(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2006-217275
(P2006-217275A)
(43)公開日　平成18年8月17日(2006.8.17)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 12/56	(2006.01)	H04L	12/56	H	5J104
H04L 12/46	(2006.01)	H04L	12/46	V	5K030
H04L 9/08	(2006.01)	H04L	9/00	601C	5K033
		H04L	9/00	601E	

審査請求 有　請求項の数 6　OL　（全 16 頁）

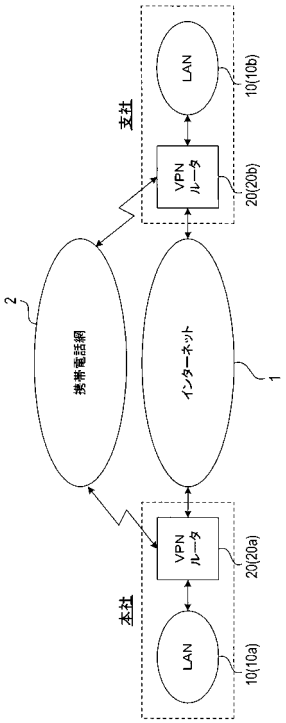
(21)出願番号　特願2005-27999(P2005-27999)
(22)出願日　平成17年2月3日(2005.2.3)

(71)出願人　599103801
株式会社　ネオテクノ
愛知県名古屋市中村区椿町１４番１３号
(74)代理人　100082500
弁理士　足立　勉
(72)発明者　竹内　正樹
愛知県名古屋市中村区椿町１４番１３号
株式会社ネオテクノ内

Fターム(参考)　5J104 AA01 AA16 EA04 EA15 EA16
JA03 NA02 NA37 PA07
5K030 GA15 HA08 HC01 HD03 HD06
KA05 MA13
5K033 AA08 CB08 CC01 DA06 DB12
DB16 DB18

(54)【発明の名称】ＶＰＮ通信装置及び通信システム

(57)【要約】
【課題】　共通鍵の受渡しに必要なデータ通信を簡略化しつつ、高いセキュリティ性を実現する。
【解決手段】　この通信システムにおいては、本社に構築されたＬＡＮ１０ａと、支社に構築されたＬＡＮ１０ｂとが、それぞれＶＰＮルータ２０ａ，２０ｂを介してインターネット１に接続されている。また、ＶＰＮルータ２０ａ，２０ｂは、携帯電話網２を介して通信可能に構成されている。そして、この通信システムでは、ＶＰＮルータ２０ａ，２０ｂ間での暗号通信によりＶＰＮが構築される。具体的には、共通鍵を用いた暗号通信を行うようになっており、一方のＶＰＮルータ２０が共通鍵を生成し、その共通鍵を携帯電話網２を介して通信先のＶＰＮルータ２０へ送信する。これにより、２つのＶＰＮルータ２０ａ，２０ｂで共通鍵が共有される。
【選択図】　図１



【特許請求の範囲】
【請求項１】
インターネットを介したデータ通信を行うための第１通信手段と、
インターネット以外の通信網を介したデータ通信を行うための第２通信手段と、
暗号通信に用いるための共通鍵が前記第２通信手段により受信された場合に、その共通鍵を用いた暗号通信を前記第１通信手段に行わせることで、インターネット上にＶＰＮを構築する暗号通信手段と、
を備えたことを特徴とするＶＰＮ通信装置。
【請求項２】
請求項１に記載のＶＰＮ通信装置において、
暗号通信に用いるための共通鍵を生成する鍵生成手段を備え、
前記暗号通信手段は、前記鍵生成手段により共通鍵が生成された場合に、その共通鍵を前記第２通信手段に送信させるとともに、その共通鍵を用いた暗号通信を前記第１通信手段に行わせることで、インターネット上にＶＰＮを構築すること
を特徴とするＶＰＮ通信装置。
【請求項３】
請求項１又は請求項２に記載のＶＰＮ通信装置において、
前記第１通信手段は、暗号通信を行っていない状態では機能しないように構成されていること
を特徴とするＶＰＮ通信装置。
【請求項４】
請求項１ないし請求項３のいずれか１項に記載のＶＰＮ通信装置において、
前記第２通信手段は、携帯電話網を介したデータ通信を行うこと
を特徴とするＶＰＮ通信装置。
【請求項５】
請求項１ないし請求項４のいずれか１項に記載のＶＰＮ通信装置を少なくとも２台備え、さらに、ＶＰＮ通信装置間の暗号通信を管理する管理装置を備えた通信システムであって、
前記管理装置は、
前記ＶＰＮ通信装置の第２通信手段とデータ通信可能な中継通信手段と、
前記ＶＰＮ通信装置から暗号通信開始を要求する旨のデータを受信した場合に、暗号通信に用いるための共通鍵を前記ＶＰＮ通信装置へ送信する処理を前記中継通信手段に行わせる鍵配布手段と、
を備えたことを特徴とする通信システム。
【請求項６】
請求項５に記載の通信システムにおいて、
前記鍵配布手段は、前記ＶＰＮ通信装置から暗号通信開始を要求する旨のデータを受信した場合に、暗号通信を許可するか否かを判定し、許可すると判定した場合に、暗号通信に用いるための共通鍵を前記ＶＰＮ通信装置へ送信する処理を前記中継通信手段に行わせること
を特徴とする通信システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、インターネットＶＰＮに関するものである。
【背景技術】
【０００２】
従来、例えば大企業においては、遠隔地にある本店と支店とのコンピュータ同士を接続してデータをやり取りするために、専用線を設置するという手法がとられていた。しかしながら、こうした専用線には、工事費や維持費等に莫大な金額がかかるという難点がある

。そこで、近年では、グローバルネットワークであるインターネットを利用し、送信側でデータを暗号化し、受信側でこれを復号することで、あたかも両者が専用線で接続されているかのような構成を実現するインターネットＶＰＮ（Ｖｉｒｔｕａｌ　Ｐｒｉｖａｔｅ　Ｎｅｔｗｏｒｋ：仮想私設網）を構築するといった手法が採用されるようになってきている。

【０００３】

こうしたインターネットＶＰＮにおいては、ＶＰＮルータ（ＶＰＮ機能を有するルータ）を両地点に設置し、このＶＰＮルータによりインターネット側へ送信するデータの暗号化及びインターネット側から受信したデータの復号を行うことで、セキュリティ性の高い暗号通信を実現する。

【０００４】

なお、上述した内容は公知・公用の技術であり、出願人は特に先行技術調査を行っていないため、先行技術文献の開示については行わない。

【発明の開示】

【発明が解決しようとする課題】

【０００５】

ところで、こうした暗号通信では、セキュリティ性を向上させるため、使用する暗号鍵を定期的に更新する必要がある。このため、ＶＰＮルータ間で暗号鍵をいかに安全に受け渡すかが問題となる。ここで、公開鍵暗号方式による暗号通信では、鍵の受渡し自体はインターネット上で容易に行うことができるものの、暗号化／復号の処理が複雑となって処理時間が長くなるため、大量のデータをやり取りする場合に不向きである。そこで、共通鍵（秘密鍵）暗号方式による暗号通信が望まれるが、インターネット上で共通鍵の受渡しを行うためには、その共通鍵を公開鍵を用いて暗号化して送信する等の対策を講じる必要があるため、データ通信が煩雑化してしまうという問題がある。

【０００６】

本発明は、こうした問題にかんがみてなされたものであり、共通鍵の受渡しに必要なデータ通信を簡略化しつつ、高いセキュリティ性を実現することを目的としている。

【課題を解決するための手段】

【０００７】

上記目的を達成するためになされた請求項１に記載の発明は、インターネットを介したデータ通信を行うための第１通信手段と、インターネット以外の通信網を介したデータ通信を行うための第２通信手段と、暗号通信に用いるための共通鍵が第２通信手段により受信された場合に、その共通鍵を用いた暗号通信を第１通信手段に行わせることで、インターネット上にＶＰＮを構築する暗号通信手段と、を備えたことを特徴とするＶＰＮ通信装置である。

【０００８】

つまり、本ＶＰＮ通信装置は、インターネット以外の通信網を介して受信した共通鍵を用いて暗号通信を行うことができるように構成されている。

したがって、本ＶＰＮ通信装置によれば、共通鍵の受取をインターネットを介して行う必要が無く、共通鍵の暗号化処理を不要とする（又は簡略化する）ことができる。この結果、共通鍵の受渡しに必要なデータ通信を簡略化しつつ、高いセキュリティ性を実現することができる。

【０００９】

ところで、暗号通信に用いるための共通鍵は、例えば、暗号通信を管理する別の通信手段（例えば、請求項５の中継通信手段）によってＶＰＮ通信装置へ送信される構成が考えられる。ただし、別の通信手段を用いることなくＶＰＮの構築を可能とするためには、請求項２のようにするとよい。

【００１０】

すなわち、請求項２に記載の発明は、上記請求項１のＶＰＮ通信装置において、暗号通信に用いるための共通鍵を生成する鍵生成手段を備え、暗号通信手段が、鍵生成手段によ

り共通鍵が生成された場合に、その共通鍵を第２通信手段に送信させるとともに、その共通鍵を用いた暗号通信を第１通信手段に行わせることで、インターネット上にＶＰＮを構築することを特徴とするものである。

【００１１】

つまり、本ＶＰＮ通信装置は、共通鍵を生成し、インターネット以外の通信網を介して送信可能に構成されている。

したがって、本ＶＰＮ通信装置を少なくとも２台用いれば、共通鍵の生成及びインターネット以外の通信網を介した共通鍵の受渡しを行うことができる。この結果、共通鍵をＶＰＮ通信装置へ送信するための通信手段を別途用いることなくＶＰＮを構築とすることが可能となる。

【００１２】

ところで、暗号通信の開始がインターネットを介してＶＰＮ通信装置へ要求される構成では、暗号通信を開始する前の状態においても、暗号通信開始の要求を検出するためにインターネット側から送信されてくるデータをチェックする必要がある。これに対し、暗号通信の開始がインターネット以外の通信網を介してＶＰＮ通信装置へ要求される構成であれば、暗号通信を開始する前の状態においては、暗号通信開始の要求を検出するためにインターネット側から送信されてくるデータをチェックする必要がない。そこで、請求項３のように構成することが考えられる。

【００１３】

すなわち、請求項３に記載の発明は、上記請求項１又は２のＶＰＮ通信装置において、第１通信手段が、暗号通信を行っていない状態では機能しないように構成されていることを特徴とするものである。

【００１４】

つまり、本ＶＰＮ通信装置は、暗号通信以外はインターネットを介したデータ通信を行わないように構成されている。

したがって、本ＶＰＮ通信装置によれば、インターネット側からの不正アクセスに対するセキュリティ性を極めて高くすることができる。

【００１５】

一方、第２通信手段がデータ通信を行う「インターネット以外の通信網」としては、例えば、固定電話が利用する固定電話網や、ＩＳＤＮ（Ｉｎｔｅｇｒａｔｅｄ　Ｓｅｒｖｉｃｅｓ　Ｄｉｇｉｔａｌ　Ｎｅｔｗｏｒｋ）などが考えられるが、より好ましくは、請求項４のようにするとよい。

【００１６】

すなわち、請求項４に記載の発明は、上記請求項１～３のいずれかのＶＰＮ通信装置において、第２通信手段が、携帯電話網を介したデータ通信を行うことを特徴とするものである。

【００１７】

このため、本ＶＰＮ通信装置によれば、共通鍵の受渡しを行うための通信線を別途設ける必要がない。しかも、携帯電話機は既に一般に広く普及しているものであるため、比較的安価に構成することができる。

【００１８】

次に、請求項５に記載の発明は、上記請求項１～請求項４のいずれか１項に記載のＶＰＮ通信装置を少なくとも２台備え、さらに、ＶＰＮ通信装置間の暗号通信を管理する管理装置を備えた通信システムであって、管理装置は、ＶＰＮ通信装置の第２通信手段とデータ通信可能な中継通信手段と、ＶＰＮ通信装置から暗号通信開始を要求する旨のデータを受信した場合に、暗号通信に用いるための共通鍵をＶＰＮ通信装置へ送信する処理を中継通信手段に行わせる鍵配布手段と、を備えたものである。

【００１９】

つまり、本通信システムでは、ＶＰＮ通信装置から管理装置へ暗号通信開始を要求する旨のデータが送信されることにより、管理装置の中継通信手段からインターネット以外の

通信網を介してＶＰＮ通信装置へ共通鍵が送信される。なお、共通鍵は、暗号通信を行うすべてのＶＰＮ通信装置へ送信してもよいが、例えば、暗号通信開始を要求する旨のデータとしてＶＰＮ通信装置で生成した共通鍵が送信される場合には、その共通鍵を、暗号通信開始の要求元のＶＰＮ通信装置の通信先となるＶＰＮ通信装置へのみ送信するようにしてもよい。

【００２０】

このような請求項５の通信システムによれば、ＶＰＮ通信装置間の暗号通信を管理装置において管理することができる。このため、例えば取引先の会社との通信のように、一時的にＶＰＮを構築したいような場合に有効である。

【００２１】

特に、請求項５に記載のように、鍵配布手段が、ＶＰＮ通信装置から暗号通信開始を要求する旨のデータを受信した場合に、暗号通信を許可するか否かを判定し、許可すると判定した場合に、暗号通信に用いるための共通鍵をＶＰＮ通信装置へ送信する処理を中継通信手段に行わせるように構成されていれば、暗号通信を許可するか否かを管理装置において管理することができる。この結果、ＶＰＮを構築すべきでない場合には許可しないようにすることができる。

【発明を実施するための最良の形態】

【００２２】

以下、本発明が適用された実施形態について、図面を用いて説明する。

［第１実施形態］

図１は、第１実施形態の通信システムの概略構成図である。

【００２３】

同図に示すように、この通信システムにおいては、ある会社の本社に構築されたＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）１０ａと、支社に構築されたＬＡＮ１０ｂとが、それぞれＶＰＮルータ２０ａ，２０ｂを介してインターネット１に接続されている。また、ＶＰＮルータ２０ａ，２０ｂは、それぞれ携帯電話網２を介して通信可能に構成されている。

【００２４】

本通信システムにおいて、本社に設置されているＶＰＮルータ２０ａと、支社に設置されているＶＰＮルータ２０ｂとは、同一構成のものである。ここで、ＶＰＮルータ２０（２０ａ，２０ｂ）の構成について、図２のブロック図を用いて説明する。

【００２５】

同図に示すように、ＶＰＮルータ２０は、ＬＡＮ通信部２１、ＷＡＮ通信部２２、携帯電話通信部２３及び制御部２４を備えている。

ＬＡＮ通信部２１は、ＬＡＮ１０（１０ａ又は１０ｂ）に接続され、ＬＡＮ１０からデータを受信して制御部２４へ送るとともに、制御部２４からのデータをＬＡＮ１０へ送信する。

【００２６】

ＷＡＮ通信部２２は、インターネット１（ＷＡＮ）に接続され、インターネット１からデータを受信して制御部２４へ送るとともに、制御部２４からのデータをインターネット１へ送信する。

【００２７】

携帯電話通信部２３は、携帯電話網２を介した無線通信を行うためのものであり、携帯電話網２からデータを受信して制御部２４へ送るとともに、制御部２４からのデータを携帯電話網２へ送信する。なお、携帯電話通信部２３は、市販の携帯電話機を組み込むことにより構成されるものであってもよい。

【００２８】

制御部２４は、ＣＰＵ、ＲＯＭ、ＲＡＭ等からなる周知のマイクロコンピュータを中心に構成されており、本ＶＰＮルータ２０の各部を制御する。

次に、本第１実施形態の通信システムで行われる処理の概要について説明する。

【００２９】
本第１実施形態の通信システムにおいては、ＶＰＮルータ２０ａ，２０ｂ間での暗号通信によりＶＰＮが構築される。具体的には、共通鍵を用いた暗号通信を行うようになっており、一方のＶＰＮルータ２０が共通鍵を生成し、その共通鍵を携帯電話網２を介して通信先のＶＰＮルータ２０へ送信する。これにより、２つのＶＰＮルータ２０ａ，２０ｂで共通鍵が共有される。なお、共通鍵を共有した後の暗号通信自体は、従来のＶＰＮと同様の方法で行うことができる。
【００３０】
このような方法でＶＰＮを構築するために、本第１実施形態の通信システムに用いられるＶＰＮルータ２０は、次の（Ａ），（Ｂ）の機能を有している。
（Ａ）：ＬＡＮ１０側に接続された機器（例えば、パーソナルコンピュータ）から通信開始指令を受信すると、暗号通信に用いる共通鍵を携帯電話網２を介して通信先のＶＰＮルータ２０へ送信し、その通信先のＶＰＮルータ２０から通信を許可する旨の許可通知を受信後、その通信先のＶＰＮルータ２０との間で暗号通信を開始する。
【００３１】
（Ｂ）：通信先のＶＰＮルータ２０から携帯電話網２を介して共通鍵を受信すると、通信を許可する旨の許可通知を携帯電話網２を介して通信先のＶＰＮルータ２０へ送信し、通信先のＶＰＮルータ２０との間で暗号通信を開始する。
【００３２】
このような機能（上記（Ａ），（Ｂ））により、本通信システムでは、一方のＶＰＮルータ２０でＬＡＮ１０側に接続された機器から通信開始指令が受信されることにより、そのＶＰＮルータ２０から他方のＶＰＮルータ２０へ携帯電話網２を介して共通鍵が送信され、さらに、他方のＶＰＮルータ２０から共通鍵送信元のＶＰＮルータ２０へ携帯電話網２を介して許可通知が返信された後、両ＶＰＮルータ２０間の暗号通信が開始されることとなる。なお、本実施形態の通信システムにおいて、通信開始指令は、ＬＡＮ１０側の機器で、通信開始指令を送信するための所定の入力操作が利用者（ユーザ）によって行われた場合に、そのＬＡＮ１０に接続されたＶＰＮルータ２０宛に送信される。
【００３３】
さらに、本第１実施形態の通信システムに用いられるＶＰＮルータ２０は、次の（Ｃ），（Ｄ）の機能を有している。
（Ｃ）：ＬＡＮ１０側に接続された機器から通信終了指令を受信すると、通信を終了する旨の通信終了通知をインターネット１を介して通信先のＶＰＮルータ２０へ送信し、暗号通信を終了する。
【００３４】
（Ｄ）：通信先のＶＰＮルータ２０からインターネット１を介して通信終了通知を受信すると、暗号通信を終了する。
このような機能（上記（Ｃ），（Ｄ））により、本通信システムでは、一方のＶＰＮルータ２０でＬＡＮ１０側に接続された機器から通信終了指令が受信されることにより、そのＶＰＮルータ２０から他方のＶＰＮルータ２０へ通信終了通知が送信されて、両ＶＰＮルータ２０間の暗号通信が終了することとなる。なお、本実施形態の通信システムにおいて、通信終了指令は、ＬＡＮ１０側の機器で、通信終了指令を送信するための所定の入力操作が利用者によって行われた場合に、そのＬＡＮ１０に接続されたＶＰＮルータ２０宛に送信される。
【００３５】
加えて、本第１実施形態の通信システムに用いられるＶＰＮルータ２０は、次の（Ｅ）の機能を有している。
（Ｅ）：暗号通信を行っていない状態では、ＷＡＮ通信部２２の機能を停止する。
【００３６】
このような機能（上記（Ｅ））により、本通信システムでは、暗号通信処理を行っていない状態におけるインターネット１側からの不正アクセスが確実に防止されることとなる

。
【００３７】
次に、ＶＰＮルータ２０の制御部２４が実行する処理の具体的内容について説明する。
まず、ＬＡＮ通信部２１により通信開始指令が受信された場合に制御部２４が実行するＬＡＮ側受信処理について、図３のフローチャートを用いて説明する。
【００３８】
このＬＡＮ側受信処理が開始されると、まず、Ｓ１０１で、暗号通信に用いるための共通鍵を、例えばランダムに生成する。
続いて、Ｓ１０２では、Ｓ１０１で生成した共通鍵を、携帯電話網２を介して通信先のＶＰＮルータ２０へ送信する処理を、携帯電話通信部２３に行わせる。なお、通信先のＶＰＮルータ２０の電話番号は、制御部２４に記憶されている。
【００３９】
続いて、Ｓ１０３では、Ｓ１０２での共通鍵の送信に対して通信先のＶＰＮルータ２０から携帯電話網２を介して送信されてくる許可通知が携帯電話通信部２３により受信されたか否かを判定する。
【００４０】
このＳ１０３で、許可通知が受信されていないと判定した場合には、Ｓ１０４へ移行し、Ｓ１０２での共通鍵の送信から所定時間（あらかじめ設定された時間）が経過したか否かを判定する。
【００４１】
そして、Ｓ１０４で、所定時間が経過していないと判定した場合には、Ｓ１０３へ戻る。
一方、Ｓ１０４で、所定時間が経過したと判定した場合には、本ＬＡＮ側受信処理を終了する。つまり、共通鍵を送信したにもかかわらず許可通知が受信されない場合には処理を終了するようにしている。
【００４２】
これに対し、Ｓ１０３で、許可通知が受信されたと判定した場合には、Ｓ１０５へ移行し、Ｓ１０１で生成した共通鍵を用いて暗号通信処理を開始する。具体的には、ＬＡＮ通信部２１により受信されたデータを共通鍵を用いて暗号化してＷＡＮ通信部２２に送信させ、ＷＡＮ通信部２２により受信されたデータを共通鍵を用いて復号してＬＡＮ通信部２１に送信させる。
【００４３】
続いて、Ｓ１０６では、ＬＡＮ通信部２１により通信終了指令が受信されたか否かを判定する。
このＳ１０６で、通信終了指令が受信されていないと判定した場合には、Ｓ１０７へ移行し、ＷＡＮ通信部２２により通信終了通知が受信されたか否かを判定する。
【００４４】
そして、Ｓ１０７で、通信終了通知が受信されていないと判定した場合には、Ｓ１０６へ戻る。
一方、Ｓ１０７で、通信終了通知が受信されたと判定した場合には、本ＬＡＮ側受信処理を終了する。
【００４５】
また、Ｓ１０６で、通信終了指令が受信されたと判定した場合には、Ｓ１０８へ移行し、通信を終了する旨の通信終了通知を、インターネット１を介して通信先のＶＰＮルータ２０へ送信する処理を、ＷＡＮ通信部２２に行わせる。その後、本ＬＡＮ側受信処理を終了する。
【００４６】
次に、携帯電話通信部２３により共通鍵が受信された場合に制御部２４が実行する携帯側受信処理について、図４のフローチャートを用いて説明する。
この携帯側受信処理が開始されると、まず、Ｓ２０１で、受信した共通鍵を記憶する。

【００４７】
続いて、Ｓ２０２では、共通鍵の送信元のＶＰＮルータ２０に対し、通信を許可する旨の許可通知を携帯電話網２を介して送信する処理を、携帯電話通信部２３に行わせる。
続いて、Ｓ２０３では、受信した共通鍵を用いて暗号通信処理を開始する。具体的には、ＬＡＮ通信部２１により受信されたデータを共通鍵を用いて暗号化してＷＡＮ通信部２２に送信させ、ＷＡＮ通信部２２により受信されたデータを共通鍵を用いて復号してＬＡＮ通信部２１に送信させる。
【００４８】
続いて、Ｓ２０４では、ＬＡＮ通信部２１により通信終了指令が受信されたか否かを判定する。
このＳ２０４で、通信終了指令が受信されていないと判定した場合には、Ｓ２０５へ移行し、ＷＡＮ通信部２２により通信終了通知が受信されたか否かを判定する。
【００４９】
そして、Ｓ２０５で、通信終了通知が受信されていないと判定した場合には、Ｓ２０４へ戻る。
一方、Ｓ２０４で、通信終了指令が受信されたと判定した場合には、本携帯側受信処理を終了する。
【００５０】
また、Ｓ２０５で、通信終了通知が受信されたと判定した場合には、Ｓ２０６へ移行し、通信を終了する旨の通信終了通知を、インターネット１を介して通信先のＶＰＮルータ２０へ送信する処理を、ＷＡＮ通信部２２に行わせる。その後、本携帯側受信処理を終了する。
【００５１】
以上説明したように、本第１実施形態の通信システムでは、ＶＰＮを構築しようとする両地点に設置されたＶＰＮルータ２０によって携帯電話網２を介して共通鍵の受渡しが行われる（Ｓ１０２）。このため、本通信システムによれば、共通鍵の受渡しをインターネット１を介して行うための煩雑な通信処理を不要としつつ、高いセキュリティ性を実現することができる。特に、本通信システムでは、共通鍵の受渡しに携帯電話網２を利用しているため、共通鍵の受渡しのための通信線と不要とするとともに、比較的安価に構成することができる。しかも、ＶＰＮルータ２０は、暗号通信を行っていない状態ではＷＡＮ通信部２２の機能を停止するように構成されているため、インターネット１側からの不正アクセスに対するセキュリティ性を極めて高くすることができる。加えて、本通信システムでは、比較的高い頻度で共通鍵を変更することが可能となるため、従来のＶＰＮで用いられている暗号アルゴリズムに比べ、簡易な暗号アルゴリズムを用いることも可能となり、暗号通信の通信速度を一層向上させることができる。
【００５２】
なお、本第１実施形態の通信システムでは、ＶＰＮルータ２０が、本発明のＶＰＮ通信装置に相当し、ＷＡＮ通信部２２が、本発明の第１通信手段に相当し、携帯電話通信部２３が、本発明の第２通信手段に相当し、ＬＡＮ側受信処理（図３）におけるＳ１０１が、本発明の鍵生成手段に相当し、ＬＡＮ側受信処理（図３）におけるＳ１０２，Ｓ１０５と、携帯側受信処理（図４）におけるＳ２０３とが、本発明の暗号通信手段に相当する。
【００５３】
［第２実施形態］
次に、第２実施形態の通信システムについて説明する。
図５は、第２実施形態の通信システムの概略構成図である。
【００５４】
同図に示すように、この通信システムにおいては、Ａ社に構築されたＬＡＮ１０ａと、Ｂ社に構築されたＬＡＮ１０ｂとが、それぞれＶＰＮルータ２０ａ，２０ｂを介してインターネット１に接続されている。また、ＶＰＮルータ２０ａ，２０ｂを管理する通信管理会社の通信管理装置３０が、インターネット１に接続されている。さらに、ＶＰＮルータ

２０ａ，２０ｂ及び通信管理装置３０は、それぞれ携帯電話網２を介して通信可能に構成されている。なお、本第２実施形態の通信システムに用いられるＶＰＮルータ２０ａ，２０ｂは、上記第１実施形態の通信システムに用いられるＶＰＮルータ２０（図２）と同一構成のものである。ただし、後述するように、制御部２４の行う処理が異なる。

【００５５】

ここで、本第２実施形態の通信システムに用いられる通信管理装置３０の構成について、図６のブロック図を用いて説明する。

同図に示すように、通信管理装置３０は、ＷＡＮ通信部３１、携帯電話通信部３２及び制御部３３を備えている。

【００５６】

ＷＡＮ通信部３１は、インターネット１に接続され、インターネット１からデータを受信して制御部３３へ送るとともに、制御部３３からのデータをインターネット１へ送信する。

【００５７】

携帯電話通信部３２は、携帯電話網２を介した無線通信を行うためのものであり、携帯電話網２からデータを受信して制御部３３へ送るとともに、制御部３３からのデータを携帯電話網２へ送信する。

【００５８】

制御部３３は、ＣＰＵ、ＲＯＭ、ＲＡＭ等からなる周知のマイクロコンピュータを中心に構成されており、本通信管理装置３０の各部を制御する。

次に、本第２実施形態の通信システムで行われる処理の概要について説明する。

【００５９】

本第２実施形態の通信システムにおいて、ＶＰＮルータ２０ａ，２０ｂ間での暗号通信によるＶＰＮを構築する場合には、まず、一方のＶＰＮルータ２０が、暗号通信に用いる共通鍵と、ＶＰＮの構築を希望する通信先の情報とを、携帯電話網２を介して通信管理装置３０へ送信する。すると、通信管理装置３０は、ＶＰＮルータ２０から受信した通信先の情報に基づき、ＶＰＮの構築を許可するか否かを判定し、許可すると判定した場合に、受信した共通鍵を通信先のＶＰＮルータ２０へ送信する。これにより、２つのＶＰＮルータ２０ａ，２０ｂで共通鍵が共有される。なお、共通鍵を共有した後の暗号通信自体は、従来のＶＰＮと同様の方法で行うことができる。

【００６０】

つまり、本第２実施形態の通信システムは、暗号化に用いる共通鍵の受渡しを、ＶＰＮルータ２０ａ，２０ｂ間で直接行うのではなく、通信管理装置３０を介して行う点で第１実施形態の通信システムと異なっている。

【００６１】

このため、本第２実施形態の通信システムに用いられるＶＰＮルータ２０が有する機能は、上記第１実施形態の通信システムに用いられるＶＰＮルータ２０が有する上記（Ａ）～（Ｅ）の機能と比較すると、次の点が異なっている。

【００６２】

上記（Ａ）については、共通鍵を通信先のＶＰＮルータ２０へ送信することに代えて、共通鍵とＶＰＮの構築を希望する通信先の情報とを通信管理装置３０へ送信する点、及び、通信先のＶＰＮルータ２０から許可通知を受信することに代えて、通信管理装置３０から受信する点。

【００６３】

上記（Ｂ）については、通信先のＶＰＮルータ２０から共通鍵を受信することに代えて、通信管理装置３０から受信する点、及び、許可通知を通信先のＶＰＮルータ２０へ送信することに代えて、通信管理装置３０へ送信する点。

【００６４】

上記（Ｃ）については、通信終了通知を通信先のＶＰＮルータ２０へ送信することに代えて、通信管理装置３０へ送信する点。

上記（Ｄ）については、通信先のＶＰＮルータ２０から通信終了通知を受信することに代えて、通信管理装置３０から受信する点。

【００６５】

次に、ＶＰＮルータ２０の制御部２４が実行する処理の具体的内容について説明する。

まず、ＬＡＮ通信部２１により通信開始指令が受信された場合に制御部２４が実行するＬＡＮ側受信処理について、図７のフローチャートを用いて説明する。

【００６６】

このＬＡＮ側受信処理が開始されると、まず、Ｓ３０１で、暗号通信に用いるための共通鍵を、例えばランダムに生成する。

続いて、Ｓ３０２では、Ｓ３０１で生成した共通鍵と、ＶＰＮの構築を希望する通信先の情報とを、携帯電話網２を介して通信管理装置３０へ送信する処理を、携帯電話通信部２３に行わせる。なお、通信管理装置３０の電話番号は、制御部２４に記憶されている。

【００６７】

続いて、Ｓ３０３では、Ｓ３０２での共通鍵の送信に対して通信管理装置３０から携帯電話網２を介して送信されてくる許可通知が携帯電話通信部２３により受信されたか否かを判定する。

【００６８】

このＳ３０３で、許可通知が受信されていないと判定した場合には、Ｓ３０４へ移行し、Ｓ３０２での共通鍵の送信から所定時間（あらかじめ設定された時間）が経過したか否かを判定する。

【００６９】

そして、Ｓ３０４で、所定時間が経過していないと判定した場合には、Ｓ３０３へ戻る。

一方、Ｓ３０４で、所定時間が経過したと判定した場合には、本ＬＡＮ側受信処理を終了する。つまり、共通鍵を送信したにもかかわらず許可通知が受信されない場合には処理を終了するようにしている。

【００７０】

これに対し、Ｓ３０３で、許可通知が受信されたと判定した場合には、Ｓ３０５へ移行し、Ｓ３０１で生成した共通鍵を用いて暗号通信処理を開始する。具体的には、ＬＡＮ通信部２１により受信されたデータを共通鍵を用いて暗号化してＷＡＮ通信部２２に送信させ、ＷＡＮ通信部２２により受信されたデータを共通鍵を用いて復号してＬＡＮ通信部２１に送信させる。

【００７１】

続いて、Ｓ３０６では、ＬＡＮ通信部２１により通信終了指令が受信されたか否かを判定する。

このＳ３０６で、通信終了指令が受信されていないと判定した場合には、Ｓ３０７へ移行し、ＷＡＮ通信部２２により通信終了通知が受信されたか否かを判定する。

【００７２】

そして、Ｓ３０７で、通信終了通知が受信されていないと判定した場合には、Ｓ３０６へ戻る。

一方、Ｓ３０７で、通信終了通知が受信されたと判定した場合には、本ＬＡＮ側受信処理を終了する。

【００７３】

また、Ｓ３０６で、通信終了指令が受信されたと判定した場合には、Ｓ３０８へ移行し、通信を終了する旨の通信終了通知を、インターネット１を介して通信管理装置３０へ送信する処理を、ＷＡＮ通信部２２に行わせる。その後、本ＬＡＮ側受信処理を終了する。

【００７４】

次に、携帯電話通信部２３により共通鍵が受信された場合に制御部２４が実行する携帯側受信処理について、図８のフローチャートを用いて説明する。

この携帯側受信処理が開始されると、まず、Ｓ４０１で、受信した共通鍵を記憶する。

【００７５】
続いて、Ｓ４０２では、通信管理装置３０に対し、通信を許可する旨の許可通知を携帯電話網２を介して送信する処理を、携帯電話通信部２３に行わせる。
続いて、Ｓ４０３では、受信した共通鍵を用いて暗号通信処理を開始する。具体的には、ＬＡＮ通信部２１により受信されたデータを共通鍵を用いて暗号化してＷＡＮ通信部２２に送信させ、ＷＡＮ通信部２２により受信されたデータを共通鍵を用いて復号してＬＡＮ通信部２１に送信させる。
【００７６】
続いて、Ｓ４０４では、ＬＡＮ通信部２１により通信終了指令が受信されたか否かを判定する。
このＳ４０４で、通信終了指令が受信されていないと判定した場合には、Ｓ４０５へ移行し、ＷＡＮ通信部２２により通信終了通知が受信されたか否かを判定する。
【００７７】
そして、Ｓ４０５で、通信終了通知が受信されていないと判定した場合には、Ｓ４０４へ戻る。
一方、Ｓ４０４で、通信終了指令が受信されたと判定した場合には、本携帯側受信処理を終了する。
【００７８】
また、Ｓ４０５で、通信終了通知が受信されたと判定した場合には、Ｓ４０６へ移行し、通信を終了する旨の通信終了通知を、インターネット１を介して通信管理装置３０へ送信する処理を、ＷＡＮ通信部２２に行わせる。その後、本携帯側受信処理を終了する。
【００７９】
次に、通信管理装置３０において、携帯電話通信部３２により共通鍵とＶＰＮの構築を希望する通信先の情報とが受信された場合に制御部３３が実行する通信管理処理について、図９のフローチャートを用いて説明する。
【００８０】
この通信管理処理が開始されると、まず、Ｓ５０１で、受信したＶＰＮの構築を希望する通信先の情報に基づき、ＶＰＮの構築（換言すれば、暗号通信）を許可するか否かを判定する。具体的には、制御部３３には、本通信管理会社に登録している複数の会社（ＶＰＮルータ２０の所有者）について、ＶＰＮルータ２０の電話番号や、ＶＰＮの構築要求があっても許可しない会社の情報等を登録したデータベースが記憶されており、このデータベースを参照することによりＶＰＮの構築を許可するか否かを判定する。
【００８１】
そして、Ｓ５０１で、ＶＰＮの構築を許可しないと判定した場合には、そのまま本通信管理処理を終了する。
一方、Ｓ５０１で、ＶＰＮの構築を許可すると判定した場合には、Ｓ５０２へ移行し、受信した共通鍵を、携帯電話網２を介して通信先のＶＰＮルータ２０へ送信する処理を、携帯電話通信部３２に行わせる。なお、通信先のＶＰＮルータ２０の電話番号は、データベースに記憶されている。
【００８２】
続いて、Ｓ５０３では、Ｓ５０２での共通鍵の送信に対して通信先のＶＰＮルータ２０から携帯電話網２を介して送信されてくる許可通知が携帯電話通信部３２により受信されたか否かを判定する。
【００８３】
このＳ５０３で、許可通知が受信されていないと判定した場合には、Ｓ５０４へ移行し、Ｓ５０２での共通鍵の送信から所定時間（あらかじめ設定された時間）が経過したか否かを判定する。
【００８４】
そして、Ｓ５０４で、所定時間が経過していないと判定した場合には、Ｓ５０３へ戻る。

一方、Ｓ５０４で、所定時間が経過したと判定した場合には、本通信管理処理を終了する。つまり、共通鍵を送信したにもかかわらず許可通知が受信されない場合には処理を終了するようにしている。

【００８５】

これに対し、Ｓ５０３で、許可通知が受信されたと判定した場合には、Ｓ５０５へ移行し、ＶＰＮ構築の要求元のＶＰＮルータ２０に対し、通信を許可する旨の許可通知を携帯電話網２を介して送信する処理を、携帯電話通信部３２に行わせる。

【００８６】

続いて、Ｓ５０６では、ＷＡＮ通信部３１により通信を終了する旨の通信終了通知が受信されたか否かを判定し、受信されたと判定した場合にＳ５０７へ移行する。

Ｓ５０６では、通信終了通知を、インターネット１を介して他方のＶＰＮルータ２０へ送信する処理を、ＷＡＮ通信部３１に行わせる。その後、本通信管理処理を終了する。

【００８７】

以上説明したように、本第２実施形態の通信システムによれば、上記第１実施形態の通信システムと同様の効果を得ることができる。

さらに、本第２実施形態の通信システムでは、例えば取引先の会社と一時的に機密性の高いデータのやり取りを行いたいといった場合に、通信管理装置３０を介して容易にＶＰＮを構築することができる。このため、電子メール等でデータをやり取りすることに比べ、セキュリティ性の高い通信を行うことができる。しかも、取引先でない会社やライバル会社等、ＶＰＮを構築したくない会社については、要求があっても許可しないようにすることができる。

【００８８】

加えて、本通信システムでは、通信管理会社が、ＶＰＮルータ２０の所有者に対し、ＶＰＮの構築以外のサービスを提供することも可能となる。例えば、通信管理装置３０をウェブサーバとして機能させ、ＶＰＮルータ２０の所有者のみが閲覧可能なウェブページを設けることができる。

【００８９】

なお、本第２実施形態の通信システムでは、ＶＰＮルータ２０が、本発明のＶＰＮ通信装置に相当し、ＷＡＮ通信部２２が、本発明の第１通信手段に相当し、携帯電話通信部２３が、本発明の第２通信手段に相当し、ＬＡＮ側受信処理（図７）におけるＳ３０１が、本発明の鍵生成手段に相当し、ＬＡＮ側受信処理（図７）におけるＳ３０２，Ｓ３０５と、携帯側受信処理（図８）におけるＳ４０３とが、本発明の暗号通信手段に相当する。また、通信管理装置３０が、本発明の管理装置に相当し、携帯電話通信部３２が、本発明の中継通信手段に相当し、通信管理処理（図９）におけるＳ５０１，Ｓ５０２の処理が、本発明の鍵配布手段に相当する。

【００９０】

以上、本発明の一実施形態について説明したが、本発明は、種々の形態を採り得ることは言うまでもない。

すなわち、上記各実施形態の通信システムでは、ＶＰＮルータ２０が、ＬＡＮ１０側に接続された機器から通信開始指令を受信することにより、暗号通信に用いる共通鍵を生成して送信するように構成されている。ここで、通信開始指令は、ＬＡＮ１０側の機器において、通信開始指令を送信するための所定の入力操作が利用者によって行われた場合に、そのＬＡＮ１０に接続されたＶＰＮルータ２０宛に送信される。

【００９１】

しかしながら、通信開始指令は、上記各実施形態のようにＶＰＮルータ２０宛に送信されるものに限ったものではない。例えば、ＶＰＮルータ２０は、特定の通信相手（通信先のＶＰＮルータ２０が設置されたＬＡＮ１０に接続されている機器等）のＩＰアドレスを通信先としたデータがＬＡＮ通信部２１から受信され、かつ、その通信相手との間で現在ＶＰＮが構築されていない状態の場合に、共通鍵を生成して送信するように構成されていてもよい。つまり、ＬＡＮ１０側の機器においてインターネット１を介した通信のために

通常行われる操作により送信されるデータを、ＶＰＮルータ２０で通信開始指令として認識するのである。このようにすれば、ＬＡＮ１０側の機器の利用者に暗号通信の開始操作を意識させることなく、暗号通信を開始することができる。

【００９２】

さらに、上記各実施形態の通信システムでは、ＶＰＮルータ２０が、ＬＡＮ１０側に接続された機器から通信終了指令を受信することにより、通信を終了する旨の通信終了通知を送信し、暗号通信を終了するように構成されている。ここで、通信終了指令は、ＬＡＮ１０側の機器において、通信終了指令を送信するための所定の入力操作が利用者によって行われた場合に、そのＬＡＮ１０に接続されたＶＰＮルータ２０宛に送信される。

【００９３】

しかしながら、通信終了指令の送信も、上記各実施形態のようにＶＰＮルータ２０宛に送信されるものに限ったものではない。例えば、ＶＰＮルータ２０は、暗号通信を行っている状態で、その通信相手のＩＰアドレスを通信先としたデータであって一連の暗号通信を終了する内容のものがＬＡＮ通信部２１から受信された場合に、暗号通信を終了するように構成されていてもよい。つまり、ＬＡＮ１０側の機器においてインターネット１を介した通信のために通常行われる操作により送信されるデータを、ＶＰＮルータ２０で通信終了指令として認識するのである。このようにすれば、ＬＡＮ１０側の機器の利用者に暗号通信の終了操作を意識させることなく、暗号通信を終了することができる。一方、ＶＰＮルータ２０が、例えば、ＶＰＮを構築した通信先との暗号通信が行われていない状態が一定時間継続したと判定した場合に、暗号通信を終了するように構成されていてもよい。

【００９４】

また、上記各実施形態の通信システムでは、暗号通信を要求したＶＰＮルータ２０は、許可通知を受信後に暗号通信処理を開始するようにしているが、このような許可通知の送受信を行うことなく暗号通信処理を開始する構成としてもよい。

【００９５】

さらに、上記各実施形態の通信システムでは、暗号通信を行っていない状態ではＷＡＮ通信部２２の機能を停止するようにしているが、暗号通信を行っていない状態でも機能する構成とすることも可能である。

【００９６】

一方、上記各実施形態の通信システムでは、携帯電話網２を介して共通鍵の受渡しを行うようにしているが、これに限ったものではなく、例えば、固定電話網やＩＳＤＮを介して共通鍵の受渡しを行う構成としてもよい。

【００９７】

また、上記各実施形態の通信システムでは、ＶＰＮルータ２０を用いてＶＰＮを構築するようにしているが、ＶＰＮ機能を有するルータ以外の通信装置を用いた構成であってもよい。例えば、電子メールサーバにＶＰＮ機能を持たせ、電子メールサーバ間でＶＰＮを構築すれば、電子メールを安全に送受信することが可能となる。

【００９８】

さらに、上記各実施形態の通信システムでは、共通鍵を用いた暗号通信により通信のセキュリティ性を確保しているが、これに加え、例えば、通信データの一部（例えば、重要な情報やキーワードとなる情報等）をインターネット１を介さず携帯電話網２を介して通信するようにすれば、セキュリティ性を一層向上させることができる。

【００９９】

加えて、上記各実施形態の通信システムでは、２台のＶＰＮルータ２０ａ，２０ｂによるＶＰＮの構築を例示したが、３台以上のＶＰＮルータで共通鍵を共有することによりＶＰＮを構築することも可能である。また、通信先のＶＰＮルータと共通鍵とを対応させて記憶することで、一つのＶＰＮルータが、同時に複数のＶＰＮを構築することも可能である。

【０１００】

一方、上記第２実施形態の通信システムでは、ＶＰＮルータ２０が生成した共通鍵を、

通信管理装置３０を介して通信先のＶＰＮルータ２０へ送信するようにしているが、これに限ったものではない。例えば、ＶＰＮルータ２０からのＶＰＮ構築の要求により、通信管理装置３０が、暗号通信を行う各ＶＰＮルータ２０へ共通鍵を配布する構成としてもよい。この場合、ＶＰＮ構築の要求は、インターネット１を介して行うようにすることも可能である。

【０１０１】

また、上記第２実施形態の通信システムでは、通信管理装置３０が、暗号通信の開始のみならず暗号通信の終了にも関与しているが、これに限ったものではなく、例えば、暗号通信の終了はＶＰＮルータ２０間で直接行うようにしてもよい。

【図面の簡単な説明】

【０１０２】

【図１】第１実施形態の通信システムの概略構成図である。

【図２】ＶＰＮルータの構成を表すブロック図である。

【図３】第１実施形態のＬＡＮ側受信処理のフローチャートである。

【図４】第１実施形態の携帯側受信処理のフローチャートである。

【図５】第２実施形態の通信システムの概略構成図である。

【図６】通信管理装置３０の構成を表すブロック図である。

【図７】第２実施形態のＬＡＮ側受信処理のフローチャートである。

【図８】第２実施形態の携帯側受信処理のフローチャートである。

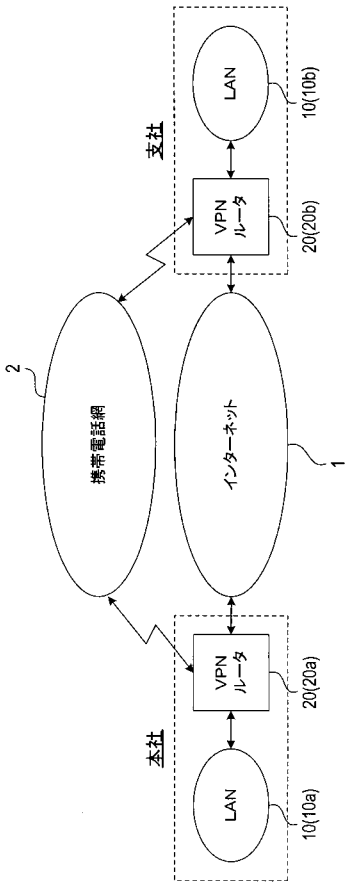
【図９】第２実施形態の通信管理処理のフローチャートである。

【符号の説明】

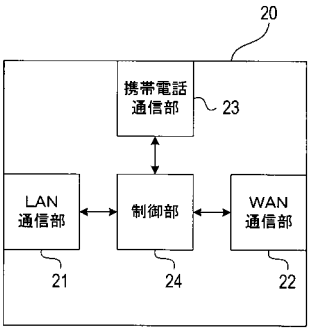
【０１０３】

１…インターネット、２…携帯電話網、１０…ＬＡＮ、２０…ＶＰＮルータ、２１…ＬＡＮ通信部、２２…ＷＡＮ通信部、２３…携帯電話通信部、２４…制御部、３０…通信管理装置、３１…ＷＡＮ通信部、３２…携帯電話通信部、３３…制御部

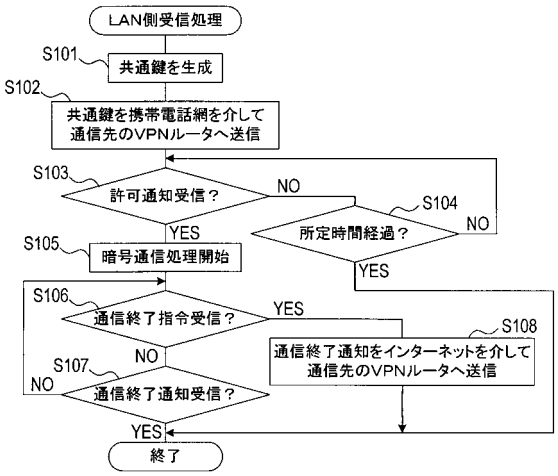
【図１】



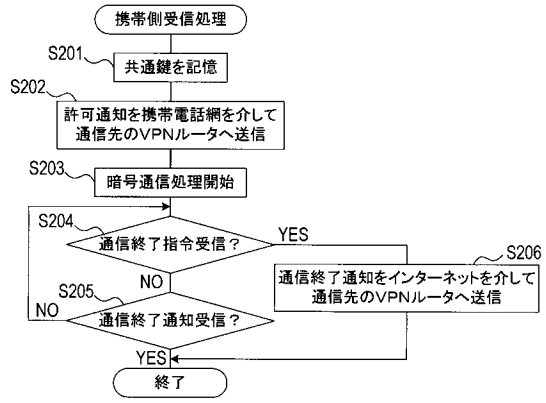
【図２】



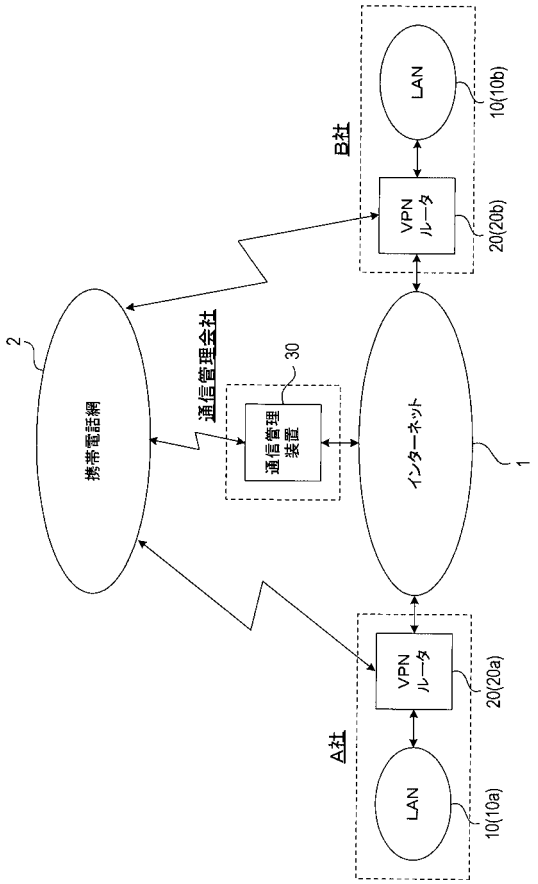
【図３】



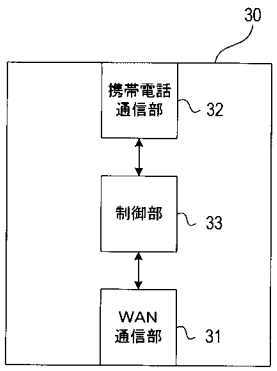
【図４】


携帯側受信処理
S201
共通鍵を記憶
S202
許可通知を携帯電話網を介して
通信先のVPNルータへ送信
S203
暗号通信処理開始
S204
通信終了指令受信？
YES
S206
通信終了通知をインターネットを介して
通信先のVPNルータへ送信
NO
S205
NO
通信終了通知受信？
YES
終了

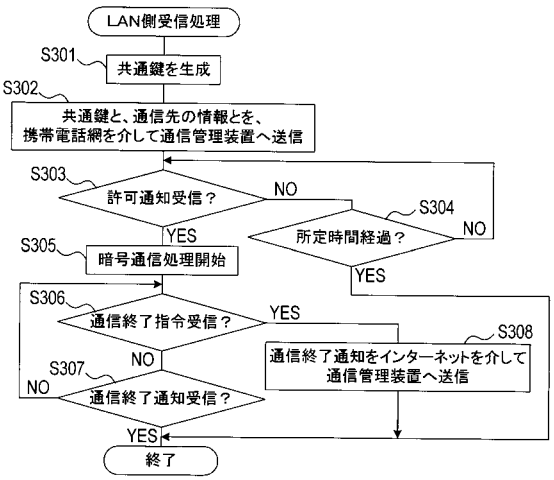
【図５】


B社
LAN
10(10b)
VPN
ルータ
20(20b)
2
携帯電話網
通信管理会社
30
通信管理
装置
インターネット
1
VPN
ルータ
20(20a)
A社
LAN
10(10a)

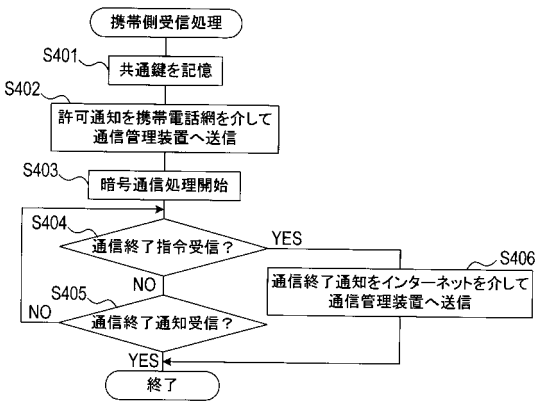
【図６】


30
携帯電話
通信部
32
制御部
33
WAN
通信部
31

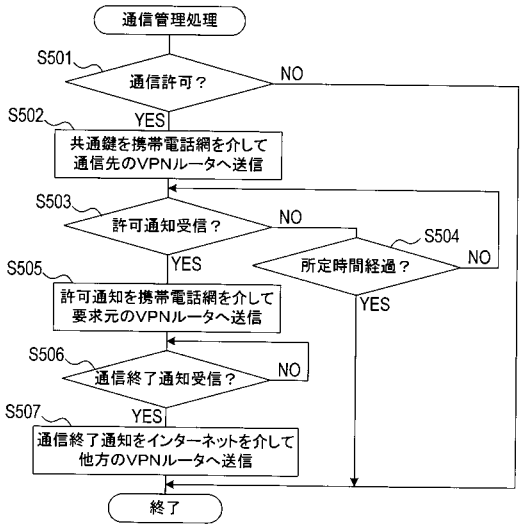
【図７】


LAN側受信処理
S301
共通鍵を生成
S302
共通鍵と、通信先の情報とを、
携帯電話網を介して通信管理装置へ送信
S303
許可通知受信？
NO
S304
所定時間経過？
NO
YES
S305
暗号通信処理開始
YES
S306
通信終了指令受信？
YES
S308
通信終了通知をインターネットを介して
通信管理装置へ送信
NO
S307
NO
通信終了通知受信？
YES
終了

【図８】


携帯側受信処理
S401
共通鍵を記憶
S402
許可通知を携帯電話網を介して
通信管理装置へ送信
S403
暗号通信処理開始
S404
通信終了指令受信？
YES
S406
通信終了通知をインターネットを介して
通信管理装置へ送信
NO
S405
NO
通信終了通知受信？
YES
終了

【図９】


通信管理処理
S501
通信許可？
NO
YES
S502
共通鍵を携帯電話網を介して
通信先のVPNルータへ送信
S503
許可通知受信？
NO
S504
所定時間経過？
NO
YES
YES
S505
許可通知を携帯電話網を介して
要求元のVPNルータへ送信
S506
通信終了通知受信？
NO
YES
S507
通信終了通知をインターネットを介して
他方のVPNルータへ送信
終了