(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2008-104040
(P2008-104040A)
(43)公開日　平成20年5月1日(2008.5.1)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/08	(2006.01)	H04L	9/00	601C	5J104
		H04L	9/00	601E	

審査請求 未請求　請求項の数 5　ＯＬ　（全 86 頁）

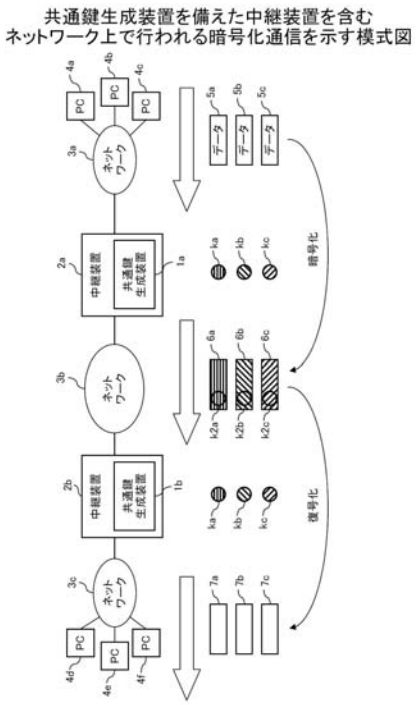
(21)出願番号　特願2006-285874 (P2006-285874)
(22)出願日　平成18年10月20日 (2006.10.20)

(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　100074099
弁理士　大菅　義之
(74)代理人　100067987
弁理士　久木元　彰
(72)発明者　飯田　貴光
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　櫻井　秀志
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】共通鍵生成装置および共通鍵生成方法

(57)【要約】
【課題】共通鍵暗号方式で用いられる共通鍵を生成する共通鍵生成装置であって、比較的簡易な構成により暗号の安全度を中程度に保つことができ、かつ、暗号化通信を行う相手の数の暗号鍵を管理する必要がない、共通鍵生成装置を提供する。
【解決手段】共通鍵生成装置１ａおよび１ｂは、データ５ａ～５ｃごとに異なる鍵素材ｋ２ａ～ｋ２ｃに基づいて共通鍵ｋａ～ｋｃを生成する。共通鍵生成装置１ａおよび１ｂは、異なる値の鍵素材に対しては、事実上、異なる値の共通鍵を生成するように構成されている。暗号化データ６ａ～６ｃは、共通鍵ｋａ～ｋｃにより暗号化された部分とクリアテキストの部分を有する。後者の部分には共通鍵生成装置１ａが用いた鍵素材ｋ２ａ～ｋ２ｃが含まれ、それらは共通鍵生成装置１ｂにおいて共通鍵ｋａ～ｋｃの生成に利用される。
【選択図】図１



【特許請求の範囲】
【請求項１】
共通鍵暗号方式に用いられる共通鍵を生成する共通鍵生成装置であって、
クリアテキストの状態のヘッダ部と、ペイロード部とを有する入力データを受け付ける受付手段と、
鍵素材を格納する鍵素材格納手段と、
前記入力データの暗号化のために前記共通鍵を生成する第一の局面では、前記鍵素材を前記鍵素材格納手段から読み取り、前記鍵素材格納手段内の前記鍵素材を更新し、前記入力データの復号化のために前記共通鍵を生成する第二の局面では、前記ヘッダ部の所定の部分から前記鍵素材を読み取る、鍵素材読み取り手段と、
前記鍵素材読み取り手段が読み取った前記鍵素材に基づいて前記共通鍵を生成する共通鍵生成手段と、
を備えることを特徴とする共通鍵生成装置。
【請求項２】
通信路上に前記共通鍵生成装置が配置され、
前記入力データは、前記通信路を通って送信元から送信先へ送られるときに前記共通鍵生成装置を経由して、前記受付手段により受け付けられ、
前記共通鍵生成手段は、前記送信元または前記送信先の少なくとも一方のアドレスに基づいて前記共通鍵を生成する、
ことを特徴とする請求項１に記載の共通鍵生成装置。
【請求項３】
事前共有鍵として同一の値を設定された二つの前記共通鍵生成装置が通信路上に配置され、
前記入力データは、前記経路を、送信元、送信側の前記共通鍵生成装置、受信側の前記共通鍵生成装置、送信先の順に経由して送信され、
前記入力データは、二つの前記共通鍵生成装置を経由する際にそれぞれの前記受付手段で受け付けられ、
二つの前記共通鍵生成装置のそれぞれの前記共通鍵生成手段は、前記事前共有鍵に基づいて前記共通鍵を生成する、
ことを特徴とする請求項１に記載の共通鍵生成装置。
【請求項４】
Ｍを２以上の整数として、前記事前共有鍵に基づいてＭ個の値を候補値として生成する候補値生成手段と、
Ｍ個の前記候補値を格納する候補値格納手段とをさらに備え、
前記共通鍵生成手段は、前記鍵素材に基づいてＭ個の前記候補値のうちの一つを選択して前記候補値格納手段から読み取り、該候補値に基づいて前記共通鍵を生成する、
ことを特徴とする請求項３に記載の共通鍵生成装置。
【請求項５】
共通鍵暗号方式において使われる共通鍵を生成する共通鍵生成方法であって、
クリアテキストの状態のヘッダ部と、ペイロード部とを有する入力データを受け付ける受付ステップと、
前記入力データの暗号化のために前記共通鍵を生成する第一の局面では、鍵素材を格納する鍵素材格納手段から前記鍵素材を読み取り、前記鍵素材格納手段内の前記鍵素材を更新し、前記入力データの復号化のために前記共通鍵を生成する第二の局面では、前記ヘッダ部の所定の部分から前記鍵素材を読み取る鍵素材読み取りステップと、
読み取った前記鍵素材に基づいて前記共通鍵を生成する共通鍵生成ステップと、
を備えることを特徴とする共通鍵生成方法。
【発明の詳細な説明】
【技術分野】
【０００１】

本発明は、共通鍵暗号方式に用いられる共通鍵を生成する装置および方法に関する。

【背景技術】

【０００２】

暗号方式には、暗号化と復号化に同じ鍵を用いる共通鍵暗号方式（秘密鍵暗号方式、または対称鍵暗号方式ということもある）と、暗号化と復号化に異なる鍵を用いる公開鍵暗号方式がある。公開鍵暗号方式に比べて、共通鍵暗号方式は暗号化や復号化を高速に行うことができるという利点があり、様々な用途で使われている。共通鍵暗号方式の代表的な規格にはＤＥＳ（Data Encryption Standard）やＡＥＳ（Advanced Encryption Standard）がある。なお、以下では共通鍵暗号方式における暗号化鍵と復号化鍵をまとめて共通鍵とよぶ。

【０００３】

しかし、共通鍵暗号方式では、第三者に共通鍵が漏洩すると暗号文が解読される危険性が高いので、第三者に対して共通鍵を秘密に保つことが重要である。具体的には下記（１）と（２）の観点を考慮する必要がある。

【０００４】

（１）暗号化通信を始める前に、メッセージの送信者と受信者（すなわち、暗号化する側と復号化する側）が共通鍵を共有する必要がある。共通鍵を共有する方法には、例えば、メッセージの送信者が共通鍵を生成して、通信路を介して受信者にその共通鍵を送信する方法がある。しかし、その場合、いかにして第三者には共通鍵の内容が分からないように共通鍵を送信するのかという問題が生じる。

【０００５】

（２）同じ一つの共通鍵を使って何度も暗号化通信を繰り返すと、第三者が暗号文を傍受して共通鍵を推測し、以降の暗号文を解読してしまうという危険性が増す。暗号文を傍受されても共通鍵が推測されにくいようにする必要がある。

【０００６】

上記（１）と（２）の問題に対しては、様々な方法が提案され実際に利用されている。

例えば、特許文献１に記載の暗号装置は、（２）で述べた危険性を減らすため、規則的なパターンが暗号文に周期的に現れるのを防いでいる。具体的には、複数のフレームからなる超フレームを暗号化する際、フレーム同期パターンを検出することにより超フレーム内でのフレーム番号を数え、フレーム番号ごとに異なる暗号鍵で当該フレームを暗号化する。そして、超フレーム同期パターンを除く超フレーム全体を別の暗号鍵で暗号化する。以上の構成によって、特許文献１に記載の暗号装置は、フレーム同期パターンが同じ暗号鍵で暗号化されるためにフレーム周期で規則的なパターンが暗号文に現れる、ということを防いでいる。

【０００７】

あるいは、一定期間が経過するたびに共通鍵を更新することにより、（２）で述べた危険性を減らすことができる。しかし、更新した新たな共通鍵を送信者と受信者が共有する際には、上記（１）の問題が再び生じる。

【０００８】

例えば、特定の一組の送信者と受信者の間でのみ暗号化通信を行う場合なら、送信者が共通鍵を生成し、共通鍵の内容を紙に書いてその紙を受信者に手渡しすることによって、上記（１）の問題を解決してもよい。ただしこの方法は、多くの相手と暗号化通信を行う場合には適さず、共通鍵を更新するたびに煩わしい手作業が必要となる、という欠点がある。

【０００９】

暗号化の対象がＩＰ（Internet Protocol）パケットの場合は、非特許文献１のＩＰｓｅｃ（Security Architecture for Internet Protocol）により上記（１）と（２）の問題をともに解決することができる。ＩＰｓｅｃは、ＩＰパケットを暗号化するための規格であり、共通鍵暗号方式を採用している。ＩＰｓｅｃは複数のプロトコルと暗号化アルゴリズムの集まりであり、そのうちの一つが鍵交換プロトコルのＩＫＥ（Internet Key Exc

hange）である。

【００１０】

ＩＫＥによって、送信者と受信者は安全に（すなわち第三者に内容を知られることなく）通信路を介して共通鍵の生成に必要な情報を交換することができ、煩わしい手動の操作を必要とせずに（１）の問題を解決することができる。共通鍵を更新することは「リキー（rekey）」と呼ばれるが、一定期間ごとに（または通信量が所定のバイト数を超えるごとに）ＩＫＥを使って自動的にリキーを行うことにより、上記（２）の問題も解決することができる。

【００１１】

しかしながら、このように自動的かつ動的に鍵交換を行うシステムには、下記（３）～（５）の問題がある。

（３）リキーを行っている最中には暗号化通信を行うことができない。

【００１２】

（４）ＩＫＥは比較的複雑な仕組みなので、ルータなどの装置の実装が複雑であり、鍵交換の際に不具合が発生しやすい。

（５）送信者と受信者の一方の装置に故障が発生すると、新たに共通鍵を共有するステップから始めなくてはならない。そのための鍵交換において、（４）の理由から、他方の装置にも不具合が発生するかもしれない。

【００１３】

また、共通鍵暗号方式には下記（６）の問題もある。

（６）送信者と受信者の組ごとに異なる共通鍵が必要である。つまり、ＡとＢの間で使われる共通鍵k_{AB}と、ＡとＣの間で使われる共通鍵k_{AC}は、異なっていなくてはならない。もしk_{AB}とk_{AC}が等しいと、ＡとＢの間の暗号化通信がＣにより解読されてしまい、秘密を保てないからである。よって、Ｎ対Ｎの関係で暗号化通信を行う場合には、相手ごとに異なる共通鍵をそれぞれの装置が管理する必要がある。

【００１４】

このように複数の共通鍵を管理する構成は、例えば特許文献２に見られる。特許文献２は、受動光ネットワーク（ＰＯＮ；Passive Optical Network）システムにおいて、下り方向に送信されるイーサネットフレームを暗号化する技術を開示している（「イーサネット」および「Ethernet」は登録商標）。

【００１５】

下り方向とは親局から子局に向かう方向である。特許文献２のシステムでは、親局であるＯＬＴ（Optical Line Terminal；光加入者線終端装置）に子局であるＯＮＴ（Optical Network Terminal；光網終端装置）が複数接続され、各ＯＮＴには複数の端末（パーソナルコンピュータ等）が接続されている。ＯＬＴはＯＮＴごとに異なる暗号鍵を保持している。下り方向のイーサネットフレームは、一つのＯＬＴからそのＯＬＴに接続された複数のＯＮＴへ同報されるが、その際にＯＬＴは、フレームの宛先がどのＯＮＴに接続された端末なのかを判別し、当該ＯＮＴに対応する暗号鍵でそのイーサネットフレームを暗号化する。したがって、他のＯＮＴはそのイーサネットフレームを受信しても復号化することができず、内容を知ることができない。

【００１６】

上記（６）の問題は、単に管理すべき共通鍵の個数が多いというだけではない。例えば、上記（２）の危険性を減らすために、それら多くの共通鍵のそれぞれについて一定期間ごとにリキーを行うことが好ましいが、共通鍵の数が多いほど、上記（３）～（５）の問題はより深刻となる。すなわち、スケーラビリティに制約がある。

【００１７】

なお、上記（６）の説明におけるＡ、Ｂ、Ｃは、一般にはネットワーク上の中継装置であって個々の端末ではない。例えば、ＩＰｓｅｃによりＩＰパケットを暗号化する場合、暗号化を行うのはルータなどのネットワーク層の中継装置である。よって、正確には、上記（６）は、ルータ同士の組ごとに異なる共通鍵が必要だという意味である。

【００１８】
例えば、図２８に示した構成のネットワークにおいてＩＰｓｅｃによる暗号化通信を行う場合、ルータ８ａと８ｂはそれぞれ共通鍵ｋｄを記憶しており、ルータ８ａと８ｂの間のネットワーク３ｂでは、ＩＰパケットが共通鍵ｋｄによって暗号化された状態で送信される。図２８において、ルータ８ａにはネットワーク３ａを介してＰＣ（Personal Computer）４ａ～４ｃが接続されており、ルータ８ｂにはネットワーク３ｃを介してＰＣ４ｄ～４ｆが接続されている。
【００１９】
ここで、ＰＣ４ａからＰＣ４ｄにＩＰパケット２５０ａを送信し、ＰＣ４ｂからＰＣ４ｅにＩＰパケット２５０ｂを送信し、ＰＣ４ｃからＰＣ４ｆにＩＰパケット２５０ｃを送信する場合、これら送信元も送信先も異なる三つのＩＰパケット２５０ａ～２５０ｃのそれぞれは、同じ共通鍵ｋｄにより暗号化されて暗号化ＩＰパケット２６０ａ～２６０ｃとなり、その後、共通鍵ｋｄにより復号化されて復号化ＩＰパケット２８０ａ～２８０ｃとなる。すなわち、共通鍵ｋｄはルータ８ａと８ｂの組に対して一意に定められているため、送信元と送信先のＰＣの組み合わせによらず、常に同じ共通鍵ｋｄが利用される。つまり、送信元と送信先のＰＣの組み合わせごとに異なる共通鍵で暗号化する場合に比べて、暗号化の粒度は粗い。
【特許文献１】実開平５－８５１４０号公報
【非特許文献１】RFC4301 Security Architecture for the Internet Protocol http://www.ietf.org/rfc/rfc4301.txt （閲覧確認：２００６年１０月６日）
【特許文献２】特開２００３－６０６３３号公報
【発明の開示】
【発明が解決しようとする課題】
【００２０】
上記のことから、共通鍵暗号方式に関する一般的な傾向として次のことが言える。手動で共通鍵を設定し、同じ共通鍵を長期間にわたって使い続ける（共通鍵が固定的である）場合には、システムは比較的簡単で済むが、暗号の安全度が低い。一方、ＩＫＥを利用するなどして自動的かつ動的にリキーを行う場合には、複雑なシステムが必要であり複雑さに起因する問題も生じるが、暗号の安全度が高い。
【００２１】
しかし、暗号化通信を行う目的や用途によっては、システムの複雑さと暗号の安全度がともに中程度となるような方法が適切である。
また、上記（６）の問題に対して、暗号化通信を行う相手の数だけ共通鍵を管理する必要をなくせば、共通鍵暗号方式の適用範囲を広げることができる。
【００２２】
本発明の目的は、共通鍵暗号方式で用いられる共通鍵を生成する共通鍵生成装置であって、比較的簡易な構成により暗号の安全度を中程度に保つことができ、かつ、暗号化通信を行う相手の数の暗号鍵を管理する必要がない共通鍵生成装置を提供することである。また、そのような共通鍵生成装置による共通鍵生成方法を提供することも本発明の目的である。
【課題を解決するための手段】
【００２３】
本発明による共通鍵生成装置は、共通鍵暗号方式に用いられる共通鍵を生成する共通鍵生成装置であって、クリアテキストの状態のヘッダ部と、ペイロード部とを有する入力データを受け付ける受付手段と、鍵素材を格納する鍵素材格納手段と、前記入力データの暗号化のために前記共通鍵を生成する第一の局面では、前記鍵素材を前記鍵素材格納手段から読み取り、前記鍵素材格納手段内の前記鍵素材を更新し、前記入力データの復号化のために前記共通鍵を生成する第二の局面では、前記ヘッダ部の所定の部分から前記鍵素材を読み取る、鍵素材読み取り手段と、前記鍵素材読み取り手段が読み取った前記鍵素材に基づいて前記共通鍵を生成する共通鍵生成手段と、を備えることを特徴とする。

【００２４】
本発明による共通鍵生成方法は、上記共通鍵生成装置によって実行される方法である。
通信路上の暗号化側と復号化側の双方に上記の共通鍵生成装置を備えて利用すると、鍵交換プロトコルによる鍵交換なしに、暗号化側と復号化側の双方が同じ値の共通鍵を生成する。すなわち、暗号化側で、ヘッダ部の所定の部分に鍵素材を含めたデータを生成すれば、復号化側に備えられた共通鍵生成装置は、上記第二の局面の動作により、暗号化に用いられたのと同じ値の共通鍵を生成する。また、暗号化側に備えられた共通鍵生成装置は上記第一の局面の動作により共通鍵を生成するので、暗号化のたびに、つまり入力データごとに、値が更新された鍵素材に基づいて共通鍵が生成される。
【発明の効果】
【００２５】
鍵素材の値が異なれば共通鍵の値も実質的に異なるように上記共通鍵生成手段を適切に構成しておくことにより、暗号化のたびに実質的に異なる鍵を生成することが可能である。また、上記のとおり、通信路上の暗号化側と復号化側にそれぞれ備えられた共通鍵生成装置は同じ値の共通鍵を生成する。よって、本発明によれば、暗号化側の装置と復号化側の装置が鍵交換プロトコルにしたがって鍵交換を行い、リキーを行う必要なしに、実質的に入力データごとに異なる鍵を使ってデータの暗号化を行うことができる。その結果、暗号が解読される危険性を減らすこともできる。
【発明を実施するための最良の形態】
【００２６】
以下、本発明の実施形態について、図面を参照しながら詳細に説明する。なお、実質的に同一のものに対しては、同じ番号または添え字のみが異なる番号を付して説明を省略する。
【００２７】
本発明の共通鍵生成装置は、データを暗号化するために共通鍵を生成するのにも用いられ、データを復号化するために共通鍵を生成するのにも用いられる。よって、好ましい実施形態の一例は、本発明の共通鍵生成装置がネットワーク上の中継装置の一部として実装される実施形態であり、以下では主にそのような実施形態について述べる。
【００２８】
まず図１～図２を参照して、本発明による共通鍵生成装置がネットワーク上の中継装置の一部として実装される実施形態について一般的な説明を行う。次に、図３を参照して本発明による共通鍵生成装置が共通鍵の生成に利用する情報を説明し、図４を参照して共通鍵生成装置の基本的な構成を説明し、図５を参照して図１のより好適な実施形態を説明する。その後、図６～図１７を参照して、ＯＳＩ（Open Systems Interconnection）参照モデルにおけるデータリンク層（レイヤ２ともいう）の中継装置の一部として本発明による共通鍵生成装置が実装される実施形態について説明する。そして、図１８～図２６を参照して、ＯＳＩ参照モデルにおけるネットワーク層（レイヤ３ともいう）の中継装置の一部として本発明による共通鍵生成装置が実装される実施形態について説明する。
【００２９】
図１は、本発明の共通鍵生成装置を備えた中継装置を含むネットワーク上で行われる暗号化通信を示す模式図である。
図１において、中継装置２ａおよび２ｂは、それぞれ共通鍵生成装置１ａおよび１ｂを備え、ネットワーク３ｂを介して接続されている。また、中継装置２ａにはネットワーク３ａを介してＰＣ４ａ～４ｃが接続されており、中継装置２ｂにはネットワーク３ｂを介してＰＣ４ｄ～４ｆが接続されている。例えばＰＣ４ａからＰＣ４ｄにデータを送るとき、そのデータは、ＰＣ４ａ、中継装置２ａ、中継装置２ｂ、ＰＣ４ｄを含む通信路を経由する。
【００３０】
詳しくは後述するが、中継装置２ａおよび２ｂは、レイヤ２の中継装置でもよく、レイヤ３の中継装置でもよい。前者の場合、送受信されるデータ（５ａ～５ｃ、６ａ～６ｃ、

７ａ～７ｃ）は例えばＭＡＣ（Media Access Control）フレームであり、後者の場合、送受信されるデータは例えばＩＰパケットである。

【００３１】

図１では、送信元のＰＣ（４ａ～４ｃのいずれか）からデータ５ａが中継装置２ａを経由して送信されるとき、中継装置２ａに備えられた共通鍵生成装置１ａが鍵素材ｋ２ａに基づいて共通鍵ｋａを生成する。そしてデータ５ａは共通鍵ｋａにより暗号化されて暗号化データ６ａとなる。なお、詳しくは後述するが、暗号化データ６ａは、共通鍵ｋａにより暗号化された部分とクリアテキストの部分とを有し、鍵素材ｋ２ａをクリアテキストの部分に含む。暗号化データ６ａはネットワーク３ｂを経由して中継装置２ｂで受信される。受信後、中継装置２ｂに備えられた共通鍵生成装置１ｂが鍵素材ｋ２ａに基づいて共通鍵ｋａを生成する。共通鍵生成装置１ａと１ｂは同じアルゴリズムにより共通鍵を生成するため、同じ鍵素材ｋ２ａからは同じ共通鍵ｋａが生成される。そして、暗号化データ６ａは共通鍵ｋａによって復号化されて復号化データ７ａとなり、送信先のＰＣ（４ｄ～４ｆのいずれか）に送信される。

【００３２】

同様にして、データ５ｂは、鍵素材ｋ２ｂに基づいて生成される共通鍵ｋｂによって暗号化されて暗号化データ６ｂ（鍵素材ｋ２ｂを含む）となり、暗号化データ６ｂは共通鍵ｋｂによって復号化されて復号化データ７ｂとなる。また、データ５ｃも同様にして、鍵素材ｋ２ｃに基づいて生成される共通鍵ｋｃによって暗号化されて暗号化データ６ｃ（鍵素材ｋ２ｃを含む）となり、暗号化データ６ｃは共通鍵ｋｃによって復号化されて復号化データ７ｃとなる。

【００３３】

ここで、鍵素材ｋ２ａ～ｋ２ｃは互いに異なる値である。つまり、データ５ａ～５ｃごとに異なる値の鍵素材ｋ２ａ～ｋ２ｃが利用される。そして、異なる値の鍵素材ｋ２ａ～ｋ２ｃからは異なる値の共通鍵ｋａ～ｋｃが生成されるように共通鍵生成装置１ａおよび１ｂが構成されている（詳細は後述）。なお、正確に言えば、その構成は、異なる値の二つの鍵素材から同じ値の共通鍵が生成される割合を、無視しても実際の運用に支障がない程度に低くする構成であればよい（つまり、理論上、異なる値の二つの鍵素材から同じ値の共通鍵が生成される可能性があってもかまわない）。そのように共通鍵生成装置１ａおよび１ｂを構成すると、事実上、共通鍵ｋａ～ｋｃは互いに異なる値となる。

【００３４】

なお、共通鍵生成装置１ａと１ｂは、同じアルゴリズムで鍵素材から共通鍵を生成する。そのアルゴリズムを第三者に対して秘密にすれば、第三者が暗号化データ６ａ～６ｃを傍受しても、そこに含まれる鍵素材ｋ２ａ～ｋ２ｃから共通鍵ｋａ～ｋｃを生成することは不可能である。あるいは、第三者には秘密の情報を共通鍵生成装置１ａと１ｂが予め共有し、その情報と鍵素材ｋ２ａ～ｋ２ｃの両方に基づいて共通鍵ｋａ～ｋｃを生成してもよい。それにより、第三者が鍵素材ｋ２ａ～ｋ２ｃから共通鍵ｋａ～ｋｃを生成して暗号化データ６ａ～６ｃを解読することを防げる。

【００３５】

いずれにしろ、事実上、共通鍵ｋａ～ｋｃは互いに異なる値である。換言すれば、中継装置２ａと２ｂの間の通信路において、暗号化のために使われる共通鍵は非常に頻繁に変更されている。共通鍵暗号方式において共通鍵を変更する頻度が高いことは、セキュリティレベルの向上に寄与する。また、上記の仕組みは、共通鍵生成装置１ａと１ｂの間でＩＫＥのような複雑なプロトコルによって情報を交換する必要がないという利点もある。さらに、データ５ａ～５ｃごとに異なる値の鍵素材ｋ２ａ～ｋ２ｃは、例えば、単純なカウンタの値でもよく、暗号化通信を行う送信元と送信先の組ごとに共通鍵を管理する必要もない。

【００３６】

図１では、共通鍵ｋａ～ｋｃの値が互いに異なることを、共通鍵ｋａ～ｋｃのハッチングの線の向きを変えることによって表している。また、暗号化データ６ａ～６ｃが互いに

異なる鍵によって暗号化されていることを、暗号化データ６ａ～６ｃのハッチングの線の向きを変えることによって表している。

【００３７】

また、データ５ａ～５ｃは、ＰＣ４ａ～４ｃのいずれが送信元でもよく、ＰＣ４ｄ～４ｆのいずれが送信先でもよい。例えば、図２に示すように、データ５ａ～５ｃの送信元と送信先が全て異なっていてもよく（場合（Ａ））、送信元が全て同じで送信先が全て異なっていてもよく（場合（Ｂ））、送信元が全て異なっており送信先が全て同じでもよく（場合（Ｃ））、送信元と送信先が全て同じでもよい（場合（Ｄ））。

【００３８】

場合（Ａ）～（Ｄ）のいずれであっても、共通鍵ｋａ、ｋｂ、ｋｃは互いに異なる値であり、共通鍵生成装置１ａと１ｂの双方が同じ値の共通鍵を生成する点は同じである。これは本発明の特徴であり、例えば従来のＩＰｓｅｃによる暗号化通信（図２８）と全く異なる特徴である。図２８では、ルータ８ａと８ｂの組に対して共通鍵ｋｄが定められており、リキーを行わない限り共通鍵ｋｄの値は変わらない。そして、その同じ共通鍵ｋｄが、異なる三つのＩＰパケット２５０ａ～２５０ｃの暗号化および復号化に使われる。このことは、暗号化ＩＰパケット２６０ａ～２６０ｃの全てを同じパターンのハッチングとすることにより図にも表してある。

【００３９】

図３は、本発明による共通鍵生成装置（図１の共通鍵生成装置１ａおよび１ｂに相当）が、このようにデータごとに異なる共通鍵を生成するために用いる情報を示す図である。図３において、実線は必須であることを示し、破線は、必須ではないが利用する方が好ましいことを示す。

【００４０】

本発明による共通鍵生成装置は、暗号化および復号化のための共通鍵ｋを生成する。共通鍵ｋを生成するのに必須の情報は、鍵素材ｋ２である。一般に鍵素材とは鍵を生成するのに必要な情報を意味するが、ここでの鍵素材ｋ２は、「暗号化の対象となるデータごとに実質的に異なる値である」という特定の条件を満たす情報である。

【００４１】

例えば、ＭＡＣフレームを暗号化するための共通鍵を生成する実施形態においては、鍵素材ｋ２として、ＭＡＣフレームごとに異なる値をとるシーケンス番号を利用することができる。また、ＩＰパケットを暗号化するための共通鍵を生成する実施形態においては、鍵素材ｋ２として、ＩＰパケットごとに異なる値をとるシーケンス番号を利用することができる。これらのシーケンス番号の詳細は後述する。

【００４２】

このように、暗号化の対象となるデータごとに実質的に異なる値である鍵素材ｋ２に基づいて共通鍵ｋを生成することにより、共通鍵ｋは、暗号化の対象となるデータごとに実質的に異なる値となる。

【００４３】

なお、鍵素材ｋ２として具体的にどのような情報を用いる場合であっても、鍵素材ｋ２のビット長は有限である。よって、理論的には、異なるデータに対して同じ値の鍵素材ｋ２を利用することもありうる。しかし、適切なビット長の鍵素材ｋ２を用いることにより、異なるデータに対して同じ値の鍵素材ｋ２が利用される頻度を、実用上無視しても問題がない程度にまで低くすることができる。よって、以下では、「鍵素材ｋ２は、暗号化の対象となるデータごとに実質的に異なる値である」と見なして説明する。

【００４４】

上記のような鍵素材ｋ２を用いて共通鍵ｋを生成することにより、例えば一定期間ごとにＩＫＥによりリキーを行う従来の構成に比べて、共通鍵ｋが変化する頻度が非常に高まる。その結果、暗号化されたデータを第三者に傍受されても共通鍵ｋが推測されにくくなる。

【００４５】

さらに暗号の強度を高めるためには、共通鍵ｋの生成に、送信先・送信元情報ｋ１およびマスター鍵ｋ３をも用いることが望ましい。特に、送信先・送信元情報ｋ１を用いることが望ましい。

【００４６】

ここで、送信先・送信元情報ｋ１は、暗号化の対象となるデータ（ＭＡＣフレームやＩＰパケットなど）の送信先および／または送信元に関する情報であり、例えば、送信先および／または送信元のアドレスの一部または全部である。また、マスター鍵ｋ３は、共通鍵生成装置内に予め設定された情報であり、漏洩や改竄が行われないように、例えばセキュリティチップ内に記録されている。マスター鍵ｋ３は、共通鍵生成装置の利用者が設定する情報である事前共有鍵ｋ０に基づいて予め生成されてもよい。事前共有鍵ｋ０もマスター鍵ｋ３と同様にセキュリティチップ内に記録されている。

【００４７】

共通鍵ｋの生成に、鍵素材ｋ２だけでなく送信先・送信元情報ｋ１やマスター鍵ｋ３も用いることが好ましい理由は次のとおりである。

例えば鍵素材ｋ２としてシーケンス番号を利用する場合に、鍵素材ｋ２だけから共通鍵ｋを生成すると、その生成アルゴリズムによっては、連続して生成される複数の共通鍵ｋに規則性が生じる可能性がある。そこで、送信先・送信元情報ｋ１を利用して、共通鍵ｋのランダム性を高めることが望ましい。一般に通信は、いつ誰が誰に対して行うのかが不規則であり、予測困難である。したがって、共通鍵ｋを生成するのに、送信先・送信元情報ｋ１のこの不規則性を利用することが望ましい。また、第三者には秘密にされている情報であるマスター鍵ｋ３を利用することにより、さらに共通鍵ｋの推測のされにくさを高めることが可能となる。

【００４８】

図４は、本発明による共通鍵生成装置の基本的な機能ブロック構成図である。図４の共通鍵生成装置１は、受付部１１と鍵素材格納部１２と鍵素材読み取り部１３と共通鍵生成部１４とを備える。共通鍵生成装置１は、入力データが入力されると共通鍵ｋを生成する。

【００４９】

ところで、共通鍵ｋを生成するのは、平文のデータである入力データを暗号化するという局面（以下、「第一の局面」とよぶ）と、暗号文のデータである入力データを復号化するという局面（以下、「第二の局面」とよぶ）との、二つの局面においてである。いずれの局面であっても、入力データはヘッダ部とペイロード部を有する所定の形式のデータであるとする。

【００５０】

例えば、ＭＡＣフレームやＩＰパケットはヘッダ部とペイロード部を有し、ヘッダ部には送信先や送信元の情報が含まれ、ペイロード部には送信対象のデータが含まれる。なお、入力データはさらにトレイラ部を有していてもよい。例えば、ＭＡＣフレームは、トレイラ部としてＦＣＳ（Frame Check Sequence）を含む。また、第二の局面においても入力データのすべてが暗号化されているわけではなく、ヘッダ部は暗号化されていないクリアテキストの状態である。

【００５１】

受付部１１は入力データを受け付ける。

鍵素材格納部１２は鍵素材ｋ２を格納している。例えば、上記のように鍵素材ｋ２がシーケンス番号であるとき、鍵素材格納部１２を実現するハードウェアはカウンタでもよい。

【００５２】

鍵素材読み取り部１３は、第一の局面と第二の局面で異なる動作をするが、いずれの局面でも、鍵素材読み取り部１３が鍵素材ｋ２を読み取る点は同じである。

第一の局面において、鍵素材読み取り部１３は、鍵素材格納部１２から鍵素材ｋ２を読み取り、鍵素材格納部１２内の鍵素材ｋ２の値を更新する。例えば、鍵素材ｋ２がシーケ

ンス番号であり鍵素材格納部１２がカウンタであるとき、鍵素材読み取り部１３は鍵素材ｋ２の値を読み取ってからカウンタをインクリメントする。

【００５３】

第二の局面において、鍵素材読み取り部１３は、受付部１１で受け付けた入力データのヘッダ部の所定の部分から、鍵素材ｋ２を読み取る。

共通鍵生成部１４は、鍵素材読み取り部１３が読み取った鍵素材ｋ２に基づいて共通鍵ｋを生成する。実施形態により、図３に示した送信先・送信元情報ｋ１やマスター鍵ｋ３をさらに利用して共通鍵ｋを生成してもよい。

【００５４】

ところで、上記では、第二の局面において入力データが鍵素材ｋ２を含むことを前提条件としている。この前提条件について、図１、３、４をあわせて参照しながら説明する。

例えば、図４の共通鍵生成装置１は、図１の共通鍵生成装置１ａや１ｂのように、中継装置２ａや２ｂの一部として実装することも可能である。また、図１の共通鍵ｋａ～ｋｃはいずれも図３の共通鍵ｋに対応し、図１の鍵素材ｋ２ａ～ｋ２ｃはいずれも図３の鍵素材ｋ２に対応する。

【００５５】

図１において、共通鍵生成装置１ａに対する入力データは、例えばデータ５ａであり、暗号化すべき平文データである。よって、共通鍵生成装置１ａ内の不図示の鍵素材読み取り手段は第一の局面における動作を行う。そして、共通鍵生成装置１ａ内の不図示の共通鍵生成手段が共通鍵ｋａを生成する。また、前述のとおり、データ５ａは共通鍵ｋａにより暗号化されて暗号化データ６ａとなるが、暗号化データ６ａは鍵素材ｋ２ａを含む。

【００５６】

一方、図１の共通鍵生成装置１ｂに対する入力データは、例えば暗号化データ６ａであり、復号化すべき暗号文データである。よって、共通鍵生成装置１ｂ内の不図示の鍵素材読み取り手段は第二の局面における動作を行う。つまり、暗号化データ６ａから鍵素材ｋ２ａを読み取る。

【００５７】

以上から分かるように、第一の局面において生成された共通鍵ｋを使って暗号化を行う際に、所定の部分に鍵素材ｋ２を含む暗号化データ（図１の暗号化データ６ａ～６ｃに相当）を生成することによって、第二の局面では入力データが鍵素材ｋ２を含むことが保証される。本発明による共通鍵生成装置１は、鍵素材ｋ２と共通鍵ｋがそのように利用される環境で使用される。図１は、そのような環境の例の一つである。

【００５８】

図５は、鍵素材ｋ２以外のデータも用いる共通鍵生成装置を備えた中継装置を含むネットワーク上で行われる暗号化通信を示す模式図である。図５は図１とよく似ているので、相違点を中心に説明する。

【００５９】

図１は、図３に示したデータのうち鍵素材ｋ２のみを用いて共通鍵ｋを生成する場合に対応する図である。一方、図５は、図３に示したデータのうち送信先・送信元情報ｋ１、鍵素材ｋ２、マスター鍵ｋ３のすべてを用いて共通鍵ｋを生成する場合に対応する図である。よって、入力データ５ａ～５ｃごとに異なる共通鍵ｋａ～ｋｃが生成され、それら異なる共通鍵ｋａ～ｋｃによって各入力データ５ａ～５ｃが暗号化される点は、図１と図５で同様である。

【００６０】

図１と比較したときの図５の第一の特徴は、各入力データ５ａ～５ｃ、暗号化データ６ａ～６ｃ、復号化データ７ａ～７ｃが送信先・送信元情報ｋ１ａ～ｋ１ｃを含むことが明示されている点である。第二の特徴は、共通鍵生成装置１ａおよび１ｂが同じ値のマスター鍵ｋ３を格納している点である。第三の特徴は、共通鍵生成装置１ａおよび１ｂがそれぞれ、送信先・送信元情報ｋ１ａ～ｋ１ｃと、鍵素材ｋ２ａ～ｋ２ｃと、マスター鍵ｋ３とから共通鍵ｋａ～ｋｃを生成する点である。

【００６１】
例えば、データ５ａ、暗号化データ６ａ、復号化データ７ａはそれぞれ、送信先・送信元情報ｋ１ａを含む。そして、共通鍵生成装置１ａおよび１ｂはそれぞれ、送信先・送信元情報ｋ１ａと鍵素材ｋ２ａとマスター鍵ｋ３とから共通鍵ｋａを生成する。データ５ａは共通鍵ｋａにより暗号化されて暗号化データ６ａとなり、暗号化データ６ａは共通鍵ｋａにより復号化されて復号化データ７ａとなる。共通鍵生成装置１ａおよび１ｂは、ＩＫＥのような鍵交換を行わなくても、予め同じ値のマスター鍵ｋ３を格納さえしていれば、同じ共通鍵ｋａを生成することができる。

【００６２】
なお、図５では共通鍵生成装置１ａおよび１ｂの内部にマスター鍵ｋ３を図示したが、図３に示したとおりマスター鍵ｋ３は事前共有鍵ｋ０から生成される。したがって、共通鍵生成装置１ａおよび１ｂが予め格納しておくのは、同じ値のマスター鍵ｋ３でもよく、同じ値の事前共有鍵ｋ０でもよい。後者の場合、共通鍵生成装置１ａおよび１ｂは、共通鍵ｋａ～ｋｃを生成するたびにマスター鍵ｋ３を生成してもよい。あるいは、電源が投入されるたびにマスター鍵ｋ３を生成し、電源がオンの状態の間は生成したマスター鍵ｋ３を揮発性メモリ（不図示）またはＴＣＧ対応チップ１０５（後述）などに格納しておき、共通鍵ｋａ～ｋｃを生成するたびにそこに格納されたマスター鍵ｋ３を読み取るのでもよい。いずれの場合でも、共通鍵ｋａ～ｋｃを生成するときには、共通鍵生成装置１ａおよび１ｂがマスター鍵ｋ３を記憶している。よって、図５では、共通鍵生成装置１ａおよび１ｂの内部にマスター鍵ｋ３を図示した。

【００６３】
次に、より具体的な例として、レイヤ２の通信を暗号化するのに本発明を利用する場合を、図６～図１７を参照しながら説明する。
図６は、本発明を適用したレイヤ２の中継装置の構成図である。図６の説明をする前に、まずレイヤ２通信の典型例について簡単に説明する。

【００６４】
レイヤ２通信の代表的なものにイーサネット通信があり、イーサネットの仕様はＯＳＩ参照モデルにおける物理層（レイヤ１）およびレイヤ２の仕様を規定している。また、イーサネットを標準化したＩＥＥＥ（Institute of Electrical and Electronic Engineers）８０２．３規格では、レイヤ２がさらに二つの副層に分かれており、レイヤ１に近いほうがＭＡＣ（Media Access Control）副層、レイヤ３に近いほうがＬＬＣ（Logical Link Control）副層である。

【００６５】
レイヤ２通信において用いられるレイヤ２の中継装置（以後「Ｌ２中継装置」と略す。「Ｌ２」はレイヤ２を表す）は、Ｌ２スイッチとも呼ばれ、スイッチングハブはその代表例である。レイヤ２通信では、データは「フレーム」という単位で送受信される。フレームには、例えばＤＩＸイーサネットのＭＡＣフレームやＩＥＥＥ８０２．３のＭＡＣフレームなど、細かい点で異なる複数の形式があるが、本発明においてその違いは重要ではない。よって、以下では総称として「フレーム」という語を用いる。

【００６６】
ところで、従来のイーサネット通信では、フレームが暗号化されずに送受信されるだけなく、フレームの盗聴自体が容易だという問題がある。複数のプロトコルを組み合わせることによってフレームを暗号化して通信を行うことは可能だが、その場合、プロトコルスタックが複雑化するなど、いくつかの欠点がある。一方、従来のＬ２中継装置に本発明を適用した図６のＬ２中継装置１０１を使う場合は、簡素な構成でフレームを暗号化して通信を行うことができる。

【００６７】
図６において、Ｌ２中継装置１０１はフレームを中継するＬ２中継装置である。Ｌ２中継装置１０１が、外部とフレームを送受信するための複数の物理的なポートを備える点（図６の例では四つのポート１０３ａ～１０３ｄがある）、およびフレームを中継するフレ

ーム中継処理部１０２を備えるという点は、従来のＬ２中継装置と同様である。

【００６８】

Ｌ２中継装置１０１は、各ポート１０３ａ～１０３ｄに対応した暗号処理モジュール１０４ａ～１０４ｄをさらに備えている。暗号処理モジュール１０４ａ～１０４ｄはそれぞれが一つのチップとして製造されてもよい。暗号処理モジュール１０４ａ～１０４ｄはそれぞれ、対応するポート１０３ａ～１０３ｄおよびフレーム中継処理部１０２と、ＧＭＩＩ（Gigabit Medium Independent Interface）やＭＩＩ（Medium Independent Interface）などの汎用のインターフェイスを介して接続されている。つまり、暗号処理モジュール１０４ａ～１０４ｄの入力と出力はともにフレームである。ＧＭＩＩやＭＩＩはレイヤ１とＭＡＣ副層とのインターフェイスであり、イーサネットで一般的に使われている。

【００６９】

なお、詳しくは後述するが、暗号処理モジュール１０４ａ～１０４ｄが行う暗号処理は、共通鍵ｋの生成と、暗号化処理および復号化処理である。以下では、「暗号化処理および復号化処理」の意味で「暗号処理」という語を用いる。また、図６の実施形態において、共通鍵ｋは、送信先・送信元情報ｋ１と鍵素材ｋ２とマスター鍵ｋ３とを利用して生成される。具体的には、送信先・送信元情報ｋ１としてＭＡＣヘッダ情報ｋ１＿ｆを利用し、鍵素材ｋ２としてシーケンス番号ｋ２＿ｎを利用する。これらの情報の詳細および、暗号処理モジュール１０４ａ～１０４ｄと図４の共通鍵生成装置１の対応関係は後述する。

【００７０】

また、Ｌ２中継装置１０１は、ＴＣＧ（Trusted Computing Group）の仕様に準拠したセキュリティチップであるＴＣＧ対応チップ１０５を搭載している。ＴＣＧ対応チップ１０５には、図３の事前共有鍵ｋ０などが格納され、暗号処理モジュール１０４ａ～１０４ｄにより利用される。ＴＣＧ対応チップ１０５に格納されたデータは外部から不正に取り出すことができないため、ＴＣＧ対応チップ１０５を使うと安全にデータを格納することができる。

【００７１】

また、Ｌ２中継装置１０１はＣＰＵ（Central Processing Unit）６を備える。ＣＰＵ１０６は、例えば不図示のＲＯＭ（Read Only Memory）に格納されたプログラムにしたがって動作し、不図示のＲＡＭ（Random Access Memory）をワーク用に用いる。後述するように、ＣＰＵ１０６は、暗号処理モジュール１０４ａ～１０４ｄに命令して暗号処理に必要なデータの生成を行わせたりする。

【００７２】

フレーム中継処理部１０２、暗号処理モジュール１０４ａ～１０４ｄ、ＴＣＧ対応チップ１０５、ＣＰＵ１０６、ＲＯＭ、ＲＡＭは、内部バス１０７に接続されている。

Ｌ２中継装置１０１では、物理的なポート１０３ａ～１０３ｄそれぞれに対応して暗号処理モジュール１０４ａ～１０４ｄが配備され、フレーム中継処理部１０２によるフレーム中継処理とは切り離されて暗号処理が行われる。つまり、フレーム中継処理部１０２は暗号に関して何も考慮する必要がなく、まったく暗号処理を行わない従来の中継装置のフレーム中継処理部をそのままフレーム中継処理部１０２として利用することが可能である。

【００７３】

なお、このように中継処理と暗号処理を切り離すために、フレーム中継処理部１０２と暗号処理モジュール１０４ａ～４ｄのインターフェイスはＧＭＩＩやＭＩＩ等のインターフェイスとなっている。まったく暗号処理を行わない従来の中継装置の場合、フレーム中継処理部はポートとＧＭＩＩやＭＩＩ等のインターフェイスで接続され、そのインターフェイスを介してフレームの中継処理を行う。図６のフレーム中継処理部１０２も同様に、ＧＭＩＩやＭＩＩ等のインターフェイスを介してフレームの中継処理だけを行う。

【００７４】

また、Ｌ２中継装置１０１では、各ポート１０３ａ～１０３ｄに対応して暗号処理モジュール１０４ａ～１０４ｄを備えているため、一般的なオフィス環境でよく使われるＮ対

Ｎのトポロジにおいてもイーサネット通信を暗号化することができる。なお、ここで「Ｎ対Ｎのトポロジ」とは、物理的なケーブル配線の意味ではなく、複数の中継装置が、それぞれ複数の中継装置との間で暗号化通信を行うことを意味している。この点については図９Ａ、図９Ｂ、図１２～図１４を参照して後述する。

【００７５】

図７は、図６と図４の関係を説明する機能ブロック構成図である。なお、ｆ、ｋ０、ｋ１、ｋ２、ｋ３、ｋなる符号がついた矢印は、それぞれ、フレーム、事前共有鍵ｋ０、送信先・送信元情報ｋ１としてのＭＡＣヘッダ情報ｋ１＿ｆ、鍵素材ｋ２としてのシーケンス番号ｋ２＿ｎ、マスター鍵ｋ３、共通鍵ｋがその矢印の方向に送られることを表す。符号のない矢印は制御の流れを表す。符号「ｋ１＿ｆ」や「ｋ２＿ｎ」の指す具体的内容は後述する。

【００７６】

図６における暗号処理モジュール１０４ａ～１０４ｄのそれぞれが、概ね図４の共通鍵生成装置１に対応する。すなわち、Ｌ２中継装置１０１は四つの共通鍵生成装置を含む。ただし、正確には、これら四つの共通鍵生成装置が一つのＴＣＧ対応チップ１０５を共用し、それぞれの共通鍵生成装置の一部として利用している。図７はその対応関係を説明する図である。なお、図６の例では、暗号処理モジュール１０４ａ～１０４ｄが同じ構成であるため、図７では単に「１０４」という符号を用いている。また、その暗号処理モジュール１０４に対応するポートを単に「１０３」という符号で表す。

【００７７】

図７の共通鍵生成装置１ｃは、図４の共通鍵生成装置１と同様に、受付部１１、鍵素材格納部１２、鍵素材読み取り部１３、共通鍵生成部１４を含む。これら四つの構成要素は、具体的には暗号処理モジュール１０４内に実装されている。

【００７８】

上記のとおり、暗号処理モジュール１０４は、ＧＭＩＩやＭＩＩなどのインターフェイスにより、対応するポート１０３およびフレーム中継処理部１０２と接続されている。受付部１１は、そのインターフェイス処理を行い、フレームのバッファリングを行う。つまり、受付部１１はバッファメモリを備えている。なお、図７では、物理的には複数のインターフェイス（つまり、ポート１０３とのインターフェイスと、フレーム中継処理部１０２とのインターフェイス）を受付部１１が備えている。

【００７９】

上述のとおり、暗号処理モジュール１０４は、共通鍵ｋの生成以外に、生成した共通鍵ｋを使った暗号処理も行うため、さらに、判定部１５、暗号化部１６、復号化部１７、出力部１９を有している。図７では、これら四つの構成要素も、共通鍵生成装置１ｃに含まれる。

【００８０】

判定部１５は、第一の局面（暗号化のために共通鍵ｋを生成するべき局面）か、第二の局面（復号化のために共通鍵ｋを生成するべき局面）かを判定する。実施形態によっては、判定部１５が、第三の局面（暗号化も復号化も行う必要がないため、共通鍵ｋを生成する必要がない局面）と判定することがあってもよい。そして、判定部１５は、判定結果を鍵素材読み取り部１３、共通鍵生成部１４、暗号化部１６、復号化部１７、出力部１９に適宜通知する。

【００８１】

暗号化部１６は、判定部１５が第一の局面と判定したとき、共通鍵生成部１４が生成した共通鍵ｋを用いて、受付部１１が受け付けたフレームの暗号化処理を行い、出力部１９に出力する。復号化部１７は、判定部１５が第二の局面と判定したとき、共通鍵生成部１４が生成した共通鍵ｋを用いて、受付部１１が受け付けたフレームの復号化処理を行い、出力部１９に出力する。

【００８２】

出力部１９は、第一の局面において暗号化部１６で暗号化されたフレーム、第二の局面

において復号化部１７で復号化されたフレーム、第三の局面において受付部１１で受け付けたままの何も処理されていないフレーム、のいずれかが入力されると、それを共通鍵生成装置１ｃの外部（暗号処理モジュール１０４の外部）に出力する機能を有する。具体的には、出力部１９は、ＧＭＩＩやＭＩＩなどのインターフェイスを介して、ポート１０３またはフレーム中継処理部１０２に、前述のいずれかのフレームを出力する。図７は機能ブロック構成図なので受付部１１と出力部１９を別のブロックにより示してあるが、例えばポート１０３との間の配線などのハードウェアは、受付部１１と出力部１９が共用してもよい。

【００８３】

図７の共通鍵生成装置１ｃは、図３の送信先・送信元情報ｋ１およびマスター鍵ｋ３をも利用して共通鍵ｋを生成する。つまり、共通鍵生成部１４は、受付部１１が受け付けたフレームから送信先・送信元情報ｋ１を抽出し、マスター鍵格納部２１からマスター鍵ｋ３を読み出して利用する。また、本実施形態では、Ｌ２中継装置１０１の電源が入れられるたびに、四つの共通鍵生成装置１ｃそれぞれにおいてマスター鍵生成部２０が、事前共有鍵格納部１８に格納された事前共有鍵ｋ０からマスター鍵ｋ３を生成し、マスター鍵格納部２１に格納する。事前共有鍵ｋ０は、予め安全に（つまり不正に読み取られることがないように）共通鍵生成装置１ｃ内に格納されていなくてはならない。図７では、ＴＣＧ対応チップ１０５の一部を事前共有鍵格納部１８として利用している。

【００８４】

つまり、図７において共通鍵生成装置１ｃは、一つの暗号処理モジュール１０４と、ＴＣＧ対応チップ１０５の一部である事前共有鍵格納部１８とからなる。なお、図６のように四つの暗号処理モジュール１０４ａ～１０４ｄがある場合、ＴＣＧ対応チップ１０５は四つの共通鍵生成装置１ｃにより共用されるが、ＴＣＧ対応チップ１０５の異なる四つの領域がそれぞれ四つの共通鍵生成装置１ｃの構成要素として使われるのでもよく、ＴＣＧ対応チップ１０５のある一つの領域が四つの共通鍵生成装置１ｃの構成要素として共用されるのでもよい。

【００８５】

図８は、図６のＬ２中継装置１０１の変形例を示す図である。図８と図６の違いは、図８では一部のポート（１０３ａ、１０３ｂ）にのみ暗号処理モジュール１０４ａ、１０４ｂが備えられている点である。他のポート（１０３ｃ～１０３ｊ）は、直接フレーム中継処理部１０２とＧＭＩＩやＭＩＩ等のインターフェイスで接続されており、暗号処理モジュールを備えていない。つまり、Ｌ２中継装置１０１は、暗号化通信の必要性などに応じて、一部のポートのみに暗号処理モジュールを備えてもよく、全部のポートに暗号処理モジュールを備えてもよい。

【００８６】

なお、フレーム中継処理部１０２は、暗号処理モジュール１０４ａ、１０４ｂとの間のインターフェイスも、暗号処理モジュールを備えていないポート１０３ｃ～１０３ｊとの間のインターフェイスも同じインターフェイス（例えばＧＭＩＩやＭＩＩ）である。よって、フレーム中継処理部１０２は、暗号処理モジュールを備えたポートとそうでないポートを区別することなく、フレームの中継に専念することができる。

【００８７】

なお、図８における暗号処理モジュール１０４ａ、１０４ｂも、図７に示した構成を有している。

図９Ａは、共通鍵生成装置を含むレイヤ２の中継装置の利用例を示す図であり、ＶＬＡＮ１１０、１２０、１３０という三つのＶＬＡＮを含むネットワーク構成を示している。

【００８８】

図９Ａにおいて、Ｌ２中継装置１０１ａ、１０１ｂは、図６または図８のＬ２中継装置１０１と同様の装置である。なお、本発明のＬ２中継装置１０１はレイヤ２のフレームを中継する機能を有するスイッチ装置なので、図９Ａ以降では「Ｌ２ＳＷ」と表記することがある。Ｌ２中継装置１０１ａ、１０１ｂにはそれぞれ、ＶＬＡＮ１１０、１２０、１３

０に属する端末（コンピュータ）が接続されている。つまり、Ｌ２中継装置１０１ａ、１０１ｂは端末と接続されているエッジスイッチである。

【００８９】

また、従来の中継装置であるコアＬ２／Ｌ３スイッチ１４１（レイヤ２またはレイヤ３の中継機能を有するが暗号処理に関する機能をもたない従来のスイッチ装置）には、Ｌ２中継装置１０１ａ、１０１ｂ、およびファイヤウォール１４３が接続されている。つまり、コアＬ２／Ｌ３スイッチ１４１はスイッチ間で中継を行うコアスイッチである。ファイヤウォール１４３はルータ１４４に接続され、ルータ１４４はインターネット１４５に接続されている。

【００９０】

ところで、ＶＬＡＮの一つの使い方は、同一の物理的なネットワーク上に複数のシステムを重畳させることである。例えば、図９Ａの例においては、Ｌ２中継装置１０１ａ、コアＬ２／Ｌ３スイッチ１４１、Ｌ２中継装置１０１ｂという装置およびこれらを接続するケーブルは物理的な存在である。そして、これらの物理的な存在が接続された物理的なネットワークを、ＶＬＡＮ１１０、１２０、１３０という三つの異なるＶＬＡＮが共有している。つまり、同一の物理的なネットワーク上に複数のシステムが重畳している。

【００９１】

それら複数のシステムには、機密情報を主に扱うシステムと、秘匿する必要のないウェブ閲覧が中心のシステムとが含まれることがある。前者と後者では、通信の機密性に対する要件が異なって当然である。したがって、ＶＬＡＮを利用している場合には、物理ポートを単位として暗号処理を行うこと（例えば、Ｌ２中継装置１０１ａからコアＬ２／Ｌ３スイッチ１４１へ送られるすべてのフレームを暗号処理モジュール１０４ａで暗号化すること）は好ましくない。なぜなら、機密データを含まない通信まで暗号化するという無駄な処理が行われるからである。

【００９２】

例えば、ある企業には部署Ａ、Ｂ、Ｃがあるとする。部署Ａ、Ｂでは機密データを扱うために通信を暗号化する必要があり、かつ機密を守るためにインターネット１４５との通信を禁じているとする。また、部署Ｃでは機密データを扱っておらず、主に電子メールの送受信やウェブの閲覧（これらはインターネット１４５との通信をともなう）を行っているとする。この場合、各部署を別のＶＬＡＮに分けて図９Ａのような構成とすることがある。つまり、部署ＡがＶＬＡＮ１１０に、部署ＢがＶＬＡＮ１２０に、部署ＣがＶＬＡＮ１３０に対応する。

【００９３】

本発明によれば、ＶＬＡＮごとに暗号化するか否かを選択し、不要な暗号処理を避けることができる。つまり、ＶＬＡＮ１１０、１２０を暗号化の対象とし、ＶＬＡＮ１３０は暗号化の対象外とすることができる。また、図９Ａに示すように、本発明によるＬ２中継装置１０１ａ、１０１ｂと従来の中継装置であるコアＬ２／Ｌ３スイッチ１４１とを混在させてネットワークを構成することができる。このことを以下で説明する。

【００９４】

図９Ｂに抜粋して示したように、Ｌ２中継装置１０１ａにはポート１０３ａ～１０３ｄがあり、ポート１０３ａはＶＬＡＮ１１０に、ポート１０３ｂはＶＬＡＮ１２０に、ポート１０３ｃはＶＬＡＮ１３０に、それぞれ割り当てられている。この割り当ては、管理者により予め設定される。ポート１０３ｄはコアＬ２／Ｌ３スイッチ１４１と接続されたポートである。Ｌ２中継装置１０１ａの内側では、ポート１０３ｄが暗号処理モジュール１０４ａとＧＭＩＩやＭＩＩ等のインターフェイスで接続されている。ポート１０３ａ～１０３ｃおよび暗号処理モジュール１０４ａは、それぞれフレーム中継処理部１０２ａとＧＭＩＩやＭＩＩ等のインターフェイスで接続されている。

【００９５】

同様に、Ｌ２中継装置１０１ｂはポート１０３ｅ～１０３ｈを備えており、ポート１０３ｅはＶＬＡＮ１１０に、ポート１０３ｆはＶＬＡＮ１２０に、ポート１０３ｇはＶＬＡ

Ｎ１３０に、それぞれ割り当てられている。また、ポート１０３ｈはコアＬ２／Ｌ３スイッチ１４１と接続されたポートである。

【００９６】

なお、表示の便宜上、図９ＡではＬ２中継装置１０１ａ、１０１ｂを示す矩形の外側に暗号処理モジュール１０４ａ、１０４ｂを表示しているが、実際の構成は図６、図８、図９Ｂに示したようになっており、暗号処理モジュールは中継装置の内部にある。以降の図でも図９Ａと同様の表現をすることがある。また、図９Ｂでは、Ｌ２中継装置１０１ａ、１ｂの構成要素のうち、ＴＣＧ対応チップなどは省略している。

【００９７】

同一のＶＬＡＮ内で図９Ａの左から右へフレームを送信する場合、どのＶＬＡＮの場合でも、フレームはＬ２中継装置１０１ａ、コアＬ２／Ｌ３スイッチ１４１、Ｌ２中継装置１０１ｂを経由する。図９Ｂを参照してより詳細に述べれば、いずれの場合も、フレーム中継処理部１０２ａ、暗号処理モジュール１０４ａ、ポート１０３ｄ、コアＬ２／Ｌ３スイッチ１４１、ポート１０３ｈ、暗号処理モジュール１０４ｂ、フレーム中継処理部１０２ｂを経由する。フレームが経由する経路のうちＶＬＡＮごとに異なるのは、図９Ｂにおいてフレーム中継処理部１０２ａより左側の部分とフレーム中継処理部１０２ｂより右側の部分のみである。

【００９８】

また、図９Ａおよび図９Ｂでは、上記のごとく、ＶＬＡＮ１３０に所属する端末はインターネット１４５との通信を行うと仮定している。このインターネット１４５との通信は、図９Ａにおいて、二つの黒い矢印（Ｌ２中継装置１０１ａから出発して、コアＬ２／Ｌ３スイッチ１４１、ファイヤウォール１４３、ルータ１４４を経由し、インターネット１４５へ向かう矢印、およびＬ２中継装置１０１ｂから出発して、コアＬ２／Ｌ３スイッチ１４１、ファイヤウォール１４３、ルータ１４４を経由してインターネット１４５へ向かう矢印）により示される。

【００９９】

このように、いずれのＶＬＡＮ内で通信する場合でも、あるいはインターネット１４５等の外部のネットワークと通信する場合でも、フレームはポート１０３ｄとコアＬ２／Ｌ３スイッチ１４１の間、および／またはポート１０３ｈとコアＬ２／Ｌ３スイッチ１４１の間を経由する。つまり、ポート１０３ｄとコアＬ２／Ｌ３スイッチ１４１の間、およびポート１０３ｈとコアＬ２／Ｌ３スイッチ１４１の間の物理的な通信路（ケーブル）は、複数のＶＬＡＮで共有される。このような通信路（１４２ａおよび１４２ｂ）は、ＶＬＡＮの規格であるＩＥＥＥ８０２．１Ｑの名にちなんで「．１Ｑトランク」とよばれる。

【０１００】

また、ポート１０３ａなどは一つのＶＬＡＮに固定的に割り当てられているが、ポート１０３ｄやポート１０３ｈは複数のＶＬＡＮで共有されている。ポート１０３ｄやポート１０３ｈは、「タグＶＬＡＮポート（tagged VLAN port）」とよばれる。管理者はポート１０３ｄとポート１０３ｈをタグＶＬＡＮポートとして予め設定する。タグＶＬＡＮポートに対しては、対応するＶＬＡＮを一意に決定することができないため、ポート１０３ｄとポート１０３ｈの間（より正確には、フレーム中継処理部１０２ａとフレーム中継処理部１０２ｂの間）で送受信されるフレームには、ＶＬＡＮを識別する情報であるＶＬＡＮ‐ＩＤが付加されている（詳細は図１０とあわせて後述する）。

【０１０１】

上記のごとく、図９Ａの例では、ＶＬＡＮ１１０とＶＬＡＮ１２０が暗号化の対象であり、ＶＬＡＮ１３０は暗号化の対象外である。管理者は、どのＶＬＡＮを暗号化の対象とするのかという設定を、Ｌ２中継装置１０１ａに入力する。すると、図９Ｂには示されていないＣＰＵ（図６のＣＰＵ１０６に相当する）が、暗号処理モジュール１０４ａに対して、入力された内容を設定するよう命令する。Ｌ２中継装置１０１ｂに関しても同様である。その結果、暗号処理モジュール１０４ａ、１０４ｂは、管理者が入力した設定にしたがって、暗号処理が必要なフレームに対してだけ暗号処理を行う。

【０１０２】
例えば、図９Ｂの左から右へＶＬＡＮ１１０内でフレームを送信する場合、ポート１０３ａで受信されたフレーム（ポート１０３ａに接続された端末から送信されたフレーム）は、フレーム中継処理部１０２ａを経由して暗号処理モジュール１０４ａに送信される。すると、図７に示した暗号処理モジュール１０４ａの各構成要素は次のように動作する。
【０１０３】
まず、受付部１１がこのフレームを受信する。
判定部１５は、このフレームをポート１０３ｄではなくフレーム中継処理部１０２ａから受信したことと、フレームに含まれるＶＬＡＮ‐ＩＤと、上記の設定内容とに基づき、第一の局面（このフレームを暗号化するために共通鍵ｋを生成すべき局面）であると判定する。
【０１０４】
そして、判定部１５の判定にしたがって、鍵素材読み取り部１３が鍵素材格納部１２から鍵素材ｋ２としてのシーケンス番号ｋ２＿ｓを読み取り、鍵素材格納部１２に格納されている値を更新する。
【０１０５】
共通鍵生成部１４は、判定部１５の判定にしたがって共通鍵ｋを生成するために、ＭＡＣヘッダ情報ｋ１＿ｆとシーケンス番号ｋ２＿ｓとマスター鍵ｋ３を取得する。ＭＡＣヘッダ情報ｋ１＿ｆは、受付部１１が受信したフレームから抽出される。シーケンス番号ｋ２＿ｓは鍵素材読み取り部１３が読み取った値である。マスター鍵ｋ３は、マスター鍵格納部２１に格納されている。取得した三つのデータに基づき、共通鍵生成部１４は共通鍵ｋを生成する。
【０１０６】
暗号化部１６は、判定部１５の判定にしたがって、共通鍵生成部１４から共通鍵ｋを受け取り、受付部１１でバッファリングされているフレームを読み出して、共通鍵ｋにより暗号化する。
【０１０７】
暗号化されたフレームは、出力部１９を介して図９Ｂのポート１０３ｄに出力される。ここで図９Ｂに戻ると、暗号化されたフレームは、ポート１０３ｄ、コアＬ２／Ｌ３スイッチ１４１、ポート１０３ｈを経由して、暗号処理モジュール１０４ｂに送信される。すると、図７に示した暗号処理モジュール１０４ｂの各構成要素は次のように動作する。
【０１０８】
まず、受付部１１がこのフレームを受信する。
判定部１５は、このフレームをフレーム中継処理部１０２ｂではなくポート１０３ｈから受信したことと、フレームに含まれるＶＬＡＮ‐ＩＤと、上記の設定内容とに基づき、第二の局面（このフレームを復号化するために共通鍵ｋを生成すべき局面）であると判定する。あるいは、後述する暗号ヘッダ１７１をこのフレームが含むことから、このフレームが復号化の対象であると判定する。
【０１０９】
そして、判定部１５の判定にしたがって、鍵素材読み取り部１３が、受信したフレームから鍵素材ｋ２としてのシーケンス番号ｋ２＿ｒを読み取る。共通鍵生成部１４の動作は、暗号処理モジュール１０４ａの共通鍵生成部１４の動作と同様である。
【０１１０】
復号化部１７は、判定部１５の判定にしたがって、共通鍵生成部１４から共通鍵ｋを受け取り、受付部１１でバッファリングされているフレームを読み出して、共通鍵ｋにより復号化する。
【０１１１】
復号化されたフレームは、出力部１９を介して図９Ｂのフレーム中継処理部１０２ｂに出力され、ポート１０３ｅへ中継される。そしてポート１０３ｅから、ポート１０３ｅに接続された端末に送信される。

【０１１２】
つまり、端末からポート１０３ａを経由して暗号処理モジュール１０４ａまでの経路、および暗号処理モジュール１０４ｂからポート１０３ｅを経由して端末までの経路では、フレームは平文の状態（暗号化されていない状態）で送信される。一方、暗号処理モジュール１０４ａと暗号処理モジュール１０４ｂの間では、フレームは暗号化された状態で送信される。ＶＬＡＮ１２０内でフレームを送信する場合も同様である。
【０１１３】
以後、平文の状態のフレームを「平文フレーム」、暗号化された状態のフレームを「暗号化フレーム」とよぶ。図９Ｂでは、平文フレームの送信を実線の矢印で示し、暗号化フレームの送信を破線の矢印で示している。
【０１１４】
図９Ｂの左から右へＶＬＡＮ１３０内でフレームを送信する場合、暗号処理モジュール１０４ａは、フレームに含まれるＶＬＡＮ‐ＩＤと上記の設定内容とに基づき、このフレームが暗号化の対象外であるため暗号化処理が不要だと判断する。そして、平文フレームのままポート１０３ｄに送信する。つまり、暗号処理モジュール１０４ａ内において、図７の判定部１５が第三の局面（暗号化処理が不要であり、共通鍵ｋを生成する必要がない局面）であると判定し、その判定にしたがって、受付部１１にバッファリングされているフレームをそのまま、出力部１９を介してポート１０３ｄに出力する。
【０１１５】
また、暗号処理モジュール１０４ｂでは、フレームに含まれるＶＬＡＮ‐ＩＤと上記の設定内容とに基づき、このフレームが暗号化の対象外であるため復号化処理が不要だと判断する（あるいは、受信したフレームに暗号ヘッダ１７１が含まれないことから、復号化処理が不要だと判断する）。そして、受信した平文フレームをそのままフレーム中継処理部１０２ｂに送信する。つまり、暗号処理モジュール１０４ｂ内において、図７の判定部１５が第三の局面であると判定し、その判定にしたがって、受付部１１にバッファリングされているフレームをそのまま、出力部１９を介してフレーム中継処理部１０２ｂに出力する。
【０１１６】
ＶＬＡＮ１３０に属するコンピュータがインターネット１４５にＩＰパケットを送信する場合、そのＩＰパケットに対応するフレームは、ポート１０３ｄまたはポート１０３ｈを経由する。例えばＬ２中継装置１０１ａ内では、ＶＬＡＮ１３０に対応するポート１０３ｃがフレーム中継処理部１０２ａに接続され、フレーム中継処理部１０２ａが暗号処理モジュール１０４ａに接続され、暗号処理モジュール１０４ａがポート１０３ｄに接続されているので、暗号処理が不要なフレームも必ず暗号処理モジュール１０４ａを経由する。
【０１１７】
しかし、ＶＬＡＮ１３０に対応するポート１０３ｃで受信したフレームをポート１０３ｄに中継する場合、暗号処理モジュール１０４ａは、ＶＬＡＮ１３０内でフレームを送信する場合と同様に、暗号処理が不要だと判断し、平文フレームをそのままポート１０３ｄに送信する。このことは、図９Ｂにおいて、実線の矢印（平文フレームの送信を示す）が、Ｌ２中継装置１０１ａからコアＬ２／Ｌ３スイッチ１４１を経由してファイヤウォール１４３に向かっていることに対応する。
【０１１８】
上記のように図９Ａでは、ＶＬＡＮごとに暗号化の対象とするか否かを設定している。つまり、例えばポート１０３ｄとコアＬ２／Ｌ３スイッチ１４１の間の．１Ｑトランク１４２ａを経由するすべてのフレームを暗号化する場合と比べて、図９Ａは暗号化の粒度がより細かい。粒度が細かいことは、機密データを含まない通信を無駄に暗号化するのを避けることができるため利点である。
【０１１９】
このようにＶＬＡＮごとに選択的に、暗号化対象とするか否かを暗号処理モジュール１

０４ａ、１０４ｂに対して設定することができるため、Ｌ２中継装置１０１ａと１０１ｂの間に従来の中継装置であるコアＬ２／Ｌ３スイッチ１４１を介在させ、コアＬ２／Ｌ３スイッチ１４１を直接ファイヤウォール１４３に接続することが可能である。

【０１２０】

仮にＶＬＡＮごとの設定ができないとすると、図９Ａにおいて、ＶＬＡＮ１３０に属する端末がインターネット１４５と通信を行う際にも、フレームが暗号処理モジュール１０４ａで暗号化されてしまう。よって、暗号化フレームを復号化してからファイヤウォール１４３の外に送信するためには、暗号処理モジュールを備えたＬ２中継装置１０１をコアＬ２／Ｌ３スイッチ１４１とファイヤウォール１４３との間に介在させる必要がある。

【０１２１】

つまり、ＶＬＡＮごとの設定を可能とすることによって、必要な装置の数を減らすことができる。換言すれば、ネットワークを構成する際の制約を減らすことができる。つまり、様々な構成に対して本発明を適用することができる。

【０１２２】

図１０は、本発明で利用するフレームの形式を説明する図である。本発明ではフレームのうちデータ部のみを暗号化する。

図１０の上段に示したフレーム１５０は、レイヤ２で送受信される通常のフレームである。フレーム１５０は、６バイトの送信先ＭＡＣアドレス１５１、６バイトの送信元ＭＡＣアドレス１５２、データ部１５３、４バイトのエラー検出用のＦＣＳ１５４からなる。

【０１２３】

ＤＩＸイーサネットのＭＡＣフレームの場合、データ部１５３の先頭は２バイトで表されるタイプであり、その後に４６～１５００バイトのデータが続く。したがって、フレームは最大で１５１８バイトである（６＋６＋２＋１５００＋４＝１５１８）。ＩＥＥＥ８０２．３規格によるＭＡＣフレームの場合、データ部１５３の先頭は２バイトで表される長さ／タイプである。その後には、具体的なフレーム形式によって異なるが、３バイトのＬＬＣヘッダや５バイトのＳＮＡＰ（Sub Network Access Protocol）ヘッダが続き、その後にデータが続く。ＬＬＣヘッダやＳＮＡＰヘッダを含めて、データ部の長さは４６～１５００バイトである。したがって、フレームの最大長は１５１８バイトである。

【０１２４】

前述のとおり、共通鍵生成装置１への入力データはヘッダ部とペイロード部からなるという前提だが、入力データがフレーム１５０の場合、ヘッダ部は送信先ＭＡＣアドレス１５１と送信元ＭＡＣアドレス１５２からなり、ペイロード部はデータ部１５３である。

【０１２５】

図１０の中段に示したタグつきフレーム１６０は、フレーム１５０にＶＬＡＮタグが挿入されたものである。タグつきフレーム１６０は、送信元ＭＡＣアドレス１５２とデータ部１５３の間に、２バイトのＴＰＩＤ（Tag Protocol Identifier）１６１と２バイトのＴＣＩ（Tag Control Information）１６２が挿入されている他は、フレーム１５０と同様である。イーサネットの場合、ＶＬＡＮを示すＴＰＩＤ１６１の値は０ｘ８１００（１６進数で８１００の意）である。ＴＣＩ１６２は、ＶＬＡＮを識別するための１２ビットのＶＬＡＮ‐ＩＤを含む。ＴＰＩＤ１６１やＴＣＩ１６２は、フレームの送信元の端末で付加される場合もあるが、一般的には中継装置で付加されることが多い。後者の場合、ＦＣＳ１５４の再計算も中継装置で行われる。

【０１２６】

図９ＡのようにＶＬＡＮごとに暗号処理を行うか否かを設定する場合、ＴＣＩ１６２に含まれるＶＬＡＮ‐ＩＤの値に基づいて、暗号処理モジュール１０４が暗号処理の要否を判定する。

【０１２７】

共通鍵生成装置１への入力データがタグつきフレーム１６０の場合、ヘッダ部は送信先ＭＡＣアドレス１５１からＴＣＩ１６２までの部分で、ペイロード部はデータ部１５３で、トレイラ部はＦＣＳ１５４である。

【０１２８】
図１０の下段に示した暗号化フレーム１７０は、タグつきフレーム１６０を暗号化して得られるフレームであり、本発明に独自のフィールドを含む。暗号化フレーム１７０をタグつきフレーム１６０と比較すると、ＴＣＩ１６２の直後に暗号ヘッダ１７１が挿入される点、データ部１５３が暗号化されて暗号化データ部１７２となる点、暗号化データ部１７２の直後にＩＣＶ（Integrity Check Value）１７３が挿入されている点で異なっている。暗号ヘッダ１７１は、復号化に必要な鍵素材ｋ２を含む。ＩＣＶ１７３は、送信先ＭＡＣアドレス１５１から暗号化データ部１７２までの範囲に基づいて算出される一種のチェックサムである。なお、フレームを暗号化する際、暗号処理モジュール１０４は、ＦＣＳ１５４の再計算も行う。
【０１２９】
共通鍵生成装置１への入力データが暗号化フレーム１７０の場合、ヘッダ部は送信先ＭＡＣアドレス１５１から暗号ヘッダ１７１までの部分で、ペイロード部は暗号化データ部１７２で、トレイラ部はＩＣＶ１７３およびＦＣＳ１５４である。
【０１３０】
暗号化フレーム１７０の第一の特徴は、データ部１５３のみが暗号化され、ＭＡＣヘッダ（送信先ＭＡＣアドレス１５１と送信元ＭＡＣアドレス１５２からなる部分）は暗号化されない点である。第二の特徴は、暗号ヘッダ１７１がＴＣＩ１６２よりも後にある点である。
【０１３１】
第一の特徴は、フレームが大きくなることや処理が複雑化することを避けられるという利点につながる。このことを以下で説明する。
ＭＡＣヘッダを含めてフレームを暗号化する方式は、どの端末とどの端末が通信しているかという情報も隠すことができるため、機密度がより高い。例えば、中継装置であるスイッチＸｓに接続された端末Ｘｔから、スイッチＹｓに接続された端末Ｙｔにフレームを送信する場合、そのフレームの送信先ＭＡＣアドレス１５１には端末ＹｔのＭＡＣアドレスが書かれ、送信元ＭＡＣアドレス１５２には端末ＸｔのＭＡＣアドレスが書かれている。ＭＡＣヘッダを含めてこのフレームを暗号化する場合、暗号化後のフレームは、先頭に別のＭＡＣヘッダが付加されてカプセル化されたフレームである。つまり、外側のフレームにおける送信先ＭＡＣアドレス１５１としてスイッチＹｓのＭＡＣアドレスが書かれ、送信元ＭＡＣアドレス１５２としてスイッチＸｓのＭＡＣアドレスが書かれる。
【０１３２】
このカプセル化されたフレームでは、端末Ｘｔと端末Ｙｔが通信しているという情報が暗号化されており、機密性が高い。しかし、付加したＭＡＣヘッダの分だけフレームが大きくなり、オーバーヘッドが生じる。また、このようにカプセル化するには、スイッチのフレーム中継処理部において、フレームごとに中継先のスイッチを判定し、それに応じたＭＡＣヘッダを付加しなくてはならない（この例では、スイッチＸｓが送信先の端末ＹｔのＭＡＣアドレスからスイッチＹｓのＭＡＣアドレスを特定する必要がある）。よって、中継処理が複雑である。
【０１３３】
一方、暗号化フレーム１７０では、送信先ＭＡＣアドレス１５１と送信元ＭＡＣアドレス１５２は暗号化されない。そのため、機密度という点では上記の方法に比べてやや劣る。しかしながら、フレームに別のＭＡＣヘッダを追加する必要がないのでフレームの大きさを抑えることができる。
【０１３４】
また、フレーム中継処理部１０２は通常の中継処理を行うだけでよい（例えば、送信先の端末ＹｔのＭＡＣアドレスからスイッチＹｓのＭＡＣアドレスを特定する必要がない）。よって、本発明では、図６や図８に示したごとく、暗号処理を行わない従来のスイッチ装置と同様のフレーム中継処理部１０２を利用することができる。そして、暗号化・復号化に関する機能は、ポートごとに必要に応じて設けられた暗号処理モジュール（１０４ａ

等）にオフロードすることができる。

【０１３５】

次に、暗号ヘッダ１７１がＴＣＩ１６２よりも後にあるという第二の特徴について説明する。第二の特徴は、本発明によるＬ２中継装置１０１と、暗号処理機能をもたない通常のレイヤ２中継装置を混在させてネットワークを構成することができるという利点につながる。

【０１３６】

仮に、ＴＰＩＤ１６１とＴＣＩ１６２をも含めて暗号化する方法を採用すると、ＭＡＣヘッダの直後（つまり送信元ＭＡＣアドレス１５２の直後）に暗号ヘッダ１７１を挿入し、その後に暗号化されたＴＰＩＤ１６１とＴＣＩ１６２を続けるのが自然である。しかしこの方法では暗号化されたフレームを復号化しないかぎり、暗号化前のオリジナルのタグつきフレーム１６０が所属するＶＬＡＮを判別することができない。そのため、ネットワークの通信経路の途中に暗号処理機能をもたない通常のレイヤ２中継装置を混在させると、当該中継装置はそのフレームがどのＶＬＡＮに対応するのか判断することができず、適切にフレームを中継することができない。よって、この方法を採用する場合、暗号処理機能をもたない通常のレイヤ２中継装置を混在させることができない。

【０１３７】

一方、図１０の暗号化フレーム１７０は、クリアテキストの状態のＴＰＩＤ１６１およびＴＣＩ１６２の後に、暗号ヘッダ１７１と暗号化データ部１７２が続いている。よって、暗号処理機能をもたない通常のレイヤ２中継装置でも、そのフレームがどのＶＬＡＮに対応するのかを判断することができ、適切にフレームを中継することができる。この場合、その通常のレイヤ２中継装置にとっては、暗号化フレーム１７０は単なるタグつきフレームとして認識される。したがって、本発明によれば、通常のレイヤ２中継装置を混在させてネットワークを構成することができ、既存の装置を有効に利用することができる。また、共通鍵生成装置１を含むＬ２中継装置１０１を様々なネットワーク構成において利用することができる。

【０１３８】

なお、図６や図８に示したＬ２中継装置１０１におけるフレーム中継処理部１０２も暗号処理機能をもたないことに注目すると、第二の特徴から得られる利点は、次のごとくである。すなわち、フレーム中継処理部１０２は、図１０の暗号化フレーム１７０を単なるタグつきフレーム１６０と同様に認識し、暗号化について何ら考慮することなく中継処理を行うことができる。つまり、フレーム中継処理部１０２は、暗号処理機能をもたない従来のレイヤ２中継装置におけるフレーム中継処理部とまったく同様の処理を行うだけでよい。また、図８に示したように、暗号処理モジュールを全ポートに搭載する必要もない。

【０１３９】

なお、ＶＬＡＮを使わない環境においては、タグつきフレーム１６０ではなくフレーム１５０を暗号化する。よって、その場合の暗号化フレームは、図１０の暗号化フレーム１７０からＴＰＩＤ１６１とＴＣＩ１６２を除いた形式となる。

【０１４０】

図１１は、暗号ヘッダ１７１の詳細を示す図である。図１１に示したとおり暗号ヘッダ１７１の長さは１２バイトである。暗号ヘッダ１７１は図１１に示すごとく、先頭から順に、２バイトのタイプ１７１１、１バイトのサブタイプ１７１２、１バイトの予約フィールド１７１３、８バイトのシーケンス番号１７１４からなる。

【０１４１】

タイプ１７１１はフレームの種別を表すグローバルユニークな値を格納するフィールドである。タイプ１７１１をグローバルユニークな値とするためには、ＩＥＥＥに値の割り当てを申請し、ＩＥＥＥに値を割り当ててもらう必要がある。タイプ１７１１がグローバルユニークな値でなくてはならない理由は、以下の通りである。

【０１４２】

図１０と図１１とから分かるとおり、ＶＬＡＮを使用する環境ではタイプ１７１１はＴ

ＣＩ１６２の直後にあり、ＶＬＡＮを使用しない環境ではタイプ１７１１は送信元ＭＡＣアドレス１５２の直後にある。したがって、フレーム１５０またはタグつきフレーム１６０におけるタイプ（データ部１５３の先頭にある）と、暗号化フレーム１７０におけるタイプ１７１１とは、同じ位置にある。よって、タイプ１７１１の値によって暗号ヘッダ１７１の有無を判別する必要がある。

【０１４３】

ところで、フレーム１５０やタグつきフレーム１６０においてデータ部１５３の先頭にあるタイプは、上位層すなわちレイヤ３が使用しているプロトコルを識別するためのグローバルユニークな値である。例えば、０ｘ０８００はＩＰを表す。タイプの値が０ｘ０８００のとき、データ部１５３はＩＰの形式にしたがったデータである。

【０１４４】

よって、タイプ１７１１にグローバルユニークな特定の値（仮にＺとする）を割り当てることによって、暗号ヘッダ１７１の有無を判別することができるようになる。つまり、ＶＬＡＮを使用する環境ではＴＣＩ１６２の直後の２バイトの値がＺなら暗号ヘッダ１７１があると判定することができ、ＶＬＡＮを使用しない環境では送信元ＭＡＣアドレス１５２の直後の２バイトの値がＺなら暗号ヘッダ１７１があると判定することができる。

【０１４５】

このようにして暗号ヘッダ１７１の有無を判定可能とすることにより、例えば、図９Ｂにおいてポート１０３ｈからフレームを受信した暗号処理モジュール１０４ｂが、受信したのが暗号化フレームなのか平文フレームなのかを暗号ヘッダ１７１の有無に基づいて判断することができるようになる。

【０１４６】

サブタイプ１７１２は、ＩＥＥＥから割り当てられた一つの値（上記のＺ）を様々な目的で利用するためのフィールドである。タイプ１７１１とサブタイプ１７１２は、上位層のデータが何を表しているのかを識別することができればよく、数値そのものに意味はない。例えば、「タイプ１７１１がＺでサブタイプ１７１２の値が０ｘ０１のとき、イーサネットの暗号化通信を行っており、暗号ヘッダ１７１に暗号化データ部１７２が続くことを表す」などと決めることができる。

【０１４７】

予約フィールド１７１３は将来の使用のために予約された１バイトである。使用例の一つを図１７とあわせて後述する。

シーケンス番号１７１４は、鍵素材としてのシーケンス番号ｋ２＿ｒを格納するフィールドである。シーケンス番号１７１４のフィールド長は８バイト、すなわち６４ビットなので、2^{64}個の番号が利用可能である。したがって、１Ｇｂｐｓや１０Ｇｂｐｓといった高速回線であっても、同じシーケンス番号が使われるには極めて長い時間が必要である。

【０１４８】

例えば、暗号処理モジュールが１秒あたり１Ｇ個のフレームを暗号化する場合、同じシーケンス番号に戻るのに

$2^{64}／10^{9}＝1.84\times10^{10}$秒　５８５年

かかる。よって、シーケンス番号１７１４は事実上ユニークと考えてよい。

【０１４９】

ただし、二つ以上の暗号処理モジュール１０４が偶然同じ値を用いることはあり得る。そこで、各暗号処理モジュール１０４におけるシーケンス番号の開始値（つまり鍵素材格納部１２の初期値）をランダムに設定することにより、偶然二つ以上の暗号処理モジュールが同じ値を用いる確率を小さくすることが望ましい。

【０１５０】

図１２から図１４は、共通鍵生成装置１を搭載したＬ２中継装置１０１を使ったネットワークの構成例を示す。Ｌ２中継装置１０１は、図６と図８に示したように、実施形態によってどのポートに暗号処理モジュール（１０４ａ等）を備えるかという点で様々に異な

る。さらに、各暗号処理モジュールは、実施形態によって、フレームが送信される方向に応じて暗号化と復号化のどちらを行うのかという点で異なる。

【０１５１】

これらの変化の組み合わせによって、Ｌ２中継装置１０１の価格や、レイヤ２の暗号化通信を実現するためのネットワーク構成の仕方が異なる。つまり、本発明は、利用者の都合に合わせて様々な形態で実施することができ、非常に柔軟である。

【０１５２】

なお、図１２から図１４では、ＴＣＧ対応チップ等の構成要素を省略している。また、平文フレームが実線の矢印に、暗号化フレームが破線の矢印に対応する。そして、暗号化通信が行われる範囲が網かけにより示されている。

【０１５３】

図１２のネットワーク構成では、一つのポートにしか暗号処理モジュールを備えていない安価なＬ２中継装置１０１ａ～１０１ｅと従来のＬ２スイッチ１４１ｂのみを用いている。

【０１５４】

図１２では、四台のＰＣ４ａ～４ｄが、Ｌ２中継装置１０１ａ～１０１ｄにそれぞれ接続されている。Ｌ２中継装置１０１ａ～１０１ｄはいずれも、暗号処理を行わない従来のＬ２スイッチ１４１ｂに接続されている。そしてＬ２スイッチ１４１ｂはＬ２中継装置１０１ｅに接続されている。つまり、ケーブルの配線という物理的な意味での図１２のトポロジは、１対Ｎのスター型のスイッチトポロジによく似たトポロジだが、暗号化通信を行うペアという論理的な意味でのトポロジは、Ｎ対Ｎの関係のトポロジである。つまり、Ｌ２中継装置１０１ａと１０１ｂのペア、Ｌ２中継装置１０１ａと１０１ｃのペア、Ｌ２中継装置１０１ａと１０１ｄのペア、Ｌ２中継装置１０１ｂと１０１ｃのペア、Ｌ２中継装置１０１ｂと１０１ｄのペア、……などの組み合わせで暗号化通信を行うので、Ｎ対Ｎの関係である。

【０１５５】

Ｌ２中継装置１０１ａ～１０１ｄのそれぞれは、Ｌ２スイッチ１４１ｂと接続されたポートに対応して暗号処理モジュール１０４ａ～１０４ｄが備えられているが、それ以外のポートには暗号処理モジュールは備えられていない。Ｌ２中継装置１０１ｅは、Ｌ２スイッチ１４１ｂと接続されたポートに対応して暗号処理モジュール１０４ｅが備えられているが、Ｌ２中継装置１０１ｅのそれ以外のポートには暗号処理モジュールは備えられていない。Ｌ２中継装置１０１ｅはファイヤウォール１４３とも接続されており、ファイヤウォール１４３はルータ１４４に接続されている。インターネット１４５など外部のネットワークとの通信は、ルータ１４４を介して行われる。

【０１５６】

図１２におけるＬ２中継装置１０１ａ～１０１ｅはいずれも、一つのポートにのみ暗号処理モジュールを備えているため、安価に製造することができる。また、図１２の暗号処理モジュール１０４ａ～１０４ｅは、いずれも対応するポートへの送信時にフレームを暗号化し、対応するポートからの受信時にフレームを復号化する。

【０１５７】

つまり、図７と対応させて説明すると、フレーム中継処理部１０２から受付部１１がフレームを受信した場合には、判定部１５が第一の局面（暗号化すべき局面）であると判定し、共通鍵生成部１４が共通鍵ｋを生成し、暗号化部１６がフレームを暗号化する。一方、対応するポート１０３から受付部１１がフレームを受信した場合には、判定部１５が第二の局面（復号化すべき局面）であると判定し、共通鍵生成部１４が共通鍵ｋを生成し、復号化部１７がフレームを復号化する。

【０１５８】

このように構成した場合の通信の例を以下で説明する。なお、図１２において、ＰＣ４ａからＰＣ４ｂに図１０のフレーム１５０を送信する場合、フレーム１５０は暗号処理モジュール１０４ａを経由する際に暗号化される。図１２の例ではＶＬＡＮを利用していな

いため、暗号化フレームは、図１０の暗号化フレーム１７０からＴＰＩＤ１６１とＴＣＩ１６２を削除した形式である。

【０１５９】

暗号化フレームは、Ｌ２中継装置１０１ａからＬ２スイッチ１４１ｂに送信され、ＰＣ４ｂと接続されたＬ２中継装置１０１ｂへと中継される。暗号化フレームのＭＡＣヘッダは暗号化されていないため、Ｌ２スイッチ１４１ｂは何ら暗号に関する処理を行うことなく、通常のフレーム１５０と同様にして暗号化フレームを中継することができる。

【０１６０】

この暗号化フレームはＬ２中継装置１０１ｂに受信され、Ｌ２中継装置１０１ｂに備えられた暗号処理モジュール１０４ｂを経由する際に復号化される。復号化されたフレームは、Ｌ２中継装置１０１ｂ内のフレーム中継処理部により、ＰＣ４ｂに接続されたポートへと中継され、そのポートからＰＣ４ｂへと送信される。

【０１６１】

次に、図１２において、ＰＣ４ａからインターネット１４５にＩＰパケットを送信する例を説明する。このＩＰパケットに対応するフレームがＰＣ４ａからＬ２中継装置１０１ａとＬ２スイッチ１４１ｂを経由してＬ２中継装置１０１ｅへ送信される。

【０１６２】

ＰＣ４ａからＬ２スイッチ１４１ｂまでの経路は上記の例とまったく同様である。Ｌ２スイッチ１４１ｂは、受信した暗号化フレームを通常のフレームと同様に中継して、Ｌ２中継装置１０１ｅへ送信する。Ｌ２中継装置１０１ｅには、Ｌ２スイッチ１４１ｂに接続されたポートに対応して暗号処理モジュール１０４ｅが備わっている。暗号化フレームは、その暗号処理モジュール１０４ｅを経由する際に復号化されて平文フレームとなり、不図示のフレーム中継処理部を経由してファイヤウォール１４３に送信される。

【０１６３】

以上のように、図１２の構成によれば、イーサネットでの通信を暗号化することができる。また、Ｌ２中継装置１０１ｅからファイヤウォール１４３へ送信されるフレームは復号化された平文フレームなので、既存のファイヤウォール１４３やルータ１４４の構成を変える必要もない。

【０１６４】

なお、図１２における暗号処理モジュール１０４ａ～１０４ｅは、暗号化処理と復号化処理のいずれかを必ず行う構成であると仮定している。すなわち、判定部１５（図７）は、第一の局面と第二の局面のいずれであるかを判定するが、それ以外の局面であると判定することはない。一方、図９Ａおよび図９Ｂにおける暗号処理モジュール１０４ａ、１０４ｂは、前述のとおり、暗号処理の要否を判定し、ＶＬＡＮ１３０に対応するフレームに対しては何も処理しないよう構成されている。つまり、判定部１５は第一、第二、第三の局面のいずれであるかを判定する。どちらの構成によっても本発明を実施することができるが、図１２のように暗号処理の要否を判定しない実施形態の方が、処理が簡素で高速になり、ハードウェア化も容易である。

【０１６５】

仮に、図１２において、暗号処理モジュール１０４ａ～１０４ｄ（特にその中の判定部１５）を、暗号処理の要否を判定するように構成すれば、インターネット１４５との通信において暗号処理モジュール１０４ｅで復号化処理を行う必要がないため、Ｌ２中継装置１０１ｅは不要である。ただし、その場合で、ＶＬＡＮを使用しないのであれば、例えば送信先ＭＡＣアドレス１５１に基づいて暗号処理の要否を暗号処理モジュール１０４ａなどが判定するといった動作が必要になる。

【０１６６】

図１３のネットワーク構成では、一つのポートにしか暗号処理モジュールを備えていない安価なＬ２中継装置１０１ａ～１０１ｄと、複数のポートに暗号処理モジュールを備えた高価なＬ２中継装置１０１ｅを用いている。

【０１６７】

図１２と図１３の大きな違いは、図１２では必要だったＬ２スイッチ１４１ｂが図１３では不要な点である。そのかわり図１３では、複数のポートに暗号処理モジュールを備えた高価なＬ２中継装置１０１ｅが必要となっている。

【０１６８】

図１３のネットワーク構成も図１２と同様に、ケーブルの配線という物理的な意味では１対Ｎのスター型のスイッチトポロジだが、暗号化通信を行うペアという論理的な意味でのトポロジはＮ対Ｎの関係のトポロジである。

【０１６９】

図１３において、四台のＰＣ４ａ～４ｄがＬ２中継装置１０１ａ～１０１ｄにそれぞれ接続されている。Ｌ２中継装置１０１ａ～１０１ｄはいずれも、Ｌ２中継装置１０１ｅに接続されている。Ｌ２中継装置１０１ａ～１０１ｄのそれぞれは、Ｌ２中継装置１０１ｅと接続されたポートに対応して暗号処理モジュール１０４ａ～１０４ｄが備えられているが、それ以外のポートには暗号処理モジュールは備えられていない。Ｌ２中継装置１０１ｅは複数のポートに暗号処理モジュールを備えている。具体的には図１３に示すように、Ｌ２中継装置１０１ａ～１０１ｄと接続された複数のポートに対応して、それぞれ暗号処理モジュール１０４ｅ～１０４ｎが備えられている。Ｌ２中継装置１０１ｅはファイヤウォール１４３とも接続されており、ファイヤウォール１４３はルータ１４４に接続されている。インターネット１４５など外部のネットワークとの通信は、ルータ１４４を介して行われる。

【０１７０】

図１３における暗号処理モジュール１０４ａ～１０４ｎは、いずれも対応するポートへの送信時にフレームを暗号化し、対応するポートからの受信時にフレームを復号化する。

つまり、図７と対応させて説明すると、フレーム中継処理部１０２から受付部１１がフレームを受信した場合には、判定部１５が第一の局面（暗号化すべき局面）であると判定し、共通鍵生成部１４が共通鍵ｋを生成し、暗号化部１６がフレームを暗号化する。一方、対応するポート１０３から受付部１１がフレームを受信した場合には、判定部１５が第二の局面（復号化すべき局面）であると判定し、共通鍵生成部１４が共通鍵ｋを生成し、復号化部１７がフレームを復号化する。

【０１７１】

例えば、ＰＣ４ａからＰＣ４ｂにフレームを送信する場合について図１３を参照して説明する。図１３のＬ２中継装置１０１ａは、図１２のＬ２中継装置１０１ａと同様の構成である。

【０１７２】

まず、ＰＣ４ａから図４のフレーム１５０が送信される。このフレーム１５０は、Ｌ２中継装置１０１ａの暗号処理モジュール１０４ａを経由する際に暗号化される。暗号化フレームは、Ｌ２中継装置１０１ａからＬ２中継装置１０１ｅに送信され、暗号処理モジュール１０４ｅを経由する際に復号化される。復号化されたフレームは暗号処理モジュール１０４ｅから不図示のフレーム中継処理部を経由して暗号処理モジュール１０４ｆに中継され、暗号処理モジュール１０４ｆにおいて再度暗号化される。暗号化されたフレームは暗号処理モジュール１０４ｆに対応するポートからＬ２中継装置１０１ｂに送信される。Ｌ２中継装置１０１ｂで受信されたフレームは、暗号処理モジュール１０４ｂを経由する際に復号化され、ＰＣ４ｃに送信される。

【０１７３】

次に、図１３においてＰＣ４ａからインターネット１４５にＩＰパケットを送信する例を説明する。このＩＰパケットに対応するフレームがＰＣ４ａからＬ２中継装置１０１ａを経由してＬ２中継装置１０１ｅへ送信される。

【０１７４】

ＰＣ４ａからＬ２中継装置１０１ｅまでの経路、およびフレームが暗号処理モジュール１０４ｅを経由する際に復号化される点は上記の例とまったく同様である。その後、復号化フレームは、不図示のフレーム中継処理部を介してファイヤウォール１４３に接続され

たポート１０３に中継され、ファイヤウォール１４３に送信される。

【０１７５】

図１３に示した構成によれば、Ｌ２中継装置１０１ｅのように高価な装置が必要ではあるものの、図１２よりも少ない装置でネットワークを構成し、イーサネットでの通信を暗号化することができる。また、Ｌ２中継装置１０１ｅからファイヤウォール１４３に送信されるのは復号化された平文フレームなので、既存のファイヤウォール１４３やルータ１４４の構成を変える必要がない。

【０１７６】

図１４のネットワーク構成では、一つのポートにしか暗号処理モジュールを備えていない安価なＬ２中継装置１０１ａ～１０１ｅのみを用いている。図１４は、Ｌ２中継装置１０１ｅの具体的な構成が図１３のＬ２中継装置１０１ｅと異なるという以外は、図１３と同様である。

【０１７７】

図１４の構成は、図１２に比べて一つ装置の数が少なくて済み（Ｌ２スイッチ１４１ｂが不要）、図１３に比べて安価な装置だけで済む（図１３のＬ２中継装置１０１ｅは高価だが図１４のＬ２中継装置１０１ｅは安価である）という利点がある。このような構成が可能となる理由は、図１２や図１３とは逆に、対応するポートへの送信時にフレームを復号化し、対応するポートからの受信時にフレームを暗号化する暗号処理モジュール１０４ｅを用いたためである。

【０１７８】

つまり、図７と対応させて説明すると、暗号処理モジュール１０４ｅにおいては、フレーム中継処理部１０２から受付部１１がフレームを受信した場合には、判定部１５が第二の局面（復号化すべき局面）であると判定し、共通鍵生成部１４が共通鍵ｋを生成し、復号化部１７がフレームを復号化する。一方、対応するポート１０３から受付部１１がフレームを受信した場合には、判定部１５が第一の局面（暗号化すべき局面）であると判定し、共通鍵生成部１４が共通鍵ｋを生成し、暗号化部１６がフレームを暗号化する。

【０１７９】

例えば、ＰＣ４ａからＰＣ４ｂにフレームを送信する場合について図１４を参照して説明する。ＰＣ４ａから送信されたフレーム１５０がＬ２中継装置１０１ａの暗号処理モジュール１０４ａで暗号化され、Ｌ２中継装置１０１ｅに送信されるまでは、図１３の場合と同様である。

【０１８０】

この暗号化フレームは、Ｌ２中継装置１０１ｅの内部において、暗号化された状態のまま中継され、Ｌ２中継装置１０１ｂへと送信される。そして、この暗号化フレームはＬ２中継装置１０１ｂで受信され、暗号処理モジュール１０４ｂを経由する際に復号化される。復号化されたフレームは、不図示のフレーム中継処理部により中継され、ＰＣ４ｂに送信される。図１４と図１３の違いは、図１４ではＰＣ４ａからＰＣ４ｂにフレームを送信する際にＬ２中継装置１０１ｅが何ら暗号に関する処理を行わない点である。

【０１８１】

次に、図１４においてＰＣ４ａからインターネット１４５にＩＰパケットを送信する例を説明する。このＩＰパケットに対応するフレームがＰＣ４ａからＬ２中継装置１０１ａを経由してＬ２中継装置１０１ｅへ送信される。

【０１８２】

ＰＣ４ａからＬ２中継装置１０１ｅまでの経路は上記の例とまったく同様である。その後、Ｌ２中継装置１０１ｅが受信した暗号化フレームは、暗号化された状態のまま不図示のフレーム中継処理部を介して中継され、暗号処理モジュール１０４ｅを経由する。その際に、暗号処理モジュール１０４ｅが暗号化フレームを復号化し、復号化された平文フレームがファイヤウォール１４３に送信される。

【０１８３】

図１４に示した構成によれば、図１２よりも少ない装置のみで、また、図１３よりも安

価な装置のみで、ネットワークを構成し、イーサネットでの通信を暗号化することができる。図１４の構成は、図１２に比べて装置の数が少ないので、コストパフォーマンスが優れているだけでなく、障害の発生率も低い。なぜなら、図１２ではＬ２スイッチ１４１ｂの障害がネットワーク全体の障害を引き起こすが、図１４の構成にはＬ２スイッチ１４１ｂが存在しないためである。また、図１４のＬ２中継装置１０１ｅからファイヤウォール１４３に送信されるのは復号化された平文フレームなので、既存のファイヤウォール１４３やルータ１４４の構成を変える必要がない。

【０１８４】

以上説明したように、暗号処理モジュールは、フレームの送受信の方向によって暗号化処理と復号化処理のいずれを行うか、という点では二種類のものがある。換言すれば、図７の共通鍵生成装置１ｃにおいて、判定部１５がどのような条件にもとづいて第一の局面と第二の局面を判定するのかという点は、実施形態によって異なる。つまり、図７でポート１０３から受付部１１がフレームを受信したときに、判定部１５が第一の局面と判定するのか、第二の局面と判定するのかという点は、実施形態によって異なる。

【０１８５】

また、図１２から図１４の例ではＶＬＡＮの使用を考慮していないため、判定部１５は必ず第一または第二の局面の一方であると判定する。しかし、ＶＬＡＮを利用する環境においては、第三の局面（暗号化も復号化も不要なので共通鍵ｋを生成する必要がない）であると判定することもある。したがって、判定部１５がどのような条件に基づき判定するのかという点と、いくつの局面の中から一つを選択して判定するのかという点において、様々な実施形態がありうる。

【０１８６】

個々の暗号処理モジュールが、フレームの送受信の方向によって暗号化処理と復号化処理のいずれを行うかという点は、任意に選択可能である。例えば、管理者がＬ２中継装置１０１に設定を入力し、ＣＰＵ１０６がその内容を個々の暗号処理モジュール１０４に設定してもよい。よって、図１２～図１４で説明したような様々な構成の中から、個々の実施形態に応じた適切な構成を利用者が選択し、その選択にあわせて暗号処理モジュール１０４の動作を設定することが可能である。

【０１８７】

図１５は、図３に示した共通鍵ｋの生成に利用される各種情報のより具体的な例を説明する図である。図１５では、ＭＡＣヘッダ情報ｋ１＿ｆ、シーケンス番号ｋ２＿ｎ、マスター鍵ｋ３の三つの情報を利用して共通鍵ｋを生成することを示している。なお、図１５の例は、図６から図１４に示したＬ２中継装置１０１内の共通鍵生成装置に適用される。

【０１８８】

図１５には、図１０と同様のフレーム１５０および暗号化フレーム１７０を示すとともに、Ｌ２中継装置１０１のうち、共通鍵ｋの生成に利用する情報に特に関係のある部分を抜粋して示してある。

【０１８９】

図１５において、事前共有鍵ｋ０は、例えば管理者等によりＬ２中継装置１０１に事前に設定される。人間が設定しやすいように、８文字以内の英数字からなるパスワードを事前共有鍵ｋ０として用いてもよい。

【０１９０】

図５に関して説明したごとく、暗号化通信を行う二台の中継装置２ａ、２ｂにおいて、マスター鍵ｋ３は同じ値でなくてはならないため、同じ値の事前共有鍵ｋ０がこれら二台の中継装置２ａ、２ｂに設定されなくてはならない。もちろん、事前共有鍵ｋ０からマスター鍵ｋ３を生成するアルゴリズムも、これら二台の中継装置２ａ、２ｂで同じでなくてはならない。すなわち、個々の中継装置２ａ、２ｂの違いによらず、同じ事前共有鍵ｋ０からは同じマスター鍵ｋ３が一意に生成されなくてはならない。

【０１９１】

設定された事前共有鍵ｋ０は、図１５に示すとおり、ＴＣＧ対応チップ１０５に格納さ

れる。よって、事前共有鍵ｋ０を外部から不正に読み取ることは不可能である。
なお、同じ値の事前共有鍵ｋ０を設定すべき中継装置の組み合わせは、実施形態により異なる。ある実施形態では、事前共有鍵ｋ０は、暗号化通信を行う範囲に含まれるすべてのＬ２中継装置１０１において同じ値が設定される。例えば、図９Ａでは、Ｌ２中継装置１０１ａ、１０１ｂの双方に同じ値の事前共有鍵ｋ０が設定され、図１４では、Ｌ２中継装置１０１ａ～１０１ｅのすべてに同じ値の事前共有鍵ｋ０が設定される。

【０１９２】

ＶＬＡＮを利用する別の実施形態では、ＶＬＡＮごとに異なる事前共有鍵ｋ０を設定してもよい。例えば、図９Ａの例ではＬ２中継装置１０１ａ、１０１ｂの双方に対し、ＶＬＡＮ１１０用の事前共有鍵ｋ０とＶＬＡＮ１２０用の事前共有鍵ｋ０’をそれぞれ設定してもよい。ただし、この場合も、Ｌ２中継装置１０１ａ、１０１ｂの双方で同じ値が設定されるという点は上記実施形態と共通である。

【０１９３】

ＭＡＣヘッダ情報ｋ１＿ｆは、送信先・送信元情報ｋ１の具体例である。図１５では、ＭＡＣヘッダ情報ｋ１＿ｆは、送信先ＭＡＣアドレス１５１および送信元ＭＡＣアドレス１５２の双方からなる情報である。他の実施形態では、ＭＡＣヘッダ情報ｋ１＿ｆは、送信先ＭＡＣアドレス１５１と送信元ＭＡＣアドレス１５２の少なくとも一方に基づく情報であってもよい。また、送信先ＭＡＣアドレス１５１や送信元ＭＡＣアドレス１５２の全部ではなく一部のみをＭＡＣヘッダ情報ｋ１＿ｆとして利用することも可能である。

【０１９４】

図１５や図１０から分かるように、ＭＡＣヘッダ情報ｋ１＿ｆは、暗号化の対象であるフレーム１５０またはタグつきフレーム１６０からも、復号化の対象である暗号化フレーム１７０からも、取得することができる。

【０１９５】

シーケンス番号ｋ２＿ｓおよびｋ２＿ｒは、鍵素材ｋ２の具体例である。上述のように鍵素材ｋ２は第一の局面と第二の局面で取得方法が異なるが、シーケンス番号ｋ２＿ｓが第一の局面に対応し、シーケンス番号ｋ２＿ｒが第二の局面に対応する。ただし、図１や図５から分かるように、シーケンス番号ｋ２＿ｓの値がシーケンス番号ｋ２＿ｒとして入力データ（フレーム１５０、タグつきフレーム１６０、暗号化フレーム１７０など）に含まれる。よって、シーケンス番号ｋ２＿ｓおよびｋ２＿ｒの両方を指す場合は、総称として「ｋ２＿ｎ」という符号を用いる。

【０１９６】

シーケンス番号ｋ２＿ｓは、暗号処理モジュール１０４ごとに、つまり図７の共通鍵生成装置１ｃごとに管理される番号である。シーケンス番号ｋ２＿ｓは鍵素材格納部１２に格納されており、判定部１５が第一の局面であると判定するたびに、鍵素材読み取り部１３により１ずつインクリメントされる。図１１のシーケンス番号１７１４は、共通鍵生成装置１への入力データとしての暗号化フレーム１７０に書き込まれたシーケンス番号ｋ２＿ｒであり、データ長が８バイトである。

【０１９７】

したがって、本実施形態における鍵素材格納部１２は８バイトのカウンタである。なお、カウンタの初期値は、前述したごとく、暗号処理モジュール１０４によってランダムに異なる値が設定されていることが望ましい。

【０１９８】

マスター鍵ｋ３は、事前共有鍵ｋ０に基づいて暗号処理モジュール１０４が生成する。マスター鍵ｋ３は事前共有鍵ｋ０よりも長いデータ長を持つことが望ましい。
マスター鍵ｋ３の生成は、例えば次のように実行される。管理者が事前共有鍵ｋ０をＬ２中継装置１０１に設定すると、ＣＰＵ１０６が暗号処理モジュール１０４にマスター鍵ｋ３の生成を命令し、暗号処理モジュール１０４内のマスター鍵生成部２０はその命令にしたがってマスター鍵ｋ３を生成してマスター鍵格納部２１に格納する。あるいは、マスター鍵ｋ３のもととなる候補値の配列であるマスター鍵配列Ｃを事前共有鍵ｋ０に基づい

て暗号処理モジュール１０４が生成してもよい。この場合、マスター鍵配列Ｃが暗号処理モジュール１０４の内部に格納され、その中からマスター鍵ｋ３が選択される（詳細は後述する）。いずれにしても、マスター鍵ｋ３は事前共有鍵ｋ０に基づいて生成される。なお、事前共有鍵ｋ０からマスター鍵ｋ３を生成する方法には、後述するようにいくつかの方法がある。

【０１９９】

図１５の例では、共通鍵ｋが、ＭＡＣヘッダ情報ｋ１＿ｆとシーケンス番号ｋ２＿ｎとマスター鍵ｋ３とから生成される。これは、ある関数ｆを用いて、

ｋ＝ｆ（ｋ１＿ｆ，ｋ２＿ｓ，ｋ３）
＝ｆ（ｋ１＿ｆ，ｋ２＿ｒ，ｋ３）
＝ｆ（ｋ１＿ｆ，ｋ２＿ｎ，ｋ３）　　……（１）

と表すことができる。式（１）に示したとおり、第一の局面（暗号化のために共通鍵ｋを生成する局面）と第二の局面（復号化のために共通鍵ｋを生成する局面）において、同じ関数ｆを用いる。

【０２００】

また、マスター鍵ｋ３は事前共有鍵ｋ０に基づいて生成されるので、ある関数ｇとｆ２を用いて、

ｋ＝ｆ（ｋ１＿ｆ，ｋ２＿ｎ，ｇ（ｋ０））
＝ｆ２（ｋ１＿ｆ，ｋ２＿ｎ，ｋ０）　　……（２）

と表すこともできる。つまり、図１５の例は、「共通鍵ｋが、送信先・送信元情報ｋ１と鍵素材ｋ２と事前共有鍵ｋ０に基づいて生成される」と表現することも可能である。なお、後述するように、関数ｆの具体的な内容は実施形態により様々に異なる。

【０２０１】

第一の局面（暗号化のために共通鍵ｋを生成する）における暗号処理モジュール１０４の動作は次のステップ（ｓ１）～（ｓ７）のとおりである。

（ｓ１）暗号化の対象となる平文フレームを、対応するポートまたはフレーム中継処理部１０２から暗号処理モジュール１０４が受信する。つまり、暗号処理モジュール１０４内の受付部１１が入力データとして平文フレームを受け付ける。

（ｓ２）判定部１５が第一の局面であると判定し、鍵素材読み取り部１３、共通鍵生成部１４に第一の局面であるという判定結果を通知する。なお、図９Ａ～図９Ｂ、図１２～図１４に関して説明したように、実施形態によってこの判定に利用される具体的な判定条件は異なる。ステップ（ｓ１）においてフレームをどこから受信したか、受信したフレームが暗号ヘッダ１７１を含むか、ＶＬＡＮを利用している環境か、ＶＬＡＮを利用している場合ＴＣＩ１６２の値は何か、などの情報を一つ以上組み合わせることにより、判定部１５はこの判定を行う。

（ｓ３）暗号処理モジュール１０４内の共通鍵生成部１４が、そのフレームからＭＡＣヘッダ情報ｋ１＿ｆを読み取る。

（ｓ４）暗号処理モジュール１０４内の鍵素材読み取り部１３が、カウンタ（つまり鍵素材格納部１２）から現在のシーケンス番号ｋ２＿ｓを読み取り、カウンタの値を１増やす。

（ｓ５）暗号処理モジュール１０４内の共通鍵生成部１４が、格納済みのマスター鍵ｋ３を読み出す、または、事前共有鍵ｋ０に基づいてマスター鍵ｋ３を生成する。

（ｓ６）暗号処理モジュール１０４内の共通鍵生成部１４が、上記の関数ｆを用いて、ｋ＝ｆ（ｋ１＿ｆ，ｋ２＿ｓ，ｋ３）　なる共通鍵ｋを生成する。

（ｓ７）暗号処理モジュール１０４内の暗号化部１６が、共通鍵ｋを用いてフレームを暗号化し、（ｓ４）で読み取った値を暗号ヘッダ１７１にシーケンス番号ｋ２＿ｒとして書き込む。

【０２０２】

第二の局面（復号化のために共通鍵ｋを生成する）における暗号処理モジュール１０４の動作は次のステップ（ｒ１）～（ｒ７）のとおりである。

（ｒ１）復号化の対象となる暗号化フレームを、対応するポートまたはフレーム中継処理部１０２から暗号処理モジュール１０４が受信する。つまり、暗号処理モジュール１０４内の受付部１１が入力データとして暗号化フレームを受け付ける。
（ｒ２）判定部１５が第二の局面であると判定する。判定部１５は、鍵素材読み取り部１３、共通鍵生成部１４に第二の局面であるという判定結果を通知する。この判定に利用される具体的な判定条件が実施形態により異なる点は、ステップ（ｓ２）に関して説明したとおりである。
（ｒ３）暗号処理モジュール１０４内の共通鍵生成部１４が、そのフレームからＭＡＣヘッダ情報ｋ１＿ｆを読み取る。
（ｒ４）暗号処理モジュール１０４内の鍵素材読み取り部１３が、そのフレームの暗号ヘッダ１７１内の所定の部分（シーケンス番号１７１４）からシーケンス番号ｋ２＿ｒを読み取る。
（ｒ５）暗号処理モジュール１０４内の共通鍵生成部１４が、格納済みのマスター鍵ｋ３を読み出す、または、事前共有鍵ｋ０に基づいてマスター鍵ｋ３を生成する。
（ｒ６）暗号処理モジュール１０４内の共通鍵生成部１４が、上記の関数ｆを用いて、
ｋ＝ｆ（ｋ１＿ｆ，ｋ２＿ｒ，ｋ３）　なる共通鍵ｋを生成する。なお、この関数ｆはステップ（ｓ６）における関数ｆと同じ関数である。
（ｒ７）暗号処理モジュール１０４内の復号化部１７が、共通鍵ｋを用いてフレームを復号化する。

【０２０３】

例えば、図９Ａでは、Ｌ２中継装置１０１ａ、１０１ｂの双方において同じ値のｋ０が設定されており、ＭＡＣヘッダ情報ｋ１＿ｆはフレームの送信時と受信時で同じ内容であり、カウンタ（鍵素材格納部１２）に格納されたシーケンス番号ｋ２＿ｓの値がシーケンス番号ｋ２＿ｒとして暗号化フレーム１７０に含まれる。よって、式（１）と（２）から、Ｌ２中継装置１０１ａ、１０１ｂの双方が同じ値の共通鍵ｋを生成することが分かる。

【０２０４】

上記の関数ｆは、以下のような点を考慮して適切に定めるのが好ましい。
ＭＡＣヘッダ情報ｋ１＿ｆは、フレームの送信元と送信先のペアごとに異なる。よって、異なるノード間の通信ではＭＡＣヘッダ情報ｋ１＿ｆが異なる。異なるＭＡＣヘッダ情報ｋ１＿ｆに対しては異なる共通鍵ｋが生成されるような関数ｆを利用すれば、異なるノード間の通信に対しては異なる共通鍵ｋが使われ、高いセキュリティレベルを実現することができる。

【０２０５】

また、シーケンス番号ｋ２＿ｎは、判定部１５が第一の局面であると判定して暗号処理モジュール１０４がフレームを暗号化するたびに１ずつ増加する番号であり、かつ、十分に長いデータ長を有する。よって、シーケンス番号ｋ２＿ｎは、同一ノード間の通信でもフレームごとに異なる値となる。よって、異なるシーケンス番号ｋ２＿ｎに対しては異なる共通鍵ｋが生成されるような関数ｆを利用すれば、フレームごとに異なる共通鍵ｋが使われ、高いセキュリティレベルを実現することができる。

【０２０６】

以上のように共通鍵ｋを生成することにより、共通鍵ｋがＭＡＣヘッダ情報ｋ１＿ｆおよびシーケンス番号ｋ２＿ｎによって異なる値となる。よって、ＩＫＥなどにしたがって動的に鍵情報の交換を行ってリキーを行わなくても、事実上フレームごとに異なる共通鍵ｋが使われる。

【０２０７】

本発明によれば、動的に鍵情報の交換を行わなくてもよいため、複雑なプロトコルを実装する必要がない。また、動的に鍵情報の交換を行う場合、一つの中継装置に障害があると全体に影響し、通信が切断されるが、本発明では他のＬ２中継装置１０１への影響はない。したがって、上記のように生成した共通鍵ｋを利用することは、セキュリティ、スケーラビリティ、信頼性のすべてを満足する効果をもつ。

【０２０８】
以下では、共通鍵ｋの生成の具体的な方法について、いくつか説明する。
共通鍵ｋを生成する第一の方法は、関数ｆとしてハッシュ関数ｈを利用することである。つまり上記の式（１）に式（３）を適用する方法である。
【０２０９】
ｆ（ｘ１，ｘ２，ｘ３）≡ｈ（ｘ１＋ｘ２＋ｘ３）　　……（３）
ここで、ハッシュ関数ｈとして、ＭＤ５（Message Digest Algorithm 5）やＳＨＡ‐１（Secure Hash Algorithm-1）等の汎用の高速ハッシュ関数を利用することができる。暗号化通信の送信側と受信側の暗号処理モジュール１０４同士が同じハッシュ関数を利用してさえいれば、ハッシュ関数ｈとして任意のハッシュ関数を用いることができる。
【０２１０】
ハッシュ関数を利用することにより、異なる二つの（ｋ１＿ｆ，ｋ２＿ｎ，ｋ３）の組から同じ共通鍵ｋが生成される確率を、無視しても問題がない程度まで低くすることができる。また、共通鍵ｋの値の分布が一様かつランダムになることが期待される。つまり、連続する二つのフレームに対する共通鍵ｋの値が大きく異なることが期待される。よって、暗号化フレームが傍受された場合でも、共通鍵ｋを推測することは非常に難しい。さらに、高速な演算が可能な汎用のハッシュ関数を利用することができるため、実装が容易である。
【０２１１】
共通鍵ｋを生成する第二の方法は、配列を用いる方法である。図１６はこの方法を説明する図であり、この方法では、上記のステップ（ｓ５）、（ｓ６）、（ｒ５）、（ｒ６）はそれぞれ以下のステップ（ｓ５‐２）、（ｓ６‐２）、（ｒ５‐２）、（ｒ６‐２）で置き換えられる。
（ｓ５‐２）暗号処理モジュール１０４内の共通鍵生成部１４が、ステップ（ｓ４）で読み取ったシーケンス番号ｋ２＿ｓに基づいて、マスター鍵配列Ｃからマスター鍵ｋ３を読み出す。
（ｓ６‐２）暗号処理モジュール１０４内の共通鍵生成部１４が、
ｋ＝ｋ３　ＸＯＲ　（ｋ１＋ｋ２＿ｓ）
なる共通鍵ｋを生成する（「ＸＯＲ」は排他的論理和を表す演算子である）。
（ｒ５‐２）暗号処理モジュール１０４内の共通鍵生成部１４が、ステップ（ｒ３）で読み取ったシーケンス番号ｋ２＿ｒに基づいて、マスター鍵配列Ｃからマスター鍵ｋ３を読み出す。
（ｒ６‐２）暗号処理モジュール１０４内の共通鍵生成部１４が、
ｋ＝ｋ３　ＸＯＲ　（ｋ１＋ｋ２＿ｒ）
なる共通鍵ｋを生成する。
【０２１２】
つまり、この第二の方法では式（１）に次の式（４）を適用する。
ｆ（ｘ１，ｘ２，ｘ３）≡ｘ３　ＸＯＲ　（ｘ１＋ｘ２）　　……（４）
図１６を参照して上記のステップについて説明する。図１５においては、事前共有鍵ｋ０から一つのマスター鍵ｋ３が生成されていたが、図１６では事前共有鍵ｋ０からＭ個の値が生成され、それらの値の配列をマスター鍵配列Ｃとして暗号処理モジュール１０４に格納しておく。例えば、マスター鍵格納部２１にかえてマスター鍵配列格納部を設け、そこにマスター鍵配列Ｃを格納してもよい。
【０２１３】
以下、マスター鍵配列Ｃで添え字がｊの値をＣ［ｊ］と表し、各Ｃ［ｊ］の値を候補値とよぶ。つまり、マスター鍵配列ＣはＭ個の候補値Ｃ［０］～Ｃ［Ｍ－１］からなる配列であり、個々の候補値は下記の式（５）により表現することができる。
【０２１４】
Ｃ［ｊ］＝ｇ２（ｋ０，ｊ）　（０≦ｊ≦Ｍ－１）　　……（５）
ステップ（ｓ５‐２）では、例えば、シーケンス番号ｋ２＿ｓをＭで割ったときの剰余

ｊを算出し、Ｃ［ｊ］の値をマスター鍵ｋ３として読み出してもよい。ステップ（ｒ５‐２）でも同様にして、マスター鍵ｋ３を読み出すことができる。この場合、Ｍは実施形態によって予め決められた定数であることから、マスター鍵ｋ３を次のように表すことができる（ここで「ｍｏｄ」は剰余を算出する演算子である）。

【０２１５】

ｋ３＝Ｃ［ｊ］
＝Ｃ［ｋ２＿ｎ　ｍｏｄ　Ｍ］
＝ｇ２（ｋ０，ｋ２＿ｎ　ｍｏｄ　Ｍ）
＝ｇ３（ｋ０，ｋ２＿ｎ）　……（６）

もちろん、実施形態によっては別の方法を使ってｊを決定し、マスター鍵配列Ｃからマスター鍵ｋ３（＝Ｃ［ｊ］）を読み出してもよい。

【０２１６】

ステップ（ｓ５‐２）や（ｒ５‐２）では、マスター鍵ｋ３がシーケンス番号ｋ２＿ｎ（ｋ２＿ｓまたはｋ２＿ｒ）に基づいて算出されるため、連続した二つの暗号化フレームで異なるマスター鍵ｋ３が用いられ、したがって、異なる共通鍵ｋが用いられる。また、暗号化フレームを傍受されたとしても共通鍵ｋが推測困難なようにするためには、マスター鍵配列Ｃを生成する際にＣ［ｉ］とＣ［ｉ＋１］のビット列が類似しないような方法で生成し、かつＭを適度に大きな値（例えば２５６）としておくことが望ましい。

【０２１７】

この第二の方法では、関数ｆとして、ハッシュ関数よりもさらに高速に演算することが可能な、簡単な関数を利用している。すなわち、ステップ（ｓ６‐２）および（ｒ６‐２）に示したごとく、関数ｆの計算に必要なのは算術加算と排他的論理和の演算のみである。

【０２１８】

したがって、この第二の方法は、共通鍵ｋの安全性と演算速度をともに考慮した方法であり、Ｇｂｐｓ級の高速通信に好適である。

ところで、図９ＡのようにＶＬＡＮを利用する環境においては、上記の第一および第二の方法を変形した方法を採用することも可能である。例えば、図９Ａの例において、ＶＬＡＮ１１０とＶＬＡＮ１２０で同じマスター鍵ｋ３を利用してもよいが、異なるマスター鍵ｋ３、ｋ３’を利用してもよい。後者の場合、暗号化対象であるＶＬＡＮ１１０、１２０にそれぞれ対応する事前共有鍵ｋ０、ｋ０’を管理者がＬ２中継装置１０１ａに設定し、暗号処理モジュール１０４ａは事前共有鍵ｋ０からマスター鍵ｋ３を生成するとともに事前共有鍵ｋ０’からマスター鍵ｋ３’を生成する。管理者は、Ｌ２中継装置１０１ｂにも同様に事前共有鍵ｋ０、ｋ０’を設定し、暗号処理モジュール１０４ｂにマスター鍵ｋ３、ｋ３’を生成させる。以上は第一の方法を変形した方法である。第二の方法も同様にして変形することができる。すなわち、暗号処理モジュール１０４ａ、１０４ｂはそれぞれ、ＶＬＡＮ１１０、１２０に対応する二つの事前共有鍵ｋ０、ｋ０’から二組のマスター鍵配列Ｃ、Ｃ’を生成する。そして、ＶＬＡＮ１１０に対応するフレームの暗号処理ではマスター鍵配列Ｃを使い、ＶＬＡＮ１２０に対応するフレームの暗号処理ではマスター鍵配列Ｃ’を使う。

【０２１９】

次に、事前共有鍵ｋ０からマスター鍵ｋ３を生成する方法についていくつか説明する。事前共有鍵ｋ０からマスター鍵ｋ３を生成する方法が異なれば、同じ事前共有鍵ｋ０、ＭＡＣヘッダ情報ｋ１＿ｆ、シーケンス番号ｋ２＿ｎから異なる共通鍵ｋが生成される。

【０２２０】

事前共有鍵ｋ０からマスター鍵ｋ３を生成する第一の方法は、ランダムなバイト列を生成する関数ｒを用いる方法である。関数ｒには引数としてシードが与えられる。関数ｒは同じシードに対しては同じ結果を返す関数である。

【０２２１】

この第一の方法による実施形態では、Ｌ２中継装置１０１のファームウェアが一意な文

字列（以下では「ファーム文字列」とよび、符号「ｆｓ」で表す）を定義しており、暗号処理モジュール１０４（より詳細には、その内部のマスター鍵生成部２０）はファーム文字列ｆｓを参照することができるようになっている。つまり、同じファームウェアが組み込まれた複数のＬ２中継装置１０１に備えられたすべての暗号処理モジュール１０４は、同じファーム文字列ｆｓを参照することができる。ファーム文字列ｆｓは、例えばファームウェアを設計してＬ２中継装置１０１に組み込んだ製造業者しか知らないものであって、Ｌ２中継装置１０１の利用者には秘密にされる。

【０２２２】

また、本実施形態では、暗号化フレームの送信側と受信側で使われる暗号処理モジュール（例えば図９Ａの１０４ａと１０４ｂ）が同じファームウェアを搭載しており、かつ同じ関数ｒを利用可能であるものとする。

【０２２３】

関数ｒに与えるシードは、ファーム文字列ｆｓと事前共有鍵ｋ０に基づいて算出される。例えば、ファーム文字列ｆｓと事前共有鍵ｋ０を文字列として連結したものをシードとしてもよく、ファーム文字列ｆｓと事前共有鍵ｋ０のビット列から排他的論理和を演算してシードとしてもよい。つまり、以下の式（７）または（８）にしたがってマスター鍵ｋ３を生成することが可能である（ここで「＆」はビット列を連結する演算子を示す）。

【０２２４】

ｋ３＝ｇ（ｋ０）＝ｒ（ｆｓ　＆　ｋ０）　……（７）

ｋ３＝ｇ（ｋ０）＝ｒ（ｆｓ　ＸＯＲ　ｋ０）　……（８）

例えば、算出すべきマスター鍵ｋ３の長さをＮバイトと定めたとする。このとき、関数ｒが長さＮバイトの値を返す関数であれば、上記のようにしてファーム文字列ｆｓと事前共有鍵ｋ０に基づいて算出したシードを関数ｒの引数として与えれば、マスター鍵ｋ３を得ることができる。

【０２２５】

あるいは、関数ｒが長さ１バイトの値を返す関数として定義されている場合は、Ｎ個のランダムなバイト値を生成し、それらを連結してＮバイトのマスター鍵ｋ３を得てもよい。この場合、Ｎ個の異なる値（以下「インデックス値」とよぶ）を使ってＮ個のシードを生成し、それらＮ個のシードを使ってＮ個のランダムなバイト値を生成する。インデックス値は、例えば１からＮの整数でもよく、別のものでもよい。例えば、インデックス値が１からＮの整数のとき、ｊ番目のシードは、ファーム文字列ｆｓと事前共有鍵ｋ０とｊとに基づいて生成される（１≦ｊ≦Ｎ）。例えば、シードを生成するための適当な関数ｓにより、マスター鍵ｋ３は、式（９）のように表すことができる。

【０２２６】

ｋ３＝ｒ（ｓ（ｆｓ，ｋ０，１））＆
　　ｒ（ｓ（ｆｓ，ｋ０，２））＆……＆
　　ｒ（ｓ（ｆｓ，ｋ０，Ｎ））　……（９）

以上、いくつか変形例を交えながら説明したが、この第一の方法によれば、暗号化フレームの送信側と受信側で同じ事前共有鍵ｋ０を設定すると、同じマスター鍵ｋ３が生成される。マスター鍵ｋ３の生成に使われるシードは、Ｌ２中継装置１０１の利用者に対して秘密にされるファーム文字列ｆｓと、管理者しか知らない事前共有鍵ｋ０とに基づいて算出される。よって、たとえ関数ｒとして汎用のライブラリ関数を利用したとしても、外部からマスター鍵ｋ３を推測することは非常に困難であり、安全にマスター鍵ｋ３を生成することができる。

【０２２７】

事前共有鍵ｋ０からマスター鍵ｋ３を生成する第二の方法はハッシュ関数ｈを用いる方法である。ハッシュ関数ｈは、同じ引数に対しては常に同じハッシュ値を算出する関数である。

【０２２８】

この第二の方法では、関数ｒのかわりにハッシュ関数ｈを用いる点以外は、第一の方法

と同様である。第二の方法では、ハッシュ関数ｈの引数はファーム文字列ｆｓと事前共有鍵ｋ０に基づいて算出される値であり、その結果得られるハッシュ値がマスター鍵ｋ３である。例えば、式（１０）または（１１）によってマスター鍵ｋ３を生成してもよい。

【０２２９】

ｋ３＝ｇ（ｋ０）＝ｈ（ｆｓ　＆　ｋ０）　　……（１０）

ｋ３＝ｇ（ｋ０）＝ｈ（ｆｓ　ＸＯＲ　ｋ０）　　……（１１）

第二の方法では、ハッシュ関数を使うのでマスター鍵ｋ３のビット配列には規則性がない。また、マスター鍵ｋ３はファーム文字列ｆｓと事前共有鍵ｋ０とに基づいて算出される。したがって、たとえハッシュ関数ｈとして汎用のライブラリ関数（例えばＭＤ５やＳＨＡ‐１など）を利用したとしても、外部からマスター鍵ｋ３を推測することは非常に困難であり、安全にマスター鍵ｋ３を生成することができる。

【０２３０】

ところで、事前共有鍵ｋ０からマスター鍵ｋ３を生成する上記の第一および第二の方法は、変更を加えることによって、図１０のようにマスター鍵配列Ｃを利用する実施形態にも適用することができる。

【０２３１】

事前共有鍵ｋ０からマスター鍵配列Ｃを生成する第一の方法は、事前共有鍵ｋ０からマスター鍵ｋ３を生成する第一の方法と類似の方法である。ただし、マスター鍵ｋ３の長さをＮバイトと定めた場合に、Ｎバイトの長さをもつ一つのマスター鍵ｋ３を生成するのではなく、それぞれがＮバイトの長さをもつＭ個の候補値を生成し、それらをＣ［０］～Ｃ［Ｍ－１］として格納する点で異なる。

【０２３２】

例えば、関数ｒが長さＮバイトの値を返す関数として定義されている場合は、Ｍ個のランダムな値を生成して候補値として格納してもよい。この場合、上記式（５）は以下のように書き換えられる。

【０２３３】

Ｃ［ｊ］＝ｇ２（ｋ０，ｊ）

＝ｒ（ｓ（ｆｓ，ｋ０，ｊ））　（０≦ｊ≦Ｍ－１）　　……（１２）

あるいは、関数ｒが長さ１バイトの値を返す関数として定義されている場合は、Ｎ×Ｍ個のランダムなバイト値を生成し、Ｎ個ずつを連結してＮバイトの長さをもつＭ個の候補値とし、それぞれをＣ［０］～Ｃ［Ｍ－１］として格納してもよい。この場合、Ｎ×Ｍ個のインデックス値を使ってＮ×Ｍ個のシードを生成し、それらのシードを関数ｒの引数とする。例えば、インデックス値として１～（Ｎ×Ｍ）の整数を使う場合、上記式（５）は以下のように書き換えられる。

【０２３４】

Ｃ［ｊ］＝ｇ２（ｋ０，ｊ）

＝ｒ（ｓ（ｆｓ，ｋ０，Ｎ×ｊ＋１））＆

ｒ（ｓ（ｆｓ，ｋ０，Ｎ×ｊ＋２））＆……＆

ｒ（ｓ（ｆｓ，ｋ０，Ｎ×ｊ＋Ｎ））　　……（１３）

この方法によれば、関数ｒとして汎用のライブラリ関数を利用したとしても、外部からマスター鍵配列Ｃの内容を推測することは非常に困難である。したがって、マスター鍵配列Ｃの中から選択されるマスター鍵ｋ３の安全性も保たれる。

【０２３５】

事前共有鍵ｋ０からマスター鍵配列Ｃを生成する第二の方法は、事前共有鍵ｋ０からマスター鍵ｋ３を生成する第二の方法と類似の方法である。ただし、一つのマスター鍵ｋ３を生成するのではなく、Ｍ個の候補値を生成し、それらをＣ［０］～Ｃ［Ｍ－１］として格納する点で異なる。

【０２３６】

この方法では、Ｍ個の候補値を生成するためにＭ個のインデックス値を使う。例えば、インデックス値が１からＭの整数のとき、ｊ番目の候補値、すなわちＣ［ｊ－１］は、フ

ァーム文字列ｆｓと事前共有鍵ｋ０とｊとに基づいて算出した値をハッシュ関数ｈの引数として得たハッシュ値である（１≦ｊ≦Ｍ）。例えば、式（５）を式（１４）または（１５）で置き換えてマスター鍵配列Ｃを生成してもよく、それ以外の方法でマスター鍵配列Ｃを生成してもよい。

【０２３７】

Ｃ［ｊ－１］＝ｇ２（ｋ０，ｊ－１）
＝ｈ（ｆｓ　＆　ｋ０　＆　（ｊ－１））　……（１４）
Ｃ［ｊ－１］＝ｇ２（ｋ０，ｊ－１）
＝ｈ（ｆｓ　ＸＯＲ　ｋ０　ＸＯＲ　（ｊ－１））　……（１５）

この方法によれば、ハッシュ関数ｈとして汎用のライブラリ関数を利用したとしても、外部からマスター鍵配列Ｃの内容を推測することは非常に困難である。したがって、マスター鍵配列Ｃの中から選択されるマスター鍵ｋ３の安全性も保たれる。また、ハッシュ関数を用いているため、Ｃ［０］～Ｃ［Ｍ－１］に格納されたそれぞれの候補値はビット配置に規則性がない。したがって、暗号化フレームを傍受したとしてもマスター鍵ｋ３を推測することは困難であり、マスター鍵ｋ３の安全性が保たれている。

【０２３８】

次に、図１７を参照しながら、フレームの分割と再構成について説明する。Ｌ２中継装置１０１は、好ましい実施形態において、暗号化フレーム１７０を分割し、分割された複数のフレームからもとの一つのフレームを再構成する機能を有している。以下では、この機能を「フラグメンテーション機能」とよび、分割された暗号化フレーム１７０を「フラグメントフレーム」とよぶ。図１７はフラグメンテーション機能を実現するための暗号ヘッダ１７１の形式を説明する図である。

【０２３９】

前述のとおり一般に、イーサネットの最大フレーム長は１５１８バイトという仕様であり、ＩＥＥＥ８０２.１Ｑ（ＶＬＡＮ）タグフレームの最大フレーム長は１５２２バイトという仕様である。また、一般に、暗号化したデータは平文データよりもデータサイズが大きくなる。さらに、暗号化フレーム１７０は暗号ヘッダ１７１を含む。よって、フレーム１５０やタグつきフレーム１６０のデータ部１５３を暗号化した場合、暗号化フレーム１７０のサイズが、上記の最大フレーム長を超えることがありうる。

【０２４０】

市販の多くのレイヤ２中継装置は、最大フレーム長を１５１８バイトや１５２２バイトよりも大きく設定することができる。よって、Ｌ２中継装置１０１と従来の中継装置とを混在させたネットワークにおいて、従来の中継装置の設定を変えることによって、１５２２バイトよりも長い暗号化フレーム１７０の送受信が可能となる。例えば図９Ａにおいて、１５２２バイトよりも長い暗号化フレーム１７０をＬ２中継装置１０１ａからＬ２中継装置１０１ｂへ送信する際に、コアＬ２／Ｌ３スイッチ１４１で最大フレーム長が適切に設定されていれば、この暗号化フレーム１７０はコアＬ２／Ｌ３スイッチ１４１を経由してＬ２中継装置１０１ｂに届く。

【０２４１】

したがって、例えばある会社が自社のオフィス用のＬＡＮとして独自に構築したネットワークなど、中継装置の設定を任意に変えることができる場合には、Ｌ２中継装置１０１の利用が問題になることは少ない。しかし、通信キャリア事業者が提供するイーサネット網を利用している場合など、利用者が好きなように中継装置の設定を変えることができない場合もある。その場合、Ｌ２中継装置１０１を利用しようとすると、最大フレーム長の制限から、暗号化フレーム１７０が送信できなくなることがありうる。

【０２４２】

そこで、Ｌ２中継装置１０１は、フラグメンテーション機能を有することが望ましい。図１７の実施形態では、Ｌ２中継装置１０１がフラグメンテーション機能を具備しており、暗号ヘッダ１７１もそれに合わせた形式となっている。フラグメンテーション機能を備えたＬ２中継装置１０１を使えば、ネットワークの経路上に従来の中継装置がある場合で

も、その中継装置で規定された最大フレーム長よりも長い暗号化フレーム１７０を送受信することができる。

【０２４３】

フラグメンテーション機能を実現するために、具体的には暗号処理モジュール１０４は以下のことを行う。第一に、暗号化した結果サイズが増加した暗号化フレーム１７０を、複数のフラグメントフレームに分割する。第二に、受信したフレームがフラグメントフレームなのか、分割されていない暗号化フレーム１７０なのかを判定する。第三に、フラグメントフレームだと判定された場合には、すべてのフラグメントフレームを受信した後、一つの暗号化フレーム１７０に復元し、復元した暗号化フレーム１７０を復号化する。

【０２４４】

図１７と図１１の暗号ヘッダ１７１を比較すると、図１７では予約フィールド１７１３の値が０ｘ０１または０ｘ０２と指定されており、２バイトのＩＤ（Identification）７１５と２バイトのフラグメントオフセット７１６の二つのフィールドが追加されている点が相違点である。

【０２４５】

本実施形態では、予約フィールド１７１３の値が０ｘ０１または０ｘ０２の場合は暗号ヘッダ１７１が図１７のように１６バイトに拡張されることを意味し、予約フィールド１７１３の値が０ｘ００の場合は暗号ヘッダ１７１が図１１のように１２バイトであることを意味する。したがって、暗号処理モジュール１０４は、受信した暗号化フレームの予約フィールド１７１３の値によって暗号ヘッダ１７１の範囲を判定することができる。

【０２４６】

分割されていない暗号化フレーム１７０において予約フィールド１７１３の値は０ｘ００である。一つの暗号化フレーム１７０をｎ個のフラグメントフレームに分割した場合、予約フィールド１７１３の値は、１番目から（ｎ－１）番目までのフラグメントフレームでは０ｘ０１であり、ｎ番目のフラグメントフレームでは０ｘ０２である。

【０２４７】

ＩＤ１７１５は、分割する前の暗号化フレーム１７０ごとに一つ割り当てられる識別番号を示すフィールドである。本実施形態においてはランダムな値を生成してＩＤ１７１５に利用する。一つの暗号化フレーム１７０をｎ個のフラグメントフレームに分割した場合、ＩＤ１７１５の値はそれらｎ個のフラグメントフレームで同一である。

【０２４８】

フラグメントオフセット１７１６は、そのフラグメントフレームが先頭から何バイト目に位置するのかを示す値が入る。

次に、このような暗号ヘッダ１７１を使ってフラグメンテーション機能を実現するための暗号処理モジュール１０４の動作について説明する。

【０２４９】

暗号処理モジュール１０４は、暗号化を行う際に以下の動作を行う。まず、暗号化フレーム１７０のデータ長が最大フレーム長（通常のイーサネットでは１５１８バイト、ＶＬＡＮ環境においては１５２２バイト）を超えるか否かを判定する。最大フレーム長を超えていたら、暗号化フレーム１７０を複数のフラグメントフレームに分割する。その際、一つのランダムな値を生成し、その値をそれぞれのフラグメントフレームのＩＤ１７１５にコピーする。また、各フラグメントフレームに対して、フラグメントオフセット１７１６、ＩＣＶ１７３、ＦＣＳ１５４の値をそれぞれ計算する。

【０２５０】

暗号処理モジュール１０４は、暗号ヘッダ１７１を含むフレームを受信したら、以下の動作を行う。まず、予約フィールド１７１３の値を調べる。この値が０ｘ００の場合、分割されていない暗号化フレームを受信したと判断し、その暗号化フレームを復号化する。予約フィールド１７１３の値が０ｘ０１の場合、ｎ個に分割されたフラグメントフレームのうち、１～（ｎ－１）番目のいずれかのフラグメントフレームを受信したと判断し、そのフラグメントフレームをの内容を一時的にバッファに格納する。予約フィールド１７１

３の値が０ｘ０２の場合、ｎ個に分割されたフラグメントフレームのうちｎ番目のフラグメントフレームを受信したと判断し、バッファに格納されている１～（ｎ－１）番目のフラグメントフレームとあわせてもとの暗号化フレームを再構成し、再構成した暗号化フレームを復号化する。なお、再構成に際しては、ｎ個のフラグメントフレームでＩＤ１７１５が同じ値か否か、フラグメントオフセット１７１６の値と矛盾なく再構成可能か否かを確認しながら再構成を行う。また、通信路の状態によっては、すべてのフラグメントフレームを受信することができないかもしれないので、所定の時間以内にすべてのフラグメントフレームが揃って再構成を行うことができなければ、バッファをクリアする。

【０２５１】

次に、ＩＰｓｅｃに本発明を適用する場合について図１８～図２７を参照しながら説明する。なお、共通鍵を生成する基本的な原理はレイヤ２の通信を暗号化する場合と同様なので、適宜説明を省略する。

【０２５２】

図１８は、本発明の共通鍵生成装置を備えた中継装置を含むネットワーク上で行われる暗号化通信およびＩＰパケットの形式を示す図である。図１８では、ＩＰｓｅｃによってＩＰパケットを暗号化するのに利用するために、本発明による共通鍵生成装置１ａ、１ｂが、レイヤ３の中継装置であるルータ２０１ａ、２０１ｂの一部として実装されている。本実施形態では、既存のＩＰｓｅｃの仕組みの多くの部分をそのまま利用している。

【０２５３】

図１８の説明をする前にＩＰとＩＰｓｅｃについて簡単に説明する。

ＩＰはレイヤ３の代表的なプロトコルであり、トランスポート層（レイヤ４）のプロトコルであるＴＣＰ（Transmission Control Protocol）とあわせてインターネットで広く利用されている。ＩＰなどのレイヤ３のプロトコルによるレイヤ３通信において用いられる中継装置には、Ｌ３（レイヤ３）スイッチやルータがある。レイヤ３通信では、データは「パケット」（データグラムともよばれる）という単位で送受信される。

【０２５４】

なお、ＩＰパケット２５０を物理媒体で送信するには、カプセル化してフレームにする必要がある。つまり、ＩＰパケット２５０の先頭にフレームヘッダとして、図１０の送信先ＭＡＣアドレス１５１、送信元ＭＡＣアドレス１５２、および、データ部１５３のうちの長さ／タイプを付加し（場合によってはＬＬＣヘッダやＳＮＡＰヘッダも付加し）、ＩＰパケット２５０の最後にフレームトレイラとして図１０のＦＣＳ１５４を付加する必要がある。よって、フレーム１５０のデータ部１５３（正確には、そのうち長さ／タイプなどを除いた部分）の具体例は、例えばＩＰパケット２５０である。しかし図１８～図２７ではレイヤ３通信に焦点を当てているので、カプセル化する前のＩＰパケット２５０に注目して説明する。

【０２５５】

ＩＰパケット２５０は、ＩＰヘッダ２５１と、送信したいデータであるＩＰデータ２５２からなる。ＩＰヘッダ２５１の形式は図２３とあわせて後述する。

ＩＰパケット２５０は、ルータ等が「ルーティング」とよばれる処理を行うことによってネットワーク内を転送され、送信元から送信先へ送信される。すなわち、ルーティング処理によって送信経路が決定され、その経路にしたがってＩＰパケットが送信される。

【０２５６】

ＩＰｓｅｃはＩＰパケット２５０を安全に送受信するための技術であり、暗号化、認証、完全性（インテグリティ、整合性ともよばれる）チェック、鍵交換などの諸機能を備えている。そのため、ＶＰＮ（Virtual Private Network）などに利用されている。上述のとおりＩＰｓｅｃでは共通鍵暗号方式を採用しているので、暗号化側と復号化側が予め共通鍵を共有している必要がある。そのような共通鍵の共有を安全に実現するためのプロトコルが前述のＩＫＥである。

【０２５７】

一方で、ＩＰｓｅｃの規格は複数のプロトコルの集まりであるから、ＩＫＥによる鍵交

換とリキーを本発明の利用に置き換え、残りの仕組みは変えずにそのまま利用して、ＩＰパケット２５０を安全に送受信することが可能である。図１８～図２７はそのような実施形態を示している。図１８～図２７は、鍵交換を行うことなく、ＩＰパケット２５０ごとに実質的に異なる共通鍵を使って暗号化をする仕組みを説明する図である。

【０２５８】

ところで、ＩＰｓｅｃによる暗号化通信には、トンネルモードとトランスポートモードという二つのモードがあり、モードによって暗号化の対象範囲が異なる。トンネルモードは、元のＩＰパケット２５０のＩＰヘッダ２５１も含めて暗号化するので、ネットワーク間での暗号化通信に適し、ＶＰＮでよく利用されている。トランスポートモードは元のＩＰパケット２５０のＩＰデータ２５２のみを暗号化するので、端末間の暗号化通信に適する。

【０２５９】

また、モードの違いは、ＩＰｓｅｃに本発明を適用する際に、暗号化ＩＰパケットのどの部分の情報を利用して共通鍵ｋの生成に利用するのかという点にも関連するが、詳しくは後述する。

【０２６０】

ただし、いずれのモードにおいても、暗号化によって最終的に生成されるものはＩＰパケットの形式を備えている（以下「暗号化ＩＰパケット」とよぶことにする）。つまり、モードによって暗号化の対象範囲が異なるが、その対象範囲を暗号化することにより得られるデータに適宜ヘッダ等を付加してＥＳＰ（Encapsulating Security Payload；カプセル化セキュリティペイロード）パケット４００とし（詳しくは後述）、そのＥＳＰパケット４００の前にＩＰヘッダ（２６１または２５１）をつけて、最終的にはＩＰパケットの形式を備えるデータを生成する。つまり、暗号化ＩＰパケット（２６０または２７０）においては、ＥＳＰパケット４００がＩＰパケット２５０におけるＩＰデータ２５２に相当する。

【０２６１】

また、いずれのモードであっても、例えばＰＣ４ａがＰＣ４ｄにＩＰパケット２５０を送信する場合、ＰＣ４ａ、ネットワーク３ａ、ルータ２０１ａ、ネットワーク３ｂ、ルータ２０１ｂ、ネットワーク３ｃ、ＰＣ４ｄからなる通信路によりＩＰパケット２５０が送信され、その通信路のうちルータ２０１ａと２０１ｂの間で暗号化通信が行われる点は同じである。つまり、ＩＰパケット２５０がその通信路上のルータ２０１ａにおいて暗号化されて暗号化ＩＰパケット（２６０または２７０）となり、それがルータ２０１ｂにおいて復号化されて復号化ＩＰパケット２８０となる。

【０２６２】

トンネルモードの暗号化ＩＰパケット２６０は、具体的には、図１８に示したように、新たなＩＰヘッダ２６１とＥＳＰパケット４００からなる。ＥＳＰパケット４００は、元のＩＰパケットの全体（ＩＰヘッダ２５１とＩＰデータ２５２の両方）を暗号化し、その前にＥＳＰヘッダ２６２を付加し、後ろにＥＳＰトレイラ２６５と認証データ２６６を付加したものである。

【０２６３】

図２３に示すように、ＩＰヘッダ２５１は、ＩＰパケット２５０の送信先ＩＰアドレス３１２と送信元ＩＰアドレス３１１を含む。よって、トンネルモードでは送信先と受信先も秘密にされる。

【０２６４】

例えば、図１８でＰＣ４ａがＰＣ４ｄにＩＰパケット２５０を送信する場合、ＩＰヘッダ２５１はＰＣ４ａとＰＣ４ｄのＩＰアドレスを含むが、暗号化ＩＰパケット２６０内では暗号化されたＩＰヘッダ２６３となるため、ＰＣ４ａとＰＣ４ｄのＩＰアドレスは秘密にされる。一方、新たに先頭に付加されるＩＰヘッダ２６１は、送信先ＩＰアドレスとしてルータ２０１ｂのＩＰアドレスを含み、送信元ＩＰアドレスとしてルータ２０１ａのＩＰアドレスを含む。このＩＰヘッダ２６１はクリアテキストの状態なので、暗号化ＩＰパ

ケット２６０を傍受すれば読み取れる。

【０２６５】

トランスポートモードの暗号化ＩＰパケット２７０では、元のＩＰパケット２５０のうちのＩＰヘッダ２５１を暗号化せずにそのまま用いており、そこに含まれる送信先ＩＰアドレスと受信先ＩＰアドレス（例えばＰＣ４ａとＰＣ４ｄのＩＰアドレス）はクリアテキストの状態である。暗号化ＩＰパケット２７０は、そのＩＰヘッダ２５１とＥＳＰパケット４００からなり、ＥＳＰパケット４００は、暗号化されたＩＰデータ２６４（ＩＰデータ２５２を暗号化したもの）の前にＥＳＰヘッダ２６２を付加し、後ろにＥＳＰトレイラ２６５と認証データ２６６を付加したものである。

【０２６６】

図４の説明において、共通鍵生成装置１への入力データはヘッダ部とペイロード部を有すると述べたが、図１８との対応関係は次のとおりである。ＩＰパケット２５０では、ＩＰヘッダ２５１がヘッダ部に相当し、ＩＰデータ２５２がペイロード部に相当する。トンネルモードの暗号化ＩＰパケット２６０では、ＩＰヘッダ２６１とＥＳＰヘッダ２６２がヘッダ部に相当し、暗号化されたＩＰヘッダ２６３と暗号化されたＩＰデータ２６４がペイロード部に相当する。トランスポートモードの暗号化ＩＰパケット２７０では、ＩＰヘッダ２５１とＥＳＰヘッダ２６２がヘッダ部に相当し、暗号化されたＩＰデータ２６４がペイロード部に相当する。

【０２６７】

つまり、共通鍵生成装置１への入力データにおけるヘッダ部とペイロード部の区切りは、ＩＰパケットとしての形式における区切りと必ずしも一致するわけではない。共通鍵生成装置１への入力データは、「送信対象の情報がペイロード部であり、送信のために必要な情報であってクリアテキストの状態の情報がヘッダ部である」という一般的な観点から見て、ヘッダ部とペイロード部を有するものであればよい。よって、暗号化ＩＰパケット（２６０と２７０）では、暗号化された部分がペイロード部に相当し（暗号化される理由は送信対象の情報だからである）、ペイロード部よりも前にあってクリアテキストの状態の部分がヘッダ部に相当する。

【０２６８】

また、図１８でいずれのモードを使う場合でも、共通鍵ｋを生成するのに、図３における送信先・送信元情報ｋ１と鍵素材ｋ２とマスター鍵ｋ３に相当する情報を利用している。それらの情報の詳細は後述するが、暗号化や復号化の対象であるＩＰパケットに含まれる情報と、共通鍵生成装置１ａおよび１ｂが格納している情報（または格納している情報から生成する情報）とが、共通鍵ｋの生成に使われるという点は、図１５や図１６の例と共通である。

【０２６９】

次に図１９を参照して、本発明を適用したルータ２０１の構成を説明する。

ルータ２０１は、ＩＰパケット（２５０、２６０、２７０）を送受信する複数のポート２０３ａ～２０３ｄを有する。ルータ２０１はさらに、ＩＰパケットを送受信するためのインターフェイスにより各ポート２０３ａ～２０３ｄと接続されているパケット中継処理部２０２と、ルーティングテーブル２０４と、セキュリティポリシーデータベース２０５と、ＴＣＧ対応チップ２０６と、ＣＰＵ２０７とを有し、これらが内部バス２０８により接続されている。

【０２７０】

パケット中継処理部２０２は、ポート２０３ａ～２０３ｄのいずれかから受信したＩＰパケットの送信先を決定し、そのＩＰパケットを中継するためにポート２０３ａ～２０３ｄのいずれかを介してそのパケットを送信する。例えば、図１８において、ＰＣ４ａからＰＣ４ｄへ送信されるＩＰパケットを、ルータ２０１ａはルータ２０１ｂに中継し、ルータ２０１ｂはＰＣ４ｄに中継する。このように各ルータ２０１ａと２０１ｂが適切な中継先を決定してＩＰパケットを中継するのがルーティング処理である。

【０２７１】

そして、パケット中継処理部２０２がルーティング処理を行う際に参照するテーブルがルーティングテーブル２０４である。ルーティングテーブル２０４には、受信したＩＰパケットの宛先アドレスに基づいて、そのＩＰパケットの中継先を決定するための情報が格納されている。

【０２７２】

また、ルータ２０１は、本発明によって共通鍵ｋを生成し、その共通鍵ｋをＩＰｓｅｃによる暗号化通信に利用するための装置であるから、パケット中継処理部２０２は共通鍵ｋを生成する機能とＩＰｓｅｃに関連する諸処理を行う機能とを有している。例えば、ＩＰｓｅｃは、暗号化を行わずにＡＨ（Authentication Header；認証ヘッダ）による認証機能のみを利用することも可能なように設計されており、また、アンチリプレイ機能（パケットを傍受して再生するリプレイ攻撃に対抗するため、同じパケットを受信したら破棄する機能）も提供している。本実施形態では、パケット中継処理部２０２は、これらのＩＰｓｅｃに関連する諸処理（以後「ＩＰｓｅｃ処理」とよぶ）も行う。

【０２７３】

セキュリティポリシーデータベース２０５は、パケット中継処理部２０２が参照するデータベースであり、どのようなＩＰパケットに対してどのような処理を行うかを定めたセキュリティポリシーが格納されている。パケット中継処理部２０２は、セキュリティポリシーにもとづき、受信したＩＰパケットを破棄するか、ＩＰｓｅｃ処理を行わずに単純に中継するか、ＩＰｓｅｃ処理を行うか、を決定する。その結果、ＩＰｓｅｃ処理を行うことを決定すると、パケット中継処理部２０２は、共通鍵ｋの生成、暗号化または復号化、必要に応じたヘッダの付加等を行い、ＩＰパケットの中継先を決定し、ポート２０３ａ～２０３ｄのいずれかを介してＩＰパケットを送信する。

【０２７４】

ＴＣＧ対応チップ２０６とＣＰＵ２０７は、図６のＴＣＧ対応チップ１０５およびＣＰＵ１０６と同様である。

パケット中継処理部２０２は、ハードウェア、ソフトウェア、ファームウェア、又はそれらの組み合わせによって実現することができる。パケット中継処理部２０２を実現するハードウェアの一部としてＣＰＵ２０７を利用してもよい。また、ルーティングテーブル２０４およびセキュリティポリシーデータベース２０５を実現するハードウェアは、例えば、書き換え可能な不揮発性メモリや磁気ディスクである。

【０２７５】

図２０は、図１９と図４の関係を説明する機能ブロック構成図である。図２０の構成は図７と共通部分が多いので、適宜説明を省略する。矢印につけられた符号も図７と同様だが、違いは、図２０では符号「ｆ」のかわりに符号「ｐ」を用いて、ＩＰパケットがその矢印の方向に送られることを表す点である。なお、本実施形態では、後述するように、送信先・送信元情報ｋ１および鍵素材ｋ２に相当する具体的な情報が、モードによっても異なり、第一の局面か第二の局面かによっても異なる。図２０では、そのような細かい違いによらない共通点を説明するために「ｋ１」や「ｋ２」などの総称的な符号を用いている。符号のない矢印は制御の流れを表す。

【０２７６】

また、パケット中継処理部２０２がセキュリティポリシーデータベース２０５を参照した結果、ＩＰパケットを破棄する場合やＩＰｓｅｃ処理を行わない場合は、本発明とは直接関係がない。よって、図２０には、ＩＰｓｅｃ処理を行う場合（つまり、暗号化または復号化を行うために共通鍵ｋを生成する必要がある場合）に関連する構成要素のみを示した。

【０２７７】

図２０の共通鍵生成装置１ｄは、図１９におけるパケット中継処理部２０２とＴＣＧ対応チップ２０６の一部に対応する。共通鍵生成装置１ｄは、図４の共通鍵生成装置１と同様に、受付部１１、鍵素材格納部１２、鍵素材読み取り部１３、共通鍵生成部１４を含む。

【０２７８】
図１９のルータ２０１において、ルーティング処理およびＩＰｓｅｃ処理を行うのはパケット中継処理部２０２である。パケット中継処理部２０２の中でも、セキュリティポリシーデータベース２０５を参照してＩＰｓｅｃ処理の要否を判定し、その判定にしたがって暗号化または復号化を行うブロックを、図２０ではＩＰｓｅｃ処理部２２として示してある。より詳細には、ＩＰｓｅｃ処理部２２は判定部１５、暗号化部１６、復号化部１７を備える。
【０２７９】
上記のとおり、パケット中継処理部２０２は、ＩＰパケットの送受信用インターフェイスにより複数のポート（図１９ではポート２０３ａ～２０３ｄ、図２０ではそのうちポート２０３ａと２０３ｂのみを図示）と接続されている。受付部１１はそのインターフェイス処理を行い、受信したＩＰパケット（暗号化されている場合と暗号化されていない場合の両方がある）をＩＰｓｅｃ処理部２２に送る。
【０２８０】
ＩＰｓｅｃ処理部２２において、判定部１５がＩＰｓｅｃ処理の要否を判定するが、この判定は、共通鍵ｋの生成の要否の判定でもある。図２０では、次の四つの局面のいずれであるかという判定を判定部１５が行う。
【０２８１】
・第一の局面であり、暗号化のために共通鍵ｋを生成する必要がある。
・第二の局面であり、復号化のために共通鍵ｋを生成する必要がある。
・第三の局面であり、ＩＰｓｅｃ処理を行わずにＩＰパケットを中継すればよい。
【０２８２】
・第四の局面であり、受信したＩＰパケットを破棄すべきである。
第一または第二の局面では、ＩＰｓｅｃ処理部２２が鍵素材読み取り部１３や共通鍵生成部１４に指示を与えて共通鍵ｋを生成させる。その際、共通鍵ｋの生成に必要な送信先・送信元情報ｋ１を共通鍵生成部１４に与える。共通鍵ｋの生成に関する鍵素材格納部１２、鍵素材読み取り部１３、共通鍵生成部１４の動作は図４や図７と同様であり、生成された共通鍵ｋは共通鍵生成部１４からＩＰｓｅｃ処理部２２に送られる。
【０２８３】
第一の局面では、受付部１１を介して受信したＩＰパケットを、ＩＰｓｅｃ処理部２２内の暗号化部１６が、共通鍵ｋを使って暗号化し、出力部１９を介して暗号化ＩＰパケットをいずれかのポートに出力する。第二の局面では、受付部１１を介して受信した暗号化ＩＰパケットを、ＩＰｓｅｃ処理部２２内の復号化部１７が、共通鍵ｋを使って復号化し、出力部１９を介して復号化ＩＰパケットをいずれかのポートに出力する。なお、出力部１９も受付部１１と同様に、複数のポート（２０３ａ、２０３ｂ）との間のインターフェイス処理を行う。
【０２８４】
なお、図２０では、ＴＣＧ対応チップ２０６が事前共有鍵格納部１８とマスター鍵格納部２１とを含み、予め事前共有鍵格納部１８に設定された事前共有鍵ｋ０に基づいて、マスター鍵生成部２０がマスター鍵ｋ３を生成し、マスター鍵格納部２１に格納しておく場合を示した。このようにして予め格納されたマスター鍵ｋ３は、第一または第二の局面で、共通鍵生成部１４により読み出される。また、事前共有鍵格納部１８とマスター鍵格納部２１はＴＣＧ対応チップ２０６内にあるので、事前共有鍵ｋ０やマスター鍵ｋ３が不正に読み取られることはない。
【０２８５】
別の実施形態では、共通鍵ｋを生成するたびにマスター鍵ｋ３を生成しても良く、その場合、ＩＰｓｅｃ処理部２２からマスター鍵生成部２０に、第一または第二の局面なのでマスター鍵ｋ３を生成するように指示を与える必要がある（図２０において、制御用の矢印をＩＰｓｅｃ処理部２２からマスター鍵生成部２０に追加する必要がある）。
【０２８６】

さらに別の実施形態では、図１６のようにマスター鍵配列Ｃを利用してマスター鍵ｋ３を生成してもよい。その場合、マスター鍵格納部２１は、Ｍ個の候補値からなるマスター鍵配列Ｃを格納するマスター鍵配列格納部（不図示）に置き換えられる。そして、事前共有鍵ｋ０の設定時やルータ２０１への電源投入時などに、マスター鍵配列生成部（不図示）がマスター鍵配列Ｃを生成してマスター鍵配列格納部（不図示）に格納する。第一または第二の局面では、ＩＰｓｅｃ処理部２２がマスター鍵生成部２０に命令を与えて、Ｍ個の候補値の中からマスター鍵ｋ３を選択させ、共通鍵生成部１４に出力させる。例えば、式（６）と同様の方法でマスター鍵ｋ３を選択しても良く、その場合、ＩＰｓｅｃ処理部２２が鍵素材読み取り部１３に、鍵素材ｋ２をマスター鍵生成部２０へ出力させる制御を行う。

【０２８７】

図２１と図２２はそれぞれ、暗号化されていないＩＰパケット２５０を受信したときと、暗号化ＩＰパケット（２６０、２７０）を受信したときの、ＩＰｓｅｃ処理部２２の動作を説明する図である。なお、受信したＩＰパケットの先頭のＩＰヘッダ（２５１、２６１)内のプロトコル３０９フィールドの値（図２３とあわせて後述）を参照することにより、受信したのが暗号化されていない通常のＩＰパケット２５０なのか暗号化ＩＰパケット（２６０、２７０）なのかを区別することができる。

【０２８８】

図２１において、ポート２０３ａ～２０３ｄのいずれかを介してＩＰパケット２５０を受信すると、ステップＳ１１でＩＰｓｅｃ処理部２２は、ＩＰヘッダ２５１に含まれる送信元や送信先のＩＰアドレスなどに基づいて、セキュリティポリシーデータベース２０５を検索する。検索の結果得られたセキュリティポリシーに基づいて、ＩＰｓｅｃ処理部２２は以下の三つのうちのいずれかの動作を行う。

【０２８９】

・そのＩＰパケット２５０を破棄する。
・そのＩＰパケット２５０を暗号化せずにそのまま送信する。
・そのＩＰパケット２５０は暗号化対象であると決定し、ステップＳ１２に進む。

【０２９０】

ステップＳ１２では共通鍵ｋが生成される。図２０の構成の場合、ステップＳ１２には、ＩＰｓｅｃ処理部２２のほかに、鍵素材格納部１２、鍵素材読み取り部１３、マスター鍵格納部２１、共通鍵生成部１４が関わる。

【０２９１】

共通鍵生成部１４はステップＳ１２で共通鍵ｋを生成すると、共通鍵ｋをＩＰｓｅｃ処理部２２に出力する。ＩＰｓｅｃ処理部２２内の暗号化部１６はその共通鍵ｋを使ってＩＰパケット２５０を暗号化する。トンネルモードとトランスポートモードのいずれであるかにより、暗号化を行う範囲やＥＳＰパケット４００の形式が異なることは既に述べた。ＩＰｓｅｃ処理部２２は、モードに応じた適切な暗号化ＩＰパケット（２６０または２７０）を生成し、中継先を決定して、出力部１９を介して適切なポート（２０３ａ～２０３ｄのいずれか）から出力する。

【０２９２】

図２２において、ポート２０３ａ～２０３ｄのいずれかを介して暗号化ＩＰパケット（２６０または２７０）を受信すると、ステップＳ２１でＩＰｓｅｃ処理部２２は、送信元や送信先のＩＰアドレスなどに基づいて、セキュリティポリシーデータベース２０５を検索する。検索に使う送信元や送信先のＩＰアドレスは、トンネルモードの場合はＩＰヘッダ２６１内のもの、トランスポートモードの場合はＩＰヘッダ２５１内のものである。検索の結果得られたセキュリティポリシーに基づいて、ＩＰｓｅｃ処理部２２は以下の二つのうちのいずれかの動作を行う。

【０２９３】

・その暗号化ＩＰパケット（２６０または２７０）を破棄する。
・その暗号化ＩＰパケット（２６０または２７０）は復号化対象であると決定し、ステ

ップＳ２２に進む。

【０２９４】

ステップＳ２２では共通鍵ｋが生成される。図２０の構成の場合、ステップＳ２２には、ＩＰｓｅｃ処理部２２のほかに、鍵素材読み取り部１３、マスター鍵格納部２１、共通鍵生成部１４が関わる。

【０２９５】

共通鍵生成部１４はステップＳ２２で共通鍵ｋを生成すると、共通鍵ｋをＩＰｓｅｃ処理部２２に出力する。ＩＰｓｅｃ処理部２２内の復号化部１７はその共通鍵ｋを使って暗号化ＩＰパケット（２６０または２７０）を復号化し、ＩＰパケット２５０を生成する。そして中継先を決定して、出力部１９を介して適切なポート（２０３ａ～２０３ｄのいずれか）からＩＰパケット２５０を出力する。

【０２９６】

図２３～図２５は、共通鍵ｋの生成に用いられる情報の具体例を説明する図である。これらの図について説明してから、共通鍵ｋの具体的な生成方法を説明する。

図２３はＩＰヘッダの形式を示す図である。次世代規格としてＩＰバージョン６（ＩＰｖ６）も策定されているが、現在広く使われているのはＩＰバージョン４（ＩＰｖ４）であるため、図２３ではＩＰｖ４のヘッダを示した。なお、図２３は表示の都合上、複数の行に分けて図示している。また、図１８のＩＰヘッダ２５１とＩＰヘッダ２６１の双方とも、図２３の形式である。

【０２９７】

図２３に示すとおり、ＩＰｖ４のヘッダは、４ビットのバージョン３０１、４ビットのＩＨＬ（Internet Header Length；ヘッダの長さ）３０２、８ビットのＴＯＳ（Type Of Service；サービスの種類）３０３、１６ビットの全長３０４、１６ビットのＩＤ３０５、３ビットのフラグ３０６、１３ビットのフラグメントオフセット３０７、８ビットのＴＴＬ（Time To Live；生存時間）３０８、８ビットのプロトコル３０９、１６ビットのヘッダチェックサム３１０、３２ビットの送信元ＩＰアドレス３１１、３２ビットの送信先ＩＰアドレス３１２、可変長のオプション３１３、可変長のパディング３１４、の各フィールドを含む。

【０２９８】

プロトコル３０９は、ＩＰデータ２５２内に含まれる上位層プロトコルを表す。例えば、６はＴＣＰを表し、５０はＩＰｓｅｃ　ＥＳＰを表し、５１はＩＰｓｅｃ　ＡＨを表す。よって、ＩＰｓｅｃに対応したルータは、ＩＰパケットを受信したときに、ＩＰヘッダ中のプロトコル３０９の値によって、通常のＩＰパケット２５０なのか、暗号化ＩＰパケット（２６０または２７０）なのかを判断することができる。

【０２９９】

ＩＰはフラグメンテーション機能を提供しており、ＩＤ３０５、フラグ３０６、フラグメントオフセット３０７の三つのフィールドがそのために使われる。これらのフィールドを使ったＩＰパケットの分割と再構成の仕組みは周知であり、上記のフレームのフラグメンテーション機能と類似であるため、フラグメンテーション機能についての説明は省略する。

【０３００】

ところで、ＩＰヘッダ２５１と２６１は、図２３に示すフィールドから構成される点では同じだが、内容が異なるフィールドがいくつかある。それらフィールドのうち、本発明と関連のあるものについて説明する。

【０３０１】

ＩＰヘッダ２５１と２６１で最も異なるのは、送信元ＩＰアドレス３１１および送信先ＩＰアドレス３１２である。例えば図１８でＰＣ４ａがＰＣ４ｄにＩＰパケット２５０を送信する場合、ＩＰヘッダ２５１において、送信元ＩＰアドレス３１１はＰＣ４ａのＩＰアドレスで送信先ＩＰアドレス３１２はＰＣ４ｄのＩＰアドレスである。一方、ＩＰヘッダ２６１においては、送信元ＩＰアドレス３１１はルータ２０１ａのＩＰアドレスで送信

先ＩＰアドレス３１２はルータ２０１ｂのＩＰアドレスである。

【０３０２】

さらにＩＰヘッダ２５１と２６１で異なるのは、ＩＤ３０５である。ＩＰヘッダ２５１内のＩＤ３０５は、送信元ホストで値が設定され、ＩＰパケット２５０がネットワークを中継されていく間その値が変わらない。例えば、送信元ホストが図１８のＰＣ４ａの場合、ＰＣ４ａが設定したＩＤ３０５の値は、ＩＰパケット２５０がネットワーク３ａ、ルータ２０１ａ、ネットワーク３ｂ、ルータ２０１ｂ、ネットワーク３ｃ、ＰＣ４ｄという通信路を中継されていく間、変わらない。もちろん、トンネルモードの場合は、その通信路の一部（ルータ２０１ａからルータ２０１ｂの間）において、ＩＤ３０５は暗号化された状態でＩＰヘッダ２６３内に含まれて送信されるが、データが意味する内容自体は変わらない。

【０３０３】

一方、ＩＰヘッダ２６１は、トンネルモードの場合に、上記の例では図１８のルータ２０１ａによって付加される。そのＩＰヘッダ２６１内のＩＤ３０５の値は、もとのＩＰヘッダ２５１内のＩＤ３０５の値とは独立に、ルータ２０１ａが割り当てる。その値は、トンネルモード暗号化ＩＰパケット２６０がルータ２０１ａ、ネットワーク３ｂ、ルータ２０１ｂという通信路を中継されていく間、変わらない。

【０３０４】

つまり、トランスポートモードの場合、送信元から送信先までの通信路上において常に同じ値のＩＤ３０５を、（復号化等の処理を必要とせずに）参照することが可能である。一方、トンネルモードの場合、通信路上にあるルータ２０１ｂは、ＰＣ４ａが設定したＩＤ３０５の値を、受信した暗号化ＩＰパケット２６０から直接読み取ることはできない（暗号化されているため）。ルータ２０１ｂが受信した暗号化ＩＰパケット２６０から直接読み取ることができるのは、ルータ２０１ａにより設定されたＩＰヘッダ２６１内のＩＤ３０５である。

【０３０５】

図２４は、ＥＳＰパケット４００の形式を示す図である。

ＥＳＰパケット４００は、ＥＳＰヘッダ２６２、ＥＳＰペイロード４０３、ＥＳＰトレイラ２６５、認証データ２６６からなる。

【０３０６】

ＥＳＰヘッダ２６２は、４バイトのＳＰＩ（Security Parameter Index）４０１、４バイトのシーケンス番号４０２からなる。ＩＰｓｅｃでは、送信側と受信側で使用する暗号アルゴリズムなどについて予め合意を結ぶ。その合意はＳＡ（Security Association）とよばれ、ＳＡを識別するために個々のＳＡに割り当てられる値がＳＰＩである。シーケンス番号４０２は、ＥＳＰパケット４００の生成ごとにインクリメントされるカウンタの値が割り当てられる。アンチリプレイ機能が有効に設定されている場合、リプレイされたＩＰパケットを判別して破棄するためにシーケンス番号４０２が利用されるが、アンチリプレイ機能が無効の場合でも、シーケンス番号４０２にはカウンタ値が割り当てられる。

【０３０７】

ＥＳＰペイロード４０３は、図中に「Payload Data」と示した可変長データの部分であり、暗号化されたＩＰパケットに対応する。トンネルモードの場合、ＥＳＰペイロード４０３は、元のＩＰパケットのＩＰヘッダ２５１とＩＰデータ２５２の双方を暗号化したものである。トランスポートモードの場合、ＥＳＰペイロード４０３は、元のＩＰパケットのＩＰデータ２５２を暗号化したものである。

【０３０８】

ＥＳＰトレイラは、０～２５５バイトのパディング４０４、１バイトのパディング長４０５、１バイトの次ヘッダ４０６からなる。次ヘッダ４０６は、上位層のプロトコルを表す。

【０３０９】

認証データ２６６は、ＳＰＩ４０１から次ヘッダ４０６までの部分に基づいて整合性チ

ェックのために算出される値である。
図２５は、マスター鍵ｋ３の生成について説明する図である。図２０では、ＴＣＧ対応チップ２０６内の事前共有鍵格納部１８に格納された事前共有鍵ｋ０をマスター鍵生成部２０が読み出してマスター鍵ｋ３を生成し、そのマスター鍵ｋ３をＴＣＧ対応チップ２０６内のマスター鍵格納部２１に格納している。図２５は、事前共有鍵ｋ０に基づいてマスター鍵ｋ３が生成されることと、その生成プロセスによらず、ＴＣＧ対応チップ２０６内に事前共有鍵ｋ０とマスター鍵ｋ３の両方が格納されることに焦点を当てた図である。
【０３１０】
図２０に関して説明したように、事前に、あるいは共通鍵ｋを生成するたびに、事前共有鍵ｋ０から一つのマスター鍵ｋ３を生成してもよく、予めマスター鍵配列Ｃを生成しておいて共通鍵ｋを生成するたびにその中からマスター鍵ｋ３を選択してもよい。
【０３１１】
マスター鍵ｋ３を生成する方法は、Ｌ２中継装置１０１に本発明を適用した場合と同様であり、上記の式（５）～（１５）に示した方法の中から任意の方法を採用することができる。なお、式（７）などのファーム文字列ｆｓを利用する式も、ファーム文字列ｆｓの定義を上記の説明とは別のものに変えることにより、図２５に適用可能である。上記の説明では、ファーム文字列ｆｓは、Ｌ２中継装置１０１のファームウェアにより定義される文字列であった。一方、図２５では、「ファーム文字列ｆｓとは、図２５のルータ２０１のファームウェアが定義する一意な文字列である」と定義する。また、マスター鍵生成部２０（図２５には不図示、図２０参照）がファーム文字列ｆｓを参照することができるようにルータ２０１が構成されているものとする。このようにファーム文字列ｆｓの定義を変えることにより、図２５にも上記式（７）などを適用することができる。
【０３１２】
次に、図３に示した各情報と図２３～図２５との対応関係について図２６Ａと図２６Ｂを参照して説明する。図２６Ａはトランスポートモードの場合、図２６Ｂはトンネルモードの場合を示す図である。
【０３１３】
なお、マスター鍵ｋ３については図２５で説明したとおりであり、モードによる違いはないので、以下では送信先・送信元情報ｋ１と鍵素材ｋ２についてのみ説明する。また、トランスポートモードの方が単純なので先に説明する。
【０３１４】
トランスポートモードでは、図２６Ａに示すとおり、第一および第二の局面の双方で、送信先・送信元情報ｋ１として、ＩＰヘッダ２５１内の送信元ＩＰアドレス３１１および送信先ＩＰアドレス３１２からなる情報であるＩＰヘッダ情報ｋ１＿ｐ１（図１８）を利用する。トランスポートモードでは、第一の局面（暗号化のために共通鍵ｋを生成すべき局面）の入力データであるＩＰパケット２５０と、第二の局面（復号化のために共通鍵ｋを生成すべき局面）の入力データである暗号化ＩＰパケット２７０は、ともにＩＰヘッダ２５１を含む。また、ＩＰヘッダ２５１のうち、送信元ＩＰアドレス３１１と送信先ＩＰアドレス３１２は、通信路上での書き換え対象ではない。よって、第一および第二の局面の双方において、ＩＰヘッダ２５１から同じ値のＩＰヘッダ情報ｋ１＿ｐ１を得ることができる。
【０３１５】
例えば、図１８でＰＣ４ａがＰＣ４ｄにＩＰパケット２５０を送信する場合、ルータ２０１ａがＩＰパケット２５０を受信すると、共通鍵生成装置１ａは第一の局面の動作をする。つまり、ＩＰパケット２５０のＩＰヘッダ２５１を参照し、そこに含まれるＰＣ４ａとＰＣ４ｄのＩＰアドレスからＩＰヘッダ情報ｋ１＿ｐ１を取得する。
【０３１６】
なお、ＩＰヘッダ情報ｋ１＿ｐ１は、二つのＩＰアドレスのうち少なくとも一方に基づいて取得することができる情報であれば何でもよい。例えば、二つのＩＰアドレスを表すビット列を連結してＩＰヘッダ情報ｋ１＿ｐ１としてもよく、ＩＰアドレスの一部のみを

利用してもよい。

【０３１７】

また、図１８でＰＣ４ａがＰＣ４ｄにＩＰパケット２５０を送信する例において、ルータ２０１ｂが暗号化ＩＰパケット２７０を受信すると、共通鍵生成装置１ｂは第二の局面の動作をする。つまり、暗号化ＩＰパケット２７０のＩＰヘッダ２５１を参照し、そこに含まれるＰＣ４ａとＰＣ４ｄのＩＰアドレスからＩＰヘッダ情報ｋ１＿ｐ１を取得する。共通鍵生成装置１ａと１ｂは、同じ値のＩＰヘッダ情報ｋ１＿ｐ１を取得することができる。

【０３１８】

次に、トランスポートモードにおける鍵素材ｋ２について説明する。第一の局面では共通鍵生成装置１ｄが備える鍵素材格納部１２（図２０）に格納されたシーケンス番号を利用し、第二の局面では入力データ（暗号化ＩＰパケット２７０）中に含まれるシーケンス番号を利用する点は、図１５や図１６と同様である。異なるのは、さらに別の値も組み合わせて鍵素材ｋ２として利用する点である。

【０３１９】

図２６Ａに示したとおり、第一の局面における鍵素材ｋ２は、符号「ｋ２＿ｓ」により表されるが、具体的には式（１６）により生成される。式（１６）の関数ｃは任意のものでよいが、最も簡単な例は式（１７）のとおりである。

【０３２０】

ｋ２＝ｋ２＿ｓ＝ｃ（ｋ２＿ｓ２，ｋ２＿ｒ１）　……（１６）

ｃ（ｘ１，ｘ２）≡ｘ１　＆　ｘ２　……（１７）

ここで符号「ｋ２＿ｓ２」は鍵素材格納部１２（カウンタ）に格納されたシーケンス番号を指し、符号「ｋ２＿ｒ１」は、ＩＰヘッダ２５１内のＩＤ３０５を指す（図１８参照）。つまり、第一の局面において、鍵素材格納部１２と入力データの双方から鍵素材読み取り部１３がそれぞれ読み取った情報に基づいて、鍵素材ｋ２が生成される。なお、ＩＰｓｅｃに本発明を適用する場合、鍵素材格納部１２は４バイトのカウンタであり、ＥＳＰパケット４００の生成時には、そこに格納されたシーケンス番号をＥＳＰヘッダ２６２内のシーケンス番号４０２として利用する。

【０３２１】

同様に、第二の局面における鍵素材ｋ２は、符号「ｋ２＿ｒ」により表されるが、具体的には式（１８）により生成される。

ｋ２＝ｋ２＿ｒ＝ｃ（ｋ２＿ｒ３，ｋ２＿ｒ１）　……（１８）

ここで符号「ｋ２＿ｒ３」はＥＳＰヘッダ２６２内のシーケンス番号４０２の値を指す。

【０３２２】

例えば、図１８でＰＣ４ａがＰＣ４ｄにＩＰパケット２５０を送信する場合、共通鍵生成装置１ａ内の不図示の鍵素材格納部１２に格納されたシーケンス番号ｋ２＿ｓ２が、暗号化ＩＰパケット２７０のＥＳＰヘッダ２６２内のシーケンス番号４０２として設定される。そして、その暗号化ＩＰパケット２７０を受信したルータ２０１ｂにおいて、共通鍵生成装置１ｂが備える鍵素材読み取り部１３が、ＥＳＰヘッダ２６２内のシーケンス番号４０２フィールドから、シーケンス番号ｋ２＿ｒ３を読み取る。鍵素材読み取り部１３はまた、ＩＰヘッダ２５１内のＩＤ３０５フィールドからＩＤ　ｋ２＿ｒ１を読み取り、式（１８）により鍵素材ｋ２を生成する。よって、共通鍵生成装置１ａと１ｂの双方の鍵素材読み取り部１３が、式（１６）と（１８）に示すように同じ関数ｃを用いることにより、同じ値の鍵素材ｋ２を生成することができる。

【０３２３】

次に、このように二つの情報から鍵素材ｋ２を生成する理由を説明する。

図２４に示すようにシーケンス番号４０２は３２ビット（＝４バイト）なので、2^{32}個の番号が利用可能である。フレームの暗号化を行う実施形態と同様に、ルータが１秒あたり１Ｇ個のＩＰパケット２５０を暗号化すると仮定すると、同じ番号に戻るのにかかる

時間は

$2^{32}/10^{9}$　４．３秒

である。図１１のシーケンス番号１７１４の長さが８バイトであるのに比べ、４バイトは短く、その分、同じ番号に戻るのにかかる時間も短い。この時間が短い点は、あまり好ましくない特徴である。

【０３２４】

しかしながら、実際には一つのＩＰパケット２５０は１ＫＢ程度の大きさのものが多く、１秒あたり１Ｇ個ものＩＰパケット２５０が暗号化されることは現実的にはない。例えば、１秒あたり１Ｍ個のＩＰパケット２５０を暗号化するという別の仮定で計算すれば、上記の時間は、

$2^{32}/10^{6}$　４２９５秒　１．２時間

となり、かなり長くなる。これでも図１１のシーケンス番号１７１４に関して例示的に計算した時間（約５８５年）よりは短いが、連続するＩＰパケット２５０に対して異なる共通鍵ｋを生成するという点は、共通鍵生成部１４を適当に構成することにより（周期とは関係なく）実現可能である。また、上記のようにＩＰヘッダ情報ｋ１＿ｐ１をあわせて利用すれば、シーケンス番号（ｋ２＿ｓ２、ｋ２＿ｒ３）に周期性があっても、それと同じ周期で同じ共通鍵ｋが使われることはない。したがって、多くの利用形態において、４バイトのシーケンス番号（ｋ２＿ｓ２、ｋ２＿ｒ３）でも実用上は問題ない。

【０３２５】

ただし、より強固なセキュリティが必要な場合もある。また、必要なセキュリティレベルは様々な要因を考慮して決定されるが、比較的簡単な方法でセキュリティレベルを上げられるなら、その方法を採用する場合もある。

【０３２６】

そこで、広く普及しているＥＳＰパケット４００の形式を変えることなく、簡単な方法でセキュリティレベルを上げるために、４バイトのシーケンス番号（ｋ２＿ｓ２、ｋ２＿ｒ３）に加えて、２バイトのＩＤ３０５を利用する。式（１７）を式（１６）および式（１８）に適用すると、シーケンス番号（ｋ２＿ｓ２またはｋ２＿ｒ３）とＩＤ　ｋ２＿ｒ１との連結により６バイト（＝４８ビット）の値が鍵素材ｋ２として得られる。もちろん、式（１７）以外の方法でも、４バイトのシーケンス番号と２バイトのＩＤから６バイトの鍵素材ｋ２を生成することは可能である。例えば、シーケンス番号とＩＤをそれぞれ複数のブロックに分けて、それらブロックを所定の順番に並べ替えても、結果として６バイトの値を得ることができる。

【０３２７】

このようにして生成された６バイトの鍵素材ｋ２を使う場合、例えば、１秒あたり１Ｍ個のＩＰパケット２５０を暗号化するという上記と同じ仮定で計算すると、

$2^{48}/10^{6}=2.81\times10^{8}$秒　８．９２年

となる。この時間は、実用上十分に長い周期であり、上記で計算した１．２時間に比べて遥かに長い。つまり、シーケンス番号（ｋ２＿ｓ２またはｋ２＿ｒ３）に加えてＩＤ　ｋ２＿ｒ１を利用するという比較的簡単な方法により、セキュリティレベルが大きく向上している。

【０３２８】

以上の理由により、式（１６）や（１８）のように、二つの情報から鍵素材ｋ２を生成している。

次に、トンネルモードの場合について図２６Ｂを参照して説明する。トンネルモードでは、図２６Ｂに示すとおり、第一および第二の局面の双方で、送信先・送信元情報ｋ１として、暗号化ＩＰパケット２６０の先頭に付加された（あるいはこれから付加される）ＩＰヘッダ２６１内の送信元ＩＰアドレス３１１および送信先ＩＰアドレス３１２からなる情報であるＩＰヘッダ情報ｋ１＿ｐ２を利用する。

【０３２９】

例えば、図１８でＰＣ４ａがＰＣ４ｄにＩＰパケット２５０を送信する場合、ＩＰヘッ

ダ２６１内の送信元ＩＰアドレス３１１はルータ２０１ａのＩＰアドレスであり、送信先ＩＰアドレス３１２はルータ２０１ｂのＩＰアドレスである。つまり、ＩＰヘッダ情報ｋ１＿ｐ２は、送信元（ＰＣ４ａ）と送信先（ＰＣ４ｄ）そのものから得られる情報ではない。第一の局面の動作を行う共通鍵生成装置１ａは、入力データであるＩＰパケット２５０からではなく、暗号化ＩＰパケット２６０の生成のためにこれからＩＰヘッダ２６１に設定する内容（ルータ２０１ａと２０１ｂのＩＰアドレス）に基づき、ＩＰヘッダ情報ｋ１＿ｐ２を取得する。一方、第二の局面の動作を行う共通鍵生成装置１ｂは、入力データである暗号化ＩＰパケット２６０のＩＰヘッダ２６１に基づいてＩＰヘッダ情報ｋ１＿ｐ２を取得する。

【０３３０】

なお、二つのＩＰアドレスからＩＰヘッダ情報ｋ１＿ｐ２を取得する方法は任意であることは、トランスポートモードの場合と同様である。

このように、トンネルモードにおける動作はこれまで述べてきた他の例に比べて変則的だが、それには下記の理由がある。

【０３３１】

もともと、共通鍵ｋの生成に送信先・送信元情報ｋ１を利用するのは、共通鍵ｋをよりランダムにするのに送信先・送信元情報ｋ１の利用が役立つからである。なぜ役立つかといえば、送信先と送信元の組み合わせ数は多く、どの送信先にどの送信元からいつ通信が行われるかが不規則なためである。したがって、送信先・送信元情報ｋ１としては、送信先と送信元である端末（図１８ではＰＣ４ａ～４ｆ）のアドレスに基づいた情報が好適である。

【０３３２】

しかし、トンネルモードでは暗号化ＩＰパケット２６０を復号化しないかぎり、暗号化されたＩＰヘッダ２６３に暗号化された状態で含まれている送信元と送信先のＩＰアドレスは得られず、したがって、トランスポートモードと同様のＩＰヘッダ情報ｋ１＿ｐ１は得られない。よって、暗号化ＩＰパケット２６０を復号化するための共通鍵ｋの生成にはＩＰヘッダ情報ｋ１＿ｐ１を利用することができない。そのため、トンネルモードではクリアテキストの状態であるＩＰヘッダ２６１内のＩＰヘッダ情報ｋ１＿ｐ２を、トランスポートモードにおけるＩＰヘッダ情報ｋ１＿ｐ１のかわりに、送信先・送信元情報ｋ１として利用している。

【０３３３】

次に、トンネルモードにおける鍵素材ｋ２について説明する。図２６Ａと図２６Ｂの比較から分かるとおり、トランスポートモードにおけるＩＤ　ｋ２＿ｒ１のかわりに、トンネルモードでは、ＩＰヘッダ２６１内のＩＤ３０５フィールドの値であるＩＤ　ｋ２＿ｒ２を利用する。その他の点は、トランスポートモードと同様である。つまり、トンネルモードの場合、第一と第二の局面における鍵素材ｋ２は、それぞれ式（１９）と式（２０）により表される。

【０３３４】

$$k2 = k2\_s = c(k2\_s2, k2\_r2) \quad \cdots\cdots (19)$$

$$k2 = k2\_r = c(k2\_r3, k2\_r2) \quad \cdots\cdots (20)$$

ＩＤ　ｋ２＿ｒ１のかわりにＩＤ　ｋ２＿ｒ２を利用する理由は、ＩＰヘッダ情報ｋ１＿ｐ１のかわりにＩＰヘッダ情報ｋ１＿ｐ２を利用する理由と同じである。つまり、図１８でＰＣ４ａがＰＣ４ｄにＩＰパケット２５０を送信する場合、共通鍵生成装置１ｂでは、暗号化ＩＰパケット２６０を復号化しないかぎり、暗号化されたＩＰヘッダ２６３内に暗号化された状態で含まれているＩＤ３０５を得られないためである。

【０３３５】

図２６Ａおよび図２６Ｂに示した情報を用いて共通鍵ｋを生成するには、前述の式（１）～（４）において、符号「ｋ１＿ｆ」を、符号「ｋ１＿ｐ１」または「ｋ１＿ｐ２」に置き換えた式にしたがって共通鍵生成部１４が動作すればよい。また、マスター鍵配列Ｃを利用してマスター鍵ｋ３を選択する実施形態の場合も、フレームの暗号化に本発明を利

用する場合と同様の動作を共通鍵生成部１４が行えばよい。その場合、式（１）は、トランスポートモードなら式（２１）に、トンネルモードなら式（２２）に、それぞれ書き換え可能なことは、上記の説明から明らかであろう。

【０３３６】

ｋ＝ｆ（ｋ１＿ｐ１，ｋ２，ｋ３）
＝ｋ３　ＸＯＲ　（ｋ１＿ｐ１＋ｃ（ｋ２＿ｓ２，ｋ２＿ｒ１））
＝ｋ３　ＸＯＲ　（ｋ１＿ｐ１＋ｃ（ｋ２＿ｒ３，ｋ２＿ｒ１））　……（２１）
ｋ＝ｆ（ｋ１＿ｐ２，ｋ２，ｋ３）
＝ｋ３　ＸＯＲ　（ｋ１＿ｐ２＋ｃ（ｋ２＿ｓ２，ｋ２＿ｒ２））
＝ｋ３　ＸＯＲ　（ｋ１＿ｐ２＋ｃ（ｋ２＿ｒ３，ｋ２＿ｒ２））　……（２２）

図２７は、本発明の共通鍵生成装置を備えたルータをブロードキャストに利用した例を示す図である。従来のＩＰｓｅｃは、共通鍵暗号方式であることから、送信先が複数であるマルチキャストには適していなかった。しかし、本発明をＩＰｓｅｃに適用すると（つまり本発明による共通鍵生成装置１を備えたルータを利用すると）、ＩＰｓｅｃの仕組みを使って簡単にマルチキャストを行うことができる。

【０３３７】

図２７では、マルチキャストの送信元であるＰＣ４ａが、ネットワーク３ａを介してルータ２０１ａに接続されている。マルチキャストの送信先は、ＰＣ４ｂ、４ｃ、４ｄである。ＰＣ４ｂと４ｃはネットワーク３ｃを介してルータ２０１ｂに接続されており、ＰＣ４ｄとＰＣ４ｅはネットワーク３ｄを介してルータ２０１ｃに接続されている。なお、ルータ２０１ａ、２０１ｂ、２０１ｃはいずれも、本発明による共通鍵生成装置１を含み、同じ値のマスター鍵ｋ３を記憶している。さらに、ＰＣ４ｆと４ｇがネットワーク３ｅを介して従来のルータ８に接続されている。ルータ２０１ａ、２０１ｂ、２０１ｃ、８は、互いにネットワーク３ｂを介して接続されている。

【０３３８】

ＰＣ４ａがＩＰパケットをマルチキャストにより、ＰＣ４ｂ、４ｃ、４ｄに送信する場合、このＩＰパケットは、ルータ２０１ａで暗号化され、ネットワーク３ｂを通ってルータ２０１ｂと２０１ｃに中継される。つまり、暗号化されたＩＰパケットは、ルータ２０１ａまたはネットワーク３ｂ内に存在する不図示のルータにおいてコピーされ、ルータ２０１ｂと２０１ｃの双方に送信される。ルータ２０１ｂは、暗号化されたＩＰパケットを復号化してコピーし、ＰＣ４ｂと４ｃに送信する。ルータ２０１ｃは、暗号化されたＩＰパケットを復号化してＰＣ４ｄに送信する。

【０３３９】

ここで、ルータ２０１ａ、２０１ｂ、２０１ｃはいずれも、本発明による共通鍵生成装置１を含み、同じ値のマスター鍵ｋ３を記憶していることから、ルータ２０１ａ内の共通鍵生成装置１が、マルチキャストされるＩＰパケット用の共通鍵ｋａとして生成したのと同じ値の共通鍵ｋａが、ルータ２０１ｂと２０１ｃでも生成される。また、そのマルチキャストと並行して、例えばＰＣ４ｅがマルチキャストとは無関係にＰＣ４ｃにＩＰパケットを送信する場合、そのための共通鍵ｋｂがルータ２０１ｃと２０１ｂでそれぞれ生成され、そのＩＰパケットはネットワーク３ｂ内を暗号化された状態で送られる。

【０３４０】

しかし、これらのルータ２０１ａ、２０１ｂ、２０１ｃにおいて管理されるべきなのはマスター鍵ｋ３（あるいは、その元となる事前共有鍵ｋ０）のみである。例えばルータ２０１ｃにおいて、マルチキャスト用、ルータ２０１ａとの通信用、ルータ２０１ｂとの通信用、などの複数の鍵を管理する必要はない。つまり、本発明をＩＰｓｅｃに適用すると、複雑な鍵の管理を不要としつつ、マルチキャストにも対応することができ、しかもＩＰパケットごとに異なる共通鍵により暗号化が行われる、という利点がある。

【０３４１】

なお、本発明は上記の実施形態に限られるものではなく、様々に変形可能である。以下にその例をいくつか述べる。

図１０では、タイプ等も含めたデータ部１５３を暗号化の対象としている。しかし、タイプ、ＬＬＣヘッダ、ＳＮＡＰヘッダまでをヘッダ部であると見なし、これらを暗号化の対象から除外してもよい。その場合、暗号化フレーム１７０における暗号ヘッダ１７１の位置は、図１０と同様にＴＣＩ１６２の直後でもよく、ＴＣＩ１６２の直後にタイプ等が続き、その後に暗号ヘッダ１７１が続き、その後に暗号化データ部が続くのでもよい。後者の場合は、暗号化の対象外となるヘッダ部分、暗号ヘッダ１７１、暗号化データ部という順になるという点で、図１０と同様である。

【０３４２】

上記の実施形態では、ｋ＝ｆ（ｋ１，ｋ２，ｋ３）なる共通鍵ｋを生成している。しかし、共通鍵ｋを生成するのに必須なのは鍵素材ｋ２のみである。よって、例えば、ハッシュ関数ｈを利用してｋ＝ｈ（ｋ２）などの計算により共通鍵ｋを生成してもよい。

【０３４３】

ただし、共通鍵ｋの強度という点からは送信先・送信元情報ｋ１およびマスター鍵ｋ３も利用することが望ましい。また、図１６のように計算を単純化して処理を高速化するためにも、鍵素材ｋ２以外の要素である送信先・送信元情報ｋ１およびマスター鍵ｋ３を利用することが望ましい。

【０３４４】

また、ＩＰｓｅｃに本発明を適用する場合、上記の実施形態ではＩＰヘッダ内のＩＤ３０５も共通鍵ｋの生成に利用していたが、利用しなくてもよい。逆に、ＳＰＩ４０１などの他の情報（暗号化ＩＰパケットにクリアテキストの状態で含まれ、通信路の途中で値が変更されない情報）をさらに利用してもよい。

【０３４５】

また、関数ｆは上記で例示した以外の関数でもよいことは無論である。

図１７では、フラグメントオフセット１７１６を利用する仕組みを採用しているが、図１１とは異なる形式の暗号ヘッダ１７１を採用して、フラグメンテーション機能を実現してもよい。例えば、予約フィールド１７１３とフラグメントオフセット１７１６に基づいて再構成を行うかわりに、「全部でいくつのフラグメントフレームがあるか」という情報と「このフラグメントフレームは何番目のフラグメントフレームであるか」という情報を暗号ヘッダ１７１に記録し、それらの情報に基づいて再構成を行ってもよい。

【０３４６】

上記では、レイヤ２またはレイヤ３の中継装置の一部として本発明による共通鍵生成装置を実装する例について説明した。それらの例では、図７や図２０に示したように、共通鍵生成装置が内部に暗号化部１６や復号化部１７をも含む。しかし、本発明による共通鍵生成装置１は、必ずしも図７や図２０に示したように判定部１５、暗号化部１６、復号化部１７を構成要素として含まなくてもよい。

【０３４７】

例えば、図２０において、共通鍵生成装置１ｄを、受付部１１、鍵素材格納部１２、鍵素材読み取り部１３、共通鍵生成部１４のみからなるように構成してもよい。その場合、ＩＰｓｅｃ処理部２２と共通鍵生成装置１ｄとは異なるハードウェア上に実装され、制御信号の送受信やデータの入出力のために、例えばバスにより接続される。

【０３４８】

この構成において、ＩＰｓｅｃ処理部２２は、ＩＰｓｅｃ処理が必要だと判定すると、前記接続を介して共通鍵生成装置１ｄに共通鍵ｋの生成を命令する。その際、共通鍵ｋの生成に必要な情報（例えば、どの局面であるかという情報や、送信先・送信元情報ｋ１や、第二の局面の場合の鍵素材ｋ２など）も、ＩＰｓｅｃ処理部２２から共通鍵生成装置１ｄに送られる。共通鍵生成装置１ｄは命令にしたがって共通鍵ｋを生成し、前記接続を介して共通鍵ｋをＩＰｓｅｃ処理部２２に送信する。また、第一の局面の場合には、鍵素材ｋ２の値もあわせてＩＰｓｅｃ処理部２２に送信する。ＩＰｓｅｃ処理部２２は、受信した共通鍵ｋ（および第一の局面の場合は鍵素材ｋ２）を利用してＩＰパケットの暗号化または復号化を行う。

【０３４９】
　また、本発明をＩＰｓｅｃに適用する例として、ＩＰｖ４上でのＩＰｓｅｃのみを上記では説明したが、ＩＰｖ６上のＩＰｓｅｃであっても、同様に本発明を適用することができる。
【０３５０】
　また、鍵素材格納部１２がカウンタである場合、鍵素材読み取り部１３は第一の局面において１ずつ鍵素材格納部１２をインクリメントするとして上記では説明したが、インクリメントのかわりにデクリメントでもよく、１ずつではなく所定の値であるｄずつ鍵素材格納部１２の値を変化させるのでもよい。
【０３５１】
　以上説明したことを概観すれば本発明は以下のような構成を備えるものである。
（付記１）
　共通鍵暗号方式に用いられる共通鍵を生成する共通鍵生成装置であって、
　クリアテキストの状態のヘッダ部と、ペイロード部とを有する入力データを受け付ける受付手段と、
　鍵素材を格納する鍵素材格納手段と、
　前記入力データの暗号化のために前記共通鍵を生成する第一の局面では、前記鍵素材を前記鍵素材格納手段から読み取り、前記鍵素材格納手段内の前記鍵素材を更新し、前記入力データの復号化のために前記共通鍵を生成する第二の局面では、前記ヘッダ部の所定の部分から前記鍵素材を読み取る、鍵素材読み取り手段と、
　前記鍵素材読み取り手段が読み取った前記鍵素材に基づいて前記共通鍵を生成する共通鍵生成手段と、
を備えることを特徴とする共通鍵生成装置。
（付記２）
　前記鍵素材が番号であり、
　前記第一の局面では、前記鍵素材読み取り手段によって１ずつ加算または減算されることにより前記鍵素材が更新される、
ことを特徴とする付記１に記載の共通鍵生成装置。
（付記３）
　前記入力データがデータリンク層のフレームであることを特徴とする付記１に記載の共通鍵生成装置。
（付記４）
　前記フレームがＶＬＡＮを識別するＶＬＡＮ識別情報を含むとき、該ＶＬＡＮ識別情報に基づいて、前記第一の局面と、前記第二の局面と、前記フレームに対応して共通鍵を生成する必要がない第三の局面とを含む複数の局面のいずれに該当するかを判定する判定手段をさらに備える、
ことを特徴とする付記３に記載の共通鍵生成装置。
（付記５）
　前記入力データがネットワーク層のパケットであることを特徴とする付記１に記載の共通鍵生成装置。
（付記６）
　前記共通鍵は、ＩＰｓｅｃのための共通鍵として利用されることを特徴とする付記５に記載の共通鍵生成装置。
（付記７）
　前記第一の局面と前記第二の局面とを含む複数の局面のいずれに該当するかを判定する判定手段をさらに備えることを特徴とする付記１に記載の共通鍵生成装置。
（付記８）
　前記受付手段が複数のインターフェイスを有し、
　該複数のインターフェイスのうちのいずれを介して前記入力データを前記受付手段が受け付けたかに基づいて、前記判定手段が判定する、

ことを特徴とする付記７に記載の共通鍵生成装置。
（付記９）
前記第一の局面に、前記鍵素材を含む第二のヘッダ部と、前記入力データの前記ペイロード部を前記共通鍵により暗号化した第二のペイロード部とを有する暗号化出力データを生成する暗号化手段と、
前記第二の局面に、前記入力データの前記ペイロード部を前記共通鍵により復号化した第三のペイロード部を有する復号化出力データを生成する復号化手段と、
をさらに有することを特徴とする付記１に記載の共通鍵生成装置。
（付記１０）
前記共通鍵生成手段がハッシュ関数を使って前記共通鍵を生成することを特徴とする付記１に記載の共通鍵生成装置。
（付記１１）
通信路上に前記共通鍵生成装置が配置され、
前記入力データは、前記通信路を通って送信元から送信先へ送られるときに前記共通鍵生成装置を経由して、前記受付手段により受け付けられ、
前記共通鍵生成手段は、前記送信元または前記送信先の少なくとも一方のアドレスに基づいて前記共通鍵を生成する、
ことを特徴とする付記１に記載の共通鍵生成装置。
（付記１２）
事前共有鍵として同一の値を設定された二つの前記共通鍵生成装置が通信路上に配置され、
前記入力データは、前記経路を、送信元、送信側の前記共通鍵生成装置、受信側の前記共通鍵生成装置、送信先の順に経由して送信され、
前記入力データは、二つの前記共通鍵生成装置を経由する際にそれぞれの前記受付手段で受け付けられ、
二つの前記共通鍵生成装置のそれぞれの前記共通鍵生成手段は、前記事前共有鍵に基づいて前記共通鍵を生成する、
ことを特徴とする付記１に記載の共通鍵生成装置。
（付記１３）
前記共通鍵生成装置のファームウェアにより一意に規定される文字列と前記事前共有鍵とに基づいて算出した値を、同じシードからは同じ値を生成するランダム関数にシードとして与えてランダムな値を生成するランダム値生成手段をさらに備え、
前記共通鍵生成手段は、前記ランダムな値に基づいて前記共通鍵を生成する、
ことを特徴とする付記１２に記載の共通鍵生成装置。
（付記１４）
前記共通鍵生成装置のファームウェアにより一意に規定される文字列と前記事前共有鍵とに基づいて算出した値をハッシュ関数の引数としてハッシュ値を算出するハッシュ値算出手段をさらに備え、
前記共通鍵生成手段は、前記ハッシュ値に基づいて前記共通鍵を生成する、
ことを特徴とする付記１２に記載の共通鍵生成装置。
（付記１５）
Ｍを２以上の整数として、前記事前共有鍵に基づいてＭ個の値を候補値として生成する候補値生成手段と、
Ｍ個の前記候補値を格納する候補値格納手段とをさらに備え、
前記共通鍵生成手段は、前記鍵素材に基づいてＭ個の前記候補値のうちの一つを選択して前記候補値格納手段から読み取り、該候補値に基づいて前記共通鍵を生成する、
ことを特徴とする付記１２に記載の共通鍵生成装置。
（付記１６）
前記候補値生成手段は、Ｍ個の前記候補値を生成する際、Ｍ個の異なるインデックス値に対してそれぞれ、前記共通鍵生成装置のファームウェアにより一意に規定される文字列

と前記事前共有鍵と当該インデックス値とに基づいてシードを算出し、同じシードからは同じ値を生成するランダム関数に該シードを与えてランダムな値を算出することによって、Ｍ個の前記候補値を生成する、
ことを特徴とする付記１５に記載の共通鍵生成装置。
（付記１７）
前記候補値生成手段は、Ｍ個の前記候補値を生成する際、Ｍ個の異なるインデックス値に対してそれぞれ、前記共通鍵生成装置のファームウェアにより一意に規定される文字列と前記事前共有鍵と当該インデックス値とに基づいて算出される値をハッシュ関数の引数として与えることによって、Ｍ個の前記候補値を算出する、
ことを特徴とする付記１５に記載の共通鍵生成装置。
（付記１８）
共通鍵暗号方式において使われる共通鍵を生成する共通鍵生成方法であって、
クリアテキストの状態のヘッダ部と、ペイロード部とを有する入力データを受け付ける受付ステップと、
前記入力データの暗号化のために前記共通鍵を生成する第一の局面では、鍵素材を格納する鍵素材格納手段から前記鍵素材を読み取り、前記鍵素材格納手段内の前記鍵素材を更新し、前記入力データの復号化のために前記共通鍵を生成する第二の局面では、前記ヘッダ部の所定の部分から前記鍵素材を読み取る鍵素材読み取りステップと、
読み取った前記鍵素材に基づいて前記共通鍵を生成する共通鍵生成ステップと、
を備えることを特徴とする共通鍵生成方法。
【図面の簡単な説明】
【０３５２】
【図１】共通鍵生成装置を備えた中継装置を含むネットワーク上で行われる暗号化通信を示す模式図である。
【図２】送信元と送信先の組み合わせの例を示す図である。
【図３】共通鍵を生成するために用いられる情報を示す図である。
【図４】共通鍵生成装置の基本的な機能ブロック構成図である。
【図５】共通鍵生成装置を備えた中継装置を含むネットワーク上で行われる暗号化通信を示す模式図である。
【図６】本発明を適用したレイヤ２の中継装置の構成図である。
【図７】図６と図４の関係を説明する機能ブロック構成図である。
【図８】図６の変形例を示す図である。
【図９Ａ】共通鍵生成装置を含むレイヤ２の中継装置の利用例を示す図である。
【図９Ｂ】図９Ａの一部を抜粋して装置の詳細を示すとともに、フレームの流れを示す図である。
【図１０】フレームの形式を説明する図である。
【図１１】暗号ヘッダの詳細を示す図である。
【図１２】共通鍵生成装置を搭載したレイヤ２の中継装置を使ったネットワークの構成例を示す図である。
【図１３】共通鍵生成装置を搭載したレイヤ２の中継装置を使ったネットワークの構成例を示す図である。
【図１４】共通鍵生成装置を搭載したレイヤ２の中継装置を使ったネットワークの構成例を示す図である。
【図１５】図３に示した各種情報のより具体的な例を示す図である。
【図１６】配列を利用して共通鍵を生成する方法を説明する図である。
【図１７】フレームの分割と再構成を実現するための暗号ヘッダの形式を説明する図である。
【図１８】共通鍵生成装置を備えた中継装置を含むネットワーク上で行われる暗号化通信およびＩＰパケットの形式を示す図である。
【図１９】本発明を適用したルータの構成図である。

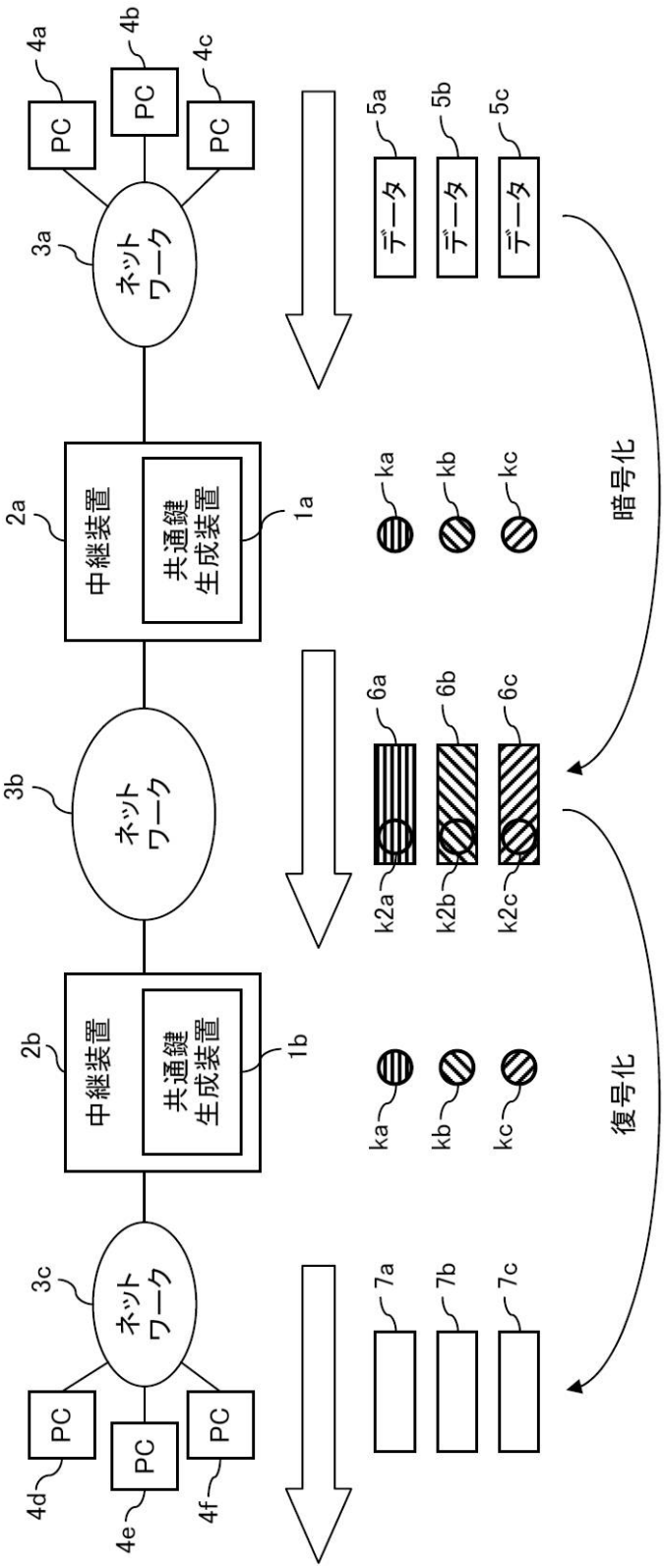
【図２０】図１９と図４の関係を説明する機能ブロック構成図である。
【図２１】暗号化されていないＩＰパケットを受信したときのＩＰｓｅｃ処理部の動作を説明する図である。
【図２２】暗号化ＩＰパケットを受信したときのＩＰｓｅｃ処理部の動作を説明する図である。
【図２３】ＩＰヘッダの形式を示す図である。
【図２４】ＥＳＰパケットの形式を示す図である。
【図２５】マスター鍵の生成について説明する図である。
【図２６Ａ】トランスポートモードにおける図３の各情報と図２３～図２５との対応関係を説明する図である。
【図２６Ｂ】トンネルモードにおける図３の各情報と図２３～図２５との対応関係を説明する図である。
【図２７】共通鍵生成装置を備えたルータをマルチキャストに利用した例を示す図である。
【図２８】ＩＰｓｅｃを利用した従来の暗号化通信を示す模式図である。
【符号の説明】
【０３５３】
１、１ａ～１ｄ　共通鍵生成装置
２ａ、２ｂ　中継装置
３ａ～３ｅ　ネットワーク
４ａ～４ｇ　ＰＣ
５ａ～５ｃ　データ
６ａ～６ｃ　暗号化データ
７ａ～７ｃ　復号化データ
８、８ａ、８ｂ　ルータ
１１　受付部
１２　鍵素材格納部
１３　鍵素材読み取り部
１４　共通鍵生成部
１５　判定部
１６　暗号化部
１７　復号化部
１８　事前共有鍵格納部
１９　出力部
２０　マスター鍵生成部
２１　マスター鍵格納部
２２　ＩＰｓｅｃ処理部
１０１、１０１ａ～１０１ｅ　Ｌ２中継装置
１０２、１０２ａ～１０２ｅ　フレーム中継処理部
１０３、１０３ａ～１０３ｏ　ポート
１０４ａ～１０４ｎ　暗号処理モジュール
１０５　ＴＣＧ対応チップ
１０６　ＣＰＵ
１０７　内部バス
１１０、１２０、１３０　ＶＬＡＮ
１４１　コアＬ２／Ｌ３スイッチ
１４１ｂ　Ｌ２スイッチ
１４２ａ、１４２ｂ　．１Ｑトランク
１４３　ファイヤウォール
１４４　ルータ

１４５　インターネット
１５０　フレーム
１５１　送信先ＭＡＣアドレス
１５２　送信元ＭＡＣアドレス
１５３　データ部
１５４　ＦＣＳ
１６０　タグつきフレーム
１６１　ＴＰＩＤ
１６２　ＴＣＩ
１７０　暗号化フレーム
１７１　暗号ヘッダ
１７２　暗号化データ部
１７３　ＩＣＶ
１７１１　タイプ
１７１２　サブタイプ
１７１３　予約フィールド
１７１４　シーケンス番号
１７１５　ＩＤ
１７１６　フラグメントオフセット
２０１、２０１ａ～２０１ｃ　ルータ
２０２　パケット中継処理部
２０３ａ～２０３ｄ　ポート
２０４　ルーティングテーブル
２０５　セキュリティポリシーデータベース
２０６　ＴＣＧ対応チップ
２０７　ＣＰＵ
２０８　内部バス
２５０、２５０ａ～２５０ｃ　ＩＰパケット
２５１　ＩＰヘッダ
２５２　ＩＰデータ
２６０、２６０ａ～２６０ｃ　暗号化ＩＰパケット
２６１　ＩＰヘッダ
２６２　ＥＳＰヘッダ
２６３　暗号化されたＩＰヘッダ
２６４　暗号化されたＩＰデータ
２６５　ＥＳＰトレイラ
２６６　認証データ
２７０　暗号化ＩＰパケット
２８０、２８０ａ～２８０ｃ　復号化ＩＰパケット
３０１　バージョン
３０２　ＩＨＬ
３０３　ＴＯＳ
３０４　全長
３０５　ＩＤ
３０６　フラグ
３０７　フラグメントオフセット
３０８　ＴＴＬ
３０９　プロトコル
３１０　ヘッダチェックサム
３１１　送信元ＩＰアドレス

３１２　送信先ＩＰアドレス
３１３　オプション
３１４　パディング
４００　ＥＳＰパケット
４０１　ＳＰＩ
４０２　シーケンス番号
４０３　ＥＳＰペイロードデータ
４０４　パディング
４０５　パディング長
４０６　次ヘッダ
ｋ、ｋａ～ｋｄ　共通鍵
ｋ０　事前共有鍵
ｋ１、ｋ１ａ～ｋ１ｃ　送信先・送信元情報
ｋ１＿ｆ　ＭＡＣヘッダ情報
ｋ１＿ｐ１、ｋ１＿ｐ２　ＩＰヘッダ情報
ｋ２、ｋ２ａ～ｋ２ｃ　鍵素材
ｋ２＿ｓ、ｋ２＿ｒ、ｋ２＿ｎ　シーケンス番号
ｋ２＿ｒ１、ｋ２＿ｒ２　ＩＤ
ｋ２＿ｒ３　シーケンス番号
ｋ３　マスター鍵
Ｃ　マスター鍵配列
ｆ　フレーム
ｐ　パケット

【図１】

共通鍵生成装置を備えた中継装置を含む
ネットワーク上で行われる暗号化通信を示す模式図



【図２】

送信元と送信先の組み合わせの例を示す図

データ	送信元	送信先
データ5a	PC4a	PC4d
データ5b	PC4b	PC4e
データ5c	PC4c	PC4f

場合（A）

データ	送信元	送信先
データ5a	PC4a	PC4d
データ5b	PC4a	PC4e
データ5c	PC4a	PC4f

場合（B）

データ	送信元	送信先
データ5a	PC4a	PC4d
データ5b	PC4b	PC4d
データ5c	PC4c	PC4d

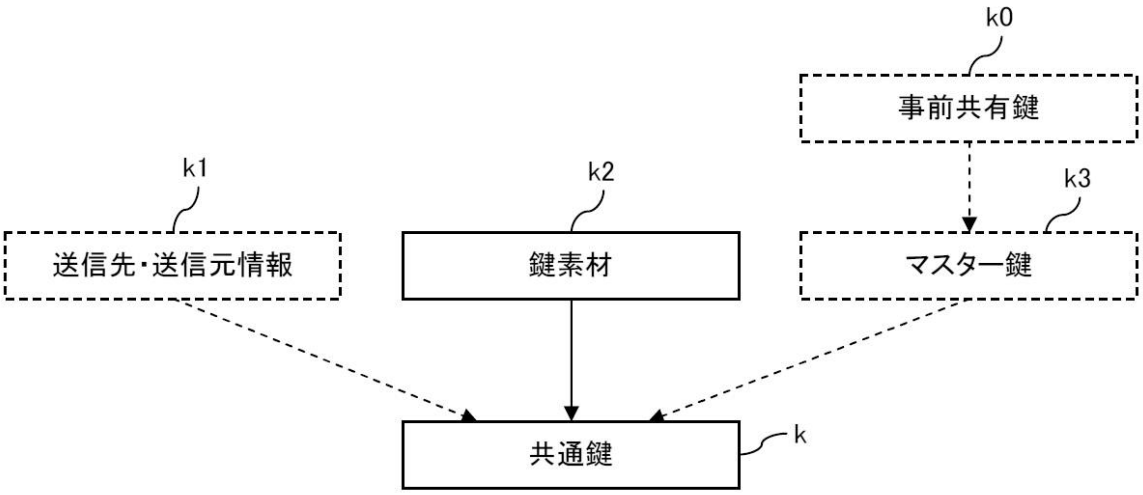
場合（C）

データ	送信元	送信先
データ5a	PC4a	PC4d
データ5b	PC4a	PC4d
データ5c	PC4a	PC4d

場合（D）

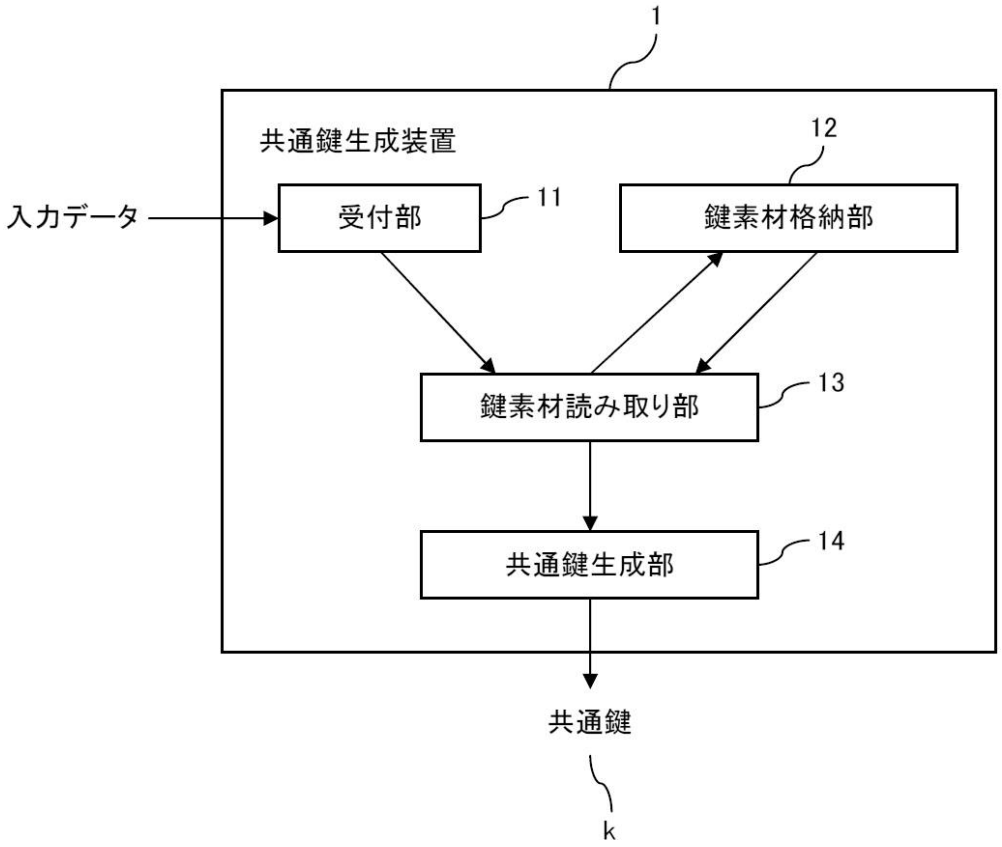
【図３】

共通鍵を生成するために用いられる情報を示す図



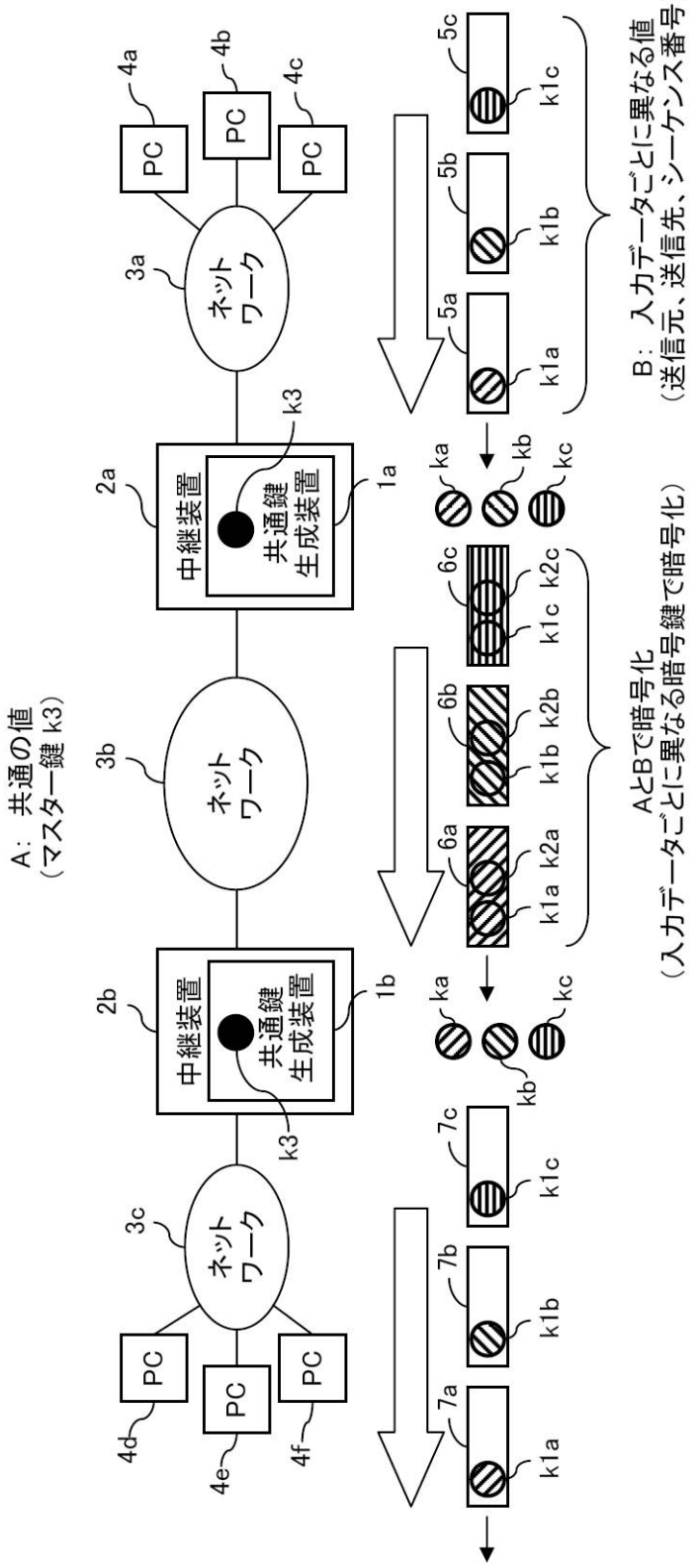
【図４】

共通鍵生成装置の基本的な機能ブロック構成図



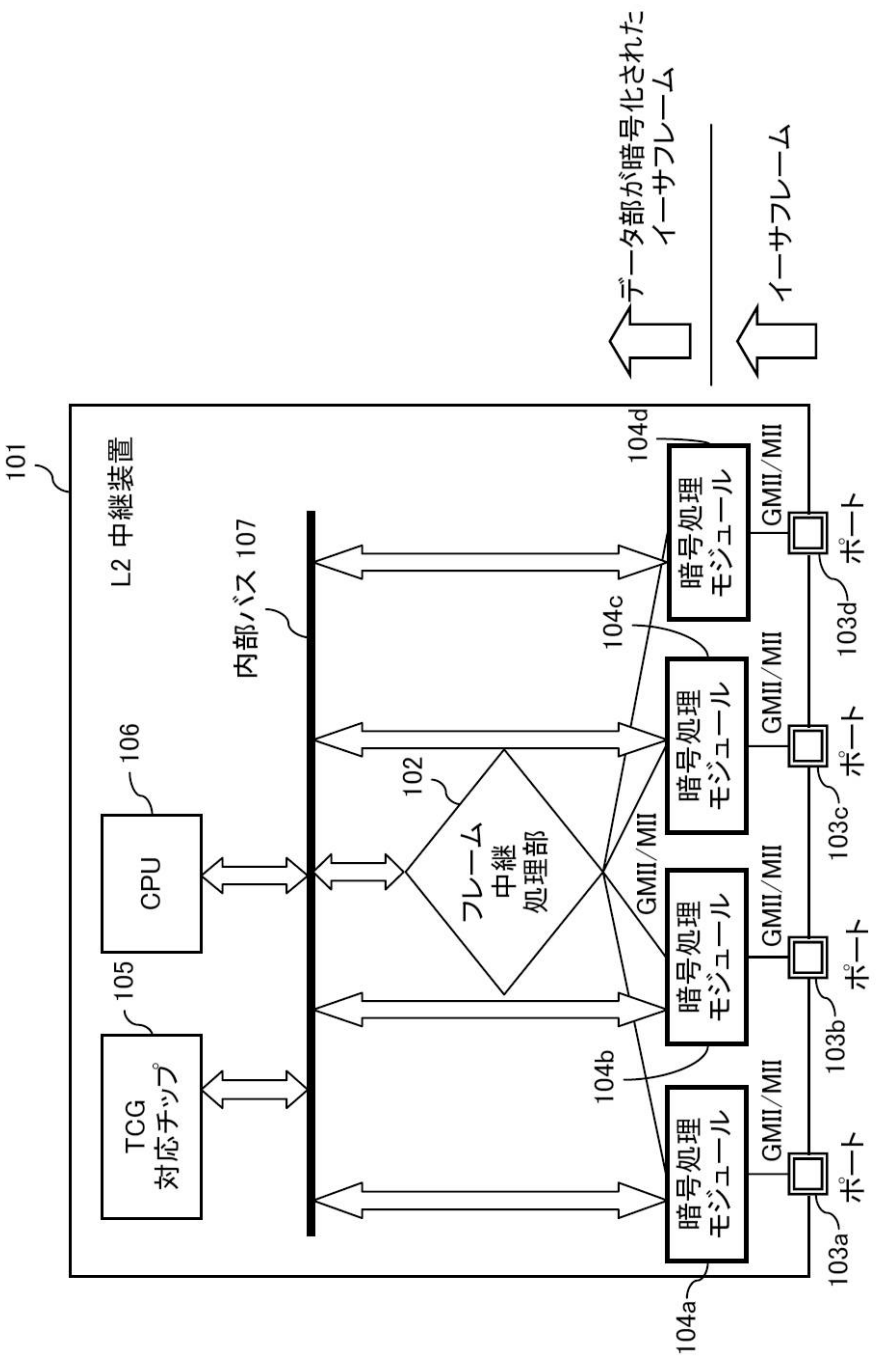
【図５】

共通鍵生成装置を備えた中継装置を含む
ネットワーク上で行われる暗号化通信を示す模式図



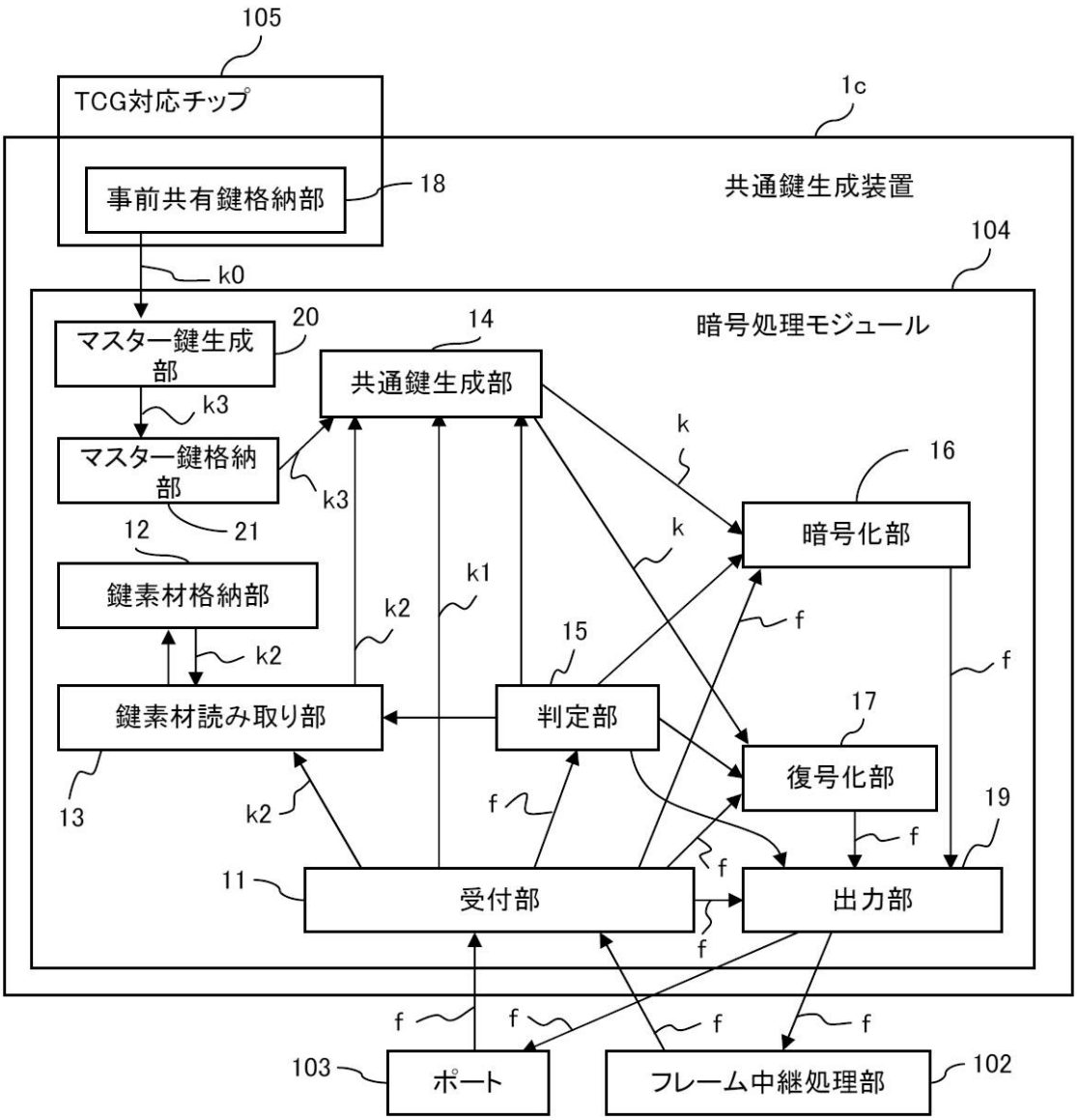
【図６】

本発明を適用したレイヤ2の
中継装置の構成図



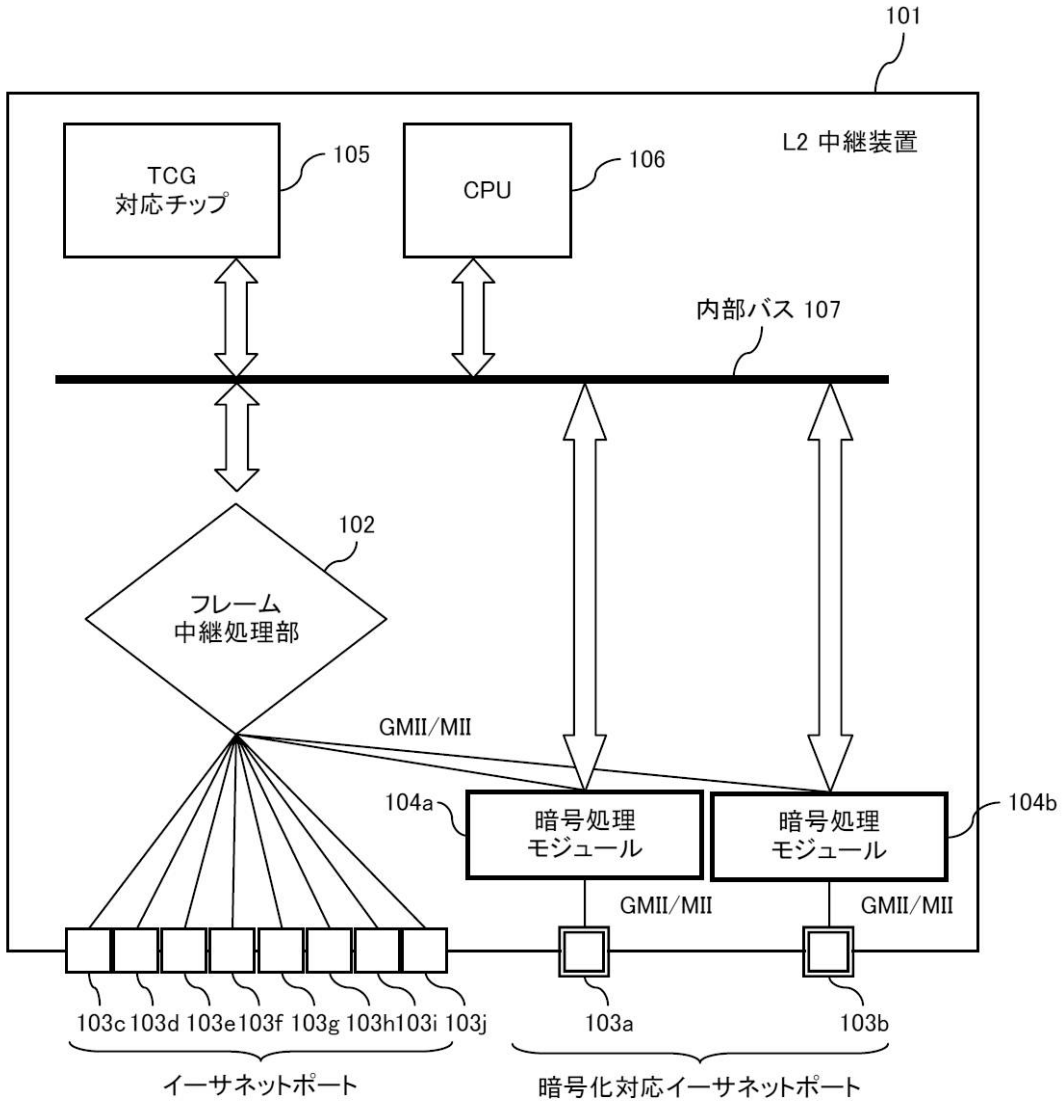
【図７】

図6と図4の関係を説明する機能ブロック構成図

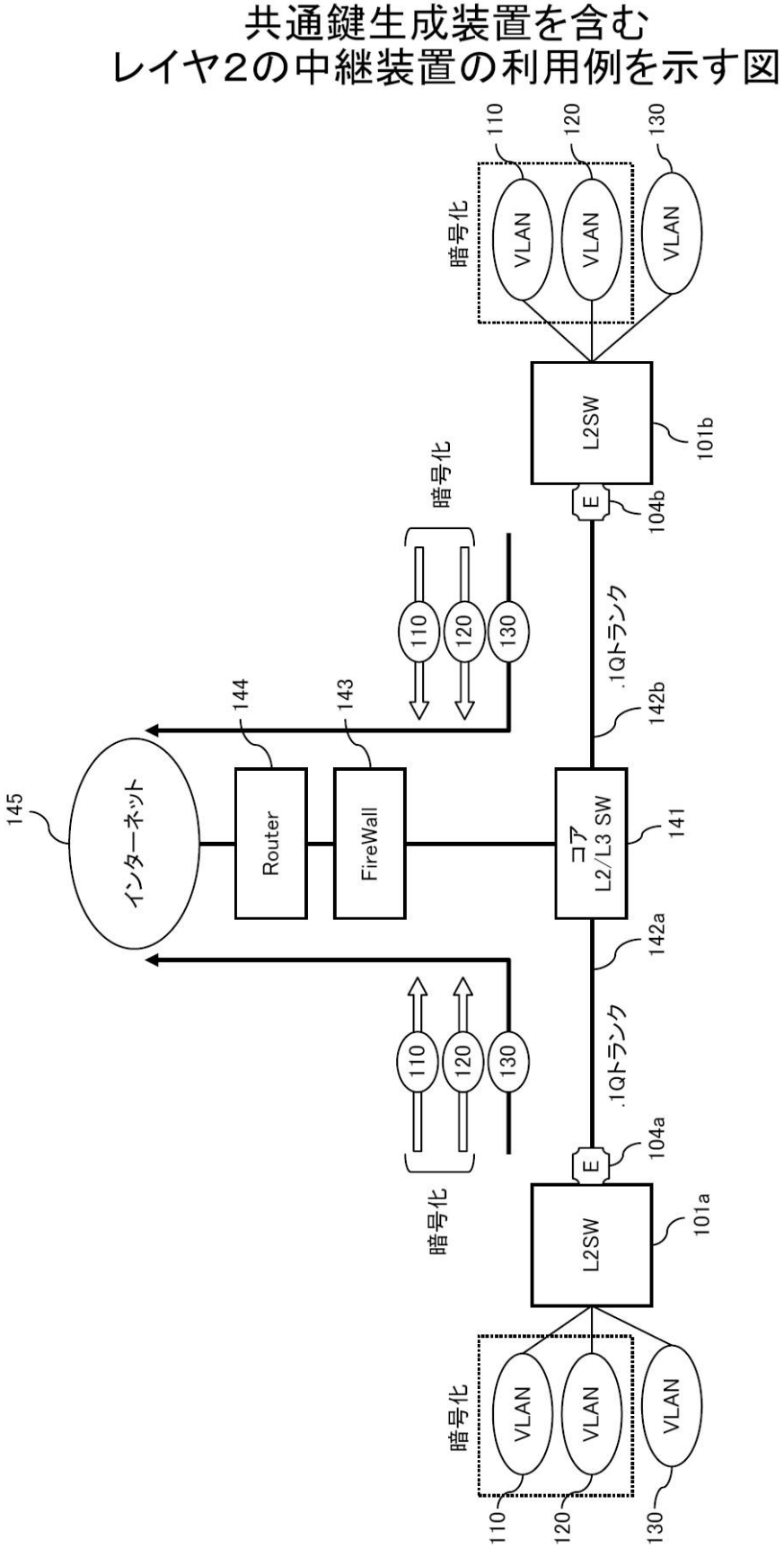


【図８】

図6の変形例を示す図

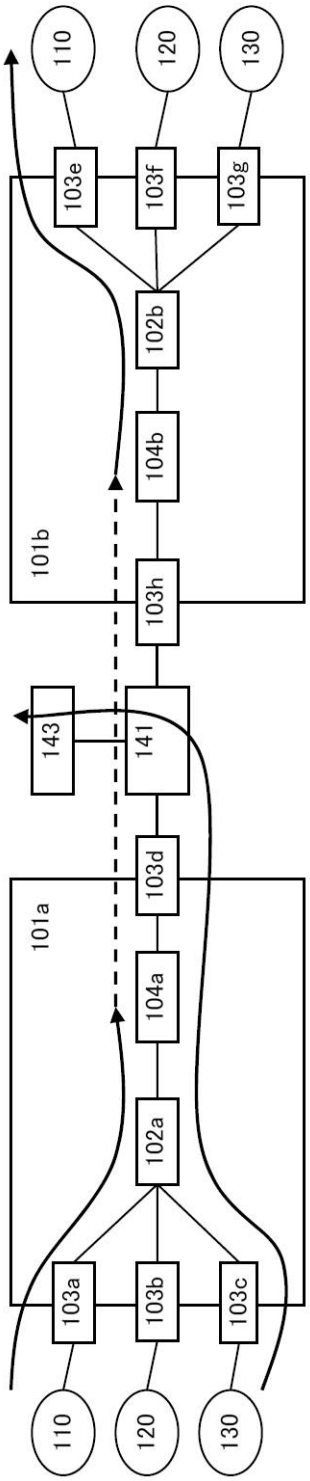


【図９Ａ】


共通鍵生成装置を含む
レイヤ2の中継装置の利用例を示す図
暗号化
VLAN
VLAN
VLAN
110
120
130
L2SW
101b
E
104b
暗号化
110
120
130
.1Qトランク
142b
144
143
インターネット
145
Router
FireWall
コア
L2/L3 SW
141
142a
110
120
130
.1Qトランク
104a
E
暗号化
L2SW
101a
暗号化
VLAN
VLAN
VLAN
110
120
130

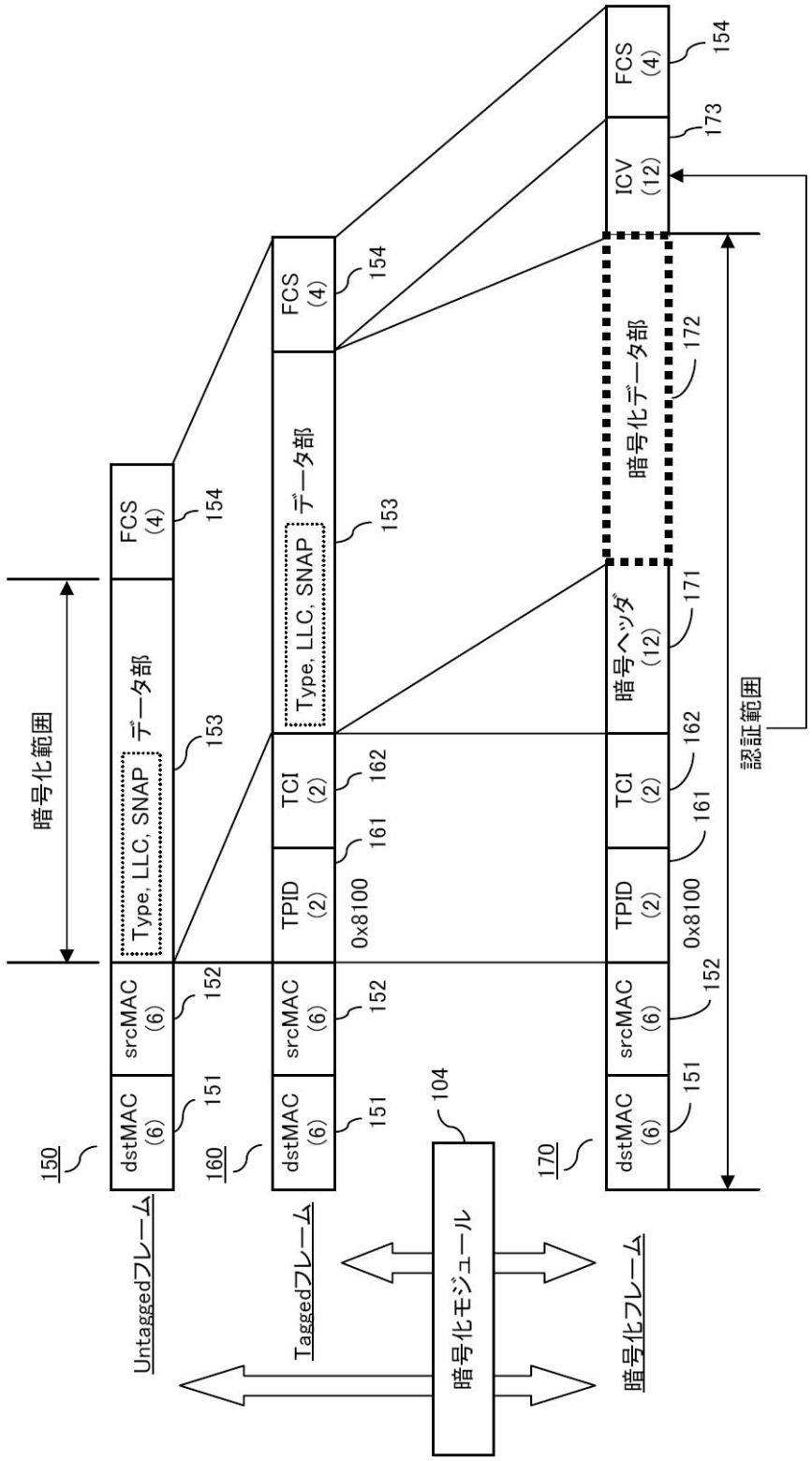
【図９Ｂ】

図9Aの一部を抜粋して装置の
詳細を示すとともに、フレームの流れを示す図



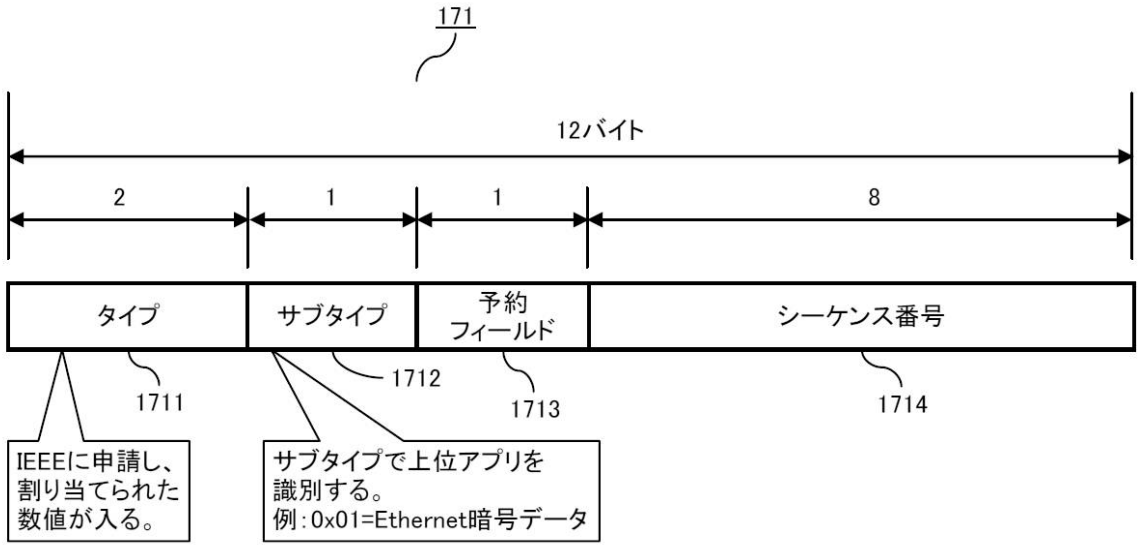
【図１０】

フレームの形式を説明する図



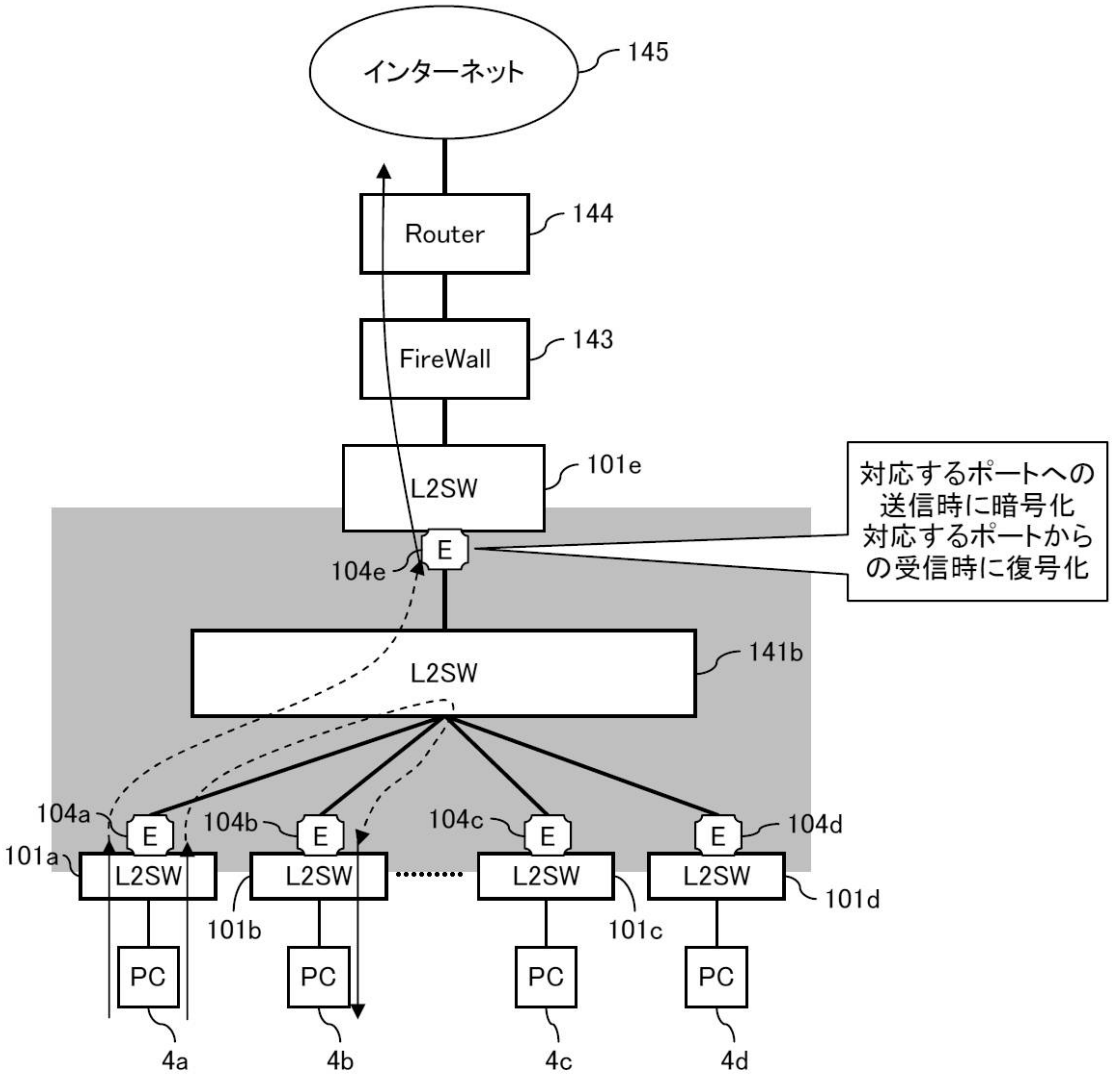
【図１１】

暗号ヘッダの詳細を示す図



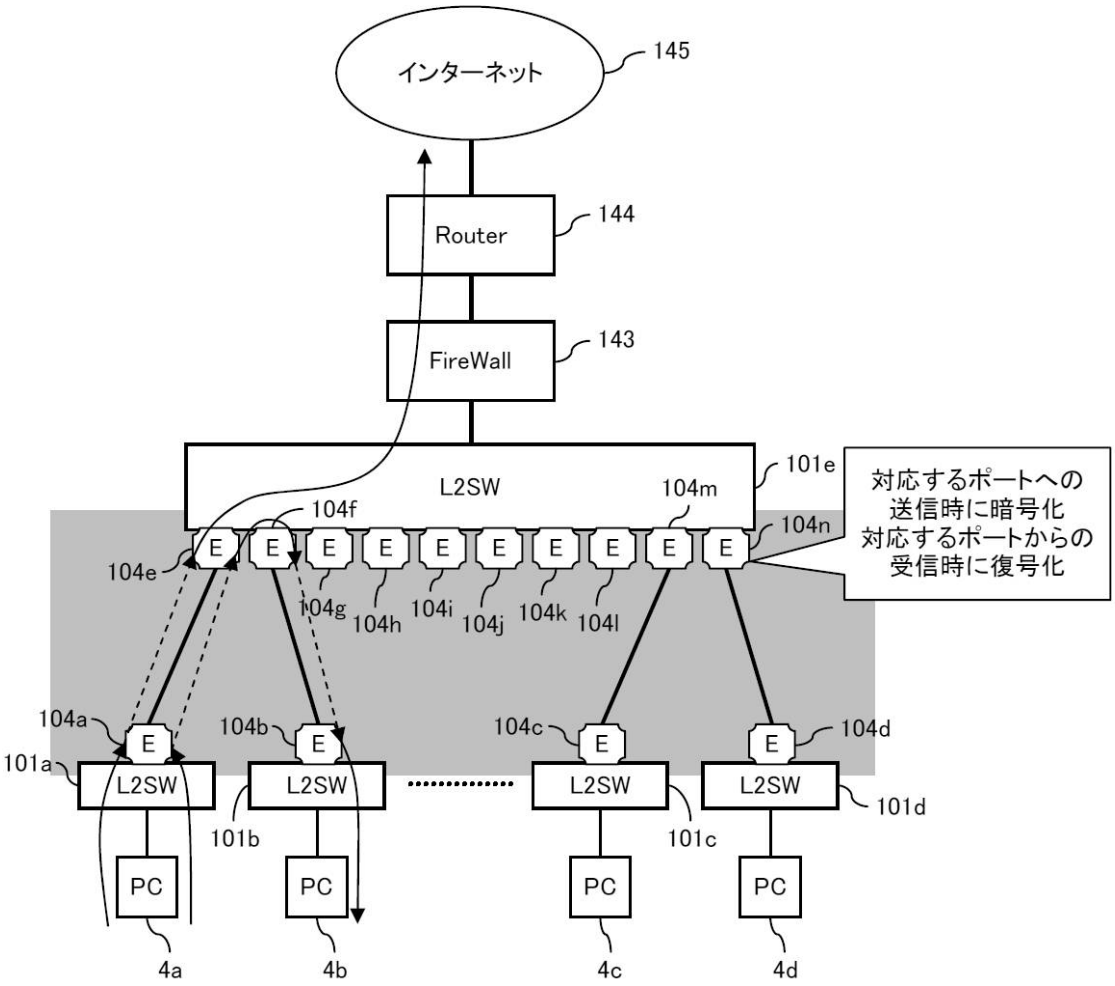
【図１２】

共通鍵生成装置を搭載したレイヤ2の
中継装置を使ったネットワークの構成例を示す図



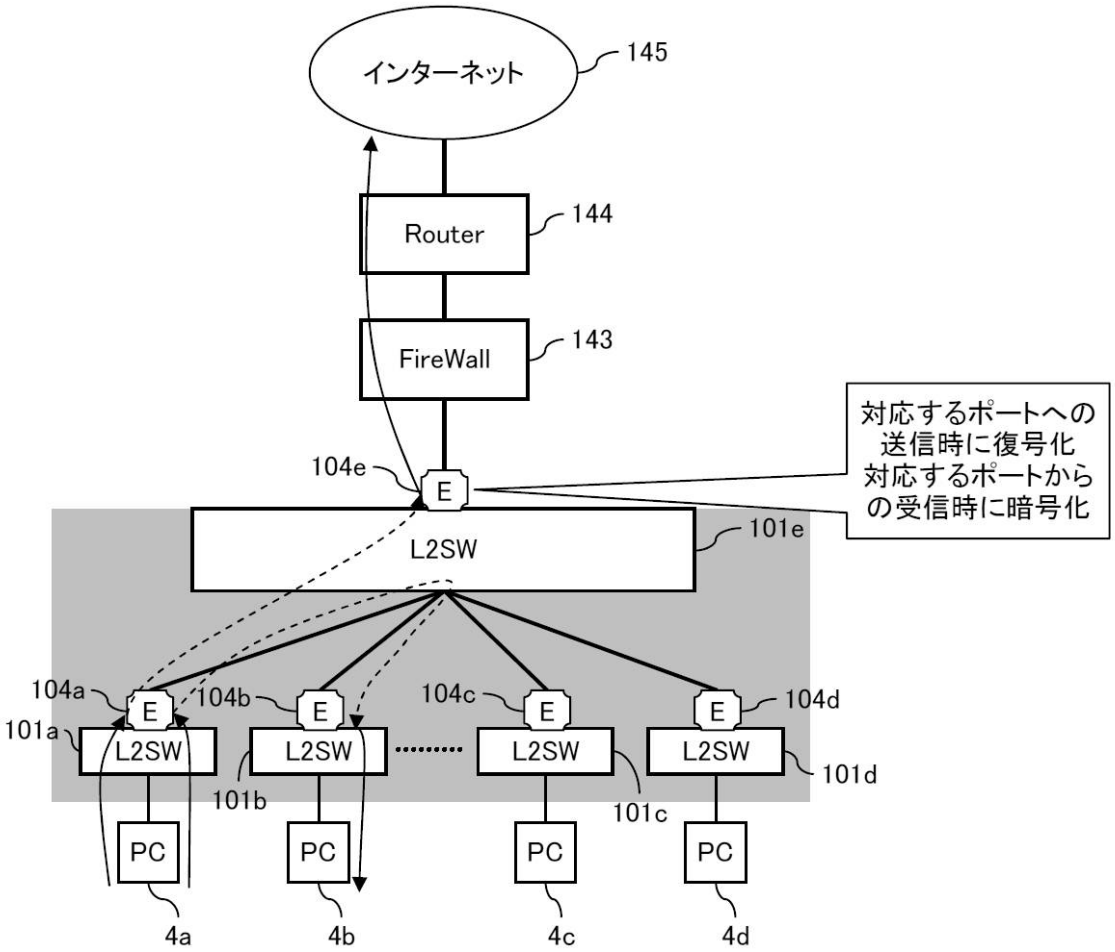
【図１３】

共通鍵生成装置を搭載したレイヤ2の
中継装置を使ったネットワークの構成例を示す図



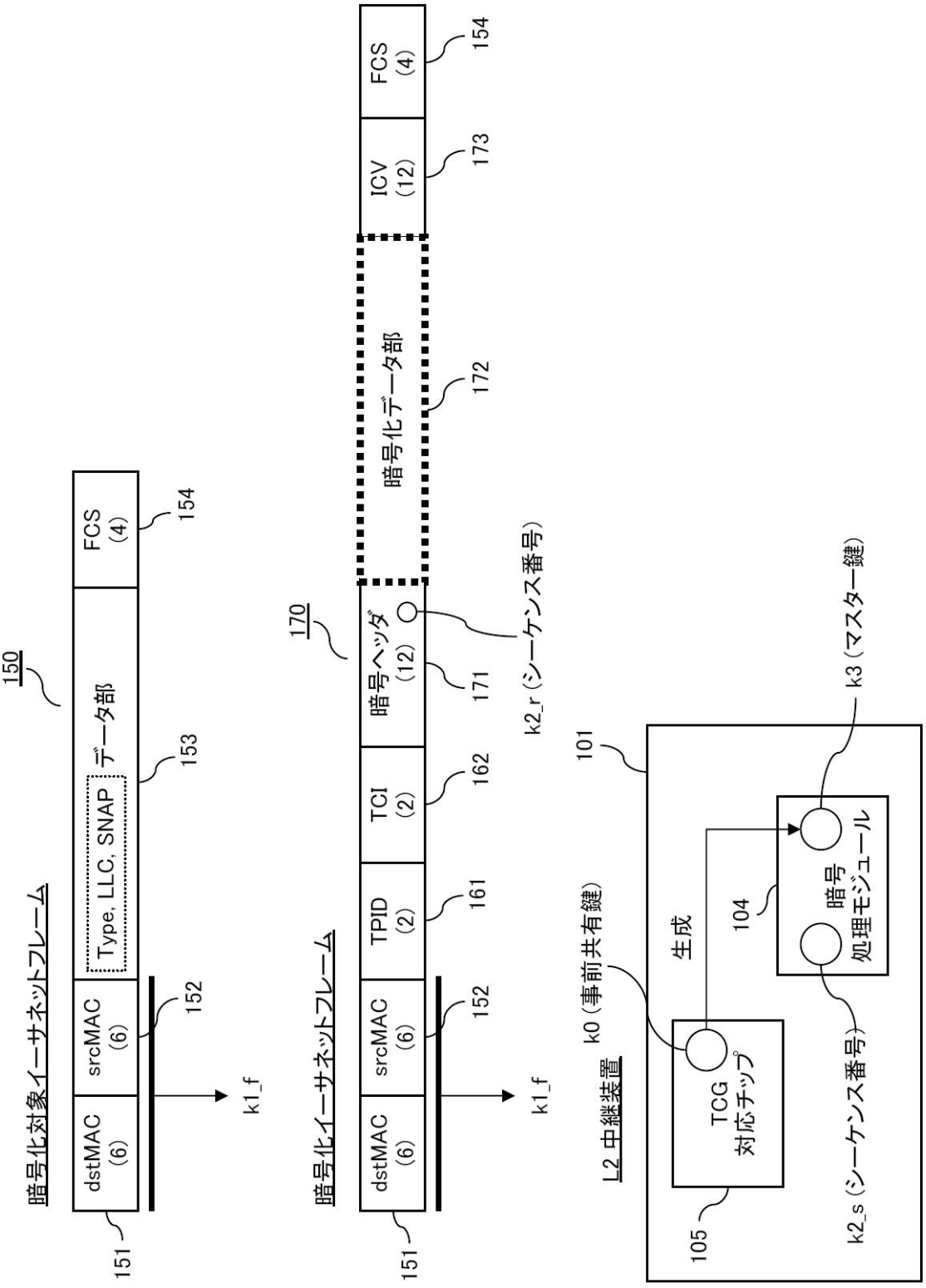
【図１４】

共通鍵生成装置を搭載したレイヤ2の
中継装置を使ったネットワークの構成例を示す図



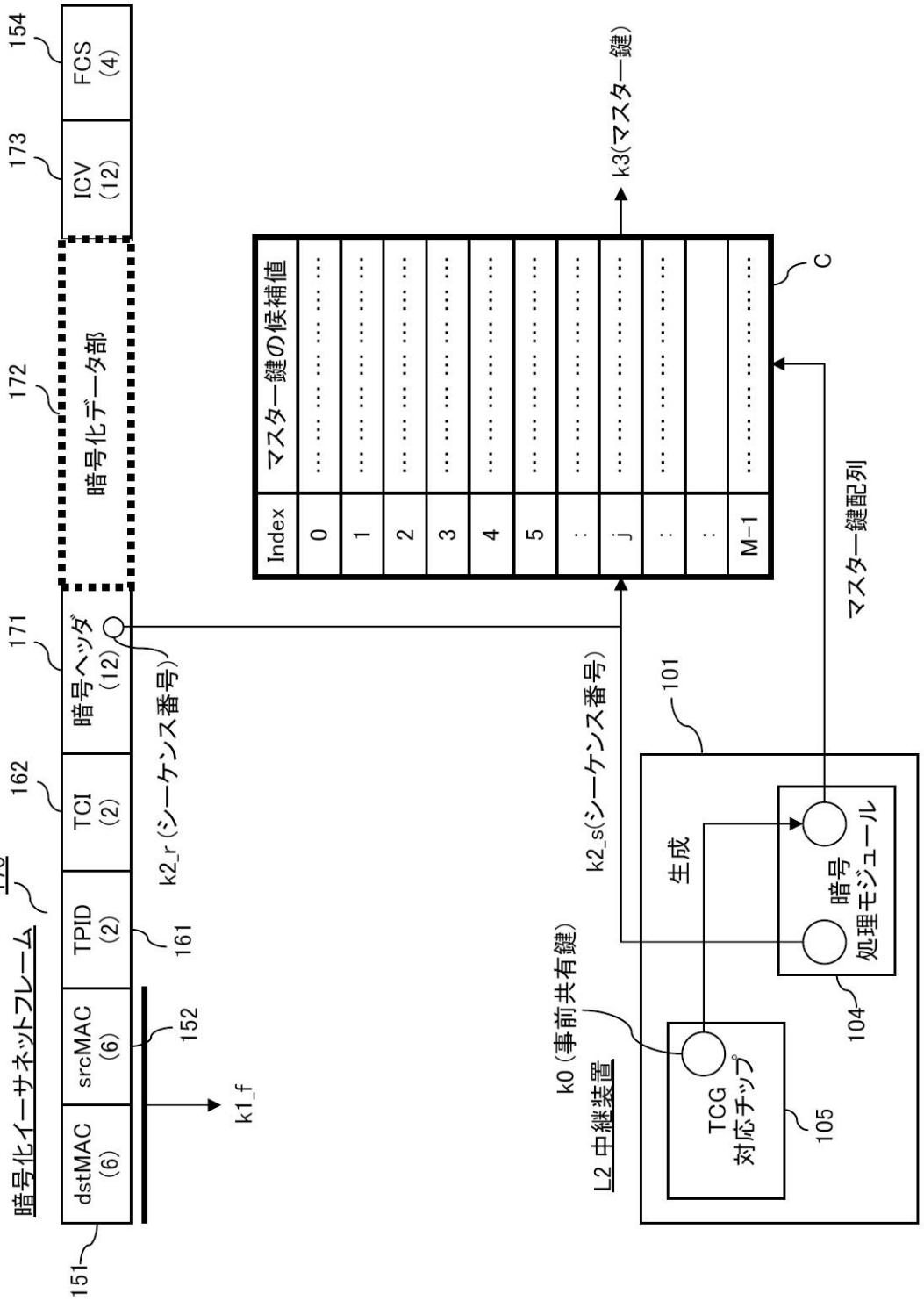
【図１５】

図3に示した各種情報のより具体的な例を示す図



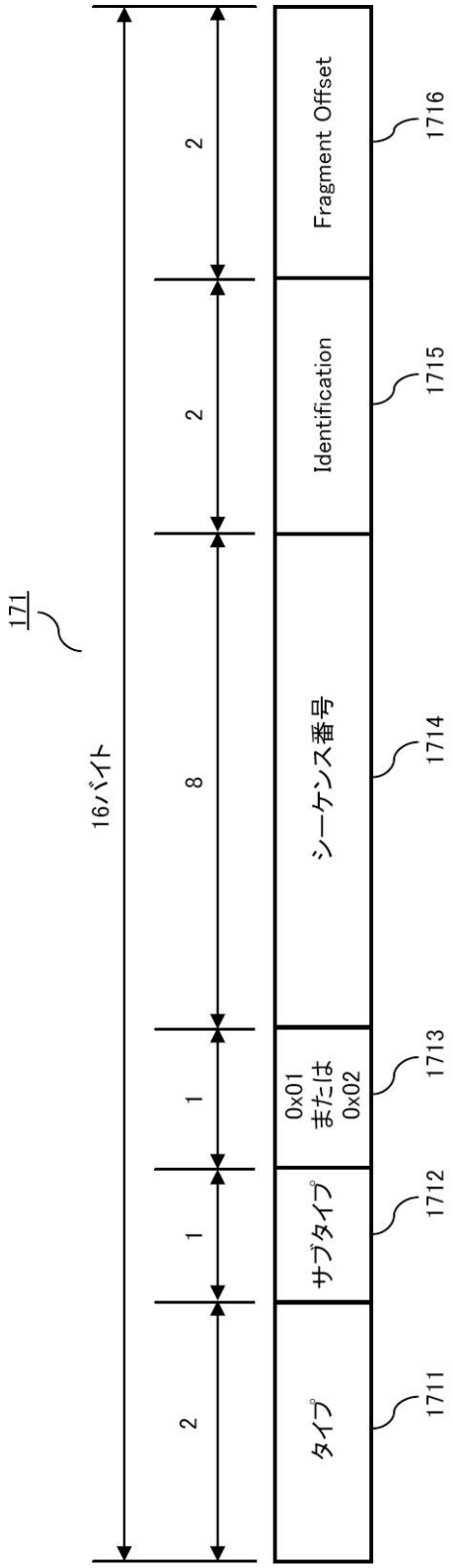
【図１６】

配列を利用して共通鍵を
生成する方法を説明する図

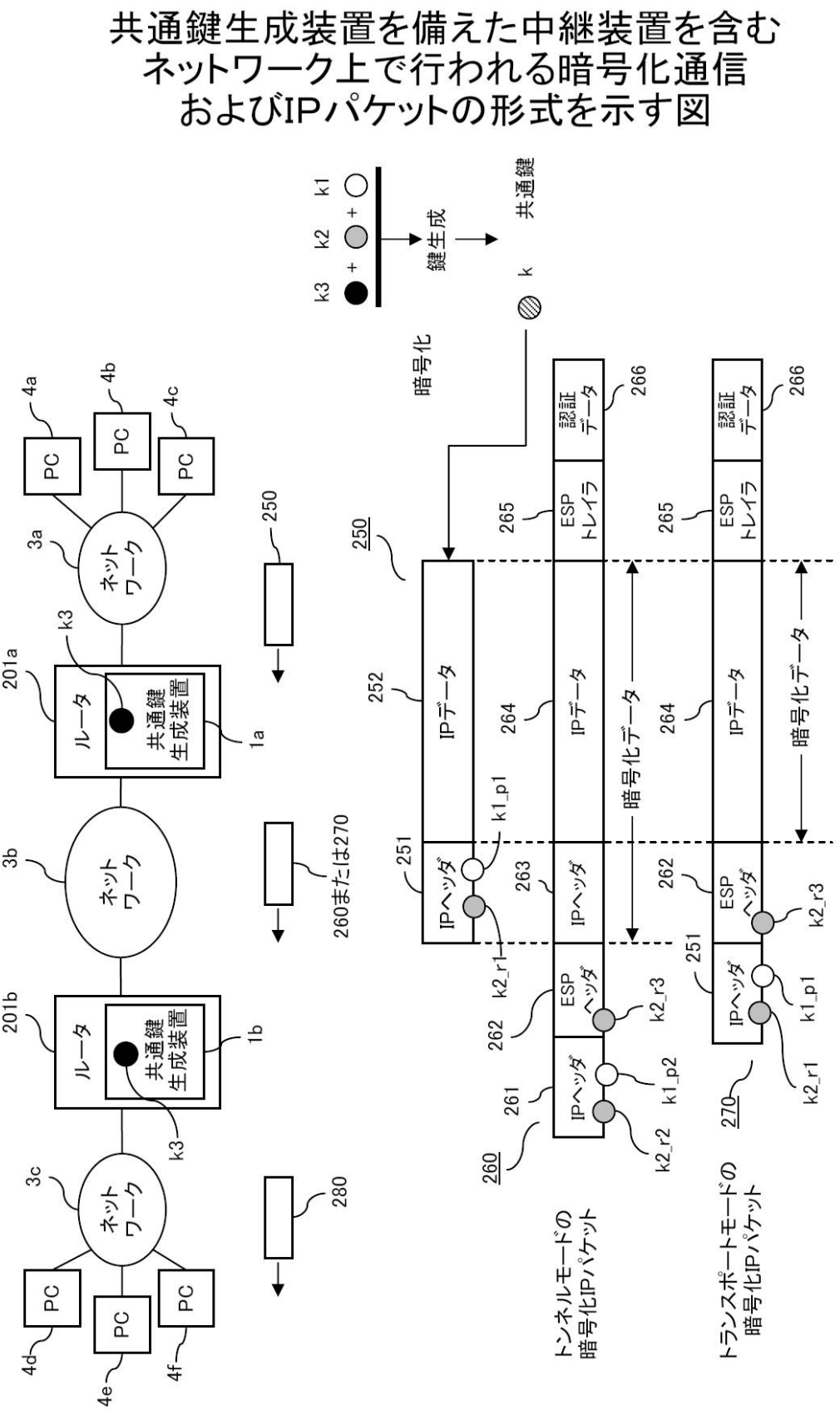


【図１７】

フレームの分割と再構成を実現するための
暗号ヘッダの形式を説明する図

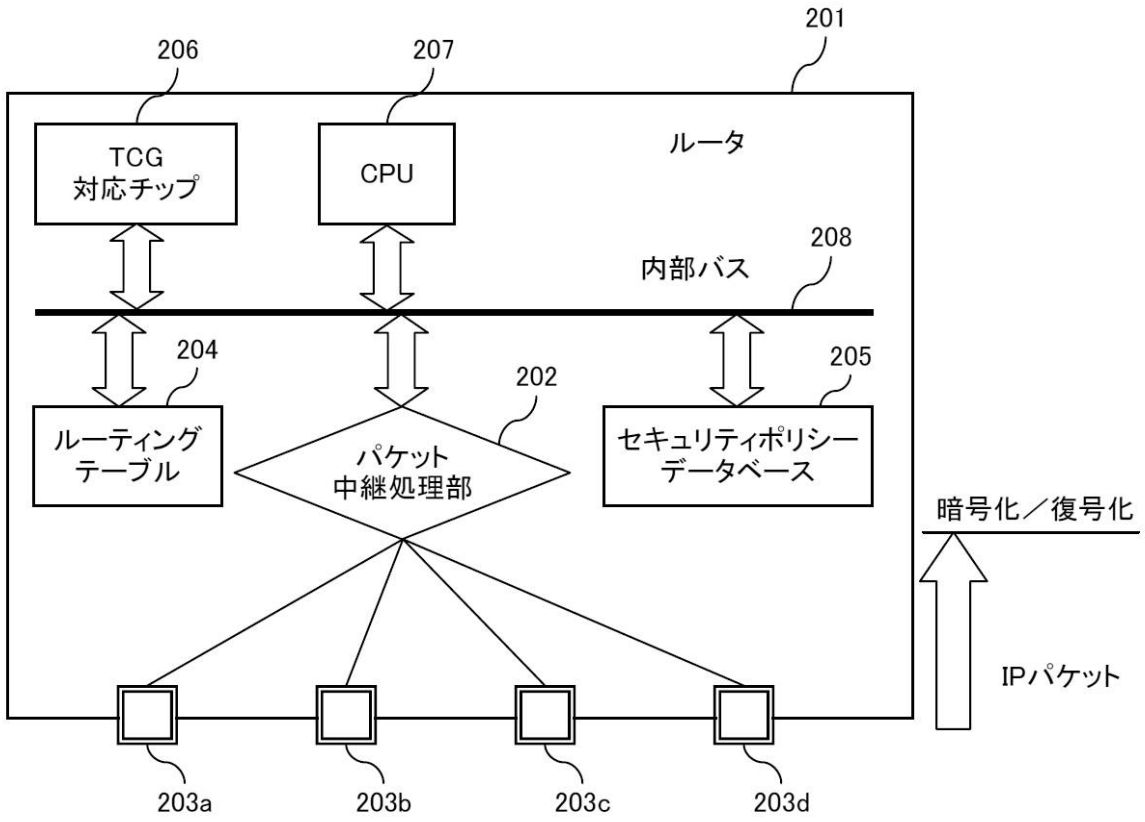


【図１８】


共通鍵生成装置を備えた中継装置を含む
ネットワーク上で行われる暗号化通信
およびIPパケットの形式を示す図
k1
k2
k3
鍵生成
k
共通鍵
暗号化
PC
4a
4b
4c
4d
4e
4f
ネットワーク
3a
3b
3c
ルータ
201a
201b
共通鍵生成装置
1a
1b
k3
250
260または270
280
IPヘッダ
IPデータ
ESPヘッダ
ESPトレイラ
認証データ
暗号化データ
k1_p1
k1_p2
k2_r1
k2_r2
k2_r3
251
252
260
261
262
263
264
265
266
270
トンネルモードの暗号化IPパケット
トランスポートモードの暗号化IPパケット

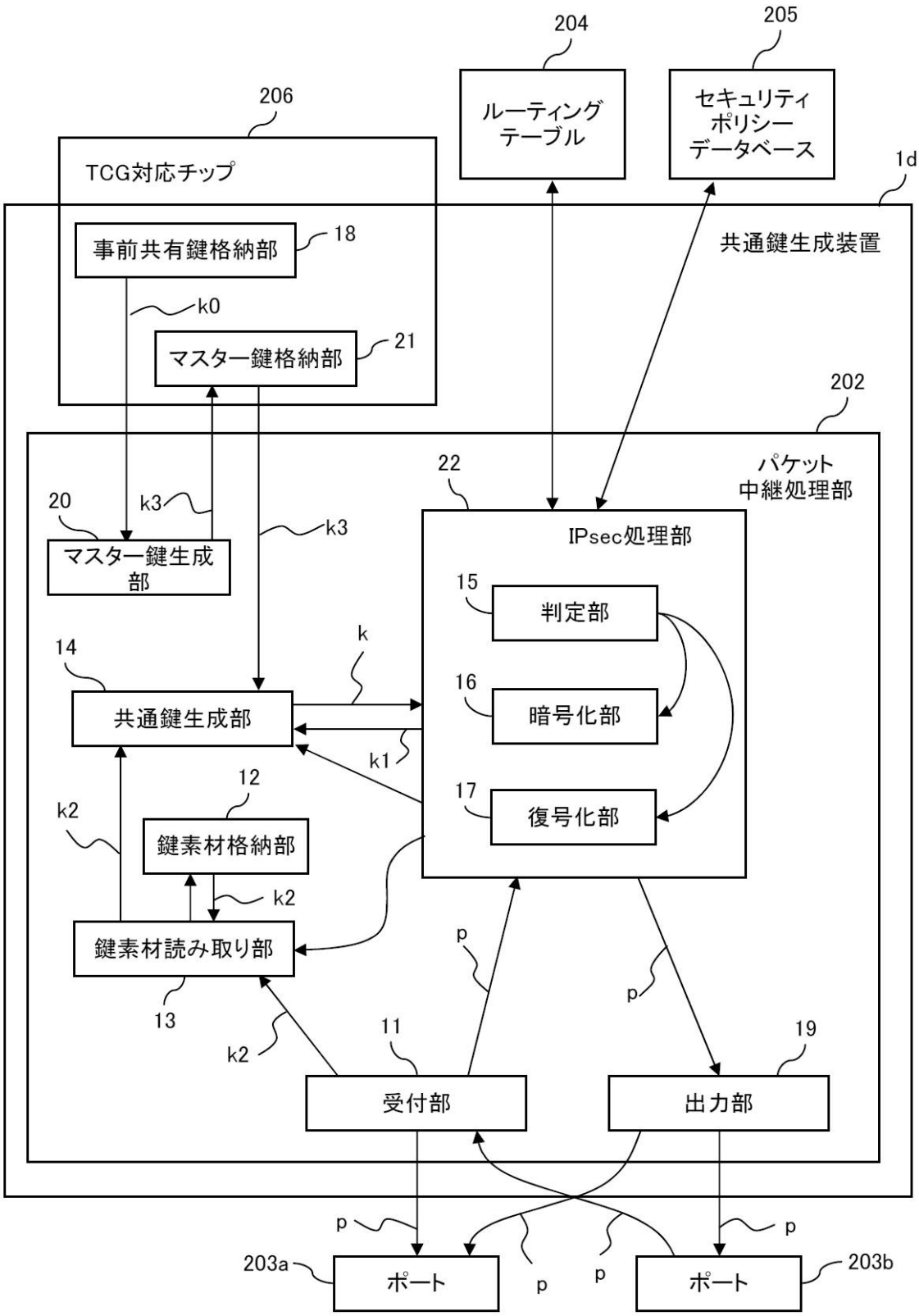
【図１９】

本発明を適用したルータの構成図



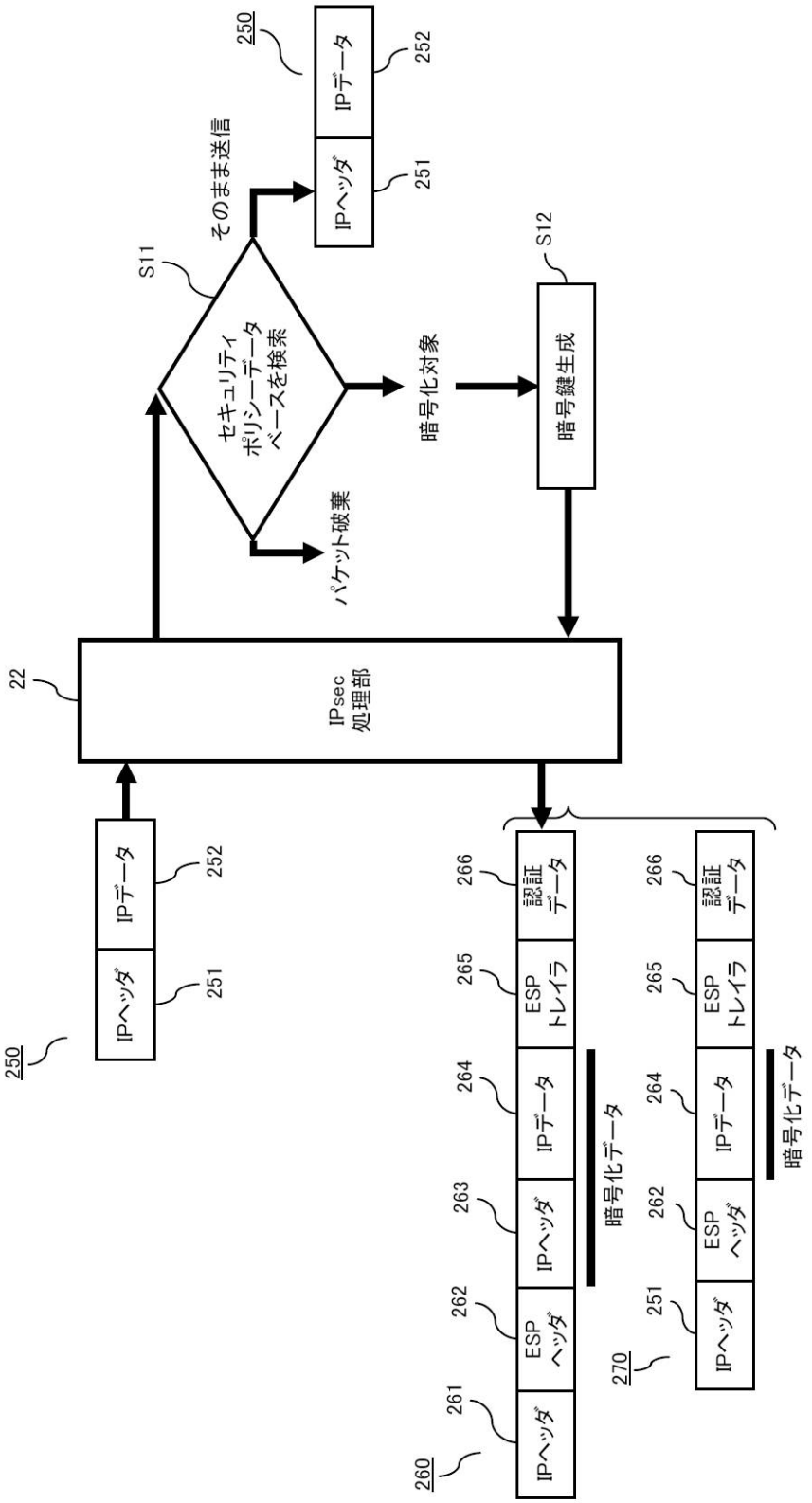
【図２０】

図19と図4の関係を説明する機能ブロック構成図



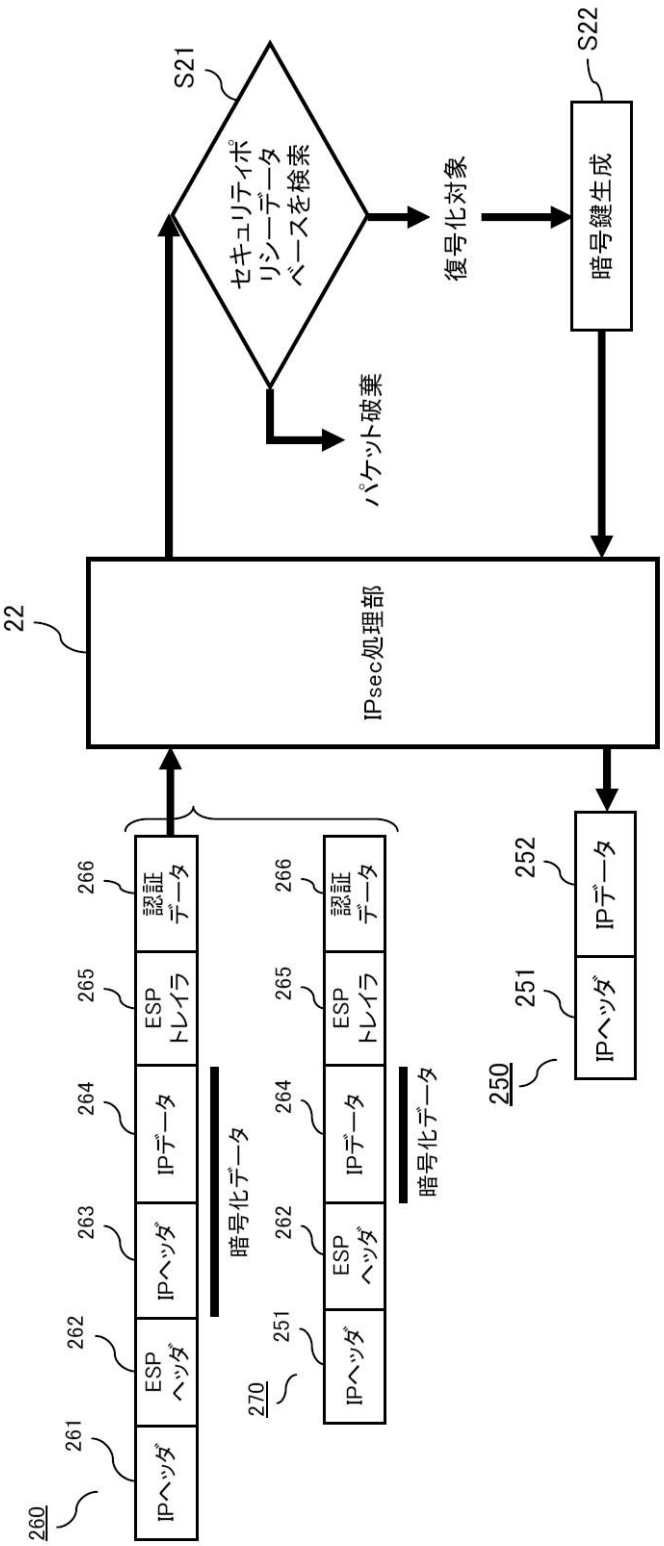
【図２１】

暗号化されていないIPパケットを受信したときのIPsec処理部の動作を説明する図



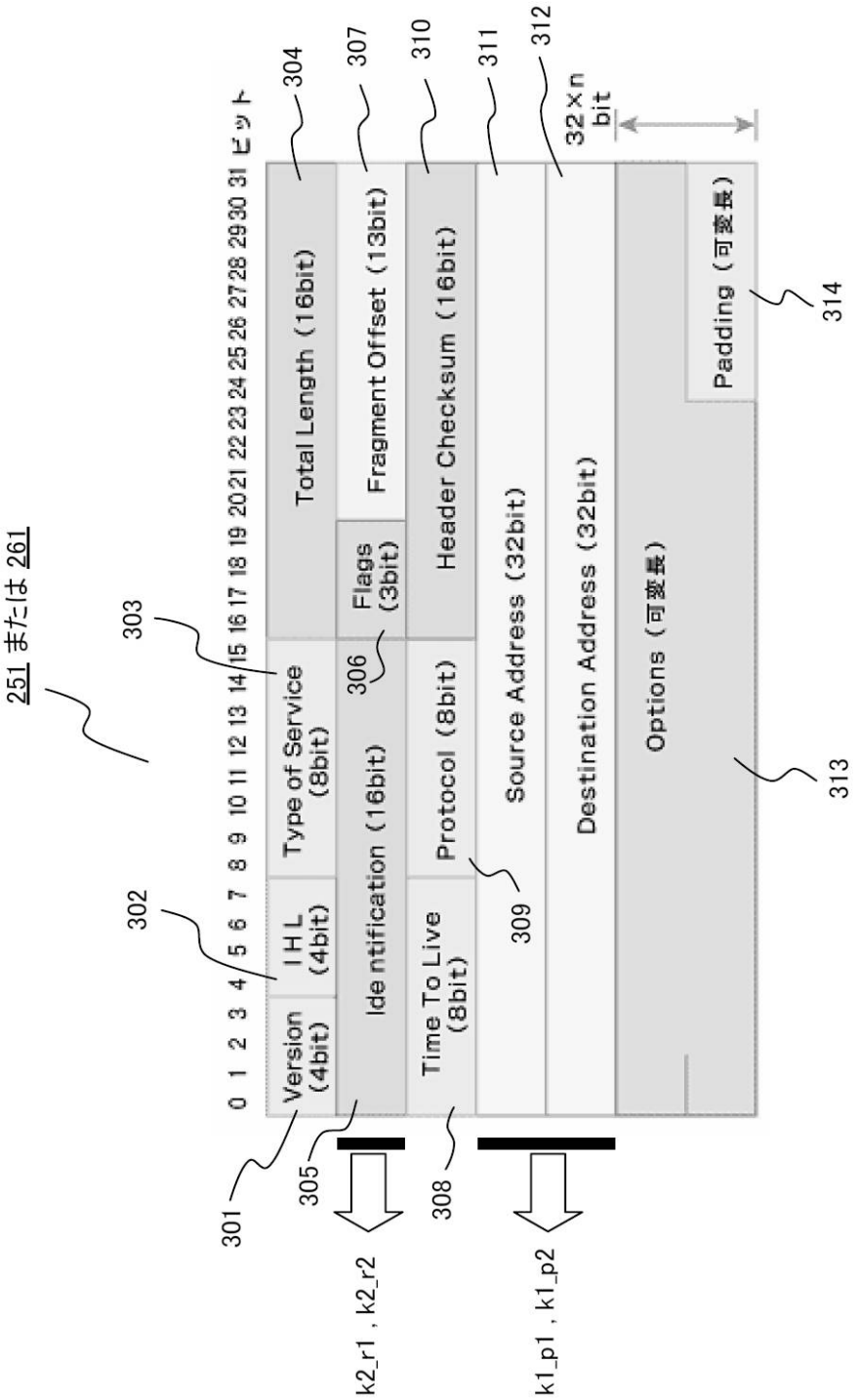
【図２２】

暗号化IPパケットを受信したときの
IPsec処理部の動作を説明する図



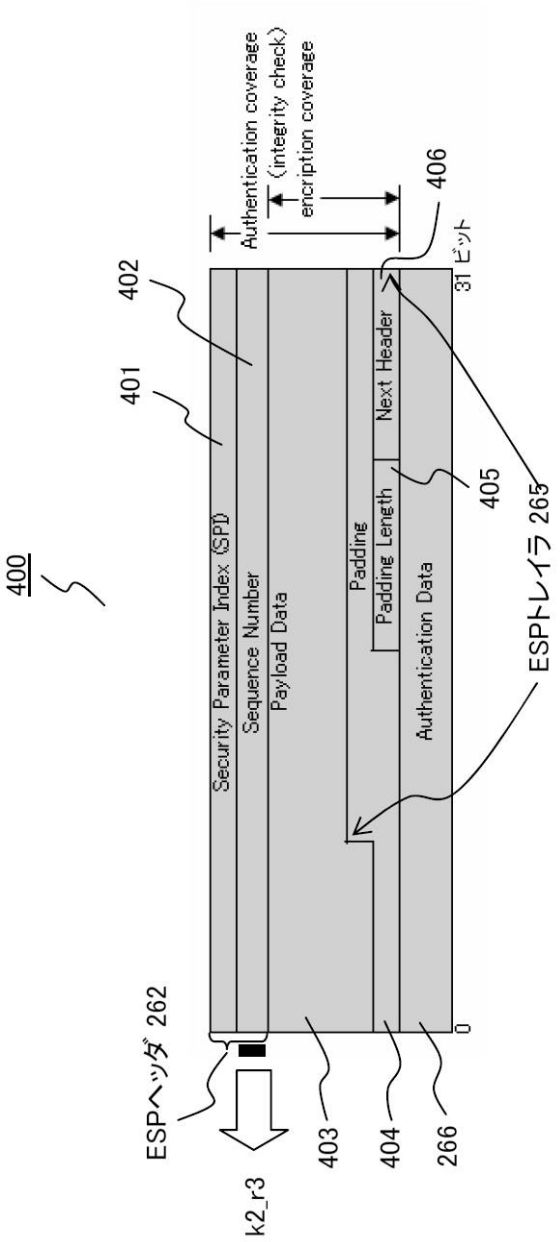
【図２３】

IPヘッダの形式を示す図



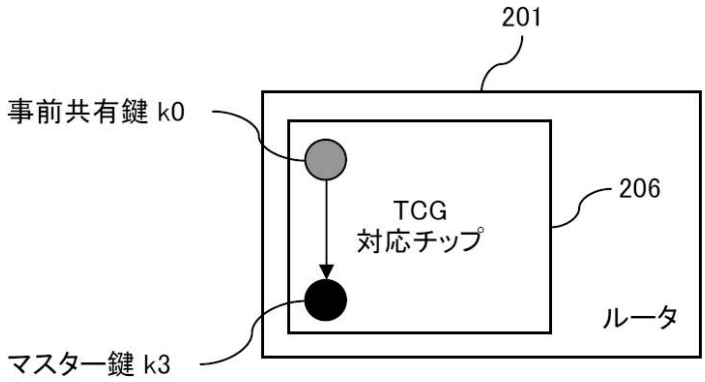
【図２４】

ESPパケットの形式を示す図



【図２５】

マスター鍵の生成について説明する図



マスター鍵は、
（１）ハッシュ関数などにより動的にまたは事前に生成する場合と、
（２）配列として事前に生成しておく場合、がある。

【図２６Ａ】

トランスポートモードにおける図3の各情報と
図23～図25との対応関係を説明する図

トランスポートモード		
局面	利用する情報	例
第一の局面	k1=k1_p1	PC4aとPC4dのIPアドレスを連結したビット列
	k2=k2_s=c(k2_s2, k2_r1)	カウンタの値k2_s2と、IPヘッダ251内のID305の値k2_r1とを連結したビット列
	k3	図25のマスター鍵k3
第二の局面	k1=k1_p1	PC4aとPC4dのIPアドレスを連結したビット列
	k2=k2_r=c(k2_r3, k2_r1)	ESPヘッダ262内のシーケンス番号402の値k2_r3と、IPヘッダ251内のID305の値k2_r1とを連結したビット列
	k3	図25のマスター鍵k3

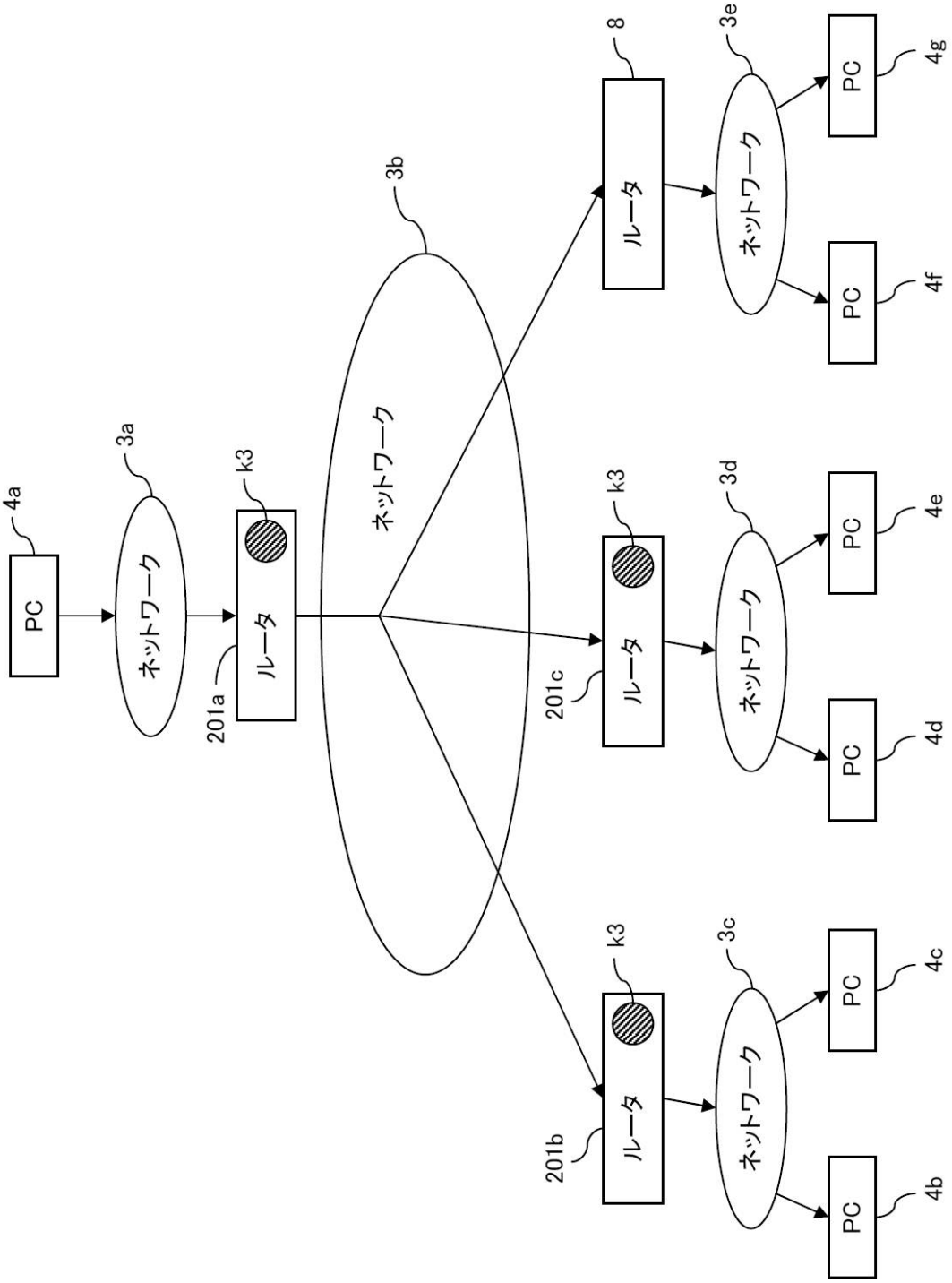
【図２６Ｂ】

トンネルモードにおける図3の各情報と
図23～図25との対応関係を説明する図

トンネルモード		
局面	利用する情報	例
第一の局面	k1=k1_p2	ルータ201aとルータ201bのIPアドレスを連結したビット列
	k2=k2_s=c(k2_s2, k2_r2)	カウンタの値k2_s2と、新たに付加するIPヘッダ261内のID305として生成した値k2_r2とを連結したビット列
	k3	図25のマスター鍵k3
第二の局面	k1=k1_p2	ルータ201aとルータ201bのIPアドレスを連結したビット列
	k2=k2_r=c(k2_r3, k2_r2)	ESPヘッダ262内のシーケンス番号402の値k2_r3と、IPヘッダ261内のID305の値k2_r2とを連結したビット列
	k3	図25のマスター鍵k3

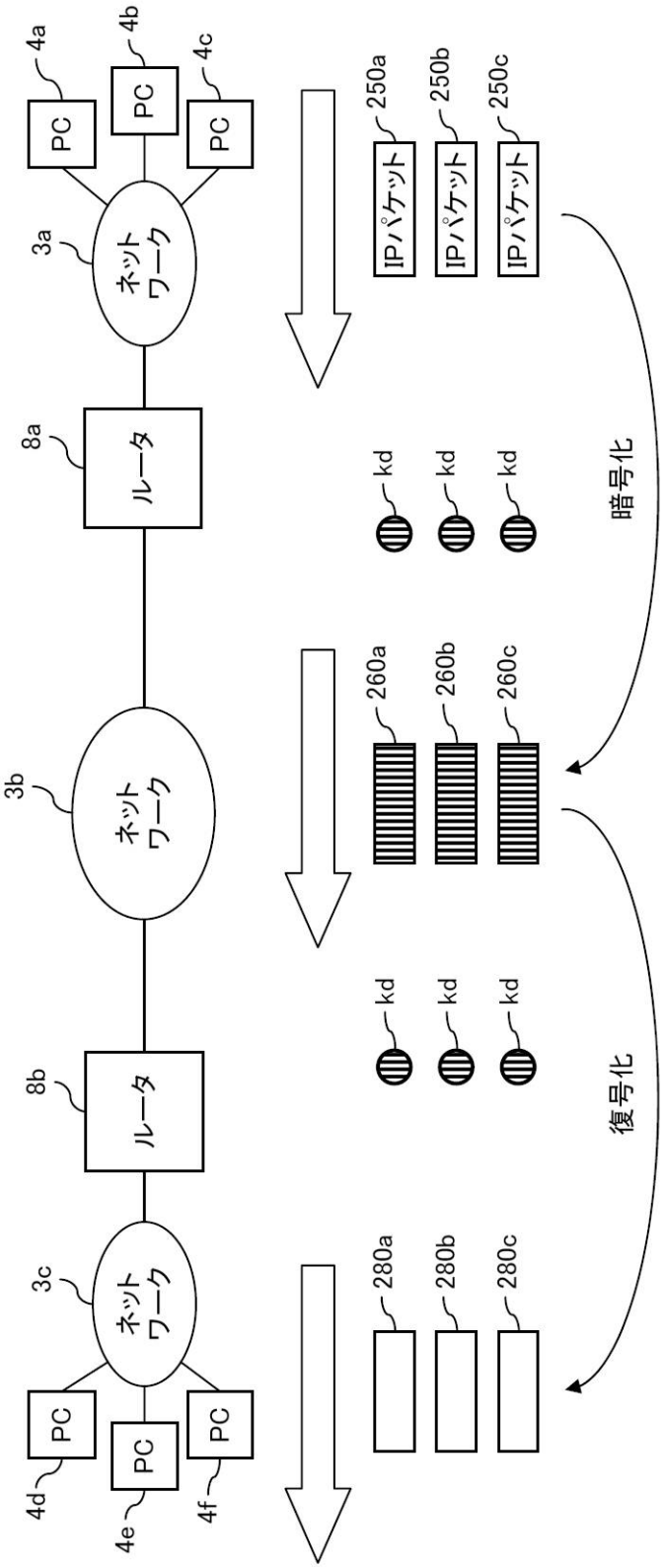
【図２７】

共通鍵生成装置を備えたルータを
マルチキャストに利用した例を示す図



【図２８】

IPsecを利用した従来の暗号化通信を示す模式図



フロントページの続き

(72)発明者　小原　聡史
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　中島　幸宏
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　佐久間　敬之
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

Ｆターム(参考) 5J104 EA23　PA07