(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2005-45473
(P2005-45473A)
(43)公開日　平成17年2月17日(2005.2.17)

(51)Int.Cl.[7]	F I		テーマコード（参考）
H04L 12/56	H04L 12/56	H	5J104
H04L 9/10	H04L 9/00	621A	5K030

審査請求 有　請求項の数 1　OL　（全 6 頁）

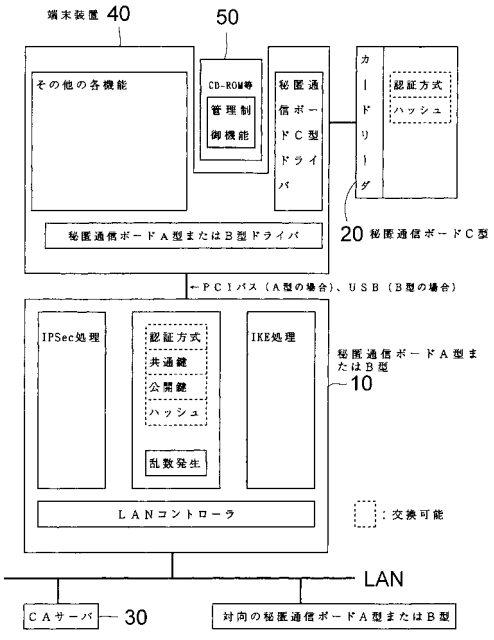
(21)出願番号　特願2003-202199(P2003-202199)
(22)出願日　平成15年7月28日(2003.7.28)

(71)出願人　390014306
防衛庁技術研究本部長
東京都新宿区市谷本村町５番１号
(74)代理人　100079290
弁理士　村井　隆
(72)発明者　加瀬　正勝
埼玉県春日部市大枝５９１－８
(72)発明者　武田　仁己
東京都新宿区大久保３－１２－２－５０８
(72)発明者　佐藤　史生
東京都目黒区大岡山１－３１－３５　細川アパート１０１
(72)発明者　櫻井　宗晃
東京都目黒区中目黒２－２－２１　Ａ－３０４

最終頁に続く

(54)【発明の名称】秘匿通信制御装置

(57)【要約】
【課題】ネットワーク上での情報漏洩、改竄等を防ぐことを目的として、クライアント～サーバ間及びサーバ～サーバ間でのＶＰＮ（Ｖｉｒｔｕａｌ　Ｐｒｉｖａｔｅ　Ｎｅｔｗｏｒｋ）を構築するための秘匿通信手段を提供する。
【解決手段】ＩＰＳｅｃに基づいて秘匿通信を実施する機能、秘匿通信に先立ち認証・鍵交換を実施する機能、暗号等のアルゴリズム等を任意に設定、変更できる機能、及び公開鍵暗号を使用する際の暗号鍵及び公開鍵証明書の作成機能を、全て秘匿通信ボード１０上で処理できる秘匿通信制御装置によって、ネットワーク上での情報漏洩、改竄等を防ぐ手段を確保する。
【選択図】　図１



【特許請求の範囲】
【請求項１】
サーバにＬＡＮで接続される端末に、又はサーバに装着されるＯＳ搭載ＬＡＮボードを備え、該ＬＡＮボードには暗号処理用のプロセッサが搭載されていて、ＩＰＳｅｃによる秘匿・鍵交換で必要となる処理エンジンが、前記端末又は前記サーバから設定できて、任意の秘匿・鍵交換方式に交換可能であり、かつＩＰＳｅｃの全過程を前記ＯＳ搭載ＬＡＮボード上で一括処理することを特徴とする秘匿通信制御装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、インターネットのようなＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）通信に用いる秘匿通信制御装置に係り、とくにＬＡＮ通信において、ネットワーク上での情報漏洩・改竄等を防ぐことを目的として、クライアント（サーバに接続される端末）～サーバ間、サーバ～サーバ間、及びクライアント～クライアント間での第三者の盗聴を防ぐＶＰＮ（仮想専用通信網）を構築するための、秘匿通信技術に関するものである。
【０００２】
【従来の技術】
従来、クライアントとして用いるパーソナルコンピュータやサーバに装着される拡張ボートとしての暗号ボードは、あらかじめ暗号ボード内に搭載された複数の暗号方式（認証及び鍵交換機能を含む）の中からのみ選択利用できる方式である。
【０００３】
また、従来ＩＰＳｅｃ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃａｌ　Ｓｅｃｕｒｉｔｙ）通信では、暗号化処理のみをホストコンピュータ（ＬＡＮボードを組み込んでＩＰＳｅｃ通信を行うコンピュータ）側で実行するものが主流であり、同一バス上を暗号化されていない平文データと暗号文データが混在して伝送されていた。
【０００４】
【発明が解決しようとする課題】
現在の暗号ボードでは、製造者があらかじめ搭載した暗号方式のなかからのみ選択利用するため、利用者がそれぞれの必要性に応じた方式を実装して使用することはできなかった。
【０００５】
また、平文と暗号文が同一バス上に混在するのは、平文がそのまま外部へ送信される可能性があり、第三者に情報が漏洩する可能性が残り、脅威となる。
【０００６】
本発明は、上記の点に鑑み、利用者側がそれぞれの必要性に応じて任意の暗号方式を実装し、選択利用できるようにし、かつＩＰＳｅｃの全過程をＬＡＮボード上で一括処理可能として平文データがクライアント～サーバ間、及びサーバ～サーバ間で伝送されないようにした秘匿通信制御装置を提供することを目的とする。
【０００７】
本発明のその他の目的や新規な特徴は後述の実施の形態において明らかにする。
【０００８】
【課題を解決するための手段】
上記目的を達成するために、本発明に係る秘匿通信制御装置は、サーバにＬＡＮで接続される端末に、又はサーバに装着されるＯＳ搭載ＬＡＮボードを備え、該ＬＡＮボードには暗号処理用のプロセッサが搭載されていて、ＩＰＳｅｃによる秘匿・鍵交換で必要となる処理エンジンが、前記端末又は前記サーバから設定できて、任意の秘匿・鍵交換方式に交換可能であり、かつＩＰＳｅｃの全過程を前記ＯＳ搭載ＬＡＮボード上で一括処理することを特徴としている。
【０００９】
【発明の実施の形態】

以下、本発明に係る秘匿通信制御装置の実施の形態を図面に従って説明する。

【００１０】

図１は本発明に係る秘匿通信制御装置の実施の形態であって、全体の機能構成図、図２はＩＰＳｅｃによる秘匿・鍵交換等で必要となるポリシーやアルゴリズムの設定、変更の概略処理フロー図である。

【００１１】

これらの図において、秘匿通信制御装置は、秘匿通信ボードＡ型又はＢ型１０、秘匿通信ボードＣ型２０、及びＣＡサーバ（ＣＡ：Ｃｅｒｔｉｆｉｃａｔｅ Ａｕｔｈｏｒｉｔｙ、認証局）３０から構成される。なお、ＩＫＥ（ＩＰＳｅｃにおける鍵交換の規定）で事前鍵配布による認証を選択した場合、ＣＡサーバは必要ない。

【００１２】

秘匿通信ボードＡ型又はＢ型１０は、端末装置４０（クライアント又はサーバ）に接続されるＯＳ搭載ＬＡＮボードであり、ＩＰＳｅｃ処理及びＩＫＥ（ＩＰＳｅｃにおける鍵交換の規定）処理のためのプロセッサ、及びＬＡＮコントローラが搭載され、図中点線枠で囲んだように、暗号方式［認証方式、共通鍵、公開鍵、及びハッシュ（圧縮方法）］の任意交換機能を有する。また、暗号化のための乱数発生機能を有する。なお、秘匿通信ボードＡ型はＰＣＩバスを通じて、Ｂ型はＵＳＢを通じて前記端末装置４０に接続されるようになっている。

【００１３】

秘匿通信ボードＣ型２０は、カードリーダを備えていて、ＩＣインターフェイスを通じて端末装置４０に接続され、図中点線枠で囲んだように、認証方式及びハッシュの任意交換機能を有する。

【００１４】

ＣＡサーバ３０は公開鍵に関する情報管理を行うものである。

【００１５】

端末装置４０は、例えば一般的なパーソナルコンピュータとしての機能を有し、拡張ボートに対するドライバ、すなわち秘匿通信ボードＡ型又はＢ型ドライバ、秘匿通信ボードＣ型ドライバを備えている。

【００１６】

ここでは、各端末装置４０の利用者とは別に暗号設定管理者をおいた例で、図２の暗号方式等の設定及び交換の概略処理フローを以下に説明する。

【００１７】

一般に暗号及び認証を利用する場合、秘密にすべき設定情報を管理するため、利用者の他に暗号設定管理者をおく。本実施の形態では、暗号設定管理者を搭載される暗号方式や秘密にすべき設定情報の責任者と位置付けている。

【００１８】

暗号設定管理者は、最初に管理者専用端末（ＰＣ）を決め、秘匿通信ボードＡ型又はＢ型１０及び秘匿通信ボードＣ型２０用のドライバプログラムをインストールする。

【００１９】

暗号設定管理者は設定を行う秘匿通信ボードＡ型又はＢ型１０及び秘匿通信ボードＣ型２０を管理者専用端末に接続し、管理制御プログラム（ＣＤ－ＲＯＭ等の記憶媒体）５０を起動させ、設定を実施する。図２にこの設定及び交換の概略処理フローを示している。なお、管理者専用端末は、秘匿通信ボードＡ型又はＢ型１０及び秘匿通信ボードＣ型２０の設定のために使用される際には、必ずしもＬＡＮに接続された状態となっている必要はない。

【００２０】

暗号設定管理者はＩＰＳｅｃ及びＩＫＥにて用いる暗号方式等を、図２のフロッピーディスク（「フロッピー」は登録商標）等の記憶媒体６０に記録（プログラミング及び保存）する。

【００２１】

前記記憶媒体６０に記録されている暗号方式等（図中点線枠で囲われた認証方式、共通鍵、公開鍵、ハッシュに対応する）を、秘匿通信ボードＡ型又はＢ型１０に読み込む。換言すれば、ＩＰＳｅｃによる秘匿（暗号化、復号）・鍵交換を実現するためのソフトウエアである所定の処理エンジンが秘匿通信ボードＡ型又はＢ型１０に設定（実装）される。

【００２２】

同様に記憶媒体６０に記録されている認証方式、ハッシュをＣ型に読み込む。各方式は複数個同時に読み込むこともできる。

【００２３】

各アルゴリズムの設定が終了した秘匿通信ボードＡ型又はＢ型１０及びＣ型２０を各端末装置４０を利用者に配布する。

【００２４】

設定の変更を行う場合は、暗号設定管理者が利用者の各ボードを回収し、再度設定をし直す。

【００２５】

この実施の形態では、インターネット通信インターフェイスとなるＬＡＮボードとして用いる秘匿通信ボードＡ型又はＢ型１０上に暗号処理用のプロセッサを搭載し、暗号ソフトの取扱を容易にするため汎用ＯＳを実装したＯＳ搭載型ＬＡＮボードとすることによって、利用者がそれぞれの必要性に応じて任意の暗号方式を実装し、選択利用できる。また、汎用ＯＳを前記ボードに実装することにより、暗号方式のソフトウェアの開発は、特殊な開発環境を利用することなく、汎用の開発環境を活用できる。例えば、秘匿通信において暗号・鍵交換等のポリシーやアルゴリズムを暗号設定管理者がプログラムし、秘匿通信制御装置（ＯＳ搭載ＬＡＮボードである秘匿通信ボードＡ型又はＢ型１０）上のＯＳを利用して任意に設定、変更することで、従来製品と比較してより幅広い暗号方式等の利用が可能となる。

【００２６】

また、利用者端末装置の不正操作により、暗号化処理を不正に無効化したり、不適切な設定状態での運用を未然に防ぐため、暗号化処理を前記ボード上のみで実行することとして設計し、ＩＰＳｅｃに係る全過程は全て前記ボードで処理される構成としている。すなわち、ＩＰＳｅｃに基づいて秘匿通信を実施する機能、秘匿通信に先立ち認証・鍵交換を実施する機能、暗号等のアルゴリズム等を任意に設定・変更できる機能、及び公開鍵暗号を使用する際の暗号鍵及び公開鍵証明書の作成機能を、全て秘匿通信ボード１０上で処理できる。このような構成とすることにより、前述の課題（利用者が任意の暗号方式を選択できない問題及び平文が外部へ送信される可能性がある問題）を解決できる。また、ホストコンピュータ側にかける負担が軽減される。

【００２７】

また、この場合、パケット毎に暗号化するＩＰＳｅｃを用いたＩＫＥプロトコルを採用して、既存の暗号処理装置との互換性を確保するだけでなく、利用者端末装置に暗号処理の負担を与えないため端末装置の処理速度を低下させることなく、さらに利用者は通信時に秘匿処理を全く意識する必要がなくなると言う利点がある。

【００２８】

また、別の利便性として、ＩＰＳｅｃを用いたＩＫＥプロトコルを使うことにより、記憶媒体から秘匿通信ボードＡ型又はＢ型に読み込んだ複数方式の中から必要に応じた方式を、通信相手先のＩＰアドレス毎に自動的に選択することができる。

【００２９】

以上本発明の実施の形態について説明してきたが、本発明はこれに限定されることなく請求項の記載の範囲内において各種の変形、変更が可能なことは当業者には自明であろう。

【００３０】

【発明の効果】

以上説明したように、本発明に係る秘匿通信制御装置は、サーバにＬＡＮで接続される端末に、又はサーバに装着されるＯＳ搭載ＬＡＮボードを備え、該ＬＡＮボードには暗号処

理用のプロセッサが搭載されていて、ＩＰＳｅｃによる秘匿・鍵交換で必要となる処理エンジンが、前記端末又は前記サーバから設定できて、任意の秘匿・鍵交換方式に交換可能であり、かつＩＰＳｅｃの全過程を前記ＯＳ搭載ＬＡＮボード上で一括処理する。このため、任意の秘匿・鍵交換方式を選択可能であり、従来製品と比較してより幅広い暗号方式等の利用が可能になる。また、本発明において、ＩＰＳｅｃに係る全過程は全て秘匿通信制御装置上で処理されるので、ホストコンピュータ側にかける負担が軽減され、かつ平文と暗号文がコンピュータ内部の同一バス上で混在することが無いため、暗号が解析されるという危険性が無くなり、また平文データがクライアント～サーバ間、及びサーバ～サーバ間で伝送されることはなくなり、第三者への情報の漏洩を防止可能であり、利用者は秘匿に関して一切意識することなく通信ができるという利便性がある。

【図面の簡単な説明】

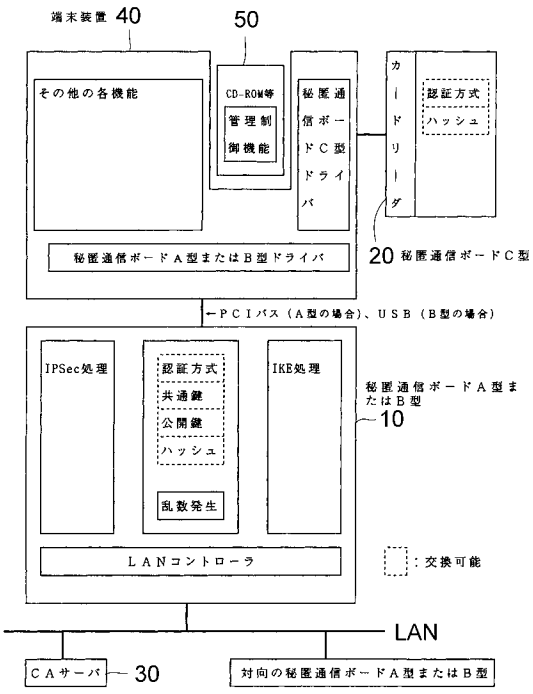
【図１】本発明に係る秘匿通信制御装置の実施の形態であって、全体の機能構成図である。

【図２】図１の構成における暗号方式等のポリシーやアルゴリズムの設定、変更の概略処理フロー図である。

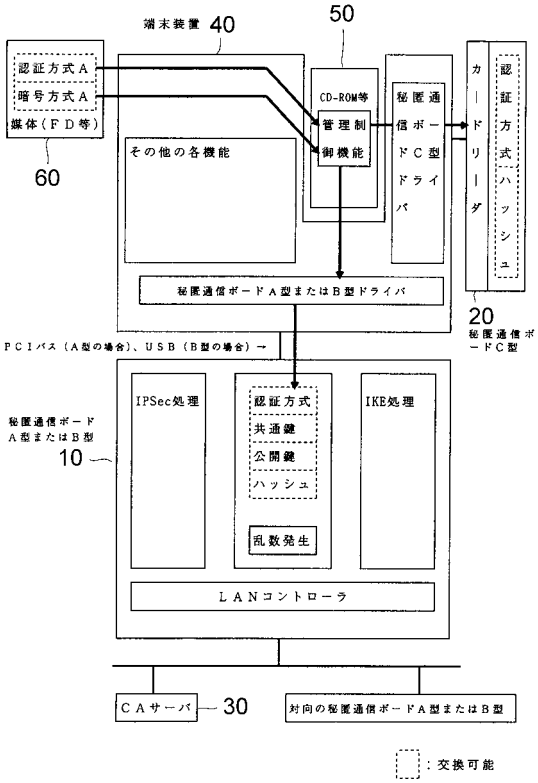
【符号の説明】

１０　秘匿通信ボードＡ型又はＢ型
２０　秘匿通信ボードＣ型
３０　ＣＡサーバ
４０　端末装置
５０　管理制御プログラム
６０　記録媒体

【図１】



【図２】



フロントページの続き

(72)発明者　數納　勝彦
東京都豊島区高松３－４－１６　パインヒルズ２０６号

Ｆターム(参考) 5J104 NA41 NA42 NA43
5K030 GA15 HC14 JA07 KA13 LD19