(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2007-295272
(P2007-295272A)
(43)公開日　平成19年11月8日(2007.11.8)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 12/58	(2006.01)	H04L	12/58	100F	5J104
H04L 9/36	(2006.01)	H04L	9/00	685	5K030
H04L 12/22	(2006.01)	H04L	12/22		

審査請求 未請求　請求項の数 3　OL　（全 22 頁）

(21)出願番号　特願2006-120823 (P2006-120823)
(22)出願日　平成18年4月25日 (2006.4.25)

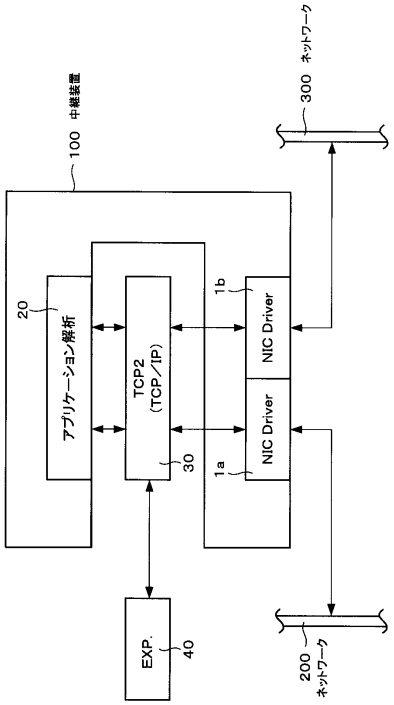
（特許庁注：以下のものは登録商標）
１．イーサネット
２．ＥＴＨＥＲＮＥＴ

(71)出願人　503287764
ティー・ティー・ティー株式会社
大阪府大阪市北区東天満１丁目１番１９号
アーバンエース東天満ビル
(74)代理人　100122884
弁理士　角田　芳末
(74)代理人　100133824
弁理士　伊藤　仁恭
(72)発明者　尾崎　博嗣
大阪府大阪市北区東天満１丁目１番１９号
アーバンエース東天満ビル　ティー・ティー・ティー株式会社内

最終頁に続く

(54)【発明の名称】中継装置

(57)【要約】
【課題】パーソナルコンピュータと外部との通信において、インターネット上でのデータの「漏洩」及び「改竄」、さらには「なりすまし」、「進入」ないし「攻撃」を防ぐ。
【解決手段】中継装置１００には、それぞれネットワーク２００、３００と接続されるＮＩＣ（Network Interface Card）ドライバ１ａ、１ｂが設けられ、これらのＮＩＣドライバ１ａ、１ｂを含む物理層とデータリンク層に対して、任意の２つのノード間で、ルーティング（routing）を行いながら通信するための通信方法を規定するアプリケーション解析２０を含むネットワーク層とトランスポート層が設けられる。そしてこれらのデータリンク層とネットワーク層との間に、本発明者が先に提案した「ＴＣＰ２」３０の機能を設ける。
【選択図】図１



【特許請求の範囲】
【請求項１】
クライアント装置でトランスポート層に位置するＴＣＰ又はＵＤＰプロトコルに暗号化機能を追加して電子化情報の通信を行う際に用いられる中継装置であって、
前記クライアント装置から受信した情報単位としてのパケットを暗号化して相手装置に送信し、また前記相手装置から受信した前記パケットを前記クライアント装置に送信する通信手段を備え、
前記通信手段は少なくとも前記クライアント装置との間で対応する暗号化及び復号化ロジックを取り決める取決め手段を有し、
前記相手装置に送信する際には、前記受信したパケットの内の少なくとも前記ＴＣＰプロトコルのペイロードを前記取決め手段により取り決めた復号化ロジックに従って復号化し、復号化した前記パケットのＳＭＴＰコマンドを解析し、前記パケットの電子メールのタイトル、本文、添付ファイルを暗号化して前記相手装置に送信し、
前記相手装置から受信した際には、前記受信した前記パケットのＰＯＰコマンドを解析し、前記パケットの電子メールのタイトル、本文、添付ファイルを復号化し、復号化した前記パケットの前記ＴＣＰプロトコルのペイロードを前記取決め手段により取り決めた暗号化ロジックに従って暗号化して前記クライアント装置に送信し、
前記トランスポート層のＴＣＰ又はＵＤＰプロトコルを用いて前記暗号化及び復号化ロジックに基づいた通信を行うことを特徴とする中継装置。
【請求項２】
前記暗号化及び復号化ロジックの取決め手段による取決め候補となりうる暗号化及び復号化ロジックをメモリに記憶ないし回路に実装し、
該記憶ないし実装した取決め候補となりうる暗号化及び復号化ロジックを定期的に変更するロジック変更手段をさらに備えた
ことを特徴とする請求項１に記載の中継装置。
【請求項３】
前記暗号化及び復号化ロジックの取決め手段が、前記暗号化及び復号化ロジックに関連して、暗号化をしないで平文を取り扱う旨を取り決める
ことができるようにした請求項１または２に記載の中継装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、例えばトランスポート層に位置するＴＣＰ又はＵＤＰプロトコルに暗号化機能を追加して電子化情報の通信を行う際に使用して好適な中継装置に関する。詳しくは、通信におけるセキュリティシステム、特に、インターネット上でのデータの「漏洩」及び「改竄」、さらには「なりすまし」、「進入」ないし「攻撃」を防ぐためのものである。
【背景技術】
【０００２】
本発明者は、先に上位アプリケーションのプログラムを変更することなく、データの漏洩、改竄、なりすまし、進入、攻撃の防止機能を強化するため、送信側と受信側とで暗号化・復号化ロジックの取決めを行い、これをトランスポート層に存在するＴＣＰ又はＵＤＰに該当するプロトコルのペイロードに適用する新規な暗号化システムＴＣＰ２を提供している（例えば、特許文献１参照。）。
【０００３】
近年、インターネットを利用した通信は、パソコンさえあれば、それをネットワークに接続するだけで、誰でもネットワーク上のコンピュータにアクセスできるため、社会の中で急速に普及拡大している。一方、このインターネット通信の普及拡大に伴って、ハッカー（hacker）やクラッカー（Cracker）が他人のコンピュータシステムに侵入して、ソフトウエアやデータを盗み見たり、改竄や破壊を行ったりするという社会問題も大きくなっている。

【０００４】
具体的な不正妨害のケースとしては、まず第１に、中心的なシステムが使えなくなるように、ネットワークから大量のメッセージを送りつけコンピュータシステムの運用を妨害するシステム妨害がある。この妨害によってホストが過負荷になるとシステムダウンに陥ってしまうことも起こりうる。
【０００５】
また、ホストのパスワードを不正に入手し、機密情報を盗んだり、情報の改竄や破壊を行ったりする「不正アクセスとなりすまし」の不正妨害がある。この妨害にはコンピュータが保有する情報を勝手に書き換え、人を陥れる卑劣のものもある。また、特定のパソコンに忍び込み、メールアドレスやパスワードなど個人の機密データを搾取するスパイウエアといわれる不正行為も発生している。このようにネットワークに接続したコンピュータが持つデータベースの内容を不正に盗み見る、いわゆる盗聴行為も頻繁に行われている可能性も否定できない。
【０００６】
また、サイト若しくはサーバの運営元で、意図的に個人情報を盗むといった行為や、社内に潜むスパイなどによるサイバーテロ（Cyber terrorism）といった危機も全くないとはいえない状況である。
【０００７】
さらに、他人のコンピュータにコンピュータ障害をもたらすプログラムである「ウイルス」を送り込むという不正妨害が最近多くなっている。この送り込まれたウイルスに、メールなどを自宅で使用したパソコンが感染し、それを社内に接続した瞬間に社内のパソコン全体が感染したり、ウイルスがコンピュータの中のファイルを破壊させたり、更には、ネットワーク全体をダウンさせたりするといった問題も生じている。
【０００８】
このため、従来のＴＣＰ／ＩＰ（Transmission Control Protocol/Internet Protocol）やＵＤＰ（User Datagram Protocol）を利用したインターネット上での通信において、データの「漏洩」、「改竄」等を防ぐ機能として、ＩＰｓｅｃ（アイピーセック：Security Architecture for Internet Protocol）やＳＳＬ（Secure Socket Layer）といわれる暗号化通信が利用されている。
【０００９】
一般に、暗号化通信には、共通鍵（秘密鍵ともいう）暗号方式と公開鍵暗号方式があるが、ＩＰｓｅｃは共通鍵暗号方式を用いたものが多い。共通鍵暗号方式の方が公開鍵暗号方式より暗号化・復号化の速度が速いという特徴がある。このＩＰｓｅｃに用いられる共通鍵暗号方式は、暗号化と復号化を同じ鍵で行う方式であり、鍵の生成は送信側又は受信側のいずれで生成してもよいが、受信側と送信側とで共通鍵を使うために、鍵の交換時に内容が外部に漏れないよう細心の注意を払わなければならない。
【００１０】
共通鍵暗号方式に用いられるアルゴリズムはＤＥＳ（Data Encryption Standard：米国ＩＢＭ社が開発した共通鍵（秘密鍵）暗号化アルゴリズム）が代表的である。ＩＰｓｅｃもこのＤＥＳを暗号アルゴリズムの１つに採用している。ＩＰｓｅｃは、ＩＥＴＦ(Internet Engineer Task Force)が標準化を進めたものであり、この特徴は、単に特定のアプリケーションだけを暗号化するのではなく、ホストから送信されるあらゆる通信をＩＰレベルで暗号化する点にある。
【００１１】
これによりユーザはアプリケーションを意識することなく安全な通信を可能とすることができる。また、ＩＰｓｅｃは、将来にわたって使えるように、それ自体の仕組みを変えることなく使用する暗号アルゴリズムを変更することを可能としている。ＩＰｓｅｃで用いられる共通暗号鍵としては、ＳＰＩ（Security Pointer Index）と呼ばれる３２ビット符合が用いられ、鍵交換プロトコルとしては、ＩＫＥ（Internet Key Exchange）が用いられる。さらに、ＩＰｓｅｃには、完全性認証のためのプロトコルＡＨ（Authentication

Header）が用意されている。

【００１２】

また、ＳＳＬは、米ネットスケープ社（現在ＡＯＬに吸収合併）の開発したセキュリティ機能付ＨＴＴＰプロトコルであり、これを利用することによりクライアントとサーバがネットワーク上でお互いを認証できるようになり、クレジットカード情報などの機密性の高い情報を暗号化してやり取りすることが可能となる。これにより、データの盗聴、再送攻撃（ネットワーク上に流れたデータを盗聴して何度も繰り返して送ってくる攻撃）、なりすまし（本人の振りをして通信する）、データの改竄などを防止することができる。

【００１３】

図８のＡは従来のＩＰｓｅｃを用いた暗号化通信を行う場合のプロトコルスタックの例を示し、図８のＢは従来のＳＳＬを用いた暗号化通信を行う場合のプロトコルスタックの例を示している。

【００１４】

ＯＳＩ参照モデルは、最下層（第１層）が物理層、第２層がデータリンク層、第３層がネットワーク層、第４層がトランスポート層、第５層がセッション層、第６層がプレゼンテーション層、最上層（第７層）がアプリケーション層になっている。このＯＳＩ参照モデルにおける７階層は、通信機能を７段階に分けたものであり、その階層毎に標準的な機能モジュールを定めている。図８のＡでは、第５層のセッション層までが示されている。プロトコルスタックとは、ネットワークの各階層における機能を実現するためのプロトコルを選び、階層状に積み上げたソフトウエア群である。

【００１５】

まず、ＯＳＩ参照モデルについて概略を説明すると、第１層の物理層は、信号線の物理的な電気特性や符号の変調方法などを規定した層である。ただ、この層だけが単独で定義・実装されることは少なく、通常は、第２層のデータリンク層と共に、たとえばイーサネットの規格、などとして定義される。

【００１６】

第２層のデータリンク層は、データのパケット化や物理的なノードアドレス、パケットの送受信方法などを規定する層である。この層は、物理的な通信媒体を通して、２つのノード間でパケットをやり取りするためのプロトコルを規定するものであり、各ノードに対して、何らかのアドレスを付け、そのアドレスに基づいてパケットの送信先を特定し、パケットを通信媒体上に送信する。

【００１７】

通信媒体としては、銅配線や無線、光ファイバなど、多様なものがある。また、接続形態（トポロジー）も、１対１の対向接続だけでなく、バス型やスター型、リング型など多くの種類がある。通信媒体上に送信されたパケットは、受信側ノードに到着した時点でそのノードに取り込まれ、さらに上位のプロトコル層へと渡される。

【００１８】

物理層とデータリンク層に渡って配置されるＮＩＣ（Network Interface Card）ドライバは、パソコンやプリンタなどを構内ネットワーク（ＬＡＮ）につなぐための拡張ボードである。単にネットワークカードという場合はイーサネットにつなぐ場合が多い。

【００１９】

このＮＩＣドライバにより、データを送信したいノード（機器）がケーブルの空き状況を監視して、ケーブルが空くと送信を開始するようにしている。このとき、もし複数のノードが同時に送信を開始するとケーブル内でデータが衝突して破壊されるので、両者は送信を中止し、ランダムな時間を待って送信を再開するのである。これによって一本のケーブルを複数のノードが共有して互いに通信することができる。

【００２０】

第３層のネットワーク層は、任意の２つのノード間での通信方法を規定する層である。ＴＣＰ／ＩＰでいえばＩＰ層に相当する。データリンク層では、同一ネットワーク媒体上のノード間での通信を行うことができるが、その機能を使って、ネットワーク上に存在す

る任意の２つのノード間で、ルーティング（routing）を行いながら通信するのがこのネットワーク層の役目である。

【００２１】

ここで、ルーティングとはＴＣＰ／ＩＰネットワークにおいて目的のホストまでパケットを送信するときに、最適な経路を選択して送信することをいう。例えば、イーサネットでは、同一セグメント上のノード同士でしかお互いに通信できないが、ネットワーク層では、２つのイーサネットセグメント間でパケットをルーティングすることによって通信を行う。

【００２２】

また、電話回線を通じてコンピュータをネットワーク（イーサネット）に接続するダイヤルアップＰＰＰ（Point to Point Protocol）回線へのルーティング、また、光ファイバを使った専用線へのルーティングなど、物理的なネットワーク媒体によらずにパケットをルーティングすることができる。この目的のため、通常は、物理媒体に依存しないアドレス（ＴＣＰ／ＩＰならば、ＩＰアドレス）を各ノードに割り当て、これに基づいてルーティングを行っている。

【００２３】

ＩＰｓｅｃは、このネットワーク層で、つまりＩＰレベルでホストから送信されるあらゆる通信を暗号化するので、ユーザはアプリケーションを意識することなく安全な通信を可能とすることができるのである。

【００２４】

第４層のトランスポート層は、各ノード上で実行されている２つのプロセス間で通信を行う機能を提供している層であり、プロトコル層である。ＴＣＰ／ＩＰでいえばＴＣＰがこれに相当する。またネットワーク層では、２つのノード間での通信を行う機能を提供しているが、これを使って、２つのプロセス（アプリケーション）間で、エラーのない、仮想的な通信路を提供するのがＴＣＰの役目である。

【００２５】

すなわち、ネットワーク層ではデータを送ることはできるが、そのデータが確実に相手に届くという保証はない。また、送信した順に正しくデータが届くという保証もない。そこで、アプリケーションにとって使いやすくするために、エラーのない通信路を提供するのがＴＣＰである。必要ならばデータの再送・回復処理などを行う。

【００２６】

このトランスポート層にはＴＣＰの他にＵＤＰも配置されるが、このＵＤＰとＴＣＰの違いは、ＴＣＰがデータの補償がされているプロトコルである分、ＵＤＰより低速であるのに対して、ＵＤＰはデータ補償がない分、高速になっている点である。コンピュータ間の通信のように主としてデータを送る場合にはＴＣＰが用いられ、ＩＰ電話のように音声や画像を送る場合にはＵＤＰが多く用いられる。この通信システムは、本発明者が特許文献１において初めて提案したものである。

【００２７】

第５層のセッション層は、セッション（通信の開始から終了まで）の手順を規定する層であり、アプリケーション間でコネクションを開設して通信ができる状態にする層である。この層に配置されるソケット（socket）は、コンピュータが持つネットワーク内の住所に当たるＩＰアドレスと、ＩＰアドレスのサブアドレスであるポート番号を組み合わせたネットワークアドレスを意味している。

【００２８】

コンピュータ同士を接続する場合は、必ずソケット（ＩＰアドレスとポート番号の組）を指定して行う。図８のＢに示すように、従来の代表的な暗号化通信技術であるＳＳＬは、このセッション層で暗号化通信を実現している。

【００２９】

第６層のプレゼンテーション層は、セッション（通信の開始から終了まで）でやり取りするデータの表現方法や符号化、暗号化などを規定する層である。ＴＣＰ／ＩＰプロトコ

ルでは、この層に相当する部分はなく、通常はアプリケーション自身でストリームデータの処理をハンドリングしている。

【００３０】

また、第７層のアプリケーション層は、アプリケーション間でのデータのやり取りを規定するための層であり、ＴＣＰ／ＩＰプロトコルではこの層に相当する部分はない。例えば、電子メールのフォーマットや、文書の内部構造など、アプリケーション間で相互にデータをやり取りする場合に必要な、共通のデータ構造などを規定する層である。

【００３１】

図８のＡは、ＩＰｓｅｃを搭載した標準プロトコルスタックであるが、まず、物理層（第１層）とデータリンク層（第２層）に、ＮＩＣ（Network Interface Card）ドライバが設けられている。このドライバは、コンピュータなどのハードウエアをネットワークに接続するためのインターフェースカードのドライバであり、その内容はデータ送受信制御ソフトウエアである。例えばEthernetに接続するためのＬＡＮボードまたはＬＡＮカードがこれに相当する。

【００３２】

第３層のネットワーク層は、一部がトランスポート層(第４層)まで伸びたＩＰエミュレータ（emulator）が存在している。このトランスポート層まで延びた部分には、トランスポートとしての機能は実装していない。セッション層に、ネットワーク層の機能を提供しているだけある。このＩＰエミュレータは、ＩＰｓｅｃによる暗号化通信を行うプロトコルと、暗号化通信を行わないプロトコルであるＩＰを用途に応じて切り換えて使う働きをする。

【００３３】

また、第３層のネットワーク層にはＡＲＰ（Address Resolution Protocol）が配置されている。このＡＲＰは、ＩＰアドレスからEthernetの物理アドレスであるＭＡＣ（Media Access Control）アドレスを求めるのに使われるプロトコルである。ＭＡＣは、媒体アクセス制御と呼ばれる、ＬＡＮなどで利用される伝送制御技術であり、データの送受信単位であるフレームの送受信方法やフレームの形式、誤り訂正などを規定する技術として利用されている。

【００３４】

また、このネットワーク層には、ＩＰのエラーメッセージや制御メッセージを転送するプロトコルであるＩＣＭＰ（Internet Control Message Protocol）と、同一のデータを複数のホストに効率よく配送するための又は配送を受けるために構成されるホストのグループを制御するためのプロトコルであるＩＧＭＰ（Internet Group Management Protocol）が設けられている。そして、ネットワーク層の上位層のトランスポート層には、ＴＣＰとＵＤＰが、そしてその上位層であるセッション層にはソケット（Socket）インターフェイスが配列されている。

【００３５】

図８のＢは、暗号化処理プロトコルとしてＳＳＬを具備した標準プロトコルの例であり、ネットワーク層にＩＰｓｅｃを搭載しない代わりにソケット（セッション層）にＳＳＬが搭載されている。この他のプロトコルは図８のＡに示したものと同じである。

【００３６】

従来の代表的な暗号化通信技術の中で、ＩＰｓｅｃは、ＩＰのパケットを暗号化して送受信するものであり、したがって、ＴＣＰやＵＤＰなどの上位のプロトコルを利用するアプリケーションソフトはＩＰｓｅｃが使われていることを意識する必要がない。

【００３７】

一方、ＳＳＬでは、互いの認証レベルではＲＳＡ（Rivest Shamir Adleman：公開鍵暗号方式を開発者３人の頭文字）公開鍵暗号技術を用いたデジタル証明書が用いられ、データの暗号化ではＤＥＳなどの共通鍵暗号技術が用いられている。このＳＳＬは第５層のセッション層にあるため、特定のアプリケーションに依存することになる。

【００３８】

ＩＰｓｅｃは、ＯＳＩにおける第4層（トランスポート層）より下位の第3層（ネットワーク層）におけるデータの「漏洩」や「改竄」を防ぐ機能として実現したものである（非特許文献１を参照。）。これに対して、ＳＳＬは、第５層のセッション層における暗号化技術であり、現在インターネットで広く使われているＷＷＷ（World Wide Web）やＦＴＰ（File Transfer Protocol）などのデータを暗号化して、プライバシーに係る情報や企業秘密情報などを安全に送受信するためのものである。

【００３９】

図９に示す表１は、ＩＰｓｅｃとＳＳＬの機能を比較して記載したものである。この表から見る限り、ＩＰｓｅｃとＳＳＬは互いに相反する利点と欠点がある。

【００４０】

例えば、クライアント－クライアント間の通信では、ＳＳＬの場合、そのコマンド体系と通信内容が主従の関係、つまりクライアント／サーバとなってしまうことから、サーバを介することなくクライアント－クライアント間の通信はできなかった。すなわち、端末Ａから端末Ｂに秘密のデータをＳＳＬにより暗号化して送る場合には、必ず間にサーバを介在する必要があった。これに対して、ＩＰｓｅｃではこのような制約がないので直接通信が可能となる。

【００４１】

また、ＰＰＰ（Point to Point Protocol）モバイル環境あるいはＡＤＳＬ(Asymmetric Digital Subscriber Line)環境においては、ＩＰｓｅｃは、データの暗号化通信を開始する前に、暗号化方式の決定、鍵の交換、相互認証に使用するプロトコルであるＩＫＥ（Internet Key Exchange）プロトコルを使用した通信の中で、接続先相手の認証を行っている。

【００４２】

したがって、ＰＰＰモバイル環境（リモートクライアント）又は、ＡＤＳＬ環境の場合、ＩＰアドレスが固定できないため、ＩＰｓｅｃのゲートウェイ間で、最も使用しているＩＫＥのＭａｉｎモード、つまり認証の際に通信相手のＩＰアドレス情報を使用するモードを使用することができない。

【００４３】

なお、解決策としては、Aggressiveモードを使用することで、ＩＤ情報にＩＰアドレスを使用しなくてもよく、ＩＤ情報に例えばユーザ情報を使用し、既知共有鍵にユーザのパスワードを使用することで相手を特定することができる。但し、Aggressiveモードでは鍵交換情報と同じメッセージの中で接続先相手のＩＤを送信するため、ＩＤは暗号化されずに平文のまま送信することになる。

【００４４】

また、ＸＡＵＴＨ（Extended Authentication within IKE）を利用することにより、認証の問題を解決することができるが、ファイアウォールの設定で、リモートクライアントからのアクセスは、ＩＰアドレスが不明であるため、ＩＫＥ、ＩＰｓｅｃを全て許可にする必要があり、セキュリティ上問題が残る。ＳＳＬは、この環境下であっても、通信することが可能である。

【００４５】

また、ＩＰｓｅｃは、ＮＡＴ（Network Address Translation）やＩＰマスカレードに対応することができないという問題がある。これらに対応するためには、例えばＵＤＰのペイロードに載せるといった他の機能と併用しなければならない。

【００４６】

ＮＡＴは、インターネットに接続された企業などが１つのグローバルなＩＰアドレスを複数のコンピュータで共有する技術であり、組織内でのみ通用するＩＰアドレス（ローカルアドレス）とインターネット上のアドレス（グローバルアドレス）を相互変換する技術である。ＮＡＴに対応できないのは、ＩＰヘッダがＡＨ（Authentication Header）の認証範囲に入っているため、このローカルアドレスからグローバルアドレスの相互変換ができなくなり、サブネットの異なるローカルアドレス同士の通信ができなくなるからである

。

【００４７】

また、ＩＰマスカレードとは、ＬＡＮ内のプライベートアドレスを持つ複数のクライアントからインターネットにアクセスすることを可能とするような仕組みであり、これを利用すると、外部(インターネット)からはＩＰマスカレードが動作している端末しか見えないのでセキュリティ上から見て望ましいといえるものである。ＩＰｓｅｃがＩＰマスカレードに対応できない理由は、ＩＰｓｅｃのＥＳＰ（Encapsulating Security Payload：暗号ペイロード）ヘッダがＩＰヘッダのすぐ後にあるためである。

【００４８】

ＩＰマスカレードを実装している通常のルータは、ＩＰヘッダのすぐ後ろには、ＴＣＰ／ＵＤＰのポート番号があると判断している。したがって、ＩＰマスカレードを実装しているルータを経由すると、このポート番号を変更してしまうため、ＩＰｓｅｃは、改竄されたと判断して、ホストの認証ができないという問題が生じる。この問題は、ＵＤＰのペイロードに乗せるためのＮＡＴ－Ｔ（NAT-Traversal）をサポートする製品を利用することで回避することができる。

【００４９】

但し、ＮＡＴ－Ｔのドラフトバージョンが異なると、ＮＡＴ－Ｔ対応製品同士でも接続することができない。ＳＳＬは、この環境下であっても、通信することが可能である。

【００５０】

これに対し、ハッカーやクラッカーといわれるネットワークの不正侵入者によるＴＣＰ／ＩＰへのさまざまな攻撃、いわゆるＤｏＳ攻撃（Denial of Service：サービスを停止させる攻撃）に対しては、ＳＳＬは無力である。ＴＣＰ／ＩＰプロトコルスタックへのＤｏＳ攻撃、例えば、ＴＣＰ切断攻撃が行われると、ＴＣＰセッションが切れてしまいＳＳＬのサービスは停止してしまうのである。

【００５１】

ＩＰｓｅｃは第３層（ＩＰ層）に実装しているため、ＩＰ層にセキュリティ機能を持つので、ＴＣＰ／ＩＰ（第４層、第３層）へのＤｏＳ攻撃を防ぐことができる。しかし、ＳＳＬは、ＴＣＰ／ＩＰ（第４層、第３層）より上の層（第５層）に実装されている暗号化プロトコルであるため、ＴＣＰ／ＩＰへのＤｏＳ攻撃を防ぐことができない。

【００５２】

さらに、物理ノイズが多く通信エラーが多発するような劣悪な通信環境化における通信に対しては、ＳＳＬの方がＩＰｓｅｃに比べて効果的である。すなわち、ＩＰｓｅｃは、エラーの検出をした場合、再送動作を上位のＴＣＰに任せることになる。ＴＣＰは、再送データをＩＰｓｅｃに送るが、ＩＰｓｅｃはこの再送データであることが認識できず、再暗号を行ってしまうのである。ＳＳＬはＴＣＰでエラー回復処理を行うので同じデータを再暗号化することはない。

【００５３】

また、ＩＰｓｅｃでは異なったＬＡＮ間の通信ができない。すなわち、ＬＡＮ内のサブネットアドレスの配布管理は、ＬＡＮ内にあるＤＨＣＰ（Dynamic Host Configuration Protocol）サーバが管理しているため、ＬＡＮ内では、同一のサブネットアドレスが割り振られることはないが、異なったＬＡＮ間の通信の場合、お互いのＬＡＮ内にあるＤＨＣＰサーバが個別にサブネットアドレスを割り振っているため、同一アドレスが割り振られる可能性がある。

【００５４】

このように同一アドレスが割り振られた場合には、ＩＰｓｅｃでは通信することができない。但し、別にＩＰｓｅｃ－ＤＨＣＰサーバを立てて、同一アドレスにならないように管理すれば、通信することができる。ＳＳＬは上述したようにＯＳＩ参照モデルの第5層（セッション層）に位置しているため、下位層のＴＣＰでエラー回復処理を行うことができ、上記のような劣悪な環境下でも通信することが可能となる。

【００５５】

また、異なったネットワーク環境下における通信に対しては、ＩＰｓｅｃは、経由するノード全てを管理し、ＩＰｓｅｃが通過できるように設定変更しなければならないため、管理が大変であるが、ＳＳＬは、この環境下であっても、経由するノードの環境を意識せず通信することが可能である。

【００５６】

また、ＳＳＬは、ＵＤＰの通信をサポートしていないため、ＵＤＰを暗号通信することができない。ＴＣＰも特定のポートしかサポートしていないため、ＴＣＰ全てのポートを暗号通信することができない。これに対して、ＩＰｓｅｃは、ＵＤＰでもＴＣＰでも暗号通信することができる。

【００５７】

さらに、ＳＳＬはアプリケーションに対する互換性を持たない点において問題がある。アプリケーションは、インターネット通信を行う際にソケット（第５層）をプログラムインターフェースとして使用する。このため、アプリケーションがＳＳＬ（第５層）を使用する場合には、このソケットインターフェースをＳＳＬインターフェースに変更しなければならない。従って、ＳＳＬにアプリケーションの互換性はない。

【００５８】

これに対し、ＩＰｓｅｃは、ソケット（第５層）の下に位置しているため、アプリケーションは、ソケット（第５層）をプログラムインターフェースとしてそのまま使用することができるのでアプリケーションの互換性がある。また、ＩＰｓｅｃは、ＩＰアドレス単位で制御することができるのに対し、ＳＳＬは、ソース単位（ＵＲＬ単位、フォルダー単位）で制御することになる。

【００５９】

さらに、ＩＰｓｅｃは最大セグメントサイズが小さくなるという問題がある。すなわち、ＩＰｓｅｃでは、ＥＳＰヘッダ、ＥＳＰトレーラを使用するため、ペイロードが小さくなるため、フラグメント（パケットの分割）が発生し、スループットが低下する。また、ＴＣＰパケットでは、フラグメントが禁止であるため、エンドエンドで、ＩＰｓｅｃの通過する環境を把握し、フラグメントが発生しない最大セグメントサイズを設定する必要がある。これに対し、ＳＳＬは、通過する環境を把握する必要がないため、最大セグメントサイズを設定する必要はない。

【００６０】

以上、表１（図９）にもとづいてＩＰｓｅｃとＳＳＬの機能比較について説明したが、上述のようにＩＰｓｅｃとＳＳＬには、互いに相反する長所と短所が混在しているものである。これに対して、本発明者は先に、これらＩＰｓｅｃとＳＳＬのすべての長所を含み、さらに他にも多くのメリットを有する画期的な暗号通信プロトコルであるＴＣＰ２を提案した（特許文献１参照。）。

【００６１】

すなわち特許文献１に記載の発明においては、コンピュータ端末への不正侵入を防ぐための「暗号化の機能」をアプリケーション・プログラムそれぞれに実装する必要がなく、したがって、アプリケーション・プログラム自体を再作成する必要もなく、かつ上記暗号化機能に対応していない通信相手とも従来の平文による通信でき、さらにはＩＰｓｅｃが利用できない環境（あるいは利用したくない状況）でも暗号化や認証の恩恵を受けることができる。

【００６２】

図１０は、本発明者が先に特許文献１において提案した暗号化通信システムの一実施の形態に用いられるプロトコルスタックを示すものである。

【００６３】

この特許文献１に記載の発明に用いられるプロトコルスタックは、図１０に示すように、ＯＳＩ７階層の物理層（第１層）とデータリンク層（第２層）に相当する階層に、ＮＩＣ（Network Interface Card）ドライバ１１が配列される。このドライバは、既に述べたように、コンピュータなどのハードウエアをネットワークに接続するためのインターフェ

ースカードのドライバであり、その内容はデータ送受信制御ソフトウエアである。例えばEthernetに接続するためのＬＡＮボードまたはＬＡＮカードがこれに相当する。

【００６４】

第３層のネットワーク層には、一部がトランスポート層（第４層）まで延びたＩＰエミュレータ（emulator）３が存在している。上記延びた部分には、トランスポートとしての機能は実装していない。セッション層に、ネットワーク層の機能を提供しているだけある。このＩＰエミュレータ３は、暗号化通信を行うプロトコルである「ＩＰｓｅｃ　ｏｎ　ＣＰ」１３ｂと、「ＩＰ　ｏｎ　ＣＰ」１３ａを用途に応じて切り換えて使う働きをする。ここで、「ｏｎ　ＣＰ」とは、クラッキング・プロテクタ（ＣＰ）による、「進入」、「攻撃」の監視、破棄、切断ないし通過制限の対象となっていること、又は、設定によりなりうることを示している。

【００６５】

また、ネットワーク層には「ＡＲＰ　ｏｎ　ＣＰ（Address Resolution Protocol on Cracking Protector）」が配列されている。この「ＡＲＰ　ｏｎ　ＣＰ」は、クラッカー（Cracker）への保護対策を具備したＩＰアドレスからEthernetの物理アドレスであるＭＡＣ（Media Access Control）アドレスを求めるのに使われるプロトコルである。ＭＡＣは、媒体アクセス制御と呼ばれる、ＬＡＮなどで利用される伝送制御技術であり、データの送受信単位であるフレームの送受信方法やフレームの形式、誤り訂正などを規定する技術として利用されている。

【００６６】

ここで、ＩＰエミュレータ１３は、本発明による各種のセキュリティ機能を、従来のＩＰ周辺のスタックに整合させるためのソフトウエア又はファームウエアである。すなわち、ＩＰのエラーメッセージや制御メッセージを転送するプロトコルであるＩＣＭＰ（Internet Control Message Protocol）１４ａ、同一のデータを複数のホストに効率よく配送するための又は配送を受けるために構成されるホストのグループを制御するためのプロトコルであるＩＧＭＰ（Internet Group Management Protocol）１４ｂ、ＴＣＰ１５、ＵＤＰ１６さらにソケット（Socket）インターフェイス１７に整合させるためのソフトウエア、又はファームウエア、ないしはハードウエア（電子回路、電子部品）である。このＩＰエミュレータ１３により、ＩＰｓｅｃの暗号化・復号化及び必要な認証情報付加・認証等の前後の適合処理を行うことができる。

【００６７】

このＩＰエミュレータ１３の上層のトランスポート層（第４層）には、ＴＣＰエミュレータ１５とＵＤＰエミュレータ１６が配置されている。ＴＣＰエミュレータ１５は、暗号化通信を行うプロトコルである「ＴＣＰｓｅｃ　ｏｎ　ＣＰ」１５ｂと、通常の通信プロトコルである「ＴＣＰ　ｏｎ　ＣＰ」１５ａを用途に応じて切り換えて使う働きをする。同様に、ＵＤＰエミュレータ１６は、暗号化通信を行うプロトコルである「ＵＤＰｓｅｃ　ｏｎ　ＣＰ」１６ｂと、通常の通信プロトコルである「ＵＤＰ　ｏｎ　ＣＰ」１６ａを用途に応じて切り換えて使う働きをする。

【００６８】

この特許文献１の最も特徴とするべき点は、このトランスポート層（第４層）に、ＴＣＰｓｅｃ１５ｂと、ＵＤＰｓｅｃ１６ｂの暗号化通信プロトコルを搭載したことである。ＴＣＰｓｅｃ１５ｂとＵＤＰｓｅｃ１６ｂについては後述する。

【００６９】

このトランスポート層（第４層）の上層のセッション層（第５層）には、ＴＣＰ及びＵＤＰ等のプロトコルとデータのやりとりを行うソケット（socket）インターフェイス１７が設けられている。このソケットの意味は、既に述べたようにコンピュータが持つネットワーク内の住所に当たるＩＰアドレスと、ＩＰアドレスのサブアドレスであるポート番号を組み合わせたネットワークアドレスを意味しており、実際には、一連のヘッダの追加ないし削除をまとめて行う、単一のソフトウエアプログラムモジュール（実行プログラム等）あるいは単一のハードウエアモジュール（電子回路、電子部品等）からなっている。

【００７０】
このソケットインターフェース１７は、さらに上位のアプリケーションからの統一的なアクセス方式を提供するものであり、引数の種類や型など従来と同様のインターフェイスを保つようにしている。
【００７１】
ＴＣＰエミュレータ１５は、トランスポート層において、データの漏洩・改竄の防止の機能、すなわち暗号化、完全性認証及び相手認証等の機能を持つＴＣＰｓｅｃ１５ｂと、このような暗号化、完全性認証、及び相手認証等の機能を持たない通常のプロトコルＴＣＰ１５ａのいずれかにパケットを振り分ける働きをもっている。また、ＴＣＰｓｅｃ１５ｂ及びＴＣＰ１５ａのいずれもクラッキング・プロテクタ（ＣＰ）を備えているため、そのいずれを選択した場合でも、クラッカーによる「進入」、「攻撃」に対して防御する機能を実現することができる。ＴＣＰエミュレータ１５は上位層であるソケットとのインターフェイスの役割も果たしている。
【００７２】
また、既に述べたようにＴＣＰがエラー補償機能を有するのに対して、ＵＤＰはエラー補償機能を持たないが、その分転送速度が速く、かつブロードキャスト機能を備えているという特徴がある。ＵＤＰエミュレータ１６は、ＴＣＰエミュレータ１５と同様に、データの漏洩・改竄の防止の機能、すなわち暗号化、完全性認証及び相手認証等の機能を持つＵＤＰｓｅｃ１６ｂと、このような暗号化、完全性認証、及び相手認証等の機能を持たない通常のプロトコルＵＤＰ１６ａのいずれかにパケットを振り分ける働きを持っている。
【００７３】
図１０に示すように、ソケット１７、ＴＣＰエミュレータ１５、ＵＤＰエミュレータ１６、「ＴＣＰｓｅｃ　ｏｎ　ＣＰ」１５ｂ、「ＵＤＰｓｅｃ　ｏｎ　ＣＰ」１６ｂ、「ＴＣＰ　ｏｎ　ＣＰ」１５ａ、「ＵＤＰ　ｏｎ　ＣＰ」１６ａ、「ＩＣＭＰ　ｏｎ　ＣＰ」１４ａ、「ＩＧＭＰ　ｏｎ　ＣＰ」１４ｂ、ＩＰエミュレータ１３、「ＩＰ　ｏｎ　ＣＰ」１３ａ、及び「ＡＲＰ　ｏｎ　ＣＰ」１２からなるプロトコルスタックが本発明の暗号化処理を行うためのプロトコルスタックであり、以下、このプロトコルスタックを総称してＴＣＰ２と呼ぶことにする。
【００７４】
なお、ＴＣＰ２には「ＩＰｓｅｃ　ｏｎ　ＣＰ」１３ｂは必須のものとして含まれていないが、「ＩＰｓｅｃ　ｏｎ　ＣＰ」１３ｂを含めてＴＣＰ２とすることもできる。
【００７５】
特許文献１に開示されているＴＣＰ２には、上述した暗号化処理を行うためのプロトコルスタックの他に、ＴＣＰ、ＵＤＰ、ＩＰ、ＩＰｓｅｃ、ＩＣＭＰ、ＩＧＭＰ、ＡＲＰの標準プロトコルスタックも含んでいる。そして、これらの標準プロトコルにＣＰ（クラッキング・プロテクト）を実装し、各プロトコルスタックに対する通信からの攻撃、及び、アプリケーション・プログラムからの攻撃（トロイの木馬、プログラムの改竄、正規ユーザの不正使用など）を防御することができるようにしている。
【００７６】
また、ＴＣＰ２では、ＴＣＰエミュレータ１５を実装し、このＴＣＰエミュレータ１５は、セッション層にあるソケット（Socket）１７、及びネットワーク層にあるＩＰエミュレータ１３から見て、互換性を保つため、外向きには標準ＴＣＰと同じに見せることができる。実際は、ＴＣＰ２の機能として、ＴＣＰとＴＣＰｓｅｃを切り替えて実行する。ＴＣＰｓｅｃは、本発明であるトランスポート層での暗号化及び認証機能である。
【００７７】
また、同様に、ＴＣＰ２では、ＵＤＰエミュレータ１６を実装しており、ＵＤＰエミュレータ１６は、セッション層であるソケット（Socket）１７、及び、ネットワーク層であるＩＰエミュレータ１３から見て、互換性を保つため、外部からは標準ＵＤＰとして見せることができる。実際は、ＴＣＰ２の機能として、ＵＤＰ、ＵＤＰｓｅｃを切り替えて実行する。ＵＤＰｓｅｃは、特許文献１に記載の発明であるトランスポート層での暗号化及

び認証機能である。

【００７８】

次に、ＴＣＰ２において、特に重要な機能である「データ漏洩」を防ぐ機能であるＴＣＰｓｅｃ１５ｂ及びＵＤＰｓｅｃ１６ｂについて説明する。

【００７９】

ＴＣＰｓｅｃ１５ｂ及びＵＤＰｓｅｃ１６ｂのための暗号化・復号化の方法（アルゴリズム、ロジック（論理））としては、公知の秘密鍵（共通鍵）暗号アルゴリズムが用いられる。例えば、１９６０年代にＩＢＭ社によって開発された秘密鍵暗号アルゴリズムであるＤＥＳ（Data Encryption Standard）や、その改良版としての３ＤＥＳが用いられる。

【００８０】

また、その他の暗号アルゴリズムとしては、1992年にスイス工科大学のJames L.Massey氏とXuejia Lai氏によって発表されたＩＤＥＡ（International Data Encryption Algorithm）も用いられる。この暗号アルゴリズムは、データを６４ビットのブロックに区切って暗号化するもので暗号鍵の長さは１２８ビットである。秘密鍵暗号を効率よく解読する線形解読法や差分解読法に対しても十分な強度を持つように設計されている。

【００８１】

また、特許文献１に記載の発明に用いられるＴＣＰｓｅｃ１５ｂ及びＵＤＰｓｅｃ１６ｂの暗号方式として、ＦＥＡＬ（Fast data Encipherment Algorithm）、ＭＩＳＴＹ、ＡＥＳ（Advanced Encryption Standard）といった暗号方式も利用されるほか、また、独自に作成した秘密の暗号化・復号化アルゴリズムを利用することもできる。ここで、ＦＥＡＬは、日本電信電話株式会社（当時）が開発した暗号方式で、暗号化と復号化に同じ鍵をもちいる秘密鍵型の暗号方式である。このＦＥＡＬは、ＤＥＳに比べて高速に暗号化と復号化ができるという利点がある。

【００８２】

次に、同じく特許文献１に記載の発明に利用される暗号方式であるＭＩＳＴＹは、三菱電機株式会社が開発した秘密鍵型の暗号方式であり、ＩＤＥＡと同様にデータを６４ビットのブロックに区切って暗号化する。鍵の長さは１２８ビットである。暗号化と復号化には同じプログラムが使われる点はＤＥＳなどと同じである。この方式も秘密鍵暗号を効率よく解読する線形解読法や差分解読法に対しても十分な強度を持つように設計されている。

【００８３】

また、ＡＥＳは、米国商務省標準技術局によって選定作業が行われている、米国政府の次世代標準暗号化方式であり、現在の標準的な暗号方式であるＤＥＳに代わる次世代の暗号標準として開発が進められたものである。世界に公募して集められて幾つかの暗号方式の中から、2000年10月に、ベルギーの暗号開発者Joan Daemen氏とVincent Rijmen氏が開発したRijndaelという方式が採用された。

【００８４】

このように、特許文献１に記載の発明に適用されるＴＣＰｓｅｃ１５ｂ及びＵＤＰｓｅｃ１６ｂの暗号方式としては、既に知られているさまざまな秘密鍵の暗号アルゴリズムを採用することができるほか、ユーザが独自に開発した秘密鍵（共通鍵）暗号方式も利用することが可能である。

【００８５】

さらに、いわゆる「なりすまし」及び「データの改竄」などを防ぐための「相手認証」及び「完全性認証」の方法として、公開鍵や事前秘密共有（Pre-shared）を利用したアルゴリズム、例えば、ＭＤ５（Message Digest 5）、ＳＨＡ１（Secure Hash Algorithm １）などの認証アルゴリズムが用いられる。また、このような公知の認証アルゴリズムに代えて独自の一方向関数を利用したアルゴリズムを採用することもできる。

【００８６】

このＭＤ５は、認証やデジタル署名に用いられるハッシュ関数（一方向要約関数）の一つであり、原文を元に固定長のハッシュ値を発生し、これを通信経路の両端で比較するこ

とにより、通信途中で原文が改竄されていないかを検出することができるものである。このハッシュ値は擬似的な乱数のような値をとり、これを基にしては原文を再生できないようになっている。また、同じハッシュ値を生成する別のメッセージを作成することも困難になっている。

【００８７】

ＳＨＡ１も、認証やデジタル署名などに使われるハッシュ関数の一つであり、２の６４乗ビット以下の原文から１６０ビットのハッシュ値を生成し、通信経路の両端で比較することにより、通信途上の原文の改竄を検出するものである。この認証アルゴリズムは従来のインターネットの暗号化通信の代表的なものであるＩＰｓｅｃにも採用されている。

【００８８】

なお、これらの認証アルゴリズムについては、ＤＨ（Diffie-Hellman）公開鍵配送法や、ＩＰｓｅｃと同様のＩＫＥ（Internet Key Exchange）プロトコル（ＵＤＰの５００番）などにより安全な鍵交換ができるように設計され、しかも、定期的に暗号化／完全性認証アルゴリズム（論理）自体やそのための鍵の集合／定義域が変更されるように、プロトコルドライバープログラム（ＴＣＰｓｅｃ１５ｂ、ＵＤＰｓｅｃ１６ｂなど）によりスケジュールされている。

【特許文献１】国際公開ＷＯ　２００５／０１５８２７　Ａ１号公報

【非特許文献１】R.Atkinson,1995年8月「Security Architecture for the Internet Protocol」RFC1825

【発明の開示】

【発明が解決しようとする課題】

【００８９】

上述したように特許文献１に記載の発明においては、本発明者が提案するＴＣＰ２を用いることによって、上位アプリケーションのプログラムを変更することなく、データの漏洩、改竄、なりすまし、進入、攻撃の防止機能を強化するため、送信側と受信側とで暗号化・復号化ロジックの取決めを行い、これをトランスポート層に存在するＴＣＰ又はＵＤＰに該当するプロトコルのペイロードに適用する新規な暗号化システムを実現することができる。

【００９０】

ところが上述した特許文献１に記載の発明においては、本発明者が提案するＴＣＰ２をトランスポート層に設けるために、そのペイロードには、いわゆる電子メール文書の送信を行う際のＳＭＴＰコマンドや、受信を行う際のＰＯＰコマンドも含まれている。従って上述のトランスポート層で暗号化の行われた情報では、ＳＭＴＰコマンドやＰＯＰコマンドも暗号化されるために、外部からは当該情報を電子メール文書として認識することができなくなってしまう。

【００９１】

すなわち、ＴＣＰ２を実施した場合には、インターネット上でのデータの「漏洩」及び「改竄」、さらには「なりすまし」、「進入」ないし「攻撃」を防ぐことができるものであるが、このままでは、暗号化の行われた情報を電子メール文書として認識することができなくなってしまう。従って、従来のＳＭＴＰコマンドやＰＯＰコマンドを用いるいわゆるメールサーバ等を利用したメールシステムでは、文書の送受信を行うことができなくなってしまうものである。

【００９２】

この発明はこのような問題点に鑑みて成されたものであって、本発明の目的は、ＴＣＰ２の機能を実現しているシステムにおいて、電子メール文書の送受信を良好に行うことのできる中継装置を実現するものである。

【課題を解決するための手段】

【００９３】

上記の課題を解決し、本発明の目的を達成するため、請求項１に記載された発明は、クライアント装置でトランスポート層に位置するＴＣＰ又はＵＤＰプロトコルに暗号化機能

を追加して電子化情報の通信を行う際に用いられる中継装置であって、クライアント装置から受信した情報単位としてのパケットを暗号化して相手装置に送信し、また相手装置から受信したパケットをクライアント装置に送信する通信手段を備え、通信手段は少なくともクライアント装置との間で対応する暗号化及び復号化ロジックを取り決める取決め手段を有し、相手装置に送信する際には、受信したパケットの内の少なくともＴＣＰプロトコルのペイロードを取決め手段により取り決めた復号化ロジックに従って復号化し、復号化したパケットのＳＭＴＰコマンドを解析し、パケットの電子メールのタイトル、本文、添付ファイルを暗号化して相手装置に送信し、相手装置から受信した際には、受信したパケットのＰＯＰコマンドを解析し、パケットの電子メールのタイトル、本文、添付ファイルを復号化し、復号化したパケットのＴＣＰプロトコルのペイロードを取決め手段により取り決めた暗号化ロジックに従って暗号化してクライアント装置に送信し、トランスポート層のＴＣＰ又はＵＤＰプロトコルを用いて暗号化及び復号化ロジックに基づいた通信を行うことを特徴とする中継装置である。

【００９４】

請求項２の記載による中継装置においては、暗号化及び復号化ロジックの取決め手段による取決め候補となりうる暗号化及び復号化ロジックをメモリに記憶ないし回路に実装し、この記憶ないし実装した取決め候補となりうる暗号化及び復号化ロジックを定期的に変更するロジック変更手段をさらに備えたことを特徴とするものである。

【００９５】

請求項３の記載による中継装置においては、暗号化及び復号化ロジックの取決め手段が、暗号化及び復号化ロジックに関連して、暗号化をしないで平文を取り扱う旨を取り決めることができるようにしたものである。

【発明の効果】

【００９６】

以上述べたように、本発明によれば、ＴＣＰ２の機能を中継装置に装備するようにしたことによって、インターネット上でのデータの「漏洩」及び「改竄」、さらには「なりすまし」、「進入」ないし「攻撃」を防ぐことができると共に、電子メール文書の送受信を良好に行うことができるものである。

【発明を実施するための最良の形態】

【００９７】

以下、図面を参照して本発明を説明するに、図１は本発明を適用した中継装置の一実施形態例の構成を示すブロック図である。

【００９８】

図１において、中継装置１００は、それ自体がパーソナルコンピュータと同等の機能を有しているものである。そこでこの中継装置１００には、それぞれネットワーク２００、３００と接続されるＮＩＣ（Network Interface Card）ドライバ１ａ、１ｂが設けられる。またこれらのＮＩＣドライバ１ａ、１ｂを含む物理層とデータリンク層に対して、ネットワーク２００、３００上に存在する任意の２つのノード間で、ルーティング（routing）を行いながら通信するための通信方法を規定するアプリケーション解析（Application Analysis）機能２０を含むネットワーク層とトランスポート層が設けられる。

【００９９】

そして、これらのデータリンク層とネットワーク層との間に、本発明者が先に提案した「ＴＣＰ２」３０の機能を設ける。なお、この「ＴＣＰ２」３０には、旧来のＴＣＰ／ＩＰを併設することもできる。さらに、この「ＴＣＰ２」３０の機能は、ソフトウエア、若しくはハードウエアとして設けることができるものであり、この「ＴＣＰ２」３０の機能を制御したり、暗号化及び復号化ロジックを定期的に変更したり、必要に応じて暗号化をしないで平文を取り扱う旨の取り決めをしたりするための手段として、外部機能（ＥＸＰ．）４０が設けられている。

【０１００】

このように、本実施形態例において、本発明者が先に提案したＴＣＰ２の機能を中継装

置に装備したことによって、例えばネットワーク２００、３００がインターネット等の公衆ネットワークであった場合にも、インターネット上でのデータの「漏洩」及び「改竄」、さらには「なりすまし」、「進入」ないし「攻撃」を防ぐことができる。

【０１０１】

図２は、上述のＴＣＰ２の機能を装備した中継装置１００を用いて構築される通信ネットワークの具体的な実施形態例を示している。

【０１０２】

この図２において、クライアント装置（パーソナルコンピュータ）４１０には、ＭＵＡ（Mail User Agent）４１１が設けられており、このＭＵＲ４１１によって電子メールの作成や表示が行われる。また、クライアント装置４１０には、上述のＴＣＰ２の機能を実現する暗号化アプリケーション４１２が設けられており、このＴＣＰ２が搭載された暗号化アプリケーション４１２によりＭＵＡ４１１で作成された平文の電子メールが暗号化される。なお、図中の◎は暗号化、●は復号化の機能を表している。

【０１０３】

上述したＭＵＡ４１１には、電子メールの送受信のためのソフトウエアが搭載されており、このＭＵＡ４１１において、ＳＭＴＰコマンドが生成されて、送信時に作成された電子メールに添付される。また、受信の際には、ＭＵＡ４１１において受信パケットが形成されると共に、受信されたパケットに添付されたＰＯＰコマンドの解析が行われる。そして、このＰＯＰコマンドの解析によって受信が完了し、受信された電子メールを表示するなどの処理がなされる。

【０１０４】

これにより、クライアント装置４１０からはＴＣＰ２で暗号化された電子メール文書が中継装置１００に送信される（◎印）。そこでこの中継装置１００には、上述のＴＣＰ２の機能１０１が装備されており、予めクライアント装置４１０との間で対応する暗号化及び復号化ロジックの取り決めがＩＫＥ（鍵交換）等により行われている。そしてクライアント装置４１０から送信された情報を受信すると、受信した情報単位としてのパケットのうち、少なくともＴＣＰプロトコルのペイロードを予め取り決めた復号化ロジックに従って復号化する（●印）。

【０１０５】

また、中継装置１００には、アプリケーション解析（Application Analysis）の機能１０２が設けられ、このアプリケーション解析機能１０２によって、復号化したパケットのＳＭＴＰコマンドの解析が行われる。そして、この中継装置１００は、解析されたＳＭＴＰコマンドに従ってパケットの電子メールのタイトル、本文、添付ファイルを再度暗号化して（◎印）インターネット５００等を通じて相手装置に送信する。なお、中継装置１００における再度の暗号化には上述のＴＣＰ２の機能１０１が用いられる。但し、この場合には、予め電子メール通信を行う相手側の中継装置６００との間で対応する暗号化及び復号化ロジックの取り決めをＩＫＥ（鍵交換）等により行う必要があることは言うまでもない。

【０１０６】

また、中継装置６００では、上述と同様のＴＣＰ２の機能６０１で復号化が行われ（●印）、アプリケーション解析の機能６０２により復号化したパケットのＳＭＴＰコマンドの解析が行われる。そして、解析されＳＭＴＰコマンドに基づいてメールサーバ装置７００のＳＭＴＰサーバ７０１にパケットの電子メールのタイトル、本文、添付ファイルが保存される。また、受信の要求があると、メールサーバ装置７００のＰＯＰ３サーバ７０２から再度中継装置６００のアプリケーション解析の機能６０２でＰＯＰ３コマンドが生成され、ＴＣＰ２の機能６０１で暗号化されて送信が行われる（◎印）。

【０１０７】

中継装置６００からの暗号化され中継装置１００で受信された電子メールは、中継装置１００のＴＣＰ２機能１０１で復号化され（●印）、アプリケーション解析の機能１０２によって、この復号化したパケットのＰＯＰ３コマンドの解析が行われる。さらに解析さ

れたＰＯＰ３コマンドとパケットの電子メールのタイトル、本文、添付ファイルに対してＴＣＰ２の機能１０１で暗号化が行われる（◎印）。なお上述の説明では、送信時と受信時の中継装置１００を同じものとしたが、この中継装置１００は別物であってもよいことは当然である。ただしその場合には、別物の中継装置と中継装置６００の間で暗号化及び復号化ロジックの取り決めがＩＫＥ（鍵交換）等により行われることが不可欠である。

【０１０８】

一方、クライアント装置４１０では、中継装置１００からのパケットがＴＣＰ２の機能を実現する暗号化アプリケーション４１２で復号化される（●印）。そして、復号化された平文の電子メールがＭＵＡ４１１に供給されて、受信された電子メールのＰＯＰ３コマンド等に基づき電子メール文書の表示等が行われる。なお、ここでは送信時と受信時のクライアント装置４１０を同じものとして説明したが、別のクライアント装置であってもよいことは言うまでもない。このようにして、トランスポート層のＴＣＰ又はＵＤＰプロトコルを用いて暗号化及び復号化ロジックに基づいた電子メールの通信を行うことができる。

【０１０９】

図２に示された通信ネットワークにおいては、クライアント装置４１０とメールサーバ側の中継装置６００との間の全ての区画でトランスポート層のプロトコルを用いて暗号化及び復号化ロジックに基づいた通信が行われる。そしてこのような通信が行われることにより、クライアント装置（パーソナルコンピュータ）と外部との通信における全ての通信区画で、データの「漏洩」及び「改竄」、さらには「なりすまし」、「進入」ないし「攻撃」を防ぐことができる。

【０１１０】

図３は、本発明者が先に提案したＴＣＰ２のパケット構造を示した図である。この図３のＡは、例えばEthernetのフレームを示したものであり、このフレームには先頭の同期用信号に続いて、開始信号と受信側ＭＡＣ（Media Access Control）アドレス、送信側ＭＡＣアドレスが設けられ、その後にフレーム長／タイプの領域とデータ領域、ＣＲＣ（Cyclic Redundancy Check）等の誤り訂正符号が配置されている。そしてこのデータ領域には図３のＢに示すように、ＩＰパケットが設けられ、このＩＰパケットはＩＰヘッダとペイロードとからなる。

【０１１１】

また、ＩＰパケットのペイロードには図３のＣに示すＴＣＰパケットが設けられ、このＴＣＰパケットはＴＣＰヘッダとペイロードとからなる。さらにＴＣＰパケットのペイロードには図３のＤに示すアプリケーションデータが設けられる。そして、電子メールの場合には、このアプリケーションデータはＳＭＴＰコマンドまたはＰＯＰ３コマンドと電子メール文書のデータとから構成されることになる。

【０１１２】

そしてこの場合に、本発明者が先に提案したＴＣＰ２による暗号化では、図３のＣに示すＴＣＰパケットのペイロードの全体が暗号化されるために、ＳＭＴＰコマンドやＰＯＰ３コマンドも暗号化され、外部からは当該情報を電子メール文書として認識することができなくなってしまう。これに対して本発明では、アプリケーションデータのＳＭＴＰコマンドまたはＰＯＰ３コマンドを解析して、これらのコマンドを除いた部分のみ暗号化することで、外部からも電子メール文書として認識できるようにするものである。

【０１１３】

図４は、送信時の処理を示したフローチャートである。

図４において、まず、ＭＵＡ４１１において送信メールが作成され（ステップＳ１１）、メールの送信処理が開始される（ステップＳ１２）。その後、クライアント装置４１０内の暗復号アプリケーション４１２にパケットが送られると、クライアント装置４１０は中継装置１００のＴＣＰ２と相互認証を行う（ステップＳ１３）。ステップＳ１３における認証がＮＧの場合、つまり認証に失敗した場合は、ＴＣＰ２の設定の見直しが行われ（ステップＳ１４）、再送信が行われる（ステップＳ１５）。

【０１１４】
ステップＳ１３において相互認証がＯＫの場合、つまり認証に成功した場合は、パケットは暗号化されて中継装置１００に送られることになる（ステップＳ１６）。続いて、中継装置１００にてパケットが復号化され、アプリケーション解析機能１０１でＳＭＴＰコマンドの解析が行われる（ステップＳ１７）。その後、中継装置１００と中継装置６００のＴＣＰ２で相互認証が行われ（ステップＳ１８）、ここで認証がＮＧ（失敗）の場合は、ＴＣＰ２の設定の見直しが行われる（ステップＳ１９）。そして、再送信が行われる（ステップＳ２０）。

【０１１５】
ステップＳ１８で認証がＯＫ（成功）の場合は、送信されるパケットのＳＭＴＰコマンド以外が暗号化され、中継装置６００に送られる（ステップＳ２１）。そして、中継装置６００にてパケットが復号化されて、アプリケーション解析機能６０２でＳＭＴＰコマンドの解析が行われる（ステップＳ２２）。そして、平文に変換されたパケットがメールサーバ７００内のＳＭＴＰサーバ７０１に送られ（ステップＳ２３）、送信が完了する（ステップＳ２４）。以上が、電子メールの送信動作の説明である。

【０１１６】
次に、電子メールの受信時の処理について説明する。図５は、受信時の処理を示すフローチャートである。
図５に示されるように、メール受信の処理が開始されると（ステップＳ３１）、メールサーバ７００内のＰＯＰ３サーバ７０２が受信メールをクライアントに送る（ステップＳ３２）。このとき、この受信メールのパケットは、まず中継装置６００に送られる（ステップＳ３３）。そして、中継装置６００におけるアプリケーション解析機能６０２によりＰＯＰコマンドの解析が行われる（ステップＳ３４）。続いて、中継装置６００は中継装置１００のＴＣＰ２と相互認証を行う（ステップＳ３５）。このステップＳ３５で相互認証がＮＧ（失敗）であった場合は、ＴＣＰ２の設定の見直しが行われ（ステップＳ３６）、受信メールパケットの再送信が行われる（ステップＳ３７）。

【０１１７】
一方、ステップＳ３５で認証がＯＫ（成功）の場合は、電子メールのパケットのＰＯＰ３コマンド以外が暗号化され、中継装置１００に送られる（ステップＳ３８）。続いて中継装置１００にて電子メールの受信パケットが復号化され、中継装置１００のアプリケーション解析機能１０２でＰＯＰ３コマンドの解析が行われる（ステップＳ３９）。
その後、中継装置１００はクライアント装置４１０のＴＣＰ２と相互認証を行い（ステップＳ４０）、このステップＳ４０で認証がＮＧ（失敗）の場合は、ＴＣＰ２の設定の見直しが行われ（ステップＳ４１）、受信メールの再送信が行われる（ステップＳ４２）。

【０１１８】
一方、ステップＳ４０で認証がＯＫ（成功）の場合は、受信メールのパケットが暗号化され、クライアント装置４１０に送られ、クライアント装置４１０内の暗復号アプリケーション機能４１２で復号化される（ステップＳ４３）。そしてクライアント端末４１０のＭＵＡ４１１に受信メールパケットが送られ（ステップＳ４４）、受信が完了する（ステップＳ４５）。以上が、電子メールの受信処理の説明である。

【０１１９】
以上説明した本発明の中継装置によれば、パーソナルコンピュータと外部との通信において、インターネット上でのデータの「漏洩」及び「改竄」、さらには「なりすまし」、「進入」ないし「攻撃」を防ぐことができる。

【０１２０】
最後に、本発明のＴＣＰ２が、従来のＩＰｓｅｃあるいはＳＳＬと比べて如何に優位であるかという点について、図６及び図７に基づいて説明する。図６は、図９に示したＩＰｓｅｃとＳＳＬの機能比較表にＴＣＰ２の機能を追加して示したものである。

【０１２１】
この図６から明らかなように、ＩＰｓｅｃ及びＳＳＬが持っている様々な問題点（これ

らについては背景技術において示した）を、ＴＣＰ２を採用することによりことごとく解決していることが分かる。例えば、ＳＳＬでは対応が困難であった、クライアント－クライアント間の通信、ＴＣＰ／ＩＰプロトコルへのＤｏＳ攻撃、全てのＵＤＰポートあるいはＴＣＰポートのセキュアな通信、ソケットプログラムを変更しなければならなかったアプリケーションでの制限などに、ＴＣＰ２は完全に対応している。

【０１２２】

また、ＩＰｓｅｃでは対応が困難であった、エラーが多発する劣悪な環境下での通信、異なったＬＡＮ間での通信、複数キャリア経由の接続、ＰＰＰモバイル環境、ＡＤＳＬ環境での通信に対しても、ＴＣＰ２は完全にサポートしている。さらに、モバイル環境下やＡＤＳＬ環境下でＶｏＩＰ（Voice over Internet Protocol）を使ったインターネットに対しては、ＩＰｓｅｃ及びＳＳＬとも表１及び表２に示すように問題があるが、本発明のＴＣＰ２によれば、どちらの環境下でも対応可能である。

【０１２３】

また、異なったＬＡＮ間でＶｏＩＰを使ったインターネット電話に対しても、ＩＰｓｅｃとＳＳＬでは対応不可能であったが、本発明のＴＣＰ２によれば完全に対応することができる。

【０１２４】

図７は、ＴＣＰ２の優位性を説明するための図であるが、セキュリティのないプロトコルスタック（ａ）に、従来のＳＳＬを適用したケース（ｂ）と、ＩＰｓｅｃを適用したケース（ｃ）と、本発明のＴＣＰ２（ＴＣＰｓｅｃ／ＵＤＰｓｅｃ）を適用したケース（ｄ）を比較して示している。

【０１２５】

図７（ｂ）のＳＳＬは既に述べたように、セッション層（第５層）のソケットに設けられているので、上位のアプリケーションに対する互換性がない。このため、ＳＳＬ自体、上述のような問題を抱えることになっている。また図７（ｃ）のＩＰｓｅｃは、ネットワーク層（第３層）にあり、ＩＰ層での互換性がないため、ネットワークを構成する上で上述したような様々な制約を受けることになる。

【０１２６】

これに対して、図７（ｄ）のＴＣＰ２（ＴＣＰｓｅｃ／ＵＤＰｓｅｃ）は、トランスポート層（第４層）に導入する暗号化技術であり、このためアプリケーションから見るとソケットをそのまま利用することができ、またネットワークから見るとＩＰもそのまま利用できるのでネットワークを構成する上での制約は受けない。

【０１２７】

以上のように、本発明の中継装置は、本発明者が先に提案したＴＣＰ２を用いることによって、既存の暗号化処理システムに比べても、特にデータの漏洩、改ざん、なりすまし、進入そして攻撃に対して極めて高いセキュリティ機能を有するものである。

【０１２８】

なお、本発明は、以上説明した実施の形態例に限定されるものではなく、特許請求の範囲に記載した本発明の要旨を逸脱しない範囲において、さらに多くの実施形態を含むものであることは言うまでもない。

【図面の簡単な説明】

【０１２９】

【図１】本発明を適用した中継装置の一実施形態の構成を示すブロック図である。

【図２】本発明による中継装置を適用した具体的な通信ネットワークの一実施形態を示す構成図である。

【図３】その説明のための図である。

【図４】その送信時の動作を説明するためのフローチャート図である。

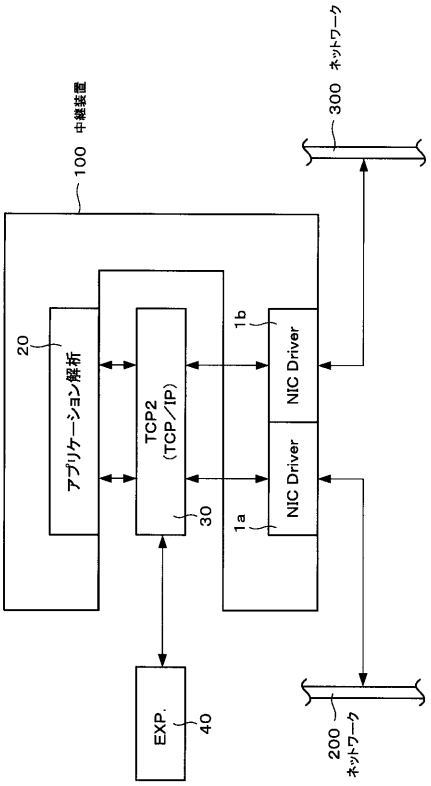
【図５】その受信時の動作を説明するためのフローチャート図である。

【図６】従来の技術との比較の説明を行うための表図である。

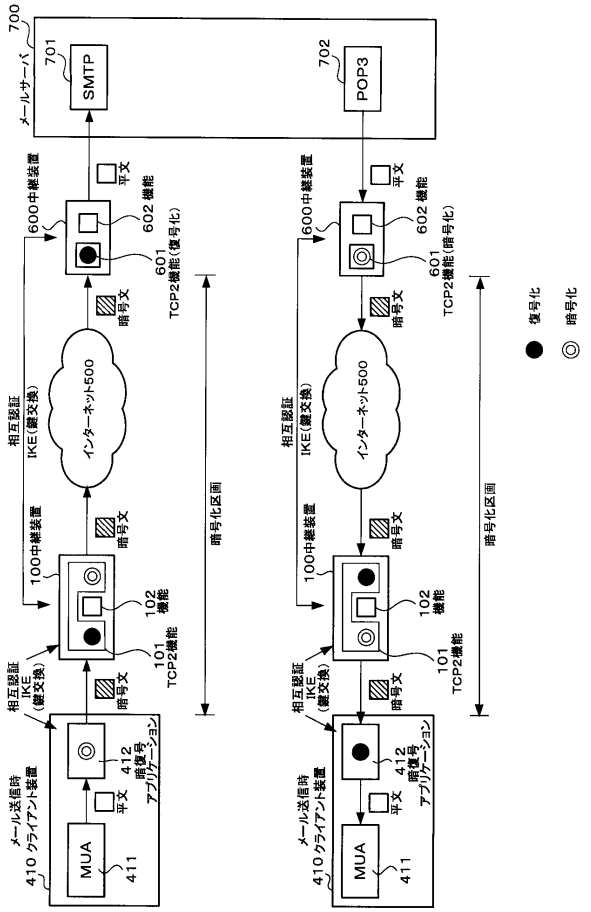
【図７】従来の技術との比較の説明を行うための説明図である。

【図８】従来のＩＰｓｅｃ及びＳＳＬを用いた標準的な通信のプロトコルスタックを示す図である。
【図９】従来の技術の説明を行うための表図である。
【図１０】本発明者が先に提案したＴＣＰ２のプロトコルスタックを示す図である。
【符号の説明】
【０１３０】
１００…中継装置、２００，３００…ネットワーク、１ａ，１ｂ…ＮＩＣドライバ、２０…アプリケーション解析機能、３０…ＴＣＰ２、４０…外部回路

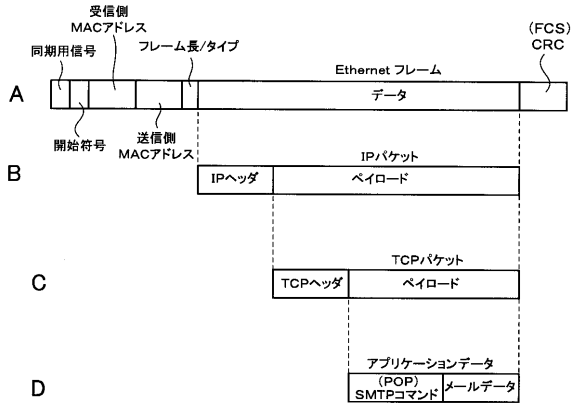
【図１】



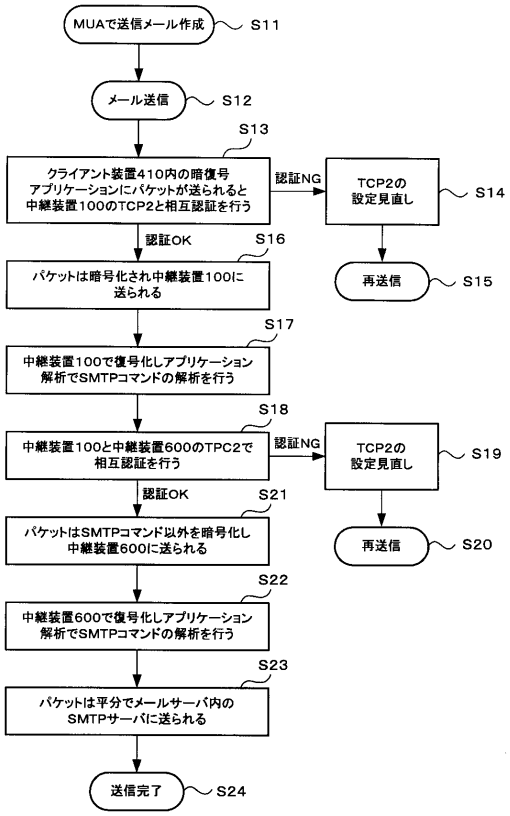
【図２】



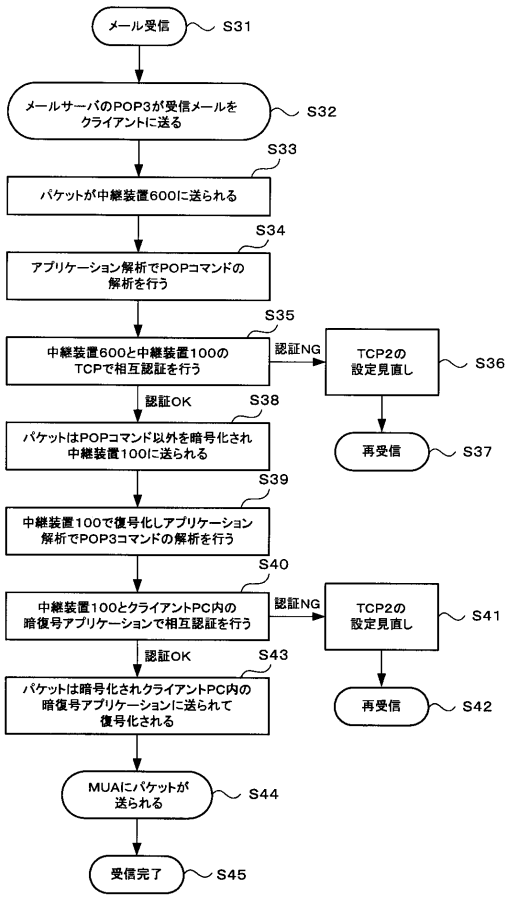
【図３】



【図４】



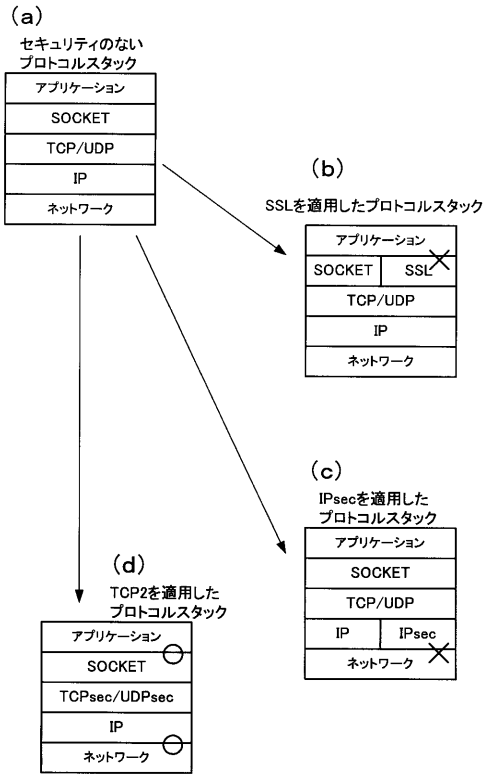
【図５】



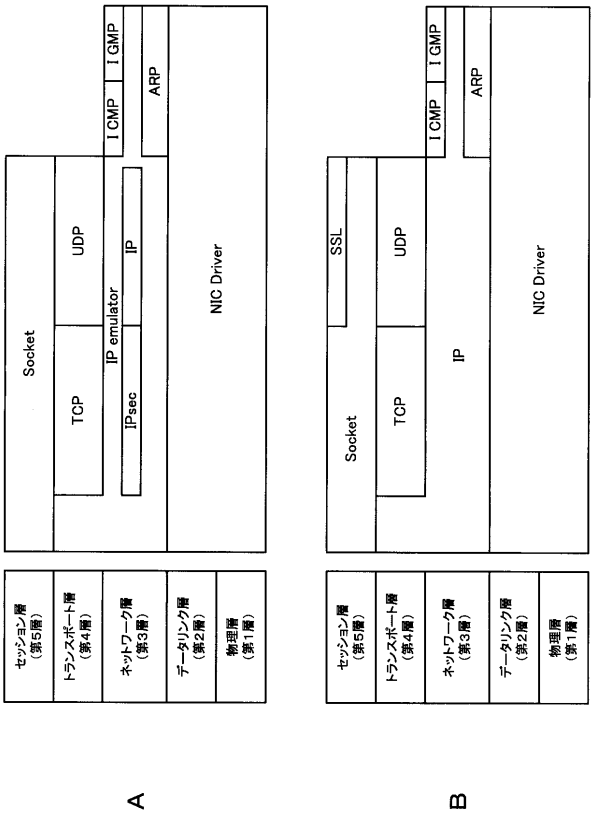
【図６】

	IPsec		SSL		TCP2	
(1)クライアント-クライアント間の通信	○	直接通信可。	×	直接通信不可。特別なサーバを介して通信することは可。	○	直接通信可。
(2)PPPモバイル環境 (3)ADSL環境	△	XAUTHを利用することで可能。但し、セキュリティ上で問題あり。	○	通信可。	○	通信可。
(4)NAT、IPマスカレード環境	△	NAT-Tと併用することで実現可。	○	通信可。	○	通信可。
(5)TCP/IPプロトコルスタック～のDoS攻撃	○	DoS攻撃への対応可。	×	対応不可。	○	DoS攻撃への対応可。
(6)劣悪な通信環境化(物理ノイズが多く通信エラーが多発する環境)	×	対応が不十分。スループットの低下を招く。	○	対応可。	○	対応可。
(7)異なったLAN間の通信	△	サブネットアドレスが同一アドレスの場合、通信不可。	○	通信可。	○	通信可。
(8)異なったネットワーク環境	△	管理が大変で困難。	○	管理の簡素化が可能。	○	管理の簡素化が可能。
(9)全てのUDPポートのセキュアな通信	○	セキュアな通信が可能。	×	通信不可。	○	通信可。
(10)全てのTCPポートのセキュアな通信	○	セキュアな通信が可能。	×	特定のTCPポート以外は通信不可。	○	通信可。
(11)アプリケーションでの制限	○	影響なし。	×	ソケットプログラムの変更が必要。	○	ソケットプログラムの部分をそのまま使用することが可能。
(12)アクセス単位		IP単位		リソース単位(URL単位、フォルダー単位)		PORT単位、セッション単位。
(13)MTU(最大セグメントサイズ)	△	調整が必要。	○	MTUを意識することなく通信可。	○	意識なく通信可。
(14)モバイル環境下で、VoIPを使ったインターネット電話	△	XAUTHを利用することで可能。但し、セキュリティ上で問題あり。	×	使用不可。	○	使用可。
(15)ADSL環境下で、VoIPを使ったインターネット電話	△	XAUTHを利用することで可能。但し、セキュリティ上で問題あり。	×	使用不可。	○	使用可。
(16)異なったLAN間で、VoIPを使ったインターネット電話	△	NAT-T、IPsec-DHCPを使用することで実現可。	×	使用不可。	○	使用可。
(17)複数キャリアLAN間で、VoIPを使ったインターネット電話	×	通信不可。	×	使用不可。	○	使用可。

【図７】



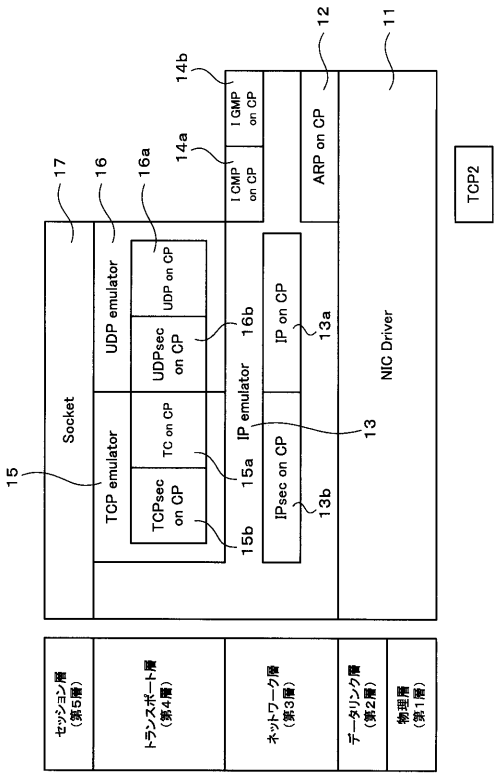
【図８】



【図９】

	IPsec		SSL	
(1)クライアント-クライアント間の通信	○	直接通信可	×	直接通信不可。特別なサーバを介して通信することは可。
(2)PPPモバイル環境	△	XAUTHを利用することで可能。但し、セキュリティ上で問題あり。	○	通信可。
(3)ADSL環境				
(4)NAT、IPマスカレード環境	△	NAT-Tと併用することで実現可。	○	通信可。
(5)TCP/IPプロトコルスタックへのDoS攻撃	○	DoS攻撃への対応可。	×	対応不可。
(6)劣悪な通信環境化(物理ノイズが多く通信エラーが多発する環境)	×	対応が不十分。スループットの低下を招く。	○	対応可。
(7)異なったLAN間の通信	△	サブネットアドレスが同一アドレスの場合、通信不可。	○	通信可。
(8)異なったネットワーク環境	△	管理が大変で困難。	○	管理の簡素化が可能。
(9)全てのUDPポートのセキュアな通信	○	セキュアな通信が可能。	×	通信不可。
(10)全てのTCPポートのセキュアな通信	○	セキュアな通信が可能。	×	特定のTCPポート以外は通信不可。
(11)アプリケーションでの制限	○	影響なし。	×	ソケットプログラムの変更が必要。
(12)アクセス単位		IP単位。		リソース単位(URL単位、フォルダー単位)
(13)MTU(最大セグメントサイズ)	△	調整が必要。	○	MTUを意識することなく通信可。
(14)モバイル環境下で、VoIPを使ったインターネット電話	△	XAUTHを利用することで可能。但し、セキュリティ上で問題あり。	×	使用不可。
(15)ADSL環境下で、VoIPを使ったインターネット電話	△	XAUTHを利用することで可能。但し、セキュリティ上で問題あり。	×	使用不可。
(16)異なったLAN間で、VoIPを使ったインターネット電話	△	NAT-T、IPsec-DHCPを使用することで実現可。	×	使用不可。
(17)複数キャリアLAN間で、VoIPを使ったインターネット電話	×	通信不可。	×	使用不可。

【図１０】



フロントページの続き

(72)発明者　小川　恵子
大阪府大阪市北区東天満１丁目１番１９号　アーバンエース東天満ビル　ティー・ティー・ティー株式会社内

Ｆターム(参考) 5J104 AA01 AA32 BA02 JA03 NA02 NA27 NA37 PA08
5K030 GA15 HA06 HC01 LD19