(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第5060081号
(P5060081)

(45)発行日　平成24年10月31日(2012.10.31)　(24)登録日　平成24年8月10日(2012.8.10)

(51)Int.Cl.		F I		
H04L 9/36	(2006.01)	H04L	9/00	685
H04L 9/14	(2006.01)	H04L	9/00	641
H04L 12/56	(2006.01)	H04L	12/56	200Z

請求項の数 5　(全 37 頁)

(21)出願番号　特願2006-216737 (P2006-216737)
(22)出願日　平成18年8月9日 (2006.8.9)
(65)公開番号　特開2008-42715 (P2008-42715A)
(43)公開日　平成20年2月21日 (2008.2.21)
審査請求日　平成21年4月9日 (2009.4.9)

(73)特許権者　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(74)代理人　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】フレームを暗号化して中継する中継装置

(57)【特許請求の範囲】
【請求項１】
データリンク層のフレームを中継する第一、第二、および第三の中継装置を含むシステムであって、
前記第一、第二、および第三の中継装置の各々は、当該中継装置の外部と前記フレームの送受信を行うための複数のポートと、前記フレームを中継するフレーム中継処理部と、一つ以上の暗号処理部を備え、
前記一つ以上の暗号処理部の各々は、
前記複数のポートのうちの、当該暗号処理部と一対一に対応する、当該暗号処理部にとっての特定の一つのポート、および前記フレーム中継処理部と、接続されており、
前記特定の一つのポートとの間で前記フレームを送受信する第一のインターフェイス、および前記フレーム中継処理部との間で前記フレームを送受信する第二のインターフェイスを有し、
前記第一または第二のインターフェイスの一方から前記フレームを受信したとき該フレームを暗号化して暗号化フレームを生成する暗号化処理を行い、
前記第一または第二のインターフェイスの他方から前記暗号化フレームを受信したとき該暗号化フレームを復号化する復号化処理を行い、
前記第一の中継装置において、前記一つ以上の暗号処理部のうちの一つである第一の暗号処理部は、前記複数のポートのうち、前記第一の暗号処理部に対応する前記特定の一つのポートである第一のポートと接続されており、前記第一のインターフェイスからの受信

の際に前記復号化処理を行い、前記第二のインターフェイスからの受信の際に前記暗号化処理を行い、
前記第二の中継装置において、前記一つ以上の暗号処理部のうちの一つである第二の暗号処理部は、前記複数のポートのうち、前記第二の暗号処理部に対応する前記特定の一つのポートである第二のポートと接続されており、前記第一のインターフェイスからの受信の際に前記復号化処理を行い、前記第二のインターフェイスからの受信の際に前記暗号化処理を行い、
前記第三の中継装置の前記複数のポートは、
前記第一の中継装置の前記第一のポートに接続されるとともに、前記第三の中継装置の前記フレーム中継処理部に接続された第三のポートと、
前記第二の中継装置の前記第二のポートと接続されるとともに、前記第三の中継装置の前記フレーム中継処理部に接続された第四のポートと、
前記第三の中継装置における前記一つ以上の暗号処理部のうちの一つである第三の暗号処理部に対応する前記特定の一つのポートである第五のポートを含み、
前記第三の暗号処理部は、前記第一のインターフェイスからの受信の際に前記暗号化処理を行い、前記第二のインターフェイスからの受信の際に前記復号化処理を行う
ことを特徴とするシステム。
【請求項２】
前記暗号化処理において、前記暗号処理部は、前記フレームのヘッダを除くデータ部を暗号化し、前記ヘッダと、前記データ部を暗号化して得られた暗号化データとの間の位置に、復号化に必要な情報を含む暗号ヘッダを配置して暗号化フレームを生成することを特徴とする請求項１に記載のシステム。
【請求項３】
前記暗号処理部はシーケンス番号を格納する番号格納部を備え、
前記暗号化処理を行うとき、前記暗号処理部は、前記シーケンス番号に基づいて暗号鍵を生成し、該暗号鍵を使って前記フレームを暗号化して前記暗号化フレームを生成し、前記シーケンス番号を該暗号化フレームに含ませ、前記番号格納部に格納された前記シーケンス番号の値を変化させ、
前記復号化処理を行うとき、前記暗号処理部は、前記暗号化フレームに含まれる前記シーケンス番号に基づいて前記暗号鍵を生成し、該暗号鍵を使って前記復号化処理を行う、
ことを特徴とする請求項１に記載のシステム。
【請求項４】
前記第一、第二、および第三の中継装置の各々において予め設定された同一の値である事前共有鍵に基づいて、前記暗号処理部が２以上の整数であるＭ個の値を生成して候補値として記憶し、
前記暗号処理部は、Ｍ個の前記候補値のうちの一つを前記シーケンス番号に基づいて選択し、選択した前記候補値に基づいて前記暗号鍵を生成することを特徴とする請求項３に記載のシステム。
【請求項５】
前記暗号化処理において、前記暗号処理部はさらに、前記暗号化フレームを分割して複数のフラグメントフレームを生成し、
前記復号化処理において、前記暗号処理部はさらに、前記フラグメントフレームを受信したのか、それとも分割されていない前記暗号化フレームを受信したのかを判定し、前記フラグメントフレームを受信したと判定した場合には、分割前の前記暗号化フレームに対応する複数の前記フラグメントフレームのすべてを受信してから、該すべてのフラグメントフレームを分割前の前記暗号化フレームに再構成する、
ことを特徴とする請求項１に記載のシステム。
【発明の詳細な説明】
【技術分野】
【０００１】

本発明は、データリンク層のフレームを暗号化して中継することによって機密通信を実現する装置に関する。

【背景技術】

【０００２】

イーサネット（登録商標）は、１０Ｍｂｐｓ、１００Ｍｂｐｓ、１Ｇｂｐｓといった高速通信を実現し、かつＮＩＣ（Network Interface Card）、ハブ、スイッチ、ケーブルなどの通信用機器が安価で入手しやすいため、個人利用から企業の基幹業務システムまで広く用いられている。

【０００３】

イーサネット（登録商標）の仕様は、ＯＳＩ（Open Systems Interconnection）参照モデルにおける物理層（レイヤ１ともいう）およびデータリンク層（レイヤ２ともいう）の仕様を規定している。また、イーサネット（登録商標）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、ネットワーク層（レイヤ３ともいう）に近いほうがＬＬＣ（Logical Link Control）副層である。レイヤ２においてデータは、フレームという単位で送受信される。

【０００４】

上記のようにイーサネット（登録商標）は広く用いられているが、イーサネット（登録商標）における通信そのものは暗号化されていない。つまり、送受信されるフレームは暗号化されていない。よって、通信を傍受されたときには重要な情報が漏洩してしまう。

【０００５】

リピータハブを用いているときには、同一ハブに接続されているすべての端末が通信を傍受することが可能である。スイッチングハブを用いれば、通常は他の端末の通信を傍受することはできないが、ＡＲＰ（Address Resolution Protocol）スプーフィングやＭＡＣフラッディングなどの攻撃手法を使うことで、容易に傍受が可能となる。このことから、イーサネット（登録商標）通信を暗号化し、通信内容を秘匿する必要性が生じている。

【０００６】

イーサネット（登録商標）通信を暗号化すること自体は、既存のプロトコル利用することで可能であり、以下に説明するようにいくつかの方法があるが、いずれも問題がある。

第一の方法は、非特許文献１に記載されたＩＰｓｅｃと非特許文献２に記載されたＥｔｈｅｒＩＰとを組み合わせる方法である（「EtherIP over IPsec」ともよばれる）。

【０００７】

ＩＰｓｅｃはインターネット通信をセキュアにするアーキテクチャであり、ＩＰ（Internet Protocol）パケットを暗号化する技術が含まれる。また、ＥｔｈｅｒＩＰは、ＩＰ上でイーサネット（登録商標）通信を実現する方式である。よって、ＩＰｓｅｃとＥｔｈｅｒＩＰを組み合わせて使用することで、イーサネット（登録商標）通信を暗号化することができる。

【０００８】

第二の方法は、非特許文献１に記載されたＩＰｓｅｃと非特許文献３に記載されたＬ２ＴＰｖ３とを組み合わせる方法である。Ｌ２ＴＰｖ３は、ＩＰ上でレイヤ２フレームを伝送する方式である。よって、ＩＰｓｅｃとＬ２ＴＰｖ３を組み合わせて使用することで、イーサネット（登録商標）通信を暗号化することができる。

【０００９】

第三の方法は、ＩＥＥＥ８０２．１ＡＥとして規格化するための準備が行われている方法であり、ＭＡＣ副層を暗号化する方法である。ＭＡＣ副層を暗号化することにより、イーサネット（登録商標）通信を暗号化することができる。

【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７月２８日）

【非特許文献２】RFC3378 EtherIP: Tunneling Ethernet（登録商標） Frames in IP Datagrams http://www.ietf.org/rfc/rfc3378.txt （閲覧確認：２００６年７月２８日）

【非特許文献３】RFC 3931 Layer Two Tunneling Protocol - Version 3 (L2TPv3) http://www.ietf.org/rfc/rfc3931.txt （閲覧確認：２００６年７月２８日）
【発明の開示】
【発明が解決しようとする課題】
【００１０】
しかし、上記第一の方法には次の問題がある。
（ａ）ＥｔｈｅｒＩＰでは特定の宛先にしかイーサフレームを転送できないため、１対１の通信トポロジに限定されてしまう。つまり、この方法では、１対１に対応する１組のスイッチ間での通信を暗号化することしかできない。しかし、一般的なオフィスＬＡＮ（Local Area Network）においては、Ｎ対Ｎの通信が行われることが多い。
（ｂ）ＥｔｈｅｒＩＰはブリッジ動作ではないため、ＭＡＣアドレスが学習されず、無駄な転送を防ぐことができない。したがって、無駄なトラフィックが生じる。
（ｃ）ルーティングが必要なＩＰと、鍵交換が必要なＩＰｓｅｃと、ＥｔｈｅｒＩＰと、という複雑なプロトコルスタックを使うため、構成定義が複雑である。よって、通信機器の運用保守も容易ではない。
（ｄ）プロトコルスタックが複雑なため、ハードウェア化することが困難である。一方、ソフトウェアで実現すると処理に時間がかかる。よって、Ｇｂｐｓ級の性能を実現するのは困難である。
【００１１】
また、上記第二の方法も第一の方法と同様の問題がある。
また、上記第三の方法には次の問題がある。
（ｅ）暗号通信をする相手のスイッチを識別する必要があり、かつ相手のスイッチごとに鍵交換プロトコルを使って鍵を交換する必要がある。よって、複数のスイッチがＮ対Ｎの関係で暗号化通信を行うトポロジには処理が複雑になりすぎるために適さない。
（ｆ）暗号化の粒度が物理的なインターフェイス単位である。つまり、特定の二つのスイッチ間で送受信されるフレームがすべて暗号化されるか、すべて暗号化されないか、のいずれかである。よって、ＶＬＡＮ（Virtual LAN）ごとに暗号化するか否かを選択するなど、より細かい粒度に対応することができない。
【００１２】
本発明の目的は、中継速度を損なわない構成、かつＮ対Ｎの関係の暗号化通信に適した構成を有した、データリンク層のフレームを暗号化して中継する中継装置を提供することである。
【課題を解決するための手段】
【００１３】
本発明による中継装置は、データリンク層のフレームを中継する中継装置であって、該中継装置の外部と前記フレームの送受信を行うための複数のポートと、前記フレームを中継するフレーム中継処理部と、一つ以上の暗号処理部とを有する。該暗号処理部は、前記複数のポートのうちの一つとの間で前記フレームを送受信する第一のインターフェイス、および前記フレーム中継処理部との間で前記フレームを送受信する第二のインターフェイスを有する。また、該暗号処理部は、前記第一または第二のインターフェイスの一方から前記フレームを受信したとき該フレームを暗号化して暗号化フレームを生成する暗号化処理を行い、前記第一または第二のインターフェイスの他方から前記暗号化フレームを受信したとき該暗号化フレームを復号化する復号化処理を行う。
【００１４】
また、前記暗号処理部がシーケンス番号を格納する番号格納部を備え、該シーケンス番号を前記暗号化処理および前記復号化処理に利用することが望ましい。つまり、前記暗号化処理を行うとき、前記暗号処理部は、前記シーケンス番号に基づいて暗号鍵を生成し、該暗号鍵を使って前記フレームを暗号化して前記暗号化フレームを生成し、前記シーケンス番号を該暗号化フレームに含ませ、前記番号格納部に格納された前記シーケンス番号の値を変化させることが望ましい。そして、前記復号化処理を行うとき、前記暗号処理部は

、前記暗号化フレームに含まれる前記シーケンス番号に基づいて前記暗号鍵を生成し、該暗号鍵を使って前記復号化処理を行うことが望ましい。

【発明の効果】

【００１５】

本発明によれば、中継装置が暗号処理部を有するのでフレームを暗号化して中継することができる。

また、暗号化処理および復号化処理は、フレーム中継処理部とは独立した暗号処理部において行われるので、フレーム中継処理部は単純に中継処理のみを行えばよい。したがって、フレーム中継処理部で暗号化処理および復号化処理を行う装置と比べて、本発明の中継装置は中継速度を高速に保つことができる。

【００１６】

また、各暗号処理部は、複数のポートのうちの一つと対応して配置されているが、一つの中継装置に設ける暗号処理部の数や、どのポートに対応させて暗号処理部を設けるかという点については、利用者の都合に合わせて任意に選択することができる。よって、様々なネットワーク構成で本発明を利用することができる。

【００１７】

また、上記のようにシーケンス番号に基づいた暗号鍵を利用することにより、動的な鍵情報の交換を不要とし、かつ比較的簡易な構成で暗号鍵を生成することが可能となる。よって、暗号化処理および復号化処理が中継装置全体の中継速度を低下させる度合いは小さい。

【発明を実施するための最良の形態】

【００１８】

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す。

また、レイヤ２で送受信されるフレームには、例えばＤＩＸイーサネット（登録商標）のＭＡＣフレームやＩＥＥＥ８０２．３のＭＡＣフレームがある。これらは、細かい点で異なるがほぼ同一の形式であり、本発明においてその区別は重要ではない。よって、以下ではこれらのＭＡＣフレームの総称として単に「フレーム」という表現をする。

【００１９】

図１は本発明による中継装置の一実施形態における構成図である。図１の中継装置１を利用することにより、中継装置（スイッチ）間でフレームを暗号化し、機密通信を実現することができる。従来のイーサネット（登録商標）通信は暗号処理がなされないだけでなく、盗聴自体が容易であるという弱点がある。しかし、本発明の中継装置１を利用すればフレームが暗号化されるため、盗聴されても機密性を保持することができる。

【００２０】

本発明による中継装置１はフレームを中継するスイッチ装置であり、具体的には例えばスイッチングハブである。すなわち、中継装置１はレイヤ２の中継機能をもち、Ｌ２スイッチの一種である。中継装置１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（図１では四つのポート３ａ～３ｄがある）、およびフレームを中継するフレーム中継処理部２を備えるという点は、従来の装置と同様である。

【００２１】

中継装置１は、各ポート３ａ～３ｄに対応した暗号処理モジュール４ａ～４ｄをさらに備えている。暗号処理モジュール４ａ～４ｄ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４ａ～４ｄはそれぞれ、対応するポート３ａ～３ｄおよびフレーム中継処理部２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４ａ～４ｄ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（登録商標）で一般的に使われている。

【００２２】

なお、詳しくは後述するが、暗号処理モジュール４ａ～４ｄが行う暗号処理は、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。

【００２３】

また、中継装置１は、ＴＣＧ（Trusted Computing Group）の仕様に準拠したＴＣＧ対応チップ５を搭載している。ＴＣＧ対応チップ５には、後述する事前共有鍵ｋ０やファーム文字列ｆｓなどのデータが格納される。これらのデータは暗号鍵に関するデータであり、暗号処理モジュール４ａ～４ｄにより利用される。ＴＣＧ対応チップ５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５を使うと安全にデータを格納することができる。

【００２４】

また、中継装置１はＣＰＵ（Central Processing Unit）６を備える。ＣＰＵ６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、ＣＰＵ６は、暗号処理モジュール４ａ～４ｄ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。

【００２５】

フレーム中継処理部２、暗号処理モジュール４ａ～４ｄ、ＴＣＧ対応チップ５、ＣＰＵ６、ＲＯＭ、ＲＡＭは、内部バス７に接続されている。

中継装置１の特徴の一つは、フレーム中継処理部２と暗号処理モジュール４ａ～４ｄが分かれていることである。これにより、フレーム中継処理と暗号処理が切り離されるため、中継処理が容易となり、中継速度の性能を出すことができる。

【００２６】

従来の装置にはフレーム中継処理部において暗号処理を行う装置があるが、そのような装置では、中継処理が複雑になり中継速度の性能を保つことが難しかった。なぜなら、中継すべきすべてのフレームに対して、そのフレームが暗号化対象か否かを判別する処理や、使用する暗号鍵を読み出す処理などを行う必要があるためである。

【００２７】

一方、本発明の中継装置１は、物理的なポート３ａ～３ｄそれぞれに対応して暗号処理モジュール４ａ～４ｄが配備され、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。よって、本発明の中継装置１においてフレーム中継処理部２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と同様の動作をするだけでよい。

【００２８】

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２と暗号処理モジュール４ａ～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１のフレーム中継処理部２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。

【００２９】

また、中継装置１の別の特徴は、各ポート３ａ～３ｄに対応して暗号処理モジュール４ａ～４ｄを備えていることである。EtherIP over IPsecなどの従来の方法は、フレームの転送先が一つに限定され、１対１の関係で暗号通信を行う二つのスイッチ間でしか使うことができなかった。しかし本発明の中継装置１を使うことにより、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（登録商標）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通信を行うことを意味している。

【００３０】

図２は本発明による中継装置の別の実施形態における構成図である。図２と図１の違いは、図２では一部のポート（３ａ、３ｂ）にのみ暗号処理モジュール４ａ、４ｂが備えられている点である。他のポート（３ｃ～３ｊ）は、直接フレーム中継処理部２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、本発明の中継装置１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。

【００３１】

なお、フレーム中継処理部２は、暗号処理モジュール４ａ、４ｂ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３ｃ～３ｊ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２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。

【００３２】

図３Ａは、ＶＬＡＮ環境における本発明の中継装置の利用例を示す。また、図３Ｂは、図３Ａ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３Ａは、ＶＬＡＮ１０、２０、３０という三つのＶＬＡＮを含むネットワーク構成を示している。

【００３３】

図３Ａにおいて、中継装置１ａ、１ｂは、図１または図２の中継装置１と同様の装置である。なお、本発明の中継装置１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３Ａ以降では「Ｌ２ＳＷ」と表記することがある。中継装置１ａ、１ｂにはそれぞれ、ＶＬＡＮ１０、２０、３０に属する端末（コンピュータ）が接続されている。つまり、中継装置１ａ、１ｂは端末と接続されているエッジスイッチである。

【００３４】

また、従来の中継装置であるコアＬ２／Ｌ３スイッチ４１（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、中継装置１ａ、１ｂ、およびファイヤウォール４３が接続されている。つまり、コアＬ２／Ｌ３スイッチ４１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４３はルータ４４に接続され、ルータ４４はインターネット４５に接続されている。

【００３５】

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３Ａの例においては、中継装置１ａ、コアＬ２／Ｌ３スイッチ４１、中継装置１ｂ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、ＶＬＡＮ１０、２０、３０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。

【００３６】

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、中継装置１ａからコアＬ２／Ｌ３スイッチ４１へ送られるすべてのフレームを暗号処理モジュール４ａ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。

【００３７】

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４５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４５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３Ａのような構成とすることがある。つまり、部署ＡがＶＬＡＮ１０に、部署ＢがＶＬＡＮ２０に、部署ＣがＶＬＡＮ３０に対応する。

【００３８】

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、ＶＬＡＮ１０、２０を暗号化の対象とし、ＶＬＡＮ３０は暗号化の対象外とすることができる。また、図３Ａに示すように、本発明による中継装置１ａ、１ｂと従来の中継装置であるコアＬ２／Ｌ３スイッチ４１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。

【００３９】

図３Ｂに抜粋して示したように、中継装置１ａにはポート３ａ～３ｄがあり、ポート３ａはＶＬＡＮ１０に、ポート３ｂはＶＬＡＮ２０に、ポート３ｃはＶＬＡＮ３０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３ｄはコアＬ２／Ｌ３スイッチ４１と接続されたポートである。中継装置１ａの内側では、ポート３ｄが暗号処理モジュール４ａ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３ａ～３ｃおよび暗号処理モジュール４ａは、それぞれフレーム中継処理部２ａとＧＭＩＩやＭＩＩ等のインターフェイスで接続されている。

【００４０】

同様に、中継装置１ｂはポート３ｅ～３ｈを備えており、ポート３ｅはＶＬＡＮ１０に、ポート３ｆはＶＬＡＮ２０に、ポート３ｇはＶＬＡＮ３０に、それぞれ割り当てられている。また、ポート３ｈはコアＬ２／Ｌ３スイッチ４１と接続されたポートである。

【００４１】

なお、表示の便宜上、図３Ａでは中継装置１ａ、１ｂを示す矩形の外側に暗号処理モジュール４ａ、４ｂを表示しているが、実際の構成は図１、図２、図３Ｂ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３Ａと同様の表現をすることがある。また、図３Ｂでは、中継装置１ａ、１ｂの構成要素のうち、ＴＣＧ対応チップなどは省略している。

【００４２】

同一のＶＬＡＮ内で図３Ａ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、フレームは中継装置１ａ、コアＬ２／Ｌ３スイッチ４１、中継装置１ｂを経由する。図３Ｂ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２ａ、暗号処理モジュール４ａ、ポート３ｄ、コアＬ２／Ｌ３スイッチ４１、ポート３ｈ、暗号処理モジュール４ｂ、フレーム中継処理部２ｂ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３Ｂにおいてフレーム中継処理部２ａより左側の部分とフレーム中継処理部２ｂより右側の部分のみである。

【００４３】

また、図３Ａおよび図３Ｂでは、上記のごとく、ＶＬＡＮ３０に所属する端末はインターネット４５との通信を行うと仮定している。このインターネット４５との通信は、図３Ａにおいて、二つの黒い矢印（中継装置１ａから出発して、コアＬ２／Ｌ３スイッチ４１、ファイヤウォール４３、ルータ４４を経由し、インターネット４５へ向かう矢印、および中継装置１ｂから出発して、コアＬ２／Ｌ３スイッチ４１、ファイヤウォール４３、ルータ４４を経由してインターネット４５へ向かう矢印）により示される。

【００４４】

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４５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３ｄとコアＬ２／Ｌ３スイッチ４１の間、および／またはポート３ｈとコアＬ２／Ｌ３スイッチ４１の間を経由する。つまり、ポート３ｄとコアＬ２／Ｌ３スイッチ４１の間、およびポート３ｈとコアＬ２／Ｌ３スイッチ４１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（４２ａおよび４２ｂ）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。

【００４５】
また、ポート３ａ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３ｄやポート３ｈは複数のＶＬＡＮで共有されている。ポート３ｄやポート３ｈは、「タグＶＬＡＮポート（tagged VLAN port）」とよばれる。管理者はポート３ｄとポート３ｈ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３ｄとポート３ｈの間（より正確には、フレーム中継処理部２ａとフレーム中継処理部２ｂ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４とあわせて後述する）。

【００４６】
上記のごとく、図３Ａの例では、ＶＬＡＮ１０とＶＬＡＮ２０が暗号化の対象であり、ＶＬＡＮ３０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、中継装置１ａに入力する。すると、図３Ｂには示されていないＣＰＵ（図１のＣＰＵ６に相当する）が、暗号処理モジュール４ａに対して、入力された内容を設定するよう命令する。中継装置１ｂに関しても同様である。その結果、暗号処理モジュール４ａ、４ｂ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。

【００４７】
例えば、図３Ｂの左から右へＶＬＡＮ１０内でフレームを送信する場合、ポート３ａで受信されたフレーム（ポート３ａ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２ａを経由して暗号処理モジュール４ａに送信される。暗号処理モジュール４ａ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であると判断し、このフレームを暗号化する。そして、暗号化されたフレームは、ポート３ｄ、コアＬ２／Ｌ３スイッチ４１、ポート３ｈを経由して、暗号処理モジュール４ｂに送信される。暗号処理モジュール４ｂ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、このフレームが復号化の対象であると判断する（あるいは、後述する暗号ヘッダ７１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断する）。そして、暗号処理モジュール４ｂがこのフレームを復号化する。復号化されたフレームは、フレーム中継処理部２ｂへ送信され、ポート３ｅへ中継される。そしてポート３ｅから、ポート３ｅに接続された端末に送信される。

【００４８】
つまり、端末からポート３ａを経由して暗号処理モジュール４ａまでの経路、および暗号処理モジュール４ｂからポート３ｅを経由して端末までの経路では、フレームは平文（クリアテキストともいう）の状態で送信される。一方、暗号処理モジュール４ａと暗号処理モジュール４ｂの間では、フレームは暗号化された状態で送信される。ＶＬＡＮ２０内でフレームを送信する場合も同様である。

【００４９】
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３Ｂ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。

【００５０】
図３Ｂの左から右へＶＬＡＮ３０内でフレームを送信する場合、暗号処理モジュール４ａ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３ｄに送信する。また、暗号処理モジュール４ｂ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７１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２ｂに送信する。

【００５１】

ＶＬＡＮ３０に属するコンピュータがインターネット４５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３ｄまたはポート３ｈを経由する。例えば中継装置１ａ内では、ＶＬＡＮ３０に対応するポート３ｃがフレーム中継処理部２ａに接続され、フレーム中継処理部２ａが暗号処理モジュール４ａに接続され、暗号処理モジュール４ａがポート３ｄ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４ａを経由する。

【００５２】

しかし、ＶＬＡＮ３０に対応するポート３ｃで受信したフレームをポート３ｄに中継する場合、暗号処理モジュール４ａは、ＶＬＡＮ３０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３ｄに送信する。このことは、図３Ｂにおいて、実線の矢印（平文フレームの送信を示す）が、中継装置１ａからコアＬ２／Ｌ３スイッチ４１を経由してファイヤウォール４３に向かっていることに対応する。

【００５３】

上記のように図３Ａ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３ｄとコアＬ２／Ｌ３スイッチ４１の間の．１Ｑトランク４２ａ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３Ａ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、本発明の利点である。

【００５４】

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４ａ、４ｂに対して設定することができるため、本発明では、中継装置１ａと中継装置１ｂの間に従来の中継装置であるコアＬ２／Ｌ３スイッチ４１を介在させ、コアＬ２／Ｌ３スイッチ４１を直接ファイヤウォール４３に接続することが可能である。

【００５５】

仮にＶＬＡＮごとの設定ができないとすると、図３Ａにおいて、ＶＬＡＮ３０に属する端末がインターネット４５と通信を行う際にも、フレームが暗号処理モジュール４ａ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４３の外に送信するためには、本発明の中継装置１をコアＬ２／Ｌ３スイッチ４１とファイヤウォール４３との間に介在させる必要がある。

【００５６】

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。

【００５７】

図４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４の上段に示したフレーム５０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５０は、６バイトの送信先ＭＡＣアドレス５１、６バイトの送信元ＭＡＣアドレス５２、データ部５３、４バイトのエラー検出用のＦＣＳ（Frame Check Sequence）５４からなる。

【００５８】

ＤＩＸイーサネット（登録商標）のＭＡＣフレームの場合、データ部５３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５３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。

【００５９】
図４の中段に示したタグつきフレーム６０は、フレーム５０にＶＬＡＮタグが挿入されたものである。タグつきフレーム６０は、送信元ＭＡＣアドレス５２とデータ部５３の間に、２バイトのＴＰＩＤ（Tag Protocol Identifier）６１と２バイトのＴＣＩ（Tag Control Information）６２が挿入されている他は、フレーム５０と同様である。イーサネット（登録商標）の場合、ＶＬＡＮを示すＴＰＩＤ６１の値は０ｘ８１００（１６進数で８１００の意）である。ＴＣＩ６２は、ＶＬＡＮを識別するための１２ビットのＶＬＡＮ‐ＩＤを含む。ＴＰＩＤ６１やＴＣＩ６２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、ＦＣＳ５４の再計算も中継装置で行われる。

【００６０】
図３Ａ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、ＴＣＩ６２に含まれるＶＬＡＮ‐ＩＤの値に基づいて、暗号処理モジュール４が暗号処理の要否を判定する。

【００６１】
図４の下段に示した暗号化フレーム７０は、タグつきフレーム６０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７０をタグつきフレーム６０と比較すると、ＴＣＩ６２の直後に暗号ヘッダ７１が挿入される点、データ部５３が暗号化されて暗号化データ部７２となる点、暗号化データ部７２の直後にＩＣＶ（Integrity Check Value）７３が挿入されている点で異なっている。暗号ヘッダ７１は、復号化に必要な情報（例えば鍵に関する情報。詳しくは後述する）を含む。ＩＣＶ７３は、送信先ＭＡＣアドレス５１から暗号化データ部７２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４は、ＦＣＳ５４の再計算も行う。

【００６２】
暗号化フレーム７０の第一の特徴は、データ部５３のみが暗号化され、ＭＡＣヘッダ（送信先ＭＡＣアドレス５１と送信元ＭＡＣアドレス５２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７１がＴＣＩ６２よりも後にある点である。

【００６３】
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５１には端末ＹｔのＭＡＣアドレスが書かれ、送信元ＭＡＣアドレス５２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５１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５２としてスイッチＸｓのＭＡＣアドレスが書かれる。

【００６４】
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。

【００６５】
一方、本発明による暗号化フレーム７０では、送信先ＭＡＣアドレス５１と送信元ＭＡ

ＣアドレスＳ２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。

【００６６】

また、フレーム中継処理部２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１や図２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２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（４ａ等）にオフロードすることができる。

【００６７】

次に、暗号ヘッダ７１がＴＣＩ６２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、本発明による中継装置１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。

【００６８】

イーサネット（登録商標）通信を暗号化する従来の方法のうち上記第三の方法では、ＭＡＣヘッダの直後（つまり送信元ＭＡＣアドレスＳ２の直後）に暗号化のためのヘッダを挿入する方式が検討されている。この方式では、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６０が所属するＶＬＡＮを判別することができない。なぜなら、判別に必要な情報であるＴＣＩ６２は、挿入されたヘッダの後に、暗号化された状態で配置されているからである。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、上記第三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。

【００６９】

一方、本発明による暗号化フレーム７０は、平文の状態のＴＰＩＤ６１およびＴＣＩ６２の後に、暗号ヘッダ７１と暗号化データ部７２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７０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、本発明の中継装置１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。

【００７０】

なお、図１や図２に示した本発明による中継装置１におけるフレーム中継処理部２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２は、図４の暗号化フレーム７０を単なるタグつきフレーム６０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２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２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。

【００７１】

なお、ＶＬＡＮを使わない環境においては、タグつきフレーム６０ではなくフレーム５０を暗号化する。よって、その場合の暗号化フレームは、図４の暗号化フレーム７０からＴＰＩＤ６１とＴＣＩ６２を除いた形式となる。

【００７２】

図５は、暗号ヘッダ７１の詳細を示す図である。図４に示したとおり暗号ヘッダ７１の長さは１２バイトである。暗号ヘッダ７１は図５に示すごとく、先頭から順に、２バイトのタイプ７１１、１バイトのサブタイプ７１２、１バイトの予約フィールド７１３、８バ

イトのシーケンス番号７１４からなる。

【００７３】

タイプ７１１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７１１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７１１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。

【００７４】

図４と図５とから分かるとおり、ＶＬＡＮを使用する環境ではタイプ７１１はＴＣＩ６２の直後にあり、ＶＬＡＮを使用しない環境ではタイプ７１１は送信元ＭＡＣアドレス５２の直後にある。したがって、フレーム５０またはタグつきフレーム６０におけるタイプ（データ部５３の先頭にある）と、暗号化フレーム７０におけるタイプ７１１とは、同じ位置にある。よって、タイプ７１１の値によって暗号ヘッダ７１の有無を判別する必要がある。

【００７５】

ところで、フレーム５０やタグつきフレーム６０においてデータ部５３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５３はＩＰの形式にしたがったデータである。

【００７６】

よって、タイプ７１１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７１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ＴＣＩ６２の直後の２バイトの値がＺなら暗号ヘッダ７１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５２の直後の２バイトの値がＺなら暗号ヘッダ７１があると判定することができる。

【００７７】

このようにして暗号ヘッダ７１の有無を判定可能とすることにより、例えば、図３Ｂにおいてポート３ｈからフレームを受信した暗号処理モジュール４ｂ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７１の有無に基づいて判断することができるようになる。

【００７８】

サブタイプ７１２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７１１とサブタイプ７１２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７１１がＺでサブタイプ７１２の値が０ｘ０１のとき、イーサネット（登録商標）の暗号化通信を行っており、暗号ヘッダ７１に暗号化データ部７２が続くことを表す」などと決めることができる。

【００７９】

予約フィールド７１３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１１とあわせて後述する。

シーケンス番号７１４は、暗号処理モジュール４がフレームを暗号化して送信するたびに１ずつ増加する番号を格納するフィールドである（暗号処理モジュール４のこの動作については図９とあわせて後述する）。シーケンス番号７１４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。

【００８０】

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７１４は事実上ユニークと考えてよい。

【００８１】

ただし、二つ以上の暗号化モジュール４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４におけるシーケンス番号の開始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化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。

【００８２】

図６Ａから図８Ｂは、本発明による中継装置１を使ったネットワークの構成例を示す。本発明による中継装置１は、図１と図２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（４ａ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。

【００８３】

これらの変化の組み合わせによって、中継装置１の価格や、レイヤ２の暗号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。

【００８４】

図６Ａ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中継装置１ａ～１ｅと従来のＬ２スイッチ４１ｂのみを用いている。図６Ｂは図６Ａ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６Ｂでは、図３Ｂと同様に、ＴＣＧ対応チップ等の構成要素は省略している。

【００８５】

図６Ａでは、四台のＰＣ（Personal Computer）４６ａ～４６ｄが本発明による中継装置１ａ～１ｄにそれぞれ接続されている。中継装置１ａ～１ｄはいずれも、暗号処理を行わない従来のＬ２スイッチ４１ｂに接続されている。そしてＬ２スイッチ４１ｂは本発明による中継装置１ｅ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６Ａ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、中継装置１ａと１ｂのペア、中継装置１ａと１ｃのペア、中継装置１ａと１ｄのペア、中継装置１ｂと１ｃのペア、中継装置１ｂと１ｄ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。

【００８６】

中継装置１ａ～１ｄのそれぞれは、Ｌ２スイッチ４１ｂと接続されたポートに対応して暗号処理モジュール４ａ～４ｄ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。中継装置１ｅは、Ｌ２スイッチ４１ｂと接続されたポートに対応して暗号処理モジュール４ｅが備えられているが、中継装置１ｅ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。中継装置１ｅはファイヤウォール４３とも接続されており、ファイヤウォール４３はルータ４４に接続されている。インターネット４５など外部のネットワークとの通信は、ルータ４４を介して行われる。

【００８７】

図６Ａにおける中継装置１ａ～１ｅ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６Ａの暗号処理モジュール４ａ～４ｅ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。例えば、図６Ｂに示すように、暗号処理モジュール４ａに対応するポートはポート３ｂである。暗号処理モジュール４ａは、フレームをフレーム中継処理部２ａから受信してポート３ｂに送信するときに暗号化し、フレームをポート３ｂから受信してフレーム中継処理部２ａに送信するときに復号化する。

【００８８】

次に、ＰＣ４６ａからＰＣ４６ｂにフレームを送信する場合について図６Ｂを参照して説明する。中継装置１ａは、ポート３ａを介してＰＣ４６ａと接続され、ポート３ｂを介してＬ２スイッチ４１ｂと接続されている。まず、ＰＣ４６ａが図４のフレーム５０（平文フレーム）を送信すると、このフレーム５０はポート３ａで受信され、フレーム中継処

理部２ａによって、暗号処理モジュール４ａが備えられたポート３ｂへと中継される。その際、フレーム５０が暗号処理モジュール４ａを経由し、ここで暗号化される。

【００８９】

図６Ａの例ではＶＬＡＮを利用していないため、暗号化フレームは、図４の暗号化フレーム７０からＴＰＩＤ６１とＴＣＩ６２を削除した形式である。暗号化フレームは、中継装置１ａのポート３ｂからＬ２スイッチ４１ｂのポート３ｅに送信される。

【００９０】

Ｌ２スイッチ４１ｂが暗号化フレームをポート３ｅで受信すると、暗号化フレームはフレーム中継処理部２ｃに送信され、フレーム中継処理部２ｃが、中継装置１ｂに接続されたポート３ｆにその暗号化フレームを中継する。この暗号化フレームは図４に関して説明したごとく、ＭＡＣヘッダが暗号化されていない。よって、Ｌ２スイッチ４１ｂのフレーム中継処理部２ｃはこの暗号化フレームを通常のフレームとして認識し、中継処理を行うことが可能である。ポート３ｆに中継された暗号化フレームは、ポート３ｆから中継装置１ｂに送信される。つまり、この暗号化フレームは、Ｌ２スイッチ４１ｂを経由している間、何ら暗号に関する処理をされない。

【００９１】

中継装置１ｂは、暗号化フレームを、暗号処理モジュール４ｂが備えられたポート３ｄで受信する。暗号処理モジュール４ｂは、ポート３ｄとフレーム中継処理部２ｂとの間に備えられており、暗号化フレームを復号化する。復号化されたフレームは、フレーム中継処理部２ｂに送信され、ＰＣ４６ｂに接続されたポート３ｃに中継され、ポート３ｃからＰＣ４６ｃに送信される。

【００９２】

以上のようにしてＰＣ４６ａからＰＣ４６ｂフレームが送信され、暗号化通信が実現される。図６Ｂは図３Ｂと同様に、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。また、図６Ａでは暗号通信が行われる範囲を網かけで示している。

【００９３】

次に、図６Ａおよび図６ＢにおいてＰＣ４６ａからインターネット４５にＩＰパケットを送信する場合について説明する。このＩＰパケットに対応するフレームがＰＣ４６ａから中継装置１ａとＬ２スイッチ４１ｂを経由して中継装置１ｅへ送信される。

【００９４】

ＰＣ４６ａからＬ２スイッチ４１ｂまでの経路は上記の例とまったく同様である。その後、Ｌ２スイッチ４１ｂのポート３ｅで受信された暗号化フレームは、フレーム中継処理部２ｃによって、中継装置１ｅに接続されたポート３ｇに中継される。そして、この暗号化フレームはポート３ｇから中継装置１ｅに送信される。

【００９５】

図６Ｂに示すごとく、中継装置１ｅは、Ｌ２スイッチ４１ｂに接続されたポート３ｈと、ポート３ｈに接続された暗号処理モジュール４ｅと、ファイヤウォール４３に接続されたポート３ｉを有している。さらに中継装置１ｅは、暗号処理モジュール４ｅとポート３ｉに接続されたフレーム中継処理部２ｅを有している。中継装置１ｅは、Ｌ２スイッチ４１ｂのポート３ｇから送信された暗号化フレームをポート３ｈで受信する。この暗号化フレームはポート３ｈに接続された暗号処理モジュール４ｅで復号化されてフレーム中継処理部２ｅに送信され、ポート３ｉに中継される。そして復号化された平文フレームがポート３ｉからファイヤウォール４３に送信される。

【００９６】

図６Ａおよび図６Ｂに示した構成によれば、イーサネット（登録商標）での通信を暗号化することができる。また、ポート３ｉからは復号化された平文フレームが送信されるため、既存のファイヤウォール４３やルータ４４の構成を変える必要もない。

【００９７】

なお、図６Ａおよび図６Ｂにおける暗号処理モジュール４ａ～４ｅ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。一方、図３Ａおよび図３Ｂに

おける暗号処理モジュール４ａ、４ｂは、前述のとおり、暗号処理の要否を判定し、ＶＬＡＮ３０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。いずれの構成によっても本発明を実施することができるが、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。

【００９８】

仮に、図６Ａおよび図６Ｂにおいて、暗号処理モジュール４ａ～４ｄ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４５との通信において暗号処理モジュール４ｅで復号化処理を行う必要がないため、中継装置１ｅ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５１に基づいて暗号処理の要否を暗号処理モジュール４ａなどが判定するといった動作が必要になる。

【００９９】

図７Ａ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中継装置１ａ～１ｄと、複数のポートに暗号処理モジュールを備えた高価な中継装置１ｅを用いている。図７Ｂは図７Ａ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７Ｂでも図３Ｂと同様に、ＴＣＧ対応チップ等の構成要素は省略している。

【０１００】

図６Ａと図７Ａの大きな違いは、図６Ａでは必要だったＬ２スイッチ４１ｂが図７Ａでは不要な点である。そのかわり図７Ａ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中継装置１ｅが必要となっている。

【０１０１】

図７Ａのネットワーク構成も図６Ａ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。

【０１０２】

図７Ａにおいて、四台のＰＣ４６ａ～４６ｄが本発明による中継装置１ａ～１ｄにそれぞれ接続されている。中継装置１ａ～１ｄはいずれも、本発明による中継装置１ｅに接続されている。中継装置１ａ～１ｄのそれぞれは、中継装置１ｅと接続されたポートに対応して暗号処理モジュール４ａ～４ｄ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。中継装置１ｅ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７Ｂに示すように、中継装置１ａ～１ｄと接続されたポート３ｅ～３ｎに対応して、それぞれ暗号処理モジュール４ｅ～４ｎが備えられている。中継装置１ｅはファイヤウォール４３とも接続されており、ファイヤウォール４３はルータ４４に接続されている。インターネット４５など外部のネットワークとの通信は、ルータ４４を介して行われる。

【０１０３】

図７Ａにおける暗号処理モジュール４ａ～４ｎ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。

例えば、ＰＣ４６ａからＰＣ４６ｂにフレームを送信する場合について図７Ｂを参照して説明する。図７Ｂの中継装置１ａは、図６Ｂの中継装置１ａと同様の構成である。まず、ＰＣ４６ａから図４のフレーム５０が送信される。このフレーム５０は、中継装置１ａの、ＰＣ４６ａに接続されたポート３ａで受信される。そして、中継装置１ａ内のフレーム中継処理部２ａによって、暗号処理モジュール４ａが備えられたポート３ｂへと中継される。その際、フレーム５０が暗号処理モジュール４ａを経由し、ここで暗号化される。暗号化されたフレームは、中継装置１ａのポート３ｂから中継装置１ｅのポート３ｅに送信される。

【０１０４】

中継装置１ｅが暗号化フレームをポート３ｅで受信すると、ポート３ｅに接続された暗号処理モジュール４ｅがこのフレームを復号化して、フレーム中継処理部２ｅに送信する。フレーム中継処理部２ｅは受信したフレームをポート３ｆに中継するが、その際、フレ

ームはポート３ｆに接続された暗号処理モジュール４ｆを経由し、暗号処理モジュール４ｆによっ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４ｆからポート３ｆに送信され、ポート３ｆから中継装置１ｂに送信される。

【０１０５】

中継装置１ｂは、暗号処理モジュール４ｂが備えられたポート３ｄで暗号化フレームを受信する。暗号処理モジュール４ｂはポート３ｄとフレーム中継処理部２ｂとの間に備えられており、フレームを復号化する。復号化されたフレームは、フレーム中継処理部２ｂに送信され、ＰＣ４６ｂに接続されたポート３ｃに中継され、ポート３ｃからＰＣ４６ｃに送信される。

【０１０６】

以上のようにしてＰＣ４６ａからＰＣ４６ｂフレームが送信され、暗号化通信が実現される。なお、図７Ｂでも図３Ｂと同様に、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。また、図７Ａでも図６Ａと同様に暗号通信が行われる範囲を網かけで示している。

【０１０７】

次に、図７ＡにおいてＰＣ４６ａからインターネット４５にＩＰパケットを送信する場合について、図７Ｂを参照して説明する。このＩＰパケットに対応するフレームがＰＣ４６ａから中継装置１ａを経由して中継装置１ｅへ送信される。

【０１０８】

ＰＣ４６ａから中継装置１ｅまでの経路は上記の例とまったく同様である。その後、中継装置１ｅのポート３ｅで受信された暗号化フレームは、暗号処理モジュール４ｅで復号化されてフレーム中継処理部２ｅに送信され、ファイヤウォール４３に接続されたポート３ｏに中継される。このフレームはポート３ｏからファイヤウォール４３に送信される。

【０１０９】

図７Ａおよび図７Ｂに示した構成によれば、中継装置１ｅのように高価な装置が必要ではあるものの、図６Ａ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（登録商標）での通信を暗号化することができる。また、ポート３ｏからは復号化された平文フレームが送信されるため、既存のファイヤウォール４３やルータ４４の構成を変える必要がない。

【０１１０】

図８Ａ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中継装置１ａ～１ｅのみを用いている。図８Ａは、中継装置１ｅの具体的な構成が図７Ａの中継装置１ｅと異なるという以外は、図７Ａと同様である。図８Ｂは図８Ａ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８Ｂでも、図３Ｂと同様に、ＴＣＧ対応チップ等の構成要素は省略している。

【０１１１】

図８Ａの構成は、図６Ａに比べて一つ装置の数が少なくて済み（Ｌ２スイッチ４１ｂが不要）、図７Ａに比べて安価な装置だけで済む（図７Ａの中継装置１ｅは高価だが図８Ａの中継装置１ｅ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６Ａや図７Ａ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４ｅを用いたためである。

【０１１２】

例えば、ＰＣ４６ａからＰＣ４６ｂにフレームを送信する場合について図８Ｂを参照して説明する。ＰＣ４６ａから送信されたフレーム５０が中継装置１ａの暗号処理モジュール４ａで暗号化され、暗号処理モジュール４ａに接続されたポート３ｂから中継装置１ｅに送信されるまでは、図７Ｂの場合と同様である。

【０１１３】

この暗号化フレームは、ポート３ｂと接続された中継装置１ｅのポート３ｅで受信される。中継装置１ｅはフレーム中継処理部２ｃを有しており、ポート３ｅはフレーム中継処理部２ｃと接続されている。また、中継装置１ｅは、中継装置１ｂと接続されたポート３

ｆを有しており、ポート３ｆはフレーム中継処理部２ｃとも接続されている。したがって、ポート３ｅで受信された暗号化フレームは、フレーム中継処理部２ｃに送信され、暗号化された状態のまま、送信先ＭＡＣアドレス５１にしたがってポート３ｆに中継される。そして、ポート３ｆから中継装置１ｂに送信される。

【０１１４】

中継装置１ｂはポート３ｄでこの暗号化フレームを受信し、ポート３ｄに接続された暗号処理モジュール４ｂがこの暗号化フレームを復号化する。復号化されたフレームは暗号処理モジュール４ｂからフレーム中継処理部２ｂに送信されて、ポート３ｃに中継され、ポート３ｃに接続されたＰＣ４６ｂに送信される。

【０１１５】

以上のようにしてＰＣ４６ａからＰＣ４６ｂフレームが送信され、暗号化通信が実現される。なお、図８Ｂでも図３Ｂなどと同様に、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。また、図８Ａでは暗号通信が行われる範囲を網かけで示している。図８Ｂと図７Ｂの違いは、図８ＢではＰＣ４６ａからＰＣ４６ｂにフレームを送信する際に中継装置１ｅが何ら暗号に関する処理を行わない点である。

【０１１６】

次に、図８ＡにおいてＰＣ４６ａからインターネット４５にＩＰパケットを送信する場合について図８Ｂを参照して説明する。このＩＰパケットに対応するフレームがＰＣ４６ａから中継装置１ａを経由して中継装置１ｅへ送信される。

【０１１７】

ＰＣ４６ａから中継装置１ｅまでの経路は上記の例とまったく同様である。その後、中継装置１ｅのポート３ｅで受信された暗号化フレームは、暗号化された状態のままフレーム中継処理部２ｃに送信される。中継装置１ｅは、ファイヤウォール４３と接続されたポート３ｇを有しており、ポート３ｇは暗号処理モジュール４ｅと接続され、暗号処理モジュール４ｅはフレーム中継処理部２ｃと接続されている。よって、フレーム中継処理部２ｃは暗号化フレームをポート３ｇに中継する。その際、フレームは暗号処理モジュール４ｅを経由し、暗号処理モジュール４ｅで復号化されて、ポート３ｇに送信される。そしてこのフレームはポート３ｇからファイヤウォール４３に送信される。

【０１１８】

図８Ａおよび図８Ｂに示した構成によれば、図６Ａよりも少ない装置のみで、また、図７Ａ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（登録商標）での通信を暗号化することができる。図８Ａの構成は、図６Ａ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６ＡではＬ２スイッチ４１ｂの障害がイーサネット（登録商標）全体の障害を引き起こすが、図８Ａの構成にはＬ２スイッチ４１ｂが存在しないためである。また、図８Ｂの中継装置１ｅのポート３ｇからは復号化された平文フレームが送信されるため、既存のファイヤウォール４３やルータ４４の構成を変える必要がない。

【０１１９】

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。つまり、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もの（例えば図８Ｂの暗号処理モジュール４ａ～４ｄ）と、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もの（例えば図８Ｂの暗号処理モジュール４ｅ）という二種類である。

【０１２０】

個々の暗号処理モジュールがどちらの動作を行うのかは、任意に選択可能である。例えば、管理者が中継装置１に設定を入力し、ＣＰＵ６がその内容を個々の暗号処理モジュール４に設定してもよい。このように二種類の動作が選択可能であるため、図６Ａ～図８Ｂ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することが可能である。

【０１２１】
図９は、本発明において暗号処理に用いられる鍵について説明する図である。本発明では暗号処理（暗号化および復号化）に秘密鍵方式（共有鍵方式ともいう）の暗号を利用しているが、暗号鍵の生成方法に特徴がある。
【０１２２】
一般に、秘密鍵方式の暗号アルゴリズムでは、暗号化を行う装置と復号化を行う装置との間で、暗号鍵を共有する必要がある。また、同じ暗号鍵を使い続けると、傍受された暗号文に基づいて暗号が破られる（解読される）確率が上がってしまう。よって、より強固なセキュリティのためには、暗号鍵を定期的に新しいものに取り換える必要がある。そのためには一般に、暗号通信を行う装置間で所定のプロトコルにしたがって動的に鍵情報を交換し、その鍵情報から新しい秘密鍵を生成する必要がある。
【０１２３】
しかし、暗号鍵の共有のために動的に鍵情報を交換する方式には欠点がある。第一に、鍵情報を交換するためのプロトコルが複雑で、鍵情報を交換する際や装置に障害が発生した際に不具合が発生しやすい。特に、Ｎ対Ｎの関係で暗号化通信を行う場合の実装は複雑である。第二に、暗号通信を行う相手の装置が多いと、鍵情報を交換する処理にかかる負荷が増大し、スケーラビリティに制約が生じる。
【０１２４】
本発明によれば、動的に鍵情報を交換する必要がなく、簡易な構成でフレームごとに異なる暗号鍵を生成することができる。よって、強固なセキュリティとスケーラビリティを両立させ、高速な処理を実現することができる。そのための具体的な方法を以下で説明する。
【０１２５】
図９において暗号鍵の生成には三種類の情報を利用するが、まず用語の定義を（ｄ１）～（ｄ５）に示す。
（ｄ１）「フレーム鍵」とは、フレームの暗号化および復号化に用いる暗号鍵であって、暗号化を行う中継装置１と復号化を行う中継装置１で共有する秘密鍵である。以下では、フレーム鍵を記号「ｋ」で表す。
（ｄ２）「事前共有鍵」とは、管理者等により中継装置１に設定されるデータである。事前共有鍵は、例えば８文字以内の英数字からなるパスワードでもよい。以下では、事前共有鍵を記号「ｋ０」で表す。
（ｄ３）「ＭＡＣヘッダ情報」とは、暗号化の対象である平文フレーム（フレーム５０またはタグつきフレーム６０）の送信先ＭＡＣアドレス５１または送信元ＭＡＣアドレス５２の少なくとも一方に基づく情報である。以下の実施形態において、ＭＡＣヘッダ情報は、送信先ＭＡＣアドレス５１と送信元ＭＡＣアドレス５２の双方からなる情報である。以下では、ＭＡＣヘッダ情報を記号「ｋ１」で表す。
（ｄ４）「シーケンス番号」とは、暗号化を行う暗号処理モジュール４ごとに管理される番号で、暗号化処理を行うたびに１ずつ増加する番号である。また、シーケンス番号は暗号化フレームに書き込まれる。シーケンス番号のデータ長は、図５の例および以下の実施形態において８バイトである。以下では、シーケンス番号を記号「ｋ２」で表す。また、暗号処理モジュール４で管理されているシーケンス番号を記号「ｋ２＿ｓ」で表し、図５のシーケンス番号７１４のように暗号化フレームに書き込まれたシーケンス番号を記号「ｋ２＿ｒ」で表して区別することもある。
（ｄ５）「マスター鍵」とは、事前共有鍵ｋ０に基づいて暗号処理モジュール４が生成するデータである。マスター鍵は事前共有鍵ｋ０よりも長いデータ長を持つことが望ましい。以下ではマスター鍵を記号「ｋ３」で表す。
【０１２６】
以下の実施形態では、フレーム鍵ｋを生成するのに、ＭＡＣヘッダ情報ｋ１、シーケンス番号ｋ２、マスター鍵ｋ３の三つの情報を利用する。
図９には、図１や図２と同様の中継装置１のうち、フレーム鍵ｋの生成に関係する部分

のみ抜粋したものが示してある。

【０１２７】

事前共有鍵ｋ０は管理者によって事前に設定され、ＴＣＧ対応チップ５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。

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本発明の中継装置１において同じ値が設定される。例えば、図３Ａの例では中継装置１ａ、１ｂの双方に同じ値の事前共有鍵ｋ０が設定され、図８Ａの例では中継装置１ａ～１ｅのすべてに同じ値の事前共有鍵ｋ０が設定される。

【０１２８】

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３Ａの例では中継装置１ａ、１ｂの双方に対し、ＶＬＡＮ１０用の事前共有鍵ｋ０とＶＬＡＮ２０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、中継装置１ａ、１ｂ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。

【０１２９】

ＭＡＣヘッダ情報ｋ１は暗号化対象のフレーム５０から読み取ることができる情報である。なお、ＶＬＡＮ環境における暗号化の対象は図４のタグつきフレーム６０だが、その場合も、ＭＡＣヘッダ情報ｋ１をタグつきフレーム６０から読み取ることができる。

【０１３０】

シーケンス番号ｋ２＿ｓは、例えば暗号処理モジュール４が内部に有するカウンタに格納されている。暗号処理モジュール４は、一つのフレームを暗号化するたびにこのカウンタの値を１ずつ増やす。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４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。このカウンタの示す値がシーケンス番号ｋ２＿ｓである。シーケンス番号ｋ２＿ｓは、暗号処理モジュール４によって、暗号化フレーム７０の中の暗号ヘッダ７１の部分にシーケンス番号ｋ２＿ｒとして配置される（シーケンス番号ｋ２＿ｒは図５のシーケンス番号７１４に相当する）。

【０１３１】

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４が生成する。管理者が事前共有鍵ｋ０を中継装置１に設定すると、ＣＰＵ６が暗号処理モジュール４にマスター鍵ｋ３の生成を命令し、暗号処理モジュール４はその命令にしたがってマスター鍵ｋ３を生成する。生成されたマスター鍵ｋ３は、暗号処理モジュール４の内部に格納される。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ｋａを事前共有鍵ｋ０に基づいて暗号処理モジュール４が生成してもよい。この場合、マスター鍵配列ｋａが暗号処理モジュール４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。

【０１３２】

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。上記のように、暗号化通信を行う範囲に含まれるすべての本発明の中継装置１において、事前共有鍵ｋ０は同じ値である。また、後述するように、中継装置１は、事前共有鍵ｋ０から一意に決まるマスター鍵ｋ３が生成されるように構成されている。すなわち、個々の中継装置１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が生成される。したがって、暗号化通信を行う範囲に含まれるすべての本発明の中継装置１において、マスター鍵ｋ３は同じ値である。

【０１３３】

暗号処理モジュール４は、フレームを暗号化および復号化する際にフレーム鍵ｋを生成する。フレームを暗号化する際の暗号処理モジュール４の動作は下記のステップ（ｓ１）～（ｓ６）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２から受信する。

（ｓ２）そのフレームからＭＡＣヘッダ情報ｋ１を読み取る。
（ｓ３）現在のシーケンス番号ｋ２＿ｓをカウンタから読み取り、カウンタの値を１増やす。
（ｓ４）マスター鍵ｋ３を読み出す。
（ｓ５）所定の関数ｆを用いて、ｋ＝ｆ（ｋ１，ｋ２＿ｓ，ｋ３）なるフレーム鍵ｋを生成する。
（ｓ６）フレーム鍵ｋを用いてフレームを暗号化し、（ｓ３）で読み取った値を暗号ヘッダ７１にシーケンス番号ｋ２＿ｒとして書き込む。

【０１３４】

フレームを復号化する際の暗号処理モジュール４の動作は下記のステップ（ｒ１）～（ｒ６）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２から受信する。
（ｒ２）そのフレームからＭＡＣヘッダ情報ｋ１を読み取る。
（ｒ３）そのフレームの暗号ヘッダ７１からシーケンス番号ｋ２＿ｒを読み取る。
（ｒ４）マスター鍵ｋ３を読み出す。
（ｒ５）所定の関数ｆを用いて、ｋ＝ｆ（ｋ１，ｋ２＿ｒ，ｋ３）なるフレーム鍵ｋを生成する。なお、この関数ｆはステップ（ｓ５）における関数ｆと同じである。
（ｒ６）フレーム鍵ｋを用いてフレームを復号化する。

【０１３５】

ステップ（ｓ４）および（ｒ４）においては、実施形態によって、単に格納されたマスター鍵ｋ３を読み出す場合もあれば、何らかの演算に基づいてマスター鍵ｋ３を決定する場合もある。

【０１３６】

ところで、シーケンス番号ｋ２は、暗号処理モジュール４が管理するシーケンス番号ｋ２＿ｓでもあり、暗号化フレームに書き込まれたシーケンス番号ｋ２＿ｒでもあるから、上記の関数ｆを用いてｋ＝ｆ（ｋ１，ｋ２，ｋ３）と表すこともできる。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。また、上記のようにマスター鍵ｋ３は事前共有鍵ｋ０に基づいて決められるため、フレーム鍵ｋはＭＡＣヘッダ情報ｋ１とシーケンス番号ｋ２と事前共有鍵ｋ０に基づいて定められている、と言うこともできる。

【０１３７】

ＭＡＣヘッダ情報ｋ１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が異なる。異なるＭＡＣヘッダ情報ｋ１に対しては異なるフレーム鍵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フレーム鍵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。

【０１３８】

また、シーケンス番号ｋ２は、暗号処理モジュール４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に対しては異なるフレーム鍵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フレーム鍵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。

【０１３９】

以上のようにフレーム鍵ｋを生成することにより、フレーム鍵ｋがＭＡＣヘッダ情報ｋ１およびシーケンス番号ｋ２によって異なる値となる。よって、動的に鍵情報の交換を行って暗号鍵を新しいものに取り換えなくても、事実上フレームごとに異なるフレーム鍵ｋが使われる。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、本発明では他の中継装置１への影響はない。したがって、上記のように生成したフレーム鍵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。

【０１４０】

以下では、フレーム鍵ｋの生成の具体的な方法について、いくつか説明する。

フレーム鍵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。この方法では、上記のステップ（ｓ５）、（ｒ５）は以下のステップ（ｓ５‐１）、（ｒ５‐１）で置き換えられる。

（ｓ５‐１）ｋ＝ｈ（ｋ１＋ｋ２＿ｓ＋ｋ３）なるフレーム鍵ｋを生成する。

（ｒ５‐１）ｋ＝ｈ（ｋ１＋ｋ２＿ｒ＋ｋ３）なるフレーム鍵ｋを生成する。

【０１４１】

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。暗号通信の送信側と受信側の暗号処理モジュール４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。

【０１４２】

ハッシュ関数を利用することにより、異なる二つの（ｋ１，ｋ２，ｋ３）の組から同じフレーム鍵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、フレーム鍵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フレーム鍵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、フレーム鍵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。

【０１４３】

フレーム鍵ｋを生成する第二の方法は、配列を用いる方法である。図１０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（ｓ４）、（ｓ５）、（ｒ４）、（ｒ５）はそれぞれ以下のステップ（ｓ４‐２）、（ｓ５‐２）、（ｒ４‐２）、（ｒ５‐２）で置き換えられる。

（ｓ４‐２）（ｓ３）で読み取ったｋ２＿ｓに基づいて、マスター鍵配列ｋａからマスター鍵ｋ３を読み出す。

（ｓ５‐２）ｋ＝ｋ３　ＸＯＲ　（ｋ１＋ｋ２＿ｓ）なるフレーム鍵ｋを生成する。

（ｒ４‐２）（ｒ３）で読み取ったｋ２＿ｒに基づいて、マスター鍵配列ｋａからマスター鍵ｋ３を読み出す。

（ｒ５‐２）ｋ＝ｋ３　ＸＯＲ　（ｋ１＋ｋ２＿ｒ）なるフレーム鍵ｋを生成する。

【０１４４】

図１０を参照して上記のステップについて説明する。図９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１０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ｋａとして暗号処理モジュール４に格納しておく。以下、マスター鍵配列ｋａで添え字がｊの値をｋａ［ｊ］と表し、各ｋａ［ｊ］の値を候補値とよぶ。

【０１４５】

ステップ（ｓ４‐２）では、例えば、ｋ２＿ｓをＭで割ったときの剰余ｊを算出し、ｋａ［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（ｒ４‐２）でも同様にして、マスター鍵ｋ３を読み出すことができる。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ｋａからマスター鍵ｋ３（＝ｋａ［ｊ］）を読み出してもよい。

【０１４６】

ステップ（ｓ４‐２）や（ｒ４‐２）では、マスター鍵ｋ３がシーケンス番号ｋ２（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、異なるフレーム鍵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フレーム鍵ｋが推測困難なようにするためには、マスター鍵配列ｋａを生成する際にｋａ［ｉ］とｋａ［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。

【０１４７】

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（ｓ５‐２）および（ｒ５‐２）に示したごとく、関数ｆの計算に必要なのは加算と排他的論理和の演算のみである。

【０１４８】

したがって、この第二の方法は、フレーム鍵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３Ａ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３Ａの例において、ＶＬＡＮ１０とＶＬＡＮ２０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ＶＬＡＮ１０、２０にそれぞれ対応する事前共有鍵ｋ０、ｋ０’を管理者が中継装置１ａに設定し、暗号処理モジュール４ａ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、中継装置１ｂ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４ｂ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４ａ、４ｂはそれぞれ、ＶＬＡＮ１０、２０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ｋａ、ｋａ’を生成する。そして、ＶＬＡＮ１０に対応するフレームの暗号処理ではマスター鍵配列ｋａを使い、ＶＬＡＮ２０に対応するフレームの暗号処理ではマスター鍵配列ｋａ’を使う。

【０１４９】

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、シーケンス番号ｋ２から異なるフレーム鍵ｋが生成される。

【０１５０】

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。

【０１５１】

この第一の方法による実施形態では、中継装置１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、記号ｆｓで表す）を定義しており、暗号処理モジュール４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中継装置１に備えられたすべての暗号処理モジュール４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中継装置１に組み込んだ製造業者しか知らないものであって、中継装置１の利用者には秘密にされる。

【０１５２】

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３Ａの４ａと４ｂ）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。

【０１５３】

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。

【０１５４】

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。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）。

【０１５５】

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、中継装置１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。

【０１５６】

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。

【０１５７】

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。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。

【０１５８】

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ｋａを利用する実施形態にも適用することができる。

【０１５９】

事前共有鍵ｋ０からマスター鍵配列ｋａ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ｋａ［０］～ｋａ［Ｍ－１］として格納する点で異なる。

【０１６０】

例えば、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ｋａ［０］～ｋａ［Ｍ－１］として格納する。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。

【０１６１】

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ｋａ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ｋａの中から選択されるマスター鍵ｋ３の安全性も保たれる。

【０１６２】
事前共有鍵ｋ０からマスター鍵配列ｋａ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ｋａ［０］～ｋａ［Ｍ－１］として格納する点で異なる。
【０１６３】
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ｋａ［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）。
【０１６４】
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ｋａ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ｋａ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、ｋａ［０］～ｋａ［Ｍ－１］に格納されたそれぞれの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。
【０１６５】
次に、図１１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。本発明による中継装置１は、好ましい実施形態において、暗号化フレーム７０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７０を「フラグメントフレーム」とよぶ。図１１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７１の形式を説明する図である。
【０１６６】
前述のとおり一般に、イーサネット（登録商標）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７０は暗号ヘッダ７１を含む。よって、フレーム５０やタグつきフレーム６０のデータ部５３を暗号化した場合、暗号化フレーム７０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。
【０１６７】
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、本発明による中継装置１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７０の送受信が可能となる。例えば図３Ａにおいて、１５２２バイトよりも長い暗号化フレーム７０を中継装置１ａから中継装置１ｂへ送信する際に、コアＬ２／Ｌ３スイッチ４１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７０はコアＬ２／Ｌ３スイッチ４１を経由して中継装置１ｂに届く。
【０１６８】
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、本発明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（登録商標）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、本発明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７０が送信できなくなることがありうる。
【０１６９】
そこで、本発明による中継装置１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１１の実施形態では、中継装置１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７１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中

継装置１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７０を送受信することができる。

【０１７０】

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４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７０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７０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７０に復元し、復元した暗号化フレーム７０を復号化する。

【０１７１】

図１１と図５の暗号ヘッダ７１を比較すると、図１１では予約フィールド７１３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。

【０１７２】

本実施形態では、予約フィールド７１３の値が０ｘ０１または０ｘ０２の場合は暗号ヘッダ７１が図１１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７１３の値が０ｘ００の場合は暗号ヘッダ７１が図５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４は、受信した暗号化フレームの予約フィールド７１３の値によって暗号ヘッダ７１の範囲を判定することができる。

【０１７３】

分割されていない暗号化フレーム７０において予約フィールド７１３の値は０ｘ００である。一つの暗号化フレーム７０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７１３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。

【０１７４】

ＩＤフィールド７１５は、分割する前の暗号化フレーム７０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ＩＤ７１５に利用する。一つの暗号化フレーム７０をｎ個のフラグメントフレームに分割した場合、ＩＤ７１５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。

【０１７５】

フラグメントオフセット７１６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７１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４の動作について説明する。

【０１７６】

暗号処理モジュール４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７０のデータ長が最大フレーム長（通常のイーサネット（登録商標）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７０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ＩＤ７１５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７１６、ＩＣＶ７３、ＦＣＳ５４の値をそれぞれ計算する。

【０１７７】

暗号処理モジュール４は、暗号ヘッダ７１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７１３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７１３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７１３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ＩＤ７１５が同じ値か否か、フラグメントオフセット７１６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。

【０１７８】

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４では、タイプ等も含めたデータ部５３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情報であると見なし、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７０における暗号ヘッダ７１の位置は、図４と同様にＴＣＩ６２の直後でもよく、ＴＣＩ６２の直後にタイプ等が続き、その後に暗号ヘッダ７１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７１、暗号化データ部という順になるという点で、図４と同様である。

【０１７９】

上記の実施形態では、ｋ＝ｆ（ｋ１，ｋ２，ｋ３）なるフレーム鍵ｋを生成している。しかし、フレーム鍵ｋを生成するのに、ＭＡＣヘッダ情報ｋ１やマスター鍵ｋ３は必須ではなく、シーケンス番号ｋ２のみが必須である。なぜなら、フレームの送信のたびに異なる要素は、シーケンス番号ｋ２のみだからである。したがって、例えば、ハッシュ関数ｈを利用してｋ＝ｈ（ｋ２）などの計算によりフレーム鍵ｋを生成してもよい。

【０１８０】

ただし、フレーム鍵ｋの強度という点からはＭＡＣヘッダ情報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１０のように計算を単純化して処理を高速化するためにも、シーケンス番号ｋ２以外の要素であるＭＡＣヘッダ情報ｋ１およびマスター鍵ｋ３を利用することが望ましい。

【０１８１】

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１１では、フラグメントオフセット７１６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７１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７１３とフラグメントオフセット７１６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７１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。

【０１８２】

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）

データリンク層のフレームを中継する中継装置であって、

該中継装置の外部と前記フレームの送受信を行うための複数のポートと、

前記フレームを中継するフレーム中継処理部と、

前記複数のポートのうちの一つとの間で前記フレームを送受信する第一のインターフェイス、および前記フレーム中継処理部との間で前記フレームを送受信する第二のインターフェイスを有し、前記第一または第二のインターフェイスの一方から前記フレームを受信したとき該フレームを暗号化して暗号化フレームを生成する暗号化処理を行い、前記第一または第二のインターフェイスの他方から前記暗号化フレームを受信したとき該暗号化フレームを復号化する復号化処理を行う、一つ以上の暗号処理部と、

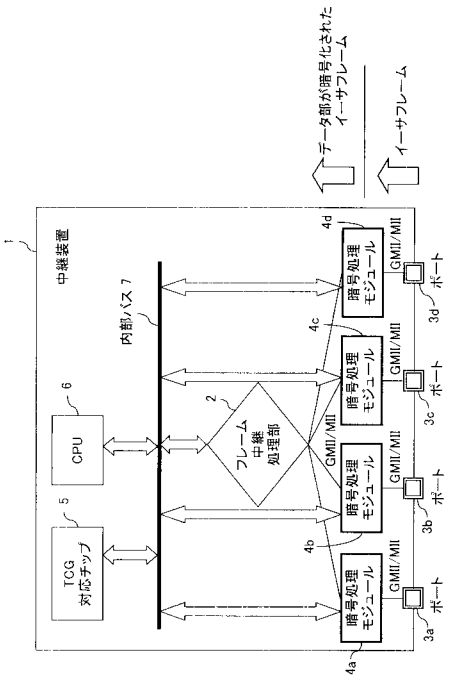
を備えることを特徴とする中継装置。
（付記２）
前記フレームがＶＬＡＮを識別するＶＬＡＮ識別情報を含むとき、前記暗号処理部は、前記ＶＬＡＮ識別情報に基づいて、受信した前記フレームに対して前記暗号化処理または前記復号化処理のうちの一方を行うか、いずれも行わないか、を決定することを特徴とする付記１に記載の中継装置。
（付記３）
前記暗号化処理において、前記暗号処理部は、前記フレームのヘッダを除くデータ部を暗号化し、前記ヘッダと、前記データ部を暗号化して得られた暗号化データとの間の位置に、復号化に必要な情報を含む暗号ヘッダを配置して暗号化フレームを生成することを特徴とする付記１に記載の中継装置。
（付記４）
前記暗号処理部は、該暗号処理部に対応する前記ポートから前記第一のインターフェイスを介して前記フレームを受信したときに前記暗号化処理を行い、前記フレーム中継処理部に前記第二のインターフェイスを介して生成した前記暗号化フレームを送信し、
前記暗号処理部は、前記フレーム中継処理部から前記第二のインターフェイスを介して前記フレームを受信したときに前記復号化処理を行い、該暗号処理部に対応する前記ポートに前記第一のインターフェイスを介して復号化した前記フレームを送信する、
ことを特徴とする付記１に記載の中継装置。
（付記５）
前記暗号処理部は、該暗号処理部に対応する前記ポートから前記第一のインターフェイスを介して前記フレームを受信したときに前記復号化処理を行い、前記フレーム中継処理部に前記第二のインターフェイスを介して復号化した前記フレームを送信し、
前記暗号処理部は、前記フレーム中継処理部から前記第二のインターフェイスを介して前記フレームを受信したときに前記暗号化処理を行い、該暗号処理部に対応する前記ポートに前記第一のインターフェイスを介して生成した前記暗号化フレームを送信する、
ことを特徴とする付記１に記載の中継装置。
（付記６）
前記暗号処理部はシーケンス番号を格納する番号格納部を備え、
前記暗号化処理を行うとき、前記暗号処理部は、前記シーケンス番号に基づいて暗号鍵を生成し、該暗号鍵を使って前記フレームを暗号化して前記暗号化フレームを生成し、前記シーケンス番号を該暗号化フレームに含ませ、前記番号格納部に格納された前記シーケンス番号の値を変化させ、
前記復号化処理を行うとき、前記暗号処理部は、前記暗号化フレームに含まれる前記シーケンス番号に基づいて前記暗号鍵を生成し、該暗号鍵を使って前記復号化処理を行う、
ことを特徴とする付記１に記載の中継装置。
（付記７）
前記暗号処理部は前記暗号鍵を生成する際、さらに、前記フレームに含まれる送信先ＭＡＣアドレスまたは送信元ＭＡＣアドレスの少なくとも一方から得られるＭＡＣヘッダ情報にも基づいて前記暗号鍵を生成することを特徴とする付記６に記載の中継装置。
（付記８）
前記暗号処理部は前記暗号鍵を生成する際、さらに、前記暗号化フレームを送受信するために組み合わせて利用される複数の前記中継装置の各々において予め設定された同一の値である事前共有鍵にも基づいて、前記暗号鍵を生成することを特徴とする付記６に記載の中継装置。
（付記９）
前記暗号処理部がハッシュ関数を使って前記暗号鍵を生成することを特徴とする付記６に記載の中継装置。
（付記１０）
前記暗号化フレームを送受信するために組み合わせて利用される複数の前記中継装置の

各々において予め設定された同一の値である事前共有鍵に基づいて、前記暗号処理部が２以上の整数であるＭ個の値を生成して候補値として記憶し、
前記暗号処理部は、Ｍ個の前記候補値のうちの一つを前記シーケンス番号に基づいて選択し、選択した前記候補値に基づいて前記暗号鍵を生成することを特徴とする付記６に記載の中継装置。
（付記１１）
前記暗号処理部は前記暗号鍵を生成する際、前記中継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し、該ランダムな値に基づいて前記暗号鍵を生成することを特徴とする付記８に記載の中継装置。
（付記１２）
前記暗号処理部は前記暗号鍵を生成する際、前記中継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し、該ハッシュ値に基づいて前記暗号鍵を生成することを特徴とする付記８に記載の中継装置。
（付記１３）
前記暗号処理部は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、前記中継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１０に記載の中継装置。
（付記１４）
前記暗号処理部は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、前記中継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１０に記載の中継装置。
（付記１５）
前記暗号化処理において、前記暗号処理部はさらに、前記暗号化フレームの長さが所定の長さを超えるとき前記暗号化フレームを分割して複数のフラグメントフレームを生成し、
前記復号化処理において、前記暗号処理部はさらに、前記フラグメントフレームを受信したのか、それとも分割されていない前記暗号化フレームを受信したのかを判定し、前記フラグメントフレームを受信したと判定した場合には、分割前の前記暗号化フレームに対応する複数の前記フラグメントフレームのすべてを受信してから、該すべてのフラグメントフレームを分割前の前記暗号化フレームに再構成する、
ことを特徴とする付記１に記載の中継装置。
【図面の簡単な説明】
【０１８３】
【図１】本発明による中継装置の一実施形態における構成図である。
【図２】本発明による中継装置の別の実施形態における構成図である。
【図３Ａ】ＶＬＡＮ環境における本発明の中継装置の利用例を示す図である。
【図３Ｂ】図３Ａ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４】本発明で利用するフレームの形式を説明する図である。
【図５】暗号ヘッダの詳細を示す図である。
【図６Ａ】本発明による中継装置を使ってネットワークを構成した例を示す図である。
【図６Ｂ】図６Ａ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７Ａ】本発明による中継装置を使ってネットワークを構成した例を示す図である。

【図７Ｂ】図７Ａ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８Ａ】本発明による中継装置を使ってネットワークを構成した例を示す図である。
【図８Ｂ】図８Ａ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９】本発明において暗号処理に用いられる鍵について説明する図である。
【図１０】本発明において暗号処理に用いられる鍵を、配列を利用して生成する方法について説明する図である。
【図１１】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。
【符号の説明】
【０１８４】
１、１ａ～１ｅ　中継装置
２、２ａ～２ｅ　フレーム中継処理部
３、３ａ～３ｏ　ポート
４ａ～４ｎ　暗号処理モジュール
５　ＴＣＧ対応チップ
６　ＣＰＵ
７　内部バス
１０、２０、３０　ＶＬＡＮ
４１　コアＬ２／Ｌ３スイッチ
４１ｂ　Ｌ２スイッチ
４２ａ、４２ｂ　．１Ｑトランク
４３　ファイヤウォール
４４　ルータ
４５　インターネット
４６ａ～４６ｄ　ＰＣ
５０　フレーム
５１　送信先ＭＡＣアドレス
５２　送信元ＭＡＣアドレス
５３　データ部
５４　ＦＣＳ
６０　タグつきフレーム
６１　ＴＰＩＤ
６２　ＴＣＩ
７０　暗号化フレーム
７１　暗号ヘッダ
７２　暗号化データ部
７３　ＩＣＶ
７１１　タイプ
７１２　サブタイプ
７１３　予約フィールド
７１４　シーケンス番号
７１５　ＩＤ
７１６　フラグメントオフセット
ｋ０　事前共有鍵
ｋ１　ＭＡＣヘッダ情報
ｋ２、ｋ２＿ｓ、ｋ２＿ｒ　シーケンス番号
ｋ３　マスター鍵
ｋａ　マスター鍵配列

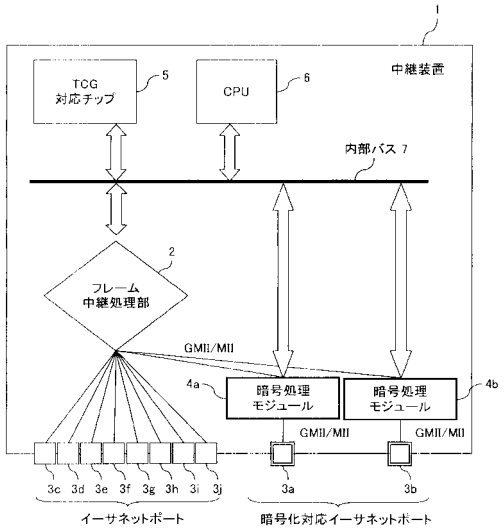
【図１】

本発明による中継装置の
一実施形態における構成図



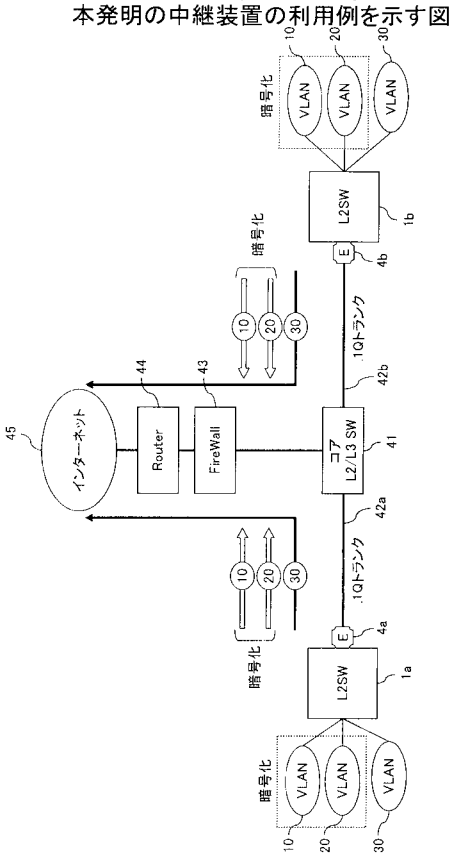
【図２】

本発明による中継装置の別の
実施形態における構成図



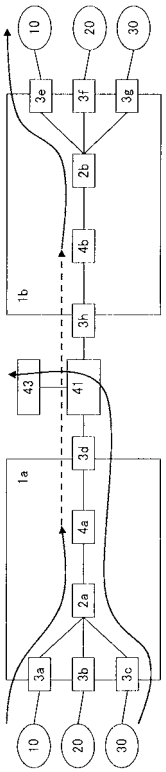
【図３Ａ】

VLAN環境における
本発明の中継装置の利用例を示す図



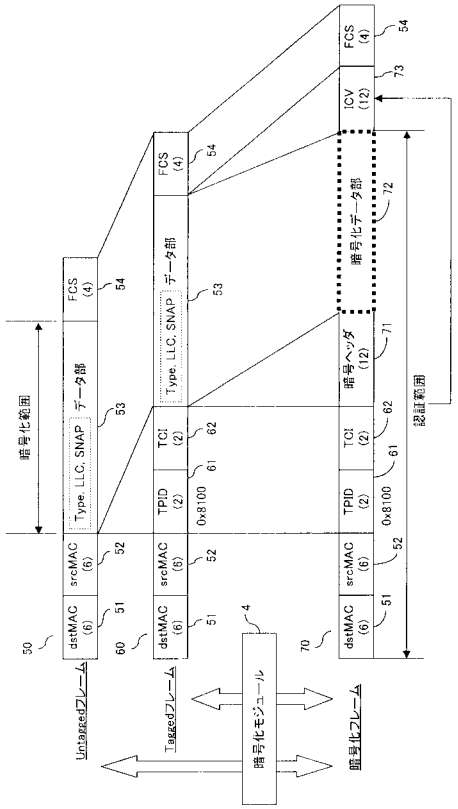
【図３Ｂ】

図3A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



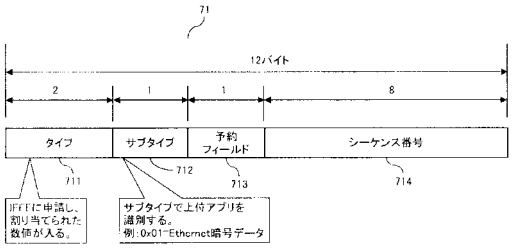
【図４】

本発明で利用するフレームの
形式を説明する図



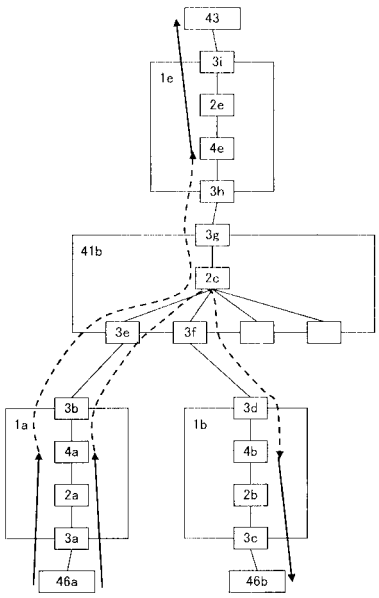
【図５】

暗号ヘッダの詳細を示す図



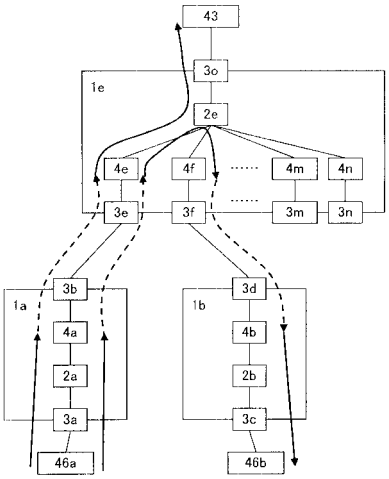
【図６Ｂ】

図6A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



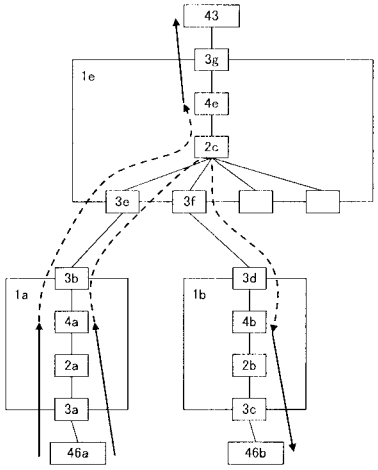
【図７Ｂ】

図7A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



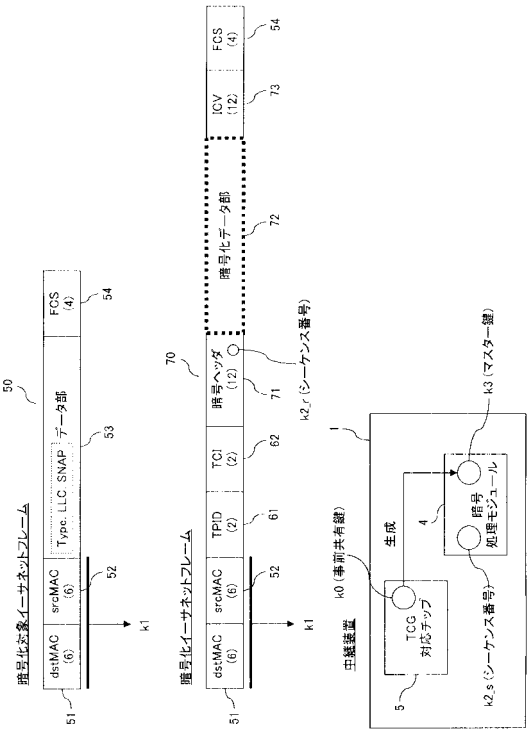
【図８Ｂ】

図8A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



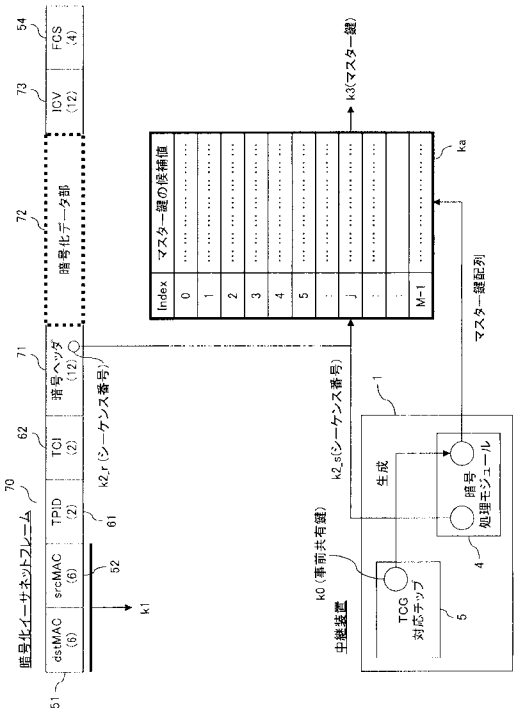
【図９】

本発明において暗号処理に用いられる
鍵について説明する図



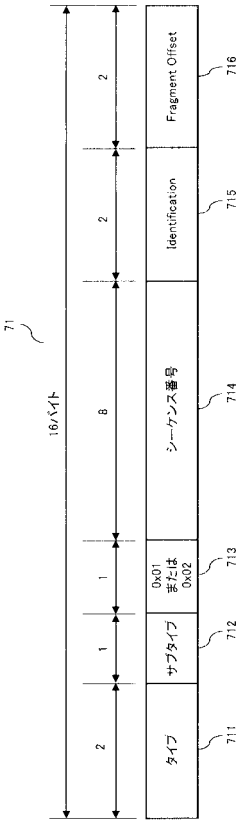
【図１０】

本発明において暗号処理に用いられる鍵を、
配列を利用して生成する方法について説明する図



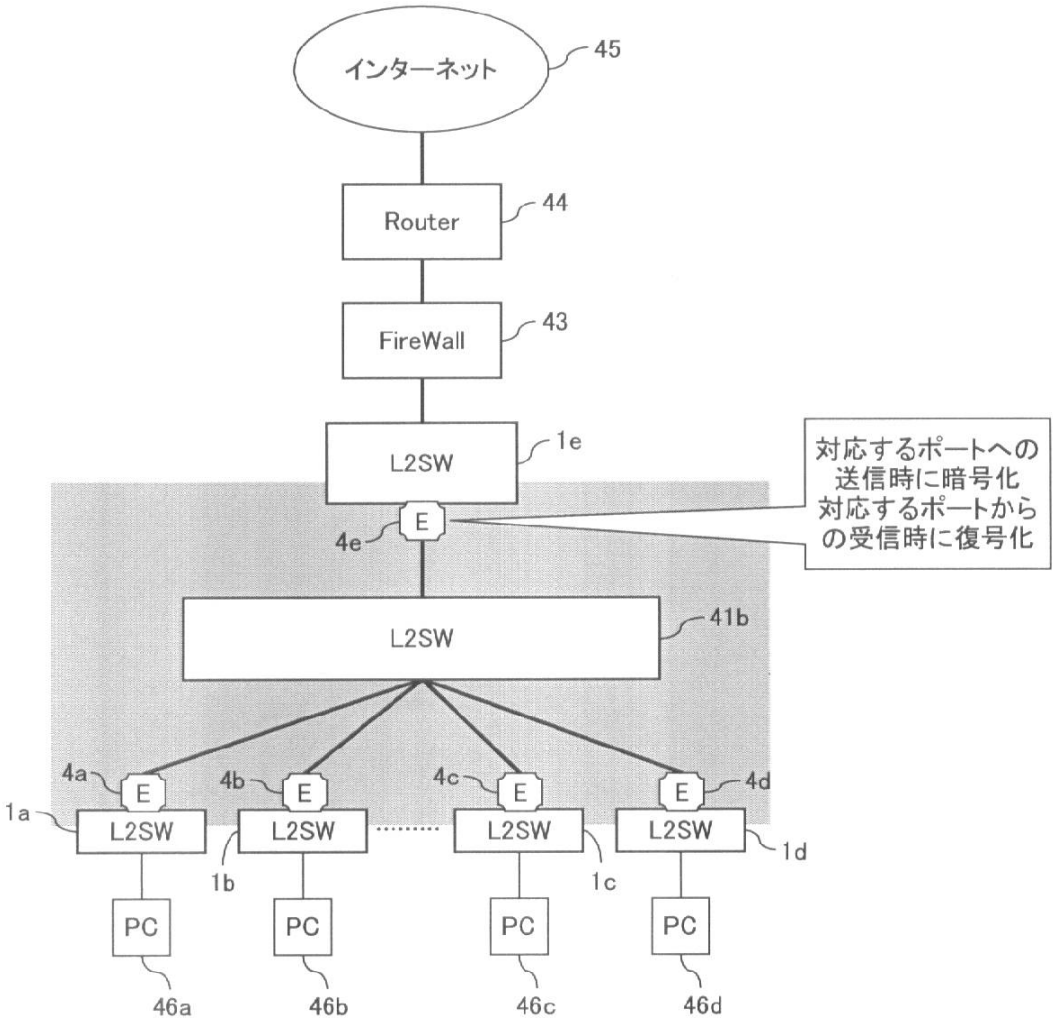
【図１１】

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



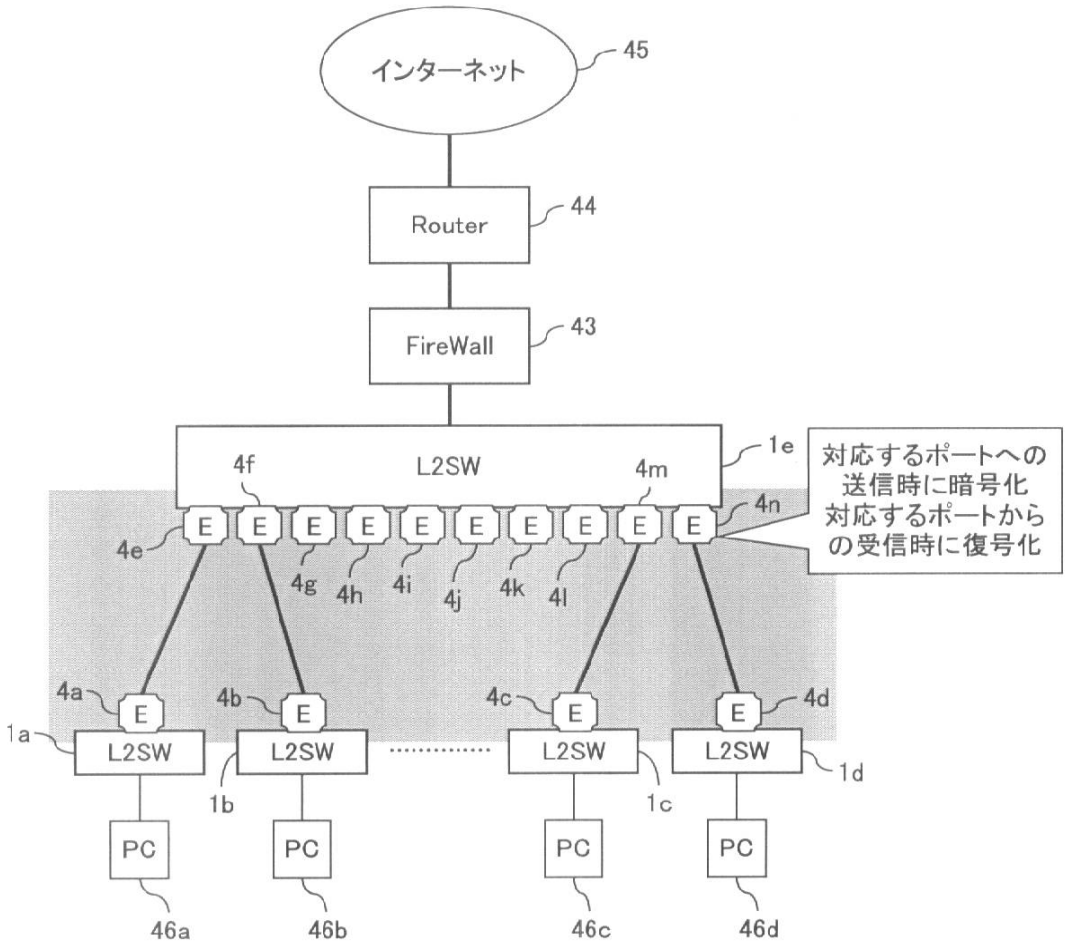
【図６Ａ】

本発明による中継装置を使って
ネットワークを構成した例を示す図



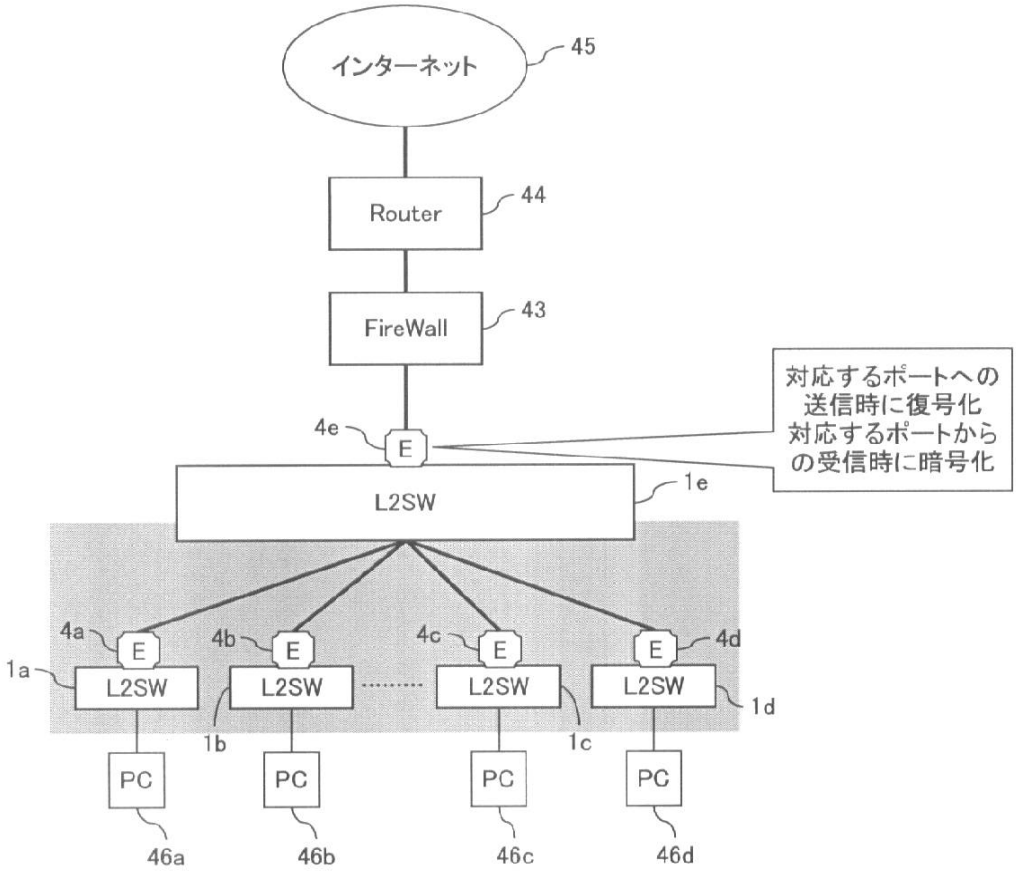
【図７Ａ】

本発明による中継装置を使って
ネットワークを構成した例を示す図



【図８Ａ】

本発明による中継装置を使って
ネットワークを構成した例を示す図



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

審査官　青木　重徳

(56)参考文献　特開２００５－２９５１０５（ＪＰ，Ａ）
特開２００３－０３７６００（ＪＰ，Ａ）
特開２００１－３３３１１０（ＪＰ，Ａ）
特開２００１－００７８４９（ＪＰ，Ａ）
特開２０００－１７４７９６（ＪＰ，Ａ）
特開平１１－１４５９７５（ＪＰ，Ａ）
特開平１１－２３９１８４（ＪＰ，Ａ）
特開平１１－０５５３２２（ＪＰ，Ａ）
特開平０６－２５２９２２（ＪＰ，Ａ）
特表２００４－５２１５２１（ＪＰ，Ａ）
国際公開第０２／０１７６３７（WO，Ａ１）
国際公開第２００３／０９８８７４（WO，Ａ１）
D. W. Davies and W. L. Price 著／上園忠弘　監訳，“ネットワーク・セキュリティ”，日本，日経マグロウヒル社，１９８５年１２月　５日，１版１刷，ｐ．１０２－１１０，３０７－３１２

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／３６
Ｈ０４Ｌ　　９／１４
Ｈ０４Ｌ　１２／５６