を通信するプロトコルである場合には、暗号化の再設定を行わないようにしてもよい。
これにより、通信が途絶えることを防止し、通信品質を保つことができる。
【００３０】
＜第２の実施の形態＞
以下、実施の形態をより具体的に説明する。

図２は、第２の実施の形態のシステムを示す図である。

【００３１】

システム１００は、ＩＰｓｅｃを使用したシステムであり、ＶＰＮサーバ１０と、固定局２０と、固定網３０と、中継網４０と、移動網（移動通信網）５１、５２と、移動親局６０ａと、移動子局７０ａとを有している。

【００３２】

ＶＰＮサーバ１０と固定局２０は、共通の固定網（ネットワーク）３０に接続されている。

ＶＰＮサーバ１０は、固定網３０外部の中継網４０から転送されるパケットを受信すると、受信したパケットの暗号を復号し、固定局２０にデータを転送する。また、固定局２０から転送されるパケットを受信すると、受信したパケットを暗号化し、中継網４０に転送する。

【００３３】

固定局２０は、例えば、会社内に設置されており、ＶＰＮサーバ１０を介して移動子局７０ａと通信を行う。

中継網４０は、固定網３０と移動網５１、５２に接続されている。この中継網４０は、ＶＰＮサーバ１０と移動網５１、５２間でやりとりされるデータを中継する機能を有している。

【００３４】

移動網５１、５２は、中継網４０に接続されている。この移動網５１、５２は、図示しない無線基地局を有しており、移動親局６０ａとの無線通信機能を実現する。

移動親局６０ａは、移動網５１、５２の通信範囲に入ることで、通信範囲に入った移動網５１、または、移動網５２に無線で接続する機能を有している。

【００３５】

この移動親局６０ａは、移動親局６０ａの通信範囲である移動局網８０内に存在する移動子局７０ａと、固定局２０との通信を中継する機能を有している。

移動親局６０ａは、特に限定されないが、例えば、自動車や電車等、図示しない交通機関にそれぞれ１つまたは複数設けられており、これらの交通機関の移動に伴って移動する。

【００３６】

移動子局７０ａは、例えば、通信機能を備えたユーザが携帯する装置である。移動子局７０ａとしては、例えば、通信機能を備えたＰＣ（Personal Computer）等が挙げられる。

【００３７】

なお、移動親局６０ａと移動子局７０ａとの通信は、有線通信であってもよいし、無線通信であってもよい。

このシステム１００では、ＶＰＮサーバ１０と移動親局６０ａとの間でＶＰＮが設定されて暗号化された情報が送受信される。

【００３８】

例えば、移動親局６０ａが設置された交通機関に移動子局７０ａを携帯した利用者が乗車（搭乗）し、ユーザが移動子局７０ａの通信機能を起動することにより、移動親局６０ａが移動子局７０ａのＶＰＮ確立要求を受信する。これにより、ＶＰＮ確立のための処理が行われ、ＶＰＮサーバ１０と移動親局６０ａとのＶＰＮが確立する。

【００３９】

この処理においては、移動親局６０ａは、移動網５１、５２毎に設定された移動親局６０ａのＩＰアドレス（以下、「実アドレス」と言う）に加え、移動網５１、５２間で共通する移動親局６０ａのＩＰアドレス（以下、「仮想ＶＰＮアドレス」と言う）を通知する。また、ＶＰＮサーバ１０は、通信に必要なセキュリティ情報を移動親局６０ａと交換する。

【００４０】

ＶＰＮ確立後、移動子局７０ａが固定局２０にアクセスした場合、移動親局６０ａは、移動親局６０ａが接続している移動網５１、または、移動網５２を介してＶＰＮサーバ１０との間でＶＰＮを用いたデータ通信を行う。

【００４１】

交通機関の移動に伴い、移動親局６０ａ、および、移動親局６０ａに接続された移動子局７０ａが、移動網５１、５２間を移動する。

この移動時に、ＶＰＮサーバ１０は、移動親局６０ａとのセキュリティ情報の再設定を行うか否かを決定する。この際、移動網５１、５２間で共通する移動親局６０ａの仮想ＶＰＮアドレスが通知されているため、この仮想ＶＰＮアドレスを用いることで、セキュリティ情報の再設定を行わず、移動前の移動網との間で設定されていたセキュリティ情報を用いて、移動後の移動網との間で通信を行うことができる。これにより、ＶＰＮの確立に必要な時間を短縮することができる。

【００４２】

なお、図２では、説明上１つのＶＰＮサーバ１０を図示しているが、ＶＰＮサーバは、複数設けられていてもよい。

また、図２では、移動親局６０ａに１つの移動子局７０ａが接続されている例を示しているが、移動親局６０ａに複数の移動子局が接続されていてもよい。

【００４３】

次に、ＶＰＮサーバ１０のハードウェア構成を説明する。

図３は、ＶＰＮサーバのハードウェア構成例を示す図である。

ＶＰＮサーバ１０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１０８を介してＲＡＭ（Random Access Memory）１０２、ハードディスクドライブ（ＨＤＤ:Hard Disk Drive）１０３、グラフィック処理装置１０４、入力インタフェース１０５、外部補助記憶装置１０６および通信インタフェース１０７が接続されている。

【００４４】

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が格納される。また、ＨＤＤ１０３内には、プログラムファイルが格納される。

【００４５】

グラフィック処理装置１０４には、モニタ１０４ａ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１０４ａ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１０５ａとマウス１０５ｂ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１０５ａやマウス１０５ｂから送られてくる信号を、バス１０８を介してＣＰＵ１０１に送信する。

【００４６】

外部補助記憶装置１０６は、記録媒体に書き込まれた情報を読み取ったり、記録媒体に情報を書き込んだりする。外部補助記憶装置１０６で読み書きが可能な記録媒体としては、例えば、磁気記録装置、光ディスク、光磁気記録媒体、半導体メモリ等が挙げられる。磁気記録装置としては、例えば、ＨＤＤ、フレキシブルディスク（ＦＤ）、磁気テープ等が挙げられる。光ディスクとしては、例えば、ＤＶＤ（Digital Versatile Disc）、ＤＶＤ－ＲＡＭ（Random Access Memory）、ＣＤ－ＲＯＭ（Compact Disc Read Only Memory）、ＣＤ－Ｒ（Recordable）／ＲＷ（ReWritable）等が挙げられる。光磁気記録媒体としては、例えば、ＭＯ（Magneto-Optical disk）等が挙げられる。

【００４７】

通信インタフェース１０７は、固定網３０に接続されている。通信インタフェース１０７は、固定網３０を介して、固定局２０や移動親局６０ａとの間でデータの送受信を行う。

【００４８】
次に、移動親局６０ａのハードウェア構成を説明する。
図４は、移動親局のハードウェア構成例を示す図である。
移動親局６０ａは、ＣＰＵ１６１によって装置全体が制御されている。ＣＰＵ１６１には、バス１６６を介してＲＡＭ１６２、メモリ１６３、通信インタフェース１６４、および、通信インタフェース１６５が接続されている。
【００４９】
ＲＡＭ１６２には、ＣＰＵ１６１に実行させるファームウェア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、ＲＡＭ１６２には、ＣＰＵ１６１による処理に必要な各種データが格納される。メモリ１６３には、アプリケーションプログラムが格納される。また、メモリ１６３内には、ファームウェアやプログラムファイルが格納される。これらファームウェアの設定は、外部から変更可能になっていてもよい。
【００５０】
通信インタフェース１６４は、移動局網８０に接続されている。通信インタフェース１６４は、移動局網８０を介して、移動子局７０ａとの間でデータの送受信を行う。
通信インタフェース１６５は、移動網５１、または、移動網５２に接続される。通信インタフェース１６５は、接続された移動網５１、または、移動網５２を介して、固定局２０との間でデータの送受信を行う。
【００５１】
以上のようなハードウェア構成によって、本実施の形態の処理機能を実現することができる。このようなハードウェア構成のＶＰＮサーバ１０内には、以下のような機能が設けられる。
【００５２】
次に、ＶＰＮサーバの機能を説明する。
図５は、ＶＰＮサーバの機能を示すブロック図である。
ＶＰＮサーバ１０は、受信部１１と、送信部１２と、ＶＰＮ管理部１３と、暗号処理部１４と、カプセル化処理部１５と、データ格納部１６とを有している。
【００５３】
受信部１１は、固定局２０、ないし、移動親局６０ａ、および、移動子局７０ａから送信されたパケットを受信する。また、受信部１１は、移動親局６０ａから受信した制御メッセージを分析する。
【００５４】
送信部１２は、固定局２０、ないし、移動親局６０ａおよび移動子局７０ａにカプセル化（後述）されたパケットを送信する。また、移動親局６０ａに送信すべき制御メッセージを生成し、送信する。
【００５５】
ＶＰＮ管理部１３は、現在、ＶＰＮ接続が確立している移動子局７０ａを管理する。
具体的には、ＶＰＮ管理部１３は、移動親局６０ａから通知される移動子局７０ａを管理するためのＶＰＮに関する各種アドレス、セキュリティ情報の対応関係を管理するテーブル（サーバ側ＶＰＮ管理テーブル）を有している。この管理テーブルの内容については後に詳述する。
【００５６】
ＶＰＮ管理部１３は、パケットを受信すると、受信したパケットに含まれている移動親局６０ａの仮想ＶＰＮアドレスが、サーバ側ＶＰＮ管理テーブルに登録されているか否かを判定する。登録されていない場合、受信したパケットに含まれている移動親局６０ａの実アドレス、仮想ＶＰＮアドレス等をサーバ側ＶＰＮ管理テーブルに登録する。
【００５７】
また、ＶＰＮ管理部１３は、ＶＰＮの確立に際し、移動親局６０ａとの間で、暗号化方式の交渉、および暗号鍵の交換処理を実行する。そして、この処理により決定された暗号化方式、暗号鍵をセキュリティ情報としてサーバ側ＶＰＮ管理テーブルに登録する。また

、同時に受信した移動速度や移動網種別も登録する。

【００５８】

一方、受信したパケットに含まれている移動親局の仮想ＶＰＮアドレスが、サーバ側ＶＰＮ管理テーブルに登録されている場合、ＶＰＮ管理部１３は、受信したパケットに含まれている仮想ＶＰＮアドレスに対応するサーバ側ＶＰＮ管理テーブル内のエントリを検索する。そして、一致するエントリを更新する。

【００５９】

暗号処理部１４は、移動親局６０ａに送信されるパケットに対する暗号化処理を行う。また、暗号処理部１４は、固定局２０に送信されるパケットに対する復号処理を行う。

カプセル化処理部１５は、移動親局６０ａに送信されるパケットに対するカプセル化（encapsulation）処理を行う。具体的には、送信されるパケットにＩＰヘッダを付加する。

【００６０】

また、カプセル化処理部１５は、固定局２０に送信されるパケットに対するデ・カプセル化処理を行う。

データ格納部１６は、通信網種別に応じた典型的なセルサイズを示すデータ（通信エリアデータ）を保持する。また、暗号鍵の交換処理に要する時間（例えば、平均処理時間）も保持する。さらに、移動網５１、５２の在圏時間内において鍵交換の実行中に通信不可となることが許容される時間の百分率Ｔ（％）を閾値として保持する。

【００６１】

図６は、通信エリアデータを示す図である。

通信エリアデータは、テーブル化されている。

通信エリア管理テーブル１６ａには、移動網種別、および、セルサイズの欄が設けられている。横方向に並べられた情報同士が互いに関連づけられている。

【００６２】

移動網種別の欄には、移動網の種別を識別する情報が設定されている。

セルサイズの欄には、通信エリアの広さを示す値が設定されている。

次に、ＶＰＮサーバ１０が管理するサーバ側ＶＰＮ管理テーブルを説明する。

【００６３】

図７は、サーバ側ＶＰＮ管理テーブルを示す図である。

サーバ側ＶＰＮ管理テーブル１３ａは、例えば、ＶＰＮサーバ１０が固定局２０から受信した移動子局７０ａ宛のパケットの転送先となる移動親局６０ａ、移動親局６０ａの仮想ＶＰＮアドレスと実アドレスの対応関係の管理に使用される。

【００６４】

また、サーバ側ＶＰＮ管理テーブル１３ａは、移動親局６０ａとの間で確立しているＶＰＮで用いられるセキュリティ情報の対応関係の管理に使用される。

サーバ側ＶＰＮ管理テーブル１３ａには、移動子局アドレス、移動親局仮想ＶＰＮアドレス、移動親局実アドレス、ＶＰＮセキュリティ情報、更新時刻、データ種別、移動速度、および、移動網種別の欄が設けられており、横方向に並べられた情報同士が互いに関連づけられている。

【００６５】

移動子局アドレスの欄には、移動子局が接続されている移動親局と関係付けられる移動子局固有のアドレスが設定されている。

移動親局仮想ＶＰＮアドレスの欄には、移動親局６０ａ、および、図示していないその他の移動親局の仮想ＶＰＮアドレスが設定されている。このアドレスは、端末の位置にかかわらず、一定のアドレスである。

【００６６】

移動親局実アドレスの欄には、移動網５１、または、移動網５２で割り当てられる、移動親局の実アドレスが設定されている。この実アドレスは、移動網５１、または、移動網５２から実アドレスが割り当てられた際に移動親局からＶＰＮサーバ１０に対して通知さ

れる。
【００６７】
ＶＰＮセキュリティ情報の欄には、ＶＰＮサーバ１０と移動親局６０ａ、および、図示していないその他の移動親局との間で確立されているＶＰＮで用いられている暗号方式、並びに、暗号鍵等のセキュリティ情報が設定されている。
【００６８】
更新時刻の欄には、暗号鍵が最近更新された時刻情報が設定されている。この時刻情報は、暗号鍵の更新の要否を判定するために使用される。
データ種別の欄には、設定されたＶＰＮを用いて、どのようなデータがやり取りされているかを示す情報が設定されている。
【００６９】
例えば、ＵＤＰ（User Datagram Protocol）であれば、動画像データの送受信を行っている可能性のあることを示している。このデータ種別は、暗号鍵の更新の要否を判定するために使用される。
【００７０】
なお、データ種別は、ＩＰヘッダのプロトコル・フィールドの値を参照することで把握することができる。ＶＰＮサーバ１０の受信部１１は、固定局２０から移動子局７０ａ宛のパケットを受信した際に、ＩＰヘッダの当該フィールドを参照することができる。また、ＶＰＮサーバ１０の送信部１２は、移動子局７０ａから固定局２０宛の（デ・カプセル化および復号された）パケットを固定網３０に転送する際に、ＩＰヘッダの当該フィールドを参照することができる。
【００７１】
移動速度の欄には、移動親局の移動速度が設定されている。
移動網種別の欄には、移動親局の移動網種別が設定されている。
なお、図７では、移動子局７０ａから固定局２０向け、固定局２０から移動子局７０ａ向けに送信されるデータ種別を分けていないが、これらを区別し得るように分けてもよい。
【００７２】
次に、移動親局６０ａの機能を説明する。
図８は、移動親局の機能を示すブロック図である。
移動親局６０ａは、受信部６１と、送信部６２と、ＶＰＮ管理部６３と、移動処理部６４と、暗号処理部６５と、カプセル化処理部６６とを有している。
【００７３】
受信部６１は、固定局２０、ＶＰＮサーバ１０、または、移動子局７０ａから送信されたパケットを受信する。また、ＶＰＮサーバ１０から受信した制御メッセージを分析する。
【００７４】
送信部６２は、固定局２０、ＶＰＮサーバ１０、または、移動子局７０ａにパケットを送信する。また、送信部６２は、ＶＰＮサーバ１０に送信すべき制御メッセージを生成する。そして生成した制御メッセージをＶＰＮサーバ１０に送信する。
【００７５】
ＶＰＮ管理部６３は、ＶＰＮに関する各種アドレス、セキュリティ情報の対応関係を管理する。
移動処理部６４は、移動網５１、５２における実アドレスを取得する。また、ＶＰＮサーバ１０への実アドレスの通知などの移動に関する処理を行う。
【００７６】
暗号処理部６５は、固定局２０、ＶＰＮサーバ１０に送信されるパケットに対する暗号化処理、および、移動子局７０ａに送信されるパケットに対する復号処理を行う。
カプセル化処理部６６は、固定局２０、ＶＰＮサーバ１０に送信されるパケットに対するカプセル化処理を行う。

【００７７】
　また、カプセル化処理部６６は、移動子局７０ａに送信されるパケットに対するデ・カプセル化処理を行う。
　次に、ＶＰＮ管理部６３が管理するデータ構造を説明する。
【００７８】
　図９は、移動親局のＶＰＮ管理部が管理するデータ構造を示す図である。
　この親局側ＶＰＮ管理テーブル６３ａは、例えば、移動親局６０ａが移動子局７０ａから受信した固定局２０宛のパケットの転送先となるＶＰＮサーバ１０、および、当該ＶＰＮサーバ１０との間で設定されているＶＰＮで用いられるセキュリティ情報の対応関係の管理に使用される。
【００７９】
　親局側ＶＰＮ管理テーブル６３ａには、移動子局アドレス、ＶＰＮサーバアドレス、ＶＰＮセキュリティ情報の欄が設けられており、横方向に並べられた情報同士が互いに関連づけられている。
【００８０】
　移動子局アドレスの欄には、移動親局６０ａ自身が接続する移動子局固有のアドレスが設定されている。
　ＶＰＮサーバアドレスの欄には、移動子局アドレスの欄に設定されている移動子局とＶＰＮが確立しているＶＰＮサーバ固有のアドレスが設定されている。
【００８１】
　ＶＰＮセキュリティ情報の欄には、ＶＰＮサーバと移動親局６０ａとの間で確立されているＶＰＮで用いられている暗号方式、および、暗号鍵等のセキュリティ情報が設定されている。
【００８２】
　次に、移動子局７０ａの機能を説明する。
　図１０は、移動子局の機能を示すブロック図である。
　移動子局７０ａは、受信部７１と、送信部７２と、ＶＰＮ管理部７３とを有している。
【００８３】
　受信部７１は、固定局および移動子局から送信されたパケットを受信する。また、移動親局６０ａから受信した制御メッセージを分析・処理する。
　送信部７２は、固定局２０、または、他の移動子局にパケットを送信する。また、移動親局６０ａに送信すべき制御メッセージを生成し、送信する。
【００８４】
　ＶＰＮ管理部７３は、移動親局６０ａに対してＶＰＮの確立または切断を要求する。
　次に、システム１００の通信処理を説明する。
　＜システム全体の通信処理＞
　図１１、図１２は、システムの処理を示すシーケンス図である。
【００８５】
　以下に示す処理は、移動網５１に接続する移動親局６０ａ、および、移動子局７０ａがＶＰＮを確立して通信中状態に遷移した後、確立したＶＰＮを維持したまま移動網５２に移動し、確立したＶＰＮを切断する場合の処理である。
【００８６】
　［ステップＳ１］
　移動網５１は、移動網５１自身の網情報（例えば、ネットワーク・アドレス、ＩＰアドレス割当のためのＤＨＣＰサーバ（図示せず）のアドレス等）を周期的に報知する。
【００８７】
　［ステップＳ２］
　移動網５２も、移動網５１と同様、移動網５２自身の網情報を周期的に報知する。但し、図１１に示すように、移動網５２からの報知は、移動親局６０ａには届いていない。
【００８８】

［ステップＳ３］
移動網５１に接続する移動親局６０ａは、移動網５１からの網情報を受信すると、移動網５１の無線基地局に対して、リンク確立要求を送信する。
【００８９】
［ステップＳ４］
移動網５１の無線基地局は、移動親局６０ａに対してリンク確立応答を送信して、リンクを確立する。
【００９０】
［ステップＳ５］
移動親局６０ａは、ステップＳ１で通知されたＤＨＣＰサーバに対して、ＩＰアドレスの割当要求を送信する。
【００９１】
［ステップＳ６］
移動網５１のＤＨＣＰサーバは、移動親局６０ａに対して移動親局６０ａの実アドレス（ＭＲｒ１１）を割り当てる。
【００９２】
［ステップＳ７］
移動子局７０ａが移動親局６０ａに対して、ＶＰＮ確立要求を送信する。このＶＰＮ確立要求には、移動子局７０ａの通信相手である固定局２０と接続するＶＰＮサーバ１０の実アドレス（ＶＰＮＳ１）、および、移動子局７０ａ自身の実アドレス（ＭＮ１）が含まれている。
【００９３】
［ステップＳ８］
移動親局６０ａは、移動子局７０ａからの要求に従い、ＶＰＮサーバ１０に対して移動親局アドレス通知を送信する。この移動親局アドレスには、移動親局６０ａの仮想ＶＰＮアドレス（ＭＲｖ１）、実アドレス（ＭＲｒ１１）、移動網５１の移動網種別、および、移動速度が含まれている。これらの情報は、サーバ側ＶＰＮ管理テーブル１３ａに登録される。
【００９４】
［ステップＳ９、ステップＳ１０］
移動親局６０ａとＶＰＮサーバ１０の間で、暗号化方式の交渉を行う。なお、暗号化方法としては、特に限定されず、例えば、公知のものを用いることができる。
【００９５】
［ステップＳ１１、ステップＳ１２］
暗号鍵の交換が必要な場合、移動親局６０ａとＶＰＮサーバ１０の間で、暗号鍵の交換を行う。
【００９６】
［ステップＳ１３］
ＶＰＮサーバ１０は、移動親局６０ａに対して、移動親局アドレス通知応答を送信する。
【００９７】
［ステップＳ１４］
移動親局６０ａは、移動親局６０ａに接続されている移動子局７０ａのアドレスをＶＰＮサーバに通知するための移動子局アドレス追加要求をＶＰＮサーバ１０に送信する。この移動子局アドレス追加要求には、移動親局６０ａの仮想ＶＰＮアドレス（ＭＲｖ１）、実アドレス（ＭＲｒ１１）、および、移動子局７０ａ自身の実アドレス（ＭＮ１）が含まれている。
【００９８】
［ステップＳ１５］
ＶＰＮサーバ１０は、移動親局６０ａのアドレス（仮想ＶＰＮアドレスや実アドレス）

と関連付けて移動子局７０ａのアドレスをサーバ側ＶＰＮ管理テーブル１３ａに登録し、移動親局６０ａに対して移動子局アドレス追加応答を送信する。

【００９９】

［ステップＳ１６］

移動親局６０ａは、移動子局７０ａに対して、ＶＰＮ確立応答を送信する。

［ステップＳ１７］

移動子局７０ａは、固定局２０との間で、ＶＰＮを介してＩＰパケットの送受信を行う。このとき、移動親局６０ａとＶＰＮサーバ１０は、移動親局６０ａとＶＰＮサーバ１０との間でやり取りされるＩＰパケットに対して、ステップＳ１１、Ｓ１２で決められた暗号鍵を用いて、暗号化処理および復号処理を行う。なお、やり取りされるパケットの構成は後述する。

【０１００】

［ステップＳ１８］

移動親局６０ａおよび移動子局７０ａが通信中に移動して、移動網５２に接近すると、移動網５２から網情報を受信し始める。これによって、移動親局６０ａが移動網５２に移動することを検出する。

【０１０１】

［ステップＳ１９］

移動網５２に在圏する移動親局６０ａは、移動網５２からの網情報を受信すると、移動網５２の無線基地局に対して、リンク確立要求を送信する。

【０１０２】

［ステップＳ２０］

移動網５２の無線基地局は、移動親局６０ａに対してリンク確立応答を送信して、リンクを確立する。

【０１０３】

［ステップＳ２１］

移動親局６０ａは、ステップＳ１で通知されたＤＨＣＰサーバに対して、ＩＰアドレスの割当要求を送信する。

【０１０４】

［ステップＳ２２］

移動網５２のＤＨＣＰサーバは、移動親局６０ａに対して移動親局６０ａの実アドレス（ＭＲｒ１２）を割り当てる。

【０１０５】

［ステップＳ２３］

移動親局６０ａは、移動親局アドレス通知をＶＰＮサーバ１０に送信する。この移動親局アドレス通知は、移動親局６０ａ自身の実アドレス（ＭＲｒ１２）が変わったことを、ＶＰＮサーバ１０に通知するものである。

【０１０６】

この移動親局アドレス通知には、移動親局６０ａの仮想ＶＰＮアドレス（ＭＲｖ１）、実アドレス（ＭＲｒ１２）、移動網５２の種別、および、移動速度が含まれている。

［ステップＳ２４］

ＶＰＮサーバ１０は、ステップＳ１５で登録した情報のうち、移動親局６０ａの実アドレス（ＭＲｒ１１）をステップＳ２３で通知されたアドレス（ＭＲｒ１２）に変更する。この際、ステップＳ１１、Ｓ１２で交換された暗号鍵を更新するためにステップＳ１１、Ｓ１２に示した暗号鍵の交換処理を行うか否かを判定する。そして、暗号鍵の交換処理を行わないと判定した場合、すなわち、セキュリティ情報の更新が必要でないと判定した場合、移動親局６０ａに対して移動親局アドレス通知応答を送信する。

【０１０７】

図１１、図１２に示す全体処理では、判定の結果、ステップＳ９、Ｓ１０に示す暗号化方式の交渉、および、ステップＳ１１、Ｓ１２に示す暗号鍵の交換を行わない例を示して

いる。これにより、ＶＰＮの確立に必要な時間を短縮することができる。

【０１０８】

なお、暗号鍵の交換処理が必要と判断した場合には、移動親局アドレス通知応答の前にステップＳ１１～Ｓ１２と同様の処理を実行する。

［ステップＳ２５］

移動親局６０ａおよびＶＰＮサーバ１０は、移動親局６０ａの新たな実アドレス（ＭＲｒ１２）を用いて、移動子局７０ａおよび固定局２０の間でやり取りされるパケットをカプセル化して、移動網５２に移動後もＶＰＮを維持する。

【０１０９】

［ステップＳ２６］

移動子局７０ａは、移動親局６０ａに対して、ＶＰＮ切断要求を送信する。この要求の送信タイミングとしては、特に限定されないが、例えば、ユーザが移動子局７０ａを操作し、通信終了を選択した場合等が挙げられる。

【０１１０】

このＶＰＮ切断要求には、ＶＰＮサーバ（ＶＰＮサーバ１０）の実アドレス（ＶＰＮＳ１）、および、移動子局７０ａの実アドレス（ＭＮ１）が含まれている。

［ステップＳ２７］

移動親局６０ａは、移動子局７０ａの通信のためにＶＰＮを確立していたＶＰＮサーバ１０に対して、通信を終了した移動子局のアドレスの削除を要求する移動子局アドレス削除要求を送信する。この移動子局アドレス削除要求には、移動親局６０ａの仮想ＶＰＮアドレス（ＭＲｖ１）、実アドレス（ＭＲｒ１２）、および、移動子局７０ａの実アドレス（ＭＮ１）が含まれている。

【０１１１】

［ステップＳ２８］

ＶＰＮサーバ１０は、受け取った移動親局６０ａの仮想ＶＰＮアドレス（ＭＲｖ１）、および、実アドレス（ＭＲｒ１２）に対応して登録されている移動子局のアドレス（ＭＮ１）をサーバ側ＶＰＮ管理テーブル１３ａから削除する。そして、移動親局６０ａに対して移動子局アドレス削除を完了した旨の通知である移動子局アドレス削除応答を送信する。この移動子局アドレス削除応答には、移動親局６０ａの仮想ＶＰＮアドレス（ＭＲｖ１）、および、実アドレス（ＭＲｒ１２）が含まれている。

【０１１２】

［ステップＳ２９］

移動親局６０ａは、ステップＳ８～Ｓ１３において確立されたＶＰＮが、移動子局７０ａ以外の移動子局によって使用されていないことを認識すると、ＶＰＮサーバ１０に対して移動親局アドレス削除要求を送信する。

【０１１３】

［ステップＳ３０］

ＶＰＮサーバ１０は、ステップＳ８～Ｓ１３において確立されたＶＰＮに関する情報をサーバ側ＶＰＮ管理テーブル１３ａから削除する。そして、移動親局６０ａに対して移動親局のアドレス削除を完了した旨の移動親局アドレス削除応答を送信する。

【０１１４】

［ステップＳ３１］

移動親局６０ａは、移動子局７０ａに対して、ＶＰＮ切断応答を送信する。

なお、ＶＰＮサーバ１０を使用して図示しない他の移動子局が通信している場合は、ステップＳ２７、Ｓ２８の処理のみを行い、ステップＳ２９、Ｓ３０の処理は行わない。

【０１１５】

以上で全体処理の説明を終了する。

なお、本実施の形態では、移動子局７０ａからＶＰＮ確立要求が発生した際の暗号化方式の交渉、および暗号鍵の交換処理として簡略化した処理を示しているが、ＩＫＥ（Internet Key Exchange）等の標準的な処理が用いられてもよい。

【０１１６】
なお、本実施の形態では、ステップＳ８～Ｓ１５の信号や、ステップＳ１８～Ｓ２４の信号を別個に送信する場合を示したが、これに限定されない。例えば、ステップＳ８に示す移動親局アドレス通知を送信の際に、ステップＳ１４に示す移動子局アドレス追加要求を同時に送るようにしてもよい。
【０１１７】
また、本実施の形態では、移動親局６０ａの移動速度情報を移動親局アドレス通知に含むようにしている。この移動速度情報は、例えば、移動親局６０ａが設置された交通機関から取得したり、移動親局６０ａにＧＰＳ（Global Positioning System）受信機を搭載し、その測位情報から速度情報を算出したりすることにより、取得することができる。
【０１１８】
また、本実施の形態では、セキュリティ情報（暗号鍵）の設定は移動網５１から移動網５２に移動したときに行うようにしている。
しかし、これに限らず、ＶＰＮサーバ１０のＶＰＮ管理情報のうち、最近鍵交換を行った時刻からの経過時間に従い、ＶＰＮセキュリティ情報（暗号鍵）の設定処理を起動してもよい。
【０１１９】
具体的には、その経過時間が一定の閾値時間を超えた場合には、移動網５２に移動しない場合でもＶＰＮセキュリティ情報（暗号鍵）の設定処理を起動するようにしてもよい。
次に、ステップＳ１７にてやり取りされる通信用のパケットを説明する。
【０１２０】
図１３は、通信用のパケットを示す図である。
図１３（ａ）は、固定局２０から移動親局６０ａを経由した移動子局７０ａ宛のパケットを示している。
【０１２１】
パケットＰ１は、先頭側（図１３（ａ）の左側）から宛先アドレスＡＤ１、送信元アドレスＡＤ２、ＩＰＳｅｃ　ＥＳＰ（IP Security Encapsulating Security Payload）ヘッダＨ１、宛先アドレスＡＤ３、送信元アドレスＡＤ４、および、データＤ１を有している。
【０１２２】
宛先アドレスＡＤ１には、移動親局６０ａの実アドレスが設定される。図１３（ａ）では、実アドレス（ＭＲｒ１１）が設定されている。
送信元アドレスＡＤ２には、ＶＰＮサーバ１０の実アドレスが設定される。図１３（ａ）では、実アドレス（ＶＰＮＳ１）が設定されている。
【０１２３】
ＩＰＳｅｃ　ＥＳＰヘッダＨ１には、セキュリティ情報を識別する情報等が設定される。
宛先アドレスＡＤ３には、移動子局７０ａの実アドレスが設定される。図１３（ａ）では、移動子局７０ａの実アドレス（ＭＮ１）が設定されている。
【０１２４】
送信元アドレスＡＤ４には、固定局２０の実アドレス（ＣＮ１）が設定される。図１３（ａ）では、固定局２０の実アドレス（ＣＮ１）が設定されている。
データＤ１には、移動子局７０ａに転送するデータが格納されている。
【０１２５】
このパケットＰ１のうち、宛先アドレスＡＤ３、送信元アドレスＡＤ４、および、データＤ１は、固定局２０が送信したパケットである。なお、宛先アドレスＡＤ３、送信元アドレスＡＤ４、および、データＤ１は、暗号処理部１４によって暗号化されている。
【０１２６】
また、パケットＰ１のうち、宛先アドレスＡＤ１、および、送信元アドレスＡＤ２が、カプセル化処理部１５により追加されるパケットＰ１の移動親局６０ａの実アドレス宛パ

ケットのＩＰヘッダである。
【０１２７】
図１３（ｂ）は、移動子局７０ａから固定局２０宛のパケットを示している。
パケットＰ２は、先頭側（図１３（ｂ）の左側）から宛先アドレスＡＤ５、送信元アドレスＡＤ６、ＩＰＳｅｃ　ＥＳＰヘッダＨ２、宛先アドレスＡＤ７、送信元アドレスＡＤ８、および、データＤ２を有している。
【０１２８】
このうち、宛先アドレスＡＤ５、および、送信元アドレスＡＤ６がパケットＰ２のＶＰＮサーバ１０宛パケットのＩＰヘッダである。
宛先アドレスＡＤ５には、ＶＰＮサーバ１０の実アドレスが設定される。図１３（ｂ）では、実アドレス（ＶＰＮＳ１）が設定されている。
【０１２９】
送信元アドレスＡＤ６には、移動親局６０ａの実アドレスが設定される。図１３（ｂ）では、実アドレス（ＭＲｒ１１）が設定されている。
ＩＰＳｅｃ　ＥＳＰヘッダＨ２には、セキュリティ情報を識別する情報等が設定される。
【０１３０】
宛先アドレスＡＤ７には、固定局２０の実アドレスが設定される。図１３（ｂ）では、実アドレス（ＣＮ１）が設定されている。
送信元アドレスＡＤ８には、移動子局７０ａの実アドレスが設定される。図１３（ｂ）では、実アドレス（ＭＮ１）が設定されている。
【０１３１】
データＤ２は、固定局２０に転送するデータが格納されている。
このパケットＰ２のうち、宛先アドレスＡＤ７、送信元アドレスＡＤ８、および、データＤ２は、移動子局７０ａが送信したパケットである。なお、宛先アドレスＡＤ７、送信元アドレスＡＤ８、および、データＤ２は、暗号処理部６５によって暗号化されている。
【０１３２】
また、宛先アドレスＡＤ５、および、送信元アドレスＡＤ６が、カプセル化処理部６６によって付与されたＶＰＮサーバ１０宛パケットのＩＰヘッダである。
次に、ＶＰＮサーバ１０が、固定局２０から移動子局７０ａ宛のパケットＰ１を受信したときの処理を説明する。
【０１３３】
＜ＶＰＮサーバのパケット転送処理＞
図１４は、ＶＰＮサーバのパケット転送処理を示すフローチャートである。
［ステップＳ４１］
ＶＰＮサーバ１０の受信部１１が、固定局２０から送信された移動子局７０ａ宛のパケットＰ１を受信する。その後、ステップＳ４２に遷移する。
【０１３４】
［ステップＳ４２］
パケットＰ１の宛先である移動子局７０ａのアドレスを用いて、サーバ側ＶＰＮ管理テーブル１３ａから移動子局７０ａと接続している移動親局６０ａの仮想ＶＰＮアドレス（ＭＲｖ１）、実アドレス（ＭＲｒ１１）、および、セキュリティ情報を求める。
【０１３５】
そして、ＶＰＮ管理部１３が、サーバ側ＶＰＮ管理テーブル１３ａを参照する。そして、仮想ＶＰＮアドレス（ＭＲｖ１）に対応して保持されるＶＰＮセキュリティ情報（暗号方式１および暗号鍵１）を暗号処理部１４に通知する。
【０１３６】
その後、暗号処理部１４が、ＶＰＮ管理部１３から通知されたＶＰＮセキュリティ情報（暗号方式１および暗号鍵１）に従って、固定局２０から送信されたパケットを暗号化する。

【０１３７】
そして、カプセル化処理部１５が、暗号化されたパケットをカプセル化する。具体的には、暗号化されたパケットに、送信元アドレスとしてＶＰＮサーバ１０自身の実アドレス（ＶＰＮＳ１）を付与する。宛先として移動子局７０ａに接続されている移動親局６０ａの実アドレス（ＭＲｒ１１）を付与する。そして、ＩＰＳｅｃ　ＥＳＰヘッダを付与する。その後、ステップＳ４３に遷移する。
【０１３８】
［ステップＳ４３］
ＶＰＮサーバ１０の送信部１２は、ステップＳ４２で暗号化およびカプセル化されたパケットＰ１を中継網４０に送出する。
【０１３９】
以上で処理を終了する。
なお、パケットＰ１を受信した移動親局６０ａは、ステップＳ４１～Ｓ４３の手順の逆の手順（復号、デ・カプセル化）を行う。そして、処理の結果得られたパケットを移動子局７０ａに転送する。
【０１４０】
次に、ＶＰＮサーバ１０が、移動子局７０ａから固定局２０宛のパケットＰ２を受信したときの処理（固定局宛パケット受信時処理）を説明する。
＜固定局宛パケット受信時処理＞
図１５は、固定局宛パケット受信時処理を示すフローチャートである。
【０１４１】
［ステップＳ５１］
ＶＰＮサーバ１０の受信部１１が、移動親局６０ａから送信された、固定局２０宛のパケットがカプセル化されたパケットＰ２を受信する。その後、ステップＳ５２に遷移する。
【０１４２】
［ステップＳ５２］
ＶＰＮ管理部１３が、当該パケットＰ２の送信元である移動親局６０ａの実アドレスを用いて、サーバ側ＶＰＮ管理テーブル１３ａから当該移動親局の仮想ＶＰＮアドレス、ＶＰＮセキュリティ情報を求める。
【０１４３】
そして、カプセル化処理部１５が、移動子局７０ａから送信されたパケットＰ２をデ・カプセル化する。そして、暗号処理部１４が、デ・カプセル化されたパケットを復号する。その後、ステップＳ５３に遷移する。
【０１４４】
［ステップＳ５３］
ＶＰＮサーバ１０の送信部１２は、ステップＳ５２で復号およびデ・カプセル化されたパケットを固定網３０に送出する。その後、処理を終了する。
【０１４５】
以上で、固定局宛パケット受信時処理の説明を終了する。
次に、全体処理における各装置の処理を詳しく説明する。
図１６および図１７は、移動親局の処理を示すフローチャートである。
【０１４６】
［ステップＳ６１］
まず、移動親局６０ａの電源が投入されると、移動処理部６４が、当該移動親局６０ａが在圏する移動網において、無線基地局との間でリンクを確立すると共に、ＤＨＣＰサーバ等から実アドレスを取得する。その後、ステップＳ６２に遷移する。
【０１４７】
［ステップＳ６２］
次に、受信部６１が、移動親局６０ａに接続した移動子局７０ａから、ＶＰＮ確立要求

を受信したか否かを判定する。

【０１４８】

受信した場合はステップＳ６３に遷移する。受信していない場合は、ステップＳ６２に遷移し、受信を待機する。

［ステップＳ６３］

ＶＰＮ管理部６３が、受信したＶＰＮ確立要求に含まれている移動子局７０ａのアドレス、およびＶＰＮを確立するＶＰＮサーバ１０のアドレスを親局側ＶＰＮ管理テーブル６３ａに登録する。その後、ステップＳ６４に遷移する。

【０１４９】

［ステップＳ６４］

送信部６２が、ステップＳ６２で移動子局７０ａから通知されたＶＰＮサーバ１０に対して、移動親局６０ａの実アドレスおよび仮想ＶＰＮアドレスを通知するための移動親局アドレス通知を送信する。その後、ステップＳ６５に遷移する。

【０１５０】

前述したように、当該通知には、移動親局６０ａの移動速度、および接続する移動網の種別（無線ＬＡＮ、携帯電話網等）も含まれている。ここでは当該仮想ＶＰＮアドレスは予め移動親局６０ａに設定されている場合について説明する。なお、これに限らず、当該通知を受信したＶＰＮサーバ１０が、仮想ＶＰＮアドレスを動的に割り当て、そのアドレスが応答通知等によって移動親局６０ａに通知されるようにしてもよい。

【０１５１】

［ステップＳ６５］

ＶＰＮサーバ１０とのやり取りによりＶＰＮの確立に必要なセキュリティ情報（暗号方式、暗号鍵等）を取得し、設定する。その後、ステップＳ６６に遷移する。

【０１５２】

本実施の形態ではＶＰＮ確立時にセキュリティ情報の設定を行う場合について説明するが、これに限らず、後述するように、セキュリティ設定の要否がＶＰＮサーバ１０によって判断され、必要な場合にのみセキュリティ設定が行われるようにしてもよい。

【０１５３】

［ステップＳ６６］

ＶＰＮ管理部６３が、ステップＳ６５で決定されたセキュリティ情報を親局側ＶＰＮ管理テーブル６３ａに登録する。その後、ステップＳ６７に遷移する。

【０１５４】

［ステップＳ６７］

受信部６１が、移動親局アドレス通知応答を受信すると、送信部６２が、移動子局アドレス追加要求をＶＰＮサーバ１０に送信する。その後、ステップＳ６８に遷移する。

【０１５５】

なお、本実施の形態では移動子局７０ａのアドレスは、移動子局７０ａに固定的に設定される場合を説明するが、次のようにして移動子局７０ａのアドレスをＶＰＮサーバ１０が動的に割り当てるようにしてもよい。

【０１５６】

移動子局７０ａは仮のアドレスを用いてステップＳ６２に示すＶＰＮ確立要求を移動親局６０ａに送信する。移動親局６０ａは、当該移動子局アドレス通知要求に仮アドレスを設定して、ＶＰＮサーバ１０に正式な移動子局アドレスの割り当てを要求する。ＶＰＮサーバ１０は、割り当てた移動子局アドレスを移動子局アドレス通知応答によって移動親局６０ａ、さらには移動子局７０ａに通知する。

【０１５７】

［ステップＳ６８］

移動親局６０ａとＶＰＮサーバ１０でＶＰＮ確立に必要な情報が決定・共有された後、以下の処理が行われる。

【０１５８】

移動親局６０ａは、受信部６１が移動子局７０ａからのパケットを受信すると、親局側ＶＰＮ管理テーブル６３ａに基づいて、当該パケットの転送先となるＶＰＮサーバ（ＶＰＮＳ１）を決定する。

【０１５９】

そして、ＶＰＮ管理部６３が、親局側ＶＰＮ管理テーブル６３ａを参照する。そして、当該仮想ＶＰＮアドレス（ＭＲｖ１）に対応して保持されるＶＰＮセキュリティ情報（暗号方式１および暗号鍵１）を暗号処理部６５に通知する。

【０１６０】

その後、暗号処理部６５が、ＶＰＮ管理部６３から通知されたＶＰＮセキュリティ情報（暗号方式１および暗号鍵１）に従って、移動子局７０ａから送信されたパケットを暗号化する。

【０１６１】

その後、カプセル化処理部６６が、暗号化したパケットを送信元アドレスとして移動親局６０ａ自身の実アドレス、宛先アドレスとしてＶＰＮサーバのアドレス（ＶＰＮＳ１）、および、ＩＰＳｅｃ　ＥＳＰヘッダを付与する。

【０１６２】

なお、移動親局６０ａの実アドレスは、移動網５１に接続しているときは、「ＭＲｒ１１」であり、移動網５２に接続しているときは、「ＭＲｒ１２」である。

送信部６２が、得られたパケットＰ２を、現在接続している移動網５１、または、移動網５２に送出する。

【０１６３】

また、受信部６１が、固定局２０から移動子局７０ａ宛のパケットＰ１を受信すると、カプセル化処理部６６が、受信したパケットＰ１をデ・カプセル化する。また、暗号処理部６５が、デ・カプセル化されたパケットを復号する。送信部６２が、復号されたパケットＰ２を、現在接続している移動子局７０ａに送出する。

【０１６４】

図１８は、移動網の移動後に移動親局とＶＰＮサーバ間でやり取りされるパケットを示す図である。

図１８（ａ）に示すパケットＰ１は、アドレスＡＤ１が、移動網５２に接続時の実アドレス（ＭＲｒ１２）である点が、図１３に示すパケットＰ１と異なっている。

【０１６５】

また、図１８（ｂ）に示すパケットＰ２は、アドレスＡＤ６が、移動網５２に接続時の実アドレス（ＭＲｒ１２）である点が、図１３に示すパケットＰ２と異なっている。

再び図１７に戻って説明する。

【０１６６】

［ステップＳ６９］

受信部６１が、通信の終了を示すＶＰＮ切断要求を移動子局７０ａから受信したか否かを判定する。ＶＰＮ切断要求を受信した場合にはステップＳ７０に遷移する。そうでなければステップＳ７５に遷移する。

【０１６７】

［ステップＳ７０］

送信部６２が、ＶＰＮを確立しているＶＰＮサーバ１０に対して、通信を終了した移動子局７０ａのアドレスの削除を要求する移動子局アドレス削除要求を送信する。その後、ステップＳ７１に遷移する。

【０１６８】

［ステップＳ７１］

ＶＰＮ管理部６３が、ＶＰＮサーバ１０から移動子局アドレス削除応答を受けると、親局側ＶＰＮ管理テーブル６３ａから、移動子局７０ａの情報を削除する。その後、ステップＳ７２に遷移する。

【０１６９】

［ステップＳ７２］
ＶＰＮ管理部６３が、通信を終了した移動子局７０ａが使用していたＶＰＮを使用している他の移動子局が存在するか否かを判定する。移動子局７０ａが使用していたＶＰＮを使用している他の移動子局が存在する場合は、ステップＳ７５に遷移する。移動子局７０ａが使用していたＶＰＮを使用している他の移動子局が存在しない場合は、ステップＳ７３に遷移する。

【０１７０】
［ステップＳ７３］
ＶＰＮ管理部６３が、ＶＰＮを切断するために、当該ＶＰＮを確立しているＶＰＮサーバ１０に対して移動親局アドレス削除要求の送信を送信部１２に指示する。これにより、送信部１２が、移動親局アドレス削除要求をＶＰＮサーバ１０に送信する。その後、ステップＳ７４に遷移する。

【０１７１】
［ステップＳ７４］
受信部６１が、ＶＰＮサーバ１０から移動親局アドレス削除完了応答を受けると、ＶＰＮ管理部６３が、親局側ＶＰＮ管理テーブル６３ａから、当該ＶＰＮサーバアドレス、および、セキュリティ情報の登録を削除する。その後、ステップＳ６２に遷移する。

【０１７２】
［ステップＳ７５］
移動処理部６４が、自身の移動により、別個の移動網に移動したか否かを判定する。この判定処理は、例えば、移動網からこれまでと異なる網情報（例えば、ＩＰアドレスのネットワーク・アドレス）を受信したか否かに基づいて行う。別個の移動網に移動したと判断した場合は、ステップＳ７６に遷移する。そうでなければステップＳ６８に遷移する。

【０１７３】
［ステップＳ７６］
ステップＳ６１と同様に、移動処理部６４が、別個の移動網において、無線基地局とリンクを確立し、ＤＨＣＰサーバ等から実アドレスを取得する。その後、ステップＳ７７に遷移する。

【０１７４】
［ステップＳ７７］
ステップＳ６４と同様に、送信部６２が、ステップＳ７６で取得した実アドレスをＶＰＮサーバ１０に通知する。その後、ステップＳ７８に遷移する。

【０１７５】
［ステップＳ７８］
ＶＰＮ管理部６３が、移動親局６０ａの移動に際して、暗号鍵を再設定する要求が存在するか否かを判定する。要求があればステップＳ７９に遷移する。そうでなければステップＳ６８に遷移する。

【０１７６】
［ステップＳ７９］
ステップＳ６５で行ったセキュリティ情報の設定のうち、暗号鍵の交換処理を実行する。その後、ステップＳ８０に遷移する。

【０１７７】
［ステップＳ８０］
ステップＳ７９で入手した暗号鍵を親局側ＶＰＮ管理テーブル６３ａに登録する。その後、ステップＳ６８に遷移する。

【０１７８】
以上で移動親局の処理の説明を終了する。
このように、移動親局６０ａに複数の移動子局が接続し、それらが同一のＶＰＮサーバ１０を介して通信を行う場合には、それらの移動子局の間でＶＰＮを共用することが可能である。

【０１７９】
この場合、最初にＶＰＮ確立要求が発生した際にＶＰＮを確立する。そして、それ以降のＶＰＮ確立要求については、移動子局のアドレスを親局側ＶＰＮ管理テーブル６３ａに登録すると共に、ＶＰＮサーバ１０に当該移動子局アドレスを通知すればよい。
【０１８０】
このような場合に対応するために、ステップＳ７２において、ＶＰＮ切断要求については、最後の１つの移動子局からの切断要求が発生するまでは、移動子局のアドレスを自身の親局側ＶＰＮ管理テーブル６３ａから削除すると共に、ＶＰＮサーバに当該移動子局アドレスの削除を要求する処理を行う。
【０１８１】
最後の１つの移動子局からの切断要求が発生した場合は、前述した処理に加えて、ＶＰＮサーバに対して移動親局のアドレスの削除要求を行い、ＶＰＮを切断する。
次に、ＶＰＮサーバ１０の処理を説明する。
【０１８２】
＜ＶＰＮサーバの移動親局アドレス通知受信処理＞
図１９は、ＶＰＮサーバのアドレス通知受信処理を示す図である。
［ステップＳ８１］
まず、受信部１１が、移動親局６０ａから移動親局アドレス通知を受信する。その後、ステップＳ８２に遷移する。
【０１８３】
［ステップＳ８２］
ＶＰＮ管理部１３が、受信した通知に含まれている移動親局の仮想ＶＰＮアドレスが、サーバ側ＶＰＮ管理テーブル１３ａに登録されているか否かを判定する。登録されていない場合、すなわち、移動親局６０ａが新規の移動親局である場合、ステップＳ８３へ遷移する。登録されている場合、すなわち、移動親局６０ａの移動により、新たな移動網に接続した場合は、ステップＳ８６に遷移する。
【０１８４】
［ステップＳ８３］
ＶＰＮ管理部１３が、ステップＳ８１で受信した通知に含まれている移動親局アドレス、仮想ＶＰＮアドレス等をサーバ側ＶＰＮ管理テーブル１３ａに登録する。その後、ステップＳ８４に遷移する。
【０１８５】
［ステップＳ８４］
当該移動親局６０ａとの間で、暗号化方式の交渉、および暗号鍵の交換処理を実行する。その後、ステップＳ８５に遷移する。
【０１８６】
［ステップＳ８５］
ＶＰＮ管理部１３が、ステップＳ８４で決定された暗号化方式、暗号鍵をサーバ側ＶＰＮ管理テーブル１３ａに登録する。その後、ステップＳ９０に遷移する。
【０１８７】
［ステップＳ８６］
ＶＰＮ管理部１３が、ステップＳ８１で受信した通知のパケットに含まれている仮想ＶＰＮアドレスに対応するサーバ側ＶＰＮ管理テーブル１３ａ内のエントリを検索する。そして、一致する仮想ＶＰＮアドレスを有するエントリを、ステップＳ８１で受信した通知のパケットに含まれている実アドレスで更新する。
【０１８８】
例えば、サーバ側ＶＰＮ管理テーブル１３ａが図７に示す状態のとき、移動親局６０ａからのアドレス通知を受信した場合を想定する。
受信した通知のパケットに、移動親局仮想ＶＰＮアドレスＭＲｖ１、移動親局実アドレスＭＲｒ１２が含まれていれば、１列目のエントリの移動親局仮想ＶＰＮアドレスＭＲｖ

１が一致する。従って、当該エントリを更新する。これにより、移動親局実アドレスの欄の実アドレスが、「ＭＲｒ１１」から「ＭＲｒ１２」に更新される。

【０１８９】

また、一致したサーバ側ＶＰＮ管理テーブル１３ａのエントリの移動速度、および、移動網種別の欄の値を、同時に受信した移動速度や移動網種別の値に更新する。その後、ステップＳ８７に遷移する。

【０１９０】

［ステップＳ８７］

受信したパケットの送信元である移動親局６０ａに対し、暗号鍵の再設定を行うか否かを判定する。暗号鍵の再設定を行う場合はステップＳ８８に遷移する。そうでなければステップＳ９０に遷移する。

【０１９１】

［ステップＳ８８］

移動親局６０ａとの間で、暗号鍵の交換処理を実行する。その後、ステップＳ８９に遷移する。

【０１９２】

［ステップＳ８９］

ステップＳ８８で決定された新たな暗号鍵をサーバ側ＶＰＮ管理テーブル１３ａのＶＰＮセキュリティ情報の欄に登録する。その後、ステップＳ９０に遷移する。

【０１９３】

［ステップＳ９０］

ステップＳ８１で受信したパケットの送信元の移動親局に対して、移動親局アドレス通知応答を送信する。その後、処理を終了する。

【０１９４】

以上で、アドレス通知受信処理の説明を終了する。

なお、移動子局アドレス追加要求については記載していないが、移動子局アドレス追加要求に含まれている移動親局アドレスに対応させる形で、サーバ側ＶＰＮ管理テーブル１３ａに移動子局アドレスを登録する。

【０１９５】

＜暗号鍵交換処理要否判定処理＞

次に、ステップＳ８７に示すＶＰＮサーバ１０の暗号鍵交換処理要否判定処理を説明する。

【０１９６】

図２０は、暗号鍵交換処理要否判定処理を示すフローチャートである。

［ステップＳ８７ａ］

ＶＰＮサーバ１０は、移動親局との間でＵＤＰによる通信を行っているか否かを判定する。

【０１９７】

具体的には、サーバ側ＶＰＮ管理テーブル１３ａを検索し、移動親局６０ａの仮想ＶＰＮアドレスに一致するエントリを検出する。そして、当該エントリのデータ種別の欄がＵＤＰであるか否かを判断する。

【０１９８】

データ種別の欄がＵＤＰである場合、すなわち、ＵＤＰによる通信を行っている場合にはステップＳ９０に遷移する。そうでなければステップＳ８７ｂに遷移する。

［ステップＳ８７ｂ］

ＶＰＮサーバ１０は、先に暗号鍵の交換を行った時刻から現在までに一定の時間が経過しているか否かを判定する。

【０１９９】

具体的には、ステップＳ８７ａにて一致したエントリの更新時刻の欄に設定されている時間からの経過時間が、予め定められた時間（閾値時間）以上であるか否かを判断する。

経過時間が、閾値時間以上である場合にはステップＳ８７ｃに遷移する。そうでなければステップＳ９０に遷移する。

【０２００】

［ステップＳ８７ｃ］

ＶＰＮサーバ１０は、新たな移動網のセルサイズ（通信エリア）と移動親局６０ａの移動速度に鑑みて、暗号鍵の再設定を行うか否かを判定する。この処理については、後に詳述する。暗号鍵の再設定を行う場合にはステップＳ８８に遷移する。そうでなければステップＳ９０に遷移する。

【０２０１】

以上で、暗号鍵交換処理要否判定処理の説明を終了する。

なお、本実施の形態では、ステップＳ８７ａ、Ｓ８７ｂ、Ｓ８７ｃの順番で処理を行ったが、処理の順番はこれに限定されない。

【０２０２】

ところで、ステップＳ８７ａにおいて、ＵＤＰは、音声や動画像等のリアルタイムでデータを転送するために用いられるプロトコルの例として挙げている。このようなリアルタイムのデータ通信では、暗号鍵の交換処理に伴う通信の瞬断が発生する場合がある。この場合、ユーザにとっては音声の途切れや、画像のノイズとして認識されるため、暗号鍵の交換処理を実行しないのが好ましい場合の例として示している。

【０２０３】

このように通信に瞬断が発生する時間が問題となるような通信に用いられるプロトコルであればＵＤＰに限定されず、他のプロトコルでも適用することができる。

なお、同一のＶＰＮにおいてＵＤＰとＴＣＰによる通信が混在するような場合があるが、そのような場合には、通信の瞬断に厳しいＵＤＰを考慮し、暗号鍵の交換を実行しないようにするのが好ましい。

【０２０４】

ところで、ステップＳ８７ｂにおいて、暗号鍵の交換処理を行わないことで、当該設定に伴う瞬断時間をなくすことができる反面、同じＶＰＮセキュリティ情報（暗号鍵）を用いる時間が長くなる。

【０２０５】

このため、ある一定の時間を閾値時間として予め用意しておき、ある暗号鍵が当該閾値時間を超えて連続的に使用されないようにすることで、セキュリティ情報の信頼性の低下を防止することができる。なお、この閾値時間は、ユーザの望むセキュリティ・レベルやプロトコルの種別に応じて、異なる値が設定されてもよい。

【０２０６】

なお、本実施の形態では、移動親局アドレス通知を受信した後に、ステップＳ８７ｂの処理を行うようにしたが、これに限らず、例えば、移動親局アドレス通知を受信しなくても、ＶＰＮサーバ１０は、先に暗号鍵の交換を行った時刻から現在までに閾値時間以上の時間が経過しているか否かを判定し、閾値時間以上の時間が経過している場合には暗号鍵の交換処理を実施するようにしてもよい。

【０２０７】

＜移動速度等に基づく鍵交換実施判定処理＞

次に、ステップＳ８７ｃの処理を詳しく説明する。

ステップＳ８７ｃにおいて、例えば、通信に使用している移動網が携帯電話網等、通信エリアが数ｋｍに及ぶような場合は、当該エリアに在圏する時間に比べて、暗号鍵の交換を行うことによる通信の瞬断時間が短い。このため、当該エリア内で通信可能な時間と比較した場合の影響は小さくなる。

【０２０８】

ところが、移動網が無線ＬＡＮのような通信エリアが数十ｍであるような場合は、移動親局が当該通信エリアに在圏中に通信可能となる時間が短くなる。このため、暗号鍵の交換設定を行うことによる瞬断時間の影響が大きくなる。

【０２０９】
従って、新たな移動網における瞬断時間の影響の大きい場合には暗号鍵の交換処理を行わないようにするのが好ましい。
このため、ステップＳ８７ｃでは、以下の処理を行うことにより、鍵交換の要否を判定している。
【０２１０】
図２１は、暗号鍵交換処理要否判定処理の詳細を示すフローチャートである。
［ステップＳ８７ｃ１］
ＶＰＮサーバ１０は、通信エリア管理テーブル１６ａを参照する。そして、ステップＳ８１にて受信した移動親局アドレス通知に含まれる移動網種別に対するセルサイズを取得する。その後、ステップＳ８７ｃ２に遷移する。
【０２１１】
［ステップＳ８７ｃ２］
ＶＰＮサーバ１０は、移動親局６０ａが、当該セルを通過する時間（通過時間）を演算する。具体的には、セルサイズを移動親局６０ａの移動速度で除算することにより、通過時間を演算する。その後、ステップＳ８７ｃ３に遷移する。
【０２１２】
［ステップＳ８７ｃ３］
ステップＳ８７ｃ２にて求めた通過時間に基づいて、暗号鍵の交換処理を実行することにより通信不可となる時間の百分率を演算する。具体的には、データ格納部１６に格納されている暗号鍵の交換処理に必要な時間を取得する。そして、処理時間／通過時間×１００を演算する。その後、ステップＳ８７ｃ４に遷移する。
【０２１３】
［ステップＳ８７ｃ４］
ステップＳ８７ｃ３にて求めた百分率に基づいて、暗号鍵の交換処理を行うか否かを判断する。具体的には、データ格納部１６に格納されている鍵交換の実行中に通信不可となることが許容される時間の百分率Ｔ（％）を取得する。そして、ステップＳ８７ｃ３にて求めた百分率が、百分率Ｔ以上か否かを判断する。ステップＳ８７ｃ３にて求めた百分率が、百分率Ｔ以上である場合、実行しないと判断し、ステップＳ９０に遷移する。ステップＳ８７ｃ３にて求めた百分率が、百分率Ｔ未満である場合、実行すると判断し、ステップＳ８８に遷移する。
【０２１４】
以上で暗号鍵交換処理要否判定処理の詳細の説明を終了する。
次に、暗号鍵交換処理要否判定処理の具体例を説明する。
なお、以下の例では、データ格納部１６に格納されている暗号鍵の交換処理に要する時間が１秒であり、百分率Ｔが１０％であるものとして説明する。
【０２１５】
また、ＶＰＮサーバ１０が、ステップＳ８１にて受信した移動親局アドレス通知には、移動親局６０ａの移動速度Ｖ（＝１１ｍ／秒）、および移動網種別（＝無線ＬＡＮ）が含まれているものとする。
【０２１６】
ＶＰＮサーバ１０は、通信エリア管理テーブル１６ａを参照する。そして、無線ＬＡＮに対するセルサイズの欄に設定されている値１００ｍを取得する。
ここで、移動親局アドレス通知を送信した移動親局６０ａが時速４０ｋｍ（１１ｍ／秒）で移動していると仮定すると、ＶＰＮサーバ１０は、当該セルを通過する時間（通過時間）を演算する。すなわち、
通過時間＝セルサイズ／移動速度（１００［ｍ］／１１［ｍ／秒］）より、約９秒が得られる。
【０２１７】
次に、この通過時間に基づいて、暗号鍵の交換処理を実行することにより通信不可とな

る時間の百分率を演算する。すなわち、
百分率＝交換処理に要する時間／当該セル在圏時間（１［秒］／９［秒］）×１００より、約１１％が得られる。
【０２１８】
これにより、暗号鍵の交換処理を実行することにより１１％が通信不可となることが分かる。
この値は、ＶＰＮサーバ１０に設定された百分率Ｔ（＝１０％）以上であるため、暗号鍵の交換処理は行わない。
【０２１９】
一方、当該移動親局アドレス通知を送信した移動親局が時速２０ｋｍ（５．６ｍ／秒）で移動していると仮定すると、ＶＰＮサーバ１０は、当該セルを通過する時間（通過時間）を演算する。すなわち、
通過時間＝セルサイズ／移動速度（１００［ｍ］／５．６［ｍ／秒］）より、約１８秒が得られる。
【０２２０】
次に、この通過時間に基づいて、暗号鍵の交換処理を実行することにより通信不可となる時間の割合を演算する。
これにより、暗号鍵の交換処理を実行することにより当該セル在圏時間１８秒間のうちの１秒、すなわち６％（＝１［秒］／１８［秒］×１００）が通信不可となることが分かる。
【０２２１】
この値は、ＶＰＮサーバ１０に設定された百分率Ｔ（＝１０％）よりも小さいため、暗号鍵の交換処理を実行する。
以上説明したように、実施の形態のシステム１００によれば、移動親局６０ａに対して移動網５１、５２間で共通する固定的な移動親局仮想ＶＰＮアドレスを設定するようにした。そして、暗号鍵の生成（セキュリティの設定）にこの仮想ＶＰＮアドレスを利用するようにした。
【０２２２】
これにより、移動子局７０ａが移動網５１、５２間を移動すると、移動親局６０ａの実アドレスは変化するが、移動親局６０ａの仮想ＶＰＮアドレスは変化しない。従って、移動親局６０ａの移動網５１、５２間の移動時に暗号鍵の再設定の処理を省略することができる。
【０２２３】
これによって、移動網５１、５２間の移動に伴う通信確立のための設定に必要な時間の短縮を図ることができる。従って、通信品質が向上する。
また、移動親局６０ａは、当該再設定が完了するまでの間に送信されたデータを蓄えておく必要がないので、移動親局６０ａが大容量のバッファを備える必要がない。
【０２２４】
なお、移動親局６０ａが携帯電話、無線ＬＡＮ等の複数の通信インタフェースをサポートしている場合には、携帯電話の基地局に接続できない場合には、無線ＬＡＮに接続する等、異なる移動網にまたがって移動してもよい。なお、本実施の形態では、再設定の対象となるセキュリティ情報として暗号鍵を用いた場合について説明したが、暗号化アルゴリズムが変更されてもよい。
【０２２５】
＜第３の実施の形態＞
次に、第３の実施の形態のシステムについて説明する。
以下、第３の実施の形態のシステムについて、前述した第２の実施の形態との相違点を中心に説明し、同様の事項については、その説明を省略する。
【０２２６】
図２２は、第３の実施の形態のシステムを示す図である。なお、図２２では、システム

１００と共通部分の図示を一部省略して示している。
第３の実施の形態のシステム１００ａは、移動局網８０に存在する移動子局７０ａ、７０ｂ間の通信を行う場合を示している。
【０２２７】
以下、本実施の形態における移動親局の処理を示す。
なお、第３の実施の形態では、ステップＳ６８の処理が異なっている。以下、本実施の形態のステップＳ６８に対応する処理を説明する。
【０２２８】
図２３は、第３の実施の形態の移動親局の処理を示すフローチャートである。
［ステップＳ９１］
受信部６１が、移動子局７０ａからパケットを受信する。その後、ステップＳ９２に遷移する。
【０２２９】
［ステップＳ９２］
受信したパケットの宛先アドレスを参照し、宛先の移動子局７０ｂが移動局網８０に存在するか否かを判定する。存在する場合は、ステップＳ９３に遷移する。そうでなければ、ステップＳ９４に遷移する。
【０２３０】
［ステップＳ９３］
受信したパケットを移動局網８０に転送する。その後、処理を終了する。
［ステップＳ９４］
宛先の移動子局７０ｂが移動局網８０に接続されていない場合は、そのパケットに対して暗号化・カプセル化を行う。これにより、パケットＰ２が生成される。その後、ステップＳ９５に遷移する。
【０２３１】
［ステップＳ９５］
ステップＳ９４で処理したパケットＰ２をＶＰＮサーバ１０に転送する。その後、処理を終了する。
【０２３２】
以上で、第３の実施の形態の移動親局６０ａの処理を終了する。
この第３の実施の形態のシステム１００ａによれば、第２の実施の形態のシステム１００と同様の効果が得られる。
【０２３３】
そして、第３の実施の形態のシステム１００ａによれば、さらに、移動局網８０に存在する移動子局７０ａ、７０ｂ間の通信においても通信品質の向上を図ることができる。
＜第４の実施の形態＞
次に、第４の実施の形態のシステムについて説明する。
【０２３４】
以下、第４の実施の形態のシステムについて、前述した第２の実施の形態との相違点を中心に説明し、同様の事項については、その説明を省略する。
図２４は、第４の実施の形態のシステムを示す図である。
【０２３５】
第４の実施の形態のシステム１００ｂは、移動親局６０ａに接続された移動子局７０ａが、移動親局６０ｂに接続された移動子局７０ｃとの間で通信を行うものである。
システム１００ｂでは、中継網４０からパケットＰ２を受信したときのＶＰＮサーバ１０の処理が、システム１００と異なっている。以下、本実施の形態の処理を説明する。
【０２３６】
図２５は、第４の実施の形態のＶＰＮサーバの処理を示すフローチャートである。
［ステップＳ１０１］
受信部１１が、中継網４０から宛先が移動子局７０ｃであるパケットＰ２を受信する。

その後、ステップＳ１０２に遷移する。

【０２３７】

［ステップＳ１０２］

カプセル化処理部１５が、ステップＳ１０１で受信したパケットＰ２のデ・カプセル化を行う。暗号処理部１４が、デ・カプセル化されたパケットを復号する。その後、ステップＳ１０３に遷移する。

【０２３８】

［ステップＳ１０３］

復号されたパケットの宛先アドレスを見て、宛先の移動子局７０ｃが固定網３０に接続されているか否かを判定する。接続されていればステップＳ１０４に遷移する。そうでなければステップＳ１０５に遷移する。

【０２３９】

［ステップＳ１０４］

宛先の移動子局７０ｃが固定網３０に接続されている場合は、そのパケットを固定網３０に転送する。その後、処理を終了する。

【０２４０】

［ステップＳ１０５］

宛先の移動子局７０ｃが固定網３０に接続されていない場合は、ステップＳ１０２でデ・カプセル化、および、復号されたパケットに対して、固定局２０から送信されたパケットに対して行う処理と同様の処理を行う。

【０２４１】

まず、ＶＰＮ管理部１３が、サーバ側ＶＰＮ管理テーブル１３ａを参照し、パケットの宛先の移動子局７０ｃが接続されている移動親局６０ｂを求める。

そして、暗号処理部１４が、パケットを暗号化する。また、カプセル化処理部１５が、パケットをカプセル化する。これにより、移動子局７０ｃを宛先とするパケットＰ１が生成される。その後、ステップＳ１０６に遷移する。

【０２４２】

［ステップＳ１０６］

送信部１２が、ステップＳ１０５で処理したパケットＰ１を中継網４０に転送する。その後、処理を終了する。

【０２４３】

以上で、第４の実施の形態のＶＰＮサーバ１０の処理の説明を終了する。

この第４の実施の形態のシステム１００ｂによれば、第２の実施の形態のシステム１００と同様の効果が得られる。

【０２４４】

そして、第４の実施の形態のシステム１００ｂによれば、さらに、移動子局７０ａ、７０ｃ間における通信においても通信品質の向上を図ることができる。

以上、本発明の通信管理装置および通信管理プログラムを、図示の実施の形態に基づいて説明したが、本発明はこれに限定されるものではなく、各部の構成は、同様の機能を有する任意の構成のものに置換することができる。また、本発明に、他の任意の構成物や工程が付加されていてもよい。

【０２４５】

なお、前述した各実施の形態では、ＩＰＳｅｃ－ＶＰＮを用いて説明したが、これに限らず、例えば、ＳＳＬ－ＶＰＮや、レイヤ２ＶＰＮ等の他のインターネットＶＰＮにも適用することができる。

【０２４６】

また、本発明は、前述した各実施の形態のうちの、任意の２以上の構成（特徴）を組み合わせたものであってもよい。

なお、上記の処理機能は、コンピュータによって実現することができる。その場合、ＶＰＮサーバ１０が有する機能の処理内容を記述したプログラムが提供される。そのプログ

ラムをコンピュータで実行することにより、上記処理機能がコンピュータ上で実現される。処理内容を記述したプログラムは、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、例えば、磁気記録装置、光ディスク、光磁気記録媒体、半導体メモリ等が挙げられる。磁気記録装置としては、例えば、ハードディスク装置（ＨＤＤ）、フレキシブルディスク（ＦＤ）、磁気テープ等が挙げられる。光ディスクとしては、例えば、ＤＶＤ（Digital Versatile Disc）、ＤＶＤ－ＲＡＭ（Random Access Memory）、ＣＤ－ＲＯＭ（Compact Disc Read Only Memory）、ＣＤ－Ｒ（Recordable）／ＲＷ（ReWritable）等が挙げられる。光磁気記録媒体としては、例えば、ＭＯ（Magneto-Optical disk）等が挙げられる。

【０２４７】

プログラムを流通させる場合には、例えば、そのプログラムが記録されたＤＶＤ、ＣＤ－ＲＯＭ等の可搬型記録媒体が販売される。また、プログラムをサーバコンピュータの記憶装置に格納しておき、ネットワークを介して、サーバコンピュータから他のコンピュータにそのプログラムを転送することもできる。

【０２４８】

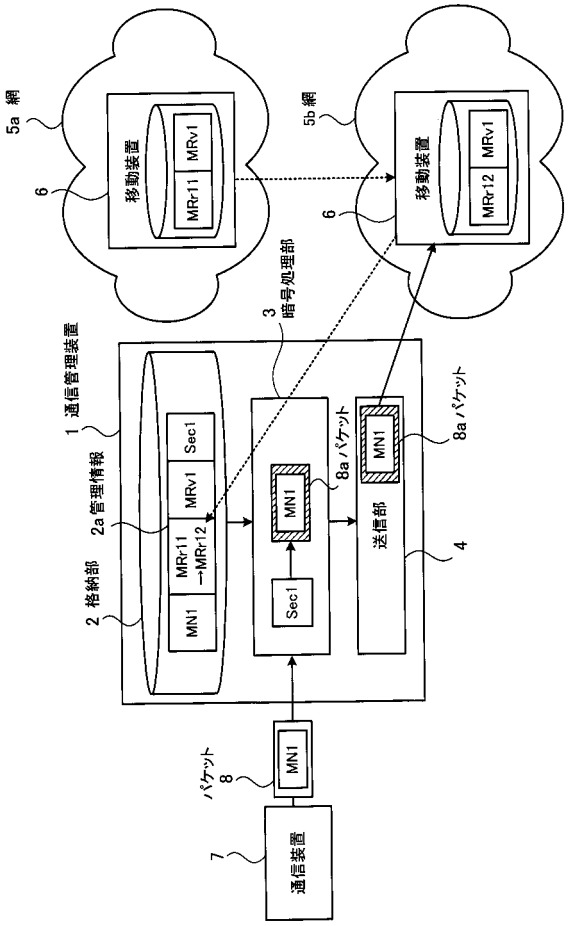
通信管理プログラムを実行するコンピュータは、例えば、可搬型記録媒体に記録されたプログラムもしくはサーバコンピュータから転送されたプログラムを、自己の記憶装置に格納する。そして、コンピュータは、自己の記憶装置からプログラムを読み取り、プログラムに従った処理を実行する。なお、コンピュータは、可搬型記録媒体から直接プログラムを読み取り、そのプログラムに従った処理を実行することもできる。また、コンピュータは、サーバコンピュータからプログラムが転送される毎に、逐次、受け取ったプログラムに従った処理を実行することもできる。

【符号の説明】

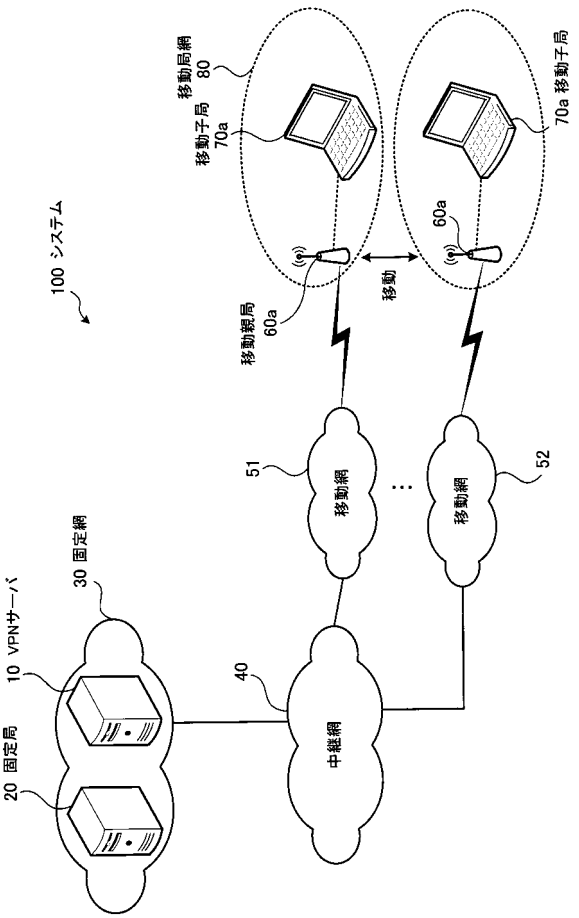
【０２４９】

１　通信管理装置
２　格納部
２ａ　管理情報
３、１４、６５　暗号処理部
４、１２、６２、７２　送信部
５ａ、５ｂ　網
６　移動装置
７　通信装置
８、８ａ、Ｐ１、Ｐ２　パケット
１０　ＶＰＮサーバ
１１、６１、７１　受信部
１３、６３、７３　ＶＰＮ管理部
１３ａ　サーバ側ＶＰＮ管理テーブル
１５、６６　カプセル化処理部
１６　データ格納部
１６ａ　通信エリア管理テーブル
２０　固定局
３０　固定網
４０　中継網
５１、５２　移動網
６０ａ、６０ｂ　移動親局
６３ａ　親局側ＶＰＮ管理テーブル
６４　移動処理部
７０ａ、７０ｂ、７０ｃ　移動子局
８０　移動局網
１００、１００ａ、１００ｂ　システム

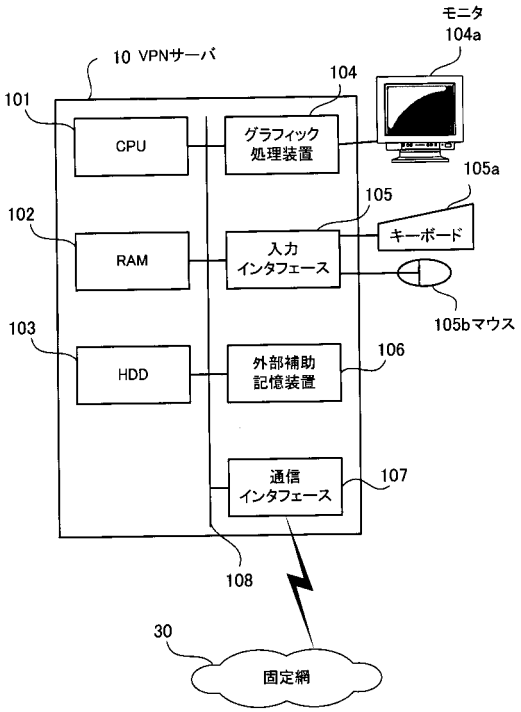
【図１】


5a 網
移動装置
MRr11
MRv1
6
5b 網
移動装置
MRr12
MRv1
6
3 暗号処理部
1 通信管理装置
2a 管理情報
Sec1
MRv1
MRr11
→MRr12
MN1
2 格納部
MN1
Sec1
8a パケット
MN1
送信部
8a パケット
4
パケット
8
MN1
7
通信装置

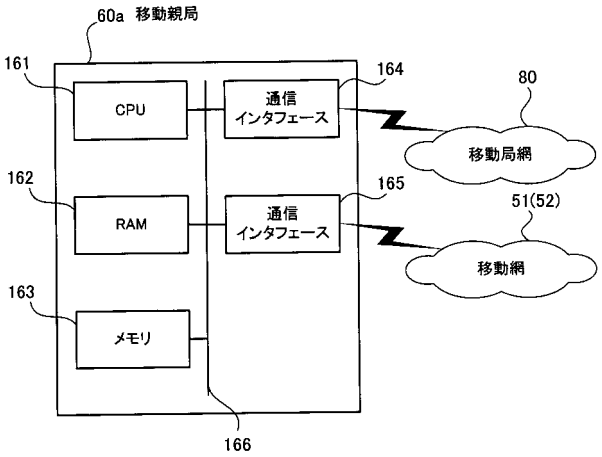
【図２】


移動局網
80
移動子局
70a
70a 移動子局
60a
移動
100 システム
移動親局
60a
51
移動網
…
移動網
52
30 固定網
10 VPNサーバ
40
中継網
20 固定局

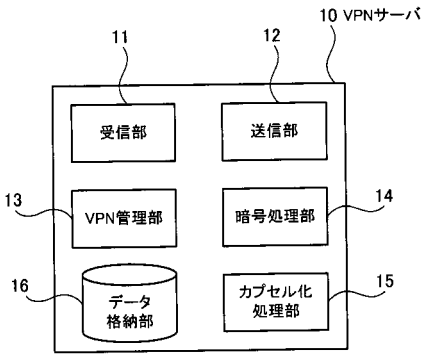
【図３】


モニタ
104a
10 VPNサーバ
104
101
CPU
グラフィック
処理装置
105a
105
102
RAM
入力
インタフェース
キーボード
105bマウス
103
HDD
外部補助
記憶装置
106
通信
インタフェース
107
108
30
固定網

【図４】


60a 移動親局
161
CPU
通信
インタフェース
164
80
移動局網
162
RAM
通信
インタフェース
165
51(52)
移動網
163
メモリ
166

【図５】



【図６】

16a 通信エリア管理テーブル

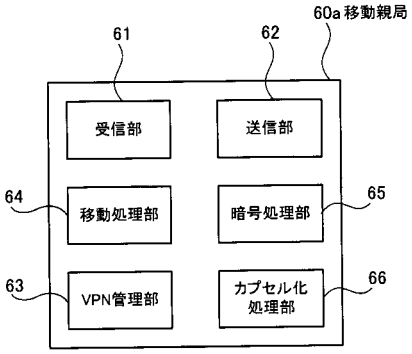
移動網種別	セルサイズ（通信エリア）
無線LAN	100m
セルラー	1km

【図７】

13a サーバ側VPN管理テーブル

移動子局アドレス	移動親局仮想VPNアドレス	移動親局実アドレス	VPNセキュリティ情報	更新時刻	データ種別	移動速度	移動網種別
MN1	MRv1	MRr11	暗号方式1、鍵1	t1	TCP	40km	無線LAN
MN2	MRv2	MRr21	暗号方式2、鍵2	t2	UDP	20km	無線LAN
…	…	…	…	…	…	…	…
MNn	MRvn	MRrnx	暗号方式n、鍵n	tn	UDP	100km	セルラー

【図８】

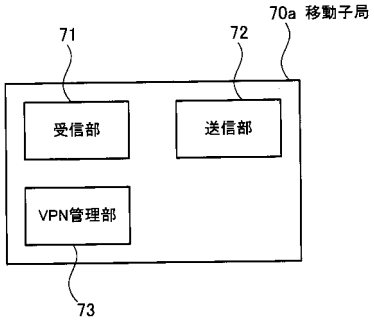


【図９】

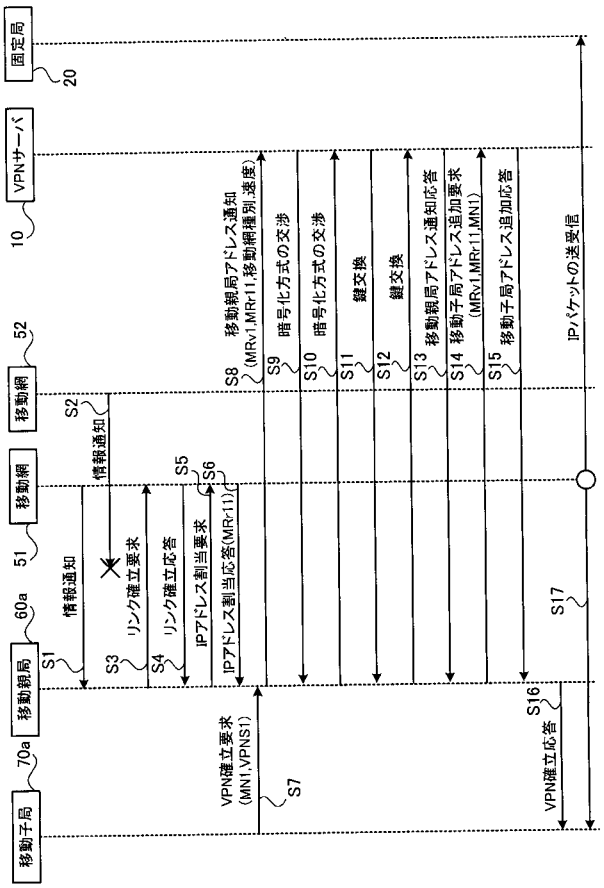
63a 親局側VPN管理テーブル

移動子局アドレス	VPNサーバアドレス	VPNセキュリティ情報
MN1	VPNS1	暗号方式1、鍵1
MN2	VPNS2	暗号方式2、鍵2
⋮	⋮	⋮
MNn	VPNSn	暗号方式n、鍵n

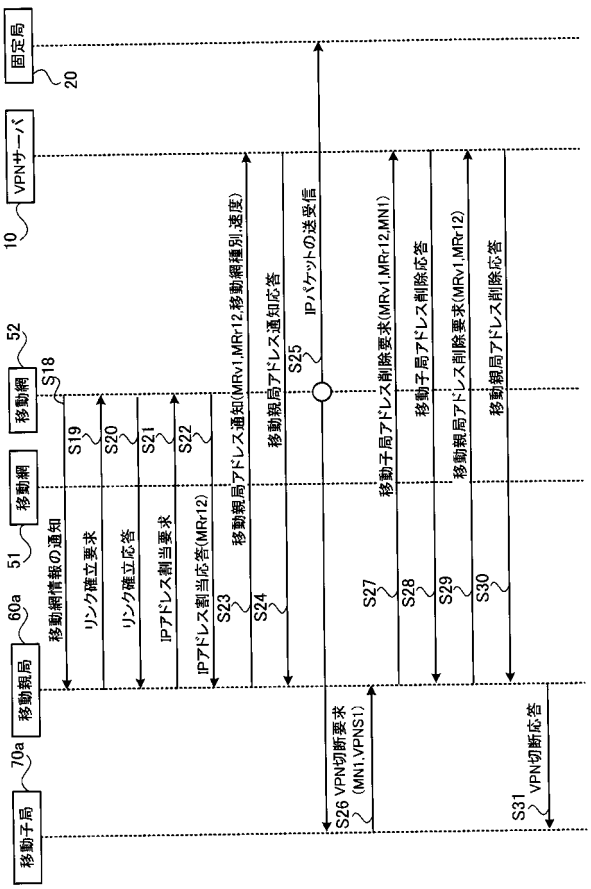
【図１０】



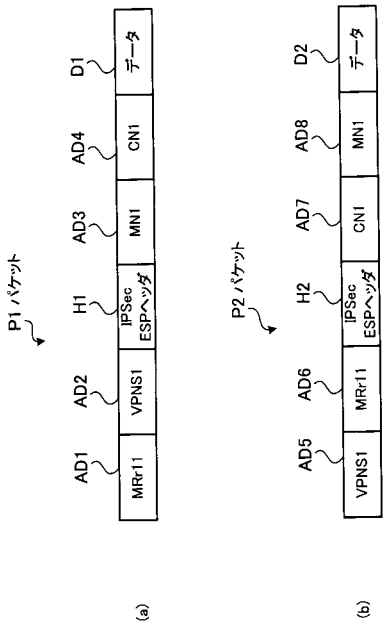
【図１１】



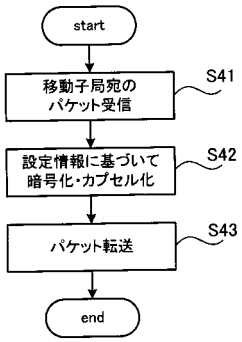
【図１２】



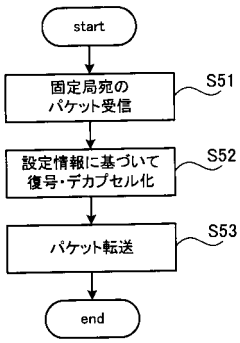
【図１３】



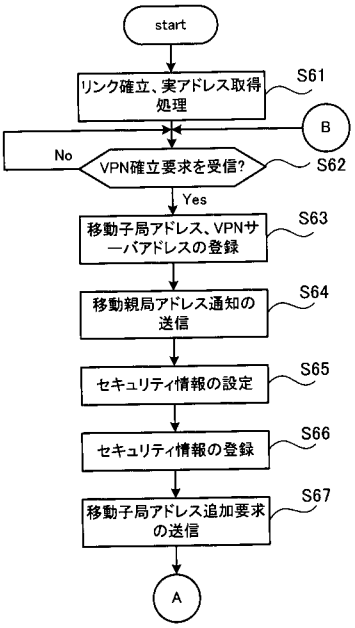
【図１４】



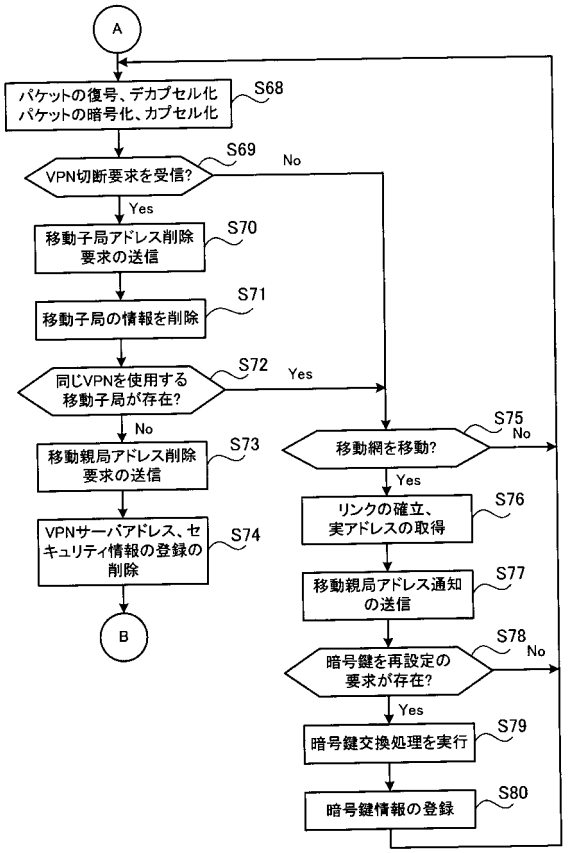
【図１５】



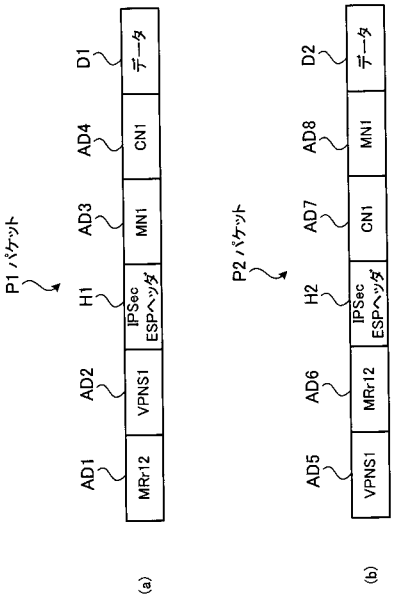
【図１６】



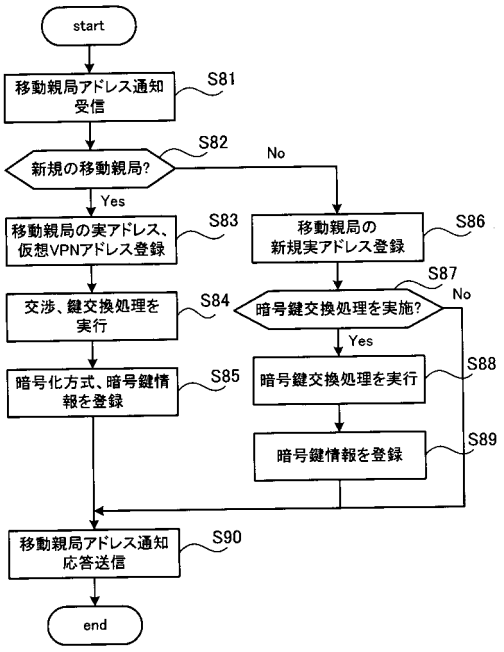
【図１７】



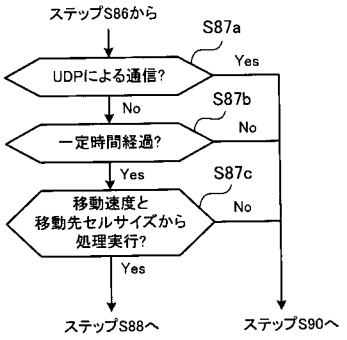
【図１８】



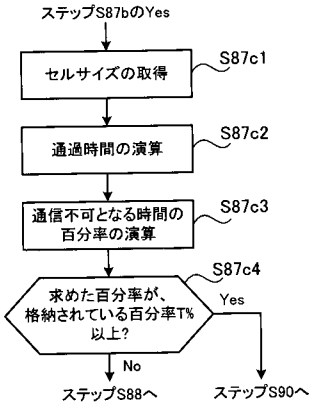
【図１９】



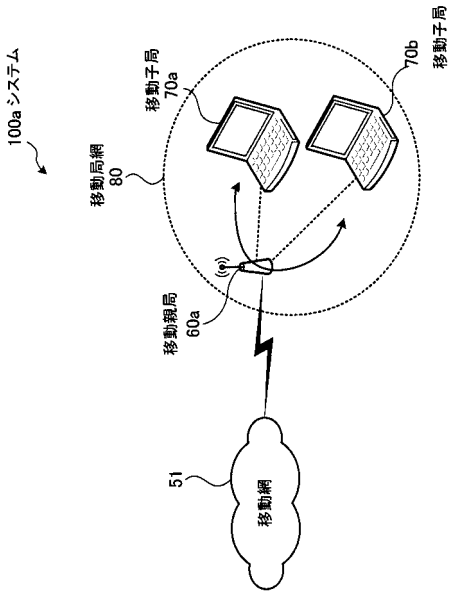
【図２０】



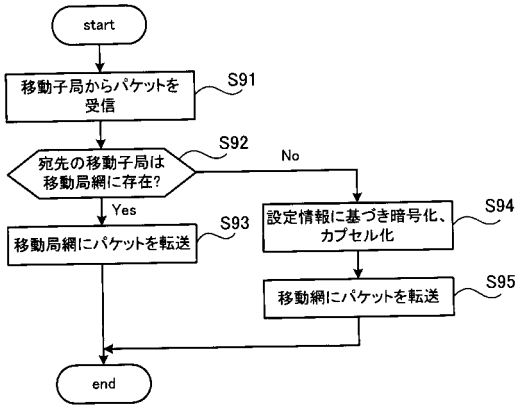
【図２１】



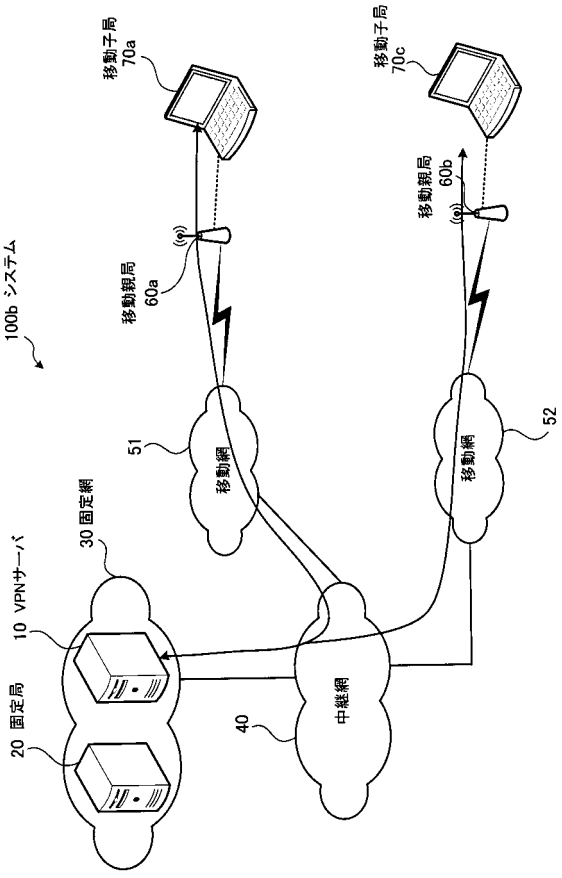
【図２２】



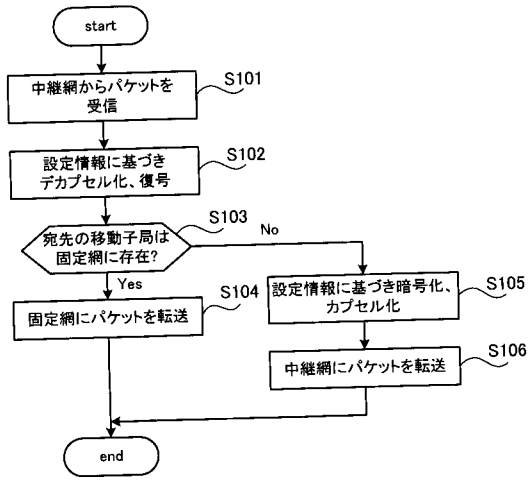
【図２３】



【図２４】



【図２５】


start
中継網からパケットを受信
S101
設定情報に基づきデカプセル化、復号
S102
宛先の移動子局は固定網に存在?
S103
No
Yes
固定網にパケットを転送
S104
設定情報に基づき暗号化、カプセル化
S105
中継網にパケットを転送
S106
end

フロントページの続き

(51)Int.Cl.	F I	テーマコード（参考）
Ｈ０４Ｌ　9/08　(2006.01)	Ｈ０４Ｌ　9/00　６０１Ｅ	

(72)発明者　村岡　和裕
福岡県福岡市早良区百道浜２丁目２番１号　富士通九州ネットワークテクノロジーズ株式会社内
(72)発明者　山本　智秀
福岡県福岡市早良区百道浜２丁目２番１号　富士通九州ネットワークテクノロジーズ株式会社内

Ｆターム(参考)　5J104 AA16　EA04　EA15　JA03　NA02　NA37　PA01
5K067 AA23　BB21　DD23　DD24　DD27　EE02　EE06　EE16　HH21　HH36