

(51)Int.Cl.

F I

H 0 4 L 12/22 (2006.01)

H 0 4 L 12/22

H 0 4 L 12/56 (2006.01)

H 0 4 L 12/56 H

H 0 4 L 9/10 (2006.01)

H 0 4 L 9/00 6 2 1 A

請求項の数1 (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)  
 (65)公開番号 特開2005-045473(P2005-45473A)  
 (43)公開日 平成17年2月17日(2005.2.17)  
 審査請求日 平成15年7月28日(2003.7.28)

(73)特許権者 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-3  
 04

最終頁に続く

(54)【発明の名称】秘匿通信制御装置

(57)【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ポ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。

## 【 0 0 0 3 】

また、従来 I P S e c ( Internet Protocal Security ) 通信では、暗号化処理のみをホストコンピュータ ( L A N ボードを組み込んで I P S e c 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。

## 【 0 0 0 4 】

## 【 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。

10

## 【 0 0 0 5 】

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。

## 【 0 0 0 6 】

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 I P S e c の全過程を L A N 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。

## 【 0 0 0 7 】

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。

20

## 【 0 0 0 8 】

## 【 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 L A N で接続される端末に、又はサーバに装着される O S 搭載 L A N ボードを備え、該 L A N ボードには暗号処理用のプロセッサが搭載されていて、I P S e c 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 I P S e c の全過程を前記 O S 搭載 L A N ボード上で一括処理することを特徴としている。

## 【 0 0 0 9 】

## 【 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。

30

## 【 0 0 1 0 】

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 I P S e c 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。

## 【 0 0 1 1 】

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 1 0、秘匿通信ボード C 型 2 0、及び C A サーバ ( C A : Certificate Authority、認証局 ) 3 0 から構成される。なお、I K E ( I P S e c 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、C A サーバは必要ない。

40

## 【 0 0 1 2 】

秘匿通信ボード A 型又は B 型 1 0 は、端末装置 4 0 ( クライアント又はサーバ ) に接続される O S 搭載 L A N ボードであり、I P S e c 処理及び I K E ( I P S e c における鍵交換の規定 ) 処理のためのプロセッサ、及び L A N 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 P C I バスを通じて、B 型は U S B を通じて前記端末装置 4 0 に接続されるようになっている。

## 【 0 0 1 3 】

秘匿通信ボード C 型 2 0 は、カードリーダーを備えていて、I C インターフェイスを通じて

50

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。

【 0 0 1 4 】

C A サーバ 30 は公開鍵に関する情報管理を行うものである。

【 0 0 1 5 】

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、拡張ポ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。

【 0 0 1 6 】

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。 10

【 0 0 1 7 】

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。

【 0 0 1 8 】

暗号設定管理者は、最初に管理者専用端末 ( P C ) 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。

【 0 0 1 9 】

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 ( C D - R O M 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 L A N に接続された状態となっている必要はない。 20

【 0 0 2 0 】

暗号設定管理者は I P S e c 及び I K E 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。

【 0 0 2 1 】

前記憶媒体 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、I P S e c 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ェ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。 30

【 0 0 2 2 】

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。

【 0 0 2 3 】

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。 40

【 0 0 2 4 】

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。

【 0 0 2 5 】

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 L A N 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 O S を実装した O S 搭載型 L A N 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 O S 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 50

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かる負担が軽減される。

10

【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。

20

【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、変更が可能なの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かる負担が軽減され、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。

30

40

【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。

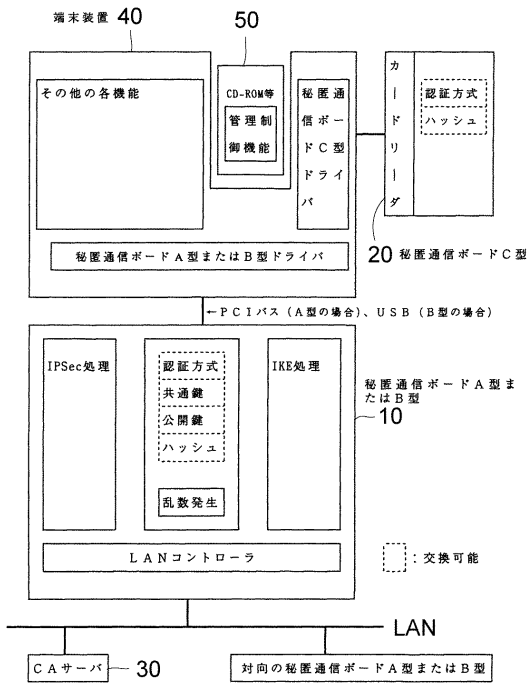
【符号の説明】

- 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

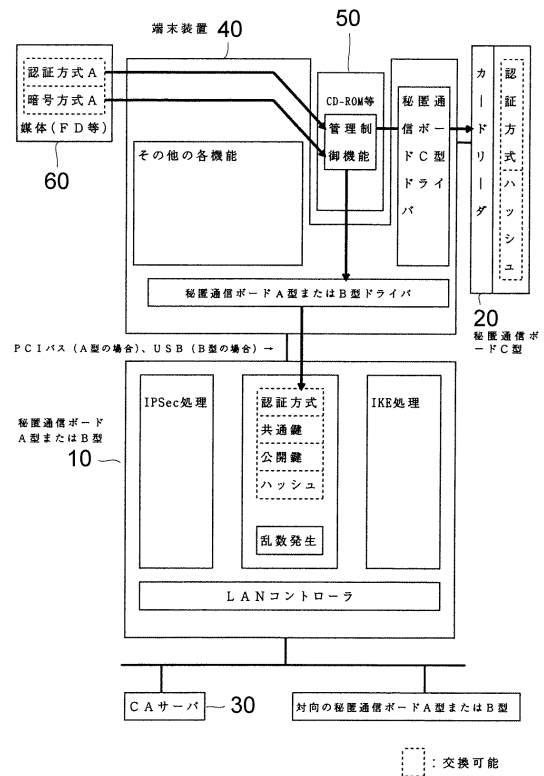
50

- 5 0 管理制御プログラム
- 6 0 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

審査官 中元 淳二

(56)参考文献 LANボード, 2001年11月13日, URL, <http://www.express.nec.co.jp/teci/tecbook-pdf/tb020122/lan.pdf>

梶崎浩嗣, 黒川恭一, 暗号処理ボードSEBSW-2の設計と性能評価, 電子情報処理学会技術研究報告, 2003年1月21日, Vol.102, No.610, pp.19-24, VLD2002-123, CPSY2002-76

(58)調査した分野(Int.Cl., DB名)

H04L 12/22

H04L 12/56

H04L 9/10